ネットワークセキュリティの現状

情報処理センター
江藤博文
etoh@cc.saga-u.ac.jp

日本でも政府機関のホームページが何者かによって書き換えられるということが新聞やテレビで話題になっています。このようにネットワークは便利な半面、常に悪意のある者により攻撃の対象となっています。佐賀大学のネットワークにおいても過去から現在に到るまで何度と無く攻撃を受け続けています。ここではネットワークセキュリティの現状について報告します。

1 ネットワーク攻撃

ネットワーク攻撃はネットワークに継っている全てのコンピュータを対象としています。ネットワークへの攻撃にはいくつかの種類があり、コンピュータが継っているかどうかの確認をするだけのものから、サーバダウンを引き起こしたものまであります。

1.1 弱点の探索

(1) telnet による接続の試み
組織内の IP アドレスに対して順に telnet 接続を試み、その応答によりシステムの種類やバージョンを確認します。システムによってはセキュリティ上問題が存在する事があり、外部から侵入される等の攻撃を受けます。

(2) ポートスキャン
ネットワークに接続されているコンピュータにはそれぞれに固有な IP アドレスが割り振られていますが、個々のコンピュータには更にメール等のサービスの種類毎にポート番号と呼ばれる番号が存在します。ポートスキャンはコンピュータの各ポートを順に探索し、弱点をみつけるものです。

1.2 サービスの不正利用

(1) メールの不正中継
メールサーバの設定が不十分のために、本来利用者ではない組織外から不正にメールサーバを利用されます。不要なメールサーバは止めるか、セキュリティの設定を強化し、不正な中継を禁止することが必要です。

(2) anonymous(匿名)FTP サーバの不正利用
anonymouse FTP サーバはネットワーク上で公開されているフリーソフトなどが置かれ誰でもダウンロードが可能となっているサーバです。サーバの設定が不十分であると、不特定の人物が勝手にファイルを置くことができ不正なファイルを中継する FTP サーバとして利用されます。

(3) プロキシ (代理) サーバの不正利用
WWW などのサービスの効率化、ネットワークの負荷軽減のために使用されるのがプロキシサーバです。セキュリティ上の設定が不十分なために、発信元を偽るなどの不正な利用が行われます。

(4) 踏台

他人になりすましてコンピュータにログインし、そこから他のコンピュータを攻撃します。これは何個所かの踏台を経由することで、攻撃元のコンピュータの場所の特定をされないようにするために行われます。不正なログインが無いかなどのチェックが必要です。

1.3 サービスの妨害

(1) 大量のメールの送信

大量のメールをメールサーバに送りつけ、サーバをダウンさせるものです。情報処理センターメールサーバにも同様の攻撃が行われ、メールサーバがダウンしました。サーバのメール配送を一時的に停止し復旧作業を行いましたが、復旧までの数時間情報処理センターのメールが使用不可能になりました。

1.4 その他

(1) SPAM メール

管理者やメールアドレスが公開されているユーザに来るダイレクトメールなどの不要なメールです。1日に数通程度来ますが、ほとんどが発信元を偽り、不正な中継を行って発信元を隠蔽しています。この発信元には上記メールサーバの不正中継が利用されています。

(2) メールに添付されるファイル

メールそのものは単なるテキストファイルなので読んだだけでは問題無いですが、ファイルが添付されている場合には注意が必要です。

(a) 添付ファイルが実行形式の場合

実行する事により感染するウィルスです。ウィルスによっては勝手にメールにウィルスを添付して被害を拡大するものもあります。

(b) 添付ファイルが Word や Excel のファイルの場合

Word や Excel などのファイルには悪意のあるマクロが書かれているものがあります。マクロによってはコンピュータ内の全てのファイルが消されたりする事があります。

(c) 添付ファイルが html ファイルの場合

添付ファイルに html が添付されている場合、Netscape などのブラウザで読むことになります。この html ファイル中に悪意のあるスクリプトを埋め込まれていた場合には何らかの被害が起こることがあります。

2 おわりに

ネットワーク攻撃に対して強固なファイアーウォールを導入することも考えられますが、引き替えに利便性が損なわれるなど、現状では導入は難しいと考えます。

最終的には自分の身は自分で守ることが重要となります。セキュリティ技術は日進月歩です。常にセキュリティに対する最新情報を入手しておきましょう。日本ではコンピュータ救急対応センター (JPCERT/CC) † 等でセキュリティに対する最新情報が報告されています。

†http://www.jpcert.or.jp