IBM SecureWay Policy Director
管理の手引き

バージョン 3.0

IBM SecureWay Policy Director
管理の手引き

バージョン 3.0

お願い

本書、および本書で記述されている製品をご使用になる前に、 309ページの『付録B. 特記事項』を必ずお読みください。

本書は、 IBM® FirstSecure Secureway® Policy Director™ 製品のバージョン 3、リリース 0、モディフィケーション 0 に適用されます。また、改訂版などで特に断りのない限り、これ以降のすべてのリリースにも適用されます。

本書は、IBM SecureWay Global Sign-On™ のバージョン 2、リリース 2、モディフィケーション 200 に代わる資料です。

本マニュアルについてご意見やご感想がありましたら

`http://www.ibm.com/jp/manuals/main/mail.html`

からお送りください。今後の参考にさせていただきます。
なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

`http://www.infocr.co.jp/ifc/books/`

をご覧ください。（URL は、変更になる場合があります）

原　典： VPOL–ADMI–00
IBM SecureWay Policy Director
Version 3.0
Administration Guide

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 1999.10

この文書では、平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財）日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

目次

本書について

本書は、IBM® SecureWay® Policy Director™ について説明します。説明の内容は次のとおりです。

- Policy Director の概念。認証、許可、クリデンシャルの取得など
- 管理コンソールを使用する一般的な管理タスク
- WebSEAL® 管理
- NetSEAL® 管理
- NetSEAT® 管理
- 管理リソース (**ivadmin** コマンド)

本書の対象読者

本書は、Policy Director のユーザー、グループ、GSO リソース、GSO リソース・グループ、プロキシー・ユーザー、アクセス制御リストと許可、および、オブジェクト・スペースを管理する管理者を対象として作成されています。

Policy Director の管理者は、認証、許可、クリデンシャルの取得についても管理する必要があり、これらのプロセスについての知識がなければなりません。

また、管理者は、 IBM 分散コンピューティング環境 (DCE™) と IBM SecureWay Directory の Lightweight Directory Access ProtocoL (LDAP™) の管理について事前に理解している必要があります。 IBM SecureWay Directory および IBM 分散コンピューティング環境サーバーは Policy Director によって使用され、 Policy Director 製品に組み込まれています。

本書の編成

本書は以下のように編成されています。

- 第 1 章から第 3 章では、Policy Director の概念について説明し、1ページの『第1章 Policy Director の紹介』、17ページの『第2章 認証およびクリデンシャルの取得』、および 37ページの『第3章 許可について』というように Policy Director の概要を示していきます。
- 第 4 章から第 12 章では、次のように一般的な Policy Directory 管理タスクを説明します。
  - 57ページの『第4章 管理コンソールの紹介』
  - 71ページの『第5章 ユーザー・アカウントとグループの管理』
  - 79ページの『第6章 GSO リソース、リソース・グループ、およびリソース・クリデンシャルの管理』
  - 85ページの『第7章 アクセス制御について』
  - 113ページの『第8章 アクセス制御の適用』
  - 119ページの『第9章 プロキシー・ユーザーの管理』
  - 129ページの『第10章 Policy Director サーバーの管理』
  - 139ページの『第11章 許可サービスの管理』
  - 151ページの『第12章 サーバー活動のログ記録と監査』

第 13 章から第 16 章では、次のように WebSEAL 管理について説明します。
- 165ページの『第13章 WebSEAL: 認証の設定』
- 185ページの『第14章 WebSEAL: 一般管理タスク』
- 195ページの『第15章 WebSEAL: スマート接合管理』
- 225ページの『第16章 WebSEAL: アプリケーションの統合』

第 17 章と第 18 章では次の NetSEAL 管理のトピックを取り上げます。
- 235ページの『第17章 NetSEAL: 概説』
- 249ページの『第18章 NetSEAL: 一般管理タスク』

第 19 章から 第 21 章では、NetSEAT 管理について説明します。
- 259ページの『第19章 NetSEAT: 概要』
- 265ページの『第20章 NetSEAT: 一般管理タスク』
- 281ページの『第21章 NetSEAT: ディレクトリー・サービス・ブローカー』

本章には、285ページの『付録A. ivadmin を使用した Policy Director 管理』および 309ページの『付録B. 特記事項』という付録が付いています。

本書で使用する規則

本書では、次の表記規則を使用します。

表記規則	意味
太字	メニュー名、メニュー選択項目、項目フィールド、アイコン、フォルダー、リスト・ボックス、アクション・ボタン、押しボタン、ラジオ・ボタン、スピン・ボタン、およびチェック・ボックスなどのユーザー・インターフェース・エレメント。太字の強調表示は、注記や注意にも使用されます。
モノスペース	構文、サンプル・コード、およびユーザーが入力しなければならないテキスト。
イタリック	Policy Director に関連のある特殊な用語が最初に出てきた場合と、その用語を強調する場合。
→	メニューからの一連の選択を示します。たとえば、**File → Run** を選択するは、 **File** をクリックした後で **Run** をクリックすることを示します。

西暦 2000 年対応

本書に出てくる製品は西暦 2000 年対応です。すなわち、本製品の資料に従って使用した場合、20 世紀から 21 世紀の範囲内の日付データの処理、提供、受け取りを正しく行うことができます。ただし、製品と共に使用されるすべての製品 (ハードウェア、ソフトウェア、およびファームウェアなど) が、正確な日付データを正しく交換できることが必要です。

サービスとサポート

IBM SecureWay FirstSecure のオファリングに含まれる全製品のサービスおよびサポートについては、IBM にご連絡ください。これらの製品の中には、IBM 以外のサポートを参照しているものもあります。そのような製品を FirstSecure のオファリングの一部として入手された場合、サービスとサポートに関しては IBM にお尋ねください。

前提条件と関連情報

Policy Director の前提条件と関連製品についての詳細は、以下の資料を参照してください。

IBM SecureWay Policy Director

PDF 形式の資料: 以下の資料は Policy Director の関連資料で、 *IBM SecureWay Policy Director Version 3.0* CD の /doc で PDF 形式で入手できます。

- 本書、*IBM SecureWay Policy Director 管理の手引き、バージョン 3.0*
- *IBM SecureWay Policy Director Programming Guide and Reference, Version 3.0*

印刷出力形式の資料: 以下の資料も Policy Director の関連資料で、ハードコピー版として、および製品パッケージと一緒に入手できます。

IBM SecureWay Policy Director Up and Running, Version 3.0 (SCT6-3KNA-00)

IBM SecureWay FirstSecure

以下の資料は IBM SecureWay FirstSecure に関連した資料です。

- *IBM SecureWay FirstSecure Planning and Integration, Version 2.0 (S564-8D11-00)*

  本書は、 FirstSecure そのものと FirstSecure を構成する製品について説明しています。本書は、あらゆる IBM SecureWay 製品の使用計画作成を開始する場合に利用できます。

IBM 分散コンピューティング環境

以下の資料は、DCE のインストール方法について説明する資料で、 IBM SecureWay Policy Director Security Services CD の /doc、または DCE Web サイトのどちらからでも PDF 形式で入手できます。

IBM DCE for Windows NT

IBM Distributed Computing Environment for Windows NT Quick Beginnings, Version 2.2。次の Web アドレスで入手できます。

`http://www.software.ibm.com/network/dce/library/publications/dcent.html`

本書は DCE for Windows NT、バージョン 2.2 について説明し、この製品についての計画の作成方法と、インストールおよび構成の方法について説明します。

IBM DCE for AIX

IBM Distributed Computing for AIX Quick Beginnings Version 2.2。次の Web アドレスで入手できます。

`http://www.software.ibm.com/network/dce/library/publications/dceaix.html`

本書は、DCE for AIX、バージョン 2.2 (DCE 2.2 for AIX) について説明し、この製品についての計画の作成方法と、インストールおよび構成の方法について説明します。

Transarc DCE for Solaris

次の Web アドレスで *Transarc DCE Version 2.0 Release Notes* および *Installation and Configuration Guide* が入手できます。

http://www.transarc.com/Library/documentation/dce/2.0/index.html

Transarc DCE Version 2.0 Release Notes には、 Transarc DCE ソフトウェアと資料に関する次の情報が記載されています。

- OSF DCE と DCE DFS 製品の違い
- DCE DFS のバージョン 2,0 とバージョン 1.1 の違い
- DCE DFS に関連した、既知の問題と制限

Installation and Configuration Guide は、DCE DFS バージョン 2.0 製品のインストール、構成、およびアップグレードについて説明します。

IBM SecureWay Directory

IBM SecureWay Directory に関して次の資料も用意されています。

- *IBM SecureWay Directory Installation and Configuration, Version 3.1.1*

  サポートされている各オペレーティング・システムごとに、それぞれ別個のバージョンがあります。
- *IBM SecureWay Directory Client SDK Programming Reference*
- *IBM SecureWay Directory Server Plug-ins Reference*

以下の資料には、 IBM SecureWay Directory (LDAP) に関するインストールと構成の説明が記載されています。

- *IBM SecureWay Directory Installation and Configuration, Version 3.1.1*

  サポートされている各オペレーティング・システムごとに、HTML 形式でそれぞれ別個のバージョンがあります。個々のオペレーティング・システムの資料は該当の CD に入っています。資料が入っている CD は次のとおりです。
  - *IBM SecureWay Directory Version 3.11 for NT*
  - *IBM SecureWay Directory Version 3.11 for AIX*
  - *IBM SecureWay Directory Version 3.11 for Solaris*

IBM SecureWay Directory に関して以下の資料も用意されています。

- *IBM SecureWay Directory Client SDK Programming Reference*
- *IBM SecureWay Directory Server Plug-ins Reference*

お客様のご意見の送り先

お客様のご意見は、正確で高品質な資料を提供するために重要です。本書またはその他の IBM SecureWay Policy Director の資料に関して何かご意見があれば、弊社の Policy Director ホーム・ページにアクセスしてください。

http://www.ibm.com/software/security/policy/library

このホーム・ページには、お客様のご意見を記入し、送付できるフィードバック・ページがあります。また、Policy Director の最新情報もここにあります。

他の IBM SecureWay FirstSecure 製品の更新に関する情報は、以下の Web アドレスで入手できます。

http: //www.ibm.com/software/security/firstsecure/library

第1章 Policy Director の紹介

IBM SecureWay Policy Director (Policy Director) は、法人組織用の Web、クライアント / サーバー、およびレガシー・アプリケーションのための完全な許可ソリューションです。 Policy Director 許可により、1 つの組織が、保護情報へのユーザー・アクセスを安全な方法で制御することができます。 Policy Director を標準のインターネット・ベース・アプリケーションと一緒に使用すると、安全性が高く、管理の行き届いたイントラネットを構築できます。

この章は、次の各節に分かれています。

エンタープライズ・ネットワーク・セキュリティーの概要

現在、多くの組織では、公衆インターネットと私用イントラネットを、グローバル通信用の媒体として効果的かつ不可欠なものとしてその価値を認めています。エレクトロニック・コマース (電子商取引) は、近年、急激に多くのビジネス・マーケティング戦略の重要な構成要素となりつつあります。教育機関では、学習者が地理的に遠方にいる場合には、インターネットに依存しています。オンライン・サービスでは、個人が電子メールを送信し、Web の膨大な知的リソースに接続することができます。ただし、従来のアプリケーション、たとえば、TELNET や POP3 もいまだに重要なネットワーク・サービスとして使用されています。

ビジネスにおいては、インターネット・テクノロジーを使用することにより、サプライ・チェーンの関係を強化し、ビジネス・パートナーとの共同作業をしやすくし、顧客の接続性を向上させることができる、という点が認識されています。 このようなことをビジネス上可能にするには、高度なセキュリティーを実現しつつ、法人組織のリソースを開示できることが前提となります。

ビジネス業界では、インターネットをグローバルな商取引と配布のための伝達手段として使用したいと考えています。しかし、安全性が証明されたセキュリティー・ポリシー・メカニズムと管理システムがないことが、このような業務を妨げています。

Policy Director は、集中化されたネットワーク・セキュリティー・サービスを組織に提供することにより、情報ポリシーを管理する解決手段を提供します。集中ネットワーク・セキュリティー・サービスを使用することにより、一貫性のあるユーザーおよびポリシー情報を実現し、保守することができます。

ネットワーク・セキュリティーの用語および定義

次に示すネットワーク・セキュリティー・サービスと概念は、本書の Policy Director の説明を読む上で重要になります。

セキュア・ドメイン
共通のサービスを共用し、通常共通の目的を持って機能するユーザー、システム、およびリソースのグループ。

認証　セキュア・ドメインにログインしようとする個人を識別するプロセス。

クリデンシャル
ユーザー、グループの関連 (存在する場合)、およびその他のセキュリティー関連識別属性を記述する、認証時に取得された詳細情報。

許可　個人が、保護リソースでの操作を実行する権利を有するかどうかを判断するプロセス。

暗号化　電子データを秘密コードに変換することで、無許可ユーザーがデータを調べられないように保護します。

保全性　電子データが、送信時と受信時の間に変更されないようになっている状態。

保護の品質　認証、保全性、およびプライバシー条件を組み合わせて判断されるデータ・セキュリティーのレベル。

スケーラビリティー
リソースにアクセスするユーザー数の増加に対応できるネットワーク・システムの機能。

ネットワーク・セキュリティーの一般的な問題

世界中に通じるインターネットでも会社の私用イントラネットでも、実に多種多様なコンピューター・システム、アプリケーション、およびネットワークに接続しています。このように異なるハードウェアとソフトウェアの混用は、通常、ネットワークに次のような影響を与えます。

- アプリケーションに関してセキュリティーの集中管理が行われない。
- リソース - 場所の統一された命名規則がない。
- アプリケーションの高可用性を可能にするための共通したサポートがない。
- 拡張を容易にするための共通したサポートがない。

新しいビジネスでは、組織が、以前では考えられなかったレベルまでその情報リソースを開示することが求められます。 それに伴い、このようなビジネスでは、これらのリソースへのアクセスを確実に制御する方法を知っておく必要が出てきました。

情報技術 (IT) マネージャーが、分散ネットワークでポリシーとユーザーを管理するのは困難なことは既知の事実です。困難な理由は、アプリケーションとシステムの個々のベンダーがそれぞれ独自の方法で許可を実現していることです。

各エンタープライズ・アプリケーションごとに新しい許可サービスを開発することは高価なプロセスであり、管理のむずかしいインフラストラクチャーに発展するという点は、各会社がよく認識しています。開発者がアプリケーション・プログラム・インターフェース (API) を使ってアクセスする集中許可サービスを使用すれば、市場に出す時間が大幅にスピードアップし、所有の合計コストも削減できます。

集中ネットワーク・セキュリティー管理システムは、次のような要件を満たす必要があります。

- 既存のファイアウォールと認証機能アーキテクチャーと共存し、それらに影響力を与えること。
- ネットワークおよびアプリケーション管理フレームワークと統合または共存すること。
- アプリケーションから独立していること。

Policy Director の概要

Policy Director は、許可、ネットワーク・セキュリティー、およびポリシー管理を提供する完結したソリューションであり、地理的に分散したイントラネットとエクストラネット上に存在するリソースについて、終端から終端までの保護を提供します。 エクストラネット は、アクセス制御とセキュリティー機能を使用してインターネットに接続された 1 つまたは複数のイントラネットの使用を、選択された加入者に制限する仮想私設網 (VPN) です。

Policy Director は、最新技術を用いたセキュリティー・ポリシー管理機能に加え、認証、許可、データ・セキュリティー、およびリソース管理機能をサポートします。 Policy Director を標準のインターネット・ベース・アプリケーションと一緒に使用すると、安全性が高く、管理の行き届いたイントラネットを構築できます。

Policy Director を使用することで、ビジネスにおいて、私用の内部ネットワーク・ベース・リソースへのアクセスを確実な方法で管理できるようになりました。 また、ビジネスは、公衆インターネットの広範囲に及ぶ接続性と使いやすさを利用することもできます。 Policy Director を法人組織用のファイアウォール・システムと併用すると、エンタープライズ・イントラネットを無許可アクセスと侵入から保護することができます。

Policy Director 許可サービス API 規格

許可サービス は、アプリケーションのセキュリティー・アーキテクチャーの重大な部分です。ユーザーが認証プロセスに合格した後、許可サービスは、次の段階としてユーザーがどのサービスと情報にアクセスできるか決定することによって業務方針を実施します。

たとえば、Web ベースの退職金基金にアクセスするユーザーは、個人の会計情報を表示できます。その情報を表示する前に、許可サーバーは、そのユーザーの識別、クリデンシャル、および特権属性を検査する必要があります。

規格ベースの Policy Director 許可 API により、アプリケーションが、集中 Policy Director 許可サービスを呼び出すことができます。これらの呼び出しを使用すれば、新しいアプリケーションごとに許可コードを作成する必要がなくなります。

Policy Director 許可 API では、ビジネスにおいて、トラステッド許可フレームワーク上の全アプリケーションを標準化することができます。 Policy Director 許可 API を使用すれば、自分のネットワーク上のリソースへのアクセスを、より強固に制御することができます。

Policy Director 許可 API の全体の情報と説明については、 *Policy Director Programmer's Guide and Reference* を参照してください。

Policy Director のコア・テクノロジー

Policy Director ネットワーク・セキュリティー管理ソリューションは、次のコア・テクノロジーを提供し、サポートします。

- 認証
- 許可
- データ保護の品質
- スケーラビリティー
- 責任能力

認証

このコア・テクノロジーには、Policy Director ユーザー名およびパスワードによる *認証メカニズム* のサポートが含まれます。

機密キー:

- ケルベロス
- Lightweight directory access protocol (LDAP)

公開 / 秘密キー:

- アプリケーション特有のユーザー名とパスワードを使って、セキュア・ソケット層 (secure socket layer) (SSL) 対応ブラウザーを通じてログインします。
  - 基本認証 (BA) メカニズム -- WebSEAL およびセキュア・ソケット層インターフェース HTTPS のみ。
  - Policy Director 書式ベース・メカニズム -- WebSEAL および HTTPS のみ。
- クライアント側の X.509 証明を使用することによって SSL を介してログインします。 Policy Director は、PKIX 準拠の公開キー・インフラストラクチャー (PKI) 製品 (IBM SecureWay Trust Authority、Version 3.1 など) または Entrust ベース PKI 製品 (IBM Vault Registry、Version 2.2.2 など) をサポートします。

  IBM SecureWay Trust Authority Version 3.1 には、完全な証明書ライフ・サイクル (登録と初期認証、キー・ペア更新、証明書の更新、証明書および証明書取り消しリスト (CRL) 資料、および証明書取り消しなど) をサポートするためのクライアント・ソフトウェア、単純登録アプリケーション、認証局、および統合ディレクトリーが含まれています。認証局 (CA)、登録権限 (RA)、およびエンティティー終了 (EE) の各要求を管理するためのグラフィカル・ユーザー・インターフェース (GUI) が提供されています。 API ライブラリーも用意されています。

クリデンシャルの取得:

- クリデンシャル取得サービス (CAS) -- カスタマイズされた認証拡張です。

許可

このコア・テクノロジーは、次のタイプの Policy Director 許可をサポートします。

- Policy Director 許可サービス
- 規格ベースの Policy Director 許可 API
- 外部許可機能

データ保護の品質

保護の品質 は、Policy Director が、クライアントとサーバーの間で伝送される情報を保護する度合いのことです。トンネル・メカニズム、暗号化規格、および変更検出アルゴリズムを組み合わせた効果によって保護の品質が決まります。

保護の品質には次のレベルがあり、セキュリティーが増大する順に示します。

1. 標準伝送制御プロトコル (TCP) 通信 (認証なし)
2. 認証のみ - ユーザーの識別を検査します。
3. 認証 + データ保全性 - ネットワーク通信の間にメッセージ (データ・ストリーム) が変更されないようにします。
4. 認証 + データ保全性 + データのプライバシー - ネットワーク通信の間に、メッセージが変更されたり、検査されないようにします。

それぞれのホストとネットワークごとに、必要な保護レベルを指定できます。

サポートされている暗号化規格: Policy Director は、次のデータ暗号化規格 (DES) および、 SSL 上のその他の暗号化暗号をサポートします。

- 40 ビット RC2
- 128 ビット RC2
- 40 ビット RC4
- 128 ビット RC4
- 40 ビット DES
- 56 ビット DES
- 168 ビット・トリプル DES

Policy Director NetSEAL と Policy Director WebSEAL は、DCE - リモート・プロシージャー呼び出し (DCE-RPC) を介して、40 ビット DES と 56 ビット DES の暗号化をサポートします。

注: インターナショナル・バージョンは、暗号化テクノロジーの輸出規制の対象になります。

トンネル・メカニズム: Policy Director は、暗号化されたデータの伝送に次のプロトコルをサポートします。

- セキュア・ソケット層 (SSL) トンネル伝送
- 総称セキュリティー・サービス (GSS) トンネル伝送

WebSEAL は、SSL 暗号化トンネルによって可能になるデータ保全性とデータ・プライバシーをサポートします。 WebSEAL および NetSEAL は RPC をサポートします。 RPC で保全性とタイム・スタンプを使用すると、*プレーバック・ハッキング* に対する保護が行われます。 プレーバック・ハッキングは、ユーザーのデータが、ユーザーのクライアントとサーバーの間を流れているときに取り込まれて起こります。これが起こると、そのデータは、最初のユーザーの偽名を使用する方法で、再生されるか、サーバーに戻されて表示されます。

SSL トンネル伝送: SSL プロトコルでは、 2 つのモデム間の通信をセットアップするためのシグナル交換ができます。 このプロトコルは、インターネット上でセキュリティーとプライバシーを実現します。 SSL は、認証のためには公開キーを使い、SSL 接続を通じて転送されるデータを暗号化するためには機密キーを使います。

Policy Director NetSEAL サーバーに SSL トンネル伝送を使用する場合には SSL を使用可能にします。この構成は、NetSEAT クライアントが、セキュリティー専用ポート (たとえば、 TELNET が使用するポート) である Policy Director NetSEAL サーバーに対して、 SSL クライアントとして働く場合に使用されます。

Policy Director WebSEAL は SSL バージョン 2 と 3 をサポートします。

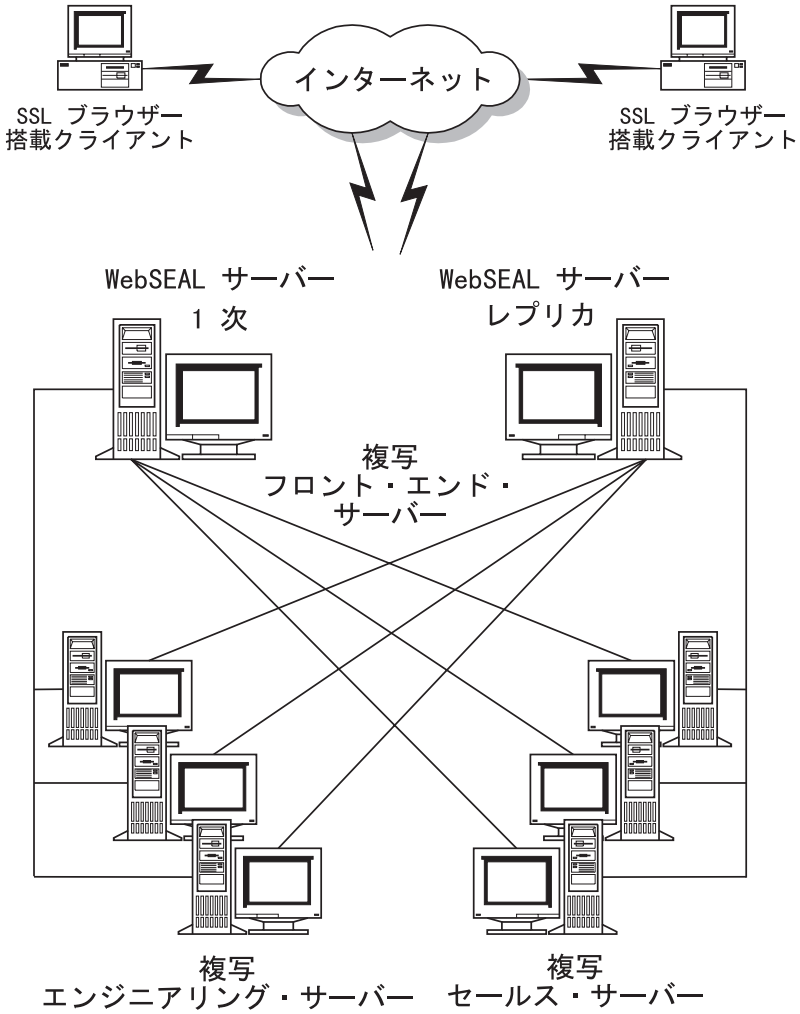
GSS トンネル伝送: GSS インターフェース (GSS API) は、アプリケーションがセキュリティー・サービスにアクセスできるようにする標準の方法です。 GSS トンネル伝送は、セキュア RPC で使用されます。 NetSEAT クライアントを、 Policy Director for Microsoft® Windows NT® または Policy Director 管理コンソールへのサポート・モジュールとして導入する場合は、このオプションを使用可能にします。

GSS トンネル伝送は、汎用方式で呼び出し元にセキュリティー・サービスを提供します。このトンネル伝送は、基礎となるメカニズムとテクノロジーの範囲内でのサポートが可能です。また、異なる環境への、アプリケーションのソース・レベルの移植性を可能にします。 GSS トンネル伝送によって、両方向にそれぞれ独立して流れているトラフィックについての保護レベルの制御が可能になります。たとえば、クライアントからサーバーに送られているデータはバルク・データ暗号化によって完全に保護され、サーバーからクライアントに送られているデータは保護されない、という場合も出てきます。

スケーラビリティー

スケーラビリティー は、セキュア・ドメインのリソースにアクセスするユーザー数の増加に対応できる能力のことです。 Policy Director は次の技法を使ってスケーラビリティーを可能にします。

- サービスの複写
  - 認証サービス
  - 許可サービス
  - セキュリティー・ポリシー
  - データ暗号化サービス
  - 監査サービス
- フロントエンド複写 WebSEAL サーバー
  - 高可用性のためにミラーリングされたリソース
  - クライアント要求のロード・バランシング
- バックエンド複写サーバー
  - バックエンド・サーバーは、WebSEAL サーバーでも第三者の Web サーバーでも可能
  - 高可用性のためにミラーリングされたリソース (一体化されたネームスペース)
  - 追加のコンテンツおよびリソース
  - Smart Junction™ テクノロジーを介する着信要求のロード・バランシング
- 認証および許可サービスを別個のサーバーにオフロードできるようにすることによるパフォーマンスの最適化
- 管理のオーバーヘッドを増加させない、サービスのスケール配置



責任能力

Policy Director には、幾つかのログ記録機能と監査機能があり、 Policy Director と DCE サーバーの両方で生成された、すべてのエラー・メッセージとすべての警告メッセージを取り込むログ・ファイルがあります。また、Policy Director と DCE サーバーの活動をモニターする監査証跡ファイルもあります。

ログ・ファイル

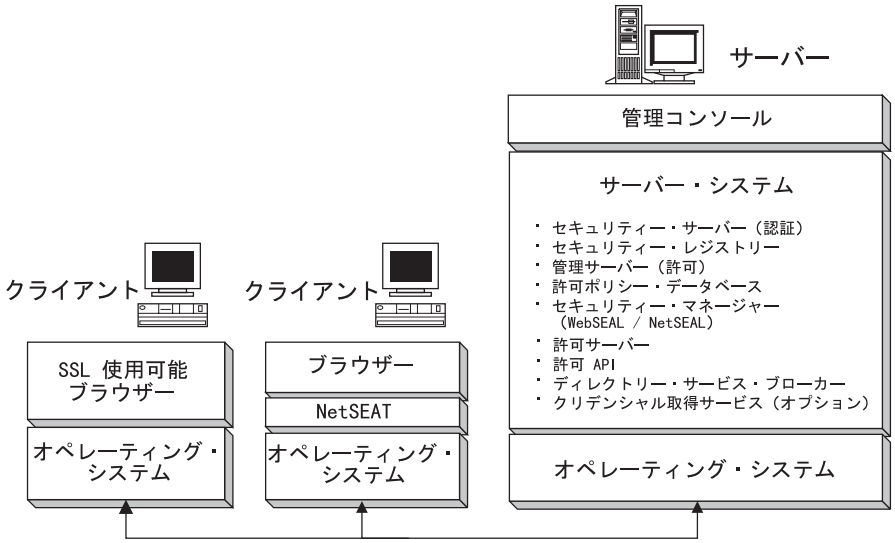
- Policy Director サーバー・ログ・ファイル
- DCE サーバー・ログ・ファイル
- DCE 保守容易性メッセージ
- 標準 HyperText Transfer Protocol (HTTP) ログ・ファイル

監査証跡ファイル

- Policy Director 許可監査証跡ファイル
- WebSEAL 監査証跡ファイル
- Policy Director 管理監査証跡ファイル
- DCE 監査証跡ファイル
- LDAP 監査証跡ファイル

Policy Director 構成要素

Policy Director には、クライアント・システムとサーバー・システム用のソフトウェアが組み込まれています。 Policy Director は、Sun Solaris、IBM AIX、および Microsoft® Windows NT® オペレーティング・システム・プラットフォームでのサポートを提供します。



管理コンソール

管理コンソールは Java ® ベースのグラフィカル・アプリケーションで、Policy Director セキュア・ドメインのセキュリティー・ポリシーを管理するために使用します。管理コンソールからは、会計レジストリーと 1 次 (マスター とも呼ばれる) 許可ポリシー・データベースを使用した管理作業を実行できます。

一般的な管理コンソール作業には、ユーザー・アカウントとグループ・アカウントの追加と削除、ネームスペース・オブジェクトへのアクセス制御リストの適用などがあります。管理コンソールはセキュア RPC を使って、セキュア通信チャネルを介してこれらの管理タスクを実行します。

管理責任をローカル・レベルに代行させることができます。たとえば、責任を限定して、特定のセキュリティー管理者を割り当てることができます。こうすると、このセキュリティー管理者は、保護オブジェクト・ネームスペースの指定部分内にあるリソースについてのみ、セキュリティー・ポリシーを管理できます。

セキュリティー・サーバー

セキュリティー・サーバー (secd) は、 LDAP サーバーまたは DCE サーバーのいずれでもかまいません。セキュリティー・サーバーは、認証サービスを提供します。 また、セキュア・ドメインに参加しているすべての有効ユーザーのアカウント項目を含む中央レジストリー・データベース (LDAP または DCE) の保守も行います。

DCE 環境では、レジストリー・データベース・ユーザーは、*プリンシパル* と呼ばれることもあります。

セキュリティー・サーバーは次に示す 2 つの重要な役割を果たします。

- セキュリティー・サーバーは、ユーザーが所属するグループと組織、およびユーザーが果たす役割を定義します。 この情報は中央レジストリー・データベースに保管されます。 Policy Director 許可サービスは、許可についての判断を下すときにこの情報を考慮します。
- セキュリティー・サーバーは、ログインのすべての試みについて認証サービスを提供します。

DCE では、セキュリティー・サーバーは、セキュア・ドメイン全体にレジストリー・データベースを複写して、障害が 1 つの場所に集中しないようにします。セキュリティー・サーバーは、1 次レジストリーで変更が行われた場合に、必ず複写データベースをすべて更新する、という役目を持っています。

管理サーバー

管理サーバー (ivmgrd) は、セキュア・ドメインの 1 次許可ポリシー・データベースを保守します。このサーバーには、セキュア・ドメインの中にある全許可データベース・レプリカの更新を行う役目もあります。 また、管理サーバーは、セキュア・ドメイン内の他の Policy Director サーバーに関する位置情報の保守も行います。

セキュリティー・マネージャー

セキュリティー・マネージャー (secmgrd) は、レプリカの許可ポリシー・データベースからの情報に基づくアクセス制御ポリシーを適用します。セキュリティー・マネージャーには次のものが含まれます。

- きめの粗い伝送制御プロトコル / インターネット・プロトコル (TCP/IP) アクセス制御のための NetSEAL 構成要素。
- きめの細かい HTTP および HTTPS アクセス制御のための WebSEAL 構成要素。

WebSEAL

WebSEAL は、セキュリティー・マネージャー (secmgrd) の 2 つの構成要素の 1 つです。

WebSEAL は、HTTP、HTTPS、および NetSEAT クライアント要求を受け入れる、ハイパフォーマンス・マルチスレッド Web サーバーです。 WebSEAL は、次のようなリソースのためのアクセス制御を管理します。

- Universal Resource Location (URL)
- URL に基づく通常の式
- Perl、C™、または C++ の共通ゲートウェイ・インターフェース (CGI) プログラム
- ハイパーテキスト・マークアップ言語 (HTML) ファイル
- Java servlet
- Java クラス・ファイル

WebSEAL は、接合サーバーとして、スマート接合テクノロジーを通じて第三者の Web サーバーを保護し、管理します。*スマート接合* によって、 Web スペースに追加のサーバー・ファイル・システムを接続し、リソースを一体化した 1 つのオブジェクト・ネームスペースとして見ることができます。

WebSEAL は、Web ベース・リソースに単一のサインオン機能を提供するために使用します。ユーザーは、標準のケルベロスまたは SSL を使って WebSEAL に対する認

証を行います。すると、WebSEAL は、 HTTP 基本認証とダイジェスト認証を使ってそのユーザーに偽名を使用します。 WebSEAL は、ユーザーの識別を CGI 変数として渡すこともできます。

NetSEAL

NetSEAL は、セキュリティー・マネージャー (secmgrd) の 2 つの構成要素の 1 つです。 NetSEAL は、すべての着信 TCP/IP 通信を保護するための仮想私設網 (VPN) ソリューションです。 NetSEAL は、宛先ポートとクライアントの識別に基づくアクセス制御を実行します。 NetSEAL は、以下のことを行うセキュリティー・ソリューションです。

- TELNET や POP3 のような従来のインターネット・サービスを認可し保護する。
- データベース・システムやネットワーク管理ツールのような、各種のアプリケーション・パッケージを認可し保護する。

NetSEAL は、サーバー上の特定のポート (たとえば、ポート 23、TELNET など) に接続できるユーザーの能力を制御するリソース・マネージャーです。 NetSEAL 構成要素は、さらに NetSEAT クライアントからトンネルされている TCP/IP トラフィックを受け入れ、許可します。

NetSEAL サーバーを使用すると、ネットワーク・アプリケーション・サーバーと Policy Director セキュリティー・サービスの統合を可能にします。NetSEAL サーバーは、すべてのネットワーク通信にセキュア・トンネル・エンドポイントを提供します。ユーザーの認証済み識別は、この SSL 作成または GSS 作成トンネルを介して、元のプロトコル要求と一緒に渡されます。NetSEAL SSL トンネルは、NetSEAT クライアントとの通信に使用します。

NetSEAT クライアント

NetSEAT はネットワーク・サポート・モジュールです。このモジュールは、クライアント・アプリケーションのセキュア・プロキシーとしてシームレスに働き、すべてのクライアント / サーバー通信の SSL または GSS トンネル上の終端から終端までの暗号化を可能にします。セキュリティー・クライアントの動的リンク・ライブラリー (DLL) のインプリメンテーションとして、NetSEAT を使用すると、ユーザーは Policy Director の機能をフルに活用することができます。 これらの機能には、データ通信の保護と高可用性アーキテクチャーの提供などがあります。

NetSEAT では、Policy Director セキュリティー・メカニズムとの完全統合が確実に行われ、クライアントのリソース管理が行われます。 NetSEAT は TCP/IP アプリケーションに対する保護を行います。 NetSEAT は、アプリケーション・データを (SSL または GSS のような) VPN トンネルに透過的に暗号化し、これを公開インターネットのようなセキュアでないリンク上で移送することができます。

この構成は、すべての発信 HTTP 要求をインターセプトし、それらを宛先 WebSEAL サーバーに転送するようにできます。 これは論理 URL を物理 WebSEAL サーバーに透過的にマップし、エンド・ユーザーに影響を与えずに Web リソースの再配置や複写を可能にします。

注: Policy Director との対話には NetSEAT は必要ありません。たとえば、クライアント・ユーザーは SSL 対応ブラウザーを使って、WebSEAL と直接通信できます。

許可 API

Policy Director アプリケーション開発キット (ADK) には、開発者が Policy Director セキュリティーと認証を、法人組織のアプリケーション内に直接構築できるようにする、許可 API サーバー (AuthAPI™) が含まれています。 Policy Director 許可 API は、 Policy Director 許可サービスに直接アクセスできるようにします。 これらの許可 API を使用すれば、開発者は各アプリケーションごとに許可コードを作成する必要がなくなることを意味します。

Policy Director 許可 API により、アプリケーション開発時間とアプリケーション開発コストの両方が減ります。許可 API はすべてのネットワーク・セキュリティーの集中管理を提供するので、所有の合計コストおよびセキュリティー違反の危険性が減少します。

許可サーバー

リモート・キャッシュ許可モードでは、アプリケーションは、 Policy Director 許可 API が提供する関数呼び出しを使って、 Policy Director 許可サーバー (ivacld) と通信します。 Policy Director 許可サーバーは、許可ポリシー・データベースのレプリカを保守し、許可の判断を下す評価者として機能します。

Policy Director 許可 API は、許可決定要求を Policy Director 許可サーバーに転送します。 Policy Director 許可サーバーは、セキュリティー・ポリシーに基づく勧告を戻します。 許可サーバーは、許可要求の詳細を含む監査レコードの書き込みもします。

ディレクトリー・サービス・ブローカー

Policy Director は、Policy Director の導入時に、ディレクトリー・サービス・ブローカー (DSB) を自動的に導入し、構成します。 Policy Director は、Policy Director 管理サーバー (IVMgr) パッケージの一部として、DSB を提供します。 DSB を使用するにはこれ以上のステップは必要ありません。

NetSEAT クライアントが Policy Director サーバーまたは管理コンソールのサポート・モジュールとして働く場合、これらのクライアントは DSB を使用します。NetSEAT クライアントが SSL トンネルだけを使用する場合は、DSB を使用しません。

DSB は、セル・ディレクトリー・サービス (CDS) の中間層のサーバーとして働きます。NetSEAT クライアントは、リソースの場所とサービスに対する要求を DSB に出します。これを受けて DSB は、要求を解決するために、セキュア・ドメインの CDS に連絡します。この後、DSB は要求された情報を、NetSEAT クライアントを実行するシステムに戻します。

クリデンシャル取得サービス (オプション)

Policy Director クリデンシャル取得サービス (CAS) は、任意選択の構成要素です。Policy Director は、Policy Director の導入時に、クリデンシャル取得サービスを自動的に導入します。

クリデンシャル取得 (Credential acquisition) とは、認証メカニズムにより提供された特定の識別情報を、共通の、ドメイン間で通用する表現形式のクライアント識別子に変換または対応付ける処理です。この共通の表現形式は、*クライアントのクリデンシャル* と呼ばれます。

クリデンシャル取得または対応付けが必要な場合には、Policy Director クリデンシャル取得サービスを Policy Director WebSEAL サーバーで使用できるように構成する必要があります。Policy Director ユーザーは、WebSEAL により自動的にクリデンシャルに対応付けられます。

外部レジストリーからの非 Policy Director SSL クライアントは、Policy Director クリデンシャル取得サービスを使用して、または独自のクリデンシャル取得サービスを作成することにより、*usernames* を Policy Director 識別に対応付けることができます。クライアント側 X.509 証明を使用してアクセスするクライアントは、Policy Director クリデンシャル取得サービスを使用して、または独自のクリデンシャル取得サービスを作成することにより、*証明書*情報を Policy Director 識別に対応付けることができます。

または、独自の CAS サーバーを作成し、セキュア・ドメインのための特有な解決方法を提供し、認証情報 (クライアント証明書、ユーザー名、トークンなど) を処理するようにカスタマイズすることができます。Policy Director クリデンシャル取得サービスの開発者か設計者が、この認証 / マッピング・サービスの全体の詳細を決めます。Policy Director では、Policy Director の外部のデータベースにマッピング規則を保管します。 Policy Director は、WebSEAL と Policy Director クリデンシャル取得サービスの間の Interface Definition Language (IDL) インターフェースを提供します。また、Policy Director は、Policy Director クリデンシャル取得サービス・サーバー機能 (始動、サーバー登録、信号処理など) を処理する汎用サーバー・フレームワークも提供します。Policy Director クリデンシャル取得サービス開発者の責任で、クリデンシャル取得サービスのフレームワークを拡張して、特定のアプリケーションで必要とされる識別マッピング機能を実行します。

セキュリティー・モデルの概要

Policy Director セキュリティーは、情報へのアクセスを制御することを意味します。Policy Director テクノロジーは、組織のセキュリティー・ポリシーを、保護ネームスペースのオブジェクトにマップします。

このアクセスは、ネットワーク・トポロジーの制約を受けずに、業務方針を基本として行うようにできます。ユーザーは、その物理的な位置ではなく、そのユーザーがだれであるか、およびその役割が何であるかに基づいて、アクセスを許可されたり、拒否されたりします。

Policy Director 構成要素は、クライアントとサーバーに基づいたアプリケーションです。相互認証とアクセス権限の割り当てを使用すれば、特定のリソースを一般的な用途に使用可能にできます。同時に、機密の内部リソースをよりセキュア (安全) に許可されたアクセスに限定することができます。情報は、許可ユーザーがセキュア・ドメイン内からデータにアクセスするか、リモート・インターネット接続を使ってデータにアクセスするかに関係なく、セキュア (安全) です。

セキュリティー・ポリシーの定義

Policy Director セキュリティー・ソフトウェアを使用すると、すべての通信を無許可のアクセスと未検出の破壊から保護する、セキュア・ドメインを作成することができます。

セキュア・ドメインの管理者は、以下のことを識別する必要があります。

- セキュア・ドメインにだれが参加でき、保護オブジェクト・ネームスペース内のオブジェクトへのアクセスを要求できるか。
- どのオブジェクトを保護すべきか。
- どの規則でそれらのオブジェクトが保護されるか。

Policy Director は、次の方法でクライアント要求を処理します。

- クライアントが認証を使用しているのはだれかを確かめる。
- 許可クリデンシャルの形式で権利を取得する。
- これらのクリデンシャルに基づいて許可の決定を下す。

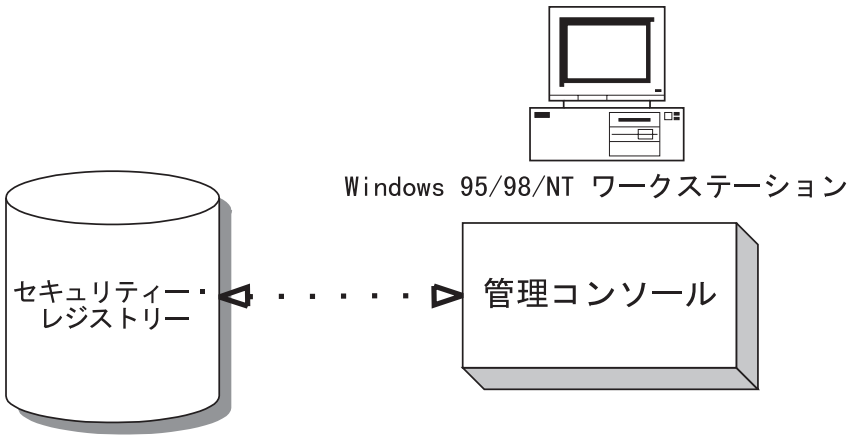
だれがセキュア・ドメインに参加できるか

管理者は、Policy Director セキュア・ドメインのメンバーであるユーザー (DCE 環境では *プリンシパル* と呼ばれる) とグループの正式リストを保守しています。したがって、これらのユーザーとグループは、リソースへのアクセスに参加できます。レジストリー・データベース (LDAP または DCE) は、このユーザーとグループの情報を保管しています。

ユーザーのアカウントを作成すると、ただちにセキュア・ドメインに参加する許可をそのユーザーに与えることができます。

管理タスク:

- ユーザーとグループのアカウントを、管理コンソールを使用して (または **ivadmin** コマンドを使用して) 作成します。



保護すべきオブジェクトはどれか、またどの規則で保護するか

Policy Director は、次のタイプのリソースを保護できます。

- Web オブジェクト (HTML ファイル、CGI プログラム、動的 HTML など)
- NetSEAL によって保護されるネットワーク・サービス (TELNET、POP3、およびカスタム・アプリケーションなど)
- 管理機能

Policy Director は、実際のリソースを保護オブジェクト・ネームスペース内のオブジェクトとして表します。それらのオブジェクトにポリシー・テンプレート を付加する

ことによって、特定のアクセス許可を割り当てます。 Policy Director は、*アクセス制御リスト* (ACL) と呼ばれるポリシー・テンプレート・タイプを使用します。 ACL は次の内容を定義します。

- だれがそのオブジェクトにアクセスできるか。
- そのオブジェクトにどの操作を実行できるか。

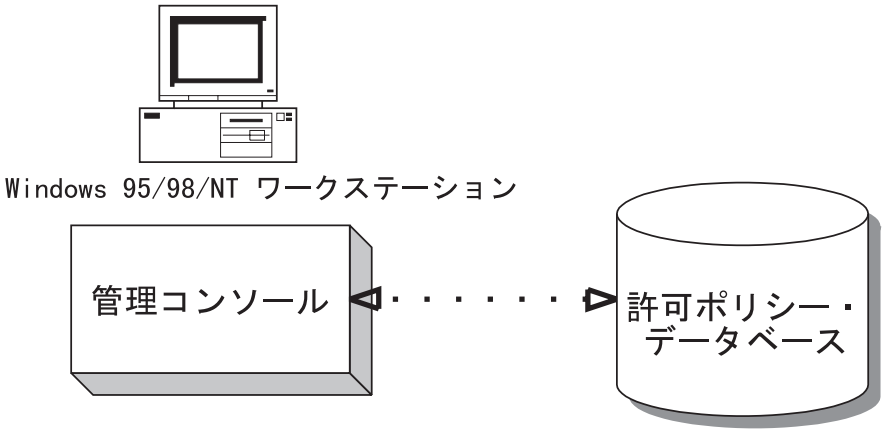
たとえば、オブジェクトの表示特権はすべてのグループに許可するが、オブジェクトの変更は 1 つのグループにしか認めない、ということが可能です。

Policy Director は、*疎 (または継承) ACL モデル* と呼ばれる、グローバル許可を設定するためのメカニズムを採用しています。疎 ACL モデルでは、階層内のすべてのオブジェクトに直接適用される ACL がないことを示します。このモデルではその代わりに ACL 継承を採用します。階層内のオブジェクトに ACL が適用されていない場合、有効な ACL は、その階層内で次に高位の ACL です。ルート・オブジェクト (/) には、継承する ACL がすべてのオブジェクトに確実に確保されるようにするため、必ず ACL が必要になります。

グローバル許可メカニズムを使用すると、各ファイルまたはディレクトリーごとに許可を設定する必要がなくなります。

管理タスク:

- 管理コンソールを使ってネームスペースのセキュリティー・ポリシーを定義し、保護の必要なオブジェクトにポリシー・テンプレート (ACL) を適用します。

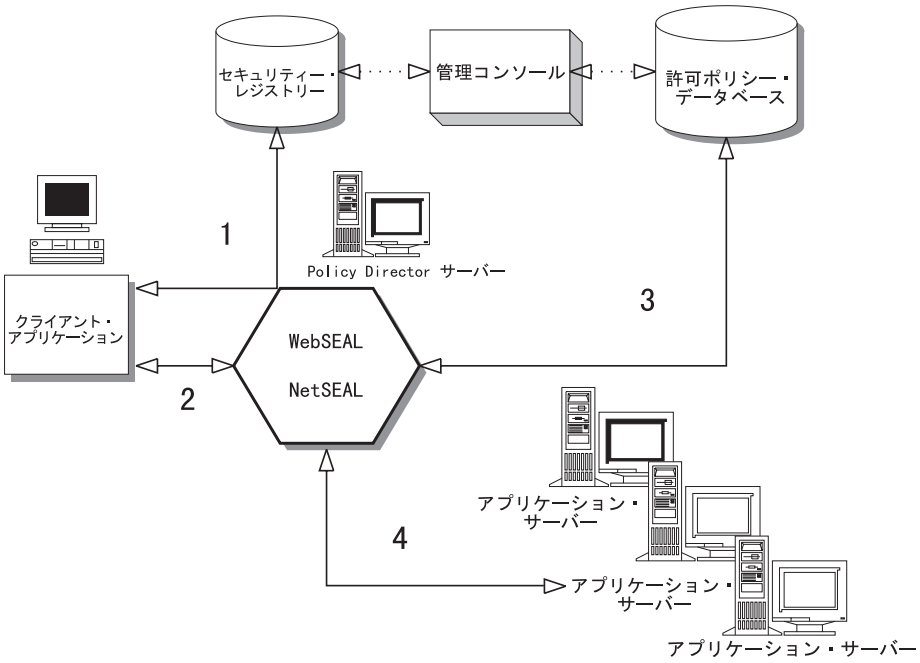


クライアント要求へのセキュリティー・ポリシーの適用

ユーザーが保護オブジェクトまたは保護アプリケーションへのアクセスを要求すると、Policy Director は、その要求を承認する前に、該当の認証および許可検査を適用します。

1. クライアント・ユーザーは、セキュリティー・サーバーに対して認証を行って、識別の証明を設定します。 Policy Director は、公開キー方式および機密キー方式の両方を使用した認証をサポートします。

   この識別に基づき、セキュリティー・サーバーはユーザーの許可クリデンシャルを戻します。 クリデンシャルは、ユーザーが所属するグループと組織、およびユーザーが果たす役割を定義します。



2. セキュア通信トンネルが、クライアント・ユーザーと Policy Director サーバーの間で確立されます。
3. 許可検査が、複写された中央許可ポリシー・データベースに対して行われます。Policy Director は、ユーザーのクリデンシャルに基づいて ACL を実施します。
4. そのユーザーのクリデンシャルで許可の設定が適切であれば、Policy Director はアプリケーション・サーバーにその要求を渡し、そのトランザクションを完了させます。

第2章 認証およびクリデンシャルの取得

認証とは、セキュア・ドメインへのログインを試みる個々のユーザーを識別するプロセスのことです。 認証のゴールは、クライアントの識別を確認し、そのクライアントを記述するクリデンシャルを取得することです。クリデンシャルは、Policy Director によって、許可、監査、およびその他のサービスに使用されます。

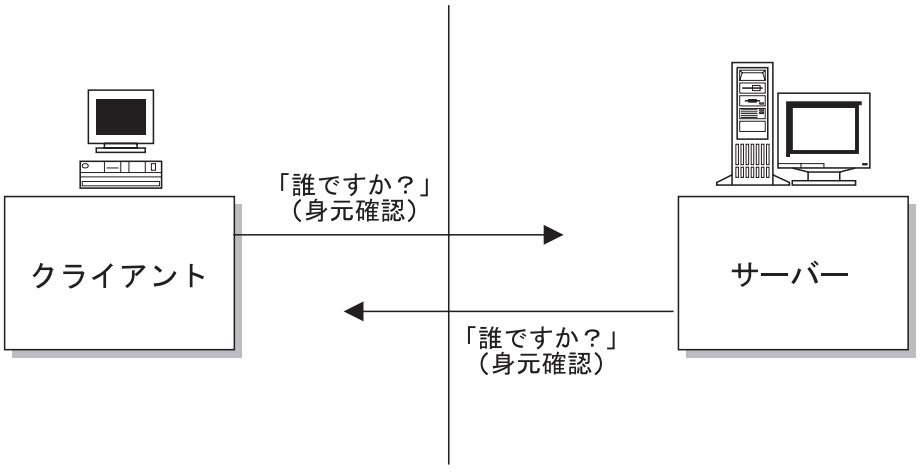
この章は、次の各節に分かれています。

認証の基本概念

サーバーがセキュア・ドメインでセキュリティーを実施するときは、各クライアントはその識別の証明を提示しなければなりません。 セキュア・ドメイン内の各リソースへのアクセスをサーバーが制御する場合、認証と許可を求めるサーバーの要求により、包括的なネットワーク・セキュリティーが実現されます。

認証 とは、セキュア・ドメインへのログインを試みる個々のユーザーを識別するプロセスのことです。

セキュリティー・システムでは、認証 (authentication) は許可 (authorization) と区別されます。*許可* は、認証されたユーザーが特定のリソースに操作を実行する権利を持つかどうかを判断します。認証は、その個人が自分で申し立てている本人であることを確認しますが、リソースに操作を実行する権利に関しては何も言いません。



Policy Director は認証に対して柔軟な方法をサポートし、物理的なネットワーク・トポロジーではなく、ビジネスの要求に基づいたセキュリティー・ポリシーを可能にします。

Policy Director は、ユーザーが保護情報にアクセスするためにセキュア・ドメインにログインする時に、ユーザーの識別を認証します。 ユーザーは、定義された多くの役割を持つことができ、それぞれの役割が、異なるアクセス許可を持つことができます。

認証のゴール

認証プロセスは、次の 2 つの重要なゴールを達成します。

1. クライアントの識別を判別する。
2. クライアントのクリデンシャルを取得する。

認証メカニズム と*クリデンシャル取得メカニズム* は、実際には 2 つの別のプロセスです。 Policy Director は、多くの認証メカニズムをサポートします (『サポートされる認証メカニズム』を参照)。

Policy Director は、クリデンシャル取得のためのデフォルトのサービス、および、カストマイズ可能なサービスも提供しています。 *クリデンシャル取得サービス* は、あるメカニズムに特有な識別情報を、 Policy Director のクリデンシャルに対応付けます。 Policy Director のクリデンシャルは、拡張特権属性証明書 (EPAC) 形式を使用しています。

クリデンシャル (Credential) は、クライアントについての情報を必要とするすべての Policy Director サービスによって使用されます。 Policy Director はクリデンシャルを、許可、監査、および権限委譲といった多くのサービスを実行するために使用します。

サポートされる認証メカニズム

Policy Director は、機密キーおよび、公開 / 秘密キーに基づく*認証メカニズム* の両方をサポートします。

機密キー:

- ケルベロス・バージョン 5
- Lightweight directory access protocol (LDAP)

公開キー / 秘密キー:

- クライアント側の X.509 証明を使用することによって SSL を介してログインします。Policy Director は、PKIX 準拠の公開キー・インフラストラクチャー (PKI) 製品 (IBM SecureWay Trust Authority、Version 3.1 など) または Entrust ベース PKI 製品 (IBM Vault Registry、Version 2.2.2 など) をサポートします。

  クリデンシャルの取得には、クリデンシャル取得サービスが必要です。

認証のタイプ

Policy Director は次のタイプの認証をサポートします。

- SSL 認証 -- インターネット認証およびイントラネット認証用

- ユーザー名とパスワードの認証 -- ユーザー識別に基づく認証用
- ケルベロス認証 -- ネットワーク認証用

SSL 認証

セキュア・ソケット層 (SSL) プロトコルは、インターネット上での認証、セキュリティー、およびプライバシーを提供します。 SSL は次のものを使用します。

- 認証用の公開キー / 秘密キーの対による暗号。
- SSL 接続上のデータの暗号化には機密キー。

認証機能として、SSL プロトコルは、サーバーのみの認証および相互認証をサポートします。

Policy Director は、SSL バージョン 2 と 3 をサポートします。

プロトコルの詳細

SSL プロトコルは TCP/IP の最上部に作成され、アプリケーションから独立しています。 SSL プロトコルは、HTTP、FTP、TELNET といったアプリケーション・プロトコルが、最上部の層に透過的に存在できるようにします。 暗号化された SSL チャネル上で作動する HTTP Web 通信プロトコルは、 *HTTPS* と呼ばれます。

SSL プロトコルは、高レベルの通信アプリケーションがデータを交換する前に、サーバーを認証するだけでなく、暗号化キーを折衝することができます。 SSL プロトコルは、暗号化、認証、およびメッセージ認証コードを使用して、伝送チャネルのセキュリティーと保全性を保守します。

第三者信任および認証局

SSL 認証は、認証当事者の片方または両方が信任できるものであることを保証する第三者の基本的信任に依存しています。この信任された第三者は、*認証局 (certificate authority)* (CA) と呼ばれます。

CA は、*ディジタル証明書* (電子識別) を発行する責任があり、この証明書は、ネットワークを使用する個々人、グループ、またはシステムを識別し、この証明書の所有者が CA により信任されていることを他人に証明します。

CA は、この証明書にディジタルで署名し、証明書の所有者の識別を証明書に含まれる公開キーと結合します。 CA を信任する者はだれでも、そのユーザーも信任することになります。

ネットワーク・ユーザーは、 CA 自体の公開キー証明書を取得し、これを使用して他のユーザーの証明書を検査することができます。 この検査により、証明書内の公開キーが示された所有者の認証キーであるという保証が得られ、その結合については、CA (これについては、ルート証明書を使用して認識し、信任する) が保証していることがわかります。

2 つの認証当事者が公開キー証明書を交換した後、これらの当事者は、セッション・データの暗号化とディジタルでの署名に進むことができます。この暗号化とディジタルでの署名により、他のだれかがセッションを盗み聞きしたり、データを不正に変更するといった可能性がなくなります。

CA は、インターネット上で証明書を販売する会社、もしくは、企業内のイントラネットで証明書を発行する責任を持つ部門でもかまいません。他者の識別を検査する機関として、どの CA が信任するに足るものであるかを決める必要があります。

セキュリティー製品の IBM SecureWay FirstSecure (FirstSecure) セットの 1 つに、 IBM SecureWay Trust Authority (Trust Authority) があります。この製品は、企業内のイントラネット用の証明書を発行する機能を提供します。 FirstSecure およびその構成要素についての最新情報が、以下の Web サイトに記載されています。

`http: //www.ibm.com/software/security/firstsecure/library`

X.509 ディジタル証明書

SSL 上の認証は、ディジタル証明書を使用して提供されます。証明書は、ある種の識別情報を含むファイルです。証明書は、信任できる認証局 (CA) から購入するか、または受け取ります。 CA の主な責任は、ユーザーが本物として認証されたものであることを証明することです。

証明書は、転送できない、偽造できないファイルであり、一種の電子的な識別バッジもしくはパスポートとして働きます。証明書は、ユーザーまたはコンピューターが自分がだれであるかを述べている本人に間違いないことを保証するのに役立ちます。このファイルは CA の秘密キーにより署名され、その認証と保全性が保証されます。

SSL 使用可能なブラウザーは、 *X.509* と呼ばれる業界標準の証明書タイプを使用します。 X.509 のバージョン 3 は、次の情報を含んでいます。

- バージョン
- 通し番号
- 署名アルゴリズム ID
- 発行者名
- 有効期限
- 対象 (ユーザー) 名
- 対象公開キー情報
- 発行者の固有識別子 (発行した認証局の識別名)
- 対象の固有識別子 (証明書により識別された個々人の識別名)
- 拡張 (バージョン 3 のみ)
- 上記にリストされたすべてのフィールドに対する署名

X.509 バージョン 3 標準では、より詳細な識別情報 (たとえば、証明書の所持者が従事しているビジネス、そのビジネスに従事している期間など) が可能です。証明書は、対象 (ユーザー) の名前とユーザーの公開キーとの間のバインディングを認証したことを示すために、発行者によって署名されます。

証明書は、人やコンピューターが自分がそうであると主張する本人であることを確実に証明するものではなく、ある CA が、その人またはコンピューターをある程度信頼しているということを意味するだけです。証明書を発行した CA を信頼する場合は、その証明書の所持者と情報を交換する時に、ある程度の安心が得られるということです。

SSL 認証メカニズムの基本概念

SSL ハンドシェーク・プロトコルとは、通信を設定するために、信号を交換するプロセスのことです。 SSL ハンドシェーク・プロトコルは、2 つのフェーズからなります。

- 『サーバー側証明書を使用したサーバー認証』
- 22ページの『クライアント側証明書を使用したクライアント認証』 (オプション)

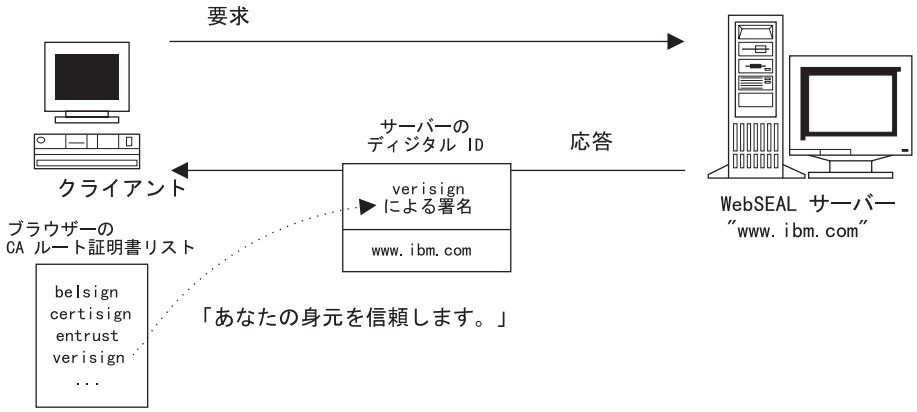
クライアントおよびサーバーの両方とも証明書を持つことができます。サーバーは、SSL 上での認証には必ず証明書を持つ必要があります。クライアントは、クライアント側の証明書があってもなくても、 SSL 上でセキュア・ドメインをアクセスすることができます。

サーバーが自分の証明書をクライアントに送信する場合、このプロセスはサーバー*認証* と呼ばれます。クライアントが自分の証明書をサーバーに送信する場合、このプロセスはクライアント*認証* と呼ばれます。サーバー認証とクライアント認証の組み合わせは、*相互認証* と呼ばれます。

サーバー側証明書を使用したサーバー認証

SSL 接続にはサーバー認証が必要です。 SSL 上のサーバー認証は、次の方法で行われます。

1. クライアントが SSL 使用可能サーバーとの接続を要求する。
2. これに応答して、サーバーはその証明書に (暗号化はしないで) 署名する。この後、サーバーはサーバーの公開キーを含む証明書をクライアントに送信する。
3. クライアントは、証明書ファイルに含まれるサーバーの公開キーを使用して、証明書の所有者が、これに署名した人と同じ人であることを検査する。
4. クライアントは、リストされた CA について、ブラウザーの CA ルート証明書データベースを検査し、証明書の発行者が、クライアントが受け取ったものであるかどうかを調べる。証明書の発行者がクライアントが受け取ったものである場合、クライアントは次のステップに進みます。そうでない場合、ブラウザーは、この証明書が未知の CA により発行されたものであることをユーザーに知らせます。この後、証明書を受け入れるか、拒否するかは、ユーザーの責任で行います。
5. この後、クライアントはマスター・キーを生成し、これをサーバーの公開キーで暗号化し、暗号化されたマスター・キーをサーバーに伝送する。
6. サーバーはマスター・キーを回復し、マスター・キーで暗号化されたメッセージを戻すことにより、サーバー自体をクライアントに認証する。後続のデータは、このマスター・キーから引き出されるキーを使用して暗号化されます。



クライアント側証明書を使用したクライアント認証

サーバーは、クライアントの公開キーを使用して、クライアントのディジタル証明書をロック解除します。クライアントの公開キー証明書は、X.509 構文に従います。

SSL 上でのクライアント側証明書を使用した認証は、次の方法で行われます。

1. サーバー認証の完了後、サーバーはクライアントにチャレンジを送信する。
2. クライアントは自分の公開キー証明書だけでなく、チャレンジ上にそのディジタル署名を戻す。ディジタル署名は、クライアントの秘密キーを使用して計算されます。
3. サーバーは、証明書ファイルに含まれるクライアントの公開キーを使用して、証明書の所有者が、これに署名した人と同じ人であることを検査する。
4. サーバーは証明書を信任された CA と突き合わせる。クライアントの CA が信任された CA のリストにない場合、サーバーによっては、トランザクションを終了し、エラーをログに記録し、クライアントにメッセージを戻す場合があります。その他のサーバーでは、この種の処理を取らずに先に進む場合もあります。
5. クライアントの CA が信任されると、サーバーはトランザクションを実行する。

クライアント側の証明書は SSL 接続上の認証にとって重要ではありません。暗号化された情報を交換することもなお可能です。クライアント証明書は、クライアントとサーバーの両者が、正しい相手に暗号化された情報を送信しているという保証を、クライアントとサーバーの両方に与えます。 真の相互認証は、クライアント証明書を使用して可能になります。

いずれの場合も、アクセス制御にクライアント証明書を必要とするように CAS サーバーを設定した場合、クライアントが有効な証明書を持たなければ、クライアントは拒否されます。

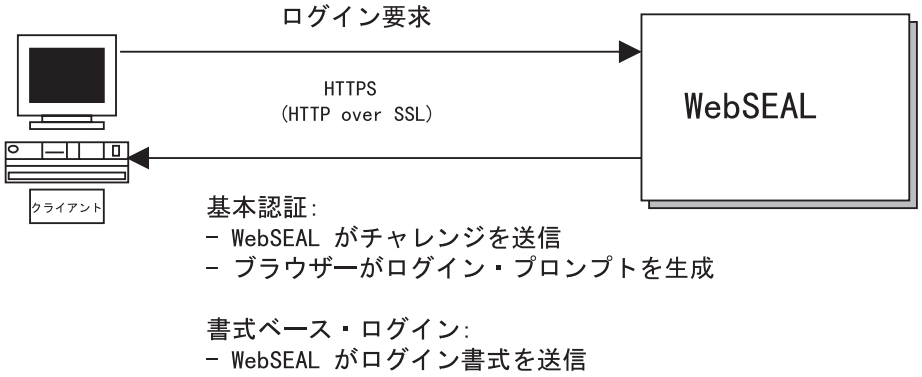
公開キーおよび秘密キーで使用されるクライアント側 X.509 証明書について詳しくは、 179ページの『X.509 証明書による認証方式』を参照してください。

ユーザー名とパスワードによる認証方式

認証プロセスでは、クライアントがログイン時に何らかの形式の識別情報を提示することを必要とします。 Policy Director WebSEAL は、ユーザー名とパスワードによる認証方式をサポートします。

この識別情報の提供には、ユーザー名とパスワードの 2 つの認証方式があります。

- 基本認証
- 書式ベース・ログイン



ユーザー名とパスワードの形式でクライアント識別情報を必要とする認証メカニズムについての全体の情報は、175ページの『ユーザー名とパスワードによる認証方式』を参照してください。

ケルベロス認証

ケルベロスのバージョン 5 は、通常はオープンなネットワーク上で安全に情報を交換する目的で、 2 つの当事者が相互に認証を行えるようにするネットワーク認証プロトコルです。

Policy Director は、次に示す交換において、ケルベロス認証を使用することができます。

- 管理コンソールから管理サーバーへ
- 管理コンソールからセキュリティー・サーバーへ
- 許可サーバーから管理サーバーへ
- WebSEAL から管理サーバーへ
- WebSEAL から DCE レジストリーへ (クライアント認証のために)

Policy Director サーバーは、ケルベロスと NetSEAT クライアント・ネットワーク・モジュールを使用して、 Policy Director セキュア・ドメイン内の他のサーバーと通信します。 NetSEAT は Policy Director セキュリティー・サービスと通信し、情報交換時にセキュアな SSL トンネルをセットアップします。

ケルベロス認証は、認証当事者の両方が信任できるものであるかどうかについて、その信頼性を保証する第三者の基本的信任に依存しています。 この信任された第三者セキュリティー管理サービスは、セキュリティー・サーバー と呼ばれます。

Policy Director セキュリティー・サーバー (secd) は、物理的に安全に保護されたサーバーであり、*レジストリー* と呼ばれるデータベース内にセキュリティー関連情報 (ユーザー名、グループ、パスワードなど) を保管しています。

ケルベロスはサーバー間の相互認証をサポートするために、共用の、セッション特有の、機密キー・メカニズム (LDAP 秘密キー) を使用します。 ケルベロスは、信任されたセキュリティー・サーバーにキーの配布を依頼します。 情報の交換は、リモート・プロシージャー呼び出し (RPC) を使用して行われます。

ケルベロス認証プロトコルは一連のメッセージを複雑に交換します。この一連のメッセージ交換には、機密キーおよび、サーバーがお互いを識別するために必要なその他の情報が含まれます。ケルベロスのゴールは、すべての参加者がお互いのキーを知らずに済むようにすることです。実際、多くのキーの存続期間は、1 つの交換の間だけに限定されます。

クリデンシャルの取得

認証プロセスの主要なゴールの 1 つは、クライアント・ユーザーを記述するクリデンシャル情報を取得することです。 Policy Director は、ユーザーの認証を、*クリデンシャルの取得* と区別します。

ユーザーの識別子は常に定数です。ただし、ユーザーが参加しているグループまたは役割を定義するクリデンシャルは、変化します。特有な文脈を持つクリデンシャルは時間の経過につれて変化します。たとえば、ある人が昇進すれば、クリデンシャルは新しい責任レベルを反映しなければなりません。ある人の仕事上のクリデンシャルは、ユーザーの銀行におけるクリデンシャルとは異なるものです。

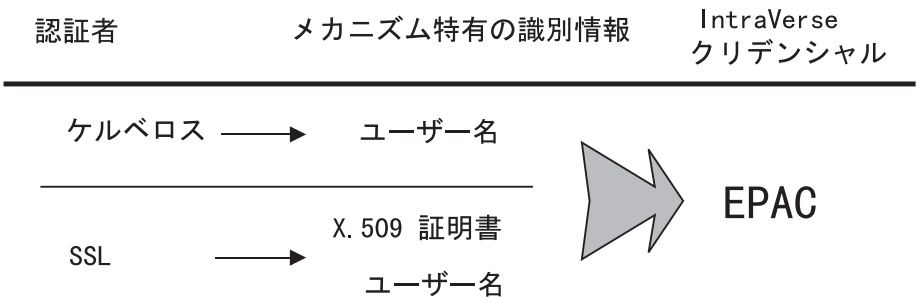
認証プロセスは、メカニズム特有のユーザー識別情報をもたらします。この後、この情報は、共通の、ドメイン全体に通用する表現と形式に変換する (*対応付ける*) 必要があります。 Policy Director は EPAC 形式を使用します。

メカニズム特有の識別情報

クリデンシャル取得サービスにとって、異なる認証メカニズムは異なるユーザー識別情報を提供します。

- ケルベロスは、ユーザー名 (とパスワード) を基にしています。
- X.509 クライアント側ディジタル証明書は、X.509 フィールド情報を提供します。
- 基本認証と書式ベース・ログイン方式 (SSL) は、ユーザー名 (とパスワード) を基にしています。

次の図は、指定された認証メカニズムから得られる識別情報の種類および、情報を EPAC 形式に変換するための SSL 上でのクリデンシャル取得サービスの使用を図示しています。



メカニズム特有な識別情報 (たとえば、パスワード、キーの対、証明書など) は、ユーザーの物理的な識別特性を表します。この情報は、サーバーとの安全なセッションを確立するために使用されます。

この結果のクリデンシャルは、セキュア・ドメイン内のユーザーの役割を表し、特定の文脈でユーザーを記述し、このセッションの存続期間中のみ有効です。

EPAC 証明書

クリデンシャルは、クライアントについての情報を必要とするすべての Policy Director サービスによって使用されます。たとえば、Policy Director 許可サービスはクリデンシャルを使用して、ユーザーがセキュア・ドメイン内の保護されたリソースに特定の操作を実行するように許可されているかどうかを判別します。

Policy Director が ACL を使用する 1 つの方法は、ユニバーサル固有識別子 (UUID) を含む EPAC を使用することです。 Policy Director は次のような他のサービスにもクリデンシャルを使用します。

- 監査サービス
- WebSEAL と NetSEAL 接合での権限委譲機能

次の EPAC フィールドが、Policy Director で使用されます。

属性	説明
セキュア・ドメイン ID	ユーザーのホーム・セキュア・ドメイン識別子
プリンシパル UUID	ユーザーの UUID (または DCE の場合、「プリンシパル」)
グループ UUID	UUID または、ユーザーが属するグループの UUID

メカニズム特有の認証情報は、 EPAC フィールドに変換する必要があります。

- Policy Director クライアントは、 WebSEAL により自動的にクリデンシャルに対応付けられます。
- 外部レジストリーからの Policy Director 以外の SSL クライアントは、外部クリデンシャル取得サービスを使用してユーザー名を Policy Director 識別に対応付けることができます。
- クライアント側 X.509 証明を使用してアクセスするクライアントは、外部クリデンシャル取得サービスを使用して、証明書情報を Policy Director 識別に対応付けることができます。

信任の連鎖

ブラウザー・クライアントと WebSEAL サーバー間の SSL プロトコル交換中に、サーバーはブラウザーに、サーバーが信任する CA の証明書のリストを渡します。これによりブラウザーは、次のいずれかのブラウザー・クライアント証明書のリストをユーザーに表示します。

- それらの CA の 1 つにより署名されたもの。
- サーバーの信任する CA の 1 つと信任の連鎖関係にあることによって信任されたもの -- クライアント証明書は CA によって署名され、その CA の署名 CA はサーバーが信任している CA である。

このプロセスは*証明書連鎖* と呼ばれます。

ブラウザー・ユーザーはこれらのクライアント証明書の 1 つを選択し、サーバーに伝送します。クライアント証明書が、サーバーが信任する CA の 1 つによって直接署名されている場合は、ブラウザーはクライアント証明書だけをサーバーに伝送します (サーバーはすでに署名 CA の証明書を持っていると想定されるので)。

クライアント証明書が、サーバーが信任する CA の 1 つによって直接署名されていない場合、ブラウザーは、クライアント証明書とサーバーの信任 CA の 1 つとの間の信任の連鎖を示す、 CA 証明書連鎖を作成し、伝送します。

この場合も、ブラウザーはサーバーが信任する CA の証明書を実際に伝送することはしません。サーバーはすでにその証明書を持っていると想定されるからです。

Policy Director の secmgrd.conf 構成ファイルは、 Policy Director が信任するルート CA 証明書のリストを含んでいます。 Policy Director は、これらの CA により発行されたクライアント証明書を信任します。

サーバーはブラウザーが伝送したそれぞれの CA 証明書を見て、次のことを検査します。

- 証明書が CA 証明書であること。
- 署名 CA の署名。
- 証明書が有効期限切れでないこと。

信任の連鎖 は、ある CA が 2 番目の CA を信任し、 2 番目の CA が 3 番目の CA を信任し、という場合に設定されます。 Policy Director がこの信任の連鎖内のいずれかの CA を信任している場合、クライアント証明書を信任できるはずです。

クリデンシャル取得サービスの概要

クリデンシャル取得 (Credential acquisition) とは、認証メカニズムにより提供された特定の識別情報を、共通の、ドメイン間で通用する表現形式のクライアント識別子に変換または対応付ける処理です。この共通の表現形式は、*クライアント・クリデンシャル* と呼ばれます。

認証プロセスからもたらされるクリデンシャルは、クライアントについての情報を必要とするすべての Policy Director サービスによって使用されます。このようなサービスの例として、許可や監査があります。 Policy Director の主な役割は、クライアントごとのクリデンシャルの有無に依存します。

Policy Director は、認証プロセスからもたらされたクリデンシャル情報を EPAC 形式を使用して表現します。

Policy Director は、次に該当する SSL クライアントのクリデンシャルを自動的に生成します。

- セキュア・ドメインのメンバー。
- 有効なユーザー名とパスワードを使用して認証されている。

この場合、提供するユーザー名とパスワードは、デフォルトのレジストリー (LDAP) 内の既存のアカウント項目と一致しなければなりません。

上記のモデルに適合しないようなクライアント・アクセスを行う、次のような別のシナリオも可能です。

- クライアントがデフォルトの Policy Director レジストリーに属していない。
- クライアント側証明書を使用してクライアント・アクセスが行われる。

このようなシナリオではすべての場合、Policy Director は、次のことができるカストマイズされた認証と対応付けのサービスに頼らなければなりません。

- これらのクライアントに対する認証の実施。
- 外部 (第三者) アカウント・レジストリーの参照。
- 外部識別情報の Policy Director 識別への対応付け。

このカスタマイズされた認証と対応付けのサービスは、*外部クリデンシャル取得サービス* (CAS) と呼ばれます。

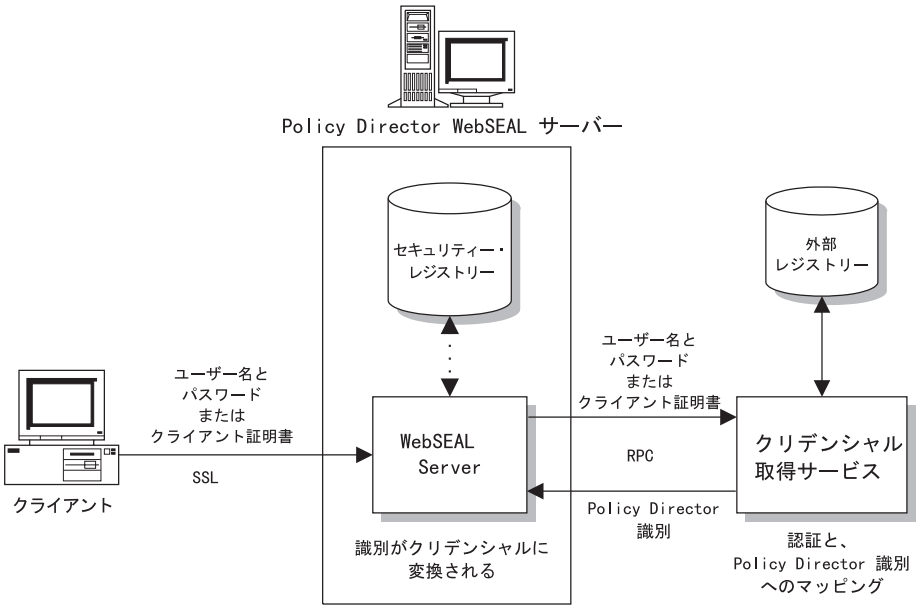
クリデンシャル取得サービスの入門

クリデンシャル取得サービス (CAS) のアーキテクチャーは、デフォルトの WebSEAL SSL 認証プロセス (ユーザー名とパスワードに基づく) を、カスタム外部認証プロセス (Policy Director セキュリティー・レジストリー以外のユーザー・レジストリーを参照できる) で置き換えられるようにします。カスタマイズされたクリデンシャル取得サービスは、任意の特別な識別情報 (証明書、トークン) を、Policy Director の識別に適切に対応付けることも行います。

クリデンシャル取得サービスは、そのセキュア・ドメインに特定したソリューションを提供するために、管理者が特別に作成およびカスタマイズしなければなりません。

クリデンシャル取得サービス (CAS) は、 WebSEAL と CAS サーバー間のすべての通信の安全を保護するために RPC を使用する必要があります。

クリデンシャル取得サービスは、デフォルトの Policy Director レジストリーにアカウントを持たないユーザーがセキュア・ドメインに参加できるようにします。クリデンシャル取得サービスは、(必要な場合、外部レジストリーを使用して) そのユーザーを認証することができます。その後クリデンシャル取得サービスは、証明に変換するために Policy Director 識別を WebSEAL に戻します。Policy Director はこれらのクリデンシャルを使用して、ユーザーがセキュア・ドメインに参加できるようにします。



クリデンシャル取得サービスは、Policy Director が通常使用するレジストリーへの移行が困難または不可能である従来型のユーザー・データベースを適応させることができます。従来型のシステムの例には、顧客 ID や PIN メカニズム (トークン) があります。 このような従来型の認証メカニズムは、固有のレジストリー・データベースを使用してユーザー情報を検査します。

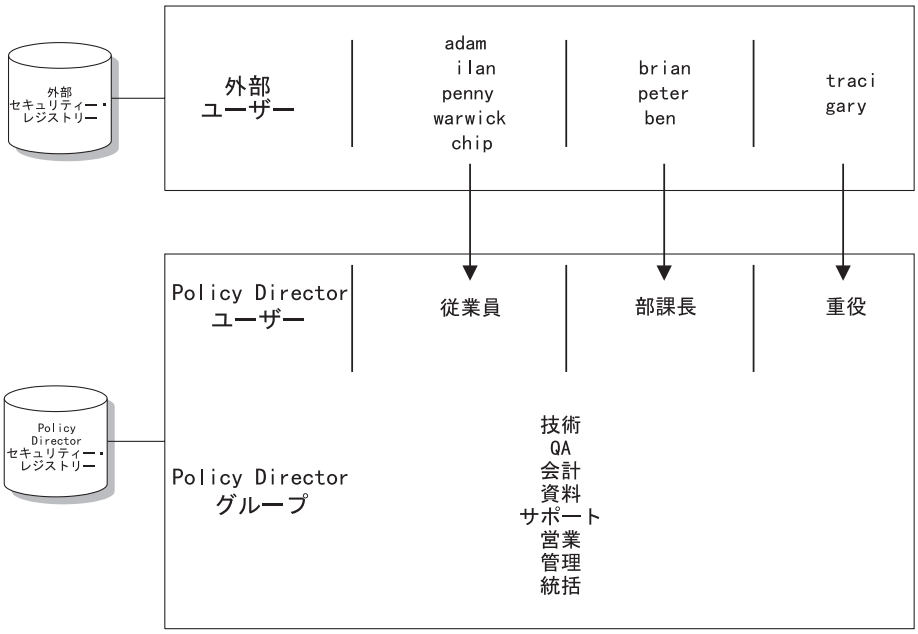
Policy Director 許可アプリケーション開発者キット (IVAuthADK) は、デモンストレーション用の CAS サーバーを提供します。このサーバーは、WebSEAL とクリデンシャル取得サービスの間のインターフェース (IDL) を定義します。ADK は、独自のクリデンシャル取得サービスを作成している場合にはソースの提供もします。

多対 1 の対応付け方式

クリデンシャル取得サービスは、*多対 1* の解決案の場合に最も適切です。つまり、モジュールを使用して、多くの従来のアカウントを 1 つの Policy Director ユーザーに対応付けることができます。

多対 1 の対応付け方式では、ある Policy Director ユーザーがグループの役割を持ち、そのグループのメンバーは従来のデータベースからのユーザーを集めたものです。 多対 1 の対応付け方式は、同じユーザーに対応付けられたすべてのユーザーに、同一のアクセス権、可視性、および責任能力を与えることになります。 特定のユーザーに対応付けられたすべてのユーザーは、まったく同じ許可を持ちます。 セキュリティー・ポリシーを決める際には、この事実を考慮する必要があります。

次の図では、外部レジストリーからのユーザーは、単一の Policy Director ユーザーに対応付けられる場合があります。たとえば、Policy Director ユーザー (Employees) は、外部レジストリーからのユーザーの集合のための役割を果たします。ユーザーは同じ Policy Director アカウントに対応付けられますが、 1 つまたは複数の Policy Director グループのメンバーとして割り当てることにより、個々に区別することもできます。 Policy Director 許可の決定は、ユーザーの識別と、どのグループのメンバーかということの両方に基づいて行うことができます。



注: 多対 1 の対応付けでは、責任能力のレベルをこまかく設定できません。監査サービスは、Policy Director ユーザーのみを追跡し、このユーザーに対応付けられている個々のユーザーは追跡しません。

機能モード

クリデンシャル取得サービスは、クライアント証明書、ユーザー名、トークンなどの認証情報を処理するように作成できます。 WebSEAL は、非レジストリー SSL クライアントを受け付け、認証情報を適切なクリデンシャル取得サービスに渡して、認証と Policy Director 識別への対応付けを行わせるように、構成する必要があります。

クリデンシャル取得サービスは、認証および識別の対応付けを、クライアントが提供した特定の識別情報に基づいて行います。したがってクリデンシャル取得サービスは、可能な次の方法の 1 つで実行するように作成することができます。

- 『X.509 証明書対応付け方式』
- 31ページの『ユーザー名の対応付け方式』

独自で作成したクリデンシャル取得サービスの使用については、35ページの『カスタム・クリデンシャル取得サービス』を参照してください。

X.509 証明書対応付け方式

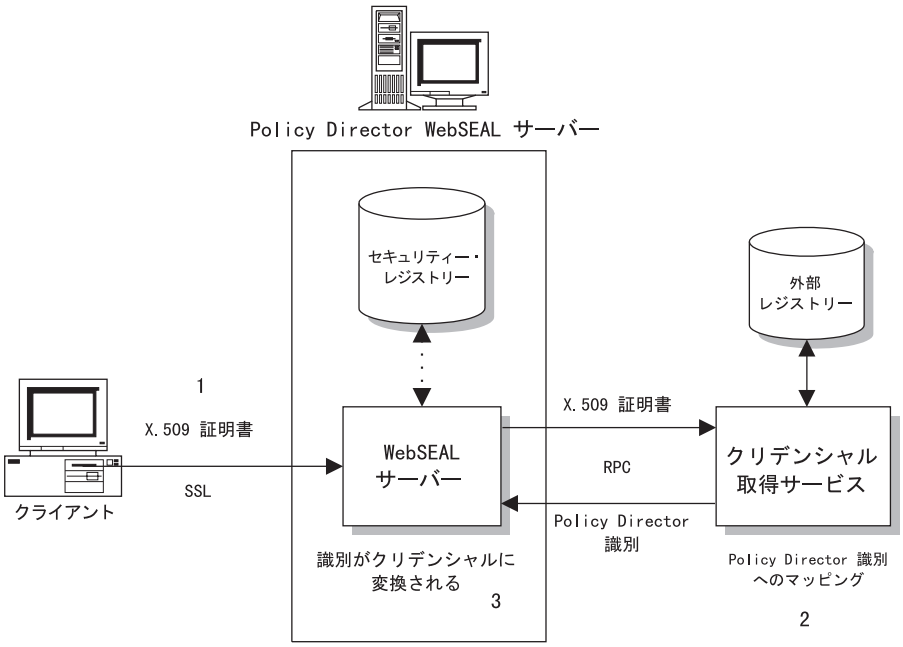
どのクリデンシャル取得サービスを使用しても、Policy Director は、 SSL 上でディジタル X.509 証明書を使用するクライアントの認証をサポートすることができます。クリデンシャル取得サービス X.509 方式は、クライアント側 X.509 ディジタル証明書に含まれる特定の情報を、 Policy Director 識別に対応付けます。この Policy Director 識別は WebSEAL に戻され、 WebSEAL はこれを該当のクリデンシャルに変換します。

X.509 方式は次の条件の下で該当します。

1. クライアントが SSL 上で通信を行う。
2. クライアントが認証に X.509 ディジタル証明書を使用する。
3. クライアントが Policy Director セキュア・ドメイン内の保護リソースへのアクセスを必要とする。

CAS サーバーは、証明書情報を 1 対 1 で、または多対 1 で、 Policy Director 識別に対応付けることができます。対応付けサービスのゴールは、 Policy Director 認証サービスに、許可の決定に役立つクリデンシャルを提供することです。

次の図は、X.509 証明書対応付けにクリデンシャル取得サービスを使用するように WebSEAL を構成した場合に、事象が起こる順序を示しています。



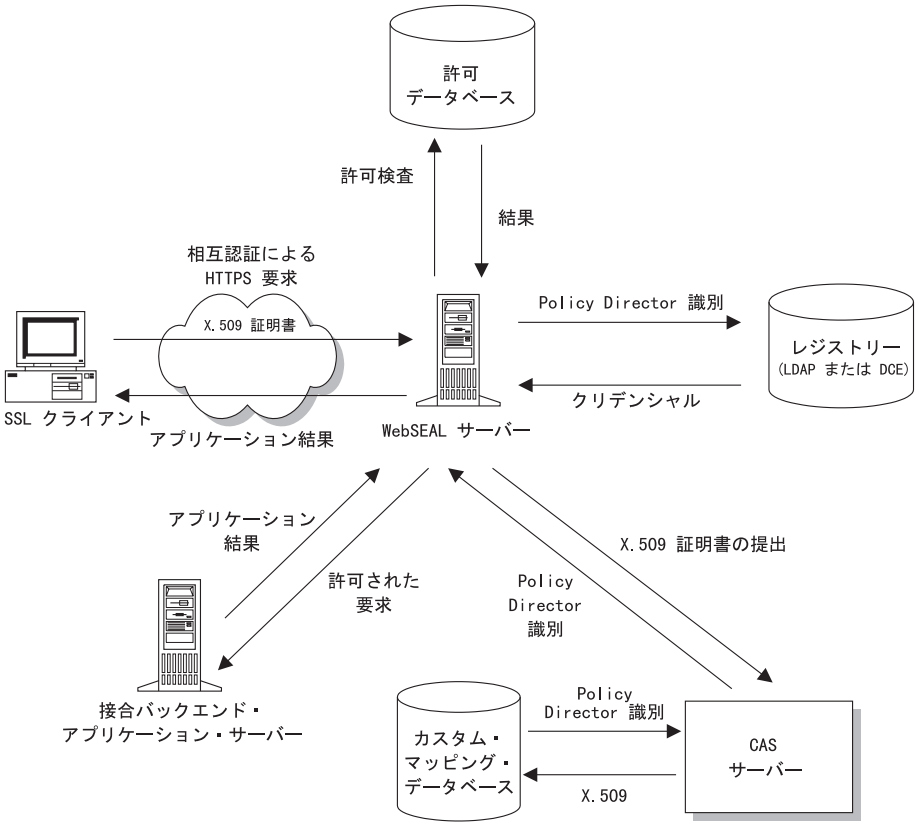
1. クライアントが SSL 上で WebSEAL をアクセスし、X.509 証明書を提示する。

   この時点では、公開キーと秘密キーの証明書交換により、認証が行われていることに注意してください。クリデンシャル取得サービスにとって残りの唯一の義務は、ユーザー・クリデンシャルを対応付けることだけです。
2. CAS サーバーは、妥当性検査された証明書から (アプリケーションに特有な) 識別情報を取り出し、この情報を既知の Policy Director 識別に対応付ける。 CAS サーバーは、外部 (第三者) レジストリーを使用することができます。
3. Policy Director 識別は WebSEAL に戻され、 WebSEAL はそのデフォルトのレジストリーを使用して、識別を該当のクリデンシャルに変換する。

X.509 モードでのクリデンシャル取得サービスの使用

次の図は、X.509 証明書を使用して WebSEAL をアクセスしているクライアントが、セキュア・ドメインにあるリソースを要求する時に起こる事象の全体の順序を示しています。

1. 証明書情報が、クリデンシャル取得サービスによって Policy Director 識別に対応付けられ、クリデンシャル取得サービスはこの識別を WebSEAL に戻す。
2. WebSEAL はこの識別からクリデンシャルを作成し、このクリデンシャルを使用して、結合されたアプリケーション・サーバー上の保護リソースに関係する許可の決定を行う。



ユーザー名の対応付け方式

ユーザー名対応付け方式は、認証および識別の対応付けの別のタイプです。ユーザー名対応付け方式を使用して、デフォルトの認証プロセスをカスタム外部プロセスで置き換えることができ、そのプロセスではデフォルトの Policy Director レジストリー (LDAP) 以外のユーザー・レジストリーを参照することができます。

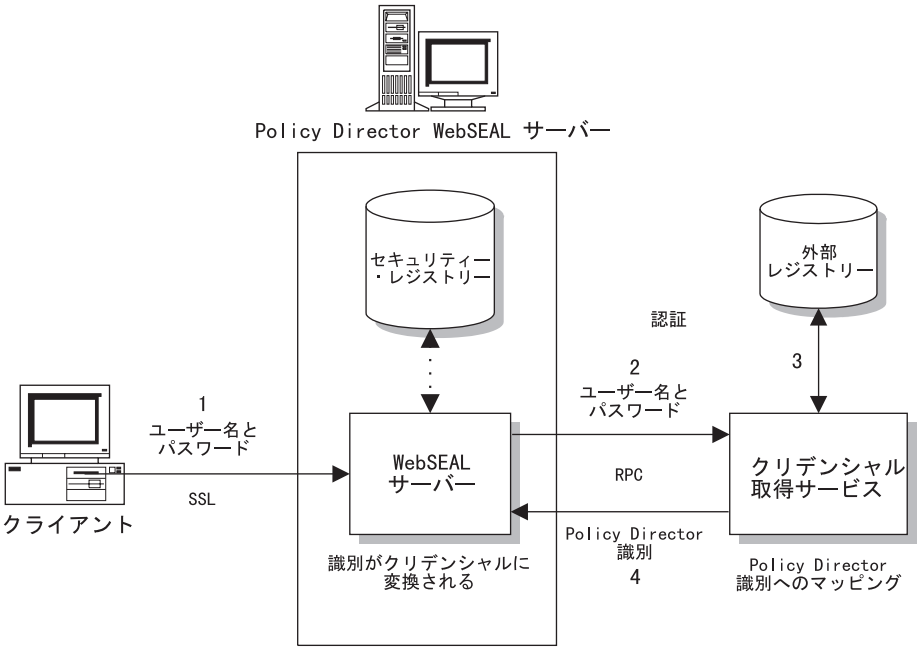
SSL を使用した標準の Policy Director 認証では、ユーザーはユーザー名とパスワードを使用してログインする必要があります。この識別用の認証とクリデンシャル取得は、 Policy Director レジストリーから判別されます。

このタイプのクリデンシャル取得サービスの主な価値は、 Policy Director レジストリーへの移行が困難または不可能である従来型のユーザー・データベースを適応させることにあります。

次の図は、ユーザー名対応付けにクリデンシャル取得サービスを使用するように WebSEAL を構成した場合に、事象が起こる順序を示しています。

1. クライアントがユーザー名とパスワードを使用して、SSL 上で WebSEAL にアクセスする。

2. WebSEAL が、認証およびクリデンシャル取得の両方を行わせるために、ユーザー名とパスワードをクリデンシャル取得サービスに渡すように構成される。



3. クリデンシャル取得サービスは、外部 (第三者) レジストリーを使用してユーザーを認証し、それからユーザーを Policy Director 識別と対応付ける。
4. Policy Director 識別は WebSEAL に戻され、 WebSEAL はそのデフォルトのレジストリーを使用して、識別をクリデンシャルに変換する。

この方式は、多対 1 の解決案として最もよく使用されます。つまり、モジュールにより、多くの従来のアカウントを 1 つの Policy Director ユーザーに対応付けることができます。 28ページの『多対 1 の対応付け方式』を参照してください。

認証サービスの選択項目

認証サービスは、次のいずれかのタイプを選択できます。

- デフォルトの Policy Director クリデンシャル取得サービス (『Policy Director によって提供される CAS』を参照)。
- 独自で作成したクリデンシャル取得サービス (35ページの『カスタム・クリデンシャル取得サービス』を参照)。

Policy Director によって提供される CAS

Policy Director は、独自のクライアント認証サービス構成要素である、Policy Director クリデンシャル取得サービス (Policy Director CAS) を提供します。Policy Director CAS は、ユーザー・レジストリーとして LDAP を使用しているときにサポートされます。

iv.conf および secmgrd.conf 構成ファイルを検査および変更して、認証に Policy Director CAS を使用するように WebSEAL を構成する必要があります (181ページの『Policy Director クリデンシャル取得サービスの構成』を参照)。

Policy Director CAS は、 SSL 使用可能ブラウザーからのクライアント・ディジタル *証明書* を Policy Director ユーザー識別にマップします。保護された Web ページにユーザーがアクセスしようとすると、SSL 使用可能ブラウザーは WebSEAL サーバーに連絡します。WebSEAL がクライアント証明書ベース認証用に構成されている場合、WebSEAL はブラウザーに X.509 証明書を要求します。WebSEAL はブラウザーから証明書を受け取ると、それを CAS サーバーに渡します。Policy Director CAS は、受け取った証明書を、Policy Director が認識しているユーザー識別にマップしようとします。

Policy Director クリデンシャル取得サービスは、次の 1 つまたは両方のクライアント側 X.509 バージョン 3 証明書を使用した SSL 上でのログインをサポートします。

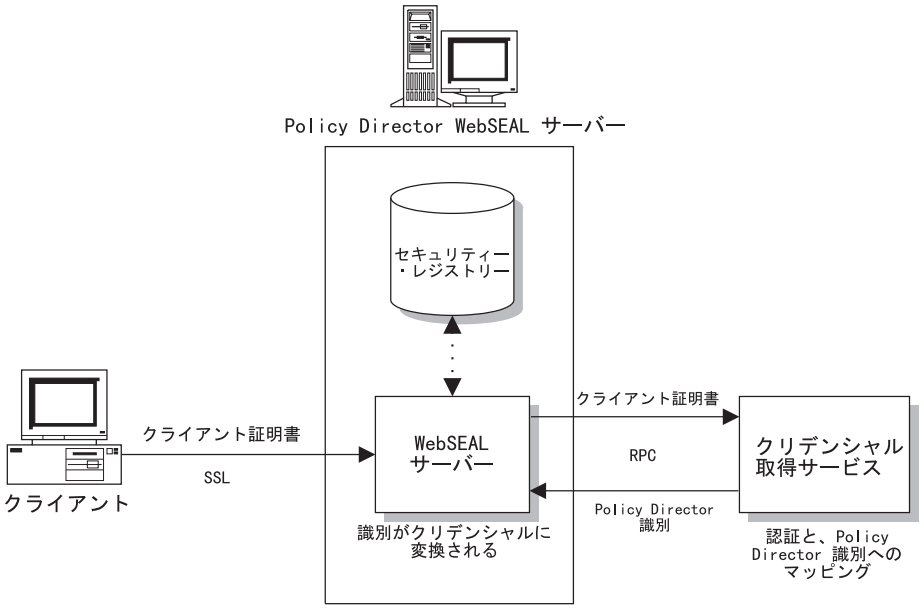
- PKIX 準拠製品 (たとえば、IBM SecureWay Trust Authority、バージョン 3.1)
- Entrust 準拠製品 (たとえば、IBM Vault Registry、バージョン 2.2.2)

すべての証明書は、伝送時に識別エンコード規則 (DER) でエンコードされます。

Policy Director クリデンシャル取得サービスと WebSEAL 間では RPC インターフェースが使用されます。 Policy Director クリデンシャル取得サービス (CAS) は、 RPC を使用して WebSEAL と CAS サーバー間のすべての通信の安全を保護します。Policy Director クリデンシャル取得サービスは DCE-RPC アプリケーションであるため、関係するクライアント識別の対応付けを行う DCE クライアントが必要です。

デフォルトの Policy Director クリデンシャル取得サービスは、

- クライアント側証明書を使用すること、またはクライアント側証明書をオプションとするように指定することを可能にします。
- 関連する証明書取り消しリスト (CRL) の検査は一切行いません。
- 証明書の連鎖をサポートします。
- 1 対 1 の対応付け解決策をサポートします。



1 対 1 の対応付け方式

Policy Director クリデンシャル取得サービスは、1 対 1 の対応付け方式を使用します。個々の従来のアカウントを単一のユーザーに *1 対 1* で対応付けると、より多くのアカウント保守が必要になります。しかし、Policy Director 管理者は、Policy Director CAS の cdas.conf 構成ファイルの中に、証明書の識別名 (DN) を Policy Director (LDAP) ユーザーの DN と関連付けるために使用するテーブルを作成することができます。

Policy Director CAS は、WebSEAL によって証明書で呼び出されると、証明書から DN を抜き出し、一致がないか、この表を調べます。 一致が見つかると、 Policy Director CAS は関連付けられた Policy Director ユーザーの正しい形式の DN を WebSEAL に返します。 WebSEAL はこの DN を受け取ると、それを使って Policy Director (LDAP) ユーザーを識別します。一致が見つからないと、 CAS は証明書からの DN を WebSEAL に返します。 この場合、証明書の DN が、Policy Director (LDAP) ユーザーを識別するために使用されます。WebSEAL サーバーは、返された DN を使用して、ユーザーのクリデンシャルを検索します。

必要な管理作業

Policy Director クリデンシャル取得サービスのセットアップに必要な管理作業には次のものがあります。

1. iv.conf および secmgrd.conf 構成ファイルを検査し、必要ならば変更して、認証に CAS を使用するように WebSEAL を構成する (181ページの『Policy Director クリデンシャル取得サービスの構成』を参照)。
2. 必要に応じて、cdas.conf 構成ファイルの DN マッピング・テーブル・セクションを更新する (183ページの『識別名のマッピング』を参照)。

クリデンシャル取得サービスの機能性

Policy Director クリデンシャル取得サービス (CAS) インターフェースは、次の機能を提供するために使用することができます。

- Policy Director CAS は 1 つの証明書を指定して WebSEAL によって呼び出されます。
- Policy Director CAS は、その証明書から DN を抜き出し、DN 対応付けテーブルを検索して一致があるか調べます。
- 一致が見つかった場合、
  - Policy Director クリデンシャル取得サービスは、関連の Policy Director ユーザーの DN を WebSEAL に戻します。
  - この場合、 WebSEAL は、この DN を使用して Policy Director ユーザーを識別します。
- 一致が見つからない場合、
  - CAS はその証明書の DN を WebSEAL に戻します。
  - 証明書の DN は、Policy Director ユーザーを識別するために使用されます。
  - WebSEAL サーバーは、返された DN を使用して、ユーザーのクリデンシャルを検索します。

カスタム・クリデンシャル取得サービス

それぞれのアプリケーション・サーバーおよび、これに関連した認証フレームワークの多様性を考えた場合、すべての要件を満たす 1 つのクリデンシャル取得サービスを作成することは困難です。 この理由から、 Policy Director には IVAuthADK パッケージの中にデモンストレーション用の CAS サーバー・ソースが含まれています。このデモンストレーション用 CAS サーバーは、アプリケーション特有のユーザー名の対応付けと対応付け管理機能を追加することで、実動用 CAS サーバーの基本的枠組みとして使用することができます。

この場合 WebSEAL は、非レジストリー SSL クライアントを受け付け、認証情報を適切なクリデンシャル取得サービスに渡して、認証と Policy Director 識別への対応付けを行わせるように、構成する必要があります。

カスタム CAS は、RPC を使って、WebSEAL と CAS サーバー間のすべての通信の安全を確保する必要があります。

X.509 証明書情報を Policy Director 識別に対応付けるための要件は、お客様によって大きな相違があります。 Policy Director は対応付けサービスを定義するための汎用的な規則を含んでいませんが、カスタマイズされた対応付けサービスをセットアップしたい管理者を支援するために、次の 2 つの規定があります。

1. Policy Director は、開発者が、X.509 証明書情報を Policy Director 識別に対応付けるための独自のサービスを作成できるようにするために、IDL インターフェースを定義しています。この IDL インターフェースの詳細は、*Policy Director Programmer's Guide and Reference* に記述されています。
2. Policy Director には、 CAS サーバーの枠組みを提供する、対応付けサービスの例が含まれており、この例は各要求に失敗だけを戻します。この枠組みにさらに追加することにより、実動用 CAS サーバーを作成することができます。

   例のサービスのソース・コードは、 Policy Director IVAuthADK 導入パッケージに含まれています。

必要な管理作業

カスタム CAS をセットアップするために必要な管理作業には、次のものがあります。

1. Policy Director が提供する IDL インターフェースを使用する、カスタム CAS を作成する。
2. 外部クリデンシャル取得サービスを認証に使用するように WebSEAL を構成する。

カスタム CAS の機能性

カスタム CAS インターフェースは、次の機能を提供するために使用することができます。

- デフォルトの Policy Director レジストリー以外のユーザー・レジストリーに対して、ユーザー名とパスワードの検査を実施する。
- 多くのユーザーを同一の Policy Director 識別に対応付ける。
- 外部ユーザー・パスワードを管理する。
- 証明に固有の監査情報を追加する。Policy Director は、クリデンシャル全体をその監査ログに書き込みます。

第3章 許可について

許可 とは、識別されたエンティティーに以下のことを実行する権利または権限があるかどうか判別するプロセスです。

- 特定のサービスを開始する。
- セキュア・ドメイン内の特定のリソースで操作を実行する。

Policy Director 許可サービスは、許可決定プロセスを制御することによって、ネットワークのセキュリティー・ポリシーの実施を支援します。

この章は、次の各節に分かれています。

許可の概念モデル

サーバーがセキュア・ドメインでセキュリティーを実施するときは、各クライアントはその識別の証明を提示しなければなりません。 それに対し、セキュリティー・ポリシーは、そのクライアントが要求されたリソースで操作を実行する許可を持つかどうかを判別します。許可サーバーは、セキュア・ドメイン内のすべてのリソースへのアクセスを制御します。 この理由により、認証と許可を求める許可サーバーの要求が、包括的なネットワーク・セキュリティーを実現することになります。

認証 とは、セキュア・ドメインへのログインを試みる個々のユーザーを識別するプロセスのことです。

セキュリティー・システムでは、認証 (authentication) は許可 (authorization) と区別されます。

- *認証* とは、セキュア・ドメインへのログインを試みる個々のユーザーを識別するプロセスのことです。 認証は、その個人が本人であるかを確認しますが、保護されたリソースに操作を実行する権利に関しては何も言いません。
- *許可* は、認証されたクライアントがセキュア・ドメイン内の特定のリソースで操作を実行する権利を有するかどうかを判断します。許可モデルでは、Policy Director はユーザー認証に使用されるメカニズムとは独立して、許可ポリシーを実施します。ユーザーは、公開 / 秘密キー、機密キー、またはユーザー定義のメカニズムを使って、ユーザーの識別を認証できます。

認証プロセスの一部には、クライアントの識別を記述するクリデンシャルの取得が含まれています。許可サービスは、許可決定をユーザーのクリデンシャルに基づいて行います。

セキュア・ドメイン内のリソースは、そのドメイン内のセキュリティー・ポリシーによって指示されたレベルの保護を受けます。セキュリティー・ポリシーは、セキュア・ドメインへの参加を認められる者と、保護を必要とする各リソースを囲む保護の度合いを定義します。

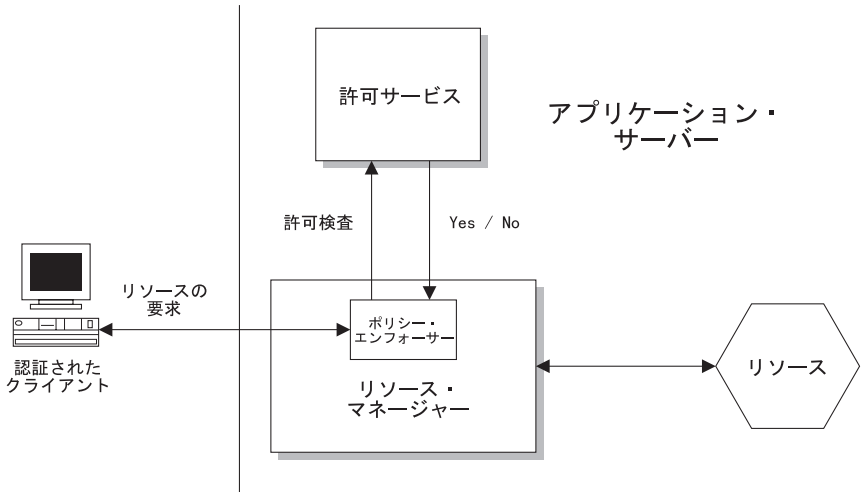
許可プロセスの基本の構成要素は次のとおりです。

リソース・マネージャー

リソース・マネージャーは、Policy Director が許可を認めたときに、要求された操作を実行する責任を負います。リソース・マネージャーの 1 つの構成要素は Policy Enforcer であり、これは、要求を、処理を行うために許可サービスに送信します。

許可サービス

許可サービスは、要求についての決定処理を行います。



従来のアプリケーションでは、ポリシー・エンフォーサー (policy enforcer) とリソース・マネージャーを 1 つのプロセスにまとめていました。この構造の例には、Policy Director WebSEAL と第三者アプリケーションが組み込まれています。 これらの許可構成要素はそれぞれ独立して機能するため、セキュリティー実施戦略の設計における柔軟性が大幅に向上します。

たとえば、この独立性により、セキュリティー管理者は次のものを制御できるようになります。

- プロセスの位置。
- プロセス用のコードを書き込む担当者。
- プロセスがそのタスクを実行する方法。

標準許可サービスの利点

ほとんどのシステム (レガシー、新規の両方のシステム) における許可は、個々のアプリケーションと密結合されています。各会社では、通常、時間をかけて、ビジネス・ニーズに対応するアプリケーションを作成します。これらのアプリケーションの多くは、それぞれ特定の形式の許可を必要とします。

結果として、多くの場合、許可インプリメンテーションがそれぞれに異なっている、多種多様なアプリケーションが作成されることになります。これらの所有許可インプリメンテーションでは、別個の管理を必要とし、統合がむずかしく、結果として所有コストが高くなります。

分散許可サービスは、これらの独立アプリケーションに標準の許可決定メカニズムを提供します。

標準許可決定サービスには次の利点があります。

- アプリケーションの開発コストおよび、そのアプリケーションへのアクセスの管理コストを削減する。
- 個別の許可システムを所有 / 管理するための合計コストを削減する。
- 既存のセキュリティー・インフラストラクチャーの優れた部分を活用できる。
- 新しいビジネスをより安全にオープンできるようになる。
- もっと多くの新しい、異なる種類のアプリケーションを使用可能にできる。
- 開発サイクルを短縮できる。
- 情報を安全に共用できる。

Policy Director 許可サービスの利点

Policy Director は、既存の従来型および発展段階のインフラストラクチャーに統合できます。 Policy Director は、安全な集中ポリシー管理機能を提供します。 Policy Director 許可サービスを WebSEAL および NetSEAL リソース・マネージャーと併用すると、ビジネス・ネットワーク・システムで標準許可メカニズムが使用できるようになります。

既存アプリケーションは、そのアプリケーションそのものを変更しなくても、許可サービスを活用できます。 Policy Director は、その許可ポリシーの基本をユーザーの役割またはグループの役割に置いています。許可ポリシーの適用対象は次のとおりです。

- ネットワーク・サーバー
- 個々のトランザクションまたはデータベース要求
- 特定の Web ベース情報
- 管理活動
- ユーザー定義のオブジェクト

Policy Director 許可 API は、既存のアプリケーションが Policy Director 許可サービスを呼び出せるようにします。許可サービスは、会社のセキュリティー・ポリシーに基づいて決定を下します。 48ページの『Policy Director 許可 API』を参照してください。

Policy Director 許可サービスは、拡張も可能です。外部 Policy Director 許可 API を使用することにより、他の許可サービスを呼び出して追加処理を行わせるように、Policy Director 許可サービスを構成することができます。

Policy Director 許可サービスには次の利点があります。

- アプリケーションから独立している。
- 言語に左右されない標準の許可コーディング・スタイル (Policy Director 許可 API) を使用する。
- このサービスは集中管理されるため、管理が容易である。たとえば、新しい従業員を追加する場合、複数のシステムにわたってその変更を行うのではなく、1 つの中央設置場所にある特権データベースを変更するだけですみます。

- 異種プラットフォーム間環境において、セキュリティー・サービスのアプリケーションを可能にする。
- 既存の非 Policy Director 許可システムを、外部許可サービス機能を通じて統合する。
- 既存のインフラストラクチャーと簡単に統合できる、拡張が容易で柔軟性の高いアーキテクチャーを持つ。
- 複数の層にわたる許可を可能にする - このサービスは、アプリケーション・プロセスまたはトランザクションの複数の層を経由して、クリデンシャル・パケットを渡します。
- 一般的かつ効果的な監査モデルを使用している。
- どの認証メカニズムからも独立している。

Policy Director 許可サービス

Policy Director 許可サービスは、ネットワーク・セキュリティー・ポリシーの実施を支援する許可決定プロセスに関する責任を負っています。許可サービスによって行われた許可の決定によって、セキュア・ドメインの保護リソースで操作を実行するためのクライアントの要求が承認または拒否されます。

Policy Director 許可サービスの構成要素

Policy Director 許可サービスを構成する 3 つの基本構成要素は次のとおりです。

- 1 次 (マスター) 許可ポリシー・データベース
- 管理サーバー
- 許可決定評価基準

マスター許可ポリシー・データベース

1 次許可ポリシー・データベースには、セキュア・ドメイン内のすべてのリソースに関するセキュリティー・ポリシー情報が入っています。このデータベースには、セキュア・ドメインの参加者に関連する、必要なクリデンシャル情報もすべて入っています。

このデータベースへの入力や内容の変更は、Policy Director 管理コンソールを使用して行います。

管理サーバー

管理サーバー (ivmgrd) は次のタスクを実行します。

- 1 次許可ポリシー・データベースを保守する。
- セキュア・ドメイン全体にこのポリシー情報を複写する。
- 1 次許可ポリシー・データベースに変更が行われた場合に必ずデータベース・レプリカを更新する。

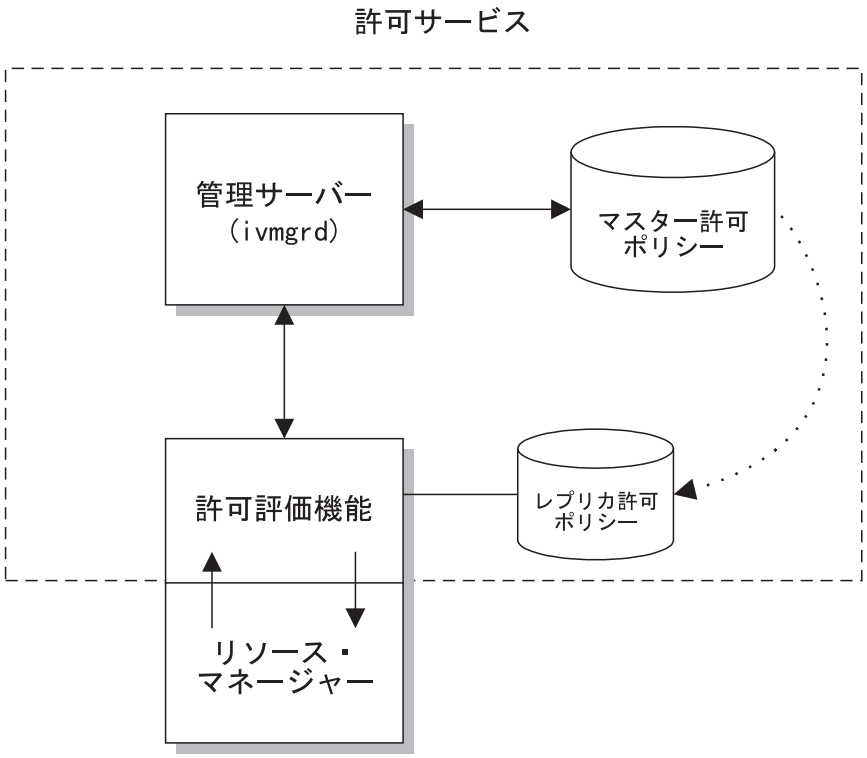
管理サーバーは、セキュア・ドメインで稼働している他の Policy Director と非 Policy Director サーバーに関する位置情報の保守も行います。

注: どのセキュア・ドメインでも管理サーバーのインスタンスは 1 つだけでなければなりません。

許可評価基準

許可評価機能は、保護リソースにアクセスするクライアントの能力を、セキュリティー・ポリシーに基づいて決定する許可決定プロセスのことです。この評価機能は、リソース・マネージャーに対して勧告を行い、リソース・マネージャーはそれにしたがって対応します。

次の図は、Policy Director 許可サービスの主な構成要素を示しています。



Policy Director 許可サービスのインターフェース

Policy Director 許可サービスには、2 つのインターフェースがあり、そこで対話が行われます。

管理インターフェース

セキュリティー管理者は、ネットワークのセキュリティー・ポリシーを管理します。セキュリティー管理者は、Policy Director 管理コンソールまたは、**ivadmin** ユーティリティーを使用して、次のことを行います。

- ネットワーク・リソースにポリシー規則 (テンプレート) を適用する。
- セキュア・ドメインの参加者のクリデンシャルを登録する。

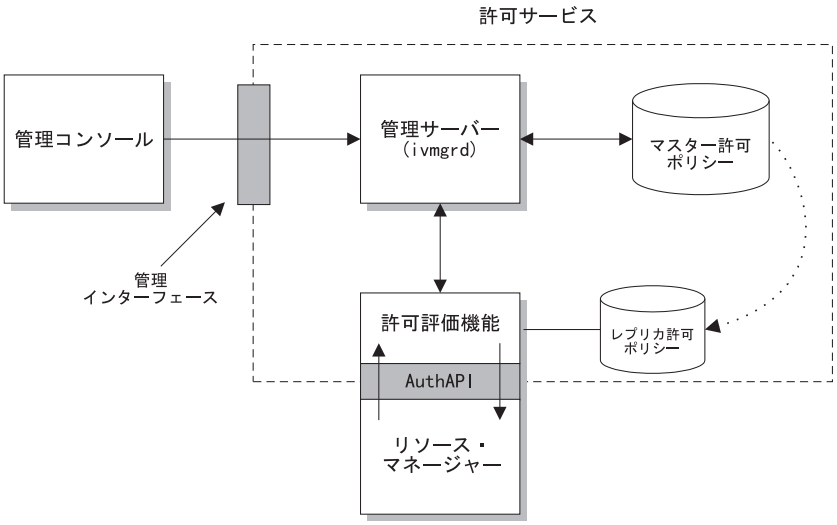
管理コンソールは、このセキュリティー・ポリシー・データを、管理サーバーを使用する 1 次許可ポリシー・データベースに適用します。

このインターフェースには、ネームスペース、ポリシー・テンプレート、クリデンシャルについての詳しい情報が含まれています。

許可 API

Policy Director 許可 API は、リソース・マネージャーからの許可決定の要求

を許可評価機能に渡し、これを受けた許可評価機能は勧告を戻します。 *Policy Director Programmer's Guide and Reference* には、この API の詳細が記載されています。



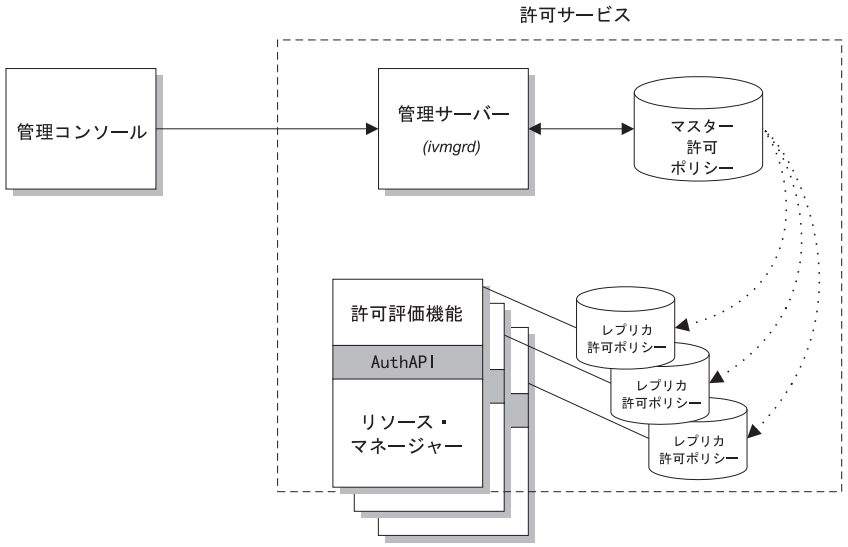
スケーラビリティーとパフォーマンスのための複写

Policy Director の許可サービス構成要素を複写して、要求量の多い環境での可用性を増すことができます。

Policy Director は必ず、ポリシー規則とクリデンシャル情報を含む 1 次許可ポリシー・データベースを自動的に複写します。許可サービスを呼び出すアプリケーションには、このデータベース情報を参照するためのオプションが 2 つあります。

- このアプリケーションは、許可評価機能とシームレスに働くように構成されている場合、データベースのローカル・キャッシュを使用します。データベースの複写は、ローカル・キャッシュ・モードで許可サービスを使用する各アプリケーションごとに行われます。
- このアプリケーションは、リモート Policy Director 許可サーバー構成要素によってキャッシュに入れられる共用レプリカを使います。 データベースの複写は、Policy Director 許可サーバーの各インスタンスごとに行われます。 多くのアプリケーションでは 1 つの許可サーバーへのアクセスが可能です。

管理サーバーから更新が通知されると、全レプリカを更新するキャッシュ・プロセスが起動されます。この更新の通知は、 1 次許可ポリシー・データベースが変更された場合には必ず行われます。



パフォーマンス上の注記:

- アプリケーション・サーバーは、更新の通知を管理サーバーから直接送られます。アプリケーション・サーバーは、数分ごとに 1 次許可ポリシー・データベースのバージョンを検査します。検査では、アプリケーション・サーバーが更新通知を受け取り損ねていないか確認されます。

  更新通知がサーバーに到達できなかった場合、Policy Director はログ項目を作成します。どちらの場合も、再試行メカニズムが、後で必ず更新が行われるようにします。
- 許可ポリシー情報がキャッシュに入れられることで、システム・パフォーマンスが向上します。 たとえば、WebSEAL は、許可検査を行うとき、それ自身のキャッシュ・バージョンのデータベースのポリシー・テンプレートを検査します。WebSEAL は、1 次データベースからこの情報を入手するためにネットワークにアクセスする必要はありません。 この結果、許可検査の応答時間 (パフォーマンス) が速くなります。
- 呼び出しアプリケーション・サーバーは、個々の許可結果をキャッシュしません。

ネットワーク・セキュリティー・ポリシー

ドメインへのユーザーの参加とグループの参加を制御する方法によって、セキュア・ドメインのセキュリティー・ポリシーが決まります。セキュリティー・ポリシーは、保護を必要とするリソースに規則を適用します。 これらの規則がポリシー・テンプレート と呼ばれるものです。

Policy Director 許可サービスは、ユーザーの識別とクリデンシャルを、要求されたリソースに割り当てられたポリシー・テンプレートと突き合わせることによってこのポリシーを実施します。 Policy Director は、結果として出された勧告をリソース・マネージャーに渡し、リソース・マネージャーが元の要求への応答を完了させます。

ネットワーク・セキュリティー・ポリシー定義

Policy Director 許可サービスは、セキュア・ドメインの全リソースと、各リソースに割り当てられたポリシー・テンプレートをリストした中央データベースを使用します。この 1 次許可ポリシー・データベースとセキュリティー・レジストリーは、ネットワーク・セキュリティー・ポリシーの定義を援助するキー構成要素です。セキュリティー・レジストリーには、ユーザー・アカウントとグループ・アカウントが入っています。

要約すると、ネットワーク・セキュリティー・ポリシーの制御対象は、次のようになります。

- セキュア・ドメインへの参加が認められたユーザーとグループ。セキュリティー・レジストリーは、この情報を含み、保守します。
- セキュア・ドメインの全オブジェクトの保護レベル。1 次許可ポリシー・データベースがこの情報を保守します。

保護オブジェクト・ネームスペース

保護オブジェクト・ネームスペース は、セキュア・ドメインに所属するリソースを階層で示したものです。階層ネームスペースに現れるオブジェクトは、実際のネットワーク・リソースを表します。

- **システム・リソース** -- 実際の物理ファイル、ネットワーク・サービス、またはアプリケーション。
- **保護オブジェクト** -- Policy Director 許可サービス、管理コンソール、およびその他の Policy Director 管理ユーティリティーが使用する実際のシステム・リソースの論理表示。

ポリシー・テンプレートをネームスペース内のオブジェクトに付加すると、そのリソースの保護を行うことができます。 Policy Director 許可サービスは、これらのテンプレートに基づいて許可の決定を下します。

Policy Director は、次のネームスペース・カテゴリーを使用します。

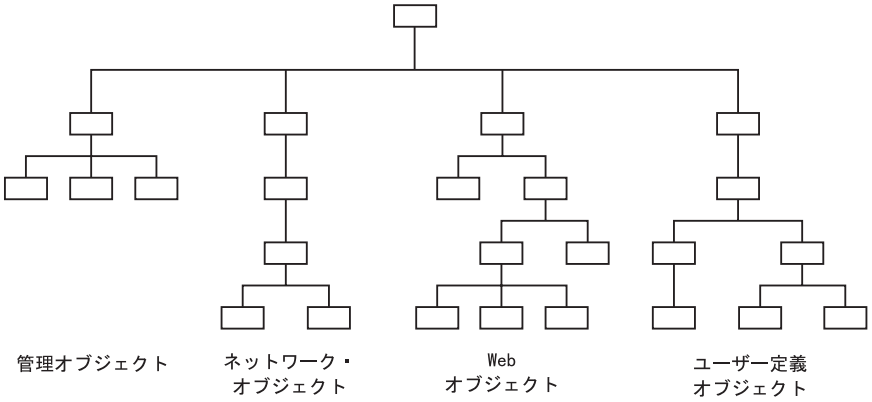
Web オブジェクト
このオブジェクトは、静的 Web ページや動的 URL など、HTTP URL がアドレス指定できるものを表します。この静的 Web ページと動的 URL は、データベース照会や、その他のタイプのアプリケーションに変換できます。

ネットワーク・オブジェクト
このオブジェクトは、アプリケーションで使用する TCP ネットワーク・アドレス (ポート) に対応付ける、 TCP ベースのアプリケーション (TELNET や FTP など) を表します。

管理オブジェクト
このオブジェクトは、Policy Director 管理コンソールを使って実行できる管理活動を表します。このオブジェクトは、ユーザーを定義し、セキュリティー・ポリシーを設定するために必要なタスクを表します。 Policy Director は、管理活動の代行をサポートし、セキュリティー・ポリシーを設定する管理者の能力を、ネームスペースのサブセットに制限することができます。

ユーザー定義のオブジェクト
このオブジェクトは、Policy Director 許可サービスを使用するアプリケーショ

ンが保護するタスクまたはネットワーク・リソースを表します (Policy Director 許可サービスは Policy Director 許可 API を使用)。



ポリシー・テンプレートの定義と適用

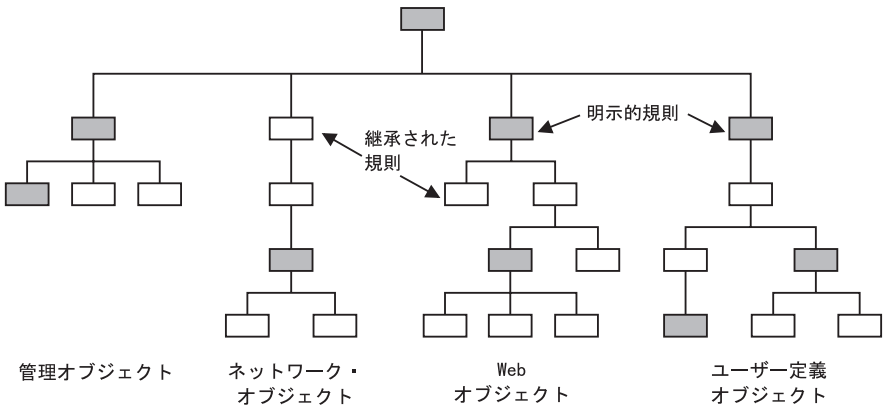
セキュリティー管理者は、ポリシー・テンプレートと呼ばれる規則を定義し、それらのテンプレートをネームスペース内のリソースのオブジェクト表示に適用することによって、システム・リソースを保護します。

Policy Director 許可サービスは、これらのオブジェクトに適用されたポリシー・テンプレートに基づいて許可の決定を下します。 Policy Director が保護オブジェクトで要求された操作を実行することを認めると、そのリソースに関する責任を負っているアプリケーションがこの操作を実行します。

1 つのポリシー・テンプレートが、多数のオブジェクトの保護パラメーターを指示できます。この規則に変更があった場合、そのテンプレートが付加されているすべてのオブジェクトに影響します。

明示的に継承されるポリシー

ポリシーは明示的に適用または継承できます。Policy Director の保護オブジェクトは、セキュリティー・ポリシー属性の継承をサポートしています。このことは、ネームスペースを管理するセキュリティー管理者にとって重要な考慮事項になります。管理者は、規則を変更しなければならない階層内の場所にだけ、明示的にポリシー・テンプレートを適用するだけですみます。



ポリシー・テンプレート・タイプの例として、次のものが挙げられます。

- ハード・コーディング規則
- 外部許可機能
- 特殊セキュア・ラベル
- アクセス制御リスト

アクセス制御リスト

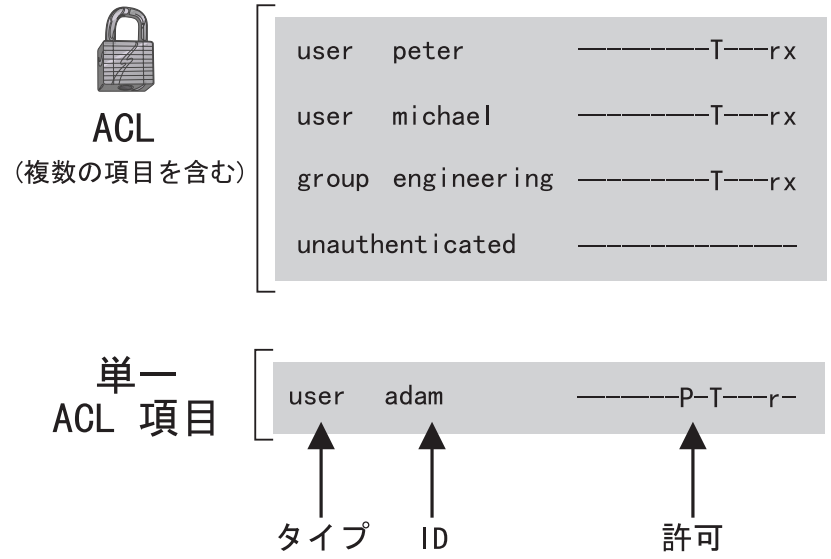
アクセス制御リスト (ACL) は、ポリシー・テンプレートの 1 例です。 Policy Director は ACL をその 1 次ポリシー・テンプレートとして使用します。

ACL は、そのリソースで特定の操作を行うために必要な条件を指定する制御 (許可) の集合です。 ACL 定義は、セキュア・ドメイン用に設定されたセキュリティー・ポリシーの重要な構成要素です。 ACL は、他のすべてのポリシー・テンプレートと同様に、組織のセキュリティー・ポリシーを、保護オブジェクト・ネームスペースで表されているリソースにスタンプするために使用します。

具体的に、ACL が制御する対象は次のとおりです。

- リソースで実行される操作。
- それらの操作を実行できる人々。

ユーザー指定とグループ指定を含む 1 つまたは複数の項目に、それらの特定の許可または権利を加えたもので ACL が構成されます。

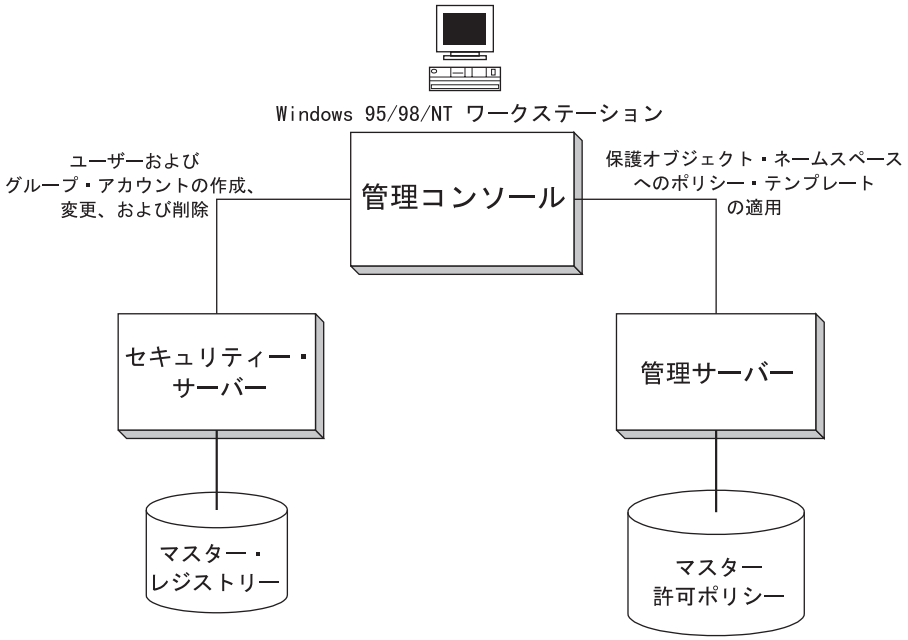


ポリシー管理

Policy Director 管理コンソールは、Java を基にしたグラフィック・アプリケーションであり、 Policy Director セキュア・ドメインのセキュリティー・ポリシーを管理するために使用されます。オプションの **ivadmin** コマンド行ユーティリティーは、管理コンソールと同じ管理機能を提供します。

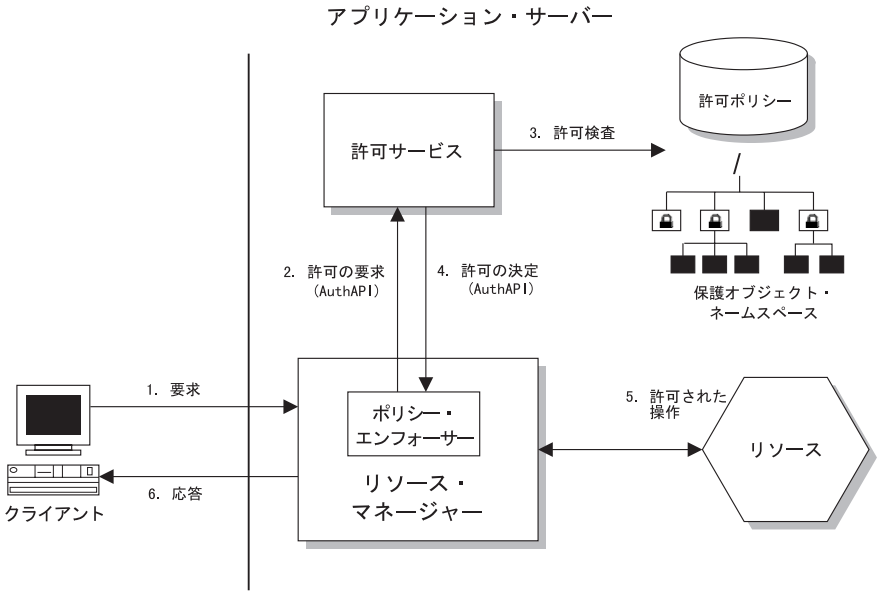
管理コンソールから、または **ivadmin** ユーティリティーを使って、セキュリティー・サーバー・レジストリー、1 次許可ポリシー・データベース、および全 Policy Director

サーバーを管理できます。 また、ユーザーとグループを追加または削除したり、ポリシー・テンプレートまたは ACL をネットワーク・オブジェクトに適用できます。



ステップバイステップの許可プロセス

次の図は、許可プロセスの全体像を示したものです。



1. Policy Director は、リソースに関する認証済みクライアント要求を、リソース・マネージャー・サーバーに送信します。ポリシー・エンフォーサー・プロセスが、その要求を代行受信します。

リソース・マネージャーは、WebSEAL (HTTP および HTTPS アクセスの場合)、NetSEAL (TCP/IP ネットワーク・アクセスの場合)、または第三者のアプリケーションのいずれでもかまいません。

2. ポリシー・エンフォーサー・プロセスは Policy Director 許可 API (『Policy Director 許可 API』を参照) を使用して、許可の決定を行うために Policy Director 許可サービスを呼び出します。
3. 許可サービスは、Policy Director 保護オブジェクト・ネームスペースのオブジェクトとして表されているリソースで許可検査を実行します。そのオブジェクトに適用されているポリシー・テンプレートは、クライアントのクリデンシャルに照らし合わせて検査をします。
4. 要求を受け入れるか拒否するかの決定に関し、リソース・マネージャーへの勧告 (ポリシー・エンフォーサーを使用) が戻されます。
5. 許可検査で要求が承認されると、リソース・マネージャーはその要求を該当のリソース担当のアプリケーションに渡します。
6. クライアントは、要求された操作の結果を受け取ります。

Policy Director 許可 API

Policy Director 許可アプリケーション・プログラム・インターフェース (API) を使用して、Policy Director アプリケーションと第三者アプリケーションは、Policy Director 許可サービスを照会して、許可の決定を下すことができます。

Policy Director 許可 API は、リソース・マネージャー (許可検査を要求する) と許可サービスそのものの間のインターフェースです。 Policy Director 許可 API によって、ポリシー実施アプリケーションが許可の決定を尋ねることができますが、 Policy Director 許可 API は、そのアプリケーションが実際の許可決定プロセスの煩雑さに煩わされないようにします。

Policy Director 許可 API は、許可要求と決定のコーディング用に標準のプログラミング・モデルを用意しています。 Policy Director 許可 API では、どのレガシー・アプリケーション、または新しく開発されたアプリケーションからでも集中管理許可サービスに標準化された呼び出しをかけることができます。

Policy Director 許可 API は、次の 2 つのモードのどちらかで使用できます。

リモート・キャッシュ・モード

このモードの場合、Policy Director は、リモート Policy Director 許可サーバー (ivacld) を呼び出して、アプリケーションに代わって許可決定を下すように API を初期化します。 Policy Director 許可サーバーは、許可ポリシー・データベースのレプリカの、それ自身のキャッシュを保守します。 このモードは、アプリケーション・クライアントからの許可要求を処理する場合に使用します。

50ページの『リモート・キャッシュ・モード』を参照してください。

ローカル・キャッシュ・モード

このモードの場合、Policy Director は、アプリケーションの許可データベースのローカル・レプリカをダウンロードし、保守するように API を初期化します。ローカル・キャッシュ・モードでは、アプリケーションが、すべての許可決定をローカルに行うため、パフォーマンスと信頼性が向上します。

しかし、データベース複写のオーバーヘッドと、このモードを使用する場合のセキュリティー上の意味を考慮すると、このモードは、トラステッド・アプリケーション・サーバーが使用するのが最適ということになります。トラステッド・アプリケーション・サーバーには WebSEAL と NetSEAL があります。

51ページの『ローカル・キャッシュ・モード』を参照してください。

Policy Director 許可 API の 1 次値と利点は、ユーザーが、許可サービス・メカニズムの煩雑さに煩わされないようにするその機能にあります。 Policy Director は、管理、保管、キャッシュ、複写、クリデンシャル・フォーマット、および認証方式の問題を、Policy Director 許可 API の背後に隠します。

Policy Director 許可 API は、その基礎となるインフラストラクチャー、クリデンシャル・フォーマット、および評価メカニズムから独立して機能します。 Policy Director 許可 API は、許可検査を要求して、その応答として単純に “yes” か “no” を受け取ることを可能にします。 許可検査メカニズムの詳細はユーザーからは見えません。

Policy Director 許可 API は、次のプラットフォームに対するサポートを提供します。

- Microsoft Windows NT、Windows 98、および Windows 95
- IBM AIX バージョン 4.3
- Sun Solaris バージョン 2.6

許可 API の例

WebSEAL と NetSEAL 許可サービスは、URL とポートでそれぞれにアクセス制御を行います。第三者アプリケーションは Policy Director 許可 API を使って、極めて限定された特殊プロセスでアクセス制御を行います。

例 1: タスク・ボタンを許可検査の結果に応じてアクティブまたは非アクティブとして動的に表示する、グラフィカル・ユーザー・インターフェース (GUI) を設計できます。

例 2: 次の図は、 Policy Director 許可 API のもう 1 つの使用法を示しています。この図は、Web アプリケーションによる CGI トランザクションの要求を表しています。

図 A に示す最下位の許可では、URL について「オール・オア・ナッシング (all-or-nothing)」、すなわち実行可能か、不可能かというアクセス制御が行われます。 この粗いレベルの許可では、クライアントが CGI プログラムが実行できるかどうかだけが決定されます。 CGI アプリケーションへのアクセスを認めると、CGI アプリケーションが操作するリソースに対してそれ以上の制御はできません。

図 B の場合、アクセス制御は CGI プログラムが操作するリソースの集合です。 Web アプリケーションは、この Policy Director 許可 API を使用するように構成されています。 ここで、 CGI プログラムは Policy Director 許可サービスを呼び出して、それが操作するリソースについての許可決定を下すことができます。 許可の決定は要求側クライアントの識別に基づいて行うことができます。

図 A

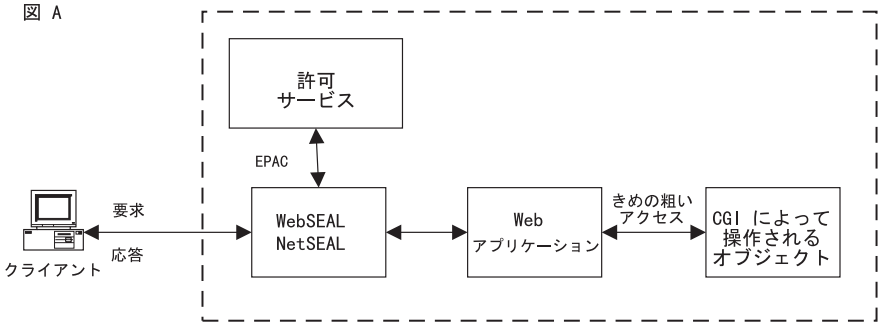
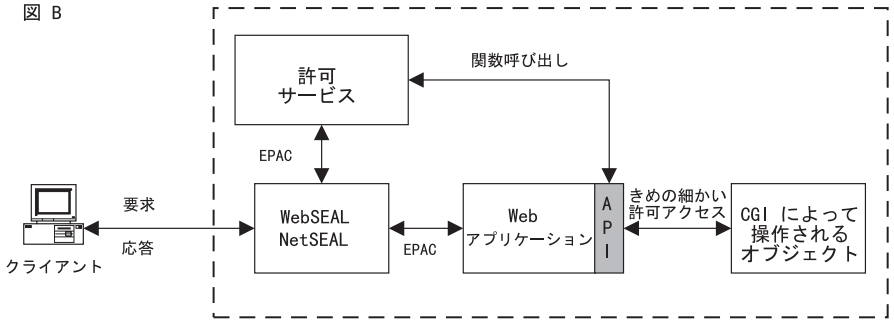


図 B

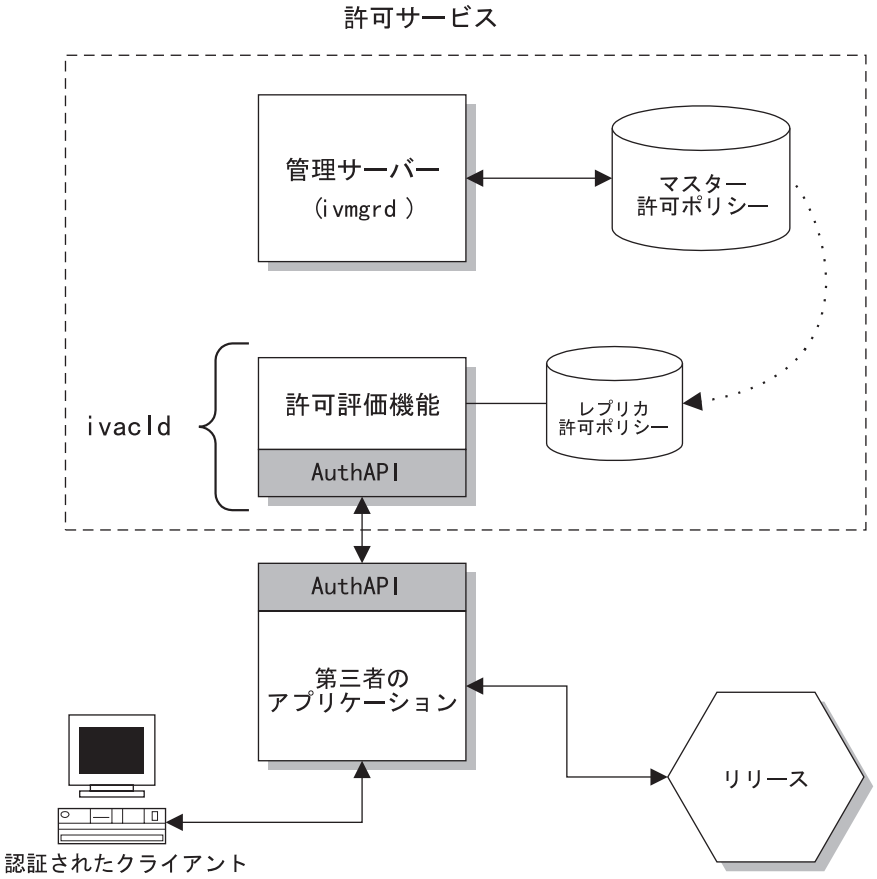


リモート・キャッシュ・モード

リモート・キャッシュ・モードでは、アプリケーションは、 Policy Director 許可 API が提供する関数呼び出しを使って、リモートの Policy Director 許可サーバー (ivacld) と通信します。 Policy Director 許可サーバーは、許可決定評価基準として機能し、それ自身の許可ポリシー・データベース・レプリカを保守しています。

Policy Director 許可サーバーは、決定を行い、 API を使ってアプリケーションに勧告を戻します。許可サーバーは、許可決定要求の詳細を含む監査レコードを書き込むこともできます。

セキュア・ドメイン内のどこかで、 Policy Director 許可サーバーが実行されていなければなりません。 Policy Director 許可サーバーはアプリケーションと同じマシン上にも、別のマシン上にも常駐できます。 また、セキュア・ドメイン内の複数のマシンに Policy Director 許可サーバーをインストールして、可用性を高めることもできます。 Policy Director 許可 API は、特定の Policy Director 許可サーバーが失敗すると、それに伴って透過的に失敗します。



ローカル・キャッシュ・モード

ローカル・キャッシュ・モード では、API は、許可ポリシー・データベースのレプリカをアプリケーションのローカル・ファイル・システムにダウンロードして保守します。このモードの API は、すべての許可決定をメモリー内で行うため、パフォーマンスと信頼性が増します。

ローカル・レプリカは、そのアプリケーションの呼び出しでは、持続性を保ちます。 API はレプリカ・モードで始動します。始動時には、1 次許可ポリシー・データベースに更新があったかどうかを検査します。この更新とは、ローカル・レプリカが作成された後に行われた可能性のあるものです。

図 A

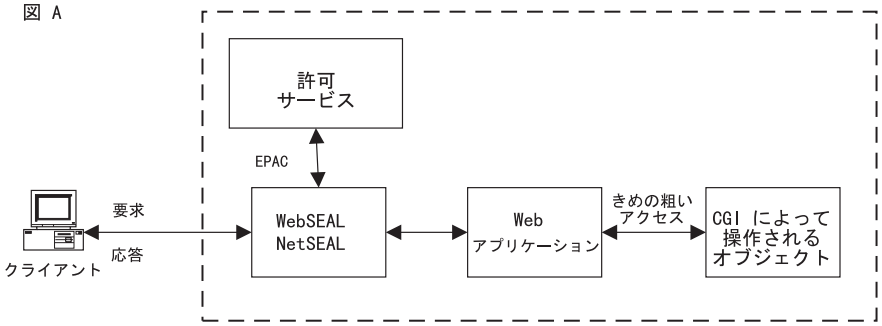
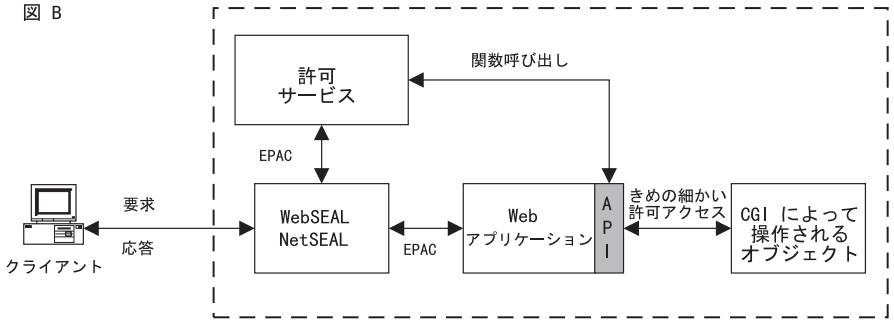


図 B



外部許可機能

一部の状況においては、Policy Director 許可の標準セットが、組織のセキュリティー・ポリシーが必要とする許可規則をすべて表せない場合があります。 Policy Director は、オプションの外部許可機能を用意して、追加の許可要件に対応できるようにしています。

外部許可サービスでは、別個の外部許可サーバー・プログラムによって指示される、追加の許可制御と条件を設けることができます。

許可サービスの拡張

Policy Director 許可サービスは外部許可機能を自動的に作成します。 外部許可サービスを構成すると、Policy Director 許可サービスは、新しい制御と条件をその評価プロセスに単純に組み込みます。

Policy Director 許可サービスを使用するアプリケーションには、WebSEAL、NetSEAL、そして Policy Director 許可 API を使用するアプリケーションなどがあります。 これらのアプリケーションは、構成された外部許可サービスの追加 (ただしシームレスの) 機能を利用できます。外部許可サービスの使用によるセキュリティー・ポリシーへの追加は、それらのアプリケーションにも同様に行われ、それらのアプリケーションを変更する必要はありません。

外部許可サービス・アーキテクチャーによって、組織の既存のセキュリティー・サービスを完全統合できます。外部許可サービスは、セキュリティー・メカニズムへの会社の初期投資をそのまま残します。この外部許可サービスでは、レガシー・サーバーを Policy Director 許可決定プロセスに組み込むことができます。

外部許可サービスの設定には、次の 2 つの一般的なステップを実行する必要があります。

1. 許可決定時に参照されるサーバー・プログラムを書き込みます。
2. 外部許可サービスを Policy Director に登録します。

このサービスを登録したら、このサービスを表す新しい許可が Policy Director 管理コンソールに表示されます。これで、この許可を任意の ACL 項目で使用できるようになります。

許可検査の間にこの許可が検出されると、外部許可サービスが、追加の許可決定があるかどうかについて参照されます。

外部許可サービスのセットアップについての詳細は *Policy Director Programmer's Guide and Reference* に記載されています。

リソース要求に関する条件

外部許可サービスを使用して、アクセス試行の正常完了と失敗について特定の条件を設けることもできます。

例には、次のような条件が含まれています。

- 外部監査メカニズムが、正常に完了した、または失敗したアクセス試行を記録するようにすること。
- アクセス試行をアクティブにモニターし、受諾不能な動作が検出された場合にアラートまたはアラームが出されるようにすること。
- 請求およびマイクロ支払いトランザクション。

許可評価プロセス

外部許可サービスを組み込む許可決定は、次の方法で行われます。

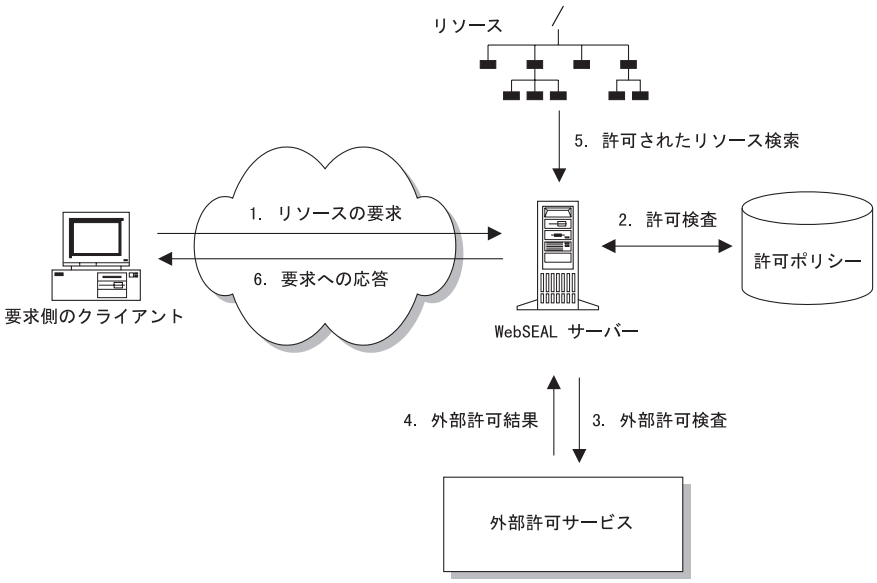
1. ACL 検査を行って、許可セットが要求側ユーザーに認められたかどうか判別します。
2. 認証済み RPC を使用する許可要求を、許可が ACL に表示されている各外部許可サービスに送信します。

   この外部許可検査は、そのユーザーに必要な許可が認められているかどうかに関係なく行われます。
3. 許可決定の結果をすべて合計します。

   拒否は、Policy Director ACL 検査またはいずれかの外部許可検査から行われます。拒否された場合、Policy Director 許可サービスは許可要求を拒否します。

例 :

次の図は、WebSEAL サーバーと外部許可サービスが関係する許可の決定を示しています。



この例で、外部許可サービスの目的は、オブジェクトへのアクセスに時間的な制限を加えることです。管理コンソールの許可を表すために割り当てられた文字は k です。

1. Policy Director WebSEAL サーバーは、機密の技術文書へのアクセスに関してクライアントから要求を受け取っています。そのクライアントは、技術グループのメンバーです。
2. WebSEAL サーバーは、最初に許可ポリシー・データベースを検査して、その文書オブジェクトに割り当てられた許可を判別します。

   ```
   group engineering rk
   ```

   ACL 項目に外部許可サービスの許可が含まれていない場合、最終的な許可決定は、この情報だけに基づいて行われます。

   上記の例で、ACL 項目には標準の読み取り許可が含まれています。この項目には、許可評価を補足するために外部許可サーバーを参照する追加の (k) 許可も含まれています。
3. Policy Director は、外部許可サーバーへの認証済み RPC を使って、要求を送信します。認められた許可セットは、2 のステップでわかります。Policy Director はこの要求とともにこの許可セットを送信して、外部許可サーバーがこの情報に基づいてその決定を行えるようにします。

   この例で、外部許可サーバーの設計では、この文書にアクセスする能力に時間的な境界を設定することができます。この文書へのアクセスは、要求が月曜日から金曜日の午前 8 時から午後 6 時の間に行われた場合にだけ可能です。
4. この例のクライアントは、火曜日の午前 10 時に要求をしています。サーバーは、WebSEAL サーバーに正常実行応答を戻します。

   上記の許可決定をすべて考慮に入れて、文書オブジェクトへのアクセスを認めるための最終勧告が行われます。
5. WebSEAL サーバーは、文書リソースを検索します。
6. WebSEAL サーバーによって、クライアントが文書を表示できます。

外部許可サービスを実行するための詳細については、*Policy Director Programmer's Guide and Reference* を参照してください。

インプリメンテーション戦略

Policy Director を使用すると、外部許可サービスを次のようにいくつかの方法で実行できます。

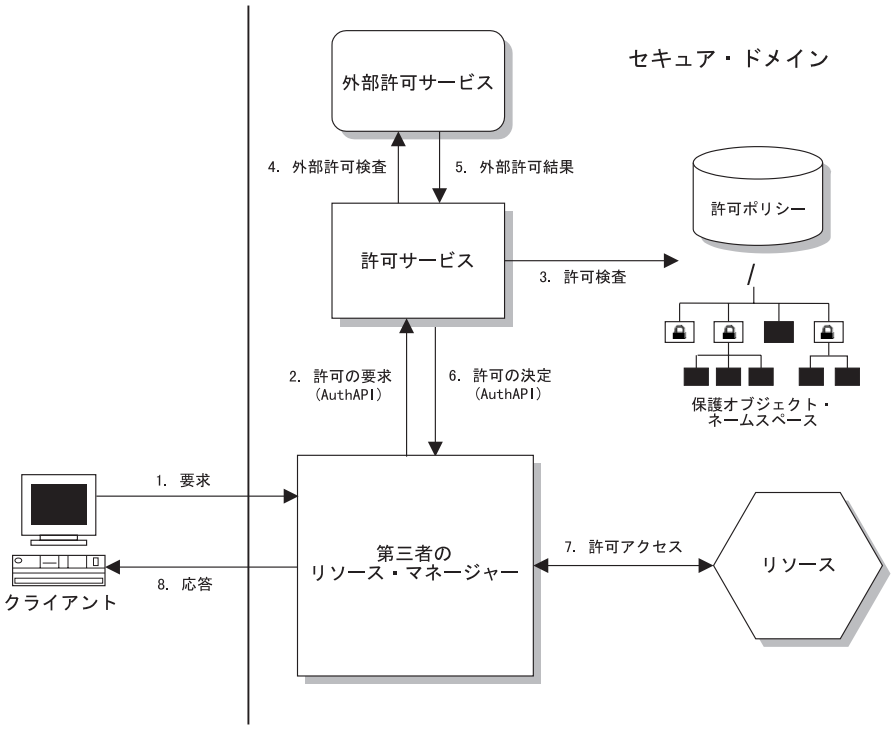
- さまざまな許可評価を履行するために、セキュア・ドメインに外部許可サービスをいくつでも追加できます。 ACL の中の個々の許可はそれぞれ 1 つのサービスを表します。
- 複数の外部許可サーバーを連鎖させることで、1 つの許可用に複数の外部サーバーを呼び出すことができます。個々の外部許可サーバーは、連鎖内の次のサーバーに認証された識別を渡し、ダウンストリームのサーバーから結果を収集します。
- セキュア・ドメイン全体に外部許可サービスを複写できます。

これらのインプリメンテーションは 1 つ 1 つが独立していて、どのように組み合わせても使用できます。

拡張性と柔軟性

Policy Director 許可 API と外部許可サービスを組み合わせると、セキュリティー・ポリシーを実行するための高い拡張性と柔軟性を備えたソリューションが実現されます。

次の図は、第三者アプリケーション用の Policy Director 許可 API と外部許可サービスのそれぞれの機能を併用して可能になる、拡張可能アーキテクチャーを示しています。



第4章 管理コンソールの紹介

Policy Director 管理コンソールは、すべての Policy Director 構成要素を安全に管理するために、分散ネットワークで使用する Java ベースのグラフィカル・アプリケーションです。管理コンソールからは、セキュリティー・サーバー・レジストリー、1 次許可ポリシー・データベース、および全 Policy Director サーバーが管理できます。管理コンソールでは、ユーザーまたはグループの追加や削除、そして ACL の適用もできます。

この章は、次の各節に分かれています。

管理コンソールの概要

Policy Director 管理コンソールは、Java を基にしたグラフィック・アプリケーションであり、 Policy Director セキュア・ドメインのセキュリティー・ポリシーを管理するために使用されます。オプションの **ivadmin** コマンド行ユーティリティーは、管理コンソールと同じ管理機能を提供します。

管理コンソールから、または **ivadmin** ユーティリティーを使用して、以下の作業を実行することができます。

- レジストリー・データベース (アカウント) を変更する。
- 1 次許可ポリシー (ACL) データベースを変更する。
- ユーザーを追加および削除する。
- グループを追加および削除する。
- ポリシー・テンプレートまたは ACL をオブジェクトに適用する。
- グローバル・サインオン (GSO) リソース、リソース・グループ、およびリソースのクリデンシャルを追加、削除、または変更する。
- プロキシー・ユーザーを追加、削除、または変更する (オプション)。

管理コンソール機能

管理コンソールは、タスクを実行するためのツールを提供し、管理コンソール・ウィンドウの中の該当領域に情報を表示します。基本のツールと表示領域は次のとおりです。

- タスク・タブ

- 管理タスク・パネル (上部と下部のパネル)
- アクション・ボタン
- ツールバー
- 掲示板 (デフォルトの下部パネル)
- 状況バー
- タイトル・バー

管理タスク・パネルのツール

管理タスク・パネルには次のツールが提供されます。

- タスク・タブ
- 管理タスク・パネル (上部と下部のパネル)
- アクション・ボタン

タスク・タブ

管理コンソールには、管理操作を実行するために次のメインタスク・タブ があります。

- ログイン
- ユーザー
- グループ
- GSO リソース
- GSO リソース・グループ
- ACL
- オブジェクト・スペース
- プロキシー・ユーザー (オプション)

管理タスク・パネル

個々のタスク・タブは管理タスク・パネルを表示し、そこには、管理コンソールの上部パネルに表示される情報ビューの集合が含まれています。

管理タスクは次のとおりです。

ログイン	ログインは、管理コンソールへのログインとログアウトの入り口点です。
ユーザー	セキュア・ドメインへのユーザーの参加者を作成し、保守できます。
グループ	セキュア・ドメイン内のグループを作成し、保守できます。
GSO リソース	GSO リソース情報を作成し、保守できます。
GSO リソース・グループ	GSO リソース・グループ情報を作成し、保守できます。
ACL	ポリシー・テンプレートまたは ACL を作成し、保守できます。
オブジェクト・スペース	ネームスペースのオブジェクトにポリシー・テンプレートを付加したり、オブジェクトからポリシー・テンプレートを除去したりできます。
プロキシー・ユーザー	プロキシー・ユーザー情報を作成し、保守できます。

アクション・ボタン

それぞれのアクション・ボタン・セットはタスク・タブを 1 つずつ伴っています。これらのアクション・ボタンは、管理操作を実行するために使用します。これらのボタンは、パネルの左側に表示されます。アクション・ボタンによって該当のデータベースが変更され、更新されます。

パネル・ビュー・タイプ

情報を管理タスク・パネルに表示する場合、次の 3 つのビューの 1 つに表示できます。各ビュー・タイプにはそれぞれの特性があります。

詳細ビュー

詳細ビューにはデータ入力用の動的フィールドが含まれます。

リスト・ビュー

リスト・ビューは、該当の列のタイトル・バーをクリックして、昇順にも降順にも分類できます。一部のリストには照会機能があります。

ツリー・ビュー

ツリー・ビューは拡大したり縮小したりできます。

いずれかのビューで項目を選択し、アクティブにすると、青く強調表示されます。

項目は選択されていても、現在アクティブでない場合はグレーになっています。

ツールバー

ツールバーは、管理コンソール・ウィンドウの最上部に表示され、そこには特定の管理コンソール機能を活動化するボタンがあります。

タスクの下方移動ボタンは、上部パネルにある現行管理タスクを下部パネルに位置変更します。

タスクの上方移動ボタンは、下部パネルにある現行管理タスクを上部パネルに位置変更します。

ピン・ビュー・ボタンは、上部パネルの現行アクティブ情報を取り出し、この情報のコピーを下部パネルに入れます。 上部パネルの現行アクティブ情報には、グループまたはユーザーのリストなどといった情報が含まれます。 このパネルには新しいタブも表示されます。 このパネルの情報は、静的コピーだけで動的ではありませんが、 その場合でも、オブジェクト・スペース・ツリーやグループ・リストなどのツリー・ビューは拡大したり、縮小できます。

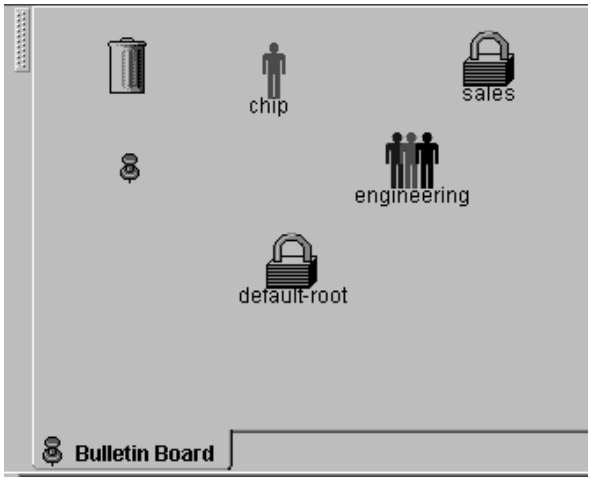
消去ボタンは、管理コンソールから現在選択されているビューを消去します。 このアクションではビューだけが消去されます。実際のデータベース情報はそのまま変更されません。

停止ボタンは、現在進行中のアクションを停止して、管理コンソールの制御を管理者に戻します。 このボタンは事実上現行アクションの結果を無視し、管理コンソールは操作が失敗した場合と同様に動作します。

掲示板

掲示板は、管理コンソールのデフォルトの下部パネルです。掲示板は、管理セッション中に複数回使用することが予想されるオブジェクトの一時記憶場所として使用します。ここで言うオブジェクトとは、ファイル、ACL、ユーザーとグループのリスト、および属性です。該当のオブジェクト・アイコンを掲示板にドラッグ・アンド・ドロップして、必要に応じてそれらを管理タスクで使用します。

掲示板の標準アイコンは、**ごみ箱**アイコンと**ピン・ビュー・**アイコンです。



ごみ箱アイコン

掲示板に保管されているアイコンは、**ごみ箱**アイコンにドラッグして除去できます。

ピン・ビュー・パネル

他の管理タスク・パネルから特定のオブジェクトと情報を選択 (強調表示) して、それらを掲示板の**ピン・ビュー**・アイコンにドロップできます。

このアクションによって、新しい下部パネルが作成され、そこに選択された情報のコピーが表示されます。新しいタブも表示されます。

このパネルの情報は、静的コピーだけで動的ではありませんが、その場合でも、オブジェクト・スペース・ツリーやグループ・リストなどのツリー・ビューは拡大したり、縮小できます。

アクティブ情報がグループのリストの場合、選択 (強調表示) されたグループだけがピン・ビュー・パネルに入れられます。

ピン・ビュー・パネルをクローズするには、ウィンドウの右上隅の「ボックス・クローズ」ボタンをクリックします。

注: 情報を選択してツールバーの**ピン・ビュー**・ボタンをクリックしても、同じアクションが行われます。

状況バー

管理コンソールの下部にある状況バーには、状況メッセージとエラー・メッセージが表示されます。

- 一般的な状況情報は**黒**で表示されます。
- 警告メッセージは**青**で表示されます。
- エラー・メッセージは**赤**で表示されます。

状況表示アイコンは、メッセージ域の左側に表示されます。


正常状況アイコン


警告状況アイコン


エラー状況アイコン

状況インディケーター・アイコンをダブルクリックすると、状況バーには以下が表示されます。

- 管理コンソールのバージョン
- 管理コンソールの活動によって影響を受けるセキュア・ドメイン
- Java のバージョン

タイトル・バー

管理コンソールのタイトル・バーには、次の 2 種類の重要情報が表示されます。

- 現在管理コンソールの活動によって影響を受けているセキュア・ドメイン。
- ユーザーのログイン状況 (UPDATE または READ-ONLY)。

1 次セキュリティー・サーバー・レジストリーが使用可能でない場合、管理コンソールからアカウント・データへの変更ができなくなります。まれにこのような状況が起こった場合、管理コンソールはそのレジストリーのレプリカから現行アカウント情報を入手します。このレジストリーに影響する情報を変更しようとすると、エラー・メッセージが表示されます。

ログイン管理タスク

ログイン・タスク・パネルは、認証されたユーザーの管理コンソールへの入り口点です。このイベントが正常に行われると、フルセットの管理タスク・タブが表示されます。

ユーザーがログアウトすると、すべてのコンテキストは失われ、タスク・タブは除去されます。

タスク・タブ

タスク・タブ: **ログイン**

管理タスク

ログイン管理タスク・パネルには、**ユーザー名** と**パスワード**の項目のフィールドが含まれています。**セキュア・ドメイン**・フィールドには、当初、NetSEAT 用に構成されたデフォルトのセキュア・ドメインが表示されます。

ログイン・メニューで、管理コンソール・タスクを実行する別のセキュア・ドメインを選択できます。

アクション・ボタン

ログイン のアクション・ボタンは、次のものです。

- ログイン
- ログアウト

ユーザー管理タスク

ユーザー管理タスク・パネルでは、セキュア・ドメインのユーザーの参加者を作成し、保守できます。リスト・ビューまたはツリー・ビューからユーザーを選択すると、詳細ビューのフィールドに現行データが記入されます。

タスク・タブ

タスク・タブ: **ユーザー**

管理タスク

ユーザー管理タスク・パネルには、ユーザー・リスト・ビュー、ユーザー詳細ビュー、およびグループ・リスト・ビューが含まれます。

グループ・ビューには、GSO リソースおよび GSO リソース・グループの追加のタブが含まれます。

アクション・ボタン

ユーザーのアクション・ボタンは、次のものです。

- 新規
- 入手
- 保管
- 削除

グループ管理タスク

グループ管理タスク・パネルでは、セキュア・ドメインのグループを作成し、保守できます。リスト・ビューまたはツリー・ビューからグループを選択すると、詳細ビューのフィールドに現行データが記入されます。

タスク・タブ

タスク・タブ: **グループ**

管理タスク

グループ管理タスク・パネルには、グループ・リスト・ビュー、グループ詳細ビュー、およびユーザー ID リスト・ビューが含まれます。

アクション・ボタン

グループのアクション・ボタンは次のものです。

- 新規
- 入手
- 保管
- 削除

GSO リソース管理タスク

GSO リソース管理タスク・パネルでは、セキュア・ドメイン内の GSO リソースを作成し、保守することができます。 GSO リソースは常に、Web リソースです。リストまたはツリー・ビューから GSO リソースを選択すると、詳細ビューのフィールドに現行データが記入されます。

タスク・タブ

タスク・タブ: **GSO リソース**

管理タスク

GSO リソース管理タスク・パネルには、リソース・リスト・ビューとリソース詳細ビューが含まれます。

アクション・ボタン

GSO リソース のアクション・ボタンは次のものです。

- 新規
- 入手
- 保管
- 削除

GSO リソース・グループ管理タスク

GSO リソース・グループ管理タスク・パネルでは、セキュア・ドメイン内の GSO リソース・グループを作成し、保守することができます。リソース・グループ は、Web サーバーのリソースを参照し、ここではグループ内のすべてのサーバーが、同じユーザー ID (userid) とパスワードのセットを持ちます。リストまたはツリー・ビューから GSO リソースを選択すると、詳細ビューのフィールドに現行データが記入されます。

リソース・グループのすべてのリソースに対して、単一のリソース・クリデンシャルを作成することができます。Policy Director は、リソース・グループ内のそれぞれのリソースごとのリソース・クリデンシャルを使用するのではなく、リソース・グループに対して、単一のリソース・クリデンシャルを使用します。

タスク・タブ

タスク・タブ: **GSO リソース・グループ**

管理タスク

GSO リソース・グループ管理タスク・パネルには、リソース・グループ・リスト・ビュー、リソース・グループ詳細ビュー、および GSO リソース・リスト・ビューが含まれます。

アクション・ボタン

GSO リソース・グループのアクション・ボタンは次のものです。

- 新規
- 入手
- 保管
- 削除

ACL 管理タスク

ACL 管理タスク・パネルでは、ACL ポリシー・テンプレートを作成し、保守できます。 **ACL リスト**・ビューから ACL を選択すると、ACL 定義ビューのフィールドに現行データが記入されます。

タスク・タブ

タスク・タブ: **ACL**

管理タスク

ACL 管理タスク・パネルには、ACL リスト・ビュー、 ACL 定義詳細ビュー、および許可ツリー・ビューを伴う ACL 項目詳細ビューが含まれます。

アクション・ボタン

ACL のアクション・ボタンは次のものです。

- 新規 ACL
- 新規項目
- 保管
- 削除
- 入手
- リスト
- 使用されている場所

オブジェクト・スペース管理タスク

オブジェクト・スペース管理タスク・パネルでは、ネームスペース内のオブジェクトに ACL を付加したり、オブジェクトから ACL を除去したりできます。

オブジェクト・スペース・ツリー・ビューのオブジェクトを選択すると、継承された ACL が順番に継承 ACL ツリー・ビューに表示されます。このリストは、継承が行われたために選択されたオブジェクトの許可に影響を与えるすべてのオブジェクトを、明示的に設定された ACL と一緒に表示します。

タスク・タブ

タスク・タブ: **オブジェクト・スペース**

管理タスク

オブジェクト・スペース管理タスク・パネルには、そのパネルのサブタブから選択された 3 つの異なる情報ビューが表示されます。

- **継承 ACL** ビュー (デフォルト)

  このビューはデフォルトのビューです。 ここには、選択されたオブジェクトに影響を与える ACL の連鎖が表示されます。オブジェクト・スペース・ツリー・ビューで選択されたオブジェクトに即時に影響を与える ACL が、常に 1 つの矢印で指し示されています。
- **ACL の編集**ビュー

  このビューは、ACL 属性を直接変更できるようにする ACL 管理パネルの部分を表示します。
- **継承**ツリー・ビュー

  このビューは、選択されたオブジェクトに直接影響を与えている ACL 継承連鎖のツリー・ビューを表示します。

アクション・ボタン

オブジェクト・スペースのアクション・ボタンは次のものです。

- ACL の付加
- ACL の除去
- ACL の検出
- ACL の保管
- リスト

プロキシー・ユーザー管理タスク

Policy Director を法人組織用のファイアウォール・システムと併用すると、エンタープライズ・イントラネットを無許可アクセスと侵入から完全に保護することができます。プロキシー・ユーザー管理タスク・パネルでは、セキュア・ドメイン内のプロキシー・ユーザーを作成し、保守することができます。ツリー・ビューからプロキシー・ユーザーを選択すると、詳細ビューのフィールドに現行データが記入されます。

タスク・タブ

タスク・タブ: **プロキシー・ユーザー**

管理タスク

プロキシー・ユーザー管理タスク・パネルには、プロキシー・ユーザー・リスト・ビューおよび、プロキシー・ユーザー詳細ビューが含まれます。

プロキシー・ユーザー詳細管理タスク・パネルには、デフォルトのプロキシー・ユーザー情報を表示するフィールドがあります。

アクション・ボタン

プロキシー・ユーザーのアクション・ボタンは次のものです。

- 保管
- 削除

管理コンソールのプロパティーおよび制御

管理コンソールでは、Microsoft Window NT または Windows 95 ないし 98 上の Policy Director NetSEAT クライアントが、セキュア通信チャネルを通じて管理タスクを実行する必要があります。 AIX および Solaris の場合、管理コンソールは、管理タスクの実行のためにシステムの DCE クライアントを使用します。

ドラッグ・アンド・ドロップ

管理コンソール操作の多くは、マウスを使ってオブジェクトを 1 つの場所からドラッグし、別の場所にそれをドロップすることによって実行できます。たとえば、グループにユーザーを追加するには、ユーザー・リストから**ユーザー**・アイコンをドラッグし、それをグループ・ツリー・ビューのグループにドロップするだけでできます。

カーソルの形は、ドラッグが認められているアイコンの上にあるときは手の形に変わります。

ドラッグ・アンド・ドロップできるのは次のオブジェクトです。

- ユーザー
- グループ
- ACL
- ACL 項目
- ネームスペースのオブジェクト
- GSO リソースおよび GSO リソース・グループ
- プロキシー・ユーザー

注: データベース更新を伴うドロップはすべて、確認アラート・ダイアログ・ボックスを表示します。

データ照会はドラッグ・アンド・ドロップ方式で実行できます。たとえば、**ACL** アイコンを掲示板から ACL 定義ビューにドラッグすると、該当のフィールドに現行データが記入されます。

この操作を受け入れない場所にオブジェクト (アイコン) をドロップすると、そのオブジェクト (アイコン) はその元の絵に戻ります。

注: ドラッグ・アンド・ドロップ操作は、管理コンソールを使用した場合のみ有効です。

上部パネルと下部パネルの活動の実行

管理コンソールの更新操作は、上部パネルと下部パネルの両方で行われます。この操作では、オブジェクトを下部パネルからドラッグして、上部パネルにドロップします。どちらのパネルの変更も、データベースに保管してください。

Policy Director は、オブジェクト・スペース・パネルと ACL パネルに表示される ACL 情報を常に同期化します。

リストの複数項目の選択

リストおよびテーブルの項目の選択は、次の標準 Windows 選択技法を使って行うことができます。

- ある項目を 1 回クリックするとその項目が選択されます。
- Ctrl キーを押したままにすると、他の項目が同時に選択されます。
- Shift + クリックの後にもう 1 回クリックすると、2 回のクリックの間のテキスト・ブロックが選択されます。
- リスト内の全項目は、**Ctrl + a** を使って選択できます。

データ入力フィールドの編集

データ入力フィールドを編集するときは、次のことを覚えておいてください。

- テキスト編集フィールドをオン、オフに切り替えるには、Enter キーを使用します。
- 編集時にフィールドへの直前のデータ入力を復元するときは、Esc キーを使用します。
- Windows のクライアント・マシンでは、標準の Windows のキーストロークを使って、管理コンソールに特定のコピーとカット・アンド・ペーストが実行できます。
- データが変更されたフィールドを終了した後は、ビューの左上隅に赤いインディケーターが表示されます。**保存**ボタンをクリックして、データベースへの変更をすべてコミットします。
- ドラッグ・アンド・ドロップを使うと、一部のデータ・フィールドへの記入もできます。

リストからの照会

リスト・ビューの多くには照会機能があります。照会アイコンは、リスト・ビュー・ウィンドウの左上隅に表示されます。

ナビゲート

フィールド間をナビゲートするには、次のようにします。

- 詳細ビューでは、タブ・キーが 1 つのデータ入力フィールドから次のデータ入力フィールドにカーソルを移動します。
- カーソルが詳細ビューの最後のフィールドに来ると、タブ・キーはそのカーソルを次のビューに移動します。カーソルは左から右に動きます。

- カーソルがリスト・ビューまたはツリー・ビューにあるとき、タブ・キーは、カーソルを次のビューに移動します。カーソルは左から右に動きます。
- Shift + タブ・キーは、カーソルを右から左に次のビューへと移動します。
- Home キーはカーソルをビューの最上部に移動します。End キーは、カーソルをビューの最下部に移動します。

詳細ビューでは、Home + End キーは、すべてのフィールドが非アクティブの場合、ビューの最上部と最下部に移動します。アクティブなフィールドがある場合、Home + End キーは、カーソルをアクティブ・フィールドの先頭と末尾に移動します。

オブジェクト・アイコンの使用

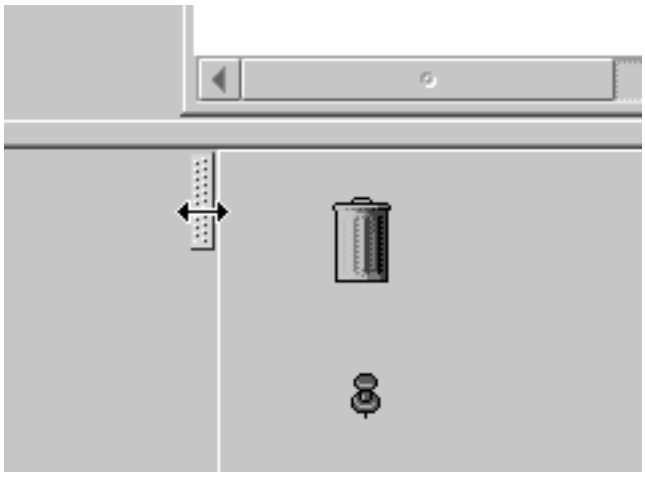
オブジェクト・アイコンを使用するときは、次のことを覚えておいてください。

- 固有のアイコンは、ネームスペース内の各オブジェクト・タイプをグラフィカルに表します。
- 個々のタスク・タブは、その管理タスクに影響されるオブジェクトのアイコンを表示します。
- 詳細ビューは、そのビューの左上隅に編集されているオブジェクトのアイコンを表示します。
- ドラッグ・アンド・ドロップ操作では、選択されたオブジェクトのアイコンが表示されます。
- オブジェクトはそのアイコンを使ってドラッグする必要があります。
- カーソルの形は、ドラッグ可能なアイコンの上にあるときは手の形に変わります。

スプリッター・アイコンを使用したビューのサイズ変更

管理タスクにはすべて 1 つまたは複数のビューが含まれています。ビューの左側の境界の一番上にあるスプリッター・アイコンを使うと、それらのビューのサイズを変更できます。また、カーソルを 2 つの列見出しの間でスプリッター・アイコンに移動すると、リスト・ビューの列のサイズを変更できます。

カーソルをスプリッターを越えて移動させると、カーソルの形は二重矢印に変わり、そのビューがサイズ変更できることを示します。



リストの分類

列のタイトル・バーをクリックすると、リスト・ビューの情報を昇順にも、降順にも切り替えることができます。タイトル・バーの右側のアイコンは現行の分類順序を示します。

リストで選択された項目は、リストの分類後も選択されたままです。

ツリー・ビューの拡大と縮小

ツリー・ビューは、ファイルおよびディレクトリーの Windows® Explorer の表示に似ています。 ノードを拡大または縮小するには、アイコン (プラスまたはマイナスが書かれたボックス) を見つけなければなりません。このアイコンをダブルクリックすると、拡大ツリー・ビューと縮小ツリー・ビューの切り替えができます。キーボードに相当するのは、**Ctrl + e** です。

ノードの下にオブジェクトまたはノードがない場合、拡大 / 縮小インディケーターをクリックすると消えます。

ルート・ノードを拡大および縮小すると、ツリー全体が最新表示されます。

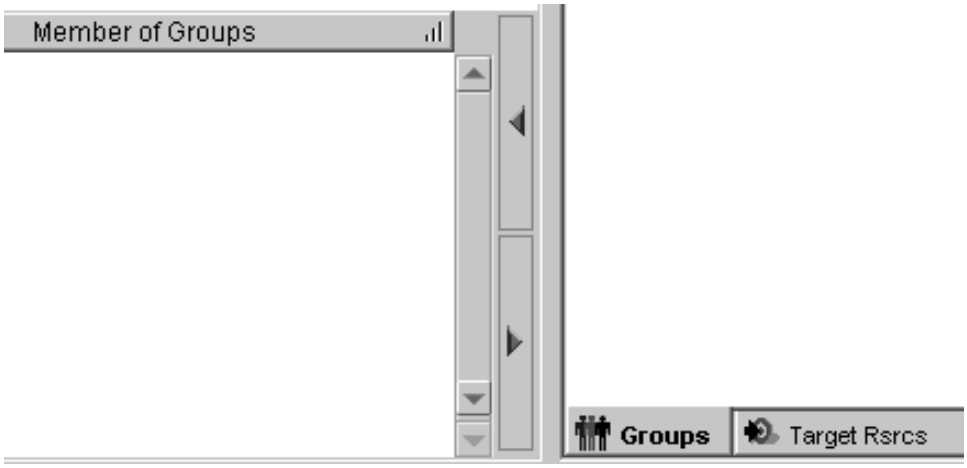
オブジェクト・スペースのノード・シフト矢印の使用

オブジェクト・スペース・ビューのタイトル・バーには 2 つの青い矢印があります。これらの 2 つの青い矢印によって、ツリー・ビューのフォーカスをツリーの分岐に制限することができます。

- **左矢印** -- この矢印は、選択されたノードまたはオブジェクトをすべて左そろえにシフトし、それらがルート位置に表示されるようにします。
- **右矢印** -- この矢印は、1 回クリックするたびにノードを 1 つずつ、ツリーを元どおりにシフトします。 左矢印を使用した後は、右矢印 (1 回または複数回のクリック) を使用して、ツリーをその通常の方向に復元します。

選択矢印の使用

選択矢印は、選択された情報を 1 つのウィンドウ・ビューから別のウィンドウ・ビューに移動します。これを行うことにより、その別のウィンドウのフィールドに新しい情報が記入されます。



第5章 ユーザー・アカウントとグループの管理

Policy Director セキュリティー・モデルでは、オブジェクトへのアクセスを許可する前に、ユーザーの認証を必要とします。ユーザー識別の認証は、ユーザー識別と暗号化されたパスワードを、 1 次レジストリー・データベース内のアカウント情報と突き合わせることで行えます。デフォルトでは、Policy Director は LDAP レジストリーを使用します。 セキュリティー管理者は管理コンソールを使用して、セキュア・ドメインに参加するユーザーとグループを作成し、管理することができます。

この章は、次の各節に分かれています。

ユーザー、グループ、およびアカウントについて

Policy Director セキュリティー・サービスは、 1 次アカウント・レジストリー (セキュア・ドメインのユーザー、グループ、およびアカウントについての情報を含むデータベース) に依存しています。デフォルトでは、Policy Director は LDAP レジストリーを使用します。

ユーザー

ユーザー とは、セキュア・ドメインのプリンシパルまたは参加者です。ユーザーには、人間のユーザー、サーバー・プロセス、マシン、または他のセキュア・ドメインを含むことができます。

ユーザーとは、別のユーザーとの認証の交換に参加できるエンティティーです。*認証* とは、ユーザーが自分が主張している本人であることを検査するプロセスです。どのユーザーも、認証に使用されるパスワードまたは機密キーを持っています。

ユーザーは、アクセス制御の許可と関連付けることができます。それぞれのユーザーは、それ自身の固有のユニバーサル固有識別子 (UUID) を持ち、これはユーザーの名前が変更された場合でも、常に変わらないままです。 Policy Director は、セキュリティーのクリデンシャルとして UUID をセキュリティー・サービスに渡します。

グループ

グループ とは、ユーザーの集まりであり、グループ名により識別されます。グループは、異なるレベルのセキュリティー上の役割または責任を表すことができます。 Policy Director は、同じグループのメンバーであるユーザーを、セキュリティー上の目的からは同一に扱います。ユーザーは役割や責任によって、複数のグループに属することができます。

グループは、セキュリティー・ポリシーの管理を容易にします。グループのセキュリティー・ポリシーを定義するには、ACL を使用します。ユーザーの役割、責任、または存在が変化した時には、このユーザーのすべての ACL 項目を変更する必要があ

ります。グループがなければ、このような個々のユーザーの項目を含むすべての ACL を変更することは、ほとんど不可能な作業になります。

グループ ACL 項目は、ユーザーの役割または責任を表すことができます。そのように表したとすれば、必要な管理作業は、グループにユーザーをメンバーとして追加または削除することだけです。

グループは、ユーザーと同様に、グループ名に加えて UUID を持ちます。このグループ UUID は、ユーザーのセキュリティー・クリデンシャルの構成要素を表します。

アカウント

アカウント とは、ユーザー、関連したグループ、および関連セキュリティー情報を含む関係です。レジストリー内のアカウントは、ユーザーのネットワーク識別を定義します。アカウントは、ユーザーを、1 つまたは複数のグループおよび、関連するすべてのセキュリティー情報 (たとえば、認証に使用されるパスワード) と関連付けることにより、ネットワーク識別を定義します。

セキュア・ドメインを経由して通信を行うすべてのユーザーについて、通信が認証されるかどうかに関係なく、アカウントを作成する必要があります。

ユーザー・アカウントは、ユーザーのパスワードおよび、ユーザーがセキュア・ドメインにログインする時に使用される任意の情報と関連付けることができます。アカウント情報には、ユーザーのホーム・ディレクトリー、ログイン・シェル、および認証ポリシー (パスワード) を含めることができます。この情報は、ユーザーのセキュア・ドメインへのアクセスの制御に役立ちます。

注: ユーザー・アカウントでグループを使用するには、その前にレジストリーにグループを追加する必要があります。

グループの管理

グループとは、1 つまたは複数のユーザーの集まりです。通常は、組織内の部門 (たとえば、販売部門、研修部門、技術部門など) を表すためにグループを作成します。あるいは、仕事に基づいたグループ・カテゴリー (たとえば、システム管理者や、定常的バックアップを行うユーザーのグループなど) を作成することもできます。

グループ・カテゴリーは、 Policy Director セキュア・ドメイン内のアクセス制御の管理を単純化できます。新しいユーザーに情報のアクセスを許すには、該当のグループ・カテゴリーのメンバーとしてユーザーを割り当てればよいのです。この方法を使用すれば、新しいユーザーごとに新しい ACL 項目を作成する必要がなくなります。

たとえば、技術部門に新しい人が入った場合、グループ・カテゴリー技術内にメンバーシップを持つ、新しいユーザー・アカウントを作成します。これで新しいユーザーは、 技術グループに許可されているすべての技術文書を読むことができるようになります。技術 ACL テンプレート内にこのユーザーの新しい ACL 項目を作成する必要はありません。

Policy Director セキュリティー・レジストリーにグループ項目を追加、変更、または削除するには、管理コンソールを使用します。

1 つまたは複数のグループ項目を作成した後で、ユーザーをグループに割り当てることができます。ユーザーは役割や責任が異なるのに応じて、複数のグループに属することができます。

グループ管理パネルの使用

セキュア・ドメインのセキュリティー管理者は、管理コンソールを使用して次のようにグループを作成します。

1. 管理者として (たとえば、cell_admin) 管理コンソールにログインする。
2. **グループ**・タスク・タブをクリックする。

   グループ管理タスク・パネルが表示されます。

グループ管理タスク用のアクション・ボタンの使用

グループ・アクション・ボタンは、グループ管理作業の実施に使用します。以下の表で、各アクション・ボタンの機能を説明します。

アクション・ボタン	説明
新規	セキュア・ドメインの新しいグループ項目を作成する。
入手	特定して指定されたグループについての情報を検索し、詳細ビュー・ウィンドウに表示する。
保管	このグループ項目を保管する。新しい項目は、該当のリスト・ウィンドウに表示される。
削除	選択されたグループをレジストリー・データベースから除去する。

グループ詳細フィールドの使用

次の表は、管理コンソールの**グループ詳細**ビュー内のフィールドを説明しています。

フィールド	説明
グループ名	セキュア・ドメインのグループに割り当てられた 1 次名。グループ名は、レジストリーに照会が行われた時に使用されるキー・フィールドです。
説明	グループを説明する情報テキスト列。説明はオプションのデータ・フィールドであり、レジストリーはこれを使用しません。
LDAP	LDAP の場合: • cn = には、一般的な名前 (credit など) を入力。 • dn = には、識別名 (cn=credit,o=IBM,ou=Austin,c=US など) を入力。

新しいグループの作成

新しいグループを作成するには、次のようにします。

1. **新規**アクション・ボタンをクリックする。

   グループ詳細域にある **グループ名**と**説明**の入力フィールドを活動化する。
2. 新しいグループ名を入力し、オプションとして、**説明**フィールドにグループの説明を入力する。

3. LDAP がデフォルトのレジストリーである場合は、必要な LDAP レジストリー情報を追加する。
4. 新しいグループにユーザーを追加するには、ユーザー・アイコンを、ユーザー ID リスト・ビューからグループ詳細ビューのユーザー ID ウィンドウにドラッグする。

   また、選択矢印を使用して、ユーザーをユーザー ID パネルの中または外に移動させることができます。
5. **保管**アクション・ボタンをクリックする。

   新しいグループ項目がグループ・リスト・ビューに表示されます。

グループ詳細の変更

既存のグループのユーザー・メンバーシップまたは名前を変更するには、次のようにします。

1. グループ・リスト・ビューからグループを選択する。

   グループについての現行情報を示して、グループ詳細ビューが表示されます。
2. グループ詳細域で、変更するフィールド(73ページの『グループ詳細フィールドの使用』参照) を選択し、新しい値を入力する。
3. 新しいユーザーをグループに追加したり、グループからユーザーを削除することもできます。

   ユーザー ID 欄から、ユーザーのアイコンをダブルクリックする。それから、新しいユーザーをグループ詳細ビュー内のユーザー ID ウィンドウにドラッグ・アンド・ドロップする。また、選択矢印を使用することもできます。
4. **保管** をクリックします。

グループの削除

グループを削除するには、次のようにします。

1. グループ・リスト・ビューから、削除したいグループの名前を選択する。

   グループ詳細ビューにグループ・メンバーのリストが表示されます。
2. 各グループ・メンバーを、一度に 1 人ずつ選択し、各ユーザーをグループから削除する。
3. グループ・リスト・ビューから、グループを選択する。
4. グループ項目を完全に削除するには、**削除**をクリックする。

ユーザー・アカウントの管理

セキュア・ドメイン内のサービスとオブジェクトにアクセスを要求するユーザーは、ユーザー自身を Policy Director に認証する必要があります。 Policy Director のセキュア・ドメインに参加を望むユーザーはすべて、 LDAP にアカウントを登録しなければなりません。

ユーザー管理パネルの使用

セキュア・ドメインのセキュリティー管理者は、管理コンソールを使用して次のようにユーザー・アカウントを作成します。

1. 管理者として (たとえば、`cell_admin`) 管理コンソールにログインする。

2. **ユーザー**・タスク・タブをクリックする。

   ユーザー管理タスク・パネルが表示されます。

ユーザー管理タスク用のアクション・ボタンの使用

ユーザー・アクション・ボタンは、ユーザー管理作業の実施に使用します。以下の表で、各アクション・ボタンの機能を説明します。

アクション・ボタン	説明
新規	セキュア・ドメイン用の新しいユーザー・アカウントを作成する。
入手	特定して指定されたユーザーについての情報を検索し、詳細ビュー・ウィンドウに表示する。
保管	このユーザー・アカウントを保管する。新しい項目は、該当のリスト・ウィンドウに表示される。
削除	選択されたユーザーをレジストリー・データベースから除去する。

ユーザー詳細フィールドの使用

次の表は、管理コンソールの**ユーザー詳細**ビュー内のフィールドを説明しています。

フィールド	説明
ユーザー ID	セキュア・ドメインのユーザーに割り当てられた 1 次名。ユーザー ID は、レジストリーに照会が行われた時に使用されるキー・フィールドです。
説明	ユーザーを説明する情報テキスト列。説明はオプションのデータ・フィールドであり、レジストリーはこれを使用しません。
有効アカウント	このチェック・ボックスは、セキュア・ドメインに参加するように (または参加しないように) ユーザーの能力を制御します。ボックスが消去されると、アカウントは有効でなくなります。ただし、アカウント情報はまだレジストリーに残っています。
有効パスワード	このチェック・ボックスは、ユーザーが次にセキュア・ドメインにログインした時に、パスワード変更を強制できるようにします。ボックスが消去されると、ユーザーはパスワードが期限切れになったことを知らされます。
GSO ユーザー	このチェック・ボックスは、ユーザーが GSO 能力を持つことを示します。
LDAP	LDAP の場合: • cn = には、一般的な名前 (Diana Lucas など) を入力。 • sn= には、surname (Lucas など) を入力。 • dn= には、識別名 (cn=Diana Lucas,o=IBM,ou=Austin,c=US など) を入力。

新しいユーザー・アカウントの追加

新しいユーザー・アカウントを追加するには、次のようにします。

1. **新規**アクション・ボタンをクリックする。

   ユーザー詳細ビューにブランクの入力フィールドが表示されます。

2. フィールドに該当データを入力する。これらのフィールドの詳細な説明については、75ページの『ユーザー詳細フィールドの使用』を参照してください。

   グループ・アイコンを、グループ・ツリー・ビューからドラッグ・アンド・ドロップして「グループのメンバー」ウィンドウに入れるか、または選択矢印を使用することができます。
3. LDAP がデフォルトのレジストリーである場合は、必要な LDAP レジストリー情報を追加する。
4. **保管**をクリックする。

アカウント特性の変更

既存のアカウントの特性を変更するには、次のようにします。

1. ユーザー ID リスト・ビューからユーザーを選択する。

   ユーザー詳細域に現行データが表示されます。
2. ユーザー詳細ビュー内で、変更したいフィールドをクリックする。
3. 新しいデータを入力します。
4. **保管** をクリックします。

ユーザー・アカウントの削除

ユーザー・アカウントを削除するには、次のようにします。

1. ユーザー ID リスト・ビューからユーザーを選択する。
2. **削除**をクリックする。

複数の管理アカウントの作成

管理ユーザーは、次のグループになければなりません。次のグループにいれば、管理ユーザーは、セキュア・ドメイン内のユーザー、グループ、および組織を、追加、変更、または削除する権限を持ちます。

- acct-admin
- subsys/dce/sec-admin
- subsys/dce/cds-admin

セキュア・ドメインを最初に作成する時に、このグループの組み合わせを含む唯一のアカウントは、cell_admin です。

セキュア・ドメインがある程度の規模になると、増大するタスクを 1 人の管理者が管理するのは非常にむづかしくなります。大規模なセキュア・ドメインを管理するには、管理責任の委譲が必要になります。

同じ能力で管理コンソールを操作できる追加の管理アカウントを作成するには、対象者を上記の 3 つのグループのメンバーとして割り当てます。このような権限の委譲についての計画と組織化は、これらのアカウントの作成と一致させる必要があります。

他のソースからの情報のインポート

ユーザー・データとグループ・データを、他のソースからレジストリーに入れることができます。

第6章 GSO リソース、リソース・グループ、およびリソース・クリデンシャルの管理

Policy Director では、IBM グローバル・サインオン (GSO) 技術と統合することによって、より柔軟な単一サインオン・ソリューションをサポートします。 この統合は、Policy Director スマート接合を作成することで達成されます。 スマート接合の詳細については、195ページの『第15章 WebSEAL: スマート接合管理』を参照してください。

WebSEAL が接合先サーバー上にあるリソースに関する要求を受信すると、WebSEAL は GSO を使用して、該当する認証情報を検索します。 GSO には、特定のリソースとアプリケーションに関してユーザー名とパスワードが用意されている、各登録ユーザーに関するマッピングのデータベースが収容されています。 Policy Director は、IBM SecureWay Directory (LDAP) に直接 GSO データを保管します。

WebSEAL と GSO の組み合わせによって、完全な単一サインオン・ソリューションが得られ、さらに利点としてデータの暗号化、高可用性、拡張容易性が付加されます。

詳しくは、217ページの『GSO と WebSEAL 単一サインオンを統合する』を参照してください。

GSO リソースおよび GSO リソース・グループについて

GSO には、GSO リソースを特定のユーザー識別 (ユーザー名) とパスワードの組み合わせに対応付ける、ユーザー用の特定のリソース・クリデンシャル が含まれています。 リソース・クリデンシャルは、この、GSO ユーザー特有のリソース (たとえば、Web サーバーや Webサーバーのグループ) 用のユーザー名とパスワードを提供します。

GSO は、WebSEAL に認証情報を提供します。ユーザーがアプリケーション・リソースを実行したい場合、 WebSEAL は GSO に、ユーザーの認証情報について問い合わせます。 GSO は、認証情報のデータベース全体を、特定の認証情報にマップされたリソースの形式で保持しています。ユーザー名とパスワードの組み合わせへのアプリケーション・リソースのマッピングは、 *GSO リソース・クリデンシャル* と呼ばれています。 GSO リソース・クリデンシャルを作成できるのは、登録ユーザーの場合だけです。

注: GSO リソースまたは GSO リソース・グループに GSO リソース・クリデンシャルを適用する場合は、その前に GSO リソースまたは GSO リソース・グループが存在していなければなりません。

GSO リソースの管理

GSO リソース は Web サーバーです。これを識別するには、Web リソースの名前を指定します。

GSO リソース管理パネルの使用

セキュア・ドメイン内のサービスとオブジェクトにアクセスを要求する GSO リソースは、自分自身を Policy Director に認証する必要があります。 Policy Director のセキュア・ドメインに参加を望む GSO リソースはすべて、 LDAP にアカウントを登録しなければなりません。

GSO リソース管理タスク用のアクション・ボタンの使用

GSO リソース管理操作を行うには、 **GSO リソース**・アクション・ボタンを使用します。以下の表で、各アクション・ボタンの機能を説明します。

アクション・ボタン	説明
新規	セキュア・ドメイン用の新しい GSO リソース・アカウントを作成する。
入手	特定して指定された GSO リソースについての情報を検索し、詳細ビュー・ウィンドウに表示する。
保管	この GSO リソース・アカウントを保管する。新しい項目は、該当のリスト・ウィンドウに表示される。
削除	選択された GSO リソースを、レジストリー・データベースから削除する。

GSO リソース詳細フィールドの使用

次の表は、管理コンソールの**リソース詳細**ビュー内のフィールドを説明しています。

フィールド	説明
リソース名	セキュア・ドメインの GSO リソースに割り当てられた名前。リソース名は、レジストリーに照会が行われた時に使用されるキー・フィールドです。
説明	リソースを説明する情報テキスト列。説明はオプションのデータ・フィールドであり、レジストリーはこれを使用しません。

新しい GSO リソースの追加

新しい GSO リソースを追加するには、次のようにします。

1. **新規**アクション・ボタンをクリックする。

   リソース詳細ビューにブランクの入力フィールドが表示されます。

2. フィールドに該当データを入力する。これらのフィールドの詳細な説明については、『GSO リソース詳細フィールドの使用』を参照してください。

   リソース・グループ・アイコンを、リソース・グループ・ツリー・ビューからドラッグ・アンド・ドロップして「GSO リソース・グループのメンバー」ウィンドウに入れるか、または選択矢印を使用することができます。

3. **保管**アクション・ボタンをクリックする。

GSO リソース用のリソース・クリデンシャルの作成

リソース定義を作成した後は、ユーザーのリソース・クリデンシャルが作成できるようになります。

リソース・クリデンシャルを作成するには、次のようにします。

1. **ユーザー (Users)** タブを選択します。
2. 該当のユーザーの名前を強調表示して、リソース・クリデンシャルを作成するユーザーを選択します。
3. 「ユーザー詳細 GSO リソース (User Detail GSO Resources)」ビューで、**リソース (Resources)** タブを選択して、現在使用可能なリソースをリストします。
4. クリデンシャルを適用するリソースを選択します。
5. 選択したリソースを、「ユーザーの詳細 (User Detail)」ビューのリソース・ペインにドラッグします。

   新しいリソース・クリデンシャルのサインオン ID とパスワード値のデフォルトは、ユーザーのアカウントと同じ値になります。
6. サインオン ID とパスワードは、**サインオン ID (Sign-on ID)** か**パスワード (Password)** ボタンをクリックし、適切な値を記入することによって、このユーザーのリソース・クリデンシャルに適した値に変更することができます。
7. **保管**アクション・ボタンをクリックする。

GSO リソース情報の変更

既存のアカウントの特性を変更するには、次のようにします。

1. リソース・リスト・ビューから GSO リソースを選択する。

   リソース詳細域に現行データが表示されます。
2. リソース詳細ビュー内で、変更したいフィールドをクリックする。
3. 既存のデータを変更するか、または新しいデータを入力する。
4. **保管**アクション・ボタンをクリックする。

GSO リソースの削除

ユーザー・アカウントを削除するには、次のようにします。

1. リソース・リスト・ビューから GSO リソースを選択する。
2. **削除**をクリックする。

GSO リソース・グループの管理

リソース・グループ は、Web サーバーのグループを指します。この場合、このグループのサーバーは、すべて、同じユーザー ID (userid) とパスワードが設定されます。

GSO リソース・グループ管理パネルの使用

セキュア・ドメインのセキュリティー管理者は、管理コンソールを使用して次のように GSO リソース・グループを作成します。

1. 管理者として (たとえば、`cell_admin`) 管理コンソールにログインする。
2. **GSO リソース・グループ**・タスク・タブをクリックする。

   GSO リソース・グループ管理タスク・パネルが表示されます。

GSO リソース・グループ管理タスク用のアクション・ボタンの使用

リソース・グループ管理操作を行うには、「GSO リソース・グループ」アクション・ボタンを使用します。以下の表で、各アクション・ボタンの機能を説明します。

アクション・ボタン	説明
新規	セキュア・ドメイン用の新しい GSO リソース・グループ項目を作成する。
入手	特定して指定された GSO リソース・グループについての情報を検索し、詳細ビュー・ウィンドウに表示する。
保管	この GSO リソース・グループ項目を保管する。新しい項目は、該当のリスト・ウィンドウに表示される。
削除	選択された GSO リソース・グループを、レジストリー・データベースから削除する。

GSO リソース・グループ詳細フィールドの使用

次の表は、管理コンソールの**リソース・グループ詳細**ビュー内のフィールドを説明しています。

フィールド	説明
リソース・グループ名	セキュア・ドメインの GSO リソース・グループに割り当てられた 1 次名。 GSO リソース・グループ名は、レジストリーに照会が行われた時に使用されるキー・フィールドです。
説明	GSO リソース・グループを説明する情報テキスト列。この記述は、単なる任意選択のデータ・フィールドであって、レジストリーでは使用されません。

新しい GSO リソース・グループの追加

新しい GSO リソース・グループを作成するには、次のようにします。

1. **新規**アクション・ボタンをクリックする。

   リソース・グループ詳細域にある **リソース・グループ名**と**説明**の入力フィールドを活動化する。
2. 新しいリソース・グループ名を入力し、オプションとして、**説明**フィールドにリソース・グループの説明を入力する。
3. GSO リソースを新しい GSO リソース・グループに追加するには、 GSO リソース・アイコンを、GSO リソース・リスト・ビューから、リソース・グループ詳細ビューの 「GSO リソース」ウィンドウにドラッグしてもできます。

   また、選択矢印を使用して、リソースを GSO リソース・パネルの中または外に移動させることができます。
4. **保管**アクション・ボタンをクリックする。

   新しい GSO グループ項目がリソース・グループ・リスト・ビューに表示されます。

GSO リソース・クリデンシャルの作成

リソース・グループのすべてのリソースに対して、単一のリソース・クリデンシャルを作成することができます。 Policy Director は、リソース・グループ内のそれぞれのリソースごとのリソース・クリデンシャルを使用するのではなく、リソース・グ

ループに対して、単一のリソース・クリデンシャルを使用します。 GSO リソース・クリデンシャルは、最初にリソース・グループを作成してからでないと作成できません。

リソース・グループ定義を作成した後に、ユーザーの GSO リソース・クリデンシャルを作成するには次のようにします。

1. **ユーザー (Users)** タブを選択して、リソース・クリデンシャルを作成するユーザーを選択します。
2. 「ユーザー詳細 GSO リソース・グループ (User Detail GSO Resource Groups)」ビューで、**リソース・グループ (Resource Groups)** タブを選択して、現在使用可能なリソース・グループをリストします。
3. クリデンシャルを適用するリソース・グループを選択します。
4. 選択したリソース・グループを、「ユーザーの詳細 (User Detail)」ビューのリソース・グループ・ペインにドラッグします。

   新しいリソース・クリデンシャルのサインオン ID とパスワード値のデフォルトは、ユーザーのアカウントと同じ値になります。
5. サインオン ID とパスワードは、**サインオン ID (Sign-on ID)** か**パスワード (Password)** ボタンをクリックし、適切な値を記入することによって、このユーザーのリソース・クリデンシャルに適した値に変更することができます。
6. **保管**アクション・ボタンをクリックする。

GSO リソース・グループ情報の変更

既存のリソース・グループのリソース・メンバーシップまたは名前を変更するには、次のようにします。

1. リソース・グループ・リスト・ビューからリソース・グループを選択する。

   リソース・グループについての現行情報を示して、リソース・グループ詳細ビューが表示されます。
2. リソース・グループ詳細域で、変更するフィールド (**リソース・グループ名**または**説明**) を選択する。新しい値を入力します。
3. 新しいリソースをリソース・グループに追加したり、グループからリソースを削除することもできます。

   リソース・グループ 欄から、リソース・グループのアイコンをダブルクリックする。それから、新しいリソースをリソース・グループ詳細ビュー内の「GSO リソース」ウィンドウにドラッグ・アンド・ドロップする。 また、選択矢印を使用することもできます。
4. **保管**アクション・ボタンをクリックする。

GSO リソース・グループの削除

GSO リソース・グループを削除するには、次のようにします。

1. リソース・グループ・リスト・ビューから、削除したい GSO リソース・グループの名前を選択する。

   リソース・グループ詳細ビューに、 GSO リソース・グループ・メンバーのリストが表示されます。

2. 各 GSO リソースを、一度に 1 つずつ選択し、GSO リソース・グループからそれを削除する。
3. リソース・グループ・リスト・ビューから、 GSO リソース・グループを選択する。
4. GSO リソース・グループ項目を完全に削除するには、**削除**をクリックする。

GSO データの移行

IBM SecureWay グローバル・サインオンのバージョン 2.0.200 または、 IBM グローバル・サインオンの以前のリリースからの GSO データがある場合、 Policy Director の当バージョンで使用できるようにするには、 GSO データを移行する必要があります。

最新の情報とツール (移行ツールなど) が、次の IBM SecureWay Policy Director Web サイトにあります。

`http://www.ibm.com/software/security/policy/library`

GSO リソース・クリデンシャル・パスワードの変更

ユーザーは、Policy Director Web ベースのパスワード・ツール chpwd.exe を使って、GSO リソースまたは GSO リソース・グループの保管 GSO パスワードを更新できます。このツールを使う前に、必ずリソース・クリデンシャルを作成しておく必要があります。このツールは、最初にそのリソースのパスワードを変更してから使用します。

このファイルは、次の場所に入っています。

UNIX: `/opt/intraverse/www/docs/cgi-bin/chpwd`

Windows: `c:¥Program Files¥www¥docs¥cgi-bin¥chpwd.exe`

Web ツールを使って GSO リソース・クリデンシャル・パスワードを変更するには、次のようにします。

1. セキュア・ブラウザーのインスタンスをオープンします。
2. 次の URL ロケーションを入力します。

   `https: //`*`webseal server`*`/cgi-bin/chpwd.exe`

   ここで、*webseal server* は、WebSEAL サーバーに割り当てられた名前です。Windows の場合、URL 指定の一部として拡張子 .exe を入力する必要があります。
3. リソース名の欄で該当のリソースの名前をクリックして選択します。
4. **ユーザー ID (User ID)** フィールドにユーザー名を入力します。
5. **新規パスワード (New Password)** フィールドに変更後のパスワードを入力します。その後に、**新規パスワードの確認 (Confirm New Password)** フィールドにそのパスワードを再度入力して確認します。
6. **更新 (Update)** をクリックします。

第7章 アクセス制御について

セキュア・ドメイン内のリソースは保護することができます。 リソースを保護するには、特別な規則を定義し、これらのテンプレートを、リソースをオブジェクト形式で表現したものに付加して行います。これらの特別な規則は、*ポリシー・テンプレート* と呼ばれます。 Policy Director は、*アクセス制御リスト* (ACL) と呼ばれるポリシー・テンプレートのタイプを認識し、使用します。セキュア・ドメインに属するリソース上に、組織のセキュリティー・ポリシーをスタンプするには、ACL を使用してください。

この章は、次の各節に分かれています。

保護オブジェクト・ネームスペース

Policy Director セキュリティー・モデルは、セキュア・ドメインにあるリソースを保護するために、規則や許可に依存します。*許可についての特定のセットは、ポリシー・テンプレート*と呼ばれます。

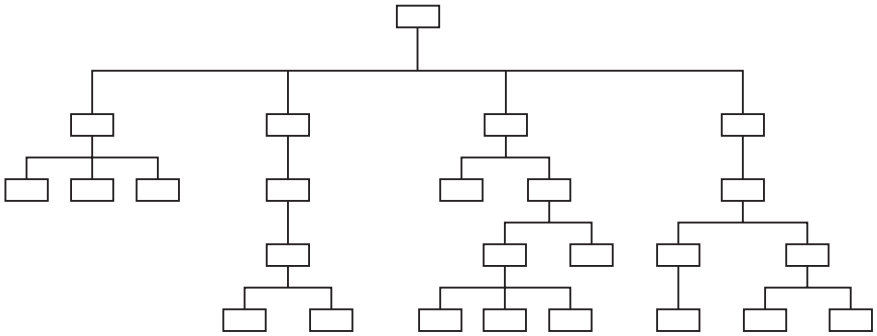
ポリシー・テンプレートは、リソースに付加されるときに、会社のセキュリティー・ポリシーをリソースに効果的に適用するものです。このセキュリティー・モデルを作成するとき、Policy Director は、セキュア・ドメインの物理リソース・インベントリーの論理オブジェクト表現を使用します。

実際の物理リソースを保護するために、ポリシー・テンプレートをネームスペース内の論理オブジェクトに付加します。 Policy Director 許可サービスは、認証中に得られたユーザーのクリデンシャルと、テンプレートで定義された許可とを比較して、許可の決定をします。

Policy Director の*保護オブジェクト・ネームスペース* は、セキュア・ドメインに所属するリソースを論理的に階層で示したものです。階層ネームスペースに現れるオブジェクトは、実際の物理的なネットワーク・リソースを表します。

システム・リソース
: 実際の物理ファイル、ネットワーク・サービス、またはアプリケーション。

保護オブジェクト
: Policy Director 許可サービス、管理コンソール、およびその他の Policy Director 管理ユーティリティーが使用する実際のシステム・リソースの論理表示。



保護オブジェクト・ネームスペースでは、次の 2 つのタイプのオブジェクトを使用します。

コンテナー・オブジェクト

コンテナー・オブジェクトは、構造を指定するもので、ネームスペースを別個の機能領域に階層的に編成するためのものです。コンテナー・オブジェクトにリソース・オブジェクトが入ります。

リソース・オブジェクト

リソース・オブジェクトは、ユーザーのセキュア･ドメインにある実際のネットワーク･リソース （サービス、ファイル、プログラム、など）を表したものです。

保護オブジェクト･ネームスペースの階層

保護オブジェクト･ネームスペースの構造上の先頭にあるのは、**ルート**コンテナー・オブジェクトです。 Policy Director 管理コンソールでは、ルートのシンボルは、スラッシュ (/) で表されます。

以下のネームスペースのカテゴリーが、ルート･オブジェクトの後に続きます。

Web オブジェクト (/WebSEAL コンテナー)

WebSEAL コンテナー・オブジェクトは、セキュア･ドメインの論理 Web スペース・ルートです。 Policy Director は、このサブツリーにある一部のオブジェクトに対して、すべての HTTP オペレーションを許可します。

Web オブジェクト は、静的 Web ページや動的 URL など、URL がアドレスできるものを表します。 Web-to-application ゲートウェイは、この静的 Web ページと動的 URL をデータベース照会や、その他のタイプのアプリケーション呼び出しに変換します。

ネットワーク・アプリケーション･オブジェクト (/NetSEAL コンテナー)

NetSEAL コンテナー･オブジェクトは、セキュア･ドメインの NetSEAL 保護サービスが入っている論理スペースのルートです。このオブジェクトは、TCP ネットワーク・アドレス (ポート) へのマップを行う TCP ベースのアプリケーション (TELNET や FTP など) を表します。アプリケーションは、これらのポートを使用します。

Policy Director 管理オブジェクト (/Management コンテナー)

Management コンテナー・オブジェクトは、すべての Policy Director 管理オペレーションを制御する論理スペースのルートです。管理オブジェクトは、ユーザーを定義し、セキュリティー・ポリシーを設定するために必要なサー

ビスを表します。このタスクは、 Policy Director 管理コンソールを使用するか、または **ivadmin** ユーティリティーを用いて実行します。

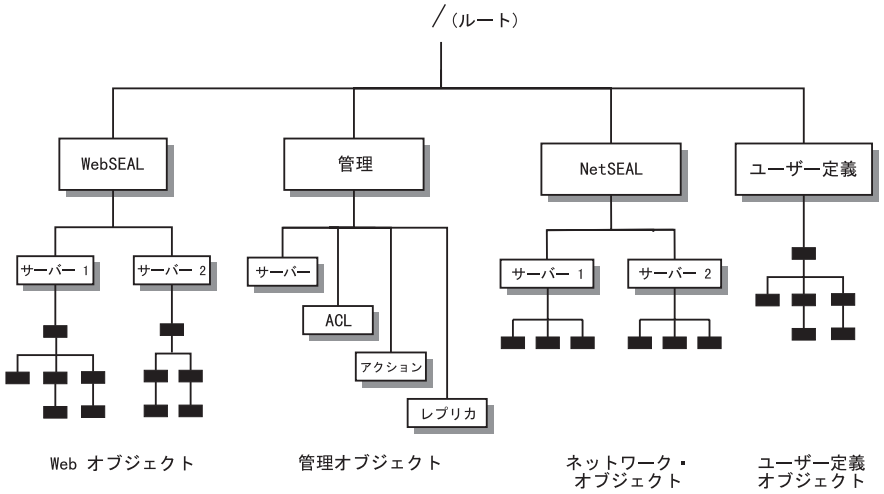
この領域のサブディビジョンには、次のものが含まれます。

- サーバー管理タスク (/Server)
- セキュリティー･ポリシー・タスク (/ACL)
- 第三者の許可制御 (/Action)
- 許可データベース複製制御 (/Replica)

Policy Director は、管理活動の代行をサポートし、セキュリティー・ポリシーを設定する管理者の能力を、ネームスペースのサブセットに限定することができます。

ユーザー定義のオブジェクト

このオブジェクトは、 Policy Director 許可サービス (これは、 Policy Director 許可 API を使用する) を使用する第三者のアプリケーションが保護するタスクまたはネットワーク・リソースを表します。



第三者のアプリケーション・ネームスペース

Policy Director は、保護オブジェクト・ネームスペースによって定義されるすべてのアプリケーション・オブジェクトに許可サービスを提供することができます。 Policy Director ファミリーの一部であるアプリケーションには、 WebSEAL (Web アプリケーションの場合) と NetSEAL (TCP ベースのアプリケーションの場合) があります。

Policy Director および第三者のアプリケーションは、Policy Director 許可 API を通して、Policy Director 許可サービスに対する呼び出しを行います。第三者のアプリケーションと Policy Director 許可サービスを統合したい場合は、次の 2 つのステップを行います。

1. 第三者のアプリケーションのネームスペースを記述します。
2. 保護を必要とするネームスペース・オブジェクトに許可を適用します。

任意選択のユーザー定義のオブジェクト・コンテナーは、ユーザーが第三者のアプリケーション・ネームスペースを作成できる場所の保護オブジェクト・ネームスペースの領域です。

保護オブジェクト・ネームスペースの中でこの第三者ネームスペースが開始されるルート (*接合ポイント*) を定義する必要があります。詳細については、139ページの『第三者アプリケーション・ネームスペースを定義する』を参照してください。

次に、管理コンソール、または **ivadmin** ユーティリティーを使用して、この新しいネームスペースで、これらのオブジェクトにある ACL の作成、付加、削除をします。

アクセス制御リスト

アクセス制御リスト (ACL) は、セキュア・ドメインにあるリソースの保護をするために、Policy Director が使用するポリシー・テンプレート・タイプです。

ACL は、保護リソースに対するオペレーションを実行するのに必要な条件を指定する規則、または許可のセットです。 ACL は、保護リソースに対して許可されるオペレーションを指定し、これらのオペレーションを実行できる人々の識別 (ユーザー、グループ、またはその両方) をリストします。たとえば、

- セキュリティー登録にあるユーザー識別およびグループ識別の定義
- 許可ポリシー・データベースにある保護オブジェクト・ネームスペースおよびポリシー・テンプレートの定義

ポリシー・テンプレートとして、Policy Director ACL は、それが表すセキュリティー・ポリシーを反映している固有名、またはラベルを持っています。そこで、保護オブジェクト・ネームスペースにあるリソースのオブジェクト表示に対して ACL を適用します。

ACL は、ユーザーの指定とグループの指定、およびそれらの特定の許可が含まれている 1 つ以上の項目から構成されます。

ACL 項目

ACL は、次に述べる 1 つ以上の項目から構成されます。

- オブジェクトへのアクセスが明示的に制御されるような、ユーザーおよびグループの UUID
- 各ユーザー、グループ、または役割に許可されている特定のオペレーション
- 『全認証』、また『非認証』の特別なユーザー・カテゴリーに許される特定のオペレーション

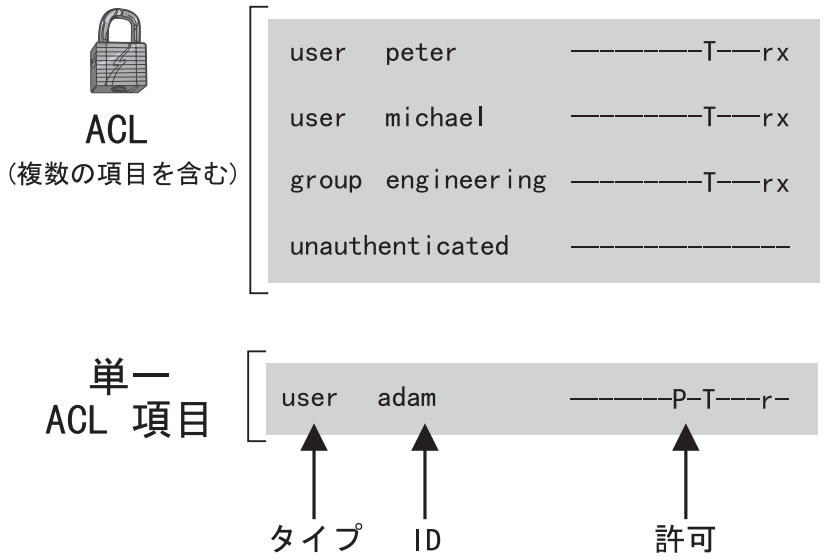
ユーザー、つまり、プリンシパルは、 Policy Director セキュリティー・サーバーから認証されている任意の識別を表します。通常、ユーザーとは、ネットワーク・ユーザーまたはアプリケーション・サーバーを表しています。

グループ とは、1 人以上のユーザーの集まりです。ネットワーク管理者は、グループ ACL 項目を使用して、同じ許可を複数のユーザーに割り当てることができます。新しいユーザーは、該当するグループのメンバーになることによって、オブジェクトへのアクセスを獲得します。このようにすると、すべての新しいユーザーに新しい ACL

項目を設定する必要がなくなります。グループは、セキュア・ドメイン内における組織上の部や課を表すことができます。グループはまた、役割や機能的な関連性を定義する際にも役立ちます。

まとめると、ユーザーとグループは、エンティティーです。

管理者は、Policy Director 管理コンソール (**ACL** 管理タブ) を用いて ACL 項目を作成、変更、削除します。



ポリシー・テンプレートとしての ACL

管理コンソールを用いて、次のことができます。

- 特定の ACL を作成する。
- それにラベルを付けて保管する。
- それを、セキュリティー・ポリシー・テンプレートとして、ネームスペースにあるオブジェクトに適用する。

ACL は、公式やレシピのように、単一のソース・テンプレートになります。 ACL には、関連する任意のオブジェクトに対して、適切なレベルの保護を提供するための特定の項目が含まれています。

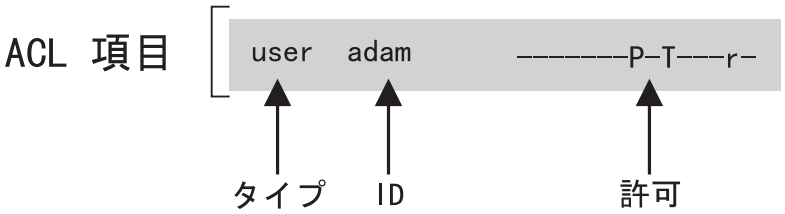
ACL リストの例に、以下のものを含めることができます。

```
ACL Name
デフォルトの management
デフォルトの netseal
デフォルトの replica
    default-root
    default-webseal
```

ACL テンプレートは、ワード・プロセッシングのドキュメントにおけるパラグラフのスタイル設定の場合と同様、単一の品質基準ソースを提供します。セキュリティー・ポリシーの要件を変えるときは、単一の ACL を編集するだけですみます。 Policy Director は、ACL が付加されているすべてのオブジェクトに対する新しいセキュリティー定義をただちに有効にします。

ACL 項目の構文

ACL 項目には、ACL 項目のタイプに応じて 2 つまたは 3 つの属性が含まれており、次のような形式で表されます。



タイプ

ACL が作成されたエンティティーのカテゴリー (ユーザーまたはグループ)。

ID (識別)

エンティティーの固有の識別 (名前)。

全認証 (any-authenticated) ACL 項目タイプ、または非認証 (unauthenticated) ACL 項目タイプはいずれも、ID 属性を必要としません。

許可

オブジェクトに対して、ユーザーまたはグループによる実行が許可されているオペレーションのセット。

ほとんどの許可では、リソースに対して特定のオペレーションを実行するクライアントの能力を記述します。リソースに対するアクションが許される場合、特定の条件が課せられる許可もあります。後者の例としては、データの強制的な暗号化、データ保全性の保護、監査サービスへの報告レコードの書き出し、ある種の外部許可条件の要求、などがあります。

この例では、Adam (type=user, ID=adam) は、この項目が含まれている ACL に関連付けられているオブジェクトを読む (表示する) 許可を持っています。 読み取り (r) 許可があると、読み取り操作が許されます。暗号化 (P) 許可は、通信チャネルがデータ暗号化を使用することを必要条件にしています。 トラバース (T) 許可は、トラバース属性を強制的にとります。

タイプ属性

ACL 項目タイプは、ACL 項目のエンティティーを指定します。4 つの ACL 項目タイプがあります。

タイプ	説明

ユーザー (user)	セキュア・ドメインの特定のユーザーに許可を設定します。ユーザー項目タイプには、アカウント名 (ID) が必要です。項目形式は、`user ID permissions` です。たとえば、次のとおりです。 `user greg -------------r-`
グループ (group)	セキュア・ドメインにある特定グループのメンバーに許可を設定します。グループの項目タイプには、グループ名 (ID) が必要です。項目形式は、`group ID permissions` です。たとえば、次のとおりです。 `group engineering -------------r-`
全認証 (any-authenticated)	すべての認証ユーザーに許可を設定します。 ID の指定は、不要です。 項目形式は、次のとおりです。 `any-authenticated -------------r-`

非認証 (unauthenticated)	セキュリティー・サーバーで認証されていないユーザーに許可を設定します。 ID の指定は、不要です。項目形式は、`unauthenticated permissions` です。 たとえば、次のとおりです。
	`unauthenticated ---------T---r-`
	この ACL 項目は、許可セットを決定するための、全認証 ACL 項目に対するマスク (ビット単位の “and” 演算) です。たとえば、非認証 ACL 項目は、
	`unauthenticated -------------r-`
	この全認証 ACL 項目に対してマスクをかけると、
	`any-authenticated ---------T---r-`
	その結果、以下のような許可になります。
	`-------------r- (read only).`

ID 属性

ACL ID は、ユーザー項目またはグループ項目タイプに対する、*固有の識別子*、つまり名前です。 ID は、セキュア・ドメイン用に作成され、レジストリー・データベースに保管されている、有効なユーザーおよびグループを表していなければなりません。

以下に、固有の識別子の例をあげます。

```
user michael
user greg
group engineering
group documentation
group accounting
```

注: 全認証および非認証 ACL 項目タイプに対して ID 属性を使用しないでください。

許可属性

ACL 項目にはそれぞれ、以下のことを記述する一連の *許可* が含まれています。

- ユーザーまたはグループによる実行が、オブジェクトで許可されている特定のオペレーション。
- オブジェクトへのアクセスのタイプでの制限、たとえば、
  - 通信チャネルでは、データ・プライバシーや保全性を必ず使用すること
  - アクセスの監査
  - 外部 (第三者) の許可要件

ACL は、次のことを制御することによって、保護リソースを制御します。

- 保護オブジェクトに対してオペレーションを実行するユーザーの能力
- オブジェクトおよび任意のサブオブジェクトに関するアクセス制御規則を変更する、管理者の能力
- ユーザーのクリデンシャルを代行する、Policy Director サーバーの能力

許可の順序

ACL 許可は、*コンテキストに依存した*許可です。コンテキストに依存した許可とは、特定の許可の動作が変化することを意味します。 この動作の変化は、許可が適用される保護オブジェクト・スペースの領域に応じて起こります。 たとえば、m 許可は、WebSEAL オブジェクトと Management オブジェクトでは、意味が異なります。

17 の標準許可が 4 つのカテゴリーに分けられており、ACL 項目で使用されると、次の順序で表示されます。

Base	Generic	NetSEAL	WebSEAL
a A b c g I P T	d m s v	C p	l r x

ACL 定義 / ACL 項目 ウィンドウには、許可のリストが表示されており、その中から選択できるようになっています。これらの許可の横にあるチェック・ボックスを選択して、許可を選択します。

Base
  (a) Attach
  (A) Audit
  (b) Browse
  (c) Control
  (g) Delegation
  (I) Integrity
  (P) Privacy
  (T) Traverse
Generic
  (d) Delete
  (m) Modify
  (s) Server Admin
  (v) View
NetSEAL
  (C) Connect
  (p) Proxy
WebSEAL
  (l) List Directory
  (r) Read
  (x) Execute

ネームスペースの領域

コンテナー・オブジェクトは、保護オブジェクト・ネームスペースの特定の領域を表すもので、以下のような重大なセキュリティー機能を行います。

1. コンテナー・オブジェクトの ACL を使用して、明示的に他の ACL が適用されないときに、その領域のすべてのサブオブジェクトの高レベルのポリシーを定義することができます。
2. コンテナー・オブジェクトの ACL を使用して、その領域のすべてのサブオブジェクトの高レベルのポリシーを定義することができます。明示的に他の ACL が適用されないときに、高レベルのポリシーを定義することができます。
3. コンテナー・オブジェクトの ACL からトラバース許可を除去することによって、この領域にあるすべてのオブジェクトへのアクセスを即座に拒否することができます。

トラバース許可

トラバース許可は、保護オブジェクト・ネームスペース全体にわたって適用される汎用の許可です。

トラバース許可	アクセス	説明
T	トラバース	リクエスターが、要求されたオブジェクトへの途中にあるオブジェクトを階層的にパススルーできるようにします。そのオブジェクトへの他のタイプのアクセスは、許されません。トラバースは、要求されたオブジェクト自体にも必要です。

アクセス条件

アクセス条件は、保護オブジェクト・ネームスペース全体に適用される汎用の許可です。

すべての保護オブジェクトのアクセス条件	アクセス	説明
A	監査	Policy Director サーバーは、オブジェクトがアクセスされるとき常に、監査レコードを監査サービスに書き出します。許可が正常に行われなかった場合も含めて、アクセスの試みをすべて監査します。
I	保全性	このオブジェクトをアクセスするときは、クライアントと Policy Director サーバーとの間で、データの保全性保護が必要になります。
P	プライバシー	このオブジェクトをアクセスするときは、クライアントと Policy Director サーバーとの間で、データの暗号化が必要になります。

制御許可

制御許可は、ACL の所有権をユーザーに与える強力な許可です。制御許可を使うと、ACL にある項目を変更することができます。制御という意味は、項目の作成、項目の削除、許可の認可、および許可のはく奪の力を持つことを意味します。

制御許可	アクセス	説明
c	制御	ACL テンプレートの所有権; この ACL の項目の作成、削除、および修正を可能にします。

管理者は、この ACL を ACL テンプレートのリストから削除できます。削除の前に、管理者は、該当の ACL の中に項目を持っている必要があります。さらに、管理者は、該当の項目の中に制御許可を持っている必要があります。

制御許可を用いて、ユーザーは、別のユーザーに管理の権限を付与することができます。たとえば、オブジェクトに ACL を付加する権限を付与することができます。ACL をオブジェクトに付加するときは、付加 (a) 許可を使用します。

制御 (c) 許可を使用するときは、所有権のプロパティーが非常に強力なので、十分注意してください。

ルート・コンテナー・オブジェクト

*ルート (/) コンテナー・オブジェクト*には、次のようなセキュリティーの考慮事項が適用されます。

- ルート・オブジェクトは、保護オブジェクト・ネームスペース全体の ACL 継承のチェーンの始まりです。
- 他の ACL を明示的に適用しないと、ルート・オブジェクトは、ネームスペース全体のセキュリティー・ポリシーを定義します (継承によって)。
- ルートの下にある任意のオブジェクトへのアクセスには、トラバース (T) 許可を使用する必要があります。

WebSEAL ネームスペース

/WebSEAL コンテナー・オブジェクトには、次のようなセキュリティーの考慮事項が適用されます。

- WebSEAL オブジェクトは、ネームスペースの WebSEAL 領域のための ACL 継承のチェーンの始まりです。
- 他の ACL を明示的に適用しないと、このオブジェクトは、Web スペース全体のセキュリティー・ポリシーを定義します (継承によって)。
- このオブジェクトおよびこのポイントの下にある任意のオブジェクトへのアクセスには、トラバース (T) 許可を使用する必要があります。

/WebSEAL/host

このサブツリーには、特定の Policy Director の WebSEAL サーバーの Web スペースが含まれています。次のようなセキュリティーの考慮事項がこのオブジェクトに適用されます。

- このポイントの下にある任意のオブジェクトへのアクセスには、トラバース (T) 許可を使用する必要があります。
- 他の ACL を明示的に適用しないと、このオブジェクトは、このマシンのネームスペース全体のセキュリティー・ポリシーを定義することになります (継承によって)。

/WebSEAL/host/file

このサブツリーは、HTTP アクセスについてチェックされるリソース・オブジェクトです。チェックされる許可は、要求されたオペレーションによって異なります。

WebSEAL 許可

以下の表で、ネームスペースの WebSEAL 領域に適用される許可について説明します。

WebSEAL ネームスペースの許可	アクセス	説明
r	読み取り	HTTP オブジェクトを表示します。
x	実行	CGI プログラムを実行します。
d	削除	HTTP オブジェクトを除去します。
m	修正	HTTP オブジェクトを PUT します (HTTP オブジェクトを WebSEAL ネームスペースに入れ、公表する)。
l	リスト	HTTP ディレクトリー自動リストを生成する。
g	代行	クライアントの代わりに処置をとるよう、WebSEAL サーバーにトラストを割り当て、接合された WebSEAL サーバーにその要求をパスします。

NetSEAL ネームスペース

/NetSEAL オブジェクトには、次のようなセキュリティーの考慮事項が適用されます。

- NetSEAL オブジェクトは、ネームスペースの NetSEAL 領域のための ACL 継承のチェーンの始まりです。
- 他の ACL を明示的に適用しないと、このオブジェクトは、ネームスペースの中のすべての NetSEAL 保護サービスのセキュリティー・ポリシーを定義します (継承によって)。
- このオブジェクトおよびこのポイントの下にある任意のオブジェクトへのアクセスには、トラバース (T) 許可を使用する必要があります。

/NetSEAL/host

このサブツリーには、特定のサーバー・マシン上にあるすべての NetSEAL 保護サービスが含まれています。次のようなセキュリティーの考慮事項がこのオブジェクトに適用されます。

- このポイントの下にある任意のリソースへのアクセスには、トラバース (T) 許可を使用する必要があります。
- 他の ACL を明示的に適用しないと、このオブジェクトは、このマシンのすべての NetSEAL 保護サービスのセキュリティー・ポリシーを定義することになります (継承によって)。

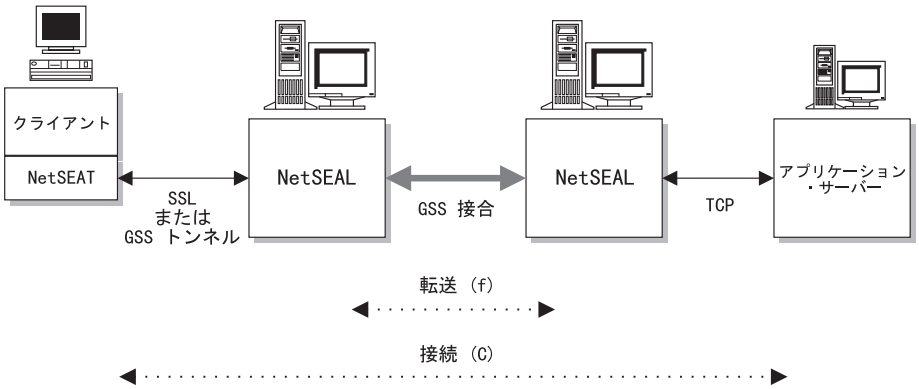
/NetSEAL/host/service

このサブツリーは、それが表している保護サービスへのアクセスについてチェックされるオブジェクトです。チェックされる許可は、要求されたオペレーションによって異なります。

NetSEAL 許可

以下の表で、ネームスペースの NetSEAL 領域に適用される許可について説明します。

NetSEAL 保護オブジェクト許可:	アクセス	説明
C	接続	NetSEAL サーバーに接続する。
f	転送	NetSEAL 接合を超える発信接続 (接合をトラバース) を許可する。



管理ネームスペース

/Management オブジェクトには、次のようなセキュリティーの考慮事項が適用されます。

- 管理オブジェクトは、ネームスペースの管理領域のための ACL 継承のチェーンの始まりです。
- 他の ACL を明示的に適用しないと、このオブジェクトは、管理ネームスペース全体のセキュリティー・ポリシーを定義します (継承によって)。
- このオブジェクトへのトラバース (T) 許可アクセスを持っている必要があります。

/Management/server

Policy Director の保護オブジェクト・ネームスペースの /Management/server コンテナーを用いて、管理者は、サーバー管理タスクを実行することができます (適切な許可が設定されていれば)。

サーバー管理制御を用いて、ユーザーが、サーバー定義の作成、変更、または削除の許可を持っているかどうか判別します。サーバー定義には、他の Policy Director サーバー (特に管理サーバー (ivmgrd)) が、そのサーバーを見つけて、通信できるようにするための情報が含まれています。

インストール・プロセスの一部として、特定のセキュリティー・マネージャー (secmgrd) または許可サーバー (ivacld) のサーバー定義を作成することができます。さらに、 Policy Director は、サーバーをアンインストールするときにサーバーの定義を削除します。

定義の作成と削除は、自動的に行われます。インストール管理者は、定義を作成するための特別なステップを実行する必要はありません。しかし、管理者は、インストール中に定義を作成するために、 /Management/Server オブジェクトに関する修正 (m) 許可を持っている必要があります。

さらに、管理者は、アンインストール中に定義を削除するために、 /Management/Server オブジェクトに関する削除 (d) 許可を持っている必要があります。

サーバー定義に対して実行できる他のオペレーションとして、ユーザーは次のようなことができます。

- **ivadmin** ユーティリティーを用いて、定義を表示する。ユーザーは、サーバー・オブジェクトに関してビュー (v) 許可を付与される必要があります。
- サーバーの開始、停止、延期、再開、またはログの削除、などの、サーバー管理オペレーションを実行する。ユーザーは、サーバー・オブジェクトに関してサーバー管理 (s) 許可を付与される必要があります。
- **ivadmin server modify** コマンドを用いて、定義の一部を変更する。ユーザーは、サーバー・オブジェクトに関して修正 (m) 許可を付与される必要があります。

サーバー管理の許可	アクセス	説明
s	サーバー	サーバー管理タスク (開始、停止、延期、再開、など) を実行します。
v	ビュー	サーバーをリストします。
m	修正	新しいサーバー定義を作成します。
d	削除	サーバー定義を削除します。

/Management/ACL

このオブジェクトを使用して、管理ユーザーは、セキュア・ドメインのセキュリティー・ポリシーに影響を与える可能性のある高レベルの ACL 管理タスクを実行することができます。

ACL 管理許可	アクセス	説明
b	ブラウズ	オブジェクトの下のネームスペースの内容を表示します。
a	付加	ACL テンプレートをオブジェクトに付加します。ACL テンプレートをオブジェクトから除去します。
m	修正	新しい ACL テンプレートを作成します。
d	削除	既存の ACL テンプレートを削除します。ACL には、この同じユーザーに対する制御 (c) 許可を持つ項目が含まれている必要があります。
v	ビュー	ACL をリストまたは表示します。

デフォルトの ACL 管理オブジェクトの中に ACL 管理者を定義する必要があります。管理者の ACL 項目に、上記の許可を含めることができます。これらの許可があると、新しい ACL テンプレートの作成、ACL のオブジェクトへの付加、および ACL テンプレートの削除の権限が管理者に与えられます。

その管理者の ACL の中に、制御 (c) 許可が含まれている項目が存在しているのでない限り、ACL 管理者は既存の ACL を変更することができません。その項目を変更できるのは、ACL の所有者だけです。

新しい ACL テンプレートの作成者は、その ACL の中で最初の項目になり、 abcT 許可がデフォルトで設定されます。

たとえば、cell_admin がデフォルト管理 ACL の中の項目で、(m) 許可を持っているとすれば、cell_admin は、新しい ACL テンプレートを作成することができます。ユーザーの cell_admin が新しい ACL の最初の項目 (abcT 許可を持つ) になります。制御 (c) 許可は、cell_admin に ACL の所有権を与えるので、 cell_admin は ACL を変更することができます。このあと、ユーザーの cell_admin は、管理の許可を、その ACL の中にある他のユーザー項目に付与できます。

デフォルト管理 ACL 自体の所有権は、ユーザーの cell-admin と、グループの iv-admin にデフォルトで与えられます。

/Management/action

このオブジェクトは、管理ユーザーが、第三者のネームスペースの中で ACL 管理タスクを実行できるようにします。アクション・タスクおよび関連する許可には、以下のものが含まれます。

アクション管理許可 (第三者の許可)	アクセス	説明
m	修正	新しいアクションを作成します。
d	削除	既存のアクションを削除します。

Policy Director は、アプリケーションに対して許可サービスを提供します。 Policy Director ファミリーの一部であるアプリケーションには、 WebSEAL (Web アプリケーションの場合) と NetSEAL (TCP ベースのアプリケーションの場合) があります。

第三者のアプリケーションは、Policy Director 許可 API を通して、 Policy Director 許可サービスに対する呼び出しを行うことができます。第三者のアプリケーションと Policy Director 許可サービスを統合するために必要な 2 つのステップで、以下のことを行います。

- アプリケーションのネームスペースを定義する。
- 保護を必要とするオブジェクト (リソース) に許可を適用する。

第三者のアプリケーションのネームスペースの管理者は、 **ivadmin** ユーティリティーを使用して、新しい許可とアクションを定義することができます。これらの許可とアクションの作成と削除をするために、管理者は、管理許可とアクション許可を持っている必要があります。

/Management/replica

Policy Director 保護オブジェクト・ネームスペースの /Management/Replica コンテナー・オブジェクトは、許可データベースの複製 (レプリカ) を制御します。このオブジェクトに対する高レベルの制御は、セキュア・ドメインにおける管理サーバーとセキュリティー・マネージャーのオペレーションに影響します。

レプリカ管理制御は、複製が正しく行われるように、1 次許可ポリシー・データベースをどのプロセスが読み取りまたは更新できるかを判別するために、使用されます。

制御および関連する許可には、以下のものが含まれます。

レプリカ管理許可	アクセス	説明
v	ビュー	1 次許可データベースを読み取ります。
m	修正	レプリカ・データベースの修正を許可します。

Policy Director サーバーはすべて、許可データベースのローカル・レプリカを保守しています。 Policy Director サーバーには、すべてのセキュリティー・マネージャー (secmgrd) および Policy Director 許可サーバー (ivacld) が含まれます。すべての Policy Director サーバーは、/Management/Replica オブジェクトに関してビュー (v) 許可を持っています。

複製プロセスは、これらのプロセスが、1 次許可ポリシー・データベースから項目を表示し、アクセスできるようにします。 Policy Director のインストールでは、許可ポリシー・データベースへのアクセスを必要とするどのサーバーに対しても、自動的に読み取り (r) 許可が付与されます。

Policy Director は、現在、修正 (m) 許可を使用していません。現在、ユーザーは、管理コンソールまたは **ivadmin** ユーティリティーを使って、1 次ポリシー許可データベースを変更します。これらのツールは、他のもっときめの細かいチェックを受けます。

セキュア・ネームスペースのガイドライン

これらのガイドラインは、ネームスペースを安全にするために役立つ情報を提供します。

- ネームスペースの最上部にあるコンテナー・オブジェクトに、高レベルのセキュリティー・ポリシーを設定します。階層の低い位置にあるオブジェクトに明示的 ACL を付けて、このポリシーに例外を設定します。
- 保護オブジェクト・スペースは、ほとんどのオブジェクトが継承によって保護される (明示的、つまり ACL ではなく) ように、配置します。

  継承 ACL の場合は、保守の必要がある ACL の数が減るので、ユーザーのツリーの保守が簡素化されます。このように、保守が少なくなると、ネットワークを危うくする恐れのあるエラーのリスクが減少します。
- 新しいオブジェクトは、適切な許可を継承するようなツリーに置くようにします。

  ユーザーのオブジェクト・ツリーは、それぞれのサブツリーが特定のアクセス・ポリシーによって支配されるような、サブツリーのセットに組み入れます。サブツリーのルートに明示的な ACL を設定することによって、サブツリー全体のアクセス・ポリシーを決定します。
- ACL テンプレートのコア・セットを作成して、必要なところでこれらの ACL を再使用します。

  ACL テンプレートは単一のソース定義なので、このテンプレートが修正されると、この ACL と関連するすべてのオブジェクトが影響を受けます。
- グループを用いることによって、ユーザー・アクセスを制御します。

  ACL をグループ項目だけで構成することも可能です。これらのグループへのユーザーの追加や、そこからのユーザーの除去では、個々のユーザーごとに効率よく、オブジェクトへのアクセスを制御することができます。

標準の管理 ACL テンプレート

セキュア・ドメインの特定の領域を機密保護するための原点として、次のようなデフォルトの管理 ACL テンプレートをお勧めします。

ユーザー (user)、グループ (group)、全認証 (any-authenticated)、および非認証 (unauthenticated) について、項目を追加することができます。これらの項目は、さらに広い範囲の制御を提供するもので、ユーザーの保護オブジェクト・スペース必要条件にもさらによく合います。

制御 (c) 許可が含まれている、それぞれの ACL の中にあるユーザーとグループについて注意してください。制御許可を持つユーザー、グループ (またはその両方) は、ACL を*所有*しており、ACL 項目を変更する権利を持っています。

ルート

デフォルトのルート ACL (デフォルト・ルート) のコア項目には、次のものが含まれています。

```
user cell_admin                    abcT
group iv-admin                     abcT
any-authenticated                  T
unauthenticated                    T
```

ルート ACL は、非常に基本的なものです。ネームスペースのトラバースは、誰でもできますが、他のアクションは、誰でも実行できるわけではありません。通常、ユーザーはこれを変更する必要はありません。しかし、ルート ACL の有用な機能の 1 つに、個々のユーザーまたはグループの、ネームスペース全体へのアクセスを即座に拒否する機能があります。

ルート ACL にある次のような項目について考えてみましょう。

```
user john ----------------
```

この項目 (許可なし) の結論は、`user john` は、ルート・コンテナー・オブジェクトをトラバースすることもできない、ということです。ツリーの中の低い位置でどのような許可が付与されていても、このユーザーは、保護オブジェクト・スペースにアクセスすることは、絶対にできません。

同じ手法を WebSEAL および NetSEAL オブジェクト・スペースに適用することができます。たとえば、/WebSEAL コンテナー・オブジェクトで、特定のユーザーからトラバース (T) 許可を取り上げることができます。取り上げられたそのユーザーは、WebSEAL ネームスペースにまったく入ることができません。そのユーザーは、それらの領域にあるオブジェクトに関してどのような許可が付与されていても、入ることはできません。

WebSEAL オブジェクト・スペース

WebSEAL ACL (デフォルトの webseal) コア項目には、以下のものが含まれています。

```
user cell_admin                    abcTdmlrx
group iv-admin                     abcTdmlrx
group webseal-servers              gTdmlrx
group ivmgrd-servers               Tl
```

インストール時に、このデフォルト ACL は、ネームスペースの中の /WebSEAL コンテナー・オブジェクトに接続されます。

このグループ webseal-servers には、セキュア・ドメインにあるそれぞれの WebSEAL サーバーの項目が含まれています。デフォルトの許可により、サーバーは、ブラウザーの要求に応答することができます。

グループ ivmgrd-servers には、管理サーバーを表す 1 つの項目だけが含まれています。管理コンソールから出されるほとんどの管理要求は、ターゲットの WebSEAL サーバーに対する管理サーバーを用いて、開始されます。したがって、管理サーバーは、ターゲット・サーバーで要求を実行する許可を持っている必要があります。

トラバース許可があると、管理コンソールで表されているように Web スペースを拡張することができます。リスト許可があると、管理コンソールは、Web スペースの内容を表示することができます。

NetSEAL オブジェクト・スペース

NetSEAL ACL (デフォルトの netseal) のコア項目には、以下のものが含まれています。

```
user cell_admin                    abcTC
group iv-admin                     abcTC
```

インストール時に、この ACL は、ネームスペースの中の /NetSEAL コンテナー・オブジェクトに接続されます。保護サービスへのアクセスのための制御 (c) 許可を付与する必要があります。

管理オブジェクト・スペース

管理 ACL (デフォルトの management) コア項目には、以下のものが含まれています。

```
user cell_admin                    abcTdmsv
group iv-admin                     abcTdmsv
group ivmgrd-servers               Ts
any-authenticated                  Tv
unauthenticated                    Tv
```

インストール時に、この ACL は、ネームスペースの中の /Management コンテナー・オブジェクトに接続されます。

レプリカ管理オブジェクト

レプリカ管理 ACL (デフォルトの replica) コア項目には、以下のものが含まれています。

```
group secmgrd-servers              dmv
group ivacld-servers               dmv
group ivmgrd-servers               m
group iv-admin                     abcTv
user cell_admin                    abcTv
```

ACL の評価

Policy Director は、ACL によって特定のユーザーに付与される許可を判別するために、特定の評価プロセスを行います。

認証された要求の評価

Policy Director は、認証されたユーザーを次の順序で評価します。

1. ユーザー ID を ACL のユーザー項目と突き合わせます。付与される許可は、一致した項目にあるものです。

   ```
   Successful: evaluation stops here. Unsuccessful: continue to the next step.
   ```

2. ユーザーが所属するグループ (複数も可) を判別し、ACL のグループ項目と突き合わせます。

   複数のグループ項目が一致した場合は、その許可は、一致した各項目から付与された許可の論理 “or” 演算 (最も多く許可) の結果になります。

   ```
   Successful: evaluation stops here.
   Unsuccessful: continue to the next step.
   ```

3. 全認証項目 (あれば) の許可を付与します。

   ```
   Successful: evaluation stops here.
   Unsuccessful: continue to the next step.
   ```

4. 全認証 ACL 項目がない場合は、暗黙的な全認証エンティティーが存在します。この暗黙的な項目は、許可を何も付与しません。

   ```
   Successful: no permissions granted.
   End of evaluation process.
   ```

非認証要求の評価

Policy Director は、ACL の非認証項目から許可を付与することによって、非認証ユーザーを評価します。

*非認証項目*は、許可を決定するときの、全認証項目に対するマスク (ビット単位の “and” 演算) です。非認証に対する許可は、許可が全認証項目の中にも出てくるときだけ、付与されます。

非認証は、全認証に応じて決まるので、ACL が全認証なしの非認証を持つことは、あまり意味がありません。全認証がないのに ACL に非認証が含まれている場合のデフォルトの応答は、非認証に許可を付与しない、ということになります。

ACL 項目の例

ユーザーは、適切な ACL 項目タイプを指定することによって、特定のユーザー、グループ、または両方に対して許可を設定します。以下の例では、グループ documentation は、全アクセス権を持っています。

```
group documentation --bcg--TdmsvC-lrx
```

全認証項目タイプを使用して、セキュア・ドメインにある他の認証ユーザー (documentation グループに属さない) へのアクセスを制限することができます。

```
any-authenticated -------T--------rx
```

セキュア・ドメインのメンバーでないユーザーの非認証項目タイプへのアクセスをさらに制限することができます。

```
unauthenticated -------T-------r-
```

注: 非認証 ACL 項目がないと、非認証ユーザーは、Policy Director セキュア・ドメインの中のどのセキュア・ドキュメントもアクセスできません。

ACL 継承のための疎 ACL モデル

保護オブジェクト・スペースにあるネットワーク・リソースを保護するために、各オブジェクトに ACL を付加する必要があります。

次の 2 つの方法のどちらかで、オブジェクトに ACL を割り当てることができます。

- オブジェクトで*明示的* ACL を付加する。
- 階層内にある先行のコンテナー・オブジェクトからその ACL を、オブジェクトが*継承* できるようにする。

ACL のスキームを継承して採用すると、セキュア・ドメイン用の管理タスクを大幅に減らすことができます。このセクションでは、継承された、すなわち疎の ACL の概念を説明します。

疎 ACL モデルの概要

この原則は、ACL 継承の権利の基礎となるものです。明示的に付加された ACL を持たないオブジェクトは、明示的に設定された ACL を持つ、最も近いコンテナーの ACL を継承します。言いかえると、明示的に付加された ACL を*持たない* すべてのオブジェクトは、明示的に付加された ACL を*持つ* オブジェクトから ACL を継承するということです。継承の特定のチェーンは、オブジェクトに明示的な ACL を付加すると、そこで切断されます。

ACL 継承の方法をとると、大きな、保護されたオブジェクト・スペースに対するアクセス制御の設定と保守の仕事が簡素化されます。典型的なオブジェクト・スペースでは、オブジェクト・スペース全体を保護するためのキー位置で、数個の ACL をいくつか付加するだけですみます。キー位置にある数個の ACL は、*疎* ACL モデルを意味します。

典型的な Policy Director のネームスペースは、ルート・コンテナー・オブジェクトに付加されている単一の明示的な ACL から始まります。ルート ACL は、常に存在していなければならず、除去することはできません。通常、これは、ほとんど制約事項のない ACL です。その下のネームスペースにあるオブジェクトはすべて、この ACL を継承します。

ネームスペースの中の領域またはサブツリーに、異なるアクセス制御の制約事項が必要な場合は、そのサブツリーのルートに明示的な ACL を付加します。このようにすると、1 次ネームスペースのルートからそのサブツリーへの、継承 ACL の流れが中断されます。継承の新しいチェーンは、新たに作成されたこの明示的な ACL から始まります。

デフォルトのルート ACL テンプレート

Policy Director は、継承のチェックを、保護されたオブジェクト・スペースのルートから始めます。ツリーの中の他のどのオブジェクトでも明示的に ACL をセットしないと、ツリー全体がこのルート ACL を継承します。

ルートで設定される明示的な ACL テンプレートが常に 1 つあります。管理者は、この ACL を、別の項目や許可の設定を持つ別の ACL と置き換えることができます。しかし、ルート ACL を完全に除去することはできません。

Policy Director は、Policy Director の最初のインストールと構成の際に、 ACL Definition/ACL Entry ウィンドウで、ルート ACL テンプレートを明示的に設定します。

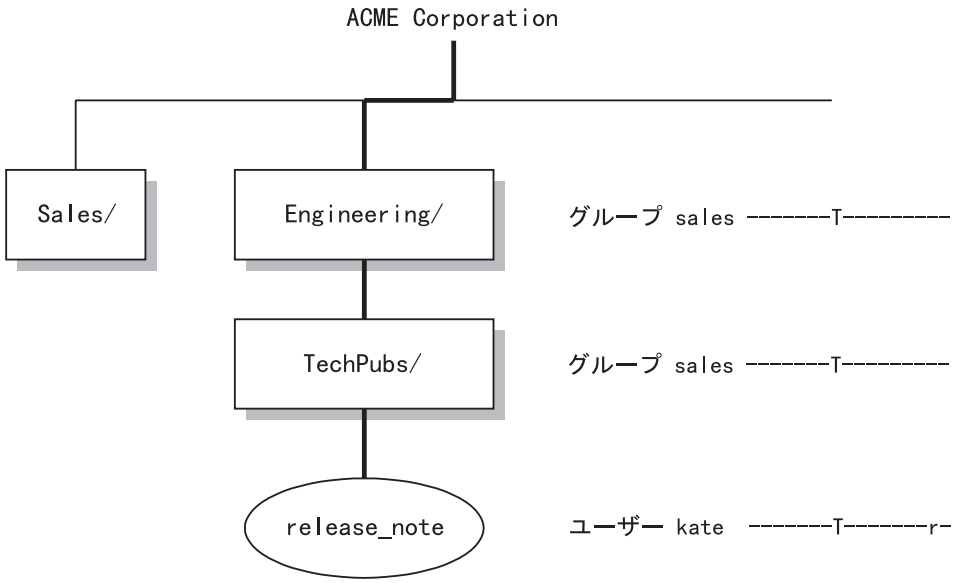
```
ACL Name     default-root
Description  Default Root ACL
```

トラバース許可

トラバース (T) 許可は、ACL 項目で識別されたエンティティーが、そのオブジェクトをパススルーする許可を持つことを指定します。項目は、階層の下の方にあるオブジェクトへのアクセスを得るために、オブジェクトをパススルーする許可を必要とします。トラバース許可は、そのオブジェクトに対して他の許可は付与しません。要求されたオブジェクト自体にも、トラバース許可を与える必要があります。

以下の図は、トラバース許可の機能を示したものです。 ACME Corporation には、Engineering ディレクトリーがあって、さらにその中に TechPubs サブディレクトリーが含まれています。Kate (user kate) は、 Sales 部門のメンバーですが、リリース・ノート・ファイルを検討するために、 /Engineering/TechPubs ディレクトリーにアクセスする必要があります。

管理者は、グループ sales の ACL 項目を、トラバース (T) 許可を付けて、/Engineering および /TechPubs ディレクトリーの両方に置いています。 user kate は、これらの 2 つのディレクトリーの中に他の許可は持っていませんが、release_note ファイルにアクセスするためにこれらのディレクトリーをパススルーすることができます。このファイルは、user kate に対してトラバース (T) と読み取り (r) 許可を持っているので、彼女はこのファイルを表示することができます。



指定のコンテナー・オブジェクトより下の階層へのアクセスを制限するのは容易です。これらのオブジェクトの個々の許可を再設定する必要はありません。単に、トラバース許可を該当の ACL 項目から除去するだけです。ディレクトリー・オブジェクトでトラバース許可を除去すると、その下の階層のすべてのオブジェクトが保護されます (これらのオブジェクトにもっと制限の少ない他の ACL が含まれていたとしても)。

たとえば、グループ sales は、Engineering ディレクトリーで、トラバース (T) 許可を持っている必要があります。グループ sales がこの許可を持っていないとすると、Kate は、このファイルに対する読み取り (r) 許可を持っていても、release_note ファイルにアクセスすることはできません。

アクセス要求の解決

継承は、ルート ACL から始まり、明示的な ACL を持つオブジェクトが出てくるまで、ネームスペースにあるすべてのオブジェクトに影響を与えます。このポイントから、継承の新しいチェーンが始まります。

明示的に設定された ACL の下にあるオブジェクトは、この新しいアクセス制御を継承します。明示的な ACL を削除すると、すべてのオブジェクトに対するアクセス制御は、明示的に設定された ACL を持つ最も近くにあるディレクトリーまたはコンテナー・オブジェクトに戻ります。

ユーザーがセキュア・オブジェクトにアクセスしようとすると、Policy Director は、そのユーザーがオブジェクトにアクセスする許可を持っているかどうかチェックします。たとえば、セキュア・オブジェクトを Web ドキュメントにすることができます。これは、正しく継承されたか、または明示的に設定された許可に関して、オブジェクト階層に沿ってすべてのオブジェクトをチェックすることによって、行われます。

管理者は、オブジェクトへのユーザーのアクセスを拒否することができます。 Policy Director は、階層の上方にある任意のディレクトリー・オブジェクトまたはコンテナ

ー・オブジェクトに、そのユーザーに対するトラバース (T) 許可が含まれていないと、アクセスを拒否します。また、Policy Director は、要求されたオペレーションを実行するのに必要な許可をターゲット・オブジェクトが十分に持っていないときは、アクセスを拒否します。

アクセス・チェックを成功させるためには、要求側は以下の両方を持っている必要があります。

1. 要求されるオブジェクトへのパスをトラバースする許可。
2. 要求されるオブジェクトに関する適切な許可。

以下の例では、ユーザーがオブジェクトを読み取る (表示する) ことができるかどうかを解決するプロセスが示されています。

```
/acme/engineering/project_Y/current/report.html
```

Policy Director は、以下のことをチェックします。

1. 明示的に設定されたルート ACL (/) でのトラバース許可。
2. ディレクトリー (acme、engineering、 project_Y、および current) に接続された明示的な ACL のトラバース許可。
3. ファイル自体 (report.html) の読み取り許可。

オブジェクト階層に沿ったこれらのポイントのいずれかで、ユーザーがアクセス・チェックに失敗すると、Policy Director は、ユーザー・アクセスを拒否します。

異なるオブジェクト・タイプに適用される ACL テンプレート

様々なオペレーションに関する ACL テンプレートの中に、許可を設定することができます。ここで可能になったオペレーションのサブセットだけが、その ACL が接続された特定のオブジェクトに関連があるものです。

この動作の原因は、管理を容易にするために設計された Policy Director の 2 つの機能に関連しています。

- ACL テンプレート
- ACL 継承

ACL テンプレートを使うと、保護オブジェクト・ネームスペースにある複数オブジェクトに、同じ ACL 定義を付加することができます。 ACL 定義は、その ACL が適用されるすべてのオブジェクトの要件に合わせて、十分な項目を用いて構成されます。しかし、それぞれの個々のオブジェクトに影響する項目数は、少しだけです。

ACL の継承モデルでは、付加された明示的 ACL を持たないオブジェクトはいずれも、ポリシーの定義を継承します。このような継承されたポリシーの定義は、それより上方の階層にあるオブジェクトに適用された ACL の中の最も近いものからとられます。

要約すると、ACL テンプレートは、それが適用されるすべてのオブジェクト・タイプにとって必要なすべての許可を記述する必要があります。 ACL テンプレートは、それが接続されているオブジェクトだけを記述するわけではありません。

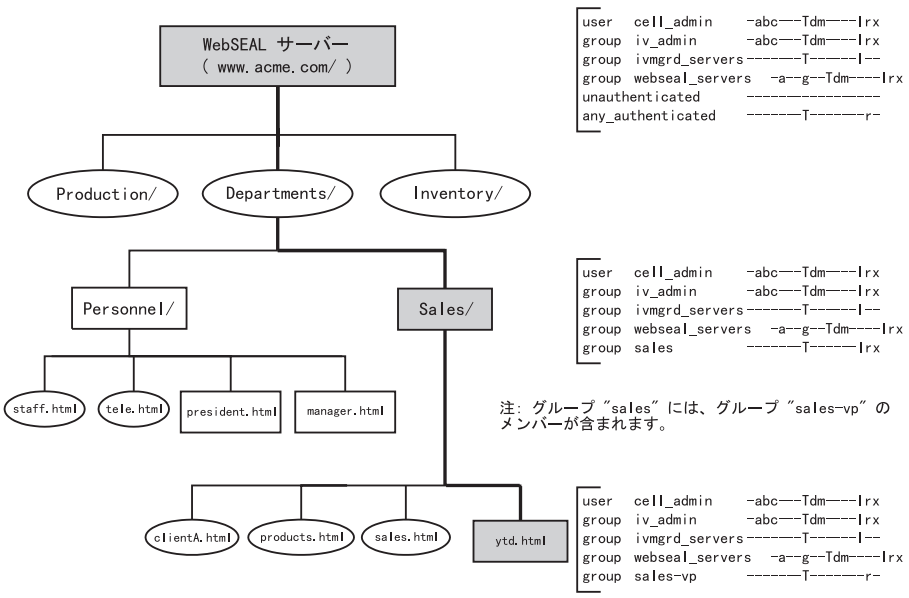
ACL 継承の例

以下の図は、ある会社のネームスペースにある継承 ACL と明示的 ACL が混合した場合の影響を示す図です。

この会社のオブジェクト・スペースは、ルート ・オブジェクトのところに汎用のセキュリティー・ポリシーを設定しています。ルートの後には、 /WebSEAL コンテナー・オブジェクトと、個々に制御される部門のサブツリーが続きます。

この例では、sales グループにその部門のサブツリーの所有権が与えられています。このサブツリー上の ACL は、非認証または全認証の項目タイプを、認識しないことに注意してください。 Year-to-Date sales ファイル (ytd.html) は、明示的 ACL を持っています。この明示的 ACL は、sales-vp グループのメンバーに対して読み取り (r) 許可を付与しています。(これらの sales-vp グループのメンバーは、sales グループのメンバーでもあります)。

注: この ACL のスキームは、セキュア・ドメイン内のユーザーの追加や削除のために変更する必要はありません。新しいユーザーは、単に適切なグループ (複数も可) に追加されるだけです。同様に、ユーザーをこれらのグループから除去することもできます。



ACL 管理の代行

セキュア・ドメインの中での管理責任の分散を管理の代行と呼びます。一般に、多くの部門やリソースの部課が含まれている大きなサイトの場合、要求が増え、管理の代行の必要性が起きてきます。

一般に、大きなオブジェクト・スペースを、これらの部門や部課を表す領域に編成することができます。ドメインの別々の領域はそれぞれ、よりよい状態に編成することができます。また、それぞれ別の領域にすると、その分野の問題点や必要性をよく理解している管理者が保守することができます。

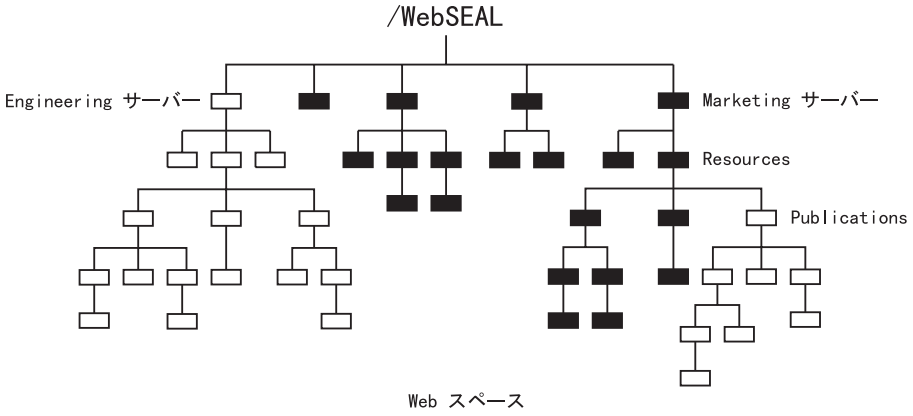
ドメインの別々の領域はそれぞれ、通常は、よりよい状態に編成されます。その分野の問題点や必要性をよく理解している管理者が、それぞれ別の領域を保守します。

Policy Director のセキュア・ドメインでは、最初は、cell_admin アカウントが、管理許可を持つ唯一のアカウントです。 cell_admin として、管理アカウントを作成し、オブジェクト・スペースの特定の領域に対する適切な制御を、これらのアカウントに割り当てることができます。

管理代行のためのネームスペースの構造化

該当の事業所に特有の分割管理責任を実行できるような、別個の領域、または事業所を入れておくオブジェクト・スペースを構造化します。

以下の例では、オブジェクト・スペースの Engineering と Publications 領域が、別々の管理制御を必要としています。これらの領域の制御は、各領域のルートから始まり、以下のすべてのオブジェクトにまで拡張されます。



デフォルトの管理ユーザーおよびグループの使用

Policy Director は、重要な管理グループをいくつか作成します。デフォルトにより、これらのユーザー、グループ、またはその両方には、セキュア・ドメインにあるすべてのオペレーションを制御し、管理するための特別な許可が与えられます。このデフォルトのセキュリティー・ポリシーは、インストール時に作成される ACL によって定義されます。

次に、インストール時にこれらのユーザーおよびグループにそれぞれ割り当てられる特定の役割を詳しく説明します。管理者は、これらの特権をあとでカスタマイズして、管理ポリシーの変更に合わせることができます。

ユーザー cell_admin

このユーザーは、セキュア・ドメインで行われるすべてのオペレーションに対する完全な権利を付与されている、セキュア・ドメインの管理者を表しています。

このポリシーは、オブジェクト・スペースが大きくなったときに変更できます。管理許可を他のユーザーに委任することによって、このポリシーを変更することがで

きます。あるいは、cell_admin からの特定の (あるいはすべての) 許可を取り消すことによって、ポリシーを変更することもできます。

グループ iv-admin

このグループは、管理者グループを表します。cell_admin と同様に、このグループのメンバーはすべて、デフォルト・ポリシーによってセキュア・ドメインの管理者であるとみなされます。デフォルトの ACL はすべて、ユーザーの cell_admin とグループ iv-admin に、まったく同じ許可を付与します。

ユーザーを iv-admin グループに加えることによって、容易にユーザーを管理者の役割に入れることができます。このプロシージャーには、なんらかの危険があることに注意してください。ユーザーがこのグループのメンバーになると、そのユーザーは、この時点からデフォルトの ACL を持つことになります。デフォルトの ACL があると、ユーザーは、ネームスペース全体で、どのオブジェクトに対してもすべてのことを行う全権を持つことになります。

このグループのデフォルト・ポリシーは、変更することができます。たとえば、管理許可を他のユーザーに代行委任することによって、デフォルト・ポリシーを変更することができます。あるいは、iv-admin から一部の管理許可あるいはすべての管理許可を取り消すことによって、デフォルト・ポリシーを変更することができます。

グループ ivmgrd-servers

このグループには、管理サーバーが含まれます。Policy Director は、現在、セキュア・ドメインに 1 つの管理サーバーが存在していることが必要です。したがって、このグループには、その 1 つの項目があるだけです。

コンソールから出されるほとんどの管理要求は、ターゲットの Policy Director サーバーに対する管理サーバーを用いて、実行されます。この処理のために、管理サーバーは、ターゲット・サーバーで要求を実行する許可を持っている必要があります。このような理由から、このグループには、デフォルト管理 ACL でのサーバー管理許可 (s) と、Web スペース全体のリスト (l) 許可が付与されます。

グループ webseal-servers

このグループには、セキュア・ドメインにあるすべての WebSEAL サーバーが含まれます。デフォルトの WebSEAL ACL は、これらのサーバーに、HTTP 特有の許可の完全なセットと、代行許可を付与します。このポリシーを使って、すべての WebSEAL サーバーは、他のすべての WebSEAL サーバーに接合することができます。このポリシーを修正すると、サーバーごとのベースでこれらの許可を付与することができます。

管理ユーザーの作成

Policy Director を使用して、責任の度合いの異なる管理アカウントを作成することができます。責任は、戦略的に管理 ACL を置くことによって、管理者に代行委任されます。以下のリストは、管理の役割として考えられるものを示したものです。

ACL 管理の責任

ACL 管理者は、管理 ACL が置かれている場所に応じて、保護オブジェクトのネームスペース領域のすべて、または一部を制御することができます。 管

理者の ACL 項目には、b、a、および T の許可、さらにまた、その領域にあるオブジェクトへのオペレーションにとって適切なその他の許可を加えたものを含めることができます。

管理者は、管理コンソールを使って、指定のネームスペースにあるオブジェクトに ACL を接続することができます。管理者は、ACL テンプレートの既存のセットを使用することができます。付加 (a) 許可を使用して、ACL が付加されます。この管理者は、ACL テンプレートを作成、変更、または削除する許可を持っていません。

ACL ポリシーの責任

ACL ポリシー管理者には、セキュア・ドメインで使用されるすべての ACL テンプレートの作成と修正を制御する責任があります。 ACL ポリシー管理者には、/Management または /Management/ACL オブジェクトでの d、b、m、および v 許可が付与されている必要があります。

この ACL ポリシー管理者は、(m) 許可を用いて新しい ACL テンプレートを作成することができます。新しいテンプレートの作成者として、管理者は、デフォルトにより、abcT 許可を持つ、新しい ACL テンプレートの中の最初の項目になります。制御 (c) 許可は、実質的に、ACL の所有権およびそれにしたがって ACL を変更する権限を、管理者に与えます。

ACL の所有者として、管理者は、管理 ACL で付与されている削除 (d) 許可を使用することができます。 管理者は、この許可を用いて、テンプレートのリストから ACL を除去します。 その ACL の所有者でない限り、ACL テンプレートを削除することはできません。

サーバー管理の責任

この管理者には、/Management/Server オブジェクトに関する d、m、s、および v 許可が付与されます。この管理者は、Policy Director サーバーに関係するオペレーションを実行することができます。

許可アクションの責任

この管理者には、/Management/Action オブジェクトで (d) および (m) 許可が付与されます。この管理者は、第三者のアプリケーション用に作成されるすべての許可を作成または削除することができます。

管理ネームスペースについての詳細は、96ページの『管理ネームスペース』を参照してください。

管理 ACL テンプレートの例

次の例では、管理権限をユーザーが取得する方法を示します。

- 以下の /WebSEAL の ACL は、`user adam` に管理権を与えるものです。

```
user cell_admin                 abcTdmlrx
group iv-admin                  abcTdmlrx
group webseal-servers           gTdmlrx
group ivmgrd-servers            Tl
user adam                       abcTdmlrx
any-authenticated               Trx
unauthenticated                 Trx
```

- 以下の /NetSEAL の ACL は、user adam に管理権を与えるものです

```
user cell_admin                    abcTC
group iv-admin                     abcTC
user adam                          abcTC
any-authenticated                  TC
unauthenticated                    TC
```

管理の代行の例

大きなオブジェクト・スペースでは、様々なサブブランチを管理するために多くの管理ユーザーが必要になります。この場合、これらの各ブランチへのパス上にあるディレクトリーの ACL に、各アカウントごとに、トラバース許可を持つ項目を含める必要があります。 多くの管理ユーザーのいるサイトでは、 ACL には、これらの管理アカウントをすべて表す項目の長いリストが含まれることになります。

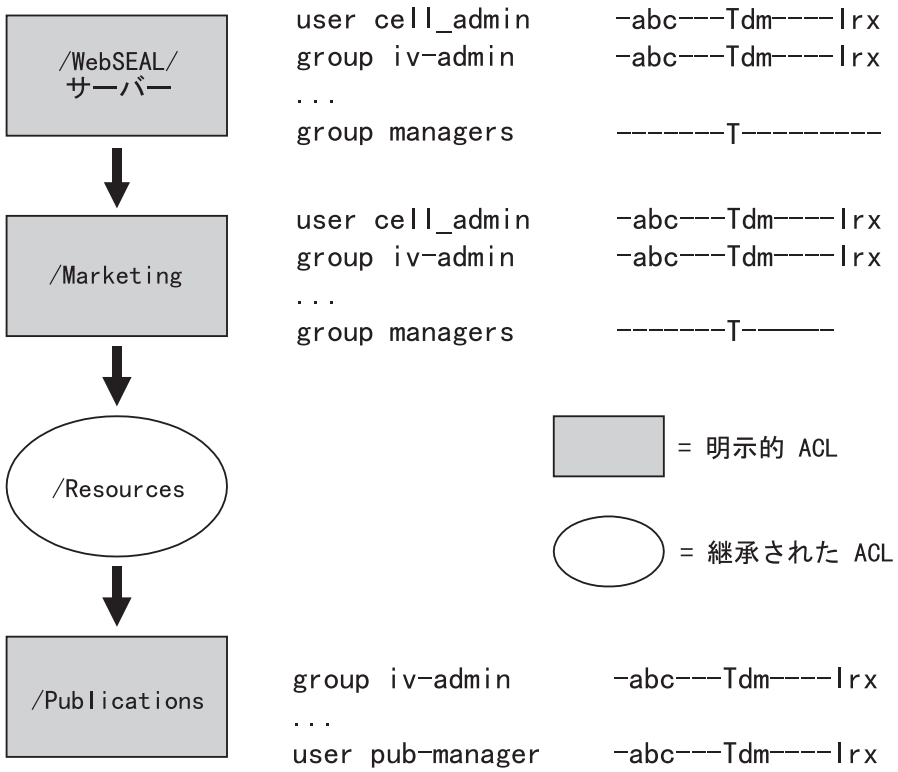
以下の手法を使うと、管理者用の多数の ACL 項目の問題が解決されます。

1. 管理者グループのアカウントを作成する。
2. 新しいすべての管理ユーザーをこのグループに追加する。
3. このグループを ACL 項目 (トラバース許可を持つ) として、それぞれのサブブランチを持ち、管理の代行を必要としているディレクトリーに追加する。
4. それぞれのブランチ・ルート ACL で、適切な管理ユーザー項目 (b、c、T、およびその他の適切な許可を持つもの) を追加する。
5. これで、管理者は、管理グループの ACL 項目 (およびその他の項目) をルートから除去できるようになります。

   これで、ユーザーはルートとその下にあるすべてのオブジェクトに対する制御を持つことができます。

以下の例では、すべての管理ユーザーを含むように managers グループが作成されています。ユーザー pub-manager は、このグループのメンバーなので、 Publications ディレクトリーにナビゲートするのに必要なトラバース許可を持っています。

Publications ディレクトリーには、その ACL に、ユーザー pub-manager の項目が含まれています。pub-manager は、このブランチの代行管理者であり、適切な許可を持っています。代行管理者として、 pub-manager は、Publications ACL から manager グループ・アカウント (およびその他の ACL 項目) を除去することができます。グループ・アカウントおよびその他の ACL 項目を除去することによって、代行管理者は、Web スペースのそのブランチに対する総合的な制御を取得します。


/WebSEAL/
サーバー
user cell_admin -abc---Tdm----lrx
group iv-admin -abc---Tdm----lrx
...
group managers -------T---------
/Marketing
user cell_admin -abc---Tdm----lrx
group iv-admin -abc---Tdm----lrx
...
group managers -------T-------
/Resources
= 明示的 ACL
= 継承された ACL
/Publications
group iv-admin -abc---Tdm----lrx
...
user pub-manager -abc---Tdm----lrx

第8章 アクセス制御の適用

セキュア・ドメインでは、ポリシー・テンプレートを使用することによって、リソースを保護することができます。ポリシー・テンプレートには、リソースの使用を制御する許可が含まれています。保護を必要とするリソースのネームスペース・オブジェクト表現に対して、ポリシー・テンプレートを付加する必要があります。

Policy Director は、ACL と呼ばれるポリシー・テンプレート・タイプを認識し、使用します。ACL は、セキュア・ドメインに属するリソースに、組織のセキュリティー・ポリシーをスタンプしておくために使用されます。

本章では、オブジェクト・スペースを管理し、アクセス制御を適用するために必要な共通のタスクについて説明します。

この章は、次の各節に分かれています。

ACL 管理の概要

管理コンソールの ACL 管理タスク・パネルを用いて、ACL テンプレートを作成、変更、および削除します。

1. ACL 管理の管理者として (`cell_admin` など)、管理コンソールにログインする。
2. **ACL** タスク・タブをクリックする。

   ACL 管理タスク・パネルが表示されます。

ACL 管理タスクのアクション・ボタン

ACL アクション・ボタンを使用して、ACL 管理オペレーションを実行します。 以下の表で、各アクション・ボタンの機能を説明します。

アクション・ボタン	説明
New ACL	新しい ACL テンプレートを作成します。
New Entry	選択された ACL テンプレートに新しい項目を追加します。
Save	この ACL テンプレートを保管します。ACL は、ACL Name リストのビューに表示されます。
Delete	選択された ACL テンプレートを削除します。
Get	特別に指定された ACL テンプレートについての情報を検索し、ACL 詳細ビューに置きます。ACL 定義セクションの ACL Name フィールドで ACL を指定します。
List	list ビューをリフレッシュします。
Where Used	選択された ACL テンプレートが接続される保護オブジェクトの完全なリストを表示します。この表示は、コンソールの Bulletin Board セクションに表示されます。

ACL 管理タスク

以下の ACL 管理オペレーションを実行することができます。

- 新しい ACL テンプレートの作成。
- ACL 項目の追加。
- ACL 項目の許可の編集。
- ACL テンプレートの削除。

新しい ACL テンプレートの作成

新しい ACL テンプレートを作成するとき、既存のデフォルトの ACL テンプレートの 1 つを用いて開始し、その ACL をユーザーの指定に変更することができます。

1. **ACL Name** リストから、使用したいデフォルトの ACL テンプレートのアイコンをドラッグします。 そのあと、新しい ACL を Bulletin Board に入れるための基礎として、このテンプレートを使用することができます。
2. ACL アクション・ボタンから、**New ACL** をクリックします。

   ACL 定義域にある以前の情報が消去され、新しい項目用のフィールドが用意されます。

   デフォルトにより、ユーザーがログインした識別子が、最初の ACL 項目 (abcT 許可を持つ) になります。 制御 (c) 許可は、ユーザーに、この ACL に対する所有権を与えます。
3. ACL の名前を **ACL Name** フィールドにタイプします。
4. **Description** フィールドにタブを合わせ、この ACL の目的を記述するフレーズ (これを適用する目的や方法について) を入力します。
5. Bulletin Board にあるデフォルトの **ACL** アイコンを、新しい ACL 定義の ACL 項目域にドラッグします。

   これで、新しい ACL には、デフォルトの ACL からの項目が入ることになります。
6. 項目に適当な修正を加えます。
7. **Save** をクリックします。

ACL 項目の追加

ACL 項目を追加するときは、次のようにします。

1. **ACL Name** リストから、ACL テンプレートを選択します。
2. **New Entry** アクション・ボタンをクリックします。

   ACL Entry 域がクリアされ、新しい項目用にリセットします。
3. マウス・ボタンで **Type** フィールドをクリックして、保留します。

   ドロップダウン・メニューが表示されます。
4. ユーザー、グループ、全認証、または非認証タイプを選択します。
5. **ID** フィールドをクリックして、適切な ID をタイプします。

   Accounts management ビューからユーザーおよびグループのアイコンをドラッグ・アンド・ドロップすることもできます。 **Accounts** タスク・タブをクリックして、 **Accounts management** ビューをコンソールの下部のパネル域に移動します。

6. 許可チェック・ボックスを使用して、適切な許可をこの項目に適用します。
7. **Save** ボタンをクリックして、項目を ACL にコミットします。

ACL 項目の許可の編集

ACL 項目の許可を編集するときは、次のようにします。

1. ACL 定義域で、項目を選択します。
2. ACL 項目域で、許可チェック・ボックスを選択するか、または選択しないで、適切な許可を選択します。
3. **Save** ボタンをクリックして、変更をコミットします。

ACL テンプレートの削除

ACL テンプレートを削除するときは、次のようにします。

1. **ACL Name** リストから、削除したい ACL テンプレートを選択します。
2. **Delete** ボタンをクリックします。

   警告ボックスが表示されます。
3. **Continue** をクリックします。

   管理コンソールは、オブジェクトにまだ接続されている ACL を削除しません。この状況を警告するメッセージが、ステータス・バーに表示されます。

例 :

`webtest` グループのメンバーのために設計された ACL を接続しました。 `webtest` グループは、新しい HTML ページの開発やテストをするグループです。テストのあとで、この明示的 ACL を除去して、セキュア・ドメインの他のメンバーがこのページを使用できるようにすることができます。

新しい ACL テンプレートを作成するためのサンプル・プロシージャー

新しい ACL テンプレートを作成するときは、

1. **New ACL** アクション・ボタンをクリックします。

   ACL 定義域にある以前の情報が消去され、新しい項目用のフィールドが用意されます。

   デフォルトにより、ユーザーがログインした識別子が、最初の ACL 項目 (abcT 許可を持つ) になります。
2. ACL の名前を **ACL Name** フィールドにタイプします。
3. **Description** フィールドにタブを合わせ、この ACL の目的を記述するフレーズ (これを適用する目的や方法について) を入力します。
4. **Save** ボタンをクリックして、この新しい ACL を ACL リストにコミットします。
5. **New Entry** ボタンをクリックします。

   ACL Entry 域がクリアされ、新しい項目用にリセットします。
6. マウス・ボタンで **Type** フィールドをクリックして、保留します。

   ドロップダウン・メニューが表示されます。
7. **unauthenticated** をクリックして、許可を付与しません。

8. **Save** ボタンをクリックします。

   ACL 定義域に項目が表示されます。
9. 同じプロシージャーを行って、許可を持たない全認証項目を追加します。
10. **Accounts** タスク・タブをクリックします。

    Accounts 管理パネルが、トップ・パネルとして表示されます。
11. **Move Task Down** ボタンをクリックして、 Accounts 管理パネルをコンソールの下の部分に置きます。
12. 新しいグループ項目を作成するときは、 **New Entry** (ACL パネル) をクリックします。
13. Accounts パネルの **Groups** リストから、 **group** アイコンを ACL Entry 域の **ID** フィールドにドラッグ・アンド・ドロップします。

    Type および **ID** フィールドは、適切な情報で満たされます。
14. 許可が適切かチェックします。
15. **Save** ボタンをクリックして、この項目を ACL にコミットします。

オブジェクト・スペース管理の概要

管理コンソールのオブジェクト・スペース管理のタスク・パネルを使用して、 ACL をオブジェクトに接続したり、オブジェクトから ACL を除去することができます。

1. ACL 管理許可を持つユーザーとして (`cell_admin` など)、管理コンソールにログインします。
2. **Object Space** のタスク・タブを、クリックします。

   Object Space management task パネルが表示されます。

オブジェクト・スペース管理タスクのアクション・ボタン

オブジェクト・スペース管理オペレーションを実行するときは、 **Object Space** アクション・ボタンを使用します。以下の表で、各アクション・ボタンの機能を説明します。

アクション・ボタン	説明
Attach ACL	ACL をオブジェクトに割り当てます。
Remove ACL	ACL をオブジェクトから除去します。
Find ACL	特定の ACL で明示的にマークを付けたすべてのオブジェクトを検索します。コンソールの下部のパネルにオブジェクトがリストされます。
Save ACL	Edit ACL ビューを使用するときに、ACL に加えられた変更を保存する機能を提供します。
List	オブジェクト・スペース・ツリーをリフレッシュします。

オブジェクト・スペース管理タスク

以下のオブジェクト・スペース管理オペレーションを実行することができます。

- ACL をオブジェクトに付加します。
- 明示的 ACL をオブジェクトから除去します。

オブジェクトへの ACL の付加

ユーザーは、ACL の付加および除去のための適切な管理許可を持っている必要があります。特に、ACL をオブジェクトに適用したり、ACL をオブジェクトから除去したりするための付加 (a) 許可を持っている必要があります。

1. ACL 管理タスク・パネルをコンソールの下部のセクションに置きます。
2. コンソールの上部パネルで Object Space パネルをクリックします。
3. オブジェクト・スペース・ツリーの該当する領域を拡張し、明示的 ACL が付加される場所のターゲット・オブジェクトを選択します。
4. **ACL Name** リストから適切な ACL テンプレートのアイコンをドラッグし、オブジェクト・スペース・ツリーの中の選択されたオブジェクトの上にドロップします。

オブジェクトからの明示的 ACL の除去

ユーザーは、ACL の付加および除去のための適切な管理許可を持っている必要があります。特に、ACL をオブジェクトに適用したり、ACL をオブジェクトから除去したりするための付加 (a) 許可を持っている必要があります。

1. **Object Space** のタスク・タブを、クリックします。
2. オブジェクト・スペース・ツリーの該当する領域を拡張し、付加された明示的 ACL を持つターゲット・オブジェクトを選択します。
3. **Remove ACL** ボタンをクリックします。

第9章 プロキシー・ユーザーの管理

セキュリティー・プロダクトに関する IBM SecureWay FirstSecure (FirstSecure) セットの 1 つに、 IBM SecureWay Boundary Server for Windows NT and AIX (Boundary Server) があります。 LDAP がデフォルトのユーザー・レジストリーである場合、Policy Director を Boundary Server と一緒に、統合 IBM Firewall および Policy Director のプロキシー・ユーザー・ソリューション用に使用することができます。

FirstSecure およびその構成要素についての最新情報が、以下の Web サイトにあります。

http: //www.ibm.com/software/security/firstsecure/library

境界セキュリティーの紹介

Policy Director と同様、Boundary Server は、 IBM SecureWay FirstSecure プロダクト・セキュリティー・パッケージと一緒に提供される構成要素の 1 つです。あるいは、Boundary Server または Policy Director を個別に購入して、あとでこれらを独立したプロダクト (完全な FirstSecure パッケージを購入せずに) として、実行することができます。

境界セキュリティーは、使用しているネットワーク、アプリケーション、情報などを保護するだけではなく、それらの有効範囲も広げます。境界セキュリティーを適切に使用するためには、そのネットワークにアクセスできる人、ネットワークに出入りする情報の両方を制御する必要があります。 Boundary Server は、ファイアウォール保護、コンテンツ・セキュリティー、および VPN を提供します。Boundary Server は、インターネットに対する境界を作成して、侵入の可能性のあるウィルスや、Java スクリプト、applets、 ActiveX コントロール、ジャンク e-mail (SPAM) などをブロックするために使用することができます。

Boundary Server の計画、インストール、構成、使用、およびトラブルシューティングの方法についての詳細は、IBM SecureWay Boundary Server プロダクトと一緒に提供される *IBM SecureWay Boundary Server Up and Running* を参照してください。

Boundary Server は、プロダクトのパッケージです。Boundary Server は、セキュリティー産業の最良の品質のテクノロジーを統合ソリューションに組み込んでいます。このソリューションには、IBM サポートおよびサービスが含まれており、任意に購入することができます。

Boundary Server の構成要素の 1 つに IBM SecureWay Firewall バージョン 4.1 (Firewall) があります。

IBM Firewall との統合

ファイアウォール の目的は、セキュア・ネットワークの中または外への、好ましくないまたは無許可の通信を防止することです。ファイアウォールは、1 つまたは複数のセキュアな内部私設ネットワークと、他の (セキュアでない) ネットワークまたは公衆インターネットとの間を封鎖するものとして働きます。

IBM Firewall は、ネットワーク・セキュリティー・プログラムです。 IBM SecureWay Firewall バージョン 4.1 には、以下の新しい機能が含まれています。

- セキュア・メールのプロキシーの拡張
- Socks Protocol、バージョン 5 の拡張
- Remote Access Service (RAS)
- HTTP プロキシー

HTTP プロキシーは、SecureWay Firewall を通したブラウザーの要求、つまり、 Web のブラウズについては socks サーバーの必要性を排除する、という要求を処理します。ユーザーは、インターネットで情報をアクセスする際に、内部ネットワークのセキュリティーを危うくせずに、また、クライアントの環境が HTTP プロキシーをインプリメントしていなくても、有用な情報をアクセスすることができます。

SecureWay Firewall をインストールするときは、その前に必須の前提条件がインストールされ、構成されているか、確認する必要があります。 さらにまた、セキュア・インターフェースを定義し、セキュリティー・ポリシーを決定して設定し、ネットワーク・オブジェクトを定義する必要があります。 以下のような、主要なネットワーク・オブジェクトを定義する必要があります。

- ファイアウォールのセキュア・インターフェース
- ファイアウォールの非セキュア・インターフェース
- セキュア・ネットワーク
- 使用しているセキュア・ネットワーク上にある各サブネット
- 使用している Security Dynamics サーバーおよび Windows NT のドメイン・サーバーのためのホスト・ネットワーク・オブジェクト (該当する場合)

インストールと構成情報に関する詳細については、 *IBM SecureWay Boundary Server Up and Running* を参照してください。この資料は、Boundary Server と一緒に提供されます。

ユーザーのタイプの記述

IBM Firewall の管理者は、プロキシー・ユーザーの定義の構成、作成、および変更について責任がありますが、他のファイアウォール管理者の定義を作成したり、修正することはできません。

ファイアウォール管理者は、以下のような管理用タスクを実行します。

- ユーザーが、自分の保護ネットワークの外にあるホストにアクセスできるように、ユーザーを IBM Firewall に追加する。
- ファイアウォールにアクセスするユーザーの属性を変更する。
- ネットワークの外にアクセスを必要としていないユーザーを削除する。

統合された IBM Firewall と Policy Director のソリューションの場合、プロキシー・ユーザーの管理を引き継ぐのは Policy Director 管理者です。

ファイアウォールのユーザー

セキュア・ネットワークのユーザーは、ネットワークのメカニズム (Socks やプロキシー、など) を使用することによって、非セキュア・ネットワークにアクセスするこ

とができます。セキュア・ユーザーが非セキュア・ネットワーク (プロキシー) を使用できるようにしたいときは、このタイプのトラフィックを許すような適正な接続を構成し、設定する必要があります。

どのサーバーに実行させるかは、プランニングの段階で行われた決定によって異なります。サービスを有効にすると、ある種の接続構成に特定のタイプのトラフィックを許すような設定が必要になることがよくあります。たとえば、自社のセキュア・ユーザーが、HTTP プロキシーを用いて、インターネット上の Web をサーフィンするのを許すとすれば、管理者は、 HTTP プロキシー・デーモンをファイアウォールに構成する必要があるばかりでなく、 HTTP トラフィックを許すような接続を設定することも必要になります。

アウトバウンドの Web アクセスのような機能の認証が必要になる場合は、それらのユーザーを IBM Firewall に定義してください。

プロキシー・ユーザー

Policy Director 管理者は、プロキシー・ユーザーを、Policy Director ユーザーの拡張として管理するように構成できます。統合された Policy Director と IBM Firewall ソリューションの場合、Policy Director 管理者は、ユーザーを Policy Director プロキシー・ユーザーとしてセットアップする必要があります。

プロキシー・ユーザーは、HTTP プロキシー・サービスなどの、ファイアウォール・サービスを使用して、企業内のネットワークからインターネットの Web サイトにアクセスする人です。プロキシー・ユーザーは、ファイアウォールを用いてサービスを使用できますが、ファイアウォール・マシンへのアクセスは持っていないので、ファイアウォール・マシンへのローカル・ログインを実行することはできません。

プロキシー・ユーザー管理の使用可能化

プロキシー・ユーザー管理を進行させるためには、前もって管理コンソールでこの機能を使用可能化しておく必要があります。プロキシー・ユーザー機能を使用可能化するには、console.properties ファイルを編集する必要があります。

console.properties ファイルは、以下のところにあります。

Windows: `C:¥Program Files¥IBM¥IVConsole¥console.properties`

UNIX: `/opt/intraverse/ivconsole/console.properties`

プロキシー・ユーザー管理を設定するには、以下のようにします。

1. テキスト・エディターを使用して、console.properties ファイルをオープンします。
2. 以下の行の先頭から、注釈シンボル (#) を除去します。

   ```
   #6, ProxyUsersTaskView              = IV.ProxyUserTask.ProxyUsersTaskView
   ```

3. 管理コンソールを再始動して、プロキシー・ユーザー管理機能を使用可能にします。

プロキシー・ユーザー管理の概要

Policy Director の場合、ファイアウォール・ユーザーは、*プロキシー・ユーザー* と呼ばれます。Policy Director の管理コンソールを用いて、管理者はプロキシー・ユーザーを管理することができます。

Policy Director の管理者は、以下のような管理用タスクを実行します。

- ファイアウォール・サービスを使用できるように、プロキシー・ユーザーとして、ユーザーを追加する。
- ファイアウォール・サービスを使用するプロキシー・ユーザーの属性を変更する。
- ファイアウォール・サービスを使用する必要がなくなったプロキシー・ユーザーを削除する。

このような管理タスクの実行方法の詳細について、ファイアウォール管理者は、 IBM Firewall 関係資料を参照してください。

プロキシー・ユーザー管理パネルの使用

Users 管理タスク・パネルには、**Users** のツリーのビューと、**Proxy User** の詳細ビューが収められています。

プロキシー・ユーザー管理タスクのアクション・ボタンの使用

プロキシー・ユーザーの管理オペレーションを実行するために、 **Proxy User** アクション・ボタンを使用します。以下の表で、各アクション・ボタンの機能を説明します。

アクション・ボタン	説明
Save	Policy Director ユーザーが、ユーザー・ツリー・ビューで選択されている場合には、新しいプロキシー・ユーザーを作成します。既存のプロキシー・ユーザーが、ユーザー・ツリー・ビューで選択されている場合には、既存のプロキシー・ユーザーを変更します。
Delete	選択したプロキシー・ユーザーを除去します。

プロキシー・ユーザーの詳細フィールドの使用

以下の表では、管理コンソール上の **Proxy User Detail** ビューにあるフィールドを説明します。

フィールド	説明
Proxy User	プロキシー・アクセスのために定義されているユーザーに対して指定される名前。これは、IBM Firewall にある TELNET または FTP サーバーにこのユーザーがログインするときに使うユーザー名。このユーザーは、管理者権限を持っていません。
Proxy Domain	ファイアウォール・プロキシー・ドメインの名前を指定します。
Password	ファイアウォール・プロキシー・ドメインにログインするときに使用するパスワードを指定します。

Description	プロキシー・ユーザーについて記述するテキスト・ストリングを指定します。この記述は、単なる任意選択のデータ・フィールドであって、レジストリーでは使用されません。
Remote Shell	リモート・ログイン・シェルがプロキシー・ユーザーのために使用されるように指定します。選択のリストには、**/bin/restrict.sh**、 **/bin/csh**、**/bin/ksh** **/bin/bsh**、 **/bin/oneact.sh**、および空ストリングが含まれます。
Local Shell	ローカル・ログイン・シェルがプロキシー・ユーザーのために使用されるように指定します。 選択のリストには、**/bin/restrict.sh**、 **/bin/csh**、**/bin/ksh** **/bin/bsh**、 **/bin/oneact.sh**、および空ストリングが含まれます。
Default Group	プロキシー・ユーザーが所属するデフォルト・グループを指定します。管理者は、表示されたグループのリストから、プロキシー・ユーザーがメンバーになっているグループを選択できます。
Secure FTP Authentication	セキュア・ネットワークからファイアウォールにアクセスするために FTP を使用する際に、このユーザーに必要となる認証のレベルを指定します。選択のリストには、**Firewall Password**、**Permit All**、**Deny All**、**SecurID Card**、**NT Logon Password**、 **User-Supplied 1**、**User-Supplied 2**、 **User-Supplied 3**、**AIX Logon Password**、および空ストリングが含まれます。
Remote FTP Authentication	非セキュア・ネットワークからファイアウォールにアクセスするために FTP を使用する際に、このユーザーに必要となる認証のレベルを指定します。選択のリストには、**Firewall Password**、**Permit All**、 **Deny All**、**SecurID Card**、**NT Logon Password**、 **User-Supplied 1**、**User-Supplied 2**、 **User-Supplied 3**、**AIX Logon Password**、および空ストリングが含まれます。
Secure Telnet Authentication	セキュア・ネットワークからログインするときに、このユーザーの識別子を何らかの方法で認証する必要があることを示します。選択のリストには、**Firewall Password**、**Permit All**、 **Deny All**、**SecurID Card**、**NT Logon Password**、**User-Supplied 1**、**User-Supplied 2**、**User-Supplied 3**、**AIX Logon Password**、および空ストリングが含まれます。

Remote Telnet Authentication	非セキュア・ネットワークからログインするときに、このユーザーの識別子を何らかの方法で認証する必要があることを示します。 選択のリストには、**Firewall Password**、**Permit All**、 **Deny All**、**SecurID Card**、**NT Logon Password**、**User-Supplied 1**、**User-Supplied 2**、**User-Supplied 3**、**AIX Logon Password**、および空ストリングが含まれます。
Secure SOCK Authentication	ファイアウォールのセキュア側から入る Socks クライアント接続のための、 Socks、バージョン 5、認証方式を指定します。選択のリストには、**Firewall Password**、**Permit All**、 **Deny All**、**SecurID Card**、**NT Logon Password**、 **User-Supplied 1**、**User-Supplied 2**、 **User-Supplied 3**、**AIX Logon Password**、および空ストリングが含まれます。
Remote SOCK Authentication	ファイアウォールの非セキュア側から入る Socks クライアント接続のために、 Socks バージョン 5 認証方式を指定します。 選択のリストには、**Firewall Password**、**Permit All**、 **Deny All**、**SecurID Card**、**NT Logon Password**、 **User-Supplied 1**、**User-Supplied 2**、 **User-Supplied 3**、**AIX Logon Password**、および空ストリングが含まれます。
Secure HTTP Authentication	アウトバウンドの HTTP プロキシー要求で、ユーザー ID とパスワードが対になったタイプの認証を指定します。選択のリストには、**Firewall Password**、**Permit All**、 **Deny All**、**SecurID Card**、**NT Logon Password**、 **User-Supplied 1**、**User-Supplied 2**、 **User-Supplied 3**、**AIX Logon Password**、および空ストリングが含まれます。
Local Authentication	ローカル認証方式を指定します。選択のリストには、**Firewall Password**、**Permit All**、 **Deny All**、**SecurID Card**、**NT Logon Password**、**User-Supplied 1**、**User-Supplied 2**、**User-Supplied 3**、**AIX Logon Password**、および空ストリングが含まれます。
Idle Disconnect Time	使用されているものが切断される前に許されるアイドル時間を指定します。
Warning Disconnect Time	切断される前にユーザーに許される警告時間の長さを指定します。
Password Valid	ユーザーにプロンプトを出して、正しいパスワードを入力するよう、ユーザーに要求するかどうか、指定します。 IBM Firewall は、このユーザーのパスワードを要求するプロンプトを出します。
Password Locked	パスワードをロックするかどうか指定します。管理者は、このフィールドを yes に設定して、ユーザーがパスワードの認証を使用できないようにします。

プロキシー・ユーザーの追加

プロキシー・ユーザーを作成するときは、次のようにします。

1. **Proxy User** タスク・タブをクリックします。
2. **Users** ツリーの該当する領域を拡張し、プロキシー・ユーザーにしたい Policy Director ユーザーを選択します。
3. **Proxy User Detail** ビューにあるフィールドに記入します。
4. **Save** ボタンをクリックします。

プロキシー・ユーザー情報の変更

プロキシー・ユーザー情報を変更するときは、次のようにします。

1. **Proxy User** タスク・タブをクリックします。
2. **Users** ツリー・ビューの該当する領域を拡張して、リストから既存のプロキシー・ユーザーを選択します。

   Proxy User Detail 域には、現在のデータが入っています。
3. 新しいデータを入力します。
4. **Save** ボタンをクリックします。

プロキシー・ユーザーの除去

プロキシー・ユーザーを削除するときは、次のようにします。

1. **Proxy User** タスク・タブをクリックします。
2. **Users** ツリー・ビューの該当する領域を拡張して、既存のプロキシー・ユーザーを選択します。
3. **Delete** ボタンをクリックします。

プロキシー・ユーザー管理のための ivadmin policy コマンドの使用

Policy Director のプロキシー・ユーザーに関してだけ使用される特定の **ivadmin policy** コマンドがあります。 **ivadmin policy** コマンドは、Policy Director ユーザーとプロキシー・ユーザーに対する汎用のポリシー情報を制御する管理コマンドのセットです。 管理者は、以下のようなポリシー属性を管理することができます。

- 『ログイン・ポリシーの管理』
- 126ページの『パスワード・ポリシーの管理』

ポリシーは、システムの全体的なセキュリティーを改善するために、ユーザー・アカウントとパスワードに課せられた制約のセットを定義します。これらの制約は、一般的に (システムにあるすべてのユーザーにグローバルに)、あるいは特別に (指定されたユーザーに対してだけ) 課せられます。ユーザーに、特定のポリシーが適用される場合は、この特定のポリシーが、定義される可能性があるどの汎用ポリシーよりも優先します。汎用ポリシーに比べて、この特定のポリシーが制約が多くても少なくても、この優先順位が適用されます。

ログイン・ポリシーの管理

IBM SecureWay Boundary Server 管理者は、以下の **ivadmin policy** コマンドを使用して、ログイン関連のポリシーを管理することができます。

ログイン関連の **policy** 管理タスク・コマンドを使用して、新しいログイン・ポリシーを作成します。これらのポリシーは、すべてのユーザーに適用されます。

ログイン関連のポリシーの場合、Policy Director は、**policy** 管理タスク・コマンドを参照するとき、相対時間は DDD-hh:mm:ss として、また絶対時間は YYYY-MM-DD-hh:mm:ss として定義します。

コマンド	説明
policy {set | get} disable-time-interval [*number*]	

	ログイン試行の失敗の最大数に達したあと、アカウントをどれだけの時間 (秒数で) 禁止すべきかを指定します。
	
	number 引き数は、アカウントを禁止すべき秒数です。
	
	例 :
	`ivadmin> policy set disable-time-interval 3`
	
	または、
	`ivadmin> policy get disable-time-interval`

policy {set | get} max-login-failures [*number*]	

	ログイン試行で失敗が許される最大の回数の新しいポリシーを作成するか、または既存のポリシーを表示します。 *number* 引き数は、ログイン試行で失敗が許される最大の回数です。
	
	例 :
	`ivadmin> policy set max-login-failures 5`
	
	または、
	`ivadmin> policy get max-login-failures`

パスワード・ポリシーの管理

IBM SecureWay Boundary Server 管理者は、以下の **ivadmin policy** コマンドを使用して、パスワードのポリシーを管理することができます。

パスワード関連のポリシーの場合、Policy Director は、**policy** 管理タスク・コマンドを参照するとき、相対時間を DDD-hh:mm:ss として定義します。

コマンド	説明
policy {set | get} max-password-age [*relative-time*]	

	パスワードの変更が必要になる前の最大時間を制御するポリシーを管理します。 *relative-time* 引き数は、指定する時間であり、 `DDD-hh:mm:ss` という形式で、日、時刻、分を表します。
	
	例 :
	`ivadmin> policy set max-password-age 031-08:30:00`
	
	または、
	`ivadmin> policy get max-password-age`

policy {set | get} max-password-repeated-chars [*number*]	

	ユーザーのパスワードの中で連続して反復できる文字の最大数を指定します。
	
	例 :
	`ivadmin> policy set max-password-repeated-chars 3`
	
	この最高 3 文字の反復文字の例を使用した場合、パスワード `deptfff` は、3 個の “f” 反復文字を超えていないので、パスワードとして設定できます。パスワード `deptffff` は、“f” 文字が 4 個あって、3 個の反復文字という制限を超えているので、パスワードとして設定できません。
	
	または、
	`ivadmin> policy get max-password-repeated-chars`

policy {set | get} min-password-alphas [*number*]	

	ユーザーのパスワードで使用すべき英字の最小桁数を指定します。
	
	例 :
	`ivadmin> policy set min-password-alphas 5`
	
	この例の場合は、パスワードに最低 5 桁の英字が含まれている必要があります。
	
	または、
	`ivadmin> policy get min-password-alphas`

policy {set | get} min-password-non-alphas [*number*]	

	ユーザーのパスワードで使用すべき英字以外の文字の最小桁数を指定します。
	
	例 :
	`ivadmin> policy set min-password-non-alphas 1`
	
	この例の場合は、有効にするためには、パスワードに最低 1 桁の英字以外の文字が含まれている必要があります。
	
	または、
	`ivadmin> policy get min-password-non-alphas`

policy {set | get} min-password-different-chars [*number*]	

	ユーザーのパスワードで使用すべき異なる文字の最小桁数を指定します。
	
	例 :
	`ivadmin> policy set min-password-different-chars 3`
	
	この例の場合は、有効にするためには、パスワードに最低 3 個の異なる文字が含まれている必要があります。 指定されたパスワードが `ddddyyyy` であると、異なる文字が 2 個だけなので (d と y)、パスワードは有効になりません。
	
	または、
	`ivadmin> policy get min-password-different-chars`

policy {set | get} min-password-length [*number*]	

	パスワードの最小長を文字数で指定します。*number* 引き数は、パスワードの許容最小長です。
	
	例 :
	`ivadmin> policy set min-password-length 8`
	
	または、
	`ivadmin> policy get min-password-length`

policy {set | get} min-password-reuse-num [*number*]	

	あるパスワードを何回変更したら、以前に使用したパスワードが再び使用可能になるかを指定します。
	
	例 :
	`ivadmin> policy set min-password-reuse-num 3`
	
	または、
	`ivadmin> policy get min-password-reuse-num`

policy {set | get} min-password-reuse-time [*relative-time*]	

	パスワードを再使用できるようにするために、経過すべき最小の時間を指定します。
	
	relative-time 引き数は、最低の時間であり、 `DDD-hh:mm:ss` という形式で、日、時刻、分を表します。ユーザーは、指定された制限時間内に (たとえば、60 日すなわち `060-00:00:00`)、同じパスワードを再度使用することはできません。
	
	例 :
	`ivadmin> policy set min-password-reuse-time 060-00:00:00`
	
	または、
	`ivadmin> policy get min-password-reuse-time`

policy {set | get} password-expiry-date [*relative-time*]	

	パスワードの有効期限が切れる日時を指定します。
	
	例 :
	`ivadmin> policy set password-expiry-date 031-08:30:00`
	
	または、
	`ivadmin> policy get password-expiry-date`

policy {set | get} password-expiry-warn [*number*]	

	パスワードの有効期限が切れることをユーザーに警告します。 *number* 引き数は、満了日の何日前に警告を始めるか (たとえば、パスワードの有効期限が切れる 4 日前、など) という日数です。
	
	例 :
	`ivadmin> policy set password-expiry-warn 4`
	
	または、
	`ivadmin> policy get password-expiry-warn`

第10章 Policy Director サーバーの管理

本章では、Policy Director サーバーのセットを管理し、構成するための汎用タスクを取り上げます。また、それぞれのサーバーをサポートする構成ファイルについても、説明します。

この章は、次の各節に分かれています。

Policy Director サーバーの紹介

Policy Director サーバーは、次のようなサーバー・プロセス (デーモン) から構成されます。

- セキュリティー・サーバー (secd)
- セキュリティー・マネージャー (secmgrd)
- 許可サーバー (ivacld)
- 管理サーバー (ivmgrd)
- ディレクトリー・サービス・ブローカー (DSB)

これらのサーバーは、プロダクトのインストール時に自動的に構成されます。

Policy Director の**セキュリティー・サーバー (secd)** は DCE サーバーのみです。セキュリティー・サーバーは、認証サービスを提供します。また、セキュリティー・サーバーは、中央レジストリー・データベースを保守します。ユーザー・レジストリーは LDAP でも DCE でもかまいませんが、ユーザー・レジストリーが DCE の場合、この中央レジストリー・データベースには、セキュア・ドメインに参加しているすべての有効ユーザーのアカウント情報が含まれます。

セキュリティー・マネージャー (secmgrd) には、 WebSEAL および NetSEAL セキュリティー・マネージャーが含まれています。

Policy Director の **許可サーバー (ivacld)** は、 Policy Director の許可 API をリモート・モードで使用する第三者のアプリケーションからの許可要求にサービスを提供します。許可サーバーは、通常、管理や構成がほとんど要りません。

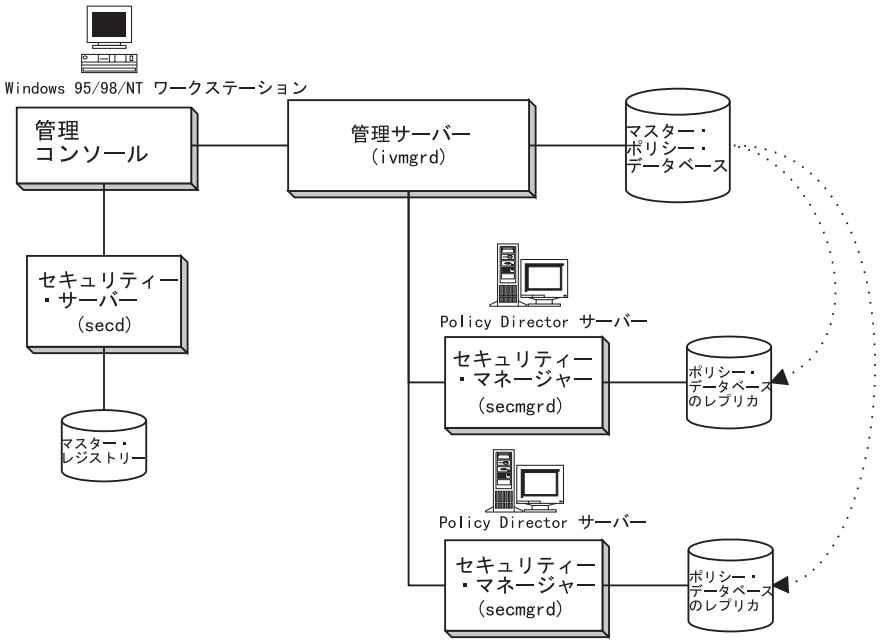
管理サーバー (ivmgrd) は、1 次 ACL データベースを管理し、セキュア・ドメインにある他の WebSEAL や NetSEAL サーバーに関する位置情報を保守します。管理サーバーは、通常、管理や構成がほとんど要りません。

ディレクトリー・サービス・ブローカー (DSB) は、管理サーバー (IVMgr) パッケージの一部として配布されます。管理コンソールは、Windows NT、Windows 95、または Windows 98 のワークステーションで実行されるとき、ディレクトリー・サービス・ブローカーがセキュア・ドメインに入っていることを必要とします。通常、ディレクトリー・サービス・ブローカーには、初期インストールのあとで、管理や構成をする必要はありません。

サーバーの依存関係

Policy Director サーバーの依存関係には、次のものが含まれます。

- どのセキュア・ドメインでも管理サーバーとその 1 次許可 (ACL) データベースのインスタンスは 1 つだけでなければなりません。
- 管理サーバーは、その ACL データベースを、セキュア・ドメインの他のすべての Policy Director サーバーに複製します。
- セキュリティー・マネージャーは、WebSEAL および NetSEAL トラップを持っており、すべての Policy Director サーバーに常駐しています。
- セキュリティー・マネージャーはそれぞれ、複製された許可、または ACL、データベースからの情報に基づくアクセス制御ポリシーを適用します。



サーバー管理ツールの概要

以下のインターフェースを介して、サーバー管理を実行することができます。

- **ivadmin** ユーティリティー
- **wandmgr** ユーティリティー (WebSEAL のみ)
- UNIX スクリプト
- Windows NT サービス制御パネル

この章では、これらの各インターフェースを用いる方法を説明します。

ivadmin、**wandmgr**、および始動スクリプトが、コマンド行インターフェースを提供します。これらは、シェル・スクリプト内のサーバー管理タスクを自動化するときに、便利です。

管理コンソール、ivadmin、および wandmgr はすべて、リモートでもローカルでも使用することができます。始動スクリプトは、ローカルに管理する必要があります。

問題を検出して訂正するとき、コマンド行ユーティリティーが個々のサーバーの状況情報を示し、制御を行います。

ivadmin ユーティリティー

Policy Director は、さらに高度なサーバー・タスクを実行するために、 **ivadmin** コマンド行ユーティリティーを提供します。 **ivadmin** は、次のような目的で使用します。

- 前のセクションにリストされているすべての管理コンソール・タスクを実行する。
- サーバーの状況を表示する。

wandmgr ユーティリティー

wandmgr コマンド行ユーティリティーは、以下のような高度の Web クライアント許可およびキャッシュ管理タスクを実行するために使用される Policy Director の WebSEAL ツールです。

- Web オブジェクトのキャッシュ状況を表示する。
- Web オブジェクトのキャッシュをメモリーから削除する。

UNIX スクリプト

Policy Director は、スクリプトを使用して、システム・ブート中にサーバーを自動的に停止 / 開始して、サーバーの状況を表示します。これらのスクリプトを次の目的で、手動で開始することができます。

- サーバーを停止する。
- サーバーの状況を表示する。
- サーバーを開始する。

Windows NT サービス制御パネル

Windows NT サービス制御パネルは、次の目的に使用されます。

- サーバーを開始する。
- サーバーを停止する。
- サーバーを一時停止 (サスペンド) する。
- 一時停止したサーバーを続行 (レジューム) する。
- 構成されたサーバーをリストする。

サーバー構成ファイル

Policy Director サーバーでは、構成ファイルを使用して、機能を指示します。

サーバー名	プロセス	構成ファイル
セキュリティー・マネージャー	secmgrd	**UNIX:** /opt/intraverse/secmgr/lib/secmgrd.conf **Windows:** ¥Program Files¥ibm¥Policy Director¥secmgr¥lib¥secmgrd.conf
管理サーバー	ivmgrd	**UNIX:** /opt/intraverse/ivmgrd/lib/ivmgrd.conf **Windows:** ¥Program Files¥ibm¥Policy Director¥ivmgrd¥lib¥ivmgrd.conf

許可サーバー	**ivacld**	**UNIX:** /opt/intraverse/ivacld/lib/ivacld.conf **Windows:** ¥Program Files¥ibm¥Policy Director¥ivacld¥lib¥ivacld.conf

構成ファイルは、情報交換用米国標準コード (ASCII) ベースで、共通エディターを使用して編集できます。ファイル項目の形式は、次のとおりです。

```
parameter=value
```

Policy Director サーバーの初期インストールでは、ほとんどのパラメーターにデフォルト値が設定されます。パラメーターには一部に静的で、決して変更できないものもありますが、それ以外は、調整したり追加したりして、サーバー機能の構成やパフォーマンスの最適化を行うことができます。

注: 構成ファイルの編集後は、Policy Director サーバーをいったん停止し、再始動してからでないと、変更は有効になりません。

各ファイルには、それぞれ**スタンザ**と呼ばれるセクションがあり、特定の構成カテゴリーに関する設定値が収められています。スタンザ・ラベルは、大括弧 [ ] に囲まれて表示されます。

たとえば、iv. conf ファイルの [intraverse] スタンザでは、セキュア・ドメイン全体に適用される一般的な Policy Director 構成設定値を定義します。スタンザ [wand-mime-types] では、ローカル・システム上で、 Policy Director WebSEAL によってサポートされる MIME タイプ定義を定義します。

ファイルには注釈が付き、各パラメーターの使用について説明しています。構成設定値を変更する必要がある場合は、ファイルを注意深く編集して、ファイルの整合性を確保します。

UNIX: Policy Director サーバーの停止と開始

サーバー・プロセスの開始と停止は、通常、システムの始動時とシャットダウン時に実行される、自動化されたスクリプトによって行われます。

また、管理者がスクリプトを使用して、サーバー・プロセスを手動で開始したり、停止したりすることもできます。この手法が役立つのは、インストールのカスタマイズ時や、問題の検出と訂正にあたる時です。なお、スクリプトを適用できるのは、ローカル・マシンの場合だけです。リモートでサーバーを停止したり、開始したりする場合は、管理コンソールや **ivadmin** ユーティリティーを使用します。

Policy Director サーバーは、開始と停止を全部同時に行うこともできるし、停止する場合は、一度に 1 つずつ個別に停止することもできます。一般的に、サーバーは、正しい順序で停止し、開始する必要があります。

NetSEAT クライアントに代わってセル・ディレクトリー・サービス (CDS) 要求を処理するには、ディレクトリー・サービス・ブローカーが必要です (Windows 版の管理コンソールでは、NetSEAT クライアントを使用します)。

iv スクリプトを使用して停止する

特定のマシン上のすべての Policy Director サーバーを正しい順序で停止する場合は、iv スクリプトを使用します。

AIX:

```
# /etc/iv/iv stop
```

Solaris:

```
# /etc/init.d/iv stop
```

このスクリプトが停止するのは、ivacld、secmgrd、ivmgrd の順だけに限られます。スクリプトは、すべてのサーバーが停止するのを待ってから、プロンプトを戻します。

手動シャットダウン

サーバーは、**kill** コマンドを使用して、個別に停止することもできます。

```
# kill <pid>          サーバーを強制的に終結シャットダウンする。
# kill -9 <pid>       終結処置なしに、サーバーを突然強制終了する。
```

Policy Director サーバーは、次の順序でシャットダウンします。

1. ディレクトリー・サービス・ブローカー (DSB)
2. 許可サーバー (ivacld)
3. セキュリティー・マネージャー (secmgrd)
4. 管理サーバー (ivmgrd)

iv スクリプトを使用して開始する

特定のマシン上のすべての Policy Director サーバーを正しい順序で開始する場合は、iv スクリプトを使用します。

AIX:

```
# /etc/iv/iv start
```

Solaris:

```
# /etc/init.d/iv start
```

このスクリプトが開始するのは、ivmgrd、secmgrd、ivacld の順だけに限られます。スクリプトは、すべてのサーバーが開始するのを待ってから、プロンプトを戻します。

手動始動

サーバーを直接開始することによって、サーバーを個別に手動で開始できます。サーバーは、それ自体で初期化します。これが正常に行われれば、サーバーは、それ自体でデーモン化します。

始動コマンドは、root や ivmgr など、管理ユーザーとして実行する必要があります。Policy Director サーバーは、次の順序で開始します。

1. 管理サーバー (ivmgrd):

   ```
   # /opt/intraverse/ivmgrd/bin/ivmgrd
   ```

2. セキュリティー・マネージャー (secmgrd):

   ```
   # /opt/intraverse/secmgr/bin/secmgrd
   ```

3. 許可サーバー (ivacld):

   ```
   # /opt/intraverse/ivacld/bin/ivacld
   ```

4. ディレクトリー・サービス・ブローカー (DSB):

   ```
   # /opt/intraverse/broker/bin/dsb
   ```

サーバー状況の表示

サーバーが稼働しているかどうかチェックする場合は、次のコマンドを使用します。

AIX:

```
# /etc/iv/iv status
```

Solaris:

```
# /etc/init.d/iv status
```

```
DCE サーバー :
サーバー                  使用可能                  稼働
dced                      yes                       yes
secd                      -                         yes
cdsd                      -                         yes
dtsd                      -                         yes
dsb                       -                         yes

Policy Director サーバー :
サーバー                  使用可能                  稼働
ivmgrd                    yes                       yes
secmgrd                   yes                       yes
ivacld                    yes                       yes
```

Windows: Policy Director サーバーの停止と開始

サーバー・プロセスを手動で開始したり、停止したりする場合は、 Windows NT サービス制御パネルを使用します。この方法が役立つのは、インストールのカスタマイズ時や、問題の検出と訂正にあたる時です。このユーティリティーを使用する場合は、管理特権が必要です。

Policy Director サーバーは、開始と停止を全部同時に行うこともできるし、停止する場合は、一度に 1 つずつ個別に停止することもできます。 一般的に、サーバーの開始と停止は正しい順序で行う必要があります。

システムを再始動 (リブート) すると、Policy Director AutoStart サービスによって、Policy Director サーバーのそれぞれが自動的に開始されます。サーバーが開始してしまうと、AutoStart サービスは終了します。

個々の Policy Director サーバーを手動で開始したり、停止したりする場合は、Windows NT サービス制御パネルを使用します。

1. Windows 制御パネルをオープンする。
2. **Services** アイコンをダブルクリックする。

「Services」ダイアログ・ボックスが表示されます。表示されるサービスには、次の例のようなものがあります。

```
Service                                    Status          Startup
Director Services Broker                   Started         Automatic
Policy Director Authorization Server       Started         Manual
Policy Director Auto-Start Service         Started         Automatic
Policy Director Management Server          Started         Manual
Policy Director Security Manager           Started         Manual
Policy Director X.509 Authorization Server Started         Manual
```

3. リスト・ボックスで、4 のステップと 5 のステップに示されている順序に従って、Policy Director サーバーを選択する。
4. 次の順序でサーバーを停止する。
   - セキュリティー・マネージャー
   - 管理サーバー
   - ディレクトリー・サービス・ブローカー
5. 次の順序でサーバーを開始する。
   - ディレクトリー・サービス・ブローカー
   - 管理サーバー
   - セキュリティー・マネージャー
   - 許可サーバー
6. ボックスの右側の該当する制御オプション・ボタン (**Start**、 **Stop**、**Startup**) をクリックする。
7. Policy Director サーバーが Policy Director AutoStart サービスによって自動的に始動することがないようにする場合は、**Startup** オプション・ボタンを使用する。このボタンをクリックすると、 Policy Director サーバーが Disabled (使用不可) に設定されます。

ブート時のサーバーの始動を自動化する

iv.conf 構成ファイルの [intraverse] スタンザには、サーバーの始動を自動化したり、自動化しないようにするパラメーターが入っています。

インストール時には、システムの再始動のたびに自動的に開始するように、セキュリティー・サーバー・デーモン (secmgrd) を構成できます。

```
[intraverse]
boot-start-secmgrd = yes
```

secmgrd が自動的に始動しないようにする場合は、次のように設定します。

```
boot-start-secmgrd = no
```

IVMgr パッケージをインストールすると、システムを再始動するたびに、 Policy Director 管理サーバー・デーモン (ivmgrd) が自動的に開始します。

```
[intraverse]
boot-start-ivmgrd = yes
```

ivmgrd が自動的に始動しないようにする場合は、次のように設定します。

```
boot-start-ivmgrd = no
```

注: 各セキュア・ドメイン (セル) が必要とする Policy Director 管理サーバー・デーモンは、それぞれ 1 つだけです。セル 1 つにつき複数のサーバーに **ivmgrd** をインストールしたり、実行したりすることがないようにします。

IVAcld パッケージをインストールすると、システムを再始動するたびに、 Policy Director 許可サーバー・デーモンが自動的に開始します。

```
[intraverse]
boot-start-ivacld = yes
```

ivacld が自動的に始動しないようにする場合は、次のように設定します。

```
boot-start-ivacld = no
```

RPC ワーカー・スレッドを構成する

構成されたワーカー・スレッドの数で、サーバーがサービスできる同時着信要求の数を指定します。 すべてのワーカー・スレッドが使用中であると、Policy Director では、到着する他の接続については、ワーカー・スレッドが使用可能になるまでバッファーに入れておきます。

着信接続にサービスできる使用可能スレッドの数を指定できます。ワーカー・スレッドの数はパフォーマンスに影響する可能性があるため、その構成は注意深く行う必要があります。

構成パラメーターが同時接続の数に上限を設けることはありません。これらのパラメーターで指定するのは、潜在的に無限の作業待ち行列にサービスするために使用可能にされるスレッドの数を指定するだけです。

ワーカー・スレッドの最適数の選択は、ネットワーク上のトラフィックの量とタイプについての理解度に左右されます。

スレッドの数を増やせば、要求処理の完了にかかる平均時間が短縮されることになります。ただし、スレッドの数を増やすと、サーバー・オーバーヘッドが増加するので、要求にサービスする平均時間が再び増えることになります。

サーバー secmgrd、ivmgrd、ivacld に関する構成ファイルのそれぞれには、 RPC ワーカー・スレッドを構成するための次のようなパラメーターが入っています。

- RPC ワーカー・スレッドの最大数
- 着信 RPC に関して listen するための TCP ポート
- 着信 RPC に関して listen するためのユーザー・データグラム・プロトコル (UDP) のポート

サーバー名	プロセス	構成ファイル
セキュリティー・マネージャー	**secmgrd**	secmgrd.conf
管理サーバー	**ivmgrd**	ivmgrd.conf
許可サーバー	**ivacld**	ivacld.conf

RPC ワーカー・スレッド・プールを設定する

Policy Director サーバーは、RPC ワーカー・スレッドを使用して、次のものを処理します。

- NetSEAT クライアントからの着信 RPC 要求
- 管理コンソールから実行される管理タスクによって生成されるデータベース更新

各サーバー構成ファイルに入っている最大 RPC ワーカー・スレッド数パラメーターには、次のデフォルト値が入っています。

```
max-rpc-worker-threads = 10
```

Policy Director サーバーが処理する NetSEAT クライアントの数が多いときは、この値を増やすことを考慮します。

着信 RPC 要求用としてサーバーを構成する

次の表には、それぞれのサーバーによる RPC listen 用のデフォルトのポート値が一覧表にしてあります。

サーバー	構成ファイル	ポート・パラメーターとそのデフォルト値
secmgrd	secmgrd.conf	`rpc-tcp-port = 6052 rpc-udp-port = 0`
ivmgrd	ivmgrd.conf	`tcp-rpc-port = 6032 udp-rpc-port = 0`
ivacld	ivacld.conf	`tcp-rpc-port = 6031 udp-rpc-port = 0`

ポート値がゼロ (0) の場合は、そのポートでの RPC listen は使用不可になります。TCP listen の使用をぜひお勧めします。UDP ポートを起動するのは、絶対に必要なときだけにします。

必要に応じて、さまざまなポートを設定できます。

secmgrd の例 :

```
rpc-udp-port = 6052
```

これで、TCP と UDP は同一のポート上で listen します。

第11章 許可サービスの管理

Policy Director 許可サービスは、許可決定プロセスを制御することによって、ネットワーク・セキュリティー・ポリシーを実施します。Policy Director 許可機能は、次のようにいくつかの方法で拡張できます。すなわち、追加のネームスペースの定義と取り込み、新規アクセス制御許可の定義、第三者 *外部許可サービス* への対処などの方法です。この章では、 Policy Director 許可サービスの構成、保守、拡張に必要なタスクについて説明します。

この章は、次の各節に分かれています。

第三者アプリケーション・ネームスペースを定義する

Policy Director セキュリティー・ポリシーは、次の要素で定義されます。

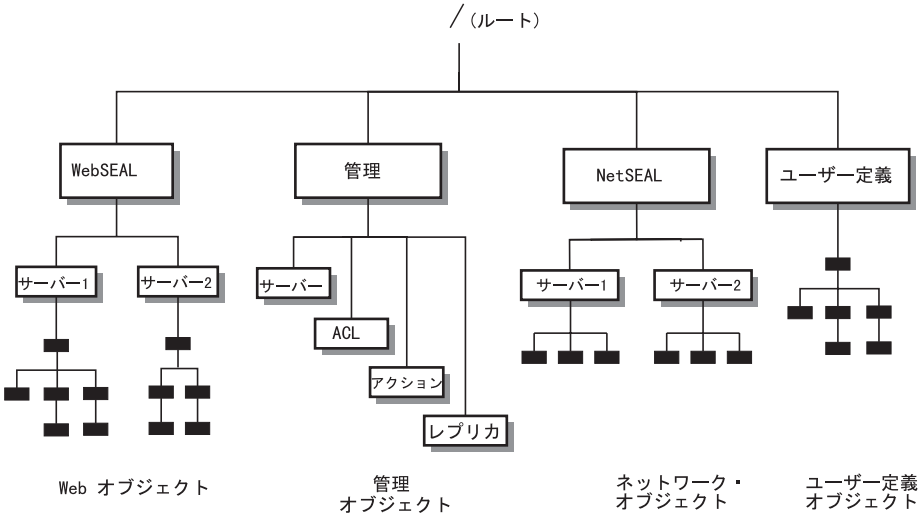
- セキュア・ドメインに参加を許されるのは?
- 保護の必要があるオブジェクトは?
- そのようなオブジェクトを保護する必要がある規則は?

Policy Director 保護オブジェクト・ネームスペースは、セキュア・ドメインに属するリソースの論理的で階層的な表示です。ネームスペース内のオブジェクトは、保護される対象であるシステム・リソース (ファイルやポートなど) を表します。セキュア・ドメイン内のリソースを保護するには、そのようなリソースのオブジェクト表示にポリシー・テンプレート (ACL) を付加します。

保護オブジェクト・ネームスペースでは、次の 2 つのタイプのオブジェクトを使用します。

コンテナー・オブジェクト
: コンテナー・オブジェクトは、ネームスペースを別々の機能領域に階層的に編成できる構造指定です。コンテナー・オブジェクトにリソース・オブジェクトが入ります。

リソース・オブジェクト
: リソース・オブジェクトは、セキュア・ドメイン内の実際のシステム・リソース (サービス、ファイル、プログラムなど) の表示です。



Policy Director では、その許可サービスを第三者ネームスペースに属するオブジェクトに拡張できます。第三者ネームスペースを Policy Director に統合するには、次の手順が必要です。

- 第三者アプリケーションのネームスペースを Policy Director に記述する。
- 保護を必要とするネームスペース・オブジェクトにポリシー・テンプレートを適用する。

特殊なマッピング・ファイルの使用によって、Policy Director に対して第三者ネームスペースの内容を記述します。このファイルには、第三者ネームスペースに属するリソース・オブジェクトがリストされ、その階層関係が示されています。

さらに、この第三者ネームスペースが収容されるルート・コンテナー・オブジェクトを定義する必要があります。ルート・コンテナー・オブジェクト名は、管理コンソール (オブジェクト・スペース・タブ) によって表示された場合は、 Policy Director ネームスペースの一部として表示されます。既存の標準的な Policy Director コンテナー・オブジェクトには、 /WebSEAL、/NetSEAL、/Management があります。

管理サーバー構成ファイル (ivmgrd.conf) で、第三者コンテナー・オブジェクトの名前と、マッピング・ファイルの場所が定義されます。

ルート・コンテナー・オブジェクト名とマップ・ファイル場所

管理サーバー構成ファイル (ivmgrd.conf) の [object-spaces] スタンザで、次の項目を両方とも定義します。

- 第三者ネームスペースに関するルート・コンテナー・オブジェクトの名前
- マッピング・ファイルの場所

各項目の形式は次のとおりです。

```
object-space-root = map-file
```

ただし、次のとおりです。

object-space-root 第三者ネームスペースを収容するコンテナー・オブジェクトの名前

map-file マップ・ファイルへの全パス名。マップピング・ファイルはどこにあっても構いません。

次の例では、第三者コンテナー・オブジェクト (Notes) とマップ・ファイルの場所 notemap.txt を定義しています。

UNIX: `/Notes = /opt/intraverse/lib/notemap.txt`

Windows: `/Notes = C:¥Program Files¥IBM¥Policy Director¥lib¥notemap.txt`

注: ivmgrd.conf ファイルに取り込む編集があった場合は、管理サーバーをいったん停止してから再始動する必要があります。

マッピング・ファイルの形式

第三者ネームスペースを記述するマッピング・ファイルは、 ASCII テキスト・ファイルです。ファイル内の各行は、それぞれがネームスペース内の各リソース・オブジェクトを表す絶対パス名です。マッピング・ファイルには、リソース・オブジェクトだけがリストされています。Policy Director では、パス名からコンテナー・オブジェクトを暗黙指定します。

追加のマップ・ファイル規則としては、次のものがあります。

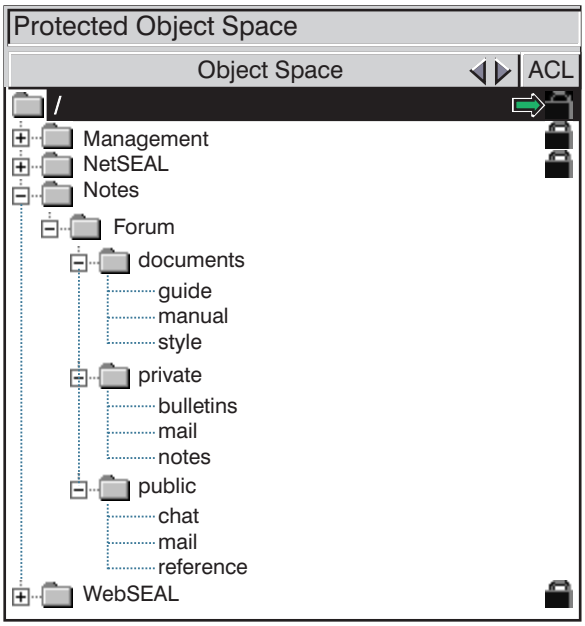
- 1 行にオブジェクトとパス名を 1 つずつリストする。
- オブジェクト・パス名は、必ずスラッシュ (/) で始まる。

マッピング・ファイルの例 :

```
/Forum/public/mail
/Forum/public/reference
/Forum/public/chat
/Forum/documents/style
/Forum/documents/guide
/Forum/documents/manual
/Forum/private/mail
/Forum/private/notes
/Forum/private/bulletins
```

管理コンソールでの階層表示

次の管理コンソール画面は、 『マッピング・ファイルの形式』 で説明しているマッピング・ファイルの例の結果表示されたものです。



カスタム ACL 許可を定義する

Policy Director では、ポリシー・テンプレートを基にして、保護オブジェクトに対してオペレーションを実行する場合に必要な条件を指定します。Policy Director では、アクセス制御リスト (ACL) と呼ばれる特定のタイプのポリシー・テンプレートを使用します。

ACL 項目

ACL をオブジェクトに付加できます。これが付加されると、ACL 内の項目によって、Policy Director がこのオブジェクトに対して許可するオペレーションと、オペレーションの実行者が指定されます。ACL 項目には、次のものが含まれます。

- ユーザー・タイプまたはグループ・タイプ

  非認証ユーザーと全認証ユーザーを表すタイプもあります。
- 固有のユーザー識別またはグループ識別
- 許可

許可

Policy Director は、広範囲にわたるオペレーションを網羅する、標準的な一組の許可を使用します。単一の印刷可能 ASCII 文字で、許可を表します。管理コンソール (**ACL** タブ) では、Policy Director は、管理対象の操作を記述するラベルを付けて、それぞれの許可を表示します。さらに、Policy Director では、ACL を、特定のネームスペースでの使用に従い、ネームスペース全体にわたって使用するために、グループに分けます。グループ・カテゴリーの例としては、基本 (Base)、
汎用 (Generic)、WebSEAL、NetSEAL があります。

オブジェクトに対するオペレーション

アプリケーション・ソフトウェアには、一般的に、保護オブジェクトに対して実行される 1 つまたは複数のオペレーションが含まれています。これらのアプリケーションでは、要求されたオペレーションの実行が許可される前に、許可サービスに呼び出しを行います。この呼び出しは、Policy Director および第三者のアプリケーションとも、Policy Director 許可 API を使用して行われます。

オブジェクトを保護する情報は、ACL 内に入っています。許可サービスではこの情報を使用して、`Does this user (group) have the "r" permission (for example) for the requested object?` という質問に対して、単純に `yes` または `no` と応答します。

ここで重要なのは、許可サービスは、読み取り (r) 許可を必要とするオペレーションについて一切関知しないということです。許可サービスにとって重要なのは、読み取り (r) 許可の有無だけです。読み取り (r) 許可は、要求側ユーザーまたはグループの ACL 項目内にあります。

この許可は、Policy Director 許可サービスの強力な機能です。サービスは、要求されているオペレーションから完全に独立しており、このことが、第三者アプリケーションへの許可サービスの利点の拡張が容易な理由になっています。

カスタム許可の要件

標準的な Policy Director 許可の範囲全体が、第三者アプリケーションで使用可能です。つまり、第三者アプリケーションで、 Policy Director 許可を使用することができるのです。これが行われると、対応するオペレーションは、Policy Director によって通常実行される実際のオペレーションに非常に緊密に一致するはずです。たとえば、保護オブジェクトへの読み取り専用アクセスを必要とするオペレーションでは、読み取り (r) 許可だけ使用すればよいはずです。

注: 第三者アプリケーションでは、オペレーションについては一切関知も関与もしない標準的な Policy Director 許可を、完全に無関係なオペレーションに使用できます。ただし、この場合は、同一許可の異種使用間の区別を必要とする管理者にとっては、困難を生じる可能性があります。

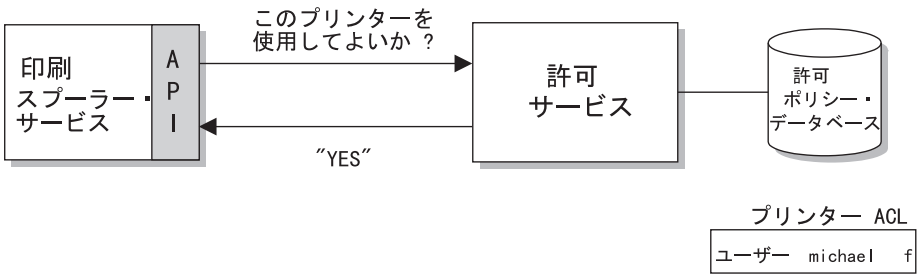
第三者アプリケーションでは、標準的な一組の許可では表されていないオペレーションを使用する場合があります。これが使用される場合は、 Policy Director で新規許可を定義できます。このアプリケーションがこの許可を使用し、この許可は許可サービスで認識されます。

例 :

この例では、特定のプリンターを無許可使用から保護することが要件です。第三者印刷スプール・サービスが、Policy Director 許可 API で作成されます。この印刷スプール・サービスが許可サービスを呼び出して、プリンターに対して行われている要求に対して、 ACL 検査を実行することになります。

標準的な Policy Director 許可には、プリンターを保護するための許可は組み込まれていません。 この例では、印刷許可が新規に作成され、プリンターを保護する必要があります。

そこで、ACL がプリンター・オブジェクトに付加されました。ユーザーが保護プリンターの使用を要求する場合は、印刷許可が含まれている ACL 項目が必要です。 印刷許可が存在していれば、許可サービスが肯定的な応答を戻し、印刷オペレーションが実行されます。 印刷許可が存在していないことを許可サービスが検出した場合は、印刷オペレーションは実行を許可されません。



許可の管理

Policy Director 管理者は次の方法で許可を管理できます。

- カスタム許可を追加する
- カスタム許可を削除する
- 使用可能なすべての許可を表示する

カスタム許可を作成する

新規許可の作成、削除、一覧表示を行う場合は、**ivadmin action** コマンドを使用します。**ivadmin** ユーティリティーを使用するには、Policy Director 管理者としてログインしている必要があります。

新規カスタム許可を作成する場合は、次のコマンド構文を使用します。

```
ivadmin> action create name description action-type
```

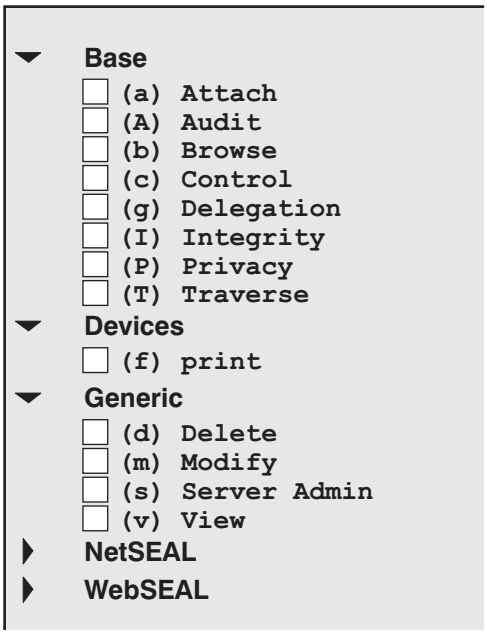
ただし、次のとおりです。

`name`	許可を表す印刷可能 ASCII 文字。
`description`	管理コンソール表示画面 (ACL タブ) で文字の右側に表示される記述ラベル。
`action-type`	この許可が管理コンソール表示画面 (ACL タブ) に表示される編成カテゴリー。

たとえば、次のように入力したとします。

```
ivadmin> action create f print Devices
```

その結果、管理コンソールの ACL 管理パネルに、この新規項目が表示されます。



カスタム許可を削除する

カスタム許可を削除する場合は、次のコマンド構文を使用します。

```
ivadmin> action delete name
```

たとえば、次のようにします。

```
ivadmin> action delete f
```

すべての使用可能許可の一覧表を表示させる

すべての使用可能許可の一覧表を表示させる場合は、次の構文を使用します。

```
ivadmin> action list
```

次のような許可の一覧表が表示されます。

```
p "Proxy" NetSEAL
r "Read" WebSEAL
v "View" Generic
x "Execute" WebSEAL
A "Audit" Base
a "Attach" Base
b "Browse" Base
c "Control" Base
C "Connect" NetSEAL
d "Delete" Generic
f "Print" Devices
g "Delegation" Base
I "Integrity" Base
l "List Directory" WebSEAL
m "Modify" Generic
P "Privacy" Base
s "Server Admin" Generic
T "Traverse" Base
...
```

外部許可サービスを定義する

外部許可サービス を使用すると、追加の許可制御と条件を設けて、標準 Policy Director 許可プロセスを補足できます。このような追加の制御と条件は、別の許可サーバー・プログラムで指示します。

Policy Director 許可サービスでは、外部許可機能を自動的に組み込みます。ユーザーが外部許可サービスを構成した場合は、 Policy Director 許可サービスでは、その評価プロセスに新しい制御と条件を取り込むだけです。

外部許可サービスの設定には、次の 2 つの一般的なステップを実行する必要があります。

1. 許可決定時に参照できるサーバー・プログラムを作成します。

   Policy Director Programmer's Guide and Reference を参照してください。
2. 外部許可サービスを Policy Director に登録します。

   『外部許可サービスを登録する』を参照してください。

サービスを登録すると、このサービスを表す新規許可が Policy Director 管理コンソールに表示されます。これで、この許可を任意の ACL 項目で使用できるようになります。

Policy Director では、許可検査時に外部許可サービスを検出すると、追加の許可決定について、外部許可サービスを参照します。

詳しい背景情報が必要な場合は、52ページの『外部許可機能』を参照してください。

外部許可サービスを登録する

Policy Director 許可サービスに外部許可サービスの存在と場所を通知する場合は、**ivadmin server register** コマンドを使用します。

適用される構文は、次のとおりです。

```
ivadmin> server register externauth server-name ns-location server-principal
         action-char action-name
```

ただし、次のとおりです。

server-name	この外部許可サービスの名前 (または、ラベル)。管理コンソールのオブジェクト・スペースの表示画面と、 ivadmin server list コマンドで表示される名前です。
ns-location	外部許可サーバーがその RPC バインディングをエクスポートする、 CDS ネームスペース内の RPC 項目。
server-principal	外部許可サーバー・プロセスに関する LDAP 名または DCE プリンシパル名。
action-char	補足許可決定のためにこの外部許可サービスの使用を指示する場合に、 ACL 内で使用される許可文字。
action-name	管理コンソール表示画面 (ACL タブ) で文字の右側に表示される記述ラベル。

このコマンドでは、デフォルトの ACL 編成カテゴリーが生成され、*外部許可* と呼ばれます。 管理コンソールは、ACL を表示するとき、デフォルトの ACL 編成カテゴリーを使用します。 すべての登録済み外部許可サービスに関する許可は、このカテゴリーのもとに表示されます。

たとえば、次のように入力したとします。

```
ivadmin> server register externauth timechecker /.:/subsys/timechk
         t-checker k time-check
```

そうすると、timechecker という名前が付けられた外部許可サービスが、許可サービスに登録されます。 timechecker がその RPC バインディングをエクスポートする、CDS ネームスペース内の RPC 項目が、 /.:/subsys/timechk です。サーバーの DCE プリンシパル名が t-checker です。このサーバーに対応する許可が時刻チェック (time-check) (k) 許可です。

この登録済み外部許可サーバーに関する許可は、管理コンソールに次のように表示されます。

```
Base
  (a) Attach
  (A) Audit
  (b) Browse
  (c) Control
  (g) Delegation
  (I) Integrity
  (P) Privacy
  (T) Traverse
Generic
  (k) time-check
Generic
  (d) Delete
  (m) Modify
  (s) Server Admin
  (v) View
NetSEAL
WebSEAL
```

外部許可サーバーを削除する

登録済み外部許可サービスを除去する場合は、**ivadmin server delete** コマンドを使用します。適用される構文は、次のとおりです。

```
ivadmin> server delete /ExternAuthzn/server-name
```

ただし、次のとおりです。

server-name	この外部許可サービスの名前 (または、ラベル)。管理コンソールのオブジェクト・スペースの表示画面に表示される名前です。

たとえば、次のとおりです。

```
ivadmin> server delete /ExternAuthzn/timechecker
```

例 1:

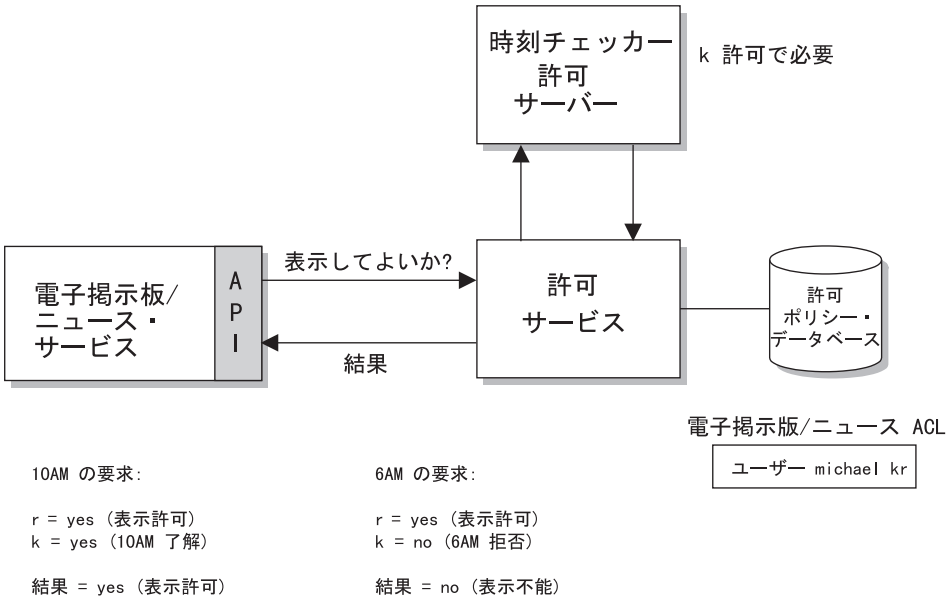
第三者電子掲示板 / ニュース・サービスは、そのオペレーションに時刻制限が設けられています。つまり、このサービスによって提供される情報をユーザーが表示させ

て見ることができるのは、8AM と 5PM の間だけです。外部許可サービスを作成して、電子掲示板 / ニュース・サービスに対して行われるすべての要求に対して、時刻チェックを実行します。

外部許可サービスを設定する場合は、**ivadmin** コマンドを使用します。

次の図には、許可プロセスのモデル・ケースとして考えられる場合が図示してあります。電子掲示板 / ニュース情報を表示させて見る場合は、ユーザーに読み取り (r) 許可が必要です。ニュース・サービスの ACL にも時刻チェック (k) 許可が組み込まれます。時刻チェック (k) 許可では、 Policy Director 許可サービスに、最終決定で時刻チェッカー許可サーバーを組み込むよう指示します。

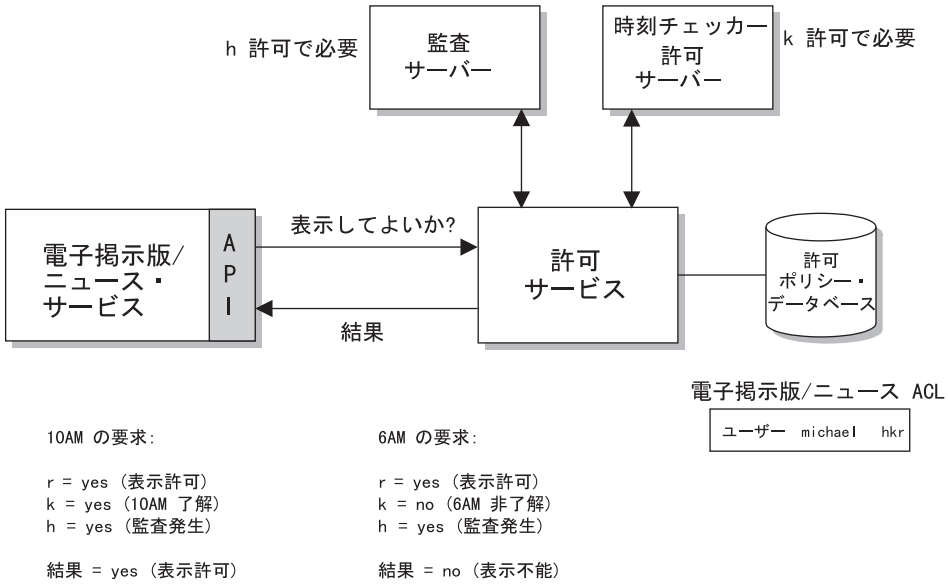
Policy Director では、すべての許可サーバー決定を総合したものを基にして最終許可決定を行います。



例 2:

この例は例 1 と同じです。ただし、この例では、電子掲示板 / ニュース・サービス上の活動を監査する、 2 番目の外部許可サービスが追加されています。

なお、時刻チェッカー許可サービスが表示を許可しないときは、活動の監査がやはり行われます。**h** 許可が存在していると、 ACL チェック時の監査許可サーバーの関与が必要です。



管理サーバーの管理

Policy Director 管理サーバー (ivmgrd) では、基本 (マスター) 許可ポリシー・データベースを管理します。また、ソース・ドメイン内の他の WebSEAL サーバーや NetSEAL サーバーについての場所情報も保守します。管理サーバーは、一般に、管理や構成がほとんど要りません。この節には、管理者にできるタスクが含めてあります。

更新通知スレッドの数を設定する

基本許可ポリシー・データベースの保守は、管理サーバー (ivmgrd) が行います。この基本データベースのレプリカを作成するのは、セキュリティー・マネージャー (secmgrd) と許可サーバー (ivacld) です。

次に、管理サーバーがセキュア・ドメイン内のすべてのデータベースの同期化を行います。基本データベースに変更が加えられると、通知スレッドがこの変更をすべてのレプリカに知らせる作業を行います。そうすると、それぞれのレプリカでは、新しい情報を基本データベースからダウンロードする必要があります。

管理サーバー構成ファイル ivmgrd.conf に、更新通知スレッドの最大数を設定するためのパラメーターが入っています。このスレッド・プールを使用すると、同時 (並列) 通知ができます。

たとえば、30 のレプリカにデータベース変更を同時に通知する場合は、スレッド・プールは少なくとも 30 に設定します。レプリカの数が 30 を超えている場合は、通知がもう 1 回繰り返されます (この例では、一度に 30)。このパラメーターの値には関係なく、すべてのレプリカに通知が保証されています。

データベースの変更をできるだけ速やかに知らせることが、更新通知スレッド値のパフォーマンス上の目標です。 一般的には、この値は既存のレプリカの数に等しく設

定します。 この値を設定した結果、単一のスレッド・プールで、すべてのレプリカに対する同時通知を速やかに達成できるという、パフォーマンス上の利点が得られます。

デフォルトのイベント通知スレッド・プールは、次のように設定されます。

```
[ivmgrd]
max-notifier-threads = 10
```

第12章 サーバー活動のログ記録と監査

Policy Director には、幾つかのログ記録機能と監査機能があり、 Policy Director と DCE サーバーの両方が生成したエラー・メッセージと警告メッセージを取り込むログ・ファイルがあります。また、Policy Director と DCE サーバーの活動をモニターする監査証跡ファイルもあります。

この章は、次の各節に分かれています。
- ログ記録と監査の概要
- 各ログ・ファイルの説明
- 各監査ファイルの説明

ログ記録と監査の概要

ログ・ファイルと監査証跡ファイルの内容は、情報源として役立ちます。ログ・ファイルや監査証跡ファイルの内容を使用して、Policy Director サーバーや DCE サーバーの活動に生じた問題の監視や検出と修正ができます。

ログ・ファイル

Policy Director サーバーと DCE サーバーでは、ログ・ファイルを使用して、警告メッセージやエラー・メッセージを保管します。ログ・ファイルは、すべてテキスト形式です。

Policy Director には、次のログ・ファイルが備えられています。

- Policy Director サーバー・ログ・ファイル

  152ページの『Policy Director サーバー・ログ・ファイル』を参照してください。
- DCE サーバー・ログ・ファイル

  153ページの『DCE サーバー・ログ・ファイル』を参照してください。
- DCE 保守容易性メッセージ

  153ページの『DCE 保守性メッセージ』を参照してください。
- 標準 HTTP ログ・ファイル

  155ページの『標準 HTTP ログ記録』を参照してください。

監査証跡ファイル

Policy Director サーバーと DCE サーバーでは、監査証跡ファイルを使用して、サーバー活動のレコードを保管します。*レコード* は、特定のサーバー・イベントの出力を指します。監査証跡とは、サーバー活動を文書化する複数のレコードの集合のことです。監査ファイルは、ほとんどが ASCII 形式です。 DCE 監査証跡ファイルは、バイナリー形式です。これらのファイルを表示させて見る場合は、**dcecp** ユーティリティーを使用する必要があります。

次の監査証跡ファイルでは、Policy Director サーバーや DCE サーバーに関するイベント情報が得られます。

- 次の 3 つの Policy Director 許可監査証跡ファイル (audit.log)
  - 管理サーバー (ivmgrd)

– セキュリティー・マネージャー (secmgrd)
– 許可サーバー (ivacld)

158ページの『Policy Director 許可監査証跡ファイル』を参照してください。

- WebSEAL 監査証跡ファイル (wand_audit_log)

  160ページの『WebSEAL 監査証跡ファイル』を参照してください。
- Policy Director 管理監査証跡ファイル

  162ページの『Policy Director 管理コマンド監査証跡ファイル』を参照してください。
- DCE 監査証跡ファイル

  163ページの『DCE サーバー監査証跡ファイル』を参照してください。

install-path 変数に関する規則

install-path 変数をこの章で使用する場合は、オペレーティング・システム・プラットフォームに応じて、次のように解釈します。

UNIX: `/opt/intraverse/`

Windows:

```
C:¥Program Files¥IBM¥
```

UNIX では、このパス名は固定されているため変更できません。

Windows プラットフォームの場合は、Policy Director ソフトウェアのインストール時に、*install-path* を定義できます。

Policy Director サーバー・ログ・ファイル

各 Policy Director サーバーでは、それぞれ警告メッセージやエラー・メッセージを動的に生成し、これが標準エラーに送信され、次いで特定のログ・ファイルに転送されます。

サーバー	プロセス	ログ・ファイルの場所
管理サーバー	**ivmgrd**	ivmgrd.conf で定義: log-file=*install-path*/ivmgrd/log/ivmgrd.log
セキュリティー・マネージャー	**secmgrd**	secmgrd.conf で定義: log-file=*install-path*/secmgr/log/secmgrd.log
許可サーバー	**ivacld**	ivacld.conf で定義: log-file=*install-path*/ivacld/log/ivacld.log
ディレクトリー・サービス・ブローカー	**nsid**	*install-path*/broker/nsid.log

サーバー・ログ・ファイルを使用可能 / 使用不可にする

Policy Director がログ記録を使用可能にするのは、構成ファイルで定義されているログ・ファイルがある場合です。

secmgrd.log の例

secmgrd.log ファイルには、次のような内容が入ります。

```
1998-09-22-21:56:36.898-04:00I----- secmgrd FATAL ivc general
exec.c 344 0x00000006
Caught signal (15)
1998-09-22-21:56:37.309-04:00I----- secmgrd ERROR ivc rpc
IVServer.cpp 1039 0x00000001
Could not unexport bindings from name service
(/.:/subsys/ibm/secmgr/server/sun,0x16c9a093
1998-09-22-21:56:37.354-04:00I----- secmgrd ERROR ivc rpc
IVServer.cpp 1048 0x00000001
Could not unregister RPC endpoints (0x16c9a042)
```

DCE サーバー・ログ・ファイル

各 DCE サーバーでは、それぞれ警告メッセージやエラー・メッセージを動的に生成し、これが標準エラーに送信され、次いで特定のログ・ファイルに転送されます。これらのログ・ファイルは、問題を検出し訂正する際に、情報源として役立ちます。

DCE サーバー・ログ・ファイルには、次のものがあります。

セキュリティー・サーバー:

UNIX: /opt/dcelocal/var/security/secd.log

Windows: ¥Program Files¥IBM¥dcelocal¥var¥security¥secd.log

DCE サーバー:

UNIX: /opt/dcelocal/var/dced/dced.log

Windows: ¥Program Files¥IBM¥dcelocal¥var¥dced¥dced.log

DCE 保守性メッセージ

ルーティング・ファイルが DCE 保守性メッセージを制御します。

UNIX: /opt/dcelocal/var/svc/routing

Windows: ¥Program Files¥IBM¥NetSEAT¥var¥svc¥routing

注: Windows システムの場合、インストール・パスはインストール時に構成可能です (¥Program Files¥IBM¥NetSEAT¥)。 環境変数 (%NETSEAT%) は、構成後のパスに解決されます。

ルーティング・ファイル内のデフォルト項目

この構成ファイル内の項目によって、ログに記録される情報のタイプが決まります。ルーティング・ファイルには、次のようなデフォルト項目が組み込まれています。

UNIX:

```
FATAL:STDERR:-;FILE:/opt/dcelocal/var/svc/fatal.log
```

```
ERROR:STDERR:-;FILE:/opt/dcelocal/var/svc/error.log
WARNING:STDERR:-;FILE:/opt/dcelocal/var/svc/warning.log
```

Windows:

```
FATAL:STDERR:-;FILE:%NETSEAT%¥var¥svc¥fatal.log
ERROR:STDERR:-;FILE:%NETSEAT%¥var¥svc¥error.log
WARNING:STDERR:-;FILE:%NETSEAT%¥var¥svc¥warning.log
```

NOTICE メッセージでは、サーバーの活動についてのエクストラ情報が得られます。デフォルトでは、Policy Director が NOTICE メッセージを使用可能にすることはありません (ファイル内に項目が存在していません)。

NOTICE メッセージを使用可能にする (そして、標準エラーに送信する) 場合は、ルーティング・ファイルの終わりに、次のように新しい NOTICE 行を追加します。

UNIX:

```
FATAL:STDERR:-;FILE:/opt/dcelocal/var/svc/fatal.log
ERROR:STDERR:-;FILE:/opt/dcelocal/var/svc/error.log
WARNING:STDERR:-;FILE:/opt/dcelocal/var/svc/warning.log
NOTICE:STDERR:-;FILE:/opt/dcelocal/var/svc/notice.log
```

Windows:

```
FATAL:STDERR:-;FILE:%NETSEAT%¥var¥svc¥fatal.log
ERROR:STDERR:-;FILE:%NETSEAT%¥var¥svc¥error.log
WARNING:STDERR:-;FILE:%NETSEAT%¥var¥svc¥warning.log
NOTICE:STDERR:-;FILE:%NETSEAT%¥var¥svc¥notice.log
```

メッセージを標準出力に送信する場合のデバッグ・モード

通常、Policy Director では、警告メッセージやエラー・メッセージを (NOTICE メッセージも含めて)、該当するログ・ファイルに転送します。

これらのメッセージを標準出力 (端末) に送信する場合は、サーバーの開始時に、**-debug** コマンド・オプションを使用します。このオプションを使用すると、サーバーがフォアグラウンドで稼働することになります (つまり、サーバー自体がデーモン化されることはありません)。 Policy Director が警告メッセージやエラー・メッセージを標準出力に書き込みます。

たとえば、セキュリティー・マネージャー (secmgrd) をデバッグ・モードで開始する場合は、次のようにコマンドを使用します。

```
# /opt/intraverse/secmgr/bin/secmgrd -debug
```

また、UNIX **tee** コマンドを使用して、サーバー出力を単一のファイルに取り込むこともできます。

次の例には、Policy Director セキュリティー・マネージャーをこのモードで開始する場合が示してあります。

```
# secmgrd -debug 2>&1 | tee /tmp/secmgrd.log
```

デバッグに関する注記

デバッグにあたっては、次のことに留意してください。

1. サーバーの活動情報の収集を完了したら、ルーティング・ファイルは、必ず通常の状態に復元しておきます。NOTICE 項目は、除去します。 NOTICE では、大量の情報が生成されて、急速に累積する可能性があります。
2. **Ctrl + c** を使用すれば、デバッグ・モードで開始したサーバー・プロセスを中断できます。サーバー・プロセスは、正しくシャットダウンして、終了します。

標準 HTTP ログ記録

Policy Director WebSEAL サーバーには、次のような 3 つの在来型 HTTP ログ・ファイルも保守されていて、メッセージではなく、活動が記録されます。

wand_request_log
157ページの『wand_request_log を表示させる』を参照してください。

wand_agent_log
157ページの『wand_agent_log を表示させる』を参照してください。

wand_referer_log
157ページの『wand_referer_log を表示させる』を参照してください。

デフォルトでは、Policy Director が上記のログ・ファイルを保守するのは、次のディレクトリーです。

UNIX: `/opt/intraverse/www/log`

Windows: `¥Program Files¥IBM¥Policy Director¥www¥log`

標準 HTTP ログを構成する

iv.conf 構成ファイルの [wand] スタンザには、標準 HTTP ログを構成するためのパラメーターが入っています。

次の表には、HTTP ログ・ファイルと構成ファイル・パラメーターの間の関係が示してあります。

ログ・ファイル	位置パラメーター	使用可/使用不可パラメーター (= yes または no)
wand_request_log	reqlog =	logreqs =
wand_referer_log	reflog =	logrefs =
wand_agent_log	agentlog =	logagents =

たとえば、**wand_request_log** のデフォルトの位置に関する iv.conf 内の項目は、次のようになります。

```
reqlog = log/wand_request_log
```

この位置のルート・ディレクトリーは、次のとおりです。

UNIX: `/opt/intraverse/www/`

Windows: `¥Program Files¥IBM¥Policy Director¥www¥`

HTTP ログ記録を使用可能 / 使用不可にする

デフォルトでは、Policy Director は、HTTP ログ記録をすべて使用可能にします。

```
[wand]
logreqs = yes
logrefs = yes
logagents = yes
```

ログ記録を使用不可にする場合は、次のように設定します。

```
<enable-parameter> = no
```

タイム・スタンプ・タイプを指定する

各ログが現地時間帯によらず、グリニッジ標準時 (GMT) で記録されるように、タイム・スタンプを選択できます。デフォルトでは、Policy Director では現地時間帯が使用されます。

```
[wand]
loggmttime = no
```

GMT タイム・スタンプを使用する場合は、次のように設定します。

```
loggmttime = yes
```

注: すべてのセキュリティー関連プロダクトの監査ファイルとログ・ファイルの読み取りをしやすくするために、すべてのログ・ファイルを、時間を同期化させて保持することを考慮してみてください。

最大ログ・ファイル・サイズを指定する

各 HTTP ログ・ファイルの最大サイズは、デフォルトでは次のように設定されます。

```
[wand]
logsize = 2000000
```

ログがこのサイズに達すると、Policy Director では、ログ・ファイルをバックアップします。

なお、このパラメーターは、 Policy Director の **wand_audit_log** 監査証跡ファイルにも影響を生じます。

ログ・ファイルについては、しばしばサイズをチェックして、大きくなり過ぎていないか、スペースを占め過ぎていないか確認します。定期的なシステム保守時には、ログ・ファイルを定期的にアーカイブします。

HTTP 共通ログ形式を使用する

Policy Director サーバーから返送される応答 (正常または障害) は、それぞれ次のような HTTP 共通ログ形式の 1 行の項目として記録されます。

```
host - authuser [date] request status bytes
```

ただし、次のとおりです。

host 要求元マシンのインターネット・プロトコル (IP) アドレスを指定します。

authuser 受信された HTTP 要求の **From:** ヘッダーの値をとります。さらに、このフィールドでは、値を `dce-rpc` に設定して、セキュア RPC 要求を伝達します。ユーザーが認証されていない場合は、このフィールドはブランクです。

date 要求の日時を指定します。

request 要求の最初の行を、クライアントからの要求どおりに指定します。

status 要求元マシンに返送される HTTP 状況コードを指定します。

bytes 要求元マシンに返送されるバイト数を指定します。言い換えれば、文書内容の長さが転送されます。

wand_request_log を表示させる

wand_request_log には、HTTP 要求の標準ログ記録が記録されます。標準ログ記録の例には、要求された URL に関する情報と、要求を行ったクライアントに関する情報 (たとえば、IP アドレス) が含まれています。

wand_request_log ファイルには、次のような内容が入ります。

```
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:33 EDT]
  "GET /~smith/private_html/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:47 EDT]
  "GET /icons HTTP/1.0" 302 93
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:59 EDT]
  "GET /icons/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue,  23 Apr 1996 17:24:04 EDT]
  "GET /~smith/private_html/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue, 23 Apr 1996 17:24:11 EDT]
  "GET /~smith/ HTTP/1.0" 403 77
dce-rpc - - [Tue, 23 Apr 1996 17:24:51 EDT]
  "GET / HTTP/1.0" 200 919
```

wand_agent_log を表示させる

wand_agent_log には、HTTP 要求内の User_Agent: ヘッダーの内容が記録されます。このログでは、それぞれの要求ごとに、アーキテクチャーやバージョン番号など、クライアント・ブラウザーについての情報が示されます。

次の例は、wand_agent_log ファイルのサンプル・バージョンを示します。

```
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
```

wand_referer_log を表示させる

wand_referer_log には、HTTP 要求のヘッダーが記録されます。それぞれの要求ごとに、要求された文書へのリンクが含まれていた文書がログに記録されます。

このログでは、次の形式が使用されます。

```
referer -> object
```

この情報が役立つのは、Web スペース内の文書への外部リンクを追跡する場合です。このログでは、referer で示されるソースに、ページ・オブジェクト へのリンクが入っていることが示されます。このログを使用すると、失効リンクを追跡し、文書へのリンクを作成している当事者を検出できます。

次の例は、wand_referer_log ファイルのサンプル・バージョンを示します。

```
http://manuel/maybam/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ivdl/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ -> /ivdl/index.html
http://manuel/maybam/ -> /ivdl/index.html
http://manuel/maybam/ivdl/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ -> /ivdl/index.html
```

Policy Director 許可監査証跡ファイル

セキュリティー関連監査可能活動が生じたときは、それぞれの Policy Director サーバーで監査イベントを取り込めます。Policy Director では、該当のサーバーの特定の活動を文書化する (記録する) 監査レコードとして、監査イベントを保管します。 複数の監査レコードで監査証跡ファイルが構成されます。

次の表には、それぞれの Policy Director サーバーとそれに対応する監査証跡ファイルの間の関係が示してあります。

サーバー	プロセス	許可監査ファイル
管理サーバー	**ivmgrd**	ivmgrd.conf で定義: audit-file= *install-path*/ivmgrd/log/audit.log
セキュリティー・マネージャー	**secmgrd**	secmgrd.conf で定義: authzn-audit-file= *install-path*/secmgr/log/audit.log
許可サーバー	**ivacld**	ivacld.conf で定義: audit-file= *install-path*/ivacld/log/audit.log

Policy Director では、ユーザーやグループに関する監査 (A) 許可が ACL 内に設定されると、該当する監査証跡ファイルに許可情報を書き込みます。その結果の監査レコードには、許可が正常に行われなかった場合も含めて、アクセスの試みがすべて含まれます。

監査証跡管理

ACL 項目での監査 (A) 許可によって、Policy Director 許可監査証跡ファイルによる活動情報の記録が起動されます。監査 (A) 許可による監査の活動化は、簡単に実行できます。

許可監査証跡ファイルの管理には、次の条件が該当します。

- ACL が付加されているオブジェクトによって、3 つの audit.log ファイルのうちで、データを収集するファイルが決まります。

  たとえば、1 つまたは複数の項目に対する監査 (A) 許可が含まれている ACL を、保護オブジェクト・ネームスペースの /Management オブジェクトに付加できます。こうして付加された場合は、データは、管理サーバー (ivmgrd) の audit.log ファイル内に収集されます。管理サーバーでは、許可ポリシー・データベース (ACL) とデータベース複製 (レプリカ) を制御します。
- 監査 (A) 許可が該当する ACL 項目内で設定されると、活動情報だけがユーザーかグループ、またはその両方に関して収集されます。

  たとえば、HTML ページ・オブジェクトに付加されている ACL 内で、認証されていない項目に対して監査 (A) 許可を付与できます。この許可によって、セキュリティー・マネージャーの audit.log ファイルが、許可されなかったオブジェクトへのアクセスの試みすべてに関する情報を収集します。

例 : 次の ACL は、デフォルト webseal ACL を表します。`cell_admin` ユーザー項目と `authenticated` 項目に監査 (A) 許可が設定されています。

```
user cell_admin                    aAbcTdmlrx
group iv-admin                     abdTdmlrx
group ivmgrd-servers               Tl
group webseal-servers              gTdmlrx
any-authenticated                  Tr
unauthenticated                    ATr
```

ACL が /WebSEAL オブジェクトに付加されているということは、保護オブジェクト・ネームスペースの WebSEAL 領域のルートに付加されていることを意味します。このように付加された場合は、Policy Director が、セキュリティー・マネージャー・サーバー (WebSEAL と NetSEAL) が関与する活動を、セキュリティー・マネージャーの audit.log ファイルに記録します。

WebSEAL ネームスペースには、許可条件を変更する他の明示的 ACL が含まれていない可能性があります。他の明示的 ACL がない場合は、Web スペース内のオブジェクトに対するすべての要求に対して、監査が行われます。

監査証跡ファイルに記録されるのは、cell_admin ユーザーと認証されていないアクセスの試みによって開始される活動だけです。

明示的 ACL が /WebSEAL オブジェクトより下でオブジェクトに付加されている場合は、 ACL 継承のチェーンが切断されます。このような明示的 ACL 内の項目には監査許可が含まれていない可能性があります。項目に監査許可が含まれていない場合は、このオブジェクトに関しても、このポイントより下の他のどのオブジェクトに関しても、監査証跡が生成されることはありません。

注: /WebSEAL オブジェクトより下のオブジェクトに明示的に付加する ACL がある場合は、その関連項目には必ず監査許可を追加してください。

管理サーバー監査証跡ファイルの例

管理サーバー監査証跡ファイルには、次のような内容が入ります。

```
START RECORD
  Protected object: /WebSEAL
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorized
END RECORD
START RECORD
  Protected object: /WebSEAL/sun
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorize
END RECORD
START RECORD
  Protected object: /WebSEAL/sun/icons
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorize
END RECORD
START RECORD
  Protected object: /WebSEAL
  Requested permissions: 0x00000100
```

```
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorize
END RECORD
```

WebSEAL 監査証跡ファイル

Policy Director WebSEAL サーバーの活動も監視できます。Policy Director では、該当のサーバーの特定の活動を文書化する (記録する) 監査レコードとして、監査イベントを保管します。 複数の監査レコードで監査証跡ファイルが構成されます。

WebSEAL 監査

WebSEAL 監査証跡ファイルを構成するためのパラメーターは、iv.conf 構成ファイルの [wand] スタンザに入っています。

次の表には、WebSEAL と監査証跡ファイルの間の関係が示してあります。

サーバー	監査ファイル
WebSEAL	iv.conf で定義: auditlog= *install-path*/www/log/wand_audit_log

WebSEAL 監査を使用可能 / 使用不可にする

デフォルトでは、WebSEAL 監査は使用不可です。

```
[wand]
logaudit = no
```

監査をオンにする場合は、次のように設定します。

```
logaudit = yes
```

注: iv.conf 構成ファイル内のこのパラメーターの編集時には、yes や no の後にスペースがあってはなりません。

ログ・ファイル位置を指定する

WebSEAL 監査ファイルのデフォルトの位置は、次のとおりです。

```
[wand]
auditlog = log/wand-audit-log
```

最大ログ・ファイル・サイズを指定する

Policy Director では、監査ログ・ファイルのデフォルトの最大サイズを、次のように設定しています。

```
[wand]
logsize = 2000000
```

ログがこのサイズに達すると、Policy Director では、バックアップ・コピーとしてそのログ・ファイルをコピーします。新しい空の監査ログ・ファイルがデフォルトの監査ログ・ファイルとなります。なお、このパラメーターは、以下の標準 HTTP ログ・ファイルにも影響を生じます。

- wand_request_log
- wand_referer_log
- wand_agent_log

WebSEAL 監査証跡ファイルの構文

WebSEAL サーバーから返送される各応答 (正常または障害) は、それぞれ次のような形式の 1 行の項目として記録されます。

```
host call_type uri iv_status_code [date] uuid group_uuid_list
```

host (and endpoint)	リモート・ホストの IP アドレスとエンドポイント情報。エンドポイント情報がない場合は、[-] が表示されます。
call_type	0 は TCP 接続を表し、1 は UNAUTH RPC を表し、2 は AUTH RPC を表します。
uri	要求を表す汎用要求標識。
iv_status_code	標準監査機能のこの Policy Director サブセットを表す状況コード。
date	要求の日時。
uuid (**-p** フラグを付けて示される)	クライアントを表す UUID。UUID 情報がない場合は、何も表示されません。
group_uuid_list (**-g** フラグを付けて示される)	グループ UUID のリスト。グループ UUID 情報がない場合は、何も表示されません。

監査証跡ファイルの内容の例

監査証跡ファイルには、次のような内容が入ります。

```
204.30.81.188[33380] 2 /audit_report.html 0x18a2141a
[21/Aug/1997:14:36:23 -0700]
-p 00000064-0f4c-21d1-9300-00c078500371
-g 0000000c-0f4c-21d1-9301-00c078500371
-g 0000044c-0f4c-21d1-8601-00c078500371
-g 0000044d-0f4c-21d1-8601-00c078500371
```

詳細:

host:	204.30.81.188
endpoint:	[33380]
call_type:	2
uri:	/audit_report.html
iv_status_code:	0x18a2141a
date:	[21/Aug/1997:14:36:23 -0700]
uuid:	-p 00000064-0f4c-21d1-9300-00c078500371
group_uuid_list:	-g 0000000c-0f4c-21d1-9301-00c078500371 -g 0000044c-0f4c-21d1-8601-00c078500371 -g 0000044d-0f4c-21d1-8601-00c078500371

注: URI ストリングがハイフンだけで表示される場合があります。このような状態が生じる原因としては、要求の早期終了や要求ストリングの形式の誤りなどがあります。

Policy Director 管理コマンド監査証跡ファイル

管理関連監査可能活動が生じたときは、それぞれの Policy Director サーバーで監査イベントを取り込めます。Policy Director では、該当のサーバーの特定の活動を文書化する (記録する) 監査レコードとして、監査イベントを保管します。 複数の監査レコードで監査証跡ファイルが構成されます。

次の表には、それぞれの Policy Director サーバーとそれに対応する監査証跡ファイルの間の関係が示してあります。

サーバー	プロセス	管理監査ファイル
管理サーバー	**ivmgrd**	ivmgrd.conf で定義: mgr-audit-file= *install-path*/ivmgrd/log/mgraudit.log

管理サーバーの責任には、1 次許可ポリシー・データベースの保守が含まれます。

このデータベースには、セキュア・ドメインの保護オブジェクト・ネームスペースの記述、ACL ポリシー・テンプレート、ACL のオブジェクトへの付加場所が含まれます。

このデータベースには、次のものが含まれます。

- セキュア・ドメインの保護オブジェクト・ネームスペースの記述
- ACL ポリシー・テンプレート
- ACL がオブジェクトに付加される場所に関する情報

管理コンソールからでも、**ivadmin** ユーティリティーの使用によっても、mgraudit.log ファイルに管理コマンド・イベントを取り込めます。

監査レコードの内容

監査レコードは、XML スタイルのブラケットでタグ付けされたレコードに書き込まれます。監査イベントには、次の情報が取り込まれます。

オリジネーター ID
適宜、UUID のリストかストリング `unauthenticated` として印刷される、着信 RPC クライアント・ハンドルから派生。

タグ : `P`

イベント ID
../ivmgrd/cmdConst.h ヘッダーに定義されている、管理コマンドを固有に識別する番号。

タグ : `I`

コマンドの結果
呼び出し側に戻される状況コードに対応する番号。

タグ : `O`

タイム・スタンプ
ACL ビット監査で現在使用されている形式と同じ形式による、コマンド完了時刻のレコード。

タグ : `D`

コマンド引き数ベクトル

コマンド入力引き数の表示。

タグ：V と A

管理サーバー監査証跡ファイルの例

管理サーバー監査証跡ファイルには、次のような内容が入ります。

```
<E><D>Fri May 30 00:00:00 1999<¥D><I>3008</I><O>0</O><P>[1]
069d9fb6-943e-11cd-a35c-0000c08adf56</P><V><A> argument
1</A><A>argument 2</A></V></E>
```

DCE サーバー監査証跡ファイル

次の DCE サーバー監査証跡ファイルでは、DCE 管理サービスを使用します。ファイルは、バイナリー形式です。ファイルを表示させて見る場合は、**dcecp** ユーティリティーを使用する必要があります。

1. DCE セキュリティー・サービス (secd) 監査証跡

   /opt/dcelocal/var/security/sec_audit_trail

   /opt/dcelocal/var/security/sec_audit_trail.md_index

2. DCE 監査サービス (auditd) 監査証跡

   /opt/dcelocal/var/security/central_trail

   /opt/dcelocal/var/security/central_trail.md_index

3. DCE タイム・サービス (dtsd) 監査証跡

   /opt/dcelocal/var/security/dts_aud_trail

   /opt/dcelocal/var/security/dts_aud_trail.md_index

sec_audit_trail の例

```
dcecp> login cell_admin
Enter Password:
dcecp>
--- Event Record number 261 ---
o Event Information:
   - Event Number:          0x101 /* 257 */
   - Event Name:          AS_Request
   - Event Outcome:          success
o Server:          /.:/hosts/eggman
o Client:          /.../eggman_cell/cell_admin
o Number of groups:          0
o Authorization Status:          Authorized with a name
o Date and Time recorded: 1998-10-20-10:42:56.248-04:00I-----
--- End of Event record number 261 ---
```

第13章 WebSEAL: 認証の設定

Policy Director WebSEAL では、LDAP 、ケルベロス、および公開キー / 秘密キーによる各認証メカニズムをサポートします。認証プロセスの重要な副次的結果として、ユーザー・クリデンシャルが取得されます。 保護リソースへのアクセス要求の許可時には、このユーザー・クリデンシャルが使用されます。

この章は、次の各節に分かれています。

WebSEAL 認証の概説

この節では、以下に関する WebSEAL サポートの説明をします。

- SSL プロトコルを介するセキュア通信
- 認証メカニズム
- 識別情報を提供する方式
- 標準認証メカニズムの拡張

SSL サポート

WebSEAL では、セキュア・ソケット層 (SSL) プロトコルを介するセキュア通信をサポートします。 SSL プロトコルを介するセキュア通信については、次の各項で説明します。

- 166ページの『WebSEAL を SSL 用として構成する』
- 169ページの『サーバー側証明書を WebSEAL 用として設定する』

認証メカニズム

認証とは、セキュア・ドメインへのログインを試みる個々のユーザーを識別するプロセスのことです。WebSEAL では、次の認証メカニズムをサポートします。

- LDAP 機密キー
- ケルベロス・バージョン 5
- 公開キーと秘密キー

クライアント識別情報

認証プロセスでは、クライアントがログイン時に何らかの形式の識別情報を提示することを必要とします。 WebSEAL では、次の方式によるこの識別情報の提示をサポートします。

1. ユーザー名とパスワード (LDAP およびケルベロスによって使用される)

- 基本認証
- 書式ベース・ログイン

175ページの『ユーザー名とパスワードによる認証方式』を参照してください。

2. クライアント側 X.509 証明書 (公開キー / 秘密キーによって使用される)

179ページの『X.509 証明書による認証方式』を参照してください。

クリデンシャルの取得

クリデンシャル取得サービスを使用して、WebSEAL でサポートされている標準的な認証メカニズムを拡張できます。 181ページの『Policy Director クリデンシャル取得サービスの構成』を参照してください。

WebSEAL を SSL 用として構成する

Policy Director WebSEAL サーバーでは、セキュア・ソケット層プロトコル (SSL) を使用するクライアント・ブラウザーとのセキュア通信をサポートします。

このプロトコルを使用すると、クライアントでは、次の 2 つの方式のどちらか一方を使用して、識別情報を WebSEAL に渡せます。

- ユーザー名とパスワード
- クライアント側 X.509 ディジタル証明書

どちらのモードでも、WebSEAL は、そのサーバー側ディジタル証明書を使用して、クライアントに対して自らを認証します。この X.509 証明書は、認証局 (CA) が発行します。Policy Director では、証明書と対応する秘密キーを、 PEM 定様式ファイルと PKCS#12 定様式ファイルのどちらかに保管します。

PEM 形式を使用するときは、Policy Director では、サーバーの秘密キーと署名公開キーを別々のファイルに保管します。 PKCS#12 形式の場合、生成され保管されるキー・ペアは、単一のファイルに一緒に常駐します。

サーバー証明書内の共通名 (CN) は、WebSEAL サーバーの完全修飾ホスト名と同じである必要があります。

必須ではありませんが、ほとんどのクライアント・ブラウザーでは、サーバー証明書を発行したのが、有効な認証局かどうか検証します。 この検証は、ルート CA 証明書データベースを使用して行われます。証明書の署名がルート CA 証明書データベース内の項目に一致しない場合は、警告が表示されます。 そのようなサーバーとの接続を受け入れるか、リジェクトするかは、ユーザーの責任で決めます。

WebSEAL に関するサーバー側 X.509 証明書の取得とインストールに関する詳細説明は、 169ページの『サーバー側証明書を WebSEAL 用として設定する』を参照してください。

クライアント側証明書モードでは、WebSEAL は、上記のように、そのサーバー側ディジタル証明書を使用して、クライアントに対して自らを認証します。さらに、WebSEAL では、クライアント側証明書を妥当性検査できる CA (認証局) からの、X.509 ルート CA 証明書を必要とします。クライアント要求がクライアント側証明書を使用して行われると、真の相互認証が得られます。

サーバー側証明書とルート CA 証明書を使用する

サーバー側 X.509 証明書では、特定の WebSEAL サーバーをクライアントに対して認証します。Policy Director では、次のように、サーバー側証明書を PEM 形式か PKCS#12 形式で保管します。

- PEM 形式 -- 別々のファイルにサーバーの秘密キーと署名公開キーを保管する。
- PKCS#12 形式 -- 単一のファイルにサーバーの秘密キーと公開キーを保管する。

注: WebSEAL が収容しサポートできるサーバー証明書は、一度には 1 つだけです。WebSEAL が同一マシン上で複数の論理 Web サーバー・インスタンスをサポートすることはありません。

ルート CA 証明書 では、特定の認証局 (CA) を識別します。 WebSEAL では、ルート CA 証明書によるクライアント側証明書の妥当性検査を必要とします。 WebSEAL では、次のようにして、ルート CA 証明書のリストを PEM 形式と PKCS#12 形式のどちらかで、または両形式の組み合わせで保持できます。

- PEM 形式 -- ルート証明書を単一のファイルに累積する。
- PKCS#12 形式 -- 共通のディレクトリーの下に別々のファイルとしてルート証明書を保管する。

証明書を保管する

secmgrd.conf 構成ファイルで、証明書ストーレッジ・パラメーターを定義します。パラメーターは、使用するパラメーターが UNIX 用か、 Windows 用かによって異なります。

パラメーター	説明
UNIX 用 : `ca-directory = /opt/intraverse/lib/certs` **Windows 用 :** `ca-directory = C:¥Program Files¥ibm¥Policy Director¥lib¥certs`	
	証明書ストーレッジ用の基本ディレクトリー
UNIX 用 :`ca-cert-file = /lib/certs/cacert.pem` **Windows 用 :** `ca-cert-file = C:¥Program Files¥ibm¥Policy Director¥lib¥certs¥cacert.pem`	
	認識されている認証局の X.509 ルート CA 証明書で、PEM 形式。WebSEAL は、トラステッド CA からの PEM 形式のクライアント側 X.509 証明書を受け入れます。他の CA からのルート証明書をこのファイルに追加できます。
UNIX 用 : `ca-cert-p12-dir = /opt/intraverse/lib/certs/ca_p12` **Windows 用 :** `ca-cert-p12-dir = C:¥Program Files¥ibm¥Policy Director¥lib¥certs¥ca_p12`	
	認識されている認証局の PKCS#12 形式による X.509 ルート証明書が収容されるファイル用の指定ディレクトリー。 WebSEAL は、トラステッド CA からの PKCS#12 形式のクライアント側 X.509 証明書を受け入れます。他の CA からのルート証明書ファイルをこのディレクトリーに保管できます。

UNIX 用 : `certificate-file = /opt/intraverse/lib/certs/svrcert.pem` **Windows 用 :** `certificate-file = C:¥Program Files¥ibm¥Policy Director¥lib¥certs¥svrcert.pem`	
	CA から取得した X.509 サーバー証明書で、 PEM 形式。 この証明書は、SSL クライアントに対して表示されます。 このファイルに入っているサンプル証明書は、トラステッド CA からの正当な証明書で置き換える必要があります。
UNIX 用 : `key-file = /opt/intraverse/lib/certs/srvkey.pem` **Windows 用 :** `key-file = C:¥Program Files¥ibm¥Policy Director¥lib¥certs¥srvkey.pem`	
	サーバー秘密キーで、PEM 形式。インストール時にこのファイルに入っているサンプル・キーは、生成した正当なキーで置き換える必要があります。
UNIX 用 : `certificate-file = /opt/intraverse/lib/certs/svrcert.p12` **Windows 用 :** `certificate-file = C:¥Program Files¥ibm¥Policy Director¥lib¥certs¥svrcert.p12`	
	CA から取得した X.509 サーバー証明書で、 PKCS#12 形式。 ファイルには秘密キーが含まれています。このファイルに入っているサンプル証明書とキーは、トラステッド CA からの正当な証明書とキーで置き換える必要があります。
UNIX 用および Windows 用: **pass-key =***passphrase*	
	秘密キー・ファイルをロック解除する場合に使用されるキー・パスワード (*passphrase*)。

証明書の処理を構成する

iv.conf 構成ファイルの [wand] スタンザには、クライアント側 X.509 証明書を処理するためのパラメーターが入っています。**verify-clients** パラメーターを設定することによって、WebSEAL でクライアント側 X.509 証明書を処理する方法を指定できます。verify-clients の値として使用できる値には、次のものがあります。

値	説明
never	クライアントに X.509 証明書を要求しません。ユーザー名とパスワードを使用して、クライアントに強制的にアクセスさせます。
optional	クライアントに X.509 証明書を要求し、提供されたら、証明書ベースの認証を使用します。クライアントが証明書を提示しない場合は、クライアントに基本認証を強制的に使用させます。
required	クライアントに X.509 証明書を要求し、証明書ベースの認証を使用します。クライアントが証明書を提示しない場合は、接続を許可しません。

デフォルトでは、WebSEAL はクライアント側証明書を要求しません。

```
[wand]
verify-clients = never
```

SSL セッション・キャッシュ・タイムアウトを設定する

secmgrd.conf 構成ファイルの [ssl] スタンザには、静的 SSL セッション・キャッシュ・タイムアウトを設定するためのパラメーターが入っています。

WebSEAL では、内部的にクリデンシャル情報をキャッシュに入れます。このクリデンシャル有効期限パラメーターによって、許可 - クリデンシャル情報がメモリー内で WebSEAL 上にとどまる時間の長さが決まります。

このパラメーターは、非活動タイムアウトではありません。その値は、「クリデンシャルのタイムアウト」でなく「クリデンシャルの存続時間」にマップされます。その目的は、Policy Director が指定タイムアウト限度に達した時点で、ユーザーに強制的に再認証させることによって、セキュリティーを増強することにあります。

デフォルトのキャッシュ・タイムアウト (秒数) は次のとおりです。

```
[ssl]
ssl-cache-timeout = 3600
```

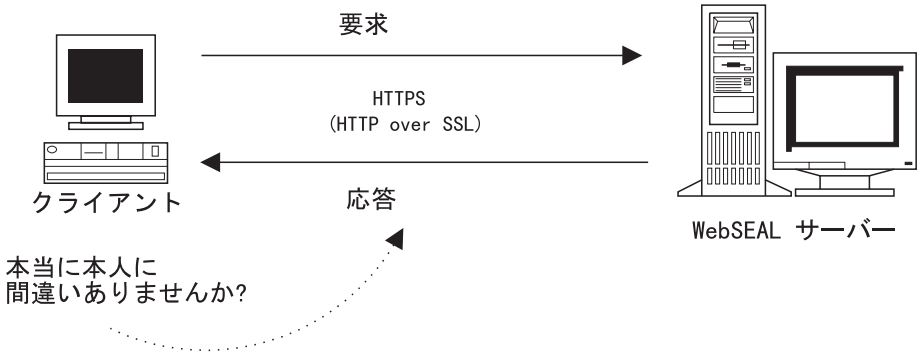
この値を調整して、サーバーが処理する必要がある SSL 要求の量に応じて、サーバーのパフォーマンスとユーザーの便宜とのバランスを図ります。

注: ブラウザーによっては、自動セッション再折衝を実行するものもあります。これに該当するブラウザーを使用している場合は、このパラメーターは無効です。

サーバー側証明書を WebSEAL 用として設定する

Policy Director WebSEAL サーバーは、SSL 使用可能クライアントがサーバーの認証性を検証できるように設定できます。 この節では、PEM 形式でサーバー側証明書をセットアップする場合に必要な管理タスクを説明していきます。

具体的には、このタスクには、有効な CA や内部的に制御された証明書生成プロダクトへの登録が伴います。登録では、 Policy Director が SSL 使用可能ブラウザーからの応答を正しく受け入れて、それに応答できるようにするサイト・サーバー証明書を取得する必要があります。

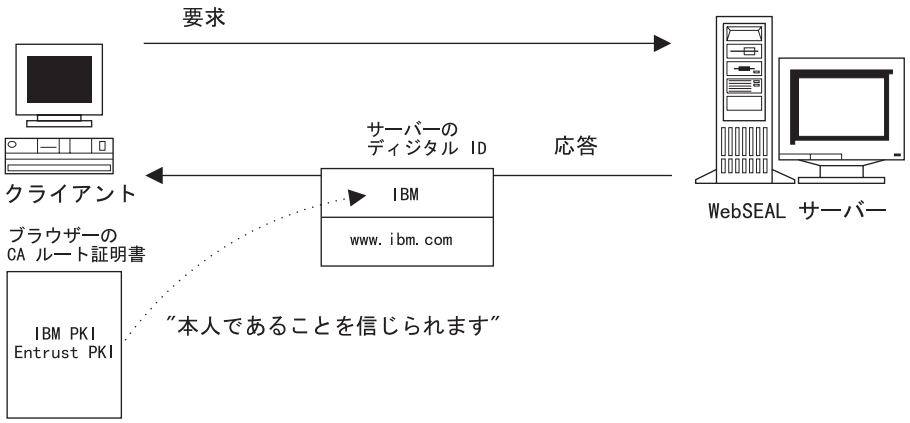


SSL を介するセキュア通信を確保する

Policy Director WebSEAL サーバーでは、「HTTP over SSL」 (HTTPS) を使用してアクセスするクライアントの認証をサポートします。WebSEAL には、これらのクライアントに応答する場合に使用するサーバー側公開 X.509 証明書がインストールされている必要があります。この X.509 証明書では、WebSEAL からの応答が許可サーバーからの着信であることをクライアントに証明します。

インターネットを介するセキュア SSL 通信の場合は、ブラウザーがサーバーを認証する必要があります。ブラウザーでは、サーバーの公開キー証明書を、一致するルート CA 証明書に突き合わせてチェックして認証します。一致する CA 証明書は、ブラウザーに組み込まれているか、ブラウザーによって取得されるかどちらかです。

CA が署名した許可サーバー証明書の場合は、偽名の可能性が防止できます。



WebSEAL には、出荷時にサンプル IBM 認証局の署名があるサンプル・サーバー証明書が付属しています。このサンプル証明書を使用すると、WebSEAL は SSL 使用可能ブラウザー要求に応答できます。ただし、サンプル証明書には IBM ルート CA 証明書が含まれていないため、ブラウザーがサンプル証明書を検証することはできません。 したがって、真のセキュア通信を提供するものではありません。

SSL を介するセキュア通信を確保するためには、トラステッド認証局からのサイト・サーバー証明書の登録が非常に大切です。サイト・サーバー証明書は、認識されている CA から取得するか、ソフトウェア (たとえば、IBM SecureWay Trust Authority など) を使って、独自の″企業内″ 証明書を生成できます。

SSL を介する通信用として Policy Director を設定する場合は、次のタスクが必要です。

- 『公開キーと秘密キーを生成する』
- 171ページの『gencsr ユーティリティーを使用する (オプション)』 (オプション)
- 173ページの『CSR を認証局に登録する』
- 173ページの『サーバー証明書をインストールする』
- 173ページの『セキュリティー・マネージャー構成ファイルを更新する』
- 174ページの『新規証明書のインストールをテストする』

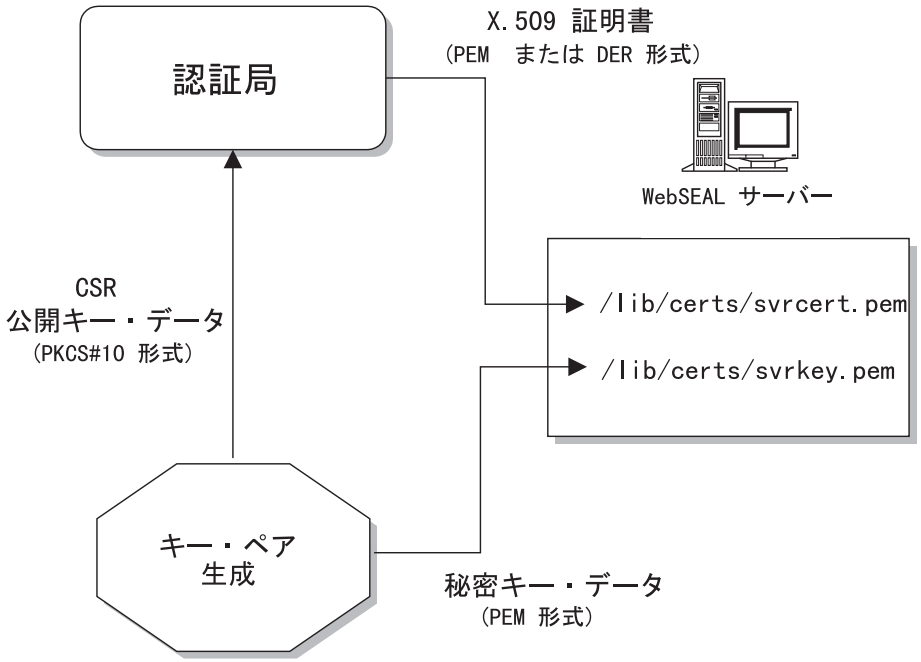
公開キーと秘密キーを生成する

CA からサイト・サーバー証明書を取得する場合は、まず最初にサーバーの公開 / 秘密キー・ペアを生成する必要があります。

秘密キー部分を保持します。

公開キー部分は、ユーザー識別情報を含み、証明書署名要求 (CSR) と呼ばれています。CSR は、サイト・サーバー証明書の登録時に CA に送信する必要がある情報です。CA ではこの情報を使用して、SSL 使用可能クライアントに応答する場合に使用される X.509 サーバー側証明書を構成します。

秘密キーと CA からのサーバー側 X.509 証明書は、保管位置を特に指定して保管する必要があります。これらの位置は、Policy Director の secmgrd.conf 構成ファイルで定義します。



公開キーと秘密キーのペアを生成する場合は、CA によって提供される生成ツールと命令を使用します。 Policy Director には、他に使用可能なユーティリティーがないときに使用できるユーティリティー (**gencsr**) があります。 **gencsr** を使用してキー・ペアを生成するタスクについては、『gencsr ユーティリティーを使用する (オプション)』で説明します。

gencsr ユーティリティーを使用する (オプション)

Policy Director には、公開キーと秘密キーのペアを生成する、オプション・ユーティリティーの **gencsr** ユーティリティーが組み込まれています。 このユーティリティーは、Policy Director インストールの一部で、/bin ディレクトリーに入っています。

UNIX: *install-path*/bin/gencsr

Windows: *install-path*¥bin¥gencsr

PKCS#10 形式

gencsr ユーティリティーでキー・ペアを生成します。このユーティリティーでは、秘密キー情報を PEM 形式でファイルに書き込みます。このユーティリティーでは、他の証明書署名要求情報と共に、公開キーを 1 つのファイルに保管します。 このユーティリティーでは、公開キー情報は PKCS#10 形式で保管されます。

公開キー暗号標準 (PKCS) に証明要求の構文が記述されています。証明要求は、識別名、公開キー、オプションの一組の属性で構成され、証明を要求する組織がこれらを一括して署名してあります。証明書署名要求は、認証局に送信されます。そこで、CA がサーバー用として固有の X.509 公開キー証明書を生成します。

gencsr ユーティリティー・コマンド構文

`gencsr [-csrfile csr_filename] [-keyfile key_filename] [-keylen key_length] [-version]`

オプション	説明
-csrfile	ファイルへの公開キー出力を指定します (PKCS#10 形式)。指定されたファイル (*csr_filename*) には、情報交換用米国標準コード (ASCII) 形式で CSR が収容されます。デフォルトでは標準出力です。
-keyfile	ファイルへの秘密キー出力を指定します (PEM 形式)。デフォルトでは標準出力です。
-keylen	公開 / 秘密キー・ペアのキーの長さ (バイト数) を指定します。デフォルトでは 512 です。
-version	ユーティリティーのバージョン番号と著作権情報を表示します。
-help	コマンド構文とオプション記述を表示します。

Gencsr ユーティリティーの手順

Policy Director **gencsr** ユーティリティーを使用する場合は、次のようにします。

1. CSR ファイルと秘密キー・ファイルの名前、およびオプションでキーの長さの適当な引き数を指定して、**gencsr** ユーティリティーを開始します。

   UNIX: `$ gencsr -csrfile filename -keyfile filename -keylen 1024`

   Windows : `gencsr -csrfile filename -keyfile filename -keylen 1024`

   公開キーと秘密キーについては、どんなファイル名を使用しても構いません。後段のステップで名前変更します。

   注: デフォルトのキーの長さは 512 バイトです。

2. ユーティリティーがプロンプトを出して、個人情報 (これには、 *PEM パスフレーズ* が含まれる) の入力を指示します。

   このパスフレーズは記憶しておく必要があります。 このパスフレーズは、後段のステップで secmgrd.conf 構成ファイルに保管します。このパスフレーズは、秘密キーに対する保護になります。

3. ユーティリティーが CSR ファイルと秘密キー・ファイルを生成します。 173ページの『CSR を認証局に登録する』では、CSR を認証局に送信する方法を説明します。

4. Policy Director に付属のサンプル秘密キー・ファイルをバックアップします。

   UNIX: `# cp svrkey.pem svrkey.pem.orig`

   Windows: `copy svrkey.pem svrkey.pem.orig`

5. 新規に生成された秘密キー・ファイルをこのサンプル・ディレクトリーに保管して、svrkey.pem という名前を付けます。

   UNIX: `# cp newkey.txt svrkey.pem`

   Windows: `copy newkey.txt svrkey.pem`

注: この秘密キーは保護する必要があります。秘密キーのインスタンスは、 1 つだけ必要であり、このことがクライアントとサーバーの間の通信を検証する上で、非常に重要なことです。

CSR を認証局に登録する

CSR を認証局に登録する場合は、次のようにします。

1. 認証局には一般的にオンライン登録書式があります。Web ブラウザーを使用して、この書式に記入します。正確な手順は、CA によって異なります。
2. 登録書式では、170ページの『公開キーと秘密キーを生成する』や 171ページの『gencsr ユーティリティーを使用する (オプション)』で生成された CSR の提供を必要とします。CSR ファイルの内容を書式に貼り付けてもよいし、ファイルを E-mail で送信しても構いません。
3. CA が新規 X.509 サーバー側公開証明書を PEM 形式で送信してきます。これには数日かかる場合があります。

WebSEAL では、PEM 形式で証明書を必要とします。PEM のエンコードは、バイナリー証明書に適用される base64 変換です。PEM 形式は、行の長さが 1 行につき 64 文字に制限されている ASCII ファイルです。この ASCII ファイルは次の文章で開始し、

```
-----BEGIN CERTIFICATE----
```

次の文章で終了します。

```
-----END CERTIFICATE----
```

サーバー証明書をインストールする

サーバー証明書をインストールする場合は、次のようにします。

1. Policy Director に付属のサンプル・サーバー証明書ファイルをバックアップします。

   PEM 形式の場合:

   UNIX: `# cp svrcert.pem svrcert.pem.orig`

   Windows: `copy svrcert.pem svrcert.pem.orig`
2. CA からの新規サーバー証明書ファイルをこの同じディレクトリーに保管して、svrkey.pem という名前を付けます (以前の値に上書きします)。

   UNIX: `# cp newcert.txt svrcert.pem`

   Windows: `copy newcert.txt svrcert.pem`

セキュリティー・マネージャー構成ファイルを更新する

secmgrd.conf 構成ファイル内の次の項目をチェックし、必要に応じて更新します。

`certificate-file =`	CA から受信された PEM 定様式証明書が入っているファイルのパス名 デフォルト : lib/certs/svrcert.pem
`key-file =`	ローカルで生成された秘密キー・ファイルのパス名 デフォルト : lib/certs/svrkey.pem

pass-key =	秘密キーを保護する場合に使用する PEM パスフレーズ

certificate-file 項目と key-file ファイル項目を変更するのは、一覧表示されているデフォルトのファイル名以外のファイル名を使用するときだけにします。

新規証明書のインストールをテストする

新規証明書インストールをテストする場合は、次のようにします。

1. Policy Director をいったん停止してから再始動して、新規証明書の使用を開始します。

   UNIX:

   ```
   # /etc/init.d/iv stop
   # /etc/init.d/iv start
   # /etc/init.d/iv status
   ```

   Windows: サービス制御パネルを使用します。

2. セキュリティー・マネージャー (secmgrd) が正常に開始しているか確認します。

   secmgrd が正常に開始していない場合は、次のログ・ファイルをチェックして、正常に開始しなかった理由を調べます。

   UNIX: *install-path*/secmgr/log/secmgrd.log

   Windows: *install-path*¥secmgr¥log¥secmgrd.log

   意味のあるエラー・メッセージが見つからないときは、デバッグ・モードで secmgrd を手動で開始します。154ページの『メッセージを標準出力に送信する場合のデバッグ・モード』を参照してください。 また、以下の IBM SecureWay Policy Director Web サイトで、問題の訂正に関する最新情報を見つけることもできます。

   http://www.ibm.com/software/security/policy/library

3. ブラウザーから、HTTPS を使用するサーバーに接続し、ブラウザーがサーバー証明書を受け入れるか確認します。

   たとえば、ブラウザーでは、広く認識されている VeriSign ルート証明書を、すでにデフォルトで保管しているはずです。したがって、警告メッセージやダイアログ・ボックスが、Policy Director のログイン・プロンプトに先立って表示されることはないはずです。

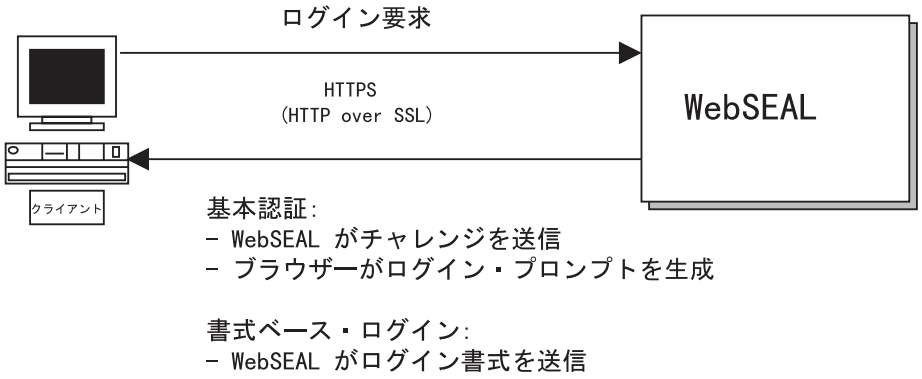
   Policy Director に付属のサンプル証明書を使用した場合は、警告メッセージが表示されます。 警告メッセージが表示される理由は、ブラウザーには IBM ルート証明書が入っていないので、サンプル・サーバー証明書を検証できないからです。このようなメッセージは、サーバー証明書を受け入れるか、リジェクトするかを決めるよう指示するプロンプトです。 ルート証明書がないので、ブラウザーでは、サーバー証明書の正当性を検証できません。したがって、証明書を受け入れるか、否認するかの責任をユーザーに渡す必要があります。

   これで、トラステッド認証局によって妥当性を検証されたサイト・サーバー証明書が存在することになります。妥当性を検証されたサーバー証明書が存在すれば、 SSL 使用可能クライアントでは、Policy Director WebSEAL サーバーを正常かつ確実に認証できます。

ユーザー名とパスワードによる認証方式

ケルベロスと LDAP 機密キー認証メカニズムでは、ユーザー名とパスワードの形式によるクライアント識別情報を必要とします。 WebSEAL では、認証用としてユーザー名とパスワードを示す方式として、次の 2 つをサポートします。

- 『基本認証方式』
- 177ページの『Policy Director 書式ベース・ログイン方式』



基本認証方式

WebSEAL では、ユーザー名やパスワードなどのユーザー情報を入手する場合は、Netscape® Communicator/Netscape Navigator® と Microsoft Internet Explorer™ (IE) で使用されている SSL プロトコルをサポートします。規約により、URL がセキュア SSL 接続の使用を反映する場合は、 **http:** ではなく、**https:** で始めることになっています。

ログインが正常に行われるためには、Policy Director では、クライアントがセキュリティー・レジストリーに記録されている Policy Director 識別を使用することを必要とします。 *基本認証* は、認証メカニズムにユーザー名とパスワードを示すための標準方式です。

最初のステップで、サーバーは、そのサーバー側証明書を使用して、クライアントに対して認証します。 クライアントがこの証明書を受け入れた場合は、サーバーは、クライアントに対してチャレンジを発行します。 ブラウザーがログイン・プロンプトを出して、ユーザー名とパスワードを要求します。

注: ブラウザーでは、このログイン情報をキャッシュに入れます。標準基本認証の場合は、後続の要求ごとにそれぞれユーザー名情報とパスワード情報が必要です。 キャッシュ認証情報の送信は、ユーザーには無関係で行われます。

基本認証に関する重要な点は、次のとおりです。

- Policy Director は、SSL をセキュア通信チャネルとして使用する。
- Policy Director は、セキュア SSL チャネルを通して、ユーザー名とパスワードを伝送する。

基本認証チャレンジの結果として、次のようなログイン・プロンプトが表示される場合があります。

```
Enter username for Policy Director [/.../www.ibm.com] at www.ibm.com
User Name:
Password:
```

ここで、**User Name** フィールドと **Password** フィールドに必要な情報を入力する必要があります。

基本認証モデル

基本認証モデルのプロセスには、次のことが含まれます。

1. クライアント・ブラウザーが、SSL を使用してサーバーに連絡します。
2. サーバーが、CA から取得した署名公開キー・サーバー証明書を返送します。
3. クライアントが、次のアクションのどれか 1 つを起こします。
   - そのデータベース内で対応するルート CA 証明書を検出して、サーバーの証明書を受け入れる。
   - そのデータベース内に対応するルート CA 証明書がないので、警告によってユーザーにプロンプトを出す。これで、証明書を受け入れるか、リジェクトするかは、ユーザーの責任で行うことになります。
4. 受け入れられた場合は、サーバーがブラウザーにチャレンジを発行します。
5. ブラウザーは、ログイン・プロンプトを出して応答し、ユーザー名とパスワードを要求します。
6. ユーザーがユーザー名とパスワード情報を入力すると、ブラウザーはその情報を Policy Director サーバーに送信します。
7. ユーザー名情報とパスワード情報が、Policy Director のユーザー・レジストリー内の既存の情報と一致したときは、Policy Director が証明を生成します。Policy Director では、この証明を使用して、認証決定を行います。 WebSEAL では、SSL セッションの期間中、この証明をキャッシュに入れておきます。
8. ブラウザーが、ユーザー名情報とパスワード情報をキャッシュに入れます。

   標準基本認証では、後続のブラウザー・ログインや要求ごとに、それぞれこのユーザー名とパスワードを必要とします。この要件は、キャッシュ認証情報の使用によって透過的に満たされます。

   注: 基本認証では、ブラウザーがユーザー名情報とパスワード情報をキャッシュに入れるため、**pkmslogout** コマンドは正しく働きません。 完全にログアウトするためには、ブラウザー・セッションをクローズする必要があります。**pkmslogout** 機能が必要な場合は、書式ベース・ログイン方式を使用します。

必須管理タスク

管理者は次のタスクを実行して、基本認証モードでの SSL アクセスに備えて、WebSEAL サーバーを準備する必要があります。

- WebSEAL サーバーにサーバー側 X.509 証明書をインストールする。
- セキュア・ドメインに参加する各ユーザーごとに、それぞれ Policy Director アカウントを作成する。

Policy Director 書式ベース・ログイン方式

Policy Director には、標準基本認証メカニズムに代わる方式として、 Policy Director 書式ベース・ログイン が用意されています。この方式によれば、基本認証チャレンジの結果として標準ログイン・プロンプトが出るのではなく、 Policy Director からの HTML ログイン書式が出ます。

書式ベース・ログインを使用すると、基本認証の場合のように、ブラウザーがユーザー名情報とパスワード情報をキャッシュに入れることはありません。 したがって、特殊 SSL セッション・ログアウト・コマンドである、**pkmslogout** が正常に使用できます。 Policy Director が証明情報を必要とする (そして、キャッシュに入れる) のは 1 回だけであるため、ブラウザー要求のつどログイン要求を繰り返す必要はありません。

iv.conf 構成ファイルの [wand] スタンザ内の **https-forms-auth** パラメーターを使用して、書式ベース・ログインを実行します。このパラメーターは、yes か no に設定できます。デフォルトでは、no です。

```
[wand]
https-forms-auth = no
```

Policy Director には、7 つのサンプル HTML 書式が組み込まれています。これらの HTML 書式をカスタマイズして、サイト固有のメッセージを含めたり、サイト固有のアクションを実行したりすることができます。

iv.conf 構成ファイルの [wand] スタンザには、SSL HTML Page Locations のもとで、これらの書式のファイル位置が定義されています。

デフォルトのディレクトリー位置は、次のとおりです。

UNIX: *install-path*/www/lib/html/

Windows: *install-path*¥www¥lib¥html¥

書式	説明
login.html	ユーザー名とパスワードの要求
login_rep.html	ログイン・エラー・メッセージ
logout.html	SSL セッションからのログアウトが正常に行われたことを示すメッセージ
passwd.html	パスワード変更書式
passwd_exp.html	パスワード有効期限切れメッセージ
passwd_rep.html	パスワード変更エラー・メッセージ
help.html	コマンド解説

これらのページで使用できるマクロも 2 つあります。これらのマクロ・ストリングは、テンプレート・ファイルに入れることができます。ルーチンによって、適当な値が動的に置換されます。

マクロ	説明
%USERNAME%	ログインしたユーザーの名前

%ERROR%	Policy Director から戻されたハード・コーディング・エラー・メッセージ

書式ベース認証モデル

書式ベース認証モデルは、次のプロセスに従います。

1. クライアント・ブラウザーが、SSL を使用してサーバーに連絡します。
2. サーバーが、CA から取得した署名公開キー・サーバー証明書を返送します。
3. クライアントが、次のアクションのどれか 1 つを起こします。
   - そのデータベース内で対応する CA 証明書を検出して、サーバーの証明書を受け入れる。
   - そのデータベース内に対応するルート CA 証明書がないので、警告によってユーザーにプロンプトを出す。これで、証明書を受け入れるか、リジェクトするかは、ユーザーの責任で行うことになります。
4. クライアントによって受け入れられると、WebSEAL は、カスタマイズされた Policy Director HTML 書式を使用して、クライアントにユーザー名とパスワードを示すよう指示するプロンプトを出します。

   Policy Director は、この書式を使用して、WebSEAL にユーザー名情報とパスワード情報を返送します。
5. ユーザー名情報とパスワード情報が、Policy Director のユーザー・レジストリー内の既存の情報と一致したときは、Policy Director がクリデンシャルを生成します。Policy Director では、認証決定にあたってこのクリデンシャルを使用します。WebSEAL では、SSL セッションの期間中、このクリデンシャルをキャッシュに入れておきます。

   基本認証の場合とは異なり、ブラウザーがユーザー名情報とパスワード情報をキャッシュに入れることは *ありません*。したがって、**pkmslogout** コマンドが正しく働きます。

必須管理タスク

管理者は次のタスクを実行して、書式ベース・ログイン・モードでの SSL アクセスに備えて、WebSEAL サーバーを準備する必要があります。

1. WebSEAL サーバーに X.509 サーバー側 CA 証明書をインストールする。
2. セキュア・ドメインに参加する各ユーザーごとに、それぞれ Policy Director アカウントを作成する。
3. Policy Director 書式をカスタマイズし、その位置を iv.conf 構成ファイル内に定義する。

ユーザー名とパスワードによる方式用のコマンド

Policy Director には、SSL 使用可能クライアントがユーザー名とパスワードによる方式を使用して認証するのをサポートするために、次のコマンドが用意されています。

- pkmslogout
- pkmspasswd

pkmslogout

現行 SSL セッションからログアウトする場合は、pkmslogout コマンドを使用します。このコマンドは、書式ベース・ログイン方式での使用に適しています。

```
https: //Web URL install-path/pkmslogout
```

たとえば、次のとおりです。

```
https: /www.ibm.com/pkmslogout
```

このログアウトに対する応答として表示されるファイルは、iv.conf 構成ファイル内に定義します。

```
# SSL HTML page locations
pkms-logout-page = lib/html/logout.html
```

logout.html ファイルは、要件に見合うように変更できます。

pkmslogout ユーティリティーでは、ユーザーが明らかに異なるバックエンド・システムからログアウトする場合のために、ネットワーク体系で別の終了画面を必要とするときは、複数ログアウト応答ページもサポートします。

次の式によって、特定の応答ファイルを識別します。

```
https://pkmslogout?filename=custom_logout_file
```

ただし、*custom_logout_file* は、ログアウト応答のファイル名です。このファイルは、デフォルトの logout.html ファイルを入れるために定義されているものと同じ /lib/html/ ディレクトリーに常駐する必要があります。

pkmspasswd

パスワードを変更する場合は、このコマンドを使用します。

```
https://Web URL install-path/pkmspasswd
```

たとえば、次のとおりです。

```
https://www.ibm.com/pkmspasswd
```

X.509 証明書による認証方式

WebSEAL では、SSL を介するクライアント側 X.509 証明書の使用による認証をサポートします。X.509 証明書では、ユーザー名とパスワードではなく、クライアントの識別情報を示します。

クライアント側 X.509 証明書サポートのセットアップ・タスク

次のタスクを実行して、クライアント側 X.509 ディジタル証明書を受け入れるための WebSEAL をセットアップします。

クライアント・タスク

クライアント・タスクを実行する場合は、次のようにします。

1. X.509 クライアント側ディジタル証明書 (署名公開キー) を CA から取得します。
2. クライアント・システムに証明書をインストールします。

WebSEAL サーバー・タスク

WebSEAL サーバー・タスクを実行する場合は、次のようにします。

1. 同一認証局のルート CA 証明書を取得します。

   この証明書は、PEM 形式でも PKCS#12 形式でも構いません。

2. ルート CA 証明書をシステム上の該当する位置にコピーし、 secmgrd.conf 構成ファイル内にこの位置を示します。

   PEM 形式 :

   ルート証明書を次のファイルに追加します。

   UNIX:`ca-cert-file = lib/certs/cacert.pem`

   Windows: `ca-cert-file = lib¥certs¥cacert.pem`

   PKCS#12 形式 :

   各ルート証明書を別々のファイルとして、次のディレクトリーに追加します。

   UNIX: `ca-cert-p12-dir = lib/certs/ca_p12`

   Windows: `ca-cert-p12-dir = lib¥certs¥ca_p12`

   注: これらの PEM 形式および PKCS#12 形式の証明書は、Policy Director が信任をおく認証局の証明書です。

3. **verify-clients** パラメーターを設定することによって、WebSEAL がクライアント側 X.509 証明書を処理する方法を指定します。許容されている verify-clients 値 (never、optional、required) の 1 つを、iv.conf 構成ファイルの `[wand]` スタンザに入力します。

   これらの値については、168ページの『証明書の処理を構成する』を参照してください。

4. iv.conf ファイルを編集し、必要に応じて [authentication-mechanisms] スタンザの **cert-cdas** パラメーターを該当するプラットフォームに合わせて変更することによって、CA サーバーを使用するように WebSEAL を構成します。

   ```
   [authentication-mechanisms]
   cert-cdas = &entry=/.:/subsys/intraverse/cdas/servers/hostname
   ```

   cas module の選択項目には、cdasauthn.dll (Windows NT の場合)、libcdasauthn.a (AIX の場合)、および libcdasauthn.so (Solaris の場合) が含まれます。

   cert-cdas パラメーターの詳細については、182ページの『Policy Director CAS の基本構成』を参照してください。

5. secmgrd.conf 構成ファイルの **certificate-file** および **key-file** パラメーターを使って、サーバー識別を定義します。ただし、サーバー秘密キーの形式は PEM 形式です。パラメーターは、使用しているプラットフォームによって異なります。

   PEM 形式の certificate-file パラメーターの場合:

   UNIX: `certificate-file = /opt/intraverse/lib/certs/svrcert.pem`

   Windows: `certificate-file = C:¥Program Files¥ibm¥Policy Director¥lib¥certs¥svrcert.pem`

   PEM 形式の key-file パラメーターの場合:

   UNIX: `key-file = /opt/intraverse/lib/certs/srvkey.pem`

Windows: `key-file = C:¥Program Files¥ibm¥Policy Director¥lib¥certs¥srvkey.pem`

secmgrd.conf 証明書ストーレッジ・パラメーターについては、167ページの『証明書を保管する』を参照してください。

6. secmgrd.conf 構成ファイルの certificate-file パラメーターを使ってサーバー識別を定義します。ただし、サーバー証明書の形式は PKCS#12 形式です。

   PKCS#12 形式の certificate-file パラメーターの場合:

   UNIX 用 : `certificate-file = /opt/intraverse/lib/certs/svrcert.p12`

   Windows 用 : `certificate-file = C:¥Program Files¥ibm¥Policy Director¥lib¥certs¥svrcert.p12`

7. クリデンシャル取得とマッピング用には、Policy Director クリデンシャル取得サービス (CAS) を使用します。

   また、独自のクリデンシャル取得 / マッピング・サービス・プログラムを作成して、サーバー・システムにインストールしても構いません。 詳しくは、 *Policy Director Programmer's Guide and Reference* と 『Policy Director クリデンシャル取得サービスの構成』を参照してください。

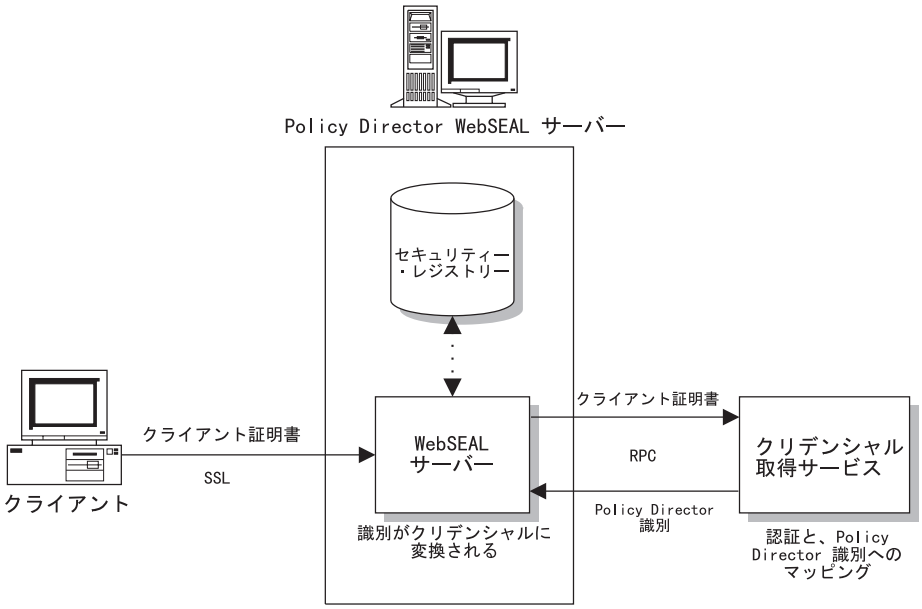
Policy Director クリデンシャル取得サービスの構成

Policy Director のクリデンシャル取得サービス (CAS) は、カスタマイズ可能なコンポーネントの 1 つで、WebSEAL でサポートされている標準認証メカニズムを拡張する場合に使用できます。 デフォルトの Policy Director クリデンシャル取得サービスは cdas_server(.exe) ファイルを使用します。182ページの『Policy Director CAS を使用するための WebSEAL の構成』を参照してください。

また、独自のクリデンシャル取得 / マッピング・サービス・プログラムを作成して、サーバー・システムにインストールしても構いません。 クリデンシャル取得サービスの作成とインストールについては、*Policy Director Programmer's Guide and Reference* を参照してください。

Policy Director CAS の概要

Policy Director クリデンシャル取得サービス (CAS) を使用すると、ユーザー識別情報 (X.509 証明書など) の認証と、Policy Director ユーザー識別へのマッピングが可能になります。セキュリティー・マネージャーが (そのデフォルト・レジストリーを使用して)、このユーザー識別に関するクリデンシャルを戻します。



Policy Director CAS については、32ページの『Policy Director によって提供される CAS』と 『Policy Director CAS を使用するための WebSEAL の構成』を参照してください。

Policy Director CAS を使用するための WebSEAL の構成

WebSEAL によってサポートされる認証メカニズムはすべて、 iv.conf 構成ファイル内の authentication-mechanisms スタンザ内で構成できます。WebSEAL によってサポートされる認証メカニズムはすべて、ローカル (処理中) 認証機能と、CAS サーバーによって有効にされる、カスタマイズされている場合もある、リモート認証機能の両方を表します。

ローカル・プラグイン・モジュール

構成ファイル内で、各認証機能をそれぞれローカル・プラグイン・モジュールに対応づけます。 UNIX プラットフォームでは、これらのモジュールは共用ライブラリーです。 Windows NT では、これらのモジュールは動的リンク・ライブラリー (DLL) です。 これらのモジュールは、Policy Director 配布の標準部分として提供されるため、カスタマイズはできません。

Policy Director には、標準プラグイン・モジュールが用意されています。第三者 CAS サーバーとのインターフェースをとる場合は、この標準プラグイン・モジュールを使用します。

プラットフォーム	CAS モジュール名
Solaris	libcdasauthn.so
AIX	libcdasauthn.a
Windows NT	cdasauthn.dll

Policy Director CAS の基本構成

X.509 認証情報に応答する Policy Director クリデンシャル取得サービス (CAS) を構成することができます。このサービスにより、 WebSEAL CAS インターフェースの

クライアント側の認証が行われます。Policy Director CAS 構成には、 CAS サーバーのバインディング情報が格納される DCE CDS ネームスペース内での位置を表す追加の引き数が必要です。

CAS サーバーを使用するよう WebSEAL を構成するには、iv.conf ファイルを編集して、 [authentication-mechanisms] スタンザ内の cert-cdas パラメーターを、該当するプラットフォームの必要に合わせて変更してください。

たとえば、次の構成シーケンス (Windows NT の場合) では、X.509 証明書ベースの認証をサポートする単一の CAS サーバーを識別します。

```
[authentication-mechanisms]
cert-cdas = cdasauthn.dll&entry=/.:/subsys/intraverse/cdas/servers/hostname
```

この場合、cdasauthn.dll は該当するプラットフォームの CAS モジュールを表し、*hostname* は単純なホスト名であり、
&entry=/.:/subsys/intraverse/cdas/servers/*hostname* は、 CAS サーバーのバインディング情報が格納される DCE CDS ネーム・スペース内での位置を表します。

構成項目の構文

認証構成項目には、次の形式が使用されます。

authn-mechanism = *module*[&*arg1*[*arg2*]...[*argN*]]

複数の Policy Director CAS サーバー

単一の Policy Director CAS で複数の認証メカニズムがサポートできます。この場合は、各メカニズムで構成情報が重複しています。

識別名のマッピング

Policy Director CAS は、 SSL 使用可能ブラウザーからのクライアント・ディジタル *証明書* を、 Policy Director ユーザー識別にマップします。保護された Web ページにユーザーがアクセスしようとすると、 SSL 使用可能ブラウザーは WebSEAL サーバーに連絡します。WebSEAL がクライアント証明書ベース認証用に構成されている場合、 WebSEAL はブラウザーに X.509 証明書を要求します。WebSEAL はブラウザーから証明書を受け取ると、それを CAS サーバーに渡します。Policy Director CAS は、受け取った証明書を、Policy Director が認識しているユーザー識別にマップしようとします。

Policy Director CAS cdas.conf 構成ファイル内で、Policy Director 管理者は、証明書識別名 (DN) を Policy Director ユーザーの DN に関連付けるのに使用されるテーブルを作成できます。 Policy Director CAS は、WebSEAL によって証明書で呼び出されると、証明書から DN を抜き出し、一致がないか、このテーブルを調べます。一致が見つかると、 Policy Director CAS は、関連付けられた Policy Director ユーザーの正しい形式の DN を WebSEAL に返します。この方式が、 *DN マッピング* と呼ばれているものです。

この場合、WebSEAL は、この DN を使用して Policy Director ユーザーを識別します。一致が見つからないと、CAS は証明書からの DN を WebSEAL に返します。この場合は、 Policy Director ユーザーを識別するのに、証明書の DN が使用されます。WebSEAL サーバーは、返された DN を使用して、ユーザーのクリデンシャルを検索します。

識別名をマップするための cdas.conf 構成ファイルは、次の場所にあります。

UNIX: `/opt/intraverse/cdas_server/lib/cdas.conf`

Windows: `C:¥Program Files¥IBM¥Policy Director¥cdas_server¥lib¥cdas.conf`

cdas.conf 構成には、次の情報が含まれています。

```
# DN mapping
# If the certificate DN is in the following table, use the corresponding LDAP
# DN.  Otherwise, use the certificate DN as is.
# Each entry should be on a single line with the following format:
# [DN in the certificate] LDAP DN to map to
# For example:
# [/C=US/O=IBM/CN=Policy Director User] cn=Policy Director User,o=IBM,c=US
# [/C=US/O=IBM/CN=User1] cn=IBM Policy Director User,o=IBM,c=US
```

証明書識別名 (DN) は、常に、テーブルの左側に、大括弧で囲んで示されます (たとえば、`[/C=US/O=IBM/CN=Policy Director User]`)。Policy Director ユーザーの DN (LDAP レジストリー DN と同様) は、常に、テーブルの右側に示されます (たとえば、 `cn=Policy Director User,o=IBM,c=US`)。Policy Director ユーザーの DN は、必ず、証明書 DN の右括弧 ( ]) の後に必須スペースが 1 つ入ってから続きます。機能が正しく働くためには、マッピング・テーブル項目の両側が記入されている必要があります。

SSL 使用可能ブラウザー (たとえば、Netscape® Communicator/Netscape Navigator®、Microsoft Internet Explorer™) を使用すると、証明書 DN 情報を表示させることができます。これらのブラウザーでの DN 情報の表示方法は異なる場合がありますが、両方のブラウザーの証明書情報には、すべての識別名の要素が含まれているはずです。

第14章 WebSEAL: 一般管理タスク

この章には、使用するネットワークに合わせて WebSEAL をカスタマイズする場合に実行できる、一般管理タスクと構成タスクを記述する情報が記載されています。

この章は、次の各節に分かれています。

- このページの 『WebSEAL セキュリティーを使用可能 / 使用不可にする』
- 『Web スペースを管理する』
- 188ページの『HTTP と HTTPS のワーカー・スレッドを構成する』
- 190ページの『タイムアウト・パラメーターを指定する』
- 191ページの『HTTP エラー・メッセージを構成する』

WebSEAL セキュリティーを使用可能 / 使用不可にする

WebSEAL を使用可能 / 使用不可にする場合は、 **ivadmin** ユーティリティーを使用します。

特定の Policy Director サーバー上で WebSEAL を使用可能にする場合は、次のようにします。

```
ivadmin> server enable /WebSEAL/
```

ただし、*hostname* は、サーバーの名前からドメイン名を除いたものです。

サービスがすでに使用可能になっているときや、サービス仕様が無効のときは、 Policy Director はエラーを戻します。

デフォルトでは、Policy Director は WebSEAL を使用可能にします。

特定の Policy Director サーバー上で WebSEAL を使用不可にする場合は、次のように **ivadmin server disable** コマンドを使用します。

```
ivadmin> server disable /WebSEAL/
```

WebSEAL サーバー状況をチェックする場合は、**ivadmin server status** コマンドを使用します。

```
ivadmin> server status hostname
```

状況報告によって次の情報が表示されます。

- WebSEAL サーバーは使用可能か使用不可か
- WebSEAL サーバーは、PING を使用して到達可能かどうか
- WebSEAL 構成データベースの状態

Web スペースを管理する

この節では、WebSEAL ネームスペースを管理する場合に必要とされるタスクについて、次のものを含めて説明します。

- 186ページの『Web 文書ツリー位置を指定する』
- 186ページの『ディレクトリー索引付けを構成する』

- 187ページの『CGI プログラム用のファイル拡張子タイプを指定する』

Web 文書ツリー位置を指定する

Web 文書ツリー位置は、サーバーによって使用可能にされている文書に関する文書ツリーのルートへの絶対パスです。デフォルト位置は、セキュリティー・マネージャーのインストール時に初期確立されます。

UNIX: *install-path*/www/docs

Windows: *install-path*¥www¥docs

この位置は、インストール・スクリプトによって変更できます。インストール後は、この位置を変更する場合は、**junctioncp** ユーティリティーを使用する必要があります。 完全なコマンド情報については、201ページの『junctioncp を使用してスマート接合を管理する』を参照してください。

次の UNIX の例は、**junctioncp** ユーティリティーを使用して位置を変更する方法を示しています。

1. **junctioncp** を実行します。

```
# junctioncp -e hostA
Attempting to bind to hostA at
/.:/subsys/intraverse/secmgr/server/hostA
junctioncp>
```

2. **list** コマンドを使用して、現行接合点をすべて表示させます。

```
junctioncp> list
/
```

3. **show** コマンドを使用して、接合の詳細を表示させます。

```
junctioncp> show /
Junction point: /
Type: Local Root
Directory: /opt/intraverse/www/docs
```

4. 新規ローカル接合を作成して、現行接合点を置き換えます。

```
junctioncp> create -t local -d /tmp/docs /
WARNING: A junction already exists at /
Do you want to replace it [no]? yes
Created junction at /
```

5. 新規接合点を一覧表示させます。

```
junctioncp> list
/
```

6. この接合の詳細を表示させます。

```
junctioncp> show /
Junction point: /
Type: Local Root
Directory: /tmp/docs
```

ディレクトリー索引付けを構成する

サーバーによって戻されるデフォルト・ファイルの名前を指定できます。これを指定するのは、ディレクトリー名を URL として示す場合です。このデフォルト・ファ

イルが存在していると、Policy Director がクライアントに戻します。存在していない場合は、 Policy Director がディレクトリー索引を動的に生成して、クライアントに戻します。

注: Policy Director が生成した索引をディスクに保管することはありません。Policy Director では、サーバーのワンドか dirindex (ディレクトリー索引) キャッシュから索引を取り出すか、ディレクトリーにアクセスされるたびに、索引を再生成するかどちらかです。

ディレクトリー索引付けを構成するためのパラメーターは、iv.conf 構成ファイルの [wand-indexing] スタンザに入っています。

デフォルト・ファイルの値は、次のとおりです。

```
[wand-indexing]
dirindex = index.html
```

サイトで使用している規則が異なれば、このファイル名を変更する必要がある場合もあります。

```
[wand-indexing]
dirindex = default.html
```

ディレクトリーの索引付けに使用される各パラメーターには、それぞれの文書タイプや MIME タイプが検出されるたびに表示されるデフォルトのアイコン (.gif ファイル) があります。

```
[wand-indexing]
image/*= /icons/image2.gif
video/* = /icons/movie.gif
audio/* = /icons/sound2.gif
text/html = /icons/html.gif
text/* = /icons/text.gif
application/* = /icons/binary.gif
```

各パラメーターごとに他のアイコンを指定できます。また、リモートでアイコンを見つけることもでき、URL をパラメーター値として使用することもできます。たとえば、次のとおりです。

```
application/* = http://www.acme.com/icons/binary.gif
```

CGI プログラム用のファイル拡張子タイプを指定する

iv.conf 構成ファイルの [wand-cgi-types] スタンザに入っているパラメーターを使用すると、Windows ファイル拡張子タイプを指定できます。 Policy Director では、CGI プログラムとして開始できる Windows ファイル拡張子タイプを認識します。

UNIX オペレーティング・システムには、ファイル名拡張子要件はありません。ただし、 Windows NT の場合は、ファイル拡張子タイプを定義する必要があります。[wand-cgi-types] スタンザには、有効な拡張子タイプがすべてリストされ、各拡張子を適当な CGI プログラムにマップしてあります (必要なとき)。

デフォルトでは、Policy Director が開始するのは、拡張子がスタンザに CGI プログラムとしてリストされているものに一致するファイルだけです。 デフォルトでは、Policy Director がプログラムとして実行するのは、拡張子が .exe のファイルであり、これらのファイルはマッピングを必要としません。 拡張子が解釈されたスクリプト・

ファイルを表す場合は、該当する解釈プログラムを提供する必要があります。 拡張子タイプの例としては、シェル・スクリプト (.sh と .ksh)、 Perl スクリプト (.pl)、Tcl スクリプト (.tcl) があります。

次の例には、代表的な [wand-cgi-types] スタンザ構成が示してあります。

```
#
# CGI file extension to command mappings (Windows NT Only)
#
# For WIN32 servers we nominate CGI file extensions and the program
# that is used to execute them. If a CGI has an extension that is not
# in this list then it is not executed.
#
[wand-cgi-types]
.exe =
.bat =
.cmd =
.pl = perl
.sh = sh
.tcl = tclsh76
```

注: .bat ファイルの使用には、重大なセキュリティー問題が伴います。 .bat ファイルは使用しないようにします。

HTTP と HTTPS のワーカー・スレッドを構成する

構成されたワーカー・スレッドの数で、サーバーがサービスできる同時着信要求の数を指定します。 すべてのワーカー・スレッドが使用中であると、Policy Director では、到着する他の接続については、ワーカー・スレッドが使用可能になるまでバッファーに入れておきます。

着信接続にサービスできる使用可能スレッドの数を指定できます。ワーカー・スレッドの数はパフォーマンスに影響する可能性があるため、その構成は注意深く行う必要があります。

この構成パラメーターが同時接続の数に上限を設けることはありません。このパラメーターで指定するのは、潜在的に無限の作業待ち行列にサービスするために使用可能にされるスレッドの数を指定するだけです。

ワーカー・スレッドの最適数の選択は、ネットワーク上のトラフィックの量とタイプについての理解度に左右されます。

スレッドの数を増やせば、一般的には、要求処理の完了にかかる平均時間が短縮されることになります。ただし、スレッドの数を増やすと、他の要因にも影響がおよび、そのためにサーバー・パフォーマンスに悪影響を生じる恐れがあります。

WebSEAL のワーカー・スレッド・プール値を設定する

WebSEAL には、単一の総称ワーカー・リストが保持され、TCP、SSL トンネル伝送、または GSS トンネル伝送を使用するクライアントからの要求を処理するための、ワーカー・スレッド・プールも保持されています。この拡張メカニズムがあるため、WebSEAL では、取り扱うロードが大幅に増えても、使用するシステム・リソースは少なくて済みます。

iv.conf 構成ファイルの [wand] スタンザ部分の worker-threads パラメーターを設定することによって、ワーカー・スレッド・プール・サイズを制御します。

```
worker-threads = 50
```

WebSEAL を HTTP 要求用として構成する

WebSEAL では、一般的に、認証されていないユーザーからの多数の HTTP 要求を処理します。たとえば、公開 Web サイトにある選択された資料に対しては、不明の (したがって、認証されていない) ユーザーからの読み取り専用アクセスを可能にすることが望ましい場合があります。

iv.conf 構成ファイルの [wand] スタンザには、TCP を介する HTTP 要求を処理するためのパラメーターが入っています。

HTTP listen を使用可能 / 使用不可にする

デフォルトでは、Policy Director は、TCP を介する HTTP 要求に関する listen を使用可能に (許可) します。

```
allow-tcp-http = yes
```

このパラメーター値を no に設定すると、HTTP listen は使用不可になります。

ポート値を設定する

TCP を介する HTTP listen のデフォルト・ポートは 80 です。

```
http-tcp-port = 80
```

ポート 8080 に変更する場合は、次のように設定します。

```
http-tcp-port = 8080
```

WebSEAL を HTTPS 要求用として構成する

iv.conf 構成ファイルの [wand] スタンザには、SSL を介する HTTPS 要求を処理するためのパラメーターが入っています。

HTTPS listen を使用可能 / 使用不可にする

デフォルトでは、Policy Director は、SSL を介する HTTPS 要求に関する listen を使用可能に (許可) します。

```
allow-ssl-http = yes
```

このパラメーター値を no に設定すると、HTTPS listen は使用不可になります。

ポート値を設定する

SSL を介する HTTPS のデフォルト・ポートは 443 です。

```
ssl-port = 443
```

ポート 4343 に変更する場合は、次のように設定します。

```
ssl-port = 4343
```

タイムアウト・パラメーターを指定する

設定できる Policy Director タイムアウト・パラメーターには、以下のものがあります。

- HTTP 通信に関するタイムアウト・パラメーター
- iv.conf 構成ファイルの [wand] スタンザに入っている追加の WebSEAL サーバー・タイムアウト・パラメーター

HTTP 通信に関するタイムアウト・パラメーター

WebSEAL では、HTTPS 通信に関する次のようなタイムアウト・パラメーターをサポートします。

ssl-init-connect-timeout (HTTPS の場合だけ)

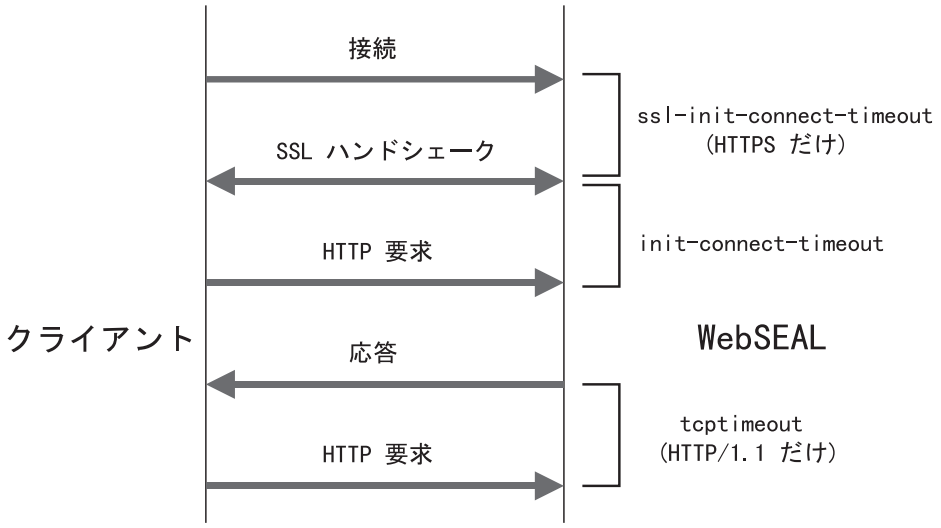
WebSEAL がブラウザーからの SSL 接続を受け入れると、 SSL プロトコル *handshake* が行われる必要があります。ハンドシェークとは、2 つのモデムの間に通信を設定するために、信号を交換するプロセスのことです。このパラメーターでは、SSL ブラウザーが SSL ハンドシェークを開始するのを、セキュリティー・マネージャーが待つ時間の長さを制御します。この初期設定が行われるのは、SSL 接続の開始時で、接続をシャットダウンする前です。

init-connect-timeout

SSL ハンドシェークが行われると、このパラメーターで、WebSEAL が初期 HTTP 要求を待つ時間の長さが指示されます。この接続は、HTTP、HTTPS、NetSEAT (HTTP と GSS) のどれでも構いません。

tcptimeout

このパラメーターは、HTTP/1.1 (HTTP/1.0 ではない) 接続に固有のものです。最初の HTTP/1.1 要求とサーバー応答の後で、このパラメーターによって、サーバーが HTTP/1.1 持続接続をオープンに保持する最大秒数を制御します。最大秒数に達すると、シャットダウンします。



パラメーター	構成ファイル	デフォルト値 (秒数)
ssl-init-connect-timeout	secmgrd.conf [ssl] スタンザ	120

init-connect-timeout	iv.conf [wand] スタンザ	120
tcptimeout	iv.conf [wand] スタンザ	5

追加の WebSEAL サーバー・タイムアウト・パラメーター

次のタイムアウト・パラメーターは、iv.conf 構成ファイルの [wand] スタンザで設定します。

パラメーター	説明	デフォルト値 (秒数)
tcp-junction-timeout	TCP 接合を通して行うバックエンド・サーバーに対する送信と読み取りのタイムアウト	120
ssl-junction-timeout	SSL 接合を通して行うバックエンド・サーバーに対する送信と読み取りのタイムアウト	120
cgi-timeout	ローカル CGI プロセスに対する送信と読み取りのタイムアウト	120
junction-ping-time	WebSEAL では、各接合先サーバーの定期的バックグラウンド PING を実行して、稼働しているかどうか判別します。WebSEAL がこれを試みる頻度は、300 秒 (または、設定されている値) に 1 回以下です。	300

HTTP エラー・メッセージを構成する

要求に対する WebSEAL サーバーによるサービスの試みは、時に失敗する場合があります。このような失敗には多くの原因が考えられます。たとえば、次のとおりです。

- ファイルが存在していない。
- 許可設定がアクセスを禁じている。
- UNIX ファイル許可に誤りがあるか、それに類似する何らかの原因で、 CGI プログラムの開始が妨げられている。

要求に対するサービスの失敗が生じると、サーバーは、HTML エラー・ページ内で、エラー・メッセージ (たとえば、403 Forbidden など) をブラウザーに戻します。幾つかのエラー・メッセージが使用可能です。 各メッセージごとに別々の HTML ファイルに保管されています。

これらのファイルは、次のディレクトリーに入っています。

UNIX:

install-path/www/lib/errors/*locale-dir*

Windows:

install-path¥www¥lib¥errors/*locale-dir*

errors ディレクトリーには、多数のロケール・サブディレクトリーがあります。サブディレクトリーには、各国語版エラー・メッセージ・ファイルが入っています。

このディレクトリーに入っているメッセージは、HTML 形式であり、ブラウザーに正しく表示されます。これらの HTML ページは編集して、その内容をカスタマイズできます。ファイルの名前は、操作の失敗時などに戻される内部エラー・コードの 16 進値です。これらのファイル名は変更できません。

比較的よく表示される一部のエラー・メッセージのファイル名と内容が、次の表にリストしてあります。

ファイル名	タイトル	説明	HTTP エラー・コード
1354a2fa.html	Non-Empty Directory	要求された操作には、非空きディレクトリーの除去が必要です。これは無許可の操作です。	
1898d25a.html	Could Not Sign User On	要求されたリソースでは、WebSEAL サーバーがユーザーを別の Web サーバーにサインオンさせることを必要としています。ただし、 WebSEAL による情報の検索中に、問題が発生しました。	
1898d25b.html	User Has No Single Sign-on Information	WebSEAL では、要求されたリソースの GSO ユーザーを見つけられませんでした。	
1898d25c.html	No Single Sign-on Target for User	WebSEAL では、要求されたリソースの GSO ターゲットを見つけられませんでした。	
1898d25d.html	Multiple Sign-on Targets for User	要求されたユーザーに関して、複数の GSO ターゲットが定義されています。GSO ターゲットの構成に誤りがあります。	
1898d25e.html	Login Required	要求されたリソースが接合先バックエンド Web サーバーによって保護されており、 WebSEAL がユーザーをその Web サーバーにサインオンさせる必要があります。そのためには、ユーザーがまず WebSEAL にログインすることが必要です。	
1898d25f.html	Could Not Sign User On	要求されたリソースでは、WebSEAL がユーザーを別の Web サーバーにサインオンさせることを必要としています。ただし、そのユーザーに関するサインオン情報に誤りがあります。	
1898d260.html	Unexpected Authentication Challenge	WebSEAL が、予期しない認証チャレンジを接合先バックエンド Web サーバーから受信しました。	
1898d421.html	Moved Temporarily	要求されたリソースが一時的に移動されました。これは、通常、転送の取り扱いを誤った場合に発生します。	302
1898d424.html	Bad Request	WebSEAL が無効の HTTP 要求を受信しました。	400

1898d425.html	Login Required	要求されたリソースは WebSEAL によって保護されているので、アクセスするためには、まずログインする必要があります。	
1898d427.html	Forbidden	要求されたリソースにアクセスする許可がユーザーにありません。	403
1898d428.html	Not Found	要求されたリソースが見つかりません。	404
1898d432.html	Service Unavailable	WebSEAL が要求の処理を完了するために必要とするサービスが、現在は使用不能です。	503
1898d437.html	Server Suspended	WebSEAL サーバーが、システム管理者によって一時的に中断状態にされています。サーバーがシステム管理者によってサービス状態に戻されるまで、要求は一切処理されません。	
1898d439.html	Session Information Lost	ブラウザー/サーバー対話が、応答しなくなっている接合先バックエンド・サーバーとの *ステートフル・セッション* でした。 WebSEAL では、このサーバー上にあるサービスが、要求の処理を完了することを必要としています。 207ページの『状態を維持する (-s オプション)』 を参照してください。	
1898d7af.html	CGI Program Failed	CGI プログラムが正しく実行されませんでした。	
default.html	Server Error	予期しないエラーのため、WebSEAL が要求を完了できませんでした。	500

マクロ・サポート

次のマクロがカスタマイズされた HTML エラー・メッセージ・ページで使用できます。マクロは、該当する使用可能な情報を動的に置換します。

マクロ	説明
ERROR_CODE	エラー・コードの数値。
ERROR_TEXT	メッセージ・カタログ内のエラー・コードに対応するテキスト。
METHOD	クライアントによって要求される HTTP メソッド。
URL	クライアントによって要求される URL。
HOSTNAME	完全修飾ホスト名。
HTTP_BASE	サーバー `http://` *`host`*`:`*`tcpport`*`/` の基本 HTTP URL。
HTTPS_BASE	サーバー `https://` *`host`*`:`*`sslport`*`/` の基本 HTTPS URL。
REFERER	要求からの参照元ヘッダーの値、または `Unknown` (ない場合)。
BACK_URL	要求からの参照元ヘッダーの値、または `/` (ない場合)。
BACK_NAME	値 `BACK` (参照元ヘッダーが要求にある場合)、または `HOME` (参照元ヘッダーがない場合)。

第15章 WebSEAL: スマート接合管理

WebSEAL は、スタンドアロン Web サーバーとして、またはバックエンド・アプリケーション・サーバーに関する認証と許可のサービスを提供する、接合サーバーとして機能できます。 WebSEAL の第 1 の強みは、バックエンド・アプリケーション・サーバー上の追加の Web リソースを統合し、保護できる機能にあります。 WebSEAL では、スマート接合テクノロジーを使用して、Web リソースの統合と保護を行います。

この章は、次の各節に分かれています。

スマート接合サーバーとしての WebSEAL の概要

Policy Director では、ネットワークに関して認証サービス、許可サービス、管理サービスを提供します。Web ベースのネットワークでは、これらのサービスは、フロントエンド WebSEAL サーバーによって提供されるのが最高です。フロントエンド WebSEAL サーバーでは、バックエンド・アプリケーション・サーバー上にある Web リソースを保護します。

WebSEAL サーバーとバックエンド・サーバーの間の接続は、*スマート接合*、または接合と呼ばれています。接合を使用して、 WebSEAL サーバーとバックエンド・サーバーの物理 Web スペースを結合して、単一の論理 Web スペース表示を構築します。

クライアントが Web リソースの物理位置を知る必要はまったくありません。WebSEAL は、論理 URL アドレスをバックエンド・サーバーが予期する物理アドレスに変換します。Web オブジェクトは、サーバー間で移動できますが、それによってクライアントによるアクセスの方法に影響が生じることはありません。

接合サーバーとしての WebSEAL では、すべての要求について、バックエンド・サーバーに渡す前に、認証検査と許可検査を実行できます。 接合によって拡張が容易な、機密保護機能のある環境が得られ、この環境では、ロード・バランシング、高可用性、状態管理の機能が、すべてクライアントには無関係に実行できます。管理者は、ネームスペースの集中管理を活用できます。

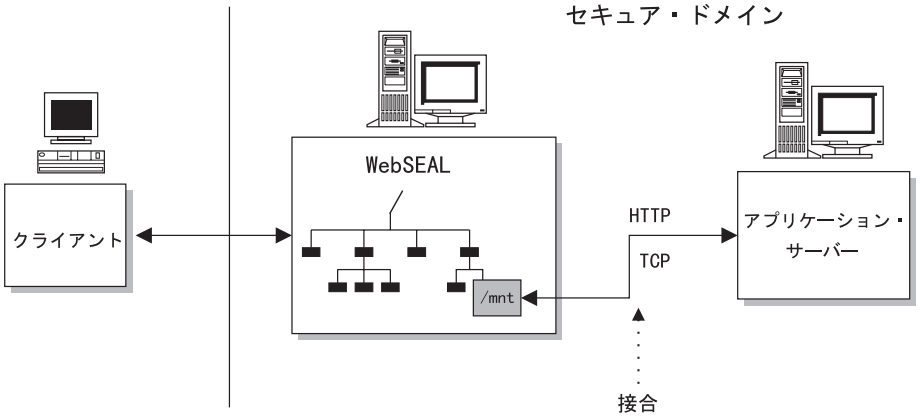
ほとんどの商業用 Web サーバーには、論理 Web ネームスペースを定義できる機能はありません。その代わりに、そのアクセス制御は物理ファイルとディレクトリー構造に接続されています。スマート接合では、標準的な Web サーバーの場合に通常

認められるように、物理マシンとディレクトリー構造を反映するのではなく、組織構造を反映するネームスペースを透過的に定義できます。

また、スマート接合によれば、単一サインオン・ソリューションの作成もできます。単一サインオン構成を使用すると、ユーザーは、1 回の初期ログインを使用するだけで、リソースの場所に関係なく、リソースにアクセスできます。バックエンド・サーバーからのログイン要件がさらに加わっても、ユーザーには無関係に処理されます。

スマート接合について

スマート接合 とは、フロントエンド WebSEAL サーバーとバックエンド・アプリケーション・サーバーの間の物理 TCP/IP 接続のことです。バックエンド・サーバーは、別の WebSEAL サーバーでも第三者アプリケーション・サーバーでも構いません。 バックエンド・アプリケーション Web スペースは、WebSEAL Web スペース内の特に指定された *接合点* (マウント・ポイント) で、 WebSEAL サーバーに *接続* します。

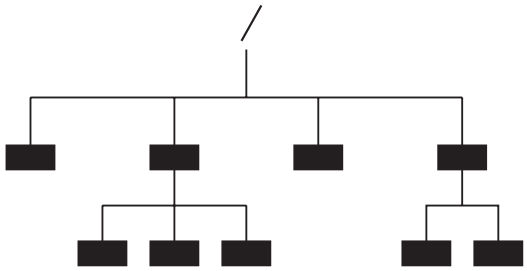


スマート接合によって、WebSEAL がバックエンド・アプリケーション・サーバーに代わって、保護サービスを提供できます。バックエンド・サーバーは、そのオブジェクトに対する密アクセス制御が必要です。このようなアクセス制御が必要とされる場合は、追加の構成ステップを実行して、 Policy Director セキュリティー・サービスに対して第三者 Web スペースを記述する必要があります。

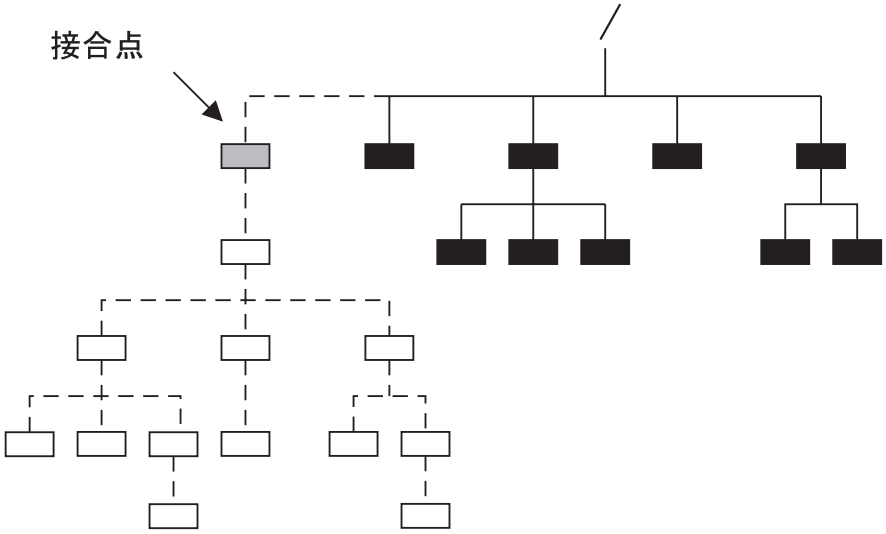
WebSEAL が適正に構成されると、認証、許可、監査などのセキュリティー・サービスを実行して、それ自体のリソースと接合先サーバー上のリソースを保護します。

スマート接合によって、WebSEAL サーバーの Web スペースをバックエンド・サーバーの Web スペースに論理的に結合するという付加価値が得られます。連携サーバー間の接合の結果として、単一の、統一された、シームレスで、ユーザーが特に意識しなくてもよい分散 Web スペースができます。

Web スペースが統一されていることで、システム管理者にとって、すべてのリソースの管理が単純化されます。管理上の利点としては、これに加えて、拡張容易性、ロード・バランシング、高可用性があります。



WebSEAL Web スペース



結合された Web スペース:
WebSEAL ＋ 接続先サーバー

スマート接合は、Web サイトの拡張を容易にするための重要なツールです。接合によって、追加のサーバーを接続することで、Web サイト上で増え続ける需要に応えることができます。

スマート接合と Web サイトの拡張容易性

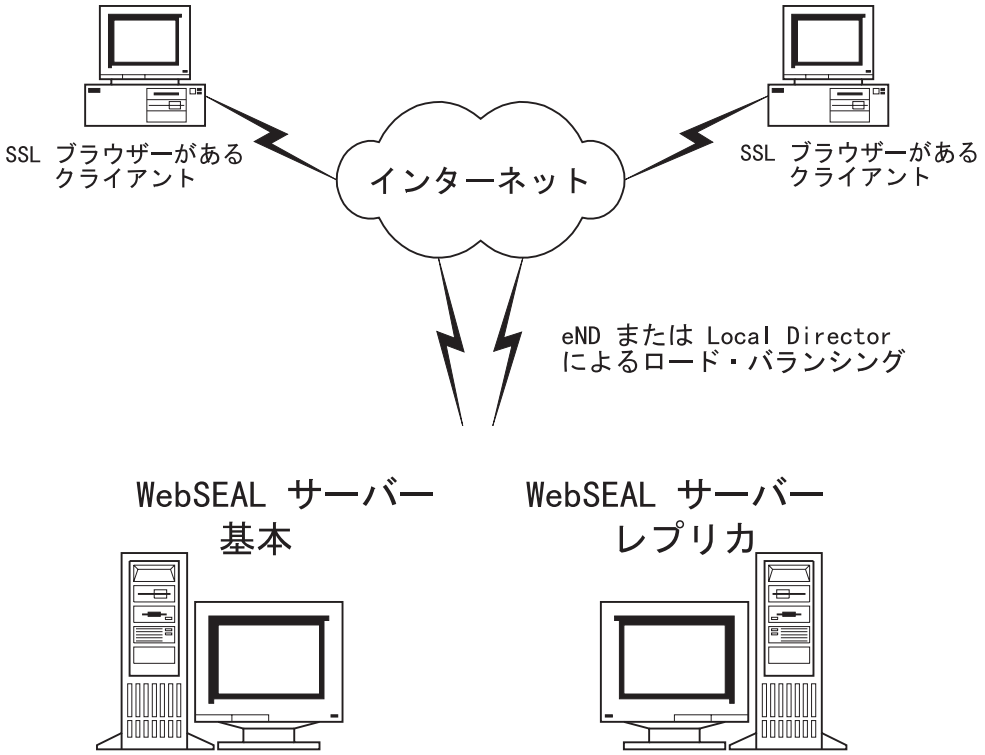
拡張が容易な Web サイトを作成する場合は、スマート接合を使用します。Web サイト上の需要の増大に応じて、サーバーを簡単に追加できるので、サイトの能力を拡張できます。追加のサーバーを追加する必要が生じるのは、次のような理由によります。

- 追加の内容によりサイトを拡張するため
- 既存の内容の重複によって、ロード・バランシング、フェールオーバー、高可用性の能力を確保するため

複製フロントエンド WebSEAL サーバー

バックエンド・サーバーに関する接合サポートは、フロントエンド WebSEAL サーバーが少なくとも 1 台あれば始まります。複製フロントエンド WebSEAL サーバーによって、サイトでは大需要時のロード・バランシングが得られます。アプリケーション (Policy Director eND や Cisco Local Director など) が、ロード・バランシング・メカニズムを処理します。

フロントエンドの複製によって、サイトではフェールオーバーの能力も得られます。 何らかの理由でサーバーに障害が起こっても、残りのレプリカ・サーバーによって引き続きサイトへのアクセスが得られます。 ロード・バランシングとフェールオーバーの機能が正常に働けば、結果的にユーザーにとってサイトの高可用性が確保されます。



フロントエンド WebSEAL サーバーの複製についての重要な点は、次の 2 つです。

- 各サーバーごとに、それぞれ Web スペースの正確なコピーを持っている必要がある。
- ユーザー・アカウント・データベースを複製して、認証の一貫性を確保する必要がある。

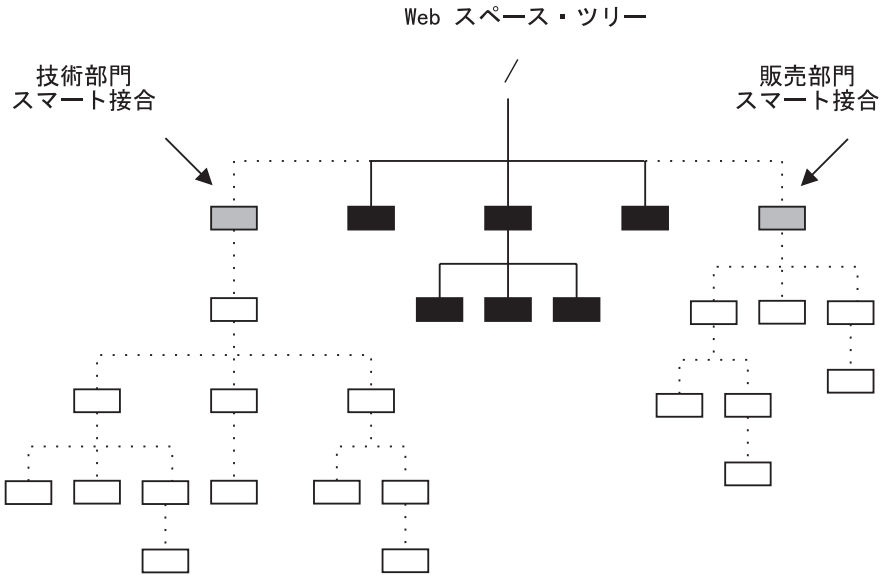
Policy Director の許可サービスでは、必要に応じて、許可データベース情報を自動的に複製します。

バックエンド・サーバーをサポートする

WebSEAL サーバー自体、バックエンド・サーバー (複数の場合もある)、またはその両方の組み合わせで、Web サイト内容にサービスできます。バックエンド・サーバーに関するスマート接合サポートを使用すると、追加の内容とリソースによって、 Web サイトを拡張できます。

固有のバックエンド・サーバーはそれぞれ、別々の接合点 (マウント・ポイント) に接合される必要があります。追加の内容とリソースに対する需要が増大すれば、それに応じてスマート接合を使用してサーバーを追加します。こうすれば、第三者 Web サーバーに対する既存の投資が大きいネットワークの場合の解決策が得られます。

次の図には、スマート接合によって、どのようにして統一された論理 Web スペースが得られるかが示してあります。この Web スペースは、ユーザーには無関係で、集中管理に対処できます。



複製バックエンド・サーバーは、『複製バックエンド・サーバー』で説明しているように、接合点に接合されます。

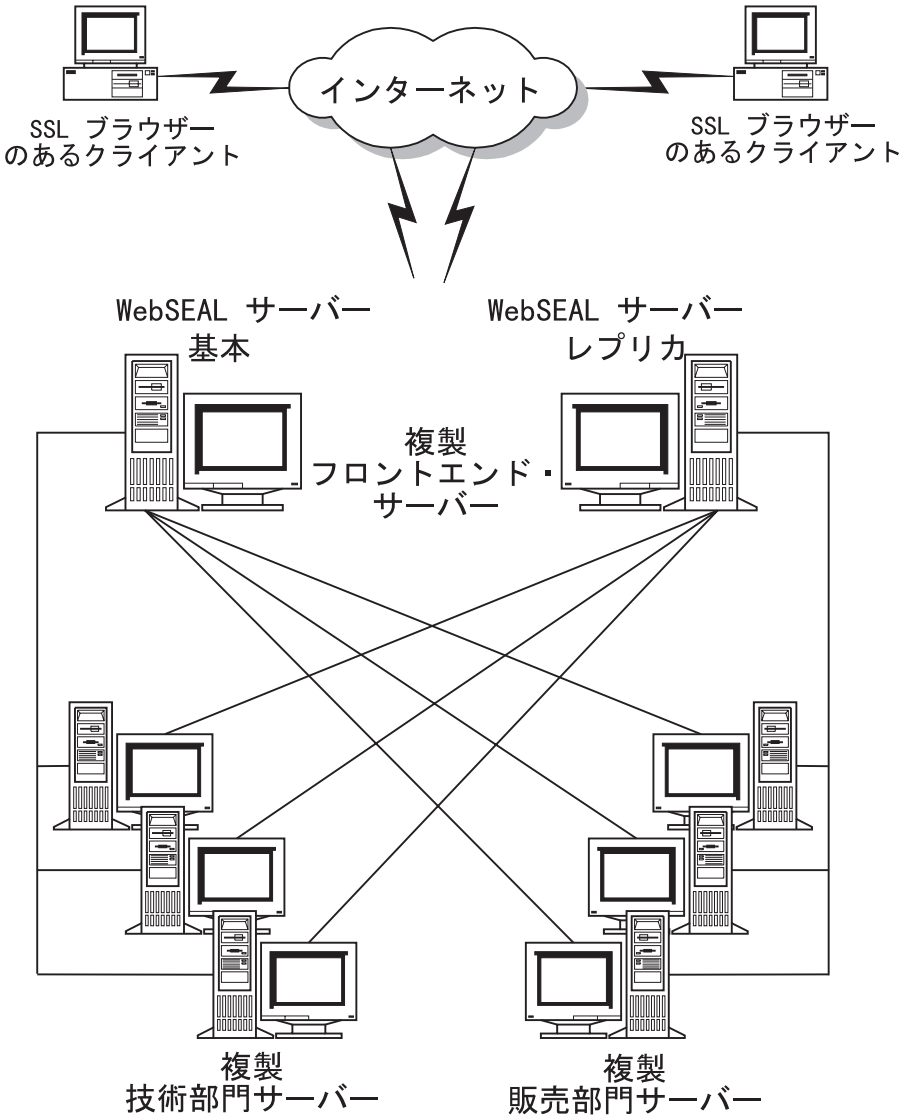
複製バックエンド・サーバー

拡張容易性機能をバックエンド・サーバー構成に拡張する場合は、バックエンド・サーバーを複製できます。複製フロントエンド・サーバーの場合と同じように、複製バックエンド・サーバーの場合も、それぞれが相互にミラー・イメージとなる、Web スペースを含む必要があります。

WebSEAL では、“一番空いている” スケジューリング・アルゴリズムを使用して、複製サーバー間のロード・バランシングを図ります。また、WebSEAL は、サーバーがダウンすると、正しくフェールオーバーし、再始動したサーバーを再度使用して開始します。

状態が複数のページにわたって保持されることが、バックエンド・アプリケーションによって必要とされる場合は、ステートフル接合を使用できます。このような ステ

ートフル接合 によって、各セッションはそれぞれ同一のバックエンド・サーバーに確実に戻ります。 207ページの『状態を維持する (-s オプション)』を参照してください。



接合の作成に関するタスク要旨

次のような接合タイプが作成できます。

- Policy Director と第三者間 ; TCP 接続
- Policy Director と第三者間 ; SSL 接続
- Policy Director とローカル・ファイル・システム間

以下のステップには、バックエンド・アプリケーション Web スペースを WebSEAL Web スペースに接合する場合に実行する必要があるタスクを要約してあります。

1. WebSEAL Web スペース内の追加サーバーの接合 (マウント) 場所を決めます。
2. ネットワークの保全性を確保するために必要なセキュリティー条件を決めます。

粗アクセス制御

粗いアクセス制御を提供するには、次のように行います。

1. Policy Director の **junctioncp** ユーティリティーを使用して、バックエンド第三者アプリケーション Web スペースとフロントエンド WebSEAL サーバーの間に、スマート接合を作成します。
2. 適当なポリシー・テンプレート (ACL) を接合点上に配して、バックエンド・サーバーに粗制御を実施します。

密アクセス制御

きめの細かいアクセス制御を提供するには、次のように行います。

1. **junctioncp** ユーティリティーを使用して、バックエンド第三者アプリケーション Web スペースとフロントエンド WebSEAL サーバーの間に、スマート接合を作成します。

   WebSEAL には、第三者ファイル・システムを自動的に 見て、理解することはできません。 **query_contents** を使用して、WebSEAL に第三者ネームスペースを通知する必要があります。このアプリケーションには、第三者 Web スペースのインベントリーがあり、WebSEAL に構造を報告します。
2. **query_contents** プログラムを第三者サーバーにコピーします。
3. 管理コンソールを使用して、ポリシー・テンプレート (ACL) を統一 Web スペース内の該当するオブジェクトに適用します。

スマート接合を作成するための指針

以下の指針には、スマート接合に関する規則が要約してあります。

- スマート接合は、1 次 WebSEAL ネームスペース内のどこにでも追加できます。
- 同じマウント・ポイント (接合点) に複数のレプリカ・サーバーを接合できます。
- 複数のレプリカ・サーバーが同じ接合点にマウントされる場合は、同じタイプである (TCP か SSL) ことが必要です。
- 第三者サーバーは連鎖できません (たとえば、Policy Director -- 第三者 -- 第三者など)。

アクセス制御と管理特権

デフォルトでは、セル管理者アカウントには、接合先サーバーも含めた、 Web スペース全体に対する全権利があります。 接合先サーバーの管理者は、そのサーバーだけの Web スペースを保守します。この管理者は、必要があれば、このサーバーに対する管理特権をセル管理者から除去します。

Policy Director は、第三者サーバーへのスマート接合全体に ACL を継承します。

junctioncp を使用してスマート接合を管理する

junctioncp ユーティリティーを使用して、接合管理タスクすべてを実行します。

- 新規接合点を作成する。
- 接合点にサーバーを追加する。
- 接合点からサーバーを除去する。
- 接合点を削除する。

- 接合点のリストを表示させる。
- 接合の詳細を表示させる。

junctioncp ユーティリティーには、対話式コマンド・プロンプトが用意されているので、そこから接合タスクが実行できます。

junctioncp を使用する前に、管理ユーザーとしてセキュア・ドメインにログインしておく必要があります。dce_login は、UNIX 環境か Windows 環境で使用できます。netseat_login は、Windows 環境で使用できます。

接合タスクを実行したいサーバー (ホスト名) を指定するための **-e** オプションを使用して、**junctioncp** ユーティリティーを開始します。 **junctioncp** コマンド・プロンプトが表示されます。

たとえば、次のようになります。

UNIX:

```
#
# junctioncp -e server-name
junctioncp>
```

Windows:

```
junctioncp -e <server-name>
junctioncp>
```

junctioncp コマンドを使用する

次のようなコマンドが **junctioncp** で使用できます。

コマンド	説明
create	初期サーバー用として新規接合を作成します。
add	既存の接合点に追加のサーバーを追加します。
remove	接合点からサーバーを除去します。
delete	接合点を除去します。
list	このサーバー上の全接合点を一覧表示します。
show	接合の詳細を表示します。
help	**junctioncp** コマンドを一覧表示します。
help *command*	特定の **junctioncp** コマンドに関して詳細なヘルプを表示します。
exit	**junctioncp** ユーティリティーを終了します。

これらのコマンドと対応するオプションの説明については、 『初期サーバー用として新規接合を作成する』を参照してください。

初期サーバー用として新規接合を作成する

操作 : 新規接合点を作成し、初期サーバーを接合する。

構文 : `create -t type -h hostname options junction-point`

タイプ

次のいずれか 1 つ • **tcp** • **ssl** • **local**		*必須。* 接合のタイプを定義します。 バックエンド第三者サーバーには **tcp** を使用します。 **ssl** オプションを使用するときは、デフォルトの TCP ポートは、80 から 443 に変更されます。 208ページの『セキュア SSL スマート接合を作成する』を参照してください。
オプション		
	TCP と SSL の接合オプション (**-t tcp** または **-t ssl** で使用)	
	-2	SSL バージョン 2 だけを使用して、バックエンド・サーバーとの通信を強制します。 208ページの『セキュア SSL スマート接合を作成する』を参照してください。
	-b *ba-value* 次のいずれか 1 つ • **filter** (デフォルト) • **ignore** • **supply** • **gso**	WebSEAL サーバーがバックエンド・サーバーに認証情報を渡す方法を定義します。 213ページの『接合先サーバーに認証情報を提供する』を参照してください。
	-c	Policy Director クライアント識別を HTTP ヘッダーに挿入します。 207ページの『クライアント識別情報を挿入する (-c オプション)』を参照してください。
	-i	WebSEAL サーバーに URL を大文字小文字を区別しないとして処理させます。 205ページの『大文字小文字を区別しない URL をサポートする (-i オプション)』を参照してください。
	-h *hostname*	*必須。* ターゲット・バックエンド・サーバーのホスト名 (DNS) を定義します。 IP アドレスを代替として指定できます。
	-p *port*	バックエンド第三者サーバーの TCP ポートを定義します。デフォルトでは、TCP 接合が 80 で、SSL 接合が 443 です。
	-q *url*	**query_contents** スクリプトの URL を定義します。 Policy Director は、/cgi_bin/ 内で **query_contents** を探索します。このディレクトリーが異なるか、**query_contents** ファイルが名前変更されているときは、このオプションを使用して、WebSEAL にファイルへの新規 URL を示します。 第三者 Win32 サーバーにスマート接合を作成する場合は、この **-q** オプションを使用します。223ページの『照会内容を探索するためのスマート接合の構成』を参照してください。

	-s	接合がステートフル・アプリケーションをサポートすることを指定します。デフォルトでは、接合は *ステートフル* ではありません。 207ページの『状態を維持する (-s オプション)』を参照してください。
	-T *resource*	GSO リソース・クリデンシャルのためにアプリケーション・リソースの名前を定義します。 **-b gso** オプションの場合に必須で、このオプションでだけ使用されます。 217ページの『GSO と WebSEAL 単一サインオンを統合する』を参照してください。
	-v *hostname*	サーバーの仮想ホスト名を定義します。
	-w	Win32 ファイル・システム・サポートを定義します。 206ページの『短いファイル名形式を禁止する (-w オプション)』を参照してください。
	ローカルと DFS 接合オプション (**-t dfs** か、 **local** で使用)。	
	-d *dir*	接合する分散ファイル・システム (DFS) またはローカル・ディレクトリーを定義します。必須。
junction-point		
	接合を作成するための WebSEAL ネームスペース内の位置を定義します。	

既存の接合に追加のサーバーを追加する

操作: 既存の接合点に追加のサーバーを追加する。

構文: `add -h hostname options junction-point`

オプション		
	TCP と SSL の接合オプション	
	-i	WebSEAL サーバーに URL を大文字小文字を区別しないとして処理させます。 205ページの『大文字小文字を区別しない URL をサポートする (-i オプション)』を参照してください。
	-h *hostname*	*必須。* ターゲット・バックエンド・サーバー・ホスト名 (DNS) を定義します。 IP アドレスを代替として指定できます。
	-p *port*	バックエンド第三者サーバーの TCP ポートを定義します。デフォルトでは、TCP 接合が 80 で、SSL 接合が 443 です。
	-q *url*	**query_contents** スクリプトの URL を定義します。 Policy Director は、/cgi_bin/ 内で **query_contents** を探索します。 このディレクトリーが異なるか、**query_contents** ファイルが名前変更されているときは、このオプションを使用して、WebSEAL にファイルへの新規 URL を示します。
	-v *hostname*	サーバーの仮想ホスト名を定義します。

	-w	Win32 ファイル・システム・サポートを定義します。 206ページの『短いファイル名形式を禁止する (-w オプション)』を参照してください。
junction-point		
	この既存の接合点にサーバーを追加します。	

他の junctioncp コマンドを使用する

junctioncp create コマンドと **junctioncp add** コマンドについては、 202ページの『初期サーバー用として新規接合を作成する』と 204ページの『既存の接合に追加のサーバーを追加する』で説明しています。次の表には、それ以外の使用可能な **junctioncp** コマンドが一覧表にしてあります。

コマンド	説明
remove	**操作 :** 接合点からバックエンド・サーバーを除去する。 **構文 :** `remove -i server-id junction-point` **オプション : -i** *server-id* 除去対象サーバーの識別。 show コマンドを使用して、特定のサーバーの ID を判別します。
delete	**操作 :** 接合点を除去する。 **構文 :** `delete junction-point`
show	**操作 :**接合点の詳細を表示する。 **構文 :** `show junction-point`
list	**操作 :**すべての接合を一覧表示する。 **構文 :** `list`
help	**操作 : junctioncp** コマンドの一覧表を表示する。 **構文 :** `help`
help *command*	**操作 :**使用可能なオプションも含めて、特定の **junctioncp** コマンドについての情報を表示する。 **構文 :** `help command`
exit	**操作 : junctioncp** ユーティリティーを終了して、オペレーティング・システム・プロンプトに戻る。 **構文 :** `exit`

大文字小文字を区別しない URL をサポートする (-i オプション)

第三者サーバーと接合するときは、**-i** オプションを使用して、WebSEAL が URL を大文字小文字を区別しないとして処理することを指定します。つまり、サーバーは、URL の構文解析にあたって、大文字と小文字の区別をしないことを意味します。デフォルトでは、サーバーが大文字小文字を区別することを予期します。

ほとんどの HTTP サーバーは、URL を大文字小文字を区別するとして定義する HTTP 仕様をサポートしますが、HTTP サーバーには、URL を大文字小文字を区別しないとして処理するものもあります。

たとえば、大文字小文字を区別しないサーバー上では、次の 2 つの URL は、同一の URL として表示されます。

```
http://server/sales/index.htm
http://server/SALES/index.HTM
```

この振る舞いにより、Policy Director では、両方の URL に対して同一のアクセス制御 (ACL) を適用する必要があります。デフォルトでは、 Policy Director は、アクセス制御を適用するにあたって、URL を大文字小文字を区別するとして処理します。**-i** オプションを指定して、第三者サーバーを接合することによって、WebSEAL では、そのサーバーに送信される URL は、大文字小文字を区別しないとして処理します。

短いファイル名形式を禁止する (-w オプション)

この目標は、アクセス制御を 1 つのオブジェクト表示だけに制限することにあります。セキュリティー・メカニズムをバイパスする裏口 は許しません。

WebSEAL では、URL に指定されているファイル・パスに基づいて、接合先バックエンド・サーバーに対するクライアント要求に対して、セキュリティー検査を実行します。Win32 ファイル・システムでは、長いファイル名にアクセスするために 2 つの異なる方式を用意しているため、このセキュリティー検査での折衷が行われる可能性があります。

最初の方式では、ファイル名全体 (`abcdefghijkl.txt`) を確認します。2 番目の方式では、後方互換性を確保するために旧 8.3 ファイル名形式を使用します (`abcdef~1.txt`)。

junctioncp コマンドに **-w** オプションを指定すると、8.3 ファイル名形式が禁止されます。ユーザーは、ファイル名の短い (8.3) 形式を使用して、長いファイル名に対する明示的 ACL を避けることはできません。サーバーは、短い形式のファイル名が入力された場合は、`403 Forbidden` エラーを戻します。

Windows では、ファイル名 “foo.” は、後書きドットのないファイル名 “foo” と同様に処理します。**-w** オプションでは、要求をバックエンド・サーバーに送信する前に、URL 内のファイル名から後書きドットを除去します。 Policy Director では、後書きドットの付かないファイル名を基にして、 ACL 検査を行います。

注: -i オプションでは、Win32 で大文字の小文字の区別をしないこと (`abced.txt = AbCdE.txt`) による問題に対処します。

例 :

Windows NT 4.0 では、ファイル ¥Program Files¥ibm corp¥readme.txt に関する次のファイル・パスに、次のようにしてアクセスできます。

1. ¥program files¥ibm corp.¥readme.txt
2. ¥program files¥ibm corp¥readme.txt
3. ¥progra~1¥ibm~2¥readm~3.txt

上記の例 1 では、“大文字小文字を区別しないこと” の影響を示しています。 **-i** オプション (**-w** オプションでなく) で、この影響に対処します。

例 2 には、Windows NT がどのようにして後書き拡張子ドットを無視するかが示されています。

例 3 には、Windows NT がディスク・オペレーティング・システム (DOS) 互換性を確保するために、別名を作成する方法が示されています。 別名については、ファイル名にスペースを含めることはできず、8.3 形式に準拠する必要があります。

-w オプションでは、例 2 と例 3 に示されている潜在的セキュリティー・ホールに対処します。**-w** で、 Policy Director が後書きドットを無視するよう指示します。また、このオプションでは、この接合先サーバーに対する要求 URL に波形記号文字 (~) が含まれている短縮ファイル名へのアクセスを、 Policy Director が禁止するように指示します。

状態を維持する (-s オプション)

ほとんどの Web 使用可能アプリケーションでは、各クライアント・セッションに入っている一連の HTTP 要求にまたがって、*状態* を維持します。たとえば、この状態を使用して、次のことを行います。

- CGI プログラムによって生成されるデータ項目形式内のフィールドを通じて、ユーザーの進行を追跡する。
- 一連のデータベース照会の実行時に、ユーザーのコンテキストを保守する。
- ユーザーが購入する品目をランダムにブラウズし選択する、オンライン・ショッピング・カート・アプリケーション内に品目のリストを保守する。

ロード共用によるパフォーマンスの向上を図るために、Web 使用可能アプリケーションを実行するサーバーを、どんなサーバーの場合とも同じように複製できます。Policy Director サーバーは、このようにして複製されたサーバーにスマート接合を提供できます。そうするときは、クライアント・セッション内に入っている要求はすべて、必ず正しいサーバーに転送されるようにする必要があります。また、ロード・バランシング規則に従って、複製されたサーバー間に、要求が必ずしもすべて配分されるとは限らないようにする必要があります。

デフォルトでは、Policy Director は、使用可能な複製サーバーすべてにわたって要求を配分することによって、サーバー・ロードのバランスを図ります。 Policy Director は “一番空いている” アルゴリズムを使用します。

このロード・バランシングをオーバーライドし、*ステートフル接合* を作成する場合は、**-s** オプションを指定して、 **junctioncp** コマンドを使用します。ステートフル接合によって、クライアントの要求が、1 つのセッション全体を通じて同一のサーバーに転送されることが保証されます。

クライアント識別情報を挿入する (-c オプション)

-c オプションを選択すると、Policy Director 固有のクライアント識別情報とグループ・メンバーシップ情報を、HTTP 要求のヘッダーに挿入できます。HTTP 要求は、接合先第三者サーバーにあてられます。Policy Director 固有の HTTP ヘッダーによって、

接合先第三者サーバー上のアプリケーションで、ユーザー固有のアクションを実行できます。ユーザー固有のアクションは、クライアントの Policy Director 識別に基づきます。

HTTP ヘッダー情報は、バックエンド・サーバー上でのサービスによって使用できるように、環境変数形式に変換する必要があります。ダッシュ (-) をすべて下線 (_) で置き換え、ストリングの先頭に “HTTP” を付加することによって、ヘッダー情報を CGI 環境変数形式に変換します。 HTTP ヘッダーの値は、新しい環境変数の値になります。

Policy Director 固有の HTTP ヘッダー項目には、次のものがあります。

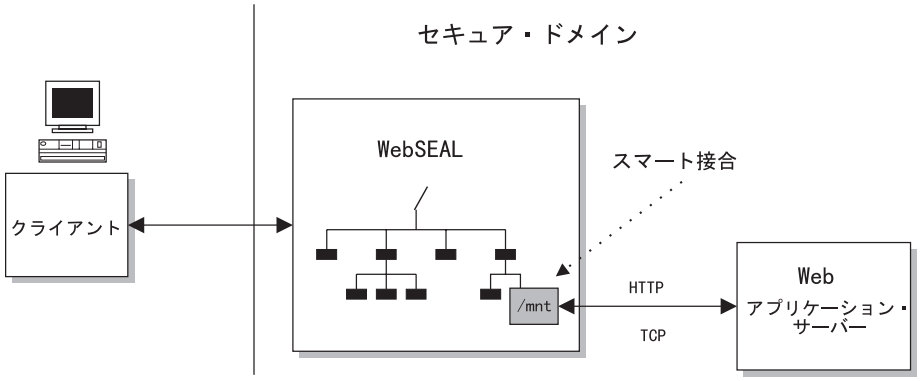
Policy Director 固有の HTTP ヘッダー	CGI 環境変数の形式	説明
iv-user	HTTP_IV_USER	クライアントの名前。クライアントが認証されていない (不明の) 場合は、デフォルトでは、**Unauthenticated** です。
iv-groups	HTTP_IV_GROUPS	クライアントが属するグループのリスト。スペースで区切られた項目で構成されます。
iv-creds	HTTP_IV_CREDS	Policy Director リソース・クリデンシャルを表す、コード化された不透明データ構造。 Policy Director 許可 API と共に使用されます。 詳しくは、*Policy Director Programmer's Guide and Reference* を参照してください。

HTTP ヘッダー項目は、環境変数 HTTP_IV_USER, HTTP_IV_GROUP と HTTP_IV_CREDS として、CGI プログラムで使用可能です。その他のアプリケーション・フレームワーク・プロダクトの場合は、HTTP 要求からヘッダーを抜き出す方法について、該当するプロダクトの資料を参照してください。

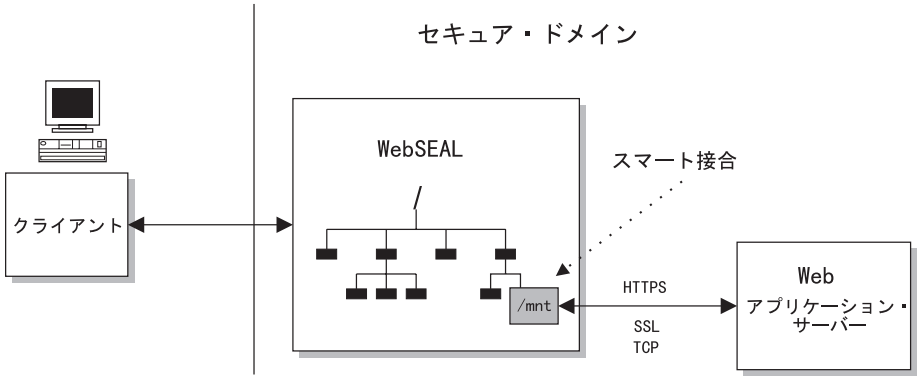
セキュア SSL スマート接合を作成する

WebSEAL では、WebSEAL とバックエンド・サーバーの間に、標準 TCP (HTTP) 接合とセキュア SSL (HTTPS) 接合の両方をサポートします。SSL 接合は、TCP 接合とまったく同様に機能しますが、WebSEAL とバックエンド・サーバーの間の通信がすべて暗号化されるという付加価値が付きます。

次の図は、非セキュア TCP (HTTP) 接合を表しています。



次の図は、セキュア SSL (HTTPS) 接合を表しています。



WebSEAL とバックエンド・サーバーの間の接合は、クライアントと WebSEAL サーバーの間の接続のタイプ (および、そのセキュリティー・レベル) からは独立しています。

SSL 接合では、セキュア終端間、ブラウザー / アプリケーション間トランザクションが可能です。クライアントから WebSEAL への通信と、WebSEAL からバックエンド・サーバーへの通信を機密保護する場合は、SSL を使用します。

セキュア SSL 接合を構成する

SSL スマート接合が機能するためには、バックエンド Web サーバーが、 HTTPS 使用可能であることが必要です。

スマート接合を作成する場合は、**junctioncp** ユーティリティーを使用します。**junctioncp** ユーティリティーの詳細は、201ページの『junctioncp を使用してスマート接合を管理する』で説明しています。

セキュア SSL 接合を作成し、初期サーバーを追加する場合は、**junctioncp create** コマンドを使用します。次の例では、セキュア SSL 接合を作成するための create コマンドの構文を示しています。

```
junctioncp> create -t ssl [-2] -h hostname [-p port] junction-point
```

-2 オプションによって、Policy Director に、 SSL バージョン 2 だけの使用によるバックエンド・サーバーとの通信を強制します。

通常は、Policy Director が、SSL プロトコルのバージョン (バージョン 2 と 3 のどちらか) を自動的に折衝します。Policy Director が **-2** オプションを導入したのは、SSL バージョン 3 の折衝を試みると、 Policy Director に障害が起こる原因となる IIS サーバーがあるからです。このようなことが発生すると、マウントは正常に行われません。バージョン 2 の使用を強制すれば、この問題は解決します。

SSL 接合の例を検討する

SSL プロトコルを使用する接合点 /sales で、ホスト sales.ibm.com を接合します。

```
create -t ssl -h sales.ibm.com /sales
```

SSL バージョン 2 プロトコルだけを使用する接合点 /admin で、ホスト admin.ibm.com を接合します。

```
create -t ssl -2 -h admin.ibm.com /admin
```

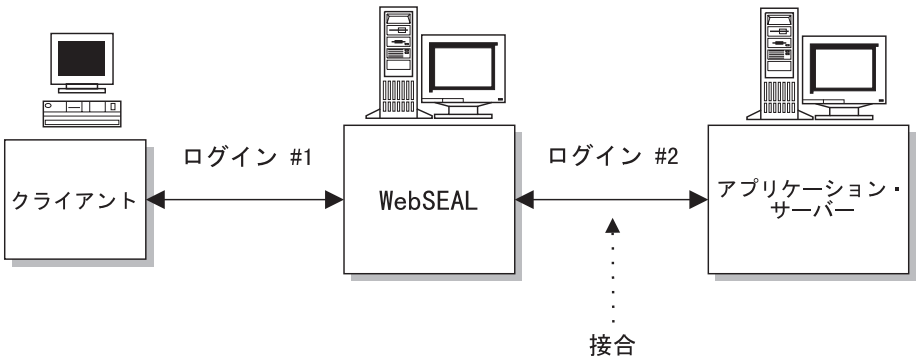
注: 上記の 2 つの例では、**-t ssl** オプションによって、デフォルト・ポート 443 が指示されています。

SSL プロトコルを使用する接合点 /travel で、ポート 4343 のホスト travel_svr を接合します。

```
create -t ssl -p 4343 -h travel_svr /travel
```

Policy Director の単一サインオン・ソリューションを使用する

保護リソースをバックエンド・サーバー上に配置すると、そのリソースを要求するクライアントは、複数のログインを実行する必要がある場合があります。複数のログインとしては、WebSEAL サーバーに関するものが 1 つと、バックエンド・サーバーのそれぞれに関するものが 1 つずつあります。それぞれのログインごとに、異なるログイン識別が必要になる可能性が大です。



複数のログイン識別の管理と保守の問題は、単一サインオン・メカニズムの使用によって解決できます。単一サインオン・ソリューションによって、ユーザーは、リソースの場所には関係なく、1 回の初期ログインだけを使用して、リソースにアクセスできます。バックエンド・サーバーからのログイン要件がさらにあっても、ユーザーには無関係に処理されます。

Policy Director の単一サインオン・メカニズムの構成にあたっては、ネットワーク・セキュリティー管理者は、次の 3 つの重要な決定を行う必要があります。

1. 認証情報がバックエンド・サーバーによって必要とされるか?

   WebSEAL では、 HTTP *基本認証* ヘッダーを使用して、認証情報を伝えます。
2. 認証情報がバックエンド・サーバーによって必要とされる場合は、この情報がどこから来るのか? (WebSEAL は HTTP ヘッダーにどんな情報を入れるのか?)
3. WebSEAL とバックエンド・サーバーの間の接続は、セキュア接続である必要があるか? (TCP 接合か SSL 接合か?)

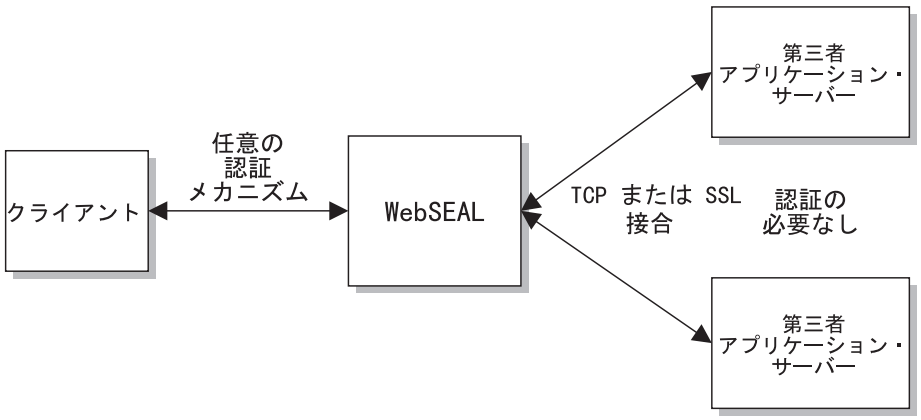
以下の各項で、一部の一般的な WebSEAL 単一サインオン構成について検討します。

バックエンド・サーバーが認証を必要としない

バックエンド・サーバーが認証情報を必要としない場合は、次の条件が存在します。

- 認証情報が接合を通って送信されるように WebSEAL を構成する必要はありません。
- WebSEAL を介するだけでバックエンド・サーバーにアクセスできます。
- WebSEAL が、すべてのバックエンド・サーバーに代わって認証を処理します。
- 必要があれば、さらなる認証アクションに備えて、ユーザー識別情報をバックエンド・サーバーに渡すための、特殊オプションがあることに変わりありません この特殊オプションとは、 **junctioncp** ユーティリティーの **-c** オプションです。

216ページの『認証情報なし』を参照してください。



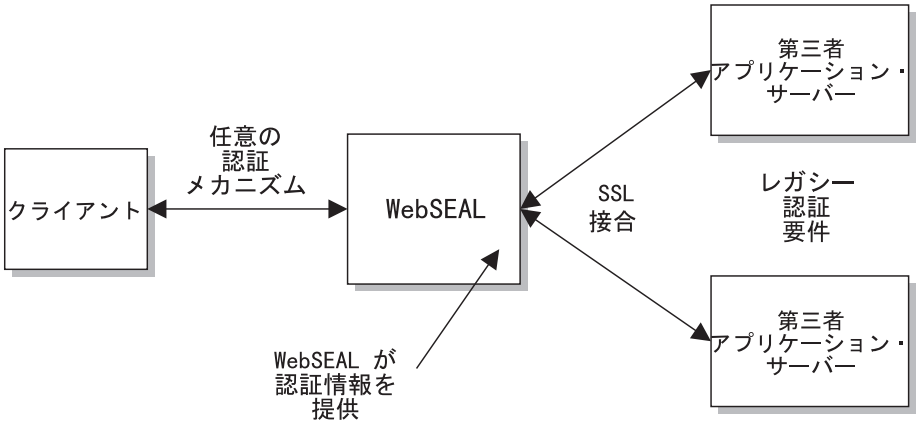
バックエンド・サーバーがレガシー認証を必要とする

バックエンド・サーバーに、サポートされる必要があるレガシー認証メカニズムが収容されている場合は、次のような条件が存在します。

- 該当する認証情報をバックエンド・サーバーに提供するように、WebSEAL を構成する必要があります。
- 認証情報は、GSO などのようなメカニズムから来る可能性が非常に大です。

  217ページの『GSO と WebSEAL 単一サインオンを統合する』を参照してください。

- Policy Director では、接合を通して機密認証情報 (ユーザー名とパスワード) を渡すため、接合のセキュリティーが重要です。したがって、Policy Director では、SSL 接合の使用を推奨しています。

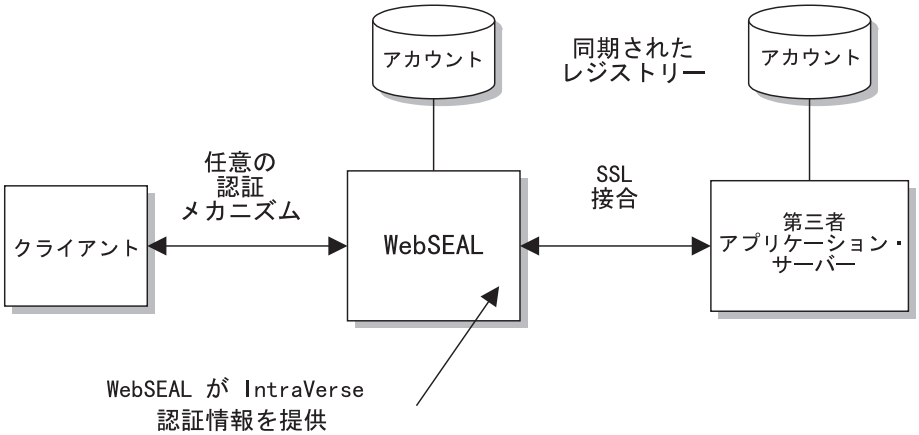


Policy Director の単一サインオン

バックエンド・サーバーが Policy Director 認証情報を必要とする場合は、次の条件が存在します。

- 元のクライアント要求に入っているユーザー名とパスワードをバックエンド・サーバーに提供するように、WebSEAL を構成する必要があります。
- バックエンド・サーバーは、HTTP 基本認証 (BA) ヘッダー内で提供される Policy Director の識別とパスワードが理解できる必要があります。したがって、 WebSEAL とバックエンド・サーバーには、同期されたユーザー・レジストリーが必要です。
- Policy Director では、接合を通して機密認証情報 (ユーザー名とパスワード) を渡すため、接合のセキュリティーが重要です。 Policy Director では、SSL 接合の使用を推奨しています。

215ページの『元のクライアント BA ヘッダー情報』を参照してください。

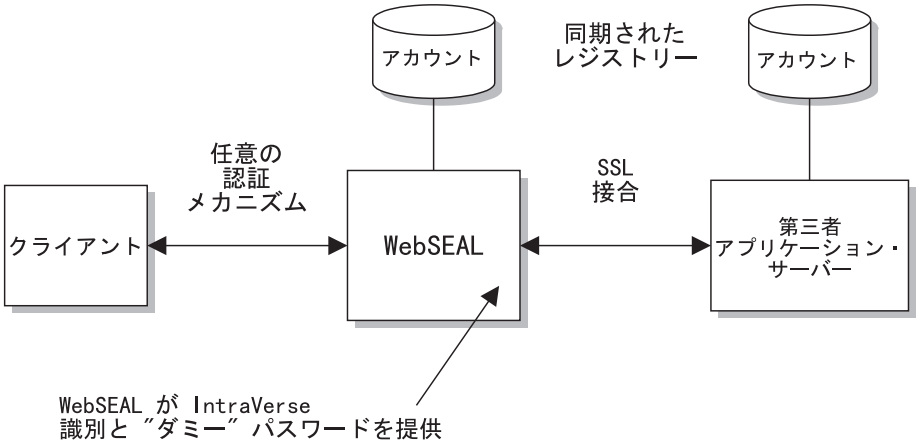


Policy Director の限定単一サインオン

Policy Director の限定サインオンが使用可能なのは、HTTP BA ヘッダーが Policy Director 識別 (ユーザー名) を提供する場合です。 静的総称パスワードも提供されます。このモデル・ケースは、ユーザー別アプリケーションの使用の場合に該当します。このソリューションが有利になりうるのは、パスワード管理が継続している必要がないからです。 次の条件が存在します。

- 元のクライアント要求に入っているユーザー名に加えて、総称 (ダミー) パスワードをバックエンド・サーバーに提供するように、 WebSEAL が構成される必要があります。
- iv.conf 構成ファイル内にダミー・パスワードを構成します。
- バックエンド・サーバーは、HTTP BA ヘッダー内で提供される Policy Director の識別が理解できる必要があります。 したがって、WebSEAL とバックエンド・サーバーには、同期されたアカウント・レジストリーが必要です。
- Policy Director では、接合を通して機密認証情報 (ユーザー名とパスワード) を渡すため、接合のセキュリティーが重要です。 Policy Director では、SSL 接合の使用を推奨しています。

214ページの『Policy Director 識別と総称パスワード』を参照してください。



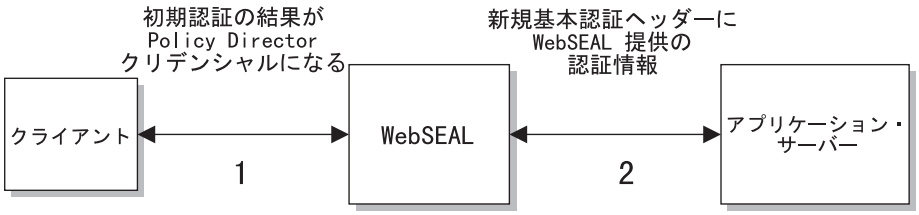
接合先サーバーに認証情報を提供する

WebSEAL からバックエンド・サーバー (複数の場合もある) に認証情報を渡すモデル・ケースは、いろいろ考えられます。 管理者としては、HTTP 基本認証ヘッダーに入っている認証情報をバックエンド・サーバーに送信するかどうか決める必要があります。

この認証情報のソースは?

クライアントと WebSEAL の間の初期認証の後、WebSEAL が新規基本認証ヘッダーを構築します。要求はこの新規ヘッダーを使用して、接合を通ってバックエンド・サーバーまでの行程を取ります。管理者は、**junctioncp** ユーティリティーによって用意されているオプションを使用して、この新規ヘッダーに入れて提供される認証情報を指示する必要があります。

ネットワーク体系とセキュリティー要件を分析した上で、接合を通過する必要があるヘッダー情報があれば、それを決めます。

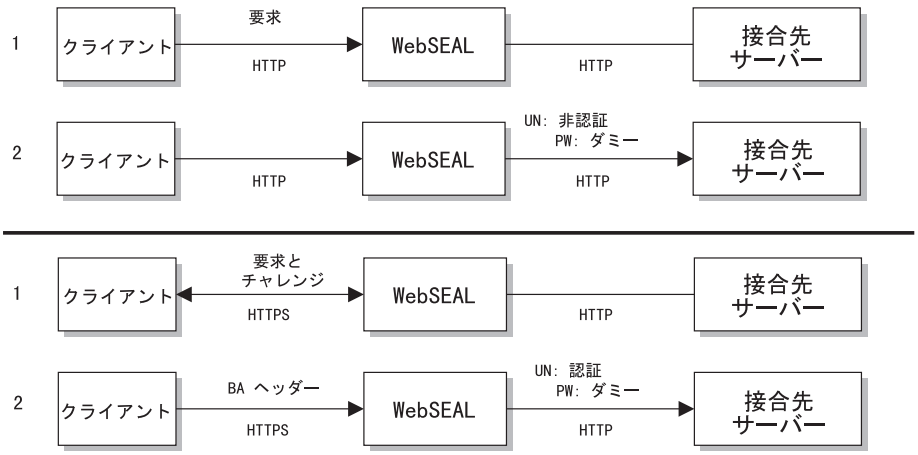


Policy Director 識別と総称パスワード

junctioncp オプション : -b supply

このオプションでは、認証された Policy Director ユーザー名 (クライアントの元の識別) を、総称 (ダミー) パスワードと共に提供するよう、WebSEAL に指示します。このモデル・ケースでは、元のクライアント・パスワードは使用しません。

このモデル・ケースでは、バックエンド・サーバーが Policy Director 識別からの認証を必要とすると想定されています。クライアント・ユーザーを既知の Policy Director ユーザーにマップすることによって、Policy Director は、バックエンド・サーバーに関する認証を管理します。また、Policy Director では、簡単でドメイン全体にわたる、単一サインオン・ソリューションも提供します。



制限 :

Policy Director では、すべての要求に同じダミー・パスワードを使用します。すべてのユーザーがバックエンド・レジストリー内に同じパスワードをもっています。クライアントが接合先サーバーにアクセスする場合に、必ず WebSEAL を通せば、この配置にセキュリティーの問題が生じることはありません。

総称パスワードによって、パスワード管理の必要がなくなり、アプリケーションはユーザー単位でサポートされます。iv.conf 構成ファイルの **basic_auth_passwd** パラメーターによって、ダミー・パスワードが設定されます。

```
basic_auth_passwd = password
```

このモデル・ケースでは、パスワード・レベルのセキュリティーがないため、バックエンド・サーバーが暗黙的に WebSEAL をトラストして、クライアントの正当性を検証する必要があります。

サーバーも、Policy Director 識別を受け入れるためには、それを理解する必要があります。これには、バックエンド・サーバー・レジストリーと WebSEAL レジストリーの同期が必要です。

共通ダミー・パスワードの使用では、ユーザー名を使用してログインするクライアントの正当性を、バックエンド・サーバーが証明するための根拠にはなりません。 したがって、考えられる他のアクセス手段からバックエンド・サーバーを物理的に保護することも重要です。

元のクライアント BA ヘッダー情報

junctioncp オプション : -b ignore

このオプションでは、クライアントによって提供される基本認証 (BA) ヘッダーを無視するよう、WebSEAL に指示します。このオプションは、ヘッダーに変更を加えないで第三者サーバーに転送するよう、WebSEAL に指示します。 WebSEAL サーバーに対しては、ログインはまったく実行されません。

このモデル・ケースは、バックエンド・サーバーが次のような場合に該当します。

- 基本認証をサポートしている。
- Policy Director セキュリティーを使用するようには構成されていない。
- クライアント提供パスワードを保守する必要がある。

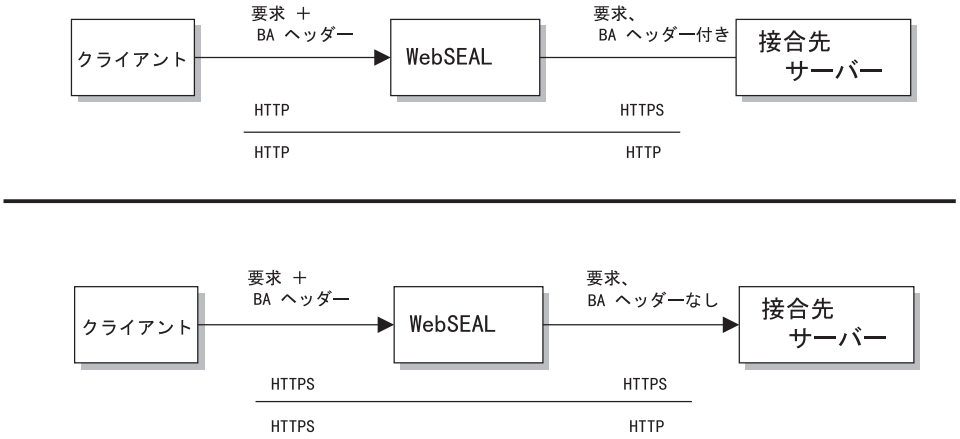
WebSEAL では、元のクライアント要求をバックエンド・サーバーに直接、妨害を受けないで渡します。

バックエンド・サーバーは、基本認証チャレンジをクライアントに返送します。 クライアントは、WebSEAL サーバーが変更を加えないで渡す、ユーザー名情報とパスワード情報を使用して応答します。

これは真の単一サインオン・メカニズムではなく、むしろ、WebSEAL には無関係に行われる、第三者サーバーへの直接ログインです。

注意:
クライアントが SSL (基本認証) を使用して、WebSEAL に対して認証した場合は、このオプションは働きません。この場合は、基本認証ヘッダーは、非セキュアの可能性がある接合を通って送信される前に、 (-b filter の場合のように) 除去されます。

バックエンド・サーバーが基本認証を使用する場合は、クライアントにチャレンジを返送します。ただし、クライアントが戻す認証情報は、もう 一度除去されることになります。要求がバックエンド・サーバーに届くことは決してありません。

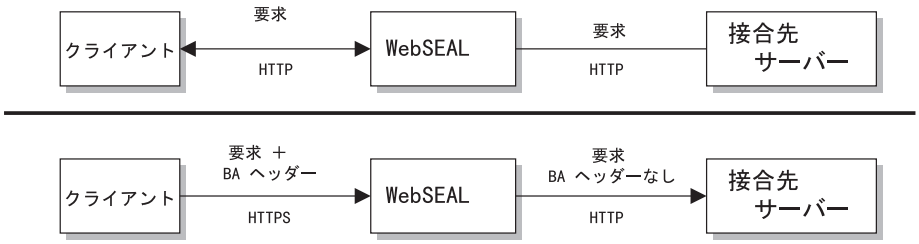


認証情報なし

junctioncp オプション : -b filter

このオプションでは、クライアント要求をバックエンド・サーバーに転送する前に、クライアント要求から基本認証ヘッダーをすべて除去するよう、WebSEAL に指示します。 WebSEAL は、単一セキュリティー・プロバイダーになります。このオプションが適切なのは、バックエンド・サーバーが基本認証を必要としないことが分かっている場合です。

このオプションと **-c** オプションを組み合わせると、 Policy Director クライアント識別情報を HTTP ヘッダーに挿入できます。 207ページの『クライアント識別情報を挿入する (-c オプション)』を参照してください。



GSO からのユーザー名とパスワード

junctioncp オプション : -b gso

このオプションでは、GSO から取得される認証情報 (ユーザー名とパスワード) をバックエンド・サーバーに提供するよう、WebSEAL に指示します。セキュリティーが WebSEAL サーバーとバックエンド・サーバーの両方で必要な場合は、このモデル・ケースに該当します。バックエンド・サーバー・アプリケーションでは、WebSEAL レジストリーには入っていない、異なるユーザー名とパスワードも必要です。

217ページの『GSO と WebSEAL 単一サインオンを統合する』で、このメカニズムを詳しく説明します。

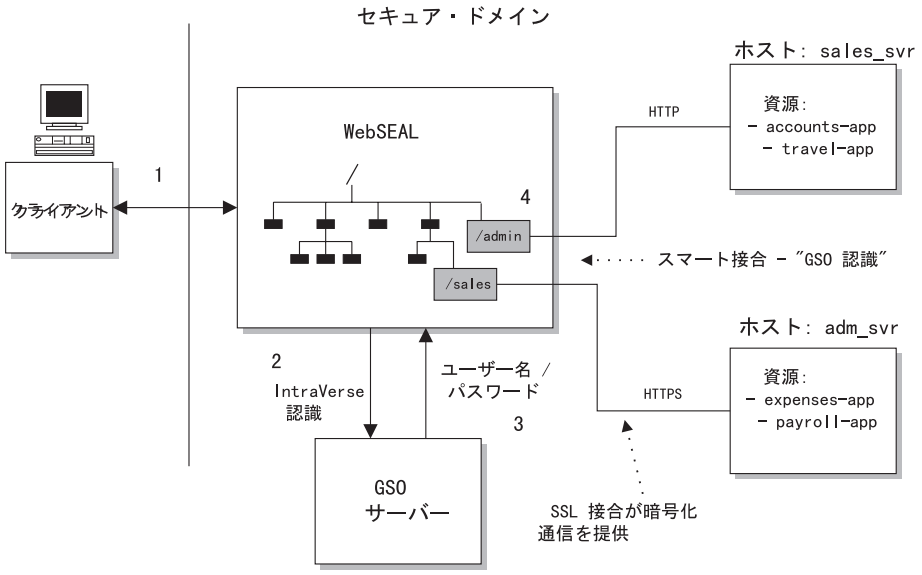
GSO と WebSEAL 単一サインオンを統合する

Policy Director では、IBM グローバル・サインオン (GSO) と統合することによって、柔軟性が増した単一サインオン・ソリューションをサポートします。IBM グローバル・サインオンは、IBM の SecureWay テクノロジーのコンポーネントの 1 つです。WebSEAL と GSO の組み合わせによって、完全な単一サインオン・ソリューションが得られ、さらに利点としてデータの暗号化、高可用性、拡張容易性が付加されます。

下の図には、WebSEAL と GSO の統合によって、バックエンド・アプリケーション・リソースに関して、ユーザー名とパスワードを検索する場合が図解してあります。

1. クライアントが、バックエンド・サーバー上のアプリケーション・リソースへのアクセスの要求で、WebSEAL に対して認証します。Policy Director 識別が取得されます。

   注: 単一サインオン・プロセスは、初期認証方式から独立しています。
2. WebSEAL が Policy Director 識別を GSO に渡します。
3. GSO が、ユーザーと要求されたアプリケーション・リソースに適した、ユーザー名とパスワードを戻します。
4. WebSEAL が、ユーザー名情報とパスワード情報を、要求の HTTP 基本認証ヘッダーに挿入します。WebSEAL が、接合を通して、要求をバックエンド・サーバーに送信します。



GSO から認証情報を取得する

次の例には、GSO が WebSEAL に認証情報を提供する方法が示してあります。ユーザー Michael が travel-app アプリケーション・リソースを実行したい場合は、WebSEAL が GSO に Michael の認証情報を要求します。

GSO は、認証情報の完全なデータベースを、特定の認証情報へのリソース・マッピングの形式で保守します。ユーザー名とパスワードの組み合わせへのアプリケーショ

ン・リソースのマッピングは、 *GSO* リソース・クリデンシャル と呼ばれています。GSO リソース・クリデンシャルを作成できるのは、登録ユーザーの場合だけです。

GSO には、リソース “travel-app” を特定のユーザー名とパスワードの組み合わせにマップする、 Michael に関する特定のリソース・クリデンシャルが入っています。

次の表に、GSO リソース・データベースの構造が示してあります。

Michael	**Paul**
resource: travel-app username=mike password=123 resource: payroll-app username=powell password=456	resource: travel-app username=bundy password=abc resource: payroll-app username=jensen password=xyz

この例では、GSO がユーザー名 mike とパスワード 123 を WebSEAL に戻します。WebSEAL がこの情報を使用するのは、接合を通して送信される要求内に HTTP 基本認証ヘッダーを構成するときです。

GSO 使用可能スマート接合を構成する

WebSEAL とバックエンド・アプリケーション・サーバーの間のスマート接合に、GSO に対する WebSEAL サポートを構成します。

GSO を使用可能にする接合を作成する場合は、**-b gso** オプションを指定して、**jctioncp create** コマンドを使用します。次の例に、 create コマンドの構文が示してあります。

```
create -t tcp -h hostname -b gso -T resource jct-point
```

次の表には、GSO スマート接合をセットアップする場合のオプションが一覧表にして示してあります。

オプション	説明
-b gso	この接合を通過するすべての要求に関して、GSO が認証情報を提供する必要があることを指定します。
-T *resource*	アプリケーション・リソースの名前を指定します。このオプションの引き数として使用されるリソース名は、 GSO データベース内にリストされているリソース名に正確に一致する必要があります。 GSO 接合の場合は必須です。

208ページの『セキュア SSL スマート接合を作成する』で説明しているように、WebSEAL と GSO ソリューションで使用される接合は、SSL によってセキュア接合にすることができます。接合の作成時に **-t ssl** オプションを適用して、セキュア接合にします。

SSL 結合は、必ず GSO で使用して、GSO リソース・クリデンシャルとすべてのデータの暗号化を確保します。

GSO 使用可能スマート接合の例:

ホスト “sales_svr” のアプリケーション・リソース “travel-app” を接合点 “/sales” に接合します。

```
create -t tcp -b gso -T travel-app -h sales_svr /sales
```

ホスト “adm_svr” のアプリケーション・リソース “payroll-app” を接合点 “/admin” に接合し、SSL で接合をセキュア接合にします。

```
create -t ssl -b gso -T payroll-app -h adm_svr /admin
```

注: 上記の例では、**-t ssl** オプションでデフォルト・ポート 443 が指示されています。

スマート接合を使用する

固有のバックエンド・サーバーはそれぞれ、別々の接合点 (マウント・ポイント) に接合される必要があります。 追加の内容とリソースに対する需要の増大に応じて、スマート接合を使用してサーバーを追加できます。

スマート接合の使用に関係する手順は、次のとおりです。

- 『複数のサーバーを同一接合にマウントする』
- 『接合先サーバーにより URL をフィルターする』
- 220ページの『CGI 処理を制御する (x 許可)』

複数のサーバーを同一接合にマウントする

複数の複製サーバーを同一接合点にマウントできます。同一接合点にマウントできるサーバーの数には制限はありません。

同一接合点にマウントされるサーバーはすべて、レプリカ (ミラーリングされた Web スペース) である必要があり、同じプロトコル (HTTP か HTTPS) を使用する必要があります。同一接合点に非類似サーバーをマウントすることはできません。

1 次 Policy Director サーバー Web スペースから、接合先サーバーに属するページにアクセスします。これらのページには (許可を得ていることが条件で) アクセスできる必要があり、これらのページには一貫性が必要です。時に、ページが見つからなかったり、ページが変更されている場合がありますが、これは、Policy Director がそのページを正しく複製しなかったことを意味します。

文書が存在し、両複製サーバーの文書ツリーで同じであるかチェックします。

接合先サーバーにより URL をフィルターする

接合先サーバーから受信される MIME タイプ “text” または “html” の文書だけがフィルターされます。

WebSEAL が変更できる URL は、絶対 (Absolute) とホスト相対 (Host Relative) の 2 組があります。

ホスト相対 URL

ホスト相対 URL では、接合先サーバーの文書ルートとの関係で URI 位置を示します。たとえば、次のようにします。

```
/dir/file.html
```

これらの URL を変更して、接合先サーバーの接合点を反映させます。たとえば、次のとおりです。

```
/jct/dir/file.html
```

絶対 URL

絶対 URL では、HOST 名か IP アドレスとネットワーク・ポートの両方との関係で、統一リソース標識 (URI) 位置を示します。たとえば、次のとおりです。

```
http://servername[:port]/file.html
```

または

```
https://servername[:port]/file.html
```

これらの URL は、次の一連の規則に従って変更できます。

1. URL が HTTP で、ホストかポートが TCP 接合先サーバーに一致するときは、URL は変更されて、接合点を反映します。たとえば、次のとおりです。

   ```
   /jct/...
   ```

2. URL が HTTPS で、ホストかポートが SSL 接合先サーバーに一致するときは、URL は変更されて、接合点を反映します。たとえば、次のとおりです。

   ```
   jct...
   ```

3. iv.conf 構成ファイル内で定義されている TAG と属性のペアの URL だけがフィルターされます。
4. リフレッシュ要求の META タグは、常にフィルターします。たとえば、次のとおりです。

   ```
   META HTTP-EQUIV="Refresh" CONTENT="5;URL=http://server/url"
   ```

5. BASE タグに HREF 属性が含まれている場合は、タグはクライアントへの応答から除去されます。

iv.conf 構成ファイルの [url-filter] スタンザには、接合先サーバーによって URL をフィルターするためのパラメーターが入っています。

[url-filter] スタンザには、HTML タグのリストが入っています。 WebSEAL サーバーでは、これらのタグをフィルターまたは変更して、接合先サーバーを介して取得された絶対 URL を調整します。

デフォルトでは、Policy Director は、一般的に使用される HTML タグすべてを構成します。URL が入っている追加の HTML を、管理者が追加する必要がある場合もあります。

CGI 処理を制御する (x 許可)

Policy Director の実行 (x) 許可は、接合をまたがっては意味がありません。x 許可で CGI スクリプトの処理は制御できません。 WebSEAL には、バックエンド・サーバー上の要求されたオブジェクトが、CGI プログラム・ファイルなのか、通常の HTTP オブジェクトなのかを判別する手段はありません。接合をまたがるオブジェクト (これには CGI プログラムも含まれる) へのアクセスは、常に読み取り (r) 許可を使用して制御します。

第三者サーバーで query_contents を使用する

Policy Director セキュリティー・サービスを使用して、第三者アプリケーション Web スペースのリソースを保護できます。 そうしたいときは、第三者 Web スペースの内容についての情報を WebSEAL に提供する必要があります。

query_contents と呼ばれる CGI プログラムによって、この情報が提供されます。**query_contents** プログラムでは、第三者 Web スペース内容を検索し、このインベントリー情報を WebSEAL の管理コンソールに提供します。このプログラムは、WebSEAL インストールに付属していますが、第三者サーバーには手動でインストールする必要があります。プログラム・ファイル・タイプは、第三者サーバーを UNIX で使用するか、Windows で使用するかに応じて異なります。

管理コンソールのオブジェクト・スペース・マネージャーでは、**query_contents** を自動的に実行できます。保護オブジェクト・スペースの接合を表す部分が、オブジェクト・スペース管理パネルで展開されると、いつでもこれを実行します。こうして、第三者アプリケーション・スペースの内容がコンソールに分かったので、この情報を表示させ、該当するオブジェクトにポリシー・テンプレートを適用できます。

query_contents をインストールする

query_contents のインストールには、 Policy Director サーバーから第三者サーバーへの 1 つか 2 つのファイルのコピーと、構成ファイルの編集が必要になります。

次の Policy Director ディレクトリーに、プログラムのテンプレートが入っています。

UNIX: *root-directory*/www/lib/query_contents

Windows: *root-directory*¥www¥lib¥query_contents

ディレクトリーの内容には、次のものがあります。

ファイル	説明
query_contents.exe	Win32 システム用のメイン実行可能プログラム。第三者 Web サーバーの cgi-bin ディレクトリーにインストールする必要があります。
query_contents.sh	UNIX システム用のメイン実行可能プログラム。第三者 Web サーバーの cgi-bin ディレクトリーにインストールする必要があります。
query_contents.c	ソース・コード。ソースが提供されるのは、**query_contents** の振る舞いを変更する必要がある場合です。ほとんどの場合は、これは必要ありません。
query_contents.html	HTML 形式のヘルプ・ファイル。
query_contents.cfg	Web サーバーの文書ルートを識別するサンプル構成ファイル。

第三者 UNIX サーバーに query_contents をインストールする

query_contents.sh という名前のシェル・スクリプトを、次のディレクトリーで見つけます。

UNIX: *install-dir*/www/lib/query_contents

第三者 UNIX サーバーに **query_contents** ユーティリティーをインストールする場合は、次のようにします。

1. 第三者 Web サーバーの機能 /cgi-bin ディレクトリーに、query_contents.sh をコピーする。
2. .sh 拡張子を除去する。
3. Web サーバーを所有するユーザー用として、UNIX “実行” ビットを設定する。

第三者 Win32 サーバーに query_contents をインストールする

query_contents.exe という名前の実行可能プログラムと、 query_contents.cfg という名前の構成ファイルを、次のディレクトリーで見つけます。

Windows: *install-dir*¥www¥lib¥query_contents

第三者 Win32 サーバーに **query_contents** ユーティリティーをインストールする場合は、次のようにします。

1. 第三者 Web サーバーに CGI ディレクトリーが正しく構成されているか確認する。
2. 第三者 Web サーバーの文書ルートに、有効な文書が存在しているか確認する。
3. 第三者 Web サーバーの CGI ディレクトリーに、query_contents.exe をコピーする。
4. Windows ディレクトリーに、query_contents.cfg をコピーする。

   次の表に、このディレクトリーのデフォルト値が示してあります。

オペレーティング・システム	Windows ディレクトリー
Windows 95	c:¥windows
Windows NT 3.5x	c:¥winnt35
Windows NT 4.x	c:¥winnt

5. query_contents.cfg ファイルを編集して、第三者 Web サーバーの文書ルート・ディレクトリーを正しく指定する。

   ファイルには、現在、 Microsoft インターネット情報サーバー™ と Netscape® FastTrack サーバーに関するサンプル項目が入っています。 このファイルのセミコロン (;) で始まる行は注釈であり、 **query_contents** プログラムでは無視されます。

構成をテストする

構成をテストする場合は、次のようにします。

1. Win32 サーバーでは、 **query_contents** プログラムが入っているディレクトリーに変更する。
2. Win32 サーバーの DOS プロンプトから、次のようにしてプログラムを実行する。

   ```
   query_contents dirlist=/
   ```

   次のような出力が表示されるはずです。

   ```
   100
   index.html
   cgi-bin//
   pics//
   ```

番号 100 は、正常に実行されたことを示す戻り状況です。非常に大切なことは、少なくとも番号 100 が最初 (で、唯一) の値として表示されることです。

この代わりにエラー・コードが表示された場合は、構成ファイルが正しい場所にないか、構成ファイルに有効な文書ルート項目がないということになります。query_contents.cfg ファイルの構成をチェックし、文書ルートの存在を確認します。

3. ブラウザーから、次の URL を入力します。

   ```
   http: //Win32 machine name/cgi-bin/query_contents.exe?dirlist=/
   ```

   このコマンドにより、前のステップの結果と同じ結果が戻されるはずです。この結果が戻されない場合は、 Web サーバーの CGI 構成に誤りがあります。サーバーの資料を参照して、問題を訂正します。

照会内容を探索するためのスマート接合の構成

query_contents スクリプトの URL を定義できます。 Policy Director は、 /cgi_bin/ 内で **query_contents** を探索します。このディレクトリーが異なるか、**query_contents** ファイルが名前変更されているときは、このオプションを使用して、WebSEAL にファイルへの新規 URL を示します。

第三者 Win32 サーバー用のスマート接合を作成する場合は、 **-q** オプションを付けて **junctioncp** コマンドを使用します。

```
junctioncp> create -t tcp -h hostname -q /cgi-bin/query_contents.exe /jct_mount_point
```

junctioncp コマンドのすべてのオプションの要約については、 202ページの『初期サーバー用として新規接合を作成する』を参照してください。

query_contents を実行する

query_contents は、URL 要求に組み込まれているディレクトリーの内容を戻すために使用します。たとえば、サーバーの Web スペース用のルート・ディレクトリーの内容を入手する場合は、ブラウザーで URL に対して、次のように **query_contents** を実行します。

```
http://third-party-server/cgi-bin/query_contents?dirlist=/
```

query_contents スクリプトでは、次のアクションを実行します。

1. 標準 CGI 環境変数 $SERVER_SOFTWARE を読み取って、サーバー・タイプを判別する。

   Policy Director では、Web サーバー・タイプに基づいて、変数 $DOCROOTDIR を一般的な文書ルート位置に設定します。

2. 要求された URL から環境変数 $QUERY_STRING を読み取って、要求された操作を取得し、オブジェクト・パスを入手します。

   変数 $OPERATION で操作値を保管し、 $OBJPATH でオプション・パスを保管します。 この例では、$OPERATION は dirlist、 $OBJPATH は例に示した “ / ” です。

3. オブジェクト・パスに対してディレクトリー・リスト作成 (ls) を実行し、 Policy Director サーバーでの使用に備えて、結果を標準出力に置きます。サブディレクトリーを示す項目には、ダブルスラッシュ (//) が付加されています。

   一般的な出力は、次のようになります。

```
100
index.html
cgi-bin//
pics//
```

番号 100 は、正常に実行されたことを示す戻り状況です。

query_contents をカスタマイズする

サーバー用として **query_contents** をカスタマイズする場合は、文書ルート・ディレクトリー設定を変更する必要がある可能性があります。

query_contents がエラー状況 (100 以外の番号) を戻し、ファイルのリストを作成しない場合は、スクリプトを調べます。必要なら、 $DOCROOTDIR 変数を変更して、サーバーの構成に一致させます。

文書ルート・ディレクトリーを正しく指定しても、スクリプトに障害が起こる場合は、cgi-bin 位置指定が誤っている可能性があります。$FULLOBJPATH 変数を調べ、それに割り当てられている値を変更して、正しい cgi-bin 位置を反映させます。

追加機能

query_contents プログラムのソース・コード (query_contents.c) は、Policy Director に付属して配布されます。

このプログラムに追加機能を追加して、一部の第三者 Web サーバーの特殊機能をサポートできます。これらの機能には、次のようなものがあります。

1. ディレクトリー・マッピング -- 文書ルートより下でないサブディレクトリーが、Web スペース内にマップされます。
2. ファイル・システム・ベースでない Web スペースの生成。
   データベース・ホスト Web サーバーの場合に該当する可能性があります。

第16章 WebSEAL: アプリケーションの統合

WebSEAL では、環境変数と動的 URL 機能による第三者アプリケーションの統合をサポートします。WebSEAL では、環境変数と HTTP ヘッダーの範囲を拡張して、第三者アプリケーションで、クライアントの識別に基づいている操作ができるようにします。さらに、WebSEAL は、動的 URL (たとえば、照会テキストが入っているものなど) に対するアクセス制御を提供できます。

この章は、次の各節に分かれています。

CGI プログラミングをサポートする

CGI プログラミングをサポートするために、WebSEAL では、標準セットの CGI 変数に、追加の環境変数を 3 つ追加します。CGI アプリケーションでは、ローカル WebSEAL サーバーと接合先バックエンド・サーバーのどちらかで実行されるこれらの環境変数を使用します。これらの変数は、Policy Director 固有のユーザー情報、グループ情報、クリデンシャル情報を CGI アプリケーションに提供します。

ローカル WebSEAL サーバー上では、要求を行うクライアントの Policy Director クリデンシャル情報によって、これらの環境変数が直接生成されます。

接合先第三者サーバーで稼働する CGI アプリケーションによって使用される環境変数は、HTTP ヘッダー情報から生成されます。 WebSEAL がサーバーに HTTP ヘッダー情報を渡します。 **junctioncp -c** オプションを使用して、*接合* を作成する必要があります。 そうすると、接合によって、Policy Director 固有の情報が、バックエンド・サーバーあての HTTP 要求に挿入されます。

207ページの『クライアント識別情報を挿入する (-c オプション)』を参照してください。

追加の Policy Director 固有の環境変数

以下に、追加の Policy Director 固有 CGI 環境変数の形式を示します。

CGI 環境変数の形式	説明
HTTP_IV_USER	要求側の Policy Director ユーザー・アカウント名
HTTP_IV_GROUPS	要求側が属する Policy Director グループ。 二重引用符で囲んだグループ名をコンマで区切ったリストとして指定します。
HTTP_IV_CREDS	Policy Director クリデンシャルを表す、コード化された不透明データ構造。リモート・サーバーにクリデンシャルを提供するので、中段のアプリケーションでは、許可 API を使用して許可サービスを呼び出せます。 *Policy Director Programmer's Guide and Reference* を参照してください。

ローカル WebSEAL サーバー上の REMOTE_USER 変数

WebSEAL の制御下にあるローカル・サーバー環境では、HTTP_IV_USER 変数の値が、標準 REMOTE_USER 変数の値として提供されます。なお、REMOTE_USER 変数は、接合先バックエンド・サーバーで実行される CGI アプリケーションの環境でも存在できます。ただし、この状態では、 WebSEAL がその値を制御することはありません。

CGI 環境変数の形式	説明
REMOTE_USER	HTTP_IV_USER フィールドと同じ値が入ります。

バックエンド・サーバー側アプリケーションをサポートする

WebSEAL には、バックエンド Web サーバーの組み込みコンポーネントとして稼働する実行可能コードに対するサポートも用意されています。このようなサーバー側実行可能コードの例としては、次のようなものがあります。

- Java servlet
- Oracle Web Listener 用カートリッジ
- サーバー側プラグイン

junctioncp ユーティリティーの **-c** オプションを使用して、バックエンド・サーバーへの接合を作成できます。 そうすると、WebSEAL がそのサーバーあての HTTP 要求のヘッダーに、 Policy Director 固有のクライアント識別情報とグループ・メンバーシップ情報を挿入します。

207ページの『クライアント識別情報を挿入する (-c オプション)』を参照してください。

Policy Director 固有の HTTP ヘッダーによって、接合先第三者サーバー上のアプリケーションで、クライアントの Policy Director 識別に基づいている、ユーザー固有のアクションが実行できます。

WebSEAL では、次のような Policy Director 固有の HTTP ヘッダーを提供します。

Policy Director 固有の HTTP ヘッダー	説明
iv-user	クライアントの名前。クライアントが認証されていない (不明の) 場合、デフォルトでは “Unauthenticated” です。
iv-groups	クライアントが属するグループのリスト。二重引用符で囲んだグループ名をコンマで区切ったリスト。
iv-creds	Policy Director クリデンシャルを表す、コード化された不透明データ構造。リモート・サーバーにクリデンシャルを提供するので、中段のアプリケーションでは、許可 API を使用して許可サービスを呼び出せます。 *Policy Director Programmer’s Guide and Reference* を参照してください。

HTTP ヘッダー項目は、環境変数 HTTP_IV_USER、HTTP_IV_GROUP、および HTTP_IV_CREDS として、CGI アプリケーションで使用可能です。 その他の非 CGI アプリケーション・フレームワークの場合は、 HTTP 要求からヘッダーを抜き出す方法について、該当するプロダクトの資料を参照してください。

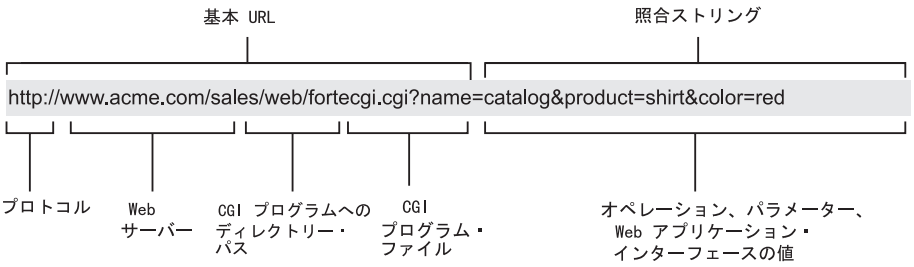
動的 URL に対するアクセス制御を提供する

現行の Web 環境では、ユーザーは、急激に変化する情報に即時にアクセスできます。多くの Web アプリケーションは、それぞれのユーザー要求に対する応答として、動的に URL を生成します。このような動的 URL は、短時間しか存在しない場合があります。動的 URL は、本質的に一時的なものには違いありませんが、望ましくない使用やアクセスに対して強力な保護が必要であることに変わりはありません。

動的 URL とは

一部の高度に精巧な Web アプリケーション・ツールでは、標準 Web ブラウザーを使用して、 Web サーバーの CGI インターフェースを介してアプリケーション・サーバーと通信します。

このようなツールはすべて、動的 URL と隠し書式要素を使用して、要求されたオペレーションを (そのパラメーター値と共に) アプリケーション・サーバーに伝えます。動的 URL は、特定のオペレーションとそのパラメーター値で標準 URL アドレスを補足します。URL の照会ストリング部分は、Web アプリケーション・インターフェースにオペレーション、パラメーター、値を提供します。



ACL ネームスペース・オブジェクトを動的 URL にマップする

WebSEAL では、保護オブジェクト・ネームスペース・モデルとポリシー・テンプレート (ACL) を使用して、データベース要求によって生成される URLs など、動的に生成された URL を機密保護します。 WebSEAL へのそれぞれの要求は、許可プロセスの最初のステップとして、特定のネームスペース・オブジェクトに解決されます。ネームスペース・オブジェクトに適用された ACL は、動的 URL がそのオブジェクトにマップされると、それに対する必要な保護を指示します。

動的 URL は一時的に存在するだけであるため、事前構成許可ポリシー・データベース項目を設けておくことはできません。 WebSEAL では、多くの動的 URL を単一の静的保護オブジェクトにマップするメカニズムを備えることで、この問題を解決しています。

テキスト・ファイルには、オブジェクトからネームスペースへのパターンのマッピングが含まれます。

UNIX: `/opt/intraverse/www/lib/dynurl.conf`

Windows: `C:¥Program Files¥IBM¥Policy Director¥www¥lib¥dynurl.conf`

このファイルを編集して、これらのマッピングを変更します。なお、このファイルは、デフォルトでは存在しないため、作成する必要があります。ファイル内の項目の形式は、次のとおりです。

object pattern

WebSEAL では、ネームスペース内に 1 つのオブジェクトを構成するパラメーターのセットを定義する、UNIX シェル・パターン (ワイルドカードを含む) のサブセットを使用します。 WebSEAL では、このようなパラメーターに一致する動的 URL をすべて、そのオブジェクトにマップします。 WebSEAL がサポートする UNIX シェル・パターン照合文字は、次のとおりです。

文字	説明
¥	円記号の後に続く文字は、特殊シーケンスの一部です。たとえば、TAB 文字です。
?	単一の文字に対応するワイルドカード。たとえば、ストリング abcde には、表現 ab?de で対応します。
*****	ゼロ個以上の文字に対応するワイルドカード。
[ ]	どれでも対応できる一組の文字を定義します。たとえば、ストリング abcde には、正規表現 ab[cty]de で対応します。
^	否定を示します。たとえば、表現 ^[ab] で、'a' または 'b' 以外のすべての文字に対応します。

次の例には、貸方残高検索を実行する動的 URL の書式を示してあります。

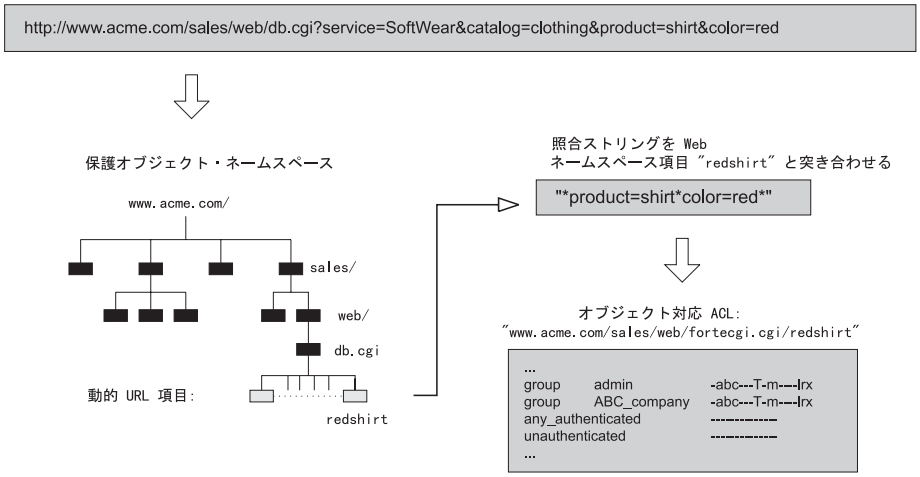
http://*server-name*/home-bank/owa/acct.bal?acc=*account-number*

この動的 URL を表すネームスペース・オブジェクトは、次のようになります。

http://<server-name>/home-bank/owa/acct.bal?acc=*

この例の動的 URL を綿密に検討してみると、特定の口座番号を記述していることが分かります。home-bank の口座残高を表すネームスペース・オブジェクトが、ACL 許可はどの口座にも適用されることを示しています。どの口座にも適用される理由は、項目 (acc=*) の最後の部分にアスタリスク・ワイルドカードが使用されており、これはすべての文字に対応するからです。

次の図には、特定の保護ネームスペース・オブジェクトにマップされた特定の動的 URL のモデル・ケースをそっくり示してあります。なお、この例では、ワイルドカードは一切使用されていません。



動的 URL 用として WebSEAL を更新する

WebSEAL 保護オブジェクト・ネームスペースを dynurl.conf 構成ファイル内に記入される項目で更新する場合は、**dynurlcp** ユーティリティーを使用します。dce_login を使用して、セキュア・ドメインにログインする必要があります。

dynurlcp ユーティリティーを使用して、 WebSEAL 保護オブジェクト・ネームスペースを更新する場合は、次のようにします。

1. dynurl.conf 構成ファイルの動的 URL 項目を作成、編集、または削除する。
2. 変更を加え終えたら、**dynurlcp** ユーティリティーを使用してサーバーを更新する。

```
dynurlcp -e /.:/subsys/intraverse/secmgr/server/ host update
```

動的 URL をネームスペース内で解決する

ネームスペース・オブジェクトへの動的 URL の解決は、 dynurl.conf 構成ファイル内の項目の配列によって異なります。

ネームスペース項目への動的 URL のマップを試みると、dynurl.conf 構成ファイル内のマッピングのリストがスキャンされます。ファイルのスキャンは、最初の一致パターンが見つかるまで、上から下へ行われます。

最初の一致が見つかると、WebSEAL では、対応するネームスペース項目を使用して、後続の許可検査を行います。一致が見つからない場合は、WebSEAL は、 URL 自体からパスの `http://server` 部分を除いたものを使用します。

限定度が高い ACL に対応するマッピングほどリストの上位に保持します。たとえば、書籍販売プロシージャー (販売受注アプリケーションの) は、 1 つのブック・クラブ・グループに限定されているとします。ただし、販売受注アプリケーションの残りには、すべてのユーザーがアクセスできます。そこで、マッピングは次の表に示す順序になるはずです。

ネームスペース項目	URL パターン
/ows/sales/bksale	/ows/db-apps/owa/book.sales*
/ows/sales/general	/ows/db-apps/owa/*

マッピング項目が逆の順序であったとすると、/ows/db-apps/owa ディレクトリー内のすべてのストアード・プロシージャーが、 /ows/sales/general ネームスペース・オブジェクトにマップすることになります。この場合は、このネームスペース解決の誤りのため、セキュリティーの侵害を招く可能性があります。

GET 方式と POST 方式のデータ伝送

URL 正規表現をネームスペース項目にマップすると、URL 形式では、形式が GET 方式から生成されたものと想定するはずです。この想定では、使用されているのが POST 方式であるか、 GET 方式であるかは問題になりません。

GET 方式のデータ伝送では、WebSEAL は、*動的データ* を URL に付加します。動的データの例としては、書式内でユーザー用として提供されるデータがあります。

POST 方式のデータ伝送では、WebSEAL は、動的データを要求の本体に組み込みます。

ACL の評価

動的 URL がネームスペース項目に解決された後は、標準 Policy Director ACL 継承モデルが使用されます。このモデルによって、要求が処理されるか、禁止される (特権が不十分のため) かが決まります。

動的 URL の例示: Travel Kingdom 社の場合

次の例には、Oracle Web Listener によって生成された URL を、どうすれば企業イントラネットで保護できるかが示してあります。

この例で使用されている動的 URL Web サーバーは、Oracle Web Listener です。このテクノロジーは、他の動的 URL Web サーバーにも応用できます。

アプリケーション

Travel Kingdom は、インターネットを通して顧客に旅行予約サービスを提供する組織です。 そこで、自社の Web サーバー上で 2 つの Oracle データベース・アプリケーションを運用して、1 つは自社ファイアウォール内から、もう 1 つはインターネットを通して、それぞれアクセスできるようにする予定です。

- **旅行予約システム**

  許可顧客の場合は、リモートで予約し、自分の予約の現在の状況について照会できます。Travel Kingdom の従業員も、電話による顧客に代わって予約を行い、変更を処理し、その他にも多くのトランザクションを実行できます。外部の顧客は、サービスに対してクレジット・カードで決済するため、WebSEAL では、そうした情報の伝送をしっかり保護する必要があります。

- **管理マネージャー**

  ほとんどの企業がそうであるように、Travel Kingdom でも、給与、地位、経験に関する情報が入っている管理データベースを保守しています。このデータには、各従業員の写真が添えられています。

インターフェース

データベースに入っている次のようなストアード・プロシージャーへのアクセスを提供するように、Oracle Web サーバーを構成できます。

/db-apps/owa/tr.browse	すべてのユーザーが旅行先、旅行代金などについて照会できるようにします。
/db-apps/owa/tr.book	予約を行う場合に使用します (旅行代理業部門従業員と認証顧客)。
/db-apps/owa/tr.change	現在の予約を検討し変更する場合に使用します。
/db-apps/owa/admin.browse	従業員であればだれもが、内線番号、E-mail アドレス、写真などのような、制限が設けられていない従業員情報を表示させて見る場合に使用します。
/db-apps/owa/admin.resume	従業員が管理データベースに入っている自分の履歴書情報を表示させて見たり、変更したりできるようにします。
/db-apps/owa/admin.update	管理部門従業員が従業員に関する情報を更新する場合に使用します。

Web スペース構造

WebSEAL サーバーを使用して、Travel Kingdom の統一 Web スペースへのセキュア・インターフェースを提供します。

旅行予約アプリケーションと管理アプリケーションの両方を実行する Oracle Web サーバーへの接合 (/ows) ができます。

セキュリティー・ポリシー

使いやすいシステムを保持しながらも、Web リソースに適切なセキュリティーを実施するために、業務上次のようなセキュリティー目標を設けました。

- 旅行代理業部門従業員は、すべての予約を完全に制御できる。
- 認証顧客の場合は、自分自身の予約については、実行も変更もできるが、自分以外の認証顧客の旅行データに干渉することはできない。
- 管理部門従業員は、管理情報のすべてに対して完全なアクセス権をもつ。
- Travel Kingdom の管理部門以外の従業員は、自分自身の履歴書情報を変更し、自分以外の従業員の部分的な情報を表示させて見ることができる。

動的 URL とネームスペースのマッピング

セキュリティー・ポリシー目標を達成するためには、動的 URL から ACL ネームスペース項目へのマッピングを構成する必要があります。 なお、このようなマッピングの配列 (順序付け) が、セキュリティー目標の達成に重要な役割を果たします。

マッピングは、次の表に示すように構成する必要があります。

ネームスペース項目	URL パターン
/ows/tr/browse	/ows/db-apps/owa/tr.browse¥?dest=*&date=??/??/????
/ows/tr/auth	/ows/db-apps/owa/tr.book¥?dest=*&depart=??/??/????&return=??/??/????
/ows/tr/auth	/ows/db-apps/owa/tr.change
/ows/admin/forall	/ows/db-apps/owa/admin.resume
/ows/admin/forall	/ows/db-apps/owa/admin.browse¥?empid=[th]???
/ows/admin/auth	/ows/db-apps/owa/admin.update¥?empid=????

セキュア・クライアント

クライアントは、機密保護機能のある、暗号化されたチャネルを通して WebSEAL に認証されます。

Web インターフェースを使用したい顧客の場合は、さらに、 Travel Kingdom Web マスターに登録して、アカウントを受け取る必要があります。

アカウント構造とグループ構造

システム上に次のようにグループを作成します。

Staff	Travel Kingdom の組織に属する従業員
TKStaff	Travel Kingdom の旅行代理業部門従業員
AdminStaff	Travel Kingdom の管理部門従業員。なお、管理部門従業員は、Staff グループにも入っています。
Customer	インターネットによる旅行の予約を希望する、 Travel Kingdom の顧客

各ユーザーには、セキュア・ドメイン内にそれぞれアカウントを与えて、 WebSEAL サーバーが個々にユーザーを識別できるようにします。WebSEAL では、ユーザーの識別を Oracle Web サーバーに渡し、Web リソースのすべてに単一サインオン・ソリューションを用意します。

アクセス制御

次の表には、前記の情報を適用した結果であるアクセス制御を一覧表にして示してあります。

/ows/tr/browse	unauthenticated	Tr
	any_authenticated	Tr
/ows/tr/auth	unauthenticated	-
	any_authenticated	-
	グループ TKStaff	Tr
	グループ Customer	PTr
/ows/admin/forall	unauthenticated	-
	any_authenticated	-
	group Staff	Tr
/ows/admin/auth	unauthenticated	-
	any_authenticated	-
	group AdminStaff	Tr

予約と旅行計画維持のオブジェクトに対する、Customer (顧客) と TKStaff の特権は同じですが、例外が 1 つあります。この例外とは、顧客の場合は、情報を暗号化して (プライバシー許可)、非トラステッド・インターネットを通して *機密データ* を提供するにあたって、さらにセキュリティーを確保する必要があるという点です。機密データとしては、たとえば、クレジット・カード情報があります。

結論

この単純な例で示したのは、次のことを行うことができるシステムを展開する概念です。

- 機密情報を機密保護する。
- ユーザーを認証する。

- 機密情報へのアクセスを許可する。

さらに、システムの認証ユーザーの識別情報は、WebSEAL と Oracle Web サーバーの両方に認識されています。この識別情報は、監査可能の単一サインオン・ソリューションを提供する場合に使用されます。

第17章 NetSEAL: 概説

Policy Director NetSEAL は、着信 TCP/IP 通信を機密保護するための仮想私設網 (VPN) ソリューションの 1 つです。リソース・マネージャーとして、NetSEAL は、特定の TCP アプリケーションに接続できるユーザーの機能を制御します。NetSEAL では、宛先ポートとクライアント識別情報に基づいたアクセス制御を実行します。 NetSEAL によって、どんなネットワーク・アプリケーション・サーバーでも、 Policy Director セキュリティー・サービスに統合できます。

この章は、次の各節に分かれています。

NetSEAL の概要

NetSEAL によって、Policy Director セキュア・ドメイン内の TCP ベースのアプリケーションとサービスへのアクセスが制御できます。Windows クライアントの場合は、Policy Director NetSEAT クライアントを通して、NetSEAL へのセキュア通信が得られます。

NetSEAT と NetSEAL との間の通信は、SSL トンネルまたは GSS トンネルのどちらかを使用して機密保護できます。NetSEAT クライアントと Policy Director サーバーの間に確立されたセキュア・リンクは、要求側クライアントのユーザー名とパスワードを使用して認証されます。

- NetSEAT と NetSEAL の間の通信を機密保護する場合は、 *SSL チャネル* を使用します。
- NetSEAL サーバーから NetSEAL サーバーへの通信を機密保護する場合は、 *GSS トンネル* か NetSEAL 接合を使用します。Policy Director サーバー間に確立された GSS トンネルは、常に、要求側クライアントに代わって接続を行っている、 Policy Director サーバー・ユーザーを使用して認証されます。 GSS トンネルを通して、2 つのサーバーは相互に相手側を認証します。 2 番目のサーバーが常にクライアントに対するアクセス制御を実行します。

NetSEAL 接合では、Policy Director サーバーを通って別の Policy Director サーバーまたはネットワークに至る通信の転送方向を確立します。 NetSEAL 接合を通る通信を機密保護する場合は、GSS トンネルを使用します。

NetSEAL アクセス制御は、粗アクセス制御です。制御は、アプリケーションが listen している特定のポートまでです。アプリケーションによって操作されるリソースには、密アクセス制御の利点はありません。

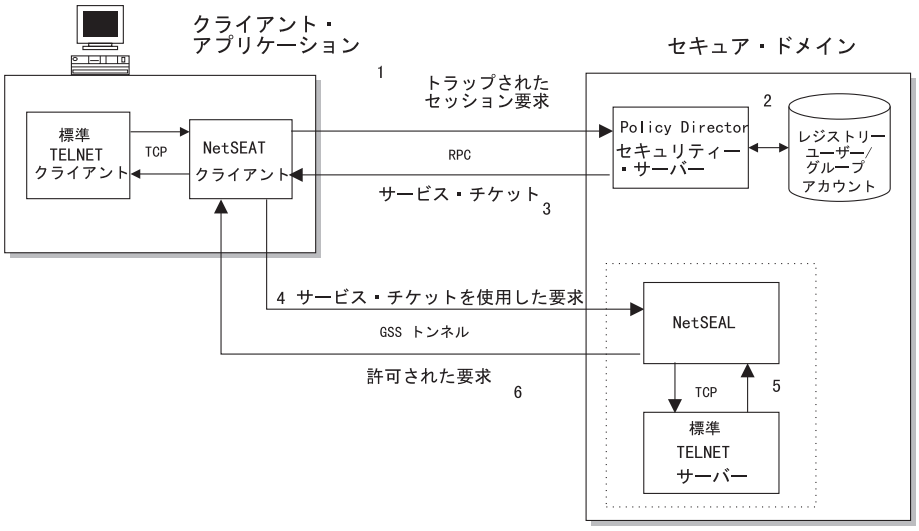
この章では、NetSEAL を使用するネットワークのモデル・ケースをいくつか説明します。 図では、TELNET リモート・ログイン・アプリケーションを TCP アプリケーションの例として使用します。 それぞれのモデル・ケースでは、NetSEAL は、次のものに基づく要求に応答します。

- 要求のソース。
- 影響を受けるオブジェクト (宛先ポートや NetSEAL 接合など) に対する許可。
- 接続にかかわるプリンシパル。

GSS トンネルを介して NetSEAT クライアントから NetSEAL へ

NetSEAT が GSS トンネルを使用するように構成されていると、NetSEAT は発信要求をトラップし、 RPC を使用して、 Policy Director セキュリティー・サーバーに対してそのクライアントを認証します。さらに、要求されたアプリケーションに関連付けられた特定のポートについて、許可検査が実行されます。

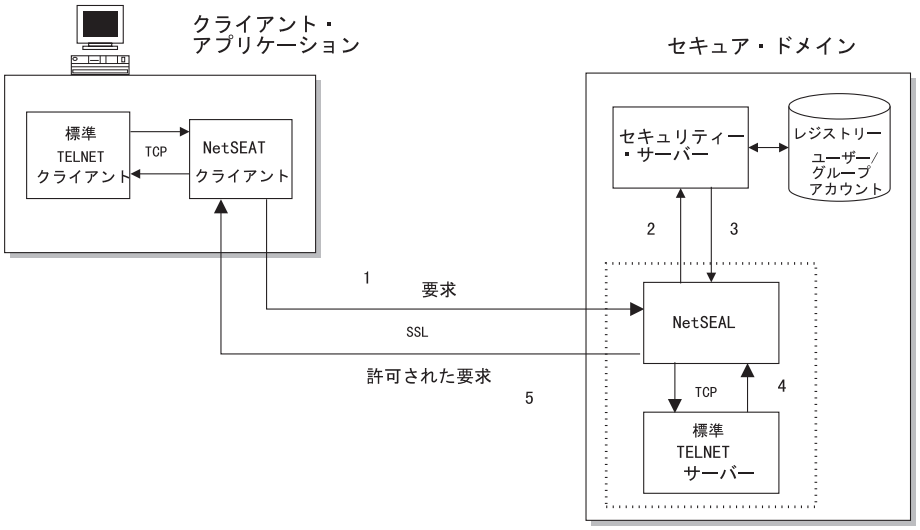
認証および許可プロセスに問題がなければ、NetSEAT と NetSEAL サーバーとの間に GSS トンネルが確立されます。要求された TCP アプリケーションに NetSEAL からアクセスするには、 TCP を使用します。



SSL を介した NetSEAT クライアントと NetSEAL

SSL を使用するように NetSEAT を構成する場合、認証と許可は、NetSEAL と Policy Director セキュリティー・サービスとの間で処理されます。NetSEAL では、クライアントの識別情報としてユーザー名とパスワードを受け入れることができます。

認証および許可プロセスで問題がなければ、Policy Director は、その要求を処理します。NetSEAL から必要な TCP アプリケーションにアクセスするには、TCP を使用します。

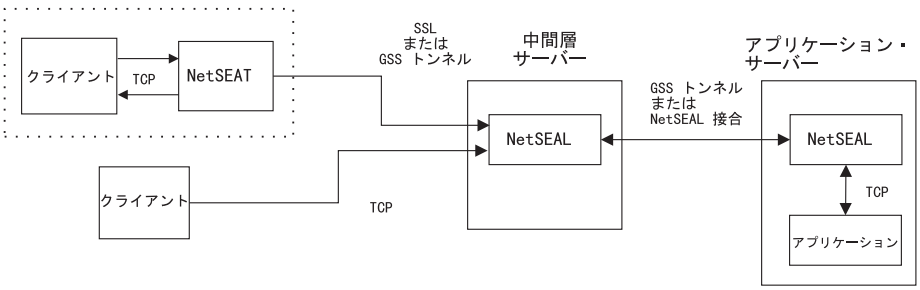


NetSEAL ネットワーク・セグメント

NetSEAL トランザクションにおける接続要求には、ネットワーク経路に沿って、さまざまなレベルの保護が使用されます。 236ページの『SSL を介した NetSEAT クライアントと NetSEAL』で説明したように、 NetSEAT クライアントは、NetSEAL サーバーとの SSL または GSS 接続をサポートします。

注: 設計によって、NetSEAL サーバー間接続は、*常に* GSS となります。 2 つの NetSEAL サーバー間では、SSL 接続を使用しないでください。

NetSEAL からローカルまたはリモートの TCP アプリケーション・ポートに至る最終経路では、常に TCP が使用されます。



次の表に、それぞれの接続セグメントごとの保護のレベルの要約を示します。

接続セグメント	保護
NetSEAT クライアントから NetSEAL サーバーへ	SSL または GSS トンネル
TCP クライアントから NetSEAL サーバーへ	なし
NetSEAL サーバーから NetSEAL サーバーへ	GSS トンネル
NetSEAL 接合	GSS トンネル
NetSEAL サーバーから TCP アプリケーション・ポートへ	なし

NetSEAL は、ローカル・アプリケーションとリモート・アプリケーションの両方に関して、同じ接続決定プロセスを使用します。

- 要求されたポートは (ACL によって) 保護されているか?
- 保護ポートに関して、ユーザーは、アクセスに対する適切な許可を得ているか?
- 無保護ポートに関しては、発信接続を許可する。

また、NetSEAL では、セキュリティー・マネージャーに必要な着信情報の問題と発信接続処理の問題とを分けて考えます。つまり、セキュリティー・マネージャーは、NetSEAT クライアントが接続要求をローカルとリモートのいずれでトラップするかを認識する必要はないということです。

クライアントと NetSEAL との間のサービスの具体的な説明

次のシナリオでは、クライアントと NetSEAL 保護の TCP アプリケーションとの間で可能な対話のタイプを具体的に説明します。クライアントには、NetSEAT クライアントと NetSEAT 以外のクライアントがあります。

ここで説明するシナリオは、次のとおりです。

- 『Policy Director サーバーとの着信トンネル接続』
- 239ページの『保護ホストとの着信トンネル接続』
- 240ページの『Policy Director サーバーとの着信 TCP 接続』

Policy Director サーバーとの着信トンネル接続

最初のこのシナリオでは、Policy Director サーバー上のアプリケーションを宛先とする発信接続をトラップするように NetSEAT クライアントを構成します。NetSEAT クライアントがこの通信をトラップした後に、Policy Director サーバー上の NetSEAL にセキュア・トンネルが確立されます。この例の場合、ポート 23 宛ての要求は、このトンネルを介して転送されます。

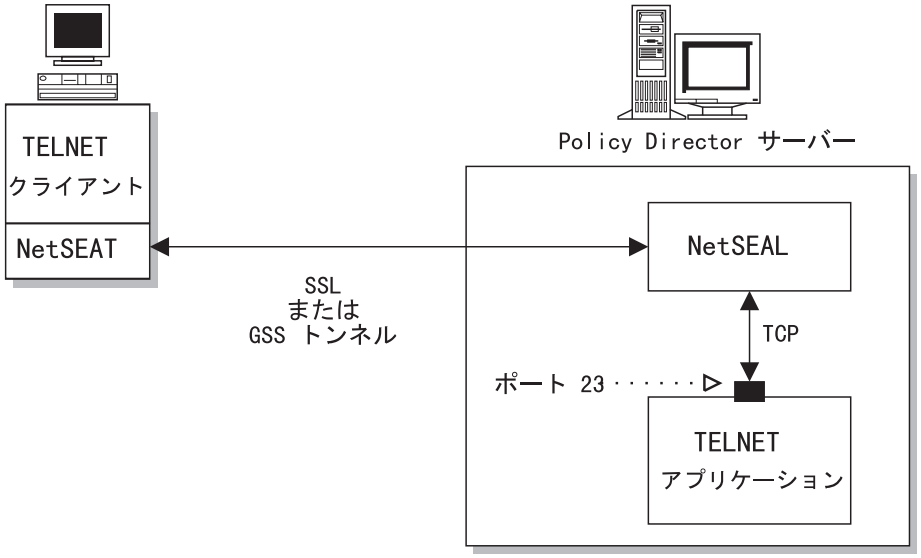
認証プロセスは、ユーザーには見えません。

NetSEAL サーバーは、次の方法でトランザクションを完了します。

1. ポートの ACL に従って、ユーザーは要求ポートと接続することができるか?

   Yes -- 要求ポートとの TCP 接続を確立する。

   No -- 接続要求を拒否する。



保護ホストとの着信トンネル接続

このシナリオでは、保護されたリモート・サーバーに常駐するアプリケーションについて考えます。アプリケーション・サーバーは、 Policy Director サーバーでも第三者サーバーでもかまいません。Policy Director は、2 つの NetSEAL サーバー間の通信に常に GSS を使用します。

このシナリオの場合、NetSEAL は、Policy Director でサポートしていないプラットフォーム上で稼働する TCP アプリケーションを保護することができるとします。

NetSEAL サーバーは、次の方法でトランザクションを完了します。

1. ユーザーは、(その ACL に従って) 宛先サーバー上の要求ポートに接続することができるか?

   Yes -- 続行する。

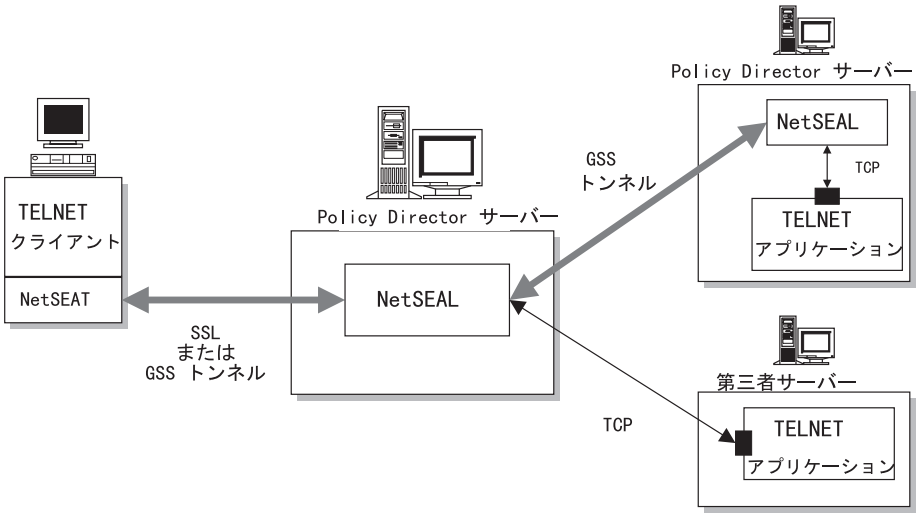
   No -- 接続要求を拒否する。

2. 宛先は、Policy Director サーバーか?

   Yes -- そのサーバーへのセキュア・トンネルを確立する。 要求ポートとの TCP 接続を確立する。

   No -- 要求ポートとの TCP 接続 (非セキュア) を確立する。

第三者アプリケーション・サーバーでは、常に、無保護 TCP 接続を使用します。このような構成は、トラステッド・ネットワーク環境内で使用してください。



Policy Director サーバーとの着信 TCP 接続

このシナリオでは、 NetSEAT 以外の TCP クライアント・ユーザーの場合について考えます。 Policy Director では、このようなクライアントを非認証であるとみなします。要求ポートが無保護 (ACL なし) であるならば、Policy Director は、そのポートへのアクセスを許可します。ACL によってポートが保護されている場合は、セキュリティー・マネージャーが非認証アクセスに関してその ACL を検査します。

この構成では、ネットワーク・サービスへの直接アクセスが保護されます。外部の許可サービスは、そのクライアントの IP アドレスを使用して、アクセス権限を決定することが可能です。

NetSEAL サーバーは、次の方法でトランザクションを完了します。

1. 要求は Policy Director (ポートの ACL) によってトラップされるか?

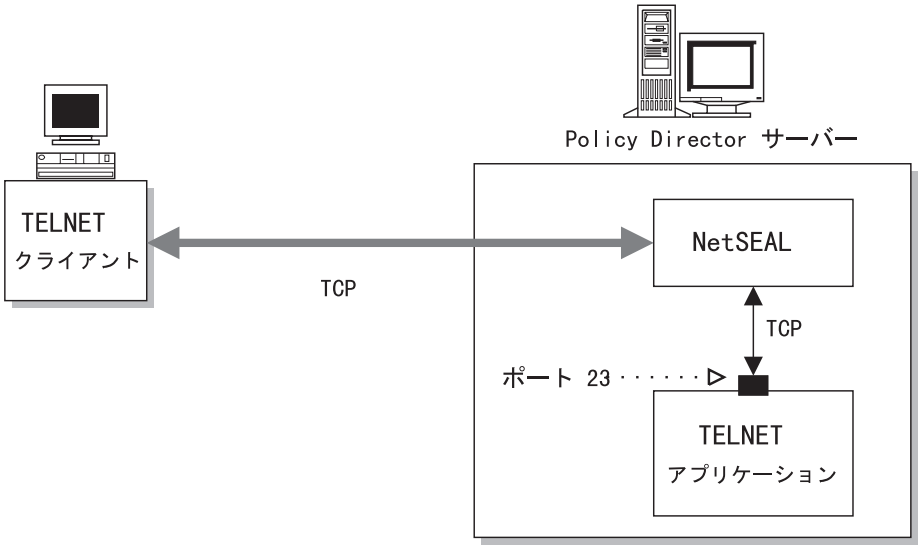
   Yes -- 要求をセキュリティー・マネージャー (secmgrd) に渡す。

   No -- 着信接続を許可する。

2. ポートの非認証要求は許可されるか?

   Yes -- 要求ポートとの TCP 接続を確立する。

   No -- 接続要求を拒否する。



NetSEAL と NetSEAL との間のサービスの具体的な説明

次のシナリオでは、2 つのサーバーの間で可能な対話のタイプを具体的に説明します。最初の NetSEAL サーバー (ローカル・クライアントがある) が、これらのシナリオで説明する接続を開始し、リモート NetSEAT クライアントから開始するのではないとします。

最初の NetSEAL サーバー (ローカル・クライアントがある) が、これらのシナリオで説明する接続を開始し、リモート NetSEAT クライアントから開始するのではないとします。このローカル・クライアントは、サーバーのコンソールから操作したり、あるいは、リモート・ロケーションからこのサーバーに Telnet でログインすることが可能です。バックエンド NetSEAL サーバーは、TCP アプリケーションを保護することができます。

ここで説明するシナリオは、次のとおりです。

- 『Policy Director サーバーとの発信接続』
- 242ページの『保護ホストとの発信接続』

Policy Director サーバーとの発信接続

GSS トンネルを使用して、2 つの Policy Director NetSEAL サーバーの間に接続を確立します。最初の NetSEAL サーバー (ローカル・クライアントがある) が接続を開始し、リモート NetSEAT クライアントから開始するのではないとします。Policy Director は、接続を許可または拒否し、許可通信を保護することができます。

Policy Director サーバーは、次の方法でトランザクションを完了します。

1. 宛先マシン上の要求ポートは (ACL で) 保護されているか?

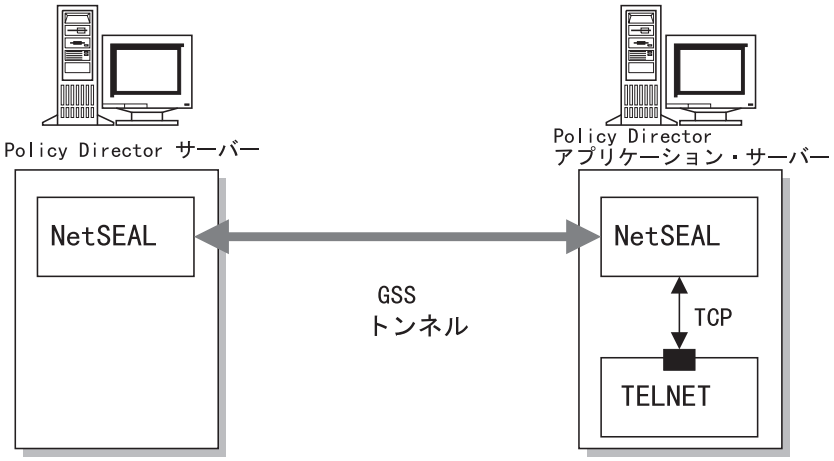
   Yes -- 要求をセキュリティー・マネージャー (secmgrd) に渡す。

   No -- 発信接続を許可する。

2. ポートの非認証要求は許可されるか?

Yes -- そのサーバーへのセキュア・トンネルを確立する。要求ポートとの TCP 接続を確立する。

No -- 接続要求を拒否する。



保護ホストとの発信接続

TCP を使用すれば、Policy Director NetSEAL サーバーと第三者サーバーとの間に接続を確立することができます。ただし、TCP を介して確立された接続は、どれも、セキュア接続にはなりません。バックエンドの第三者サーバー上には、NetSEAL サーバーは存在しません。Policy Director は、バックエンド・サーバーとの接続を許可または拒否するだけです。Policy Director は、この接続を使用する通信を機密保護することはできません。

Policy Director サーバーは、次の方法でトランザクションを完了します。

1. 宛先マシン上の要求ポートは (ACL で) 保護されているか?

   Yes -- 要求をセキュリティー・マネージャー (secmgrd) に渡す。

   No -- 発信接続を許可する。

2. 宛先サーバー上の要求ポートにアクセスする許可がユーザーに与えられているか?

   Yes -- 続行する。

   No -- 接続要求を拒否する。

3. ポートに保全性とプライバシーが設定されているか?

   Yes -- 接続要求を拒否する。

   No -- 要求ポートへの TCP 接続を確立する。

NetSEAL 接合の概要

NetSEAL 接合 には、Policy Director サーバーのネットワークを介し、通信を安全確実に宛先サーバーや宛先ネットワークに転送するためのメカニズムが備わっています。NetSEAL 接合によって、Policy Director サーバーを介して転送するパケットの方向が決まります。

NetSEAL 接合は、単一方向の静的経路です。単一方向接合を使用すれば、それぞれの Policy Director サーバーのマネージャーは、それらのネットワークへのアクセスをより確実に制御することが可能になります。伝送のそれぞれの方向ごとに、別個の NetSEAL 接合が必要です。ただし、NetSEAL 接合を通るデータ・フローは、常に、両方向となります。

GSS トンネルは、NetSEAL 接合を通る通信を機密保護します。その上で、通信パス内の最終の Policy Director サーバーが宛先ポートとの TCP 接続を使用します。この宛先ポートは、Policy Director サーバー自体に存在する場合もあります。

NetSEAL 接合によって、組織を通る通信に関してデータ保護とセキュリティーが提供されます。組織は、地理的または機能的に区分けすることができます。たとえば、NetSEAL 接合は、地理的に分離された 2 つの Policy Director サーバーの間に非トラステッド・ネットワークが存在している場合に役に立ちます。また、これら 2 つの Policy Director サーバーは、同じセキュア・ドメインのメンバーでもあります。

それぞれの接合ごとに、ソースの Policy Director サーバー、宛先、および経路指定方向が指定されます。この宛先は、別の Policy Director サーバーやネットワーク仕様であってもかまいません。接合を使用することで、ファイアウォール構成が容易になります。これは、その接合を横断するすべての通信では、そのファイアウォールを通る 1 つの経路だけが必要だからです。

NetSEAL 接合の構成

管理者は、**ivadmin** ユーティリティーを使用して NetSEAL 接合を作成することができます。この **ivadmin** ユーティリティーには、NetSEAL 接合を追加、削除、およびリストするためのコマンドが組み込まれています。接合は、Policy Director サーバー相互間、あるいは、Policy Director サーバーとネットワークとの間に作成することができます。

285ページの『付録A. ivadmin を使用した Policy Director 管理』を参照してください。

NetSEAL 接合とアクセス制御

NetSEAL では、アプリケーション・サーバー上のポートへのアクセスを制御するための 2 つの ACL 許可が認識されます。

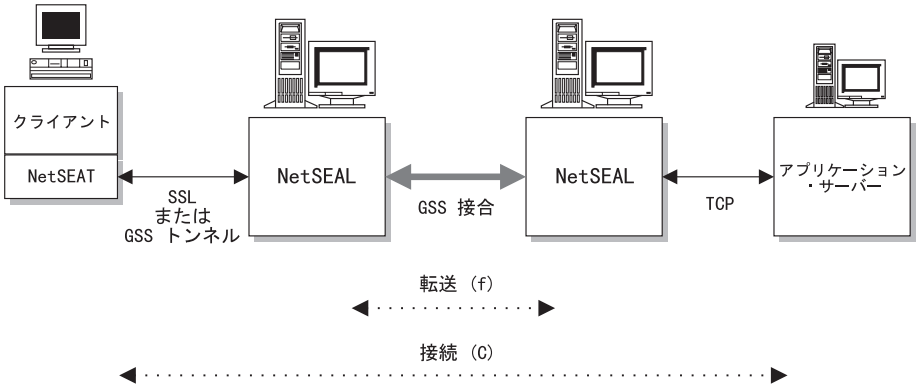
宛先ポート・オブジェクトの ACL では、そのポートへのアクセスを制御します。ACL 記入項目には、ユーザーまたはグループがそのポートにアクセスできるようにするための接続 (C) 許可を指定する必要があります。

Policy Director サーバー上の ACL は、発信接続を対象としており、NetSEAL 接合を通るトラバースを制御します。ACL 記入項目には、ユーザーまたはグループがその接続を横断してアクセスできるようにするための転送 (f) 許可を指定する必要があります。

接合サーバーのチェーンの中間にあるそれぞれの Policy Director サーバー・オブジェクトごとに、転送 (f) 許可を使用し検査します。

NetSEAL 保護オブジェクト許可	アクセス	説明

C	接続	NetSEAL サーバーを介してローカルまたはリモートの保護サービスに接続する。
f	転送	NetSEAL 接合を横断する発信接続、つまり接合のトラバースを許可する。



NetSEAL 接合によって制御するサービスの具体的な説明

NetSEAL 接合によって、組織を通る通信に関してデータ保護とセキュリティーが提供されます。組織は、地理的または機能的に区分けすることができます。たとえば、NetSEAL 接合は、地理的に分離された 2 つの Policy Director サーバーの間に非トラステッド・ネットワークが存在している場合に役に立ちます。また、これら 2 つの Policy Director サーバーは、同じセキュア・ドメインのメンバーでもあります。

ここで説明するシナリオは、次のとおりです。

- 『Policy Director サーバーとの着信接合接続』
- 245ページの『保護ホストとの着信接合接続』
- 245ページの『接合 Policy Director サーバーとの発信接続』
- 246ページの『接合保護ホストとの発信接続』

Policy Director サーバーとの着信接合接続

このシナリオでは、保護されたリモート Policy Director サーバーに常駐するアプリケーションについて考えます。このシナリオでは、NetSEAL 接合としての Policy Director サーバー相互間に GSS トンネルを明示的に確立するものとします。 この時点で、宛先ポートへのアクセス制御に、転送許可に関する考慮事項を組み入れます。

Policy Director サーバーは、次の方法でトランザクションを完了します。

1. ユーザーは、(その ACL に従って) 宛先サーバー上の要求ポートと接続することができるか?

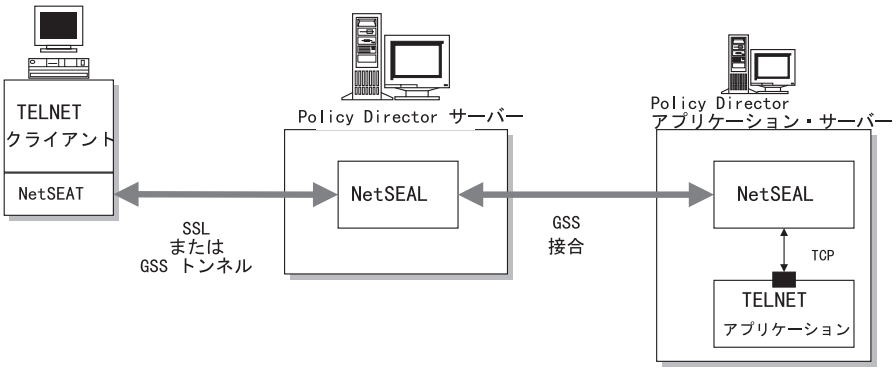
   Yes -- 続行する。

   No -- 接続要求を拒否する。

2. ユーザーは、その接合を横断して転送することができるか?

   Yes -- GSS 接合を横断して要求を転送する。 要求ポートとの TCP 接続を確立する。

   No -- 接続要求を拒否する。



保護ホストとの着信接合接続

このシナリオでは、保護されたリモート第三者サーバーに常駐するアプリケーションについて考えます。このシナリオでは、NetSEAL 接合としての Policy Director サーバー相互間に GSS トンネルを明示的に確立するものとします。 この時点で、宛先ポートへのアクセス制御に、転送許可に関する考慮事項を組み入れます。

Policy Director サーバーは、次の方法でトランザクションを完了します。

1. ユーザーは、(その ACL に従って) 宛先サーバー上の要求ポートと接続することができるか?

   Yes -- 続行する。

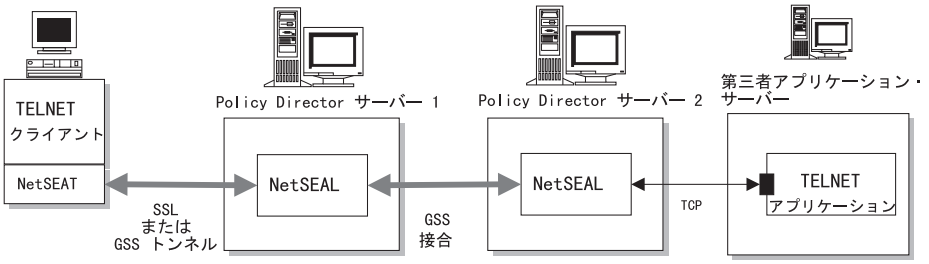
   No -- 接続要求を拒否する。

2. ユーザーは、接合を横断して転送することができるか?

   Yes -- 接合を横断して要求を転送する。 要求ポートとの TCP 接続を確立する。

   No -- 接続要求を拒否する。

第三者アプリケーション・サーバーでは、常に、無保護 TCP 接続を使用します。このような構成は、トラステッド・ネットワーク環境内で使用してください。



接合 Policy Director サーバーとの発信接続

このシナリオでは、保護されたリモート Policy Director サーバーに常駐するアプリケーションについて考えます。このシナリオでは、NetSEAL 接合としての Policy Director サーバー相互間に GSS トンネルを明示的に確立するものとします。 この時点で、宛先ポートへのアクセス制御に、転送許可に関する考慮事項を組み入れます。これによって、中間層のサーバーを確実に保護できるようになります。

Policy Director サーバーは、次の方法でトランザクションを完了します。

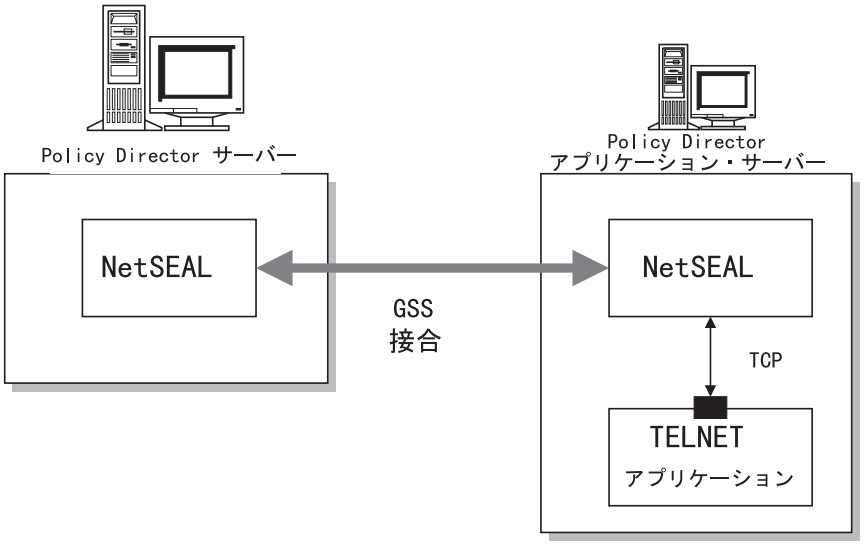
1. 宛先マシン上の要求ポートは (ACL で) 保護されているか?

   Yes -- 要求をセキュリティー・マネージャー (secmgrd) に渡す。

   No -- 発信接続を許可する。
2. ユーザーは、接合を横断して転送することができるか?

   Yes -- 接合を横断して要求を転送する。 要求ポートとの TCP 接続を確立する。

   No -- 接続要求を拒否する。



接合保護ホストとの発信接続

このシナリオでは、保護されたリモート第三者サーバーに常駐するアプリケーションについて考えます。このシナリオでは、NetSEAL 接合としての Policy Director サーバー相互間に GSS トンネルを明示的に確立するものとします。 この時点で、宛先ポートへのアクセス制御に、転送許可に関する考慮事項を組み入れます。

Policy Director サーバーは、次の方法でトランザクションを完了します。

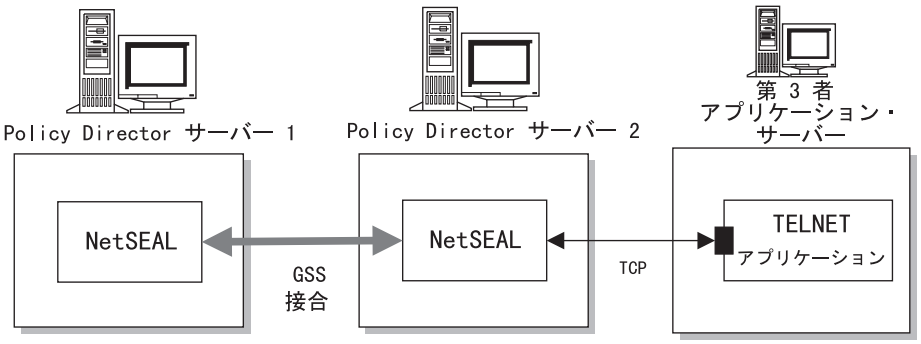
1. 宛先マシン上の要求ポートは (ACL で) 保護されているか?

   Yes -- 要求をセキュリティー・マネージャー (secmgrd) に渡す。

   No -- 発信接続を許可する。
2. ユーザーは、接合を横断して転送することができるか?

   Yes -- 接合を横断して要求を転送する。 要求ポートとの TCP 接続を確立する。

   No -- 接続要求を拒否する。



TCP サービスの保護

TCP サービス・ポートの ACL では、これらのポートへのアクセスを制御します。NetSEAL クライアント・ユーザーは、そのユーザーに対する接続 (C) 許可がポート・オブジェクトの ACL に指定されていれば、特定の TCP サービスにアクセスすることができます。

管理者は、ACL 内の該当の記入項目から接続許可を除去することで、TCP サービスへのアクセスを拒否することができます。

ACL 許可で、NetSEAL 通信の保護の品質を制御することも可能です。データ保全性許可とプライバシー許可のある種の組み合わせによって、保護の品質が決まります。NetSEAL 接合を介して、発信通信の保護の品質を制御することができます。 保護の品質を制御するには、宛先ポート・オブジェクトの ACL の記入項目に、保全許可とプライバシー許可を指定する必要があります。

テストされる ACL は、オブジェクトのネットワーク・アドレスとネットワーク・マスクによって最大限に特定されます。ACL 検査の実行対象である要求オブジェクトを見つける際には、宛先ポートの ACL の有無は考慮に入れられません。

たとえば、次のように ACL が構成されている場合、10.0.0.1 に Telnet でログインするクライアントには、 ACL 3 に従ってアクセスが許可されます。Policy Director は、一致するネットワーク上のポート 23 に明示的 ACL が入っている場合でもアクセスを許可します。

10.0.0.0:255.255.255.0	ACL1
10.0.0.0:255.255.255.0/Port 23	ACL2
10.0.0.1:255.255.255.255	ACL3

第18章 NetSEAL: 一般管理タスク

Policy Director NetSEAL は、着信 TCP/IP 通信を機密保護するための仮想私設網 (VPN) ソリューションの 1 つです。リソース・マネージャーとして、NetSEAL は、ユーザーが特定の TCP アプリケーションと接続できるかどうかを制御します。この章では、ネットワークに合わせて NetSEAL をカスタマイズする場合に実行できる一般管理タスクについて説明します。

この章は、次の各節に分かれています。

NetSEAL セキュリティーを使用可能 / 使用不可にする

NetSEAL を使用可能 / 使用不可にするには、**ivadmin** ユーティリティーを使用します。

NetSEAL を使用可能にする

特定の Policy Director サーバー上の NetSEAL を使用可能にするには、次のように入力します。

```
ivadmin> server enable /NetSEAL/hostname
```

ただし、 *hostname* は、サーバーのホスト名からドメイン名を除いたものです。

サービスがすでに使用可能になっている場合やサービスの指定が無効の場合、Policy Director はエラーを戻します。

Policy Director 配布の NetSEAL トラップ (IVTrap) 構成要素がインストールされていない場合、Policy Director は、デフォルトの設定により、NetSEAL を使用不可にします。

NetSEAL を使用不可にする

特定の Policy Director サーバー上の NetSEAL を使用不可にするには、次のように入力します。

```
ivadmin> server disable /NetSEAL/hostname
```

NetSEAL 状況

NetSEAL サーバー状況を検査するには、次の **server status** コマンドを使用します。

```
ivadmin> server status /NetSEAL/hostname
```

状況報告によって次の情報が表示されます。

- NetSEAL サーバーは使用可能と使用不可のいずれにされているか。
- NetSEAL サーバーは使用可能か。
- レプリカ NetSEAL 構成のデータベースは更新されているか否か。

NetSEAL アクセス制御の使用

Policy Director ACL 許可は、次のようなセキュリティーの問題を処理する場合に、NetSEAL 接続で使用することができます。

- 宛先ポートなどの TCP サービスへのアクセスの許可
- NetSEAL 接合を横断するパケット転送の許可
- データ保全性とプライバシーの保証

宛先ポート・オブジェクトの ACL では、そのポートへのアクセスを制御します。ACL 記入項目には、ユーザーまたはグループがそのポートをアクセスできるようにするための接続 (C) 許可を指定する必要があります。接続許可では、保護ネットワーク上のアプリケーション・サーバーへのアクセスも制御します。

Policy Director サーバー上の ACL は、発信接続を対象としており、 NetSEAL 接合を通るトラバースを制御します。ACL 記入項目には、ユーザーまたはグループがその接続を横断してアクセスできるようにするための転送 (f) 許可を指定する必要があります。

接合サーバーのチェーンの中間にあるそれぞれの Policy Director サーバー・オブジェクトごとに、転送 (f) 許可を使用し検査します。

	アクセス	説明
C	接続	NetSEAL サーバーを介してローカルまたはリモートの保護サービスに接続する。
f	転送	NetSEAL 接合を横断する発信接続、つまり接合のトラバースを許可する。

ACL 許可で、NetSEAL 通信の保護の品質を制御することも可能です。データ保全性許可とプライバシー許可のある種の組み合わせによって、保護の品質が決まります。

NetSEAL 接合を介して、発信通信の保護の品質を制御することができます。 宛先ポート・オブジェクトの ACL 内の記入項目に、保全性 (I) 許可とプライバシー (P) 許可を指定する必要があります。データ保全性とプライバシーは、トラステッド・ネットワーク上の第三者 (Policy Director 以外の) アプリケーション・サーバーまで拡張することはできません。

保護ネットワークの管理

ネットワークは、NetSEAL によって保護されている Policy Director 以外のサーバーとみなすことができます。**ivadmin** ユーティリティーを使用して、ネットワークを定義および管理します。このコマンドには、保護ネットワークの追加、削除、リストがあります。

コマンド	説明
netseal network add *network netmask* **[***network-alias***]**	
	NetSEAL によって保護される新しいネットワークを作成します。network/netmask のペアは、標準の IP ネットワーク・アドレス番号とネットマスクを表します。ネットワークは、ネットワークの別名をオプションで使用して識別することができます。別名を指定しなかった場合は、ネットワークを network と netmask のペアで識別する必要があります。そのネットワークがすでに存在している場合は、エラーが戻されます。
netseal network delete *network-id*	
	network-id が次のいずれかと一致している指定したネットワークを、システムから削除します。 • *network/netmask* のペア • *network-alias* network-id 引き数は、network/netmask のペアかネットワーク別名のどちらでもかまいません。システム内のこのネットワークの参照は、すべて、NetSEAL 接合も含めて除去されます。データベースにこのネットワークがない場合は、エラーが戻されます。
netseal network list	
	データベース内のすべてのネットワークを表示します。これには、ネットワークとネットマスクのペアのほかに、定義されているすべての別名も含まれます。

例 :

```
ivadmin> netseal network add 10.125.0.0 255.255.255.0 west
```

このコマンドでは、NetSEAL で保護するネットワークの指定に、ネットワーク・ノード 10.125.0.0 ～ 10.125.0.255 を追加します。また、このコマンドでは、別名 `west` をこのネットワークの指定に割り当てます。

NetSEAL 接合の管理

NetSEAL 接合によって、Policy Director サーバーを介して伝送される通信の方向が決まります。 接合は、2 つのPolicy Director サーバー間、あるいは、Policy Director サーバーとネットワークとの間に作成することができます。 GSS トンネルを使用すれば、2 つの Policy Director サーバー間の接合を横断する通信が機密保護されます。

ivadmin ユーティリティーを使用して、NetSEAL 接合を定義および管理します。このコマンドには、NetSEAL 接合の追加、削除、およびリストがあります。

コマンド	説明
netseal junction add *hostname destination*	

	NetSEAL サーバーから指定の宛先への接合を作成します。この場合の *hostname* には、NetSEAL サーバー名からドメイン名を取り去ったものを指定します。また、*destination* は、次のいずれでもかまいません。 • *pd-server* • *network/netmask* のペア • *network-alias* この接合がすでに存在しているか、ホスト・サーバーが存在していないか、あるいは、宛先が存在していない場合には、エラーが戻されます。
netseal junction delete *hostnamedestination*	
	NetSEAL サーバーから指定の宛先への接合を削除します。この場合の *hostname* には、NetSEAL サーバー名からドメイン名を取り去ったものを指定します。また、*destination* は、次のいずれでもかまいません。 • *pd-server* • *network/netmask* のペア • *network-alias* この接合が現在存在していない場合には、エラーが戻されます。このコマンドは、現行接続には無効です。
netseal junction list *hostname*	
	指定の NetSEAL サーバーのすべての NetSEAL 接合を表示します。

例 :

```
ivadmin> netseal junction add clipper west
```

このコマンドでは、NetSEAL サーバー `clipper` から、別名 `west` で定義しているネットワークへの接合を作成します。このコマンドでは、経路指定の方向 (`clipper` から `west`) も定義します。NetSEAL 接合は単一方向です。

保護ポートの管理

Policy Director NetSEAL サーバーでは、特定のポート、ホスト、およびネットワークに対して、セキュリティー・サービスを提供します。たとえば、特定ポート上の Telnet の通信を保護するように NetSEAL サーバーを構成することができます。

ivadmin netseal ユーティリティーを使用して、NetSEAL で保護するポートのリストを定義します。このコマンドには、保護ポートの追加、削除、およびリストがあります。Policy Director サーバーやネットワークのポートを指定することができます。

コマンド	説明
netseal port add *destination port-id*	

	指定の *port-id* 上の指定の宛先への接続を保護します。この場合の *destination* は、次のいずれでもかまいません。 • *pd-server* • *network netmask* • *network-alias* また、*port-id* は、次のいずれでもかまいません。 • *port* • *port-range* • *port-alias* このポートがすでに保護されている場合、サーバーが存在していない場合、または、ポート別名が存在していない場合には、エラーが戻されます。
netseal port delete *destination port-id*	
	指定のポート上の指定の宛先への接続の保護を停止します。この場合の *destination* は、次のいずれでもかまいません。 • *pd-server* • *network netmask* • *network-alias* また、*port-id* は、次のいずれでもかまいません。 • *port* • *port-range* • *port-alias* このポートがもう保護されていない場合、サーバーが存在していない場合、または、ポート別名が存在していない場合には、エラーが戻されます。
netseal port list *destination*	
	指定の宛先のすべてのポートのリストを表示します。この場合の *destination* は、次のいずれでもかまいません。 • *pd-server* • *network netmask* • *network-alias* サーバーが存在していない場合には、エラーが戻されます。

注: ポートの範囲をダッシュで区切った 2 つのポート番号 (22-88 など) で表します。

例 :

```
ivadmin> port add west 23
```

このコマンドでは、ネットワーク別名 “west” で指定しているネットワーク上のポート番号 23 を NetSEAL 保護ポートとして定義します。

保護ポートの別名の管理

ivadmin ユーティリティーを使用して、ポート別名を定義および管理します。このコマンドには、ポート別名の追加、削除、およびリストがあります。 ポート別名を使用して、トラップ・ポートの範囲をもっと分かりやすい方法で識別します。

コマンド	説明
netseal port-alias add *port-spec port-alias*	
	指定のポート仕様の新しいポート別名を作成します。この場合の *port-spec* は、次のどちらでもかまいません。 • *port* • *port-range* このポート範囲に別の名前ですでに別名が指定されている場合には、エラーが戻されます。
netseal port-alias delete *port-id*	
	システムから、指定の port-id のポート別名を削除します。この場合の *port-id* は、次のいずれでもかまいません。 • *port* • *port-range* • *port-alias* データベースにこのポート別名がない場合には、エラーが戻されます。
netseal port-alias list	
	データベースにあるすべてのポート別名を表示します。

例 :

```
ivadmin> netseal port-alias add 23 telnet
```

このコマンドでは、ポート番号 23 のポート別名 telnet を作成します。

```
ivadmin> netseal port-alias add 5000-5010 pilot
```

このコマンドでは、ポート範囲 5000 ～ 5010 のポート別名 “pilot” を作成します。

トラステッド・ホストとトラステッド・ネットワークの構成

Policy Director NetSEAL サーバーでは、特定のポート、ホスト、およびネットワークに対して、セキュリティー・サービスを提供します。たとえば、Policy Director 上の特定ポートの Telnet の通信を機密保護するように NetSEAL サーバーを構成することができます。さらに、NetSEAL サーバーは、システムをトラストしたり (トラステッド・ホスト)、ホストの集合をトラストする (トラステッド・ネットワーク) こともできます。

secmgrd.conf 構成ファイルの [trusted_hosts] スタンザや [trusted_networks] スタンザには、トラステッド・ホストとトラステッド・ネットワークを識別するためのパラメーターを指定します。

トラステッド・ホスト

NetSEAL サーバーは、信頼度の高い特定のトラステッド・サーバー (ホスト) と頻繁に通信を行います。NetSEAL がこれらのサーバーから出される着信要求からアクセス制御を免除できるようにすることで、パフォーマンスの最適化を図ることができます。

注: トラステッド・ホストを識別することにより、システムは、IP スプーフィングのハッキングを受けやすくなります。このようなハッキングからすべてのトラステッド・ホストを確実に保護するようにしてください。

デフォルトでは、Policy Director は、どのトラステッド・ホストも識別することはありません。

トラステッド・ホストを識別するには、[trusted_hosts] スタンザを使用して、IP アドレスとサーバー名をリストします。

たとえば、IP アドレスが 220.12.35.102 の “typhoon” という名前のサーバーから出されるすべての要求をトラストするには、次のように入力します。

```
[trusted_hosts]
220.12.35.102 = typhoon
```

NetSEAL トラップを使用してマシンを機密保護している場合は、頻繁にローカル・マシンのトラストが必要になります。ローカル・マシンをトラストすれば、そのマシン上で実行されるサービスは機能し続けることができます。これらのサービスは、ポートやポートの範囲に対して非認証アクセスがオフにされた場合でも続行します。

Policy Director は、ローカル・マシンをトラスト するために次の記入項目を必要とします。

- ローカル・ホスト用の 1 つの記入項目
- そのマシンに関連付けられているそれぞれの IP アドレス用の記入項目

たとえば、NetSEAL サーバー typhoon に、IP アドレス 220.12.35.102 を指定しているとします。同サーバー上の別のプロセスには、127.0.0.1 というローカル・ホスト IP アドレスを指定しているとします。NetSEAL サーバー typhoon に関して同サーバー上の他のプロセスから出されるすべてのローカル要求をトラストするには、次のように入力します。

```
[trusted_hosts]
220.12.35.102 = typhoon
127.0.0.1 = localhost
```

通常、IP アドレスは、1 つのマシンにつき 1 つしか指定されませんが、複数のネットワークに接続され、複数のアドレスが指定されるマシンもあります。

トラステッド・ネットワーク

ネットワークにサブネット全体、または、トラステッド・システムのローカル・エリア・ネットワークが組み込まれている場合は、それぞれのホストをリストしなくても、サブネット全体を指定することができます。

デフォルトでは、Policy Director は、どのトラステッド・ネットワークも定義することはありません。

トラステッド・ネットワークを識別するには、[trusted_networks] スタンザを使用して、サブネットの IP アドレスとネットマスクをリストします。

たとえば、サブネット 192.96.32.0 から出されるすべての要求をトラストするには、次のように入力します。

```
[trusted_networks]
192.96.32.0 = 255.255.255.0
```

SSL タイムアウト・パラメーターの設定

設定できる SSL タイムアウト・パラメーターには、次のものがあります。

- 『SSL セッション・キャッシュ・タイムアウトの設定』
- 『SSL 接続タイムアウトの設定』

SSL セッション・キャッシュ・タイムアウトの設定

secmgrd.conf 構成ファイルの [ssl] スタンザには、静的 SSL セッション・キャッシュ・タイムアウトを設定するためのパラメーターが入っています。

NetSEAL では、内部的にクリデンシャル情報をキャッシュに入れます。セッション・キャッシュ・タイムアウト・パラメーターによって、許可-クリデンシャル情報が NetSEAL 上のメモリー内にとどまる時間の長さを指示します。

このパラメーターは、非活動タイムアウトではありません。この値は、*クリデンシャル・タイムアウト* ではなく、*クリデンシャル存続時間* にマップされます。この目的は、指定のタイムアウト限度に達した時点でユーザーに再認証を強制することによって、セキュリティーを強化することにあります。

デフォルトのキャッシュ・タイムアウト (秒数) は次のとおりです。

```
[ssl]
ssl-cache-timeout = 3600
```

この値を調整して、サーバーが処理する必要がある SSL 要求の量に応じて、サーバーのパフォーマンスとユーザーの便宜とのバランスを図ります。

SSL 接続タイムアウトの設定

secmgrd.conf 構成ファイルの [ssl] スタンザには、SSL 接続タイムアウトを設定するためのパラメーターが入っています。

NetSEAL が NetSEAT クライアントから NetSEAL SSL トンネルを介して SSL 接続を受け入れると、SSL プロトコル・ハンドシェークが行われる必要があります。このパラメーターでは、SSL 接続の開始時に NetSEAT が SSL ハンドシェークを始めるまでのセキュリティー・マネージャーの待ち時間を制御します。この時間が経過すると、セキュリティー・マネージャーは接続をシャットダウンします。

デフォルトの SSL 接続タイムアウト (秒数) は次のとおりです。

```
[ssl]
ssl-init-connect-timeout = 120
```

NetSEAL 接続の割り振り

NetSEAL 接続を割り振るためのパラメーターは、secmgrd.conf 構成ファイルの [netseal] スタンザに入っています。

NetSEAL で許可する同時接続の最大数を指定するには、max-connections を使用します。

Policy Director のインストール時に、次のようなデフォルト値が設定されています。

```
[netseal]
max-connections = 32
```

ネットワーク内の通信量条件に最適な値になるように、この値を大きくすることも可能です。max-connections の設定が小さ過ぎると、厳しい負荷条件下で接続が拒否されます。この値の設定が大き過ぎると、リソースが浪費され、サーバーのパフォーマンスが低下します。

注: この構成パラメーターの下限は 20 です。20 よりも小さい設定値を指定しようとしても、この値は、デフォルトによって 20 に設定されます。

第19章 NetSEAT: 概要

Policy Director NetSEAT クライアントを使用すると、 Policy Director セキュア・ドメインへの Windows クライアントの参加が可能になります。NetSEAT によって、Windows クライアントと Policy Director サーバーとの間にセキュア・トンネル伝送が提供されます。 NetSEAT は、 SSL または GSS トンネル伝送を使用することで通信を暗号化します。

この章は、次の各節に分かれています。

NetSEAT クライアントの概要

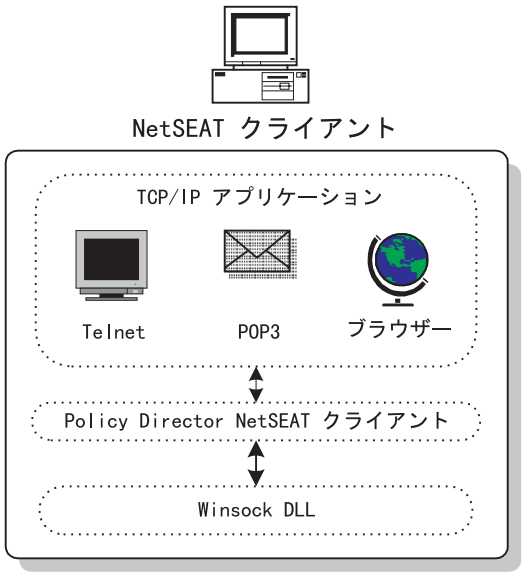
Policy Director NetSEAT クライアントを使用すると、Windows クライアントは、Policy Director の WebSEAL および NetSEAL サーバーと安全な通信を行うことができるようになります。NetSEAT を Windows ワークステーションに追加することで、そのワークステーションを Policy Director セキュア・ドメインの中に入るように構成できます。セキュア・ドメインとは、NetSEAT が Policy Director の認証および許可のセキュリティー・サービスを使用できるところです。

NetSEAT は、ネットワーク・プロトコル・レベルで認証とメッセージ保護を提供します。アプリケーションは、NetSEAT を使用するために再コンパイルや再リンクを行う必要はありません。

NetSEAT は、ネットワーク要求が Winsock 層を通過する前に、それらの要求を代行受信することで、Windows クライアントと Policy Director サーバーとの間のネットワーク通信を機密保護します。NetSEAT では、その構成情報を使用して、汎用 TCP/IP アプリケーションから出された要求を認識します。汎用 TCP/IP アプリケーションには、TELNET、POP3、または HTTP などがあります。

クライアント要求が Policy Director サーバー上のアプリケーションに対して出されると、 NetSEAT は、その Policy Director サーバーへのセキュア・トンネルを透過的に確立します。その上で、NetSEAT は、そのトンネルを介してクライアント要求をリダイレクトします。

NetSEAT は、SSL トンネルまたは GSS トンネルを使用して、Policy Director サーバーとの通信を機密保護および暗号化します。SSL トンネルでは、SSL を使用して通信を暗号化します。 GSS トンネルは、GSS API を使用して通信を暗号化します。



サポートされている構成

以下の項目で説明しているように、いくつかの異なる目的で NetSEAT クライアントを配置することができます。

- 『仮想私設網クライアント』
- 『Windows NT 上の Policy Director のサポート・モジュール』
- 261ページの『Policy Director 管理コンソールのサポート・モジュール』

仮想私設網クライアント

NetSEAT は、Policy Director NetSEAL サーバーとのセキュア通信リンクを提供するためにセキュア・トンネルを使用する仮想私設網 (VPN) クライアントとして構成することができます。

VPN クライアントとして、NetSEAT は、次のタイプのトンネルを使用して通信を暗号化することができます。

- SSL
- GSS

Windows NT 上の Policy Director のサポート・モジュール

Policy Director では、Policy Director for Windows NT のサーバー構成要素のインストールごとに、サポート・モジュールとして NetSEAT をインストールします。Policy Director for Solaris and AIX の場合は、 NetSEAT クライアントからこのサポートを得る必要はありません。

この役割において、NetSEAT クライアントは、Policy Director セキュリティー・サービスによる内部使用のためにカーネル・トラップを提供します。

Policy Director for Windows NT のサポート・モジュールとして、NetSEAT は、以下のサービスを必要とします。

- ディレクトリー・サービス・ブローカー
- GSS トンネル伝送

GSS トンネル伝送は、 Policy Director for Windows NT または Windows 上の Policy Director 管理コンソールのいずれかに対するサポート・モジュールとして NetSEAT クライアントをインストールする場合に使用します。

Policy Director 管理コンソールのサポート・モジュール

Windows クライアント上で Policy Director 管理コンソールを実行する場合は、NetSEAT をサポート・モジュールとしてインストールする必要があります。 このような構成で NetSEAT を使用すると、管理者は、管理コンソールを使用して、Windows システムから管理タスクを実行することができます。Windows システムに、Policy Director サーバー構成要素をインストールする必要はありません。

管理コンソールのサポート・モジュールとして、NetSEAT は、以下のサービスを必要とします。

- ディレクトリー・サービス・ブローカー
- GSS トンネル伝送

GSS トンネル伝送は、 Policy Director for Windows NT または Windows 上の Policy Director 管理コンソールのいずれかに対するサポート・モジュールとして NetSEAT クライアントをインストールする場合に使用します。

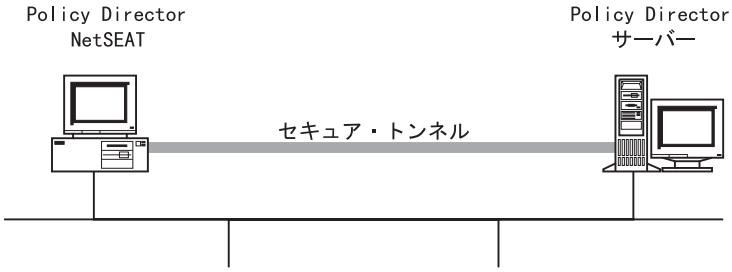
セキュア・トンネル伝送

クライアント要求を転送する前に、NetSEAT では、セキュア・トンネルを使用して、(適切なセキュア・ドメインを得るために) Policy Director セキュリティー・サーバーに連絡します。また、NetSEAT では、セキュア・トンネルを使用して、クライアントの識別とクリデンシャルの確立も行います。クライアントの認証が正常に行われた時点で、NetSEAT は、別のセキュア・トンネル内の要求トランザクションをカプセル化します。また、NetSEAT は、適用できるセキュリティー設定に従って、要求トランザクションを完了します。

たとえば、Web ブラウザーで、WebSEAL によって機密保護されているサービスやリソースへのアクセスを要求した場合、NetSEAT は、その要求を透過的に代行受信します。これが Policy Director への最初の要求であり、認証が必要とされる場合、NetSEAT は、ユーザーに対して、ログイン・ダイアログ・ボックスを使用してプロンプトを出します。

Policy Director がユーザーを認証したら、NetSEAT は、それらのクリデンシャルに従っている後続の要求とセキュア・トンネルを透過的に許可します。NetSEAT では、それらのクリデンシャルを使用して、それぞれの要求に関して許可決定を下します。

NetSEAT は、262ページの『SSL トンネル伝送の使用』および 262ページの『GSS トンネル伝送の使用』で説明しているように、 2 つの異なるタイプのセキュア・トンネルを確立することができます。



SSL トンネル伝送の使用

SSL トンネル伝送 という用語は、SSL プロトコルを使用するセキュア・トンネルを表します。NetSEAT は、Policy Director NetSEAL の VPN クライアントとして配置された場合に SSL トンネル伝送を使用します。SSL トンネルを使用することで、NetSEAT 構成が単純化されます。このシナリオの場合、管理者は、Policy Director セキュア・ドメイン内の DCE サービスの構成を指定する必要はありません。

SSL トンネルは、クライアントがファイアウォールによって保護されているデータへのアクセスを必要とする場合にも役に立ちます。このモードにある場合、NetSEAT は、ファイアウォールの後方にある Policy Director サーバーとのすべての通信に単一ポートを使用します。Policy Director は、セキュア・トンネル内のポートを介するすべての通信をカプセル化します。

NetSEAT の構成時に、ファイアウォールを横断するときに使用するポート番号を指定することができます。このポート番号は、NetSEAL サーバー上に構成されているポートと一致する必要があります。

SSL トンネル伝送は、LDAP ユーザー・レジストリーまたは DCE ユーザー・レジストリーのいずれかを介して認証されるユーザーが使用できます。

GSS トンネル伝送の使用

用語 *GSS トンネル伝送* は、一般セキュリティー・サービス API (GSS API) の使用に基づくセキュア・トンネルのことです。NetSEAT は、 DCE セルと通信する際に GSS トンネルを使用します。

このモードでは、NetSEAT は、DCE セル内の他のサーバー上にあるセキュリティー・マネージャー (secd) およびタイム・サーバー (dtsd) を使用するクライアントです。NetSEAT は、 Policy Director ディレクトリー・サービス・ブローカーを使用して、DCE セル内の別の場所にあるセル・ディレクトリー・サービス (cdsd) に対してネームスペース・ルックアップ要求の代理委任も行います。

セキュア GSS トンネルは、ユーザーの PKI ログインを、Entrust クライアントを介して、 Policy Director のセキュア・ドメインにあるユーザーの識別に統合する際に使用されます。このシナリオでは、ユーザーは、 Entrust PKI クライアントを使用してそれぞれのワークステーションにログインします。ユーザーが Policy Director 認証および許可サービスを使用しようとすると、 NetSEAT と Policy Director サーバーとの間にセキュア・トンネルが確立されます。Policy Director サーバーは、認証および許可決定を行うために、 PKI ログイン識別をユーザーの Policy Director 識別に自動的にマップします。

LDAP レジストリーによって認証されたユーザーには、 GSS トンネル伝送を使用できません。

保護サーバーへのアクセス

NetSEAT クライアントは、Policy Director NetSEAL サーバーへのそのセキュア・トンネルを使用して、要求を任意のリモート・アプリケーション・サーバーに送信することができます。これらのリモート・アプリケーション・サーバーは、NetSEAL サーバーによって保護されます。NetSEAT の構成時に、管理者は次のものを指定することができます。

- アプリケーション・サーバーの名前。
- それを保護する NetSEAL サーバー。
- NetSEAT と NetSEAL との間で使用されるセキュア・トンネルのタイプ (SSL トンネルまたは GSS トンネル)。

この情報を使用して構成した場合、NetSEAT は、アプリケーション・サーバーに対する Windows クライアントの要求を代行受信します。その上で、NetSEAT は、セキュア・トンネルを介して、それらの要求を Policy Director NetSEAL サーバーに経路指定します。

NetSEAT は、Policy Director NetSEAL がサブネットを保護している場合に、保護サブネット全体をアクセスするように構成することも可能です。この例としては、Policy Director NetSEAL サーバーによってインターネットから保護されているイントラネットが上げられます。

ディレクトリー・サービス・ブローカー

NetSEAT は、 Policy Director サーバーおよび Windows 上の管理コンソールのサポート・モジュールとして使用した場合 (GSS トンネル伝送)、ディレクトリー・サービス・ブローカー (DSB) のサービスを必要とします。DSB は、 Policy Director サーバーとの通信に必要です。 DSB プロキシーのネーム・スペースでは、同じセキュア・ドメイン内にあるセル・ディレクトリー・サービス・サーバーに対してルックアップを行います。

Policy Director は、Policy Director 管理サーバー (IVMgr) パッケージの一部として、DSB を自動的にインストールします。NetSEAT クライアントは、ディレクトリー・サービス・ブローカーのホストとしての役割を果たすサーバー・システムの名前を認識するように構成する必要があります。

第20章 NetSEAT: 一般管理タスク

この章では、NetSEAT クライアントの構成、セキュリティー・コンテキストの管理、および問題の検出と訂正 (トラブルシューティング) を行う場合のシステム管理タスクについて説明します。

この章は、次の各節に分かれています。

NetSEAT クライアントの構成

それぞれの NetSEAT クライアントは、Policy Director セキュア・ドメインに入るように構成します。NetSEAT クライアントは、インストール時に構成することができますが、インストール後でも構成することができます。 NetSEAT 構成ツール (ユーティリティー) には、グラフィカル・ユーザー・インターフェースが用意されています。これを使用すれば、管理者は、クライアントを簡単に構成できます。

構成した NetSEAT を参加させるセキュア・ドメインのコンテキスト内で、すべての構成タスクを実行します。

構成タスクの中には、1 つのセキュア・トンネル・タイプ (GSS か SSL) の場合の構成だけにしか適用されないものもあります。NetSEAT では、これらのセキュア・トンネルを使用して、Policy Director サーバーとの通信を行います。単に NetSEAL サーバーの SSL クライアントになるように構成された NetSEAT クライアントは、構成タスクの限定サブセットだけを必要とします。

次の表は、それぞれのセキュア・トンネル・タイプに対応する構成タスクを示します。

トンネル・タイプ	構成タスク

GSS と SSL の両方	• 『セキュア・ドメイン内への NetSEAT の追加』 • 269ページの『NetSEAL サーバーの構成』 • 277ページの『ネットワーク・リソースへのアクセスの拒否』
GSS のみ	• 267ページの『DCE サーバーの追加』 • 268ページの『DCE サーバー・プロパティーの設定』 • 272ページの『統合ログインの構成』 • 275ページの『拡張ログイン (PKI 統合) の構成』 • 276ページの『最大時間デルタの設定』
SSL のみ	277ページの『SSL プロキシーの構成』

NetSEAT では、数種類の DCE セキュリティー・ユーティリティーの拡張機能を提供し、さらに、DCE サービスの可用性を検査するためのユーティリティーも提供します。

これらのユーティリティーは、GSS トンネル伝送を使用するように NetSEAT を構成する場合にのみ使用してください。

これらのユーティリティーについては、次の節で説明します。

- NetSEAT セキュリティー・ユーティリティーの使用 (278ページの『NetSEAT セキュリティー・ユーティリティーの使用』を参照)。
- **netseat_ping** を使用した問題の検出と訂正 (279ページの『netseat_ping によるトラブルシューティング』を参照)。

NetSEAT 構成ツールの開始

初期のインストールと構成を完了した後に NetSEAT を再構成するには、NetSEAT 構成ツールを使用します。また、初期インストールの途中で構成を延期した場合に行う NetSEAT の構成にも、NetSEAT 構成ツールを使用します。

NetSEAT 構成ツールは、次の 2 通りの方法で開始することができます。

- NetSEAT 構成ツールを Windows デスクトップから開始する方法。**Start → Programs → Policy Director → NetSEAT → NetSEAT Configuration** の順序でクリックします。
- NetSEAT 構成ツールをシステム・トレイの **NetSEAT** アイコンから開始する方法。**NetSEAT** アイコン上で右マウス・ボタン・クリックしてから **Properties** を選択します。

セキュア・ドメイン内への NetSEAT の追加

NetSEAT をセキュア・ドメインの中に追加するには、次のステップを完了します。

1. NetSEAT 構成ツールを開始します。 始動時に、NetSEAT 構成ツールは、「NetSEAT 構成 (NetSEAT configuration)」ウィンドウ内に **Secure Domains** タブを表示します。
2. **Add** をクリックします。

   これによって、「新規セキュア・ドメイン (New Secure Domain)」ダイアログ・ボックスが表示されます。

3. NetSEAT の所属先とするセキュア・ドメインの名前を入力します。
4. このドメインに対してサポートされているプロトコルを選択してから、**OK** をクリックします。
   - **Enable GSS** を選択した場合は、『DCE サーバーの追加』に進んでください。
   - **Enable SSL only** を選択した場合は、269ページの『NetSEAL サーバーの構成』に進んでください。
5. **GSS tunneling only** -- 複数のドメインを構成している場合は、**Secure Domains** タブに戻ります。ユーザー・ログインに使用するデフォルト・ドメインを強調表示します。次いで、**Set as Default** をクリックします。

   構成しているドメインが 1 つだけの場合は、自動的にそのドメインがデフォルトになります。
6. **OK** をクリックします。

DCE サーバーの追加

GSS セキュア・トンネルを使用できるようにドメインを構成する場合は、他の構成オプションを設定する必要あります。

NetSEAT が結合するセキュア・ドメイン (またはセル) のために、セル内に指定されている Policy Director セキュリティー・サーバー・システムの名前を入手します。それぞれのシステムで提供する基本セキュリティー (DCE) サービスを識別します。それぞれのサーバーごとに、次のものを提供しているかどうかを判別します。

- **Security** -- セキュリティー・サービス (secd)
- **Time** -- タイム・サービス (dtsd)
- **DSB** -- ディレクトリー・サービス・ブローカー (dsb)
- **CDS** -- セル・ディレクトリー・サービス (cdsd)

  NetSEAT は、ディレクトリー・サービス・ブローカー (DSB) が NetSEAT クライアント上で実行されている場合にのみ、CDS の位置を知る必要があります。 通常、DSB は、Policy Director 管理サーバー (IVMgr) と同じサーバー上で実行するように構成されます。

「新規セキュア・ドメイン (New Secure Domain)」の記入項目を作成し、**OK** をクリックすると、「セキュア・ドメイン特性 (Secure Domain Properties)」ダイアログ・ボックスが表示されます。

1. **Add** をクリックします。

   「DCE サーバーの追加 (Add a DCE Server)」ダイアログ・ボックスが表示されます。
2. このセキュア・ドメイン内で DCE サービスを提供するサーバーの名前を入力します。
3. それぞれのサーバーについて、サービス **Security**、**Time**、**DSB**、**CDS** のなかから 1 つまたは複数選択します。
4. この DCE サーバーに対して何らかの拡張プロパティーを設定する必要のある場合は、オプションとして、**Advanced** をクリックすることができます。

   268ページの『DCE サーバー・プロパティーの設定』を参照してください。

5. **OK** をクリックして、指定の DCE サーバー上でサポートされるサービスの設定を完了します。

   「セキュア・ドメインの特性 (Secure Domain Properties)」ダイアログ・ボックスが再度表示されます。

6. 次のデフォルトの設定を受け入れます。
   - 統合ログイン・サポート : **Disabled**
   - 拡張ログイン : **DCE Login only**

   セキュア・ドメインに対して、オプションとして、統合ログイン・サポートと拡張ログインを構成する場合は、以下の節を参照してください。
   - 統合ログインの構成 (272ページの『統合ログインの構成』を参照)。
   - 拡張ログインの構成 (275ページの『拡張ログイン (PKI 統合) の構成』を参照)。

7. この DCE サーバーの構成を終えたら、**OK** をクリックします。

   「セキュア・ドメイン (Secure Domain)」ウィンドウが再度表示されます。これで、DCE サーバーの追加に必要な構成タスクは完了です。

DCE サーバー・プロパティーの設定

以下の値は、DCE サーバーの構成時に、「拡張 DCE サーバーの特性 (Advanced DCE Server Properties)」ダイアログ・ボックスで設定することができます。この構成タスクはオプションです。

プロトコルとポート

それぞれの DCE サーバーごとに、オプションとして、それぞれのセキュリティー・サービスで使用するプロトコル (TCP または UDP) を指定することができます。 この機能を使用すると、 IBM SecureWay Boundary Server 製品の構成要素の 1 つである IBM SecureWay Firewall バージョン 4.1 などのファイアウォールを通じてオペレーションを構成することができます。

たとえば、DCE サービスに関して UDP アクセスの選択を解除して、ファイアウォール管理者が構成した TCP ポート番号を指定することができます。

優先順位

使用可能な 1 つまたは複数のサービスの複数コピーをもつドメインを定義する場合は、NetSEAT がそれぞれのサービスをアクセスする順序を指定することができます。それぞれのサービスに正の整数を割り当てて、その優先順位を設定することができます。数値が大きくなるに従って、優先順位も高くなります。

この機能を使用すれば、管理者は、電子的に最も近くにあるサービスを NetSEAT に最初にアクセスさせることで、パフォーマンスを最適化することができます。そのサービスが使用できなければ、NetSEAT は、デフォルトとして、次に高い優先順位のサービスのコピーにアクセスします。

1. 拡張プロパティーを構成するには、「DCE サーバーの追加 (Add a DCE Server)」ダイアログ・ボックスを使用します。
2. **DCE server** を選択します。
3. **Advanced** をクリックします。

これによって、「拡張 DCE サーバーの特性 (Advanced DCE Server Properties)」ダイアログ・ボックスが表示されます。

4. DCE サービスとの連絡に使用するプロトコルを制限するには、該当の DCE サービスの隣に表示されているチェック・ボックスの選択を解除します。このチェック・ボックスの選択を解除することで、使用可能にする必要のないプロトコルが除去されます。
5. 必要に応じ、該当の DCE サーバーの隣のフィールドにポート番号を入力します。
6. それぞれの DCE サービスごとに、優先順位を設定します。
7. **OK** をクリックします。

NetSEAL サーバーの構成

NetSEAL サーバーと通信するように NetSEAT を構成するには、次のステップを完了します。

1. **NetSEAL Servers** タブを選択し、ドロップダウン・リストからセキュア・ドメインを選択します。
2. **Add** をクリックします。

   「NetSEAL サーバーの追加 (Add a NetSEAL Server)」ダイアログ・ボックスが表示されます。
3. NetSEAL サーバーのマシン名を入力します。
4. NetSEAL で GSS トンネル伝送や SSL トンネル伝送にデフォルト以外のポートを使用している場合は、該当のフィールドにそれらのポート番号を入力します。デフォルト・ポートを使用している場合は、そのデフォルト値を受け入れてください。
   - セキュア・ドメインの記入項目の作成時に使用可能にされなかったプロトコルは、ぼかし表示されています。
   - GSS トンネル伝送が使用可能にされている場合は、**Specify Principal Name** チェック・ボックスを選択しないでください。この機能は、前のバージョンとの逆方向の互換性のためだけに使用します。
5. SSL トンネル伝送を使用しており、しかも、NetSEAT 構成に SSL プロキシー・サーバーが構成されている場合、Policy Director は、自動的に **Use Proxy Server** チェック・ボックスを選択します。

   SSL プロキシー・サーバーを使用可能にしていない場合、**Use Proxy Server** チェック・ボックスは非アクティブです (選択解除されており、ぼかし表示になっています)。NetSEAT 構成内の SSL プロキシー・サーバーを使用可能にするには、277ページの『SSL プロキシーの構成』を参照してください。
6. **OK** をクリックします。

   NetSEAL Server タブが再表示されます。これで、NetSEAL サーバーは NetSEAT 構成に追加されました。

保護サーバーの追加

NetSEAL サーバーによって保護されているアプリケーション・サーバーとの通信チャネルを指定するように NetSEAT を構成することができます。

このオプションは、NetSEAT クライアントが GSS トンネル伝送か SSL トンネル伝送を使用している場合に使うことができます。

アプリケーション・サーバーを NetSEAT の構成に追加すると、NetSEAT は、そのアプリケーション・サーバーに対する Windows クライアントの要求を代行受信します。その上で、NetSEAT は、セキュア・トンネルを介して、それらの要求を NetSEAL サーバーに経路指定します。

保護サーバーを NetSEAT 構成に追加するには、次の情報を指定します。

フィールド	定義
Machine name	TCP/IP ドメイン内でアプリケーション・サーバーを認識するための名前。
Tunnel destination	アプリケーション・サーバーを保護している NetSEAL サーバーの名前。
Port range	NetSEAL サーバーによって保護されている保護サーバー上のポート番号。このポートまたはポートの範囲は、NetSEAL サーバー上で ivadmin コマンドによって指定されます。
Selected Protocol	トンネル伝送プロトコル。GSS と SSL は、両方とも、セキュア・ドメインに対して使用可能にすることができます。Policy Director の場合は、SSL トンネル伝送を指定してください。NetSEAL 間接続には、GSS トンネル伝送を使用します。

保護サーバーに対する発信要求を認識するように NetSEAT を構成するには、次のステップを完了します。

1. **Host Security** タブをクリックします。
2. **Add** をクリックします。

   「保護サーバーの追加 (Add a Protected Server)」ダイアログ・ボックスが表示されます。
3. 「マシン名 (Machine Name)」 には、NetSEAL サーバーで保護するサーバーのマシン名を入力します。

   NetSEAL サーバー 1 台につき、1 つのアプリケーション・サーバーだけを保護することができます。
4. 「トンネル宛先 (Tunnel Destination)」に関しては、ドロップダウン・リストを使用して、サーバーを保護する NetSEAL サーバーを選択します。
5. 必要に応じ、ドロップダウン・リストを使用して、適切なトンネル伝送プロトコルを選択します。
6. **Add** をクリックします。

   「ポート範囲の追加 (Add a Port Range)」ダイアログ・ボックスが表示されます。
7. NetSEAL が保護アプリケーション・サーバーとの通信に使用する NetSEAL サーバー上のポートまたはポートの範囲を指定します。
8. **OK** をクリックします。

   「保護サーバーの追加 (Add a Protected Server)」ダイアログ・ボックスが再表示されます。

   たとえば、下記の例では、ダイアログ・ボックスの記入項目の値が次のように設定されます。

- “sunshine” という名前の NetSEAL サーバーが “thunder” という名前の保護サーバーを保護します。
- サーバー sunshine は、ポート 5000 ～ 5005 上で thunder との通信を保護します。
- Policy Director は、NetSEAT クライアントと NetSEAL サーバー “sunshine” との間にセキュア・トンネルを定義します。
- このセキュア・トンネルのタイプは SSL トンネル伝送です。

9. **OK** をクリックします。

   Host Security タブが再表示されます。

   Policy Director は、保護サーバーを NetSEAT 構成に追加します。

保護サブネットの追加

NetSEAL サーバーによって保護されているサブネットとの通信チャネルを指定するように NetSEAT を構成することができます。このオプションは、NetSEAT クライアントが GSS トンネル伝送か SSL トンネル伝送を使用する場合に使うことができます。

アプリケーション・サブネットを NetSEAT の構成に追加すると、NetSEAT は、そのアプリケーション・サブネットへの Windows クライアントの要求を代行受信します。その上で、NetSEAT は、セキュア・トンネルを介して、それらの要求を NetSEAL サーバーに経路指定します。

保護サブネットを NetSEAT 構成に追加するには、次の情報を指定します。

フィールド	定義
Name of Any Machine in the Subnet	保護サブネット上のサーバーの名前。
Netmask	サブネットのネットマスク (たとえば、255.255.0.0 など)。
Tunnel Destination	サブネットを保護している NetSEAL サーバーの名前。
Select Protocol	トンネル伝送プロトコル。GSS と SSL は、両方とも、セキュア・ドメインに対して使用可能にすることができます。Policy Director の場合は、SSL トンネル伝送を指定してください。 NetSEAL 間接続には、GSS トンネル伝送を使用します。

NetSEAL サーバーによって保護されているサブネットへの発信要求を認識するように NetSEAT を構成するには、次のステップを完了します。

1. **Subnet Security** タブをクリックします。
2. (サブネットを保護する) NetSEAL サーバーが入っているセキュア・ドメインを選択します。
3. **Add** をクリックします。

   「保護サブネットの追加 (Add A Protected Subnet)」ダイアログ・ボックスが表示されます。
4. NetSEAL サーバーで保護するサブネット上のマシンの名前を入力します。

   NetSEAL サーバー 1 台につき、1 つのアプリケーション・サブネットだけを保護することができます。
5. サブネットのネットマスクを入力します。

6. 「トンネル宛先 (Tunnel Destination)」に関しては、ドロップダウン・リストを使用して、サブネットを保護する NetSEAL サーバーを選択します。
7. 必要に応じ、ドロップダウン・リストを使用して、適切なトンネル伝送プロトコルを選択します。

   たとえば、以下の記入項目の場合、NetSEAT は、ネットマスク 255.255.0.0 のサブネットにアクセスできるようになります。“thunder” という名前のシステムがサブネット上に存在します。SSL トンネル宛先でもある NetSEAL サーバー “sunshine” が、このサブネットを保護します。

   Name of Any Machine in the Subnet: `thunder`

   Netmask: `255.255.0.0`

   Tunnel Destination `sunshine`

   Select Protocol `SSL`
8. **OK** をクリックします。

   Subnet Security タブが再表示されます。

   これで、Policy Director は、保護サブネットと通信するように NetSEAT クライアントを構成しました。

統合ログインの構成

NetSEAT のインストール時に、オプションとして、統合ログイン・サポートをインストールすることができます。NetSEAT のインストールにより、統合ログインをサポートするよう Windows NT レジストリーを変更します。

統合ログインをインストールした後は、NetSEAT 構成ツールによって、それぞれのセキュア・ドメインごとに統合ログインを使用可能にしたり使用不可にすることができます。

NetSEAT の初期のインストールと構成時に統合ログインを構成することができます。あるいは、後で統合ログインを構成することもできます。それぞれのセキュア・ドメインごとに、独立した統合ログイン構成を設定します。

統合ログインを構成する前に、NetSEAT ユーザーは次のタスクを完了しておく必要があります。

- 自動ログインを必要とするそれぞれのセキュア・ドメイン内にアカウントを確保する。
- それぞれのセキュア・ドメインのメンバーになるように NetSEAT クライアントを構成する。
- セキュア・ドメイン・ログインに使用するユーザー名およびパスワードを Windows NT ドメインで使用されるユーザー名およびパスワードと同期させる。

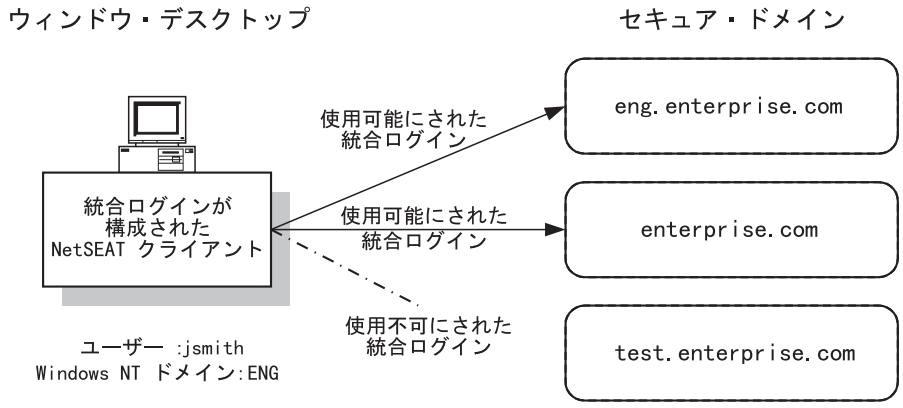
統合ログイン構成例の検討

John Smith という名前のエンジニアは、Windows ユーザー名 jsmith を使用して、通常、Windows NT ドメイン ENG にログインするとします。このユーザーは、次のように、数種類のセキュア・ドメインにログインします。

セキュア・ドメイン名	セキュア・ドメイン・ユーザー・アカウント	セキュア・ドメインの説明
eng.enterprise.com	jsmith	技術部セキュア・ドメイン。
enterprise.com	ENG/jsmith	会社共通セキュア・ドメイン。
test.enterprise.com	test_user	テストの目的でのみ使用される小型のセキュア・ドメイン。テスト・セルは、フル・ユーザー名レジストリーを保守しません。代わりに、ユーザーは、test_user としてログインします。

John Smith は、NetSEAT 構成ツールを使用して、次のように、それぞれのセキュア・ドメインごとに統合ログインを構成します。

セキュア・ドメイン	統合ログイン構成
eng.enterprise.com	Microsoft Windows NT ユーザー jsmith をセキュア・ドメイン・ユーザー jsmith にマップし、自動的に jsmith を eng.enterprise.com にログインするために使用可能にされ構成された統合ログイン。
enterprise.com	Microsoft Windows NT ユーザー jsmith をセキュア・ドメイン・ユーザー ENG/jsmith にマップし、自動的に ENG/jsmith を enterprise.com にログインするために使用可能にされ構成された統合ログイン。
test.enterprise.com	jsmith はユーザー test_user としてこのセルに手動でログインする必要があるために、使用不可にされた統合ログイン。



統合ログインの構成

統合ログインを構成するには、以下のステップを実行します。

1. NetSEAT 構成ツールを開始します。

   Secure Domains タブが表示されます。
2. 統合ログインの構成の対象とするセキュア・ドメインを選択します。
3. **Edit** をクリックします。

   「セキュア・ドメインの特性 (Secure Domain Properties)」ウィンドウが表示されます。

4. **Integrated Login Support** メニュー選択でいずれか 1 つの項目を選択します。

   Integrated Login Support がぼかし表示されている場合は、統合ログイン・サポートをインストールしていないために、このセキュア・ドメインに統合ログインを使用可能にすることはできません。

   - **Disabled** を選択し、このセキュア・ドメインに対して統合ログイン・サポートを使用不可にします。
   - このセキュア・ドメイン内のユーザー名が Windows ユーザー名と一致しているならば、**Enabled--DCE user name is Windows user name** を選択します。
   - このセキュア・ドメイン内のユーザー名に Windows ドメイン名が含まれているならば、**Enabled--DCE user name is Windows domain name/ Windows user name** を選択します。
5. **OK** をクリックします。

   Secure Domains タブが表示されます。
6. **OK** をクリックします。

統合ログイン通知モードの構成

セキュア・ドメインのパスワードと Windows NT ドメイン・パスワードとが一致しない場合があります。 この不一致が生じる場合、Windows レジストリーの記入項目によって、セキュア・ドメイン・ログインが無音で失敗するか否かを指示します *(無音モード)*。あるいは、セキュア・ドメインに使用する現行パスワードを入力するよう、ユーザーにプロンプトが出されます *(対話モード)*。無音モードの場合、Policy Director は、そのユーザーを、Windows NT ドメインにはログインさせますが、セキュア・ドメインにはログインさせません。対話モードの場合は、セキュア・ドメイン・パスワードと Windows パスワードとを同期させることができます。

通知モードを変更するには、レジストリー・エディターを使用して、この Windows レジストリー記入項目を編集します。

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥NetSEAT¥Parameters
```

次の値を変更します。

```
InfoLevel:
0x00000001 (1)
```

InfoLevel は、次のいずれかの値です。

レジストリー値	モード	説明
0	無音	ログインを試みた後に、ログインが成功したか失敗したかが、ユーザーに報告されません。
1	対話式	ログインを試みた後に、ユーザーに、ログインが失敗したことが報告され、さらに、処置を講じるよう指示するプロンプトが出されます。
2	冗長	ログインを試みた後に、ユーザーに、ログインが成功した場合も失敗した場合も、報告されます。

拡張ログイン (PKI 統合) の構成

この構成タスクは、オプションとして行われるもので、使用可能にされた GSS トンネル伝送を使っている NetSEAT クライアントだけに適用されます。

ユーザーの公開キー・インフラストラクチャー (PKI) ログインとユーザーの NetSEAT (ケルベロス) ログインとを統合するよう NetSEAT を構成することができます。

デフォルトでは、PKI ログインとの統合は使用不可になるよう設定されています。NetSEAT 構成ツールを実行して、PKI ログインを使用可能にします。NetSEAT クライアントの参加先であるそれぞれのセキュア・ドメインごとに、個別に、PKI ログインを使用可能または使用不可にします。

サポートされている PKI リリース

NetSEAT は、Entrust バージョン 4.0 とのユーザー・ログインの統合だけをサポートします。

注: Entrust バージョン 4.0 のクライアントは、NetSEAT PKI ログインを構成する前にインストールしておく必要があります。

NetSEAT ログイン・ユーティリティーの使用

NetSEAT ログイン・ユーティリティーは、 Windows **Start** メニューから呼び出されると、ログイン時に **PKI Login** チェック・ボックスを表示します。このチェック・ボックスには、現行のセキュア・ドメイン用に構成されている拡張ログインの設定が表示されます。

PKI ログイン・チェック・ボックスの使用

NetSEAT ログイン時に、ユーザーは、**PKI Login** チェック・ボックスを使用して、ログインごとに PKI ログイン構成をオーバーライドすることができます。このオーバーライドは、**PKI Login with fallback to DCE Login** の設定が構成時に選択された場合に役に立ちます。ユーザーは、PKI ログインの試行をスキップして DCE ログインを実行する場合にオーバーライドすることができます。この場合、ユーザーは、**PKI Login** チェック・ボックスの選択を解除して、DCE ログインを強制的に実行します。

ユーザーが構成時に **PKI Login only** を構成している場合は、ログイン時に **PKI Login** チェック・ボックスの選択を解除しても無効です。

ユーザーが構成時に **DCE Login only** を構成している場合は、ログイン時に **PKI Login** チェック・ボックスを選択すると、エラー・メッセージが出されます。

システム・トレイ・ログインの使用

システム・トレイ内の **NetSEAT** アイコンを使用して、NetSEAT ログインを実行することができます。ドロップダウン・リストを使用して、ログイン先のドメインを選択します。PKI ログインが構成されている場合は、Entrust ログイン・プロンプトが表示されます。

PKI ログインが失敗した場合、**PKI Login with fallback to DCE Login** が構成されているならば、Policy Director は、DCE ログインを完了させるよう指示するプロンプトを表示します。

拡張ログインの構成

PKI ログインと NetSEAT ログインを統合するには、以下のステップを実行します。

1. NetSEAT 構成ツールを開始します。

   Secure Domains タブが表示されます。

2. PKI ログインの構成の対象とするセキュア・ドメインを選択します。
3. **Edit** をクリックします。

   これによって、「新規セキュア・ドメイン (New Secure Domain)」ダイアログ・ボックスが表示されます。

4. **Configure** をクリックします。

   「セキュア・ドメインの特性 (Secure Domain Properties)」ウィンドウが表示されます。

5. 「拡張ログイン (Advanced Login)」域で、拡張ログイン・ドロップダウン・リストからいずれか 1 つの項目を選択します。
   - **DCE Login only** を選択すれば、ユーザーは、ユーザー名とパスワードを使用して Policy Director セキュア・ドメインにログインできるようになります (ケルベロス・ログイン)。
   - **PKI Login with fallback to DCE Login** を選択すれば、ユーザーは、PKI ログインを試行できるようになります。このログインが失敗すると、NetSEAT は、DCE ログインに使用するユーザー名とパスワードを入力するように指示するプロンプトを出します。
   - ユーザーに X.509 証明書を使用してログインするよう要求する場合は、**PKI Login only** を選択します。
6. **OK** をクリックします。

   これによって、「新規セキュア・ドメイン (New Secure Domain)」ダイアログ・ボックスが表示されます。

7. **OK** をクリックします。

   Secure Domains タブが再表示されます。

最大時間デルタの設定

この構成タスクは、オプションとして行われるもので、Policy Director 管理コンソール上、ならびに、Policy Director 用の Windows NT サーバー上の NetSEAT クライアントだけに適用されます。

NetSEAT では、GSS トンネル伝送を使用するように構成されている場合にリモート・タイム・サービスを使用します。セキュア・ドメイン時刻と NetSEAT システムのクロックとの間で許容される最大時間デルタを構成することができます。あるいは、デフォルト値の 15 分を使用します。

最大時間デルタを設定するには、次のようにします。

1. **General** タブをクリックします。
2. 必要に応じ、**Maximum Time Delta** フィールドに設定値を入力します。
3. **OK** または **Apply** をクリックします。

ネットワーク・リソースへのアクセスの拒否

この構成タスクは、オプションとして行われるもので、GSS トンネル伝送か SSL トンネル伝送を使用可能にしている NetSEAT クライアントに適用されます。

ユーザーがワークステーションから無保護の TELNET、RLOGIN、または HTTP 要求を出さないようにすることができます。 これらのネットワーク・サービスへのアクセスを拒否または制限するように NetSEAT クライアントを構成します。アクセスを拒否または制限すると、クライアント・ワークステーションは、ネットワーク会話時に、保護されて暗号化された Policy Director 通信チャネルだけを使用するように強制されます。

この機能のデフォルトの設定はオフです。この機能は、特殊な目的の高度のセキュア・ネットワークの場合にのみオンにしてください。

無保護ネットワーク・サービスへのアクセスを拒否するには、次のようにします。

1. **General** タブを選択します。
2. 必要に応じ、 **Deny access to unprotected network services** チェック・ボックスを選択します。
3. **OK** または **Apply** をクリックします。

SSL プロキシーの構成

この構成タスクは、オプションとして行われるもので、SSL トンネル伝送を使用可能にしている NetSEAT クライアントだけに適用されます。

NetSEAT クライアントからの要求をネットワークの SSL プロキシー・サーバーを介して送信する必要がある場合は、そのプロキシー・サーバーを使用するように NetSEAT クライアントを構成することができます。**General** タブの **Enable Proxy Server** チェック・ボックスで、プロキシー・サーバーをすべての NetSEAL サーバーで使用できるようにします。

このチェック・ボックスの選択を解除すると、NetSEAT 構成に追加された NetSEAL サーバーは、どれも、プロキシー・サーバーにアクセスすることができなくなります。

SSL プロキシー・サーバーを指定するには、次のステップを完了します。

1. **General** タブをクリックします。
2. 必要に応じ、**Maximum Time Delta** フィールドに指定されている分数を変更します。デフォルトは 15 分です。
3. **Deny access to unprotected network services** チェック・ボックスを選択していないことを確認してください。
4. **Enable Proxy Server** チェック・ボックスを選択します。
5. **Proxy Server Machine Name** フィールドに名前を入力します。
6. **Proxy Server Port** フィールドにポート番号を入力します。
7. **OK** または **Apply** をクリックします。

NetSEAT セキュリティー・ユーティリティーの使用

NetSEAT クライアントには、従来の DCE のインプリメンテーションに備わっている DCE セキュリティー・サービス・ユーティリティーが用意されています。NetSEAT 固有のアーキテクチャーにより、**klist**、**kdestroy**、および **dce_login** のそれぞれのユーティリティーごとに、標準機能の拡張が可能になります。

klist

klist コマンドは、デフォルトのクリデンシャル・キャッシュに保持されている 1 次ユーザー (*principal*) とチケットをリストします。また、**-c** オプションを使用した場合、このコマンドは、キャッシュ名で識別されるキャッシュに保持されているユーザーとチケットをリストします。

NetSEAT は、標準の **klist** コマンド・オプションを実行し、拡張オプションを追加します。

標準オプションは次のとおりです。

オプション	説明
-c *cachename*	これを指定すると、キャッシュ名によって識別されるキャッシュの内容が、デフォルト・キャッシュの内容の代わりに表示されます。
-e	有効期限切れのチケットを表示に組み込みます。このオプションを使用しなかった場合は、現行チケットだけが表示されます。
-f	チケットに関するオプションの設定を表示します。

拡張オプションは次のとおりです。

オプション	説明
-C *cellname*	*cellname* によって識別される DCE セル内にユーザー用に保持されている 1 次ユーザーとチケットを記述します。
-m	DCE ログイン・コンテキストがユーザーによって所持されているすべての DCE セル内にユーザー用に保持されている 1 次ユーザーとチケットを記述します。
-s	ユーザーのログイン先であるすべてのセルの短い要約、および、それぞれのセルに使用するユーザーのログイン名を表示します。

kdestroy

kdestroy コマンドは、ユーザーのログイン・コンテキストとユーザーのクリデンシャルを破棄します。Policy Director がそれらのクリデンシャルを再確立するまで、そのユーザー、ならびに、そのユーザーによって作成されたすべてのプロセスは、非認証アクセスに限定されます。

NetSEAT クライアントは、標準の **kdestroy** オプションをサポートしており、また、拡張オプションを追加します。

標準オプションは次のとおりです。

オプション	説明

-c *cachename*	これを指定すると、キャッシュ名に使用するログイン・コンテキストとその関連のクリデンシャルは、デフォルト・キャッシュ内のログイン・コンテキストやクリデンシャルの代わりに破棄されます。

拡張オプションは次のとおりです。

オプション	説明
-C *cellname*	指定のセル *cellname* に使用するログイン・コンテキストとその関連のクリデンシャルを破棄します。
-m	ログイン・コンテキストがユーザーによって所有されているすべてのセルに使用するそのユーザーのログイン・コンテキストとその関連のクリデンシャルを破棄します。

dce_login

dce_login コマンドは、ユーザーの識別情報の妥当性を検査し、そのユーザーのネットワーク・クリデンシャルを取得してから、DCE ログイン・コンテキストを確立します。

ユーザーは、principal_name (ユーザー名) とパスワードを入力する必要があります。これらの値をコマンド行引き数として指定しなかった場合、**dce_login** は、それらの値を求めるプロンプトを出します。

NetSEAT クライアントは、次のような標準の **dce_login** オプションをサポートします。

オプション	説明
-exec *command_string*	ログイン後に、*command_string* で指定したコマンドを実行します。*command_string* をフルパス名なしで指定すると、PATH 変数に従ってディレクトリーを検索してパスの接頭部を入手します。
-k *keytab_file_name*	これを指定すると、**dce_login** は、ユーザー (プリンシパル) 名とパスワードを keytab ファイル *keytab_file_name* から入手します。
-r	ユーザーのチケットの有効期限が切れる前に、そのユーザーの DCE ログイン・コンテキストを最新表示します。

Policy Director は、次のような拡張 dce_login オプションをサポートします。

オプション	説明
-C *cellname*	これを指定すると、ユーザーは、デフォルト・セルではなく、セル *cellname* にログインされます。

注: NetSEAT クライアントでは、**dce_login -c** オプションはサポートしません。

netseat_ping によるトラブルシューティング

NetSEAT クライアントには、**netseat_ping** ユーティリティーが用意されています。このユーティリティーを使用すれば、ユーザーは、1 つまたは複数のセル内の DCE サービスに関する状況情報を入手することができます。**netseat_ping** を使用して、以下のサービスが使用可能であるか否かを判別します。

- セキュリティー・サービス
- タイム・サービス
- セル・ディレクトリー・サービス
- ディレクトリー・サービス・ブローカー

ユーザーがログイン・コンテキストを保持しているすべてのセル内のサービスに関する状況を入手するには、次のように入力します。

```
netseat_ping
```

たとえば、セル redback に参加するよう NetSEAT クライアントを構成すると、出力は次のようになります。

```
/.../redback:
       SecurityServers:
                    ncacn_ip_tcp:redback[ ] is available
                    ncadg_ip_udp:redback[ ] is available
       CdsServers:
                    ncacn_ip_tcp:redback[ ] is available
                    ncadg_ip_udp:redback[ ] is available
       TimeServers:
                    ncacn_ip_tcp:redback[ ] is available
                    ncadg_ip_udp:redback[ ] is available
       DsbServers:
                    ncacn_ip_tcp:redback[ ] is available (v3.0)
                    ncacn_ip_udp:redback[ ] is available (v3.0)
```

Policy Director は、以下の **netseat_ping** オプションをサポートします。

オプション	説明
-C *cellname*	ユーザーがセル *cellname* 用に構成したすべてのサーバーのバインディングのリストを生成します。
-t -C *cellname*	セル *cellname* 内のタイム・サーバーのバインディングを表示します。
-s -C *cellname*	*cellname* 内のセキュリティー・サーバーのバインディングを表示します。
-c -C *cellname*	セル *cellname* 内の CDS サーバーのバインディングを表示します。
-d -C *cellname*	セル *cellname* 内の DSB サーバーのバインディングを表示します。

セルに複数のセキュリティー・サーバー、タイム・サーバー、セル・ディレクトリー・サーバー、または DSB がある場合、**netseat_ping** は、それらすべてに対して PING (ネットワーク接続検査) を試みます。

第21章 NetSEAT: ディレクトリー・サービス・ブローカー

この章では、ディレクトリー・サービス・ブローカー (DSB) の概要、ならびに、環境に合わせて DSB 構成をカスタマイズする方法について説明します。

この章は、次の各節に分かれています。

ディレクトリー・サービス・ブローカーの概要

Policy Director NetSEAT クライアントは、RPC ネーム・サービス・インターフェースの機能をディレクトリー・サービス・ブローカー (DSB) にオフロードします。DSB は、セル・ディレクトリー・サービス (CDS) の中間層のサーバーとして動作します。

NetSEAT クライアントは、リソースとサービスの位置に関する要求を DSB に送ります。次いで、DSB は、セキュア・ドメインの CDS と連絡をとって、その要求を解決します。その後で、DSB は、NetSEAT クライアントを実行するシステムに要求情報を戻します。

Policy Director は、Policy Director のインストール時に、自動的に、DSB をインストールおよび構成します。Policy Director は、Policy Director 管理サーバー (IVMgr) パッケージの一部として、DSB を提供します。DSB を使用するための追加ステップはありません。

- DSB は、Policy Director サーバーと管理コンソールのサポート・モジュールとしての役割を担う NetSEAT クライアントによって使用されます。
- SSL トンネル伝送を使用する NetSEAT クライアントでは、DSB を使用しません。

DSB は、多数の NetSEAT クライアントをサポートすることができます。より大きなセキュア・ドメインの場合は、セル・ディレクトリー・サービスを提供するサーバー上で DSB を実行することによって、パフォーマンスを最適化することができます。

高可用性を提供したり、あるいは、非常に大規模なネットワーク内の負荷のバランスを取るために、管理者は、1 つのセキュア・ドメインに複数の DSB を配置したい場合があります。追加の DSB は、手動でインストールおよび構成することができます。

ディレクトリー・サービス・ブローカーの構成オプション

DSB は、デーモンまたはサービスとして実行されます。DSB は、システム・リブートで自動的に始動するよう構成することができます。ほとんどの場合、DSB は管理を必要としません。

管理者が DSB 構成パラメーターを調整する方法については、以下の節を参照してください。

- 『DSB ログ・ファイルの位置の指定』

DSB ポートの設定

DSB は、ポートで要求を listen します。デフォルトでは、DSB はポートをランダムに選択します。

オプションとして、管理者は、以下のいずれかのファイルに値を入力して、ポート番号を指定することができます。

UNIX: /etc/services

Windows: *install-path*¥system32¥drivers¥etc¥services

たとえば、UNIX システム上の DSB にポート 5000 で listen するよう指示するには、次の記入項目を /etc/services に入れます。

```
dsb                 5000/tcp              # Directory Services Broker
```

DSB ログ・ファイルの位置の指定

DSB では、通知、エラー、警告、および回復不能 (致命的) エラーのログ記録に DCE 保守ログ・ファイルを使用します。DCE インストール・システムで DCE 保守を使用している場合、DSB は、その出力を 1 つまたは複数の保守ログ・ファイルに書き込みます。DCE 保守ログ・ファイルは、ディレクトリー *DCELOCAL*/var/svc の中にあります。 *DCELOCAL* は、DCE インストール・ディレクトリーを表します。

メッセージの状況、たとえば、通知、エラー、または警告などを反映するファイルは、複数存在することがあります。これらのファイルの位置は、ルーティング・ファイル *DCELOCAL*/var/svc/routing の中に記入項目を入れることで指定できます。

たとえば、次のようにします。

```
NOTICE:FILE:DCELOCAL/var/svc/notice
```

また、環境変数 *SVC_NOTICE* を使用して、位置を指定することも可能です。環境変数定義は、ルーティング・ファイルの指定をオーバーライドします。たとえば、次のように入力することで、通知ファイルの指定に、 UNIX 環境変数を定義することができます。

```
export SVC_NOTICE=FILE:DCELOCAL/var/svc/notice
```

コマンド行の例:

ルーティング・ファイルに NOTICE を定義し、以下のように、コマンド行から DSB を開始すると、

```
SVC_NOTICE=FILE:DCELOCAL/var/dsb/dsb.log dsb -q -f -U cell_admin -P *****
```

DSB は、次のタスクを実行します。

- それ自体を無音で構成および開始する。
- *DCELOCAL*/var/dsb/dsb.log に、すべての通知を記録する。
- ルーティング・ファイル内の指定に従って、すべてのエラー、警告、および回復不能 (致命的) エラーをログに記録する。

- どのようなログ記録出力も表示しない。

ルーティング・ファイルの形式、ならびに、環境変数の SVC_* グループの使用に関する詳細については、DCE 保守情報を参照してください。IBM Policy Director セキュリティー・サービス CD 上の DCE に関する、以下のインストールおよび構成文書は、/doc ディレクトリーに入っています。

- DCE22_QuickBeginnings_AIX.pdf
- DCE22_QuickBeginnings_NT.pdf
- DCE20_InstallGuide_Solaris.pdf
- DCE20_ReleaseNotes_Solaris.pdf

ディレクトリー・サービス・ブローカーのコマンド行オプション

以下の表に、DSB コマンド行オプションを示します。

オプション	説明
-d	UNIX デーモンや Microsoft Windows NT サービスとしてではなく、フォアグラウンドで実行します。このオプションは、主に、デバッグに使用されます。
-f	DSB の DCE セキュリティー記入項目の再構成を強制します。 このフラグは、Policy Director/dsb-servers グループ (そのグループがまだ作成されていない場合)、キー・テーブル・ファイル、および intraverse/dsb/default/*fully_qualified_DNS_name* プリンシパル (ユーザー) (この場合の *fully_qualified_DNS_name* には、DSB が実行されているシステムを指定) を作成します。 このオプションは、初期の DSB 始動時に使用されます。これは、最初にプリンシパル (ユーザー) 記入項目、グループ記入項目、およびキー・テーブル・ファイルを除去せずに、何度も呼び出すことができます。
-h	コマンド行使用メッセージ。
-q	標準出力を stdout や stderr でなくログ・ファイルに送信します。通知は画面に表示されません。
-r	DSB の構成を解除します。 このオプションは、DSB の DCE セキュリティー記入項目 (上記の **-f** オプションの説明を参照) を除去します。 **-r** フラグは、単独、または、**-q** と一緒に使用されます。それ以外のコマンド行フラグは、**-r** と一緒に使用できません。
-t	DSB が使用するサーバー・スレッドの数を指定します。 このスレッドの数は、同時に処理できるクライアント要求の数を定義します。
-P *password*	DCE ログイン・プリンシパル (ユーザー) のパスワードを指定します。 **-U** フラグとだけ一緒に使用します。

-U *principal_name*	DSB の構成を実行するのに使用される DCE ログイン・プリンシパル (ユーザー)。 このオプションを使用して、DSB セキュリティー記入項目 (上記の **-f** オプションの説明を参照) を作成する権限の代行者とするユーザーを指定します。
-b	*Microsoft Windows* の場合のみ -- 実行可能 DSB バイナリーのファイル名を指定します。 このオプションは、DSB がデフォルト以外の位置にインストールされている場合に使用します。 このオプションは、DSB の位置を Microsoft Windows NT レジストリー内に保管します。Microsoft Windows NT では、DSB を Microsoft Windows NT サービスとして構成するときにレジストリーの設定値を使用します。
-v	*Microsoft Windows* の場合のみ -- DSB バージョンと DCE ベンダー・メッセージを表示します。

付録A. ivadmin を使用した Policy Director 管理

ivadmin ユーティリティーは、管理コンソールに相当するコマンド行ユーティリティーで、ユーザーは、これを使用して、Policy Director 管理タスクを実行することができます。

この章は、次の各節に分かれています。

ivadmin ユーティリティーの概要

ivadmin ユーティリティーは、管理コンソールに代わるコマンド行ユーティリティーです。ある一定の管理機能の自動化を望む管理者は、**ivadmin** を使用するスクリプトを作成することにより、その自動化を行うことができます。

ivadmin コマンドの多くのものは、管理コンソールに備わっている機能と重複します。それに加え、**ivadmin** には、管理コンソールでは使用することができない、いくつかの拡張管理機能が備わっています。Policy Director を実行するシステムにインストールされる IVBase パッケージは、このパッケージの一部として、このユーティリティーもインストールします。

ivadmin ユーティリティーの開始

ivadmin ユーティリティーを開始するには、**dce_login** を使用して、セキュア・ドメインにログインします。その後で次のように入力します。

UNIX: `# ivadmin`

Windows: `ivadmin`

ivadmin プロンプトが表示されます。

```
ivadmin>
```

このプロンプトに応じて、適切なコマンド、オプション、および引き数を入力します。 286ページの『ivadmin コマンドの使用』のコマンド表を参照してください。

たとえば、**ivadmin** ヘルプ・メッセージを表示するには、次のように入力します。

```
ivadmin> help
```

ivadmin ユーティリティーの終了

ユーティリティーを終了し、コマンド・プロンプトに戻るには、**ivadmin exit** コマンドを入力します。

```
ivadmin> exit
```

ivadmin コマンドの使用

ivadmin コマンドには、次のものがあります。

- 『server コマンド』
- 288ページの『object コマンド』
- 288ページの『action コマンド』
- 289ページの『ACL コマンド』
- 290ページの『NetSEAL コマンド』
- 294ページの『構成管理コマンド』
- 294ページの『ユーザー管理コマンド』
- 299ページの『グループ管理コマンド』
- 302ページの『リソース管理コマンド』
- 307ページの『レジストリー・ポリシー管理コマンド』

注: ivadmin コマンドは、すべて、単一コマンドとして 1 行で入力する必要があります。 本書で使用している例には、長過ぎて次の行にまたがっているものもあります。

server コマンド

ivadmin server コマンドには、管理コンソールでは現在取り扱っていない機能が備わっています。

コマンド	説明
server flush_logs *server-name*	
	WebSEAL サーバー・ログをメモリーからハード・ディスクに書き込みます。サーバー・イベントの即時追跡を可能にします。
server list	
	すべての構成済みサーバーをリストします。
server resume *server-name*	
	中断されていた WebSEAL サーバーを再開します。
server show *server-name*	
	指定されているサーバーのプロパティー、たとえば名前、記述、ホスト名、NS ロケーション、プリンシパル、およびルート URL などを表示します。
server start *server-name*	
	指定されているサーバーを開始します。secmgrd (NetSEAL および WebSEAL) と ivacld を開始します。
server stop *server-name*	
	指定されているサーバーを停止します。secmgrd (NetSEAL および WebSEAL) と ivacld を停止します。
server suspend *server-name*	
	指定されている WebSEAL サーバーを中断します。サーバーの保守を行う場合に役に立ちます。

以下の **ivadmin server** コマンドは、管理コンソールの機能を拡張します。

コマンド	説明
server delete /ExternAuthzn/*server-name*	
	外部許可サーバーだけを削除します。通常、このコマンドは、アンインストール・プログラムが非対話式で使用します。 **注:** このコマンドを使用して、他のサーバーを一切削除しないようにしてください。
server modify *server-name* **baseurl** *mount-point*	
	このサーバーで使用する ACL スペースの分岐を指定します。複写 WebSEAL サーバーで使用されるのが目的です。これを指定すると、指定されている分岐 *mount-point* が、ACL 管理のために管理コンソールで使用するマスター分岐になります。この分岐内の ACL は、このマウント・ポイント (接合点) に接合されているすべての複写サーバーに適用され、それらの複写サーバーは、すべての ACL 変更を即時に反映します。 *mount-point* は、/WebSEAL コンテナー・オブジェクトの相対位置にあり、 WebSEAL ディレクトリー内に入れる必要があります (サブディレクトリー内には入れないでください)。
server register externauth *server-name ns-location server-principal action-char action-name*	
	外部許可サーバーの存在を登録します。このコマンドを使用して、外部許可サーバーが存在していること、ならびに、保護オブジェクトに対する許可特権の解決時にその外部許可サーバーに相談する必要があることを Policy Director 許可サービスに通知します。
server status *server-name*	
	サーバーは稼働しているか停止しているか、また、サーバーの ACL データベース・レプリカは最新の変更によって更新されているか否かを判別します。

技術上の注:

マシン chevelle 上の WebSEAL サーバーの特性を表示するには、次のように入力します。

```
ivadmin> server show /WebSEAL/chevelle
Type: WebSEAL Server
Name: /WebSEAL/chevelle
Description: chevelle
Hostname: chevelle
NS Location: /.:/subsys/intraverse/secmgr/server/chevelle
Principal: secmgr/chevelle Root URL: /chevelle
```

server-name 引き数は、**ivadmin server list** コマンドの出力で示される形式のとおりに正確に入力する必要があることに注意してください。

たとえば、次のとおりです。

```
ivadmin> server list
         /WebSEAL/chevelle
         /NetSEAL/chevelle
         /ExternAuthzn/timechecker
```

object コマンド

次の **ivadmin object** コマンドには、管理コンソールのコマンドのうち、同等のオブジェクト・スペース管理タスク・コマンドと同じ機能が備わっています。

コマンド	説明
object list *directory-name*	
	指定されているディレクトリーのもとにグループ化されたオブジェクトをリストし、それぞれのオブジェクトに関連付けられている ACL の名前を表示します。 このコマンドでは、このディレクトリーを超えるようなツリーの拡張は行わないことに注意してください。
object show *object-name*	
	object-name 情報とそれに関連付けられている ACL の名前を表示します。 関連付けられている ACL がなければ、No ACL という句が表示されます。

action コマンド

以下の **ivadmin action** コマンドを使用して、管理コンソール上で行われる追加の Policy Director 許可処置 (許可) を定義します。

たとえば、**ivadmin action** コマンドを使用して、使用可能な ACL 許可のリストに外部許可メカニズムを追加します。

ivadmin action コマンドには、管理コンソールでは現在取り扱っていない機能が備わっています。

コマンド	説明
action create *name description action-type*	
	新しい Policy Director 許可処置 (許可) を定義します。管理コンソール上のこの処置を表す新しい ACL 許可コードを作成します。 *name* 引き数で、新しい単一文字の許可コードを指定します。*description* 引き数では、管理コンソールで表示される新規チェック・ボックスのラベルを指定します。*action-type* 引き数では、管理コンソールで表示される処置カテゴリーのラベルを指定します。 例: `ivadmin> action create k time Ext-Authzn`
action delete *name*	
	action create コマンドで作成した既存の許可処置 (許可) を削除します。 例: `ivadmin> action delete k`
action list	

	以下の形式の既存の ACL アクション (許可) をすべてリストします。
	permission name permission description action type
	
	例:
	`ivadmin> action list`
	
	これによって、下記と同じような情報が表示されます。
	`r read WebSEAL`
	`...`

ACL コマンド

次の **ivadmin acl** コマンドには、管理コンソールのコマンドのうち、同等の **ACL** 管理タスク・コマンドと同じ機能が備わっています。

コマンド	説明
acl attach *obj-name acl-name*	
	ACL テンプレートをオブジェクトに接続します。
acl create *acl-name*	
	ACL テンプレート・データベース内に新しいテンプレートを作成します。このコマンドでは、ACL 記入項目を作成しないことに注意してください。
acl delete *acl-name*	
	ACL テンプレート・データベースから ACL テンプレートを削除します。
acl detach *obj-name*	
	現行の ACL テンプレートを、指定されているオブジェクトから切り離します。このコマンドでは、ACL テンプレート・データベースから ACL テンプレートを削除しないことに注意してください。
acl find *acl-name*	
	指定されている ACL テンプレートが接続されたすべてのオブジェクトを検出およびリストします。
acl list	
	ACL テンプレート・データベース内のすべての ACL テンプレートをリストします。
acl modify *acl-name* **description** *desc*	
	これを指定すると、指定されている ACL テンプレートに関連付けられている記述フィールドの作成または編集が可能になります。この記述が表示される場所の 1 つは、管理コンソールの「ACL management task」パネルの ACL 定義域の中にあります。
acl modify *acl-name* **remove user** *user-name*	
	これを指定すると、指定されている ACL テンプレート定義から既存のユーザー ACL 記入項目を削除することが可能になります。
acl modify *acl-name* **remove group** *group-name*	
	これを指定すると、指定されている ACL テンプレート定義から既存のグループ ACL 記入項目を除去することが可能になります。
acl modify *acl-name* **remove any-other**	

	これを指定すると、指定されている ACL テンプレート定義から全認証 ACL 記入項目を除去することが可能になります。
acl modify *acl-name* **remove unauthenticated**	
	これを指定すると、指定されている ACL テンプレート定義から非認証 ACL 記入項目を除去することが可能になります。
acl modify *acl-name* **set user** *user-name perms*	
	これを指定すると、指定されている ACL テンプレート定義内のユーザー ACL 記入項目 (pubs) を作成または編集することが可能になります (この場合の許可 (*perms*) は bPTr です)。 例: `ivadmin> acl modify pubs set user peter bPTr`
acl modify *acl-name* **set group** *group-name perms*	
	これを指定すると、指定されている ACL テンプレート定義内のグループ ACL 記入項目を作成または編集することが可能になります。 例: `ivadmin> acl modify pubs set group sales Tr`
acl modify *acl-name* **set any-other** *perms*	
	これを指定すると、指定されている ACL テンプレート定義内の全認証 ACL 項目 (pubs) を作成または編集することが可能になります。 例: `ivadmin> acl modify pubs set any-other r`
acl modify *acl-name* **set unauthenticated** *perms*	
	これを指定すると、指定されている ACL テンプレート定義内の非認証 ACL 記入項目を作成または編集することが可能になります。 例: `ivadmin> acl modify pubs set unauthenticated r`
acl show *acl-name*	
	指定されている ACL テンプレートの定義を構成している記入項目の完全なセットをリストします。 `ivadmin> acl show pubs`

NetSEAL コマンド

以下の NetSEAL 管理タスクは、**ivadmin** ユーティリティーを使用して実行することができます。

- 『保護ネットワークの管理』
- 291ページの『NetSEAL 接合の管理』
- 292ページの『保護ポートの管理』
- 293ページの『保護ポートの別名の管理』

保護ネットワークの管理

ネットワーク は、 NetSEAL によって保護された Policy Director 以外のサーバーとみなすことができます。保護ネットワークを追加、削除、およびリストする場合は、**ivadmin netseal** コマンドを使用することができます。

コマンド	説明
netseal network add *network netmask* **[***network-alias***]**	
	NetSEAL によって保護される新しいネットワークを作成します。 network と netmask のペアは、標準の IP ネットワーク・アドレス番号とネットマスクを表すものです。ネットワークは、ネットワークの別名をオプションで使用して識別することができます。別名を指定しなかった場合は、ネットワークをこの network と netmask のペアで識別する必要があります。そのネットワークがすでに存在している場合は、エラーが戻されます。
netseal network delete *network-id*	
	network-id が次のいずれかと一致しているシステムから、指定したネットワークを削除します。 • *network/netmask* のペア • *network-alias* データベースにこのネットワークがない場合は、エラーが戻されます。
netseal network list	
	データベース内のすべてのネットワークを表示します。これには、ネットワークとネットマスクのペアのほかに、定義されているすべての別名も含まれます。

NetSEAL 接合の管理

NetSEAL 接合によって、Policy Director サーバーを通る通信の方向が決まります。接合は、2 つの Policy Director サーバー間、あるいは、Policy Director サーバーとネットワークとの間に作成することができます。GSS トンネルを使用して、2 つの Policy Director サーバー間の接合を横断する通信を機密保護します。

ivadmin netseal junction コマンドを使用して、NetSEAL 接合を追加、削除、およびリストします。

コマンド	説明
netseal junction add *hostname destination*	
	NetSEAL サーバーから指定の宛先への接合を作成します。この場合の *hostname* には、NetSEAL サーバー名からドメイン名を取り去ったものを指定します。また、*destination* は、以下のいずれでもかまいません。 • *pd-server* • *network/netmask* の組み • *network-alias* この接合がすでに存在しているか、ホスト・サーバーが存在していないか、あるいは、宛先が存在していない場合には、エラーが戻されます。
netseal junction delete *hostname* **destination**	

	NetSEAL サーバーから指定の宛先への接合を削除します。この場合の *hostname* には、NetSEAL サーバー名からドメイン名を取り去ったものを指定します。また、*destination* は、以下のいずれでもかまいません。 • *pd-server* • *network/netmask* のペア • *network-alias* この接合が現在存在していない場合には、エラーが戻されます。このコマンドは、現行接続には無効です。
netseal junction list *hostname*	
	指定の NetSEAL サーバーのすべての NetSEAL 接合を表示します。

保護ポートの管理

Policy Director NetSEAL サーバーでは、特定のポート、ホスト、およびネットワークに対して、セキュリティー・サービスを提供します。たとえば、特定ポート上の Telnet の通信を機密保護するように NetSEAL サーバーを構成することができます。

ivadmin netseal port コマンドを使用して、保護ポートを追加、削除、およびリストします。Policy Director サーバーやネットワークのポートを指定することができます。

コマンド	説明
netseal port add *destination port-id*	
	destination が次のいずれかに一致する指定ポート ID 上の指定宛先への接続を保護します。 • *pd-server* • *network/netmask* のペア • *network-alias* また、この場合、*port-id* は、以下のいずれでもかまいません。 • *port* • *port-range* • *port-alias* このポートがすでに保護されている場合、サーバーが存在していない場合、または、ポート別名が存在していない場合には、エラーが戻されます。
netseal port delete *destination port-id*	

	指定のポート上の指定の宛先への接続の保護を停止します。この場合の *destination* は、以下のいずれでもかまいません。 • *pd-server* • *network/netmask* のペア • *network-alias* また、この場合、*port-id* は、以下のいずれでもかまいません。 • *port* • *port-range* • *port-alias* このポートがもう保護されていない場合、サーバーが存在していない場合、または、ポート別名が存在していない場合には、エラーが戻されます。
netseal port list *destination*	
	指定の宛先のすべてのポートのリストを表示します。この場合の *destination* は、以下のいずれでもかまいません。 • *pd-server* • *network/netmask* のペア • *network-alias* サーバーが存在していない場合には、エラーが戻されます。

注: port range は、ダッシュで区切った 2 つのポート番号 (22-88 など) で表す必要があります。

保護ポートの別名の管理

ivadmin port-alias コマンドを使用して、ポートの別名を追加、削除、およびリストします。トラップ・ポートの範囲をもっと分かりやすい方法で識別するには、*port aliases* を使用します。

コマンド	説明
netseal port-alias add *port-spec port-alias*	
	指定のポート仕様の新しいポート別名を作成します。この場合の *port-spec* は、以下のいずれでもかまいません。 • *port* • *port-range* このポート範囲に別の名前ですでに別名が指定されている場合には、エラーが戻されます。
netseal port-alias delete *port-id*	
	システムから、指定のポート ID のポート別名を削除します。この場合の *port-id* は、以下のいずれでもかまいません。 • *port* • *port-range* • *port-alias* *port-id* は、ポート、ポート範囲、またはポート別名のいずれでもかまいません。データベースにこのポート別名がない場合には、エラーが戻されます。
netseal port-alias list	

	データベースにあるすべてのポート別名を表示します。

構成管理コマンド

ivadmin admin 構成管理コマンドでは、サーバーに関する情報を表示します。

コマンド	説明
admin show configuration	

	ユーザー・レジストリーが LDAP と DCE のいずれにあるかという情報を表示します。
	
	例:
	
	`ivadmin> admin show configuration`
	
	これによる出力は、下記のようなものになります。
	
	`LDAP: TRUE`
	`SECAUTHORITY: Default`
	`GSO: TRUE`

ユーザー管理コマンド

以下の **ivadmin user** コマンドには、管理コンソールのコマンドのうち、同等の **Users** 管理タスク・コマンドと同じ機能が備わっています。管理コマンドのこのセットにより、デフォルトの LDAP レジストリー内のユーザー記入項目を制御します。

ユーザー は、Policy Director ユーザーです。 *GSO user* は、Web サーバーなどの Web リソースを使用して作業するための追加権限を持っている Policy Director ユーザーです。

コマンド	説明
user create [-gsouser] ***user-name dn cn sn pwd***	

	デフォルトの LDAP レジストリー・データベースに識別名がまだ収められていないユーザーの新しい Policy Director ユーザー (secUser) アカウントを、LDAP ユーザー・レジストリーに作成します。
	
	-gsouser 引き数はオプションです。 オプションのコマンドには、ダッシュ (-) を付ける必要があります。 -gsouser 引き数を指定した場合、ユーザーは、GSO ユーザー (gsouser) にもなります。
	
	user-name 引き数は、作成されるユーザーの名前です。 この名前には、固有名を指定する必要があります。
	
	dn 引き数は、作成されるユーザーに割り当てられる LDAP 識別名です (たとえば、`cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US` など)。 この DN には、固有名を指定する必要があります。
	
	cn 引き数は、作成されるユーザーに割り当てられる共通名です (たとえば、`Diana Lucas` など)。
	
	sn 引き数は、作成されるユーザーの名字です (たとえば、`Lucas` など)。
	
	pwd 引き数は、この新しいユーザーに設定されるパスワードです。パスワードは、Policy Director 管理者が設定するパスワード・ポリシーに従う必要があります (たとえば、`mypasswd` など)。
	
	例:
	
	`ivadmin> user create -gsouser dlucas`
	`cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US`
	`"Diana Lucas" Lucas` *`mypasswd`*
	
	ユーザー・アカウントを有効にするには、ユーザー情報を変更してこのユーザーを手動で活動化する必要があります。この情報を変更するには、アカウント有効フラグを “yes” に設定してください。
	
	ユーザーに関する記述を追加するには、**ivadmin modify user** コマンドを使用して、ユーザー・アカウント情報を変更する必要があります。

user import [-gsouser] ***user-name dn***	

	これを指定すると、デフォルトの LDAP レジストリー・データベースにすでに収められている識別名の既存ユーザーを Policy Director 情報で更新し、セキュア・ドメインに参加できるようにすることが可能になります。
	
	例:
	
	`ivadmin> user import -gsouser mlucaser`
	`cn=Mike Lucaser,ou=Austin,o=Wesley Inc,c=US`

user modify ***user-name*** **description** *description*	

	管理者がこのユーザーをもっと簡単に識別できるようにする情報の記述を追加します。 例: `ivadmin> user modify dlucas description "Diana Lucas, Credit Dept HCUS`
user modify *user-name* password *password*	
	ユーザーのパスワードを現行パスワードから新規パスワードに変更します。このパスワードの確認は必要ありません。 例: `ivadmin> user modify dlucas password newpasswd`
user modify *user-name* authentication-mechanism *mech*	
	認証に使用するメカニズムを変更します。 例: `ivadmin> user modify dlucas authentication-mechanism dce`
user modify *user-name* account-valid {yes | no}	
	アカウントがアクティブか非アクティブかを指定します。アカウントを活動化するには “yes” を選択し、非活動化するには “no” を選択します。 例: `ivadmin> user modify dlucas account-valid yes`
user modify *user-name* password-valid {yes | no}	
	パスワードがアクティブか非アクティブかを指定します。パスワードを活動化するには “yes” を選択し、非活動化するには “no” を選択します。 例: `ivadmin> user modify dlucas password-valid no`
user modify *user-name* gsouser {yes | no}	
	指定している Policy Director ユーザーを GSO ユーザーにもするか否かを指定します。このユーザーを GSO ユーザーとして追加するには “yes” を選択し、GSO ユーザーとして除去するには “no” を選択します。 例: `ivadmin> user modify dlucas gsouser no`
user delete *user-name*	

	既存ユーザー・アカウントを LDAP ユーザー・レジストリーから削除します。Policy Director ユーザー・アカウントを削除すると、GSO ユーザー・アカウント情報もデフォルトの LDAP レジストリーから削除されます。 例: `ivadmin> user delete dlucas` ユーザー・アカウントと関連付けられているすべてのリソース・クリデンシャルが、そのユーザー・アカウントの削除と同時に自動的に除去されます。
user show *user-name*	
	指定されているユーザーに関するユーザー・アカウント情報を表示します。 例: `ivadmin> user show dlucas`
user show-dn *dn*	

	識別名 (DN) を指定すると、ユーザーに関する追加情報を提供します。
	
	例:
	
	`ivadmin> user show-dn`
	`cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US`

user show-groups *username*	

	指定されているユーザーがメンバーのグループを表示します。
	
	例:
	
	`ivadmin> user show-groups dlucas`
	
	これによって、下記のようなリストが生成されます。
	
	`sales`
	`credit`
	`engineering`

user list *pattern max-return*	

	指定されたパターンのすべての構成ユーザー・アカウントのリストを生成します。これは、ユーザー名別にリストされます。このリストは、そのユーザー・アカウントの作成順に表示されます。
	
	pattern 引き数によって、リストする対象のパターンを指定します。 ワイルドカードはユーザー名と突き合わせられます。パターンは、ワイルドカードとストリング定数の組み合わせを組み入れることができ、大文字小文字は区別されます (たとえば、`*luca*` など)。
	
	max-return 引き数は、1 つの要求ごとに検出されて戻される記入項目の数を制限します (たとえば、2 など)。 この数値は、LDAP サーバーの構成によっても制御されます。この LDAP サーバーの場合、検索操作の一部として戻すことができる結果の最大数を指定することができます。 Policy Director は、*max-return* の最小値と LDAP サーバー内に収められている構成値を戻します。
	
	例:
	`ivadmin> user list *luca* 2`
	
	これによって、下記のようなリストが生成されます。
	`dlucas`
	`mlucaser`

user list-dn *pattern max-return*	

	識別名の一部分だけしか認識されていない場合は、すべての構成ユーザー・アカウントの (識別名別にリストされる) リストが生成されます。このリストは、そのユーザー名の作成順に表示されます。
	
	ワイルドカードは、そのユーザーの識別名の `cn=` 部分を除く CN 部分と突き合わせられます。
	
	max-return の数値は、LDAP サーバーの構成によっても制御されます。 この LDAP サーバーの場合、検索操作の一部として戻すことができる結果の最大数を指定することができます。 Policy Director は、*max-return* の最小値と LDAP サーバー内に収められている構成値を戻します。
	
	例:
	`ivadmin> user list-dn *luca* 2`
	
	これによって、下記のようなリストが生成されます。
	`Diana Lucas,ou=Austin,o=Wesley Inc,c=US`
	`Mike Lucaser,ou=Austin,o=Wesley Inc,c=US`

技術上の注:

user show-dn コマンドと **user show-groups-dn** コマンドの *dn* 引き数は、形式どおりに正確に入力する必要があることに注意してください。*dn* 引き数にスペースが含まれている場合は、二重引用符 (″) を使用してください。

たとえば、次のとおりです。

```
cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US
```

user show コマンドと **user show-dn** コマンドは、ユーザー Diana Lucas の場合、下記のような情報を表示します。

```
Login ID: dlucas
LDAP dn: cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US
LDAP cn: Diana Lucas
LDAP sn: Lucas
Description: Diana Lucas, Credit Dept HCUS
IS SecUser: true
IS GSO user: false
Account valid: true
Password valid: true
Authorization mechanism:
Default: LDAP
```

グループ管理コマンド

以下の **ivadmin group** コマンドは、管理コンソールの**グループ**管理タスク・コマンドに相当します。この管理コマンドのセットによって、LDAP ディレクトリー・レジストリーのグループ記入項目を制御します。

グループ とは、同じような属性が指定されている Policy Director ユーザー・アカウントの集合です。グループに分けることによって、管理者は、アクセス制御リスト (ACL) にグループ名を使用することが可能になり、すべてのユーザーを個別にリストする必要がなくなります。

どのグループ記入項目も削除または変更することができます。さらに、グループまたはグループ・メンバーシップに関する情報を表示することができます。管理者として、すべての構成グループをリストすることも可能です。

コマンド	説明
group create *groupname dn cn*	
	新しい Policy Director グループ (SecGroup) を LDAP ユーザー・レジストリー内に作成します。 *groupname* 引き数は、作成されるグループの名前です。この名前には、固有名を指定する必要があります。 *dn* 引き数は、作成されるアクセス・グループに割り当てられる LDAP 識別名です (たとえば、cn=credit,ou=Austin,o=Wesley Inc,c=US など)。 *cn* 引き数は、グループに割り当てられる共通名です (たとえば、Credit など)。 例: ivadmin> group create credit cn=credit,ou=Austin,o=Wesley Inc,c=US Credit
group import *groupname dn*	

	既存の LDAP レジストリー・グループに関する情報をインポートして Policy Director グループを作成します。このグループを LDAP レジストリーの中に前もって入れておかなければ、Policy Director グループは、情報をインポートしてそのグループを作成することができません。作成されるグループの名前には、固有名を指定する必要があります。 例: `ivadmin> group import engineering cn=engineering,ou=Austin,o=Wesley Inc,c=US`
group modify *groupname* description *description*	
	Policy Director 管理者がもっと簡単に識別できるように、指定されているグループの記述を追加します。 例: `ivadmin> group modify credit description "Credit, Dept HCUS`
group modify *groupname* add *user-name*	
	指定されているグループに新しいユーザーを追加します。 例: `ivadmin> group modify engineering add dlucas`
group modify *groupname* remove *user-name*	
	指定されているグループから既存ユーザーを削除します。 例: `ivadmin> group modify engineering remove dlucas`
group delete *groupname*	
	既存グループとそのグループに関連付けられているすべての記入項目を削除します。 例: `ivadmin> group delete engineering`
group show *groupname*	
	指定されているグループに関する詳細を表示します。 例: `ivadmin> group show credit`
group show-dn *dn*	
	指定されている識別名のグループ名を提供します。 例: `ivadmin> group show-dn cn=credit,ou=Austin,o=Wesley Inc,c=US`
group show-members *groupname*	

	指定されているグループのメンバーを、その識別名別にリストして表示します。
	
	例:
	
	`ivadmin> group show-members credit`
	
	これによって、下記と同じような情報が表示されます。
	
	`dlucas`
	`mlucaser`

group list *pattern max-return*	

	指定されているパターンに一致する名前のすべての構成グループのリストを生成します。これは、グループ名別にリストされます。
	
	pattern 引き数によって、リストする対象のパターンを指定します。ワイルドカードはグループ名と突き合わせられます。パターンは、ワイルドカードとストリング定数の組み合わせを組み入れることができ、大文字小文字は区別されます (たとえば、`*Austin*` など)。
	
	max-return 引き数は、1 つの要求ごとに検出されて戻される記入項目の数を制限します (たとえば、2 など)。この数値は、LDAP サーバーの構成によっても制御されます。この LDAP サーバーの場合、検索操作の一部として戻すことができる結果の最大数を指定することができます。Policy Director は、*max-return* の最小値と LDAP サーバー内に収められている構成値を戻します。
	
	これによって、下記と同じような情報が表示されます。
	
	`credit`
	`marketing`

group list-dn *pattern max-return*	

	識別名の一部分だけしか認識されていない場合は、すべての構成グループのリストが生成されます。これは、指定されているパターンの識別名別にリストされます。
	
	ワイルドカードは、そのグループの識別名の `cn=` 部分を除く CN 部分と突き合わせられます。
	
	max-return の数値は、LDAP サーバーの構成によっても制御されます。この LDAP サーバーの場合、検索操作の一部として戻すことができる結果の最大数を指定することができます。 Policy Director は、*max-return* の最小値と LDAP サーバー内に収められている構成値を戻します。
	
	例:
	
	`ivadmin> group list-dn *t* 2`
	
	これによって、下記と同じような情報が表示されます。
	
	`cn=credit,ou=Austin,o=Wesley Inc,c=US`
	`cn=marketing,ou=Boston,o=Austin Sale,c=US marketing`

技術上の注:

dn 引き数は、**group show-dn** コマンドの出力で示される形式のとおりに正確に入力する必要があることに注意してください。*dn* にスペースが含まれている場合は、二重引用符 (″) を使用してください。

たとえば、次のとおりです。

```
cn=credit,ou=Austin,o=Wesley Inc,c=US
```

group show コマンドと **group show-dn** コマンドは、グループ credit の場合、下記のような情報を表示します。

```
Group ID: credit
LDAP dn: cn=credit,ou=Austin,o=Wesley Inc,c=US
Description: Credit, Dept HCUS
LDAP cn: credit
Is SecGroup: true
```

リソース管理コマンド

以下の Policy Director **ivadmin** コマンドは、リソース関連情報を制御する一連の管理コマンドです。

リソース管理情報には、次のものがあります。

- 『リソースの管理』
- 303ページの『リソース・グループの管理』
- 305ページの『リソース・クリデンシャルの管理』

リソースの管理

以下の **ivadmin rsrc** コマンドを使用すれば、管理者は、GSO ユーザー向けの Web サーバーなどのさまざまなリソースを管理できるようになります。

リソース は Web サーバーです。スマート接合定義における **-T** という ID は、該当の Web サーバーを識別します。

ivadmin rsrc コマンドは、該当の Web リソースの名前を識別します。

以下の **ivadmin rsrc** コマンドには、管理コンソールのコマンドのうち、同等の **GSO リソース**管理タスク・コマンドと同じ機能が備わっています。

コマンド	説明
rsrc create *resource-name* [-desc *description*]	
	リソースとして Web サーバーを作成して命名します。 *resource-name* 引き数は、Web リソースにそれ自体を識別するために指定される名前です (たとえば、engwebs01 など)。 *description* 引き数は、オプションとして指定できる記述で、これを追加することで、Policy Director 管理者はこのリソースをもっと簡単に識別できるようになります。オプション・パラメーターは、すべて、先頭にダッシュ (-) を付ける必要があります。スペースが含まれている記述は、二重引用符 (″) で囲む必要があります。 `ivadmin> rsrc create engwebs01 -desc "Engineering Web server - Room 4807"`
rsrc delete *resource-name*	

	指定されているリソースを、記述情報も含めて削除します。このリソースは存在していなければなりません。存在していない場合は、エラーが表示されます。 例: `ivadmin> rsrc delete engwebs01`
rsrc list	

	LDAP ディレクトリー内に定義されているすべての Web リソースの名前を、リソース名別にリストして表示します。
	
	例:
	
	`ivadmin> rsrc list`
	
	これによって、下記と同じような情報が表示されます。
	
	`engwebs01`
	`engwebs02`
	`engwebs03`

rsrc show *resource-name*	

	指定されているリソースに関する Web リソース情報を表示します。
	
	このリソースは存在していなければなりません。存在していない場合は、エラー・メッセージが表示されます。
	
	例:
	
	`ivadmin> rsrc show engwebs01`
	
	これによって、下記と同じような情報が表示されます。
	
	`Web Resource Name: engwebs01`
	`  Description: Engineering Web server - Room 4807`

リソース・グループの管理

以下の **ivadmin rsrcgroup** コマンドは、GSO リソース情報を制御する **GSO リソース・グループ**管理タスク・コマンドに相当します。これらのコマンドを使用すれば、管理者は、さまざまなリソース・グループ関連属性を管理できるようになります。

リソース・グループ は、Web サーバーのグループを指します。この場合、このグループのサーバーには、すべて、同じユーザー ID (userid) とパスワードが設定されます。リソース・グループのすべてのリソースに対して、単一のリソース・クリデンシャルを作成することができます。Policy Director では、リソース・グループのそれぞれのリソースごとにリソース・クリデンシャルを使用するのではなく、単一のリソース・クリデンシャルをリソース・グループに使用します。

以下の **ivadmin rsrcgroup** コマンドには、管理コンソールのコマンドのうち、同等の **GSO リソース・グループ**管理タスク・コマンドと同じ機能が備わっています。

コマンド	説明
rsrcgroup create *resource-group-name* [-desc *description*]	

	Web リソース・グループを作成して命名します。 *resource-group-name* 引き数は、リソース・グループの名前です。 *description* 引き数は、オプションとして指定できる記述で、これを追加することで、このリソースを識別できるようになります。オプションの **-desc** パラメーターは、先頭にダッシュ (-) を付ける必要があります。スペースが使用されている記述は、二重引用符 (″) で囲む必要があります。 例: `ivadmin> rsrcgroup create webs4807 -desc "Web servers, Room 4807"`
rsrcgroup delete *resource-group-name*	
	指定されているリソース・グループを、記述情報も含めて削除します。このリソース・グループは、存在していなければなりません。 例: `ivadmin> rsrcgroup delete webs4807`
rsrcgroup modify *resource-group-name* add rsrcname *resource-name*	
	Web リソースを既存のリソース・グループに追加します。このリソース・グループは、存在していなければなりません。 例: `ivadmin> rsrcgroup modify webs4807 add rsrcname engwebs02`
rsrcgroup modify *resource-group-name* remove rsrcname *resource-name*	
	既存のリソース・グループから Web リソース名を削除します。 例: `ivadmin> rsrcgroup modify webs4807 remove rsrcname engwebs02`
rsrcgroup list	

	LDAP ディレクトリーに定義されているすべての Web リソース・グループの名前を表示します。“list” に続く情報は無視されます。
	
	例:
	
	`ivadmin> rsrcgroup list`
	
	これによって、下記と同じような情報が表示されます。
	
	`webs4807`
	`websbld3`
	`websbld4`

rsrcgroup show *resource-group-name*	

	指定されているリソース・グループに関する Web リソース・グループ情報を表示します。
	
	このリソース・グループは存在していなければなりません。存在していない場合は、エラー・メッセージが表示されます。
	
	例:
	
	`ivadmin> rsrcgroup show webs4807`
	
	これによって、下記と同じような情報が表示されます。
	
	`Resource Group Name: webs4807`
	`Description: Web servers, Room 4807`
	`Resource Members:`
	`  engwebs01`
	`  engwebs02`
	`  engwebs03`

リソース・クリデンシャルの管理

以下の **ivadmin rsrccred** コマンドを使用すれば、管理者は、さまざまなリソース・クリデンシャル関連属性を管理できるようになります。

リソース・クリデンシャル によって、GSO ユーザー特定リソース (Web サーバーや Web サーバーのグループなど) に対して、ユーザー識別とパスワードを提供します。

ivadmin rsrccred コマンドを使用するときは、リソースのタイプとして、“web” または “group” と指定するだけで済みます。

注: リソースやリソース・グループが存在していなければ、リソース・クリデンシャル・コマンドを適用することはできません。

コマンド	説明
rsrccred create ***resource-name*** **rsrcuser** ***resource-userid*** **rsrcpwd** ***resource-password*** **rsrctype {web | group} user** ***user-name***	

	リソース・クリデンシャルを作成して命名します。リソース・クリデンシャルを作成するためには、ユーザーとリソース (またはリソース・グループ) が両方ともすでに存在していなければなりません。ユーザー、リソース、またはリソース・グループが存在していなかったり、あるいは、指定されなかった場合は、エラー・メッセージが表示されます。 リソース・クリデンシャル管理コマンドを参照するときは、リソースのタイプに、“web” または “group” リソースだけを指定します。 *resource-name* 引き数は、リソースの作成時にそのリソースに指定される名前です (たとえば、`engwebs01` など)。 *resource-userid* 引き数は、Web サーバーのユーザーの固有のユーザー識別 (userid) です (たとえば、`4807ws01` など)。 *resource-password* 引き数は、Web サーバーのユーザーのパスワードです (たとえば、*`rsrcpwd`* など)。 *user-name* 引き数は、リソース・クリデンシャル情報の適用対象であるユーザーの名前です (たとえば、`dlucas` など)。 例: `ivadmin> rsrccred create engwebs01 rsrcuser 4807ws01 rsrcpwd rsrcpwd rsrctype web user dlucas`
rsrccred modify *resource-name* rsrctype {web | group} set [-rsrcuser *resource-userid*] [-rsrcpwd *resource-password*] user *user-name*	
	指定されているリソースのユーザー ID とパスワード・リソース・クリデンシャル情報を変更します。 ユーザーのリソース・ユーザー ID またはパスワード情報を変更または再設定するには、これらのオプション・コマンドの先頭にダッシュ (-) を付ける必要があります。リソースやリソース・グループ、およびユーザーがすでに存在していなければ、リソース・クリデンシャル情報を変更することはできません。 指定するリソースのタイプは、最初の作成時に割り当てられたリソース・タイプ (“web” または “group” など) と一致させる必要があります。 例: `ivadmin> rsrccred modify engwebs01 rsrctype group set -rsrcuser 4807ws01 -rsrcpwd newrsrpw user dlucas`
rsrccred delete *resource-name* rsrctype {web | group} user *user-name*	

	既存ユーザーに関するリソース・クリデンシャル情報だけを削除します。 リソースのタイプは、最初の作成時に割り当てられたリソース・タイプ (“web” または “group” など) と一致させる必要があります。 例: `ivadmin> rsrccred delete engwebs01 rsrctype group user dlucas`
rsrccred list user *user-name*	

	指定されているユーザーのすべての定義済みリソースの名前とそれらのタイプを表示します。
	
	例:
	
	`ivadmin> rsrccred list user dlucas`
	
	これによって、下記と同じような情報が表示されます。
	
	`Resource name: engwebs01`
	`Resource Type: group`
	`Resource name: engwebs02`
	`Resource Type: web`

rsrccred show *resource-name* rsrctype {web | group} user *user-name*	

	指定されているユーザーに関するリソース・クリデンシャル情報を表示します。
	
	リソース・クリデンシャルとユーザーは、両方とも、存在していなければなりません。存在していない場合は、エラー・メッセージが表示されます。
	
	例:
	
	`ivadmin> rsrccred show webs4807 rsrctype group user dlucas`
	
	これによって、下記と同じような情報が表示されます。
	
	`Resource Name: engwebs01`
	`Resource Type: group`
	`Resource User Id: dlucas`

レジストリー・ポリシー管理コマンド

ivadmin policy コマンドは、Policy Director ユーザーに関する一般的なポリシー情報を制御する一連の管理コマンドです。管理者は、以下のようなポリシー属性を管理することができます。

- 308ページの『ログイン・ポリシーの管理』
- 308ページの『パスワード・ポリシーの管理』

ポリシーは、システムの全体的なセキュリティーを改善するために、ユーザー・アカウントとパスワードに課せられる制約のセットを定義します。これらの制約は、一般的に (システムにあるすべてのユーザーにグローバルに)、あるいは特別に (指定されたユーザーに対してだけ) 課せられます。ユーザーに、特定のポリシーが適用される場合は、この特定のポリシーが、定義される可能性があるどの一般ポリシーよりも優先します。一般ポリシーに比べて、この特定のポリシーが制約が多くても少なくても、この優先順位が適用されます。

ログイン・ポリシーの管理

以下の **ivadmin policy** コマンドを使用すれば、管理者は、ログイン関連のポリシーを管理できるようになります。

ログイン関連の **policy** 管理タスク・コマンドを使用して、新しいログイン・ポリシーを作成したり、あるいは、既存のログイン・ポリシーをコピーします。さらに、ユーザー・アカウントのログイン・ポリシーに関する情報を表示することもできます。

ログイン関連のポリシーの場合、Policy Director は、**policy** 管理タスク・コマンドを参照するとき、相対時間は DDD-hh:mm:ss として、また絶対時間は YYYY-MM-DD-hh:mm:ss として定義します。

コマンド	説明
policy {set | get} max-account-age [*relative-time*] [-user *user-name*]	

	ユーザーに属するアカウントが満了するまでの最大日数と時間などの時間枠を制御するポリシーを管理します。
	例 :
	`ivadmin> policy set max-account-age 031-12:30:00 dlucas`
	または
	`ivadmin> policy get max-account-age dlucas`

policy {set | get} account-expiry-date [*absolute-time*] [-user *user-name*]	

	個々のユーザー・アカウントが満了する絶対日時を指定します。すべてのユーザー・アカウントが同時に満了する日時の指定にも使用できます。
	例 :
	`ivadmin> policy set account-expiry-date 1999-12-30-23:30:00 dlucas`
	または
	`ivadmin> policy get account-expiry-date dlucas`

パスワード・ポリシーの管理

以下の **ivadmin policy** コマンドを使用すれば、管理者は、さまざまなパスワード関連ポリシーの属性を管理できるようになります。

パスワード関連のポリシーの場合、Policy Director は、**policy** 管理タスク・コマンドを参照するとき、相対時間を DDD-hh:mm:ss として定義します。

コマンド	説明
policy {set | get} min-password-length [*number*]	

	パスワードの最小長を文字数で指定します。*number* 引き数は、パスワードの許容最小長です。
	例 :
	`ivadmin> policy set min-password-length 8`
	または
	`ivadmin> policy get min-password-length`

付録B. 特記事項

本書において、日本では発表されていないIBM製品（機械およびプログラム）、プログラミングまたはサービスについて言及または説明する場合があります。しかし、このことは、弊社がこのようなIBM製品、プログラミングまたはサービスを、日本で発表する意図があることを必ずしも示すものではありません。本書で、 IBMライセンス・プログラムまたは他のIBM製品に言及している部分があっても、このことは当該プログラムまたは製品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。これらのプログラムまたは製品に代えて、IBMの知的所有権を侵害することのない機能的に同等な他社のプログラム、製品またはサービスを使用することができます。ただし、IBMによって明示的に指定されたものを除き、これらのプログラムまたは製品に関連する稼働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および他社は、本書で説明する主題に関する特許権（特許出願を含む）商標権、または著作権を所有している場合があります。本書は、これらの特許権、商標権、および著作権について、本書で明示されている場合を除き、実施権、使用権等を許諾することを意味するものではありません。実施権、使用権等の許諾については、下記の宛先に、書面にてご照会ください。

〒106-0032 東京都港区六本木3丁目2-31
AP事業所
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

本書において、IBM 以外の Web サイトを参照している場合がありますが、それらはどのような場合にも、便宜のためだけに参照しているのであり、どのような意味においても、それらの Web サイトの内容を保証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当製品の資料の一部ではなく、それらの Web サイトの利用はユーザー自身の責任において行われるものとします。

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 LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

本プログラムに関する上記の情報は、適切な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。

本書において示されるパフォーマンス・データは、いずれも制御された環境で決定されたものです。したがって、稼働環境が異なれば、得られる結果は著しく異なる場合があります。また、測定値によっては開発過程で得られたものである場合があり、一般的に使用可能なシステムにおいても、これらと同様な測定値が得られると

いう保証はありません。さらに、測定値によっては推定によって見積もられたものである場合があります。実際の結果は異なる場合があります。本書を読まれるユーザーは、ユーザー固有の環境に適用可能なデータを確認してください。

他社の製品に関する情報は、それらの製品の提供者、それらの製品の発表資料、またはその他の一般に入手可能な情報源から入手しました。 IBM はそれらの製品をテストしておらず、パフォーマンスの精度、互換性、またはその他の他社製品に関するいかなる記述をも保証するものではありません。他社製品の能力に関するご質問は、それらの製品の提供者に送るようにお願い致します。

IBM の将来の方向または意向に関して記述がなされていたとしても、それらは予告なしに変更または撤回される場合があり、単に目標を示しているものです。

IBM は、お客様が提供する情報を IBM が適当と考える何らかの方法で、使用または配布する場合がありますが、そのことによって、IBM がお客様に対して何らかの義務を負うことはないものとします。

この説明には、日常の業務で使用されるデータやレポートの例が含まれています。このような例についてはできるだけ完全を期すために、個人名、会社名、ブランド名、製品名などが使用されています。こうした名前はすべて架空のものであり、実際の企業や団体で使用されている名前や住所に類似するものがあっても、まったくの偶然に過ぎません。

著作権許諾:

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ソース言語で書かれたサンプル・アプリケーション・プログラムが掲載されています。このサンプル・プログラムは、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、または配布を目的として、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。

これらの例は、すべての場合について完全にテストされたものではありません。 IBM はこれらのプログラムに信頼性、可用性、および機能について法律上の瑕疵担保責任を含むいかなる明示または暗示の保証責任も負いません。

これらのサンプル・プログラムのいかなる部分の複製物または二次的著作物にも、第三者に配布または提供する場合には、次の著作権表示を行うものとします。

© (プログラム開発者の会社名) (年)。このコードの一部は、IBM Corp. のサンプル・プログラムの派生物です。
© Copyright IBM Corp. *(年)* All rights reserved.

このマニュアルのソフトコピーを見る場合は、写真と色つきの絵が表示できないことがあります。

商標

次のものは、IBM Corporation の商標です。

AIX
DCE
IBM
FirstSecure
Global Sign-On
GSO
LDAP
Policy Director
SecureWay

他の会社名、製品名およびサービス名等はそれぞれ各社の商標または登録商標です。

AuthAPI	DASCOM, Inc.
DASCOM	DASCOM, Inc.
IntraVerse	DASCOM, Inc.
Internet Information Server (IIS)	Microsoft Corporation
Internet Explorer	Microsoft Corporation
Netscape and the Netscape logos	Netscape Communications Corporation
Netscape logos	Netscape Communications Corporation
Netscape FastTrack	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM, Inc.
NetSEAT	DASCOM, Inc.
Smart Junctions	DASCOM, Inc.
Solaris	Sun Microsystems, Inc
WebSEAL	DASCOM, Inc.

Java およびすべての Java 関連の商標は、Sun Microsystems, Inc. の商標です。

Microsoft、Windows、Windows NT、および Windows ロゴは、Microsoft Corporation の商標です。

UNIX は、 X/Open Company Limited がライセンスしている米国およびその他の国における登録商標です。

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。

[ア行]

[カ行]

[サ行]

[タ行]

［ナ行］

[ハ行]

［マ行］

[ヤ行]

[ラ行]

［ワ行］

［数字］

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

[特殊文字]

用語集

この用語集では、本書で使用されている、新規または関心が高いと考えられる用語および省略語を定義しています。この用語集には、以下のものから引用した用語および定義が含まれています。

- IBM Dictionary of Computing (New York: McGraw-Hill, 1994)。
- American National Standard Dictionary for Information Systems、 ANSI X3.172-1990 (米国規格協会 (ANSI) が 1990 年に著作権を取得)。
- Answers to Frequently Asked Questions, Version 3.0 (California: RSA Data Security, Inc., 1998)。

A

アクセス制御リスト (ACL) (access control list (ACL)). 特定のリソースの使用を許可ユーザーに限定するためのメカニズム。

ACL. アクセス制御リスト (Access control list)。

アクション履歴 (action history). クリデンシャルのライフ・サイクル内の累積イベント。

情報交換用米国標準コード (ASCII) (American National Standard Code for Information Interchange (ASCII)). データ処理システム、データ通信システム、および関連機器の間での情報交換に使用される標準コード。 ASCII セットは、7 ビットのコード化文字 (パリティー検査用のビットを含めて 8 ビット) から構成されるコード化文字セットを使用する。この文字セットは、制御文字とグラフィック文字で構成されている。

米国規格協会 (ANSI) (American National Standards Institute (ANSI)). 認定組織が米国の自主業界標準を作成して維持するための手順を決める組織。これは、生産者、消費者、および一般の関係団体から構成される。

ANSI. 米国規格協会 (American National Standards Institute)。

API. アプリケーション・プログラム・インターフェース (Application program interface)。

アプレット (applet). Java で作成され、 Java 互換の Web ブラウザーで稼働するコンピューター・プログラム。Java アプレットとも呼ばれる。

アプリケーション・プログラム・インターフェース (API) (application program interface (API)). Policy Director では、高水準言語で作成されたアプリケーション・プログラムに、特定の Policy Director 機能の使用を許可する機能インターフェース。規格ベースの Policy Director 許可 API により、アプリケーションは、集中 Policy Director 許可サービスを呼び出すことができる。これらの呼び出しを使用すれば、新しいアプリケーションごとに許可コードを作成する必要がなくなる。Policy Director 許可 API により、ビジネスにおいて、トラステッド許可フレームワーク上の全アプリケーションを標準化することができる。 Policy Director 許可 API を使用すれば、ネットワーク上のリソースへのアクセスをさらに制御することができる。Policy Director 許可 API の詳細については、 *Policy Director Programmer's Guide and Reference* を参照。

ASCII. 情報交換用米国標準コード (American National Standard Code for Information Interchange)。

監査ログ (audit log). 1 つの監査イベントにつきレコードを 1 つ保管するデータベース内のテーブル。

監査サーバー (audit server). 監査クライアントから監査イベントを受け取り、それらを監査ログに書き込むサーバー。

監査証跡 (audit trail). 一連のイベントをリンクする、論理経路形態のデータ。監査証跡により、トランザクションや所定のアクティビティーの履歴の追跡が可能になる。

認証 (authentication). 通信しているパーティーの識別の、信頼性の高い判別のプロセス。

許可 (authorization). リソースへのアクセスの許可。

B

base64 コード化 (base64 encoding). MIME をもつバイナリー・データを伝達する一般的な手段の 1 つ。

ブラウザー (browser). 「Web ブラウザー (Web browser)」を参照。

ブラウザー証明書 (browser certificate). ディジタル証明書は、クライアント側証明書とも呼ばれる。これは、SSL 使用可能 Web サーバーを介して CA によって発行される。暗号化されたファイル内のキーを使用すると、証明書の持ち主はデータの暗号化、暗号化解除、および署名を行える。一般的に、これらのキーは Web ブラウザーが保管する。アプリケーションによっては、スマー

ト・カードやその他のメディアにキーを保管できるものがある。 「ディジタル証明書 (digital certificate)」も参照。

C

CA. 認証局 (Certificate authority)。

CA 証明書 (CA certificate). ユーザーの要求により、Web ブラウザーが認識していない CA から受け入れる証明書。ブラウザーは、この証明書を使用して、その CA によって発行された証明書を保持するサーバーとの通信を認証することができる。

CAS. クリデンシャル取得サービス (Credentials Acquisition Service)。

CAS サーバー (CAS server). Policy Director クリデンシャル取得サービス (CAS) コンポーネント用のサーバー。

認証局 (CA) (certificate authority (CA)). 組織のセキュリティー・ポリシーにしたがい、セキュリティー電子識別を証明書の形態で割り当てる役目を担うソフトウェア。 CA は、登録局 (RA) からの、証明書の発行、更新、および取り消しの要求を処理することができる。CA は、IBM SecureWay Trust Authority プロダクトの RA と対話して、ディレクトリー内で証明書および CRL を発行する。「ディジタル証明書 (digital certificate)」も参照。

証明書拡張 (certificate extension). 証明書に追加フィールドを含められるようにする、X.509v3 証明書形式の任意選択機能。標準拡張とユーザー定義拡張がある。標準拡張には、キーおよびポリシーの情報、サブジェクトおよび発行者の属性、証明書経路制約を含め、さまざまな目的のためのものがある。

証明書ポリシー (certificate policy). 共通のセキュリティー要件をもつ特定のクラスのアプリケーションに対する証明書の適用性を示す、名前付きの規則の集まり。たとえば、特定の証明書タイプでユーザーが所定の価格範囲内の商品について取り引きを行うことを許可するかどうかを証明書ポリシーが示す場合がある。

証明書プロファイル (certificate profile). 必要とされる証明書のタイプ (SSL 証明書、IPSec 証明書など) を定義する特性の集まり。プロファイルは、証明書の仕様および登録を管理するのに役立つ。発行者は、プロファイルの名前を指定するほか、必要な証明書の特性 (妥当性期間、キーの使用、識別名 (DN) 制約、など) を指定することができる。

証明書取り消しリスト (CRL) (certificate revocation list (CRL)). 認証局が取り消した証明書の、ディジタル署名された、タイム・スタンプ付きのリスト。このリストにある証明書は、受諾不能とみなす必要がある。 「ディジタル証明書 (digital certificate)」も参照。

認証 (certification). 承認済みのサード・パーティーが、個人識別、業務識別、または組織識別を保証する電子証明書を発行するプロセス。

CGI. 共通ゲートウェイ・インターフェース (Common Gateway Interface)。

連鎖検証 (chain validation). 所定の証明書が発行された信頼階層内のすべての CA 署名の検証。たとえば、ある CA がその署名証明書を別の CA によって発行されている場合、ユーザーが提示した証明書の検証中に両方の署名が検証される。

クラス (class). オブジェクト指向設計またはプログラミングにおいて、共通の定義を共用し、そのために共通のプロパティー、操作、および動作を共用するオブジェクトのグループ。

クリア・テキスト (cleartext). 暗号化されていないデータ。「非暗号化テキスト (plaintext)」の同義語。

クライアント (client). (1) サーバーから共用サービスを受け取る機能単位。 (2) 別のコンピューターまたはプログラムにサービスを要求するコンピューターまたはプログラム。

クライアント / サーバー (client/server). 一方の側のプログラムが相手側のプログラムに要求を送信して応答を待つという、分散処理におけるモデル。要求側プログラムをクライアントといい、応答側プログラムをサーバーという。

コード署名 (code signing). ディジタル署名で実行可能プログラムに署名するための技法。コード署名は、インターネットで配布されるソフトウェアの信頼性を高めるよう設計されている。

共通暗号体系 (CCA) (Common Cryptographic Architecture (CCA)). 主要な IBM コンピューティング・プラットフォーム上で一貫した暗号手法を使用できるようにする IBM ソフトウェア。各種のプログラミング言語で作成されたアプリケーション・ソフトウェアをサポートしています。アプリケーション・ソフトウェアは、CCA サービスを呼び出して、DES および RSA 暗号化を含め、各種の暗号機能を実行することができる。

共通ゲートウェイ・インターフェース (CGI) (Common Gateway Interface (CGI)). Web ページと Web サーバー間で情報を転送する標準方式。

機密性 (confidentiality). 無許可パーティーに暴露されないという特性。

クリデンシャル (credential). 認証交換である人の識別を証明するのに使用される機密情報。ネットワーク・コンピューティングの環境において、もっとも一般的なタイプのクリデンシャルは、 CA が作成して署名してある証明書である。

クリデンシャル取得サービス (CAS) (Credentials Acquisition Service (CAS)). Policy Director クリデンシャル取得サービス (CAS) コンポーネント。

CRL. 証明書取り消しリスト (Certificate revocation list)。

CRL 発行間隔 (CRL publication interval). CA 構成ファイルに設定され、ディレクトリーに対する CRL の定期的な発行の時間間隔。

相互認証 (cross-certification). 1 つの CA がその専用署名キーと関連付けられた公開キーを含む証明書を別の CA に対して発行するときに使用する信頼モデル。相互認証証明書があると、1 つの管理ドメイン内のクライアント・システムまたはエンド・エンティティーが、別のドメイン内のクライアント・システムまたはエンド・エンティティーと安全に通信することができる。

暗号の (cryptographic). データの意味を隠すためのデータの変換に関する用語。

暗号 (cryptography). コンピューター・セキュリティーにおいては、非暗号化テキストの暗号化および暗号化されたテキストの暗号化解除の原理、手段、および方式。

D

デーモン (daemon). バックグラウンドでタスクを実行するプログラム。このプログラムの支援を必要とする状態が発生すると、暗黙的に呼び出される。通常、システムがデーモンを自動的に spawn するため、ユーザーはデーモンを意識する必要はない。デーモンが永続的に存在する場合もあれば、システムが間隔をおいてデーモンを再生成する場合もある。

用語 (デーモン と発音されるもの) は神話に由来する。後になって、Disk And Execution MONitor を表す頭字語 DAEMON (デーモン) という合理的な説明がなされた。

データ暗号化規格 (DES) (Data Encryption Standard (DES)). 暗号化ブロック暗号の 1 つで、1977 年に米国政府により正式規格として定義され、承認されたもの。最初は、IBM によって開発された。DES は、発表以来、徹底的に研究され、今では、広く知られ、さまざまに使用される暗号システムとなっている。

DES は対称暗号システムである。DES を通信に使用する場合、送信側と受信側の両方が同じ機密キーを認識している必要がある。このキーは、メッセージの暗号化および暗号化解除に使用される。 DES は、ハード・ディスク上のファイルを暗号形式で保管するなど、単一ユーザー暗号化にも使用できる。DES は 64 ビットのブロック・サイズをもっており、暗号化時に 56 ビット・キーを使用する。これは、当初、ハードウェアに実装できるように設計された。 NIST は DES を正式な米国政府暗号化規格として 5 年ごとに認証し直してきた。

データ記憶域ライブラリー (data storage library). 証明書、CRL、キー、ポリシー、その他のセキュリティー関連オブジェクトの持続データ・ストアにアクセスできるようにするモジュール。

暗号化解除する (decrypt). 暗号化プロセスを取り消すこと。

DER. Distinguished Encoding Rules。

DES. データ暗号化規格 (Data Encryption Standard)。

ディジタル証明書 (digital certificate). 承認済みのサード・パーティーによって個人またはエンティティーに対して発行される電子証明書。各証明書には、CA の秘密キーで署名が付けられる。個人識別、業務識別、または組織識別について保証する。

CA の役割次第で、証明書は、インターネットを通じて e-business を行うために持参人の権限を証明することもできる。ある意味では、ディジタル証明書は、自動車の運転免許や医師免許に似た役割を果たす。該当する秘密キーの持参人が特定の e-business 活動を行う権限をもっていることを証明する。

証明書には、それが証明するエンティティーに関する情報、つまり、それが個人であるか、マシンであるか、あるいはコンピューター・プログラムであるのかが含まれている。そのエンティティーの認証済み公開キーが組み込まれている。

ディジタル認証 (digital certification). 「認証 (certification)」を参照。

ディジタル署名 (digital signature). 文書またはデータに付加される、送信側の識別を保証するコード化メッセージ。

ディジタル署名は、物理的な署名よりも高いレベルのセキュリティーを提供できる。その理由は、ディジタル署名は暗号化名でも、一連の単純な識別コードでもないためである。ディジタル署名は、署名されているメッセージの暗号化された要約である。したがって、メッセージにディジタル署名を添付することにより、送信側を厳密に識別することができる。 (署名を作成できるのは送信側

のキーだけである。) また、署名されているメッセージのコンテンツも固定される (暗号化されたメッセージの要約がメッセージ・コンテンツと一致している必要がある。一致していない場合、署名は無効である)。したがって、あるメッセージからディジタル署名をコピーして、別のメッセージに適用することはできない。要約、つまりハッシュが一致しないからである。署名付きのメッセージに変更が行われると、その署名は無効になる。

ディジタル署名アルゴリズム (digital signature algorithm). ディジタル署名規格 (Digital Signature Standard) の一部として使用される公開キー・アルゴリズムの 1 つ。これは、暗号化には使用できない。ディジタル署名専用である。

ディレクトリー (Directory). 通信 (E メール、暗号交換など) に関係する情報のグローバル・リポジトリーとして使用するための階層構造。ディレクトリーは、公開キー、証明書、および認証取り消しリストを含め、PKI 構造に欠かせない特定の項目を格納する。

ディレクトリー内のデータは、ツリーの形で階層状に編成され、ツリーのトップにルートが置かれる。通常、上位のレベル編成が、各国、政府、または企業を表す。ユーザーおよび装置は、一般的に、各ツリーのリーフとして表される。これらのユーザー、組織、区域、国、および装置は、それぞれ固有の記入項目をもつ。各記入項目は、型属性で構成される。型属性は、記入項目が表すオブジェクトに関する情報を提供する。

ディレクトリー内の各記入項目は、関連付けられた識別名 (DN) と結合される。実社会のオブジェクトに固有なものであると分かっている属性がその記入項目に含まれている場合、これは固有なものとなる。次の DN の例を考えてみる。この場合、国 (C) は US、組織 (O) は IBM、組織単位 (OU) は Trust、共通名 (CN) は CA1 である。

```
C=US/O=vnet/OU=Trust/CN=CA1
```

識別コード化規則 (DER) (Distinguished Encoding Rules (DER)). DER は、コード化規則が許すコード化タイプのなかから 1 つだけ選択し、送信側のオプションをすべて除去する。

識別名 (DN) (distinguished name (DN)). ディレクトリーに格納されるデータ入力項目の固有な名前。DN は、ディレクトリーという階層構造内での記入項目の位置を固有に識別する。

DN. 識別名 (Distinguished name)。

文書暗号化キー (document encrypting key). 一般的には、DES などの対称暗号機能キー。

ドメイン (domain). 「 セキュリティー・ドメイン (security domain)」 および「登録ドメイン (registration domain)」を参照。

E

e-business. 複数のネットワークにまたがる、コンピューターを介した商取引。商品やサービスの売買が含まれる。ディジタル通信を通じた資金の転送も含まれる。

e-commerce. ビジネス間の取り引き。インターネット上での (顧客、提供業者、ベンダー、その他との) 商品やサービスの売買が含まれる。 e-business の基本要素の 1 つである。

エンド・エンティティー (end-entity). CA ではない、証明書の対象。

暗号化する (encrypt). 該当する暗号化解除コードをもつ誰かある人だけが暗号化解除により元の情報を取得できるように情報をごちゃまぜにすること。

暗号機能 (encryption/decryption). 目的の受信側の公開キーを使用してその人のためにデータを暗号化すること。その人は、対をなす秘密キーを使用して、そのデータを暗号解読する。

エクストラネット (extranet). 類似するテクノロジーを使用する、インターネットの派生物。企業は、 Web 発行、電子取り引き、メッセージ伝送、およびグループウェアを、顧客、パートナー、社内スタッフの複数の共同体に適用し始めている。

F

ファイル転送プロトコル (FTP) (File Transfer Protocol (FTP)). コンピューター間でのファイルの転送に使用するためのインターネット・クライアント / サーバー・プロトコル。

ファイアウォール (firewall). ネットワーク間の情報の流れを制限する、ネットワークを結ぶゲートウェイ。通常、ファイアウォールの目的は、外側から無許可で使用されないように内部ネットワークを保護することである。

FTP. ファイル転送プロトコル (File Transfer Protocol)。

G

ゲートウェイ (gateway). 互換性のないネットワークまたはアプリケーションが互いに通信できるようにする機能単位。

H

HTML. ハイパーテキスト・マークアップ言語 (Hypertext Markup Language)。

HTTP. ハイパーテキスト・トランザクション・プロトコル (Hypertext Transaction Protocol)。

HTTP サーバー (HTTP server). ブラウザーや、ネットワーク内の他のプログラムとの Web ベースの通信を扱うサーバー。

ハイパーテキスト (hypertext). 読み手がマウスでクリックすると別の文書を検索して表示できる、語、句、またはグラフィックが含まれているテキスト。これらの語、句、グラフィックスはハイパーリンクと呼ばれる。それらを検索することを、それらにリンクするという。

ハイパーテキスト・マークアップ言語 (HTML) (Hypertext Markup Language (HTML)). Web ページをコーディングするためのマークアップ言語。これは SGML に基づいている。

ハイパーテキスト・トランザクション・プロトコル (HTTP) (Hypertext Transaction Protocol (HTTP)). Web を越えてハイパーテキスト・ファイルを転送するためのインターネット・クライアント / サーバー・プロトコル。

I

ICL. 発行済み証明書リスト (Issued certificate list)。

インスタンス (instance). DB2 では、インスタンスは、データを格納し、アプリケーションを実行するための論理データベース管理環境である。これにより、複数のデータベースの構成パラメーターの共通セットを定義することができる。

保全性 (integrity). システムは、無許可の修正を防止する場合はデータの保全性を保護する (無許可の開示を防止する場合の、データの機密性の保護とは逆のもの)。

保全性検査 (integrity checking). 外部コンポーネントとのトランザクションによって生じた監査レコードの検査。

内部構造 (internal structure). 「スキーマ (schema)」を参照。

インターネット (Internet). コンピューター間の電子的接続を提供するネットワークの世界規模の集合。これにより、ネットワークは、電子メールや Web ブラウザーなどのソフトウェア装置を介して互いに通信することができる。たとえば、いくつかの大学が 1 つのネットワーク上にあると、他の類似のネットワークとリンクして、インターネットを形成することができる。

イントラネット (intranet). 企業内のネットワークで、通常、ファイアウォールの裏側に常駐する。これは、類似するテクノロジーを使用する、インターネットの派生物である。技術的には、イントラネットはインターネットの拡張にすぎない。HTML および HTTP は、その構成員の一部である。

IPSec. IETF によって開発された、インターネット・プロトコル ・セキュリティー規格。 IPSec はネットワーク層プロトコルの 1 つで、認証、保全性、アクセス制御、および機密性の組み合わせを柔軟にサポートする暗号セキュリティー・サービスを提供するために設計されたもの。その高度な認証機能により、IPSec は、インターネットを介して確実なポイントツーポイント接続を確立するためのプロトコルとして多くの VPN プロダクト・ベンダーによって採用されてきている。

発行済み証明書リスト (ICL) (issued certificate list (ICL)). すでに発行された証明書と、それぞれの現在の状況が示された完全リスト。証明書には、通し番号と状態で索引が付けられている。このリストは、CA によって保守され、 CA データベースに保管される。

J

Java. Sun Microsystems 社が開発した、ネットワークを意識した、プラットフォーム固有でないコンピューター・テクノロジー。Java 環境は、 Java OS、各種プラットフォーム用の仮想計算機、オブジェクト指向 Java プログラミング言語、およびいくつかのクラス・ライブラリーで構成される。

Java アプレット (Java applet). 「アプレット (applet)」を参照。 「Java アプリケーション (Java application)」と対比。

Java アプリケーション (Java application). Java 言語で作成されたスタンドアロン・プログラム。Web ブラウザーのコンテキストの外側で実行する。

Java 言語 (Java language). Sun Microsystems 社によって開発されたプログラミング言語の 1 つ。特に、アプレットおよびエージェント・アプリケーションで使用するために設計されている。

Java 仮想計算機 (JVM) (Java Virtual Machine (JVM)). バイトコードの解釈を担当する Java 実行時環境の一部。

K

キー (key). 情報の暗号化または暗号解読するために暗号で使用される数量。

キー・ペア (key pair). 非対称暗号で使用される対応するキー。一方のキーは暗号化に、もう一方のキーは暗号化解除に使用される。

L

LDAP. 軽量ディレクトリー・アクセス・プロトコル (Lightweight Directory Access Protocol)。

軽量ディレクトリー・アクセス・プロトコル (Lightweight Directory Access Protocol). ディレクトリーにアクセスするのに使用されるプロトコル。

M

MIME (マルチパーパス・インターネット・メール・エクステンション) (MIME (Multipurpose Internet Mail Extensions)). 各種文字セットをもつ言語で作成されたテキストの交換を可能にする、自由に使用できる仕様のセット。インターネット・メール規格を使用する数多くの各種コンピューター・システム間でのマルチメディア E メールも可能にする。たとえば、E メール・メッセージに、US-ASCII、リッチ化テキスト、イメージ、およびサウンドを含めることができる。

N

各国語サポート (NLS) (National Language Support (NLS)). 言語、通貨、日付と時間の形式、および数値表現を含め、ロケールの差異についての、プロダクト内のサポート。

国家安全保障局 (NSA) (National Security Agency (NSA)). 米国政府の公式のセキュリティー組織。

NLS. 各国語サポート (National language support)。

非否認 (non-repudiation). 文書の署名者がその文書に署名したことを誤って否定しないようにするためのディジタル秘密キーの使用目的。

O

オブジェクト (object). オブジェクト指向設計またはプログラミングにおいて、データおよびそのデータと関連付けられた操作を暗号化する抽象概念。「クラス (class)」も参照。

オブジェクト・タイプ (object type). IBM SecureWay ディレクトリーに格納できる種類のオブジェクト。たとえば、組織、会議室、装置、人員、プログラム、またはプロセス。

P

PEM. プライバシー拡張メール (Privacy-enhanced mail)。

PKCS. 公開キー暗号規格 (Public Key Cryptography Standards)。

PKCS#10. 「公開キー暗号規格 (Public Key Cryptography Standards)」を参照。

PKCS#12. 「公開キー暗号規格 (Public Key Cryptography Standards)」を参照。

PKI. 公開キー・インフラストラクチャー (Public key infrastructure)。

PKIX. X.509v3 ベース PKI。

PKIX 証明書管理プロトコル (CMP) (PKIX certificate management protocol (CMP)). PKIX 互換アプリケーションとの接続を使用できるようにするプロトコル。PKIX CMP は、その基本転送メカニズムとして TCP/IP を使用するが、複数のソケットにまたがる抽象概念層が存在する。このプロトコルは、追加のポーリング転送のサポートを使用できるようにする。

非暗号化テキスト (plaintext). 暗号化されていないデータ。「クリア・テキスト (cleartext)」の同義語。

事前登録 (preregistration). IBM SecureWay Trust Authority において、あるユーザー (通常、管理者) が他のユーザーを登録できるようにするプロセス。要求が承認された場合、登録権限 (RA) により、そのユーザーが Trust Authority クライアント・アプリケーションを使用して後で証明書を取得できるようにする情報が提供される。

プライバシー (privacy). 無許可データの開示からの保護。

プライバシー拡張メール (PEM) (privacy-enhanced mail (PEM)). インターネット・プライバシー拡張メール規格。インターネット設計者委員会 (IAB) がインターネットで確実な電子メールを提供するために採用したもの。PEM プロトコルは、暗号化、認証、メッセージ保全性、およびキー管理に必要なものを提供する。

秘密キー (private key). 公開 / 秘密キー・ペアのうち、所有者のみが使用できるキー。所有者が専用トランザクションを受け取ったり、ディジタル署名を行えるように

する。秘密キーで署名したデータは、対応する公開キーでのみ検証できる。 「公開キー (public key)」と対比。「公開 / 秘密キー・ペア (public/private key pair)」も参照。

プロトコル (protocol). コンピューター間の通信についての承認済みのきまり。

プロキシー・サーバー (proxy server). アクセスを要求するコンピューター (コンピューター A) とアクセスされるコンピューター (コンピューター B) との間の仲介役。したがって、エンド・ユーザーがコンピューター A に対してリソースを要求すると、この要求はプロキシー・サーバーに転送される。プロキシー・サーバーは、この要求を行い、コンピューター B から応答を入手すると、その応答をエンド・ユーザーに転送する。プロキシー・サーバーは、ファイアウォールの内側から WWW リソースにアクセスするのに役立つ。

公開キー (public key). 公開 / 秘密キー・ペアのうち、他の人が使用できるようになっているキー。このキーを使用して、他の人は、トランザクションをキーの所有者に転送したり、ディジタル署名を検証することができる。公開キーを使用して暗号化されたデータは、対応する秘密キーでのみ暗号化解除できる。「秘密キー (private key)」と対比。「公開 / 秘密キー・ペア (public/private key pair)」も参照。

公開キー暗号規格 (PKCS) (Public Key Cryptography Standards (PKCS)). 1994 年に RSA Laboratories によって開発された、各種のコンピューター・ベンダーからの表現をもつ、非公式のベンダー間の規格。これらの規格は、RSA 暗号化、Diffie-Hellman 協定、パスワード・ベースの暗号化、拡張証明書構文、暗号メッセージ構文、秘密キー情報構文、および認証構文に適用される。

- PKCS#10 は、認証要求の標準構文を指定する。
- PKCS#12 は、ユーザーの秘密キー、証明書、各種の機密などを保管または転送するための移送可能形式を指定する。

公開キー・インフラストラクチャー (PKI) (public key infrastructure (PKI)). 公開キー暗号に基づく、セキュリティー・ソフトウェアの規格。 PKI は、ディジタル証明書、認証権限、登録権限、認証管理サービス、および分散ディレクトリー・サービスのシステムである。インターネットでのトランザクションに関係する各パーティーの識別および権限を検証するのに使用される。これらのトランザクションは、識別検証が必要な操作を必要とする場合がある。たとえば、提議送信権要求の発信元、E メール・メッセージの作成者、または金融取り引きを確認する場合がある。

PKI は、ユーザーの公開暗号化キーおよび証明書を、有効な個人または法人による認証に使用できるようにすることによって、これを実現する。ディジタル証明書、認証、およびディジタル署名の検証で使用される公開暗号化キーおよび証明書が含まれているオンライン・ディレクトリーを提供する。

PKI は、公開暗号化キーについての検証照会および要求に対して、迅速かつ能率よく応答する手段を提供する。システムに対して潜在的なセキュリティーの脅威を識別したり、セキュリティー・ブリーチ (抜け穴) を扱うためにリソースの保守も行う。最後に、PKI は、重要な商取引のためにディジタル・タイム・スタンプ・サービスも提供する。

公開 / 秘密キー・ペア (public/private key pair). 公開 / 秘密キー・ペアは、キー・ペア暗号の概念 (キー管理問題を解決するために 1976 年に Diffie と Hellman により採り入れられた) の一部である。この概念では、各人は、1 つは公開キーと呼ばれ、もう 1 つは秘密キーと呼ばれる、キーのペアを取得する。各人の公開キーは、秘密キーが秘密にされている間は共通になっている。送信側と受信側が秘密情報を共用する必要はない。通信はすべて公開キーだけを必要とし、秘密キーが送信されたり、共用されることはない。なんらかの通信チャネルを、盗聴または漏えいの心配がないものとして信頼する必要はなくなった。必要なことは、公開キーを、信頼できる (認証された) 方法で (たとえば、トラステッド・ディレクトリー内で) それぞれのユーザーと関連付けなければならないことだけである。誰でも、公衆情報を使用して、機密メッセージを送信できる。ただし、メッセージは、秘密キーでのみ暗号化解除できる。秘密キーは、目的の受信側だけが所有している。さらに、キー・ペア暗号は、プライバシー (暗号化) のためだけでなく、認証 (ディジタル署名) のためにも使用できる。

R

RA. 登録権限 (Registration authority)。

RC2. Ron Rivest によって RSA データ・セキュリティー用に設計された、可変キー・サイズ・ブロック暗号。*RC* は *Ron's Code* または *Rivest's Cipher* を表す。これは、DES よりも高速であり、DES のドロップイン置き換えとして設計されている。適切なキー・サイズを使用することによって、徹底的なキー検索に対する保証を DES よりも大きくすることも、小さくすることもできる。64 ビットのブロック・サイズをもち、ソフトウェアでは DES の 2 倍ないし 3 倍の速さである。RC2 は、DES と同じモードで使用できる。

ソフトウェア発行者協会 (SPA) と米国政府間の同意により、RC2 は特殊な状況が与えられている。これにより、エクスポート承認プロセスは、通常の暗号エクスポート・プロセスよりも単純になっている。ただし、高速エクスポート承認に適格となるためには、プロダクトは、

いくつかの例外はあっても、RC2 キー・サイズを 40 ビットに制限する必要がある。追加のストリングを使用して、可能な暗号化の大きなルックアップ・テーブルを先行して計算しようとするハッカーの裏をかくことができる。

RC4. Ron Rivest によって RSA データ・セキュリティー用に設計された、可変キー・サイズ・ブロック暗号。*RC* は *Ron's Code* または *Rivest's Cipher* を表す。これは、RC2 と似ているが、ブロック・サイズが 128 ビットである。

登録権限 (RA) (registration authority (RA)). 組織の業務方針が記載要求の最初の受け取りから認証取り消しまで必ず適用されるようにディジタル証明書を管理する IBM SecureWay Trust Authority ソフトウェア。

登録データベース (registration database). 認証要求および発行済みの証明書に関する情報が含まれているもの。このデータベースには、記載データのほか、そのライフ・サイクル中の認証データへのすべての変更が格納される。

登録ドメイン (registration domain). 特定の認証登録プロセスに関係するリソース、ポリシー、および構成オプションのセット。ドメイン名は、登録アプリケーションを実行するのに使用される URL のサブセットである。

否認する (repudiate). 虚偽であるとして拒否すること。たとえば、特定のメッセージを送信したか、特定の要求を実行依頼したことを否定すること。

要求識別子 (request ID). RA に対する認証要求を固有に識別する 24 ～ 32 文字の ASCII 値。この値を認証要求トランザクションで使用すると、その要求またはそれと関連付けられた証明書の状況を検索できる。

S

スキーマ (schema). IBM SecureWay ディレクトリーに関しては、異なるオブジェクト・タイプ間の関係を定義する内部構造。

セキュア・ソケット層 (SSL) (Secure Sockets Layer (SSL)). エンド・ユーザーに対して可能なかぎり透過的な組み込みセキュリティー・サービス付きの、 IETF 標準通信プロトコル。ディジタル式の確実な通信チャネルを提供する。

SSL 使用可能サーバーは、通常、標準 HTTP 要求を要求するものとは別のポート上で SSL 接続要求を受け入れる。 SSL は 1 つのセッションを作成するが、このセッションでは、 2 つのモデム間での通信をセットアップする交換信号が 1 回だけ発生する必要がある。その後で、通信は暗号化される。メッセージ保全性検査は、SSL セッションが満了するまで続行する。

セキュリティー・ドメイン (security domain). 同じ CA によって認証された証明書をもつグループ (会社、作業グループまたはチーム、研修または行政上のもの)。CA によって署名された証明書をもつユーザーは、同じ CA によって署名された証明書をもつ別のユーザーの識別を信頼することができる。

サーバー (server). (1) ネットワークにおいて、他の端末に機能を提供するデータ装置。たとえば、ファイル・サーバー。(2) TCP/IP では、別のサイトにあるシステムの要求を扱う、ネットワーク内のシステム。クライアント / サーバーと呼ばれる。

サーバー証明書 (server certificate). Web サーバーが SSL ベースのトランザクションを行えるように CA によって発行されたディジタル証明書。ブラウザーが SSL プロトコルを使用してサーバーに接続すると、サーバーは、自分の公開キーをブラウザーに送信する。これにより、サーバーの識別の認証が可能になる。暗号化情報もサーバーへ送信できるようにする。 「CA 証明書 (CA certificate)」、「ディジタル証明書 (digital certificate)」、および 「ブラウザー証明書 (browser certificate)」も参照。

servlet. Java の可能なサーバーに追加機能を与えるサーバー側のプログラム。

SGML. 標準汎用印刷指定言語 (Standard Generalized Markup Language)。

署名する (sign). 秘密キーを使用して、署名を生成すること。署名は、自分が責任者であり、署名しているメッセージを承認していることを証明する手段である。

署名と検証 (signing and verifying). 署名するとは、秘密ディジタル・キーを使用して署名を生成することである。検証するとは、対応する公開キーを使用して署名を検証することである。

シンプル・メール転送プロトコル (SMTP) (Simple Mail Transfer Protocol (SMTP)). インターネットで電子メールを転送するプロトコル。

サイト証明書 (site certificate). CA 証明書と似ているが、特定の Web サイトについてのみ有効なもの。 「CA 証明書 (CA certificate)」も参照。

S/MIME. インターネットで伝送される E メールの署名および暗号化をサポートする規格。 「MIME」を参照。

SMTP. シンプル・メール転送プロトコル (Simple Mail Transfer Protocol)。

SSL. セキュア・ソケット層 (Secure Sockets Layer)。

標準汎用印刷指定言語 (SGML) (Standard Generalized Markup Language (SGML)). マークアップ言語を記述するための規格。HTML は SGML に基づいている。

T

TCP/IP. 伝送制御プロトコル / インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)。

トップ CA (top CA). PKI CA 階層のトップにある CA。

伝送制御プロトコル / インターネット・プロトコル (TCP/IP) (Transmission Control Protocol/Internet Protocol (TCP/IP)). ローカル・エリア・ネットワークと広域ネットワークについて対等接続機能をサポートする 1 組の通信プロトコル。

トリプル DES (triple DES). 非暗号化テキストを 3 回暗号化する対称アルゴリズム。これを行う方法は多数あるが、複数の暗号化の最も確実な形体は、別個のキーを 3 つもつトリプル DES である。

Trust Authority. ディジタル証明書の発行、更新、および取り消しをサポートする、統合 IBM SecureWay セキュリティー・ソリューション。これらの証明書をさまざまなインターネット・アプリケーションで使用して、ユーザーを認証し、信頼できる通信を保証する手段を提供できる。

信頼ドメイン (trust domain). 同じ CA によって認証された証明書をもつ 1 組のエンティティー。

信頼モデル (trust model). 認証局が他の認証局を証明する方法を管理する構造化規則。

トンネル (tunnel). VPN 用語では、インターネットを通じて作成される、オンデマンド仮想対等接続。リモート・ユーザーは、接続されていれば、トンネルを使用して、団体の私設網上のサーバーと安全な、暗号化され、カプセル化された情報を交換することができる。

タイプ (type). 「オブジェクト・タイプ (object type)」を参照。

U

Unicode. ISO 10646 によって定義された、16 ビット文字セット。Unicode 文字コード化規格は、情報処理のための国際的な文字コードである。Unicode 規格は、世界の主要なスクリプトを包含し、ソフトウェアの国際化対応および地域化対応のための基礎を提供する。 Java プログラミング環境のソース・コードはすべて、Unicode で作成されている。

統一リソース標識 (URI) (Uniform Resource Indicator (URI)). 絶対 URL では、HOST 名か IP アドレスとネットワーク・ポートの両方との関係で、 URI 位置を示す。

URL (Uniform Resource Locator (URL)). インターネット上のリースをアドレス指定するための体系。URL は、プロトコル、ホスト名、または IP アドレスを指定する。特定のマシンからリソースにアクセスするのに必要なポート番号、経路、およびリソース明細も組み込まれている。

URI. 統一リソース標識 (Uniform Resource Indicator)。

URL. URL (Uniform Resource Locator)。

ユーザー認証 (user authentication). メッセージの発信元が識別可能であり、許可を受けたメッセージの所有者であることを確認するプロセス。予想したエンド・ユーザーまたはシステムと通信しているかどうかも確認する。

UTF-8. 変換形式の 1 つ。8 ビット文字セットしか扱わない情報処理システムが、情報を失わずに、16 ビット Unicode を 8 ビットの同等に変換し、その逆の変換も行えるようにする。

V

VPN. 仮想私設網 (Virtual Private Network)。

仮想私設網 (VPN) (Virtual Private Network (VPN)). 電話回線ではなくインターネットを使用してリモート接続を確立する私設データ・ネットワーク。ユーザーは電話会社ではなくインターネット・サービス・プロバイダー (ISP) を通じて団体ネットワーク・リソースにアクセスするため、組織は、リモート・アクセスのコストを著しく軽減できる。VPN は、データ交換のセキュリティーも向上させる。従来のファイアウォール・テクノロジーでは、メッセージ・コンテンツは暗号化できるが、送信元アドレスおよび宛先アドレスは暗号化されない。VPN テクノロジーでは、ユーザーはトンネル接続を確立することができる。この接続では、情報パケット (コンテンツとヘッダー) は暗号化され、カプセル化される。

W

Web ブラウザー (Web browser). デスクトップ PC 上で実行し、ユーザーが WWW ページまたはローカル HTML ページを表示できるようにするクライアント・ソ

フトウェア。これは、 Web およびインターネットで使用可能な大量のハイパーメディア・データのコレクションに自在にアクセスできるようにする検索ツールである。ブラウザーによっては、テキストとグラフィックスを表示できるものもあるが、テキストしか表示できないものもある。ほとんどのブラウザーは、 FTP トランザクションなど、主要な形式のインターネット通信を扱うことができる。

Web サーバー (Web server). ブラウザー・プログラムから情報リソースについての要求に応答するサーバー・プログラム。 「サーバー (server)」も参照。

ワールド・ワイド・ウェブ (WWW) (World Wide Web (WWW)). ハイパーメディア・データが含まれているコンピューター間で接続のネットワークが確立されているインターネットの部分。このデータは、情報を提供し、WWW およびインターネット内の他のデータにリンクできるようにする。 WWW リソースは、Web ブラウザー・プログラムを通じてアクセスされる。

X

X.509 証明書 (X.509 certificate). セキュア・インターネット・ネットワークを越えてディジタル署名付きの証明書の確実な管理および配布をサポートするよう設計された、広く受け入れられている証明書規格。 X.509 証明書は、承認済みのサード・パーティーによってディジタル署名された公開キーの配布手順を提供するデータ構造を定義する。

X.509 バージョン 3 証明書 (X.509 Version 3 certificate). X.509v3 証明書は、証明書アプリケーション情報、証明書配布情報、証明書取り消し情報、ポリシー情報、およびディジタル署名の格納および検索を行うための拡張データ構造をもっている。

X.509v3 プロセスは、すべての証明書についてタイム・スタンプ付きの CRL を作成する。証明書が使用されるたびに、X.509v3 の機能により、アプリケーションは、証明書の妥当性を検査することができる。また、証明書が CRL 上にあるかどうかもアプリケーションが判別できるようにする。X.509v3 CRL は、特定の妥当性期間の間構成することができる。また、証明書を無効にする可能性のあるその他の状況に基盤を置くこともできる。たとえば、ある従業員が組織を辞めた場合、その証明書は CRL 上に置かれる。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12