IBM® SecureWay® Policy Director

概説

バージョン 3 リリース 0

SB88-8503-00
(英文原典：SCT6-3KNA-00)

IBM® SecureWay® Policy Director

概説

バージョン 3 リリース 0

SB88-8503-00
(英文原典：SCT6-3KNA-00)

お願い

本書、および本書で記述する製品をご使用になる前に、103ページの『付録. 特記事項』 を必ずお読みください。

本書は、IBM 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。また新版で特に断りがない限り、それ以降のすべてのリリースおよびモディフィケーションにも適用されます。

本書は、IBM SecureWay Global Sign-On, Version 2.0.200 に置き換わるものです。

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： SCT6–3KNA–00
IBM® SecureWay® Policy Director
Up and Running
Version 3 Release 0

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 1999.11

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 (Policy Director) のインストールおよび構成についての情報を記載しています。 Policy Director サーバーは、以下のオペレーティング・システムにインストールできます。

- Microsoft® Windows NT®
- AIX®
- Solaris®

NetSEAT クライアントは、以下のオペレーティング・システムにインストールできます。

- Windows® 95
- Windows 98
- Windows NT

本書の対象読者

本書は、Policy Director の計画とインストールを担当する管理者を対象にしています。

管理者は、IBM 分散コンピューティング環境 (DCE) および IBM SecureWay Directory の Lightweight Directory Access Protocol (LDAP) のインストールと構成を十分理解している必要があります。 IBM SecureWay Directory サーバーおよび 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。

本書の構成

本書には、以下の章が含まれています。

- 1ページの『第1章 Policy Director の概要』では、Policy Director とその構成要素の概要を説明します。
- 15ページの『第2章 システム要件』では、ご使用の操作環境で満たす必要があるソフトウェアとハードウェアの情報について説明します。
- 19ページの『第3章 Policy Director の計画』には、Policy Director の計画、編成、および管理に役立つ情報を記載しています。

- 29ページの『第4章 IBM SecureWay Directory のインストールと構成』では、LDAP ユーザー・レジストリーを選択する場合に、IBM SecureWay Directory バージョン 3.1.1 (LDAP) Client SDK およびサーバーのインストールと構成についての情報を記載しています。 Policy Director をインストールする前に、LDAP サーバーをインストールし、構成しておく必要があります。また、Policy Director をインストールする前に、LDAP サーバーが実行されている必要があります。
- 47ページの『第5章 Policy Director (Windows 用) のインストール』では、Windows NT オペレーティング・システムへの Policy Director のインストールと構成について説明します。
- 63ページの『第6章 Policy Director (AIX 用) のインストール』では、IBM AIX オペレーティング・システムへの Policy Director のインストールと構成について説明します。
- 81ページの『第7章 Policy Director (Solaris 用) のインストール』は、Sun Solaris オペレーティング・システム上への Policy Director のインストールと構成について説明します。
- 97ページの『第8章 関連資料』には、Policy Director 用のその他の資料と関連製品の資料の参照先を記載しています。

このリリースでの新しい機能

このリリースの Policy Director には、以下の新しい機能が組み込まれています。

- ユーザーとグループのクリデンシャル情報を保管するための IBM SecureWay ディレクトリーのサポート。
- Open Group からの許可 API 仕様の最新更新。
- Policy Director 管理コンソールを使用した、IBM ファイアウォール・プロキシー・ユーザー・クリデンシャルの定義と編集の機能。
- 外部認証サービスの使用をサポートする Policy Director クリデンシャル取得サービス (CAS)。
- 新しい Policy Director クリデンシャル取得サービスを使用した、クライアント側の証明書ベース認証に対するサポート。
- WebSEAL と Policy Director CAS 間の Interface Definition Language (IDL) インターフェースを使用した、カスタマイズされた独自のクリデンシャル取得サービスを作成する機能。また、Policy Director は、Policy Director CAS サーバー機能 (始動、サーバー登録、シグナル処理など) を処理する汎用サーバー・フレームワークも提供します。

- 汎用セキュリティー・サービス (GSS) トンネル伝送に加えて、セキュア・ソケット・レイヤー (SSL) トンネル伝送メカニズムの使用を選択可能。
- ログインとパスワード・ポリシーを管理するための、Policy Director コマンド行インターフェースの使用。
- 単一サインオン・ユーザー、グループ、およびリソース (ターゲット) を管理するための、Policy Director 管理コンソールまたはコマンド行インターフェースの使用。
- Web ベースの単一サインオン・リソース・パスワード管理ツール。
- 統合されたインストール・プロセス。

西暦 2000 年対応

本製品は、2000 年問題に対応しています。本製品と一緒に使用されるすべての製品 (たとえば、ハードウェア、ソフトウェア、およびファームウェア) が、正確な日付データを本製品と正しく交換する場合、本製品は、関連資料にしたがって使用すれば、20 世紀と 21 世紀内の日付データ、および 20 世紀と 21 世紀間の日付データを正しく処理し、提供し、受信することができます。

サービスとサポート

IBM SecureWay FirstSecure オファリングに含まれているすべての製品に対するサービスとサポートについては、IBM にお問い合わせください。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があります。これらの製品を、FirstSecure オファリングの一部として取得する場合、サービスとサポートについて IBM にお問い合わせください。

表記規則

本書では、以下の表記規則を使用します。

表記規則	意味
太字	チェック・ボックス、ボタン、およびリスト・ボックス内の項目などの、ユーザー・インターフェース要素。
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任意のテキスト。
イタリック	Policy Director に関連した特殊用語の強調および初回使用。
→	メニューからの一連の選択項目を表示します。たとえば、「**File** → **Run**」をクリックするということは、「**File**」をクリックしてから、「**Run**」をクリックするという意味です。

Web 情報

Policy Director の最新の更新についての情報は、以下の Web アドレスで入手できます。

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

その他の IBM SecureWay FirstSecure 製品の更新についての情報は、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 の概要

IBM SecureWay Policy Director (Policy Director) は、IBM SecureWay FirstSecure の構成要素として、または独立した製品として入手できます。

IBM SecureWay FirstSecure について

IBM SecureWay FirstSecure (FirstSecure) は、IBM 統合セキュリティー・ソリューションに含まれています。FirstSecure は、以下のことを企業が行うのに役立つ、包括的な統合製品セットです。

- 安全な e-business 環境を確立する。
- セキュリティー計画を単純化して、セキュリティー所有者であるための合計コストを削減する。
- セキュリティー・ポリシーを導入する。
- 効果的な e-business 環境を作成する。

IBM SecureWay 製品には、以下のものが含まれています。

Policy Director

IBM SecureWay Policy Director (Policy Director) は、認証、許可、データ・セキュリティー、および Web リソース管理を提供します。

Boundary Server

IBM SecureWay Boundary Server (Boundary Server) は、以下の機能を備えています。

- フィルター処理、プロキシー、および回線レベル・ゲートウェイの重要なファイアウォール機能
- 仮想私設網 (VPN) と IBM ファイアウォールとの接続
- インターネット・セキュリティー用の構成要素
- モバイル・コード・セキュリティー・ソリューション

構成 GUI は、Policy Director のプロキシー・ユーザー機能を Boundary Server のファイアウォール製品と結合します。

Intrusion Immunity

Intrusion Immunity は、不法侵入の検出とウイルス防止保護を行います。

Trust Authority

IBM SecureWay Trust Authority (Trust Authority) は、暗号と相互運用性のための公開キー・インフラストラクチャー (PKI) 標準をサポートします。 Trust Authority は、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します。これらの証明書は、ユーザーを認証し、信頼される通信を確保する手段を提供します。

Toolbox

IBM SecureWay Toolbox (Toolbox) は、アプリケーション・プログラマーが自分のソフトウェアの中でセキュリティーを統合するのに使用できる、1 組のアプリケーション・プログラミング・インターフェース (API) です。 FirstSecure の一部として Toolbox を入手できます。 Policy Director と Toolbox にはいずれも、Policy Director API ライブラリーと資料が含まれています。

各 IBM SecureWay FirstSecure 製品は、独立してインストールすることができるので、機密保護機能のある環境への管理された移行を計画することができます。この機能により、環境を保護する複雑さとコストが削減され、Web アプリケーションとリソースを速やかに配置できるようになります。

FirstSecure 構成要素の詳細、および IBM SecureWay 製品資料のリストについては、 FirstSecure *Planning and Integration* の資料を参照してください。

IBM SecureWay Policy Director について

Policy Director は、許可とセキュリティー管理を提供する独立型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。

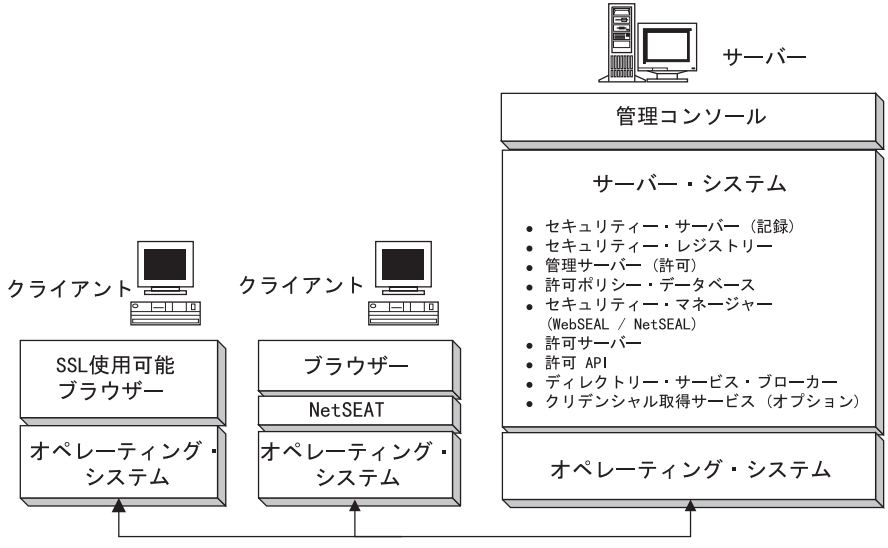
Policy Director は、認証、許可、データ・セキュリティー、およびリソース管理のサービスを提供します。Policy Director を標準のインターネット・ベース・アプリケーションと一緒に使用すると、保護され、管理の行き届いたイントラネットとエクストラネットを構築できます。

Policy Director は、Windows NT、AIX、および Solaris オペレーティング・システムで動作します。

Policy Director の構成要素

Policy Director には、以下の構成要素が含まれています。

- IBM SecureWay ディレクトリーの Lightweight Directory Access Protocol (LDAP) および IBM 分散コンピューティング環境 (DCE) のクライアントとサーバー
- Policy Director Base
- 管理サーバー
- WebSEAL と NetSEAL で構成されるセキュリティー・マネージャー
- クリデンシャル取得サービス (CAS)
- 許可サーバー
- 許可アプリケーション・プログラミング・インターフェース (API)
- NetSEAT クライアント
- 管理コンソール
- ディレクトリー・サービス・ブローカー (DSB)



Policy Director をインストールする前に、ご使用のネットワークでどのセキュリティー機能と管理機能が必要かを決定しておく必要があります。以下の節を使用して、必要な Policy Director 構成要素を決定してください。

IBM SecureWay Directory サーバーと DCE サーバー

IBM SecureWay Directory サーバーおよび 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。

Policy Director は、LDAP ユーザー・レジストリーか、DCE ユーザー・レジストリーのどちらかを使用できます。 Policy Director のインストール時に、ユーザー・レジストリーのタイプを選択するように求めるプロンプトが出されます。

LDAP ユーザー・レジストリーを使用する計画の場合、LDAP クライアントをインストールし、LDAP サーバーを構成してから、Policy Director をインストールする必要があります。 29ページの『第4章 IBM SecureWay Directory のインストールと構成』の説明に従ってください。 DCE ユーザー・レジストリーを使用する計画の場合は、LDAP のインストールと構成についての節を飛ばしてもかまいません。

IBM SecureWay ディレクトリー・サーバー

SecureWay Directory は、Lightweight Directory Access Protocol (LDAP) を提供して、保管、更新、検索、および交換用に中央設置場所にディレクトリー情報を保持します。ユーザー・レジストリーに LDAP を使用する場合、Policy Director は LDAP を使用して、ユーザーに権限を付与します。

IBM 分散コンピューティング環境サーバー

分散コンピューティング環境 (DCE) には、異種コンピューティング環境における分散アプリケーションの作成、使用、および保守をサポートするサービスとツールが含まれています。 DCE は、Policy Director サーバーが相互にユーザーを認証し、安全に通信できるセキュア・ドメインを形成します。Windows NT オペレーティング・システムでは、NetSEAT クライアントが DCE クライアントとして機能します。

Policy Director Base

Policy Director Base (IVBase) 構成要素は、すべての Policy Director 構成要素が使用する、共通参照ソフトウェアです。この構成要素は、他の Policy Director 構成要素をインストールすると (ただし、Windows に管理コンソールをインストールする場合を除く) 自動的にインストールされます。

AIX の場合、SMIT Setup (IV.Smit) 構成要素が、IV.Base パッケージの一部として組み込まれています。このパッケージには、SMIT によって使用される構成情報が入っています。このパッケージは、すべての AIX サーバーにインストールする必要があります。

管理サーバー

管理サーバー (IVMgr) は、セキュア・ドメイン全体の 1 次許可サーバーです。管理サーバーは、マスター許可ポリシー・データベースを制御し、保持します。すべてのデータは、管理サーバーを通じて流れます。

管理サーバーをセキュア・ドメイン内のコンピューターにインストールしてから、セキュリティー・マネージャーまたは許可サーバーをインストールする必要があります。ただし、必ずしも同じコンピューターにインストールする必要はありません。特定のセキュア・ドメインにインストールされる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。

管理サーバーの各インスタンスでは、以下の構成要素を管理サーバーと同じコンピューターにインストールする必要があります。

- DCE クライアント
- LDAP クライアント (ユーザー・レジストリーとして LDAP を使用する場合)
- Policy Director Base
- 管理サーバー

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 (IVNet) 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、以下の構成要素が含まれています。

- WebSEAL -- 密な Hypertext Transfer Protocol (HTTP) と Secure Sockets Layer interface (HTTPS) アクセス制御用
- NetSEAL -- 粗い Transmission Control Protocol/Internet Protocol (TCP/IP) アクセス制御用

NetSEAL と WebSEAL 構成要素は、これらの機能を構成し、使用可能にする必要があります (デフォルトでは、使用不可に設定されています)。

WebSEAL

WebSEAL (IVWeb) は、セキュリティー・マネージャーの HTTP サーバー構成要素です。 WebSEAL は、HTTP、HTTPS、および NetSEAT クライアントをサポートするセキュア Web サーバーです。WebSEAL は、Policy Director クリデンシャル取得サービス (CAS) と組み合わせて、 Policy Director ユーザーに対する X.509 証明書ベースの認証をサポートします。

NetSEAL

NetSEAL (IVTrap) は、TCP/IP サーバーに粗いアクセス制御を提供します。 NetSEAL は、TCP/IP サーバー上で設定されている 1 組のポートへのアクセスを制御します。

Policy Director 製品セットは、インターネットと専用イントラネットにまたがる、クライアント / サーバー・データ交換用のセキュリティーを提供します。 Policy Director NetSEAL および Policy Director WebSEAL は、サーバー側の製品であり、DCE によって定義されるセキュア・ドメイン内のネットワーク・データを制御し、管理します。

許可サーバー

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アプリケーションからの許可要求を処理します。許可サーバーは、第三者アプリケーション用のセキュア・ドメイン内で、少なくとも 1 つのコンピューターにインストールされている必要があります。

許可アプリケーション・プログラミング・インターフェース (API)

Policy Director 許可アプリケーション開発キット、または ADK (IVAuthADK) 構成要素には、Policy Director 許可アプリケーション・プログラミング・インターフェース (API) が組み込まれています。この API を使用すると、Policy Director 許可を使用するアプリケーションを構築することができます。

Policy Director アプリケーション開発キット (ADK) には、開発者が、企業アプリケーションに Policy Director セキュリティーと許可を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 許可サービスを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。

ADK には、C サンプル・プログラムが組み込まれています。

ADK には、Policy Director クリデンシャル取得サービス (CAS) デモンストレーション・サーバーと外部許可サービス・デモンストレーション・サーバー用のソースも含まれています。

NetSEAT クライアント

Policy Director NetSEAT クライアントは、Windows 95、Windows 98、または Windows NT 用の負荷の軽いクライアントです。 NetSEAT は、Policy Director サーバーとの保護された通信チャネルを提供します。

NetSEAT クライアント・ソフトウェアを使用すると、クライアントは、セキュア・ドメインに結合されて、WebSEAL サーバーと NetSEAL サーバーが提供する拡張セキュリティー・サービスを使用することができるようになります。NetSEAT は、クライアントのすべてのネットワーク通信を保護し、すべての Web ベースのクライアント / サーバーのトラフィックの終端間の暗号化を可能にします。

NetSEAT は、クライアントの TCP/IP トラフィック (たとえば、Telnet や POP3 のようなサービスによって生成されるトラフィック) を保護する機能を備えています。 NetSEAT を使用すると、システム管理者は、ワークステーションのネットワーク活動を介して、粗い制御を実行できます。この制御は、ユーザーを認証し、許可特権をユーザーとリソースに付加する、セキュア・ドメインの機能を使用することにより得られます。

管理コンソール

管理コンソール (IVConsole) は、Java ベースのグラフィカル・アプリケーションであり、Policy Director セキュア・ドメイン用のセキュリティー・ポリシーの管理に使用されます。管理コンソールを使用すると、会計レジストリーと 1 次許可ポリシー・データベースを使用した管理作業を実行できます。管理コンソールでは、DCE クライアントが、セキュア・ドメインにログインし、Policy Director 管理サーバーに対するセキュア管理のリモート・プロシージャー呼び出し (RPC) を実行する必要があります。管理コンソールは、Windows 95、Windows 98、または Windows NT 上で NetSEAT クライアントによって提供される負荷の軽い DCE サービス (実行時サービス) を使用します。

ディレクトリー・サービス・ブローカー

ディレクトリー・サービス・ブローカー (DSB) は、管理サーバー構成要素の一部として配布されます。Windows 95、Windows 98、または Windows NT ワークステーションで稼働する場合、管理コンソールと NetSEAT クライアントは、DSB がセキュア・ドメイン内に入っていることが必要です。通常、DSB は、初期インストールの後で、管理や構成をする必要はありません。

クリデンシャル取得サービス (任意選択)

Policy Director クリデンシャル取得サービス (CAS) は、任意選択で構成される構成要素です。

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。

クリデンシャルの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。

クライアント側の X.509 証明を使用して Policy Director に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するか、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* 情報を Policy Director 識別に対応付けることができます。

ユーザーが他の外部レジストリー内で定義されている場合、カスタマイズされた CAS サーバーを使用して、そのユーザー名を Policy Director 識別に対応付けることができます。独自の CAS サーバーを作成し、セキュア・ドメインに固有の解決方法を提供し、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、この認証とマッピングのサービスの詳細全体を決めます。 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、シグナル処理など) を処理する汎用サーバー・フレームワークも提供します。クリデンシャル取得サービス・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するようにするのは、Policy Director クリデンシャル取得サービスの開発者の仕事になります。

Policy Director の各構成要素の詳細については、*Policy Director 管理の手引き* を参照してください。

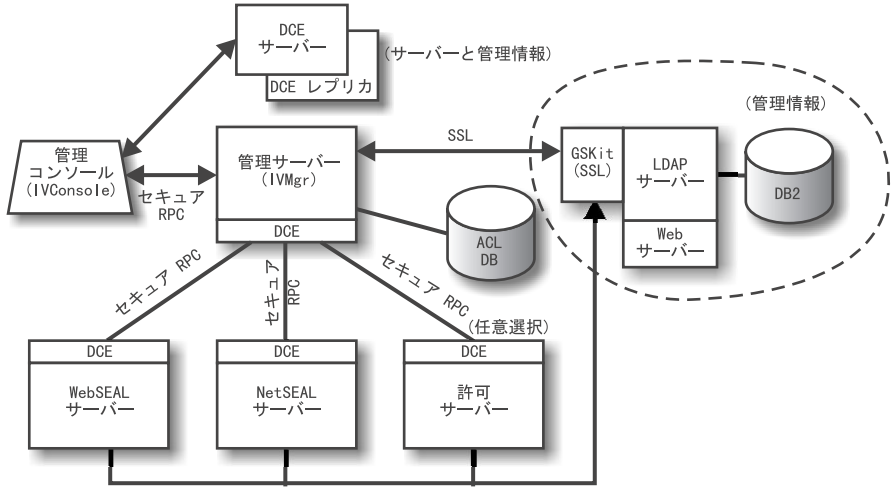
Policy Director の働き

以下の節では、Policy Director の通常の使用の実例を示す、4 つのシナリオを示しています。

- 管理者が管理コンソールを使用する場合
- ユーザーが、保護された Web リソースに Web ブラウザーからアクセスする場合
- ユーザーが、保護された TCP/IP サーバーに NetSEAT クライアントを使用してアクセスする場合
- ユーザーが、保護された第三者サーバーにアクセスする場合

管理コンソールを使用した管理

以下の図は、管理者が管理コンソールを使用して Policy Director を管理する場合のデータの流れを示しています。点線で表示されている LDAP 構成要素が必要なのは、ユーザー・レジストリーとして LDAP を使用する場合だけです。



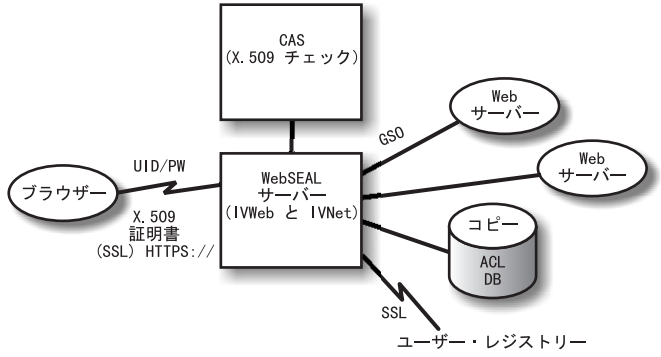
管理コンソールを使用する管理者は、セキュア・ドメインに対して認証され、クリデンシャルを受け取ります。

管理者が管理コンソールからユーザーまたはグループを管理する場合、管理コンソールは、セキュア RPC を介して管理サーバーに要求を送信します。管理サーバーは、管理サーバーの識別名 (DN) とパスワードを使用して、以前に確立された SSL 接続を介して、対応する変更を LDAP サーバーに送信します。

管理者がアクセス制御リスト (ACL) を追加、変更、または適用する場合、管理コンソールは、セキュア RPC を介して管理サーバーにデータを送信します。次に、管理サーバーは、ACL データベースのローカル・コピーにその変更を保管します。必要な ACL データベースが変更されると、管理サーバーは、ACL データベースが変更されたことを、セキュア RPC を介して他のすべてのサーバーに知らせます。 WebSEAL、NetSEAL、および許可サーバーも、ACL データベース内に更新があるかどうかについて、管理サーバーを定期的にチェックします。

保護された Web リソースに Web ブラウザーからユーザーがアクセスする場合

以下の図は、ユーザーが、保護された Web リソースに Web ブラウザーからアクセスする場合のデータの流れを示しています。



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の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。 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。 CAS の構成ファイル内で、Policy Director 管理者は、証明書 DN を Policy Director ユーザーの DN と関連付けるのに使用される表を作成できます。 CAS は、証明書を指定して WebSEAL によって呼び出されると、その証明書から DN を抜き出し、一致するものがないか、この表を調べます。一致が見つかると、CAS は、関連付けられた 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と、CAS は証明書からの DN を WebSEAL に戻します。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、戻された DN を使用して、ユーザーのクリデンシャルを検索します。

X.509 証明書の詳細は、以下の Web アドレスを参照してください。

`http://www.ietf.org`

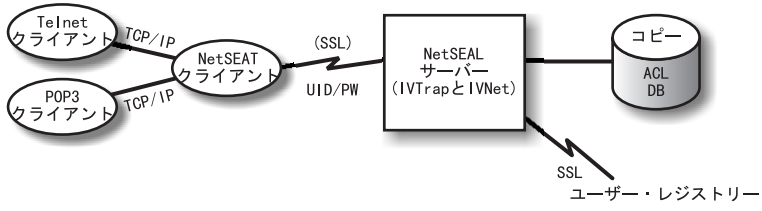
WebSEAL がユーザーの認証を正常に完了すると、WebSEAL は、ACL データベースのローカル・レプリカを使用して、このユーザーが、要求された通りに Web オブジェクトにアクセスする権限があるかどうかを判断します。

WebSEAL サーバーと、アクセスしようとする Web リソースが入っているバックエンド・サーバーとの間の接続が、グローバル・サインオン (GSO) ジャンクションである場合、 WebSEAL は、LDAP 内にそのジャンクションがあるかどうか、GSO クリデンシャルを検索し、Web サーバーにユーザー名とパスワードを渡します。

GSO リソースと GSO リソース・グループの管理については、 *Policy Director 管理の手引き* 内の管理コンソールの情報を参照してください。

保護された TCP/IP サーバーに NetSEAT クライアントを使用してユーザーがアクセスする場合

以下の図は、ユーザーが、NetSEAT クライアントを使用して、保護された TCP/IP サーバーにアクセスする場合のデータの流れを示しています。



Telnet クライアントを使用するユーザーは、NetSEAL によって保護されたサーバーに Telnet でログインし、このサーバーは、ユーザーがアクセスを要求していることを識別します。 NetSEAL は、ユーザー名とパスワードを要求し、ユーザー情報を提供し、その情報をユーザー・レジストリーに保管されている値と比較して、ユーザーの識別を確認します。 NetSEAL は、ユーザーが、指定されたポートを介してコンピューターにアクセスできるかどうかを検証します。

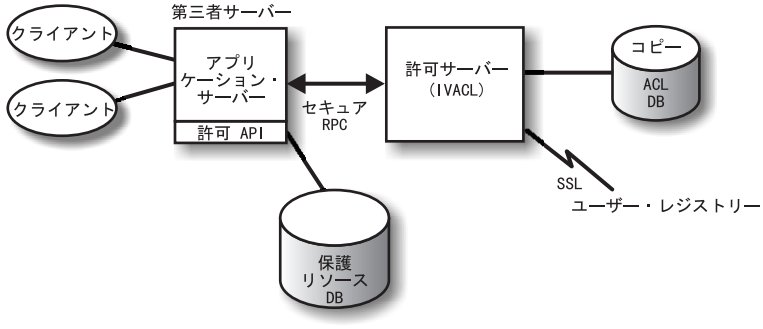
NetSEAT は、要求をセキュア Policy Director サーバーに透過的に転送し、セキュア SSL トンネルを通じて情報を送信します。 NetSEAT では、その構成情報を使用して、汎用 TCP/IP アプリケーション (Telnet、 POP3、または HTTP) からセキュア・サーバーに対する要求を認識します。 NetSEAT は、SSL を介した基本認証を使用して、NetSEAT ユーザーの識別とクリデンシャルを設定します。認証の設定後、セキュア SSL は、適用できるセキュリティー設定にしたがって要求トランザクションをカプセル化し、完了します。

たとえば、Web ブラウザーで、Policy Director セキュリティー・マネージャーによって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、それを該当するサーバーに経路

指定します。これが Policy Director への最初の要求であり、認証を必要とする場合、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。ユーザーが認証されると、Policy Director は、以後に情報が要求されるたびに、該当するクリデンシャルを透過的に付加します。このプロセスにより、Policy Director が管理するすべての Winsock アプリケーションに対する、シングル・サインオン環境が可能になります。さらに、Policy Director はこのクリデンシャルを使用して、ユーザーが、要求された Policy Director 保護リソースにアクセスできるかどうかを判別します。

保護された第三者サーバーにユーザーがアクセスする場合

以下の図は、保護された第三者サーバーにユーザーがアクセスする場合のデータの流れを示しています。



クライアントが、保護された第三者サーバー上の保護データにアクセスしようとすると、第三者サーバーがユーザーを認証し、そのユーザーを Policy Director ユーザーと対応付けます。アプリケーション・サーバーは、Policy Director ユーザー情報を許可サーバーに渡し、この許可サーバーが LDAP (または、ユーザー・レジストリーに使用される、 DCE などの別の製品) に連絡し、ユーザーのクリデンシャルを取り出します。次に、アプリケーション・サーバーは、クリデンシャル、ユーザーがアクセスしようとするオブジェクトの名前、およびユーザーが実行しようとする操作を許可サーバーに渡し、許可サーバーは、この操作が許可されているかどうかの指示を戻します。その後、アプリケーション・サーバーはこのアクセスを許可または拒否します。

Policy Director パッケージの内容

IBM SecureWay Policy Director 製品のバージョン 3.0 は、5 枚の CD に収められています。この CD の表題と内容が、以下の表に示されています。

CD の表題	内容
IBM SecureWay Policy Director Version 3.0	• IBM Policy Director バージョン 3.0
IBM SecureWay Policy Director Security Services	• IBM DCE for AIX バージョン 2.2 • IBM DCE for Windows NT バージョン 2.2 • Transarc DCE for Solaris バージョン 2.0
IBM SecureWay Directory Version 3.1.1 for AIX	• IBM SecureWay Directory バージョン 3.1.1 • IBM DB2 バージョン 5.2 (Fix Pack 7 付き) • IBM Global Security Kit SSL Runtime Toolkit バージョン 3.0.1 (GSKit)
IBM SecureWay Directory Version 3.1.1 for NT	• IBM SecureWay Directory バージョン 3.1.1 • IBM DB2 バージョン 5.2 (Fix Pack 7 付き) • IBM Global Security Kit SSL Runtime Toolkit バージョン 3.0.1 (GSKit)
IBM SecureWay Directory Version 3.1.1 for Solaris	• IBM SecureWay Directory バージョン 3.1.1 • IBM DB2 バージョン 5.2 (Fix Pack 8 付き) • IBM Global Security Kit SSL Runtime Toolkit バージョン 3.0.1 (GSKit)

第2章 システム要件

ご使用の操作環境は、以下の節で説明されているソフトウェアとハードウェアの要件を満たしている必要があります。システム要件の最新情報については、Policy Director の README ファイルを参照してください。 README ファイルには、製品資料に優先する情報が記載されています。

最新の README ファイルを入手するには、以下の IBM SecureWay Policy Director Web サイトのライブラリー・ページにアクセスしてください。

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

Policy Director DCE、LDAP、NetSEAT、およびサーバー構成要素をインストールする前に、必ず、以下の節にリストされている、必要なハードウェアとソフトウェアを用意しておいてください。

ハードウェア要件

メモリー使用量、バッファーとキャッシュの管理、および制御構造は、容易に拡張できます。ただし、基本オペレーティング・システムの基本要件、前提となる DCE と LDAP クライアントの要件、およびクライアント・アプリケーションの要件では、設定に必要な最小限のディスク・スペースとメモリーの要件を示しています。

Policy Director サーバーのハードウェア要件は、以下のとおりです。

プラットフォーム	最小ディスク・スペース	最小メモリー
Intel または Intel と互換性のある 80486 133 MHz 以上を備えた、Windows NT サーバー	16MB	64MB
AIX 4.3.1 を実行するハードウェアを備えた AIX サーバー	16MB	64MB
Solaris 2.6 を実行するハードウェアを備えた Solaris サーバー	16MB	64MB

Policy Director クライアントのハードウェア要件は、以下のとおりです。

プラットフォーム	最小ディスク・スペース	最小メモリー

Intel または Intel と互換性のある 80486 133 MHz 以上を備えた、Windows NT クライアント	16MB	32MB
AIX 4.3.1 を実行するハードウェアを備えた AIX サーバー	16MB	32MB
Solaris 2.6 を実行するハードウェアを備えた Solaris サーバー	16MB	24MB

ソフトウェア要件

Policy Director のインストールを計画する場合、必ず、以下の節に示されている、正しいバージョンのオペレーティング・システムと前提となるその他のソフトウェアを用意しておいてください。 Policy Director サーバー、NetSEAT クライアント、および管理コンソール用のオペレーティング・システムの要件は、以下のとおりです。

Policy Director サーバー

Policy Director サーバーは、以下のオペレーティング・システムにインストールできます。

- Service Pack 4 を備えた Windows NT サーバーのバージョン 4.0 以上
- AIX バージョン 4.3.1 以上
- Sun Solaris バージョン 2.6

NetSEAT クライアント

Policy Director NetSEAT クライアントは、以下のオペレーティング・システムにインストールできます。

- Service Pack 4 を備えた Windows NT バージョン 4.0 以上
- Windows 98
- Windows 95

管理コンソール

Policy Director 管理コンソールは、以下のオペレーティング・システムにインストールできます。

- Service Pack 4 を備えた Windows NT サーバー、バージョン 4.0 以上
- Windows NT、Windows 95、または Windows 98
- AIX バージョン 4.3.1 以上、(Java Runtime 1.1.6 以上を含む)
- Sun Solaris バージョン 2.6

その他のソフトウェア要件

Policy Director には、DCE サーバー (LDAP をユーザー・レジストリーとして使用する場合) と LDAP サーバーが必要です。 1 つのサーバー (LDAP または DCE) が、セキュア・ドメイン内の少なくとも 1 つのコンピューター上に存在していなければなりません。 DCE および LDAP のクライアントとサーバーは、Policy Director 製品の一部として提供されます。これらをインストールしてから、Policy Director をインストールするか、または正しいレベルの既存の DCE および LDAP のインストールを使用できます。

Windows NT および AIX

Windows NT および AIX プラットフォーム上では、Policy Director サーバーに、以下のソフトウェアが必要です。

- Windows NT サーバー用の IBM DCE for Windows NT バージョン 2.2 以上、または AIX サーバー用の IBM DCE for AIX バージョン 2.2 以上
- DB2® バージョン 5.2 と Fix Pack 7 が組み込まれている、IBM SecureWay Directory バージョン 3.1.1 (LDAP)。LDAP が必要なのは、LDAP をユーザー・レジストリーとして使用する場合だけです。
- セキュア・ソケット・レイヤー (SSL) バージョン 3.0 以上
- Policy Director クリデンシャル取得サービス (CAS) と WebSEAL には、以下の Web ブラウザーのいずれか 1 つが必要です。
  - Microsoft Internet Explorer バージョン 4 以上
  - Netscape Communicator バージョン 4.5 以上
  - Netscape Navigator バージョン 4.5 以上
- Windows 95 の Policy Director クライアントの場合だけ、Winsock バージョン 2.0 以上が必要です。

Solaris

Solaris プラットフォームでは、Policy Director サーバーに、以下のソフトウェアが必要です。

- Transarc DCE バージョン 2.0
- DB2 バージョン 5.2 と Fix Pack 8 が組み込まれている、 IBM SecureWay Directory (LDAP) バージョン 3.1.1。LDAP が必要なのは、LDAP をユーザー・レジストリーとして使用する場合だけです。
- セキュア・ソケット・レイヤー (SSL) バージョン 3.0 以上

- Policy Director CAS と WebSEAL には、以下の Web ブラウザーのいずれか 1 つが必要です。
  - Microsoft Internet Explorer バージョン 4 以上
  - Netscape Communicator バージョン 4.5 以上
  - Netscape Navigator バージョン 4.5 以上

第3章 Policy Director の計画

以下の節では、Policy Director のインストールと構成を準備し、計画するために必要な情報を記載しています。インストールを計画する前に、1ページの『第1章 Policy Director の概要』を読んで、どの Policy Director 構成要素が必要かを決定しておいてください。

一般的な構成

この節で示されている構成は、ご使用のネットワークに適した構成を決定するのに役立ちます。20ページの『一般的な構成に必要な構成要素』の表を使用して、構成に必要な構成要素を決定してください。次に、Policy Director のインストール時にこれらの構成要素を選択します。WebSEAL と NetSEAL は、どのコンピューターにもインストールできることに注意してください。一般的な Policy Director 構成要素の構成が、以下に示されています。

管理サーバーのみ

セキュア・ドメインに対して管理サーバーの 1 つのインスタンスを実行するサーバー。このシナリオでは、管理サーバーはそれ自体のシステムに単独で置かれます。管理サーバーは、セキュア・ドメインのマスター許可データベースを維持管理し、セキュア・ドメイン全体でこのデータベースを複写し、セキュア・ドメイン内の他の Policy Director サーバー・コンピューターについての位置情報を維持管理します。

WebSEAL サーバーを備えたセキュリティー・マネージャー

セキュリティー・マネージャー (IVNet) と WebSEAL (IVWeb) という 2 つの構成要素が WebSEAL を構成します。 WebSEAL サーバーは、Web スペースを保護します。 WebSEAL は、スマート・ジャンクション またはジャンクションを通じて、高可用性と耐障害性を保つためにバックエンド・サーバーをサポートします。

NetSEAL サーバーを備えたセキュリティー・マネージャー

セキュリティー・マネージャー (IVNet) と NetSEAL (IVTrap) という 2 つの構成要素が NetSEAL を構成します。 NetSEAL サーバーは、仮想私設網 (VPN) を保護し、既存のネットワーク・サービスと第三者ネットワーク・サービスに対するアクセス制御を提供します。

WebSEAL と NetSEAL サーバーを備えたセキュリティー・マネージャー
WebSEAL と NetSEAL サーバーの組み合わせ。

許可サーバー
Policy Director 許可 API を使用して、第三者アプリケーション用の Policy Director 許可サービスへのアクセスを提供するサーバー。

許可サーバーと ADK
許可サービスの呼び出しに Policy Director 許可 API を使用する第三者アプリケーションを構築しようとする開発者に、開発環境を提供するサーバー。

管理コンソール
Policy Director セキュア・ドメイン用のセキュリティー・ポリシーの管理に使用される、Java ベースのグラフィカル・アプリケーション。IVBase は、Windows の管理コンソールには必要ありません。

すべての構成要素
上記のすべての構成のサービスを結合して提供するサーバー。

一般的な構成に必要な構成要素

19ページの『一般的な構成』に記載されている Policy Director 構成が、以下の表にリストされています。この表は、各構成にどの構成要素をインストールする必要があるかを示しています。左から右の順に、構成要素が、正しいインストール順序で表示されています。

WebSEAL と NetSEAL のどちらも、2 つの構成要素で構成されていることに注意してください。

WebSEAL セキュリティー・マネージャー (IVNet) と WebSEAL (IVWeb)

NetSEAL セキュリティー・マネージャー (IVNet) と NetSEAL (IVTrap)

IVBase に対する注:

- IVBase は、Windows の管理コンソールには必要ありません。
- IV.Smit は、AIX では、IV.Base と一緒に自動的にインストールされます。

シナリオ	インストール・パッケージ							
	IVBase	IVMgr	IVNet	IVWeb	IVTrap	IVAcld	IVAuthADK	IVConsole
管理サーバーのみの 1 つのインスタンス	X	X						
WebSEAL を備えたセキュリティー・マネージャー	X	X***	X	X				
NetSEAL を備えたセキュリティー・マネージャー	X	X***	X		X			
WebSEAL と NetSEAL サーバーを備えたセキュリティー・マネージャー	X	X***	X	X	X			
許可サーバー	X	X***				X		
許可サーバーと ADK	X	X***				X	X	
管理コンソール	X							X
すべての構成要素	X	X***	X	X	X	X	X	X

*** これがセキュア・ドメイン内の最初または唯一のコンピューターである場合、管理サーバー (IVMgr) をインストールする必要があります。これが、既存の管理サーバーを備えた既存のセキュア・ドメイン内に追加するコンピューターである場合、別の管理サーバーをインストールしてはなりません。どのセキュア・ドメインでも、管理サーバーは 1 つだけでなければなりません。

インストールの前に必要な情報

Policy Director のインストールを開始する前に、Policy Director ソフトウェアのインストールに必要なシステム情報をメモしておいてください。

Policy Director サーバー

- セル管理者 (cell_admin) のユーザー名
- セル管理者 (cell_admin) のパスワード
- WebSEAL: HTTP ポート (デフォルト)
- WebSEAL: Web 文書のルート・ディレクトリー

NetSEAT クライアント (Windows のみ)

- セル名
- セキュリティー・サーバー・ホスト名
- タイム・サーバー・ホスト名
- ディレクトリー・サービス・ブローカー・ホスト名

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、以下のプロトコルをサポートします。

- セキュア・ソケット・レイヤー (SSL) トンネル伝送
- 汎用セキュリティー・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提供される、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 での保全性とタイム・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・ハッキングが発生するのは、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間で流れる間に取り込まれた場合です。次に、そのデータは、再生されるか、またはその最初のユーザーの偽名を使用する手段としてサーバーに戻されます。

SSL トンネル伝送: SSL プロトコルでは、2 つのワークステーション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 では、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、SSL を使用可能にします。この構成は、NetSEAT クライアントが、特定のポート (たとえば、Telnet が使用するポート) を保護する 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 のバージョン 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、Microsoft® Windows NT® 用の Policy Director 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てください。

GSS トンネル伝送は、一般的な方法で呼び出し側にセキュリティー・サービスを提供します。基本となるさまざまなメカニズムとテクノロジーを使用してサポートできます。これを使用すると、さまざまな環境に対して、ソース・レベルでアプリケーションを移植することが可能になります。 GSS トンネル伝送により、両方向に移動するトラフィック上で、それぞれの方向が独立して保護レベルを制御できます。たとえば、クライアントからサーバーに移動するデータはバルク・データ暗号化で完全に保護するが、サーバーからクライアントに移動するデータは保護しないようにすることが可能です。

セキュア・ドメインのインストール要件

Policy Director は、1 つまたは複数のコンピューターに、さまざまな設定で構成要素をインストールできる、高度に分散されたセキュリティー・システムです。以下に、セキュア・ドメインでインストールする必要がある構成要素を示します。

- DCE サービス
- ユーザー・レジストリー。(IBM SecureWay Directory が必要なのは、LDAP をユーザー・レジストリーとして使用する場合だけです)
- Policy Director サーバー
- Policy Director 管理コンソール
- Policy Director 許可 ADK

DCE または LDAP の既存のインストールを使用しようとする場合には、必ず、既存のインストールが正しいレベルであることを確認してください。正しいレベルについては、17ページの『その他のソフトウェア要件』を参照してください。 Policy Director 製品をインストールする前に、以下の依存関係を確認してください。

分散コンピューティング環境サービス

各 Policy Director セキュア・ドメイン (DCE セル) には、Policy Director サーバー間の通信を保護するために、少なくとも 1 つのコンピューターに、完全な DCE サービスをインストールする必要があります。 DCE サービスは、Policy Director サーバーと同じホストに置くか、またはネットワークのリモート・ホストに置くことができます。

DCE のインストールについては、必要なプラットフォームのインストールと管理に関する解説書とテクニカル・サポートのリソースを参照してください。DCE 資料のリストについては、98ページの『IBM 分散コンピューティング環境の資料』を参照してください。

DCE をインストールする際には、以下のガイドラインを使用してください。

- 1 つのホスト・システムに新しい Policy Director セキュア・ドメインを作成しようとする場合、DCE サーバーの完全インストールを行ってください。
- DCE サーバーがリモート・ホストに置かれている場合は、ローカル・ホストに Policy Director をインストールして、新しいセキュア・ドメインを作成してください。
- 既存の Policy Director セキュア・ドメイン内に Windows NT 用の Policy Director をインストールしようとする場合は、NetSEAT クライアントを使用して、必要な DCE サービスへのアクセスを提供してください。 Windows NT サーバー用の Policy Director と同じホストに NetSEAT クライアントをインストールしてください。

ユーザー・レジストリー

Policy Director は、そのユーザー・レジストリーとして、IBM SecureWay Directory (LDAP) ユーザー・レジストリーでも、DCE ユーザー・レジストリーでも使用することができます。

ユーザー・レジストリーとして LDAP を使用する場合、Policy Director をインストールする前に、LDAP サーバーをインストールして、構成しておく必要があります。また、各 Policy Director コンピューターに LDAP クライアントをインストールしておく必要もあります。

LDAP のインストールについては、*IBM SecureWay Directory Installation and Configuration, Version 3.1.1* を参照してください。この LDAP 資料がどの CD に入っているかは、100ページの『IBM SecureWay Directory の資料』を参照してください。

または、DCE のインストールについては、98ページの『IBM 分散コンピューティング環境の資料』にリストされている DCE 製品情報を参照してください。

Policy Director サーバー

Policy Director サーバーのインストールには、以下の要件が適用されます。

- 正しく通信するために、すべての Policy Director Windows NT サーバーには、Policy Director NetSEAT クライアントが必要です。
- Policy Director サーバーのすべてのインストールには基本構成要素が必要であり、これは自動的にインストールされます。
- セキュア・ドメインに*初めて* または*唯一* のコンピューターをインストールしようとする場合には、そのコンピューターに管理サーバーをインストールする必要があります。
- 既存の管理サーバーを持つ既存のセキュア・ドメイン内にコンピューターを*追加* してインストールしようとする場合は、別の管理サーバーをインストールしないでください。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。
- WebSEAL、NetSEAL、および第三者許可サーバーの構成要素は、任意選択です。
- セキュリティー・マネージャーは、WebSEAL と組み合わせて WebSEAL HTTP サーバー構成要素と密な HTTP アクセス制御を提供し、NetSEAL と組み合わせて NetSEAL の粗い TCP/IP アクセス制御構成要素を提供します。
- AIX および Solaris 上のすべての Policy Director サーバーには、完全な DCE クライアントが必要であり、LDAP をユーザー・レジストリーとして使用する場合は、LDAP クライアントも必要です。

管理コンソール

管理コンソールには、セキュア・ドメインと管理サーバーをインストールし、構成する必要があります。また、管理コンソールには DCE クライアントも必要であり、Windows コンピューター上に管理コンソールがある場合は、NetSEAT クライアントも必要です。

許可 ADK

アプリケーション開発コンピューターに Policy Director 許可 ADK をインストールしてください。許可 ADK を使用すると、保護されている第三者サーバーにユーザーがアクセスできるようにするアプリケーションを開発することができます。許可 ADK には基本構成要素が必要であり、この基本構成要素は、許可 ADK のインストール時に自動的にインストールされます。

アプリケーションが実行されるセキュア・ドメインでは、少なくとも 1 つのコンピューターに許可サーバーをインストールする必要があります。通常の開発環境では、許可 ADK と同じシステムに許可サーバーを組み込みます。

ステップごとの Policy Director インストールの概要

Policy Director のインストールには、以下のステップが必要です。

1. 旧バージョンの IBM SecureWay Policy Director がインストールされているときに、そのインストール・システムを移行したい場合は、Policy Director の Web ページにある移行情報を参照します (viiiページの『Web 情報』を参照)。
2. ご使用のオペレーティング・システムが Policy Director をサポートしていることを確認します。

   サポートされているオペレーティング・システムについては、16ページの『Policy Director サーバー』 を参照してください。
3. どのサーバー構成要素が要件に最もよく適合しているか、およびこれらの構成要素をどのコンピューターにインストールするかを決定します。

   19ページの『一般的な構成』を参照してください。
4. セキュア・ドメインが SSL トンネル伝送を使用するのか、または GSS トンネル伝送を使用するのかを決定します。

   詳しくは、22ページの『トンネル・メカニズム』を参照してください。
5. DCE インフラストラクチャーが存在していない場合は、それをインストールし、構成します。

   必要な DCE サービスについては、23ページの『分散コンピューティング環境サービス』を参照してください。
6. セキュア・ドメインで、LDAP ユーザー・レジストリーを使用するのか、または DCE ユーザー・レジストリーを使用するのかを決定します。ユーザー・レジストリーに IBM SecureWay Directory (LDAP) を使用し、既存の LDAP は使用しないという場合は、LDAP をインストールし、構成してください。

   LDAP のインストールについては、29ページの『第4章 IBM SecureWay Directory のインストールと構成』を参照してください。
7. Policy Director サーバーに使用する DCE および LDAP クライアントをコンピューターにインストールします。

   DCE のインストールについては、98ページの『IBM 分散コンピューティング環境の資料』にリストされている DCE 製品情報を参照してください。
8. Policy Director サーバー構成要素をインストールします。

   使用するオペレーティング・システム・プラットフォームについては、インストールの章を参照してください。以下のいずれかを参照してください。

- 47ページの『第5章 Policy Director (Windows 用) のインストール』
- 63ページの『第6章 Policy Director (AIX 用) のインストール』
- 81ページの『第7章 Policy Director (Solaris 用) のインストール』

9. クライアント証明書の認証に Policy Director CAS を使用する場合は、Policy Director クリデンシャル取得サービス (CAS) を構成します。

   Policy Director CAS については、『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。

10. 管理コンソールをインストールします。

    使用するオペレーティング・システム・プラットフォームについては、インストールの章を参照してください。以下のいずれかを参照してください。

    - Windows NT の場合、57ページの『Windows での管理コンソールのインストール』を参照してください。
    - AIX では、DCE ユーザー・レジストリーを使用する場合は 77ページの『管理コンソールのインストール』を参照し、LDAP ユーザー・レジストリーを使用する場合は 68ページの『管理コンソールの構成と始動』を参照してください。
    - Solaris の場合、93ページの『管理コンソールのインストール』を参照してください。

Policy Director の再インストール

パッケージを再インストールする必要がある場合、まず最初に既存のパッケージを削除してから、必要なパッケージを再インストールしてください。その方法については、78ページの『Policy Director の削除』を参照してください。

クリデンシャル取得サービスの構成

Policy Director クリデンシャル取得サービス (CAS) は、カスタマイズ可能な Policy Director の構成要素の 1 つであり、WebSEAL でサポートされている標準の認証メカニズムを拡張するために使用することができます。

Policy Director CAS は自動的にインストールされます。 Policy Director CAS をクリデンシャル取得サービスとして使用したい場合は、それを構成する必要があります。Policy Director CAS の概要と構成については、*Policy Director 管理の手引き* の第 2 章と第 13 章を参照してください。

第4章 IBM SecureWay Directory のインストールと構成

DCE ユーザー・レジストリーの使用を計画している場合は、IBM SecureWay Directory (LDAP) のインストールと構成の際に、この節を飛ばすことができます。

Policy Director のインストール時に、LDAP ユーザー・レジストリーか、DCE ユーザー・レジストリーのどちらを選択するかが尋ねられます。

- LDAP を選択する場合は、Policy Director をインストールする前に、IBM SecureWay Directory バージョン 3.1.1 (LDAP) Client SDK とサーバーをインストールしてから、LDAP サーバーを構成しておく必要があります。
- LDAP サーバーへのアクセスに SSL を使用する場合は、LDAP クライアントも構成する必要があります。

LDAP サーバーとクライアントのインストール

ユーザー・レジストリーとして LDAP を使用しようとする場合、Policy Director に LDAP サーバーとクライアントが必要です。

LDAP サーバーは、セキュア・ドメイン内の少なくとも 1 つのコンピューターに存在していなければなりません。LDAP クライアントとサーバーは、Policy Director 製品の一部として提供されます。これらをインストールしてから、Policy Director をインストールする必要があります。または、正しいレベルの既存の LDAP のインストールを使用することもできます。

LDAP のインストール時に、**SecureWay Directory および Client SDK** をインストールすることを選択してください。

LDAP のインストールと構成の詳細については、*IBM SecureWay Directory Installation and Configuration, Version 3.1.1* を参照してください。サポートされるオペレーティング・システムごとに、該当する CD 上に HTML 形式で本書の別のバージョンが収められています。文書のアクセス方法については、100 ページの『IBM SecureWay Directory の資料』を参照してください。

LDAP クライアントのみのインストール

ユーザー・レジストリーとして LDAP を使用する場合は、Policy Director を実行する各システムに LDAP クライアントをインストールする必要があります。 LDAP クライアントは、Policy Director 製品の一部として提供されます。LDAP クライアントをインストールしてから、Policy Director をインストールしてください。

Policy Director 用にすでに正しいレベルでインストールされ、構成されている既存の LDAP サーバーがある場合だけ、LDAP のインストール時に、**SecureWay Client SDK** をインストールすることを選択してください。

LDAP サーバーの構成

ユーザー・レジストリーとして LDAP を使用する場合は、最初の Policy Director サーバーをインストールする前に、LDAP サーバーを構成しておく必要があります。最初の Policy Director システムで LDAP サーバーを構成した後は、Policy Director サーバーを追加するときには、LDAP サーバーを再構成する必要はありません。

LDAP サーバーの構成時に LDAP サーバーへの SSL アクセスを使用可能にした場合、SSL アクセスを使用するコンピューターを追加するごとに、そのコンピューターにクライアントとサーバーのキー・リングのペアをコピーする必要があります。詳しくは、34ページの『SSL アクセスの使用可能化 (任意選択)』を参照してください。

LDAP サーバーを構成するには、セキュア・ドメインごとに 1 回だけ、以下に挙げる構成ステップを実行する必要があります。

1. 必要なサフィックスを追加する。その方法については、31ページの『サフィックスの追加』を参照してください。
2. セキュリティー・スキーマのオブジェクトと属性をインストールする。 32ページの『セキュリティー・スキーマのオブジェクトと属性のインストール』を参照してください。
3. LDAP アクセス制御を使用可能にする。その方法については、44ページの『LDAP アクセス制御の使用可能化』を参照してください。
4. SSL アクセスを使用可能にする。その方法については、34ページの『SSL アクセスの使用可能化 (任意選択)』を参照してください。

SSL アクセスを使用可能にした場合、LDAP サーバーへのアクセスに SSL を使用する LDAP クライアント (Policy Director サーバー) を追加するたびに、40ページの『SSL アクセス用の LDAP クライアントのセットアップ』のステップを実行してください。

注: LDAP 管理者は、LDAP データベースにパスワード暗号化の設定を指定できます。LDAP では、暗号化されていない通常のテキストとしてパスワードを保管することが許されるため、セキュリティー上のリスクになる可能性があります。ユーザー・パスワードの属性を適切な暗号化レベルに設定する方法については、ご使用の LDAP の資料を参照してください。

サフィックスの追加

IBM SecureWay Directory で、以下のステップを実行して新しいサフィックスを作成してください。

1. Web ブラウザーを使用して、以下の Web アドレスにある IBM SecureWay Directory サーバー Web 管理ツールにアクセスする。

   ```
   http://servername/ldap
   ```

   Web インターフェースを通じて LDAP 管理者 (たとえば、`cn=root`) としてログインしてください。
2. 「**Suffixes → Add a suffix**」をクリックする。
3. 「**Suffix DN**」フィールドに、以下のサフィックスを追加する。

   ```
   secAuthority=Default
   ```

   `secAuthority=Default` のオブジェクトが、管理サーバーの構成時に作成されます。
4. 「**Add a new suffix**」ボタンをクリックする。
5. 別のサフィックスを追加する場合には、「**Add a suffix**」リンクをクリックして、直前のウィンドウに戻る。
6. 必要に応じて、Policy Director ユーザーとグローバル・サインオン (GSO) データ用のサフィックスを追加する。たとえば、以下のようにします。

   ```
   o=IBM,c=US
   ```

   ご使用のインストール・システムに適した名前をサフィックスに指定できます。この場合、 `o=` は所属組織の省略名であり、`c=` は国名です。

   このステップでは、GSO データ用およびユーザーとグループ用のサフィックスを作成します。これらのサフィックスは、LDAP Web 管理ツールを使用して作成されます。

7. 「**Add a new suffix**」ボタンをクリックする。
8. 組織に必要な新しいサフィックスを追加するごとに、この手順を繰り返す。
9. サフィックスの追加が完了したら、現行の LDAP 管理ツール Web ページ上で「**restart the server**」リンクをクリックして、LDAP サーバーを再始動する。

セキュリティー・スキーマのオブジェクトと属性のインストール

Policy Director は、1 組の LDAP オブジェクトと属性を使用して、LDAP サーバー内でユーザー・クリデンシャルを維持管理します。

セキュリティー・オブジェクトと属性がインストールされているかどうかを判別するには、IBM SecureWay Directory Management Tool (DMT) を使用します。まだ存在しない場合は、インストールしてください。 DMT は、IBM SecureWay Directory パッケージの一部としてインストールされます。

Policy Director セキュリティーのオブジェクトと属性がインストールされているかどうかを判別するには、以下のステップを実行してください。

1. Directory Management Tool を LDAP クライアント上で始動する。

   注: secAuthority=Default サフィックスの項目がないというメッセージが表示されても、問題なく先に進めます。 secAuthority=Default サフィックスのオブジェクトは、管理サーバーの構成時に作成されます。
2. 「**Schema → Object classes → View object classes**」をクリックする。
3. 以下の Policy Director オブジェクトと属性がすべて存在するかどうかを検証する。

   オブジェクト・クラス
   secAuthorityInfo
   secGroup
   secMap
   secPolicy
   secPolicyData
   secUser
4. 「**Schema → Attributes → View attributes**」をクリックする。
5. 以下の Policy Director オブジェクトと属性がすべて存在するかどうかを検証する。

   属性
   secUUID

secLoginType
secAuthority
secAcctValid
secPwdValid
secDN
secPwdMgmtBind
secAcctExpires
secAcctInactivity
secAcctLife
secPwdAlpha
secPwdSpaces
secPwdFailures
secPwdLastChanged
secPwdLastUsed

6. 32ページのステップ 3 と 32ページのステップ 5 の結果に基づいて、以下のいずれか 1 つを実行する。
   - すべてのオブジェクトが存在する場合、それ以上の処置は必要ありません。 34ページの『SSL アクセスの使用可能化 (任意選択)』に進みます。
   - オブジェクトの全部ではなく、一部 しか存在しない場合は、ステップ 7 に進みます。
   - オブジェクトがまったくない 場合は、ステップ 8 に進みます。
7. Policy Director オブジェクトと属性の全部ではなく、一部しかない場合、既存の Policy Director オブジェクトと属性を削除する。

   DMT 内で以下のようにクリックして、オブジェクト・クラスを削除します。

   「**Schema → Object classes → Delete object classes**」

   次に、「**Schema → Attributes → Delete attributes**」をクリックして、属性を削除します。
8. Policy Director オブジェクトと属性がまったくない場合は、 *IBM SecureWay Policy Director Version 3.0* CD を挿入する。
9. コマンド・プロンプトで、**ldapmodify** を使用してスキーマ・ファイルをロードする。たとえば、以下のように入力します。

   UNIX:

   ```
   ldapmodify -h hostname -p 389 -D cn=root -w password -f /schema/secschema.def
   ```

   Windows:

   ```
   ldapmodify -h hostname -p 389 -D cn=root -w password -f x:¥schema¥secschema.def
   ```

ここでは、*x:* は、ご使用の Windows CD-ROM ドライブのドライブ名です。

10. Policy Director を使用して SecureWay Boundary Server ユーザーの管理を計画している場合、Policy Director スキーマ・ファイルからオブジェクトと属性も追加する。

    コマンド・プロンプトで **ldapmodify** コマンドを使用して、スキーマ・ファイルをロードします。たとえば、以下のように入力します。

    Windows:

    ```
    ldapmodify -h hostname -p 389 -D cn=root -w password -f x:¥schema¥puschema.def
    ```

    UNIX:

    ```
    ldapmodify -h hostname -p 389 -D cn=root -w password -f /schema/puschema.def
    ```

    ここで、*x:* は、ご使用の CD-ROM ドライブのドライブ名です。

SSL アクセスの使用可能化 (任意選択)

LDAP サーバーへの SSL アクセスが必要ない場合は、この節を飛ばして、 44 ページの『LDAP アクセス制御の使用可能化』に進んでください。

LDAP サーバーに SSL アクセスが必要な場合は、この節を続行してください。この手順は、LDAP サーバーと LDAP クライアント間で初めて SSL 通信を設定する場合だけ実行する必要があります。

Policy Director サーバーと LDAP サーバー間の通信を保護するために、任意選択で SSL の使用を可能にすることができます。

IBM Global Security Kit (GSKit) SSL Runtime Toolkit バージョン 3.0.1 は、LDAP のインストール時にインストールされます。 GSKit は、2 つのバージョンのキー管理ツールを備えています。1 つのバージョンは、ウィンドウ化バージョン **ikmguiw** であり、もう 1 つのバージョンは、非ウィンドウ化バージョン **ikmgui** です。以下の手順で **ikmguiw** が呼び出されるときには、どちらのバージョンでも使用できます。

このツールの使用法の詳細な指示は、LDAP の資料の中にあります。 100ページの『IBM SecureWay Directory の資料』を参照してください。

または、以下の縮約された手順を実行して、Policy Director の SSL アクセスを具体的に使用可能にすることができます。

キー・データベース・ファイルと証明書の作成

LDAP サーバーで SSL サポートを使用可能にするには、このサーバーで、証明書 (このサーバーを識別し、*個人用証明書* として使用できるもの) が必要です。この個人用証明書は、クライアントがサーバーを認証できるようにするためにサーバーがクライアントに送信する証明書です。この証明書および公開キーと秘密キーのペアは、キー・データベース・ファイル内に保管されます。顧客は通常、たとえば VeriSign などの認証局 (CA) から*署名入り証明書* を入手します。

ただし、*自己署名入り* 証明書を使用することもできます。自己署名入り証明書を使用する場合、その証明書が生成されるマシンが、CA になります。

キー・データベース・ファイルと証明書の作成には、GSKit のキー管理ツール (**ikmguiw**) を使用します。キー・データベース・ファイルと証明書 (自己署名入り、または署名入り) を作成するには、以下のステップを実行します。

1. IBM Global Security Kit (GSKit) SSL Runtime Toolkit バージョン 3.0.1 および Java ベースのキー管理ツールが、LDAP サーバーと、SSL を使用するすべての LDAP クライアントの両方にインストールされていることを確認する。

   Windows: `C:¥Program Files¥IBM¥GSK¥bin¥ikmguiw.exe`

   Solaris: `/opt/IBM/GSK/bin/ikmguiw`

   AIX: `/usr/lpp/ibm/gsk/bin/ikmguiw`
2. IBM キー管理ツール (**ikmguiw**) を始動する。
3. 「**Key Database File → New**」をクリックする。
4. 「**CMS key database file**」が、キー・データベース・タイプとして選択されていることを確認する。
5. キー・データベース・ファイルを入れたい場所の情報を「**File Name**」と「**Location**」フィールドに入力する。キー・データベース・ファイルの拡張子は *.kdb* です。
6. 「**OK**」をクリックする。
7. キー・データベース・ファイルのパスワードを入力し、それを確認する。

   キー・データベース・ファイルを編集する際に必要なので、このパスワードを覚えておいてください。
8. デフォルトの有効期限を受け入れるか、または所属組織の要件に応じて変更する。
9. パスワードをマスクし、stash ファイルに保管したい場合は、「**Stash the password to a file**」をクリックする。

stash ファイルは、一部のアプリケーションで使用でき、アプリケーションでパスワードを知らなくても、キー・データベース・ファイルを使用できるようにします。 stash ファイルの位置と名前は、キー・データベース・ファイルと同であり、拡張子は *.sth* です。

10. 「**OK**」をクリックする。

これで、キー・データベース・ファイルの作成が完了しました。 1 組のデフォルトの署名者証明があります。これらの署名者証明は、認識されるデフォルトの認証局になります。

個人用証明書の作成

認証局 (たとえば、VeriSign) からの証明書を使用しようとする場合は、認証局 (CA) に証明書を要求し、証明書の完成後に受け取る必要があります。 『証明書の受け取り』内のステップを実行してください。

証明書の受け取り: 自己署名入り証明書ではなく、認証局 (たとえば VeriSign) からの証明書を使用しようとする場合は、以下のステップを実行してください。

1. **ikmguiw** を使用して、CA に証明書を要求してから、新しい証明書を受け取り、キー・データベース・ファイルに入れる。
2. キー・データベース・ファイルの「**Personal Certificate Requests**」セクションをクリックする。
3. 「**New**」をクリックする。
4. すべての情報を指定して、認証局に送信する要求を作成する。
5. 「**OK**」をクリックする。
6. CA が証明書を戻した後、「**Personal Certificates**」セクションをクリックしてから、「**Receive**」をクリックして、キー・データベース・ファイルに証明書を入れる。
7. LDAP サーバーの証明書をキー・データベース・ファイルに入れた後、LDAP サーバーを構成して、SSL を使用可能にする。

証明書がまだ認識されていない場合は、CA の証明書をクライアント・マシンにコピーしてください。

証明書が、すでに認識されている CA (たとえば VeriSign) によって生成される場合、それ以上の処置は必要ありません。 38ページの『SSL を使用可能にするための LDAP サーバーの構成』に進みます。

自己署名入り証明書の作成: 自己署名入り証明書ではなく、認証局 (たとえば、VeriSign) からの証明書を使用する計画の場合は、36ページの『証明書の受け取り』のステップを実行してください。

新しい自己署名入り証明書を作成し、それをキー・データベース・ファイルに保管するには、以下のステップを実行します。

1. 「**Create → New Self-Signed Certificate**」をクリックする。
2. 「**Key Label**」フィールドに、キー・データベース内のこの新しい証明書を識別するために GSKit が使用できる名前を入力する。

   たとえば、ラベルは、LDAP サーバーのマシン名にすることができます。
3. 「**Version**」フィールドのデフォルト (X509 V3) および「**Key Size**」フィールドのデフォルトを受け入れる。
4. デフォルトのマシン名を受け入れるか、またはこの証明書用の「**Common Name**」フィールドに別の識別名を入力する。
5. 「**Organization**」フィールドに企業名を入力する。
6. オプション・フィールドに入力するか、ブランクのままにしておく。
7. 「**Country**」フィールドのデフォルトおよび「**Validity Period**」フィールドの 365 を受け入れるか、または所属企業の要件に合わせてそれらのフィールドを変更する。
8. 「**OK**」をクリックする。

   GSKit は、新しい公開キーと秘密キーのペアを生成し、証明書を作成します。

   キー・データベース・ファイル内に複数の証明書がある場合、GSKit は、このキーをデータベースのデフォルトのキーにしたいかどうかを照会します。これらのいずれか 1 つをデフォルトとして受け入れることができます。どの証明書を使用するかを選択するためのラベルが指定されていない場合は、デフォルトの証明書が実行時に使用されます。

これで、LDAP サーバーの個人用証明書の作成が完了しました。この証明書は、キー・データベース・ファイルの Personal Certificates セクションに表示されているはずです。キー・データベース・ファイル内に保持されている証明書のタイプを選択するには、キー管理ツールの真ん中のバーを使用してください。

次に、LDAP サーバーの証明書を Base64 コード化 ASCII データ・ファイルに取り出す必要があります。

自己署名入り証明書の取り出し

証明書が自己署名されている場合、キー・データベース・ファイルから署名者証明を取り出す必要があります。以下の取り出し手順を続けてください。

ここで取り出されたものは、クライアント・マシンのセットアップに使用されます。 37ページの『自己署名入り証明書の作成』で自己署名入り証明書を作成した場合は、キー・データベース・ファイルの Signer Certificates セクションにも表示されます。これは、自己署名入り証明書であるからです。キー・データベースの Signer Certificates セクションに表示されている場合は、新しい証明書が存在することを確認してください。

署名者証明を取り出すには、以下の手順を実行します。

1. **ikmguiw** を使用して、LDAP サーバーの証明書を Base64 コード化 ASCII データ・ファイルに取り出す。このファイルは、40ページの『SSL アクセス用の LDAP クライアントのセットアップ』の手順で使用されます。
2. 37ページの『自己署名入り証明書の作成』で追加したばかりの自己署名入り証明書を強調表示する。
3. 「**Extract Certificate**」をクリックする。
4. データ・タイプとして「**Base64-encoded ASCII data**」をクリックする。
5. 新たに取り出された証明書に証明書ファイル名を入力する。証明書ファイルの拡張子は *.arm* です。
6. 取り出された証明書を保管しておきたい位置を入力する。
7. 「**OK**」をクリックする。
8. 取り出されたこの証明書を LDAP クライアント・マシンにコピーする。
9. これで、LDAP サーバーを構成して、SSL を使用可能にできるようになります。

SSL を使用可能にするための LDAP サーバーの構成

LDAP サーバーを構成して SSL を使用可能にするには、以下のステップを実行します。

1. ユーザー・レジストリーとして LDAP を使用する場合は、LDAP サーバーがインストールされ、動作していることを確認する。その詳細な説明については、29ページの『第4章 IBM SecureWay Directory のインストールと構成』を参照してください。
2. 以下の URL で Web ベースの LDAP 管理ツールを使用する。

   ```
   http://servername/ldap
   ```

   ここで、*servername* は LDAP サーバー・マシンの名前です。

3. LDAP 管理者としてログオンしていない場合は、LDAP 管理者 (たとえば cn=root) としてログオンする。
4. 「**Server → SSL**」をクリックする。
5. SSL と非 SSL を使用可能にする「**SSL On**」をクリックするか、または設定したい SSL 状況に対して「**SSL Only**」をクリックする。
6. 認証方式のタイプに対して「**Server Authentication**」をクリックする。
7. ポート番号を入力するか、デフォルトのポート番号 636 を受け入れる。
8. 『キー・データベース・ファイルと証明書の作成』のステップ 5 で指定したキー・データベース・パスとファイル名を入力する。

   キー・データベース・ファイルの拡張子は *.kdb* です。
9. LDAP サーバーの証明書をキー・データベースに保管した場合は、識別に使用した名前を「**Key Label**」フィールドに入力する。たとえば、ラベルは、LDAP サーバーのマシン名にすることができます。
10. キー・データベース・ファイルのパスワードを入力し、それを確認する。または、LDAP サーバーが stash ファイルを使用するようにしたい場合は、パスワード・フィールドをブランクにすることができます。
11. 「**Apply**」をクリックする。
12. 「**restart the server**」リンクをクリックして、LDAP サーバーを再始動し、この変更を有効にする。

SSL アクセスのテスト: SSL が使用可能になったことをテストするには、LDAP サーバーのコマンド行から以下のコマンドを入力してください。

```
ldapsearch -h servername -Z -K keyfile -P key_pw -b "" -s base ¥
objectclass=*
```

このコマンドで円記号 (¥) が必要なのは、コマンドが 1 行に入力できない場合だけです。

ただし、以下のとおりです。

オプション	説明
servername	LDAP サーバーの DNS ホスト名。
keyfile	生成されたキー・リングの完全修飾パス名。
key_pw	生成されたキー・リングのパスワード。

このコマンドは、LDAP サーバー上のサフィックスが含まれている LDAP 基本情報を戻します。

これで、サーバー SSL のセットアップが完了しました。次は、SSL アクセス用に LDAP クライアントをセットアップします。

SSL アクセス用の LDAP クライアントのセットアップ

SSL アクセス用に LDAP サーバーをセットアップした後、SSL アクセス用に LDAP クライアントをセットアップする必要があります。

キー・データベース・ファイルの作成: GSKit がクライアント上にインストールされていることを確認してから、 35ページの『キー・データベース・ファイルと証明書の作成』に説明されているように、IBM キー管理ツールを使用して新しいキー・データベース・ファイルを作成します。

クライアントが LDAP サーバーを認証できるようにするには、クライアントが、LDAP サーバーの証明書を作成した認証局 (署名者) を認識する必要があります。 LDAP サーバーが自己署名入り証明書を使用する場合、クライアントが、LDAP サーバーの証明書を生成したマシンを、トラステッド・ルート (認証局) として認識できるようにする必要があります。

署名者証明の追加: キー・データベース・ファイルが作成された後で署名者証明を追加するには、以下のステップを実行します。

1. 38ページの『自己署名入り証明書の取り出し』でキー・データベース・ファイルから取り出された証明書が、クライアント・マシンにコピーされていることを確認する。コピーされていない場合は、ただちにコピーしてください。
2. クライアントの CMS キー・データベース・ファイルの「**Signer Certificates**」セクションをクリックする。
3. 「**Add**」をクリックする。
4. 「**Base64-encoded ASCII data**」をクリックして、データ・タイプを設定する。
5. 証明書のファイル名とその位置を指示する。証明書ファイルの拡張子は *.arm* です。
6. 「**OK**」をクリックする。
7. 追加しようとする署名者証明のラベルを入力する。たとえば、ラベルに LDAP サーバーのマシン名を使用することができます。
8. 「**OK**」をクリックする。

   自己署名入り証明書が、クライアントのキー・データベース内に署名者証明として表示されます。
9. 新たに追加された署名者証明を強調表示し、「**View/Edit**」をクリックする。

10. 「**Set the certificate as a trust root**」が選択されていることを確認して、この証明がトラステッド・ルートとしてマークされていることを確認する。

    LDAP サーバーの証明書が正規の認証局によって生成された場合は、その認証局が署名者証明としてリストされ、トラステッド・ルートとしてマークされていることを確認してください。そうでない場合は、認証局の証明を署名者証明として追加してから、それがトラステッド・ルートであることを指定します。

この時点で、クライアントは LDAP サーバーとの SSL セッションを確立することができます。

SSL が使用可能かどうかのテスト: SSL が使用可能になったことをテストするには、LDAP クライアントのコマンド行から、以下のコマンドを入力します。

```
ldapsearch -h servername -Z -K client_keyfile -P key_pw -b "" ¥
-s base objectclass=*
```

このコマンドで円記号 (¥) が必要なのは、コマンドが 1 行に入力できない場合だけです。

ただし、以下のとおりです。

オプション	説明
servername	LDAP サーバーの DNS ホスト名。
client_keyfile	生成されたキー・リングの完全修飾パス名。
key_pw	生成されたキー・リングのパスワード。

このコマンドは、LDAP サーバーのサフィックスが含まれている LDAP 基本情報を戻します。

これで、SSL のセットアップが完了しました。

LDAP サーバーとクライアントの認証タイプの使用 (任意選択)

この構成セクションは任意選択です。

1. 38ページの『SSL を使用可能にするための LDAP サーバーの構成』に説明されている手順を実行します。ただし、**サーバー認証**のために LDAP サーバーを構成するのではなく、**サーバー認証とクライアント認証**の両方を行うことを選択してください。

   この場合、サーバーがその証明をクライアントに送信し、クライアントによって認証された後、サーバーはクライアントの証明を要求します。 LDAP サーバーが両方を認証するよう構成されている場合、クライアント・マシンに対しても証明を確立する必要があります。
2. クライアント・マシンでは、クライアント・マシンの証明は、以下に説明された手順で設定されます。
   - 35ページの『キー・データベース・ファイルと証明書の作成』
   - 自己署名入り証明書である場合は 37ページの『自己署名入り証明書の作成』、署名者証明である場合は 36ページの『証明書の受け取り』
   - 38ページの『自己署名入り証明書の取り出し』
   - 38ページの『SSL を使用可能にするための LDAP サーバーの構成』

3. LDAP サーバー上で、クライアントの個人用証明書が作成され、クライアントのキー・データベース・ファイルに追加された後、そのクライアント証明書を作成した認証局が、署名者証明 (トラステッド・ルート) として認識される必要があります。認証局証明書は、40ページの『署名者証明の追加』に説明されている通りに、LDAP サーバーのキー・データベースに追加されます。

SSL アクセスのテスト: LDAP サーバーが、クライアントの個人用証明書を作成した認証局を認識した後、以下のコマンドを使用して、セットアップをテストすることができます。

```
ldapsearch -h servername -Z -K client_keyfile -P key_pw -N client_label ¥
-b "" ¥ -s base objectclass=*
```

このコマンドで円記号 (¥) が必要なのは、コマンドが 1 行に入力できない場合だけです。

ただし、以下のとおりです。

オプション	説明
servername	LDAP サーバーの DNS ホスト名。
client_keyfile	生成されたクライアント・キー・リングの完全修飾パス名。
key_pw	生成されたキー・リングのパスワード。
client_label	キーに関連したラベル (存在する場合)。このフィールドは任意選択であり、このフィールドが必要なのは、LDAP サーバーがサーバーとクライアントの両方の認証を実行するように構成されている場合だけです。

このコマンドは、LDAP サーバーのサフィックスが含まれている LDAP 基本情報を戻します。 **-N** パラメーターは、クライアントの個人用証明書がクライアントのキー・データベース・ファイルに追加されたときに指定されたラベルを示していることに注意してください。

LDAP サーバーの署名者証明のラベルを指定しないでください。 **-N** パラメーターは、どのクライアント証明書が、要求されたときにサーバーに送信されるかを、GSKit に示します。ラベルが指定されていない場合、サーバーがクライアントの証明書を要求するときに、デフォルトの個人用証明書が送信されます。

これで、SSL のセットアップが完了しました。

LDAP アクセス制御の使用可能化

Policy Director セキュリティーを LDAP ユーザー・レジストリーと統合させるためには、以下のステップを実行して、ユーザー・レジストリーを制御する LDAP ACL を更新してください。

1. 「**スタート → プログラム → IBM SecureWay Directory → Directory Management Tool**」をクリックして、LDAP クライアントまたは LDAP サーバーのどちらかから Directory Management Tool を始動する。
2. 以下の手順でサーバーを再バインドする。
   a. 「**Server → Rebind**」をクリックする。
   b. 「**Authenticated**」をクリックする。
   c. ユーザー DN (たとえば、cn=root) を入力する。
   d. パスワードを入力する。
   e. 「**OK**」をクリックする。
3. 「**OK**」をクリックするか、警告メッセージが表示されるたびに、警告メッセージ・ウィンドウを閉じる。
4. Policy Director セキュリティー・デーモン・グループに、31ページの『サフィックスの追加』で作成されたサフィックスに対する完全な制御権を与える。
   a. 「**Entries → Add Entry**」をクリックする。
   b. Policy Director ユーザーと GSO ユーザー・データベースのサフィックスを、「**Entry RDN**」に入力する。たとえば、以下のようにします。

      ```
      o=IBM,c=US
      ```

   c. 「**Organization**」をクリックする。
   d. 「**Next**」をクリックする。

      「Create an LDAP Entry」ウィンドウが表示されます。
   e. 所属組織に該当する情報を追加してから、「**Create**」ボタンをクリックする。
   f. 「**Tree → Refresh tree**」をクリックする。 Browse ディレクトリー・ツリー内に新しい項目が表示されるはずです。
5. **ACL** タブをクリックして、各制御 LDAP ACL の所有者のリストに以下を追加することにより、Policy Director セキュリティー・デーモン・グループに完全な制御権を与える。

   ```
   cn=SecurityGroup,secAuthority=Default
   ```

   「**Edit an LDAP ACL**」ウィンドウが表示されます。

a. DN フィールドに cn=SecurityGroup,secAuthority=Default と入力してから、ドロップダウン・リストから「**group**」をクリックする。

b. 「**Add**」ボタンをクリックする。

c. 「Granted Rights for Add, Delete, and Class」の下にあるチェック・ボックスをすべて選択する。

d. 完了したら、「**Change**」をクリックする。そうすると、サフィックス DN の ACL のリスト内に cn=SecurityGroup,secAuthority=Default が表示されます。

e. 所有者のリストに複数のサフィックスを追加する場合、サフィックスごとにこの手順を繰り返す。

これで、LDAP の構成が完了しました。

第5章 Policy Director (Windows 用) のインストール

この章の節では、サポートされている Windows および Windows NT プラットフォーム上で Policy Director をインストールし、構成する方法を説明します。

Policy Director のインストールを開始する前に、必ず、『Policy Director (Windows 用) をインストールする前に』の情報に目を通してください。

Policy Director (Windows 用) をインストールする前に

NetSEAT と Policy Director のインストールを開始する前に、以下の情報をお読みください。

- NetSEAT と Policy Director をインストールする前に、まず Windows NT サーバーをインストールし、構成する必要があります。
- Windows NT ドメイン管理者およびセキュア・ドメイン管理者 (たとえば、cell_admin account) のパスワードを知っている必要があります。必ず、管理者権限を入手しておいてください。
- Windows NT オペレーティング・システムに Policy Director サーバーをインストールする際に、新しい DCE セルを作成しようとする場合は、以下のことが必要です。
  - DCE サーバーもインストールし、構成する必要があります。
  - ユーザー・レジストリーに LDAP を使用しようとする場合は、LDAP サーバーもインストールし、構成する必要があります。
- 23ページの『セキュア・ドメインのインストール要件』に説明があるように、Policy Director の配置に関するすべての情報を十分に理解しておいてください。

NetSEAT と Policy Director のインストール

Policy Director のインストールを開始する前に、必ずすべてのアプリケーションをクローズしておいてください。 Policy Director のインストールが終了したら、コンピューターをいったんシャットダウンしてから、再始動する必要があります。

セキュア・ドメイン・インベントリーの作成

インストール時に、以下のような、セキュア・ドメインの構成に固有の情報を提供する必要があります。

- セキュア・ドメイン名 (DCE セル)。たとえば cell_admin。
- 以下のサービスを提供するコンピューターの名前。
  - セキュリティー
  - タイム
  - セル・ディレクトリー・サービス (CDS)
  - ディレクトリー・サービス・ブローカー (DSB)

NetSEAT のインストール

Policy Director NetSEAT セットアップ・ファイルは、NetSEAT ファイルをハード・ディスクにコピーしてから、NetSEAT 構成ユーティリティーを自動的に始動します。

NetSEAT をインストールするには、以下のステップを実行してください。

1. 管理者権限のあるユーザーとしてログインする。
2. *IBM SecureWay Policy Director Version 3.0* CD を CD-ROM ドライブに挿入する。
3. CD 上の ¥win32¥client ディレクトリーに変更する。
4. Setup.exe ファイルをダブルクリックする。InstallShield プログラムが始動します。
5. 「Choose Installation Language」ウィンドウが表示されたら、該当する言語を選択する。
6. 「**Next**」をクリックする。「Policy Director Welcome」ウィンドウが表示されます。
7. 「**Next**」をクリックする。
8. 「Choose Components to Install」ウィンドウが表示されたら、「**Client for Policy Director server products**」をクリックする。
9. 「**Next**」をクリックする。
10. 「Choose Setup Type」ウィンドウが表示されたら、「**Typical**」をクリックする。

    通常のインストールの場合のデフォルト位置は、以下のとおりです。

    ```
    c:¥Program Files¥ibm¥netseat¥
    ```

または、「**Custom**」をクリックする場合は、NetSEAT をインストールする先のドライブとディレクトリーを指定してください。

「Choose Destination Location」ウィンドウが表示されます。

11. 「**Next**」をクリックする。

    NetSEAT ファイルは、ハード・ディスクのデフォルトの NetSEAT 位置にコピーされます。「NetSEAT Configuration」ウィンドウが表示されます。

NetSEAT の構成

NetSEAT 構成タスクでは、セキュア・ドメインについての情報 (たとえば、DCE サーバー名、位置、およびサービス) を NetSEAT に指定します。

すべての NetSEAT ファイルがハード・ディスクにコピーされた後、「NetSEAT Configuration」ウィンドウ (**Secure Domains** タブ) が表示されます。

NetSEAT を構成するには、以下のステップを実行してください。

1. 新しいセキュア・ドメイン用の項目を追加するために、「**Add**」をクリックする。

   「New Secure Domain」ウィンドウが表示されます。
2. NetSEAT が属するセキュア・ドメイン (DCE セル) の名前 (たとえば、cell_admin) を入力する。
3. 「**Enable GSS**」または「**Enable SSL**」チェック・ボックスのどちらかを選択する。
4. 「**OK**」をクリックする。

   「Secure Domain Properties」ウィンドウが表示されます。
5. DCE サーバーと、DCE サーバーが提供するサービスを追加するために、「**Add**」をクリックする。

   「Add a DCE Server」ウィンドウが表示されます。

   このウィンドウを使用して、セキュア・ドメイン内の既存の DCE サーバーと、各サーバーが提供するサービスを NetSEAT に知らせます。複数の DCE サーバーを追加することができます。すべてのサービスを 1 つのコンピューターで実行することも、複数のコンピューターに分割することもできます。

   ここで説明するシナリオは、以下のとおりです。

   - **新しいセキュア・ドメイン (1 つのホスト・システム)**

1 つのホスト・システムだけで構成される新しいセキュア・ドメインを作成する場合は、そのホスト・システムがすべての DCE サービスを提供します。ホスト・システムの名前を「**Machine Name**」フィールドに入力してください。1 つまたは複数のサービスを選択します。 DSB がまだインストールされていない場合であっても、DSB を選択してください。

- **新しいセキュア・ドメイン (複数のホスト)**

  新しいセキュア・ドメインを作成するときに、DCE サービスが別のホストに置かれている場合は、ローカル・ホストは DSB サービスだけを提供します。この場合、DCE サービス (セキュリティー、タイム、CDS) を提供する DCE サーバーを最初に追加します。次に、ローカル・システムを表す `localhost` という名前が付けられた別の DCE サーバーを追加し、DSB チェック・ボックスを選択します。 DSB がまだインストールされていない場合であっても、DSB を選択できます。

- **既存のセキュア・ドメイン**

  既存のセキュア・ドメインに Policy Director を追加する場合は、セキュリティー、タイム、および CDS を提供する DCE サーバーの名前を追加します。次に、DSB が自動的にインストールされる Policy Director 管理サーバーが組み込まれている DCE サーバーの名前を追加します。このシステムの DSB チェック・ボックスを選択します。このシナリオでは、DSB を含めてすべてのサービスが、同じホスト・システムに置かれている場合があります。

6. サーバーごとに、セキュア・ドメイン内の既存のサーバーの完全 DN マシン名を入力する (たとえば、SFF98732.austin.ibm.com)。
7. サーバーごとに、以下の 1 つまたは複数のサービスをサーバー用に選択する。
   - セキュリティー
   - DSB
   - タイム
   - CDS
8. 「**OK**」をクリックする。

   「Secure Domain Properties」ウィンドウが、新しい項目を表示します。
9. 必要に応じて、ステップ 5 〜ステップ 8 を繰り返して、追加のサーバーとサービスを追加する。
10. 「Secure Domain Properties」ウィンドウから、デフォルトの拡張ログイン構成 **DCE Login only** を受け入れる。

「Secure Domains Properties」ウィンドウの統合ログイン区域は、この NetSEAT インストールでは使用されません。

11. 「**OK**」をクリックする。

    「NetSEAT Configuration」ウィンドウが表示されます。

12. 「**OK**」をクリックする。

    「System Restart Required」ウィンドウが表示されます。

13. 「**Yes**」をクリックして、コンピューターを再始動する。
14. 「**OK**」をクリックする。

    コンピューターが再始動すると、NetSEAT が自動的に始動します。NetSEAT アイコンが Windows タスクバーに表示されます。

    これで、NetSEAT のインストールと構成が完了しました。

NetSEAT クライアント構成の検証

Policy Director サーバーをインストールする前に、NetSEAT クライアントが正常に構成され、指定されたセキュア・ドメインに入れられたことを確認してください。 **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てください。

- 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 (DSB)

NetSEAT クライアントが必要なサービスと通信できることを確認するには、以下のステップを実行してください。

1. 「**スタート → プログラム → NetSEAT → NetSEAT Login**」をクリックして、cell_admin としてログインする。

   または、コマンド行で **netseat_login** コマンドを使用してログインしてください。

2. ご使用の構成に特に必要な場合を除いて、PKI Login を選択しないでください。
3. Policy Director 管理者のユーザー名とパスワードを入力する。
4. 「**OK**」をクリックする。
5. コマンド行で、**netseat_ping** コマンドを使用して、構成の状況を入手する。

たとえば、NetSEAT クライアントが構成され、″redback″ と呼ばれるセキュア・ドメインに入れられる場合、DOS プロンプトで以下のコマンドを入力して、状況を入手します。

```
netseat_ping -C redback
```

以下の出力と同じような情報が表示されます。

```
/.../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[ ] not available
                    ncacn_ip_udp:redback[ ] not available
```

ただし、新しいセキュア・ドメインを作成する予定である場合は、DSB がまだ動作しないことに注意してください。この場合、DSB に対する **netseat_ping** 出力は、`not available` と表示されます。このように表示されるのは、このシナリオの場合、予想されるものです。 Policy Director 管理サーバー構成要素のインストールでは、DSB が自動的にインストールされ、構成され、始動されるので、問題なく Policy Director のインストールを続行できます。 DSB がすでに動作している場合は、DSB の出力は `is available (v3.1)` と表示されます。

6. DSB 以外のサービスが使用不能である場合は、Policy Director サーバーをインストールする前に、その問題を解決しておく。

Policy Director サーバーのインストール

Policy Director サーバーのインストールを開始する前に、必ず、管理者のユーザー名とパスワードを入手しておいてください。

Policy Director サーバー構成要素をインストールするには、以下のステップを実行します。

1. ユーザー・レジストリーとして LDAP を使用しようとする場合は、LDAP サーバーがインストールされ、動作していることを確認する。その詳細な説明については、29ページの『第4章 IBM SecureWay Directory のインストールと構成』を参照してください。
2. *IBM SecureWay Policy Director Version 3.0* CD を CD-ROM ドライブに挿入する。

3. CD 上の ¥win32¥server ディレクトリーに変更する。
4. Setup.exe ファイルをクリックする。InstallShield プログラムが始動します。
5. 「Choose Installation Language」ウィンドウが表示されたら、該当する言語を選択する。
6. 「**Next**」をクリックする。「Policy Director Welcome」ウィンドウが表示されます。
7. 「**Next**」をクリックする。

   「Choose Destination Location」ウィンドウが表示されます。
8. プログラム・ファイルのデフォルトのディレクトリー位置を受け入れるか、または「**Browse**」ボタンをクリックして別のディレクトリーを作成または選択する。

   デフォルトの位置は、 `C:¥Program Files¥IBM¥` です。

   デフォルト以外の位置に NetSEAT をインストールした場合は、同じ位置に Policy Director サーバーをインストールしてください。
9. 「**Next**」をクリックする。

   「Select Components」ウィンドウが表示されます。
10. 該当する Policy Director サーバー構成要素を選択する。選択に役立つ情報を得るには、19ページの『一般的な構成』を参照してください。

    セキュア・ドメイン内には Policy Director 管理サーバー (IVMgr) のインスタンスは、1 つだけでなければなりません。
11. 「**Next**」をクリックする。
12. WebSEAL を選択しなかった場合は、 54ページのステップ 14 に進む。

    WebSEAL (IVWeb) 構成要素を選択した場合は、「Choose Web Document Root Location」ウィンドウが表示されます。このウィンドウでは、Web スペースのルート・ディレクトリーの位置を指定するように求められます。Web サイトに属しているリソースはすべて、このディレクトリーの下に置かれます。
13. デフォルトのルート・ディレクトリー位置を受け入れるか、または「**Browse**」ボタンをクリックして別のディレクトリーを作成または選択する。デフォルトの位置は、以下のとおりです。

    ```
    C:¥...¥IBM¥Policy Director¥www¥docs
    ```

    これで、Policy Director ファイルが CD からハード・ディスクにコピーされます。セキュア・ドメインの「Administrator Login」ウィンドウが表示さ

れます。このステップは、セキュリティー・クリデンシャルを確立し、構成プロセスを完了するのに必要です。

14. DCE セル管理者の名前とパスワードを入力する。
15. 管理サーバー構成要素 (IVMgr) を選択した場合、「**LDAP Registry**」か「**DCE Registry**」を選択するように求めるプロンプトが表示される。

    管理サーバーを選択しなかった場合は、既存のセキュア・ドメインのユーザー・レジストリー・タイプが、自動的に検出されます。

    - LDAP ユーザー・レジストリーが検出されると、『LDAP ユーザー・レジストリーの使用』に説明されている通りに、インストールが続行します。
    - DCE ユーザー・レジストリーが検出されると、55ページの『DCE ユーザー・レジストリーの使用』に説明されている通りに、インストールが続行します。
16. ユーザー・レジストリーに対して以下のどちらかをクリックする。
    - 「**LDAP User Registry**」を選択した場合は、 『LDAP ユーザー・レジストリーの使用』に進みます。
    - 「**DCE User Registry**」を選択した場合は、 55ページの『DCE ユーザー・レジストリーの使用』に進みます。

LDAP ユーザー・レジストリーの使用

Policy Director セキュア・ドメインが LDAP ユーザー・レジストリーを使用する場合、または IVMgr をインストールしようとするときに、「**LDAP Registry**」が選択されている場合、「LDAP Server Information」ウィンドウが表示されます。

1. LDAP サーバー構成に必要な以下の情報を入力する。
    - LDAP ホスト名
    - ポート番号
    - SSL ポート番号 (SSL を使用して LDAP サーバーにアクセスする場合のみに必要)
    - GSO データベース用の LDAP DN (たとえば、o=ibm,c=us)
2. 「**Next**」をクリックする。

    「Communication with the LDAP Server」ウィンドウが表示されます。
3. Policy Director と LDAP サーバー間の SSL 通信を使用可能にするか、使用不可にするかを選択する。 SSL 通信を使用可能にするには「**Yes**」をクリックし、SSL 通信を使用不可にするには「**No**」をクリックします。

Windows NT では、ホスト・システムにあるすべての Policy Director サーバーと LDAP サーバーとの間で一度に SSL 通信が使用可能になります。

SSL 通信を使用可能にした場合は、ステップ 4 に進みます。

SSL 通信を使用不可にした場合は、ステップ 5 に進みます。

4. 以下のプロンプトに値を指定する。
   - SSL キー・ファイル位置
   - SSL ファイル DN (キー・ラベル)
   - SSL キー・ファイル・パスワード

   35ページの『キー・データベース・ファイルと証明書の作成』を参照してください。
5. 「**Next**」をクリックする。

   「LDAP Administrator Login」ウィンドウが表示されます。
6. LDAP 管理者名 (たとえば、cn=root) とパスワード情報を入力し、「**OK**」をクリックする。

   サーバーが構成され、始動されます。これには、数分かかる場合があります。「System Information」ウィンドウが表示され、登録情報を含めて、サーバーの状況を表示します。
7. 「**Next**」をクリックする。

   「Policy Director Setup Complete」ウィンドウが表示されます。
8. 「**Yes**」をクリックして再始動する。

   再始動オプションに対して「**No**」にチェックを付けた場合は、後で Windows NT を再始動して、構成プロセスを完了する必要があります。これで、Policy Director のインストールが完了しました。
9. 「**Finish**」をクリックする。

   システムを再始動するように求めるプロンプトが表示されます。

DCE ユーザー・レジストリーの使用

Policy Director セキュア・ドメインが DCE ユーザー・レジストリーを使用する場合、または IVMgr をインストールしようとするときに、「**DCE User Registry**」が選択されている場合、以下のようにインストールが続行します。

1. WebSEAL (IVWeb) 構成要素を選択した場合は、「Choose Web Document Root Location」ウィンドウが表示されます。このウィンドウでは、Web スペースのルート・ディレクトリーの位置を入力するように求められます。Web サイトに属しているリソースはすべて、このディレクトリーの下に置かれます。

WebSEAL を選択しなかった場合は、ステップ 3 に進みます。

2. デフォルトのルート・ディレクトリー位置を受け入れるか、または「**Browse**」ボタンをクリックして別のディレクトリーを作成または選択する。デフォルトの位置は、以下のとおりです。

   ```
   C:¥Program Files¥IBM¥Policy Director¥www¥docs
   ```

3. 「**Next**」をクリックする。

   これで、Policy Director ファイルが CD からハード・ディスクにコピーされます。セキュア・ドメインの「Administrator Login」ウィンドウが表示されます。

4. LDAP 管理者名とパスワード情報を入力し、「**OK**」をクリックする。

   サーバーが構成され、始動されます。これには、数分かかる場合があります。「System Information」ウィンドウが表示され、登録情報を含めて、サーバーの状況を表示します。

5. 「**Next**」をクリックする。

   「Policy Director Setup Complete」ウィンドウが表示されます。

6. 「**Finish**」をクリックする。

   システムを再始動するように求めるプロンプトが表示されます。

7. 「**Yes**」をクリックして再始動する。

   再始動オプションに対して「**No**」にチェックを付けた場合は、後で Windows NT を再始動して、構成プロセスを完了する必要があります。これで、Policy Director のインストールが完了しました。

クリデンシャル取得サービスの構成

Policy Director CAS は自動的にインストールされます。 CAS をクリデンシャル取得サービスとして使用したい場合は、それを構成する必要があります。その方法については、*Policy Director 管理の手引き* のクリデンシャル取得サービスの構成についての情報を参照してください。

Windows NT での NetSEAL トラップの使用

Policy Director NetSEAL (IVTrap) は、特定のポートに対する要求をトラップします。 NetSEAL トラップを使用するには、指定されたポートを使用するすべてのアプリケーションをいったん停止してから、再始動する必要があります。

Policy Director NetSEAL を構成して特定ポートをトラップする方法の詳細は、*Policy Director 管理の手引き* の NetSEAL についての概要を参照してください。

Windows での管理コンソールのインストール

Policy Director は、Policy Director セキュリティー・システムの多くの構成要素を Windows クライアント・デスクトップから管理する、管理コンソールを提供します。管理コンソールは、以下のオペレーティング・システムのいずれかにインストールできます。

- Windows 95
- Windows 98
- Service Pack 4 を備えた Windows NT バージョン 4.0 以上

Policy Director を実行する各 Windows オペレーティング・システムには、Policy Director NetSEAT クライアントが必要です。

NetSEAT クライアントは、DCE 実行時クライアントか、Policy Director サーバーに対するクライアントのいずれかとして構成できます。管理コンソールにはどちらの構成でも受け入れることができますが、Policy Director サーバーには、Policy Director サーバーに対する完全なクライアントが必要です。

構成要素を再インストールする必要がある場合、再インストールを行う前に、既存の構成要素を削除しておく必要があります。

サーバー構成要素付きでの管理コンソールのインストール

52ページの『Policy Director サーバーのインストール』で Policy Director サーバー構成要素がインストールされ、構成された後、以下のステップを実行します。

1. *IBM SecureWay Policy Director Version 3.0* CD を CD-ROM ドライブに挿入する。
2. ¥win32¥Console ディレクトリーに変更する。
3. Setup.exe ファイルをダブルクリックする。InstallShield プログラムが始動します。
4. 「Choose Installation Language」ウィンドウが表示されたら、該当する言語を選択する。
5. 「**Next**」をクリックする。「Policy Director Welcome」ウィンドウが表示されます。
6. 「**Next**」をクリックする。「Choose Destination Location」ウィンドウが表示されます。
7. ファイルをインストールする場所を指定する。

   ファイルが、Windows コンピューターの正しい位置にコピーされます。情報ウィンドウが表示され、インストールが成功したことを示します。

8. Windows を再始動するかどうかを照会されたら、「**yes**」をクリックする。
9. 「**OK**」をクリックする。
10. 59ページの『管理コンソールの始動』に進む。

サーバー構成要素なしでの管理コンソールのインストール

追加の Windows システムからの Policy Director セキュリティー管理を使用可能にするには、Policy Director サーバー構成要素がインストールされていない Windows システムに、管理コンソールをインストールすることができます。この方法で管理コンソールをインストールすると、NetSEAT クライアントを、DCE 実行時クライアントか、Policy Director サーバーに対するクライアントのいずれかとして構成できます。

サーバー構成要素なしで管理コンソールをインストールするには、Windows デスクトップ・システムに進み、以下のステップを実行します。

1. Windows オペレーティング・システムが、サポートされているプラットフォームであることを確認する。 16ページの『Policy Director サーバー』を参照してください。
2. Policy Director NetSEAT クライアントをインストールする。 48ページの『NetSEAT のインストール』の説明に従ってください。
3. NetSEAT クライアントが正しく構成され、管理コンソールが実行されているセキュア・ドメイン内に入っていることを確認する。 51ページの『NetSEAT クライアント構成の検証』を参照してください。
4. *IBM SecureWay Policy Director Version 3.0* CD を CD-ROM ドライブに挿入する。
5. ¥win32¥Console ディレクトリーに変更する。
6. Setup.exe ファイルをダブルクリックする。InstallShield プログラムが始動します。
7. 「Choose Installation Language」ウィンドウが表示されたら、該当する言語を選択する。
8. 「**Next**」をクリックする。「Policy Director Welcome」ウィンドウが表示されます。
9. 「**Next**」をクリックする。「Choose Destination Location」ウィンドウが表示されます。
10. ファイルをインストールする場所を指定する。

    ファイルが、Windows コンピューターの正しい位置にコピーされます。情報ウィンドウが表示され、インストールが成功したことを示します。

11. 「**OK**」をクリックして、インストールを完了する。
12. 管理コンソールを始動するには、『管理コンソールの始動』に進む。

管理コンソールの始動

管理コンソールを始動するには、以下のステップを実行してください。

1. Policy Director サーバーがインストールされ、動作していることを確認する。
2. 「**スタート → プログラム → Policy Director → Management Console**」をクリックする。

   「Policy Director Management Console」ウィンドウが表示されます。
3. 管理者権限を持つユーザー (cell_admin など) として管理コンソールにログインする。

Policy Director の削除

Policy Director 構成要素を削除するには、必ず、管理者としてログオンしてください。管理者クリデンシャルを持つユーザーとして、Windows ドメインにログインしてください。たとえば、以下のとおりです。

```
dce_login cell_admin password
```

正しいセキュア・ドメイン・クリデンシャルを持たずに構成要素を削除しようとすると、「Authorization Failure」メッセージ・ウィンドウが表示されます。

インストールとはまったく逆の順序で Policy Director 構成要素を削除する必要があります。 Policy Director を削除するには、コントロール・パネルから「**アプリケーションの追加と削除**」アイコンを使用します。

Policy Director のインストール全体をアンインストールするには、以下の手順を、表示されている順に実行してください。

1. 管理コンソールを削除する。
2. サーバー構成要素を削除する。
3. NetSEAT クライアントを削除する。

管理コンソールの削除

管理コンソールを削除するには、以下のステップを実行してください。

1. 管理コンソールが実行されている場合は、これをクローズする。

2. コントロール・パネルの「**アプリケーションの追加と削除**」に進み、「**Policy Director Management Console**」をクリックする。
3. 「**追加と削除**」ボタンをクリックする。
4. 本当に削除するかどうかの照会が出されたら、「**はい**」をクリックして、プログラムを削除することを確認する。
5. 「**OK**」をクリックする。

サーバー構成要素の削除

Policy Director サーバー構成要素を削除するには、権限とクリデンシャルを入手してから、その構成要素を削除する必要があります。

サーバー構成要素を削除するには、以下のステップを実行してください。

1. Policy Director サーバーがインストールされ、動作していることを確認する。
2. コントロール・パネルの「**アプリケーションの追加と削除**」に進み、最初に削除したい Policy Director サーバー構成要素を選択する。
3. インストールした順序とまったく逆の順序で、Policy Director サーバー構成要素を削除する。

   たとえば、すべての構成要素をインストールした場合は、以下の順序で削除します。

   - 許可 ADK (IVAuthADK)
   - 許可サーバー (IVAcld)
   - NetSEAL (IVTrap)
   - WebSEAL (IVWeb)
   - セキュリティー・マネージャー (IVNet)
   - 管理サーバー (IVMgr)
   - Base (IVBase)。この構成要素は、常に自動的にインストールされます。

   Policy Director 管理コンソールは、どの時点でも削除できます。構成要素をインストールする順序の詳細は、26ページの『ステップごとの Policy Director インストールの概要』を参照してください。
4. 「**追加と削除**」ボタンをクリックする。
5. 要求されたら、LDAP 管理者ユーザー名とパスワードを入力する。
6. Policy Director サーバー構成要素ごとに、ステップ 2 〜 ステップ 5 を繰り返す。
7. 終了したら、「**OK**」をクリックする。

NetSEAT クライアントの削除

Policy Director NetSEAT 構成要素を削除するには、Windows NT 管理者権限が必要です。

1. コントロール・パネルの「**アプリケーションの追加と削除**」に進み、「**インストールと削除**」タブをクリックする。
2. このタブのリスト・ウィンドウから、「**Policy Director NetSEAT Client**」をクリックする。
3. 「**追加と削除**」をクリックする。
4. 「**OK**」をクリックする。

第6章 Policy Director (AIX 用) のインストール

この章の本節では、AIX オペレーティング・システムでの Policy Director のインストールおよび構成方法について解説します。

Policy Director のインストールを開始する前に、必ず、『Policy Director (AIX 用) をインストールする前に』の情報に目を通してください。

Policy Director (AIX 用) をインストールする前に

NetSEAT と Policy Director のインストールを開始する前に、以下の情報をお読みください。

- Policy Director サーバーをインストールする際に新しい DCE を作成する場合には、以下のとおりです。
  - DCE サーバーもインストールし、構成する必要があります。
  - ユーザー・レジストリーに LDAP を使用する場合は、LDAP サーバーもインストールし、構成する必要があります。
- 23ページの『セキュア・ドメインのインストール要件』に記載されている、Policy Director の配置に関するすべての情報に精通しておいてください。

管理コンソールのインストール

Policy Director は、Policy Director システムのすべての構成要素を管理するのに使用できる管理コンソールを提供します。管理者は、AIX システムまたは Windows システム、あるいはその両方での管理コンソールのインストールを選択できます。

AIX 用の管理コンソールは、IV.Console という名前のパッケージとして配布されます。パッケージのインストールおよび構成には、SMIT を使用してください。

Policy Director のインストール

Policy Director を AIX にインストールするには、以下の手順で行います。

1. LDAP をユーザー・レジストリーとして使用しようとする場合は、LDAP サーバーがインストールされ、実行していることを確認する。その詳細な説明については、29ページの『第4章 IBM SecureWay Directory のインストールと構成』を参照してください。
2. root としてログインする。
3. *IBM SecureWay Policy Director Version 3.0* CD を CD-ROM ドライブに挿入する。
4. SMIT を開始する。
5. 「**Software Installation and Maintenance**」をクリックする。

   「Software Installation and Maintenance」メニューが表示されます。
6. 「**Install and Update Software**」をクリックする。

   「Install and Update Software」メニューが表示されます。
7. 「**Install and Update Software by Package Name**」をクリックする。

   「Install and Update Software by Package Name」ウィンドウが表示されます。
8. ソフトウェアのインストール元となる装置の名前を入力する。

   たとえば、以下のとおりです。
   - CD 装置からインストールしようとする場合は、`/dev/cd0` と入力します
   - 取り付けられたサーバーのディレクトリーからインストールしようとする場合は、 `/mnt/user/lpp/IV` と入力します。

     装置名を入力すると、「Multi-select List」ウィンドウが表示されます。
9. 「**IV**」をクリックする。

   「Multi-select List」ウィンドウに、Policy Director ソフトウェア・パッケージのリストが表示されます。
10. インストールしたいパッケージを選択する。
    - Policy Director パッケージをすべてインストールする場合は、 **IV** というエントリーをクリックする。
    - 一部の Policy Director パッケージだけをインストールする場合は、23ページの『セキュア・ドメインのインストール要件』に記載されているインストールの依存性に注意してください。
11. 「**OK**」をクリックする。

「SMIT」メニューの「Install and Update Software by Package Name」ウィンドウが表示されます。

12. 以下のラベルが付いているフィールドに対して、「**yes**」をクリックする。

    `AUTOMATICALLY install requisite software?`

    このステップにより、Policy Director Base (IV.Base) および SMIT Setup (IV.smit) パッケージが確実にインストールされます。これらのパッケージは、その他の Policy Director パッケージの前提条件ソフトウェアです。このフィールドを「**no**」に設定するよう選択した場合は、パッケージ選択メニューに戻ります。IV.Base と IV.Smit が選択してあるか確認してください。

13. 他のフィールドを、自分の導入システムに該当する値に設定する。
14. 「**OK**」をクリックする。

    SMIT により、以下の内容を含む、状況メッセージが表示されます。

    - Policy Director ソフトウェア・パッケージの事前インストール検査
    - パッケージのファイルの抽出時の各パッケージの名前
    - 各パッケージについての構成の作成メニュー
    - ファイル抽出の完了時の成功を示す状況メッセージ

15. ファイル抽出が完了したら、『LDAP ユーザー・レジストリー付きでの Policy Director の構成』に記載されている情報を使用して、Policy Director パッケージを構成する。あるいは、DCE レジストリーを使用している場合は、72ページの『DCE ユーザー・レジストリー付きでの Policy Director の構成』を参照してください。

LDAP ユーザー・レジストリー付きでの Policy Director の構成

Policy Director ソフトウェア・パッケージを構成する前に、それらをインストールする必要があります。Policy Director パッケージをまだインストールしていない場合は、 64ページの『Policy Director のインストール』を参照してください。

DCE ユーザー・レジストリー付きで Policy Director をインストールした場合は、72ページの『DCE ユーザー・レジストリー付きでの Policy Director の構成』に進んでください。

インストールした各 Policy Director パッケージを構成する必要があります。ただし、SMIT Setup は例外です。パッケージの構成は、一度に 1 つずつ行いま

す。Policy Director パッケージのなかには、構成中に管理者が画面のプロンプトに応答しなければならないものがあります。

Policy Director パッケージを構成するには、以下のように行います。

1. SMIT を開始する。

   「System Management」メニューが表示されます。

2. 「**Communications Applications and Services**」をクリックする。

   インストール済みのソフトウェア・パッケージのリストが表示されます。たとえば、以下のとおりです。

   - TCP/IP
   - NFS
   - DCE (分散コンピューティング環境)
   - Policy Director

3. 「**Policy Director**」をクリックする。

   「Policy Director」メニューが、以下のオプション付きで表示されます。

   - Policy Director Configuration
   - Policy Director Unconfiguration

4. 「**Policy DirectorConfiguration**」をクリックする。

   以下のような、インストール済みの Policy Director パッケージのリストが表示されます。

   - Policy Director Base Configuration
   - Policy Director Management Server Configuration
   - Policy Director Management Console Configuration
   - Policy Director Security Manager Configuration
   - Policy Director WebSEAL Configuration
   - Policy Director Authorization Server Configuration
   - Policy Director NetSEAL Configuration
   - Policy Director Authorization ADK Configuration

5. 構成するパッケージを、一度に 1 つずつクリックする。

   Policy Director パッケージは、Policy Director 構成リストに記載されている順序で構成する必要があります。各パッケージを、上から下へ順に選択してください。

次に、以下の節で該当する構成手順を使用して Policy Director パッケージを構成する必要があります。

Base パッケージの構成

Base パッケージは、他のパッケージのどれをインストールしてもコンピューターにインストールされます。Base パッケージを構成するには、Policy Director 構成リスト内の「**Policy Director Base**」をクリックしてください。

Policy Director Base パッケージの構成は、ユーザー入力なしで完了します。

管理サーバーの構成

管理サーバーを構成するには、以下のように行います。

1. Policy Director 構成リスト内の「**Policy Director Management Server**」をクリックする。

   ユーザー・レジストリー・タイプの選択を求めるプロンプトが表示されます。

2. ユーザー・レジストリーとして LDAP を使用しようとする場合は、LDAP レジストリーに「2」を入力する。

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。

3. プロンプトが表示されたら、DCE セル管理者のアカウント名とパスワードを入力する。

   ユーザー・レジストリーとして LDAP を使用しようとする場合は、管理サーバーと LDAP サーバーとの間に通信を構成するよう求める一連のプロンプトが表示されます。

4. LDAP サーバー構成に必要な以下の情報を入力する。
   - LDAP サーバー・ホスト名
   - LDAP サーバー・ポート番号
   - LDAP サーバー SSL ポート番号 (任意選択)
5. LDAP 管理者ユーザーのユーザー名とパスワードを入力する (たとえば、`cn=root`)。ここで、Policy Director セキュリティー情報が LDAP サーバーに登録されます。
6. 管理サーバーと LDAP サーバー間の SSL 通信を使用可能にするか、使用不可にするかを選択する。

   注: 各サーバーと LDAP サーバー間の SSL 通信を、個別に使用可能にするか、使用不可にすることができます。ここでは、管理サーバー (IVMgr) と LDAP サーバーとの間の SSL 通信を設定します。
7. SSL 通信を使用不可にした場合は、68ページのステップ 8 に進む。SSL 通信を使用可能にした場合は、以下についてのプロンプトに値を指定する。

- SSL キー・リング・ファイル位置
- SSL キー・ラベル
- SSL キーのパスワード

8. GSO データベース・サフィックスに DN を指定することにより、 GSO データベース・アクセスを使用可能にする。このサフィックスは、 31ページの『サフィックスの追加』で追加したものです。

   たとえば、以下のようにします。

   ```
   o=IBM,c=US
   ```

   GSO データベース・アクセスが構成されると、Policy Director 構成マネージャーはディレクトリー・サービス・ブローカーを自動的に構成します。一連のメッセージにより、自動化された各ステップが、完了するたびにリストされます。

   IVMgr パッケージのインストールが正常に行われたことを示すメッセージが表示されます。

   選択可能なパッケージのリストが再度表示されます。

管理コンソールの構成と始動

管理コンソールを構成するには、Policy Director 構成リストの「**Policy Director Management Console**」をクリックします。

Policy Director 管理コンソールの構成は、ユーザー入力なしで完了します。

AIX 版の管理コンソールを始動するには、以下のように行います。

1. Policy Director サーバーがインストールされ、動作していることを確認する。
2. 以下のコマンドを入力する。

```
$ /opt/intraverse/bin/ivconsole
```

あるいは、Windows クライアント版の管理コンソールを使用している場合は、59ページの『管理コンソールの始動』の手順にしたがってください。

セキュリティー・マネージャーの構成

セキュリティー・マネージャー (IVNet) を構成するには、以下のように行います。

1. Policy Director 構成リスト内の「**Policy Director Security Manager**」をクリックする。

セキュリティー・マネージャーを LDAP サーバーと統合するために、一連のプロンプトが表示されます。

2. プロンプトで指示された場合は、LDAP サーバー構成に必要な以下の情報を入力する。
   - LDAP サーバー・ホスト名
   - LDAP サーバー・ポート番号
   - LDAP サーバー SSL ポート番号 (任意選択)

   これらのプロンプトは、Policy Director 管理サーバーまたは許可サーバーのどちらかが以前に構成されている場合は表示されません。
3. LDAP 管理者のユーザー名とパスワードを入力する。ここで、Policy Director セキュリティー情報が LDAP サーバーに登録されます。
4. セキュリティー・マネージャーと LDAP サーバー間の SSL 通信を使用可能にするか、使用不可にするかを選択する。

   注: 各 Policy Director サーバーと LDAP サーバー間の SSL 通信を、個別に使用可能にするか、使用不可にすることができます。ここでは、セキュリティー・マネージャー (WebSEAL と NetSEAL で使用する場合は IVNet) と LDAP サーバーとの間の SSL 通信を設定します。
5. SSL 通信を使用不可にした場合は、ステップ 6 に進む。 SSL 通信を使用可能にした場合は、以下についてのプロンプトに値を指定する。
   - SSL キー・リング・ファイル位置
   - SSL キー・ラベル
   - SSL キーのパスワード
6. GSO データベース・サフィックスに DN を指定することにより GSO データベース・アクセスを使用可能にする。このサフィックスは、 31ページの『サフィックスの追加』で追加したものです。

   たとえば、以下のようにします。

   ```
   o=IBM,c=US
   ```

   このプロンプトは、Policy Director 管理サーバーまたは許可サーバーのどちらかが以前に構成されている場合は表示されません。

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。
7. プロンプトが表示されたら、DCE セル管理者のアカウント名とパスワードを入力する。

セキュリティー・マネージャーが構成され、始動されます。CAS サーバーも始動されます。

セキュリティー・マネージャー・パッケージのインストールが正常に行われたことを示すメッセージが表示されます。

Policy Director WebSEAL の構成

Policy Director WebSEAL (IVWeb) を構成するには、以下のように行います。

1. Policy Director 構成リスト内の「**Policy Director WebSEAL**」をクリックする。

   Policy Director WebSEAL 構成メニューに、以下のものを確認する値が入って表示されます。

   - HTTP および HTTPS クライアント・アクセス
   - 必要とする伝送制御プロトコル (TCP) ポート
   - デフォルトの Web 文書ルート・ディレクトリー

2. 以下の画面で、現行の構成値を確認する。

```
Please check Web Server configuration:
1. Enable TCP HTTP?                    Yes
2. HTTP Port                           80
3. Enable HTTPS?                       Yes
4. HTTPS Port                          443
5. Web document root directory         /opt/Policy Director/www/docs
a. Accept configuration and continue with installation
x. Exit installation
Select item to change: a
```

3. 「a」を入力してこの構成を受け入れてインストールを続行するか、変更する値の数値を入力する。

   DCE セル管理者の名前とパスワードの入力を求める Policy Director セキュリティー・マネージャー構成プロンプトが表示されます。

4. DCE セル管理者のアカウント名とパスワードを入力する。

   Policy Director セキュリティー・マネージャーが再始動します。

   インストールにより、コンピューター上で Policy Director WebSEAL が構成され、使用可能になります。

Policy Director 許可サーバーの構成

Policy Director 許可サーバー (IVAcld) を構成するには、以下のように行います。

1. Policy Director 構成リスト内の「**Policy Director Authorization Server**」をクリックする。

Policy Director 許可サーバーを LDAP サーバーと統合するために、1 つまたは複数のプロンプトが表示されます。

2. プロンプトで指示された場合は、LDAP サーバー構成に必要な以下の情報を入力する。
   - LDAP サーバー・ホスト名
   - LDAP サーバー・ポート番号
   - LDAP サーバー SSL ポート番号 (任意選択)

   これらのプロンプトは、Policy Director 管理サーバーまたは許可サーバーのどちらかが以前に構成されている場合は表示されません。
3. LDAP 管理者ユーザーのユーザー名とパスワードを入力する。ここで、Policy Director セキュリティー情報が LDAP サーバーに登録されます。
4. セキュリティー・マネージャーと LDAP サーバー間の SSL 通信を使用可能にするか、使用不可にするかを選択する。

   注: 各 Policy Director サーバーと LDAP サーバー間の SSL 通信を、個別に使用可能にするか、使用不可にすることができます。ここでは、許可サーバー (IVAcld) と LDAP サーバーの間の SSL 通信を設定します。
5. SSL 通信を使用不可にした場合は、ステップ 6 に進む。 SSL 通信を使用可能にした場合は、以下についてのプロンプトに値を指定する。
   - SSL キー・リング・ファイル位置
   - SSL キー・ラベル
   - SSL キーのパスワード
6. GSO データベース・サフィックスに DN を指定することにより GSO データベース・アクセスを使用可能にする。このサフィックスは、 31ページの『サフィックスの追加』で追加したものです。

   たとえば、以下のとおりです。

   ```
   o=IBM,c=US
   ```

   このプロンプトは、Policy Director 管理サーバーまたは許可サーバーのどちらかが以前に構成されている場合は表示されません。

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。
7. プロンプトが表示されたら、DCE セル管理者のアカウント名とパスワードを入力する。

   許可マネージャーが構成され、始動されます。

許可サーバー・パッケージのインストールが正常に行われたことを示すメッセージが表示されます。

Policy Director NetSEAL の構成

Policy Director NetSEAL を構成するには、以下のように行います。

1. Policy Director 構成リスト内の「**Policy Director NetSEAL**」をクリックする。

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。

2. LDAP 管理者のユーザー名とパスワードを入力する。ここで、Policy Director セキュリティー情報が LDAP サーバーに登録されます。

   Policy Director NetSEAL パッケージ構成が完了します。

Policy Director NetSEAL は、特定のポートに対して行われる要求をトラップします。NetSEAL トラップを使用するには、指定されたポートを使用するすべてのアプリケーションをいったん停止してから、再始動する必要があります。Policy Director NetSEAL の使用について詳しくは、77ページの『AIX での NetSEAL トラップの使用』を参照してください。

Policy Director 許可 ADK の構成

Policy Director 許可 ADK を構成するには、Policy Director 構成リスト内の「**Policy Director Authorization ADK**」をクリックしてください。

Policy Director 許可パッケージ構成は、ユーザー入力なしで完了します。

Policy Director クリデンシャル取得サービスの構成

Policy Director CAS は自動的にインストールされます。 Policy Director CAS をクリデンシャル取得サービスとして使用したい場合は、それを構成する必要があります。 *Policy Director 管理の手引き* に記載されている Policy Director CAS に関する情報および WebSEAL サーバーに合わせたその構成方法を参照してください。

DCE ユーザー・レジストリー付きでの Policy Director の構成

Policy Director ソフトウェア・パッケージを構成する前に、それらをインストールする必要があります。Policy Director パッケージをまだインストールしていない場合は、まず最初に 64ページの『Policy Director のインストール』を参照してください。

LDAP ユーザー・レジストリー付きで Policy Director をインストールした場合は、65ページの『LDAP ユーザー・レジストリー付きでの Policy Director の構成』に進んでください。

インストールした各 Policy Director パッケージを構成する必要があります。ただし、SMIT Setup は例外です。パッケージの構成は、一度に 1 つずつ行います。Policy Director パッケージのなかには、構成中に管理者が画面のプロンプトに応答しなければならないものがあります。

Policy Director パッケージを構成するには、以下のように行います。

1. SMIT を開始する。

   「System Management」メニューが表示されます。
2. 「**Communications Applications and Services**」をクリックする。

   インストール済みのソフトウェア・パッケージのリストが表示されます。たとえば、以下のとおりです。

   - TCP/IP
   - NFS
   - DCE (分散コンピューティング環境)
   - Policy Director
3. 「**Policy Director**」をクリックする。

   「Policy Director」メニューが、以下のオプション付きで表示されます。

   - Policy Director Configuration
   - Policy Director Unconfiguration
4. 「**Policy DirectorConfiguration**」をクリックする

   以下のような、インストール済みの Policy Director パッケージのリストが表示されます。

   - Policy Director Base Configuration
   - Policy Director Management Server Configuration
   - Policy Director Management Console Configuration
   - Policy Director Security Manager Configuration
   - Policy Director WebSEAL Configuration
   - Policy Director Authorization Server Configuration
   - Policy Director NetSEAL Configuration
   - Policy Director Authorization ADK Configuration
5. 構成するパッケージを、一度に 1 つずつクリックする。

Policy Director パッケージは、Policy Director 構成リストに記載されている順序で構成する必要があります。 各パッケージを、上から下へ順に選択してください。

次に、以下の節で該当する構成手順を使用して Policy Director パッケージを構成する必要があります。

Base パッケージの構成

Base パッケージは、他のパッケージのどれをインストールしてもコンピューターにインストールされます。Base パッケージを構成するには、Policy Director 構成リスト内の「**Policy Director Base**」をクリックしてください。

Policy Director Base パッケージ構成は、ユーザー入力なしで完了します。

管理サーバーの構成

管理サーバーを構成するには、以下のように行います。

1. Policy Director 構成リスト内の「**Policy Director Management Server**」をクリックする。

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。
2. プロンプトが表示されたら、DCE セル管理者のアカウント名とパスワードを入力する。

   インストールにより、管理サーバーが構成され、始動されます。

管理コンソールの構成と始動

管理コンソールを構成するには、Policy Director 構成リストの「**Policy Director Management Console**」をクリックする。

Policy Director 管理コンソール構成は、ユーザー入力なしで完了します。

AIX 版の管理コンソールを始動するには、以下のように行います。

1. Policy Director サーバーがインストールされ、動作していることを確認する。
2. 以下のコマンドを入力する。

```
$ /opt/intraverse/bin/ivconsole
```

セキュリティー・マネージャーの構成

セキュリティー・マネージャー (IVNet) を構成するには、以下のように行います。

1. Policy Director 構成リスト内の「**Policy Director Security Manager**」をクリックする。
2. プロンプトが表示されたら、DCE セル管理者のアカウント名とパスワードを入力する。

インストールにより、セキュリティー・マネージャーが構成され、始動されます。

Policy Director WebSEAL の構成

Policy Director WebSEAL (IVWeb) を構成するには、以下のように行います。

1. Policy Director 構成リスト内の「**Policy Director WebSEAL**」をクリックする。

   Policy Director WebSEAL 構成メニューに、以下のものを確認する値が入って表示されます。

   - HTTP および HTTPS クライアント・アクセス
   - 必要とする伝送制御プロトコル (TCP) ポート
   - デフォルトの Web 文書ルート・ディレクトリー
2. 以下の画面で、現行の構成値を確認する。

```
Please check Web Server configuration:
1. Enable TCP HTTP?                        Yes
2. HTTP Port                               80
3. Enable HTTPS?                               Yes
4. HTTPS Port                              443
5. Web document root directory        /opt/Policy Director/www/docs
a. Accept configuration and continue with installation
x. Exit installation
Select item to change: a
```

3. 「a」を入力してこの構成を受け入れてインストールを続行するか、変更する値の数値を入力する。

   DCE セル管理者の名前とパスワードの入力を求める Policy Director セキュリティー・マネージャー構成プロンプトが表示されます。
4. DCE セル管理者のアカウント名とパスワードを入力する。

   Policy Director セキュリティー・マネージャーが再始動します。

   インストールにより、コンピューター上で Policy Director WebSEAL が構成され、使用可能にされます。

Policy Director 許可サーバーの構成

Policy Director 許可サーバー (IVAcld) を構成するには、以下のように行います。

1. Policy Director 構成リスト内の「**Policy Director Authorization Server**」をクリックする。

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。
2. DCE セル管理者のアカウント名とパスワードを入力する。

   許可マネージャーが構成され、始動されます。

Policy Director NetSEAL の構成

Policy Director NetSEAL を構成するには、以下のように行います。

1. Policy Director 構成リスト内の「**Policy Director NetSEAL**」をクリックする。

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。
2. LDAP 管理者ユーザーのユーザー名とパスワードを入力する。ここで、Policy Director セキュリティー情報が LDAP サーバーに登録されます。

   Policy Director NetSEAL 構成は完了します。

Policy Director NetSEAL は、特定のポートに対して行われる要求をトラップします。NetSEAL トラップを使用するには、指定されたポートを使用するすべてのアプリケーションをいったん停止してから、再始動する必要があります。Policy Director NetSEAL の使用について詳しくは、77ページの『AIX での NetSEAL トラップの使用』を参照してください。

Policy Director 許可 ADK の構成

Policy Director 許可 ADK を構成するには、Policy Director 構成リスト内の「**Policy Director Authorization ADK**」をクリックしてください。

Policy Director 許可パッケージ構成は、ユーザー入力なしで完了します。

Policy Director クリデンシャル取得サービスの構成

Policy Director CAS は自動的にインストールされます。 Policy Director CAS をクリデンシャル取得サービスとして使用したい場合は、それを構成する必要があります。 *Policy Director 管理の手引き*に記載されている Policy Director CAS に関する情報および WebSEAL サーバーに合わせたその構成方法を参照してください。

管理コンソールのインストール

Policy Director は、Policy Director セキュリティー・システムの多くの構成要素を Windows クライアント・デスクトップから管理する、管理コンソールを提供します。管理コンソールは、以下のオペレーティング・システムのいずれかにインストールできます。

- Windows 95
- Windows 98
- Service Pack 4 を備えた Windows NT バージョン 4.0 以上
- AIX バージョン 4.3.1.0 以上

Policy Director を実行する各 Windows オペレーティング・システムには、Policy Director NetSEAT クライアントが必要です。

NetSEAT クライアントは、DCE 実行時クライアントか、Policy Director サーバーに対するクライアントのいずれかとして構成できます。管理コンソールにはどちらの構成でも受け入れることができますが、Policy Director サーバーには、Policy Director サーバーに対する完全なクライアントが必要です。

構成要素を再インストールする必要がある場合、再インストールを行う前に、既存の構成要素を削除しておく必要があります。

AIX での NetSEAL トラップの使用

Policy Director NetSEAL トラップを使用するためには、保護された (トラップされた) ポートにアクセスするあらゆるアプリケーションより前に、NetSEAL デーモン・セキュリティー・マネージャー (secmgrd) を始動する必要があります。/etc/inittab というエントリーを使用して、始動プロセス中にアプリケーションより前に secmgrd が確実に始動するようにしてください。

Telnet、RLOGIN、および POP3 などのネットワーキング・アプリケーションで NetSEAL トラップを使用してください。**inetd** デーモンがこれらのアプリケーションを制御します。 Policy Director 始動スクリプト /etc/iv/iv は secmgrd を始動し、次に、inetd デーモンを停止して、再始動します。このプロシージャーにより、システムの始動後にこれらのアプリケーションが正常にトラップされます。

Policy Director を停止して再始動する場合、トラップされたポートに対して要求を行うアプリケーションがあれば、それもすべて停止して再始動する必要があります。このプロセスを自動化するために、/etc/iv/iv にコードを追加すると、secmgrd が始動した後でアプリケーションを停止したり、始動したりする

ことができます。他のアプリケーションの停止および始動方法についてのテンプレートとして **inetd** を停止および始動するために /etc/iv/iv スクリプトの手法を使用します。

Policy Director NetSEAL を構成して特定ポートをトラップする方法の詳細は、*Policy Director 管理の手引き* の NetSEAL に関する情報を参照してください。

Policy Director の削除

Policy Director (AIX 用) は、構成解除してからでないと、削除できません。

- Policy Director の構成解除については、『Policy Director パッケージの構成解除』を参照してください。
- Policy Director の削除については、79ページの『Policy Director パッケージの削除』を参照してください。

Windows 版の管理コンソールを削除する場合は、59ページの『管理コンソールの削除』を参照してください。

Policy Director パッケージの構成解除

Policy Director サーバーを構成解除するには、以下のステップを完了します。

1. SMIT を開始する。
2. 「**Communications Applications and Services**」をクリックする。
   「Communications Applications and Services」メニューが表示されます。
3. 「**Policy Director**」をクリックする。
   「Policy Director」メニューが表示されます。
4. メニューから、「**Policy Director Unconfiguration**」をクリックする。
   構成済み Policy Director パッケージのリストが表示されます。
   構成解除するパッケージを選択します。表示されると考えられるパッケージは、以下のものです。
   - Policy Director Authorization Server Unconfiguration
   - Policy Director Authorization ADK Unconfiguration
   - Policy Director NetSEAL Unconfiguration
   - Policy Director WebSEAL Unconfiguration
   - Policy Director Security Manager Unconfiguration
   - Policy Director Management Server Unconfiguration
   - Policy Director Management Console Unconfiguration
   - Policy Director Base Unconfiguration

- IV Smit menu Unconfiguration

5. パッケージの構成解除は、一度に 1 つずつ行います。

   注: パッケージの構成解除は、インストールの場合と逆の順番で行う必要があります。確実にこの順番を守るために、メニューの上から下へパッケージの構成解除を行います。

6. コンピューターからすべての Policy Director を削除したいために Policy Director パッケージを構成解除しようとする場合は、他のすべての Policy Director パッケージを構成解除した後で「**Policy Director Smit menu Unconfiguration**」をクリックする。

   このステップにより、Policy Director パッケージ情報が SMIT データベースから削除されます。

7. 『Policy Director パッケージの削除』を参照して、Policy Director を削除する。

Policy Director パッケージの削除

Policy Director の削除を試みる前に、まず最初に、Policy Director ソフトウェアが構成解除されているか検査してください。78ページの『Policy Director パッケージの構成解除』に、構成解除の手順が示されています。

Policy Director を削除するには、以下のように行います。

1. SMIT を開始する。
2. 「**Software Installation and Maintenance**」をクリックする。

   「Software Installation and Maintenance」メニューが表示されます。

3. 「**Software Maintenance and Utilities**」をクリックする。

   「Software Maintenance and Utilities」メニューが表示されます。

4. 「**Remove Installed Software**」をクリックする。

   「Remove Installed Software」ウィンドウが表示されます。

5. 削除する Policy Director パッケージを選択する。一度に複数のパッケージを選択できます。

   すべての Policy Director パッケージを削除するためには、IV と入力します。

Policy Director ソフトウェアが削除されます。

管理コンソールおよび NetSEAT の削除

Windows 上の管理コンソールおよび Windows 上の NetSEAT クライアントは、InstallShield アンインストール機能を使用して削除できます。

- 管理コンソールを削除する。 手順については、59ページの『管理コンソールの削除』を参照してください。
- NetSEAT クライアントを削除する。 手順については、61ページの『NetSEAT クライアントの削除』を参照してください。

第7章 Policy Director (Solaris 用) のインストール

この章の本節では、Solaris オペレーティング・システム上での Policy Director のインストールおよび構成方法について解説します。

Policy Director のインストールを開始する前に、必ず、『Policy Director (Solaris 用) をインストールする前に』の情報に目を通してください

Policy Director (Solaris 用) をインストールする前に

Policy Director のインストールを開始する前に、以下の情報をお読みください。

このリリースの Policy Director のためのインストール手順には、**pkgadd** コマンドが必要です。**pkgadd** コマンドを実行するために、コマンド・プロンプトで以下のように入力してください。

```
# pkgadd -d /cdrom/cdrom0/solaris
```

pkgadd コマンドは、Policy Director ソフトウェアをインストールするのに使用します。**pkgadd** コマンドは、通常、標準的な作業手順では指示されない補足プロンプトを表示します。これらのプロンプトは、ご使用のシステムに固有のセットアップおよび構成の状態に応じて表示されます。標準プロシージャーの外側で発生するこれらのプロンプトのいずれかに対して、必ず、「y」と応答してください。

Policy Director をインストールする前に、以下のことが必要です。

- DCE クライアントをインストールする。
- ユーザー・レジストリーに LDAP を使用する場合は、LDAP クライアントもインストールする。

Policy Director のインストールを開始する前に、Transarc DCE リモート管理機能を使用可能にする必要があります。リモート管理機能が使用可能になっていない場合、Policy Director のインストールを完了できません。

一部のリモート管理機能を使用すると、セル管理者は、ローカル root アカウントと基本的に同等になることができます。Transarc DCE は、通常、これらのリモート管理機能を使用不可にします。しかし、Policy Director ソフトウェアには、これらの機能が必要です。

リモート管理機能を使用可能にする方法については、*Transarc Release Notes, Release 1.1* (DCE-D1002-01) の 4.2.1 節を参照してください。

インストールの画面出力

本書の標準的な手順では、**pkgadd** コマンドから考えられるすべての画面出力は示していません。文書で扱われていないほとんどの画面出力は、実行している操作に関する補足情報を提供するものです。一般的に、本書に記載されている標準的な手順は、ユーザー応答を必要とするメッセージだけを示しています。

LDAP レジストリー付きでの Policy Director サーバーのインストール

DCE ユーザー・レジストリー付きで Policy Director をインストールしようとする場合は、89ページの『DCE ユーザー・レジストリー付きでの Policy Director サーバーのインストール』に進んでください。

サーバー・パッケージは、*IBM SecureWay Policy Director Version 3.0* CD 上の /solaris ディレクトリーに入っています。

Policy Director パッケージをインストールするためには、root ユーザーとしてログオンする必要があります。

パッケージを再インストールする必要がある場合、必要なパッケージを再インストールする前に、まず最初に既存のパッケージ (**pkgrm**) を削除してください。

管理サーバーをインストールするには、以下のように行います。

1. ユーザー・レジストリーとして LDAP を使用しようとする場合は、LDAP サーバーがインストールされ、動作していることを確認する。詳細な手順については、29ページの『第4章 IBM SecureWay Directory のインストールと構成』を参照してください。
2. **pkgadd** コマンドを入力して、選択可能なパッケージを CD からリストする。

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   選択可能なパッケージのリストが表示されます。

   別の CD-ROM マウント・ポイントを使用する場合は、上記のコマンドでそれに置き換えてください。
3. Policy Director Base ファイルをインストールするための IVBase の選択番号を入力し、次に「Enter」を押す。

このコマンドにより、CD からファイルが抽出され、ハード・ディスク上の指定した場所にインストールされます。

IVBase パッケージのインストールが正常に行われたことを示すプロンプトが表示されます。選択可能なパッケージのリストが再度表示されます。

次のステップに進む前に、セキュア・ドメイン内には管理サーバー (IVMgr) のインスタンスは 1 つだけでなければならないことに注意してください。これがスタンドアロン・システムのインストールの場合は、次のステップに進みます。2 次サーバーにインストールする場合は、必ず、23 ページの『セキュア・ドメインのインストール要件』に目を通してください。

4. Policy Director 管理サーバー・ファイルをインストールするための IVMgr の選択番号を入力する。「Enter」を押す。

   このコマンドにより、CD からファイルが抽出され、ハード・ディスク上の指定した場所にインストールされます。

   ユーザー・レジストリー・タイプの選択を求めるプロンプトが表示されます。

5. ユーザー・レジストリーに LDAP を使用しようとする場合は、LDAP レジストリーに「2」を入力する。

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。

6. 以下に、DCE セル管理者アカウントにアクセスするために必要な情報を入力する。

   ```
   Enter the user name of the Cell Administrator [cell_admin]:
   Enter the password for the Cell Administrator:
   ```

   管理サーバーと LDAP サーバーとの間に通信を構成するよう求める一連のプロンプトが表示されます。

7. LDAP サーバー構成に必要な以下の情報を入力する。
   - LDAP サーバー・ホスト名
   - LDAP サーバー・ポート番号
   - LDAP サーバー SSL ポート番号
8. LDAP 管理者ユーザーの DN とパスワードを入力する (たとえば、`cn=root`)。これで、LDAP サーバーに Policy Director セキュリティー情報が入ります。
9. 管理サーバーと LDAP サーバー間の SSL 通信を使用可能にするか、使用不可にするかを選択する。

各 Policy Director サーバーと LDAP サーバー間の SSL 通信を、個別に使用可能にするか、使用不可にすることができます。ここでは、管理サーバーと LDAP サーバーとの間の SSL 通信を設定します。

10. SSL 通信を使用不可にした場合、このステップをスキップする。 SSL 通信を使用可能にした場合は、以下についてのプロンプトに値を指定する。
    - SSL キー・リング・ファイル位置
    - SSL キー・ラベル
    - SSL キーのパスワード
11. GSO データベース・サフィックスに DN を指定することにより GSO データベース・アクセスを使用可能にする。このサフィックスは、 31ページの『サフィックスの追加』で追加したものです。

    たとえば、以下のとおりです。

    ```
    o=IBM,c=US
    ```

    GSO データベース・アクセスが構成されると、Policy Director 構成マネージャーは DSB を自動的に構成します。一連のメッセージにより、自動化された各ステップが、完了するたびにリストされます。

    IVMgr パッケージのインストールが正常に行われたことを示すメッセージが表示されます。選択可能なパッケージのリストが再度表示されます。

WebSEAL および NetSEAL 用のセキュリティー・マネージャーのインストール

セキュリティー・マネージャー・パッケージ (IVNet) には、Base パッケージからのリソースが必要です。 IVNet をインストールする前に Base 構成要素がインストールされているか確認してください。

1. Policy Director セキュリティー・マネージャー・ファイルをインストールするための IVNet の選択番号を入力し、次に「Enter」を押す。

   ファイルが CD から抽出され、ハード・ディスク上のデフォルトのディレクトリーにインストールされます。

   ユーザー・レジストリーとして LDAP を使用する場合は、セキュリティー・マネージャーを LDAP サーバーと統合するための一連のプロンプトが表示されます。
2. プロンプトで指示された場合は、LDAP サーバー構成に必要な以下の情報を入力する。
   - LDAP サーバー・ホスト名
   - LDAP サーバー・ポート番号

- LDAP サーバー SSL ポート番号

上記の LDAP サーバー構成プロンプトは、このシステム上の他のどの Policy Director パッケージについても LDAP サーバーとの通信が以前に構成されたことがない場合にのみ表示されます。管理サーバー (IVMgr) または許可サーバー (IVAcld) がこのシステム上に構成されている場合、先に示したプロンプトはこのステップでは表示されません。

3. LDAP 管理者ユーザーの DN とパスワードを入力する。

   これで、LDAP サーバーに Policy Director セキュリティー情報が入ります。

4. セキュリティー・マネージャーと LDAP サーバー間の SSL 通信を使用可能にするか、使用不可にするかを選択する。

   各 Policy Director サーバーと LDAP サーバー間の SSL 通信を、個別に使用可能にするか、使用不可にすることができます。ここでは、セキュリティー・マネージャーと LDAP サーバーとの間の SSL 通信を設定します。

5. SSL 通信を使用不可にした場合、このステップをスキップする。 SSL 通信を使用可能にした場合は、以下についてのプロンプトに値を指定する。
   - SSL キー・リング・ファイル位置
   - SSL キー・ラベル
   - SSL キーのパスワード
6. GSO データベース・サフィックスに DN を指定することにより GSO データベース・アクセスを使用可能にする。このサフィックスは、 31ページの『サフィックスの追加』で追加したものです。

   たとえば、以下のとおりです。

   ```
   o=IBM,c=US
   ```

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。

7. 以下に、DCE セル管理者アカウントにアクセスするために必要な情報を入力する。

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

   セキュリティー・マネージャーが構成され、始動されます。

   CAS サーバーが構成され、始動されます。

   IVNet パッケージのインストールが正常に行われたことを示すプロンプトが表示されます。選択可能なパッケージのリストが再度表示されます。

WebSEAL 構成要素の使用可能化

WebSEAL 構成要素を使用可能にしたい場合は、WebSEAL (IVWeb) パッケージをインストールする。

1. WebSEAL HTTP サーバー構成要素を使用可能にするのに必要なファイルをインストールするための IVWeb の選択番号を入力する。
2. 「Enter」を押して、作業を続行する。

   ファイルが CD から抽出され、ハード・ディスク上にインストールされます。

   構成リストが、HTTP および HTTPS クライアント・アクセスを確認する値、必要なポート、およびデフォルトの Web 文書ルート・ディレクトリーを伴って表示されます。
3. 以下の画面で、現行の構成値を確認する。

   ```
   Check Web Server configuration:
   1. Enable TCP HTTP? Yes
   2. HTTP Port 80
   3. Enable HTTPS? Yes
   4. HTTPS Port 443
   5. Web document root directory /opt/Policy Director/www/docs
   a. Accept configuration and continue with installation
   x. Exit installation
   Select item to change: a
   ```
4. この構成を受け入れてインストールを続行するために「a」を入力してから、「Enter」を押す。
5. 以下に、DCE セル管理者アカウントにアクセスするために必要な情報を入力する。

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

   インストールにより、コンピューター上で WebSEAL が構成され、使用可能にされます。セキュリティー・マネージャーが自動的に再始動します。

NetSEAL 構成要素の使用可能化

NetSEAL 構成要素を使用可能にしたい場合は、NetSEAL (IVTrap) パッケージをインストールします。

1. 粗い NetSEAL TCP/IP アクセス制御構成要素を使用可能にするのに必要なファイルをインストールするための IVTrap の選択番号を入力してから、「Enter」を押す。

   NetSEAL が構成され、使用可能になります。

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。

2. DCE セル管理者アカウントにアクセスするために必要な情報を入力する。

   ivadmin コマンドを使用して保護ポートを指定する必要があることを示すメッセージが表示されます。

   もう 1 つメッセージが表示され、すべての保護ポートが NetSEAL の制御を受けるようにするためにシステムを再始動 (リブート) する必要があることを示します。

   IVTrap パッケージのインストールが正常に行われたことを示すプロンプトが表示されます。選択可能なパッケージのリストが再度表示されます。

Policy Director NetSEAL は、特定のポートに対して行われる要求をトラップします。 NetSEAL トラップを使用するには、指定されたポートを使用するすべてのアプリケーションをいったん停止してから、再始動する必要があります。Policy Director NetSEAL の構成方法の詳細は、*Policy Director 管理の手引き* に記載されている NetSEAL の概要を参照してください。

許可サーバーのインストール

許可サーバーをインストールするには、以下のように行います。

1. Policy Director 許可サーバー・ファイルをインストールするための IVAcld の選択番号を入力し、次に「Enter」を押す。

   ファイルが CD から抽出され、ハード・ディスク上のデフォルトのディレクトリーにインストールされます。

   ユーザー・レジストリーとして LDAP を使用しようとする場合は、許可サーバーを LDAP サーバーと統合するための一連のプロンプトが表示されます。

2. プロンプトで指示された場合は、LDAP サーバー構成に必要な以下の情報を入力する。

   - LDAP サーバー・ホスト名
   - LDAP サーバー・ポート番号
   - LDAP サーバー SSL ポート番号

   上記の LDAP サーバー構成プロンプトは、このシステム上の他のどの Policy Director パッケージについても LDAP サーバーとの通信が以前に構成されたことがない場合にのみ表示されます。 管理サーバー (IVMgr) またはセキュリティー・マネージャー (IVNet) がこのシステム上に構成されている場合、先に示したプロンプトはこのステップでは表示されません。

3. LDAP 管理者ユーザーの DN とパスワードを入力する。

   これで、LDAP サーバーに Policy Director セキュリティー情報が入ります。

4. 管理サーバーと LDAP サーバー間の SSL 通信を使用可能にするか、使用不可にするかを選択する。

   各 Policy Director サーバーと LDAP サーバー間の SSL 通信を、個別に使用可能にするか、使用不可にすることができます。ここでは、管理サーバーと LDAP サーバーとの間の SSL 通信を設定します。

5. SSL 通信を使用不可にした場合、このステップをスキップする。 SSL 通信を使用可能にした場合は、以下についてのプロンプトに値を指定する。
   - SSL キー・リング・ファイル位置
   - SSL キー・ラベル
   - SSL キーのパスワード

6. GSO データベース・サフィックスに DN を指定することにより GSO データベース・アクセスを使用可能にする。このサフィックスは、 31ページの『サフィックスの追加』で追加したものです。

   たとえば、以下のとおりです。

   ```
   o=IBM,c=US
   ```

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。

7. 以下に、DCE セル管理者アカウントにアクセスするために必要な情報を入力する。

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

   許可サーバーが構成され、始動されます。

   IVAcld パッケージのインストールが正常に行われたことを示すプロンプトが表示されます。選択可能なパッケージのリストが再度表示されます。

許可 API 構成要素のインストール

許可 API (C 用) ファイルをインストールするためには、IVAuthADK の選択番号を入力してから、「Enter」を押してください。

ファイルが CD から抽出され、ハード・ディスク上のデフォルトのディレクトリーにインストールされます。

IVAuthADK パッケージのインストールが正常に行われたことを示すプロンプトが表示されます。選択可能なパッケージのリストが再度表示されます。

DCE ユーザー・レジストリー付きでの Policy Director サーバーのインストール

LDAP ユーザー・レジストリー付きで Policy Director をインストールしようとする場合は、82ページの『LDAP レジストリー付きでの Policy Director サーバーのインストール』に進んでください。

サーバー・パッケージは、*IBM SecureWay Policy Director Version 3.0* CD 上の /solaris ディレクトリーに入っています。

Policy Director パッケージをインストールするためには、root ユーザーとしてログオンする必要があります。

パッケージを再インストールする必要がある場合、必要なパッケージを再インストールする前に、まず最初に既存のパッケージ (**pkgrm**) を削除してください。

管理サーバーをインストールするには、以下のように行います。

1. **pkgadd** コマンドを入力して、選択可能なパッケージを CD からリストする。

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   選択可能なパッケージのリストが表示されます。

   別の CD-ROM マウント・ポイントを使用する場合は、上記のコマンドでそれに置き換えてください。

2. Policy Director Base ファイルをインストールするための IVBase の選択番号を入力し、次に「Enter」を押す。

   このコマンドにより、CD からファイルが抽出され、ハード・ディスク上の指定した場所にインストールされます。

   IVBase パッケージのインストールが正常に行われたことを示すプロンプトが表示されます。 選択可能なパッケージのリストが再度表示されます。

   次のステップに進む前に、セキュア・ドメイン内には管理サーバー (IVMgr) のインスタンスは 1 つだけでなければならないことに注意してください。これがスタンドアロン・システムのインストールの場合は、次のステップに進みます。 2 次サーバー上にインストールしようとする場合は、必ず、23ページの『セキュア・ドメインのインストール要件』に目を通してください。

3. Policy Director 管理サーバー・ファイルをインストールするための IVMgr の選択番号を入力する。「Enter」を押す。

   このコマンドにより、CD からファイルが抽出され、ハード・ディスク上の指定した場所にインストールされます。

ユーザー・レジストリー・タイプの選択を求めるプロンプトが表示されます。

4. ユーザー・レジストリーに DCE を使用しようとする場合は、「1」を入力する。

   DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。

5. 以下に、DCE セル管理者アカウントにアクセスするために必要な情報を入力する。

   ```
   Enter the user name of the Cell Administrator [cell_admin]:
   Enter the password for the Cell Administrator:
   ```

   IVMgr パッケージのインストールが正常に行われたことを示すメッセージが表示されます。 選択可能なパッケージのリストが再度表示されます。

WebSEAL および NetSEAL 用のセキュリティー・マネージャーのインストール

セキュリティー・マネージャー・パッケージ (IVNet) には、Base パッケージからのリソースが必要です。 IVNet をインストールする前に Base 構成要素がインストールされているか確認してください。

1. Policy Director セキュリティー・マネージャー・ファイルをインストールするための IVNet の選択番号を入力し、次に「Enter」を押す。

   ファイルが CD から抽出され、ハード・ディスク上のデフォルトのディレクトリーにインストールされます。 DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。

2. 以下に、DCE セル管理者アカウントにアクセスするために必要な情報を入力する。

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

   セキュリティー・マネージャーが構成され、始動されます。

   IVNet パッケージのインストールが正常に行われたことを示すプロンプトが表示されます。選択可能なパッケージのリストが再度表示されます。

WebSEAL 構成要素の使用可能化

WebSEAL 構成要素を使用可能にしたい場合は、WebSEAL (IVWeb) パッケージをインストールする。

1. WebSEAL HTTP サーバー構成要素を使用可能にするのに必要なファイルをインストールするための IVWeb の選択番号を入力する。

2. 「Enter」を押して、作業を続行する。

   ファイルが CD から抽出され、ハード・ディスク上にインストールされます。

   構成リストが、HTTP および HTTPS クライアント・アクセスを確認する値、必要なポート、およびデフォルトの Web 文書ルート・ディレクトリーを伴って表示されます。

3. 以下の画面で、現行の構成値を確認する。

```
Check Web Server configuration:
1. Enable TCP HTTP? Yes
2. HTTP Port 80
3. Enable HTTPS? Yes
4. HTTPS Port 443
5. Web document root directory /opt/Policy Director/www/docs
a. Accept configuration and continue with installation
x. Exit installation
Select item to change: a
```

4. この構成を受け入れてインストールを続行するためには、「a」を入力してから、「Enter」を押す。
5. 以下に、DCE セル管理者アカウントにアクセスするために必要な情報を入力する。

```
Type the user name of the Cell Administrator [cell_admin]:
Type the password for the Cell Administrator:
```

   インストールにより、コンピューター上で WebSEAL が構成され、使用可能にされます。セキュリティー・マネージャーが自動的に再始動します。

NetSEAL 構成要素の使用可能化

NetSEAL 構成要素を使用可能にしたい場合は、NetSEAL (IVTrap) パッケージをインストールします。

1. 粗い NetSEAL TCP/IP アクセス制御構成要素を使用可能にするのに必要なファイルをインストールするための IVTrap の選択番号を入力してから、「Enter」を押す。

   NetSEAL が構成され、使用可能になります。

   DCE セル管理の名前とパスワードの入力を求めるプロンプトが表示されます。

2. DCE セル管理者アカウントにアクセスするために必要な情報を入力する。

   ivadmin コマンドを使用して保護ポートを指定する必要があることを示すメッセージが表示されます。

もう 1 つメッセージが表示され、すべての保護ポートが NetSEAL の制御を受けるようにするためにシステムを再始動 (リブート) する必要があることを示します。

IVTrap パッケージのインストールが正常に行われたことを示すプロンプトが表示されます。選択可能なパッケージのリストが再度表示されます。

Policy Director NetSEAL は、特定のポートに対して行われる要求をトラップします。 NetSEAL トラップを使用するには、指定されたポートを使用するすべてのアプリケーションをいったん停止してから、再始動する必要があります。Policy Director NetSEAL の構成方法の詳細は、*Policy Director 管理の手引き* に記載されている NetSEAL の概要を参照してください。

許可サーバーのインストール

許可サーバーをインストールするには、以下のように行います。

1. Policy Director 許可サーバー・ファイルをインストールするための IVAcld の選択番号を入力し、次に「Enter」を押す。

   ファイルが CD から抽出され、ハード・ディスク上のデフォルトのディレクトリーにインストールされます。 DCE セル管理者の名前とパスワードの入力を求めるプロンプトが表示されます。
2. 以下に、DCE セル管理者アカウントにアクセスするために必要な情報を入力する。

   ```
   Type the user name of the Cell Administrator [cell_admin]:
   Type the password for the Cell Administrator:
   ```

   許可サーバーが構成され、始動されます。

   IVAcld パッケージのインストールが正常に行われたことを示すプロンプトが表示されます。選択可能なパッケージのリストが再度表示されます。

許可 API 構成要素のインストール

許可 API (C 用) ファイルをインストールするためには、IVAuthADK の選択番号を入力してから、「Enter」を押してください。

ファイルが CD から抽出され、ハード・ディスク上のデフォルトのディレクトリーにインストールされます。

IVAuthADK パッケージのインストールが正常に行われたことを示すプロンプトが表示されます。選択可能なパッケージのリストが再度表示されます。

クリデンシャル取得サービスの構成

Policy Director CAS は自動的にインストールされます。 Policy Director CAS をクリデンシャル取得サービスとして使用したい場合は、それを構成する必要があります。その方法については、*Policy Director 管理の手引き* のクリデンシャル取得サービスの構成についての情報を参照してください。

管理コンソールのインストール

Policy Director は、Policy Director 構成要素の多くを管理する管理コンソールを提供します。

管理コンソール (Solaris 用) は、IVConsole インストール・パッケージを使用してインストールされます。パッケージのインストールおよび構成には、**pkgadd** を使用してください。

1. root としてログインする。
2. *IBM SecureWay Policy Director Version 3.0* CD を Policy Director サーバー・システムの CD-ROM ドライブに挿入する。
3. 以下のように入力して、選択可能なパッケージのリストを表示する。

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

4. IVBase がまだインストールされていない場合は、その選択番号を入力する。 IVBase がすでにインストールされている場合は、ステップ 6 に進む。
5. 「y」を入力して、作業を続行する。

   パッケージのリストが表示されます。
6. IVConsole の選択番号を入力する。
7. 「y」を入力して、作業を続行する。

   インストールが成功したことを示すプロンプトが表示されます。これで、管理コンソールは始動できる状態になりました。

管理コンソールの始動

管理コンソールを始動するには、以下のステップを実行してください。

1. Policy Director サーバーがインストールされ、動作していることを確認する。
2. 以下のコマンドを入力する。

```
$ /opt/intraverse/bin/ivconsole
```

Policy Director の削除

pkgrm ユーティリティーを使用して、コンピューターから Policy Director サーバーを削除します。パッケージは、インストールされたときの順序と逆の順序で削除する必要があります。コマンド **pkgrm** および **pkgadd** は、同じユーティリティー・ファミリーのメンバーであり、同じユーザー・インターフェースをもっています。 **pkgrm** は root ユーザーが実行します。

このコマンドを使用する方法はいくつかあります。

- **pkgrm** コマンドを、引き数を付けずに開始する。

  コンピューター上の現行パッケージの番号付きリストが表示されます。削除したいパッケージの選択番号を 1 つ入力します。
- **pkgrm** コマンドを開始し、コマンドに対する引き数としてパッケージ名を 1 つ指定する。たとえば、以下のようにします。

  ```
  # pkgrm IVBase
  ```
- **pkgrm** コマンドを開始し、コマンドに対する複数の引き数として一連のパッケージ名を指定する。 たとえば、以下のとおりです。

  ```
  # pkgrm IVAuthADK IVAcld IVTrap IVWeb IVNet IVMgr IVBase
  ```

pkgrm コマンドの詳細については、Solaris オペレーティング・システムの資料を参照してください。

注: Policy Director パッケージの削除は、インストールに必要な順序の逆の順で行う必要があります。

Policy Director を削除するには、以下のように行います。

1. Solaris オペレーティング・システムに root としてログインする。

   前述の **pkgrm** コマンドの開始方法のいずれかを使用します。
2. Policy Director 構成要素は、以下の順序で削除する必要があります。
   - IVTrap
   - IVWeb
   - IVNet
   - IVAuthADK
   - IVAcld
   - IVMgr
   - IVBase

コンピューター・システム構成に、前述のリストに示されているすべてのパッケージが組み込まれているとは限りません。Policy Director 管理コンソール (IVConsole) は、 IVBase より前であればいつでも削除できます。

管理コンソールの削除

管理コンソールを削除するには、以下のステップを実行してください。

1. ユーザー root としてログインする。
2. 以下のコマンドを入力する。

```
# pkgrm ivconsole
```

第8章 関連資料

本章にリストしてある資料を使用すると、Policy Director バージョン 3.0 および関連製品の詳細を入手できます。

Policy Director の資料

本書、*IBM SecureWay Policy Director 概説 バージョン 3.0* は、 Policy Director 製品と一緒に提供されるほか、文書パックでも入手できます。 Policy Director 文書パックには、本書と Policy Director ライセンス情報情報が入っています。

Policy Director に関する情報が本書のほか、以下の資料に入っており、これらの資料は、*IBM SecureWay Policy Director Version 3.0* CD のサブディレクトリー /doc にポストスクリプト文書形式 (PDF 形式) で用意されています。

- *IBM SecureWay Policy Director 管理の手引き、バージョン 3.0*

  この資料では、Policy Director を管理するための手順を詳しく解説しています。ここでは、以下のような IBM SecureWay Policy Director に関する情報が記載してあります。

  - 認証、許可、およびクリデンシャル取得といった、Policy Director の概念
  - 管理コンソールを使用して一般的な管理作業
  - WebSEAL の管理
  - NetSEAL の管理
  - NetSEAT の管理
  - 管理リソース (**ivadmin** コマンド)

- *IBM SecureWay Policy Director Programming Guide and Reference, Version 3.0*

  この資料では、許可 API 構成要素および以下の作業の実行方法について説明しています。

  - 許可 API を使用したアプリケーションの作成
  - Policy Director 許可サーバーの初期化
  - アプリケーション・サーバーまたはクライアントの認証
  - ユーザー・クリデンシャルの取得
  - 許可決定の作成
  - 任意選択タスクの実行

– クリーンアップとシャットダウン
– 許可 API を使用したアプリケーションの配置

Policy Director README ファイルには、Policy Director 情報に関する最新情報が入っており、製品の資料の内容より優先する場合があります。

最新の README ファイルを入手するには、以下の IBM SecureWay Policy Director Web サイトのライブラリー・ページにアクセスしてください。

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

IBM SecureWay FirstSecure の資料

以下の資料には、FirstSecure に関する情報が入っています。

- *IBM SecureWay FirstSecure 計画および統合の手引き バージョン 2 (SB88-8502-00)*

  この資料では、FirstSecure および FirstSecure を構成する製品について説明し、あらゆる IBM SecureWay 製品を使用する計画を始める上で役に立ちます。

IBM SecureWay Policy Director (Policy Director) は、IBM SecureWay FirstSecure の構成要素として、または独立した製品として入手できます。ご使用のバージョンの Policy Director が FirstSecure オファリングに含まれている場合、この資料は FirstSecure に付属しています。ご使用のバージョンの Policy Director が独立した製品としてご購入いただいたものである場合は、この資料を以下に示す FirstSecure の Web ページで入手できます。

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

IBM 分散コンピューティング環境の資料

以下の資料は、DCE のインストール方法について解説しており、 *IBM SecureWay Policy Director Security Services* CD のディレクトリー /doc で PDF 形式で入手するか、あるいは以下の DCE Web サイトで入手することができます。

`http://www.ibm.com/network/dce/library/`

IBM DCE for Windows NT

IBM Distributed Computing Environment for Windows NT Quick Beginnings Version 2.2 は、以下の Web アドレスで入手可能です。

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

この資料は、分散コンピューティング環境の DCE for Windows NT バージョン 2.2 について解説し、製品に合わせた計画、インストール、および構成方法について説明しています。

IBM Distributed Computing Environment for Windows NT Quick Beginnings Version 2.2 は、*IBM SecureWay Policy Director Security Services* CD の /doc/DCE22_QuickBeginnings_NT.pdf でも入手可能です。

IBM DCE for AIX

IBM Distributed Computing for AIX Quick Beginnings Version 2.2。これは、以下の Web アドレスで入手可能です。

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

この資料は、IBM 分散コンピューティング環境の DCE for AIX バージョン 2.2 (DCE 2.2 for AIX) について解説し、製品に合わせた計画、インストール、および構成方法について説明しています。

資料 *IBM Distributed Computing Environment for AIX Quick Beginnings Version 2.2* は、*IBM SecureWay Policy Director Security Services* CD の /doc/DCE22_QuickBeginnings_AIX.pdf でも入手可能です。

Transarc DCE for Solaris

Transarc DCE Version 2.0 Release Notes および *Installation and Configuration Guide* は、以下の Web アドレスで入手可能です。

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

Transarc DCE Version 2.0 Release Notes には、Transarc DCE ソフトウェアおよび資料に関する、以下の情報が記載してあります。

- 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 に関連する、判明している障害と制約事項

Transarc DCE Version 2.0 Release Notes は、*IBM SecureWay Policy Director Security Services* CD の /doc/DCE20_ReleaseNotes_Solaris.pdf でも入手可能です。

Installation and Configuration Guide には、DCE DFS 2.0 製品のインストール、構成、およびアップグレードの手順が記載してあります。

Installation and Configuration Guide は、*IBM SecureWay Policy Director Security Services* CD の /doc/DCE20_InstallGuide_Solaris.pdf でも入手可能です。

IBM SecureWay Directory の資料

以下の資料には、IBM SecureWay Directory (LDAP) のインストールおよび構成情報が記載されています。

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

  サポートされるオペレーティング・システムごとに、HTML 形式で本書の別のバージョンが収められています。各オペレーティング・システムの資料は、該当する CD の /doc/wparent.htm に収められています。 CD は、以下のものです。

  – *IBM SecureWay Directory Version 3.1.1 for NT*

  – *IBM SecureWay Directory Version 3.1.1 for AIX*

  – *IBM SecureWay Directory Version 3.1.1 for Solaris*

  LDAP のインストール後、インストールおよび構成の .HTM 文書ファイルの位置は以下のようになります。

  ```
  C:¥Program Files¥IBM¥LDAP¥nls¥html¥enUS1252¥config¥wparent.htm
  ```

HTML ファイルに入っている、以下の資料には、IBM SecureWay の管理方法に関する情報が収められています。

- *IBM SecureWay Directory Administration Guide, Version 3.1.1*

  1. Web ブラウザーを使用して、LDAP のデフォルトのインストール後に、この Web アドレスにある資料にアクセスする。

     ```
     C:¥Program Files¥IBM¥LDAP¥nls¥html¥enUS1252¥config¥wparent.ht
     ```

HTML 形式の以下の資料には、IBM SecureWay Directory クライアントに関する情報が収められています。

- *IBM SecureWay Directory Client SDK Programming Reference, Version 3.1.1*

  この資料には、以下の LDAP 情報へのリンクが含まれています。

  – LDAP Client SDK Plugin Programming Reference の情報

    1. Web ブラウザーを使用して、LDAP のデフォルトのインストール後に、この Web アドレスにある資料にアクセスする。

       ```
       C:¥Program Files¥IBM¥doc¥progref.htm
       ```

    2. 「*IBM SecureWay Directory Client SDK Programming Reference*」文書をオープンする。
    3. 「**Appendices**」をクリックする。
    4. 「**LDAP Client SDK Plugin Programming Reference**」をクリックする。

– SSL アクセスをサポートするよう LDAP サーバーを構成するための GSKit およびキー管理ツール **ikmguiw** の使用法に関する情報

1. 「*IBM SecureWay Directory Client SDK Programming Reference*」文書がまだオープンされていない場合は、オープンする。
2. 「**API categories**」をクリックする。
3. 「**SSL**」をクリックする。
4. 「**LDAP_SSL API**」をクリックする。
5. 「**Using IKMGUI**」リンクを見つけてクリックし、該当する HTML ファイルをオープンする。

以下の資料は、IBM SecureWay Directory サーバーについても使用できます。

- *IBM SecureWay Directory Server Plug-ins Reference*

付録. 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

本書に記載されている Web サイトの参照先はユーザーの皆様の便宜を図ることを目的とするものであり、いかなる意味においてもこれらの Web サイト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に関するデータは、いずれも制御された環境で決定されるものです。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。

本書に示されている価格は IBM の希望する小売価格であり、本書作成時のものですが、予告なしに変更されることがあります。販売業者によって価格は異なる場合があります。

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。

商標

以下の用語は、米国およびその他の国における International Business Machines Corporation の商標です。

AIX
DB2
FirstSecure
IBM
Policy Director
SecureWay

その他の社名、製品名、サービス名は、他社の商標やサービス・マークである場合があります。

AuthAPI	DASCOM, Inc.
DASCOM	DASCOM, Inc.
Internet Explorer	Microsoft Corporation
Netscape および Netscape のロゴ	Netscape Communications Corporation
Netscape Communicator	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM, Inc.
NetSEAT	DASCOM, Inc.
Solaris	Sun Microsystems, Inc.
WebSEAL	DASCOM, Inc.

Java、およびすべての Java ベースの商標およびロゴは、米国ならびに他の国における Sun Microsystems, Inc. の商標です。

Microsoft、Windows、Windows NT、および Windows ロゴは、米国ならびに他の国における Microsoft Corporation の商標です。

UNIX は、X/Open Company Limited がライセンスしている、米国ならびに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］

A

B

C

D

F

G

I

L

N

P

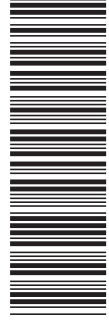
S

T

W

部品番号: CT63KJA

Printed in Japan



CT63KJA

SB88-8503-00

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