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

2007－ＣＳＥＣ－38（８）
2007／7／19

2007年情報セキュリティ調査から見た情報セキュリティ状況の比較

山口 健太郎† 内田 勝也†

†情報セキュリティ大学院大学 情報セキュリティ研究科

〒221-0085 神奈川県横浜市神奈川区鶴屋町2-14-1

E-mail: †mgs064512@iisec.ac.jp, uchida@iisec.ac.jp

あらまし インターネットが国境を持たない世界規模のネットワークであることから、その脅威もまた同様の性格を持つ。それゆえ、情報セキュリティを考える上では、グローバルな視点にたって捉えていくことが重要であると考えられる。

本稿は、その試みの一つとして、米国CSI（Computer Security Institute）において行われた調査と、それとほぼ同様の項目について、日本において行った調査の結果を比較し、日米における情報セキュリティについての取り組みの相違などについて概観するものである。

キーワード CSI, 情報セキュリティ，調査，比較

Japan-U.S. comparisons of information security survey

Kentarou YAMAGUCHI† Katsuya UCHIDA†

† Graduate School of Information Security INSTITUTE of INFORMATION SECURITY

2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-shi Kanagawa, 221-0085 Japan

E-mail: †mgs064512@iisec.ac.jp, uchida@iisec.ac.jp

Abstract The internet is borderless network and the threat at the internet is also similar. Therefore, it is very important to think about information security from a global aspect we did the computer crime & security survey in Japan which is almost same as CSI computer crime and security survey and compared its findings to the CSI for finding the difference of the approach of the information security in Japan vs. US.

Keyword CSI, Information Security, Survey, Comparison

1. 調査の概要

1.1. CSIについて

Computer Security Institute（CSI、http://www.gocsi.com/）は1974年に設立された会員組織の情報セキュリティ団体であり、主なイベントとして毎年6月にNetSec、11月にCSI Annual Computer Security Conference and Exhibitionを開催している。前者がセミナー中心であるのに比べ、後者は展示会が主体という傾向があるものの、米国セキュリティ関係者の認識度は非常に高く、特にAnnualの方は2007年で34回目となる歴史のあるものである。

CSI自体の会員数は公表されていないが、米国を中心に約2万人程度の会員がいると言われている。

1.2. CSI調査について

CSIが1996年から、サンフランシスコの米国連邦捜査局のコンピュータ侵入対策チームと共同で行っているのが「CSI/FBI Computer Crime and Security Survey」（以下「CSI調査」と呼ぶ）である。

調査開始後、現在に至るまで、質問項目の多くをあまり変えずに行っていることもあり、米国における情報セキュリティ調査のベンチマーク的な役割を果たしている。

最近の調査においては、毎年1月のはじめに約5,000人の専門家に対して調査資料を送付し、匿名での回答を得る形で行っている。

対象者は、送付者側で抽出するのではなく、原則として自薦によるものであるらしい。

回答数は2004年494名、2005年699名、2006年615名となっており、回答率約10%強、この種の調査としては、平均的な回答率のものと判断できよう。

自薦の情報セキュリティ専門家に送付している状況は、後述する日本での調査とは異なる点である。これが、平均的な値を示さないのではないかという指摘もあるが、それについてCSIは「回答者のセキュリティ経験は豊富であり、所属組織のセキュリティ体制は優れている。このためCSI調査は平均値より優れている可能性があるとともに、的確な回答を得ていると考

えられる」と述べている。

つまり、全体的な傾向については的確であるものの、そのレベルについては、米国の平均値より高い可能性があるということである。

1.3. 国内調査について

中央大学が文部科学省の「21 世紀 COE プログラム」において、2002 年に「電子社会の信頼性向上と情報セキュリティ」拠点として採択されるとともに、内田もその事業推進担当者の一人として任命され、2003 年から CSI 調査とほぼ同じ項目での調査を試みている。

これまで同様の継続的調査が無かったことと、CSI 調査との比較によって、日米の情報セキュリティに対する取り組みの相違が見えてくると考えたからである。

調査については、「情報セキュリティアンケート」（以下「国内調査」という）としてこれまでに 4 回実施している。

第 2 回目以降は 1 月に調査票を送付するというスタイルについても CSI 調査に倣って行っている。（第 1 回のみ年末に調査票を送付した。）

国内調査の対象は、CSI 調査とは異なり、送付者側が、会社四季報(上場企業、未上場企業)、大学関係、法律事務所、自治体等などから選択した約 8,600 の企業、組織である。

当初は記名式の回答であったが、2006 年送付分からは記名・無記名は回答者に任せる形をとっている。

方法が固まってからの回答は 2006 年 1004 件、2007 年 782 件と約 10%程度となっており、CSI 調査と比べても大差ない回答率といって良いだろう。

1.4. 日米の比較と継続的調査の意義

CSI 調査に限らず、米国では様々な調査が行われているし、日本においても、情報セキュリティに関する調査が皆無であるというわけではない。ただ、日米同様の項目について、継続的に比較できるような調査はほとんど存在しないといって良いだろう。

もちろん、日本と米国の企業の状況は異なるものであるし、単純に数値の比較を行うことが有効でないものも多い。前述したように調査方法や対象も異なることから、ここで見いだした相違が意味を持たない場合もあると考えられる。

しかしながら、ネットワークが世界規模で機能している現在、情報セキュリティを検討する際に、日本国内のみ、米国のみといった見方ではなく、複数の国の状況から、全体としての傾向や分析を行うことは大変重要である。

コンピュータウィルスや不正アクセス、サービス停止攻撃（DoS）などの脅威は国など関係なく、それらを相手にする情報セキュリティについても同様であるからである。

継続的に調査を行うことも重要な点の一つである。

継続的な実施は、経年的な変化を発見できることになるし、何よりベンチマークとしての条件といえる。

また、毎年同様の調査を行うことで、調査対象者に意識の変容や啓発を促す効果があるのではないかとも考えている。

たとえば、日経パソコンや日経コンピュータといった冊子が実施する調査が、しばしばランキングといった形で掲載されることがある。その場合に、その調査項目が、企業などにおいて対処すべき項目として認識され、年を追うごとに実施率の上昇するようなものがある。

CSI 調査などにおいても、情報セキュリティ事故(インシデント）に対して発生費用を質問した項目において、1999 年には回答者の 31%しか金銭的な損失を計算していなかったのが、2005 年には全体の 91%が損失の計算を行っているといった状況がある。

この件について、追跡調査を行ったわけではないが、毎年同一の項目があることによって、対象者が触発され、必要性を認識し、実施に至ったと考えることもできる。

評価や結果の公表によって、自らのポジションが明らかになることは、その件に直接携わる担当者にとって強い動機付けとなるということだろう。

「継続的な調査」は、結果として情報セキュリティの認識と必要性を高め、間接的にそれを引き上げる効果もあるのではないかと思う。

2. 調査結果について

本稿では主に CSI 調査の 2006 年結果、国内調査については 2007 年の結果を基に特徴的な部分について比較検討を行う。

本来であれば、同一年の結果を比較することが望ましいが、CSI 調査については、毎年 6 月頃に結果が発表されているため、それを反映させて行う国内調査については、どうしても時間的なずれが生じてしまう。その点についてはやむを得ないところであり、当面はこのような形での比較を行うこととした。

2.1. 調査対象について

調査対象については、日米に大きな差異があると考えられる。それら各項目について述べていく。

2.1.1. 企業規模について

昨年までの調査の傾向と変わらないが、調査対象を従業員の規模で見る限り、CSI 調査と国内調査では分布に大きな違いがある。

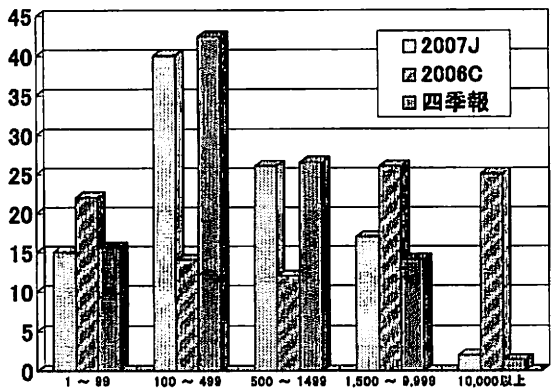
CSI 調査においては、ほぼ平均的に分散している従業員数だが、国内調査の場合、最も多いのは 100～499 名の規模で全体の 40%を占めている。CSI 調査において 25%を占める 10,000 人以上の企業は 2%と極端に少ない。

これは、母集団の状況がそのまま企業の規模に出たものといって良いと考えられる。

CSI 調査については、特に自薦のセキュリティ専門家が回答者になっていることも、この傾向を助長する要因と考えてよいだろう。大企業ほど、そのような専門家を配置し、適切に情報セキュリティに対処していると想像できるからである。

一方で、国内調査の結果が極端なものかということであるが、これについては、やはり、母集団の性格がそのまま出ていると考えて良いと思う。

会社四季報での企業の従業員分布から見ると、ほぼ同様の分布となっており、一見極端に見える回答の分布も、それからすると自然な分布であり、母集団が元々持っている分布がそのまま出たということが言えそうである。母集団の分布とあまり変わらない形での回答となったということは、少なくとも従業員規模で見る限りは、各階層ともに、まんべんなく回答が寄せられたということであろうし、それなりに情報セキュリティに対しての関与が認められると言うことなのだろう。



（単位：人／%）

	1 ～ 99	100～ 499	500～ 1499	1,500～ 9,999	10,000 以上
2007J	15	40	26	17	2
2006C	22	14	12	26	25
四季報	16	42	27	14	1

グラフ 1：従業員数分布（縦軸：%、横軸：人）
2007J：2007 年国内調査、2006C：2006 年 CSI 調査
四季報：会社四季報の分類による企業数

2.1.2. 業種の内訳

業種については、選択肢が CSI 調査と国内調査で異なるため、回答率の高いものから表示をする。

国内調査 2007		CSI 調査 2006	
製造業	27%	金融・保険業	17%
卸売・小売業	15%	コンサルティング	14%
教育・学習支援	13%	ハイテク	11%
公務（政府・自治体）	13%	製造業	9%
建設業	7%	連邦政府	8%
情報通信業	7%	教育・学習支援	8%
複合サービス業	3%	医療・福祉	7%
運輸業	3%	通信業	4%
金融・保険業	3%	州政府	3%
不動産業	2%	地方政府	3%
飲食店・宿泊業	1%	電気・ガス・水道業	3%
医療・福祉	1%	法律	1%
ハイテク	1%	運輸業	1%
電気・ガス・水道業	0%	卸売・小売業	1%
その他	6%	その他	11%

表 1：業種別分布
（回答数：CSI 調査=615 件　国内調査=782 件）

業種において特徴的なのは、CSI 調査での金融・保険及びコンサルティング会社の多さであろう。この分野において、米国ではすでに SOX 法等への対処から相当に専門性を持つ担当者がいることが考えられ、それが金融・保険及びコンサルティング会社が比率的多くなることの原因となっているように思われる。また、国内調査においてそれらの業種が少ないことは、主に母集団の内容に起因するものであろう。

国内調査において卸売・小売業、教育・学習支援、公務(政府・自治体)などが上位にあるのは、調査に対して回答を返しやすいと考えられることや、いずれも個人情報を扱う団体であり、個人情報保護法などの観点で、セキュリティへの関心が高いといった傾向を反映している可能性があるのではないだろうか。

2.1.3. 回答者のプロフィール

回答者プロフィールにおいて特徴的なのは、国内調査における「システム管理者」の比率 44%が CSI 調査の 12%に比べてずば抜けて多いことである。逆に、CSI 調査でほぼ分散して 10%前後存在する CIO や CISO などの役職が、国内調査の場合はほとんどいない。

どうも、日本の場合は情報セキュリティに関して特別な役職を設けているわけではなく、従来の枠組みの中で位置づけている傾向があるようだ。

「セキュリティ部門管理職」に分類された数値についてそれほど差は見いだせない。

2.1.4. パソコン台数

CSI 調査の項目にはないが、国内調査では実施したものである。結果は、企業の規模に比例しているものとなった。

調査結果は昨年とほとんど変わらず、100～999 台に 53%が集中している。1,000 台未満は全体で 72%と多く、

中小規模の企業等が多いことがわかる。

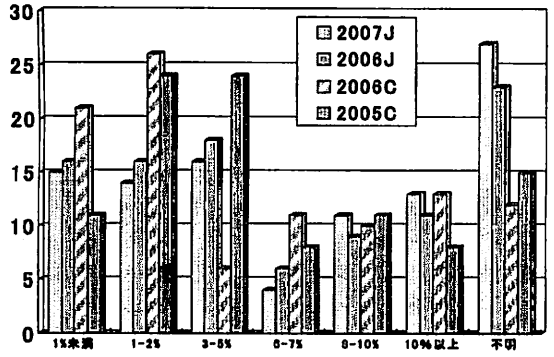
パソコン台数は、セキュリティ対策を実際に行う規模の目安になるものだが、これだけでは、社員にどの程度行き渡っているかを知ることができない。

端末がどの程度いき渡っており、一般化しているかは、セキュリティ対策の「幅」にかかわる部分であり、今後はそのような把握も必要になるかもしれない。

2.2. 情報セキュリティのコスト

2.2.1. 情報セキュリティの予算割合

情報セキュリティ予算について、情報システム予算のどの程度の割合かを調査した項目である。



（単位：%）

	1%未満	1～2%	3～5%	6～7%	8～10%	10%以上	不明
2007J	15	14	16	4	11	13	27
2006J	16	16	18	6	9	11	23
2006C	21	26	6	11	10	13	12
2005C	11	24	24	8	11	8	15

グラフ２：情報セキュリティ予算割合（縦軸：%、横軸：人）
2007J、2006J：2007、2006 年国内調査
2006C、2005C：2006,2005 年 CSI 調査

この質問については、適切に調査結果が出ているとはいいにくい部分がある。システム関係の予算のうち、情報セキュリティ関連の予算をどの範囲と考えるかで、大きく回答が異なってくるからである。

たとえば、機器に付属してくる認証装置や建物そのものに付随するセキュリティ設備、各種の運用経費のなどのうち、どこまでをセキュリティ経費と見るかは、回答者の主観に依存する部分が多く、調査において標準的な形を示しているわけではない。回答にあたって数値をどのように計算したのかは様々であると言える。そのため、およその目安と考えるべきであろう。

全体としては国内調査のほうが「不明」と答えた数が多く、CSI 調査のほぼ倍近くの割合である。これは、SOX 法対応などで、情報資産の洗い出しとそのコストの明確化が進んできた米国と、まだ途上にある日本との差が出ているとも考えられる。

そのほかは、あまり特徴がなく、経年的な変化も乏しい分布であるといって良いが、CSI 調査においては 2005 年の結果と 2006 年の結果において、3～5%と答えた数が大幅に減少し 1%未満の答えが増加しているのが特徴的である。

コンピュータの性能は年々高度化していることから、セキュリティ機器についてもコストパフォーマンスの良いものが出てきているのは事実である。また、より正確にコストを算出することができるようになったという状況もあるかもしれない。

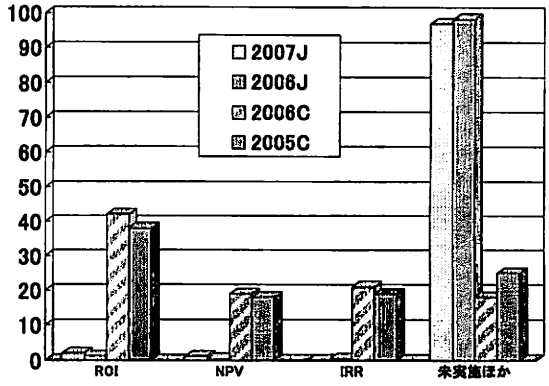
効率的に効果を出すことができているのであれば、歓迎すべきことであるが、この項目については、調査方法の改善やより詳細な調査が必要であろう。

2.2.2. 情報セキュリティ投資効果

情報セキュリティ投資効果について、その実施の有無について聞くとともに、実施している場合の方法について回答を求めたものである。

この項目については国内調査と CSI 調査との明確な差が出ている。

日本においては回答数にほんの若干の増加が見られるものの、依然として傾向は変わらず、「行っていない、わからない」と答えたものだけで 94%を占める。CSI 調査の回答では 82%が何らかの方法で効果測定を行っていることに比べると全く逆の状況であることがわかる。



（単位：%）

	ROI	NPV	IRR	未実施ほか
2007J	2	1	0	97
2006J	1	0.3	0.4	98.3
2006C	42	19	21	18
2005C	38	18	19	25

グラフ３：情報セキュリティ予算割合（縦軸：%、横軸：項目）
2007J、2006J：2007、2006 年国内調査
2006C、2005C：2006,2005 年 CSI 調査
ROI：Return On Investment【投資収益率】
NPV：Net Present Value【純現在価値】
IRR：Internal Rate of Return【内部収益率】

前項の調査結果において、それなりに情報セキュリティへの投資自体は行われていると考えると、日本においてはその投資が、明確な投資効果の計算なしに実施されている状況ということになる。

セキュリティ事故が発生するたびに、関連セキュリティ商品が売り上げを伸ばすような状況があることを考えあわせると、日本においては、投資対効果を明確

にして計画的にセキュリティ対策を行うということではなく、とにかく、対策を対症療法的に行っている状況なのかもしれない。

また、セキュリティ事故により失われるコストの定量的な把握については、事故発生前に行う方法論が確立されてはいないことも、投資対効果の算出を難しくしている理由であろう。

情報セキュリティについてのコストを明確化する方法は近年研究が進んでおり、情報セキュリティ大学院大学の高津、内田による研究[1][2]などは、これまでの方法を改善しているものの一つといえるが、それにしても、いわゆる事務的な経費等を含めた計算方法は確立されておらず、より効率的に計算する方法論の確立を待っている状況である。

近年の情報漏洩事故を例に挙げるまでもないが、大量の情報が簡単に流出、持ち出しされるものが多く、その影響は非常に大きいものとなっている。事故をなくすことはできないが、情報セキュリティについて明確な投資対効果を考えることは、企業のリスクをコントロールしていく上で、非常に重要な点であるといえ、日本の企業は、その点にもっと注力すべきであるといえる。

2.2.3. その他の項目

そのほかの項目としては、「情報セキュリティ保険加入の有無」「情報セキュリティ監査実施の有無」「情報セキュリティの外注割合」「情報セキュリティ教育実施レベル」などがある。

「情報セキュリティ保険加入の有無」「情報セキュリティ監査実施の有無」については、経年的に見るといずれも漸増の傾向があり、CSI 調査の結果のほうがいずれも高い割合である。

「情報セキュリティの外注割合」についても昨年までの傾向とあまり変わったことはなかった。

「外注」についても、特に増加の傾向はない。

しかし、外注については、高度化、複雑化するセキュリティ事故の対策について、専門的な技術を持つスタッフによって適切、迅速に対処することがその後の拡大や問題の発生を抑制することにつながる場合も多いことなどから、自社で技術者を育成することの困難さを考えると、投資対効果が明確になってきた場合には、もっと増加していくとも考えられる。

他の項目と関連して変化する項目の一つであるとも言えるだろう。

「情報セキュリティ教育実施レベル」については、今年から項目に加わったもので、0 から 7 の範囲で選択する方法をとっている。

今回の結果は 0～3 までが全体の 70%、4 以上が 30%と「控えめ」というか「まだまだ」という状況であることがわかる。

これらの調査についての詳細は別の機会に譲ることとしたい。

2.3. 情報セキュリティの利用技術

セキュリティ利用技術については、候補をあげ、複数選択方式での回答としたものである。

	CSI 調査 2006		国内調査 2007	
1	ファイアウォール	98%	ワクチン（アンチウィルス）ソフトウェア	95%
2	ワクチン（アンチウィルス）ソフトウェア	97%	ファイアウォール	92%
3	アンチ・スパイウェア	79%	一般的なパスワード	82%
4	アクセス制御（サーバ用）	70%	アクセス制御(サーバ用)	69%
5	侵入検知システム：IDS	69%	アンチ・スパイウェア	47%
6	送信中のデータ暗号化	63%	ログ管理ソフトウェア	37%
7	保存ファイルの暗号化	48%	送信中のデータ暗号化	35%
8	一般的なパスワード	46%	IC カード／ワンタイムパスワード	26%
9	侵入防止システム：IPS	43%	侵入検知システム：IDS	24%
10	ログ管理ソフトウェア	41%	保存ファイルの暗号化	19%
11	アプリケーションレベルファイアウォール	39%	アプリケーションレベルファイアウォール	17%
12	IC カード／ワンタイムパスワード	38%	侵入防止システム：IPS	15%
13	フォレンジックスソフトウェア	38%	無線 LAN セキュリティソフトウェア	12%
14	ＰＫＩ	36%	ＰＫＩ	9%
15	無線 LAN セキュリティソフトウェア	32%	バイオメトリックス	9%
16	クライアント用セキュリティソフトウェア	31%	その他	4%
17	バイオメトリックス	20%	フォレンジックスソフトウェア	2%
18	その他	4%	クライアント用セキュリティソフトウェア	－

表２　情報セキュリティ利用技術（複数選択回答）
※割合はそれぞれ返却回答数に対してのもの
（回答数：CSI 調査=615 件　国内調査=782 件）

結果を見てわかるとおり、全体としてセキュリティツールの導入については圧倒的に CSI 調査の値が高い。上位 3～4 番目までのものはともかく、そのほかは、半分以下の導入であるものも多い。一番低いバイオメトリクスでさえ、CSI 調査の場合は 20%である。日本の状況はやはり、まだまだと言えるだろう。

また、特徴があるのは、CSI 調査の 3 位に入っているアンチ・スパイウェアだ。

最近は、攻撃者の目的が、技術の誇示や愉快犯的なものから金銭に移行してきたことで、不正プログラムの傾向が変化してきているといわれている。「目立つような挙動をとる」ものから「できるだけ目立たずに目的を遂行する」ものへと変化しているのである。

この「アンチ・スパイウェア」の割合の高さは、それらの「目立たない」不正プログラムを用いた攻撃、いわゆるスピア型攻撃（Targeted Attack）などにより、情報が流出することや、それに端を発するフィッシングやファーミング等の詐欺、密かに仕掛けられていく bot などへの対策の必要性が高くなってきている状況を表しているのではないだろうか。

国内調査において 3 位にあるのは「一般的なパスワード」である。CSI 調査の結果に比べ圧倒的に大きな値となっている。手軽で安心ということなのだろうか。

IDS や IPS などの不正アクセスの検出・防御などをインテリジェントに行う機器の導入は、昨年に比べ微増したものの全体としては少なく、そのほかのセキュリティツールの導入も進んでいるとは言えない。

ツールを導入したから安全というわけではないが、ここに、日米のセキュリティ対策の差、経験の差が現れているといってよいだろう。

2.4. 情報セキュリティ事故(インシデント)

ここでは選択肢の中から、実際に発生したインシデントについて選択をしてもらっている。

	CSI 調査 2006			国内調査 2007	
1	ウイルス感染	65%	1	ウイルス感染	84%
2	ノート PC などの盗難	47%	2	発生していない	43%
3	内部者のネット・アクセス乱用	42%	3	ノート PC などの盗難	30%
4	情報への不正アクセス	32%	4	内部者のネット・アクセス乱用	22%
5	DoS 攻撃	25%	5	DoS 攻撃	14%
6	システム侵入	15%	6	情報への不正アクセス	5%
7	無線 LAN の無許可利用	14%	6	ウェブの改ざん	5%
8	情報資産の盗難	9%	8	システム侵入	4%
8	金融詐欺	9%	8	その他	4%
10	通信詐欺	8%	10	情報資産の盗難	3%
11	ウェブの改ざん	6%	11	ファイル破壊／改ざん	2%
11	公開ウェブの悪用	6%	11	無線 LAN の無許可利用	2%
13	ファイル破壊／改ざん	3%	13	パスワード盗聴	1%
—	システムがボットネットに悪用された	—	13	通信詐欺	1%
—	システムが Phishing に悪用された	—	13	システムがボットネットに悪用された	1%
—	IM（インスタントメッセージ）の悪用	—	13	システムが Phishing に悪用された	1%
—	パスワード盗聴	—	17	金融詐欺	0%
—	DNS サーバが悪用された	—	17	IM（インスタントメッセージ）の悪用	0%
—	その他	—	17	DNS サーバが悪用された	0%
—	発生していない	—	—	公開ウェブの悪用	—

表3　情報セキュリティ事故（インシデント）（複数選択回答）
※割合はそれぞれ返却回答数に対してのもの。
（回答数：CSI 調査=615 件　国内調査=782 件）
数値部分が「－」で項目に網がかかっているものはそれぞれの調査において選択肢にないもの。

表を見てわかるとおり、大きな差がある。

CSI 調査においては、「事故（インシデント）が発生していない」という回答はないのに比べて、国内調査では 43%もの率でこの「発生していない」が選択されている。また、この値は、2006 年の調査時には 23%であったのに比べ倍増している。少々違和感のある数値である。

確かに、少しずつではあるが、セキュリティツールの導入もすすみ、啓発も行われていることもあり、それらが全く効果をあげていないとは言えないだろう。しかし、これほど劇的な数値の差が出るほどの効果をあげているとは到底思えない。

相変わらず、電子メールによるウイルスは数多く送信されているし、新しい攻撃手法も日々編み出されている状態である。また、数値的に整合しないのは、そもそも 84%がウイルス感染にあったという回答をしているのだから、43%が何も起こしていないはずがないのであり、何を事故（インシデント）と認識するのかということ自体にも考え方の相違がありそうだ。

国内調査においては特に数値的に伸びを見せているのがウイルス感染である。

2006 年度 67%だったものが 84%と 17 ポイントも増加している。そのほかのものも増加しているのだが、ウイルス感染の増加は著しいものである。

ワクチン（アンチウィルス）ソフトウェアは、ツールとしての導入率は高いのだが、その効果が有効に発揮されていないということを表しているともいえる。

要は、導入したことで安心してしまい、パターンファイルの更新などを適切に行っていないという状況があるということではないか。なかなか対策の進まない一般ユーザーの環境などにも問題はあり、このあたり、一層の啓発が必要といえよう。

CSI 調査において、「ノート PC などの盗難」は相変わらず高い割合だが、国内調査においても 2006 年に 23%だったものが 30%と 7 ポイント増加している。これなどは、パソコンに保存されている情報をねらうというよりは、持ち出しやすく、比較的高額で換金しやすい対象として盗難の対象になっているとも考えられる。情報流出による 2 次的被害により致命的な損害を被らないよう、十分な盗難対策を講じるべきであろう。

国内調査の結果において、いわゆるネットワークを介した攻撃などについては、総じて数値が低いが、これはそのまま「発生していない」ととらえるのは早計であろう。

根拠となる数字がある訳ではないが、攻撃に気がつかない場合も多く、単に数値として表れないだけとも考えられるからである。

このほかに、インシデントの発生回数やその頻度、発生源（内部か外部か）などについても回答を得ているが、これまでと大きく傾向が変わることはなかった。

2.5. 情報セキュリティ事故(インシデント)の費用

この費用計算については、計算モデルがあるわけではないため、計算方法は回答者に任されている。

一般的な傾向をつかむにとどまる部分であるが、CSI 調査のほうが明らかに回答数が多い。

以前の調査においては、CSI 調査において、699 人中 639 人（91.4%）の回答者が費用計算を行っていたのに対し、国内調査では 1004 件中 216 人（21.5%）しか行っていない。

しかし、費用計算について 2007 年には 782 人中 246 人（31.4%）と漸増し、投資対効果などの観点での対応が徐々に広がっている兆しが見える。

2.6. その他の項目

そのほか、調査においては、「インシデント発生時の対応」「セキュリティ組織への所属状況」「情報セキュリティの確保に効果的と思われるもの」等を聞いている。これら詳細については、また別の機会に述べたい。

3. 全体を通じて

3.1. 今後の調査について

国内調査については 2007 年までで 4 回実施したこ

とになる。

COE プログラムにおける実施はとりあえず今回で終了することになるが、できるだけ今後も実施し、データの集積を続けることにより、国内のセキュリティ状況を経年的につかむデータを提供できるようにしたいと考えている。

また、今回行ったのは CSI 調査との単純な比較であるが、個別項目の経年変化やクロス集計により、様々な分析が可能であろうと考えられる。

データを広く共有することで、より深く、広範囲な分析が可能となるだろう。

また、自治体等については、総務省が毎年、基礎的な事項について調査を実施している。そういった調査との項目の共通化ということも、検討が必要であると言える。

3.2. 今後の課題

3.2.1. 回答率の低さの改善

相当数の調査票を発送しているにもかかわらず、回答率は決して高いとは言えない。

標本として数が不十分というほどではないが、もう少し多くの回答があれば、より有効なデータとなるだろう。

このような調査自体は、担当者の時間を消費させることになるが、きちんとまとめて共有できる数値とすることで、回答にかかわった方々の苦労に報いることができると思う。

また、セキュリティの情報について、何でもかんでも隠しておくことが安全につながるという考え方も根強い。こういった考え方によって、回答を行わない企業なども多いと聞く。

しかし、本当にそうであろうか？

我々に必要なのは、現況を適切にとらえ、それを分析し、対応していくことであるはずで、そのためには、共有できる情報はできるだけ共有して、そこから有効な対策を見いだすことが求められているのではないだろうか。

今回の国内調査の調査項目が、回答することでセキュリティを低下させるものかどうか、今一度検討してみていただきたいとおもう。

さらに、今後は以下のような方向での取り組みを検討したい。

（1）CSI 調査が FBI と協力しているように、警察庁などと協働した調査としていくこと。これにより調査自体のステータスの確保とより高い安全性を担保することができる。
（2）CSI 調査や同様の項目により行われているオーストラリアの情報セキュリティ調査との連携や項目の調整。
（3）被調査者、調査者双方にとってより負担の少ない調査方法の実現。
（4）費用計算や判断の共通化に役立つモデルなどの検討。

このような取り組みを進めていくことで、これまでの調査をより効果的、効率的な形で進めることができると考えている。

4. 謝辞

本稿の元になった「情報セキュリティアンケート」は、文部科学省「21 世紀 COE プログラム」の一環で 2002 年度に採択された中央大学 21 世紀 COE プログラム「電子社会の信頼性向上と情報セキュリティ」の活動の中で調査・研究を実施したものである。

本調査を行うにあたり、回答をいただいた多くの方々に対し、ご協力に厚くお礼を申し上げたい。

文　献

[1] 高津 岳志，内田 勝也，“情報セキュリティインシデントにおける定量的分析に関する一考察”,情報セキュリティ大学院大学修士論文, Mar.2007.

[2] 高津 岳志，内田 勝也，“情報セキュリティインシデントにおける定量的分析に関する一考察”,日本セキュリティ・マネジメント学会第 21 回大会発表要旨, pp.89-94, Jun.2007.

参考資料

1 （株）東洋経済新報社，会社四季報 CD-ROM2007 年 3 集

2 内田勝也,”第 3 回情報セキュリティ調査　情報セキュリティ調査から見た日米情報セキュリティ比較”, URL :
http://www.uchidak.com/chuo/2006_Japan_CSI.pdf
2007 年 6 月 27 日アクセス

3 CSI/FBI Computer Crime and Security Survey
URL:
http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml;jsessionid=WYIHG5PW2MG2CQSNDBCSKH0CJUMEKJVN