

不正アクセス手法と技術的対策に関する調査

不正アクセス動向調査報告書

平成 13 年 3 月

情報処理振興事業協会

目 次

1. はじめに	1
2. 全体の動向	2
2.1. 全体の推移	2
2.1.1. インシデント報告件数の推移.....	2
2.1.2. 脆弱性の発見件数の推移.....	4
2.2. 不正アクセス手法の流布と対策の普及	7
3. サーバ別の攻撃手法の傾向	9
3.1. メールサーバ	9
3.1.1. 不正中継への悪用.....	9
3.1.2. 送信元の偽造.....	10
3.1.3. 侵入.....	11
3.2. Web サーバ	12
3.2.1. 侵入.....	12
3.2.2. 機密の漏洩.....	13
3.2.3. サービス妨害.....	13
3.3. ファイアウォール	15
3.3.1. トロイの木馬によるポートリダイレクト.....	15
3.3.2. サービス妨害.....	15
4. 環境別の攻撃手法の傾向	17
4.1. Windows 環境に対する攻撃	17
4.1.1. Windows NT 4.0 + IIS 4.0 に対する攻撃.....	17
4.1.2. Windows 2000 + IIS 5.0 に対する攻撃.....	18
4.2. UNIX 系環境に対する攻撃	20
4.2.1. Red Hat Linux 7.0 に対する攻撃とその対策.....	20
5. 結論	22
付録：不正アクセス情報コンテンツの書式	24

1.はじめに

インターネットが広く普及したことにより、世界中の人々がインターネットにアクセス可能となった。その結果、幅広い分野において多くの人々が、インターネットのもたらす利益を享受するに到った。

しかし、インターネットの普及は、必然的に悪意のある人々のインターネットへの流入も促した。その結果、インターネットにおけるソフトウェアやネットワークの脆弱性に付け込んで、頻繁に不正アクセスが行われる事態となっている。

現在における不正アクセス手法は、そのほとんどがソフトウェアやネットワークの脆弱性に依拠したものであり、脆弱性を不正アクセス手法と呼ぶことも多い。

こうした状況を加味した上で、本稿では、不正アクセス手法に関してその傾向を読み取る。まず、インシデント報告件数と脆弱性発見件数の推移から、不正アクセス手法の全体的な動向を見る。また、脆弱性の公表から不正アクセス手法の流布、対策の普及までの一連の流れを事例より検証する。

さらに、サーバ別あるいは環境別に主だった攻撃手法と対策を述べ、概要を整理し、その傾向を示す。最後に結論として、2000年から2001年初頭における不正アクセス手法の傾向をまとめ、効果的な対策の将来像について簡単に触れる。

2. 全体の動向

本章においては、不正アクセス手法の全体の動向を述べる。

2.1. 全体の推移

2.1.1. インシデント報告件数の推移

図1 - 1に、JPCERT/CC に報告されたインシデントの件数の推移を示す。

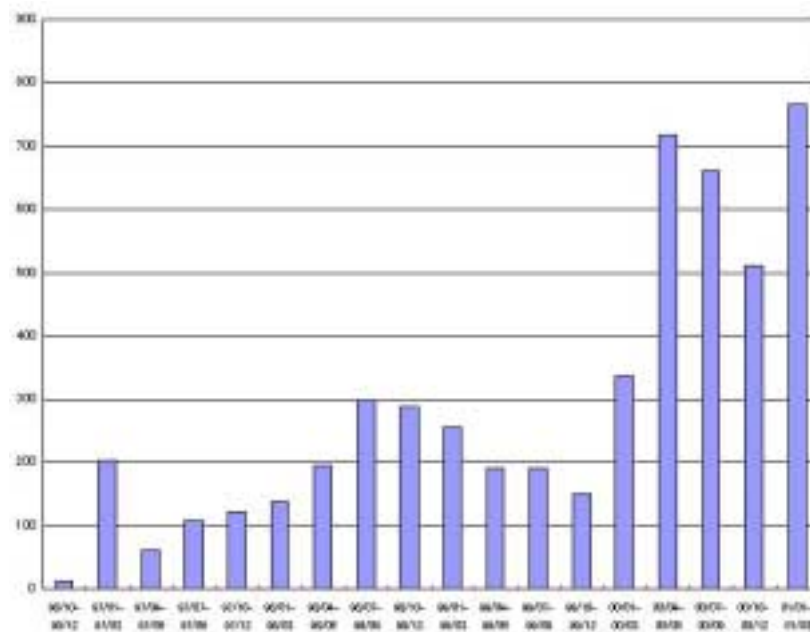


図1 - 1 報告されたインシデント件数の推移

(<http://www.jpcert.or.jp/stat/stats.jpg> より引用)

件数は JPCERT/CC への報告件数であり、実際に起きた全てのインシデントの発生数を正確に示すものではない。グラフにおいて2000年以降の件数が急増している背景としては、以下のような理由が考えられる。

- ・ 被害対象となるサイト数自体の増加：

容易にインターネットサーバを構築可能な OS パッケージが提供された。また、国内において常時接続サービスが普及した。これらの要因により未熟な管理者が「とりあえず」サーバを構築することが容易になり、セキュリティ関連対策が不十分なサイトが増えたものと想定される。

- ・ 不正アクセスを行う攻撃者数の増加：

脆弱性が公表されてから攻撃ツールが開発され流布されるまでの期間は日々短縮される傾向にある。このため、さしたる知識をもたない攻撃者でも致命的な攻撃を実行できる機会が増加したと考えられる。

- ・ 管理者・組織のセキュリティに関する認識の変化：

2000年に入り、複数のWebサイトへの相次ぐ侵入と改竄が大きく報じられた。また、企業サイトからの情報漏洩、ウイルス感染メールの配信など、ネットワークセキュリティに関する事件の発生が一気に日常化した。このような背景のもとで、管理者・組織がセキュリティに対する関心が強まったことから、インシデント発生時の届出事例数も増加したと推論される。

インシデントの増加を抑える要因としては、公表された脆弱性に関する対策手段の迅速な提供が挙げられる。

2001年現在では影響力の大きなソフトウェアに関する脆弱性の修正プログラムや新バージョンのプログラムの多くは、脆弱性の公表とほぼ同時に提示されている。また、ベンダ、公的機関、報道機関等により、インターネット上での管理者への情報提供が短い更新周期で行われている。

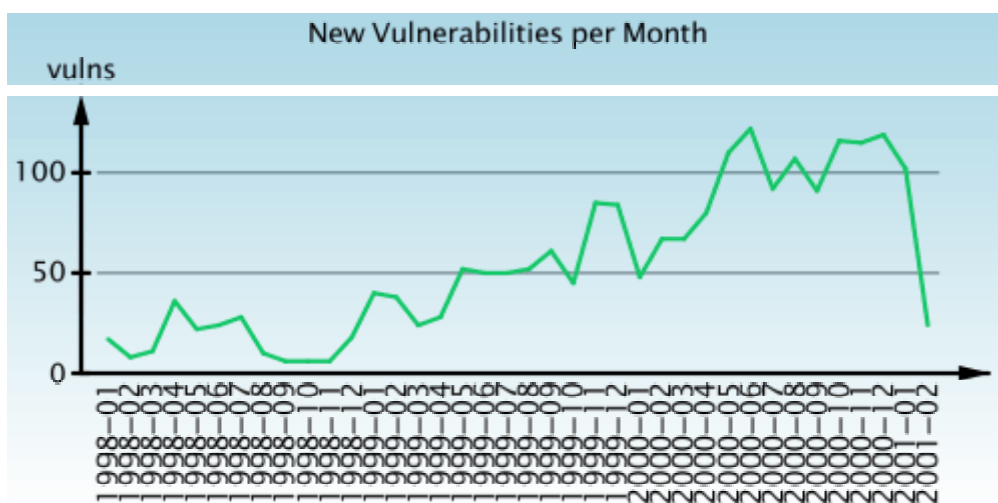
しかしながら、現在のところこれらの情報はあくまで関心のある管理者に向けた手法で提供されており、管理者自身が能動的に情報収集と学習に努めなければ伝達・理解されない。また提供される情報については、具体性、予想される被害の軽重、緊急度、対象者等について不明確なものも未だ多い。今後は受け手のニーズに合った信頼のおける情報源の確立が求められると言える。

2.1.2.脆弱性の発見件数の推移

(1)脆弱性の全体像

各種の OS 別にソフトウェア等の脆弱性に関する情報提供を行っている Bugtraq / SecurityFocus によれば、Bugtraq / SecurityFocus が自サイトに新規に掲載した脆弱性情報の数は、図 1 - 2 のように推移している。

グラフは 2001 年 2 月半ばまでの数字を示す。これらの報告にはベンダが自社のサイトで公開した脆弱性だけでなく、同サイトに寄せられた報告が含まれている。



(2) OS 別脆弱性

図 1 - 3 に、SecurityFocus による OS 別の脆弱性情報数の推移を示す。

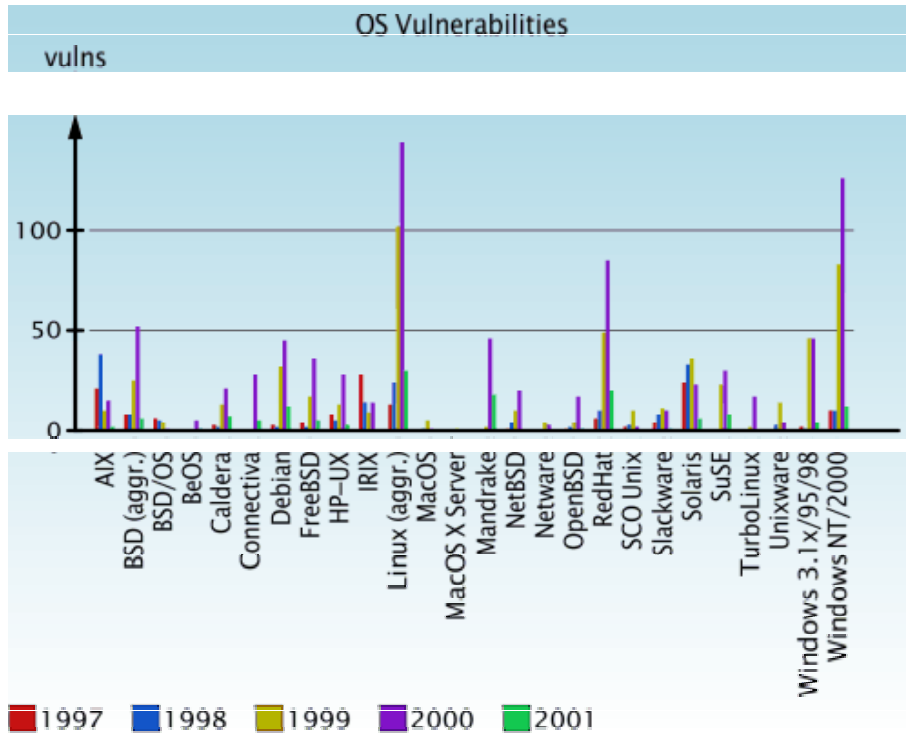


図 1 - 3 OS 別に見た脆弱性情報数の推移

(<http://www.securityfocus.com/images/vdb/vperos1.gif> より引用)

グラフより各 OS とも脆弱性に関する報告数は年を追うごとに増加する傾向があることが判る。特に、Linux と Windows NT/2000 に関する脆弱性の報告数は急激な伸びを見せている。これらが急速に普及し注目を集めていること、機能の追加や拡張が繰り返され新たな脆弱性が潜在的に存在し得る箇所が増えつづけていることが理由に挙げられる。Solaris に関しては毎年ほぼ同数の脆弱性が報告されている。

さらに、同じく SecurityFocus によると、OS 別の脆弱性の累計は、図 1 - 4 のようになっている。

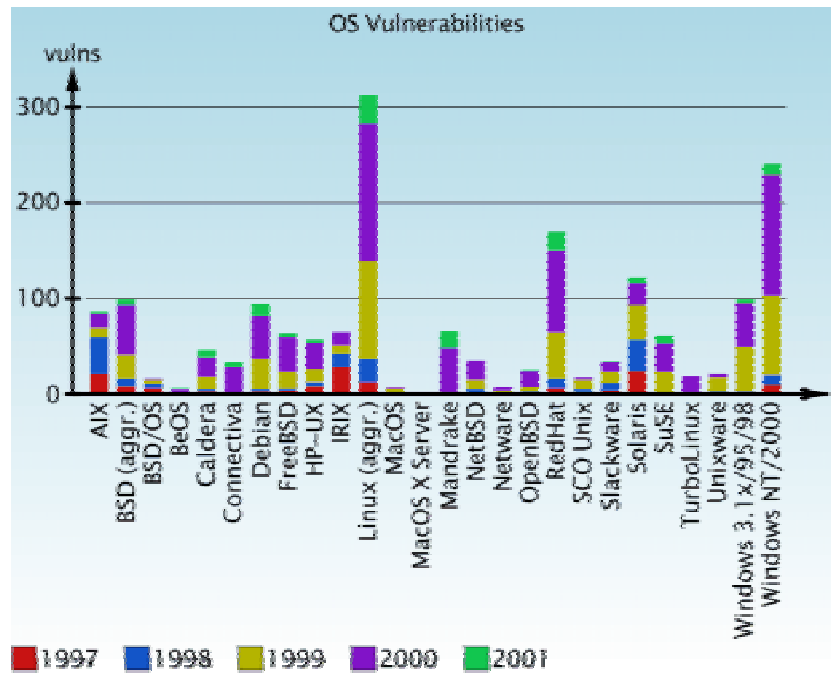


図 1 - 4 OS 別に見た脆弱性情報数の累計

(<http://www.securityfocus.com/images/vdb/vperos2.gif> より引用)

ここでも Linux (RedHat Linux) と Windows NT/2000 に関する報告数が他の OS に比べ特に多いことが見取れる。背景には、これらの OS が急速に普及し、インターネット上でサーバとしての利用数が増加した点や、機能拡張が頻繁に行われソフトウェアが早いペースで更新されるため、開発時に見逃された脆弱性が多く存在することがあると考えられる。

2.2.不正アクセス手法の流布と対策の普及

図1 - 5に、特定の脆弱性を狙った攻撃手法に基づく不正アクセス件数の推移の例を示す。これはCERT/CCに報告が行われたインシデントのうち、1999年にCERT/CCが勧告CA-1999-14においてBINDに関する脆弱性を示した後の、この脆弱性に基づく不正アクセス事例の件数をまとめたものである。この勧告に示された脆弱性に基づく攻撃手法は深刻なものであり、攻撃者はリモートからシステムの管理者権限を取得可能となる。

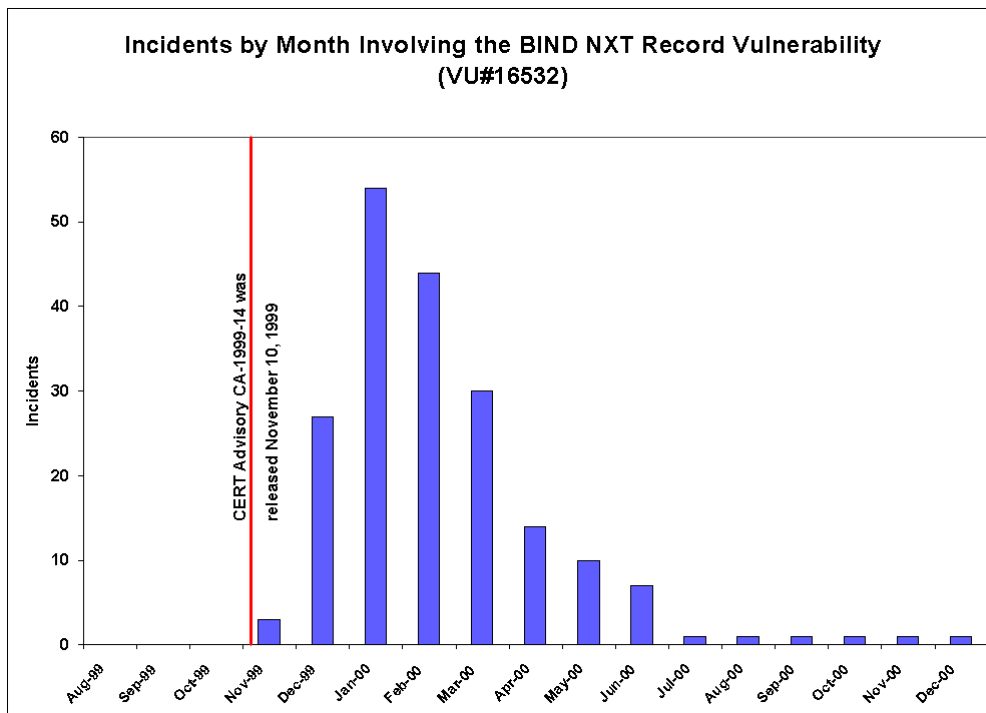


図1 - 5 BIND NXT脆弱性に関するインシデント報告件数の変化
(<http://www.cert.org/advisories/CA-2001-02/nxt-history.png> より引用)

グラフに示されたインシデント数は、被害がCERT/CCに報告されたものだけを示す点に注意が必要である。

1999年11月10日にCERT/CCが勧告を発した後、2000年初頭にかけて関連インシデント報告数は急激な伸びを見せ、2000年2月にピークに達し、その後は急速な減少を示している。

わずか3ヶ月間での報告数の急激な増加は、以下の複数の理由によるものと分析される。

- 不正アクセスを試みる側(攻撃者)は、新たに発見された致命的な脆弱性に関する情報を収集し、多くのシステム管理者が適切な対策を取る前に攻撃に利用する。公表からしばらく後に攻略プログラム(スクリプト)が出回り、攻撃に必要な知識と手間は大きく削減されるため、攻撃者の数が増加する。

- ・ 管理者は、勧告後しばらくの間、新たな攻撃手法に特に注目している。このため勧告後数ヶ月の間は積極的に報告が行われる。

報告数の爆発的な増加からは、勧告によりその攻撃手法が攻撃者と報告者の関心を広く集めることが読み取れる。

事例の報告数は脆弱性の公表から 3 ヶ月後より急速に減少し、数ヶ月で横ばいになっている。以下の複数の要因が挙げられる。

- ・ 対策手法の普及と浸透。報告を行う可能性のある管理者ならば、システムに対して適切な対策を数ヶ月のうちに施すものと考えられる。
- ・ 攻撃者の手法の変更。公表から一定期間が経つと対策を施したシステムが増える。このため、容易に成功するような攻撃ばかりを狙う攻撃者は、別の新たな脆弱性を利用した攻撃手法に手口を切り変えると想定される。
- ・ 攻撃対象の変更。攻撃者は対策が取られないまま放置されたシステムを探索し、攻撃を行う。このようなシステムに対する攻撃は被害が報告されることも少ないと考えられる。グラフが横ばいを続けていることから、攻撃手法は放棄されることなく、対象をより手薄なシステムに変えて続けられていると確認される。

実際にはこれらの複数の要因が組み合わさり、グラフ上に報告数の減少として示されたものと考察される。

3. サーバ別の攻撃手法の傾向

ここでは各用途のサーバに対する不正アクセスの傾向を述べる。サーバの種類としては、メールサーバ、Webサーバ、ファイアウォールを取り上げる。

3.1. メールサーバ

メールサーバに対する不正アクセスには以下のような傾向が見られる。

- ・ 不正中継への利用
- ・ 発信元の偽造
- ・ 侵入

実際には、不正中継への利用と発信元の偽造を組み合わせ、スパムメールの配信を行うことを目的とした攻撃が最も多いと思われる。不正中継の利用を狙う攻撃手法はその殆どが sendmail の設定ミスをつくものであり、適切な管理により防止可能である。

侵入を受けたメールサーバは、スパム等の迷惑メールの大量送信に悪用される場合が多い。メール処理の異常な遅延や、内部ユーザあるいは外部からメール管理者に宛てられた苦情により、管理者が不正アクセスに気が付く事例が複数報告されている。

3.1.1. 不正中継への悪用

(1) 概要

第三者のメールサーバの資源を盗用してメールの不正中継を行わせる手法。近年になって、スパムと呼ばれる不特定多数を対象とした広告メールの配信のために無関係なメールサーバを踏み台に悪用する行為が、大きな問題として取り上げられている。

(2) 分析

第三者のメールサーバを中継に用いる理由は、発信元の隠蔽と配信処理能力の借用のためである。

- ・ 発信元の隠蔽：
送信元の偽造（スプーフィング）と組み合わせることで、スパム発信者の追跡をより困難にできる。
- ・ 配信処理能力の借用：
メールメッセージのエンベロープ内の「RCPT TO:」レコードに複数のメールアドレスを列記し、中継するサーバでアドレスを展開させる。発信者が膨大なアドレスを付加した本文を1度中継サーバに送れば、後はサーバプログラムに各アドレス宛てのメールを作成して送信する処理を行わせることができる。sendmail プログラムが実行される環境では、この展開と配送の処理を行うと処理能力の殆どを奪われるため、通常のメールの送受がほ

ば不可能になる。

不正中継への悪用の手法は古くから知られるが、被害は報告され続けている。被害を受けるサーバの多くは旧バージョンの sendmail を不適切な設定のまま使い続けているものと想定される。

第三者からのメールを中継する誤った設定が施されたサーバはスパムメールの中継に悪用される可能性が非常に高い。2000 年度にも企業・公的機関のメールサーバがスパムメールの不正中継に悪用された事件が大きく報道された。

スパムの中継を長期に渡って放置するなどの不適切な対応を取れば、メールサーバがスパム配信元ブラックリストに登録されることも考えられる。ブラックリストに登録された場合は、送信したメールの受信を拒否されるなど利用者のメール利用が阻害されることや、組織の信用が失墜する可能性もある。

(3) 対策

不正中継はサーバの設定ミスを突く攻撃手法であり、事前に適切な対策を取ることが可能である。管理者は、旧バージョンの sendmail プログラムを用いている場合は最新版に更新し、適切な設定を施す必要がある。実際にテストメールを送信して外部ネットワークからの不正な中継ができないことを慎重に確認することが望ましい。

中継に関する設定はおおよそ以下のようにまとめられる：

- ・ 自ネットワーク内からのメールは全てリレーする。
- ・ 外部からのメールは自ネットワーク内宛のメールのみ受け取り、外部からきた外部の RECIPIENT 宛のメールは配送を拒否する。

代表的なサーバプログラムである sendmail ではバージョン 8.8.x で導入された check_relay ルーチンを利用し、中継に関する設定を徹底することができる。

他ドメインからのメールサーバへのアクセスを許可する必要がある場合は無関係な外部ユーザからの不正中継を防ぐために POP before SMTP を導入することが考えられる。これは SMTP 利用の前に POP によるメール受信を行うことでユーザの認証を行うものである。

3.1.2. 送信元の偽造

(1) 概要

メールヘッダの送信元欄 (From 行) などを偽り、実際とは異なるアドレスを持つ送信者からのメールを装う手法が知られている。この手法は、スパムの送信やメール爆弾等のサービス妨害・嫌がらせ行為の際に送信者の追跡を困難にするために、あるいは、受信者を騙してメールの内容を信用させ、パスワード等の機密情報を明かさせるために用いられる。

(2) 分析

全く無関係な外部のユーザによりメールアドレスが悪用される場合と、メールサー

バにアカウントを持つ正規のユーザが、送信元を偽ったメールを作成してメールを送信する場合の 2 通りの問題が考えられる。

電子メールの送信元の偽造は容易に行える。メールメッセージは SMTP (Simple Mail Transfer Message) により平文 (7 ビット ASCII コード) のまま送受され、送り手に関する情報の整合性の確認も通常は行われぬ。このようなメールのシステムが本来持っている脆弱さが送信元の偽造の根本的原因となっている。

送信元を騙られた場合には苦情やエラーのメールが大量に送られてくることや、電話等での苦情や問い合わせが集中することが予想される。

メールアドレスの偽造は攻撃手法として単体で用いられることは少なく、不正中継やメールボム等の手法と組み合わせられることが多い。

(3) 対策

メッセージが送信者から発せられたことを保証する手段としては署名技術の利用が挙げられる。

自らが管理するメールサーバにおいて送信アドレスを確認する機構を付加し、偽造アドレスが付されたメールの発信を防止することが可能である。内部ユーザによる From 行の詐称を防ぐためには、送信前に From 行内のドメイン名をチェックし、ドメイン名が一致しない場合はメールの送信を拒否する。

3.1.3. 侵入

(1) 概要

メールサーバに対する侵入手法としてはサーバにおいて動作するソフトウェアの脆弱性の攻略が挙げられる。OS あるいはメール関連のプログラムの脆弱性だけでなく、サーバ上で動作するその他のプログラムの脆弱性を攻略される場合もある。

(2) 分析

sendmail 等の MTA (Mail Transfer Agent) や OS に存在する脆弱性などが狙われることが多い。最も良く使われる MTA である sendmail にはこれまでのバージョンに複数の脆弱性が報告されている。

メールサーバへの侵入は、メールの覗き見等による機密情報の取得、サーバの機能を不正利用したスパムメール等の発信、ネットワークの他のサーバへの踏み台等を意図して行われる。

(3) 対策

サーバ全般における基本的な侵入対策が適用可能である。サーバプログラムや OS の脆弱性については修正プログラムの適用やバージョンアップで対応する。sendmail は多くの脆弱性以外にもデフォルト設定の問題点が報告されている。適切な設定を確認し、不要なサービスを停止する。サービス設定の変更後は特に挙動のチェックを念入りに行う。

3.2.Web サーバ

Web サーバに対する不正アクセスには、以下のような傾向が見られる。

- ・ 侵入（アクセス権の奪取）：CGI プログラムやサーバソフトウェアのセキュリティホールを利用した侵入手法が知られている。
- ・ 機密の漏洩：侵入により重要な情報が攻撃者に奪われる場合、セキュリティホールを用いてサーバ上の情報を参照される場合、管理者の設定ミスや管理の不徹底により重要な情報が公開された状態になる場合などがある。
- ・ サービス妨害：サービス妨害攻撃手法によるサーバの停止あるいは破壊。

Web サーバに対する不正アクセス手法は、Web サーバ自体（httpd）の脆弱性に基づく攻撃手法や、OS の脆弱性に基づく攻撃手法だけではなく、Web サーバの機能を拡張するサーバアプリケーション（CGI 等）の脆弱性に基づく攻撃手法が数多く存在する。古いバージョンのサーバにデフォルトでインストールされているテストスクリプトやサンプルスクリプトが抱える脆弱性や、商用/非商用の著名なスクリプトに存在する脆弱性は、攻撃の糸口にされやすい。

3.2.1.侵入

（１）概要

外部に対して公開された Web サーバは脆弱性の攻略による侵入（攻撃者によるアクセス権の取得）の対象となる。

（２）分析

代表的な侵入手法としては、メモリ上でバッファオーバーフローを起こす脆弱性を利用し、攻撃者の意図したコードを実行する手法が知られている。この種の脆弱性が外部からアクセスされるサーバプログラムやCGI等のWebアプリケーションプログラムに存在する場合は、攻撃者はサービスプロセスの持つ権限で任意のコードをリモートから実行できるため、極めて危険なものとなる。

また、CGI 等のサーバ側で実行されるプログラムの脆弱性をつく攻撃手法には、フォーマットストリング攻撃と呼ばれる手法が見られる。この手法では入力をシェルに渡す関数の適切なチェックが行われないバッファが狙われ、コマンドを含む入力を送りつけられる。攻撃者はサーバの権限によるコード実行が可能となる。

侵入の影響としては、Web サーバ上のコンテンツの改竄、機密情報の取得、他のサーバへの不正アクセスへの踏み台としてのサーバ利用など複数の影響が考えられる。事例では侵入経路自体が不明確になる場合も多く見られる。

（３）対策

サーバ全般における基本的な侵入対策が適用可能である。サーバプログラムやOSの脆弱性については修正プログラムの適用やバージョンアップで対応する。適切な設定を確

認し、不要なサービスを停止する。サービス設定の変更後は特に挙動のチェックを念入りに行う。

Web アプリケーションについては、脆弱性を含まないように意識して作られた、信頼のおけるWebアプリケーションを利用する。不要なWebアプリケーション機能は停止し、ファイル拡張子に関する関連付け設定も不要なものは解除する。

3.2.2. 機密の漏洩

(1) 概要

想定外のアクセス手法によって、本来外部に公開することを意図していない情報(機密情報)がアクセスされてしまうケース。機密情報は、電子商取引サービスの取引記録、Web サイトでのアンケート結果、Web サイトへのアクセス記録などのサイトでの活動により収集蓄積された情報と、Web アプリケーションのソースコード、パスワード等のローカルファイルに大別できる。

(2) 分析

攻撃手法は、脆弱性を攻略して情報を引き出す手法と、管理側のミスによりアクセス可能な状態に置かれた情報を取得する手法とに分けられる。

脆弱性攻略手法のうち代表的なものには、親ディレクトリ(「../」で表される)に関するプログラムの処理の脆弱性を攻略する手法がある。本来は公開されないローカルなファイルを取得することが可能である。これらのアクセス権の無いファイルを取得するための手法はディレクトリトラバース攻撃(dot dot 攻撃)とも呼ばれる。

また、サーバで実行されるプログラムのソースコードを狙った脆弱性攻略手法も多く知られている。ある特定の条件の下でアプリケーションがパーズされず、通常のテキストやHTMLで書かれたコンテンツと同様に出力されるという脆弱性がいくつか報告されている。攻撃者は取得したソースコードから、アクセス権を取得するための脆弱性を探すことや、他のファイルに関する情報を得ることができる。

管理側のミスによりアクセス可能となる情報の例としては、アクセス権限設定の誤りにより本来は訪問者による読取を禁止すべきディレクトリが閲覧可能になる場合が多い。

(3) 対策

運用するサーバプログラムに関する脆弱性対策が有効となる。管理ミスを無くすためには、サイトのデザイン時より、扱う情報の重要性和漏洩時の危険性を意識し、収集する情報適切なポリシーを設定することが重要である。

3.2.3. サービス妨害

(1) 概要

Web サイトを対象にしたサービス妨害攻撃の事例が報告されている。

(2) 分析

サービス妨害攻撃は簡単に入手可能な攻撃ツールを利用して実行可能である。最も一般的なサービス妨害攻撃は、コンピュータやネットワークの帯域幅や接続性を狙う。帯域幅攻撃は、ネットワークに大量のデータを送り込み、利用可能なネットワーク資源を全て消費し、正規ユーザのリクエスト処理を困難なものにする。接続性攻撃は、ネットワークに大量の接続リクエストを送りこみ、利用可能な OS 資源を全て消費し、コンピュータによる正規ユーザの要求処理を困難なものにする。

この他にもソフトウェアの致命的な脆弱性を突くサービス妨害攻撃手法が知られている。この種のサービス妨害攻撃手法としては、不正なプロトコル手順による攻撃、例外的な処理の誤りを突く攻撃、バッファオーバーフロー攻撃などが報告されている。これらの攻撃を受けた場合は実行中のサーバプログラムが停止するか、ホストマシンが停止することが考えられる。

分散型サービス妨害攻撃 (DDoS 攻撃) 手法により、強固なセキュリティを持つ大規模サイトが狙われる事例が頻繁に伝えられている。このような攻撃のための踏み台としては、適切な設定や脆弱性対策が施されていない管理の甘いサーバに仕込まれたエージェントが用いられている。

(3) 対策

未対策のセキュリティホールや設定の不備により、被害が増大化する場合がある。修正プログラムの適用やバージョンアップを行う。サービスへの要求が増大した場合の対応方法を考慮し設定を適切なものに更新する。

DDoS 攻撃については、仕込まれたエージェントによって無自覚のうちに攻撃者に加担することを避ける必要がある。侵入を受けないよう基本的対策を施し、エージェントプログラムがシステムに仕込まれていないことをチェックする。また、エンドユーザも不審な Web サイトや添付ファイルから入手した不審なプログラムを実行しないよう心掛けなければならない。

3.3. ファイアウォール

攻撃者による攻撃の前段階の情報収集が、外部と内部の境界上に位置するサーバに対して絶えず行われている。

ファイアウォールにおける適切なアクセス制限機能を無効化する手法としてはトロイの木馬ソフトウェアを用いた攻撃手法が知られている。また、ファイアウォールによるアクセス制限の実行率を低下させるためにパケットフィルタリング機能に対するサービス妨害を狙った攻撃が見られる。

3.3.1. トロイの木馬によるポートリダイレクト

(1) 概要

ファイアウォールによりフィルタリングされるポートを避けて、チェックを受けないポートを用いて通信を迂回させるプログラムを内部ネットワークのホストに仕込む。

(2) 分析

ポートリダイレクト機能を持つトロイの木馬ソフトウェアが既に広く出回っている。これらはウイルス同様の感染機能を持ち、電子メールに添付されたファイルや Web サイト訪問者によるダウンロードによって拡散している。攻撃者はソフトウェアが仕込まれたマシンを踏み台に使い、ファイアウォールによる制限を受けずに、ネットワーク内部から内部のホストマシンに対して攻撃を行える。外部ネットワークとの境界上に位置するサーバに比べ、内部ネットワークに位置するサーバは適切なセキュリティ対策が施されていないことが多いため、深刻な被害を受ける。

(3) 対策

各ホストをスキャンすることで、トロイの木馬プログラムが外部に向けて開いたポートを検知し、これを除去することができる。

3.3.2. サービス妨害

(1) 概要

ファイアウォールを構成するマシンは外部ネットワークにさらされているため、直接攻撃を受けることが考えられる。OS およびファイアウォールアプリケーションのレベルでの攻撃を受けることが考えられる。

(2) 分析

サービス妨害攻撃は簡単に入手可能な攻撃ツールを利用して実行可能である。最も一般的なサービス妨害攻撃は、コンピュータやネットワークの帯域幅や接続性を狙う。帯域幅攻撃は、ネットワークに大量のデータを送り込み、利用可能なネットワーク資源を全て消費し、正規ユーザのリクエスト処理を困難なものにする。接続性攻撃は、ネットワークに大量の接続リクエストを送りこみ、利用可能な OS 資源を全て消費し、

コンピュータによる正規ユーザの要求処理を困難なものにする。

この他にもソフトウェアの致命的な脆弱性を突くサービス妨害攻撃手法が知られている。この種のサービス妨害攻撃手法としては、不正なプロトコル手順による攻撃、例外的な処理の誤りを突く攻撃、バッファオーバーフロー攻撃などが報告されている。これらの攻撃を受けた場合は実行中のサーバプログラムが停止するか、ホストマシンが停止することが考えられる。

(3) 対策

未対応のセキュリティホールや設定の不備により、被害が増大化する場合がある。修正プログラムの適用やバージョンアップを行う。サービスへの要求が増大した場合の対応方法を考慮し設定を適切なものに更新する。

4. 環境別の攻撃手法の傾向

環境別の攻撃手法の傾向について述べる。

4.1. Windows 環境に対する攻撃

近年 Windows NT/2000 による Web サーバあるいはアプリケーションサーバの普及が進んだため、基本ソフトウェアとなる IIS 4.0/5.0 に対する侵入およびサービス妨害を意図した攻撃が多く見られる。IIS に関してはクリティカルな脆弱性の報告例も多いため、管理者のこまめな対応が必要とされる。

また、Windows 環境についてはクライアントセキュリティの脆弱性を突いた攻撃も数多く報告されている。ネットワーク内部への裏口プログラムの作成、分散型サービス妨害攻撃 (DDoS 攻撃) エージェントの密かなインストール、パスワードやシステム情報の取得を意図した攻撃である。これらの攻撃はブラウザやメーラーの脆弱性を突いて行われるため管理者だけではなくエンドユーザを含めた対策を要する。

Windows 環境における具体的なセキュリティ対策は、以下のように整理される。

- ・ セキュリティ視点からのシステムのチューニング (セキュリティを考慮したインストール、不要なサービスの削除や無効化、各種設定の適正化)
- ・ アクセス権の管理の徹底
- ・ サービスバックあるいは修正プログラムの適用

以下に典型的運用環境として、Windows NT 4.0 と IIS 4.0 を組み合わせた環境と Windows 2000 と IIS 5.0 を組み合わせた環境を取り上げ、これらに対し頻繁に実行される攻撃手法と対策をまとめる。

4.1.1. Windows NT 4.0 + IIS 4.0 に対する攻撃

Windows NT 4.0 と IIS4.0 を組み合わせたサーバ環境は、多くのサイトにおいて従来から運用が続けられている。この環境についてはこれまでに多くの脆弱性が報告されている。

2000 年度に報告された脆弱性を用いた攻撃手法のうち、特に大きく被害が報じられたものとしては、以下の手法があげられる。

- ・ IIS によるファイル要求の解析に関する脆弱性を利用した攻撃：
実行可能ファイル (.bat あるいは .cmd) のファイル名に OS コマンドを付加したリクエストを送信すると cmd.exe にそのまま渡され、ファイル処理後に付加された OS コマンドが IUSR_machinename 権限で実行される脆弱性を利用した攻撃手法。リモートからの攻撃者は IUSR_machinename 権

限で任意の命令の実行、権限の向上、ファイルの取得/削除/追加/変更が可能となる。攻撃者に通常の対話的ログオンユーザと同等の権利が与えられる。攻撃者は権限の向上を謀るための情報の収集も可能となる。対策としてはマイクロソフトの提供する修正プログラム（MS00-086：「Web サーバーによるファイル要求の解析」の脆弱性に対する対策）の適用が推奨される。

Windows NT 4.0 + IIS 4.0 環境で高いセキュリティを実現するためにはインストール時のデフォルト設定を鵜呑みにせず適切な選択を行い、運用前に慎重なチェックと調整を行う必要がある。当然ながら 2000 年以前に報告されている脆弱性についてもサービスパックと修正プログラムの適用で対策を施しておく必要がある。

4.1.2. Windows 2000 + IIS 5.0 に対する攻撃

Windows 2000 と IIS 5.0 を組み合わせたサーバ環境は、Windows NT 4.0+ IIS 4.0 環境に比べ容易に導入可能であり、NT 4.0 に対するサポートの縮小やクライアント環境との統合が進むにつれ、今後 Windows 2000 サーバへの切り替えも加速されると予想される。

Windows 2000 と IIS 5.0 を組み合わせたサーバ環境について 2000 年度に報告された脆弱性のうち、特に大きく被害が報じられた攻撃手法に利用されたものを以下にあげる。

- ・ IIS によるファイル要求の解析に関する脆弱性を利用した攻撃：
実行可能ファイル（.bat あるいは.cmd）のファイル名に OS コマンドを付加したリクエストを送信すると cmd.exe にそのまま渡され、ファイル処理後に付加された OS コマンドが IUSR_machinename 権限で実行される脆弱性を利用した攻撃手法。リモートからの攻撃者は IUSR_machinename 権限で任意の命令の実行、権限の向上、ファイルの取得/削除/追加/変更が可能となる。攻撃者に通常の対話的ログオンユーザと同等の権利が与えられる。攻撃者は権限の向上を謀るための情報の収集も可能となる。対策としてはマイクロソフトの提供する修正プログラム（MS00-086：「Web サーバーによるファイル要求の解析」の脆弱性に対する対策）の適用が推奨される。
- ・ IIS 5.0 の ISAPI エクステンションの脆弱性：
IPP（Internet Printing Protocol）サポート用の ISAPI エクステンションのバッファに対して適切なチェックが行われなかったため、バッファオーバーフローを起こすことが可能である。この脆弱性をつく攻撃手法により攻撃者はリモートから SYSTEM 権限を取得できる。対策としてはマイ

クロソフトの提供する修正プログラム (MS01-023 : ISAPI エクステンションの未チェックのバッファにより IIS 5.0 サーバーのセキュリティが侵害される) の適用が推奨される。

Windows NT 4.0 + IIS 4.0 環境に比べると Windows 2000 + IIS 5.0 環境は比較的容易に導入可能である。より高いセキュリティを実現するための定義ファイルや設定方法に関する情報が整備されているので目的に合わせて選択的に適用することが望ましい。運用前に慎重なチェックと調整を行う必要がある。当然ながら発見された新たな脆弱性に関してはサービスパックと修正プログラムのすみやかな適用が求められる。

4.2.UNIX 系環境に対する攻撃

攻撃対象となるサーバとしては、Web サーバ、メールサーバ、ネームサーバが多い。これらのサーバのセキュリティ設定ミスや放置された脆弱性を狙った攻撃が行われる。

OS としては、近年インターネットサーバに利用されることが多い Linux、Solaris が攻撃の対象となることが多い。

ブラウザ(Netscape)を含めた多様なクライアントに対する攻撃手法は Windows 同様に報告されている。

以下では典型的な環境として RedHat Linux 7.0 に基づく環境を取り上げ、これに対し頻繁に実行される攻撃手法と対策をまとめる。

4.2.1.Red Hat Linux 7.0 に対する攻撃とその対策

RedHat Linux 7.0 システムは高いシェアを持つ Linux システムである。ここでは RedHat Linux 7.0 システムに対して頻繁に取られる攻撃手法のうち、侵入につながる脆弱性に基づくもので、特に 2000 年度に深刻な被害をもたらしたものを取り上げる。

- BIND の脆弱性をつく攻撃手法：
BIND に関しては複数の脆弱性が CERT/CC 等の機関から数度に渡り指摘されている（CA-2001-02 などを参照のこと）。リモートからの攻撃者はルート権限を取得し、任意のコードを実行可能である。対策としては DNS が不要な場合は停止し、動作させる必要がある場合は、ベンダの提供する最新のプログラムに必ず更新することが求められる。
- LPRng の syslog へ渡されるフォーマット文字列を用いた攻撃：
LPRng の use_syslog()関数において、ユーザから入力された文字列をフォーマット文字列として syslog にそのまま渡している。リモートからの攻撃者はルート権限を取得し、任意のコードを実行可能である。対策としては各ベンダ提供のパッチ、最新版パッケージを使用する。
- ftpd の SITE EXEC コマンドにおけるフォーマット文字列を用いた攻撃：
SITE EXEC の実装に関する脆弱性。ireplay 関数内において信頼のおけないフォーマット文字列が printf関数にチェックされないまま渡される。このためスタックのリターンアドレス等の重要なデータを上書きするために用いることが可能である。リモートからの攻撃者はルート権限を取得し、任意のコードを実行できる。対策としては各ベンダが提供する最新パッチをインストールする。
- rpcd.stated の脆弱性を用いた攻撃：
rpc.statd におけるログ生成コードは syslog()関数を用いるが、ユーザが

フォーマット文字列を渡した場合にこれを適切に取り除かない。プロセスのアドレス空間内にコードを送り、関数のリターンアドレスを上書きして実行することができる。rpc.statd は root 権限で動作するため実行されるコードは root 権限をもつ。リモートの攻撃者はルート権限を取得し任意のプログラムを実行可能である。対策としてはプログラムのバージョンアップが必要となる。

2000 年末よりこれらの脆弱性に対する攻撃手法はワームやウイルスに組み込まれ、バックドアや DDoS のエージェントが自動的に仕掛けられるようになった。Ramen、Lion、Adore などのワームの存在が知られている。

攻撃手法が確立するまでの期間に短縮化傾向があることを考え合わせると、このような自動化攻撃ソフトウェアは今後より大きな脅威に育つ可能性を持つ。管理者は脆弱性情報の公開後に修正を急ぐなど、十分な注意が必要と考えられる。

5. 結論

ネットワークサービスの普及と急速な高度化・複雑化に伴い、インシデント発生件数と脆弱性発見件数はどちらも増加する傾向にある。

脆弱性情報等の不正アクセス対策に必要な情報の公開は、攻撃者に情報を与えるマイナスの側面があるものの、インシデントを正確に把握し対策手段を講じることを促すプラスの側面から不可欠と考えられる。しかしながら、インシデント防止対策の普及は攻撃手法の拡散に比べ緩やかな速度で進むため、脆弱性の公表後に対策が浸透するまでの期間に攻撃者が無防備なシステムを襲う可能性を排除し切れていない。

2001年初頭の時点では、広範囲のシステムに影響する重大な脆弱性については、脆弱性の公表とほぼ同時にベンダから修正プログラムが素早く示されるようになり、対策の迅速な適用が可能となりつつある。また、公的機関や大手ベンダを中心とした管理者への注意喚起の強化や提供される情報の最適化も進められている。

このような流れはシステムセキュリティ向上に積極的に取り組む管理者を育成支援する環境を整備する動きとして高く評価できる。

その一方で、不正なアクセスに対して無防備なまま放置されているシステムが未だに数多く存在する。システムに適切なセキュリティ対策が施されない要因は、管理者の問題（知識不足、怠慢、過剰な作業の集中）、管理体制の問題（管理者の不在、セキュリティポリシーの未徹底）、ソフトウェアの問題（無数の脆弱性の存在、誤った/甘いデフォルト設定、入手困難な修正プログラム）など多岐に渡る。

不正アクセスの被害報告は任意であるため実態把握が極めて困難だが、例えば Web ページの改竄という目に見えやすい形で侵入が露呈するケースだけを取ってみても、日に数十件という一定したペースで被害が途絶えること無く増え続けていることが判る。Web ページの改竄だけがクラッカーの目的ではない。管理が不十分なシステムが Web サーバに限られずに狙われていることは間違い無いが、密かに侵入を受けて長期間気付かなかった場合などの被害は殆ど公表されていない。

「見えない」被害が実際にどれだけ広範で深刻なものであるかについては決して楽観視できない。

適切な対策が取られていないシステムに対しては、古典的・類型的な手法を集めた脆弱性情報収集スキャナ等のツールが有効であり、攻撃者は特に選り好みしなければ容易に標的のマシンを数多く集めることができる。

攻撃ツールの自動化は近年強く推し進められ、既に脆弱性を攻略し裏口ツールを仕掛けるワームの被害が既に出ている。この種の自動化された攻撃により密かにマシンの群れが

被害を受け、大規模な分散型サービス妨害攻撃に悪用されるシナリオは、極めて現実的な脅威として想定されるものとなった。

様々な要因で管理が不十分なまま放置されているシステムを減らすために、現在の管理者に依存する対策とは異なる、新たな対策が求められている。

脆弱性を極力排除するソフトウェア開発手法、リアルタイムでシステムの脆弱性の有無を随時チェックし修正プログラムの適用を促す機構など、セキュリティホールを減少させるための技術的解決策の確立と、不正アクセス被害後の迅速かつ適切な対応を促すための連絡および支援体制を整える必要があると言えよう。

付録：不正アクセス情報コンテンツの書式

不正アクセス情報コンテンツの例を下表に示す

表：4 - 1 不正アクセス情報コンテンツ例

ID	0004
日付	20000111
名称	不正な IMAP リクエストに関する脆弱性
対象プラットフォーム名 / OS 名とバージョン	Windows NT 4.0
対象ソフトウェア名 / サービス名とバージョン	Microsoft Commercial Internet System 2.5 Microsoft Commercial Internet System 2.0 Microsoft Commercial Internet System (MCIS) Mail server
手法	MCIS Mail に含まれる IMAP サービスに、適切にチェックされないバッファが存在する。バッファオーバーフローを引き起こすことが可能。
影響	リモートからの攻撃者はサービスをクラッシュさせることでサービス不能攻撃が可能。Web パブリッシング、IMAP、SMTP、LDAP、等のサービスが影響を受ける。また、サーバ上で任意のコードを実行可能。
予防対策	修正プログラムの適用
被害拡大防止策	
ベンダが提供する情報へのポインタ	MS00-001
修正プログラムへのポインタ	PC/AT 互換機用 http://www.microsoft.com/downloads/release.asp?ReleaseID=17136 Alpha 用 http://www.microsoft.com/downloads/release.asp?ReleaseID=17134
CVE 番号	CVE-2000-0053
SecurityFocus 番号 (BID)	BID:912
関連情報へのポインタ	XF:mcis-malformed-imap http://www.microsoft.com/japan/technet/security/SecFaq.asp?sec_cd=ms00-001
備考	

作成した不正アクセス情報コンテンツにおける、各項目の記述指針を以下に説明する。

(1) ID

作成したコンテンツ 1 件につき 1 つ、固有の番号を与えている。

(2) 日付

該当する脆弱性がデータソースに報告された日付を示す。

(3) 名称

脆弱性の概要を表す名称を与えている。

(4) 対象プラットフォーム名 / OS 名とバージョン

該当する脆弱性が存在するプログラムがどのような OS において動くかを示す。

(5) 対象ソフトウェア名 / サービス名とバージョン

該当する脆弱性がどのようなプログラムに存在するかを示す。

(6) 手法

脆弱性とそれを用いた攻撃手法の詳細を示す。典型的な手法としては以下のような攻撃手法が含まれる (詳細は別冊子の対策集に記す)

- ・ バッファオーバーフロー攻撃
- ・ フォーマットストリング攻撃 (シェルメタキャラクタ攻撃)
- ・ ディレクトリトラバース攻撃
- ・ ブルートフォース攻撃

(7) 影響

脆弱性を狙った攻撃手法によりどのような影響が及ぼされるかを示す。主な影響の例としては以下のようなものがある :

- ・ サービス妨害
- ・ パスワード / アクセス権の取得
- ・ プロセスの実行
- ・ ファイルの取得 / 追加 / 変更 (改竄) / 削除

対象となるマシンと攻撃者との位置関係 (リモート / ローカル) 攻撃の結果として獲得される権限 (管理者権限、プロセス権限、ユーザ権限) 等についても具体的に示す。

(8) 予防対策

攻撃手法に対して、事前に適用可能な対策方法を示す。プログラムの修正や更新を適用可能なものはその旨を記し、設定等の変更により対策可能なものについては手法を簡潔に記す。

(9) 被害拡大防止策

攻撃後に特に被害拡大を防止するための対策があるものについてはこれを記す。

(1 0) ベンダが提供する情報へのポインタ

関連するセキュリティ情報について、ベンダより Web 上で提供される情報へのポインタを URL で示す。

マイクロソフト社のセキュリティ情報については、その番号を示しているが、以下の URL よりデータベースを参照可能である。

<http://www.microsoft.com/japan/technet/security/current.asp>

(1 1) 修正プログラムへのポインタ

ベンダより提供される修正プログラムを取得するための参考 URL を示す。

(1 2) CVE 番号

CVE のうち、該当する脆弱性を説明するものの番号を示す。以下のアドレスより参照することが可能である。

<http://cve.mitre.org/>

<http://icat.nist.gov/icat.cfm>

(1 3) Security Focus 番号 (Bugtraq ID : BID)

Security Focus サイトのデータベースにおいて該当する脆弱性を説明するものの番号を示す。以下のアドレスより参照可能である。

<http://www.securityfocus.com/>

(1 4) 関連情報へのポインタ

その他複数の情報源へのポインタを URL で示す。

(1 5) 備考

特に注意が必要な事柄についてはこれを記す。