「米国企業における情報セキュリティ・ガバナンス」

渡辺弘美@JETRO/IPA NY

1. 増える企業のセキュリティ投資

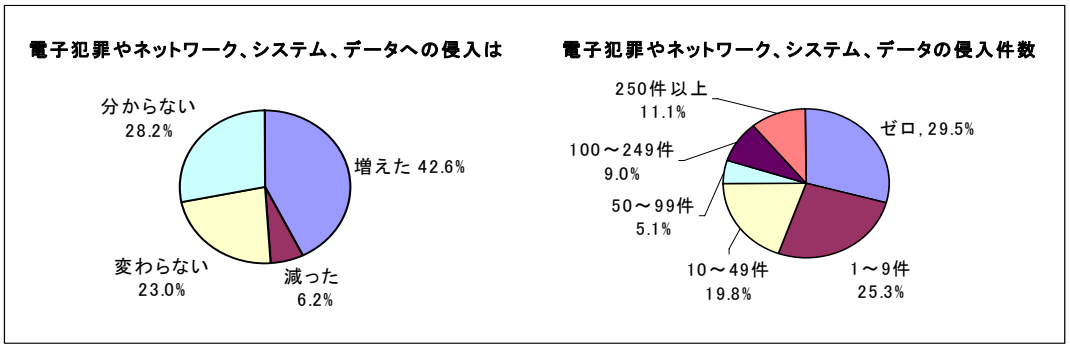
ウィルスやワームによる攻撃、サービス妨害（DoS）、顧客データの窃盗などの電子犯罪は毎年深刻さを増している。加えて、連邦や州政府によって、企業のセキュリティ強化を求める関連規制も増えている。こうした背景を受けて、米国企業は情報セキュリティ対策を引き続き最重要課題として認識し、セキュリティ関連投資を拡大し続けてきている。

(1) 増加するセキュリティ上の脅威

① 電子犯罪の増加

CSO Magazine（CSO Online）は 2004 年 4 月、米国シークレット・サービス（Secret Service）、CERT Coordination Center（CERT/CC）とともに、米国の企業や機関を中心に、電子犯罪に関する包括的な調査を行なった。この調査結果「E-Crime Watch」によれば、回答企業・機関の 42.6%が「電子犯罪は増加している」と回答しており、「減少した」と回答したのはわずか 6.2%である。また、回答企業・機関の約 7 割が、少なくとも 1 回以上、電子犯罪による攻撃を受けたと回答しており、平均で 136 件の攻撃を受けたとされている。

電子犯罪やネットワーク、システム、データへの侵入



さらに今年に入ってから、こうした電子犯罪の深刻さを浮き彫りにするような事件が立て続けにおこっている。例えば、データ事業者大手の ChoicePoint 社（14 万 5000 件の顧客情報が盗まれた）、LexisNexis 社（最高で 31 万件の顧客情報が盗まれた）、Polo Ralph Lauren 社（一部のマスターカードを利用した顧客のうち、最高 18 万件の顧客情報が盗まれた）、通信大手 MCI 社（社員 1.7 万人の情報が盗まれた）、Bank of America 社（6 万件の顧客情報が社員によって盗まれ

た）、Wachovia 社（4.8 万件の顧客情報が社員によって盗まれた）など、さまざまな企業で顧客情報や社員情報（社会保障番号や免許証番号、クレジットカード情報など）の窃盗が発覚し、電子犯罪の脅威は社会問題化している（「ニューヨークだより 2005 年 4 月」参照）。

また、前述の「E-Crime Watch」の調査結果によれば、電子犯罪が外部者（非従業員、非契約者）または内部者（現・元従業員又は契約者）によって行なわれる割合は、外部者が 71.4%である一方、内部者による電子犯罪の割合も 28.6%となっており、内部者による電子犯罪の可能性が低くないことは注目に値する。

電子犯罪の内容については、「ウィルスまたはその他の悪質な攻撃」を受けた企業・機関が 77.2%と最も多く、サービス妨害（DoS）攻撃（43.6%）、違法なスパム・メール（38.3%）の順となっている（複数回答）。

電子犯罪の内容（複数回答）

電子犯罪の内容	回答率	電子犯罪の内容	回答率
ウィルスまたは悪質な攻撃	77.2%	その他の独自情報の窃盗	16.4%
サービス妨害（DoS）攻撃	43.6%	従業員の個人情報窃盗	12.0%
違法なスパム・メール	38.3%	内部者によるサボタージュ	10.8%
内部者による不正アクセス	35.7%	外部者によるサボタージュ	10.8%
フィッシング（Phishing）	31.0%	外部者による恐喝	3.2%
外部者による不正アクセス	27.2%	内部者による恐喝	2.6%
詐欺	21.9%	その他	11.1%
知的財産の窃盗	20.5%	不明	7.9%

② 被害の実態

こうした電子犯罪によって受けた被害の内容については、17%が「被害はなかった」と回答している。また、具体的に被害を受けた企業・機関の場合、その内容は、事業運営面での被害が 56.4%、財政的被害が 24.6%となっている。2003 年の電子犯罪による被害額は合計 6 億 6600 万ドルと試算されている。

電子犯罪による被害額

被害額	割合
10 万ドル未満	26.3%
10 万～50 万ドル未満	11.2%
50 万ドル～100 万ドル未満	5.0%
100 万ドル～1000 万ドル未満	5.0%
1000 万ドル～1 億ドル未満	2.4%
1 億ドル以上	0.3%
不明	49.7%
平均値	392 万ドル
中央値	10 万ドル
合計（各層の中間点を使って算出）	6 億 6600 万ドル

（2） セキュリティ強化を迫る各種法規制の動向

情報セキュリティ問題が深刻な懸念となるのに伴い、米国の連邦政府および州政府は、企業の情報セキュリティに一定の基準を設け、それに違反した場合は、厳しい罰則を科す規制をいくつか導入している。こうした規制のコンプライアンスも、企業の情報セキュリティ関連投資を加速する要因となっている。Price Waterhouse Coopers 社の Jerry Lewis 氏は、「政府による規制へのコンプライアンスや損害賠償の可能性が、企業の情報セキュリティ強化の大きな要因となっている」と指摘している。

例えば、企業の情報管理に影響を及ぼす法律としては、企業責任の厳格化や情報開示の強化を定めた企業改革法（通称：サーベインズ・オクスレー法、対象は公開企業）がある。また、州レベルでは、カリフォルニア州が 2003 年に、顧客の個人情報が侵害された場合やその可能性がある場合は、顧客に通知することを義務付けた California Security Breach Information Act（通称：SB136、civil code 1798.82）を成立させている（「ニューヨークだより 2005 年 4 月」参照）。

情報セキュリティに関連する法律

法律名	概要（情報セキュリティ関連部分）	対象となる企業・機関	懲罰
企業改革法（Sarbaines-Oxley Act of 2002）	投資家などへの情報開示の正確性の強化。	米国で株式公開している企業	刑事罰および民事罰
GLB 法（Gramm-Leach-BilleyAct of 1999）	顧客情報に関するプライバシー・ポリシーを策定し、定期的に顧客に開示しなくてはならない。	米国内の金融機関	刑事罰および民事罰
HIPAA 法（Health Insurance Privacy and Accountability Act、医療保険の携行性と責任に関する法律）	カルテの電子化。患者の個人情報や医療情報のセキュリティ強化。	米国内の医療機関	民事罰金および刑事罰
California Security Beach Information Act （SB 1386, civil code 1798.82）	暗号化されていない顧客情報が侵害された場合またはその可能性がある場合、企業・機関は顧客へ通知しなくてはいけない。	州政府機関および州内で事業を営む企業	民事罰金および、個人が訴訟する権利
連邦情報セキュリティ管理法（Federal Information Security Management Act：FISMA）	連邦政府機関における情報セキュリティの強化。	連邦政府機関	IT 予算の喪失

さらに現在、連邦議員の間では、連邦政府として電子犯罪対策に取り組むべきではないかという議論も起きている。カリフォルニア州選出の Diane Feinstein 上院議員（民主党）は、2005 年 1 月、California Security Breach Information Act を基礎とした法案を連邦議会に提出している（現在、上院司法委員会にて審議中）。また、下院国土安全保障委員会（House Homeland Security Committee）の経済セキュリティ・インフラストラクチャー保護・サイバーセキュリティ小委員会（Economic Security, Infrastructure Protection and Cybersecurity Subcommittee）も、連邦レベルでの情報セキュリティ対策の必要性を検討している。

しかし、同小委員会の要請を受けて連邦レベルの取り組みの可能性について調査した議会調査局（Congressional Research Service: CRS）の報告書（2005 年 3 月）によれば、以下の 4 つの要素から、連邦レベルでサイバーセキュリティを強化しようとするのは現時点では難しいであろうと結論を出している。

- 連邦政府が情報セキュリティ強化のために規制や政策を制定し、その枠組みの中で、強化を実施していこうとすると、逆に市場のメカニズムによってサイバーセキュリティ技術を向上させることが難しくなる可能性がある。
- サイバースペースはグローバルなものであることから、関係機関との協調が難しい。
- サイバースペースの安全性を強化するための最善な方法に関してコンセンサスが存在していない。
- 技術的変化が早く、規制的枠組みを作ろうとする努力がそれに追いつかない。

議会調査局の同報告書では、このようなハードルはあるものの、もし連邦レベルで敢えて情報セキュリティに取組むとした場合、取り組みのモデルとして参考とすべきアプローチとして、以下の 2 つの前例を挙げている。

- コンピュータ 2000 年問題の際の対応
  証券取引委員会が企業に対して 2000 年問題対応に関する報告を義務付けるとともに、議会は、この義務付けを遵守した企業は賠償責任の保護を受けられる法案を可決した。

- 食品の安全性や環境に関する連邦規制
  連邦機関が規制を定め、遵守状況を監視する。議会調査局は、サイバースペース業界の規制当局候補として、国土安全保障省を挙げている。

（3）　IT 投資対象として注目されるセキュリティ関連の投資

増加するセキュリティ問題や、企業へのコンプライアンス関連規制などが増えるにつれて、情報セキュリティ対策の必要性に対する認識が企業幹部の間でも着実に高まっている。

調査会社 Gartner 社が、米国を中心に世界の 1300 人の CIO（Chief Information Officers: 最高情報責任者）を対象に行なった調査によれば、2005 年におけるテクノロジー面の優先案件として「セキュリティ強化」がトップになっている。また、ビジネス全体の優先案件においても、「セキュリティ対策全般」「データ保護およびプライバシー対策」がそれぞれ 2 位、5 位にランキングされている。

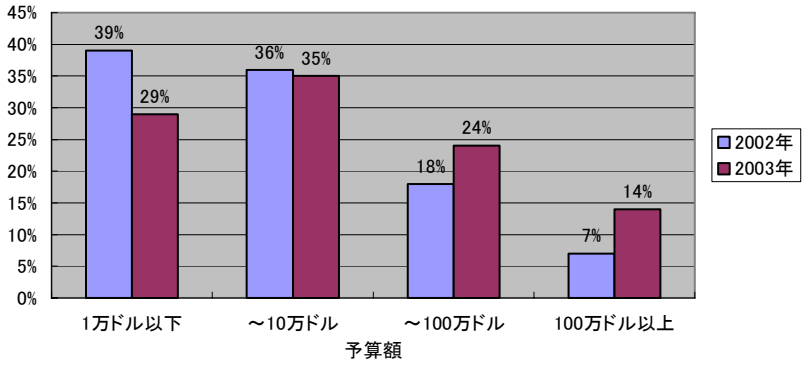
2005 年におけるビジネスおよびテクノロジー上の優先案件

順位	ビジネス上の優先案件	テクノロジー上の優先案件
1	ビジネス・プロセスの改善	セキュリティ強化ツール
2	セキュリティ対策全般	ビジネス・インテリジェンス・アプリケーション
3	企業全体の事業コストの見直し	モバイル・ワークフォースの強化
4	競争上有利な点の強化	ワークフロー管理の整備
5	データ保護およびプライバシー対策	ERP のアップグレード
6	収入増加	ストレージ管理
7	製品やサービスの知的利用	IP を使った音声およびデータ送受信の統合
8	内部統制の強化	CRM
9	ビジネス・スキルの補強	ビジネス・プロセスの統合ツール
10	技術革新およびサイクルのスピードアップ	サーバ仮想化技術

このような懸念を反映し、企業による情報セキュリティへの投資の増加はなお続いている。CSO Onilen、CIO Mgazne、Price Waterhouse Coopers 社が米国企業を中心に約 55 カ国の企業の約 8000 名の情報セキュリティ幹部を対象とした調査年次レポート「情報セキュリティの現状 2003 年版（The State of Information Security, 2003）」によれば、情報セキュリティの予算が 1 万ドル未満の企業は 2002 年の 39%から 2003 年には 29%へ減少したのに対し、高額予算を充てる企業の割合が増加している。この増加傾向は 1990 年代後半から続いており、情報セキュリティ予算は拡大傾向にある。

同年次レポートの最新版（2004 年版）によれば、2004 年の情報セキュリティ予算を増やすとの回答が全体で 64%に達しており、前年に引き続き増加傾向にある。ただし、2003 年と異なり、情報セキュリティ予算を「少し増やす」と回答した企業の割合が 56%と過半数で 2003 年（45%）より多かったのに対し、「大幅（30%以上）に増やす」と回答した企業は 8%で 2003 年（17%）より減少しており、予算枠の増加率が安定に向かっていると見ることができる。

情報セキュリティ予算（2002 年、2003 年）



2. 情報セキュリティ・ガバナンス強化のフレームワーク

(1) 情報セキュリティ・ガバナンスの必要性

情報セキュリティに対する企業の関心が高まるなか、セキュリティ・ガバナンスのためのフレームワークの必要性が高まってきている。ソフトウェア業界団体のビジネス・ソフトウェア・アライアンス（Business Software Alliance: BSA）は、2003 年 10 月に発表した報告書、「情報セキュリティ・ガバナンス：行動のためのフレームワークに向けて（Information Security Governance: Toward a Framework for Action）」のなかで、現在の情報セキュリティを取り巻く環境のキーファインディングとして以下の 4 点を指摘し、フレームワーク構築の重要性を説いている。

① 政府による情報セキュリティに関する規制枠組み整備は十分である。

業界や消費者の間では、「情報セキュリティは重要である」との認識はすでに確立されており、企業や個人ユーザはより優れた情報セキュリティを望み、ベンダは、より優れたセキュリティ製品を提供する努力している。また、こうした懸念に応える形で、米国政府は情報セキュリティに関する法律を複数成立させてきた。政府による法整備努力はすでに十分である。今後、新たな法律や規制、さらには政府による関与が実施された場合、さらに高まるコンプライアンスの要求や、潜在的な賠償責任問題などへの対処コストが増大し、企業への負担増につながる可能性がある。また、企業や機関による情報システムや情報の危険性や複雑さはさまざまに異なるため、単一の法律や規制などによって情報セキュリティ全般を強化することは難しい。したがって、今後、政府による新たな規制を増やすよりむしろ、各企業で適切なリスク管理を実施することが最善の方法である。

② 情報セキュリティ問題は、単なる技術的問題として扱われることが多いが、実際にはコーポレート・ガバナンス問題として扱うべき問題である。

数々の法律や規制を見ても分かるように、情報セキュリティ問題は、単なる技術的問題ではなく、コーポレート・ガバナンスとしての問題である。情報セキュリティ問題は通常、CIO や CSO といった幹部の責任となる一方、CEO や役員会の強い関心を集める問題ではない。しかし、情報セキュリティ担当幹部の権限は限られており、複数の部署にわたって権限を行使できる立場にはないため、役員会や上級管理職全体による積極的な支援や関与が必要である。

③ 情報セキュリティ問題を解決するために何をすべきかという問題に関して、包括的な共通見解はまとまってきている。

これまでにさまざまなガイダンスやイニシアチブが発表されており、いずれも、セキュリティ・プログラムの管理体制やセキュリティ・チェックリスト、ベストプラクティスなどを提案しており、組織としてどのような対策を講じるべきかに関して共通の見解があることが分かる。しかし一方で、いずれも内容が具体的すぎるか、組織全体として実行するには無理がある内容となっており、組織全体で取り組む情報セキュリティ・ガバナンスの包括的なフレームワークを提示しているものはない。情報セキュリティに関する国際標準である ISO/IEC 17799 や連邦政府向けに制定された連邦情報セキュリティ管理法（FISMA）は、情報セキュリティ・ガバナンスのフレームワーク作りに効果的な土台となり得るが、ISO/IEC17799 は CEO の役割に集中し過ぎており、FISMA は連邦機関のみを対象としている。

④ 情報セキュリティに進展が見られない理由は、情報セキュリティ・ガバナンスのためのフレームワークが欠落しているためである。

情報セキュリティを強化するためのさまざまなソリューションが提案され、情報セキュリティに関する共通見解も存在するものの、情報セキュリティに進展が見られないのは、民間の企業や機関が即座に利用できる情報セキュリティ・ガバナンスのフレームワークが欠落しているためである。ガバナンスには、情報セキュリティ機能を組織的に実施および監督することが必要である。そのため、ベストプラクティスを提案するだけでは不十分であり、それを組織として効果的に導入するためのガバナンス・フレームワークと組み合わせることが重要なのである。

(2)　情報セキュリティ・ガバナンスのフレームワークの例：NCSP

最近では、情報セキュリティ・ガバナンスのためのフレームワークがさまざまな機関によって発表されている。ここでは具体的な例として、全米サイバーセキュリティ・パートナーシップ（National Cyber Security Partnership: NCSP）のコーポレート・ガバナンス作業部会（Corporate Governance Task Force）が 2004 年 4 月に発表した「情報セキュリティ・ガバナンス：行動の呼びかけ（Information Security Governance: A call to action）」によるフレームワークの内容について概観する。

なお、NCSP は、サイバーセキュリティや重要情報インフラの強化を目的として 2003 年 12 月に設立された官民パートナーシップであり、ビジネス・ソフトウェア・アライアンス(BSA)、米国情報技術協会(Information Technology Association of America: ITAA)、IT 企業の経営幹部達で構成されるテックネット（TechNet）、米国商工会議所（U.S. Chamber of Commerce）などが構成メンバーとなっている。

同フレームワークは、企業における情報セキュリティ・ガバナンスの目的を明らかにした上で、具体的に、セキュリティ・ガバナンスを実施するための企業内役職別の責任及び役割、部門別セキュリティ対策プログラムの実施法及びその報告・評価について言及している。また、フレームワーク実施のための参考モデルとして、カーネギーメロン大学 SEI (Software Engineering Institute) による IDEAL モデルについて紹介している。

①　情報セキュリティ・ガバナンスの目的

企業の情報セキュリティ・ガバナンスとは、不当な利用、開示、混乱、修正、破壊から情報や情報システムを保護し、情報の機密性（confidentiality）、信頼性（integrity）、有用性（availability）を確保することである。

情報セキュリティ・ガバナンスの目的

- 機密性（confidentiality）：情報が持つ機密性を適切に保護する。
- 信頼性（integrity）：不当な情報修正や破壊から情報を保護するとともに、不当な否認防止や情報の信憑性を確実にする。
- 有用性（availability）：情報へのタイムリーで信頼性の高いアクセスや利用を確実にする。

②　役職別責任と役割分担

企業が情報セキュリティ・ガバナンスを導入する際には、役員会や企業の上級幹部、管理職、従業員など、各レベルに応じた役割や責務を明確にすることが重要である。各レベルにおける役割や責務は、以下のようにまとめることができる。

情報セキュリティにおける社内の各役割と責務

レベル	役割や責務
取締役会またはそれに類するガバナンス部門	役員会またはそれに類するガバナンス部門の者は、情報セキュリティに関して戦略的監督を行なうこと。戦略的監督を行なうには、以下の点が重要である。 ・ 情報や情報セキュリティが組織にとって非常に重要な要素であることを理解する。 ・ 情報セキュリティに対する投資を、組織戦略やリスク管理と組み合わせて監査する。
上級エグゼクティブ（CEO）	上級エグゼクティブとはおもに、役員会（またはそれに類するガバナンス部門）への報告義務を持つ CEO であり、組織全体の包括的な情報セキュリティ・プログラムを監督する。 ・ 情報セキュリティ・プログラム上のさまざまな機能の責務、説明責任、権限を、組織内の適切な人材に任命する。 ・ 情報セキュリティ・プログラムが適切に遵守されているかどうか監督する。 ・ 情報セキュリティ・プログラムの遵守状況および、残っているリスクの危険性や情報セキュリティ・プログラムの重大な欠点とその対処方法について、役員会に適切な報告を行なう。 ・ 情報セキュリティ・プログラムを遂行する上級情報セキュリティ責任者を任命する。責任者には、専門的知識を持ち、豊富な教育や訓練を受けた者とし、情報セキュリティ部門のトップとしての使命と資金を与える。
上級情報セキュリティ責任者（CSO = Chief Security Officer）	CEO への報告義務を持つ上級幹部は、情報セキュリティに関する社内の方針や慣行状況を監督する。 ・ 情報セキュリティの方針、原則、ガイドラインの作成や導入を監督する。 ・ 情報セキュリティの管理プロセスが組織戦略や事業計画に合致しているか監視する。 ・ 情報セキュリティの方針や手続きが、それらに関連する情報管理の方針や手続きと一致するよう調整する。 ・ 企業（またはその代理）によって運営されている情報や情報システムが、不当な使用や開示、混乱、修正、破壊による影響を受けた場合のリスクや被害に見合った情報セキュリティ保護策を講じる。 ・ 各部門による情報セキュリティ・プログラムの開発、維持を監督する。 ・ 上級情報セキュリティ担当幹部やその他の部門長が、CEO へ、情報セキュリティ・プログラムの効果や矯正策の進展状況について、定期的に報告を行なう。 ・ 各部門のマネジャーが抱える情報セキュリティの責任に関して、上級情報セキュリティ担当幹部が適切な支援を行なう。

社内各部門の上級マネジャー	・ 情報または情報システムに対する不当な使用や開示、混乱、修正、破壊による被害の規模やリスクを評価する。 ・ リスク評価や情報セキュリティのリスクを許容範囲に削減する際、コスト評価に基づいた方針や手順を導入する。 ・ 情報や情報システムを保護するための適切な情報セキュリティ・レベルを判断する。 ・ 情報セキュリティのコントロール状況や技術を定期的にテスト評価する。 ・ 各部門が情報セキュリティ・プログラムを遵守するために、企業として十分な人事教育を行なっているかチェックする。 ・ 全従業員や契約労働者、情報ユーザが、情報セキュリティ・プログラムの遵守に関する責務を認識しているかチェックする。
全従業員、契約労働者、ユーザ	・ 社内の情報セキュリティの方針、慣行および関連するガイダンスを理解する。 ・ 情報および情報システムに関するセキュリティの方針や手続きを遵守する。 ・ セキュリティやセキュリティ方針に影響する脆弱性やインシデントを適切な管理者へ報告する。

③　部門別セキュリティ対策プログラム実施におけるポイント

企業内の独立部門ごとに、情報セキュリティ・プログラムを開発、文書化し、導入することが重要である。また、そのプログラムには、以下のような点を盛り込むべきである。

- 不当な使用や開示、混乱、修正、破壊によって、情報または情報システムが受けるリスクや被害規模の定期的な評価。
- リスク評価やコスト評価に基づく、情報セキュリティのリスクを許容範囲に削減するための方針や手順。
- 各情報システムのライフサイクルを通して問題に対処する情報セキュリティ・プログラム。
- 企業としての方針や手順、その他の関連する法律や規制に合致すること。
- 必要に応じて、ネットワークや施設、システムなどに適切な情報セキュリティを提供するための代替プラン。
- 業務に伴う情報セキュリティのリスクや、企業の方針や手順に従うことの重要性を認識させる社員教育（契約者や情報システム・ユーザも含める）。
- 情報セキュリティの方針、手順、慣行の定期的な検査や評価。
- 情報セキュリティの方針や手順、慣行上の欠陥がある場合、その対処の検討方法。

- セキュリティ上のインシデントの探知、報告、対応方法（インシデントに伴うリスクの軽減方法、連邦または業界による情報セキュリティ・インシデント・センターや法規に基づく情報開示機関や当局への通知など）
- 事業や企業の資産を支える情報システムを継続的に運営するための計画や手順。

④　部門別セキュリティ対策プログラム実施報告及び評価

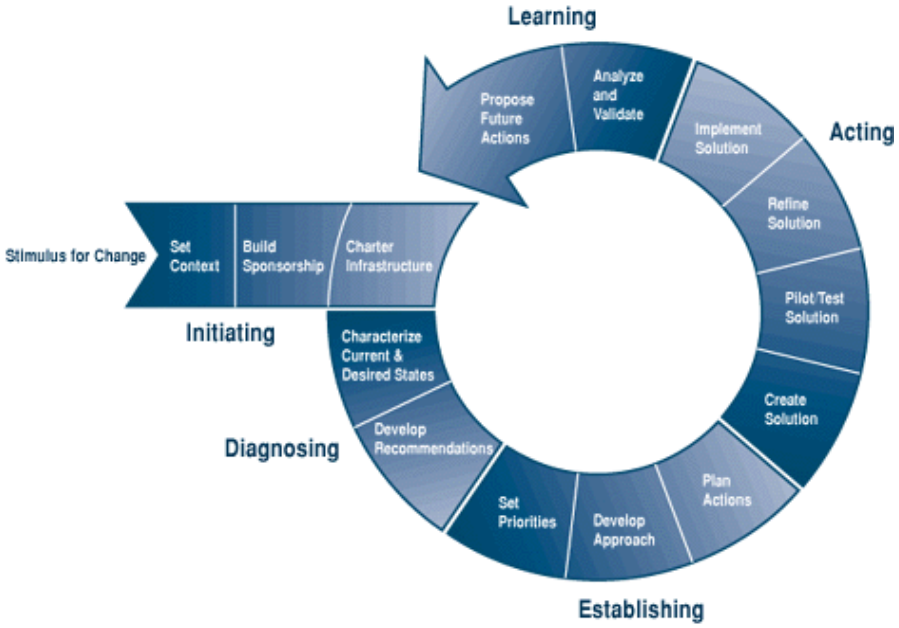
各部門はまた、以下のように適切な報告や評価を行なう。

- 情報セキュリティ・プログラムの妥当性や効果および、遵守状況に関して、上級幹部へ定期的に報告する。
- 部門の予算、投資、パフォーマンス計画などと照らし合わせ、情報セキュリティ・プログラムの妥当性や効果を分析する。
- 社内の情報セキュリティ慣行で見つかった重大な欠陥および、それへの対処方法、残っているリスクの見通しなどについて報告する。
- 上級幹部と相談の上、情報セキュリティ・プログラムを導入する上で必要な予算、人員、社員教育、スケジュール、予算などについて報告する。
- 情報セキュリティ・プログラムの導入によって影響を受ける関係者や機関に、タイムリーな通知をするとともに、意見提案の機会を提供する。

⑤　効果的な情報セキュリティ構築のための「IDEAL」モデル

企業がコーポレート・ガバナンスの一部として情報セキュリティ・プログラムを構築する上で、カーネギーメロン大学の SEI が開発した IDEAL モデルは非常に有効と考えられている。IDEAL モデルは本来、ソフトウェア開発の改善を目的として開発されたものだが、そのプロセスは、情報セキュリティにも利用できるものとなっている。IDEAL は、始動（Initiating）、診断（Diagnosing）、確立（Establishing）、行動（Acting）、学習（Learning）という 5 つのフェーズの頭文字であり、改善のためのロードマップを示すものとなっている。

IDEAL モデル



Initiating（始動）： 改善努力を成功させるための土台作り	Set Context（改善すべき内容を明確にする）
	Build Sponsorship（上級レベルのサポートを得る）
	Charter Infrastructure（変化を確立するための組織構造を明確にする）
Diagnosing（診断）： 目標の設定	Characterize Current & Desired States（現状および変化達成後の理想的状況を描写する）
	Develop Recommendations（現状と理想のギャップを分析し、ビジネス戦略に沿った勧告を決める）
Establishing（確立）： 目的を到達するための具体的な計画の策定	Set Priorities（変化を達成するための優先順位を決める）
	Develop Approach（アプローチ方法を決める）
	Plan Actions（アプローチ方法に基づき、具体的な計画を策定する）
Acting（行動）： 計画に基づき、実施	Create Solution（目的にあったソリューションを策定し、パイロット/テスト・グループを決める）
	Pilot/Test Solution（パイロット/テスト・プログラムを行い、フィードバックを集める）
	Refine Solution（フィードバックに基づき、ソリューションを改良する）
	Implement Solution（ソリューションを導入する）
Learning（学習）： 経験を次回に活かす	Analyze and Validate（より優れた導入のため、分析評価を行なう）
	Propose Future Actions（今後のための提言）

3. CSO 設置の状況とその効果

(1) CSO の職務と位置づけ

企業幹部の間で情報セキュリティ強化の必要性が高まるのに伴い、情報セキュリティ担当者の役割は、IT 部門という単一の部門でのセキュリティ担当から、企業のセキュリティ全般を管轄する役割へと拡大しつつあり、企業情報セキュリティ専門のセキュリティ担当幹部として、「最高セキュリティ責任者（Chief Security Officer: CSO）」という職務が重要視されつつある。

CSO が IT セキュリティのみを担当する企業もまだまだ多いものの、IT セキュリティに加えて、物理的なセキュリティや従業員や企業施設、資産などの安全確保も含め、企業のセキュリティ全般を担い、幹部としても上級の位置づけを得る CSO は着実に増えている。最近では、CSO のほか、最高情報セキュリティ責任者（Chief Information Security Officer: CISO）という役職を新設する企業も増えつつある（CISO と言った場合は、情報セキュリティ対策のみに専念する職務の場合が多いようである）。企業の情報セキュリティ対策に関わる役職としては、下記のような役職が挙げられる。

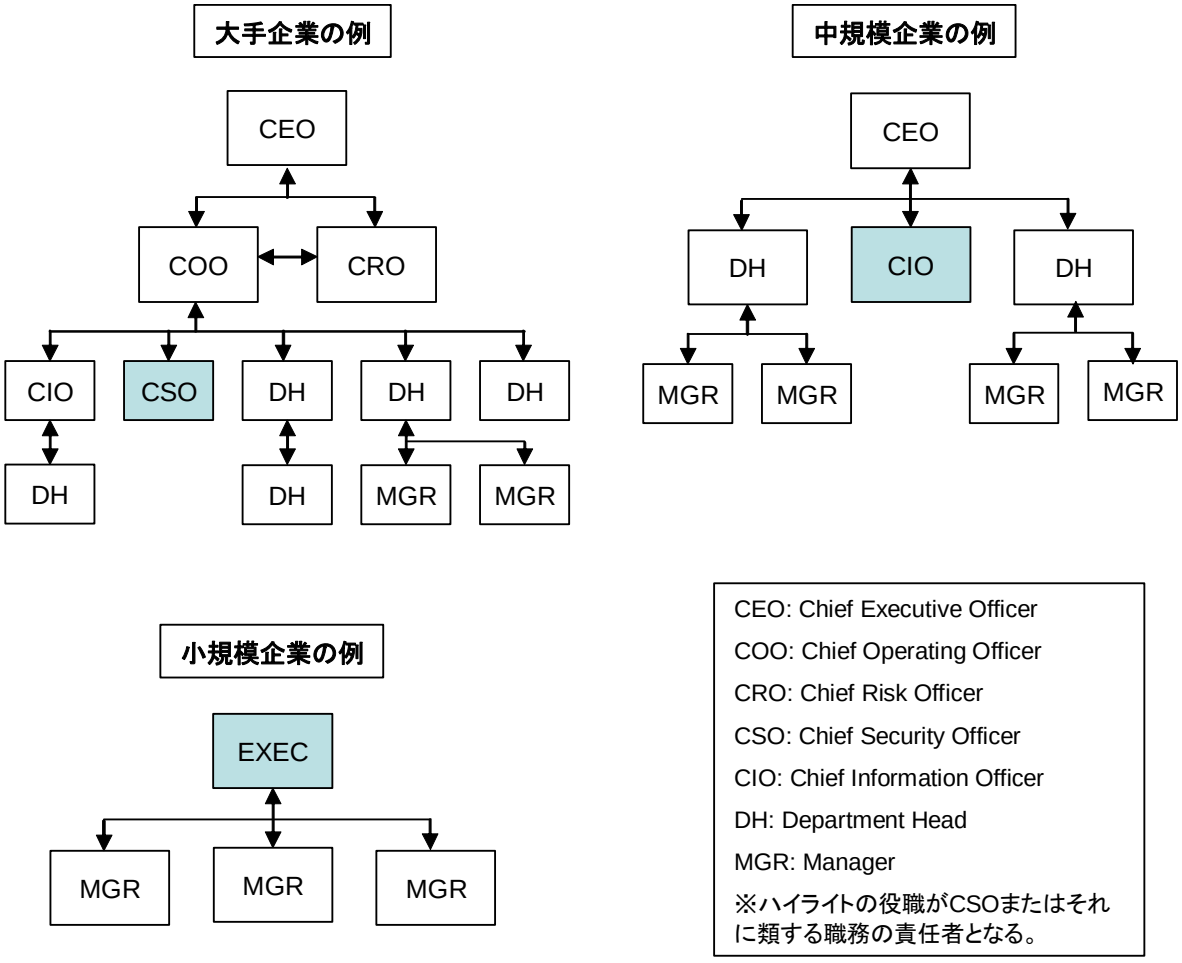
CSO およびそれに類する役職

- 最高セキュリティ責任者（Chief Security Officer: CSO）
- 最高情報セキュリティ責任者（Chief Information Security Officer: CISO）
- 最高情報責任者（Chief Information Officer: CIO）
- 最高プライバシー責任者（Chief Privacy Officer: CPO）
- 最高リスク責任者（Chief Risk Officer: CRO）

CSO（またはそれに類する役職、以下「CSO」と表記）が企業幹部として位置づけられている場合、CSO は、IT、人事、通信、法的面、施設管理など企業におけるセキュリティ対策全般を担当し、セキュリティのプログラムや基準の確立などを行なう。また、上級エグゼクティブ（最高経営責任者（Chief Executive Officer: CEO）、最高執行責任者（Chief Operating Officer: COO）、最高財務責任者（Chief Financial Officer: CFO）、法務部長など）に直接報告を行なう立場となる場合が多い。

前述した、全米サイバーセキュリティ・パートナーシップ(NCSP)のコーポレート・ガバナンス作業部会による「情報セキュリティ・ガバナンス：行動の呼びかけ」では、CSO の位置づけに関して、企業の規模別に、以下のような組織構造を提案している。

CSO およびそれに類する職務の位置づけ



CSO Online が 2004 年 9 月に発表した「グローバル情報セキュリティ調査（Global Information Security Survey）」（世界 62 カ国の 8100 社が回答）によれば、「過去 1 年に CSO や CISO の役職を新設した」と回答した企業は 31%に上り、2003 年版調査の 15%から大きく増加している。さらに、「中央管理化したセキュリティ管理システムを導入した」と回答した企業の割合は、2003 年の 11%から、2004 年には 39%と急増している。こうしたことから、コーポレート・ガバナンスとしての情報セキュリティや、それを担う CSO、CISO の必要性に対する認識は着実に高まっているといえよう。

(2) CSO の効果と課題

① 効果

CSO の新設を含め、企業の総合的なセキュリティ対策がプラスの効果を生んでいることが、前述の「グローバル情報セキュリティ調査」で明らかになっている。

同調査では、情報セキュリティ関連のインシデント数と、それによる被害について 2003 年と 2004 年で比較を行った。これによると、情報セキュリティ関連のインシデント数「ゼロ」とした企業が 2003 年は 35%、「1～9 件」と回答した企業が約 45%であったが、2004 年には「ゼロ」と回答した企業は約 20%に減少した一方、「1～9 件」と回答した企業は 55%と増えており、インシデント数自体は増えている。

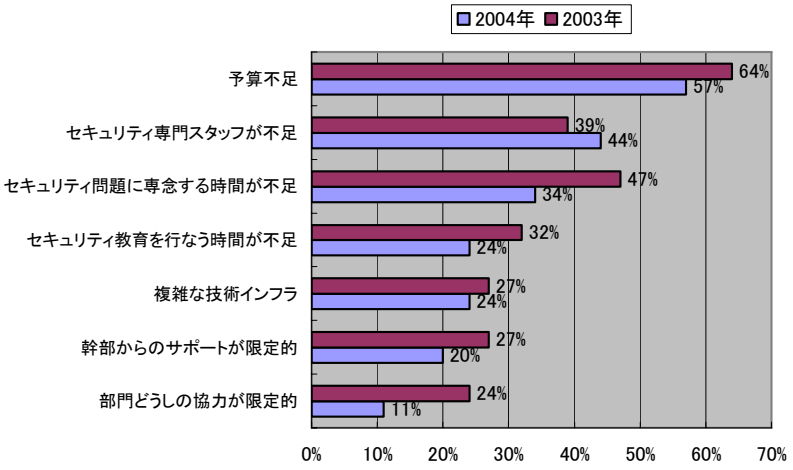
しかし、こうしたインシデントによって受けた被害となると、2003 年の調査では、ダウンタイム（不稼動時間）を「ゼロ」と回答した企業は約 25%、財政的被害を「ゼロ」と回答した企業は 30%未満であったが、2004 年の調査では、約 35%の企業が、ダウンタイム、財政的被害とも「ゼロ」と回答している。つまり、2004 年にインシデントの件数は増えたものの、実際の被害は減少しており、企業による情報セキュリティ対策が効果を上げていることが分かる。

こうした情報セキュリティ対策向上の主要因として、CIO Online は CSO の新設も含め、適切なインシデント対策、危機対策を講じている企業が増えたことを挙げている。また、エンドユーザに対する情報セキュリティ教育が普及しつつあることも主要因であるとしている。

② 課題

情報セキュリティをコーポレート・ガバナンスの一部としてとらえる企業が増え、CSO の認知度や必要性は高まっている。これにより、企業の情報セキュリティ担当幹部（CSO や CIO など）は、「優れた情報セキュリティを実施する上での障害」は減少傾向にあり、情報セキュリティの必要性は企業内で広く認識されつつあると言うことができる。

情報セキュリティを実施する上での障害（2003 年、2004 年）



しかし、一方で、「CSO は IT 部門の責任者」と認識している上級幹部も依然少なくはなく、CSO が企業全般のセキュリティ強化に取り組もうとする場合、予算や人材の面で壁に直面するケースも珍しくはない。上記の CSO Online 調査でも、一部の CSO は、「自分はしばしば、CSO や CISO として他者に紹介されるが、自分が報告するのはマネジャーであり、そのマネジャーはシニア・ディレクターへ報告し、シニア・ディレクターが CIO へ報告するといった具合で、実際には幹部や管理職の立場は与えられていない」、「『CSO は IT 部門担当』という社内の認識を変えるのは、小汚いボートを豪華なクイーン・メリー号に変身させるのと同じぐらい至難の業である」と、情報セキュリティをめぐる企業文化の変革の難しさを指摘している。

かつて「情報セキュリティ」とは、「事故やトラブルを発生させないことで価値が生まれる」という、ネガティブな見方が一般的であった。しかし、ネットワークや事業のグローバル化に伴い、情報セキュリティによって付加価値（企業の信頼性強化や事業拡大など）を生み出すというポジティブな見方を強調していくことが、CSO として成功する鍵であるといえよう。

4. 情報セキュリティに対する企業の取り組み

(1) 米国民間セクターによる取り組み

米国民間セクターでは、前述した CSO や CSIO を新設することによって、セキュリティ・ガバナンス体制を構築することに加えて、電子犯罪対策技術を導入したり、エンドユーザの教育、技術的対策などを通じて、情報セキュリティの強化に取り組んでいる。

① 電子犯罪対策技術

前述した「E-Crime Watch」報告書によれば、電子犯罪対策として最も多く利用されている技術はファイヤーウォールで、98.2%の企業・機関が導入している。ファイヤーウォールはまた、企業が考える「最も効果的な技術」の 1 位になっている。

電子犯罪対策として導入されている技術

技術	利用率
ファイヤーウォール	98.2
物理的なセキュリティシステム	94.2
手動パッチ管理	91.0
重要な伝送データの暗号化	85.4
アクセス・コントロール	85.4
侵入探知システム（人間による監視）	81.0
Information Assurance technology	76.4
自動パッチ管理	74.4
侵入探知システム（自動システムによる監視）	74.0
ストレージにある重要データの暗号化	70.8
ERP や会計部門との共同作業による詐欺防止技術	63.0
二因子認証システム	56.2
ワイヤレス監視	53.6
各ユーザのキー・ストロークの監視	39.4

最も効果的な技術		最も非効果的な技術	
ファイヤーウォール	71.3%	手動パッチ管理	23.1%
重要な伝送データの暗号化	63.0%	ワイヤレス監視	19.8%
・ストレージにある重要データの暗号化 ・二因子認証システム	55.9% 55.5%	各ユーザのキー・ストロークの監視	15.7%
侵入探知システム（自動システムによ	51.4%	自動パッチ管理	13.7%
物理的なセキュリティシステム	47.8%	Information assurance technologies	13.4%

② NCSP 「サイバーセキュリティ進展報告」

前述の全米サイバーセキュリティ・パートナーシップ(NCSP)は、2005 年 2 月、米国の民間企業がどのようにしてサイバーセキュリティ強化に取り組んできたか、またどのような成果を達成したかを調べるため、65 の民間企業・機関を対象にアンケート調査を行い、「サイバーセキュリティ進展報告（The National Cyber Security Progress Report）」として発表した。「サイバーセキュリティ進展報告」によれば、各企業の取り組み成果としては、以下のような進展があったとしている。

米国企業・機関による取り組みの成果

- 大規模なネットワーク侵入を探知するための能力や、早期警告システムを通じてサイバー上の脅威や攻撃パターンに関する情報交換の能力が拡大した。
- 業界内または業界同士でセキュリティ関連情報を共有するための仕組みが増えた。
- 情報セキュリティのベストプラクティスやユーザ教育、脆弱性や適切な対策に関する認識を普及させるためのガイダンスや白書などが数多く発表された。
- セキュリティ強化のための製品に大規模な投資を行う企業が増えた。
- オンライン・サービスの一環として無料でウィルス対策を提供するサービスが増えた。
- オンライン・セキュリティ・システムやアプリケーション・ソフトウェアを自動的に更新する機能が拡大した。
- サイバーセキュリティのリスクを軽減するため、ビジネス手法を大幅に変更する企業・機関が増えた。
- 複数の業界が、サイバーセキュリティの標準や測定基準、パフォーマンス基準を確立するため、共同で取り組んだ。
- サイバーセキュリティを分析、評価するための認定プログラムが創設された。
- サイバーセキュリティ強化のための研究所や共同研究、教育用ソフトウェア開発、大学レベルでの教育などが実施されるようになった。
- ウェブサイトなどによるサイバーセキュリティ普及活動が拡大した。

また、同報告書では、ブッシュ政権が 2003 年 2 月に発表した「サイバースペース・セキュリティのための全米戦略（National Strategy to Secure Cyber Space）」報告で提案されたサイバーセキュリティ強化 5 分野に沿って、各企業・機関の取り組みを紹介している。

ブッシュ政権が提案したサイバーセキュリティ強化 5 分野

①	サイバーセキュリティ対応システム
②	サイバーセキュリティの脅威および脆弱性を削減するためのプログラム
③	サイバーセキュリティに関する認識を普及させるための教育プログラム
④	政府機関のサイバースペースのセキュリティ
⑤	サイバーセキュリティに関する国際協力

以下は、同 5 分野に分けて、米国企業・機関の情報セキュリティ対策の例をまとめたものである。

米国企業・機関によるサイバーセキュリティ強化対策

企業・機関名	内　容
①サイバーセキュリティ対応システム	
Information Technology ISAC (IT-ISAC)	IT-ISAC（加盟メンバーに、セキュリティ情報をシェアする非営利組織）は、国土安全保障省などと協力し、信頼性のあるサイバーセキュリティ情報を 24 時間体制で共有するシステムを確立。
Symantec	早期警告システムや対応システムを盛り込んだ脅威管理システム「Deepsight」を開発。Symantec の Managed Security Services と組み合わせることで、顧客は、脆弱性や脅威に関する情報を早期に入手することができ、迅速かつ効果的な対応が可能になった。
Business Roundtable	米国大手企業の CEO および国土安全保障省長官の間で、緊急通信機能（CEO COM LINK）を創設。
②サイバーセキュリティの脅威および脆弱性を削減するためのプログラム	
AOL	セキュリティや安全性の強化に特化した新製品、AOL 9.0 Security Edition を発表（2004 年 11 月）。AOL ユーザは、McAfee VirusScan（ウィルス保護プログラム）、AOL Spyware Protection および SpyZapper（スパイウェア対策）、McAfee Personal Firewall Express（高速通信ユーザ向けファイアウォール）などのセキュリティを無料で受けられる。
Cisco Systems	セキュリティ強化のためのソリューション「Self-Defending Network（SDI）」を開発（2003 年）。SDI は、「セキュア・コネクティビティ・システム」（暗号機能や認証機能を使い、あらゆるネットワーク上で確実な伝送を確保する）、「脅威防衛システム」（セキュリティ・ソリューションとインテリジェンス・ネットワーク技術により、内外からの脅威を判別、軽減する）、「信頼認識システム」（ネットワークに認識、認証、セキュリティ機能をもたせることで、ネットワークのセキュリティを強化する）のシステムで構成される。
VISA USA	Visa、MasterCard、American Express、Discover、Diners Club のカード会社は、小売店や第三機関に対するデータセキュリティ条件を統一することで合意、カード決済業界データセキュリティ基準（Payment Card Industry Data Security Standard）を確立した。
③サイバーセキュリティに関する認識を普及させるための教育プログラム	
Information Technology Association of America (ITAA)	「Information Security Awareness Certification」（オンラインテスト）を開発。このオンラインテストを利用することで、企業は、平均的な従業員の情報セキュリティに関する認識度を測定することができる。テストに合格した企業には、ITAA から認証が与えられる。
United States Chamber of Commerce	Internet Security Alliance、NCSP、100 社の小規模事業者と共同で、「スモールビジネス向けのサイバーセキュリティに関するコモンセンス・ガイド」を作成。ウェブサイトで掲示するとともに 2 万 5000 部を配布。
McAfee, Inc.	Anti-virus and Vulnerability Emergency Response Team や、企業セミナー、研修、オンラインセミナーなどを通じて、ホームユーザ、政府関係者、企業関係者などあらゆるユーザの情報セキュリティに関する認識を強化することに力を入れている。

④政府機関のサイバースペースのセキュリティ	
BearingPoint	国土安全保障省の運輸保安局による Transportation Worker Identification Credential プログラム（輸送機関労働者の身元を正しく認識するためのシステムの開発）の第 3 フェーズにおいて、BearngPoint はシステムインテグレータとして参加。
Center for Internet Security (CIS)	情報セキュリティの強化を目的に OS のベンチマークやセキュリティツールを作成している CIS の活動により、米空軍はパッチ・システムの経費を大幅に削減できた。CIS には、NIST、国土安全保障省、エネルギー省、IBM、シマンテックなどが参加。
⑤サイバーセキュリティに関する国際協力	
Carnegie Mellon University CyLab	サイバー技術の向上を目的とする CyLab は、アウトリーチ活動の一環として、韓国や日本の関係者と協力し、CyLab Korea、CyLab Japan を発足。次世代のインシデント対応システムやオンデマンド式の脆弱性分析システムの共同開発に取り組んでいる。
RSA Security	欧州、米国、日本で業界向け情報セキュリティ・フォーラムを開催。官民の情報セキュリティ専門家が情報交換やネットワーク作りを行なう場を提供している。

(2)　官民連携によるサイバーセキュリティ技術の R&D 促進提案

ホワイトハウスの大統領 IT 諮問委員会（President's Information Technology Advisory　Committee: PITAC） は、本年 2 月 28 日にブッシュ大統領宛に提出した報告書「Cyber Security: A Crisis of Prioritization （サイバーセキュリティ：優先すべき危機）」を発表し、米国 IT インフラのセキュリティは脆弱であり、サイバーセキュリティの強化のために、連邦政府は民間企業の研究開発に対して、研究助成、研究成果の共有、人材交流、連邦政府機関の研究成果の民間への技術移転などを積極的に行っていく必要があると提言した。

同報告書では、現在の米国のサイバーセキュリティに関して、4 つの観点から現状と勧告を以下のようにまとめている。

米国サイバーセキュリティの現状および勧告

①民間によるサイバーセキュリティ R&D への連邦助成	
＜現状＞ ・　民間のサイバーセキュリティ R&D は、短期的なものが多いため、連邦政府による長期的な助成が必要である。 ・　連邦政府助成は、長期的 R&D 助成から短期的助成へ、また民間 R&D への助成から国防・諜報関連の助成へと変化している。	＜勧告＞ ・　民間のサイバーセキュリティ R&D を強化するため、全米科学財団（NSF）の予算を 9000 万ドル増額する。 ・　国土安全保障省や国防総省を中心に、民間サイバーセキュリティ R&D への助成を増額する。

②サイバーセキュリティ基礎研究のコミュニティ	
＜現状＞ ・ サイバーセキュリティの専門家が非常に少ない（報告書では 250 名以下と試算）。 ・ サイバーセキュリティの基礎研究を行なう民間のコミュニティは規模が非常に小さい。	＜勧告＞ ・ 大学や研究機関でサイバーセキュリティを研究する教授や学生を増加させる努力をし、10 年以内にサイバーセキュリティ基礎研究のコミュニティを倍増する。 ・ 民間におけるサイバーセキュリティの基礎研究への支援を拡大する。
③研究を実際の製品にするための技術移転	
＜現状＞ ・ IT の R&D に対する長期的な連邦助成によって優れた技術移転が数々実現し、IT 業界は重要な産業へ成長した。 ・ しかしサイバーセキュリティ分野では、「事故が発生しなかった」という成果の評価が難しいため、技術移転がなかなか進まない。	＜勧告＞ ・ 民間とのサイバーセキュリティ技術移転に関する連携を強化する。 ・ 新製品やベストプラクティス評価のためのメトリックスやモデルなどの開発を重視する。 ・ 民間と共同でコンファレンスを開催し、サイバーセキュリティ研究の成果発表の場を作る。 ・ 業界による技術移転努力に助成を行なう。 ・ 連邦の助成を受けた学生が業界で経験を積むことを奨励する。
④連邦政府機関によるサイバーセキュリティ R&D の調整	
＜現状＞ ・ 現在の連邦機関全体におけるサイバーセキュリティ R&D は、研究項目やプログラムなどが調整されておらず、非効率的である。 ・ 各機関はそれぞれの役割や目的に専念してしまい、全体としてのニーズが見落とされがちである。	＜勧告＞ ・ 重要情報インフラ保護に関する省庁間ワーキンググループ（IWG/CIIP）を連邦サイバーセキュリティ R&D の調整役として機能させる。 ・ Networking and Information Technology Research and Development（NITRD）（省庁横断型の情報技術開発計画プログラム）がこれを支援する。

(参考資料)

http://www.csoonline.com/releases/ecrimewatch04.pdf
http://www.cccure.org/Documents/Governance/governance.pdf
http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
http://library.law.unc.edu/bankinglaw/glb_paper.pdf
http://aspe.hhs.gov/admnsimp/index.shtml
http://www.darwinmag.com/read/100103/calif.html
http://csrc.nist.gov/sec-cert/
http://www.fcw.com/article88407-03-25-05-Web
http://www.gartner.com/press_releases/asset_117739_11.html
http://www.csoonline.com/csoresearch/report64.html
http://www2.cio.com/research/surveyreport.cfm?id=75
http://www.bsa.org/resources/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=5841&hitboxdone=yes
http://www.cyberpartnership.org/InfoSecGov4_04.pdf
http://www.sei.cmu.edu/ideal/
http://www.csoonline.com/research/security_exec/cso_role.html
http://www.csoonline.com/read/090104/survey.html?action=print
http://www.itaa.org/infosec/docs/accomplishmentsbypriority.doc
http://www.hpcc.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

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。