NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

絵で見るネットワークの脆弱性と脅威

不正プログラム調査WG
渡部　章
2005 年 6月13日

目次

 Page 2

はじめに

- 近年、不正プログラムがセキュリティ問題の中核を成していることを鑑み、特に注意を要するネットワーク上の脆弱性と脅威について、わかりやすく取りまとめた。
  - その骨組みとして攻撃頻度の高い脆弱性を技術的に取りまとめた「SANSインターネットセキュリティ脆弱性トップ20」を利用し、特筆すべき近年の脅威について追加した。
- 攻撃頻度の高い脆弱性を取り上げる理由について
  - ワームや攻撃のほとんどが、オペレーティングシステムに存在する脆弱性を悪用している。
  - 攻撃者は、よく知られている欠陥を、容易に入手可能な攻撃ツールで攻略しようとする。
  - 攻撃者は、問題を解決していない組織や、脆弱なシステムを探して無差別的に攻撃する。
- ここに上げた脆弱性と脅威について
  - 最も危険なセキュリティホールから優先順位を付けて列挙している。
  - 即座に対処が必要なものばかりである。
  - 脆弱性と脅威は常に新しいものが発生するので、最新情報を入手し対処するべきである。
- 出典： http://www.sans.org/top20/
  - The Twenty Most Critical Internet Security Vulnerabilities The Experts Consensus Version 5.0, October 8, 2004 Copyright (C) 2001-2004, SANS Institute
  - コメントや情報の連絡先：

 Page 3

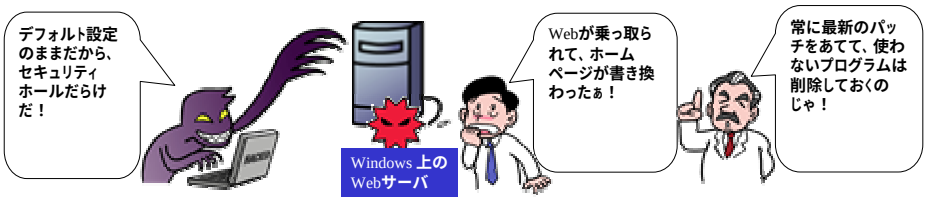
Windowsシステムでの脆弱性トップ10

1. WebサーバとWebサービス
2. Workstationサービス
3. Windowsリモートアクセスサービス
4. Microsoft SQL Server (MSSQL)
5. Windows認証
6. Webブラウザ
7. ファイル共有アプリケーション
8. LSASS
9. メールクライアント
10. インスタントメッセージ

 Page 4

1. WebサーバとWebサービス

概要	IIS、Apache、およびiPlanet（現在のSunOne）のようなHTTPサーバには多数の問題があり、デフォルト設定では攻撃を受ける余地が多分に残されている。
攻撃による影響	● サービス妨害攻撃（DoS） ● 機密ファイルまたはデータの露呈、入手 ● サーバ上での任意のコマンドの実行 ● サーバの完全な乗っ取り
対策方法	●該当サーバのすべてのパッチ更新に追従し、常に最新版が動作している状態を維持する必要がある ●設定を最適化し、Webサイトを適正に運営するために必要とされる最小機能のみを許可するようにする ●定期的にネットワークを監査し、意図しないWebサーバが存在しないかを確認する
関係する製品	Webサーバがインストールされたすべて Microsoft Windowsシステム Microsoft IIS、Apache HTTP Server、Sun Java System / Sun One / iPlanet Web Server



2. Workstationサービス

概要	Workstationサービスには、スタックベースのバッファオーバーフローの問題がある。これは、特別に細工したDCE/RPCコールによって引き起こされる。
攻撃による影響	●“SYSTEM”権限で任意のコードを実行可能 ●マシンの制御を完全に取得
対策方法	● Windowsシステムに最新のセキュリティパッチのすべてを確実に適用する ●ファイアウォールにより、ネットワークの境界部でポート139/tcpおよび445/tcpをブロックする
関係する製品	Windows 2000 SP2、SP3、SP4 / XP / XP 64-Bit Edition

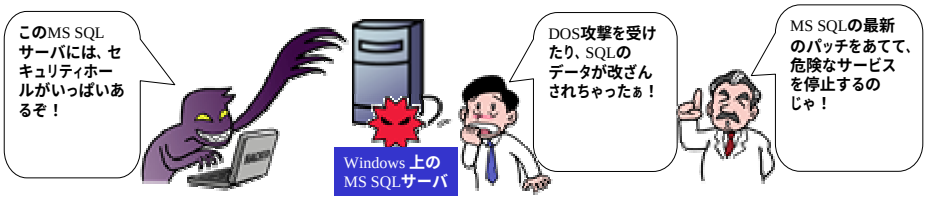
3. Windowsリモートアクセスサービス

概要	Windowsオペレーティングシステムのネットワークテクノロジには、NETBIOSネットワーク共有、匿名ログオン、NULLセッション、リモートレジストリアクセス、リモートプロシジャーコールなどが原因でセキュリティ侵害が起こされる。
攻撃による影響	●リモートでファイルを操作することができる ●重要なシステムファイルが露出される可能性がある ●悪意のあるユーザーまたはプログラムがホストを完全に制御できる可能性がある ●ユーザー、グループ、共有、およびパスワードポリシーに関する情報を表示できる
対策方法	オペレーティングシステムおよびアプリケーションのセキュリティ脆弱性に対してサービスパックおよびホットフィックスで対応する
関係する製品	Windows 95 / 98 / NT / Me / 2000 / XP / 2003

 Page 7

4. Microsoft SQL Server (MSSQL)

概要	Microsoft SQL Server (MSSQL) には、リモートアタッカーが機密情報を入手したり、データベースの内容を変更したり、SQLサーバを攻略したり、構成によってはサーバホストが完全に乗っ取られてしまうといった重大な脆弱性がいくつか含まれている。
攻撃による影響	● サービス妨害攻撃 (DoS) ●データベースのレコード改竄や情報漏洩 ● サーバの完全な乗っ取り
対策方法	● UDPポート1434上のSQL/MSDE Monitor Serviceを無効にする ● Microsoft SQL/MSDEサーバまたはMSDE 2000、あるいはその両方を対象とする最新のサービスパックおよび最新のセキュリティパッチのすべてを確実に適用する
関係する製品	Microsoft SQL/MSDE Server 7.0 Microsoft SQL Server 2000 MSDE Server Desktop Engine 2000 (MSDE 2000)



 Page 8

5. Windows認証

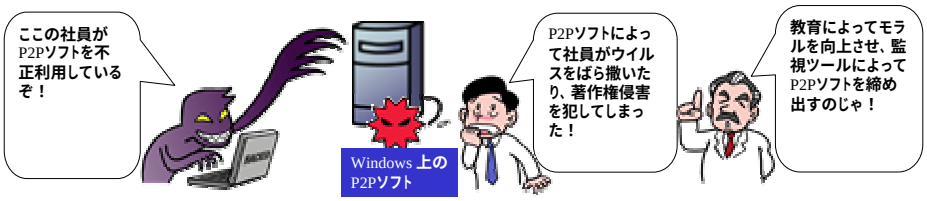
概要	Windows認証には，ネットワークを流れる認証パケットからパスワードを推測できる可能性があるなどの脆弱性が存在する．簡単なパスワードを利用するなど，パスワードの適切な管理を怠ることで，なりすまされる可能性がある．また，最近の研究ではハッシュ関数自身の脆弱性なども指摘されている．
攻撃による影響	●なりすましなど
対策方法	● 推測されにくいパスワードの利用 ● ワンタイムパスワード ● 生態認証
関係する製品	Microsoft Windowsシステムのすべて

6. Webブラウザ

概要	Microsoft Internet Explorer (IE) は、脆弱性発見からパッチ対応までの時間が長く、多数の脆弱性がパッチ未対応である。ActiveXの使用により、OSのセキュリティ構成を迂回してホストマシンを攻撃できる。Spyware/Adwareの脆弱性の影響を受けやすい。また、IEをOSカーネルに統合することにより攻撃に対するOSの脆弱性が増すなどのセキュリティ問題を抱えている。
攻撃による影響	● IEの脆弱性はWindowsの脆弱性を攻撃するために利用 ● cookieやローカルファイル、データなどの漏洩 ● ローカルプログラムの実行や任意のコードのダウンロードや実行 ● システムの完全な制御取得
対策方法	Windowsシステムに最新のセキュリティパッチのすべてを確実に適用する
関係する製品	Microsoft Internet Explorer バージョン6、Mozillaバージョン1.4〜1.7.1、Netscapeバージョン7.x Operaバージョン7.x

7. ファイル共有アプリケーション

概要	P2Pソフトウェアを使用する場合は、技術的脆弱性、社会的脆弱性、法的脆弱性の3つの脆弱性が存在する。
攻撃による影響	● 技術的脆弱性：サービス妨害攻撃、帯域幅の消費。ドライブの共有による情報漏洩の問題 ● 社会的脆弱性：ウイルス、トロイの木馬、ワーム、その他のマルウェアの生成 ● 法的脆弱性：入手できるコンテンツによる著作権侵害
対策方法	● 企業インターネット接続に関し使用方法を規定、P2Pソフトのインストール制限 ● プロキシサーバの使用、出側フィルタリングによる不要ポートへのアクセス制限 ● ネットワーク内のP2Pトラフィックの有無の監視 ● アンチウイルスソフトウェアの使用
関係する製品	現在使用されているすべてのWindowsオペレーティングシステムと、UnixおよびLinuxシステムの各バージョンで使用可能な各種バージョンのP2Pソフトウェアが存在する。



8. LSASS

概要	Windows Local Security Authority Subsystem Service (LSASS) に、バッファオーバーフローの脆弱性がある。この脆弱性が悪用された場合、完全にシステムの制御が奪われる可能性がある。
攻撃による影響	● LSASRV.dllのログ機能がオーバーフローする ●完全にシステムの制御が奪われる可能性がある ●リモートで容易に悪用できる
対策方法	● ファイアウォールでポートをブロックする ● Microsoftの最新パッチを適用する ● システムで高度なTCP/IPフィルタリングを有効にする
関係する製品	Windows 2000 / XP / XP 64-Bit Edition / 2003 Windows Server 2003 / Server 2003 64-Bit

9. メールクライアント

概要	Microsoft Outlook及びMicrosoft Outlook Expressは、Microsoft社が持っている利便性を追及する自動化機能が多くの脆弱性を産み出す結果となっている。
攻撃による影響	● ウイルスやワームによる感染 ― 組み込みスクリプトによって悪意のあるコードがまき散らされる ● スパム ― 無差別の大量Eメール ● Webビーコン：メールの受取人がメッセージを開くことにより、Eメールアドレスが確認される
対策方法	● アプリケーションの最新のセキュリティパッチのすべてを確実に適用する ● 設定オプションの［セキュリティ］を［高］に設定し、その他に、プレビュー機能をOFFにする ● 実行ファイルの拡張子を持つ添付ファイルのブロックを設定 ● HTML電子メール内のコンテンツ自動的ダウンロード機能のOFF
関係する製品	Microsoft Windowsの全バージョン Microsoft Officeがインストールされたマシン

10. インスタントメッセージ

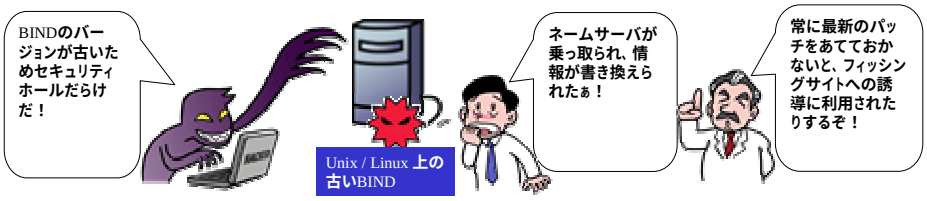
概要	インスタントメッセージは Windows上で動作するアプリケーションである以上、バッファオーバフローなどの脆弱性を持つ可能性は常にある．また，近年ユーザの拡大が著しいインスタントメッセージはウイルスの感染手段となる可能性もある．
攻撃による影響	● リモートから任意のコマンドの実行 ● サービス停止など
対策方法	● パッチを適用し最新を維持する ● パッチを適用しないユーザへサービスの制限(サーバ側での対策)
関係する製品	Windows Messenger MSN Messenger Yahoo Messenger AOL Instant Messenger

Unixシステムでの脆弱性トップ10

1. BINDドメインネームシステム
2. Webサーバ
3. 認証
4. バージョン管理システム
5. メール転送サービス
6. Simple Network Management Protocol (SNMP)
7. Open Secure Sockets Layer (SSL)
8. エンタープライズサービスNIS/NFSの設定ミス
9. データベース
10. カーネル

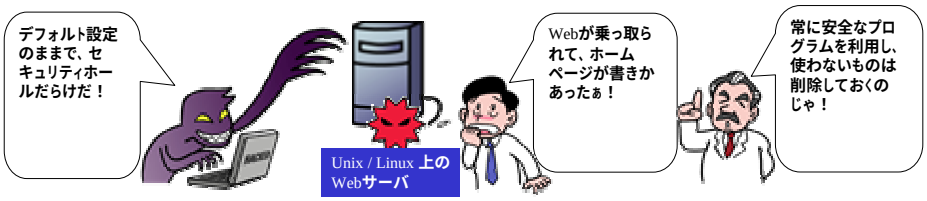
1. BINDドメインネームシステム

概要	BINDドメインネームシステムは世界で最も普及しており、頻繁に攻撃の標的となっている。常に最新バージョンが提供されているが、期限切れ、設定ミス、脆弱性などがあるサーバが依然として稼動している。
攻撃による影響	サービス妨害攻撃 (DOS) を引き起こしネーミングサービスを停止させる。またバッファオーバーフローやDNSキャッシュ汚染を実施する。システムの悪用や踏み台攻撃に利用する
対策方法	● セキュリティ警告レポートの購読または勧告を遵守する ● 最新の脆弱性スキャナにより脆弱性を診断する ● DNSサーバではないシステム上ではBINDデーモンを無効にする ● すべてのパッチを適用し、DNSサーバを最新バージョンにアップグレードする
関係する製品	BINDのバージョンと一緒に配布するUnixシステムおよびLinuxシステム Windows対応のBINDにも存在する。



2. Webサーバ

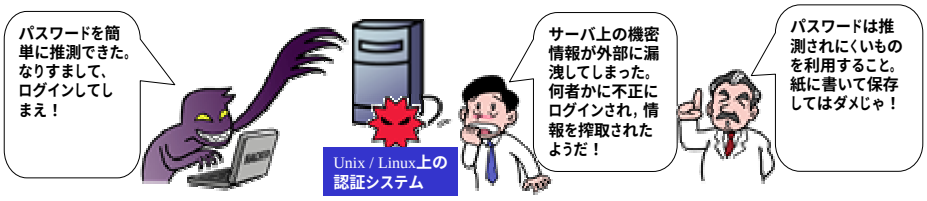
概要	Webサーバ自体の脆弱性の他、アドオンモジュールなどその他の脆弱性を攻撃される可能性がある。 システムをインストールした時の設定ミスおよび定期保守の未実施による脆弱性を攻撃される可能性がある。
攻撃による影響	●サービス妨害攻撃（DoS） ●ウェブサイトの書き換え ●サーバの完全な乗っ取り
対策方法	●ベンダなどから提供される製品のセキュリティ更新を適用し最新状態を保つ ●設定を最適化する
関係する製品	UNIXおよびLinuxシステム ApacheおよびiPlanet/Java Systemをインストールした Windowsなどのその他のOS



 Page 17

3. 認証

概要	認証の形式とファイルおよびデータ保護は、ユーザーまたはベンダが指定したパスワードに大きく依存している。パスワードには一般的な脆弱性がある。
攻撃による影響	● 破ったパスワードを利用することで、検知されることなく、システムを内部から探索することができる ● アタッカーはユーザーの利用可能な任意リソースへの完全なアクセスが可能となり、 さらに他のアカウント、他のマシン、そしておそらく管理者権限にさえアクセスできる可能性がある
対策方法	● パスワードを確実に強力にして保護する ● アカウントを厳密に管理して、ログインを暗号化 する ● 監査証跡
関係する製品	パスワードを使用するすべての認証システム



 Page 18

4. バージョン管理システム

概要	バージョン管理システムConcurrent Versions System (CVS)と、Subversionは、一度、攻撃を受けると、バックドアやバグを用いてソースファイル等に感染できるので、2次的な被害を引き起こす危険性がある。
攻撃による影響	● “Entry-Lines” により、ヒープ型のバッファオーバーフローを引き起こされる ● 脆弱性がアタッカーの悪用により、CVSサービス妨害、CVSサーバで任意のコードが実行される ● "get-dated-rev" svnコマンドにより、スタック型のバッファオーバーフローが引き起こされる
対策方法	● CVS/ Subversionソフトウェアにパッチを適用し最新を維持する ● リモートアクセスには、SSHプロトコルを使用し、"chroot"環境でCVSサーバを稼動する ● 社内/企業内ネットワーク境界ではポート2401/tcpをブロックし、ポート3690/tcpへのアクセスをブロックする ● 匿名アクセスについては読み込みアクセスのみを許可するように設定する ● "svn"プロトコルを使用するのでなく、webDAVからSubversionリポジトリをアクセスするように設定する
関係する製品	Linux、FreeBSD、AIX、HP-UX、Solaris、SGI等のCVS、Subversionを実行できるオペレーティングシステム

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 19

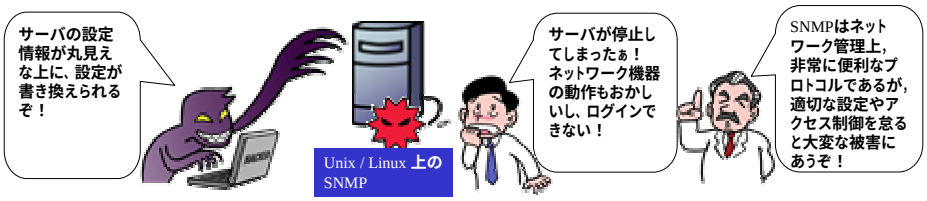
5. メール転送サービス

概要	メール転送サービスにおける MTAは，自身の持つ脆弱性に関するもの，設定ミスによる不正中継，迷惑メールなどさまざまな危険にさらされている。
攻撃による影響	●リモートから任意のコマンドの実行 ●サービス停止 ●不正中継，迷惑メール送信の幇助，コンピュータやネットワーク資源の浪費
対策方法	●パッチを適用し最新を維持する ●ファイアウォールポリシーを適用 ●内部メールトラフィックを処理する内部 MTAを設置 ●権限レベルを制限しその権限の下でMTAを実行するか，chroot環境の利用
関係する製品	Sendmail、qmail、Exim、Postfix

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 20

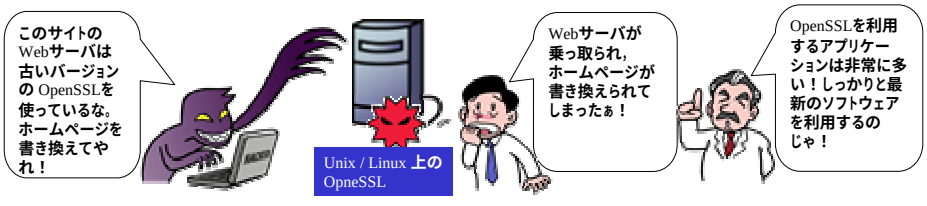
6. Simple Network Management Protocol (SNMP)

概要	Simple Network Management Protocol (SNMP)の通信で利用されているメッセージの処理方法と認証メカニズムには重大な脆弱性が存在している。
攻撃による影響	● サービス妨害攻撃によるシャットダウンや、SNMP対応マシンへリモートで不正な設定や管理が可能 ● SNMPトラフィックが盗聴され、ネットワーク構造および接続されているシステムの情報が露出
対策方法	● SNMPが必須でなければ、それを無効にする ●パッチを適用し最新を維持する ● ネットワークへの入口でSNMPをフィルタリングする ● SNMPエージェントシステムでホストベースのアクセス制御を採用する
関係する製品	SNMPがインストールされたUnixおよびLinuxシステム 他のSNMP対応ネットワークデバイスとオペレーティングシステム



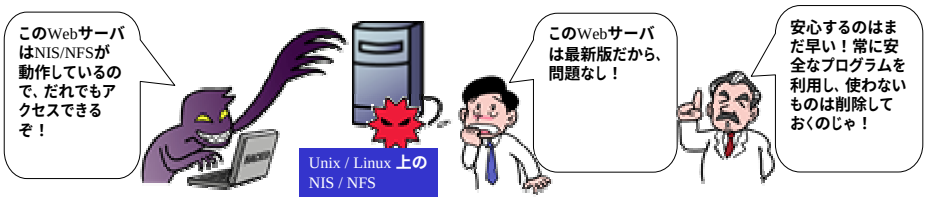
7. Open Secure Sockets Layer (SSL)

概要	OpenSSLライブラリでは複数の脆弱性が発見されている。 OpenSSLライブラリが多数のアプリケーションに統合されているので、こうしたアプリケーションを通してライブラリに内在する脆弱性が悪用される。
攻撃による影響	リモートからOpenSSLライブラリの脆弱性を攻撃することで、OpenSSLライブラリを使用するアプリケーションの特権レベルを用いて任意のコードが実行される
対策方法	● OpenSSLを最新バージョンにアップグレードする ● ファイアウォールツールを使用し、OpenSSLを有効にしたサーバへの接続を制限する
関係する製品	0.9.7c以前、0.9.61以前のバージョンのOpenSSLを実行しているUnixまたはLinuxシステム



8. エンタープライズサービス NIS/NFSの設定ミス

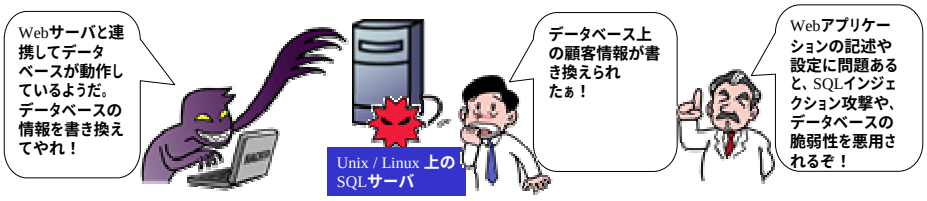
概要	Network File System (NFS)およびNetwork Information Service (NIS)のサービスには、バッファオーバーフロー、DoSおよび脆弱な認証の問題があり、攻撃の対象になる。NFS/NISサービスの設定ミスが原因である。
攻撃による影響	●セキュリティホールは容易に攻略されユーザーによってローカルからもリモートからも容易にアクセス可能 ●パスワードファイルを取り出すことが可能 ●サーバの設定によっては任意のユーザーがリモートファイルシステムをマウントし探索することが可能
対策方法	● NISクライアント上で、パスワードファイル内に必ず+:*:0:0:::を含める ● NFSファイルシステムへのアクセスを制限し、SSHのような安全なプロトコルを使用 ● ファイアウォールポリシーで、不要なすべてのポートを必ずブロックする ● NIS/NFSサーバを最新のバージョンに更新する ● NFS/NISサーバになることが認証されていないシステム上ではNFS/NISデーモンを無効にする
関係する製品	Unixシステムおよびバージョンの、NFS/NISのバージョンがインストールされたシステム



Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 23

9. データベース

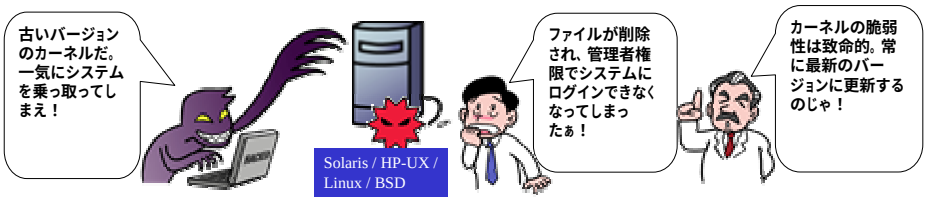
概要	データベースは極めて複雑なアプリケーションであり、正しく設定し安全性を保つことが困難な場合が多い。多数のデータベースでは、特徴と機能の集まりが悪用され、データの機密性、可用性、および整合性が損なわれている。基本データベースを損なうような脆弱性がOracleやMySQLに複数存在する。
攻撃による影響	●データベースアプリケーションには、リソースおよびテーブルに各種レベルでアクセスできる。 ●大部分のデータベースはフロントエンドアプリケーション、ウェブベースアプリケーションと緊密に結ばれているため、アプリケーションの記述、設定に不手際があると、アタッカーがSQLインジェクション攻撃を仕掛けるか、データベース脆弱性の一部を悪用できる
対策方法	●パッチを適用し最新を維持する ●データベースシステムや連携しているアプリケーションの設定が適切に行われているかを確認する
関係する製品	Oracle、MySQL、PostgreSQL



Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 24

10. カーネル

概要	カーネルとはその名の通り，オペレーティングシステムの中核をなす部分である． カーネルは特権モードで動作するため，カーネルに関する脆弱性は甚大な被害を招く可能性が高い．
攻撃による影響	●特権ユーザでの任意のコードの実行 ●サービス妨害 ●LKM Rootkit
対策方法	●パッチを適用し最新を維持する ●カーネルパラメータのチューニング ● Rootkit検査ツール
関係する製品	Solaris、HP-UX、Linux、BSD



その他の脆弱性および脅威

1. フィッシング詐欺
2. スパイウェア
3. ボット

1. フィッシング詐欺

概要	金融機関などの正規のメールを偽装して、ユーザを偽のWebサイトに誘導し、暗証番号やクレジットカード番号などの個人情報を不正に入力させて利用する詐欺行為のこと。Internet Explorerなどの脆弱性を悪用し、本物のURLを表示させるなど手の込んだ偽装も少なくない。
攻撃による影響	●個人名義サービスの不正利用 ●金銭詐欺。
対策方法	●Internet Explorerの脆弱性への修正プログラムを利用する。 ●メールの送信者欄を信用しない。 ●不用意にWebページでクレジット･カード番号や暗証番号などを入力しない。 ●フォームの送受信にSSLが利用されているか確認する。 ●正規の電話窓口やWebページなどから案内が本物かどうかを確認する。 ●別のブラウザで正規のURLを入力してアクセスする。
関係する製品	メールソフト、ブラウザ

 Page 27

2. スパイウェア

概要	ユーザの行動や個人情報などを収集するアプリケーションソフト。他のアプリケーションソフトとセットで配布されたり、メール添付やWeb閲覧中に侵入されたり、盗聴目的で第三者によってインストールされる。また、バックグラウンドで動作するため活動に気づきにくい。
攻撃による影響	● セキュリティの侵害、ユーザの個人情報の漏洩、ユーザのキー操作、画面、Web閲覧履歴の漏洩 ● パフォーマンスの低下、CPUやメモリ リソースの消費、不要なポップアップによる操作性の低下、バグによるシステムの不安定化
対策方法	● インストール時に表示される利用条件の確認 ● ブラウザによるActiveXやJavaの制限 ● ウイルス対策ソフト、スパイウェア対策ソフト、パーソナルファイアウォールの利用
関係する製品	メールソフト、ブラウザ、スパイウェアを含む一般アプリケーション

 Page 28

3. ボット(ゾンビ、悪質エージェント)

概要	ウイルスやトロイの木馬としてマシンに侵入し、外部からそのマシンを操って被害を与えたり悪用できるようにするための攻撃プログラム。 ボットという言葉は「ロボット(Robot)」から来ている。 同義語として、「ゾンビ」や「悪質エージェント」がある。
攻撃による影響	●インストールされたマシンを外部から自由に操作される。 ●複数のボットが協調して動作すれば、DDOS攻撃やスパム送信が可能となる。このような複数のボットで構成した仮想的なネットワークをボットネットとか、ボットネットワークと呼ぶ。
対策方法	● 信頼できないファイルは開かない、信頼できないリンクはクリックしない。 ● セキュリティ・ホールをふさぐ。 ● パスワードをきちんと管理する。 ● 不要なポート、不要なサービスは止める。 ● ウイルス対策ソフト、スパイウェア対策ソフト、パーソナルファイアウォールを利用する。
関係する製品	Microsoft Windowsシステムのすべて

 Page 29

WGメンバー

- 石川 章史 (Ishikawa Akifumi)
  株式会社ぷららネットワークス
  ネットワーク管理部
- 飯沼 正枝 (Iinuma Masae)
  グローバルナレッジネットワーク株式会社
  エデュケーションソリューション部
- 西野 一行 (Kazuyuki Nishino)
  株式会社ニコンシステム
  管理本部 企画部
- ピョー ナィン トォン (Phyo Naing Tun)
  株式会社アークン
  R&D事業本部
- 米澤 一樹 (Kazuki Yonezawa)
  セキュアコンピューティングジャパン株式会社
- 渡部 章 (Akira Watanabe)
  株式会社アークン

(敬称略、順不同)

 Page 30

JNSA

JNSA

・成果物の取扱いについて
成果物の著作権、使用等の権利は、著者及びＪＮＳＡとの共有とします。引用した文章、図表についての著作権は各作成者にあります。この成果物の配布、複製、修正についきましては、JNSA事務局までお問い合わせください。

 Page 31