IBM

System i

System i 与因特网安全性

V6R1

System i

System i 与因特网安全性

V6R1

注意

在使用本资料及其支持的产品之前，请务必阅读第 25 页的『声明』中的信息。

本版本适用于 IBM i5/OS V6R1M0（产品编号 5726-SS1）及所有后续发行版和修订版，直到在新版本中另有声明为止。本版本不能在所有精简指令集计算机（RISC）机型上运行，也不能在 CISC 机型上运行。

目录

System i 与因特网安全性

从局域网（LAN）访问因特网要求您重新评估网络安全性要求。

IBM® System i™ 产品的集成软件解决方案和安全性体系结构使您能够构建强大的防御系统，以防御因特网潜在的安全性缺陷和入侵者。通过使用这些安全性产品，可确保您的客户、职员和业务合作伙伴在安全的环境中获取他们所需的信息。

本主题集说明有关众所周知的安全性威胁，同时说明这些风险如何危及您的因特网和电子商务目标。本主题集还会讨论如何评估风险，以及使用系统为对付这些风险所提供的各种安全性选项所带来的好处。可确定如何使用此信息来开发适合您的商务要求的网络安全规划。

System i 与因特网安全性的 PDF 文件

可查看和打印此信息的 PDF 文件。

要查看或下载此文档的 PDF 版本，请选择 《System i 与因特网安全性》（大约 456 KB）。

您可以查看或下载以下相关主题:

- Intrusion detection（大约 285 KB）。可以制订侵入检测策略，它审计通过 TCP/IP 网络进入的可疑侵入事件，如不正确创建的 IP 信息包。还可以编写应用程序以分析审计数据并在可能遭受 TCP/IP 侵入时向安全性管理员报告。
- Enterprise Identity Mapping（EIM）（大约 1954 KB）。企业身份映射（EIM）是一种机制，用于将个人或实体（如服务）映射到整个企业中的各种用户注册表中相应的用户身份。
- Single sign-on（大约 1203 KB）。单点登录解决方案可减少用户必须执行的注册次数，以及用户访问多个应用程序和系统所需的密码数目。
- Planning and setting up system security（大约 3992 KB）。规划和设置系统安全性提供有关如何有效地系统规划和配置系统级别安全性的信息。

保存 PDF 文件

要将 PDF 保存在您的工作站上以便查看或打印:

1. 右键单击浏览器中的 PDF 链接。
2. 单击以本地方式保存 PDF 的选项。
3. 浏览至要保存 PDF 的目录。
4. 单击**保存**。

下载 Adobe Reader

您需要在系统上安装 Adobe® Reader 来查看或打印这些 PDF。可从 Adobe Web 站点（www.adobe.com/products/acrobat/readstep.html）  下载免费副本。

相关概念

侵入检测

企业身份映射（EIM）

单点登录

规划和设置系统安全性

System i 与因特网安全性注意事项

有关因特网的安全性问题是很重要的。本主题概述 i5/OS® 的安全性优点及安全性产品。

将 System i 平台连接至因特网时，首先要想到的一个问题通常是“关于安全性与因特网，我应该知道些什么？”本主题可帮助您回答此问题。

您需要知道的信息取决于您使用因特网的方式。您最初涉足因特网可能是希望向内部网络用户提供对 Web 和因特网电子邮件的访问。您可能还希望具有将敏感信息从一个站点传送到另一个站点的能力。最后，您可能还计划使用因特网来进行电子商务，或在您的公司与业务合作伙伴和供应商之间创建外部网。

涉足因特网之前，应该思考希望做什么及如何去做。确定如何使用因特网及其安全性比较复杂。

注: 如果对安全性和与因特网相关的术语不熟悉，看完此资料之后，可查看常见安全性术语。

明白如何使用因特网进行电子商务以及安全性问题、可用的安全性工具、功能和产品之后，您可以制订安全策略和安全目标。许多因素都将影响在制订安全策略时所做的选择。将组织扩展到因特网上之后，安全策略就是确保系统与资源安全的重要基础。

i5/OS 安全性特征

除了许多用来在因特网上保护系统的特定安全性产品之外，i5/OS 操作系统还具有下列安全性特征:

- 集成安全性，与其他系统所提供的附加安全性软件包相比，这项功能是很难被绕过的。
- 基于对象的体系结构，它使得创建与传播病毒在技术上十分困难。在 i5/OS 操作系统上，文件不能假装成程序，一个程序也不能更改另一个程序。i5/OS 完整性功能部件需要使用系统提供的接口访问对象。不能通过对象在系统中的地址直接访问对象。不能采用偏移地址和将地址转变为指针或创建指针。指针操作是黑客在其他系统体系结构上常用的一种技术。
- 灵活性，允许设置系统安全性以满足特定要求。可使用安全性规划程序来帮助您确定哪种安全性建议适合您的安全性需要。

i5/OS 高级安全性产品

i5/OS 操作系统还提供了几种特定的安全性产品，在连接到因特网时可选择使用它们以提高系统安全性。根据使用因特网的方式，可以利用以下产品中的一种或多种:

- 虚拟专用网（VPN）是企业专用内部网在公用网络（如因特网）上的扩展。可以使用 VPN 创建安全专用连接，主要是通过在公用网络上创建专用隧道来实现。VPN 是 i5/OS 操作系统的集成功能部件，可通过 System i 导航器界面获取。
- 信息包规则是 i5/OS 操作系统的集成功能部件，可通过 System i 导航器界面获取。通过使用此功能部件，可配置 IP 信息包过滤规则和网络地址转换（NAT）规则来控制进出系统的 TCP/IP 通信流。
- 借助安全套接字层（SSL）协议，可将应用程序配置为使用 SSL，以在服务器应用程序与其客户机之间建立安全连接。最初开发 SSL 是为了保护 Web 浏览器和服务器应用程序，但也可以使其他的应用程序使用 SSL。许多应用程序现在支持 SSL，包括 IBM HTTP Server for i5/OS、System i Access for Windows®、文件传输协议（FTP）、Telnet 等等。

相关概念

第 5 页的『安全策略和目标』

安全策略定义要保护的对象以及期望用户实现的安全目标。

第 22 页的『使用虚拟专用网保护专用通信』
虚拟专用网（VPN）是公司内部网基于公用或专用网络的扩展，可帮助您在公司内部以专用方式安全通信。

第 6 页的『方案: JKL 玩具公司电子商务计划』
一个典型方案是 JKL 玩具公司，该公司决定使用因特网扩展其业务目标，这可能对您设置您自己的电子商务方案有所帮助。

相关信息

连接至因特网

eServer 安全性规划程序

IP 过滤和网络地址转换

安全套接字层

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

规划因特网的安全性

制订因特网使用计划时，必须规划因特网安全性要求。

必须收集有关因特网使用计划的详细信息并记录内部网络的配置。根据收集的信息，可以准确地评估您的安全性需要。

例如，您需要整理并描述下列信息:

- 当前网络配置。
- 域名系统（DNS）和电子邮件服务器配置信息。
- 与因特网服务提供商（ISP）的连接。
- 希望通过因特网使用的服务。
- 希望对因特网用户提供的服务。

记录此类信息有助于确定哪里有安全性漏洞且需要使用何种安全性措施以尽量避免这些漏洞。

例如，您决定允许内部用户使用 Telnet 连接到位于专用研究所的主机。内部用户需要此服务以帮助他们为公司开发新的产品；然而，您有些担心机密数据在因特网上以不受保护的方式流动。如果竞争对手捕获并利用了此数据，那么您的公司可能会面临财务风险。确定了使用要求（Telnet）和相关的风险（暴露机密信息）后，可以确定必须实现的附加安全性措施以确保此用法的数据机密性，例如，启用安全套接字层（SSL）。

安全性的分层防御方法

安全性策略会定义要保护的对象以及对系统用户的期望。

安全性策略在设计新的应用程序或扩展当前网络时提供了安全性规划的基础。它描述了用户的职责（如保护机密信息和创建有效密码）。

注: 需要为组织创建和制订安全策略以将内部网络风险降到最低。如果对 i5/OS 操作系统的固有安全性功能配置正确，那么它可将许多风险降到最低。但是，将系统连接到因特网时，需要提供附加安全性措施以确保内部网络的安全。

许多风险与使用因特网访问进行商务活动关联。在创建安全策略时，必须使提供服务与控制对功能及数据的访问保持平衡。使用联网的计算机，保证安全性更加困难，因为通信信道自身是开放的，所以容易受到攻击。

一些因特网服务比其他服务更容易受到某些类型的攻击。因此，了解想要使用或提供的每个服务所强加的风险非常关键。此外，了解可能的安全性风险会帮助您确定一系列明确的安全性目标。

因特网是对因特网通信安全性造成威胁的多种个体的发源地。下面的列表描述了可能遇到的一些典型安全性风险:

- **被动攻击**

  在被动攻击的情况下，作恶者监控网络流量以尝试获取秘密。这种攻击可以是基于网络的（跟踪通信链路）或者基于系统的（用“特洛伊木马”程序替换系统组件以在不知不觉中捕获数据）。检测被动攻击很困难。因此，您需要假定有人在窃听您在因特网上发送的一切消息。

- **主动攻击**

  在主动攻击的情况下，作恶者尝试突破防御进入网络系统。主动攻击有以下几种类型:
  - 在**试图访问系统**时，攻击者试图利用安全漏洞来获取对客户机或服务器系统的访问和控制。
  - 在**电子欺骗**攻击的情况下，攻击者试图通过假冒成可信系统来突破防御，或者某用户劝说您向他发送秘密信息。
  - 在**拒绝服务攻击**情况下，攻击者尝试通过重定向流量或用垃圾邮件轰击系统来干扰或关闭您的操作。
  - 在**密码攻击**情况下，攻击者将试图猜测、偷取您的密码或者使用专门工具尝试对加密的数据解密。

多层防御

因为潜在的因特网安全性风险可能会发生在各种级别上，需要设置提供多层防御的安全性措施来避免这些风险。通常，当您连接到因特网时，不应对是否会遇到侵入尝试或拒绝服务攻击感到疑惑。而是应该认为将会遇到安全性问题。因此，最好的防御措施是周密的主动进攻。规划因特网安全策略时，使用分层方法可确保穿过一层防御的攻击者会被后续层阻止。

安全策略必须包括对传统网络计算模型的以下各层提供保护的措施。通常，您需要按照从最基本的（系统级别安全性）到最复杂的（事务级别安全性）顺序来规划安全性。

系统级别安全性

系统安全性措施是防御基于因特网安全性问题的最后防线。因此，制订整个因特网的安全策略的第一步必须是正确配置基本系统安全性。

网络级别安全性

网络安全性措施控制对 i5/OS 操作系统及其他网络系统的访问。将网络连接到因特网时，需要确保已有足够的网络级别安全性措施以保护内部网络资源不受未经授权的访问和侵入。防火墙是提供网络安全性的最常见的方式。因特网服务提供商（ISP）可对您的网络安全性规划提供重要的元素。网络安全性方案需要概述 ISP 所要提供的安全性措施（如 ISP 路由器连接的过滤规则及公共域名系统（DNS）预防措施）。

应用程序级别安全性

应用程序级别安全性措施控制用户与特定应用程序进行交互的方式。通常，您应该对所使用的每个应用程序都配置安全性设置。但是，对那些通过因特网使用或向因特网提供的应用程序和服务，应特别注意设置安全性。未经授权的用户寻找途径以访问网络系统，使这些应用程序和服务很容易被滥用。决定要使用的安全性措施需要包括服务器端和客户机端的安全漏洞。

传输级别安全性

传输级别安全性措施保护网络内部及网络间的数据通信。在不可信网络（如因特网）上通信时，无法控制流量从源到目的地的流动方式。它传输的流量与数据通过了许多无法控制的不同系统。除非设置安全性措施（如配置应用程序以使用安全套接字层（SSL）），否则路由的数据可供任何人查看和使用。传输级别安全性措施可以保护数据，就像数据在其他安全级别边界之间流动一样。

开发整个因特网安全策略时，应该对每个层单独开发安全策略。另外，您应该描述每套策略与其他策略的交互方式以对您的业务提供综合的安全性网络。

相关概念

第 8 页的『基本因特网就绪的安全级别』
在连接至因特网之前，应决定为保护系统需要采用的安全级别。

第 9 页的『网络安全性选项』
要保护内部资源，请选择适当的网络级别安全性措施。

第 14 页的『应用程序安全性选项』
某些选项可用来管理若干常用因特网应用程序和服务的安全性风险。

第 19 页的『传输的安全性选项』
为了在不可信网络（如因特网）上传输数据时保护数据，应采取适当的安全性措施。这些措施包括安全套接字层（SSL）、System i Access for Windows 和虚拟专用网（VPN）连接。

『安全策略和目标』
安全策略定义要保护的对象以及期望用户实现的安全目标。

第 16 页的『电子邮件安全性』
在因特网或其他不可信网络间使用电子邮件会暴露系统的安全性风险，即使系统受到防火墙的保护也是如此。

相关参考


System i Security Guide for IBM i5/OS V5R4

安全策略和目标

安全策略定义要保护的对象以及期望用户实现的安全目标。

您的安全策略

您所使用或提供的每个因特网服务都会对系统及相连的网络造成风险。安全策略是一套规则，适用于属于某个组织的计算机和通信资源的活动。这些规则包括了几个领域（如物理安全性、人员安全性、管理安全性和网络安全性）。

安全策略定义希望保护的对象以及对系统用户的期望。它在设计新的应用程序或扩展当前网络时提供了安全性规划的基础。它描述了用户的职责（如保护机密信息和创建有效密码）。安全策略还应该描述将如何监控安全性措施的有效性。这种监控可帮助您确定是否有人正试图绕过您的安全措施。

要制订安全策略，必须明确定义安全性目标。创建了安全策略之后，必须采取措施来实施其所包含的规则。这些步骤包括训练职员并添加必需的软件和硬件来实施该规则。另外，当更改计算环境时，应该更新安全策略。这是为了确保处理更改可能带来的任何新风险。

您的安全性目标

创建并执行安全策略时，必须有明确的目标。安全性目标分为以下一种或几种类别:

资源保护
资源保护方案确保只有已授权的用户才能访问系统中的对象。System i 具有保护所有类型系统资源的能力。您应该谨慎定义能够访问您的系统的用户的不同类别。还应该定义您希望授予这些用户组的访问权限并将其作为创建安全策略的一部分。

认证 确保或验证会话另一端的资源（人或机器）确实是它所声明的资源。可靠的认证可保护系统免受冒名的安全性风险，即发送方或接收方使用假身份来访问系统。通常，系统使用密码和用户名进行认证;

数字证书能提供更安全的认证方法，同时也能提供其他安全性好处。当将系统链接到公用网络（如因特网）时，用户认证变得更加复杂。因特网和内部网之间的重要差别在于您信任注册的用户身份的能力，因此，应该认真考虑这个想法 – 使用比登录程序提供的传统用户名和密码更强的认证方法。根据用户的授权级别，已认证用户可以拥有不同类型的许可权。

授权 确保会话另一端的个人或计算机有权执行请求。授权是确定谁或什么可以访问系统资源或在系统上执行某种活动的过程。通常，授权在认证的上下文中执行。

完整性 确保到达信息与发送信息相同。了解完整性要求您理解数据完整性和系统完整性的概念。

- **数据完整性**: 保护数据以避免未授权的更改或篡改。数据完整性防御操作安全性风险，即某人拦截和更改未对他/她授权的信息。除保护存储在网络中的数据之外，当数据从不可信的源进入系统时，可能需要附加安全性来确保数据完整性。当进入系统的数据来自公用网络时，可能需要安全性方法以执行下列任务:
  - 通常采用数据加密的手段来保护数据不被窃听和解释。
  - 确保数据的传输没有改变（数据完整性）。
  - 证实传输发生（不可抵赖性）。将来可能需要已注册或认证的邮件的电子等效物。
- **系统完整性**: 系统按预期性能提供一致的和预期的结果。对于 i5/OS 操作系统，系统完整性是通常最容易忽略的安全性组件，因为它是 i5/OS 体系结构的基础部件。例如，当使用安全级别 40 或 50 时，i5/OS 体系结构就使得黑客模仿或更改操作系统程序变得异常困难。

不可抵赖性

发生交易的证明，或您发送或接收到消息的证明。使用数字证书和公用密钥密码术来对事务、消息和文档进行签名，支持不可抵赖性。发送方和接收方都承认交换发生。数据上的数字签名提供了必需的证据。

机密性 确保敏感信息是私有的且对偷看者不可见。机密性对整个数据安全性来说非常关键。通过使用数字证书和安全套接字层（SSL）或虚拟专用网（VPN）连接加密数据，可帮助您确保在不可信网络间传输数据时实现机密性。安全策略应决定如何对网络中的信息以及与网络脱离之后的信息提供机密性。

审计安全性活动

监控安全性相关的事件以提供包括成功和不成功（被拒绝）访问的记录。成功访问记录告诉您谁正在您的系统上做什么，不成功（被拒绝）访问记录告诉您某人正试图破坏您的安全性或某人访问您的系统有困难。

相关概念

第 2 页的『System i 与因特网安全性注意事项』
有关因特网的安全性问题是很重要的。本主题概述 i5/OS 的安全性优点及安全性产品。

第 3 页的『安全性的分层防御方法』
安全性策略会定义要保护的对象以及对系统用户的期望。

配置 DCM

安全套接字层（SSL）

『方案: JKL 玩具公司电子商务计划』
一个典型方案是 JKL 玩具公司，该公司决定使用因特网扩展其业务目标，这可能对您设置您自己的电子商务方案有所帮助。

方案: JKL 玩具公司电子商务计划

一个典型方案是 JKL 玩具公司，该公司决定使用因特网扩展其业务目标，这可能对您设置您自己的电子商务方案有所帮助。

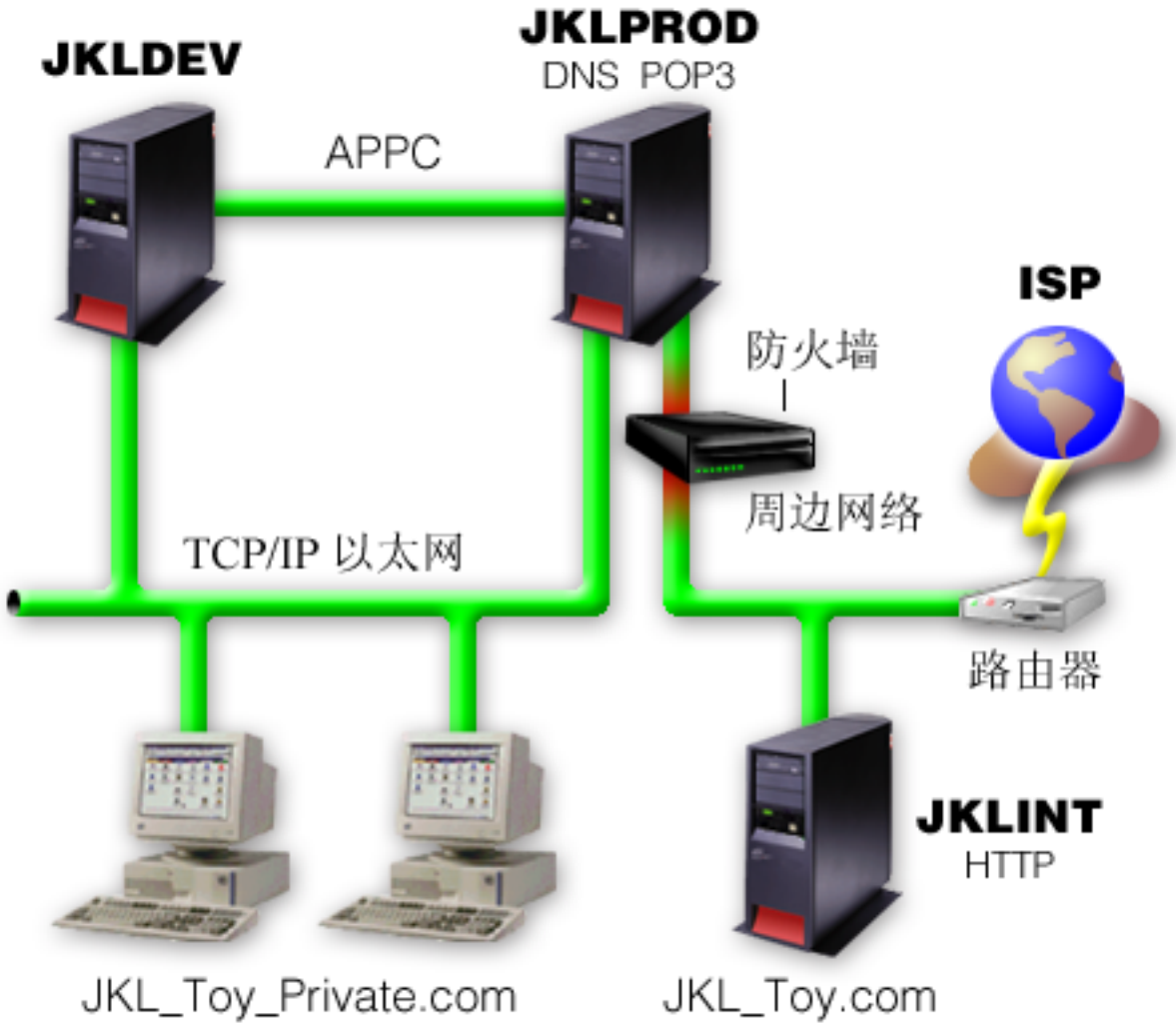
JKL 玩具公司是一家小型玩具制造公司，但发展极为迅速。公司总经理非常关心业务的发展，以及其新的 i5/OS 操作系统能如何减轻发展的负担的问题。财务部经理 Sharon Jones 负责系统管理和系统安全性。

JKL 玩具公司对其内部应用程序已成功使用其安全策略有一年多的时间。公司现在计划安装内部网以更有效率地共享内部信息。公司还计划开始使用因特网以使业务目标更上一层楼。这些目标包括计划创建公司因特网销售网点（包括联机目录）。他们也想使用因特网将敏感信息从远程站点传送至公司总部。另外，公司想让设计实验室的职员可以访问因特网以供研究和开发之用。最后，公司希望客户能够使用他们的 Web 站点进行直接在线采购。Sharon 正在写一个报告，描述关于这些活动特定的潜在安全性风险及公司应采取何种安全性措施使这些风险降到最低。Sharon 将负责更新公司安全策略并实施公司决定采用的安全性措施。

使用这种增强的因特网的目标如下所述:

- 全面提升公司形象并作为整个营销活动的一部分。
- 为客户和销售人员提供在线产品目录。
- 改善客户服务。
- 为职员提供电子邮件和万维网访问权。

确保其系统具有强大的基本系统安全性之后，JKL 玩具公司决定购买并使用防火墙产品以提供网络级别的保护。防火墙将保护其内部网络免受许多潜在的与因特网相关的风险。下图描述了该公司的因特网或网络配置。



如图所示，JKL 玩具公司拥有两个主要系统。他们将一个系统用于开发应用程序（JKLDEV），将另一个系统用于生产应用程序（JKLPROD）。这两个系统都处理关键任务数据和应用程序。因此，他们对在这些系统上运行其因特网应用程序感到担心。他们已选择添加一个新系统（JKLINT）来运行这些应用程序。

公司已将新系统放置在周边网络上，并在其与公司主要内部网络之间使用了防火墙，以确保将他们的网络和因特网更好地隔离开来。这种隔离降低了公司内部系统容易遭受到来自因特网攻击的风险。通过将新的系统指定为纯因特网服务器，公司也降低了管理其网络安全性的复杂性。

此时，公司不会在新的系统上运行任何关键任务应用程序。在电子商务计划的此阶段中，新系统将仅提供静态公用 Web 站点。然而，公司希望实现安全性措施以保护系统及其运行的公共 Web 站点以防止服务中断和其他可能的攻击。因此，公司将用信息包过滤规则和网络地址转换（NAT）规则及强大的基本安全性措施来保护系统。

随着公司开发更高级的公共应用程序（如电子商务 Web 站点或外部网访问），他们将实现更高级的安全性措施。

相关概念

第 5 页的『安全策略和目标』
安全策略定义要保护的对象以及期望用户实现的安全目标。

第 2 页的『System i 与因特网安全性注意事项』
有关因特网的安全性问题是很重要的。本主题概述 i5/OS 的安全性优点及安全性产品。

第 9 页的『网络安全性选项』
要保护内部资源，请选择适当的网络级别安全性措施。

第 19 页的『传输的安全性选项』
为了在不可信网络（如因特网）上传输数据时保护数据，应采取适当的安全性措施。这些措施包括安全套接字层（SSL）、System i Access for Windows 和虚拟专用网（VPN）连接。

基本因特网就绪的安全级别

在连接至因特网之前，应决定为保护系统需要采用的安全级别。

系统安全性措施是防御基于因特网安全性问题的最后防线。制订整个因特网的安全策略的第一步一定是正确配置 i5/OS 基本安全性设置。 请执行以下任务以确保您的系统安全性满足最低要求:

- 将安全级别（QSECURITY 系统值）设置为 50。安全级别 50 提供了最高级别的完整性保护，建议在高风险环境（如因特网）中使用此级别保护您的系统。

  注: 如果当前在低于 50 的安全级别上运行，可能需要更新操作过程或应用程序。在更改为使用更高安全级别之前，需要复查《System i 安全性参考》。
- 将安全性相关的系统值设置为至少与推荐设置的限制级别相同。可使用 System i 导航器安全性向导来配置建议的安全性设置。
- 确保没有用户概要文件（包括 IBM 提供的用户概要文件）有缺省密码。使用“分析缺省密码”（ANZDFTPWD）命令检查是否有缺省密码。
- 使用对象权限保护重要的系统资源。在系统上使用限制方法。即，在缺省情况下限制每个人（PUBLIC *EXCLUDE）访问系统资源（如库和目录）。仅允许某些用户访问这些受限资源。在因特网环境中只通过菜单限制访问是不够的。
- 必须在系统上设置对象权限。

为了配置这些最低系统安全性要求，可使用 eServer 安全性规划程序或安全性向导（可从 System i 导航器界面获得）。根据您对一系列问题的回答，安全性规划程序为您提供了一组推荐的安全性设置。然后可以使用这些推荐设置配置您需要的系统安全性设置。与安全性规划程序不同，安全性向导使用推荐设置来配置系统安全性设置。

正确配置和管理 i5/OS 固有安全性功能可将许多风险降到最低。但是，将系统连接到因特网时，需要提供附加安全性措施以确保内部网络的安全。确保具有一般系统安全性之后，可在规划因特网使用的综合安全性时配置其它安全性措施。

相关概念

第 3 页的『安全性的分层防御方法』
安全性策略会定义要保护的对象以及对系统用户的期望。

相关参考

安全级别系统值

安全性参考

网络安全性选项

要保护内部资源，请选择适当的网络级别安全性措施。

与不可信网络连接时，安全策略必须描述一个综合性的安全性方案，包括将在网络级别实现的安全性措施。安装防火墙是部署一系列综合网络安全性措施的最好方法之一。

因特网服务提供商（ISP）可对您的网络安全性规划提供重要的元素。网络安全性方案应该概要地描述 ISP 所要提供的安全性措施（如 ISP 路由器连接的过滤规则及公共域名系统（DNS）预防措施）。

虽然防火墙在整个安全性规划中无疑是主要防御措施之一，但它不应该是唯一的防御措施。因为潜在的因特网安全性风险可能会发生在各种级别上，需要设置提供多层防御的安全性措施来避免这些风险。

每当系统或内部网络连接到因特网时，应考虑将防火墙用作主要防御措施。尽管不能再购买 IBM Firewall for the i5/OS 产品，而且 IBM 也不再提供对该产品的支持，但有其他许多产品可供使用。

因为商业防火墙产品提供了全面的网络安全性技术，所以 JKL 玩具公司选择了其中一种来保护其网络。因为他们选择的防火墙不能保护操作系统，所以他们增加了通过使用 i5/OS 信息包规则而获得的安全性功能部件。这允许他们创建过滤规则和 NAT 规则来控制因特网服务器的流量。

相关概念

第 3 页的『安全性的分层防御方法』
安全性策略会定义要保护的对象以及对系统用户的期望。

第 6 页的『方案：JKL 玩具公司电子商务计划』
一个典型方案是 JKL 玩具公司，该公司决定使用因特网扩展其业务目标，这可能对您设置您自己的电子商务方案有所帮助。

侵入检测

相关信息

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

防火墙

防火墙是安全内部网络和不可信网络（如因特网）之间的屏障。

尽管也可以使用防火墙来保护一个内部网络免受另一个内部网络的侵害，但大多数公司还是使用防火墙将内部网络安全地连接到因特网上。

在安全内部网络和不可信网络之间，防火墙提供受控的单一联系点（称为*阻塞点*）。防火墙的功能如下:

- 允许内部网络中的用户使用位于外部网络上的授权资源。
- 防止外部网络上的未授权用户使用内部网络上的资源。

使用防火墙作为因特网（或其他网络）的网关时，就在相当程度上降低了内部网络的风险。由于防火墙功能执行许多安全策略指示，因此使用防火墙还使得管理网络安全性更加容易。

防火墙如何工作

要了解防火墙如何工作，将网络想像成您希望控制访问的建筑物。建筑物有一个作为唯一入口点的门廊。在此门廊里，有迎宾的接待员、监控来宾的保安员、记录来宾行为的摄像机和确认进入建筑物的来宾证件阅读器。

这些措施可以很好地控制对建筑物进行的访问。但是，如果未经授权的人成功进入建筑物，就无法保护建筑物不受此闯入者的破坏。然而，如果监控该闯入者的行动，就有机会检测他的任何可疑行为。

防火墙组件

防火墙是硬件和软件的集合，软硬件一起使用时可防止对网络某一部分的未授权访问。防火墙由以下组件组成:

- **硬件**

  防火墙硬件通常由一台单独的计算机或专门用来运行防火墙软件功能的设备组成。

- **软件**

  防火墙软件提供多种应用程序。就网络安全性而言，防火墙通过多种技术来提供这些安全性控件:

  – 因特网协议（IP）信息包过滤
  – 网络地址转换（NAT）服务
  – SOCKS 服务器
  – 多种服务（如 HTTP、Telnet 和 FTP 等）的代理服务器
  – 邮件中继服务
  – 分割域名系统（DNS）
  – 记录
  – 实时监控

  注: 一些防火墙提供虚拟专用网（VPN）服务，以便可在您的防火墙和其他兼容的防火墙之间设置加密会话。

使用防火墙技术

可以使用防火墙代理服务器、SOCKS 服务器或者 NAT 规则为内部用户提供对因特网服务的安全访问。代理服务器和 SOCKS 服务器在防火墙处中断 TCP/IP 连接，以便对不可信网络隐藏内部网络信息。服务器还提供附加记录能力。

可以使用 NAT 向因特网用户提供对防火墙后的公共系统的轻松访问。由于 NAT 隐藏了您的内部 IP 地址，因此防火墙还保护着您的网络。

防火墙还能通过提供防火墙所使用的 DNS 服务器来保护内部信息。实际上，您拥有两台 DNS 服务器: 一台用于有关内部网络的数据，防火墙上的另一台用于有关外部网络和防火墙自身的数据。这允许控制对有关内部系统信息的外部访问。

定义防火墙策略时，您可能认为禁止对组织构成风险的任何行为而允许其他任何行为就足够了。然而，由于计算机犯罪者在不断创造新的攻击方法，因此您必须预先考虑防止这些攻击的方法。就象建筑物示例一样，您还需要监控是否有人以某种方式突破了防御的迹象。通常来讲，由于非法侵入而导致的损害和花费要比采取预防性措施的花费大得多。

在有防火墙的情况下，最佳策略是只允许那些经过测试并信任的应用程序进行访问。如果您遵循此策略，就必须完全定义必须在您的防火墙上运行的服务列表。可以按连接方向（从内向外或从外向内）来定义每个服务的特征。还应该列示用户，您将授权这些用户使用每项服务以及可以对该服务发出连接的机器。

对于保护您的网络，防火墙所能做的

在您的网络和因特网（或其他不可信网络）的连接点之间安装防火墙。这样，防火墙会限制进入网络的入口点。防火墙在您的网络与因特网之间提供单一联系点（称为阻塞点）。因为具有单一联系点，所以可以对允许出入网络的流量有更多控制。

防火墙对外界表现为单个地址。防火墙通过代理或 SOCKS 服务器或网络地址转换（NAT）提供对不可信网络的访问，同时隐藏内部网络地址。因此，防火墙维护了内部网络的保密性。将网络信息保密是防火墙用来降低冒名攻击（电子欺骗）可能性的一个途径。

防火墙允许控制出入网络的流量，以将对网络攻击的风险降到最低。防火墙安全地过滤所有进入网络的流量，只允许到达特定目的地的特定类型的流量进入。这使某人可能使用 Telnet 或文件传输协议（FTP）来访问内部系统的风险降到最低。

对于保护您的网络，防火墙所无法做的

尽管防火墙提供了免受某类攻击的强大保护，但防火墙只是整个安全性解决方案的一部分。例如，防火墙不一定能够保护通过应用程序（例如，简单邮件传输协议（SMTP）邮件、FTP 和 Telnet）在因特网上发送的数据。除非选择对此数据进行加密，否则，因特网上的任何人都可在数据传输到其目的地期间访问该数据。

i5/OS 信息包规则

可使用 i5/OS 信息包规则来保护系统。信息包规则是 i5/OS 操作系统的功能，可通过 System i 导航器界面获得。

可使用信息包规则来配置两种核心网络安全性技术，从而控制 TCP/IP 流量:

- 网络地址转换（NAT）
- IP 信息包过滤

因为 NAT 和 IP 过滤是 i5/OS 操作系统的集成部件，它们为您提供一种经济的途径来保护系统。在一些情况下，这些安全性技术可提供您所需的所有功能而不必另行购买。然而，这些技术并不能创建真正有效的防火墙。根据安全性要求和目标，可单独使用 IP 信息包安全性，或者与防火墙一起使用。

注: 系统安全性应该优先于成本。为确保对生产系统提供最大限度的保护，应考虑使用防火墙。

网络地址转换和 IP 信息包过滤

网络地址转换（NAT）更改流经系统的信息包的源或目标 IP 地址。NAT 提供防火墙的代理服务器和 SOCKS 服务器的更透明选择。通过使具备不兼容寻址结构的网络互相连接，NAT 还可简化网络配置。因此，可使用

NAT 规则，以便 i5/OS 操作系统可充当两个具有冲突或不兼容寻址方案的网络之间的网关。也可使用 NAT 通过动态替换一个或多个真实地址来隐藏一个网络的真实 IP 地址。因为 IP 信息包过滤和 NAT 互相补充，通常可一起使用它们以增强网络安全性。

使用 NAT 还使得在防火墙后运行公共 Web 服务器更容易。Web 服务器的公共 IP 地址转换为专用内部 IP 地址。它减少必需的注册 IP 地址的数量并使对现有网络的影响最小。它还为内部用户提供在访问因特网的同时隐藏专用内部 IP 地址的机制。

IP 信息包过滤提供根据信息包头信息有选择地阻塞或保护 IP 流量的能力。可在 System i 导航器中使用“因特网设置向导”快速简易地配置基本过滤规则以阻挡不需要的网络流量。

可使用 IP 信息包过滤执行以下任务:

- 创建一组过滤规则以指定允许或拒绝哪些 IP 信息包访问您的网络。创建过滤规则时，将它们应用到物理接口（例如，令牌环或以太网线路）。可将规则应用于多个物理接口，或者对每个接口应用不同的规则。
- 创建规则，以允许或禁止基于以下头信息的特定信息包:
  - 目标 IP 地址
  - 源 IP 地址协议（例如，TCP、UDP 等）
  - 目标端口（例如，对于 HTTP 是端口 80）
  - 源端口
  - IP 数据报方向（入站或出站）
  - 转发或本地
- 防止不想要或不必要的流量达到系统上的应用程序。另外，还可防止流量转发到其他系统。这包括低级的不需要特定应用程序服务器的因特网控制报文协议（ICMP）信息包（例如，PING 信息包）。
- 指定过滤规则是否创建包含与系统日志中的规则匹配的信息包信息的记录项。信息写入到系统日志之后，不能更改该记录项。因此，日志是审计网络活动的理想工具。

通过信息包过滤规则，可根据您定义的条件拒绝或者接受 IP 信息包来保护计算机系统。NAT 规则允许通过使用公共 IP 地址替代内部 IP 地址信息来对外部用户隐藏内部系统信息。尽管 IP 信息包过滤和 NAT 规则是核心网络安全性技术，但它们不能提供功能完备的防火墙产品所提供的相同级别的安全性。要决定使用全功能防火墙产品还是 i5/OS 信息包规则功能部件时，应该仔细分析您的安全性要求和目标。

相关概念

网络地址转换（NAT）

IP 信息包过滤

侵入检测

*侵入检测*包括收集有关通过 TCP/IP 网络进入的未授权访问尝试和攻击的信息。整体安全性策略有一部分专门用于侵入检测。

i5/OS 文档中用*侵入检测*表达两种含义。在第一种含义中，侵入检测指的阻止和检测安全性漏洞。例如，黑客可能尝试使用无效用户标识进入系统，或者没什么经验但具有很高权限的用户可能会改变某些系统库中的重要对象。

在第二种含义中，侵入检测指的是新的侵入检测功能，它使用一些策略来监视系统上可疑的通信数据。可以制订侵入检测策略以审计通过 TCP/IP 网络进入的可疑侵入事件。

选择 i5/OS 网络安全性选项

您需要根据您的因特网使用计划选择网络安全性选项。

预防未授权访问的网络安全性解决方案，通常依靠防火墙技术提供保护。要保护您的系统，可使用全功能防火墙产品，也可以选择将特定网络安全性技术用作 i5/OS TCP/IP 实现的一部分。此实现由信息包规则功能部件（包括 IP 过滤和 NAT）和 HTTP for i5/OS（代理服务器许可程序）组成。

是选择使用信息包规则功能部件还是选择使用防火墙，取决于网络环境、访问要求和安全性要求。每当系统或内部网络连接到因特网或其他非可信网络时，应考虑将防火墙产品用作主要防御措施。

在这种情况下，防火墙更为可取，因为防火墙通常是具有有限个可供外部访问的接口的专用硬件和软件设备。使用 i5/OS TCP/IP 技术保护因特网访问时，所使用的就是一个对外部访问开放无数个接口和应用程序的通用计算平台。

注: 您可能要同时使用防火墙和集成 i5/OS 网络安全性技术。这可以帮助系统抵御内部攻击以及可能穿透防火墙（因为错误配置或其他方法）的任何攻击。

出于许多原因，这个差别很重要。例如，专用防火墙产品不提供任何超出构成防火墙自身的其他功能或应用程序。因此，如果攻击者成功绕过防火墙并获得对防火墙的访问，攻击者也不能做出很多攻击。然而，如果攻击者绕过了系统上的 TCP/IP 安全性功能，攻击者就潜在地能够访问多种有用的应用程序、服务和数据。那时攻击者就可以利用这些对系统自身造成破坏或者获得对内部网络中的其他系统的访问。

象您所做的所有安全性选择一样，您必须将您的决定建立在所希望的成本收益比上。您必须分析业务目标，并决定您希望接受的风险程度以及为安全性所花费的成本，以使这些风险降到最低。下表提供了有关何时适合使用 TCP/IP 安全性功能或者适合使用全功能防火墙设备的信息。可以使用此表来确定您需要使用防火墙、TCP/IP 安全性功能还是二者的组合来为您的网络和系统提供保护。

安全性技术	i5/OS TCP/IP 技术的最佳使用	全功能防火墙的最佳使用
IP 信息包过滤	• 用于对单个 i5/OS 操作系统（如公共 Web 服务器或包含敏感数据的内部网系统）提供附加保护。 • 用于在 i5/OS 操作系统对网络的其余部分充当网关（临时路由器）时保护公司内部网的子网。 • 用于控制通过 i5/OS 操作系统充当网关的专用网络或外部网与部分可信的伙伴进行的通信。	• 用于保护整个企业网络不受因特网或您的网络所连接的其他不可信网络的侵害。 • 用于保护具有很大流量的大型子网不受企业网络的其余子网的侵害。
网络地址转换（NAT）	• 用于启用具有不兼容寻址结构的两个专用网络的连接。 • 在子网中对较不可信网络隐藏地址。	• 用于隐藏访问因特网或其他不可信网络的客户机地址。用作“代理服务器”和“SOCKS 服务器”的替代。 • 用于使专用网络中的系统服务对因特网上的客户机可用。
代理服务器	• 用于当中央防火墙提供对因特网的访问时在企业网络的远程位置提供代理。	• 用于访问因特网时为整个企业网络提供代理。

相关参考

IP 过滤和网络地址转换

HTTP Server for i5/OS

相关信息

AS/400 Internet Scenarios: A Practical Approach

应用程序安全性选项

某些选项可用来管理若干常用因特网应用程序和服务的安全性风险。

应用程序级别安全性措施控制用户与特定应用程序进行交互的方式。通常，您必须对所使用的每个应用程序都配置安全性设置。但是，对那些通过因特网使用的或向因特网提供的应用程序和服务，需要特别注意设置安全性。未经授权的用户寻找途径以访问网络系统，使这些应用程序和服务很容易被滥用。您所使用的安全性措施需要同时包括服务器端和客户机端的安全性漏洞。

尽管保护您所使用的每个应用程序很重要，但安全性措施只占全局安全策略实现的很小一部分。

相关概念

第 3 页的『安全性的分层防御方法』
安全性策略会定义要保护的对象以及对系统用户的期望。

Web 服务安全性

在向访问者提供 Web 站点访问时，不要将关于如何设置站点和生成页面所使用的编码信息暴露给浏览者。只需要让这些访问者轻松、迅速又顺利地访问您的页面，将所有工作放在后台进行。

作为管理员，您希望确保安全性实践不致对 Web 站点有负面影响，并且它们又能实现您选择的安全方式。为此，需要在构建到 IBM HTTP Server for i5/OS 中的安全性功能部件之间进行选择。

IBM HTTP Server (powered by Apache) Redbook 中有关部署安全性的章节描述如何使用认证、访问控制和加密来实现安全性功能部件。

超文本传输协议（HTTP）提供了显示数据的能力，但不能修改数据库文件中的数据。但是，有时您可能要编写一些需要更新数据库文件的应用程序。例如，您可能要创建一些表单，一旦用户填完这些表单，那么将更新一个 i5/OS 数据库。可使用公共网关接口（CGI）程序来完成此任务。

您可以使用的另一个安全性功能部件是代理服务器。它接收面向其他服务器的请求，然后执行、转发、重定向或拒绝这些请求。

HTTP Server 提供了访问记录，可以用于监控通过该服务器进行与试图进行的访问。

Web 页面上除了使用 CGI 程序之外，还可使用 Java™ 编程。在将 Java 添加至 Web 页面之前，需要了解 Java 安全性。

相关概念

第 15 页的『Java 因特网安全性』
在当今的计算环境中，Java 编程日益普及。应准备处理与 Java 相关联的安全性因素。

相关信息

HTTP Server（powered by Apache）的代理服务器类型和使用

HTTP Server 的安全性提示

公共网关接口

Java 因特网安全性

在当今的计算环境中，Java 编程日益普及。应准备处理与 Java 相关联的安全性因素。

虽然防火墙能够很好地防御大多数常见因特网安全性风险，但它不能对使用 Java 所带来的许多风险提供保护。安全策略应该包括保护系统不受涉及 Java 的应用程序、applet 和 servlet 这三个方面干扰的详细信息。还应该了解在 Java 程序的认证和授权方面，Java 和资源安全性是如何进行交互的。

Java 应用程序

作为一种语言，Java 具有一些防止 Java 程序员粗心犯错误的特征，这些粗心错误会导致完整性问题。（其他 PC 应用程序常用的语言，例如 C 或 C++，不像 Java 那样能有效防止程序员粗心犯错误。）例如，Java 使用强类型化，毫无例外地强制执行类型规则，可防止程序员以意外的方式使用对象。Java 不允许指针操作，这防止程序员偶然超出程序的内存边界。从应用程序开发的角度来看，可以象查看其他高级语言一样来查看 Java。您需要对应用程序设计应用对系统上的其他语言应用的安全性规则。

Java applet

Java applet 是可包括在 HTML 页面中的 Java 小程序，可在客户机上运行，但也可访问 i5/OS 操作系统。例如，系统用于处理应用程序或用作 Web 服务器时，在网络中的 PC 上运行的开放式数据库连接（ODBC）程序或高级程序间通信（APPC）程序还可潜在访问操作系统。通常，Java applet 只能与产生 applet 的 i5/OS 操作系统建立会话。因此，仅当 applet 来自 i5/OS 操作系统时，Java applet 才能通过连接的 PC 访问 i5/OS 操作系统。

applet 会尝试连接至系统上的任何 TCP/IP 端口。它并非必须同用 Java 编写的软件服务器进行通话。但是，对于用 IBM Toolbox for Java 编写的系统，applet 在建立与系统的连接时必须提供用户标识和密码。在本资料中，描述的系统都是 i5/OS 操作系统。（Java 应用程序服务器不需要使用 IBM Toolbox for Java。）通常，IBM Toolbox for Java 类在第一次连接时向用户提示用户标识和密码。

仅当用户概要文件具有访问那些功能的授权时，applet 才能在 i5/OS 操作系统上执行那些功能。因此，当开始使用 Java applet 来提供新的应用程序功能时，好的资源安全性方案是必要的。当系统处理来自 applet 的请求时，不会使用在用户概要文件中指定的有限功能值。

applet 查看器允许在 i5/OS 操作系统上测试 applet；然而这并不受限于浏览器安全性限制。因此，您应该仅使用 applet 查看器来测试自己的 applet，而一定不能从外部源运行 applet。Java applet 通常会写至用户的 PC 驱动器，这可能会对 applet 提供执行破坏性操作的机会。然而，可以使用数字证书签署 Java applet 以建立其真实性。已签署的 applet 就可以写入 PC 机的本地驱动器，即使浏览器的缺省设置防止这样做。已签署的 applet 还可以写至系统上的映射驱动器，因为对 PC 机来说这些映射驱动器就是本地驱动器。

对于源自系统的 Java applet，您可能需要使用已签署的 applet。然而，您需要通知您的用户一般情况下不要接受来自未知源的已签名 applet。

从 V4R4 开始，可以使用 IBM Toolbox for Java 设置安全套接字层（SSL）环境。还可以使用 IBM Developer Toolkit for Java 使 Java 应用程序受 SSL 的保护。将 SSL 与 Java 应用程序配合使用可确保数据的加密，包括在客户机和服务器之间传递的用户标识和密码。可以使用数字证书管理器（DCM）配置已注册的 Java 程序来使用 SSL。

Java servlet

Servlet 是用 Java 编写的服务器端组件，可动态扩展 Web 服务器的功能而不必更改 Web 服务器代码。包括在 IBM Web Enablement for i5/OS 中的 IBM WebSphere® Application Server 提供在 i5/OS 操作系统上使用 servlet 的支持。

必须对系统使用的 servlet 对象使用资源安全性。然而，对 servlet 应用资源安全性并不足以保护 servlet。Web 服务器装入 servlet 后，资源安全性就不能防止其他人也运行该 servlet。因此，除了使用 HTTP Server 安全性控件和伪指令之外，还需要使用资源安全性。例如，不要允许 servlet 仅在 Web 服务器的概要文件下运行。还需要使用由 servlet 开发工具（如在 WebSphere Application Server for i5/OS 中所找到的）提供的安全性功能。

查看以下资源以了解有关 Java 的一般安全性措施的更多信息:

- IBM Developer Kit for Java: Java 安全性。
- IBM Toolbox for Java: 安全性类。
- 因特网浏览器的安全性注意事项。

对资源的 Java 认证和授权

IBM Toolbox for Java 包含安全性类，用于提供用户标识认证，并可选择将该标识指定给在 i5/OS 操作系统上运行的应用程序或 servlet 的操作系统线程。资源安全性的后续检查以已分配的身份进行。

IBM Developer Kit for Java 为 Java 认证和授权服务（JAAS）提供支持，JAAS 是 Java 2 Software Development Kit（J2SDK）标准版的标准扩展。目前，J2SDK 提供访问控制，这种控制基于代码的产生源和代码的签署者（基于代码源的访问控制）。

使用 SSL 保护 Java 应用程序

可使用安全套接字层（SSL）保护您使用 IBM Developer Kit for Java 开发的 i5/OS 应用程序的通信。使用 IBM Toolbox for Java 的客户机应用程序也可以利用 SSL。对您自己的 Java 应用程序启用 SSL 的过程与对其他应用程序启用 SSL 的过程有点不同。

相关概念

第 14 页的『Web 服务安全性』
在向访问者提供 Web 站点访问时，不要将关于如何设置站点和生成页面所使用的编码信息暴露给浏览者。只需要让这些访问者轻松、迅速又顺利地访问您的页面，将所有工作放在后台进行。

配置 DCM

认证服务

相关信息

Java 认证和授权服务

安全套接字层（SSL）

电子邮件安全性

在因特网或其他不可信网络间使用电子邮件会暴露系统的安全性风险，即使系统受到防火墙的保护也是如此。

您必须了解这些风险以确保您的安全策略描述了如何将这些风险降到最低。

电子邮件同其他通信形式一样。通过电子邮件发送任何机密信息之前先要进行判断，这点很重要。因为在收到电子邮件之前，它经过了许多系统传送，他人很可能拦截并阅读您的电子邮件。因此，您可能要使用安全性措施来保护电子邮件的机密性。

常见电子邮件安全性风险

以下是使用电子邮件所存在的一些风险:

- **溢流**（一种拒绝服务攻击）在系统有多个电子邮件消息而变得过载时发生。攻击者很容易便能创建一个简单的程序，将数百万个电子邮件消息（包括空消息）发送给单个电子邮件服务器以试图使该服务器发生溢

流。如果没有正确的安全性，那么目标服务器就可能由于其存储磁盘被填充无用的消息而遭受到拒绝服务攻击。系统也可能由于所有系统资源都参与处理来自攻击源的邮件而停止响应。

- **垃圾邮件**（垃圾电子邮件）是另一种常见的电子邮件攻击类型。随着通过因特网提供电子商务业务量的增长，我们收到了大量不需要或未请求的商务性电子邮件。这就是垃圾邮件，这类邮件发送给涵盖范围很广的分发列表上的电子邮件用户，占满了每个用户的电子邮件箱。
- **机密性**是一种通过因特网将电子邮件发送给另一人时存在的风险。此电子邮件到达预期的收件人手中之前，要通过许多系统。如果未对消息加密，黑客就可能在传输路径上的任何位置拦截并阅读您的电子邮件。

电子邮件安全性选项

要预防溢流及垃圾邮件的风险，必须正确配置电子邮件服务器。大多数服务器应用程序提供了对付这些攻击类型的方法。还可以与因特网服务提供商（ISP）合作以确保 ISP 提供一些免受这些攻击的附加保护。

所需要的附加安全性措施取决于所需要的机密性级别，以及电子邮件应用程序提供的安全性功能。例如，保持电子邮件消息内容的机密性是否就足够了？或者您是否希望保持与电子邮件关联的所有信息（如源及目标 IP 地址）足够的机密性?

一些应用程序集成了可以对您提供所需要保护的安全性功能。例如，Lotus Notes® Domino® 提供一些集成安全性功能，包括对整个文档或者文档的个别字段提供加密功能。

为了加密邮件，Lotus Notes Domino 对每个用户都创建了唯一的公用密钥和专用密钥。可以使用专用密钥对消息进行加密，以便该消息只对那些拥有公用密钥的用户可读。必须将公用密钥发送至预期的消息接收方，以便他们能够使用该公用密钥对加密的消息进行解密。如果他人向您发送了加密的邮件，那么 Lotus Notes Domino 将使用发送方的公用密钥为您解密该消息。

可以在程序的联机帮助文件中查找有关使用这些 Notes® 加密功能部件的信息。

如果您希望对在分支办事处、远程客户机或者业务合作伙伴之间流动的电子邮件或者其他信息提供更高机密性，有几种选择。

如果电子邮件服务器应用程序支持安全套接字层（SSL），那么可使用它创建在服务器与电子邮件客户机之间的安全通信会话。当编写客户机应用程序以使用 SSL 时，SSL 也对可选的客户端认证提供支持。由于整个会话是加密的，因此 SSL 也确保数据传输时的数据完整性。

另一种可用的选择是配置虚拟专用网（VPN）连接。可使用系统配置各种 VPN 连接，包括远程客户机与系统之间的连接。使用 VPN 时，在通信端点之间流动的所有流量都被加密，这样可确保数据机密性与数据完整性。

相关概念

第 18 页的『FTP 安全性』
文件传输协议（FTP）提供了在客户机（另一系统上的用户）与服务器之间传输文件的功能。您需要了解使用 FTP 时可能遇到的安全性风险，以确保安全性策略能够描述如何将风险降至最低。

第 3 页的『安全性的分层防御方法』
安全性策略会定义要保护的对象以及对系统用户的期望。

虚拟专用网（VPN）

相关参考

安全性术语

相关信息

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 安全性

文件传输协议（FTP）提供了在客户机（另一系统上的用户）与服务器之间传输文件的功能。您需要了解使用 FTP 时可能遇到的安全性风险，以确保安全性策略能够描述如何将风险降至最低。

可使用远程命令功能向服务器提交命令。因此，FTP 对使用远程系统或在系统之间移动文件非常有用。然而，在因特网上或者其他不可信的网络上使用 FTP 会使您面临某些安全性风险。了解这些风险可帮助您保护系统。

- 当系统上允许 FTP 时，您的对象权限方案可能不能提供足够的保护。

  例如，对象的公共权限可能是 *USE，但是您现在正在通过使用菜单安全性防止大多数用户访问那些对象。（菜单安全性防止用户做不在其菜单选项中的任何事情。）由于 FTP 用户不受菜单的限制，他们可以读取您系统上的所有对象。

  以下是控制此安全性风险的一些选项:

  – 在系统上实施全面的 i5/OS 对象安全性（换句话说，将系统的安全性模式从菜单安全性更改为对象安全性。它是最好的且最安全的选项）。
  – 编写 FTP 的出口程序以限制对可能通过 FTP 传送的文件进行访问。这些出口程序需要至少提供与菜单程序提供的安全性等同的安全性。您可能希望使 FTP 访问控制受到更多的限制。此选项仅适用于 FTP，而不适用于开放式数据库连接（ODBC）、分布式数据管理（DDM）或分布式关系数据库体系结构（DRDA®）之类的其他接口。

    注: 文件的 *USE 权限允许用户下载该文件。文件的 *CHANGE 权限允许用户上载该文件。
- 黑客可能对您的 FTP 服务器进行拒绝服务攻击，以禁用系统上的用户概要文件。通过重复尝试使用用户概要文件的错误密码登录直到该用户概要文件被禁用，来实现攻击。如果这种类型攻击的注册数达到最大次数 3 次，概要文件就会被禁用。

  要避免这类风险，您所能做的是分析对希望增强安全性以使攻击最小化与向用户提供轻松访问之间的权衡方案。FTP 服务器通常实施 QMAXSIGN 系统值以防止黑客无限次尝试猜测密码，从而进行密码攻击。以下是您需要考虑使用的一些选项:

  – 使用 FTP 服务器登录出口程序，以拒绝任何系统用户概要文件和指定不允许 FTP 访问的那些用户概要文件的登录请求。（使用这样的出口程序时，对于不允许的用户概要文件，服务器登录出口点拒绝的尝试登录的次数不计入概要文件的 QMAXSIGN 计数。）
  – 使用 FTP 服务器登录出口程序以限制允许给定的用户概要文件访问 FTP 服务器的客户机。例如，如果允许“财务部”的一个人访问 FTP，那么只允许该用户概要文件从具有“财务部”IP 地址的计算机访问 FTP 服务器。
  – 使用 FTP 服务器登录出口程序以记录进行所有 FTP 登录尝试的用户名和 IP 地址。定期查看这些记录，当概要文件被最大密码尝试数禁用时，使用该 IP 地址信息以识别作恶者并采取适当的措施。
  – 使用侵入检测系统检测系统上的拒绝服务攻击。

另外，可以使用 FTP 服务器出口点对临时用户提供匿名 FTP 功能。安装安全且匿名的 FTP 服务器同时要求 FTP 服务器登录和 FTP 服务器请求确认出口点的出口程序。

可以使用安全套接字层（SSL）对您的 FTP 服务器提供安全的通信会话。使用 SSL 确保所有的 FTP 传输是加密的以维护 FTP 服务器与客户机之间传输的所有数据（包括用户名和密码）的机密性。FTP 服务器也支持使用数字证书进行客户机认证。

除了这些 FTP 选项之外，您可能还要考虑使用匿名 FTP 以为用户提供一种轻松便捷地访问非机密资料的方法。匿名 FTP 启用对有关远程系统的选定信息的未保护访问（无需密码）。远程站点决定可用于一般访问的信息。此类信息被视为可公共访问的信息，且可由任何人阅读。在配置匿名 FTP 之前，应权衡安全风险并考虑使用出口程序保护您的 FTP 服务器。

相关概念

第 16 页的『电子邮件安全性』

在因特网或其他不可信网络间使用电子邮件会暴露系统的安全性风险，即使系统受到防火墙的保护也是如此。

相关任务

配置匿名文件传输协议

使用文件传输协议出口程序来管理访问

相关信息

保护 FTP

使用 SSL 保护 FTP 服务器

传输的安全性选项

为了在不可信网络（如因特网）上传输数据时保护数据，应采取适当的安全性措施。这些措施包括安全套接字层（SSL）、System i Access for Windows 和虚拟专用网（VPN）连接。

记住 JKL 玩具公司方案有两个主要系统。他们将一个系统用于开发，另一个系统用于生产应用程序。这两个系统都处理关键任务数据和应用程序。因此，他们选择了在周边网络上添加新的系统以处理其内部网应用程序和因特网应用程序。

建立周边网络以确保在内部网与因特网之间具有某些物理隔离。这种隔离降低了公司内部系统容易遭受到来自因特网攻击的风险。通过将新的系统指定为纯因特网服务器，公司也降低了管理其网络安全性的复杂性。

由于对因特网环境安全性的普遍要求，IBM 仍在不断地开发安全性产品，以确保在因特网上实施电子商务的安全联网环境。在因特网环境下，必须确保同时提供特定于系统及特定于应用程序的安全性。然而，通过企业内部网或者因特网连接传输机密信息，更增加了对制订更强的安全性解决方案的要求。为抵抗这些风险，需要采取安全性措施以保护在因特网上传输的数据。

可使用 i5/OS 操作系统的两种特定传输级别安全性产品（SSL 安全通信和 VPN 连接）将有关在不可信系统之间移动信息的风险降至最低。

SSL 协议是保护客户机与服务器之间的通信的业界标准。SSL 最初是为 Web 浏览器应用程序开发的，但是现在越来越多的其他应用程序也能使用 SSL。对于 i5/OS 操作系统，它们包括:

- IBM HTTP Server for i5/OS（最初由 Apache 开发并提供支持）
- FTP 服务器
- Telnet 服务器
- 分布式关系数据库体系结构（DRDA）与分布式数据管理（DDM）服务器
- System i 导航器中的中央管理
- 目录服务服务器（LDAP）

- System i Access for Windows 应用程序，包括 System i 导航器以及写至应用程序编程接口（API）的 System i Access for Windows 集合的应用程序
- 用 Developer Kit for Java 开发的程序和使用 IBM Toolkit for Java 的客户机应用程序
- 用可以在应用程序上用来启用 SSL 的安全套接字层（SSL）应用程序可编程接口（API）开发的程序。有关如何编写使用 SSL 的程序的更多信息，请参阅安全套接字层 API。

这些应用程序中的一些程序还支持使用数字证书进行客户机认证。SSL 依靠数字证书对通信各方进行认证并创建安全连接。

虚拟专用网

可以使用 VPN 连接在两个端点之间建立安全通信信道。像 SSL 连接一样，可以对在端点之间传输的数据加密，因而可以同时提供数据机密性与数据完整性。然而，VPN 连接允许限制流动到指定端点的流量并限制可以使用该连接的流量类型。因此，VPN 连接通过帮助保护网络资源免受未授权者的访问，提供某种网络级别的安全性。

您应该使用哪种方法

SSL 和 VPN 都可满足安全认证、数据机密性和数据完整性的需要。您应该使用这些方法中的哪种方法，取决于以下几个因素。您需要考虑的因素包括：您正在与谁通信、与其通信所使用的应用程序、需要通信的安全级别和为保护此通信而在成本和性能之间做出的权衡。

另外，如果您希望特定的应用程序与 SSL 配合使用，那么必须将该应用程序设置为使用 SSL。尽管许多应用程序不能使用 SSL，但许多其他应用程序（如 Telnet 和 System i Access for Windows）已具有 SSL 功能。然而，VPN 允许保护在特定连接端点之间流动的所有 IP 流量。

例如，当前可以通过 SSL 使用 HTTP 以允许业务合作伙伴与内部网络上的 Web 服务器通信。如果 Web 服务器是在您与业务合作伙伴之间所需的唯一安全应用程序，那么您可能不希望切换至 VPN 连接。然而，如果您希望扩展通信，那么可能要使用 VPN 连接。另外，可能有需要保护部分网络中的流量的情况，但是不希望为使用 SSL 单独配置每个客户机和服务器。可以对网络的该部分创建网关至网关的 VPN 连接。这种 VPN 连接可保护流量，但是对该连接任一端上单独的客户机和服务器来说，该连接是透明的。

相关概念

第 3 页的『安全性的分层防御方法』
安全性策略会定义要保护的对象以及对系统用户的期望。

第 6 页的『方案：JKL 玩具公司电子商务计划』
一个典型方案是 JKL 玩具公司，该公司决定使用因特网扩展其业务目标，这可能对您设置您自己的电子商务方案有所帮助。

相关参考

安全套接字 API

相关信息

安全套接字层（SSL）

虚拟专用网（VPN）

对 SSL 使用数字证书

数字证书是使用安全套接字层（SSL）进行安全通信的基础并作为一种更强的认证手段。

i5/OS 操作系统使您能够轻松地使用数字证书管理器（DCM）创建和管理系统和用户的数字证书，DCM 是 i5/OS 集成功能。

另外，可配置一些应用程序（如 IBM HTTP Server for i5/OS），以将数字证书用作代替用户名和密码的更强的客户机认证方法。

数字证书是什么

数字证书是一种验证证书所有者身份的数字凭证，类似于护照的功能。称为认证中心（CA）的可信第三方向用户和服务器发出数字证书。信任 CA 是信任证书即为有效凭证的基础。

每个 CA 都有一个策略来确定为发出证书 CA 所需要标识的信息内容。某些因特网 CA 可能需要很少的信息（例如，只需要专有名称）。它是 CA 向其发出数字证书地址和数字电子邮件地址的个人或系统的名称。为每个证书生成一个专用密钥和一个公用密钥。证书包含公用密钥，而浏览器或安全文件则存储专用密钥。与证书相关联的密钥对可用来签署并加密数据（如在用户和服务器之间发送的消息和文档）。这种数字签名确保项的来源的可靠性并保护该项的完整性。

尽管许多应用程序不能使用 SSL，但许多其他应用程序（如 Telnet 和 System i Access for Windows）已具有 SSL 功能。

相关概念

配置 DCM

安全套接字层（SSL）

相关参考

安全性术语

使用安全套接字层保护 Telnet 访问

可以将 Telnet 服务器配置为使用安全套接字层（SSL）以保护 Telnet 通信会话。

要配置 Telnet 服务器以使用 SSL，必须使用数字证书管理器（DCM）配置证书供 Telnet 服务器使用。缺省情况下，Telnet 服务器处理安全与非安全的连接。然而，可以配置 Telnet 以便它只允许安全 Telnet 会话。另外，可以配置 Telnet 服务器以使用数字证书进行更强的客户机认证。

在选择对 Telnet 使用 SSL 时，您将获得一些强安全性的好处。对于 Telnet，除服务器认证外，数据在任何 Telnet 协议数据流动之前就可加密。建立 SSL 会话后，对所有 Telnet 协议（包括用户标识和密码交换）进行加密。

使用 Telnet 服务器时，要考虑的最重要的因素是在客户机会话中所使用的信息的敏感性。如果信息是敏感的或专用的，那么您可能会发现使用 SSL 设置 Telnet 服务器是很有好处的。对 Telnet 应用程序配置数字证书时，可通过 SSL 与非 SSL 客户机运行 Telnet 服务器。如果安全策略要求总是对 Telnet 会话加密，那么可禁用所有非 SSL 的 Telnet 会话。不需要使用 SSL Telnet 服务器时，可关闭 SSL 端口。借助“更改 Telnet 属性”（CHGTELNA）命令和“允许使用安全套接字层”（ALWSSL）参数，可控制使用 SSL 保护 Telnet 会话。为了确保在适当时没有应用程序能够使用 SSL 或非 SSL 端口，还可使用“添加 TCP/IP 端口限制”（ADDTCPPORT）命令进行限制。

为便于您了解 Telnet 以及使用和不使用 SSL 保护 Telnet 的安全性技巧的更多信息，有关 Telnet 的 IBM Systems Software Information Center 主题提供了在 i5/OS 操作系统上使用 Telnet 时所需的信息。

相关概念

Telnet 方案: 使用 SSL 保护 Telnet

规划 DCM

相关信息

Telnet

使用安全套接字层保护 System i Access for Windows

要保护 System i Access for Windows 通信会话，可将 System i Access for Windows 配置为使用安全套接字层（SSL）。

使用 SSL 可确保对 System i Access for Windows 会话的所有通信数据进行加密。它防止数据在本地与远程主机之间传输时被他人读取。

相关信息

安全套接字层管理

Java 安全性

安全性类

使用虚拟专用网保护专用通信

虚拟专用网（VPN）是公司内部网基于公用或专用网络的扩展，可帮助您在公司内部以专用方式安全通信。

随着 VPN 的使用及其提供的安全性的增加，JKL 玩具公司正在研究通过因特网传输数据的选项。他们最近收购了另一家小型玩具制造公司，打算将其作为子公司来经营。JKL 将需要在这两个公司之间传递信息。两家公司都使用 i5/OS 操作系统和 VPN 连接，它们能提供在两个网络之间通信所需的安全性。创建 VPN 比使用传统非交换线路更合算。

以下是一些可能从使用 VPN 连接获益的用户:

- 远程用户和移动用户。
- 总公司到分支办事处或其他非现场位置。
- 企业到企业的通信

如果不限制用户访问敏感系统，就会发生安全性风险。如果不限制可以访问系统的用户，就会增加公司信息不能保密的可能性。需要制订一个计划，仅允许那些需要共享系统信息的用户访问该系统。VPN 提供重要的安全性功能（如认证和数据保密性）的同时还允许您控制网络流量。创建多个 VPN 连接允许对每个连接控制谁可以访问哪些系统。例如，“财务部”和“人力资源部”可以通过其自己的 VPN 链接在一起。

当允许用户通过因特网连接到系统时，可能会通过公用网络发送敏感的企业数据，从而使这些数据暴露于攻击之下。保护传输的数据的一种选择是使用加密和认证方法确保数据对于无关人员来说是保密和安全的。VPN 连接为特定安全性要求提供了解决方案: 保护系统之间的通信。VPN 连接为在连接的两个端点之间流动的数据提供保护。另外，还可以使用信息包规则安全性定义允许什么 IP 信息包通过 VPN。

可以使用 VPN 创建安全连接来保护在受控的和可信的端点之间流动的流量。然而，您还必须知道对 VPN 伙伴提供了多少访问。当数据在公用网络上传输时，VPN 连接可以加密该数据。但是，通过因特网流动的数据可能无法通过 VPN 连接传输，这取决于配置 VPN 连接的方式。在这种情况下，当数据在通过该连接进行通信的内部网络上流动时，可能不加密这些数据。因此，应该仔细规划设置每个 VPN 连接的方式。确保只允许 VPN 伙伴访问那些希望他们访问的内部网络上的主机或资源。

例如，可能有某位供应商需要得到有关您库存有哪些部件的信息。可以在内部网上在用于更新 Web 页面的数据库中获得此信息。您想允许这位供应商通过 VPN 连接直接访问这些页面。但并不希望该供应商能够访问其他系统资源（如数据库自身）。您可以配置 VPN 连接，以便将两个端点之间的流量限制在端口 80 上。端口 80 是 HTTP 流量使用的缺省端口。因此，您的供应商只能通过该连接发送和接收 HTTP 请求和响应。

由于可以限制通过 VPN 连接流动的流量类型，因此该连接提供了一种网络级别安全性方法。然而，VPN 控制进出系统流量的工作方式与防火墙不同。另外，VPN 连接并不是保护 i5/OS 操作系统和其他系统间通信的唯一可用的方法。根据您的安全性要求，可能会发现使用 SSL 是一种更合适的方法。

VPN 连接是否能提供您所需要的安全性，取决于您希望保护什么。另外还取决于为了提供该安全性希望所做的权衡方案。象对有关安全性所做的任何决定一样，应该考虑 VPN 连接如何才能实现支持安全策略。

相关概念

第 2 页的『System i 与因特网安全性注意事项』

有关因特网的安全性问题是很重要的。本主题概述 i5/OS 的安全性优点及安全性产品。

虚拟专用网（VPN）

附录. 声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往:

IBM Director of Licensing
IBM CorporationNorth Castle DriveArmonk, NY 10504-1785
U.S.A.

有关双字节（DBCS）信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-kuTokyo 106-0032, Japan

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区: International Business Corporation “按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证，因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本资料中描述的产品和／或程序进行改进和／或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: （i）允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及（ii）允许对已经交换的信息进行相互使用，请与下列地址联系:

IBM CorporationSoftware Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本文档中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议、IBM 机器代码许可协议或任何同等协议中的条款提供。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的，实际结果可能会有差异。本文档的用户应当验证其特定环境的适用数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

本信息仅用于规划目的。在所描述的产品可用之前，此处的信息可能更改。

本信息包含在日常业务经营中使用的数据和报告的示例。为了尽可能完整地说明这些示例，这些示例中可能会包括个人、公司、品牌和产品的名称。所有这些人名或名称均系虚构，如与实际商业企业使用的名称和地址有任何雷同，纯属巧合。

版权许可:

本信息包括源语言形式的样本应用程序，这些样本说明不同操作平台上的编程方法。如果是为按照在编写样本程序的操作平台上的应用程序编程接口（API）进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例并未在所有条件下进行完全测试。因此，IBM 不能担保或暗示这些程序的可靠性、可维护性或功能。

凡这些样本程序的每份拷贝或其任何部分或任何衍生产品，都必须包括如下版权声明:

©（贵公司的名称）（年）。此部分代码是根据 IBM 公司的样本程序衍生出来的。© Copyright IBM Corp. （输入年份）. All rights reserved.

如果您正以软拷贝格式查看本信息，图片和彩色图例可能无法显示。

编程接口信息

这些 System i 和因特网安全性出版物文档适用于允许客户编写程序以获取 IBM i5/OS 服务的编程接口。

商标

以下各项是 International Business Machines Corporation 在美国和／或其他国家或地区的商标:

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

Adobe、Adobe 徽标、PostScript 和 PostScript 徽标是 Adobe Systems Incorporated 在美国和／或其他国家或地区的注册商标或商标。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和／或其他国家或地区的商标。

Java 和所有基于 Java 的商标是 Sun Microsystems,Inc. 在美国和 / 或其他国家或地区的商标。

其他公司、产品和服务名称可能是其他公司的商标或服务标记。

条款和条件

如果符合以下条款和条件，那么授予使用这些出版物的准用权。

个人使用: 只要保留所有的专有权声明，您就可以为个人、非商业使用复制这些出版物。未经 IBM 明确同意，您不可以分发、展示或制作这些出版物或其中任何部分的演绎作品。

商业使用: 只要保留所有的专有权声明，您就可以仅在企业内复制、分发和展示这些出版物。未经 IBM 明确同意，您不可以制作这些出版物的演绎作品，或者在您的企业外部复制、分发或展示这些出版物或其中的任何部分。

除非本准用权中有明确授权，不得把其他准用权、许可或权利（无论是明示的还是暗含的）授予这些出版物或其中包含的任何信息、数据、软件或其他知识产权。

当使用该出版物损害了 IBM 的利益，或者根据 IBM 的规定，未正确遵守上述指导说明时，则 IBM 保留自主决定撤销本文授予的准用权的权利。

您不可以下载、出口或再出口本信息，除非完全遵守所有适用的法律和法规，包括所有美国出口法律和法规。

IBM 对这些出版物的内容不作任何保证。本出版物“按现状”提供，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的关于适销、非侵权和适用于某种特定用途的保证。

中国印刷