大学におけるセキュリティ対策

大学におけるセキュリティ対策

大阪府立大学総合情報センター
宮本 貴朗

aki@center.osakafu-u.ac.jp

1 はじめに

インターネットは重要な社会的なインフラとなり，企業や大学などの組織のみならず，個人にとっても重要な情報交換のツールとして利用されている．また，多くの企業などの組織においては，電子商取引の基盤として利用されるとともに，個人向けの広告媒体としても利用されている．さらに，現在政府が進めている電子政府や電子自治体などにおいても，インターネットは重要な基盤として利用される．これらのことは，すでにインターネットは社会全体のインフラであり，創世記のインターネットにおいては先導的な役割を果たしてきた大学や研究機関などの組織は，もはやインターネットにおけるメインプレイヤーではないことを示している．大学や研究機関はインターネット社会の一員であることを認識し，インターネット社会に対する義務と責任を負うことが求められている．

では，社会基盤としてのインターネットの信頼性はどうであろうか．古き良き時代のボランティアベースのインターネットは，利用者が研究者に限定されていたため，セキュリティの問題を気にする必要はなかった．しかし，1990 年代に入りインターネットが急速に一般に普及するに伴い，誰でもが利用できるネットワークとなった．現在では，インターネットは connectivity の面では滅多に停止することなく安定的に運用され，障害発生時の復旧作業が短時間に行える状態にある．では，安全に安心して誰でもが利用できるのかというといまだ問題が多い．いわゆるセキュリティの問題である．

インターネットにおけるセキュリティに関する対策は社会的に大きな問題であるが，特に商用でインターネットを利用している企業などでは重要な問題であり，電子商取引などにおいて損害を被る恐れがあるだけでなく，場合によっては企業の信用問題にもなることがある．そのため，人的にも費用的にも相当のコストをセキュリティ対策に支出している．大学においても信用問題は重要な要素であるが，たとえ侵入されても研究データしかないので何ら問題は無いと未だに考えている人も多い．確かに直接的には入試関連の情報など以外は，情報そのものに大きな価値のあるものは少ないかもしれないが，侵入者の目的はそうではない．セキュリティ対策が弱い所を踏み台にするのが目的であり，大学への侵入そのものが目的である場合は少ない．また，いわゆるコンピュータウィルスのように侵入目的を特に限定していない場合も多い．特に，踏み台にされたホストは被害者であるとともに加害者であり，深刻な事態が引き起こされた場合にはそのホストの管理者は法的責任 (刑事罰，民事責任) を負うケースも十分にあり得る状況にある．コンピュータウィルスもその範疇に入る．ウィルスに感染して本人の知らないところで他の組織のホストに多大な損害を与えた場合，もはや知らなかったでは済まされる時代では無くなってきている．

そこで本稿では，大学においてのセキュリティ対策の一般論とともに，本学においてのセキュリティ対策について考えてみたい．

2 何から何を守るのか

まず，セキュリティ対策を考えるにあたり，ネットワークがその組織においてどのように定義されているかを考える必要がある．ネットワークは，大学においては教育と研究およびその支

援，それと大学運営に関わる業務の基盤であるとともに，社会人教育，産学官連携，地域連携など社会的貢献の活動基盤と考えるのが妥当であろう (現に，本学のネットワーク利用規定でもそのように定義されている)．その視点にたてば，大雑把にいえばネットワークを利用して行われている教育・研究・運営活動すべてが守る対象であり，それらの活動に支障をきたすものすべてから守ると考えれば理解しやすい．また言うまでもないが，本学のホストが被害者となるだけでなく，他人に迷惑をかけるような行為，例えば本学のホストが侵入されて踏台にされて他のサイトへの攻撃を行うような場合やウィルスの二次感染などの発生を防ぐという意味でも，本学のネットワークおよびホストが加害者にならないように防御することも必要である．

3 まず敵を知ろう

3.1 攻撃の目的

攻撃の目的としては，大きく分けて2つあると考えられている．愉快犯と確信犯である．愉快犯は，自分の技術力を自慢したいがために，システムへの侵入を行ったりウィルスを作成し流布し，問題が大きく取り上げられることを目的としている．確信犯は，システムに侵入してデータを盗んで利益を得ることが目的であったり，政府や企業に対する抗議行動と称して攻撃を行ったりする．確信犯の多くは，攻撃元を隠蔽するために直接自ホストから攻撃を行わずに，踏み台を用いることが普通に行われ，踏み台として企業に比べセキュリティレベルが低い大学や研究機関が集中的に狙われているようである．

また，最近では攻撃ツールが簡単に入手できることが背景となり，いわゆるスクリプトキディ (スクリプティキッズ) による攻撃が増大している．これら攻撃ツールは，以前は高度な知識を要した攻撃手法を用いているものもあり，クリックするだけで自動的にセキュリティレベルの低いホストを探索し，システムへ侵入することができるツールもある．さらに，インターネットが一般家庭にも高速な常時接続の形態で普及しつつあることから，事の重大性を認識せずに自覚がないままゲーム感覚で攻撃ツールを使用するケースも増えつつある．

3.2 システム攻撃の方法

3.2.1 ネットワークサーバへの攻撃

現在，一般的なシステムへの侵入にはバッファ・オーバーフローというソフトウェアの脆弱性 (バグ) を突くものが非常に多い．バッファ・オーバフローはアプリケーションソフトウェアのみならず，OSそのものやシェアードライブラリにも存在するものであり，特定のプログラムをネットワークを経由して送り込み，実行させることができる脆弱性である．攻撃者はバッファ・オーバーフローの脆弱性を利用するために，以下のような手順で侵入を試みるケースが多い．

1. アドレス・スキャン
   実際に稼働しているホストのIPアドレスを手当たりしだいにICMP(ping) などを使って調べる

2. ポート・スキャン
   アドレス・スキャンで得たIPアドレスに対して，どのサービスが稼働しているかを調べる

3. バナー・チェック
   稼働しているサービスで使用しているサーバソフトの種類とバージョンなどを調べる

4. システムへの侵入
   脆弱性が存在するソフトウェア，バージョンであれば，その脆弱性を利用してリモートか

らプログラムを送り込んで起動する

5. 侵入後
   ログの改竄，システムプログラムの改竄，バックドアの設置，踏み台，攻撃エージェントの設置，他ホストへの攻撃を行う

現実には，これら一連の攻撃は，従来のように侵入者がコンピュータを手動で操作して攻撃をしかけているのではなく，前述したような攻撃のためのツールを用いている事が多く，実際には1秒未満で簡単にシステムへの侵入が行われる．そのため，仮にアドレス・スキャンやポート・スキャンなどの兆候を発見したとしても対応が間に合わず，すでに侵入されていることが多い．

3.2.2 パスワード・クラック

厳重な技術的なセキュリティ対策を施しているサイトは，ネットワークを経由して侵入するよりも，パスワードを何とか入手して正規のユーザを騙る方がコストがかからないこともある．そのため，依然としてパスワードの不正入手やパスワード・クラッキングはシステムへの侵入の方法として用いられている．パスワードの不正入手を防ぐためには，パスワードを付けていないアカウントが有ればロックもしくは削除すること，システムに標準的に設けられているアカウントの有無の確認やそれらのパスワードの変更を行うことが基本である．また，パスワードのメモをディスプレイにタックシールなどで張り付けている人がいるようであるが，それではパスワードの意味をなさない．さらに企業などを対象によく使われる例では，職員やベンダーになりすまして電話でアカウントやパスワードを聞き出すソーシャル・エンジニアリングという方法もある．また，少し手法としては異なるが，Microsoft 社のセキュリティーアップデートに見せかけたウィルスを DM として送りつける事件も発生している．

現在のネットワークの伝送速度やコンピュータの計算速度はますます高速になっているため，リモートから何度もログインを自動的に試す「ブルート・フォース」という古典的な方法も今だに有効的に用いられている．また，暗号化されていてもパスワード・クラックプログラムによりパスワードが簡単に解析される可能性があるため，辞書に載っている単語や個人情報に基づいたパスワードにしないことは当然である．パスワードファイルの流出に対しても注意が必要である．特に，Web サーバや ftp サーバを立ち上げている場合には，それらのサーバにアクセスすることによりパスワードファイルを得ようとする攻撃もあり，設定に不備があると不正入手される可能性もあるので注意が必要である．

3.2.3 電子メール

インターネットを利用することでユーザが最も恩恵を受けているのは電子メールであろう．電子メールはインターネットの最も初期のころから利用されているアプリケーションの1つであり，古き良き時代にセキュリティなど考慮することなくプロトコルが規定された．そのため，現在においては種々のセキュリティ的な問題が発生している．良く知られているのは SPAM，E-mail アドレス詐称，メール爆弾などである．電子メールの配送における根本的な問題は，メーラが電子メール送信の際に認証を行わないことであり，この問題の改善策として SMTP-AUTH が RFC2554 で規定され，一部のメールサーバプログラムでは実装されている．しかし，現実にはインターネット全体が SMTP-AUTH 機能を有するメールサーバのみで構築されない限り，SPAM も E-mail アドレス詐称も無くならない．また，POP/IMAP もそうであるが，インターネット上を認証のためのアカウントとパスワードが平文で流れるため，盗聴されればメールアカウントが不正利用される可能性もあり，今後はメーラからメールサーバ間の電子メールの送受信には，認証+暗号化 (POP over SSL/TLS, IMAP over SSL/TLS, SMTP AUTH など) が標準的に必要

となるであろう.

電子メールにおいてのセキュリティ的な脅威といえば，コンピュータウィルスを思い浮かべる事が多い．ウィルス対策ソフトを導入しているから大丈夫と思い勝ちだが，実際にはウィルス対策ソフトが有効に機能しないコンピュータウイルスも存在する．また，今だに添付ファイルをクリックしなければ大丈夫と誤った認識が横行しているが，電子メールの本文をプレビューしただけでも感染するケースもある．電子メールにおけるコンピュータウィルスの感染は，多くの場合にはメーラや関連するWebブラウザのバグに起因し，防御のためには最低限ウィルス対策ソフトを導入し，関連するソフトウェアのバージョンアップもしくはパッチの適用を必ず行うことが必須である.

3.2.4 Web

現在，コンピュータウィルスの次にインターネットでのセキュリティの脅威は，Webサーバへの攻撃/侵入およびWebページの書き換えであろう．複数の省庁が公的に運営しているWebサーバの書き換え事件や，文科省のWebサーバに対するDoS攻撃は記憶に新しい．その時のマスコミで報道された,「どこどこの省庁ではFirewallを設置していたから大丈夫であった」という報道がなされたが，当然のことながらFirewallの設置の有無は本質的な問題ではない．Firewallは，守るべきホストやサービスを少なくするための技術であって，安全にWebサーバを運用するには，セキュリティの問題の無い安全なWebサーバソフトを使用し，特権ユーザでない権限でサーバソフトを稼働させ，適切なファイルシステム上に問題のないコンテンツを置くことが必要である．それに加えて，Webサーバの設定も重要であり，Webサーバ自体がいくら安全に構築されていても，動作設定が誤っていればセキュリティが守れていないケースが多々ある．特に，CGIなどのアクティブにページを生成するプログラムをWebサーバで運用することは，非常に難しい．安全性の確保のためには，慎重にそれらのプログラムを実装し，安全に実行できる環境を構築し，運用にも注意を払わなければならない.

最近では，Webサーバに対する攻撃のみならず，Webブラウザの脆弱性を利用したクライアントに対する攻撃が多数報告されている．汚染されたWebページを参照するだけで，個人情報が流出したり，Webブラウザもしくは OS のハングアップ，ファイルの消去，ウィルスの感染，最悪の場合にはホストが乗っ取られるという悪質なケースもある．防御のためには，まずセキュリティ的に安全なWebブラウザを使用することであり，特にIE(Internet Explorer)を使用している場合には，常に最新のパッチを適用することを怠らないことが必要である．また，Java Script, Java applet, Active Xなどはインターネットにおいては安全に使用することが困難になりつつあるので，よほど信用できる相手(Webサーバ)と通信する場合以外には使用しないよう設定すべきである.

4 最近の事例

4.1 Code Red/Code Red II

2001年7月13日ごろに出現したCode Redおよび8月4日ごろに確認されたCode Redの亜種であるCode Red IIは，いずれもMicrosoft社のIIS(Internet Information Server)の持つ脆弱性(MS01-033)を利用するワームであり，発見当初は猛烈な勢いで感染を広げ，一部の報告では9時間で250,000ホストに感染したとも言われている．このワームはWindowsを搭載したホストのみならず，ルータなどのネットワーク機器に搭載されている管理用のWebインターフェースにも攻撃を行い，一部の実装としてIISを搭載していたルータにも感染を引き起こしたため，その結果一時期Code Redのトラフィックがインターネットのバックボーンの帯域を圧迫する事

態まで引き起こした.

Code Red はそれまで発見されていたワームやウィルスとは異なり，感染してもファイルを一切書き換えずにメモリ上に常駐する形式であったため，ウィルス対策ソフトでは発見が困難であるという特徴を持つ．逆にファイルの書き換えが行われていないため，再起動するだけでシステムは復旧するが，IIS の脆弱性に対する対策を行わずに再起動したために再度感染する事例も数多くあった．日付によって行動パターンを変えることも特徴的であり，システムの保持している時刻が 1–19 日の間は他のホストに対しての攻撃を行い，20–27 日の間は Whitehouse の Web サーバに DoS 攻撃を行い，28–月末は休眠するといった動作である．

Code Red II は Code Red とは異なり，ファイルやレジストリの書き換えを行い，バックドアをインストールする．感染後 24–48 時間は他のホストへの攻撃を継続的に行い，その後サーバをリブートして攻撃活動を停止する．また，感染後に攻撃するホストの選択方法も異なり，次の攻撃対象とする IP アドレスを Code Red ではランダムに生成していたが，Code Red II では感染したホストに近いものを優先的に攻撃するという特徴があり，組織内に一度感染が広がるとなかなか収束しない組織も多数あった．

4.2 コンピュータウィルス

古くはフロッピーを媒体として，現在では主にネットワークを経由してコンピュータに侵入し，ファイルの破壊やハードディスクの初期化などのコンピュータに被害をもたらしたり，悪意のあるプログラムを実行させることにより，ネットワークに接続された他のコンピュータの攻撃を行ったりするプログラムである．

ここでは，個別のウィルスの種類や感染方法については言及しないが，注意して欲しいことは以下のことである．

- 添付ファイルを実行しなければ大丈夫は迷信
  最悪のケースでは，電子メールをプレビューした時点で感染する．
- ウィルス対策ソフトを過信するな
  ウィルス対策ソフトは既知のウィルスのみに有効であるため，新種のウィルスには無効であることが多く，最近の統計では新種ウィルスが発見されてからウィルス対策ソフトベンダーがパターンファイルを作成するまでには少なくとも半日程度はタイムラグがある．しかし，最近観測した結果では，ウィルスは発見されてから 2〜3 時間後には本学に到達する．
- 既知のセキュリティホールを放置するな
  例えば，Code Red II と Nimda の IIS への攻撃のケースでは，攻撃対象となるセキュリティホールは同一であったため，少なくとも Code Red II の時に対策を施していれば IIS においては Nimda には感染しなかった．ウィルス対策ソフトに頼るのではなく，既知のセキュリティホールを塞いでおくのが本筋である．
- Web も安全ではない
  E-mail だけではなく，Web ページの閲覧により感染するウィルスが最近の流行．Java Script, Java applet, Active X などは必要な時以外は使用しない．

4.2.1 Sircam

2001 年 7 月 17 日ごろに出現した Sircam は，電子メールを媒体とするウィルスであるため，これまでと異なる 2 つの点で感染が拡大した．1 つは感染したホストの「マイドキュメント」フォルダにある任意のファイルを添付ファイルとして送信すること，もう 1 つは Subject(件名) にも

同様に感染したホストの「マイドキュメント」フォルダにある任意のファイルから任意の文字列を使用することである．そのため，日本人が開いてみたいという興味をそそる日本語の添付ファイル名となることも多く，実際にウィルス検知/除去ソフトでウィルスに感染しているのを承知の上で，ウィルスを除去した上で興味本位で添付ファイルを閲覧したという人も多いらしい．

Sircam での大きな問題は，ウィルスの感染の問題もあるが，それ以上に情報漏洩の問題が発生することである．大学においては，研究データなどはそれほど社会的な問題にはならないケースが多いと思われるが，たとえば試験 (入試) 問題，解答例，成績関連データ，人事/会計関連データなどが漏洩した場合には社会的に大きな問題となる．これら重要な情報はネットワークに接続されたコンピュータに放置せず，必要な時以外は外部記憶媒体に退避しておくべきである．

4.2.2 Nimda

2001 年 9 月 18 日ごろに出現した Nimda は，Windows および Windows のアプリケーションに存在する複数の脆弱性を利用し，強力な感染力で短時間で世界中で蔓延した．このウィルスにより攻撃された脆弱性は以下ようなものであった．

- IE では，ウィルスが感染した Web ページを閲覧しただけで感染．それ以外の Web ブラウザにおいても，JavaScript を利用してウィルスを取り込んでしまう可能性がある．
- Outlook/Outlook Express では，電子メールを閲覧しただけで感染．それ以外のメーラにおいても添付ファイルを実行することで感染する．
- Windows の共有フォルダを介して感染．また，ネットワーク上の共有可能なフォルダを検索し，自分自身をコピーする．
- IIS の脆弱性を利用して感染．Web ページにウィルスを読み込むような Java Script を混入させる．

Nimda は複数の脆弱性を攻撃し，特にサーバとクライアントで動作するアプリケーションを同時に攻撃する複合型という意味では，登場が予測されていたとはいえウィルスも新たな世代になったと実感させられる．複合型ウィルスの最も恐ろしいところは，クライアントの感染だけにとどまらず，ネットワークサーバへの感染が内部から起こり得ることである．いったん電子メールなどのコンテンツに潜んだ形で Firewall 内のホストがウィルスに感染してしまうと，ネットワークサーバは Firewall 内部から攻撃を受けることになり，セキュリティパッチを当てるなどの対策を施していないサーバはすぐさま感染することになる．Nimda の場合，唯一の救いは自己増殖をメインとしていたことであり，Sircam のような情報漏洩を引き起こしたり，HDD のフォーマットなどのより悪質な振る舞いをしていたらと考えると恐ろしいことである．今後そのような悪質なコンピュータウィルスが出現することも十分考えられる．

5 守る技術

5.1 Firewall

ネットワークサーバへの攻撃に対する防御として最初に上げられるのは，Firewall にてインターネットからアクセスできるサーバを制限することにより，セキュリティ対策が必要となるホストを限定することである．その上で，学外に公開するネットワークサーバのセキュリティホールを塞ぐ作業を行う．安全なネットワークサーバを運用するには，以下の条件を満たす必要がある．

- セキュリティに問題のないサーバソフトを使用すること．サーバソフトの種類とバージョンを確認し，常に最新のものを使用すること．
- サーバの実行権限に注意すること．できれば特権ユーザではない権限でサーバソフトを稼働させること．
- サーバの設定を適切に行うこと．サーバソフトに脆弱性がなくとも，設定が誤っていれば侵入可能な状態になり得る．
- コンテンツの設置場所に注意すること．ファイルシステムやディレクトリ，ファイルの所有者とパーミッションを適切に設定すること．
- サーバソフトから起動されるプログラム (例えばWebサーバにおけるCGIなど) の安全性に細心の注意を払うこと．

最近では，組織やサイト単位でFirewallを運用する以外に，各ホスト単位で使用できるPersonal Firewall(大抵は，ウィルス対策ソフトとパッケージになっている) が安価に入手できる．組織全体で運用しているFirewallでは，どうしても緩くなりがちなアクセス制限に対し，Personal Firewallではそのホストの利用方法に基づいてホスト単位で設定できるため，ネットワークサーバとしての機能を有しない一般のクライアントホストでは，ほとんどの外部からのアクセスを制限することでセキュリティを高めることができる．

5.2 コンテンツセキュリティ対策

一般に，Firewallでは電子メールやWebコンテンツの中身の検査ができないため，いわゆるコンピュータウィルスはFirewallをすり抜けて内部のホストに感染する可能性がある．特に注意が必要なのは，先に紹介したNimdaなどの最近の複合型のコンピュータウィルスは，感染したホストがネットワークサーバを攻撃する場合があるため，インターネットに公開していないためにセキュリティレベルの低い状態にあるネットワークサーバが攻撃を受けることになる．

電子メールやWebコンテンツの内容の検査を行うためには，ウィルス対策ソフトを導入することになるが，実際にはウィルス対策ソフトが有効に機能しないコンピュータウィルスも存在する．また，どうしてもコンピュータウィルスが発見されてからそれに対応するパターンファイルがウィルス対策ソフトベンダーから提供されるまでのタイムラグが発生するので，頻繁にパターンファイルのアップデート設定を行っていたとしてもコンピュータウィルスの感染を完全に防ぐ事はできない．そのため，ウィルス対策ソフトを導入するとともに，メーラやWebブラウザに関連するソフトウェアのバージョンアップもしくはパッチの適用を必ず行うことが必須である．

5.3 暗号化

インターネットを経由するような電子メールやファイルの転送においては，重要なデータを送受信するために暗号化することも視野に入れるべきである．特に，電子メールはメールサーバ経由で配送されるためEnd-Endで直接通信を行うサービスよりも盗聴や改竄の可能性が比較的高い．PGP(Pretty Good Privacy) などの電子メールやファイルを暗号化したり電子署名するためのアプリケーションはフリーソフトとして容易に入手可能であるので，たとえ学内同士の通信であっても重要な内容 (試験問題，成績情報など) を電子メールで送付する際には積極的に活用するべきである．また，重要な情報はファイル単位で暗号化して保存しておくのも有効な手段である．

6 問題への対処

ネットワークセキュリティ的な問題が発生した場合，その後の処置を如何に迅速に行うかは，非常に重要な問題である．最悪の場合，事後対処を誤ったために二次被害などが発生し，加害者(攻撃者)になってしまう可能性がある．

問題が発生したという兆候を感じたら，まず最初に，そのホストをネットワークから隔離する．そうすれば，原因究明のための時間的余裕を得ることができるし，なにより他のホストへの二次的な被害の拡大を防ぐことができる．また，いきなりシャットダウンやリブートはしないほうが良い．ほとんどの場合，そうしても問題は解決しないことが多いし，場合によってはログ情報を失ってしまい，原因調査が行えなくなることもある．

次に，システムの状態，ログ情報，ファイルのサイズやタイムスタンプなどから原因の調査を行う．残された各種の痕跡から，特にコンピュータウィルスなどの情報であれば，ウイルス対策ベンダーが提供している情報やインターネットで検索を行えばほとんどの場合には原因の特定が可能である．なお，当然であるが，インターネットでの情報収集は問題が発生したコンピュータ以外で行う必要がある．また，原因の特定作業が完了しても，修復作業を行う前に残されたログ情報やプロセスの状態をMOやCD-Rなどの何らかの形で保全することも重要である．

原因が特定できたら，復旧のためのツールや脆弱性を除去するためのパッチやアップデートプログラムを入手し，修復作業を行う．この時に注意して欲しいのは，ウィルス対策ソフトベンダーから提供される修復ツールはあまり信用しないことである．場合によっては不完全にしか修復できないことも多く，レジストリやシステムファイルなど壊された部分の修復が困難なケースもある．できれば，重要なファイルだけを外部メディアにバックアップした上で，ハードディスクの内容をすべて消去し，OS部分から再インストールし，バックアップしたファイルを別のホストで検査した上で書き戻す方法を取るべきである．また，修復作業後には忘れずに必ずパッチもしくはアップデートを適用する．

最後に，分かる範囲でできるだけ詳細に，ネットワーク管理者へ報告する．その際，他の人の個人情報が含まれるケースもあるので，その場合には本人の同意を得るなどの注意が必要である．

7 おわりに

セキュリティ対策は非常に難しい問題であり，インターネットが重要な社会的なインフラとなるにしたがい，緊急を要する重要な課題となってきている．新たなセキュリティホールは毎日のように報告され，攻撃する側も日々新たな攻撃手法を考案している．今日，万全の対策を施したとしても，明日には万全とは決して言えない状況にあるため，セキュリティレベルを保つためには継続的な努力が必要である．セキュリティ対策に必要となる費用や人的コストは今後も増え続けるであろう．しかし残念なことにセキュリティ対策は，必要性は認められながらも何か新しいものを生み出すためのものではないため，そのコストの負担がなかなか認められない傾向にある．大学や研究機関における教育研究活動をサポートするという意味において，ネットワークの利便性，信頼性，安全性の確保が不可欠であり，そのために必要十分な予算と要員の確保が極めて重要な課題である．また，利用者の意識改革も必要であろう．キャンパスネットワークは大学で運用・管理されているネットワークであるとともに，広くインターネットを通じて世界中のネットワークと接続されており，このことを個人個人が十分に考慮・認識して利用する必要がある．

最後に，本稿は筆者の個人的な見解で述べた部分が多い．しかし，官公庁や大学におけるセキュリティ対策が遅れていることは一般的な認識であることも紛れもない事実である．