CSI（Computer Security Institute）は、サンフランシスコFBI（連邦捜査局）コンピューター侵入特捜班（Investigation's Computer Intrusion Squad）の協力を得て、毎年、コンピューター犯罪と情報セキュリティの調査「CSI/FBI Computer Crime & Security Survey」を行っている。2004年で9回目を迎えた。情報セキュリティ分野では最も長期に行われている調査と言える。

2002年からは、CSIのウェブ（http://www.gocsi.com/）に調査結果が公表されるようになった[1]が、それ以前は、ウェブで公開されるのはニュースリリースのみであったため、詳細な調査結果はCSIのメンバーか、CSIが毎年主催する6月のNetsecか11月のAnnual Conferenceに参加しないと入手できなかった。このため多くの誤った引用が行われてきたのである。

典型的な誤用は、「CSI／FBIの調査資料によると、70～80％は内部犯行である」という内部犯罪と外部犯罪の割合である。

以前にも述べた[2]が、2001年、2002年の調査報告書には、そのようなことを言った覚えはない旨、記述されていた。

この調査の特徴は、大部分の調査項目が初回から一貫して変わっていない点にある。このため、多くの調査項目について、過去から現在までの変化を読み取ることができる。従って、コンピューターウイルス被害やコンピューター犯罪等や、ユーザーが利用している情報セキュリティ機器・ソフトウエア等がどのように変化してきたのかが、はっきり分かる。

今回は、従来の質問に加えて左記に示す通り、新たに発生している問題についても調査を行っている。

（1）セキュリティ投資の効果測定の方法
（2）IT予算のうち、セキュリティへの投入割合
（3）セキュリティ教育関連

2004 CSI/FBI Computer Crime & Security Survey[1]

米国のコンピューター犯罪とサイバーセキュリティ

『注目の“2004CSI/FBI調査”を読む』

今年の調査結果（2004 CSI/FBI Computer Crime & Security Survey）は、何を物語っているか。

金融（Financial）	19%	州政府（State Gov.）	3%	合計　101% （回答者数＝486）
ハイテク産業（High-Tech）	13%	小売（Retail）	3%	
製造業（Manufacturing）	12%	地方政府（Local Gov.）	3%	
連邦政府（Federal Gov.）	7%	通信（Telecom）	2%	
教育（Education）	7%	法律（Legal）	1%	
医療（Medical）	6%	運輸業（Transportation）	1%	
電気・ガス（Utilities）	5%	その他（Other）	19%	

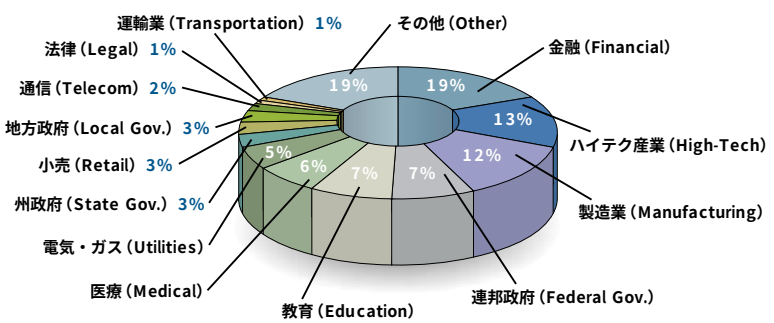

図1　回答企業・組織の業種　回答者数＝486（回答者数は筆者が割合から逆算したもの。以下も同様）

(4) セキュリティ費用
(5) セキュリティに関するアウトソーシング
(6) SOX法のセキュリティへの影響
(7) セキュリティ監査と保険の活用

回答者494人のプロフィール

今年の調査では、最大で494人が回答している。回答者のプロフィールは以下の通りである。

(1) 回答者が所属している業種では、金融関係が19%で最も多く、ハイテク産業の13%、製造業の12%が続いている。政府・自治体は合計で13%を占め、連邦政府、州政府、地方政府が各々、7%、3%、3%となっている(図1)。

1~99人	19%
100~499人	15%
500~1,499人	13%
1,500~9,999人	31%
10,000~49,999人	14%
50,000人以上	7%
合計(回答者数=491)	99%

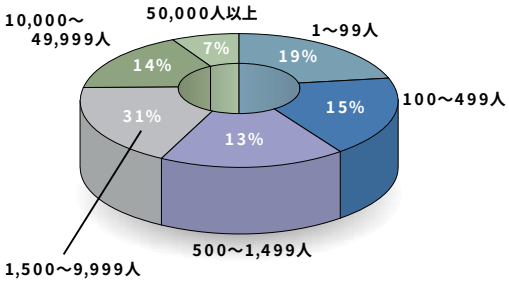

図2 回答企業・組織の従業員数 回答者数=491

内田勝也

情報セキュリティ大学院大学助教授／中央大学研究開発機構助教授／
日本セキュリティ・マネジメント学会理事
uchidak@gol.com

電気通信大学経営工学科卒。オフコンディーラーでシステム開発・ユーザー支援等、在日外国銀行でシステム監査等、大手損害保険会社にてコンピューター包括保険開発・情報セキュリティ調査研究等に従事。コンピューターウイルス、ネットワーク犯罪、情報セキュリティ分野の最新技術や政策に関するさまざまな論文を発表。

KATSUYA UCHIDA

(2) 回答者の所属する企業・組織の従業員数では、1500~9999人が最も多い31%で、次に1~99人が19%と続いている。

1500人以上の従業員を擁する組織に所属している回答者が合計で52%あり、日本国内等での情報セキュリティ調査と比較しても、CSI/FBI調査は大企業中心になっていると言える(図2)。

(3) 回答企業・組織の総収入は、37%が10億ドル(110円/ドルで、1100億円)以上で、1000万~9900万ドルが23%と続いている。1億ドル(110億円)以上が57%を占め、ここでも比較的規模の大きな企業・組織が回答者の中心になっていることが分かる(図3)。

総収入	回答者数	%
1,000万ドル未満	78	20%
~9,900万ドル	91	23%
~10億ドル	78	20%
10億ドル以上	145	37%
合計	392	

図3 回答企業・組織の総収入 回答者数=392

(4) 今回初めて、回答者の役職を聞いている。当然ながら、情報システムや情報セキュリティ関係の回答者が多い(図4)。

Security関係のOfficer/Manager/Directorが半数以上の53%を占める。役員クラスも全体で18%となっており、内訳はCSO(Chief Security Officer)6%、CIO(Chief Information Officer)8%、

CEO	4%
CIO	8%
CSO	6%
Security Officer/Manager/Director	53%
System Administrator	9%
Other	19%

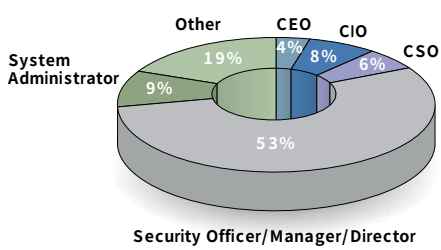

図4 回答者の役職 回答者数=489

CEO(Chief Executive Officer)4％である。また、システム管理者(System Administrator)が9％いる。

情報セキュリティ予算について初めて調査

セキュリティの重要性が高まってきていたことを受けて、今回初めて、情報セキュリティ予算等に関連する質問を行っている。

(1)図5は、情報システム(IT)予算に対して情報セキュリティの予算の割合を聞いた結果である。1～5％(1～2％が24％、3～5％が22％)で全体の46％を占めており、1％以下が16％と続いている。

(2)図6は、情報セキュリティ予算を業務運営費と投資金額に分けて、企業規模(総収入)別にどの程度であるかを聞いたものである。

一般的に言えば、規模が大きくなる程1人当たりの予算は少なくなる。これは全従業員がコンピューターを利用していないためと考えられる。

総収入が1000万ドル未満では、従業員1人当たり約500ドル(業務運営費＝334ドル、投資金額＝163ドル)で、10億ドル以上では、1

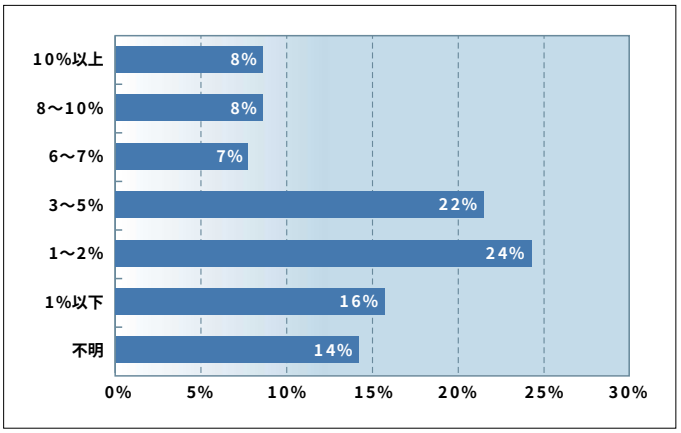

図5　IT予算に対する情報セキュリティ予算割合　回答者数＝481

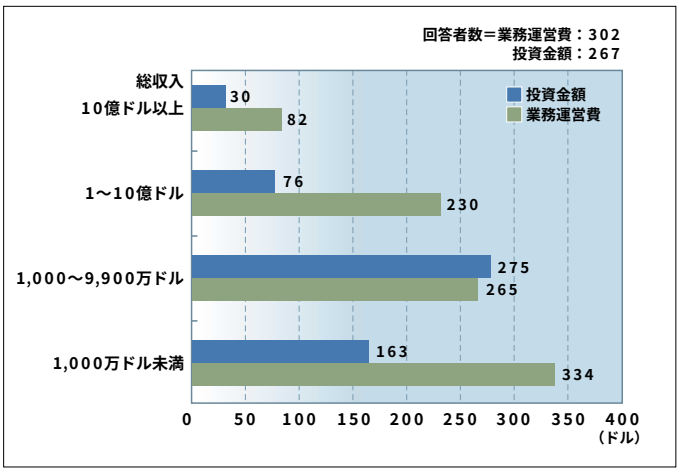

図6　従業員1人当たりの情報セキュリティ業務運営費、投資金額の総収入別金額

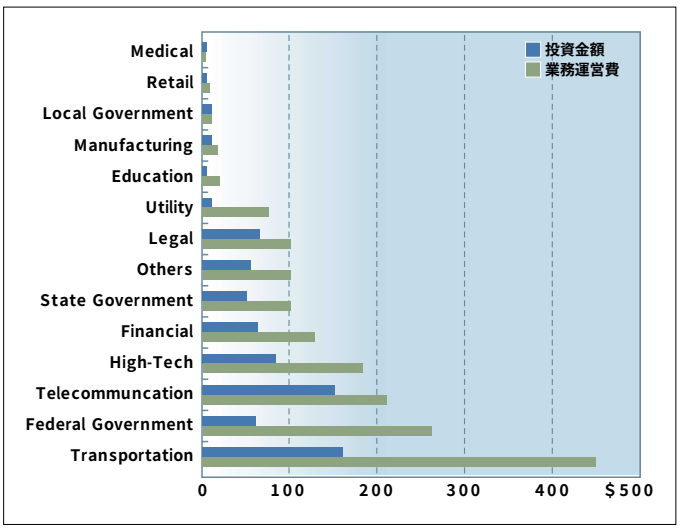

図7　従業員1人当たりの情報セキュリティ業務運営費、投資金額の業態別金額

12ドル(業務運営費＝82ドル、投資金額＝30ドル)となっている。

(3)業種別に従業員1人当たりの業務運営費及び投資金額を調べた結果が図7である。

従業員1人当たりで最も大きい金額を費やしているのは「運輸業」で、総額が608ドル、内訳は、業務運営費449ドル、投資金額159ドルとなっている。次いで多いのは連邦政府で、総額322ドル、内訳は、業務運営費が261ドル、投資金額が61ドルという結果である。

1人当たりの業務運営費は、運輸業が449ドルで最も多く、連邦政府261ドル、通信209ドル、ハイテク産業183ドルと続いている。

1人当たりの投資金額は、運輸業159ドル、通信150ドル、ハイテク産業83ドルの順である。

なお、この部分は原図の図7と本文の説明で業務運営費と投資金額とが逆になっていたが、前項(2)を考慮すると、本文が正しく、原図の図7が誤っているものと思われる(左の図は投資金額、業務運営費を入れ替えてある)。CSIへ確認をした結果、11月のコンファレンスのプレゼンテーションに参加して、話をすることになった。

(4)情報セキュリティ予算の投資効果について、評価基準を使っているか否かを聞いた結果が図8である。

米国でも当然ながら、情報セキュリティへの投資効果が求められており、いろいろな所で投資効果の議論がされている。そのような背景から、今回初めてこの種の質問を行ったと思われる。

所属企業が情報セキュリティ費用に対する費用対効果を定量化する際、ROI(注1)、NPV(注2)、IRR(注3)は適切であるかどうかを聞いている。質問に対して七つの回答から選択する。1～3は適切でない、4はどちらでもない、5～7は適切であると認めたもので、55％がROI、28％がIRR、25％がNPVを利用していると答えた。

意外と少ないアウトソースと保険対応

今回の調査では更に、情報セキュリティリスク管理への対応として、アウトソースと保険について質問している(図9)。

(1)セキュリティ業務のアウトソースについての回答は、一般的な推測とかなり異なっていた。

つまり、組織の情報セキュリティ業務の41％以上をアウトソースしていると回答したのは、わずかに7％であった(元資料の本文では、「20％以上をアウトソースしているという回答」と述べているが、図9からは41％以上の合計が7％となっているので、本稿は図9を基にした)。

更に、63％は情報セキュリティ機能をアウトソースしていないと回答している。

(2)情報セキュリティリスク管理のために、保険を利用しているかどうかを聞いているが、回答者の28％が利用していると回答している(図10)。

パスワード、生体認証、アンチウイルスソフト、侵入検知システムなどで技術的な情報セキュリティ対策を行っていても、完全にセキュリティ侵害をなくすことは不可能で、財務上の損失を防ぐことができない。このような現状を考えると、技術的な対応でカバーできない部分を保険でカバーすることも考える必要があるが、保険を掛けていると回答した者は28％しかいなかった。

情報セキュリティリスクがゼロにならないことを考えれば、28％の値は少ないと言えないだろうか。ただし、情報セキュリティに関しての保険数理上のデータが十分でないために、保険会社の情報セキュリティ保険の設計が適切でないことが保険利用に影響しているとも考えられる。

ROI	55%
NPV	25%
IRR	28%

図8　組織で利用している投資評価基準(ROI、NPV、IRR)の割合
回答者数=320

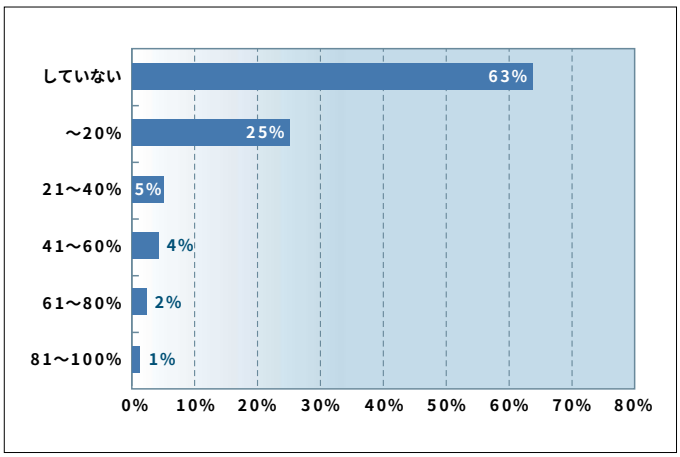

図9　セキュリティ機能をアウトソースしている割合　回答者数=478

保険を掛けている	28%
保険を掛けていない	72%

図10　情報セキュリティリスク管理のために保険を掛けているか

変貌するセキュリティ侵害のかたち

(1)図11は、成功した無権限アクセスを表したものである。

今回は、無権限アクセスがあったと53％が回答しているが、調査開始時の1996年から2000年までの増加傾向が、2001年から減少に転じており、その傾向は今年も続いている。

無権限アクセスを経験しないと回答した割合も、同じ傾向にある。

(2)図12は、インシデントの回数である。全体、外部、内部に分けて、その割合を示している。

インシデントの経験は1～5回が47％で、経験した組織の約半数になり、6～10回も20％ある。

(3)図13は、過去にどのような種類の攻撃や誤使用があったかを聞いた結果である。

	有り	無し	不明	回答者数
2004年	53	35	11	481
2003年	56	29	15	524
2002年	60	27	12	481
2001年	64	25	11	532
2000年	70	16	12	585
1999年	62	17	21	512
1998年	64	18	18	515
1997年	50	33	19	391
1996年	42	37	21	410

図11　コンピューターシステムへの無権限アクセスの有無

コンピューターウイルス被害を受けたという回答は78％で最も多く、次いで内部者によるネットアクセスの乱用が59％、ノートPCの盗難が49％と続いている。

全体的には漸減傾向にあるが、特に、内部者のネットアクセスの乱用、システム侵入、情報の窃盗は激減している。

今年から新たに追加された3項目については、ワイヤレスネットワークの乱用が15％、ウェブ改ざんが7％、ウェブアプリケーションの誤使用が10％であった。

(4)図14は、ウェブサイトでのインシデントを経験した回数で、大部分(89％)は、1～5回で、10回以上のインシデントに遭った回答者は5％となっている。

全体の回答者数は494人であるので、回答者全体での割合は、10回以上が1％、6～10回が2％、1～5回が24％に相当し、インシデントがなかった所が73％と推測される。

(5)図15は、インシデント種類ごとに回答者単位の損失金額を推計したものである。

合計損失金額は1億4150万ドルで、2003年の2億180万ドルに比べて減少している。

これは494人の回答者の内、269人が推計したものである。

過去5年間、情報資産の盗難が最大損害金額であったが、今回、DoS(サービス妨害)攻撃が初めて最大の損失金額を記録した。この原因として、昨年のコンピューターウイルスのDoS攻撃が影響していたことが考えられる。例えば、MyDoomワームの変種は、時刻で発病するDoS攻撃の機能を持っていた。

多岐にわたるセキュリティ技術の利用

(1)図16は、利用しているセキュリティ技術への回答である。

今年はいくつかを追加したり、削除したりしたため、厳密な意味では前年までと同じではない。

アンチウイルスソフトは全体の99％が導入しており、ファイアウォールも98％が導入していた。

一方、サーバーのアクセス管理リストは71％、侵入検知が68％、移動中のデータの暗号化が64％などとなっている。

個人認証では、固定(Reusable)パスワードが56％、

インシデント回数(全体)	1～5	6～10	10以上	不明
2004	47	20	12	22
2003	38	20	16	26
2002	42	20	15	23
2001	33	24	11	31
2000	33	23	13	31
1999	34	22	14	29
インシデント回数(外部から)	**1～5**	**6～10**	**10以上**	**不明**
2004	52	9	9	30
2003	46	10	13	31
2002	49	14	9	27
2001	41	14	7	39
2000	39	11	8	42
1999	43	8	9	39
インシデント回数(内部から)	**1～5**	**6～10**	**10以上**	**不明**
2004	52	6	8	34
2003	45	11	12	33
2002	42	13	9	35
2001	40	12	7	41
2000	38	16	9	37
1999	37	16	12	35

図12　インシデント発生回数(全体・外部・内部)　2004年の回答者数=280

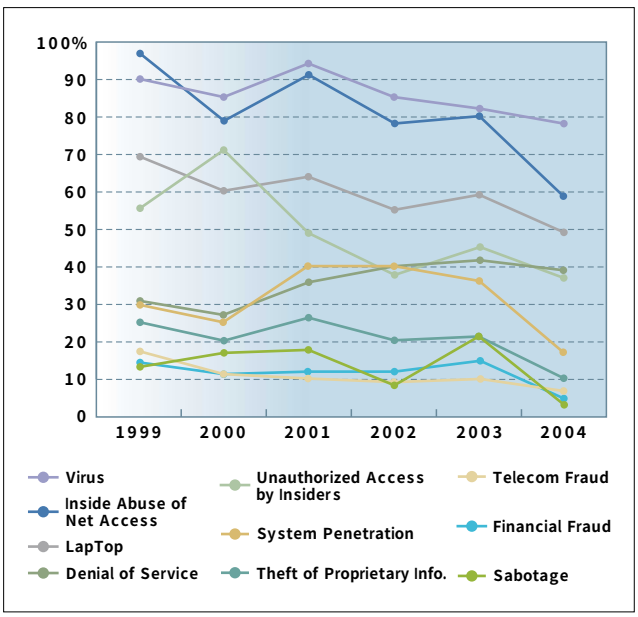

図13　成功した攻撃種類や誤使用の割合

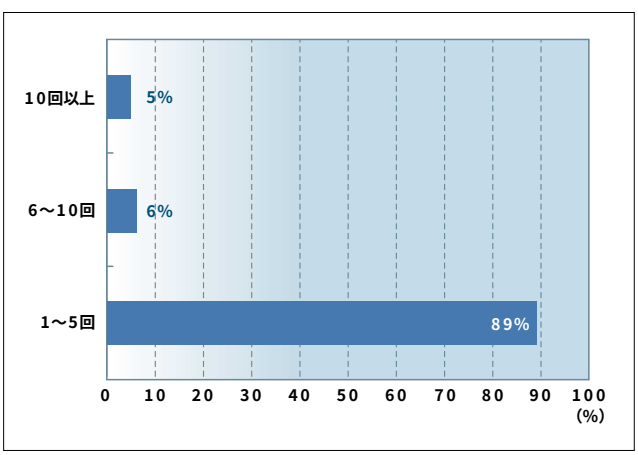

図14　ウェブサイトでのインシデント　回答者数=132

ICカードやワンタイムパスワードが35％、PKIシステムが30％、生体認証システムが11％、それぞれ導入されている。

進むセキュリティ監査、予算不足のセキュリティ周知研修

(1)セキュリティを推進する観点から新しい調査項目を追加している。図17はセキュリティ監査を実施しているか否かを聞いた結果だが、82％が実施していると回答した。

(2)セキュリティ研修についての質問は、図18の「セキュリティ周知に適切な金額を投資しているか」というもので、回答者に7段階で評価をしてもらっているが、すべてが十分満足いく金額が投資されていないと回答している。

(3)図19は、セキュリティ周知研修で、どのセキュリティ分野が最も重要であると思うか、結果を示したものである。

セキュリティポリシーとネットワークセキュリティが70％で最も重要とされ、次いで、アクセス制御システムが64％、セキュリティマネジメントが63％、セキュリティの経済面が51％となっている。

進展が見られない情報共有

最近は、国家安全保障省やコンピューターセキュリティコミュニティのリーダーが情報共有を推進しているが、このCSI／FBI調査ではセキュリティ侵入についての情報共有は特に進展しているようには見えない。

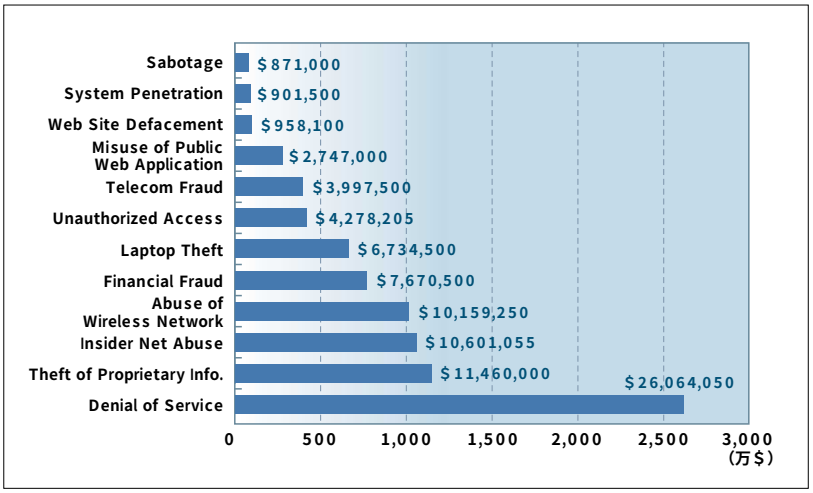

図15　侵入種類別の損失金額　回答者数=269

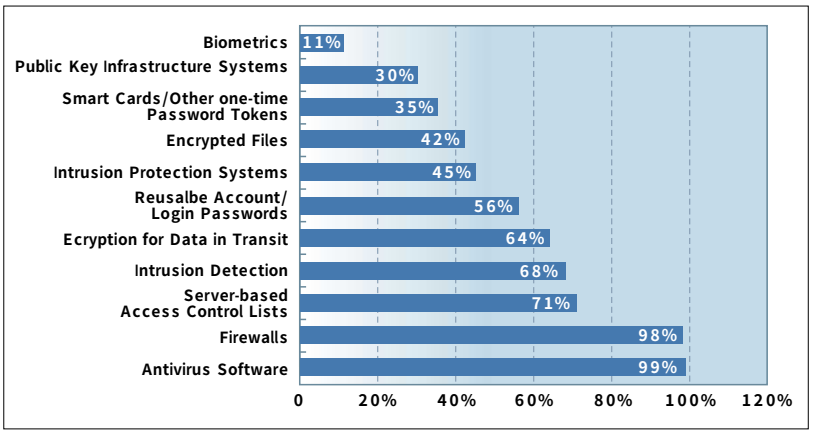

図16　利用しているセキュリティ技術　回答者数=483

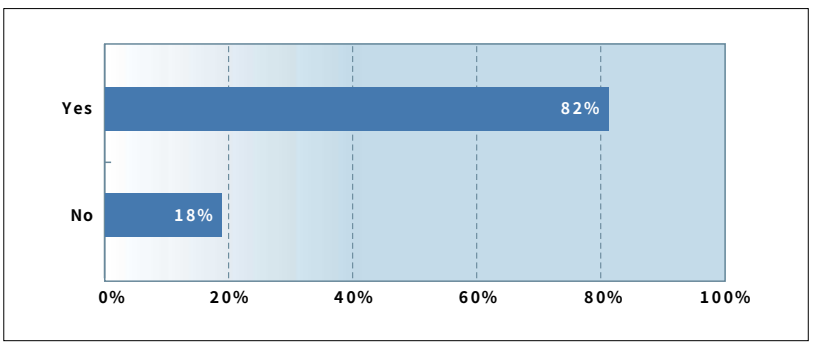

図17　セキュリティ監査の実施状況　回答者数=470

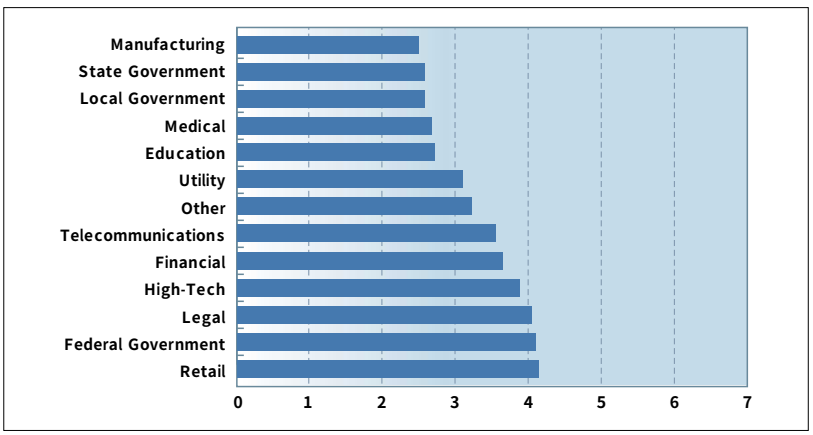

図18　セキュリティ教育に適切な費用を払っているか。7段階評価　回答者数=488

(1)図20は、セキュリティ侵入を経験した時に、何を行ったかを示したものである。

(2)図21は、組織が報告を行わない理由を回答したものである。意外にも18%が、法執行機関が関心を持っていると思わなかったと回答している。コンピューターシステムへの侵入を犯罪と認識していないのか、あるいは大した犯罪でないという判断が働いたのかもしれない。

(3)図22は、情報共有のために企業・組織が所属している団体を調査した結果である。この調査も今回新たに加わった。

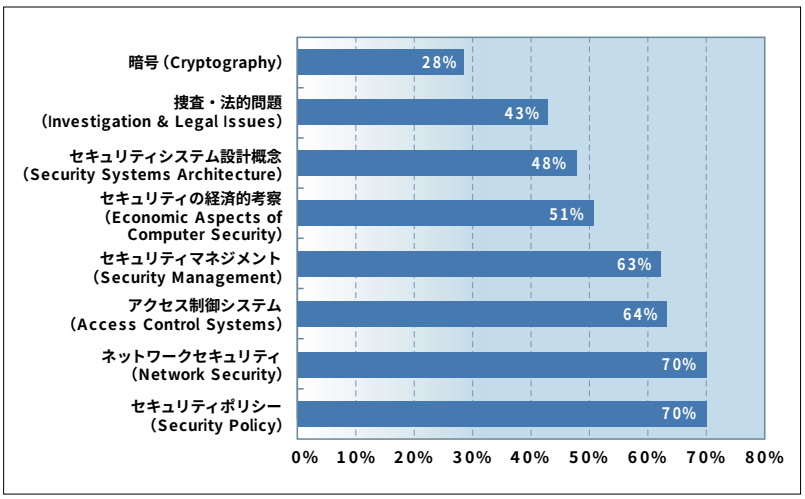

図19　セキュリティ周知教育で何が最も重要と思うか　回答者数=480

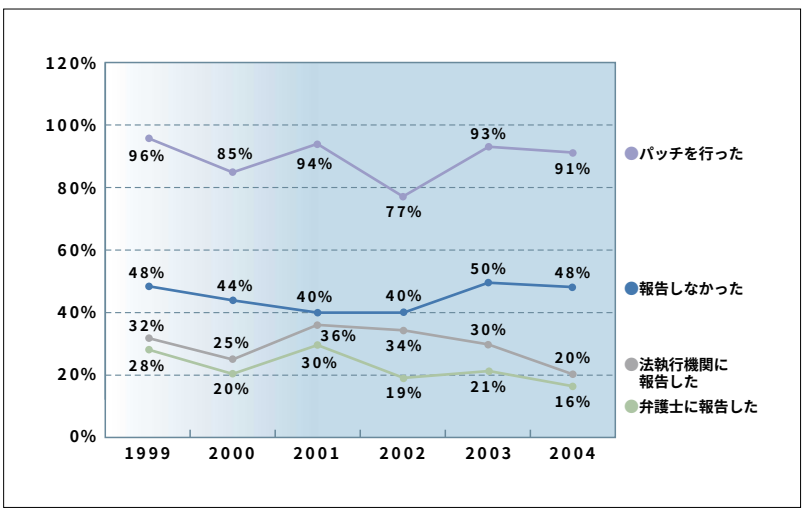

図20　セキュリティ侵入があった場合、次に何を行ったか

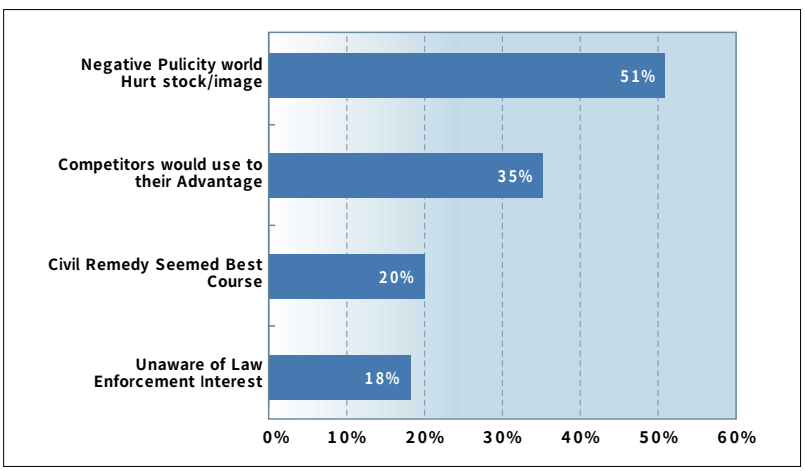

図21　法執行機関に報告しなかった理由　回答者数=267

Sarbanes-Oxley法の影響

エンロン、ワールドコムなどにおける企業統治、会計事務所の独立性、証券会社の利益相反などの問題が顕在化したことを受けて、米国では2002年7月にサーベインス・オクスレー(Sarbanes-Oxley)法(企業改革法、SOX法)が成立した。

このSOX法によって、経営者は内部統制に対する大きな責任を負い、違反すれば刑事責任を負うことになる。

図23は、このSOX法の影響について、①SOX法が情報技術から企業統治へ重点を移したか、②SOX法が情報セキュリティへの関心を高めたか、という2点の回答を求めた結果である。

金融機関、電気・ガス、通信業界では②が50%以上を占めている。通信、製造、電気・ガス業界では、①が40~50%程度となっている。

重視される管理面からのセキュリティ対応

1990年の中頃から出現したインターネットの普及に伴い、コンピューターセキュリティも次第に変化してきた。

当初は技術面、暗号、アクセス制御、侵入検知セキュリティなどに関心が集まっていたが、最近は、経済、財務、リスク管理などの観点についても重要であるという認識が高まってきた。ただし、管理面での対応は技術を代替するものではなく、補完するものであろう。

難しくなる「過去」、「各国」との比較

CSI/FBI Computer Crime and Security Surveyは今年で9年目を迎えたが、今回は質問項目を大きく変えた。その理由としては、情報セキュリティ分野も大きく変化してきており、技術から情報セキュリティ投資効果やSOX法に代表される企業・組織内部統制の問題も考えざるを得ないほど、情報セキュリティの重要性が高まってきたからと推測できる。

ただし、項目が過去の質問と異なるため、すべての質問について過去との比較ができない項目も出てきてしまった点は残念である。また、SOX法の影響調査などは、厳密には米国だけの問題ではないと言えるだろうが、日本を始め、豪州、韓国など、他の国々が行っている同様のセキュリティ調査とも比較ができない。

そこで、我が国ならば、SOX法の影響の代わりに「個人情報保護法」による影響を調べてみるのも面白いのではないかと思っている。

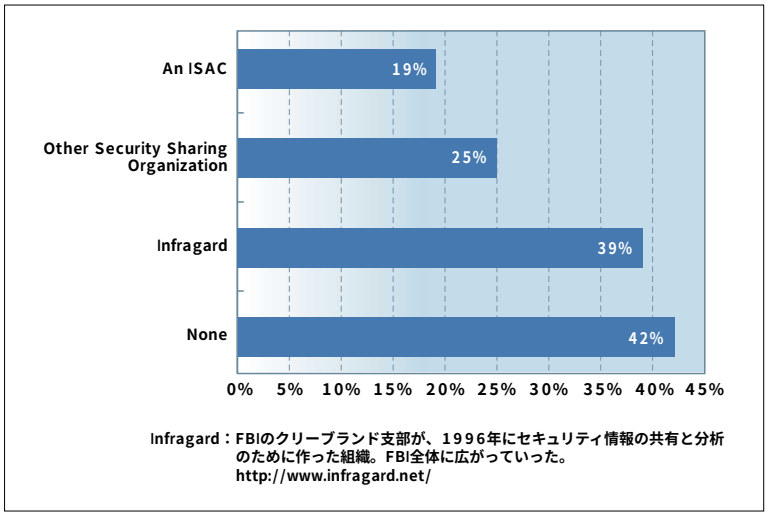

図22　情報共有組織への参加割合　回答者数= 445

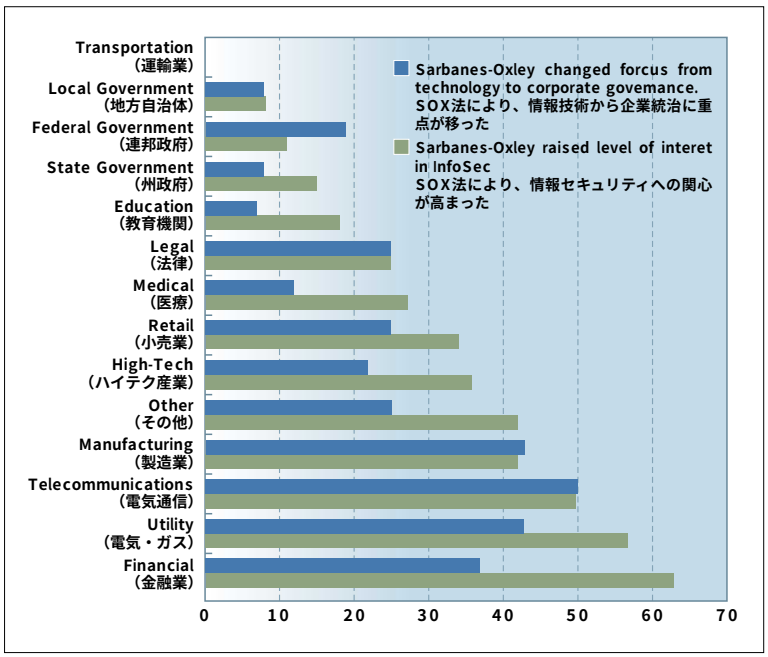

図23　情報セキュリティへのSOX法の影響　回答者数= 464

（注1）ROI（Return On Investment）　投下資本利益率。投下資本が生みだす利益を測定する方法で、会計上は、

投下資本利益率＝（経常利益＋支払利息）／（株主資本＋有利子負債）　と表されるが、簡略化して、

投下資本利益率＝利益／投下資本　と計算することもある。投下資本には初期投資だけでなく、運用経費も含めて考える必要もある。

（注2）NPV（Net Present Value）　正味現在価値。将来時点の利益を現在の時点に換算した値と投下資本の現在価値を比較したもの。

（注3）IRR（Internal Rate of Return）　内部利益率。将来のキャッシュフローを現在の時点に換算した値と投下資本の現在価値を比較したもの。

参考文献

[1] 2004 CSI/FBI Computer Crime & Security Survey
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf
[2] 内田勝也「CSI/FBI Computer Crime & Security Surveyを読む」、CYBER SECURITY MANAGEMENT、2004年3月号