情報セキュリティ対策のルールと技術

多くの企業が、情報セキュリティ対策を西暦2000年問題（Y2K）対応の次の重要なテーマとしてとらえている。情報セキュリティ対策では、情報の機密性・インテグリティ（完全性）・可用性への社内外からの脅威を見定め、予防・発見・対処の観点からルールと技術（システム）の両面による対策を併用することが重要である。

ポストY2K対応の情報セキュリティ対策

Y2K対応も一段落した現在、情報システムに関する次の大きなテーマとして、情報セキュリティ対策がある。

図１はNRI（野村総合研究所）が、2000年１月末に情報システムの担当者向けのセミナーで行ったアンケートの結果である。回答があった76社中、実に73社、率にして96％の方々が、情報セキュリティ対策を次の重要なテーマとしてとらえていることがわかる。

この理由としては、Y2K対応のために、情報セキュリティ対策の優先順位が一時的に下がっていたが、見直す時期となったことに加え、脅威の複雑化および増大、制度の制定、対策技術の進歩、eビジネスの拡大などの要因が考えられる。

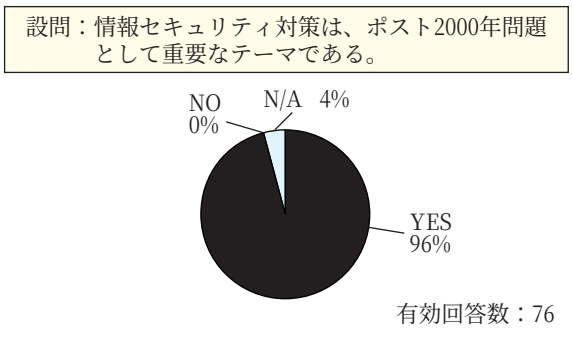


図１　ポストY2K問題としての情報セキュリティ対策の認識

また、図２は同じアンケートにおいて、ビジネス上の取引相手に対する意識についての設問で、情報セキュリティ対策がきちんと行われていない会社と取引するのは抵抗があるとの回答が75社中57社から寄せられた。「NO」(そうは思わない）との回答はゼロであった。BtoC（企業と消費者の間）のビジネスにおいても、BtoB（企業間）のビジネスにおいても、情報セキュリティの対策が十分であるか否かが、ビジネスパートナーの決定において重要な判断指標の１つであると認識されている。

情報セキュリティに対する脅威の現状

今日の企業では業務の電子化が進み、重要な情報の多くはコンピュータ上にファイルで保管されている。また、生産ラインの制御や顧客へのサービスの提供、社内の事務処理など、業務の多くにコンピュータやネットワークが利用されている。

このようなコンピュータ化・ネットワーク化された企業において現在の情報セキュリティ上の脅威はどういったものであろうか。

図３は、CSI/FBI（米国コンピュータセキュリティ協会）が毎年行っている調査結果の

一部である。実際に経験した情報の不正使用およびコンピュータシステムへのアタック（攻撃）の状況に関する質問で、「社内におけるネットの悪用」が1999年の調査では「コンピュータウィルス」を抑えて最も多く検知されており、回答を寄せた521社中394社で、およそ４社に３社の割合である。

また、「情報への社内からの不正アクセス」が223社（43%）、「外部からの侵入」が124社（24%）と、社内と社外の双方から不正なアクセスが試みられている実態がわかる。

また、「ノートPCの盗難」「所有する情報の盗難」「盗聴・傍受」といったデータの機密性に関わる脅威に加えて、「データ、ネットワークの破壊や妨害」「サービス不能攻撃」「詐欺的行為」などの、情報のインテグリティ（完全性）、可用性に対する脅威も経験していることがわかる。

図４は、別の調査で世界の企業2700社を対象にして不正な行為が誰によって行われているかを調べたものである。約半数近くの回答者が「コンピュータ・ハッカーやテロリスト」のように会社の外部の人間としている一方、「正規ユーザーや従業員」「許可がないユーザーや従業員」「元従業員」といった社内の人員をあげる回答者も２～４割に上っている。また、「契約サービス・プロバイダー」

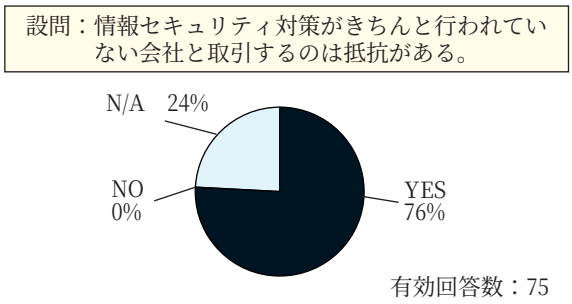
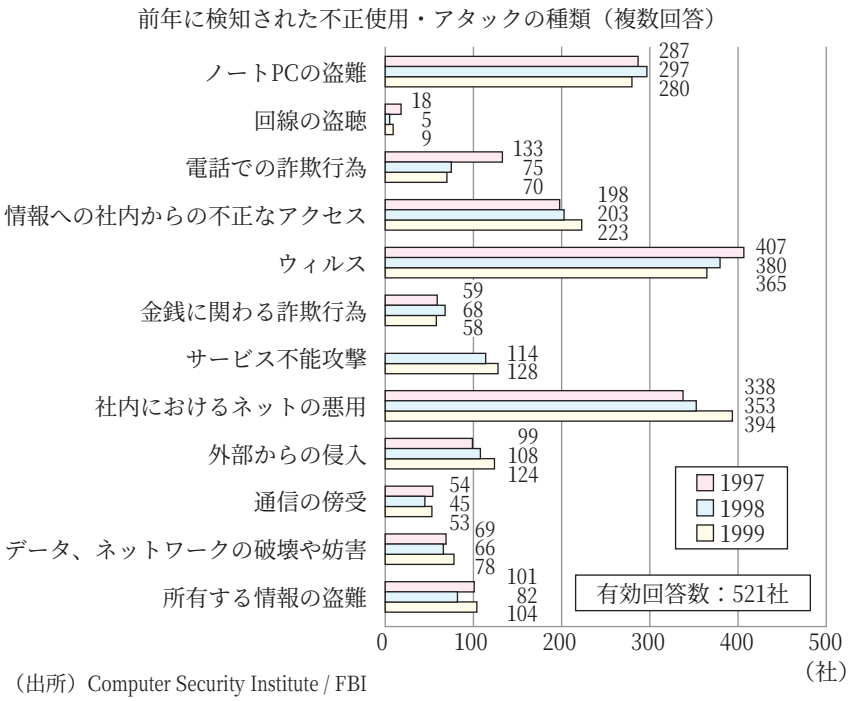
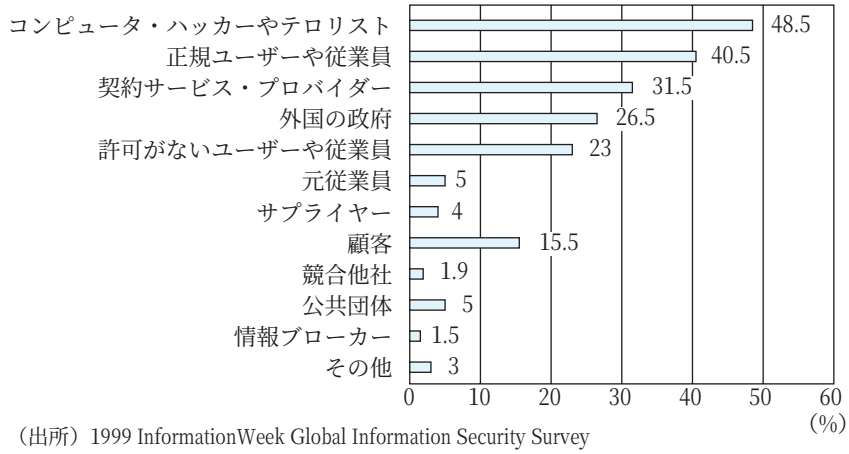


図２　取引相手に対する情報セキュリティ対策の要請



（出所）Computer Security Institute / FBI
1999 CSI/FBI Computer Crime and Security Survey

図３　企業が直面している情報セキュリティ上の脅威



（出所）1999 InformationWeek Global Information Security Survey
49カ国2700名のセキュリティ業務従事者へのアンケート調査

図４　不正行為の容疑者（推測を含む）

「顧客」のように契約関係にある組織や人間も、不正行為を行っていると考えている企業もある（それぞれ31.5%、15.5%）。

社内の人間は、重要な情報がどこに存在するのか、また、社内のセキュリティ対策がどのようになっているのかを知り得るだけに、特定の情報や情報システムを攻撃することが可能な立場にあるといえる。

有効な情報セキュリティ対策

このように、企業は情報や情報システムに対して、社内と社外の双方からデータの漏洩、書き換え、サービス停止といった脅威に曝されている状況にあるといえる。

セキュリティ対策はともすると技術によるシステム的な対策のみが重要視されがちである。技術による対策は対象としている脅威に対しては有効に機能するが、すべての脅威に対して対処できるわけではない。

セキュリティ対策をどのように運用するのか、また、そもそもセキュリティ対策について企業の中で誰がどういう職責を担っているのかを、明確にルールで定めなければ技術的な対策も有効でなくなる。たとえば、あるシステムのログファイルと別の台帳を照合することによって発見できる不正の場合、その照合を行うタイミング、方法、人などをルールで規定することで初めて有効な対策となる。

セキュリティ対策の落とし穴

情報セキュリティの対策の策定には、いくつかの落とし穴がある。以下に代表的なものについて説明する。

①過剰な対策

セキュリティ対策を規定する担当者は、抜けのない対策を策定しようとするあまり、過剰な対策に走りがちである。当然、守るべき大事なものに対して、適切な対策を取ることは必要なことである。その結果、業務効率の低下をともなってしまう場合もある。しかし、がんじがらめの対策では業務そのものがうまく機能せず、逆に実行されることのない名目

だけの対策となってしまう恐れがある。

②予防に偏った対策

予防さえしっかりしておけば、セキュリティ上の問題は発生しないと考えている企業も多い。セキュリティ対策上、情報や情報システムへの侵害を予防するための対策は重要である一方、検知や対処のための対策も重要である。

セキュリティ対策の担当者は、情報や情報システムへの侵害がいつどのように何件発生したかを把握し報告すること、また、発生した場合に迅速かつ効果的に対処することも重要である。また、自社のホームページに対して、どういうアタックがなされているかの傾向をつかむことは、その後の対策方法の検討時に役立つばかりでなく、予算獲得のための根拠となり得る。

③対策を維持していく観点の欠如

策定したセキュリティ対策がビジネスの実態と乖離しないよう、対策を維持・改善していくことを忘れてはならない。また、策定した対策を社内に普及・徹底させることも重要である。

④他社事例の功罪

対策の策定に当たって、他社のセキュリティ対策は参考にはなるが、そのまま採用することはできない。これは扱う情報、保有する情報システム、組織の構造、社風などが異なるためである。まず、自社独自で対策を策定し、最終段階で観点の漏れをチェックするために他社事例を参照すると良い。

対策の事例

A社は、情報漏洩に対する対策の１つとして、社外宛ての電子メールをすべて記録・保管し、漏洩した情報の範囲の把握に備えている。これに加えて、電子メールの宛先、発信者、タイトル、サイズなどについて、発信者の上席者に毎日報告が届く仕組みを構築している。また、保管している電子メールの内容をその上席者が参照するルールも定めており、これらすべてを全社員に告知している。

この例では、①社員に告知することによる牽制効果、②報告の電子メールが上席者に届くことによる、上席者自身が職責を認識する効果、③一連の処理を技術によって自動化することで運用負荷を下げる効果――といった技術とルールをうまく組み合わせた対策で効果を上げている。

セキュリティ対策の策定に際して、自社の持つ情報資産（情報と情報システム）とそれに対する脅威を整理したうえで、どのように回避・対処するかを一つ一つ決めて行くことが重要である。これは大変手間のかかる作業であるが、一度決めてしまえばそれを維持するのは困難ではない。策定に際して業界のガイドラインや他社の対策、専門家などをうまく使うことも重要である。

（野村総合研究所　菅谷光啓）