

## 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みた日米情報セキュリティ比較

情報セキュリティ大学院大学  
兼 中央大学研究開発機構  
内田 勝也

### 1. はじめに

インターネットの急速な発展はサイバー空間においては、最早、時間的、空間的な距離がなくなってきた。このことは、インターネットにおける犯罪や犯罪的行為も同様で、インターネット等へのサイバー攻撃は国内はもとより、海外からも攻撃されている。地理的な問題がないことは、時間的にも問題もなく、攻撃は四六時中行われる。また、最近は特定の企業や組織を標的にする攻撃だけでなく、無作為に攻撃が行われるため、企業・組織の大小、有名・無名等に関係なく被害を受ける可能性が高い。

このため、情報セキュリティ対策もグローバルな状況を捉えることが大切であろう。

### 1.1 CSI調査について

#### (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、6月にNetSec、11月にCSI Annual Computer Security Conference and Exhibitionを開催している。その他、全米各地で情報セキュリティセミナーを開催している。また、月刊のニュースレター「ALERT」、四半期毎に「Computer Security Journal」等を発行している。会員の公表はされていないが、米国を中心に世界各国から2万人程度がいると言われている。

#### (2) CSI調査

海外では古くから情報セキュリティに関係する調査が行われているが、CSIは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、1996年から調査を行っている。正式には「CSI/FBI Computer Crime and Security Survey」(以下、CSI調査と呼ぶ)と言われており、調査開始以来、質問項目の多くがあまり変わっていない、また、これ程長期間に渡って実施している情報セキュリティ調査はないため、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CSI調査では、毎年1月始めに約5,000人の専門家に対して調査資料を送付している。回答者は、米国企業、政府(連邦、州、地方政府)、金融機関、医療機関、大学などに勤務している情報セキュリティ専門家を対象としている。送付は印刷物として郵送するだけでなく、電子メールでも行っている。回答は印刷物の場合も、電子メールの場合も、匿名での回答になっている。送付は無差別に行うのではなく、調査者は原則として自薦になっているようである。2005年は699人、2004年は494名から回答を得ている。

専門家に送付しているため、回答が片寄っているとの指摘に対して、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り、的確な回答を得ている』と述べている。

これは、情報セキュリティの専門家がいる企業・組織は、情報セキュリティの専門家がない企業・組織より、情報セキュリティのレベルは高いと考えることができる。この点は、国内で行われている情報セキュリティ調査を含め、多少、高いレベルの値がでることは十分考えられる。

### 1.2 国内調査について

中央大学は、文部科学省「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た。筆者は事業推進担当者に一人として任命されたのを受け、2003年より、CSI調査とほぼ同一の調査を試み、日米の情報セキュリティに対する取組について検証を行っている。

## 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みた日米情報セキュリティ比較

現在、第3回までの調査を実施してきたが、第1回目は年末に実施したが、第2回目以上は、CSI調査と同様1月に調査票を郵送し、前年度の状況について回答を求めた。

本調査は、CSI調査と異なり、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、約8,600の企業・組織に対して送付している。2006年は約1,000から回答を得ることができた（回答率は約12%となっている）。なお、当初は記名式を原則として調査を行っていたが、2006年の調査からは記名・無記名は回答者に任せるようにした。

### 2. 調査の目的

#### 2.1 日米における情報セキュリティの比較

CSI調査は長期間行われており、国内では情報セキュリティに関する調査が行われているが、海外の調査との比較を継続的にしているものがあまりない。

インターネットの普及は、情報セキュリティ分野における事件・事故は国境を越えて発生することが多く、単に国内だけを見るのではなく、海外も含めてみるのが大切であると考えた。

ただ、調査方法が同一でないことやそれぞれの国の環境も必ずしも同一でないため、回答結果を見て単純に比較をすることが必ずしも適当でないこともある。

例えば、米国では、SOX法が、2002年に成立し、この法律の影響により情報システム分野における内部統制を考え、情報セキュリティマネジメント体制の確立が重要なものの1つになってきた。しかしながら、国内ではSOX法に相当するものを金融庁が検討しているが、早くても2009年頃に導入されるとされており、SOX法による情報セキュリティへの影響と言った質問を調査項目に含めることはできない。

「日本版SOX法の導入が予定されているが、そのために何をすべきと考えているか」と言ったような質問項目を設けることが可能であったとしても、二国間での比較が可能になることはない。

#### 2.2 継続的調査

毎年、調査対象が同じではないが、同一の質問内容に対する回答を得ることにより、全体的な傾向が見える場合が多い。

例えば、個人認証システムの1つである「固定パスワード」の利用について、CSI調査では1998年から2005年までの8年間の調査結果があるが、調査年ごとに多少の変化はあるがほぼ半数以上が固定パスワードを利用していると回答している。一方、生体認証の利用については、次第に増加する傾向があるが、固定パスワードを凌ぐほどにはなっていないことがわかる。

このような傾向をみることにより、固定パスワードをより安全に利用できる仕組みを考えることは、情報セキュリティレベルを高めるためには、必要なことではないかと考えることができる。更に、継続的な調査を行うことは、調査対象企業・組織に対して、重要事項を気づかすことができる面もあると考えた。

CSI調査では、情報セキュリティでのインシデントに対して、発生費用を質問しているが、1999年には、金銭的な損失に対して回答者521人の内、51%があると感じているが、損失を計算しているのは、31%でしかないと述べている。

しかしながら、2005年の調査結果をみると、699人の回答者の内、639人が回答しており、全体の91%が回答していることになる。

回答者の多くが、毎年同一の質問があることによって、その質問で期待している事柄を所属している企業・組織でも行う必要があるのではないかと考えるに至ったと考えることもできる。

また、回答結果や質問内容から、情報セキュリティ分野での予算を獲得するために、経営者を説得する材料になると考え、それらを利用して所属企業・組織での実施を提言し、予算を獲得できたため、次年度からは回答ができるようになると考えても不思議ではない。

本調査では、簡単な質問を並べて回答を得るだけであるため、多くを語ることはなかなか難しい。

### 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みた日米情報セキュリティ比較

面接調査や回答回収後に確認などを行っていないため、質問が十分に調査者に伝わっていなかったりすると思われるものもある。

しかしながら、この調査が、情報セキュリティ分野でのベンチマーク的な存在になることを目指して、今後も調査を継続したいと考えている。

#### 3 調査結果

ここでは、2005年CSI調査と2006年の国内の調査を対象に比較を試みた。同一年のものを対象に比較をすることが望ましいが、CSI調査については毎年5月前後に発表されている。CSI調査の質問内容を事前に取得できないため、公表された質問内容を見ながら、国内調査を行っている。時間的なずれはあるが、この方法で比較を行うことが当面の方法としては最善であると考えている。

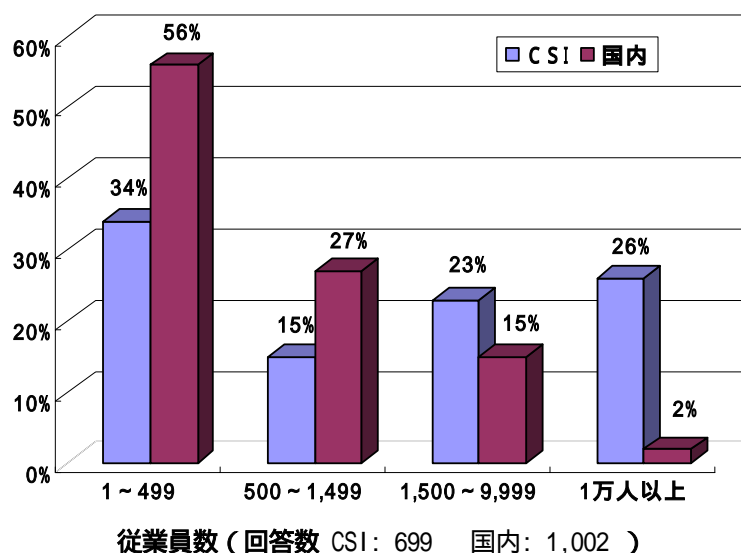
##### 3.1 調査対象の概要

調査対象企業・組織の概要は以下の通りである。

###### (1) 従業員数

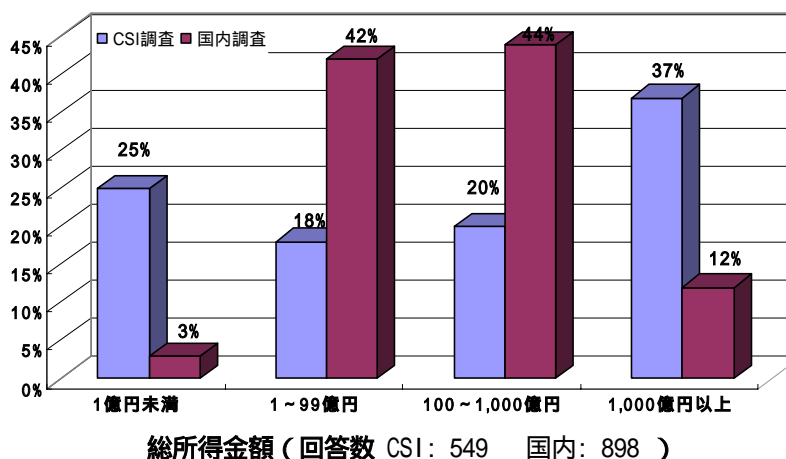
調査対象の規模を従業員で見ると、CSI調査は比較的大規模な組織が多く、国内では小規模な組織からの回答が多い。

この1つの理由は、CSI調査では、情報セキュリティの専門家に送っているため、そのような専門家がいる所は、比較的大規模の大きい組織になると思われる。一方、国内では、会社四季報等を利用して送付していることも理由であろうと思われる。但し、国内で行われている情報セキュリティ調査をみても、従業員数の少ない所の回答が多い傾向が強い。



###### (2) 総所得金額

CSI調査では、1,000億円以上が他より多いが、平均的に分布している。国内調査では、1億円から1,000億円までが大部分を占めている。CSI調査は、1億円未満が国内の8倍強あり、



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みた日米情報セキュリティ比較

1,000億円以上も3倍強を占めている。

(3) 業種

業種は、日米で異なっているため、回答率の高い順に表示した。

米国では、金融業、ハイテク産業、製造業、連邦政府、医療の順になっているが、国内調査では、製造業、卸・小売業、教育・学習支援、建設業、通信業の順になっている。

なお、国内調査で、電気・ガス・水道業、及び法務・法律は0%となっているが、それぞれ、2件、1件の回答があった。

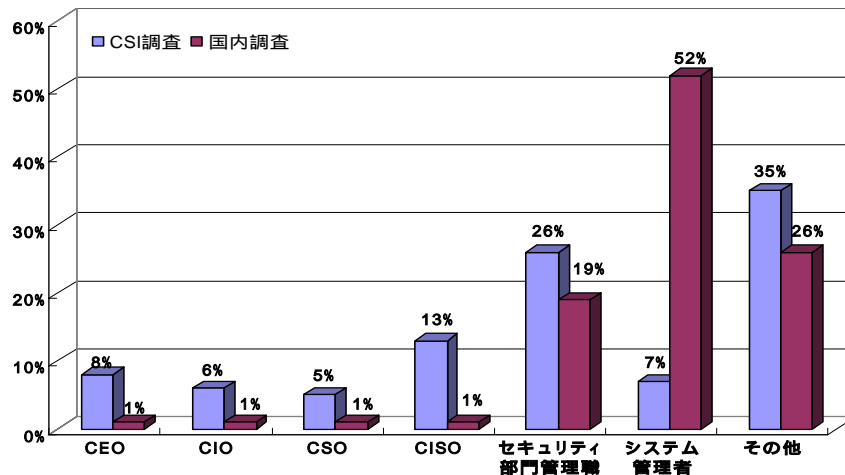
CSI 調査		国内調査	
金融業	17%	製造業	34%
ハイテク産業	15%	卸売・小売業	14%
製造業	9%	教育・学習支援	12%
連邦政府	9%	建設業	8%
医療	7%	情報通信業	7%
教育	6%	公務(政府・自治体)	5%
州政府	5%	複合サービス業	5%
通信業	4%	運輸業	3%
電気・ガス・水道	4%	金融・保険業	2%
地方政府	2%	不動産業	2%
運輸業	1%	飲食店・宿泊業	1%
小売業	1%	医療・福祉	1%
法律	1%	ハイテク	1%
その他	19%	電気・ガス・水道業	0%
		法務・法律	0%
		その他	6%

**業種 (回答数 CSI: 699 国内: 1,004)**

(4) 回答者のプロフィール

CSI 調査では職種 (Job Description) を聞いているが、国内調査では「該当する役職」として聞いた。

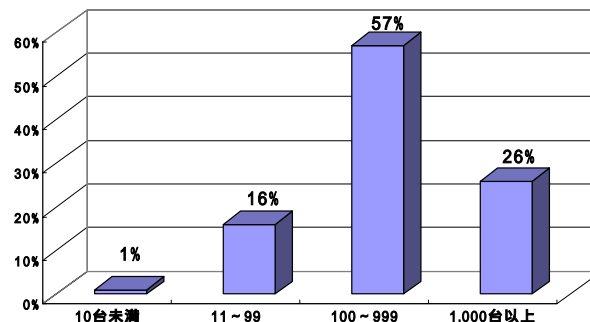
なお、日米で役職が微妙に異なるが、セキュリティ部門管理職は、Security Officer/Manager/Director とし、また、システム管理者は、Systems Administrator とした。



回答者のプロフィール (回答数 CSI: 690 国内: 1,004)

(5) パソコン台数

CSI 調査では実施していないが、国内調査では実施してみた。PC 台数は、従業員数とも関係するが、100~999台が約6割を占め、1,000台未満が4分の3を占めた。



パソコン台数 (国内: 1,004)

### 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みた日米情報セキュリティ比較

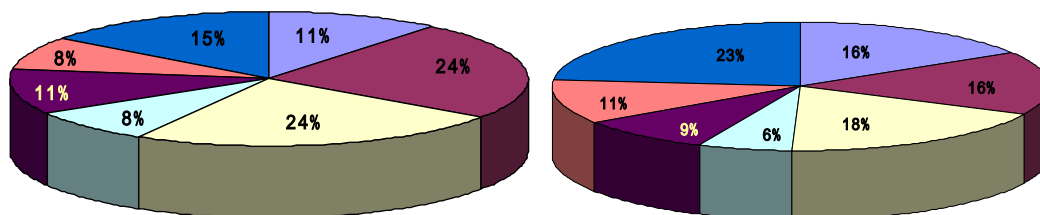
#### 3.2 情報セキュリティ予算、利用技術など

##### (1) 情報セキュリティ予算割合

情報セキュリティ予算は情報システム予算のどの程度の割合かを調べた。

『最近の環境を考えると、情報セキュリティの予算割合は必ずしも適切に計算できない』との指摘がある。例えば、最近のノートパソコンの多くは指紋認証装置を標準で持っており、その指紋認証装置を使って、個人認証を行うことを考えると指紋認証装置は情報セキュリティ予算として考える必要があるが、ノートパソコンの価格の何%を占めているかを計算することは難しい。このため、おおよその目安として考えることが大切であろう。

CSI 調査では、情報システム予算の1~5%が情報セキュリティ予算であると半数弱が回答しているが、国内調査では1~5%が34%となっており、5%以下が半数と回答している。



	1%未満	1~2%	3~5%	6~7%	8~10%	10%以上	不明
CSI 調査	11%	24%	24%	8%	11%	8%	15%
国内調査	16%	16%	18%	6%	9%	11%	23%

情報セキュリティ予算割合 (回答数 CSI: 690 国内: 964 )

##### (2) 情報セキュリティ投資効果の計算

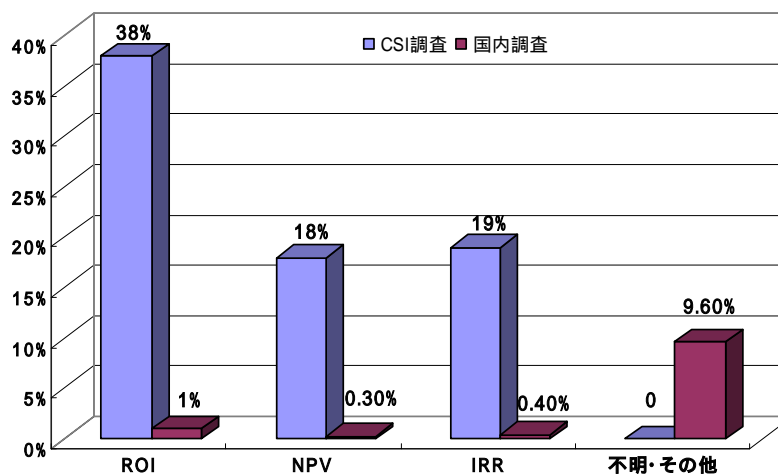
情報セキュリティ投資について、投資効果を計算しているかを聞き、計算している場合には、どのような方法で計算しているかをたずねた。

CSI 調査では、599 人から回答 (回答率: 86%) を得ているが、国内調査では、17 人のみが、ROI、NPV、IRR と回答しており、不明・その他の 94 人を含めても、回答者 (980 人) の 11% 余りでしか情報セキュリティ投資対効果は計算されていない。

最近発生している

「情報暴露型」コンピュータウイルスで明らかになった中央官庁や各県の警察等の情報漏洩からも分かることは、投資対効果を考えることが必要であろう。

なお、表中では国内調査で、「実施していない」と回答した 88.7%については表示してない



情報セキュリティ投資効果の計算 (回答数 CSI: 599 国内: 980 )

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みた日米情報セキュリティ比較

い。

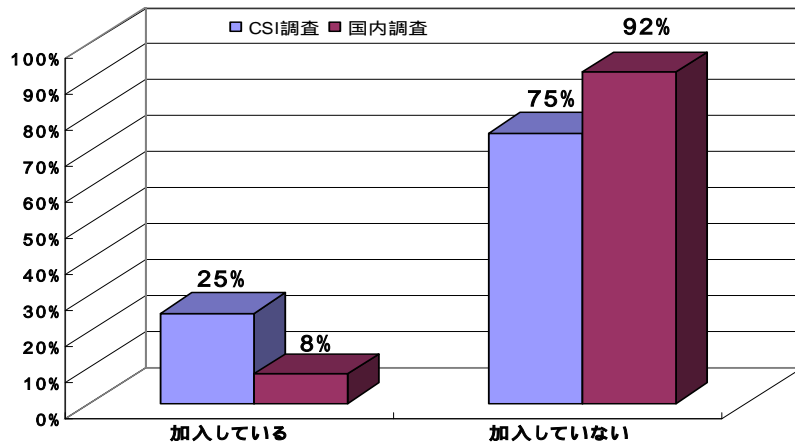
(3) 情報セキュリティ保険の有無

国内外で情報セキュリティ保険が発売されているが、保険を利用しているかたずねた。米国でも25%の加入割合であり、必ずしも加入率が高いとは言えない。国内では、更に少なく8%にとどまっている。

適切な保険が発売されているかも問題になるが、以前から比べると国内でも情報セキュリティ関連の保険が増えてきているが、これからであろう。

一般に、保険の加入数が多いと、それだけ正確に損害率がわかり、保険料も適正なものになる。ある保険が発売され始め

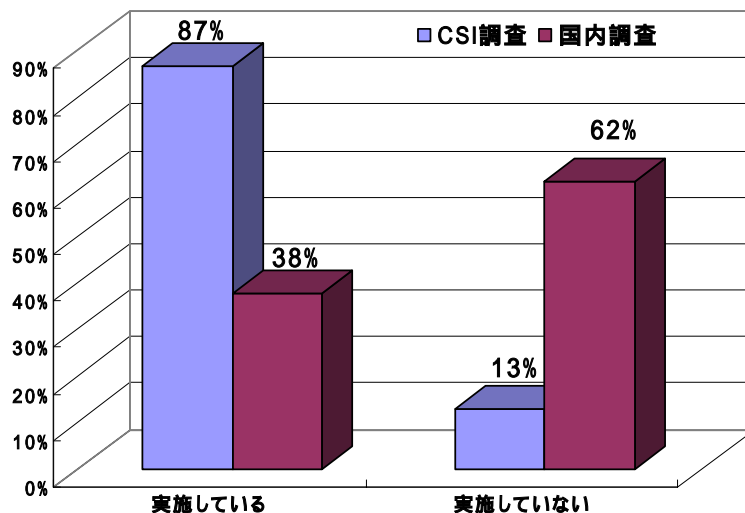
た頃は、当然ながら加入が少なく、保険を必要とする者が加入する傾向がある。そのため、保険料も高止まりする傾向があるとも言われている。



情報セキュリティ保険の有無 (回答数 CSI: 652 国内: 997 )

(4) 情報セキュリティ監査の有無

情報セキュリティ監査については、CSI 調査と国内調査では、かなり相違がある。CSI 調査では、90%弱(592人)が実施していると回答しているが、国内調査では、40%弱(382人)のみが実施していると回答している。



セキュリティ監査の有無 (回答数 CSI: 652 国内: 997 )

(5) 情報セキュリティの外注割合

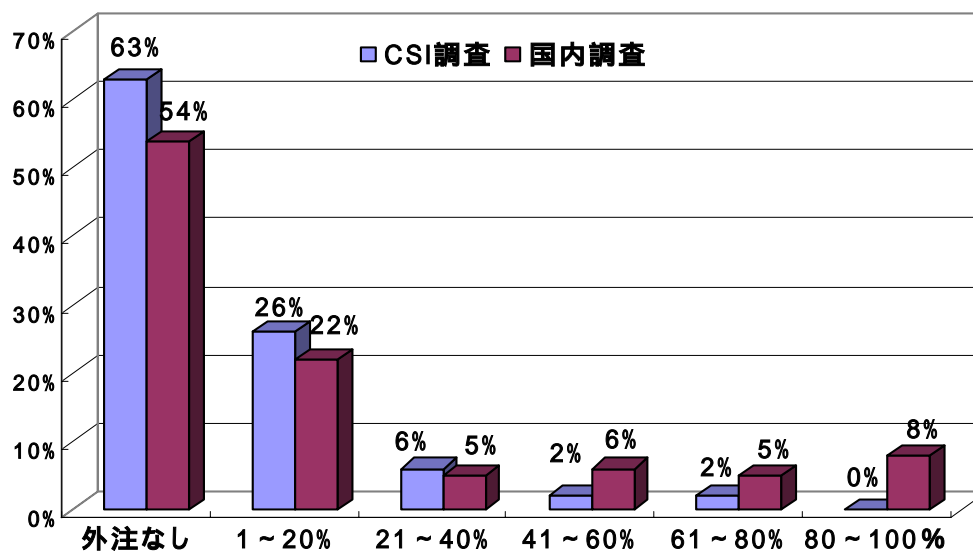
CSI 調査、国内調査ともに「外注なし」が多い。情報セキュリティのような重要なものを外注すべきでないとの考えもある。

ただ、総所得金額別の外注割合を見ると、CSI 調査では規模の大小に係わらず、あまり外注はしていないことが分かる。

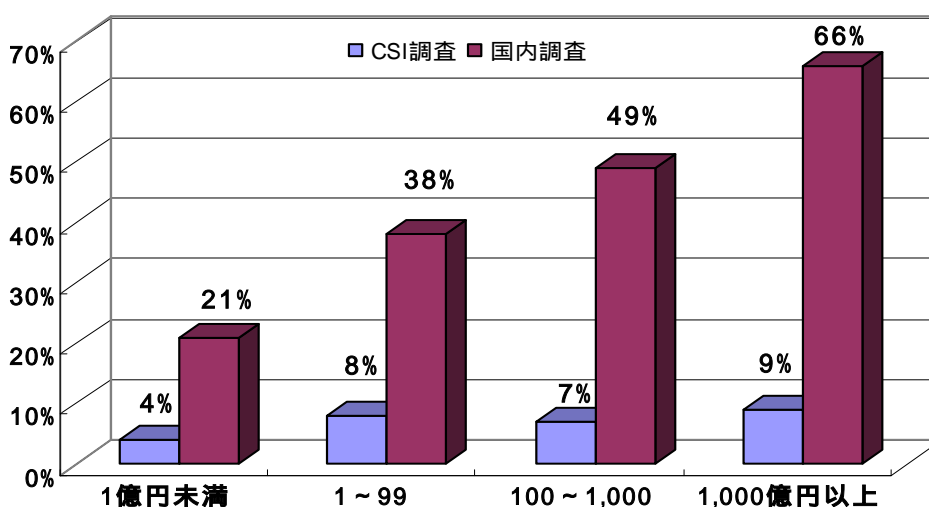
一方、国内調査では、規模が大きくなるにつれ、外注割合が増えており、総所得金額が1,000億円以上の企業・組織では、66%が外注していることがわかる。

### 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みた日米情報セキュリティ比較

国内では、企業規模が小さい程外注を行っていないことになるが、「外注すべきではない」と考えているのか、「外注の必要性がない」のかは不明である。この状況を推測してみると、企業規模が小さい程、ウェブでは情報発信等が中心であり、また、社内ネットワークの管理を外部に委託する必要がないためとも考えられる。今後の調査で確認をしたいと考えている。



情報セキュリティの外注割合 (回答数 CSI: 682 国内: 923 )



総所得金額別情報セキュリティの外注割合 (回答数 CSI: 682 国内: 923 )

#### (6) 情報セキュリティの利用技術

CSI 調査と国内調査では、普及率の高い上位3つはあまり相違がない。しかしながら、侵入検知システムや暗号化（送信中のデータの暗号化、ファイルの暗号化）や新しい概念の個人認証技術（ICカード、ワンタイムパスワード、PKI、バイオメトリックス）等については、国内調査では、CSIの半分程度の導入率にとどまっている。

国内では、本格的な情報セキュリティ対策はこれからであると考えているのか、あるいは、多くの企業ではそれ程の情報セキュリティ対策は不要な状況にあるとも考えられる。

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みた日米情報セキュリティ比較

	CSI 調査	国内調査
ワクチンソフト(Anti-Virus Software)	96%	94%
ファイアウォール(Firewall)	97%	91%
アクセス制御(Server-based access control lists)	70%	75%
侵入検知システム(Intrusion Detection System: IDS)	72%	21%
送信中のデータ暗号化(Encryption for data in transit)	68%	32%
一般的なパスワード(Reusable account/login passwords)	52%	83%
侵入防止システム(Intrusion Protection System: IPS)	35%	10%
ファイルの暗号化(Encryption files)	46%	27%
ICカード(Smart cards/other one-time password tokens)	42%	15%
ワンタイムパスワード		11%
PKI(Public Key Infrastructure)	35%	10%
バイOMETRICS(Biometrics)	15%	9%
その他	-	5%

情報セキュリティの利用技術 (回答数 CSI: 687 国内: 987 )

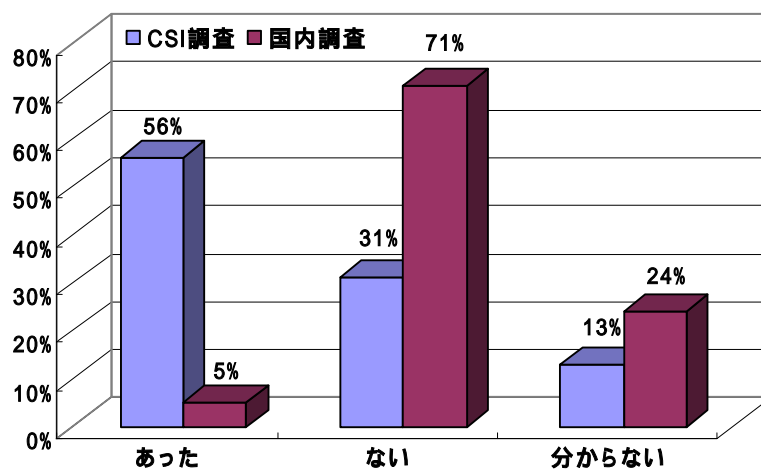
### 3.3 情報セキュリティインシデントについて

#### (1) 無権限者によるコンピュータ利用

顕著な相違がでている回答の1つで、CSI 調査では、56%が「あった」と回答しているのに対し、

国内調査では、「あった」は5%で、「ない」が71%となっている。

この理由は分からないが、最近の「情報暴露型ウイルス」等のように、情報漏洩に気づいていないケースもあり、国内では「ない」と単純に思っているだけではないかとの指摘もある。



無権限者によるコンピュータ利用 (回答数 CSI: 693 国内: 984 )

#### (2) 発生したセキュリティインシデント

CSI 調査では、ノート PC 等の盗難 75%、通信詐欺 48%、DoS 攻撃 48%、ウイルス感染 32%、情報への不正アクセス 32%等の順になっているが、国内調査では、ウイルス感染 67%、ノート PC 等の盗難 23%、インシデントは発生していない 23%、内部者のネットワークアクセス乱用 18%、DoS 攻撃 11%となっている。

CSI 調査では、「インシデントは発生していない」との回答はないが、国内では 23%がインシデントが発生していないと回答している。

ノート PC 等の盗難とウイルス感染は、CSI 調査と国内調査では、逆の近い形で現れている。米国ではオフィス内での盗難が多いことが、この結果に現れているように思われる。

国内では、ウイルス対策用のワクチンソフトの導入割合は表 3 - 1 2 に示すように、CSI 調査との



### 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みた日米情報セキュリティ比較

相違はあまりないが、ウイルス感染が70%近くあり、ワクチンソフトが導入されているが、導入後の維持管理、パターンファイルの更新や利用者への教育・周知等が正しく行われていない可能性が高い。

最近のワクチンソフトでは、パターンファイルの更新は自動的に行うことができる仕組みになっているが、自動更新処理を行わない設定にしているなどが考えられる。少し前に、ベンダーでのワクチンソフトのパターンファイルの作成が不適切であったため、利用者のパソコンが利用できないということが影響している可能性も否定できない。

	CSI 調査	国内調査
ウイルス感染(Virus)	32%	67%
内部者のネットワークアクセス乱用 (Insider Abuse of Net Access)	9%	18%
ノート PC 等の盗難(Laptop/Mobile Theft)	75%	23%
情報への不正アクセス(Unauthorized access to Information)	32%	5%
システム侵入(System Penetration)	10%	4%
DoS 攻撃(Denial of Service)	48%	11%
情報資産の盗難(Theft of Proprietary Info)	2%	2%
システム破壊(Sabotage)	7%	1%
金融詐欺(Financial Fraud)	14%	0%
通信詐欺(Telecom Fraud)	48%	0%
無線 LAN の無許可利用(Abuse of Wireless Network)	16%	3%
公開ウェブの悪用(Misuse of Public Web Application)	5%	0%
ウェブ改ざん(Web Site Defacement)	5%	3%
その他	-	2%
発生していない	-	23%

発生したセキュリティインシデント (回答数 CSI: 700 国内: 984 )

#### (3) セキュリティインシデント発生回数

過去1年間にセキュリティインシデントが発生した回数を聞いた。

「CSI 調査によると内部犯行が70～80%ある」という『都市伝説』がある。CSI 調査報告では、以前から内部犯行の割合の70%とか80%と言ったことはないと言っている。

今回の国内調査結果を見ている限りにおいて、内部犯行と外部犯行の割合は、5対4の割合になっており、国内調査もCSI 調査と大きな相違はないと言えるであろう。

		1～5回	6～10回	11～30回	31回以上	分からない	発生ゼロ
CSI 調査	内部	46%	7%	3%		44%	-
	外部	47%	10%	8%		35%	-
国内調査	内部	31%	3%	1%	1%	12%	52%
	外部	42%	4%	3%	1%	9%	41%

セキュリティインシデント年間発生回数 (回答数 CSI: 453 国内: 887 )

#### (4) ウェブサイトのセキュリティインシデント

### 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みた日米情報セキュリティ比較

CSI 調査では、10 回以上発生したとの回答が 95%であるが、国内では 1 から 5 回が 73%となっており、対照的な結果になった。

なお、国内調査では、回答者数（974 件）の内、92%（895 件）がウェブインシデントはなかったと回答している。一般的には、単なる情報発信しかしていない場合には、インシデントの発生はほとんどない。このことが理由になっている可能性もあるが、今回の調査では判断ができない。

	1～5 回	6～10 回	10 回以上
CSI 調査	2%	3%	95%
国内調査	73%	1%	6%

**ウェブサイトのセキュリティインシデント（回答数 CSI: 453 国内: 887）**

#### (5) セキュリティインシデントの費用

CSI 調査では、639 人の回答者が費用計算を行っており、費用総額は 1 億 3 千万ドル（130 億円）、国内調査では、インシデント発生があった内、216 人が費用計算を行っており、費用総額は、11 億 5,200 万円となっている。

CSI 調査では、ウイルス感染、不正アクセス、情報資産の盗難が大きいですが、国内調査では、ウイルス感染（5 億円）とノート PC 盗難（3.8 億円）が上位を占めているが、それ以外は、少なく

	CSI 調査		国内調査	
ウイルス感染	4,278,77	1	502,985	1
ノート PC 等の盗難	410,730	6	376,934	2
内部者のネットアクセス乱用	685,645	5	57,999	3
DoS 攻撃	731,073	4	25,813	4
情報資産の盗難	3,093,300	3	23,038	5
情報への不正アクセス	3,123,310	2	21,320	6
システム侵入	84,140	9	6,431	7
金融詐欺	256,500	7	5,000	8
ウェブ改ざん	11,500	13	3,859	9
通信詐欺	24,200	12	2,000	10
システム破壊	34,060	11	1,220	11
公開ウェブアプリケーションの悪用	222,750	8	1,210	12
無線 LAN の無許可利用	54,470	10	1,130	13
その他	-	-	123,116	-
<b>費用総額</b>	<b>13,010,454</b>		<b>1,152,054</b>	

単位：千円、100 円/ドルで換算

表 3-1 セキュリティインシデント費用（回答数 CSI: 639 国内: 216）

#### (6) 侵入後の対応

侵入が発覚した後どのような事を行ったかについての質問で、パッチを実行したことが最も高い割合を示している。事前にパッチを行っていない可能性が高く、事前にパッチを実行していれば侵入を避けることができたとも言える。

警察に届けたり、弁護士に相談することについては、国内調査では非常に少ないが、そのようなことをする程のものではなかった可能性もあるが、企業・組織内で対応することで外部に公表したくないとの考えもある。

**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みた日米情報セキュリティ比較**

	CSI 調査	国内調査
セキュリティパッチを実行した	73%	67%
外部へ報告しなかった	37%	16%
警察へ届けた	20%	8%
弁護士に相談した	12%	2%

**侵入後の対応（回答数 CSI: 320 国内: 230）**

(7) 侵入を警察等に届けなかった理由

CSI 調査でも、外部からのマイナスイメージを気にしているが、国内調査では圧倒的に多い。国内で発生した事件・事故後に経営者の対応をみていると、いわゆる「リスクコミュニケーション」対応ができていないことが大部分である。このため、事件・事故自体の問題よりは、事件・事故後の対応のまずさにより、経営トップの退陣を招くことが多い。このようなことが極端な対応を行う結果になっているのではないかと思われる。

	CSI 調査	国内調査
外部からマイナスイメージを持たれる恐れがあったため	43%	94%
競合他社に利用される恐れがあったため	33%	6%
社内対応で十分だと判断した	16%	0%
報告しようという考に至らなかった	16%	1%

**侵入を警察等に届けなかった理由（回答数 CSI: 423 国内: 241）**

4. 国内における課題

国内の調査は、今まで3回の調査を行ったが、事前に分かっていた課題もあるが、実際に行ってみて分かった課題もある。

4.1 調査上の課題

(1) 比較調査での課題

CSI 調査との整合性をもう少し取る必要があると考えており、CSI に対して申し入れをしているが、残念ながら目的を達成できていない。

比較調査の場合、対象期間等も含め可能な限り同一にできることが良いと考えている。

そこで、法制度等を考えると同一環境ではないこともあるため、各国共通の部分と調査国独自の調査項目を考えて調査票を作って調査ができればよい工夫を考えたい。

また、現在、CSI 調査を基にした調査は、オーストラリアが、2002年から実施しており、米国だけでなく、他の国を含めて比較することは考えてみたい。

(2) データの有効利用

調査データを色々な視点から分析することを考える必要があると感じている。現在は調査データを1つとして取り扱っているが、業種、規模等により分析を行うことも考えてみたい。

一部のCSI 調査データの数値が公表されていないため、正確な比較ができていない。

4.2 調査対象の課題

(1) データ収集について

国内調査の場合、本調査だけの問題ではないが、企業規模の大きい所からの回答が少ない。

CSI 調査では、従業員数が、「10,000~49,999人」で、112人、「50,000人以上」で、77人が回答している。一方、国内調査では、それぞれ、21人(2.1%)、2人(0.2%)でしかない。もう少し

### 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みた日米情報セキュリティ比較

増やす方法を考える必要があると考えている。

#### 5. 謝辞

本調査は、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」の研究として、調査を行っている。

また、調査を行うにあたり、多くの方々から回答を得ており、それらの方々のご協力にも厚くお礼申し上げます。