最近のセキュリティインシデントと情報セキュリティ対策推進室の活動

竹 内 義 則

Ⅰ．ウィルス

３月の終わりからNICE内部でNetsky.Qが大流行しました。これは，ウィルススキャンサーバのデータベース更新前に学内に大量にウィルスメールが入り込んだためです。しかし，このウィルスは，Windowsの修正パッチがあたっていないコンピュータでプレビューするか，添付ファイルを意図的に開かない限り，感染することはありません。これが，学内で広まったということは，修正パッチのあたっていないWindowsが多いか，ウィルスに対する認識が欠如している（疑いもせずに添付ファイルを開いてしまう）ことを示していると思います。

その騒ぎが収束した５月の終わりごろ，今度はSassorが広まりました。これは去年流行ったMSBLASTと同じように，Windowsの修正パッチがあたっていないコンピュータを探して，つぎつぎに攻撃していきます。しかし，MSBLASTとは，感染に使用するポートが違っています。MSBLASTの場合，普通は使用しない135番ポートだったため，ルータで遮断することによって感染をサブネット内に封じ込めることができました。しかし，Sassorの場合，445番ポートを使用します。これは，プリンタ共有などで問題が出る可能性があるので遮断していません。したがって，学内に１台でも感染しているホストがあると，サブネットを越えて攻撃し，修正パッチがあたっていないコンピュータは感染します。この種のウィルスの特徴は，感染するとすぐに攻撃を始めることです。ウィルスの被害者のみならず，同時に加害者になってしまいます。このウィルスは，Windows Updateによって，最新のセキュリティパッチをあてておくだけで，容易に防げるものです。いまだに，MSBLASTやWelchiaに感染している端末があるということから，学内にWindows Updateがあたっていないコンピュータが，まだ多くあるということがわかります。

Ⅱ．P2Pによる著作権侵害問題

WinMX，WinnyなどのP2Pソフトウェアを使用して，音楽ファイルなどを送信しているという苦情が届いています。このような他人の著作権を侵害する行為は，大学内はもちろんのこと自宅でも絶対にしないでください。もちろん，刑事処分の対象となり，現に逮捕者が出て，罰金40万円の略式命令も出ています。また，刑事処分のみならず，権利者から民事上の差止請求及び損害賠償請求の対象にもなります。特に，大量の著作物を長期間に渡って送信し続けた場合には，高額の損害賠償請求になり得ます。

WinMXは，７月２日に最新版（3.53）がリリースされています。この際，通信で利用するサーバのアドレスが一部変更されたために，学内からサーバにアクセスできる状態になっていました。

これについては，９月１日に新たに遮断するように対策をとりました。

Winnyは，５月10日に開発者が逮捕され，世間の注目を集めました。Winnyは，通信が暗号化されているからわからないということは，すでに崩れ去っています。６月28日に東京電機大学で行われた「Winny事件を契機に情報処理技術の発展と社会的利益について考えるワークショップ」で，暗号化アルゴリズムの詳細があきらかにされました。それによると，通信直後に共通鍵がそのまま入っているため，簡単に解読できてしまうそうです。したがって，Winnyの通信を傍受することも十分可能です。WinMX，Winnyは，いろいろな組織で著作権侵害の有無について監視しています。大学，企業等でP2Pの使用状況を監視するサービスを提供する会社もあらわれています。九州大学に導入し，監視を開始した事例はニュースにもなりました。

一方，最近ではP2Pソフトウェア（bittorrent）を使って，DebianやFedoraなどのLinuxのディストリビューションやMozilla（webブラウザ）などのオープンソースソフトウェアの配布が始まっています。大きなファイルのダウンロードは，従来のクライアントサーバ方式では，たくさんのアクセスが特定のサーバに集まるので，サーバに負荷が集中してしまいます。一方，P2P方式では，それぞれの端末がダウンロードとアップロードを同時に行うため，ファイルの提供者に負荷が集中しにくくなります。このような使い方は，ファイルの入手だけでなく，研究成果を多くの人に配布し使ってもらうといったことに有用です。

情報セキュリティ対策推進室では，書面やパンフレットなどで著作権侵害行為を行わないように呼びかけているところですが，今後も，啓発活動を続けていきます。

Ⅲ．オープンプロキシによる不正な中継

プロキシサーバとは，ユーザに代わって業務を代行するサーバのことです。インターネットとローカルネットを遮断した状態は，インターネットからの不正な侵入や，内部からインターネットへの不正なアクセスを防ぐセキュリティを実現しています。この状態で，内部から外部へのウェブの通信を行いたい場合にプロキシサーバがよく使われます。すなわち，インターネットとローカルネットを繋ぐファイアウォールでプロキシサーバを起動し，ローカルネットのユーザの通信をプロキシサーバが代理として行うことによって，通信が可能になります。

また，ウェブのデータを一時的にキャッシュしておくことによって，次回，同じデータが必要な場合は，そのキャッシュからすぐに取り出せます。このように，無駄な通信の削減に役立ちます。以上のような理由から，プロキシサーバは広く使われています。通常，プロキシサーバは，ローカルネット内のユーザなど限られた人物から使用されています。

しかし，もし学内に誰でもアクセスできるプロキシサーバがあると，そのネットワークに多大な迷惑がかかります。このような誰でもアクセスできるプロキシサーバを，オープンプロキシサーバといいます。オープンプロキシサーバの情報は，ウェブサイトなどで共有されているので，世界中からそのサーバにアクセスがかかります。場合によっては，そのネットワークのバンド幅を食いつぶしてしまうかもしれません。

また，学外の人が学内のプロキシサーバを使ってアクセスした場合，アクセスされたウェブサ

イトは，学外からではなくて，学内からアクセスがあったと判断されます。その結果，もし，アクセスした人物が掲示板に落書きした場合，学内からその掲示板に対して落書きしたと思われます。また，学内の人がダウンロードできるように図書館で契約しているオンラインジャーナルも，学外の人物がダウンロードできてしまいます。実際，以上のような苦情もきています。学内専用として公開しているウェブページも，学内のプロキシサーバを経由すれば学外から見えてしまうのも問題として挙げられます。

このような問題があるため，学内にオープンプロキシサーバは存在してはいけません。各コンピュータの管理者の方は，設定ミスでオープンプロキシサーバになることを防ぐのはもちろんのこと，セキュリティに関するパッチをあてて，外部から侵入されてオープンプロキシサーバを立ち上げられるといったことのないように，日ごろの管理の徹底をお願いします。

（たけうち　よしのり：名古屋大学情報セキュリティ対策推進室）