学校におけるセキュリティ対策

南山大学数理情報学部情報通信学科教授
後藤邦夫

1．はじめに

学校がインターネットに接続され，教育に活用されることは素晴らしいことだが，そのためには，学校のネットワークとコンピュータなどの機器と蓄積され流通する情報がきちんと管理されていなければならない。管理が不十分であれば，学外から悪意やいたずらによる不正アクセスの被害を受けるだけでなく，何らかの方法で校内に侵入した不届き者や内部のいたずら者による他組織への迷惑行為が起きることもある。

本稿では，このような問題が起きないようにするための考え方と不幸にして問題が起きてしまったときの対処例を紹介する。

2．セキュリティポリシ

問題がめったに起こらないのであれば，起こったときに，個別に判断すればよいが，急激に増えて来たウイルス感染から，個人情報流出に至るまでの様々な事件が発生する今日では，あらかじめ方針を立てておかなければ，対処しきれない。その方針をセキュリティポリシと呼ぶ。ここでいうセキュリティとは直訳すると安全性だが，情報の漏洩防止（機密性），情報やそれらの処理が正確であること（完全性），そして正当な利用者がいつでもシステムを使えること（可用性）の 3つを維持することである。人為的な攻撃だけでなく，地震，落雷，ビル内の水洩れなども安全性に対する脅威となることを忘れてはならない。

2.1　情報セキュリティポリシとマネジメントシステム

セキュリティポリシを策定するときに，ネットワークだけを対象とする場合と情報システム全体を対象とする場合がある。後者を情報セキュリティポリシと呼び，情報とその取り扱い，情報を蓄積・加工するコンピュータ，そして情報を伝送するためのネットワークのすべてを対象に含むので，できれば各学校では，情報セキュリティポリシの方を考えてみて頂きたい。

この2年間に多数の事件が報道され，日本でもセキュリティポリシの重要性が認知されてきたといえる。例えば，http://www.atmarkit.co.jp/fsecurity/で公開されている読者を対象とした調査（回答数296）では，読者の勤務先のポリシ策定率は44％，予定/検討中が26％ である。教育機関では，コンピュータやネットワーク利用規則がほとんど整備されているが，セキュリティポリシをすでに持っている学校は少ないと思われる。大学ではポリシ策定に取り組みはじめているところである。小中高校でも簡単なものを考え始めるべき時期に来ているだろう。

セキュリティポリシは，結局文書として表現されるものだが，作文すればおしまいではない。ポリシ文書は最高責任者はもとより全構成員が認めるものでなければならず，さらに実際に運用できる体制も整える必要がある。したがって，予算や人事も関係してくるので，最高責任者を含めた委員会組織で検討する必要がある。この体制も含めた一連のシステム，すなわち「情報セキュリティマネジメントシステム （ISMS)」を構築することが重要といわれていて，国際標準、認証システムなどもできつつある。

2.2　情報セキュリティポリシの作り方

文書はいちから作成するのには大変な手間がかかる。業者にコンサルティングを受けることもできるが，多大な費用がかかる。あまり楽をすると文書作成だけにおわってしまい，だれも守らない全く役に立たないものができあがってしまうので作成過程における議論をとばしてしまわないように注意する。最初は文書例を調べ，それを各学校の実態に合わせて修正するのが現実的である。例えば，大学向けの考え方は，

http://www.sinet.ad.jp/info/policy/index.html
で公開されている。

文書は以下の3層で構成することが多い。

1）簡潔な基本方針
2）対策基準（ウイルス対策，サーバ管理，など分野別）
3）実施手順（管理者，利用者など対象別向けガイドなど）

これらの文書のうち，実施手順の一部の利用者向けガイド（利用規則），管理規則など，すでにある文書もこの機会に上位の方針と基準に合わせて改訂する必要がある。対策基準は，公開すると情報システムの構成情報などを用いた攻撃を受けるおそれがあるので，非公開とする。一方，基本方針は公開できる程度の抽象的なものであってよく，利用規則は，多くの利用者に配布されるので，非公開としても，機密文書とはいえない。なおこれらの文書は定期的に見直し，改善しなければならない。

情報システムの規模によるが，ポリシ作成には，図1のように1年程度の時間を見込んでおく。

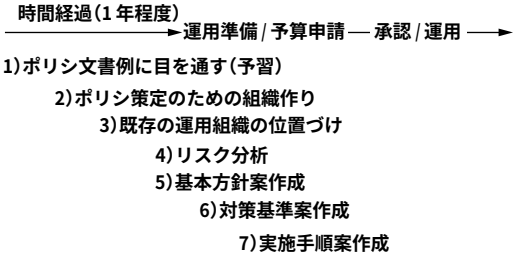
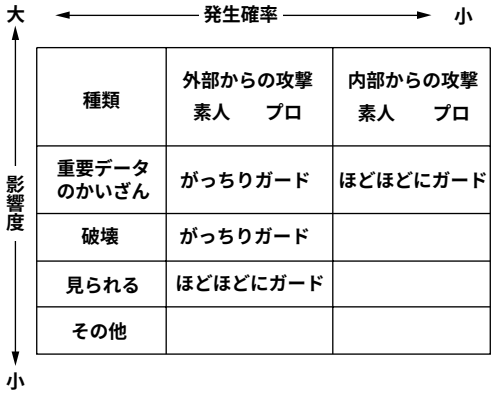


図1．セキュリティポリシ作成から運用まで

難しいのは，図1の2）と4）である。2）では，ポリシ策定のための組織として，おえらがたの委員会を構成するために校長先生にやる気になってもらう必要がある。4）のリスク分析は，管理にかけられる費用と手間には限りがあるので，重点的に守るべきものを決めるために行う。コンピュータ内の情報，紙書類や信用など無形のものも含め守るべき項目を「情報資産」として洗い出し，各資産の価値（重要度），脅威の起こりやすさからリスクを評価する。次に高いリスクをもつ情報資産に，現行の対策を適用してもリスクが許容水準まで下がらなければ，新たな対策を施す必要があることがわかる。ただし，リスク分析を厳密にやりすぎると，いつまでたっても終わらないので，最初は図2の程度に大雑把にしておいたほうがよい。



種類	外部からの攻撃 素人	外部からの攻撃 プロ	内部からの攻撃 素人	内部からの攻撃 プロ
重要データのかいざん	がっちりガード		ほどほどにガード	
破壊	がっちりガード			
見られる	ほどほどにガード			
その他				

図2．大雑把なリスク分析表の例

3．とりあえずどうするか

問題発生時の対処方法は，対策基準と（管理者向け）実施手順に明記されているべきものであるが，現実にはポリシが完成するまで待っていられない。そこでここでは，ポリシができあがるまでの暫定的な不正アクセスなどに対する対策を具体的に述べる。

3.1　予防策

まず，学校のネットワークを守るためには，インターネットへの出入り口における通信の制限と記録・監視に加え，LAN内の各ホスト（ネットワークに接続されたコンピュータ）の適切な設定が重要である。出入口での通信制限だけでは，内部に侵入されホストを乗っ取られたとき，内部のいたずらには対処できない。

ネットワーク出入り口付近での対策としては，ルータまたはファイアウォール専用機での通信制限，公開サーバを特に監視をする場所に集める，ウイルスチェック機能つきメイルサーバの導入と運用，ネットワーク型侵入検出システム（NIDS; Network Intrusion Detection System）の導入などが考えられる。

各ホストでは，ユーザID・パスワードによる利用者の認証，ウイルス対策ソフトウェアの一括導入（数が多いときに安上がり），ホスト型侵入検出システム，ファイルかいざん防止ソフトウェア，セキュリティ試験の実施などがある。

直接インターネットに接続している学校では，これらすべての対策を検討すべきである。一方，安全対策済みの学校専用ネットワークに接続している場合は，その対策の内容を十分理解して，残る危険への対策を考える。

これらの技術的対策に加えて利用者教育が重要である。とくに最近多い「受動的攻撃」のわなにはまらないように注意を呼びかける必要がある。受動的攻撃とは，悪意のある人が用意したプログラムなどをユーザが知らずに，あるいはだまされて実行してしまうことによって受ける攻撃のことである。

電子メイルの添付ファイル，おかしなWebページを見て，それに含まれるウイルスプログラムや変な命令を自動的に実行してしまうとウイルスに感染したり，ハードディスクから重要なデータを盗まれたりする。2001年度に流行したSircamというウイルスは，ハードディスクの中のファイルにウイルスを添えて，電子メイルで多数ばらまくもので，例えば自分のPC（パーソナルコンピュータ）に保存した生徒の名簿や成績表がばらまかれてしまうという事故につながる。重要なデータはきちんと管理されたコンピュータに置く，暗号化するなどの対策をとるとよい。

3.2 問題が起こってしまったとき

不幸にして，問題が起こってしまったときはどうしたらよいだろうか。次の重大な場合について考えてみよう。

1）攻撃や侵入を受けて大きな被害を受けた。

2）学内から攻撃を受けたとクレームがあった。

まず，通信記録を調査し，事実を確認すべきであるが，もともと記録がない，技術的知識がなく，調査が困難という場合もある。いずれにしても，重大な事件であれば，学校の危機管理と考えて，すぐに対処を開始する。

1）の場合は，侵入を受けたと思われるコンピュータをネットワークから切り離してじっくり調べる。ネットワークから切り離しておけば被害はそれ以上広がらない。その後，相手が使用したと思われるネットワークの管理者への問い合わせ，IPAセキュリティセンターや，警察，信頼できる技術者への相談など，学校のトップと相談して対処する。

2）の場合は最初の返事が遅れると相手が感情的になることがあるので，とりあえず調査すると返事しておくべきであろう。その後，利用記録，通信記録などを調査する。攻撃が続いているようであれば，そのコンピュータをネットワークから切り離して調べるが，たまにしか起こらない現象であれば，不正な通信がないか，つないだまま監視を続ける。もし，学内から外に本当に攻撃があったことがわかったら，問題の重要度に応じ，学校トップと相談して，信頼できる技術者，弁護士等と相談して対処する。

3.3 技術的調査と回復手順の例

以下に侵入を受けてしまったと思われるコンピュータの調査と回復手順の例を述べる。☆マークは，高度な技術的知識が必要なので，無理なら省略するか業者に頼むとよい。調子が悪くなったコンピュータのディスクは，フォーマットしてOSをいれかえる。

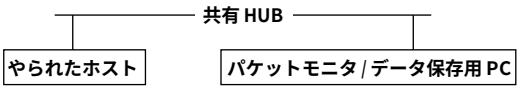


図3．データ保存，試験時の接続

1）LANから切り離す

図3のように独立したHUBにつなぎかえる。通信をモニタしたい場合は，スイッチではなく10Base-Tなどの共有HUBを用いる。（DHCPサーバでIPアドレスを設定していた場合は，手動でIPアドレスを設定する必要がある。）

2）データの保存

HDDのデータを別のホストや媒体に保存する。そのために調査用HUBに接続する必要があるかもしれない。データに汚染がないことを確認して，必要なら文書データを安全性を確認した別のサーバに移す。

☆汚染されたデータを時間があるときに調査する。

3）☆不正な通信の調査

そのまま起動し，調査用HUBでパケットをモニタし，どんな通信が発生するか確認する。

LANでは，できれば攻撃されたホストのIPアドレスに対するパケットを継続してモニタし，どこから，何をしようとしたのかつきとめる。

データ保存方法

以下のうち可能な方法をとることになる。ネットワーク経由の侵入であれば，敵が使う必要があるので，ネットワークファイル転送機能やアーカイブ作成プログラムは侵入後も使える可能性があるが十分注意する必要がある。

1）CD-Rが動けば，そこにデータを直接書き込む。
2）汚染されたデータを含んだHDDを外して，別のホストにつなぎ，データを読む。プログラム類は実行しないように注意（使う前に内容を十分チェックすること）。
3）HDDとりはずしが困難な場合は，調査用HUBにつなぎ，読みだし専用として，ファイル共有サービスを動かし，他のホストでデータを読む（Windowsファイル共有，UNIX NFSなど）。
4）空きディスク領域があり，アーカイブプログラムが正常に稼働するなら，いくつかの部分に分けて圧縮し，ネットワークファイル転送で別のホストに移す（lha, tar, gzip, ftpなどの利用）。

パケットをモニタするソフトウェアには市販のものもあるが，無料で利用できるtcpdump, ethereal（Windows用もある）が良く使われる。ただし，これらは，単に流れているパケットの内容の一部を表示するもので，簡単に表示結果の意味がわかるものではない。

LANの出入口などでの監視には，パケットをモニタして，怪しい通信を警告してくれるネットワーク型侵入検出システムが役に立つ。無料で使用できるものとしてはSnort（http://www.snort.org/）があるので，興味があれば試すとよい。

4．まとめ

前半のセキュリティポリシの話題は抽象的，後半は技術的な話題でやや難しかったかもしれない。従来はこのような問題はコンピュータやネットワーク管理者だけが認識していればよかったが，ネットワーク利用が普及した現在では，そういっていられなくなった。本稿がトップを含めて学校の先生方が，このような問題に対する意識を持っていただくきっかけになれば幸いである。