

IBM

@server

iSeries

iSeries とインターネット・セキュリティー

バージョン 5 リリース 3





@server

iSeries

iSeries とインターネット・セキュリティー

バージョン 5 リリース 3

ご注意

本書および本書で紹介する製品をご使用になる前に、45 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM OS/400 (製品番号 5722-SS1) のバージョン 5、リリース 3、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、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適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

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

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.ibm.com/jp/manuals/> の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

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

原 典： iSeries
iSeries and Internet security
Version 5 Release 3

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 2005.8

この文書では、平成明朝体™W3、平成明朝体™W7、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™W7、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

© Copyright International Business Machines Corporation 1999, 2005. All rights reserved.

© Copyright IBM Japan 2005

目次

第 1 部 iSeries とインターネット・セキュリティ	1
第 1 章 トピックの印刷	3
第 2 章 iSeries とインターネット・セキュリティ上の考慮事項	5
第 3 章 インターネット・セキュリティの計画	7
セキュリティ対策の階層的アプローチ	7
セキュリティ・ポリシーと目的	9
シナリオ: JKL Toy Company の e-business 計画	11
第 4 章 インターネットの基本準備としてのセキュリティのレベル	15
第 5 章 ネットワーク・セキュリティ・オプション	17
ファイアウォール	18
iSeries パケット・ルール	20
iSeries ネットワーク・セキュリティ・オプションの選択	21

第 6 章 アプリケーション・セキュリティ・オプション	23
Web サーバーにおけるセキュリティ	23
Java インターネット・セキュリティ	24
電子メール・セキュリティ	27
FTP セキュリティ	28
第 7 章 伝送セキュリティ・オプション 31	
SSL のためのデジタル証明書の使用	32
Telnet のセキュア・アクセスのための SSL	33
セキュア iSeries Access Express のための SSL	33
セキュア専用通信のための VPN (仮想プライベート・ネットワーク)	34
第 8 章 インターネット・セキュリティ用語	37
第 2 部 付録	43
付録. 特記事項.	45
商標	46
資料に関するご使用条件	46

第 1 部 iSeries とインターネット・セキュリティ

LAN からインターネットへアクセスすることは、ネットワークの発展における重要なステップであり、セキュリティ要件の再検討が必要になります。幸いにも、iSeries™ サーバーには、統合ソフトウェア・ソリューションとセキュリティ・アーキテクチャーが組み込まれており、潜在的なインターネット・セキュリティの抜け穴と侵入者に対する強力な防護機能を構築することが可能です。iSeries のセキュリティ・オファリングを適切に使用することで、顧客、従業員、およびビジネス・パートナーは、ビジネスを行うために必要な情報をセキュリティ機能のある環境で手に入れることができます。

この資料をご覧になれば、すでに分かっているセキュリティの脅威について、またそのリスクが自分のインターネットおよび e-business の目標とどうかかわるかについて知ることができます。また、リスクと、iSeries の提供するそれらのリスクに対処するためのさまざまなセキュリティ・オプションを使用することの利点とを比較検討する方法も学習します。そして、自分のビジネスの必要性に合うネットワーク・セキュリティ計画を開発するためには、ここでの情報をどう使用すればよいのかが分かるようになるでしょう。

インターネット・セキュリティのリスクと、システムとリソースを保護するために使用できる iSeries セキュリティ・ソリューションの詳細については、以下の情報を検討してください。

- **トピックの印刷**

このトピックの Adobe Acrobat 版をアクセスおよび印刷するには、この情報を参照してください。

- **iSeries とインターネット・セキュリティ上の考慮事項**

e-business における iSeries セキュリティの強みと使用可能な iSeries セキュリティ・オファリングに関する一般的な知識については、この情報を参照してください。

- **インターネット・セキュリティの計画**

インターネットと e-business のセキュリティ要件をカバーするセキュリティ・ポリシーの作成方法については、この情報を参照してください。

- **インターネットの基本準備としての iSeries システム・セキュリティのレベル**

インターネットに接続する前に準備するシステム・セキュリティについては、この情報を参照してください。

- **ネットワーク・セキュリティ・オプション**

内部リソースを保護するために使用を考慮すべきネットワーク・レベルのセキュリティ措置については、この情報を参照してください。

- **アプリケーション・セキュリティ・オプション**

各種の一般的なインターネット・アプリケーションおよびサービスに関する共通のインターネット・セキュリティ・リスクと、そのリスクを管理するための措置については、この情報を参照してください。

- **伝送セキュリティ・オプション**

インターネットなど、非トラステッド・ネットワーク上で送信されるデータを保護するために使用可能なセキュリティ措置については、この情報を参照してください。Secure Sockets Layer (SSL)、iSeries Access Express、および VPN (仮想プライベート・ネットワーク) 接続を使用するセキュリティ措置について、さらに詳しく説明されています。

- **iSeries インターネット・セキュリティ・オプション**

インターネットの使用法と e-business の計画に基づいてシステムとリソースを保護するオファリングを選択する際に、ここでの iSeries セキュリティ・オプションについての簡潔なディスカッションを役立ててください。

注: セキュリティーおよびインターネット関連の用語で疑問が生じた場合は、必要に応じて一般的なセキュリティー用語の説明を参照してください。

第 1 章 トピックの印刷

この文書の PDF 版を参照用または印刷用にダウンロードし、表示することができます。PDF ファイルを表示したり印刷したりするには、Adobe(R) Acrobat(R) Reader が必要です。これは、Adobe Web サイト



から、ダウンロードできます。

PDF 版をダウンロードし、表示するには、『iSeries とインターネット・セキュリティー』(約 582 KB、56 ページ) を選択します。

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. ブラウザーのメニューから「ファイル」をクリックする。
3. 「名前を付けて保存」をクリックする。
4. PDF を保存したいディレクトリーに進む。
5. 「保存」をクリックする。

第 2 章 iSeries とインターネット・セキュリティー上の考慮事項

システムをインターネットへ接続するためのオプションを模索する iSeries 所有者から頻繁に出される最初の質問は、「インターネットをビジネス目的でどのように使用すればよいのでしょうか」というものです。2 番目の質問は、「セキュリティーとインターネットについてどのようなことを知っておかなければならないのでしょうか」というものです。この資料の主題は、この 2 番目の質問への解答を見付けられるようにすることにあります。


「セキュリティーとインターネットについて知っておくべきことは何でしょうか」という質問に対する答えは、インターネットをどのように利用したいのかによって異なります。インターネットに関連するセキュリティー問題は重要です。取り組まなければならない課題は、インターネットをどう利用するつもりなのかによって異なってきます。インターネットに乗り出す最初の試みは、内部ネットワークのユーザーに Web とインターネット電子メールへのアクセスを許可することです。また、あるサイトから別のサイトに機密性の高い情報を転送する機能も必要かもしれません。当然、インターネットを e-commerce に使用する計画を立てたり、自社とビジネス・パートナーやサービス提供元との間でエクストラネットを構築したりすることもありうるでしょう。

インターネットにどっぷりとつかる前に、何をしたいのか、どのように実行したいのか、について考えておかなければなりません。インターネットの利用とインターネットのセキュリティーに関して決定を下すのは、複雑な作業です。『シナリオ: JKL Toy Company の e-business 計画』のページを検討すれば、インターネットの使用法に関し独自の計画を策定するのに役立つでしょう。(注: セキュリティーおよびインターネット関連の用語で疑問が生じた場合は、必要に応じて一般的なセキュリティー用語を参照してください。)

e-business に関してインターネットをどのように使用したいのか、セキュリティー問題と利用可能なセキュリティー・ツール、機能、オフリングについて理解した上で、セキュリティー・ポリシーと目的を明らかにすることができます。セキュリティー・ポリシーの開発過程で行う選択には、多くの要因が影響します。組織をインターネットにまで拡張するとき、セキュリティー・ポリシーは、システムとリソースを保護するための重要な礎石になります。

iSeries サーバー・システム・セキュリティーの特性

インターネット上でシステムを保護するための各種の特別なセキュリティー・オフリングのほか、iSeries サーバーは、以下のような非常に強力なシステム・セキュリティー特性を持っています。

- 他のシステムに追加導入されたセキュリティー・ソフトウェア・パッケージと比較して、抜け道を見つけることがきわめて困難な統合化セキュリティー。
- ウィルスの作成と伝搬が技術的に困難となるオブジェクト・ベースのアーキテクチャー。iSeries サーバーでは、ファイルをプログラムであるかのように見せかけたり、プログラムから別のプログラムを変更することはできません。iSeries の統合機能では、オブジェクトにアクセスするには、システム提供のインターフェースを使用する必要があります。システム内でオブジェクトのアドレスを直接使用してそれにアクセスすることはできません。オフセットを取り、それをポインターにしたり、ポインターを「製造する」ことはできません。他のシステム・アーキテクチャーの場合、ポインター操作はハッカーがよく使用する技法です。
- 特定の要件を満たすようなシステム・セキュリティーをセットアップ可能にする柔軟性。  **eServer Security Planner** は、ニーズに応じたセキュリティーの推奨事項を判別するのに役立ちます。

iSeries 拡張セキュリティー・オファリング

iSeries は、インターネット接続時のシステム・セキュリティーを強化するために、特定のセキュリティー・オファリングをいくつか提供しています。インターネットの利用方法によりませんが、以下の諸機能を利用することができます。

- VPN (仮想プライベート・ネットワーク) とは、企業の専用イントラネットを、インターネットのような公衆ネットワークに拡張したものです。VPN を使用すると、基本的には私用の「トンネル」を公衆ネットワーク上に作成することで、安全な私用接続を確立することができます。VPN は、iSeries ナビゲーター・インターフェースから利用可能な OS/400[®] の統合機能です。
- パケット・ルールは、iSeries ナビゲーターから利用可能な、OS/400 の統合機能です。この機能により、IP パケット・フィルターとネットワーク・アドレス変換 (NAT) 規則を構成して、iSeries サーバーに出入りする TCP/IP のトラフィックの流れを制御することができます。
- Secure Sockets Layer (SSL) のアプリケーション通信セキュリティーでは、SSL を使用してサーバー・アプリケーションとそのクライアントとの間で安全な接続を確立するようにアプリケーションを構成することができます。SSL は本来、安全な Web ブラウザーとサーバー・アプリケーションのために開発されたものですが、他のアプリケーションでも使用することができます。IBM[®] HTTP Server for iSeries、iSeries Access Express、ファイル転送プロトコル (FTP)、および Telnet など、現在では多くの iSeries サーバー・アプリケーションで SSL が利用可能です。

インターネットをどのように使用したいのか、セキュリティー問題と利用可能なセキュリティー・ツール、機能、オファリングについて理解した上で、セキュリティー・ポリシーと目的を明らかにする準備が整ったこととなります。セキュリティー・ポリシーの開発過程で行う選択には、多くの要因が影響します。組織をインターネットにまで拡張するとき、セキュリティー・ポリシーは、システム保護を行うための重要な礎石となります。

注: ビジネス目的でインターネットを始める方法の詳細は、以下のオンラインによる Information Center トピック、および IBM レッドブックを参照してください。

- インターネット接続
- AS/400[®] Internet Security: Protecting Your AS/400 from HARM on the Internet (SG24-4929)

第 3 章 インターネット・セキュリティの計画

インターネット使用計画を作成するときは、インターネット・セキュリティのニーズを注意深く計画しなければなりません。インターネット使用計画に関する詳細な情報を収集し、内部ネットワーク構成を文書化しなければなりません。この情報収集の結果に基づいて、セキュリティのニーズを正確に評価することができます。

たとえば、以下のような項目を文書化および記述してください。

- 現在のネットワーク構成。
- DNS および電子メールのサーバー構成情報。
- インターネット・サービス・プロバイダー (ISP) への接続。
- インターネットで利用したいサービス内容。
- インターネット・ユーザーに提供したいサービス内容。

セキュリティがリスクにさらされる場所、およびこれらのセキュリティ・リスクを最小限に抑えるのに必要なセキュリティ措置を決定するのに、この種の情報を文書化することが役立ちます。

たとえば、特殊な研究所にあるホストに Telnet を使用してアクセスすることを内部ユーザーに許可とします。内部ユーザーは、会社の新製品開発に役立つこのサービスが必要です。ただし、インターネットを流れる無保護の機密データが気になるところです。もし競合他社がこのデータを入手して、それを利用しようとしたなら、自分の会社は財政危機に見舞われることにもなりかねません。使用目的 (Telnet) とそれに伴うリスク (機密情報の露出) が確認できたならば、この用途でのデータ機密性を得るために、他に講じるべきセキュリティ措置を決定します (Secure Sockets Layer (SSL) の使用可能性)。

インターネット使用計画とセキュリティ計画を作成するときは、以下のトピックを検討すると有効です。

- 『**セキュリティ対策の階層的アプローチ**』では、包括的なセキュリティ計画を作成するときに伴う問題に関して情報を示しています。
- 『**セキュリティ・ポリシーと目的**』では、包括的なセキュリティ計画を作成するときに伴う問題の理解に役立つ情報を示しています。
- **シナリオ: JKL Toy Company の e-business 計画**では、参考にすることができる、典型的な会社におけるインターネット使用法とセキュリティ計画について、現実的なモデルを示しています。

セキュリティ対策の階層的アプローチ

セキュリティ・ポリシーでは、保護したいものと、システム・ユーザーに期待するものを定義しています。セキュリティ・ポリシーは、新規アプリケーションを設計したり、現行のネットワークを拡張する場合に、セキュリティ計画の基盤を提供します。セキュリティ・ポリシーには、機密情報の保護や重要なパスワードの作成など、ユーザーが行わなければならない作業が記述されます。

注: 内部ネットワークへのリスクを最小限にするためのセキュリティ・ポリシーを組織のために作成し、実施しなければなりません。iSeries 400 固有のセキュリティ機能を適切に構成すれば、多くのリスクを最小限に抑えることができます。ただし、iSeries をインターネットに接続する場合は、内部ネットワークの安全性を保証するためのセキュリティ措置をさらに講じる必要があります。

ビジネス活動を推進するためにインターネット・アクセスを使用すると、多くのリスクが伴います。セキュリティ・ポリシーを作成する場合は常に、サービスの提供と、機能やデータへのアクセス制御との間でバ

ランスをとらなければなりません。ネットワーク化されたコンピューターでは、セキュリティはより難しくなります。通信チャンネル自体がアタックにさらされるからです。

どのような種類のアタックに対して弱点があるかは、インターネット・サービスによって異なります。したがって、使用あるいは提供しようと考えているサービスごとに、それによって生じるリスクを理解しておくことが重要になります。さらに、潜在的なセキュリティ・リスクを理解しておけば、セキュリティの目的も明確に決定できます。

インターネットは、インターネット通信のセキュリティに脅威を与えるさまざまな人たちの根城になります。以下のリストは、遭遇する可能性のある典型的なセキュリティ・リスクをいくつか解説したものです。

- **受動的なアタック:** 受動的なアタックでは、アタッカーは機密事項を知ろうとして、単にネットワークのトラフィックを監視するだけです。そのようなアタックは、ネットワーク・ベース (通信リンクをトレースする) か、システム・ベース (こっそりとデータを奪ってしまうトロイの木馬プログラムで、システム・コンポーネントを置き換える) のいずれかです。受動的なアタックは、最も検出しにくいものです。したがって、インターネットでは、送信内容はすべて盗聴されうると考えておかなければなりません。
- **能動的なアタック:** 能動的なアタックでは、アタッカーは防御の突破とネットワーク・システム内への侵入を試みます。能動的なアタックには、以下のようないくつかの種類があります。
 - **システム・アクセス試行**では、アタッカーはセキュリティの抜け穴を探し、クライアントまたはサーバーのシステムへのアクセスを得て、それを制御します。
 - **スプーフィング・アタック**では、アタッカーが信頼のおけるシステムになりすまして防御を突破したり、ユーザーが自分に機密情報を送信するよう促したりします。
 - **サービス妨害攻撃**では、アタッカーは、トラフィックの宛先変更を行ったり、ジャンク・データをシステムに送信し続けたりして、オペレーションに干渉したり、シャットダウンさせようとします。
 - **暗号アタック**では、アタッカーは、パスワードを推測したり、それを盗もうとします。または、特殊なツールを暗号化されたデータの暗号を解除しようとします。

多重階層による防御

インターネット上の潜在的なセキュリティ・リスクはさまざまなレベルで発生しうるため、これらのリスクに対しては多重階層による防御が可能なセキュリティ措置を講じる必要があります。通常、インターネットに接続するときは、侵入行為やサービス妨害攻撃が発生しても、珍しいことではありません。むしろ、セキュリティ問題は発生して当然、と考えるべきです。したがって、最良の防御とは、十分に計画され、事前の対策を講じた先制攻撃を仕掛けることにはかなりません。インターネット・セキュリティの戦略を立てるときに階層的なアプローチを使用すれば、アタッカーがある層を突破しても、その次の層で阻止されることが保証されます。

セキュリティ戦略では、以下に示す従来のネットワーク・コンピューティング・モデルの各層にわたって保護が可能な措置を講じる必要があります。一般に、最も基本的な層 (システム・レベル・セキュリティ) から、最も複雑な層 (トランザクション・レベル・セキュリティ) までの計画を立てます。

システム・レベル・セキュリティ

システム・セキュリティの措置は、インターネット関連のセキュリティ問題に対する最終防御ラインを表します。したがって、インターネット・セキュリティ戦略全般における第一歩は、iSeries 基本システム・セキュリティ設定を適切に構成することになります。

ネットワーク・レベル・セキュリティ

ネットワーク・セキュリティの措置は、iSeries および他のネットワーク・システムへの

アクセスを制御します。ネットワークをインターネットへ接続するときは、適切なネットワーク・レベル・セキュリティの措置を講じて、無許可アクセスや侵入者から内部のネットワーク・リソースを保護することが必要です。ファイアウォールは、ネットワーク・セキュリティを可能にする最も代表的な手段です。インターネット・サービス・プロバイダー (ISP) は、ネットワーク・セキュリティ計画において重要な役割を果たすことが可能であり、また義務でもあります。ネットワーク・セキュリティ計画では、ISP ルーター接続やパブリック DNS 対策に関する規則のふり分けなど、ISP が提供するセキュリティ措置の内容について概要を示すことが必要です。

アプリケーション・レベル・セキュリティ

アプリケーション・レベル・セキュリティの措置では、ユーザーが特定のアプリケーションとどのように対話するかを制御します。一般に、使用するアプリケーションごとに、セキュリティ設定を構成することが必要です。一方、インターネットから使用したり、インターネットに提供するアプリケーションやサービスについては、セキュリティのセットアップに特別な配慮をしてください。このようなアプリケーションやサービスは、ネットワーク・システムへアクセスする方法を模索している無許可ユーザーによって、不正に使用される危険があります。使用するセキュリティの措置では、サーバー側とクライアント側の両方における機密漏れをカバーしている必要があります。

伝送レベル・セキュリティ

伝送レベル・セキュリティの措置は、ネットワークの内部や相互間でのデータ通信を保護します。インターネットなど、非トラステッド・ネットワークで通信をするときは、出発地点から目的地点までのトラフィックの流れを制御することができません。トラフィックとそれが運ぶデータは、送信元では制御不能な多数の異なるサーバー間を伝達されていきます。アプリケーションが Secure Sockets Layer (SSL) を使用するよう構成するなどセキュリティ措置を講じない限り、経路指定されたデータは第三者に見られたり、使用されたりする危険があります。伝送レベル・セキュリティの措置によって、他のセキュリティ・レベルの境界間を伝達されるデータを保護します。

インターネット全般のセキュリティ・ポリシーを明らかにする場合には、各層について個別にセキュリティ戦略を立ててください。さらに、各戦略が他の戦略との間でどのように相互作用するかも記述して、ビジネスのための包括的セキュリティ・セーフティー・ネットを構築します。

セキュリティ・ポリシーと目的

セキュリティ・ポリシー

使用または提供する各インターネット・サービスは、iSeries システムとそれが接続されているネットワークにリスクを課します。セキュリティ・ポリシーとは、組織に所属するコンピューターおよび通信リソースに対する操作に適用される規則の集まりです。これらの規則は、物理的セキュリティ、人的セキュリティ、管理セキュリティ、およびネットワーク・セキュリティなどの領域にわたります。

セキュリティ・ポリシーでは、保護したいものと、システム・ユーザーに期待するものを定義しています。セキュリティ・ポリシーは、新規アプリケーションを設計したり、現行のネットワークを拡張する場合に、セキュリティ計画の基盤を提供します。セキュリティ・ポリシーには、機密情報の保護や重要なパスワードの作成など、ユーザーが行わなければならない作業が記述されます。セキュリティ・ポリシーには、セキュリティ措置の効果をモニターする方法も記述しなければなりません。このようなモニターは、安全防護柵をすり抜けようとする人物がいるかどうかを判別するのに役立ちます。

セキュリティ・ポリシーを開発するには、セキュリティの目的を明確に定義しなければなりません。セキュリティ・ポリシーを立てたならば、そこに含まれる規則を実行に移すためのステップを取らなければ

なりません。これらのステップでは、規則を施行するために、従業員の訓練、必要なソフトウェアおよびハードウェアの追加が行われます。また、コンピューター環境を変更する場合は、セキュリティ・ポリシーを更新しておかなければなりません。これは、変更によって生じる新しいリスクに対処することが目的です。iSeries Information Center のトピック「基本システム・セキュリティおよび計画」で JKL Toy Company のセキュリティ・ポリシーの例を参照することができます。

セキュリティの目的

セキュリティ・ポリシーを作成および実行するには、目的を明確にしておかなければなりません。セキュリティの目的は、以下に示すカテゴリーの 1 つ以上に分類されます。

リソース保護 (Resource protection)

リソース保護により、許可ユーザーしかシステムのオブジェクトにアクセスできないようにします。あらゆる種類のシステム・リソースを保護できるということが、iSeries の長所の 1 つです。システムにアクセス可能なユーザーのさまざまなカテゴリーを注意深く定義する必要があります。また、セキュリティ・ポリシー作成の一環として、これらのグループのユーザーにどのようなアクセス権を与えるかを定義しなければなりません。

認証 (Authentication)

セッションの相手のリソース (人またはマシン) が、実際に当の本人またはマシンであることを確認または検査すること。堅固な認証により、偽名を使用してシステムを使用するというセキュリティ・リスクから保護してくれます。このように偽名を使う場合、送信者または受信者は、偽の ID を使用してシステムにアクセスします。従来、システムでは認証にパスワードとユーザー名を使用してきました。デジタル証明書では、さらに安全な認証方法を使用することができると同時に、他にもセキュリティ上の利点があります。インターネットのような公衆ネットワークにシステムをリンクする場合は、ユーザー認証が新しい次元を引き受けます。イントラネットがインターネットと異なる重要な点は、サインオンするユーザーの身元を信用できることです。したがって、従来のユーザー名とパスワードによるログオン手続きによる認証よりも、さらに強力な認証方法の採用を真剣に考えなければなりません。認証されたユーザーは、その許可レベルに基づいて、さまざまな種類の権限が認められます。

許可 (Authorization)

セッションの相手の人またはコンピューターが、要求を実行する許可を持っていることを確認すること。許可は、システム・リソースへのアクセス権を持つ、またはシステムにおける操作を実行できる人またはものを決定するプロセスです。通常、許可は、認証のコンテキスト内で実行されます。

健全性 (Integrity)

着信情報とその送信情報と同一であることを確認すること。健全性を理解するには、データの健全性とシステムの健全性の概念を理解しておかなければなりません。

- **データ健全性:** データが未認証の変更または損傷から保護されていることです。データ健全性により、許可されていない者が情報を代行受信したり変更するというセキュリティ・リスクから保護されます。ネットワーク内に保管されているデータの保護の他に、信頼性に欠けるソースのデータがシステムに進入してきた場合に、データ健全性を保証するセキュリティがさらに必要になることもあります。システムに入ってくるデータが公衆ネットワークからのものである場合は、以下のようなことを可能にするためのセキュリティ方式が必要になることがあります。
 - データが「監視」されたり解釈されたりするのを防ぎます。通常、これには暗号化を伴います。

- 伝送が変更されていないことを保証します (データ保全性)。
- 伝送が行われたことを証明します (非拒否)。将来は、登録済みまたは証明済みメールの電子的な等価物が必要になるかもしれません。
- **システム保全性:** 予期されるパフォーマンスで、システムが一貫性のある、予期される結果を生み出すことです。iSeries の場合、システムの保全性は、最も見落とされがちなセキュリティ要素です。それは、システムの保全性が、iSeries アーキテクチャーの基本的な部分だからです。たとえば、セキュリティ・レベルを 40 または 50 にしていると、iSeries アーキテクチャーは、アタッカーにとって、オペレーティング・システムのプログラムをまねたり、変更するのがきわめて難しくなります。

非拒否 (Non-repudiation)

非拒否は、トランザクションが発生したこと、あるいはメッセージを送信または受信したことを証明するものです。トランザクション、メッセージ、およびドキュメントに「署名」するためのデジタル証明書と公開鍵暗号では、非拒否をサポートしています。送信側および受信側の両者が、交換が行われたことに同意します。データ上のデジタル署名が、必要な証明を提供します。

機密性 (Confidentiality)

機密情報がプライベートのまま、盗聴者からは守られていることを確認すること。機密性は総合的なデータ・セキュリティにとって重要です。デジタル証明書と Secure Sockets Layer (SSL) によるデータの暗号化は、非トラステッド・ネットワークでデータを転送する場合に、機密性を確実なものにするのに役立ちます。セキュリティ・ポリシーでは、ネットワーク内の情報と、ネットワークから出て行く場合の情報に対してどのように機密性を提供するかについて言及していなければなりません。

セキュリティ活動の監査 (Auditing security activities)

セキュリティ関連のイベントをモニターして、成功アクセスも不成功 (拒否) アクセスも記録します。成功アクセス・レコードは、システムで誰が何を行っているかを示します。不成功 (拒否) アクセス・レコードは、セキュリティを破ろうとしたか、あるいはシステムへのアクセスに悪戦苦闘しているものがあることを知らせます。

セキュリティの目的を理解しておくことは、ネットワーク・セキュリティのニーズと、インターネット・セキュリティのニーズをすべて盛り込んだセキュリティ・ポリシーを作成するのに役に立ちます。JKL Toy Company の e-business のシナリオを検討すれば、目的を定義し、セキュリティ・ポリシーを作成するのに役に立ちます。シナリオに登場する会社のインターネット使用法とセキュリティ計画は、実社会における数多くの実装の代表例です。

シナリオ: JKL Toy Company の e-business 計画

このシナリオでは、典型的なビジネスの例として、JKL Toy Company を取り上げます。同社では、インターネットを使用したビジネス対象の拡張を計画しています。この会社はフィクションですが、e-business のためのインターネット利用計画やその結果としてのセキュリティ・ニーズは、実社会におけるさまざまな会社の状況を代表しています。

JKL Toy Company は、大手ではないが急成長しているおもちゃ製造会社で、縄跳びからたこ、かわいい縫いぐるみのヒョウまでを扱います。この会社の社長の関心事は、ビジネスの成長と、その成長に伴う負荷を新規に導入した iSeries がいかに軽減してくれるかということです。会計マネージャーの Sharon Jones は、iSeries のシステム管理とシステム・セキュリティを任されています。

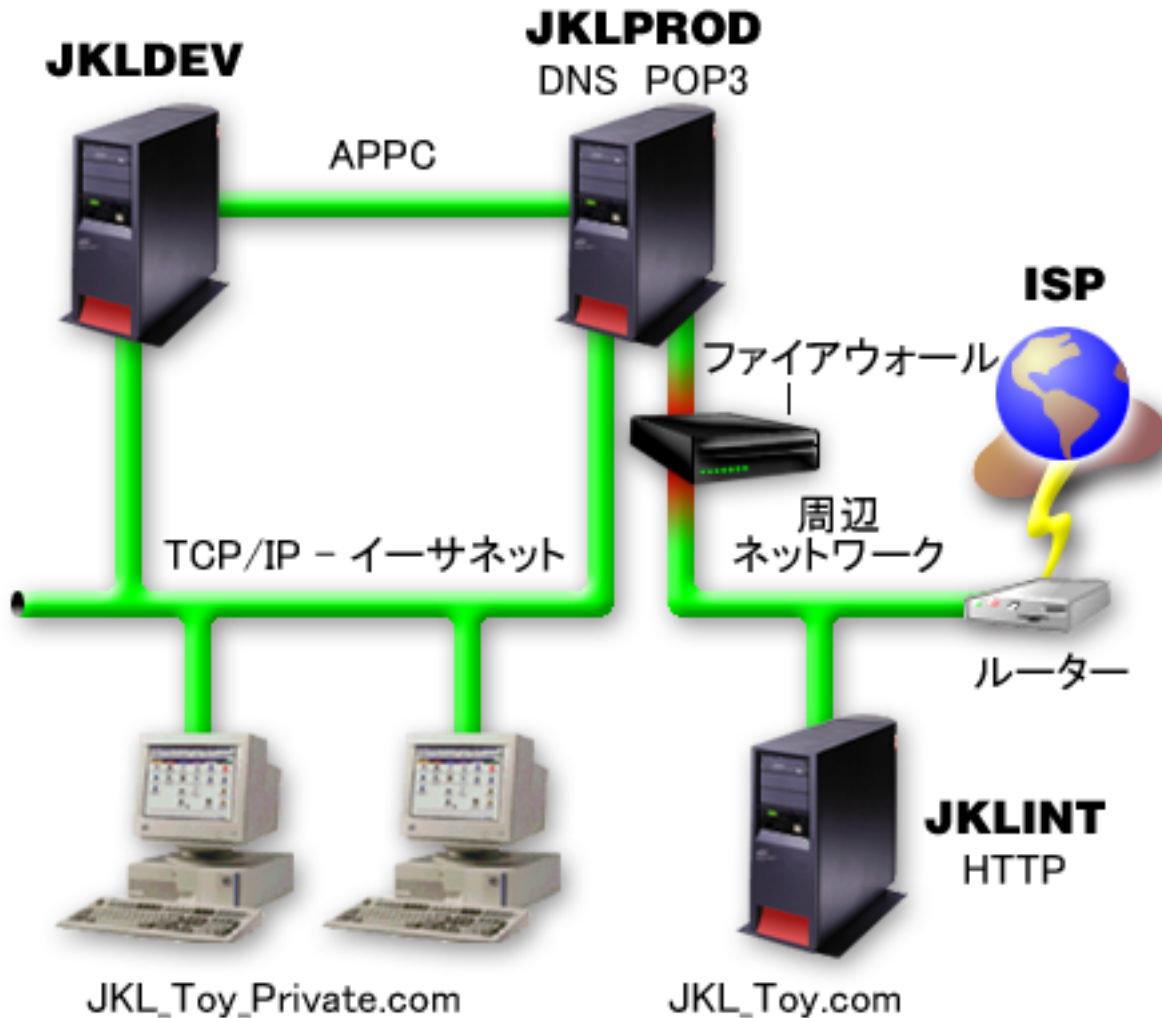
JKL Toy Company では、内部アプリケーションに関するセキュリティ・ポリシーが、1 年以上の間、問題なく運用されています。同社は現在、より効率的に内部情報を共有するために、イントラネットの構築を

計画しています。さらに、ビジネスをさらに推進するために、インターネットの導入も計画しています。これらの目的には、オンライン・カタログを含むインターネット・マーケティング参入の計画も含まれます。同時に、インターネットを利用して機密情報をリモート・サイトから会社のオフィスに送信することも希望しています。また、設計室の従業員に研究開発の目的でインターネットへのアクセスを許可したいという希望もあります。最終的には、顧客が同社の Web サイトを利用して直接オンライン購入ができるようにしたいと考えています。Sharon は、これらの活動に潜在的に伴う特定のセキュリティー・リスクと、そのリスクを最小限にするために必要なセキュリティー措置に関する報告書を作成しています。Sharon は、会社のセキュリティー・ポリシーを更新し、採用が決定したセキュリティー措置を実行に移すときの責任者になる予定です。

この会社がインターネットへの参入を強化する目的は、以下のとおりです。

- 総合的なマーケティング・キャンペーンの一環として、一般的な企業イメージとその存在感を高める。
- 顧客および販売スタッフにオンラインの製品カタログを提供する。
- 顧客サービスを改善する。
- 従業員に電子メールと WWW へのアクセスを提供する。

JKL Toy company では、iSeries サーバーに強力な基本システム・セキュリティーを確立した上で、ネットワーク・レベルでの保護を行うためにファイアウォール製品の購入と使用を決定しました。このファイアウォールは、インターネットに関連する多数の潜在的なリスクから、内部のネットワークを遮断してくれます。以下に、この会社におけるインターネット / ネットワークの構成を図示します。



図に示すように、JKL Toy company には、2 つの主要な iSeries サーバーが存在します。1 つは開発用 (JKLDEV) のシステム、もう 1 つは本番用 (JKLPROD) アプリケーションのシステムです。これらのシステムはいずれもが、主幹業務のデータとアプリケーションを扱っています。そのため、これらのシステムでインターネット・アプリケーションを実行することは望ましくありません。そこで、iSeries サーバーを新規に追加し (JKLINT)、インターネット・アプリケーションを実行することにしました。

この会社では周辺ネットワーク上に新規システムを配置し、これと社内の主要内部ネットワークとの間でファイアウォールを使用することにより、自社ネットワークとインターネットとの適切な分離が保証されています。このように分離することにより、内部システムがさらされるインターネット・リスクを減少させることができます。この会社では、新規の iSeries をインターネット・サーバー専用とすることにより、ネットワーク・セキュリティーの管理をより簡潔なものにしています。

この段階では、新規の iSeries サーバー上で主幹業務のアプリケーションを実行することはありません。e-business 計画のこの段階では、新規システムにより、静的な公衆 Web サイトのみを提供しています。しかし、会社では、サービスの中断やその他可能性のあるアタックを防止するために、システムや運営する Web サイトを保護するセキュリティー措置を講じることを希望しています。そこで、強力な基本セキュリティー措置のほかに、パケット・フィルタ操作規則と、ネットワーク・アドレス変換 (NAT) 規則でシステムを保護する予定を立てています。

この会社では、より高度な公用アプリケーション (e-commerce Web サイトやエクストラネット・アクセスなど) を開発するにしたがって、より高度なセキュリティー措置を講じていくことになります。

第 4 章 インターネットの基本準備としてのセキュリティのレベル

システム・セキュリティの措置は、インターネットの基本セキュリティ問題に対する最終防御ラインを表します。したがって、インターネット・セキュリティ戦略全般における第一歩とは、OS/400 の基本セキュリティ設定を適切に構成することにあります。以下を実行して、システム・セキュリティが最小要件を確実に満たすようにしてください。

- セキュリティ・レベル (QSECURITY システム値) を 50 に設定します。セキュリティ・レベル 50 では、最高レベルの保全性保護を提供します。インターネットのようなりスクの高い環境でシステムを保護するには、レベル 50 を強くお勧めします。



注: 高度なトランザクション指向のシステム、または統合ファイル・システムを広く使用するアプリケーションを使用している場合は、セキュリティ・レベル 50 での操作によって、システムまたはアプリケーションの性能が低下することがあります。

各 iSeries セキュリティ・レベルの詳細については、「iSeries セキュリティの手引き」を参照してください。

注: 現在セキュリティ・レベルが 50 より下で実行されている場合は、操作手順かアプリケーションを更新する必要があるかもしれません。より高いセキュリティ・レベルへの変更を行う前に、

「iSeries 機密保護解説書」 の内容を確認してください。

- セキュリティ関連システム値を少なくとも推奨設定値に近い値に設定します。iSeries ナビゲーターのセキュリティ・ウィザードを使用し、推奨されるセキュリティ設定を構成することができます。
- IBM 提供のユーザー・プロファイルを含め、ユーザー・プロファイルにデフォルト・パスワードがないことを確認します。デフォルト・パスワード分析 (ANZDFTPWD) コマンドを使用して、デフォルト・パスワードがあるかどうかを検査します。
- オブジェクト権限を使用して重要なシステム・リソースを保護します。システムでは限定されたアプローチを取ってください。つまり、デフォルトでは、誰もがライブラリーやディレクトリーなどのシステム・リソースへのアクセスが制限されています (PUBLIC *EXCLUDE)。このような制限付きリソースにアクセスできるユーザーは、少数に限定します。メニューを介したアクセス制限は、インターネット環境では十分ではありません。
- システムにオブジェクト権限を設定する必要があります。オブジェクト権限に関する詳細は、「iSeries セキュリティの手引き」の『iSeries ナビゲーター』の章を参照してください。

システム・セキュリティの最小要件を構成する際には、 **server Security Planner** ( **server Information Center Web** サイトから利用可能) または**セキュリティ・ウィザード** (iSeries ナビゲーター・インターフェースから利用可能) を使用すると便利です。Security Planner では、一連の質問に対する回答を基にして、セキュリティの一連の推奨事項が提示されます。これらの推奨設定を参考にして、必要なシステム・セキュリティの設定を構成することができます。機密保護ウィザードでも、一連の質問に対する応答を基にして推奨設定を提示します。セキュリティ・アドバイザーとは異なり、この推奨設定を基にしてウィザードに自分のシステム・セキュリティ設定を構成させることが可能です。

iSeries 固有のセキュリティ機能を適切に構成および管理すれば、多くのリスクを最小限に押さえることができます。ただし、iSeries をインターネットに接続する場合は、内部ネットワークの安全性を得るためのセキュリティ措置をさらに講じる必要があります。iSeries の汎用システム・セキュリティが問題な

く機能することが確認できたならば、インターネット使用のための包括的セキュリティー計画の一環として、さらに進んだセキュリティー措置を講じる準備が整ったことになります。

第 5 章 ネットワーク・セキュリティ・オプション

非トラステッド・ネットワークに接続するときは、ネットワーク・レベルで実装するセキュリティ措置も含め、セキュリティ・ポリシーに包括的なセキュリティ機構を記述することが必要です。ファイアウォールのインストールは、包括的なネットワーク・セキュリティ措置を展開するには、最良の方法の 1 つです。

さらに、インターネット・サービス・プロバイダー (ISP) は、ネットワーク・セキュリティ計画において重要な役割を果たすことが可能であり、またそうすべきでもあります。ネットワーク・セキュリティ機構では、ISP ルーター接続のフィルター規則やパブリック・ドメイン・ネーム・サービス (DNS) 対策など、インターネット・サービス・プロバイダー (ISP) が提供するセキュリティ措置の内容について概要を示すことが必要です。

ファイアウォールは確かに、総合セキュリティ計画における中心的な防御ラインとなりますが、それが**唯一の防御ラインというわけではありません**。インターネット上の潜在的なセキュリティ・リスクはさまざまなレベルで発生しうるため、これらのリスクに対しては多重階層による防御が可能なセキュリティ措置を講じる必要があります。

ファイアウォールによってある種のアタックからは十分に保護されていても、ファイアウォールはセキュリティ・ソリューション全体の一部でしかありません。たとえば、SMTP メール、FTP、および TELNET のようなアプリケーションを介してインターネット上に送信するデータを、ファイアウォールは必ずしも保護することはできません。このデータを暗号化しない限り、インターネット上の誰でもが、データが宛先に届くまでにこのデータにアクセスすることができます。

iSeries サーバーや内部ネットワークをインターネットに接続する場合は、ファイアウォール製品を中心的な防御ラインとして使用することを真剣に検討すべきです。IBM Firewall for AS/400 はもう購入することができず、この製品を対象とするサポートも受けられなくなりましたが、これ以外の使用可能な製品は数多くあります。さまざまな移行オプションに関する詳細なシナリオについては、「All You Need to Know When Migrating from IBM Firewall for AS/400」を参照してください。

商用ファイアウォール製品では、ネットワーク・セキュリティ・テクノロジーの全域をカバーしており、JKL Toy Company でも、その e-business セキュリティのシナリオにおいて、そうしたファイアウォールをネットワークの保護に使用することにしました。しかし、新規に導入した iSeries インターネット・サーバーに対しては、ファイアウォールは一切の保護を行いません。そこで、この会社では iSeries パケット・ルール機能を実装して、インターネット・サーバーのトラフィックを制御するためのフィルターと NAT 規則を作成することにしました。

iSeries パケット・ルールについて

パケット・フィルター規則は、定義した基準に従って IP パケットを拒否または受諾することで、コンピューター・システムを保護することが可能です。NAT 規則では、ある IP アドレスを別の IP アドレス (公衆 IP アドレス) に置き換えることで、外部ユーザーから内部のシステム情報を隠蔽することが可能です。IP パケット・フィルターと NAT 規則は、ネットワーク・セキュリティ・テクノロジーのコアですが、完全に機能するファイアウォール製品と同レベルのセキュリティは提供していません。完全なファイアウォール製品と iSeries パケット・ルール機能のどちらに決定するかについては、セキュリティのニーズと目的を慎重に分析する必要があります。

トピック『iSeries ネットワーク・セキュリティー・オプションの選択』を検討して、セキュリティー・ニーズに応じたアプローチを決定するために役立ててください。

ファイアウォール

ファイアウォールは、保護された内部ネットワークと、インターネットのような非トラステッド・ネットワークの間の障壁です。多くの企業で、内部ネットワークを安全にインターネットに接続するためにファイアウォールを使用していますが、ある内部ネットワークを別の内部ネットワークから保護するために使用することもできます。

ファイアウォールでは、保護された内部ネットワークと非トラステッド・ネットワークの間に、制御された1つの接点(チョークポイントと呼ばれる)があります。ファイアウォールは次のことを行います。

- 内部ネットワークのユーザーが、ネットワークの外側にある許可されたリソースを使用できるようにします。
- ネットワークの外側の許可されていないユーザーが、内部ネットワークのリソースを使用するのを防ぎます。

ファイアウォールを、インターネット(またはその他のネットワーク)へのゲートウェイとして使用すると、内部ネットワークへのリスクを著しく削減することができます。ファイアウォール機能がセキュリティー・ポリシーの指示の多くを実行するため、ファイアウォールを使用することでネットワーク・セキュリティーの管理も簡単になります。

ファイアウォールの仕組み

ファイアウォールの仕組みを理解するために、ネットワークをアクセス制御の対象となるビルであると考えてみます。このビルの入り口はロビーしかありません。このロビーには、訪問者を迎える受付係、訪問者を監視する警備員がおり、訪問者の行動を記録するためのビデオ・カメラ、それにこのビルの訪問者を認証するバッジ読み取り装置が配備されています。

これらの手段は、このビルへのアクセスを問題なく制御しているかもしれませんが、しかし、もし認証を受けていない人物がこのビルにうまく入り込めば、この侵入者の行動からビルを守る方法はありません。ただし、この侵入者の動きを監視していれば、この侵入者が取る不審な行動を見つける機会もあります。

ファイアウォールのコンポーネント

ファイアウォールはハードウェアとソフトウェアの集合であり、一緒に使用することにより、ネットワークの一部への無許可アクセスを防ぐことができます。ファイアウォールは次のコンポーネントからなります。

- ハードウェア。ファイアウォールのハードウェアは、通常、ファイアウォールのソフトウェア機能実行専用の、別々のコンピューターや装置からなります。
- ソフトウェア。ファイアウォールのソフトウェアにはさまざまなアプリケーションがあります。ネットワーク・セキュリティーという観点において、ファイアウォールは、各種のテクノロジーによって以下のようなセキュリティー制御を実現しています。
 - インターネット・プロトコル (IP) パケット・フィルター操作
 - ネットワーク・アドレス変換 (NAT) サービス
 - SOCKS サーバー
 - HTTP、Telnet、FTP、など、各種サービスのための Proxy サーバー
 - メール・リレー・サービス
 - 分割ドメイン・ネーム・サービス (DNS)
 - ログ記録
 - リアルタイム・モニター

注: 一部のファイアウォールでは、VPN (仮想プライベート・ネットワーク) サービスを提供しているの
で、使用しているファイアウォールとその他の互換性のあるファイアウォールの間で暗号化されたセ
ッションをセットアップすることができます。

ファイアウォール・テクノロジーの使用

ファイアウォール、Proxy サーバー、SOCKS サーバー、または NAT 規則を使用すると、内部ユーザーは
インターネット上のサービスに安全にアクセスすることができます。Proxy サーバーと SOCKS サーバー
は、内部情報を非トラステッド・ネットワークから隠蔽するために、ファイアウォールで TCP/IP 接続を切
断します。またサーバーは、追加ログ記録機能も持っています。

NAT を使用すると、インターネット・ユーザーは、ファイアウォールの背後にある公衆サーバーに簡単に
アクセスすることができます。その場合でもファイアウォールはネットワークを保護してくれます。これ
は、NAT が内部の IP アドレスを隠蔽するからです。

ファイアウォールは、ファイアウォールが使用する DNS サーバーを提供することで、内部情報を保護する
こともできます。DNS サーバーは実際には 2 つです。1 つは内部ネットワークに関するデータに使用す
るもの、ファイアウォール上のもう 1 つは、外部ネットワークとファイアウォール自身に関するデータ用
です。これによって、内部システムに関する情報への外部からのアクセスを制御することができます。

ファイアウォール戦略を定義する場合、組織にリスクを与えるようなものはすべて禁止し、それ以外はす
べて許可するだけで十分であると考えられるかもしれませんが。コンピューター犯罪者は絶えず新しいア
タック方法を作り出してくるので、これらのアタックを防ぐ方法を前もって考えておかなければなりませ
ん。上述のビルの場合のように、何らかの方法で、誰かが防御を突破した兆候を監視する必要があります。一
般に、侵入を防ぐよりは、侵入から回復する方が損害が大きく、コストもかかります。

ファイアウォールの場合、最良の戦略は、テスト済みの信頼性のあるアプリケーションだけを許可するとい
うものです。この戦略に従えば、ファイアウォール上で実行すべきサービスのリストを完全に定義しなけれ
ばなりません。各サービスは、接続の方向 (内側から外側、または外側から内側) によって表現すること
ができます。各サービスの使用を許可されるユーザーと、そのための接続ができるマシンもリストしてくださ
い。

ネットワーク保護のためにファイアウォールでできること

ファイアウォールを、ユーザーのネットワークと、インターネット (またはその他の非トラステッド・ネッ
トワーク) との接続点の間にインストールします。するとファイアウォールにより、ユーザーのネットワ
ークへの入り口点を制限することができます。ファイアウォールにより、ユーザーのネットワークとインター
ネットの間に単一の接点 (チョークポイントと呼ばれる) が設けられます。接点が 1 つなので、ネットワ
ークに出入りするトラフィックの許可をより簡単に制御することができます。

ファイアウォールは単一のアドレスとして公開されます。ファイアウォールは、内部ネットワーク・アドレ
スは隠蔽したまま、Proxy サーバーまたは Socks サーバーやネットワーク・アドレス変換 (NAT) を介し
て、非トラステッド・ネットワークへのアクセスを提供します。こうして、ファイアウォールは内部ネット
ワークのプライバシーを保守します。ネットワークに関する情報をプライベートにしておくことは、ファイ
アウォールで偽名を使用したアタック (スプーフィング) を受けにくくするための方法の 1 つです。

ネットワークへのアタックのリスクを最小化するために、ファイアウォールはユーザーがネットワークへの
トラフィックの出入りを制御できるようにします。ファイアウォールはネットワークに入るトラフィックす
べてを安全にフィルターに掛け、特定の宛先への、特定のタイプのトラフィックしか入れないようにしま
す。こうすることで、誰かが TELNET やファイル転送プロトコル (FTP) を使用して、内部システムへの
アクセスを獲得するリスクを最小化します。

ネットワーク保護のためにファイアウォールではできないこと

ファイアウォールによってある種の攻撃からは十分に保護されていても、ファイアウォールはセキュリティー・ソリューション全体の一部でしかありません。たとえば、SMTP メール、FTP、および TELNET のようなアプリケーションを介してインターネット上に送信するデータを、ファイアウォールは必ずしも保護することはできません。このデータを暗号化しない限り、インターネット上の誰でもが、データが宛先に届くまでにこのデータにアクセスすることができます。

iSeries パケット・ルール

iSeries パケット・ルール は、iSeries ナビゲーター・インターフェースから利用可能な OS/400 の統合機能です。パケット・ルール機能では、2 種類のコアとなるネットワーク・セキュリティー・テクノロジーを構成して、iSeries システムを保護するために TCP/IP トラフィックの流れを制御することができます。

- ネットワーク・アドレス変換 (NAT)
- IP パケット・フィルタ操作

NAT および IP フィルタ操作は、OS/400 に統合されたパーツであり、経済的にシステムを保護するための手段となりえます。場合によっては、何も買い足すことなく、このセキュリティー・テクノロジーですべてがまかなえることもあります。しかし、これらのテクノロジーは、本当の意味でのファイアウォール機能を作り出すわけではありません。セキュリティーのニーズと目的に合わせ、IP パケット・セキュリティーを単独で使用したり、またはファイアウォールと併せて使用することができます。

注: iSeries 実動システムの保護を計画している場合は、コスト削減ということは念頭に置くべきではありません。このような状況では、システムのセキュリティーはコストより優先されます。実動システムに対して最大限の保護を保証するためには、ファイアウォールの使用を考慮してください。

NAT と IP パケット・フィルタ操作、および両者の協調関係

ネットワーク・アドレス変換 (NAT) は、システムを流れるパケットのソースまたは宛先の IP アドレスを変更します。NAT は、Proxy サーバーおよび SOCKS サーバーに代わる、より透過性のあるサーバーを提供します。また、NAT は互換性のないアドレッシング構造を持つネットワーク同士の相互接続を可能にすることで、ネットワーク構造を簡単にすることができます。そのため、NAT の規則を使用すると、競合していたり互換性のないアドレッシング方式を使用している 2 つのネットワーク間のゲートウェイとして iSeries システムを機能させることができます。さらに、NAT を使用すれば、実アドレスを 1 つ以上のアドレスに動的に置き換えることで、あるネットワークの実 IP アドレスを隠蔽することもできます。IP パケット・フィルタ操作と NAT はお互いに補足し合うものであるため、ネットワーク・セキュリティーを強化するためにこれらの機能を一緒に使うことが頻繁にあります。

NAT を使用すれば、ファイアウォールの背後にある公衆 Web サーバーの操作が簡単になります。Web サーバーの公開 IP アドレスは、私用の内部 IP アドレスに変換されます。これにより、必要な登録 IP アドレスの数が少なくなり、既存ネットワークへの影響が最小限に抑えられます。また、内部ユーザーが、私用の内部 IP アドレスを隠蔽しながら、インターネットにアクセスできる機構を提供します。

IP パケット・フィルタ操作 は、パケットのヘッダー情報に基づいて、IP トラフィックを選択的にブロックまたは保護することができます。iSeries ナビゲーターのインターネット・セットアップ・ウィザードを使用すれば、望ましくないネットワーク・トラフィックをブロックする基本的なフィルタ操作規則を、短時間で簡単に構成することができます。

IP パケット・フィルタ操作を使用して、以下のようなことが可能になります。

- 一組のフィルター規則を作成して、ネットワークに入ることを許可する IP パケットと、ネットワークへのアクセスを拒否する IP パケットを指定することができます。フィルター規則の作成時に、それらの規則を物理インターフェース (たとえば、トークンリングやイーサネット回線など) に適用します。複数の物理インターフェースに、この規則を適用することができます。あるいは、インターフェースごとに別々の規則を適用することもできます。
- 特定の packets を許可または拒否するための規則は、以下のヘッダー情報に基づいて作成することができます。
 - 宛先 IP アドレス
 - ソース IP アドレス・プロトコル (たとえば、TCP、UDP など)
 - 宛先ポート (たとえば、HTTP 用のポート 80)
 - ソース・ポート
 - IP データグラム方向 (インバウンドまたはアウトバウンド)
 - 転送またはローカル
- 望ましくないトラフィックや不要なトラフィックが、システムのアプリケーションに届かないようにすることができます。また、トラフィックを別のシステムに転送できないようにすることもできます。これには、特定のアプリケーション・サーバーを必要としない低水準 ICMP パケット (たとえば、PING パケットなど) が含まれます。
- フィルター規則が、規則と一致する packets に関する情報を持つログ項目をシステム・ジャーナルに作成するかどうかを指定します。一度情報がシステム・ジャーナルに書き込まれると、ログ項目を変更することはできません。したがって、ログは、ネットワーク活動を監査する理想的なツールとなります。

iSeries ネットワーク・セキュリティ・オプションの選択

一般に、未承認アクセスに対するガードであるネットワーク・セキュリティ・ソリューションは、保護を提供するファイアウォール技術に依存しています。iSeries システムを保護するために、フル装備のファイアウォール製品を使用することも、OS/400 TCP/IP 実装の一環として、特定のネットワーク・セキュリティ・テクノロジーを有効にすることもできます。この実装は、パケット・ルール機能 (IP フィルター操作と NAT を含む) および HTTP for iSeries Proxy サーバー機能から成り立っています。

パケット・ルール機能とファイアウォールのどちらを使用するかは、ネットワーク環境、アクセス要件、およびセキュリティ・ニーズによって異なります。iSeries サーバーや内部ネットワークをインターネットや非トラステッド・ネットワークに接続する場合は、ファイアウォール製品を中心的な防御ラインとして使用することを真剣に検討すべきです。

一般にファイアウォールは、外部アクセスへのインターフェースの数が限られている、専用ハードウェアとソフトウェアからなる装置であるため、このケースではファイアウォールが望ましいでしょう。インターネットのアクセス保護のために OS/400 TCP/IP テクノロジーを使用するときは、外部アクセスにオープンなインターフェースとアプリケーションを無数にもつ汎用プラットフォームを使用しています。



この違いの重要な理由はいくつかあります。たとえば、ファイアウォール専用製品は、ファイアウォール自身を構成するもの以外に他にどのような機能もアプリケーションも提供しません。したがって、アタッカーがファイアウォールを逃れてアクセスに成功したとしても、アタッカーはたいしたことはできません。一方、iSeries 上の TCP/IP セキュリティ機能を回避できたアタッカーは、さまざまな種類の有用なアプリケーション、サービス、およびデータにアクセスできる可能性があります。アタッカーはそれらを使用して、そのシステム自身で破滅的大破壊を行ったり、内部ネットワークの他のシステムへのアクセスを獲得したりできます。

iSeries TCP/IP セキュリティ機能の使用に対応できますか? 行おうとしているすべてのセキュリティの選択において、コスト対利益のトレードオフに基づいて決定を下さなければなりません。ビジネスのゴール

を分析して、リスクを最小化するためのセキュリティにかけられる費用と、どの程度までそれらのリスクを負えるのかについて、見極める必要があります。次の表では、TCP/IP セキュリティ機能と完全な機能のファイアウォール装置とを比較して、それぞれどのような場合に適しているのかを示しています。この表を使用すると、ネットワークとシステムの保護を提供する際に、ファイアウォールを使用するべきか、TCP/IP セキュリティ機能を使用するべきか、あるいは両方の組み合わせを使用するべきかを判断することができます。

セキュリティ・テクノロジー	OS/400 TCP/IP テクノロジーに最適な使用法	完全な機能のファイアウォールに最適な使用法
IP パケット・フィルタ操作	<ul style="list-style-type: none"> 機密データを扱う公衆 Web サーバーやイントラネット・システムなどの単一 iSeries サーバー用に、追加の保護を行う。 社内イントラネットのサブネットワークを保護する。iSeries サーバーが残りの社内ネットワークに対するゲートウェイ (カジュアル・ルーター) として機能している場合。 iSeries サーバーがゲートウェイとして機能している VPN (プライベート・ネットワーク) またはエクストラネットを介して、多少信頼性のあるパートナーとの通信を制御する。 	<ul style="list-style-type: none"> 社内ネットワークが接続しているインターネットまたはその他の非トラステッド・ネットワークから社内ネットワーク全体を保護する。 トラフィックの多い大規模サブネットワークを、社内ネットワークの残りの部分から保護する。
ネットワーク・アドレス変換 (NAT)	<ul style="list-style-type: none"> 非互換のアドレッシング構造を持つ 2 つの VPN (プライベート・ネットワーク) を接続できるようにする。 非トラステッド・ネットワークからサブネットワークのアドレスを隠す。 	<ul style="list-style-type: none"> インターネットまたはその他の非トラステッド・ネットワークにアクセスするクライアントのアドレスを隠す。Proxy と SOCKS サーバーの代わりとして使用する。 インターネットのクライアントが、プライベート・ネットワークのシステムのサービスを使用できるようにする。
Proxy サーバー	<ul style="list-style-type: none"> 中央ファイアウォールがインターネットへのアクセスを提供するときに、社内ネットワークのリモート・ロケーションで Proxy を行う。 	<ul style="list-style-type: none"> インターネットにアクセスするときに、社内ネットワーク全体の Proxy を行う。

OS/400 TCP/IP セキュリティ機能の使用法についての詳細は、次の資料を参照してください。

- パケット・ルール (フィルタ操作と NAT)
- HTTP Server Documentation Center 
- AS/400 Internet Security Scenarios: A Practical Approach  (SG24-5954)

第 6 章 アプリケーション・セキュリティ・オプション

アプリケーション・レベル・セキュリティの措置では、ユーザーが特定のアプリケーションとどのように対話するかを制御します。一般に、使用する各アプリケーションごとに、セキュリティ設定を構成することが必要です。一方、インターネットから使用したり、インターネットに提供するアプリケーションやサービスについては、セキュリティのセットアップに特別の配慮をしてください。このようなアプリケーションやサービスは、ネットワーク・システムへアクセスする方法を模索している無許可ユーザーによって、不正に使用される危険があります。採用するセキュリティの措置では、サーバー側とクライアント側の両方でセキュリティがさらされるリスクをカバーしている必要があります。

使用する各アプリケーションの保護は重要ですが、セキュリティ・ポリシーの実装全体でセキュリティ措置が果たす役割は小さいものです。

一般的なインターネット・アプリケーションを保護するための詳細については、以下のページを検討してください。

- 『Web サーバーにおけるセキュリティ』
- 24 ページの『Java インターネット・セキュリティ』
- 27 ページの『電子メール・セキュリティ』
- 28 ページの『FTP セキュリティ』

Web サーバーにおけるセキュリティ

Web サイトに訪問者のアクセスを認めるときも、サイトのセットアップ方法やページの生成に使用するコーディングまで公開することは、望ましくありません。すべての作業は舞台裏で行い、ページへのアクセスは、簡単、高速、かつシームレスに行えるようにすることが目標です。管理者は、セキュリティを実施することによって Web サイトにマイナスの影響を与えてしまわないようにする必要があります。iSeries を Web サーバーとして使用する場合は、以下の点を考慮してください。

- サーバー管理者は、クライアントと HTTP サーバーとの対話が可能になる前に、サーバーに関するディレクティブを定義することが必要です。セキュリティ・チェックを作成するには、2 通りの方法、つまり汎用サーバーのディレクティブとサーバー保護のディレクティブがあります。Web サーバーへの要求はすべて、サーバーが要求を受け付ける前にディレクティブが提供する制約事項をすべて満たす必要があります。
- これらのディレクティブの作成と編集には、サーバーにおけるサーバー構成用の Web 管理ページを使用します。サーバー・ディレクティブを使用すると、Web サーバーの全体の振る舞いを制御できます。サーバー保護ディレクティブを使用すると、Web サーバーが処理する特定の URL にサーバーが使用するセキュリティ・モデルを指定し、制御できます。
- サーバーを構成するには、マップまたはパス・ディレクティブとサーバーの Web 管理ページを使用することができます。
 - iSeries の Web サーバーでファイル名をマスクするために、MAP または PASS ディレクティブを使用します。さらに詳しくいえば、Web サーバーが処理する URL が置かれているディレクトリーを制御する PASS サーバー・ディレクティブと、MAP サーバー・ディレクティブがあります。また、CGI-BIN プログラムが常駐するライブラリーを制御する EXEC サーバー・ディレクティブもあります。

サーバーの URL ごとに保護ディレクティブを定義します。すべての URL に保護ディレクティブが必要なわけではありません。ただし、URL のリソースへのアクセス方法またはアクセスする人を制御したい場合は、その URL の保護ディレクティブが必要です。

- また、WRKHTTPCFG (HTTP 構成の処理) コマンドを使用してディレクティブを入力するのではなく、サーバーの Web 管理ページを使用して、サーバーを構成することができます。コマンド行インターフェイスから保護ディレクティブを使用すると、作業が非常に複雑になることがあります。したがって、ディレクティブを確実に正しくセットアップするには、Web 管理ページを使用してください。

HTTP にはデータを表示する機能はありますが、データベース・ファイルのデータを変更することはできません。しかし、データベース・ファイルを更新する必要があるアプリケーションを作成することもあります。これを行うときは、CGI-BIN プログラムを使用することができます。たとえば、ユーザーがフォームへの記入を完了した時点で、iSeries データベースを更新するフォームを作成しようとすることもあります。セキュリティ管理者は、そのユーザー・プロファイルの権限と CGI プログラムが実行する機能をモニターするようにしてください。また、機密オブジェクトが不適切な共通権限を持つ可能性も検討してください。

注: CGI (共通ゲートウェイ・インターフェイス) は、Web サーバーと Web サーバーの外部にあるコンピューター・プログラム間の情報交換のための業界標準です。このプログラムは、Web サーバーが稼働中のオペレーティング・システムでサポートされているプログラム言語であれば、どれを使用しても作成することができます。

Web ページでは、CGI プログラムを使用する以外に、Java™ を使用したい場合があります。Web ページに Java を追加する前に、必ず Java セキュリティーについて理解しておいてください。

HTTP サーバーは、サーバーを通じたアクセスとアクセス試行の両方をモニターするのに使用できるアクセス・ログを提供します。

Proxy サーバーは、Web ブラウザーから HTTP 要求を受け取り、それらの要求を Web サーバーに再送します。要求を受け取る Web サーバーは、Proxy サーバーの IP アドレスしか認知しません。要求を受け取る Web サーバーは、その要求の送信元である PC の名前やアドレスを判別できません。Proxy サーバーは、HTTP、ファイル転送プロトコル (FTP)、Gopher、および WAIS についての URL 要求を処理できます。

Web アクセスを統合するために、IBM HTTP Server for iSeries の HTTP Proxy サポートを使用することもできます。Proxy サーバーは、トラッキングの目的で、URL 要求をすべてログに記録することもできます。こうすれば、そのログを検討して、ネットワーク・リソースの使用および誤用をモニターすることができます。

この件についての詳細は、「iSeries セキュリティーの手引き」 を参照してください。

Java インターネット・セキュリティ

Java プログラミングは、今日のコンピューティング環境に広く浸透してきています。たとえば、システムで、IBM Toolbox for Java や IBM Development Kit for Java を使用して新規のアプリケーションを開発しているかもしれません。したがって、Java に関連するセキュリティ問題に取り組む準備をしなければなりません。ファイアウォールは、一般的なインターネットのセキュリティ・リスクに対する優れた防壁ではありませんが、Java の使用によって生じる多くのリスクに対する防壁にはなりません。セキュリティ・ポリシーには、アプリケーション、アプレット、およびサーブレットという Java の 3 つの重要な領

域に対して、システムを保護するための詳細を組み込まなければなりません。また、Java プログラムの認証と権限の点から、Java とリソース・セキュリティーの相互作用について理解する必要があります。

Java アプリケーション

言語としての Java は、Java プログラマーが保全性の問題を起こすような不注意によるエラーを犯さないようにするための、いくつかの特性を持っています。(C や C++ など、PC アプリケーションでよく使用される他の言語の場合は、プログラマーの不注意によるエラーに対しては、Java で行っているような強力な防止策は取られていません。)たとえば、Java は強力な分類方法を使用して、プログラマーがオブジェクトを不注意に使用しないようにします。Java では、ポインター操作は許されません。このため、プログラマーが間違っただけでプログラムのメモリー境界を超えたりすることはありません。アプリケーション開発の観点からは、Java を他の高水準言語と同様に扱うことができます。アプリケーション設計については、iSeries サーバー上の他の言語の場合と同じセキュリティー規則を適用する必要があります。

Java アプレット

Java アプレットは、HTML ページに組み込むことのできる小さな Java プログラムです。アプレットはクライアント上で実行されるので、その実行内容は、クライアント側での関心事になります。ただし、Java アプレットは、iSeries サーバーにアクセスする可能性があります。(ネットワーク内の PC で動作する ODBC プログラムまたは拡張プログラム間通信 (APPC) プログラムも同様に、iSeries へアクセスすることができます。)一般に、Java アプレットは、それが生成されたサーバーとのみセッションを確立することができます。したがって、Java アプレットは、自分が iSeries サーバー (たとえば、Web サーバー) から生成されたときのみ、接続 PC から iSeries にアクセスすることができます。

アプレットは、サーバー上の任意の TCP/IP ポートに接続を試みることができます。Java で作成されたソフトウェア・サーバーに送信する必要はありません。ただし、IBM Toolbox for Java で作成されたサーバーの場合、アプレットはサーバーへの逆方向接続を確立する際に、ユーザー ID とパスワードを提供しなければなりません。この資料で解説されているサーバーはすべて iSeries サーバーです。(Java で作成されたサーバーは、IBM Toolbox for Java を使用する必要はありません)。一般に、IBM Toolbox for Java のクラスは、最初の接続時にユーザーに対して、ユーザー ID とパスワードを入力するようプロンプトを出します。

アプレットが iSeries サーバーで機能を実行できるのは、ユーザー・プロファイルがその機能に対する許可を持っている場合のみです。したがって、Java アプレットを使用して新規のアプリケーション機能を提供するときは、適切なリソース・セキュリティー方式が不可欠になります。システムがアプレットからの要求を処理するときは、ユーザー・プロファイルの限定機能値を使用しません。

アプレット・ビューアーを使用すると、サーバー・システム上でアプレットをテストできますが、ブラウザーのセキュリティー制限には従いません。したがって、アプレット・ビューアーは、自分のアプレットのみをテストするために使用し、外部ソースからアプレットを実行することはしないでください。Java アプレットは、よくユーザーの PC ドライブに書き込みを行います。これはアプレットに、破壊的なアクションを実行する機会を与えているようなものです。ただし、認証性を確立するために、デジタル証明書を使用して Java アプレットに署名することができます。署名済みのアプレットは、ブラウザーのデフォルト設定によって PC ローカル・ドライブへの書き込みが禁止されていても、それを行うことができます。署名済みのアプレットは、iSeries サーバー上のマップされたドライブにも書き込むことができます。なぜならば、PC には、これらのドライブがローカル・ドライブのように見えるからです。

注: 上述の振る舞いは、一般に Netscape Navigator と MS Internet Explorer に当てはまります。実際に何が起るかは、使用するブラウザーをどのように構成し、管理しているかによって大きく異なります。

iSeries から生成された Java アプレットの場合は、署名済みアプレットを使用しなければならないことがあります。しかし、ソースのはっきりしない署名済みアプレットは受け入れないようユーザー一般を指導しておく必要があります。

V4R4 以降では、IBM Toolbox for Java を使用して Secure Sockets Layer (SSL) 環境をセットアップすることができます。また、IBM Developer kit for Java を使用して Java アプリケーションを SSL で保護することができます。Java アプリケーションで SSL を使用することによって、クライアントとサーバー間で渡されるユーザー ID とパスワードを含む、データの暗号化が保証されます。デジタル証明書マネージャーを使用して、SSL を使用するために登録済み Java プログラムを構成することができます。

Java サブレット

サブレットは、Java で作成されたサーバー側のコンポーネントです。これは、Web サーバーのコードを変更せずに、Web サーバーの機能性を動的に拡張します。IBM HTTP Server for iSeries に付属している IBM WebSphere® Application Server は、iSeries システムでのサブレットの使用をサポートしています。

リソース・セキュリティーは、サーバーが使用するサブレット・オブジェクトに対して使用しなければなりません。ただし、リソース・セキュリティーをサブレットに適用しても、それを十分に保護してくれません。Web サーバーがサブレットをロードしてしまうと、リソース・セキュリティーは他のサーバーでもそれが実行されるのを阻止することはありません。したがって、HTTP サーバーのセキュリティー管理とディレクティブに加えて、リソース・セキュリティーを使用しなければなりません。たとえば、サブレットを、Web サーバーのプロファイルのみで実行できるようにはしないでください。さらに、HTTP サーバー・グループとアクセス制御リスト (ACL) を使用して、どのユーザーがサブレットの実行を許可されているのかを管理します (保護ディレクティブでキーワードをマスクします)。また、WebSphere Application Server for iSeries にあるような、サブレット開発ツールが提供するセキュリティー機能を使用しなければなりません。

Java の一般的なセキュリティー措置については、以下の資料を検討してください。

- IBM Developer Kit for Java Java セキュリティー
- IBM Toolbox for Java セキュリティー・クラス
- iSeries セキュリティーの手引き

リソースに対する Java 認証と許可

IBM Toolbox for Java にはセキュリティーのためのクラスが含まれており、ユーザーの ID 検査を行うとともに、オプションとして、iSeries システム上で実行中のアプリケーションまたはサブレットについてオペレーティング・システムのスレッドにその ID を割り当てます。その後のリソース・セキュリティー・チェックは、割り当てられた ID のもとで行われます。これらのセキュリティー・クラスの詳細については、「IBM Toolbox for Java」の『認証サービス』を参照してください。

IBM Developer Kit for Java は、Java 2 Software Development Kit (J2SDK) 標準版の標準拡張である Java Authentication and Authorization Service (JAAS) のサポートを提供します。現在、J2SDK は、コードが作成された場所とコードに署名した人に基づいたアクセス制御 (コード・ソース・ベースのアクセス制御) を提供しています。J2SDK の使用についての詳細は、「Java Authentication and Authorization Service」を参照してください。

SSL による Java アプリケーションの保護

Secure Sockets Layer (SSL) を使用して、IBM Developer Kit for Java で開発した iSeries アプリケーションの通信を保護することができます。IBM Toolbox for Java を使用するクライアント・アプリケーション

でも、SSL を利用することは可能です。独自の Java アプリケーションで SSL を有効にするときのプロセスは、他のアプリケーションの場合とはやや異なります。

Java アプリケーションでの Secure Sockets Layer 管理の詳細については、以下の Information Center トピックを参照してください。

- IBM Toolbox for Java の『Secure Sockets Layer (SSL) 環境』
- IBM Developer Toolkit for Java を使用して『Java アプリケーションを SSL で保護する』

電子メール・セキュリティ

インターネットあるいはその他の非トラステッド・ネットワークで電子メールを使用すると、ファイアウォールを使用しても保護できないようなセキュリティ・リスクにさらされることとなります。このようなリスクを理解し、セキュリティ・ポリシーに、これらのリスクを最小限に抑えるための方法を記述しておくなければなりません。

電子メールは、通信の別形態と考えられます。電子メールで機密情報を送信する場合には、慎重になることが大切です。電子メールは、多くのサーバーを経て受信されます。したがって、誰かが電子メールを傍受してそれを読む可能性もあります。そこで、電子メールの機密性を保護するためのセキュリティ措置を使用する必要が生じます。

一般的な電子メールのセキュリティ・リスク

電子メールの使用に関連して、いくつかのリスクが存在します。

- **フラッディング** (サービス妨害攻撃の一種) は、システムが多数の電子メール・メッセージで過負荷になると発生します。単一の電子メール・サーバーに何百万という電子メール・メッセージ (空のメッセージを含む) を送信してサーバーをあふれさせる単純なプログラムを作成することは、アタッカーにとって比較的簡単です。適切なセキュリティがないと、サーバーの保管ディスクが無用のメッセージでいっぱいになってしまうために、ターゲット・サーバーはサーバー妨害となります。あるいは、サーバー・リソースがすべてアタッカーからのメールの処理に携わってしまうため、サーバーが応答を停止します。
- **スパミング** (ジャンク電子メール) も、電子メールでよく発生するタイプの攻撃です。インターネット上で e-commerce を展開するビジネスが盛んになるにつれ、不必要または一方的なビジネス関連の電子メールが爆発的に増加しています。これがジャンク・メールであり、電子メール・ユーザーの大規模な配布先リストに基づいて送られ、各ユーザーの電子メール・ボックスを一杯にしてしまいます。
- **機密性**は、インターネット経由で他者に電子メールを送信することに関連したリスクです。この電子メールは、予定した宛先に到達するまでに数多くのサーバーを通過します。メッセージを暗号化していない場合、ハッカーは送信経路の任意の地点でメールを傍受し、読み取ることが可能になります。

電子メール・セキュリティ・オプション

フラッディングやスパミングのリスクから保護するには、電子メール・サーバーを適切に構成しなければなりません。ほとんどのサーバー・アプリケーションで、これらの攻撃に対処する方法を提供しています。また、インターネット・サービス・プロバイダー (ISP) と一緒に作業をして、ISP にこのような攻撃からの保護を提供してもらうこともできます。





さらに必要となるセキュリティ措置は、電子メールのアプリケーションが提供するセキュリティ機能と、必要な機密性のレベルに応じて異なります。たとえば、電子メールのメッセージの内容は十分に機密にされていますか。あるいは、発信および宛先の IP アドレスのような、電子メールに関連するすべての情報を機密にしておきたいですか。

アプリケーションによっては、必要な保護を提供するセキュリティー機能を統合しているものもあります。例えば、Lotus® Notes® Domino® では、文書全体または文書内の個々のフィールドを暗号化する機能など、いくつかの統合されたセキュリティー機能を提供しています。

Lotus Notes Domino では、メールを暗号化するために、ユーザーごとに固有の公開鍵と秘密鍵を作成します。ユーザーの秘密鍵を使用してメッセージを暗号化するので、そのユーザーの公開鍵をもつユーザーだけがこのメッセージを読むことができます。宛先であるメモの受信者には公開鍵を送信する必要があり、これによって受信者はメモの暗号解読をすることができます。誰かから暗号化されたメールが送信された場合、Lotus Notes Domino は送信側の公開鍵を使用して内容の暗号解読を行います。

プログラムのオンライン・ヘルプ・ファイルに、Notes の暗号化機能の使用法についての情報が記載されています。

iSeries 上の Domino のセキュリティーについての詳細は、以下を参照してください。

- Lotus Domino Reference Library. 
- Lotus Notes ユーザー・アシスタンス Web サイト 
- Lotus Notes and Domino R5.0 Security Infrastructure Revealed  (SG24-5341)
- Lotus Domino for AS/400 Internet Mail and More  (SG24-5990)

電子メールで機密情報や、事業所、リモート・クライアント、またはビジネス・パートナーにその他の情報を送信したいときには、いくつかのオプションがあります。

電子メール・サーバー・アプリケーションがこれをサポートする場合は、Secure Sockets Layer (SSL) を使用して、サーバーと電子メール・クライアントの間のセキュア通信セッションを作成することができます。SSL は、これを使用するようにクライアント・アプリケーションが作成されている場合、オプションのクライアント側の認証もサポートします。セッション全体が暗号化されるため、SSL は、データが転送中の間のデータ保全性も保証します。

他に使用可能なオプションとして、VPN (仮想プライベート・ネットワーク) 接続の構成があります。V4R4 からは、iSeries を使用して、リモート・クライアントと iSeries システム間の VPN も含めて、さまざまな VPN 接続を構成することができます。VPN を使用すると、通信エンドポイント間でのトラフィックがすべて暗号化され、データ機密性もデータ保全性も保証されます。

FTP セキュリティー

FTP (ファイル転送プロトコル) は、クライアント (別のシステムのユーザー) とサーバーとの間のファイル転送機能を提供します。また、FTP のリモート・コマンド機能を使用すると、サーバーに対してコマンドを投入することもできます。したがって、FTP は、リモート・システムを使用した作業、あるいはシステム間でのファイルの移動に非常に役に立ちます。しかし、インターネットあるいは他の非トラステッド・ネットワークで FTP を使用すると、いくつかのセキュリティー・リスクにさらされることになります。このようなリスクについて理解して、セキュリティー・ポリシーにこれらのリスクを最小限に抑えるための方法を記述しておかなければなりません。

- オブジェクト権限方式では、システムで FTP を許可するときに十分な保護を提供しない可能性があります。

たとえば、オブジェクト群の共通権限は *USE であっても、今日に関しては、「メニュー・セキュリティ」を使用して、ほとんどのユーザーがそのオブジェクト群にアクセスできないようにするとします。(メニュー・セキュリティによって、ユーザーはメニュー・オプションにないものは一切実行できなくなります。) FTP ユーザーはメニューに対して何の制限もないため、システムにあるすべてのオブジェクトを読み取ることができます。このセキュリティ・リスクを制御するためのオプションを示します。

- システム上の iSeries オブジェクト・セキュリティを完全に機能させます。(言い換えれば、システムのセキュリティ・モデルを、「メニュー・セキュリティ」から「オブジェクト・セキュリティ」に変更します。) これは最良で、かつ最も安全なオプションです。
- FTP のための出口プログラムを書き、FTP を経由して転送される可能性のあるファイルへのアクセスを制限します。これらの出口プログラムは、少なくともメニュー・プログラムによって提供されるセキュリティと同等であるセキュリティを提供します。FTP アクセス制御を、さらに制限的にすることを希望している顧客も多いはずで、このオプションは FTP のみをカバーするもので、ODBC、DDM、または DRDA[®] など、他のインターフェースはカバーしません。

注: ファイルに対する *USE 権限は、ユーザーがファイルをダウンロードすることを許可します。ファイルに対する *CHANGE 権限は、ユーザーがファイルをアップロードすることを許可します。

- ハッカーは、FTP サーバーによって「サービス妨害」攻撃をしかけることで、システム上のユーザー・プロファイルを使用不可にすることができます。これは、ユーザー・プロファイルが使用できなくなるまで不正なパスワードでのログオンを繰り返すことによって行われます。このような攻撃によってサインオンの限度である 3 回目に達すると、プロファイルは使用不可になります。

このリスクを避けるためにできることに、アタックを最小化するためのセキュリティの増加と、アクセスの簡便さという問題に関するトレードオフの分析があります。FTP サーバーは通常、QMAXSIGN システム値を実行することで、ハッカーがパスワードを推測してパスワード・アタックをしかけるということを、無制限にできないようにします。使用を考慮すべきオプションを示します。

- FTP サーバーのログオン出口プログラムを使用して、FTP アクセスが許可されないように指定したあらゆるシステム・ユーザー・プロファイル、およびユーザー・プロファイルによるログオン要求を拒否します。(このような出口プログラムを使用するとき、ブロックするユーザー・プロファイルについてのサーバーのログオン出口点によって拒否されたログオン試行は、プロファイルの QMAXSIGN 回数としてカウントされません。)
- FTP サーバーのログオン出口プログラムを使用して、FTP サーバーへのアクセスが許可される特定のプロファイルからクライアント・マシンを制限します。たとえば、会計の者が FTP を許可されている場合、会計部門の IP アドレスがあるコンピューターからの FTP サーバー・アクセスについてのみユーザー・プロファイルは許可されます。
- FTP サーバーのログオン出口プログラムを使用して、すべての FTP ログオン試行についてユーザー名と IP アドレスをログに記録します。このログは定期的に検討して、パスワード試行の限度に達して使用不可になったプロファイルがあれば、IP アドレス情報によってハッカーを識別し、しかるべき手段をとります。

さらに、FTP サーバーの出口点を使用すると、ゲスト・ユーザーに対する匿名の FTP 機能を提供することができます。安全な匿名の FTP サーバーを設定するには、FTP サーバーのログオンと、FTP サーバーの要求検証の出口点の、両方の出口プログラムが必要になります。

V5R1 からは、Secure Sockets Layer (SSL) を使用して、FTP サーバーについて安全な通信セッションを提供することができます。SSL を使用すると、FTP サーバーとクライアントの間で渡される、ユーザー名やパスワードを含むすべてのデータについて機密性を維持するために、すべての FTP 伝送が暗号化されます。FTP サーバーは、クライアント認証のためのデジタル証明書の使用もサポートします。

FTP の使用法、そのリスク、および可能なセキュリティー措置の詳細については、次の資料を検討してください。

- セキュア FTP
- FTP サーバーを SSL で保護する

これらの FTP オプションに加え、ユーザーが機密以外の資料へ簡単にアクセスできるようにする、匿名 FTP の使用についても検討してください。匿名 FTP では、リモート・システム上の選ばれた情報への (パスワードを必要としない) 無保護アクセスが可能です。リモート・サイト側で、一般のアクセスに対応させる情報を決定します。その情報は、公共アクセス可能と見なされ、誰でも読み取ることができます。匿名 FTP を構成する前に、セキュリティー・リスクについて評価し、FTP サーバーを出口プログラムで保護することを検討してください。

- 匿名 FTP の構成
- FTP 出口プログラムを使用するアクセスの管理

第 7 章 伝送セキュリティ・オプション

JKL Toy company のシナリオには、2 種類のプライマリー iSeries システムがあったことを思い出してください。1 つは開発用、もう 1 つは本番用アプリケーション用でした。これらのシステムはいずれもが、主幹業務のデータとアプリケーションを扱っています。そこで、イントラネットとインターネットのアプリケーションを扱うために、周辺ネットワーク上に新規 iSeries システムを追加することに決定しました。

周辺ネットワークを確立することにより、内部ネットワークとインターネットの間を、物理的に分離できることが保証されます。このように分離することにより、内部システムがさらされるインターネット・リスクを減少させることができます。この会社では、新規の iSeries をインターネット・サーバー専用とすることにより、ネットワーク・セキュリティの管理をより簡潔なものにしています。

インターネット環境では広範囲にわたってセキュリティが必要になるため、IBM では、インターネット上で e-business を行うためのセキュア・ネットワーク環境を保証するセキュリティ・オフリングの開発を続けてきました。インターネット環境では、システム固有のセキュリティとアプリケーション固有のセキュリティの両方が行われているようにしなければなりません。ただし、社内イントラネットまたはインターネット接続によって機密情報を転送するには、より強力なセキュリティ・ソリューションを実装する必要が増大します。このようなリスクと闘うには、インターネットを流れている間にデータの伝送を保護するセキュリティ措置を実装する必要があります。

信頼性に欠けるシステムを介して情報を転送することに伴うリスクを最小限にするため、iSeries における 2 種類の伝送レベルによるセキュリティ・オフリングを利用することができます。すなわち、Secure Sockets Layer (SSL) によるセキュア通信と、VPN (仮想プライベート・ネットワーク) による接続です。

SSL によるアプリケーションの保護

Secure Sockets Layer (SSL) プロトコルは、クライアントとサーバー間での通信を保護するための業界標準です。SSL は本来、Web ブラウザー・アプリケーションのために開発されたものですが、現在では他のアプリケーションにも SSL を使用できるものが増加しています。iSeries サーバーの場合次のものが含まれます。

- IBM HTTP Server for iSeries (オリジナルと Apache による拡張版)
- FTP サーバー
- Telnet サーバー
- 分散リレーショナル・データベース・アーキテクチャー (DRDA) と分散データ管理
- (DDM) サーバー
- iSeries ナビゲーターのマネージメント・セントラル
- Directory Services Server (LDAP)
- iSeries ナビゲーターおよび一連の iSeries Access Express アプリケーション・プログラミング・インターフェース (API) に対して作成されたアプリケーションを含む、iSeries Access Express アプリケーション
- Developer Kit for Java を使用して開発されたプログラムと IBM Toolkit for Java を使用するクライアント・アプリケーション
- アプリケーションで SSL を使用可能にするために使用できる、Secure Sockets Layer (SSL) アプリケーション・プログラミング・インターフェース (API) を使用して開発したプログラム。SSL を使用するプログラムの書き方についての詳細は、「Secure Sockets Layer API」を参照してください。

これらのアプリケーションのいくつかは、クライアント認証のためのデジタル証明書の使用もサポートします。SSL では、デジタル証明書によって、通信相手の認証や、セキュア接続の確立を行っています。

iSeries VPN (仮想プライベート・ネットワーク)

iSeries の VPN 接続を使用すれば、2 エンドポイント間でのセキュア通信チャネルが確立できます。SSL 接続と同様に、エンドポイント間で転送されるデータを暗号化することで、データ機密性とデータ保全性の両方が保証されます。しかし、VPN 接続では、指定したエンドポイントへのトラフィックの流れを限定し、その接続を使用可能なトラフィックの種類を制限することができます。そのため、VPN 接続では、無許可アクセスからネットワーク・リソースを保護する手助けをすることで、ネットワーク・レベルでのセキュリティを実現します。

使用すべき方式について

どちらのセキュリティ方式でも、セキュア認証、データ機密性、およびデータ保全性の必要は考慮しています。どちらの方式を使用するかについては、いくつかの要素によって決定します。考慮すべき要素は、通信相手は誰か、通信に使用するアプリケーションは何か、通信にどの程度のセキュリティを期待するか、その通信を保護するためにコストとパフォーマンスのトレードオフをどのようにするか、などです。

さらに、SSL と共に特定のアプリケーションを使用する場合は、そのアプリケーションで SSL を使用できるようにセットアップする必要があります。多くのアプリケーションではまだ SSL を利用することはできませんが、Telnet や iSeries Access Express など、SSL 機能を追加しているアプリケーションも多数あります。一方、VPN では、特定の接続のエンドポイント間を流れるすべての IP トラフィックを保護することが可能です。

たとえば、現在 SSL 上で HTTP を使用し、ビジネス・パートナーに内部ネットワークの Web サーバーへ接続を許可しているという場合があります。Web サーバーが、自分とビジネス・パートナーの間で必要となる唯一のセキュア・アプリケーションである場合、あえて VPN 接続への切り替えは考えないでしょう。しかし、通信の拡張を考えている場合では、代わりに VPN を使用することが期待されます。また、ネットワークの一部でトラフィックを保護する必要はあっても、SSL を使用するように各クライアントとサーバーを個別に構成することは望まない、という状況もありえます。このようなネットワークの一部に対しては、ゲートウェイ間 VPN 接続を確立することができます。これにより、トラフィックは保護されますが、接続は、その両側における個々のサーバーとクライアントにとって透過的なものとなります。

SSL のためのデジタル証明書の使用

デジタル証明書は、強力な認証方法であり安全な通信に役立つ Secure Sockets Layer (SSL) を使用するための基盤を提供します。iSeries サーバーでは、OS/400 の統合化機能である デジタル証明書マネージャー (DCM) によって、デジタル証明書を容易に作成かつ管理する機能をシステムとユーザーに提供します。

さらに、IBM HTTP Server for iSeries などのアプリケーションを構成して、クライアント認証の強力な手段として、ユーザー名とパスワードの代わりにデジタル証明書を使用することができます。

デジタル証明書とは

デジタル証明書は、パスポートと同様、証明書の所有者の ID を検査するデジタル信任状です。認証局 (CA) と呼ばれる信頼できる第三者機関が、デジタル証明書をユーザーとサーバーに発行します。CA の信頼性は、有効な認証としての証明書の信頼基盤となっています。

CA ごとに、CA が認証を発行するのに必要な識別情報を決定するための方針があります。インターネット CA では、識別名のみなど、わずかな情報のみを必要としている場合があります。識別名は、CA によるデジタル証明のアドレスと、デジタル電子メールのアドレスの発行先となる個人またはサーバーの名前です。秘密鍵と公開鍵が、それぞれの認証ごとに生成されます。証明書には公開鍵が含まれ、ブラウザまたは保護ファイルには秘密鍵が含まれます。証明書の所有者は、これらの鍵を使用して、メッセージやドキュメントなどのデータに「署名」し、それを暗号化してユーザーとサーバー間で送信します。そのようなデジタル署名により、アイテムの発行元の信頼性が保証され、そのアイテムの保全性が保護されます。

多くのアプリケーションではまだ SSL を利用することはできませんが、Telnet や iSeries Access Express など、SSL 機能を追加しているアプリケーションも多くあります。iSeries アプリケーションで SSL を使用する方法については、iSeries Information Center で「SSL によるアプリケーションの保護」を参照してください。


Telnet のセキュア・アクセスのための SSL

Secure Sockets Layer (SSL) を使用して Telnet 通信セッションを保護するように、Telnet サーバーを構成することができます。SSL を使用するように Telnet サーバーを構成するには、デジタル証明書マネージャー (DCM) を使用して、使用する Telnet サーバーで証明書を構成しなくてはなりません。デフォルトで、Telnet サーバーは、セキュア接続と非セキュア接続の両方を扱います。ただし、Telnet でセキュア・セッションのみが可能となるように、Telnet を構成することが可能です。さらに、より強力なクライアント認証のためのデジタル証明書を使用するように Telnet サーバーを構成することができます。

Telnet で SSL の使用を選択することは、セキュリティ上の強力な利点があります。Telnet の場合、サーバー認証のほかに、Telnet プロトコルでのあらゆるデータ・フローに先立ち、データの暗号化が行われます。SSL セッションが確立されると、ユーザー ID とパスワード交換を含むすべての Telnet プロトコルが暗号化されます。

Telnet サーバーの使用にあたって考慮すべき最も重要な要素は、クライアント・セッションで使用する情報の機密性です。情報が重要かつ機密である場合は、SSL を使用して iSeries Telnet サーバーをセットアップすると有効です。Telnet アプリケーションについてデジタル証明書を構成する場合、Telnet サーバーは、SSL クライアントでも、非 SSL クライアントでも動作することができます。セキュリティ・ポリシーが、Telnet セッションを必ず暗号化するよう要求している場合は、すべての非 SSL Telnet セッションを使用できないようにします。SSL Telnet サーバーを使用する必要がない場合は、SSL ポートをオフにすることができます。ADDTCPPORT コマンドを使用して、ポートを使用不可にすることができます。そのポートをオフにすると、サーバーはクライアントに非 SSL Telnet を提供し、SSL Telnet セッションは使用できなくなります。

Telnet および、SSL の有無にかかわらず Telnet のためのセキュリティ・ヒントについての詳細は、以下の資料を参照してください。

- Information Center の「Telnet」トピックでは、iSeries サーバー上で Telnet を使用するために必要な情報を提供しています。
- 「iSeries セキュリティの手引き」 では、TCP/IP セクションでの Telnet セキュリティに関する詳細情報を提供しています。

セキュア iSeries Access Express のための SSL

Secure Sockets Layer (SSL) を使用して、iSeries Access Express 通信セッションを保護するように iSeries Access Express サーバーを構成することができます。たとえば、成長するにしたがって、JKL Toy company では、各地の外交販売員を多数、スタッフに加えました。これらの販売員は、各本拠地のオフィスにおける

iSeries 実動システムから、出荷可能なおもちゃ、および製造日の状況に関する情報にアクセスする必要があります。このデータは機密のため、JKL Toy では、販売員が安全な iSeries Access Express を介してのみ情報にアクセスできるようにしました。

SSL を使用すると、iSeries Access Express におけるセッションのすべてのトラフィックを暗号化することができます。これにより、データがローカル・ホストとリモート・ホスト間で転送される過程で、読み取られてしまうことを防止します。

SSL を使用した iSeries Access Express に関する詳細は、以下の資料を検討してください。

- Secure Sockets Layer 管理
- IBM Developer Kit for Java SSL
- IBM Java Toolbox SSL

セキュア専用通信のための VPN (仮想プライベート・ネットワーク)

VPN (仮想プライベート・ネットワーク) と、これによって提供されるセキュリティーの使用が普及すると同時に、JKL Toy company でも、インターネット上でデータを転送するためのオプションを模索しています。同社では、最近になってある小規模なおもちゃ製造会社を買収しており、子会社として運営していく方針です。JKL では、両社の間で情報を交換することが必要になります。両社とも iSeries サーバーを使用しており、VPN 接続を使用することで、2 つのネットワーク間の接続に必要なセキュリティーが提供されます。VPN では、従来の専用回線よりコストを削減することができます。

VPN 接続を使用すると、事業所、外回りの従業員、供給会社、ビジネス・パートナー、その他との接続を制御および保護することができます。

接続に VPN を使用するとメリットのあるユーザーの例として、以下のようなユーザーが挙げられます。

- リモートまたはモバイルのユーザー
- ホーム・オフィスから事業所までのユーザー、あるいはそれ以外のオフサイトに位置するユーザー
- 企業間 (B2B) 通信

機密性の高いシステムへのユーザー・アクセスを制限しなければ、セキュリティー・リスクが発生します。システムにアクセスできる者を制限しないと、社内情報の機密性が保たれない危険が増します。システム上の情報を共有する必要があるだけに、システムへのアクセスを許可する計画が必要になります。VPN では、認証やデータ・プライバシーなど、セキュリティー上の重要な機能を提供すると共に、ネットワーク・トラフィックを制御することも可能です。複数の VPN 接続を確立すると、各接続について誰がどのシステムにアクセスできるかを制御することが可能になります。たとえば、会計と人事は、それぞれの VPN を介してリンクします。

ユーザーにインターネットを介してシステムに接続する許可を与えると、企業の機密データを、アタックを受ける可能性のある公衆ネットワーク上に送信する可能性があります。転送データを保護するためのオプションの 1 つは、外部者からのプライバシーとセキュリティーを保証する暗号化方法と認証方法を使用することです。VPN 接続は、システム間の通信を保護するという特定のセキュリティー・ニーズにソリューションを提供します。VPN 接続では、接続の 2 つのエンドポイント間を流れるデータを保護することができます。さらに、パケット・ルール・セキュリティーを使用して、VPN 上で許可される IP パケットの種類を定義することもできます。

VPN を使用して、信頼性のある制御されたエンドポイント間を流れるトラフィックを保護するためのセキュア接続を作成することができます。それでも、VPN を使用するパートナーに対してどれだけのアクセスを提供するかについて考えておかなければなりません。VPN 接続は、公衆ネットワークを伝搬するデータ

を暗号化することができます。しかし、VPN 接続の構成方法によっては、その接続を介して通信を行う内部ネットワーク上を流れるデータを暗号化しないことがあります。したがって、各 VPN 接続のセットアップ方法については注意深く計画しなければなりません。VPN のパートナーに対しては、アクセスさせたい内部ネットワーク上のホストまたはリソースだけにアクセスを許可するようにしてください。

たとえば、在庫がある部品にはどのようなものがあるかという情報を必要としている取引先があるとしませす。この情報は、イントラネットの Web ページを更新するのに使用するデータベースにあります。この取引先に対しては、VPN 接続によって、これらのページへの直接アクセスを許可することを希望していません。ただし、データベースそれ自身のような他のシステム・リソースに、取引先をアクセスさせたくはありません。幸いにも、両エンドポイント間のトラフィックをポート 80 に制限するように、VPN 接続を構成することができます。ポート 80 は、HTTP トラフィックが使用するデフォルト・ポートです。したがって、その取引先は、この接続だけでしか HTTP 要求や応答を送受信することができません。

VPN 接続上を流れるトラフィックの種類を制限できることから、この接続ではネットワーク・レベルでのセキュリティ措置を提供します。ただし、VPN では、システムに出入りするトラフィックを規制するのに、ファイアウォールと同様の機能をすることはありません。また VPN 接続は、iSeries と他のシステムとの間の通信を保護するために利用できる唯一の手段ではありません。セキュリティのニーズ次第では、SSL を使用した方がふさわしいこともあります。

必要としているセキュリティを VPN 接続が提供してくれるかどうかは、何を保護したいかによって異なります。また、そのセキュリティを提供するために、どこまでトレードオフができるかによっても異なります。セキュリティに関して下す決定はどれもそうですが、VPN 接続がどの程度セキュリティ・ポリシーをサポートするのかを考慮しなければなりません。

第 8 章 インターネット・セキュリティ用語

インターネット・セキュリティを検討するための基礎として、まず、いくつかのインターネット用語を定義します。すでにインターネット用語に熟知している人は、このセクションをスキップすることができます。

認証 (Authentication)

認証とは、リモート・クライアントまたはサーバーが実際に名乗る通りのものであるかを検査することです。認証により、接続する相手側が信頼に足るものであることが保証されます。

クラッカー (Cracker)

悪意を持ったハッカー。

暗号 (Cryptography)

データを保護するための方法。暗号を使用すると、関係のない者が保管情報を読み取ったり、通信を傍受したりできないようにしておいて、情報を保管したり、他の相手と通信したりすることを可能にします。暗号化により、理解可能なテキストを、判読できないデータの断片 (暗号文) に変換します。暗号解除は、判読不能のデータを理解可能なテキストに復元します。いずれのプロセスも、数学公式あるいはアルゴリズムと、連続した機密データ (鍵) を使用します。

暗号には、次の 2 つの種類があります。

- 共用/秘密鍵 (対称) 暗号では、1 つの鍵が通信する 2 者で共用する秘密鍵です。暗号化と暗号解除は、いずれも同じ鍵を使用します。
- 公開鍵 (非対称) 暗号では、暗号化と暗号解除ではそれぞれ別の鍵を使用します。一方の通信者は公開鍵と秘密鍵を持っています。これら 2 つの鍵は数学的に関係していますが、公開鍵から秘密鍵を取り出すのは実際上は不可能です。誰かの公開鍵で暗号化されたメッセージは、それに関連付けられた秘密鍵でないと暗号解除できません。あるいは、サーバーまたはユーザーが秘密鍵を使用して文書に「署名」し、公開鍵を使用してデジタル署名を暗号解除します。これによって文書のソースを検証します。

デジタル証明書 (Digital certificate)

デジタル証明書は、パスポートと同様、証明書の所有者の ID を検査するデジタル文書です。認証局 (CA) と呼ばれる信頼できる者が、デジタル証明書をユーザーとサーバーに発行します。CA の信頼性は、有効な認証としての証明書の信頼基盤となっています。以下の用途に使用することができます。

- 識別 - ユーザーが誰であるか。
- 認証 - ユーザーが、当の本人であることを保証します。
- 保水性 - 送信者のデジタル「署名」を検査して、文書の内容が変更されたかどうかを判断します。
- 非拒否 - ユーザーが何らかのアクションを実行していないと主張できないことを保証します。たとえば、ユーザーは、クレジット・カードを使用した電子購買を許可したことに異を唱えられません。

デジタル署名 (Digital signature)

電子文書のデジタル署名は、手書きの文書の署名と等価です。デジタル署名は、文書の出所を証明するものです。証明書の所有者は、その証明書に関連付けられた秘密鍵を使用して文書に「署名」します。その文書の受信側は、対応する公開鍵を使用して署名の暗号解除を行い、送信者がその文書のソースであることを検証します。

デジタル証明書マネージャー (Digital certificate manager) (DCM)

デジタル証明書マネージャーは、OS/400 がローカルの認証局 (CA) となることを許可します。DCM を使用して、サーバーやユーザーが使用するデジタル証明書を作成することができます。他の CA が発行するデジタル証明書をインポートすることも可能です。また、デジタル証明書を OS/400 ユーザー・プロファイルと関連付けることもできます。DCM を使用すると、安全な通信のための Secure Sockets Layer (SSL) を使用するようにアプリケーションを構成することができます。

識別名 (Distinguished name)

識別名は、認証局 (CA) によるデジタル証明書の発行先の個人またはサーバーの名前です。証明書は、証明書の所有権を示すためにこの名を提供します。証明書を発行する CA の方針によっては、識別名に他の許可情報を組み込むことができます。

ドメイン・ネーム・サーバー (Domain name server) (DNS)

インターネット名を IP アドレスに変換するインターネット・ホスト。多くの場合、この変換は、インターネットの他の DNS と対話することによって行われます。たとえば、多くの DNS サーバーでは、

vnet.ibm.com

を識別できます。しかし、おそらく次の完全な IP アドレスを識別できる DNS はほんのわずかしかなかったりません。

system1.vnet.ibm.com

インターネットに接続すると、インターネット・クライアントはドメイン・ネーム・サーバーを使用して、通信する相手のホスト・システムの IP アドレスを決定します。

暗号化 (Encryption)

暗号化は、正しい暗号解除の方法を知らない者にとっては読むことのできない形式にデータを変換します。許可されていない者でも情報を代行受信することは可能です。ただし、正しい暗号解除の方法を知らないと、その情報は理解不能です。

エクストラネット (Extranet)

企業ファイアウォールの外部に配置された複数の協同部門の私用ビジネス・ネットワーク。エクストラネット・サービスは、標準サーバー、電子メール・クライアント、および Web ブラウザーなど、既存のインターネットのインフラストラクチャーを使用します。このためエクストラネットは、所有権を主張できるネットワークを作成・保守する場合よりも費用が少なく済みます。エクストラネットの場合は、共通の利害を持つ取引先、サービス提供元、および顧客は、この拡張インターネットを使用して、緊密なビジネス関係と強力な通信結合を形成することができます。

ファイアウォール (Firewall)

内部ネットワークと外部ネットワーク (たとえば、インターネット) の間の論理バリア。ファイアウォールは、1 つ以上のハードウェアおよびソフトウェア・システムから構成されます。ファイアウォールは、安全なシステム (信頼性のあるシステム) と安全でないシステム (信頼性に欠けるシステム) との間の情報のアクセスと流れを制御します。

ハッカー (Hacker)

導入先のシステムに割り込もうとする無許可の人。

ハイパーテキスト・リンク (Hypertext Links)

ある情報 (ハイパーテキスト・ノードと呼ばれる) と他の情報との間を接続 (ハイパーテキスト・リンクと呼ばれる) して、それをオンラインで提示する方法。

ハイパーテキスト・マークアップ言語 (Hypertext markup language) (HTML)

ハイパーテキスト文書を定義するための言語。HTML を使用すると、文書の体裁 (強調表示および書体、など) を示したり、他の文書あるいはオブジェクトへのリンクを示すことができます。

ハイパーテキスト転送プロトコル (Hypertext transport protocol) (HTTP)

ハイパーテキスト文書にアクセスするための標準の方式。

インターネット (Internet)

相互に接続された世界的規模の『ネットワークのネットワーク』。そして、この「ネットワークのネットワーク」に接続されているコンピューターの相互通信を可能にする、協調関係にある一連のアプリケーション。インターネットは、ブラウズ可能な情報、ファイル転送、リモート・ログイン、電子メール、ニュース、その他のサービスを提供します。インターネットは、『ネット』と呼ばれることもあります。

インターネット・クライアント (Internet client)

インターネットを使用して、インターネット・サーバー・プログラムに要求を出したり、インターネット・サーバー・プログラムから結果を受け取ったりするプログラム (またはユーザー)。複数の異なるクライアント・プログラムが用意されており、これを使用して、それぞれ異なるタイプのインターネット・サービスを要求することができます。Web ブラウザーは、クライアント・プログラムの 1 つのタイプです。ファイル転送プロトコル (FTP) はまた別のタイプのクライアント・プログラムです。

インターネット・ホスト (Internet host)

インターネットまたはイントラネットに接続されているコンピューター。インターネット・ホストは、複数のインターネット・サーバー・プログラムを実行することがあります。たとえば、インターネット・ホストは、FTP サーバーを実行して、FTP クライアント・アプリケーションからの要求に応答することがあります。同一のホストで HTTP サーバーを実行して、Web ブラウザーを使用したクライアントからの要求に応答することがあります。サーバー・プログラムは、通常、ホスト・システムのバックグラウンドで (バッチで) 実行されます。

インターネット鍵交換 (Internet key exchange) (IKE)

IKE プロトコルは、IPSec と一緒に使用され、暗号鍵の自動生成と更新だけでなく、セキュリティ関連の自動折衝もサポートします。一般に、IKE は VPN (仮想プライベート・ネットワーク) の一部として使用されます。

インターネット名 (Internet name)

IP アドレスの別名。IP アドレスは、10.5.100.75 のように、長い数字形式をしており、覚えるのが面倒です。この IP アドレスをインターネット名に割り当てることができます。たとえば、次のとおりです。

system1.vnet.ibm.com

インターネット名は、完全修飾ドメイン・ネームとも呼ばれます。「弊社のホーム・ページをご覧ください」といった広告では、ホーム・ページ・アドレスには、IP アドレスではなく、インターネット名が記載されています。これは、インターネット名の方が覚えやすいからです。

完全修飾ドメイン・ネームはいくつかの部分からなります。たとえば、

system1.vnet.ibm.com

は、以下の部分で構成されています。

com: すべての商用ネットワーク。ドメイン・ネームのこの部分は、インターネット 関係機関 (外部組織) によって割り当てられます。異なる種類のネットワークには異なる文字が割り当てられます (たとえば、商用の場合は com、教育機関の場合は edu)。

ibm: 組織のための ID。ドメイン・ネームのこの部分も、インターネット関係機関によって割り当てられ、しかもそれは固有です。次の ID は世界で 1 つの組織しか持つことができません。

ibm.com

vnet: 次のコード内のシステムのグループ分けの 1 つ。

ibm.com

この ID は、内部的に割り当てられます。ibm.com の管理者は、1 つ以上のグループ分けを作成することができます。

system1:

vnet.ibm.com グループ内の 1 つのインターネット・ホストの名前。

インターネット・サーバー (Internet server)

インターネットを介して対応するクライアント・プログラムからの要求を受け入れ、インターネットを介してこれらのクライアントに回答するプログラム (または一組のプログラム)。インターネット・サーバーは、インターネット・クライアントがアクセスできるサイトと考えることができます。複数の異なるサーバー・プログラムが、次のようなそれぞれ異なるサービスをサポートしています。

- ブラウズ (『ホーム・ページ』、および他の文書やオブジェクトとのリンク)。
- ファイル転送。たとえば、クライアントは、サーバーから自分あてにファイルを転送するように要求することができます。このファイルとしては、ソフトウェア更新、製品リスト、文書などがあります。
- エレクトロニック・コマース (電子商取引)。たとえば、情報の要求や製品のオーダーなど。

インターネット・サービス・プロバイダー (Internet service provider) (ISP)

ローカルの電話会社がユーザーを世界的規模の電話ネットワークに接続するのと同じような方法で、ユーザーをインターネットに接続する組織。

イントラネット (Intranet)

部門内部のネットワークで、Web ブラウザーや FTP などのインターネット・ツールを使用します。

IP アドレス (IP address)

インターネット・プロトコル (IP) アドレスは、TCP/IP ネットワーク上でユーザーを認識させる方法です (インターネットは、非常に大きな TCP/IP ネットワークです)。インターネット・サーバーは、通常、割り当て済みの固有な IP アドレスを持っています。インターネット・クライアントは、ISP によって割り振られた、一時的ではあっても固有な IP アドレスを使用することがあります。

IP データグラム (IP datagram)

TCP/IP ネットワークを介して送信される情報の単位。IP データグラム (パケットとも呼ばれる) には、データと、起点と宛先の IP アドレスなどのヘッダー情報が含まれています。

IP フィルター (IP filters)

IP フィルター操作は、ファイアウォールのための基本的な保護機構です。IP フィルター操作により、どのようなトラフィックが IP セッション詳細に基づいてフィルターを通ったのかを決定することができます。これにより、高度でないテクニック (たとえば、セキュア・サーバーのスキャン)、あるいはきわめて高度なテクニック (たとえば、IP アドレスのスプーフィング) を使う外部者からも、安全なネットワークを保護します。このフィルター操作機能は、他のツールを構成するための基盤と考えてください。これは、他のツールが動作するときのインフラストラクチャーであり、きわめて大胆なクラッカーを除くあらゆるアクセスを拒否します。

IPSec IP レイヤーにおける安全なパケット交換をサポートする一組のプロトコル。IPSec は、iSeries とその他の多くのシステムが、VPN を実現するために使用する標準のセットです。

IP スプーフィング (IP spoofing)

通常は信頼するシステム (IP アドレス) になりすまして、インストール・システムにアクセスしようとする。この侵入志望者は、信頼する IP アドレスを使用してシステムをセットアップします。ルーター製造業者は、システムに保護機能を組み込んで、スプーフィングの試みを検出し拒否しようとしています。

ネットワーク・アドレス変換 (Network address translation) (NAT)

Proxy サーバーおよび SOCKS サーバーに代わる、より透過性のあるサーバーを提供します。また、NAT は、非互換のアドレッシング構造を接続できるようにすることで、ネットワーク構造を簡単にします。NAT には、2 つの主要機能があります。NAT は、内部ネットワーク内から操作する公衆 Web サーバーを保護することができます。NAT では、サーバーの「真の」アドレスを公開するアドレスの背後に隠蔽することにより、この保護機能を提供します。また、内部ユーザーが、内部の私有 IP アドレスを隠蔽しながら、インターネットにアクセスできる機構を提供します。NAT は、内部ユーザーにインターネット・サービスへのアクセスを許可する場合に保護機能を提供します。それは、内部ユーザーの私有アドレスを隠蔽することができるからです。

非拒否 (Non-repudiation)

非拒否は、トランザクションが発生したこと、あるいはメッセージを送信または受信したことを証明するものです。トランザクション、メッセージ、およびドキュメントに「署名」するためのデジタル証明書と公開鍵暗号では、非拒否をサポートしています。

パケット (Packet)

イーサネット、トークンリング、フレーム・リレーなど、回線プロトコルに関する情報が含まれているデータグラム。

プロキシ (Proxy)

Proxy サーバーは、内部の安全なネットワークのクライアントと、非トラステッド・ネットワーク上のサーバーとの間で、要求と応答の再送信を行う TCP/IP アプリケーションです。Proxy サーバーは、TCP/IP 接続を切断し、内部ネットワーク情報 (たとえば、内部の IP アドレス) を隠蔽します。ネットワーク外部のホストは、Proxy サーバーを通信のソースと見なします。

公開鍵インフラストラクチャー (Public key infrastructure) (PKI)

デジタル証明のシステムで、CA およびインターネット・トランザクションに関係する各者の妥当性を検査および認証するその他の登録局。

Secure Sockets Layer (SSL)

Netscape 社が考案した Secure Sockets Layer (SSL) は、クライアントとサーバー間のセッションの暗号化のための事実上の業界標準になっています。SSL は、対称鍵の暗号化を使用し、サーバーとクライアント (ユーザー) の間のセッションを暗号化します。クライアントとサーバーは、デジタル証明書の交換中に、このセッションを折衝します。クライアントとサーバーの各 SSL セッションごとに、別の鍵が作成されます。したがって、未承認のユーザーがセッション鍵を代行受信して暗号を解除しても (その可能性は低いとはいえ)、それを使用して現在、未来、または過去の SSL セッションを盗聴することはできません。

盗聴 (Sniffing)

電子電送をモニターしたり盗聴したりすること。インターネットで送信される情報は、多くのルーターを通過して宛先に到達します。ルーター製造業者、ISP、オペレーティング・システム開発者などは、盗聴がインターネット・バックボーンで行われないようにするために日夜努力を重ねてきました。盗聴が成功するケースは、急速に減少しています。ほとんどの盗聴は、インターネット・バ

ックボーンそれ自体ではなく、インターネットに接続された私用 LAN で発生しています。しかし、ほとんどの TCP/IP 伝送は暗号化されていないので、盗聴の可能性を忘れてはなりません。

SOCKS

SOCKS は、TCP/IP トラフィックを安全なゲートウェイを介して転送する、クライアント / サーバー・アーキテクチャーです。SOCKS サーバーは、Proxy サーバーと共通するサービスの多くを実行します。

スプーフィング (Spoofing)

アタッカーが信頼性のあるシステムになりすまして、機密情報を送信するように要求すること。

TCP/IP

インターネットで使用される主要通信プロトコル。TCP/IP は、Transmission Control Protocol/Internet Protocol (伝送制御プロトコル / インターネット・プロトコル) の略称です。内部ネットワークでも、TCP/IP を使用することができます。

トロイの木馬 (Trojan horse)

トロイの木馬は、役に立つ無害な機能を実行するかのようには装ったコンピューター・プログラムです。実際はその中に、プログラムが開始されるとユーザーに割り当てられた正当な許可を使用する、隠蔽された機能を含んでいます。たとえば、コンピューターから内部の許可情報をコピーし、それをトロイの木馬の送信元に送り返したりします。

VPN (仮想プライベート・ネットワーク) (Virtual private network)

企業の専用イントラネットを拡張したもの。インターネットのような公衆ネットワークでこれを使用すると、基本的に専用「トンネル」を介して安全な専用接続を確立することができます。VPN は、他のユーザーと自分のシステムを接続しているインターネットを介して、情報を安全に送信します。この仮想プライベート・ネットワークには以下のものが含まれます。

- リモート・ユーザー
- 事業所
- ビジネス・パートナーとサービス提供元

Web ブラウザー (Web browser)

HTTP クライアント・アプリケーション。Web ブラウザーは、HTML を解釈して、ユーザーにハイパーテキスト文書を表示します。ユーザーは、現行文書のある区域をクリック (選択) して、ハイパーリンク・オブジェクトにアクセスすることができます。この区域は、しばしば**ホット・スポット**と呼ばれます。Internet Explorer および Netscape Navigator が Web ブラウザーの例です。

ワールド・ワイド・ウェブ (World Wide Web) (WWW)

文書作成のための標準形式 (HTML) と文書アクセスのための標準形式 (HTTP) を使用する、サーバーやクライアントを網目のように相互に接続したもの。サーバーからサーバーへ、また文書から文書へこのようにリンクした網目は、クモの巣にたとえて **Web** と呼ばれます。

第 2 部 付録

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

- | IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

- | IBM Corporation
- | Software Interoperability Coordinator, Department 49XA
- | 3605 Highway 52 N
- | Rochester, MN 55901
- | U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

- | 本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム
- | 契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項
- | に基づいて、IBM より提供されます。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

以下は、IBM Corporation の商標です。

Application System/400
AS/400
DRDA
e(logo) server
IBM
iSeries
Operating System/400
OS/400WebSphere

- | Lotus, Freelance, Notes および WordPro は、IBM Corporation の商標です。

Java およびすべての Java 関連の商標は、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。

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

資料に関するご使用条件

- | お客様がダウンロードされる資料につきましては、以下の条件にお客様が同意されることを条件にその使用
- | が認められます。
- | **個人使用:** これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業
- | 的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これら
- | の資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映
- | を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれるデータ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態を提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

これらの資料の著作権はすべて、IBM Corporation に帰属しています。

お客様が、このサイトから資料をダウンロードまたは印刷することにより、これらの条件に同意されたものとさせていただきます。



Printed in Japan