System i

セキュリティー
System i とインターネット・セキュリティー

バージョン 6 リリース 1

System i

セキュリティー
System i とインターネット・セキュリティー

バージョン 6 リリース 1

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、 33 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 i5/OS (プロダクト番号 5761-SS1) のバージョン 6、リリース 1、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。

IBM 発行のマニュアルに関する情報のページ

http://www.ibm.com/jp/manuals/

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(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： System i
Security
System i and Internet security
Version 6 Release 1

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 2008.2

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

目次

System i とインターネット・セキュリティー

ローカル・エリア・ネットワーク (LAN) からインターネットにアクセスする場合は、セキュリティー要件の再検討が必要になります。

IBM® System i™ 製品の統合ソフトウェア・ソリューションとセキュリティー・アーキテクチャーにより、潜在的なインターネット・セキュリティー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できます。これらのセキュリティー・オファリングを使用することで、顧客、従業員、およびビジネス・パートナーは、機密保護された環境で必要な情報を入手することができます。

ここでは、既知のセキュリティーの脅威について、およびそのリスクがご使用のインターネットおよび e-business の目標とどう関わるかについて説明します。また、リスクと、それらのリスクに対処するためにシステムに用意されている各種セキュリティー・オプションを使用するメリットを比較検討する方法も説明します。ここでの情報をどう活用すればビジネスのニーズに合ったネットワーク・セキュリティー計画を策定できるかを判断することができます。

System i とインターネット・セキュリティーの PDF ファイル

この情報の PDF ファイルを表示および印刷することができます。

この文書の PDF 版を表示またはダウンロードするには、「System i とインターネット・セキュリティー」を選択します。

以下に示す関連トピックを表示したり、ダウンロードすることができます。

- 侵入検出。侵入検知ポリシーを作成して、不正に作成された IP パケットなど、TCP/IP ネットワークを介して着信した疑わしい侵入イベントを監査することができます。また、TCP/IP 侵入が進行している可能性がある場合に、監査データを分析したり、セキュリティー管理者に報告するアプリケーションを作成することもできます。
- EIM (エンタープライズ識別マッピング。EIM (エンタープライズ識別マッピング) は、エンタープライズ全体のさまざまなユーザー・レジストリー内で、ユーザーまたはエンティティー (サービスなど) を適切なユーザー ID にマッピングするためのメカニズムです。
- シングル・サインオン。シングル・サインオン・ソリューションは、ユーザーが実行する必要があるサインオン数、およびユーザーが複数のアプリケーションやシステムにアクセスするために必要なパスワード数を削減します。
- システム・セキュリティーの計画とセットアップ。「システム・セキュリティーの計画とセットアップ」では、システム・レベルのセキュリティーを効果的かつ体系的に計画および構成する方法を説明します。

PDF ファイルの保存

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. ご使用のブラウザーで PDF のリンクを右クリックする。
2. ローカルに PDF を保存するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「**保存**」をクリックする。

Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、Adobe® Reader がシステムにインストールされている必要があります。Adobe Reader は、 Adobe の Web サイト (www.adobe.com/products/acrobat/readstep.html) から無償でダウンロードすることができます。

関連概念

侵入検知

EIM (エンタープライズ識別マッピング)

シングル・サインオン

システム・セキュリティーの計画とセットアップ

System i とインターネット・セキュリティー上の考慮事項

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。ここでは、i5/OS® のセキュリティーの強さとセキュリティー・オファリングの概要を説明します。

System i プラットフォームをインターネットに接続する場合、 1 つ目の質問は一般に、「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か」です。このトピックを学習すれば、この質問の答えを知ることができます。

知っておかなければならないことは、インターネットの使い方によって異なります。インターネットを使用する一番の目的は、内部ネットワークのユーザーが Web にアクセスしたり、インターネット電子メールを利用したりできるようにすることかもしれません。また、サイト間で機密情報を転送する機能を必要としていることもあります。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。

注: セキュリティーおよびインターネット関連の用語について詳しく知らない場合は、必要に応じて、共通の「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かということや、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。

i5/OS のセキュリティー特性

インターネット上のシステムを保護するための多数の特定のセキュリティー・オファリングの他に、 i5/OS オペレーティング・システムには次のようなセキュリティー特性も備わっています。

- 統合セキュリティー。他のシステムに導入されているアドオンのセキュリティー・ソフトウェア・パッケージと比べて、抜け道を見つけることが非常に難しくなります。
- オブジェクト・ベースのアーキテクチャー。ウィルスの作成と伝搬が技術的に難しくなります。 i5/OS オペレーティング・システムでは、ファイルをプログラムのように見せたり、プログラムから別のプログラムを変更したりすることはできません。 i5/OS 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。オフセットを取ってそれをポインターにする、つま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。 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。

i5/OS 拡張セキュリティー・オファリング

i5/OS オペレーティング・システムには、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場合に選択することができる、特定のセキュリティー・オファリングもいくつか用意されています。インターネットの利用方法によりますが、以下の諸機能を利用することができます。

- 仮想プライベート・ネットワーク (VPN) は、企業の専用イントラネットを、インターネットなどの公衆ネットワークに拡張したものです。 VPN では、基本的にはプライベートのトンネルを公衆ネットワーク上に作成することによって、安全なプライベート接続を確立することができます。 VPN は、i5/OS オペレーティング・システムの統合機能で、 System i ナビゲーター インターフェースから使用することができます。
- パケット・ルールも、i5/OS オペレーティング・システムの統合機能で、 System i ナビゲーター インターフェースから使用することができます。この機能を使用して 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、システムとの間の TCP/IP 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) プロトコルでは、 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 i5/OS、 System i Access for Windows®、ファイル転送プロトコル (FTP)、Telnet など、現在では多くのアプリケーションが SSL に対応しています。

関連概念

7 ページの『セキュリティー・ポリシーと目的』
セキュリティー・ポリシーでは、保護する必要があるものを定義し、 セキュリティーの目的では、ユーザーに期待することを表します。

29 ページの『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)』
仮想プライベート・ネットワーク (VPN) は、 社内のイントラネットを公衆ネットワークまたはプライベート・ネットワークのいずれかの既存のフレームワークに拡張するもので、 組織内の通信を公開せず機密を保護することを支援します。

9 ページの『シナリオ: JKL Toy Company の e-business 計画』
独自の e-business 計画を策定するときに役立つ、 JKL Toy Company の一般的なシナリオを取り上げます。 この会社は、インターネットを使用してビジネス対象を拡張することを決定しました。

関連情報

インターネット接続

eServer Security Planner

IP フィルター操作とネットワーク・アドレス変換

Secure Sockets Layer

AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet

インターネット・セキュリティーの計画

インターネット使用計画を策定するときは、インターネット・セキュリティーのニーズを考慮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。収集した情報に基づいて、セキュリティーのニーズを正確に評価することができます。

例えば、次の情報を文書化して記述する必要があります。

- 現在のネットワーク構成。
- ドメイン・ネーム・システム (DNS) および電子メール・サーバーの構成情報。
- インターネット・サービス・プロバイダー (ISP) への接続。
- インターネットから使用するサービス。
- インターネット・ユーザーに提供するサービス。

セキュリティー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ー・リスクを最小限に抑えるのに必要なセキュリティー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。

例えば、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するとします。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、機密データがインターネット上を保護されていない状態で流れることに注意しなければなりません。もし競合他社がこのデータを入手して、それを利用すれば、会社は財政危機に陥るかもしれません。使用目的 (Telnet) とそれに伴うリスク (機密情報の露出) を特定することで、この用途でデータ機密性を確保するために適用すべき追加のセキュリティー措置 (Secure Sockets Layer (SSL) 対応など) を決定することができます。

セキュリティー対策の階層的アプローチ

セキュリティー・ポリシーでは、保護する必要があるもの、およびシステム・ユーザーに期待することを定義します。

セキュリティー・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、セキュリティー計画の基盤を提供します。セキュリティー・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ー・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。 i5/OS オペレーティング・システム固有のセキュリティー機能を適切に構成すれば、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、システム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ー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。セキュリティー・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、セキュリティーはより難しくなります。通信チャ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脆弱であるかは、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ー・リスクを理解しておけば、セキュリティー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ーに脅威を与えるさまざまな人たちの根城になります。次のリストに、発生する可能性のある代表的なセキュリティー・リスクを示します。

- **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、ネットワークのトラフィックを監視します。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、インターネットを経由して送信した内容は、すべて第三者によって傍受される可能性があると考えておく必要があります。

- **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もの種類があります。

  - **システム・アクセス試行**では、アタッカーはセキュリティーの抜け穴を探し、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、特殊なツールを使用して、暗号化されたデータの暗号化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ー・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ー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場合、侵入試行やサービス妨害アタックが発生することは珍しいことではありません。むしろ、セキュリティーの問題が発生するのは当然であると考えるべきです。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ほかなりません。インターネット・セキュリティー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。

セキュリティー戦略では、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できる措置を講じることが必要です。通常は、最も基本的なレベル (システム・レベル・セキュリティー) から最も複雑なレベル (トランザクション・レベル・セキュリティー) までのセキュリティー計画を策定する必要があります。

システム・レベル・セキュリティー
: システム・セキュリティーの措置は、インターネットの基本セキュリティー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・セキュリティー戦略全般における第一歩とは、基本的なシステム・セキュリティーを適切に構成することにほかなりません。

ネットワーク・レベル・セキュリティー
: ネットワーク・セキュリティーの措置では、 i5/OS オペレーティング・システムおよびその他のネットワーク・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・セキュリティーの措置を講じて、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・セキュリティー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・セキュリティー計画で重要な要素を提供することができます。ネットワーク・セキュリティー計画では、ISP ルーター接続でのフィルタリング規則やパブリック DNS 対策など、 ISP が提供するセキュリティー措置の概要を記述することが必要です。

アプリケーション・レベル・セキュリティー

アプリケーション・レベル・セキュリティーの措置では、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、セキュリティー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、セキュリティー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。使用するセキュリティーの措置には、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盛り込む必要があります。

伝送レベル・セキュリティー

伝送レベル・セキュリティーの措置は、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システム間を伝達されていきます。アプリケーションが Secure Sockets Layer (SSL) を使用するように構成するなどのセキュリティー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・セキュリティーの措置によって、他のセキュリティー・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ー・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ー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ー・セーフティー・ネットを構築します。

関連概念

11 ページの『基本的なインターネット準備のためのセキュリティーのレベル』
インターネットに接続する前に、 システムを保護するために必要なセキュリティー・レベルを決定しなければなりません。

12 ページの『ネットワーク・セキュリティー・オプション』
内部リソースを保護するには、適切なネットワーク・レベルのセキュリティー措置を選択します。

19 ページの『アプリケーション・セキュリティー・オプション』
よく使用される数多くのインターネット・アプリケーションやインターネット・サービスに対するセキュリティー・リスクを管理するオプションを使用することができます。

26 ページの『伝送セキュリティー・オプション』
データがインターネットなどの非トラステッド・ネットワーク上を流れるときにそのデータを保護するには、 適切なセキュリティー措置を実施する必要があります。 これらの措置には、Secure Sockets Layer (SSL)、System i Access for Windows、仮想プライベート・ネットワーク (VPN) 接続などが含まれます。

7 ページの『セキュリティー・ポリシーと目的』
セキュリティー・ポリシーでは、保護する必要があるものを定義し、 セキュリティーの目的では、ユーザーに期待することを表します。

22 ページの『電子メール・セキュリティー』
インターネットまたは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、 システムがファイアウォール下で保護されていても、システムはセキュリティー・リスクにさらされます。

関連資料

セキュリティー・ポリシーと目的

セキュリティー・ポリシーでは、保護する必要があるものを定義し、セキュリティーの目的では、ユーザーに期待することを表します。

セキュリティー・ポリシー

インターネット・サービスを使用または提供するたびに、システムと、システムが接続されているネットワークがリスクにさらされます。セキュリティー・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ー、人的セキュリティー、管理セキュリティー、およびネットワーク・セキュリティーなどの領域にわたります。

セキュリティー・ポリシーでは、保護する必要があるもの、およびシステム・ユーザーに期待することを定義します。セキュリティー・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、セキュリティー計画の基盤を提供します。セキュリティー・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。セキュリティー・ポリシーには、セキュリティー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。

セキュリティー・ポリシーを開発するには、セキュリティーの目的を明確に定義しなければなりません。セキュリティー・ポリシーを策定したら、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、セキュリティー・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可能性がある新しいリスクに対処するためです。

セキュリティーの目的

セキュリティー・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。セキュリティーの目的は、次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
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、 System i 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、セキュリティー・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 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ー・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。ディジタル証明書では、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ー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 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。

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

- **データ保全性**: 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。データ保全性により、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ー・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、データ保全性を保証するセキュリティー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ー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 (否認防止)。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。i5/OS オペレーティング・システムの場合、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ー要素です。それは、システムの保全性が、i5/OS アーキテクチャーの基本的な部分だからです。例えば、セキュリティー・レベルを 40 または 50 にしていると、i5/OS アーキテクチャーは、ハッカーにとって、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。

否認防止
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は、否認防止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。データ上のディジタル署名が、必要な証明を提供します。

機密性 機密情報がプライベートのままで、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・セキュリティーにとって重要です。非トラステッド・ネットワークでデータを転送する場合は、デジタル証明書と Secure Sockets Layer (SSL) によるデータの暗号化、または仮想プライベート・ネットワーク (VPN) 接続によって機密性を確保することができます。セキュリティー・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。

セキュリティー活動の監査
セキュリティー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、セキュリティーを破ろうとしたか、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いることを知らせます。

関連概念

2 ページの『System i とインターネット・セキュリティー上の考慮事項』
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。 ここでは、i5/OS のセキュリティーの強さとセキュリティー・オファリングの概要を説明します。

4 ページの『セキュリティー対策の階層的アプローチ』
セキュリティー・ポリシーでは、保護する必要があるもの、 およびシステム・ユーザーに期待することを定義します。

DCM の構成

Secure Socket Layer (SSL)

『シナリオ: JKL Toy Company の e-business 計画』
独自の e-business 計画を策定するときに役立つ、 JKL Toy Company の一般的なシナリオを取り上げます。 この会社は、インターネットを使用してビジネス対象を拡張することを決定しました。

シナリオ: JKL Toy Company の e-business 計画

独自の e-business 計画を策定するときに役立つ、 JKL Toy Company の一般的なシナリオを取り上げます。この会社は、インターネットを使用してビジネス対象を拡張することを決定しました。

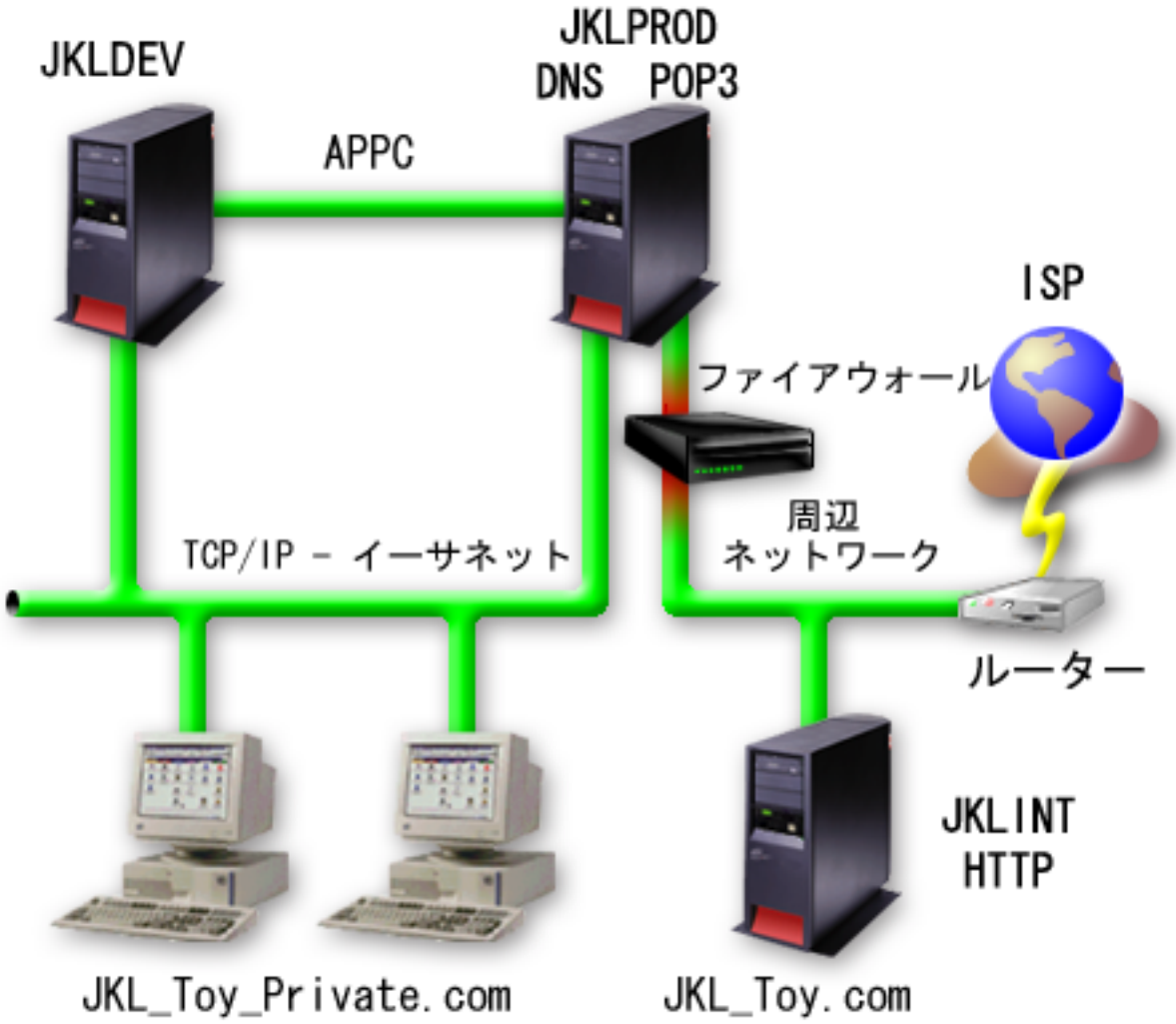
JKL Toy Company は、大手ではありませんが、急成長しているおもちゃ製造会社です。この会社の社長の関心事は、ビジネスの成長と、その成長に伴う負荷を新規に導入した i5/OS オペレーティング・システムがいかに軽減してくれるかということです。会計マネージャーの Sharon Jones は、システム管理とシステム・セキュリティーを任されています。

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ー・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買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、システム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。次の図に、この会社のインターネットまたはネットワーク構成を示します。



図に示すように、JKL Toy company には、2 つの主要なシステムが存在します。 1 つは開発アプリケーション用のシステム (JKLDEV)、もう 1 つは実動アプリケーション用のシステム (JKLPROD) 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、これらのアプリケーション用の新しいシステム (JKLINT) を追加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。また、新規システムをインターネット・サーバー専用として指定することで、ネットワーク・セキュリティー管理の簡易化も実現されます。

この段階では、新規のシステム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公衆 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・フィルター操作規則と、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。

関連概念

7 ページの『セキュリティー・ポリシーと目的』
セキュリティー・ポリシーでは、保護する必要があるものを定義し、 セキュリティーの目的では、ユーザーに期待することを表します。

2 ページの『System i とインターネット・セキュリティー上の考慮事項』
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。 ここでは、i5/OS のセキュリティーの強さとセキュリティー・オファリングの概要を説明します。

12 ページの『ネットワーク・セキュリティー・オプション』
内部リソースを保護するには、適切なネットワーク・レベルのセキュリティー措置を選択します。

26 ページの『伝送セキュリティー・オプション』
データがインターネットなどの非トラステッド・ネットワーク上を流れるときにそのデータを保護するには、 適切なセキュリティー措置を実施する必要があります。 これらの措置には、Secure Sockets Layer (SSL)、System i Access for Windows、仮想プライベート・ネットワーク (VPN) 接続などが含まれます。

基本的なインターネット準備のためのセキュリティーのレベル

インターネットに接続する前に、システムを保護するために必要なセキュリティー・レベルを決定しなければなりません。

システム・セキュリティーの措置は、インターネットの基本セキュリティー問題に対する最終防御ラインを表します。インターネット・セキュリティー戦略全般における第一歩とは、 i5/OS の基本セキュリティー設定を適切に構成することにあります。 システム・セキュリティーが最小必要条件を確実に満たすようにするには、次のタスクを実行します。

- セキュリティー・レベル (QSECURITY システム値) を 50 に設定します。セキュリティー・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リスクの高い環境でシステムを保護するには、レベル 50 をお勧めします。

  注: 現在セキュリティー・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ー・レベルに変更する場合は、事前に「System i 機密保護解説書」を参照してください。
- セキュリティー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。 System i ナビゲーターのセキュリティー・ウィザードを使用し、推奨されるセキュリティー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。

システム・セキュリティーの最小要件を構成する際には、 eServer Security Planner またはセキュリティー・ウィザード (System i 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、セキュリティー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・セキュリティーの設定を構成することができます。 Security Planner と異なり、ウィザードでは、この推奨設定を基にしてシステム・セキュリティー設定が自動的に構成されます。

i5/OS 固有のセキュリティー機能を適切に構成して管理すれば、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、システム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ー措置をさらに講じる必要があります。一般的なシステム・セキュリティーが問題なく機能することが確認できたら、インターネットを使用する場合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ことができます。

関連概念

4 ページの『セキュリティー対策の階層的アプローチ』
セキュリティー・ポリシーでは、保護する必要があるもの、 およびシステム・ユーザーに期待することを定義します。

関連資料

セキュリティー・レベルのシステム値

セキュリティー機密保護解説書

ネットワーク・セキュリティー・オプション

内部リソースを保護するには、適切なネットワーク・レベルのセキュリティー措置を選択します。

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・レベルで有効にするセキュリティー措置も含め、セキュリティー・ポリシーに包括的なセキュリティー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・セキュリティー措置を展開するには、最良の方法の 1 つです。

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・セキュリティー計画で重要な要素を提供することができます。ネットワーク・セキュリティー計画では、ISP ルーター接続でのフィルタリング規則やパブリック DNS 対策など、 ISP が提供するセキュリティー措置の概要を記述することが必要です。

ファイアウォールは確かに、総合セキュリティー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ー・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ー措置を講じる必要があります。

システム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、必ず中心的な防御ラインとしてファイアウォール製品を使用することを検討してください。 IBM Firewall for the i5/OS 製品の販売は中止され、この製品のサポートはもう提供されていませんが、これ以外にも使用できる製品は数多くあります。

商用ファイアウォール製品はネットワーク・セキュリティー・テクノロジーの全域をカバーしているので、JKL Toy Company はネットワークを保護するためにそのうちの 1 つを選択しました。 JKL Toy Company が選択したファイアウォールは、使用しているオペレーティング・システムを保護しないため、 i5/OS パケット・ルールを使用することで別のセキュリティー機能を追加しています。これによって、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ができます。

関連概念

4 ページの『セキュリティー対策の階層的アプローチ』
セキュリティー・ポリシーでは、保護する必要があるもの、 およびシステム・ユーザーに期待することを定義します。

9 ページの『シナリオ: JKL Toy Company の e-business 計画』
独自の e-business 計画を策定するときに役立つ、 JKL Toy Company の一般的なシナリオを取り上げます。 この会社は、インターネットを使用してビジネス対象を拡張することを決定しました。

侵入検知

関連情報

Redbook: All You Need to Know When Migrating from IBM Firewall for AS/400

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。ファイアウォールの機能は次のとおりです。

- 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。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・システム (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システム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ることがあるかもしれません。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。上述のビルの例のように、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もあります。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。これで、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ー・ソリューション全体の一部でしかありません。例えば、SMTP メール、FTP、Telnet などのアプリケーションを介してインターネット上で送信するデータを、ファイアウォールは必ずしも保護できません。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。

i5/OS パケット・ルール

i5/OS パケット・ルールを使用して、システムを保護することができます。パケット・ルールとは、i5/OS オペレーティング・システムの機能で、System i ナビゲーター インターフェースから使用することができます。

パケット・ルールを使用して、TCP/IP トラフィックの流れを制御するように 2 つの中核を成すネットワーク・セキュリティー・テクノロジーを構成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・フィルター操作

NAT と IP フィルター操作は i5/OS オペレーティング・システムに統合されたパーツであるため、経済的にシステムを保護する方法として利用することができます。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: 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。

ネットワーク・アドレス変換と 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) 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、ファイアウォールの 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 i5/OS オペレーティング・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・フィルター操作と 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・フィルター操作 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。 System i 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ー操作規則を、短時間で簡単に構成することができます。

IP パケット・フィルター操作を使用することで、以下のタスクを実行することができます。

- 一連のフィルター規則を作成して、ネットワークへのアクセスを許可する IP パケットと拒否する 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 (例えば、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。
- 特定のパケット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 (例えば、TCP、UDP など)
  - 宛先ポート (例えば、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 Internet Control Message Protocol (ICMP) パケット (例えば、PING パケットなど) が含まれます。
- フィルター規則が、規則と一致するパケット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。情報がシステム・ジャーナルに書き込まれた後で、ログ項目を変更することはできません。ログは、ネットワーク活動を監査する理想的なツールです。

パケット・フィルター規則を使用して、定義した基準に従って IP パケットを拒否または受け入れることで、コンピューター・システムを保護することができます。 NAT 規則では、内部 IP アドレス情報の代わりに 1 つの公衆 IP アドレスを使用することで、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

できます。 IP パケット・フィルターと NAT 規則は、ネットワーク・セキュリティー・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ーは提供していません。完全なファイアウォール製品と i5/OS パケット・ルール機能のどちらに決定するかについては、セキュリティーのニーズと目的を慎重に分析する必要があります。

関連概念

ネットワーク・アドレス変換 (NAT)

IP パケット・フィルター操作

侵入検知

*侵入検出*では、TCP/IP ネットワークを介する無許可アクセスの試みやアタックについての情報を収集する必要があります。全体的なセキュリティー・ポリシーには、侵入検出専用のセクションを作成します。

*侵入検出*という用語は、i5/OS 資料では 2 つの意味で使用されています。 1 つ目は、機密漏れの防止と検出という意味です。例えば、ハッカーが無効なユーザー ID を使用してシステムに侵入しようとしたり、過剰な権限を持つ経験の浅いユーザーがシステム・ライブラリー内の重要なオブジェクトを変更しようとしている可能性があります。

2 つ目は、ポリシーを使用してシステム上の不審なトラフィックをモニターする新しい侵入検出機能という意味です。 TCP/IP ネットワークを介して侵入してくる不審な侵入イベントを監査する侵入検出ポリシーを作成することができます。

i5/OS ネットワーク・セキュリティー・オプションの選択

ネットワーク・セキュリティー・オプションは、インターネット使用計画に従って選択する必要があります。

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・セキュリティー・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。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、 i5/OS TCP/IP 実装の一環として、特定のネットワーク・セキュリティー・テクノロジーを適用することもできます。この実装は、パケット・ルール機能 (IP フィルター操作および NAT を含む) および HTTP for i5/OS (Proxy サーバー・ライセンス・プログラム) から成り立ちます。

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ー・ニーズによって異なります。システムや内部ネットワークをインターネットまたはその他の非トラステッド・ネットワークに接続する場合は、必ず中心的な防御ラインとしてファイアウォールを使用することを検討しなければなりません。

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 i5/OS 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。

注: ファイアウォールと統合 i5/OS ネットワーク・セキュリティー・テクノロジーの両方を使用することもできます。こうすることで、システムを (ファイアウォールの内側で発生する) 内部アタックから守るだけでなく、構成ミスやその他の手段が原因でファイアウォールを破って侵入してくる可能性があるアタックからも守ることができます。

この違いの重要な理由はいくつかあります。例えば、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、

システム上の TCP/IP セキュリティー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、システムそのものを破壊したり、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することが可能性があります。

行おうとしているすべてのセキュリティーの選択において、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ー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 セキュリティー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 セキュリティー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。

セキュリティー・テクノロジー	i5/OS 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・フィルター操作	• 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、単一の i5/OS オペレーティング・システムに対し追加保護を提供する。 • i5/OS オペレーティング・システムがネットワークの残りの部分に対するゲートウェイ (一時的なルーター) として機能している場合に、社内イントラネットのサブネットワークを保護する。 • i5/OS オペレーティング・システムがゲートウェイとして機能しているプライベート・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。	• 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)	• 非互換のアドレッシング構造を持つ 2 つのプライベート・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。	• 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	• 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。	• 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。

関連資料

IP フィルター操作とネットワーク・アドレス変換

HTTP Server for i5/OS

関連情報

AS/400 Internet Scenarios: A Practical Approach

アプリケーション・セキュリティー・オプション

よく使用される数多くのインターネット・アプリケーションやインターネット・サービスに対するセキュリティー・リスクを管理するオプションを使用することができます。

アプリケーション・レベル・セキュリティーの措置では、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、セキュリティー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、セキュリティー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ーの措置に、サーバー側とクライアント側の両方で機密漏れを盛り込む必要があります。

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

関連概念

4 ページの『セキュリティー対策の階層的アプローチ』
セキュリティー・ポリシーでは、保護する必要があるもの、 およびシステム・ユーザーに期待することを定義します。

Web サーバーにおけるセキュリティー

Web サイトへのアクセスを認める場合、ユーザーにサイトの構成やページの生成に使用するコーディングを公開してはなりません。ページへのアクセスは、ユーザーが意識することなく、簡単に、高速で、円滑に行うことができるようにする必要があります。

管理者は、セキュリティーの適用が Web サイトにマイナスの影響を与えないこと、およびそのセキュリティーの適用によって選択したセキュリティー・モデルが実装されることを保証する必要があります。これを実現するには、IBM HTTP Server for i5/OS に組み込まれているセキュリティー機能の中から選択する必要があります。

IBM HTTP Server (powered by Apache) の Redbook  のセキュリティーの展開についての章では、認証、アクセス制御、および暗号化を使用して、セキュリティー機能を実装する方法が説明されています。

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・ファイルの更新を必要とするアプリケーションを作成しなければならないこともあります。例えば、ユーザーが入力した後で、 i5/OS データベースを更新するフォームを作成する必要があるとします。これを行うには、コモン・ゲートウェイ・インターフェース (CGI) プログラムを使用します。

Proxy サーバーも、セキュリティー機能として使用することができます。他のサーバーを宛先とする要求を代わりに受信して、その要求を満たす、転送する、リダイレクトする、または拒否することができます。

HTTP Server は、サーバーを通るアクセスとアクセス試行の両方のモニターに使用できるアクセス・ログを提供します。

Web ページでは、CGI プログラムを使用する以外に、Java™ プログラミングを使用することもできます。Web ページに Java を追加する前に、必ず Java のセキュリティーについて理解しておいてください。

関連概念

『Java インターネット・セキュリティー』
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。Java に関連するセキュリティー問題に取り組む準備も必要です。

関連情報

HTTP Server (powered by Apache) に対する Proxy サーバーのタイプと使用法

HTTP Server のセキュリティーのヒント

コモン・ゲートウェイ・インターフェース

Java インターネット・セキュリティー

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。Java に関連するセキュリティー問題に取り組む準備も必要です。

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ー・リスクに対する優れた防御壁ではありますが、Java の使用によって生じる多くのリスクに対する防御にはなりません。セキュリティー・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。) 例えば、Java は強い型定義を使用することで、つまり例外の余地のない型規則を厳格に適用することで、プログラマーによるオブジェクトの誤使用を回避しています。 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て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、システム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、クライアント上で実行されるものの、i5/OS オペレーティング・システムにアクセスする可能性がある HTML ページに組み込むことができる、小さな Java プログラムです。ネットワーク内の PC 上で動作する Open Database Connectivity (ODBC) プログラムや拡張プログラム間通信 (APPC) プログラムも、システムがアプリケーション・サーバーとして使用されていたり、Web サーバーとして使用されていたりする場合は、オペレーティング・システムにアクセスする可能性があります。通常、Java アプレットは、そのアプレットの発行元である i5/OS オペレーティング・システムとしかセッションを確立できません。したがって、Java アプレットが、接続先の PC から i5/OS オペレーティング・システムにアクセスできるのは、そのアプレットの発行元がその i5/OS オペレーティング・システムである場合に限ります。

アプレットは、システム上の任意の 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 で作成されたシステムの場合、アプレットはシステム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、システムと言う場合は、すべて i5/OS オペレーティング・システムを指します (Java アプリケーション・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 i5/OS オペレーティング・システム上の機能を実行できるのは、ユーザー・プロファイルにそれらの機能の権限が付与されている場合に限ります。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場合は、適切なリソース・セキュリティー計画が不可欠です。アプレットからの要求を処理するときに、システムはユーザー・プロファイルで指定されている限定された機能の値を使用しません。

アプレット・ビューアーを使用して、 i5/OS オペレーティング・システム上でアプレットをテストすることはできますが、ブラウザーのセキュリティー制限は適用されません。したがって、アプレット・ビューアーは、独自のアプレットをテストする場合にのみ使用して、外部ソースからのアプレットの実行には使用しないでください。 Java アプレットは、ユーザーの PC ドライブに書き込みを行うことがよくあります。これは、アプレットに破壊アクションを実行する機会を与えるようなものです。ただし、認証性を確立するために、ディ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、システム上のマップされたドライブにも書き込みを実行できます。なぜなら、PC は、これらのドライブをローカル・ドライブと見なすためです。

ご使用のシステムから Java アプレットを発行する場合は、署名済みのアプレットを使用しなければならないこともあります。しかし、通常は、署名済みのアプレットでも発行元がはっきりしない場合は受け入れないようにユーザーを指導する必要があります。

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 (DCM) を使用して、SSL を使用するように登録済みの Java プログラムを構成することができます。

Java サーブレット

サーブレットは、 Web サーバーのコードを変更せずに Web サーバーの機能を動的に拡張する、 Java で作成されたサーバー・サイドのコンポーネントです。 IBM Web Enablement for i5/OS に付属している IBM WebSphere® Application Server は、 i5/OS オペレーティング・システム上でのサー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、システムが使用するサーブレット・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ー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 サーバーがサー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。例えば、サーブレットを、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。また、WebSphere Application Server for i5/OS にあるような、サーブレット開発ツールに用意されているセキュリティー機能も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の詳細は、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

- インターネット・ブラウザーのセキュリティーに関する考慮事項

リソースに対する Java 認証と承認

IBM Toolbox for Java には、セキュリティー・クラスが含まれており、ユーザーの ID 検査を行うだけでなく、必要に応じて i5/OS オペレーティング・ システム上で実行中のアプリケーションまたはサーブレットのオペレーティング・システム・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。

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。

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 i5/OS 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。

関連概念

19 ページの『Web サーバーにおけるセキュリティー』
Web サイトへのアクセスを認める場合、 ユーザーにサイトの構成やページの生成に使用するコーディングを公開してはなりません。 ページへのアクセスは、ユーザーが意識することなく、簡単に、高速で、円滑に行うことができるようにする必要があります。

DCM の構成

認証サービス

関連情報

Java 認証・承認サービス

Secure Sockets Layer (SSL)

電子メール・セキュリティー

インターネットまたは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、システムがファイアウォール下で保護されていても、システムはセキュリティー・リスクにさらされます。

このようなリスクを理解し、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。

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、多くのシステム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ー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ー・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ーがないと、サーバーの保管ディスクが無用な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・サーバーはサービス妨害となります。また、すべてのシステム・リソースがアタックからのメールの処理に費やされてしまうため、サーバーが応答を停止する可能性もあります。

- **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アタックです。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システムを通過します。メッセージを暗号化していないと、ハッカーが送信経路の任意の地点で電子メールを傍受し、読み取ってしまう可能性があります。

電子メール・セキュリティー・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、これらのアタック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 にこのようなアタック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ー措置は、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ー機能と、必要な機密性のレベルに応じて異なります。例えば、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®/Lotus 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/Lotus 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/Lotus 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、 Lotus 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。

事業所、リモート・クライアント、またはビジネス・パートナーとの間でやりとりする電子メールやその他の情報に、より機密性を持たせたい場合は、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。システムを使用して、リモート・クライアントとシステム間の接続を含め、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。

関連概念

『FTP セキュリティー』
ファイル転送プロトコル (FTP) 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。 セキュリティー・ポリシーでリスクを最小限に抑える方法を確実に表すためには、 FTP を使用したときに発生する可能性があるセキュリティー・リスクを理解しなければなりません。

4 ページの『セキュリティー対策の階層的アプローチ』
セキュリティー・ポリシーでは、保護する必要があるもの、 およびシステム・ユーザーに期待することを定義します。

VPN (仮想プライベート・ネットワーク)

関連資料

セキュリティー用語

関連情報

Lotus Domino Reference Library

Lotus Documentation

Lotus Notes and Domino R5.0 Security Infrastructure Revealed Redbook

Lotus Domino for AS/400 Internet Mail and More Redbook

FTP セキュリティー

ファイル転送プロトコル (FTP) 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。セキュリティー・ポリシーでリスクを最小限に抑える方法を確実に表すためには、 FTP を使用したときに発生する可能性があるセキュリティー・リスクを理解しなければなりません。

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・システムを利用したり、システム間でファイルを移動したりする場合に役立ちます。しかし、インターネット、またはその他の非トラステッド・ネットワークで FTP を使用すると、特定のセキュリティー・リスクにさらされます。これらのリスクを理解することが、システムの保護につながります。

- 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。

  例えば、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・セキュリティー」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・セキュリティーによって、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。

  このセキュリティー・リスクを制御するためのオプションを示します。

  – システム上で完全な i5/OS オブジェクト・セキュリティーを実施します (つまり、システムのセキュリティー・モデルを、メニュー・セキュリティーからオブジェクト・セキュリティーに変更します。これが、最善で、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

キュリティーと同等であるセキュリティーを提供します。また、FTP のアクセス制御をさらに制限することが必要になる場合もあります。このオプションは、FTP のみを対象とするもので、Open Database Connectivity (ODBC)、分散データ管理 (DDM)、分散リレーショナル・データベース体系 (DRDA®) など、その他のインターフェースには適用されません。

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ーの増加と、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。使用を検討する必要があるオプションは、次のとおりです。

  – 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。例えば、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。
  – 侵入検知システムを使用して、システムに対するサービス妨害アタックを検出します。

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。

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ィジタル証明書の使用もサポートします。

これらの FTP オプションに加え、非機密資料へのユーザー・アクセスを簡易化する便利な方法を提供する、匿名 FTP の使用を検討することが必要になることもあります。匿名 FTP では、リモート・システムについて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 を構成する場合は、事前にセキュリティー・リスクを評価し、 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。

関連概念

22 ページの『電子メール・セキュリティー』
インターネットまたは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、 システムがファイアウォール下で保護されていても、システムはセキュリティー・リスクにさらされます。

関連タスク

匿名 FTP の構成

FTP 出口プログラムの使用によるアクセスの管理

関連情報

FTP の保護

SSL の使用による FTP サーバーの保護

伝送セキュリティー・オプション

データがインターネットなどの非トラステッド・ネットワーク上を流れるときにそのデータを保護するには、適切なセキュリティー措置を実施する必要があります。これらの措置には、Secure Sockets Layer (SSL)、System i Access for Windows、仮想プライベート・ネットワーク (VPN) 接続などが含まれます。

JKL Toy Company のシナリオには、2 つの基本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。したがって、周辺ネットワーク上に、イントラネットおよびインターネット・アプリケーションを処理するための新規システムを追加することを決定しました。

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。 また、新規システムを専用のインターネット・サーバーとして指定することで、ネットワーク・セキュリティー管理の簡易化も実現されます。

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ーが必要になるため、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ー・オファ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ーとアプリケーション固有のセキュリティーの両方が行われているようにしなければなりません。しかし、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ことにより、より強力なセキュリティー・ソリューションを実装する必要性が増大します。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ー措置を講じる必要があります。

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、 i5/OS オペレーティング・システムでは 2 種類の伝送レベルによるセキュリティー・オファリングを利用することができます。すなわち、SSL によるセキュア通信と VPN 接続です。

SSL プロトコルは、クライアントとサーバー間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。 i5/OS オペレーティング・システムの場合は、次のものが含まれます。

- IBM HTTP Server for i5/OS (オリジナル版および powered by Apache 版)
- FTP サーバー
- Telnet サーバー
- 分散リレーショナル・データベース体系 (DRDA) と分散データ管理 (DDM) サーバー
- System i ナビゲーター のマネージメント・セントラル

- Directory Services Server (LDAP)
- System i ナビゲーター を含む、 System i Access for Windows アプリケーション、および System i Access for Windows のアプリケーション・プログラミング・インターフェース (API) セットに対して作成されたアプリケーション
- 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ィジタル証明書の使用もサポートします。 SSL では、ディ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。

仮想プライベート・ネットワーク

VPN 接続を使用して、エンドポイント間でセキュアな通信チャネルを確立することができます。 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ーを実現します。

使用すべき方式について

SSL および VPN のどちらも、セキュア認証、データ機密性、およびデータ保全性のニーズに対応します。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。通信先、通信に使用するアプリケーション、通信に必要なセキュリティー・レベル、この通信を保護する場合にかかるコストと期待されるパフォーマンスのトレードオフなどを検討する必要があります。

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。 SSL を利用できないアプリケーションはまだたくさんありますが、 Telnet や System i Access for Windows など、SSL 機能を備えているアプリケーションも数多くあります。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。

例えば、HTTP over SSL を使用して、ビジネス・パートナーに内部ネットワーク上の Web サーバーへの接続を許可することができます。 Web サーバーが、ビジネス・パートナーと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は、あえて VPN 接続に切り替える必要はありません。ただし、通信を拡張する場合は、VPN 接続の使用を検討する必要があるかもしれません。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したくない状況もあります。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。

関連概念

4 ページの『セキュリティー対策の階層的アプローチ』
セキュリティー・ポリシーでは、保護する必要があるもの、 およびシステム・ユーザーに期待することを定義します。

9 ページの『シナリオ: JKL Toy Company の e-business 計画』
独自の e-business 計画を策定するときに役立つ、 JKL Toy Company の一般的なシナリオを取り上げます。 この会社は、インターネットを使用してビジネス対象を拡張することを決定しました。

関連資料

セキュア・ソケットの API

関連情報

Secure Sockets Layer (SSL)

仮想プライベート・ネットワーク (VPN)

SSL のためのディジタル証明書の使用

ディジタル証明書は、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。

i5/OS オペレーティング・システムは、 i5/OS の統合機能であるデジタル証明書マネージャー (DCM) を使って、ユーザーが使用中のシステムでデジタル証明書を簡単に作成および管理できる機能を提供します。

さらに、ユーザー名とパスワードに代わるより強力なクライアント認証手段としてデジタル証明書を使用するように、 IBM HTTP Server for i5/OS などのアプリケーションを構成することもできます。

デジタル証明書とは何か

ディジタル証明書は、パスポートと同様、証明書の所有者の ID を検査するディジタル信任状です。認証局 (CA) と呼ばれる信頼のおける第三者機関が、ユーザーおよびサーバーにデジタル証明書を発行します。 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 の中には、識別名だけを要求するなど、ほとんど情報を必要としないものもあります。識別名は、CA がデジタル証明書アドレスおよびデジタル電子メール・アドレスを発行するユーザーまたはシステムの名前です。 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、ブラウザーまたは保護ファイルには秘密鍵が含まれます。証明書に関連した鍵ペアを使用して、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。こ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、そのアイテムの整合性が確保されます。

SSL を利用できないアプリケーションはまだたくさんありますが、 Telnet や System i Access for Windows など、SSL 機能を備えているアプリケーションも数多くあります。

関連概念

DCM の構成

Secure Sockets Layer (SSL)

関連資料

セキュリティー用語

Telnet のセキュア・アクセスのための Secure Sockets Layer

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、ディ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ィ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、セキュリティー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 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ィ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。セキュリティー・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。Telnet セッションでの SSL の使用は、 Change Telnet Attributes (CHGTELNA) コマンドの Allow Secure Socket Layer (ALWSSL) パラメーターを使用して制御することができます。また、必要に応じてアプリケーションが SSL ポートまたは非 SSL ポートを使用できないようにするには、 Add TCP/IP Port Restriction (ADDTCPPORT) コマンドを使用して制限することもできます。

Telnet、および Telnet が SSL 対応の場合と SSL 非対応の場合のセキュリティー・ヒントについての詳細は、「Telnet」の 『IBM Systems Software Information Center』のトピックを参照してください。 i5/OS オペレーティング・システムで Telnet を使用するために必要な情報が記載されています。

関連概念

Telnet シナリオ: SSL による Telnet の保護

DCM に合わせた計画

関連情報

Telnet

セキュアな System i Access for Windows のための Secure Sockets Layer

System i Access for Windows 通信セッションを保護するために、 Secure Sockets Layer (SSL) を使用するように System i Access for Windows を構成することができます。

SSL を使用すると、System i Access for Windows 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。

関連情報

SSL の管理

Java セキュリティー

セキュリティー・クラス

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)

仮想プライベート・ネットワーク (VPN) は、社内のイントラネットを公衆ネットワークまたはプライベート・ネットワークのいずれかの既存のフレームワークに拡張するもので、組織内の通信を公開せず機密を保護することを支援します。

VPN 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、i5/OS オペレーティング・システムと VPN 接続を使用することで、 2 つのネットワーク間の通信に必要なセキュリティーを提供することができます。 VPN を作成すれば、従来の非交換回線よりもコストを削減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。システムについての情報を共有する必要がある人だけに、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。例えば、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、公衆ネットワーク上に送信してアタックを受ける危険にさらす可能性があります。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。ただし、VPN 接続の構成方法によっては、インターネット上を流れるデータが VPN 接続を介してトランスポートされないことがあります。このような場合は、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が暗号化されません。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。

例えば、どの部品に在庫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す。この情報は、イントラネット上の Web ページを更新する場合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必要があります。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。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ー措置を提供します。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、 i5/OS オペレーティング・システム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。セキュリティーのニーズ次第では、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ーを 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、そのセキュリティーを提供するために、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。セキュリティー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ー・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。

関連概念

2 ページの『System i とインターネット・セキュリティー上の考慮事項』
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。 ここでは、i5/OS のセキュリティーの強さとセキュリティー・オファリングの概要を説明します。

VPN (仮想プライベート・ネットワーク)

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。

〒106-8711
東京都港区六本木 3-2-12
IBM World Trade Asia Corporation
Intellectual Property Law & 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で提供し、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 YBWA
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。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

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

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。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

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。

プログラミング・インターフェース情報

この System i およびインターネット・セキュリティーの文書には、プログラムを作成するユーザーが IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、International Business Machines Corporation の米国およびその他の国における商標です。

Lotus Domino
Distributed Relational Database Architecture (DRDA)
i5/OS
IBM
IBM (ロゴ)
Lotus Notes
System i
WebSphere

Adobe、Adobe ロゴ、PostScript、および PostScript ロゴは、 Adobe Systems Incorporated 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。

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。

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。

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です。

資料に関するご使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

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情報、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で提供され、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。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12