「サイバー攻撃に対する米国政府の取り組みとセキュリティ技術市場の動向」

渡辺弘美@JETRO/IPA NY

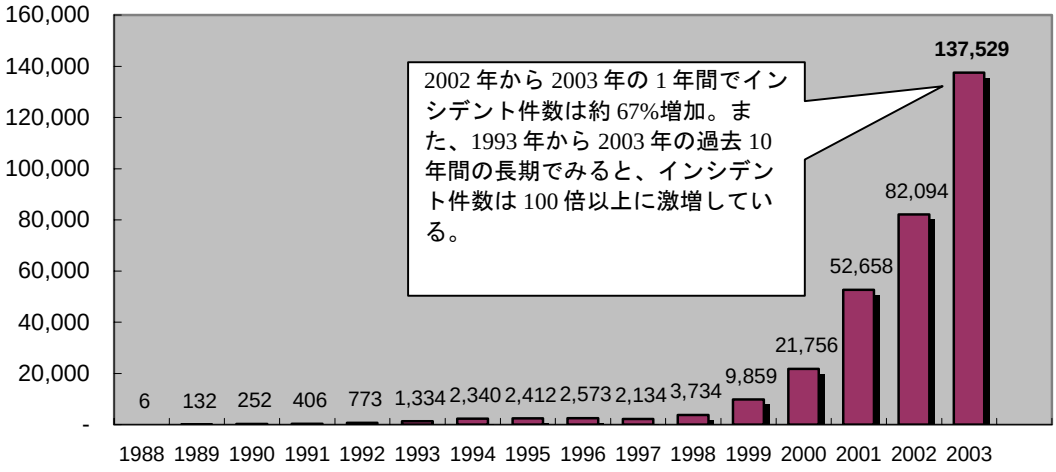
１．　米国におけるサイバー攻撃被害の現状

(1)　米国におけるサイバー攻撃の増加

米国におけるサイバー攻撃は年々急激な増加傾向をたどっている。米国カーネギーメロン大学内に設置された連邦政府財源のインターネットセキュリティ専門組織である CERT Coordination Center（CERT/CC）は、コンピュータの被害に関するデータを収集している。それによると、CERT/CC が 2003 年に対応したコンピュータセキュリティ・インシデント件数は 13 万 7,000 件以上にのぼるという。

なお、自動攻撃ツールの氾濫により、インターネットに接続するシステムへの攻撃は日常茶飯事のインシデントとなったため、攻撃のスコープや規模を評価するには、単なるインシデント数だけでは不十分であることから CERT/CC はこのインシデント数の発表を 2004 年から中止し、より意義のあるメトリックスの開発に取り組んでいる。

CERT/CC が対応したコンピュータセキュリティ・インシデント件数の推移（単位：件数）



また、CERT/CC は、2003 年中に、個人や組織からコンピュータセキュリティ・インシデント報告や情報の照会に関する電子メールを 54 万 2,754 通およびホットラインコールを 934 本以上を受け取った。さらに、2004 年第 1 四半期から第 3 四半期の間に受け取った電子メール数は 55 万 2,320 通、ホットラインコール数は 650 本以上と、電子メール数は 2003 年に受け取った数をすでに上回っているという。

CERT/CC は 2003 年に報告を受けた中で最も悪質なサイバー攻撃として、「W32/Sobig.F ワーム」と、「W32.Slammer ワーム」の 2 種類を取り上げている。前者は、ウィルス自身のコピーを添付したメールを大量に頒布し、後者は、SQL Server 2000 と MSDE 2000 システムを標的としてネットワークトラフィックを増加させ、サービス拒否を引き起こす。

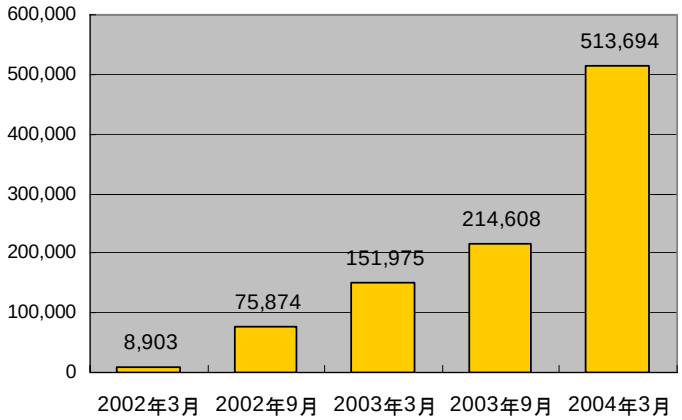
(2)　2004 年に話題となっているサイバー攻撃例

①　スパイウェアの氾濫

2004 年に入って、特に話題となっているサイバー攻撃の一つとして、「スパイウェア」が挙げられる。このスパイウェアはコンピュータユーザの個人情報を収集、また、コンピュータのプロセッサを濫用する悪質なプログラムである。

この問題は、連邦取引委員会（FTC）が 2004 年 4 月に開催したワークショップにおいても大きく取り上げられた。同ワークショップにおいて、McAfee Security 社のシニア・プロダクト・マネージャである Bryson Gordon 氏は、「（同社が）2003 年 8 月に検知したスパイウェア数は 200 万未満であったが、2004 年 3 月までのその数は 1,400 万以上に急増し、スパイウェアがウィルスよりも深刻なテクニカルサポート問題となった」と述べている。また、Computerworld 誌によると、スパイウェアのスキャンと駆除ツールベンダである PestPatrol 社(2004 年 8 月に Computer Associates International（CA）社に買収)が、2002 年 3 月時点でまとめた顧客によるスパイウェア報告件数は 8,903 件であったが、2 年後の 2004 年 3 月にはその数 51 万 3,000 件以上と、約 58 倍に激増したと報告されている。

PestPatrol 社によるスパイウェア報告件数の推移（単位：件数）

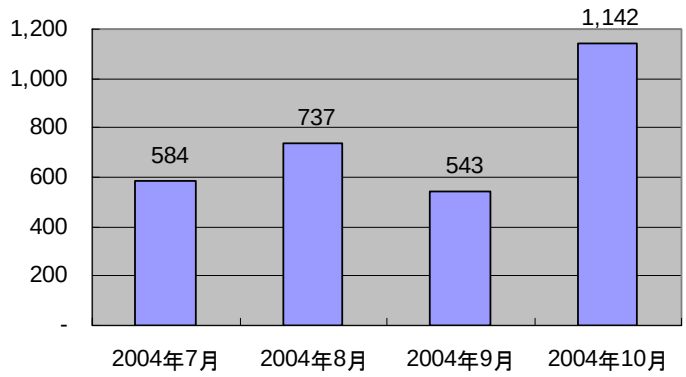


②　フィッシング（Phishing）の被害増大

また、インターネットを利用した詐欺行為も深刻なサイバー犯罪として警戒されている。中でも、最近、大手企業や銀行になりすまして電子メールを送り、ユーザからクレジットカード番号などの個人情報を盗み出す詐欺行為である「フィッシング（Phishing）」による被害が拡大している（「ニューヨークだより 2004 年 9 月号」参照）。

Gartner 社によると、米国民の約 5,700 万人がフィッシングメールやサイト情報を受信しており、2003 年におけるフィッシングによる個人情報の盗難による米国の銀行やクレジットカード発行会社の損失額は 12 億ドルに及ぶと推定されるという。また、VISA 社などの金融機関や Microsoft 社といった IT 企業など多数の組織から構成される、フィッシングなどの電子メール詐欺問題に取り組む産業団体である「Anti-Phishing Working Group」によると、2004 年 10 月に同団体に報告されたフィッシングサイト数は 1,000 サイト数を突破している。

Anti-Phishing Working Group に報告されたフィッシングサイト数の推移
（単位：サイト数）



(3)　個人ユーザの被害実態

コンピュータユーザの多くは、自宅のコンピュータ内にウィルスやスパイウェアまたは「アドウェア」（オンライン広告目的で個人情報を収集するスパイウェアに似た悪質プログラムでありスパイウェアと同類視される）を侵入させたまま知らずに、または、対処できずに放置しているケースが多い。それにもかかわらず、ユーザの多くは、自宅のコンピュータに個人情報など重要なデータを保存しており、「自分のコンピュータは安全だ」と楽観視している傾向がある。こういった現状がサイバー攻撃を助長させている可能性も高いとアナリストは見解している。

2004 年 10 月に発表された America Online 社とサイバーセキュリティを促進する官民共同団体である「National Cyber Security Alliance（NCSA）」によって、329 世帯を対象に実施された「オンライン安全性調査（Online Safety Study）」は次のような結果を示している。

ウィルスとスパイウェアによる被害状況

調査内容		調査結果
ウィルス	いままでにウィルスに感染したことがあるユーザの割合	63%
	ウィルススキャンの結果、現在コンピュータ内に 1 つまたは複数のウィルスが発見されたユーザの割合	59%
	コンピュータ 1 台あたり発見された平均ウィルス数	2.4 件
スパイウェア/アドウェア	スパイウェア/アドウェアスキャンの結果、現在コンピュータ内にスパイウェアプログラムが発見されたユーザの割合	80%
	コンピュータ 1 台あたり発見された平均スパイウェアまたはアドウェアのコンポーネント数	93 個

ユーザの不十分なセキュリティ対策と知識の低さ

調査内容	調査結果
アンチウィルスソフトを導入していない、または、1 週間以上更新していないユーザの割合	67%
スパイウェア/アドウェアのインストールを許可した覚えがないユーザの割合	95%
スパイウェア/アドウェアプログラムは何なのか、何をするのか知らないユーザの割合	90%
スパイウェア/アドウェアの駆除方法（アンインストール）を知らないユーザの割合	76%

ユーザの安易なコンピュータ利用とサイバー攻撃に対する楽観傾向

調査内容	調査結果
自宅のコンピュータに重要な個人情報を保存しているユーザの割合	84%
自宅のコンピュータがサイバー攻撃からかなり、または、幾分安全であると思っているユーザの割合	77%

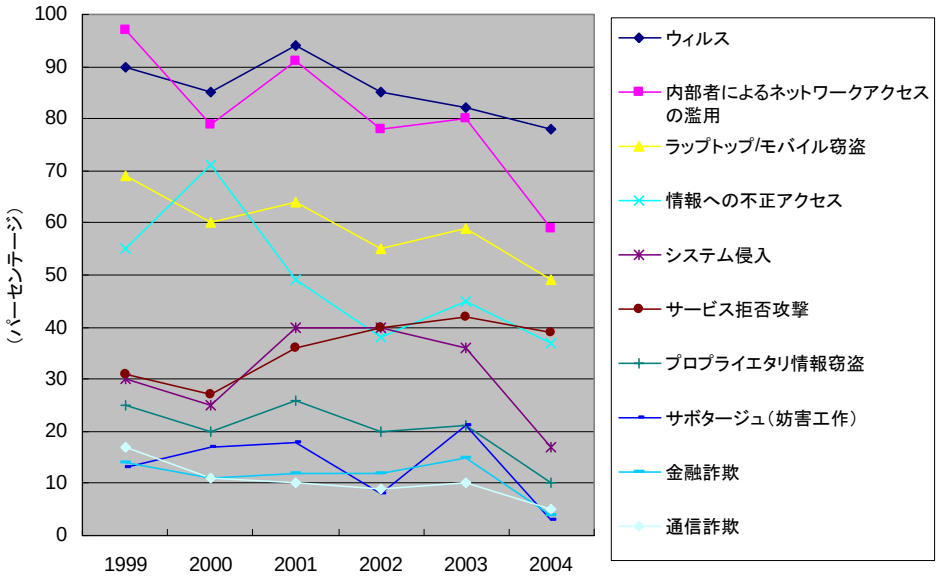
(4)　企業・政府機関に対するサイバー攻撃状況

一方、別の調査結果では、米国のサイバー攻撃の被害の低減を示すケースもある。コンピュータや情報セキュリティに関するトレーニングやサービスを提供する会員組織である Computer Security Institute（CSI）は連邦捜査局（FBI）との共同で、各種企業および政府機関のセキュリティ担当やシステムアドミニストレータなど約 500 人を対象にコンピュータ犯罪とセキュリティに関する調査

（Computer Crime and Security Survey）を毎年実施している。その調査結果によると、種類別のサイバー攻撃を経験した調査対象者数は 1999 年から 2004 年にかけて、サイバー攻撃の種類によって多少の増減の波はあるものの全体的にゆるやかな減少傾向を示している。

これによると、2004 年の各種攻撃が及ぼした損失額の総額が約 1 億 4,150 万ドルと、2003 年の約 2 億 179 万ドルに比べて約 30%も減額している。CSI のディレクタである Chris Keating 氏は「サイバー犯罪は依然、米国の組織に対する重大な脅威であるものの、調査対象者である政府機関や企業は情報セキュリティに取り組み、その成果が表れているようだ」と述べている。この結果、政府や企業によるセキュリティ対策がサイバー攻撃経験数や損失額の低減に貢献していると分析する見方もある。

サイバー攻撃種類別の経験者数の推移（単位：%）



ただし、大手セキュリティ製品ベンダである Internet Security Systems（ISS）社のシニアアナリストである Carter Schoenberg 氏は、この調査はたった約 500 人を対象としたいわゆる“氷山の一角”を見ていることに過ぎないこと、また、企業は法執行機関にハッキングなどのインシデント報告を行うことを避けていることを考慮するべきだとしている。事実、2004 年の損失額の回答者数は、2003 年と同様、調査対象者の約半数であり、損失額を回答できない、または回答したがらない者が多いことからも、同氏の指摘は否定できない。

このように、CSI/FBI 調査結果から、企業によってはセキュリティ対策の改善によって、サイバー攻撃を回避し、損失額を低減しているというケースもあるものの、同調査に参加していない大多数の米国企業や組織、さらに、サイバー攻撃

にあったにもかかわらず CERT に報告しなかった個人や組織の総数を考慮すると、米国におけるサイバー攻撃の被害は未知数であるといっても過言ではない。

２．　サイバー攻撃に対する連邦政府の取り組み

(1)　国土安全保障省（DHS）の取り組み

2003 年 1 月に始動した国土安全保障省は、米国における情報セキュリティ政策における重要な位置づけにある。その沿革として、まず、2001 年 9 月 11 日の同時多発テロ事件をきっかけに、同年 10 月に「大統領令（Executive Order）13231」が発令され、米国連邦政府における重要インフラであるサイバーセキュリティの強化を目的として「大統領重要インフラ保護委員会（President’s Critical Infrastructure Protection Board：PCIPB）」が発足した。

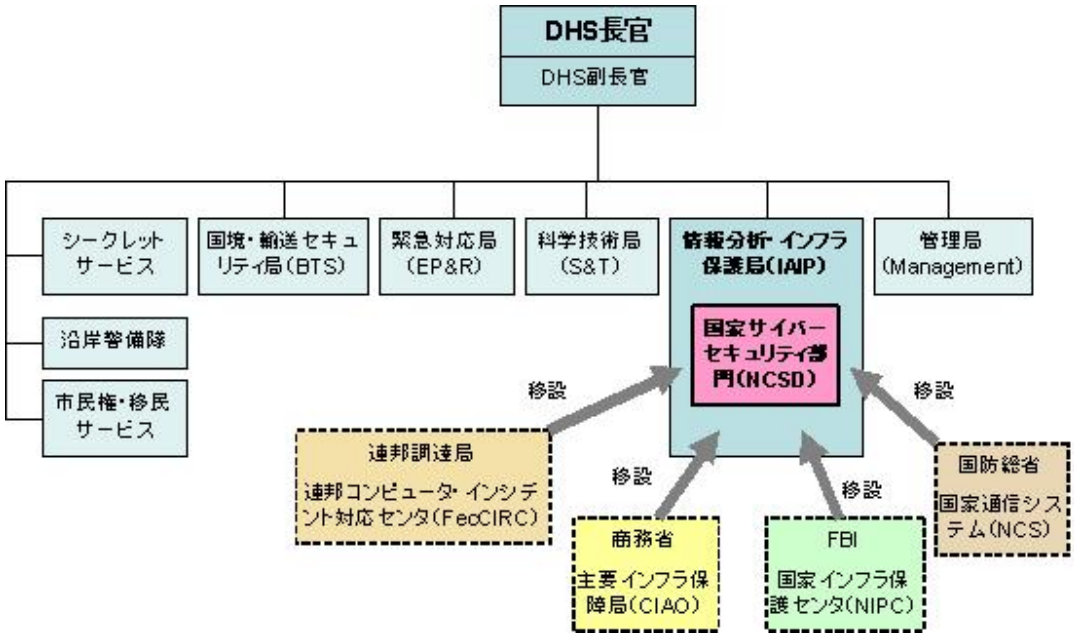
しかし、その後、2003 年 2 月に発令された「大統領令 13286」において、サイバーセキュリティの所管が PCIPB から、国土安全保障省に全面的に移行することが決定し、PCIBP は事実上廃止となった。また、ブッシュ政権が同月に発表した「サイバーセキュリティ国家戦略（The National Strategy to Secure Cyberspace：NSSC）」においても国土安全保障長官がサイバーセキュリティに関する責任を負う立場であることが明記されている。

＜国家サイバーセキュリティ部門の新設＞

このような背景のもと、2003 年 6 月、国土安全保障省はサイバーセキュリティに取り組む責務を果たすために「国家サイバーセキュリティ部門（National Cyber Security Division：NCSD）」を新設した。同省が発行したプレスリリースによると、この部門は、同省の情報分析・インフラ保護局（Information Analysis and Infrastructure Protection：IAIP）内に設置され、同省設立にあたって IAIP に他の省庁から移設されてきた次の部門によって機能を土台としている。

- 商務省管轄下の主要インフラストラクチャー保証局（Critical Infrastructure Assurance Office：CIAO）
- FBI 管轄下の国家インフラ保護センタ（National Infrastructure Protection Center：NIPC）
- 連邦調達局管轄下の連邦コンピュータ・インシデント対応センタ（Federal Computer Incident Response Center：FedCIRC）
- 国防総省管轄下の国家通信システム（National Communications System：NCS）

国家サイバーセキュリティ部門の位置づけ



NCSD は、サイバー脅威や脆弱性の分析や緩和、脅威に関する警告の発令、インシデント対応の調整、オペレーションの継続性や復旧計画における技術的補佐など、24 時間体制で稼動している。

ちなみに、NCSD が設置されている IAIP は、この NCSD のサイバーセキュリティ以外に次のような機能を備えている。

- 対テロ対策のための政府と民間セクタの間の情報共有の推進と国内インシデントの管理
- テロリスト関連の諜報分析と警告の発信
- 重要インフラの保護（ここでの対象は情報・通信ネットワークだけでなく、鉄道や航空、電力やガスなどの物理インフラも含まれるなど幅広い）

＜NCSD の活動内容＞

これまでの NCSD の重要な取組みとして次の 2 つが挙げられる。

① US-CERT の設立

2003 年 9 月、官民パートナーシップによる国家のためのコンピュータ緊急準備チームとして、US-CERT（Computer Emergency Readiness Team）を設立。NCSD は US-CERT の先導役として、民間セクタのサイバーセキュリティベンダ、学術機関、連邦・州・地方政府機関、および、その他国内外の組織といった様々な提携機関と共に米国のコンピュータセキュリティ体制やサイバー攻撃対応の改善に取

り組む。また、前述したカーネギーメロン大学の CERT/CC とも密接な協力関係を築いている。

② National Cyber Alert System の運用開始

2004 年 1 月、米国国民や企業および政府機関などにコンピュータセキィリティの脆弱性や脅威を軽減するための対策などに関する情報をタイムリーに提供する National Cyber Alert System の運用開始を発表。NCSD は US-CERT という立場から同システムを管理することになる。また、同システムによる情報サービスは事前に登録（無料）することによって電子メール経由で利用可能。

＜NCSD の不安定な組織体制＞

NCSD は上記のような活動を進めてはいるが、その組織体制は不安定であり、サイバーセキュリティ組織として確立するにはまだしばらく時間がかかりそうである。同省の内部監査室（Office of Inspector General）は、2004 年 7 月に発表した報告書の中で、NCSD の組織体制の構築の遅れを指摘し、NCSD が抱える課題として次の内容を挙げている。

- NCSD は掲げている目標やイニシアチブに優先順位をつけていない。よって、これまでの取組みが“マイルストーン（標石）”をクリアしてきたのかどうか評価できない。
- NCSD の目標達成に必要な長期計画としての予算や必要なリソースを確認できていない。
- 目標達成のための戦略的計画が開発されていない。
- 国土安全保障省内における正式なコミュニケーション方法が確立されていない。
- 国土安全保障省、他の政府機関、民間政府向けにサイバーセキュリティ問題に関するガイダンスを監督・発行する正式なプロセスを開発していない。

内部監査室は NCSD にこれらの課題を克服するよう勧告している。また、スタッフ数に関して、内部監査室は、NCDS は 2004 年度の計画では目標達成に 112 人のスタッフが必要と判断したにもかかわらず、2004 年 2 月 23 日の時点で 84 人しか確保できていないことも指摘している。

また、NCSD の初代ディレクタであった Amit Yoran 氏は、就任後約 1 年となる 2004 年 9 月末に辞任を表明した。前職は Symantec 社のマネッジド・セキュリティサービス部門 VP であった同氏は「コア・ミッションは達成した」と辞任のコメントを述べているが、関係者は、Yoran 氏には連邦政府のサイバーセキュリティ体制を構築するには不十分な権限しか与えられておらず、サイバーセキュリティ活動に消極的な現政権の態度が同氏の辞任を招いたとコメントしている。現在、NCSD の副ディレクタであった Andy Purdy 氏が暫定ディレクタと任命されている

が、関係者によると、2004 年 12 月中旬までに正式なディレクタが選定される予定になっている。

過去を振り返ると、このようなセキュリティ組織の体制が不安定であるのは今だけではないことが分かる。ホワイトハウス内に設置されていた前述の「大統領重要インフラ保護委員会（PCIPB）」の委員長を務めていたサイバースペース担当大統領特別顧問だった Richard Clarke 氏は、サイバーセキュリティ機能をホワイトハウスから国土安全保障省に移行することはサイバーセキュリティの重要性を格下げすると見なし、この決定を受け入れずに 2003 年 2 月辞任した。同氏は、クリントン政権時には国家安全保障会議（NSC）において主要インフラやサイバーシステムの保護、およびテロ対策をまとめる「全米コーディネータ」を務めるなど、9/11 テロ事件以前から米国のサイバーセキュリティ対策を指揮してきた重要人物であった。その後、PCIPB 副委員長であった Howard Schmidt 氏が委員長に就任したが、同じく、ブッシュ政権のサイバーセキュリティの位置付けに不満を示し、2 ヶ月後の同年 4 月に辞任した。このような背景もあり、NCSD は 2003 年 6 月にディレクタ不在のまま発足し、同年 9 月にようやく Yoran 氏を起用していることからも、Clarke 氏や Shmidt 氏といったサイバーセキュリティ先導者を失った後、NCSD のディレクタの選定はかなり困難であったと推測できる。

このように、NCSD の組織体制は揺らいでおり、国家のサイバーセキュリティ機関として確実に機能するために解決すべき課題は多い。その一方で、Tom Ridge 国土安全保障省長官は、Yoran 氏辞任後、2004 年 10 月 12 日、サイバーセキュリティ担当の長官補佐官（Assistant Secretary）を設置する計画があることを公表した。Ridge 氏の表明直後に、同省のスポークスマンである Brian Roehrkassee 氏は、「同ポジションが長官補佐官であるかはまだ決定していない」と訂正しているものの、サイバーセキュリティ監督者の権限を高めることで、同省のサイバーセキュリティ組織体制を安定化させようという動きが伺われる。

(2)　司法省のサイバー犯罪取締り

コンピュータを利用した犯罪は州の境界をまたぐことが多いため、サイバー犯罪の捜査や犯人の検挙は主に司法省（Department of Justice）の刑事局（Criminal Division）と連邦捜査局（FBI）の管轄となっている。また、多くのサイバー犯罪において、この 2 局が共同捜査し、さらに、州・地方自治体レベルの法執行機関やその他関連組織とが提携するケースも顕著に見られる。このことから、サイバー犯罪取締りにかかわる機関間における密接な協力体制が確立している。

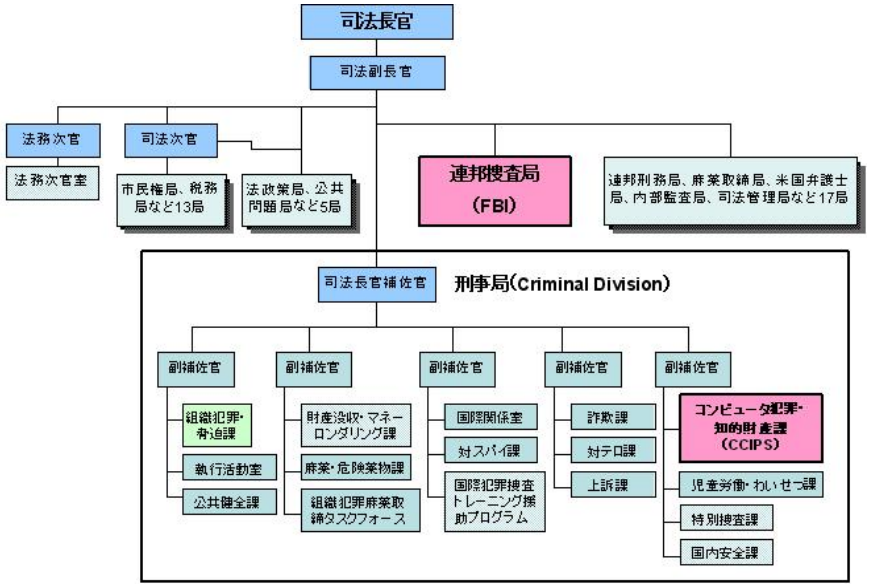
①　サイバーフォレンジックス(Cyber Forensics)

サイバー犯罪の取締りには、犯罪に関与したコンピュータ内に残っている証拠の取扱が必要となるが、この捜査手段は特に「サイバーフォレンジックス（Cyber Forensics）」と呼ばれている。このサイバーフォレンジックスとは、「証拠の完全性、検出情報の正式報告、また、法廷における専門家としての証言などを含んだコンピュータによる証拠を特定・抽出・解釈・文書化する技術的捜査手段」である。1998 年から 2001 年の間、コンピュータが関与した犯罪数の増加率は 680%と爆発的に増えるといった現象を踏まえ、2002 年、FBI はサイバーフォレンジックス調査を行う組織である「地域コンピュータフォレンジックス研究所(Regional Computer Forensics Laboratory : RCFL)」を開設し、全米各地に同研究所の設置を推進している。1999 年、カリフォルニア州サンディエゴに最初の RCFL が設立されて以来、2004 年 4 月時点において全米 5 箇所で RCFL が運営されている。さらに、8 箇所における開設が決定している。現在米国ではサイバー犯罪取締りにサイバーフォレンジックスは重要な手段として活用されている。

② 司法省のコンピュータ犯罪・知的財産課（CCIPS）

司法省は、サイバー犯罪に取り組む主要組織として、司法副長官が直接管轄している刑事局内にコンピュータ犯罪・知的財産課（Computer Crime and Intellectual Property Section：CCIPS）を設置している。

司法省におけるコンピュータ犯罪・知的財産課の位置づけ



同課は、刑事局内に過去設置されていた一般法廷訴訟・法律課（General Litigation and Legal Advice Section）内のコンピュータ犯罪ユニット

（Computer Crime Unit）（1991 年開設）が、1996 年に刑事局の一課として昇格して出来た組織である。

同課は、コンピュータや知的財産犯罪に関する問題に特化した約 40 人の弁護士から構成されている。同部門の弁護士団は、電子プライバシー法、コンピュータの捜査や差押え、電子商取引、ハッカー捜査、知的財産犯罪といった幅広い分野の専門知識を備えており、連邦検察官や法執行機関への助言、法制定の提案、コンピュータ犯罪と戦うための国際的な取組みの調整、法廷訴訟、法執行機関の教育などを行っている。また、CCIPS が最近起訴した事件には、2004 年 10 月 28 日、盗難された個人情報やクレジットカード番号などの不正に販売する不法ウェブサイトの運営組織に関与した 19 人を起訴したケースなどがある。このケースは、国土安全保障省のシークレットサービスやその他法執行組織との共同捜査によるもので捜査範囲は海外にも及ぶ大規模なものであった。

③　「CHIP」ユニットによる地域別の取締り

また、司法省は 2001 年、地域単位でサイバー犯罪の取締りを強化するために、「CHIP（Computer Hacking and Intellectual Property）」と呼ばれるコンピュータや知的財産犯罪を取り締まるプログラムを開始、現在までに、ニューヨーク州ブルックリンやバージニア州アレキサンドリアなどを含む全国 14 箇所に CHIP ユニットが設置されることとなった。

この CHIP ユニットは、前述の CCIPS の活動を補完し、さらに、FBI や他の法執行機関と密接に共同活動を行っている。CHIP ユニットによる犯罪起訴例として、カリフォルニア州の男性が元雇用企業の機密取引情報を個人利益（約 6 万ドル）のために利用したケースや、フロリダ州の男性が偽造コンピュータプログラムを販売し、コンピュータプログラム会社 3 社に総額約 200 万ドルの損害を与えたケースなどがある。どちらのケースも FBI が共同捜査を行っている。

司法省は 2004 年 10 月、全国の CHIP ユニットが 2003 年会計年度に起訴した犯罪者数は、2003 年度以前の 4 年間における年平均起訴数よりも 46%増加したと CHIP ユニットの成果を公表している。また同時に、同省は、さらに、コロンビア特別行政区、ペンシルバニア州ピッツバーグ、テネシー州ナッシュビル、フロリダ州オーランドの 4 箇所にもユニットを新設する計画も発表するなど、CHIP ユニットのさらなる拡張を促進している。

④　連邦捜査局（FBI）サイバー局

連邦捜査局（FBI）は、国家をサイバー攻撃から保護することを、対テロ、対海外諜報活動に続く、第 3 番目のプライオリティに位置付けており、積極的にサイバー犯罪を取り締まっている。

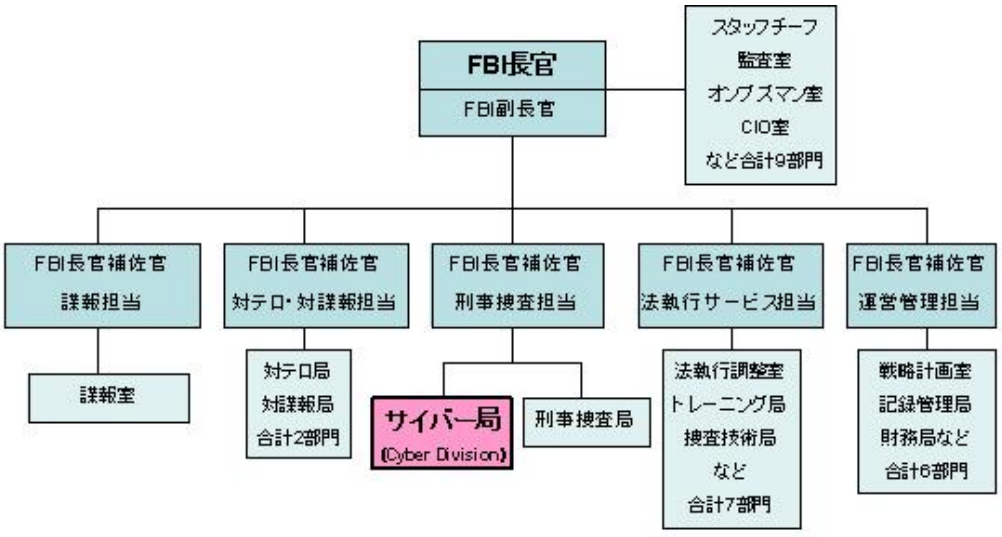
FBI は、それまで分散していたサイバー犯罪対策に関する機能の効率化するために組織の再編成実施し、サイバー局（Cyber Division）を 2002 年 4 月に開設した。同局は、次のようなミッションを担っている。

- テロリスト組織、外国政府、または犯罪者がインターネットやコンピュータシステムを悪質行為の主要手段として利用する、または攻撃対象とするといった連邦規模のサイバー犯罪に関する FBI の捜査を調整・監督・促進する。
- 官民による協力体制を構築・維持し、対テロおよびサイバー対応機能を強化するための教育やトレーニングを充実する。

同局は FBI ワシントン DC 本部において、刑事捜査を担当する FBI 長官補佐官によって刑事捜査局（Criminal Investigative Division）と共に管轄されている。

また、各地に点在する FBI 支部の多くはサイバーアクションチーム（Cyber Action Teams：CATS）と呼ばれる特別サイバー班を配置している。CATS は専門知識を活用し、各地のサイバー犯罪捜査を補佐する役目を果たす。

FBI 本部サイバー局の位置づけ



⑤ FBI のリクルート戦略

FBI は最近とくにサーバーセキュリティの取締り体制を強化するために、コンピュータサイエンス専攻者の採用に力を入れている。FBI は 2004 年に 1,200 人の職員を新しく採用する予定であるが、FBI が求めているのは犯罪学専攻者ではなく、コンピュータサイエンス、および、経理・ファイナンス分野の経営管理の専攻者であるという。

⑥ サイバー犯罪の一斉摘発イニシアチブ

司法省は、サイバー犯罪を一斉摘発する共同捜査を頻繁に実施している。これらはそれぞれ特定または複数の種類のサイバー犯罪を対象としており、CCISP や FBI をはじめ、各地の法執行機関が共同捜査している。

＜最近実施された一斉捜査例＞

【Operation Fastlink】　実施時期 2004 年 4 月
インターネットによる著作権侵害に関する犯罪を国際的に取り締まった。CCIPS が中心となり、FBI および各地の法執行機関による共同捜査は米国 27 州、海外 10 カ国で実施され、200 台以上のコンピュータを押収、回収されたソフトウェアや音楽・映画・ゲームなどの偽造データ価値は総額 5,000 万ドルを超える。

【Operation WebSnare】　実施時期 2004 年 6 月 1 日～2004 年 8 月
犯罪スパム、フィッシング、クレジットカード詐欺、知的財産の侵害、コンピュータ侵入、取引機密情報の盗難などのサイバー犯罪を対象とした大規模な取締りで、「Direct Marketing Association（DMA）」（1917 年に設立された通信販売に関する米国の産業団体で 5,200 社以上が会員）や「Business Software Alliance（BSA）」（1988 年に設立されたソフトウェアの権利保護の促進を目的とした世界的な業界団体で多数の大手ベンダが加入）などを含む産業組織も協力した。捜査件数 160 件以上（被害者総数 15 万人以上、損失総額は 2 億 1,500 万ドル以上の規模）において、150 人の容疑者を検挙しており、起訴件数は 117 件に上る。

【Operation Digital Gridlock】　実施時期 2004 年 8 月
前述の「Operation Fastlink」同様、オンライン著作権侵害の摘出であるが、P2P（ピア・ツー・ピア）ネットワーク上での不正データ配信に特化したもので、5 つのネットワークから 40 テラバイトもの不正データを押収した。

⑦　インターネット詐欺苦情センタ

インターネット詐欺苦情センタ（Internet Fraud Complaint Center：IFCC）は、インターネット詐欺問題に取り組むために、FBI と「米国ホワイトカラー犯罪センタ（National White Collar Crime Center：NW3C）」（経済犯罪やハイテク犯罪の捜査や起訴に取り組む機関を補佐する非営利団体として連邦政府から資金を受けて 1980 年に設立）によって共同運営されている。IFCC はインターネット詐欺に関連した苦情のレポジトリや詐欺動向の統計データの提供や、詐欺パターンの特定などのサービスを法執行機関に提供する。前述の「Operation Websnare」において捜査協力を提供している。

(3)　その他の連邦政府機関の取組み

連邦政府機関内部におけるサイバーセキュリティ対策は国土安全保障省も含めて、まだまだ発展途上であり、政府が保持する情報やシステムはサイバー脅威にさらされた状態が続いている。

各省庁は、2002 年に制定された「連邦情報セキュリティ管理法（Federal Information Security Management Act：FISMA）」に従い、毎年、情報セキュリティ対策を自己評価しその結果を OMB に報告する義務がある。この自己評価をもとに下院政府改革委員会（Committee on Government Reform）が発表した 2003 年度の連邦政府全体のセキュリティ対策の評価は“D”（A、B、C、D、F の 5 段階に加え、各段階の中でもマイナス（-）、プラス（+）という補助段階がある）であり、前年 2002 年度の評価“F”に比べやや改善されたものの、政府全体におけるセキュリティ対策の遅れは隠せない。

連邦政府コンピュータセキュリティリポートカード（2003 年 12 月 9 日）

省庁名	2003	2002	省庁名	2003	2002
原子力規制委員会（NRC）	A	C	連邦調達局（GSA）	D	D
全米化学財団（NSF）	A-	D-	財務省（TREUS）	D	F
社会保障局（SSA）	B+	B-	人事局（OPM）	D-	F
労務省（DOL）	B	C+	航空宇宙局（NASA）	D-	D+
教育省（ED）	C+	D	エネルギー省（DOE）	F	F
退役軍人省（VA）	C	F	司法省（DOJ）	F	F
環境保護局（EPA）	C	D-	保健福祉省（HHS）	F	D-
商務省（DOC）	C-	D+	内務省（DOI）	F	F
中小企業庁（SBA）	C-	F	農務省（USDA）	F	F
国際開発庁（USAID）	C-	F	住宅都市開発省（HUD）	F	F
運輸省（DOT）	D+	F	国務省（DOS）	F	F
国防総省	D	F	国土安全保障省	F	--

このような劣悪な評価成績を向上するためにも、各省庁は 2004 年度、各自のコンピュータセキュリティ体制の改善のために様々な取組みを展開している。その一方、2004 年度もあいかわらずサイバー攻撃の被害を受けた機関（例、環境保護局、エネルギー省）もみられる。各省庁は FISMA に基づいた 2004 年度の自己評価報告書を 2004 年 10 月 6 日までに OMB に提出することになっており、現在、2004 年 12 月に発表される下院政府改革委員会の評価を待っている状態である。多くの省庁はまだ各自の報告書を一般公開していないようであるが、公開している省庁の中から次の 3 省庁の報告書の概要を紹介する。

① 社会保障局（2003 年度評価 B+）

社会保障局（SSA）は、2003 年度に B+と比較的高い評価に甘んずることなく、2004 年度にはさらなるコンピュータセキュリティプログラムの改善を試みている。

同局の 2004 年度 FISMA 報告によると、同局のコンピュータセキュリティプログラムは継続して改善傾向にあると結論付けている。同報告書の中で報告されている 2004 年度に実施した取組み例は次のとおり。

- 自動セキュリティ自己評価・改善トラッキングシステム（Automated Security Self-Evaluation and Remediation Tracking：ASSERT)を導入することで、すべてのシステムにおける脆弱ポイントや各システムの脆弱性の改善段階をモニタリングすることが可能となった。
- 同局内のすべてのプログラムとシステムのインベントリを完了した。

また、2004 年度のあいだ、同局が内部報告、または US-CERT や法執行機関に報告しなければならないインシデント数はゼロと、サイバー攻撃の被害を受けなかったことも報告している。一方、改善の余地がある分野として、“職員向けの情報セキュリティトレーニング方法の開発”と“オペレーション継続のための計画”が指摘されている。

② 環境保護局（2003 年度評価 C）

環境保護局（EPA）は 2004 年度、同局のコンピュータセキュリティプログラムにおける全体的な改善を見せており、成績評価の向上が期待できると考えられる。

同局の 2004 年度の FISAM 報告によると、同局は情報リソースのセキュアを確保するために積極的に取り組んでおり、2004 年度に内部監査によって指摘された“コンフィグレーション制御における脆弱性”や“ファイヤウォールセキュリティの強化”などは 2004 年度末までに適切な改善措置を行ったという。また、同局は、2004 年度にサービス拒否攻撃 1 件、ウィルス/ワーム感染 224 件を報告しているが、同局の文書化されたポリシーと対処方法に遵守してそれらのインシデントの検知と対応の実施に成功している。

③ エネルギー省（2003 年度評価 F）

エネルギー省（DOE）は 2004 年度、前年度に引き続き同省が情報セキュリティ対策の改善に苦戦している状態が見られる。

同省の 2004 年度 FISMA 報告によると、同省はサイバーセキュリティ政策の改善に引き続き取り組んでおり、次のような取り組みを実施したという。

- 脆弱ポイントを改善するための新しいサイバーセキュリティポリシーの導入
- 同省の主要アプリケーションやサポートシステムの特定の開始
- サイバーセキュリティ・インシデント報告の改善

一方、同省が包括的なリスクマネジメントプログラムの導入を完了しなかった点が指摘されている。具体的に実施を怠った内容の例は次のとおり。

- 主要システムのリスクの特定が不完全である
- ミッションクリティカルなシステムの継続性を確立するためのポリシーの開発されていない
- アクセス権限の制御などを含むセキュリティコントロールが不確定

また、2004 年度に同省は 119 件のコンピュータ侵入被害によって 3,531 のシステムがその影響を受けるなど、同省のシステムが深刻なセキュリティ問題を抱えていることが分かる。

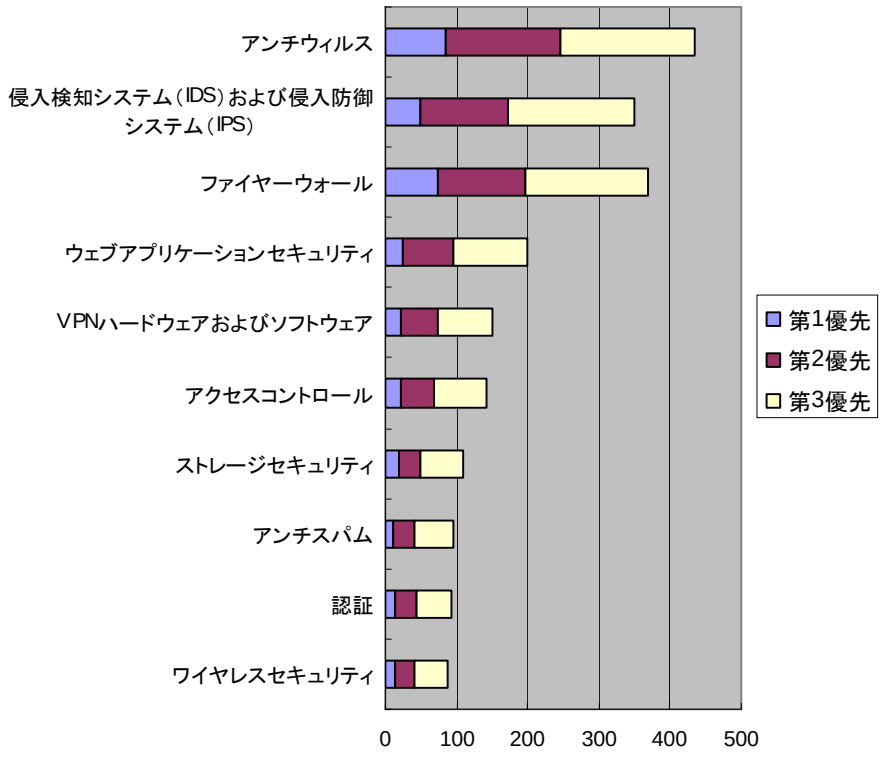
３．　セキュリティ技術市場の動向

連邦政府による取り組みに続き、企業における取り組みをいくつか紹介する。

(1)　企業が利用するセキュリティ技術

Yankee Group 社が 2004 年 2 月に発表した調査（調査対象は 404 人の大中企業の意思決定担当者）によると、2004 年度における投資額の大きいセキュリティ技術は以下の通りである。

2004 年度企業セキュリティ技術上位 10（単位：回答者数）



この調査によると、多くの企業は、アンチウィルス、侵入検知システム（IDS）/侵入防御システム（IPS）、ファイヤーウォールの 3 つのソリューションに比較的多く投資しているのが分かる。また、それら以外の上位 10 のセキュリティソリューションのいずれも企業のシステムや情報資産を保護するために重要なものであると考えられる。

(2)　ベンダによるセキュリティ技術開発例

セキュリティ関連ベンダは、上記のようなセキュリティ技術をはじめ、企業や一般ユーザをサイバー攻撃から保護するための技術開発を促進している。ここでは、ユビキタス環境が発達してきたという最近の傾向に焦点を当てて、（１）ワイヤレス LAN、（２）エンドポイント、（３）トラステッドコンピューティングの 3 つの分野におけるセキュリティ技術市場の動向を紹介する。

①　ワイヤレス LAN のセキュリティ

ワイヤレス LAN（WLAN）技術はすでに、カフェや空港などの公共の場所、自宅、職場などあらゆる場所に普及している一方、現時点では WLAN のセキュリティ技術はまだ完全とはいえない。しかし、各ベンダによるセキュリティ技術開発は急速に推進されている。

＜WLAN の脆弱なセキュリティ＞
WLAN を構築するアクセスポイントと端末におけるセキュリティは脆弱でありサイバー攻撃の被害を受けやすい。2004 年 6 月に発表された Gartner 社の調査によると、WLAN 攻撃の原因の 70%は WLAN アクセスポイントと端末側のソフトウェアの誤ったコンフィグレーションであるという状態が 2006 年まで続くと予測されている。同調査によると、ハッカーは保護されていないアプリケーション経由で企業の WLAN に侵入し、気付かれることなく WLAN を不正利用することができるという。

＜WLAN セキュリティ市場の成長＞
このように脆弱なセキュリティが指摘されながらも、その利用性から WLAN を導入する企業は後をたたない。前述の Yankee Group 社の調査によると、調査対象者のうち約 50%は現在すでに WLAN を導入しており、さらに、約 30%は 2004 年または 2005 年に導入予定と答えている。Internet.com 誌の 2004 年 9 月 22 日付け記事によると、Frost & Sullivan 社の調査を基に、「企業における WLAN 導入が促進されると同時に、WLAN セキュリティ市場も急速に成長することは確実であると見解されている。一方、同調査は、ネットワークセキュリティの対象となる攻撃や問題は流動的であることからどのセキュリティ技術がどのように成長し続けるかは不透明である」と指摘している。

＜ベンダによるセキュリティ改善の動き＞
　このような WLAN 市場の成長を後押しするかのように、セキュリティ技術ベンダは WLAN セキュリティ技術開発に取り組んでいる。2004 年 11 月 1 日に発表された Inforetics Research 社の調査によると、セキュリティ問題は今も昔も WLAN の導入に対する第一の障害である一方、企業は脅威を理解し、昨年以降、ベンダが開発してきたセキュリティ機能を上手く利用し始めているという。WLAN スイッチやその他の新しい機器は、アクセスコントロールのリアルタイム・アドミニストレーションなど重要なセキュリティ機能を備え始めており、例として、主要 WLAN セキュリティベンダである AirDefense 社は 2004 年 11 月 8 日、業界初の WLAN 向け自己管理型侵入検知システムを発売している。このシステムは WLAN 上のセキュリティリスクや不正アクセスなどの自動特定やポリシーに違反したアクセスの自動拒否を実現する。

② エンドポイントのセキュリティ

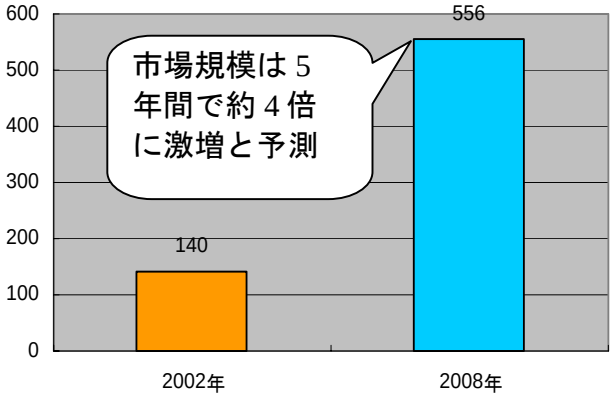
　エンドポイントセキュリティとは、ネットワークのエンドポイントである PC などの端末をウィルスやスパイウェアなどのサイバー脅威から保護するソフトウェア技術である。社員が社内だけでなく自宅や出張先などの様々なネットワークに端末を接続する機会が増えるとともに、端末がサイバー脅威にさらされる機会も増える。よって、そのような端末を保護するこのエンドポイントセキュリティ市場は今後成長すると考えられている。

＜エンドポイントの危険性＞
　企業のネットワークにアクセスする社員は、社内だけでなく自宅や出張先など様々なネットワーク環境を利用している。また、1 台のコンピュータを複数の社員で共有するケースや、仕事用の PC を私用のファイルダウンロードやインスタントメッセージに利用するケースも考えられる。よって、社員が利用する端末は予期していなかったウィルスやスパイウェアなどのサイバー攻撃にさらされる機会が多く、端末経由で企業のネットワークにもサイバー攻撃の影響が及ぶ恐れが考慮できる。さらに、社員が社外で利用する端末内のアンチウィルスソフトウェアが常に更新された状態に保つことは困難である。これらのことから、企業のセキュリティマネージャにとって、所構わずインターネットと接続されるエンドポイントは頭痛の種の一つであるという。

＜エンドポイント機器市場の拡大＞
　このような背景もあり、オンライン情報サイト「iApplianceweb」の 2003 年 12 月 2 日付けの記事によると、Frost & Sullivan 社の調査を基に、エンドポイントセキュリティ製品の市場規模は 2002 年の 1.4 億ドルから 2008 年には 5.56 億ドルに拡大すると予測されている。
　また、エンドポイントセキュリティ市場は投資家からも注目されており、エンドポイントセキュリティソフトウェアベンダである Senforce Technologies 社が

120 万ドル以上のベンチャーキャピタルを受けたという事例も 2004 年 11 月に報道されている。

エンドポイントセキュリティ製品市場の予測



＜主なベンダの動向＞

エンドポイントセキュリティ製品は、単なるファイヤーウォールだけでなく、ワイヤレスアクセス保護、問題の検出・対応・報告、セキュリティポリシーの設定・実行といった複数の機能を備えている。この市場の主なプレーヤーは Sygate Technologies 社や前述の Senforce Technologies 社などのエンドポイントセキュリティに特化したソフトウェアベンダ、または、CheckPoint 社や Symantec 社などのコンピュータセキュリティ製品ベンダである。しかし、最近、大手総合 IT ベンダも積極的な動きを見せており、例えば、IBM 社と Cisco 社は 2004 年 10 月 14 日に、両社の技術提携によって、ネットワークを脆弱性から保護し、脅威が企業の日常業務に及ぼす影響を最小化するための統合エンドポイントセキュリティソリューションを提供することを発表している。

③トラステッドコンピューティング(Trusted Computing)

クライアントレベルのセキュリティは、上述したエンドポイントセキュリティ以外に、データの暗号化や公開鍵基盤（PKI）などを利用することで改善されるが、暗号化のための暗号鍵がソフトウェアによって生成され、ソフトウェア内に保管されるようなソフトウェアベースの暗号技術はハッカーに攻撃される危険性があり、十分なセキュリティを確保できない。そこで、ハードウェアベースのセキュリティ技術である「トラステッドコンピューティング」の導入が大手ベンダによって推進されている。

＜トラステッドコンピューティングの概要＞

トラステッドコンピューティングは、国際的なハードウェア・ソフトウェアベンダによって構成される企業団体「Trusted Computing Group（TCG）」（TCG はト

ラステッドコンピューティング技術を推進するために 1999 年に発足した「Trusted Computing Platform Alliance（TCPA）」を母体としている）によって推進されている。この TCG に加盟する企業には、IBM 社、Intel 社、Microsoft 社、Sony 社、Sun 社などの大手ベンダが名を連ねる。トラステッドコンピューティングは、トラステッドプラットフォームモジュール（Trasted Platform Module：TPM）と呼ばれる暗号技術によって実現される。この TPM は、暗号鍵、パスワード、電子証明書などの重要データを保管できるマイクロコントローラーであり、PC に搭載されたシリコンチップ内部に埋め込まれている。ハードウェア内のデータは、ソフトウェアと比較して、外部からのソフトウェア攻撃や PC の盗難から極めてセキュアである。また、TPM はシリコンチップ内に保護された重要データへの不正アクセスを拒否する機能を備えているため、この TPM のプラットフォーム上のアプリケーションはすべて、常にセキュアに保つことができる。

＜主なベンダの動き＞

Intel 社、Amtel 社、Infineon 社などの世界的半導体ベンダは TPM に準拠したシリコンチップを開発しており、これらのシリコンチップは IBM 社や Hewlett-Packard 社の PC にすでに搭載されている。中でも IBM 社関係者によると、同社は 2004 年夏以降に製造される同社のラップトップ「Thinkpad」はすべて、TPM ベースのシリコンチップを実装しているという。

＜トラステッドコンピューティングの課題＞

一方、トラステッドコンピューティングを批判する声もある。主な批判内容は、TPM による厳重なシステム制御によってユーザが自由にシステムを調整するできなくなる、または、他の機器やソフトウェアとの相互運用が困難になるといったものである。これに対して、TCG はこのような複雑な問題解決に取り組むためにも、国土安全保障省、EU インターネットデータ保護局、ドイツ省庁などとも定期的に会合を開き、外部者からフィードバックを基にベストプラクティスの開発を試みている。

（参考資料）

http://www.cert.org/stats/cert_stats.html
http://www.cert.org/annual_rpts/cert_rpt_03.html#incident
http://news.com.com/2100-1028_3-5195222.html?tag=st.lh
http://www.eweek.com/article2/0,1759,1636359,00.asp
http://www.computerworld.com/printthis/2004/0,4814,92784,00.html
http://www4.gartner.com/5_about/press_releases/asset_71087_11.jsp
http://www.antiphishing.org/APWG_Phishing_Activity_Report-Oct2004.pdf
http://www.staysafeonline.info/news/safety_study_v04.pdf
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf
http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss426_art696,00.html
http://www.fas.org/irp/offdocs/eo/eo-13231.htm
http://www.fas.org/irp/offdocs/eo/eo-13286.htm
http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
http://www.dhs.gov/dhspublic/display?content=916
http://www.dhs.gov/dhspublic/display?theme=52
http://www.us-cert.gov/aboutus.html
http://www.dhs.gov/dhspublic/display?content=3086
http://www.dhs.gov/interweb/assetlibrary/OIG_CyberspaceRpt_Jul04.pdf
http://www.eweek.com/article2/0,1759,1669892,00.asp?kc=EWRSS03119TX1K0000594
http://www.eweek.com/article2/0,1759,1679514,00.asp
「CyberSecurity Chief Quits」（Information Week, 10/4/2004）
http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A17694-2003Mar12&notFound=true
http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A52162-2003Apr18&notFound=true
http://www.washingtonpost.com/wp-dyn/articles/A28019-2004Oct12.html
http://www.cybersecurityinstitute.biz/forensics.htm
http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3145543.htm
http://www.usdoj.gov/dojorg.htm
http://www.usdoj.gov/criminal/Cdorgch.htm
http://www.cybercrime.gov/ccips.html
http://www.cybercrime.gov/mantovaniIndict.htm
http://www.cybercrime.gov/chang_sent.htm
http://www.cybercrime.gov/mitchellSent.htm
http://www.usdoj.gov/criminal/cybercrime/chips101904.htm
http://www.fbi.gov/priorities/priorities.htm

http://financialservices.house.gov/media/pdf/040303jf.pdf
http://www.govexec.com/dailyfed/0402/040802td1.htm
http://www.fbi.gov/aboutus/todaysfbi/orgchart.pdf
http://www.cert.org/tech_tips/FBI_investigates_crime.html
http://www.rcfl.gov/downloads/documents/intro_to_RCFLs.doc
http://www.fbi.gov/pressrel/pressrel04/forensic040104.htm
http://www.ifccfbi.gov/index.asp
「Operation Cyber Sweep; FBI team cracks down on high-tech crime」(EL Paso Time)
http://www.usdoj.gov/opa/pr/2004/April/04_crm_263.htm
http://www.usdoj.gov/opa/pr/2004/August/04_crm_583.htm
http://www.usdoj.gov/ag/speeches/2004/82504ag.htm
http://www.reform.house.gov/UploadedFiles/Computer%20Security%20Report%20card%202%20years.pdf
http://www.whitehouse.gov/omb/memoranda/fy04/m04-25.pdf
http://www.ssa.gov/oig/ADOBEPDF/A-14-04-14040.pdf
http://www.epa.gov/oigearth/reports/2004/20040930-2004-S-00007.pdf
http://www.ig.doe.gov/pdf/ig-0662.pdf
http://www.securitymanagement.com/library/Yankee_EnterpriseSecurity0604.pdf
http://www.infonetics.com/resources/purple.shtml?upna04.wireless.nr.shtml
http://www.airdefense.net/newsandpress/11_08_04.shtm
http://www.computerworld.com/securitytopics/security/story/0,10801,94107,00.html
http://www.iapplianceweb.com/story/OEG20031202S0019.htm
http://www.softwaremag.com/L.cfm?Doc=2004-11/2004-11endpoint-security
http://www.networkingpipeline.com/news/49901778
https://www.trustedcomputinggroup.org/about/members/members
https://www.trustedcomputinggroup.org/about/faq/
http://www.computerweekly.com/Article117449.htm
http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php

このレポートに対するご質問、ご意見、ご要望がありましたら、
hiroyoshi_watanabe@jetro.go.jpまでお願いします。