社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2003－IS－86 (6)
2003／11／19

企業における情報セキュリティと認証制度

北野博之†

セキュリティ対策に関しては、多岐に渡り、かつ多様化しており、日常の活動のありとあらゆる場面で必要となることが多くなり、一部の技術者だけでは対処できなくなってきている。そのためには、管理職を含めたすべての従業者にまで認識と対処が必要になってきており、そのための備えが必要となってきている。その備えの裏づけとして各種認証制度が利用されることも多くなってきている。

情報セキュリティの取り巻く環境と認証制度の移り変わりを踏まえて、事業者で行うべき行動の参考になるべく、具体事例を交えて説明する。

Information Security and Certification Systems for Public Enterprises

Hiroyuki Kitano

Security measurement has spread widely and related to various things. Only specific engineers cannot deal with it, so all employees include managers need to join security measurement activity. Information security environments and certification systems have changed as the times passed by. This paper introduces some examples and experiences, and suggests what public enterprises should do.

1. はじめに

日本では、最近特にセキュリティとプライバシーについて多く語られるようになってきたが、これは住基ネット稼動や個人情報保護法の制定の影響が大きいようにも思われる。セキュリティというキーワードは、2000年の官公庁の不正アクセスやラブレターウィルスあたりから、新聞にも掲載されるようになってきた。日本では1995年頃からインターネットブームが始まり、同じ頃に米国Netscape社が暗号プロトコルであるSSLを搭載したウェブブラウザを登場させ、既にこの頃からクレジットカード番号についてはSSLを使用すべき、ということは謳われていた。最近ではコンピュータ専門のニュースサイトの記事に限らず、ほぼ毎日耳にするようになってきており、インターネットやコンピュータにあまり詳しくない一般の人も口にするようになってきた。

不正アクセスに関しては、OS(基本ソフト)やアプリケーションの欠陥以外に、2002年夏にはウェブサーバの設定ミスによって、隠しておくべきファイルが不特定多数の人に閲覧可能な状態で放置され、なおかつ削除した後も検索エンジンのキャッシュに残ったままで、二次被害を食い止められなかったといった事例が立て続けに起きた。防衛庁の件や郵政公社の件では、それぞれアウトソー

† 元 (財)日本情報処理開発協会 http://www.antai.net/

サーが漏らした、ルールにない行動をとった、と報道されている。また９月のJRの中央線の架橋工事でのトラブルでは、設計書のミスであったと報道されているのも記憶に新しい。

このようにセキュリティに関しても、使用するOSやソフトウェアに欠陥があるというケースとは別に、ベンダーや利用者の設計ミスや実装ミスといったようなインテグレーションや運用側の問題にもフォーカスが当たってきている。

2. 情報セキュリティに関する歴史

コンピュータが民間に使われ出した頃は、コンピュータセキュリティというと、第三者の出入り、水害、ダウンタイムなど、物理的な側面が大きかった。これはまだまだコンピュータ自体や記憶媒体が大きかったのもあるが、基本的にネットワークに繋がれず、オペレーション用の端末専用機を除いてほぼスタンドアローンで使われていたためである。

この頃の日本では、情報セキュリティに関する基準[1]として、1977年に「電子計算機システム安全対策基準」が制定され、その後「情報システム安全対策基準」(以下、「安対基準」と表す)と名前を変え、1995年に最後の改訂が行われた。また、1981年から2001年の間には、この安対基準をベースに物理的対策と運用管理に関する認定制度が行われた。

インターネットの登場で情報セキュリティ対策は大きく変わったと言える。最初のワームと呼ばれているのは、インターネット黎明期であった1988年のモーリス・ワームであり、メールサーバなどの脆弱性を突いて次々に感染させ、当時のインターネット接続されたサーバの半分が感染し、ダウンしたと言われている。これを機にCERT/CC(Computer Emergency Response Team/Coordination Center)が設立されたのは有名な話である。

日本では、大学や研究施設は1990年過ぎからインターネット接続実験が始まったが、商業ベースとしては1995年あたりから企業にインターネットが繋がり始めた。海外ではこの頃から既にISSやSatanなどのセキュリティチェックツールが使われ始めており、ファイアウォールの製品も出始めていた。日本では、インターネットの登場の時点で、セキュリティ必要性が併せて言われていた。情報セキュリティ政策としては、1996年に「不正アクセス対策基準」が作られ、同じ年にJPCERT/CCが設立された。法律としては、数年遅れて1999年に「不正アクセス禁止法」が制定され、翌2000年から施行された。

一方、違った視点で見てみると、欧米は1980年代後半まで長い冷戦時代があり、軍事的なスパイや産業スパイといった視点からの情報セキュリティの考えがあった。これらは、上司の名を騙って重要情報を聞き出すような「ソーシャルエンジニアリング(社会工学)」の手法もよく使われていたと言われている。一見これは子供じみたやり方にも思えるが、今の時代でもパスワードや認証情報を聞き出すのは、サーバを不正アクセスするよりも遥かに簡単であると言われている。最近でも、米国のオンライン決済会社であるPayPalの偽サイトなど、そっくりなウェブページを作り、電子メールなどで消費者を騙してこのサイトに誘導し、パスワードを入力されるような事件も起きている。

個人保護保護に関しては、社会保険番号などの国民総背番号制が実施された国では、古くから

個人情報のコンピュータ利用が行われてきており、ヨーロッパ各国では1970年代初頭から個人情報保護法が制定されていった。これらの状況を受けて、1980年にOECD(世界経済開発機構)が「個人データ保護に関するガイドライン[2]」を制定した。日本での個人情報保護政策[3]に関しては、1989年に、通商産業省(現経済産業省)の、いわゆる情報保護ガイドラインが制定され、1998年に一度同ガイドラインは改訂され、1999年にJIS Q 15001[4]、今年2003年に個人情報保護法制定という流れになっている。

3. グローバル化の現状

米国では市内電話の固定料金制度があったため、以前から常時接続環境が家庭でも実現できていたが、21世紀に入り日本でもADSLを中心として家庭のブロードバンド化が進んできた。日本のADSLの費用は今や世界最安値となり、光ファイバーやCATVなども含めたブロードバンドユーザは1000万人を越えた。LinuxやFreeBSDなどのオープンソフトのサーバOSが実用にも使えるようになり、家庭でもサーバを設置することが可能となった。

2000年以降はLoveLetter、Nimda、CodeRedなど、Microsoft社のWindows OSを標的としたウィルスやワームが多く発生した。OS、アプリケーションが共通化していく状況では、最もシェアの高いOS、アプリケーションがターゲットなることは必然のことである。韓国ではウィルスによりかなりの感染を受け、ISPのネームサーバがダウンするほどまで被害を受けたというニュースも記憶に新しい。低額なブロードバンド化による常時接続が可能になったことにより、家庭や企業で十分なセキュリティ対策なしに安易に接続するケースも増え、広告メールや不正アクセスなどの不正中継に使われるケースも出ている。

最近は、特定のメールソフトとHTTPをターゲットとしたウィルスや不正アクセスが増えてきている。実際、ファイアウォールを導入していても、対外からメールサーバとウェブサーバへのアクセスは許可せざるを得ず、必然的に攻撃のターゲットとなりやすい。メールソフトやウェブブラウザソフトなどのクライアント向けソフトもグローバル化され、言語を問わず共通仕様になっているので、必然的に脆弱性も世界共通となってきており、ウィルスの感染力を加速させている。

また最近では、ウェブブラウザのCookieに関するセキュリティやクロスサイトスクリプティング(XSS)などの問題も起きている。これらはOSや製品個々のバグではなく、アプリケーションをターゲットとした不正アクセスである。つまり、OSやアプリケーション自体の脆弱性とは別に、情報システムのインテグレーションと、ウェブコンテンツのコーディング時のバグによる脆弱性も問題となりつつある。

4. セキュリティに関する認証基準

それぞれの時代背景の元、認定、認証基準が制定され、それぞれ認定、認証のための審査、または試験が行われている。代表的なものをいくつか概略的に説明する。

(1) 安全対策事業者認定制度

1981年にスタートした情報処理施設の物理的対策と運用管理に関する認定制度であり、2001年3月に終了し、下記ISMS制度へとバトンタッチした。20年間で210事業所認定。ただし、認定期間が3年であるので、制度廃止後も認定期間まで認定書は有効である。

参考：http://www.jisa.or.jp/committee/safetyguard/index-j.html#anchor1044128

(2) プライバシーマーク制度

1998年より(財)日本情報処理開発協会が行っているJIS Q 15001[2]に基づく個人情報保護に関する事業者認定制度。2003年9月末現在589社認定。

参考：http://privacymark.jp/

(3) ISMS制度(情報セキュリティマネジメントシステム適合性評価制度)

英国規格のBS 7799-2をベースとした情報全般に関わる情報セキュリティの認定制度。1年間のパイロット認証の後、2002年よりスタート。2003年9月末現在205事業所。

参考：http://www.isms.jipdec.jp/

(4) ISO/IEC 15408

2002年3月より製品評価技術基盤機構で行われている製品に対するセキュリティ評価制度。各国政府の調達基準をベースに1999年にISO化され、2000年にJIS X 5070が制定された。

参考：http://www.nite.go.jp/asse/its/jisec-index.html

(5)セキュリティアドミニストレータ試験

2002年10月より(財)日本情報処理開発協会の情報処理技術者試験センターで開始された技術者向けの試験制度で、該当試験は年1回行われる。上記プライバシーマークやISMSなどのマネジメントの知識と経験が必要であり、技術者といってもマネージャー向けの試験である。

参考：http://www.jitec.jp/1_11seido/h13/ss.html

(6) SSE-CMM(Systems Security Engineering - Capability Maturity Model)

カーネギーメロン大学のCMMをベースに作成。CMMとは、組織としての能力の熟成度をレベル化して測るための手法であり、ソフトウェア開発の能力を測るものとして使われている。SEE-CMMはこれをセキュリティ分野へも適用したものである。ISO/IEC 21827は2002年に制定されたが、JIS化はまだである。CMM同様、初期レベルから熟成されたレベルまで、それぞれの段階での認証が可能。

上記以外にも、GAO(米国会計検査院)の基準や、 ISACA(Information Systems Audit Control Association) が作った COBIT (Control Objectives for Information and Related Technology) などの基準がある。また、ドイツやカナダでは日本の「安対基準」に近いセキュリティ基準がある。

以前は、製品、建物といった「見える物」に対する審査と認証がメインであったが、最近では多様化と移り変わりが速いことにより、それらを作り出すプロセスを対象とした審査が多い。つまり、物からPDCAサイクルを含んだマネジメントシステムに対する審査がメインになってきている。

6. 企業に求められること

最近では、ウィルスや不正アクセスについては、世界同時的に発生するようになってきている。海外からもウィルスや不正アクセスを受けたり、逆に国内から海外という事態も起きており、感染や被害にも時差がほとんどなくなり、たった1日で世界中に伝播したりなどスピードが速くなってきている。個人情報の漏えいに関して言えば、P2Pや掲示板などを経由して、かなりのスピードで不特定多数に伝播し、回収が不可能になる事例も出ている。そのため、自社のシステムの監視が必要であり、事が起きた場合の事態の把握と緊急事態の迅速な対処が必要となる。

また、ウィルスに関連して言えば、SQLサーバなどサーバ機も感染する事例が出てきたので、クライアント機へのウィルス対策ソフトを導入するのは当然のこととして、メールサーバやファイルサーバにも冗長的に導入したり、ファイアウォールの導入以外に、IDS(不正侵入監視システム)の設置や、統合型のアプライアンスの導入、アウトソーシングの利用も必要になってくるであろう。一概にウィルス対策ソフトやファイアウォールを導入しているから安心ということではなく、それらがきちんと機能しているかなどの定期的なチェックと、世の中の動向や技術動向などの情報収集も欠かさず行うことが必要となるであろう。

防衛庁や郵政公社のニュースに関しては、情報システムの問題と言うより、人的要因の問題が大きいように思える。セキュリティに関しては、損害などの実被害と併せて風評被害も気にしなければならない。例えば、ウィルスに感染した場合の業務停止や修復作業などの実被害よりも、「あの会社はウィルスに感染した」というように、会社の技術レベルを疑われることもある。まだまだ各製品のセキュリティベンダーがばらばらであり、クロスプラットフォームで自ら情報システムをインテグレーションしないといけない場合も多い。組み合わせによっては盲点となる部分も発生するので、それらのチェックも必要になり、これらに臨機応変に対応できる組織作りと人員の養成が必須になってきている。併せて要員の管理などのマネジメントも不可欠となってきた。

クロスサイトスクリプティング(XSS)に関しては、アプリケーションソフト自体の問題もあるが、それ以外に、プログラマーのコーディング時のバグも含まれている。これはサーバークライアントシステム開発時に、パスワードを暗号化したり、通信には暗号を使うことと同じくらい重要なこととなるであろう。例えば、システム開発時には、間違った使い方をしないように、確認画面をつけたり、エラーメッセージをつけたりなど、ユーザインターフェースに工夫をしているはずである。セキュリティに関しても同様で、発注者に言わなくても実装するようにならないといけなくなるであろう。そういう意味では、セキュリティ対策は社会的な暗黙の仕様とも言えるだろう。

また、個人情報に関しては、今年５月に個人情報保護法が制定されたが、制定や施行前であっても、損害賠償や社会的制裁を受ける事例をニュースで耳にすることがある。事故を起こして消費者や発注者から見放されてしまうなど、社会的制裁による損失は、損害賠償や罰金の金額と比べ物にならないこともあり得る。それらを防ぐためには、個人情報を取り巻くリスクを認識し、これに対して合理的な対策をとる必要がある。例えば、個人情報を一括してデータをコピーできないように、ある一定の数に分割して管理するなど、リスク分散的な措置も必要であろう。

セキュリティを取り巻く環境は動向が速いので、セキュリティ対策は100%ということはありえないし、セキュリティ対策とは0か1かを選択することではない。結果的に費用対効果など総合的に判断して採用することになるが、状況によってはスピードが求められる事態も発生する。そのためには日頃からマネジメント的な手法を使って備えておかなければならない。マネジメントというと管理職のような印象もあるであろうが、万が一の場合にうまく機能させるには、日頃からの取り組みと組織的な経験が必要で、そのためには組織やチームの一人一人の役割と協力が重要となる。

様々な認証制度があるが、定期的に第三者に違った視点でチェックしてもらうのは、事業者にとっても有益なことであると思われる。目的をしっかり据えて、それに応じて利用するのはに効果的だと思われるが、認証自体が目的となると、目的と手段が入れ替わってしまい、何のための認証であるか本末転倒となってしまうので注意が必要である。

7. おわりに

個人的な経験であるが、プライバシーマークの審査をしていた頃、「プライバシーマークの神聖に伴って社内の仕組み全部を見直すこともできた」というような副産物的な効果を挙げる事業者も多かった。これは、既存の業務プロセスを適宜見直すことによって、効率化を図ったり、情報共有といった、特に横方向のナレッジマネジメントの仕組みが確立されたりすることを意味していると思われる。結果的に、経験を踏まえて作業効率やROI(費用対効果)も改善することもあるであろう。ただし、このような状態にまで至るには時間がかかるので、日頃からアンテナを張り巡らせてセキュリティに関する技術情報を適宜収集して必要な情報をキャッチし、早めに対処できる体制が必要であろう。

8. 参考文献

1) http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm
2) http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.html
3) http://www.meti.go.jp/policy/it_policy/privacy/privacy.htm
4) http://privacymark.jp/ref/jisq15001.html