Windows 環境のセキュリティ

最近のセキュリティ情報

2000.2.26

同朋学園本部事務局経理課
河邊憲二

Windows 環境のセキュリティ

Windows 環境のセキュリティ

同朋学園本部事務局経理課　河邊憲二

2000.2.26-27 セキュリティ講座

主催:東海スクールネット研究会

於：ホテル魚半日吉苑

このレポートは、東海スクールネット研究会主催の
セキュリティ講座用に、Windows 環境のセキュリティ
情報を、経験に基づき簡単にまとめたものである。

1. Windows を使う場合のセキュリティに関する教訓

これまで、Windows 環境を使ってインターネットサーバーを運用してきた経験上、特にセキュリティに関しては、次の３つの教訓がネットワーク管理の初心者には役立つと思う。

a. Windows 環境は常に最新のものを利用する。
b. Windows 環境では Microsoft 社のアプリをできるだけ使う。
c. Windows 環境をデフォルトのまま使ってはいけない。

この教訓をもとにセキュリティに関する情報を簡単にまとめる。はじめに、ここでは上の教訓により、最新版を利用するということが守られていることを前提にするので、古いバージョンについては取り上げない。古いバージョンではセキュリティ対策のできない問題もあるし、最新版に比べて対策すべき問題も多い。Microsoft 社のセキュリティに関する情報も最新版の方が収集しやすい。

手元の Windows 環境の最新バージョンは
Microsoft Windows 98 Second Edition 4.10.2222 A
MS IE 5.01 日本語版 5.00.2919.6307 暗号強度:56-bit build 52919.6307
＊ 英語版には暗号強度 128-bit がすでに出ている。
Windows NT 4.0 Server build 1381 + SP6a
＊ Windows 2000 環境はまだ十分テストしていないのでここでは取り上げない。

2. MS IE 5.01 のセキュリティ

Windows をインターネット接続が可能なクライアントとして利用している場合、セキュリティ上問題となる場合がある。たいていの場合、悪意ある Web サイトへ接続した場合に、ユーザーのコンピュータ上にあるファイルを読むことが可能になるというものであるが、中にはシステムにダメージを与えられるプログラムが送り込めるというものもある。Windows 環境で動作するブラウザやメールソフトは数多く存在するが、ここでは IE5.01 のみを取り上げる。Windows 環境でセキュリティ問題の影響を受ける他社製品はその対応が遅れるので、ここでも Microsoft 社の製品を使うという教訓に従う。

Windows 環境のセキュリティは Windows Update サイトより修正プログラムをダウンロードすることで通常は対策をする。現在、Windows Update からダウンロード可能な修正プログラム（2 月 24 日現在）は、次の通りである。

Windows Update からダウンロード可能な修正プログラム（2 月 24 日現在）

* 以下 Microsoft 社のホームページから引用

・Internet Explorer ファイルの場所の修正プログラム

Internet Explorer のコンポーネントや修正プログラムをダウンロードするために使用するファイルの場所を変更します。この修正プログラムをインストールすると、ダウンロードの際に、継続的なアクセスが確保されます。

・Internet Explorer Schannel.dll 修正プログラム

Web 上でリリースされた Internet Explorer 5.01 には、Schannel.dll ファイルに誤った内部キーが含まれています。これによって、SSL (Secure Socket Layer) または SSPI (Security Support Provider Interface) を使用しているプログラムやサービスが機能しなくなる可能性があります。この修正プログラムをインストールすると、修正された Schannel.dll ファイルによって問題が解決されます。

・Windows セキュリティ問題の修正プログラム - 1999 年 12 月 (1)

この修正プログラムによって、Microsoft Windows 98 の "Spoofed Route Pointer" 問題が修正されます。この問題によって、悪意のあるユーザーがお使いのコンピュータでソース ルーティングを実行し、ネットワーク情報やその他の情報を取得する可能性があります。お使いのコンピュータでソース ルーティングを無効にしていても、この問題は発生します。この修正プログラムをインストールすることによって問題が解決され、ソース ルーティングで追加コントロールを利用できます。

・Windows セキュリティ問題の修正プログラム - 1999 年 12 月

この修正プログラムによって、Microsoft Windows 95 の "File Access URL" 問題が修正されます。この修正プログラムをインストールすると、悪意のある Web サイトや電子メールのメッセージからこの問題を利用してコンピュータをクラッシュさせたり、悪意のあるコードを実行できなくなります。

・Internet Explorer セキュリティ問題の修正プログラム - 2000 年 1 月

このセキュリティ問題の修正プログラムをインストールすると、Internet Explorer の"Server-Side Page Reference Redirect" 問題が修正されます。この修正プログラムは、悪意のある Web サイト オペレータが、ユーザーのコンピュータにあるファイルを読み取ることができないようにします。ファイルを正しく読み込むために、悪意のある人物はファイル名とファイルの存在するフォルダ名を正確に知る必要があります。この修正プログラムには、以前にリリースされた "ImportExportFavorites" 問題の修正プログラムも含まれています。"ImportExportFavorites" 問題の修正プログラムをまだインストールしていない場合は、この新しい修正プログラムをインストールするだけで、両方の問題を解決できます。

・Windows 98 Telnet クライアントのセキュリティ問題修正プログラム

この修正プログラムは、Windows 98 に含まれる Telnet クライアントのセキュリティ問題を解決します。この問題を悪用した Web ページでは、ページを訪れたユーザーのコンピュータに被害を与える可能性があります。

・Windows 98 Second Edition シャットダウン問題の修正

シャットダウン問題の修正は、Windows 98 Second Edition に特有のハードウェア/ソフトウェア構成のシステムで、シャットダウン時に発生する問題に対処する修正プログラムです。この修正プログラムをインストールすると、"シャットダウン" を選択してもシステムが再起動する問題やシャットダウン中にシステムがハングアップする問題を解決できます。

・Microsoft virtual machine のセキュリティ問題修正プログラム

この修正プログラムを使用すると、Microsoft virtual machine (Microsoft VM) の"Virtual Machine Verifier" 問題が修正されます。この問題では、Web ページ上の悪意のある Java アプレットによって、ページを訪れたユーザーのコンピュータにあるファイルの読み書きや削除が実行される可能性があります。

・Microsoft virtual machine

最も速く最も信頼できる方法で Java アプリケーションをコンピュータ上で実行でき、アニメーションなどの高度な Web ページ機能を体験できます。注: これは、Microsoft VM のアップデート版です。

Windows Update 以外にもある修正プログラム

日本語版 IE5.01 の個別の問題について、現在修正プログラムで対応できる問題は次のようである。もちろん IE4.0 で問題となったものは、IE5.01 の標準の機能で対応されている。

・Java "VM File Reading" 脆弱性 MS00-011

・"Image Source Redirect" 脆弱性 MS00-009

・IE 5.01 Schannel.dll の問題 Q247367

・サーバー側参照リダイレクト脆弱性 MS99050(Q246094)

この他、IE5.01 で問題となるもので最近報告されているのは

- **Outlook Express 5 vulnerability**
  - Active Scripting may read email messages (2000.02.01)
- **IE 5.01 vulnerabilities in external.NavigateAndFind() (1999.12.22)**
- **IE 5.0 XML HTTP redirect problems (1999.11.23)**
- **IE 5.0 and Windows Media Player ActiveX object allow checking the existence of local files and directories (1999.11.14)**

これらはアクティブスクリプティングを無効とすることで回避できる。デフォルトのセキュリティレベル高に設定するだけでは不十分なので、教訓によりデフォルトの設定を変更する。ただし、世の中のたいていの Web サイトは大変閲覧しにくくなるので、あまりムキになってはいけない。セキュリティ問題はいまやそれほど単純なものではなくなってきているので、ムキになるとインターネットは使えなくなる。例えば、Cross-Site Scripting 問題は、Web ユーザーからデータを受け取り、それをもとにダイナミックに生成したページをブラウザに返しているような Web サイトに関連するセキュリティ問題で、CGI 等経由で JavaScript など Web スクリプトを埋め込んでしまうことによる攻撃が可能というものである。この問題はクライアント側の対策だけでは不十分で、Windows に限ったことでもない。スクリプトが実行できることが問題になる。

* この問題の詳しい解説は「Cross-Site Scripting 問題とは？」を参照のこと。
http://plaza14.mbn.or.jp/~sysport/sysport/kb/security/css.htm

3. Windows NT 4.0 Server のセキュリティ

最近学校関係に Windows NT 4.0 Server が導入されているケースが多いが、セキュリティに関してはおそらく十分だとは言い切れない。その理由は多くが WINS を使う設定であり、業者がインストール済みのサーバーを持ち込んで設定していくケースがほとんどだからである。そしていったん稼働するとその後サービスパックすらインストールしないで、そのまま運用され続けることが多い。以前から提案しているように Windows NT 4.0 Server をインターネットサーバーとして利用するなら、スタンドアロンでインストールし WINS は使わないのが望ましい。できれば NetBIOS サービスもバインドしない方がよい。ここでも教訓を思い出し、デフォルトでは使わないようにしなければならない。サーバーのセキュリティ設定は OS をインストールするときから始まるので、構成をよく考えた上でインストールとセットアップをおこなうのが大切である。その上で情報収集をして、最新の修正プログラムやサービスパックを導入し、必要なら再構築、再インストールを行わなければならない。

Windows 環境のセキュリティについて、詳細な解説は次の「**Windows NT/2000 セキュリティ対策**」を参照のこと。http://www.port139.co.jp/ntsec_ppt.htm

数十ページのパワーポイントの資料で、オープンコンテンツライセンスとなっている。HTML版も用意されている。このページの作者である伊原秀明氏は次の書籍の監修者でもある。

（株）翔泳社　Windows NT セキュリティ　Tom Sheldon 著　トップスタジオ訳

また、IIS サーバーインストールの作法については、次の手順が参考になる。

IIS 4.0 インストール(2000/2/8 更新)

http://www.port139.co.jp/ntsec_iisinstall.htm

MSKK 推奨手順

http://www.asia.microsoft.com/japan/products/ntupdate/nt4sp5/sequence.htm#iis40

Windows NT Server 4.0 インストール ガイド （SP6a までのインストール）

http://www.microsoft.com/japan/technet/deployment/NT4Inst/

Windows NT 4.0 Server SP6a 以降の修正プログラム

現在サービスパックの最新版は 6a である。サービスパックもただあてるだけでは効果がない場合もあるので、レジストリの追加変更するなどの設定が必要である。

例：ソースルーティングを無効にする

サービスパック 6a を適用するとソースルート制御ができるようになる。ただし、デフォルトでは有効になっていないので、教訓に従いデフォルトを変更する必要がある。それにはレジストリを追加設定する。

レジストリキー：

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters

値の名：DisableIPSouceRouting

データ型：REG_DWORD

値：0･･･ソースルーティングを有効にする（デフォルト設定）

1･･･IP 転送が有効な時にソースルーティングを有効にする

2･･･ソースルーティングを完全に無効にする

SP6a 以後に見つかったセキュリティ問題

- **ワークステーションの共有でごみ箱のアクセス権が設定できてしまう (J052253)**
- **Patch Available for "Spoofed LPC Port Request" Vulnerability(J052067)**
- **Syskey Keystream Reuse Patch (MS99-057 "Malformed Security Identifier Request" Vulnerability の修正を含む) (J051850,J051851)**
- **Malformed Resource Enumeration Request (Q246045)**
- **Unchecked Print Spooler Buffer May Expose System Vulnerability (J050919)**
- **How to Prevent Predictable TCP/IP Initial Sequence Numbers (J050737)**
- **Security Descriptor Allows Privilege Elevation on Remote Computers (J050713)**

さて、仮に最新のサービスパックをあて、修正プログラムをインストールし、port139 の作法に従ってWindows NT IIS サーバーを構築したとしても安心はできない。セキュリティに完全はないとよく言われるように、サーバーだけでセキュリティが守れるわけではない。必要なセキュリティポリシーを実現するために、それではどうするのかというと、Windows 環境以外でのセキュリティ対策でカバーすることである。

・ルータやRRAS やProxy のパケットフィルタで不要なパケットを落とす

例：ログに記録された不正利用の発信元やポートを止める

00/01/05　　午後 6:58:54　Dns　　警告　　なし　　5000　N/A　　NS

DNS ｻｰﾊﾞｰは大量のﾗﾝﾀｲﾑ ｲﾍﾞﾝﾄﾛｸﾞを記録しています。 これは通常、不良、または予期しないﾊﾟｹｯﾄの受信、 過剰な複製ﾄﾗﾌｨｯｸに関する問題、または複製ﾄﾗﾌｨｯｸ自体に原因があります。 不良ﾊﾟｹｯﾄの発信元に関する情報については、以前のｲﾍﾞﾝﾄ ﾛｸﾞ ｴﾝﾄﾘを参照してください。 これらのｲﾍﾞﾝﾄ ﾛｸﾞを現在収集していません。

00/01/05　　午後 5:05:27　Dns　　警告　　なし　　5504　N/A　　NS

DNS ｻｰﾊﾞｰは、192.117.147.131 からのﾊﾟｹｯﾄに無効なﾄﾞﾒｲﾝ名を検出しました。
ﾊﾟｹｯﾄは拒否されました。

・公開するWWW データはZIP ドライブに入れてライトプロテクトをかける

ホームページの書き換え事件が頻発しているが、ZIP などにデータを移しライトプロテクトをかけることにより、それをはずさない限り管理者でも書き換えはできなくなる。バックアップを兼ねて同じ内容のものを２枚用意しておけば、データの更新なども ZIP の入れ替えだけですむ。パフォーマンスがハードディスクより落ちるが、Proxy などでキャッシュをすることによりカバーできる。

・Microsoft Proxy Server 2.0 + SP1 を導入してクライアントを内部へ入れる。

Proxy サーバーを導入することで、内部のLAN を守ることはある程度可能である。WWW を内部に置いてProxy で外部からの要求を選択的に中継することもできる。ただし、Proxy そのものが不正中継に利用されることがあるので注意が必要である。教訓に従い最新のサービスパックをあて、セキュリティ対策を怠らないこと。

＊ Microsoft Proxy Server の詳細情報や評価版は次を参照のこと。
http://www.microsoft.com/JAPAN/BackOffice/Proxy/default.htm

4. 情報を知らないことが最大のセキュリティホール

Windows 環境に限らず、管理者はセキュリティ情報の収集につとめなければならない。新しいセキュリティホールが見つかれば、それを利用した攻撃ツールが現れる。そして多くの場合、新しい攻撃ツールに対する対策をしないまま運用されているサイトが被害に遭う。最近話題の DDos (Distributed Denial of Service) attack ツール TFN2K は、ICMP echo などを使うらしく Linux, Solaris, Windows 環境で動作するし、BIND も実験しようと思っている間に 8.2.2 でも patchlevel により古いものは安心して使えないといわれる。以前は Microsoft を使わなければ良いなどといわれたが、いまやすべてのプラットフォームにセキュリティホールはある。ただ Microsoft ほど話題にならなかったり、公表されていなかったりの違いがあるだけである。情報を知らないことが最大のセキュリティホールになるのが、今のインターネット社会である。Windows 環境に限らず、サーバーを公開することによるリスクを知り、情報を収集して適切な対応をとることが必要である。

kenji@kawabe.net