IBM® SecureWay® FirstSecure

計画および統合の手引き

バージョン 2

SB88-8502-00
(英文原典：SCT7-EHNA-00)

IBM® SecureWay® FirstSecure

計画および統合の手引き

バージョン 2

SB88-8502-00
(英文原典：SCT7-EHNA-00)

お願い

本書の情報とそこでサポートされている製品をご使用になる前に、 103ページの『付録. 特記事項』 に記載されている一般情報を必ずお読みください。

本書は、IBM SecureWay FirstSecure バージョン 2 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： SCT7–EHNA–00
IBM® SecureWay® FirstSecure
Planning and Integration
Version 2

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

図

表

本書について

IBM® SecureWay® FirstSecure は、FirstSecure とも呼ばれ、企業のために役立つ広範囲のフレームワークであり、以下のことが可能です。

- Web および他のネットワークを通したネットワーキングのすべての面の保護を行う。
- e-business に対する現在の投資の上に構築できる。モジュラー・オファリングによって、計画された展開でセキュリティーを追加することができます。
- セキュア e-business のための所有者の合計コストを削減する。

本書では、FirstSecure と FirstSecure を構成している製品について説明し、これらの製品の使用計画について概説します。

本書で説明するこれらの製品は、段階的にリリースされる製品の一部です。すべての製品が、同時に、またはすべての国で使用可能になるとは限りません。これらの製品が使用可能かどうかについては、IBM 営業担当員にご相談ください。

本書の図

本書の図は、計画の目的にのみ使用するためのものです。それぞれの図は、ユーザーの組織で適していると思われる、サーバー、クライアント、およびアプリケーションの無数にある配置のうちの 1 つを表しているにすぎません。

表示される図の形式は、ブックの配布メカニズムによって異なります。

- PDF 形式バージョンのブックのほとんどの図は、ディスク・スペースを節約するためと、印刷を速くするために、より単純化されています。
- 印刷バージョンの図はもっと複雑になっており、記憶スペースがもっと必要であり、印刷時間がかかります。

どちらのバージョンの図も、機能的には同等であり、表題や中にある文章は同じです。

本書の対象読者

本書は、Web ベースのシステムのセキュリティーについての計画と統合を行う、システム管理者を対象としています。読者は、ネットワークと自社の e-business アプリケーションについての知識をすでに持っている必要があります。

本書の構成

本書には、以下の部が含まれています。

- 1ページの『第1部 FirstSecure の概要』では、FirstSecure、その構成要素製品、および使用可能なオファリングについての概要を説明します。
- 17ページの『第2部 セキュア e-business ネットワークの計画』では、セキュア e-business ネットワークの計画について説明します。
- 57ページの『第3部 インストールと統合の考慮事項』では、インストール要件と FirstSecure 製品の統合の詳細について説明します。
- 91ページの『第16章 FirstSecure と一緒に提供される文書』では、FirstSecure で使用可能なすべての文書について説明します。
- 107ページの『用語集』では、本書で使用されているセキュリティー関連の用語を定義します。

本書にはまた、それぞれの製品の文書を記述した『参考文献』が含まれています。

西暦 2000 年対応

IBM SecureWay FirstSecure の西暦 2000 年対応について、以下に説明します。

IBM SecureWay FirstSecure の中の IBM 製品

これらの製品は、2000 年対応になっています。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。

他のベンダー製品

他の製品は、2000 年対応になっていることを IBM に表明しています。しかし、IBM は、これらの製品の 2000 年対応について、表明することも、保証することもしません。これらの製品についての 2000 年対応について質問があれば、その製品の製造元にお問い合わせください。 IBM 以外の製品およびサー

ビスに関する情報は、他社が、提供する製品およびサービスに関して提供した情報をベースにした、「Information and Readiness Disclosure」条例に基づいて『再公表』したものです。他のベンダーは、それらの製品が 2000 年対応であることを IBM に表明しています。しかし、IBM は、これらの製品の 2000 年対応について、表明することも、保証することもしません。この製品についての 2000 年対応について質問があれば、その製品の製造元にお問い合わせください。 IBM では、これらの『再公表』の内容について独立的には検証しておらず、そのような再公表に含まれた情報の完全性について、いかなる責任をも負うものではありません。

サービスおよびサポート

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。これらの製品のうちのあるものは、IBM 以外のサポートを参照しています。これらの製品を、SecureWay 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。

- **太字体**は、ユーザーが選択する項目の名前、コマンドの名前、ユーザーが入力するテキスト、または実行中のテキストの例を表します。
- モノスペースは、例 (架空のパスまたはファイル名) または画面に表示されるテキストを表します。

Web 情報

FirstSecure の最新の更新についての情報は、インターネットの www.ibm.com/software/security の以下のロケーションで入手できます。

IBM SecureWay FirstSecure

www.ibm.com/software/security/firstsecure

文書は www.ibm.com/software/security/firstsecure/library で入手できます。

IBM SecureWay Policy Director

www.ibm.com/software/security/policy

文書は www.ibm.com/software/security/policy/library で入手できます。

IBM SecureWay Boundary Server

www.ibm.com/software/boundary

文書は www.ibm.com/software/boundary/library で入手できます。

IBM SecureWay Trust Authority

www.ibm.com/software/security/trust

文書は www.ibm.com/software/securitytrust/library で入手できます。

ITSO レッドブック *Understanding the IBM SecureWay FirstSecure Framework*, SG24-5498-00 は、インターネットの www.ibm.com/redbooks で入手できます。

第1部 FirstSecure の概要

この部では、FirstSecure およびその構成要素製品の概要を説明します。ここには、各製品についての概略説明が含まれています。

この部ではまた、IBM Implementation Services についても説明します。

第1章 FirstSecure とは何か

IBM SecureWay FirstSecure は、IBM の統合セキュリティー・ソリューションの一部です。 FirstSecure は、以下のことを企業が行うのを援助する、広範囲の組み立てブロックの集まりです。

- セキュア 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・ポリシーをより容易に導入する。
- より効果的な e-business 環境を作成する。

FirstSecure 構成要素には、ウィルス保護、不法侵入の検出、アクセス制御、トラフィック内容の制御、暗号化、ディジタル証明書、ファイアウォール・テクノロジー、およびアプリケーション開発ツールキットが含まれています。これらの機能は、IBM SecureWay セキュリティー製品ファミリーによって、ならびに複数のセキュリティー・ベンダーの最適な構成要素を組み合わせた、他のベンダーからのオファリングによって提供されます。さらに、選択された FirstSecure 構成要素に対しては、Implementation Services が利用可能です。 FirstSecure の組み立てブロックには、以下のものがあります。

- SecureWay Policy Director
- SecureWay Boundary Server
- Intrusion Immunity
- Public Key Infrastructure (IBM SecureWay Trust Authority により提供)
- IBM SecureWay Toolbox

FirstSecure は独立してインストールすることができる製品の集合であるため、セキュリティー機能のある環境に、計画を立てて移行することができます。ある 1 つの分野から開始して、改善の程度を確認しながら、さらに継続してセキュリティー機能を高めることができます。これによって、複雑さとコストが低減され、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 がなぜ必要か

データとリソースは、e-business にとって最も重要なものです。さらに、 FirstSecure 製品は、以下のものを提供します。

許可 だれでもが、従うべき規則を持ちます。「許可」は、承認されたユーザーに、システム、データ、アプリケーション、およびアプリケーションのアクセスを認めます。

責任能力
だれが、何をいつ実行したかがわかります。「責任能力」により、だれがアクションを行い、指定された時間間隔の間にどのアクションが発生したかを判別することができます。

確認 システムが予定どおりにセキュリティーを保持しているかどうかを確認できます。この保護によって、要求されたレベルのセキュリティー保護が実施されていることを、証明および検証することができます。

可用性 システムが、必要なときにいつでも使えます。この保護は、システム、データ、ネットワーク、およびアプリケーションを、従業員、サプライヤー、パートナー、および顧客がいつでも使用可能なように保持するのに役立ちます。

管理 システム管理者が規則を定義できます。この保護により、ポリシー情報の定義、維持管理、監視、および変更ができます。

これらの保護は、企業全体のポリシーに基づいて設定し、企業内のネットワーク、システム、およびアプリケーションの全セットに渡る、保護のメッシュを提供することができます。そのメッシュ内の製品間に 1 つでも危険性のあるリンクが存在すると、残りのインフラストラクチャーが無用のものになってしまう可能性があります。

本書では、SecureWay の組み立てブロックとなる製品のそれぞれを、提供されている保護のリストと結び付けています。

FirstSecure の組み立てブロックとなるものは何か

FirstSecure には、すべての製品を 1 つのグループとして入手するか、または別々の関連製品として入手できる、構成要素の製品が含まれています。つまり、これらの製品は、1 つまたは複数の構成要素の製品を持っている場合があります。任意の製品から始めて、完全なセキュリティー・ソリューションを構築することができます。

Policy Director

Policy Director は、セキュリティー計画の中心となるものです。 Policy Director は、地理的に分散しているイントラネットとエクストラネット上に存在する Web リソースについて、終端間のセキュリティーの許可と管理を提供します。 Policy Director は、認証、許可、データ・セキュリティー、およびリ

ソース管理を提供します。 Policy Director を標準のインターネット・ベースの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を構築できます。 Policy Director には、以下のものが含まれます。

- セキュリティー・サービス
- 管理コンソール
- 管理サーバー
- セキュリティー・マネージャー (NetSEAL および WebSEAL)
- NetSEAT クライアント
- ディレクトリー・サービス・ブローカー
- 許可サーバー (第三者アプリケーション・サポート)

Policy Director は、Windows NT、AIX、および Solaris で実行されます。

Policy Director についてのより詳細な説明は、35ページの『第5章 ネットワークにおける Policy Director の計画』を参照してください。

SecureWay Boundary Server

SecureWay Boundary Server 製品は、Web ベースの e-business アプリケーションに対する、確認、管理、および責任能力を提供します。セキュア境界がどこにでも (技術部門と人事部門などの部門の間、本社ネットワークとリモート・オフィスの間、社内ネットワークとインターネットの間、社内の Web アプリケーションと顧客の間、および社内ネットワークとビジネス・パートナーの間) 必要です。適切な境界セキュリティーを達成するためには、そのネットワークをアクセスできる人と、ネットワークに出入りする情報との両方を制御する必要があります。

本節では、SecureWay Boundary Server の組み立てブロックについて説明します。計画と統合の考慮事項については、63ページの『第12章 SecureWay Boundary Server の要件とインストールの注意点』を参照してください。

IBM SecureWay Firewall

IBM SecureWay Firewall は、IBM Firewall とも呼ばれ、インターネットとの間のすべての通信を制御することによって、安全な、セキュア e-business を可能にします。 IBM Firewall は、高いレベルのセキュリティーと柔軟性の両方を与える、 3 つの重要なファイアウォール (フィルター処理、プロキシー、およびサーキット・レベル・ゲートウェイ) を提供します。

ACE/Server

Security Dynamic の ACE/Server には、SecurID トークン (2 ユーザー・ライセンスおよび 2 トークン) が含まれています。 ACE/Server は、IBM SecureWay Firewall に対して、管理者ログオンと*仮想私設網* (VPN) 接続を追加します。

MIMEsweeper for IBM SecureWay リリース 2

Content Technology の MIMEsweeper には、インターネット・セキュリティーのための構成要素が含まれています。 MAILsweeper は、電子メールを検査して、機密情報が e-business から出ていかないこと、および許可されない電子メールが入ってこないことを確認します。

WEBsweeper は、希望しない Web データがビジネスに入り込まないよう保持します。この製品は、許可された Java アプレット、実行可能コード、または Web サイトからのみ、データをスキャンして受け入れます。

SurfinGate

Finjan Software Ltd. の SurfinGate は、e-business のためのモバイル・コードのセキュリティー・ソリューションです。モバイル・コードは、現在では、イントラネットの外部から e-business に、自動的かつ定常的にしばしば入ってくるので、ファイアウォールよりも高度に保護する必要があります。 SurfinGate は、ネットワークを Java、ActiveX、および JavaScript コードからのハッキングから保護します。この製品は、敵意のあるハッキングを識別して、ネットワークに侵入する前に、重要なリソースから遠ざけるようにします。この製品は、疑わしいデータを検査して、それを受け入れる前に隔離します。

Intrusion Immunity

Intrusion Immunity は、企業での検出と保護のための製品という形で、「保証」を提供します。 Intrusion Immunity の要件については、71ページの『第13章 Intrusion Immunity の要件とインストールの注意点』を参照してください。
Intrusion Immunity には、Tivoli Cross-Site for Security と Norton AntiVirus が含まれます。

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security は、ハッキングの危険性のあるシステムに対する、不法侵入の検出を提供します。 Tivoli Cross-Site for Security を使用すれば、以下のことが可能になります。

- ネットワークに Cross-Site for Security エージェントをインストールして、疑わしい問題を Cross-Site for Security 管理サーバーに報告する。
- あらかじめ定義されたカスタム・レポートで、不法侵入のデータを見る。

- 許可されていない、疑わしい活動をリアルタイムに検出してログに記録する。
- セキュリティー・エージェントをチューニングして、偽のアラームの回数を減らす。

Norton AntiVirus

Symantec Corporation の製品である Norton AntiVirus は、世界でも先進的なアンチウィルスのソフトウェア製品です。 Norton AntiVirus は、バックグラウンドで常に実行して、ウィルスからコンピューターを安全に守るのを援助します。ウィルスは、電子メールの添付、ActiveX コントロール、 Java アプレット、インターネットのダウンロード、ディスケット、ソフトウェア CD、またはネットワークを通して送られたファイルから入ってくる可能性があります。 Norton AntiVirus を使用すれば、ウィルスに感染したファイルを隔離することができます。 Norton AntiVirus を構成して、更新されたウィルスおよび新しく発見されたウィルスを自動的に通知させることができます。

Public Key Infrastructure

IBM FirstSecure は、IBM SecureWay Trust Authority を提供することによって、暗号と相互操作性についての Public Key Infrastructure (PKI) 標準をサポートします。

SecureWay 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するセキュリティー・ソリューションです。これらの証明書は広範囲のインターネット・アプリケーションで使用することができ、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。 Trust Authority は、*Internet Engineering Task Force* (IETF) の *Public Key Infrastructure* (PKI) Working Group の仕様に基づいてします。この製品には、以下のものが含まれます。

- IBM AIX および Microsoft Windows NT サーバーのサポート
- 登録局 (RA)
- 認証局 (CA)
- 証明書を要求し、発行された証明書を管理するためのユーザー・インターフェース
- 統合された *IBM SecureWay Directory*
- 監査 サブシステム
- SecureWay 4758 暗号コプロセッサーのサポート
- スマート・カード のサポート

このインフラストラクチャーは、完全な証明書のライフ・サイクル (登録と最初の証明、キー・ペアの更新、証明書の更新、証明書と証明書取り消しリストの発行、および証明書取り消し) をサポートします。詳しくは、79ページの『第14章 Public Key Infrastructure の要件とインストールの注意点』を参照してください。

Toolbox

FirstSecure Toolbox は、1 組のセキュリティーとセキュリティー関連のツールキットであり、 FirstSecure の主要な構成要素の一部であるか、またはそれらと相互操作が可能なものです。ツールキットは、以下のことを行うのに役立ちます。

- アプリケーションを FirstSecure に統合する。
- FirstSecure を使用するソリューションおよびアプリケーションをカスタマイズする。
- FirstSecure を利用する ISV および OEM アプリケーションを作成する。

FirstSecure Toolbox ツールキット API は、以下のセキュリティー機能をサポートします。

- 許可サービス
- 証明および管理サービス
- ディレクトリー・サービス
- セキュア・ソケット・レイヤー・プロトコル・サービス
- KeyWorks 暗号およびトラスト管理サービス
  - IBM Key Recovery Service Provider 1.1.3.0 API。 IBM Key Recovery Service Provider により、暗号化された情報の回復が可能になります。
  - IBM Key Recovery Server 1.1.3.0。IBM Key Recovery Server 1.1.3.0 は 1 つのアプリケーションであり、許可された要求があると、キーが使用不能になるか、失われるか、または損傷を受けたときに、暗号化された情報を回復することができます。

    これらの 2 つのツールキットは、セキュリティー・プロバイダーがツールキットにプラグインするために使用できる標準インターフェースだけでなく、アプリケーションが重要なセキュリティー・サービスを起動するために使用できる標準インターフェースを提供します。標準インターフェースは、共通データ・セキュリティー・アーキテクチャー (CDSA) に基づいています。これらのツールキットは、Windows NT、Solaris、および AIX で使用可能です。

Implementation Services

FirstSecure Implementation Services を使用すれば、e-business で、FirstSecure を速やかに、かつ効率的に立ち上げて、実行することができます。これらの別料金になったサービスは、IBM によって提供され、経験のあるコンサルタント・チームによって実施されます。 FirstSecure Implementation Services には、FirstSecure Implementation Workshop と製品レベルの QuickStart インストール・サービスが含まれています。 IBM では、ユーザーの個々の環境に合わせてカスタマイズされた、 FirstSecure システム統合サービスを提供することもできます。

この情報と価格オプションについては、IBM 担当員に問い合わせてください。

第2章 リリース 2 の新機能

リリース 2 では、IBM SecureWay FirstSecure 製品の計画とインストールを単純化しています。個々の製品がさらに統合され、製品が追加されており、管理と制御がより集中化されています。

Policy Director

Policy Director は、以下の機能強化が行われています。

- 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 Directory 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 Firewall 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の選択。
- ログインとパスワード・ポリシーを管理するための、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。
- 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・ターゲット・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。

SecureWay Boundary Server

SecureWay Boundary Server は、以下の機能強化が行われています。

- SecureWay Boundary Server と Policy Director の一部の機能を一緒に結び付ける、構成 GUI。
- SecureWay Boundary Server と Policy Director の一部の機能を一緒に結び付ける、新しい構成 TaskGuide。

AIX および NT 版 IBM SecureWay Firewall の新機能

IBM SecureWay Firewall (IBM Firewall とも呼ばれる) は、以下の機能強化が行われています。

セキュア・メールのプロキシーの拡張

IBM Firewall Secure Mail Proxy は、以下の新しい機能が含まれるよう機能強化されています。

- わかっている spam (迷惑メール) 発信者からのメッセージのブロック (除外リスト) を含む spam 防止アルゴリズム、メッセージの妥当性と応答能力の検査 (希望しないメッセージをブロックする方法として知られている)、メール・メッセージの宛先の数の構成可能限界、メッセージの最大サイズの構成可能限界
- 強力な認証メカニズムの統合を含む詐称防止サポート
- SNMP トラップ・サポートおよび MADMAN MIB のサポート
- ファイアウォールとドミノ間のメッセージを継ぎ目なく追跡するための機能を含むメッセージ追跡

Socks プロトコルのバージョン 5 の機能強化

Socks プロトコルのバージョン 5 は、ユーザー名とパスワードの認証 (UNPW)、チャレンジ / 応答認証 (CRAM)、および認証プラグインを含むようアップグレードされました。

ログ記録は、ログ・メッセージのクラス分けと、ログ・レベルの指定について、ユーザーがさらに制御できるよう機能強化されています。

HTTP プロキシー

IBM SecureWay Firewall は、IBM Web Traffic Express (WTE) 製品に基づいた、完全装備の HTTP プロキシーを提供します。 HTTP プロキシーは、IBM Firewall を通したブラウザー要求を効率的に処理するものであり、Web のブラウズのための socks サーバーが必要なくなります。ユーザーは、内部ネットワークのセキュリティーを損なうことな

く、しかも HTTP プロキシーを導入するためにクライアント環境を変更することなく、インターネット上の便利な情報にアクセスすることができます。

リモート・アクセス・サービス

Windows NT リモート・アクセス・サービス (RAS) は、2 地点間プロトコル (PPP) を使用して、ダイヤル呼び出し、ISDN、または X.25 媒体を介したネットワーク接続を提供します。 NDISWAN はネットワーキング・ドライバーの 1 つであり、RAS の一部として提供され、下部の PPP データを類似のイーサネット LAN データに変換します。

AIX に対する IBM SecureWay Firewall の機能強化

AIX 版の IBM SecureWay Firewall は、多くの拡張機能を提供します。

拡張 IPSec サポート

拡張 IPSec サポートには、新しいヘッダーのサポートが含まれています。これはまた、いくつかの IBM サーバーとルーターの相互操作、ならびに新しいヘッダーをサポートする多くの IBM 以外の VPN 製品の相互操作もサポートします。

マルチプロセッサー (MP) サポート

ファイアウォールのユーザーは、スケーリングとパフォーマンスの向上のために、RS/6000 のマルチプロセッサー・フィーチャーを活用することができます。

フィルターの機能強化

構成で、パフォーマンスが向上し、柔軟性が増します。異なるタイプのフィルター規則をどこに配置するかを選択することによって、 IBM SecureWay Firewall のパフォーマンスをチューニングすることができます。頻度標識は、ある接続が使用された回数を提供します。

ネットワーク・アドレスの変換

多対 1 のアドレス・マッピングをサポートします。これらのマッピングは、複数の内部の未登録または私用のアドレスから、ポート番号を使用した登録済みの正規のアドレスに対して行うもので、固有のマッピングを作成します。

セットアップ・ウィザード

IBM Firewall の初期構成を援助するウィザードです。このセットアップ・ウィザードを使用すれば、IBM Firewall に関する広範囲の知識を持たないユーザーでも、インストール後に、基本構成を速やかに立ち上げて、実行することができます。

Network Security Auditor

Network Security Auditor (NSA) は、ネットワーク・サーバーおよび IBM Firewall に、セキュリティー上の抜け穴や構成エラーがないかどうかを検査します。これは、より高速で、強力になりました。

MIMEsweeper for IBM SecureWay リリース 2 の新機能

MAILsweeper の機能強化には、以下のものがあります。

- いやがらせや中傷のメールをブロックしたり、会社を退職する人が価値あるデータを持ち出さないよう保護するために、キーとなる語をスキャンする
- 着信する不要な電子メールをブロックする
- 個人またはグループが指定されたタイプのファイルを受信または送信するのをブロックする
- ネットワークの競合を避けるために、ファイルをサイズごとにブロックするか遅らせる

WEBsweeper の機能強化には、以下のものがあります。

- 仕事に無関係と思われる指定されたサイトからの従業員の通信をブロックする
- HTML または電子メール・アドレスを介した文書および cookie を介したサイト情報が、ハッキングで抜き出されるのを防止するのを援助する

SurfinGate の新機能

SurfinGate は、以下の機能強化が行われています。

- JavaScript の内容の検査
- 重要な任務を持つもののパフォーマンスの監視
- ポリシー管理の強化
- ファイル転送プロトコル (FTP) と HTTPS プロトコルのサポート
- ファイアウォール HTTP プロキシーとのプラグイン統合
- 特定の実行ファイルがユーザーのコンピューターにダウンロードされるのをブロックする機能

Intrusion Immunity

Intrusion Immunity 製品には、 Tivoli Cross-Site for Security が組み込まれるようになりました。

Tivoli Cross-Site for Security の新機能

Tivoli Cross-Site for Security は、不法侵入の検出を提供します。これを使用して、e-business の完全性に対するネットワーク・ハッキングを監視することができます。

Norton AntiVirus Solution Suite の新機能

Norton AntiVirus Solution Suite リリース 3.0.4 には、以下の更新済みバージョンが含まれています。

- Norton AntiVirus 5.02 (Windows 95/98 および Windows NT ワークステーション用)
- Norton AntiVirus 5.02 (Windows NT サーバー用)
- Norton AntiVirus (IBM OS/2 5.02 用)
- Norton AntiVirus OS/2 (Lotus Notes 2.0 用)
- Norton AntiVirus (Lotus Notes 2.0 用)
- Norton AntiVirus (Microsoft Exchange 1.5.2 用)

Public Key Infrastructure

Public Key Infrastructure 構成要素は、Trust Authority を含むようになりました。 Trust Authority は、以下のものが含まれます。

- Windows NT で簡単にインストールできるようガイドするインストール・ウィザード。
- 4758 暗号カード用の事前設定構成。この情報を変更することができます。
- バックグラウンド構成プログラムが開始する前にデータの妥当性を検査する、構成ウィザード。
- エラー・メッセージおよびレポート作成。
- オンライン文書 (セットアップ・ウィザード、Registration Authority Desktop、およびエンド・エンティティー・クライアント・アプリケーションに対するコンテキスト依存のヘルプを含む)。

IBM SecureWay Toolbox

Toolbox は、以下の機能強化が行われています。

- Policy Director API および文書。
- ディレクトリー・サービス API。
- Public Key Infrastructure (PKIX) API および文書。
- IBM Key Recovery Server 1.1.3.0 が、Toolbox の中に組み込まれるようになりました。これは、英語版のみが使用可能です。

第2部 セキュア e-business ネットワークの計画

第 2 部では、セキュア e-business ネットワークの計画について説明します。

以下の章では、典型的なインターネットのトラフィックとセキュリティーの問題について説明し、次に、e-business ネットワーク内で FirstSecure 製品がどのように作動するかについて説明します。

この部には、以下の章が含まれています。

- 19ページの『第3章 e-business ネットワークの概要』では、典型的な e-business ネットワークと、ネットワーク内に存在するユーザー、リソース、および対話の種類について説明します。ご使用のネットワークは、ここで説明するネットワークよりもフィーチャーが多いかまたは少ない場合がありますが、同じセキュリティー上の問題があり、同じセキュリティー保護が必要です。
- 31ページの『第4章 e-business ネットワークにおける FirstSecure の計画』では、FirstSecure 製品をネットワークに結合します。
- 35ページの『第5章 ネットワークにおける Policy Director の計画』
- 39ページの『第6章 ネットワークにおける SecureWay Boundary Server の計画』
- 45ページの『第7章 ネットワークにおける Intrusion Immunity の計画』
- 51ページの『第8章 ネットワークにおける Public Key Infrastructure の計画』

第3章 e-business ネットワークの概要

e-business ネットワークは、リソース (データおよびデータベース、ユーザー、顧客、サプライヤー、プログラマー、ハードウェア、企業情報など) から構成されています。以下に、これらのエリアを挙げ、どこにセキュリティーが必要かを説明します。

インターネットは、複合した作成物です。データは、サーバーからサーバーへ、およびユーザーからユーザーへと転送されますが、そのパスは、伝送のたびに変更されるため未定義です。

インターネットを通して伝送されるビジネス・データは、その他のすべてのインターネット・トラフィックと混じり合っています。このようにして、ビジネスにとって重要なデータが、どこかのサーバーを通して、どこにでも渡される可能性があります。また、いずれかのインターネット・ユーザーが、この企業のリソース、従業員、およびデータにアクセスしようと試みる場合があります。残念なことに、インターネットは、教育、ビジネス、および娯楽のための合法的なトラフィックだけでなく、意図的である場合とそうでない場合の両方で、悪意を持ったトラフィックも伝送されます。 20ページの図1 は、インターネットの様子を示したものであり、トラフィックが、他のすべての人のトラフィックでいっぱいのインターネットを介して渡されています。

FirstSecure は、自分の伝送を他のすべてのトラフィックと分離して保護するのに役立ちます。

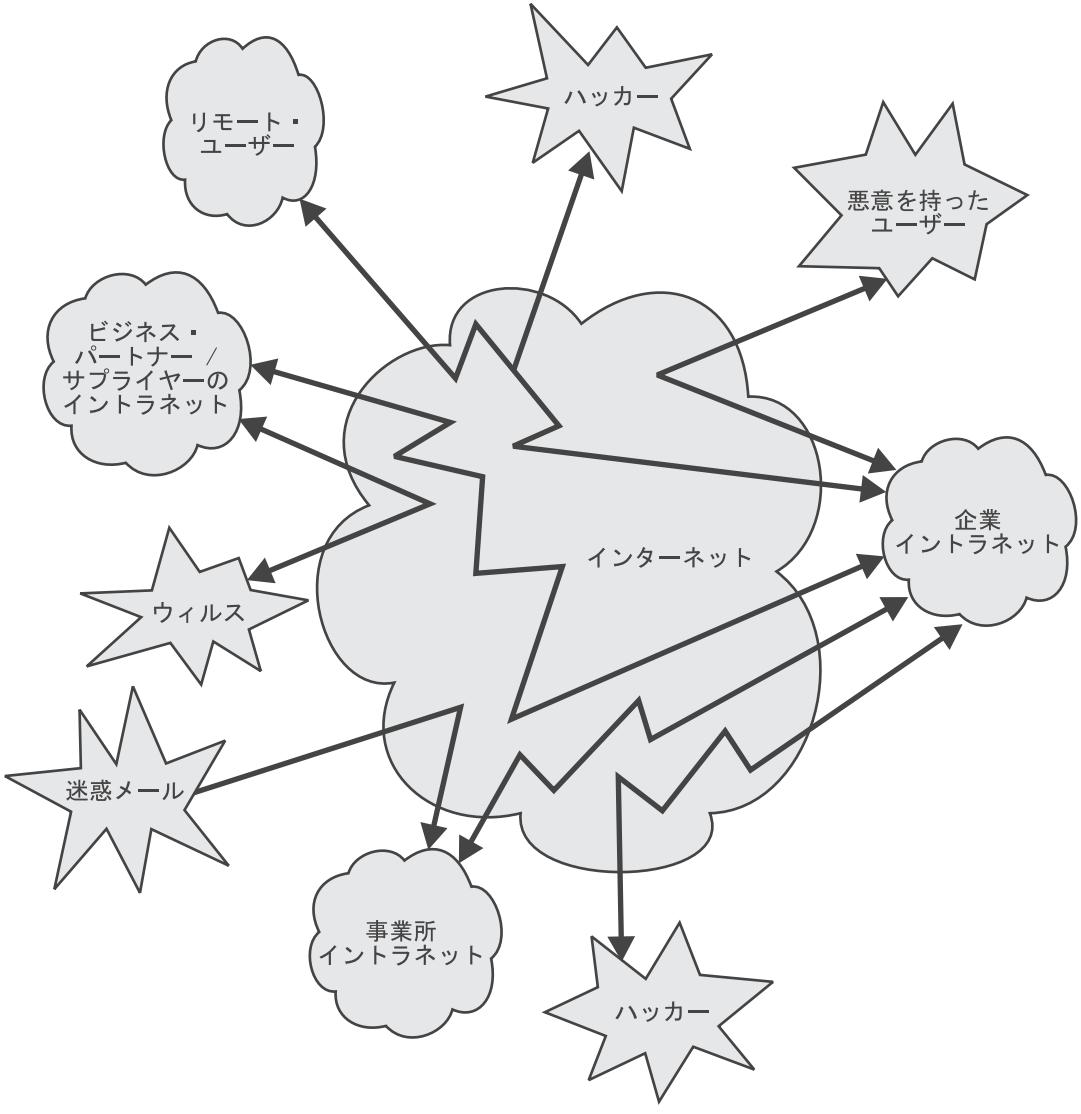


図 1. 無関係の活動でいっぱいになったインターネットの概要

このような状態のインターネットでは、操作したくはありません。 21ページの図2 に示すように、インターネットが FirstSecure によって保護された状態にしたいはずです。

FirstSecure によって保護された理想的なインターネット

e-business のトラフィックの多くは、インターネットを介して行われます。しかし、大量のランダム・データの集まりが、ホーム・コンピューターを使用してほとんど誰でもが見ることができるという、典型的なインターネットの形態を希望するわけではありません。 図2 に、望ましいインターネットを示します。

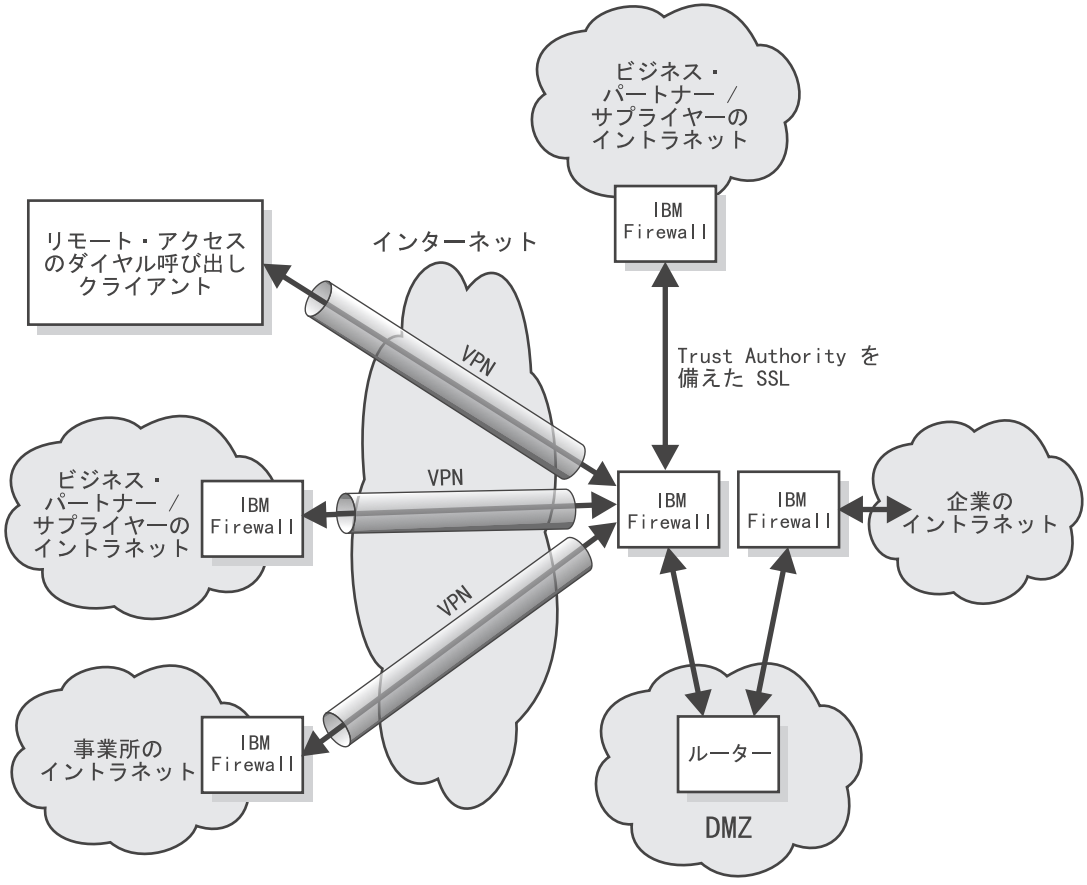


図2. 望ましいインターネット

インターネットを介した多くの良質の情報がある一方で、そこからビジネスを防御したいアプリケーション、データ、およびアクセスがあります。以下のことが確実に行われるようにする必要があります。

- 従業員が、気を散らすことなく割り当てられた作業を行える。
- 従業員が、不適切な電子メールから保護される。

- 機密性のあるビジネス情報が、外部に漏れない。

仮想私設網

仮想私設網 (VPN) は、他からアクセスできない、インターネットを介した私用接続の概念です。 図3 に、典型的な VPN を示します。この接続では、それぞれの端のユーザーは、希望しないユーザーまたはアプリケーションからの不法侵入に対して保護されます。 IBM SecureWay Firewall などの FirstSecure 製品は、VPN のセットアップとサポートを援助します。

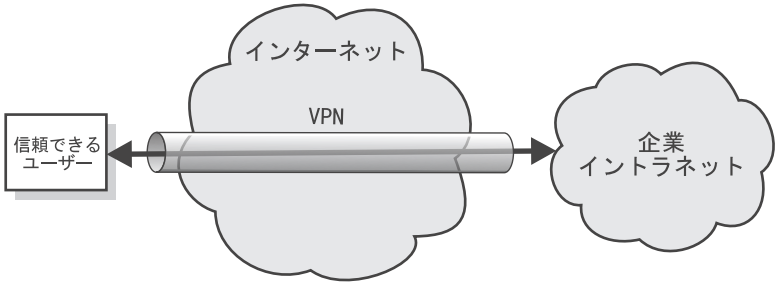


図 3. 典型的な仮想私設網

非武装地帯 (DMZ)

非武装地帯 (DMZ) は、外部のユーザーにアクセスを許すリソースの本体です。 IBM Firewall、MIMEsweeper、および他の FirstSecure 製品を使用すれば、希望するユーザーだけが DMZ にアクセスでき、しかも指定されたリソースだけをアクセスできるようにできます。 DMZ に出入りするトラフィックは、それが適切かどうかを判断するために監視すべきです。

企業のカタログは、潜在的な顧客がブラウズできるよう、DMZ に入れておいてもかまいません。あるいは企業の内容を記述した、パンフレットを入れてもかまいません。 FirstSecure 構成要素を使用すれば、信頼できるユーザーだけが、DMZ を越えて情報にアクセスするようにできます。

23ページの図4 に、典型的な DMZ を示します。

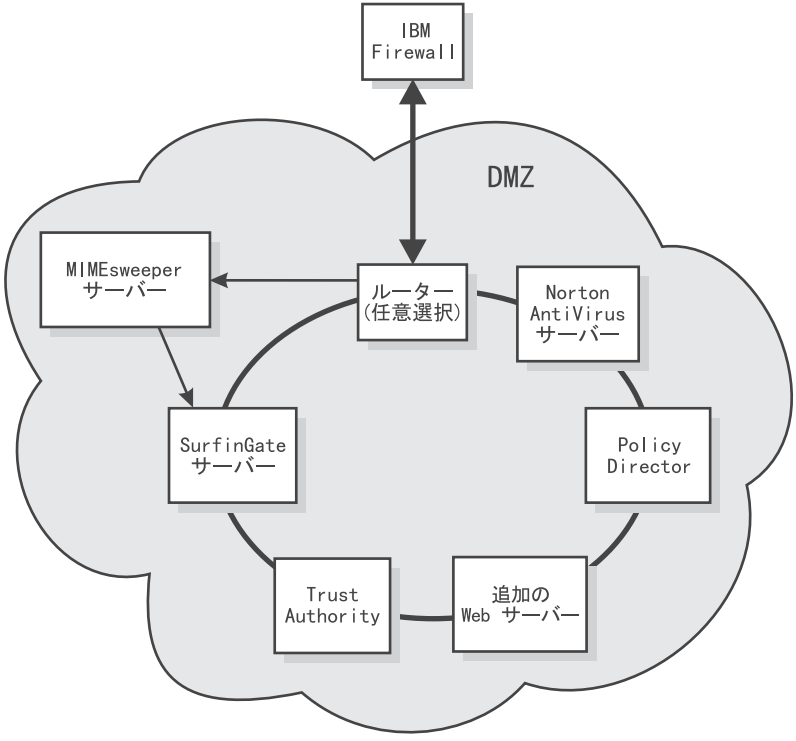


図 4. システム・リソースを備えた典型的な DMZ

保護アプリケーションを開発する際に、これらのアプリケーションに対する共通アクセスを許可する前に、イントラネット・テスト・ベッドとして DMZ を使用することができます。

次に、インターネットとイントラネットで使用する情報の種類について説明します。

典型的な企業イントラネット

企業イントラネットは、企業内で通信を行う場所です。企業イントラネットには、インターネットとは共用できない情報とリソースが含まれています。従業員は、データを共用し、お互いに電子メールを送り、データベース、プリンター、およびスキャナーなどの企業リソースにアクセスします。 24ページの図5に、典型的な企業イントラネットを示します。

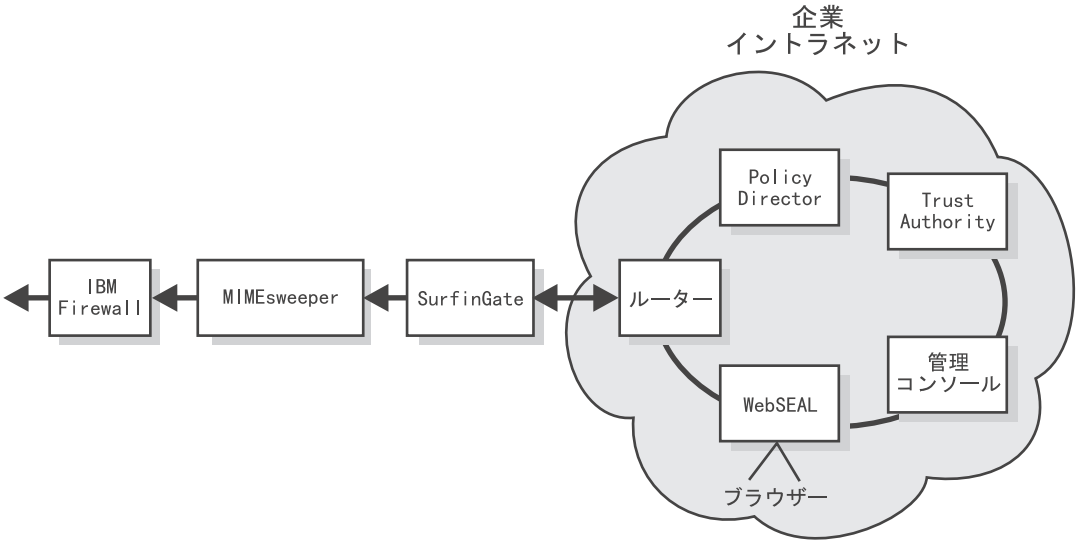


図5. 典型的な企業イントラネットの概要

企業の機密情報が企業内にとどまり、許された人だけがそのデータへのアクセスを許されるようにしなければなりません。ただし、顧客に使用させ、アクセスさせたいデータも一部あります。たとえば、取り引き銀行の預金係に対しては、会計勘定を検査できるようにはしたいが、雇用記録にはアクセスさせたくありません。 IBM Firewall は、プライベート情報をプライベート用として保持します。

IBM FirstSecure 製品は、イントラネットを保護するのに役立ちます。 Policy Director を使用して、アクセス規則を設定することができます。 IBM SecureWay Trust Authority により、ユーザーが、本人であるかどうかを確認できます。 Tivoli Cross-Site for Security によって、イントラネット・リソースに対する無許可のアクセスの試みがあるかどうかを知ることができます。

典型的な企業の事業所イントラネット

事業所にいるリモートの従業員は、本社の従業員と同じデータやその他のリソースをアクセスする必要があります。しかし、情報の送受信のための電話接続は、速度が遅く、悪意を持った妨害に対する保護がありません。しかし、コスト削減の手段として、およびトランザクションに保護を加える手段として、インターネットを使用したいとします。 25ページの図6 は、インターネットを介して中央のオフィスと通信を行う、典型的な事業所を示したものです。

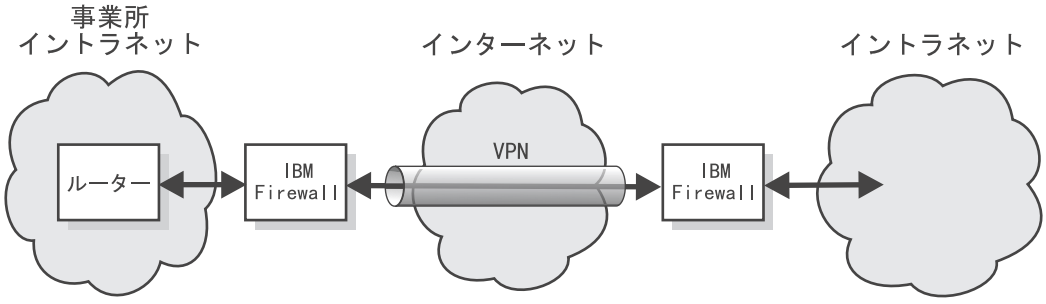


図 6. VPN (仮想私設網) を介してメイン・オフィスに接続された事業所

伝送およびデータが、企業内で 1 つの場所にあるかのように保護されるようにしたいとします。*仮想私設網* (VPN) は、インターネットを介したトンネルです。インターネットを、私設のイントラネット・ネットワークであるかのように使用することができます。

典型的なリモート・アクセスの従業員

従業員の一部は、一時的または永続的に、メイン・オフィスと離れたリモートで働きます。従業員は、ダイヤル呼び出しを使用したインターネットまたは専用回線接続を介して、メイン・オフィスのネットワークにアクセスする場合があります。

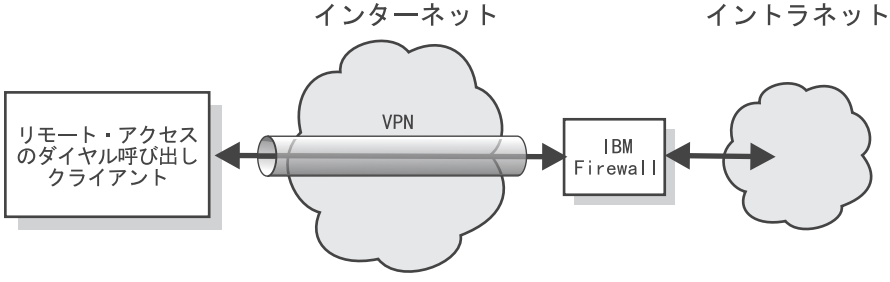


図 7. VPN (仮想私設網) を介してメイン・オフィスに接続されたリモート・アクセスのダイヤル呼び出しクライアント

IBM Firewall は、この従業員の伝送を保護します。

典型的なビジネス・パートナーまたはサプライヤーのイントラネット

ビジネス・パートナーやサプライヤーが一部のデータを直接アクセスできれば、ビジネスはもっと効率的になります。あるサプライヤーは、在庫レベルを検査して、指定されたレベルになるよう在庫品を補充することが許されている場合があります。また、別のビジネス・パートナーは、選ばれたレコードにアクセスできる場合があります。会計士は、他の税金のレコードはアクセスする必要があるが、ビジネス・パートナーのレコードにはアクセスする必要はありません。 図8 と 27ページの図9 は、典型的なサプライヤーまたはビジネス・パートナーを示したものです。ビジネス・トランザクションを、専用回線接続を介して伝送するかのように、インターネットで送りたいとします。

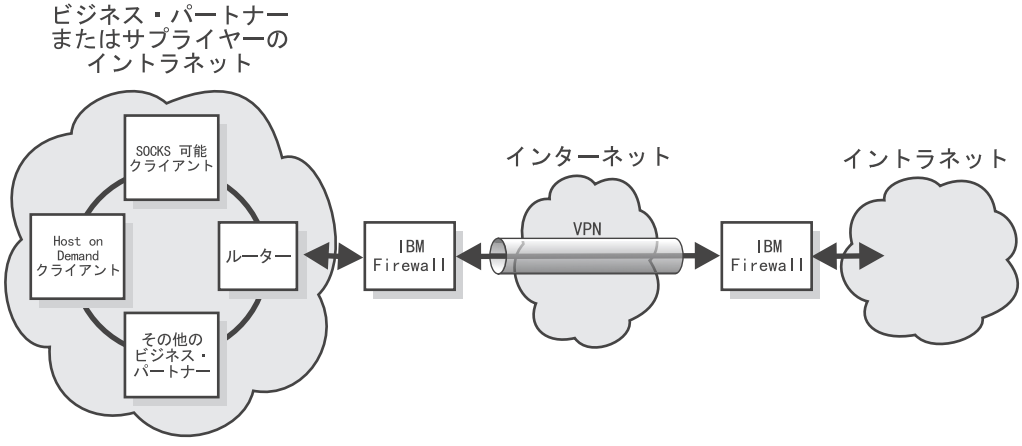


図 8. 仮想私設網 (VPN) を使用した典型的なビジネス・パートナーまたはサプライヤーのイントラネット

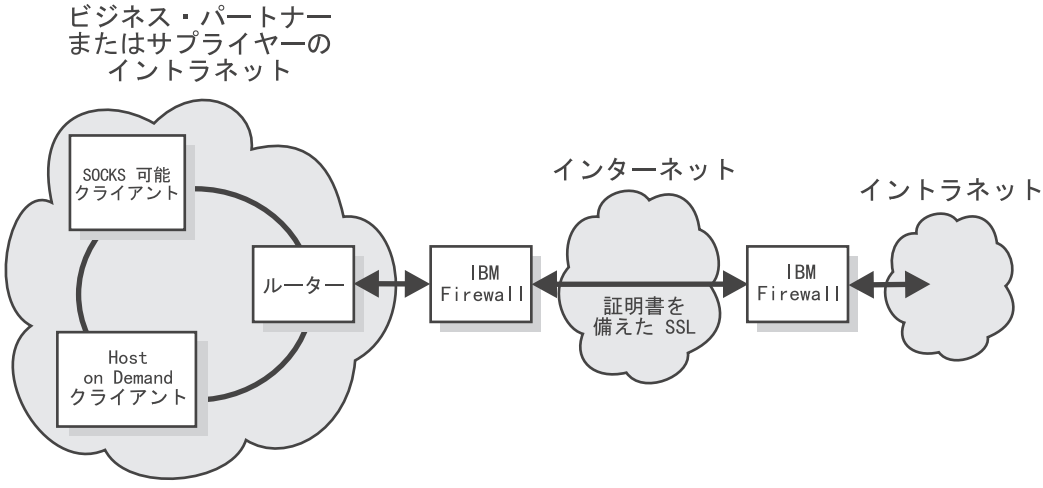


図 9. セキュア・ソケット・レイヤー (SSL) を使用した典型的なビジネス・パートナーまたはサプライヤーのイントラネット

このビジネス・パートナーは、伝送が終端から終端まで暗号化されるので、VPN を使用する代わりにセキュア・ソケット・レイヤー (SSL) を使用しています。 (ユーザーは、1 つの追加のセキュリティー層として VPN を使用することもできます。)

これらのユーザーは、ユーザー相互間、悪意ある妨害、および不法侵入から保護する必要があります。これらのユーザーのデータ伝送は、無許可の受信者や無許可の送信者から保護する必要があります。また、これらのユーザーが許されたデータだけをアクセスするようにする必要があります。さらに、これらの各ユーザーが、そのユーザー本人であることを確認したい場合があります。

データおよびデータベース

データは、どのビジネスでも所有している、もっとも価値あるリソースの 1 つです。一部の e-business データは、すべてのインターネット・ユーザーが使用可能なように設計されています。たとえば、あるハードウェアの流通業者は、オンライン・ショッピングで使用可能なように、自分の在庫と価格表を持っています。ある衣料の小売業者は、オンライン・ショッピングのために、スタイル、カラー、およびサイズを示した、オンライン・カタログを持っています。

データに対するアクセスを許可する前に、その要求者が誰であり、なぜそのデータを必要とするかを知る必要があります。 Trust Authority を使用すれば、信頼できるユーザーに証明書を発行できます。

その他の保護すべきエリア

本書では、セキュリティーの他のエリアについての対抗策については説明しません。しかし、以下のことも計画する必要があります。

- サイトのセキュリティー、入退出、および間仕切り
- ラップトップ・コンピューター、パーソナル・コンピューターとワークステーション、および他のコンテナーの物理的なセキュリティー
- 個人的なセキュリティーの背景の検査
- 債務や契約などの法律的な断わり書き
- キー管理、情報制御、およびセキュリティーの認識と教育などの、運用上での実践

オペレーティング・システム

ほとんどのオペレーティング・システムは、高可用性と豊富な機能セットを備えるよう構成されています。効率的な保護のアプローチでは、与えられた作業を行うのに必要な、最低限の機能だけを備えればよいことになります。不法侵入者にアクセスさせたくないすべてのオペレーティング・システムのフィーチャーは、アンインストールするか、使用不可にしておく必要があります。

典型的なユーザー

インターネットには、多くのさまざまな種類のユーザー (望ましいユーザーと望ましくないユーザー) がいます。 e-business では、オンラインで検索して購入する、顧客であるユーザーを必要とします。また、e-business では、在庫を検査して、製造の決定を下すため、またはビジネス内の計画と活動についてコメントするために、ビジネス・パートナーが特定のデータにアクセスできる必要もあります。 e-business ではまた、従業員が、割り当てられた仕事を行うのに必要なデータにアクセスできる必要もあります。

インターネットにはまた、ハッカーや spam (迷惑メール) の発信者、ウィルスをばらまく者、機密データにアクセスしたいユーザーなど、e-business にとって望ましくないユーザーもいます。これらのユーザーは、自分の e-business 内にさえ存在します。

何らかのリソースに対するアクセスを許可する前に、だれが要求しているユーザーであるか、データおよびアプリケーションに対してユーザーにどのようなアクセスをさせるか、およびユーザー・アクセスについてのどのような記録を保持するかについて知っている必要があります。

アプリケーションとアプリケーションの作成

アプリケーションは、セキュリティーを組み込むよう設計することができます。伝送されるデータの暗号化、アクセスを要求しているユーザーの認証、ユーザーおよびトランザクションの監査ログを利用することができます。

Toolbox API を使用すれば、アプリケーションにセキュリティーを追加することができます。

ハードウェア・セキュリティー

サーバーとデータ・バンクは、セキュア・システムの一部です。本書ではハードウェアについては説明していませんが、セキュリティーを管理するために使用されるサーバーとワークステーションの物理的なセキュリティーについて計画する必要があります。

Trust Authority ハードウェア・セキュリティー

この節では特に Trust Authority 構成要素について説明していますが、この考慮事項は、すべての FirstSecure 構成要素に適用可能です。

エリアの分離

サーバーは、CA 活動専用の分離した部屋に設置します。可能であれば、部屋は、補強された壁と、一枚板か鋼鉄製のドアを持ち、ドロップ・パネル (柱頭板) のない固定構造の天井を備えたものである必要があります。部屋はまた、火災の際の放水から保護するために、上げ床である必要もあります。

エリアの維持

部屋は、コンピューター用の無停電電源装置、照明設備、動揺検出器、および冷暖房システムを備えている必要があります。また、機器が発生する熱に対して、部屋の温度が適切になるよう、部屋の換気も監視する必要があります。

エリアへの出入りの制御

物理的なエリアへの出入りは、たとえば、バッジを使用するとか、番号キー付きのドア・ロックを使用するなど、多くの方法で制御できます。個人による悪意をもった損傷を防ぐために、少なくとも 2 人の信頼できる個人による正規の証明書の提示を必要とするような、出入りの制御をインストールする必要があります。

また、部屋を監視して、セキュア・エリアに出入りがあるたびに、だれが出入りしたかを追跡する必要もあります。最大限のセキュリティーを実現するためには、ドアの内側と外側の両方に、動揺検出器をインストールします。

通信の制御

Trust Authority サーバーには、予備のオープン・ポートが無いようにする必要があります。明示的に活動状態の Trust Authority アプリケーションに割り当てられた、これらのポートの要求のみを聴取するよう、システムを構成する必要があります。

e-business に使用されるハードウェアの保護は、それぞれのビジネスでの独自の手順および要件に従ってください。

第4章 e-business ネットワークにおける FirstSecure の計画

この部の以降の章では、FirstSecure に組み込まれている製品を e-business に結び付けます。これらの章では、19ページの『第3章 e-business ネットワークの概要』にある図に沿って説明します。それぞれの製品について、より詳細に説明します。製品についての完全な情報については、その製品に付属する資料を参照してください。展開のシナリオは、単なる提案にすぎません。

それぞれの展開のシナリオにおいて、以下の同じ基本ステップを実行してください。

1. ログの監査をより単純に、しかもより正確に行うために、ネットワークのすべての部分で、共通の時刻を参照するようにする。
2. イントラネット内から開始して、構成要素のインストールとテストを行う。
3. イントラネット内で問題がなければ、非武装地帯 (DMZ) 内でのアプリケーションの構築を開始する。
4. イントラネットと非武装地帯 (DMZ) の間のトラフィックは、ファイアウォールを介して移動させる必要がある。
5. 外部インターネット・アプリケーションを構築して、それらのテスト・データを使用してテストする。
6. ファイアウォールをインストールして、インターネットと DMZ の間のトラフィックを保護する。
7. ユーザーにネットワークをアクセスさせる。

完全な FirstSecure システムの計画

以下は、FirstSecure 製品をネットワークに展開するために推奨される順序です。これは、かなり単純化されたものです。各製品のハードウェアとソフトウェアの要件の詳細、および統合についての考慮事項については、57ページの『第3部 インストールと統合の考慮事項』を参照してください。また、それぞれの製品に付随している、インストール要件と指示を参照してください。多くの製品が、最新の情報をインターネット上でも持っています。 xiiiページの『Web 情報』に、FirstSecure 情報を持つ Web サイトをリストしています。レッドブック *Understanding the IBM SecureWay FirstSecure Framework,* SG24-5498 には、いくつかのより詳細なシナリオが記載されています。

1. 必要とされるセキュリティー要件を計画する。

2. それらの要件に合わせて、Policy Director をインストールする。
3. 顧客のサーバー・アプリケーションを作成し、テストする。このアプリケーションは、今のところイントラネット内に保持しておき、インターネットではまだ使用可能にはしないでください。
4. 顧客のサーバー・アプリケーションを保護するための IBM Firewall をインストールする。
5. SurfinGate を DMZ に追加する。
6. 非武装地帯 (DMZ) に MIMEsweeper と Norton AntiVirus を追加して、アプリケーションをインターネット上で使用可能にしたときに、そのアプリケーションが保護されるようにする。これらのアプリケーションが外部のトラフィックで使用可能にするときに、それらが自分のサーバーをポイントするよう構成してください。
7. 不法侵入の防止と検出のために、Tivoli Cross-Site for Security 製品をインストールする。
8. DMZ 内に、以下を追加する。
   - Web サーバー
   - Web カタログ・サーバー
   - Web インベントリー・サーバー
   - 顧客のクライアント・アプリケーション
   - 保護された顧客のクライアント・アプリケーション
   - 1 つ以上の Cross-Site for Security エージェント

   すべてのアプリケーションは、それらをトラフィックで開示する前に、ファイアウォール内でテストしてください。設定した規則をテストするためには、SecureWay Boundary Server の Network Security Auditor ツールを使用してください。
9. IBM SecureWay Firewall の 1 つのインスタンスをインストールして、DMZ 内のソフトウェアを保護する。デフォルト構成では『No traffic』にして、共通に開示する前に導入システムをテストできるようにすべきです。
10. Trust Authority をインストールして、信頼できるユーザーに証明書を発行する。
11. すべてのテストか完了したら、アプリケーションをインターネットで開示する。
12. システムの外部から Network Security Auditor を実行して、アクセスを共通的に公表する前に、規則をテストする。

13. 不都合なことがないことを確認するために、FirstSecure 構成要素のプログラムが作成した監査ログを検査する。
14. 継続して監査ログを検査し、アプリケーションをネットワークに追加したら、Cross-Site for Security エージェント を追加する。

第5章 ネットワークにおける Policy Director の計画

FirstSecure は、異機種 Web 環境に対して、統合された、ポリシー主導の制御ポイントを与えます。ユーザーがブラウザーを介して複数のバックエンド Web サーバーにアクセスする環境では、Policy Director は、以下のものを提供します。

- 各 Web ユーザーに対する単一サインオン
- 識別検査
- 保護された Web ページにアクセスを要求しているユーザーの許可検査

このサポートを使用すれば、以下の許可と保護を行うことができます。

- HTML、Telnet、および POP3 などの TCP/IP 交換
- データベース・システムなどの第三者アプリケーション
- ネットワーク管理ツール
- 内部で開発したアプリケーション

FirstSecure を使用すれば、ユーザーは、以下のメカニズムを使用して、 Policy Director に対する認証を行うことができます。

- セキュア・ソケット・レイヤー (SSL) による基本認証
- SSL による書式ベース・ログイン
- クライアント証明書を使用する SSL
- ケルベロス・ログイン

これで FirstSecure は、個別の Web オブジェクトとネットワーク・サービスに対する認証済みユーザーのアクセスを制御し、これらのリソースのサブセットに対する無許可のユーザーを制限することができます。

Policy Director の展開

Policy Director は、ユーザーおよびグループと、リソースとの間のマッピングを管理します。 Policy Director 管理コンソールを使用して、以下のことを行います。

- リソースを使用する予定のユーザーおよびグループを定義する。
- 保護が必要なオブジェクトを定義する。オブジェクトには、Web、TCP ポート、方式、およびインターフェースがあります。

- ユーザーがリソースをアクセスする方法を定義し、リソースを読み取り、変更、管理、実行、または削除などにおいて保護する規則を定義する。

以下の表は、共通の Policy Director 構成要素の構成を示したものです。この表で、自分のネットワークに適した構成を判別してください。次に、これらの構成要素をインストール中に選択してください。

詳しくは、*IBM SecureWay Policy Director 概説* を参照してください。

構成例	インストール済み構成要素
セキュア・ドメイン用の管理サーバーの単一のインスタンスが実行されるサーバー。 このシナリオでは、管理サーバーは、それ自体、独自のシステムに常駐します。管理サーバーは、セキュア・ドメイン用のマスター許可データベースを維持管理し、このデータベースをセキュア・ドメイン内で複製し、そのセキュア・ドメイン内の他の Policy Director サーバー・マシンについての位置情報を維持管理します。	管理サーバーのみ
WebSEAL サーバー。 このシナリオは、Web スペースを保護するためのソリューションを表します。 WebSEAL は、高可用性とフォールト・トレランスのために、バックエンド・サーバーをサポートします。	WebSEAL を備えたセキュリティー・マネージャー
NetSEAL サーバー。 このシナリオは、仮想私設網 (VPN) を保護するためのソリューションを表し、既存のネットワーク・サービスおよび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。	NetSEAL を備えたセキュリティー・マネージャー
WebSEAL と NetSEAL のサーバーの組み合わせ。	WebSEAL と NetSEAL を備えたセキュリティー・マネージャー
第三者アプリケーションに対して、Policy Director Authorization Service へのアクセスを提供するサーバー。	許可サーバー
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。	許可サーバーと ADK
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。	すべての構成要素

Policy Director は、1 つまたは複数のマシンに、さまざまな設定で構成要素を展開できる、高度に分散化されたセキュリティー・システムです。以下に、ネットワークにおける Policy Director の展開についての概要を説明します。完全なインストールの指示は、*IBM SecureWay Policy Director 概説* に説明があります。

1. Policy Director セキュリティー・サーバーをインストールします。

   セキュア・ドメインの中の少なくとも 1 つのコンピューターは、Policy Director セキュア・ドメインをセットアップするために、Policy Director セキュリティー・サーバーが含まれている必要があります。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。

   残りのサーバーは、DCE クライアントのインストール (または Windows NT システムの NetSEAT) でのみ機能します。

2. SecureWay Directory (LDAP) サーバーをインストールします。
3. Policy Director をインストールします。
   - Policy Director セキュリティー・サーバーを、最初に展開する必要があります (ステップ 1 参照)。
   - すべての Policy Director サーバーのインストールで、Policy Director Base が必要です。
   - これがセキュア・ドメイン内の*最初* または*唯一の* マシンである場合、管理サーバー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* マシンである場合、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。
4. 管理コンソールをインストールします。

   管理コンソールでは、オペレーティング・システムに DCE クライアント (または Windows NT 用の NetSEAT) がインストールされている必要があります (ステップ 1 参照)。

5. 許可 ADK を使用して開発されたアプリケーションには、以下の依存関係があります。
   - Policy Director パッケージが必要です。
   - アプリケーション・マシンに IVAuthADK をインストールしてください。
   - アプリケーションを実行するオペレーティング・システムは、 DCE クライアントまたは Windows NT システム用の NetSEAT のいずれかである必要があります。
   - アプリケーションが実行されるセキュア・ドメインには、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インストールされた許可サーバーが必要です。通常の開発環境では、許可 ADK と同じオペレーティング・システムに、許可サーバーを組み込みます。

第6章 ネットワークにおける SecureWay Boundary Server の計画

FirstSecure は、セキュア・ソケット・レイヤー (SSL)、SOCKS、および IPSec などの既存のセキュリティー標準を利用する Web ベース・アプリケーションに対して、セキュリティーを提供します。

操作環境に、異なるトラスト特性を持つ 2 つのネットワークの部分の接続が含まれている場合、FirstSecure の SecureWay Boundary Server 構成要素は、以下の要件を満たすことに取り組むのに役立ちます。

- 私設網に対する無許可アクセスの可能性を最小化する、インターネットに対する安全な接続
- ビジネス・パートナーおよびベンダーと選択的にデータを共用するための、大規模なエクストラネット・インフラストラクチャー
- インターネットまたは比較的信頼性のないネットワーク・セグメントを仮想私設網 (VPN) として使用して、信頼性のないネットワークのインフラストラクチャーを介してメッセージを渡しても、メッセージの機密性が保たれるようする

FirstSecure の SecureWay Boundary Server は、ネットワーク・アドレス・フィルター処理、内容のフィルター処理、プロキシー、およびサーキット・レベル・ゲートウェイのテクノロジーを使用しています。これらのテクノロジーを組み合わせることで、 SecureWay Boundary Server は、異なるトラスト特性を持ったネットワーク間の通信を制御することによって、ポリシー主導で、安全な、セキュア e-business 操作を可能にしています。

SecureWay Boundary Server には、以下のものが含まれます。

- IBM SecureWay Firewall (ACE/Server を含む)
- MIMEsweeper for IBM SecureWay リリース 2
- SurfinGate 4.05 for Windows NT
- ポリシー管理に対する機能強化

完全な SecureWay Boundary Server のインストールにおけるデータの流れの概要については、40ページの図10 を参照してください。

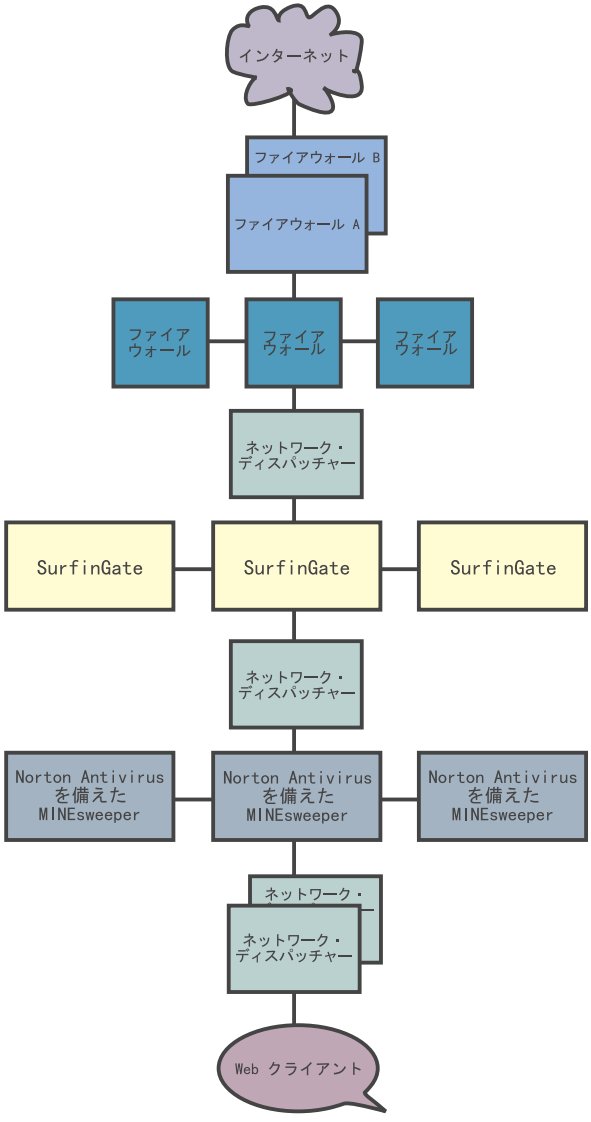


図 10. SecureWay Boundary Server 製品におけるデータの流れの概要

IBM SecureWay Firewall の展開

IBM SecureWay Firewall は、IBM Firewall とも呼ばれ、インターネットとの間の通信を制御します。ファイアウォール・テクノロジーが、IBM 自体の資産を保護しています。

インストールの注意点については、65ページの『SecureWay Boundary Server 構成要素の考慮事項』を参照してください。

ネットワーキングに関する問題点は、以下のとおりです。

- インターネットに接続する必要はあるが、自分のネットワーク、アプリケーション、およびデータに対する無許可アクセスを阻止したい
- 内部ユーザーによってネットワーキング資産が悪用される
- ビジネス・パートナーとベンダーに対する大規模なエクストラネット・インフラストラクチャーを計画する方法はあるが、構成管理に高いコストがかかる
- 専用回線で接続された事業所には高いコストがかかる
- パートナーおよびベンダーとの、不十分で、遅い、または誤解される通信が原因で、ビジネスの生産性が低下する
- ネイティブ言語以外でソフトウェアを管理するため、高い管理コストがかかる

IBM Firewall は、これらの問題に対応するものです。ファイアウォールを介した明示的に許可されたトラフィックだけを許すことによって、IBM Firewall は、ネットワークを外部から保護しています。それ以上の保護については、IBM Firewall に含まれている、外部から攻撃されやすいかどうかを検査するソフトウェアによって、IBM Firewall が実行されているサーバーを*堅固* なものにして、ハッカーが、ファイアウォールに侵入するか、またはそれを越えて侵入することができないようにすることができます。 IP アドレスと内部ネットワークの構成は、信頼性のないネットワークから隠されます。ファイアウォールを介したすべてのトラフィックはログに記録され、ユーザーの活動レポートを生成するために使用できます。

IBM Firewall およびその VPN 構成アプリケーションによって、大規模な VPN インフラストラクチャーを展開して、安価に管理することができます。ネットワークに関する調査では、顧客は、VPN を使用することで、専用回線を利用した場合のコストよりも大幅な削減を実現することができます。

IBM Firewall を使用すれば、各事業所にファイアウォールを配置して、IPSec ベースのトンネルを使用することによって、事業所をインターネットで接続することができます。

IBM Firewall は、Security Dynamics Technologies, Inc. の製品である ACE/Server と一緒に納入されます。 ACE/Server は、企業ネットワークに対して、強力で、集中化された認証サービスを提供することで、許可ユーザーだけが、ネットワーク・ファイル、アプリケーション、および通信にアクセスできるようにしています。 Security Dynamics Technologies, Inc. が特許を持っている SecurID トークン・テクノロジーに加えて、ACE/Server は、無許可アクセ

スに対するバリアを作成します。認証は、2 つの要因に依存しています。つまり、ユーザーは、認証されるためには、あるもの (SecurID トークン・カード) を*持っていること* と、あるもの (PIN) を*知っていること* の両方が要求されます。

MIMEsweeper の展開

Content Technologies Ltd. の製品である MIMEsweeper は、インターネットとイントラネットのデータの内容ベースの分析を実行して、隠された脅威を識別して、ネットワーク・ユーザーをこれらの脅威から保護します。

インストールの注意点については、65ページの『SecureWay Boundary Server 構成要素の考慮事項』を参照してください。

MIMEsweeper には、MAILsweeper と WEBsweeper の 2 つの基本モジュールが含まれており、ユーザーを異なる方法で保護します。メールおよび他の Web データが MIMEsweeper に入ると、MIMEsweeper は、送信者と受信者のアドレスを検査した後、ファイルを反復的にその構成要素の部分に分解します。次に、MAILsweeper と WEBsweeper は、それらの部分を分析して、脅威が私設網の中に侵入する危険性を最小にします。

FirstSecure には、MAILsweeper 4.0 と WEBsweeper 3.2_5 の両方が含まれます。それぞれは、別個にインストールし、構成し、使用することができます。

MAILsweeper は、以下のことができます。

- 選択されたウィルス・スキャナーとともに作動して、分解されたファイルがウィルスに感染していないかどうか検査する
- マクロ爆弾を検出してブロックする
- 以下のためにキーワードをスキャンする
  - 電子メールの中のいやがらせや攻撃的な言葉から保護するのを援助する
  - 価値あるデータの社外への流出を保護するのを援助する
- 着信する電子メールによる spam (迷惑メール) をブロックして、ネットワークの混雑を少なくし、従業員の生産性のロスを最小化する
- 個人またはグループが、AVI または MPEG など、特定のタイプのファイルを受信または送信するのをブロックする
- ネットワークがトラフィックに対応できるようになるまで、そのサイズに基づいて、ファイルをブロックするか、遅らせる

WEBsweeper は、以下のことができます。

- 仕事に無関係と思われる特定のサイトから、従業員の通信をブロックするのを援助する
- 機密文書または重要文書が不注意によって失われるのを保護するのを援助する

さらに、MIMEsweeper には、第三者の URL ブロッカーを統合するために使用できる、アプリケーション・プログラミング・インターフェース (API) が含まれています。

MIMEsweeper は、インターネットからのセキュリティー上の脅威から、企業とそのユーザーを保護するための主要な資産となり得ます。

注: SecureWay FirstSecure オファリングまたは SecureWay Boundary Server オファリングの一部として MIMEsweeper for IBM SecureWay リリース 2 を入手する場合、 MIMEsweeper の資料に、サービスとサポートについての Content Technologies の連絡先が提供されている場合がありますが、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。

SurfinGate の展開

Finjan Software Ltd. の製品である SurfinGate は、JavaScript コード、Java アプレット、および ActiveX コントロールなどのモバイル・コードを検査して、データの変更、情報の削除、および不法なデータ収集などの損傷から、ネットワークを保護します。 SurfinGate は、ゲートウェイ・レベルでモバイル・コードを検査して、ネットワークに侵入する前に、脅威となるコードを識別します。モバイル・コードは選択的にブロックするか、またはユーザーごとまたは部門ごとに許可することができ、コードは、それが意図する機能に基づいて、ネットワークへのアクセスを許可または拒否することができます。 SurfinGate を使用すれば、管理者は、モバイル・コードを使用可能にして、ActiveX、Java、JavaScript、Visual Basic Script、plug-in、および cookie に対する企業全体のセキュリティー・ポリシーを管理、制御、および強制することができます。

SurfinGate には、以下の構成要素が含まれています。
- SurfinGate Server
- SurfinConsole
- SurfinGate データベース
- WTE 統合用の Plugin

SurfinGate Server は、HTTP プロキシー・サービスとして、またはファイアウォールまたはプロキシーに対するサービスとして働きます。 SurfinGate Server

は、企業ファイアウォールと他のいずれかの既存プロキシーの後に置くことができ、HTTP サーバーとしても働きます。このアーキテクチャーによって、モバイル・コードのトラフィックを停止させ、ハッキングが発生する前に検査することができます。

ネットワーク管理者は、SurfinConsole を使用して、モバイル・コードに対する中央の企業セキュリティー・ポリシーの管理と設定を行います。 SurfinConsole は、ネットワーク上の複数の SurfinGate Server を制御することができ、ユーザーごとまたはグループごとに、あるいは受け入れ可能でないコードと受け入れ可能なコードについてのカスタム・リストによって、企業全体でのモバイル・コードに関する規則を強制することができます。

SurfinGate データベースは、ユーザーとグループに関する情報およびそれらの対応するセキュリティー・ポリシーが入っている、Applet Security Profile (ASP) の詳細を保管します。 SurfinGate がすべてのモバイル・コードの内容を動的に検査しているので、このデータベースはセキュリティーのためには必要ありませんが、大規模の操作ではパフォーマンスを向上させるのに役立ちます。

注: SecureWay FirstSecure オファリングまたは SecureWay Boundary Server オファリングの一部として Windows NT 用の SurfinGate を入手する場合、SurfinGate の資料に、サービスとサポートについての Finjan の連絡先を提供している場合がありますが、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。

第7章 ネットワークにおける Intrusion Immunity の計画

セキュリティー・テクノロジーでは、これまでは、セキュリティー上の脅威からの保護を強調して記述してきました。しかし、セキュリティーの面で等しく重要なのは、脅威を検出することです。 FirstSecure の中の不法侵入回避のための製品では、企業でセキュリティー上の脅威を検出できるようにするために、不法侵入の検出とアンチウィルスの機能を提供しています。

アンチウィルス・ソフトウェアは、トロイの木馬、ワーム、マクロ・ウィルス、不正 ActiveX コントロール、不正 Java アプレットなどを含む、悪意を持ったコードからの保護を提供します。ウィルス保護は、どのセキュリティー・ソリューションでも不可欠の部分です。 FirstSecure のアンチウィルス製品は、以下の主要なアンチウィルスの要件に対応しています。

- 定常クライアントとモバイル・クライアントの両方のアンチウィルスのニーズに対して、包括的な一貫したアプローチを行うための広範囲なクライアントのセットをカバーすること。
- ウィルスのこん跡に対する加入サービス。ウィルスのこん跡を定期的に更新することは、悪意をもつ最新の形態のコードからの効果的な保護を維持するために重要なことです。
- アンチウィルスのポリシーが有効なことを確実にするために、サーバーからクライアントにポリシー主導でアンチウィルスの更新を配布すること。

Tivoli Cross-Site for Security の展開

Tivoli Cross-Site for Security は、ハッキングの危険性のあるシステムに対する、ネットワーク・ベースでの不法侵入の検出を提供します。管理ドメインがインターネットに接続するところであれば、どこにでも Tivoli Cross-Site for Security エージェントを配置することができます。 Tivoli Cross-Site for Security は、ネットワークを監視して、内部と外部のハッキングを検出します。これによって、以下の利点をもたらします。

- Cross-Site for Security の管理者に潜在的なハッキングについての警報を出す、リアルタイムの不法侵入検出
- DMZ 内のエージェントに対してとイントラネット上のエージェントに対して、異なるポリシーを設定できる、構成可能なポリシー
- 環境の変更に速やかに応答できる、セキュリティー・エージェント・ポリシーのオンライン変更

- Tivoli 企業管理システムを増大できるようにするための、 Tivoli の企業アプリケーションとの統合

Tivoli Cross-Site for Security は、以下のことができます。

- スキャンおよびあふれの検出
- IP トラフィックの監視
- ポート・サービスの監視
- DNS、取り付けサービス、およびネットワーク・ファイル・システムの要求と応答の検出
- ポートマッパー・サービス要求と応答ダンプの検出
- RStatd 呼び出しの検出
- 特定のマップ名とファイル名の検出
- PC ファイル・サーバーに対する SMB ベースのハッキングの検出
- インターネット制御メッセージ・プロトコルの検出

Cross-Site for Security を使用すれば、ネットワークのトラフィックを監視して、ハッキングや不法侵入を検出することができます。これは、インターネットからイントラネットを遮へいするための DMZ と、内部ネットワークとの両方のトラフィックを監視します。

Cross-Site for Security が検出できる不法侵入のタイプには、以下のものがあります。

- こん跡、つまりパターンの検出
- あふれの検出
- ネットワーク・ベースのハッキング
- Windows ネットワークのハッキング
- リモート・プロシージャーのハッキング
- サービスの利用
- 無許可のネットワーク・トラフィック
- 疑わしい活動

Cross-Site for Security は、Cross-Site for Security エージェントと Cross-Site for Security 管理サーバーを使用してネットワークを保護します。エージェントが重大なハッキングを検出すると、エージェントは、暗号化されたイベントを Cross-Site for Security 管理サーバーに送り、そこで直ちに、情報と応答をログに記録します。 Cross-Site for Security 管理サーバーを構成して、警報をコン

ソールに送るか、管理者に電子メールで通知するか、あるいは常駐していない管理者にポケット・ベルで知らせることができます。

Tivoli Cross-Site for Security ライセンス・キーの取得

Tivoli Cross-Site for Security 製品を使用可能にするためには、カスタマイズされたライセンス・キーが必要です。

Tivoli Cross-Site Web サイトで、以下のステップを実行することによって、ライセンス・キーを受け取ることができます。

1. FirstSecure 製品に付いている Passport Advantage Proof of Entitlement 文書を見つけます (これは Tivoli Cross-Site for Security CD-ROM と、*Tivoli Cross-Site for Security Installation* にも入っています)。
2. Passport Advantage Proof of Entitlement で、オーダー番号 (5 で始まる 8 桁の番号) および顧客 (サイト) 番号 (7 で始まる 7 桁の番号) を見つけます。これらの番号を使用して、最初に Tivoli Cross-Site Web サイトにアクセスします。
3. インターネットにアクセスできるコンピューターで、Web ブラウザーを使用して Tivoli Cross-Site Web サイトにログインします。 Web サイトの URL は、`www.cross-site.com/support/licensing/` です。
4. オーダー番号、顧客番号、および契約情報を入力します。 Tivoli Cross-Site for Security をインストールしようとしているサーバーのドメイン名も提供する必要があります。
5. Web 上のその他の指示に従ってください。
6. Tivoli Cross-Site ライセンス・キーのアクセスでトラブルが発生した場合は、licensing@cross-site.com に電子メールを送るか IBM 担当員にお問い合わせください。

関連 Tivoli Cross-Site 製品

Tivoli Cross-Site 製品ファミリーには、FirstSecure ファミリーの一部ではない他の構成要素が含まれています。

- Tivoli Cross-Site for Availability は、エンド・ユーザーが Web サイトをどのように正常にアクセスできるかを監視し、報告します。
- Tivoli Cross-Site for Deployment は、企業の到達範囲を拡張して、インターネット上での重要なアプリケーションと情報の配布と管理を可能にします。

これらの製品は、Tivoli Cross-Site for Security の資料の中に説明されていますが、別途購入する必要があります。

Tivoli Cross-Site for Security を使用したトラフィックの監視

Cross-Site for Security エージェントは、高機能のネットワーク探知機能です。これは、ネットワーク上のパケットを連続的に監視します。 Cross-Site for Security エージェントはこれらのパケットをフィルターに掛けて、疑わしい活動を表す、さまざまなこん跡を探します。これらのこん跡は、ネットワーク上でのハッキングを示している可能性があります。

Cross-Site for Security エージェントは、UNIX ではデーモンとして実行され、Windows NT では NT サービスとして実行されます。 Cross-Site for Security は、システムがブートされるときに、自動的に開始されるよう構成されます。これは、常駐として残り、ユーザーがログインしたかどうかにかかわらず、システムのバックグラウンドで実行されます。

潜在的なハッキングが検出されると、エージェントは、その重大度を判別して、管理サーバーに直ちに通知するか、警報をローカル・ファイルに記録するかを決定します。ログは、定期的に管理サーバーにアップロードされます。

エージェントはまた、Cross-Site for Security 管理サーバーと定期的に連絡をとり、エージェントが活動状態で実行中であることを知らせます。このタイプの通信は、ハートビートと呼ばれます。ハートビートのインターバルを構成することができます。

管理サーバーがエージェントからハートビートを受け取ると、管理サーバーは、更新された構成情報、新しいこん跡、およびアップロード・スケジュールがあれば、エージェントに通知します。エージェントは、これらの更新を自動的にダウンロードしてインストールします。

ネットワークにおける Tivoli Cross-Site for Security

Cross-Site for Security を構成して、ビジネスの要件に合わせることができます。主な決定事項は、以下のものです。

- どこに Cross-Site for Security 管理サーバーをインストールするか
- どれだけの数の Cross-Site for Security エージェントが必要か
- どこに Cross-Site for Security エージェント をインストールするか

これらの考慮事項は、サイズ、トポロジー、およびネットワークの帯域幅とトラフィックに加えて、管理サーバーとエージェントの数を決定するために重要です。 Tivoli Cross-Site for Security のインストールの注意点については、71 ページの『Intrusion Immunity のハードウェアとソフトウェアの要件』を参照してください。

注: SecureWay FirstSecure オファリングの一部として Tivoli Cross-Site for Security を入手する場合、 Tivoli Cross-Site for Security の資料にサービスとサポートについての説明がある場合がありますが、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。

Norton AntiVirus の展開

Symantec Corporation の Norton AntiVirus は、世界でも先進的なアンチウィルスのソフトウェア製品の 1 つです。 Norton AntiVirus は、以下のことができます。

- ウィルスに感染したファイルの隔離
- ウィルスからの保護、および悪意を持った ActiveX コントロールと Java アプレットからの保護
- 電子メールの添付、インターネットのダウンロード、フロッピー・ディスケット、ソフトウェア CD、またはネットワークからくる可能性があるウィルスからの保護

Norton AntiVirus をバックグラウンドで定常的に実行するようスケジュールして、コンピューターを安全に保持することに役立てることができます。 Symantec の研究者は、Norton AntiVirus が検出できるウィルスを継続して追加し続けています。 LiveUpdate フィーチャーを使用して、Symantec からの新しいアンチウィルス定義を 1 週間に一度、自動的に受け取ることができます。

Norton AntiVirus の隔離フィーチャーは、感染したか、その疑いがあるファイルをコンピューターの安全な場所に隔離して、他のファイルと分離し、ファイルを修正している間にウィルスが広がるのを防止します。

Scan and Deliver ウィザードを使用して、疑わしいファイルを検査のために Symantec に送ることができます。 Symantec AntiVirus Research Center (SARC) が、問題の修正のための援助に応じます。

Norton AntiVirus スキャナーである *Bloodhound* はバックグラウンドで実行され、新しいウィルスに感染した可能性があるアプリケーションの動作を観察し、分類します。あるアプリケーションがウィルスのような振る舞いをして、他のプログラムに感染しようとすると、 Bloodhound はそのプログラムを停止して、新しいウィルス更新を受け取るまで、他のファイルへの感染を防ぎます。

FirstSecure で提供される Norton AntiVirus Solution Release 3.04 製品は、以下のとおりです。

- デスクトップ・ソリューション:

  - Norton AntiVirus 4.08 for DOS
  - Norton AntiVirus 4.08 for Windows 3.51
  - Norton AntiVirus 5.02 for Windows 95/98
  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.02 for Windows NT 4.0
  - Norton AntiVirus 5.03 for Macintosh
  - Norton AntiVirus 5.02 for OS/2
- サーバー・ソリューション:
  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.02 for Windows NT 4.0
  - Norton AntiVirus 4.04 for NetWare
  - Norton AntiVirus 2.0 for Lotus Notes™ and OS/2
  - Norton AntiVirus 1.52 for Microsoft Exchange
- ゲートウェイ・ソリューション:
  - Norton AntiVirus 1.02A for Internet E-mail Gateways for NT
  - Norton AntiVirus 1.04 for Firewalls
- 管理:
  - Norton System Center 3.1
  - Norton AntiVirus 5.03 for Macintosh Administrator
  - Norton AntiVirus Plus 5.0 for Tivoli Enterprise
  - Norton AntiVirus Plus 5.0 for Tivoli IT Director
  - その他の管理ツール (Norton AntiVirus Network Manager (NAV32/NAVNETW) v3.01 を含む)

Norton AntiVirus に関する詳細な情報は、Norton AntiVirus CD のルート・ディレクトリーの中の contents.txt ファイルに入っています。

注: SecureWay FirstSecure オファリングの一部として Norton AntiVirus Solution Release 3.04 を入手する場合、 Norton AntiVirus の資料で、サービスとサポートについて、Symantec の連絡先を提供している場合がありますが、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。

詳細なインストール・ステップについては特定の製品に付いている資料を参照し、ハードウェアとソフトウェアの要件については、71ページの『第13章 Intrusion Immunity の要件とインストールの注意点』を参照してください。

第8章 ネットワークにおける Public Key Infrastructure の計画

Public Key Infrastructure の Trust Authority 構成要素は、ユーザーを認証し、信頼性のある通信を行うためのインターネット・アプリケーションを提供します。暗号化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) 標準の上に構築された Trust Authority システムは、ディジタル証明書の発行、公表、および管理に必要なインフラストラクチャーを提供します。この製品には、以下のものが含まれます。

- IBM AIX および Microsoft Windows NT サーバー・プラットフォームのサポート。
- ユーザー登録の背後にある管理用タスクを取り扱う、登録局 (RA)。この管理は、自動処理または人間の意思決定によって実施することができますが、以下のタイプの作業が含まれます。
  - ユーザーの識別を確認する
  - 証明書の取得、更新、または取り消しの要求を承認または拒否する
  - ユーザーが、証明書の中の公開キーに関連する秘密キーの所有権を持っているかどうか検査する
  - 特定のタイプのユーザーに特定のタイプの証明書を発行するために、指定されたビジネス・プロセスまたは証明プロファイルの規則に従う

  RA はまた、統合された公開キー・ディレクトリーである IBM SecureWay LDAP Directory の証明書についての情報も公表します。
- 信頼性のある認証局 (CA)。CA は、以下のことを行います。
  - ディジタル証明書を発行し、証明書を認証するためのディジタル・キー・ペアを生成する
  - 最初の登録から、証明書の更新および取り消しまで、証明書の完全なライフ・サイクルをサポートする
  - 証明書が取り消されると、RA がディレクトリーを即時に更新する
  - 保護キーに対する能力を拡張するために、IBM SecureWay 4758 PCI 暗号コプロセッサーおよびスマート・カードなどの暗号化ハードウェアを使用することができる
- ブラウザーの証明書、サーバーの証明書、および Smart Card などの特定のデバイスのための証明書を容易に取得できるようにするための Web ベース

の登録インターフェースである、Credential Central。管理者は、これらの登録フォームを使用して、PKIX 証明書のエンド・ユーザーを事前に登録することもできます。

- ユーザーが Web ブラウザーを使用せずに PKIX 証明書の取得、更新、および取り消しができる、独立型 Windows インターフェースである、Trust Authority Client。
- 管理者が、証明書の取得、更新、または取り消しの要求を承認または拒否できるようにする Web ベースの管理インターフェースである、RA Desktop。
- Trust Authority RA および CA から受け取ったイベントを確実に認証できるようにするための、メッセージ確認コード (MAC) を使用する監査サブシステム。構成可能なオプションによって、監査レコードを、ログ記録されたときに保全性が保護されるようにすることもできます。
- システムの構成、セキュア・パスワードの変更、CA の相互証明、監査ログの保全性検査、およびシステム構成要素の安全な開始と停止に対する、いくつかの管理インターフェース。
- アプリケーション開発者がカスタム PKI アプリケーションを書くことができるようにする、アプリケーション・プログラミング・インターフェース (API)。
- IBM DB2 Universal Database に対する統合実行時サポート。別個のデータベースが、IBM SecureWay Directory 用と、RA、CA、および監査構成要素用に存在します。

Trust Authority の展開

詳細な計画とインストールについての情報は、*IBM SecureWay Trust Authority Up and Running* を参照してください。この資料には、Windows NT サーバーおよび AIX でのインストールについてのシナリオとステップが含まれています。

第9章 企業における SecureWay Toolbox の計画

FirstSecure Toolbox を、ネットワークではなく、開発環境にインストールすることを計画してください。アプリケーションを、外部のユーザーに使用させる前に、開発環境の中でテストしてください。

許可サービス

許可サービスによって、だれが Web サイトにアクセスする許可を持っているかを監視することができます。認証は、パスワードまたは公開キーをベースに行います。これらの手段によって、サイトのデータの保全性と機密性を保護します。許可サービスはアクセス制御リスト (ACL) を作成して、サイトのオブジェクトにアクセスできる人、およびそれらの人がオブジェクトにアクセスできる方法を定義します。また、許可サービスにより、保護オブジェクトを定義して、単一サインオンのためのパスワードを作成することもできます。これらのセキュリティー・ツールのすべてが、セキュリティー・ポリシーの管理を容易にするために、集中化されています。許可サービスは、IBM SecureWay Policy Director 許可 API によってサポートされます。

認証局サービス

認証局サービスは、X.509 Public Key Infrastructure for Multiplatforms と IBM KeyWorks Toolkit によってサポートされます。

認証局サービスによって、ディジタル証明書を使用したセキュリティーが確実に行われるようになります。これらのサービスには、これらの証明書の完全なライフ・サイクル (発行、更新、および取り消し) のための API が含まれています。認証局はまた、証明書の取り消しリストも公表しています。この API は、証明書のユーザーを認証するための手段として、公開キーとスマート・カードのテクノロジーを利用しています。

X.509 Public Key Infrastructure for Multiplatforms は、PKIX とも呼ばれ、PKIX API を介して提供されます。これらの API により、エンド・エンティティー (EE)、認証局 (CA)、および登録局 (RA) の構成要素を介して、証明書の作成、管理、保管、配布、および取り消しを行うことができます。これらの API は、IBM SecureWay Trust Authority とのインターフェースが可能であり、IBMKeyWorks をベースとしています。

PKIX API については、*IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference* を参照してください。 IBM KeyWorks についての詳細は、91ページの『第16章 FirstSecure と一緒に提供される文書』で、Toolbox と一緒に提供される資料のリストを参照してください。

ディレクトリー・サービス

ディレクトリー・サービスは、IBM SecureWay Directory Client によってサポートされます。

ディレクトリー・サービスは、Lightweight Directory Access Protocol (LDAP) を使用して、ディレクトリーの編成、制御、およびアクセスを行います。これらのサービスは、LDAP サーバーへのクライアント・アクセスを提供する、クライアント / サーバーのモデルをベースにしています。ディレクトリー・サービスは、保管、更新、検索、および交換のために、ディレクトリー情報を中央設置場所で維持管理するための手段を提供します。ディレクトリー・サービスは、セキュア・ソケット・レイヤー (SSL) を使用して情報を暗号化します。

ディレクトリー・サービスについての詳細は、91ページの『第16章 FirstSecure と一緒に提供される文書』で、 Toolbox と一緒に提供される IBM SecureWay Directory Client の資料のリストを参照してください。

KeyWorks 暗号およびトラスト管理サービス

暗号およびトラスト管理サービスは、IBM KeyWorks Toolkit (KeyWorks とも呼ばれます) によってサポートされます。

KeyWorks 暗号および管理サービスは、情報にアクセスできる人を制御するために、情報の暗号化と暗号化解除を行います。これらのサービスは、ディジタル署名の作成と検査を行い、ネットワーク上の個人とコンピューターの識別を認証します。キーを配布せずに暗号化された情報の回復を可能にする、キー回復システムが IBM Key Recovery Service Provider に組み込まれています。

KeyWorks は、暗号化されたトラスト・サービスのツールキットです。これは、1 組の階層化されたセキュリティー・サービスと、統合された情報と通信のセキュリティー機能のセットを備えた、関連するプログラミング・インターフェースからなります。各層は、そのすぐ下の層にある、より基本的なサービスの上に構築されています。これらの層は、低い層にある暗号アルゴリズム、乱数、および固有の識別情報などの基本的な構成要素から始めて、高い層のデ

ィジタル証明書、キー管理と回復メカニズム、およびセキュア・トランザクション・プロトコルが構築されています。

KeyWorks は、各国語サポート (NLS) が可能であり、これによって、製品が、どの言語、スクリプト、文化、およびコード化文字にも依存しないようになります。

KeyWorksC API についての詳細は、91ページの『第16章 FirstSecure と一緒に提供される文書』で、 Toolbox と一緒に提供される KeyWorks の資料のリストを参照してください。

セキュア・ソケット・レイヤー・プロトコル・サービス

セキュア・ソケット・レイヤー・プロトコル・サービスは、IBMセキュア・ソケット・レイヤー (SSL) Toolkit によってサポートされます。

SSL プロトコル・サービスにより、データをだれにアクセスさせるかを決定することができます。これらのサービスは、ユーザー認証、無許可のクライアントによるアクセス防止、データの悪用の防止など、いくつかの目的のために、公開キーと秘密キーを使用してデータを暗号化します。証明書を発行する相手を制御することで、データを信頼してアクセスさせる相手を制御することができます。 SSL テクノロジーは、データの暗号化とパスワードの作成のためのいくつかの他の API にも組み込まれています。

第3部 インストールと統合の考慮事項

この部では、構成要素を一緒に適合させる方法について説明します。ここでは、各製品のハードウェアとソフトウェアの要件、および必要とされるアプリケーションまたはデータベース製品について挙げます。

第10章 FirstSecure のインストールの計画

FirstSecure 構成要素製品をインストールする前に、以下の節を読んで、必要なハードウェアとソフトウェアが揃っているかどうか確認してください。FirstSecure の更新された最新情報は、www.ibm.com/software/security/firstsecure にあります。製品のインストールを開始する前に、更新された最新情報について、この Web サイトを調べてください。

FirstSecure の構成要素製品のインストールと構成を行うためのステップバイステップの詳細は、それぞれの構成要素製品の資料に記載されています。

一般的なシステム要件

この節では、FirstSecure 製品についての全体的なシステム要件について説明します。それぞれの構成要素製品に固有のハードウェアとソフトウェアの要件については、その特定の構成要素製品の節を参照してください。

FirstSecure 構成要素をインストールするには、以下のサーバー・オペレーティング・システムのうちの 1 つが実行できるハードウェアが必要です。

- Microsoft Windows NT Version 4 (Service Pack 5 付き)。
- AIX バージョン 4.3.1 またはそれ以上。
- Sun Solaris バージョン 2.6 またはそれ以上。

  注: Solaris の場合、Toolbox は、Sun Solaris バージョン 2.6 (1999 年 5 月の Fix Pack 付き) が必要です。

FirstSecure 構成要素製品のそれぞれは、少なくとも上記に挙げるオペレーティング・システムの 1 つで実行します。それぞれの構成要素製品の節に、サポートされているオペレーティング・システム・プラットフォームと、各構成要素製品の前提条件となる他のソフトウェアについてが示されています。これらのオペレーティング・システムの範囲内で、サーバー、管理コンソール、およびクライアント・システムが必要になります。以下の節では、これらの要件について概説します。

サーバーおよびクライアントのためのオペレーティング・システムの要件

SecureWay 製品のオペレーティング・システムの要件については、60ページの表1 を参照してください。

表 1. サーバーおよびクライアントのためのオペレーティング・システムの要件

オペレーティング・システム	最低サーバー・レベル	最低クライアント・レベル
Windows NT	バージョン 4.0、Service Pack 5	バージョン 4.0、Service Pack 5
IBM AIX	バージョン 4.3.1	バージョン 4.3.1
Sun Solaris	バージョン 2.6	バージョン 2.6
Windows 95	N/A	サポートされるすべてのバージョン
Windows 98	N/A	サポートされるすべてのバージョン
Windows 3.1 (Norton AntiVirus のみ)	N/A	サポートされるすべてのバージョン
IBM OS/2 (Norton AntiVirus のみ)	N/A	バージョン 4.0、FixPak 6 またはそれ以上

構成要素製品の詳細と要件

以降の節で、FirstSecure の構成要素製品のハードウェアとソフトウェアの要件を示します。以下の章で、各組み立てブロックについての詳細を説明し、それぞれのハードウェアとソフトウェアの要件を示します。これらの章ではまた、それぞれの製品のインストールと構成についても概説しますが、これには、他の構成要素との統合についての説明が含まれます。

- 61ページの『第11章 Policy Director の要件とインストールの注意点』
- 63ページの『第12章 SecureWay Boundary Server の要件とインストールの注意点』
- 71ページの『第13章 Intrusion Immunity の要件とインストールの注意点』
- 79ページの『第14章 Public Key Infrastructure の要件とインストールの注意点』
- 85ページの『第15章 Toolbox のインストール要件と考慮事項』

第11章 Policy Director の要件とインストールの注意点

この章では、Policy Director のハードウェアとソフトウェアの要件について挙げます。また、他の FirstSecure 製品との統合についてのインストールの注意点があれば、それも説明します。

Policy Director のハードウェアとソフトウェアの要件

表2 は、Policy Director のハードウェア要件のリストです。

表 2. Policy Director のハードウェア要件

プラットフォーム	最小ディスク・スペース	最小メモリー
Windows NT サーバー: Intel または Intel 互換の 80486 133 MHZ 以上	16 MB	64 MB
AIX サーバー: AIX 4.3.1 を実行できるハードウェア	16 MB	64 MB
Solaris サーバー: Solaris 2.6 を実行できるハードウェア	16 MB	64 MB

Policy Director 構成要素のソフトウェア要件は、以下のとおりです。

Policy Director サーバー

- Windows NT サーバー バージョン 4.0、Service Pack 5
- AIX バージョン 4.3.1
- Sun Solaris, Version 2.6

NetSEAT クライアント

- Windows NT サーバー バージョン 4.0、Service Pack 5
- Windows 95
- Windows 98

管理コンソール

- Windows NT ワークステーション
- Windows NT サーバー・クライアント
- AIX バージョン 4.3.1 クライアント
- Sun Solaris, Version 2.6 クライアント

Policy Director には、パッケージに含まれている他のソフトウェアが必要です。 Policy Director の配置に必要なソフトウェアをインストールするには、*IBM SecureWay Policy Director 概説* の指示に従ってください。

Policy Director のインストールの注意点

www.ibm.com/software/security/policy に、Policy Director に対するソフトウェア前提条件を更新したものがリストされています。

Policy Director と Trust Authority の統合

IBM SecureWay Trust Authority は、それぞれのユーザーが本人であるかどうかを確認することによる認証を提供します。 Trust Authority は、IBM SecureWay Directory (Lightweight Directory Access Protocol または LDAP と呼ばれることがあります) の情報に基づいて、ユーザーに証明書を発行します。

次に、Policy Director は、これらの証明書を使用して、それぞれのユーザーが許されたリソースにだけアクセスできるようにすることによって、許可を行います。 Policy Director は、その情報をそれと同じ IBM SecureWay Directory に格納します。

e-business では、すべての Policy Director 許可、およびすべての Trust Authority 情報を使用した、単一ユーザー定義を持つことができます。 SecureWay Boundary Server 情報を IBM SecureWay Directory にも格納した場合は、 Policy Director がその情報も管理します。

第12章 SecureWay Boundary Server の要件とインストールの注意点

この章では、SecureWay Boundary Server のハードウェアとソフトウェアの要件について挙げます。また、他の SecureWay Boundary Server 製品との統合についてのインストールの注意点があれば、それも説明します。

SecureWay Boundary Server のハードウェアとソフトウェアの要件

SecureWay Boundary Server 構成要素製品のハードウェア要件は、表3 と 64ページの表4 にあります。

表 3. SecureWay Boundary Server 構成要素製品のハードウェア要件

SecureWay Boundary Server 構成要素	マシン・タイプ	ディスク・スペース	メモリー	その他
IBM SecureWay Firewall[1]	NT: Pentium® 133 MHz 以上 AIX: AIX 4.3.2 をサポートする RS/6000 マシン	NT: 24 MB[2] AIX: 307 MB	NT: 64 MB AIX: 64 MB	ネットワーク・インターフェース・カード 2 枚
ACE/Server	NT: Pentium 166 MHz 以上 (シングル・プロセッサーのみ) AIX: AIX 4.2 をサポートするマシン	1 次サーバー・ソフトウェア: 50 MB バックアップ・サーバー: 22 MB 初期ユーザー・データベース: 4 MB インストール: 240 MB	最小: 32 MB	実際の記憶域要件は、ユーザー数によって決まります。
SurfinGate				

表 3. SecureWay Boundary Server 構成要素製品のハードウェア要件 (続き)

SecureWay Boundary Server 構成要素	マシン・タイプ	ディスク・スペース	メモリー	その他
サーバー	Pentium 233 MHz 以上	20 MB	最小: 128 MB 推奨: 256 MB	
コンソール	Pentium 233 MHz 以上	15 MB	最小: 32 MB 推奨: 64 MB	
MIMEsweeper for IBM SecureWay リリース 2				
MAILsweeper	Pentium 200 MHz 以上	1 GB	64 MB	ネットワーク・インターフェース・カード 1 枚
WEBsweeper	Pentium 400 MHz 以上	1 GB	128 MB + (各並行 Web 接続ごとに) 1 MB	ネットワーク・インターフェース・カード 1 枚

注:
1. 詳細については、IBM Firewall に含まれる資料を参照してください。
2. Netscape ブラウザーの場合、13 MB のディスク・スペースも必要です。

表 4. SecureWay Boundary Server 構成要素製品のソフトウェア要件

SecureWay Boundary Server 構成要素	Microsoft Windows プラットフォーム		AIX	Solaris
	クライアント	サーバー	サーバー	サーバー
IBM SecureWay Firewall	Windows 95、IPSec クライアント	Windows NT サーバー バージョン 4.0、Service Pack 5[1]	AIX 4.3.2	利用不能
ACE/Server	Windows NT Workstation 4.0、Service Pack 2 以上	Windows NT Server バージョン 4.0、Service Pack 5 以上	AIX 4.2	Solaris 2.5.1
SurfinGate 4.05				
サーバー	利用不能	Windows NT 4.0[2]	利用不能	利用不能

表 4. SecureWay Boundary Server 構成要素製品のソフトウェア要件 (続き)

SecureWay Boundary Server 構成要素	Microsoft Windows プラットフォーム		AIX	Solaris
	クライアント	サーバー	サーバー	サーバー
コンソール	Windows NT 4.0 以上[2] Windows 95、Windows 98	利用不能	利用不能	利用不能
MIMEsweeper for IBM SecureWay リリース 2				
MAILsweeper	利用不能	Windows NT 4.0[3]	利用不能	利用不能
WEBsweeper	Windows NT Workstation 4.0、Service Pack 3 以上	Windows NT 4.0[4]	利用不能	利用不能

注:

1. 必要な修正については、IBM Firewall for Windows NT と一緒に提供された資料を調べてください。
2. さらに、以下のとおりです。
   - Microsoft Windows 用の Windows ネットワーク・クライアントが必要です。
   - Windows NT Workstation はサポートされません。
3. さらに、以下のとおりです。
   - NT 3.5.1 および Windows NT Workstation はサポートされません。
   - 以下の環境のうちの 1 つが必要です。
     - Microsoft Exchange
     - SMTP
     - cc:Mail™
     - Groupwise
     - Lotus Notes
4. MIMEsweeper の推奨事項については、69ページの『MIMEsweeper の考慮事項』を参照してください。

SecureWay Boundary Server 構成要素の考慮事項

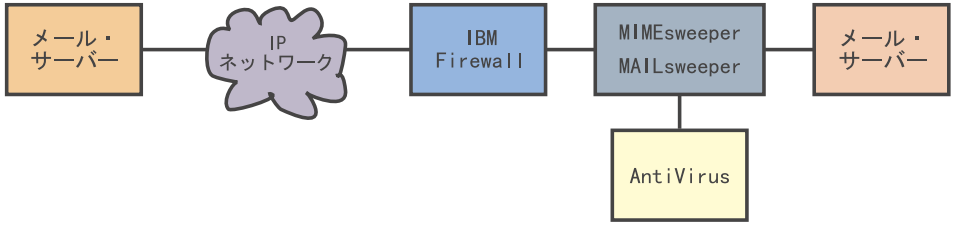
以下の節では、SecureWay Boundary Server 構成要素製品のインストールと構成についての考慮事項について説明します。

IBM Firewall の考慮事項

IBM Firewall に対する考慮事項は、主に、他の SecureWay Boundary Server 製品との関連でインストールした場合のトラフィックの流れにあります。

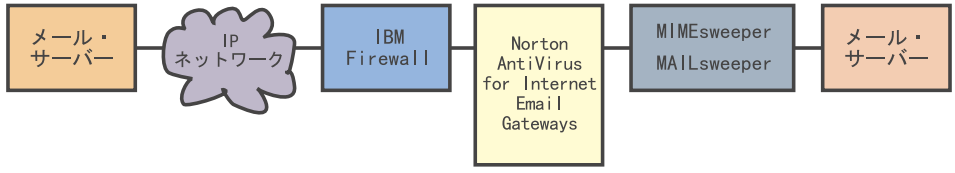
サンプル構成

IBM Firewall と MAILsweeper のサンプル構成: IBM Firewall と MIMEsweeper の両方をインストールする場合は、この節に説明された構成を使用することができます。



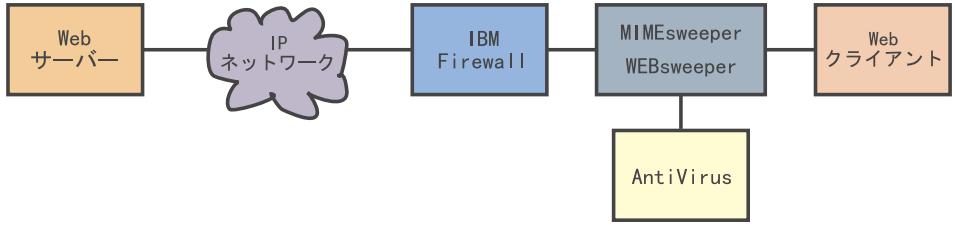
- MAILsweeper は、MIMEsweeper の一部であり、メール・メッセージの内容を検査します。 MAILsweeper には、アンチウィルスの検査を可能にする機能があります。
- MAILsweeper は、IBM Firewall とセキュア SMTP サーバーの間に置かれます。
- IBM Firewall は、メール転送のためのメール・ホストとして、MAILsweeper をポイントします。
  - IBM Firewall では、事前定義のメール規則を設定して、メールのトラフィックが流れるようにする必要があります。
- SMTP サーバーも、メール転送のためのメール・ホストとして、MAILsweeper をポイントする必要があります。
- MAILsweeper は、転送された両方向に流れるメール・メッセージの内容を検査します。

IBM Firewall、Norton AntiVirus for Internet Email Gateways、および MIMEsweeper のサンプル構成: IBM Firewall、Norton AntiVirus for Internet Email Gateways、および MIMEsweeper をインストールする場合は、この節に説明された構成を使用することができます。このシナリオでは、IBM Firewall、Norton AntiVirus for Internet Email Gateways、および MAILsweeper をチェーンで結合して、以下の図に示したように、ウィルスの有無と内容について、メールを検査します。



- ファイアウォールは、そのセキュア・メール・サーバーとして、 Norton AntiVirus for Internet Email Gateways をポイントします。この特定のトラフィックを可能にするには、正しいファイアウォール規則を設定する必要があります。
- Norton AntiVirus for Internet Email Gateways は、セキュア・メールのメール転送先として MAILsweeper をポイントし、外部宛てのメールにはファイアウォールをポイントします。
- MAILsweeper は、自分に転送されたメールを受け取って検査します。次に、そのメールを、経路指定テーブルまたは MX レコード・ルックアップに従って、正しいサーバーに転送します。 MAILsweeper と Norton AntiVirus for Internet Email Gateways が同じマシンに存在する場合、 MAILsweeper 用の受信ポートを変更して、Norton AntiVirus for Internet Email Gateways との競合を避ける必要があります。

IBM Firewall と WEBsweeper のサンプル構成: IBM Firewall と MIMEsweeper の両方をインストールする場合は、この節に説明された構成を使用することができます。



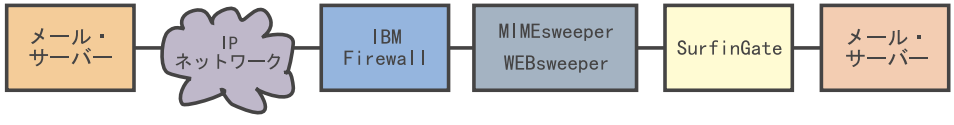
- WEBsweeper は、MIMEsweeper の一部であり、Web のトラフィックを検査します。 WEBsweeper には、アンチウィルスの検査を可能にする機能があります。
- WEBsweeper は、中間プロキシーとして働きます。クライアントは、そのプロキシーとして WEBsweeper をポイントします。次に、WEBsweeper は、トラフィックをファイアウォール・プロキシーに転送するよう設定します。
- プロキシー・トラフィックを可能にするためには、ファイアウォール上で規則を設定する必要があります。

- プロキシー要求は、ファイアウォールの後方にあるセキュア・ネットワークからのみ送ることができます。
- WEBsweeper は HTTPS を取り扱いません。 HTTPS を使用するためには、ファイアウォールでの問題を回避し、すべての Web トラフィックを検査するようにするために、WEBsweeper をう回する必要があります。ファイアウォール・プロキシーには、直接ポイントする必要があります。 Web トラフィックはそれでも保護されますが、WEBsweeper による検査は行われません。

IBM Firewall と SurfinGate のサンプル構成: IBM Firewall と SurfinGate をインストールする場合は、この節に説明された構成を使用することができます。

- SurfinGate は、ActiveX コントロールおよび他の項目について、Web トラフィックを検査します。
- SurfinGate は、中間の Web プロキシーとして働きます。クライアントは、HTTP、FTP、および HTTPS に対するプロキシーとして、SurfinGate をポイントします。次に SurfinGate は、その要求を IBM Firewall プロキシーに転送します。
- プロキシー・トラフィックを可能にするためには、ファイアウォール上で規則を設定する必要があります。
- プロキシー要求は、ファイアウォールの後方にあるセキュア・ネットワークからのみ送ることができます。

IBM Firewall、MIMEsweeper、および SurfinGate のサンプル構成: IBM Firewall、MIMEsweeper、および SurfinGate をインストールする場合は、この節に説明された構成を使用することができます。



- SurfinGate は、ActiveX コントロールおよび他の項目について、Web トラフィックを検査します。これは、MIMEsweeper の WEBsweeper 構成要素とは異なる検査を行います。

- SurfinGate と WEBsweeper は、中間の Web プロキシーとして働きます。クライアントは、HTTP および FTP に対するプロキシーとして SurfinGate をポイントします。次に SurfinGate は、その要求を WEBsweeper に転送します。さらに WEBsweeper は、その要求を IBM Firewall プロキシーに転送します。
- プロキシー・トラフィックを可能にするためには、ファイアウォール上で規則を設定する必要があります。これらの規則は、*IBM eNetwork Firewall Version 3.3 for Windows NT User's Guide* に定義されています。
- プロキシー要求は、ファイアウォールの後方にあるセキュア・ネットワークからのみ送ることができます。
- WEBsweeper は HTTPS を取り扱いません。 HTTPS を使用する場合、ファイアウォールでの問題を回避し、すべての Web トラフィックを検査するようにするために、WEBsweeper をう回する必要があります。ファイアウォール・プロキシーには、直接ポイントする必要があります。 Web トラフィックはそれでも保護されますが、WEBsweeper による検査は行われません。

MIMEsweeper の考慮事項

以下は、典型的な WEBsweeper システムです。

- Intel Pentium 400 MHz 以上
- 1GB のディスク・スペースと 128 MB の RAM
- Windows NT Server または Workstation バージョン 4.0 Server Service Pack 3 以上
- TCP/IP プロトコル (ホスト名とドメイン名を含む)
- アンチウィルス・ツール

以下は、並行ユーザーが最大 500 人までの、典型的な大規模の WEBsweeper 環境です。

- デュアルの Intel Pentium II、450 MHz 以上
- 3GB のディスク・スペースと 256 MB の RAM
- Windows NT Server または Workstation バージョン 4.0 Server Service Pack 3 以上
- TCP/IP プロトコル (ホスト名とドメイン名を含む)
- アンチウィルス・ツール

500 人を超える並行ユーザーをサポートする環境では、複数の WEBsweeper サーバーを使用することをお勧めします。

第13章 Intrusion Immunity の要件とインストールの注意点

この章では、Intrusion Immunity の構成要素である、Tivoli Cross-Site for Security と Norton AntiVirus のハードウェアとソフトウェアの要件について挙げます。

Intrusion Immunity のハードウェアとソフトウェアの要件

以下の節では、Intrusion Immunity 構成要素製品のインストールと構成について説明します。

Tivoli Cross-Site for Security のハードウェアとソフトウェアの要件は、表5、72ページの表6、および 72ページの表7 にあります。 Norton AntiVirus 構成要素のハードウェアとソフトウェアの要件は、73ページの表8 と 73ページの表9 にあります。

表5. Tivoli Cross-Site for Security サーバーのハードウェアとソフトウェアの要件

サーバーの要件	
オペレーティング・システム	• AIX 4.3.2 • Windows NT バージョン 4.0、Service Pack 5 • Solaris 2.5.1 または 2.6
Java	JDK 1.1.6 revision 04 以上
Web サーバー	Netscape Enterprise Server 3.51
データベース	• IBM DB2 リリース 5.2 • Oracle 7.3.4 (または 8.0.4 を推奨) • Microsoft SQL Server
ディスク・スペース	• Windows NT 290 MB • AIX 180 MB • Solaris 180 MB
メモリー	256 MB
スワップ・スペース	300 MB (400 MB を推奨)
注: 1. Netscape Enterprise Server 3.51 と 3.6 はサポートされません。 2. Tivoli Cross-Site for Security のインストールの資料で、Solaris のパッチの要件を参照してください。	

表 6. Tivoli Cross-Site for Security 管理コンソールのハードウェアとソフトウェアの要件

管理コンソールの要件	
オペレーティング・システム	• Windows 95 • Windows 98 • Windows NT バージョン 4.0、Service Pack 5 (166 MHz 以上のマシンを推奨) • Sun SPARC で実行される Solaris 2.5.1 または 2.6
ディスク・スペース	すべてのプラットフォームで 25 MB
メモリー	• Windows NT 40 MB • AIX 64 MB • Solaris 40 MB

表 7. Tivoli Cross-Site for Security エージェントのハードウェアとソフトウェアの要件

エージェントの要件	
オペレーティング・システム	• Windows NT バージョン 4.0、Service Pack 5 以上 • AIX 4.3.2 • Sun SPARC で実行される Solaris 2.5.1 または 2.6
Java	Solaris 上の JDK 1.1.6 revision 04 以上 (UNIX の場合のみ必要)
ディスク・スペース	• Windows NT 上に 15 MB • AIX 上に 10 MB • Solaris 上に 10 MB
メモリー	• Windows NT 上に 32 MB • AIX 上に 32 MB • Solaris 上に 20 MB
注: 1. Netscape Enterprise Server 3.51 と 3.6 はサポートされません。 2. Tivoli Cross-Site for Security のインストールの資料で、Solaris のパッチの要件を参照してください。	

73ページの表8 は、Norton AntiVirus のハードウェア要件のリストです。

表 8. Norton AntiVirus のハードウェア要件

Intrusion Immunity 構成要素	マシン・タイプ	ディスク・スペース	メモリー	その他
Norton AntiVirus	Intel CPU	24 MB	最小: 16 MB 推奨: 32 MB	CD-ROM ドライブ
Norton AntiVirus for Internet E-mail Gateways	Pentium 133 以上	6 MB	32 MB	CD-ROM ドライブ 効率的なメール操作のためには 500 MB ～ 5 GB

表 9. Norton AntiVirus のソフトウェア要件

Intrusion Immunity 構成要素	Microsoft Windows プラットフォーム		OS/2
	クライアント	サーバー	クライアント
Norton AntiVirus[1]	Windows NT 4.0 Windows 95、Windows 98	Windows NT 4.0	OS/2 2.11 以上

注:

1. さらに、Norton AntiVirus for Internet Email Gateways には、TCP/IP インターネット接続が必要です。

Norton AntiVirus は、AIX および Solaris では利用不能です。

Tivoli Cross-Site for Security のインストールの注意点

以下の図は、e-business ネットワークにおける、Cross-Site for Security エージェントと Cross-Site for Security 管理サーバーの典型的な配置を示したものです。

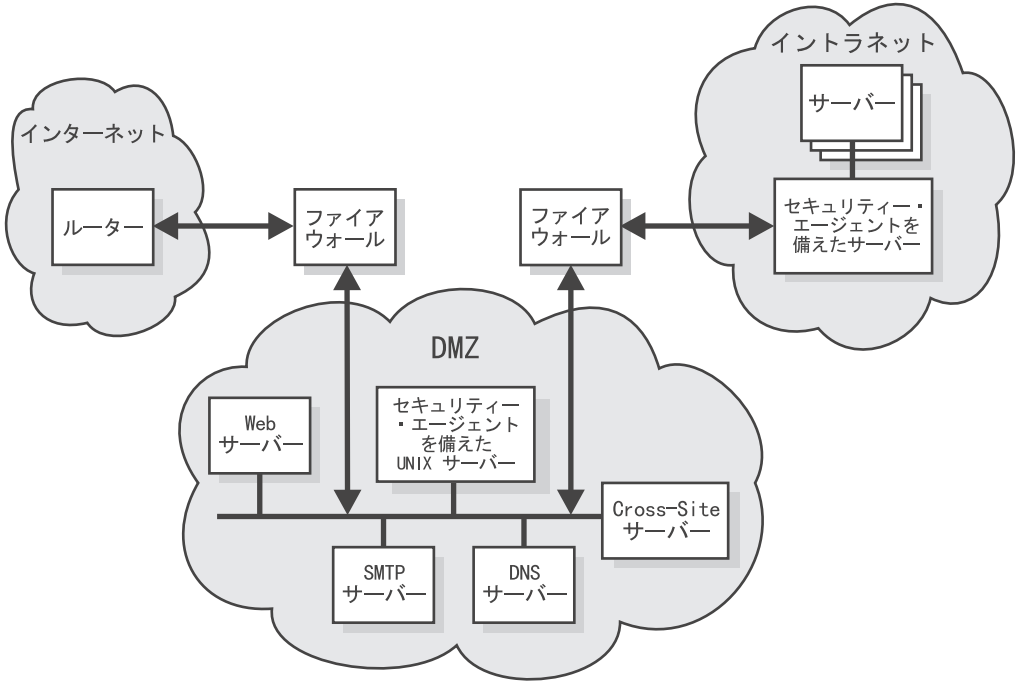


図 11. DMZ への Cross-Site for Security 管理サーバーのインストール

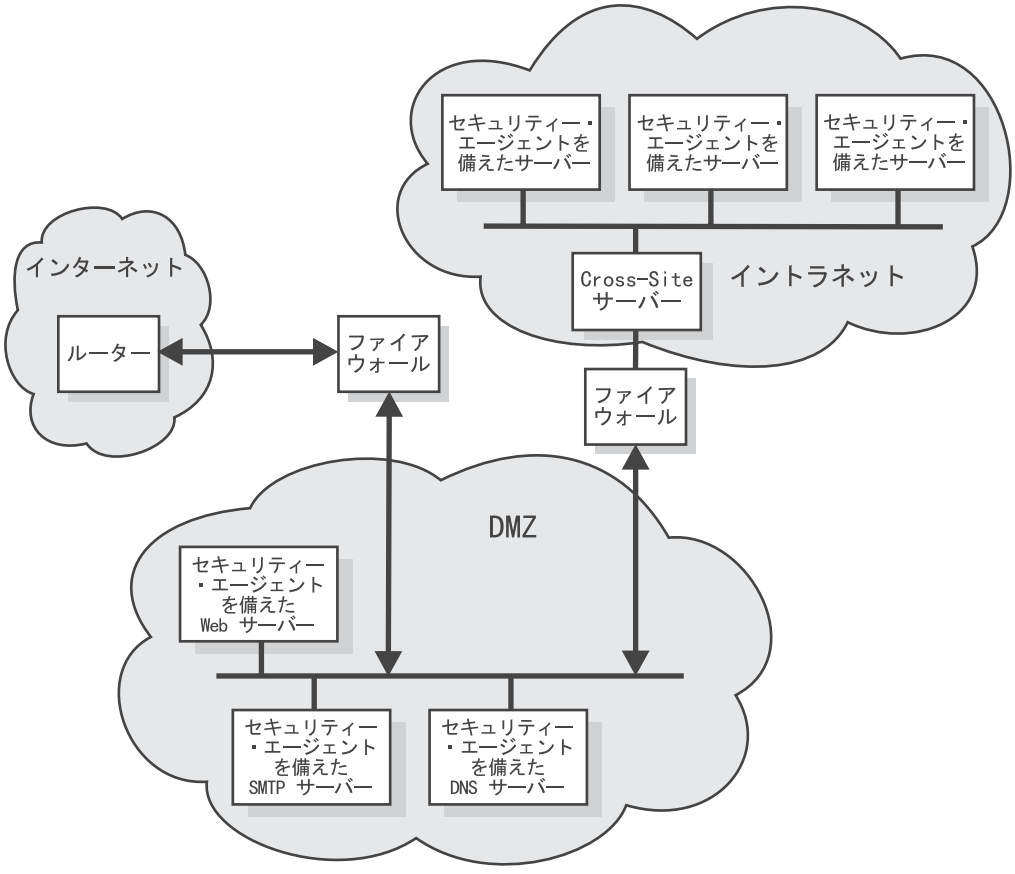


図 12. イントラネットへの Cross-Site for Security 管理サーバーのインストール

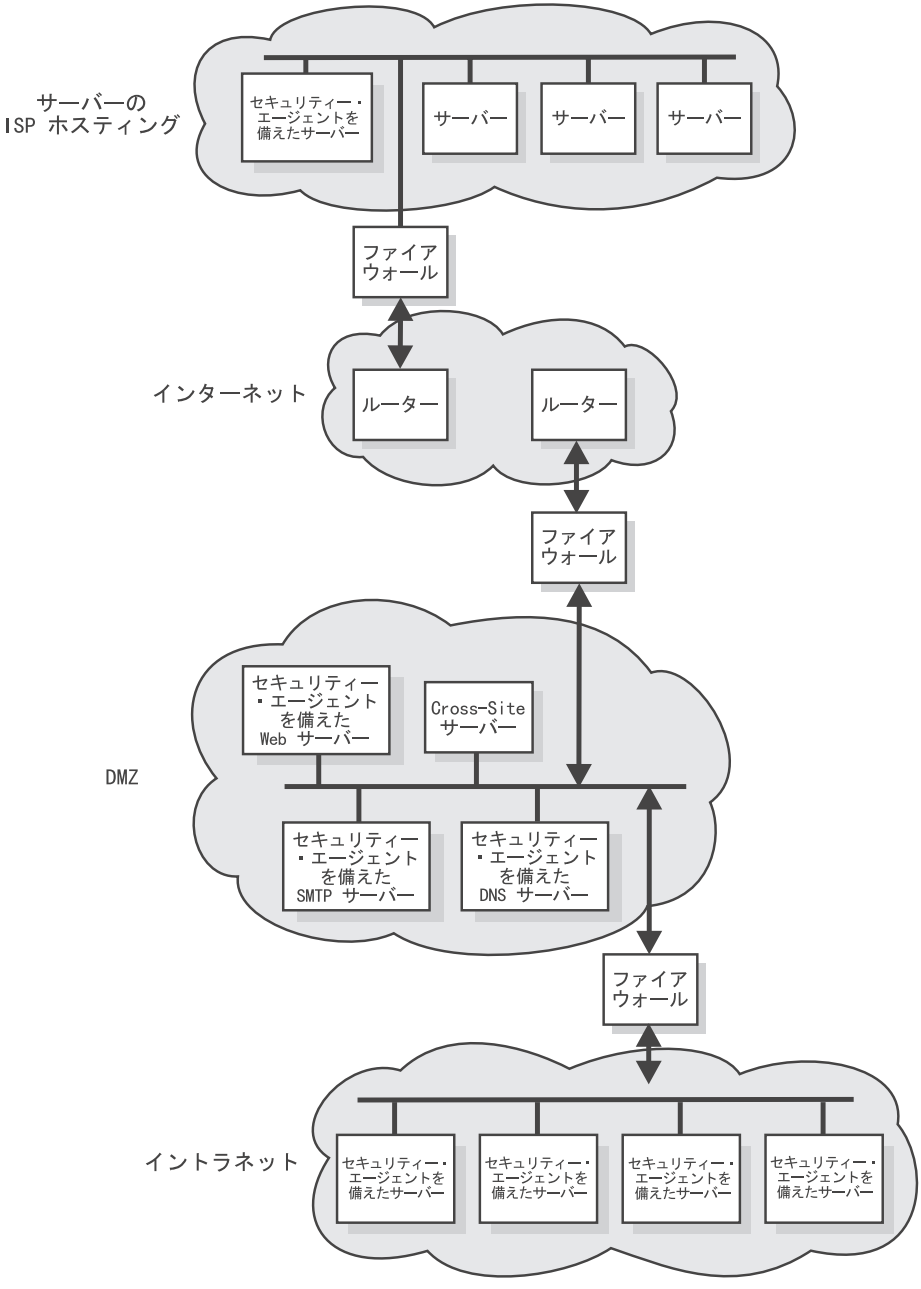


図 13. インターネットに接続されたサーバーをサポートする DMZ 内の Cross-Site for Security 管理サーバーのインストール

Norton AntiVirus のインストールの注意点

Norton AntiVirus のインストールについての情報は、contents.txt という名前のファイルの中にありますが、これは製品 CD のルート・ディレクトリーにあります。

第14章 Public Key Infrastructure の要件とインストールの注意点

今日の企業では、セキュア e-business アプリケーションのための公開キー・インフラストラクチャーを必要としていますが、FirstSecure Trust Authority は、公開キー・インフラストラクチャーを導入するために、以下の 2 つのレベルの機能を提供しています。

- 以下のものを提供する、ディジタル証明書の完全なライフ・サイクルの管理
  - 証明書の要求、更新、および取り消しを行うための機能
  - 認証要求を承認する登録局
  - ディジタル証明書と取り消しリストを作成するための認証局
- ビジネスが、信頼性のある e-business エンティティーをオンラインで登録できるようにするための、拡張された登録機能。登録アプリケーションは、以下の原則で構築されています。
  - 発行および管理される証明書は、機密性の高い e-business アプリケーションで必要とされる、信頼に値するものでなければならず、同じ高度の信頼性とセキュリティーの要件に合わせるために、登録局を構築する必要があります。
  - アプリケーションは、手作業または自動による承認、柔軟性のあるオンサイトまたはオフサイトの認証、および登録ポリシーを別個の信頼性のあるドメインと分離するためのオプションなど、さまざまな登録ポリシーをサポートするための柔軟性を備えたものである必要があります。

トラスト・モデルは、電子取り引きのアクセス可能性、機密性、整合性、出所を保証するのに役立ちます。ディジタルでの暗号化、認証、および署名を使用して、 Trust Authority は、インターネット、イントラネット、または VPN (仮想私設網) を介したセキュア e-business の遂行を可能にします。署名キーの拡張セキュリティーのために、認証局は、暗号ハードウェアを使用して作業を行うよう設計されています。

Trust Authority サーバーのハードウェアとソフトウェアの要件

Trust Authority 構成要素に対するサーバーのソフトウェア要件は、80ページの表10 にリストされています。

表 10. Public Key Infrastructure Trust Authority 構成要素に対するサーバー・ソフトウェアと任意選択ハードウェアの要件

製品	注
以下のオペレーティング・システムの 1 つ • IBM AIX/6000 (AIX)、バージョン 4.3.2 • Microsoft Windows NT、バージョン 4.0 (Service Pack 5 付き)	• 必須。 • すべての Trust Authority サーバーを同じプラットフォームにインストールする必要があります。同じシステム構成の中に AIX と Windows NT のマシンを混ぜることはできません。
IBM SecureWay Directory バージョン 3.1.1	• 必須: Trust Authority コードと統合。 • Trust Authority のインストール中に、Trust Authority をインストールしたのと同じマシンに Directory ソフトウェアをインストールするか、またはそれをリモート・マシンにインストールすることができます。
IBM WebSphere Application Server Version 2.02、標準版。 IBM HTTP Server バージョン 1.3.3 と Sun Java Development Kit (JDK) 1.1.7 を含む。	• 必須: Trust Authority の媒体パッケージの中に入れて提供。 • Trust Authority をインストールする前に、Trust Authority と Trust Authority サーバー・ソフトウェアをインストールする予定である、同じマシンに Web サーバー・ソフトウェアをインストールしておく必要があります。
IBM DB2 ユニバーサル・データベース・エンタープライズ・エディションのバージョン 5.2 (保守パッチ 9 付きのもの)。	• 必須: Trust Authority の媒体パッケージの中に入れて提供。 • 固有のデータベース・インスタンスが、各サーバー構成要素ごとに存在します。 Trust Authority をインストールする前に、Trust Authority サーバーとして使用を予定している各マシンに、DB2 をインストールしておく必要があります。
• IBM SecureWay 4758 PCI Cryptographic Coprocessor、Model 001 • IBM SecureWay 4758 CCA Support Program、バージョン 1.3.0.0 (保守パッチ 1.3.0.1 付き)	• *任意選択* で、AIX システムでのみ使用可能: この製品は、通常の IBM 製品の発注方法で注文する必要があります。 • Trust Authority をインストールする前に、Trust Authority CA をインストールする予定のサーバーに、4758 ハードウェアをインストールしておく必要があります。 • 4758 暗号カードは、RS/6000 上に PCI バスを 1 つ必要とします。

81ページの表11 と 82ページの表12 に、Trust Authority のサーバー・ハードウェアの要件をリストしています。

表11 と 82ページの表12 は、以下を前提としています。

- 小規模の実稼働環境で、毎日、100 件程度の証明書を発行する。
- 中規模の実稼働環境で、毎日、1000 件程度の証明書を発行する。
- 大規模の実稼働環境で、毎日、数千件の証明書を発行する。これはまた、他の組織に第三者 CA サービスを提供するシステムにもなります。

Windows NT で Trust Authority を実行する計画である場合、IBM では、Trust Authority を IBM Netfinity® サーバーにインストールすることをお勧めしています。以下の表は、Trust Authority Certificate Authority を介して発行すると予想される証明書の数をベースにした、推奨されるシステム・サイズを提供するものです。

表 11. サンプル Windows NT マシン構成

マシン・タイプ	プロセッサー	ディスク・スペース	メモリー
小規模の実稼働環境			
Netfinity 3000	1 (450 MHz, Pentium II)	2 ドライブ (9.1 GB)	256 MB
Netfinity 5000	2 (450 MHz, Pentium II)	2 ドライブ (9.1 GB)	512 MB
中規模の実稼働環境			
Netfinity 3000	1 (500 MHz, Pentium III)	4 ドライブ (18.2 GB)	768 MB
Netfinity 5000	2 (500 MHz, Pentium III)	4 ドライブ (9.1 GB)	1 GB

表 11. サンプル Windows NT マシン構成 (続き)

マシン・タイプ	プロセッサー	ディスク・スペース	メモリー
大規模の実稼働環境			
Netfinity 5500	2 (450 MHz, Pentium III)	4 ドライブ (9.1 GB 高速)	1 GB
Netfinity 5500	4 (500 MHz, Pentium III Xeon, 1024K L2 キャッシュ付き)	4 ドライブ (9.1 GB 高速)	1 GB
Netfinity 7000	2 (500 MHz, Pentium III, 512K L2 キャッシュ付き)	4 ドライブ (9.1 GB 高速)	1 GB
Netfinity 7000	4 (500 MHz, Pentium III Xeon, 1024K L2 キャッシュ付き)	4 ドライブ (18.2 GB)	2 GB

AIX で Trust Authority を実行する計画である場合、 Trust Authority を IBM® RISC System/6000® マシンにインストールする必要があります。以下の表は、Trust Authority Certificate Authority を介して発行すると予想される証明書の数をベースにした、推奨されるシステム・サイズを提供するものです。

表 12. サンプル AIX マシンのハードウェア構成

マシン・タイプ	プロセッサー	ディスク・スペース	メモリー
小規模の実稼働環境			
F40	2 (233 MHz)	2 ドライブ (9.1 GB, Ultra 2 Fast Wide)	512 MB
中規模の実稼働環境			
F40	2 (233 MHz)	3 ドライブ (9.1 GB, Ultra 2 Fast Wide)	1 GB
大規模の実稼働環境			
F50	4 (332 MHz)	5 ドライブ (1 ドライブの 9.1 GB Ultra 2 Fast Wide と 4 ドライブの 9.1 GB SSA)	2 GB

表 12. サンプル AIX マシンのハードウェア構成 (続き)

マシン・タイプ	プロセッサー	ディスク・スペース	メモリー
H50	4 (332 MHz)	5 ドライブ (1 ドライブの 9.1 GB Ultra 2 Fast Wide と 4 ドライブの 9.1 GB SSA)	2 GB
R50	6 (200 MHz)	2 ドライブ (9.1 GB Ultra 2 Fast Wide)	1 GB
R50	8 (200 MHz)	5 ドライブ (1 ドライブの 9.1 GB Ultra 2 Fast Wide と 4 ドライブの 9.1 GB SSA を備えた 7133 SSA ラック)	2 GB

Trust Authority クライアントのハードウェアとソフトウェアの要件

IBM では、ブラウザー登録フォームを使用するためと、Trust Authority クライアント・アプリケーションを実行するために、以下のワークステーション構成をお勧めしています。

- 以下の物理マシン・セットアップ:
  - 最小限 32 MB メモリーを備えた 166 MHz Intel 486 プロセッサー (少なくとも、 64 MB のメモリーを備えた 200 MHz Intel Pentium プロセッサーが望ましい)
  - グラフィックス・カード
  - VGA ビデオ・ディスプレイ、またはそれ以上のもの
  - マウスまたはマウス互換のポインティング・デバイス
- 以下のオペレーティング・システムの 1 つ:
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT、バージョン 4.0
- 以下の Web ブラウザーの 1 つ:
  - Netscape Navigator または Netscape Communicator、バージョン 3.0 以上
  - Microsoft Internet Explorer、バージョン 4.0 以上 (Java が使用可能なもの)

IBM KeyWorks Toolkit と IBM SecureWay Trust Authority の相互作用

IBM KeyWorks Toolkit は、IBM SecureWay Trust Authority と同じサーバーにはインストールしないでください。

第15章 Toolbox のインストール要件と考慮事項

FirstSecure Toolbox は、e-business でセキュア・アプリケーションを開発するのに役立つ、1 組の API です。

- 許可サービス
- 証明および管理サービス
- ディレクトリー・サービス
- セキュア・ソケット・レイヤー・プロトコル・サービス
- KeyWorks 暗号およびトラスト管理サービス
  - IBM Key Recovery Service Provider 1.1.3.0 API。 IBM Key Recovery Service Provider により、暗号化された情報の回復が可能になります。
  - IBM Key Recovery Server 1.1.3.0。IBM Key Recovery Server 1.1.3.0 は 1 つのアプリケーションであり、許可された要求があると、キーが使用不能になるか、失われるか、または損傷を受けたときに、暗号化された情報を回復することができます。

    これらの 2 つのツールキットは、セキュリティー・プロバイダーがツールキットにプラグインするために使用できる標準インターフェースだけでなく、アプリケーションが重要なセキュリティー・サービスを起動するために使用できる標準インターフェースを提供します。標準インターフェースは、Common Data Security Architecture (CDSA) に基づいています。これらのツールキットは、Windows NT、Solaris、および AIX で使用可能です。

Toolbox のハードウェアとソフトウェアの要件

Toolbox のハードウェア要件を、表13 に示します。

表 13. Toolbox のハードウェア要件

プラットフォーム	ディスク・スペース	メモリー
バージョン 4.0、Service Pack 5	2 〜 4 GB	64 MB
AIX 4.3.2	9.1 GB	1 GB
Sun Solaris, Version 2.6 (1999 年 5 月の Fix Pak 付き)	4.2 GB	128 MB

表 14. Toolbox 構成要素製品のハードウェア要件

ツールキット	マシン・タイプ	ディスク・スペース	メモリー
IBM KeyWorks Toolkit	以下で実行する製品をサポートするハードウェア: Windows NT バージョン 4.0、Service Pack 5 以上 Windows 95 AIX 4.2 以上 Sun Solaris	50 MB	32 MB
IBM Key Recovery Service Provider	以下で実行する製品をサポートするハードウェア: Windows NT バージョン 4.0、Service Pack 5 以上 Windows 95 AIX 4.2 以上 Sun Solaris	50 MB	32 MB

Toolbox 構成要素製品のソフトウェア要件は、以下の表に示されています。

表 15. Toolbox 構成要素製品のソフトウェア要件

Toolbox 構成要素	Microsoft Windows プラットフォーム		AIX	Solaris
	クライアント	サーバー	サーバー	サーバー
IBM KeyWorks Toolkit	Windows NT バージョン 4.0、Service Pack 5 以上 Windows 95	Windows NT バージョン 4.0、Service Pack 5 以上 Windows 95	AIX 4.2 以上[1]	Sun Solaris
IBM Key Recovery Service Provider	Windows NT バージョン 4.0、Service Pack 5 以上[2] Windows 95	Windows NT バージョン 4.0、Service Pack 5 以上	AIX 4.2 以上	Sun Solaris

注:
1. AIX クライアントもサポートされます。
2. さらに、IBM KeyWorks Toolkit が必要です。

IBM KeyWorks Toolkit 1.1

IBM KeyWorks Toolkit 1.1 は、アプリケーションの開発者に対して、異なる操作環境にまたがって、暗号化機能および他のセキュリティー機能にアクセスするための、オープンで、拡張可能な、標準の手段を提供します。

IBM KeyWorks Toolkit は、 Service Provider アドイン・モジュールがツールキットとインターフェースをとるために使用できる標準インターフェースだけでなく、アプリケーションが重要な暗号、トラスト、およびセキュリティーのサービスを起動するために使用できる標準インターフェース (API) を提供します。これらの標準インターフェースは、Common Data Security Architecture (CDSA) をベースとしたものです。 CDSA は、Open Group からの標準であり、最初は Intel™ Corporation によって開発され、 IBM によって KeyWorks Toolkit に拡張されたものです。標準インターフェースを使用すると、以下のようになります。

- 企業では、ニーズに最も敵した暗号化とトラストの導入を選択することができ、セキュリティー・サービスを使用するアプリケーションを変更する必要はありません。
- アプリケーションとミドルウェアのプログラマーの生産性が向上します。

IBM KeyWorks Toolkit は、アプリケーションとクラスとしてのミドルウェアとの間、および暗号化機能と Service Provider との間に、1 つの遮へい層を提供します。ツールキットには、フレームワークと Service Provider のプラグイン・モジュールが含まれています。

アプリケーションに対しては、フレームワークで、Intel Corporation の CDSA から、機能的に優れた Common Security Services Manager (CSSM) API を提供します。 IBM では、キー回復機能を追加することによって、CSSM API を拡張しています。 IBM KeyWorks Toolkit を使用すれば、アプリケーションでは、以下のことが可能になります。

- 情報の暗号化と暗号化解除
- さまざまな目的でのディジタル署名の検査
- ディレクトリーからの証明書および証明書取り消しリストの検索
- キー回復と暗号バックアップのためのキー回復フィールドの作成
- ユーザーの指示でシステム設計者およびプログラマーによって設定された基準に基づいた、証明書が信頼できるかどうかの判断

通常、企業または OEM では、IBM KeyWorks Toolkit および IBM Key Recovery Service Provider Toolkit をアプリケーションおよびミドルウェアと統合して、CSSM フレームワークで CSSM API を使用できるようにしています。このようにして統合した製品は、サーバーおよびクライアント用の 1 組の実行時アプリケーションおよびミドルウェアであり、その操作環境内または他の複数の環境に配布されます。 FirstSecure の他の要素は、常時、すべての暗号サービスとトラスト・ポリシー操作について、IBM KeyWorks Toolkit に依存することになります。

IBM KeyWorks Toolkit を使用する統合業者は、ミドルウェアやフレームワークだけでなく、暗号化の設計とプログラミングに対してかなりの広範囲な経験を持ったシステム・エンジニアとプログラマーを有しているか、またはそのような経験を持つ統合業者または OEM と契約を結んでアクセスできる必要があります。

Key Recovery Service Provider の場合、このフレームワークは、標準の Service Provider Interface (SPI) である Open Group の CDSA を提供します。 IBM では、キー回復機能を追加して SPI を拡張しています。

IBM KeyWorks Toolkit (SDK) には、オープン標準と所有者の公開キー証明をサポートする、プラグインの Key Recovery Service Provider モジュールが含まれています。これらのモジュールには、PKCS#11、RSA Data Security の BSAFE 暗号機能、 X.509V3 認証、Entrust and Verisign のトラスト・ポリシ

ー、および Lightweight Directory Access Protocol (LDAP) があります。このフレームワークは、独立した Key Recovery Service Provider モジュールによって提供された、暗号機能、トラスト機能、およびセキュリティー機能の継ぎ目のない統合を提供します。

IBM KeyWorks Toolkit は、以下のものを含む、重要な管理機能を提供することができます。

- KeyWorks がサポートするプロセスの中の重要なステップをう回しないよう保護する
- Service Provider プラグイン・モジュールが使用する前に変更されていないことを検査する
- Service Provider プラグイン・モジュールを、フレームワークを介してのみ使用する
- 国固有および企業固有の暗号およびトラスト・ポリシーの使用法をサポートする

IBM KeyWorks Toolkit は、企業に対して、以下の利点を提供します。

- アプリケーションおよびミドルウェアの書き直しをせずに、Service Provider モジュールを変更または置き換えができる
- ハードウェアの暗号化とディジタル署名に対して、継ぎ目のないサポートを提供する
- LDAP ディレクトリーと DSA 署名の標準をサポートする
- 特定の認証局を使用する必要がない

IBM KeyWorks Toolkit の詳細については、*IBM KeyWorks Toolkit Developer's Guide* に説明があります。

IBM KeyWorks Toolkit と IBM SecureWay Trust Authority の相互作用

IBM KeyWorks Toolkit は、IBM SecureWay Trust Authority と同じサーバーにはインストールしないでください。

IBM Key Recovery Service Provider Toolkit 1.1

ツールキット・フォーマットで提供される IBM Key Recovery Service Provider 1.1.3.0 は、 IBM KeyWorks Toolkit によって提供される標準機能を使用する Service Provider モジュールです。IBM Key Recovery Service Provider を使用すると、秘密キーを集めて第三者が管理したり、暗号化の弱点が単一点にならないようにしなくても、保管された暗号化情報および伝送された暗号化情報の回復が可能になります。

IBM Key Recovery Service Provider は、IBM KeyWorks Toolkit によって提供される標準機能を使用するので、異なる暗号提供者、さまざまな認証局からの標準の証明書、Verisign and Entrust からのトラスト・ポリシー、および LDAP によってアクセスできるどのディレクトリーでも、このキー回復機能を使用することができます。IBM Key Recovery Service Provider は、通信者相互間の通信に関連するセッション・キーに基づいて、キー回復情報を作成します。

IBM Key Recovery Service Provider の詳細については、*Key Recovery Server Installation and Usage Guide* に説明があります (この資料は、FirstSecure 文書パックの中で提供されます)。

第16章 FirstSecure と一緒に提供される文書

FirstSecure に含まれている構成要素の各製品には、それぞれ独自の文書があります。本章では、各 FirstSecure 構成要素製品に含まれている文書についての情報を説明します。

媒体パックと文書パックが、 SecureWay FirstSecure、SecureWay Policy Director、および SecureWay Boundary Server に対して使用可能です。媒体パックには、オファリングの中の構成要素製品をインストールするための製品 CD が含まれており、それらの CD の一部にはオンライン文書が含まれています。文書パックには、それらを提供するこれらの構成要素製品についてのハードコピーのブックが含まれています。 100ページの『FirstSecure 文書パック』に、文書パックの内容を挙げます。

Policy Director

以下の文書は、Policy Director 構成要素製品と一緒に提供されます。

IBM SecureWay Policy Director 概説
: IBM SecureWay Policy Director をインストールして構成する方法について説明します。

IBM SecureWay Policy Director 管理の手引き
: IBM SecureWay Policy Director を管理する方法について説明します。このブックは、PDF 形式で提供されます。

IBM SecureWay Policy Director Programming Guide and Reference
: IBM SecureWay Policy Director 用のプログラムの書き方を説明しています。このブックは、PDF 形式で提供されます。

製品のREADME
: この情報は、www.ibm.com/software/security/policy の Web サイトで使用可能です。

SecureWay Boundary Server

以下のブックは、SecureWay Boundary Server 構成要素製品と、それらの要件、およびそれらの相互作用について説明しています。

IBM SecureWay Boundary Server for Windows NT and AIX: 概説
SecureWay Boundary Server 構成要素製品を説明しているハードコピー・ブック。

以下の節では、SecureWay Boundary Server 構成要素製品と一緒に提供される文書について説明します。

IBM SecureWay Firewall

すべての IBM Firewall の文書は、ソフトコピーで提供されます。 IBM Firewall は、以下の文書を提供します。

IBM SecureWay Firewall for AIX Setup and Installation
IBM SecureWay Firewall for AIX のインストールとセットアップのための説明。

IBM SecureWay Firewall for Windows NT Setup and Installation
IBM SecureWay Firewall for Windows NT のインストールとセットアップのための説明。

IBM SecureWay Firewall for AIX User's Guide
IBM SecureWay Firewall for Windows NT のインストールとセットアップのための説明。

IBM SecureWay Firewall for Windows NT User's Guide
IBM Firewall for Windows NT の使用に関する情報。

IBM SecureWay Firewall for Windows NT Reference
IBM Firewall for Windows NT を使用するための参照情報が含まれます。

IBM SecureWay Firewall for AIX Reference
IBM Firewall for AIX を使用するための参照情報が含まれます。

IBM SecureWay Firewall Problem Determination Guide for Windows NT and AIX
問題判別についての説明が含まれます。

IBM SecureWay Firewall VPN Client User's Guide
VPN (仮想私設網) のセットアップと使用法について説明しています。

MIMEsweeper

MIMEsweeper には、以下の文書が含まれています。

MIMEsweeper Administrator's Guide
リリース情報に関する節の後に、管理者に対する情報があり、これには計画とインストールについての情報が含まれます。

このブックは、HTML 形式で製品 CD に入って提供されます。このブックは、Web ブラウザーを使用して、¥DOC¥MANUAL.HTM という名前のファイルを表示することによって、オンラインで見ることができます。

MIMEsweeper Release Notes
更新された文書が含まれており、これには、インストール情報と、文書をオンラインで見るための説明が含まれています。

このブックは、HTML 形式で製品 CD に入って提供されます。このブックは、Web ブラウザーを使用して、¥DOC¥RELNOTES.HTM という名前のファイルを表示することによって、オンラインで見ることができます。

MIMEsweeper Configuration Editor Help
MIMEsweeper 構成ファイルの編集についての情報が含まれています。

この文書は、HTML 形式で製品 CD に入って提供されます。

SurfinGate

SurfinGate には、以下のソフトコピー文書が含まれています。

SurfinGate Installation Guide
SurfinGate 4.05 構成要素を Windows NT でインストールおよび構成する場合の情報。 *SurfinGate Installation Guide* の PDF 形式のバージョンは、製品 CD の ¥docs¥install.pdf というファイルに入っています。

SurfinGate User Guide
SurfinGate の計画と使用に関する情報。 *SurfinGate User Guide* の PDF 形式のバージョンは、製品 CD の ¥docs¥manual.pdf というファイルに入っています。

SurfinGate 4.05 for Windows NT Release Notes
SurfinGate 4.05 についての情報で、システム要件と製品の制限事項が含まれています。 *SurfinGate 4.05 for Windows NT Release Notes* の PDF 形式のバージョンは、製品 CD の ¥docs¥relnotes.pdf というファイルに入っています。

SurfinGate for Windows NT/UNIX Solaris Release Notes, Appendix A
SurfinGate に対する変更について説明したオンライン文書。この文書は、製品 CD の ¥docs¥rnappen.pdf というファイルに入っています。

Intrusion Immunity

以下の節では、Intrusion Immunity 構成要素製品と一緒に提供される文書について説明します。

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security、バージョン 1.1 には、以下の文書が .pdf 形式で含まれています。

Tivoli Cross-Site for Security Installation
この文書は、インストールの詳細な要件について説明し、インストール・ステップについて順を追って説明しています。

Tivoli Cross-Site for Security User's Guide
この文書は、製品の概要、コンソールの使用とタスクの実行についての説明、コマンド行インターフェースなどの参照情報、構成ファイル、および用語集があります。この文書には、製品 CD-ROM でアクセスできます。

Norton AntiVirus

Norton AntiVirus には、FirstSecure でサポートされる構成要素について、以下の文書が含まれています。 contents.txt ファイルを除くすべての文書は、PDF 形式で Norton AntiVirus CD に入れて納入されます。 contents.txt ファイルは、製品 CD に入った ASCII ファイルです。

Norton AntiVirus Solution Release 3.04 CD の文書の内容

¥contents.txt という名前の Norton AntiVirus Solution Release 3.04 CD ファイルは、その CD に入っているすべての文書をリストしています。

管理ソリューション:

Norton AntiVirus Solution Implementation Guide
製品 CD の ¥docs¥admin¥navimp.pdf を参照してください。

Norton AntiVirus Command-Line Scanner
製品 CD の ¥docs¥navc¥navcugd.pdf を参照してください。

Emergency Rescue Disk creation
製品 CD の ¥navc¥readme.txt を参照してください。

サーバー・ソリューション:

Norton AntiVirus for Windows NT Server Administrator's Guide
製品 CD の ¥docs¥admin¥navnts50.pdf を参照してください。

Norton AntiVirus for NetWare User's Guide
製品 CD の ¥docs¥NAVNLM¥NVN4.pdf を参照してください。

Norton AntiVirus for Lotus Notes Installation Guide
製品 CD の ¥docs¥NAVNOTES¥NAVNOTES.pdf を参照してください。

Norton AntiVirus for Lotus Notes Installation Guide
製品 CD の ¥docs¥NAVNOTES¥NAVNOTES.pdf を参照してください。

Norton AntiVirus for OS/2 Lotus Notes Installation Guide
製品 CD の ¥docs¥NOTESOS2¥NOTESOS2.pdf を参照してください。

Norton AntiVirus for Microsoft Exchange Installation Guide
製品 CD の ¥docs¥NAVXCHNG¥NAVXCHNG.pdf を参照してください。

ゲートウェイ・ソリューション:

Norton AntiVirus for Internet Email Gateway User's Guide
製品 CD の ¥docs¥navieg¥navieg.pdf を参照してください。

Norton AntiVirus for Firewalls Administrator's Guide
製品 CD の ¥docs¥navfw¥navfw.pdf を参照してください。

デスクトップ・ソリューション:

Norton AntiVirus User's Guide for Windows 3.1/DOS
製品 CD の ¥docs¥navwks¥nav4dusr.pdf を参照してください。

Norton AntiVirus Reference Guide for Windows 3.1/DOS
製品 CD の ¥docs¥navwks¥nav4dref.pdf を参照してください。

Norton AntiVirus for Windows 95/98 User's Guide
製品 CD の ¥docs¥navwks¥nav98usr.pdf を参照してください。

Norton AntiVirus for Windows 95/98 Reference Guide
製品 CD の ¥docs¥navwks¥nav98ref.pdf を参照してください。

Norton AntiVirus for Windows NT User's Guide
製品 CD の ¥docs¥navwks¥nav5nusr.pdf を参照してください。

Norton AntiVirus for Windows NT Reference Guide
製品 CD の ¥docs¥navwks¥nav5nref.pdf を参照してください。

Norton AntiVirus v4.0 User's Guide for Windows NT
製品 CD の ¥docs¥351¥navntugd.pdf を参照してください。

Norton AntiVirus v4.0 Reference Guide for Windows NT
製品 CD の ¥docs¥351¥navntref.pdf を参照してください。

Norton AntiVirus User's Guide for OS/2
製品 CD の ¥docs¥navos2¥navos2ug.pdf を参照してください。

Norton AntiVirus Distribution Guide for OS/2
製品 CD の ¥docs¥navos2¥navos2dg.pdf を参照してください。

Norton AntiVirus for Macintosh User's Guide
製品 CD の ¥docs¥navmac¥navmac.pdf を参照してください。

Norton AntiVirus Solution Release 3.04 CD 上のホワイト・ペーパー:
CD には、ディレクトリー ¥sarc の中にホワイト・ペーパーも入っています。それぞれのホワイト・ペーパーは、.pdf 形式になっています。

Norton AntiVirus Solution Release 3.04 CD 上のビデオ: CD には、ビデオも入っています。ビデオを見るためには、Media Player か、または .AVI ファイルを再生できる他のプログラムが必要です。ビデオは、以下のファイルに入っています。

SARC ¥sarc¥sarc.avi

About Viruses
¥sarc¥aboutvir.avi

Norton AntiVirus: the Guided Tour
¥navtour¥guided¥demo32.exe

How to Respond When Norton AntiVirus Alerts You
¥navtour¥alert¥demo32.exe

A Tour of Norton System Center
¥nsctour¥setup.exe

または、CD からツアーを直接実行する場合、

¥nsctour¥demo32.exe

ツアーについての詳細は、¥ncstour¥readme.txt というファイルに入っています。

Trust Authority

IBM SecureWay Trust Authority 製品の文書は、*Trust Authority 文書* CD-ROM で、 PDF 形式と HTML 形式で使用可能です。多くの情報は、Trust Authority がサポートする言語に翻訳されています。選択した言語で資料をアクセスする方法については、製品の *Readme* ファイルを参照してください。 *Readme* ファ

イルの最新バージョンは、 http://www.ibm.com/software/security/trust/library にある IBM SecureWay Trust Authority Web サイトの Library ページで常に使用可能です。

Trust Authority ライブラリーには、以下の文書が含まれています。

IBM SecureWay Trust Authority Up and Running
このブックは、製品の概要です。インストール手順を含む、製品の要件がリストされ、各構成要素ごとに使用可能なオンライン・ヘルプのアクセス方法についての情報を提供します。文書 CD-ROM で使用可能なことに加えて、このブックは、印刷され、製品と一緒に配布されます。

IBM SecureWay Trust Authority System Administration Guide
このブックには、Trust Authority システムの管理についての一般情報が含まれています。このブックには、サーバーの開始と停止、パスワードの変更、認証局の管理、監査の実施、およびデータ保全性検査の実行についての手順が含まれています。

IBM SecureWay Trust Authority Configuration Guide
このブックには、Trust Authority システムを構成するための セットアップ・ウィザード の使用方法についての情報が含まれています。ウィザードのオンライン・ヘルプを見ながら、このガイドの HTML バージョンにアクセスすることができます。

IBM SecureWay Trust Authority Registration Authority Desktop Guide
このブックには、証明書ライフ・サイクル全体を通して証明書を管理するための RA Desktop の使用方法についての情報が含まれています。デスクトップのオンライン・ヘルプを見ながら、このガイドの HTML バージョンにアクセスすることができます。

IBM SecureWay Trust Authority User's Guide
このブックには、証明書を取得する方法についての情報が含まれています。このブックは、Trust Authority 登録フォームを使用して、ブラウザー、サーバー、およびデバイスについての証明書を要求する手順を提供します。このブックはまた、ユーザーに対して、PKIX 証明書の事前登録の方法、および PKIX 証明書を保管および管理するための Trust Authority クライアントの使用方法についても示します。クライアントのオンライン・ヘルプを見ながら、このガイドの HTML バージョンにアクセスすることができます。

Toolbox

以下の節では、Toolbox 構成要素製品と一緒に提供される文書について説明します。

Toolbox API

すべての Toolbox 文書は、
www.ibm.com/software/security/firstsecure/library の Web サイトで使用可能です。以下の文書が含まれています。

IBM SecureWay Secure Sockets Layer Toolkit Programming Guide and Reference
API と iKeyman の概要を提供します。それぞれの API、その構文、およびその使用法を定義します。

IBM SecureWay Directory Client SDK Programming Reference
さまざまな LDAP サンプル・クライアント・プログラムと、アプリケーションに LDAP サーバーへのアクセスを提供する LDAP クライアント・ライブラリーが含まれています。サポートは、C 用と Java 用が提供されます。

IBM SecureWay Policy Director Programming Guide and Reference
それぞれの API、その構文、およびその使用法を定義します。

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Installation Guide
インストールの指示と要件を提供します。

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference
IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms (PKIX とも呼ばれます) を使用してアプリケーションを開発しているプログラマーに対して情報を提供します。製品の概要、別々の PKIX 構成要素ごとのプログラム作成のための指示、および PKIX API の説明が含まれています。

IBM KeyWorks Toolkit

IBM KeyWorks Toolkit と一緒に提供されるすべての文書は、オンラインであり、製品 CD に PDF 形式で入っています。文書は、以下のとおりです。

IBM KeyWorks Toolkit Developer's Guide
ツールキットの概要を提供します。また、ツールキットをアプリケーションの中に組み込む方法も説明され、サンプル・アプリケーションが入っています。

IBM KeyWorks Toolkit Application Programming Interface (API) Specification
フレームワークおよびサービス提供者のモジュールによって提供されたセキュリティー・サービスにアクセスするために、アプリケーション開発者が使用するインターフェースを定義します。

IBM KeyWorks Toolkit Service Provider Module Structure & Administration
すべてのツールキットのサービス提供者モジュールに共通のフィーチャーを説明します。この文書は、サービス提供者を構築するために、個別のサービス提供者インターフェースと一緒に使用する必要があります。

IBM KeyWorks Toolkit Cryptographic Service Provider Interface Specification
ツールキットを介してアクセス可能なようにするために、暗号化のためのサービス提供者モジュールが従う必要のあるインターフェースを定義します。

IBM Key Recovery Service Provider Interface (KRSPI) Specification
ツールキットを介してアクセス可能なようにするために、キー回復のためのサービス提供者モジュールが従う必要のあるインターフェースを定義します。

IBM KeyWorks Toolkit Trust Policy Interface Specification
認証局、証明書の発行者、およびポリシーを作成するアプリケーション開発者など、ポリシー作成者が、モデルまたはアプリケーション固有のポリシーにツールキットを展開するために従う必要のあるインターフェースを定義します。

IBM KeyWorks Toolkit Certificate Library Interface (CLI) Specification
多くのツールキット・アプリケーションとトラスト・ポリシー・モジュールに対するフォーマット固有の証明書操作サービスを提供するために、証明書ライブラリーの開発者が従う必要のあるインターフェースを定義します。

IBM KeyWorks Toolkit Data Storage Library Interface (DLI) Specification
フォーマット固有またはフォーマットと独立した持続性のある証明書の保管場所を提供するために、ライブラリーの開発者が従う必要のあるインターフェースを定義します。

IBM Key Recovery Service Provider

以下の文書は、IBM Key Recovery Service Provider と一緒に、PDF 形式で製品 CD に入れて提供されます。

IBM Key Recovery Service Provider Key Recovery Server Installation and Usage Guide　キー回復の概念についての理解、組織のためのキー回復ソリューション

のセットアップのガイダンス、および IBM Key Recovery Server のインストール、構成、操作の手順を提供します。

セキュリティーに関するレッドブック

IBM International Technical Support Organization (ITSO) によって作成された、以下のレッドブックは、セキュリティー関連の製品およびプロセスについて説明しています。これらは、www.us.ibm.com/redbooks で使用可能です。

- *Understanding the IBM SecureWay FirstSecure Framework*
- *High Availability IBM eNetwork Firewall*

文書パック

以下の文書パックが、IBM SecureWay FirstSecure 用として使用可能です。

FirstSecure 文書パック

FirstSecure 文書パックには、以下のブックが含まれています。

- FirstSecure License Information
- *IBM SecureWay FirstSecure 計画および統合の手引き*
- *IBM SecureWay Policy Director 概説*
- *IBM SecureWay Boundary Server for Windows NT and AIX: 概説*
- *IBM SecureWay Trust Authority Up and Running*
- *Tivoli Cross-Site for Security Installation*

Policy Director 文書パック

Policy Director 文書パックには、以下のブックが含まれています。

- Policy Director License Information
- *IBM SecureWay Policy Director 概説*

SecureWay Boundary Server 文書パック

SecureWay Boundary Server 文書パックには、以下のブックが含まれています。

- SecureWay Boundary Server License Information
- *IBM SecureWay Boundary Server for Windows NT and AIX: 概説*

第4部 付録および後付け

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。

商標

次のものは、IBM Corporation の米国およびその他の国における商標です。

AIX
AIX/6000
DB2
DB2 Universal Database
eNetwork
Global Sign-On

GSO
IBM
Netfinity
OS/2
RS/6000
SecureWay
Websphere

Intel および Pentium は、Intel Corporation の米国およびその他の国における登録商標です。

Java、およびすべての Java 関連の商標およびロゴは Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

Lotus、Lotus Notes、Domino、および cc:Mail は、Lotus Development Corporation の米国およびその他の国における商標です。

Microsoft、Windows、Windows NT、および Windows ロゴは Microsoft Corporation の米国およびその他の国における商標です。

Tivoli は Tivoli Systems Inc. の米国およびその他の国における商標です。

UNIX は、X/Open Company Limited がライセンスしている米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標または登録商標です。

用語集

この用語集は、本書で使用されている用語と省略語を定義したものであり、新しい用語または見慣れない用語、および関心のある用語が含まれている場合があります。この用語集には、以下のものからの用語が含まれています。

- IBM Dictionary of Computing, New York: McGraw-Hill, 1994。
- American National Standard Dictionary for Information Systems, ANSI X3.172-1990, American National Standards Institute (ANSI), 1990。
- Answers to Frequently Asked Questions, Version 3.0, California: RSA Data Security, Inc., 1996。

A

アクセス制御 (Access control). コンピューター・セキュリティーでは、コンピューター・システムのリソースを、許可されたユーザーが許可された方法でアクセスできるようにするプロセス。

アクセス制御リスト (access control list). 特定のリソースの使用を許可されたユーザーに限定するためのメカニズム。

ACL. アクセス制御リスト (Access Control List)。

ActiveX. Microsoft のプログラミングでは、オブジェクト指向テクノロジーと用語のセット。

エージェント (agent). Tivoli Cross-Site for Security では、パケットをキャッチし、異なるネットワーク層での異常な点を検査し、確立された接続の状態と統計を追跡する、スマート IP パケット・モニターの 1 つ。

Apache サーバー (Apache server). 1 組の自由に使用できる Web サーバー・ソフトウェア。

API. アプリケーション・プログラミング・インターフェース (Application programming interface)。

アプレット (Applet). Java で書かれたプログラムで、Netscape Navigator など、Java 互換のブラウザー内で実行される。 Java アプレットとも呼ばれる。

アプリケーション・プログラム・インターフェース (application program interface). 高水準言語で書かれたアプリケーション・プログラムが、特定の機能を使用できるようにするための機能的なインターフェース。

監査証跡 (audit trail). 論理経路の形式でのデータで、一連のイベントをリンクする。監査証跡は、特定の活動のトランザクションまたは履歴をトレースするために使用できる。たとえば、顧客アカウントの活動を追跡する。

認証 (authentication). 通信の相手先の識別を確実に判別するためのプロセス。

許可 (Authorization). あるユーザーが、どのタイプの活動の実行を許されているかを判別するプロセス。通常、許可は、認証の後で行われる。

B

Bloodhound. Norton AntiVirus では、ウィルスを追跡する構成要素。

C

セル (cell). DCE では、ユーザー、システム、およびリソースのグループで、通常、共通の目的で中央に集められて、セキュリティー、管理、および命名の境界を共有する。通常、セルは、ユーザー、マシン、およびリソースからなり、共通の目的と、セル外のユーザー、マシン、およびリソースに比べて、より大きな信頼性のレベルを共有している。

セル・ディレクトリー・サービス (Cell directory service). 分散コンピューティング環境 (DCE) の 1 つの構成要素であり、 DCE セル内のリソースに関する情報のデータベースを管理する。

認証局 (certificate authority). 組織のセキュリティー・ポリシーに従い、証明書という形で保護のための電子識別を割り当てる、ソフトウェア・アプリケーションまたは人間のエンティティー。認証局は、証明書の発行、更新、および取り消しの要求を処理する。

チャネル (Channel). シグナルを送ることができるパス。

サーキット・レベル・ゲートウェイ (Circuit-level gateway). ファイアウォールでは、ファイアウォールを介して、クライアントの要求を意図したサーバーに転送するプロキシー・サーバー。

クライアント (Client). (1) サーバーから共有のサービスを受け取る機能単位。 (2) 別のコンピューターまたはプログラムのサービスを要求するコンピューターまたはプログラム。

内容フィルター処理 (Content filtering). 伝送が特定の内容の標準に合っているかどうかを判別するために、内容の読み取りで伝送したものを隠すこと。

D

デーモン (daemon). AIX では、要求をサービスするために、常駐のまま残っているプログラム。

DCE. 分散コンピューティング環境 (Distributed Computing Environment)。

ディジタル証明書 (Digital certificate). 信頼された第三者からある個人またはエンティティーに発行された、電子的な証明書。証明書には、それが証明するエンティティーに関する情報が含まれている。

分散コンピューティング環境 (Distributed Computing Environment). 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およびツール。

E

e-business. ネットワークおよびコンピューターを介して、商取引を運営すること。これには、商品およびサービスの売買が含まれる。また、ディジタル通信を介した資金の転送も含まれる。

e-commerce. ビジネス相互間のトランザクションを運営すること。これには、(顧客、サプライヤー、ベンダーなど) とのインターネット上での商品およびサービスの売買が含まれる。これは e-business の主要な要素である。

暗号化 (encrypt). 情報をごちゃまぜにして、該当する暗号化解除コードを知っている者のみが、暗号化解除を行って元の情報を取得できるようにすること。

エクストラネット (extranet). インターネットから派生したもので、類似のテクノロジーを使用する。企業では、顧客、パートナー、および内部スタッフの複数のコミュニティーに対して、Web で

の公表、エレクトロニック・コマース、メッセージ交換、およびグループウェアの適用を始めている。

F

ファイル転送プロトコル (File Transfer Protocol (FTP)). コンピューター間でのファイルの転送に使用できる、インターネットでのクライアント / サーバーのプロトコルの 1 つ。

ファイアウォール (firewall). 2 つ以上のネットワークの間に強制的に境界を作る、1 つのシステムまたはシステムの組み合わせ。

G

ゲートウェイ (gateway). 互換性のないネットワークまたはアプリケーションが、相互に通信できるようにするためのシステム。

H

ハッカー (hacker). 正当な許可を持たずに、マシンまたはシステムにアクセスを試みる個人。通常、ハッカーは、リソースを許可なく使用する傾向にある。

ハートビート (heartbeat). 活動を確認するための、あるプログラムから管理プログラムへの通信。プログラムは、管理プログラムに対して、まだ活動状態であり、自身のタスクを実行中であることを通知する。

I

IDE. 統合開発環境 (Integrated development environment)。

インプリメンテーション・サービス (Implementation Services). IBM によってサポートされるオンサイト・インストール・サポート。

誤動作 (incident). Tivoli Cross-Site for Security では、システムがハッキングされた可能性のある、疑わしい活動。

統合開発環境 (integrated development environment). アプリケーション開発のためのプログラムの 1 つであり、アプリケーションをコーディングし、それを中断点付きで実行し、プログラム・エラーに対する診断ヘルプを受け取ることができる。

インターネット (Internet). コンピューター間での電子通信を提供する、全世界にまたがるネットワークの集合。電子メールや Web ブラウザーのようなソフトウェア・デバイスを介して、コンピューター相互間の通信を可能にする。たとえば、一部の大学は、他の類似のネットワークと順次リンクしてインターネットを形成する、ネットワーク上に開設されている。

イントラネット (intranet). 企業内のネットワークの 1 つであり、通常はファイアウォールの背後に置かれている。これは、インターネットから派生したもので、類似のテクノロジーを使用している。技術的には、イントラネットは、単にインターネットの延長にすぎない。 HTML (情報のグラフィカル表示に使用される言語) および HTTP (インターネットを通してハイパーテキスト・ファイルを移動するプロトコル) が、その共通要素である。

IntraVerse サーバー (IntraVerse server). IntraVerse において、IntraVerse サーバー・ソフトウェアが含まれており、 NetSEAT クライアント・ソフトウェアで実行されているすべてのホスト・システムと通信することができる、ネットワーク上の 1 つのシステム。 IntraVerse サーバーは、その製品の関連プログラムを実行しているシステムまたはシステムの組み合わせを指す。

IPSec. IETF によって開発された、インターネット・プロトコル・セキュリティー規格。 IPSec は、認証、保全性、アクセス制御、および機密性の組み合わせを柔軟にサポートする、暗号セキュ

リティー・サービスを提供するために設計された、ネットワーク層プロトコルである。その強力な認証機能のために、多くの VPN ベンダーによって、インターネットを介した保護 2 地点間接続を確立するためのプロトコルとして採用されている。

ISV. Independent Software Vendor。

J

Java. Sun Microsystems, Incorporated によって開発された、ネットワークを意識した、特定のプラットフォームに依存しないコンピューター・テクノロジーのセット。 Java 環境は、Java OS、さまざまなプラットフォーム用の仮想計算機、オブジェクト指向の Java プログラム言語、およびいくつかのクラス・ライブラリーからなる。

JavaScript. Java に類似したスクリプト言語であり、Netscape ブラウザーで使用するために Netscape によって開発された。

K

ケルベロス (Kerberos). コンピューターを要求しているサービスを認証するためのセキュア方式の 1 つ。ケルベロスは、マサチューセッツ工科大学 (MIT) の Athena プロジェクトで開発された。ギリシャ神話のケルベロスは、ハデスの門を守る 3 つの頭を持った犬である。ケルベロスにより、ユーザーは認証プロセスからの暗号化されたチケットを要求できるが、そのチケットは、サーバーからの特定のサービスを要求するために使用できる。ユーザーのパスワードを、ネットワークを通して渡す必要はない。

L

LDAP. Lightweight Directory Access Protocol。

Lightweight Directory Access Protocol. IBM SecureWay Directory において、LDAP は、保管、更新、検索、および交換のために中央設置場所でディレクトリー情報を維持管理する方法を提供する。

M

マクロ爆弾 (macro bomb). 他のユーザーに送信され、保管されたコマンドのシーケンスであり、望ましくない結果をもたらす。

MPEG. 動画およびアニメーションをディジタル形式で圧縮して保管するための、Moving Pictures Experts Group によって開発中の規格。

モバイル・コード (mobile code). 頻繁にさまざまな場所に移動して、異なるタイプのネットワーク接続 (たとえば、ダイヤル呼び出し、LAN、または無線) をするユーザーによって、携帯用コンピューターで実行される計算のこと。

N

ネームスペース (namespace). ディレクトリーに関連して、ユーザーがアクセス可能な名前の外部構造。

ネットワーク・アドレス・フィルター処理 (network address filtering). 受信者または送信者が受け入れ可能かどうかを検査するために、着信または発信する電子メールのアドレスを検査するプロセス。

拒否回避 (non-repudiation). 文書の署名者が、署名するのを誤って拒否してしまうのを防止するための、ディジタル秘密キーの使用法。

O

オブジェクト要求ブローカー (object request broker). オブジェクト指向プログラミングにおいて、透過的にオブジェクトが要求と応答を交換できるようにすることにより、仲介として働くソフトウェア。

OEM. 相手先商標製造会社 (Original equipment manufacturer)。

P

プラグイン (plug-in). Web ブラウザーの一部として使用できるプログラム。

プリンシパル (principal). DCE において、DCE セキュリティーを介して別のエンティティーと安全に通信できるエンティティー。プリンシパルには、ユーザー、サーバー、またはコンピューターがなり得る。

プロキシー・サーバー (proxy server). アクセスを要求するコンピューター (A) とアクセスされるコンピューター (B) の仲介となるもの。これによって、あるエンド・ユーザーがコンピューター A からのリソースを要求すると、この要求は、プロキシー・サーバーに送られる。プロキシー・サーバーは、要求を行い、コンピューター B からの応答を受け取って、その応答をエンド・ユーザーに転送する。プロキシー・サーバーは、ファイアウォールの内部からワールド・ワイド・ウェブ (WWW) のリソースをアクセスするのに便利である。

公開キー (public key). 公開キー / 秘密キーのペアの中のキーで、他の人に使用させるキー。これによって他の人は、トランザクションをキーの所有者に送るか、またはディジタル署名を検査できるようになる。公開キーを使用して暗号化されたデータは、対応する秘密キーでのみ暗号化解除することができる。公開キー / 秘密キーのペア (public/private key pair) も*参照*。

公開キー / 秘密キーのペア (public/private key pair). 公開キー / 秘密キーのペアは、キー・ペア暗号 (キー管理の問題を解決するために Diffie and Hellman によって 1976 年に紹介されたもの) の概念の一部である。この概念では、それぞれの人がキーのペアを入手するが、その 1 つを公開キーと呼び、もう 1 つを秘密キーと呼ぶ。秘密キーは秘密性が保持されるが、それぞれの人の公開キーは公表される。送信者と受信者は秘密情報を共用する必要はなく、すべての通信に公開キーだけが含まれ、秘密キーは、伝送も共用もされない。これによって、一部の通信チャネルが、盗聴または漏えいに対する保護について信頼性のあるものである必要がなくなる。この方式の唯一の要件は、公開キーが信頼性のある (許可された) 方法で (たとえば信頼性のあるディレクトリーに入れて) ユーザーと関連付けられることである。公開された情報を使用すれば、だれでも機密メッセージを送信することができる。しかし、このメッセージは、秘密キー (これは意図した受信者が所有している) を使用してしか暗号化解除することができない。さらに、キー・ペアによる暗号は、プライバシー (暗号化) のためだけでなく、認証 (ディジタル署名) のためにも使用することができる。

R

リモート・プロシージャー呼び出し (remote procedure call). (1) クライアントが、サーバーからプロシージャー呼び出しの実行を要求するために使用する機能。この機能には、ライブラリー・プロシージャーと外部データ表示が含まれる。 (2) 別のノードにあるサービス提供者に対するクライアント要求。

RPC. DCE では、リモート・プロシージャー呼び出し

S

セキュア・ソケット・レイヤー (Secure Sockets Layer (SSL)). (1) 可能なかぎりエンド・ユーザーが意識しなくても済むように透過性を持たせた、組み込みセキュリティー・サービスを備えた IETF の標準通信プロトコルの 1 つ。ディジタルによるセキュア通信チャネルを提供する。 (2) SSL 可能サーバーは、通常、標準の HTTP 要求とは異なるポートで SSL 接続要求を受け入れる。 SSL は、その間にハンドシェークが 1 度だけしか必要としないセッションを作成

する。ハンドシェークが完了すると、通信が暗号化される。 SSL セッションが満了するまでメッセージの整合性検査が行われる。

SecurID トークン (SecurID token). Security Dynamics の ACE/Server 認証方式には、ユーザー ID と SecurID トークンが含まれている。リモートでログインすると、SecurID トークンからパスワードを受け取る。パスワードは 60 秒ごとに変更され、1 回だけの使用には便利である。開放されたネットワーク上でだれかがパスワードを傍受したとしても、そのパスワードは、その他の使用には無効になる。

サーバー (server). (1) ネットワークにおいて、他のステーションに対して機能を提供するデータ・ステーションであり、たとえば、ファイル・サーバーがある。 (2) TCP/IP では、別のサイトにある、クライアント / サーバーと呼ばれるシステムの要求を扱う、ネットワーク内のシステム。

SOCKS プロトコル (SOCKS protocol). セキュア・ネットワーク内のアプリケーションが、socks サーバーを介して、ファイアウォールを通した通信を可能にするためのプロトコル。

socks サーバー (socks server). 保護されていないネットワーク内のアプリケーションに対して、ファイアウォールを介して、保護された 1 方向接続を提供するサーキット・レベル・ゲートウェイ。

spam. 要求しないのに送り付けられる迷惑な電子メールで、多数の宛先に送られることがある。

T

TCP/IP. 伝送制御プロトコル / インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)。

telnet. インターネット用のプロトコルの組の中で、リモート端末接続サービスを提供するプロトコル。これにより、ユーザーは、あるホストからリモート・ホストにログオンして、そのホストに直接接続されている端末のユーザーと対話することができる。

伝送制御プロトコル / インターネット・プロトコル (Transmission Control Protocol/Internet Protocol). ローカルおよび広域ネットワークに対する対等通信接続機能をサポートする、 1 組の通信プロトコル。

U

Universal Resource Locator (URL). ワールド・ワイド・ウェブ (WWW) で使用される命名規則であり、そこでは、Web オブジェクトは、たとえば、
http://www.ibm.com/software/security/firstsecure のように、サービス名、組織名、パス、およびファイル名で始まる。

URL. Universal Resource Locator。

V

ボールト (vault). ボールトは、暗号化を使用して、システム管理者や他のボールトの所有者など、無許可の人に開示されないように情報を保護する。また、ボールトは、ディジタル署名を使用してデータの悪用を保護し、ディジタル認証を使用して未知の相手との通信を保護する。また、暗号化、署名、および認証を使用して、情報を安全に他のボールトに伝送する。

仮想私設網 (virtual private network). リモート接続を確立するために、電話回線ではなく、インターネットを使用する私用のデータ・ネットワーク。ユーザーは、電話会社ではなく、インターネット・サービス・プロバイダー (ISP) を通して企業のネットワーク・リソースにアクセスするので、企業の組織では、リモート・アクセスのコストを大幅に削減することができる。 VPN はまた、データ交換のセキュリティーを強化する。伝統的なファイアウォール・テクノロジーでは、メ

ッセージの内容を暗号化できるが、発信元と宛先のアドレスは暗号化できない。 VPN テクノロジーでは、ユーザーは、トンネル接続を確立することができ、その中では、情報パケット全体 (内容とヘッダー) が暗号化され、カプセル化される。

VPN. 仮想私設網 (Virtual Private Network)。

W

Web アプリケーション (Web application). ワールド・ワイド・ウェブ (WWW) を通してアクセスするよう設計されたアプリケーション。

Web ブラウザー (Web browser). デスクトップ PC で実行されるクライアント・ソフトウェアであり、ワールド・ワイド・ウェブ (WWW) またはローカルのページをブラウズすることができる。これは、Web およびインターネット内で使用可能な大量のハイパーメディアの素材に対するユニバーサル・アクセスを提供する、検索ツールである。例として、Netscape Navigator および Microsoft Internet Explorer がある。サーバー (server) も*参照*。

Web オブジェクト (Web object). Web ブラウザーを介して使用可能なデータ。 Web オブジェクトには、Web ページ、Web ページの一部、ファイル、イメージ、ディレクトリー、CGI プログラム、または Java アプレットがある。

Web サーバー (Web server). ブラウザー・プログラムからの情報リソースの要求に応答するサーバー・プログラム。

ウィザード (wizard). 特定のタスクについてユーザーをガイドするために、ステップバイステップの指示を使用する、アプリケーション内のダイアログ。

ワーム (worm). 害を与える可能性のあるコンピューター・ウィルス。

X

X.509. セキュア管理と、セキュア・インターネット・ネットワークに渡ってディジタル署名された PKI 証明書を配布するのをサポートするために設計された、広く受け入れられている証明書規格の 1 つ。 X.509 証明書では、信頼性のある第三者によってディジタル署名された公開キーの配布に関連するプロシージャーを提供するデータ構造を定義する。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

［マ行］

［ヤ行］

［ラ行］

［ワ行］

A

B

D

E

F

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X

部品番号: CT7EHJA

Printed in Japan

CT7EHJA

SB88-8502-00

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