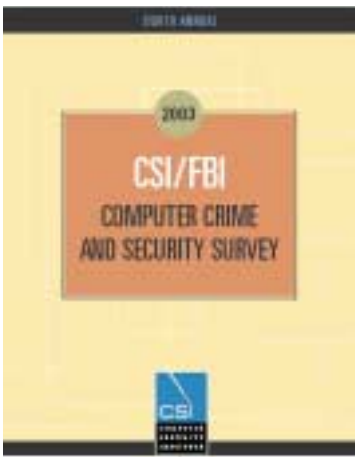
『CSI/FBI Computer Crime and Security Survey』を読む

CSI／FBIの調査資料は、情報セキュリティの参考文献として最も注目され、引用もされているが、疑問点が多く、誤解や誤用も少なくない。

CSM2004年1月号で報告した通り、昨年11月に開催された「30th CSI Annual Computer Security Conference & Exhibition」で、初めて「CSI/FBI Computer Crime & Security Survey」のセッションが設けられた。これに参加したお陰で、今まで感じていた疑問がいくつか解消された。



現時点での最新版「2003 CSI/FBI Computer Crime & Security Survey」の表紙

一方、国内に同調査と比較できるような同様の資料がないことから、中央大学「21世紀COE」では、研究の一環として、昨年末に国内でほぼ同一の内容の調査票を配布し、回収した。現在、その分析を行っている。

これらのことから、今回はCSI／FBI調査に焦点を当ててみる。

現時点での最新版は、2003年の調査資料である。今年（2004年）の調査結果は4月末頃にCSI（Computer Security Institute<http://www.gocsi.com/>）のウェブからダウンロードできると思われるので、それも参考にして頂ければ幸いである。

なお、2003年版、2002年版などと記されているが、これらは報告書が発表された年を示しており、調査はその前年を対象にしている。

アンケートの送付先は？

アンケートは3500～5000人に送られているが、無差別に送付されるのでなく、セキュリティの専門家の自薦になっている。しかしCSIでは、回答が片寄っているとは考えておらず、むしろ、回答者のセキュリティ経験は豊富で、所属組織のセキュリティ体制は優れているとしている。

従業員が1000人以上いる組織に属している回答者は2003年では59％であり（図1）、総収入も1億ドル（約110億円）以上が約60％あり、比較的大きな企業に属している人たちが回答していることがうかがえる（図2）。

また、調査報告書は、「回答者はCSI等のセキュリティ専門団体に所属していない人たちよりも、セキュリティ事件・事故やコンピューター犯罪に対して、十分な注意を払っており、何とか防止しようとしているように思われる」とも述べている。

内田勝也【うちだ・かつや】
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 常任理事
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。

回答者の所属組織はまちまちであり、2003年版の回答者の所属は表1のようになっている。

利用セキュリティ技術は？

組織を保護するために利用しているセキュリティ技術についての調査がある（図3）。

利用技術項目としては、次のものから複数を選択するようになっている。

①デジタルID（Digital IDs）
②侵入検知（Intrusion Detection）
③PCMCIAカード（PCMCIA）
④物理的セキュリティ（Physical Security）
⑤暗号化ログイン（Encrypted Login）
⑥ファイアウォール（Firewalls）
⑦再利用可能ユーザーID（Reusable Passwords）
⑧アンチ・ウイルスソフト（Anti-virus Software）
⑨暗号化ファイル（Encrypted Files）
⑩生体認証（Biometrics）
⑪アクセス制御（Access control）

この中の多くについては、特に説明の必要はないと思われるが、①Digital IDsは、公開鍵基盤（PKI=Public Key Infrastructure）システムと考えて良いだろう。ネットワークにおける安全性・信頼性を確保するための「基盤」といえる。

③PCMCIAカードには、秘匿と署名の機能を提供するものとしてFORTEZZAと呼ばれる米国政府標準がある(注1)。マイクロソフト社のIISでもサポートされており、主に米国政府内で利用されている。なお、FORTEZZAの詳細は「http://www.nstissc.gov/Assets/pdf/nstissi3028.pdf」にある。

国内ではこれを利用しているケースはほとんどないと思われるが、最近、USBポートを利用したメモリーにセキュリティ機能を搭載できるようなもの(注2)が発売されており、機能的にはこのPCMCIAカードに近いかもしれない。

⑦Reusable Passwordsとは、通常利用されているユーザーID／パスワードシステムのことである。

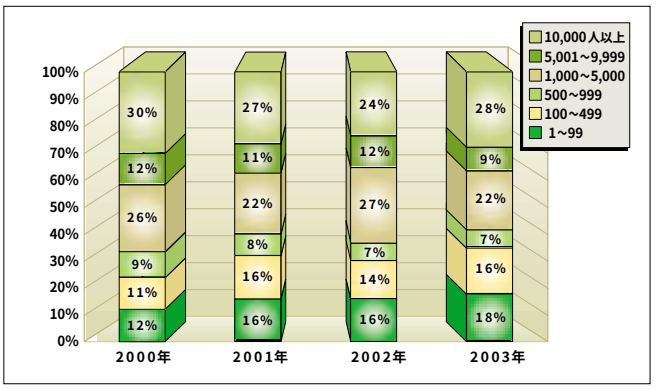


図1　回答者の所属組織の従業員数

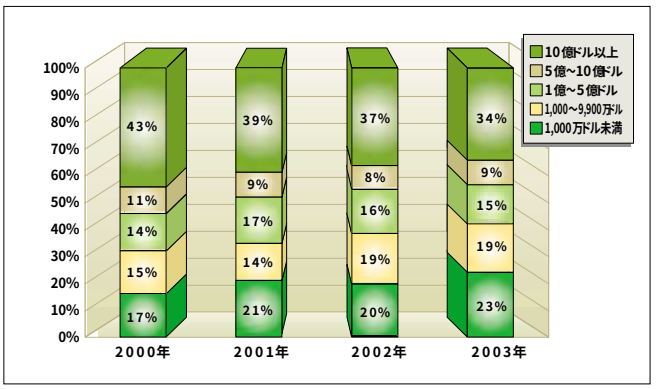


図2　回答者の所属組織の総収入

表1　回答者の所属組織

業種	割合（%）	回答数
ハイテク（High-Tech）	17	90
金融業（Financial）	15	79
製造業（Manufacturing）	11	58
医療・病院（Medical）	8	42
連邦政府（Fedral Gov.）	7	37
教育機関（Education）	5	26
州政府（State Gov.）	5	26
公益サービス（Utility）	4	21
通信（Telecom）	4	21
小売（Retail）	3	15
地方政府（State Gov.）	3	15
法律事務所（Legal）	1	5
運輸（Transportation）	1	5
その他（Others）	17	90
合計		530

（注）丸め誤差のため、割合%は101%になる。また、各業種の回答数は割合を基に計算。

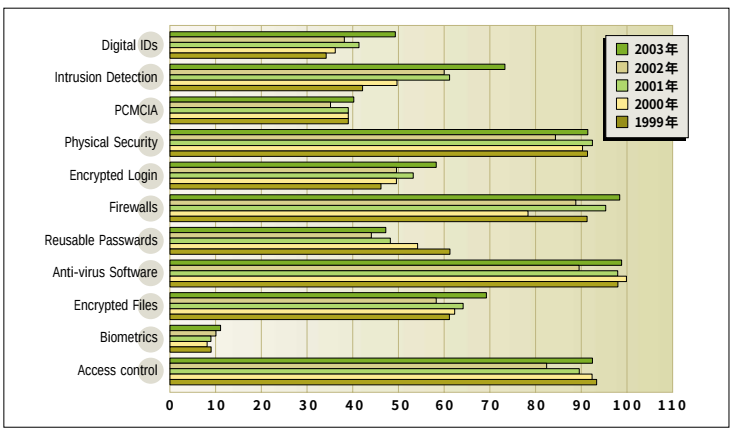


図3　利用している技術について

攻撃や誤使用については？

具体的には、いかなる攻撃を受け、また従業員がどのように使用を誤ったか（誤使用）についての質問がある。

攻撃・誤使用の項目として、以下のものから複数を選択するようになっている。

①サービス妨害（Denial of Service）
②ノートPC盗難（Laptop）
③通信傍受（Active Wiretap）
④通信詐欺（Telecom Fraud）
⑤内部者による無権限アクセス（Unauthorized Access by Insider）
⑥コンピューターウイルス（Virus）
⑦金融詐欺（Financial Fraud）
⑧内部者によるアクセス乱用（Insider Abuse of Net Access）
⑨システム侵入（System Penetration）
⑩盗聴（Telecom Eavesdropping）
⑪サーバー上のデータ破壊（Sabotage）
⑫情報資産の盗難・漏えい（Theft of Proprietary Information）

このうち、③通信傍受（Active Wiretap）と⑩盗聴（Telecom Eavesdropping）の相違はあまり明確ではないようで、11月のセッション参加時に質問してみたが、明確な回答は得られなかった。ただ、⑩盗聴の場合には、ネットワーク上を流れる情報を盗聴する行為として良いと考えている。

④通信詐欺（Telecom Fraud）としては、次のような場合が考えられる。例えば、グローバルな企業では、社内の電話回線として国際間の回線を持っており、長距離の国内や国際電話を掛けるときに、外出先や自宅から社内の特別な電話番号に掛け、そこから相手先の近くまで社内回線を利用して、電話を掛けることがあるが、この回線を悪用することが挙げられる。また、通信サービス費用を他人（組織）のクレジットカードや電話等に請求させてしまうことなども考えられる。

⑤内部者による無権限アクセス（Unauthorized Access by Insider）は、権限を持っていない内部者が、他の内部者のユーザーID、パスワードを盗用したり、推測することによって、権限のないデータベースやコンピューターを利用するものである。

⑧内部者によるアクセス乱用（Insider Abuse of Net Access）は、ポルノ画像のダウンロード、プログラム等の違法コピー、私用メール利用等といった組織のセキュリティポリシー違反に該当することを行うことである。2003年版にはないが、2002年版などでは、「Downloading pornography or pirated software, or inappropriate use of e-mail systems」と書いてある。

80%は内部犯行説？　CSI/FBI調査資料は、すでに1997年版から否定し続けている（写真と本文は関係ありません）

80%は内部犯行？

今でも時々、CSI／FBI調査資料に「情報セキュリティ犯罪の80%は内部犯行」とあると指摘する人もいるが、すでに1997年版で「社会通念としていわれている『情報セキュリティ問題の80%は内部犯行である』というのは、もはや真実ではない」（These responses indicate the "conventional wisdom" that "80% of information security problems are internal "is no longer true）と述べている。また、「内部からの脅威が減少したのでなく、インターネットの利用により、外部からの脅威が劇的に増加していることによるものである」とも述べている。

内部・外部犯行に関する質問項目としては、以下のようなものがある。

①事件・事故（インシデント）の全体件数、外部犯行件数、内部犯行件数
②攻撃場所（内部システム、リモートダイアルイン、インターネット）は？
③誰が攻撃者と思うのか？

①の内容を表2、表3、表4に示す。

②攻撃場所（内部システム、リモートダイアルイン、インターネット）は、図4の通りである。

③「誰が攻撃者と思うか」は、図5の通りである。80％内部犯行説については、よほど気になっていると思われる。なぜなら、2000年版では、Bob Dylanのアウトロー・ブルースの歌詞を引用して(資料1)、2001年版でもガリレオの名前を出して(資料2)、80％内部犯行説を否定しているからである。

コンピューター犯罪被害の費用が大き過ぎないか？

コンピューター犯罪被害の費用を表示している(表5)。国内等での調査と比べて金額が大き過ぎるという批判を聞くこともある。しかし、内容を見ると、最低費用、最高費用、平均費用、合計の年間損失費用が示されている。

表5は、コンピューター犯罪やセキュリティ侵害に関して、48カ月間の累計金額(The aggregate cost of computer crimes and security breaches over a 48-month period)としている。

2003年版は、4年間(2000年から2003年まで)が表になっているため、48カ月と書いてあるが、1年ごとの損失額が表示されている。

ここで注意すべきは、「累積(aggregate)」と書いてあることである。すなわち、

表2　事故・事件発生件数(%)

	1～5	6～10	11～30	31～60	61～	不明
2003年	38%	20%	16%	0%	0%	26%
2002年	42%	20%	8%	2%	5%	23%
2001年	33%	24%	5%	1%	5%	31%
2000年	33%	23%	5%	2%	6%	31%
1999年	34%	22%	7%	2%	5%	29%

表3　外部者による事故・事件発生件数(%)

	1～5	6～10	11～30	31～60	61～	不明
2003年	46%	10%	13%	0%	0%	31%
2002年	49%	14%	5%	0%	4%	27%
2001年	41%	14%	3%	1%	3%	39%
2000年	39%	11%	2%	2%	4%	42%
1999年	43%	8%	5%	1%	3%	39%

表4　内部者による事故・事件発生件数(%)

	1～5	6～10	11～30	31～60	61～	不明
2003年	45%	11%	12%	0%	0%	33%
2002年	42%	13%	6%	2%	1%	35%
2001年	40%	12%	3%	0%	4%	41%
2000年	38%	16%	5%	1%	3%	37%
1999年	37%	16%	9%	1%	2%	35%

資料1　80%は内部犯行?

2000 CSI/FBI Computer Crime & Security Survey

What about the origin of attacks?
Well, although many Pollyannas still cling to the "conventional wisdom" that "80% of the problem is insiders, and only 20% of the problem is outsiders," the number of respondents reporting their Internet connections as a frequent point of attack has increased every year -- rising from 37% in 1996 to 59% in 2000. Meanwhile, the number of respondents citing their internal systems as frequent point of attack actually fell from 51% in 1999 to 38% in 2000. In the 1965 ballad "Outlaw Blues," Bob Dylan boasted, "Don't ask me nothing about nothing, I just might tell you the truth."

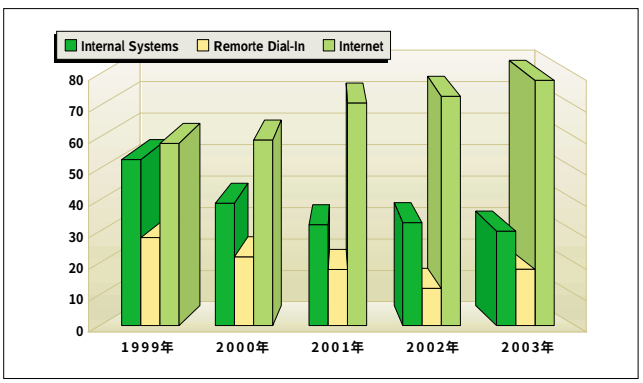


図4　攻撃場所

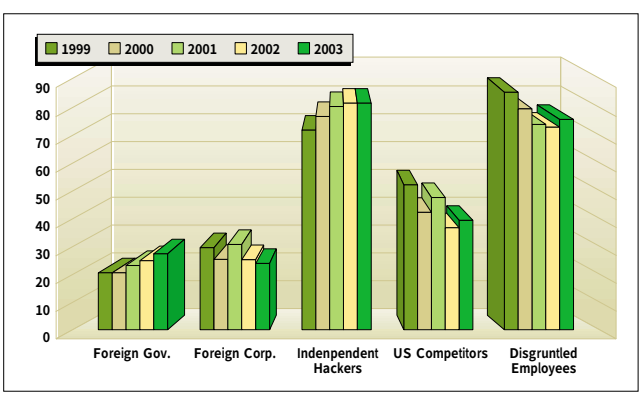


図5　誰が攻撃者か?

この金額は1件ではなく、各組織で、各項目で発生した事件・事故の損失金額の年間合計を示している。複数回発生した組織では金額が大きくなることは十分考えられる。国内では多くの場合、1件の損失金額を計上していることが多いため、単純な比較はできない。

（注1）FORTEZZA　古いシステムであるが、以下で販売している。
http://fortezza-support.com/content/products/FORTEZZA_CryptoCard_N7.asp
以下URLには、価格も表示されている。
http://www.spyrus.com/content/products/FORTEZZA_Plus/fp_order.pdf

（注2）セキュリティキー「LOCK STAR-SK Ver3.0」と、フラッシュメモリ（64M）を結合した製品で、各種機能をユーザーのニーズに合わせ自由に組み合わせて購入できる。基本的には両者の特徴を持っている。

●LOCK STAR-SK Ver3.0の特徴
・Windowsへのログオン管理機能
・USBキーの抜き差しでファイル／フォルダの自動暗号化機能
・シングルサインオン機能
・電子証明書管理機能
・不要ファイル完全削除機能
・ログなどの管理機能

●フラッシュメモリ（64M）の特徴
・通常のフラッシュメモリデータ記憶機能
・パスワードで保護されたセキュリティ領域の設定機能
・LOCK STAR-SKによるデータ暗号化機能
〈http://www.logicaltech.co.jp/index1.html〉

資料2　80%は内部犯行？

2001 CSI/FBI Computer Crime & Security Survey

Conventional wisdom says "80% of computer security problems are due to insiders, 20% are due to outsiders." There are people who cling to this axiom as if some Galileo had just suggested that the Earth might actually be round. But for the fourth yea in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%). Indeed, the number of those citing their Internet connection as a frequent point of attack has been rising, while the number of those reporting both dial-up remote access and their own internal systems as a frequent point of attack have been declinging.

表5　コンピューター犯罪費用

The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 48-month period

In 2003, 75% of our survey respondents acknowledged financial losses, but only 47% could quantify the losses.

How Money Was Lost

	Lowest Reported				Highest Reported				Average Losses				Total Annual Losses			
	00	01	02	03	00	01	02	03	00	01	02	03	00	01	02	03
Theft of proprietary info.	$1K	$100	$6K	$2K	$25M	$50M	$50M	$35M	$3,032,818	$4447,900	$6,571,000	$2,699,842	$66,708,000	$151,230,000	$170,827,000	70,195,500
Sabotage of data of networks	1K	100	1K	500	15M	3M	10M	2M	969,577	199,351	541,000	234,521	27,248,000	5,183,100	15,234,000	5,348,500
Telecom eavesdropping	200	1K	5K	1K	500K	500K	5M	50K	66,080	55,375	1,205,000	15,200	991,200	886,001	346,0000	76,100
System penetration by outsider	1K	100	1K	100	5M	10M	5M	1M	244,965	453,967	226,000	56,212	7,204,000	19,066,600	13,855,001	2,754,400
Insider abuse of Net access	240	100	1K	100	15M	10M	10M	6M	307,524	357,160	536,000	135,255	27,984,740	35,001,650	50,099,000	11,767,200
Financial fraud	500	500	1K	1K	21M	40M	50M	4M	1,646,941	4420738	4,632,000	328,594	55,996,000	92,935,500	115,753,000	10,186,400
Denial of service	1K	100	1K	500	5M	2M	50M	60M	108,717	122,389	297,000	1,427,028	8,247,500	4,285,600	18,370,501	65,643,300
Virus	100	100	1K	40	10M	20M	9M	6M	180,092	243,835	283,000	199,871	29,171,700	45,288,150	49,979,100	27,382,340
Unauthorized insider access	1K	1K	2K	100	20M	5M	1.5M	100K	1,324,725	275,636	300,00	31,254	22,554,500	6,264,000	4,503,000	406,300
Telecom fraud	1K	500	1K	100	3M	8M	100K	250K	212,000	502,278	22,000	50,307	4,028,000	9,041,000	6,015,00	701,500
Active wiretapping	5M	0	0	5K	5M	0	0	700K	5M	0	0	352,500	5,000,000	0	0	705,000
Laptop theft	500	1K	1K	2400	12M	2M	5M	2M	58,754	61,881	89,000	47,107	10,404,300	8,849,000	11,766,500	6,830,500
												Total Annual Losses	265,337,490	377,828,700	455,848,001	208,797,340

CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute