

## 学校におけるインターネットの安全対策（事例として）

### 1 問題の発生

#### (1)「テレビ会議」システムを授業で使う準備

コンピュータの教育利用を考えている本校の教員とMS-Messengerを「テレビ会議」として利用できないか実験するために、校長宅にADSL回線を引いた。自宅に設置したルータは工場出荷時には、UPnPに対応していなかったため、ファームウェアをルータ製造会社のWebページからインストールした。

##### ①ルータの設定（ポートの開放）

学校ホームページを校長宅からも更新できるようにしてあったが、ルータ設置後「ファイル転送プログラム」がWebサーバに接続できなくなってしまった。マニュアルを調べてみると、ルータのファイアウォール機能の設定により、外部から内部へのすべてのポートが閉じてあった。さらに、『フィルタリング設定』の項目に『FTPサーバにアクセスできない場合は、インターネット側からホーム側へ、エントリ60番の項目を「許可」にしてください』と書かれていたので、設定変更を行った。これが問題を発生した。

##### ②安全対策の研究

また、ハッカーやアングラ(地下組織つまりUnderGroundの略)といわれる人達は、どんなことをしようとしているのかを調べて、管理職(校長)として安全対策をしようと考え、それらのホームページを閲覧した。実は、これが後に問題を引き起こす原因となった。

#### (2)不正使用者の発覚

##### ①プロバイダへの接続不良

一ヶ月過ぎた頃、妙にWebの表示速度が遅くなったのに気づいて、回線速度を測定してみると、当初の5Mbpsから500K～1Mbps程度に落ちている。さらに、午後8時から10時くらいの時間帯にホームページを更新しようとする、「ファイル転送プログラム」がWebサーバに接続できないという状況が発生してきた。そこで、プロバイダに『回線が込み合っている場合は、接続できないことがあるのか?』と問い合わせたところ『そういうことはない。』という回答だった。プロバイダのSEが回線状況を調査して、結果をメールで送ってくれるということになった。

##### ②多重接続と侵入の確認

SEからの回答によると、『多重接続が確認された。その時間帯にインターネット接続やメール接続もできないならそれが原因と考えられる。また、ルータを利用しているなら、その誤動作も考えられるので、同時接続を行う設定になっていないかどうか確認してほしい。さらに、インターネットやメール接続に問題がないなら、パソコンで自動プログラムが起動されていないかどうか確認してほしい。』とのことであった。

ルータの設定を調べたが同時接続はしていない。また、自動プログラムが動いているかどうかを調べたが、わからなかった。

そのうちに、OutlookExpress が繋がらないという状況が頻繁に発生するようになってきた。しばらくすると WindowsXP を終了する時に、『他の人がこのコンピュータに LogOn しています。いま電源を切るとその人のデータが失われる可能性があります。よろしいですか(y/n)?』という表示が出るようになった。今度こそまちがいなくパソコンに外部から侵入されたことがわかった。

### ③ IDとパスワードの盗難

IPAセキュリティセンターにメールで助言をお願いしたところ、『おそらく怪しいページを閲覧したときに不正なプログラムを埋め見込まれたか、あるいはIPアドレスを特定されて侵入されたと思われる。不正なプログラムはワクチンソフトやスパイウェア検出ツールなどでは発見されない可能性が高い。このような場合は、PCを再インストールすることを勧める。また、多重接続されているとのことから、利用しているユーザIDとパスワード情報を盗まれ、プロバイダに同じIDとパスワードを使って接続されているためと思われる。再インストール後に不正アクセスを防止するためのパーソナルファイヤーウォールソフトのインストールをお勧めする。その後パスワードを変更する。また、今後怪しいサイトにはアクセスしないようにする。ホームページを閲覧しただけで不正なプログラムを送り込まれる可能性が十分にある。』との助言をいただいた。

## 2 問題発生の原因

### (1)ルータのポートの開放

先にエントリ 60 番の項目を許可したと述べたが、次のように設定してあった。

No	タイプ	方向	送信元		宛先		プロトコル
			IP アドレス	ポート	IP アドレス	ポート	
..	..	...	..省略..	...	.....	...	.....
60	許可	W→L	*	*	*	*	TCPEST
61	禁止	W→L	*	137-139	*	137-139	TCP&UDP
62	禁止	W→L	*	*	*	*	TCP&UDP
63	禁止	W→L	*	137-139	*	137-139	TCP&UDP
64	禁止	W→L	*	*	*	*	TCP&UDP

そのため、外部 (W) から内部 (L) へデータを通過させるポートをガラアキにしてしまい、侵入しやすくしてしまっていたことが原因の一つであった。

二つめの原因は、UPnP にあった。UPnP に設定しておく、Messenger を起動したときに「TV 会議」や「ファイル転送」などに必要な TCP&UDP のポートを大量に開けてしまうのである。しかし、Messenger を終了しても開けたポートを自動的に閉じてはくれない。ルータの UPnP 設定で、「無制限、1 時間、2 時間・・・」の中から指定することで、

その時間が経過するとポートを閉じるという仕組みになっていた。本校の場合は、「無制限」に設定され、開いたままになっていたことも大きな原因であった。

#### (2)スパイウェアの検索と駆除

加入しているプロバイダのSEからは、「最近、パソコンの動作がなんとなく遅くなっていませんか？ スパイウェアが送り込まれて、見えないところで動いていて、パソコンの中のデータを送信している可能性もあるので、SpyBot\_Search&Destroyというスパイウェア除去ソフトをダウンロードして実行してみてください。」といわれた。このソフトを実行してみたところ、レジストリやクッキーなど、15個がスパイウェアに汚染されていた。SEの話によると、このソフトでも検出できないものがあるので、パソコンの再インストールを行うことにした。

### 3 安全対策

#### (1)SEからの助言

プロバイダのSEからの指導は、次のようなものであった。

①PCの再インストールをする。

②パーソナルファイヤーウォールをインストールする。

※ パーソナルファイヤーウォールをインストールする前にインターネットに接続しないこと。このわずかな間にもパソコンに侵入される可能性がある。

③その後、インターネットに接続する。

④スパイウェア駆除ソフト(SpyBot\_Search&Destroy)をダウンロードし、パソコンにインストールして実行する。そして、免疫をかけておく。

⑤Windowsのアップデートをする。

⑥プロバイダに接続するためのパスワードを変更する。

※ それでもダメなときは、IDとパスワードの両方を変える。

⑦ルータのファイヤーウォールをきちんと設定する。

※ 必要最低限のポートのみ開け、他はすべて閉じること。

⑧UPnP機能は使わない様に設定しておく。

⑨無線LANも使わない様に設定しておく。

※ 無線LANから侵入される場合もある。

⑩使わないときはルータの電源を切っておく。

※ ルータの電源が切れていれば、外部からポートをスキャンできない。

#### (2)パーソナルファイヤーウォール

安全対策を施した後に、NortonInternetSecurityをインストールした。このパーソナルファイヤーウォールを選定した理由は、Messengerやチャットをしている時でも常時外部からの侵入、内部からの個人情報の漏洩などを監視できるからである。パーソナルファイヤーウォールの中には、チャット中の監視ができないものもあるので、利用形態によって選定する必要がある。その後、インターネットに接続し、SpyBot\_Search&Destroyをダウ

ンロードし、スパイウェアの削除と免疫化を実行した。さらに、プロバイダに接続するためのパスワードを変更した。

### (3)ポートの閉鎖

ルータのファイヤーウォール設定で、最初のようにエントリ 60 番の項目を許可にしてみようとポートがガラアキになって侵入されやすくなる。そこで必要最小限のポートだけ開けることにした。

ルータのマニュアルには、Web サーバにアクセスできるようにするために、『インターネット側からホーム側に TCP20 番ポートを通過するフィルタを設定する』と記載されていたので、TCP の 20 番ポートの W→L を許可にしたが、Web サーバにアクセスできなかった。Web 作成ソフトのマニュアルには、「ファイル転送」プログラムは 21 番ポートを利用するとあったので、21 番ポートの W→L を許可にしたが、それでもダメであった。

数日経って、あるホームページに、ADSL 回線の場合は「ファイル転送」プログラムの「詳細設定」の中から『パッシブ(Passive)モード』に設定するようにと書いてあったので、そのように設定したところ、やっと Web サーバに接続できるようになった。

### (4)Windows のアップデート

Windows には、様々なバグがあり、ハッカー達はそのバグを利用して不正侵入やウイルスを作成しているようである。Windows のバグが見つかるとその修正プログラムが Web で提供されるので、常に最新の状態に保っておくことが必要である。そのため、Windows のアップデートを行い、その後は自動アップデートに設定した。

### (5)ハッキングツール対策

#### ①無線LAN

ある SE は、マンションの 3 階に住む会員から「最近、Web の表示が妙に遅くなった。」との苦情を受け調べてみると、多重接続が確認されたという。早速訪問して PC を再インストールし、パスワードも変更してみたが、それでも多重接続されている。結局、2 週間も苦労してわかったことは、近所のアパートに越してきた男が、無線 LAN の不正接続ツールを使って不正接続し、Web の閲覧をしていたということだった。

ワゴン車に PC を積み、無線 LAN の不正接続ツールを使って接続できる地点を調べ、Web 上の地図にマークを付ける「マーカー」という遊びがハッカー達の間で流行しているという。ハッカー達は、これを踏み台にして、他のコンピュータに不正侵入を試みているという。個人のセキュリティをしっかりとしないと、日本は大変なことになりそうである。

#### ②スパイウェア

スパイウェアの中には、キーボードを叩いた通りに、キーのアルファベットを記録し、それをメールで送信する「キーロガー」というものがあるという。これを送り込まれたら、PC に LogOn するための ID やパスワードも簡単に盗まれてしまう。また、キャッシュカードを利用している場合は、ID やパスワードを盗まれて不正使用されてしまう。スパイウェアを侮ってはならない。

③インターネットセキュリティ

その後しばらく PC を使っているとインターネットセキュリティソフトから、『外部から不正にアクセスされています。どこからアクセスされているか調べますか?』というメッセージが出た。「yes」をクリックすると、世界地図が出て関東のある県に「×」印が表示された。おそらくセキュリティソフトを入れてなかったら、不正アクセスにも気づかなかったであろう。私達が考える以上に、不正アタックは頻繁になされていると見る必要がある。

④インターネット関連雑誌

最近、コンビニに様々なインターネット関係の雑誌が並んでいる。その中に「ハッカーからこうして PC を守れ!」という特集があった。付録の CD には、侵入するために使うハッキングツールが入っており、これを使えば、ちょっとパソコンの知識がある者なら、簡単にハッキングができる。私達は、世の中はこんな状況になっていることを知った上で、しっかりとしたセキュリティ対策を施しておく必要がある。

その雑誌に載っていた内容であるが、学校のコンピュータにファイルのダウンロードツールを忍び込ませ、夜中にアダルト画像や音楽ファイルをダウンロードし、自宅の PC に自動送信させたり、翌日に USB 対応のハードディスクを持って行って抜き取ったりするなどという方法が解説してあった。

また、先生用のパソコンが起動していたら、キーロガーというツールをインストールしておき、先生がキーボードを打ったときの「キー情報」を記録しておき翌日それを見れば、ID やパスワードが簡単に盗めるなどというものであった。

操作能力が高まってくると、中・高校生ではこの位の操作は簡単にやれそうである。

4 学校内における情報セキュリティポリシーの確立

(1)ファイヤーウォールの設定

開いているポートが多いほど外部から侵入されやすくなるので、日常使うために必要な最小限のポートだけを開け、他は閉じておく必要がある。

大量のポートを開けてしまう Messenger やテレビ会議システムなどを利用するためには、中途半端な知識を持った教員にルータのファイヤーウォールの設定を任せるべきではない。やはり、豊富な知識を持った専門の SE に任せるべきである。

(2)ネットワークセキュリティ

①無線 LAN

最近は無線 LAN Card の規格が統一されたため、不正接続がしやすくなっている。電波は 50m 位飛ぶため、道路に止めたワゴン車などの中から、接続ツールを使って侵入し、ID やパスワードを盗まれるという事件が多発しているそうである。不正接続された PC から他のコンピュータに侵入したり、学校のサーバに保存してある生徒の住所・電話番号や成績データなどを盗まれたりする可能性もある。使用しない場合は、無線 LAN アンテナのス

イッチを切っておくなどの慎重な対策が必要である。

②インターネットセキュリティソフト

メールに添付されてくるウイルス対策も重要であるが、現在では、コンピュータに侵入されたり、スパイウェアを送り込まれて知らないうちにIDやパスワードを盗まれたりすることの方が心配である。インターネットセキュリティという、ウイルス駆除、スパイウェア駆除、外部からの不正な接続の監視、外部への不正なデータ送信の監視、各ポートの監視、外部からの不正なソフトの送り込みの監視、怪しいWebページにアクセスできないようにするフィルタリングなどを自動的に行ってくれる「総合ソフト」が必要になっている。

チャットやMessenger、TV会議などを使う場合は、その最中でも監視してくれる機能をもったセキュリティソフトをインストールしておくは必須である。

③スパイウェア

スパイウェアは、リサーチ会社が商品販売などに必要なデータを収集するため、その人が閲覧したWebページのアドレス等をこっそりと送信させるためのソフトであった。これはクッキーと同様なものであるため、入ったことにまったく気づかない。ただし、見えないうちで常時実行されているため、いくつも入っているとコンピュータの処理速度が遅くなっていく。

キーロガーのように入力したキーボードのアルファベットを記録し、コンピュータから送り出すものもある。カード決済をしている人の場合、IDとパスワードを盗まれ、カードを不正使用される危険がある。したがって、これらのスパイウェアが活動して内部からデータを送り出すのを遮断するためにもインターネットセキュリティは必要である。

また、スパイウェア駆除ソフトのデータを最新に保ちつつ、定期的に行うことも必要である。

(3) 日常的なセキュリティ対策

①フィルタリング

アダルトやハッカーなどの怪しいホームページにはIPアドレスや生のメールアドレスを抜き出す仕掛けがしてある。そのIPアドレスを手がかりにしてコンピュータに侵入を試みたり、コンピュータからIDやパスワードを自動送信させたりするツールを添付したメールを送りつけてくる。したがって、怪しいページを見たら手遅れである。学校では、怪しいページが見られないようにしっかりとフィルタリングをかけておく必要がある。

②ウイルス駆除ソフト

これも自動アップデートに設定して、ウイルスに対応する新しいデータが出たらすぐにダウンロードしてウイルスチェックをする必要がある。コンピュータ主任を中心として、常時活動していく校内組織を整備しておく必要がある。

③Windowsのアップデート

Windowsは、かなりバグを含んだままのOSであり、ハッカーはこのバグを利用してコンピュータに侵入する。それを防ぐには、そのバグを修正するためのソフトを自動的にダ

ウンロードするように設定しておく必要がある。

④ルータや無線 LAN アンテナの電源

コンピュータを使用していない真夜中などに外部から侵入を試みられないように、使わない時間帯はルータの電源を切っておく。電源が切ってあれば、外からルータを見ることはできないため、ポートスキャンをかけたり、侵入を試みられたりする心配はない。無線 LAN についても同様である。

⑤教員のパソコンのセキュリティ

学校に教員用のパソコンがないため、教員は個人のパソコンを使って仕事をしている場合が多いと聞く。今回の場合の教訓でもあるが、学校のセキュリティがいくらしっかりしていても、教員の自宅のセキュリティが甘かったら、それが弱点となって学校のシステムに侵入される可能性がある。教員個人のパソコンにも、安全対策として公費でセキュリティソフトを購入してインストールさせるくらいの補助が必要である。