

**IBM Intelligent Operations Center**



**IBM Intelligent Operations Center  
製品資料**

*バージョン1 リリース5*



**IBM Intelligent Operations Center**



**IBM Intelligent Operations Center  
製品資料**

*バージョン1 リリース5*

**お願い**

本書および本書で紹介する製品をご使用になる前に、397 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM Intelligent Operations Center バージョン 1 リリース 5 モディフィケーション 0 に適用されます。本書は、新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

**原典：** IBM Intelligent Operations Center  
IBM Intelligent Operations Center  
Product Documentation  
Version 1 Release 5

**発行：** 日本アイ・ビー・エム株式会社

**担当：** トランスレーション・サービス・センター

第1刷 2013.5

© Copyright IBM Corporation 2011, 2012.

# 目次

図	vii
---	-----

## 第 1 章 ソリューションの概要 . . . . . 1

対象読者	2
機能	2
ユーザーおよび利点	4
コンポーネント	6
イベント管理	8
バージョン 1.5 の新機能	9
ユーザーのための新機能	9
管理者のための新機能	10

## 第 2 章 インストールおよび構成 . . . . . 13

インストールの準備	13
IBM Intelligent Operations Center システム・サービス	13
IBM Intelligent Operations Center ハードウェア要件	14
前提ソフトウェア要件	15
サポートされるブラウザ	15
メディアのパッケージ化	16
インストール・チェックリスト	16
チェックリスト - IBM Installation Manager を使用したインストール	16
チェックリスト - ステップ・バイ・ステップでインストール	18
サーバーの準備	20
TCP/IP ネットワーキング	24
インストール・サーバーへのインストール・パッケージのコピー	28
Java ランタイム環境のインストール	29
Installation Manager を使用した IBM Intelligent Operations Center のインストール	30
インストール・コンポーネント	34
構成オプション	35
Installation Manager を使用したインストールの再開	38
IBM Intelligent Operations Center のステップ・バイ・ステップでインストール	39
インストール・パッケージの準備	39
インストール・スクリプトの検証	40
インストール・プロパティのカスタマイズ	40
インストール・トポロジー・ファイル	41
事前検査ツールの実行	48
Linux セキュリティー設定	49
installTopology コマンド	50
IBM Intelligent Operations Center のコンポーネントのインストール用オプション	51
ステップ・バイ・ステップでインストール中の IBM Intelligent Operations Center アーキテクチャーのインストールの再開	55

プラットフォーム制御ツールのインストール	55
システム検査チェック・ツールのインストール	56
IBM Intelligent Operations Center アプリケーションのインストール	57
インストールの検証	58
インストール後の IBM Intelligent Operations Center の構成	59
IPv6 用のコラボレーション・サービスの構成	59
コラボレーション・サービス用のシングル・サインオンの構成	60
セッション・タイムアウトの設定	61
Semantic Model Services のインストールおよび構成	62
プラットフォーム制御ツールの構成	67
Tivoli Service Request Manager 管理パスワードの暗号化	68
EventProcessor のスレッドの最小数の設定	69
Default および WebContainer スレッド・プール・サイズの変更	69
Cyber Hygiene のステップ・バイ・ステップでインストールと実行	70
Linux オペレーティング・システムへの変更	72
Cyber Hygiene ログの確認	72
リモートの root ログオンの再有効化	73
ssh アクセスを必要とするユーザーの構成	74
ソリューションに付属するツールのインストール	74
サンプル・ユーザーの削除	75
実動システムからのインストール・サービスの削除	76

## 第 3 章 ソリューションの保護 . . . . . 77

ユーザーの役割とアクセス権	78
サンプル・ユーザー	80
ユーザー役割グループと許可権限	81
ユーザー・カテゴリ・グループとデータ権限	83
ユーザーまたはグループの追加	84
グループ・メンバーシップの表示または変更	86
ユーザー・プロファイルの表示または編集	87
ユーザーまたはグループの削除	87
ユーザーおよびグループのインポート	88
ユーザー権限サマリー	90
Cyber Hygiene の概要	91
サイバー・セキュリティ	92
Cyber Hygiene のチェックリスト	93
Cyber Hygiene のデフォルト構成	95
修復ツール	99
Cyber Hygiene の資料	100

## 第 4 章 ソリューションの統合 . . . . . 101

統合できるシステムの例	101
統合点とプロトコル	101
イベントと KPI	101

共通アラート・プロトコルとの統合	103
パブリッシャー・サービスを使用したイベントの作成	112
テスト・イベントの作成およびパブリッシュ	115
サンプル・パブリッシャー	115
イベント・スクリプト記述	120
KPI の作成および統合	123
モニター・モデルと KPI	124
モニター・コンテキスト・インスタンス	125
KPI のモデル化	125
KPI 階層の定義	128
OWL を使用した KPI 階層の定義	129
IBM WebSphere Business Monitor と IBM Intelligent Operations Center の間の KPI イベント通信	130
モニター・モデルのデプロイ	134
KPI 表示値	134
KPI のキャッシュ	136
サンプル KPI	136
Tivoli Service Request Manager の構成	138
Tivoli Service Request Manager ユーザー・インターフェースの使用	139
Tivoli Service Request Manager での新規ユーザーの構成	141
標準操作手順	143
リソースの管理	148
標準操作手順、ワークフロー、およびリソースのサンプル	154

## 第 5 章 ソリューションのカスタマイズ 157

ユーザー・インターフェースのカスタマイズ	157
ユーザー・インターフェースのローカライズ	157
ポートレットのリスト	157
ページの作成またはカスタマイズ	161
ポートレットのカスタマイズ	162
ポートレット・ヘルプのカスタマイズ	183
ポートレット・ヘルプ・ファイルのロケーション	184
KPI のカスタマイズ	185
重要業績評価指標	186
KPI をカスタマイズする前にバックアップする	190
イベント関連のカスタマイズ	191
イベント関連およびルール・アプリケーション	191
イベント関連設定のカスタマイズ	192
ロケーション・マップ・マネージャー	195
マップ・メニューへの種別の追加	195
ポートレットへのマップの追加	195
ロケーション・マップのエリアの追加または変更	196
「ロケーション・マップ・マネージャー」ポートレットのカスタマイズ	196
システム全体の構成データの指定	197
システム・プロパティ・テーブルの更新	202
レポートを作成するための IBM Cognos Business Intelligence の構成	203
「レポート」ポートレットの作成	203
「レポート」ポートレットのレイアウトの編集	204

レポートを表示するためのポートレットのカスタマイズ	204
レポート URL の検索	205
データ・モデルの操作	205

## 第 6 章 ソリューションの管理 215

製品情報	215
サービスの制御	216
サービスの開始	216
Tivoli Netcool/OMNIBus プローブの開始と停止	219
サービスの停止	219
サービス状況の照会	222
プラットフォーム制御ツールのヘルプの入手	223
管理コンソール	224
サービスの管理	226
コンポーネントの検証	232
システム検査チェック・ツールの使用方法	232
システム検査チェック・テスト	233

## 第 7 章 ソリューションの保守 287

データのバックアップ	287
パフォーマンスの調整	288
アプリケーション・サーバーの調整	289
WebSphere Application Server の調整	289
ログ・ファイルの管理	289
シングル・サインオンのための LTPA トークンの更新	289
保守のヒント	292

## 第 8 章 ソリューション・インターフェースの使用 293

ログオン	293
ログオフ	294
ユーザー・プロファイルの表示または編集	294
ページの使用	295
「スーパーバイザー: 状況」ビュー	295
「スーパーバイザー: 操作」ビュー	296
「オペレーター: 操作」ビュー	297
スーパーバイザー: レポート	298
オペレーター: レポート	299
「ロケーション・マップ」ビュー	299
ポートレットの使用	299
連絡先	300
詳細	301
イベントとインシデントの管理	303
リソースの管理	303
「詳細」ポートレットのカスタマイズ	304
重要業績評価指標のドリルダウン	304
ロケーション・マップ	305
マップ・コントロール	307
マップのイベント・カテゴリーの選択	307
「ロケーション・マップ」ポートレットのカスタマイズ	308
マップ	309
マップ・コントロールの使用	310
マップのイベント・カテゴリーの選択	311

マップのリソースの機能の選択	311
マップのリセット	312
イベントの追加	312
「マップ」ポートレットのカスタマイズ	313
マイ・アクティビティー	314
通知	316
レポート	318
状況	321
<b>第 9 章 トラブルシューティングとサポート</b>	<b>323</b>
問題のトラブルシューティング手法	323
トレースの使用可能化およびログ・ファイルの表示	325
アプリケーション・サーバーのログ・ファイル	325
イベント・サーバーのログ・ファイル	326
インストール収集必須ツールの実行	330
コンポーネントのトラブルシューティング	331
IBM Support Assistant Lite のインストールと使用	334
IBM Intelligent Operations Center のメッセージ	335
知識ベースおよび IBM サポートの使用	355
知識ベースの検索	355
Fix Central からのフィックスの入手	356
IBM サポートへの連絡	357
サポート更新情報のサブスクリプション	358
IBM との情報の交換	360
既知の問題および解決策	361
IBM Intelligent Operations Center インストール時の接続エラー	363
IPv6 ネットワーキングが開始されない	363
Tivoli Service Request Manager が開始しない	364
ユーザー・インターフェースの新規ページを作成できない	364
ポートレットのアクセシビリティに関する回避策	365
「レポート」ポートレットで日付を選択するためのアクセシビリティの対処法	365
「詳細」ポートレットで新規イベントが表示されない	366
認証メカニズムが使用できない	368
サード・パーティー・サーバーが応答していません	369
「マイ・アクティビティー」ポートレットでアクティビティーが表示されない	369
サンプル・データを使用したトラブルシューティング	369
Tivoli Service Request Manager の状況の検証	370
ユーザー権限の検証	371
ワークフローと標準操作手順の関連付けの検証	372
ログ・ファイルの確認	373

「状況」ポートレットまたは「重要業績評価指標のドリルダウン」ポートレットに KPI データが表示されない	373
「状況」ポートレットまたは「重要業績評価指標のドリルダウン」ポートレットでイベントが更新されない	374

## 第 10 章 リファレンス . . . . . 377

IBM Intelligent Operations Center に組み込まれている製品およびコンポーネント	377
root アカウントで実行されるプロセス	378
Cyber Hygiene の例外	380
システム管理者の評価を必要とするファイル権限	380
製品およびコンポーネントのセキュリティ認証	381
PDF ライブラリー	383
用語集	383
A	383
B	384
C	384
D	385
E	386
F	386
G	386
H	387
I	387
J	387
K	388
L	388
M	389
N	389
O	389
P	390
R	390
S	391
T	391
U	392
V	393
W	393
X	393
製品に関する追加情報	394
著作権表示および商標	395
著作権表示	395
商標	396
<b>特記事項</b>	<b>397</b>
商標	398
<b>索引</b>	<b>401</b>









---

## 第 1 章 ソリューションの概要

多くの組織や事業体では、業務の効率的な監視と調整が必要になります。すべての組織や事業体に共通するのは、適切な要員が迅速で正確な決定を行い、その決定の効果を追跡できるように、正しい情報を収集する必要があるということです。IBM® Intelligent Operations Center は、業務の効率的な監督と調整を促進するために設計されたソフトウェア・ソリューションです。

組織は、中核システムや、相互接続されているシステムの改善について共通の課題に直面しています。先見の明のある組織は、よりスマートな中核システムの効率性と有効性の改善を行いたいと思っています。そのような組織はこれらのシステムについて、新しい考え方や使用法を導入しています。高度情報技術を導入することで、組織は振る舞いやイベントのパターンをより適切に把握および予測して、賢明に対処できます。

例えば IBM は、情報技術 (IT) を適用して街のインフラストラクチャーを計画、設計、構築、および運用することで実現される生活の質と経済的福祉の改善の観点からインテリジェント・シティを定義しています。インテリジェント・シティは主に「最新テクノロジー」を指すものではありません。これは、テクノロジーを使用して既存リソースを最も効率的に利用し、市民の生活を改善するための方法を見つけることです。

IBM Intelligent Operations Center は、以下を行うことで、コンピューター・システムによって生成される現実世界のデータの利点を活用します。

- 適切なデータを収集して管理する
- そのデータを統合して分析する
- 情報への簡単かつ時宜を得たアクセスを促進する
- 関連情報を一貫した方法で提供する

このソリューションの利点は、次のとおりです。

- システムを調整し、得られた洞察に基づいて結果を達成する
- 全体的なレポートおよびモニター手法を使用して、計画済みの業務と未計画の業務を最適化する
- コミュニケーションとコラボレーションを促進することで、組織内の複数の領域をまとめる
- イベントを調整することでサービス品質を高め、費用を削減する

業務は個々の領域に分割できます。これらの領域は通常、組織構造と、関係者の専門知識に一致していません。例えば、市当局では輸送、水道、および公共安全などの部門に専門知識を持つ者が配置されます。

ある領域内で業務の複雑性が増すと、より高度にカスタマイズされたソリューションが必要になります。IBM Intelligent Operations Center には多数の異なる統合ポイントが用意されており、これを使用してカスタマイズを行うことができます。これらの統合ポイントと組み込まれているインフラストラクチャーによって、IBM ビジネス・パートナー、サービス・プロバイダー、およびお客様は広範囲にわたる強力なソリューションを柔軟に構築することができます。

---

## 対象読者

このインフォメーション・センターは、IBM Intelligent Operations Center の使用、インストール、管理、および保守を行う担当者を対象としています。また、ソリューションのカスタマイズと、IBM Intelligent Operations Center が必要とする外部基本システムの統合に関する実装資料も含まれています。

このインフォメーション・センターは、ユーザーがこのソリューションに含まれているコンポーネント製品の使用に関する予備知識を持っているか、それらのコンポーネント製品の使用に習熟しているという前提に基づいています。また、このインフォメーション・センターは、ユーザーが Red Hat Enterprise Linux オペレーティング・システムの基本的な知識を持っているという前提にも基づいています。コンポーネント製品やオペレーティング・システムのトレーニングについては、このインフォメーション・センターでは扱っていません。これらの製品のトレーニングが必要な場合は、システム・インテグレーターまたは IBM 担当員に問い合わせ、基本コンポーネントのトレーニング機会に関する情報を入手してください。

『リファレンス』セクションにコンポーネント製品資料へのリンクが記載されています。このトピックの末尾にあるリンクを参照してください。

### 関連概念:

394 ページの『製品に関する追加情報』  
以下の追加リソースは、オンラインで参照できます。

---

## 機能

IBM Intelligent Operations Center には、測定、モニター、およびモデリング機能が備わっており、これらを使用して基本システムを 1 つのソリューションに統合し、業務の効率、計画、および調整を改善できます。

IBM Intelligent Operations Center は、IBM Smarter Cities<sup>®</sup> Software Solutions 製品ファミリー内のソリューションです。IBM Intelligent Operations Center は、既存のハードウェアにインストールすることも (オンプレミス)、クラウドにデプロイすることもできます。IBM Intelligent Operations Center はそれ自体でインストールすることも、IBM Smarter Cities Software Solutions 製品ファミリーから他のソリューションを使用してインストールすることもできます。

IBM Intelligent Operations Center は GUI ベースのソリューションであり、組織や基本となる領域のイベントに役割ベースでアクセスできます。イベント管理、統合されたマッピング、リソース・モニターの各機能が提供されています。このソリューションは、イベントに備えたアクティビティやイベントに応答するアクティビティのための適切な手順やワークフローを提供および追跡することができます。また、効率をさらに高めるための重要業績評価指標 (KPI)、レポート作成、およびコラボレーションの各機能も提供されています。これらの機能によって、組織の上層部は、複数の領域を統合して、協調性と意思決定能力を高めることができます。

## イベントおよびインシデントの管理

IBM Intelligent Operations Center にはイベント・レポート作成と追跡のためのメカニズムが備わっており、これを使用して、基盤となるすべての領域を識別して把握することができます。予測されたイベント、計画されたイベント、および現在のイベントを、それらの進行に沿って管理できます。例えば、道路の下を通っている配管の交換は、水道の運用と交通の運用の双方に関係する、計画されたイベントまたは作業指示書です。今後 24 時間以内に生じる悪天候は、予測されたイベントです。交通渋滞は、道路工事と天気の両方によって影響を受ける現在のイベントです。

統合された地理情報システム (GIS) またはロケーション計画では、イベントが視覚的にマップされるため、対話式のマッピングとシナリオ分析を通じてイベントの影響を測定できます。

## リソース、応答、およびアクティビティ管理

IBM Intelligent Operations Center は、イベントに関連したアクティビティに基づいて適切な手順およびワークフローを格納するためのシステムを提供します。ワークフローの進行状況を追跡したり、自分に割り当てられているアクティビティの状況をモニターしたり更新したりすることができます。

使用可能なリソースの範囲についての情報をマップ上で強調表示できます。いつでも、どこでも、必要に応じて情報に簡単にアクセスできます。

## 状況のモニター

IBM Intelligent Operations Center には、KPI を作成して表示するためのツールが備わっています。基本となるデータの変更に合わせて、KPI を更新できます。このツールを使用して、以下を行うことができます。

- 単一の領域、または複数の領域にわたって、エグゼクティブ・レベルの状況を要約する
- 問題を明らかにし、課題を特定する
- KPI の詳細まで深く掘り下げて、さらなる調査を行う。

## インスタント通知およびインスタント・メッセージ

IBM Intelligent Operations Center には、注意を要する問題に対するアラートを維持できるワークスペースが備わっています。特に、ニュースを知らせる他のポートレットが表示されていない場合、このワークスペースを使用してニュースやイベントをモニターできます。

IBM Lotus® Sametime® には統合されたコラボレーションおよび通信用ツールが備わっており、必要な場所で必要な時期に、そのツールをインスタント・メッセージに使用できます。

## レポートの作成

IBM Intelligent Operations Center には統合されたレポート作成機能が備わっているため、このソリューションで提供されるイベントおよび KPI を使用してレポートを設定および実行することができます。この機能を使用して、最も有用な情報を随時および定期的に収集および提供することができます。この機能により、調整された要約やグラフィカル表示のすべての利点を活用できるようになります。

## ユーザーおよび利点

IBM Intelligent Operations Center は、組織、政府機関、または地方自治体で業務管理に携わっている要員 (エグゼクティブ、監督者、およびオペレーター) 向けに設計されています。

以下の表には、IBM Intelligent Operations Center の使用に関連するユーザーと利点が示されています。

表 1. IBM Intelligent Operations Center のユーザーと利点

ユーザー	このソフトウェアが役立つ操作
エグゼクティブ	<ul style="list-style-type: none"><li>• マップ、ダッシュボード、およびアラートを通じて、イベントおよびインシデントのエグゼクティブ・レベルの要約を取得する</li><li>• 重要業績評価指標 (KPI) を使用して組織の成功度を評価する</li><li>• レポートを通じて問題を特定し、追跡する</li><li>• 提供されるデータに基づいて、ポリシーの優先順位と実施を指示する</li></ul>
監督者	<ul style="list-style-type: none"><li>• マップ、ダッシュボード、およびアラートに示された競合および問題を特定して処理する</li><li>• 新しいイベントの追加、既存のイベントの編集、イベントの取り消し、およびインシデントへのイベントのエスカレートを行ってイベントを管理する</li><li>• リソースについての情報を提供し、リソースを管理する</li><li>• イベントに関連した手順およびワークフローを格納してその実行を管理する</li><li>• KPI をモニターする</li><li>• 重要事項を素早く簡単に伝える</li><li>• 有用なレポートを設計する</li></ul>
オペレーター	<ul style="list-style-type: none"><li>• リストで表示する状況イベントおよびインシデントを作成、編集、およびモニターする</li><li>• 割り当てられたアクティビティの状況を受け取って更新する</li><li>• 使用可能なリソースを確認する</li><li>• 定期的なレポートや随時のレポートを実行する</li><li>• 適切な同僚、責任者、またはエグゼクティブに対するアラートを通知、更新、および発行する</li><li>• 緊急時や応答が必要なその他の状況で、素早く簡単に連絡する</li></ul>
ユーザー管理者	<ul style="list-style-type: none"><li>• 新しいユーザーを追加し、適切な認証を持つグループに割り当てる</li><li>• カテゴリと、適切な権限を持つ役割ベースの許可グループを使用して、データ・セキュリティを確保する</li><li>• 必要な専門知識とデータの分野に適した許可を設定する</li></ul>

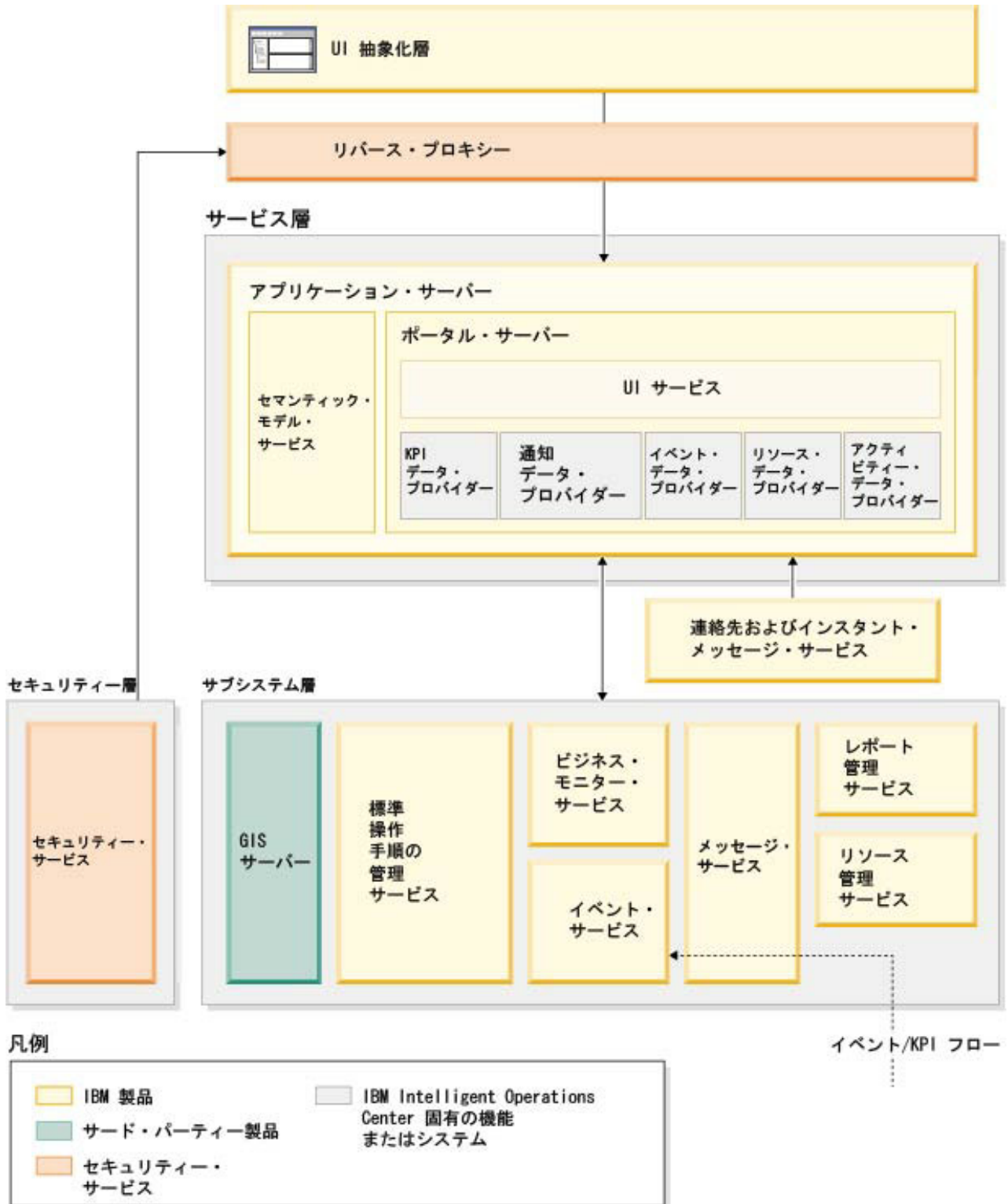
表 1. IBM Intelligent Operations Center のユーザーと利点 (続き)

ユーザー	このソフトウェアが役立つ操作
システム管理者	<ul style="list-style-type: none"> <li>• ページおよびポートレットを組織に合わせてカスタマイズする</li> <li>• 管理要件に従って、表示されるイベントおよび KPI をカスタマイズする</li> <li>• テスト・イベントを作成し、公開する</li> <li>• レポートおよび配布を構成する</li> </ul>

## コンポーネント

IBM Intelligent Operations Center の構造は、主要コンポーネント、サブシステム、およびサービスに大まかに分けることができます。

次の図は、IBM Intelligent Operations Center の概略を示します。





## UI 抽象化層

IBM Intelligent Operations Center では、イベントの情報、全体的な状況、および詳細への、Web ベースのワンストップ・ポータルを使用できます。ユーザー・インターフェース (UI) では、共通の形式で事前構成されたさまざまなビューで、カスタマイズされた情報が示されます。簡単に使用できるダッシュボードを介してすべての情報が表示されます。

## セキュリティー層

情報に対するすべてのアクセス権限は、組織上の役割とデータ・カテゴリーを介してセキュリティー層によって制御されます。この制御によって、権限の付与を簡単に管理しながら、無許可アクセスを回避できます。

## サービス層

サービス層は共通のウィジェットと共通の UI サービス・フレームワークを使用してイベント・データを受け取り、イベント管理を介してそのイベント・データをメッセージ・システムに渡します。IBM Intelligent Operations Center データ・プロバイダーは UI サービスを拡張します。基盤となる運用システムからはさまざまなデータが提供されるため、データは標準セマンティック参照モデルに従って正規化されます。このモデルは、関係をマッピングするための共通ディクショナリーを提供します。このモデルを使用することで、情報の複数の変換データを用意しなくても、効果分析とイベントへの対処をより素早く行うことができます。セマンティック・モデルを使用することで、基盤となる領域の KPI や階層情報にアクセスできるようになります。データに対する高度分析を行い、意思決定とガバナンスを導くのに役立つ最適化と予測を特定できます。

## サブシステム層

ソリューションによって、基本となる領域の運用システムとソリューション間の情報交換を促進するためのメディエーション層が提供されます。構成可能なさまざまなソースからのデータをゲートウェイを介してサブシステム層に提供できます。これによって、アラート、KPI、およびイベントが生成されます。この統合層により、さまざまな形式 (可能な場合はオープン・スタンダード) でメッセージの両方向通信を行うことができます。業界標準ツールを使用してソースからリファレンス・セマンティック・モデルへの変換を行っているため、基盤となる運用システムを変更する必要はありません。適切なワークフローを得るために、緊急対応システムや他の対応システムを IBM Intelligent Operations Center に接続することができます。

IBM Intelligent Operations Center の構成では、以下がサポートされます。

- 業務状態の把握、イベントおよびインシデントの管理、およびオペレーション・センターの制御下にある複数の領域の連結のための中心ポイント
- イベント、インシデント、およびリソースを空間的および視覚的にマッピングするための、地理情報システム (GIS)、ロケーション・マップ図または計画との統合
- 基盤となる領域のシステムへの接続を介してデータの変更に合わせて更新される重要業績評価指標 (KPI) の作成およびモニター
- イベントに関連したワークフローおよびアクティビティーに関する標準操作手順 (SOP) の作成およびモニター
- 緊急対応または標準対応が必要なアラートを含む、フィールドから出されるアラート。
- IBM Lotus Sametime を使用したインスタント・メッセージ機能によるコラボレーション機能

- イベントまたは KPI データに基づく随時レポートと定期的レポートの作成および配布
- 役割ベースのセキュリティー・モデル

IBM Intelligent Operations Center のシステム・サービスについて詳しくは、このトピックの末尾にあるリンクを参照してください。

#### 関連概念:

13 ページの『IBM Intelligent Operations Center システム・サービス』  
IBM Intelligent Operations Center サーバーは、多くのサービスを提供しています。

---

## イベント管理

IBM Intelligent Operations Center ソリューションでは、中央のオペレーション・ハブで、ドメイン内部および複数のドメインにまたがる情報を、リアルタイムかつ長期にわたって統合し最適化することに重点を置いています。イベント・データ管理により、IBM Intelligent Operations Center では、複数のシステムからのデータを取り込み、絶えず予測を行い、重要なイベントやトレンドに対処することができます。

イベント・メッセージは、基本的ではあるが完全な情報を含む自己完結型のデータ項目で、受信者はそのメッセージに対し応答することができます。 イベント・メッセージは、IBM Intelligent Operations Center によってキューに配置され、イベント処理サービスによって処理されます。

イベントは、中央のオペレーション・ハブの操作やドメインの性質に基づき、さまざまな形式で IBM Intelligent Operations Center に受信されます。 イベントの形式の例としては、トリガー、しきい値、複合イベント、手動生成イベントなどがあります。

トリガーは、何かが発生することで生成されるイベントであり、通常は受信者によるアクションの実行が必要です。トリガーの例には以下のようなものがあります。

- 火災報知機または煙探知機が作動した。
- 情報技術システムがダウンした。
- 侵入検出器が作動した。
- 自然のイベント (弱い地震など) にセンサーが反応した。

IBM Intelligent Operations Center は、このようなイベントに関する情報を外部システムから受信し、それをアラートに変換して受信者に提供します。 一般に、低レベル標識は要約されることが多く、より広い範囲の注意に値する場合にのみ IBM Intelligent Operations Center に渡されます。例えば、すべての火災がイベントとして報告されるわけではありません。しかし、危険物があるために消防隊の複数の部隊と環境保護の専門家が出動するような火災は、オペレーション・センターに報告する価値があるといえます。

しきい値イベントは、センサーまたはその他のソースから取得した計測値が、正常範囲の外に出たかどうかを判断するのに役立ちます。基本的なしきい値イベントでは、複数の計測値を比較してトレンドを報告します。さらに高度なしきい値イベントでは、計測値と履歴情報によって作成されたしきい値とを比較することができます。 しきい値イベントの例を以下に示します。

- 温度超過および温度不足のアラーム
- 高水位および低水位
- 環境基準に違反する大気質や水質
- 過剰な電力使用量

IBM Intelligent Operations Center では、これらのイベントを重要業績評価指標 (KPI) の形式で管理できます。

複合イベントでは、複数のシステムからの情報を一緒にまとめて、関連イベントのグループとして報告するかどうかを判別します。例えば、有料道路通行料金収受の管理者が、クレジットカード認証のコンピューター・リンクがダウンしていることを示すトリガー・イベントをモニター・システムから受信し、ほどなくして、認証されていない決済の信用限度に近づいていることを警告するしきい値イベントを金融システムから受信したとします。これらの2つの問題の組み合わせは、いずれか一方のみの場合よりはるかに重大なので、注意を喚起し解決に向けての調整をするために複合イベントが生成されます。

手動入力イベントは、都市には特に重要です。これらの中には、犯罪や交通事故など、監視の対象となるインシデントがあります。このほかの手動入力イベントの例としては、市民からの緊急通報、都市職員が作成したレポート、都市の状況を報告する管理システムなどから生成されるイベントなどがあります。最も一般的なタイプの手動入力イベントには以下のものがあります。

- 重大な気象警報
- 犯罪レポート
- 火災
- 道路交通インシデント - 事故、混雑、過積載
- 近く予定されるイベント - ロック・コンサート、ロード・レース、パレード

複合イベント処理により、都市は都市システムに対する例外を容易に判別でき、場合によっては、関係のないデータからトレンドを識別したり、将来の問題を予測したりすることができます。

---

## バージョン 1.5 の新機能

IBM Intelligent Operations Center 1.5 では、管理者やユーザーのための有用な新機能が導入されています。


### ユーザーのための新機能

IBM Intelligent Operations Center 1.5 を使用すると、イベントに関連付けられているリソースおよびアクティビティを管理できます。

### リソースの管理とロケーション・マップの対話形式の操作

新しい「ロケーション・マップ」ポートレットと拡張された「マップ」ポートレットでは、以下を実行できます。


- 地理的マップに基づいてイベント周辺で使用可能なリソースを評価する。
- 対話式エリアが定義された新しいタイプのマップ (ロケーション・マップ) を操作する。例えば、ロケーション・マップは、輸送システムの経路の計画に基づくことができます。
- マップ上の同じ場所に集まっている複数のイベントを表示する。

 新しい「ロケーション・マップ」ポートレットおよび拡張された「マップ」および「詳細」ポートレットについて詳しくは、このトピックの末尾にあるリンクを参照してください。

### イベントに関連したアクティビティの状況の追跡

新しい「マイ・アクティビティ」ポートレットでは、以下を実行できます。


- 自分のグループの、手順およびイベントに関連付けられているオープン・タスクを表示する。
- 自分に割り当てられているタスクの状況を表示する。
- 自分に割り当てられているタスクの状況を変更する。

 「マイ・アクティビティー」ポートレットについて詳しくは、このトピックの末尾にあるリンクを参照してください。

## レポートの作成

新しい「レポート」ポートレットでは、以下を実行できます。

- イベントのレポートを最大 6 つまでグラフとして表示する。
- 選択した基準およびデータに基づいてカスタム・レポートを作成する (日付または日付範囲別のイベントのレポートなど)。
- レポート URL をコピーして、レポートがポートレットの右側のフレームに表示されるようにする。

 「レポート」ポートレットについて詳しくは、このトピックの末尾にあるリンクを参照してください。

### 関連概念:

305 ページの『ロケーション・マップ』

「ロケーション・マップ」ポートレットでは、ロケーション・マップでマークされているイベントを確認することができます。IBM Intelligent Operations Center のロケーション・マップは、対話用に事前に定義されているエリア (大規模なスポーツ・スタジアムの座席エリアなど) を含むマップまたは計画です。

309 ページの『マップ』

「マップ」ポートレットを使用して、イベントおよびリソースをマップ上で確認します。

301 ページの『詳細』

「詳細」ポートレットを使用して、IBM Intelligent Operations Center でイベントの表示、モニター、および管理を行います。

314 ページの『マイ・アクティビティー』

「マイ・アクティビティー」ポートレットには、インターフェースにログオンしているユーザーがメンバーとして所属するグループが所有するアクティビティーの動的なリストが表示されます。

318 ページの『レポート』

「レポート」ポートレットでは、イベントのレポートをグラフとして表示することができます。このポートレットは、イベントのグループ化の基準となる各種のオプションを提供します。さらに、特定の日付または日付範囲を指定してイベントを選択することができます。レポートは、現在および将来のイベントへの対応について計画を策定するのに役立ちます。


## 管理者のための新機能

バージョン 1.5 では、ポートレットおよびページ・レイアウトをカスタマイズできます。また、標準操作手順およびワークフローを設定することもできます。

## ポートレットのカスタマイズ

新しいポートレット構成オプションを使用すると、各ポートレットで以下を設定できます。

- 個々のポートレットに固有のプロパティー (例えば、マップの中心点やズーム・レベルの設定など)
- すべてのポートレットにわたる汎用のプロパティー (例えば、ポートレットの高さの設定など)

 ポートレットのカスタマイズについて詳しくは、このトピックの末尾にあるリンクを参照してください。

## 標準操作手順およびワークフローを使用したイベントの管理

以下のように、イベントに関連した手順およびアクティビティを定義できます。

- 業務計画に基づいて標準操作手順を定義する。
- ワークフローを作成する。
- イベントのパラメーターに基づいて、標準操作手順を選択するためのパラメーターを定義する。



イベントに関連付けられているアクティビティの関連付けについては、このトピックの末尾にある「標準操作手順」のリンクを参照してください。

## イベントのスクリプト記述およびパブリッシュ

新しい「イベント・スクリプト記述」ポートレットを使用して、事前に定義された時間間隔でパブリッシュされるイベントの順次リストを作成できます。



イベントのスクリプト記述およびイベントのパブリッシュについては、このトピックの末尾にあるリンクを参照してください。

## サービス状況の確認

新しいシステム検査チェック・ツールを使用して、IBM Intelligent Operations Center サービスの運用状況を確認できます。



システム検査チェック・ツールについては、このトピックの末尾にあるリンクを参照してください。

## プロトコルのサポート

IBM Intelligent Operations Center は、共通アラート・プロトコル以外のプロトコルを使用するイベントをサポートするようになりました。以下を行うことができます。

- 共通アラート・プロトコル・イベントおよび非共通アラート・プロトコル・イベントの列挙型を拡張する。
- 「詳細」ポートレットのポップアップ・メニューをカスタマイズする。
- ポートレットに表示するために複数の領域のイベントを受け入れる。



統合点とプロトコルについては、このトピックの末尾にあるリンクを参照してください。

#### 関連概念:

143 ページの『標準操作手順』

標準操作手順およびアクティビティを定義することで、IBM Intelligent Operations Center で受信するイベントを管理できます。「標準操作手順」ポートレットを使用して、Tivoli® Service Request Manager® で、標準操作手順、標準操作手順の選択マトリックス、およびワークフロー・デザイナーの各アプリケーションにアクセスします。

120 ページの『イベント・スクリプト記述』

「イベント・スクリプト記述」ポートレットを使用して、事前に定義された時間間隔でパブリッシュされるイベントの順次リストを作成するスクリプトを記述します。

232 ページの『コンポーネントの検証』

システム検査チェックツールは、IBM Intelligent Operations Center 内のコンポーネントをテストし、アクセス可能であるか、および操作可能であるかを判別します。

101 ページの『統合点とプロトコル』

他のシステムは、IBM Intelligent Operations Center のサービスとポリシーを使用して、ソリューションと統合することができます。データは、共通アラート・プロトコル (CAP) 形式で受け取ることができます。他のプロトコルもサポートされています。

#### 関連タスク:

162 ページの『ポートレットのカスタマイズ』

管理者は、ポートレットの設定値を変更してポートレットをカスタマイズすることができます。



---

## 第 2 章 インストールおよび構成

IBM Intelligent Operations Center には、IBM Intelligent Operations Center に必要な環境をインストールするデプロイメント・ウィザードが用意されています。この環境および IBM Intelligent Operations Center パッケージをデプロイした後に、いくつかの追加構成が必要になります。

---

### インストールの準備

IBM Intelligent Operations Center をデプロイする前に、IBM Intelligent Operations Center のシステム構成について理解し、環境の前提条件が満たされていることを確認します。

### IBM Intelligent Operations Center システム・サービス

IBM Intelligent Operations Center サーバーは、多くのサービスを提供しています。

#### 分析サービス

データ分析および表示サービスを提供します。

#### アプリケーション・サーバー

製品をサポートする Java Enterprise Edition サービスを提供します。

#### セキュリティー

ユーザーにシステムの使用権限があるかどうかを判別し、システム内でのユーザーの特権を定義するサービスを提供します。

#### 許可サービス

各種サービスについて、ユーザーに使用権限があるかどうかを判別するサービスを提供します。

#### ビジネス・モニター

ビジネス・プロセスおよびアクティビティー情報を、リアルタイムで集計、分析、および表示します。

#### インスタント・メッセージ・サーバー

ユーザーとアプリケーションについての、リアルタイムでのコラボレーション機能を提供します。

#### 構成サービス

製品の構成を管理します (在庫管理および変更管理を含む)。

#### データベース

アプリケーション・データ用およびシステム・データ用のデータベース・マネージャーを提供します。

#### ディレクトリー

名前と値との間のマッピングを提供します。データ・サービスは、ユーザー名およびパスワードのリポジトリーとして使用されます。

#### イベント処理

システム・イベントの収集、集計、表示、および処理を行います。

#### メッセージング・サービス

製品に対するメッセージ・サービスおよびワークフロー・サービスを提供します。

#### モニター・サービスおよびエージェント

製品内でのモニター・アクティビティーを提供します。

## ポータル

製品とのユーザー対話をサポートするサービスを提供します。

## セマンティック・モデル

アプリケーションによって実社会のオブジェクトおよび関係をモデル化できるようにするサービスを提供します。

## 関連概念:

6 ページの『コンポーネント』

IBM Intelligent Operations Center の構造は、主要コンポーネント、サブシステム、およびサービスに大まかに分けることができます。

## IBM Intelligent Operations Center ハードウェア要件

IBM Intelligent Operations Center のインストールには、最小要件を満たす 5 つのサーバーが必要です。

サーバーは、64 ビット x86 サーバーである必要があります。

IBM Intelligent Operations Center で使用される最小要件のサーバーを、表 2 に示します。推奨される最小ディスク・スペースには、ブート区画用およびスワップ区画用のスペースは含まれません。

表 2. 最小ハードウェア要件

リソース	アプリケーション・サーバー	イベント・サーバー	データ・サーバー	管理サーバー	インストール・サーバー
CPU	4	4	4	4	2
メモリー	24 GB	16 GB	16 GB	24 GB	4 GB
ネットワーク・アダプター	1	1	1	1	1
ディスク・スペース	113 GB	108 GB	108 GB	108 GB	108 GB
インストール時に必要な追加ディスク・スペース	90 GB	90 GB	90 GB	90 GB	90 GB

ブート区画およびスワップ区画に必要なスペースを除外した、各サーバーのディレクトリーの最小要件を、表 3 に示します。

表 3. 各ディレクトリーの最小スペース所要量

ディレクトリー	最小スペース	注
/	8 GB	
/opt	35 GB または 40 GB	40 GB はアプリケーション・サーバーに必要で、35 GB はその他のすべてのサーバーに必要です。
/usr	8 GB	
/home	5 GB	
/tmp	10 GB	
/chroot	1 GB	
/datahome	25 GB	
/loghome	8 GB	
/installMedia	90 GB	このディレクトリーはインストール後に削除できます。



表 3. 各ディレクトリーの最小スペース所要量 (続き)

ディレクトリー	最小スペース	注
/var	8 GB	

#### 関連タスク:

20 ページの『サーバーの準備』

IBM Intelligent Operations Center をインストールする前に、サーバー構成要件を満たしていることを検証してください。事前検査ツールでは、これらの要件の多くが実装済みであることを確認します。

#### 関連情報:



システム要件

## 前提ソフトウェア要件

IBM Intelligent Operations Center をインストールする前に、サーバーには適切なソフトウェアをインストールしておく必要があります。

IBM Intelligent Operations Center では、Red Hat Enterprise Linux (RHEL) バージョン 5、サーバー x86-64 アップデート 5 またはそれ以降を、全サーバーにインストールする必要があります。Red Hat Enterprise Linux バージョン 6 はサポートされていません。

#### 関連タスク:

20 ページの『サーバーの準備』

IBM Intelligent Operations Center をインストールする前に、サーバー構成要件を満たしていることを検証してください。事前検査ツールでは、これらの要件の多くが実装済みであることを確認します。

#### 関連情報:



システム要件

## サポートされるブラウザ

IBM Intelligent Operations Center ソリューション・インターフェースは複数のブラウザをサポートします。一部のブラウザは制限付きで使用できます。

IBM Intelligent Operations Center は、以下のブラウザでテストが完了しており、サポートされています。

- Microsoft Internet Explorer 8.x (32 ビットのみ)
- Microsoft Internet Explorer 9.x (32 ビットのみ)
- Mozilla Firefox 10 ESR

## Internet Explorer Compatibility View

IBM Intelligent Operations Center は Internet Explorer 8 または Internet Explorer 9 の Compatibility View をサポートしません。

注: ユーザー・インターフェース用の新規ページの作成時に問題が発生した場合、Compatibility View が一時的にオンになることがあります。詳しくは、このトピックの末尾にあるリンクを参照してください。

## Internet Explorer 8.x のパフォーマンス

ユーザーが Internet Explorer 8.x を使用すると、パフォーマンスの低下が発生する場合があります。

この問題を避けるには、Internet Explorer 9.x または Firefox 10 ESR を使用します。

## 最小画面解像度

IBM Intelligent Operations Center は、最小で 1280 x 800 の画面解像度で実行されるように設計されています。

### 関連タスク:

364 ページの『ユーザー・インターフェースの新規ページを作成できない』

Microsoft Internet Explorer 9 を使用している場合に新規ページを作成する際に発生する問題を解決します。

## メディアのパッケージ化

IBM Intelligent Operations Center は、DVD パッケージで注文することも、パスポート・アドバンテージから入手することもできます。

製品番号は 5725-D69 です。

### 関連情報:

 [パスポート・アドバンテージ](#)

 [IBM Intelligent Operations Center バージョン 1.5 のイメージ・ファイルをダウンロードします。](#)

---

## インストール・チェックリスト

IBM Intelligent Operations Center の、2 つの異なるインストール・オプションに、インストール・チェックリストを使用できます。これらのチェックリストはインストール手順の概要を示すものであり、インストールの進行を追跡するのに使用できます。

## チェックリスト - IBM Installation Manager を使用したインストール

このチェックリストは、IBM Installation Manager を使用して IBM Intelligent Operations Center をインストールするときに、インストール・ステップを追跡するために使用します。

### このタスクについて

印刷用のチェックリストは、このトピックの末尾にある関連リンクから入手可能です。

### 手順

- \_\_\_ 1. 必要なハードウェアがあることを確認します。
- \_\_\_ 2. 必要なソフトウェアがハードウェアにインストールされていることを確認します。
- \_\_\_ 3. サーバーを準備します。
- \_\_\_ 4. インストール・パッケージをインストール・サーバーにコピーします。
- \_\_\_ 5. Java ランタイム環境をインストールします。
- \_\_\_ 6. IBM Installation Manager をインストールします。

- \_\_ 7. IBM Installation Manager を再始動して、「トポロジーの構成」パッケージをインストールします。
- \_\_ 8. IBM Installation Manager を再始動して、「ターゲット・サーバーの準備」パッケージをインストールします。このステップが正常に完了した場合は、ステップ 9 をスキップしてください。
- \_\_ 9. IBM Installation Manager を再始動して、「システム・チェック・エラーを無視する」パッケージをインストールします。システム・チェック・エラーを解決した後で、またはインストールを続行できると判断した後で IBM Installation Manager を実行する場合、2 回目の実行時には「ターゲット・サーバーの準備」および「システム・チェック・エラーを無視する」の両方を選択します。
- \_\_ 10. IBM Installation Manager を再始動して、「環境の準備」パッケージをインストールします。
- \_\_ 11. IBM Installation Manager を再始動して、「インストールおよびプラットフォームの構成 - パート 1」パッケージをインストールします。

**ヒント:** パート 1 とパート 2 を同時に選択しないでください。これらのステップの実行には最も時間がかかります。両方を一緒に実行して万一障害が発生した場合、片方が成功していた場合でも、両方を再実行することが必要になります。

**重要:** インストールの各フェーズ間でサーバーをシャットダウンしないでください。各フェーズの間でのサーバーのシャットダウンはテストされていないため、このようなシャットダウンを行うと予測不能な結果になる可能性があります。

- \_\_ 12. IBM Installation Manager を再始動して、「インストールおよびプラットフォームの構成 - パート 2」パッケージをインストールします。
- \_\_ 13. IBM Installation Manager を再始動して、「プラットフォーム制御ツールのインストール」パッケージをインストールします。
- \_\_ 14. IBM Installation Manager を再始動して、「システム検査チェック・ツールのインストール」パッケージをインストールします。
- \_\_ 15. すべての IBM Intelligent Operations Center サーバーを再始動します。
  - a. プラットフォーム制御ツールを使用して、すべての IBM Intelligent Operations Center サーバーをシャットダウンします。
  - b. オペレーティング・システムからすべてのサーバーをシャットダウンして、再始動します。
  - c. プラットフォーム制御ツールを使用して、すべての IBM Intelligent Operations Center サーバーを開始します。
- \_\_ 16. IBM Installation Manager を再始動して、「アプリケーションのインストール」パッケージをインストールします。これにより、IBM Intelligent Operations Center アプリケーションがインストールされます。
- \_\_ 17. IBM Intelligent Operations Center アーキテクチャーを構成します。
  - \_\_ a. IPv6 を使用する場合は、コラボレーション・サービスを構成します。
  - \_\_ b. コラボレーション・サービス用のシングル・サインオンを構成します。
  - \_\_ c. Semantic Model Services をインストールして構成します。
  - \_\_ d. プラットフォーム制御ツールを構成します。
  - \_\_ e. Tivoli Service Request Manager の管理パスワードを暗号化します。
  - \_\_ f. EventProcessor の最小スレッド数を設定します。
  - \_\_ g. デフォルトのスレッド・プール・サイズおよび WebContainer スレッド・プール・サイズを変更します。
- \_\_ 18. その他のアプリケーションをすべてインストールします。

- \_\_ 19. IBM Installation Manager を再始動して、**Cyber Hygiene** パッケージを実行します。 Cyber Hygiene は、IBM Intelligent Operations Center システムに対して、追加のセキュリティーを提供します。

注: Cyber Hygiene のインストールと実行は、同一ステップで行われます。

- \_\_ 20. ssh アクセスとパスワードを必要とするユーザーを構成します。

## タスクの結果

IBM Intelligent Operations Center アーキテクチャーおよび IBM Intelligent Operations Center アプリケーションがインストールされ、使用の準備が整います。

## 次のタスク

インストール問題の診断に役立つインストール・ログを収集するために、収集必須ツールが提供されています。

### 関連概念:

91 ページの『Cyber Hygiene の概要』

IBM Intelligent Operations Center の Cyber Hygiene 機能は、インストール済みシステムに存在する可能性のある機密漏れを修正するサービスを提供できるように設計されています。

### 関連情報:



印刷用のチェックリスト

## チェックリスト - ステップ・バイ・ステップでインストール

スクリプトおよびコマンドを使用して IBM Intelligent Operations Center をインストールする場合、このチェックリストを使用して、インストール・ステップを追跡します。

## このタスクについて

印刷用のチェックリストは、このトピックの末尾にある関連リンクから入手可能です。

## 手順

- \_\_ 1. 必要なハードウェアがあることを確認します。
- \_\_ 2. 必要なソフトウェアがハードウェアにインストールされていることを確認します。
- \_\_ 3. サーバーを準備します。
- \_\_ 4. Java ランタイム環境をインストールします。
- \_\_ 5. インストール・パッケージをインストール・サーバーにコピーします。
- \_\_ 6. インストール・パッケージを解凍して準備します。
- \_\_ 7. インストール・プロパティを定義します。
- \_\_ 8. トポロジー・プロパティ・ファイルを編集して、インストール用のトポロジーを定義します。
- \_\_ 9. 鍵ファイルの暗号化に使用するトポロジー・パスワードを生成します。
- \_\_ 10. トポロジー・ファイルを生成します。
- \_\_ 11. 事前検査ツールを実行して、環境で IBM Intelligent Operations Center をインストールする準備ができたかどうかを検査します。
- \_\_ 12. 付属のツールを使用するか、一連のコマンドを実行して、Linux セキュリティー設定を構成します。

- \_\_ 13. IBM Intelligent Operations Center アーキテクチャーをインストールします。これは 1 フェーズまたは 3 フェーズで実行できます。仮想化環境で実行している場合は、複数フェーズでインストールすることで、インストール・フェーズ間でのスナップショットを作成することができます。
- IBM Intelligent Operations Center を 1 フェーズでインストールする。インストールには、最大 14 時間かかります。
  - IBM Intelligent Operations Center を 3 フェーズでインストールする。3 つのフェーズとは以下のとおりです。
    - a. インストール・ファイルをインストール・サーバーからターゲット・サーバーにコピーします。このフェーズには約 2 時間かかります。
    - b. トポロジーの最初のフェーズをインストールします。このフェーズには約 9 時間かかります。
    - c. トポロジーの 2 番目のフェーズをインストールします。このフェーズには約 3 時間かかります。
- 重要:** インストールの各フェーズ間でサーバーをシャットダウンしないでください。各フェーズの間でのサーバーのシャットダウンはテストされていないため、このようなシャットダウンを行うと予測不能な結果になる可能性があります。
- \_\_ 14. プラットフォーム制御ツールをインストールします。
- \_\_ 15. システム検査チェック・ツールをインストールします。
- \_\_ 16. IBM Intelligent Operations Center アーキテクチャーが正しくインストールされていることを確認します。
- \_\_ 17. IBM Intelligent Operations Center アーキテクチャーを構成します。
- \_\_ a. IPv6 を使用する場合は、コラボレーション・サービスを構成します。
  - \_\_ b. コラボレーション・サービス用のシングル・サインオンを構成します。
  - \_\_ c. Semantic Model Services をインストールして構成します。
  - \_\_ d. Tivoli Service Request Manager の管理パスワードを暗号化します。
  - \_\_ e. EventProcessor の最小スレッド数を設定します。
  - \_\_ f. デフォルトのスレッド・プール・サイズおよび WebContainer スレッド・プール・サイズを変更します。
- \_\_ 18. IBM Intelligent Operations Center アプリケーションをインストールします。
- \_\_ 19. その他のアプリケーションをすべてインストールします。
- \_\_ 20. Cyber Hygiene をインストールして実行します。Cyber Hygiene は、IBM Intelligent Operations Center システムに対して、追加のセキュリティーを提供します。
- 注: Cyber Hygiene のインストールと実行は、同一ステップで行われます。
- \_\_ 21. ssh アクセスとパスワードを必要とするユーザーを構成します。

## タスクの結果

IBM Intelligent Operations Center アーキテクチャーおよび IBM Intelligent Operations Center アプリケーションがインストールされ、使用の準備が整います。

## 次のタスク

インストール問題の診断に役立つインストール・ログを収集するために、収集必須ツールが提供されています。

## 関連概念:

91 ページの『Cyber Hygiene の概要』

IBM Intelligent Operations Center の Cyber Hygiene 機能は、インストール済みシステムに存在する可能性のある機密漏れを修正するサービスを提供できるように設計されています。

## 関連情報:



印刷用のチェックリスト

---

## サーバーの準備

IBM Intelligent Operations Center をインストールする前に、サーバー構成要件を満たしていることを検証してください。事前検査ツールでは、これらの要件の多くが実装済みであることを確認します。

### このタスクについて

仮想環境で稼働している場合は、以下のステップのテンプレートを使用するとセットアップ時間を短縮できます。

### 手順

1. サーバーがハードウェア要件およびソフトウェア要件を満たしていることを確認します。
2. TCP/IP ネットワーキングをセットアップします。
  - a. DNS サーバーを使用するか、`/etc/hosts` ファイル内の定義によって、完全修飾名および短縮ホスト名を定義します。
  - b. TCP/IP 構成を検証します。以下のテストが正常に完了すれば、サーバーは正しく構成されています。
    - 1) `hostname -s` コマンドは、サーバーの定義された短縮ホスト名を返します。
    - 2) `hostname -f` コマンドは、サーバーの完全修飾ドメインとホスト名を返します。
    - 3) サーバーごとに短縮ホスト名を指定した `ping` コマンド (IPv6 環境の場合は `ping6` コマンド) の結果は、サーバーがアクセス可能であることを示します。
    - 4) サーバーごとに完全修飾名を指定した `ping` コマンド (IPv6 環境の場合は `ping6` コマンド) の結果は、サーバーがアクセス可能であることを示します。
  - c. `/etc/hosts` ファイル内の各サーバーに対して、ローカル・ループバック・アドレッシングを有効にします。
  - d. ローカル・ループバック・アドレッシングを検証します。以下のテストが正常に完了すれば、サーバーは正しく構成されています。
    - 1) `ping -n localhost` コマンドが、アドレス `127.0.0.1` を返す。
    - 2) `ping -n localhost.localdomain` コマンドが、アドレス `127.0.0.1` を返す。
    - 3) IPv6 環境で、`ping6 -n localhost6` コマンドが、アドレス `::1` を返す。
    - 4) IPv6 環境で、`ping6 -n localhost6.localdomain6` コマンドが、アドレス `::1` を返す。
  - e. IBM Intelligent Operations Center が必要とするポートが使用可能であることを確認してください。各サーバーに必要なポートを、21 ページの表 4 に示します。



表 4. 製品の使用に必要となるポート

サーバー	製品の使用に必要となるポート
アプリケーション	80, 82, 389, 390, 443, 2814, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7234, 7276, 7278, 7279, 7280, 7281, 7283, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 8008, 8880, 8882, 8883, 8885, 8887, 8889, 8890, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9060, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9357, 9359, 9361, 9363, 9364, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9449, 9633, 9634, 9635, 9636, 9638, 9640, 9641, 9810, 9811, 9812, 9813, 9814, 9815, 10000, 10001, 10002, 10003, 10004, 10005, 10006, 10007, 10008, 10009, 10010, 10011, 10012, 10013, 10014, 10015, 10016, 10017, 10025, 10026, 10027, 10028, 10029, 10030, 10031, 10032, 10033, 10034, 10035, 10036, 10037, 10038, 10039, 10040, 10041, 10042, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016
イベント	80 82, 84, 389, 390, 1414, 8008, 9060, 9080, 20000, 31000, 31001, 31002, 31003, 31004, 31005, 31006, 31007, 31008, 31009, 31010, 31011, 31012, 31013, 31014, 31015, 31016
データ	389, 390, 50000, 50001, 50002, 50003, 50004, 50005, 50006, 50007, 50008
管理	80, 82, 389, 390, 1098, 1099, 1527, 1918, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 7135, 7136, 7137, 7276, 7278, 7279, 7280, 7282, 7284, 7286, 7287, 7288, 7289, 7290, 7291, 7292, 7293, 8008, 8880, 8882, 8884, 8886, 8888, 8890, 8892, 9043, 9044, 9045, 9046, 9047, 9048, 9049, 9050, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9101, 9102, 9103, 9104, 9105, 9106, 9107, 9354, 9356, 9358, 9360, 9362, 9364, 9366, 9404, 9405, 9406, 9407, 9408, 9409, 9410, 9411, 9412, 9413, 9414, 9415, 9416, 9417, 9418, 9419, 9420, 9421, 9422, 9423, 9424, 9443, 9444, 9445, 9446, 9447, 9448, 9449, 9633, 9634, 9635, 9637, 9639, 9641, 9643, 9810, 9811, 9812, 9813, 9814, 9815, 9816, 13100, 13101, 13104, 41001, 50001

f. 以下のサーバーについては、`/etc/security/limits.conf` ファイルの `nofile` パラメーターで定義されているオープン・ファイル記述子の最大数が 20480 に設定されていることを確認してください。

- アプリケーション・サーバー
- イベント・サーバー
- データ・サーバー
- 管理サーバー

このためには、`/etc/security/limits.conf` ファイルに次の行を追加します。

```
* soft nofile 20480
* hard nofile 20480
```

これにより、すべてのユーザーのオープン・ファイル数のソフト・リミット (デフォルト) とハード・リミット (最大数) がそれぞれ 20480 に設定されます。他のアプリケーションが 20480 を超える数のファイルを必要とする場合は、ハード・リミットを増やすことができます。

g. 以下のサーバーについて、`/etc/sysctl.conf` ファイルの `net.ipv4.tcp_fin_timeout` パラメーターが 30 になるように追加または更新します。

- アプリケーション・サーバー
- イベント・サーバー

- データ・サーバー
  - 管理サーバー
3. すべての Linux ファイアウォールを無効にします。
  4. SELinux (Security Enforcing Linux) を無効にします。それには、`/etc/selinux/config` ファイルを編集して、SELINUX を `disabled` に変更します。構成を変更したら、サーバーをリブートします。
  5. Linux オペレーティング・システムで指示されているものと同じ時刻と日付が、すべてのサーバーに設定されていることを確認します。時刻同期サービスを使用できます。
  6. `/etc/init.d/sshd start` コマンドを実行して、各サーバー上で `sshd` サービスを有効にします。このサービスは、パスワード認証を使用した `root` ログインのために有効にする必要があります。TCP/IP ポート 22 は、インストール処理中に使用するための、利用可能な `ssh` アクセス・ポートとして、オペレーティング・システムで構成する必要があります。プラットフォーム制御ツールの `ssh` アクセス用の TCP/IP ポート番号は、トポロジー・プロパティ・ファイルに指定されています。構成されたポートは、プラットフォーム制御ツールのみが使用します。
  7. `yum install package_name` コマンドを使用して、表 5 に示す Linux パッケージを各サーバーにインストールします。これらのパッケージは Red Hat から入手できます。

表 5. IBM Intelligent Operations Center ターゲット・サーバー用の必須およびオプションの Linux パッケージ

パッケージ	アプリケーション・サーバー	データ・サーバー	イベント・サーバー	管理サーバー
<code>compat-libstdc++-33-3*</code>	必須	必須	必須	必須
<code>libXp-1.0.0-8*</code>	必須	オプション	必須	必須
<code>libXmu-1*</code>	必須	オプション	必須	必須
<code>libXtst-1*</code>	必須	オプション	必須	必須
<code>pam-0*</code>	必須	オプション	オプション	オプション
<code>rpm-build-4*</code>	必須	オプション	オプション	必須
<code>libaio-0*</code>	必須	必須	オプション	必須
<code>libstdc++-4*</code>	必須	必須	必須	必須
<code>libXft-2*</code>	必須	オプション	オプション	必須
<code>compat-db-4*</code>	必須	オプション	オプション	必須
<code>elfutils-libs-0*</code>	必須	オプション	オプション	必須
<code>elfutils-0*</code>	必須	オプション	オプション	必須
<code>libgcc-4*</code>	必須	オプション	必須	オプション
<code>compat-glibc-2*</code>	必須	オプション	必須	オプション
<code>openmotif22-2*</code>	必須	オプション	必須	オプション
<code>audit-libs-1*</code>	必須	オプション	オプション	オプション
<code>glibc-2*</code>	必須	オプション	オプション	オプション
<code>glibc-common-2*</code>	必須	オプション	オプション	オプション
<code>glibc-headers-2*</code>	オプション	必須	オプション	必須
<code>glibc-devel-2*</code>	オプション	必須	オプション	必須
<code>compat-gcc*</code>	オプション	必須	オプション	必須
<code>libXft-2*</code>	オプション	オプション	必須	オプション
<code>libXpm-3*</code>	オプション	オプション	必須	オプション



表 5. IBM Intelligent Operations Center ターゲット・サーバー用の必須およびオプションの Linux パッケージ (続き)

パッケージ	アプリケーション・サーバー	データ・サーバー	イベント・サーバー	管理サーバー
xorg-x11-xauth*	オプション	オプション	必須	オプション
ksh-*	オプション	オプション	オプション	必須

以下のコマンドを使用して、必須パッケージを各サーバーにインストールできます。パッケージがすでにインストールされている場合、再インストールされることはありません。

#### アプリケーション・サーバー

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* pam-0*
rpm-build-4* libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0*
elfutils-0* libgcc-4* compat-glibc-2* openmotif22-2* audit-libs-1* glibc-2*
glibc-common-2*
```

#### データ・サーバー

```
yum install compat-libstdc++-33-3* libaio-0* libstdc++-4* glibc-headers-2*
glibc-devel-2* compat-gcc*
```

#### イベント・サーバー

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* libstdc++-4*
libgcc-4* compat-glibc-2* openmotif22-2* libXft-2* libXpm-3* xorg-x11-xauth*
```

#### 管理サーバー

```
yum install compat-libstdc++-33-3* libXp-1.0.0-8* libXmu-1* libXtst-1* rpm-build-4*
libaio-0* libstdc++-4* libXft-2* compat-db-4* elfutils-libs-0* elfutils-0*
glibc-headers-2* glibc-devel-2* compat-gcc* ksh-*
```

8. Java 1.6 がいずれのサーバーにもインストールされていないことを確認します。

- インストール・サーバー
- アプリケーション・サーバー
- イベント・サーバー
- データ・サーバー
- 管理サーバー

#### 関連概念:

15 ページの『前提ソフトウェア要件』

IBM Intelligent Operations Center をインストールする前に、サーバーには適切なソフトウェアをインストールしておく必要があります。

14 ページの『IBM Intelligent Operations Center ハードウェア要件』

IBM Intelligent Operations Center のインストールには、最小要件を満たす 5 つのサーバーが必要です。

#### 関連タスク:

30 ページの『Installation Manager を使用した IBM Intelligent Operations Center のインストール』

IBM Intelligent Operations Center は、付属のグラフィカル・インストーラーを使用してインストールできます。

#### 関連情報:



<http://www.redhat.com/>

## TCP/IP ネットワーキング

IBM Intelligent Operations Center をインストールする前に、サーバー間の TCP/IP ネットワーキングを正しくセットアップする必要があります。

インストール・サーバーを含め、IBM Intelligent Operations Center で使用されるすべてのサーバーは、短縮ホスト名および完全修飾ホスト名を使用して構成する必要があります。これらのホスト名は、各サーバー上で正しい IP アドレスに解決されている必要があります。構成は、DNS サーバーを使用して、または /etc/hosts ファイルに定義を追加することで実行することができます。

各サーバーの完全修飾ホスト名には、少なくとも 3 つの構成要素が必要です。例えば、myhost.mydomain.com となります。ここで、最上位のドメインは、標準インターネット・トップレベル・ドメインです。

**重要:** 短縮ホスト名および完全修飾ホスト名は、正しい大/小文字で指定する必要があります。例えば、MyCompany.MyDomain.com を mycompany.mydomain.com と指定することはできません。

IPv6 ネットワーキングは IBM Intelligent Operations Center でサポートされていますが、IPv4 も同様にインストールして構成する必要があります。IPv4 アドレスをサーバーに割り当てる必要はありませんが、IPv4 ループバック・アドレス (127.0.0.1) を有効化し、localhost ホスト名を 127.0.0.1 に解決する必要があります。

構成変更について、25 ページの表 6 に示します。これは、Linux ネットワーク構成ファイルを編集することによって IBM Intelligent Operations Center インストール・サーバーおよびターゲット・サーバーで TCP/IP ネットワーキングをセットアップするためのガイドラインです。25 ページの表 6 の構成に関する注は、単なるガイドラインです。先に説明した要件に準拠するネットワーク・セットアップで機能することを確認してください。

表 6. TCP/IP 構成のガイドライン

ファイル	注
/etc/hosts	<p>hosts ファイルは、TCP/IP 名を IP アドレスに解決します。構成に DNS サーバーがない場合は、すべてのサーバーとその IP アドレス、短縮ホスト名、および完全修飾名をこのファイルで定義する必要があります。また、ローカル・ループバック・アドレスおよびホスト名も、このファイルで定義します。</p> <p>DNS サーバーを使用している場合は、DNS で解決されているホストをこのファイルに含める必要はありません。</p> <p><b>重要:</b> IPv4 を使用している場合は、ローカル・ループバック・アドレス 127.0.0.1 を localhost および localhost.localdomain ホスト名にマップする必要があります。</p> <p>以下は、IPv4 アドレスを使用した /etc/hosts ファイルのサンプルです。</p> <pre># local loopback definitions -- do not remove # or alter these! 127.0.0.1 localhost.localdomain localhost # use the following if IPv6 is enabled in your # network definitions ::1 localhost6.localdomain localhost6  # installation server 192.168.0.205 IOC15Install.IOC15.com IOC15Install  # target runtime servers 192.168.0.211 IOC15App.IOC15.com IOC15App 192.168.0.212 IOC15Event.IOC15.com IOC15Event 192.168.0.213 IOC15DB.IOC15.com IOC15DB 192.168.0.214 IOC15Mgmt.IOC15.com IOC15Mgmt</pre> <p>IPv6 の静的アドレスを割り当てるには、IPv6 のアドレス表記を使用します。</p> <p>IPv6 アドレスと IPv4 アドレスの両方を同一のサーバーで定義することができます。</p>

表 6. TCP/IP 構成のガイドライン (続き)

ファイル	注
<p>/etc/sysconfig/network-scripts/ifcfg-<i>adapter_name</i></p>	<p>ifcfg-<i>adapter_name</i> ファイルでは、指定のネットワーク・アダプターの基本ネットワーク設定を定義します。Linux により割り当てられたネットワーク・アダプターの名前は、<i>adapter_name</i> によって指定します。<i>adapter_name</i> の代表的な値は eth0 ですが、ご使用の環境では異なる場合があります。</p> <p>IPv4 ネットワーキングの場合は、以下のパラメーターを定義する必要があります。</p> <p><b>IPADDR</b> 構成中のサーバーの IPv4 IP アドレスを指定します。</p> <p><b>NETMASK</b> 構成中のサーバーの IPv4 ネットワーク・マスクを指定します。</p> <p><b>GATEWAY</b> 構成中のサーバーの、デフォルトの IPv4 ネットワーク IP アドレスを指定します。</p> <p><b>BOOTPROTO</b> 固定 IP アドレッシングを使用している場合は、none を指定します。</p> <p><b>NM_CONTROLLED</b> ネットワーク管理サービスが ifcfg-<i>adapter_name</i> ファイルを変更できないようにするには、no を指定します。</p> <p><b>ONBOOT</b> アダプターを自動的に開始するには、yes を指定します。</p> <p><b>IPV6INIT</b> アダプターが IPv6 ネットワーキングを使用するようにする場合は、yes を指定します。</p> <p><b>IPV6ADDR</b> IPV6INIT=yes が指定されている場合は、サーバー IPv6 IP アドレスを指定します。</p> <p><b>IPV6_DEFAULTGW</b> IPV6INIT=yes が指定されている場合は、サーバー IPv6 デフォルト・ネットワーク・ゲートウェイ IP アドレスを指定します。</p>

表 6. TCP/IP 構成のガイドライン (続き)

ファイル	注
/etc/sysconfig/network	<p>network ファイルでは、汎用ネットワーク・パラメーターを指定します。</p> <p>IPv4 ネットワーキングの場合は、以下のパラメーターを定義する必要があります。</p> <p><b>NETWORKING</b> IPv4 ネットワーキングを有効にするには、yes を指定します。</p> <p><b>NETWORKING_IPV6</b> IPv6 ネットワーキングも必要な場合は、yes を指定します。</p> <p><b>HOSTNAME</b> サーバーの短縮ホスト名を指定します。</p>
/etc/resolv.conf	<p>resolv.conf ファイルは、ネットワークおよびデフォルトの検索ドメイン用の DNS サーバーを定義する場合に使用されます。DNS サーバーを使用していない場合は、このファイルは空にしてください。</p> <p>DNS サーバーを使用する場合は、resolv.conf には以下の行を含めてください。</p> <pre>search domain_name nameserver first_DNS_server nameserver second_DNS_server</pre> <p>例えば、以下のようなものがあります。</p> <pre>search yourcompany.com nameserver 10.75.20.10 nameserver 10.75.20.11</pre> <p>search の値は、デフォルトの検索ドメインを指定します。最初の nameserver の値は、DNS サーバーの IP アドレスです。2 番目の nameserver の値は、2 次 DNS サーバーを指定する場合に使用できます。2 番目の nameserver の指定はオプションです。</p>
/etc/modprobe.conf	<p>modprobe.conf ファイルでは、システムでロードされたモジュールの構成オプションを定義します。</p> <p>IPv6 ネットワーキングでは、以下の行をコメント化してサーバーをリブートすることが必要な場合があります。</p> <pre>alias ipv6 off options ipv6 disable=1</pre>

正しく構成されている場合は、各サーバーが以下のテストを正常にパスする必要があります。

1. **hostname -s** コマンドは、サーバーの定義された短縮ホスト名を返します。
2. **hostname -f** コマンドは、サーバーの完全修飾ドメインとホスト名を返します。
3. サーバーごとに短縮ホスト名を指定した **ping** コマンド (IPV6 環境の場合は **ping6** コマンド) の結果は、サーバーがアクセス可能であることを示します。

4. サーバーごとに完全修飾名を指定した **ping** コマンド (IPv6 環境の場合は **ping6** コマンド) の結果は、サーバーがアクセス可能であることを示します。

#### 関連タスク:

20 ページの『サーバーの準備』

IBM Intelligent Operations Center をインストールする前に、サーバー構成要件を満たしていることを検証してください。事前検査ツールでは、これらの要件の多くが実装済みであることを確認します。

363 ページの『IPv6 ネットワーキングが開始されない』

IPv6 ネットワーキングがサーバーで開始されない場合は、`/etc/modprobe.conf` ファイルの変更が必要な場合があります。

48 ページの『事前検査ツールの実行』

インストール・パッケージをターゲット・サーバーにアップロードする前に、事前検査ツールを実行して、ターゲット・サーバーでインストールの準備ができていないかどうかを確認します。

---

## インストール・サーバーへのインストール・パッケージのコピー

IBM Intelligent Operations Center をインストールする前に、この製品のインストール・パッケージをインストール・サーバーにコピーします。

### 始める前に

インストール・サーバーにインストール・パッケージをコピーする前に、すべてのサーバーの準備が正しく完了していることを確認してください。

### 手順

1. インストール・サーバーに、インストール・ファイル用のディレクトリー (例えば `/installHome`) を作成します。
2. 作成したディレクトリーへの絶対パスをメモしておいてください。例えば、作成したディレクトリーが `ibmadmin` ユーザー用の `installHome` の場合、絶対パスは `/home/ibmadmin/installHome` になります。他のインストールの説明では、このディレクトリー・パスを `install_home` と呼びます。
3. 物理 DVD ごとに、またはパスポート・アドバンテージからダウンロードされた ISO イメージごとに、以下を行います。
  - a. ディレクトリーを作成して DVD をマウントします。例えば、`mkdir /mnt/ba15` コマンドを実行します。
  - b. DVD をマウントします。例えば、ISO イメージを使用する場合は、`mount -o loop ISO_directory/ISO_filename /mnt/ba15` コマンドを実行します。ここで、`ISO_directory` は ISO イメージのロケーションであり、`ISO_filename` は ISO ファイルです。
  - c. DVD の内容を、ステップ 1 で作成されたディレクトリーにコピーします。例えば、ISO イメージを使用する場合は、`cp /mnt/ba15/* install_home` コマンドを実行します。
  - d. DVD をアンマウントします。例えば、ISO イメージを使用する場合は、`umount /mnt/ba15` コマンドを実行します。
4. `install_home` ディレクトリーに移動します。
5. `ba15_media_prep.sh combine` コマンドを実行します。このコマンドは、他のすべてのインストール・ステップの実行前に実行する必要があります。

注: `install_home` ディレクトリーが `/installMedia` 以外の場合は、スクリプトを実行する前に、`ba15_media_prep.sh` ファイルを編集し、`MEDIA_BASE` の値を各自の `install_home` ディレクトリーに変更

してください。

このコマンドは、DVD または ISO イメージの全体にわたって分割されているファイルを結合します。

This

#### 関連概念:

35 ページの『インストール・メディアの場所』

IBM Installation Manager では、IBM Intelligent Operations Center のインストール時に、インストール・パッケージを配置する場所をインストール担当者が指定することができます。

#### 関連タスク:

30 ページの『Installation Manager を使用した IBM Intelligent Operations Center のインストール』

IBM Intelligent Operations Center は、付属のグラフィカル・インストーラーを使用してインストールできます。

『Java ランタイム環境のインストール』

IBM Intelligent Operations Center をインストールする前に、Java 6 ランタイム環境をインストール・サーバーにインストールする必要があります。

---

## Java ランタイム環境のインストール

IBM Intelligent Operations Center をインストールする前に、Java 6 ランタイム環境をインストール・サーバーにインストールする必要があります。

### このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### 手順

1. root としてログオンするか、**su -** コマンドを実行して root アカウントに切り替えます。
2. IBM Intelligent Operations Center インストール・ファイルをコピーした先のディレクトリーに移動します。
3. **yum --nogpgcheck install install\_media/ibm-java-x86\_64-jre-6.0-10.1.x86\_64.rpm** コマンドを実行します。
4. **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre** コマンドを実行します。
5. **echo \$JAVA\_HOME** コマンドを実行して /opt/ibm/java-x86\_64-60/jre が返されることを確認することで、Java 環境を検証します。

## 関連タスク:

28 ページの『インストール・サーバーへのインストール・パッケージのコピー』

IBM Intelligent Operations Center をインストールする前に、この製品のインストール・パッケージをインストール・サーバーにコピーします。

67 ページの『プラットフォーム制御ツールの構成』

IBM Intelligent Operations Center で提供されるものとは別の Java™ JRE をインストール済みの場合は、IBM Intelligent Operations Center をインストールした後で、プラットフォーム制御ツールが使用する JRE ロケーションを定義する必要があります。

『Installation Manager を使用した IBM Intelligent Operations Center のインストール』

IBM Intelligent Operations Center は、付属のグラフィカル・インストーラーを使用してインストールできます。

---

## Installation Manager を使用した IBM Intelligent Operations Center のインストール

IBM Intelligent Operations Center は、付属のグラフィカル・インストーラーを使用してインストールできます。

### 始める前に

製品パッケージをインストール・サーバーの *install-home* ディレクトリーにコピーしてから、以下のステップに従ってください。

### このタスクについて

インストール中は進行状況が表示されます。ただし、インストール・タスクはターゲット・サーバー上でリモートに実行されるため、進行状況表示はインストールの真の残り時間を示しているわけではありません。34 ページの『インストール・コンポーネント』に、各コンポーネントの概算のインストール時間が示されています。

いずれかの時点でインストールを取り消す場合は、IBM Installation Manager ユーザー・インターフェースの「キャンセル」をクリックします。

**重要:** 最初のコンポーネントのインストールに成功した後は、**launchpad.sh** コマンドを実行しないでください。インストールを変更するためのオプションは提供されていません。代わりに、ステップ 24 (32 ページ) に示すとおり、**/opt/IBM/InstallationManager/eclipse/IBMIM** コマンドを使用してインストーラーを再始動してください。

### 手順

1. **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre** コマンドを実行します。
2. **BA\_1.5\_GUI\_Installer\_Lite\_Launchpad.zip** ファイルを、*install\_home* に解凍します。
3. **install\_home/launchpad.sh** コマンドを実行して、インストール・ランチパッドを開始します。
4. IBM Installation Manager をインストールします。
  - a. 「**IBM Installation Manager のインストール (Install IBM Installation Manager)**」をクリックします。
  - b. 「次へ」をクリックします。
  - c. ライセンス情報を読んでください。



- d. ライセンス条項に同意する場合は、「使用条件の条項に同意します」を選択してから、「次へ」をクリックします。 インストールが続行されます。
- e. ライセンス条項に同意しない場合は、「使用条件の条項に同意しません」を選択してから、「次へ」をクリックします。 インストールは終了します。
- f. IBM Installation Manager をインストールする場所を選択します。
- g. 「次へ」をクリックします。
- h. 「インストール」をクリックします。
- i. IBM Installation Managerを再始動します。

IBM Installation Manager がインストールされます。

5. IBM Installation Manager がインストールされたら、IBM Installation Manager を閉じて再始動する必要があります。 IBM Installation Manager をランチパッドから起動すると、IBM Intelligent Operations Center 用のトポロジー・ファイルがピックアップされます。
6. 「**IBM Intelligent Operations Center のインストール**」をクリックします。
7. IBM Intelligent Operations Center - バージョン 1.5 パッケージを選択します。
8. 「次へ」をクリックします。
9. ライセンス情報を読んでください。
  - a. ライセンス条項に同意する場合は、「使用条件の条項に同意します」を選択してから、「次へ」をクリックします。 インストールが続行されます。
  - b. ライセンス条項に同意しない場合は、「使用条件の条項に同意しません」を選択してから、「次へ」をクリックします。 インストールは終了します。
10. インストール用の「共有リソース・ディレクトリー (Shared Resource Directory)」を指定します。 インストール・サーバーを使用して製品をインストールするために IBM Installation Manager を使用した場合はいつでも、このディレクトリーが使用されます。サーバー上で使用可能なスペースが最も大きいドライブを指定するようにしてください。
11. 「次へ」をクリックします。
12. 「新規パッケージ・グループの作成 (Create a new package group)」を選択して、新規パッケージ・グループを作成します。「IBM Intelligent Operations Center」を選択します。
13. インストール・ディレクトリーの名前を指定します。 インストール・ディレクトリーが作成されず。インストーラーは、必要に応じて、このディレクトリーの下にサブディレクトリーを作成します。
14. 「アーキテクチャー選択 (Architecture Selection)」で、64 ビットを選択します。
15. 「次へ」をクリックします。
16. すべてのオプションを選択解除します。
17. 「トポロジーの構成」を選択します。
18. 「次へ」をクリックします。
19. 構成オプションを入力します。 定義済みのパスワードはすべてメモしてください。
20. 「次へ」をクリックします。
21. インストール・オプションを確認し、「次へ」をクリックしてインストールを開始します。
22. インストールが完了したら、IBM Installation Manager およびランチパッドを閉じます。ステップ 3 (30 ページ) でランチパッドを開始した端末ウィンドウには JAVA\_HOME 環境セットが含まれているので、この端末ウィンドウは閉じないでください。 この端末ウィンドウを閉じた場合、続行する前に JAVA\_HOME をエクスポートし直す必要があります。

23. トポロジー・パスワードに入力された値の長さが 15 文字より大きい場合は、以下のようにして、ITM.ADMIN.USER.PWD のパスワードを長さ 15 文字以下で定義してください。
  - a. インストール・サーバーで、`install_home/ioc/topology/iop_lite_topo.properties` ファイルを編集します。ここで、`install_home` は、IBM Intelligent Operations Center インストール・パッケージがコピーされたディレクトリーです。
  - b. ITM.ADMIN.USER.PWD に定義されている値を、15 文字以下の値に変更します。sysadmin ユーザーにログインするときに、このパスワードがトポロジー・パスワードの代わりに使用されます。
  - c. 変更を保存します。
24. `/opt/IBM/InstallationManager/eclipse/IBMIM` コマンドを実行して、IBM Installation Manager を始動します。
25. 「変更」 > 「次へ」をクリックします。
26. 「ターゲット・サーバーの準備」を選択します。
27. 「次へ」 > 「変更」をクリックします。
28. エラーがある場合は、`/var/ibm/InstallationManager/logs/native` ディレクトリーにあるログ・ファイルを確認してください。ログ・ファイル名は、インストール・ツールが実行された際のログに相関付けるのに使用できるタイム・スタンプで始まっています。
29. ログ内で見つかったシステム関連のエラーや警告をすべて修正し、インストールを完了してから、次のコンポーネントをインストールするようにしてください。警告およびエラーの中には無視できるものもあります。例えば、IPv6 を有効にしていない場合や、構成がドメイン・ネーム・サービス (DNS) に接続されていない場合は、IPv6 に関する警告は無視できます。
30. エラーを修正したら、ステップ 25 に戻ります。システム・チェック・エラーを無視するオプションがあります。ステップ 26 のリストで、次のコンポーネントを選択します。このプロセスを、Cyber Hygiene のインストールの直前まで続けます。

**重要:** インストールの各フェーズ間でサーバーをシャットダウンしないでください。各フェーズの間でのサーバーのシャットダウンはテストされていないため、このようなシャットダウンを行うと予測不能な結果になる可能性があります。

Cyber Hygiene は、IBM Intelligent Operations Center システムに追加のセキュリティーを提供するため、ベスト・プラクティスの構成を適用します。Cyber Hygiene をインストールする前に、インストール後の構成を完了してください。インストール後の構成が完了したら、ステップ 24 に戻り、Cyber Hygiene をインストールして実行します。以前に IBM Installation Manager を実行したときに正常にインストールされたコンポーネントには、チェック・マークが付いています。これらのコンポーネントのチェック・マークを外さないでください。外すと、IBM Installation Manager を再び実行したときに、そのコンポーネントがアンインストールされてしまいます。

仮想化環境で実行している場合は、1 つのインストール・ステップが正常に完了した後で、次のコンポーネントをインストールする前に、すべてのサーバーのメモリーを指定してスナップショットを取ってください。万一エラーが発生した場合には、このスナップショットを使用して、正常な状態からインストールを再開することができます。

Cyber Hygiene がスキャンと修復を実行する時間を削減するには、セキュリティーの評価に必要なファイル・システムをすべてアンマウントします。例えば、各サーバーの `install_media` ディレクトリーは、すべてのインストール・ステップが完了した後は削除できます。このようなディレクトリーは、Cyber Hygiene の実行前に削除またはアンマウントできます。

注: Cyber Hygiene のインストールと実行は、同一ステップで行われます。

Cyber Hygiene は、システムを実動状態に移す前、またはシステムでセキュリティー・グッド・プラクティスに取り組む必要がある場合の、最終ステップとしてください。最終システムのスキャンや修復の適用ができるよう、Cyber Hygiene を実行する前に、すべてのアプリケーションおよびソリューションをインストールして構成しておいてください。

Cyber Hygiene によってシステムに変更が適用されると、他のアプリケーションおよびソリューションに問題が発生する可能性があります。例えば、他のアプリケーションおよびソリューションに、セキュリティー・グッド・プラクティスに合致しない Linux 環境要件があったとします。アプリケーションまたはソリューションをインストールまたは実行するために、システムに root ユーザーとしてログインすることが必要になる場合があります。このような場合には、Cyber Hygiene の変更の一部を一時的または永続的に変更するか、そのアプリケーションまたはソリューションのサプライヤーから別のソリューションを入手することが必要になる可能性もあります。

Cyber Hygiene の変更が行われた後は、それを変更するための自動化された方法はありません。変更には、Linux オペレーティング・システムを手動で更新するか、ファイルまたはディレクトリーについての権限を変更することが必要になります。

## 関連概念:

76 ページの『実動システムからのインストール・サービスの削除』

IBM Intelligent Operations Center のインストールが完了したら、インストール・サービスを実動システム・サーバーから削除できます。サービスの一部が保守アクティビティで必要になる可能性があるため、インストール・サーバーを保持しておくことをお勧めします。

59 ページの『インストール後の IBM Intelligent Operations Center の構成』

インストール・マネージャーを使用するかステップ・バイ・ステップで IBM Intelligent Operations Center アーキテクチャーをインストールした後で、インストールを完了するためのインストール後構成ステップをいくつか実行する必要があります。

91 ページの『Cyber Hygiene の概要』

IBM Intelligent Operations Center の Cyber Hygiene 機能は、インストール済みシステムに存在する可能性のある機密漏れを修正するサービスを提供できるように設計されています。

## 関連タスク:

20 ページの『サーバーの準備』

IBM Intelligent Operations Center をインストールする前に、サーバー構成要件を満たしていることを検証してください。事前検査ツールでは、これらの要件の多くが実装済みであることを確認します。

58 ページの『インストールの検証』

IBM Intelligent Operations Center のインストール後に、製品が正常にインストールされたことを確認します。

28 ページの『インストール・サーバーへのインストール・パッケージのコピー』

IBM Intelligent Operations Center をインストールする前に、この製品のインストール・パッケージをインストール・サーバーにコピーします。

29 ページの『Java ランタイム環境のインストール』

IBM Intelligent Operations Center をインストールする前に、Java 6 ランタイム環境をインストール・サーバーにインストールする必要があります。

## インストール・コンポーネント

IBM Intelligent Operations Center は 7 つのコンポーネントとしてインストールされます。

表 7. IBM Intelligent Operations Center インストール・コンポーネント

コンポーネント	インストールの見積時間	インストール対象
インストールの準備	事前チェック: 10 分間 アップロード: 2 時間	サーバー環境が最小要件を満たしているかがチェックされ、インストールに必要なファイルがターゲット・サーバーにコピーされます。
環境の準備	10 分間	IBM Intelligent Operations Center で要求されているように、 <code>/etc/sudoers</code> ファイルと <code>~/.ssh/known_hosts</code> ファイルが更新されます。
プラットフォームのインストールと構成	フェーズ 1: 12 時間 フェーズ 2: 3 時間	必要なプラットフォームがターゲット・サーバーにインストールされます。インストールは 2 つのフェーズに分けて実行されます。
プラットフォーム制御ツール	10 分間	IBM Intelligent Operations Center サーバーの始動、停止、および状況の照会に必要なツールが管理サーバーにインストールされます。
プラットフォームのシステム検査チェック	15 分間	ツールを使用して、主要なプラットフォーム機能がアプリケーション・サーバーにインストールされているかどうかを判別されます。

表7. IBM Intelligent Operations Center インストール・コンポーネント (続き)

コンポーネント	インストールの見積時間	インストール対象
アプリケーション	3 時間	IBM Intelligent Operations Center アプリケーションがターゲット・サーバーにインストールされます。
Cyber Hygiene	最長 1.5 時間	既知のサイバー機密漏れを軽減および改善するための機能がターゲット・サーバーにインストールされます。処理時間は、ハードウェアの速度と、ターゲット・サーバー上に余分なファイルや不要なファイルがあるかどうかで決まります。

## 構成オプション

IBM Installation Manager を使用して、IBM Intelligent Operations Center のインストール中に、インストーラーは構成オプションを指定できます。

### トポロジー・パスワード

IBM Installation Manager を使用して、インストーラーは IBM Intelligent Operations Center で使用されるパスワードを指定できます。

インストーラーは、表 8 に示されているパスワードを指定できます。

表 8. IBM Intelligent Operations Center のパスワード

パスワード	説明
トポロジー・パスワード	トポロジー・パスワードとは、インストール・プロセス中に特に要求されたパスワードと、passwd として定義され、変更できない iicsystemuser パスワードを除く、IBM Intelligent Operations Center インストーラーによって作成されたすべてのアカウントに対して使用されるパスワードを指します。トポロジー・パスワードは、 <b>createSecretKey</b> コマンドによって作成された秘密鍵も保護します。  1 つのアカウントのパスワードは 15 文字を超えることはできません。トポロジー・パスワードの長さが 15 文字を超える場合、このアカウントのパスワードを再定義するための特別な構成ステップ実行する必要があります。
管理ユーザー・パスワード	Linux ユーザー ibmadmin に対して設定された管理者パスワード。このユーザーは、ターゲット・サーバーのコンポーネントを管理するときに、プラットフォーム制御ツールによって使用されます。
暗号化シード	暗号化シード値は、ユーザー・パスワードと、データベース内の他の機密データを暗号化するために使用されます。暗号化シードは 12 文字から 1016 文字までの印刷可能な ASCII 文字の値である必要があります。  強固なストリングを使用してください。例えば、大/小文字混合文字、数字、および特殊文字で構成され、通常の単語や句が含まれない長いストリングがそれにあたります。
暗号化ソルト	暗号化ソルト値は、ユーザー・パスワードと、データベース内の他の機密データを暗号化するために使用されます。暗号化ソルトは、コード・ポイント 33 と 126 の間の 12 文字の印刷可能な ASCII 文字の値である必要があります。

## インストール・メディアの場所

IBM Installation Manager では、IBM Intelligent Operations Center のインストール時に、インストール・パッケージを配置する場所をインストール担当者が指定することができます。

インストール担当者は、表9 に示されているインストール・ディレクトリーを指定できます。

表9. IBM Intelligent Operations Center のインストール・ディレクトリー

ディレクトリー	説明	推奨値
ローカル・イメージ・ベース・ディレクトリー	IBM Intelligent Operations Center インストール・ファイルを含むインストール・サーバーのディレクトリーの名前。これは、インストール・ツールの実行前にインストール・メディア・ファイルがコピーされたディレクトリーです。その他のインストールの説明では、このディレクトリーを <i>install_media</i> と呼びます。	/installMedia
ローカル・イメージ一時ディレクトリー	インストール時に一時ファイルを格納するために使用される、インストール・サーバーのディレクトリー。	/installMedia
ローカル・バックアップ・ディレクトリー	このディレクトリーは、内部専用です。	/tmp/loc/backup
リモート・イメージ・ディレクトリー	インストール対象のパッケージがコピーされる、ターゲット・サーバーのディレクトリー。	/installMedia/loc/image
リモート・スクリプト・ディレクトリー	実行対象のインストール・スクリプトがコピーされる、ターゲット・サーバーのディレクトリー。	/installMedia/loc/script

#### 関連タスク:

28 ページの『インストール・サーバーへのインストール・パッケージのコピー』

IBM Intelligent Operations Center をインストールする前に、この製品のインストール・パッケージをインストール・サーバーにコピーします。

## データ・サーバーのロケーション

IBM Installation Manager を使用して、IBM Intelligent Operations Center のインストール中に、インストーラーはデータ・サーバーへの接続を定義できます。

インストーラーは、表 10 に示されているデータ・サーバーの接続オプションを指定できます。

表 10. IBM Intelligent Operations Center データ・サーバーの接続情報

オプション	説明	推奨値
データ・サーバー・ホスト名	サーバーの完全修飾ホスト名。	なし。値はインストール済み環境によって異なります。
データ・サーバー・ユーザー	インストール・プロセスの間に使用される Linux ユーザー・アカウント。	root
データ・サーバー・パスワード	「データ・サーバー・ユーザー」に指定されているアカウントのパスワード。	なし。値はインストール済み環境によって異なります。

サーバーへの接続をテストするには、「**接続のテスト**」をクリックします。



## アプリケーション・サーバーのロケーション

IBM Installation Manager を使用して、IBM Intelligent Operations Center のインストール中に、インストーラーはアプリケーション・サーバーへの接続を定義できます。

インストーラーは、表 11 に示されているアプリケーション・サーバーの接続オプションを指定できます。

表 11. IBM Intelligent Operations Center アプリケーション・サーバーの接続情報

オプション	説明	推奨値
アプリケーション・サーバー・ホスト名	サーバーの完全修飾ホスト名。	なし。値はインストール済み環境によって異なります。
アプリケーション・サーバー・ユーザー	インストール・プロセスの間に使用される Linux ユーザー・アカウント。	root
アプリケーション・サーバー・パスワード	「アプリケーション・サーバー・ユーザー」に指定されているアカウントのパスワード。	なし。値はインストール済み環境によって異なります。

サーバーへの接続をテストするには、「**接続のテスト**」をクリックします。

## イベント・サーバーのロケーション

IBM Installation Manager を使用して、IBM Intelligent Operations Center のインストール中に、インストーラーはイベント・サーバーへの接続を定義できます。

インストーラーは、表 12 に示されているイベント・サーバーの接続オプションを指定できます。

表 12. IBM Intelligent Operations Center イベント・サーバーの接続情報

オプション	説明	推奨値
イベント・サーバー・ホスト名	サーバーの完全修飾ホスト名。	なし。値はインストール済み環境によって異なります。
イベント・サーバー・ユーザー	インストール・プロセスの間に使用される Linux ユーザー・アカウント。	root
イベント・サーバー・パスワード	「イベント・サーバー・ユーザー」に指定されているアカウントのパスワード。	なし。値はインストール済み環境によって異なります。

サーバーへの接続をテストするには、「**接続のテスト**」をクリックします。

## 管理サーバーのロケーション

IBM Installation Manager を使用して、IBM Intelligent Operations Center のインストール中に、インストーラーは管理サーバーへの接続を定義できます。

インストーラーは、表 13 に示されている管理サーバーの接続オプションを指定できます。

表 13. IBM Intelligent Operations Center 管理サーバーの接続情報

オプション	説明	推奨値
管理サーバー・ホスト名	サーバーの完全修飾ホスト名。	なし。値はインストール済み環境によって異なります。

表 13. IBM Intelligent Operations Center 管理サーバーの接続情報 (続き)

オプション	説明	推奨値
管理サーバー・ユーザー	インストール・プロセスの間に使用される Linux ユーザー・アカウント。	root
管理サーバー・パスワード	「管理サーバー・ユーザー」に指定されているアカウントのパスワード。	なし。値はインストール済み環境によって異なります。

サーバーへの接続をテストするには、「**接続のテスト**」をクリックします。

## Cyber Hygiene の構成

IBM Installation Manager を使用して、IBM Intelligent Operations Center のインストール中に、インストーラーは Cyber Hygiene に必要なオプションを指定できます。

インストーラーは、表 14 に示されている Cyber Hygiene オプションを指定できます。

表 14. IBM Intelligent Operations Center の Cyber Hygiene オプション

オプション	説明	推奨値
GRUB パスワード	システムのブート・ローダー・パスワード。すべてのターゲット・サーバーにこのパスワードが使用されます。	お客様によって指定され、お客様の組織のパスワード・ポリシーと整合するパスワード。
リモート root ログインの無効化	すべてのターゲット・サーバーの root ユーザーに対してリモート・アクセスが無効になるかを定義します。	<p>選択したオプションとともに、チェック・ボックスが表示されます。このオプションをクリアすることはできません。リモート root ログインを無効にする必要があります。このオプションが表示されることによって、インストーラーはリモート root ログインが無効になっていることを認識します。</p> <p>この構成によって、コンソールからの root としてのログオンや、サーバーへのログオン時の su コマンドを使用した root ユーザーへの切り替えが無効になることはありません。</p>

## Installation Manager を使用したインストールの再開

インストールが失敗した場合、そのインストールを再開することができます。

### このタスクについて

インストールが失敗した場合は、そのセッション中に行われた変更がインストール・ツールによってロールバックされます。複数のインストール・コンポーネントを選択していた場合、一部のステップが正常に完了していたとしても、すべての選択済みのステップがロールバックされます。

失敗したインストールを再開するには、以下のようにします。

### 手順

1. 「アプリケーション」 > 「IBM Installation Manager」 > 「IBM Installation Manager」をクリックします。



2. どのコンポーネントも正常にインストールされなかった場合は、「新規」を選択して、最初からインストールを再開します。
3. 1 つ以上のコンポーネントが正常にインストールされていた場合は、「変更」を選択して、既存のインストールの変更内容をそのままにしておきます。 インストールするコンポーネントを選択します。

注: インストーラーを使用して、一度に 1 つずつコンポーネントをインストールすることを推奨します。 こうすることにより、後続のコンポーネントのインストールが失敗した場合に、正常にインストールされたコンポーネントのロールバックを限定することができます。

---

## IBM Intelligent Operations Center のステップ・バイ・ステップでインストール

IBM Intelligent Operations Center は、ステップ・バイ・ステップでインストール手順およびスクリプトを使用してインストールできます。

### インストール・パッケージの準備

インストール・スクリプトを実行する前に、インストール・パッケージを解凍して準備する必要があります。

### このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。 以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### 手順

1. インストール・パッケージを *install\_home* にコピーします。
2. インストール・パッケージを解凍します。
3. *BA\_1.5\_GUI\_Installer\_Lite\_Launchpad.zip* を、*install\_home* ディレクトリーに解凍します。
4. *install\_home/repository/native* ディレクトリーに移動します。
5. *com.ibm.iop.ba.lite\_1.5.0.9.zip* を、*install\_home* ディレクトリーに解凍します。
6. *com.ibm.iop.cat.lite\_1.5.0.9.zip* を、*install\_home* ディレクトリーに解凍します。
7. *com.ibm.iop.isp.lite\_1.5.0.zip* を、*install\_home/isp/* ディレクトリーに解凍します。
8. *com.ibm.iop.cyber.hygiene.install.lite\_1.5.0.zip* を、*install\_home/ch* ディレクトリーに解凍します。
9. **cp ../ files/com.ibm.iop.cyber.hygiene.scripts.lite\_1.5.0.zip [install-home]/ch/install** コマンドを実行します。
10. *com.ibm.iop.ioc.solution.lite\_1.5.0.20120807.1518.zip* を、*install\_home/ioc/spec* ディレクトリーに解凍します。
11. *com.ibm.iop.ioc.topology.lite\_1.5.0.20120807.1518.zip* を、*install\_home/ioc/topology* ディレクトリーに解凍します。
12. **find install\_home -name ¥\*.sh -exec chmod +x {} ¥;** コマンドを実行します。
13. **find install\_home -name ¥\*.sh -exec dos2unix {} ¥;** コマンドを実行します。

## インストール・スクリプトの検証

コマンドを実行して、インストーラー上の文書を表示することができます。これは、インストール・パッケージが作動可能であることも示しています。

### このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### 手順

1. `root` としてログオンするか、`su -` コマンドを実行して `root` アカウントに切り替えます。
2. `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` コマンドを実行します。
3. `install_home/ioc/bin/ba.sh` コマンドを実行します。インストール文書が表示されます。

## インストール・プロパティのカスタマイズ

インストール・プロパティ・ファイルおよびトポロジー・プロパティ・ファイルは、インストール・スクリプトで必要とされる定義を提供します。

### このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### 手順

オプション: 必要な場合は、`install_home/ioc/resource/custom.properties` ファイルを編集して、以下のプロパティ値を変更してください。ファイル内の、表 15 にリストされていないプロパティ値は変更しないでください。

表 15. IBM Intelligent Operations Center のインストール・プロパティ

プロパティ	説明	デフォルト値
<code>image.basedir.local</code>	IBM Intelligent Operations Center インストール・ファイルを含むインストール・サーバーのディレクトリーの名前。これは、インストール・ツールの実行前にインストール・メディア・ファイルがコピーされたディレクトリーです。その他のインストールの説明では、このディレクトリーを <i>install_media</i> と呼びます。	<code>/installMedia</code>
<code>image.tmpdir.local</code>	インストール時に一時ファイルを格納するために使用される、インストール・サーバーのディレクトリー。	<code>/installMedia</code>
<code>backup.local</code>	このディレクトリーは、内部専用です。	<code>/tmp/loc/backup</code>
<code>Unix.image.basedir.remote</code>	インストール対象のパッケージがコピーされる、ターゲット・サーバーのディレクトリー。	<code>/installMedia/loc/image</code>

表 15. IBM Intelligent Operations Center のインストール・プロパティ (続き)

プロパティ	説明	デフォルト値
Unix.script.basedir.remote	実行対象のインストール・スクリプトがコピーされる、ターゲット・サーバーのディレクトリー。	/installMedia/loc/script
connection.timeout	ターゲット・サーバーへの接続を待つ時間 (ミリ秒)。この時間が過ぎると接続は失敗します。	120000
waiting.time	失敗した接続を再試行する前に待つ時間 (ミリ秒)。	120000
retry.count	失敗した接続を再試行する回数。この回数を超えるとインストールは失敗します。	6

変更しなかった場合は、デフォルト値が使用されます。

#### 関連概念:

44 ページの『パスワード情報』

IBM Intelligent Operations Center ソリューションで使用されるさまざまなユーザー ID のパスワードは、トポロジー・プロパティ・ファイルで定義します。セキュリティ上の理由により、IBM Intelligent Operations Center の出荷時に設定されているデフォルトのパスワードは、変更してください。

## インストール・トポロジー・ファイル

IBM Intelligent Operations Center は、トポロジー・ファイルを使用してインストールされます。トポロジー・ファイルは、IBM Intelligent Operations Center を複数のサーバーにわたってデプロイするときに使用するパラメーターおよび値を定義した XML ファイルであり、コンポーネントをデプロイするために使用するシーケンスを定義します。

テキスト・エディターでトポロジー・ファイルを編集すると、エラーが入り込む可能性があります。このため、お客様がカスタマイズ可能なプロパティは、すべてトポロジー・プロパティ・ファイルで定義されます。トポロジー・テンプレート・ファイルは、トポロジーの構造を提供します。

**parameterizeTopology** コマンドは、トポロジー・プロパティ・ファイルで定義された名前/値のペアと、トポロジー・テンプレート・ファイルで提供された構造を取得し、インストール時に使用される有効なトポロジー・ファイルを作成します。

IBM Intelligent Operations Center は、以下のトポロジー・ファイルを提供します。

ファイル名	用途
<code>install_home/ioc/resource/custom.properties</code>	インストール・メディアのロケーション、作業ディレクトリー、およびその他のプロパティを定義します。このファイルは、お客様の環境のニーズに合わせて編集することができます。
<code>install_home/ioc/topology/iop_lite_topo.properties</code>	お客様がカスタマイズ可能なデプロイメント用プロパティ (ホスト名およびパスワードを含む) を定義します。このファイルは、お客様の環境のニーズに合わせて編集することができます。
<code>install_home/ioc/topology/iop_lite_topo.template.xml</code>	デプロイするトポロジーの構造を定義します。このファイルは、プロパティ・ファイルで定義された値を使用します。このファイルは編集しないでください。

ファイル名	用途
<code>install_home/ioc/topology/iop_lite_topo.xml</code>	デプロイするトポロジーを定義します。このファイルは、 <b>parameterizeTopology</b> コマンドによって、プロパティおよびテンプレート・ファイル内の情報を使用して作成されます。インストール障害から復旧するために必要な場合を除き、このファイルは編集しないでください。
<code>install_home/ioc/topology/iop_lite_topo.chk</code>	IBM Intelligent Operations Center のインストール済み環境に対し、サーバーが適切に構成されているかどうかを判断するために、事前検査ツールで使用する規則を定義します。このファイルは編集しないでください。

#### 関連タスク:

55 ページの『プラットフォーム制御ツールのインストール』

プラットフォーム制御ツールは、IBM Intelligent Operations Center サーバー環境を管理するために使用されます。このツールは、本製品とは別にインストールします。

### トポロジー・プロパティ・ファイル

トポロジー・プロパティ・ファイルは、IBM Intelligent Operations Center の、お客様がカスタマイズ可能なデプロイメント用プロパティを定義します。このファイルは、お客様の環境のニーズに合わせて編集する必要があります。付属のトポロジー・プロパティ・ファイル内のプロパティのうち、ここに記載されていないものは変更しないでください。

トポロジー・プロパティ・ファイルを変更した後は、コピーを安全な場所に保存してください。このファイルには、システムのユーザー名およびパスワードなどの、セキュリティ上重要な情報が平文で記載されています。無許可のユーザーがこのファイルにアクセスすると、そのユーザーはシステムへの全アクセス権限を持つことになります。

トポロジー・プロパティ・ファイルは、インストール後に以下の方法で使用できます。

- パスワードを忘れた場合に、パスワード情報のリポジトリとして。
- システムでパスワードを変更する場合に、パスワードのリポジトリとして。変更済みのトポロジー・プロパティ・ファイルを使用して、プラットフォーム制御ツールで使用するパスワードを更新することができます。
- システムの再インストールが必要な場合に、インストール情報のバックアップとして。トポロジー・プロパティ・ファイルを使用すると、インストール・パラメーターをすべて再定義する必要がなくなります。

#### 関連タスク:

47 ページの『トポロジー・ファイルの生成』

IBM Intelligent Operations Center のインストール・ステップを実行する前に、インストールに必要なパラメーターを使用してトポロジー・ファイルを生成します。

#### ターゲット・サーバー情報:

トポロジー・プロパティ・ファイルの `SERVERS` セクションでは、ターゲット・サーバーのプロパティを定義します。

43 ページの表 16 に、トポロジー・プロパティ・ファイルで指定可能な、サーバーのプロパティ値を示します。

表 16. ターゲット・サーバーのプロパティ

プロパティ	説明
DB.1.HOST	データ・サーバーのホスト名
DB.1.ACCOUNT.PWD	データ・サーバーの root パスワード
DB.1.SSH_PORT	データ・サーバーへの ssh アクセス用のポート番号
APP.1.HOST	アプリケーション・サーバーのホスト名
APP.1.ACCOUNT.PWD	アプリケーション・サーバーの root パスワード
APP.1.SSH_PORT	アプリケーション・サーバーへの ssh アクセス用のポート番号
EVENT.1.HOST	イベント・サーバーのホスト名
EVENT.1.ACCOUNT.PWD	イベント・サーバーの root パスワード
EVENT.1.SSH_PORT	イベント・サーバーへの ssh アクセス用のポート番号
MGMT.1.HOST	管理サーバーのホスト名
MGMT.1.ACCOUNT.PWD	管理サーバーの root パスワード
MGMT.1.SSH_PORT	管理サーバーへの ssh アクセス用のポート番号

**重要:** ホスト名の値は、大/小文字を区別して入力された、完全修飾ホスト名である必要があります。例えば、IOC15App.IOC15.com は、ioc15app.ioc15.com と同じではありません。

ssh ポート番号は、サーバーごとに設定可能です。ただし、構成済みのポート番号は、プラットフォーム制御ツールでのみ使用されます。ポート 22 は、各サーバー上での ssh アクセスに向けて使用可能にする必要があります。インストール時の、IBM Intelligent Operations Center による ssh アクセスには、ポート 22 が必須です。

#### ディレクトリー・サービス情報:

トポロジー・プロパティ・ファイルでは、ユーザー・パスワードと、その他ディレクトリー内の機密データを暗号化するために使用する値を定義します。

暗号化は、LDAP.SEED および LDAP.SALT という 2 つの値に基づいています。

値は印刷可能な ASCII 文字である必要があります。印刷可能な ASCII 文字とは、コード・ポイント値が 33 から 126 までの文字です。ブランク・スペースは使用できません。

表 17. ディレクトリー・サービスのプロパティ

プロパティ	説明
LDAP.SEED	<p>コード・ポイント 33 から 126 の間の印刷可能な ASCII 文字で構成される、12 文字から 1016 文字のストリング。</p> <p>強固な暗号方式のストリングを使用してください。例えば、大/小文字混合文字、数字、および特殊文字で構成され、通常の単語や句が含まれない長いストリングがそれにあたります。</p>

表 17. ディレクトリー・サービスのプロパティー (続き)

プロパティー	説明
LDAP.SALT	コード・ポイント 33 から 126 の間の印刷可能な ASCII 文字で構成される 12 文字のストリング。 <b>重要:</b> LDAP.SALT は、正確に 12 文字の長さにする必要があります。文字数がそれ以上またはそれ以下の値を使用すると、インストールは失敗します。

LDAP.SEED および LDAP.SALT の値をシステムの外部に記録しておいてください。これらの値は、ディレクトリー項目をエクスポートまたは複製する必要がある場合に、必要になります。

### パスワード情報:

IBM Intelligent Operations Center ソリューションで使用されるさまざまなユーザー ID のパスワードは、トポロジー・プロパティー・ファイルで定義します。セキュリティ上の理由により、IBM Intelligent Operations Center の出荷時に設定されているデフォルトのパスワードは、変更してください。

パスワードには、英数字 (a から z、A から Z、0 から 9) のみを使用できます。別途説明がない限り、パスワードは 30 文字以内にする必要があります。

表 18. パスワード・プロパティー

プロパティー	関連付けられるユーザー名	説明
LDAP.DB.PWD	dsrdbm01	LDAP ディレクトリーのデータベース
LDAP.ADMIN.DN.PWD	cn=root	LDAP 管理者バインド
LDAP.BIND.DN.PWD	cn=bind	LDAP バインド
LDAP.PROXY.INSTANCE.PWD	tdsproxy	LDAP プロキシ・インスタンス
LDAP.PROXY.ADMIN.DN.PWD	cn=root	LDAP プロキシ管理者バインド
LDAP.PROXY.BIND.DN.PWD	cn=bind	LDAP プロキシ・バインド
TAM.SECMASTER.PWD	なし	セキュリティ・サービスのマスター・パスワード  このユーザーには、ターゲット・サーバー上で root ユーザーと同等の特権が認可されます。このユーザーに与えられるアクセス権限はこのように大きいため、このパスワードは必ず、他のパスワードとは異なる長整数値にして、安全に保管してください。
TAM.WEBSEAL.ADMIN.PWD	sec_master	セキュリティ・サービスの管理者  このユーザーには、ターゲット・サーバー上で root ユーザーと同等の特権が認可されます。このユーザーに与えられるアクセス権限はこのように大きいため、このパスワードは必ず、他のパスワードとは異なる長整数値にして、安全に保管してください。
WBM.DB.USER.PWD	db2ibm	ビジネス・アクティビティー・モニター・サービスのデータベース



表 18. パスワード・プロパティ (続き)

プロパティ	関連付けられるユーザー名	説明
WODM.DB.USER.PWD	db2wodm	意思決定管理サービスのデータベース
WODM.ADMIN.UID.PWD	resAdmin1	意思決定管理サービスの管理者
WODM.DEPLOYER.UID.PWD	resDeployer1	意思決定管理サービス規則のデプロイヤー
WODM.MONITOR.UID.PWD	resMonitor1	意思決定管理サービス・モニター
WODM.DB.DC.USER.PWD	wodmdc	意思決定コンソールのデータベース
WODM.rtsAdmin.UID.PWD	rtsAdmin	意思決定コンソールの管理者
WODM.rtsConfig.UID.PWD	rtsConfig	意思決定コンソールの構成
WODM.rtsUser.UID.PWD	rtsUser	意思決定コンソールのユーザー
UDDI.DB.USER.PWD	db2uddi	UDDI サービスのデータベース
IHS.KEYSTORE.PWD	なし	HTTP サーバーの鍵ストア
WAS.ADMIN.ACCOUNT.PWD	waswebadmin	アプリケーション・サービスの管理者
WAS.LTPA.PWD	なし	LTPA トークン
PORTAL.ADMIN.ACCOUNT.PWD	waswebadmin	WebSphere® Portal サーバー用の WebSphere Application Server コンソールの管理者
PORTAL.ADMIN.UID.PWD	wpsadmin	WebSphere Portal サーバーの管理者
PORTAL.DB.USER.PWD	db2port1	WebSphere Portal データベース
OMNIBUS.ADMIN.ACCOUNT.PWD	netcool	イベント・サービスの管理者
IMPACT.WAS.ACCOUNT.PWD	wasadmin	システム・イベント・サービスの管理者
TSRM.WAS.ADMIN.PWD	waswebadmin	サービス要求マネージャーの管理者
TSRM.DB.USER.PWD	maximo	サービス要求マネージャーのデータベース
TSRM.ADMIN.USER.PWD	maxadmin	サービス要求マネージャーの管理者
TSRM.REG.USER.PWD	maxreg	サービス要求マネージャーのユーザー
TSRM.INITADM.USER.PWD	maxintadm	サービス要求マネージャーの統合ユーザー
MGMT.WAS.ADMIN.PWD	waswebadmin	アプリケーション・サービスの管理者
TEPS.DB.USER.PWD	itmuser	Enterprise Portal のデータベース
TIM.STORE.PWD	なし	ID 管理ストア
TIM.ADMIN.USER.PWD	waswebadmin	ID マネージャーの管理者
DOMINO.USER.PWD	notes	コラボレーション・ユーザー
DOMINO.ORG.PWD	IBM	コラボレーション組織
DOMINO.ADMIN.PWD	notes admin	コラボレーションの管理者
DOMINO.ST.ADMIN.PWD	wpsadmin	コラボレーション・ポータル管理者
DOMINO.ST.BIND.PWD	wpsbind	コラボレーション LDAP バインド
DEFAULT.PWD.DAS	dausr1、dausr2、dausr3、dausr4、 dausr5、dausr6、dausr7、dausr8	データベース・サービスの管理サーバー



表 18. パスワード・プロパティ (続き)

プロパティ	関連付けられるユーザー名	説明
DEFAULT.PWD.DB2	db2inst1、 db2inst2、 db2inst3、 db2inst4、 db2inst5、 db2inst6、 db2inst7、 db2inst8	データベース・サービスのデータ・サーバー
DEFAULT.PWD.IHS	ihsadmin	HTTP サーバー
DEFAULT.PWD.MQM	mqm	メッセージング・サービスのユーザー
MQM.CONN.USER.PWD	mqmconn	メッセージング・サービスの接続
DEFAULT.PWD.TAI	taiuser	アプリケーション・サービスのセキュリティ
ITM.ADMIN.PWD	sysadmin	システム管理の管理者 <b>制約事項:</b> パスワードは 15 文字以内である必要があります。
IOP.ADMIN.USER.PWD	ibmadmin	システム管理ツール  このユーザーには、ターゲット・サーバー上で root ユーザーと同等の特権が認可されます。 プラットフォーム制御ツールは、このユーザー名の下で実行されます。 このユーザーに与えられるアクセス権限はこのように大きいため、このパスワードは必ず、他のパスワードとは異なる長整数値にして、安全に保管してください。
IOP.USER.USER.PWD	ibmuser	システム的一般ユーザー

#### 関連概念:

77 ページの『第 3 章 ソリューションの保護』

IBM Intelligent Operations Center は不可欠な操作の中核を成しているため、このソリューション内のセキュリティは重要です。 セキュリティを確保するためには、デフォルト設定を把握していることと、ソリューションのユーザーを管理して正しいレベルのアクセス権限をすべてのユーザーに付与することが重要です。

#### 関連タスク:

40 ページの『インストール・プロパティのカスタマイズ』

インストール・プロパティ・ファイルおよびトポロジー・プロパティ・ファイルは、インストール・スクリプトで必要とされる定義を提供します。

#### 関連資料:

80 ページの『サンプル・ユーザー』

IBM Intelligent Operations Center のデプロイメント中に、サンプル・ユーザーが作成されます。

### トポロジー・パスワードの作成

トポロジー・パスワードは、インストール・プロセス中に、ソリューション・トポロジーを定義するファイルを暗号化するため、およびそのファイルにアクセスするために使用されます。

## このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### 手順

1. root としてログオンするか、**su -** コマンドを実行して root アカウントに切り替えます。
2. **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre** コマンドを実行します。
3. *install\_home/ioc* ディレクトリーに移動します。
4. **bin/ba.sh createSecretKey -p password** コマンドを実行します。ここで、*password* は、トポロジー用に作成するパスワードです。このコマンドは、*install\_home/ioc/resource/ioc.keystore* ファイルを作成します。このファイルには、トポロジー・プロパティー・ファイルを暗号化するために使用される鍵が含まれています。*ioc.keystore* ファイルも、**createSecretKey** コマンドで指定されているパスワードを使用して暗号化されます。インストール用のパスワードおよび鍵を変更するには、*install\_home/ioc/resource/ioc.keystore* ファイルを削除してから、**createSecretKey** コマンドを再実行します。他のインストール・ステップで使用する場合に備えて、パスワードをメモしておいてください。

### 関連タスク:

『トポロジー・ファイルの生成』

IBM Intelligent Operations Center のインストール・ステップを実行する前に、インストールに必要なパラメーターを使用してトポロジー・ファイルを生成します。

## トポロジー・ファイルの生成

IBM Intelligent Operations Center のインストール・ステップを実行する前に、インストールに必要なパラメーターを使用してトポロジー・ファイルを生成します。

## このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### 手順

1. root としてログオンするか、**su -** コマンドを実行して root アカウントに切り替えます。
2. **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre** コマンドを実行します。
3. *install\_home/ioc/topology* ディレクトリーに移動します。
4. *iop\_lite\_topo.properties* ファイルを編集して、ご使用の環境に必要な変更を加えます。
5. **cp iop\_lite\_topo.template.xml iop\_lite\_topo.xml** コマンドを実行して、トポロジー・テンプレート・ファイルをトポロジー・ファイルにコピーします。
6. *install\_home/ioc* ディレクトリーに移動します。
7. **bin/ba.sh parameterizeTopology -t iop\_lite\_topo -r topology/iop\_lite\_topo.properties -p password** コマンドを実行します。ここで、*password* は、トポロジー・パスワードです。トポロジー・プロパティー・ファイルに定義されているパラメーターが、トポロジー・ファイルに適用されます。

- オプション: トポロジー・ファイル内のパスワードを暗号化するには、**bin/ba.sh encryptTopology -t iop\_lite\_topo -p password** コマンドを実行します。ここで、*password* は、トポロジー・パスワードです。

**重要:** トポロジー・ファイル内のパスワードのみが暗号化されます。その他のファイル (トポロジー・プロパティ・ファイルなど) の中のパスワードは暗号化されません。

#### 関連概念:

42 ページの『トポロジー・プロパティ・ファイル』

トポロジー・プロパティ・ファイルは、IBM Intelligent Operations Center の、お客様がカスタマイズ可能なデプロイメント用プロパティを定義します。このファイルは、お客様の環境のニーズに合わせて編集する必要があります。付属のトポロジー・プロパティ・ファイル内のプロパティのうち、ここに記載されていないものは変更しないでください。

#### 関連タスク:

46 ページの『トポロジー・パスワードの作成』

トポロジー・パスワードは、インストール・プロセス中に、ソリューション・トポロジーを定義するファイルを暗号化するため、およびそのファイルにアクセスするために使用されます。

## 事前検査ツールの実行

インストール・パッケージをターゲット・サーバーにアップロードする前に、事前検査ツールを実行して、ターゲット・サーバーでインストールの準備ができているかどうかを確認します。

### このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### 手順

- root としてログオンするか、**su -** コマンドを実行して root アカウントに切り替えます。
- export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre** コマンドを実行します。
- install\_home/ioc* ディレクトリーに移動します。
- bin/ba.sh precheckTopology -t iop\_lite\_topo -p password** コマンドを実行します。ここで、*password* は、トポロジー・パスワードです。各サーバーに対する事前検査のテストごとに、メッセージが表示されます。各テストの状態は、[Pass] または [Fail] です。すべてのテストの実行後に、失敗したテストをすべて示す要約が表示されます。
- 失敗があった場合は、適切なアクションを実行して問題を修正し、失敗がなくなるまで事前検査ツールを再実行してください。

### タスクの結果

メッセージ **CHK0101W** が発行された場合は、環境に構成済みの DNS サーバーが存在しないか、DNS サーバーにご使用のサーバーが定義されていません。/etc/hosts ファイル内で固定 IP アドレッシングを使用してサーバーを定義してある場合は、この警告を無視できます。

## 関連概念:

24 ページの『TCP/IP ネットワーキング』

IBM Intelligent Operations Center をインストールする前に、サーバー間の TCP/IP ネットワーキングを正しくセットアップする必要があります。

## Linux セキュリティー設定

プラットフォーム制御ツールを使用可能にするには、Linux セキュリティー設定を変更する必要があります。

設定を変更するには、一連のコマンドを実行するか、またはスクリプトを使用します。

スクリプトは、コマンドで指示された変更を実行します。コマンドがご使用のインストール済み環境のニーズを満たしていない場合、またはスクリプトを使用したセキュリティ変更が企業プロセスにより許可されていない場合は、個別コマンドを使用して設定を変更してください。

## Linux セキュリティー設定の手動による調整

一連のコマンドを実行することにより、必要な Linux セキュリティー設定を行うことができます。

### 手順

1. インストール・サーバーで、root としてログオンするか、**su -** コマンドを実行して root アカウントに切り替えます。
2. プラットフォーム制御ツールを使用可能にするには、以下を実行します。これらのステップは、以下のターゲット・サーバーごとに実行する必要があります。
  - アプリケーション・サーバー
  - データ・サーバー
  - イベント・サーバー
  - 管理サーバー
  - a. **visudo** コマンドを実行します。 /etc/sudoers ファイルが編集用に開きます。
  - b. 文字 **i** を入力して、ファイルの変更を行うことができる挿入モードに変更します。
  - c. 以下の行を見つけます。

```
#%wheel ALL=(ALL) NOPASSWD: ALL
```

この行を次のように変更します。

```
%wheel ALL=(ALL) NOPASSWD: ALL
```
  - d. ファイル末尾に以下の行を追加します。

```
Defaults:%wheel !requiretty
```
  - e. Esc キーを押します。挿入モードが終了します。
  - f. **:wq** を入力します。ファイルが保存されます。
  - g. **exit** コマンドを実行します。システムはインストール・サーバーのログインに戻ります。
- 4 つのサーバーのすべてについて完了すると、Linux セキュリティーにより、wheel グループのユーザーは、**sudo** コマンドを使用して、システム・コマンドをローカルまたはリモート・セッションから実行できます。

#### 関連タスク:

『スクリプトを使用した Linux セキュリティー設定の調整』  
スクリプトを実行することにより、必要な Linux セキュリティー設定を行うことができます。

### スクリプトを使用した Linux セキュリティー設定の調整

スクリプトを実行することにより、必要な Linux セキュリティー設定を行うことができます。

#### このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

#### 手順

1. *install\_home/ioc* ディレクトリーに移動します。
2. **bin/install-prepare-env.sh -d *install\_home/ioc* -f *topology/iop\_lite\_topo.properties* -p *password*** コマンドを実行します。ここで、*password* は、トポロジー・パスワードです。

#### 関連タスク:

49 ページの『Linux セキュリティー設定の手動による調整』  
一連のコマンドを実行することにより、必要な Linux セキュリティー設定を行うことができます。

## installTopology コマンド

**installTopology** コマンドは、トポロジー・ファイル内の情報を使用して IBM Intelligent Operations Center をインストールします。

IBM Intelligent Operations Center のインストールにトポロジー・ファイルを使用する前に、**installTopology** コマンドは、インストール・ファイルがターゲット・サーバーにコピーされているかどうかを検査します。ファイルがまだコピーされていない場合、**installTopology** コマンドは、先に進む前に、必要なファイルをコピーします。

**installTopology** コマンドは、トポロジー・ファイルをガイドとして使用して、IBM Intelligent Operations Center の各コンポーネントをインストールし、必要な構成を行います。インストール中は、インストールの進行を示すメッセージが表示されます。

**installTopology** コマンドの処理中にエラーが発生した場合、1 つ以上のコンポーネントのインストールが失敗した原因を解決した後で、インストールを再開できる場合があります。失敗したインストールは、トポロジー・ファイルのインストール状況により示されます。

注: 仮想環境では、**installTopology** コマンドを実行するより前に、正常に完了した各インストールの後で、環境のスナップショットを作成することが推奨されます。

#### インストール状況

トポロジー・ファイルの **Status** 属性は、各コンポーネントのインストール状況を示します。**installTopology** コマンドを実行した場合、コンポーネントの状況に応じて、51 ページの表 19 に示されているアクションが実行されます。

表 19. インストール状況およびアクション

値	状況	installTopology のアクション
New	コンポーネントはインストールされていません。	状況は <b>Uncertain</b> に変化し、コンポーネントがインストールされます。コンポーネントのインストールが成功すると、状況は <b>Ready</b> に変わります。
Ready	コンポーネントは正常にインストールされました。	<b>installTopology</b> コマンドを再び実行した場合、このコンポーネントのインストールはスキップされます。
Uncertain	コンポーネントが正常にインストールされなかったか、インストールが進行中です。	コンポーネントがインストールされます。コンポーネントのインストールが成功すると、状況は <b>Ready</b> に変わります。

## IBM Intelligent Operations Center のコンポーネントのインストール用オプション

IBM Intelligent Operations Center のインストールには何時間もかかる場合があります。必要な時間が大きいため、IBM Intelligent Operations Centerは、1 フェーズと複数フェーズのいずれでもインストールできます。

単一フェーズでのインストールでは、すべてのコンポーネントがインストールされるまで、またはインストール中に障害が発生するまで、インストール・プロセスが実行されます。インストールが失敗した場合は、最初からインストールを再開する必要があります。

複数フェーズでのインストールでは、インストール・プロセスは 3 つの別個のフェーズに分割されます。

### uploadTopology

インストール・サーバーからターゲット・サーバーにインストール・ファイルをコピーします。

#### フェーズ 1

IBM Intelligent Operations Center の一部のコンポーネントをインストールし、残りのコンポーネントをインストールするためのベースを作成します。

#### フェーズ 2

IBM Intelligent Operations Center の残りのコンポーネントをインストールします。

仮想化環境で実行している場合、再始動が必要になる場合は、各フェーズ後にスナップショットを取る必要があります。

**uploadTopology** フェーズは別個のコマンドとして実行します。インストール・ファイルが既にターゲット・サーバーにコピーされている場合、再びコピーされることはありません。

実行するフェーズは、トポロジー・プロパティ・ファイルで定義されています。**Status.Phase1** プロパティおよび **Status.Phase2** プロパティは、**installTopology** コマンドの実行時にインストール・フェーズを実行するかどうかを決定します。New に設定されている場合は、フェーズが実行されます。Ready に設定されている場合は、フェーズがスキップされます。

## 単一フェーズでの IBM Intelligent Operations Center アーキテクチャーのインストール

IBM Intelligent Operations Center で使用されているアーキテクチャーは、単一フェーズでインストールできます。仮想化環境でインストールする場合、インストールを単一フェーズで実行すると、インストール・プロセス中にスナップショットを取ることはできません。



## このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### 手順

1. インストール・サーバーで端末ウィンドウを開き、**root** としてログオンします。 **root** としてログオンしていない場合、**su -** コマンドを実行して **root** アカウントに切り替えます。
2. インストールに必要なファイルをターゲット・サーバーにコピーして、IBM Intelligent Operations Center をインストールします。
  - a. *install\_home/ioc* ディレクトリーに移動します。
  - b. **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre** コマンドを実行します。
  - c. **bin/ba.sh installTopology -t iop\_lite\_topo -p password** コマンドを実行します。ここで、*password* はトポロジーのパスワードです。

必要なインストール・ファイルがターゲット・サーバーにコピーされ、IBM Intelligent Operations Center がインストールされます。

インストールの進行状況を示すメッセージが表示されます。このメッセージはインストールされるコンポーネントの状況を示します。この状況は次のいずれかになります。

#### [ OK ]

コンポーネントは正常にインストールされました。

#### [ Fail ]

コンポーネントのインストールは失敗しました。

## タスクの結果

インストール処理には、14 時間ほどかかる場合があります。すべてのメッセージが [ OK ] 状況で完了すれば、IBM Intelligent Operations Center アーキテクチャーは正常にインストールされています。

## 複数フェーズでの IBM Intelligent Operations Center アーキテクチャーのインストール

IBM Intelligent Operations Center で使用されているアーキテクチャーは、複数フェーズでインストールできます。複数フェーズ・インストールを使用すると、インストール・プロセス全体が完了するのを待たずに、インストールの問題を早期に解決することができます。仮想化環境でインストールする場合は、インストールを複数フェーズで実行することで、インストール・プロセスの実行時にスナップショットを取ることもできます。

## このタスクについて

**重要:** インストールの各フェーズ間でサーバーをシャットダウンしないでください。各フェーズの間でのサーバーのシャットダウンはテストされていないため、このようなシャットダウンを行うと予測不能な結果になる可能性があります。

### 手順

1. インストール・サーバーで端末ウィンドウを開き、**root** としてログオンします。 **root** としてログオンしていない場合、**su -** コマンドを実行して **root** アカウントに切り替えます。
2. **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre** コマンドを実行します。



3. インストール・ファイルをターゲット・サーバーにコピーします。
  - a. `install_home/ioc` ディレクトリーに移動します。
  - b. `bin/ba.sh uploadImage -t iop_lite_topo -threadCount 4 -p password` コマンドを実行します。ここで、`password` は、トポロジー・パスワードです。 `-threadCount` パラメーターは、インストール・ファイルをコピーするときに使用するスレッドの数を指定します。この値は、必要に応じて変更できます。

各ターゲット・サーバーに必要なファイルが、インストール・サーバーからターゲット・サーバーにコピーされます。このステップの実行には、2 時間ほどかかる場合があります。

アップロードの進行を示すメッセージが表示されます。メッセージは、アップロードされるコンポーネントの状況を示します。この状況は次のいずれかになります。

[ OK ]

コンポーネントが正常にアップロードされました。

[ Fail ]

コンポーネントのアップロードが失敗しました。

4. オプション: 仮想化環境でインストールしている場合は、すべてのターゲット・サーバーのスナップショットを取ってください。ディスク・スペースと処理時間を節約するには、スナップショットを取る前に仮想マシンをシャットダウンします。スナップショットの取得後に、仮想マシンを再始動してください。後続のインストール処理中にエラーが発生した場合は、スナップショットを使用して、このポイントからインストールを再開できます。

5. インストール・フェーズ 1 の実行準備をします。

- a. テキスト・エディターを使用して、トポロジー・プロパティー・ファイル `install_home/ioc/topology/iop_lite_topo.properties` を編集します。
- b. 状況値を以下のように変更します。

```
Status.Phase1="New"  
Status.Phase2="Ready"
```

ここでは、第 1 フェーズをインストールし、第 2 フェーズをスキップするよう、インストール・プログラムに指示しています。

- c. `install_home/ioc` ディレクトリーに移動します。
- d. `cp topology/iop_lite_topo.template.xml topology/iop_lite_topo.xml` コマンドを実行します。トポロジー・テンプレート・ファイルが、トポロジー・ファイルにコピーされます。
- e. `bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p password` コマンドを実行します。ここで、`password` は、トポロジー・パスワードです。トポロジー・プロパティー・ファイルに定義されているプロパティー値が、トポロジー・ファイルに適用されます。
- f. オプション: `bin/ba.sh encryptTopology -t iop_lite_topo -p password` コマンドを実行します。ここで、`password` は、ユーザーのトポロジー・パスワードです。トポロジー・ファイル内のパスワードが、指定されたトポロジー・パスワードを使用して暗号化されます。

6. インストール・フェーズ 1 を実行します。

- a. `install_home/ioc` ディレクトリーに移動します。
- b. `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` コマンドを実行します。
- c. `bin/ba.sh installTopology -t iop_lite_topo -p password` コマンドを実行します。ここで、`password` はトポロジーのパスワードです。

このインストールでは、IBM Intelligent Operations Center に必要となる、基本コンポーネントをインストールします。このステップの実行には、9 時間ほどかかる場合があります。

インストールの進行状況を示すメッセージが表示されます。このメッセージはインストールされるコンポーネントの状況を示します。この状況は次のいずれかになります。

**[ OK ]**

コンポーネントは正常にインストールされました。

**[ Fail ]**

コンポーネントのインストールは失敗しました。

7. オプション: 仮想化環境でインストールしている場合は、すべてのターゲット・サーバーのスナップショットを取ってください。スナップショットを取る前には、仮想サーバーをシャットダウンしないでください。スナップショットを取る際は、仮想マシンのメモリーのスナップショットも含めてください。後続のインストール処理中にエラーが発生した場合は、スナップショットを使用して、このポイントからインストールを再開できます。

8. インストール・フェーズ 2 の実行準備をします。

- a. テキスト・エディターを使用して、トポロジー・プロパティ・ファイル `install_home/ioc/topology/iop_lite_topo.properties` を編集します。

- b. 状況値を以下のように変更します。

```
Status.Phase1="Ready"  
Status.Phase2="New"
```

ここでは、第 2 フェーズをインストールし、第 1 フェーズをスキップするよう、インストール・プログラムに指示しています。

- c. `install_home/ioc` ディレクトリーに移動します。

- d. `cp topology/iop_lite_topo.template.xml topology/iop_lite_topo.xml` コマンドを実行します。トポロジー・テンプレート・ファイルが、トポロジー・ファイルにコピーされます。

- e. `bin/ba.sh parameterizeTopology -t iop_lite_topo -r topology/iop_lite_topo.properties -p password` コマンドを実行します。ここで、`password` は、トポロジー・パスワードです。トポロジー・プロパティ・ファイルに定義されているプロパティ値が、トポロジー・ファイルに適用されます。

- f. オプション: `bin/ba.sh encryptTopology -t iop_lite_topo -p password` コマンドを実行します。ここで、`password` は、ユーザーのトポロジー・パスワードです。トポロジー・ファイル内のパスワードが、指定されたトポロジー・パスワードを使用して暗号化されます。

9. インストール・フェーズ 2 を実行します。

- a. `install_home/ioc` ディレクトリーに移動します。

- b. `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` コマンドを実行します。

- c. `bin/ba.sh installTopology -t iop_lite_topo -p password` コマンドを実行します。ここで、`password` はトポロジーのパスワードです。

このインストールでは、IBM Intelligent Operations Center に必要となる、残りのコンポーネントをインストールします。このステップの実行には、4 時間ほどかかる場合があります。

インストールの進行状況を示すメッセージが表示されます。このメッセージはインストールされるコンポーネントの状況を示します。この状況は次のいずれかになります。

**[ OK ]**

コンポーネントは正常にインストールされました。

## [ Fail ]

コンポーネントのインストールは失敗しました。

### タスクの結果

すべてのメッセージが [ OK ] 状況で完了すれば、IBM Intelligent Operations Center アーキテクチャーは正常にインストールされています。

## ステップ・バイ・ステップでインストール中の IBM Intelligent Operations Center アーキテクチャーのインストールの再開

アーキテクチャーのインストールが失敗した場合、そのインストールを再開することができます。

### このタスクについて

失敗したインストールを再開するには、以下のようにします。

### 手順

1. トポロジー・ファイルを編集画面で表示し、どのコンポーネントが失敗したのかを判別します。これは、Status="Uncertain" で示されています。
2. エラーの原因を判別し、訂正してください。 インストール収集必須ツールは、確認用のインストール・ログを収集する場合に使用できます。
3. **installTopology** コマンドを再実行します。 インストールが再試行されます。 Status="New" および Status="Uncertain" のコンポーネントは、すべてインストールされます。 Status="Ready" のコンポーネントは、正常にインストール済みなので、スキップされます。

### 次のタスク

インストールが失敗したコンポーネントについては、正常にインストールされない場合があります。 その場合は、**installTopology** コマンドの実行前に環境を再作成してから、インストールを再開する必要があります。 仮想化されている環境の場合は、その環境のスナップショットを使用すると、システムを **installTopology** コマンドが実行される前の状態に素早く戻すことができます。

#### 関連タスク:

330 ページの『インストール収集必須ツールの実行』

IBM Intelligent Operations Center のインストール中には、ログ・ファイルが生成されます。 ツールを使用して、これらのログ・ファイルを分析用に収集することができます。

## プラットフォーム制御ツールのインストール

プラットフォーム制御ツールは、IBM Intelligent Operations Center サーバー環境を管理するために使用されます。 このツールは、本製品とは別にインストールします。

### 始める前に

プラットフォーム制御ツールをインストールする前に、IBM Intelligent Operations Center 製品をインストールしておく必要があります。

## このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### 手順

1. インストール・サーバーで端末ウィンドウを開き、**root** としてログオンします。 **root** としてログオンしていない場合、**su -** コマンドを実行して **root** アカウントに切り替えます。
2. *install\_home/isp/mgmt/setup* ディレクトリーに移動します。
3. **./iopmgmt-install.sh -f install\_home/ioc/topology/iop\_lite\_topo.properties -p password** コマンドを実行します。ここで、*password* は、ツールにアクセスするために使用するパスワードです。このパスワードは、ツールの実行時に必要になるので、覚えておいてください。すべてのコンポーネントが [ OK ] 状況でインストールされたことが表示されていれば、プラットフォーム制御ツールは正常に管理サーバーにインストールされています。
4. オプション: IBM Intelligent Operations Center で提供されている Java を使用しない場合は、管理サーバーで、*/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh* ファイルおよび */opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh* ファイルを編集してください。各ファイルの **export JAVA\_HOME=** の値を、サーバー上の Java JRE ロケーションに変更します。

### 次のタスク

プラットフォーム制御ツールを使用してサービスの開始、停止、および照会を実行して、プラットフォーム制御ツールが正しくインストールされたことを確認してください。

#### 関連概念:

41 ページの『インストール・トポロジー・ファイル』

IBM Intelligent Operations Center は、トポロジー・ファイルを使用してインストールされます。トポロジー・ファイルは、IBM Intelligent Operations Center を複数のサーバーにわたってデプロイするときに使用するパラメーターおよび値を定義した XML ファイルであり、コンポーネントをデプロイするために使用するシーケンスを定義します。

#### 関連タスク:

216 ページの『サービスの開始』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサーバーで実行中のサービスを開始することができます。

219 ページの『サービスの停止』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスを停止できます。

222 ページの『サービス状況の照会』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスの状況を判別することができます。

## システム検査チェック・ツールのインストール

システム検査チェック・ツールを使用して、IBM Intelligent Operations Center 内のコンポーネントの運用状況を検査することができます。このツールは、本製品とは別にインストールします。

## 始める前に

システム検査チェック・ツールをインストールする前に、IBM Intelligent Operations Center 製品をインストールしておく必要があります。

## このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

## 手順

1. インストール・サーバーで端末ウィンドウを開き、**root** としてログオンします。 **root** としてログオンしていない場合、**su -** コマンドを実行して **root** アカウントに切り替えます。
2. **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre** コマンドを実行します。
3. *install\_home*/cat/bin ディレクトリーに移動します。
4. **./install-cat-lite.sh -d install\_home/cat -f install\_home/ioc/topology/iop\_lite\_topo.properties -p password** コマンドを実行します。ここで、*password* は、トポロジー・パスワードです。

注: このコマンドは、*install\_home*/cat/bin ディレクトリーから実行する必要があります。すべてのコンポーネントが [ OK ] 状況でインストールされたことが表示されていれば、システム検査チェック・ツールは正常にインストールされています。

5. すべての IBM Intelligent Operations Center サーバーを再始動します。
  - a. プラットフォーム制御ツールを使用して、すべての IBM Intelligent Operations Center サーバーをシャットダウンします。
  - b. オペレーティング・システムからすべてのサーバーをシャットダウンして、再始動します。
  - c. プラットフォーム制御ツールを使用して、すべての IBM Intelligent Operations Center サーバーを開始します。

## 次のタスク

システム検査チェック・ツールを実行して、システム検査チェック・ツールが正しくインストールされたことを確認してください。

### 関連タスク:

232 ページの『システム検査チェック・ツールの使用方法』

システム検査チェック・ツールは、IBM Intelligent Operations Center システムから成るサービスの運用状況を判別するために使用します。

219 ページの『サービスの停止』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスを停止できます。

216 ページの『サービスの開始』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサーバーで実行中のサービスを開始することができます。

## IBM Intelligent Operations Center アプリケーションのインストール

システム検査チェックやプラットフォーム制御ツールなどの IBM Intelligent Operations Center アーキテクチャーをインストールした後に、IBM Intelligent Operations Center アプリケーションをインストールします。

## 始める前に

IBM Intelligent Operations Center アーキテクチャーをインストールして、すべてのサービスを開始する必要があります。

### 手順

1. インストール・サーバーで端末ウィンドウを開き、`root` としてログオンします。 `root` としてログオンしていない場合、`su -` コマンドを実行して `root` アカウントに切り替えます。
2. `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` コマンドを実行します。
3. `install_home/ioc` ディレクトリーに移動します。
4. `cp topology/iop_lite_topo.xml topology/iop_lite_topo_phase2.xml` コマンドを実行します。
5. `bin/ba.sh installTopology -t ioc_lite_topo -p password` コマンドを実行します。ここで、`password` はトポロジー・パスワードです。インストール処理では、IBM Intelligent Operations Center アプリケーションがインストールされます。このステップの実行に、1 時間を要する場合があります。

インストールの進行状況を示すメッセージが表示されます。このメッセージはインストールされるコンポーネントの状況を示します。この状況は次のいずれかになります。

#### [ OK ]

コンポーネントは正常にインストールされました。

#### [ Fail ]

コンポーネントのインストールは失敗しました。

## タスクの結果

IBM Intelligent Operations Center アプリケーションが正常にインストールされると、すべてのメッセージが [ OK ] ステータスで完了します。

---

## インストールの検証

IBM Intelligent Operations Center のインストール後に、製品が正常にインストールされたことを確認します。

### 手順

すべてのサービスを開始します。

1. `start all` パラメーターを指定してプラットフォーム制御ツールを実行することによって、すべての IBM Intelligent Operations Center サービスを開始します。
  2. 表示されるメッセージを検討して、すべてのサービスが正常に開始されていることを確認します。
  3. システム検査チェックツールで、すべてのテストを実行します。
  4. すべてのテストが正常に実行されていることを確認します。
- 必要に応じて、すべてのサービスをシャットダウンして再開します。
5. `stop all` パラメーターを指定してプラットフォーム制御ツールを実行することによって、すべての IBM Intelligent Operations Center サービスを停止します。
  6. 表示されるメッセージを検討して、すべてのサービスが正常に停止されていることを確認します。
  7. 全サーバーの Linux オペレーティング・システムをシャットダウンします。
  8. 全ランタイム・サーバーをパワーダウンしてパワーアップするか、全サーバーをリブートします。



9. **start all** パラメーターを指定してプラットフォーム制御ツールを実行することによって、すべての IBM Intelligent Operations Center サービスを開始します。
10. 表示されるメッセージを検討して、すべてのサービスが正常に開始されていることを確認します。
11. システム検査チェックツールで、すべてのテストを実行します。
12. すべてのテストが正常に実行されていることを確認します。

## 次のタスク

何らかのエラーが認められた場合は、エラーを解決して、これらのステップを再実行してください。

### 関連概念:

215 ページの『製品情報』

「製品情報」ポートレットを使用して、インストール済みの IBM Intelligent Operations Center および統合された IBM Smarter Cities Software Solutions のバージョンの詳細を表示します。インストール後に適用した更新の詳細も表示できます。

### 関連タスク:

216 ページの『サービスの開始』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサーバーで実行中のサービスを開始することができます。

30 ページの『Installation Manager を使用した IBM Intelligent Operations Center のインストール』

IBM Intelligent Operations Center は、付属のグラフィカル・インストーラーを使用してインストールできます。

219 ページの『サービスの停止』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスを停止できます。

232 ページの『システム検査チェック・ツールの使用方法』

システム検査チェック・ツールは、IBM Intelligent Operations Center システムから成るサービスの運用状況を判別するために使用します。

---

## インストール後の IBM Intelligent Operations Center の構成

インストール・マネージャーを使用するかステップ・バイ・ステップで IBM Intelligent Operations Center アーキテクチャーをインストールした後で、インストールを完了するためのインストール後構成ステップをいくつか実行する必要があります。

**重要:** すべてのインストール後構成作業は、Cyber Hygiene のインストール前に実行する必要があります。

### 関連タスク:

30 ページの『Installation Manager を使用した IBM Intelligent Operations Center のインストール』

IBM Intelligent Operations Center は、付属のグラフィカル・インストーラーを使用してインストールできます。

## IPv6 用のコラボレーション・サービスの構成

インストール済み環境で IPv6 ネットワーキングを使用する場合は、コラボレーション・サービス用の構成ステップが必要です。

### このタスクについて

IPv6 ネットワーキングをコラボレーション・サービス用に構成する前に、IBM Intelligent Operations Center アーキテクチャーをインストールしておく必要があります。




## 手順

1. Lotus Domino® の資料のステップに従って、Lotus Domino を IPv6 アドレッシング用に構成します。
2. Lotus Sametime Standard の資料のステップに従って、Lotus Sametime Standard を IPv6 アドレッシング用に構成します。
3. イベント・サーバーに割り当てられている IPv4 アドレスを持つ IPv4 ネットワークを使用していない場合は、WebSphere Portal の資料に記載されたステップに従って Sametime 連絡先リスト・ポートレットのための信頼を構成してください。

### 関連情報:

 IPv6 アドレッシング用 Lotus Domino の構成

 IPv6 をサポートするための Sametime Community Server の構成

 Sametime 連絡先リスト・ポートレットのための信頼の構成

## コラボレーション・サービス用のシングル・サインオンの構成

WebSphere Portal SSO LTPA トークンをイベント・サーバーにインポートすると、ユーザーは資格情報を再入力しなくてもコラボレーション・サービスにアクセスできるようになります。

### このタスクについて

Lightweight Third Party Authentication (LTPA) トークンをインポートする前に、IBM Intelligent Operations Center アーキテクチャーをインストールしておく必要があります。

このトークンは、IBM Intelligent Operations Center アーキテクチャーのインストール時に作成されています。

## 手順

1. Lotus Notes® 8.5.x クライアントをワークステーションにインストールします。既存のインストール済み環境を使用できます。ワークステーションは、完全修飾ホスト名を使用して、TCP/IP 経由でイベント・サーバーに接続できるようにしておく必要があります。
2. アプリケーション・サーバーから、Lotus Notes を実行中のワークステーションに、`/opt/pdweb/etc/stproxy.ltpa` ファイルをコピーします。これが、コラボレーション・サービス・ディレクトリーにインポートされる LTPA トークンです。
3. イベント・サーバー から、Lotus Notes を実行中のワークステーションに、`/local/notesdata/admin.id` ファイルをコピーします。これは、コラボレーション・サービス管理者用の ID ファイルです。この ID を使用して、コラボレーション・サービス・ディレクトリーにログインします。
4. ワークステーションで Lotus Notes クライアントを開始して、`admin.id` ファイルを使用してログオンします。
  - a. Lotus Notes のログオン・パネルで、「ユーザー名」をクリックします。
  - b. `admin.id` ファイルのコピー先のディレクトリーにナビゲートし、当該ファイルを選択します。
  - c. トポロジー・プロパティー・ファイルに `DOMINO.ADMIN.PWD` プロパティー用として定義されているパスワードを入力します。
  - d. セキュリティー警告が表示された場合は、「はい」をクリックします。
5. `names.nsf` ファイルを開きます。
  - a. 「ファイル」 > 「開く」 > 「Lotus Notes アプリケーション」をクリックします。

- b. 「検索対象 (Look In)」に、イベント・サーバーの完全修飾ホスト名を入力します。
  - c. 「ファイル名」に、names.nsf と入力します。
  - d. 「開く」をクリックします。
6. 「Web」 > 「Web 構成」にナビゲートします。
  7. 「LTPA トークン用の Web SSO 構成 (Web SSO Configuration for LTPA Token)」を選択して、「文書の編集」をクリックします。
  8. 「鍵」 > 「WebSphere LTPA 鍵のインポート (Import WebSphere LTPA Keys)」をクリックします。既存の鍵の上書きに関する警告を受け取った場合は、「OK」をクリックします。
  9. stproxy.ltpa ファイルをコピーした場所へのパスを入力します。「OK」をクリックします。
  10. LTPA トークンのパスワードを入力します。このパスワードは、トポロジー・プロパティー・ファイルの WAS.LTPA.PWD プロパティーに定義されています。
  11. 「OK」 > 「保存して閉じる」をクリックします。
  12. プラットフォーム制御ツールを使用して、コラボレーション・サービスを再開します。
    - a. 管理サーバーにログオンして、端末ウィンドウを開きます。
    - b. `su -ibmadmin` を実行します。
    - c. `/opt/IBM/ISP/mgmt/scripts/IOControl.sh stop st password` を実行します。ここで、*password* は、プラットフォーム制御ツールのインストール時に定義されたプラットフォーム制御ツールのパスワードです。
    - d. `/opt/IBM/ISP/mgmt/scripts/IOControl.sh start st password` を実行します。ここで、*password* は、プラットフォーム制御ツールのインストール時に定義されたプラットフォーム制御ツールのパスワードです。

## セッション・タイムアウトの設定

セッション・タイムアウトは、セッションが終了し、ユーザーによる再度のログインが必要になるまでの、ユーザーがアイドル状態のままいることのできる時間を決定します。セッション・タイムアウトには、管理者のポータル・サービス経由でのログインを含みます。

### このタスクについて

IBM Intelligent Operations Center のインストール時には、セッション・タイムアウトは定義されていません。セッションがアイドル状態であっても、ユーザーは、ログアウトするまではログインしたままになります。

ユーザーの組織のセキュリティー・ポリシーにより、一定期間アイドルであればセッションのログアウトが必要となる場合は、以下のステップを使用して、IBM Intelligent Operations Center システムのセッション・タイムアウトを定義してください。

### 手順

1. Web ブラウザーを使用して `http://application_server:9060/ibm/console` に移動します。ここで、*application\_server* は、アプリケーション・サーバーのホスト名です。
2. トポロジー・プロパティー・ファイルの `PORTAL.ADMIN.ACCOUNT.PWD` で定義されたパスワードを指定して、waswebadmin ユーザーとしてログオンします。
3. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Servers」 > 「WebSphere Portal」をクリックします。

4. 「コンテナ設定値 (Container Settings)」 > 「セッション管理」 > 「タイムアウトの設定」をクリックします。
5. 所定のタイムアウト値を分単位で入力します。
6. 「OK」をクリックします。
7. 「保存」をクリックします。
8. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Servers」 > 「STProxyServer1」をクリックします。
9. 「コンテナ設定値 (Container Settings)」 > 「セッション管理」 > 「タイムアウトの設定」をクリックします。
10. 所定のタイムアウト値を分単位で入力します。
11. 「OK」をクリックします。
12. 「保存」をクリックします。
13. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Servers」 > 「CongnosX\_GW1」をクリックします。
14. 「コンテナ設定値 (Container Settings)」 > 「セッション管理」 > 「タイムアウトの設定」をクリックします。
15. 所定のタイムアウト値を分単位で入力します。
16. 「OK」をクリックします。
17. 「保存」をクリックします。
18. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Servers」 > 「CongnosX\_Displ1」をクリックします。
19. 「コンテナ設定値 (Container Settings)」 > 「セッション管理」 > 「タイムアウトの設定」をクリックします。
20. 所定のタイムアウト値を分単位で入力します。
21. 「OK」をクリックします。
22. 「保存」をクリックします。
23. アプリケーション・サーバーを停止して再始動します。
24. アプリケーション・サーバーで、トポロジー・プロパティ・ファイルの IOP.ADMIN.USER.PWD で定義されたパスワードを指定して、ibmadmin ユーザーとしてログオンします。
25. **sudo su -** コマンドを実行して、root ユーザーに切り替えます。
26. /opt/pdweb/etc/webseald-default.conf ファイルをテキスト・エディターで編集します。
27. SESSION CACHE SETTINGS セクションで、timeout = 0 値を、目的のセッション・タイムアウト (秒) に変更します。タイムアウトは、ポータル・サービスに設定したものと同一時間にする必要があります。ただし、ポータル値は分単位で設定し、セッション・キャッシュ設定は秒単位で指定します。セッション・キャッシュ設定のタイムアウト値は、ポータル・サービスに設定した値の、ちょうど 60 倍にする必要があります。例えば、ポータル値が 30 (分) の場合、セッション・キャッシュ設定の値は、1800 (秒) にする必要があります。
28. **/usr/bin/pdweb restart** コマンドを実行して、セキュリティー・サービスを再始動します。

## Semantic Model Services のインストールおよび構成

IBM Intelligent Operations Center には、Semantic Model Services アプリケーションおよびサンプル・モデルがあります。このサービスを使用するには、事前にサービスをインストールして構成しておく必要があります。

## Jazz チーム・サーバーの構成

IBM Intelligent Operations Center Semantic Model Servicesは、Jazz チーム・サーバーにインストールされます。IBM Intelligent Operations Center Semantic Model Services をインストールする前に、Jazz チーム・サーバーを構成しておく必要があります。

### このタスクについて

Jazz チーム・サーバーを構成する前に、IBM Intelligent Operations Center アーキテクチャーをインストールしておく必要があります。

### 手順

1. Web ブラウザーで `http://management_host:82/jts/setup` に移動します。ここで、*management\_host* は、管理サーバーの完全修飾ホスト名です。
2. ユーザー ID `iicsystemuser` とパスワード `passwd0rd` を使用してログオンします。
3. 「次へ」をクリックします。
4. 「パブリック URI の構成」ページで、「パブリック URI ルート」の値を `https://management_host:9448/jts` の形式で入力し、「パブリック URI は、一度設定すると変更できないことを了解しています」を選択します。「次へ」をクリックします。
5. 「接続のテスト」をクリックします。構成テストが成功したことを示すメッセージが表示されるのを確認してください。
6. 「次へ」をクリックして、設定を保存して先へ進みます。
7. 「データベースの構成」ページで、データベースを構成します。
  - a. 「データベース・ベンダー」には、DB2 を選択します。
  - b. 「接続タイプ」には、JDBC を選択します。
  - c. 「JDBC パスワード」には、トポロジー・プロパティ・ファイルで `DEFAULT.PWD.DB2` プロパティとして定義されている DB2 データベース・パスワードを入力します。表示されるパスワード・メッセージは無視してください。
  - d. 「JDBC ロケーション」には、`//db_host:50005/JTS:user=db2inst5;password={password};` を入力します。ここで、*db\_host* は、データ・サーバーのホスト名です。{password} スtring は、示されているとおりに入力する必要があります。パスワード値に置換しないでください。
  - e. 「接続のテスト」をクリックします。エラーが発生した場合は、検査して該当項目を訂正します。項目が正しい場合は、データ・サーバーでプラットフォーム制御ツールを使用してデータベース・サービスが開始されていることを確認してください。
  - f. Jazz テーブルがデータベースに存在していないというメッセージが表示された後で、「テーブルの作成」をクリックします。処理が完了するまでに数分かかります。
  - g. 「次へ」をクリックします。
8. 「電子メール通知を有効にする」ページで、値を「無効」に設定し、「次へ」をクリックします。
9. 「アプリケーションの登録」ページに、「新規アプリケーションは検出されませんでした」と表示されるのを確認してください。「次へ」をクリックします。
10. 「ユーザー・レジストリーのセットアップ」ページのステップ 1 で、「ユーザー・レジストリー・タイプ」に「LDAP」を選択します。
11. ステップ 2 で、Jazz チーム・サーバー・レジストリーの LDAP を構成します。
  - a. 「LDAP レジストリー・ロケーション」には、`ldap://mgmt_host:389` を入力します。ここで、*mgmt\_host* は、管理サーバーの完全修飾ホスト名です。

- b. 「基本ユーザー DN」には、OU=USERS,OU=SWG,O=IBM,C=US を入力します。
  - c. 「ユーザー・プロパティ名のマッピング」には、userId=uid,name=cn,emailAddress=mail を入力します。
  - d. 「基本ユーザー DN」には、OU=GROUPS,OU=SWG,O=IBM,C=US を入力します。
  - e. 「Jazz から LDAP グループへのマッピング」では、JazzAdmins=JazzAdmins, JazzUsers=JazzUsers, JazzDAdmins=JazzDAdmins, JazzProjectAdmins=JazzProjectAdmins, JazzGuests=JazzGuests に値が設定されていることを確認します。
  - f. 「グループ名プロパティ」には、cn を入力します。
  - g. 「グループ・メンバー・プロパティ」には、cn を入力します。
12. 「接続のテスト」をクリックします。警告メッセージが表示されたら、「詳細の表示」をクリックします。mail プロパティに関する警告の場合は、メッセージを無視できます。
  13. 「クライアント・アクセス・ライセンス・タイプ」では、「IBM Integrated Information Core - IIC モデル・サーバー (IBM Integrated Information Core - IIC Model Server)」を選択します。
  14. 「次へ」をクリックします。
  15. 「データウェアハウスの構成」では、「今はデータウェアハウスを構成しません」チェック・ボックスを選択します。
  16. 「要約」ページで、「終了」をクリックします。

## タスクの結果

これで、Jazz チーム・サーバーは作動可能になりました。

## Semantic Model Services のインストール

IBM Intelligent Operations Center には、Semantic Model Services およびサンプル・アプリケーションが用意されています。

### このタスクについて

Semantic Model Services を使用する前に、管理サーバー上に Jazz Team Server を構成する必要があります。

### 手順

1. Web ブラウザーで [http://management\\_host:82/jts/admin](http://management_host:82/jts/admin) に移動します。ここで、*management\_host* は、管理サーバーの完全修飾ホスト名です。
2. 「サーバー管理」ページで、「サーバー」 > 「構成」 > 「アプリケーションの登録」をクリックします。
3. 「登録済みアプリケーション」ページで、「追加」をクリックします。
4. 「アプリケーションの追加」ページで、モデル・サーバー・アプリケーションを追加します。
  - a. 「アプリケーション名」に、Model Server と入力します。
  - b. 「ディスカバリー URL」に、[http://management\\_host:82/modelserver/scr](http://management_host:82/modelserver/scr) と入力します。ここで、*management\_host* は、管理サーバーの完全修飾ホスト名です。
  - c. 値を選択して、「コンシューマーの秘密情報」に入力します。この値は、アプリケーションへのアクセスを提供するために使用されます。この値は、パスワードと同じセキュリティで取り扱う必要があります。
  - d. 「機能 ID」に、iicsystemuser と入力します。



「アプリケーション・タイプ」が Model Server に変更されます。

5. エラーがない場合は、「終了」をクリックします。

## Semantic Model Services の構成の検証

IBM Intelligent Operations Center には Semantic Model Services のサンプル・アプリケーションが用意されているので、それを使用して Semantic Model Services のインストールと構成が正しいかどうかを検証できます。

### 手順

1. サンプル・モデル・ファイルを準備します。
  - a. インストール・サーバーの *install\_media* ディレクトリー内で、*iic15\_2\_stagebuiltdtoserver.xx.jar* ファイルを見つけます。
  - b. 選択したディレクトリーに *iic15\_2\_stagebuiltdtoserver.xx.jar* ファイルを解凍します。これ以降のステップでは、このディレクトリーを *model\_home* と呼びます。
2. サンプル・モデルをインストールします。
  - a. *model\_home* が配置されているサーバー上の Web ブラウザーで [http://mgmt\\_host:82/iic/console](http://mgmt_host:82/iic/console) に移動します。ここで、*mgmt\_host* は、管理サーバーの完全修飾ホスト名です。
  - b. *iicsystemuser* ユーザーとして、パスワードに *passw0rd* を使用してログオンします。
  - c. 「モデル・マネージャー」 > 「オントロジー (Ontologies)」 > 「参照」をクリックします。
  - d. *install\_media/ioc/image/IIC/install/modelServices/post\_install/* ディレクトリーにナビゲートします。
  - e. *rsm.owl* ファイルを開きます。
  - f. 「ロード」をクリックします。ファイルがロードされます。
  - g. 「モデル・マネージャー」 > 「オントロジー (Ontologies)」 > 「参照」をクリックします。
  - h. *install\_media/ioc/image/IIC/install/modelServices/post\_install/* ディレクトリーにナビゲートします。
  - i. *modelServer.owl* ファイルを開きます。
  - j. 「ロード」をクリックします。ファイルがロードされます。
  - k. 「モデル・マネージャー」 > 「オントロジー (Ontologies)」 > 「参照」をクリックします。
  - l. *install\_media/ioc/image/IIC/install/ktpRuntimeServices/post\_install/* ディレクトリーにナビゲートします。
  - m. *kpi.owl* ファイルを開きます。
  - n. 「ロード」をクリックします。ファイルがロードされます。
  - o. 「モデル・マネージャー」 > 「ロード」 > 「参照」をクリックします。
  - p. *install\_media/ioc/image/IIC/samples/rdf/rsm/* ディレクトリーにナビゲートします。
  - q. *IBMOilDownstreamSampleRDF.xml* ファイルを開きます。
  - r. 「ロード」をクリックします。ファイルがロードされます。
  - s. 「モデル・マネージャー」 > 「ロード」 > 「参照」をクリックします。
  - t. *install\_media/ioc/image/IIC/samples/rdf/rsm/* ディレクトリーにナビゲートします。
  - u. *IBMOilUpstreamSampleRDF.xml* ファイルを開きます。
  - v. 「ロード」をクリックします。ファイルがロードされます。
  - w. 「モデル・マネージャー」 > 「ロード」 > 「参照」をクリックします。

- x. `install_media/ioc/image/IIC/samples/rdf/rsm/` ディレクトリーにナビゲートします。
  - y. `IBMOilDownstreamSampleReferenceRDF.xml` ファイルを開きます。
  - z. 「ロード」をクリックします。ファイルがロードされます。
  - aa. 「モデル・マネージャー」 > 「ロード」 > 「参照」をクリックします。
  - ab. `install_media/ioc/image/IIC/samples/rdf/rsm/` ディレクトリーにナビゲートします。
  - ac. `IBMOilUpstreamSampleReferenceRDF.xml` ファイルを開きます。
  - ad. 「ロード」をクリックします。ファイルがロードされます。
3. サンプル・モデルが正しくインストールされていることを確認します。
    - a. 「モデル・マネージャー」 > 「照会」 > 「照会」をクリックします。事前定義された照会が実行されます。XML 構造が、照会結果と共に表示されます。最上位のタグは `spargl` で、2 次タグ `head` および `results` があります。
    - b. 「モデル・エクスプローラー」をクリックして、モデルを表示できることを確認します。
  4. このモデルを使用して、モデル・マネージャー のインストールを検証します。
    - a. 管理サーバーの Web ブラウザーで `http://mgmt_host:82/iic/ibmoil` に移動します。ここで、`mgmt_host` は、管理サーバーの完全修飾ホスト名です。
    - b. 「IBM Oil Company」 > 「変数」をクリックします。Web サービスの URL が表示されます。

## タスクの結果

Semantic Model Services および IBMOil サンプル・モデルがインストールされます。

## Semantic Model Services のパフォーマンスの改善

IBM Intelligent Operations Center で提供されている Semantic Model Services を構成して、モデルに対して照会を実行する場合のパフォーマンスを改善できます。

### 手順

1. Web ブラウザーで `http://management_host:82/iic/console` に移動します。ここで、`management_host` は、管理サーバーの完全修飾ホスト名です。
2. 表 20 のプロパティー値を「OPCWEBSERVICE」カテゴリーに追加します。

表 20. OPCWEBSERVICE プロパティー

プロパティー	値
<code>cache.browse.timetolive.second</code>	3600
<code>cache.timetolive.second</code>	2592000
<code>cache.wait.second.after.create.action</code>	1

3. RSM カテゴリーで、以下の 67 ページの表 21 のプロパティーおよび値を更新または追加します。



表 21. RSM プロパティ

プロパティ	値
mvmViewPath.0	http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity ##iec.ch/TC57/CIMgeneric# ISA95_Site##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.ManagedBy_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity##http:// iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.has_measurement##http:// iec.ch/TC57/CIMgeneric#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric#RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIMgeneric#RSM_MeasurementValue
mvmViewPath.1	http://iec.ch/TC57/CIMgeneric# ISA95_Enterprise##http://iec.ch/TC57/CIMgeneric# RSM_OrganizationalEntity.ManagesAspectOf_PhysicalEntity ##iec.ch/TC57/CIMgeneric# ISA95_Area##http://iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.contains_PhysicalEntity##http:// iec.ch/TC57/CIMgeneric# ISA95_ProductionUnit##http://iec.ch/TC57/CIMgeneric# ISA95_WorkCenter.Contains_Equipment##http:// iec.ch/TC57/CIMgeneric# RSM_WorkEquipment##http:// iec.ch/TC57/CIMgeneric# RSM_PhysicalEntity.has_measurement##http:// iec.ch/TC57/CIMgeneric#RSM_Measurement##http:// iec.ch/TC57/CIMgeneric# RSM_Measurement.HasA_MeasurementValue##http:// iec.ch/TC57/CIMgeneric#RSM_MeasurementValue
mvmDownLevelPreRequest	3
mvmCacheProperty.0	cim:RSM_IdentifiedObject.name
mvmMaxQueryURI	500
mvmMaxSparqlEntry	4000

- 「パブリッシュ」をクリックします。新規プロパティおよび変更プロパティが保存されます。
- プラットフォーム制御ツールを使用してSemantic Model Services を再始動します。
- Web ブラウザーで `http://management_host:82/iic/console` に移動します。ここで、`management_host` は、管理サーバーの完全修飾ホスト名です。
- 必要に応じて、ソリューションまたはアプリケーション固有の変更を行ってください。変更が必要な場合には、製品またはソリューション・ドキュメンテーション内で変更が識別されます。

## プラットフォーム制御ツールの構成

IBM Intelligent Operations Center で提供されるものとは別の Java JRE をインストール済みの場合は、IBM Intelligent Operations Center をインストールした後で、プラットフォーム制御ツールが使用する JRE ロケーションを定義する必要があります。

### 手順

- 管理サーバーで、`/opt/IBM/ISP/mgmt/scripts/CommandEngine.sh` ファイルを編集します。
- `export JAVA_HOME=` を、Java JRE が使用するロケーションに変更します。
- 変更を保存します。

4. 管理サーバーで、/opt/IBM/ISP/mgmt/scripts/UpdateProperty.sh ファイルを編集します。
5. export JAVA\_HOME= を、Java JRE が使用するロケーションに変更します。
6. 変更を保存します。

#### 関連タスク:

29 ページの『Java ランタイム環境のインストール』

IBM Intelligent Operations Center をインストールする前に、Java 6 ランタイム環境をインストール・サーバーにインストールする必要があります。

## Tivoli Service Request Manager 管理パスワードの暗号化

以下の手順に従って、Tivoli Netcool/Impact で Tivoli Service Request Manager 管理パスワードを暗号化します。

### 手順

1. `http://event_host:9080/nci/main` にある Tivoli Netcool/Impact 管理コンソールにログオンします。ここで、`event_host` は、イベント・サーバーのホスト名です。ユーザー `admin` とパスワード `netcool` を使用してログオンします。
2. 「**IOC プロジェクト (IOC Project)**」をクリックします。
3. 「ポリシー」セクションで、ポリシー「**IOC\_Sample\_Password\_Encoder**」をダブルクリックします。ポリシーが「ポリシー・エディター」ウィンドウで開きます。
4. 「パスワードをここに入力 (**Enter Password Here**)」フィールドに `Maxadmin` のパスワードを入力します。パスワード `Maxadmin` は、インストール中に入力した管理ユーザー・パスワードです。
5. ポリシーを保存するには、「**保存**」をクリックします。
6. 「**ポリシーのトリガー**」アイコンをクリックします。
7. 「**実行**」をクリックします。
8. 「サービスのステータス」セクションで「**ポリシー・ロガー**」までスクロールし、「**ポリシー・ロガーのログの表示 (View log for PolicyLogger)**」(下矢印付きのアイコン)をクリックします。
9. ポリシー・ロガー・ウィンドウ内で、以下のステートメントと似たステートメントを見つけます。  
11 May 2012 14:19:12,260: [IOC\_Sample\_Password\_Encoder][pool-1-thread-46]Parser log: {aes}FF877B74ADF4DF1C2002F94ACB38FAFF
10. このステートメントから暗号化された `Maxadmin` パスワードをコピーします。以下に例を示します。  
{aes}FF877B74ADF4DF1C2002F94ACB38FAFF
11. Tivoli Netcool/Impact 管理コンソールの「ポリシー」セクションで、ポリシー「**UTILS\_LIBRARY\_IOC\_TSRM**」をダブルクリックします。ポリシーが「ポリシー・エディター」ウィンドウで開きます。
12. 以下のように `MAXAdminPassword` の値を、ステップ 10 でコピーした暗号化された値で置き換えます。  
`MAXAdminPassword = "{aes}FF877B74ADF4DF1C2002F94ACB38FAFF";`
13. ポリシーを保存するには、「**保存**」をクリックします。
14. 「**IOC プロジェクト (IOC Project)**」をクリックします。
15. 「ポリシー」セクションで、ポリシー「**IOC\_Sample\_Password\_Encoder**」をダブルクリックします。ポリシーが「ポリシー・エディター」ウィンドウで開きます。
16. 「パスワードをここに入力 (**Enter Password Here**)」フィールドで `Maxadmin` のパスワードを削除します。
17. ポリシーを保存するには、「**保存**」をクリックします。

## EventProcessor のスレッドの最小数の設定

EventProcessor のスレッドの最小数は、パフォーマンス上の理由から、25 に設定する必要があります。

### 手順

1. `http://event_host:9080/nci/main` にある Tivoli Netcool/Impact 管理コンソールにログオンします。ここで、`event_host` は、イベント・サーバーのホスト名です。
2. 「サービスのステータス」 > 「EventProcessor」をクリックします。
3. 「スレッドの最小数」に 25 と指定します。

注: 「スレッドの最小数」の値は、「スレッドの最大数」の値より大きくすることはできません。

4. 「OK」をクリックします。
5. プロセスの停止アイコンをクリックして、EventProcessor を停止します。
6. プロセスの開始アイコンをクリックして、EventProcessor を開始します。

## Default および WebContainer スレッド・プール・サイズの変更

標準操作手順のパフォーマンスを向上させるには、Default および WebContainer のスレッド・プール・サイズ設定を変更する必要があります。

### 手順

1. WebSphere Portal 管理インターフェースのイベント・サーバーで、「Intelligent Operations」 > 「管理ツール」 > 「管理コンソール」をクリックします。
2. イベント・サーバーで、「Standard Operating Procedure Application Server」をクリックします。
3. WebSphere Application Server 管理者としてログオンします。IBM Intelligent Operations Center がインストールされたときに、トポロジー・プロパティ・ファイルにおいて、ユーザー ID は `WAS.ADMIN.ACCOUNT` プロパティで定義され、パスワードは `WAS.ADMIN.ACCOUNT.PWD` プロパティで定義されました。
4. 「サーバー」 > 「アプリケーション・サーバー」 > 「MXServer1」 > 「スレッド・プール」 > 「WebContainer」をクリックします。
5. 「サイズの下限」に 50 と入力します。
6. 「サイズの上限」に 50 と入力します。
7. 「OK」をクリックします。
8. 「サーバー」 > 「アプリケーション・サーバー」 > 「MXServer1」 > 「スレッド・プール」 > 「Default」をクリックします。
9. 「サイズの下限」に 20 と入力します。
10. 「サイズの上限」に 50 と入力します。
11. 「OK」をクリックします。
12. TSRMCluster を再始動します。
  - a. 「サーバー」 > 「クラスター」をクリックします。
  - b. TSRMCluster を選択します。
  - c. 「停止」をクリックします。
  - d. 状況が赤に変わるのを待機します。
  - e. 「開始」をクリックします。

---

## Cyber Hygiene のステップ・バイ・ステップでインストールと実行

Cyber Hygiene は、IBM Intelligent Operations Center とは別個にインストールして実行します。また、他のすべての IBM Intelligent Operations Center コンポーネントのインストールおよび構成が完了して作動可能になった後で、インストールして実行する必要があります。Cyber Hygiene ではデフォルトのオペレーティング・システム構成をよりセキュアなオプション・セットに変更できるので、IBM Intelligent Operations Center システムのためのさらにセキュアな基盤を確保するために役立ちます。

### 始める前に

注: Cyber Hygiene のインストールと実行は、同一ステップで行われます。IBM Installation Manager を使用して IBM Intelligent Operations Center をインストールする場合は、以下のステップを使用しないでください。IBM Installation Manager のインストールでは、Cyber Hygiene をインストールして実行するオプションが用意されています。

Cyber Hygiene がスキャンと修復を実行する時間を削減するには、セキュリティーの評価に必要なファイル・システムをすべてアンマウントします。例えば、各サーバーの *install\_media* ディレクトリーは、すべてのインストール・ステップが完了した後は削除できます。このようなディレクトリーは、Cyber Hygiene の実行前に削除またはアンマウントできます。

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### このタスクについて

Cyber Hygiene は、IBM Intelligent Operations Center をインストールした後の最終ステップでなければなりません。スキャンおよび修復では、デフォルトのオペレーティング・システムおよび IBM Intelligent Operations Center 製品をインストールした後に存在している構成の機密漏れに対処します。適用される修復は、IBM Intelligent Operations Center サービスが正しく作動することを確認するテストが済んだものです。

Cyber Hygiene によってシステムに変更が適用されると、他のアプリケーションおよびソリューションに問題が発生する可能性があります。例えば、他のアプリケーションおよびソリューションに、セキュリティー・グッド・プラクティスに合致しない Linux 環境要件があったとします。アプリケーションまたはソリューションをインストールまたは実行するために、システムに *root* ユーザーとしてログオンすることが必要になる場合があります。このような場合には、Cyber Hygiene の変更の一部を一時的または永続的に変更するか、そのアプリケーションまたはソリューションのサプライヤーから別のソリューションを入手することが必要になる可能性もあります。

Cyber Hygiene の変更が行われた後は、それを変更するための自動化された方法はありません。変更には、Linux オペレーティング・システムを手動で更新するか、ファイルまたはディレクトリーについての権限を変更することが必要になります。

### 手順

1. インストール・サーバーで端末ウィンドウを開き、*root* としてログオンします。*root* としてログオンしていない場合、**su -** コマンドを実行して *root* アカウントに切り替えます。
2. **export JAVA\_HOME=/opt/ibm/java-x86\_64-60/jre** コマンドを実行します。JAVA\_HOME 変数が Java ランタイム環境 (JRE) に設定されます。
3. *install\_home/ch/install* ディレクトリーに移動します。

4. テキスト・エディターを使用して、`iop-ch-install.xml` ファイルを編集します。
5. `iop-ch-install.xml` ファイル内のパラメーターを、ご使用のシステムに該当する値に置き換えます。

表 22. *Cyber Hygiene* のインストール・パラメーター

パラメーター	値
<code>\${APP.1.HOST}</code>	アプリケーション・サーバーの完全修飾ホスト名
<code>\${APP.1.ACCT}</code>	SSH でアプリケーション・サーバーにアクセスするための Linux ユーザー名
<code>\${APP.1.ACCT.PWD}</code>	<code>\${APP.1.ACCT}</code> のパスワード
<code>\${APP.1.SSH_PORT}</code>	アプリケーション・サーバーの SSH ポート
<code>\${DB.1.HOST}</code>	データ・サーバーの完全修飾ホスト名
<code>\${DB.1.ACCT}</code>	SSH でデータ・サーバーにアクセスするための Linux ユーザー名
<code>\${DB.1.ACCT.PWD}</code>	<code>\${DB.1.ACCT}</code> のパスワード
<code>\${DB.1.SSH_PORT}</code>	データ・サーバーの SSH ポート
<code>\${EVENT.1.HOST}</code>	イベント・サーバーの完全修飾ホスト名
<code>\${EVENT.1.ACCT}</code>	SSH でイベント・サーバーにアクセスするための Linux ユーザー名
<code>\${EVENT.1.ACCT.PWD}</code>	<code>\${EVENT.1.ACCT}</code> のパスワード
<code>\${EVENT.1.SSH_PORT}</code>	イベント・サーバーの SSH ポート
<code>\${MGMT.1.HOST}</code>	管理サーバーの完全修飾ホスト名
<code>\${MGMT.1.ACCT}</code>	SSH で管理サーバーにアクセスするための Linux ユーザー名
<code>\${MGMT.1.ACCT.PWD}</code>	<code>\${MGMT.1.ACCT}</code> のパスワード
<code>\${MGMT.1.SSH_PORT}</code>	管理サーバーの SSH ポート

6. ファイルを保存します。
7. `install_home/ch` ディレクトリーに移動します。
8. `install_home/ch/install/iop-ch-install.sh -r iop-ch-install-messages.properties -f 'com.ibm.iop.cyber.hygiene.scripts.lite_1.5.0.zip' -d install_media/ioc/image -p GRUB_password` コマンドを実行します。ここで、`GRUB_password` は、サーバー上の GRUB ブート・ローダーのパスワードです。`GRUB_password` は、すべてのターゲット・サーバーに適用されます。サーバーの再始動時には、一般にパスワードは不要です。ただし、*Cyber Hygiene* をインストールした後は、Linux オプションを使用してサーバーを始動する場合 (単一ユーザー・モードで始動する場合など)、サーバー・コンソールで `GRUB_password` を入力する必要があります。

## タスクの結果

処理時間は、ハードウェアの速度と、ターゲット・サーバー上に余分なファイルや不要なファイルがあるかどうかで決まります。処理には最大 1.5 時間かかる場合があります。その時間中に、ターゲット・サーバーがスキャンされ、適切な修復が適用されます。

## 次のタスク

*Cyber Hygiene* のログを調べて、エラーがあるかどうかを確認します。このログには、適用された修復とオプションの手動ステップも示されます。



## 関連概念:

91 ページの『Cyber Hygiene の概要』

IBM Intelligent Operations Center の Cyber Hygiene 機能は、インストール済みシステムに存在する可能性のある機密漏れを修正するサービスを提供できるように設計されています。

## Linux オペレーティング・システムへの変更

Cyber Hygiene は、Linux オペレーティング・システムをスキャンして既知の機密漏れがあるかどうかを調べ、適宜変更を加えます。スキャンされた機密漏れと、Linux OS のポリシーおよび設定に加えられた変更は、ログに示されています。

ログには、検出されたが変更は加えられなかった機密漏れもリストされます。これには以下のようなものがあります。

- システムが既に、Cyber Hygiene で変更する場合と同様に構成されている。
- 変更のためには、システム管理者がアクションを実行するか、変更が環境にとって適切かどうかを決定する必要があります。
- 変更が、自動化スクリプトでは実行できない。例えば、機密漏れが組織全般のセキュリティー・ポリシーに関連している場合がこれに該当します。

Cyber Hygiene によって適用された修復は、必要な場合には後で変更することができます。Cyber Hygiene のログには、システムに適用された変更に関する情報が提供されています。Cyber Hygiene によって加えられた変更が他のアプリケーションまたはソリューションを使用するシステムと互換性がない場合、そのようなシステムを使用するための変更が必要になることがあります。

## Cyber Hygiene ログの確認

Cyber Hygiene をインストールして実行した後で、ログを確認して、システムに加えられた変更および残っている機密漏れを把握してください。

### このタスクについて

インストール・サーバーで、IBM Intelligent Operations Center インストール・パッケージがコピーされているディレクトリーに移動します。以下のステップでは、このディレクトリーを *install\_home* と呼びます。

### 手順

1. インストール・サーバーの `/var/ibm/InstallationManager/logs/native` ディレクトリーにある Cyber Hygiene ログを確認して、すべてのアクションがすべてのサーバーに対して実行され、完了したことを確認します。ログを見つけるには、**`fgrep yber *.log`** コマンドを実行します。このログ・ファイルには、各サーバーの情報が表示されます。通常、ログ情報に関するステップは以下のとおりです。
  - Cyber Hygiene タスクを実行する環境の準備。
  - スタンドアロン修復プログラムの実行。これにより、スキャンする必要のない機密漏れが修正されます。GRUB ブート・ローダーのパスワードを設定する、監査をオンにするなどです。
  - リモートの root ログオンの無効化。
  - 機密漏れのスキャン。これはバックグラウンドで実行され、メインタスクはスキャンが完了するまで待機します。
  - スキャン中に検出された機密漏れに対処するための、修復プログラムの実行。
  - 修復後のスキャン。これにより、初期スキャンで検出されなかった機密漏れを識別できます。

- 2 回目のスキャン中に検出された追加の機密漏れに対処するための、修復プログラムの実行。完了しなかった修復は、ログに記録されます。
2. 各ターゲット・サーバーの `/var/BA15/CH/results` ディレクトリーにある、詳細な Cyber Hygiene ログを確認します。 `standrem-date_time.log` に、スタンドアロン修復プログラムの結果が示されています。 `standrem-disableRemoteRoot-date_time.log` には、リモートの root ログオンを無効化した結果が示されています。 `scanrem-combined-log-date_time.log` には、スキャンされた修復プログラムのアクションの結果が示されています。 2 つのスキャン/修復ステップに対応する、2 つのログがあります。
    - a. ログ・ファイルで、`Vulnerability` というテキストで始まる行を確認します。各行に、実行されたアクションが示されています。これには、以下のものがあります。
      - スキャンの検出結果
      - 選択された修復
      - 適用された修復の詳細
    - b. 2 回目のスキャンおよび修復のログで `NOT DONE` というテキストで示されている修復があれば、それに関する追加の手動アクションについて調べることが必要な場合があります。

## リモートの root ログオンの再有効化

Cyber Hygiene は、`ssh` コマンドを使用した root アカントへのリモート・ログオンを無効にします。`telnet` コマンドおよび `rsh` コマンドは、Linux オペレーティング・システムでは完全に無効になります。必要に応じて、リモート・ログオンを再有効化できます。

### このタスクについて

root ユーザーに対するリモート・ログオンの再有効化は不要な場合があります。適正な特権を持つユーザーは、`su` コマンドおよび `sudo` コマンドを使用することで root ユーザーとして操作できます。root ユーザーとして操作する特権ユーザーは、監査のためにログに記録されます。

IBM Intelligent Operations Center は、`ibmadmin` ユーザーをホイール・グループに定義します。ホイール・グループのユーザーは、`sudo su -` コマンドを使用して、root としての処理を実行できます。

### 手順

`ssh` コマンドを使用したルート・ログオンを有効にするには、以下を実行します。

1. `ssh` またはリモート端末を使用して root としてリモート・ログインすることが必要なサーバーで、`/etc/ssh/sshd_config` ファイルを編集します。
2. `PermitRootLogin` パラメーターを `yes` に変更してファイルを保存します。 `ssh` コマンドを使用したりリモート・ログインを無効にする必要がある場合は、このパラメーターを `no` に変更します。
3. ファイルを保存します。
4. `service sshd restart` コマンドを実行して `ssh` サーバーを再始動します。  
リモート端末を使用した root アカントへのリモート・ログオンは、Cyber Hygiene によって無効になります。物理的にサーバーに接続された画面およびキーボードのみが、root ユーザーとしてログオンできます。リモート端末からサーバーへのリモート root ログオンを再有効化するには、以下を実行します。
5. `ssh` またはリモート端末を使用して root としてリモート・ログオンすることが必要なサーバー上で、`/etc/securetty` ファイルを編集します。
6. root ユーザーとしてリモートでログオンする権限のある端末の Linux 装置名を追加します。例えば、`ttyl` を追加する場合は、読み取り用のリストを次のように変更します。



```
console
tty1
```

端末を無効にするには、無効にする端末の前に # 文字を置きます。以下に例を示します。

```
console
#tty1
```

7. ファイルを保存します。

---

## ssh アクセスを必要とするユーザーの構成

IBM Intelligent Operations Center では、特定のユーザーに ssh アクセスとパスワードを設定する必要があります。

### このタスクについて

インストール・サーバーとすべてのターゲット・サーバーで ssh アクセスとパスワードを設定する必要があります。あるユーザーを以下に示します。

- ibmadmin
- ibmuser
- mqconn

---

## ソリューションに付属するツールのインストール

IBM Intelligent Operations Center には、ツールキットと開発ツールが付属しています。これらは、IBM Intelligent Operations Center をカスタマイズするときに使用します。

Rational® Application Developer を除き、これらのツールは、IBM Intelligent Operations Center デベロッパーズ・ツールキットの DVD またはイメージに収録されています。Rational Application Developer は、別の DVD またはイメージで IBM Intelligent Operations Center に付属しています。

### Lotus Sametime Client

Lotus Sametime Clientのインストールおよび使用に関する情報については、Lotus Domino および Lotus Notes インフォメーション・センターを参照してください。

### WebSphere Message Broker Toolkit

WebSphere Message Broker Toolkit のインストールおよび使用に関する情報については、WebSphere Message Broker インフォメーション・センターを参照してください。

### IBM WebSphere Business Monitor 開発ツールキット

IBM WebSphere Business Monitor 開発ツールキットのインストールおよび使用に関する情報については、IBM WebSphere Business Monitor インフォメーション・センターを参照してください。

### Rational Application Developer

Rational Application Developer のインストールおよび使用に関する情報については、Rational Application Developer インフォメーション・センターを参照してください。

## 関連概念:

123 ページの『KPI の作成および統合』

重要業績評価指標 (KPI) モデルは、ビジネス・モニター開発ツールキットおよび KPI 管理ポートレットを使用して作成および変更することができます。

## 関連情報:



Lotus Domino および Lotus Notes インフォメーション・センター



WebSphere Message Broker インフォメーション・センター



IBM Business Monitor インフォメーション・センター



Rational Application Developer インフォメーション・センター

---

## サンプル・ユーザーの削除

IBM Intelligent Operations Center にはサンプル・ユーザーが付属しています。セキュリティ上の理由から、IBM Intelligent Operations Center が実稼働環境にインストールされた後に、これらのユーザーを削除する必要があります。

### このタスクについて

事前に定義されているユーザーを削除するには、以下のステップを実行します。

### 手順

1. アプリケーション・サーバーで、WebSphere Portal にサインインします。
2. 「管理」ポータルで、「アクセス」 > 「ユーザーおよびグループ」 > 「すべての認証ポータル・ユーザー」をクリックします。
3. 以下のユーザーの削除アイコンをクリックします。
  - tdelorne
  - scollins
  - akelly

**重要:** 以下の必須ユーザーは削除しないでください。これらのユーザーを削除すると、IBM Intelligent Operations Center が正しく動作しなくなります。

- admin
- iicsystemuser
- maxadmin
- maxintadm
- maxreg
- notesadmin
- resAdmin1
- resDeployer1
- resMonitor1
- rtsAdmin

- rtsConfig
- rtsUser
- taiuser
- SRMSELSERVICEUSR
- wasadmin
- waswebadmin
- wpsadmin
- wpsbind
- 「PM」で始まるすべてのユーザー ID

#### 関連資料:

80 ページの『サンプル・ユーザー』

IBM Intelligent Operations Center のデプロイメント中に、サンプル・ユーザーが作成されます。

---

## 実動システムからのインストール・サービスの削除

IBM Intelligent Operations Center のインストールが完了したら、インストール・サービスを実動システム・サーバーから削除できます。サービスの一部が保守アクティビティーで必要になる可能性があるため、インストール・サーバーを保持しておくことをお勧めします。

インストールが完了し、インストールを検証した後は、インストール・プロセスのみに使用されるコンポーネントは実動システム・サーバー (アプリケーション・サーバー、イベント・サーバー、管理サーバー、データ・サーバー) から削除できます。これには以下のものがあります。

- トポロジー・プロパティ・ファイル内の `Unix.image.basedir.remote` プロパティによって定義されたディレクトリー。
- トポロジー・プロパティ・ファイル内の `Unix.script.basedir.remote` プロパティによって定義されたディレクトリー。
- トポロジー・プロパティ・ファイル内の `image.basedir.local` プロパティによって定義された `install_media` ディレクトリー。

**注:** 今後使用する必要が生じる場合に備えて、インストール・サーバーを保持しておいてください。トポロジー・プロパティ・ファイルにはパスワードが平文で含まれているため、このサーバーは安全な場所に配置する必要があります。

#### 関連タスク:

30 ページの『Installation Manager を使用した IBM Intelligent Operations Center のインストール』

IBM Intelligent Operations Center は、付属のグラフィカル・インストーラーを使用してインストールできます。

---

## 第 3 章 ソリューションの保護

IBM Intelligent Operations Center は不可欠な操作の中核を成しているため、このソリューション内のセキュリティは重要です。セキュリティを確保するためには、デフォルト設定を把握していることと、ソリューションのユーザーを管理して正しいレベルのアクセス権限をすべてのユーザーに付与することが重要です。

### デフォルト・パスワード

ソリューションを保護するための最初の作業は、すべてのデフォルト・パスワードの変更です。デフォルト・パスワードについて詳しくは、このトピックの末尾にあるリンクを参照してください。

### セキュア接続

IBM Intelligent Operations Center では、デフォルトで HTTPS が有効になっています。IBM Intelligent Operations Center 内の以下の個々のサービスの HTTPS 設定を変更することができます。

- KPI を処理するビジネス・モニター・サービス
- リソースおよび標準操作手順の管理サービス

個々のサービスの HTTPS 設定を変更する場合は、対応するポート設定も更新する必要があります。システム・プロパティ・テーブル内のこれらの設定を変更する方法については、このトピックの末尾にあるリンクを参照してください。

### ユーザー認証

ユーザー認証は、該当する機能およびデータへのユーザー・アクセス権限を提供する許可権限に関連付けられています。IBM Intelligent Operations Center は、シングル・サインオンを行うために、既存のセキュリティ・インフラストラクチャーとの統合をサポートします。

IBM Intelligent Operations Center のユーザー権限は、WebSphere Portal のユーザーおよびグループを介して管理されます。WebSphere Portal は、データ・サーバーで実行されている Tivoli Directory Server に付属する Lightweight Directory Access Protocol (LDAP) データベースを使用します。

IBM Intelligent Operations Center に付属するセキュリティ・システムは、多数のユーザー・グループ、役割、および権限を処理できます。多数のユーザー・グループ、役割、および権限を処理することで、セキュリティ体制が管理しにくくなる可能性があります。管理者には、グループと権限の数を制限することを推奨します。

### ユーザー役割と権限

役割ベースのユーザー・グループのメンバーシップにより、IBM Intelligent Operations Center へのアクセスを制御することができます。グループ内のユーザーには、彼らの役割に対応するソリューションの機能に対するアクセス権のみが付与されています。役割ベースのユーザー・グループのメンバーになることで、ユーザーは該当するタスクに集中することもできます。標準的な役割は、エグゼクティブ、監督者、およびオペレーターです。

ユーザーを IBM Intelligent Operations Center に追加するには、以下の手順を実行します。

1. 組織内のユーザーの役割に適合するグループを選択し、ユーザーをそのグループのメンバーにします。

2. ユーザーのプロファイルを完成させ、少なくともユーザー ID、名前、およびパスワードを含めます。

## データ・カテゴリと権限

IBM Intelligent Operations Center 内のデータベースに格納されているデータのセキュリティは、役割ベースのアクセスをデータベースに実装することで管理されます。 IBM Intelligent Operations Center の機能にアクセスできる場合でも、そのユーザーがすべてのデータを手に入れるわけではありません。 データ・セキュリティはサーバー・レベルで適用され、ユーザーには該当するデータのみが表示されるように設定されます。 標準的なカテゴリは、気象、輸送、気象学的、環境、インフラストラクチャー、化学、生物、安全、セキュリティ、レスキュー、火災、ヘルス、およびその他です。

## ポータル

ポータル・サービスは、必要なユーザー・セットを収容するために拡張することが可能なプラットフォームを提供します。 また、必要な組織構造を反映するよう調整できる、役割ベースのアクセス権も提供します。「**ユーザーおよびグループの管理 (Manage Users and Groups)**」ポートレットを使用して、ユーザーまたはユーザー・グループを表示、作成、および削除できます。また、グループのメンバーシップを変更することもできます。 このポートレットについて詳しくは、このトピックの末尾にあるリンクを参照してください。

### 関連概念:

44 ページの『パスワード情報』

IBM Intelligent Operations Center ソリューションで使用されるさまざまなユーザー ID のパスワードは、トポロジー・プロパティ・ファイルで定義します。 セキュリティ上の理由により、IBM Intelligent Operations Center の出荷時に設定されているデフォルトのパスワードは、変更してください。

### 関連情報:



IBM WebSphere Portal 7 の製品資料

---

## ユーザーの役割とアクセス権

IBM Intelligent Operations Center は、ユーザー役割に基づいて機能へのアクセスを制限することによってセキュリティを実装します。

IBM Intelligent Operations Center の特定の機能を使用するには、その機能を使用するために必要なアクセス権限が提供されているユーザー役割グループのメンバーである必要があります。 ユーザーは、管理者によってユーザー役割グループのメンバーに指定されます。 以下の表には、IBM Intelligent Operations Center で、ログイン・アクセス・レベルを使用して実際の役割がユーザー役割グループにどのようにマップされるかが示されています。

表 23. 仕事上の役割と IBM Intelligent Operations Center のユーザー役割グループ

仕事上の役割	責務	ユーザー役割グループ
エグゼクティブ	<ul style="list-style-type: none"> <li>• イベント、インシデント、および重要業績評価指標 (KPI) の入力要件としきい値を定義する</li> <li>• 以下に関する大まかな視覚的要約、詳細、およびレポートを表示する               <ul style="list-style-type: none"> <li>- KPI</li> <li>- イベント</li> </ul> </li> <li>• ポリシー、長期指示事項、または大まかな決定事項を伝える</li> </ul>	市統括エグゼクティブ
監督者または管理者	<ul style="list-style-type: none"> <li>• イベントとインシデントを管理する</li> <li>• KPI レポートを作成してモニターする</li> <li>• アラートを出す</li> <li>• 状況またはアクション要件の変更に関してイベントを分析する</li> <li>• 短期修正手段を決定する</li> </ul>	市統括監督者
オペレーター	<ul style="list-style-type: none"> <li>• イベント情報をモニターする</li> <li>• アラートをモニターする</li> <li>• 詳細を表示する</li> <li>• 通信を実行する</li> <li>• 以下のような追加情報を使用して、イベントまたはインシデント・データを更新する               <ul style="list-style-type: none"> <li>- 電話レポート</li> <li>- 建設または保守からの入力データ</li> </ul> </li> </ul>	市統括オペレーター
ユーザー管理者	<p>グループの定義、グループへの権限の割り当て、グループへのユーザーの割り当てなど、ユーザーのすべての側面を管理します。ユーザーに適切なアクセス・レベルを提供します。アクセス・レベルは、グループ・メンバーシップに基づいて割り当てられます。</p>	wpsadmins

役割をカスタマイズして、組織に応じてユーザーを定義する前に、IBM Intelligent Operations Center のセキュリティ・システムを把握しておきます。

## 関連タスク:

84 ページの『ユーザーまたはグループの追加』

グループを選択してユーザー・プロファイルを作成し、新規ユーザーを IBM Intelligent Operations Center に追加します。新規グループに追加するユーザー名を選択します。

## 関連資料:

81 ページの『ユーザー役割グループと許可権限』

IBM Intelligent Operations Center の機能にアクセスするための権限セットは、各ユーザー役割グループに関連付けられています。

83 ページの『ユーザー・カテゴリ・グループとデータ権限』

IBM Intelligent Operations Center のデータ・カテゴリにアクセスするための権限は、各ユーザー・カテゴリ・グループに関連付けられています。

## サンプル・ユーザー

IBM Intelligent Operations Center のデプロイメント中に、サンプル・ユーザーが作成されます。

一般的なサンプル・ユーザーは、ユーザー役割グループおよびそれに対応するアクセス権限を使用して定義されます。これらのサンプル・ユーザーは単に例として定義されたものであり、以下の表に示されています。ソリューションを管理するための他のユーザーも必要です。

表 24. IBM Intelligent Operations Center に定義されているユーザー

ユーザー ID	ユーザー役割グループ
サンプル・ユーザー	
tdelorne	市統括エグゼクティブ
scollins	市統括監督者
akelly	市統括オペレーター
必須ユーザー	
wpsadmin	wpsadmins

組織のユーザーを定義する準備が整ったら、サンプル・ユーザーのみを削除してください。wpsadmin ユーザーは削除しないでください。wpsadmin ユーザーは、IBM Intelligent Operations Center に関連する管理タスクに不可欠です。必須ユーザーについて詳しくは、このトピックの末尾にあるリンクを参照してください。

**重要:** wpsadmin ユーザーのデフォルト・パスワードを新規パスワードに置き換えてください。ポータル管理者のユーザー ID とパスワードの更新については、WebSphere Portal の資料を参照してください。



## 関連概念:

44 ページの『パスワード情報』

IBM Intelligent Operations Center ソリューションで使用されるさまざまなユーザー ID のパスワードは、トポロジー・プロパティ・ファイルで定義します。 セキュリティー上の理由により、IBM Intelligent Operations Center の出荷時に設定されているデフォルトのパスワードは、変更してください。

## 関連タスク:

75 ページの『サンプル・ユーザーの削除』

IBM Intelligent Operations Center にはサンプル・ユーザーが付属しています。 セキュリティー上の理由から、IBM Intelligent Operations Center が実稼働環境にインストールされた後に、これらのユーザーを削除する必要があります。

## 関連情報:



IBM WebSphere Portal 7 の製品資料

## ユーザー役割グループと許可権限

IBM Intelligent Operations Center の機能にアクセスするための権限セットは、各ユーザー役割グループに関連付けられています。

管理者は、ユーザーを、対応するユーザー役割グループのメンバーにすることで、そのユーザーに役割を割り当てます。 各ユーザーは、1 つ以上のユーザー役割グループのメンバーシップに割り当てられます。

次の表には、IBM Intelligent Operations Center で提供されるユーザー役割グループごとの権限がリストされています。 各ユーザー役割グループに対して、IBM Intelligent Operations Center の機能ごとに許可権限が付与されます。

表 25. IBM Intelligent Operations Center の機能および関連付けられているユーザー役割グループの権限

機能タイプ	機能名	市統括エグゼクティブ	市統括監督者	市統括オペレーター	wpsadmins
ページ	スーパーバイザー: 状況	ユーザー権限	ユーザー権限	なし	管理者権限
	スーパーバイザー: 操作	ユーザー権限	なし	なし	管理者権限
	スーパーバイザー: レポート	なし	ユーザー権限	なし	管理者権限
	オペレーター: 操作	なし	なし	ユーザー権限	管理者権限
	オペレーター: レポート	なし	なし	ユーザー権限	管理者権限
	ロケーション・マップ	なし	ユーザー権限	ユーザー権限	管理者権限
	管理	なし	なし	なし	管理者権限

表 25. IBM Intelligent Operations Center の機能および関連付けられているユーザー役割グループの権限 (続き)

ポータルレット	状況	ユーザー権限	ユーザー権限	なし	管理者権限
	重要業績評価指標のドリルダウン	ユーザー権限	ユーザー権限	なし	管理者権限
	通知	ユーザー権限	ユーザー権限	ユーザー権限	管理者権限
	連絡先	ユーザー権限	ユーザー権限	ユーザー権限	管理者権限
	マップ	ユーザー権限	なし	ユーザー権限	管理者権限
	詳細	ユーザー権限	なし	ユーザー権限	管理者権限
	マイ・アクティビティ	ユーザー権限	ユーザー権限	ユーザー権限	管理者権限
	ロケーション・マップ	なし	ユーザー権限	ユーザー権限	管理者権限
	レポート	なし	ユーザー権限	ユーザー権限	管理者権限
	Intelligent Operations Center - 製品情報	なし	なし	なし	管理者権限
	管理コンソール	なし	なし	なし	管理者権限
	システムチェック	なし	なし	なし	管理者権限
	ユーザー権限サマリー	なし	なし	なし	管理者権限
	重要業績評価指標	なし	なし	なし	管理者権限
	ロケーション・マップ・マネージャー	なし	なし	なし	管理者権限
	標準操作手順	なし	なし	なし	管理者権限
	イベント・スク립ト記述	なし	なし	なし	管理者権限
	サンプル・パブリッシャー	なし	なし	なし	管理者権限
	ユーザーおよびグループ	なし	なし	なし	管理者権限

IBM Intelligent Operations Center の許可権限は、Lightweight Directory Access Protocol (LDAP) グループに基づいて割り当てられます。これらの権限は、以下のように定義されます。

- ユーザー権限は、機能を表示および操作するためのアクセス権限を与えるためにユーザーに付与される権限です。
- 管理者権限は、以下を行うためのアクセス権限を与えるために管理者に付与される権限です。
  - 機能の構成
  - ユーザーおよびユーザー・グループの作成、変更、または削除

IBM Intelligent Operations Center のデータにアクセスするには、ユーザーは必要なデータ権限が付与されているユーザー・カテゴリ・グループのメンバーである必要があります。

## 関連概念:

90 ページの『ユーザー権限サマリー』

「ユーザー権限サマリー」ポートレットでは、IBM Intelligent Operations Center のユーザーおよびグループに関連付けられている権限を確認することができます。

78 ページの『ユーザーの役割とアクセス権』

IBM Intelligent Operations Center は、ユーザー役割に基づいて機能へのアクセスを制限することによってセキュリティを実装します。

## 関連タスク:

84 ページの『ユーザーまたはグループの追加』

グループを選択してユーザー・プロファイルを作成し、新規ユーザーを IBM Intelligent Operations Center に追加します。新規グループに追加するユーザー名を選択します。

86 ページの『グループ・メンバーシップの表示または変更』

グループ・メンバーシップを表示または変更して、IBM Intelligent Operations Center内のユーザーのアクセス権限を管理します。

## 関連資料:

『ユーザー・カテゴリー・グループとデータ権限』

IBM Intelligent Operations Center のデータ・カテゴリーにアクセスするための権限は、各ユーザー・カテゴリー・グループに関連付けられています。

## 関連情報:



IBM WebSphere Portal 7 の製品資料

## ユーザー・カテゴリー・グループとデータ権限

IBM Intelligent Operations Center のデータ・カテゴリーにアクセスするための権限は、各ユーザー・カテゴリー・グループに関連付けられています。

管理者は、ユーザーを、該当するユーザー・カテゴリー・グループのメンバーにすることで、そのユーザーにデータ・アクセス権を割り当てます。各ユーザーは、1 つ以上のユーザー・カテゴリー・グループのメンバーシップに割り当てられます。

次の表には、IBM Intelligent Operations Centerがカバーしているデータ・カテゴリーと、それに対応し、イベント、重要業績評価指標 (KPI)、およびアラート・データの特定に使用されるユーザー・カテゴリー・グループがリストされています。例えば、ユーザーが市の水道局に関連するイベントを表示できるようにする場合、そのユーザーはグループ `ioc_base_infrastructure` のメンバーである必要があります。

表 26. ユーザー・カテゴリー・グループの説明と ID

データ・カテゴリー	説明	ユーザー・カテゴリー・グループ
CBRNE	化学、生物、放射性物質、核、大型爆発物の脅威または攻撃	<code>ioc_base_chemical</code> , <code>ioc_base_biological</code> , <code>ioc_base_radiological</code> , <code>ioc_base_nuclear</code> , <code>ioc_base_explosive</code>
Env	環境: 汚染その他の環境関連	<code>ioc_base_environmental</code>
Fire	消火とレスキュー	<code>ioc_base_fire</code>
Geo	地理・地形 (地すべりなど)	<code>ioc_base_geophysical</code>
Health	医療と公衆衛生	<code>ioc_base_health</code>

表 26. ユーザー・カテゴリー・グループの説明と ID (続き)

データ・カテゴリー	説明	ユーザー・カテゴリー・グループ
Infra	インフラストラクチャー: 公益事業、通信、その他輸送以外のインフラストラクチャー	ioc_base_infrastructure
Met	気象 (洪水など)	ioc_base_meteorological
Rescue	レスキューと復旧	ioc_base_rescue
Safety	一般的な緊急事態と公共の安全	ioc_base_safety
Security	法的処置、軍事、国と地域/個人のセキュリティー	ioc_base_security
Transport	公共および私設の輸送	ioc_base_transportation
Other	その他のイベント、KPI、またはアラート	ioc_base_other

IBM Intelligent Operations Center の機能にログインしてアクセスするには、必要な許可権限が付与されているユーザー役割グループのメンバーである必要があります。

#### 関連概念:

90 ページの『ユーザー権限サマリー』

「ユーザー権限サマリー」ポートレットでは、IBM Intelligent Operations Center のユーザーおよびグループに関連付けられている権限を確認することができます。

78 ページの『ユーザーの役割とアクセス権』

IBM Intelligent Operations Center は、ユーザー役割に基づいて機能へのアクセスを制限することによってセキュリティーを実装します。

#### 関連タスク:

『ユーザーまたはグループの追加』

グループを選択してユーザー・プロファイルを作成し、新規ユーザーを IBM Intelligent Operations Center に追加します。新規グループに追加するユーザー名を選択します。

86 ページの『グループ・メンバーシップの表示または変更』

グループ・メンバーシップを表示または変更して、IBM Intelligent Operations Center内のユーザーのアクセス権限を管理します。

#### 関連資料:

81 ページの『ユーザー役割グループと許可権限』

IBM Intelligent Operations Center の機能にアクセスするための権限セットは、各ユーザー役割グループに関連付けられています。

#### 関連情報:



IBM WebSphere Portal 7 の製品資料

## ユーザーまたはグループの追加

グループを選択してユーザー・プロファイルを作成し、新規ユーザーを IBM Intelligent Operations Center に追加します。新規グループに追加するユーザー名を選択します。

### このタスクについて

新規ユーザーを追加するときは、最初にユーザーの役割グループを選択して、正しいレベルのアクセス権限を設定します。次に、「プロファイル管理」ページのフィールドに入力して、新規ユーザーを追加するた

めに必要な情報を IBM Intelligent Operations Center に設定します。「プロフィール管理」ページのフィールドに入力できる情報について詳しくは、トピックの末尾にあるリンクを参照してください。

## 手順

1. 管理ユーザーとして `http://app-host/wpsv70/wps/myportal/` にログオンします。
2. ページの上部にあるナビゲーション・バーの「管理」をクリックします。
3. サイドバー・メニューの「アクセス」をクリックします。
4. サブメニューの「ユーザーおよびグループ」をクリックします。
5. 新規ユーザーを追加するときは、グループのメンバーシップを指定して、役割を選択します。グループのリストの「すべてのポータル・ユーザー・グループ」をクリックしてグループを検索し、必要なグループをクリックします。
6. 「新規ユーザー」または「新規グループ」をクリックします。
7. ユーザー・グループを作成する場合は、ユーザー・グループの名前を入力します。
8. 新規ユーザーを追加するときは、アスタリスクで示す、ユーザー・プロフィールのすべての必須フィールドに入力するようにします。
9. 「OK」をクリックして、新規プロフィールまたはグループを送信します。

## タスクの結果

送信が正常に完了すると、それを確認するメッセージが表示されます。新規ユーザー・プロフィールが作成され、グループ・リストに表示されるか、新規グループが表示されます。新規ユーザーは、選択した役割グループに割り当てられている権限に従って、IBM Intelligent Operations Center へのアクセスが許可されます。

## 次のタスク

- 必要なデータ権限に従って、新規ユーザーにデータ・カテゴリー・グループのメンバーシップを指定します。
- 新規グループが追加されたら、グループを WebSphere Application Server Network Deployment ジャンクション ACL に追加します。
- 新規グループが追加されたら、許可権限もそのグループに設定する必要があります。許可権限によって、グループのメンバーがどの機能とデータを表示したり変更したりできるかが定義されます。許可権限の設定について詳しくは、トピックの末尾にある IBM WebSphere Portal 7 製品資料リンクを参照して、ページへのアクセス権の割り当てに関する情報を検索して確認してください。
- 新規ユーザーを、Tivoli Service Request Manager のセキュリティー・グループと担当者グループに割り当てます。

注：時間を節約するには、既存ユーザーに基づいて新規ユーザーのグループ割り当てを複製します。新規ユーザーを選択して、「複製 (Duplicate)」アイコンをクリックします。既存のユーザーを選択して、グループ・メンバーシップを複製します。

#### 関連概念:

78 ページの『ユーザーの役割とアクセス権』

IBM Intelligent Operations Center は、ユーザー役割に基づいて機能へのアクセスを制限することによってセキュリティを実装します。

#### 関連タスク:

141 ページの『Tivoli Service Request Manager での新規ユーザーの構成』

IBM Intelligent Operations Center でユーザーを追加したら、Tivoli Service Request Manager で、そのユーザーに権限および担当者グループを割り当てます。

#### 関連資料:

81 ページの『ユーザー役割グループと許可権限』

IBM Intelligent Operations Center の機能にアクセスするための権限セットは、各ユーザー役割グループに関連付けられています。

83 ページの『ユーザー・カテゴリ・グループとデータ権限』

IBM Intelligent Operations Center のデータ・カテゴリにアクセスするための権限は、各ユーザー・カテゴリ・グループに関連付けられています。

#### 関連情報:

 IBM WebSphere Portal 7 の製品資料

---

## グループ・メンバーシップの表示または変更

グループ・メンバーシップを表示または変更して、IBM Intelligent Operations Center内のユーザーのアクセス権限を管理します。

### このタスクについて

メンバーシップを表示または変更する対象の役割またはデータ・カテゴリに対応するグループを選択します。役割グループのメンバーシップによって、その役割に適したソリューション部分へのアクセス権限がユーザーに付与されます。カテゴリ・グループのメンバーシップによって、ユーザーに対し、そのカテゴリに関連付けられているイベント、重要業績評価指標 (KPI)、およびアラートへのアクセス権が付与されます。

アイコンの上にカーソルを移動すると、そのアイコンの目的を示す吹き出しヘルプが表示されます。

### 手順

1. 管理ユーザーとして <http://app-host/wpsv70/wps/myportal/> にログオンします。
2. ページの上部にあるナビゲーション・バーの「管理」をクリックします。
3. サイドバー・メニューの「アクセス」をクリックします。
4. サブメニューから「ユーザーおよびグループ」をクリックします。
5. グループのリストの「すべてのポータル・ユーザー・グループ」をクリックして、必要なグループをクリックします。そのグループのメンバーがリストされます。
6. グループ・メンバーシップに関連する以下のアクションを実行できます。
  - ユーザー ID に対して「メンバーシップの表示」をクリックして、他のグループのメンバーシップを表示します。
  - 「メンバーの追加」をクリックして追加するユーザーを選択し、グループにユーザーを追加します。
  - ユーザー ID に対して「除去」をクリックして、グループからユーザーを除去します。



#### 関連資料:

81 ページの『ユーザー役割グループと許可権限』

IBM Intelligent Operations Center の機能にアクセスするための権限セットは、各ユーザー役割グループに関連付けられています。

83 ページの『ユーザー・カテゴリ・グループとデータ権限』

IBM Intelligent Operations Center のデータ・カテゴリにアクセスするための権限は、各ユーザー・カテゴリ・グループに関連付けられています。

#### 関連情報:



IBM WebSphere Portal 7 の製品資料

---

## ユーザー・プロファイルの表示または編集

ユーザーのプロファイルを表示または編集して、パスワードを含め、すべてのユーザー・プロファイル属性を設定またはリセットします。このユーザー ID を変更することはできません。

### このタスクについて

認証ポータル・ユーザー・リストからユーザーを選択してユーザー・プロファイルを開き、プロファイルの詳細を変更します。各ユーザーは、自分のプロファイルを変更することもできます。

アイコンの上にカーソルを移動すると、そのアイコンの目的を示す吹き出しヘルプが表示されます。

### 手順

1. 管理ユーザーとして `http://app-host/wpsv70/wps/myportal/` にログオンします。
2. 上部のナビゲーション・バーから「管理」をクリックします。
3. サイドバー・メニューの「アクセス」項目をクリックします。
4. サブメニューから「ユーザーおよびグループ」をクリックします。
5. ユーザーのリストの「すべての認証ポータル・ユーザー」をクリックします。
6. ユーザーの編集アイコンをクリックして、「プロファイル管理」ページを表示します。ユーザー・プロファイルの属性フィールドが表示されます。
7. パスワードを変更するには、「新規パスワード:」フィールドおよび「パスワードの確認:」フィールドに新規パスワードを入力します。
8. 残りの任意のフィールドで、情報の入力、編集、または削除をすることができます。
9. 「OK」をクリックして、行った変更を送信します。

### タスクの結果

送信した変更で、ユーザー・プロファイルが更新されます。

#### 関連情報:



IBM WebSphere Portal 7 の製品資料

---

## ユーザーまたはグループの削除

IBM Intelligent Operations Center からユーザーまたはグループを削除します。



## このタスクについて

ユーザーを削除するには、認証ポータル・ユーザーのリストからユーザーを選択して削除します。グループを削除するには、ポータル・ユーザー・グループのリストからグループを選択して削除します。

アイコンの上にカーソルを移動すると、そのアイコンの目的を示す吹き出しヘルプが表示されます。

注: IBM Intelligent Operations Center からユーザーを削除すると、IBM Smarter Cities™ Software Solutions 製品ファミリー内の他のソリューションへのアクセス権限も削除されることに注意してください。グループを削除した場合も、他のソリューションからそのグループが削除されます。

## 手順

1. 管理ユーザーとして `http://app-host/wpsv70/wps/myportal/` にログオンします。
2. 上部のナビゲーション・バーにある「管理」をクリックします。
3. サイドバー・メニューの「アクセス」をクリックします。
4. サブメニューの「ユーザーおよびグループ」をクリックします。
  - 「すべてのポータル・ユーザー・グループ」をクリックして、グループのリストを表示します。
  - 「すべての認証ポータル・ユーザー」をクリックして、ユーザーのリストを表示します。
5. 削除するユーザーまたはグループに対応する「削除」アイコンをクリックします。

## タスクの結果

削除したユーザーまたはグループが、IBM Intelligent Operations Center 内に存在しなくなります。グループを削除しても、グループのメンバーは削除されません。

### 関連情報:



IBM WebSphere Portal 7 の製品資料

---

## ユーザーおよびグループのインポート

ポータル・サービスを使用して、IBM Intelligent Operations Center にユーザーを一括してインポートすることができます。

## このタスクについて

ポータル管理者は、ポータル管理コンソールを使用して、IBM Intelligent Operations Center にユーザーを一括してインポートすることができます。このタスクに必要な XML ファイルは、アプリケーション・サーバーの `/opt/IBM/WebSphere/PortalServer/doc/xml-samples/CreateUser.xml` にあります。この XML ファイルを変更して、IBM Intelligent Operations Center にユーザーを追加することができます。

注: 複数のユーザーを追加する場合は、ユーザーをグループに追加する前に、まずすべてのユーザーを追加してください。このトピックの最後にある例を参照してください。

以下の手順の代わりに、アプリケーション・サーバーにある `xmlaccess.sh` スクリプトをコマンド行から実行することもできます。

## 手順

1. `CreateUser.xml` ファイルを更新して、新しいユーザーと、それらのユーザーが属するグループを含めません。

2. 管理ユーザーとして `http://app-host/wpsv70/wps/myportal/` にログオンします。
3. 「管理」をクリックします。
4. 「ポータルの設定 (Portal Settings)」で、「XML のインポート (Import XML)」をクリックします。
5. 更新された XML ファイルを参照して指定します。
6. 「インポート」をクリックします。

## タスクの結果

WebSphere Portal Server は、Tivoli Directory Server のディレクトリーと Tivoli Access Manager WebSEAL に、関連するエントリーを自動的に作成します。

## 例

以下の例では、XML ファイルを変更して、2 人のユーザーを IBM Intelligent Operations Center に追加し、それぞれのユーザーを 1 つの役割グループと 1 つのカテゴリー・グループに追加しています。

```
<?xml version="1.0" encoding="UTF-8"?>
<request xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PortalConfig_7.0.0.xsd" type="update"
create-oids="true">
<portal action="locate">
<user action="update" name="cityuser003" firstname="City"
lastname="user003" password="passwd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user003</parameter>
</user>
<user action="update" name="cityuser004" firstname="City"
lastname="user003" password="passwd">
<parameter name="preferredLanguage" type="string"
update="set">en_US</parameter>
<parameter name="cn" type="string" update="set">City user004</parameter>
</user>
<group action="update" name="City Executive">
<member-user update="set" id="cityuser003">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser003">
<group action="update" name="City Executive">
<member-user update="set" id="cityuser004">
</group>
<group action="update" name="ioc_base_fire">
<member-user update="set" id="cityuser004">
</group>
</portal>
</request>
```

## 関連概念:

224 ページの『管理コンソール』

「管理コンソール」ポートレットを使用して、ソリューションによって提供されるサービスを管理します。

## 関連情報:



IBM WebSphere Portal 7 の製品資料



Tivoli Directory Server インフォメーション・センター



Tivoli Access Manager インフォメーション・センター

---

## ユーザー権限サマリー

「ユーザー権限サマリー」ポートレットでは、IBM Intelligent Operations Center のユーザーおよびグループに関連付けられている権限を確認することができます。

「ユーザー権限サマリー」ポートレットは、ユーザーに付与されているグループ・メンバーシップおよび権限の詳細を表示します。

「ユーザー権限サマリー」ポートレットにアクセスするには、WebSphere Portal 管理インターフェースで「**Intelligent Operations**」 > 「管理ツール」 > 「ユーザー権限サマリー」をクリックします。

「ユーザー」タブでは、ユーザーの権限を確認することができます。ユーザー ID を入力して、以下の情報を表示します。

- IBM Intelligent Operations Center で使用可能なすべてのデータ・カテゴリーとユーザー・カテゴリー・グループの完全なリスト。
- 指定したユーザーに割り当てられているデータ・カテゴリー権限のリスト。
- 指定したユーザーがメンバーであるすべてのグループ、ユーザー役割グループ、およびユーザー・カテゴリー・グループのリスト。
- 指定したユーザーがそのカテゴリーについての権限があるかどうかを示す各データ・カテゴリーのリスト。

「サマリー」タブでは、ユーザー権限およびグループ権限に関する統計のサマリーを確認することができます。以下の情報を表示することが可能です。

- IBM Intelligent Operations Center 内のグループの総数。
- IBM Intelligent Operations Center に対してアクセス権限があるユーザーの総数。
- データ・カテゴリー別のユーザー総数のリスト。
- ユーザー役割グループ別のユーザー総数のリスト。

## 関連資料:

81 ページの『ユーザー役割グループと許可権限』

IBM Intelligent Operations Center の機能にアクセスするための権限セットは、各ユーザー役割グループに関連付けられています。

83 ページの『ユーザー・カテゴリ・グループとデータ権限』

IBM Intelligent Operations Center のデータ・カテゴリにアクセスするための権限は、各ユーザー・カテゴリ・グループに関連付けられています。

---

## Cyber Hygiene の概要

IBM Intelligent Operations Center の Cyber Hygiene 機能は、インストール済みシステムに存在する可能性のある機密漏れを修正するサービスを提供できるように設計されています。

注: 一般的に、「ぜい弱性」という用語は、セキュリティのぜい弱性と機密漏れの両方を指して使用されます。Cyber Hygiene ではぜい弱性を、セキュリティ・ブリーチ (抜け穴) を可能にする、アプリケーションのプログラミング・エラーと定義しています。Cyber Hygiene では、機密漏れは、オペレーティング・システムまたはアプリケーションの構成の選択内容のセキュリティが低いことと定義しています。よりセキュアな構成オプションを選択することで、機密漏れに対処できます。例えば、ディレクトリーは、全ユーザーがファイルを格納できるように構成可能です。これを、よりセキュアな構成にして、所有者のみがディレクトリーにファイルを格納できるようにすることも可能です。

Cyber Hygiene には、以下の 2 つのキー・エレメントがあります。

- Linux オペレーティング・システムとその関連のユーザー、ディレクトリー、およびファイルに存在する、既知の機密漏れを軽減し、修正します。これは、一連のツールとスクリプトによって実行されます。
- オペレーティング・システム、製品、およびシステム構成内の、約 1000 件の既知のぜい弱性および機密漏れについてのアセスメントを文書化しています。

インストール・プロセスの実行中に機密漏れを処理することによって、デプロイ済みのシステムでセキュリティ・レベルを強化するためにお客様が行う必要のある作業を軽減します。

例えば政府機関では、Cyber Hygiene の修復機能と資料を使用して、セキュア・ネットワークへのデプロイメント用のシステムの認定と認可をサポートする場合に役立ちます。営利事業のお客様は、同じプロセスを使用して、ご使用の環境のセキュリティを向上させることができます。

サイバー・セキュリティは、リスクを防止するものではなく、リスクを軽減するものです。システムが価値を提供するためには、稼働状態でありアクセス可能になっている必要があるため、システムの情報やその制御が漏えいの危険にさらされるリスクは常に存在します。

Cyber Hygiene は、サービス妨害や SQL インジェクションなどの脅威をアプリケーションが処理する方法を含め、アプリケーション固有のぜい弱性には対処しません。代わりに Cyber Hygiene は、特定のアプリケーションを対象とせず、汎用性のある方法でユーザー、ディレクトリー、およびファイルの機密漏れに対処することによって、アプリケーション・セキュリティのための基盤を提供します。Cyber Hygiene は、製品のインストール後に実行され、システムおよびアプリケーションのユーザー、ディレクトリー、およびファイルの一般的なぜい弱性を修正します。Linux オペレーティング・システムで使用するアプリケーションは、アプリケーション固有のぜい弱性を個別に査定する必要があります。

Cyber Hygiene で使用されている既知のぜい弱性および機密漏れのカタログは、United States Defense Information Services Agency (DISA) による、分類されていない非機密情報のチェックリストに基づいてい

ます。Cyber Hygiene の適用可能性について、これらのリストの項目が評価されます。スキャン・スクリプトは、機密漏れを検索して、そのインスタンスを記録します。そして、該当する場合には、問題に対処する修復スクリプトの入力として、それらのログ・ファイルを使用します。セキュリティについての検出事項には、異なる処理が必要となるものも少数あります。

IBM Intelligent Operations Center コンポーネントの既知のぜい弱性と、それらのぜい弱性を軽減するために Cyber Hygiene が取るアクションをリストした資料が、IBM Intelligent Operations Center で提供されています。

#### 関連タスク:

16 ページの『チェックリスト - IBM Installation Manager を使用したインストール』

このチェックリストは、IBM Installation Manager を使用して IBM Intelligent Operations Center をインストールするときに、インストール・ステップを追跡するために使用します。

18 ページの『チェックリスト - ステップ・バイ・ステップでインストール』

スクリプトおよびコマンドを使用して IBM Intelligent Operations Center をインストールする場合、このチェックリストを使用して、インストール・ステップを追跡します。

30 ページの『Installation Manager を使用した IBM Intelligent Operations Center のインストール』

IBM Intelligent Operations Center は、付属のグラフィカル・インストーラーを使用してインストールできます。

70 ページの『Cyber Hygiene のステップ・バイ・ステップでインストールと実行』

Cyber Hygiene は、IBM Intelligent Operations Center とは別個にインストールして実行します。また、他のすべての IBM Intelligent Operations Center コンポーネントのインストールおよび構成が完了して作動可能になった後で、インストールして実行する必要があります。Cyber Hygiene ではデフォルトのオペレーティング・システム構成をよりセキュアなオプション・セットに変更できるので、IBM Intelligent Operations Center システムのためのさらにセキュアな基盤を確保するために役立ちます。

## サイバー・セキュリティ

IT 環境の保護は、これまで長い間にわたり各国政府にとって懸案事項であり、重要インフラストラクチャー・システムにおける IT 環境保護の重要性が高まっています。IBM Intelligent Operations Center などのような重要インフラストラクチャーを実現する製品とソリューションでは、製品とソリューションを提供する前に、可能な限り既知のぜい弱性を除去しておく必要があります。

サイバー・セキュリティは、リスクを防止するものではなく、リスクを軽減するものです。IT システムが価値を提供するには、稼働状態でありアクセス可能になっている必要があるため、システムの情報やその制御が漏えいの危険にさらされるリスクが常に存在します。サイバー・セキュリティは、静的な要素と動的な要素の両方で構成されます。IBM Intelligent Operations Center の Cyber Hygiene は、サイバー・セキュリティの静的な要素に対応します。サイバー・セキュリティの動的な要素に対応するには、その他のツールとプロセスが必要です。このようなツールとプロセスには、物理的セキュリティ手続きおよび人的セキュリティ手続きや、ネットワーク侵入対処ツールなどがあります。

IBM Intelligent Operations Center の Cyber Hygiene 機能は、ぜい弱なセキュリティ構成、ソフトウェア・エラー、システム管理エラー、システム・セキュリティ・プロセス・エラーなどの分野に対応するように設計されています。このサポートを提供するため、Cyber Hygiene はオペレーティング・システムを構成するインストール機能および構成機能と、保護設定を行い主要セキュリティ関連フィックスパックをインストールする管理機能を備えています。例えば、ユーザー ID には常にパスワードが設定されており、



ftp、snmp、rlogin などの安全性が低い Linux サービスを無効にするようにシステムが構成されています。ただし、社内の特定のセキュリティー・プラクティスに対応するようにシステムを自動的に構成することはできません。

## Cyber Hygiene のチェックリスト

Cyber Hygiene は、米国国防情報システム局 (DISA) の無制限チェックリストおよび定期的なぜい弱性アラートに基づくチェックリストを使用します。

### チェックリスト項目の分析

米国国防情報システム局 (DISA) の無制限チェックリストに示されるぜい弱性ごとに、そのぜい弱性に関するデータが定義されています。

各ぜい弱性について提供される情報は次のとおりです。

- 固有 ID。この ID は、セキュリティー技術導入ガイド (STIG) ID およびぜい弱性管理システム (VMS) キーからなります。
- ぜい弱性を要約した短い名前。
- ぜい弱性の重大度。記述されている重大度レベルは以下のとおりです。

**I** 重大度高

**II** 重大度中

**III** 重大度低

- 影響を受ける製品。
- 影響を受けるバージョン。
- ぜい弱性の説明 (ユース・ケース、コンテキスト、および他のソフトウェアとの相互作用など)。
- 推奨処置。パッチまたはアップグレードで修復が提供されない場合、推奨される軽減処置が含まれていることがあります。
- 特定のアラートにより置き換えられるすべてのアラート。

各ぜい弱性について、ぜい弱性が IBM Intelligent Operations Center に影響するかどうかを理解しておくことが重要です。例えば、以下のようなものがあります。

- IBM Intelligent Operations Center に含まれている製品のリリースとフィックス・レベルが影響を受けるかどうか。その問題が新しいリリースまたはフィックスから発生した可能性があるために、古い製品リリースまたはフィックスではその問題による影響がない場合があります。
- IBM Intelligent Operations Center に含まれている製品が、ぜい弱性を生じるような方法で使用されているかどうか。例えば、製品が別の製品のサービスを使用する場合にのみ問題が発生することがあります。これらのサービスが IBM Intelligent Operations Center 構成で使用されていない場合は、修復は不要なことがあります。
- 製品のぜい弱性が、使用するオペレーティング・システムに影響するかどうか。特定のオペレーティング・システムを実行する場合にのみ発生するぜい弱性があります。

チェックリストの項目ごとに上記の要因が分析され、IBM Intelligent Operations Center に必要なアクションが判別されました。この分析と修復の結果は次の 4 つのアセスメントのいずれかになります。

### 適用外 (NA)

影響を受ける製品または構成は、IBM Intelligent Operations Center 環境の一部ではありません。

## 未検出 (NF)

インストールされている製品のバージョンとフィックス・レベルは影響を受けないか、またはぜい弱性が発生するような方法で製品が使用されていません。このアセスメントは、構成でぜい弱性が生じない場合にも使用されます。

## 開通

インストールされている製品のバージョンとフィックス・レベルにぜい弱性が該当するが、製品に対して使用可能な修復がありません。このアセスメントは、ぜい弱性が生じるような方法でシステムが構成されている場合にも使用されます。例えば、製品で world-write 権限が必要であるために、ディレクトリーに対する world-write 権限を許可する場合などです。このアセスメントは、パスワードの長さや文字の混用に関するポリシーなどの組織のポリシーに基づいて修復が適用される可能性がある場合にも使用されます。

## 修正済み

未解決のぜい弱性に対する修復が適用され、検証されました。

表 27 に分析の例を示します。2 番目の例では、どの IBM Intelligent Operations Center サーバーにもインストールされていない製品の扱いが示されています。

表 27. ぜい弱性アセスメントの例

ID	名前	重大度	アプリケーション・サーバー	イベント・サーバー	データ・サーバー	管理サーバー	説明
2011-B-0082	IBM Websphere Application Server の複数のぜい弱性	I	NF	開通	NA	NF	6.1.0.39 以前のバージョンおよびバージョン 7.0.0.19 に影響します。
2011-B-0085	Wireshark の複数のサービス妨害のぜい弱性	I	NA	NA	NA	NA	Wireshark はインストールされていません

## チェックリスト選択

各サーバーで使用されるチェックリストは、そのサーバーにインストールされているソフトウェアに基づいています。チェックリストの中には、製品タイプ (データベースなど) のぜい弱性を扱うチェックリストがあります。また、あるカテゴリーの特定の製品 (DB2® など) に関する問題を扱うチェックリストもあります。

すべての製品タイプに固有のチェックリストがあるわけではありません。一般的なぜい弱性は、「アプリケーション・セキュリティ」チェックリストまたはオペレーティング・システム関連のリストに記載されています。

Cyber Hygiene で使用されるチェックリストのタイプを以下に示します。

### アプリケーション・セキュリティ

システム・レベルのぜい弱性がリストされています。ソフトウェアの開発およびテストの実践に関連するぜい弱性と、ユーザー認証で暗号化パスワードを使用しないなどのアプリケーション固有のぜい弱性があります。

### Unix/Linux

構成、パスワード管理、ファイル・システム・パーティショニングなどに関連するぜい弱性がリストされています。

### Web サーバー

HTTP サーバーに関連するぜい弱性がリストされています。

### データベース

データベース・サーバーに関連するぜい弱性がリストされています。

### ディレクトリー・サーバー

LDAP サーバーに関連するぜい弱性がリストされています。



## エンタープライズ・システム管理

エンタープライズ・システム管理ツールおよびシステム管理プロセスに関連するぜい弱性がリストされています。

ネットワーク・セキュリティ構成は顧客のポリシーおよびネットワーク体系に基づいて決定する必要があるため、チェックリストではネットワーク・セキュリティは扱われません。ネットワーク・セキュリティ構成は、各インストール済み環境のニーズに基づいて行われる必要があります。

## Cyber Hygiene のデフォルト構成

Cyber Hygiene 機能は、Linux のデフォルト構成およびポリシーを、デフォルトのオペレーティング・システムのインストールで設定されるオプションよりさらにセキュアなオプションに設定します。システム管理者は、インストール先のセキュリティ・ポリシーに合わせて、これらのデフォルト設定を容易に変更することができます。

企業の IT 運用管理グループは、社内システムのセキュリティを担当します。これには、ネットワーク・アクセスや、社内のセキュリティ・ポリシーおよびプロセスの管理などがあります。

Cyber Hygiene のデフォルト設定が企業のポリシーと矛盾する場合は、企業のポリシーを優先する必要があります。ローカル・セキュリティ・ポリシー設定がシステム機能に与える影響についてはテストされていない点に注意してください。IBM Intelligent Operations Center にセキュリティ・ポリシーを適用するときには、Cyber Hygiene を使用してデプロイされていない製品にセキュリティ・ポリシーを適用する場合と同様の注意を払ってください。

IBM Intelligent Operations Center は個々の企業セキュリティ・ポリシーに合わせて自動的に構成することはできませんが、既知のぜい弱性を取り除くように IBM Intelligent Operations Center を構成することは可能です。Cyber Hygiene は、デフォルトのベスト・プラクティス・ポリシーのセットを使用して IBM Intelligent Operations Center を構成します。これが、システム管理者が特定の組織ポリシーとプラクティスを適用する際に使用する基盤となります。

## デフォルトのパスワード管理ポリシー

Cyber Hygiene は、Linux オペレーティング・システムのデフォルトのパスワード管理ポリシーを構成します。

Cyber Hygiene によって設定されるデフォルトのパスワード管理ポリシーを、表 28 に示します。

表 28. Cyber Hygiene のデフォルトのパスワード管理ポリシー

ポリシー	値または設定値
パスワードの最小長	8 文字
受け入れられる文字	大文字、小文字、数値、特殊文字 (: ; ! ` ~ @ # \$ % ^ & * ( ) - _ = + [ { ] } ¥   ' " , < . > / ? およびスペース文字)
コンテンツ規則	なし
ユーザーをロックアウトするまでのログオン試行の失敗回数	3
パスワードの変更から次の変更までの最小時間	1 日
パスワードの変更から次の変更までの最大時間	60 日
アカウントに対してパスワードを必須にするかどうか	yes
同じパスワードを再使用可能にする時期	異なるパスワードを 5 つ使用した後

表 28. Cyber Hygiene のデフォルトのパスワード管理ポリシー (続き)

ポリシー	値または設定値
非活動状態後にログインが必要になるまでの時間	非活動状態が 15 分続いた場合
ログオンの失敗間の遅延	4 秒

Cyber Hygiene のデフォルト・ポリシーの設定時に、`/etc/pam.d/system-auth` ファイルおよび `/etc/login.defs` ファイルが変更されます。

これらの設定は、妥当なセキュリティ・プラクティスのために最小限必要なものです。ユーザーの組織のセキュリティ・ポリシーに合わせて、これらの設定を変更してください。デフォルト設定を変更する可能性があるエリアを以下に示します。

- デフォルト構成では最小パスワード長が 8 文字に設定されていますが、セキュア・システムのベスト・プラクティスでは一般に安全なパスワードの長さは 14 文字以上とされています。
- 最大パスワード変更間隔は、組織に適した値に設定する必要があります。これは `/etc/shadow` ファイルの **inactive** パラメーターで定義されます。ユーザーは、定義された時点でログオンのパスワードを変更することを強制されます。ユーザーがパスワードを変更できなかった場合は、特権ユーザーがパスワードを再設定する必要があります。`/etc/shadow` ファイルに指定されている値が使用されるかどうかは、`/etc/default/useradd` ファイルに指定されているデフォルト・アクションによって決まります。`/etc/default/useradd` ファイルに `-1` が指定されている場合、パスワードの有効期限は無制限になります。`/etc/default/useradd` に `0` が指定されている場合、アカウントはロックされません。`/etc/default/useradd` ファイルにその他の値が定義されている場合、`/etc/shadow` の **inactive** パラメーター値がパスワードの有効期限に使用されます。
- 企業セキュリティ・ポリシーに基づいて、パスワードの複雑さと内容に関する規則を策定および導入する必要があります。

パスワード・ポリシーの管理について詳しくは、Linux の資料を参照してください。

## Linux サービスの無効化

Cyber Hygiene は、ぜい弱な Linux サービスを無効化またはアンインストールします。これらのサービスはシステムへのアクセスを許可できるため、これらのサービスが必要な場合にのみ始動またはインストールしてください。

以下の Linux サービス (デーモン) は、デフォルトでは開始されません。これらは必要に応じて開始できます。

- `inetd/xinetd`
- `portmap`
- `avahi-daemon`
- `bluetooth`
- `cups`
- `hidd`
- `isdn`
- `rhnsd`
- `canna`
- `pcmcia`
- `ybind`

- autofs
- smartd
- netfs
- snmpd
- nfs
- samba

これらのサービスは、**service service\_name start** コマンドを使用することで開始できます。

注: これらのサービスが適正に構成されていないと、システムが危険にさらされ、システムへの無許可アクセスができるようになってしまう場合があります。そのため、システム・セキュリティ上の目的で、デフォルトではこれらは開始されません。

以下の Linux サービスは削除されます。これらのサービスは、必要に応じて **rpm** または **yum** コマンドを使用して再インストールできます。例えば、**yum install httpd** コマンドによって、HTTP デーモン・パッケージがインストールされます。

- tcpdump
- sendmail
- squid
- vnc-server
- httpd
- mod\_python
- mod\_perl
- mod\_ssl
- webalizer
- httpd-manual

注: これらのサービスは、サーバー環境で機密漏れを引き起こす可能性が高いため、Linux から削除されます。

## ユーザー ID の削除

標準の Linux インストールには、セキュアな実稼働環境には好ましくないユーザー ID がいくつか含まれています。Cyber Hygiene は、これらのユーザー ID を Linux のユーザー・レジストリーと `/etc/passwd` ファイルから削除します。関連付けられているホーム・ディレクトリーも削除されます。

以下のユーザー ID が削除されます。これらは必要に応じて再作成することができます。

- games
- news
- ftp
- halt
- shutdown
- reboot
- who
- gopher

- lp
- rpcuser
- uucp

これらのユーザー ID が必要な場合は、標準の Linux 管理プロシージャを使用して作成することができます。

## 監査規則

監査ファイルのサイズが短期間で大きくなる可能性があるため、Linux での標準監査は最小限です。ただしセキュリティが課題となる場合は、インシデントで何が発生したかを判別できるようにするため、監査の強化が非常に重要になります。Cyber Hygiene スクリプトは、すべての Linux 実行レベルについて、追加監査規則のセットを追加します。これらの規則に一致するイベントは、標準のシステム・ログ・ファイルに記録されます。

以下の Linux 監査規則が追加されます。これらは、必要な場合には変更することができます。

- プログラムおよびファイルへのアクセス試行の失敗
- プログラムおよびファイルの削除
- 管理アクション、セキュリティ・アクション、および特権アクション
- アクセス制御権限の変更

優れた監査ログを持つことは、セキュリティ・グッド・プラクティスとなります。Cyber Hygiene で定義された監査に、何らかの理由により変更が必要な場合は、`/etc/audit/auditd.conf` ファイルおよび `/etc/audit/audit.rules` ファイルを変更する必要があります。Cyber Hygiene は、Red Hat Enterprise Linux の 5 つのランタイム・レベルすべてについて監査を有効にします。

## ファイルおよびディレクトリーの権限

Cyber hygiene は、既存のファイルおよびディレクトリーの権限を、セキュリティのベスト・プラクティスを満たすように変更します。

Cyber Hygiene が行うファイルおよびディレクトリーの権限の変更は、以下のとおりです。

### システム・スクリプトの制限

重要なセキュリティ・システム・スクリプトには、適正な特権を持たないユーザーはアクセスできません。

### world-write 権限の除去

ユーザーは、パブリックでないディレクトリーには書き込みできません。ファイルおよびディレクトリーの変更を行う必要があるアプリケーションおよびユーザーは、そのファイルやディレクトリーの所有者またはグループのメンバーである必要があります。

### world-read および world-execute 権限の除去

多くのファイルおよびディレクトリーについて、world-readable (誰でも読み取り可能) 権限および world-executable (誰でも実行可能) 権限が除去されます。具体的には、ユーザーのホーム・ディレクトリーからこれらの権限が除去されます。ファイルの読み取りまたは実行をする必要があるアプリケーションおよびユーザーは、そのファイルやディレクトリーの所有者またはグループのメンバーである必要があります。

## その他の変更

Cyber Hygiene は、機密漏れに対処するために、他の変更も行います。

### バッチ・プログラム - at コマンド

特定の時刻にバッチ・プログラムを実行する **at** コマンドを非特権ユーザーが使用することを防ぐために、Cyber Hygiene は **at.deny** ファイルを削除して、空の **at.allow** ファイルを作成します。

**at.allow** ファイルは、**at** コマンドの実行を許可するユーザーを定義します。**at.allow** ファイルにユーザー ID が指定されていない場合、特権システム ID 以外には、**at** コマンドを実行できるユーザーがいないことを意味します。**at** コマンドの使用を明示的に許可しないユーザーを定義する **at.deny** ファイルが存在し、**at.allow** ファイルが存在していない場合、**at.deny** ファイルで定義されているユーザーを除くすべてのユーザーに対し、**at** コマンドの実行が許可されます。いずれのファイルも存在しない場合、**at** コマンドを実行できるのはスーパーユーザーのみです。

デフォルトでは、Red Hat Enterprise Linux はユーザーが **at** コマンドを実行できるように構成されています。

### バッチ・プログラム - cron コマンド

管理権限のないユーザーは、バッチ・プログラムをスケジュールする **cron** コマンドを実行することはできません。

### Ctrl-Alt-Del

Ctrl-Alt-Del キーの組み合わせは無効にされるため、このキーを使用してシステムをシャットダウンすることはできなくなります。

## 修復ツール

IBM Intelligent Operations Center Cyber Hygiene 機能には、インストールされている IBM Intelligent Operations Center システムのぜい弱性を修正する修復ツールがあります。

修復ツールは、IBM Intelligent Operations Center のインストール完了後に Cyber Hygiene が実行されるときに実行されます。これらのツールは、システムが実動環境で使用されている場合にも実行できます。ツールを実行することで、その他の製品がサーバーにインストールされたとき、またはシステムを使用した結果として生じる可能性があるぜい弱性が検出および修正されます。

### ぜい弱性スキャナー

このスキャナーは、IBM Intelligent Operations Center システムを確認し、ぜい弱性を特定するスクリプトで構成されています。例えばスキャナーは、すべてのユーザーに対して書き込み特権が設定されているディレクトリーを特定します。

スキャナーは、修復スクリプトにより使用される検出結果ファイルを作成します。検出結果ファイルには、IBM Intelligent Operations Center システム内で特定されたぜい弱性がリストされます。

スキャナーのスクリプトは、IBM Intelligent Operations Center システムを変更しません。スキャナーは、ぜい弱性の特定のみを行います。修復後に、修復スクリプトによって行われた変更を検証するために使用できます。

## ぜい弱性修復スクリプト

Cyber Hygiene には 3 種類の修復スクリプトがあります。

- スキャンが不要であり、容易にリバースでき、システムに対し実行時に大きく影響しない構成変更を行うスクリプト。例えば、マニュアル・ページのデフォルトのファイル・アクセス権限を 644 に変更する場合などです。
- root アカウントによるリモート・ログオンを無効にするスクリプト。
- スキャナーにより作成される検出結果ファイル进行处理し、特定されたぜい弱性を解決するスクリプト。

追加製品のインストール後にこのスクリプトを使用する場合は、注意してください。一部の製品では、厳重な設定をしないようにする必要があり、そのような製品はスクリプトの実行後に誤動作する可能性があります。修復スクリプトの実行前に、スキャナー・スクリプトによって作成された検出結果ファイルを調べ、発生する可能性があるリスクを確認してください。

## 修復ログ

スキャン・スクリプトと修復スクリプトは、各 IBM Intelligent Operations Center サーバーで 4 つのログ・ファイルにそのアクションを記録します。これらのログは、/var/BA15/CH/results ディレクトリーにあります。サブディレクトリーには、スキャンおよび修復の結果の作業用コピーが含まれています。


スキャナーは 2 回実行されます。1 回目はぜい弱性を修復し、2 回目は実行されなかった修復をログに記録します。管理者は 2 番目の実行のログを使用して、手動での修復ステップが必要であるかどうかを判断します。

## Cyber Hygiene の資料

資料は、インストール済みの IBM Intelligent Operations Center システムに適用された変更についてお客様が評価する際のヘルプとして使用可能です。この資料は、実動使用に向けたシステムの認定と認可を支援します。

資料には、Cyber Hygiene 戦略全体の概要、いくつかのデフォルトを実装した根拠、および DISA フラグ付きの個々のぜい弱性の状況を文書化したスプレッドシートが含まれています。このスプレッドシートは、製品のセキュリティー・アセスメントの際に使用できます。

### 関連情報:

 [IBM Intelligent Operations Center 1.5 における Cyber Hygiene の実装](#)



---

## 第 4 章 ソリューションの統合

イベントに関連するデータを取り込むことにより、製品とサービスを IBM Intelligent Operations Center に統合することができます。

IBM Intelligent Operations Center に伝達されたイベント・データは、共通アラート・プロトコルで処理することも、他のプロトコルで処理することもできます。

イベントは、IBM Intelligent Operations Center によってモニターされる重要業績評価指標 (KPI) に関連付けることができます。IBM Intelligent Operations Center 内のイベントは、標準操作手順および使用可能なリソースに関連付けることもできます。ソリューションは、レポート管理サービスを提供します。これにより、イベント・データの最新のレポートと要約を生成することができます。

---

### 統合できるシステムの例

製品およびサービスを IBM Intelligent Operations Center に統合できます。

システムおよびサービスの例を以下に示します。

- 公共安全の問題についてレポートするシステム。
- 交通イベントについてレポートするシステム。
- 水質および水利用についてレポートするシステム。
- 関連する作業指示書の障害および状況についてデータを提供するシステム。

これらのシステムは、IBM Intelligent Operations Center と通信できるようにする必要と、サポートされているプロトコルでイベントおよび測定を IBM Intelligent Operations Center インバウンド・イベント・キューに送信できるようにする必要があります。

#### 関連概念:

111 ページの『IBM Intelligent Operations Center に対し定義されているインバウンド・イベント・キューの使用』

CAP イベントを組み込みの WebSphere Message Broker インスタンスに送信することで、これらのイベントを IBM Intelligent Operations Center にパブリッシュできます。

103 ページの『共通アラート・プロトコルとの統合』

共通アラート・プロトコル (CAP) は、IBM Intelligent Operations Center と外部システムとの間でイベント情報をやり取りするために使用されます。

---

### 統合点とプロトコル

他のシステムは、IBM Intelligent Operations Center のサービスとポリシーを使用して、ソリューションと統合することができます。データは、共通アラート・プロトコル (CAP) 形式で受け取ることができます。他のプロトコルもサポートされています。

### イベントと KPI

IBM Intelligent Operations Center は、イベントと重要業績評価指標 (KPI) を処理して、情報の表示方法を決定します。



他の製品およびサービスは、メッセージング・バス・サービスを通じて IBM Intelligent Operations Center と統合できます。 KPI は、ビジネス・モニター・サービスによってモニターされます。

イベントは、IBM Intelligent Operations Center が受信します。 これらのイベントは、「詳細」ポートレットで表示することができ、「マップ」ポートレットの表示内容に影響を与えます。

KPI 定義により、「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットで KPI がどのように表示されるかが決定されます。 KPI 定義で、イベントに関する情報を表示する方法も決定されることがあります。 例えば、KPI しきい値を超過した場合、イベントに高い緊急度または重大度のフラグを立てる場合があります。 対応する KPI 定義を持たないイベントは、イベントに関して受け取った情報に従って表示されます。

KPI の作成および統合の方法については、このトピックの末尾にあるリンクを参照してください。

#### 関連概念:

123 ページの『KPI の作成および統合』

重要業績評価指標 (KPI) モデルは、ビジネス・モニター開発ツールキットおよび KPI 管理ポートレットを使用して作成および変更することができます。

### KPI 更新情報のポリシー

IBM Intelligent Operations Center ポリシーは、着信イベントが KPI イベント更新情報であるかどうかを判別し、そのイベントを送信して、パラメーターに応じて KPI 更新情報またはアラートを生成する処理を行います。 KPI イベントは、共通アラート・プロトコル XML のアラート・ブロックにある `<code>KPI</code>` によって判別されます。

イベントが KPI 更新情報として確認されると、ポリシーは KPI パラメーターを検査して KPI イベント XML を生成し、処理のために IBM WebSphere Business Monitor へ送信します。

以下の表に、KPI イベント更新情報のサンプルを示します。

表 29. KPI イベント・プロパティのサンプル

プロパティ	値
差出人	security@rtp.city.gov
イベント・タイプ	犯罪の応答時間
イベント状況	実動 - すべての対象受信者が実行可能
イベントのスコープ	パブリック - 無制限の対象者に一般的に配布
カテゴリー	セキュリティー
重大度	重度
確信度	可能性が高い
緊急度	即時
メッセージ・タイプ	アラート - 対象受信者が注意する必要がある初期情報
説明	窃盗
送信日時	2012-02-17T17:06:00+01:00
開始日時	2012-02-16T15:47:00+01:00
応答日時	2012-02-17T17:06:00+01:00

以下の表に、表 29 の KPI イベント更新情報に関連付けられている KPI パラメーターのサンプルを示します。

表 30. KPI イベント・パラメーターのサンプル

パラメーター	値
レポート番号	1111
警察管区	警察管区 1
応答日時	2011-02-15T15:05:07-05:00

#### 関連概念:

321 ページの『状況』

「状況」ポートレットでは、単独または複数の組織の重要業績評価指標 (KPI) の状況を確認することができます。

316 ページの『通知』

「通知」ポートレットを使用して、アラート・メッセージとその詳細を表示します。

## 共通アラート・プロトコルとの統合

共通アラート・プロトコル (CAP) は、IBM Intelligent Operations Center と外部システムとの間でイベント情報をやり取りするために使用されます。

CAP は、さまざまなネットワーク上で緊急アラートおよび一般警告をやり取りするための汎用フォーマットです。CAP は、すべてのタイプのアラートおよび通知を対象とした、オープンで非独占のデジタル・メッセージ・フォーマットを提供します。CAP は、Web サービスなど新たに出現した技術との互換性を持つ一方で、より高度な機能も提供しています。これらの機能には、以下のようなものがあります。

- 緯度や経度のシェイプその他 3 次元の地理空間表現を使用した、柔軟な地理的ターゲット設定
- 複数言語および複数の対象者に対応したメッセージ作成
- 段階的適用と遅延に対応した有効期間および期限
- 高度なメッセージ更新および取り消し機能
- 完全かつ効果的な警告メッセージの枠組みを提供するテンプレートのサポート
- デジタル暗号化および署名との互換性
- デジタル・イメージおよびオーディオ機能

イベントは、すべてのコンポーネントへの送信、またはこれらのコンポーネントによる使用が可能な、必要なものを完備したデータ・メッセージです。イベントは、トピック・キューにパブリッシュすることができ、IT システムをサブスクライブしているすべての潜在的利害関係者は、このイベントを読むことができます。CAP を使用すると、イベントの内容を標準化できるので、複数のドメインが、共通の規則を使用して、共通のフォーマットでイベントを送受信できるようになります。この標準は、イベント・レコード内の必須フィールドとオプション・フィールド、およびこれらのフィールドの受け入れ可能な値を定義しています。イベント処理を管理することにより、既存のフォーマットと標準化されたフォーマットとの間を媒介することができます。CAP は、緊急事態だけでなく、日常の運用を処理するように拡張することができます。

イベントには、少なくとも以下の要素が含まれている必要があります。

- 以下の項目を含む一意のイベント ID
  - 送信者 (システムまたは担当者)
  - イベントの送信側組織
  - 送信側システム内のシリアル番号
  - イベント作成のタイム・スタンプ

- 受信者による対応の定義および優先順位付けを可能にする、以下のような情報
  - 緊急度 - 受信者がどの程度迅速にアラートに対応する必要があるか
  - 生命および資産に対する脅威のレベル
  - 確信度 - 100% (イベントの発生が確認された) から 0% (現時点でイベントの発生は予測されていない) の範囲で表現される可能性。
  - 今後発生する可能性のあるイベントの予測時間
  - 以前に報告されており、その継続が報告されているイベントの期間
  - 直ちに修正不可能な状態であることを表す、イベントの予測期間
  - 推奨されるか必須のアクションおよび指示
- イベントの相互関連付けを可能にする、以下のような情報
  - 都市セマンティック・モデルの参照 (存在する場合)
  - 地理空間座標
  - 前提条件イベントまたは促進要因となったイベントへの参照
  - 関係資産の一意的資産 ID
- 人間が判別できる、以下のようなテキストによる記述
  - 位置の説明
  - アクティビティの説明

CAP を使用すると、イベントごとのデータ交換を最小限に抑えることができます。 イベントは XML フォーマットで表現されるため、さまざまなシステムがデータ・フォーマットを記述して読み取ることができます。 これにより、意味のないデータや危険な混乱を招くデータのやり取りを防止できます。

IBM Intelligent Operations Center には、CAP アラートの永続的ストレージと、これらのアラートを表示するための標準インターフェースが用意されています。

IBM Intelligent Operations Center では、CAP の構造全体が受け入れられますが、重要業績評価指標 (KPI) の計算時に IBM Intelligent Operations Center が使用するデータは、そのほんの一部です。

IBM Intelligent Operations Center は、WebSphere Message Broker を使用して、CAP を使用したイベントを統合します。

IBM Intelligent Operations Center は、OASIS 共通アラート・プロトコル・バージョン 1.2 をサポートしています。

## 関連概念:

107 ページの『KPI イベントに対する CAP の使用』

IBM Intelligent Operations Center の一部として提供されている WebSphere Message Broker は、CAP イベント・メッセージを受け入れ、重要業績評価指標 (KPI) の計算にそのデータを使用します。

111 ページの『KPI の計算に使用されないイベントに対する CAP の使用』

CAP データを使用して、KPI 計算に関連付けられていないイベントに関するデータを提供することもできます。

## 関連情報:



OASIS 共通アラート・プロトコル・バージョン 1.2

## CAP の構造

各 CAP アラート・メッセージは、1 つ以上の `<info>` セグメントを含むことが可能な、1 つの `<alert>` セグメントから成っています。各 `<info>` セグメントには、1 つ以上の `<area>` セグメントを含めることができます。ほとんどの場合、`<msgType>` の値が `alert` である CAP メッセージには、少なくとも 1 つの `<info>` エレメントが含まれています。

主なメッセージ・エレメントは以下のとおりです。

- `<alert>`

`<alert>` セグメントは、現在のメッセージに関する基本情報 (目的、ソース、および状況) を提供します。メッセージの固有 ID、および他の関連メッセージへのリンクも含まれています。`<alert>` セグメントは、メッセージの確認応答、取り消し、またはその他のシステム機能用に、単体で使用することができます。しかし、ほとんどのアラート・セグメントには、少なくとも 1 つの `<info>` セグメントが含まれています。

- `<info>`

`<info>` セグメントは、予想されるイベントまたは実際のイベントを、緊急度 (準備に使用可能な時間)、重大度 (影響の強度)、および確信度 (観測または予測の信頼性) の観点から記述します。対象イベントのカテゴリ記述およびテキスト記述も提供されます。`<info>` セグメントは、メッセージ受信者の適切な応答に関する指示や、その他の詳細情報を提供する場合もあります。これには、障害の継続時間、技術的パラメーター、連絡先情報、および追加情報のソースへのリンクなどがあります。複数の `<info>` セグメントを使用することで、さまざまなパラメーター (さまざまな可能性帯域や強度帯域など) の記述や、複数の言語での情報提供ができます。

- `<resource>`

`<resource>` セグメントは、`<info>` セグメントに関連する追加情報への参照を、オプションとして提供します。画像ファイルや音声ファイルなどのデジタル資産を参照することもできます。

- `<area>`

`<area>` セグメントは、`<info>` セグメントの適用先となる地域について記述します。テキスト記述およびコード記述 (郵便番号など) がサポートされていますが、推奨表示では、地理空間の形状、多角形や円、および指定の地理空間データに従い標準の緯度、経度、および高度を単位として表現される高度または高度範囲が使用されます。

## 関連概念:

107 ページの『KPI イベントに対する CAP の使用』

IBM Intelligent Operations Center の一部として提供されている WebSphere Message Broker は、CAP イベント・メッセージを受け入れ、重要業績評価指標 (KPI) の計算にそのデータを使用します。

111 ページの『KPI の計算に使用されないイベントに対する CAP の使用』

CAP データを使用して、KPI 計算に関連付けられていないイベントに関するデータを提供することもできます。

## イベント・タイプ

IBM Intelligent Operations Center では、いくつかの CAP イベント・タイプがサポートされています。

## 実際のイベントと予測されるイベント

実際のイベントおよび予測されるイベントのメッセージは、異常条件または例外に関してさまざまなドメインから送信される非送信請求メッセージです。これらのメッセージでは、イベントが作成される場所での重要業績評価指標 (KPI) 違反も取り扱います。

## 確認応答

確認応答は、<alert> エlementに以下のフィールド値が入力されている CAP メッセージです。

- <msgType> 値は **ACK** に設定されています。これは、<references> で識別されるメッセージの受信と受理を送信者が確認したことを意味します。
- <references> フィールドには、確認応答により参照される、これ以前の CAP メッセージの拡張メッセージ ID (sender, identifier, sent の形式) が含まれています。
- 

注: <info> エlementは、確認応答の場合はオプションです。

## 応答

応答は、<alert> エlementに以下のフィールド値が入力されている CAP メッセージです。

- <msgType> 値は **Alert** です。
- <note> 値は **Response** です。
- <references> エlementには、このメッセージの応答先となる CAP メッセージの ID が入力されている必要があります。

例えば、市のオペレーターが **City Brownout Advisory** を各種ドメインに送信すると、それらのドメインは、その個々の機能に対する影響分析を実行した後で、このアドバイザリーに対する応答を送り返します。

## インシデント

インシデントは、同じインシデントの異なる側面を参照する複数のメッセージを照合するために使用されません。インシデント CAP メッセージは、1 つの特定のインシデントに関連するすべてのイベントのコンテナとしての役割を果たします。これらのイベントは異なるドメインに含まれている場合もあります。

ドメインがアドバイザリーに対して、複数のドメインへの影響があるために調整アクションが必要であることを示す応答を送り返した場合は、アドバイザリーがインシデントにプロモートされます。すべての関連イベントの <incident> エlementに、そのインシデント・イベントの <identifier> 値が取り込まれます。関連イベントとは、<references> 値がインシデント・イベントの <identifier> 値と同じイベントです。

インシデントは、<alert> エlementに以下のフィールド値が入力されている CAP メッセージです。

- <msgType> 値は **Alert** です。
- <note> 値は **Incident** です。
- <references> Elementには、このイベントの親 (根本原因) である CAP メッセージの ID が入力されている必要があります。
- <incidents> Elementには、独自の ID が含まれている必要があります。

## 更新

更新は、<alert> Elementに以下のフィールド値が入力されている CAP メッセージです。

- <msgType> は **update** に設定されています。これは、この更新が、<references> Elementで識別されている、これ以前のメッセージに取って代わることを意味します。
- <references> Elementには、更新により参照されている、これ以前の CAP メッセージの拡張メッセージ ID (sender,identifier,sent の形式) が含まれています。

## キャンセル

取り消しは、<alert> Elementに以下のフィールド値が入力されている CAP メッセージです。

- <msgType> Elementは **Cancel** に設定されています。これは、このメッセージが、<references> Elementで識別されている、これ以前のメッセージを取り消すことを意味します。
- <references> Elementには、この取り消しにより参照されている、これ以前の CAP メッセージの拡張メッセージ ID (sender,identifier,sent の形式) が含まれています。
- <note> Elementには、このアラートがクリアされる理由または方法の説明が含まれています。

## 関連情報:



OASIS 共通アラート・プロトコル・バージョン 1.2

## KPI イベントに対する CAP の使用

IBM Intelligent Operations Center の一部として提供されている WebSphere Message Broker は、CAP イベント・メッセージを受け入れ、重要業績評価指標 (KPI) の計算にそのデータを使用します。

表 31 は、KPI の計算に使用されるデータ・Elementをリストしたものです。

表 31. IBM Intelligent Operations Center による KPI の計算に使用される CAP 要素

必須またはオプション	データ・Element (標準)	説明
必須	Message_ID (identifier)	固有のメッセージ ID
必須	Sender_ID (sender)	固有の送信者 ID



表 31. IBM Intelligent Operations Center による KPI の計算に使用される CAP 要素 (続き)

必須またはオプション	データ・エレメント (標準)	説明
必須	SentDateTime (sent)	メッセージが送信された日時。  例: 2011-02-07T 16:49:00-05:00 には、メッセージが送信された日時が含まれています。最後の 6 文字は、グリニッジ標準時 (GMT) に対する、CAP イベント・タイム・ゾーンを示します。このケースでは、イベントは、GMT から 5 時間を引いた東部標準時 (EST) の 16:49:00 に発生しました。このコードは、イベントが表示される時、EST からユーザーのタイム・ゾーンに変換されることを意味します。CAP イベントを GMT でコーディングする場合は、2011-02-07T 16:49:00-00:00 という例のように、接尾部を -00:00 に変更します。
必須	MessageStatus (status)	メッセージの状況。以下のいずれかのオプションになります。  <ul style="list-style-type: none"> <li>• Actual</li> <li>• Exercise</li> <li>• System</li> <li>• Test</li> <li>• Draft</li> </ul>
必須	MessageType (msgType)	メッセージのタイプ。以下のいずれかのオプションになります。  <ul style="list-style-type: none"> <li>• Alert</li> <li>• Update</li> <li>• Cancel</li> <li>• Ack</li> <li>• Error</li> </ul>
オプション	Source (source)	メッセージのソース
必須	Scope (scope)	Public という値が指定されます
必須	Code (code)	このイベントが「イベント」ポートレット・リストに表示されないように、KPI という値が指定されます

表 31. IBM Intelligent Operations Center による KPI の計算に使用される CAP 要素 (続き)

必須またはオプション	データ・エレメント (標準)	説明
必須	EventCategory (category)	以下のいずれか <ul style="list-style-type: none"> <li>• Geo</li> <li>• Met</li> <li>• Safety</li> <li>• Security</li> <li>• Rescue</li> <li>• Fire</li> <li>• Health</li> <li>• Env</li> <li>• Transport</li> <li>• Infra</li> <li>• CBRNE</li> <li>• Other</li> </ul>
必須	EventType (event)	イベントまたは KPI の説明。 例: Police_Department_Budget
必須	Urgency (urgency)	以下のいずれか <ul style="list-style-type: none"> <li>• Immediate</li> <li>• Expected</li> <li>• Future</li> <li>• Past</li> <li>• Unknown</li> </ul>
必須	Severity (severity)	重大度は、以下のいずれかのオプションで示されます。 <ul style="list-style-type: none"> <li>• Extreme</li> <li>• Severe</li> <li>• Moderate</li> <li>• Minor</li> <li>• Unknown</li> </ul>
必須	Certainty (certainty)	確信度は、以下のいずれかのオプションで示されます。 <ul style="list-style-type: none"> <li>• Observed</li> <li>• Likely</li> <li>• Possible</li> <li>• Unlikely</li> <li>• Unknown</li> </ul>
オプション	EventCode (eventCode)	イベント・タイプの名前と値のペア。
オプション	OnsetDateType (onset)	イベントが開始する日時 例: 2011-02-08T16:49:00-05:00

表 31. IBM Intelligent Operations Center による KPI の計算に使用される CAP 要素 (続き)

必須またはオプション	データ・エレメント (標準)	説明
オプション	SenderName (senderName)	アラートを開始したエンティティの名前。 例: Police Department
オプション	EventDescription (description)	イベントまたは KPI の詳細説明
オプション	Parameter (parameter)	イベントまたは KPI に関連付けられた追加データ。
オプション	AreaGeocode (geocode)	イベントまたは KPI がロケーションに依存する場合に、情報提供のために使用できるフィールド

詳しくは、このトピックの末尾にある OASIS 共通アラート・プロトコル仕様への関連リンクを参照してください。

以下のコードは、自動車事故を報告するイベントの例です。

```
<?xml version="1.0" encoding="UTF-8"?>
<cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2 CAP-v1.2-os.xsd ">
  <cap:identifier>1112</cap:identifier>
  <cap:sender>Transportation</cap:sender>
  <cap:sent>2011-02-17T15:00:00-05:00</cap:sent>
  <cap:status>Actual</cap:status>
  <cap:msgType>Alert</cap:msgType>
  <cap:scope>Public</cap:scope>
  <cap:code>KPI</cap:code>
  <cap:info>
    <cap:category>Transport</cap:category>
    <cap:event>Traffic_Accident</cap:event>
    <cap:urgency>Unknown</cap:urgency>
    <cap:severity>Extreme</cap:severity>
    <cap:certainity>Unknown</cap:certainity>
    <cap:eventCode>
      <cap:valueName>OwningOrg</cap:valueName>
      <cap:value>Police</cap:value>
    </cap:eventCode>
    <cap:onset>2011-02-17T15:00:00-05:00</cap:onset>
    <cap:senderName>Transportation</cap:senderName>
    <cap:description>Single car crash</cap:description>
    <cap:parameter>
      <cap:valueName>accident number</cap:valueName>
      <cap:value>1112</cap:value>
    </cap:parameter>
  </cap:info>
</cap:alert>
```

## 関連概念:

157 ページの『ユーザー・インターフェースのローカライズ』  
ブラウザ設定により、IBM Intelligent Operations Center ユーザー・インターフェースの言語および日時  
の設定が決まります。 管理者は、日付および時刻の形式をカスタマイズできます。

361 ページの『既知の問題および解決策』  
このセクションでは、よく発生する問題のリストと、各項目の解決方法を示します。

## 関連情報:

 OASIS 共通アラート・プロトコル・バージョン 1.2

## KPI の計算に使用されないイベントに対する CAP の使用

CAP データを使用して、KPI 計算に関連付けられていないイベントに関するデータを提供することもできます。

定義された KPI に関連付けられていない CAP データが IBM Intelligent Operations Center で受信されると、そのデータは IBM Intelligent Operations Center 内の「イベント」ポートレットと「マップ」ポートレットに追加されます。

以下のコードは、KPI の計算に使用されないイベントの例です。 KPI の計算に使用されないイベントの場合は、code タグの値を Event に設定する必要があることに注意してください。

```
<p>  
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">  
  <identifier>f30f190c-41fd-431e-ace9-88b725f1a3fc</identifier>  
  <sender>TestGenerator</sender>  
  <sent>2012-03-26T15:47:24-00:00</sent>  
  <status>Actual</status>  
  <msgType>Alert</msgType>  
  <scope>Public</scope>  
  <restriction/>  
  <code>Event</code>  
  <info>  
    <language>en_US</language>  
    <category>Infra</category>  
    <event>Water Main Break</event>  
    <urgency>Immediate</urgency>  
    <severity>Moderate</severity>  
    <certainty>Observed</certainty>  
    <headline>Major water line leak at NW 20th St.</headline>  
    <description>Leak is located at the intersection of NW 20th Street and NW 9th Avenue.  
    Street flooding starting to occur. Immediate action required.</description>  
    <area>  
      <circle>25.79518,-80.21110 0</circle>  
    </area>  
  </info>  
</alert>  
</p>
```

## IBM Intelligent Operations Center に対し定義されているインバウンド・イベント・キューの使用

CAP イベントを組み込みの WebSphere Message Broker インスタンスに送信することで、これらのイベントを IBM Intelligent Operations Center にパブリッシュできます。

パブリッシュを行うクライアントは WebSphere Message Broker CAP イベント入力キューを直接指示するように構成でき、またパブリッシュを行うクライアントは、ポータル・サーバーで定義されている WebSphere Application Server JMS リソースを使用できます。これらの JMS リソースは、CAP イベント

を受信する WebSphere Message Broker キューを指示します。 IBM Intelligent Operations Center のインストール時には、以下の JMS リソースが作成されます。

- キュー接続ファクトリー
  - 名前: ioc.mb.con.factory
  - JNDI 名: jms/ioc.mb.con.factory
- キュー
  - 名前: ioc.cap.in.q
  - JNDI 名: jms/ioc.cap.in.q

#### 関連概念:

130 ページの『IBM WebSphere Business Monitor と IBM Intelligent Operations Center の間の KPI イベント通信』

IBM WebSphere Business Monitor は、モニター・コンテキストまたは重要業績評価指標 (KPI) コンテキストから IBM Intelligent Operations Center へ、アウトバウンド・イベントを送信できます。

## パブリッシャー・サービスを使用したイベントの作成

Web サービスからパブリッシャー・サービスを介して、IBM Intelligent Operations Center にイベントを送信することができます。

IBM Intelligent Operations Center のデプロイ済みインスタンスに統合できるクライアント・アプリケーションを作成できます。クライアント・アプリケーションを使用することで、パブリッシャー・サービスのユーティリティー・クラスによって公開されているメソッドと IBM Intelligent Operations Center パブリッシャー・サブレットを呼び出して、サード・パーティーのクライアント・アプリケーションからの CAP アラートを IBM Intelligent Operations Center に渡すことができます。

### 共通ユーティリティー・クラスを使用した開発

パブリッシャー・サービスを呼び出すクライアント・アプリケーションを作成する場合は、作業を始める前に、共通ユーティリティー・クラスをセットアップする必要があります。クライアント・アプリケーションの開発が完了したら、このアプリケーションを WAR ファイルとしてエクスポートしてから、WebSphere Application Server にインポートします。

#### このタスクについて

共通ユーティリティー・クラスを使用するクライアント・アプリケーションを作成するには、以下の手順を実行します。

- クライアント・アプリケーションを開発する前に、iss\_common および icu4j-4\_4\_2 の各 JAR ファイルを、プロジェクトのビルド・パスに追加します。これらの JAR ファイルは、コンパイル時に必要です。
- クライアント・アプリケーションの開発が完了したら、これを WAR ファイルとしてエクスポートします。
- この WAR ファイルを WebSphere Application Server にインポートし、共有ライブラリーを参照するように構成します。

#### 手順

1. IBM Intelligent Operations Center のインストール・ディレクトリー /opt/IBM/iss/common/lib で、iss\_common.jar ファイルと icu4j-4\_8\_1\_1.jar ファイルを見つけます。

2. iss\_common.jar ファイルと icu4j-4\_8\_1\_1.jar ファイルを、開発マシン上のロケーションにコピーします。
3. JAR ファイルをプロジェクトのビルド・パスに追加するには、IBM Intelligent Operations Center API で、iss\_common.jar と icu4j-4\_8\_1\_1.jar に対して以下のサブステップを実行します。
  - a. 「ポートレット・プロジェクト (Portlet Project)」を右クリックします。
  - b. 「ビルド・パス (Build Path)」 > 「ビルド・パスの構成 (Configure Build Path)」をクリックします。
  - c. 「ライブラリー (Libraries)」タブをクリックし、「外部 JAR の追加... (Add External JARs...)」をクリックします。
  - d. JAR ファイルが保存されているディレクトリーを参照します。
  - e. JAR ファイルをクリックし、「開く (Open)」をクリックします。
4. クライアント・アプリケーションの開発が完了したら、これを WAR ファイルとしてエクスポートします。
5. WebSphere Application Server 管理コンソールで、インポート・ウィザードを使用して、クライアント・アプリケーションの WAR ファイルをインポートします。
6. 共有ライブラリー参照を参照するよう WAR ファイルを構成するには、以下のサブステップを実行します。
  - a. WebSphere Application Server 管理コンソールで、インポートした WAR ファイルの横にあるチェック・ボックスを選択して、「更新」をクリックします。
  - b. 「共有ライブラリー参照」をクリックします。
  - c. 「共有ライブラリー参照」ウィンドウで、「アプリケーション」チェック・ボックスを選択します。
  - d. 「参照共有ライブラリー」をクリックします。
  - e. 「ISSCommonJars」と「IOCCCommonJars」を、「使用可能」リストから「選択済み」リストに移動して、「OK」をクリックします。
  - f. 変更内容を保存するには、「OK」をクリックします。

## パブリッシャー・サービスの使用

パブリッシャー・サービスのイベント・インジェクター・ツールは、Java ユーティリティーとして提供されます。パブリッシャー・サービスによって公開されたメソッドを呼び出すことで、CAP XML を IBM Intelligent Operations Center に渡すクライアント・アプリケーションを作成できます。通知の形で渡すこともできます。

パブリッシャー・サービスは、プロジェクト iss\_common\_utils 内のユーティリティー・クラスです。このプロジェクトは iss\_common.jar ファイルにビルドされます。パブリッシャー・サービスは、静的メソッド publishEvent および publishNotification を公開します。パブリッシャー・サービス用のクライアント・アプリケーションを作成する前に、共通ユーティリティー・クラスをセットアップする必要があります。詳しくは、トピックの末尾にあるリンクを参照してください。

パブリッシャー・サービスを呼び出すために使用されるコードが、正しい JMS キュー構成にアクセスできるようにするには、それをアプリケーション・サーバーにデプロイする必要があります。

以下のコード例は、パブリッシャー・サービスを呼び出す方法を示しています。

```
import com.ibm.iss.common.publisher.Publisher;

String capMessage = request.getParameter(EVENT_TEXT_KEY);

int status = Publisher.publishEvent(capMessage);
```



```

if (status == Publisher.STATUS_SUCCESS) {
logger.traceFine(this, methodName, "Event submit request was performed successfully");
}
else if (status == Publisher.STATUS_EXCEPTION_NAMING) {
logger.traceFine(this, methodName, "Error sending CAP Event Message. Requires defining JMS Resources.");
}
else if (status == Publisher.STATUS_EXCEPTION_JMS) {
logger.traceFine(this, methodName, "Error sending CAP Event Message. Failed to connect to JMS resources.");
}
else { //Other error code
logger.traceFine(this, methodName, "Error sending CAP Event Message. Returned status = " + status);
}

```

「サンプル・パブリッシャー」ポートレットを使用する場合は、パブリッシャー・サービスを呼び出すためのコードを作成したり、CAP メッセージを記述したりする必要はありません。

#### 関連概念:

115 ページの『サンプル・パブリッシャー』

「サンプル・パブリッシャー」ポートレットでは、共通アラート・プロトコル (CAP) イベントを IBM Intelligent Operations Center にパブリッシュすることができます。

#### 関連タスク:

112 ページの『共通ユーティリティ・クラスを使用した開発』

パブリッシャー・サービスを呼び出すクライアント・アプリケーションを作成する場合は、作業を始める前に、共通ユーティリティ・クラスをセットアップする必要があります。クライアント・アプリケーションの開発が完了したら、このアプリケーションを WAR ファイルとしてエクスポートしてから、WebSphere Application Server にインポートします。

## パブリッシャー・サーブレットの使用

パブリッシャー・サーブレットは POST 要求でパラメーターを受け入れて、CAP XML のパブリッシュ、新しいイベントの作成、または既存のイベントまたはインシデントから変更されたイベントの作成を行います。

### パブリッシャー・サーブレットへの POST 要求の送信

パブリッシャー・サーブレットはパブリッシャー・サービスを呼び出して、IBM Intelligent Operations Center にフィードされるキューに CAP XML を配置します。パブリッシャー・サーブレットは `/ibm/iss/common/rest/publisher` にあります。以下の表には、パブリッシャー・サーブレットに POST 要求を送信する方法が示されています。

表 32. パブリッシャー・サーブレットの POST 要求

パブリッシュするイベントのタイプ	POST 要求コード
新しい CAP イベントのパブリッシュ	<code>action=publishEvent&amp;source=xml&amp;xml=CAP_event_XML</code>
既存イベントの変更	<code>action=publishEvent&amp;source=existing&amp;id=event_id</code>
空白の新しいイベントのパブリッシュ	<code>action=publishEvent&amp;source=new</code>

### オプション・パラメーター

`&parameter_name=new_value` というコードを POST 要求に付加することで、各パブリッシュ・オプションにオプション・パラメーターを適用できます。

次のオプション・パラメーターを使用できます。

- `areaDesc`

- category
- certainty
- code
- contact
- description
- event
- headline
- 緯度 (latitude)
- 経度 (longitude)
- msgType
- randomize
- randomizeid
- randomizeArea
- randomizeTime
- sender
- senderName
- severity
- status
- urgency

例えば、空白の新しいイベントをパブリッシュしてから見出しを Traffic に設定するには、POST 要求コードは `servletURL&action=publishEvent&source=new&headline=Traffic Accident` のようになります。

---

## テスト・イベントの作成およびパブリッシュ

IBM Intelligent Operations Center には、テスト・イベントを作成してパブリッシュするための「サンプル・パブリッシャー」ポートレットおよび「イベント・スクリプト記述」ポートレットが用意されています。

### 関連概念:

112 ページの『パブリッシャー・サービスを使用したイベントの作成』

Web サービスからパブリッシャー・サービスを介して、IBM Intelligent Operations Center にイベントを送信することができます。

## サンプル・パブリッシャー

「サンプル・パブリッシャー」ポートレットでは、共通アラート・プロトコル (CAP) イベントを IBM Intelligent Operations Center にパブリッシュすることができます。

「サンプル・パブリッシャー」ポートレットは、ソリューションを管理または検証する管理者を対象とする自動テスト・ツールです。管理者は、「サンプル・パブリッシャー」ポートレットをクライアント・アプリケーションとして使用することで、IBM Intelligent Operations Center における CAP メッセージのパブリッシュをテストすることができます。「サンプル・パブリッシャー」ポートレットを使用すれば、テスト・クライアント・アプリケーションを手動で作成する必要がなくなります。

## イベントと通知の作成

「サンプル・パブリッシャー」ポートレットを起動するには、WebSphere Portal 管理インターフェースで「**Intelligent Operations**」 > 「デモンストレーション・ツール」 > 「サンプル・イベント・パブリッシャー」をクリックします。

「サンプル・パブリッシャー」ポートレットの「**イベント CAP**」タブでは、フォームに入力し、XML を使用してイベントを設計することができます。 フォームを送信して、システムに対するサンプルの CAP イベントのフローをアクティブにします。

「サンプル・パブリッシャー」ポートレットには、新規イベントを作成する際に XML を編集する必要がない場合のための、「**イベント・フォーム**」タブも用意されています。「**イベント・フォーム**」タブでフォームに入力して、CAP イベントの詳細を送信します。 既存のイベントのプロパティを基にプロパティを指定して新規イベントを作成する場合は、その既存のイベントの CAP アラート ID を「**ID**」フィールドに入力します。

「サンプル・パブリッシャー」ポートレットには、IBM Intelligent Operations Center の通知サブシステムをテストするための「**通知**」タブがあります。「**通知**」タブで、フォームに入力して、指定したグループへのアラート通知を送信します。「**通知**」ポートレットのリストに表示されるのは既存のユーザー・グループに対応するアラートのみなので、「**グループに送信済み**」に入力する値は、例えば、CityWideOperator や CityWideExecutive などのような、既存のユーザー・グループに対応するものになります。

## ランダム値

「**イベント CAP**」タブおよび「**イベント・フォーム**」タブで、「**イベントのランダム化**」チェック・ボックスを選択すると、ポートレットがパブリッシュするイベントのプロパティに関する以下の内容のアラートが自動的に発行されます。

- 「**ID**」: イベント ID は IBM Intelligent Operations Center 内で一意である必要があるため、イベントごとに固有の ID スtring が生成されます。
- 「**タイム・スタンプ**」: 連続するそれぞれのイベントが異なる時間に到着できるように、送信されるイベントごとにタイム・スタンプの値がインクリメントされます。
- 「**ロケーション**」: 緯度、経度、および半径に必要な形式に準拠するように、それぞれのイベントの緯度と経度が範囲内でランダム化されます (例: 32.9525,-115.5527 5)。半径の設定は変更されません。

## 「サンプル・パブリッシャー」ポートレットのカスタマイズ

このポートレットはカスタマイズすることができます。 ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。 共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

### 関連資料:

181 ページの『「サンプル・パブリッシャー」ポートレットの設定』  
「共有設定」ウィンドウのフィールドの設定値を変更することによって、「サンプル・パブリッシャー」ポートレットをカスタマイズできます。

## XML を使用したサンプル・イベントの作成

「**イベント CAP**」タブでは、イベントの表示、変更、およびパブリッシュを行うために使用できるサンプルの CAP イベント・テンプレートを選択できます。

## 始める前に

最初に、イベントのカテゴリを選択します。カテゴリは、イベントの分割先となる 1 次エリアを表します。

表 33. イベントのカテゴリ

カテゴリ	説明
CBRNE	化学、生物、放射性物質、核、大型爆発物の脅威または攻撃
環境	汚染その他の環境関連イベント
火災	消火とレスキュー
地理・地形	地すべりなどの地理・地形イベント
ヘルス	医療と公衆衛生イベント
インフラストラクチャー	公益事業、通信、その他輸送以外のインフラストラクチャー・イベント
気象	洪水などの気象イベント
レスキュー	レスキューと復旧
安全	一般的な緊急事態と公共の安全
セキュリティ	法的処置、軍事、国と地域/個人のセキュリティ
輸送	公共および私設の輸送
その他	その他のイベント

## このタスクについて

イベント・プロパティについて詳しくは、このトピックの末尾にある「詳細」ポートレットのトピックへのリンクを参照してください。

## 手順

1. WebSphere Portal Administration インターフェースで、「**Intelligent Operations**」 > 「**デモンストレーション・ツール**」 > 「**サンプル・イベント・パブリッシャー**」をクリックします。
2. 「**イベント CAP**」タブをクリックします。
3. 「**カテゴリ**」リストで、イベントのカテゴリを選択します。
4. 「**イベント・メッセージ**」フィールドでは、以下のいずれかのオプションを選択します。
  - 事前に書かれた、対応する CAP メッセージの XML を、「**イベント・メッセージ**」フィールドに自動的に挿入するには、「**サンプル・イベント**」リストからイベントを選択します。必要な場合は、要件に合わせて XML を編集します。
  - 「**イベント・メッセージ**」フィールドで、CAP メッセージの XML を、最初から手動で入力します。
5. 「**イベント・インスタンス数**」フィールドでは、必要なメッセージの数を入力するか、矢印を使用して必要なメッセージの数を選択します。単一の CAP メッセージを送信することも、自動化された一連のメッセージを送信することもできます。
6. オプション: 「**イベントのランダム化**」チェック・ボックスを選択します。「**イベントのランダム化**」を選択すると、一連の CAP メッセージが、ランダムな ID を適用された状態でパブリッシュされます。これらのメッセージは、時間間隔をインクリメントしながら、範囲内のランダムな場所にパブリッシュされます。
7. 「**イベントの送信**」をクリックします。

## タスクの結果

サンプル・パブリッシャーは、IBM Intelligent Operations Center にイベント・データを取り込んで、KPI を起動できます。

### 関連概念:

301 ページの『詳細』

「詳細」ポートレットを使用して、IBM Intelligent Operations Center でイベントの表示、モニター、および管理を行います。

## XML を使用しない新規 CAP イベントの作成または既存イベントの更新

「イベント・フォーム」タブでは、フォームに記入することで、XML を使用せずに、新規 CAP イベントの作成または既存イベントの更新を行うことができます。

### このタスクについて

フォームを使用して、新規イベントの作成、または既存イベントの値に基づいたイベントの作成を行うことができます。既存イベントに基づいてイベントを作成する場合は、CAP アラート ID を使用して既存イベントを参照します。フォームに値を入力すると、既存 CAP イベントから継承された値が上書きされます。イベント・プロパティについて詳しくは、このトピックの末尾にある「詳細」ポートレットのトピックへのリンクを参照してください。

### 手順

1. WebSphere Portal Administration インターフェースで、「**Intelligent Operations**」 > 「デモンストレーション・ツール」 > 「サンプル・イベント・パブリッシャー」をクリックします。
2. 「イベント・フォーム」タブをクリックします。
3. イベントのソースを指定するには、「ソース」の横にある以下のオプションのうちいずれかをクリックします。
  - フォームに入力した値に基づく値で新規イベントを作成する場合は、「**新規**」をクリックします。
  - CAP イベント・テーブル内の既存イベントに基づく値で、CAP アラート ID を使用してイベントを作成する場合は、「**既存**」をクリックします。
4. 新規イベントを作成するか、既存の CAP アラート ID に基づくイベントを作成するかに応じて、「**ID**」フィールドに以下のようにして ID を入力します。
  - 新規イベントを作成する場合は、必要に応じて「**ID**」フィールドに値を入力します。値を入力しない場合は、固有 ID が自動的に生成されます。
  - 既存の CAP アラート ID の値に基づいてイベントを作成する場合は、CAP アラート ID を「**ID**」フィールドに入力します。フォームに値を入力すると、既存 CAP イベントから継承された値が上書きされます。
5. 新規イベントを作成する場合は、「**イベント・タイプ**」フィールドに、以下のイベント・タイプのいずれかを入力します。

#### アラート

新規イベント。

**更新** 以前に作成されたイベントの更新。

#### 取り消し (Cancellation)

以前に作成されたイベントの取り消し。

6. 「**見出し**」フィールドに、見出しを入力します。

7. 「メッセージ・タイプ」リストから、メッセージ・タイプを選択します。
8. 新規イベントを作成する場合は、「イベント・コード」リストから、「イベント」または「インシデント」を選択します。インシデントは、イベントよりも重大度が上です。
9. 「カテゴリ」リストから、カテゴリを選択します。
10. 「緊急度」リストから、緊急度を選択します。
11. 「重大度」リストから、重大度を選択します。
12. 「確信度」リストから、確信度を選択します。
13. 「説明」フィールドに、説明を入力します。
14. 「送信者」フィールドに、イベントの送信者の説明を入力します。
15. 「イベント・インスタンス数」フィールドで、必要なメッセージ数を選択します。単一の CAP メッセージを送信することも、自動化された一連のメッセージを送信することもできます。
16. オプション: 「イベントのランダム化」チェック・ボックスを選択します。「イベントのランダム化」を選択すると、一連の CAP メッセージが、ランダムな ID を適用された状態でパブリッシュされます。これらのメッセージは、時間間隔をインクリメントしながら、範囲内のランダムな場所にパブリッシュされます。
17. 「イベントの送信」をクリックします。

#### 関連概念:

301 ページの『詳細』

「詳細」ポートレットを使用して、IBM Intelligent Operations Center でイベントの表示、モニター、および管理を行います。

## テスト通知

「通知」タブを使用して、IBM Intelligent Operations Center で通知サブシステムをテストするためのテスト通知を作成します。

### このタスクについて

「通知」タブでフォームに入力し、指定したグループへのアラートを送信します。ユーザーが通知で指定された「送信先グループ」のいずれかのメンバーである場合のみ、その特定のユーザーに対してアラート通知メッセージが「通知」ポートレットに表示されます。

### 手順

1. WebSphere Portal Administration インターフェースで、「Intelligent Operations」 > 「デモンストレーション・ツール」 > 「サンプル・イベント・パブリッシャー」をクリックします。
2. 「通知」タブをクリックします。
3. アラートを作成するには、「タイプ」リストから Alert を選択します。
4. オプション: 「カテゴリ」リストから、カテゴリを選択します。
5. オプション: 「見出し」フィールドに見出しを入力します。
6. オプション: 「説明」フィールドに説明を入力します。
7. オプション: 「送信者」フィールドに、イベントの送信者の説明を入力します。
8. オプション: 「送信先グループ」フィールドに、アラートの送信先となるグループをセミコロンで区切ったリストを入力します。例えば、;CityWideOperator;CityWideExecutive; のように入力します。

注: 各グループ名の間セミコロンを挿入するほかに、リストの最初と最後にセミコロンを挿入するようにしてください。



パブリッシュすると、CityWideOperator グループと CityWideExecutive グループのメンバーであるユーザーに対してのみ、「通知」ポートレットにこのアラート通知が表示されます。

9. オプション: 必要に応じて、以下のいずれかを行います。

- 「**アラートへの参照**」フィールドに、新しいアラートの参照先となる CAP イベント ID をセミコロンで区切ったリストを入力します。
- 「**KPI への参照**」フィールドに、新しいアラートの参照先となる KPI をセミコロンで区切ったリストを入力します。

10. 「**通知の送信**」をクリックします。

#### 関連概念:

316 ページの『通知』

「通知」ポートレットを使用して、アラート・メッセージとその詳細を表示します。

## イベント・スクリプト記述

「イベント・スクリプト記述」ポートレットを使用して、事前に定義された時間間隔でパブリッシュされるイベントの順次リストを作成するスクリプトを記述します。

「イベント・スクリプト記述」ポートレットを起動するには、WebSphere Portal 管理インターフェースで「**Intelligent Operations**」 > 「**デモンストレーション・ツール**」 > 「**イベント・スクリプト記述**」をクリックします。

「イベント・スクリプト記述」ポートレットでは、パブリッシュされるイベントを IBM Intelligent Operations Center データベースのサンプル・イベント・テーブルに記録されているイベント ID に基づいて参照するスクリプトを記述することができます。スクリプトでは、パブリッシュされるイベント間の遅延を指定することができます。スクリプトを実行すると、システムでバックエンドを使用してイベントがパブリッシュされます。ただし、イベント・フローは、外部ソースからシステムに入ってくるイベントのそれと同じです。

また、イベントを IBM Intelligent Operations Center データベースから消去することもできます。イベントを IBM Intelligent Operations Center データベースから消去すると、「マップ」ポートレットおよび「詳細」ポートレットに表示されているすべてのイベントが削除されます。

「イベント・スクリプト記述」ポートレットを使用する前に、イベントを IBM Intelligent Operations Center データベースのサンプル・イベント・テーブルで確認することができます。

「イベント・スクリプト記述」ポートレットでは、事前に定義された時間間隔でパブリッシュされるイベントの順次リストを定義する JSON スクリプトを、サンプルに従って作成できます。スクリプトを実行する前に、「**クリーンアップと検証**」ボタンをクリックして、スクリプトをクリーンアップして検証する必要があります。

イベントは、特定の ID を使用して 1 回だけパブリッシュすることができます。同じ ID を再び使用してイベントをパブリッシュするには、その前に、すべてのイベントを IBM Intelligent Operations Center データベースから削除する必要があります。ただし、「**ID のランダム化**」チェック・ボックスを選択すれば、「イベント・スクリプト」ポートレットによって同じイベントが再びパブリッシュされ、そのイベントにはランダム ID が適用されます。



## サンプル・イベント・テーブルでのサンプル・イベントと KPI イベントの表示

「イベント・スクリプト記述」ポートレットは、IBM Intelligent Operations Center データベースのサンプル・イベント・テーブルから、サンプル・イベントをパブリッシュします。以下の手順に従って、サンプル・イベント・テーブルでイベントを表示します。

### 手順

1. VNC クライアントを使用してデータ・サーバーに root ユーザーとしてログオンし、コマンド・ウィンドウを開きます。以下の手順では、データ・サーバーで開いた直後のコマンド・ウィンドウにコマンドを入力します。
2. DB2 Control Center を開くことができるようにするには、アクセス制御を一時的にオフにする必要があります。このためには、コマンド `xhost +` を入力します。
3. DB2 Control Center で、以下のようにしてサンプル・イベント・テーブルにあるサンプル・イベントを表示し、サンプル・イベントの ID 番号を取得します。
  - a. DB2 Control Centerを開くには、以下のコマンドを入力します。

```
su - db2inst1
db2cc
```
  - b. DB2 Control Center で、「すべてのデータベース」 > 「IOCDB」 > 「表」 > 「REF\_SAMPLEEVENTS」をクリックします。
  - c. 「REF\_SAMPLEEVENTS」表を右クリックし、「開く」をクリックします。サンプル・イベント・テーブルには 40 行がありますが、イベントのパブリッシュ後は 1 から 8 までのイベントのみが「詳細」ポートレットに表示されます。その他のイベントは KPI のテスト用です。「イベント・スクリプト記述」ポートレットで「ID のランダム化」チェック・ボックスを選択すると、同じ 8 つのイベントを繰り返しパブリッシュできます。
  - d. 「イベント・スクリプト記述」ポートレットでイベント・スクリプトを作成するときに参照するため、各サンプル・イベントの **SAMPLEID** に注意してください。 **SAMPLEID** の値は、イベント ID に対応します。
4. サンプル・イベントの表示が終了したら、DB2 Control Center を閉じます。
5. root ユーザーに戻すには、コマンド `exit` を入力します。
6. アクセス制御を再びオンにするには、コマンド `xhost -` を入力します。

### 関連概念:

136 ページの『サンプル KPI』

IBM Intelligent Operations Center では、サンプル KPI が提供されています。このサンプル KPI は、IBM WebSphere Business Monitor 開発ツールキットを使用してさまざまなタイプの KPI を実装するためのガイダンスを提供するように設計されています。水道、輸送、および公共安全用のサンプル・モニター・モデルが提供されています。

## イベント・スクリプトの作成

一連のイベントを事前に定義された時間間隔でパブリッシュする、イベント・スクリプトを作成します。

### 始める前に

「イベント・スクリプト記述」ポートレットを使用してイベントをパブリッシュする前は、IBM Intelligent Operations Center データベースのサンプル・イベント・テーブルにイベントが表示されています。

## このタスクについて

「イベント・スクリプト記述」ポートレットでイベント・スクリプトを作成するには、以下のステップを実行します。

注: イベントは、特定の ID を使用して 1 回だけパブリッシュすることができます。同じ ID のイベントを再度パブリッシュできるようにするには、「データベースのリセット」をクリックして、すべてのイベントを IBM Intelligent Operations Center データベースから削除します。別の方法として、ランダムな ID を適用して同じイベントをパブリッシュするには、「ID のランダム化」チェック・ボックスを選択します。

### 手順

1. WebSphere Portal Administration インターフェースで、「**Intelligent Operations**」 > 「**デモンストレーション・ツール**」 > 「**イベント・スクリプト記述**」をクリックします。
2. 「イベント・スクリプト記述」ポートレットに示されている例を使用して、事前に定義された時間間隔でパブリッシュされるイベントの順次リストを定義する JSON スクリプトを作成します。スクリプトは、例の左側にあるフィールドに入力します。「イベント・スクリプト記述」ポートレットに示されている JSON スクリプトの例を、以下のコードにも示します。

```
[
  {
    "id": 2
    //ID of element in Sample Events table
    "delayAfter": 4000
    //Milliseconds to wait after publishing the event with the current ID
  },
  {}, //Empty objects are ignored
  {
    "id": 1
    //If the command specifies only an ID, the next command is processed
    //directly after the previous command
  },
  {
    "delayAfter": 0
    //If the command specifies only a delay, no event is published and the
    //script waits until the next command is due
  }
]
```

3. オプション: ランダムな ID を適用して同じイベントを再度パブリッシュするには、「**ID のランダム化**」チェック・ボックスを選択します。
4. 必須: スクリプトを実行する前に、このスクリプトをクリーンアップして検証するには、「**クリーンアップと検証**」をクリックします。スクリプトの構文が検証され、コメントが削除されます。解決できないスクリプト内に間違ったマークアップが検出されると、メッセージが表示されます。
5. スクリプトを実行するには、「**イベント・スクリプトを実行**」をクリックします。
6. IBM Intelligent Operations Center データベースからすべてのイベントを削除して、その後スクリプトがイベントをパブリッシュしないようにするには、「**データベースのリセット**」をクリックします。

#### 関連タスク:

121 ページの『サンプル・イベント・テーブルでのサンプル・イベントと KPI イベントの表示』  
「イベント・スクリプト記述」ポートレットは、IBM Intelligent Operations Center データベースのサンプル・イベント・テーブルから、サンプル・イベントをパブリッシュします。以下の手順に従って、サンプル・イベント・テーブルでイベントを表示します。

---

## KPI の作成および統合

重要業績評価指標 (KPI) モデルは、ビジネス・モニター開発ツールキットおよび KPI 管理ポートレットを使用して作成および変更することができます。

IBM WebSphere Business Monitor 開発ツールキットは、Rational Application Developer とともにインストールできます。どちらも IBM Intelligent Operations Center で提供されています。また IBM WebSphere Business Monitor 開発ツールキットは、WebSphere Integration Developer とともにインストールできます。

KPI を定義または変更する前に、KPI が基づく 共通アラート・プロトコル (CAP) アラートを理解する必要があります。例えば、水源の水位を追跡する KPI を定義する場合、水源の名前や水深 (フィート単位) など、追跡する必要がある要素を含む CAP 要素を認識する必要があります。KPI をこのように追加または変更した後、その KPI を IBM WebSphere Business Monitor サーバーにデプロイする必要があります。

IBM WebSphere Business Monitor および IBM WebSphere Business Monitor 開発ツールキットの使用に関する追加情報については、IBM WebSphere Business Monitor インフォメーション・センターを参照してください。

IBM WebSphere Business Monitor を通じて KPI モデルおよびメトリックを設定したら、「重要業績評価指標」ポートレットを使用して、KPI を開発および変更することができます。

## 関連概念:

136 ページの『サンプル KPI』

IBM Intelligent Operations Center では、サンプル KPI が提供されています。このサンプル KPI は、IBM WebSphere Business Monitor 開発ツールキットを使用してさまざまなタイプの KPI を実装するためのガイドランスを提供するように設計されています。水道、輸送、および公共安全用のサンプル・モニター・モデルが提供されています。

101 ページの『イベントと KPI』

IBM Intelligent Operations Center は、イベントと重要業績評価指標 (KPI) を処理して、情報の表示方法を決定します。

185 ページの『KPI のカスタマイズ』

IBM Intelligent Operations Center では、ビジネス・プロセスに適合するよう重要業績評価指標 (KPI) モデルをカスタマイズできます。

## 関連資料:

74 ページの『ソリューションに付属するツールのインストール』

IBM Intelligent Operations Center には、ツールキットと開発ツールが付属しています。これらは、IBM Intelligent Operations Center をカスタマイズするときに使用します。

## 関連情報:



IBM WebSphere Business Process Management バージョン 7.0 インフォメーション・センター

## モニター・モデルと KPI

モニター・モデルは、メトリックおよび重要業績評価指標 (KPI)、着信イベントに対するこれらの依存関係、ビジネス・アクションを必要とする状態、およびビジネス・アクションを起動する可能性のある状態を知らせるアウトバウンド・イベントを定義します。

モニター・モデルには、以下のサブモデルを収容できます。

- モニター詳細モデル
- KPI モデル (KPI model)
- 寸法モデル
- 視覚モデル
- イベント・モデル

モニター詳細モデルには、ほとんどのモニター・モデル情報が収容されています。

IBM Intelligent Operations Center に付属のサンプル・モニター・モデルでは、視覚モデルまたはディメンション・モデルは使用しません。

モニター詳細モデルは、1 つ以上のモニター・コンテキストを定義します。モニター・コンテキストは、1 つ以上の着信イベントから収集されモニターされる情報を定義します。IBM Intelligent Operations Center の場合、モニター対象エンティティは CAP アラートです。これらのアラートから収集される情報を使用して、KPI を計算します。

KPI モデルには、1 つ以上の KPI コンテキストが含まれています。これらは、KPI と KPI に関連付けられたトリガーおよびイベントを定義します。KPI コンテキストは、インバウンド・イベントを処理し、繰り返し発生する待機時間トリガーを評価して、アウトバウンド・イベントを送信できます。例えば、KPI コンテキストは、KPI が定義済みの範囲外にあるかどうかを検査して、通知を送信できます。

イベント・モデルは、モニター・モデル内で使用されるすべてのイベント・インバウンド定義およびイベント・アウトバウンド定義を参照します。 イベント・モデルは、個々のイベント部分の構造を記述したスキーマを参照します。

#### 関連概念:

136 ページの『サンプル KPI』

IBM Intelligent Operations Center では、サンプル KPI が提供されています。 このサンプル KPI は、IBM WebSphere Business Monitor 開発ツールキットを使用してさまざまなタイプの KPI を実装するためのガイドランスを提供するように設計されています。 水道、輸送、および公共安全用のサンプル・モニター・モデルが提供されています。

#### 関連情報:



IBM Business Monitor インフォメーション・センター

## モニター・コンテキスト・インスタンス

モニター・コンテキスト・インスタンスは、モニター・コンテキスト内で特定の時点で収集される情報です。

IBM Intelligent Operations Center では、モニター・コンテキスト・インスタンスは CAP アラートに対応します。 CAP アラートが受信されると、モニター・コンテキスト・インスタンスが作成または再利用され、そのコンテキスト・インスタンス内のメトリックに、モニター・コンテキストに基づいて、CAP アラートの値が設定されます。

モニター・コンテキストは、各 CAP アラートに対して新規インスタンスを作成するよう、または既存のインスタンスを再利用するよう定義することができます。 例えば、特定のリソースについて、水量レベルを毎日サンプリングして、KPI で 1 週間の平均水量レベルを計算する場合は、各 CAP アラートに対して新規モニター・コンテキスト・インスタンスを作成します。 各インスタンスには、その日の水量レベルが格納されており、KPI によって 7 日間の測定値の平均が算出されます。

KPI は、モニター・コンテキストに定義されたメトリックを使用して計算されます。 集約 KPI を定義するときは、モニター・コンテキストと、KPI 集約関数の入力として使用するメトリックを指定します。

KPI の評価時には、モニター・コンテキスト・インスタンスのメトリック値が集約関数によって使用され、KPI 値が計算されます。

#### 関連概念:

136 ページの『サンプル KPI』

IBM Intelligent Operations Center では、サンプル KPI が提供されています。 このサンプル KPI は、IBM WebSphere Business Monitor 開発ツールキットを使用してさまざまなタイプの KPI を実装するためのガイドランスを提供するように設計されています。 水道、輸送、および公共安全用のサンプル・モニター・モデルが提供されています。

#### 関連情報:



IBM Business Monitor インフォメーション・センター

## KPI のモデル化

KPI をモデル化するには、IBM WebSphere Business Monitor 開発ツールキットがインストールされている Rational Application Developer または WebSphere Integration Developer を使用します。 Rational Application Developer および IBM WebSphere Business Monitor 開発ツールキットは、IBM Intelligent Operations Center の一部として組み込まれています。

## このタスクについて

KPI は、Rational Application Developer または WebSphere Integration Developer のいずれかと IBM WebSphere Business Monitor 開発ツールキットを使用してモデル化されます。これらのツールの使用について詳しくは、これらの製品のインフォメーション・センターを参照してください。

モニター・モデルは、ビジネス・モニター・プロジェクト内に収容されています。モデルおよびプロジェクトは、IBM WebSphere Business Monitor 開発ツールキットで提供される Rational Application Developer ビジネス・モニター・ウィザードを使用して作成されます。

KPI をモデル化するには、以下の手順に従います。

### 手順

1. IBM Intelligent Operations Center が受け取る CAP アラートの内容を把握します。
2. KPI の目的を把握します。制限に達するか超えた場合に、KPI はアクションを生成しますか。履歴データまたは統計データを計算するのに KPI を使用しますか。
3. モニター・コンテキストの名前を決めます。IBM Intelligent Operations Center の命名規則では、CAP イベント・タイプを名前として使用することになっています。IBM Intelligent Operations Center に付属のサンプルは、IBM WebSphere Business Monitor に送信される CAP アラート・メッセージごとに、異なるモニター・コンテキストを作成します。
4. IBM WebSphere Business Monitor 開発ツールキットがインストールされている Rational Application Developer または WebSphere Integration Developer で、モニター・コンテキストに対して、インバウンド・イベント、キー、および一連のメトリックを定義します。インバウンド・イベントは、コンテキストによってモニターされる CAP アラート・メッセージを定義し、キーはコンテキスト・インスタンスを一意的に定義し、メトリックは CAP アラート・メッセージから抽出された情報を定義します。
5. イベントの CAP スキーマを指定します。このスキーマは、モニター・プロジェクトに存在する必要があります。IBM Intelligent Operations Center には、サンプルの `icoc_sample_monitor_models` モデリング・プロジェクトに CAP v1.2 スキーマのコピーがあります。
6. ビジネス・モニター・インバウンド・イベントごとに、名前および ID を指定します。イベント ID には、スペースや特殊文字を含めることはできません。デフォルトでは、スペースを下線で置換した名前から ID が作成されます。IBM Intelligent Operations Center に付属するすべてのサンプルは、デフォルトの要素 ID を使用します。
7. スキーマを指定します。スキーマは、IBM WebSphere Business Monitor へのインバウンド・イベントの構造を定義します。
8. 目的に合わせて、CAP メッセージのフィルター処理を定義します。例えば、モニターの対象を特定のイベント・タイプまたは重大度に制限します。
9. CAP メッセージから抽出するメトリックを指定します。
10. モニター・コンテキスト・インスタンスを一意的に識別するコンテキスト・キーを定義します。キー値は、モニター・コンテキストが作成されると、インバウンド・イベントによって指定されます。
11. インバウンド・イベントの相関を取るかどうかを指定します。
12. KPI コンテキストを指定します。KPI コンテキストは、KPI と KPI 関連トリガーおよびイベントのコンテナです。モニター・コンテキストとは異なり、KPI コンテキストにはキーもメトリックもありません。KPI コンテキストは、KPI を作成する前にコンテナとして作成しておく必要があります。
13. 前に定義した KPI コンテキストの内部に、KPI を作成します。
14. KPI のタイプ（「**10 進数**」または「**期間**」）を指定します。



15. KPI の範囲、値、および色インジケータを定義します。 IBM Intelligent Operations Center KPI の大半のサンプルでは、3 つの範囲とそれに関連する色が定義されます。

表 34. サンプル KPI の範囲および色の定義

名前	色	RGB
許容可能	緑	699037
注意	黄	FDBA1A
対処	赤	C32E14

16. KPI の計算方法を定義します。 KPI の値は、2 つの方法のうちいずれか一方で決まります。 集約関数を使用したメトリックから値を計算した場合、KPI は集約 KPI と呼ばれます。 他の KPI またはユーザー定義の XPath 関数に基づいて値を計算した場合、KPI は式 KPI と呼ばれます。

IBM Intelligent Operations Center のサンプルでは、最低レベルの KPI (子のない KPI) が集約 KPI として定義されます。 より高いレベルの KPI (子を持つ KPI) は式 KPI として定義されます。

集約 KPI の値は、IBM WebSphere Business Monitor サーバーに送信された CAP アラート・メッセージで送信されるデータを取り込んだメトリックを基に計算されます。 その後、このデータに対して集約関数が実行されます。 集約関数には、以下の関数が含まれます。

- 平均
- 最大
- 最小
- 合計
- 出現回数
- 標準偏差

値は、定量化できる測定値として表されます。 例えば、犯罪の平均応答時間 (5 分 7 秒) や平均水位 (100.5) などです。

式 KPI の値は、KPI の範囲および計算値を基に計算されます。 IBM Intelligent Operations Center のサンプルでは、親 KPI の計算値により、KPI の値が、その子 KPI の値に応じて 0、1、または 2 と求められます。 値 0 は許容可能な範囲に、値 1 は注意の範囲に、値 2 は対処の範囲に対応付けられます。 このサンプルは、計算式を使用して、KPI の値をその子 KPI の最高の緊急度に設定します。

17. オプション: 集約 KPI の時間フィルターを指定します。 集約 KPI では、KPI 値の計算時間を制限するオプションの時間フィルターを設定できます。 この時間は、繰り返しの間隔 (最終完了期間や現在の期間など)、回転間隔、または固定間隔のいずれでも構いません。 IBM Intelligent Operations Center 集約 KPI のすべてのサンプルには、時間フィルターが定義されています。
18. オプション: KPI のデータ・フィルターを指定します。 例えば、犯罪の平均応答時間を計算するとき、警察管区 1 が対象で、他の管区は対象外にする場合は、データ・フィルターを使用して、他のモニター・コンテキストをすべて削除できます。
19. トリガー、IBM WebSphere Business Monitor サーバーへのインバウンド・イベント、および IBM Intelligent Operations Center へのアウトバウンド・イベントなどの、KPI 値を更新する方法を定義します。
20. KPI をテストします。 IBM WebSphere Business Monitor 開発ツールキットには、デプロイ前に KPI をテストするためのテスト環境があります。 詳しくは、このトピックの末尾にあるリンクを参照してください。
21. モニター・モデル・アプリケーションをデプロイします。

## 関連概念:

### 『KPI 階層の定義』

KPI 間の親子関係を定義して、KPI が IBM Intelligent Operations Center 内でどのように表示されるかを設計できます。 ビジネス・プロセスに適した方法で KPI を参照できるよう、独自の KPI 階層を設計します。

### 136 ページの『サンプル KPI』

IBM Intelligent Operations Center では、サンプル KPI が提供されています。 このサンプル KPI は、IBM WebSphere Business Monitor 開発ツールキットを使用してさまざまなタイプの KPI を実装するためのガイダンスを提供するように設計されています。 水道、輸送、および公共安全用のサンプル・モニター・モデルが提供されています。

### 130 ページの『IBM WebSphere Business Monitor と IBM Intelligent Operations Center の間の KPI イベント通信』

IBM WebSphere Business Monitor は、モニター・コンテキストまたは重要業績評価指標 (KPI) コンテキストから IBM Intelligent Operations Center へ、アウトバウンド・イベントを送信できます。

## 関連タスク:

### 134 ページの『モニター・モデルのデプロイ』

重要業績評価指標 (KPI) とそのモニター・モデルを定義した後、モニター・モデルを IBM Intelligent Operations Center アプリケーション・サーバーで実行されている IBM WebSphere Business Monitor にデプロイする必要があります。

## 関連資料:

### 74 ページの『ソリューションに付属するツールのインストール』

IBM Intelligent Operations Center には、ツールキットと開発ツールが付属しています。 これらは、IBM Intelligent Operations Center をカスタマイズするときに使用します。

## 関連情報:



Rational Application Developer インフォメーション・センター



IBM Business Monitor インフォメーション・センター



XML Path Language (XPath) 2.0 (Second Edition)

## KPI 階層の定義

KPI 間の親子関係を定義して、KPI が IBM Intelligent Operations Center 内でどのように表示されるかを設計できます。 ビジネス・プロセスに適した方法で KPI を参照できるよう、独自の KPI 階層を設計します。

IBM WebSphere Business Monitor では、ある KPI の値に基づいた別の KPI は許可されますが、KPI 間の親子関係の定義は許可されません。 このタスクを簡素化するため、IBM Intelligent Operations Center には、管理者向けの「重要業績評価指標」ポートレットが用意されています。 このポートレットについては、このトピックの末尾にあるリンクを参照してください。

IBM Intelligent Operations Center のサンプル KPI は、階層設計により、一連の Police Department KPI を以下のように定義します。

```
Police Department ----- level 1
  Crime Response Time ----- level 2
    Crime Response Time Precinct One ----- level 3
    Crime Response Time Precinct Two ----- level 3
```

この例では、Police Department に、1 つの子 Crime Response Time があります。Crime Response Time には、2 つの子 Crime Response Time Precinct One および Crime Response Time Precinct Two があります。

2 つのレベル 3 の KPI が、KPI モデル内に集約 KPI として定義されます。つまり、これらの値は、メトリック値および集約関数を使用して計算されます。このセット内にある他のすべての KPI は式 KPI であり、それらの値は他の KPI の値を基に計算されます。例えば、以下のようなものがあります。

- Crime Response Time は、Crime Response Time Precinct One および Crime Response Time Precinct Two の値に基づいています。
- Police Department は、Crime Response Time の値に基づいています。

IBM Intelligent Operations Center は、「重要業績評価指標」ポートレットの使用に代わる、KPI 関係を定義するための手段をサポートしています。システム・プロパティ・テーブルで **UseDBModelReader** パラメーターが TRUE に設定された「重要業績評価指標」ポートレットがデフォルトの方法です。システム・プロパティ・テーブルでの設定の変更については、このトピックの末尾にあるリンクをクリックしてください。KPI 関係を定義する代替方法については、このトピックの末尾にあるリンクをクリックしてください。

#### 関連概念:

186 ページの『重要業績評価指標』

「重要業績評価指標」ポートレットでは、IBM Intelligent Operations Center の重要業績評価指標 (KPI) およびそれらの階層表示をカスタマイズすることができます。

197 ページの『システム全体の構成データの指定』

IBM Intelligent Operations Center システム・プロパティ・テーブルは、IBM Intelligent Operations Center の構成データを保管します。

『OWL を使用した KPI 階層の定義』

IBM Intelligent Operations Center は、KPI 親子関係を定義する手段として、「重要業績評価指標」ポートレットを使用する代わりに、OWL (Web オントロジー言語) の使用をサポートしています。

## OWL を使用した KPI 階層の定義

IBM Intelligent Operations Center は、KPI 親子関係を定義する手段として、「重要業績評価指標」ポートレットを使用する代わりに、OWL (Web オントロジー言語) の使用をサポートしています。

KPI 親子関係は、IBM Intelligent Operations Center が読み取って処理する OWL で定義できます。この定義は、RDF (Resource Description Framework) ファイルで保管されます。

KPI データベース・モデルを RDF ファイルから読み取るようにするかどうかを指定できます。システム・プロパティ・テーブルでこのプロパティを変更する方法については、このトピックの末尾にあるリンクを参照してください。

Police Department サンプル KPI セットの OWL 定義の例を以下に示します。

```
<icop:KPIDefinition rdf:ID="Police_Department">
<icop:KPIBase.name>Police Department</icop:KPIBase.name>
<icop:KPIBase.id>Police_Department</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_ModelDefinition
  rdf:resource= "#icoc_sample_public_safety_monitor_model"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time">
<icop:KPIBase.name>Crime Response Time</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Police_Department"/>
```

```

</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_One">
<icop:KPIBase.name>Crime Response Time Precinct One</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_One</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >

<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_Two">
<icop:KPIBase.name>Crime Response Time Precinct Two</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_Two</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >

```

注: OWL は RDF に基づいて作成される言語です。 OWL と RDF は似ていますが、OWL の方が強力な言語です。 OWL は、RDF よりも語彙が豊富で、構文が強力であり、機械の解釈可能度が高い言語です。

#### 関連概念:

128 ページの『KPI 階層の定義』

KPI 間の親子関係を定義して、KPI が IBM Intelligent Operations Center 内でどのように表示されるかを設計できます。 ビジネス・プロセスに適した方法で KPI を参照できるよう、独自の KPI 階層を設計します。

186 ページの『重要業績評価指標』

「重要業績評価指標」ポートレットでは、IBM Intelligent Operations Center の重要業績評価指標 (KPI) およびそれらの階層表示をカスタマイズすることができます。

197 ページの『システム全体の構成データの指定』

IBM Intelligent Operations Center システム・プロパティ・テーブルは、IBM Intelligent Operations Center の構成データを保管します。

## IBM WebSphere Business Monitor と IBM Intelligent Operations Center の間の KPI イベント通信

IBM WebSphere Business Monitor は、モニター・コンテキストまたは重要業績評価指標 (KPI) コンテキストから IBM Intelligent Operations Center へ、アウトバウンド・イベントを送信できます。

IBM WebSphere Business Monitor サーバーからのアウトバウンド・イベントは、外部メッセージ・キューに置かれます。 IBM Intelligent Operations Center はこの仕組みを使用して、KPI 更新情報を非同期で受信します。

注: IBM WebSphere Business Monitor への接続について、セキュア接続のために SSL を使用するかどうかを指定できます。 システム・プロパティ・テーブルでこのプロパティを変更する方法については、このトピックの末尾にあるリンクを参照してください。

## 関連概念:

197 ページの『システム全体の構成データの指定』

IBM Intelligent Operations Center システム・プロパティ・テーブルは、IBM Intelligent Operations Center の構成データを保管します。

111 ページの『IBM Intelligent Operations Center に対し定義されているインバウンド・イベント・キューの使用』

CAP イベントを組み込みの WebSphere Message Broker インスタンスに送信することで、これらのイベントを IBM Intelligent Operations Center にパブリッシュできます。

## トリガー

トリガーは、何らかの処理の発生を検出し、その発生に対応して追加処理を起動できるメカニズムです。

IBM Intelligent Operations Center に付属の KPI サンプルによって、2 つのタイプのトリガーが定義されます。最初のトリガーは、インバウンド・イベントとしても知られる CAP アラート・メッセージが、定義済みの KPI セットに対して IBM WebSphere Business Monitor サーバーによって受信されると起動します。CAP アラート・メッセージによって、KPI が変更される場合と変更されない場合があります。IBM Intelligent Operations Center は、IBM WebSphere Business Monitor サーバーからイベント通知を受信するときに、KPI が変更されるかどうかを決定します。

アウトバウンド・イベントの場合は、トリガーによって、イベントが送信されるタイミングが決定されます。

KPI 計算用の入力値が変更された場合に、イベント・ベースのトリガーを使用して IBM Intelligent Operations Center に通知を送信できます。ただし、定義済みの期間を超過した後に KPI 値が変更された場合に、イベント・トリガーを使用してその状況に対処することはできません。IBM Intelligent Operations Center のサンプルでは、短期間の定義が設定された KPI の場合、時間ベースのトリガーを使用して IBM Intelligent Operations Center に通知が送信されます。

例えば、Severe Traffic Accidents KPI が、1 時間ごとに期限切れになるように定義されているとします。この KPI で 10:00 に値が 3 であり、次の 1 時間以内にその KPI に対して CAP アラート・メッセージが受信されない場合、その時間枠は期限切れになり、KPI 値は 0 (ゼロ) にリセットされます。

## IBM WebSphere Business Monitor へのインバウンド・イベントの定義

IBM Intelligent Operations Center のサンプルでは、インバウンド・イベントを使用して、トリガーが起動される時期が決定されます。KPI コンテキストのインバウンド・イベントは、モニター・コンテキストのインバウンド・イベントと同様の方法で定義します。

## このタスクについて

インバウンド・イベントの定義は、Rational Application Developer または WebSphere Integration Developer を IBM WebSphere Business Monitor 開発ツールキットと共に使用して行います。これらのツールの使用について詳しくは、これらの製品のインフォメーション・センターを参照してください。

インバウンド・イベントを定義するには、以下の手順を実行します。

## 手順

1. インバウンド・イベントの KPI コンテキストを選択します。
2. インバウンド・イベントを作成し、イベント名と ID を指定します。
3. CAP スキーマを指定します。



4. フィルター条件を指定します。
5. KPI コンテキストを選択し、新規インバウンド・イベントを作成します。
6. インバウンド・イベントの新規トリガーを作成します。
7. トリガーのソースが更新されてトリガー条件が満たされるたびにトリガーが起動するよう、トリガーが反復可能であることを確認します。
8. トリガーのソースを選択します。
9. トリガー条件を定義します。トリガー条件が満たされると、トリガーが起動します。

## 例

IBM Intelligent Operations Center のモニター・モデル例は、IBM WebSphere Business Monitor サーバーが CAP アラート・メッセージを受信するたびにトリガーが起動するように定義されています。

### 関連タスク:

125 ページの『KPI のモデル化』

KPI をモデル化するには、IBM WebSphere Business Monitor 開発ツールキットがインストールされている Rational Application Developer または WebSphere Integration Developer を使用します。Rational Application Developer および IBM WebSphere Business Monitor 開発ツールキットは、IBM Intelligent Operations Center の一部として組み込まれています。

### 関連情報:



IBM Business Monitor インフォメーション・センター



Rational Application Developer インフォメーション・センター

## IBM Intelligent Operations Center へのアウトバウンド・イベントの定義

アウトバウンド・イベントは、トリガーの起動時に IBM WebSphere Business Monitor から IBM Intelligent Operations Center に送信される情報を定義します。

### このタスクについて

IBM Intelligent Operations Center は、IBM WebSphere Business Monitor サーバーから送信されるアウトバウンド通知を使用して、KPI に変化があったかどうかを判断します。KPI に変化があった場合、IBM Intelligent Operations Center は、KPI データを IBM WebSphere Business Monitor サーバーから取得し、KPI キャッシュ情報を更新して、IBM Intelligent Operations Center データを更新します。

アウトバウンド・イベントの定義は、Rational Application Developer または WebSphere Integration Developer を IBM WebSphere Business Monitor 開発ツールキットと共に使用して行います。これらのツールの使用について詳しくは、これらの製品のインフォメーション・センターを参照してください。

アウトバウンド・イベントを定義するには、以下のステップを実行します。

### 手順

1. アウトバウンド・イベントの KPI コンテキストを選択します。
2. アウトバウンド・イベントを作成し、イベント名と ID を指定します。
3. 通知スキーマを指定します。スキーマは `ioc-notification-v1.0.xsd` ファイル内にあります。スキーマは `icoc_sample_monitor-models` プロジェクト内にあります。
4. アウトバウンド・イベントのコンテキストを定義します。コンテキストは通知スキーマに基づいていません。



5. **notification** の下にある **sentfrom** の値に「Monitor」と入力します。
6. 以下のサブステップの定義に従って、イベント・コンテキストにパラメーター要素を追加します。
  - a. 最初のパラメーターとして、**parameterName** に modelID と指定し、**parameterValue** にモニター・モデル ID を指定します。例: icoc\_sample\_public\_safety\_monitor\_model。
  - b. KPI セット内の各 KPI について、パラメーターを追加して KPI ID と KPI 値を指定します。KPI ID は **parameterName** 要素を使用して指定し、KPI 値は **parameterValue** 要素を使用して指定します。KPI ID は、KPI セット内の KPI に関連付ける必要があります。KPI 値を文字列として指定するには、`xs:string()` 関数を使用します。例えば、**parameterName** に `Police_Department` と指定し、**parameterValue** に `xs:string(Police_Department)` と指定することができます。

## 例

IBM Intelligent Operations Center に送信される通知の例を以下に示します。

```
<ns1:notification>
  <ns1:notificationType> Alert</ns1:notificationType>
  <ns1:sentFrom> Monitor</ns1:sentFrom>
  <ns1:headline> Police Department KPI Changed</ns1:headline>
  <ns1:description> Police Department KPI Changed</ns1:description>
  <ns1:kpiLink> Police Department</ns1:kpiLink>
  <ns1:category> Safety</ns1:category>
  <ns1:parameter>
    <ns1:parameterName> modelId</ns1:parameterName>
  <ns1:parameterValue>
    icoc_sample_public_safety_monitor_model</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Police_Department</ns1:parameterName>
    <ns1:parameterValue> 0</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time</ns1:parameterName>
    <ns1:parameterValue> 0</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time_Precinct_One</ns1:parameterName>
    <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
  </ns1:parameter>
  <ns1:parameter>
    <ns1:parameterName> Crime_Response_Time_Precinct_Two</ns1:parameterName>
    <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
  </ns1:parameter>
</ns1:notification>
```

## 関連タスク:

125 ページの『KPI のモデル化』

KPI をモデル化するには、IBM WebSphere Business Monitor 開発ツールキットがインストールされている Rational Application Developer または WebSphere Integration Developer を使用します。 Rational Application Developer および IBM WebSphere Business Monitor 開発ツールキットは、IBM Intelligent Operations Center の一部として組み込まれています。

## 関連情報:



IBM Business Monitor インフォメーション・センター



Rational Application Developer インフォメーション・センター

## モニター・モデルのデプロイ

重要業績評価指標 (KPI) とそのモニター・モデルを定義した後、モニター・モデルを IBM Intelligent Operations Center アプリケーション・サーバーで実行されている IBM WebSphere Business Monitor にデプロイする必要があります。

## このタスクについて

IBM WebSphere Business Monitor が使用するモニター・モデルをデプロイするには、定義済みのモデルから Java Enterprise Edition (JEE) プロジェクトを生成する必要があります。 JEE プロジェクトが生成された後、モデル・アプリケーションを EAR ファイルとしてエクスポートできます。 EAR ファイルはその後、IBM Intelligent Operations Center アプリケーション・サーバーで実行されている IBM WebSphere Business Monitor にデプロイできます。

## 手順

1. IBM WebSphere Business Monitor 開発ツールキットがインストールされている Rational Application Developer または WebSphere Integration Developer の「エンタープライズ・エクスプローラー」タブで、プロジェクト生成を必要とするモニター・モデルを右クリックします。 例:  
icoc\_sample\_public\_safety\_monitor\_model。
2. 「**Monitor JEE プロジェクトの生成**」をクリックします。 次のプロジェクトが作成されます:  
modelApplication、modelLogic、および modelModerator。
3. modelApplication プロジェクトを右クリックし、「エクスポート」 > 「EAR」をクリックして、モニター・モデル・アプリケーションをエクスポートします。
4. EAR ファイルを IBM WebSphere Business Monitor にデプロイする前に、KPI をテストします。
5. IBM WebSphere Business Monitor インフォメーション・センターの指示を使用して、EAR ファイルを IBM WebSphere Business Monitor サーバーにデプロイします。

## 関連情報:



IBM Business Monitor インフォメーション・センター



Rational Application Developer インフォメーション・センター

## KPI 表示値

IBM Intelligent Operations Center リソース・バンドルを使用することで、IBM WebSphere Business Monitor モデルによって得られる表示値から、代替の表示値が得られます。

KPI 表示名および範囲名は、IBM Intelligent Operations Center に付属の IBM WebSphere Business Monitor モデルのサンプルで定義されます。 KPI 表示名の例を以下に示します。

- 水
- 水質

範囲名の例を以下に示します。

- 許容可能な状況値
- 注意が必要な状況値
- 対処が必要な状況値

KPI や範囲など、IBM WebSphere Business Monitor で定義された各作成物の ID は、表示名と関連付けられています。 ID にはスペースを含めることができませんが、表示値にはスペースを含めても構いません。 ID は、リソース・バンドル内で値を参照するためのキーとして使用されます。 IBM Intelligent Operations Center は、これらの ID を使用して KPI 表示値を選択します。 ID のリソース・バンドルに値を指定しなかった場合は、IBM WebSphere Business Monitor 定義で指定された値が使用されます。

KPI 表示値は、IBM WebSphere Business Monitor サーバーの ISO 言語および国別コードを使用して、IBM WebSphere Business Monitor によってローカライズされます。例えば、KPI パーセント値は、ロケールが en\_US の場合は 12.61% の形式で表示され、ロケールが fr\_FR の場合は 12,61% の形式で表示されます。リソース・バンドル定義は、これらの値には使用されません。

デフォルトの IBM Intelligent Operations Center プロパティのリソース・バンドルは、com.ibm.iss.icoc.rest.monitor.resources.Messages.properties です。このバンドルは、icoc\_rest\_monitor\_resources\_utils にあります。

リソース・バンドルの例を以下に示します。

```
kpi.NO.VALUE=KPI 値を決定するデータがありません  
kpi.RANGE.UNDETERMINED=決定不能  
Flood_Control=治水  
Water_Levels=水位  
Flow_Discharge_City_River=市内河川の放水  
Water_Level_City_Lake=市内湖沼の水位
```

この例では、IBM WebSphere Business Monitor の KPI が NULL 値を返した場合、kpi.NO.VALUE および kpi.RANGE.UNDETERMINED の値が IBM Intelligent Operations Center によって使用されます。例えば、市内湖沼の水位の KPI は、日次で繰り返される時間帯において、直前の完全な時間帯に基づいて定義されます。該当の KPI の CAP イベントを日曜日に受信せず、その KPI を月曜日に要求された場合は、前日に有効なデータが存在しないため、NULL が返されます。表示値は「KPI 値を決定するデータがありません」に設定され、範囲表示名は「決定不能」に設定されます。

その他の項目である、Flood\_Control、Water\_Levels、Flow\_Discharge\_City\_River、および Water\_Level\_City\_Lake は、IBM Intelligent Operations Center によって提供され icoc sample water monitor model サンプル・モニター・モデル内で定義された、KPI ID の表示値を定義します。これらの項目では、IBM WebSphere Business Monitor モニターで指定された値から代替テキストを指定できます。例えば、モデル自体を変更する代わりに、リソース・バンドルを使用して、変換された値を示すことができます。

## 関連概念:

『サンプル KPI』

IBM Intelligent Operations Center では、サンプル KPI が提供されています。このサンプル KPI は、IBM WebSphere Business Monitor 開発ツールキットを使用してさまざまなタイプの KPI を実装するためのガイドランスを提供するように設計されています。水道、輸送、および公共安全用のサンプル・モニター・モデルが提供されています。

## KPI のキャッシュ

IBM Intelligent Operations Center 構成設定は、KPI 値が IBM WebSphere Business Monitor から取得されるタイミングに影響します。

IBM Intelligent Operations Center では、KPI 値はキャッシュに保持されます。デフォルトでは、KPI は、IBM WebSphere Business Monitor からキャッシュにロードされます。このキャッシュは、システム・プロパティー・テーブルの **KpiCacheRefreshInterval** プロパティーで指定された時間間隔に従ってリフレッシュされます。このリフレッシュ時間は、更新済みの KPI を IBM Intelligent Operations Center に送信する要件に基づき変更できます。システム・プロパティー・テーブル内のプロパティーの変更については、トピックの末尾にあるリンクを参照してください。

「重要業績評価指標」ポートレットで KPI を作成した場合、KPI への更新はキャッシュ・リフレッシュにのみ依存することに注意してください。IBM WebSphere Business Monitor で KPI が定義されている場合、トリガー・メカニズムを定義して、その KPI の変更に応じた追加処理を実装できます。

## 関連概念:

197 ページの『システム全体の構成データの指定』

IBM Intelligent Operations Center システム・プロパティー・テーブルは、IBM Intelligent Operations Center の構成データを保管します。

---

## サンプル KPI

IBM Intelligent Operations Center では、サンプル KPI が提供されています。このサンプル KPI は、IBM WebSphere Business Monitor 開発ツールキットを使用してさまざまなタイプの KPI を実装するためのガイドランスを提供するように設計されています。水道、輸送、および公共安全用のサンプル・モニター・モデルが提供されています。

最も低いレベルの KPI は集約 KPI として定義されます。集約 KPI は、平均、最大、最小、合計、出現回数、または標準偏差などの集約関数と、着信 CAP アラート・メッセージに含まれている値から計算されます。これらの値は、定量化可能な測定値として表現されます。低いレベルの KPI 値は、IBM WebSphere Business Monitor サーバーのロケールに基づいて適切なフォーマットにローカライズされます。より高いレベルの KPI は、サンプル KPI の作成時に定義されたマッピングに基づいて値にマップされます。

より高いレベルのサンプル KPI の値は、色および推奨応答レベルに相当する数字です。値 0 は許容可能、値 1 は注意、値 2 は対処です。最も低いレベルの KPI の値は、その値が表す KPI に応じて、期間、10 進数、パーセント、または通貨になります。例えば、以下のようなものがあります。

- 15% は、一定の期間の特定の空港で遅延が生じたフライトのパーセントを表す KPI の実際の値です。
- 5 分 7 秒は、一定の期間の所定の場所における平均犯罪応答時間を表す KPI の実際の値です。

サンプル IBM Intelligent Operations Center モニター・モデルのソース・ファイルは、IBM WebSphere Business Monitor ツールキットがインストールされている Rational Application Developer または

WebSphere Integration Developer にインポートできるアーカイブ・ファイルで提供されます。このアーカイブ・ファイルを変更して、KPI 定義を変更、追加、または削除することができます。その後、定義を再生成して、IBM Intelligent Operations Center に再デプロイできます。

IBM Intelligent Operations Center に付属のサンプル・モデルは以下のとおりです。

- icoc\_sample\_public\_safety\_monitor\_model
- icoc\_sample\_transportation\_monitor\_model
- icoc\_sample\_water\_monitor\_model

これらのモデルには、以下の KPI サンプルが含まれています。

- 水
  - 治水
    - 水位
      - 市内河川の放水
      - 市内湖沼の水位
  - 水管理
    - 戦略的計画
      - 漏水
      - 水の供給と需要
  - 水質
    - 物理的標識
      - 濁度
      - pH
- 輸送
  - 空港
    - フライト遅延
      - 空港 1 でフライト遅延
      - 空港 2 でフライト遅延
  - 道路と交通
    - 道路イベント
      - 重大な交通事故
  - 輸送管理
    - 収益
      - 橋とトンネルの通行料
      - 駐車施設の収益
- 公共安全
  - 消防署
    - 消防士の負傷
      - 消防署 1 の消防士負傷
      - 消防署 2 の消防士負傷
  - 警察署

- 犯罪の応答時間
  - 警察管区 1 の犯罪応答時間
  - 警察管区 2 の犯罪応答時間
- 公共安全管理
  - 公共安全の予算
    - EMS 部門の予算
    - 消防署の予算
    - 警察署の予算

#### 関連概念:

321 ページの『状況』

「状況」ポートレットでは、単独または複数の組織の重要業績評価指標 (KPI) の状況を確認することができます。

304 ページの『重要業績評価指標のドリルダウン』

KPI カテゴリと、そのカテゴリの基礎となる KPI の状況に関する追加の情報を表示するには、「重要業績評価指標のドリルダウン」ポートレットを使用します。

123 ページの『KPI の作成および統合』

重要業績評価指標 (KPI) モデルは、ビジネス・モニター開発ツールキットおよび KPI 管理ポートレットを使用して作成および変更することができます。

185 ページの『KPI のカスタマイズ』

IBM Intelligent Operations Center では、ビジネス・プロセスに適合するよう重要業績評価指標 (KPI) モデルをカスタマイズできます。

#### 関連タスク:

134 ページの『モニター・モデルのデプロイ』

重要業績評価指標 (KPI) とそのモニター・モデルを定義した後、モニター・モデルを IBM Intelligent Operations Center アプリケーション・サーバーで実行されている IBM WebSphere Business Monitor にデプロイする必要があります。

121 ページの『サンプル・イベント・テーブルでのサンプル・イベントと KPI イベントの表示』

「イベント・スクリプト記述」ポートレットは、IBM Intelligent Operations Center データベースのサンプル・イベント・テーブルから、サンプル・イベントをパブリッシュします。以下の手順に従って、サンプル・イベント・テーブルでイベントを表示します。

---

## Tivoli Service Request Managerの構成

Tivoli Service Request Manager ユーザー・インターフェースでは、標準操作手順、ワークフロー、およびリソースを管理できます。

標準操作手順、ワークフロー、およびリソースの名前に共通接頭部を追加する場合は、検索でデータをフィルタリングするほうが簡単です。例えば、顧客プロジェクトの場合は、共通接頭部 CX を使用します。

**TSRMServerSecurityEnabled** プロパティを設定して、Tivoli Service Request Manager への接続に SSL が使用されるかどうかを指定できます。このプロパティと他の Tivoli Service Request Manager プロパティについて詳しくは、このトピックの末尾にあるリンクを参照してください。



## 関連概念:

229 ページの『イベント・サーバー』

197 ページの『システム全体の構成データの指定』

IBM Intelligent Operations Center システム・プロパティ・テーブルは、IBM Intelligent Operations Center の構成データを保管します。

## Tivoli Service Request Manager ユーザー・インターフェースの使用

Tivoli Service Request Manager ユーザー・インターフェースにアクセスする方法を習得します。 Tivoli Service Request Manager Start Centerをカスタマイズして頻繁に使用する機能へのリンクを組み込むことで、より簡単に素早く使用できるようにします。

## Tivoli Service Request Manager アプリケーションの開始

Tivoli Service Request Manager アプリケーションを、WebSphere Portal Administration インターフェースを介して開くには、「ソリューション管理ツール」か、または「標準操作手順」ポートレットを使用します。 IBM Intelligent Operations Center インターフェースを介して Tivoli Service Request Manager 内でリソースを表示することもできます。

### 始める前に

IBM Intelligent Operations Center インターフェースを介して Tivoli Service Request Manager 内でリソースを表示できるようにするには、シングル・サインオンを構成する必要があります。

### 手順

- WebSphere Portal Administration インターフェースを介して Tivoli Service Request Manager Start Center を開くには、以下のサブステップを実行します。
  1. 「**Intelligent Operations**」 > 「**管理ツール**」 > 「**管理コンソール**」をクリックします。
  2. 「**標準操作手順の管理**」をクリックします。
  3. Tivoli Service Request Manager Start Centerに管理者としてログオンします。
- 標準操作手順に関連した Tivoli Service Request Manager アプリケーションを開くには、以下のよう  
「標準操作手順」ポートレットを使用します。
  1. 「標準操作手順」ポートレットを開くには、WebSphere Portal Administration インターフェースで「**Intelligent Operations**」 > 「**カスタマイズ・ツール**」 > 「**標準操作手順**」をクリックします。
  2. 次のオプションのいずれかを選択してください。
    - 標準操作手順アプリケーションを開くには、「**標準操作手順**」をクリックします。
    - 標準操作手順の選択マトリックスのアプリケーションを開くには、「**標準操作手順の選択マトリックス**」をクリックします。
    - ワークフロー・デザイナー・アプリケーションを開くには、「**ワークフロー・デザイナー**」をクリックします。
- IBM Intelligent Operations Center インターフェースを介して Tivoli Service Request Manager ユーザー・インターフェースでリソースを表示するには、以下の手順を実行します。
  1. 「**詳細**」ポートレットの「**イベントとインシデント**」タブで、イベント・リストの行を右クリックします。
  2. イベントの周辺にあるリソースのリストを表示するには、「**近隣リソースの表示**」をクリックして、絞り込む領域の半径を選択します。 リソースのリストが「**リソース**」タブに表示されます。

3. 「リソース」タブで、リソース・リストの行を右クリックして、「プロパティ」をクリックします。リソースは、Tivoli Service Request Manager の「リソース」タブに表示されます。

注: Tivoli Service Request Manager から完全にサインアウトするには、Tivoli Service Request Manager ユーザー・インターフェースの Web ブラウザー・ウィンドウを閉じる必要があります。

#### 関連タスク:

60 ページの『コラボレーション・サービス用のシングル・サインオンの構成』

WebSphere Portal SSO LTPA トークンをイベント・サーバーにインポートすると、ユーザーは資格情報を再入力しなくてもコラボレーション・サービスにアクセスできるようになります。

## Tivoli Service Request Manager Start Centerでのお気に入りのアプリケーションの設定

お気に入りのアプリケーションにより簡単にアクセスできるよう、Tivoli Service Request Manager Start Centerでお気に入りのアプリケーションを更新します。

### このタスクについて

Tivoli Service Request Manager の各ユーザーには、ユーザー固有の Tivoli Service Request Manager Start Centerがあり、「お気に入りのアプリケーション」の下にユーザー固有のカスタマイズ・リストがあります。

### 手順

1. Tivoli Service Request Manager Start Centerを表示するには、Tivoli Service Request Manager ユーザー・インターフェースの上部で、「スタート・センター」をクリックします。
2. Tivoli Service Request Manager Start Centerで、「お気に入りのアプリケーション」の横にある「ポートレットの編集」アイコンをクリックします。
3. 「お気に入りのアプリケーションの設定」ウィンドウで、「アプリケーションの選択」をクリックします。
4. 「アプリケーションの選択」ウィンドウで、「お気に入りのアプリケーション」の下に表示するアプリケーションを選択します。以下のリストには、IBM Intelligent Operations Center ユーザーに役立つアプリケーションを示します。

#### CRONTASK

クローン・タスクのセットアップ

#### DOMAINADM

ドメイン

#### PERSON

担当者

#### PERSONGR

担当者グループ

#### PLUSIMTRIX

SOP 選択マトリックス

#### PLUSIRES

リソース

#### PLUSIWO

SOP アクティビティ

**USER** ユーザー

**WFDESIGN**

ワークフロー・デザイナー

5. 「お気に入りのアプリケーション」の下でのアプリケーションの表示位置を規定するには、以下の手順を実行します。
  - a. 「お気に入りのアプリケーションの設定」ウィンドウで、アプリケーションを選択します。
  - b. 「順序」フィールドに数値を入力します。
6. 更新情報を保存するには、「終了」をクリックします。

## Tivoli Service Request Manager での新規ユーザーの構成

IBM Intelligent Operations Center でユーザーを追加したら、Tivoli Service Request Manager で、そのユーザーに権限および担当者グループを割り当てます。

### デフォルトの挿入サイトの設定

新規ユーザーが新規リソースを追加し、標準操作手順を適用できるようにするには、ユーザーのデフォルトの挿入サイトを設定する必要があります。

#### 手順

1. Tivoli Service Request Manager Start Centerに管理者としてログオンします。
2. 「移動」 > 「セキュリティ」 > 「ユーザー」をクリックします。
3. ユーザーを検索するには、「リスト」タブの「ユーザー」フィールドに、ユーザー名の一部またはユーザー名全体を入力します。
4. リストでユーザー名をクリックし、「ユーザー」タブをクリックします。
5. 「ユーザー設定」で、「デフォルトの挿入サイト」フィールドの横にある「値の選択」アイコンをクリックします。
6. 「値の選択」ウィンドウで、デフォルトの挿入サイトの名前を探してクリックします (例: 「PMSCRTP」)。PMSCRTP は、IBM Intelligent Operations Center と共にインストールされるサンプル・サイトです。
7. 「ユーザーの保存」アイコンをクリックします。

### セキュリティ・グループへのユーザーの割り当て

該当するセキュリティ・グループにユーザーを追加することで、Tivoli Service Request Manager でユーザーが該当するアプリケーションにアクセスできるようにします。

#### このタスクについて

ユーザーをグループに追加するには、以下の手順を実行します。

#### 手順

1. Tivoli Service Request Manager Start Centerに管理者としてログオンします。
2. 「移動」 > 「セキュリティ」 > 「ユーザー」をクリックします。
3. ユーザーを検索するには、「リスト」タブの「ユーザー」フィールドに、ユーザー名の一部またはユーザー名全体を入力します。
4. リスト内でユーザーの名前をクリックし、「グループ」タブをクリックします。

5. ユーザーの追加先となるグループを検索するには、「グループ」フィールドにグループの名前の一部またはすべての文字を入力します。
6. 必要なグループの名前がリストされていない場合は、「新規行」をクリックします。
7. 「グループ」フィールドの横にある「詳細」の下で、「詳細」メニュー・アイコンをクリックしてから、「値の選択」をクリックします。
8. 「値の選択」ウィンドウで、必要なグループの名前を検索してクリックします。
9. 「ユーザーの保存」アイコンをクリックします。

## 担当者グループへのユーザーの割り当て

標準操作手順では、事前に定義された担当者グループにタスクを割り当てることができます。特定の担当者グループに割り当てられたタスクを表示するには、ユーザーはその担当者グループのメンバーである必要があります。

## 始める前に

IBM Intelligent Operations Center のインストール時に提供されるサンプルの担当者グループを使用するか、独自の担当者グループを作成することができます。Tivoli Service Request Manager で担当者グループを作成する方法については、Maximo® Asset Management インフォメーション・センターを参照してください。

**注:** すべての担当者グループの名前が同じ長さになるようにしてください。これにより、ユーザーがメンバーである担当者グループに割り振られているタスクのみが、それらのユーザーに割り当てられるようになります。

## このタスクについて

ユーザーを担当者グループに割り当てするには、以下の手順を実行します。

## 手順

1. Tivoli Service Request Manager Start Centerに管理者としてログオンします。
2. 「移動」 > 「管理」 > 「リソース」 > 「担当者グループ」をクリックします。
3. 必要な担当者グループを検索するには、「一覧」タブの「担当者グループ」フィールドに担当者グループの名前の一部またはすべての文字を入力します。
4. リスト内で、担当者グループの名前をクリックします。
5. 「担当者」の下にある「担当者グループ」タブで、「新規行」をクリックします。
6. 「担当者」フィールドの横にある「詳細」の下で、「詳細」メニュー・アイコンをクリックしてから、「値の選択」をクリックします。
7. 「値の選択」ウィンドウで、担当者グループに追加するユーザーの名前を検索してクリックします。
8. 「順序」フィールドに、使用可能な次の増分番号を入力します。
9. 「担当者グループの保存」アイコンをクリックします。

## 関連情報:

 Maximo Asset Management インフォメーション・センター

## 標準操作手順

標準操作手順およびアクティビティーを定義することで、IBM Intelligent Operations Center で受信するイベントを管理できます。「標準操作手順」ポートレットを使用して、Tivoli Service Request Manager で、標準操作手順、標準操作手順の選択マトリックス、およびワークフロー・デザイナーの各アプリケーションにアクセスします。

「標準操作手順」ポートレットを起動するには、WebSphere Portal 管理インターフェースで「**Intelligent Operations**」 > 「**カスタマイズ・ツール**」 > 「**標準操作手順**」をクリックします。

標準操作手順とは、パラメーターが特定の事前定義の条件を満たすイベントが発生するとトリガーされる一連のアクティビティーを定義するものです。それぞれのアクティビティーは手動タスクと自動タスクのいずれかに対応しています。自動タスクにはワークフローを割り当てることができます。それぞれのアクティビティーは所有者グループに割り当てられ、ユーザーは担当者グループのメンバーシップによって所有者グループに割り当てられます。所有者グループに割り当てられているすべてのユーザーは、「マイ・アクティビティー」ポートレットを使用してアクティビティーを管理することができます。

標準操作手順のアクティビティーの一部または全部について、実行する順序を指定することができます。例えば、直前のアクティビティーが完了するか、またはスキップされない限り、特定のアクティビティーが開始されないように指定することができます。

標準操作手順アプリケーションを開始するには、「標準操作手順」ポートレットで、「標準操作手順」をクリックします。

## 標準操作手順の選択マトリックス

標準操作手順の選択マトリックスで、特定のイベントのために標準操作手順が開始されるかどうかを決定するイベント・パラメーターを定義します。それぞれの標準操作手順には、1 つ以上の選択基準のセットを使用できます。ただし、選択基準の各セットは固有でなければなりません。

標準操作手順の選択マトリックスアプリケーションを開始するには、「標準操作手順」ポートレットで、「標準操作手順の選択マトリックス」をクリックします。

## ワークフロー・デザイナー

ワークフロー・デザイナーを使用して、標準操作手順のアクティビティーに自動化タスクとして割り当てることができるワークフローを設計できます。

ワークフロー・デザイナーアプリケーションを開始するには、「標準操作手順」ポートレットで、「ワークフロー・デザイナー」をクリックします。

## 「標準操作手順」ポートレットのカスタマイズ

このポートレットはカスタマイズすることができます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

## 関連概念:

314 ページの『マイ・アクティビティー』

「マイ・アクティビティー」ポートレットには、インターフェースにログオンしているユーザーがメンバーとして所属するグループが所有するアクティビティーの動的なリストが表示されます。

## 関連資料:

181 ページの『「標準操作手順」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「標準操作手順」ポートレットをカスタマイズできます。

## ワークフローの作成

Tivoli Service Request Manager では、標準操作手順アクティビティーに自動タスクとして含めることができるワークフローを作成できます。

## このタスクについて

ワークフローを作成する方法については、トピックの末尾にある Maximo Asset Management インフォメーション・センターへのリンクを参照してください。

## 手順

1. 「標準操作手順」ポートレットを開くには、WebSphere Portal Administration インターフェースで「**Intelligent Operations**」 > 「**カスタマイズ・ツール**」 > 「**標準操作手順**」をクリックします。
2. ワークフロー・デザイナー・アプリケーションを開くには、「**ワークフロー・デザイナー**」をクリックします。
3. 「ワークフロー・デザイナー」ウィンドウで、「**キャンバス**」タブをクリックします。
4. 「**キャンバス**」タブで、該当するアイコンをクリックして、ワークフローに必要なノードと矢印を挿入します。

## 関連情報:



Maximo Asset Management インフォメーション・センター

## 標準操作手順の作成

標準操作手順を作成し、所有者グループに割り当てます。ユーザーは、担当者グループのメンバーシップによって所有者グループに割り当てられます。

## 手順

1. 「標準操作手順」ポートレットを開くには、WebSphere Portal Administration インターフェースで「**Intelligent Operations**」 > 「**カスタマイズ・ツール**」 > 「**標準操作手順**」をクリックします。
2. 標準操作手順アプリケーションを開くには、「**標準操作手順**」をクリックします。
3. 「標準操作手順」ウィンドウの「**リスト**」タブで、「**新規 SOP**」アイコンをクリックします。ブランクの標準操作手順が「**標準操作手順**」タブに表示されます。
4. 「**SOP 名**」に名前を入力し、「**SOP 名**」の隣のフィールドに説明を入力します。標準操作手順の名前には、サンプルの標準操作手順の名前（悪天候からの避難の準備（準備）など）のような、一貫性のある形式を使用してください。また、名前の最後の文字が右括弧の場合は、双方向テキストのレンダリングに関連した問題が発生する可能性を防ぐために、記述方向制御（左から右）マーク（LRM）文字を追加してください。例えば、前の例で使用した名前の場合、悪天候からの避難の準備（準備）&#x200E;と入力します。標準操作手順を保存した後は、LRM 文字はユーザー・インターフェー



スに表示されません。また、ご使用のすべての標準操作手順の名前に共通接頭部を追加する場合は、検索内でご使用の標準操作手順をフィルタリングするほうが簡単です。例えば、顧客プロジェクトの場合は、共通接頭部 **CX** を使用します。

5. より長い説明を入力するには、説明フィールドの隣のアイコンをクリックして、表示されるウィンドウに説明を入力します。
6. 「詳細」の下で、「**テンプレート型**」リストから、「**アクティビティ**」を選択します。
7. 「詳細」の下で、標準操作手順に所有者グループを割り当てます。
  - a. 「**所有者グループ**」フィールドの隣のアイコンをクリックします。
  - b. 「**値の選択**」ウィンドウで、リスト内の値をクリックして選択します。
8. オプション: 「**所要時間**」に、標準操作手順を完了する必要がある制限時間を入力します。制限時間の形式は *hh:mm* です。ここで *hh* は時間数、*mm* は分数です。期限は所要時間に基づいて計算されません。
9. 必要に応じて、標準操作手順にタスクを追加します。
  - a. Tivoli Service Request Manager ユーザー・インターフェースの右下近くにある「**新規行**」をクリックします。「**SOP のステップ (SOP Steps)**」で、タスク順序のリストに新規タスク行が追加されません。
  - b. 「**シーケンス**」および「**タスク**」に、同じ番号を入力します。タスクに番号を付けるときには、10、20、30 などのパターンを使用します。このパターンを使用すると、後でタスクを追加および削除する場合の柔軟性が高くなります。
  - c. 「**説明**」にタスクの説明を入力します。以前に入力した説明を選択するには、説明フィールドの隣のアイコンをクリックします。
  - d. オプション: ワークフローを割り当てるには、以下のようにします。
    - 1) 「**ワークフロー名**」については、「**値の選択**」アイコンをクリックします。
    - 2) 「**値の選択**」ウィンドウで、リスト内の値をクリックして選択します。リストを絞り込むには、リストの先頭に表示されているフィルター・フィールドに、使用するワークフロー名の最初の数文字を入力します。
    - 3) タスク行を展開し、「**詳細**」の下で、必要に応じて追加の詳細を入力します。必要な場合、所有者グループとフロー制御設定を指定できます。タスクの所有者グループとフロー制御設定を指定しなかった場合、タスクは、これらの設定を親の標準操作手順から継承します。
10. 標準操作手順を保存するには、Tivoli Service Request Manager ユーザー・インターフェースの上部付近にある「**SOP の保存**」アイコンをクリックします。
11. 標準操作手順を標準操作手順の選択マトリックスで指定したイベントに適用する場合は、必ずステータスを **DRAFT** から **ACTIVE** に変更してください。
  - a. 「**ステータスの変更**」アイコンをクリックします。
  - b. 「ステータスの変更」ウィンドウの「**新規ステータス**」リストから、「**アクティブ**」を選択します。
  - c. オプション: 「**変更日**」および「**メモ**」の値を入力します。
  - d. 「**OK**」をクリックします。
12. 使用可能な標準操作手順を確認するには、以下のステップを実行します。
  - a. 「**リスト**」タブをクリックします。
  - b. 「**SOP の作業標準 (SOP Job Plans)**」で、以下のいずれかのオプションを選択します。
    - フィルター・フィールドで **Enter** キーを押して、使用可能なすべての標準操作手順を表示します。

- フィルター・フィールドに、標準操作手順の名前の最初の数文字を入力します。
- c. 標準操作手順の詳細を表示するには、リスト内の標準操作手順の名前をクリックします。「標準操作手順」タブに詳細が表示されます。

## 次のタスク

標準操作手順のアクティビティーの一部または全部について、実行する順序を指定できるようにするには、「詳細」にある「フロー制御を行う (Flow Controlled?)」チェック・ボックスを選択します。ユーザーまたはグループに割り当てるアクティビティーを標準操作手順に基づいて順序付ける方法については、Maximo Asset Management インフォメーション・センターを参照し、フロー制御 について検索し確認してください。


標準操作手順の選択マトリックスで、標準操作手順を選択するイベントを決定するイベント・パラメーターを定義します。

### 関連タスク:

142 ページの『担当者グループへのユーザーの割り当て』

標準操作手順では、事前に定義された担当者グループにタスクを割り当てることができます。特定の担当者グループに割り当てられたタスクを表示するには、ユーザーはその担当者グループのメンバーである必要があります。

### 関連情報:

 Maximo Asset Management インフォメーション・センター

## 標準操作手順の選択マトリックスの項目の確認

標準操作手順の選択マトリックスで、それぞれの標準操作手順の選択基準を確認します。選択基準はイベント・パラメーターに基づきます。

### 手順

1. 「標準操作手順」ポートレットを開くには、WebSphere Portal Administration インターフェースで「Intelligent Operations」 > 「カスタマイズ・ツール」 > 「標準操作手順」をクリックします。
2. 標準操作手順の選択マトリックスのアプリケーションを開くには、「標準操作手順の選択マトリックス」をクリックします。
3. 「標準操作手順の選択マトリックス」ウィンドウでフィルター行を表示するには、「フィルター」アイコンをクリックします。
4. 次のうちから使用するフィルター・フィールドを決定します。
  - カテゴリー
  - 重大度
  - 緊急度
  - 確信度
  - SOP 名
5. 次のオプションのいずれかを選択してください。
  - フィルター・フィールドで Enter キーを押して、選択したパラメーターまたは標準操作手順名に関連する既存の項目をすべて表示します。
  - フィルター・フィールドに、フィルタリングの基準とする値の最初の数文字を入力します。
  - パラメーター値でフィルタリングする場合は、「値の選択」ウィンドウを使用して値を入力します。

- a. フィルター・フィールドの横にある「**値の選択**」アイコンをクリックします。
- b. 「値の選択」ウィンドウで、リスト内の値をクリックして選択します。
- 「標準操作手順」ウィンドウを使用して、フィルタリングの基準とする標準操作手順の名前を選択するには、以下のようになります。
  - a. 「**SOP 名**」フィルター・フィールドの横にある「**詳細**」メニュー・アイコンをクリックし、「**標準操作手順へ移動**」をクリックします。
  - b. 「標準操作手順」ウィンドウで、「**リスト**」タブをクリックします。
  - c. 「SOP の作業標準 (SOP Job Plans)」で、フィルター・フィールドに標準操作手順の名前の最初の数文字を入力します。
  - d. 標準操作手順の詳細を表示するには、リスト内の標準操作手順の名前をクリックします。「**標準操作手順**」タブに詳細が表示されます。
  - e. 「**標準操作手順**」タブで表示される標準操作手順の名前を返すには、右上の隅にある「**値を入力して戻る**」をクリックします。名前が選択マトリックスの「**SOP 名**」フィルター・フィールドに表示されます。
6. 表示された選択基準項目のリストをさらに絞り込むには、ステップ 4 でリストされているその他のフィルター・フィールドのいずれかを使用して、ステップ 5 を繰り返します。

## 標準操作手順の選択マトリックスでのパラメーターの定義

標準操作手順の選択マトリックスで、特定のイベントについて標準操作手順を選択するかどうかを決定するイベント・パラメーターを定義します。

### このタスクについて

同一の選択基準が 2 行ある標準操作手順の選択マトリックスを保存することはできません。該当する場合、標準操作手順の選択基準には一意のセットを定義する必要があることを通知する検証メッセージが表示されます。

### 手順

1. 「標準操作手順」ポートレットを開くには、WebSphere Portal Administration インターフェースで「**Intelligent Operations**」 > 「**カスタマイズ・ツール**」 > 「**標準操作手順**」をクリックします。
2. 標準操作手順の選択マトリックスのアプリケーションを開くには、「**標準操作手順の選択マトリックス**」をクリックします。
3. 「標準操作手順の選択マトリックス」ウィンドウでフィルター行を表示するには、「**フィルター**」アイコンをクリックします。
4. 「**SOP 選択マトリックス**」ウィンドウの、右下の隅にある「**新規行**」をクリックします。選択マトリックスに新規行が追加されます。
5. 以下の各パラメーターに値を入力します。
  - カテゴリー
  - 重大度
  - 緊急度
  - 確信度

以下のいずれかのオプションを使用して、各パラメーターに値を入力します。

- 「値の選択」ウィンドウを使用して値を入力するには、以下のようになります。
  - a. パラメーター・フィールドの横にある「**値の選択**」アイコンをクリックします。

- b. 「値の選択」ウィンドウで、リスト内の値をクリックして選択します。
- パラメーターの名前を手動で入力するには、以下のようにします。
  - a. パラメーターの値の最初の数文字をフィールドに入力します。
  - b. TAB キーを押してカーソルを次のフィールドに移動すると、パラメーターの値が自動的に入力されます。
- 6. 標準操作手順の名前を「SOP 名」フィールドに入力するには、以下のいずれかのオプションを選択します。
  - 「標準操作手順」ウィンドウを使用して標準操作手順の名前を入力するには、以下のようにします。
    - a. 「SOP 名」フィールドの横にある「詳細」メニュー・アイコンをクリックし、「標準操作手順へ移動」をクリックします。
    - b. 「標準操作手順」ウィンドウで、「リスト」タブをクリックします。
    - c. 「SOP の作業標準 (SOP Job Plans)」で、フィルター・フィールドに標準操作手順の名前の最初の数文字を入力します。
    - d. 標準操作手順の詳細を表示するには、リスト内の標準操作手順の名前をクリックします。「標準操作手順」タブに詳細が表示されます。
    - e. 「標準操作手順」タブで表示される標準操作手順の名前を返すには、右上の隅にある「値を入力して戻る」をクリックします。名前が選択マトリックスにある新規行の「SOP 名」フィールドに表示されます。
  - 標準操作手順の名前を手動で入力します。
- 7. 「マトリックスを保存」アイコンをクリックします。

## リソースの管理

リソースは、Tivoli Service Request Manager で管理します。

### サンプル・リソースとIBM Intelligent Operations Center データベースとの同期化

IBM Intelligent Operations Center と共にインストールされたサンプル・リソースを使用する場合は、サンプル・リソースを手動で IBM Intelligent Operations Center データベースと同期化する必要があります。

#### 手順

1. Tivoli Service Request Manager Start Centerに管理者としてログオンします。
2. 「移動」 > 「資産」 > 「IOC リソース (IOC Resources)(IntOpCtr)」をクリックします。
3. IBM Intelligent Operations Center のすべてのサンプル・リソースを表示するには、「リソース (IntOpCtr) (Resources (IntOpCtr))」ウィンドウの「リスト」タブで、「リソース」フィールドをクリックして、Enter キーを押します。
4. IBM Intelligent Operations Center データベースと同期化するリソースごとに、リソースを更新します。例えば、「説明」の内容を変更して、変更内容を保存します。
5. 同期化されたリソースが、以下の IBM Intelligent Operations Center データベース表にリストされていることを確認します。
  - IOC.RESOURCE
  - IOC.RESOURCE\_X\_CAPABILITY

## 次のタスク

サンプル・リソースが IBM Intelligent Operations Center データベースと正しく同期しない場合は、Tivoli Netcool/Impact プローブのログ・ファイルを調べてください。以下のコマンドを入力します。

```
tail -f /opt/IBM/netcool/omnibus/log/ioc_xml1.log
```

また、/opt/IBM/netcool/impact/log/NCI\_policylogger.log の Tivoli Netcool/Impact ポリシー・ログ・ファイルも確認してください。Tivoli Netcool/Impact ポリシー・ログ・ファイルを使用可能にするには、以下の手順を実行します。

1. `http://event_server:9080/nci` で Tivoli Netcool/Impact 管理コンソールにログオンします。ユーザー `admin` とパスワード `netcool` を使用してログオンします。
2. 「**IOC プロジェクト (IOC Project)**」をクリックします。
3. 「**サービス**」タブで、「**ポリシー・ロガー**」をクリックします。
4. 「**最上位のログ・レベル**」の値を 0 から 3 に変更します。
5. 変更を保存します。
6. テストを実行します。

トラブルシューティング・ログ・ファイルについて詳しくは、このトピックの末尾にあるリンクを参照してください。

### 関連概念:

326 ページの『イベント・サーバーのログ・ファイル』

イベント・サーバーの一部のシステムについてトレースを使用可能にしてログを表示するには、以下の手順を実行します。

## イベント・カテゴリから機能へのマッピングの作成または変更

リソースは、選択したイベントのカテゴリ、およびマップされたリソース機能に応じて、「マップ」ポートレットに表示されます。リソースを作成する前に、リソースの機能を適切なイベント・カテゴリにマップします。

### 始める前に

確実にリソース機能が更新されるようにするには、Tivoli Service Request Manager 管理ユーザー (例えば `maxadmin`) のパスワードの値を `maxadmin` に設定する必要があります。

### このタスクについて

リソース機能をイベント・カテゴリにマップすることで、IBM Intelligent Operations Center の「詳細」ポートレットで近隣リソースを表示したときに、適切なリソースが「マップ」ポートレットに表示されるようになります。例えば、イベントの気象学カテゴリの近隣リソースを表示する場合、土嚢を保管する倉庫が表示されます。ここで、倉庫はリソース・タイプ、土嚢は倉庫のマップされた機能です。

### 手順

1. Tivoli Service Request Manager Start Centerに管理者としてログオンします。
2. 「**移動**」 > 「**システム構成**」 > 「**プラットフォームの構成**」 > 「**ドメイン**」をクリックします。
3. 以下から該当するオプションを選択します。
  - イベント・カテゴリから機能へのマッピングを作成する場合は、「**新規行**」をクリックし、該当する詳細情報をフィールドに入力します。



- イベント・カテゴリから機能への既存のマッピングを変更する場合は、フィルター・フィールドを使用して該当するイベント・カテゴリのマッピングを表示してから、編集する行をクリックし、詳細情報を変更します。
  - イベント・カテゴリから機能への既存のマッピングを削除する場合は、フィルター・フィールドを使用して該当するイベント・カテゴリのマッピングを表示してから、削除する行の末尾にある「**行を削除対象にマーク**」アイコンをクリックします。
4. 「**ドメインの保存**」アイコンをクリックします。
  5. マップされたリソースが、以下の IBM Intelligent Operations Center データベース表にリストされていることを確認します。
    - IOC.RESOURCE
    - IOC.RESOURCE\_X\_CAPABILITY

## タスクの結果

現在選択されているイベントのイベント・カテゴリに機能がマップされている新規リソースが、IBM Intelligent Operations Center の「マップ」ポートレットにただちに表示されます。現在選択されているイベントのイベント・カテゴリに機能がマップされている、更新されたリソースは、IBM Intelligent Operations Center の「マップ」ポートレットが含まれるページが再ロードされた後にのみ表示されます。

## 次のタスク

- マップされたリソースが IBM Intelligent Operations Center データベースで正しくリストされていない場合は、Tivoli Netcool/Impact ログ・ファイルを調べてください。以下のコマンドを入力します。

```
tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

トラブルシューティング・ログ・ファイルについては、このトピックの末尾にあるリンクを参照してください。

- 3 個以上のイベント・カテゴリを 1 つの機能にマップする場合は、DB2 コマンドを使用してマッピングを行います。以下のステップを実行します。

1. データ・サーバーに Tivoli Service Request Manager データベース・ユーザーとしてログオンするには、コマンド `su - db2inst6` を入力します。
2. IBM Intelligent Operations Center データベースに接続するには、コマンド `db2 connect to maximo` を入力します。
3. イベント・カテゴリを機能にマップするには、以下のコマンドを入力します。

```
insert into synonymdomain
(domainid, maxvalue, value, description, defaults, synonymdomainid, valueid) values
('PLUSICATCPLMAP', 'category_name', 'capability_name',
'mapping_description', 0, NEXTVAL FOR synonymdomainseq,
'PLUSICATCPLMAP|mapping_key');
```

上記のコマンドで、変数 `category_name`、`capability_name`、`mapping_description`、および `mapping_key` を適切な値に置き換えます。 `mapping_key` では、適切な値を作成します。例えば、以下のコマンドは、イベント・カテゴリ `Met` を機能 `COT` にマップし、値 `METCOT` を `mapping_key` に割り当てます。

```
insert into synonymdomain
(domainid, maxvalue, value, description, defaults, synonymdomainid, valueid) values
('PLUSICATCPLMAP', 'Met', 'COT', 'Has cots', 0, NEXTVAL FOR synonymdomainseq,
'PLUSICATCPLMAP|METCOT');
```

4. データベースへの書き込みを完了するには、コマンド `db2 commit;` を入力します。



## リソースの作成

Tivoli Service Request Manager ユーザー・インターフェースでリソースを作成します。

### 始める前に

新規リソースの機能がカテゴリーにマップされ、それによりリソースが IBM Intelligent Operations Center ユーザー・インターフェースの「マップ」ポートレットに表示されていることを確認してください。

### 手順

1. Tivoli Service Request Manager Start Centerに管理者としてログオンします。
2. 「移動」 > 「資産」 > 「リソース (IntOpCtr) (Resources (IntOpCtr))」をクリックします。
3. 「IOC リソース (IOC Resources)」ウィンドウで、「新規リソース」アイコンをクリックします。
4. 「リソース」タブで、以下の詳細情報を入力します。

#### リソース

リソースの一意の ID。

#### 詳細説明

IBM Intelligent Operations Center ユーザー・インターフェースの「詳細」ポートレットの「リソース」タブに表示されるリソースの名前。

#### 簡略説明

IBM Intelligent Operations Center ユーザー・インターフェースの「マップ」ポートレットでリソースにマウス・ポインターを移動したときに、ホバー・ヘルプとして表示されるリソースの簡略説明。

**緯度** リソースの場所を緯度で表した位置。

**経度** リソースの場所を経度で表した位置。

5. 「機能」タブをクリックします。
6. 「分類」フィールドの横にある「詳細」メニュー・アイコンをクリックして、「分類」をクリックします。
7. 「分類 (Classify)」ウィンドウで、ナビゲーション・ツリーを参照して、適切なリソースの分類を特定します。
8. 分類名 (「倉庫」など) をクリックします。 分類に関連付けられた機能の表が、「IOC リソース (IOC Resources)」ウィンドウに表示されます。
9. 「機能」表で、該当する機能をクリックし、「数値」に入力します。
10. 「リソースの保存」アイコンをクリックします。

### 次のタスク

リソースが以下の IBM Intelligent Operations Center データベース表にリストされていることを確認します。

- IOC.RESOURCE
- IOC.RESOURCE\_X\_CAPABILITY

## 関連タスク:

149 ページの『イベント・カテゴリから機能へのマッピングの作成または変更』  
リソースは、選択したイベントのカテゴリ、およびマップされたリソース機能に応じて、「マップ」ポートレットに表示されます。リソースを作成する前に、リソースの機能を適切なイベント・カテゴリにマップします。

## リソースの表示、更新、または削除

IBM Intelligent Operations Center ユーザー・インターフェースを介して Tivoli Service Request Manager ユーザー・インターフェースにアクセスし、リソースの表示、更新、または削除を行います。

### このタスクについて

以下の手順では、IBM Intelligent Operations Center ユーザー・インターフェースを介して Tivoli Service Request Manager のリソース・データにアクセスする方法について説明します。Tivoli Service Request Manager を介してリソース・データに直接アクセスするには、以下の手順に従います。

1. Tivoli Service Request Manager Start Centerにログオンします。
2. 「移動」 > 「資産」 > 「リソース (IntOpCtr) (Resources (IntOpCtr))」をクリックします。
3. すべての IBM Intelligent Operations Center リソースをリスト表示するには、「リソース (IntOpCtr) (Resources (IntOpCtr))」ウィンドウの「リスト」タブで、「リソース」フィールドをクリックして、Enter キーを押します。
4. リストで、変更するリソースの行をクリックします。
5. 必要に応じて、「リソース」タブまたは「機能」タブをクリックします。

### 手順

1. IBM Intelligent Operations Center ユーザー・インターフェースを開きます。
2. 「詳細」ポートレットの「イベントとインシデント」タブで、表示、更新、または削除の対象にするリソースのあるイベントを、リストから指定します。
3. イベントの周辺にあるリソースのリストを表示するには、イベントを右クリックし、「近隣リソースの表示」をクリックして、絞り込む領域の半径を選択します。リソースのリストが「リソース」タブに表示されます。
4. 「リソース」タブで、リソース・リストの行を右クリックしてメニューからオプションを選択します。
  - リソースの情報を更新するには、「更新」をクリックします。
  - リストとマップからリソースを削除するには、「削除」をクリックします。
  - リソースの情報を表示するには、「プロパティ」をクリックします。どのオプションを選択しても、リソースは Tivoli Service Request Manager の「リソース」タブに表示されます。
5. Tivoli Service Request Manager の「リソース」タブでは、リソースに対して以下のアクションを実行できます。
  - リソース名、説明、緯度、および経度を更新します。
  - リソースを削除するには、「アクションの選択」リストで「リソースの削除」を選択します。
6. 「機能」タブでは、リソースの機能に対して以下のアクションを実行することを選択できます。
  - 該当する機能をクリックし、「数値」を変更します。機能をリソースにマップするには、値を 1 以上にする必要があります。
  - 機能を選択し、行の末尾にある「行を削除対象にマーク」アイコンをクリックします。

7. リソースの更新が終了したら、「リソースの保存」アイコンをクリックします。

## 次のタスク

更新済みのリソース・データを IBM Intelligent Operations Center ユーザー・インターフェースで表示できるようにするには、「マップ」をリセットします。その後、イベントのリソースを、「詳細」ポートレットを介して確認します。

## リソース・タイプの作成

Tivoli Service Request Manager でリソース・タイプを作成します。

### このタスクについて

リソース・タイプの階層を定義できるため、リソース・タイプが子リソース・タイプを持ち、その子リソース・タイプが子リソース・タイプを持つ、ということが可能です。

### 手順

1. Tivoli Service Request Manager Start Centerに管理者としてログオンします。
2. 「移動」 > 「管理」 > 「分類」をクリックします。
3. 既存のすべての IBM Intelligent Operations Center リソース・タイプを表示するには、「リスト」タブの「説明」フィールドに RESOURCE と入力します。階層内のすべてのリソース・タイプが表示されません。
4. 子リソース・タイプを作成する対象のリソース・タイプまたは子リソース・タイプをクリックします。新規リソース・タイプの親の種別の詳細情報が「種別」タブに表示されます。
5. 「種別」タブの「子」の下で「新規行」をクリックします。
6. リスト末尾に追加された空白行で、新規リソース・タイプ用に以下の値を入力します。
  - a. 「種別」列に名前を入力します。
  - b. 「種別の説明」列に説明を入力します。
  - c. リソース・タイプを保存するときにリソース・タイプ名が変更されないようにするには、「説明の生成」チェック・ボックスをクリアします。
7. 「分類の保存」アイコンをクリックします。
8. 新規リソース・タイプのグラフィック・アイコンを追加するには、以下のサブステップを実行します。
  - a. 2 つのサイズのグラフィックのコピーを、PNG フォーマットで保存します。大きい方のグラフィック・アイコンは「マップ」ポートレットに表示され、小さい方のグラフィック・アイコンは「詳細」ポートレット内のイベント・リストに表示されます。

**サイズ 24 ピクセル x 24 ピクセル**

例: `new_resource_24.png`

**サイズ 16 ピクセル x 16 ピクセル**

例: `new_resource_16.png`

- b. 各 PNG ファイルを、以下のようなアプリケーション・サーバー上の該当するディレクトリーにコピーします。
  - `/opt/IBM/WebSphere/wp_profile/installedApps/ICPWPSNode/iss_portal_ear.ear/iss_common_widgets_web.war/images/resource_icons/PNG-24x24/Normal_State`
  - `/opt/IBM/WebSphere/wp_profile/installedApps/ICPWPSNode/iss_portal_ear.ear/iss_common_widgets_web.war/images/resource_icons/PNG-16x16/Normal_State`

- c. 各アイコンが、以下の該当する Web ブラウザー・リンクで正しく表示されることを検証します。
- [http://appserver/ibm/iss/common/widgets/images/resource\\_icons/PNG-24x24/Normal\\_State/new\\_resource\\_24.png](http://appserver/ibm/iss/common/widgets/images/resource_icons/PNG-24x24/Normal_State/new_resource_24.png)
  - [http://appserver/ibm/iss/common/widgets/images/resource\\_icons/PNG-16x16/Normal\\_State/new\\_resource\\_16.png](http://appserver/ibm/iss/common/widgets/images/resource_icons/PNG-16x16/Normal_State/new_resource_16.png)

## リソース・タイプへの機能の追加

Tivoli Service Request Manager で機能を作成します。

### 手順

1. Tivoli Service Request Manager Start Centerに管理者としてログオンします。
2. 「移動」 > 「管理」 > 「分類」をクリックします。
3. IBM Intelligent Operations Center の既存のリソース分類をすべて表示するには、「リスト」タブで、RESOURCE を対象にフィルター操作を行います。
4. 「分類」タブをクリックします。
5. 「子」のリストで、機能の追加先にするリソース・タイプをクリックします。
6. 分類を保存するときにリソース名が変更されないようにするには、「説明の生成」チェック・ボックスをクリアします。
7. 「属性」で、「新規行」をクリックします。
8. 以下の手順で、新規機能の詳細を入力します。
  - a. 「属性」の名前を入力します。
  - b. 「属性」フィールドの右側のフィールドに説明を入力します。
  - c. 「データ型」の値を入力するには、「値の選択」アイコンをクリックして、「値の選択」ウィンドウの値を選択します。
  - d. 子リソースがこの機能を継承することを指定するには、「下位階層に適用しますか」を選択します。
9. 「分類の保存」アイコンをクリックします。

## 標準操作手順、ワークフロー、およびリソースのサンプル

標準操作手順、ワークフロー、およびリソースのサンプルは、IBM Intelligent Operations Center バージョン 1.5 をインストールすると、それに付属しています。

### 標準操作手順

以下の 3 つの標準操作手順が付属しています。

#### PLUSIMITIG: 悪天候に対する最初の準備 (軽減)

PLUSIMITIG には、以下の手順が含まれます。

1. 天候について、重大度を確認します。 関連するワークフローがない、手動の手順です。
2. 必要に応じて、重大度の等級を大きくします。 関連するワークフローがない、手動の手順です。

#### PLUSIPREPA: 悪天候からの避難の準備 (準備)

PLUSIPREPA には、以下の手順が含まれます。

1. 避難所を準備します。 関連するワークフロー PLUSISOP00 がある、手動の手順です。
2. 避難の支援リソースを特定します。 関連するワークフロー PLUSISOP00 がある、手動の手順です。

3. 支援リソースの可用性を評価します。 関連するワークフロー PLUSISOP00 がある、手動の手順です。

### PLUSIRESPO: 影響を受けたエリアの避難 (対応および復旧)

PLUSIRESPO には、以下の手順が含まれます。

1. 避難指示を承認します。 関連するワークフローがない、手動の手順です。
2. 避難経路が明確であることを確認します。 関連するワークフローがない、手動の手順です。

標準操作手順の選択マトリックスには、以下の表に示すように、3 つの標準操作手順を選択するトリガーとなるデータが取り込まれます。

表 35. 標準操作手順の選択マトリックスのサンプル・データ

カテゴリー	重大度	緊急度	確信度	標準操作手順の名前
該当	重度	期限前	監視対象	PLUSIMITIG
該当	重度	期限前	可能性が高い	PLUSIMITIG
該当	極度	期限前	監視対象	PLUSIPREPA
該当	極度	期限前	可能性が高い	PLUSIPREPA
該当	極度	即時	監視対象	PLUSIRESPO

## ワークフローのサンプル

ワークフローのサンプルは、以下の 1 つです。

### PLUSISOP00: アクティビティ・アクションの完了

PLUSISOP00 ワークフローは、アクティビティの状況を COMP (完了) に変更するアクションをトリガーします。

PLUSISOP00 ワークフローは、標準操作手順のサンプルである PLUSIPREPA の各手順に関連付けられています。 いずれかの手順を開始すると、その手順の状況に、完了のマークが自動的に付けられます。

## リソースのサンプル

以下の表にリソースのサンプルを示します。これらは、PLUSICATCPLMAP ドメインにあります。

表 36. リソースのサンプル

リソース	説明	リソース・タイプ
BASCOMEMEY	Bascombe Eye Institute (眼科)	RESOURCES¥HOSPITAL
BLUEFISHW	Blue Fish Warehouse (倉庫)	RESOURCES¥WAREHOUSE
DOCTORSH	Doctor's Hospital (病院)	RESOURCES¥HOSPITAL
MERYCYH	Mercy Hospital (病院)	RESOURCES¥HOSPITAL
MAMICHILD	Miami Children's Hospital (小児病院)	RESOURCES¥HOSPITAL
SFFOODDIST	South Florida Food Distribution (食品流通業)	RESOURCES¥WAREHOUSE
TITLEASING	Tropical Trailer Leasing Corporation (トレーラーのリース会社)	RESOURCES¥WAREHOUSE
UNIMIAMI	University of Miami Hospital (大学病院)	RESOURCES¥HOSPITAL
WTDCDIST	WTDC Distribution Center Miami (物流センター)	RESOURCES¥WAREHOUSE





---

## 第 5 章 ソリューションのカスタマイズ

特定の運用に合わせたソリューションのカスタマイズには、このセクションで説明する、ユーザー・インターフェースおよびシステム・プロパティ・テーブルに関するタスクが含まれます。カスタマイズはソリューションの統合と密接な関係があり、該当するリンクがこのセクションのイベントおよび重要業績評価指標 (KPI) のトピックの中にあります。

---

### ユーザー・インターフェースのカスタマイズ

IBM Intelligent Operations Center ユーザー・インターフェースの要素は、操作に合わせてカスタマイズできます。

ポートレットのレイアウトや外観をカスタマイズできるだけでなく、新規ページを作成することもできます。詳しくは、WebSphere Portal 製品資料を参照してください。

#### 関連情報:



IBM WebSphere Portal 7 の製品資料

### ユーザー・インターフェースのローカライズ

ブラウザ設定により、IBM Intelligent Operations Center ユーザー・インターフェースの言語および日時の設定が決まります。管理者は、日付および時刻の形式をカスタマイズできます。

IBM Intelligent Operations Center では、ご使用のブラウザの設定によってテキストの言語が決まります。その言語が IBM Intelligent Operations Center で利用できない場合は、最も近い関係にある言語が使用されます。例えば、カナダのフランス語の場合はフランス語に戻され、フランス語の場合は常に使用可能な英語に戻されます。ブラウザ設定は、表示されるすべての日時の時間帯も決定します。IBM Intelligent Operations Center の日時は、ブラウザの時間帯に合わせて自動的に調整されます。

すべての日時は、ご使用の時間帯で、システム・プロパティ・データベース表で指定されている形式で表示されます。日時の書式制御ストリングは、システム・プロパティに保持されています。プロパティを編集してデータベース内の値を変更するには、このトピックの末尾にあるリンクに従ってください。

#### 関連概念:

197 ページの『システム全体の構成データの指定』

IBM Intelligent Operations Center システム・プロパティ・テーブルは、IBM Intelligent Operations Center の構成データを保管します。

107 ページの『KPI イベントに対する CAP の使用』

IBM Intelligent Operations Center の一部として提供されている WebSphere Message Broker は、CAP イベント・メッセージを受け入れ、重要業績評価指標 (KPI) の計算にそのデータを使用します。

### ポートレットのリスト

IBM Intelligent Operations Center は、ポータル・テクノロジーを使用してツールを提供したり情報を表示したりする、ポートレット・ベースのソリューションです。以下のセクションに、IBM Intelligent Operations Center に含まれているすべてのポートレットがリストされています。

## ユーザー・ポートレット

IBM Intelligent Operations Center に含まれるユーザー・ポートレットを以下の表に示します。この表は、各ポートレットが使用可能なサンプル・ページ・ビューでも示します。

このポートレットはカスタマイズできます。詳しくは、トピックの末尾にあるリンクを参照してください。

表 37. IBM Intelligent Operations Center のユーザー・ポートレット

ポートレット	説明	サンプル・ページ・ビュー
300 ページの『連絡先』	「連絡先」ポートレットを使用すると、カテゴリ別に分類された連絡先のリストを表示することができます。連絡する必要がある相手に基づいたカテゴリ別に、連絡先を分類できます。例えば、一般的な作業連絡先のカテゴリや、プロジェクト作業連絡先の別のカテゴリを設定できます。「連絡先」ポートレットを使用して、それらの連絡先とやり取りしたり、自身のオンライン状況、連絡先、またはグループを変更したりすることができます。	<ul style="list-style-type: none"> <li>295 ページの『「スーパーバイザー：状況」ビュー』</li> <li>296 ページの『「スーパーバイザー：操作」ビュー』</li> <li>297 ページの『「オペレーター：操作」ビュー』</li> </ul>
301 ページの『詳細』	「詳細」ポートレットは対話式のリスト・ポートレットです。ユーザーに表示権限があるすべてのイベントが、イベント・リストと、「詳細」ポートレットにリンクされた任意のマップ・ポートレットに表示されます。	<ul style="list-style-type: none"> <li>296 ページの『「スーパーバイザー：操作」ビュー』</li> <li>297 ページの『「オペレーター：操作」ビュー』</li> <li>299 ページの『「ロケーション・マップ」ビュー』</li> </ul>
304 ページの『重要業績評価指標のドリルダウン』	「重要業績評価指標のドリルダウン」ポートレットで特定の KPI カテゴリに絞り込んで表示するには、「状況」ポートレットでそのカテゴリをクリックします。こうすることで、そのカテゴリのみが「重要業績評価指標のドリルダウン」ポートレットに表示されるようになります。そのリストを使用して、状況が変わる原因となった KPI の詳細に到達するまで、基礎となる KPI を調べることができます。	<ul style="list-style-type: none"> <li>295 ページの『「スーパーバイザー：状況」ビュー』</li> </ul>
305 ページの『ロケーション・マップ』	「ロケーション・マップ」ポートレットでは、ロケーション・マップでマークされているイベントを確認することができます。IBM Intelligent Operations Center のロケーション・マップは、対話用に事前に定義されているエリア（大規模なスポーツ・スタジアムの座席エリアなど）を含むマップまたは計画です。	<ul style="list-style-type: none"> <li>299 ページの『「ロケーション・マップ」ビュー』</li> </ul>

表 37. IBM Intelligent Operations Center のユーザー・ポートレット (続き)

ポートレット	説明	サンプル・ページ・ビュー
309 ページの『マップ』	<p>「マップ」ポートレット内には以下のものがあります。</p> <p>イベント・マーカーおよびリソース・マーカーが表示される地理的領域のマップ。</p> <p>マップ上および「マップ」ポートレットにリンクしているポートレット内に表示されるイベントのカテゴリを選択するためのフィルター・フォーム。</p> <p>マップ上およびリンクしている「詳細」ポートレットの「リソース」タブ内に表示されるリソースの機能を選択するためのフィルター・フォーム。このフォームを表示するには、まず、「詳細」ポートレットで「近隣リソースの表示」を選択します。</p>	<ul style="list-style-type: none"> <li>• 296 ページの『「スーパーバイザー：操作」ビュー』</li> <li>• 297 ページの『「オペレーター：操作」ビュー』</li> </ul>
314 ページの『マイ・アクティビティ』	<p>ログオンしているユーザーは、「マイ・アクティビティ」ポートレットで、これらの所有者に割り当てられたアクティビティを表示することができます。「マイ・アクティビティ」ポートレット内のアクティビティは、その親の標準操作手順でグループ化されています。それぞれの標準操作手順は、個々のイベントに対応します。</p>	<ul style="list-style-type: none"> <li>• 295 ページの『「スーパーバイザー：状況」ビュー』</li> <li>• 296 ページの『「スーパーバイザー：操作」ビュー』</li> <li>• 297 ページの『「オペレーター：操作」ビュー』</li> </ul>
316 ページの『通知』	<p>「通知」ポートレットは、KPI および関連イベントの変更により発生したアラートの動的な対話式リストを提供します。このポートレットの役割は、KPI またはイベント状況の変更に注意を促すことです。このリストには各アラートの重要な詳細情報が含まれています。</p>	<ul style="list-style-type: none"> <li>• 295 ページの『「スーパーバイザー：状況」ビュー』</li> <li>• 296 ページの『「スーパーバイザー：操作」ビュー』</li> <li>• 297 ページの『「オペレーター：操作」ビュー』</li> </ul>
318 ページの『レポート』	<p>「レポート」ポートレットでは、イベントのレポートをグラフとして表示することができます。このポートレットは、イベントのグループ化の基準となる各種のオプションを提供します。さらに、特定の日付または日付範囲を指定してイベントを選択することができます。レポートは、現在および将来のイベントへの対応について計画を策定するのに役立ちます。</p>	<ul style="list-style-type: none"> <li>• 298 ページの『「スーパーバイザー：レポート」』</li> <li>• 299 ページの『「オペレーター：レポート」』</li> </ul>

表 37. IBM Intelligent Operations Center のユーザー・ポートレット (続き)

ポートレット	説明	サンプル・ページ・ビュー
321 ページの『状況』	「状況」ポートレットには、表示する権限のある複数の組織全体にわたって、KPI の状況に関するエグゼクティブ・レベルのサマリーが表示されます。計画を立て、必要に応じて対処できるように、このポートレットを使用して、KPI の状況に関する最新の変更を確認します。	<ul style="list-style-type: none"> <li>295 ページの『「スーパーバイザー：状況」ビュー』</li> </ul>

#### 関連タスク:

162 ページの『ポートレットのカスタマイズ』

管理者は、ポートレットの設定値を変更してポートレットをカスタマイズすることができます。

### 管理ポートレット

IBM Intelligent Operations Center に含まれる管理ポートレットを以下の表に示します。管理ポートレットは「管理」ページ内にあります。

表 38. IBM Intelligent Operations Center の管理ポートレット

ポートレット	説明
215 ページの『製品情報』	「製品情報」ポートレットを使用して、インストール済みの IBM Intelligent Operations Center および統合された IBM Smarter Cities Software Solutions のバージョンの詳細を表示します。インストール後に適用した更新の詳細も表示できます。
224 ページの『管理コンソール』	「管理コンソール」ポートレットを使用して、ソリューションによって提供されるサービスを管理します。
232 ページの『コンポーネントの検証』	システム検査チェックツールは、IBM Intelligent Operations Center 内のコンポーネントをテストし、アクセス可能であるか、および操作可能であるかを判別します。
90 ページの『ユーザー権限サマリー』	「ユーザー権限サマリー」ポートレットは、ユーザーに付与されているグループ・メンバーシップおよび権限の詳細を表示します。
186 ページの『重要業績評価指標』	「重要業績評価指標」ポートレットでは、KPI を表示、変更、コピー、作成、および削除することができます。また、「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットに表示される KPI 階層をカスタマイズすることもできます。
195 ページの『ロケーション・マップ・マネージャー』	「ロケーション・マップ・マネージャー」ポートレットでは、「ロケーション・マップ」ポートレットをカスタマイズすることができます。
143 ページの『標準操作手順』	標準操作手順およびアクティビティを定義することで、IBM Intelligent Operations Center で受信するイベントを管理できます。「標準操作手順」ポートレットを使用して、Tivoli Service Request Manager で、標準操作手順、標準操作手順の選択マトリックス、およびワークフロー・デザイナーの各アプリケーションにアクセスします。

表 38. IBM Intelligent Operations Center の管理ポータルレット (続き)

ポータルレット	説明
120 ページの『イベント・スクリプト記述』	「イベント・スクリプト記述」ポータルレットを使用して、事前に定義された時間間隔でパブリッシュされるイベントの順次リストを作成するスクリプトを記述します。
115 ページの『サンプル・パブリッシャー』	「サンプル・パブリッシャー」ポータルレットは、ソリューションを管理または検証する管理者を対象とする自動テスト・ツールです。管理者は、「サンプル・パブリッシャー」ポータルレットをクライアント・アプリケーションとして使用することで、IBM Intelligent Operations Center における CAP メッセージのパブリッシュをテストすることができます。「サンプル・パブリッシャー」ポータルレットを使用すれば、テスト・クライアント・アプリケーションを手動で作成する必要がなくなります。

#### 関連タスク:

162 ページの『ポータルレットのカスタマイズ』

管理者は、ポータルレットの設定値を変更してポータルレットをカスタマイズすることができます。

## ページの作成またはカスタマイズ

IBM Intelligent Operations Center に組み込む新規ページを作成し、それらのページにどのポータルレットを表示するかを指定することができます。各ページに組み込むポータルレットの外観およびレイアウトをカスタマイズできます。

### このタスクについて

ページおよびポータルレットをカスタマイズするには、WebSphere Portal ユーザー・インターフェースを使用します。

注: ページ・レイアウトを作成または編集するときには、ポータルレットが以下の規則に従って正しく動作することを確認してください。

- 「マップ」ポータルレットからイベントを追加できるようにするため、「マップ」ポータルレットと「詳細」ポータルレットは同一グループに属し、同一ページ上に存在する必要があります。
- 「マイ・アクティビティ」ポータルレットからイベント詳細を要求できるようにするか、または「詳細」ポータルレットから標準操作手順の詳細を要求できるようにするため、「マイ・アクティビティ」ポータルレットと「詳細」ポータルレットは同一グループに属し、同一ページ上に存在する必要があります。

### 手順

- WebSphere Portal を開くには、「管理」タブをクリックします。
- WebSphere Portal で、「ポータル・ユーザー・インターフェース」をクリックします。
- 必須指定のオプションをクリックします。
  - ページの処理または新規ページの作成を行うには、「ページの管理」をクリックします。
  - テーマとスキンの登録、デフォルトのテーマの設定、および各テーマのデフォルトのスキンの設定を行うには、「テーマとスキン」をクリックします。
  - バナー、ナビゲーション、フォント、色など、テーマでのキー・サイト・エレメントをカスタマイズするには、「テーマ・カスタマイザー」をクリックします。

4. 必要な変更を加えます。 WebSphere Portal を使用してポートレットをカスタマイズする方法について詳しくは、WebSphere Portal 製品資料のトピックの末尾にあるリンクを参照してください。

#### 関連情報:

 IBM WebSphere Portal 7 の製品資料

## ポートレットのカスタマイズ

管理者は、ポートレットの設定値を変更してポートレットをカスタマイズすることができます。

### このタスクについて

カスタマイズのモードには以下の 2 つが指定でき、各モードはすべてのユーザーのポートレット設定を変更します。

- 「共有設定の編集」は、設定の変更時にユーザーが使用しているポートレットのインスタンスに対してのみ、ポートレットを変更します。
- 「構成」は、ポートレットのグローバル設定を変更します。この変更は、ポートレットのインスタンスの発生場所にかかわらず、すべてのインスタンスに対して行われます。

ユーザーが使用可能なカスタマイズのモードは、ユーザー ID に関連付けられた権限により異なります。グローバル設定は共有設定によって置き換えられます。

### 手順

1. ソリューション・ポータルに管理者としてログオンします。
2. ポートレットの右上隅をクリックし、ポートレット・メニューを表示します。
3. 「共有設定の編集」または「構成」をクリックします。
4. 表示されるフィールドに使用する設定値を入力します。
5. 設定ウィンドウを閉じるには、以下のいずれかのボタンをクリックします。
  - 変更を保存する場合は、「保存」
  - 変更を取り消す場合は、「キャンセル」
  - デフォルトのグローバル設定に戻すには、「デフォルト値にリセット」

### タスクの結果

保存した新しい設定値は、次回そのポートレットを最新表示したときに有効になります。リセットされなかったパラメーターには、IBM Intelligent Operations Center で提供されるデフォルトのグローバル設定が使用されます。

#### 「製品情報」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「製品情報」ポートレットをカスタマイズできます。

#### カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「製品情報」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 39. 「製品情報」ポートレットのカスタマイズ・パラメーター

パラメーター	説明	デフォルト値
--------	----	--------



表 39. 「製品情報」ポータルレットのカスタマイズ・パラメーター (続き)

ポータルレットの高さ	ポータルレットの標準的な高さを示すピクセル数。	400
ポータルレットの最大の高さ	ポータルレットの最大の高さを示すピクセル数。	600

#### 関連概念:

215 ページの『製品情報』

「製品情報」ポータルレットを使用して、インストール済みの IBM Intelligent Operations Center および統合された IBM Smarter Cities Software Solutions のバージョンの詳細を表示します。インストール後に適用した更新の詳細も表示できます。

### 「管理コンソール」ポータルレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「管理コンソール」ポータルレットをカスタマイズできます。

#### カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「管理コンソール」ポータルレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 40. 「管理コンソール」ポータルレットのカスタマイズ・パラメーター

パラメーター	説明	デフォルト値
デフォルトのヘルプ JSP	ポータルレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	AdministrationConsolePortletHelp
ポータルレットの高さ	ポータルレットの標準的な高さを示すピクセル数。	400
ポータルレットの最大の高さ	ポータルレットの最大の高さを示すピクセル数。	450
ポータルレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、「管理コンソール」という、ソリューションによって提供されたタイトルが表示されます。
リソース・バンドル	プロパティの値 (ポータルレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。

## 関連概念:

224 ページの『管理コンソール』

「管理コンソール」ポートレットを使用して、ソリューションによって提供されるサービスを管理します。

## 「連絡先」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「連絡先」ポートレットをカスタマイズできます。

## カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「連絡先」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 41. 「連絡先」ポートレットのカスタマイズ・パラメーター

パラメーター	説明	デフォルト値
デフォルトのヘルプ JSP	ポートレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	SametimeWebClientPortletHelp
ポートレットの高さ	ポートレットの標準的な高さを示すピクセル数。	250
ポートレットの最大の高さ	ポートレットの最大の高さを示すピクセル数。	600
ポートレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、タイトルはソリューションによって提供され、「連絡先」が表示されます。
リソース・バンドル	プロパティの値 (ポートレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。

## 関連概念:

300 ページの『連絡先』

ソリューション内でインスタント・メッセージを送信するには、「連絡先」ポートレットを使用します。

## 「詳細」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「詳細」ポートレットをカスタマイズできます。

## カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「詳細」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 42. 「詳細」ポートレットのカスタマイズ・パラメーター

パラメーター名	説明	デフォルト値
---------	----	--------

表 42. 「詳細」 ポートレットのカスタマイズ・パラメーター (続き)

列	リストに表示される列の仕様および順序	[{"id": "commonevents.headline", "width": "20"}, {"id": "commonevents.eventType", "width": "7"}, {"id": "commonevents.category", "width": "10"}, {"id": "commonevents.severity", "width": "10"}, {"id": "commonevents.certainty", "width": "10"}, {"id": "commonevents.urgency", "width": "10"}, {"id": "commonevents.sent", "width": "12", "sortPriority": "1", "sortAscending": "false"}]
Conditions	イベントまたはリソースの表示の追加条件。追加条件は、ツールバーまたはマップ・フィルターを使用してオーバーライドすることはできません。デフォルトでは、追加条件は適用されません。	[]
デフォルトのヘルプ JSP	ポートレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	CommonEventsPortletHelp
追加イベントの非表示	「イベントの追加」 ボタンとポップアップ・メニュー・オプションを表示するか非表示にするかを定めるための true または false の設定。	true
追加リソースの非表示	「リソース」 タブの「リソースの追加」 ボタンを表示するか非表示にするかを定めるための true または false の設定。	true
イベントの非表示	「イベントおよびインシデント」 タブを表示するか非表示にするかを定めるための true または false の設定。	false
リソースの非表示	「リソース」 タブを表示するか非表示にするかを定めるための true または false の設定。	false
ツールバーの非表示	リストの上部にツールバーを表示するか非表示にするかを定めるための true または false の設定。	true
リソース・モード取り消しの無視	「マップ」 ポートレットから着信するリソース・モード取り消しメッセージを確認するか無視するかを定めるための true または false の設定。	false
イベント作成の無視	ユーザーが「マップ」 ポートレットで作成したイベントを確認するか無視するかを定めるための true または false の設定。	false

表 42. 「詳細」ポートレットのカスタマイズ・パラメーター (続き)

イベント・フィルター変更の無視	ユーザーが「マップ」ポートレットで行ったイベント・フィルター選択を確認するか無視するかを決めるための true または false の設定。	false
イベント選択の無視	ユーザーが「マップ」ポートレットで行った着信イベント選択を確認するか無視するかを決めるための true または false の設定。	false
イベント・タスクの無視	すべてのイベント・ポップアップ・メニュー選択を確認するか無視するかを決めるための true または false の設定。	false
マップ・リセットの無視	ポートレットの「リソース」ボタンのクリックを確認するか無視するかを決めるための true または false の設定。	false
変更されたリソース・フィルターの無視	ユーザーが「マップ」ポートレットで行ったリソース・フィルター選択を確認するか無視するかを決めるための true または false の設定。	false
リソース・タスクの無視	すべてのリソース・ポップアップ・メニュー選択を確認するか無視するかを決めるための true または false の設定。	false
ポートレット・グループ ID	このポートレットが属しているグループの名前。 共通名は、同一ページでの「マップ」、「詳細」、および「ロケーション・マップ」の各ポートレットの間の通信をセットアップします。	default
ポートレットの高さ	ポートレットの標準的な高さを示すピクセル数。	350
ポートレットの最大の高さ	ポートレットの最大の高さを示すピクセル数。	600
ポートレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、タイトルはソリューションによって提供され、「詳細」が表示されます。
リソース・バンドル	プロパティの値 (ポートレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。 この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。 リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。

注: リソース・バンドルを指定した場合にポートレット・タイトルがどうなるかに関する説明は、同じリソース・バンドルがソースとなっている列タイトルについても適用されます。

## Columns パラメーター

**columns** パラメーターの値は、表 43 の説明に従って構成できる、JSON オブジェクトの配列です。

表 43. 「詳細」ポートレットの *columns* パラメーター値内部のオブジェクト

オブジェクト	内容
id	列を表示することを示す列 ID。
width	列の幅を示すピクセル数。
format	日時列に使用する形式を表す文字列。この項目は、 <code>sysprop</code> テーブル内の設定をオーバーライドします。
sortAscending	<ul style="list-style-type: none"> <li>• <code>true</code> の場合、列項目に対して昇順のソート順を使用します。</li> <li>• <code>false</code> の場合、列項目に対して降順のソート順を使用します。</li> </ul>
sortPriority	<ul style="list-style-type: none"> <li>• すべての列の中での、その列のソート優先順位を示す番号。番号が若いほど、優先順位は高くなります。</li> <li>• 値なしで空白のままの場合、列のデフォルトのソート優先順位を使用します。</li> <li>• 値 <code>-1</code> の場合、列のデフォルトのソート優先順位を使用不可にします。</li> </ul>
title	列見出しのタイトル。デフォルトの見出しタイトルを使用する場合は、空白のままにします。

列は、**columns** パラメーターの値を形成する JSON オブジェクトに指定されたのと同じ順序でポートレットに表示されます。この値以内に指定された列 ID を持つ列のみが表示され、その他の列はすべて非表示になります。**columns** パラメーターの値を省略すると、164 ページの表 42 の 1 行目に示されているデフォルトの設定に従って列が表示されます。

列 ID に指定可能な値を表 44 に示します。

表 44. 「詳細」ポートレットに有効な列 ID

列 ID	説明
<code>commonevents.id</code>	共通イベント・テーブルのイベントに指定された UUID。
<code>commonevents.externalEventid</code>	イベント送信者が割り当てたイベント ID。
<code>commonevents.specification</code>	イベントの前にくる形式指定 (例えば CAP)。
<code>commonevents.eventType</code>	イベントがエスカレートされたかどうかを示す、システム固有コードの未変換の値。Event または Incident です。
<code>commonevents.sent</code>	イベント送信者の送信時刻によるもの。
<code>commonevents.headline</code>	イベントを説明する見出しテキスト。
<code>commonevents.hover text</code>	イベントを説明する吹き出しテキスト。
<code>commonevents.category</code>	未変換のカテゴリ値。
<code>commonevents.certainty</code>	未変換の確信度値。
<code>commonevents.severity</code>	未変換の重大度値。

表 44. 「詳細」ポートレットに有効な列 ID (続き)

列 ID	説明
commonevents.urgency	未変換の緊急度値。
commonevents.url	イベントについての追加情報の URL Web アドレス。
commonevents.externalWorkOrderId	関連の作業指示書 ID。通常は Tivoli Service Request Manager 標準操作手順 ID です。
commonevents.areaId	ロケーション・マップ・エリア ID (イベントがロケーション・マップにリンクされている場合)。
commonevents.largeIcon	マップ上でイベントを表すために使用されるアイコン。
commonevents.largeHiliteIcon	マップ上でイベントを強調表示するとき使用されるアイコン。
commonevents.largeGreyIcon	マップ上のイベントを無効にするときに使用されるアイコン。
commonevents.smallIcon	リスト内のイベントに使用されるアイコン。
commonevents.user1	Tivoli Netcool/Impact ポリシー内部で設定される値。
commonevents.user2	Tivoli Netcool/Impact ポリシー内部でユーザーが設定する値。
commonevents.user3	Tivoli Netcool/Impact ポリシー内部でユーザーが設定する値。
commonevents.user4	Tivoli Netcool/Impact ポリシー内部でユーザーが設定する値。
commonevents.user5	Tivoli Netcool/Impact ポリシー内部でユーザーが設定する値。

## Conditions パラメーター

**conditions** パラメーターの値は、表 45 の説明に従って構成できる、JSON オブジェクトの配列です。

表 45. 「詳細」ポートレットの conditions パラメーター値内部のオブジェクト

オブジェクト・タイプ	内容
selector	操作を適用する列の ID。
operator	セレクターの値に適用される SQL 演算子。オプションは以下のとおりです。 <ul style="list-style-type: none"> <li>contains セレクター列に値が含まれる場合。これがデフォルトです。</li> <li>equals セレクター列が値と等しい場合。</li> <li>notEquals セレクター列が値と等しくない場合。</li> <li>startsWith セレクター列が値で始まる場合。</li> <li>endsWith セレクター列が値で終わる場合。</li> </ul>
values	表示列の値。値は、前の表に指定されている未変換のキー値である必要があります。

注:



**conditions** パラメーターは、「マップ」ポートレットのフィルターで提供される基準に追加する基準を定義します。これらの基準は、マップ・フィルターまたはツールバーで指定されている条件をオーバーライドします。

注: ツールバーはデフォルトでは非表示です。

例えば、列に以下のような変更が必要だとします。

- 「送信済み」、「見出し」、「カテゴリ」、および「URL」の列のみを表示する。
- 「送信済み」列の幅を 12 に変更する。
- 「送信済み」列の形式を d-MMM-yyyy HH:mm に変更する。
- ソート順優先順位を、「送信済み」列で「2」に、「カテゴリ」列で「1」に変更する。

これらの変更は、「列」フィールドに以下を入力して設定を保存すると表示されます。

```
[{"id": "commonevents.sent", "width": "10", "format": "d-MMM-yyyy HH:mm", "sortPriority": "2"}, {"id": "commonevents.headline"}, {"id": "commonevents.category", "sortPriority": "1"}, {"id": "commonevents.url"}]
```

例えば、以下の条件を両方とも満たすイベントのみを表示するとします。

- 「重大度」が「Extreme」または「Severe」である。
- 「イベント・タイプ」が「Incident」である。

これらの変更は、「条件」フィールドに以下を入力して設定を保存すると表示されます。

```
[{"selector": "commonevents.severity", "operator": "equals", "values": ["Extreme", "Severe"]}, {"selector": "commonevents.eventType", "operator": "equals", "values": ["Incident"]}]
```

#### 関連概念:

301 ページの『詳細』

「詳細」ポートレットを使用して、IBM Intelligent Operations Center でイベントの表示、モニター、および管理を行います。

### 「重要業績評価指標のドリルダウン」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「重要業績評価指標のドリルダウン」ポートレットをカスタマイズできます。

#### カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「重要業績評価指標のドリルダウン」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 46. 「重要業績評価指標のドリルダウン」ポートレットのカスタマイズ・パラメーター

パラメーター	説明	デフォルト値
列	リストに表示される列の仕様および順序	[{"sortPriority": "1", "sortAscending": "true", "id": "kpi.NAME"}]
カスタム KPI 色	KPI の状況を示すためにポートレットで使用される色。例えば、以下のように入力できます。  {"acceptable": "#7f7f7f", "take_action": "#34333"}  ここで入力した色は、ソリューションによって提供される色をオーバーライドします。	{}

表 46. 「重要業績評価指標のドリルダウン」ポートレットのカスタマイズ・パラメーター (続き)

デフォルトのヘルプ JSP	ポートレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	KpiDrillDownPortletHelp
KPI フィルターの有効化	<b>KPI filter</b> パラメーター設定の情報に従って KPI フィルターを有効または無効にするための true または false の設定。	false
ツールバーの非表示	ポートレットの上部にツールバーを表示するかしないかを定めるための true または false の設定。	true
KPI フィルター	ポートレットについて <b>Enable KPI filter</b> を true に設定したときに表示される、KPI の ID。例えば、以下のように入力できます。  ["Transportation", "Airports", "Roads_and_Traffic", "Public_Safety", "Fire_Department", "Water", "Delayed_Flights", "Delayed_Flights_Airport_Two"]	[]
ポートレット・グループ ID	このポートレットが属しているグループの名前。 共通名は、同一ページでの「重要業績評価指標のドリルダウン」ポートレットと「状況」ポートレットの間の通信をセットアップします。	default
ポートレットの高さ	ポートレットの標準的な高さを示すピクセル数。	350
ポートレットの最大の高さ	ポートレットの最大の高さを示すピクセル数。	600
ポートレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、タイトルはソリューションによって提供され、「重要業績評価指標のドリルダウン」が表示されます。
リソース・バンドル	プロパティの値 (ポートレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。

注: リソース・バンドルを指定した場合にポートレット・タイトルがどうなるかに関する説明は、同じリソース・バンドルがソースとなっている列タイトルについても適用されます。

## Columns パラメーター

`columns` パラメーターの値は、以下の表の説明に従って構成できる、JSON オブジェクトの配列です。

表 47. 「重要業績評価指標のドリルダウン」ポートレットの `columns` パラメーター値内部のオブジェクト

オブジェクト	内容
<code>sortPriority</code>	<ul style="list-style-type: none"><li>すべての列の中での、その列のソート優先順位を示す番号。番号が若いほど、優先順位は高くなります。</li><li>値なしでブランクのままの場合、列のデフォルトのソート優先順位を使用します。</li><li>-1 の場合、列のデフォルトのソート優先順位を使用不可にします。</li></ul>
<code>sortAscending</code>	<ul style="list-style-type: none"><li><code>true</code> の場合、列項目に対して昇順のソート順を使用します。</li><li><code>false</code> の場合、列項目に対して降順のソート順を使用します。</li></ul>
<code>id</code>	列を表示することを示す列 ID。

列は、`columns` パラメーターの値を形成する JSON オブジェクトに指定されたのと同じ順序でポートレットに表示されます。この値以内に指定された列 ID を持つ列のみが表示され、その他の列はすべて非表示になります。`columns` パラメーターの値を省略すると、169 ページの表 46 の 1 行目に示されているデフォルトの設定に従って列が表示されます。

列 ID に指定可能な値を以下の表に示します。

表 48. 「重要業績評価指標のドリルダウン」ポートレットに有効な列 ID

列 ID	説明
<code>kpi.NAME</code>	KPI の名前。
<code>kpi.CURRENT.VALUE</code>	KPI の現行値。
<code>kpi.CURRENT.STATUS</code>	KPI の現在の状況。
<code>kpi.CALCULATION.TIME</code>	KPI が計算された時刻。

### 関連概念:

304 ページの『重要業績評価指標のドリルダウン』

KPI カテゴリと、そのカテゴリの基礎となる KPI の状況に関する追加の情報を表示するには、「重要業績評価指標のドリルダウン」ポートレットを使用します。

## 「重要業績評価指標」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「重要業績評価指標」ポートレットをカスタマイズできます。

## カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「重要業績評価指標」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 49. 「重要業績評価指標」ポートレットのカスタマイズ・パラメーター

パラメーター	説明	デフォルト値
--------	----	--------

表 49. 「重要業績評価指標」ポータルレットのカスタマイズ・パラメーター (続き)

デフォルトのヘルプ JSP	ポータルレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	KpiManagerPortletHelp
ポータルレットの高さ	ポータルレットの標準的な高さを示すピクセル数。	500
ポータルレットの最大の高さ	ポータルレットの最大の高さを示すピクセル数。	600
ポータルレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、タイトルはソリューションによって提供され、「重要業績評価指標」が表示されます。
リソース・バンドル	プロパティの値 (ポータルレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。

#### 関連概念:

186 ページの『重要業績評価指標』

「重要業績評価指標」ポータルレットでは、IBM Intelligent Operations Center の重要業績評価指標 (KPI) およびそれらの階層表示をカスタマイズすることができます。

### 「ロケーション・マップ」ポータルレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「ロケーション・マップ」ポータルレットをカスタマイズできます。

#### カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、ポータルレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 50. 「ロケーション・マップ」ポータルレットのカスタマイズ・パラメーターの値

パラメーター	説明	デフォルト値
デフォルト・フィルターの選択	マップに表示されるデフォルトのイベント・カテゴリー。名前を入力します。複数の名前を入力する場合は、スペースを使用せずにセミコロンで区切ります。	CBRNE;Env;Fire;Geo;Health;Infra;Met;Rescue;Safety;Security;Transport;Other
デフォルトのエリア強調表示色	カーソルを使用してエリア上を移動するときに強調表示されるエリアのデフォルトの色。	#808080
デフォルトのヘルプ JSP	ポータルレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	LocationMapPortletHelp
デフォルト・マップの選択	ポータルレットに表示されるロケーション・マップの名前。	Miami SunLife Stadium

ポートレットの最大の高さ	ポートレットの最大の高さを示すピクセル数。	600
ポートレットの高さ	ポートレットの標準的な高さを示すピクセル数。	400
ポートレット・グループ ID	このポートレットが属しているグループの名前。 共通名は、同一ページでの「マップ」、「詳細」、および「ロケーション・マップ」の各ポートレットの間の通信をセットアップします。	default
ポートレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、タイトルはソリューションによって提供され、「ロケーション・マップ」が表示されます。
リソース・バンドル	プロパティの値 (ポートレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。 この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。 リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。

#### 関連概念:

305 ページの『ロケーション・マップ』

「ロケーション・マップ」ポートレットでは、ロケーション・マップでマークされているイベントを確認することができます。 IBM Intelligent Operations Center のロケーション・マップは、対話用に事前に定義されているエリア (大規模なスポーツ・スタジアムの座席エリアなど) を含むマップまたは計画です。

### 「ロケーション・マップ・マネージャー」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「ロケーション・マップ・マネージャー」ポートレットをカスタマイズできます。

#### カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、ポートレットのカスタマイズ・パラメーターの値が入力されています。 カスタマイズ・パラメーターについては、以下の表で説明します。

表 51. 「ロケーション・マップ・マネージャー」ポートレットのカスタマイズ・パラメーターの値

パラメーター	説明	デフォルト値
選択された新規エリアのデフォルト色	マップ上で選択された描画エリアのデフォルトの色。	#4AA02C
選択された保存済みエリアのデフォルト色	マップ上で選択された保存済みエリアのデフォルト色。	#808080
新規エリアのデフォルト色	マップ上で描画されたエリアのデフォルト色。	#009900

保存済みエリアのデフォルト色	マップ上で保存されたエリアのデフォルト色	#808080
デフォルトのヘルプ JSP	ポートレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	LocationMapManagerPortletHelp
ポートレットの高さ	ポートレットの標準的な高さを示すピクセル数。	400
ポートレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、タイトルはソリューションによって提供され、「ロケーション・マップ・マネージャー」が表示されません。
リソース・バンドル	プロパティの値 (ポートレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。

#### 関連概念:

195 ページの『ロケーション・マップ・マネージャー』

「ロケーション・マップ・マネージャー」ポートレットでは、「ロケーション・マップ」ポートレットをカスタマイズすることができます。

### 「マップ」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「マップ」ポートレットをカスタマイズできます。

#### カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「マップ」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 52. カスタマイズ・パラメーターの値

パラメーター	説明	デフォルト値
センター緯度	マップの中心点を設定する、特定の座標。マップの現在位置がフィールドの右に表示されます。必要な場所までマップをズームまたはパンして、表示された値をカット・アンド・ペーストすることにより、対応するフィールドに取り込むことができます。	25.780416
センター経度		-80.203629



表 52. カスタマイズ・パラメーターの値 (続き)

ズーム・レベル	マップの標準倍率レベル。使用可能な有効ズーム・レベルの範囲は、基本マップによって異なります。一般に、この範囲は 1 以上です。1 の値は最低ズーム・レベルであり、マップが最低倍率で表示されます。例えば、ソリューションに付属しているデフォルトの ArcGIS 基本マップでは、最大ズーム・レベル 12 までの地理的詳細が表示されます。	11
基本層のタイプ	基本マップのタイプの値。	ARC_GIS_REST
基本層の URL	基本マップの URL。この URL には、マップの x、y、および z の座標を表すプレースホルダーが正しい順序で含まれている必要があります。マップは、インストール済みの Esri GIS サーバーまたは公的に利用できる GIS サービスから選択できます。	http://services.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer/tile/{z}/{y}/{x}
KML フィードまたはファイルの URL	<p>KML データを表示するための URL。同じドメインとポートを持つポートレットと同じサーバーでの位置を表す URL を入力してください。この条件を確実に実装するには、「/」(スラッシュ文字) で始まる URL のみを入力して、ブラウザが現在のドメインおよびポートを選択するようにします。複数の URL スtring の場合は、URL 間にセミコロンを使用し、スペースは入れないでください。目的の Web サイトがローカルではない場合は、ご使用のポータル・サーバー上のプロキシ・サーバーを使用してサイトにアクセスします。</p> <p><b>注:</b> このオプションは、小規模なローカル調整に使用します。ただし、データが原因で表示過剰になったりパフォーマンスに影響が出たりしないよう、対象となるデータの量を考慮してください。</p>	ソリューションによって提供されるデフォルト値はありません。

表 52. カスタマイズ・パラメーターの値 (続き)

表示する項目の量	ビューに表示するマーカーの数の 限度。 表示できるマーカーの最大 数を入力してください。 ビュー内 のマップ領域のマーカー数がこの 限度を超えると、マーカーは表示 されなくなり、警告メッセージが 表示されます。 ユーザーは、マー カーをロードするか、ビューを変 更するかを選択することができます。	250
デフォルト・フィルターの 選択	マップに表示されるデフォルトの イベント・カテゴリー。 名前を入 力します。 複数の名前を入力する 場合は、スペースを使用せずにセ ミコロンで区切ります。	CBRNE;Env;Fire;Geo; Health;Infra;Met;Rescue; Safety;Security;Transport; Other
ポートレットの最大の高さ	ポートレットの最大の高さを示す ピクセル数。	600
ポートレット・グループ ID	このポートレットが属しているグ ループの名前。 共通名は、同一ペ ージでの「マップ」、「詳細」、 および「ロケーション・マップ」 の各ポートレットの間の通信をセ ットアップします。	default
ポートレットのタイトル	ソリューションによって提供され るタイトルをオーバーライドする タイトル。	このパラメーターに値を入力しなかった場合、タイ トルはソリューションによって提供され、「マッ プ」が表示されます。
デフォルトのヘルプ JSP	ポートレットのメニューからヘル プが選択されたときに表示される JSP ヘルプ・ファイルの名前。	NavigatorPortletHelp
リソース・バンドル	プロパティの値 (ポートレッ ト・タイトルなど) のソースとし て提供するリソース・バンドルの 場所。 この場所は、提供するリソ ース・バンドル内のプロパティ ー・キーとしてタイトルを指定す る場合に必要です。 リソース・バ ンドルを指定しない場合、キーの 探索は行われず、ソリューション によって提供されるタイトルが表 示されます。	デフォルトのリソース・バンドルはありません。

**関連概念:**

309 ページの『マップ』

「マップ」ポートレットを使用して、イベントおよびリソースをマップ上で確認します。

**「マイ・アクティビティー」ポートレットの設定**

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「マイ・アクティビティー」ポ  
ートレットをカスタマイズできます。

## カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「マイ・アクティビティー」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 53. 「マイ・アクティビティー」ポートレットのカスタマイズ・パラメーター

パラメーター	説明	デフォルト値
デフォルトのヘルプ JSP	ポートレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	ActivitiesPortletHelp
ポートレット・グループ ID	このポートレットが属しているグループの名前。 共通名は、同一ページでのポートレット間の通信をセットアップします。 例えば、共通名によって「マイ・アクティビティー」ポートレットと「詳細」ポートレットの間の通信をセットアップできます。	default
ポートレットの高さ	ポートレットの標準的な高さを示すピクセル数。	200
ポートレットの最大の高さ	ポートレットの最大の高さを示すピクセル数。	600
ポートレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、タイトルはソリューションによって提供され、「マイ・アクティビティー」が表示されます。
リソース・バンドル	プロパティの値 (ポートレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。 この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。 リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。

### 関連概念:

314 ページの『マイ・アクティビティー』

「マイ・アクティビティー」ポートレットには、インターフェースにログオンしているユーザーがメンバーとして所属するグループが所有するアクティビティーの動的なリストが表示されます。

## 「通知」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「通知」ポートレットをカスタマイズできます。

## カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「通知」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 54. 「通知」ポートレットのカスタマイズ・パラメーター

パラメーター	説明	デフォルト値
--------	----	--------

表 54. 「通知」ポータルレットのカスタマイズ・パラメーター (続き)

列	リストに表示される列の仕様および順序	[{"id": "notifications.HEADLINE"}, {"id": "notifications.SENTFROM"}, {"id": "notifications.SENTTIME", "width": "10", "format": "yyyy-MM-dd HH:mm:ss"}]
デフォルトのヘルプ JSP	ポータルレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	CityCoordinatorPortletHelp
ツールバーの非表示	ポータルレットの上部にツールバーを表示するかしないかを定めるための true または false の設定。	true
ポータルレットの高さ	ポータルレットの標準的な高さを示すピクセル数。	200
ポータルレットの最大の高さ	ポータルレットの最大の高さを示すピクセル数。	600
ポータルレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、タイトルはソリューションによって提供され、「通知」が表示されます。
リソース・バンドル	プロパティの値 (ポータルレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。

注: リソース・バンドルを指定した場合にポータルレット・タイトルがどうなるかに関する説明は、同じリソース・バンドルがソースとなっている列タイトルについても適用されます。

## Columns パラメーター

**columns** パラメーターの値は、表 55 の説明に従って構成できる、JSON オブジェクトの配列です。

表 55. 「通知」ポータルレットの *columns* パラメーター値内部のオブジェクト

オブジェクト	内容
id	列を表示することを示す列 ID。
width	列の幅を示すピクセル数。
format	日時列に使用する形式を表す文字列。この項目は、 <b>sysprop</b> テーブル内の設定をオーバーライドします。
sortAscending	<ul style="list-style-type: none"> <li>• true の場合、列項目に対して昇順のソート順を使用します。</li> <li>• false の場合、列項目に対して降順のソート順を使用します。</li> </ul>

表 55. 「通知」ポートレットの `columns` パラメーター値内部のオブジェクト (続き)

オブジェクト	内容
<code>sortPriority</code>	<ul style="list-style-type: none"> <li>すべての列の中での、その列のソート優先順位を示す番号。番号が若いほど、優先順位は高くなります。</li> <li>値なしで空白のままの場合、列のデフォルトのソート優先順位を使用します。</li> <li>-1 の場合、列のデフォルトのソート優先順位を使用不可にします。</li> </ul>
<code>title</code>	列見出しのタイトル。デフォルトの見出しタイトルを使用する場合は、空白のままにします。

列は、`columns` パラメーターの値を形成する JSON オブジェクトに指定されたのと同じ順序でポートレットに表示されます。この値以内に指定された列 ID を持つ列のみが表示され、その他の列はすべて非表示になります。`columns` パラメーターの値を省略すると、177 ページの表 54 の 1 行目に示されているデフォルトの設定に従って、列が表示されます。

列 ID に指定可能な値を 表 56 に示します。

表 56. 「通知」ポートレットに有効な列 ID

列 ID	説明
<code>notifications.ID</code>	通知テーブルの通知に指定された UUID
<code>notifications.CATEGORY</code>	通知に関連するイベントまたは KPI のカテゴリーの未変換の値
<code>notifications.SENTFROM</code>	通知を生成したサービス
<code>notifications.SENTTOGROUP</code>	通知にアクセスできるグループのリスト
<code>notifications.SENTTIME</code>	通知を送信したサービスによって生成された時刻
<code>notifications.HEADLINE</code>	通知を説明する短いテキスト
<code>notifications.DESCRPTION</code>	通知を説明する詳細なテキスト
<code>notifications.ALERTLINK</code>	通知に関連する CAP アラートのリスト
<code>notifications.KPILINK</code>	通知に関連する KPI

#### 関連概念:

316 ページの『通知』

「通知」ポートレットを使用して、アラート・メッセージとその詳細を表示します。

## 「レポート」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「レポート」ポートレットをカスタマイズできます。

### カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 57. 「レポート」ポートレットのカスタマイズ・パラメーターの値

パラメーター	説明	デフォルト値
--------	----	--------

表 57. 「レポート」ポートレットのカスタマイズ・パラメーターの値 (続き)

デフォルトのヘルプ JSP	ポートレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	ReportsIntegrationPortletHelp
ポートレットの高さ	ポートレットの標準的な高さを示すピクセル数。	600
ポートレットの最大の高さ	ポートレットの最大の高さを示すピクセル数。	800
ポートレットのタイトル	「レポート」ポートレットのタイトル。	Custom Report
レポート URL	表示されるレポートの URL を指定します。	http://ioc1bvtlite1.rtp.raleigh.ibm.com/cognos/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run&ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_cap_model%27%5d%2ffolder%5b%40name%3d%27reports%27%5d%2ffolder%5b%40name%3d%27User_defined_reports%27%5d%2freport%5b%40name%3d%27User_defined_report%27%5d&ui.name=User_defined_report&run.outputFormat=&run.prompt=true&cv.toolbar=false&cv.header=false
リソース・バンドル	プロパティの値 (ポートレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。リソース・バンドルを指定しない場合、キーの探索は行われず、「共有設定」ウィンドウのポートレットのタイトル・フィールドに示されているタイトルが表示されます。	デフォルトのリソース・バンドルはありません。
ページ上での URL フィールドの表示	「レポート」ポートレット・ページに「レポート URL」ボタンを組み込むには、「True」を選択します。このボタンによって、管理者だけでなく、すべてのユーザーがカスタム・レポートの作成とレポート URL の設定を実行できるようになります。「レポート」ポートレット・ページから「レポート URL」ボタンを削除するには、「False」を選択します。	False



## 関連概念:

318 ページの『レポート』

「レポート」ポートレットでは、イベントのレポートをグラフとして表示することができます。このポートレットは、イベントのグループ化の基準となる各種のオプションを提供します。さらに、特定の日付または日付範囲を指定してイベントを選択することができます。レポートは、現在および将来のイベントへの対応について計画を策定するのに役立ちます。

## 「サンプル・パブリッシャー」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「サンプル・パブリッシャー」ポートレットをカスタマイズできます。

## カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「サンプル・パブリッシャー」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 58. 「サンプル・パブリッシャー」ポートレットのカスタマイズ・パラメーター

パラメーター	説明	デフォルト値
デフォルトのヘルプ JSP	ポートレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	SamplePublisherPortletHelp
ポートレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、タイトルはソリューションによって提供され、「サンプル・パブリッシャー」が表示されます。
リソース・バンドル	プロパティの値 (ポートレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。

## 関連概念:

115 ページの『サンプル・パブリッシャー』

「サンプル・パブリッシャー」ポートレットでは、共通アラート・プロトコル (CAP) イベントを IBM Intelligent Operations Center にパブリッシュすることができます。

## 「標準操作手順」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「標準操作手順」ポートレットをカスタマイズできます。

## カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「標準操作手順」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 59. 「標準操作手順」ポートレットのカスタマイズ・パラメーター

パラメーター	説明	デフォルト値
--------	----	--------

表 59. 「標準操作手順」ポートレットのカスタマイズ・パラメーター (続き)

デフォルトのヘルプ JSP	ポートレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	SOPManagerPortletHelp
ポートレットの高さ	ポートレットの標準的な高さを示すピクセル数。	440

#### 関連概念:

143 ページの『標準操作手順』

標準操作手順およびアクティビティーを定義することで、IBM Intelligent Operations Center で受信するイベントを管理できます。「標準操作手順」ポートレットを使用して、Tivoli Service Request Manager で、標準操作手順、標準操作手順の選択マトリックス、およびワークフロー・デザイナーの各アプリケーションにアクセスします。

### 「状況」ポートレットの設定

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「状況」ポートレットをカスタマイズできます。

### カスタマイズ・パラメーター

「共有設定」ウィンドウのフィールドには、「状況」ポートレットのカスタマイズ・パラメーターの値が入力されています。カスタマイズ・パラメーターについては、以下の表で説明します。

表 60. 「状況」ポートレットのカスタマイズ・パラメーター

パラメーター	説明	デフォルト値
カスタム KPI 色	KPI の状況を示すためにポートレットで使用される色。例えば、以下のように入力できます。 <pre>{"acceptable": "#7f7f7f", "take_action": "#343333"}</pre> ここで入力した色は、ソリューションによって提供される色をオーバーライドします。	{}
デフォルトのヘルプ JSP	ポートレットのメニューからヘルプが選択されたときに表示される JSP ヘルプ・ファイルの名前。	KpiStatusPortletHelp
KPI フィルターの有効化	<b>KPI filter</b> パラメーター値の情報に従って、ポートレットについて追加の KPI フィルターを有効または無効にするための、true または false の設定。	false
KPI フィルター	ポートレットについて「KPI フィルターの有効化」を true に設定したときに表示される、KPI の ID。例えば以下のようになります。 <pre>["Transportation", "Airports", "Roads_and_Traffic", "Public_Safety", "Fire_Department", "Water", "Delayed_Flights", "Delayed_Flights_Airport_Two"]</pre>	[]
ポートレット・グループ ID	このポートレットが属しているグループの名前。共通名は、同一ページでの「重要業績評価指標のドリルダウン」ポートレットと「状況」ポートレットの間の通信をセットアップします。	default
ポートレットの高さ	ポートレットの標準的な高さを示すピクセル数。	200
ポートレットの最大の高さ	ポートレットの最大の高さを示すピクセル数。	600

表 60. 「状況」ポートレットのカスタマイズ・パラメーター (続き)

ポートレットのタイトル	ソリューションによって提供されるタイトルをオーバーライドするタイトル。	このパラメーターに値を入力しなかった場合、タイトルはソリューションによって提供され、「状況」が表示されます。
リソース・バンドル	プロパティの値 (ポートレット・タイトルなど) のソースとして提供するリソース・バンドルの場所。この場所は、提供するリソース・バンドル内のプロパティ・キーとしてタイトルを指定する場合に必要です。リソース・バンドルを指定しない場合、キーの探索は行われず、ソリューションによって提供されるタイトルが表示されます。	デフォルトのリソース・バンドルはありません。
凡例の表示	ポートレットに凡例を表示するかしないかを定めるための true または false の設定	true
ソート順	KPI リストをソートするときに使用される KPI プロパティ。デフォルトでは、KPI 名の英字の昇順でソートします。その他のオプションは、kpi.CURRENT.VALUE、kpi.CURRENT.STATUS、および kpi.CALCULATION.TIME です。	+kpi.NAME

#### 関連概念:

321 ページの『状況』

「状況」ポートレットでは、単独または複数の組織の重要業績評価指標 (KPI) の状況を確認することができます。

## ポートレット・ヘルプのカスタマイズ

IBM Intelligent Operations Center ポートレット用に代替ヘルプをデプロイすることができます。

### このタスクについて

各ポートレットの使用に関するヘルプについては、ポートレットの右上隅をクリックし、表示されるメニューから「ヘルプ」を選択します。

ポートレットに表示されるレイアウトまたはデータを変更した場合、表示されるヘルプの変更も必要ことがあります。

### 手順

1. 代替ヘルプを JSP ファイルとして作成します。
2. ファイルには任意の名前を付けることができますが、ご使用の言語に対応する正しい接尾部を使用する必要があります。言語設定は、ブラウザの言語に基づいています。ご使用の言語の標準ロケール ID を使用してください。例えば、以下のようになります。

オプション	説明
_pt_BR	ブラジル・ポルトガル語
_en	英語
_fr	フランス語
_de	ドイツ語

オプション	説明
_es	スペイン語

3. ポートレットの「共有設定」ウィンドウを使用して、**DefaultHelpJSP** パラメーターを代替ヘルプ・ファイル名と共に設定します。言語接尾部も .jsp ファイル拡張子も含めないでください。
4. 代替ヘルプ JSP ファイルを正しいロケーション (/opt/IBM/WebSphere/wp\_profile/installedApps/cell1/ioc\_portal\_ear.ear/portlet\_war/portlet\_root/jsp/html/help) にコピーします。 *portlet\_war* 変数および *portlet\_root* 変数のポートレットごとの値は、別々のトピックに記載されています。これらの値のリストについては、このトピックの末尾にあるリンクを参照してください。

注: ユーザー権限サマリーのヘルプ・ファイルを変更する際には、このステップで示されたパス内で *ioc\_portal\_ear.ear* を *iss\_portal\_ear.ear* に置き換えます。

## 次のタスク

デフォルトの言語を含むすべてのサポートされる言語について、代替ヘルプ・ファイルの翻訳を提供してください。

### 関連情報:

 IBM WebSphere Portal 7 の製品資料

## ポートレット・ヘルプ・ファイルのロケーション

デフォルトのポートレット・ヘルプを代替 JSP ヘルプ・ファイルに置き換える場合、ポートレットごとにロケーション値を指定する必要があります。

表 1 および表 2 に、ユーザー・ポートレットのヘルプ・ファイルおよび管理ポートレットのヘルプ・ファイルのロケーションの値を示します。

表 61. ユーザー・ポートレットでの代替ヘルプ・ファイルのロケーションの値

ポートレット	<i>portlet_war</i>	<i>portlet_root</i>
詳細	icoc_ui_common_events_portlet.war	_icoc_ui_common_events_portlet
重要業績評価指標のドリルダウン	icoc_ui_kpi_drilldown_portlet.war	_icoc_ui_kpi_drilldown_portlet
ロケーション・マップ	icoc_ui_location_map_portlet.war	_icoc_ui_location_map_portlet
マップ	icoc_ui_navigator_portlet.war	_icoc_ui_navigator_portlet
マイ・アクティビティ	icoc_ui_activities_portlet.war	_icoc_ui_activities_portlet
通知	icoc_ui_city_coordinator_portlet.war	_icoc_ui_city_coordinator_portlet
レポート	icoc_ui_reports_portlet.war	_icoc_ui_reports_portlet
状況	icoc_ui_kpi_status_portlet.war	_icoc_ui_kpi_status_portlet

表 62. 管理ポートレットでの代替ヘルプ・ファイルのロケーションの値

ポートレット	<i>portlet_war</i>	<i>portlet_root</i>
管理コンソール	icoc_ui_administration_console_portlet.war	_icoc_ui_administration_console_portlet
イベント・スクリプト記述	icoc_ui_event_scripting_portlet.war	_icoc_ui_event_scripting_portlet
重要業績評価指標	icoc_ui_kpi_manager_portlet.war	_icoc_ui_kpi_manager_portlet

表 62. 管理ポータルでの代替ヘルプ・ファイルのロケーションの値 (続き)

ポータル	<i>portlet_war</i>	<i>portlet_root</i>
ロケーション・マップ・マネージャー	icoc_ui_location_map_manager_portlet.war	_icoc_ui_location_map_manager_portlet
サンプル・パブリッシャー	icoc_ui_sample_publisher_portlet.war	_icoc_ui_sample_publisher_portlet
標準操作手順	icoc_ui_sop_manager_portlet.war	_icoc_ui_sop_manager_portlet
ユーザー権限サマリ	iss_ui_security_portlet.war	_iss_ui_security_portlet

## KPI のカスタマイズ

IBM Intelligent Operations Center では、ビジネス・プロセスに適合するよう重要業績評価指標 (KPI) モデルをカスタマイズできます。

KPI は、トレンドを分析したり問題領域を示したりするために使用できる統計データを提供するように設計されています。KPI データは、IBM Intelligent Operations Center 内部のイベントによって更新されます。

IBM Intelligent Operations Center には、KPI 状況の更新に使用できる KPI およびイベントのサンプル・セットがあります。IBM Intelligent Operations Center には、公共の安全、輸送、および水道のモニター・プロセスとビジネス・プロセスに基づく、以下の 3 つのサンプル KPI モデルが用意されています。IBM Intelligent Operations Center に用意されているサンプル KPI について詳しくは、このトピックの末尾にあるリンクに従ってください。

IBM Intelligent Operations Center の各ソリューションの前に、特定のビジネス環境に必要な KPI をセットアップするための KPI 作成および統合プロセスを示します。IBM WebSphere Business Monitor を使用して、ユーザー独自の KPI モデルを作成することもできます。IBM Intelligent Operations Center を使用して KPI を作成および統合する方法について詳しくは、このトピックの末尾にあるリンクに従ってください。

「重要業績評価指標」ポータルを使用して、IBM Intelligent Operations Center 内で KPI をカスタマイズします。「重要業績評価指標」ポータルは、ソリューション・カスタマイズ・ツールのオプションの 1 つとして管理者に提供されます。

このポータルを使用して、KPI のプロパティーの表示、KPI の作成、コピー、または変更、および KPI モデルの階層表示を表示または変更することができます。

「**KPI 定義**」タブを使用して、IBM Intelligent Operations Center の特定の KPI モデルに関連付ける KPI を定義します。

- KPI モデルに所属する KPI の現行リストを表示する。
- 既存の KPI のプロパティーを表示する。
- 既存の KPI のプロパティーを更新する。
- KPI モデル用の新規 KPI を作成する。
  - 定義済みのメトリックを使用して、計算された KPI を集約する。
  - 他の KPI に基づいて KPI 値を表す。
- KPI を削除する。

更新は、IBM Intelligent Operations Center データベースに格納されている IBM WebSphere Business Monitor モデルに保存されます。また、更新は「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットを次回最新表示するときにも反映されます。

「**KPI 表示階層 (KPI Display Hierarchy)**」タブを使用して、「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットに表示される KPI 階層を更新します。

- 既存の KPI 階層を表示する。
- KPI のメイン・プロパティを表示する。
- KPI 階層内の項目を移動または削除して、ツリー構造を変更する。
- 事前に定義された KPI を階層に追加する。

更新は、「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットを次回最新表示するときにも反映されます。

注: 表示階層に対する変更は、KPI モデルからは独立したものであり、KPI モデルのロジックに従った更新にするためには、KPI モデルについて把握しておく必要があります。

#### 関連概念:

123 ページの『KPI の作成および統合』

重要業績評価指標 (KPI) モデルは、ビジネス・モニター開発ツールキットおよび KPI 管理ポートレットを使用して作成および変更することができます。

136 ページの『サンプル KPI』

IBM Intelligent Operations Center では、サンプル KPI が提供されています。このサンプル KPI は、IBM WebSphere Business Monitor 開発ツールキットを使用してさまざまなタイプの KPI を実装するためのガイダンスを提供するように設計されています。水道、輸送、および公共安全用のサンプル・モニター・モデルが提供されています。

## 重要業績評価指標

「重要業績評価指標」ポートレットでは、IBM Intelligent Operations Center の重要業績評価指標 (KPI) およびそれらの階層表示をカスタマイズすることができます。

「重要業績評価指標」ポートレットでは、KPI を表示、変更、コピー、作成、および削除することができます。また、「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットに表示される KPI 階層をカスタマイズすることもできます。

「重要業績評価指標」ポートレットにアクセスするには、WebSphere Portal 管理インターフェースで「**Intelligent Operations**」 > 「**カスタマイズ・ツール**」 > 「**重要業績評価指標**」をクリックします。

### KPI 階層の表示

「**関係と表示**」タブを使用して、「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットで表示されるとおりの形で、KPI モデルを表示することができます。

#### このタスクについて

「**関係と表示**」ウィンドウの左側には、表示する権限のある KPI 階層について、ルート・レベルのノードのリストが表示されます。それらのノードは、「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットで表示されるとおりの形で、KPI モデルを表しています。



## 手順

1. ルート・レベルのノードを展開して、確認する下位のモデルのツリーを表示します。
2. ルート・レベルのノードのタイトルをクリックして、ウィンドウの右側に表示される詳細をプレビューします。表示される情報について以下の表で説明します。

オプション	説明
名前	ルート・レベルのノードのタイトル。
タイプ	ルート・レベルのノードのタイプ
モデル ID	対応する KPI モデルの ID。
カテゴリー	モデルの種別
アイコン	ルート・レベルのノードを表すアイコン

3. KPI をクリックして、「関係と表示」ウィンドウの右側に表示される詳細をプレビューします。

## KPI 階層の変更

「関係と表示」タブを使用して、「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットで表示されるとおりの形で、KPI モデルを変更または削除することができます。

## 手順

1. 「関係と表示」ウィンドウの左側で、ルート・レベルのノードおよびサブ項目をクリックして、目的のレベルまで階層ツリーを展開します。
2. 既存の項目は、以下のようにして、移動、追加、変更、または削除することができます。
  - ツリー内のサブ項目を移動するには、その項目を目的の位置までドラッグします。緑色または赤色のインディケータは、移動が許可されているかどうかを示します。
  - KPI モデルの既存のサブ項目のリストからツリーに項目を追加するには、サブ項目に含める項目を右クリックして「**KPI の追加**」をクリックします。
  - 「**KPI プロパティ**」ウィンドウに移動してサブ項目を変更するには、その項目を右クリックして「**編集**」をクリックします。
  - ルート・レベルのノードまたはサブ項目をツリーから削除するには、その項目を右クリックしてから「**除去**」をクリックします。ルート・ノード項目を削除すると、その項目に含まれているすべてのサブ項目が削除されます。
3. 「**保存**」をクリックして、更新内容を保存します。

注: ここでは、所有する組織の名前やルート・レベルのノードの名前を編集することはできません。所有する組織を変更する場合は、それを削除して別の名前に置き換えます。

## 所有する組織の追加

「関係と表示」タブを使用して、「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットに表示するルート・レベルのノードを追加することができます。

## 手順

1. 「関係と表示」ウィンドウの左上で「**所有する組織の追加**」をクリックします。
2. 表示名を入力します。
3. 「**モデル**」フィールドのドロップダウン・リストで、追加するルート・レベルのノードを選択します。
4. 「**カテゴリー**」フィールドのドロップダウン・リストで、ルート・レベルのノードのカテゴリーを選択します。

- 「アイコン」フィールドのドロップダウン・リストで、ルート・レベルのノードを表すアイコンのファイル名を選択します。
- 「OK」をクリックします。新規ノードが「関係と表示」ウィンドウの左側に追加されます。
- 「保存」をクリックします。「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットの表示内容が更新されます。

## KPI の凡例の変更

「関係と表示」タブを使用して、「状況」ポートレットの KPI の凡例を変更することができます。

### 手順

- 「関係と表示」ウィンドウの左上で「KPI 凡例」をクリックします。
- 以下のようにして、KPI の凡例の表示を変更します。
  - 範囲を追加するには、「行の追加」をクリックします。
  - 範囲を変更するには、「範囲名」、「色」、および「アイコン」の下にある各フィールドを編集します。
  - 範囲を削除するには、「削除」をクリックします。
- 「OK」をクリックします。「状況」ポートレットおよび「重要業績評価指標のドリルダウン」ポートレットの表示内容が更新されます。

## KPI モデルの表示

「KPI 定義」タブを使用して、IBM Intelligent Operations Center の KPI モデルに属している KPI を表示することができます。

### 手順

「モデル別フィルター」フィールドには、表示する権限のあるビジネス・プロセス・モデルのドロップダウン・リストが表示されます。すべてのモデルを選択するか、または KPI を表示するモデルを選択します。表示される KPI 情報について以下の表で説明します。

オプション	説明
KPI 名	KPI のタイトル。 KPI 名をクリックすると、プロパティを確認することができます。
モデル	KPI が属しているモデルの名前。
作成済み	KPI の作成方法 <ul style="list-style-type: none"> <li>モデル化された KPI とは、IBM WebSphere Business Monitor を使用してモデル・レベルで作成された KPI です。</li> <li>ダッシュボード KPI とは、「重要業績評価指標」ポートレットを使用して作成された KPI です。</li> </ul>
タイプ	KPI の種類 <ul style="list-style-type: none"> <li>集約 KPI は、選択されたメトリックと集約方式に基づく値を使用します。</li> <li>式 KPI は、ユーザーが定義した XPath 式を使用して、他の KPI やユーザー定義関数に基づく値を使用します。</li> </ul>

オプション	説明
アクセス	<p>KPI のアクセス・レベル</p> <ul style="list-style-type: none"> <li>共有 KPI とは、それを表示するアクセス権限を他のユーザーが持っている KPI です。</li> <li>プライベート KPI とは、所有者以外のユーザーと共有できない KPI です。</li> </ul>

## KPI の表示または変更

「**KPI 定義**」タブを使用して、IBM Intelligent Operations Center のモデルに属している既存の KPI を表示または変更することができます。

### 手順

1. KPI を選択します。「**KPI 定義**」ウィンドウの左上で「**編集**」をクリックします。「**KPI プロパティ**」ウィンドウが開きます。
2. KPI を変更するには、「プロパティ」ウィンドウのタブのフィールドを編集します。これらのフィールドを編集して集約 KPI や式 KPI を作成する方法については、このトピックの末尾にあるリンクをクリックして参照してください。

注: ここでは、モデル化された KPI の定義を変更することはできません。

3. 更新された「**KPI プロパティ**」を保存してウィンドウを終了するには、「**OK**」をクリックします。KPI をコピーして、それを保存してから変更を続行するには、「**適用**」をクリックします。保存せずに終了するには、「**キャンセル**」をクリックします。

## KPI のコピー

「**KPI 定義**」タブを使用して、IBM Intelligent Operations Center のモデル用に既存の KPI をコピーすることができます。

### 手順

1. KPI を選択します。「**KPI 定義**」ウィンドウの左上で、「**追加のアクション**」 > 「**コピー**」をクリックします。「**KPI プロパティ**」ウィンドウが開きます。
2. 「**KPI 名**」フィールドに、新規 KPI 名を入力します。
3. KPI の変更手順のステップ 3 および 4 に従って、コピーした KPI のプロパティを編集します。

## KPI の作成

「**KPI 定義**」タブを使用して、IBM Intelligent Operations Center のモデル用に KPI を作成することができます。

### 手順

1. 「**KPI 定義**」ウィンドウの左上で「**作成**」をクリックします。
2. 「**新規集約 KPI**」または「**新規式 KPI**」をクリックします。「**KPI プロパティ**」ウィンドウが開きます。
3. KPI の変更手順のステップ 3 および 4 に従って、新規 KPI のプロパティを編集します。

## 次のタスク

KPI の作成について詳しくは、このトピックの末尾にある IBM Websphere Business Monitor 資料のリンクを参照してください。

## サンプル KPI

ソリューションには、一連のサンプル KPI が付属しています。こうした KPI は、さまざまなタイプの KPI をユーザーの組織に合わせて計画および実装する際の手引きとなるように設計されています。水道、輸送、公共安全の各分野のサンプルが用意されています。

### 「重要業績評価指標」ポートレットのカスタマイズ

このポートレットはカスタマイズすることができます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

#### 関連概念:

321 ページの『状況』

「状況」ポートレットでは、単独または複数の組織の重要業績評価指標 (KPI) の状況を確認することができます。

304 ページの『重要業績評価指標のドリルダウン』

KPI カテゴリと、そのカテゴリの基礎となる KPI の状況に関する追加の情報を表示するには、「重要業績評価指標のドリルダウン」ポートレットを使用します。

#### 関連資料:

171 ページの『「重要業績評価指標」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「重要業績評価指標」ポートレットをカスタマイズできます。

#### 関連情報:



IBM WebSphere Business Process Management バージョン 7.0 インフォメーション・センター

## KPI をカスタマイズする前にバックアップする

IBM WebSphere Business Monitor を使用して、または「重要業績評価指標」ポートレットを使用して作成または変更された KPI を、バックアップおよび復元します。

### このタスクについて

KPI モデルのカスタマイズおよび KPI の変更を行う前に、既存のモデルをバックアップするとよいでしょう。このトピックの手順は、指定されたモデルのすべての KPI を、指定されたファイルにエクスポートし、指定されたファイルから指定されたモデルに KPI をインポートします。

### 手順

1. アプリケーション・サーバーにログオンします。
2. IBM WebSphere Business Monitor プロファイルの bin ディレクトリー (/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin) に移動します。
3. KPI をエクスポートするには、以下のコマンドを実行します。

```
./wsadmin.sh -wsadmin_classpath
"../../../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../../../plugins/
com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../../../scripts/wbm/kpi/exportKpis.jy"
"xml_file_path" model_ID model_version ALL
```

*xml\_file\_path* は、KPI のエクスポート先の XML ファイルの名前およびパスです。*model\_ID* および *model\_version* は、KPI のエクスポート元の KPI モデルの ID およびバージョンです。

4. KPI をインポートするには、以下のコマンドを実行します。./wsadmin.sh -wsadmin\_classpath  
"../../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:../../../../plugins/  
com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../../scripts/wbm/kpi/importKpis.jy"  
"xml\_file\_path"

xml\_file\_path は、KPI のインポート元の XML ファイルの名前およびパスです。

## 例

モデル icoc\_sample\_public\_safety\_monitor\_model からすべての KPI を /tmp/kpis.xml にエクスポートするには、以下のコマンドを実行します。コマンドで、xml\_file\_path の値は /tmp/kpis.xml、model\_ID の値は icoc\_sample\_public\_safety\_monitor\_model、model\_version の値は 2011-02-18T10:49:46 です。

```
./wsadmin.sh -wsadmin_classpath "../../../../plugins/com.ibm.wbimonitor.lifecycle.spi.jar:  
../../../../plugins/com.ibm.wbimonitor.repository.jar" -lang jython -f "../../../../scripts/wbm  
/kpi/exportKpis.jy" "/tmp/kpis.xml" icoc_sample_public_safety_monitor_model  
2011-02-18T10:49:46 ALL
```

詳しくは、トピックの末尾にある WebSphere Business Monitor インフォメーション・センターのリンクを参照してください。

### 関連資料:

287 ページの『データのバックアップ』

IBM Intelligent Operations Center 内の重要なデータの損失を防ぐため、特定のファイル、ディレクトリ、データベースを一定の間隔でバックアップしてください。

### 関連情報:



IBM Smarter Cities Software Solutions Redbooks

---

## イベント関連のカスタマイズ

このセクションでは、イベント関連について説明し、新規デシジョン・テーブルの変更方法と作成方法を説明します。また、ルール・アプリケーションについても説明します。

## イベント関連およびルール・アプリケーション

このトピックでは、イベント関連プロセスの概要を示し、ルール・アプリケーションについて簡潔に説明します。

WebSphere Operational Decision Management にベースを置くイベント関連ルール・アプリケーションを使用することで、IBM Intelligent Operations Center または WebSphere Operational Decision Management の高度な技術的知識が無くても関連ルールを変更および拡張することができます。ただし、共通アラート・プロトコル イベントおよび WebSphere Operational Decision Management の基本的な知識は必要です。

ソース・イベント、ターゲット・イベント、およびデシジョン・テーブルの 3 つの変数によって、イベントがどのように関連するかが決まります。

共通アラート・プロトコル・イベントが着信するたびに、既存のイベントのいずれかがその着信イベントと関連しているかどうかを判断するために、ルール・アプリケーションが呼び出されます。ソース・イベントは、常に新規着信イベントであり、関連をトリガーします。関連プロセスは、ソース・イベントをデータベース内のイベントと照合します。ソース・イベントと関連するイベントがデータベース内で検出された場合、このイベントはターゲット・イベントと呼ばれます。潜在的な関連が検出された場合はいつでも、「通知」ポートレットがアラートを送信します。

判別は単一方向で行われます。 相関を判別するルールは対称である必要がないため、この概念は重要です。 例えば、イベント A がイベント B と相関する場合、それはイベント B がイベント A と相関することを意味するわけではありません。

ルール・アプリケーションは、要件に最も適合するサンプル相関表を 1 つ提供します。 相関ルールをカスタマイズするさまざまな方法については、『イベント相関設定のカスタマイズ』を参照してください。

## イベント相関設定のカスタマイズ

このセクションでは、イベント相関の設定をカスタマイズする方法について説明します。

デシジョン・テーブル (Decision Center で編集できます) には、2 つのタイプの列があります。 左側の列は、決定列と呼ばれます。 この列は、右側のどのアクション列を使用するかを決定します。 デシジョン・テーブルは、異なる行の値に応じて左から右へチェックされ、右側のアクション列まで進みます。 アクション列は、特定の行に到達したときに何が実行されるかを定義します。

イベント相関設定を拡張および変更する方法として推奨されるのは、既存のデシジョン・テーブルを編集する方法です。 以下の項目では、デシジョン・テーブルのフォーマット設定方法を説明します。

- デシジョン・テーブルの左側 (背景が白) に決定列があります。 これは、アクション列 (背景がグレー) 内のどの列を実行するかを決定します。
- テーブル内の最後のアクション列は、照会およびパブリケーション・サービスを呼び出します。 相関照会およびパブリケーションとして必要としないアクション行がある場合、この最後の列でその項目を非アクティブにします。
- アクション列内の「SQL 照会の設定 (set SQL Query)」列は、照会パラメーターをオーバーライドすることができます。 照会パラメーターのオーバーライドは煩雑であり、ほとんどのアプリケーションで必要ありません。 この照会の要件は、照会結果に以下の 3 つの名前付きの列が含まれていることです。
  - event\_headline - 相関の説明で使用されるタイトル。 このテキストは、通知の説明となります。
  - event\_external\_id - イベントの外部 ID (CAP-ID など)
  - event\_internal\_id - 通知プロパティの「アラートへの参照」フィールドの見出しにマップするために「通知」ポートレットが使用する内部 ID (CapAlertId など)。

このセクションには、以下のトピックが含まれています。

### 決定プロパティの変更

WebSphere Operational Decision Management で Decision Center ユーザー・インターフェースを使用して、イベント相関設定を変更します。 このトピックでは、デシジョン・テーブルでの決定プロパティの変更について詳しく説明します。 WebSphere Operational Decision Management 資料へのリンクも記載しています。

### このタスクについて

ユーザー・インターフェースは、[http://app\\_server:9084/teamservice](http://app_server:9084/teamservice) という URL にあるポータル・サーバーのインストール済み環境のノード 1 にあります。 waswebadmin としてログオンします。

変更のほとんどは、193 ページの『デシジョン・テーブルの編集』で説明されているように、ルール・アプリケーション内で実行できます。 その他の変更には、以下のものに対する変更が含まれることがあります。

- Tivoli Netcool/Impact ポリシー



- 影響ポリシーからのメッセージをメッセージ駆動 Bean 形式に変換する WebSphere Message Broker Java 計算ノード
- クエリー実行可能オブジェクト・モデル (XOM) およびビジネス・オブジェクト・モデル (BOM)

XOM および BOM の変更の詳細と手順、メッセージ・ブローカー・ノード、および Decision Center については、以下のリンクを使用して WebSphere Operational Decision Management インフォメーション・センターと WebSphere Message Broker インフォメーション・センターを参照してください。

#### 関連情報:



IBM WebSphere Operational Decision Management インフォメーション・センター



WebSphere Message Broker 資料

## デシジョン・テーブルの編集

このトピックでは、デシジョン・テーブルを簡潔に説明し、デシジョン・テーブルのプロパティーを変更するためのステップを示します。

IBM Intelligent Operations Center WebSphere Operational Decision Management ルール・アプリケーションでは、イベントのカテゴリおよびタイプを使用して、実行するアクション行を決定する基本相関表が定義されています。

現在、アクション行は同一ですが、要件に適合するように変更することができます。例えば、火災イベントが他のイベントとは異なって扱われ、水道イベントおよびその他の火災イベントのみと相関するように定義することができます。要件に適合するように値を変更するには、その行の「カテゴリ」列のセルをアクティブにして、セルに「Fire, Water」と入力します。イベントとインシデントを区別するためのルールが必要な場合は、適宜、この決定列およびアクション列に行を追加します。

相関イベントの検索の半径を変更するには、「**検索半径の設定 (Set search radius)**」の値を変更します。入力された整数は、ソース・イベントの中央からのメートル数として解釈されます。そのため、2000 と入力した場合、ソース・イベントから 2000 メートルよりも近いイベントのみと相関します。

## デシジョン・テーブルのプロパティーの変更

### 手順

1. `http://app_server:9084/teamserver` に、`rtsadmin`としてログオンします。
2. ブラウザーのエクスペローラーに移動します。
3. 「**capCorrelationRules**」をクリックします。
4. 「**simpleCorrelationPolicy**」をクリックします。
5. 「**編集**」をクリックします。プロパティー・ページが表示されます。
6. プロパティー・ページで「**次へ**」をクリックします。
7. テーブルを編集します。デシジョン・テーブルに追加できる列の例については、テンプレート・フォルダーで提供されているテンプレートを参照してください。
8. テーブルのプロパティーの変更を完了したら、「**終了**」をクリックします。

### 次のタスク

以下の関連リンクを使用して、Decision Center からルール・アプリケーションをエクスポートします。

## 関連タスク:

『IBM Intelligent Operations Center フローへの変更されたルール・セットのデプロイ』  
このトピックを使用して、変更されたルール・セットを Rule Execution Server にデプロイします。

## IBM Intelligent Operations Center フローへの変更されたルール・セットのデプロイ

このトピックを使用して、変更されたルール・セットを Rule Execution Server にデプロイします。

### このタスクについて

デシジョン・テーブルでプロパティまたは項目を変更した場合、変更されたルール・セットを、IBM Intelligent Operations Center 内のイベント・フローにデプロイする必要があります。変更されたルール・セットを Rule Execution Server にデプロイした後は、変更内容に応じて、相関ルールは異なった動作をします。Rule Execution Server は、着信イベントで、潜在的な相関がないかどうかをチェックします。

変更されたルール・セットをデプロイするには、以下のステップを実行します。

### 手順

1. 以下のようにして、Decision Center からルール・アプリケーションをエクスポートします。
  - a. `app_server:9084/teamserver/` に移動します。
  - b. `rtsadmin` としてログオンします。
  - c. 「プロジェクト」 > 「ルール・セットの生成」にナビゲートします。
  - d. 「次へ」をクリックし、何も選択しないで、RuleApp jar ファイルをダウンロードします。
2. 以下のようにして、ルール・アプリケーションを Rule Execution Server にインポートします。
  - a. `app_server:9083/res` に移動します。
  - b. 「エクスプローラー」タブをクリックします。
  - c. 「`icoc_wodm_correlation_ruleApp`」 > 「ルール・セットの追加」をクリックします。
  - d. ルール・セットに名前を付け、新規ルール・セットのパス (`/icoc_wodm_correlation_ruleApp/1.0/yourChosenName/version`) を書き留めます。

各部の意味は、次のとおりです。

- `yourChosenName` は、ルール・セット用に選択した名前です。
- `version` は、ルール・セットのバージョンです。

3. 以下のようにして、Impact ポリシーでルール・セットの新しいパスを設定します。
  - a. `event_server:9080/nci/login_main.jsp` に移動します。
  - b. 左側のドロップダウン・メニューから、IBM Intelligent Operations Center を選択します。
  - c. 「ポリシー」をクリックし、「`IOC_Event_Correlation`」ポリシーを選択します。
  - d. `JMSProps.ilog_rules_bres_mdb_rulesetPath` フィールドの値を、新しいパス `/icoc_wodm_correlation_ruleApp/1.0/yourChosenName/version` に変更します。

各部の意味は、次のとおりです。

- `yourChosenName` は、ルール・セット用に選択した名前です。
  - `version` は、ルール・セットのバージョンです。
- e. 「保存」をクリックします。

## 関連タスク:

193 ページの『デシジョン・テーブルのプロパティの変更』

---

## ロケーション・マップ・マネージャー

「ロケーション・マップ・マネージャー」ポートレットでは、「ロケーション・マップ」ポートレットをカスタマイズすることができます。

「ロケーション・マップ」ポートレットでカスタマイズできる対象は以下のとおりです。

- ポートレットの左側のメニューに表示される種別名。
- ポートレットに表示されるマップ。
- マップ内のエリア。

マップ内のエリアは、エリア ID コードで識別されます。エリア ID コードを持つイベントは、そのエリアが定義されているすべてのロケーション・マップに表示されます。

エリアに親 ID を付けることも可能です。親 ID を使用してエリアの階層を作成できます。例えば、スポーツ・スタジアムの 1 階の観客席を表すエリアを作成します。各席は、スタジアム 1 階の詳細なロケーション・マップで定義されます。さらに、各席に親 ID を与えて、その席がスタジアムの 1 階にあることを示します。席の 1 つに与えられているエリア ID を持つイベントは、1 階の席の詳細なマップに表示されます。このイベントは、スタジアムの概要マップにも表示されます。この 1 階のエリア ID は、観客席の親 ID として使用される ID と同じだからです。

「ロケーション・マップ・マネージャー」ポートレットにアクセスするには、WebSphere Portal 管理インターフェースで「Intelligent Operations」>「カスタマイズ・ツール」>「ロケーション・マップ・マネージャー」をクリックします。

## マップ・メニューへの種別の追加

「ロケーション・マップ」ポートレットのマップ・メニューに種別を追加して表示するには、「種別」タブを使用します。

### 手順

1. 「種別名」フィールドに、名前を入力します。必要に応じて説明を追加することもできます。
2. 「送信」をクリックして、種別をポートレットに追加します。

### タスクの結果

「ロケーション・マップ」ポートレットのページを最新表示すると、新規の種別がポートレットに表示されます。

## ポートレットへのマップの追加

「ロケーション・マップ」ポートレットにロケーション・マップを追加して表示するには、「ロケーション・マップ」タブを使用します。

### 手順

1. 「種別名」フィールドに、名前を入力します。ドロップダウン・リストから選択することができます。
2. 「マップ名」フィールドに、ロケーション・マップ名を入力します。必要に応じてマップの説明を追加することもできます。

3. ロケーション・マップの URL を「イメージ」フィールドに入力します。
4. 「送信」をクリックして、マップをメニューに追加します。

## タスクの結果

「ロケーション・マップ」ポートレット・メニューのページを最新表示すると、マップがポートレットに表示されます。これで、マップを選択して表示することができます。

## ロケーション・マップのエリアの追加または変更

「ロケーション・マップ」ポートレットのロケーション・マップに表示されるエリアを新規作成、変更、または削除するには、「エリア」タブを使用します。

### 手順

1. 「マップ名」フィールドに、ロケーション・マップ名を入力します。マップのドロップダウン・リストから選択することができます。
2. 新規エリアをマップ上に描くには、ボックスの右上隅にあるポリゴン・シンボルをクリックします。マップ上で該当の位置をクリックしてから、それぞれの角をクリックしてポリゴンを描きます。ポリゴンの描画を終了するには、ダブルクリックします。デフォルトでは、新規エリアは緑色で表示されます。
3. エリアの詳細を入力するには、ボックスの右上隅にある手形シンボルをクリックします。更新するエリアをクリックします。
4. 「エリア名」フィールドに、エリア・マップ名を入力します。必要に応じて説明を追加することもできます。
5. 「エリア ID」フィールドに、エリア ID を入力します。必要に応じて親エリア ID を追加することもできます。
6. マップ上のエリアを更新するには、「エリアの更新」をクリックします。マップ上のエリアを削除するには、「エリアの除去」をクリックします。
7. 「送信」をクリックして、マップに変更を加えます。

## タスクの結果

「ロケーション・マップ」ポートレットのページを最新表示すると、変更した内容がポートレットに表示されます。

## 「ロケーション・マップ・マネージャー」ポートレットのカスタマイズ

このポートレットはカスタマイズすることができます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

## 関連概念:

305 ページの『ロケーション・マップ』

「ロケーション・マップ」ポートレットでは、ロケーション・マップでマークされているイベントを確認することができます。IBM Intelligent Operations Center のロケーション・マップは、対話用に事前に定義されているエリア (大規模なスポーツ・スタジアムの座席エリアなど) を含むマップまたは計画です。

## 関連資料:

173 ページの『「ロケーション・マップ・マネージャー」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「ロケーション・マップ・マネージャー」ポートレットをカスタマイズできます。

---

## システム全体の構成データの指定

IBM Intelligent Operations Center システム・プロパティ・テーブルは、IBM Intelligent Operations Center の構成データを保管します。

以下は、IBM Intelligent Operations Center が使用するシステム全体のプロパティです。

表 63. IBM Intelligent Operations Center が使用するシステム全体の値

レラム	対象	名前	タイプ	値
システム	*	ActivityCollectionRefreshInterval	Integer	サーバーのコレクション・リフレッシュ・レート (秒)。デフォルトは 300 (5 分) です。このプロパティは、UI サービスでのアクティビティのリフレッシュ・レートに影響します。
システム	*	ActivityProviderEJBNDIName	String	アクティビティ・プロバイダーのリモート・インターフェースの JNDI バインディング名。このインターフェースを通じて、独自のアクティビティ・プロバイダーをデプロイしてプロセスまたはワークフローの管理システムを処理することができます。アクティビティ・プロバイダーは iss_common.jar のアクティビティ・インターフェースを実装する EJB です。
システム	*	AppMonitorPort	String	Tivoli Monitoring が使用する Web ポート。
システム	*	ApplicationServerHostname	String	アプリケーション・サーバーが使用するホスト名または IP アドレス。
システム	*	CollectionRefreshInterval	Integer	サーバーのコレクション・リフレッシュ・レート (秒)。デフォルトは 15 秒です。このプロパティは、UI サービスでのイベントおよび通知のリフレッシュ・レートに影響します。
システム	*	DatabaseServerHostname	String	データ・サーバーが使用するホスト名または IP アドレス。

表 63. IBM Intelligent Operations Center が使用するシステム全体の値 (続き)

レーム	対象	名前	タイプ	値
システム	*	DateFormat	String	IBM Intelligent Operations Center が日付を表示する際に使用される形式。デフォルトは yyyy-MM-dd です。 任意の有効な Java <code>java.text.SimpleDateFormat</code> 日付パターンを指定できます。
システム	*	DateTimeFormat	String	IBM Intelligent Operations Center が日時を表示する際に使用される形式。デフォルトは yyyy-MM-dd HH:mm:ss です。 任意の有効な Java <code>java.text.SimpleDateFormat</code> 日時パターンを指定できます。
システム	*	DisableTSRMSync	Boolean	Tivoli Service Request Manager の同期を無効にするかどうかを指定します。デフォルトは false です。デプロイメントに Tivoli Service Request Manager のインストールが含まれない場合は、true に設定します。
システム	*	EventContainerDeleteEvent	String	Tivoli Netcool/OMNIBus のオブジェクト・サーバー・データベースからイベントを削除するかどうかを指定します。IBM Intelligent Operations Center データベースがイベントによって更新されたときに、Tivoli Netcool/Impact ポリシーによって削除が実施されます。デフォルトは true です。  値が true である場合、イベントはオブジェクト・サーバー・データベースから消去されます。  値が false である場合、イベントはオブジェクト・サーバー・データベースから消去されません。
システム	*	EventRouterPollDelay	Integer	UI ポーリング間隔の遅延 (ミリ秒)。この遅延は、次のポーリング間隔までのミリ秒数です。デフォルトは 0 です。
システム	*	EventRouterPollErrorDelay	Integer	エラー発生後の UI ポーリング間隔の遅延 (ミリ秒)。この遅延は、エラー発生後の次のポーリング間隔までのミリ秒数です。デフォルトは 5000 です。
システム	*	EventRouterTimeout	Integer	UI ポーリング間隔 (秒)。ポーリング間隔は、タイムアウトになる前にイベントをポーリングする時間間隔です。デフォルトは 20 です。
システム	*	EventServerHostname	String	イベント・サーバーが使用するホスト名または IP アドレス。
システム	*	MgmtServerHostname	String	管理サーバーが使用するホスト名または IP アドレス。



表 63. IBM Intelligent Operations Center が使用するシステム全体の値 (続き)

レーム	対象	名前	タイプ	値
システム	*	ModelManagerServerEJBPort	String	Semantic Model Services が使用する EJB ポート。
システム	*	ModelManagerServerHostname	String	Semantic Model Services が使用するホスト名または IP アドレス。
システム	*	MonitorServerHostname	String	IBM WebSphere Business Monitor が使用するホスト名または IP アドレス。
システム	*	MonitorServerWebPort	String	IBM WebSphere Business Monitor REST サービス・ゲートウェイが使用する Web ポート。
システム	*	MonitorServerSecurityEnabled	Boolean	IBM WebSphere Business Monitor への接続で、セキュア HTTP 接続のために SSL を使用するかどうかを指定します。 デフォルトは true です。  値が true である場合、接続で SSL を使用します。  値が false である場合、接続で SSL は使用されません。
システム	*	PortalServerHostname	String	WebSphere Portal Server が使用するホスト名または IP アドレス。
システム	*	PortalServerWebPort	String	WebSphere Portal Server が使用する Web ポート。
システム	*	RegExpEmail	System	E メール・アドレスを検証するために使用される正規表現。 デフォルトは .+ です。
システム	*	RegExpTelephone	System	電話番号を検証するために使用される正規表現。 デフォルトは .+ です。
システム	*	SecurityUserPrefix	String	ユーザーを LDAP 識別名にマップするために使用されるユーザー ID の接頭部。 デフォルトは uid です。
システム	*	SecurityUserSuffix	String	ユーザーを LDAP 識別名またはローカル識別名にマップするために使用されるユーザー ID の接尾部。 デフォルトは ou=users,ou=SWG,o=IBM,c=US であり、LDAP セキュリティーを指定してポータルを実行する場合に使用されます。 LDAP セキュリティーを指定せずにローカル・ポータルを実行する場合は、値を o=defaultWIMFileBasedRealm に設定します。
システム	*	TdsPort	String	Tivoli Directory Server Web Administration Tool が使用する Web ポート。
システム	*	TimeFormat	String	IBM Intelligent Operations Center が時間を表示する際に使用される形式。デフォルトは HH:mm:ss です。 任意の有効な Java <code>java.text.SimpleDateFormat</code> 時間パターンを指定できます。

表 63. IBM Intelligent Operations Center が使用するシステム全体の値 (続き)

レーム	対象	名前	タイプ	値
システム	*	TSRMDirectServerHostname	String	Tivoli Service Request Manager が使用するホスト名または IP アドレス。
システム	*	TSRMDirectServerWebPort	String	Tivoli Service Request Manager が使用する Web ポート。
システム	*	TSRMServerActivityUri	String	Tivoli Service Request Manager が使用するアクティビティーおよびタスク・アプリケーションの URI。 デフォルトは /tsrm/maximo/ui/maximo?event=loadapp&value=Activity&uniqueid={0} です。 {0} はアクティビティー ID の値で置換されます。
システム	*	TSRMServerResourceAddUri		Tivoli Service Request Manager が使用する追加リソース URI。 デフォルトは /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additional=event=INSERT です。 {0} は外部リソース ID の値で置換されます。
システム	*	TSRMServerResourceDeleteUri		Tivoli Service Request Manager が使用する削除リソース URI。 デフォルトは /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additional=event=useqbe&additional=eventvalue=LOCATION={0} です。 {0} は外部リソース ID の値で置換されます。
システム	*	TSRMServerResourcePropertiesUri		Tivoli Service Request Manager が使用するリソース・プロパティー URI。 デフォルトは /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additional=event=useqbe&additional=eventvalue=LOCATION={0} です。 {0} は外部リソース ID の値で置換されます。
システム	*	TSRMServerResourceUpdateUri		Tivoli Service Request Manager が使用する更新リソース URI。 デフォルトは /tsrm/maximo/ui/maximo?event=loadapp&value=plusires&additional=event=useqbe&additional=eventvalue=LOCATION={0} です。 {0} は外部リソース ID の値で置換されます。
システム	*	TSRMServerSecurityEnabled	Boolean	Tivoli Service Request Manager への HTTP 接続で SSL を使用するかどうかを指定します。デフォルトは false です。  値が true である場合、接続で SSL を使用します。  値が false である場合、接続で SSL は使用されません。

表 63. IBM Intelligent Operations Center が使用するシステム全体の値 (続き)

レلم	対象	名前	タイプ	値
システム	*	TSRMServerWorkflowUri	String	Tivoli Service Request Manager が使用するワークフロー URI。デフォルトは /maximo/ui/?event=loadapp&value=sr &&additionalevent=useqbe &additionaleventvalue=TICKETID={0} です。 {0} はインシデント ID の値で置換されます。
システム	*	UseDBModelReader	Boolean	KPI データベース・モデルが RDF ファイルから読み取られるかどうかを指定します。デフォルトは true です。  値が true である場合、KPI モデルは RDF ファイルから読み取られません。  値が false である場合、KPI モデルは RDF ファイルから読み取られます。
システム	*	WebSEALServerHostname	String	Tivoli Access Manager WebSEAL が使用するホスト名または IP アドレス。

以下のプロパティを変更して KPI を処理する方法を構成できます。

表 64. KPI 処理に影響を与えるプロパティ

レلم	対象	名前	タイプ	値
KPI	*	CacheKpis	Boolean	IBM WebSphere Business Monitor から取得された KPI をキャッシュするかどうかを指定します。デフォルトは true です。  値が true の場合は、KPI は再利用のためにキャッシュされます。キャッシュがリフレッシュされる頻度は KpiCacheRefreshInterval で指定されます。  値が false の場合は、IBM Intelligent Operations Center が KPI 情報を要求すると、KPI は常に IBM WebSphere Business Monitor から取得されます。
KPI	*	KpiCacheRefreshInterval	Integer	KPI キャッシュがリフレッシュされる頻度を指定します。間隔は秒単位で指定します。デフォルトは 300 (5 分) です。CacheKpis が false として指定されている場合、KpiCacheRefreshInterval は無視されます。
KPI	*	KpiSentToGroup	String	KPI 通知を受信するグループを指定します。グループ名はセミコロン (;) で区切ります。デフォルト値は CityWideExecutive;CityWideSupervisor です。

表 64. KPI 処理に影響を与えるプロパティ (続き)

レーム	対象	名前	タイプ	値
KPI	*	PreLoadKpis	Boolean	<p>IBM Intelligent Operations Center の始動時に IBM WebSphere Business Monitor から KPI を取得するかどうかを指定します。デフォルトは true です。</p> <p>true の場合は、IBM Intelligent Operations Center の始動時にすべての KPI が IBM WebSphere Business Monitor から取得されます。KPI は再利用のためにキャッシュされます。KpiCacheRefreshInterval はキャッシュがリフレッシュされる頻度を指定します。</p> <p>false の場合は、IBM Intelligent Operations Center が KPI 情報を要求したときのみ、KPI は IBM WebSphere Business Monitor から取得されます。</p> <p>注: PreLoadKpis が true の場合、CacheKpis は指定値に関係なく true であると見なされます。</p>

## システム・プロパティ・テーブルの更新

システム全体の IBM Intelligent Operations Center 構成データを変更するには、システム・プロパティ・テーブルを更新します。

### このタスクについて

VNC クライアントを使用してデータ・サーバーのデータベース・サーバーにログオンし、コマンド・ウィンドウを開きます。以下の手順では、コマンド・ウィンドウにコマンドを入力します。

### 手順

1. root としてデータ・サーバーにログオンします。
2. DB2<sup>®</sup> コントロール・センターを開くには、アクセス制御を一時的にオフにして、以下のコマンドを入力します。

```
xhost +
su - db2inst1
db2cc
```
3. 以下のようにして、DB2 コントロール・センターで、システム・プロパティ・テーブルを開きます。
  - a. DB2 コントロール・センターを開くには、コマンド `db2cc` を入力します。
  - b. DB2 コントロール・センターで、「すべてのデータベース」 > 「IOCDB」 > 「表」 > 「SYSPROP」をクリックします。
  - c. 「SYSPROP」テーブルを右クリックし、「開く」をクリックします。
  - d. 必須フィールドを変更し、「コミット」をクリックします。
  - e. テーブルを閉じます。
4. DB2 コントロール・センターを閉じます。
5. root ユーザーに戻るには、コマンド `exit` を入力します。
6. アクセス制御を再びオンにするには、コマンド `xhost -` を入力します。

注: 加えた変更を実装するには、ポータル・サーバーを再始動する必要があります。 IOCControl スクリプトを使用してポータル・サーバーを再始動することができます。 サービスの開始については、このトピックの末尾にあるリンクを参照してください。

#### 関連タスク:

216 ページの『サービスの開始』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサーバーで実行中のサービスを開始することができます。

---

## レポートを作成するための IBM Cognos Business Intelligence の構成

IBM Intelligent Operations Center は、IBM Cognos® Business Intelligence を使用してレポートの作成と管理を行うレポート作成サブシステムを提供します。 IBM Intelligent Operations Center には、最大 6 つのレポートを表示できるレポート・ページが付属しています。 また、レポート・ページを手動で作成し、ポートレットのレイアウトをカスタマイズすることもできます。

レポート作成サブシステムはアプリケーション・サーバーにインストールされており、分析データ・モデルを使用します。

### 「レポート」ポートレットの作成

このトピックの情報を参照して、IBM Intelligent Operations Center コンソールを使用して既存のポートレットをコピーすることにより、「レポート」ポートレット・ページを作成します。

#### このタスクについて

既存のポートレットをコピーし、プロパティを設定して新規レポート・ページを作成するには、以下のステップを完了します。

#### 手順

1. IBM Intelligent Operations Center に管理者としてログオンします。
2. 「管理」 > 「ポートレット管理 (Portlet Management)」 > 「ポートレット」にナビゲートします。
3. 「検索」フィールドに「レポート」と入力し、「検索」をクリックします。「レポート」ポートレット・ウィンドウが表示されます。
4. コピーするポートレットの横にある「ポートレットのコピー (Copy portlet)」アイコンをクリックします。「ポートレットのコピー (Copy portlet)」ウィンドウが表示されます。
5. 新規ポートレットの名前として、「CognosReport」と入力します。
6. 「OK」をクリックします。新しいポートレットが「ポートレットの管理 (Manage Portlets)」ウィンドウに表示されます。
7. 「管理」 > 「ポータル・ユーザー・インターフェース」 > 「ページの管理」にナビゲートします。
8. 「コンテンツ・ルート」 > 「市全域」をクリックし、「新規ページ (New Page)」タブをクリックします。「ページ・プロパティ (Page Properties)」ページが表示されます。
9. 新規レポート・ページの以下のプロパティを入力します。
  - a. 「タイトル」フィールドに、レポート・ページのタイトルを入力します。例えば、「オペレーター: レポート」などのタイトルを付けます。
  - b. 「一意の名前」フィールドに、このレポート・ページを明確に識別する名前を入力します。例えば、「com.ibm.iss.ioc.citywide.OperatorReports」などの一意の名前を付けます。
  - c. 「分かりやすい名前」フィールドに、「report」と入力します。

- d. 「テーマ」フィールドでは、デフォルトの「親テーマを継承 (Inherit Parent Theme)」をそのまま使用します。
  - e. 「テーマ・スタイル」フィールドで、デフォルトの「親テーマ・ポリシーを継承 (Inherit Parent Theme Policy)」をそのまま使用します。
  - f. 「集約レンダリング・モード (Aggregation-Render Mode)」で、「親レンダリング・モードを継承 (Inherit Parent Render Mode)」を選択します。
  - g. 「OK」をクリックします。
- 新規レポート・ページがポートレット・ページのリストに追加されます。

## 「レポート」ポートレットのレイアウトの編集

「レポート」ポートレット・ページのレイアウトをフォーマット設定するには、以下のステップを使用します。

### このタスクについて

IBM Intelligent Operations Center コンソールを使用して「レポート」ポートレット・ページのレイアウトを選択するには、以下のステップを実行します。

### 手順

1. IBM Intelligent Operations Center に管理者としてログオンします。
2. 「管理」 > 「ポータル・ユーザー・インターフェース」 > 「ページの管理」にナビゲートします。
3. 編集するページの横にある「ページ・レイアウトの編集 (Edit Page Layout)」アイコンをクリックします。「レイアウトの編集 (Edit Layout)」ページが表示されます。
4. ページの真下に行がある横並びページのレイアウト・アイコンを選択します。このアイコンは、左から 5 番目のアイコンです。
5. ポートレットを追加するフレームで、「ポートレットの追加 (Add Portlets)」をクリックします。
6. 「CognosPortlet」チェック・ボックスを探して選択し、「OK」をクリックしてポートレットをページ・レイアウトに追加します。ポートレットが追加されたことを確認するメッセージが表示されます。
7. ステップ 5 および 6 を繰り返して、その他のポートレットを追加します。最大で 6 個のポートレットを追加できます。
8. 「完了」をクリックします。

### 次のタスク

ポートレットごとに共有設定を編集できます。編集するポートレットの右上隅にある矢印をクリックし、メニューから「共有設定の編集」を選択します。詳しくは、『レポートを表示するためのポートレットのカスタマイズ』を参照してください。

## レポートを表示するためのポートレットのカスタマイズ

このトピックの情報を使用し、IBM Intelligent Operations Center ポートレットをカスタマイズして IBM Cognos Business Intelligence レポートを表示します。

### 手順

1. ソリューション・ポータルに管理者としてログオンします。
2. レポートを表示するためにカスタマイズするビューおよびポートレットを選択します。
3. ポートレットの右上隅にあるポートレット表示メニューにナビゲートします。



4. 「**共用設定の編集**」をクリックします。
5. 表示されるフィールドに使用する設定値を入力します。
  - a. レポートのタイトルを入力します。
  - b. レポートの「**URL**」を入力します。トピック『**レポート URL の検索**』の説明に従って、必要な URL を見つけます。  
  
Example: CAP\_events\_by\_type\_status\_and\_date:  
`http://9.161.84.100:9082/ServletGateway/servlet/Gateway?b_action=cognosViewer&ui.action=run  
&ui.object=%2fcontent%2fpackage%5b%40name%3d%27ioc_model%27%5d%2ffolder%5b%40n  
ame%3d%27reports%27%5d%2freport%5b%40name%3d%27CAP_events_by_type_status_and_d  
ate%27%5d&ui.name=CAP_events_by_type_status_and_date&run.outputFormat=&run.prompt=tr  
ue`
  - c. ポータルの「**幅**」を 600 に設定します。
  - d. ポータルの「**高さ**」を 600 に設定します。
  - e. 「**保存**」をクリックします。
  - f. ポートレット表示メニューで「**戻る**」をクリックし、メインのポートレット・ビューに戻ります。

## タスクの結果

レポート・ポートレットが更新され、直近の選択に従ってレポートが表示されます。

## レポート URL の検索

このトピックではレポートの URL を検索するステップについて説明します。

### 手順

1. IBM Cognos Connection にログオンします。
2. 「共有フォルダー」 > 「ioc\_model」 > 「レポート」にナビゲートします。
3. レポートを選択して「**プロパティを設定**」アイコンをクリックします。
4. 「全般」タブで「**検索パス、ID、URL を表示**」をクリックしてレポート URL を表示します。
5. 必要に応じて、「**デフォルト操作の URL**」セクションで URL をコピーしてポートレットに貼り付けます。

## データ・モデルの操作

IBM Intelligent Operations Center は、レポートの生成時に使用される 2 つのデータ・モデルを提供します。メタモデルは、モデル形成の基となる言語およびプロセスを定義します。

IBM Intelligent Operations Center のレポートは 2 つのデータ・モデルに基づいて作成されます。

- 共通スキーマ・データ・モデル
- 共通アラート・プロトコル (CAP) スキーマ・データ・モデル

IBM Intelligent Operations Center データ・モデルは 2 つともレイヤーとして編成されています。レポート作成者のためにプレゼンテーション・ビューまたはレイヤーが使用可能になっており、以下の名前空間で構成されています。

### ビジネス

辞書、フィルター、およびデータが含まれます。

### ディメンション

レポートおよび分析のイベント・ディメンションが含まれます。

## カスタム照会

リレーショナル・レポートのカスタム照会を作成するために使用できる照会対象が含まれます。

## 共通スキーマ・データ・モデル・レポートの生成

このトピックでは、共通スキーマ・データ・モデル・レポートの生成方法について説明します。これらのレポートは、マネージャーと監督者がイベントをモニターし、発生するイベントに対応し、今後発生するイベントに備えて計画を立てる際に役立ちます。

### このタスクについて

IBM Intelligent Operations Center コンソールを使用して以下の手順を実行し、共通スキーマ・データ・モデル・レポートを生成します。レポート生成オプションについては、このトピックの末尾にある参照リンクを参照してください。

### 手順

1. IBM Intelligent Operations Center コンソールの「管理」タブで「**Intelligent Operations**」 > 「管理ツール」 > 「管理コンソール」をクリックします。「管理コンソール」ページが表示されます。
2. アプリケーション・サーバーの下で、「レポート管理」をクリックします。「IBM Cognos Connection」ページが表示されます。
3. 「ioc 共通モデル (ioc common model)」をクリックします。Cognos 共有フォルダーが表示されます。
4. 「レポート」をクリックします。
5. 生成するレポートのタイプを選択します。
  - 円グラフ・レポートを生成するには、「円グラフ」をクリックします。共通スキーマ円グラフ・レポートが表示されます。
  - テーブル・チャート・レポートを生成する場合は、「テーブル・チャート (Table charts)」をクリックします。共通スキーマ・テーブル・チャート・レポートが表示されます。
6. 生成するレポートを選択します。

### 円グラフ・オプション:

このトピックでは、共通円グラフ・レポートで選択できるオプションを説明します。

「IBM Cognos Connection」ページから円グラフ・レポートにアクセスするには、「共有フォルダー」 > 「ioc\_common\_model」 > 「レポート」 > 「円グラフ」をクリックします。

表 65. 共通スキーマ・データ・モデル・レポートの円グラフ・オプション

レポート	説明
カテゴリ別イベント (Event by category)	イベント・カテゴリに基づいてイベントを表示します。例えば、「環境」、「火災」、「輸送」などのすべてのイベントを表示できます。
確信度別イベント (Event by certainty)	発生する可能性に基づいてイベントを表示します。例えば、交通事故が発生した場合、確信度は「監視対象」となります。
送信日時別イベント (Event by date sent)	このレポートは、特定の日に送信されたイベントを表示します。
イベント・タイプ別イベント (Event by event type)	タイプに基づいてイベントを表示します。例えば、接近中の竜巻や交通事故などのイベントです。

表 65. 共通スキーマ・データ・モデル・レポートの円グラフ・オプション (続き)

レポート	説明
見出し別イベント (Event by headline)	イベントの作成時に入力された記述に基づいてイベントを表示します。このため、見出しは実際にはイベント記述になります。
重大度別イベント (Event by severity)	重大度に基づいてイベントを表示します。例えば、「極度」や「重度」などのイベントです。
仕様別イベント (Event by specification)	仕様別にイベントを表示します。例えば、イベントが 共通アラート・プロトコル・イベントまたは非共通アラート・プロトコル・イベントであるとしています。この場合このグラフには 共通アラート・プロトコル・イベントと非共通アラート・プロトコル・イベントのパーセンテージが表示されます。
緊急度別イベント (Event by urgency)	緊急度に基づいてイベントを表示します。例えば、イベントが発生して、「即時」として表記される場合があります。
URL 別イベント (Event by URL)	イベント作成時にイベントに対して入力された URL 別にイベントを表示します。

#### テーブル・チャート・オプション:

このトピックでは、共通テーブル・チャート・レポートに対して生成できる情報について説明します。

「IBM Cognos Connection」ページからテーブル・チャート・レポートにアクセスするには、「共有フォルダー」 > 「ioc\_common\_model」 > 「レポート」 > 「テーブル・チャート (Table charts)」をクリックします。

共通スキーマ・データ・モデル・レポートのテーブル・チャート・オプションは、「イベント・リスト」のみです。イベント・リストには、すべてのイベントが、イベントごとの詳細情報と共にリストされます。イベント・リストに表示される情報の例のいくつかを、以下に説明します。

表 66. 共通テーブル・チャートのイベント・リスト情報

レポート・フィールド	説明
ID	報告書を識別します。
外部イベント ID	イベント作成時に生成されたイベント ID です。
仕様	イベントが共通アラート・プロトコル・イベントまたは非共通アラート・プロトコル・イベントのいずれであるかを指定します。
イベント・タイプ	タイプに基づいてイベントを表示します。例えば、接近中の竜巻や交通事故などのイベントです。
送信済み	イベントが送信された日付および時刻。
見出し	イベントの説明。
カテゴリー	イベント・カテゴリーに基づいてイベントを表示します。例えば、「環境」、「火災」、「輸送」などのすべてのイベントを表示できます。
確信度	発生する可能性に基づいてイベントを表示します。例えば、交通事故が発生した場合、確信度は「監視対象」となります。

表 66. 共通テーブル・チャートのイベント・リスト情報 (続き)

レポート・フィールド	説明
重大度	重大度に基づいてイベントを表示します。例えば、「極度」や「重度」などのイベントです。
緊急度	緊急度に基づいてイベントを表示します。例えば、イベントが発生して、「即時」として表記される場合があります。
URL	レポートに関連付けられている URL です。

## 共通アラート・プロトコル スキーマ・データ・モデル・レポートの生成

このトピックでは、共通アラート・プロトコル スキーマ・データ・モデル・レポートの生成方法について説明します。これらのレポートは、マネージャーと監督者がイベントをモニターし、発生するイベントに対応し、今後発生するイベントに備えて計画を立てる際に役立ちます。

### このタスクについて

IBM Intelligent Operations Center コンソールを使用して以下の手順を実行し、共通アラート・プロトコル スキーマ・データ・モデル・レポートを生成します。レポート生成オプションについては、このトピックの末尾にある参照リンクを参照してください。

### 手順

1. IBM Intelligent Operations Center コンソールの「管理」タブで「**Intelligent Operations**」 > 「管理ツール」 > 「管理コンソール」をクリックします。「管理コンソール」ページが表示されます。
2. アプリケーション・サーバーの下で、「**レポート管理**」をクリックします。「IBM Cognos Connection」ページが表示されます。
3. 「**ioc cap モデル (ioc cap model)**」をクリックします。Cognos 共有フォルダーが表示されます。
4. 「**レポート**」をクリックします。
5. 生成するレポートのタイプを選択します。
  - このページにリストされているデータ・モデル・レポートを生成するには、そのレポートを選択します。
  - 円グラフ・レポートを生成するには、「**円グラフ**」をクリックします。共通スキーマ円グラフ・レポートが表示されます。リストから選択してください。
  - ユーザー定義レポートを生成するには、「**ユーザー定義レポート (User-defined reports)**」をクリックします。Cognos カスタム・レポート・ページが表示されます。カスタム・レポートのフィールドに情報を入力し、「**更新**」をクリックします。

### データ・モデル・レポート・オプション:

このトピックでは、共通アラート・プロトコル レポートの生成について選択できるオプションを説明します。

「IBM Cognos Connection」ページから以下のレポート・オプションにアクセスするには、「**共有フォルダー**」 > 「**ioc\_cap\_model**」 > 「**レポート**」をクリックします。

表 67. 共通アラート・プロトコル レポートの情報に関するオプション

レポート	説明
タイプ、状況、および日付別の 共通アラート・プロトコル イベント (共通アラート・プロトコル events by type, status, and date)	このレポートには、共通アラート・プロトコル イベントがイベント・タイプ、イベント状況、およびイベント日付に基づいて表示されます。例えば、イベント・タイプが「事故」、状況が「緊急」であることが考えられます。日付として本日の日付を使用できます。
日付別 共通アラート・プロトコル イベント KPI メトリック (共通アラート・プロトコル events KPI metrics by date)	このレポートは、特定の日付または日付範囲における KPI メトリックに基づく 共通アラート・プロトコル イベントを表示します。
部門別 共通アラート・プロトコル イベント KPI メトリック (共通アラート・プロトコル events KPI metrics by department)	このレポートは、特定の部門またはエリアの KPI メトリックに基づく 共通アラート・プロトコル イベントを表示します。例えば、このレポートには水道局の KPI メトリックと市内の特定エリアの KPI メトリックが表示されることがあります。
共通アラート・プロトコル 詳細情報 (共通アラート・プロトコル full details)	このレポートには、共通アラート・プロトコル イベントに関する完全な詳細情報が表示されます。例えば、詳細情報には 共通アラート・プロトコル ID、送信者、送信日時、状況、メッセージ・タイプ、ソースなどがあります。
重要度別のすべての日付の IBM Intelligent Operations Center イベント (IBM Intelligent Operations Center events by severity anytime)	このレポートには、すべての IBM Intelligent Operations Center イベントが重大度に基づいてリストされます。例えば、「極度」などのイベントです。
重大度別の進行中の IBM Intelligent Operations Center イベント (IBM Intelligent Operations Center events by severity in progress)	このレポートには、現在発生しているすべての IBM Intelligent Operations Center イベントが重大度別に表示されます。例えば、進行中のイベントの重大度が、現在発生している異常気象であることがあります。

## 円グラフ・オプション:

このトピックでは、共通アラート・プロトコル 円グラフ・レポートを生成するためのオプションについて説明します。

「IBM Cognos Connection」ページから円グラフ・レポートにアクセスするには、「共有フォルダー」 > 「ioc\_cap\_model」 > 「レポート」 > 「円グラフ (Pie charts)」をクリックします。

表 68. 共通アラート・プロトコル 円グラフ・レポートの情報のオプション

レポート	説明
カテゴリー別 CAP (Cap by category)	特定のカテゴリー別に共通アラート・プロトコルを表示します。例えば、「環境」、「火災」、「輸送」などのすべてのイベントを表示できます。
確信度別 CAP (Cap by certainty)	発生する可能性に基づいて共通アラート・プロトコル・イベントを表示します。例えば、交通事故が発生した場合、確信度は「監視対象」となります。
送信日別 CAP (Cap by date sent)	特定の日に送信された 共通アラート・プロトコル イベントを表示します。
イベント・タイプ別 CAP (Cap by event type)	タイプに基づいて共通アラート・プロトコル・イベントを表示します。例えば、接近中の竜巻や交通事故などのイベントです。

表 68. 共通アラート・プロトコル 円グラフ・レポートの情報のオプション (続き)

レポート	説明
処理コード別 CAP (Cap by handling code)	処理コード別に共通アラート・プロトコル・イベントを表示します。例えば、「イベント」などの処理コードがあります。
メッセージ・タイプ別 CAP (Cap by message type)	「更新」や「アラート」などのメッセージ・タイプに基づいて共通アラート・プロトコル・イベントを表示します。
スコープ別 CAP (Cap by scope)	スコープ別に共通アラート・プロトコル・イベントを表示します。例えばスコープ別イベントが「パブリック」であることがあります。
送信者別 CAP (Cap by sender)	差出人名別に共通アラート・プロトコル・イベントを表示します。
重大度別 CAP (Cap by severity)	重大度に基づいて共通アラート・プロトコル・イベントを表示します。例えば、「極度」や「重度」などのイベントです。
ソース別 CAP (Cap by source)	特定のソース別に共通アラート・プロトコルを表示します。例えば、「輸送」などのソースです。
状況別 CAP (Cap by status)	スコープ別に共通アラート・プロトコル・イベントを表示します。以下のような状況があります。 <ul style="list-style-type: none"> <li>・ 許容可能</li> <li>・ 注意</li> <li>・ 対処</li> </ul>
緊急度別 CAP (Cap by urgency)	緊急度に基づいて共通アラート・プロトコル・イベントを表示します。例えば、イベントが発生して、「即時」として表記される場合があります。
カテゴリー別通知	特定のカテゴリーに基づいて 共通アラート・プロトコル形式のアラート・メッセージを表示します。例えば、「環境」、「火災」、「輸送」などのすべてのイベントを表示できます。
タイプ別通知 (Notification by type)	タイプ別に 共通アラート・プロトコル 形式で通知を表示します。例えば、タイプが「更新」および「アラート」であることがあります。

#### ユーザー定義イベント・レポートのオプション:

このトピックでは、イベントに関する 共通アラート・プロトコル ユーザー定義レポートの生成のオプションについて説明します。

「IBM Cognos Connection」ページからユーザー定義レポートにアクセスするには、「共有フォルダー」 > 「ioc\_cap\_model」 > 「レポート」 > 「ユーザー定義レポート (User-defined reports)」 > 「イベント」をクリックします。

表 69. 共通アラート・プロトコル イベントのオプション

レポート	説明
カテゴリー別のすべての日付のイベント (Events by Category Anytime)	日付に関わらず、カテゴリー別にすべてのイベントを表示します。例えば、「環境」、「火災」、「輸送」などのすべてのイベントを表示できます。



表 69. 共通アラート・プロトコル イベントのオプション (続き)

レポート	説明
確信度別のすべての日付のイベント (Events by Certainty Anytime)	日付に関わらず、確信度別にすべてのイベントを表示します。例えば、交通事故が発生した場合、確信度は「監視対象」となります。
イベント・タイプ別のすべての日付のイベント (Events by Event Type Anytime)	日付に関わらず、イベント・タイプ別にすべてのイベントを表示します。例えば、任意の日付に発生した交通事故や接近中の竜巻などのイベントがあります。
重大度別のすべての日付のイベント (Events by Severity Anytime)	日付に関わらず、重大度別にすべてのイベントを表示します。例えば、すべての日付の極度イベントと重度イベントが表示されます。
緊急度別のすべての日付のイベント (Events by Urgency Anytime)	日付に関わらず、緊急度別にすべてのイベントを表示します。例えば、イベントが発生して、「即時」として表記される場合があります。

### ユーザー定義のカスタム・レポート・オプション:

このトピックでは、共通アラート・プロトコル ユーザー定義カスタム・レポートの生成に関するオプションについて説明します。

「レポート」ポートレットを使用して、イベントのカスタム・レポートを作成することができます。まず、イベントをグループ化する方法を選択します。例えば、特定のカテゴリのすべてのイベントを表示するには、「グループ化」フィールドで「カテゴリ」を選択します。次に、「データの選択」フィールドで、表示する情報に固有のデータを選択します。また、レポートのイベントについて日付または日付範囲を指定することもできます。「更新」をクリックすると、グラフが変更され、要求した情報が反映されます。

新規レポートの URL を取得するには、「このレポートの URL」をクリックします。

「IBM Cognos Connection」ページからカスタムのユーザー定義レポートにアクセスするには、「共有フォルダー」 > 「ioc\_cap\_model」 > 「レポート」 > 「ユーザー定義レポート (User-defined\_reports)」 > 「ユーザー定義レポート (User-defined report)」をクリックします。

表 70. 共通アラート・プロトコル ユーザー定義カスタム・オプション

レポート	説明
グループ化	イベントをグループ化する基準のオプションを選択します。
重大度	重大度に基づいてイベントを表示します。例えば、「極度」や「重度」などのイベントです。
確信度	発生する可能性に基づいてイベントを表示します。例えば、交通事故が発生した場合、確信度は「監視対象」となります。
緊急度	緊急度に基づいてイベントを表示します。例えば、イベントが発生して、「即時」として表記される場合があります。
イベント・カテゴリ	イベント・カテゴリに基づいてイベントを表示します。例えば、「環境」、「火災」、「輸送」などのすべてのイベントを表示できます。

表 70. 共通アラート・プロトコル ユーザー定義カスタム・オプション (続き)

レポート	説明
イベント・タイプ	タイプに基づいてイベントを表示します。例えば、接近中の竜巻や交通事故などのイベントです。
開始日	イベントを表示する日付を入力します。日付範囲の場合は、開始日を入力します。
終了日	いつまでのイベントを表示するか、その日付を入力します。

## 共通スキーマ・データ・モデル・レポートの構成

このトピックを使用して、共通スキーマ・データ・モデル・レポートの一般プロパティと固有のプロパティを設定します。

### 始める前に

この手順を実行するには、管理者アクセス権限が必要です。

### このタスクについて

IBM Intelligent Operations Center コンソールを使用してこれらのレポートを構成します。

### 手順

1. IBM Intelligent Operations Center コンソールの「管理」タブで「**Intelligent Operations**」 > 「管理ツール」 > 「管理コンソール」をクリックします。「管理コンソール」ページが表示されます。
2. アプリケーション・サーバーの下で、「**レポート管理**」をクリックします。「IBM Cognos Connection」ページが表示されます。
3. 「**ioc 共通モデル (ioc common model)**」チェック・ボックスを選択し、「**その他**」をクリックします。「使用可能なアクション」ページが表示されます。
4. 「**プロパティの設定**」をクリックします。「一般プロパティ」ページが表示されます。
5. 一般レポート・プロパティの値を選択します。
6. 「**権限**」タブで、共通スキーマ・データ・モデル・レポートの権限を選択します。
7. 「**機能**」タブで、レポートの機能を選択します。
8. 「**OK**」をクリックします。

## 共通アラート・プロトコル スキーマ・データ・モデル・レポートの構成

このトピックを使用して、共通アラート・プロトコル スキーマ・データ・モデル・レポートの一般プロパティの設定、権限の設定、およびユーザー・タイプへの機能の割り当てを行います。

### 始める前に

この手順を実行するには、管理者アクセス権限が必要です。

### このタスクについて

IBM Intelligent Operations Center コンソールを使用してこれらのレポートを構成します。

## 手順

1. IBM Intelligent Operations Center コンソールの「管理」タブで「Intelligent Operations」 > 「管理ツール」 > 「管理コンソール」をクリックします。「管理コンソール」ページが表示されます。
2. アプリケーション・サーバーの下で、「レポート管理」をクリックします。「IBM Cognos Connection」ページが表示されます。
3. 「ioc cap モデル (ioc cap model)」チェック・ボックスを選択してから、「その他」をクリックします。「使用可能なアクション」ページが表示されます。
4. 「プロパティの設定」をクリックします。「一般プロパティ」ページが表示されます。
5. 一般レポート・プロパティの値を選択します。
6. 「権限」タブで 共通アラート・プロトコル スキーマ・データ・モデル・レポートに対する権限を選択します。
7. 「機能」タブで、レポートのユーザーの機能を選択します。
8. 「OK」をクリックします。

## その他のレポート・オプション

このトピックでは、共通レポートと 共通アラート・プロトコル レポートのその他のレポート・オプションについて説明します。

これらのレポート・オプションにアクセスするには、特定のレポートのリンクの右側にある「その他」をクリックします。

表 71. 各レポートで使用可能な追加オプション

オプション	説明
プロパティを設定	選択したレポートの一般プロパティを設定します。
出力レポート・バージョンを表示	形式のハイパーリンクをクリックして、表示する出力バージョンを選択します。
権限を表示	このエントリーに対する自分のアクセス権を表示します。
オプションを指定して実行	レポートの実行方法と受け取り方法を選択します。例えば HTML、PDF などです。
Report Studio で開く	Report Studio を使用してレポートを別のブラウザで表示します。
Business Insight Advanced で開く	IBM Cognos Business Insight Advanced を使用してレポートを別のブラウザで表示します。
スケジュールの新規作成	さまざまな条件に基づいてレポートをスケジュールします。
移動	レポートを別の位置に移動します。
コピー	レポートをある位置から別の位置にコピーします。
このエントリーのショートカットを作成	レポートにアクセスするためのショートカットをデスクトップ上に作成します。
このレポートのレポート・ビューを作成	ローカル・ディレクトリーに保存されているこのレポートのビューをデスクトップ上に作成します。
削除	表示されているレポートを削除します。



---

## 第 6 章 ソリューションの管理

このセクションの各トピックでは、IBM Intelligent Operations Center の管理用タスクを実行する方法について説明します。

---

### 製品情報

「製品情報」ポートレットを使用して、インストール済みの IBM Intelligent Operations Center および統合された IBM Smarter Cities Software Solutions のバージョンの詳細を表示します。インストール後に適用した更新の詳細も表示できます。

「製品情報」ポートレットを起動するには、WebSphere Portal 管理インターフェースで「**Intelligent Operations**」 > 「製品情報」をクリックします。

「製品情報」ポートレットは以下の情報を提供します。

- インストール済みのすべてのソフトウェア製品およびコンポーネントの場所
- インストール済み製品の名前とバージョン
- インストール済みコンポーネントの名前とバージョン
- 適用済みのフィックスの詳細

識別されるコンポーネントは、コンポーネント、または製品の一部です。以下に例を示します。

- 専用の保守ストリームまたはサービス・ストリームを持つ製品の一部
- オプションとしてインストール可能な、製品の一部
- 複数の製品で共有される、製品の一部

注: 各フィックスについて表示される情報は、そのフィックスで提供されたインストールの指示で該当する手順を完了したかどうかによって変わります。

### 「製品情報」ポートレットのカスタマイズ

このポートレットはカスタマイズすることができます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

#### 関連タスク:

58 ページの『インストールの検証』

IBM Intelligent Operations Center のインストール後に、製品が正常にインストールされたことを確認します。

#### 関連資料:

162 ページの『「製品情報」ポータルレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「製品情報」ポータルレットをカスタマイズできます。

---

## サービスの制御

IBM Intelligent Operations Center サーバー上で実行されている IBM Intelligent Operations Center サービスは、制御および照会の対象とすることができます。

## サービスの開始

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサーバーで実行中のサービスを開始することができます。

### このタスクについて

**IOCControl.sh** コマンドは、`ibmadmin` ユーザーとして実行する必要があります。 `ibmadmin` としてログオンしていない場合、`su - ibmadmin` コマンドを実行して `ibmadmin` ユーザーに切り替えます。

**重要:** 個別サービスの開始は、熟練した IBM Intelligent Operations Center 管理者のみが行ってください。必要とされる順序でサービスが開始されなかった場合は、予測不能な結果が起こることがあります。

### 手順

IBM Intelligent Operations Center のすべてのサービスを開始するには、管理サーバーで以下のコマンドを実行します。

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start all password
```

ここで、`password` は、プラットフォーム制御ツールのインストール時に定義されたプラットフォーム制御ツールのパスワードです。

サービスは、必要とされる順序で開始されます。前提条件サービスは、従属サービスより前に開始されません。例えば、データベース・サービスとディレクトリー・サービスは最初に開始されます。

1 つのサービスのみを開始するには、以下のコマンドを実行します。

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start service_ID password
```

ここで、`service_ID` は、**IOCControl** ヘルプの「ターゲット・オプション (Target Options)」にリストされている ID、`password` は プラットフォーム制御ツールのインストール時に定義されたプラットフォーム制御ツールのパスワードです。

### タスクの結果

要求された IBM Intelligent Operations Center サービスが開始されます。



## 次のタスク

**IOCControl.sh** コマンドの実行後に、`/opt/IBM/ISP/mgmt/logs` ディレクトリーのログを確認します。ログには、**IOCControl.sh** コマンドの結果が含まれています。

### 関連タスク:

219 ページの『サービスの停止』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスを停止できます。

222 ページの『サービス状況の照会』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスの状況を判別することができます。

223 ページの『プラットフォーム制御ツールのヘルプの入手』

プラットフォーム制御ツールのアクションおよびターゲット・オプションに関する情報が使用可能になります。

58 ページの『インストールの検証』

IBM Intelligent Operations Center のインストール後に、製品が正常にインストールされたことを確認します。

55 ページの『プラットフォーム制御ツールのインストール』

プラットフォーム制御ツールは、IBM Intelligent Operations Center サーバー環境を管理するために使用されます。このツールは、本製品とは別にインストールします。

56 ページの『システム検査チェック・ツールのインストール』

システム検査チェック・ツールを使用して、IBM Intelligent Operations Center 内のコンポーネントの運用状況を検査することができます。このツールは、本製品とは別にインストールします。

## 必要とされる開始順序

IBM Intelligent Operations Center のサービスは、特定の順序で開始する必要があります。

IBM Intelligent Operations Center のサービスを開始するには、プラットフォーム制御ツールを使用します。プラットフォーム制御ツール **start all** オプションを使用してすべてのサービスを開始することが推奨されますが、個別にサービスを開始することが必要な場合もあります。

一部のサービスには他のサービスへの従属関係があるため、サービスは特定の順序で開始する必要があります。

通常は、サービスを以下の 3 つのグループに分けて開始してください。

### グループ 1

tds、db24po、db24sms、db24wbm、db24ana、db24tsrm、db24sol、db24mgmt

### グループ 2

ihs、appdmgr、st

### グループ 3

残りのすべてのサービス

グループ 1 のサービスを最初に開始し、次にグループ 2 を開始し、最後にグループ 3 を開始します。各グループ内のサービスは任意の順序で開始できます。

表 72. IBM Intelligent Operations Center のサービス開始順序の従属関係

サービス	説明	このサービスの開始前から実行されている必要のあるサービス
db24po	DB2 Enterprise Server Edition for WebSphere Portal Server	なし
db24wbm	DB2 Enterprise Server Edition for WebSphere Business Modeler	なし
db24sol	DB2 Enterprise Server Edition for IBM Intelligent Operations Center	なし
db24ana	DB2 Enterprise Server Edition for Cognos	なし
db24mgmt	Tivoli Enterprise Portal サービス用の DB2 Enterprise Server Edition	なし
db24tsrm	DB2 Enterprise server for Tivoli Service Request Manager	なし
db24sms	DB2 Enterprise server for Semantic Model Services	なし
tds	Tivoli Directory Server	なし
tdspxyapp	Tivoli Directory Server Proxy (アプリケーション・サーバー)	tds
tdspxyevt	Tivoli Directory Server Proxy (イベント・サーバー)	tds
tdspxymgt	Tivoli Directory Server Proxy (管理サーバー)	tds
tdsappsrv	Tivoli Directory Server Application Server	なし
tamps	Tivoli Access Manager Policy Server	tamas
tamas	Tivoli Access Manager Authorization Server	tds
tamwpm	Tivoli Access Manager Web Portal Manager	なし
tamweb	Tivoli Access Manager WebSEAL	tamas
tems	Tivoli Monitoring Enterprise Monitoring Server	なし
teps	Tivoli Monitoring Enterprise Portal Server	tems、db24mgmt
tim	Tivoli Identity Manager	tds
appdmgr	WebSphere Application Server Network Deployment	なし
cplex	WebSphere Application Server for CPLEX	db24sms
ihs	HTTP Server for Runtime (アプリケーション・サーバー)	なし
ihsevt	HTTP Server for Runtime (イベント・サーバー)	ihs
ihsmtgt	HTTP Server for Runtime (管理サーバー)	ihs
ncob	Tivoli Netcool/OMNIBus	なし
nci	Tivoli Netcool/Impact	ncob
wbm	IBM WebSphere Business Monitor	db24wbm
st	Lotus Sametime	なし
stpxy	Lotus Sametime Proxy Application Server	st
wpe	WebSphere Portal Extend	tdspxyapp、db24po、appdmgr
wmb	WebSphere Message Broker	なし
cognos	IBM Cognos Business Intelligence	db24ana、appdmgr
tsrm	Tivoli Service Request Manager	appdmgr、db24tsrm
wodm	WebSphere Operations Decision Manager	appdmgr
wodmdc	WebSphere Operations Decision Manager (Decision Center)	なし

表 72. IBM Intelligent Operations Center のサービス開始順序の従属関係 (続き)

サービス	説明	このサービスの開始前から実行されている必要のあるサービス
smsclt	Semantic Model Services (クライアント・サービス)	appdmgr
smsdaq	Semantic Model Services (データ・サービス)	appdmgr
smsmdl	Semantic Model Services (モデル・サービス)	appdmgr
smsgmt	Semantic Model Services (管理サービス)	appdmgr
smsrtc	Semantic Model Services (RTC サービス)	appdmgr
iocxml	IBM Intelligent Operations Center XML probe	db24sol

## Tivoli Netcool/OMNIBus プロープの開始と停止

IBM Intelligent Operations Center のすべてのサーバーが開始された後で、Tivoli Netcool/OMNIBus プロープを開始します。

### このタスクについて

プローブは、IOCControl スクリプトの一部です。プローブの開始および停止は、Tivoli Netcool/OMNIBus の開始および停止のときに行われます。Tivoli Netcool/OMNIBus プロープは、スクリプト内で Tivoli Netcool/OMNIBus とリンクされています。プローブの停止、開始、および状況の検査を行うには、以下の手順を使用します。

### 手順

1. プロープを停止するには、管理サーバーで以下を実行します。  

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop ncoab password
```
2. プロープを開始するには、管理サーバーで以下を実行します。  

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start ncoab password
```
3. プロープの状況を検査するには、以下のようになります。
  - 管理サーバーで、以下のコマンドを実行します。  

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start iocxml password
```
  - イベント・サーバーで、以下のコマンドを実行します。  

```
tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

## サービスの停止

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスを停止できます。

### このタスクについて

**IOCControl.sh** コマンドは、ibmadmin ユーザーとして実行する必要があります。ibmadmin としてログオンしていない場合、**su - ibmadmin** コマンドを実行して ibmadmin ユーザーに切り替えます。

**重要:** 個別サービスの停止は、熟練した IBM Intelligent Operations Center 管理者のみが行ってください。必要とされる順序でサービスが停止されなかった場合は、予測不能な結果が起こることがあります。

## 手順

IBM Intelligent Operations Center のすべてのサービスを停止するには、管理サーバーで以下のコマンドを実行します。

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh stop all password
```

ここで、*password* は、プラットフォーム制御ツールのインストール時に定義されたプラットフォーム制御ツールのパスワードです。

1 つのサービスのみを停止するには、以下のコマンドを実行します。

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh stop service_ID password
```

ここで、*service\_ID* は、**IOControl** ヘルプの「**ターゲット・オプション (Target Options)**」にリストされている ID、*password* は プラットフォーム制御ツールのインストール時に定義されたプラットフォーム制御ツールのパスワードです。

## タスクの結果

要求された IBM Intelligent Operations Center サービスが停止されます。

## 次のタスク

**IOControl.sh** コマンドの実行後に、`/opt/IBM/ISP/mgmt/logs` ディレクトリーのログを確認します。ログには、**IOControl.sh** コマンドの結果が含まれています。

### 関連タスク:

216 ページの『サービスの開始』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサーバーで実行中のサービスを開始することができます。

222 ページの『サービス状況の照会』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスの状況を判別することができます。

223 ページの『プラットフォーム制御ツールのヘルプの入手』

プラットフォーム制御ツールのアクションおよびターゲット・オプションに関する情報が使用可能になります。

58 ページの『インストールの検証』

IBM Intelligent Operations Center のインストール後に、製品が正常にインストールされたことを確認します。

55 ページの『プラットフォーム制御ツールのインストール』

プラットフォーム制御ツールは、IBM Intelligent Operations Center サーバー環境を管理するために使用されます。このツールは、本製品とは別にインストールします。

56 ページの『システム検査チェック・ツールのインストール』

システム検査チェック・ツールを使用して、IBM Intelligent Operations Center 内のコンポーネントの運用状況を検査することができます。このツールは、本製品とは別にインストールします。

## 必要とされる停止順序

IBM Intelligent Operations Center のサービスは、特定の順序で停止する必要があります。

IBM Intelligent Operations Center のサービスを停止するには、プラットフォーム制御ツールを使用します。プラットフォーム制御ツールの **stop all** オプションを使用してすべてのサービスを停止することが推奨されますが、個別にサービスを停止することが必要な場合もあります。

一部のサービスには他のサービスへの従属関係があるので、サービスは特定の順序で停止する必要があります。

通常は、サービスを以下の 3 つのグループに分けて停止してください。

#### グループ 1

tds、db24po、db24sms、db24wbm、db24ana、db24tsrm、db24sol、db24mgmt

#### グループ 2

ihs、appdmgr、st

#### グループ 3

残りのすべてのサービス

グループ 3 のサービスを最初に停止し、次にグループ 2 を停止し、最後にグループ 1 を停止します。各グループ内のサービスは任意の順序で停止できます。

表 73. IBM Intelligent Operations Center のサービス停止順序の従属関係

サービス	説明	このサービスの停止前に停止されている必要のあるサービス
db24po	DB2 Enterprise Server Edition for WebSphere Portal Server	wpe
db24wbm	DB2 Enterprise Server Edition for WebSphere Business Modeler	wbm
db24sol	DB2 Enterprise Server Edition for IBM Intelligent Operations Center	iocxml
db24ana	DB2 Enterprise Server Edition for Cognos	cognos
db24mgmt	Tivoli Enterprise Portal サービス用の DB2 Enterprise Server Edition	teps
db24tsrm	DB2 Enterprise server for Tivoli Service Request Manager	tsrm
db24sms	DB2 Enterprise server for Semantic Model Services	cplex
tds	Tivoli Directory Server	tdsprxyapp、tdspxyevt、tdspxygmt、tamas、tim
tdsprxyapp	Tivoli Directory Server Proxy (アプリケーション・サーバー)	wpe
tdspxyevt	Tivoli Directory Server Proxy (イベント・サーバー)	なし
tdspxygmt	Tivoli Directory Server Proxy (管理サーバー)	なし
tdsappsrv	Tivoli Directory Server Application Server	なし
tamps	Tivoli Access Manager Policy Server	なし
tamas	Tivoli Access Manager Authorization Server	tamps
tamwpm	Tivoli Access Manager Web Portal Manager	なし
tamweb	Tivoli Access Manager WebSEAL	なし
tems	Tivoli Monitoring Enterprise Monitoring Server	teps
teps	Tivoli Monitoring Enterprise Portal Server	なし
tim	Tivoli Identity Manager	なし
appdmgr	WebSphere Application Server Network Deployment	wpe、cognos、tsrm、wodm、smsclt、smsdaq、smsmdl、smsrtc、smsgmt
cplex	WebSphere Application Server for CPLEX	なし

表 73. IBM Intelligent Operations Center のサービス停止順序の従属関係 (続き)

サービス	説明	このサービスの停止前に停止されている必要のあるサービス
ihc	HTTP Server for Runtime (アプリケーション・サーバー)	ihsevt、ihsmgt
ihsevt	HTTP Server for Runtime (イベント・サーバー)	なし
ihsmgt	HTTP Server for Runtime (管理サーバー)	なし
ncob	Tivoli Netcool/OMNibus	nci
nci	Tivoli Netcool/Impact	なし
wbm	IBM WebSphere Business Monitor	なし
st	Lotus Sametime	stpxy
stpxy	Lotus Sametime Proxy Application Server	なし
wpe	WebSphere Portal Extend	なし
wmb	WebSphere Message Broker	なし
cognos	IBM Cognos Business Intelligence	なし
tstrm	Tivoli Service Request Manager	なし
wodm	WebSphere Operations Decision Manager	なし
wodmhc	WebSphere Operations Decision Manager (Decision Center)	なし
smsclt	Semantic Model Services (クライアント・サービス)	なし
smsdaaq	Semantic Model Services (データ・サービス)	なし
smsmdl	Semantic Model Services (モデル・サービス)	なし
smsmgmt	Semantic Model Services (管理サービス)	なし
smsrtc	Semantic Model Services (RTC サービス)	なし
iocxml	IBM Intelligent Operations Center XML probe	なし

## サービス状況の照会

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスの状況を判別することができます。

### このタスクについて

**IOControl.sh** コマンドは、`ibmadmin` ユーザーとして実行する必要があります。 `ibmadmin` としてログオンしていない場合、`su - ibmadmin` コマンドを実行して `ibmadmin` ユーザーに切り替えます。

### 手順

IBM Intelligent Operations Center のすべてのサービスの状況を照会するには、管理サーバーで以下のコマンドを実行します。

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password
```

ここで、`password` は、プラットフォーム制御ツールのインストール時に定義されたプラットフォーム制御ツールのパスワードです。

1 つのサービスのみを検査するには、以下のコマンドを実行します。

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status service_ID password
```



ここで、*service\_ID* は、**IOControl** ヘルプの「ターゲット・オプション (Target Options)」にリストされている ID、*password* は プラットフォーム制御ツールのインストール時に定義されたプラットフォーム制御ツールのパスワードです。

## タスクの結果

開始されているサービスについては **[on]** と表示されます。開始されていないサービスについては **[off]** と表示されます。

## 次のタスク

**IOControl.sh** コマンドの実行後に、`/opt/IBM/ISP/mgmt/logs` ディレクトリーのログを確認します。ログには、**IOControl.sh** コマンドの結果が含まれています。

### 関連タスク:

216 ページの『サービスの開始』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサーバーで実行中のサービスを開始することができます。

219 ページの『サービスの停止』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスを停止できます。

『プラットフォーム制御ツールのヘルプの入手』

プラットフォーム制御ツールのアクションおよびターゲット・オプションに関する情報が使用可能になります。

55 ページの『プラットフォーム制御ツールのインストール』

プラットフォーム制御ツールは、IBM Intelligent Operations Center サーバー環境を管理するために使用されます。このツールは、本製品とは別にインストールします。

## プラットフォーム制御ツールのヘルプの入手

プラットフォーム制御ツールのアクションおよびターゲット・オプションに関する情報が使用可能になります。

## このタスクについて

**IOControl.sh** コマンドは、`ibmadmin` ユーザーとして実行する必要があります。 `ibmadmin` としてログオンしていない場合、`su - ibmadmin` コマンドを実行して `ibmadmin` ユーザーに切り替えます。

## 手順

**IOControl** コマンドのオプションを表示するには、管理サーバーで以下のいずれかのコマンドを実行します。

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh help
```

or

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh
```

## タスクの結果

**IOControl** コマンドのオプションが表示されます。

## 関連タスク:

216 ページの『サービスの開始』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサーバーで実行中のサービスを開始することができます。

219 ページの『サービスの停止』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスを停止できます。

222 ページの『サービス状況の照会』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスの状況を判別することができます。

---

## 管理コンソール

「管理コンソール」ポートレットを使用して、ソリューションによって提供されるサービスを管理します。

「管理コンソール」ポートレットにアクセスするには、WebSphere Portal 管理インターフェースで「**Intelligent Operations**」 > 「管理ツール」 > 「管理コンソール」をクリックします。

各サービスについて、「管理コンソール」ポートレット内のリンクを利用することで、管理コンソールにアクセスしたり、管理へのアクセス方法に関する情報を確認したりすることができます。

注: Microsoft Internet Explorer バージョン 8.0 を使用している場合は、レポート管理へのリンクで問題が発生する可能性があります。その場合、「要求されたリソースが見つかりません」という意味のメッセージが表示されます。解決策は、ブラウザのアドレス・フィールドで URL を編集して、ホスト名と /ServletGateway の間に /cognos を追加することです。

## アプリケーション・サーバー

表 74. アプリケーション・サーバーでの管理

コンソール	管理
アプリケーション・サーバー	IBM Intelligent Operations Center によって提供されるさまざまなサービスを管理するには、WebSphere Application Server の Web ベースのコンソールへのリンクを使用します。サーバーの制御、リソースおよびサービス・プロバイダーの管理、ホストおよびその他の環境設定の変更を行えます。
レポート管理	レポートのセットアップを行うには、IBM Cognos Connection の Web ベースのコンソールへのリンクを使用します。新規レポートの作成や、既存のレポートの変更が行えます。また、データ・ソースの構成、公開フォルダーや専用フォルダーのセットアップ、権限および配布の定義、レポートの自動実行のスケジュール作成なども行えます。

## データ・サーバー

表 75. データ・サーバーでの管理

コンソール	管理
データベース	DB2 Enterprise Server Edition を使用したデータベースの管理方法について詳しくは、インフォメーション・センターへのリンクを使用してください。 データベース・コントロール・センター GUI またはコマンド行を使用して作業を実行できます。

## イベント・サーバー

表 76. イベント・サーバーでの管理

コンソール	管理
連絡先	names.nsf データベースの現在の設定を表示するには、Lotus Domino サーバーの Web ベースのコンソールへのリンクを使用します。 names.nsf は、Lotus Domino サーバーを構成するために使用します。構成変更は、Domino Administration クライアントを使用して行えます。
連絡先管理	Domino Administration クライアントをダウンロードして Lotus Domino 連絡先管理のためにセットアップする方法について詳しくは、インフォメーション・センターへのリンクを使用してください。
イベント処理	オブジェクト・サーバー GUI を使用してイベント処理を管理するには、Tivoli Netcool/OMNibus の Web ベースのコンソールへのリンクを使用します。
イベント処理と拡張	イベント処理を管理するには、Tivoli Netcool/Impact の Web ベースのコンソールへのリンクを使用します。例えば、データベース接続、データ・ソース接続、イベント処理の開始、ポリシー状況、ログについて確認できます。
インスタント・メッセージ・サーバー	インスタント・メッセージを管理するには、Lotus Sametime コミュニティー・サーバーの Web ベースのコンソールへのリンクを使用します。
メッセージング・バス	WebSphere Message Broker を使用したメッセージの状況の確認方法について詳しくは、インフォメーション・センターへのリンクを使用してください。
標準操作手順の管理	リソースおよび標準操作手順を定義するには、Tivoli Service Request Manager Start Center用の Web ベースのコンソールへのリンクを使用します。 イベント管理に使用可能なリソースおよびアクティビティの定義は、IBM Intelligent Operations Center で行えます。
標準操作手順 アプリケーション・サーバー	管理するには、WebSphere Application Server の Web ベースのコンソールへのリンクを使用します。これによって Tivoli Service Request Manager が提供されます。

## 管理サーバー

表 77. 管理サーバーでの管理

コンソール	管理
アプリケーション・モニター	アプリケーション・モニターを管理するには、Tivoli Monitoring の Web ベースのコンソールへのリンクを使用します。このコンソールを使用してシステム・ヘルス・チェックが行えます。
管理用アプリケーション・サーバー	統合アプリケーションを管理するには、WebSphere Application Server の Web ベースのコンソールへのリンクを使用します。この管理には、Tivoli Access Manager と WebSEAL を使用したセキュリティー管理が含まれます。
データベース	DB2 Enterprise Server Edition を使用したデータベースの管理方法について詳しくは、インフォメーション・センターへのリンクを使用してください。データベース・コントロール・センター GUI またはコマンド行を使用して作業を実行できます。
ディレクトリー	ユーザーのディレクトリーを管理するには、Tivoli Directory Server の Web ベースのコンソールへのリンクを使用します。Tivoli Directory Server の Web ベースのコンソールの使用方法について詳しくは、インフォメーション・センターのリンクを使用してください。

### 「管理コンソール」ポートレットのカスタマイズ

このポートレットはカスタマイズすることができます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

#### 関連資料:

163 ページの『「管理コンソール」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「管理コンソール」ポートレットをカスタマイズできます。

#### 関連情報:

 [IBM Lotus Domino および Lotus Notes インフォメーション・センター](#)

 [IBM DB2 データベース・インフォメーション・センター](#)

 [IBM Tivoli Directory Server インフォメーション・センター](#)

## サービスの管理

「管理コンソール」ポートレットは、ソリューションによって提供されるサービスを管理できる場所、またはサービスの管理に関するさらに詳細な情報を検索できる場所へのリンクを提供します。

## アプリケーション・サーバー

### アプリケーション・サーバー・サービス

共通の Web ベース・コンソール Integrated Solutions Console で、以下のような多種多様なアプリケーション管理タスクを実行することができます。

- サーバーのステータスの確認
- サーバーおよびクラスターの開始および停止
- アプリケーションまたはパッチのデプロイ
- 使用可能なポートレットのリストの管理
- サービスのモニター
- アプリケーション・サービス・ポリシーの処理
- REST サービス・プロバイダーなど、サービス・プロバイダーの管理
- リソースの管理
- アプリケーションのセキュリティーの管理
- 仮想ホストおよびその他の環境設定の処理
- システム管理の実行
- サービス統合の管理
- HTTP サーバーの管理
- ログイングおよびトレースの管理

アプリケーション・サービスについて詳しくは、Integrated Solutions Console のオンライン・ヘルプを参照するか、アプリケーション・サーバーのセクションの末尾にある WebSphere Application Server インフォメーション・センターへのリンクを参照してください。


### レポート管理サービス

IBM Intelligent Operations Center 内でのレポートの提供に関連するすべてのタスクで、Web ベースのレポート管理コンソールを使用できます。

- データ・ソースのセットアップ
- レポートの作成、編集、および削除
- レポートへのアクセスの管理
- レポートのスケジュール
- レポートの配布のセットアップ

レポート管理サービスについて詳しくは、アプリケーション・サーバーのセクションの末尾にある IBM Cognos Business Intelligence インフォメーション・センターへのリンクを参照してください。

## 関連情報:

 [WebSphere Application Server バージョン 7.0 インフォメーション・センター](#)

 [IBM Cognos Business Intelligence インフォメーション・センター](#)

## データ・サーバー

### データベース・サービス

データ・サーバーでホストされるデータベース・サービス・インスタンスを介して、IBM Intelligent Operations Center データベースを管理できます。データベース・サービス・インスタンスは、サーバー上で実行される分離した独立処理です。1つのインスタンスが複数のデータベースをホストすることができます。各インスタンスには名前 *instance-name* があります。以下のインスタンスは、データ・サーバーでホストされます。

表 78. データ・サーバーでホストされるデータベース・インスタンス

インスタンス	使用側
dsrdbm01	ディレクトリー・サービス
db2inst1	ソリューション用に予約済み
db2inst2	ポータル・サーバー
db2inst3	レポート管理
db2inst4	ビジネス・ルールおよびビジネス・モニター・サービス
db2inst5	セマンティック・モデル・サービス
db2inst6	標準操作手順の管理サービス
db2inst7	ID 管理サービス
db2inst8	アプリケーション用に予約済み

端末ウィンドウからインスタンスを管理するには、以下のようにします。

1. *instance-name* ユーザーとしてログインします。
2. **db2** コマンドを実行してコマンド・モードに入ります。
3. **?** を入力して、使用可能なコマンドのリストを表示します。多くのコマンドでは、データベースへのアクティブな接続が必要です。
  - インスタンスに使用可能なデータベースを表示するには、**list database directory** コマンドを実行します。
  - データベースに接続するには、**connect to database\_name** コマンドを実行します。
4. データベースから切断してプロンプト・コマンド・モードを終了するには、**terminate** コマンドを実行します。

データベースサービスについて詳しくは、データ・サーバーのセクションの末尾にある DB2 データベース・インフォメーション・センターへのリンクを参照してください。



## 関連情報:

 IBM DB2 データベース・インフォメーション・センター

## イベント・サーバー

### 連絡先、連絡先管理、およびインスタント・メッセージ・サービス

以下の方法で、連絡先、連絡先管理、インスタント・メッセージ・サービスを管理できます。

- Lotus Domino Server コンソールで現在の連絡先を表示する。
- Lotus Domino Administration Client で、シングル・サインオンを構成し、インスタント・メッセージ・サーバー、および Lotus Sametime Clientを管理する。
- Lotus Sametime Community Server でインスタント・メッセージ・サーバーの使用可能性をログに記録し、確認する。

注: Lotus Domino Server コンソールに表示される連絡先は、「連絡先」ポートレットのみに適用されるものであり、IBM Intelligent Operations Center ユーザーと同じではありません。

連絡先、連絡先管理、およびインスタント・メッセージ・サービスについては、イベント・サーバーのセクションの末尾にある Lotus Domino および Lotus Notes インフォメーション・センターへのリンクを参照してください。

## イベント処理サービス

Tivoli Netcool/OMNIBUS オブジェクト・サーバー GUI を使用して、IBM Intelligent Operations Center のイベントの収集と保管を管理できます。

1. X Window System 対応の端末セッションを開きます。
2. root としてサーバーにログオンします。
3. /opt/IBM/netcool/omnibus ディレクトリーに移動します。
4. GUI アプリケーションを開くには、bin/nc\_config コマンドを実行します。

イベント処理サービスについては、イベント・サーバーのセクションの末尾にある Tivoli Netcool/Impact インフォメーション・センターへのリンクを参照してください。

## イベント処理と拡張サービス

Tivoli Netcool/Impact の Web ベースのコンソールを使用して、以下のようなイベント処理を管理することができます。

- データベースおよびデータ・ソース接続の確認
- EventProcessor が実行されているかどうかの確認
- 既存のポリシーのロギングの確認、およびログ・レベルの更新
- 既存のポリシーの更新、または新規ポリシーの作成

イベント処理と拡張サービスについては、イベント・サーバーのセクションの末尾にある Tivoli Netcool/Impact インフォメーション・センターへのリンクを参照してください。

## メッセージング・バス

メッセージング・バス・サービスを管理する 3 つの主な方法は以下のとおりです。

- コマンド行

- エクスプローラー: Eclipse ベースの管理アプリケーション
- ツールキット: 管理とアプリケーション開発の両方ができる Eclipse ベースのアプリケーション

GUI 開発ツールを使用して、通信フロー、定義テスト、変換、統合、およびロギングを管理することができます。

IBM Intelligent Operations Center には WebSphere Message Broker Toolkit が用意されています。このツールキットのインストールおよび使用については、イベント・サーバーのセクションの末尾にある WebSphere Message Broker インフォメーション・センターへのリンクを参照してください。

コマンド行環境をセットアップし、WebSphere Message Broker インスタンスを照会するには、以下のようになります。

- ユーザー mqm としてサーバーにログオンします。
- /opt/IBM/mqsi/8.0.0.0 ディレクトリーに移動します。
- 環境をセットアップするには、source bin/mqsiprofile コマンドを実行します。
- WebSphere Message Broker インスタンスを照会するには、bin/mqsilist コマンドを実行します。

メッセージング・バス・サービスについては、イベント・サーバーのセクションの末尾にある WebSphere Message Broker インフォメーション・センターへのリンクを参照してください。

### **標準操作手順管理サービス**

Web ベースの標準操作手順の管理コンソールである Tivoli Service Request Manager スタート・センターを使用して、イベントを管理するリソースおよびアクティビティを定義することができます。

標準操作手順の管理サービスについては、イベント・サーバーのセクションの末尾にある Tivoli Service Request Manager インフォメーション・センターへのリンクを参照してください。

### **標準操作手順アプリケーション・サービス**

Tivoli Service Request Manager のサーバーとして機能する WebSphere Application Server の Web ベースのコンソールを使用して、リソースおよびアクティビティに関連するアプリケーションを管理することができます。

標準操作手順アプリケーション・サービスについては、オンライン・ヘルプを参照するか、アプリケーション・サーバーのセクションの末尾にある WebSphere Application Server バージョン 7.0 インフォメーション・センターへのリンクを参照してください。

## 関連概念:

138 ページの『Tivoli Service Request Managerの構成』

Tivoli Service Request Manager ユーザー・インターフェースでは、標準操作手順、ワークフロー、およびリソースを管理できます。

## 関連情報:



IBM Lotus Domino および Lotus Notes インフォメーション・センター



IBM Tivoli Netcool/Impact インフォメーション・センター



IBM WebSphere Message Broker インフォメーション・センター



IBM Tivoli Service Request Manager インフォメーション・センター

## 管理サーバー

### アプリケーション・モニター・サービス

Tivoli Monitoring の Web ベースのコンソールを使用して、アプリケーション・モニターを管理することができます。アプリケーションをダウンロードして実行することで、サーバーの状況を確認し、実行中のすべてのモニター・エージェントを表示できます。ログオンするには、ユーザー ID とパスワードを入力します。デフォルトのユーザー ID は sysadmin で、パスワードはインストール時に入力されたトポロジー・パスワードです。

アプリケーション・モニター・サーバーについて詳しくは、このトピックの末尾にある「Tivoli Enterprise Portal ユーザーズ・ガイド (Tivoli Enterprise Portal User's Guide)」へのリンクを参照してください。

### 管理サービス用のアプリケーション・サーバー

Tivoli Access Manager WebSEAL のジャンクションを共通 Web ベース・コンソールである Integrated Solutions Console で管理することができます。

このサービスについて詳しくは、オンライン・ヘルプを参照するか、アプリケーション・サーバーのセクションの末尾にある WebSphere Application Server バージョン 7.0 インフォメーション・センターへのリンクを参照してください。

### データベース・サービス

管理サーバーでホストされる データベース・サービス・インスタンスが 1 つあります。db2inst2 です。このインスタンスは、Tivoli Access Manager のシステム管理および固有データ・ストレージに使用できます。

データベース・サービスについて詳しくは、データ・サーバーのセクションの末尾にある IBM DB2 データベース・インフォメーション・センターへのリンクを参照してください。

### ディレクトリー・サービス

Tivoli Directory Server の Web ベースのコンソールを使用してユーザー・ディレクトリーを管理し、LDAP 内のユーザーを表示、追加、または変更することができます。

ディレクトリー・サービスについて詳しくは、このトピックの末尾にある Tivoli Directory Server インフォメーション・センターへのリンクを参照してください。

## 関連情報:



IBM Tivoli Monitoring Tivoli Enterprise Portal ユーザーズ・ガイド



IBM Tivoli Directory Server インフォメーション・センター

---

## コンポーネントの検証

システム検査チェックツールは、IBM Intelligent Operations Center 内のコンポーネントをテストし、アクセス可能であるか、および操作可能であるかを判別します。

## システム検査チェック・ツールの使用方法

システム検査チェック・ツールは、IBM Intelligent Operations Center システムから成るサービスの運用状況を判別するために使用します。

### このタスクについて

システム検査チェック・ツールはシステムの機能を検証します。




テストが失敗した場合のトラブルシューティングと個々のテストの詳細については、そのテストの「ヘルプ」をクリックします。

「プロパティ」には、IBM ソフトウェア・サポートに連絡する際に使用する、テストの追加情報が示されます。

### 手順

1. 管理者権限を持つユーザーとして IBM Intelligent Operations Center にログオンします。
2. 「Intelligent Operations」 > 「管理ツール」 > 「システム検査チェック」をクリックします。
3. 以下のいずれかを行って、実行対象のテストを 1 つまたは複数選択します。
  - 実行対象の特定のテストをクリックします。
  - 「すべてのテストを実行」をクリックして、選択したすべての機能をテストします。

### タスクの結果

テストが正常に完了すると、 アイコンが表示されます。テストが失敗すると、 アイコンが表示されます。テストが失敗した場合、エラーを解決するためにテストの問題判別の指示に従います。これらの指示は、 アイコンまたは「ヘルプ」をクリックしてアクセスすることもできます。

特定のテストが実行された場合は、テストの実行結果がテストの実行時間とともにポートレットの下部に表示されます。「すべてのテストを実行」が選択された場合は、この情報は表示されません。

### 次のタスク

このツールは、「リセット」をクリックすることにより、リセットされて結果をすべてクリアできます。

## 関連タスク:

58 ページの『インストールの検証』

IBM Intelligent Operations Center のインストール後に、製品が正常にインストールされたことを確認します。

56 ページの『システム検査チェック・ツールのインストール』

システム検査チェック・ツールを使用して、IBM Intelligent Operations Center 内のコンポーネントの運用状況を検査することができます。このツールは、本製品とは別にインストールします。

## システム検査チェック・テスト

IBM Intelligent Operations Center は、さまざまな IBM Intelligent Operations Center のサービスおよびコンポーネントの運用状況を判断するために使用できる、いくつかのシステム検査チェック・テストを提供します。

これらのテストは、コラボレーションやモニターなどの機能ごとに、論理的にグループ化されています。

## アカウント管理 (Tivoli Identity Manager API) テスト

アカウント管理 (Tivoli Identity Manager API) テストは、IIOP ポートにアクセスして、Tivoli Identity Manager API へのアクセスをテストします。

## リソース

アカウント管理 (Tivoli Identity Manager API) テストでは、以下のリソースを使用します。

- (管理サーバー上の) Tivoli Identity Manager Server

## 問題判別

アカウント管理 (Tivoli Identity Manager API) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. アプリケーション・サーバーと管理サーバーの間にネットワーク接続があることを確認します。これを行うには、アプリケーション・サーバーで、管理サーバーの短縮ホスト名と完全修飾ホスト名の両方を指定して、**ping** コマンドを送信します。**ping** コマンドの結果は、ホスト名が DNS または `/etc/hosts` ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. 管理サーバーでは、以下の Tivoli Identity Manager ログを確認します。
    - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log`
    - `/opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log`
    - `/var/idsldap/` ディレクトリーの `V6` サブディレクトリーにあるすべてのログ
3. アプリケーション・サーバーおよび管理サーバーのファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
4. Tivoli Identity Manager サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。

- a. 管理サーバー・システムで、ibmadmin としてログオンします。
- b. コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
- c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh コマンドを使用して、nodeagent を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。
- a. メッセージ「ADMU0509I: The Application Server "timServer1" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1 コマンドを使用して、timServer1 を始動します。メッセージ「ADMU0508I: The Application Server "timServer1" is STARTED.」が表示された場合、このステップを省略します。timServer1 を始動する必要があった場合、次のようなメッセージが表示されます。ADMU3000I: Server timserver open for e-business; process id is 26654

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. timServer1

以下の順序でサーバーを停止します。


- a. timServer1
- b. nodeagent


timServer1 サーバーを停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

nodeagent を停止するには、管理サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

5. Tivoli Identity Manager サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。

- a. [http://MANAGEMENT\\_SERVER\\_HOST:9060/admin](http://MANAGEMENT_SERVER_HOST:9060/admin) で、WebSphere Application Server の管理 ID である admin およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。MANAGEMENT\_SERVER\_HOST は、管理サーバーのホスト名です。
- b. 「サーバー」 > 「サーバー・タイプ」 > 「**WebSphere Application Server**」をクリックして、timServer1 サーバーの状況を表示します。

 アイコンは、サーバーが開始済みであることを示します。必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。

 アイコンは、サーバーが停止していることを示します。サーバーを選択して「開始」をクリックし、サーバーを開始してください。



② アイコンは、サーバー状況が使用不可であることを示します。 ノード・エージェントが実行されていない可能性があります。ノード・エージェントを開始するには、コマンド・ウィンドウで `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. timServer1

以下の順序でサーバーを停止します。

- a. timServer1
- b. nodeagent

timServer1 サーバーを停止するには、サーバーを選択して「**停止**」をクリックします。

nodeagent を停止するには、管理サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

6. 次の URL を使用して、アプリケーション・サーバーにおいて、WebSphere Portal システムから Tivoli Identity Manager コンソールにアクセスできることを確認してください。 `http://MANAGEMENT_SERVER_HOST:9080/itim/console/main`。 `MANAGEMENT_SERVER_HOST` は、管理サーバーのホスト名です。ユーザー ID `itim manager` でログオンします。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## アカウント管理 (Tivoli Identity Manager コンソール) テスト

アカウント管理 (Tivoli Identity Manager コンソール) テストは、Tivoli Identity Manager Administration URL にアクセスして、Tivoli Identity Manager がアクセス可能かどうか判別します。

## リソース

アカウント管理 (Tivoli Identity Manager コンソール) テストでは、以下のリソースを使用します。

- (管理サーバー上の) Tivoli Identity Manager Server

## 問題判別

アカウント管理 (Tivoli Identity Manager コンソール) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. アプリケーション・サーバーと管理サーバーの間にネットワーク接続があることを確認します。これを行うには、アプリケーション・サーバーで、管理サーバーの短縮ホスト名と完全修飾ホスト名の両方を指定して、`ping` コマンドを送信します。 `ping` コマンドの結果は、ホスト名が DNS または `/etc/hosts` ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。

- /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
  - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
- b. 管理サーバーでは、以下の Tivoli Identity Manager ログを確認します。
- /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log
  - /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log
  - /var/idsldap/ ディレクトリーの V6 サブディレクトリーにあるすべてのログ
3. アプリケーション・サーバーおよび管理サーバーのファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
4. Tivoli Identity Manager サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。
- a. 管理サーバー・システムで、ibmadmin としてログオンします。
- b. コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
- c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh コマンドを使用して、nodeagent を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。
- a. メッセージ「ADMU0509I: The Application Server "timServer1" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startServer.sh timServer1 コマンドを使用して、timServer1 を始動します。メッセージ「ADMU0508I: The Application Server "timServer1" is STARTED.」が表示された場合、このステップを省略します。timServer1 を始動する必要があった場合、次のようなメッセージが表示されません。ADMU3000I: Server timserver open for e-business; process id is 26654

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。




- a. nodeagent
- b. timServer1

以下の順序でサーバーを停止します。

- a. timServer1
- b. nodeagent

timServer1 サーバーを停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopServer.sh timServer1 -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

nodeagent を停止するには、管理サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

5. Tivoli Identity Manager サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。
  - a. `http://MANAGEMENT_SERVER_HOST:9060/admin` で、WebSphere Application Server の管理 ID である `admin` およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。 `MANAGEMENT_SERVER_HOST` は、管理サーバーのホスト名です。
  - b. 「サーバー」 > 「サーバー・タイプ」 > 「**WebSphere Application Server**」をクリックして、`timServer1` サーバーの状況を表示します。
    -  アイコンは、サーバーが開始済みであることを示します。 必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。
    -  アイコンは、サーバーが停止していることを示します。 サーバーを選択して「開始」をクリックし、サーバーを開始してください。
    -  アイコンは、サーバー状況が使用不可であることを示します。 ノード・エージェントが実行されていない可能性があります。 ノード・エージェントを開始するには、コマンド・ウィンドウで `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/startNode.sh` コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. `nodeagent`
- b. `timServer1`

以下の順序でサーバーを停止します。

- a. `timServer1`
- b. `nodeagent`

`timServer1` サーバーを停止するには、サーバーを選択して「停止」をクリックします。

`nodeagent` を停止するには、管理サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/timProfile/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

6. 次の URL を使用して、アプリケーション・サーバーにおいて、WebSphere Portal システムから Tivoli Identity Manager コンソールにアクセスできることを確認してください。 `http://MANAGEMENT_SERVER_HOST:9080/itim/console/main`。 `MANAGEMENT_SERVER_HOST` は、管理サーバーのホスト名です。 ユーザー ID `itim manager` でログオンします。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## アカウント管理 (Tivoli Directory Integrator のリストのアセンブリー) テスト

アカウント管理 (Tivoli Directory Integrator のリストのアセンブリー) テストでは、Tivoli Directory Integrator リスト・アセンブリー・リソースが使用可能であるかどうかを判別します。 これを行うには、管理サーバーで `tdisrvctl` コマンドを実行します (このコマンドは、構成、アセンブリー・ライン、およびその他の機能をリモート管理)。テストでは、返す対象の `---- AssemblyLines ----` を検索します。

## リソース

アカウント管理 (Tivoli Directory Integrator のリストのアセンブリー) テストでは、以下のリソースを使用します。

- Tivoli Directory Server (データ・サーバー上)
- Tivoli Directory Integrator (管理サーバー上)

## 問題判別

アカウント管理 (Tivoli Directory Integrator のリストのアセンブリー) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. アプリケーション・サーバーとデータ・サーバーの間にネットワーク接続があることを確認します。これを行うには、アプリケーション・サーバーで、データ・サーバーの短縮ホスト名と完全修飾ホスト名の両方を指定して、**ping** コマンドを送信します。 **ping** コマンドの結果は、ホスト名が **DNS** または **/etc/hosts** ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の **WebSphere Portal** ログを確認します。
    - **/opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log**
    - **/opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log**
3. データ・サーバー・システムおよびアプリケーション・サーバー・システムのファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
4. Tivoli Directory Integrator サーバー が実行されていることを確認します。
  - a. 管理サーバーの端末セッションに **ibmadmin** としてログオンします。
  - b. **ps -ef | grep ibmdisrv** コマンドを実行します。結果は以下のようになります。

```
ibmadmin    11411      1  0 Sep06 pts/1    00:00:00 /bin/sh /opt/IBM/TDI/V7.1/ibmdisrv -s /opt/IBM/TDI/V7.1/timsol -c ITIM_RMI.xml -d
ibmadmin    32080 19149  0 23:17 pts/1    00:00:00 grep ibmdisrv
```

この例は、Tivoli Directory Integrator のサーバー・デーモン (**ibmdisrv**) が実行されていることを示しています。

5. Tivoli Directory Integrator サーバー (**ibmdisrv**) が実行されていない場合、これを始動します。
  - a. 管理サーバーの端末セッションに **root** としてログオンします。
  - b. **/etc/init.d/ITIMAd start** を実行します。
6. Tivoli Directory Server (LDAP サーバー) が実行されていることを確認してください。
  - a. データ・サーバーの端末セッションに **root** としてログオンします。
  - b. **ps -ef | grep ibmslapd** コマンドを実行します。結果は以下のようになります。

```
dsrdbm01 13797      1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root      32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
```

この例は、Tivoli Directory Server デーモンの **ibmslapd** が実行されていることを示します。

- c. **ps -ef | grep ibmdiradm** コマンドを実行します。結果は以下のようになります。

```
root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
dsrdbm01 11055      1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

この例は、Tivoli Directory Server デーモンの **ibmdiradm** が実行されていることを示します。

7. Tivoli Directory Server の **ibmslapd** が実行されていない場合、以下を行います。

- a. Linux の `root` ユーザーとして `/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01` を実行して Tivoli Directory Server を始動します。
8. Tivoli Directory Administration Server の `ibmdiradm` が実行されていない場合、以下を行います。
  - a. データ・サーバーの端末セッションで `su - dsrdbm01` を実行します。
  - b. `/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t` を実行してアプリケーション・サーバーを開始します。
9. Tivoli Directory Server の `ibmslapd` が実行されている場合、以下を行います。
 

注: このステップは、Tivoli Directory Server が前のステップで始動されている場合でも行います。

  - a. データ・サーバーの端末セッションに `dsrdbm01` としてログオンします。
  - b. `idsldapsearch -h localhost -D "cn=root" -w "ADMIN_PASSWORD" -s sub uid=*` を実行します。ここでの `ADMIN_PASSWORD` は LDAP の `root` 管理者のアカウント・パスワードです。既存の LDAP ユーザー・オブジェクトが表示されます。
10. Tivoli Directory Server Web Administration Tool が実行されていることを確認してください。Tivoli Directory Server Web Administration Tool は、LDAP インスタンスの停止と開始を行い、ユーザーまたはアカウントを追加し、ログ・ファイルを表示するために使用されます。
  - a. 管理サーバーの端末セッションに `ibmadmin` としてログオンします。
  - b. `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PASSWORD` コマンドを管理サーバー上で実行します。ここでの `WAS_ADMIN_PASSWORD` は WebSphere Application Server の管理者パスワードです。このツールを実行すると、以下のようなメッセージが返されます。
 

```
ADMU0508I: The Application Server "tdsServer" is STARTED
```

以下のメッセージが返された場合、`tdsServer` を始動する必要があります。

```
ADMU0509I: The Application Server "tdsServer" cannot be reached. It appears to be stopped.
```
  - c. `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer` コマンドを実行して、`tdsServer` を始動します。`tdsServer` サーバーが始動されて、以下のようなメッセージが表示されます。
 

```
ADMU3000I: Server tdsServer open for e-business; process id is 26654
```
11. `http://MANAGEMENT_SERVER_HOST:9062/IDSWebApp/IDSjsp/Login.jsp` で、Tivoli Directory Server Web Administration Tool にアクセスします。ここでの `MANAGEMENT_SERVER_HOST` は管理サーバーのホスト名です。
12. LDAP の `root` 管理者アカウント (`cn=root`) および適切なパスワードを指定してログオンします。LDAP サーバー名は `DATABASE_DIRECTORY_SERVER_HOST:389` にする必要があります。ここでの `DATABASE_DIRECTORY_SERVER_HOST` はデータ・サーバーのホスト名です。
13. 「サーバー管理」 > 「サーバーの始動/停止/リセット」をクリックします。LDAP サーバー状況が表示されます。また、このページを使用して LDAP サーバーを始動、停止、またはリセットすることもできます。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## アカウント管理 (Tivoli Directory Server) テスト

アカウント管理 (Tivoli Directory Server) テストでは、サーバーに HTTP 要求を送信することで、Tivoli Directory Server が使用可能であるかどうかを判別します。



## リソース

アカウント管理 (Tivoli Directory Server) テストでは、以下のリソースを使用します。

- Tivoli Directory Server (データ・サーバー上)

## 問題判別

**Tivoli Directory Server** の HTTP テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  2. データ・サーバー上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
  3. Tivoli Directory Server (LDAP サーバー) が実行されていることを確認してください。
    - a. データ・サーバーの端末セッションに **root** としてログオンします。
    - b. **ps -ef | grep ibmslapd** コマンドを実行します。結果は以下のようになります。

```
dsrdbm01 13797      1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root      32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
```

この例は、Tivoli Directory Server デーモンの **ibmslapd** が実行されていることを示します。

- c. **ps -ef | grep ibmdiradm** コマンドを実行します。結果は以下のようになります。

```
root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
dsrdbm01 11055      1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

この例は、Tivoli Directory Server デーモンの **ibmdiradm** が実行されていることを示します。

4. Tivoli Directory Server の **ibmslapd** が実行されていない場合、以下を行います。
  - a. Linux の **root** ユーザーとして **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** を実行して Tivoli Directory Server を始動します。
5. Tivoli Directory Administration Server の **ibmdiradm** が実行されていない場合、以下を行います。
  - a. データ・サーバーの端末セッションで **su - dsrdbm01** を実行します。
  - b. **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** を実行してアプリケーション・サーバーを開始します。
6. Tivoli Directory Server の **ibmslapd** が実行されている場合、以下を行います。

注: このステップは、Tivoli Directory Server が前のステップで始動されている場合でも行います。

- a. データ・サーバーの端末セッションに **dsrdbm01** としてログオンします。
  - b. **idsldapsearch -h localhost -D "cn=root" -w "ADMIN\_PASSWORD" -s sub uid=\*** を実行します。ここでの **ADMIN\_PASSWORD** は LDAP の **root** 管理者のアカウント・パスワードです。既存の LDAP ユーザー・オブジェクトが表示されます。
7. Tivoli Directory Server Web Administration Tool が実行されていることを確認してください。Tivoli Directory Server Web Administration Tool は、LDAP インスタンスの停止と開始を行い、ユーザーまたはアカウントを追加し、ログ・ファイルを表示するために使用されます。
    - a. 管理サーバーの端末セッションに **ibmadmin** としてログオンします。



- b. `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PASSWORD` コマンドを管理サーバー上で実行します。ここでの `WAS_ADMIN_PASSWORD` は WebSphere Application Server の管理者パスワードです。このツールを実行すると、以下のようなメッセージが返されます。

```
ADMU0508I: The Application Server "tdsServer" is STARTED
```

以下のメッセージが返された場合、tdsServer を始動する必要があります。

```
ADMU0509I: The Application Server "tdsServer" cannot be reached. It appears to be stopped.
```

- c. `/opt/IBM/WebSphere/AppServer/profiles/tdsProfile/bin/startServer.sh tdsServer` コマンドを実行して、tdsServer を始動します。tdsServer サーバーが始動されて、以下のようなメッセージが表示されます。

```
ADMU3000I: Server tdsServer open for e-business; process id is 26654
```

8. `http://MANAGEMENT_SERVER_HOST:9062/IDSWebApp/IDSjsp/Login.jsp` で、Tivoli Directory Server Web Administration Tool にアクセスします。ここでの `MANAGEMENT_SERVER_HOST` は管理サーバーのホスト名です。
9. LDAP の root 管理者アカウント (cn=root) および適切なパスワードを指定してログオンします。LDAP サーバー名は `DATABASE_DIRECTORY_SERVER_HOST:389` にする必要があります。ここでの `DATABASE_DIRECTORY_SERVER_HOST` はデータ・サーバーのホスト名です。
10. 「サーバー管理」 > 「サーバーの始動/停止/リセット」をクリックします。LDAP サーバー状況が表示されます。また、このページを使用して LDAP サーバーを始動、停止、またはリセットすることもできます。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## 分析 (Cognos ゲートウェイ・コンソール) テスト

分析 (Cognos ゲートウェイ・コンソール) テストでは、Cognos Servlet Gateway および Cognos Administration Portal URL を使用して、アプリケーション・サーバー上の Cognos にアクセスできるかどうかを判別します。

## リソース

分析 (Cognos ゲートウェイ・コンソール) テストでは、以下のリソースを使用します。

- Cognos (アプリケーション・サーバー・システム上)。

## 問題判別

分析 (Cognos ゲートウェイ・コンソール) テストが失敗した場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. アプリケーション・サーバーでは、以下の Cognos ログを確認します。
    - `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Disp1/SystemOut.log`

- /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX\_Displ/SystemErr.log
  - /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX\_GW1/SystemOut.log
  - /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX\_GW1/SystemErr.log
  - /opt/IBM/cognos/c10\_64/logs/ ディレクトリーにあるすべてのログ
2. アプリケーション・サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
  3. Cognos Dispatcher サーバーおよび Cognos Gateway サーバーが始動されていることを確認します。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。
    - a. アプリケーション・サーバー・システムで、cgnsadm (Cognos ユーザー) としてログオンします。
    - b. コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
    - c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、コマンド (/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh) を使用して、この nodeagent を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。
    - d. メッセージ「ADMU0509I: The Application Server "CognosX\_Displ" cannot be reached. It appears to be stopped.」が表示された場合、コマンド (/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX\_Displ) を使用して CognosX\_Displ を始動します。メッセージ「ADMU0508I: The Application Server "CognosX\_Displ" is STARTED.」が表示された場合、このステップはスキップします。CognosX\_Displ を始動する必要があった場合、「ADMU3000I: Server CognosX\_Displ open for e-business; process id is 26654」のようなメッセージが表示されます。
    - e. メッセージ「ADMU0509I: The Application Server "CognosX\_GW1" cannot be reached. It appears to be stopped.」が表示された場合、コマンド (/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startServer.sh CognosX\_GW1) を使用して CognosX\_GW1 を始動します。メッセージ「ADMU0508I: The Application Server "CognosX\_GW1" is STARTED.」が表示された場合、このステップはスキップします。CognosX\_GW1 を始動する必要があった場合、「ADMU3000I: Server CognosX\_GW1 open for e-business; process id is 26676」のようなメッセージが表示されます。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. CognosX\_Displ
- c. CognosX\_GW1




以下の順序でサーバーを停止します。

- a. CognosX\_GW1
- b. CognosX\_Displ
- c. nodeagent

アプリケーション・サーバーのコマンド・ウィンドウでコマンド (/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX\_GW1 -username waswebadmin -password WAS\_ADMIN\_PWD) を実行することで、CognosX\_GW1 サーバーが停止します。WAS\_ADMIN\_PWD は、WebSphere の管理者パスワードです。

アプリケーション・サーバーのコマンド・ウィンドウでコマンド (/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopServer.sh CognosX\_Displ -wasadmin admin -password WAS\_ADMIN\_PWD) を実行することで、CognosX\_Displ サーバーが停止します。WAS\_ADMIN\_PWD は、WebSphere の管理者パスワードです。

アプリケーション・サーバーのコマンド・ウィンドウでコマンド (/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD) を実行することで、nodeagent が停止します。WAS\_ADMIN\_PWD は、WebSphere の管理者パスワードです。

4. Cognos Dispatcher サーバーおよび Cognos Gateway サーバーが始動されていることを確認します。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。
  - a. `http://APPLICATION_SERVER_HOST:9060/admin` で、WebSphere Application Server の管理 ID である `admin` およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。`APPLICATION_SERVER_HOST` は、アプリケーション・サーバーのホスト名です。
  - b. 「サーバー」 > 「サーバー・タイプ」 > 「**WebSphere Application Server**」をクリックして、CognosX-Disp1 サーバーおよび CognosX\_GW1 サーバーの状況を確認します。
    -  アイコンは、サーバーが開始済みであることを示します。必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。
    -  アイコンは、サーバーが停止していることを示します。サーバーを選択して「開始」をクリックし、サーバーを開始してください。
    -  アイコンは、サーバー状況が使用不可であることを示します。ノード・エージェントが実行されていない可能性があります。ノード・エージェントを開始するには、コマンド・ウィンドウで `/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/startNode.sh` コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. CognosX\_Displ
- c. CognosX\_GW1

以下の順序でサーバーを停止します。

- a. CognosX\_GW1
- b. CognosX\_Displ
- c. nodeagent

CognosX\_GW1 サーバーおよび CognosX\_Displ サーバーを停止するには、サーバーを選択して「停止」をクリックします。

アプリケーション・サーバーのコマンド・ウィンドウでコマンド (/opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD) を実行することで、nodeagent が停止します。WAS\_ADMIN\_PWD は、WebSphere の管理者パスワードです。

- アプリケーション・サーバーにおいて、URL (http://APPLICATION\_SERVER\_HOST:9081/ServletGateway/servlet/Gateway) を使用して、WebSphere Portal システムから Cognos Administration Portal にアクセスできることを確認します。APPLICATION\_SERVER\_HOST は アプリケーション・サーバー のホスト名です。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## アプリケーション・サーバー (WebSphere Application Server Web サービス) テスト

アプリケーション・サーバー (WebSphere Application Server Web サービス) テストは、DrpGeoSvc Web サービスにアクセスして、WebSphere Application Server Web サービスへのアクセスをテストします。

## リソース

アプリケーション・サーバー (WebSphere Application Server Web サービス) テストでは、以下のリソースを使用します。

- (アプリケーション・サーバー上の) WebSphere Application Server。

## 問題判別

アプリケーション・サーバー (WebSphere Application Server Web サービス) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

- 実行時例外については、ログ・ファイルを確認してください。
  - アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - アプリケーション・サーバーでは、以下の WebSphere UDDI Registry 構成ログを確認します。
    - /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemErr.log
- アプリケーション・サーバー 上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
- cpudServer1 サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。
  - アプリケーション・サーバー・システムで、ibmadmin としてログオンします。
  - コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
  - メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/startNode.sh コマンドを使用して、nodeagent を始動します。メッセージ「ADMU0508I: The

Application Server "nodeagent" is STARTED.]が表示された場合、このステップはスキップします。 nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。

- a. メッセージ「ADMU0509I: The Application Server "cpudServer1" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1 コマンドを使用して、cpudServer1 を始動します。メッセージ「ADMU0508I: The Application Server "cpudServer1" is STARTED.」が表示された場合、このステップを省略します。 cpudServer1 を始動する必要があった場合、次のようなメッセージが表示されず。ADMU3000I: Server cpudServer1 open for e-business; process id is 26654

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。




- a. nodeagent
- b. cpudServer1

以下の順序でサーバーを停止します。

- a. cpudServer1
- b. nodeagent

cpudServer1 サーバーを停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

4. cpudServer1 サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。
  - a. [http://APPLICATION\\_SERVER\\_HOST:9060/admin](http://APPLICATION_SERVER_HOST:9060/admin) で、WebSphere Application Server の管理 ID である admin およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。APPLICATION\_SERVER\_HOST はアプリケーション・サーバーのホスト名です。
  - b. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Server」をクリックして、cpudServer1 サーバーの状況を表示します。
    -  アイコンは、サーバーが始動済みであることを示します。必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。
    -  アイコンは、サーバーが停止していることを示します。サーバーを選択して「開始」をクリックし、サーバーを開始してください。
    -  アイコンは、サーバー状況が使用不可であることを示します。ノード・エージェントが実行されていない可能性があります。ノード・エージェントを開始するには、コマンド・ウィンドウで /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。



以下の順序でサーバーを開始します。

- a. nodeagent
- b. cpudServer1

以下の順序でサーバーを停止します。

- a. cpudServer1
- b. nodeagent

cpudServer サーバーを停止するには、サーバーを選択して「停止」をクリックします。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

5. WebSphere UDDI ユーザー・コンソールにアクセスできることを確認してください。
  - a. アプリケーション・サーバーで、`https://APPLICATION_SERVER_HOST:9080/uddigui/` にアクセスします。ここでの `APPLICATION_SERVER_HOST` はアプリケーション・サーバーのホスト名です。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## ビジネス・ルール (WebSphere Operational Decision Manager JRules コンソール) テスト

ビジネス・ルール (WebSphere Operational Decision Manager JRules コンソール) テストは、Rule Execution Server コンソールにアクセスして、WebSphere Operational Decision Management JRules へのアクセスをテストします。

## リソース

ビジネス・ルール (WebSphere Operational Decision Manager JRules コンソール) テストでは、以下のリソースを使用します。

- (アプリケーション・サーバー上の) WebSphere Operational Decision Management JRules。

## 問題判別

ビジネス・ルール (WebSphere Operational Decision Manager JRules コンソール) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. アプリケーション・サーバーでは、以下の WebSphere Operational Decision Management 構成ログを確認します。
    - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log`
    - `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log`



2. アプリケーション・サーバー 上のファイル・システムが最大容量に達していないことを確認してください。これは `df -h` コマンドを使用して判別することができます。
3. Rule Execution Server が始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。
  - a. アプリケーション・サーバー・システムで、`ibmadmin` としてログオンします。
  - b. コマンド・ウィンドウで、コマンド (`/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD`) を実行します。`WAS_ADMIN_PWD` は、WebSphere Application Server の管理者パスワードです。
  - c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、`/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` コマンドを使用して、`nodeagent` を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。`nodeagent` を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。
  - a. メッセージ「ADMU0509I: The Application Server "wodmServer1" cannot be reached. It appears to be stopped.」が表示された場合、`/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1` コマンドを使用して、`wodmServer1` を始動します。メッセージ「ADMU0508I: The Application Server "wodmServer1" is STARTED.」が表示された場合、このステップを省略します。`wodmServer1` を始動する必要があった場合、次のようなメッセージが表示されます。ADMU3000I: Server wodmServer1 open for e-business; process id is 26654

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. `nodeagent`
- b. `wodmServer1`

以下の順序でサーバーを停止します。


- a. `wodmServer1`
- b. `nodeagent`


`wodmServer1` サーバーを停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。


`nodeagent` を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

4. Rule Execution Server が始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。
  - a. `http://APPLICATION_SERVER_HOST:9060/admin` で、WebSphere Application Server の管理 ID である `admin` およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。`APPLICATION_SERVER_HOST` は、アプリケーション・サーバー のホスト名です。

- b. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Server」をクリックして、wodmProfile サーバーの状況を表示します。

 アイコンは、サーバーが開始済みであることを示します。必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。

 アイコンは、サーバーが停止していることを示します。サーバーを選択して「開始」をクリックし、サーバーを開始してください。

 アイコンは、サーバー状況が使用不可であることを示します。ノード・エージェントが実行されていない可能性があります。ノード・エージェントを開始するには、コマンド・ウィンドウで `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. wodmServer1

以下の順序でサーバーを停止します。

- a. wodmServer1
- b. nodeagent

wodmProfile サーバーを停止するには、サーバーを選択して「停止」をクリックします。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

5. `http://APPLICATION_SERVER_HOST:9083/res` を指定して、アプリケーション・サーバーから Rule Execution Server コンソールにアクセスできることを確認してください。ここでの `APPLICATION_SERVER_HOST` はアプリケーション・サーバーのホスト名です。ユーザー ID `resAdmin1` を使用してログオンします。
6. Rule Execution Server コンソール内で、「診断」タブを開きます。「診断の実行」をクリックします。テストが実行されて、レポートが表示されます。「すべて展開」をクリックして、各テストの詳細について表示します。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## ビジネス・ルール (WebSphere Operational Decision Manager JRules ルール) テスト

ビジネス・ルール (WebSphere Operational Decision Manager JRules ルール) テストは、Rules Execution Server にインストールされている `cardTransactionRuleApp` ビジネス・ルールを呼び出してその出力を検証することにより、WebSphere Operational Decision Management JRules Rule Engine へのアクセスをテストします。

## リソース

ビジネス・ルール (WebSphere Operational Decision Manager JRules ルール) テストでは、以下のリソースを使用します。

- (アプリケーション・サーバー上の) WebSphere Operational Decision Management JRules。

## 問題判別

ビジネス・ルール (WebSphere Operational Decision Manager JRules ルール) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. アプリケーション・サーバーでは、以下の WebSphere Operational Decision Management 構成ログを確認します。
    - /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log
2. アプリケーション・サーバー 上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
3. Rule Execution Server が始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。
  - a. アプリケーション・サーバー・システムで、ibmadmin としてログオンします。
  - b. コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
  - c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh コマンドを使用して、nodeagent を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。
    - a. メッセージ「ADMU0509I: The Application Server "wodmServer1" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/startServer.sh wodmServer1 コマンドを使用して、wodmServer1 を始動します。メッセージ「ADMU0508I: The Application Server "wodmServer1" is STARTED.」が表示された場合、このステップを省略します。wodmServer1 を始動する必要があった場合、次のようなメッセージが表示されます。ADMU3000I: Server wodmServer1 open for e-business; process id is 26654

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. wodmServer1

以下の順序でサーバーを停止します。


- a. wodmServer1
- b. nodeagent


wodmServer1 サーバーを停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopServer.sh wodmServer1 -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。


nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

4. Rule Execution Server が始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。

- a. `http://APPLICATION_SERVER_HOST:9060/admin` で、WebSphere Application Server の管理 ID である `admin` およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。`APPLICATION_SERVER_HOST` は、アプリケーション・サーバー のホスト名です。
- b. 「サーバー」 > 「サーバー・タイプ」 > 「**WebSphere Application Server**」をクリックして、wodmProfile サーバーの状況を表示します。

 アイコンは、サーバーが開始済みであることを示します。必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。

 アイコンは、サーバーが停止していることを示します。サーバーを選択して「開始」をクリックし、サーバーを開始してください。

 アイコンは、サーバー状況が使用不可であることを示します。ノード・エージェントが実行されていない可能性があります。ノード・エージェントを開始するには、コマンド・ウィンドウで `/opt/IBM/WebSphere/AppServer/profiles/wodmServer1/bin/startNode.sh` コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. wodmServer1

以下の順序でサーバーを停止します。

- a. wodmServer1
- b. nodeagent

wodmProfile サーバーを停止するには、サーバーを選択して「停止」をクリックします。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

5. `http://APPLICATION_SERVER_HOST:9083/res` を指定して、アプリケーション・サーバーから Rule Execution Server コンソールにアクセスできることを確認してください。ここでの `APPLICATION_SERVER_HOST` はアプリケーション・サーバーのホスト名です。ユーザー ID `resAdmin1` を使用してログオンします。
6. Rule Execution Server コンソール内で、「診断」タブを開きます。「**診断の実行**」をクリックします。テストが実行されて、レポートが表示されます。「**すべて展開**」をクリックして、各テストの詳細について表示します。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## コラボレーション (Lotus Domino コンソール) テスト

コラボレーション (Lotus Domino コンソール) テストでは、その URL を使用して Domino ディレクトリにアクセスできるかどうかを判別します。

## リソース

コラボレーション (Lotus Domino コンソール) テストでは、以下のリソースを使用します。

- Domino サーバー (イベント・サーバー上)。

## 問題判別

コラボレーション (Lotus Domino コンソール) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. イベント・サーバーでは、以下の Lotus Domino ログを確認します。
    - `/local/notesdata/console.out`
    - `/local/notesdata/log.nsf`
    - `/local/notesdata/IBM_TECHNICAL_SUPPORT/` ディレクトリーのすべてのログ
2. イベント・サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。これは `df -h` コマンドを使用して判別することができます。
3. Lotus Domino プロセス・コンポーネントが実行されていることを確認します。
  - a. Lotus Domino ディレクトリー・コンソールにログインします (`http://EVENT_SERVER_HOST:84/names.nsf`)。 `EVENT_SERVER_HOST` は、イベント・サーバーのホスト名です。Domino 管理者のユーザー名およびパスワードを使用してログインします。
  - b. コンソールにアクセスできない場合、イベント・サーバーで `ps -ef | grep notes` コマンドを実行して、Lotus Domino プロセスが実行されているかどうかを判別します。Lotus Domino プロセスは以下のとおりです。
    - `server`
    - `event`
    - `update`
    - `replica`
    - `router`
    - `adminp`

- calconn
  - sched
  - http
  - rnmgr
  - staddin
4. 一部のプロセスのみ (すべてのプロセスではない) が実行されている場合、すべてのプロセスを再開する前に、実行中のプロセスを停止します。
    - a. イベント・サーバーに、notes ユーザーとしてログインします。
    - b. /local/notesdata ディレクトリーに移動します。
    - c. "nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &" コマンドを実行して、実行されているすべての Lotus Domino プロセスを停止します。
    - d. ps -ef | grep notes コマンドを実行して、すべてのプロセスが停止していることを確認します。
    - e. 実行されている Lotus Domino プロセスがまだ存在する場合、kill -9 pid コマンドを使用して停止します。pid は、Lotus Domino プロセスのプロセス ID です。
  5. Lotus Domino プロセスが実行されていない場合、Lotus Domino サーバー・コンポーネントを始動します。
    - a. イベント・サーバーに、notes ユーザーとしてログインします。
    - b. /local/notesdata ディレクトリーに移動します。
    - c. "nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &" コマンドを実行して、すべての Lotus Domino サーバー・コンポーネントを始動します。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## コラボレーション (Lotus Sametime コンソール) テスト

コラボレーション (Lotus Sametime コンソール) テストでは、その URL を使用して Sametime コンソールにアクセスできるかどうかを判別します。

## リソース

コラボレーション (Lotus Sametime コンソール) テストでは、以下のリソースを使用します。

- Sametime サーバー (イベント・サーバー上)。

## 問題判別

コラボレーション (Lotus Sametime コンソール) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. Sametime Community Server の構成ファイルおよびログ・ファイルを収集し、確認します。
  - a. notes ユーザーとして イベント・サーバーにログオンします。
  - b. /local/notesdata ディレクトリーに移動します。
  - c. sh stdiagzip.sh コマンドを実行します。このコマンドは、該当するすべてのログ・ファイルを収集し、/local/notesdata/ ディレクトリーに書き込みます。
  - d. /local/notesdata/ ディレクトリーにあるログを確認します。



2. イベント・サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
3. Sametime プロセス・コンポーネントが実行されていることを確認します。
  - a. Sametime ホーム・ページ ([http://EVENT\\_SERVER\\_HOST:84/stcenter.nsf](http://EVENT_SERVER_HOST:84/stcenter.nsf)) にログインします。  
*EVENT\_SERVER\_HOST* は、イベント・サーバーのホスト名です。Domino 管理者のユーザー名およびパスワードを使用してログインします。
  - b. Sametime ホーム・ページで、「サーバーの管理」をクリックします。
  - c. 「サーバー - 概要」ページで、すべての Sametime サービスが実行されていることを確認します。
4. 一部のプロセスのみ (すべてのプロセスではない) が実行されている場合、すべてのプロセスを再開する前に、実行中のプロセスを停止します。
  - a. イベント・サーバーに、notes ユーザーとしてログインします。
  - b. `/local/notesdata` ディレクトリーに移動します。
  - c. `"nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &"` コマンドを実行して、実行されているすべての Sametime プロセスを停止します。
  - d. `ps -ef | grep notes` コマンドを実行して、すべてのプロセスが停止していることを確認します。
  - e. 実行されているプロセスがまだ存在する場合、`kill -9 pid` を使用して停止します。*pid* は、Lotus Domino プロセスのプロセス ID です。
5. Sametime プロセスが実行されていない場合、Lotus Sametime サーバー・コンポーネントを始動します。
  - a. イベント・サーバーに、notes ユーザーとしてログインします。
  - b. `/local/notesdata` ディレクトリーに移動します。
  - c. `"nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &"` コマンドを実行して、すべての Lotus Sametime サーバー・コンポーネントを始動します。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## コラボレーション (Lotus Sametime Proxy) テスト

コラボレーション (Lotus Sametime Proxy) テストでは、Lotus Sametime Proxy Web アプリケーション URL を使用して、Lotus Sametime Proxy Web アプリケーションにアクセスできるかどうかを判別します。

## リソース

コラボレーション (Lotus Sametime Proxy) テストでは、以下のリソースを使用します。

- Sametime Proxy (アプリケーション・サーバー上)。

## 問題判別

コラボレーション (Lotus Sametime Proxy) テストが失敗した場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`

- /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
- b. アプリケーション・サーバーでは、以下の Sametime Proxy Server ログを確認します。
    - /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log
  2. アプリケーション・サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
  3. Sametime Proxy Server が始動されていることを確認します。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。
    - a. アプリケーション・サーバー・システムで、ibmadmin としてログオンします。
    - b. コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
    - c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、コマンド (/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh) を使用して、この nodeagent を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。
    - d. メッセージ「ADMU0509I: The Application Server "STProxyServer1" cannot be reached. It appears to be stopped.」が表示された場合、コマンド (/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/startServer.sh STProxyServer1) を使用して STProxyServer1 を始動します。メッセージ「ADMU0508I: The Application Server "STProxyServer1" is STARTED.」が表示された場合、このステップはスキップします。STProxyServer1 を始動する必要があった場合、「ADMU3000I: Server STProxyServer1 open for e-business; process id is 26654」のようなメッセージが表示されます。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。




- a. nodeagent
- b. STProxyServer1

以下の順序でサーバーを停止します。

- a. STProxyServer1
- b. nodeagent

アプリケーション・サーバーのコマンド・ウィンドウでコマンド (/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopServer.sh STProxyServer1 -username waswebadmin -password WAS\_ADMIN\_PWD) を実行することで、STProxyServer1 が停止します。WAS\_ADMIN\_PWD は、WebSphere の管理者パスワードです。

アプリケーション・サーバーのコマンド・ウィンドウでコマンド (/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD) を実行することで、nodeagent が停止します。WAS\_ADMIN\_PWD は、WebSphere の管理者パスワードです。

4. Sametime Proxy Server が始動されていることを確認します。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。
  - a. `http://APPLICATION_SERVER_HOST:9060/admin` で、WebSphere Application Server の管理 ID である `admin` およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。`APPLICATION_SERVER_HOST` は、アプリケーション・サーバー のホスト名です。
  - b. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Server」をクリックして、STProxyServer1 サーバーの状況を確認します。
    -  アイコンは、サーバーが開始済みであることを示します。必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。
    -  アイコンは、サーバーが停止していることを示します。サーバーを選択して「開始」をクリックし、サーバーを開始してください。
    -  アイコンは、サーバー状況が使用不可であることを示します。ノード・エージェントが実行されていない可能性があります。ノード・エージェントを開始するには、コマンド・ウィンドウで `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. `nodeagent`
- b. `STProxyServer1`

以下の順序でサーバーを停止します。

- a. `STProxyServer1`
- b. `nodeagent`

`STProxyServer1` サーバーを停止するには、サーバーを選択して「停止」をクリックします。

アプリケーション・サーバーのコマンド・ウィンドウでコマンド (`/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD`) を実行することで、`nodeagent` が停止します。`WAS_ADMIN_PWD` は、WebSphere の管理者パスワードです。

5. アプリケーション・サーバーにおいて、URL (`http://APPLICATION_SERVER_HOST:9085/stwebclient/popup.jsp`) を使用して、WebSphere Portal システムから Sametime Proxy コンソールにアクセスできることを確認します。`APPLICATION_SERVER_HOST` は アプリケーション・サーバー のホスト名です。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## データベース (DB2) テスト

データベース (DB2) テストでは、Web アプリケーションとデータ・サーバーの間で JDBC 接続にアクセスできるかどうかを判別します。JDBC タイプ 4 接続が確立され、動的 SQL 照会が発行されて、データベース内に存在する表の数がカウントされます。

## リソース

データベース (DB2) テストでは、以下のリソースを使用します。

- UDDIDB データベース用の接続を含む UddiDataSource 定義 (アプリケーション・サーバー上)。
- UDDIDB データベース (データ・サーバー上の db2inst4 インスタンス)。

## 問題判別

データベース (DB2) テストでデータ・サーバーにアクセスできない場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. テストが開始されたアプリケーション・サーバーと、データベースが存在するデータ・サーバーの間にネットワーク接続があることを確認します。 これを行うには、アプリケーション・サーバーで、データ・サーバーの短縮ホスト名と完全修飾ホスト名の両方を指定して、**ping** コマンドを送信します。  
**ping** コマンドの結果は、ホスト名が DNS または /etc/hosts ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
3. データ・サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。 これは **df -h** コマンドを使用して判別することができます。
4. データ・サーバーが使用するデータベースが始動されていることを確認します。
  - a. データ・サーバーで、db2inst4 ユーザーとしてコマンド・ウィンドウから以下のコマンドを実行します。

```
ps -ef | grep db2 | grep db2inst4
```

以下を含む DB2 プロセスが、db2inst4 インスタンス・ユーザーとして実行されている必要があります。

```
db2sysc
db2vend
db2acd
```
5. DB2 プロセスが実行されていない場合、db2inst4 ユーザーとしてコマンド・ウィンドウから **db2start** を実行して、当該プロセスを始動します。
6. DB2 ログで、このテストに使用されたデータベース・インスタンスに関連するエラーを確認します。このログは、データ・サーバーの /datahome/db2inst4/sql1lib/db2dump ディレクトリーにあります。
7. db2diag.log ログで、このテストに使用されたデータベースの始動時に発生したエラーを確認します。
8. WebSphere Application Server 管理コンソールを使用して、DataSource Web コンテナ・リソースへの接続を確認します。
  - a. アプリケーション・サーバーで、WebSphere Application Server 管理コンソール ([https://APPLICATION\\_SERVER\\_HOST:9043/ibm/console](https://APPLICATION_SERVER_HOST:9043/ibm/console)) にアクセスします。  
**APPLICATION\_SERVER\_HOST** は、アプリケーション・サーバーのホスト名です。
  - b. 「リソース」 > 「JDBC」 > 「データ・ソース」をクリックします。

- c. 「接続のテスト」をクリックしてデータ・ソースへの接続をテストし、UddiDataSource データ・ソースを確認します。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## データベース (DB2 インスタンス - *instance*) テスト

データベース (DB2 インスタンス - *instance*) では、**db2status** スクリプトを実行することで、データ・サーバー上の DB2 インスタンスの DB2 マネージャー状況をテストします。

## リソース

データベース (DB2 インスタンス - *instance*) テストでは、以下のリソースを使用します。

- DB2 *instance* (データ・サーバー上)

## 問題判別

データベース (DB2 インスタンス - *instance*) テストが失敗した場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. テストが開始されたアプリケーション・サーバーと、データベースが存在するデータ・サーバーの間にネットワーク接続があることを確認します。 これを行うには、アプリケーション・サーバーで、データ・サーバーの短縮ホスト名と完全修飾ホスト名の両方を指定して、**ping** コマンドを送信します。  
**ping** コマンドの結果は、ホスト名が DNS または /etc/hosts ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
3. データ・サーバー・システム上のファイル・システムが、最大容量に達していないことを確認します。これは **df -h** コマンドを使用して判別することができます。
4. データ・サーバーが使用するデータベースが始動されていることを確認します。
  - a. データ・サーバーで、ユーザー名を *instance* として、コマンド・ウィンドウから以下のコマンドを実行します。*instance* は、以下のテスト名で示される DB2 インスタンスの名前です。

```
db2 get snapshot for dbm | grep status
```

  
*instance* についてデータベース・マネージャーが始動されている場合、メッセージ「Database manager status = Active」が表示されます。
5. DB2 プロセスが実行されていない場合、root ユーザーとして行うときは、コマンド・ウィンドウから **su - instance** を実行して始動します。それ以外のユーザーとして行うときは、**db2start** を実行してデータベース・マネージャーを始動します。
6. DB2 ログで、このテストに使用されたデータベース・インスタンスに関連するエラーを確認します。このログは、データ・サーバーの /datahome/*instance*/sql1lib/db2dump ディレクトリにあります。
7. db2diag.log ログで、このテストに使用されたデータベースの始動時に発生したエラーを確認します。



## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## ディレクトリー (UDDI V3 と UDDI V3 HTTPS) テスト

ディレクトリー (UDDI V3 と UDDI V3 HTTPS) テストは、WebSphere UDDI Registry の HTTP および HTTPS URL を使用して、WebSphere UDDI Registry にアクセスできるかどうか判別します。

## リソース

ディレクトリー (UDDI V3 と UDDI V3 HTTPS) テストでは、以下のリソースを使用します。

- (アプリケーション・サーバー上の) WebSphere Application Server。

## 問題判別

ディレクトリー (UDDI V3 と UDDI V3 HTTPS) テストが失敗した場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. アプリケーション・サーバーでは、以下の WebSphere UDDI Registry 構成ログを確認します。
    - /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log
2. アプリケーション・サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
3. cpudServer1 サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。
  - a. アプリケーション・サーバー・システムで、ibmadmin としてログオンします。
  - b. コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
  - c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh コマンドを使用して、nodeagent を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。
  - a. メッセージ「ADMU0509I: The Application Server "cpudServer1" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1 コマンドを使用して、cpudServer1 を始動します。メッセージ「ADMU0508I: The Application Server "cpudServer1" is STARTED.」が表示された場合、このステップを省略します。cpudServer1 を始動する必要があった場合、次のようなメッセージが表示されません。ADMU3000I: Server cpudServer1 open for e-business; process id is 26654



**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。




- a. nodeagent
- b. cpudServer1

以下の順序でサーバーを停止します。

- a. cpudServer1
- b. nodeagent

cpudServer1 サーバーを停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

4. cpudServer1 サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。
  - a. `http://APPLICATION_SERVER_HOST:9060/admin` で、WebSphere Application Server の管理 ID である `admin` およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。`APPLICATION_SERVER_HOST` はアプリケーション・サーバーのホスト名です。
  - b. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Server」をクリックして、cpudServer1 サーバーの状況を表示します。
    -  アイコンは、サーバーが始動済みであることを示します。必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。
    -  アイコンは、サーバーが停止していることを示します。サーバーを選択して「開始」をクリックし、サーバーを開始してください。
    -  アイコンは、サーバー状況が使用不可であることを示します。ノード・エージェントが実行されていない可能性があります。ノード・エージェントを開始するには、コマンド・ウィンドウで `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh` コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. cpudServer1

以下の順序でサーバーを停止します。

- a. cpudServer1
- b. nodeagent

cpudServer サーバーを停止するには、サーバーを選択して「停止」をクリックします。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

5. 次の URL を使用して、アプリケーション・サーバーにおいて、WebSphere UDDI Registry ユーザー・コンソールに WebSphere Portal システムからアクセスできることを確認してください。  
`http://APPLICATION_SERVER_HOST:9080/uddigui/` ここで、`APPLICATION_SERVER_HOST` は アプリケーション・サーバー のホスト名です。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## 内部診断 (リモートの Echo REST) テスト

内部診断 (リモートの Echo REST) テストでは、当該 URL にアクセスすることで、Remote Responder へのアクセス性をテストします。これはシステム検査チェックの診断であり、システム検査チェックモジュール間のリンクを検査します。

## リソース

内部診断 (リモートの Echo REST) では、以下のリソースを使用します。

- WebSphere Application Server (アプリケーション・サーバー上)。

## 問題判別

内部診断 (リモートの Echo REST) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. アプリケーション・サーバーでは、以下の WebSphere UDDI Registry 構成ログを確認します。
    - `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemOut.log`
    - `/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/logs/cpodServer1/SystemErr.log`
2. アプリケーション・サーバー 上のファイル・システムが最大容量に達していないことを確認してください。これは `df -h` コマンドを使用して判別することができます。
3. cpudServer1 サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。
  - a. アプリケーション・サーバー・システムで、ibmadmin としてログオンします。
  - b. コマンド・ウィンドウで、コマンド (`/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS_ADMIN_PWD`) を実行します。  
`WAS_ADMIN_PWD` は、WebSphere Application Server の管理者パスワードです。
  - c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、`/opt/IBM/WebSphere/AppServer/profiles/cpodProfile1/bin/`

startNode.sh コマンドを使用して、nodeagent を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。

- a. メッセージ「ADMU0509I: The Application Server "cpudServer1" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startServer.sh cpudServer1 コマンドを使用して、cpudServer1 を始動します。メッセージ「ADMU0508I: The Application Server "cpudServer1" is STARTED.」が表示された場合、このステップを省略します。cpudServer1 を始動する必要があった場合、次のようなメッセージが表示されます。ADMU3000I: Server cpudServer1 open for e-business; process id is 26654

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. cpudServer1


以下の順序でサーバーを停止します。


- a. cpudServer1
- b. nodeagent


cpudServer1 サーバーを停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopServer.sh cpudServer1 -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

4. cpudServer1 サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。
  - a. `http://APPLICATION_SERVER_HOST:9060/admin` で、WebSphere Application Server の管理 ID である admin およびパスワードを使用して WebSphere Application Server 管理コンソールにログインします。APPLICATION\_SERVER\_HOST はアプリケーション・サーバーのホスト名です。
  - b. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Server」をクリックして、cpudServer1 サーバーの状況を表示します。

 アイコンは、サーバーが始動済みであることを示します。必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。

 アイコンは、サーバーが停止していることを示します。サーバーを選択して「開始」をクリックし、サーバーを開始してください。

 アイコンは、サーバー状況が使用不可であることを示します。ノード・エージェントが実行されていない可能性があります。ノード・エージェントを開始するには、コマンド・ウィンドウで /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/startNode.sh コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. cpudServer1

以下の順序でサーバーを停止します。

- a. cpudServer1
- b. nodeagent

cpudServer サーバーを停止するには、サーバーを選択して「停止」をクリックします。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

5. WebSphere UDDI ユーザー・コンソールにアクセスできることを確認してください。
  - a. アプリケーション・サーバーで、`https://APPLICATION_SERVER_HOST:9080/uddigui/` にアクセスします。ここでの `APPLICATION_SERVER_HOST` はアプリケーション・サーバーのホスト名です。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## メッセージング (WebSphere Message Broker パブリッシュ/サブスクライブのトピック) テスト

メッセージング (WebSphere Message Broker パブリッシュ/サブスクライブのトピック) テストは、WebSphere Message Broker のパブリッシュ機能およびサブスクライブ機能をテストします。このテストは、`.jms/IopCatWmbPub` としてプロパティーにリストされている JNDI 名を持つトピックに対して、メッセージをパブリッシュします。WebSphere Message Broker はメッセージを受信すると、リターン・メッセージを `IOP.CAT.PUB` トピックにパブリッシュします。応答メッセージが受信された場合、テストは成功です。エラーがある場合、あるいはプロパティー・ファイルで指定されているタイムアウト期間内に応答メッセージが受信されない場合、テストは失敗です。

## リソース

メッセージング (WebSphere Message Broker パブリッシュ/サブスクライブのトピック) テストでは、以下のリソースを使用します。

- (アプリケーション・サーバー 上の) WebSphere Portal Server。
- (イベント・サーバー上の) WebSphere Message Queue。
- (イベント・サーバー上の) WebSphere Message Broker。

## 問題判別

メッセージング (WebSphere Message Broker パブリッシュ/サブスクライブのトピック) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. アプリケーション・サーバーとイベント・サーバーの間にネットワーク接続があることを確認します。これを行うには、短縮ホスト名と完全修飾ホスト名の両方を指定して、サーバー間で相互に **ping** コマンドを送信します。 **ping** コマンドの結果は、ホスト名が DNS または `/etc/hosts` ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. イベント・サーバーおよびアプリケーション・サーバーのファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
4. WebSphere Message Queue キュー・マネージャーと WebSphere Message Broker ブローカーが実行されていることを確認してください。
  - a. イベント・サーバーに WebSphere Message Queue 管理者としてログオンします。例えば、mqm です。
  - b. コマンド・ウィンドウで、**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq** を実行します。以下のようなメッセージが表示されます。

```
QMNAME(IOC.MB.QM) STATUS(Running)
```
  - c. 「実行中」以外の状況が返された場合、次のコマンドを使用して WebSphere Message Queue キュー・マネージャーを開始します。**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**
  - d. イベント・サーバーに WebSphere Message Broker 管理者としてログオンします。例えば、mqm です。
  - e. コマンド・ウィンドウで、**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist** を実行します。以下のようなメッセージが表示されます。

```
BIP1284I: Broker 'IOC_BROKER' on queue manager 'IOC.MB.QM' is running.
```
  - f. 「実行中」以外の状況が返された場合、次のコマンドを使用して WebSphere Message Broker ブローカーを開始します。**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsisstart IOC\_BROKER**
5. ログにエラーがないかチェックします。ログは、イベント・サーバーの `/var/log/messages` ディレクトリに配置されています。接頭部「BIP」が付いたメッセージを探します。また、キュー名と、テストが実行されたときのタイム・スタンプも探します。
6. ブローカーまたはキュー・マネージャーが開始されていないと思われる場合は、イベント・サーバーを始動してシステムの始動スクリプトを実行することにより開始することもできます。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## メッセージング (WebSphere Message Queue パブリッシュ/サブスクライブのトピック) テスト

メッセージング (WebSphere Message Queue パブリッシュ/サブスクライブのトピック) テストは、WebSphere Message Queue のパブリッシュ機能およびサブスクライブ機能をテストします。このテストはプロパティに指定されているトピックを作成します。次に、メッセージをトピックにパブリッシュして、パブリッシュされたメッセージの読み取りをすぐに試行します。送信されたメッセージを読み取るこ



とができる場合、テストは成功です。 エラーがある場合、あるいは 15 秒 (15000 ミリ秒) 以内にメッセージを読み取ることができない場合、テストは失敗です。

## リソース

メッセージング (WebSphere Message Queue パブリッシュ/サブスクライブのトピック) テストでは、以下のリソースを使用します。

- (アプリケーション・サーバー 上の) WebSphere Portal Server。
- (イベント・サーバー上の) WebSphere Message Queue。

## 問題判別

メッセージング (WebSphere Message Queue パブリッシュ/サブスクライブのトピック) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. アプリケーション・サーバーとイベント・サーバーの間にネットワーク接続があることを確認します。これを行うには、短縮ホスト名と完全修飾ホスト名の両方を指定して、サーバー間で相互に **ping** コマンドを送信します。 **ping** コマンドの結果は、ホスト名が DNS または /etc/hosts ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
3. サーバー上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
4. WebSphere Message Queue キュー・マネージャーが実行されていることを確認してください。
  - a. イベント・サーバーに WebSphere Message Queue 管理者としてログオンします。例えば、mqm です。
  - b. コマンド・ウィンドウで、**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq** を実行します。以下のようなメッセージが表示されます。

```
QMNAME(IOC.MB.QM) STATUS(Running)
```
  - c. 「実行中」以外の状況が返された場合、次のコマンドを使用して WebSphere Message Queue キュー・マネージャーを開始します。**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**
5. ログにエラーがないかチェックします。ログは、イベント・サーバーの /var/log/messages ディレクトリに配置されています。接頭部「BIP」が付いたメッセージを探します。また、キュー名と、テストが実行されたときのタイム・スタンプも探します。
6. キュー・マネージャーが開始されていないと思われる場合は、イベント・サーバーを始動してシステムの始動スクリプトを実行することにより開始することもできます。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。



## メッセージング (WebSphere Message Broker/Queue のインストール・チェック) テスト

メッセージング (WebSphere Message Broker/Queue のインストール・チェック) テストでは、WebSphere Message Queue および Message Broker にアクセスできるかどうかを判別します。これは、WebSphere Message Broker を実行しているシステム上で、WebSphere Message Broker の **mqsilist** コマンドを実行することで、行うことができます。

### リソース

メッセージング (WebSphere Message Broker/Queue のインストール・チェック) では、以下のリソースを使用します。

- WebSphere Portal Server (アプリケーション・サーバー上)。
- WebSphere Message Queue および Message Broker (イベント・サーバー上)。

### 問題判別

メッセージング (WebSphere Message Broker/Queue のインストール・チェック) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

### 手順

1. WebSphere Portal システム (アプリケーション・サーバー上) と WebSphere Message Broker システム (イベント・サーバー上) の間にネットワーク接続があることを確認します。これを行うには、アプリケーション・サーバーで、イベント・サーバーの短縮ホスト名と完全修飾ホスト名の両方を指定して、**ping** コマンドを送信します (逆も同様)。**ping** コマンドの結果は、ホスト名が DNS または `/etc/hosts` ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
3. アプリケーション・サーバー・システムおよびイベント・サーバー・システムのファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
4. WebSphere Message Queue キュー・マネージャーと WebSphere Message Broker ブローカーが実行されていることを確認してください。
  - a. イベント・サーバーに WebSphere Message Queue 管理者としてログオンします。例えば、`mqm` です。
  - b. コマンド・ウィンドウで、**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; dspmq** を実行します。以下のようなメッセージが表示されます。

```
QMNAME(IOC.MB.QM) STATUS(Running)
```
  - c. 「実行中」以外の状況が返された場合、次のコマンドを使用して WebSphere Message Queue キュー・マネージャーを開始します。**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**
  - d. イベント・サーバーに WebSphere Message Broker 管理者としてログオンします。例えば、`mqm` です。
  - e. コマンド・ウィンドウで、**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist** を実行します。以下のようなメッセージが表示されます。

BIP1284I: Broker 'IOC\_BROKER' on queue manager 'IOC.MB.QM' is running.

- f. 「実行中」以外の状況が返された場合、次のコマンドを使用して WebSphere Message Broker ブローカーを開始します。 **source /opt/IBM/mqsi/8.0.0.0/bin/mqsipprofile; mqsistart IOC\_BROKER**
5. ログにエラーがないかチェックします。 ログは、イベント・サーバーの /var/log/messages ディレクトリに配置されています。 接頭部「BIP」が付いたメッセージを探します。 また、キュー名と、テストが実行されたときのタイム・スタンプも探します。
6. ブローカーまたはキュー・マネージャーが開始されていないと思われる場合は、イベント・サーバーを始動してシステムの始動スクリプトを実行することにより開始することもできます。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## メッセージング (WebSphere Message Broker/Queue のキュー) テスト

メッセージング (WebSphere Message Broker/Queue のキュー) テストは、メッセージをキューに入れて、WebSphere Message Queue をテストします。

## リソース

メッセージング (WebSphere Message Broker/Queue のキュー) テストでは、以下のリソースを使用します。

- (アプリケーション・サーバー 上の) WebSphere Portal Server。
- (イベント・サーバー上の) WebSphere Message Queue。
- (イベント・サーバー上の) WebSphere Message Broker。

## 問題判別

メッセージング (WebSphere Message Broker/Queue のキュー) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. アプリケーション・サーバーとイベント・サーバーの間にネットワーク接続があることを確認します。 これを行うには、短縮ホスト名と完全修飾ホスト名の両方を指定して、サーバー間で相互に **ping** コマンドを送信します。 **ping** コマンドの結果は、ホスト名が DNS または /etc/hosts ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
3. アプリケーション・サーバー・システムおよびイベント・サーバー・システムのファイル・システムが最大容量に達していないことを確認してください。 これは **df -h** コマンドを使用して判別することができます。
4. WebSphere Message Queue キュー・マネージャーと WebSphere Message Broker ブローカーが実行されていることを確認してください。
  - a. イベント・サーバーに WebSphere Message Queue 管理者としてログオンします。 例えば、mqm です。
  - b. コマンド・ウィンドウで、**source /opt/IBM/mqsi/8.0.0.0/bin/mqsipprofile; dspmq** を実行します。 以下のようなメッセージが表示されます。

QMNAME(IOC.MB.QM) STATUS(Running)

- c. 「実行中」以外の状況が返された場合、次のコマンドを使用して WebSphere Message Queue キュー・マネージャーを開始します。**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; strmqm IOC.MB.QM**
  - d. イベント・サーバーに WebSphere Message Broker 管理者としてログオンします。例えば、mqm です。
  - e. コマンド・ウィンドウで、**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsilist** を実行します。以下のようなメッセージが表示されます。  
BIP1284I: Broker 'IOC\_BROKER' on queue manager 'IOC.MB.QM' is running.
  - f. 「実行中」以外の状況が返された場合、次のコマンドを使用して WebSphere Message Broker ブローカーを開始します。**source /opt/IBM/mqsi/8.0.0.0/bin/mqsiprofile; mqsistart IOC\_BROKER**
5. ログにエラーがないかチェックします。ログは、イベント・サーバーの /var/log/messages ディレクトリに配置されています。接頭部「BIP」が付いたメッセージを探します。また、キュー名と、テストが実行されたときのタイム・スタンプも探します。
  6. ブローカーまたはキュー・マネージャーが開始されていないと思われる場合は、イベント・サーバーを始動してシステムの始動スクリプトを実行することにより開始することもできます。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## モニター (Netcool Impact コンソール) テスト

モニター (Netcool® Impact コンソール) テストでは、Netcool Impact Console が実行されているかどうか、および Netcool Impact Console URL によってアクセスできるかどうかを判別します。

## リソース

モニター (Netcool Impact コンソール) テストでは、以下のリソースを使用します。

- Netcool Impact Server (イベント・サーバー上)

## 問題判別

モニター (Netcool Impact コンソール) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. イベント・サーバーでは、以下の Netcool Impact ログを確認します。
    - /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log
    - /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log
2. イベント・サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
3. server1 サーバーが始動されていることを確認します。
  - a. イベント・サーバー・システムで、wasadmin としてログオンします。

- b. コマンド・ウィンドウで、コマンド (`/opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/serverStatus.sh -all -username wasadmin -password WAS_ADMIN_PWD`) を実行します。  
`WAS_ADMIN_PWD` は、WebSphere Application Server の管理者パスワードです。
- c. メッセージ「ADMU0509I: The Application Server "server1" cannot be reached. It appears to be stopped.」が表示された場合、コマンド `/opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/startServer.sh server1` を使用して、この server1 サーバーを始動します (これにより Netcool Impact Console サーバーも始動されます)。メッセージ「ADMU0508I: The Application Server "server1" is STARTED」が表示された場合、このステップはスキップします。server1 サーバーを始動する必要があった場合、「ADMU3000I: Server server1 open for e-business; process id is 26654」のようなメッセージが表示されます。

イベント・サーバーのコマンド・ウィンドウでコマンド (`/opt/IBM/netcool/eWAS/profiles/ImpactProfile/bin/stopServer.sh server1 -username wasadmin -password WAS_ADMIN_PWD`) を実行することで、server1 が停止します。`WAS_ADMIN_PWD` は、WebSphere の管理者パスワードです。

4. イベント・サーバー (`http://EVENT_SERVER_HOST:9080/nci`) から Netcool Impact Console にアクセスできることを確認します。`EVENT_SERVER_HOST` は、イベント・サーバーのホスト名です。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## モニター (Netcool OMNibus) テスト

モニター (Netcool OMNibus) テストでは、Netcool Omnibus が使用可能であるかどうかを判別します。これは、`nco_pa_status -server NCO_PA` コマンドを実行することで、行うことができます。

## リソース

モニター (Netcool OMNibus) テストでは、以下のリソースを使用します。

- Netcool Omnibus Server (イベント・サーバー上)

## 問題判別

モニター (Netcool OMNibus) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. アプリケーション・サーバーとイベント・サーバーの間にネットワーク接続があることを確認します。これを行うには、アプリケーション・サーバーで、イベント・サーバーの短縮ホスト名と完全修飾ホスト名の両方を指定して、`ping` コマンドを送信します。`ping` コマンドの結果は、ホスト名が DNS または `/etc/hosts` ファイルにより正しく解決されているかどうかを表します。
2. プロセス制御サーバー・サービスおよびエージェントが実行されていることを確認します。
  - a. イベント・サーバーのコマンド・ウィンドウから、`netcool Linux` ユーザーとして `$NCHOME/omnibus/bin/nco_pa_status -server NCO_PA` コマンドを実行します。
  - b. サービスが開始または実行されていない場合、イベント・サーバーで、`root Linux` ユーザーとして `/etc/init.d/nco start` コマンドを実行し、サーバーを始動します。
  - c. プロセス・エージェントが実行されていない場合、イベント・サーバーで、`netcool Linux` ユーザーとして `$NCHOME/omnibus/bin/nco_pad` コマンドを実行し、エージェントを始動します。
3. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。

- /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
  - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
- b. イベント・サーバーでは、以下のディレクトリーにある NCO で始まるログをすべて確認します。
- /opt/IBM/netcool/log
  - /opt/IBM/netcool/omnibus/log
4. イベント・サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
5. アプリケーション・サーバー ([http://EVENT\\_SERVER\\_HOST:9060/ibm/console](http://EVENT_SERVER_HOST:9060/ibm/console)) から「Netcool Omnibus」ポートレットにアクセスできることを確認します。*EVENT\_SERVER\_HOST* は、イベント・サーバーのホスト名です。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## モニター (Tivoli Composite Application Manager エージェント - *server*) テスト

モニター (Tivoli Composite Application Manager エージェント - *server*) テストでは、**cinfo** コマンドを実行することで、Tivoli Composite Application Manager エージェントが実行されているかどうかをテストします。

## リソース

モニター (Tivoli Composite Application Manager エージェント - *server*) テストでは、以下のリソースを使用します。

- Tivoli Composite Application Manager
  - Tivoli Composite Application Manager エージェント (アプリケーション・サーバー上)
  - Tivoli Composite Application Manager エージェント (イベント・サーバー上)
  - Tivoli Composite Application Manager エージェント (データ・サーバー上)
  - Tivoli Composite Application Manager エージェント (管理サーバー上)

## 問題判別

モニター (Tivoli Composite Application Manager エージェント - *server*) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. アプリケーション・サーバー、管理サーバー、イベント・サーバー、および データ・サーバーの間にネットワーク接続があることを確認します。これを行うには、アプリケーション・サーバーで、管理サーバー、イベント・サーバー、およびデータ・サーバーの短縮ホスト名と完全修飾ホスト名の両方を指定して、**ping** コマンドを送信します。**ping** コマンドの結果は、ホスト名が DNS または */etc/hosts* ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log



3. アプリケーション・サーバー上、管理サーバー上、イベント・サーバー、およびデータ・サーバー上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
4. アプリケーション・サーバー、管理サーバー、イベント・サーバー、およびデータ・サーバーでこのステップを繰り返し、Tivoli Monitoring コンポーネントが実行されていることを確認します。
  - a. サーバー上の端末セッションに **root** としてログオンします。
  - b. **/opt/IBM/ITM/bin/cinfo -r** コマンドを実行します。以下のような結果が表示されます。サーバーが異なれば、エージェントも異なります。エージェントの状況は、実行中である必要があります。

```
***** Sun May 13 02:13:26 EDT 2012 *****
User: root Groups: root bin daemon sys adm disk wheel idslldap tdsproxy ivmgr tivoli
Host name : baapp2 Installer Lvl:06.22.01.00
CandleHome: /opt/IBM/ITM
```

```
*****
Host  Prod  PID  Owner  Start  ID  ..Status
baapp2 lz    31042 root    May09  None  ...running
baapp2 ht    18755 root    May09  None  ...running
baapp2 yn    4190 root    02:11  None  ...running
```

- c. 実行されていない Tivoli Composite Application Manager エージェントを始動します。
    - 1) サーバー上の端末セッションに **root** としてログオンします。
    - 2) **/opt/IBM/ITM/bin/itmcmd agent start PRODUCT\_CODE** を実行します。**PRODUCT\_CODE** は、**/opt/IBM/ITM/bin/cinfo -o** コマンドの結果に表示されるエージェントの PID 値です。
5. 例外については、ログ・ファイルを確認してください。
  - a. 管理サーバーでは、以下の Tivoli Enterprise Monitoring Server と Tivoli Enterprise Portal Server のログを確認します。
    - Tivoli Enterprise Monitoring Server: **/opt/IBM/ITM/logs/\*\_PRODUCT\_CODE\_{nnnnnn}.log**
    - Tivoli Enterprise Portal Server: **/opt/IBM/ITM/logs/\*\_PRODUCT\_CODE\_{nnnnnn}.log**
 ここでの **PRODUCT\_CODE** は、**/opt/IBM/ITM/bin/cinfo -o** コマンドで返される PID です。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## モニター (Tivoli Enterprise Monitoring Server) テスト

モニター (Tivoli Enterprise Monitoring Server) テストは、管理サーバーで実行されている Tivoli Enterprise Monitoring Server が使用可能かどうか判別します。コンポーネント状況を要求する照会は、Tivoli Monitoring Web Services SOAP サーバーに送信されます。この照会には、システムに対して無効なユーザー ID とパスワードが含まれます。応答では、無効な ID またはパスワードが使用されたことが示されません。エラーは、Tivoli Enterprise Monitoring Server が正常に作動していることを示します。

## リソース

モニター (Tivoli Enterprise Monitoring Server) テストでは、以下のリソースを使用します。

- (管理サーバー上の) Tivoli Enterprise Monitoring System
  - Tivoli Monitoring Web Services SOAP サーバー
  - Tivoli Enterprise Portal Server
  - Tivoli Enterprise Portal Server DB2 データベース

## 問題判別

モニター (Tivoli Enterprise Monitoring Server) テストが失敗した場合、以下を実行し、問題を特定して解決してください。



## 手順

1. アプリケーション・サーバーと管理サーバーの間にネットワーク接続があることを確認します。これを行うには、アプリケーション・サーバーで、管理サーバーの短縮ホスト名と完全修飾ホスト名の両方を指定して、**ping** コマンドを送信します。 **ping** コマンドの結果は、ホスト名が DNS または `/etc/hosts` ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. 管理サーバーでは、以下の管理サーバーのログを確認します。
    - Tivoli Event Monitoring Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnn}.log`
    - Tivoli Event Portal Server: `/opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnn}.log`
    - 組み込み WebSphere Application Server のログ:
      - エラー・ログ: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log`
      - 出力ログ: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log`
      - 開始ログ: `/opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log`
3. 管理サーバー上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
4. Tivoli Monitoring コンポーネントが管理サーバーで実行されていることを確認してください。
  - a. 管理サーバーの端末セッションに `root` としてログオンします。
  - b. `/opt/IBM/ITM/bin/cinfo -r` コマンドを実行します。
5. Tivoli コンポーネント・データベースが作動可能であることを確認してください。
  - a. 管理サーバーの端末セッションに `db2inst1` としてログオンします。
  - b. `ps -ef | grep db2inst1` コマンドを実行します。
  - c. DB2 プロセスが実行されていることを確認してください。これらのプロセスには、`db2sysc`、`db2vend`、および `db2acd` が含まれます。
  - d. DB2 プロセスが実行されていない場合、`>$ db2start` コマンドを実行します。
  - e. Tivoli コンポーネントで使用される開始中のデータベースに関連したデータベース・エラーがないかどうか、データ・サーバーの DB2 ログを確認します。ログ・ファイルは、データ・サーバーの `/datahome/db2inst1/sqlllib/db2dump` ディレクトリーにあります。
6. その結果について、`ms` の項目を探すことにより、Tivoli Enterprise Monitoring Server が実行されていることを確認してください。その項目がリストされていない場合、Tivoli Enterprise Monitoring Server は実行されていません。
7. Tivoli Enterprise Monitoring Server が実行されていない場合は始動します。
  - a. 管理サーバーの端末セッションに `root` としてログオンします。
  - b. `/opt/IBM/ITM/bin/itmcmd server start HUB_MWOS` コマンドを実行します。
8. ステップ 4 の結果について、`cq` の項目を探すことにより、Tivoli Enterprise Portal Server が実行されていることを確認してください。その項目がリストされていない場合、Tivoli Enterprise Portal Server は実行されていません。
9. Tivoli Enterprise Portal Server が実行されていない場合は始動します。
  - a. 管理サーバーの端末セッションに `root` としてログオンします。

- b. `/opt/IBM/ITM/bin/itmcmd agent start cq` コマンドを実行します。
10. ステップ 4 (271 ページ) の結果について、その他の有効なサブコンポーネントが実行されていることを確認してください。

表 79. Tivoli Monitoring のコンポーネント

コンポーネント	説明
kf	Eclipse Help Server
cq	Tivoli Enterprise Portal Server
lz	Monitoring Agent for Linux OS
ms	Tivoli Enterprise Monitoring Server
yn	IBM Tivoli Composite Application Manager Agent for WebSphere Applications

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## モニター (WebSphere Business Monitor Business Space コンソール) テスト

モニター (WebSphere Business Monitor Business Space コンソール) テストは、WebSphere Business Monitor Business Space HTTP URL を使用して、WebSphere Business Monitor Business Space にアクセスできるかどうか判別します。

## リソース

モニター (WebSphere Business Monitor Business Space コンソール) テストでは、以下のリソースを使用します。

- (アプリケーション・サーバー上の) WebSphere Application Server。

## 問題判別

モニター (WebSphere Business Monitor Business Space コンソール) テストが失敗した場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log`
    - `/opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log`
  - b. アプリケーション・サーバーでは、以下の WebSphere Business Monitor ログを確認します。
    - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log`
    - `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log`
2. アプリケーション・サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。これは `df -h` コマンドを使用して判別することができます。
3. WebSphere Business Monitor サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。

- a. アプリケーション・サーバー・システムで、ibmadmin としてログオンします。
- b. コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
- c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh コマンドを使用して、nodeagent を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。
- a. メッセージ「ADMU0509I: The Application Server "WBM\_DE.AppTarget.WBMNode1.0" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM\_DE.AppTarget.WBMNode1.0 コマンドを使用して、WBM\_DE.AppTarget.WBMNode1.0 を始動します。メッセージ「ADMU0508I: The Application Server "WBM\_DE.AppTarget.WBMNode1.0" is STARTED.」が表示された場合、このステップを省略します。WBM\_DE.AppTarget.WBMNode1.0 を始動する必要があった場合、次のようなメッセージが表示されます。ADMU3000I: Server WBM\_DE.AppTarget.WBMNode1.0 open for e-business; process id is 26654

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. WBM\_DE.AppTarget.WBMNode1.0

以下の順序でサーバーを停止します。

- a. WBM\_DE.AppTarget.WBMNode1.0
- b. nodeagent

WBM\_DE.AppTarget.WBMNode1.0 サーバーを停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh WBM\_DE.AppTarget.WBMNode1.0 -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

4. WebSphere Business Monitor サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。
  - a. [http://APPLICATION\\_SERVER\\_HOST:9060/admin](http://APPLICATION_SERVER_HOST:9060/admin) で、WebSphere Application Server の管理 ID である admin およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。APPLICATION\_SERVER\_HOST は、アプリケーション・サーバー のホスト名です。
  - b. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Server」をクリックして、WBM\_DE.AppTarget.WBMNode1.0 サーバーの状況を表示します。

➡ アイコンは、サーバーが開始済みであることを示します。 必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。

✖ アイコンは、サーバーが停止していることを示します。 サーバーを選択して「開始」をクリックし、サーバーを開始してください。

Ⓜ アイコンは、サーバー状況が使用不可であることを示します。 ノード・エージェントが実行されていない可能性があります。 ノード・エージェントを開始するには、コマンド・ウィンドウで `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh` コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. WBM\_DE.AppTarget.WBMNode1.0

以下の順序でサーバーを停止します。

- a. WBM\_DE.AppTarget.WBMNode1.0
- b. nodeagent

WBM\_DE.AppTarget.WBMNode1.0 サーバーを停止するには、サーバーを選択して「停止」をクリックします。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

5. 次の URL を使用して、アプリケーション・サーバーにおいて、WebSphere Business Monitor Business Space に WebSphere Portal システムからアクセスできることを確認してください。  
`http://APPLICATION_SERVER_HOST:9084/BusinessSpace` ここで、`APPLICATION_SERVER_HOST` は アプリケーション・サーバー のホスト名です。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## モニター (WebSphere Business Monitor モバイル・デバイス・コンソール) テスト

モニター (WebSphere Business Monitor モバイル・デバイス・コンソール) テストは、WebSphere Business Monitor Mobile HTTP URL を使用して、WebSphere Business Monitor Mobile にアクセスできるかどうか判別します。

## リソース

モニター (WebSphere Business Monitor モバイル・デバイス・コンソール) テストでは、以下のリソースを使用します。

- (アプリケーション・サーバー上の) WebSphere Application Server。

## 問題判別

モニター (WebSphere Business Monitor モバイル・デバイス・コンソール) テストが失敗した場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. アプリケーション・サーバーでは、以下の WebSphere Business Monitor ログを確認します。
    - /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM\_DE.AppTarget.WBMNode1.0/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM\_DE.AppTarget.WBMNode1.0/SystemErr.log
2. アプリケーション・サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
3. WebSphere Business Monitor サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。
  - a. アプリケーション・サーバー・システムで、ibmadmin としてログオンします。
  - b. コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
  - c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh コマンドを使用して、nodeagent を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。
    - a. メッセージ「ADMU0509I: The Application Server "WBM\_DE.AppTarget.WBMNode1.0" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startServer.sh WBM\_DE.AppTarget.WBMNode1.0 コマンドを使用して、WBM\_DE.AppTarget.WBMNode1.0 を始動します。メッセージ「ADMU0508I: The Application Server "WBM\_DE.AppTarget.WBMNode1.0" is STARTED.」が表示された場合、このステップを省略します。WBM\_DE.AppTarget.WBMNode1.0 を始動する必要があった場合、次のようなメッセージが表示されます。ADMU3000I: Server WBM\_DE.AppTarget.WBMNode1.0 open for e-business; process id is 26654

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. WBM\_DE.AppTarget.WBMNode1.0

以下の順序でサーバーを停止します。




- a. WBM\_DE.AppTarget.WBMNode1.0
- b. nodeagent

WBM\_DE.AppTarget.WBMNode1.0 サーバーを停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopServer.sh



WBM\_DE.AppTarget.WBMNode1.0 -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

4. WebSphere Business Monitor サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。
  - a. [http://APPLICATION\\_SERVER\\_HOST:9060/admin](http://APPLICATION_SERVER_HOST:9060/admin) で、WebSphere Application Server の管理 ID である admin およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。APPLICATION\_SERVER\_HOST は、アプリケーション・サーバー のホスト名です。
  - b. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Server」をクリックして、WBM\_DE.AppTarget.WBMNode1.0 サーバーの状況を表示します。
    -  アイコンは、サーバーが始動済みであることを示します。必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。
    -  アイコンは、サーバーが停止していることを示します。サーバーを選択して「開始」をクリックし、サーバーを開始してください。
    -  アイコンは、サーバー状況が使用不可であることを示します。ノード・エージェントが実行されていない可能性があります。ノード・エージェントを開始するには、コマンド・ウィンドウで /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/startNode.sh コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. WBM\_DE.AppTarget.WBMNode1.0

以下の順序でサーバーを停止します。

- a. WBM\_DE.AppTarget.WBMNode1.0
- b. nodeagent

WBM\_DE.AppTarget.WBMNode1.0 サーバーを停止するには、サーバーを選択して「停止」をクリックします。

nodeagent を停止するには、アプリケーション・サーバーのコマンド・ウィンドウでコマンド /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/bin/stopNode.sh -username waswebadmin -password WAS\_ADMIN\_PWD を実行します。ここでの WAS\_ADMIN\_PWD は WebSphere の管理者パスワードです。

5. 次の URL を使用して、アプリケーション・サーバーにおいて、WebSphere Business Monitor Mobile に WebSphere Portal システムからアクセスできることを確認してください。 [http://APPLICATION\\_SERVER\\_HOST:9084/mobile](http://APPLICATION_SERVER_HOST:9084/mobile) ここで、APPLICATION\_SERVER\_HOST は アプリケーション・サーバー のホスト名です。



## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## ポリシー (Tivoli Service Request Manager Maximo コンソール) テスト

ポリシー (Tivoli Service Request Manager Maximo コンソール) テストは、Tivoli Service Request Manager Maximo スタート・センター・ページを使用して、Tivoli Service Request Manager Maximo にアクセスできるかどうか判別します。

## リソース

ポリシー (Tivoli Service Request Manager Maximo コンソール) テストでは、以下のリソースを使用します。

- (イベント・サーバー上の) Tivoli Service Request Manager Maximo

## 問題判別

ポリシー (Tivoli Service Request Manager Maximo コンソール) テストが失敗した場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
    - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
  - b. イベント・サーバーでは、以下の Tivoli Service Request Manager ログを確認します。
    - /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log
    - /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log
2. イベント・サーバー・システムおよびアプリケーション・サーバー・システムのファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
3. Tivoli Service Request Manager サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。手動のステップは以下のとおりです。
  - a. イベント・サーバー・システムで、ibmadmin としてログオンします。
  - b. コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
  - c. メッセージ「ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh コマンドを使用して、nodeagent を始動します。メッセージ「ADMU0508I: The Application Server "nodeagent" is STARTED.」が表示された場合、このステップはスキップします。nodeagent を始動する必要があった場合、「ADMU3000I: Server nodeagent open for e-business; process id is 26654」のようなメッセージが表示されます。
    - a. メッセージ「ADMU0509I: The Application Server "MXServer1" cannot be reached. It appears to be stopped.」が表示された場合、/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startServer.sh MXServer1 コマンドを使用して、MXServer1 を始動します。メッセージ

「ADMU0508I: The Application Server "MXServer1" is STARTED.」が表示された場合、このステップを省略します。 MXServer1 を始動する必要があった場合、次のようなメッセージが表示されます。 ADMU3000I: Server MXServer1 open for e-business; process id is 26654

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. MXServer1


以下の順序でサーバーを停止します。


- a. MXServer1
- b. nodeagent


MXServer1 サーバーを停止するには、イベント・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopServer.sh MXServer1 -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

nodeagent を停止するには、イベント・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

4. Tivoli Service Request Manager サーバーが始動済みであることを確認してください。この確認は、WebSphere Application Server 管理コンソールを使用するか、手動のステップを行うことで実行できます。WebSphere Application Server 管理コンソールを使用する手順は、以下のとおりです。
  - a. `http://EVENT_SERVER_HOST:9061/admin` で、WebSphere Application Server の管理 ID である `admin` およびパスワードを使用して WebSphere Application Server 管理コンソールにログオンします。`EVENT_SERVER_HOST` は、イベント・サーバーのホスト名です。
  - b. 「サーバー」 > 「サーバー・タイプ」 > 「WebSphere Application Server」をクリックして、MXServer1 サーバーの状況を表示します。

 アイコンは、サーバーが始動済みであることを示します。必要な場合は、サーバーを選択して「再始動」をクリックし、サーバーを再始動してください。

 アイコンは、サーバーが停止していることを示します。サーバーを選択して「開始」をクリックし、サーバーを開始してください。

 アイコンは、サーバー状況が使用不可であることを示します。ノード・エージェントが実行されていない可能性があります。ノード・エージェントを開始するには、コマンド・ウィンドウで `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/startNode.sh` コマンドを実行します。

**重要:** サーバーは、指定された順序で開始および停止する必要があります。

以下の順序でサーバーを開始します。

- a. nodeagent
- b. MXServer1

以下の順序でサーバーを停止します。

- a. MXServer1
- b. nodeagent

MXServer1 サーバーを停止するには、サーバーを選択して「停止」をクリックします。

nodeagent を停止するには、イベント・サーバーのコマンド・ウィンドウでコマンド `/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin/stopNode.sh -username waswebadmin -password WAS_ADMIN_PWD` を実行します。ここでの `WAS_ADMIN_PWD` は WebSphere の管理者パスワードです。

5. 次の URL を使用して、イベント・サーバーにおいて、Tivoli Service Request Manager Maximo スタート・センター・ページに WebSphere Portal システムからアクセスできることを確認してください。  
`http://EVENT_SERVER_HOST:31015/maximo/ui/login` ここでの `EVENT_SERVER_HOST` はイベント・サーバーのホスト名です。ユーザー ID は `maxadmin` です。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## セキュリティー (Tivoli Access Manager) テスト

セキュリティー (Tivoli Access Manager) テストでは、管理サーバーから `pd_start` コマンドを送信して、その結果を確認することで、Tivoli Access Manager が実行されているかどうかを判別します。

## リソース

セキュリティー (Tivoli Access Manager) テストでは、以下のリソースを使用します。

- Tivoli Access Manager (Policy Server および Authorization Server を含む) (管理サーバー上)

## 問題判別

セキュリティー (Tivoli Access Manager) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## このタスクについて

以下のステップでは、`pdmgrd` を Tivoli Access Manager Authorization Server、`pdmgrproxyd` を Policy Proxy Server、`webseald-default` を Tivoli Access Manager WebSEAL サーバーとします。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. 管理サーバーでは、以下の Tivoli Access Manager ログを確認します。
    - `/var/PolicyDirector/log/msg_pdmgrd_utf8.log`
    - `/var/PolicyDirector/log/msg_pdacl_d_utf8.log`
  - b. アプリケーション・サーバーでは、以下の Tivoli Access Manager ログを確認します。
    - `/var/pdweb/log/msg_*.log`。ここでの `*` は任意の値です。
    - `/var/pdweb/log/config_data_*.log`。ここでの `*` は任意の値です。
2. 管理サーバー・システムおよびアプリケーション・サーバー・システムのファイル・システムが最大容量に達していないことを確認してください。これは `df -h` コマンドを使用して判別することができます。
3. 必要な Tivoli Access Manager コンポーネントが実行されていることを確認してください。

- a. 管理サーバーの端末セッションに `root` としてログオンします。
- b. `pd_start status` コマンドを実行します。結果は以下のようになります。

Tivoli Access Manager servers

Server	Enabled	Running
pdmgrd	yes	yes
pdacld	yes	yes
pdmgrproxyd	no	no

- c. pdmgrd サーバーまたは pdacld サーバーが実行されていない場合、`pd_start start` コマンドを実行して始動します。

注: pdmgrd サーバーと pdacld サーバーのみが管理サーバー上で使用可能です。この両方のサーバーは `pd_start start` コマンドで始動し、`pd_start stop` コマンドで停止できます。

4. 必要な Tivoli Access Manager WebSEAL コンポーネントが実行されていることを確認してください。

- a. アプリケーション・サーバーの端末セッションに `root` としてログオンします。
- b. `pd_start status` コマンドを実行します。結果は以下のようになります。

Tivoli Access Manager servers

Server	Enabled	Running
pdmgrd	no	no
pdacld	no	no
pdmgrproxyd	no	no
webseald-default	yes	yes

- c. webseald-default サーバーが実行されていない場合、`pd_start start` コマンドを実行して始動します。

注: webseald-default サーバーのみがアプリケーション・サーバー上で使用可能です。このサーバーは `pd_start start` コマンドで始動し、`pd_start stop` コマンドで停止できます。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## セキュリティ (Tivoli Access Manager Web Portal Manager) テスト

セキュリティ (Tivoli Access Manager Web Portal Manager) テストでは、Tivoli Access Manager Web Portal アプリケーション URL を使用して、Tivoli Access Manager Web Portal アプリケーションにアクセスできるかどうかを判別します。

## リソース

セキュリティ (Tivoli Access Manager Web Portal Manager) テストでは、以下のリソースを使用します。

- Tivoli Access Manager - Web Portal Manager (管理サーバー上)。

## 問題判別

セキュリティ (Tivoli Access Manager Web Portal Manager) テストが失敗した場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の WebSphere Portal ログを確認します。

- /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemOut.log
  - /opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal/SystemErr.log
- b. 管理サーバーでは、以下の Tivoli Access Manager - WebSphere Portal Manager ログを確認します。
    - /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log
    - /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log
2. 管理サーバー システム上のファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。
  3. Tivoli Access Manager - Web Portal Manager が始動されていることを確認します。
    - a. 管理サーバーで、ibmadmin としてログインします。
    - b. コマンド・ウィンドウで、コマンド (/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/serverStatus.sh -all -username waswebadmin -password WAS\_ADMIN\_PWD) を実行します。WAS\_ADMIN\_PWD は、WebSphere Application Server の管理者パスワードです。
    - c. メッセージ「ADMU0509I: The Application Server "dmgr" cannot be reached. It appears to be stopped.」が表示された場合、コマンド (/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/startManager.sh) を使用して dmgr を始動します。メッセージ「ADMU0508I: The Application Server "dmgr" is STARTED.」が表示された場合、このステップはスキップします。dmgr を始動する必要があった場合、「ADMU3000I: Server dmgr open for e-business; process id is 26654」のようなメッセージが表示されます。

管理サーバーのコマンド・ウィンドウでコマンド (/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/stopManager.sh -username waswebadmin -password WAS\_ADMIN\_PWD) を実行することで、WebSphere Application Server デプロイメント・マネージャー (Tivoli Access Manager - Web Portal Manager を含む) が停止します。WAS\_ADMIN\_PWD は、WebSphere の管理者パスワードです。

4. WebSphere Portal システムから Tivoli Access Manager - Web Portal Manager にアクセスできることを確認します。
  - a. 管理サーバーで、URL ([http://MANAGEMENT\\_SERVER\\_HOST9060/admin](http://MANAGEMENT_SERVER_HOST9060/admin)) にアクセスします。MANAGEMENT\_SERVER\_HOST は、管理サーバーのホスト名です。
  - b. 「Tivoli Access Manager」 > 「Web Portal Manager」 > 「ユーザー」 > 「ユーザーの検索」をクリックします。
  - c. sec\_master ユーザーとしてログオンします。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## セキュリティ (WebSEAL コンソール) テスト

セキュリティ (WebSEAL コンソール) テストでは、ポート 80 で WebSEAL HTTP URL にアクセスし、ストリング「Intelligent Operations Center」に関して返されたページを検証することで、Tivoli Access Manager および Tivoli Access Manager WebSEAL が必要なリソースを使用して実行されているかどうかを判別します。

## リソース

セキュリティ (WebSEAL コンソール) テストでは、以下のリソースを使用します。

- Tivoli Access Manager (Policy Server および Authorization Server を含む) (管理サーバー上)
- Tivoli Access Manager WebSEAL (アプリケーション・サーバー上)

## 問題判別

セキュリティー (WebSEAL コンソール) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## このタスクについて

以下のステップでは、pdmgrd を Tivoli Access Manager Authorization Server、pdmgrproxyd を Policy Proxy Server、webseald-default を Tivoli Access Manager WebSEAL サーバーとします。

## 手順

1. 実行時例外については、ログ・ファイルを確認してください。
  - a. 管理サーバーでは、以下の Tivoli Access Manager ログを確認します。
    - /var/PolicyDirector/log/msg\_\_pdmgrd\_utf8.log
    - /var/PolicyDirector/log/msg\_\_pdacld\_utf8.log
  - b. アプリケーション・サーバーでは、以下の Tivoli Access Manager ログを確認します。
    - /var/pdweb/log/msg\_\_\*.log。ここでの \* は任意の値です。
    - /var/pdweb/log/config\_data\_\_\*.log。ここでの \* は任意の値です。
2. 管理サーバー・システムおよびアプリケーション・サーバー・システムのファイル・システムが最大容量に達していないことを確認してください。これは **df -h** コマンドを使用して判別することができます。

3. 必要な Tivoli Access Manager コンポーネントが実行されていることを確認してください。

- a. 管理サーバーの端末セッションに **root** としてログオンします。
- b. **pd\_start status** コマンドを実行します。結果は以下のようになります。

Tivoli Access Manager servers

Server	Enabled	Running
-----		
pdmgrd	yes	yes
pdacld	yes	yes
pdmgrproxyd	no	no

- c. pdmgrd サーバーまたは pdacld サーバーが実行されていない場合、**pd\_start start** コマンドを実行して始動します。

注: pdmgrd サーバーと pdacld サーバーのみが管理サーバー上で使用可能です。この両方のサーバーは **pd\_start start** コマンドで始動し、**pd\_start stop** コマンドで停止できます。

4. 必要な Tivoli Access Manager WebSEAL コンポーネントが実行されていることを確認してください。

- a. アプリケーション・サーバーの端末セッションに **root** としてログオンします。
- b. **pd\_start status** コマンドを実行します。結果は以下のようになります。

Tivoli Access Manager servers

Server	Enabled	Running
-----		
pdmgrd	no	no
pdacld	no	no
pdmgrproxyd	no	no
webseald-default	yes	yes

- c. webseald-default サーバーが実行されていない場合、**pd\_start start** コマンドを実行して始動します。



注: webseald-default サーバーのみがアプリケーション・サーバー上で使用可能です。このサーバーは `pd_start start` コマンドで始動し、`pd_start stop` コマンドで停止できます。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## Web サーバー (IBM HTTP Server コンソール) テスト

Web サーバー (IBM HTTP Server コンソール) テストでは、IBM HTTP Server URL にアクセスすることで、IBM HTTP Server へのアクセス性をテストします。

## リソース

Web サーバー (IBM HTTP Server コンソール) では、以下のリソースを使用します。

- IBM HTTP Server (アプリケーション・サーバー上)。

## 問題判別

Web サーバー (IBM HTTP Server コンソール) テストが失敗した場合、以下を実行し、問題を特定して解決してください。

## 手順

1. アプリケーション・サーバーへのネットワーク接続があることを確認します。これを行うには、アプリケーション・サーバーの短縮ホスト名と完全修飾ホスト名の両方を指定して、`ping` コマンドを送信します。`ping` コマンドの結果は、ホスト名が DNS または `/etc/hosts` ファイルにより正しく解決されているかどうかを表します。
2. 実行時例外については、ログ・ファイルを確認してください。
  - a. アプリケーション・サーバーでは、以下の IBM HTTP ログを確認します。
    - `/opt/IBM/HTTPServer/logs/error_log`
    - `/opt/IBM/HTTPServer/logs/access_log`
3. アプリケーション・サーバー 上のファイル・システムが最大容量に達していないことを確認してください。これは `df -h` コマンドを使用して判別することができます。
4. WebSphere Portal システムから IBM HTTP Server のデフォルト・ページにアクセスできることを確認します。
  - a. アプリケーション・サーバーで、`https://APPLICATION_SERVER_HOST:82/` にアクセスします。`APPLICATION_SERVER_HOST` は、アプリケーション・サーバーのホスト名です。
  - b. デフォルト・ページにアクセスできない場合、`ps -ef | grep HTTPServer` コマンドを実行して、IBM HTTP Server プロセスが実行されているかどうかを判別します。IBM HTTP Server プロセスは、`/opt/IBM/HTTPServer/bin/httpd` で始まります。7 個のプロセスが存在します。
  - c. 一部のプロセスのみ (すべてのプロセスではない) が実行されている場合、すべてのプロセスを再開する前に、実行中のプロセスを停止します。
    - 1) アプリケーション・サーバーで、`root` としてログインします。
    - 2) `/opt/IBM/HTTPServer/bin` ディレクトリーに移動します。
    - 3) 次のコマンドを実行して、実行されているすべての IBM HTTP プロセスを停止します。

```
./apachectl stop
./adminctl stop
```

- 4) `ps -ef | grep HTTPServer` コマンドを実行して、すべてのプロセスが停止していることを確認します。
- 5) 実行されている IBM HTTP Server プロセスがまだ存在する場合、`kill -9 pid` コマンドを使用して停止します。 `pid` は、IBM HTTP Server プロセスのプロセス ID です。
- d. HTTP Server プロセスが実行されていない場合、IBM HTTP Server コンポーネントを始動します。
  - 1) アプリケーション・サーバーで、`root` としてログオンします。
  - 2) `/opt/IBM/HTTPServer/bin` ディレクトリに移動します。
  - 3) 次のコマンドを実行して、実行されているすべての IBM HTTP プロセスを開始します。

```
./adminctl start
./apachectl start
```
  - 4) `ps -ef | grep HTTPServer` コマンドを実行して、すべてのプロセスが開始されていることを確認します。

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## Intelligent Operations Center イベント・フロー・テスト

Intelligent Operations Center イベント・フロー・テストでは、IBM Intelligent Operations Center のイベント・プロセスに関連する重要なコンポーネントが予想したとおりに機能しているかどうかを検証します。そのために、外部イベントをシミュレートして、予想したとおりの結果が得られるかどうかを判別します。

## リソース

Intelligent Operations Center イベント・フロー・テストでは、以下のリソースを使用します。

- IBM WebSphere Message Broker (アプリケーション・サーバー上)
- IBM WebSphere Message Queue (アプリケーション・サーバー上)
- IBM Netcool/OMNIBus (イベント・サーバー上)
- IBM Netcool/Impact (イベント・サーバー上)
- IBM DB2 (データ・サーバー上)

## 問題判別

Intelligent Operations Center イベント・フロー テストが失敗した場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. IBM Intelligent Operations Center コンポーネントが実行されていることを確認してください。
  - a. 管理サーバーのコマンド・ウィンドウで、`/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password` を実行します。ここでの `password` は、IBM Intelligent Operations Center が配置されたときに定義される IBM Intelligent Operations Center の管理者パスワードです。
  - b. 実行されていないコンポーネントがある場合、`/opt/IBM/ISP/mgmt/scripts/IOControl.sh start component_ID password` を実行してそれらのコンポーネントを開始します。ここでの `password` は、IBM Intelligent Operations Center が配置されたときに定義される IBM Intelligent Operations Center の管理者パスワードであり、`component_ID` は、`/opt/IBM/ISP/mgmt/scripts/IOControl.sh help` の実行時に「ターゲット・オプション」の下にリストされる ID です。

2. エラーがないかどうか、イベント・サーバーの Netcool/OMNIBus ログ (/opt/IBM/netcool/omnibus/log/ioc\_xml.log) を確認します。
3. 必要に応じて、イベント・サーバーで以下を実行して、Tivoli Netcool/OMNIBus プローブを開始します。

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log  
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。

## Intelligent Operations Center 通知フロー・テスト

Intelligent Operations Center 通知フロー・テストでは、IBM Intelligent Operations Center の通知プロセスに関連する重要なコンポーネントが予想したとおりに機能しているかどうかを検証します。そのために、外部通知をシミュレートして、予想したとおりの結果が得られるかどうかを判別します。

## リソース

Intelligent Operations Center 通知フロー・テストでは、以下のリソースを使用します。

- IBM WebSphere Message Queue (アプリケーション・サーバー上)
- IBM Netcool/OMNIBus (イベント・サーバー上)
- IBM Netcool/Impact (イベント・サーバー上)
- IBM DB2 (データ・サーバー上)

## 問題判別

Intelligent Operations Center 通知フロー テストが失敗した場合、以下を実行し、アクセス関連の問題を特定して解決してください。

## 手順

1. IBM Intelligent Operations Center コンポーネントが実行されていることを確認してください。
  - a. 管理サーバーのコマンド・ウィンドウで、**/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password** を実行します。ここでの *password* は、IBM Intelligent Operations Center が配置されたときに定義される IBM Intelligent Operations Center の管理者パスワードです。
  - b. 実行されていないコンポーネントがある場合、**/opt/IBM/ISP/mgmt/scripts/IOControl.sh start component\_ID password** を実行してそれらのコンポーネントを開始します。ここでの *password* は、IBM Intelligent Operations Center が配置されたときに定義される IBM Intelligent Operations Center の管理者パスワードであり、*component\_ID* は、**/opt/IBM/ISP/mgmt/scripts/IOControl.sh help** の実行時に「ターゲット・オプション」の下にリストされる ID です。
2. エラーがないかどうか、イベント・サーバーの Netcool/OMNIBus ログ (/opt/IBM/netcool/omnibus/log/ioc\_xml.log) を確認します。
3. 必要に応じて、イベント・サーバーで以下を実行して、Tivoli Netcool/OMNIBus プローブを開始します。

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log  
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```

## 次のタスク

見つかった問題やエラーをすべて解決し、テストを再試行します。



---

## 第 7 章 ソリューションの保守

このセクションで説明しているタスクを実行して、ソリューションが常にスムーズに実行されるようにしてください。

---

### データのバックアップ

IBM Intelligent Operations Center 内の重要なデータの損失を防ぐため、特定のファイル、ディレクトリ、データベースを一定の間隔でバックアップしてください。

IBM Intelligent Operations Center を拡張する場合、追加した項目のバックアップ手順を作成することをお勧めします。追加項目の例を以下に示します。

- レポート
- 補助データベース
- データベース表
- カスタム分析
- ポートレット
- Java アプリケーション

以下のような累積データのバックアップも検討してください。

- Common Access Protocol (CAP) データベース・データ
- IBM WebSphere Business Monitor データベース・データ
- Lightweight Directory Access Protocol (LDAP) ユーザー・レジストリー・データ
- 地理情報システム (GIS) データ

追加した拡張を簡単に識別できるように、命名規則を使用してください。通常は、元のソリューションのインストール後に作成または蓄積したデータを追跡します。ソリューションのアップグレード時に重要なデータを失わないように、データをバックアップするための手順を実行してください。

### データベースのバックアップ

IBM Intelligent Operations Center でのバックアップが推奨されるデータベースを、以下の表に示します。

表 80. IBM Intelligent Operations Center データベース

サービスまたはコンポーネント	データベース・インスタンス	データベース名	サーバー
Intelligent Operations Center データベース	db2inst1	• IOCDB	データ・サーバー

表 80. IBM Intelligent Operations Center データベース (続き)

サービスまたはコンポーネント	データベース・インスタンス	データベース名	サーバー
ポータル	db2inst2	<ul style="list-style-type: none"> <li>• CUSTDB</li> <li>• FDBKDB</li> <li>• LKMDDDB</li> <li>• JCRDB</li> <li>• COMMDB</li> <li>• RELDB</li> </ul>	データ・サーバー
ビジネス・インテリジェンス	db2inst3	<ul style="list-style-type: none"> <li>• CXLOGDB</li> <li>• CXCONTDB</li> </ul>	データ・サーバー
ビジネス・ルールおよびビジネス・アクティビティ・モニター	db2inst4	<ul style="list-style-type: none"> <li>• UDDIDB</li> <li>• WODMDCDB</li> <li>• MONITOR</li> <li>• WBMDB</li> <li>• RESDB</li> </ul>	データ・サーバー
セマンティック・モデル	db2inst5	<ul style="list-style-type: none"> <li>• JTS</li> <li>• IIC</li> </ul>	データ・サーバー
サービス要求の管理	db2inst6	<ul style="list-style-type: none"> <li>• MAXIMO</li> </ul>	データ・サーバー
ID 管理	db2inst7	<ul style="list-style-type: none"> <li>• TIMDB</li> </ul>	データ・サーバー
アプリケーション	db2inst8	<ul style="list-style-type: none"> <li>• LDAPDB</li> <li>• LDAPDB2B</li> </ul>	データ・サーバー

## 仮想インフラストラクチャー・スナップショットの作成

ほとんどの仮想インフラストラクチャーには、特定の時点での仮想環境の状態とデータを保持するスナップショット機能があります。大規模な変更を実行する前に、現在の環境のスナップショットを取ることを強くお勧めします。多くの仮想インフラストラクチャー管理ツールが用意されていますが、それらのほとんどで、スナップショット機能が独自に実装されています。仮想インフラストラクチャー・ベンダーが提供する管理ガイドの指示を注意深く読んで、仮想環境を正しくバックアップする方法についての具体的な要件と手順を理解することが重要です。

### 関連タスク:

190 ページの『KPI をカスタマイズする前にバックアップする』

IBM WebSphere Business Monitor を使用して、または「重要業績評価指標」ポートレットを使用して作成または変更された KPI を、バックアップおよび復元します。

### 関連情報:


 IBM Smarter Cities Software Solutions Redbooks

## パフォーマンスの調整

以下の各セクションでは、アプリケーション・サーバーと WebSphere Application Server を調整する方法について説明します。



## 関連情報:

 [IBM Websphere Portal バージョン 7.0 パフォーマンス・チューニング・ガイド](#)

 [IBM Websphere Application Server、Network Deployment、バージョン 7.0 インフォメーション・センター](#)

## アプリケーション・サーバーの調整

### このタスクについて

パフォーマンス・テストの結果に基づく以下のガイドラインを使用して、Java 仮想マシンのヒープ・サイズを設定します。

### 手順

1. 最小ヒープ・サイズと最大ヒープ・サイズを同じ値に設定します。
2. 物理メモリーに適合し、かつ 2 GB を超える値にヒープ・サイズを設定します。

### 次のタスク

詳しくは、このトピックの終わりにある関連リンクを参照してください。

## WebSphere Application Server の調整

WebSphere Application Server バージョン 7 のパフォーマンスの調整については、このトピックの末尾にある関連リンクを参照してください。

---

## ログ・ファイルの管理

IBM Intelligent Operations Center では、いくつかの異なる場所にログ・ファイルが保管されます。システム・パフォーマンスの問題を回避するために、定期的にログ・ファイルをアーカイブし、元のログ・ファイルを削除します。

ログ・ファイルを管理しておらず、ログ・ファイルの数が無制限に増えると、ファイル・システム・パーティションが最終的にログ・ファイルでいっぱいになってしまう可能性があります。ファイル・システム・パーティションがいっぱいになると、悪影響を与えることがあり、システムが停止する可能性があります。

IBM Intelligent Operations Center で使用可能なログ・ファイルについて詳しくは、このトピックの末尾にあるリンクを参照してください。

### 関連概念:

331 ページの『コンポーネントのトラブルシューティング』

システム検査チェック・ツールを使用して、IBM Intelligent Operations Center のコンポーネントのトラブルシューティングを実行できます。

---

## シングル・サインオンのための LTPA トークンの更新

IBM Intelligent Operations Center では、Lightweight Third-Party Authentication (LTPA) トークンを使用して、多くのサービス間でのシングル・サインオンを有効にします。インストール時に生成されたトークンおよび鍵には、有効期限はありません。これは、定期的に LTPA トークンを再生成し、そのトークンを使用してサービスを更新するための、セキュリティー・グッド・プラクティスです。

## 始める前に

IBM Intelligent Operations Center 製品をインストールしてすべてのサービスを開始してから、LTPA トークンを更新する必要があります。

この手順では、すべてのサービスを停止して開始する必要があるため、システムが実動状態にある場合は更新を行わないでください。システムにログインしたユーザーのサービスが中断され、データが失われる可能性があります。

## 手順

アプリケーション・サーバーの新規 LTPA トークンを生成します。

1. アプリケーション・サーバーで Web ブラウザーを開き、`http://application_host:9060/ibm/console` に移動します。ここで、`application_host` は、アプリケーション・サーバーのホスト名です。
2. トポロジー・プロパティ・ファイルの `WAS.ADMIN.ACCOUNT.PWD` パラメーターで指定されているパスワードを使用して、`webwasadmin` ユーザーとしてログオンします。
3. 「セキュリティ」 > 「グローバル・セキュリティ」 > 「認証メカニズムおよび有効期限」 > 「LTPA」 > 「鍵の生成」をクリックします。
4. 新規 LTPA トークンのパスワードを 2 回入力します。このパスワードは、LTPA トークンの暗号化に使用されます。このパスワードは、LTPA トークンのインポート時にも使用されます。このパスワードは、トポロジー・プロパティ・ファイルの `WAS.LTPA.PWD` パラメーターとして記録してください。
5. LTPA トークンの保存場所のパスとファイル名を入力します。例えば `/tmp/newapp.ltpa` とします。別のパスまたはファイル名を指定する場合は、残りのステップで、`/tmp/newapp.ltpa` をご使用のパスおよびファイル名に置き換えてください。
6. 「鍵のエクスポート」をクリックします。新規 LTPA トークンが `/tmp/newapp.ltpa` として保存されます。
7. 「メッセージ」 > 「保存」をクリックします。更新が保存されます。シングル・サインオンのドメインが定義されていないことについての警告は無視してください。

新規 LTPA トークンを、イベント・サーバーにコピーします。

8. アプリケーション・サーバーで、`root` ユーザーとしてログオンし、端末ウィンドウを開きます。
9. `cp /tmp/newapp.ltpa /tmp/stproxy.ltpa` コマンドを実行します。これにより、IBM Intelligent Operations Center のインストール時に作成されたファイルを置き換えます。
10. `scp /tmp/newapp.ltpa root@event_host :/tmp/newapp.ltpa` コマンドを実行します。ここで、`event_host` は、イベント・サーバーのホスト名です。プロンプトが表示されたら、イベント・サーバーの `root` パスワードを入力します。LTPA トークンが、イベント・サーバーにコピーされます。

新規 LTPA トークンをインポートします。

11. イベント・サーバーで Web ブラウザーを開き、`http://event_host:9061/ibm/console` に移動します。ここで、`event_host` は、イベント・サーバーの完全修飾ホスト名です。
12. トポロジー・プロパティ・ファイルの `TSRM.WAS.ADMIN.PWD` パラメーターで指定されているパスワードを使用して、`webwasadmin` ユーザーとしてログオンします。
13. 「セキュリティ」 > 「セキュア管理、アプリケーション、およびインフラストラクチャー」 > 「認証メカニズムおよび有効期限」をクリックします。
14. LTPA トークンのパスワードと、ファイル名の `/tmp/newapp.ltpa` を入力します。
15. 「鍵のインポート」をクリックします。

16. 「メッセージ」 > 「保存」をクリックします。更新が保存されます。イベント・サーバーの新規 LTPA トークンを生成します。
17. 「認証メカニズムおよび有効期限」 > 「鍵の生成」をクリックします。
18. 新規 LTPA トークンのパスワードを 2 回入力します。このパスワードは、LTPA トークンのインポート時にも使用されます。
19. LTPA トークンの保存場所のパスとファイル名を入力します。例えば /tmp/newevent.ltpa とします。別のパスまたはファイル名を指定する場合は、残りのステップで、/tmp/newevent.ltpa をご使用のパスおよびファイル名に置き換えてください。
20. 「鍵のエクスポート」をクリックします。新規 LTPA トークンが /tmp/newevent.ltpa として保存されます。
- イベント・サーバーの新規 LTPA トークンを、アプリケーション・サーバーにコピーします。
21. アプリケーション・サーバーで、root ユーザーとしてログオンし、端末ウィンドウを開きます。
22. `scp /tmp/newevent.ltpa root@event_host :/tmp/newevent.ltpa` コマンドを実行します。ここで、*event\_host* は、イベント・サーバーのホスト名です。プロンプトが表示されたら、イベント・サーバーの root パスワードを入力します。LTPA トークンが、イベント・サーバーにコピーされます。新規 LTPA トークンを指定して、セキュリティー・サービスを更新します。
23. アプリケーション・サーバーで、root ユーザーとしてログオンし、端末ウィンドウを開きます。
24. `cp /tmp/newapp.ltpa /opt/pdweb/etc/` コマンドを実行します。
25. `cp /tmp/newevent.ltpa /opt/pdweb/etc/` コマンドを実行します。
26. 以下のコマンドを含む、/tmp/pd.com という名前のコマンド・ファイルを作成します。

```
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebclient
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stbaseapi
server task default-webseald-application_host create -t tcp -h application_host -p 9086 -x -b
ignore -i -f -A -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw /stwebapi
server task default-webseald-application_host create -t tcp -h application_host -p 9081 -b
supply -c iv-user,iv-creds -i -j -f -J trailer -A -2 -F /opt/pdweb/etc/newapp.ltpa -Z appLTPApw
/cognosserver task default-webseald-application_host create -t tcp -h event_host -p 82 -i
-j -f -J trailer -A -2 -F /opt/pdweb/etc/newevent.ltpa -Z eventLTPApw /tsrm
```

ここで、

*application\_host*

アプリケーション・サーバーの完全修飾ホスト名です。

*event\_host*

イベント・サーバーの完全修飾ホスト名です。

*appLTPApw*

アプリケーション・サーバーの LTPA トークンの作成時に指定したパスワードです。

*eventLTPApw*

イベント・サーバーの LTPA トークンの作成時に指定したパスワードです。

27. `/opt/PolicyDirector/bin/pdadmin -a sec_master -p password / tmp/pd.com` コマンドを実行します。ここで、*password* は、トポロジー・プロパティ・ファイルの TAM.WEBSEAL.ADMIN.PWD パラメーターで定義されたパスワードです。

コラボレーション・サービスのシングル・サインオンを更新します。

28. 60 ページの『コラボレーション・サービス用のシングル・サインオンの構成』のステップに従って、コラボレーション・サービスのシングル・サインオンを更新します。

すべてのサービスを停止して再開します。

29. プラットフォーム制御ツールを使用して、すべてのサービスを停止します。

30. プラットフォーム制御ツールを使用して、すべてのサービスを開始します。 LTPA トークンが、すべてのサービスに反映されます。

---

## 保守のヒント

ソリューションの保守に関する詳細なヒントについては、IBM サポート・ポータルに個々の技術情報の形式で文書化されています。

次のリンクをクリックすると、すべてのバージョンの IBM Intelligent Operations Center について、稼働中のサポート知識ベースのカスタマイズされた照会が起動します。 IBM Intelligent Operations Center の保守のヒントをすべて表示する。

---

## 第 8 章 ソリューション・インターフェースの使用

IBM Intelligent Operations Center は、ポータル・テクノロジーを使用する Web ベースのソリューションです。このソリューションには、サポートされるいずれかの Web ブラウザーを使用してアクセスできます。

サポートされる Web ブラウザーについては、トピックの末尾にあるリンクを参照してください。

### 関連情報:



IBM Intelligent Operations Center でサポートされるブラウザー

---

## ログオン

ログオンして IBM Intelligent Operations Center ユーザー・インターフェースにアクセスします。

### 始める前に

ローカル管理者に連絡して、ユーザー ID とパスワードを取得してください。組織内におけるユーザーの役割に適したセキュリティ・アクセス・レベルを付与することは、管理者の担当業務です。また、管理者は、ソリューション・ポータルにアクセスするための Web アドレス URL もユーザーに提供します。

### このタスクについて

以下の手順に従い、新規ブラウザー・セッションを開始して、IBM Intelligent Operations Center にアクセスします。また、ご使用の環境にインストールされている他の IBM Smarter Cities Software Solutionsからこのソリューションにアクセスすることもできます。ポータルの上部にあるメイン・ナビゲーション・バーで、「**Intelligent Operations Center**」を選択してください。

### 手順

1. ブラウザーのアドレス・フィールドに URL を入力します。

注: URL には完全修飾ドメイン名 (例: `http://application_server_hostname/wpsv70/wps/myportal`) を使用する必要があります。登録された完全修飾ドメインの代わりに IP アドレスを使用すると、ポートレットが正しく表示されないことがあります。

2. ログイン・ページで、ユーザー ID とパスワードを入力します。
3. 「サインイン」をクリックします。

### タスクの結果

アクセスを許可されたページ、機能、およびデータのみが表示されます。追加のアクセス権限が必要な場合は、管理者に連絡してください。

## 関連タスク:

『ログオフ』

ログオフして IBM Intelligent Operations Center ユーザー・インターフェースを終了し、サーバー・セッションを終了させます。デフォルトでは、「ログアウト」リンクは IBM Intelligent Operations Center の右上隅に表示されます。

---

## ログオフ

ログオフして IBM Intelligent Operations Center ユーザー・インターフェースを終了し、サーバー・セッションを終了させます。デフォルトでは、「ログアウト」リンクは IBM Intelligent Operations Center の右上隅に表示されます。

## 関連タスク:

293 ページの『ログオン』

ログオンして IBM Intelligent Operations Center ユーザー・インターフェースにアクセスします。

---

## ユーザー・プロファイルの表示または編集

IBM Intelligent Operations Center のユーザー・プロファイルの情報は、表示または変更することができます。

### このタスクについて

ユーザー・プロファイルには、ユーザー自身または管理者によって事前に入力された情報が含まれています。属性フィールドで情報を編集して、プロファイルを更新することができます。例えば、既存のパスワードを新しいパスワードに変更することができます。

表 81. IBM Intelligent Operations Center のユーザー・プロファイル属性

属性	説明	ユーザーによる編集の可否
ユーザー ID*	それぞれの新規ユーザーには、識別を可能にするため、管理者によって ID が割り当てられます。	いいえ
パスワード*	パスワードは、セキュリティのため、管理者によって割り当てられます。パスワードは固有のものであり、長さは 5 から 60 文字の範囲である必要があります。有効なパスワードとみなされるためには、文字 a から z、A から Z、ピリオド (.)、ダッシュ (-)、および下線 (_) のみを使用する必要があります。	はい
名	名 (姓に対する名) は、管理者またはユーザーが入力することができます。	はい
姓*	姓 (名字) は、管理者が入力します。	はい
E メール	E メール・アドレスは、管理者またはユーザーが入力することができます。	はい

注: アスタリスクが付いている属性は、新規ユーザーの正常な作成に必須です。アスタリスクが付いていない属性は、オプションです。

## 手順

1. 上部のナビゲーション・バーの右側にある「マイ・プロファイルの編集」を選択します。ユーザー自身のプロファイルの属性が表示されます。
2. パスワードを変更するには、以下のようにします。
  - a. 現在のパスワードを入力します (パスワード・テキストは表示されません)。



- b. 「新規パスワード」フィールドおよび「パスワードの確認」フィールドに、新規パスワードを入力します。
3. 残りの任意のフィールドで、情報を入力または編集します。
4. 変更を実行依頼するため、「OK」をクリックします。

## タスクの結果

変更内容に基づいてユーザー・プロフィールが更新されます。

---

## ページの使用

ページは 1 つまたは複数の補助ポートレットから構成されています。 IBM Intelligent Operations Center を使用すると、ページのポートレットと対話して、必要な情報にアクセスし、必要に応じてイベントに対応できます。

IBM Intelligent Operations Center には、6 つの異なるサンプル・ページ・ビューが用意されています。

### Administrator

管理者権限がある場合、ページを管理するためのポータル・サービスにアクセスできます。ページの編集や新規ページの作成を実行できます。ページ名タブの右側をクリックし、ページ・メニューからオプションを選択します。詳しくは、トピックの末尾にあるリンクを参照してください。

#### 関連タスク:

161 ページの『ページの作成またはカスタマイズ』

IBM Intelligent Operations Center に組み込む新規ページを作成し、それらのページにどのポートレットを表示するかを指定することができます。各ページに組み込むポートレットの外観およびレイアウトをカスタマイズできます。

## 「スーパーバイザー: 状況」ビュー

「スーパーバイザー: 状況」ビューでは、重要業績評価指標 (KPI) と主要なイベントをまとめて表示することができます。複数の組織にわたる職務を担当するユーザーは、「スーパーバイザー: 状況」ビューを使用して、組織の業績と福利の主要分野について、状況の変化をモニターおよび管理し、その変化に対応することができます。

「スーパーバイザー: 状況」ビューは、対話式 Web ページです。このページには、表 82 にリストされているポートレットが含まれています。これらのポートレットは、エグゼクティブ・レベルで総合情報および対話を提供するために相互に連携するページ内の独立したセクションです。

表 82. 「スーパーバイザー: 状況」ビューのポートレット

ポートレット	説明
321 ページの『状況』	「状況」ポートレットには、表示する権限のある複数の組織全体にわたって、KPI の状況に関するエグゼクティブ・レベルのサマリーが表示されます。計画を立て、必要に応じて対処できるように、このポートレットを使用して、KPI の状況に関する最新の変更を確認します。

表 82. 「スーパーバイザー: 状況」ビューのポートレット (続き)

ポートレット	説明
304 ページの『重要業績評価指標のドリルダウン』	「重要業績評価指標のドリルダウン」ポートレットで特定の KPI カテゴリに絞り込んで表示するには、「状況」ポートレットでそのカテゴリをクリックします。こうすることで、そのカテゴリのみが「重要業績評価指標のドリルダウン」ポートレットに表示されるようになります。そのリストを使用して、状況が変わる原因となった KPI の詳細に到達するまで、基礎となる KPI を調べることができます。
316 ページの『通知』	「通知」ポートレットは、KPI および関連イベントの変更により発生したアラートの動的な対話式リストを提供します。このポートレットの役割は、KPI またはイベント状況の変更に注意を促すことです。このリストには各アラートの重要な詳細情報が含まれています。例えば、KPI の状況が黄色から赤色に変わると、アラートが「通知」ポートレットに送信されます。
314 ページの『マイ・アクティビティー』	ログオンしているユーザーは、「マイ・アクティビティー」ポートレットで、これらの所有者に割り当てられたアクティビティーを表示することができます。「マイ・アクティビティー」ポートレット内のアクティビティーは、その親の標準操作手順でグループ化されています。それぞれの標準操作手順は、個々のイベントに対応します。
300 ページの『連絡先』	「連絡先」ポートレットを使用すると、カテゴリ別に分類された連絡先のリストを表示することができます。連絡する必要がある相手に基づいたカテゴリ別に、連絡先を分類できます。例えば、一般的な作業連絡先のカテゴリや、プロジェクト作業連絡先の別のカテゴリを設定できます。「連絡先」ポートレットを使用して、それらの連絡先とやり取りしたり、自身のオンライン状況、連絡先、またはグループを変更したりすることができます。

## 「スーパーバイザー: 操作」ビュー

「スーパーバイザー: 操作」ビューを使用して、イベントが発生した時点でその概要を把握することができます。「スーパーバイザー: 操作」ビューは、現在のイベントをモニターし、将来のイベントについて計画を策定するスーパーバイザーおよび管理者を対象としています。

「スーパーバイザー: 操作」ビューは、対話式 Web ページです。このページには、297 ページの表 83 にリストされているポートレットが含まれています。これらのポートレットは、管理レベルで総合情報および対話を提供するために相互に連携するページ内の独立したセクションです。

表 83. 「スーパーバイザー: 操作」ビューのポートレット

ポートレット	説明
309 ページの『マップ』	<p>イベント・マーカーおよびリソース・マーカーが表示される地理的領域のマップ。</p> <p>マップ上および「マップ」ポートレットにリンクしているポートレット内に表示されるイベントのカテゴリを選択するためのフィルター・フォーム。</p> <p>マップ上およびリンクしている「詳細」ポートレットの「リソース」タブ内に表示されるリソースの機能を選択するためのフィルター・フォーム。このフォームを表示するには、まず、「詳細」ポートレットで「近隣リソースの表示」を選択します。</p>
301 ページの『詳細』	<p>「詳細」ポートレットは対話式のリスト・ポートレットです。ユーザーに表示権限があるすべてのイベントが、イベント・リストと、「詳細」ポートレットにリンクされた任意のマップ・ポートレットに表示されます。</p>
316 ページの『通知』	<p>「通知」ポートレットは、KPI および関連イベントの変更により発生したアラートの動的な対話式リストを提供します。このポートレットの役割は、KPI またはイベント状況の変更に注意を促すことです。このリストには各アラートの重要な詳細情報が含まれています。例えば、関連するインシデントが所定のエリア内で発生すると、アラートが「通知」ポートレットに送信されます。</p>
314 ページの『マイ・アクティビティ』	<p>ログオンしているユーザーは、「マイ・アクティビティ」ポートレットで、これらの所有者に割り当てられたアクティビティを表示することができます。「マイ・アクティビティ」ポートレット内のアクティビティは、その親の標準操作手順でグループ化されています。それぞれの標準操作手順は、個々のイベントに対応します。</p>
300 ページの『連絡先』	<p>「連絡先」ポートレットを使用すると、カテゴリ別に分類された連絡先のリストを表示することができます。連絡する必要がある相手に基づいたカテゴリ別に、連絡先を分類できます。例えば、一般的な作業連絡先のカテゴリや、プロジェクト作業連絡先の別のカテゴリを設定できます。「連絡先」ポートレットを使用して、それらの連絡先とやり取りしたり、自身のオンライン状況、連絡先、またはグループを変更したりすることができます。</p>

## 「オペレーター: 操作」ビュー

「オペレーター: 操作」ビューを使用して、イベントとそれらの位置を常時把握することができます。「オペレーター: 操作」ビューは、最新のイベントのモニターとそれらへの対応を担当するオペレーター、管理者、またはその他のユーザーを対象としています。

「オペレーター: 操作」ビューは、対話式 Web ページです。このページには、298 ページの表 84 にリストされているポートレットが含まれています。これらのポートレットは、操作レベルで総合情報および対話を提供するために相互に連携するページ内の独立したセクションです。

表 84. 「オペレーター: 操作」ビューのポートレット

ポートレット	説明
309 ページの『マップ』	<p>イベント・マーカーおよびリソース・マーカーが表示される地理的領域のマップ。</p> <p>マップ上および「マップ」ポートレットにリンクしているポートレット内に表示されるイベントのカテゴリを選択するためのフィルター・フォーム。</p> <p>マップ上およびリンクしている「詳細」ポートレットの「リソース」タブ内に表示されるリソースの機能を選択するためのフィルター・フォーム。このフォームを表示するには、まず、「詳細」ポートレットで「<b>近隣リソースの表示</b>」を選択します。</p>
301 ページの『詳細』	<p>「詳細」ポートレットは対話式のリスト・ポートレットです。ユーザーに表示権限があるすべてのイベントが、イベント・リストと、「詳細」ポートレットにリンクされた任意のマップ・ポートレットに表示されます。</p>
316 ページの『通知』	<p>「通知」ポートレットは、KPI および関連イベントの変更により発生したアラートの動的な対話式リストを提供します。このポートレットの役割は、KPI またはイベント状況の変更に注意を促すことです。このリストには各アラートの重要な詳細情報が含まれています。</p> <p>例えば、2 つの「重度」のイベントが位置的にも時間的にも近い間隔で発生すると、アラートが「通知」ポートレットに送信されます。</p>
314 ページの『マイ・アクティビティ』	<p>ログオンしているユーザーは、「マイ・アクティビティ」ポートレットで、これらの所有者に割り当てられたアクティビティを表示することができます。「マイ・アクティビティ」ポートレット内のアクティビティは、その親の標準操作手順でグループ化されています。それぞれの標準操作手順は、個々のイベントに対応します。</p>
300 ページの『連絡先』	<p>「連絡先」ポートレットを使用すると、カテゴリ別に分類された連絡先のリストを表示することができます。連絡する必要がある相手に基づいたカテゴリ別に、連絡先を分類できます。例えば、一般的な作業連絡先のカテゴリや、プロジェクト作業連絡先の別のカテゴリを設定できます。「連絡先」ポートレットを使用して、それらの連絡先とやり取りしたり、自身のオンライン状況、連絡先、またはグループを変更したりすることができます。</p>

## スーパーバイザー: レポート

「スーパーバイザー: レポート」ビューで、実行されている事前定義のレポートから生成されるイベント・データのサマリーを確認することができます。また、「スーパーバイザー: レポート」ビューを使用して、パーソナライズ・レポートの作成や事前定義のレポートの構成を行うことができます。これらのレポートは、現在のイベントのモニターと将来のイベントの計画策定を担当するオペレーター、管理者、またはその他のユーザーを対象としています。

「スーパーバイザー: レポート」ビューは、選択したデータに基づくさまざまなレポートがある対話式 Web ページで、スーパーバイザー・レベルで総合情報および対話を提供します。この情報は、システム内のイベント・データのサマリーを示すグラフに表示されます。

「スーパーバイザー: レポート」ビューでは、318 ページの『レポート』ポートレットでレポートを構成および表示できます。デフォルトで、一部の「レポート」ポートレットにサンプルのレポートが表示されません。

## オペレーター: レポート

「オペレーター: レポート」ビューを使用して、レポート、イベント、およびアラートを常時把握することができます。「オペレーター: レポート」ビューは、レポートのモニターを担当するオペレーター、管理者、またはその他のユーザーを対象としています。

「オペレーター: レポート」ビューには、事前定義のレポートの実行によって生成されたイベント・データのサマリーが表示されます。また、「オペレーター: レポート」ビューを使用して、パーソナライズ・レポートを表示することもできます。これらのレポートは、現在のイベントのモニター、イベントを処理するためのアクションの実行、および将来のイベントの計画に役立ちます。

「オペレーター: レポート」ビューは、対話式 Web ページです。オペレーター・レベルで総合情報および対話を提供するさまざまな複数のレポートを表示するように選択できます。

「オペレーター: レポート」ビューでは、318 ページの『レポート』ポートレットでレポートを構成および表示できます。デフォルトで、一部の「レポート」ポートレットにサンプルのレポートが表示されます。

## 「ロケーション・マップ」ビュー

「ロケーション・マップ」ビューを使用して、イベントとそれらの位置をロケーション・マップで常時把握することができます。「ロケーション・マップ」ビューは、最新のイベントのモニターとそれらへの対応を担当するオペレーター、管理者、またはその他のユーザーを対象としています。

「ロケーション・マップ」ビューは、対話式 Web ページです。このページには、表 85 にリストされているポートレットが含まれています。これらのポートレットは、操作レベルで総合情報および対話を提供するために相互に連携するページ内の独立したセクションです。

表 85. 「ロケーション・マップ」ビューのポートレット

ポートレット	説明
305 ページの『ロケーション・マップ』	イベントのマーカーが付けられているロケーションの図。 マップ上に表示されるイベントのカテゴリを選択するためのフィルター・フォーム。 種別ごとに整理されている、使用可能なロケーション・マップのリスト。
301 ページの『詳細』	「詳細」ポートレットは対話式のリスト・ポートレットです。ユーザーに表示権限があるすべてのイベントが、イベント・リストと、「詳細」ポートレットにリンクされた任意のマップ・ポートレットに表示されます。

## ポートレットの使用

ポータル・ページで表示および対話形式で操作できる情報にはポートレットからアクセスすることができます。

IBM Intelligent Operations Center には、いくつかの異なるポートレットが用意されています。

各ポートレットの使用に関するヘルプについては、ポートレットの右上隅をクリックし、表示されるメニューから「ヘルプ」を選択します。

ポートレットのサイズを変更するには、ポートレットの右上隅をクリックし、表示されるメニューから以下の手順でオプションを選択します。

- ポートレットをページ全体まで広げるには、「最大化」をクリックします。



- タイトル・バー以外のポートレットの内容を非表示にするには、「**最小化**」をクリックします。
- 最小化または最大化されたポートレットをデフォルトの表示に戻すには、「**元に戻す**」をクリックします。

## Administrator

### ポートレットのカスタマイズ

管理者としてポートレット設定を変更するには、ポートレットの右上隅をクリックし、ポートレット・メニューでオプションを選択します。

カスタマイズのモードには以下の 2 つが指定でき、各モードはすべてのユーザーのポートレット設定を変更します。

- 「**共有設定の編集**」は、設定の変更時にユーザーが使用しているポートレットのインスタンスに対してのみ、ポートレットを変更します。
- 「**構成**」は、ポートレットのグローバル設定を変更します。この変更は、ポートレットのインスタンスの発生場所にかかわらず、すべてのインスタンスに対して行われます。

ユーザーが使用可能なカスタマイズのモードは、ユーザー ID に関連付けられた権限により異なります。グローバル設定は共有設定によって置き換えられます。

IBM Intelligent Operations Center に付属しているポートレットには、ポートレット・タイプに固有の設定がいくつかあります。例えば、マップ用のデフォルトのズーム・レベルの設定などです。また、ポートレット・タイトルなど、提供されているポートレット間で共通な汎用のポートレット・パラメーターを設定することもできます。

### 連絡先

ソリューション内でインスタント・メッセージを送信するには、「連絡先」ポートレットを使用します。

「連絡先」ポートレットを使用すると、カテゴリー別に分類された連絡先のリストを表示することができます。連絡する必要がある相手に基づいたカテゴリー別に、連絡先を分類できます。例えば、一般的な作業連絡先のカテゴリーや、プロジェクト作業連絡先の別のカテゴリーを設定できます。「連絡先」ポートレットを使用して、それらの連絡先とやり取りしたり、自身のオンライン状況、連絡先、またはグループを変更したりすることができます。

ポートレットの上部の以下のメニューをクリックします。

- 「**ファイル**」を選択して、連絡先を追加したり、グループを変更したり、ログアウトしたりします。
- 「**ツール**」を選択して、チャット、ミーティング、またはアナウンスをセットアップしたり、ユーザー自身のプライバシー設定を変更したりします。
- 「**ヘルプ**」を選択して、ポートレットの使用方法に関する詳細を確認します。

ユーザー自身の状況をクリックすると、その状況およびメッセージを変更することができます。デフォルトの状況は、ユーザーが応答化であることを示します。離席中、会議中、または応答不可であることを示すようにユーザーの状況を変更できます。

ログオンしているユーザーの状況が「連絡先」ポートレットに表示されます。ログオンしているユーザーがブラウザー・ウィンドウを閉じるか WebSphere Portal からログオフした場合、セッションの有効期限が切れるまで、そのユーザーの状況はログオン状態のまま表示されます。しかし、ログオンしているユーザーがブラウザー・ウィンドウを閉じるかログオフした後で、このユーザーにメッセージを送信しても、メッセージは配信されません。したがって、メッセージを送信しようとしているユーザーにはエラー・メッセージ



が表示されます。「連絡先」ポートレットで自分の状況が即時に更新されるようにするには、「ファイル」 > 「ログアウト」をクリックしてログオフします。

注: このポートレットが適切に機能するためには、IBM Intelligent Operations Center アプリケーション・サーバー の完全修飾ドメイン名を使用して、ソリューション・ポータルにログオンする必要があります。登録された完全修飾ドメイン名の代わりに IP アドレスまたはホスト名の別名を使用してポータルにログオンした場合、このポートレットは正しく表示されません。

### Administrator

管理者権限がある場合、このポートレットをカスタマイズできます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

「連絡先」ポートレット用に変更できる設定を以下に示します。

- ヘルプ・ファイル
- ポートレットの高さ
- 最大化した場合のポートレットの高さ
- ポートレットのタイトル
- リソース・バンドル

#### 関連資料:

164 ページの『「連絡先」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「連絡先」ポートレットをカスタマイズできます。

## 詳細

「詳細」ポートレットを使用して、IBM Intelligent Operations Center でイベントの表示、モニター、および管理を行います。

「詳細」ポートレットは対話式のリスト・ポートレットです。ユーザーに表示権限があるすべてのイベントが、イベント・リストと、「詳細」ポートレットにリンクされた任意のマップ・ポートレットに表示されます。

イベントの周辺にあるリソースをリソース・リストとマップに表示できます。

## イベントとリソース

「詳細」ポートレットには、以下の表に示すとおり、2 つの対話式インターフェース・エレメントがあります。

表 86. 「詳細」ポートレットの表示

インターフェース・エレメント	説明
イベントとインシデント	イベントのリストには各イベントの重要な詳細情報が含まれています。 イベントのより詳細な説明を表示するには、リストの行の上にカーソルを移動します。
リソース	イベントの周辺にあるリソースの重要な詳細情報は、選択したイベントを右クリックするとリストされます。 リソースのより詳細な説明を表示するには、リストの行の上にカーソルを移動します。

最初に IBM Intelligent Operations Center を開くと、「詳細」ポートレットにユーザーに関連するイベントがすべて表示されます。

「マップ」ポートレットで、表示するイベントのカテゴリおよびリソースの機能を選択します。イベントのカテゴリは、「イベントとインシデント」タブに表示されるものと「マップ」ポートレットに表示されるものが同じです。リソースの機能は、「リソース」タブに表示されるものと「マップ」ポートレットに表示されるものが同じです。

イベント・リストは、新規イベントと更新により定期的によりリフレッシュされ、表示されるカテゴリを制限するために設定したすべてのフィルターの影響を受けます。

リストの末尾にあるアクション・バーの左隅のカウンターは、表示された項目数と項目数の合計を示します。アクション・バーの中央では、一度に表示する項目数を選択できます。一度に表示できる行数よりも行数が多い場合は、アクション・バーの右隅にあるボタンをクリックすれば、ページを進めたり戻したりすることができます。

## イベント・プロパティ

以下の表に、イベントを記述するプロパティの概要を示します。

表 87. イベント・プロパティ

プロパティ	内容
<b>関係者</b>	
差出人	送信元またはユーザー ID
連絡先の名前	追加情報用の連絡先の担当者
連絡先電子メール	連絡先担当者の電子メール・アドレス
連絡先電話番号	連絡先担当者の電話番号
<b>対象</b>	
イベント・タイプ*	イベントのタイプをカテゴリ内に表示するテキスト
イベント状況*	イベント処理の説明
イベントのスコープ*	メッセージの対象読者
制限	イベント・スコープが「制限付き」の場合に必要な追加情報
ヘッドライン*	イベントの簡略説明
カテゴリ*	イベントの上位種別
重大度*	イベントの影響の強度
確信度*	イベント予測の信頼性
緊急度*	イベントに対する応答のアクションの時間枠
メッセージ・タイプ	メッセージの性質
説明	イベントの追加説明
Web アドレス	イベントについての追加情報の Web アドレス
<b>日時</b>	
送信日時	メッセージがサブミットまたは送信された日時
発効日時	メッセージが有効な日時
開始日時	イベントの開始が予想される日時
有効期限 (日付)	イベントの終了が予想される日時

表 87. イベント・プロパティ (続き)

プロパティ	内容
関係者	
場所	
エリア説明	影響を受けたエリアの説明
緯度/経度	イベントのロケーションの座標

注: 表の中でアスタリスクが付いたプロパティは、イベントの新規作成が成功するために必要です。アスタリスクが付いていないプロパティは、イベント作成時のオプションです。

## イベントとインシデントの管理

「詳細」ポートレットの「イベントとインシデント」タブで、リストのイベントに各種のアクションを実行できます。「マップ」ポートレットで、「詳細」ポートレットのマップおよびイベント・リストの両方に表示されるイベントを追加できます。

### 手順

「イベントとインシデント」タブで、イベント・リストの行を右クリックしてメニューからオプションを選択します。

- イベントの情報を更新するには、「**イベントの更新**」をクリックします。イベントの情報を含んだフィールドがあるウィンドウに変更内容を入力できます。イベント・レコードが更新されると、メッセージ・タイプ・プロパティは更新に変更されます。
- イベント状況をインシデントに変更するには、「**インシデントへのエスカレート**」をクリックしてウィンドウを表示し、連絡先の詳細情報を入力します。イベント・レコードがエスカレートされると、プロパティの変更とマップのアイコンの変更が行われます。
- リストとマップからイベントを削除するには、「**イベントのキャンセル**」をクリックしてウィンドウを表示し、連絡先の詳細情報を入力します。
- イベントに関連付けられた標準操作手順 (SOP) およびワークフロー・アクティビティを表示するには、「**標準操作手順の詳細の表示**」をクリックします。イベントに関連付けられた標準操作手順がない場合、このオプションは利用不可です。関連付けられた標準操作手順がある場合は、「標準操作手順の詳細」ウィンドウが表示されます。「マイ・アクティビティ」ポートレットを使用して、標準操作手順に関連付けられたワークフロー・アクティビティを管理します。
- イベントの周辺にあるリソースのリストを表示するには、「**近隣リソースの表示**」をクリックして、フォーカスするエリアの半径を選択します。リソースのリストが「**リソース**」タブに表示されます。
- イベントの情報を表示するには、「**プロパティ**」をクリックして、イベントの情報を持つフィールドがあるウィンドウを表示します。

## リソースの管理

「リソース」タブのリストにあるリソースに各種のアクションを実行できます。

### 手順

「リソース」タブで、リソース・リストの行を右クリックしてメニューからオプションを選択します。

- リソースの情報を更新するには、「**更新**」をクリックします。
- リストとマップからリソースを削除するには、「**削除**」をクリックします。

- リソースの情報を表示するには、「プロパティ」をクリックします。

どのオプションを選択しても、リソースは Tivoli Service Request Manager の「リソース」タブに表示されます。また、リソースの機能を Tivoli Service Request Manager 「機能」タブに表示することもできます。リソースを更新または削除するには、リソースを選択して、「アクションの選択」リストから適切なオプションを選択します。

## 「詳細」ポートレットのカスタマイズ

### Administrator

管理者権限がある場合、このポートレットをカスタマイズできます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

「詳細」ポートレットのパラメーターを以下のように設定します。

「詳細」ポートレットのパラメーターを設定することにより、以下の操作を行えます。

- 列のレイアウト、見出し、ソート順、および優先度を指定します。
- 表示されるイベントまたはリソースをフィルタリングするために、追加条件を指定します。
- 以下を表示または非表示にします。
  - 「イベントの追加」ボタン
  - 「リソースの追加」ボタン
  - 「イベント」タブ
  - 「リソース」タブ
  - リストの上部のツールバー
- グループ名を指定して、その他のマップおよび「詳細」ポートレットとの通信を使用可能にします。
- グループ内にある他のポートレットから生じる特定のタイプのメッセージを確認または無視するようにポートレットを設定します。

また、ヘルプ・ファイルの位置、ポートレットの高さ、ポートレット・タイトル、リソース・バンドルなど、ポートレット間で共通な汎用のポートレット・パラメーターを設定することができます。

### 関連資料:

164 ページの『「詳細」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「詳細」ポートレットをカスタマイズできます。

## 重要業績評価指標のドリルダウン

KPI カテゴリと、そのカテゴリの基礎となる KPI の状況に関する追加の情報を表示するには、「重要業績評価指標のドリルダウン」ポートレットを使用します。

「重要業績評価指標のドリルダウン」ポートレットには、「状況」ポートレットに表示される組織または KPI カテゴリに関連付けられているすべての基礎となる KPI が表示されます。KPI は、ネストされたリストの形で表示され、展開したり折りたたんだりできます。基礎となる各 KPI の状況は、「状況」ポー

ポートレットに表示される KPI カテゴリが色分けされるのと同じ方法で、色分けして表示されます。基礎となる KPI の値によって、親 KPI の色が制御されます。KPI の状況を表示するには、その KPI の上にカーソルを移動させます。

「重要業績評価指標のドリルダウン」ポートレットで特定の KPI カテゴリに絞り込んで表示するには、「状況」ポートレットでそのカテゴリをクリックします。こうすることで、そのカテゴリのみが「重要業績評価指標のドリルダウン」ポートレットに表示されるようになります。そのリストを使用して、状況が変わる原因となった KPI の詳細に到達するまで、基礎となる KPI を調べることができます。

## Administrator

### 「重要業績評価指標のドリルダウン」ポートレットのカスタマイズ

管理者権限がある場合、このポートレットをカスタマイズできます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

「重要業績評価指標のドリルダウン」ポートレットのパラメーターを設定することにより、以下の操作を行います。

- 列のレイアウト、見出し、ソート順、および優先度を指定します。
- KPI の色をカスタマイズする。
- 追加の KPI フィルターを使用可能にする。
- リストの上部のツールバーを表示または非表示にします。
- 「重要業績評価指標のドリルダウン」ポートレットとの通信を可能にするグループ名を指定する。

また、ヘルプ・ファイルの位置、ポートレットの高さ、ポートレット・タイトル、リソース・バンドルなど、ポートレット間で共通な汎用のポートレット・パラメーターを設定することができます。

#### 関連概念:

186 ページの『重要業績評価指標』

「重要業績評価指標」ポートレットでは、IBM Intelligent Operations Center の重要業績評価指標 (KPI) およびそれらの階層表示をカスタマイズすることができます。

#### 関連資料:

169 ページの『「重要業績評価指標のドリルダウン」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「重要業績評価指標のドリルダウン」ポートレットをカスタマイズできます。

## ロケーション・マップ

「ロケーション・マップ」ポートレットでは、ロケーション・マップでマークされているイベントを確認することができます。IBM Intelligent Operations Center のロケーション・マップは、対話用に事前に定義されているエリア (大規模なスポーツ・スタジアムの座席エリアなど) を含むマップまたは計画です。

「ロケーション・マップ」ポートレットでは、イベントについてその発生位置を視覚的に確認することができます。「ロケーション・マップ」ポートレットを「マップ」ポートレットおよび「詳細」ポートレットと併せて使用することで、問題、位置パターン、競合、および相乗効果を特定することができます。

「ロケーション・マップ」ポートレット、「マップ」ポートレット、および「詳細」ポートレットを相互にリンクさせることで、表示されるイベントに関する入力情報および変更が共有されるようにすることができます。

ます。「ロケーション・マップ」ポートレットでは、表示するイベントのカテゴリを選択することができます。選択内容は、「ロケーション・マップ」ポートレットおよびそれにリンクしている「マップ」ポートレットと「詳細」ポートレットに表示されるイベントに影響します。

## ロケーション・マップのインターフェース

「ロケーション・マップ」ポートレットには、以下の表に示す 3 つの対話式インターフェース・エレメントがあります。

表 88. 「ロケーション・マップ」ポートレットのインターフェース・エレメント

インターフェース・エレメント	説明
ロケーション・マップ	イベントのマーカーが付けられているロケーションの図。
内容の選択: イベント・カテゴリ	マップ上に表示されるイベントのカテゴリを選択するためのフィルター・フォーム。
マップ・メニュー	種別ごとに整理されている、使用可能なロケーション・マップのリスト。

このポータル・ページでは、最初に「ロケーション・マップ」ポートレットが開き、ユーザーに関連するすべてのイベントがロケーション・マップに表示されます。表示されるカテゴリを制限するために設定されたフィルターに応じて、マップが更新されて新しいイベントが表示されます。使用可能なすべてのマップのリストを含むメニュー・バーが、マップの左側に表示されます。

エリア内で発生したイベントは、ロケーション・マップ上で対応する位置にマーカーで表されます。マップのイベント・マーカーの上にカーソルを移動させると、イベントの見出しと説明を確認できます。イベントが発生したエリアの名前と説明がウィンドウに表示されます。同じエリア内で複数のイベントが発生している場合、それらのイベントはまとめられてクラスター・マーカーで表されます。このマーカーの上にカーソルを移動させると、各イベントの見出しがウィンドウに表示されます。また、マップ内で事前に定義されておりイベントが発生していないエリアの上にカーソルを移動させて、そのエリアの名前と説明を表示することもできます。

ポートレットがリンクされている場合は、そのポートレットでイベントをクリックすると、グループ内の他のポートレットでも、それに対応するイベントが選択されます。同様に、リンクしているポートレットのいずれかでイベントが選択されると、このポートレットで当該イベントが強調表示されます。

注: イベントには、「ロケーション・マップ」ポートレットに表示されるエリア ID があります。また、イベントには、「ロケーション・マップ」ポートレットと「マップ」ポートレットの両方に表示される経度と緯度の座標があります。イベントにエリア ID または座標がない場合、そのイベントは「詳細」ポートレットにのみ表示されます。

## マップ・マーカー

マップでは、以下のいずれかのタイプのマーカーによって、イベントの位置が表されます。

表 89. マップ・マーカー

マーカーのタイプ	説明
アイコン	マップ上で、イベントの位置をそれぞれのイベント・カテゴリに固有のアイコンで指し示します。
クラスター	同じエリア内に複数のイベントが発生していることを、そのエリアでのイベントの数をを使用して示します。



イベント・タイプを表すアイコンは、「詳細」ポートレットの「イベントとインシデント」タブにあるイベント詳細のカテゴリ・フィールドで定義します。イベントがインシデントにエスカレートされる場合、マップに表示されるアイコンのカテゴリ固有のシンボルは維持されますが、アイコンの周囲に赤色の輪郭線が追加されます。

## マップ・コントロール

マウスまたはキーボードを使用して、マップ内でカーソルを移動できます。

### マップ・コントロールの場所はマップの左上

マップ・コントロールはマップの左上にあります。以下のもので構成されます。

- パン矢印 (上、下、左、右)
- ズームイン
- 世界表示 (最大の範囲までズームアウト)
- ズームアウト

### マップ内を移動するためのパン・コントロール

マップ内を移動する方法は以下のとおりです。

- マウスを使用してマップをクリックし、ドラッグする
- 上方向パン矢印か、キーボードの上矢印キーを押して北へ移動する
- 下方向パン矢印か、キーボードの下矢印キーを押して南へ移動する
- 右方向パン矢印か、キーボードの右矢印キーを押して東へ移動する
- 左方向パン矢印か、キーボードの左矢印キーを押して西へ移動する

### マップの縮尺を拡大または縮小するためのズーム・コントロール

マップのズームインまたはズームアウトを行う方法は以下のとおりです。

- マップの中心にズームインするには「+」マップ・アイコンをクリックし、マップの中心からズームアウトするには「-」マップ・アイコンをクリックする
- 選択した位置にマップの中心を合わせてズームインするには、マウスをダブルクリックする
- ズームアウトを最大にして世界表示にするには、「世界表示」アイコンをクリックする
- ズームインするには、キーボードの + キーを押す
- ズームアウトするには、キーボードの - キーを押す
- ズームインの対象領域を囲む長方形を描くには、Shift キーを押しながらマウスを使用する

## マップのイベント・カテゴリの選択

「イベント・カテゴリ」フィルターを使用して、マップ上で表示するイベントをカテゴリで選択します。

フィルター・フォームを表示するには、**内容の選択**をクリックします。マップおよび関連付けられているポートレットに表示されるイベントのカテゴリは、ここフィルター・フォームで選択する項目によって変更できます。フィルターを使用して不要なイベント・カテゴリを非表示にすることにより、分析するイベントのカテゴリに集中することができます。フィルター・フォームが変更されると、それに応じてマップに表示される内容が変わります。選択内容が変更されると、マップが更新され、選択されたカテゴリに該当するイベントの位置のみがマップ上にプロットされます。フィルター・フォームでチェック・ボツ

クスを選択または選択解除することにより、表示されるイベントのカテゴリーを変更します。フィルター・フォームを閉じるには、「**内容の選択**」をクリックします。ポータル・ページを離れて元の画面に戻ると、フィルターはデフォルトの選択内容に応じてリセットされます。

「詳細」ポートレットでチェック・ボックスを選択することにより、分析する個々のイベントに集中することができます。こうしたイベントは、リンクされているポートレットでも強調表示されます。

## 「ロケーション・マップ」ポートレットのカスタマイズ

### Administrator

管理者権限がある場合、このポートレットをカスタマイズできます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

「マップ」ポートレットおよび「ロケーション・マップ」ポートレットも、グローバル設定を変更してカスタマイズすることができます。グローバル設定は、すべてのユーザーの当該ポートレットの内容、および当該ポートレットのすべてのオカレンスに影響します。ただし、グローバル設定よりも共有設定が優先されます。

「ロケーション・マップ」ポートレットに関して変更できる設定は、以下のとおりです。

- 「イベント・カテゴリー」フィルターのデフォルトの選択項目
- 表示されるデフォルトのロケーション・マップの名前
- カーソルを使用してエリア上を移動するときのデフォルトのエリア強調色
- 他のマップおよび「詳細」ポートレットとの通信を可能にするグループの名前

また、ヘルプ・ファイルの位置、ポートレットの高さ、ポートレット・タイトル、リソース・バンドルなど、ポートレット間で共通な汎用のポートレット・パラメーターを設定することができます。

### ロケーション・マップのカスタマイズ

「ロケーション・マップ・マネージャー」ポートレットを使用して、「ロケーション・マップ」ポートレットの以下の要素をカスタマイズできます。

- ポートレットの左側のメニューに表示される種別名。
- ポートレットに表示されるマップ。
- マップ内のエリア。

## 関連概念:

195 ページの『ロケーション・マップ・マネージャー』

「ロケーション・マップ・マネージャー」ポートレットでは、「ロケーション・マップ」ポートレットをカスタマイズすることができます。

## 関連資料:

172 ページの『「ロケーション・マップ」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「ロケーション・マップ」ポートレットをカスタマイズできます。

## マップ

「マップ」ポートレットを使用して、イベントおよびリソースをマップ上で確認します。

「マップ」ポートレットでは、イベントおよびリソースをマップ上で視覚的に確認することができます。

「マップ」ポートレットを「ロケーション・マップ」ポートレットおよび「詳細」ポートレットと組み合わせて使用することで、位置パターン、競合、問題、および相乗効果を特定します。

「マップ」ポートレット、「ロケーション・マップ」ポートレット、および「詳細」ポートレットを相互にリンクさせることで、表示されるイベントに関する入力情報および変更が共有されるようにすることができます。「マップ」ポートレットでは、表示するイベントのカテゴリおよびリソースの機能を選択することができます。選択内容は、「マップ」ポートレットおよびそれとリンクしている「ロケーション・マップ」ポートレット「詳細」ポートレットに表示される内容に影響します。

## マップ・インターフェース

「マップ」ポートレットには、以下の表に示す 3 つの対話式インターフェース・エレメントがあります。

表 90. 「マップ」ポートレットのインターフェース・エレメント

インターフェース・エレメント	説明
マップ	イベント・マーカ―およびリソース・マーカ―が表示される地理的領域のマップ。
内容の選択: イベント・カテゴリ	マップ上および「マップ」ポートレットにリンクしているポートレット内に表示されるイベントのカテゴリを選択するためのフィルター・フォーム。
内容の選択: リソース	マップ上およびリンクしている「詳細」ポートレットの「リソース」タブ内に表示されるリソースの機能を選択するためのフィルター・フォーム。このフォームを表示するには、まず、「詳細」ポートレットで「 <b>近隣リソースの表示</b> 」を選択します。

このポータル・ページでは、最初に、「マップ」ポートレットが開き、ユーザーに関連するすべてのイベントがマップに表示されます。イベントに緯度と経度の値が指定されている場合には、イベントの位置がマップ上にアイコン・マーカ―で示されます。マップのイベント・マーカ―の上にカーソルを移動させると、イベントの見出しと説明を確認できます。同じ位置に複数のイベントが集まっている場合、イベントの数がマーカ―の上に示されます。そのクラスター・マーカ―の上にカーソルを移動すると、各イベントの見出しがウィンドウに表示されます。表示されるカテゴリを制限するために設定されたフィルターに応じて、マップが更新されて新しいイベントが表示されます。

ポートレットがリンクされている場合は、ポートレットでイベント・マーカ―をクリックすると、グループ内の他のポートレットでも該当のイベントが選択されます。

マップに表示できるマーカーの数は制限されます。ビューのエリア内のマーカーの数がしきい値を超えた場合、マーカーは表示されません。ユーザーは使用可能なマーカーの数およびしきい値数を示すメッセージを受け取ります。使用可能なすべてのマーカーを表示するには以下の 2 つの選択肢があります。

- マーカーの数がしきい値未満のエリアにズームインまたはパンする。
- 「ビュー内のすべての項目をロード」をクリックする。

2 番目を選択した場合は、マーカーがマップに表示されるスピードが少し遅くなります。3 番目の選択肢は、フィルターを使用して、選択されているカテゴリの数を減らすことです。

「詳細」ポートレットでイベントについて「近隣リソースの表示」を選択すると、事前に選択した半径および機能に基づいてリソースがマップに表示されます。

表示されるカテゴリを制限するために設定されたフィルターに応じて、マップに新しいイベントが追加されて、マップが常に最新の状態に維持されます。

注: イベントに緯度と経度の座標だけでなくエリア ID も設定されている場合、そのイベントは「ロケーション・マップ」ポートレットと「マップ」ポートレットの両方に表示されます。すべてのイベントは「詳細」ポートレットで確認することができます。

## マップ・マーカー

マップでは、以下のいずれかのタイプのマーカーによって、イベントまたはリソースの位置が表されます。

表 91. マップ・マーカー

マーカーのタイプ	説明
アイコン	マップ上のイベントまたはリソースの位置をそれぞれのイベント・カテゴリまたはリソース・タイプに固有のアイコンで指し示します。
ポリゴン	特定のイベントに関連付けられているエリアの形状をマップ上に示します。
クラスター	同じ位置で複数のイベントが発生していることを、イベントの数を使用して示します。
半径	イベントに関して、「近隣リソースの表示」で選択されたエリアの形状をマップ上に示します。

イベント・タイプを表すアイコンは、「詳細」ポートレットの「イベントとインシデント」タブにあるイベント詳細のカテゴリ・フィールドで定義します。イベントがインシデントにエスカレートされる場合、マップに表示されるアイコンのカテゴリ固有のシンボルは維持されますが、赤色の輪郭線が追加されます。マップでイベント・マーカーをクリックすると、関連付けられているイベントが「詳細」ポートレットで強調表示されます。

リソースを表すアイコンは、「詳細」ポートレットの「リソース」タブにあるリソース詳細のタイプ・フィールドで定義します。リソース・アイコンを表示するには、まず、「詳細」ポートレットで「近隣リソースの表示」を選択します。

## マップ・コントロールの使用

マウスまたはキーボードを使用して、マップ内でカーソルを移動できます。

### マップ・コントロールの場所はマップの左上

マップ・コントロールはマップの左上にあります。以下のもので構成されます。

- パン矢印 (上、下、左、右)

- ズームイン
- 世界表示 (最大の範囲までズームアウト)
- ズームアウト

## マップ内を移動するためのパン・コントロール

マップ内を移動する方法は以下のとおりです。

- マウスを使用してマップをクリックし、ドラッグする
- 上方向パン矢印か、キーボードの上矢印キーを押して北へ移動する
- 下方向パン矢印か、キーボードの下矢印キーを押して南へ移動する
- 右方向パン矢印か、キーボードの右矢印キーを押して東へ移動する
- 左方向パン矢印か、キーボードの左矢印キーを押して西へ移動する

## マップの縮尺を拡大または縮小するためのズーム・コントロール

マップのズームインまたはズームアウトを行う方法は以下のとおりです。

- マップの中心にズームインするには「+」マップ・アイコンをクリックし、マップの中心からズームアウトするには「-」マップ・アイコンをクリックする
- 選択した位置にマップの中心を合わせてズームインするには、マウスをダブルクリックする
- ズームアウトを最大にして世界表示にするには、「世界表示」アイコンをクリックする
- ズームインするには、キーボードの + キーを押す
- ズームアウトするには、キーボードの - キーを押す
- ズームインの対象領域を囲む長方形を描くには、Shift キーを押しながらマウスを使用する

## マップのイベント・カテゴリーの選択

「イベント・カテゴリー」フィルターを使用して、マップ上で表示するイベントをカテゴリーで選択します。

フィルター・フォームを表示するには、**内容の選択**をクリックします。「マップ」ポートレットに表示されるイベントのカテゴリーは、フィルター・フォームで選択する項目によって変更できます。フィルターを使用して不要なイベント・カテゴリーを非表示にすることにより、分析するイベントのカテゴリーに集中することができます。フィルター・フォームが変更されると、それに応じてマップに表示される内容が変わります。フィルター・フォームへの変更は、同じグループ内の他のポートレットにも影響します。選択内容が変更されると、マップが更新され、選択されたカテゴリーに該当するイベントの位置のみがマップ上にプロットされます。フィルター・フォームでチェック・ボックスを選択または選択解除することにより、表示されるイベントのカテゴリーを変更します。フィルター・フォームを閉じるには、「**内容の選択**」をクリックします。ポータル・ページを離れて元の画面に戻ると、フィルターはデフォルト (すべてのカテゴリーが選択されている状態) にリセットされます。

「詳細」ポートレットでチェック・ボックスを選択することにより、分析する個々のイベントに集中することができます。それらのイベントはマップ上で強調表示されます。

## マップのリソースの機能の選択

「詳細」ポートレットで「**近隣リソースの表示**」を選択すると、「イベント・カテゴリー」フィルターが「リソース」フィルターに変わります。「リソース」フィルターを使用して、マップ上で表示するリソースを機能に基づいて選択します。



フィルター・フォームを表示するには、**内容の選択**をクリックします。マップおよび「詳細」ポートレットに表示されるリソースの機能は、フィルター・フォームで選択する項目によって変更できます。フィルターを使用して不要な機能を非表示にすることにより、分析する機能に集中することができます。フィルター・フォームが変更されると、それに応じてマップに表示される内容が変わります。フィルター・フォームへの変更は、同じグループ内の「詳細」ポートレットにも影響します。選択内容が変更されると、マップが更新され、選択された機能に該当するリソースの位置のみがマップ上にプロットされます。フィルター・フォームでチェック・ボックスを選択または選択解除することにより、表示されるリソースの機能を変更します。フィルター・フォームを閉じるには、「**内容の選択**」をクリックします。ポータル・ページを離れて元の画面に戻ると、フィルターはデフォルト（すべての機能が選択されている状態）にリセットされます。デフォルトで選択される機能は、イベントのカテゴリーおよびそのカテゴリーがどのように機能にマップされているかによって異なります。

## マップのリセット

「マップ」ポートレットは、IBM Intelligent Operations Center で設定されているデフォルトのビューにリセットすることができます。

### 手順

1. 「マップ」ポートレットで、「**マップのリセット**」をクリックするか、右上隅の矢印をクリックします。
2. 以下のオプションのいずれかを選択します。
  - 「**マップのリセット**」は、マップにズームインし、デフォルト設定の位置を中心にして表示します。
  - 「**マップをリセットしてフィルターを解除**」は、マップにズームインし、デフォルト設定の位置を中心にして表示し、「**内容の選択**」で設定されている値をデフォルト値に戻します。

### タスクの結果

選択されたオプションに応じてマップがリセットされます。ただし、この変更が適用されるのは、現行のユーザーおよびビューのみです。

## イベントの追加

イベントを作成して、「マップ」ポートレットのマップと「詳細」ポートレットのリストに同時に追加することができます。マップとリストを使用することで、同じ情報を 2 つの方法で確認できます。

### このタスクについて

「**イベントの追加**」ダイアログを使用して、以下の表に示すイベント・プロパティを指定します。

表 92. イベント・プロパティ

プロパティ	内容
<b>関係者</b>	
差出人	送信元またはユーザー ID
連絡先の名前	追加情報用の連絡先の担当者
連絡先電子メール	連絡先担当者の電子メール・アドレス
連絡先電話番号	連絡先担当者の電話番号
<b>対象</b>	
イベント・タイプ*	イベントのタイプをカテゴリー内に表示するテキスト
イベント状況*	イベント処理の説明



表 92. イベント・プロパティ (続き)

プロパティ	内容
関係者	
イベントのスコープ*	メッセージの対象読者
制限	イベント・スコープが「制限付き」の場合に必要な追加情報
ヘッドライン*	イベントの簡略説明
カテゴリー*	イベントの上位種別
重大度*	イベントの影響の強度
確信度*	イベント予測の信頼性
緊急度*	イベントに対する応答のアクションの時間枠
メッセージ・タイプ	メッセージの性質
説明	イベントの追加説明
Web アドレス	イベントについての追加情報の Web アドレス
日時	
送信日時	メッセージがサブミットまたは送信された日時
発効日時	メッセージが有効な日時
開始日時	イベントの開始が予想される日時
有効期限 (日付)	イベントの終了が予想される日時
場所	
エリア説明	影響を受けたエリアの説明
緯度/経度	イベントのロケーションの座標

## 手順

1. マップ上の位置を右クリックしてから「イベントの追加」をクリックして、「イベントの追加」ダイアログを起動します。 イベント・プロパティの一部は自動的に指定されます。
2. ダイアログのフィールドで、残りのイベント・プロパティを指定します。 アスタリスクが付いたプロパティは、イベントの新規作成が成功するために必要です。 アスタリスクが付いていないプロパティは、オプションです。
3. 「OK」をクリックしてイベントを保存するか、または「キャンセル」をクリックしてイベントの追加を終了します。

## タスクの結果

新規イベントのカテゴリーを表すアイコンがマップ上の指定の位置に表示されます。 リンクされている「詳細」ポートレットのリストで、新規イベントの詳細を確認できます。

## 「マップ」ポートレットのカスタマイズ

### Administrator

管理者権限がある場合、このポートレットをカスタマイズできます。 ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

「マップ」ポートレットおよび「ロケーション・マップ」ポートレットも、グローバル設定を変更してカスタマイズすることができます。グローバル設定は、すべてのユーザーの当該ポートレットの内容、および当該ポートレットのすべてのオカレンスに影響します。ただし、グローバル設定よりも共有設定が優先されます。

「マップ」ポートレットに固有の、以下の設定を変更することができます。

- マップのデフォルトの中心点およびズーム・レベルをリセットする。
- 基本マップを選択する (デフォルトは Esri によって提供される ArcGIS マップ)。
- 追加データを表すため、キーホール・マークアップ言語 (KML) を使用して、マップの地理的注釈および視覚化層を追加する。
- 警告メッセージが発行されることなく表示できるマーカー数のしきい値を設定する。
- 「**内容の選択**」をクリックしたときに表示されるマップ・フィルターのデフォルトの選択項目を設定する。
- 他のマップおよび「詳細」ポートレットとの通信を可能にするグループの名前を指定する。

また、ヘルプ・ファイルの位置、ポートレットの高さ、ポートレット・タイトル、リソース・バンドルなど、ポートレット間で共通な汎用のポートレット・パラメーターを設定することができます。

#### 関連資料:

174 ページの『「マップ」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「マップ」ポートレットをカスタマイズできます。

## マイ・アクティビティ

「マイ・アクティビティ」ポートレットには、インターフェースにログオンしているユーザーがメンバーとして所属するグループが所有するアクティビティの動的なリストが表示されます。

イベントで標準操作手順がトリガーされるたびに、標準操作手順の選択マトリックスで定義されている選択基準に従って、関連付けられているアクティビティが所有者に割り当てられます。標準操作手順について詳しくは、トピックの末尾のリンクを参照してください。

ログオンしているユーザーは、「マイ・アクティビティ」ポートレットで、これらの所有者に割り当てられたアクティビティを表示することができます。「マイ・アクティビティ」ポートレット内のアクティビティは、その親の標準操作手順でグループ化されています。それぞれの標準操作手順は、個々のイベントに対応します。

標準操作手順ごとに、「マイ・アクティビティ」ポートレットにはオープン・アクティビティのみが表示され、クローズ・アクティビティまたは完了済みアクティビティは表示されません。オープン・アクティビティには、既に開始されているアクティビティ、および開始される予定のアクティビティが含まれます。例えば、標準操作手順に指定されている 1 つ以上のアクティビティを順番に並べた場合、その順番内の現在のアクティビティだけが表示されます。特定のアクティビティが先行アクティビティに依存している (先行アクティビティの完了後に開始される) 場合、先行アクティビティが完了するかスキップされるまで、そのアクティビティは表示されません。

次にアクティビティが予定されていることを示すアイコンは、「マイ・アクティビティ」ポートレットの上部付近に表示されます。

#### 期限過ぎ

完了期限を過ぎているアクティビティ。

今日 今日完了する予定のアクティビティー。

期限前 将来完了する予定のアクティビティー。

アクティビティーが開始されると、開始時刻にアクティビティーの所要時間を加算することで、期限が計算されます。アクティビティーの期限日を使用して、アクティビティーの各期限アイコンに表示される数字が計算されます。

「マイ・アクティビティー」ポートレットでは、期限が過ぎたアクティビティーがある標準操作手順がまず表示され、次に残りの標準操作手順がアルファベット順に表示されます。

リスト内の期限過ぎアクティビティーがある各標準操作手順の横で、赤色のアイコンが期限が過ぎているアクティビティーの数を示します。期限過ぎアクティビティーがある標準操作手順は、それぞれが含む期限過ぎアクティビティーの数に従ってソートされます。期限過ぎとなっているアクティビティーの数が最も多い標準操作手順が、リストの先頭に表示されます。

## 「マイ・アクティビティー」ポートレットでのアクティビティーの管理

「マイ・アクティビティー」ポートレットでアクティビティーを管理します。

- 標準操作手順の詳細を表示するには、目的の標準操作手順の名前を展開します。
  - その標準操作手順をトリガーしたイベントの名前が表示されます。イベント名にマウス・カーソルを移動すると、ホバー・ヘルプ情報が表示されます。この情報には、イベントの開始日時、カテゴリ、重大度、確信度、および緊急度が示されます。
  - 「詳細」ポートレットがページ上に表示されている場合に、イベント・プロパティを表示するには、イベント名をクリックします。イベントの「プロパティ」ウィンドウが表示されます。
  - 進行中のステップまたは開始予定のステップが表示されます。また、各ステップの状況および期限も表示されます。
- ステップのさらに詳しい情報（ユーザーがそのステップに追加したコメントや参照など）を表示するには、そのステップの名前を展開します。
- ステップを開始、完了、またはスキップするには、ステップの名前を展開して、以下のいずれかのオプションを選択します。
  - ステップを開始するには、リストから「開始」を選択します。ステップが標準操作手順で自動タスクとして定義されている場合、そのタスクに割り当てられているワークフローが自動的に開始され、ステップが自動的に終了します。ステップを開始するユーザーがそのステップの所有者となり、そのユーザーの名前が「所有者」フィールドに表示されます。
  - ステップをスキップするには、リストから「スキップ」を選択します。
  - ステップを終了するには、リストから「終了」を選択します。
- ステップにコメントを追加するには、以下のサブステップを実行します。
  1. ステップの名前を展開します。
  2. リストから「コメントの追加」を選択します。
  3. 「コメントの追加」ウィンドウの「コメント」フィールドにコメントを入力します。「コメント入力者名」と「アクティビティー名」は読み取り専用フィールドです。これらのフィールドには、入力された値が自動的に設定されます。
  4. 「OK」をクリックします。
  5. ステップの名前を再度展開します。新しいコメントが、ステップに対する既存のコメントおよび参照のリストの末尾に表示されます。
- ステップに参照を追加するには、以下のサブステップを実行します。

1. ステップの名前を展開します。
  2. リストから「参照の追加」を選択します。
  3. 「参照の追加」ウィンドウで、「参照名」と「参照 URI」の値を入力します。「アクティビティ名」は読み取り専用フィールドです。このフィールドには、自動的に入力された値が設定されます。
  4. 「OK」をクリックします。
  5. ステップの名前を再度展開します。新しい参照が、ステップに対する既存のコメントおよび参照のリストの末尾にリンクとして表示されます。
- 標準操作手順の詳細を表示するには、標準操作手順の名前の横にある **i** アイコンをクリックします。「標準操作手順の詳細」ウィンドウには、標準操作手順に含まれるすべてのアクティビティ・ステップ (進行中、開始予定、完了済み、クローズ状態などのステップ) が表示されます。各ステップの状況および期限も表示されます。ステップに関する詳細をさらに確認するには、ステップ名を展開します。

## Administrator

### 「マイ・アクティビティ」ポートレットのカスタマイズ

管理者権限がある場合、このポートレットをカスタマイズできます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

「マイ・アクティビティ」ポートレットでは、グループ名を指定して、他のポートレット (「詳細」ポートレットなど) との通信を有効にすることができます。

また、ヘルプ・ファイルの位置、ポートレットの高さ、ポートレット・タイトル、リソース・バンドルなど、ポートレット間で共通な汎用のポートレット・パラメーターを設定することができます。

#### 関連概念:

143 ページの『標準操作手順』

標準操作手順およびアクティビティを定義することで、IBM Intelligent Operations Center で受信するイベントを管理できます。「標準操作手順」ポートレットを使用して、Tivoli Service Request Manager で、標準操作手順、標準操作手順の選択マトリックス、およびワークフロー・デザイナーの各アプリケーションにアクセスします。

#### 関連資料:

176 ページの『「マイ・アクティビティ」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「マイ・アクティビティ」ポートレットをカスタマイズできます。

## 通知

「通知」ポートレットを使用して、アラート・メッセージとその詳細を表示します。

「通知」ポートレットは、ユーザーに関連したすべての現在のアラートのリストを含む対話式ウィンドウです。自分がメンバーであるユーザー・グループに送信されたアラートのみが表示されます。アラートは、以下の状況で受信される通知です。

- 複数のイベントが同一周辺で同様の時間に発生している。そのため、競合状態にあるか調整が必要である場合がある。
- 定義済みの重要業績評価指標 (KPI) 値の変更がアラート・トリガーとして管理者により定義されている場合に、変更が行われた。

また、ポートレットを使用して、アラートの詳細を表示することもできます。

## 通知のリスト

「通知」ポートレットは、KPI および関連イベントの変更により発生したアラートの動的な対話式リストを提供します。このポートレットの役割は、KPI またはイベント状況の変更に注意を促すことです。このリストには各アラートの重要な詳細情報が含まれています。

アラートのより詳細な説明を表示するには、行の上にカーソルを移動します。そのアラートに関連するすべての情報をウィンドウに表示するには、対象の行を右クリックして「プロパティ」を選択します。

最初にポータル・ページを開くと、ポートレットに現在のアラートがすべて表示されます。行を右クリックして「アラートを閉じる」を選択することにより、ポートレットから任意のアラートを削除します。この方法で、複数の行を選択して複数のアラートを閉じることが可能です。アラートを適切に処理した後のみ、アラートを閉じます。理由は、アラートを閉じると、すべての受信者のアラートが削除されるためです。

ウィンドウの右上隅にあるボタンをクリックし、アラートを取り消してリストに戻ります。

リストの末尾にあるアクション・バーの左隅のカウンターは、表示された項目数と項目数の合計を示します。アクション・バーの中央では、一度に表示する項目数を選択できます。一度に表示できる行数よりも行数が多い場合は、アクション・バーの右隅にあるボタンをクリックすれば、ページを進めたり戻したりすることができます。

## アラート・プロパティ

アラート詳細のウィンドウは以下のプロパティを表示します。

表 93. アラート・プロパティ

プロパティ	内容
見出し	アラートの簡略説明
カテゴリ	イベントまたは KPI の上位種別
差出人	アラートの送信元
グループに送信済み	アラートが送信されたグループ
送信済み	アラートが送信された日時
説明	アラートの追加説明
アラートへの参照	関連イベントによってアラートが発生した場合のイベント ID
KPI への参照	KPI の値を変更したことによってアラートが発生した場合の KPI の名前

### Administrator

## 「通知」ポートレットのカスタマイズ

管理者権限がある場合、このポートレットをカスタマイズできます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

「通知」ポートレットのパラメーターを設定することにより、以下の操作を行えます。

- 列のレイアウト、見出し、ソート順、および優先度を指定します。



- リストの上部のツールバーを表示または非表示にします。

また、ヘルプ・ファイルの位置、ポートレットの高さ、ポートレット・タイトル、リソース・バンドルなど、ポートレット間で共通な汎用のポートレット・パラメーターを設定することができます。

#### 関連資料:

177 ページの『「通知」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「通知」ポートレットをカスタマイズできます。

## レポート

「レポート」ポートレットでは、イベントのレポートをグラフとして表示することができます。このポートレットは、イベントのグループ化の基準となる各種のオプションを提供します。さらに、特定の日付または日付範囲を指定してイベントを選択することができます。レポートは、現在および将来のイベントへの対応について計画を策定するのに役立ちます。

### レポートの作成

「レポート」ポートレットを使用して、イベントのカスタム・レポートを作成することができます。まず、イベントをグループ化する方法を選択します。例えば、特定のカテゴリのすべてのイベントを表示するには、「グループ化」フィールドで「カテゴリ」を選択します。次に、「データの選択」フィールドで、表示する情報に固有のデータを選択します。また、レポートのイベントについて日付または日付範囲を指定することもできます。「更新」をクリックすると、グラフが変更され、要求した情報が反映されません。

新規レポートの URL を取得するには、「このレポートの URL」をクリックします。

イベントのグループ化の基準となるオプションを、表 1 に示します。

表 94. カスタム・レポート

グループ化	説明
イベント・タイプ	タイプに基づいてイベントを表示します。例えば、接近中の竜巻や交通事故などのイベントです。
重大度	重大度に基づいてイベントを表示します。例えば、「極度」や「重度」などのイベントです。
確信度	発生する可能性に基づいてイベントを表示します。例えば、交通事故が発生した場合、確信度は「監視対象」となります。
緊急度	緊急度に基づいてイベントを表示します。例えば、イベントが発生して、「即時」として表記される場合があります。
イベント・カテゴリ	イベント・カテゴリに基づいてイベントを表示します。例えば、「環境」、「火災」、「輸送」などのすべてのイベントを表示できます。
メッセージ・タイプ	「更新」や「アラート」などのメッセージ・タイプに基づいてイベントを表示します。



表 94. カスタム・レポート (続き)

グループ化	説明
状況	状況別にイベントを表示します。 以下のような状況があります。 <ul style="list-style-type: none"> <li>• 許容可能</li> <li>• 注意</li> <li>• 対処</li> </ul>
差出人	特定の差出人別にイベントを表示します。 例えば、セキュリティ問題や、IBM Intelligent Operations for Water に影響を及ぼす問題などのイベントです。
インシデント	インシデントのタイプに基づいてイベントを表示します。 例えば、すべての交通事故やすべての道路建設を表示することができます。
処理コード	処理コード別にイベントを表示します。 例えば、「イベント」などの処理コードがあります。
差出人名	差出人名別にイベントを表示します。

レポートについて選択できるデータを、表 2 に示します。

表 95. データの選択

データの選択	説明
重大度	重大度に基づいてイベントを表示します。 例えば、「極度」や「重度」などのイベントです。
確信度	発生する可能性に基づいてイベントを表示します。 例えば、交通事故が発生した場合、確信度は「監視対象」となります。
緊急度	緊急度に基づいてイベントを表示します。 例えば、イベントが発生して、「即時」として表記される場合があります。
イベント・カテゴリ	イベント・カテゴリに基づいてイベントを表示します。 例えば、「環境」、「火災」、「輸送」などのすべてのイベントを表示できます。
イベント・タイプ	タイプに基づいてイベントを表示します。 例えば、接近中の竜巻や交通事故などのイベントです。
開始日	イベントを表示する日付を入力します。日付範囲の場合は、開始日を入力します。
終了日	いつまでのイベントを表示するか、その日付を入力します。

注: このポートレットが適切に機能するためには、IBM Intelligent Operations Center アプリケーション・サーバー の完全修飾ドメイン名を使用して、ソリューション・ポータルにログオンする必要があります。登録された完全修飾ドメイン名の代わりに IP アドレスまたはホスト名の別名を使用してポータルにログオンした場合、このポートレットは正しく表示されません。

## レポート URL のコピー

レポート URL をコピーして、レポートがポートレットの右側のフレームに表示されるようにするには、URL を右クリックして「リンク・アドレスのコピー」を選択します。「リンク・アドレスのコピー」オプションの文言は、ご使用のブラウザによって異なります。

### 重要:

ユーザー定義レポートを保存して、ここでコピーしたリンクを使用するには、昨日の日付を「開始日」フィールドに入力し、明日の日付を「終了日」フィールドに入力します。これらの日付を指定することにより、必要なすべてのデータがユーザー定義レポートに含まれるようになります。例えば、8/10/2012 から 8/18/2012 までの日付範囲の場合は、以下の日付をフィルター基準に入力します。

- 開始日 - 8/9/2012 を入力する
- 終了日 - 8/19/2012 を入力する

## レポートのサンプル

IBM Intelligent Operations Center の「レポート」ポートレットには、「イベント」ポートレットのデータに基づき、グラフィカル・レポートが表示されます。

大きめのレポート・フレームで、レポート・グラフに表示する情報のパラメーターを選択します。

ポートレットの右側に表示される 2 つのフレームには、ユーザー定義のレポートがコピーされます。

ページの一番下に表示されるレポートは、事前に定義されているチャートです。これらのレポートでイベントが日付または日付範囲に基づいて表示されるように構成するには、「レポートの構成」をクリックします。日付を入力し、「レポートの表示」をクリックします。

## レポートの統合

「レポート」ポートレットには、IBM Cognos Business Intelligence のレポートまたはページを埋め込むための IFrame が用意されています。ポートレットに統合するレポートまたはページの URL を指定してください。

### Administrator

## 「レポート」ポートレットのカスタマイズ

管理者権限がある場合、このポートレットをカスタマイズできます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

ヘルプ・ファイルの位置、ポートレットの高さ、ポートレットの幅、ポートレット・タイトルなど、ポートレット間で共通な汎用のポートレット・パラメーターを設定できます。表示されるレポートの URL を指定することもできます。

## 関連資料:

179 ページの『「レポート」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「レポート」ポートレットをカスタマイズできます。

## 状況

「状況」ポートレットでは、単独または複数の組織の重要業績評価指標 (KPI) の状況を確認することができます。

「状況」ポートレットには、表示する権限のある複数の組織全体にわたって、KPI の状況に関するエグゼクティブ・レベルのサマリーが表示されます。計画を立て、必要に応じて対処できるように、このポートレットを使用して、KPI の状況に関する最新の変更を確認します。

## KPI の色分け

各列には、列の最上部に名前が示されている組織の KPI 情報が表示されます。各組織に関連付けられた KPI のカテゴリは、色分けされたセルによって表示されます。KPI カテゴリの背景色は、その状況を反映しています。列に表示される KPI の数が 6 を超える場合、各セルのサイズは、追加の KPI を表示できるようにするため、小さくなります。

ソリューションのサンプル KPI で提供される背景色の色分けは、以下のようになっています。

- 緑色は、対象の KPI のパラメーターに基づき、受け入れ可能な状況であることを示します。
- 黄色は、注意またはモニターが必要であることを示します。
- 赤色は、対処が推奨されることを示します。
- 灰色は、KPI の状況について計算するのに使用可能なデータが十分でないことを示します。

色分けは、ポートレットの上部の凡例で定義されています。

未確定の状況は、その KPI に関して定義された期間内で使用できる KPI の値がないことを示しています。この状態は、KPI に関するメッセージを、指定した期間内にソリューションが受信しなかった場合に発生します。例えば、水源の水位が毎日計算されるとします。この場合、特定の日に、この水源の水位に関するメッセージを受信しないと、KPI の値を確定するデータが存在しないことになります。

KPI 名、および KPI の色で表される状況の定義を確認するには、セルの上にカーソルを移動します。

## KPI の更新

基礎となる KPI が変化すると、その変化が「状況」ポートレットに反映されます。例えば、サンプル KPI には水質 KPI の変化の状況を判別するためのものがありますが、その KPI の状況が「許容可能」から「注意」に変わったとします。「水質」セルの背景色が緑色から黄色に変わることにより、この変化がポートレットに反映されます。さらに、「通知」ポートレットで、KPI が変化したことが示されます。

KPI の計算に関するメッセージをソリューションが受信すると、色が即時に変わります。この機能は、リアルタイムで変更が受信される可能性が高い KPI カテゴリ (航空機関の遅延など) の場合に役立ちます。この機能は、履歴の KPI を持つカテゴリ (治水など) には該当しません。このような KPI カテゴリの場合、日次の測定が定期的に行われ、その間に状況に影響する急激な変動が発生する可能性は低いと考えられます。

それぞれの KPI について、基礎となる KPI すべてと詳細を、「状況」ポートレットにリンクしている「重要業績評価指標のドリルダウン」ポートレットで確認できます。

「重要業績評価指標のドリルダウン」ポートレットで特定の KPI に絞り込んで表示するには、「状況」ポートレットの表で当該 KPI のセルをクリックします。また、所有する組織の名称（「水道」など）をクリックして、関連するすべての KPI を確認することもできます。

## Administrator

### 「状況」ポートレットのカスタマイズ

管理者権限がある場合、このポートレットをカスタマイズできます。ポートレットの右上隅にあるボタンをクリックして、ポートレット・メニューのカスタマイズ・オプションを表示します。共有設定は、すべてのユーザーの当該ポートレットの内容に影響を与えますが、影響を与える範囲は当該ポートレットの現行のオカレンスのみです。

「状況」ポートレットのパラメーターを設定することにより、以下の操作を行えます。

- KPI の色をカスタマイズする。
- 追加の KPI フィルターを使用可能にする。
- KPI の凡例を表示または非表示にする。
- KPI のソート方法を定義する。
- 「重要業績評価指標のドリルダウン」ポートレットとの通信を可能にするグループ名を指定する。

また、ヘルプ・ファイルの位置、ポートレットの高さ、ポートレット・タイトル、リソース・バンドルなど、ポートレット間で共通な汎用のポートレット・パラメーターを設定することができます。

### KPI のカスタマイズ

ソリューションには、一連のサンプル KPI が付属しています。こうした KPI は、さまざまなタイプの KPI をユーザーの組織に合わせて計画および実装する際の手引きとなるように設計されています。水道、輸送、公共安全の各分野のサンプルが用意されています。

#### 関連概念:

186 ページの『重要業績評価指標』

「重要業績評価指標」ポートレットでは、IBM Intelligent Operations Center の重要業績評価指標 (KPI) およびそれらの階層表示をカスタマイズすることができます。

#### 関連資料:

182 ページの『「状況」ポートレットの設定』

「共有設定」ウィンドウのフィールドの設定値を変更することによって、「状況」ポートレットをカスタマイズできます。

---

## 第 9 章 トラブルシューティングとサポート

IBM ソフトウェアに関する各種の問題を切り分けて解決するために、トラブルシューティング情報およびサポート情報を使用できます。これには、ご使用の IBM 製品に付属している問題判別リソースの使用方法が含まれます。

---

### 問題のトラブルシューティング手法

トラブルシューティングとは、問題を解決するための体系的な方法です。トラブルシューティングの目標は、予想したように動作しなかった原因およびその問題の解決方法を判別することです。

トラブルシューティングの最初の手順は、問題を完全に記述することです。問題記述によって、ユーザーと IBM 技術サポートの担当者が問題の原因を見つけるために、どこから開始するべきかを知るのに役立ちます。この手順には、お客様自身で確認が必要な、基本的な質問が含まれます。

- 問題にはどのような症状がありますか?
- どこで問題が発生していますか?
- いつ問題が発生しますか?
- どのような条件下で問題が発生しますか?
- 問題は再現できますか?

一般に、これらの質問に回答することで問題を適切に記述することができ、これにより問題解決につながります。

#### 問題にはどのような症状がありますか?

問題の記述を開始するとき、最も明白な質問として「何が問題であるのか」ということが挙げられます。この質問は単純なように思われますが、これをいくつかのさらに絞り込んだ質問に分解し、問題をさらに具体的に記述することができます。細分化した質問には以下のようなものがあります。

- 問題を報告しているのは誰または何ですか?
- エラー・コードおよびメッセージは何ですか?
- システムにどのような障害が発生しますか? 例えば、ループ、停止、異常終了、性能低下、または間違った結果などですか。

#### どこで問題が発生していますか?

問題が発生している場所の判別は必ずしも容易ではありませんが、問題解決においては最も重要な手順の 1 つです。障害を報告したコンポーネントと障害が発生したコンポーネントの間には、何層ものテクノロジーが存在する可能性があります。ネットワーク、ディスク、およびドライバーは、問題を調査する際に考慮すべきコンポーネントの一部に過ぎません。

以下の質問は、問題の発生場所に焦点を絞って、問題のレイヤーを特定するのに役立ちます。

- 問題は 1 つのプラットフォームまたはオペレーティング・システムに特定のものですか、それとも複数のプラットフォームまたはオペレーティング・システムに共通していますか?
- 現行の環境および構成はサポートされていますか?



あるレイヤーが問題を報告している場合、問題が発生しているのは必ずしもそのレイヤー内ではありません。問題の発生場所を特定するためには、その問題が存在する環境を理解することも必要です。オペレーティング・システムとバージョン、対応するすべてのソフトウェアとバージョン、およびハードウェア情報など、時間をかけて問題の環境を完全に記述してください。サポートされる構成の環境で稼働していることを確認してください。問題の多くは、ソフトウェア・レベルの非互換性に原因がある場合が多く、それらのソフトウェアは、同時に実行されることを意図していないか、または同時に実行する場合のテストが十分に行われていません。

## いつ問題が発生しますか？

特に発生が 1 回限りのケースについては、障害に至るイベントの詳細なタイムラインを作成します。作業をさかのぼることによって、タイムラインを簡単に作成できます。エラーが報告された時点 (できるだけ詳細に、ミリ秒単位まで) から開始します。使用できるログと情報を逆方向にたどります。通常、確認する必要があるのは、診断ログで見つけた最初の疑わしいイベントまでの部分だけです。

イベントの詳細なタイムラインを作成するには、次の質問に答えます。

- 問題が発生するのは、一日の特定の時刻だけですか？
- 問題はどのくらいの頻度で発生しますか？
- 問題が報告される時刻に至るまで、どういうイベントのシーケンスがありますか？
- 問題が発生するのは、ソフトウェアやハードウェアのアップグレードやインストールなど、環境を変更した後ですか？

これらの種類の質問に回答することによって、問題の調査における参照の枠組みを提示できます。

## どのような条件下で問題が発生しますか？

問題の発生時に稼働しているシステムおよびアプリケーションを把握することは、トラブルシューティングの重要な部分です。次の環境に関する質問は、問題の根本原因を特定するのに役立ちます。

- 問題が発生するのは、いつも同じタスクが実行されているときですか？
- 問題が表面化するには、イベントが特定の順序で発生する必要がありますか？
- 同時に他のアプリケーションにも障害が発生しますか？

これらの質問に答えることで、問題が発生する環境を説明し、依存関係に関連付けることができます。ほぼ同時に複数の問題が発生する場合でも、それらの問題が関連しているとは限らないことに注意してください。

## 問題は再現できますか？

トラブルシューティングの観点からすると、問題は再現可能であることが理想的です。通常、問題が再現できる場合は、調査に役立つ大規模なツールやプロシーチャーのセットがあります。したがって、再現できる問題は、多くの場合、デバッグや解決が容易です。ただし、再現可能な問題で不都合が生じる可能性もあります。問題によって業務に大きな影響が出る場合、問題を繰り返し発生させることは望ましくありません。可能であれば、テストまたは開発用の環境で問題を再作成します。これらの環境では通常、調査時の柔軟性が高まり、制御しやすくなります。

- テスト・システムで問題を再現できますか？
- 複数のユーザーまたは複数のアプリケーションで同じタイプの問題が発生していますか？
- 単一コマンド、コマンドのセット、または特定のアプリケーションで問題を再現できますか？

### 関連情報



355 ページの『知識ベースの検索』

IBM 知識ベースを検索することで、問題の解決策が見つかることがあります。使用可能なリソース、サポート・ツール、および検索方法を使用して、結果を最適化できます。

---

## トレースの使用可能化およびログ・ファイルの表示

IBM Intelligent Operations Center での問題をトラブルシューティングするには、いくつかのシステムのログ・ファイルを分析することが必要な場合があります。以下のトピックでは、ログ・ファイルへのアクセス方法についていくつか説明しています。

トレースを開始してログを表示するには、実行時に root ユーザーとしてコマンドを入力してください。

### 関連概念:

232 ページの『コンポーネントの検証』

システム検査チェックツールは、IBM Intelligent Operations Center 内のコンポーネントをテストし、アクセス可能であるか、および操作可能であるかを判別します。

334 ページの『IBM Support Assistant Lite のインストールと使用』

IBM Support Assistant Lite (ISA Lite) は、一般的な問題の分析に役立つ一般的診断データを収集するツールです。

### 関連タスク:

330 ページの『インストール収集必須ツールの実行』

IBM Intelligent Operations Center のインストール中には、ログ・ファイルが生成されます。ツールを使用して、これらのログ・ファイルを分析用に収集することができます。

## アプリケーション・サーバーのログ・ファイル

アプリケーション・サーバーの一部のシステムについてトレースを使用可能にしてログを表示するには、以下の手順を実行します。

以下のシステムのトレースを使用可能にしてログを表示する方法については、以下の手順で説明します。

- WebSphere Portal
- IBM WebSphere Business Monitor

## WebSphere Portal でのトレースの使用可能化とログの表示

### このタスクについて

WebSphere Portal ログは、/opt/IBM/WebSphere/wp\_profile1/logs/WebSphere\_Portal にあります。以下の手順にある各ステップに従って、トレースを開始し、ログを表示します。

### 手順

1. `http://app-host:9060/ibm/console` で管理コンソールにログオンします。ここで、**app-host** はアプリケーション・サーバーの完全修飾ホスト名です。
2. 「トラブルシューティング」 > 「ログおよびトレース」をクリックします。
3. 「WebSphere Portal」 > 「ログ・レベル詳細の変更 (Change log level details)」をクリックします。
4. 「実行時間」タブをクリックし、以下のコマンドを貼り付けます。

```
**warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
```

5. 「OK」をクリックします。
6. ログを表示するには、以下のコマンドを入力します。

```
cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
tail -f trace.log
```

## アプリケーション・サーバー上の IBM WebSphere Business Monitor のトレースの使用可能化およびログの表示

### このタスクについて

アプリケーション・サーバー上の IBM WebSphere Business Monitor のログは、`/opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/` にあります。以下の手順にある各ステップに従って、トレースを開始し、ログを表示します。

### 手順

1. `http://app-host:9060/ibm/console` で管理コンソールにログオンします。ここで、**app-host** はアプリケーション・サーバーの完全修飾ホスト名です。
2. 「トラブルシューティング」 > 「ログおよびトレース」をクリックします。
3. 「WBM\_DE.AppTarget.WBMNode1.0」 > 「ログ・レベル詳細の変更 (Change log level details)」をクリックします。
4. 「ランタイム」タブをクリックし、次のトレース・レベル・コードを貼り付けます。  
`com.ibm.wbm.*=finest: com.ibm.events.*=all: com.ibm.wbimonitor.xsp.cei.*=all:  
com.ibm.wbimonitor.xsp.eventselector.*=all`
5. 「OK」をクリックします。

### 関連情報:

 IBM WebSphere Portal 7 の製品資料

## イベント・サーバーのログ・ファイル

イベント・サーバーの一部のシステムについてトレースを使用可能にしてログを表示するには、以下の手順を実行します。

以下のシステムのトレースを使用可能にしてログを表示する方法については、以下の手順で説明します。

- Tivoli Service Request Manager
- WebSphere MQおよびWebSphere Message Broker
- Tivoli Netcool/OMNIbus XML プローブ
- Tivoli Netcool/OMNIbus (オブジェクト・サーバー) データベース
- Tivoli Netcool/OMNIbus (プロセス・エージェント) データベース
- Tivoli Netcool/Impact

## Tivoli Service Request Manager のトレースの使用可能化とログ・ファイルの表示

### このタスクについて

Tivoli Service Request Manager から IBM Intelligent Operations Center への情報の流れをデバッグするには、以下の手順を実行します。

### 手順

1. Tivoli Service Request Manager ユーザー・インターフェースで、「移動」 > 「システム構成」 > 「プラットフォームの構成」 > 「ロギング」をクリックします。

2. 「ルート・ロガー」で、フィルター・フィールドに `integration` と入力します。
3. 「**integration**」を展開します。
4. 以下のようにして、「integration」ロガーを構成します。
  - a. 「ログ・レベル」では、「値の選択」アイコンをクリックします。「値の選択」ウィンドウで、「**DEBUG**」をクリックします。
  - b. 「アペンダー」では、「アペンダーの管理」アイコンをクリックします。「アペンダーの管理」ウィンドウで、「日次ローリング (Dailyrolling)」チェック・ボックスを選択して、「**OK**」をクリックします。
  - c. 「アクティブ?」チェック・ボックスを選択します。
  - d. 「ロガーの保存」アイコンをクリックします。
5. 「アクションの選択」リストで、「ロギング・ルート・フォルダーの設定」を選択します。
6. 「ロギング・ルート・フォルダーの設定」ウィンドウの「ルート・ロギング・フォルダー」で、`/opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1` と入力して「**OK**」をクリックします。
7. 「ロガーの保存」アイコンをクリックします。
8. 「アクションの選択」リストで、「設定の適用」を選択します。
9. ログを表示するには、Tivoli Service Request Manager のサーバー端末で、以下のコマンドを入力します。

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/maximo/logs
tail -f event-host_MXServer_maximo_scheduled.log
```

ここで、`event-host` は、イベント・サーバー のホスト名です。

#### 関連タスク:

373 ページの『ログ・ファイルの確認』

Tivoli Netcool/OMNIBus ポリシー・ログ・ファイルと Tivoli Service Request Manager ログ・ファイルを確認します。

## WebSphere MQ および WebSphere Message Broker のトレースの使用可能化とログ・ファイルの表示

### このタスクについて

WebSphere MQ および WebSphere Message Broker のログは、以下の場所に保管されます。

- `/var/mqm/errors`
- `/var/mqm/qmgrs/IOC!MB!QM/errors`

トレース・ファイルは `/var/mqm/trace` ディレクトリーに書き込まれます。以下の手順で示すように、トレースをオンにする対象は、単一のキュー・マネージャーでもすべてのキュー・マネージャーでも構いません。

#### 手順

1. トレースの開始、終了、またはフォーマット設定を行うには、以下のように該当のコマンドを選択します。
  - すべてのプロセスのトレースを開始するには、コマンド `strmqtrc -e` を入力します。
  - IBM Intelligent Operations Center キュー・マネージャーのトレースを開始するには、コマンド `strmqtrc -m IOC.MB.QM` を入力します。

- IBM Intelligent Operations Center キュー・マネージャーの高詳細トレースを開始するには、コマンド `strmqtrc -t all -t detail -m IOC.MB.QM` を入力します。
  - すべてのトレースを終了するには、コマンド `endmqtrc -a` を入力します。
  - バイナリー・トレース・ファイルを ASCII フォーマットに設定するには、コマンド `dspmqtrc *.TRC` を入力します。
2. WebSphere Message Broker の状況を確認するには、以下の手順を実行します。
    - a. コマンド `ps -ef | grep IOC_BROKER` を入力します。
    - b. 以下のプロセスの状況を確認します。
      - `bipservice IOC_BROKER`
      - `bipbroker IOC_BROKER`
      - `biphttplistener IOC_BROKER`
      - `DataFlowEngine IOC_BROKER 5fe69373-2f01-0000-0080-9ab9c3579b15 default`

## Tivoli Netcool/OMNibus XML プローブのトレースの使用可能化とログ・ファイルの表示

### このタスクについて

WebSphere Portal ログは、`/opt/IBM/netcool/omnibus/log/ioc_xml.log` にあります。以下の手順にある各ステップに従って、トレースを開始し、ログを表示します。

### 手順

1. イベント・サーバーの端末を開きます。
2. コマンド `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log` を入力します。
3. メッセージ `Connection status OK` がファイルの下部に表示されない場合は、現在のログ・ファイルの名前を変更するために、コマンド `mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log` を入力します。
4. メッセージ `Connection status OK` が表示されない場合は、メッセージ `Probe shutting down` が表示されることもあります。プローブを再始動するには、以下のコマンドを入力します。
 

```
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```
5. 約 1 分後に、コマンド `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log` をもう一度入力します。
6. メッセージ `Connection status OK` が引き続き表示されない場合は、`/opt/IBM/netcool/omnibus/log/ioc_xml.log` ファイルを調べてエラーの有無を確認します。接続の問題は、オブジェクト・サーバーがダウンしていることを意味する場合があります。次のセクション『*Tivoli Netcool/OMNibus (オブジェクト・サーバー) データベースのトレースの使用可能化とログの表示*』を参照してください。

## Tivoli Netcool/OMNibus (オブジェクト・サーバー) データベースのトレースの使用可能化とログ・ファイルの表示

### このタスクについて

ログ・ファイルは以下の場所にあります。

- `/opt/IBM/netcool/omnibus/log/ioc_xml.log`
- `/opt/IBM/netcool/omnibus/log/NCOMS*.*`。以下に例を示します。
  - `/opt/IBM/netcool/omnibus/log/NCOMS.log`
  - `/opt/IBM/netcool/omnibus/log/NCOMS_trigger_stats.log1`

– /opt/IBM/netcool/omnibus/log/NCOMS\_profiler\_report.log1

以下の手順にある各ステップに従って、トレースを開始し、ログを表示します。

## 手順

1. root ユーザーとして端末にログオンします。
2. コマンド `/opt/IBM/netcool/omnibus/bin/nco_config &` を入力します。
3. `omni.dat` からインポートするかを尋ねられた場合は、「はい」をクリックして、「完了」をクリックします。
4. プロセス・エージェントのウィンドウを最小化します。
5. 「NCOMs」を右クリックします。
6. 以下から該当するオプションを選択します。
  - 「接続方法... (Connect As...)」オプションが表示されない場合は、以下のようにして NCOMS オブジェクト・サーバーを始動する必要があります。
    - a. NCOMS オブジェクト・サーバーを始動するには、`nco_config` を閉じてコマンド `/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &` を入力します。
    - b. NCOMS オブジェクト・サーバーが始動しない場合は、`/opt/IBM/netcool/omnibus/var` ディレクトリで `NCOMS.pid` ファイルを見つけて削除し、NCOMS オブジェクト・サーバーをもう一度始動してみます。
  - 「接続方法... (Connect As...)」オプションが表示される場合は、「接続方法... (Connect As...)」をクリックし、ユーザー名に `root` と入力して、パスワードを入力します。
7. NCOMS サーバーを始動したら、以下のコマンドを入力してプローブを再始動します。

```
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```
8. ログ・ファイルを表示するには、コマンド `tail -f /opt/IBM/netcool/omnibus/log/NCOMS.log` を入力します。

## Tivoli Netcool/OMNibus (プロセス・エージェント) データベースのログ・ファイル

Tivoli Netcool/OMNibus (プロセス・エージェント) データベースのログ・ファイルは、`/opt/IBM/netcool/omnibus/log/NCO_PA.log` にあります。

## Tivoli Netcool/Impact ログ・ファイルの使用可能化と表示

### このタスクについて

ログ・ファイルは `opt/IBM/netcool/impact/log/` にあります。以下の手順にある各ステップに従って、トレースを開始し、ログを表示します。

## 手順

1. ユーザー名 `admin` を使用して、`http://event-host:9080/nci` で Tivoli Netcool/Impact 管理コンソールにログオンします。ここで、`event-host` はイベント・サーバーの完全修飾ホスト名です。ログイン・プロンプトが表示されない場合は、端末ウィンドウで以下のコマンドを入力します。

```
su - netcool
/opt/IBM/netcool/bin/ewas.sh start
```
2. 「サービス状況」ウィンドウをスクロールダウンし、以下のサービスが実行されていることを確認します (緑の記号で示されます)。
  - `IOC_CAP_Event_Reader`
  - `IOC_Notification_Reader`

3. 同様に、「サービス状況」ウィンドウで、「ポリシー・ロガー」の横にある「ログの表示」アイコンをクリックし、ログに表示されているエラーがあるかどうかを確認します。
4. ログに 1 つ以上のエラーがある場合、詳細については、`/opt/IBM/netcool/impact/log/` ディレクトリにあるログ・ファイルを参照してください。
5. 詳細が必要な場合は、ログ・レベルをより高く設定します。「ポリシー・ロガー」をクリックし、「最上位のログ・レベル」の値を 3 に設定して、該当するチェック・ボックスを選択します。

## 次のタスク

WebSphere Application Server 管理コンソールを使用して、実行時に各種のログをオンにすることができます。ポータルトレースをオンにすることや、WebSphere Portal で使用できるその他のトレースをオンにすることについて詳しくは、このトピックの冒頭付近にある WebSphere Portal 製品資料のリンクを参照して、『ロギングとトレース』を検索して確認してください。

### 関連タスク:

373 ページの『ログ・ファイルの確認』

Tivoli Netcool/OMNIBus ポリシー・ログ・ファイルと Tivoli Service Request Manager ログ・ファイルを確認します。

## インストール収集必須ツールの実行

IBM Intelligent Operations Center のインストール中には、ログ・ファイルが生成されます。ツールを使用して、これらのログ・ファイルを分析用に収集することができます。

### 手順

1. インストール・サーバーに root ユーザーとしてログオンし、端末ウィンドウを開きます。
2. `install_home/ioc/bin` ディレクトリに移動します。
3. `export JAVA_HOME=/opt/ibm/java-x86_64-60/jre` コマンドを実行し、`JAVA_HOME` 変数を設定して、Java 6 ランタイム JRE を使用するようになります。
4. `./mustgather.sh -p password` コマンドを実行します。ここで、`password` は、トポロジー・パスワードです。このツールは、初回実行時にトポロジー・プロパティ・ファイルをスキャンします。ツールの実行後にトポロジー・プロパティ・ファイルを変更する場合は、コマンドに `-n` を追加して、ツールがトポロジー・プロパティ・ファイルを再スキャンするようにします。例えば、`./mustgather.sh -n -p password` のようにします。

### タスクの結果

収集されたログおよびその他の情報は、インストール・サーバーの `install_media/mustGather` ディレクトリに書き込まれます。`.tar` という拡張子のファイルが、各サーバーに 1 つずつ作成されます。

収集される情報は以下のとおりです。

- すべてのインストール・フェーズのログ。これには、各ノードにインストールされた各コンポーネントのログも含まれます。
- システム検査チェック・ツールのインストール・ログ。
- トポロジー XML ファイル。
- インストール処理中に使用されるすべてのスクリプト。
- Cyber Hygiene で処理されるすべてのぜい弱性。
- Cyber Hygiene スクリプト。



## 関連概念:

325 ページの『トレースの使用可能化およびログ・ファイルの表示』

IBM Intelligent Operations Center での問題をトラブルシューティングするには、いくつかのシステムのログ・ファイルを分析することが必要な場合があります。以下のトピックでは、ログ・ファイルへのアクセス方法についていくつか説明しています。

『コンポーネントのトラブルシューティング』

システム検査チェック・ツールを使用して、IBM Intelligent Operations Center のコンポーネントのトラブルシューティングを実行できます。

## 関連タスク:

55 ページの『ステップ・バイ・ステップでインストール中の IBM Intelligent Operations Center アーキテクチャーのインストールの再開』

アーキテクチャーのインストールが失敗した場合、そのインストールを再開することができます。

360 ページの『IBM との情報の交換』

問題を診断または識別するには、ご使用のシステムのデータおよび情報を IBM サポートに提供する必要があります。場合によっては、問題の判別には使用するためのツールまたはユーティリティが IBM サポートによって提供されることもあります。

---

## コンポーネントのトラブルシューティング

システム検査チェック・ツールを使用して、IBM Intelligent Operations Center のコンポーネントのトラブルシューティングを実行できます。

システム検査チェック・ツールについて詳しくは、このトピックの末尾にあるリンクを参照してください。

以下のセクションの表に、IBM Intelligent Operations Center に含まれる各サーバーのログ・ファイルの場所を示します。すべてのログ・ファイルは自動的に作成されます。該当する tail コマンドを使用して表示してください。

### インストール・サーバー

インストール・ログ・ファイルの収集については、インストール収集必須ツールの実行に関するトピックを参照してください。このトピックの末尾にあるリンクに移動してください。

### アプリケーション・サーバー

表 96. アプリケーション・サーバーのコンポーネントとログ・ファイル

コンポーネント	ログ・ファイル
IBM Cognos Administration	<ul style="list-style-type: none"><li>• /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Displ/SystemOut.log</li><li>• /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_Displ/SystemErr.log</li><li>• /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemOut.log</li><li>• /opt/IBM/WebSphere/AppServer/profiles/cognosProfile1/logs/CognosX_GW1/SystemErr.log</li><li>• /opt/IBM/cognos/c10_64/logs/ ディレクトリーにあるすべてのログ</li></ul>

表 96. アプリケーション・サーバーのコンポーネントとログ・ファイル (続き)

コンポーネント	ログ・ファイル
IBM HTTP Server	<ul style="list-style-type: none"> <li>• /opt/IBM/HTTPServer/logs/error_log</li> <li>• /opt/IBM/HTTPServer/logs/access_log</li> </ul>
IBM WebSphere Business Monitor	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/wbmProfile1/logs/WBM_DE.AppTarget.WBMNode1.0/SystemErr.log</li> </ul>
IBM Lotus Sametime Proxy Server	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log</li> </ul>
Tivoli Access Manager	<ul style="list-style-type: none"> <li>• /var/pdweb/log/msg_*.log。ここでの * は任意の値です。</li> <li>• /var/pdweb/log/config_data_*.log。ここで、* は任意の値です。</li> </ul>
Tivoli Access Manager WebSEAL	<ul style="list-style-type: none"> <li>• /var/pdweb/log/msg_webseald-default.log</li> <li>• /var/pdweb/www-default/log/ ディレクトリーにあるすべてのログ</li> </ul>
Tivoli Directory Server プロキシ構成ログ	<ul style="list-style-type: none"> <li>• /datahome/proxy/idsslapd-tdsproxy/logs/ibmslapd.log</li> </ul>
WebSphere Operational Decision Management	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/wodmProfile1/logs/wodmServer1/SystemErr.log</li> </ul>
WebSphere Portal	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemOut.log</li> <li>• /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal/SystemErr.log</li> </ul>
WebSphere UDDI Registry	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/cpudProfile1/logs/cpudServer1/SystemErr.log</li> </ul>

## データ・サーバー

表 97. データ・サーバーのコンポーネントとログ・ファイル

コンポーネント	ログ・ファイル
Tivoli Directory Server	<ul style="list-style-type: none"> <li>• /datahome/dsrdm01/idsslapd- dsrdm01/logs/ibmslapd.log</li> <li>• /datahome/dsrdm01 /idsslapd- dsrdm01/logs/ ディレクトリーにあるすべてのログ</li> </ul>

## イベント・サーバー

表 98. イベント・サーバーのコンポーネントとログ・ファイル

コンポーネント	ログ・ファイル
Lotus Domino	<ul style="list-style-type: none"> <li>• /local/notesdata/console.out</li> <li>• /local/notesdata/log.nsf</li> <li>• /local/notesdata/IBM_TECHNICAL_SUPPORT/ ディレクトリーのすべてのログ</li> </ul>
Lotus Sametime Community Server	<p>該当するすべてのログ・ファイルを収集して /local/notesdata/ ディレクトリーに書き込むには、以下のコマンドを入力します。</p> <pre>/local/notesdata/sh stdiagzip.sh</pre>
Tivoli Netcool/Impact	<ul style="list-style-type: none"> <li>• /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemOut.log</li> <li>• /opt/IBM/netcool/eWAS/profiles/ImpactProfile/logs/server1/SystemErr.log</li> </ul>
Tivoli Netcool/OMNIBus	<ul style="list-style-type: none"> <li>• /opt/IBM/netcool/log</li> <li>• /opt/IBM/netcool/omnibus/log</li> </ul>
Tivoli Service Request Manager	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/logs/MXServer1/SystemErr.log</li> </ul>

## 管理サーバー

表 99. 管理サーバーのコンポーネントとログ・ファイル

コンポーネント	ログ・ファイル
管理サーバー	<ul style="list-style-type: none"> <li>• Tivoli Event Monitoring Server: /opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_ms_{nnnnnn}.log</li> <li>• Tivoli Event Portal Server: /opt/IBM/ITM/logs/{MGMT_SERVER_HOST}_cq_{nnnnnn}.log</li> <li>• 組み込み WebSphere Application Server のログ: <ul style="list-style-type: none"> <li>– エラー・ログ: /opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log</li> <li>– 出力ログ: /opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log</li> <li>– 開始ログ: /opt/IBM/ITM/li6263/iw/profiles/ITMProfile/logs/ITMServer/startServer.log</li> </ul> </li> </ul>
Tivoli Access ManagerおよびWebSphere Portal Manager	<ul style="list-style-type: none"> <li>• /var/PolicyDirector/log/msg_pdmgrd_utf8.log</li> <li>• /var/PolicyDirector/log/msg_pdacld_utf8.log</li> </ul>

表 99. 管理サーバーのコンポーネントとログ・ファイル (続き)

コンポーネント	ログ・ファイル
Tivoli Access Manager	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log</li> </ul>
Tivoli Enterprise Monitoring Agent	<ul style="list-style-type: none"> <li>• /opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log</li> </ul>
Tivoli Enterprise Portal	<ul style="list-style-type: none"> <li>• /opt/IBM/ITM/logs/*_PRODUCT_CODE_{nnnnnn}.log</li> </ul>
Tivoli Identity Manager	<ul style="list-style-type: none"> <li>• /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemOut.log</li> <li>• /opt/IBM/WebSphere/AppServer/profiles/timProfile/logs/timServer1/SystemErr.log</li> <li>• /var/idsldap/ ディレクトリーの V6 サブディレクトリーにあるすべてのログ</li> </ul>

#### 関連概念:

289 ページの『ログ・ファイルの管理』

IBM Intelligent Operations Center では、いくつかの異なる場所にログ・ファイルが保管されます。システム・パフォーマンスの問題を回避するために、定期的にログ・ファイルをアーカイブし、元のログ・ファイルを削除します。

#### 関連タスク:

330 ページの『インストール収集必須ツールの実行』

IBM Intelligent Operations Center のインストール中には、ログ・ファイルが生成されます。ツールを使用して、これらのログ・ファイルを分析用に収集することができます。

#### 関連情報:

システム検査チェック・ツールの使用方法

システム検査チェック・ツールは、IBM Intelligent Operations Center システムから成るサービスの運用状況を判別するために使用します。

---

## IBM Support Assistant Lite のインストールと使用

IBM Support Assistant Lite (ISA Lite) は、一般的な問題の分析に役立つ一般的診断データを収集するツールです。

ISA Lite は以下の種類の情報を収集します。

- プラットフォームの問題判別ファイル
- システム・ログおよびトレース・ファイル
- プラットフォーム・プロビジョニング・ファイル
- システム構成ファイル
- Java™ ダンプ・ファイル
- 問題判別フレームワークの内部ログ・ファイル

IBM Intelligent Operations Center 1.5 用の ISA Lite をダウンロードするには、このトピックの末尾にあるリンクを参照してください。

ISA Lite をインストールして使用するには、ダウンロード・パッケージに含まれる「Quick Start Guide」に記載されている説明に従ってください。

#### 関連情報:



IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5 のダウンロード

## IBM Intelligent Operations Center のメッセージ

各メッセージのトピックは、IBM Intelligent Operations Center で特定のエラー状態が発生する原因を特定するのに役立つ、また、エラーを解決するための推奨処置を示します。

IBM Intelligent Operations Center を使用しているときに発生する可能性のあるエラーを理解できるようにするために、各メッセージのトピックは、IBM Intelligent Operations Center またはそのログに表示されるメッセージ、説明、および処置という 3 つのセクションに分割されています。

### メッセージ

2 つの ID が含まれ、それぞれがエラー ID と、関連付けられているテキストを示します。エラー ID はメッセージ ID です。これは、メッセージを識別する固有の番号です。最後の文字 E はメッセージがエラーに起因することを示し、W は警告メッセージ、I は情報メッセージであることを示します。

**説明** メッセージの追加説明です。

### ユーザーの処置

エラーを解決するための修正処置が示されています。

エラー・メッセージについての情報を検索するには、インフォメーション・センターの検索フィールドにエラー・メッセージの ID 番号を入力します。

**注:** このセクションのトピックには、IBM Intelligent Operations Center に固有のメッセージのみが含まれています。他のすべてのメッセージについては、製品資料を参照してください。

#### CIYBA0101E トポロジー・ファイル {0} が無効です。

**説明:** インストーラーは {0} トポロジー・ファイルの検証を試み、トポロジー・ファイルにエラーが含まれていることを検出しました。以下のエラーがあります。

- 必要なコンポーネントがトポロジー・ファイル内にすべて存在しているわけではない。
- 前提条件コンポーネントが従属コンポーネントよりも前にリストされていない。
- 順次デプロイする必要のあるコンポーネントが、並列開発スタンプ内に存在している。

**ユーザーの処置:** トポロジー・ファイルを修正し、インストールを再実行してください。

#### CIYBA0102E トポロジーまたはトポロジー仕様ファイルが見つかりませんでした。

**説明:** それぞれのインストール・トポロジーには、関連する .xml ファイルと仕様があります。これらのファイルの一方または両方を検出できませんでした。

**ユーザーの処置:** すべてのインストール・ファイルがインストール・サーバーに解凍されているかどうかを確認してください。custom.properties ファイル内の image.basedir.local プロパティが正しいロケーションに設定されているかどうかを確認してください。custom.propeties ファイルは、インストール・パッケージが解凍されたインストール・サーバー上の /resource サブディレクトリに格納されています。

#### CIYBA0103E コンポーネントをインストールするための {0} スクリプトが存在しません。

**説明:** インストール・プログラムがコンポーネントのスクリプトを検出しようとしたましたが、スクリプトが見つかりませんでした。

**ユーザーの処置:** インストール・メディアがインストール・サーバーに解凍されているかどうかを確認してください。custom.properties ファイルで、ベース・ディレクトリが正しく構成されているかどうかを確認してください。ベース・ディレクトリを使用して、インス

ツール・スクリプトのロケーションが取得されます。

---

**CIYBA0104E トポロジー・ファイルに、無効なエントリ  
ーが含まれています。**

**説明:** インストーラーが、トポロジー・ファイルを読み取り、各コンポーネント用にデプロイ可能な単位を作成しているときに、エラーを検出しました。これは、カスタム・トポロジーをインストールしている場合を除き、通常は内部エラーです。

トポロジー・ファイルが破損しているか、または誤って指定されている可能性があります。

**ユーザーの処置:** トポロジー・ファイルで以下の問題があるかどうかを調べてください。

- コンポーネント ID が重複している。
- コンポーネント ID または型属性が指定されていない。
- 接続属性の指定に親コンポーネントが存在しない。
- トポロジーが XML スキーマ検証に合格しない。

---

**CIYBA0105E {0} ファイルが見つかりませんでした。**

**説明:** インストール・プログラムが {0} ファイルを検出できませんでした。

**ユーザーの処置:** すべてのインストール・ファイルがインストール・サーバーに解凍されているかどうかを確認してください。 custom.properties ファイル内の image.basedir.local プロパティーが正しいロケーションに設定されているかどうかを確認してください。 custom.propeties ファイルは、インストール・パッケージが解凍されたインストール・サーバー上の /resource サブディレクトリーに格納されています。

---

**CIYBA0106E {0} ファイルを保存できませんでした。**

**説明:** インストール・プログラムは {0} という名前のファイルに書き込もうとしましたが、ファイル入出力エラーが返されました。

**ユーザーの処置:** インストーラーのユーザー ID を使用して、指定されたロケーションにアクセスできるかどうかを確認してください。 ディスク上に十分なスペースがあるかどうか、パーティションが破損していないかどうかを確認してください。

---

**CIYBA0107E プロパティー参照 {0} がトポロジー・フ  
ァイル {1} が見つかりませんでした。**

**説明:** インストール中に、一部のコンポーネントで、前提条件ソフトウェアからのプロパティー値が必要になります。 これらのコンポーネントは、トポロジー・ファイル内のプロパティー参照を使用して、必須プロパティ

ーの値を判別します。 このプロパティー参照が、トポロジー・ファイル内で見つかりませんでした。

**ユーザーの処置:** トポロジー・ファイルが破損していません。 これは、手動の編集によって無効なエントリが作成されたか、インストール時にトポロジー・ファイルが正しい値で書き込まれなかったことが原因で発生した可能性があります。 どのコンポーネントが誤ってインストールされたかを判別してください。 誤ってインストールされたコンポーネントをすべて削除し、トポロジー・ファイルを修正してから、再インストールしてください。

---

**CIYBA0108E コンポーネント {0} がトポロジー・フ  
ァイル {1} が見つかりませんでした。**

**説明:** インストール・プログラムは、{0} コンポーネント ID が {1} トポロジー・ファイル内で見つかることを予期していましたが、そのコンポーネント ID は見つかりませんでした。 この問題は、別のコンポーネントの接続要素で依存関係が誤って指定されたために発生した可能性があります。

**ユーザーの処置:** {0} への参照について、トポロジー・ファイルで確認してください。 {0} コンポーネントの誤った接続要素をすべて修正してから、再インストールしてください。

---

**CIYBA0109E トポロジー・ファイル {2} のプロパティ  
ー {0}、{1} が無効です。**

**説明:** トポロジー・ファイルと仕様プロパティー・ファイルで、このプロパティーが見つかりませんでした。

**ユーザーの処置:** 仕様プロパティー・ファイルまたはトポロジー・ファイルにこのプロパティーが指定されていない場合は、追加してください。 プロパティーのミススペルが原因で、このエラーが発生した可能性もあります。 トポロジー・ファイルまたは仕様プロパティー・ファイルを修正してから、再インストールしてください。

---

**CIYBA0110E トポロジー・ファイル {2} のプロパティ  
ー {0}、{1} が見つかりません。**

**説明:** デプロイ可能な単位が、役割 {1} で指定された別のデプロイ可能な単位を参照しています。 従属するデプロイ可能な単位が見つからないか、役割が一致していません。

**ユーザーの処置:** 上記のトポロジー・ファイルには、上記のプロパティーへの参照が含まれていますが、そのプロパティーの定義がトポロジー・ファイル内で見つかりません。 トポロジー・ファイルを手動で編集してコンポーネントを削除し、そのコンポーネントへの参照がま



だ存在する場合に、この状況が発生する可能性があります。

---

**CIYBA0111E コンポーネント {0} のマスター・ホストを取得できません。**

**説明:** トポロジー・コンポーネントは、ターゲット・ホストに関連付けられている必要があります。それにもかかわらず、孤立したトポロジー・コンポーネントが指定されています。

**ユーザーの処置:** {0} トポロジー・コンポーネントを調べて、ホスト属性を含むコンポーネントを最終的に持つことになる、一連の接続属性のシーケンスが含まれているかどうかを確認してください。

---

**CIYBA0112E トポロジー・ファイル {0} の読み取りに失敗しました。**

**説明:** インストール・プログラムが、指定されたトポロジー・ファイルを読み取ることができませんでした。

**ユーザーの処置:** 上記のトポロジー・ファイルがインストール・ディレクトリーに存在するかどうか、インストール・プログラムがそのディレクトリーにアクセスできるかどうかを確認してください。

---

**CIYBA0113E ファイル {0} を保存できませんでした。**

**説明:** インストール・プログラムが、上記のファイルを保存できませんでした。

**ユーザーの処置:** インストール・プログラムがインストール・ディレクトリーへのアクセス権限を持っているかどうかを確認してください。

---

**CIYBA0114E {0},{1} プロパティを設定できません。**

**説明:** インストール・プログラムが、上記のプロパティを更新できませんでした。

**ユーザーの処置:** トポロジー・ファイルが破損しているか、手動で編集されて無効なプロパティ値が設定されています。トポロジー・ファイルを修正し、インストールを再実行してください。

---

**CIYBA0115E トポロジー・ファイル {0} が見つかりません。**

**説明:** インストール・プログラムが、上記のトポロジー・ファイルにアクセスすることができませんでした。

**ユーザーの処置:** トポロジー・ファイルが、インストール・プログラムによって指定されたディレクトリー内に存在するかどうか、インストール・プログラムがそのデ

レクトリーにアクセスできるかどうかを確認してください。

---

**CIYBA0116E プロパティ・ファイル {0} に書き込むことができません。**

**説明:** インストール・プログラムが、上記のプロパティ・ファイルに書き込むことができませんでした。

**ユーザーの処置:** インストール・プログラムが使用するユーザー ID に、ターゲット・サーバー上の一時ディレクトリーへのアクセス権限があるかどうかを確認してください。一時インストール・スクリプトが書き込まれるターゲット・サーバー上のディレクトリーは、`custom.properties` ファイル内の `Unix.script.basedir.remote` プロパティによって指定されます。このプロパティが誤って指定されている場合は、修正してください。

---

**CIYBA0117E インストーラーが、鍵ストアを作成できませんでした。**

**説明:** インストール・プログラムが、鍵ストアを作成できませんでした。

**ユーザーの処置:** インストール・プログラムが使用するユーザー ID に、インストール・メディアが解凍されているすべてのサブディレクトリーへのアクセス権限があるかどうかを確認してください。

---

**CIYBA0118E インストーラーが、指定されたパスワードを使用して鍵ストアにアクセスできませんでした。パスワードが誤っているか、鍵ストアが破損しています。**

**説明:** インストール・プログラムが、鍵ストアにアクセスすることができませんでした。

**ユーザーの処置:** 指定されたパスワードが正しいかどうか、鍵ストアが破損していないかどうかを確認してください。ソリューションを再インストールすることにより新規パスワードで鍵ストアを再生成してください。

---

**CIYBA0119E トポロジー・ファイル {1} のプロパティ {0} を暗号化できません。**

**説明:** インストール・プログラムは、トポロジー・ファイルで指定されたパスワードを使用して、上記のプロパティを暗号化しようとしたましたが、暗号化できませんでした。

**ユーザーの処置:** 鍵ストアが破損していないかどうか、トポロジーのパスワードが正しいかどうかを確認してください。必要な場合は、再インストールを行って、新規パスワードで鍵ストアを再作成してください。

---

**CIYBA0120E トポロジー・ファイル {1} のプロパティ  
ー {0} を暗号化解除できません。**

**説明:** 上記のプロパティを読み取り、暗号化を解除しようとしたが、失敗しました。

**ユーザーの処置:** インストール・プログラムが使用するユーザー ID が、上記のトポロジーにアクセスできるかどうか、トポロジー・ファイルが正しいロケーションに存在するかどうかを確認してください。また、パスワードと秘密鍵が正しいかどうかを確認してください。インストールを再実行してください。

---

**CIYBA0121E 鍵ストア・ファイル {0} は既に存在しません。**

**説明:** IBM Installation Manager インストールを使用した場合、このエラーは発生しません。IBM Installation Manager は、インストールのフローを制御し、鍵ストアの再生成が試行されないようにします。

**ユーザーの処置:** インストールがまだ実行されていないことを確認してください。以前のインストール試行で生成された既存の鍵ストアを削除してから、インストーラーを再実行してください。

---

**CIYBA0122E トポロジーの鍵ストアが存在しません。  
createSecretKey コマンドを実行してください。**

**説明:** IBM Installation Manager インストールを実行した場合、このエラーは発生しません。IBM Installation Manager インストールは、自動的に SecretKey を受け入れ、鍵ストアを生成します。

**ユーザーの処置:** ステップ・バイ・ステップのインストールを実行する場合は、鍵ストアを生成するステップを実行してください。

---

**CIYBA0123E トポロジー {0} が完全にはインストール  
されていません。**

**説明:** インストール・プログラムにより、トポロジー内の一部のコンポーネントがインストールされていないことが検出されました。

**ユーザーの処置:** トポロジー・ファイルを調べて、どのコンポーネントがインストールされていないかを判別してください。インストールを再開してください。

---

**CIYBA0124E {0} プロパティ・ファイルが見つかり  
ません。**

**説明:** インストール・プログラムが、上記のプロパティ・ファイルを読み取ろうとしたが、ファイルが見つかりませんでした。

**ユーザーの処置:** インストール・パッケージが正しく解凍されているかどうかを確認してください。インストール・プログラムが使用するユーザー ID に、パッケージが解凍されているすべてのディレクトリーへのアクセス権限があるかどうかを確認してください。

---

**CIYBA0125E プロパティ・ファイル {0} に書き込む  
ことができません。**

**説明:** インストール・プログラムが、ランタイム変数の値を使用してファイルを更新しようとしたが、入力例外が返されました。

**ユーザーの処置:** インストール・プログラムのユーザー ID を使用して、指定されたロケーションにアクセスできるかどうかを確認してください。ファイル・システム内に十分なスペースがあるかどうか、ディスク・パーティションが破損していないかどうかを確認してください。

---

**CIYBA0126E トポロジー・ファイル {1} のプロパティ  
ー {0} の値を設定できません。**

**説明:** インストール・プログラムが、指定されたプロパティ値を設定できませんでした。

**ユーザーの処置:** 上記のトポロジー・ファイル内の上記のプロパティが、正しい XML 構文で記述されているかどうかを確認してください。このトポロジー・ファイルが破損していないかどうか、形式が正しいかどうかを確認してください。ファイル内の特殊文字をすべて削除してから、インストールを再開してください。

---

**CIYBA0127E ソリューション仕様ファイル {0} を読み  
取ることができません。**

**説明:** インストール・プログラムは、上記のファイルを読み取ろうとしたが、ファイル入出力エラーが返されました。

**ユーザーの処置:** このファイルが、指定されたロケーションに存在するかどうかを確認してください。インストール・プログラムが使用するユーザー ID に、パッケージが解凍されているすべてのディレクトリーへのアクセス権限があるかどうかを確認してください。

---

**CIYBA0128E {0} ファイルを保存できませんでした。**

**説明:** インストール・プログラムは、上記のファイルに書き込もうとしたが、ファイル入出力エラーが返されました。

**ユーザーの処置:** インストール・プログラムが使用するユーザー ID により、指定されたロケーションにアクセスできるかどうかを確認してください。ファイル・シ

ステム内に十分なスペースがあるかどうか、ディスク・パーティションが破損していないかどうかを確認してください。

---

**CIYBA0129E ソリューション・パッケージ・ファイル {0} を読み取ることができません。**

**説明:** インストール・プログラムは、上記のファイルを読み取ろうとしましたが、ファイル入出力エラーが返されました。

**ユーザーの処置:** このファイルが、指定されたロケーションに存在するかどうかを確認してください。インストール・プログラムが使用するユーザー ID に、パッケージが解凍されているすべてのディレクトリーへのアクセス権限があるかどうかを確認してください。

---

**CIYBA0130E ソリューション・パッケージ・ファイル {0} が存在しません。**

**説明:** インストール・プログラムは、上記のファイルを読み取ろうとしましたが、ファイル入出力エラーが返されました。

**ユーザーの処置:** メッセージに示されているファイルの権限を確認してください。インストール・プログラムが使用するユーザー ID に、このファイルを読み取る権限があるかどうかを確認してください。必要に応じてファイル権限を変更してください。

---

**CIYBA0131E インストーラーが {0} トポロジー・ファイルをロードできませんでした。ファイル入出力メッセージは {1} でした。**

**説明:** 指定されたトポロジー・ファイルをインポートしようとしたときに、上記のエラーが返されました。

**ユーザーの処置:** 上記のトポロジー・ファイルが正しいディレクトリーに存在するかどうかを確認してください。このトポロジー・ファイルに無効な文字が含まれていないかどうかを確認してください。インストール・プログラムが、このトポロジー・ファイルが存在するディレクトリーにアクセスできるかどうかを確認してください。

---

**CIYBA0140E 必要なインストール・ファイルにアクセスできません。**

**説明:** インストール・プログラムは、必要なファイルを読み取ろうとしましたが、読み取ることができませんでした。

**ユーザーの処置:** インストール・プログラムが使用するユーザー ID により、インストール・パッケージが解凍されているロケーションにアクセスできるかどうかを確

認してください。ディスク・パーティションが破損していないかどうかを確認してください。インストール・パッケージを再度解凍し、インストールを再試行してください。

---

**CIYBA0141E インストール・ファイル {0} が見つかりません。**

**説明:** インストール・プログラムは、上記のファイルを読み取ろうとしましたが、ファイル入出力エラーが返されました。

**ユーザーの処置:** このファイルが、指定されたロケーションに存在するかどうかを確認してください。インストール・プログラムが使用するユーザー ID が、解凍されたインストール・パッケージが格納されているすべてのディレクトリーにアクセスできるかどうかを確認してください。

---

**CIYBA0142E インストール・ファイル {0} に書き込むことができません。**

**説明:** インストール・プログラムは、上記のファイルに書き込もうとしましたが、ファイル入出力エラーが返されました。

**ユーザーの処置:** インストール・プログラムが使用するユーザー ID に、解凍されたインストール・パッケージが格納されているすべてのディレクトリーへのアクセス権限があるかどうかを確認してください。ディスク・パーティションが破損していないかどうか、スペースが不足していないかどうかを確認してください。

---

**CIYBA0143E インストール・プログラムが、トポロジー・ファイル进行处理できませんでした。**

**説明:** インストール・プログラムは、トポロジー・ファイルを読み取り、ランタイム値を含む中間ファイルを生成します。インストール・プログラムは、トポロジー・ファイル进行处理して中間ファイルを書き込んでいるときにエラーを検出しました。このエラーの原因として考えられるのは、ファイル入出力エラーです。

**ユーザーの処置:** インストール・プログラムが使用するユーザー ID に、インストール・パッケージが解凍されているすべてのディレクトリーへのアクセス権限があるかどうかを確認してください。ディスク・パーティションが破損していないかどうか、スペースが不足していないかどうかを確認してください。

---

**CIYBA0150E トポロジー仕様ファイル {0} を読み取ることができません。**

**説明:** インストール・プログラムは、上記のファイルを読み取ろうとしましたが、ファイル入出力エラーが返されました。

**ユーザーの処置:** このファイルが、指定されたロケーションに存在するかどうかを確認してください。インストール・プログラムが使用するユーザー ID に、インストール・パッケージが解凍されているすべてのディレクトリへのアクセス権限があるかどうかを確認してください。

---

**CIYBA0160E ルール仕様ファイルが {0} ディレクトリで見つかりませんでした。**

**説明:** インストール・プログラムは、事前検査ルールを定義する rule-spec.xml ファイルをロードしようとしたのですが、ロードできませんでした。

**ユーザーの処置:** 上記のディレクトリが存在するかどうかを確認してください。また、インストール・プログラムが使用するユーザー ID でこのディレクトリにアクセスできるかどうかを確認してください。

---

**CIYBA0161E ルール名 {0} は無効です。**

**説明:** インストール・プログラムは、rule-spec.xml ファイルで誤ったルール名を検出しました。このファイルは、事前検査ステップで使用されるルールを定義します。

**ユーザーの処置:** rule-spec.xml ファイルで、ルール名が正しいかどうかを確認してください。正しいルール名については、rule-spec.xml ファイルの未変更のバージョンを参照してください。

---

**CIYBA0162E インストール前提条件の検査がトポロジー {0} で失敗しました。**

**説明:** 事前検査ステップが失敗しました。サポートされるシステム要件を満たしていない構成ターゲットが 1 つ以上あります。

**ユーザーの処置:** 計画されたトポロジーが、サポートされる最小限の要件を満たしているかどうかを確認してください。

---

**CIYBA0163W ターゲット・サーバー {0} の OS タイプが {1} ではありません。**

**説明:** 事前検査ステップは、上記のターゲット・サーバー上で、サポートされていないオペレーティング・システムを検出しました。

**ユーザーの処置:** ターゲット・サーバー上のオペレーティング・システムが、サポートされるシステム要件を満たすようにしてください。

---

**CIYBA0164W {0} サーバーでは {1} ビット OS の使用が予期されていました。**

**説明:** 事前検査ステップにより、ターゲット・サーバーで誤ったオペレーティング・システムが検出されました。

**ユーザーの処置:** ターゲット・サーバーのオペレーティング・システムのタイプがシステム要件を満たしていることを確認してください。

---

**CIYBA0165W ターゲット・サーバー {0} の CPU が x86 でも s390 64 ビット CPU でもありません。**

**説明:** 事前検査ステップにより、示されているターゲット・サーバーの CPU タイプがサポートされていないことが検出されました。

**ユーザーの処置:** ターゲット・サーバーの CPU タイプが、システム要件を満たしていることを確認してください。

---

**CIYBA0166E ターゲット・サーバー {0} に接続できません。**

**説明:** 事前検査ステップの実行時に、インストール・プログラムはリモート・サーバーに接続できませんでした。

**ユーザーの処置:** インストール・サーバーとターゲット・サーバーの間の接続を確認してください。他のエラーがないか、事前検査ログを調べてください。

---

**CIYBA0167E 正しくないホスト名、アカウント、またはパスワードが指定されたため、サーバー {0} に接続できません。**

**説明:** 事前検査ステップの実行時に、インストール・プログラムが失敗しました。インストール・プログラムは、ターゲット・サーバーに接続できませんでした。

**ユーザーの処置:** ホスト名の形式が正しいこと、およびリモート・サーバー用に正しいログイン詳細が指定されていることを確認してください。追加情報がないか、事前検査ログを調べてください。



---

**CIYBA0168E** サーバー {0} と {0} の時間または時間帯が同期していません。

**説明:** サーバーに設定されている時間または時間帯に差があります。

**ユーザーの処置:** すべてのサーバーで時間および時間帯が同じであることを確認してください。

---

**CIYBA0169W** サーバー {0} の OS タイプおよび CPU アーキテクチャーを確認してください。

**説明:** インストール・プログラムの事前検査ステップで、ターゲット・サーバーのオペレーティング・システムおよび CPU アーキテクチャーがサポートされていないことが検出されました。

**ユーザーの処置:** すべてのサーバーが、ソリューションのシステム要件を満たすようにしてください。

---

**CIYBA0170W** すべてのサーバーの時間帯および日時を確認してください。

**説明:** このメッセージの後ろに「合格」または「失敗」という語が続きます。これらの語によって、取るべきアクションが決まります。

**ユーザーの処置:** メッセージの後ろに「合格」が続く場合、応答は不要です。メッセージの後ろに「失敗」が続く場合、サーバーを同期する必要があります。時間帯、日時のシステム・パラメーターは、トポロジーの各ノードで同じでなければなりません。

---

**CIYBA0171I** インスタンス {0} を使用してインストール前提条件の検査を開始しています。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0172I** インストール前提条件の検査が正常に完了しました。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0173I** インストール前提条件の検査が完了しましたが、{0} 件の警告と {1} 件のエラーが発生しました:

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0176E** サーバー {0} のログイン情報が正しくありません。サーバーで使用するユーザー ID とパスワードを確認してください。

**説明:** インストール・プログラムの事前検査ステップで、ターゲット・サーバーのログイン情報が正しくないことが検出されました。

**ユーザーの処置:** サーバーのアカウント詳細に、正しいユーザー ID とパスワードが指定されていることを確認してください。

---

**CIYBA0177W** リモート・サーバーに接続できません。再試行を待っています。

**説明:** インストール・プログラムの事前検査ステップで、リモート・サーバーに接続できませんでした。接続が再試行されます。

**ユーザーの処置:** アクションは不要です。インストール・プログラムは、custom.properties ファイルの waiting.time プロパティに指定されている時間待機してから接続を再試行します。

---

**CIYBA0178W** {0} に接続できません。{1} ミリ秒待ってから次の接続試行を行います。

**説明:** システムに接続の問題があります。

**ユーザーの処置:** 接続試行が複数回失敗する場合は、ネットワーク管理者に連絡して、接続の問題を解決してインストールを再試行してください。

---

**CIYBA0179E** トポロジー・プロパティ・ファイルでキー {0} に値が指定されませんでした。

**説明:** インストール・プログラムの事前検査ステップで、ホスト名、ユーザー名、またはパスワードの値をプロパティ・ファイルから取得できませんでした。

**ユーザーの処置:** ホスト名、ユーザー名、およびパスワードが、プロパティ・ファイルに正しく指定されていることを確認してください。

---

**CIYBA0180E** サーバー {0} に対して入力されたユーザー ID には root 特権がありません。

**説明:** インストール・プログラムの事前検査ステップで、示されているサーバーに使用されているアカウントに root 特権がないことが検出されました。

**ユーザーの処置:** サーバーに使用されているユーザー ID を root 特権のあるユーザー ID に変更するか、サーバーに指定されているユーザー ID に root 特権を追加します。

---

**CIYBA0181E** サーバー {0} で使用する root ユーザー ID とパスワードを確認してください。

**説明:** インストール・プログラムの事前検査ステップで、サーバーに使用されているユーザー ID のアクセス権限が不十分であると判別されました。

**ユーザーの処置:** アカウントに十分なアクセス権限があることを確認してください。

**CIYBA0182E** インストール・サーバーから {0} への接続を確認してください。

**説明:** インストール・プログラムの事前検査ステップで、インストール・サーバーとターゲット・サーバーを接続できませんでした。

**ユーザーの処置:** サーバー間の接続を確認してください。追加情報がないか、事前検査ログを確認してください。

**CIYBA0183E** 鍵 {1} の値 {0} が無効です。「EM64T」、AMD64、または S390 である必要があります。

**説明:** 鍵の値は、指定されている値のいずれかでなければなりません。

**ユーザーの処置:** 値を訂正し、インストールを再実行してください。

**CIYBA0184E** 鍵 {1} の値 {0} が有効なホスト名ではありません。

**説明:** インストール・プログラムの事前検査ステップで、提供された値が有効なホスト名でないことが判別されました。

**ユーザーの処置:** ホスト名が正しい形式であることと、正しい値を持っていることを確認してください。

**CIYBA0185E** インストール前提条件の検査がルール {0} で失敗しました。

**説明:** インストール・プログラムの事前検査ステップが、指定されたルールの検査時に失敗しました。

**ユーザーの処置:** 追加メッセージがないか、事前検査ログを調べてください。エラーを訂正し、インストールを再実行してください。

**CIYBA0187E** SSH 鍵ストア「{0}」が指定されましたが、アクセスできませんでした。証明書ベース SSH プロトコルは使用できません。詳細: {1}。

**説明:** インストール・プログラムの事前検査ステップで、ターゲット・サーバーへの接続の試行時に SSH 鍵ストア内で無効なデータが検出されました。

**ユーザーの処置:** メッセージの詳細を確認して、提供された鍵ストアに適切な項目があることを確かめてください。

**CIYBA0190E** トポロジー・ファイルでは、コンポーネント {0} はコンポーネント {1} より前に記述されている必要があります。

**説明:** トポロジー・ファイルが誤って変更されました。前提条件コンポーネントが、そのコンポーネントに依存するコンポーネントより後に記述されています。

**ユーザーの処置:** 従属関係を持つコンポーネントが、依存先のコンポーネントより後に記述されるようにトポロジー・ファイルを変更してください。

**CIYBA0191E** トポロジー・ファイルで、コンポーネント {0} とコンポーネント {1} の間に従属関係があります。これらのコンポーネントを並列にデプロイすることはできません。

**説明:** コンポーネント間に従属関係がある場合、それらのコンポーネントを並列にデプロイすることはできません。例えば、コンポーネント 2 が、コンポーネント 1 の前提条件である場合などです。

**ユーザーの処置:** トポロジー・ファイルの並列スタンプからコンポーネントを除去してください。

**CIYBA0192E** トポロジー・ファイルで、プロパティー {1}、{2} の参照値 {0} が無効です。

**説明:** メッセージに含まれている参照値が、示されているプロパティーで無効です。

**ユーザーの処置:** ID フィールドを使用してプロパティー定義を検索し、このプロパティーに対するすべての参照が正しい値を持つようにしてください。

**CIYBA0193E** トポロジー・ファイルで、コンポーネント {0} に重複する接続 {1} があります。

**説明:** トポロジー・ファイルで、コンポーネントの接続が重複して定義されています。

**ユーザーの処置:** トポロジー・ファイルの重複している接続情報を除去して、インストール・プログラムを再実行してください。



**CIYBA0194E** コンポーネント {0} でプロパティ {0} が重複しています。

**説明:** コンポーネントに重複したプロパティが定義されています。

**ユーザーの処置:** プロパティ・ファイルで、コンポーネントの重複したプロパティを除去してください。

**CIYBA0195E** トポロジー・ファイルのコンポーネント {0} に、無効なプロパティ {0} があります。

**説明:** 指定されたプロパティは、示されているコンポーネントで予期されていませんでした。プロパティがミススペルされていること、またはプロパティ仕様からプロパティが欠落していることが原因と考えられます。

**ユーザーの処置:** 指定されたプロパティをプロパティ・ファイルまたはトポロジーに追加してください。プロパティがミススペルされていた場合は、ミススペルを訂正してください。トポロジー・ファイルまたは仕様プロパティ・ファイルを訂正して、インストールを再開してください。

**CIYBA0196E** コンポーネント {1} にプロパティ {0} がありません。

**説明:** コンポーネントには、示されているプロパティが必要です。プロパティがミススペルされていること、またはプロパティ仕様ファイルからプロパティが欠落していることがエラーの原因と考えられます。

**ユーザーの処置:** プロパティを仕様プロパティ・ファイルまたはトポロジーに追加してください。ミススペルがエラーの原因である場合は、ミススペルを訂正してください。インストールを再開してください。

**CIYBA0197E** コンポーネント {1} に無効なコンポーネント・タイプ {1} が指定されています。

**説明:** コンポーネントに無効なコンポーネント・タイプが指定されていました。

**ユーザーの処置:** コンポーネントの仕様ファイルに、コンポーネント・タイプが含まれていることを確認してください。コンポーネント仕様ファイルは、インストール・サーバーの `install_home/spec/component` サブディレクトリにあります。

**CIYBA0198E** コンポーネント {1} では接続 {0} は無効です。

**説明:** このコンポーネントでは、定義された接続は無効です。

**ユーザーの処置:** コンポーネントのトポロジー・ファイルで接続のスペルを確認して、ミススペルがないようにしてください。

**CIYBA0199E** {0} 接続がコンポーネント {1} にありませんでした。

**説明:** 示されているコンポーネントに接続が定義されていません。

**ユーザーの処置:** コンポーネント仕様ファイルを確認して、接続情報が含まれるようにしてください。

**CIYBA0200E** {0} の接続情報が存在しません。

**説明:** 示されているコンポーネントの接続 ID が欠落しています。

**ユーザーの処置:** 接続 ID がトポロジー・ファイルに指定されていることを確認してください。接続 ID が正しくスペルされていることと、その接続 ID の関連コンポーネントを定義するトポロジー・ファイルのスタンザを参照していることを確認してください。

**CIYBA0201E** リモート・サーバー {0} に接続できません。

**説明:** インストール・プログラムが、示されているサーバーへの接続の問題を検出しました。

**ユーザーの処置:** サーバー間に接続の問題がないことを確認してください。インストール・プログラムの事前検査ステップを実行して、接続の問題があれば解決してください。

**CIYBA0202E** サーバー {0} に対するユーザー名またはパスワードが無効です。

**説明:** インストール・プログラムが、示されているサーバーの資格情報が無効であることを検出しました。

**ユーザーの処置:** トポロジー・ファイルでサーバー資格情報が正しいことを確認してください。

**CIYBA0203E** ファイル {0} が存在しません。

**説明:** プロパティ・ファイルのロードを試行してエラーが返されました。

**ユーザーの処置:** プロパティ・ファイルへのパスが正

しいことと、ファイルが存在することを確認してください。

---

**CIYBA0204E** ファイル {0} の読み取り/書き込みを実行できません。

**説明:** インストール・プログラムはプロパティ・ファイルのロードを試行しましたが、エラーが返されました。

**ユーザーの処置:** プロパティ・ファイルのパスが正しいことと、示されているファイルが存在することを確認してください。

---

**CIYBA0205E** {1} にディレクトリー {0} を作成できません。

**説明:** インストール・プログラムは、リモート・サーバーにディレクトリーを作成できませんでした。

**ユーザーの処置:** リモート・サーバーに十分なスペースがあること、またインストール・プログラムで使用されるユーザー ID にディレクトリーを作成するための十分なアクセス権と適切な権限があることを確認してください。

---

**CIYBA0206E** サーバー {2} のリモート・ディレクトリー {1} にファイル {0} をアップロードできません。

**説明:** インストール・プログラムは、リモート・サーバーの示されているディレクトリーにファイルをコピーできませんでした。

**ユーザーの処置:** リモート・サーバーに十分なスペースがあること、またインストール・プログラムで使用されるユーザー ID に、リモート・サーバーにファイルを書き込むための十分なアクセス権と適切な権限があることを確認してください。

---

**CIYBA0207E** {0} のイメージが定義されていません。

**説明:** インストール・プログラムは、プロパティ・ファイルのイメージ・データを取得できませんでした。

**ユーザーの処置:** プロパティ・ファイルに、データ・コンポーネントが入っているイメージ・フィールドが含まれていることを確認してください。

---

**CIYBA0208E** リモート・サーバー {1} にコンポーネント {0} のイメージをアップロードできません。

**説明:** インストール・プログラムは、リモート・サーバーのディレクトリーにイメージ・ファイルをコピーできませんでした。

**ユーザーの処置:** リモート・サーバーに十分なスペースがあること、またインストール・プログラムで使用されるユーザー ID に、リモート・サーバーのディレクトリーに書き込むための十分なアクセス権と適切な権限があることを確認してください。また、リモート・ディレクトリー名が正しいことも確認してください。

---

**CIYBA0209I** ホスト名: {0}。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0210I** OS タイプ = {0}、OS ビット = {1}、CPU アーキテクチャー = {2}。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0211I** リモート・パス: {0}。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0212I** ローカル・パス: {0}。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0213E** リモート・サーバー {1} からファイル {0} をダウンロードできません。

**説明:** インストール・プログラムは、リモート・ディレクトリー・サーバーからローカル・サーバーにイメージ・ファイルをコピーできませんでした。

**ユーザーの処置:** ローカル・サーバーに十分なスペースがあること、またインストール・プログラムで使用されるユーザー ID に、ディレクトリーに書き込むための十分なアクセス権と適切な権限があることを確認してください。また、ローカル・ディレクトリー名とリモート・ディレクトリー名が正しいことも確認してください。

---

**CIYBA0214E** ファイル {0} をダウンロードします。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0215I** コマンド: {0}。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0216I コマンド出口コード: {0}。**

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0217I コマンド出力: {0}。**

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0218E コマンドが戻りコード {0} で失敗しました。**

**説明:** コマンドは正常に完了しませんでした。

**ユーザーの処置:** 詳しくは、ログ・ファイルを確認してください。

---

**CIYBA0219I ファイル {0} をアップロードします。**

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0220I ローカル・イメージ・ディレクトリー: {0}。**

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0221I リモート・イメージ・ディレクトリー: {0}。**

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0222E リモート・イメージ {0} は既に存在しません。**

**説明:** このファイルは既にターゲット・サーバーに存在します。インストール・プロセスには、メディアをターゲット・サーバーに転送することが含まれています。このメッセージは、必要なイメージが既に転送されていることを示しています。

**ユーザーの処置:** このメッセージは、前のインストール試行のメディアがターゲット・サーバーにまだ存在していることを示しています。ユーザーが新しいインストールの開始を意図している場合は、メディアをもう一度アップロードできるよう、そのメディアを削除する必要があります。

---

**CIYBA0223E サーバー {0} でコマンドを起動できません。**

**説明:** インストール・プログラムは、リモート・サーバーからローカル・サーバーに対して **IOC** コマンドを実行できませんでした。

**ユーザーの処置:** ローカル・サーバーとリモート・サーバーの間の接続を確認してください。インストール・プログラムで使用されるユーザー ID に、コマンドを実行するための十分なアクセス権と適切な権限があることを確認してください。

---

**CIYBA0224E サーバー {1} のフォルダー {0} からバックアップ・ファイルを取得します。**

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0225E サーバー {1} のフォルダー {0} からバックアップ・ファイルを取得できません。**

**説明:** インストール・プログラムは、リモート・バックアップ・フォルダーからローカル・フォルダーにファイルを取り出すことができませんでした。

**ユーザーの処置:** ローカル・サーバーとリモート・サーバーの間の接続を確認してください。インストール・プログラムで使用されるユーザー ID に、フォルダーにアクセスするための十分なアクセス権と適切な権限があることを確認してください。

---

**CIYBA0226E サーバー {1} にバックアップ・フォルダー {0} が存在しません。**

**説明:** インストール・プログラムは、リモート・バックアップ・フォルダーからローカル・フォルダーにファイルを取り出すことができませんでした。

**ユーザーの処置:** リモート・ディレクトリーとフォルダーが存在することを確認してください。

---

**CIYBA0227E ID およびパス属性に値が指定されている必要があります。**

**説明:** インストール時に、コンポーネント ID とパス属性を識別できませんでした。

**ユーザーの処置:** コンポーネント ID とパス引数が、タスク引数内で提供されていることを確認してください。

---

---

**CIYBA0228I** 実行コマンド: {0}。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0229E** ターゲット・ディレクトリー {0} のディスク・スペースが不足しています。

**説明:** インストール・プログラムは、ターゲット・ディレクトリー内で十分なスペースを検出できませんでした。

**ユーザーの処置:** 示されているディレクトリーが、十分な割り振りスペースを持っていること、またインストール・プログラムで使用されるユーザーID によってアクセス可能であることを確認してください。

---

**CIYBA0230I** IOC コマンド行バージョン: {0}

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0231I** トポロジー「{0}」が正常にインポートされました。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0232E** ../topology フォルダー下にトポロジー名「{0}」が見つかりません。

**説明:** インストール・プログラムは、示されているトポロジーを ../topology フォルダー内で検出できませんでした。

**ユーザーの処置:** トポロジー・ファイルが ../topology フォルダーに存在すること、また有効な XML 形式になっていることを確認してください。

---

**CIYBA0233I** 現在のトポロジーは「{0}」です。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0234E** ANT\_HOME が設定されていないか、設定が誤っています。ANT\_HOME を設定してください。

**説明:** インストール・プログラムが、ANT\_HOME 環境変数で問題を検出しました。

**ユーザーの処置:** ANT\_HOME 変数が、有効な ANT バージョンに設定されていることを確認してください。

---



---

**CIYBA0237E** コンポーネント ID 「{0}」は無効です。

**説明:** インストール・プログラムが、トポロジー・ファイル内で誤ったコンポーネント ID を検出しました。

**ユーザーの処置:** トポロジー・ファイル内で、コンポーネント ID が存在すること、また正しい名前になっていることを確認してください。

---

**CIYBA0238E** コンポーネント ID 「{1}」に対するアクション「{0}」は無効です。

**説明:** 示されているアクションは、トポロジー・ファイル内の現在のコンポーネントでは正しくありません。

**ユーザーの処置:** トポロジー・ファイルを調べて、定義されているアクションがコンポーネントで適切なものとなるようにしてください。

---

**CIYBA0239E** より詳細な操作メッセージについては、{0} を確認してください。

**説明:** コマンドは正常に完了しませんでした。

**ユーザーの処置:** 取るべきアクションについては、{0} で示されているログ・ファイルを確認してください。

---

**CIYBA0240I** コマンドが正常に完了しました。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

---

**CIYBA0241E** コマンドが失敗しました:

**説明:** 表示されているコマンドが失敗しました。

**ユーザーの処置:** 取るべきアクションは、失敗したコマンドによって異なります。コマンドとログを調べて、失敗の原因を判別してください。

---

**CIYBA0242E** パラメーター「{0}」から「.xml」を除去してください。

**説明:** 示されているパラメーターにファイル拡張子.xml が含まれています。

**ユーザーの処置:** XML ファイル名パラメーターに、.xml 拡張子が含まれていてはなりません。パラメーターから.xml を除去して、コマンドを再実行してください。

---

**CIYBA0243E** IOP\_CIPHER\_ALG または IOP\_CIPHER\_KEYSIZE 環境変数の設定が誤っています。適切な JCE 準拠値に設定してください。

---

**説明:** インストール・プログラムは、暗号化に使用される暗号の正しい値を識別できませんでした。

**ユーザーの処置:** CIPHER\_ALG および IOP\_CIPHER\_KEYSIZE 環境値が正しく設定されていることを確認してください。

**CIYBA0244E** 「{0}」は無効なパラメーターです。

**説明:** 示されているパラメーターは、有効なパラメーターではありません。

**ユーザーの処置:** パラメーターを除去するか訂正して、コマンドを再試行してください。

**CIYBA0245E** 「-{0}」にパラメーターがありません。

**説明:** 示されているパラメーターは必須ですが、コマンドで欠落しています。

**ユーザーの処置:** 欠落しているパラメーターを指定して、コマンドを再実行してください。

**CIYBA0249I** 操作スクリプトを準備します。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0250I** 操作が完了しました。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0251I** 操作シーケンスが開始されました。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0252I** 操作シーケンスが完了しました。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0253I** コンポーネントの [{0}] イメージをホスト [{1}] にアップロードします。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0254I** コンポーネント [{0}] をホスト [{1}] にインストールします。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0255I** コンポーネント [{0}] をホスト [{1}] からアンインストールします。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0256I** ホスト [{1}] でコンポーネント [{0}] を始動します。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0257I** ホスト [{1}] でコンポーネント [{0}] を停止します。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0258I** ホスト [{1}] でコンポーネント [{0}] を伝搬します。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0259I OK**

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0261I** {0} 個のタスクが実行中です。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0262I** 合計 {0} 個のタスクが実行されます。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0263I** ホスト [{1}] でコンポーネント [{0}] をバックアップします。

**説明:** これは単なる通知メッセージです。

**ユーザーの処置:** アクションは不要です。

**CIYBA0264E** ログ構成ファイル {0} をロードできません。

**説明:** ロギング機能が、ロギング構成パラメーターを含むプロパティ・ファイルを検出できません。

**ユーザーの処置:** インストール・パッケージが完全に解



## CIYBA0265E • CIYBA0274E

凍されていること、またこのパッケージがインストール・プログラムを実行するユーザー ID からアクセス可能なファイル・システムに置かれていることを確認してください。

---

**CIYBA0265E ログのファイル・ハンドラーを作成できません。**

**説明:** ログ機能、システム・ファイル・ハンドラーを使用してファイルを開こうとしましたが、開けませんでした。

**ユーザーの処置:** システム管理者に、システムで使用可能なファイル・ハンドラーの数を確認するように依頼してください。インストール・パッケージが解凍されたファイル・システムが破損していないことを確認してください。

---

**CIYBA0266E 必須 RPM パッケージ {0} が {1} サーバーにインストールされていません。**

**説明:** 示されている RPM パッケージがサーバーにインストールされていません。

**ユーザーの処置:** サポートされる RPM パッケージをサーバーにインストールしてください。

---

**CIYBA0267E {1} サーバーのディスク・スペースが不十分です。 {0} のディスク・スペースが必要です。**

**説明:** サーバーのディスク・スペースが十分でないか、サーバーがディスク・スペースのシステム要件を満たしていません。

**ユーザーの処置:** 最小スペース要件が満たされるように、ファイルを削除してサーバー上のスペースを使用可能にしてください。

---

**CIYBA0268E {1} サーバーのメモリーが不十分です。 {0} GB のメモリーが必要です。**

**説明:** 示されているサーバーの RAM が不十分です。サーバーは、最小 RAM のシステム要件を満たしていません。

**ユーザーの処置:** サーバーに RAM を追加してください。

---

**CIYBA0269E サーバー {1} で {0} ディレクトリーを作成できません。このディレクトリーは既に存在します。**

**説明:** 指定されたディレクトリーは、サーバーに既に存在します。

**ユーザーの処置:** サーバー上のこのディレクトリーを除去してください。

---

**CIYBA0270E TCP IP ポート {0} は、サーバー {1} で既に使用されています。これは必須ポートであり、インストール前に使用可能な状態にしておく必要があります。**

**説明:** プログラムまたはプロセスは、サーバー上の必須 TCP/IP ポートを使用するよう既に構成されています。

**ユーザーの処置:** 必須ポートを使用できるようにサーバーを再構成してください。インストールを再実行してください。

---

**CIYBA0271E サーバー {1} に、必要な完全修飾ホスト名が設定されていません。必要な FQH は {0} です。**

**説明:** サーバーに、必要な完全修飾ホスト名が設定されていません。

**ユーザーの処置:** IBM Installation Manager を使用したインストールの場合は、サーバーの完全修飾ホスト名を入力してください。ステップ・バイ・ステップのインストールの場合は、トポロジーのプロパティ・ファイルの SERVERS セクションに完全修飾ホスト名を入力してください。エラー・メッセージにリストされているサーバーを訂正します。

---

**CIYBA0272E サーバー {1} からサーバー {0} へのネットワーク接続が切断されています。**

**説明:** 示されている 2 つのサーバー間にネットワーク接続がありません。

**ユーザーの処置:** サーバー間の接続を確認してください。問題が解決しない場合は、システム・ネットワーク管理者に連絡してください。

---

**CIYBA0273E サーバー {0} で、サポートされない SELinux が実行されています。**

**説明:** SELinux は、IBM Intelligent Operations Center ではサポートされていません。

**ユーザーの処置:** サポートされる Linux バージョンをインストールしてください。

---

**CIYBA0274E サーバー {0} でアクティブなファイアウォールが検出されました。インストール前に、すべてのファイアウォールを無効にしておく必要があります。**

**説明:** サーバーのファイアウォールがアクティブになっています。



**ユーザーの処置:** インストール処理中は、サーバーのファイアウォールを無効にしてください。

---

**CIYBA0275E** サーバー {0} の DNS 項目が見つかりません。 IP またはホスト名による DNS 参照が失敗しました。

**説明:** サーバーが DNS で正しく構成されていないか、DNS が正しく機能していません。 IP アドレスまたはホスト名による DNS 参照コマンドがサーバーで失敗しました。

**ユーザーの処置:** このサーバーのシステム・ネットワーク管理者に連絡して、DNS の DNS 項目を訂正してください。

---

**CIYBA0276E** サーバー {1} のシステム設定が、インストール要件を満たしていません。 オープン・ファイルの最大数 [unlimit] が {0} より小さいです。

**説明:** オープン・ファイルの最大数のシステム設定が、インストール要件を満たしていません。

**ユーザーの処置:** ulimit 設定を示されている値に変更する必要があります。

---

**CIYBA0277E** 検出された Linux 要求が、インストール要件を満たしていません。 必要なリリースは {0} です。

**説明:** 示されているサーバーにインストールされている Linux はサポートされていません。

**ユーザーの処置:** サポートされる Linux バージョンをインストールしてください。

---

**CIYBA0278E** 検出された Linux ディストリビューションが要件を満たしていません。 必要なディストリビューションは {0} です。

**説明:** インストールされている Linux はサポートされていません。

**ユーザーの処置:** サポートされる Linux ディストリビューションをインストールしてください。

---

**CIYBA0279E** サーバー {4} で WebSphere Application Server プロファイル {0} が開始されていないか、アカウントまたはパスワードが無効です。

**説明:** WebSphere Application Server プロファイルが開始されていないか、無効な資格情報を使用して開始しようとした。

**ユーザーの処置:** 正しいユーザー ID とパスワードを使用して、WebSphere Application Server プロファイルを開始してください。

---

**CIYBA0281E** サーバー {0} で IPv6 が有効になっていません。 インストール前に、サーバーで IPv6 を有効にしてください。

**説明:** 示されているサーバーで IPv6 が構成されていません。

**ユーザーの処置:** 示されているサーバーで IPv6 を有効にしてください。

---

**CIYBA0282E** メディア・サーバーの {0} ディレクトリーにある一部のファイルが破損しています。

**説明:** すべてのインストール・ファイルには、インストール前に検証される必要がある MD5 チェックサムがあります。 示されているディレクトリーにある一部のファイルの MD5 チェックサムが、有効な MD5 チェックサムではありません。

**ユーザーの処置:** インストール・パッケージをもう一度解凍するか、このディレクトリーにファイルを再コピーしてください。

---

**CIYBA0283E** サーバー {0} で SSH が正しく構成されていません。 SSH を使用したパスワード認証が必要ですが、サーバーで構成されていません。

**説明:** 示されているサーバーの SSH 構成が正しくありません。

**ユーザーの処置:** /etc/ssh/sshd\_config ファイルを、以下のように再構成してください。

- すべての AllowUsers ステートメントを除去します。
- PermitRootLogin に YES を指定します。
- Password Authentication に YES を指定します。

この変更により、root ユーザーのみが、パスワード認証による SSH を使用してサーバーにアクセスできるようになります。

---

**CIYBA0284E** シンボリック [ソフト] リンクとなる {0} が検出されました。 シンボリック・リンクは許可されません。

**説明:** ファイルまたはディレクトリーへのシンボリック・リンクまたはソフト・リンクはサポートされていません。

**ユーザーの処置:** シンボリック・リンクを除去して、直

接パスまたはファイル名を指定してください。

---

**CIYBA0285E Tivoli Directory Server インスタンス {0} がサーバー {1} で始動されていません。**

**説明:** 示されている Tivoli Directory Server インスタンスを始動する必要があります。

**ユーザーの処置:** Tivoli Directory Server を始動してください。

---

**CIYBA0286E IBM DB2 インスタンス {0} がサーバー {1} で始動されていません。**

**説明:** 示されている DB2 インスタンスが始動されていません。

**ユーザーの処置:** DB2 インスタンスを始動してください。

---

**CIYBA0287E プロファイル {0} の WebSphere Application Server {1} がサーバー {2} で始動されていません。**

**説明:** 示されている WebSphere Application Server プロファイルが、示されているサーバーで始動されていません。

**ユーザーの処置:** WebSphere Application Server プロファイルを始動してください。

---

**CIYBA0288E サーバー {0} の「localhost」が 127.0.0.1 にマップされていません。**

**説明:** 各サーバーのホスト・ファイルで、localhost 項目が 127.0.0.1 にマップされている必要があります。

**ユーザーの処置:** サーバーのホスト・ファイルを更新して、localhost 値を 127.0.0.1 にマップしてください。

---

**CIYBA0289E サーバー {0} の CPU リソースが不十分です。サーバーの CPU リソース数は {1} です。**

**説明:** サーバーの CPU リソースが不十分で、要件を満たしていません。

**ユーザーの処置:** 示されているサーバーに CPU リソースを追加してください。

---

**CIYBA0301E テストを実行するためのボタンがクリックされましたが、一致するプロパティがプロパティ・ファイル内に見つかりませんでした。**

**説明:** テストのためのプロパティが、プロパティ・

ファイル内で見つかりませんでした。

**ユーザーの処置:** 「リセット」をクリックします。これにより、変更が行われた場合に、プログラムが現在のプロパティ・ファイルを読み取るようになります。テストを再試行してください。

---

**CIYBA0302E すべてのテストには特定のプロパティが必要です。class は、その 1 つです。パラメーター: {0}: クラス名 {1}: メソッド名 {2}: シーケンス番号**

**説明:** テスト定義に class プロパティがありません。

**ユーザーの処置:** プロパティ・ファイル内でシーケンス番号を検索します。テスト用の class プロパティを追加します。これはテストのクラス名です。通常、これはリモート実行エージェントのクラス名です (実行のためにテスト要求を IopCatRemoteResponder に転送するコード)。

例えば、以下のようなものがあります。

```
0070.classname=com.ibm.iop.cat.fw.remote.IopCatRemoter
```

---

**CIYBA0303E すべてのテストには特定のプロパティが必要です。表示ラベルは、その 1 つです。パラメーター: {0}: クラス名 {1}: メソッド名 {2}: シーケンス番号**

**説明:** テスト定義に表示ラベルがありません。

**ユーザーの処置:** プロパティ・ファイル内でシーケンス番号を検索します。テスト用の displaylabel プロパティを追加します。これがボタンに表示されるテキストです

---

**CIYBA0304E テストを実行するためのボタンがクリックされましたが、一致するテストがプロパティ・ファイル内に見つかりませんでした。**

**説明:** 現在ロードされているプロパティ・ファイルは、要求されたテストを定義していません。

**ユーザーの処置:** 「リセット」をクリックします。現在のプロパティ・ファイルが再ロードされます。

---

**CIYBA0305E テストを実行するためのボタンが押されましたが、テスト用の構成情報が見つかりませんでした。**

**説明:** 構成情報がテストで使用できません。

**ユーザーの処置:** 「リセット」をクリックします。現在のプロパティ・ファイルが再ロードされます。

**CIYBA0306E** クラスによって指定されているコードが見つかりませんでした。パラメーター: {0}: クラス名 (未検出)

**説明:** classname がプロパティ・ファイル内で正しく指定されていないか、コードが見つかりませんでした。

**ユーザーの処置:** IopCatRemoteResponder アプリケーションの共有ライブラリーを調べて、1 つ以上の共有ライブラリーが欠落していないか、または指定されていないかどうかを確認してください。

**CIYBA0307E** 共通変数はすべてのテストに適用されません。共通変数を使用して、名前、クラス、またはデバッグを設定することはできません。パラメーター: {0}: クラス名 {1}: メソッド名 {2}: プロパティ・キー・ストリング

**説明:** Common を使用して、name、class、または debug が設定されています。

**ユーザーの処置:** キーを探して、問題の行を除去してください。例えば、すべてのテストに同じ名前を付けるために使用された common.name などです。

**CIYBA0308E** クラス {0}、メソッド {1} で例外が発生しました。詳細 {2}

**説明:** 例外が発生しました。

**ユーザーの処置:** 例外ストリングを調べて、テストが失敗した理由を判別してください。これは通常のテスト障害と考えられます。例えば、「接続が拒否されました (Connection refused)」は、通常、指定のポートで listen していたプログラムがなかったため、サービスが実行されていないことを意味します。

**CIYBA0309E** {0}、{1}() - テスト [{2}] - 例外: {3}

**説明:** 示されているテストで実行時例外が発生しました。

**ユーザーの処置:** 詳細については、エラー・メッセージを確認してください。

**CIYBA0310E** このテストの実行中に予期しない例外が発生しました。

**説明:** 予期しない例外が発生しました。

**ユーザーの処置:** 追加の詳細については、他の例外を確認してください。

**CIYBA0311I** このストリングは内部診断エコー・テストから返されました。パラメーター {0}: テストへの入力プロパティ。

**説明:** テストの入力プロパティを表示しています。

**ユーザーの処置:** これは通常のメッセージであり、エラーを示しているわけではありません。

**CIYBA0312E** Web テストで、予期される HTTP 応答コードを受信しました (200 番台またはプロパティ expectedRcode で指定された値)。パラメーター: {0}: クラス名

**説明:** テストが成功したことを示しています。

**ユーザーの処置:** アクションは不要です。

**CIYBA0313E** Web テストで、予期される HTTP 応答コードを受信されませんでした (200 番台またはプロパティ expectedRcode で指定された値)。パラメーター: {0}: クラス名 {1}: HTTP 応答コード

**説明:** 予期しない HTTP 応答コードを受け取りました。

**ユーザーの処置:** ブラウザーまたは wget コマンドを使用して、hosturl プロパティで指定されている URL を調べてください。

**CIYBA0314E** テスト応答のストリング表記。パラメーター: {0}: 応答コード {1}: 応答テキスト {2}: テスト固有の追加テキスト

**説明:** このメッセージは、テスト応答をストリングとして返します。

**ユーザーの処置:** アクションは不要です。

**CIYBA0315E** すべてのテストでプロパティが必要です。このテストにプロパティが渡されませんでした。

**説明:** テストの呼び出しでプロパティがありませんでした。

**ユーザーの処置:** プロパティはフレームワークによって渡されるため、このメッセージは表示されないはずですが、IBM ソフトウェア・サポートに連絡してください。

**CIYBA0320E** テキスト・プロパティーで、予想されるストリングが検出されませんでした。クラス名 {0}、出力テキスト {1}

**説明:** SSH テストはサーバーにログインし、コマンドを実行し、予想されるストリングがコマンドからの出力にないか検査します。このテストのプロパティーで、予想されるストリングが指定されていませんでした。

**ユーザーの処置:** テストの expected キーを確認してください。プロパティーを追加または変更して、commmands プロパティーに指定されているコマンドの出力に含まれると予想されるストリングを指定してください。

**CIYBA0322E** 予想されるストリングが出力で検出されませんでした。クラス名 {0}、出力テキスト {1}

**説明:** SSH テストはサーバーにログオンし、コマンドを実行し、予想されるストリングがコマンドからの出力にないか検査します。予想されるストリングが出力で検出されませんでした。

**ユーザーの処置:** テストと出力テキストの expected キーを確認してください。これはテストが失敗したことを示している可能性があります。出力テキストに「キーボード対話は許可されていません (keyboard interactive not allowed)」が含まれている場合は、リモート・サーバーにログオンするために使用されたユーザー ID またはパスワードが間違っている可能性があります。テストの user、password、および hostname の各プロパティーを確認してください。パスワードは、鍵ストアのパスワードの別名です。

**CIYBA0323E** 予期しない例外がクラス名 {0} で発生しました。例外: {1}

**説明:** 予期しない例外が発生しました。

**ユーザーの処置:** 出力テキストに「キーボード対話は許可されていません (keyboard interactive not allowed)」が含まれている場合は、リモート・サーバーにログオンするために使用されたユーザー ID またはパスワードが間違っている可能性があります。テストの user、password、および hostname の各プロパティーを確認してください。パスワードは、鍵ストアのパスワードの別名です。

**CIYBA0340E** テスト実行エージェント (IopCatRemoteResponder) が入力 JSON データを解析できませんでした。パラメーター: {0}: クラス名 {1}: メソッド名 {2}: POST データ

**説明:** ユーザー・インターフェースおよびテスト実行エージェントは、JSON を使用して通信します。このエラーは、テスト実行エージェント (IopCatRemoteResponder) が、入力 JSON データを解析できなかったことを意味します。

**ユーザーの処置:** POST データを調べて、正しい JSON 形式になっていることを確認してください。

**CIYBA0341E** テストの実行中に例外が発生しました。パラメーター: {0}: クラス名 {1}: メソッド名 {2}: 例外ストリング

**説明:** テストの実行中に例外が発生しました。

**ユーザーの処置:** 例外ストリングを調べて、テストが失敗した理由を判別してください。これは通常のテスト障害と考えられます。例えば、「接続が拒否されました」の場合は、通常、ポートで listen していたプログラムがなかったため、サービスが実行されていないことを意味します。

**CIYBA0342E** テスト実行エージェント (IopCatRemoteResponder) がユーザー・インターフェースに応答を返信できませんでした。パラメーター: {0}: クラス名 {1}: メソッド名 {2}: 例外ストリング

**説明:** ユーザー・インターフェースおよびテスト実行エージェントは、JSON を使用して通信します。このエラーは、テスト実行エージェント (IopCatRemoteResponder) が、ユーザー・インターフェースに応答を返信できなかったことを意味します。

**ユーザーの処置:** 例外ストリングを調べて、応答を送信できなかった理由を判別してください。このエラーは、テストに要した時間が長すぎたため、ユーザー・インターフェースがもはや待機していない場合に発生することがあります。

**CIYBA0343E** 予想されるキー接頭部がありません。パラメーター: {0}: クラス名 {1}: メソッド名 {2}: プロパティー・キー・ストリング

**説明:** 特定のテストのすべてのプロパティーには、接頭部として同じ数値が付きます。これにより、プロパティー・ファイルは位置で判断されなくなるため、グローバル化が可能になります。

**ユーザーの処置:** プロパティー・ファイル内でキーを検索して、適切な接頭部を追加してください。例えば、以下は誤りです。

```
classname      = com.ibm.iop.cat.fw.remote.IopCatRemoter
0050.rhosturl   = https://$[APP_HOSTNAME_1]:9443/IopCatRemoteResponder/IopCatRemoteResponder
0050.remoteclassname= com.ibm.iop.cat.fw.Echo
0050.displaylabel = Internal Diagnostic [Echo REST remoteds]
0050.comment    = Self diagnostic CAT check. Tests link between to CAT modules.
0050.fullinfoage = cct_echo_rest_remoteds_test.html
```



以下のようにする必要があります。

```
0050.classname      = com.ibm.iop.cat.fw.remote.IopCatRemote
0050.rhosturl       = https://$!APP_HOSTNAME:$!9443/IopCatRemoteResponder/IopCatRemoteResponder
0050.remoteclassname = com.ibm.iop.cat.fw.Echo
0050.displaylabel   = Internal diagnostic (Echo REST remoted)
0050.comment        = Self diagnostic CAT check. Tests link between to CAT modules.
0050.failinfopage   = cct_echo_rest_remoted_test.html
```

**CIYBA0345E 無効なキー - キー接頭部が数値ではありません。パラメーター: {0}: クラス名 {1}: メソッド名 {2}: シーケンス番号 CCT\_RESULTS\_INFO = {0},{1}0 - クラス: {2} 結果 - 応答コード [{3}] 応答テキスト [{4}]**

**説明:** すべてのテストには、特定のテストのすべてのプロパティをグループ化する数値接頭部が必要です。

指定した接頭部が数値ではありません。

**ユーザーの処置:** プロパティ・ファイル内でシーケンス番号を検索します。接頭部を数値に変更し、この同じ接頭部をテストの残りのプロパティに使用してください。

**CIYBA0347E 例外が発生しました。パラメーター: {0}: クラス名 {1}: メソッド名 {2}: 例外ストリング**

**説明:** 例外が発生しました。

**ユーザーの処置:** 例外ストリングを調べて、テストが失敗した理由を判別してください。これは通常のテスト障害と考えられます。例えば、「接続が拒否されました」の場合は、通常、ポートで listen していたプログラムがなかったため、サービスが実行されていないことを意味します。

**CIYBA0348E テストを実行するためのボタンがクリックされましたが、一致するプロパティがプロパティ・ファイル内に見つかりませんでした。**

**説明:** テストでプロパティが見つかりませんでした。プロパティ・ファイルが変更された可能性があります。

**ユーザーの処置:** 「リセット」をクリックします。現在のプロパティ・ファイルが再ロードされます。

**CIYBA0349E クラスによって指定されているコードが見つかりませんでした。パラメーター: {0}: クラス名 (未検出)**

**説明:** classname がプロパティ・ファイル内で正しく指定されていないか、コードが見つかりませんでした。

**ユーザーの処置:** IopCatRemoteResponder の共有ライブラリーを調べて、1 つ以上の共有ライブラリーが欠落していないかどうかを確認してください。

**CIYBA0401E IOPMGMT プロパティ・テンプレート・ファイル名が指定されなかったか、正しくありませんでした。**

**説明:** IOPMGMT プロパティ・テンプレート・ファイルのパラメーターがありません。

**ユーザーの処置:** IOPMGMT プロパティ・ファイルの正しい名前を入力してください。

**CIYBA0402E トポロジー・プロパティ・ファイル名が指定されなかったか、正しくありませんでした。**

**説明:** トポロジー・プロパティ・ファイルのパラメーターがないか、正しくありません。

**ユーザーの処置:** トポロジー・プロパティ・ファイルの正しい名前を入力してください。

**CIYBA0403E IOPMGMT プロパティ・テンプレート・ファイル名が指定されなかったか、正しくありませんでした。**

**説明:** IOPMGMT プロパティ・テンプレート・ファイルを指定しているパラメーターがありません。

**ユーザーの処置:** トポロジー・プロパティ・ファイルの正しいファイル名を入力してください。

**CIYBA0404E トポロジー・プロパティ・ファイルが見つかりません。**

**説明:** トポロジー・プロパティ・ファイルが見つかりません。

**ユーザーの処置:** トポロジー・プロパティ・ファイルが、インストール・サーバーの *install\_home/topology* ディレクトリーに配置されていることを確認してください。

**CIYBA0405E トポロジー・ファイルに次のプロパティのパスワードがありません:**

**説明:** 示されているトポロジー・プロパティ・ファイルでパスワードが見つかりませんでした。

**ユーザーの処置:** トポロジー・ファイルのパスワードが必要です。トポロジーのパスワードを入力してください。

**CIYBA0501E Base Architecture Cyber Hygiene メディアの必須パラメーターがありません。**

**説明:** IBM Intelligent Operations Center Cyber Hygiene メディアの必須パラメーターがありません。

## CIYBA0502E • CIYUI0004E

**ユーザーの処置:** Cyber Hygiene スクリプトに、インストール・メディアのロケーションへの正しいパスが指定されていることを確認してください。

---

**CIYBA0502E トポロジー・プロパティ・ファイルの必須パラメーターがありません。**

**説明:** トポロジー・プロパティ・ファイルのファイル名パラメーターがありません。

**ユーザーの処置:** トポロジー・プロパティ・ファイルの正しいファイル名を指定してください。

---

**CIYBA0503E Base Architecture Cyber Hygiene 宛先ディレクトリーの必須パラメーターがありません。**

**説明:** Cyber Hygiene 宛先ディレクトリーの必須パラメーターがありません。

**ユーザーの処置:** 正しい宛先ディレクトリーを指定してください。

---

**CIYCC0002E 以下の構成エラーを訂正してください:**  
{0}

**説明:** 「共有セッションの編集 (Edit Shared Sessions)」構成ページにエラーがあります。エラーは {0} によって示されています。

**ユーザーの処置:** エラーを訂正して要求を再試行してください。

---

**CIYCC0005E イベントを送信できません。 イベントの送信を再試行してください。 問題が解決しない場合は、管理者またはヘルプ・デスクに連絡してください。**

**説明:** ユーザーがイベントの更新、エスカレート、または取り消しを試行したときに、パブリッシャー・サブレット・エラーが発生しました。

**ユーザーの処置:** 管理者またはヘルプ・デスクがパブリッシャー・サブレット・エラーを解決するようにしてください。

---

**CIYCC0006W レコードが別のユーザーによって更新されました。 ページを最新表示して、更新されたレコードを取り出してください。**

**説明:** ユーザーによって要求された更新が、サーバー上で発生した別の変更と競合しています。これは、2人のユーザーがアクティビティの状態を同時に変更しようとする場合に発生することがあります。

**ユーザーの処置:** ページを最新表示してください。 も

う一方のユーザーによって行われた更新が表示されません。その後、必要な変更を行ってください。

---

**CIYUI0001E 指定された JSON 配列にエラーが含まれており、構文解析できません。**

**説明:** スクリプトを入力するウィンドウにユーザーが JSON ストリングを入力しましたが、ストリングに構文エラーがあり、構文解析できませんでした。

**ユーザーの処置:** JSON ストリングを訂正してください。

---

**CIYUI0002E イベントが見つかりません。 イベントのプロパティを表示できません。**

**説明:** データベース内でプロパティが見つからなかったため、イベントのプロパティを表示するという要求が失敗しました。

**ユーザーの処置:** ページを最新表示して、要求を再試行してください。

---

**CIYUI0004E ロケーション・マップ・マネージャー・データ送信エラー。**

**説明:** ロケーション・マップ・マネージャー・データの設定中に問題が発生しました。

**ユーザーの処置:** 詳しくは、追加のメッセージを参照してください。

「種別」タブの追加のメッセージ。

**データ送信エラー**

新しい種別がデータベースに入力されていません。

「ロケーション・マップ」タブの追加のメッセージ。

**データ送信エラー**

新しいロケーション・マップがデータベースに入力されていません。

「エリア」タブの追加のメッセージ。

**入力されたエリア ID は無効です。 エリア ID は既にマップ上に存在します。**

ユーザーが、既にマップ上に存在するエリアをマップに入力しています。

**入力されたエリア ID は無効です。**

エリア ID は無効です。ブランクであるか、エリア ID が親エリア ID と同じです。

**入力されたエリア・データは無効です。**

エリア・データは無効です。お客様は、各エリアのすべての必須フィールドを入力したことを確認する必要があります。



親エリア ID が現在のマップ上にエリアとして存在することはできません。

入力した親エリア ID が、マップ上のエリアとして存在しています。 エリアは、マップ上のエリアである親エリアを持つことはできません。 親エリアは別のマップ上に存在しなければなりません。

エリアとその親エリアとの間に循環参照があります。循環参照を除去してください。

IBM Intelligent Operations Center データベースから循環親エリア関係を除去してください。

データ送信エラーです。

新しいエリア・タブがデータベースに入力されていません。

---

**CIYUI0003I** データは正常に送信されました

説明: これは単なる通知メッセージです。このメッセー

ジは、IBM Intelligent Operations Center データベース、ロケーション・マップ・マネージャー ポートレット、および ロケーション・マップ ポートレットが更新されたことを通知します。

**ユーザーの処置:** アクションは不要です。

---

**CIYUI0004I** 正常に送信されました。

説明: これは単なる通知メッセージです。このメッセージは、ロケーション・マップ・マネージャー ポートレット UI のみが更新されており、変更内容が IBM Intelligent Operations Center データベースに保管されていないことを通知します。変更を送信せずに ロケーション・マップ・マネージャー ポートレットを終了すると、更新がキャンセルされます。

**ユーザーの処置:** IBM Intelligent Operations Center データベースと ロケーション・マップ ポートレットを更新するには、「送信」をクリックします。

---

## 知識ベースおよび IBM サポートの使用

このセクションは、知識ベース、Fix Central、および IBM サポートを使用したトラブルシューティング情報の検索に関するトピックで構成されています。

### 知識ベースの検索

IBM 知識ベースを検索することで、問題の解決策が見つかることがあります。使用可能なリソース、サポート・ツール、および検索方法を使用して、結果を最適化できます。

### このタスクについて

IBM Intelligent Operations Center のインフォメーション・センターを検索することによって役立つ情報を見つけることができますが、疑問点を解消したり問題を解決したりするために、場合によってはインフォメーション・センター以外でも調べる必要が生じます。

### 手順

知識ベースで必要な情報を検索するには、以下の方法を 1 つ以上使用します。

- IBM Support Assistant Lite (ISA Lite) を使用してコンテンツを検索します。

ISA Lite は、IBM ソフトウェア製品に関する疑問の答えを見つけ、それらの製品に関する問題を解決するために役立つ、無償のソフトウェア・ツールです。ISA Lite のダウンロードおよびインストールの方法については、このトピックの末尾にあるリンクを参照してください。

- IBM サポート・ポータルを使用して必要なコンテンツを検索します。

IBM サポート・ポータルは、IBM のシステム、ソフトウェア、およびサービスのすべてについての技術サポート・ツールと情報が統合され、中央管理されているビューです。IBM サポート・ポータルでは、1 つの場所から IBM 電子サポート・ポータルフォリオにアクセスできます。問題を防止したり、問題を短時間で解決したりするために必要な情報とリソースを重点的に表示するように、ページを調整することができます。このツールについてのデモ・ビデオ ([https://www.ibm.com/blogs/SPNA/entry/the\\_ibm\\_support\\_portal\\_videos](https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos)) を表示して、IBM サポート・ポータルに慣れてください。これらのビデオ

オでは、IBM Support Portal の紹介、トラブルシューティングやその他のリソースの検索、およびポートレットを移動、追加、または削除してページを調整する方法の説明を行います。

- IBM Intelligent Operations Center に関する内容を検索するには、以下の追加技術リソースのいずれかを使用します。
  - IBM Intelligent Operations Center の技術情報と APAR (問題報告書)
  - IBM Intelligent Operations Center サポート・ポータル・ページ
  - IBM Intelligent Operations Center フォーラムおよびコミュニティのページ
  - IBM Smarter Cities Software Solutions Redbooks®
- IBM マストヘッド検索を使用してコンテンツを検索します。任意の [ibm.com](http://ibm.com)® ページの上部にある「検索」フィールドに検索ストリングを入力することによって、IBM マストヘッド検索を使用できます。
- Google、Yahoo、または Bing などの外部検索エンジンを使用してコンテンツを検索します。外部検索エンジンを使用する場合、結果に [ibm.com](http://ibm.com) ドメイン以外のものが含まれる可能性が高くなります。ただし、[ibm.com](http://ibm.com) 以外のニュースグループ、フォーラム、およびブログなどで IBM 製品の問題解決に関して役立つ情報が見つかる場合があります。

**ヒント:** IBM 製品に関する情報を検索する場合は、「IBM」と製品の名前を検索に含めてください。

#### 関連概念:

215 ページの『製品情報』

「製品情報」ポートレットを使用して、インストール済みの IBM Intelligent Operations Center および統合された IBM Smarter Cities Software Solutions のバージョンの詳細を表示します。インストール後に適用した更新の詳細も表示できます。

334 ページの『IBM Support Assistant Lite のインストールと使用』

IBM Support Assistant Lite (ISA Lite) は、一般的な問題の分析に役立つ一般的診断データを収集するツールです。

#### 関連情報:



IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5 のダウンロード

## Fix Central からのフィックスの入手

Fix Central を使用して、IBM Intelligent Operations Center などのさまざまな製品を対象として IBM サポートが推奨するフィックスを探すことができます。Fix Central を使用すると、任意の配信オプションを指定してシステムのフィックスを検索、選択、オーダー、およびダウンロードすることができます。問題解決のために、IBM Intelligent Operations Center 製品のフィックスを利用できる場合があります。

### 手順

フィックスを検索してインストールするには、以下の手順を実行します。

1. フィックスの取得に必要なツールを入手します。インストールされていない場合は、製品の更新インストーラーを入手します。インストーラーは Fix Central からダウンロードできます。このサイトには、更新インストーラーのダウンロード、インストール、および構成に関する説明が記載されています。
2. 製品として IBM Intelligent Operations Center を選択し、解決する問題に関連したチェック・ボックス (複数可) を選択します。
3. 必要なフィックスを特定して選択します。
4. フィックスをダウンロードします。

- a. ダウンロード資料を開き、「パッケージのダウンロード (Download Package)」セクションのリンクをたどります。
  - b. ファイルをダウンロードするときに保守ファイルの名前を変更しないでください。この変更には、意図的な変更のほか、特定の Web ブラウザーやダウンロード・ユーティリティーに起因する意図しない変更も該当します。
5. フィックスを適用するために、ダウンロード資料の『インストールの説明 (Installation Instructions)』セクションに記載されている説明に従います。
  6. オプション: フィックスをはじめとする IBM サポートの更新を毎週お知らせする E メール通知に加入してください。

#### 関連タスク:

358 ページの『サポート更新情報のサブスクリプション』

使用する IBM 製品についての重要な情報を受け取り続けるには、更新をサブスクリプションでできます。

#### 関連情報:



Fix Central のヘルプ

## IBM サポートへの連絡

IBM サポートでは、製品の問題点についての支援、FAQ への回答、および再ディスカバリーの実行を行っています。

### 始める前に

他の自助的方法 (技術情報の参照など) により回答や解決策を検索しても、目的の内容が見つからない場合は、IBM サポートに連絡してください。IBM サポートに連絡するには、ユーザーの企業が有効な IBM ソフトウェア・サブスクリプションおよびサポート契約を保持し、ユーザーが IBM に問題を送信する権限を持っている必要があります。使用可能なサポートのタイプについては、「*Software Support Handbook*」の『Support portfolio』のトピックを参照してください。

### 手順

問題について IBM サポートに連絡するときは、以下のステップを実行してください。

1. 問題を明確にし、背景情報を収集し、問題の重大度を判断してください。詳しくは、「*Software Support Handbook*」の『Getting IBM support』のトピックを参照してください。
2. 診断情報を収集します。IBM Support Assistant Lite を使用して IBM Intelligent Operations Center のログ・ファイルを収集する方法については、このトピックの末尾にあるリンクを参照してください。
3. 以下のいずれかの方法で、問題を IBM サポートに送信します。
  - IBM Support Assistant Lite (ISA Lite) を使用。このトピックの末尾にあるリンクを参照してください。
  - IBM Intelligent Operations Center サポート・ポータル・ページを介したオンライン: 「サービス・リクエスト」ページの「サービス・リクエスト」ポートレットから、お客様のすべてのサービス要求を開き、更新し、表示することができます。
  - 電話: お客様の地域の連絡先電話番号については、Directory of worldwide contacts の Web ページを参照してください。

## タスクの結果

お客様が提出した問題が、ソフトウェア障害または資料の不正確さや欠落が原因である場合、IBM サポートはプログラム診断依頼書 (APAR) を作成します。APAR には問題が詳細に記述されます。可能なときには常に、IBM サポートは、APAR が解決されてフィックスが配信されるまで、お客様が実装できる回避策を提供します。IBM は解決済みの APAR を IBM サポート Web サイトに毎日公開し、同じ問題を経験した他のユーザーが、同じ解決策を利用できるようにしています。

## 次のタスク

IBM Assist On-Site (使用しているコンピューターにダウンロードできるリモート・アシスタンス・プラグイン) を使用して、IBM 技術サポート担当者として作業するための準備を行ってください。IBM 技術サポート担当者は、IBM Assist On-Site を使用して、ユーザーのデスクトップを表示し、マウスおよびキーボードの制御を共有できます。このツールにより、問題の特定、必要なデータの収集、および問題の解決に要する時間を短縮できます。詳しくは、IBM Assist On-Site を参照してください。

### 関連概念:

215 ページの『製品情報』

「製品情報」ポータルレットを使用して、インストール済みの IBM Intelligent Operations Center および統合された IBM Smarter Cities Software Solutions のバージョンの詳細を表示します。インストール後に適用した更新の詳細も表示できます。

334 ページの『IBM Support Assistant Lite のインストールと使用』

IBM Support Assistant Lite (ISA Lite) は、一般的な問題の分析に役立つ一般的診断データを収集するツールです。

### 関連情報:



IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5 のダウンロード

## サポート更新情報のサブスクライブ

使用する IBM 製品についての重要な情報を受け取り続けるには、更新をサブスクライブできます。

### このタスクについて

更新を受け取るようにサブスクライブすることによって、特定の IBM サポート・ツールおよびリソースの重要な技術情報と更新を受け取ることができます。次の 2 つの方法のうちいずれかを使用して、更新をサブスクライブできます。

#### RSS フィード

IBM Intelligent Operations Center には、*IBM Intelligent Operations Center* の RSS フィードを使用できます。

開始手順および RSS 対応の IBM Web ページのリストなど、RSS についての一般情報については、「IBM ソフトウェア・サポート RSS フィード」のサイトを参照してください。

#### My Notifications

My Notifications を使用すると、任意の IBM 製品に対するサポートの更新をサブスクライブできます。（「通知」は、以前に使用されていた類似のツール My Support に置き換わるものです。）

「My Notifications」を使用して、毎日または毎週 E メールによる告知を受け取るように指定できます。また、受信する情報のタイプ（資料、ヒント、製品フラッシュ（アラートとも呼びます）、

ダウンロード情報、およびドライバーなど)を指定できます。「My Notifications」を使用することで、通知を希望する対象製品や、ニーズに応じた最適な配布方法をカスタマイズおよびカテゴリー化できます。

## 手順

サポート更新をサブスクライブするには、以下のようにします。

1. *IBM Intelligent Operations Center* の RSS フィードをサブスクライブするには、以下のサブステップに従います。
  - a. リンク *IBM Intelligent Operations Center* RSS フィード を開きます。
  - b. 「ライブ・ブックマークのサブスクライブ (Subscribe with Live Bookmark)」ウィンドウで、RSS フィードのブックマークを保存するフォルダーを選択し、「サブスクライブ (Subscribe)」をクリックします。

RSS フィードのサブスクライブについて詳しくは、このトピックの末尾にある関連情報セクションの「*IBM* ソフトウェア・サポート RSS フィード」リンクを参照してください。
2. *My Notifications* をサブスクライブするには、*IBM* サポート・ポータルにアクセスし、「通知」ポートレット内の「**My Notifications**」をクリックします。
3. *IBM ID* およびパスワードを使用してサインインし、「送信」をクリックします。
4. 受信する更新情報のタイプと受信方法を指定します。
  - a. 「サブスクライブ」タブをクリックします。
  - b. *IBM Intelligent Operations Center*を選択し、「続行」をクリックします。
  - c. 更新情報を受信する方法 (E メール、オンライン上の指定フォルダー、または RSS や Atom フィード) の設定を選択します。
  - d. 受信する資料更新のタイプ (製品ダウンロードに関する新情報やディスカッション・グループのコメントなど) を選択します。
  - e. 「送信」をクリックします。

## タスクの結果

使用している RSS フィードや「通知」設定を変更しない限り、要求した内容および方法で更新情報が通知されます。必要に応じて (例えば、1 つの製品の使用を停止して別の製品の使用を開始する場合など) に設定を変更できます。

### 関連タスク:

356 ページの『Fix Central からのフィックスの入手』

Fix Central を使用して、*IBM Intelligent Operations Center* などのさまざまな製品を対象として *IBM* サポートが推奨するフィックスを探すことができます。Fix Central を使用すると、任意の配信オプションを指定してシステムのフィックスを検索、選択、オーダー、およびダウンロードすることができます。問題解決のために、*IBM Intelligent Operations Center* 製品のフィックスを利用できる場合があります。

### 関連情報



[IBM ソフトウェア・サポート RSS フィード](#)



[「My Notifications」サポート・コンテンツの更新のサブスクライブ](#)



[My notifications for IBM technical support](#)



## IBM との情報の交換

問題を診断または識別するには、ご使用のシステムのデータおよび情報を IBM サポートに提供する必要があります。場合によっては、問題の判別を使用するためのツールまたはユーティリティが IBM サポートによって提供されることもあります。

### 関連概念:

325 ページの『トレースの使用可能化およびログ・ファイルの表示』

IBM Intelligent Operations Center での問題をトラブルシューティングするには、いくつかのシステムのログ・ファイルを分析することが必要な場合があります。以下のトピックでは、ログ・ファイルへのアクセス方法についていくつか説明しています。

334 ページの『IBM Support Assistant Lite のインストールと使用』

IBM Support Assistant Lite (ISA Lite) は、一般的な問題の分析に役立つ一般的診断データを収集するツールです。

### 関連タスク:

330 ページの『インストール収集必須ツールの実行』

IBM Intelligent Operations Center のインストール中には、ログ・ファイルが生成されます。ツールを使用して、これらのログ・ファイルを分析用に収集することができます。

### 関連情報:

 IBM Support Assistant Lite for IBM Intelligent Operations Center 1.5 のダウンロード

## IBM サポートへの情報の送信

問題解決にかかる時間を短縮するため、トレースおよび診断情報を IBM サポートに送信することができます。

### 手順

診断情報を IBM サポートに送信するには、次のようにします。

1. サービス・リクエスト・ツールを使用して、問題管理レコード (PMR) を開きます。
2. 必要な診断データを収集します。診断データがあると、PMR の解決に掛かる時間を短縮するのに役立ちます。診断データは、以下のように自動でも手動でも収集できます。
  - IBM Support Assistant Lite (ISA Lite) を使用してデータを自動的に収集する。このトピックの冒頭付近のリンクを参照してください。
  - データを手動で収集する。IBM Intelligent Operations Center のログ・ファイルについては、このトピックの冒頭付近にあるリンクを参照してください。
3. ZIP または TAR 形式を使用して、ファイルを圧縮します。
4. ファイルを IBM に転送します。以下のいずれかの方法を使用して、ファイルを IBM に転送できます。
  - サービス・リクエスト・ツール
  - 標準的なデータ・アップロード方式: FTP、HTTP
  - セキュアなデータ・アップロード方式: FTPS、SFTP、HTTPS
  - E メール



これらのデータ交換方法は、すべて IBM サポートのサイトで説明されています。

## IBM サポートからの情報の受信

時として、IBM 技術サポート担当員が、お客様に対して診断ツールやその他のファイルをダウンロードするようお願いすることがあります。それらのファイルは FTP を使用してダウンロードできます。

### 始める前に

IBM 技術サポート担当者から、ファイルのダウンロードに使用する優先サーバーと、アクセス先の正確なディレクトリー名およびファイル名が提供されていることを確認してください。

### 手順

IBM サポートからファイルをダウンロードするには次のようにします。

1. FTP を使用して、IBM 技術サポート担当員が指定したサイトに接続し、`anonymous` としてログオンします。パスワードには E メール・アドレスを使用します。
2. 以下の該当するディレクトリーに移動します。
  - a. `/fromibm` ディレクトリーに移動します。

```
cd fromibm
```
  - b. IBM 技術サポート担当員から通知されたディレクトリーに移動します。

```
cd nameofdirectory
```
3. セッションでバイナリー・モードを有効にします。

```
binary
```
4. `get` コマンドを使用して、IBM 技術サポート担当員によって指定されたファイルをダウンロードします。

```
get filename.extension
```
5. FTP セッションを終了します。

```
quit
```

---

## 既知の問題および解決策

このセクションでは、よく発生する問題のリストと、各項目の解決方法を示します。

### 一定期間後に重要業績評価指標の処理が停止する

IBM Intelligent Operations Center で、夜間など、一定期間後に重要業績評価指標 (KPI) 処理が停止することがあります。この問題の解決については、このトピックの末尾にあるリンクからトラブルシューティングの技術情報『*Key performance indicator processing stops after a period of time*』を参照してください。

### セキュリティ設定が変更されるとポートレットにデータが取り込まれない

ポートレットに KPI データ、アクティビティー・データ、またはリソース・データが期待通りに取り込まれない場合は、ポート設定を確認してください。システム・プロパティー・テーブルを使用して HTTPS 設定を変更した場合は、それに応じたポート設定の変更を行わないと、ポートレットへのデータの取り込みの問題が発生します。

### Cognos レポート接続エラー

Cognos レポート接続エラーを受信した場合は、ページを最新表示してください。

## Cognos レポートが正しく表示されない

「スーパーバイザー: レポート」ページまたは「オペレーター: レポート」ページを開いたときに Cognos レポートが正しく表示されない場合は、ページの最新表示を実行します。

ページの最新表示を実行しても Cognos レポートが正しく表示されない場合は、Cognos アプリケーション・サーバー・クラスターが停止している可能性があります。WebSphere Application Server 管理コンソールにログオンし、WebSphere Application Server クラスターの状況を確認します。クラスターの状況に赤い X が表示されている場合は、そのクラスターを選択して「開始」をクリックします。

## Cognos レポートのデータが見つからない

Cognos レポートが正しく表示されず、「No data found」メッセージが表示される場合は、選択基準に一致するデータがデータベースにない可能性があります。選択基準を再定義してください。例えば、カスタム・レポートの「開始日」フィールドと「終了日」フィールドをクリアしてから、「更新」をクリックします。次にレポート URL をコピーし、Cognos ポートレットに貼り付けます。

## 「レポート URL」ボタンを使用してレポート URL をコピーするとレポートが表示されない

サンプル・ユーザーが「レポート URL」ボタンを使用してレポート URL をコピーしてから、「レポート」ポートレット・ページに直接移動すると、レポートが表示されません。この問題を修正するには、F5 を押して最新表示してください。レポートが正しく表示されるようになります。

## 「詳細」ポートレットで編集済みのリソースが表示されない

Tivoli Netcool/Impact が使用不可のときに Tivoli Service Request Manager でリソースを編集すると、「詳細」ポートレットにリソースが表示されないことがあります。例えば、「イベントとインシデント」タブでイベントを右クリックしてから「近接リソースの表示」をクリックすると、編集されたリソースが表示されないことがあります。この問題を解決するには、Tivoli Service Request Manager でリソースをもう一度編集します。

## ログアウトしたユーザーの状況が「連絡先」ポートレットに正しく表示されない

ログオンしているユーザーの状況が「連絡先」ポートレットに表示されます。ログオンしているユーザーがブラウザ・ウィンドウを閉じるか WebSphere Portal からログオフした場合、セッションの有効期限が切れるまで、そのユーザーの状況はログオン状態のまま表示されます。しかし、ログオンしているユーザーがブラウザ・ウィンドウを閉じるかログオフした後で、このユーザーにメッセージを送信しても、メッセージは配信されません。したがって、メッセージを送信しようとしているユーザーにはエラー・メッセージが表示されます。「連絡先」ポートレットで自分の状況が即時に更新されるようにするには、「ファイル」>「ログアウト」をクリックしてログオフします。

## スーパーバイザー・レポート・ページで「更新」を複数回選択した場合

IBM Intelligent Operations Center ユーザー・インターフェースの「スーパーバイザー: レポート」ページで、変更を行わずに「更新」を選択すると、「開始日」および「終了日」フィールドに今日の日付が取り込まれます。変更を行わずに、もう一度「更新」を選択すると、「データが見つかりません」というメッセージが表示されます。

この動作は、「開始日」および「終了日」フィールドに自動的にデータが取り込まれるために起こります。

## 見出しが長いとレポートのグラフが使用に適さなくなる

イベントの見出しが 20 から 30 文字を超えていると、「すべてのイベント (見出し別) (All Events, by **Headline**)」円グラフのレポートの表示方法が影響を受け、グラフが使用に適さなくなります。 イベントの見出しが円グラフの各セクションのラベルとなり、ラベルが収まるように円グラフが縮小されるため、円グラフのイメージが小さくなりすぎて、各セクションが区別できなくなります。

## ブラウザーの時間帯の変換で予期しない結果となる

ブラウザーの時間帯の変換で予期しない結果となるのは、共通アラート・プロトコル (CAP) イベントで時間帯が不適切にコーディングされていることに原因があると考えられます。 詳しくは、このトピックの末尾にあるリンクを参照してください。

### 関連概念:

107 ページの『KPI イベントに対する CAP の使用』

IBM Intelligent Operations Center の一部として提供されている WebSphere Message Broker は、CAP イベント・メッセージを受け入れ、重要業績評価指標 (KPI) の計算にそのデータを使用します。

### 関連情報:



一定期間後に停止する重要業績評価指標処理についてのトラブルシューティング技術情報

## IBM Intelligent Operations Center インストール時の接続エラー

IBM Intelligent Operations Center のインストール時に SOAPException メッセージが出た場合にどうすればよいかについて説明します。

次のようなメッセージが出た場合は、サーバーへの接続が失われています。

```
[SOAPException: faultCode=SOAP-ENV:Client; msg=Read timed out
```

これが発生した場合、サーバーを停止してから再始動します。 その後で、インストーラーを再始動するか、インストール・コマンドを再実行してください。

## IPv6 ネットワーキングが開始されない

IPv6 ネットワーキングがサーバーで開始されない場合は、`/etc/modprobe.conf` ファイルの変更が必要な場合があります。

### このタスクについて

この問題は、VMWare をリリース 5 にアップグレードした場合に発生することがあります。

### 手順

1. `/etc/modprobe.conf` ファイルを編集します。
2. 以下の行を変更します。

```
alias ipv6 off
```

上記の行を以下のように変更します。

```
# alias ipv6 off
```

3. 以下の行を変更します。

```
options ipv6 disable=1
```

上記の行を以下のように変更します。

```
# options ipv6 disable=1
```

4. ファイルを保存します。
5. サーバーを再始動します。

## Tivoli Service Request Manager が開始しない

Tivoli Service Request Manager がプラットフォーム制御ツールで開始できないが、システム検査チェック・ツールでは作動中として表示されている場合に、どうすればよいかについて説明します。

### このタスクについて

Tivoli Service Request Manager を再始動するには、以下のようにします。

#### 手順

1. プラットフォーム制御ツールを使用して、すべてのサービスを停止します。
2. イベント・サーバーをシャットダウンして、再始動します。
3. プラットフォーム制御ツールを使用して、すべてのサービスを開始します。

## ユーザー・インターフェースの新規ページを作成できない

Microsoft Internet Explorer 9 を使用している場合に新規ページを作成する際に発生する問題を解決します。

### このタスクについて

この問題は、「管理」ページまたは「市全域」ユーザー・ページから新規ページを作成する際に発生することがあります。新規ページがロードされません。この問題を解消するには、ブラウザを一時的に「互換表示」に切り替えます。IBM Intelligent Operations Center では Internet Explorer 8 または Internet Explorer 9 の互換表示がサポートされていないため、新規ページを作成したら「互換表示」をオフにする必要があります。

#### 手順

1. Internet Explorer 9 を開きます。
2. 管理者として IBM Intelligent Operations Center にログオンします。
3. 「管理」 > 「ポータル・ユーザー・インターフェース」 > 「ページの管理」とクリックする。
4. ブラウザー上部のツールバーで「ツール」を選択します。
5. メニューから「Compatibility View」を選択します。
6. 検索ボックスに citywide と入力します。
7. 検索結果が返されたら、「citywide」をクリックします。
8. 「新規ページ」をクリックします。
9. 新規ページがロードされたら、ブラウザ・ツールバーに戻り「互換表示」を選択解除します。

## 関連概念:

15 ページの『サポートされるブラウザ』

IBM Intelligent Operations Center ソリューション・インターフェースは複数のブラウザをサポートします。一部のブラウザは制限付きで使用できます。

## ポートレットのアクセシビリティに関する回避策

一部の IBM Intelligent Operations Center ポートレットに関連するアクセシビリティの問題に対応する回避策があります。

- 「詳細」ポートレットおよび「通知」ポートレットでは、ポップアップ・メニューにアクセスするために、以下のキーボード制御を使用します。

### Windows

専用のメニュー・キーを押します。

### Mac

テンキーがあるかどうかに応じて、該当するオプションを選択します。

- テンキーがある場合は、マウス・キーが使用可能であることを確認して、Ctrl+5 を押します。
- テンキーがない場合は、マウス・キーを使用可能にして、Ctrl+I を押します。
- 「イベントの追加」ウィンドウを開くには、「詳細」ポートレットで、「イベントとインシデント」タブをクリックするか、Tab キーを押します。これにより、スクリーン・リーダーがタブの名前を読み取ります。その後、リストから適切なキーボード制御を選択します。

### Mozilla Firefox

Ctrl+Alt+V

### Safari

fn+control+option+V

### Internet Explorer

Ctrl+Alt+V

- 「詳細」ポートレットの「イベントの追加」ウィンドウでは、スクリーン・リーダーは以下の値を読み取りません。
  - 発効日付
  - 発効時刻
  - 開始日付
  - 開始時刻
  - 有効期限 (日付)
  - 有効期限 (時刻)

## 「レポート」ポートレットで日付を選択するためのアクセシビリティの対処法

「レポート」ポートレットでは、キーボードを使用してカレンダーから日付を選択することはできません。

### このタスクについて

「レポート」ポートレットでは、事前定義レポートを構成するには、日付または日付の範囲を入力する必要があります。ただし、キーボードではカレンダー日付ピッカーにアクセスできません。カレンダーは表示されますが、キーボードを使用してカレンダーから日付を選択することはできません。カレンダーからの日付の選択は、マウスを使用する場合にのみ機能します。

この問題に対処するには、以下の手順に従って、キーボードを使用して日付を手動で入力します。

## 手順

1. 「レポート」ポートレットで、ページの下部にある事前定義レポートを選択し、「レポートの構成」をクリックします。
2. 「開始日」フィールドに、情報を表示する日付を入力します。日付範囲を入力する場合、この日付は最初の日です。
3. 「終了日」フィールドに、レポート情報の日付の範囲内の最終日を入力します。
4. 「レポートの表示」をクリックします。

## 「詳細」ポートレットで新規イベントが表示されない

「詳細」ポートレットで新規イベントが表示されない問題を解決する方法は複数あります。

## このタスクについて

最初の方法で問題を解決できない場合は、次の方法に進んでください。問題が解決するまで、さまざまな方法を使用します。

## 手順

1. IBM Intelligent Operations Center XML プローブの状況を確認します。
  - a. イベント・サーバーに root としてログオンし、以下のコマンドを入力します。

```
- tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```
  - b. ファイルの終わりに「Connection status OK」が表示されるかどうかを確認します。
  - c. 「Probe shutting down」メッセージが表示される場合、または日時が現行サーバー時刻と一致しない場合は、以下の手順を実行します。
    - 1) 以下のコマンドを入力して、現在のログを名前変更します。

```
- mv /opt/IBM/netcool/omnibus/log/ioc_xml.log  
/opt/IBM/netcool/omnibus/log/old_ioc_xml.log
```
    - 2) 以下のコマンドを入力して、プローブを再始動します。

```
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile  
/opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```
    - 3) 約 1 分間待ってから、以下のコマンドを入力します。

```
- tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log
```

「Connection Status OK」を検索します。接続状況が OK ではない場合は、ファイルでエラーを調べます。接続の問題は、オブジェクト・サーバーがダウンしていることを意味する場合があります。ステップ 2 を参照してください。
2. IBM Intelligent Operations Center XML プローブが引き続きシャットダウンする場合は、以下の手順に従って Tivoli Netcool/OMNIBus データベースの状況を確認します。IBM Intelligent Operations Center XML プローブがシャットダウンしなくなった場合は、ステップ 3 (367 ページ) に進みます。
  - a. イベント・サーバーに ibmadmin としてログオンし、以下のコマンドを入力します。

```
- /opt/IBM/netcool/omnibus/bin/nco_config &
```
  - b. omni.dat からのインポートを求めるプロンプトが出されたら、「はい」を選択して「終了」をクリックします。
  - c. プロセス・エージェント・ウィンドウを最小化し、「NCOMS」を右クリックします。



「接続方法 (Connect As)」オプションが使用可能な場合はこのオプションをクリックし、root として接続し、トポロジー・パスワードを使用します。

「接続方法 (Connect As)」オプションが表示されない場合は、nco\_config を閉じ、NCOMS オブジェクト・サーバーを始動する以下のコマンドを ibmadmin として入力します。

```
- /opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
```

NCOMS オブジェクト・サーバーが始動しない場合は、/opt/IBM/netcool/omnibus/var を開き、NCOMS.pid ファイルを見つけて削除してから、以下のコマンドを入力します。

```
/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &
```

注: NCOMS オブジェクト・サーバーの始動後に、IBM Intelligent Operations Center XML プロンプトを再始動する必要があります。ステップ 1 (366 ページ) を参照してください。

3. Tivoli Netcool/Impact の状況を確認します。

- a. `http://EventsHost:9080/nci/login_main.jsp` のイベント・サーバーに admin としてログオンします。

ログオンできない場合は、イベント・サーバーで以下のコマンドを実行します。

```
su - netcool  
/opt/IBM/netcool/bin/ewas.sh start
```

- b. 「サービス状況」ウィンドウをスクロールダウンし、以下のサービスが実行中であることを確認します。

- **EventProcessor**
- **IOC\_CAP\_Event\_Reader**
- **IOC\_Notification\_Reader**

注: 実行中のサービスの横には緑色のチェック・マークが表示されます。

- c. 「サービス状況」ウィンドウで「ポリシー・ロガー」の横にある「ログの表示」アイコンをクリックし、ログ・ファイルでエラーがあるかどうかを確認します。

ログでエラーが見つかったら、/opt/IBM/netcool/impact/log/ にあるログ・ファイルの詳細を表示できます。更に詳細な情報については、「ポリシー・ロガー」をクリックして「最上位のログ・レベル」を 3 に設定し、関連するチェック・ボックスを選択します。

4. イベントが WebSphere MQ キューのいずれかでスタックしているかどうかを確認します。

- a. VNC クライアントを使用してイベント・サーバーにログオンし、以下のコマンドを入力して WebSphere MQ エクスプローラーを開きます。

```
xhost +  
su - mqm  
strmqcfg &
```

注: ウェルカム・ページが開いたら、そのページを閉じます。

- b. 「IBM WebSphere MQ」 > 「キュー・マネージャー」 > 「IOC.MC.QM」 > 「QueuesLocate」を展開し、Queues フォルダーを選択します。
- c. 「キュー」テーブルで、IOC\_ で始まるすべての照会の「現行キュー項目数」を確認します。例: IOC\_KPI\_IN\_INTERNAL\_USE\_ONLY\_DO\_NOT\_MODIFY。

時間の長さに関係なく、0 より大きいキュー項目数は問題があることを示している可能性があります。

5. CAP イベントが IBM Intelligent Operations Center データベースに到達していることを確認します。

- a. VNC クライアントを使用してデータ・サーバーにログオンし、以下のコマンドを入力して DB2 Control Center を開きます。

```
xhost +
su - db2inst1
Db2cc &
```

- b. 「**IOCDB**」 > 「**表**」をクリックし、**IOC\_COMMON** スキーマの「**イベント**」を右クリックし、「**開く**」をクリックします。システムに送信されたイベントのリストが表示されます。
- c. データベースにイベントが存在していることを確認します。

注: システムでのイベントの数に応じて、取り出す行を増やす必要がある場合があります。

6. ポータル・サーバーでトレースを使用可能にするには、以下の手順に従います。
  - a. `http://app-host:9060/ibm/console` (app-host はアプリケーション・サーバーの完全修飾ホスト名) で管理コンソールにログオンします。
  - b. 「**トラブルシューティング**」 > 「**ログおよびトレース**」をクリックします。
  - c. 「**WebSphere\_Portal**」 > 「**ログ・レベル詳細の変更 (Change log level details)**」をクリックします。
  - d. 「**実行時間**」タブをクリックし、以下のコマンドを貼り付け、「**OK**」をクリックします。

```
*=warning: com.ibm.iss.*=all: com.ibm.ioc.*=all
```
  - e. ログを表示するには、以下のコマンドを入力します。

```
cd /opt/IBM/WebSphere/wp_profile1/logs/WebSphere_Portal
tail -f trace.log
```

ログの表示について詳しくは、このトピックの末尾にある関連概念のリンクを参照してください。

#### 関連概念:

325 ページの『[トレースの使用可能化およびログ・ファイルの表示](#)』  
IBM Intelligent Operations Center での問題をトラブルシューティングするには、いくつかのシステムのログ・ファイルを分析することが必要な場合があります。以下のトピックでは、ログ・ファイルへのアクセス方法についていくつか説明しています。

## 認証メカニズムが使用できない

WebSphere Portal へのログオン後に「HPDIA0119W 認証メカニズムが使用できません」というエラー・メッセージが表示されたら、Tivoli Directory Server とアプリケーション・サーバーの Tivoli Directory Server プロキシの状況を確認してください。 server.

### 手順

1. 管理サーバーに `ibmadmin` としてログオンし、以下のコマンドを入力します。

```
su - ibmadmin
cd /opt/IBM/ISP/mgmt/scripts
./iopmgmt.sh status tds topology_password
```

サーバーが稼働中の場合は、次の例のようなメッセージが表示されます。

```
照会コマンドを実行中です.....完了しました。
IBM Tivoli Directory Server [ on ]
コマンドが正常に完了しました。
```

2. サーバーが稼働していない場合は、`./iopmgmt.sh start tds topology_password` と入力します。
3. ステップ 1 と 2 の実行後にサーバーが稼働していない場合は、管理サーバーに `ibmadmin` としてログオンし、次のコマンドを入力します。

```
su - ibmadmin
cd /opt/IBM/ISP/mgmt/scripts
./iopmgmt.sh status tdspxyapp topology_password
```

サーバーが稼働中の場合は、次の例のようなメッセージが表示されます。

```
照会コマンドを実行中です.....完了しました。
IBM Tivoli Directory Server [ on ]
コマンドが正常に完了しました。
```

4. サーバーが稼働していない場合は、`./iopmgmt.sh start tdspxyapptopology_password` と入力します。

## サード・パーティー・サーバーが応答していません

WebSphere Portal ポータルへのログオン後に「サード・パーティーのサーバーが応答しない」というエラー・メッセージが表示されたら、WebSphere Portal の状況を調べてください。

### 手順

1. 管理サーバーに `ibmadmin` としてログオンし、以下のコマンドを入力します。

```
su - ibmadmin
cd /opt/IBM/ISP/mgmt/scripts
./iopmgmt.sh status wpe topology_password
```

ポータルが実行中の場合は、次のようなメッセージが表示されます。

```
照会コマンドを実行中です.....完了しました。
IBM WebSphere Portal Extend [ on ]
コマンドが正常に完了しました。
```

2. ポータルが稼働していない場合は、`./iopmgmt.sh start wpe topology_password` と入力します。

## 「マイ・アクティビティ」ポートレットでアクティビティが表示されない

「マイ・アクティビティ」ポートレットにアクティビティが表示されない場合に考えられるいくつかの原因について、以降のセクションで説明します。

## サンプル・データを使用したトラブルシューティング

サンプル・データを使用してイベントを作成し、その結果から、アクティビティが表示されない原因として考えられるものを絞り込みます。

### 手順

1. IBM Intelligent Operations Center 管理インターフェースに `wpsadmin` としてログオンします。
2. 「ハリケーンの接近」イベントを作成します。
  - a. 「マップ」ポートレットで、マップを右クリックし、「イベントの追加」をクリックします。
  - b. 「イベント・タイプ」で「ハリケーンの接近」を選択します。その他のフィールドに値が事前に自動的に取り込まれます。
  - c. 「緊急度」で「早急」を選択します。
  - d. その他のイベント・パラメーターはデフォルト値のままにして、「OK」をクリックします。

「ハリケーンの接近」イベントのパラメーターは、標準操作手順の選択マトリックスのサンプル標準操作手順にマッピングされています。

3. 約 5 分後に、「ハリケーンの接近」イベントに対応する新しいアクティビティが「マイ・アクティビティ」ポートレットに表示されることを確認します。

## タスクの結果

- 「ハリケーンの接近」イベントに対応するアクティビティーが「マイ・アクティビティー」ポートレットに表示されていない場合、他のユーザーに対してアクティビティーが表示されない問題は、Tivoli Service Request Manager の問題が原因となっている可能性があります。
- 「ハリケーンの接近」イベントに対応するアクティビティーが「マイ・アクティビティー」ポートレットに表示されている場合、別のユーザーに対してアクティビティーが表示されない問題は、以下のいずれかが原因となっている可能性があります。
  - ユーザー権限が、正しく構成されていない。
  - 標準操作手順が正しく構成されていない。
  - 標準操作手順の選択マトリックスが正しく構成されていない。

### 関連資料:

154 ページの『標準操作手順、ワークフロー、およびリソースのサンプル』

標準操作手順、ワークフロー、およびリソースのサンプルは、IBM Intelligent Operations Center バージョン 1.5 をインストールすると、それに付属しています。

## Tivoli Service Request Manager の状況の検証

サンプル・データを使用してイベントを作成しても「マイ・アクティビティー」ポートレットにアクティビティーが表示されない場合は、以下の手順に従って Tivoli Service Request Manager のトラブルシューティングを行います。

### 始める前に

Tivoli Service Request Manager 管理パスワードが正しく暗号化されていることを確認します。詳しくは、手順の末尾にあるリンクを参照してください。

### このタスクについて

次のいずれかのオプションを選択します。

### 手順

- プラットフォーム制御ツール を使用して Tivoli Service Request Manager の状況を確認します。
  1. `putty` コマンドを使用して、イベント・サーバーに `ibmadmin` としてログオンします。
  2. `opt/IBM/ISP/mgmt/scripts` ディレクトリーに移動します。
  3. Tivoli Service Request Manager の状況を取得し、Tivoli Service Request Manager を停止および開始するため、プラットフォーム制御ツール を使用します。プラットフォーム制御ツールの実行について詳しくは、この手順の末尾にあるリンクを参照してください。
- あるいは、Tivoli Service Request Manager を手動で再始動するには以下の手順を実行します。
  1. `putty` コマンドを使用して、イベント・サーバーに `ibmadmin` としてログオンします。
  2. Tivoli Service Request Manager を停止するには、コマンド行に以下のコマンドを入力します。

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
./stopServer.sh MXServer1 -user waswebadmin -password password
./stopNode.sh -user waswebadmin -password password
../../ctgDmgr01/bin/stopManager.sh -user waswebadmin -password password
```

ここで、`password` は、トポロジー・パスワードです。

3. Tivoli Service Request Manager を開始するには、以下のコマンドを入力します。

```
cd /opt/IBM/WebSphere/AppServerV61/profiles/ctgAppSrv01/bin
../../ctgDmgr01/bin/startManager.sh
./startNode.sh -user waswebadmin
./startServer.sh MXServer1
exit
```

#### 関連タスク:

222 ページの『サービス状況の照会』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスの状況を判別することができます。

216 ページの『サービスの開始』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサーバーで実行中のサービスを開始することができます。

219 ページの『サービスの停止』

プラットフォーム制御ツールを使用して、IBM Intelligent Operations Center のサービスを停止できます。

68 ページの『Tivoli Service Request Manager 管理パスワードの暗号化』

以下の手順に従って、Tivoli Netcool/Impact で Tivoli Service Request Manager 管理パスワードを暗号化します。

## ユーザー権限の検証

標準操作手順に関連付けられているアクティビティを表示する権限がユーザーにあることを確認します。

### 手順

1. 「標準操作手順」ポートレットを開くには、WebSphere Portal Administration インターフェースで「Intelligent Operations」 > 「カスタマイズ・ツール」 > 「標準操作手順」をクリックします。
2. 標準操作手順の選択マトリックスのアプリケーションを開くには、「標準操作手順の選択マトリックス」をクリックします。
3. 「SOP 名」列で、ユーザー権限を検証する標準操作手順の名前を見つけます。
4. 「SOP 名」フィールドの横にある「詳細」メニュー・アイコンをクリックし、「標準操作手順へ移動」をクリックします。
5. 「所有者グループ」フィールドの横にある「詳細」メニュー・アイコンをクリックし、「担当者グループに移動 (Go To Person Groups)」をクリックします。
6. ユーザーが担当者グループのメンバーになっていることを確認します。

### 次のタスク

ユーザーが 担当者グループのメンバーではない場合は、以下のいずれかの操作を実行します。

- 標準操作手順に関連付けられているアクティビティを表示する権限をユーザーに付与しない。
- 担当者グループに割り当てられているすべてのアクティビティがユーザーに対して表示されるようにするため、担当者グループにユーザーを追加する。
- 標準操作手順に関連付けられている別の担当者グループにユーザーを追加する。

ユーザーの構成について詳しくは、このタスクの末尾にあるリンクを参照してください。

## 関連タスク:

141 ページの『Tivoli Service Request Manager での新規ユーザーの構成』  
IBM Intelligent Operations Center でユーザーを追加したら、Tivoli Service Request Manager で、そのユーザーに権限および担当者グループを割り当てます。

## ワークフローと標準操作手順の関連付けの検証

標準操作手順の選択マトリックスで定義した一連の選択基準に一致するパラメーターを持つイベントを作成します。関連付けられているワークフロー・アクティビティーが「マイ・アクティビティー」ポートレットに表示されることを確認します。

### このタスクについて

以下の各ステップについて詳しくは、手順の末尾にあるリンクを参照してください。

#### 手順

1. ワークフローを作成します。
2. 標準操作手順を作成し、前のステップで作成したワークフローに関連付けます。
3. 標準操作手順の選択マトリックスで標準操作手順の項目を作成します。
4. 「マップ」ポートレットで、標準操作手順の選択マトリックスで定義したパラメーターに一致するイベントを作成します。
5. 関連付けられているワークフロー・アクティビティーが「マイ・アクティビティー」ポートレットに表示されることを確認します。

### 次のタスク

アクティビティーが「マイ・アクティビティー」ポートレットに表示されない場合は、ワークフロー、標準操作手順、標準操作手順の選択マトリックス、およびイベントを正しく構成したかどうかを確認します。構成が正しい場合は、Tivoli Netcool/OMNIBus ポリシー・ログ・ファイルと Tivoli Service Request Manager ログ・ファイルを調べます。



#### 関連概念:

309 ページの『マップ』

「マップ」ポートレットを使用して、イベントおよびリソースをマップ上で確認します。

314 ページの『マイ・アクティビティ』

「マイ・アクティビティ」ポートレットには、インターフェースにログオンしているユーザーがメンバーとして所属するグループが所有するアクティビティの動的なリストが表示されます。

#### 関連タスク:

144 ページの『ワークフローの作成』

Tivoli Service Request Manager では、標準操作手順アクティビティに自動タスクとして含めることができるワークフローを作成できます。

144 ページの『標準操作手順の作成』

標準操作手順を作成し、所有者グループに割り当てます。ユーザーは、担当者グループのメンバーシップによって所有者グループに割り当てられます。

147 ページの『標準操作手順の選択マトリックスでのパラメーターの定義』

標準操作手順の選択マトリックスで、特定のイベントについて標準操作手順を選択するかどうかを決定するイベント・パラメーターを定義します。

## ログ・ファイルの確認

Tivoli Netcool/OMNIBus ポリシー・ログ・ファイルと Tivoli Service Request Manager ログ・ファイルを確認します。

### 手順

- Tivoli Netcool/OMNIBus ポリシー・ログ・ファイルを確認します。
  1. Tivoli Netcool/OMNIBus ポリシー・ログ・ファイルを使用可能にします。ログ・ファイルを使用可能にして使用方法については、この手順の末尾にあるリンクを参照してください。
  2. Tivoli Netcool/OMNIBus ポリシー・ログ・ファイルで、イベントを見つけるため、CallMaximoEnterpriseServices を検索します。Tivoli Netcool/OMNIBus ポリシー・ログ・ファイルは、イベントをパラメーター (Category、Severity など) によって解析し、各イベントとその関連作業指示書 ID をリストします。標準操作手順の選択マトリックスに対してイベントを突き合わせることができます。イベントが Tivoli Netcool/OMNIBus ポリシー・ログ・ファイルにリストされない場合の原因としては、イベント・パラメーターと一致する標準操作手順がないことが考えられます。
  3. 「server error 500」を検索します。これは、Tivoli Service Request Manager サーバー・エラーを示します。このエラーがある場合は、Tivoli Service Request Manager ログ・ファイルを確認します。この手順の末尾にあるリンクを参照してください。
- Tivoli Service Request Manager のログ・ファイルを確認します。ログ・ファイルを使用可能にして使用方法については、この手順の末尾にあるリンクを参照してください。

#### 関連タスク:

329 ページの『Tivoli Netcool/Impact ログ・ファイルの使用可能化と表示』

326 ページの『Tivoli Service Request Manager のトレースの使用可能化とログ・ファイルの表示』

## 「状況」ポートレットまたは「重要業績評価指標のドリルダウン」ポートレットに KPI データが表示されない

「状況」ポートレットまたは「重要業績評価指標のドリルダウン」ポートレットに KPI データが表示されない場合は、手順に従って問題を解決します。

## 手順

1. IBM WebSphere Business Monitor の状況を確認するため、WebSphere Application Server 管理コンソールにログオンします。管理コンソールへのアクセスについては、このトピックの末尾にあるリンクを参照してください。
2. IBM WebSphere Business Monitor が停止中の場合は、再起動します。IBM WebSphere Business Monitor が停止していない場合は最初に停止してから再始動します。問題が解決しない場合は、ステップ 3 に進みます。
3. IBM WebSphere Business Monitor のログを調べ、IBM WebSphere Business Monitor の問題を調査して解決します。ログの確認については、このトピックの末尾にあるリンクを参照してください。
4. IBM WebSphere Business Monitor の問題がすべて解決されたら、WebSphere Application Server 管理コンソールにログオンして IBM WebSphere Business Monitor を再始動します。

### 関連概念:

325 ページの『アプリケーション・サーバーのログ・ファイル』

アプリケーション・サーバーの一部のシステムについてトレースを使用可能にしてログを表示するには、以下の手順を実行します。

224 ページの『管理コンソール』

「管理コンソール」ポートレットを使用して、ソリューションによって提供されるサービスを管理します。

## 「状況」ポートレットまたは「重要業績評価指標のドリルダウン」ポートレットでイベントが更新されない

KPI イベント・データが「状況」ポートレットまたは「重要業績評価指標のドリルダウン」ポートレットで更新されない場合は、問題が解決するまで手順の各ステップを順に実行します。

## 手順

1. KPI イベント更新が IBM Intelligent Operations Center に到達していることを確認するには、このトピックの末尾にある「詳細」ポートレットで新規イベントが表示されないのリンクに移動し、手順に従って操作します。
2. イベントが IBM WebSphere Business Monitor に到達していることを確認します。
  - a. WebSphere Application Server 管理コンソールにログオンします。管理コンソールへのアクセスについては詳しくは、このトピックの末尾にあるリンクを参照してください。
  - b. 「トラブルシューティング」 > 「モニター・モデル」 > 「失敗したイベント・シーケンス」をクリックします。このページに表示される KPI イベントをすべて削除します。
  - c. IBM WebSphere Business Monitor を再始動します。
  - d. 「アプリケーション」 > 「モニター・サービス」 > 「記録済みイベントの管理」 > 「イベント・レコードの使用可能/使用不可」をクリックし、イベントの記録を有効にします。
  - e. 「アプリケーション」 > 「モニター・サービス」 > 「記録済みイベントの管理」 > 「イベントの管理」をクリックします。このページで、IBM Intelligent Operations Center に送信される各 KPI イベントに対して 2 つ以上のイベントが作成されていることを確認します。
3. KPI イベントの更新が「重要業績評価指標」ポートレットに到達していることを確認します。「重要業績評価指標」ポートレットについて詳しくは、このトピックの末尾にあるリンクを参照してください。「重要業績評価指標」ポートレットで KPI 値が更新されている場合は、IBM WebSphere Business Monitor で値が更新されています。

**関連概念:**

224 ページの『管理コンソール』

「管理コンソール」ポートレットを使用して、ソリューションによって提供されるサービスを管理します。

186 ページの『重要業績評価指標』

「重要業績評価指標」ポートレットでは、IBM Intelligent Operations Center の重要業績評価指標 (KPI) およびそれらの階層表示をカスタマイズすることができます。

**関連タスク:**

366 ページの『「詳細」ポートレットで新規イベントが表示されない』

「詳細」ポートレットで新規イベントが表示されない問題を解決する方法は複数あります。



## 第 10 章 リファレンス

以下のトピックには、有用な追加参照情報が記載されています。

### IBM Intelligent Operations Center に組み込まれている製品およびコンポーネント

IBM Intelligent Operations Center ソリューションは、多くのソフトウェア製品およびコンポーネントをインストールします。

ソフトウェア製品およびコンポーネントと、それらのインストール先のサーバーを、表 100 に示します。

表 100. IBM Intelligent Operations Center と共にインストールされる製品

製品	アプリケーション・サーバー	データ・サーバー	イベント・サーバー	管理サーバー
IBM WebSphere Business Monitor 7.5	インストールされる	インストールされない	インストールされない	インストールされない
IBM Cognos Business Intelligence 10.1.1	インストールされる	インストールされない	インストールされない	インストールされない
DB2 Enterprise Server Edition with DB2 Spatial Extender 9.7.0.5	インストールされない	インストールされる	インストールされない	インストールされる
Semantic Model Services	インストールされない	インストールされない	インストールされない	インストールされる
IBM ILOG® CPLEX® Optimization Studio 12.4	インストールされる	インストールされない	インストールされない	インストールされない
Jazz Foundation Server (Semantic Model Services 用) 3.0.1	インストールされない	インストールされない	インストールされない	インストールされる
Lotus Domino 8.5.3.1	インストールされない	インストールされない	インストールされる	インストールされない
Lotus Sametime Standard 8.5.2 + IFR1	インストールされない	インストールされない	インストールされる	インストールされない
Tivoli Access Manager for e-Business 6.1.1.4	インストールされない	インストールされない	インストールされない	インストールされる
Tivoli Composite Application Manager 7.1	インストールされない	インストールされない	インストールされない	インストールされる
Tivoli Directory Integrator 7.1.0.5	インストールされない	インストールされない	インストールされない	インストールされる
Tivoli Directory Server 6.3.0.8	インストールされない	インストールされる	インストールされない	インストールされない
Tivoli Identity Manager 5.1	インストールされない	インストールされない	インストールされない	インストールされる

表 100. IBM Intelligent Operations Center と共にインストールされる製品 (続き)

製品	アプリケーション・サーバー	データ・サーバー	イベント・サーバー	管理サーバー
Tivoli Monitoring 6.2.2.1	インストールされない	インストールされない	インストールされない	インストールされる
Tivoli Netcool/Impact 5.1.1.1 + IF003	インストールされない	インストールされない	インストールされる	インストールされない
Tivoli Netcool/OMNIBus 7.3.1.2 および XML プローブ	インストールされない	インストールされない	インストールされる	インストールされない
Tivoli Service Request Manager 7.2.1.2	インストールされない	インストールされない	インストールされる	インストールされない
WebSphere Application Server 1.1.0.0 Web 2.0 およびモバイル用フィチャー・パック	インストールされる	インストールされない	インストールされない	インストールされない
WebSphere Application Server Network Deployment 7.0.0.21	インストールされる	インストールされない	インストールされない	インストールされる
WebSphere Application Server 6.1.0.29 for Tivoli Service Request Manager	インストールされない	インストールされない	インストールされる	インストールされない
WebSphere Message Broker 8.0	インストールされない	インストールされない	インストールされる	インストールされない
WebSphere MQ 7.0.1.7	インストールされない	インストールされない	インストールされる	インストールされない
WebSphere Operational Decision Management 7.5.1 (ルール・エンジン)	インストールされる	インストールされない	インストールされない	インストールされない
WebSphere Portal Enable 7.0.0.2	インストールされる	インストールされない	インストールされない	インストールされない

## root アカウントで実行されるプロセス

Cyber Hygiene の実行後に、root アカウントを使用して実行する必要があるプロセスがあります。

root アカウントで実行されるプロセスは、ユーザーまたはプロセスが特権エスカレーションによって root 特権を取得できる場合にぜい弱となることがあります。通常、これはユーザーによって出されるサービス処理要求でのみ問題となります。ユーザーによって出される要求には不正に構成された入力が含まれている可能性があり、このような入力によってサーバーのセキュリティが侵害される可能性があります。ユーザー要求を処理するサービスは、ユーザー・インターフェースまたはアクセス可能なアプリケーション・プログラミング・インターフェース (API) を提供するシステムです。

Linux デーモンは、始動、停止、または適切に定義されたシステム・イベントへの応答のみを実行することが多いため、これらのデーモンでは通常はリスクはありません。多くの場合、これらのデーモンは root ア



カウントとして実行する必要があります。これにより、デーモンはその他のプロセスを制御し、重要なシステム・イベントに応答できます。ユーザーがアクセス可能なサーバー自体が root として実行されていない限り、root アカウントで実行されているデーモンによって重大な機密漏れが生じることはありません。

Tivoli Netcool/OMNIBus を除き、IBM Intelligent Operations Center のすべての製品サーバーは、システム特権のない ID で構成されています。Tivoli Netcool/OMNIBus には、すべての IBM Intelligent Operations Center ホストおよびサーバーにわたるモニター・サービスおよび管理サービスが含まれています。

表 101 に、Cyber Hygiene の実行後も root アカウントとして実行されるプロセスをリストします。

表 101. root として実行される IBM Intelligent Operations Center 環境のプロセス

サーバー	製品	プロセス名	説明
データ・サーバーおよび管理サーバー	DB2	db2wdog	このデーモン・プロセスは、システム・イベントを受信し、複数の子プロセスに伝搬します。db2wdog プロセスは db2sync プロセスを管理し、ルート・レベル管理を必要とします。
データ・サーバーおよび管理サーバー	DB2	db2chkpwd	このデーモンは、データベースに接続するユーザーまたはアプリケーションのユーザー ID とパスワードを認証します。db2chkpwd プロセスは /etc/shadow パスワード・ファイルを読み取る必要があります。
データ・サーバーおよび管理サーバー	DB2	/opt/IBM/DB2/bin/db2fmcd	このデーモンは障害モニター・コーディネーターとして機能します。すべての DB2 インスタンスをモニターするため、root として実行する必要があります。
データ・サーバーおよび管理サーバー	DB2	/usr/sbin/rcst/bin/rmcd および /usr/sbin/rcst/bin/IBM.ConfigRMd	これらのコマンドは、DB2 の高可用性ソリューションを管理します。高可用性に対応して構成されているサーバーのすべてのデータベースにアクセスできる必要があります。
イベント・サーバー	Lotus Domino 用 IBM Tivoli Monitoring エージェント	kgbagent, kgbclient, kslagent	Lotus Domino サーバー・アクティビティを追跡するため、これらのモニター・エージェントは root として実行する必要があります。
アプリケーション・サーバー、イベント・サーバー、および 管理サーバー	IBM HTTP Server	httpd -d, http -f	Linux では、1024 より小さい番号のポートで listen するために root アクセス権限が必要です。標準 HTTP ポートは 80 から 443 です。IBM Intelligent Operations Center はポート 82 を使用します。httpd -d プロセスと http -f プロセスは root として実行する必要があります。代替構成はすべて、包括的なネットワークおよびセキュリティのポリシーおよび構成の一部としてインストール時に行われます。
データ・サーバー	IBM Tivoli Monitoring エージェント	klzagent, kcawd	モニターおよび管理エージェント・プロセスです。これらのプロセスはオペレーティング・システムとアプリケーションのプロセスおよびリソースをモニターします。
アプリケーション・サーバー	IBM Tivoli Monitoring エージェント	klzagent, kcawd, khtagent, kynagent	モニターおよび管理エージェント・プロセスです。これらのプロセスはオペレーティング・システムとアプリケーションのプロセスおよびリソースをモニターします。
イベント・サーバー	IBM Tivoli Monitoring エージェント	klzagent, kcawd, khtagent, kynagent, kmcrca, kgbagent, kgbstart.sh, kgbclient, kslagent, kmqagent, /opt/IBM/ITM/JRE/1x8266/bin/java	モニターおよび管理エージェント・プロセスです。これらのプロセスはオペレーティング・システムとアプリケーションのプロセスおよびリソースをモニターします。
管理サーバー	IBM Tivoli Monitoring エージェント	cms, kdsmain, KfwServices, klzagent, kcawd, kynagent, /opt/IBM/ITM/1i6263/iw/java/jre/bin/java, /opt/IBM/ITM/1i6263/iw/java/bin/java	モニターおよび管理エージェント・プロセスです。これらのプロセスはオペレーティング・システムとアプリケーションのプロセスおよびリソースをモニターします。

表 101. root として実行される IBM Intelligent Operations Center 環境のプロセス (続き)

サーバー	製品	プロセス名	説明
イベント・サーバー	Tivoli Netcool/OMNIBus	/usr/ibm/common/acsi/jre/bin/java, /opt/IBM/netcool/omnibus/platform/ linux2x26/bin/nco_pad	nco_pad プロセスは、すべてのプロセス・エージェントをモニターするプロセス・エージェント・デーモンです。このデーモンは、システム・リソースへのアクセス権限を必要とします。このプロセス・エージェント・デーモンはユーザー・インターフェースを表示しません。その他のプロセスの管理のみを行います。

## Cyber Hygiene の例外

Cyber Hygiene の実行後に、優先されるセキュリティ構成に関する既知の例外が残ります。

ベスト・プラクティスの設定に例外がない構成が理想的です。ただしほとんどのシステムでは例外があります。このような例外は重大なリスクを生じるものではありませんが、理解していないと問題となることがあります。例えば一部のプログラムは **suid** ビットを設定して実行する必要があります。

セキュリティ管理者は、システムのセキュリティが侵害されているかどうかを確認できるようにするために、例外を理解しておく必要があります。システム管理者はスキャンを実行する際に、マルウェアとは対照的な、意図的な例外について理解できます。

表 102. 優先されるセキュリティ構成における Cyber Hygiene の例外

ぜい弱性	サーバー	インスタンス	説明
GEN000360: GID が Linux のシステム範囲 (0 から 499) の値に設定されている。	データ・サーバー	dasadm1	dasadm1 グループ ID (GID) が 102 に設定されています。これは、DB2 ランタイム・インスタンス ID の管理グループです。このグループは、DB2 がインストールされている場合に自動的に作成されます。

## システム管理者の評価を必要とするファイル権限

Cyber Hygiene は、すべてのファイル権限と所有権における機密漏れに関する変更は行いません。自動変更により一部のシステム機能が動作不能となる可能性があるため、このような機密漏れの一部をシステム管理者が評価および修復する必要があります。

Cyber Hygiene スクリプトは、影響を受ける可能性があるリソースに関する情報をログに記録します。システム管理者は検出内容をレビューし、適切なシステム変更を行うことができます。

検出結果ファイルは各 IBM Intelligent Operations Center サーバーの /var/BA15/CH/results ディレクトリにあります。このファイルの名前は scanrem-combined-log-date-time.log です。タイム・スタンプは、Cyber Hygiene の実行時刻を示します。

381 ページの表 103 に、レビューが必要なぜい弱性と推奨処置を示します。

表 103. システム管理者による評価が必要なぜい弱性

STIGID	説明	重大度	推奨
GEN001220	システム・ディレクトリー内のファイル、アプリケーション、およびディレクトリーは、システム・アカウントまたはアプリケーション・アカウントにより所有されている必要があります。	II	リソースの所有権を確認し、必要に応じて手動で変更するか、または文書に記述します。
GEN001240	システム・ディレクトリー内のファイル、アプリケーション、およびディレクトリーは、システム・グループまたはアプリケーション・グループにより所有されている必要があります。	II	リソースのグループ所有権を確認し、必要に応じて手動で変更するか、または文書に記述します。
GEN001500	/etc/passwd ファイルでユーザーに対してリストされているホーム・ディレクトリーは、ユーザーによって所有されている必要があります。	II	ホーム・ディレクトリーの所有権を確認し、所有権を手動で変更するか、または所有権を変更できない理由を文書に記述します。
GEN001520	/etc/passwd ファイルでユーザーに対してリストされているホーム・ディレクトリーは、そのユーザーの 1 次グループにより所有されている必要があります。	II	ホーム・ディレクトリーのグループ所有権を確認し、グループ所有権を手動で変更するか、または所有権を変更できない理由を文書に記述します。
GEN001560	ホーム・ディレクトリー内の始動ファイル以外のファイルには、750 より大きい権限を設定しないでください。	III	例外がまだ文書に記述されていない場合は、権限を変更します。
GEN002520	パブリック・ディレクトリーは、root アカウントまたはアプリケーション・ユーザー ID により所有されている必要があります。	II	所有権を確認し、適切に割り当てます。
GEN002540	パブリック・ディレクトリーは、root、sys、bin、またはアプリケーション・グループにより所有されている必要があります。	II	グループ所有権を確認し、適切に割り当てます。

## 製品およびコンポーネントのセキュリティ認証

IBM Intelligent Operations Center ソリューションの一部として含まれている製品とコンポーネントの一部は、セキュリティ認証を取得しています。

表 104. IBM Intelligent Operations Center と共にインストールされる製品のセキュリティ認証

製品	コモン・クライテリア		FIPS 140-2		IPV6
	リリース	レベル	リリース	認証済み?	
IBM WebSphere Business Monitor	なし	なし	7.5	はい	はい
IBM Cognos Business Intelligence	10.1.1	なし	なし	なし	はい

表 104. IBM Intelligent Operations Center と共にインストールされる製品のセキュリティー認証 (続き)

製品	コモン・クライテリア		FIPS 140-2		IPV6
	リリース	レベル	リリース	認証済み?	
DB2 Enterprise Server Edition with DB2 Spatial Extender	9.7	EAL4+ALC_FLR.1	9.1 FP2	はい	はい
IBM HTTP Server	7.0.0.19		7.0	はい	はい
Lotus Domino	なし	なし	8.0.1	はい	はい
Lotus Sametime Standard	なし	なし	8.5	はい	はい
Tivoli Access Manager for e-Business	6.0 FP3	EAL3+ALC_FLR.1	6.0	はい	はい
Tivoli Composite Application Manager	なし	なし	なし	なし	はい
Tivoli Directory Integrator	なし	なし	7.0	はい	はい
Tivoli Directory Server	6.2	EAL4+ALC_FLR.1	6.1	はい	はい
Tivoli Identity Manager	5.0	EAL3+ALC_FLR.1	なし	なし	はい
Tivoli Monitoring	なし	なし	6.2.0.1	はい	はい
Tivoli Netcool/Impact	なし	なし	5.1	はい	はい
Tivoli Netcool/OMNIBus and XML probe	7.1	EAL2	すべて	はい	はい
Tivoli Service Request Manager	なし	なし	すべて	はい	はい
WebSphere Application Server Network Deployment	6.1.0.2	EAL4+ALC_FLR.1	すべて	はい	はい
WebSphere Application Server for Tivoli Service Request Manager	6.1.0.2	EAL4+ALC_FLR.1	すべて	はい	はい
WebSphere Message Broker	6.0.0.3	EAL4+ALC_FLR.2 (de)	6.1	はい	はい
WebSphere MQ	6.0.1.1.	EAL4+ALC_FLR.2	すべて	はい	はい
WebSphere Operational Decision Management (Rules Engine)	なし	なし	なし	なし	はい
WebSphere Portal Enable	5.0	EAL2	すべて	はい	はい

FIP 104-2 認証を取得している製品は通常、C および Java 向け IBM Crypto モジュールを採用していることから、この認証を取得しています。これらの製品の認証番号については表 105 を参照してください。

表 105. FIPS 140-2 証明書

モジュール	証明書番号
IBM Crypto for C (V8.0.0)	1433
IBM CryptoLite for Java (V4.2)	910
IBM CryptoLite for C (V4.5)	899
IBM Java JCE 140-2 Cryptographic Module	497
IBM Java JSSE FIPS 140-2 Cryptographic Module	409
IBM SSL Lite for Java	406

## 関連情報:

 コモン・クライテリア: <http://www.commoncriteriaportal.org/>

 Security Evaluations for IBM Products

---

## PDF ライブラリー

このトピックでは、PDF 形式で提供されているインフォメーション・センターの内容へのリンクを示します。

インフォメーション・センターの内容は、印刷しやすいように以下の PDF で提供されています。

- IBM Intelligent Operations Center インフォメーション・センター

---

## 用語集

この用語集には、IBM Intelligent Operations Center の用語および定義が含まれています。

この用語集では以下の相互参照が使用されています。

- 「を参照」は、該当する用語から優先される同義語への参照や、頭字語または省略語から定義済みの完全な形への参照を示します。
- 「も参照」は、関連する用語や対比する用語への参照を示します。

他の IBM 製品の用語集を参照するには、[www.ibm.com/software/globalization/terminology](http://www.ibm.com/software/globalization/terminology) にアクセスしてください (新しいウィンドウで開きます)。

『A』 384 ページの 『B』 384 ページの 『C』 385 ページの 『D』 386 ページの 『E』 386 ページの 『F』 386 ページの 『G』 387 ページの 『H』 387 ページの 『I』 387 ページの 『J』 388 ページの 『K』 388 ページの 『L』 389 ページの 『M』 389 ページの 『N』 389 ページの 『O』 390 ページの 『P』 390 ページの 『R』 391 ページの 『S』 391 ページの 『T』 392 ページの 『U』 393 ページの 『V』 393 ページの 『W』 393 ページの 『X』

## A

### 抽象構文記法 1 (ASN.1) (Abstract Syntax Notation One (ASN.1))

情報データの構文を定義する国際標準。これは、多数の単純データ型を定義し、これらのデータ型を参照したり、データ型の値を指定したりするための記法を指定する。情報を伝送する際のエンコード方法を一切制約することなく、情報の抽象構文を定義する必要がある場合には、常に ASN.1 表記を適用できる。

### アクセス制御リスト (ACL) (access control list (ACL))

コンピューター・セキュリティーにおいて、オブジェクトにアクセスできるすべてのサブジェクトおよびそれらのアクセス権限を識別する、オブジェクトに関連したリスト。

**ACL** アクセス制御リスト (access control list)を参照。

### 管理者権限 (administrator permission)

ポータルのリソースまたはユーザーを作成、構成、および削除するためのアクセス権を与えるために、管理者に付与される権限。この権限は、ユーザー役割グループのメンバーシップによって付与される。

### **集約 KPI (aggregation KPI)**

集約関数を使用して測定基準から計算された KPI 値。

### **アラート (alert)**

イベントまたは重要業績評価指標 (KPI) の状況が変更されたことを通知するメッセージ。

### **アラート・トリガー (alert trigger)**

事前定義された重要業績評価指標 (KPI) 値の変更で、「座標 - アラート」ポートレットにアラート通知が送信される原因となるもの。

**APAR** プログラム診断依頼書 (authorized program analysis report) を参照。

**ASN.1** 抽象構文記法 1 (Abstract Syntax Notation One) を参照。

### **非同期 (asynchronous)**

時間内に同期しないイベント、あるいは定期的または予測可能な時間間隔で発生しないイベントに関する用語。

### **属性 (attribute)**

エンティティを説明する、エンティティの特性または特徴。例えば、従業員の電話番号は、従業員の属性の 1 つ。

### **認証ポータル・ユーザー (authenticated portal user)**

パスワードとユーザー ID が格納されたプロファイルによって認証される、WebSphere Portal 内の包括的グループのメンバーであるユーザー。

### **認証 (authentication)**

コンピューター・システムのユーザーが本人であることを証明するセキュリティ・サービス。このサービスを実装する一般的な手段として、パスワードやデジタル署名などがある。

### **許可 (authorization)**

ユーザー、システム、またはプロセスに、オブジェクト、リソース、または機能への完全なアクセス権限または制限付きのアクセス権限を付与するプロセス。

### **許可権限 (authorization permission)**

グループのメンバーシップに関連付けられたポータル、リソース、またはデータに対するアクセス権限。

### **プログラム診断依頼書 (APAR) (authorized program analysis report (APAR))**

IBM から提供されるプログラムのサポート対象リリースにおける問題点に対する修正の要求。

## **B**

### **基本マップ (base map)**

背景となる参照情報 (地形、道路、ランドマーク、政治的境界など) を描写するマップ。このマップ上に、別のテーマに関する情報が配置される。基本マップは、位置参照に使用され、多くの場合、その構造の一部として測地基準点網を組み込む。

## **C**

### **キャッシュ (cache)**

命令またはデータ、もしくはその両方へのアクセス時間を短縮するために使用されるメモリー。キャッシュ・メモリー内のデータは、通常、より低速で低コストのストレージ内の他の場所 (ディスク上や別のネットワーク・ノード上など) に存在するデータのコピーである。

**CAP** 共通アラート・プロトコル (CAP) (Common Alerting Protocol (CAP)) を参照。



### クラウド・アプリケーション (cloud application)

インターネットを経由したアクセスが可能となるよう拡張されるアプリケーション。クラウド・アプリケーションは、Web アプリケーションと Web サービスをホストする、大規模データ・センターおよび強力なサーバーを使用する。

### 共通アラート・プロトコル (CAP) (Common Alerting Protocol (CAP))

あらゆる種類のネットワークで危険に関する緊急アラートおよび一般警告のすべてを交換するための、単純であるが汎用の形式。

### 共通ウィジェット (common widget)

特定の製品に関連付けられていない、IBM が提供するウィジェット。ウィジェット (widget) も参照。

### 構成 (configuration)

1. システム、サブシステム、またはネットワークのハードウェアとソフトウェアが編成され、相互接続される方法。
2. インストールされている装置、オプション機能、およびプログラム製品を使用できるようにするために、システムに対して記述する処理。カスタマイズ (customization) も参照。

### CSV ファイル (CSV file)

コンマ区切りの値が含まれるテキスト・ファイル。CSV ファイルは、一般に、使用フォーマットが異なるデータベース・システムおよびアプリケーション間でファイルを交換するときに使用される。

### カスタマイズ (customization)

1. ユーザーによるポータル・ページまたはポートレットの変更。WebSphere Portal では、ユーザーはページ・レイアウトを変更し、装置ごとに表示されるポートレットを選択することによって、ポータル・ページをカスタマイズできる。パーソナライゼーション (personalization) も参照。
2. システムにインストールされて使用可能な状態に構成されているソフトウェア・プログラムのデフォルト設定を、必要に応じて変更する過程。構成 (configuration) も参照。

## D

### ダッシュボード (dashboard)

1. ビジネス・データをグラフィカルに示す 1 つ以上のウィジェットを含むことが可能な Web ページ。
2. 各種のソースから取得したデータを統合し、関連情報やコンテキスト情報を一括表示するためのインターフェース。

### データ・アクセス権限 (data access permission)

特定のカテゴリーのデータ (例えば、医療および公衆衛生データ、環境データ) に対するアクセス権限。このアクセス権限は、データ・カテゴリー・グループに関連付けられる。

### データ・カテゴリー・グループ (data category group)

特定のカテゴリーのデータ (例えば、医療および公衆衛生データ、環境データ) に対するアクセス権限を持つメンバーからなるグループ。データに対する適切なレベルのアクセス権限をユーザーに与えるために、データ・カテゴリー・グループのメンバーシップがユーザーに割り当てられる。各ユーザーは、適切なグループ (複数可) のメンバーとして追加される。

## ドメイン (domain)

主要な事業の個々の部門。通常は、組織構造および関係者が有する専門知識に合わせて分かれている。例えば、都市行政機関は、運輸、水道、公衆安全のそれぞれを扱う部門に分かれている。

## E

**EAR** エンタープライズ・アーカイブ (enterprise archive)を参照。

**EJB** Enterprise JavaBeans を参照。

### エンタープライズ・アーカイブ (EAR) (enterprise archive (EAR))

Java EE 標準で定義され、Java EE アプリケーションを Java EE アプリケーション・サーバーにデプロイするために使用される、特殊なタイプの JAR ファイル。EAR ファイルには、EJB コンポーネント、デプロイメント記述子、個々の Web アプリケーション用の Web アーカイブ (WAR) ファイルが含まれる。Java アーカイブ (Java archive) も参照。

### Enterprise JavaBeans (EJB)

オブジェクト指向の分散型エンタープライズ・レベル・アプリケーション (Java EE) の開発とデプロイメントのため、Sun Microsystems によって定義されたコンポーネント・アーキテクチャー。

**event** 特定の場所と時間で起きた、重要な事象の発生。 インシデント (incident) も参照。

### イベント相関 (event correlation)

パターン、一般的な原因、および根本原因を特定するためにイベント・データを分析する過程。イベント相関は、事前定義のルールを使用し、事前定義の関係と照合して、事前定義の状態について着信イベントを分析する。

### 式 KPI (expression KPI)

他の KPI の値から値が計算される KPI。

### Extensible Markup Language (XML)

Standard Generalized Markup Language (SGML) に基づいたマークアップ言語を定義する標準メタ言語。

## F

### フィルター・フォーム (filter form)

マップとリストに表示されるコンテンツを選択するために使用できるフォーム。

## G

### GDDM

図形データ表示管理プログラム (GDDM) (Graphical Data Display Manager (GDDM)) を参照。

### 地理情報システム (GIS) (geographical information system (GIS))

地理的特徴に関する空間情報の作成と分析に使用される、オブジェクト、データ、およびアプリケーションの複合システム。

### 地理空間 (geospatial)

地球の地理的特性に関する用語。

**GIS** 地理情報システム (geographical information system) を参照。

### 図形データ表示管理プログラム (GDDM) (Graphical Data Display Manager (GDDM))

ディスプレイまたはプリンターに出力するテキストおよびグラフィックスを定義および表示する、IBM コンピューター・グラフィックス・システム。

## グループ (group)

保護リソースに対するアクセス権限を共有することができるユーザーの集合。

## H

### ヒープ (heap)

Java プログラミングにおいて、Java 仮想マシン (JVM) が実行時に Java オブジェクトを格納するために使用するメモリー・ブロック。Java ヒープ・メモリーは、使用されなくなった Java オブジェクトを自動的に割り振り解除するガーベッジ・コレクターによって管理される。

### 吹き出しヘルプ (hover help)

グラフィカル・ユーザー・インターフェース (GUI) の項目 (アイコン、フィールド、テキスト・ストリングなど) の上にカーソルを移動することによって表示できる、説明テキスト。吹き出しヘルプにはリッチ・テキストとリンクを組み込むことができる。

## I

### インシデント (incident)

サービスの標準操作には含まれていないイベントのうち、サービス品質やユーザーの生産性に混乱または低下をもたらす可能性のあるもの。イベント (event) も参照。

### 統合 (integration)

独立したソフトウェアのコンポーネントが 1 つの実行可能な総体に組み合わされる、ソフトウェア開発の作業。

### ISO モデル (ISO model)

国際標準化機構 (ISO) の認可を受けた、データ通信に関するルールのセット。ISO プロトコルにより、別のベンダーから提供されたシステムを接続し、通信させることが可能となる。それらはオープン・システム間相互接続 (OSI) 標準の基本である。

## J

**J2EE** Java Platform, Enterprise Edition を参照。

**JAR** Java アーカイブ (Java archive) を参照。

### Java アーカイブ (JAR) (Java archive (JAR))

Java プログラムをインストールおよび実行するために必要なすべてのリソースを単一ファイルで保管するための、圧縮されたファイル・フォーマット。エンタープライズ・アーカイブ (enterprise archive) も参照。

### Java EE

Java Platform, Enterprise Edition を参照。

### Java Naming and Directory Interface (JNDI)

Java プラットフォームの拡張により、異機種の命名サービスとディレクトリー・サービス用の標準インターフェースが提供される。

### Java Platform, Enterprise Edition (J2EE, Java EE)

Oracle によって定義された、エンタープライズ・アプリケーションの開発とデプロイを行うための環境。Java EE プラットフォームは、多層 Web ベース・アプリケーションを開発するための機能を提供する、一連のサービス、アプリケーション・プログラミング・インターフェース (API)、およびプロトコルから構成されます。(Sun)

### **JavaScript Object Notation (JSON)**

JavaScript のオブジェクト・リテラル表記に基づいた、軽量のデータ交換フォーマット。JSON はプログラミング言語に対して中立であるが、C、C++、C#、Java、JavaScript、Perl、Python などの言語での規則を使用する。

### **Java 仮想マシン (JVM) (Java virtual machine (JVM))**

コンパイル済み Java コード (アプレットおよびアプリケーション) を実行するプロセッサのソフトウェア実装。

**JNDI** Java Naming and Directory Interface を参照。

**JSON** JavaScript Object Notation を参照。

**JVM** Java 仮想マシン (Java virtual machine) を参照。

## **K**

### **鍵穴マークアップ言語 (KML) (keyhole markup language (KML))**

地理的特性 (点、線、イメージ、ポリゴンなど) のモデリングと保管のための XML 文法およびファイル・フォーマット。

### **重要業績評価指標 (KPI) (key performance indicator (KPI))**

ビジネス・プロセスの重要成功要因を追跡するために設計された数量化可能な指標。

**KML** 鍵穴マークアップ言語 (KML) (keyhole markup language (KML)) を参照。

**KPI** 重要業績評価指標 (key performance indicator) を参照。

### **KPI モデル (KPI model)**

KPI コンテキストを含むモニター・モデルの一部。KPI コンテキストには、重要業績評価指標と、それに関連するトリガーおよびイベントが含まれる。

### **KPI ポリシー (KPI policy)**

着信イベントが KPI イベントの更新であるかどうかを判別し、パラメーターに応じて KPI 更新またはアラートを生成する処理のために、そのイベントを送信するポリシー。

## **L**

### **緯度 (latitude)**

地球の赤道を基準とした、北または南の地点の角距離。通常は度数と分数で表現される。

### **レイヤー (layer)**

追加の地理空間情報を提供するためにマップ上に配置できるオーバーレイ。

**LDAP** Lightweight Directory Access Protocol を参照。

### **LDAP Directory Interchange Format (LDIF)**

ディレクトリー情報のほか、ディレクトリーに適用する必要がある変更 (LDAP を使用しているディレクトリー・サーバーの間で交換できるディレクトリー情報など) の記述に使用するファイル形式。

**LDIF** LDAP Directory Interchange Format を参照。

### **サービス・レベル (LOS) (level of service (LOS))**

運輸業界の交通技術者が、運輸インフラストラクチャーの要素の効率性を算出するために使用する、量的な指標。この指標は、「Highway Capacity Manual」に定義されている交通運用条件を記述する。

### **Lightweight Directory Access Protocol (LDAP)**

TCP/IP を使用して X.500 モデルをサポートするディレクトリーへのアクセスを提供し、より複雑な X.500 ディレクトリー・アクセス・プロトコル (DAP) のリソース要件に制約されない、オープン・プロトコル。例えば、LDAP を使用してインターネットやイントラネット・ディレクトリー内の人、組織、およびその他のリソースの場所を探索できる。

### **線形参照 (linear reference)**

道路沿い (通常は路肩) にあり、経路でのその位置を示すロケーション参照マーカー。そのマーカーの一例には、マイル標がある。

### **ロケーション・マップ (location map)**

IBM Intelligent Operations Center 内で定義されている対話式エリアを含むマップまたはプラン。これらの 1 つ以上のエリアをイベントに関連付けることができる。例えば、主要なスポーツ・スタジアムの観客席エリアの図を定義し、発生したイベントを該当するエリアに関連付けることができる。

### **論理ゾーン (logical zone)**

地理的エリア内の資産またはイベントの論理グループ。

### **経度 (longitude)**

イングランドのグリニッジ天文台を経線とした、東または西の地点の角距離。通常は度数と分数で表現される。

**LOS** サービス・レベル (level of service) を参照。

## **M**

### **モニター・コンテキスト・インスタンス (monitoring context instance)**

モニター・コンテキスト内で特定の時点に収集される IBM WebSphere Business Monitor の情報。

### **モニター・モデル (monitor model)**

ビジネス・モデルのビジネス・パフォーマンス管理面を記述するモデル。これには、リアルタイム・ビジネス・モニターに必要なイベント、ビジネス・メトリック、および重要業績評価指標 (KPI) などが含まれる。

## **N**

### **ネストされた KPI (nested KPI)**

親 KPI の子として定義された KPI。

## **O**

### **オントロジー (ontology)**

対象の何らかの分野に存在し得るオブジェクト、概念、その他のエンティティと、それらの間の関係を表現するための、明示的で一定の形式にかなった仕様。

### **運用ビュー (operations view)**

運用レベルでの包括的な情報提供および対話の促進に協力できるポートレットが含まれる Web ページ。現行イベントをモニターし、将来のイベントを計画するために使用される。

**OWL** Web オントロジー言語 (OWL) (Web ontology language (OWL)) を参照。

## P

### ページ (page)

ポータル環境で、1 つ以上のポートレットを含むインターフェース・エレメント。

### パーソナライゼーション (personalization)

ビジネス・ルールとユーザー・プロファイル情報に基づいて、特定のユーザー向けの情報を使用可能にするプロセス。カスタマイズ (customization) も参照。

### プラグイン (plug-in)

既存のプログラム、アプリケーション、またはインターフェースに機能を追加する、個別にインストール可能なソフトウェア・モジュール。

**PMR** 問題管理記録 (problem management record) を参照。

### ポリゴン (polygon)

GDDM 機能において、ある領域を囲む一連の隣接した直線。

### ポータル (portal)

さまざまな情報、アプリケーション、ユーザーにアクセスできる安全な単一アクセス・ポイント。カスタマイズとパーソナライズが可能。

### ポートレット (portlet)

ポータルのコンテキストに示される特定の情報またはサービスを提供する Web アプリケーションの一部である、再使用可能コンポーネント。

### 問題管理レコード (PMR) ((problem management record (PMR))

IBM サポート機構内の番号であり、お客様とのサービス・インシデントを表す。

## R

**RDF** Resource Description Framework (RDF) を参照。

### Really Simple Syndication (RSS)

Really Simple Syndication 仕様 (RSS 2.0) に基づく、シンジケーション Web コンテンツの XML ファイル・フォーマット。RSS XML ファイル・フォーマットは、RSS フィードを提供している Web サイトにインターネット・ユーザーがサブスクライブするために使用される。

### Representational State Transfer (REST)

ワールド・ワイド・ウェブなどの分散ハイパーメディア・システム用のソフトウェア・アーキテクチャー・スタイル。この用語は、SOAP などの追加メッセージング層を使用せずに、HTTP 経由で XML (または YAML、JSON、プレーン・テキスト) を使用する、単純なインターフェースを指すときにも使用されることが多い。

### リソース・バンドル (resource bundle)

1. ストア・ページのテキストが含まれるクラス。Java PropertyResourceBundle API に従いバンドル・ファイルが作成され、アクセスされます。
2. プログラムのローカライズで使用するデータ (リソース) にキー値のマッピングを提供する、構造化されたデータの集合。値は一般的にストリングであるが、値自体を構造化データにすることもできる。

### Resource Description Framework (RDF)

Web 上の情報を表すためのフレームワーク。

**REST** Representational State Transfer を参照。

**RSS** Really Simple Syndication を参照。



## S

### Secure Sockets Layer (SSL)

通信のプライバシーを提供するセキュリティー・プロトコル。SSL を使用することにより、クライアント/サーバー・アプリケーションは、盗聴、不正アクセス、およびメッセージ偽造を防止するように設計された方法で通信できる。

**SGML** Standard Generalized Markup Language を参照。

### シェイプ・ファイル (shape file)

地理情報システム・ソフトウェアのデジタル・ファイル・フォーマット。

### シングル・サインオン (SSO) (single sign-on)

ユーザー ID とパスワードを 1 回入力するだけで、複数のシステムやアプリケーションにアクセスできる認証プロセス。

### スキン (skin)

グラフィカル・ユーザー・インターフェースの外観をその機能に影響を与えずに変更するための、インターフェースの変更可能なエレメント。

**SOAP** 非集中分散環境で情報を交換するための、軽量の XML ベースのプロトコル。SOAP を使用して、インターネットを介して情報をクエリーしたり戻したり、サービスを起動することが可能。Web サービス (web service) も参照。

### ソリューション (solution)

お客様の特定の問題またはプロジェクトを扱う製品の組み合わせ。

### SPARQL

さまざまなデータ・ソースにまたがる照会を記述するための RDF 向け照会言語。SPARQL 照会言語の構文とセマンティックは W3 仕様により定義されている。

**SSL** セキュア・ソケット・レイヤー (Secure Sockets Layer) を参照。

**SSO** シングル・サインオン (single sign-on) を参照。

### Standard Generalized Markup Language (SGML)

ISO 8879 標準に基づくマークアップ言語を定義するための標準メタ言語。SGML では、情報の表示よりも情報の構造化に焦点を当て、表示から構造と内容を分離している。電子媒体間での文書の交換も容易にする。

### 標準操作手順 (Standard Operating Procedure)

特定の事前定義の条件を満たすパラメーターを持つイベントが発生した場合にトリガーされる一連のアクティビティを定義する手順。

### 標準操作手順の選択マトリックス (Standard Operating Procedure selection matrix)

特定のイベントについて標準操作手順を開始するかどうかを決定するイベント・パラメーターの固有のセットを含むマトリックス。

### システム・プロパティー・テーブル (system properties table)

IBM Intelligent Operations Center のシステム全体の構成データを格納するテーブル。

## T

**TAI** トラスト・アソシエーション・インターセプター (trust association interceptor) を参照。

### TCP/IP

TCP/IP プロトコル (Transmission Control Protocol/Internet Protocol) を参照。

### テーマ (theme)

プレースに特定の形状をもたらすスタイル・エレメント。ポータルは、仮想壁紙と同様、プレースの作成時に選択可能ないくつかのテーマを提供する。

### TCP/IP プロトコル (TCP/IP) (Transmission Control Protocol/Internet Protocol (TCP/IP))

異なるタイプの相互接続ネットワーク上のアプリケーション間で信頼できるエンドツーエンド接続を提供する、業界標準の一般通信プロトコルのセット。

### トリガー (trigger)

発生を検出し、それに応じて追加の処理を引き起こすことができるメカニズム。

### トラスト・アソシエーション・インターセプター (TAI) (trust association interceptor (TAI))

プロキシ・サーバーによって受信されたすべての要求の信頼性を製品環境で検証するためのメカニズム。検証の手法は、プロキシ・サーバーとインターセプターによって合意される。

## U

### Uniform Resource Identifier (URI)

1. テキストのページ、ビデオや音声クリップ、静止画像やアニメーション画像、プログラムなど、Web 上のコンテンツを識別するために使用される固有アドレス。URI の最も一般的な形式は Web ページ・アドレスで、これは Uniform Resource Locator (URL) と呼ばれる URI の特定の形式またはサブセットである。通常、URI は、リソースへのアクセス方法、リソースが存在するコンピューター、およびコンピューター上のリソースの名前 (ファイル名) について記述する。
2. 抽象的または物理的なリソースを識別するための簡潔な文字ストリング。

### Uniform Resource Locator (URL)

インターネットなどのネットワーク内でアクセス可能な情報リソースの固有アドレス。URL には、情報リソースへのアクセスに使用されるプロトコルの省略名、および情報リソースを見つけるためにプロトコルによって使用される情報が含まれる。

**URI** Uniform Resource Identifier を参照。

**URL** Uniform Resource Locator を参照。

### ユーザー管理者 (user administrator)

新規ユーザーを追加し、適切な権限が設定された役割ベースの許可グループのメンバーシップをユーザーに付与することでセキュリティーを確保する管理者。

### ユーザー許可 (user permission)

ポータル・リソースを表示および操作するためのアクセス権限を与えるために、ユーザーに付与される権限。この権限は、ユーザー役割グループのメンバーシップによって付与される。

### ユーザー・プロファイル (user profile)

ユーザーのログオン時に取得される、ユーザー ID、ユーザー名、パスワード、アクセス権限などの属性情報が含まれているユーザーの記述。

### ユーザー役割グループ (user role group)

ソリューションへの適切なレベルのアクセス権限を新規ユーザーに与えるために、メンバーシップを割り当てるグループ。新規ユーザーは、それぞれ適切な役割グループのメンバーとして追加される。役割グループごとに異なる権限レベルが関連付けられている。

## V

### 仮想ネットワーク・コンピューティング (VNC) (Virtual Network Computing (VNC))

リモート・フレーム・バッファ (RFB) プロトコルを使用して別のコンピューターをリモート側で制御する、グラフィカル・デスクトップ共有システム。ネットワーク経由で、あるコンピューターから別のコンピューターにキーボード・イベントとマウス・イベントを伝送し、グラフィカル画面の更新を反対方向に中継する。

VNC 仮想ネットワーク・コンピューティング (Virtual Network Computing)を参照。

## W

### Web Map Service (WMS)

マップ・サーバーが GIS データベースのデータを使用して生成した地理空間情報を参照するマップ・イメージをインターネットで提供するための標準プロトコル。この仕様は、オープン地理空間コンソーシアムによって開発され、1999 年に初めて公開された。

### Web オントロジー言語 (OWL) (Web ontology language (OWL))

語彙中の用語の意味とそれらの用語間の関係を明示的に表すために使用される言語。人間に内容のみを表示する場合とは対照的に、OWL は、文書に含まれる情報をアプリケーションで処理する場合に使用される。

### Web サービス (Web service)

標準のネットワーク・プロトコルを使用して、ネットワーク経由で公開、ディスカバー、および呼び出しを行うことのできる、自己完結型で自己記述型のモジュラー・アプリケーション。通常、データのタグ付けには XML、データの転送には SOAP、使用可能なサービスの記述には WSDL、使用可能なサービスのリスト作成には UDDI が使用される。SOAP、Web サービス記述言語 (WSDL) (Web Service Definition Language (WSDL)) も参照。

### Web サービス記述言語 (WSDL) (Web Service Definition Language (WSDL))

ドキュメント指向またはプロシージャー指向のいずれかの情報を含むメッセージを操作するエンドポイントのセットとして、ネットワーク・サービスを記述するための XML ベースの仕様。Web サービス (web service) も参照。

### ウィジェット (widget)

ボタン、スクロール・バー、制御域、テキスト編集域などの、再使用可能なユーザー・インターフェース・コンポーネント。キーボードまたはマウスからの入力を受信し、アプリケーションまたは別のウィジェットと通信することができる。共通ウィジェット (common widget) も参照。

WMS Web Map Service (WMS) を参照。

WO 作業指示書 (work order) を参照。

### ワークフロー (workflow)

特定の状況に適した、特定のアクションのセット。例えば、緊急応答システムに接続するなど、適切なワークフローをトリガーするために、ソリューションをカスタマイズすることができる。

### 作業指示書 (WO) (work order (WO))

実行する必要がある作業に関する情報を含むレコード。

WSDL Web サービス記述言語 (Web Service Definition Language) を参照。

## X

XML Extensible Markup Language を参照。

## XML スキーマ (XML schema)

どのエレメントがどの組み合わせで許可されているかを示すことによって、XML ファイルのコンテンツを記述および制約するためのメカニズム。XML スキーマは、文書タイプ定義 (DTD) に代わるものであり、データの入力、継承、表示における機能を拡張するために使用できる。

---

## 製品に関する追加情報

以下の追加リソースは、オンラインで参照できます。

### WebSphere Portal

- WebSphere Portal 製品サポート・ページ: [http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere\\_Portal](http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere_Portal)
- WebSphere Portal 情報ライブラリー: <http://www.ibm.com/software/genservers/portal/library/>
- WebSphere Portal Wiki: <http://www.lotus.com/ldd/portalwiki.nsf>

### WebSphere Application Server

- WebSphere Application Server 製品サポート・ページ: <http://www.ibm.com/software/webservers/appserv/was/support/>
- WebSphere Application Server 情報ライブラリー: <http://www.ibm.com/software/webservers/appserv/was/library/index.html>
- WebSphere Application Server 7.0.x インフォメーション・センター: <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>

### インフォメーション・センター

- Cognos Business Intelligence インフォメーション・センター: <http://publib.boulder.ibm.com/infocenter/cbi/v10r1m1/index.jsp>
- DB2 インフォメーション・センター: <http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp>
- IBM ILOG CPLEX Optimization Studio インフォメーション・センター: <http://pic.dhe.ibm.com/infocenter/cosinfoc/v12r4/index.jsp>
- Lotus Domino インフォメーション・センター: <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>
- Lotus Notes インフォメーション・センター: <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>
- Lotus Sametime Standard インフォメーション・センター: <http://publib.boulder.ibm.com/infocenter/sametime/v8r5/index.jsp>
- Rational Application Developer インフォメーション・センター: [http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=/com.ibm.rad.legal.doc/helpindex\\_rad.html](http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=/com.ibm.rad.legal.doc/helpindex_rad.html)
- Tivoli Access Manager インフォメーション・センター: <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Tivoli Composite Application Manager インフォメーション・センター: <http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp>
- Tivoli Directory Integrator インフォメーション・センター: [http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDS.doc\\_7.1/welcome.htm](http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDS.doc_7.1/welcome.htm)
- Tivoli Directory Server インフォメーション・センター: <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>

- Tivoli Identity Manager インフォメーション・センター: <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml>
- Tivoli Netcool/Impact インフォメーション・センター: <http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcoolimpact.doc5.1.1/welcome.html>
- Tivoli Netcool/OMNIBus インフォメーション・センター: [http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcool\\_OMNIBus.doc\\_7.3.1/omnibus/wip/welcome.htm](http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm)
- Tivoli Service Request Manager インフォメーション・センター: [http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=/com.ibm.srm.doc/srm\\_welcome.htm](http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=/com.ibm.srm.doc/srm_welcome.htm)
- IBM WebSphere Business Monitor インフォメーション・センター: <http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r0mx/index.jsp?topic=/com.ibm.btools.help.monitor.doc/home/home.html>
- WebSphere Message Broker インフォメーション・センター: <http://publib.boulder.ibm.com/infocenter/wmbhelp/v8r0m0/index.jsp>
- WebSphere MQ インフォメーション・センター: <http://publib.boulder.ibm.com/infocenter/wmqv7/v7r1/index.jsp>
- WebSphere Operational Decision Management インフォメーション・センター: <http://pic.dhe.ibm.com/infocenter/dmanager/v7r5/index.jsp>

## Redbooks

- Redbooks Domain: <http://www.redbooks.ibm.com/>

## その他の Web リソース

- Tivoli トレーニングおよび認定: <http://www.ibm.com/software/tivoli/education/>
- OASIS 共通アラート・プロトコル・バージョン 1.2 <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>
- Red Hat Web サイト: <http://www.redhat.com/>

### 関連概念:

2 ページの『対象読者』

このインフォメーション・センターは、IBM Intelligent Operations Center の使用、インストール、管理、および保守を行う担当者を対象としています。また、ソリューションのカスタマイズと、IBM Intelligent Operations Center が必要とする外部基本システムの統合に関する実装資料も含まれています。

---

## 著作権表示および商標

### 著作権表示

© Copyright IBM Corporation 2011, 2012. All rights reserved. IBM プログラムを使用するための契約条件に従うことを条件に、使用することができます。いかなる形式または手段（電子的、機械的、磁氣的、光学的、科学的、手動またはその他の形式/手段を含む。）であっても、IBM Corporation の書面による事前の許諾なしに、本書のいかなる部分も、複製、送信、複写、検索システムへの記録、または任意のコンピュータ言語への変換を行うことはできません。IBM Corporation は、お客様ご自身が使用する目的でハードコピーまたは機械可読形式の文書の複製物を作成する制限された権利を許諾しますが、その複製物にはすべて、IBM Corporation の著作権表示を付するものとします。著作権に基づくその他の権利は、IBM Corporation の書面による事前の許諾なしに付与されることはありません。この文書は、生産的な使用を意図しておらず、いかなる保証もなしに特定物として現存するままの状態を提供されます。本書には、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含め、いかなる保証も適用されません。

---

## 商標

IBM、IBM ロゴおよび [ibm.com](http://ibm.com) は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、<http://www.ibm.com/legal/copytrade.shtml> をご覧ください。

Microsoft、Windows および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Pentium は Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Adobe、PostScript は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。



---

## 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510

東京都中央区日本橋箱崎町19番21号

日本アイ・ビー・エム株式会社

法務・知的財産

知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation

Department T81B F6/Building 503

4205 S. Miami Boulevard

Durham NC 27709-9990

U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態を提供されるものであり、いかなる保証も提供されません。IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

---

## 商標

IBM、IBM ロゴおよび [ibm.com](http://ibm.com) は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、<http://www.ibm.com/legal/copytrade.shtml> をご覧ください。

Microsoft、Windows および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Pentium は Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Adobe、PostScript は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。



---

## 索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

### [サ行]

商標 395

新機能

概要 9

### [タ行]

特記事項 395

### [ヤ行]

用語集 383









Printed in Japan