

- 情報セキュリティの現状と管理の在り方 -

株式会社 エムズ・ネット・スクエア 杉村倫代

- 2000 July -

1. はじめに

インターネットが個人の生活や社会への関わりを深めつつ迎えた 2000 年は、複数省庁のホームページ改ざんというアクシデントにより、日本にとってはこれからの情報化社会を考えさせられる機会を与えてくれる幕開けの年となった。この 5 月にもラブ・ウィルスが世界を駆け巡り、その感染力に改めてネットワーク時代における情報伝達の素早さと影響力、そして情報セキュリティの脆弱性に驚かされたところである。

日本では、政府ミレニアムプロジェクトの一貫として、電子政府の実現を目指しインターネットを利用した各種電子申請や情報共有のための情報化施策について、2003 年をめどに取りまとめているが、一部自治体では、電子政府の実現を待つまでも無く、インターネットによる情報化を進めており、住民・法人との電子申請、一部決済などの業務や、出先機関との VPN による情報経路の確保、認証・証明機能を持たせた自治体間の情報交換など、インターネットを利用した業務形態の活用が盛んに実用化されている。

また企業では、インターネットを情報収集のツールと捉える段階から、直接的な商取引に劇的な効果をもたらす、情報発信型の戦略的な情報インフラと捉える段階を迎えている。対企業、対個人との電子商取引の場面においては、極めて機密性の高い情報を、正しく安全にやり取りできる仕組み作りが、今強く求められている。自治体や企業にとって、組織の情報資源や社会的信用をさまざまなセキュリティ・リスクから守るために確保すべき対策が、果たして適切に採れているのか、自信が持てない組織は多い。セキュリティを脅かす事故のニュースが報じられる都度、組織の情報セキュリティに対する強度評価や対策立案のコンサルテーションを求めて、外部へのセキュリティ監査の希望が急増している。

ここでは、筆者が最近関わった情報セキュリティにかかわるいくつかの調査研究プロジェクトから得られた知見をもとに、被害の実態や対策技術の動向をまとめつつ、組織として情報セキュリティ管理をどのように進めていけば効果的な施策となりうるか整理していく。

2. 情報セキュリティ被害の現状

この 5 月のラブ・ウィルス感染による世界全体の被害総額は、把握しきれない部分の推定も含め、100 億ドルに達する可能性があるという調査結果が米国会計検査院でまとめられた。これは過去最悪といわれた 1999 年のメリッサ・ウィルスによる被害総額の約 100 倍とも推測されている。

(表 1) (表 2) は、米国 ICISA 社 (前身は NCSA 社で、情報セキュリティ製品の安全性を認定する

産業 (n=24)	損失を出した組織数	損失額(回答組織の計) 単位	平均損失額 単位 \$1000
航空 (n=24)	3	53	18
銀行・金融 (n=92)	15	6,290	419
通信 (n=41)	6	3,165	528
コンサルティング (n=81)	10	5,211	521
教育 (n=40)	4	131	33
政府系・公的機関 (n=129)	11	2,246	204
情報・ハイテク・コンピュータ (n=112)	10	4,286	429
保険・不動産・法曹 (n=32)	3	26	9
製造・流通 (n=53)	8	306	38
医療・製薬・バイオ (n=30)	2	102	51
軍関連組織 (n=32)	6	815	136
その他 (n=77)	13	692	53
回答者全体 (n=745)	91	23,323	256

米国における産業別セキュリティ損失額(過去1年間)

(ICISA調査、1999) <http://www.infosecurymag.com>より作成)

組織。1998 年に社名変更) が 1999 年に実施した産業別情報セキュリティ調査 (回答数: 745 組織) 結果の一部である。

この調査では、セキュリティ被害による損失額を計上できたケースが全体の 12% (91 組織) であったが、それら計上できた企業の平均損失額は 25.6 万ドル/年と報告されている。一方、セキュリティ被害を経験した組織をみると、ウィルス被害 77%、内部社員の不正アクセス 52%、外部からの不正アクセスとデータなどの盗難・破壊がそれぞれ 23% と、極めて高い被害発生割合が報告されている。

(表 1)

同年行われた米国 F B I と C S I (コンピュータ・セキュリティ協会) によるセキュリティ調査にお

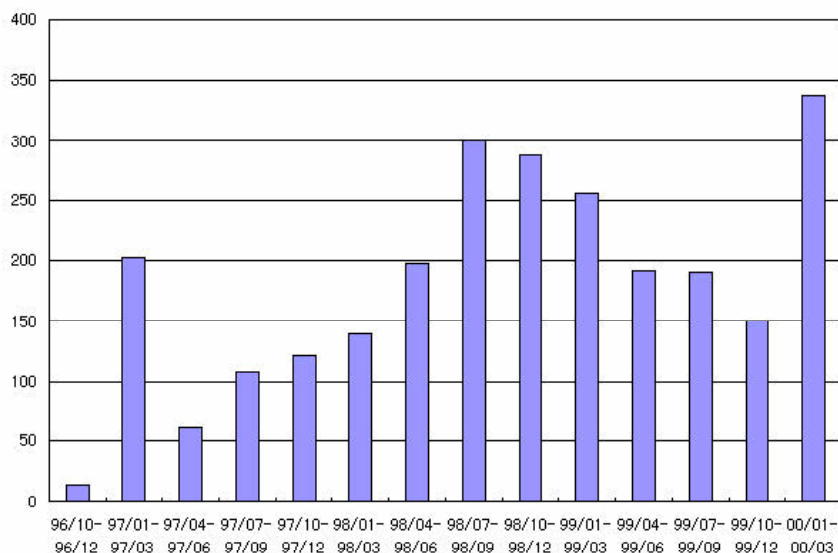
セキュリティ被害 (回答数: 745)	1999	1998	+(-) %
1. ウィルス	77%	73%	5.4
2. 社員による不正なアクセス	52%	54%	(3.7)
3. 外部者による不正なアクセス (ハッカー、産業スパイ、情報テロリストを含む)	23%	12%	91.6
4. コンピュータ資源の盗難、破壊	23%	25%	(8.0)
5. 重要情報の漏洩	18%	19%	(5.2)
6. 情報データの盗難、破壊	15%	19%	(21.0)
7. 正式な協働者による不正なアクセス (業務委託先、販売先、ベンダを含む)	14%	14%	N/C
8. PHONE/PBX/VIMのハッキング	12%	N/A	N/A
9. その他	5%	7%	(28.6)

セキュリティ被害の発生率 (ICSA調査、1999)
<http://www.infosecuritymag.com>より作成)

いても、回答組織数 521 のうち正確な被害の実態や被害額を把握できていないとの回答が 1 / 3 にのぼっていたものの、全体で、1 億 2000 万ドルを超える被害損失額が報告された。この種の情報は把握しにくいものであるが、実際、米国 DISA (Defense Information Systems Agency) が実施したアタック実験によると、全アタック 38,000 件のうち、65 % は侵入に成功し、全体の 4 % がその侵入を検知したにもかかわらず、侵入検知時の報告先となっているはずの DISA にレポートされたのは全体の 0.7 % に過ぎなかったことが明らかとなっている。現状は更に深刻である。

(表 2)

日本では、セキュリティ被害に関するデータの一つとして JPCERT/CC (コンピュータ緊急対応センター) が把握している最新の不正アクセス件数が公表されている。JPCERT/CC は、1996 年以降、不正アクセスによる被害の受付と対応、セキュリティ教育などの啓発活動を行っている機関である。日本におけるセキュリティ被害の報告率は、米国よりさらに低いとみられているものの、このような機関への届け出に対する認知度は上がりつつある。平成 12 年以降で約 100 件強 / 月の不正アクセスが報告されている。(図 1)



うち Web ページの改ざんなどの実被害につながったと報告されたケースは、1999 年で数%に留まっている。

図 1 JPCERT/CC が受け付けたインシデント報告件数の推移 (3ヶ月単位)

3. 情報セキュリティへの脅威と対策技術の動向

情報セキュリティを確保する上で組織にとって守るべきものは、情報資産であり社会的信用である。ネットワーク化の進んだ今日、従来型のコンピュータシステムに対する脅威とは異なるセキュリティ侵害の形態は多様化しそれを把握することも徐々に困難になっている。これら脅威とセキュリティ対策技術は、およそ 図 2 のようなものである。

技術的なセキュリティ対策では、ファイアウォールによるアクセス制御管理 (内部、外部からの怪しげなアクセスやファイル、内部から外部への不穏な行為を監視し制御する) 侵入や侵入への準備行為であるポートスキャンなどに対する検知システム (侵入検知システム, IDS) の導入、ウィルスに対する最新ワクチンソフトの頻繁な適用、重要ファイルに対する保管時の暗号化、通信時の暗号化、通常の認証システムに加え、指紋や虹彩などによるバイオメトリクス認証やワンタイムパスワードなど

セキュリティ上の脅威

対策技術

盗聴(覗き見)	通信路上で他者に通信文を覗かれたり、改ざんされる	暗号化(通信路,ファイル)
なりすまし	インターネット上で、他者を認証するもの入手し、他者として振舞われる(誹謗中傷,詐欺など)	認証(ユーザ認証,デジタル署名)
事後否認	インターネット上で情報を送ったりした後で、その行為を否認する(詐欺など)	
ウィルス	インターネットを介して取り込んだファイル,又はFDに感染したウィルスが起動し、データなど破壊される	ワクチンソフト
侵入	そのシステム領域へのアクセスを許可された者以外が入り、データ破壊などされる	アクセス制御 検知・監視機能 (ファイアウォールの導入) (侵入検知システムの導入)
DOS 攻撃	サービスを停止する(Denial of Services)ことを目的にサーバ資源に負荷のかかる処理をさせる	
踏み台	インターネットを介して不正に他システムに侵入する前に、攻撃対象以外のネットワークに一旦進入する	セキュリティホールの除去
ポートスキャン	不正侵入など攻撃前に、攻撃対象のファイアウォールの防御のないポートを探す	

図2 主なセキュリティ上の脅威と主な対策技術

を組み合わせ、より厳密なユーザ認証の導入、デジタル署名による確実なデータ送受信の仕組み、などがある。また、OS やメールソフトなどが持つセキュリティホールと呼ばれる1種のバグへの迅速な対処も、対策技術の効用を左右する重要なポイントとなる。

前述の米国FBIとCSIによるセキュリティ調査によると、セキュリティ対策技術のうち、アクセス制御、ワクチン、ファイアウォールなどは9割以上、他の対策技術についてもその導入は年々進んでいる。(図3)

しかしながら一方で、情報セキュリティ担当者は、予算不足、上層部の認識不足により、十分なセキュリティ対策が採られていないことを心配しているとも報告されている。

これらの対策を支えるセキュリティ技術のうち、対企業、対個人の電子商取引などの発展と共にその役割の大きさを増し、急ピッチでその普及と更なる検討が進められているのが暗号技術と暗号技術をベースにした認証の仕組みである。

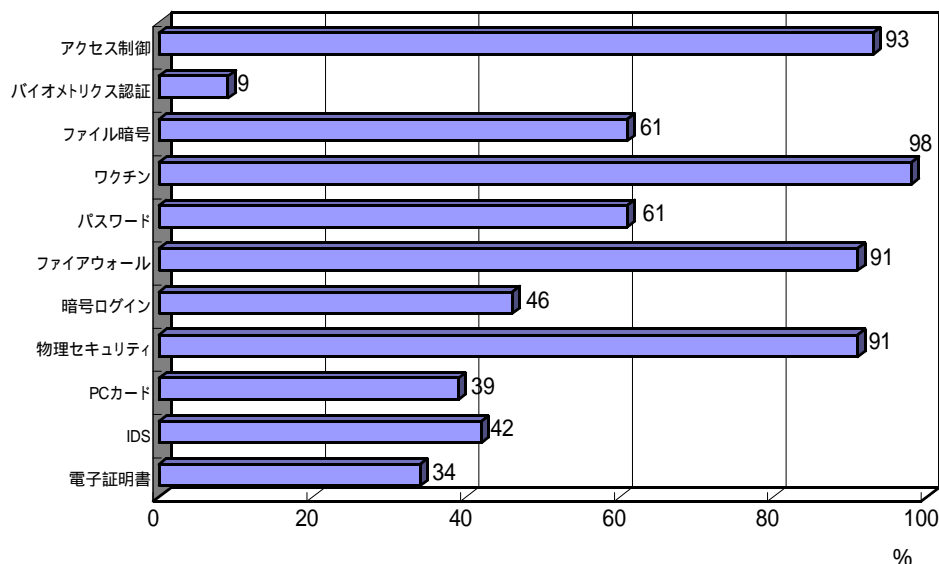


図3 使用されているセキュリティ技術 (FBI/CSI 調査, 1999)

4. 暗号技術と情報セキュリティ

暗号は、情報セキュリティ上の守りの基本となる技術である。軍事利用として2000年の歴史を持つ

と言われる暗号が、コンピュータ通信技術として、新たにその使命をおびたのが、1970年代後半である。暗号技術は、情報を秘匿するという役割に加えて、通信相手や通信文が正しいか否かを認証するという役割を果たすようになった。ここでは、組織の外部あるいは内部間でやりとりする情報を安全に取扱う際に、日常的に不可欠な基本技術となるこの秘匿の技術と認証の技術の動向について概観しておく。

< 秘密鍵暗号と公開鍵暗号、その併用による安全なデータの秘匿 >

1970年代後半、はじめて暗号化・複号化のアルゴリズムが公開された標準暗号 DES (Data Encryption Standard) が米国政府により制定され、初の商用目的の暗号として普及していった。正しい受信者のみが複合できる「鍵」を送信者から受信者に予め配送し、共通の鍵を秘密にしておくこの方法を「秘密鍵暗号 (共通鍵暗号)」と呼び、DES (鍵長:56bit) は現在でもこの代表格である。日本でも数社がそれぞれ鍵長 64 ~ 128bit の秘密鍵暗号方式を開発している。先頃も三菱電機が開発した暗号 MISTY (鍵長 128bit) の日欧の次世代携帯電話への採用が報じられ話題になったところである。

秘密鍵暗号が、通信する相手毎に共通の鍵を保管しなければならず、また通信前に相手に鍵を安全に渡しておく必要があるのに対して、公開鍵暗号方式では、暗号化のための鍵は複合化鍵と別々にし、暗号化鍵は予め渡す必要がなく、公開されるため、インターネット商取引における不特定多数の相手との暗号通信を可能とする。暗号化鍵とペアで生成される複号化鍵は秘密にしておく。公開鍵暗号で現在最も広く利用されているのが RSA データセキュリティ社の RSA 暗号 (鍵長 1024bit) である。

秘密鍵暗号は、取引相手毎に共通の鍵を作成しなければならない面倒があったが、暗号化・複号化の処理時間が短く効率がよかった。しかしコンピュータの処理能力が各段に向上した現在では、解読時間もまた短縮され、十分な安全性が保てなくなった。そこでインターネットでの商取引などでは、処理時間がかかるが安全性の高い公開鍵暗号を使って短い秘密鍵データを暗号化・配送し、秘密鍵暗号で長い通信文を暗号化する、などのように併用させる方法で広く用いられている。

次世代の標準暗号は、インターネット電子商取引の他、金融機関の電子決済や公的機関での通信などに広く利用されることになる。日本でも、現在開発中の暗号を、2003年を目処に構築する電子政府で次世代標準暗号として採用していく方針であり、また国際標準化機構 (ISO) が 2002年にまとめようとしている次世代標準暗号の候補としても提案していく計画がある。

< 認証技術と認証機関 >

認証には、通信相手の認証と通信データの正当性の認証がある。相手の認証には、パスワード認証が未だ主流であるが、秘密鍵暗号を用いた認証システムや、1分毎にパスワードが変わるワンタイムパスワード、指紋や虹彩などによる生物学的認証システム、デジタル署名方式によるものなどがある。

通信文が正しいことを証明するために用いられる技術がデジタル署名であり、公開鍵暗号技術が利用される RSA 署名が有名である。文書そのもの全部または一部を作成者の秘密にしておく方の鍵を使ってデジタル署名を生成する。受信者は送られた文書の正当性を確認するため、送り主の公開鍵を使って、間違い無く送り主が作成した文書が改ざんされていないことを検証できる。

公開鍵暗号やデジタル署名の利用は、公開鍵が正しく保管されていてはじめてその安全性が確保できるものである。公開鍵の登録者の身元を正しく認証し、公開鍵に対する電子証明書を発行するための機関が認証局 (Certification Authority, CA) であり、CA そのものを認証できるさらに上位の CA がある階層型の認証機関を形成する。電子証明書を発行する機関としては現在、米国ベリサイン社が最も有名であるが、日本でも数社が認証機関としてサービスを提供している。また、電子政府構想において、各省庁で求められる認証機関の仕組みや機能などについて現在議論されているところである。

5 . セキュリティ対策における運用管理の重要性

組織のセキュリティ・リスクから情報資産を守るための対策として、前述のセキュリティ機器やソフトウェアを導入することは勿論重要である。ただし、その運用を誤ると、薬剤の処方や大工道具の使い方同様、折角の効用が現れないということになる。ウィルスやなりすましといったセキュリティに対する直接的な脅威は、新しいワクチンソフトが適用されていなかったとか、アクセスログをとってもそれを見過ごした、といった間接的な脅威が存在することによって、具体的な被害につながってしまうのである。(図4)

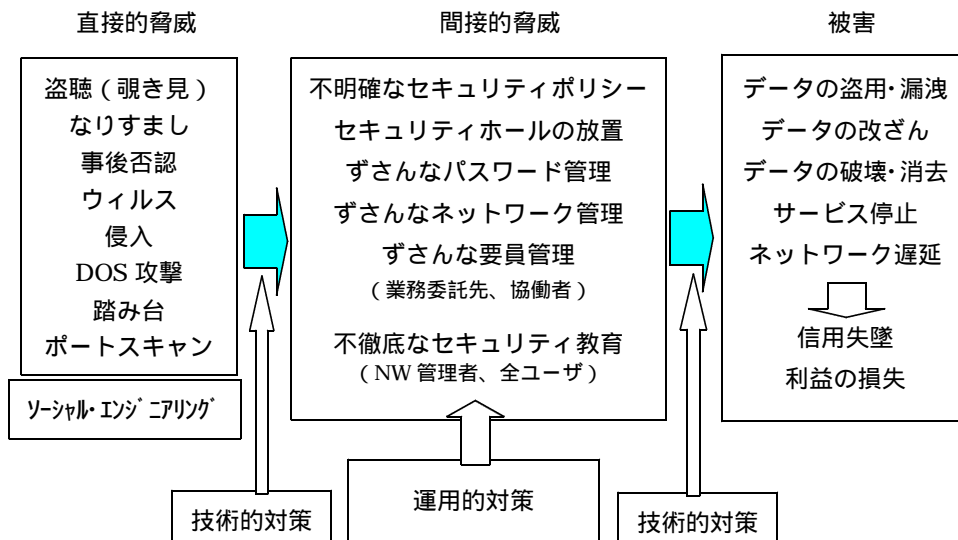


図4 セキュリティ被害をもたらす間接的脅威の存在

情報セキュリティへの脅威というと、インターネットを介した怪しげな行為のみが脅威の対象として捉えられがちであるが、同時に指摘されるべきは、組織内のセキュリティ管理体制そのものである。社員のパスワードを電話口で言葉巧みに聞き出す、などの原始的な情報入手行為（ソーシャルエンジニアリング）にあっては、高度なセキュリティ技術の適用も役に立たない。また、社員のセキュリティに対するモラル向上のための啓蒙活動、ネットワーク管理者が果たすべき情報収集を怠らないための運用体制作りなど、たとえ被害が発生しても最小限にとどめられる管理体制の周知徹底が、セキュリティ対策のカナメとなるともいえよう。

情報セキュリティに対する管理計画を構築していく時、組織全体として取組む姿勢が明確か否かは、その後の運用に大きな影響を与えるため、できるだけこだわりたいところである。また組織を脅かす不心得者は、インターネット上というよりも、社内や業務委託業者先の中により多く存在する、と複数の調査で指摘されている。まず自分たちの組織にとってセキュリティ・リスクはどのように存在するか分析し、セキュリティ対策全般に渡って、マクロレベルからマイクロレベルのセキュリティ・ポリシーを定め、明文化し、周知徹底していく努力が、全ての組織に求められている。（図5）

管理対象		明確化すべきポイントなど
ヒト	組織（本体、出先機関、業務委託先等）	<ul style="list-style-type: none"> 組織のトップを巻き込んだセキュリティ委員会の設置 組織のビジョンをセキュリティポリシーに反映 委託先組織も考慮した適用範囲、責任範囲の明確化など
	個人（社員、ネットワーク管理者、遠隔地ユーザ、協働者等）	<ul style="list-style-type: none"> それぞれの個人が、履行すべきこと、そうでないことを認知 それぞれの個人が、怠けずに履行する体制（含、罰則規定）
モノ	情報資産	<ul style="list-style-type: none"> 機密性、重要度により情報資産を分類、分類に応じた施策を採択 情報の価値、所有者の責任、アクセス権限との関連
	媒体・装置・端末	<ul style="list-style-type: none"> 情報の保管された媒体全ての特定と取扱いの制約 特にノートPC(組織所有、個人所有)の扱い
流れ	ウイルス	<ul style="list-style-type: none"> NW管理者、ユーザ個人が日常的に果たすべき予防行為 トラブル発生時の詳細な手順
	電子メール	<ul style="list-style-type: none"> ユーザ個人が日常的に果たすべき予防行為 トラブル発生時の詳細な手順
	アクセス制御	<ul style="list-style-type: none"> アクセス制御の方針、運用規程、アクセス権割当て ファイアウォールによるアクセス制御方針
	検知・監視	<ul style="list-style-type: none"> 検知・ログ監視の方針、分析方針 内外からのシステム、データへのアクセス状況にかかわるログ項目
	モバイル	<ul style="list-style-type: none"> モバイル機器や設備の運用管理 リモート接続にかかわるアクセス手順
	監査・レビュー	<ul style="list-style-type: none"> レビューのタイミングの規定、責任者の設置 セキュリティポリシーの有効性も適宜レビュー

図5 セキュリティポリシー、ガイドラインとして明文化すべき項目例

6. おわりに

前述の ICSA 社の調査によると、日本における売上高に占める IT 費は、米国が 3.15 % に対して、0.67 % と極めて低い上、IT 総予算に占めるセキュリティ予算も、米国に比してさらに低い。情報セキュリティの専門要員にかかる人件費の差はその大きな要因の一つであり、これはそのままセキュリティに対する上層部の認識の違いであると指摘する声もある。セキュリティの確保にはコストがかかるものであるという上層部への説得努力が更に求められる。

また最近では顧客情報などのプライバシーにかかわる情報を戦略的に扱う機会が増加し、その情報の価値はますます高くなっているが、一方でネットワーク化が進みそのような情報の持ち出しは容易になったといえる。EU はネットワーク社会を前提とした個人情報保護に対して早くから強い姿勢を示してきたが、日本でも最近、個人情報を扱う企業に対して一定の保護基準を満たしていると評価される企業に対するプライバシーマーク制度の運用を始めた。組織が個人情報の処理をアウトソースする際の企業の選定基準となりうる実効性のあるプログラムであると思われる。個人情報を扱う社員一人一人の意識レベルに達するセキュリティ体制が整っているか、再三レビューされるべき重要なポイントであろう。最後は個人のモラルに帰着する。

インターネットは、組織にとって情報セキュリティの概念を大きく変えた。ネット犯罪がますます狡猾な仕組みになって新たな被害が出ようとも、我々は先に進んでいくしか道は無い。インターネットはそれほど広く深く、我々の仕事や生活の中に高い利便性や効率性をもたらしてしまった。暗号技術と情報の運搬の歴史も、様々な妨害との知恵比べの歴史といえるが、インターネットを人類の知恵で更に安全で便利なインフラに成長させていくことはできるはずである。

* 参考文献 *

1. 杉村倫代 (1997):
企業におけるインターネット利用のセキュリティポリシーへの取組み方：経営情報学会
秋季全国研究発表大会予稿集, 262-265.
2. CSI / FBI Security Survey, 1999
3. Briney, Andrew L.:
"Got Security?: ICSA 1999 Info Security Industry Survey." Information Security, July 1999.
4. Information security management: BS7799-1:1999 : BSI
5. 辻井重男 (1999): 暗号と情報社会 : 文藝春秋社

この記事は、エストレーラ (統計情報研究開発センター発行) 2000 年 7 月号に掲載されたものです。