「情報セキュリティ保険市場の動向」

渡辺弘美@JETRO/IPA NY

1. 増大する情報セキュリティ・リスク

近年、情報セキュリティに対する関心が高まっているにもかかわらず、情報セキュリティに関する事件や事故は多発かつ多様化している。さらには、こうした事件や事故が訴訟につながるケースも目立ち始めている。今年の春には大手企業による個人情報の漏洩事故が次々と明らかになり、情報セキュリティ・リスクの増大が指摘されるようになった。現在、企業には、より高度で包括的な情報セキュリティ対策が求められている。

(1) 相次ぐ個人情報漏洩事件

2005 年 3 月、信用調査会社チョイスポイント（ChoicePoint）は、自社のデータベースから約 14 万 5000 人の消費者の個人情報（住所、ソーシャルセキュリティ番号、クレジットカード情報）が漏洩したと発表した。その後、銀行のバンク・オブ・アメリカ（Bank of America）、情報サービス企業のレキシスネキシス（LexisNexis）、小売店のポロ・ラルフ・ローレン（Polo Ralph Lauren）などで次々と個人情報の漏洩が明らかになった。主な個人情報漏洩事件の被害内容や対策などは以下の通りである。

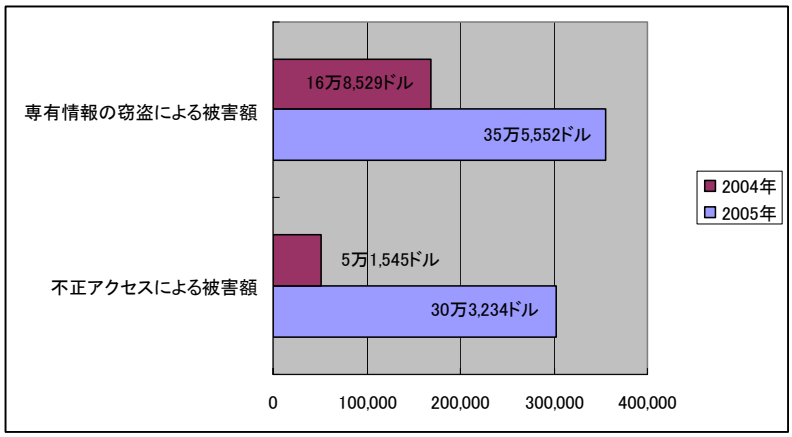
主な個人情報漏洩事件（2005 年春）

企業 (事件の公表月)	被害者数など	漏洩した データの内容	漏洩方法	対策
ChoicePoint（2 月）	約 14 万 5000 人。750 件の詐欺行為が発生	住所、ソーシャルセキュリティ（SS）番号、信用情報	正規顧客が情報を購入するフリをして情報を窃盗	連邦当局に報告。情報の売却先を制限。
Bank of America（2 月）	最大 120 万人（連邦職員向けカードの保有者）	SS 番号	バックアップ・テープの紛失	連邦当局および顧客へ通知。
DSW Shoe Warehouse（靴小売）（2 月）	最大 10 万人	クレジットカード情報、顧客の買い物履歴	ハッカーが、103 店舗のデータベースに侵入	連邦当局へ報告。顧客消費者にカード履歴の確認を奨励。

LexisNexis（3 月）	最大 31 万人。51 件の違法行為が発生	SS 番号、免許証番号	ログインとパスワードの不正使用による侵入	連邦当局および顧客消費者へ通知。セキュリティ強化。
Boston College（3 月）	12 万人（卒業生）	住所、SS 番号	外部機関が運営管理する大学のコンピュータにハッカーが侵入	該当する卒業生へ通知。
Polo Ralph Lauren（4 月）	最大 18 万人	クレジットカード情報	不明	取引銀行（HSBC）に連絡。同行が利用客へ通知。

また、コンピュータ・セキュリティ研究所（Computer Security Institute: CSI）と連邦捜査局（FBI）が毎年発表している『コンピュータ犯罪およびセキュリティに関する調査（Computer Crime and Security Survey）』の 2005 年版によれば、コンピュータ犯罪による被害額は、全体的には低下の傾向にあるものの、専有情報の窃盗と不正アクセスは増加傾向にあるという。専有情報の窃盗による被害額（1 社当たりの平均被害額）は、2004 年の 16 万 8529 ドルから 2005 年には 35 万 5552 ドルに、不正アクセスによる被害額（同）は、2004 年の 5 万 1545 ドルから 2005 年には 30 万 3234 ドルに急増している。

コンピュータ犯罪による被害総額



(2)　情報セキュリティ関連訴訟

一方、情報セキュリティを巡る訴訟も発生している。2001 年には、カリフォルニア州とニュージャージー州が、「玩具小売大手のトイザラス（Toys R Us）

が、ウェブサイト上で『個人情報は、トイザラス・ドット・コムや親会社、関連子会社以外には提供しない』と明記しているにもかかわらず、ウェブ分析を行う市場調査会社のコアメトリクス(Coremetrics)と契約し、トイザラスのウェブサイトにアクセスする消費者の個人情報を詳細に調査、分析させていることは、個人情報関連法に違反する」として、トイザラスとコアメトリクスを提訴した（コアメトリクスは、cookies やウェブバグなどを使って、トイザラスのウェブサイトへアクセスした者の動向を調査するとともに、これらの結果をトイザラスの顧客情報とあわせて利用客の分析を行っていた。訴訟はその後、トイザラスとコアメトリクスが和解金を支払うとともに、プライバシー方針を明確にすることで和解）。

前述のチョイスポイントのケースでも、カリフォルニア州に住むある女性が、事件直後に、チョイスポイントのずさんな管理によって極めて重要な個人情報が漏洩されとして、損害賠償金の支払いを求め、同社を提訴した。原告は、チョイスポイントは、ビジネス慣行について定めた州法（California Business and Professions Code Section 17200）などに違反すると主張している。また、本訴訟を、チョイスポイントが情報を保有していた消費者および情報漏洩の対象となった消費者を代表する団体訴訟として認めるよう要請している。情報漏洩によって実際に金銭的被害が発生していないため、被害を金額で示すことは非常に難しい。このため、損害賠償金を勝ち取るのは難しいのではないかといった指摘もあるが、情報漏洩事件が団体訴訟につながる可能性は、関係者の大きな注目を集めている。
同様の団体訴訟は、レキシスネキシスに対しても起きている。さらに、DSW の本社があるオハイオ州では州司法長官が、漏洩被害を受けた全ての消費者に対して直接書面による個別の通知を行うよう求めて、同社を提訴した（当時、DSW の発表によれば、被害を受けた消費者の約半分（70 万人）に個別の書面通知が行われることになっており、オハイオ州司法長官は、残りの 70 万人に対しても同じ措置を取るよう求めた）。

また、2004 年 3 月に、「会員（800 万人）のクレジットカード情報が漏洩した」と発表したディスカウントストア大手の BJ’s Wholesale Club は、その後、被害にあったクレジットカード保有者の口座閉鎖および新規口座開設などに伴う費用の負担を求める信用組合などから提訴された。さらに、連邦取引委員会（Federal Trade Commission: FTC）は、消費者保護の観点から、「BJ は、簡単に解明できるパスワードを使っているほか、ワイヤレス・ネットワークのセキュリティ、重要なデータの暗号化などを怠っている」と指摘、その後、FTC と BJ は、今後、20 年間にわたり、外部の監査企業によるセキュリティ評価を半年ごとに提出することなどを定めた合意命令書（consent order）を交わした。

個人情報漏洩事件が拡大するのに伴い、市民の関心は高まり、企業の賠償責任を問う声は大きくなりつつある。「ずさんな情報セキュリティに対する訴訟は、今後、ますます増えていくであろう」と、元司法省検察官で、現在は、セキュリティ監査企業の役員を務めるマーク・ラッシュ（Mark Rasch）氏は述べている。

(3)　各種法律による個人情報保護規定

情報セキュリティを巡る事故や事件が数多く発生し、企業はこれらの事故や事件を巡って消費者から訴えられるという問題に直面する一方、政府機関から法律違反で提訴されるというリスクも高まっている。連邦および州政府は、消費者や投資家保護の観点から企業の情報セキュリティ体制を義務付ける法律を次々と制定している。連邦レベルでこうした法律の代表的なものとしては、金融機関による個人情報の取り扱いを定めた「グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act: GLBA）」（金融機関に対して、消費者の金融情報の取り扱いに関するセキュリティとプライバシー管理を義務付け）、医療機関による個人情報の取り扱いを定めた「医療保険の相互運用性と説明責任に関する法律（Health Insurance Portability and Accountability: HIPAA）」（医療関連機関に対して患者情報の共有や暗号の利用を制限するとともに、プライバシーとセキュリティの保護を義務付け）、上場企業に適正な財務報告を義務付けた「企業改革法（Sarbanes-Oxley Act）」（株式上場企業に対して、財務報告に関連する内部コントロールを確実にし、正しい財務報告を行うことを義務付け）などがある。

一方、州レベルで、個人情報の漏洩に対策を講じようとする動きも出てきている。こうした動きの先駆けはカリフォルニア州で、2003 年に、個人情報が漏洩した可能性が発生した場合、企業は該当する州民に通知することを義務付ける法律が制定された。2005 年には、同州の法律を基にして作成された個人情報保護法がニュージャージー州で成立している。これらの法律の内容は以下の通りである。

- カリフォルニア州情報漏洩対策法（California Security Breach Information Act）：
  カリフォルニア州民の特定個人情報を電子的に保管している企業は、システムが侵害され、個人情報漏洩の可能性が発生した場合、該当する州民に通知しなくてはいけない。なお同州では 2003 年に施行された同法に続き、2004 年には、カリフォルニア金融情報プライバシー保護法（California Financial Information Privacy Act）が施行された。同法では、カリフォルニア州でビジネスを行う金融機関に対し、顧客（州民）の個人情報を資本関係のない第三機関と共有する場合、事前に書面による合意を得ることを義務付けている。

● ニュージャージー州個人情報保護法（New Jersey Identity Theft Protection Act）:
　カリフォルニア州情報漏洩対策法をモデルとした法律で、2005 年 9 月に成立、2006 年 1 月 1 日から施行される。個人情報（氏名、署名、ソーシャルセキュリティ番号、身体的特徴、住所、電話番号、パスポート番号、運転免許書およびその他身元を証明する証書の番号など幅広い）が漏洩した場合、漏洩発覚から 15 日以内に報告しなくてはならない。

　現在、カリフォルニア州の情報漏洩対策法を連邦レベルに拡大しようという動きもあり、議会では、個人情報漏洩対策に関する法律がいくつか提出されている。10 月 20 日には、上院司法委員会（Senate Judiciary Committee）が、1000 人以上の個人情報が漏洩した場合、情報の保有者に報告するよう義務付ける法案（S 1326）を承認している。同法案では、規定に違反した場合、最高 25 万ドルの罰金などが課されている。法案の草案者は、ジェフ・セッションズ（Jeff Sessions）（共和党、アラバマ州）上院議員であるが、同法案は、団体訴訟を起こせるのは州司法長官のみに限定するなど、カリフォルニア州選出のダイアン・ファインスタイン（Dianne Feinstein）上院議員（民主党）らが提案した法案に比べると、狭義の内容となっている。

2.　米国における情報セキュリティ保険の概要

(1)　注目を集め始めた情報セキュリティ保険

①　情報セキュリティ保険誕生の背景

　アンチウィルスやファイアウォールといった「ブロック型」のベーシックなセキュリティ技術の導入は大方普及し、よりセキュアなコミュニケーション体制の確立や高度な認証技術の利用など、企業の情報セキュリティ対策はその他の分野へと拡大しつつある。しかし、たとえこれらの最新技術を全て導入したとしても、リスクを完全になくすことは事実上不可能である。そこで企業は、リスクが発生した際に、経済的損失を補償するための保険、「情報セキュリティ保険」に注目しつつある（なお、情報セキュリティ保険には、他にも「ネットワーク・セキュリティ保険」「サイバー保険」「ハッカー保険」など、さまざまな名称が使われている）。

情報セキュリティ保険は、歴史の長い保険業界においては新しい保険であり、その登場は 1990 年代の後半とされている。当時、企業が顧客情報や企業情報などの大量のデータを電子的に管理するようになり、インターネットが商業手段として広く利用されてきたことから、偶発的事故や犯罪などによる経済的損失に対して何らかの保護策が必要であるとの考えが生まれ、企業幹部たちは、「保険」にこれらの役割を求めるようになった。しかし、従来型の保険では不十分な点も多く（後述参照）、新たに情報セキュリティを対象とした保険が開発されるようになったのである。

再保険会社大手のスイス・リー（Swiss Re）は 2000 年に発表した報告書『E ビジネスが保険業界にもたらす影響：変革へのプレッシャーとチャンス（The impact of e-business on the insurance industry: Pressure to adapt – chance to reinvent）』で、「（当時）台頭し始めた E ビジネスに伴うリスクの特徴ゆえ、新たなタイプの保険（情報セキュリティ保険）が必要とされている」と指摘した。同報告書が指摘した E ビジネスに伴うリスクとは、以下の 4 点である。

E ビジネスの台頭に伴うリスク

技術的リスク	E ビジネス技術の成長により、技術的欠陥（停電、システム不全、ウィルス感染やハッカー攻撃など）に影響される可能性が高まっている。
賠償責任に関するリスク	E ビジネスにより、賠償責任のリスクは増加する。 ・ インターネットは自動的に世界に情報配信されることから、各国の異なる法律に対応する必要がある。消費者保護に関する法律などは国によってさまざまである。 ・ 個人情報の保護はさらに強化する必要がある（消費者の信頼を失うほか、賠償責任を問われる可能性もある）。 ・ 特に新興企業においては、業務が賠償責任問題に発展する可能性が高い。
信用および財政面のセキュリティに関するリスク	B2B においては匿名性が高まることから、信用や財政面におけるリスクが高くなる。
事業上のリスク	アウトソーシングが進めば、さまざまなトラブルが生じる可能性がある。

② 情報セキュリティ保険市場

情報セキュリティ保険は登場から数年しか経っておらず、市場に関する詳細なデータは明らかになっていない。現在、情報セキュリティ保険の商品としては、AIG の netAdvantage、CNA Pro の CNA NetProtect 、Chubb の Cyber Security など、

さまざまな種類があり（後述参照）、そのうち最大手は AIG で、市場の 7 割を占めるとされている。

情報セキュリティ保険市場の今後の動向については、多くの者が「市場は今後、拡大し続ける」との見方で一致しているようである。保険会社大手 AIG の幹部は、「2001 年に 1 億ドル前後弱だった情報セキュリティ保険市場は、2007 年には少なくとも 10 億ドルに成長する」と述べている。

また、保険情報研究所（Insurance Information Institute: III）では、「情報セキュリティ保険市場は、2005 年までに 25 億ドルに成長する」と予測している。さらに、2005 年 6 月にハーバード大学の Kennedy School of Government で開催された情報セキュリティ経済に関するワークショップ（Workshop on the Economics of Information Security）の発表者の一人、ドレスデン工科大学のレイナー・ボーム（Rainer Böhme）氏によれば、「楽観派の予測では、2007 年までに 60 億ドル、慎重派の予測では 2009 年ごろまでに 20 億ドルに成長する」との見方が示された。

前述の CSI と FBI が 2005 年に発表した報告書『コンピュータ犯罪およびセキュリティに関する調査』によれば、回答企業・機関（652 社）のうち、「情報セキュリティを強化するため保険を利用している」と回答した企業・機関はわずか 25%であった。しかし、同報告書は、「2005 年の調査結果は、情報セキュリティ保険がまだ勢いづいていないことを示しているものの、多くの関係者が、状況は今後変わっていくと考えている」と述べている。

③　情報セキュリティ保険に関する政策動向

かつて、ホワイトハウスで情報セキュリティ担当特別補佐官を務めていたリチャード・クラーク（Richard Clarke）氏は、情報セキュリティ保険の利用を積極的に推進していた。クラーク氏と保険業界との間で情報セキュリティ保険の推進に関する話し合いがしばしばもたれ、情報セキュリティ保険の問題点を検討する官民ワークショップの検討などが行われていた。さらに、2003 年に発表された『サイバーセキュリティ国家戦略（National Strategy To Secure Cyberspace）』の暫定版では情報セキュリティ保険の積極的な導入を推進する項目が盛り込まれた。しかし、クラーク氏が 2003 年 1 月に辞任した後、2 月に発表されたサイバーセキュリティ国家戦略の最終版では、情報セキュリティ保険に関する項目は見られなかった。また、クラーク氏に続いて情報セキュリティ保険の推進を行う人物はおらず、連邦政府による情報セキュリティ保険の奨励は小休止となっている。

一方、民間団体から情報セキュリティ保険の重要性を喚起する動きが出てきている。電気業界連盟（Electronic Industries Alliance: EIA）と、カーネギーメロン大

学の CyLab のコラボレーションによって発足した非営利団体であるインターネット・セキュリティ・アライアンス（Internet Security Alliance: ISAlliance）は、2004 年 3 月、『小規模事業者向けのサイバーセキュリティに関するガイド（Common Sense Guide to Cyber Security for Small Businesses）』を発表し、「情報セキュリティのための取り組み」として 12 の奨励項目を挙げた。この中で、11 番目の奨励項目として「セキュリティ財政リスク管理計画を確立、推進するとともに、適切な保険を利用すること」を推奨している。また別の項目の中でも、現在利用している保険が、データや情報システム、知的財産保護などをカバーしているかどうか確認するよう奨励しており、今後、関連の動きが活発化する可能性がある。

(2)　情報セキュリティ保険の補償対象

①　従来型事業保険では保障されない事例（サイバー倒産）

事業をしているほとんどの企業が、何らかの保険を利用しているが、E ビジネスに関連して発生した事故やトラブルは、従来型の事業保険では補償されていないことが多い。しかし、このことに気づくのは実際に事故やトラブルが発生した後で、補償を得られず事業閉鎖に追い込まれる、という最悪のケースもある。

オンライン小売業者 Viznet の元従業員は、同社のコンピュータ内にあるデータにアクセスしてダメージを与えた上、同社の顧客に「Viznet は小児愛グループの偽の姿である（経営者の妻が託児所を運営していた）」との電子メールを大量に送りつけた。財政および信用面で大きな被害を受けた ViZnet は、データや企業信頼の回復に巨額の費用を要したため、契約していた保険会社に連絡して、これらの被害総額（合計 34 万ドル）の補償を求めたところ、「契約していた保険ではサイバー上の補償は含まれていない」として支払いを拒否された。結局、経営者は事業の売却に追い込まれたという。

AIG の netAdvantage のパンフレット中で、従来型事業保険では保障されない可能性が高い情報セキュリティ関連事項として説明されているものを次に示す。

従来型事業保険では保障されない可能性が高い情報セキュリティ関連事項

データや非物理的資産のリスクは、従来型の保険における「資産」の対象とはならないことが多い。
従来型保険の職業賠償責任（errors and omissions）では、「意図的な行為」を対象外としており、組織関係者によるサイバー攻撃が行われた際、補償の対象外となる。
これまでの訴訟判決では、「データは有形資産ではない」との意見が支持されており、第三者における電子データの窃盗や破損を起因とする賠償責任は、通常の企業総合賠償責任保険（Commercial General Liability: CGL）では補償されないことが多い。
一般的に、CGLは、ウェブサイトのコンテンツによる個人的事故や広告に関する事故の補償を限定している。
従来型保険で犯罪被害の補償の対象となるのは、主に、金銭、セキュリティ、有形資産であり、情報や電子データの窃盗はカバーされないことが多い。

② 情報セキュリティ保険の補償対象

では、情報セキュリティ保険ではどのような内容をカバーしているのだろうか。まだ新しい保険のため、具体的な補償内容は保険会社によって異なるが、一般的には以下のようなものが情報セキュリティ保険の対象となっている。

- データの損失や破損：ウィルスや悪質コード、トロイの木馬（内部に入り込んでデータに害を与える悪質なプログラム）などの結果、損失または破損した重要な情報資産。

- 事業妨害：ネットワーク攻撃により事業が妨害された場合（denial of service など）の被害。さらに、事業妨害の捜査のための経費も補償する。

- 賠償責任：個人情報の漏洩や、アウトソーシング、企業ウェブサイト上における知的財産の侵害などを理由とし、訴訟で賠償責任を問われた場合の弁護や和解のためのコスト。また、懲罰的賠償金の補償を含む保険もある。

- サイバー上の恐喝：企業ネットワークがハッカーなどから脅迫された場合の和解金や、恐喝者の発信源をつきとめ、交渉することを目的としたセキ

ュリティ会社との契約費用。

- 広報活動：サイバー攻撃に関連した広報の費用や、消費者からの信頼回復のための広報活動の費用。

- 捜査協力への報奨金：サイバー攻撃を受けた際、犯人逮捕や有罪宣告につながる情報を提供した者へ与える報奨金。

- サイバーテロ：テロ行為による被害（テロリズム・リスク保険法（Terrorism Risk Insurance Act of 2002）で定められた範囲）。一部には、同法の範囲を超えて補償する保険もある。

- 個人情報窃盗：顧客や従業員の個人情報が窃盗された場合の被害。

これらの補償は、当事者（first party）リスクおよび（または）第三者（third party）リスクに適用される。当事者リスクとは、機密情報や顧客情報の窃盗、被保険者の資産（ソフトウェア、ハードウェア、データなど）の破損、ハッカーからの恐喝などによる被保険者のリスクを指す。一方、第三者リスクとは、被保険者のダメージが直接的または間接的に第三者に害を及ぼした場合に直面するリスク（コンピュータ・ウィルスが第三者に伝染してしまった場合、ハッカー攻撃によって被保険者の配達システムが滞り、契約どおりに商品を配達できなかった場合、被保険者のウェブサイトに著作権侵害などのコンテンツが含まれていた場合などに発生する賠償責任など）のことを指す。

(3)　付保時の審査基準

情報セキュリティ保険の補償内容や保険料、最大補償金額などはさまざまであるが、いずれにおいても付保時には、情報セキュリティに関する監査が実施される。

保険ブローカー、パルマー＆ケイ（Palmer & Cay）のメレディス・パール（Meredith Pearl）氏によれば、情報セキュリティ保険に関心を持つ企業の幹部（財務担当幹部やリスク管理担当幹部）と話をする際、その企業が情報セキュリティ保険の対象になるかどうかについて最初に判断する材料の一つとして、以下のような質問を尋ねるという。

- ソーシャルセキュリティ番号やクレジットカード番号、福利厚生プラン、その他の重要なデータを社内でどのように保管しているか？
- 売上の何割ぐらいをインターネットを使った事業から得ているか？
- どのようなファイアウォールやアンチウィルス製品を導入しているか？　ネットワークをどのように保護しているか？　それらはどれぐらいの頻度でアップデートしているか？
- システムへのアクセスを制限するために、どのような策を取っているか？
- プライバシーに関する方針の内容。
- システム・バックアップや復旧に関する方針。

実際に顧客企業が保険を購入するとなった場合は、申込書の提出となる。この申込書の提出はオンライン上でできるようにしているところも多い。申込書提出後、情報セキュリティの監査が行われる。たとえば、AIG の情報セキュリティ保険商品、AIG netAdvantage の購入を望む大手企業の場合、申込書とともに IT セキュリティ自己評価フォームを提出し、その後、現場での監査が行われる。
AIG netAdvantage の情報セキュリティ監査では、ISO17799 をセキュリティ・リスク評価のベンチマークとして利用しているという。IT セキュリティ自己評価フォームの項目は下記のように 10 項目で構成されている。

IT セキュリティ自己評価フォーム項目（AIG netAdvantage）

１）組織としてのセキュリティへの取り組み	６）アクセス管理
２）セキュリティ方針と標準	７）システム開発および管理
３）物理的セキュリティ対策とその状況	８）コンプライアンス
４）コンピュータおよびネットワークの管理	９）ベンダ管理
５）緊急時の事業続行に関するプラン	10）ネットワーク・セキュリティの損失と財政的管理

この 10 項目の下には、それぞれさらに細かく質問が設定されており、フォームは 16 ページに及んでいる。以下ではその一例として、「２）セキュリティ方針と標準」と、「７）システム開発および管理」「10）ネットワーク・セキュリティの損失と財政的管理」の項目から一部の質問を紹介する。

● IT セキュリティ自己評価フォームの一例

＜セキュリティ方針と標準＞

主要なビジネス・アプリケーションに対して、テクニカル・セキュリティ・コンフィギュレーションの文書化は実施されていますか？ ☐Yes　☐No	以下のテクニカル・セキュリティ・コンフィギュレーションの文書化は実施されている ☐ ファイアウォール ☐ ルータ ☐ OS ☐ その他の主要ビジネス・アプリケーション ☐　テクニカル・セキュリティ・コンフィギュレーションの文書は少なくとも１年に２回見直しをし、セキュリティの新たな脆弱性が見つかった場合はすぐに見直しをしている。

＜システム開発と管理＞

新たなシステムを開発、購入する際、セキュリティも考慮されていますか？ ☐Yes　☐No	☐　新規プロジェクト計画には、必ずセキュリティ上の必要条件も検討される ☐　セキュリティはシステム構築の中で定義されている ☐　企業のセキュリティ・コード基準がある ☐　新規プロジェクトにはセキュリティ専門家が関与する

＜ネットワーク・セキュリティの損失と財政的管理＞

あなたの企業は、セキュリティが破損し、予期せぬ経済的損失が発生した時のための資金調達について計画を持っていますか？ ☐Yes　☐No	資金調達計画の内容は・・ ☐　手持ち現金 ☐　準備金 ☐　信用 ☐　ネットワーク・セキュリティ保険 ☐　その他の保険

また、保険会社 CNA Pro の情報セキュリティ保険「NetProtect」では、保険が適用される企業の優先条件として、（a）3 年以上、事業をしていること、（b）収益があること、（c）米国に本社があること、（d）収入が 5000 万ドル～10 億ドルであることを挙げているほか、一部の事業（アダルト・コンテント、ゲームやギャンブル、アルコール・タバコ・武器などの販売、オンライン証券取引）を行っている企業は保険の対象外とするなど規定を設けている。さらに、被保険企業が補償を全面的に得るための条件として、「全てのコンピュータ機器にアンチウィルス・ソフトウェアを導入すること」、「ウィルスや脅威に関する情報を発信する

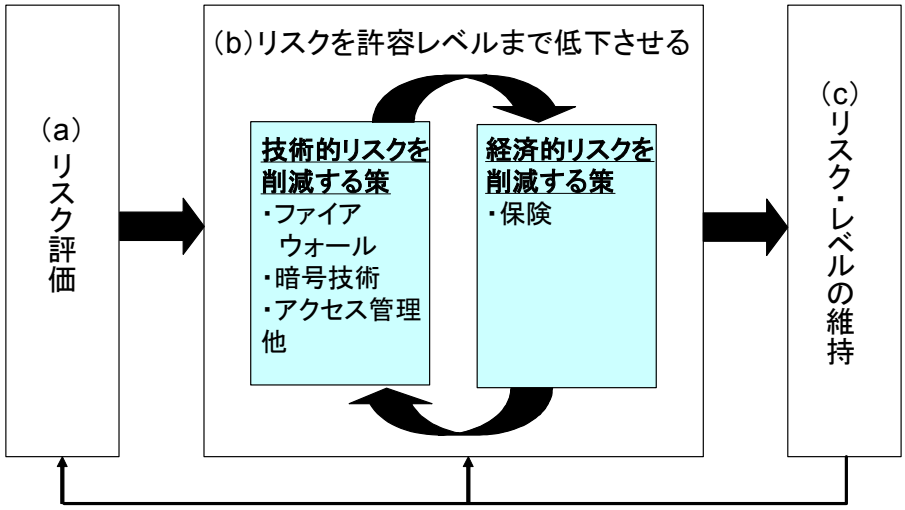
機関から自動的に情報を受信すること」など、13 件の「最低限のリスク・コントロール」を実施するよう求めている（詳細後述）。

(4)　情報セキュリティ保険のフレームワーク

①　情報セキュリティのリスク管理

メリーランド大学ビジネス・スクールのローレンス・ゴードン（Lawrence A. Gordon）教授（会計管理、情報確証）は、『保険を利用したサイバーリスク管理のフレームワーク（A framework for Using Insurance for Cyber-Risk Management）』という論文の中で、情報セキュリティ保険を効果的に利用するための前段として、情報セキュリティのリスク管理について説明している。同教授によれば、情報セキュリティのリスク管理のプロセスは、（a）リスク評価、（b）リスクを許容レベルまで低下させるための措置、（c）許容レベルまで低下させたリスクの維持、となっている。

情報セキュリティのリスク管理プロセス



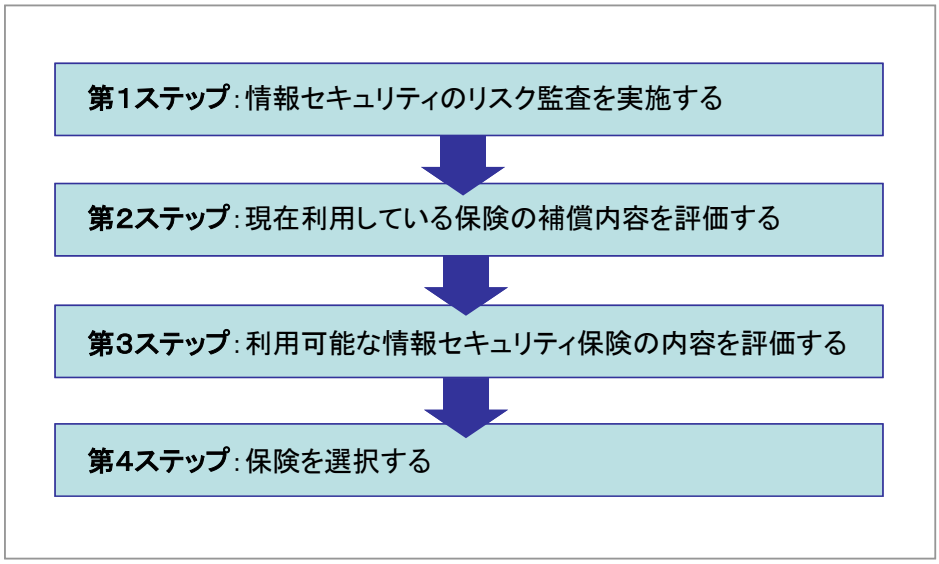
まず、「（a）リスク評価」で、組織内にあるそれぞれの情報を、「価値」と「脅威に対する脆弱性」に分類し、価値と脆弱性の双方が高い情報にセキュリティ予算の大半を当てるようにする。次に、「（b）リスクを許容レベルまで低下させる」の段階では、第一に、実際に情報セキュリティの破損が起きるのを防ぐための策（ファイアウォールや暗号技術、アクセス管理など）を検討、導入する。しかし、最新の技術を導入したとしても、情報セキュリティの破損を完全に防ぐ

ことは難しい。そのため第二の策として、経済的リスクを削減するため、保険を利用する。これらの対策は、それぞれの情報の価値と脆弱性に基づいて行う。リスクを許容レベルまで低下させた後は、「（c）リスク・レベルの維持」に取り組む。これには、侵入探知システムへの投資や、情報セキュリティの不測の事態に備えた対策計画の確立が必要となる。そしてこれらのプロセスは反復的に行われるものである。

② 保険を利用したサイバーリスク管理のフレームワーク

情報セキュリティのリスク管理プロセスを行い、情報セキュリティ保険の必要性 が明確になった後、実際に購入する保険の選択を行う。保険の選択までの流れは、以下の通りである。

情報セキュリティ保険の選択までの 4 つのステップ



情報セキュリティ保険選択までの流れの第１ステップは、組織全体の現行の情報セキュリティ・リスクに関する綿密な監査を実施することである（情報セキュリティのリスク監査）。なお、いかに優れた情報セキュリティ保険でも、情報セキュリティの破損が適切に証明（文書化）されなければ、全面的な補償はなされないため、いざという時に実際に破損が生じたことを証明できるよう、侵入探知システムを確実に導入することが重要である。

次に、「現在利用している保険の補償内容を評価」する。企業幹部たちは、現在利用している資産および賠償責任に関する保険の補償内容を詳しく検査し、さらに、現在利用している保険のインターネット関連の補償内容について評価する（多くの従来型の保険は、サイバーリスク関連の補償内容を除外する傾向にあるので、その点をよく注意すること）。

第３ステップとして、「利用可能な情報セキュリティ保険の内容を評価」する。情報セキュリティ保険はまだ新しい分野であることから、補償内容や価格は保険会社やプログラムによってさまざまである。情報セキュリティの綿密な監査の結果と、現在利用している保険の補償内容を基に、「ギャップ」となっているサイバーリスクを効果的に埋めることができる保険を探す。

第４ステップ「保険を選択する」として、候補となった保険の中から、組織特有の状況に対応するとともに、価格面で許容範囲にある保険を選ぶ。この時、保険に補償してもらいたいと考える部分と、自らリスクを請け負う部分を決定し、組織としてのリスク許容度を明確にすることが、適切な保険を選ぶ鍵である。また、情報セキュリティ・リスクの軽減という目的と、情報セキュリティ保険のコストの間のバランスを十分に考慮すべきである。

(5)　情報セキュリティ保険の動向

①　情報セキュリティ保険の問題点

情報セキュリティ保険は将来を有望視されているものの、今後、同保険が成長していくためには、いくつかの問題も指摘されている。最も大きな問題の一つは、「情報セキュリティ保険に対する認識が広まっていない」という点である。これについては、「情報セキュリティ保険が存在する」という点のみならず、「（E ビジネス関連の事故やトラブルは通常の保険では補償されないため）E ビジネスを行う企業には情報セキュリティ保険が必要である」という認識を広めることが必要であろう。

第二の問題点は、情報セキュリティに関する正確な情報が不足しているという点である。保険会社は、過去の損失やリスクに基づいて保険のポリシーや補償額、保険料などを決めるが、情報セキュリティ分野は過去の実績が多くないためにこれらの作業が難しい。

第三に、情報資産の価値を測定することが難しいという点がある。たとえば、顧客の個人情報に関するデータベースを盗まれた場合、そのデータベースの価値を算出するのは容易ではない。

最後に、企業は情報セキュリティに関する事故やトラブルを公表するのを避ける傾向にあるという問題がある。これは企業としての評判や信用に傷が付くことを最も恐れるためである。企業のこうした傾向は今後も続くと考えられることから、正確な情報は限定され、情報セキュリティ保険市場の発展には時間がかかるであろう。

② 保険会社の取り組み

情報セキュリティ保険の成長に期待をかける保険会社は、保険会社としてのリスクを高めないよう慎重になりつつ、同保険の発展につながるような策を講じている。

たとえば、脆弱性が高いとみなされるソフトウェアを使っている場合、保険料を高く設定する一方、保険会社が推奨するセキュリティ・ソフトウェアを利用している場合、保険料の割引が適用される。
一例として、英国保険市場ロイズ・オブ・ロンドン（Lloyd's of London）のシンジケート保険会社である SVB は、同社の情報セキュリティ保険、e-Comprehensive を購入する顧客に対し、トリップワイアー（Tripwire）のセキュリティ・ソフトウェアを適切に導入している場合、保険料を 10%割引している。
また、AIG netAdvantage は、情報セキュリティ団体、インターネット・セキュリティ・アライアンス（ISAlliance、既出）の加盟企業に対して、保険料の 5%割引を提供している上、ISAlliance による『上級マネジャーのためのベストプラクティス・ガイド（Best Practices Guide for Senior Managers）』にコンプライアンスしている企業に対しては、さらに保険料の最大 10%割引を提供している。これらは、「ISAlliance に加盟している企業は、より適切なセキュリティ方針を実践する可能性が高い」との認識によるものである。AIG netAdvantage は ISAlliance と協力し、前述の『IT セキュリティ自己評価フォーム』の共同開発なども行っている。

情報セキュリティ保険会社は、保険を購入しようとする企業に対して、情報セキュリティ方針や企業が利用している情報セキュリティ・サービス提供会社、製品などに関する要件を設定し、それらを満たすことを義務付けることから、「今後、情報セキュリティ保険によって情報セキュリティのデファクト・スタンダードが形成され、情報セキュリティ・ビジネスの発展の原動力になる可能性がある」といった見方もある。

3. 主な情報セキュリティ保険商品の概要

(1) American Insurance Group（AIG）

保険会社大手の AIG の e ビジネス・リスク・ソリューション（eBusiness Risk Solutions）は、情報セキュリティ保険の草分け的存在であり、情報セキュリティ保険におけるシェアは約 70%を占める。同社は 2000 年頃より「AIG ネットアドバンテージ・シリーズ（AIG netAdvantage Suite）」を発売している。同シリーズでは、Network Security Liability、Web Content Liability、Internet Professional Liability などの具体的な補償内容（13 種類）の組み合わせにより、ベーシックである AIG netAdvantage から、包括的な AIG netAdvantage Complete まで、7 種類の商品がある。7 種類の商品とそれらの具体的な補償内容は以下の通りである。

AIG netAdvantage シリーズ

	AIG netAdvantage®	AIG netAdvantage Professional®	AIG netAdvantage® Commercial	AIG netAdvantage Liability®	AIG netAdvantage® Property	AIG netAdvantage Security®	AIG netAdvantage Complete®
1）Network Security Liability			✓	✓		✓	✓
2）Web Content Liability	✓	✓	✓	✓		✓	✓
3）Internet Professional Liability		✓		✓			✓
4）Network Business Interruption					✓	✓	✓
5）Information Asset Coverage					✓	✓	✓
6）Identity Theft			✓	✓	✓	✓	✓
7）Extra Expense					✓	✓	✓
8）Cyber Extortion			✓*	✓*	✓	✓	✓
9）Cyber Terrorism*	✓	✓	✓	✓	✓	✓	✓
10）Criminal Reward Fund					✓	✓	✓
11）Crisis Communication Fund					✓	✓	✓
12）Punitive, Exemplary and Multiple Damages	✓	✓	✓	✓		✓	✓
13）Physical Theft of Data on hardware/firmware			✓	✓		✓	✓

AIG netAdvantage シリーズの 13 の補償内容

	名称	内容
1）	Network Security Liability（ネットワークセキュリティ補償）	被保険企業のネットワークに対するコンピュータ攻撃によって受けた損害および防衛用コストを補償。コンピュータ・ウィルスや不正アクセス、denial-of-service、機密情報の不正開示、個人情報窃盗による賠償責任も含む。

２）	Web Content Liability （ウェブ・コンテンツ補償）	被保険企業のウェブサイトに表示された内容を理由とする名誉毀損、中傷、著作権・所有権・商標の侵害、プライバシーの侵害など、コンテンツ・ベースの賠償責任に対する補償。
３）	Internet Professional Liability （インターネットの業務サービスに関する補償）	さまざまなインターネット業務サービス（アプリケーション・サービス・プロバイダ、インターネット・サービス・プロバイダ、ネットワークセキュリティ・サービス管理、ホスティング、メディアサービス、電子取引およびインターネット・オークション、サーチ・エンジンなど）から発生する職業賠償責任（errors and omissions）に対する補償。
４）	Network Business Interruption （ネットワーク・ビジネス妨害）	コンピュータ攻撃によって生じた被保険企業のオンラインおよびオフライン上の収入損失を補償。ビジネス妨害が長引いた場合に発生する損失も補償する。
５）	Information Asset （情報資産）	被保険企業の重要な情報資産が損害、混乱、破壊を受けた場合の補償。
６）	Identity Theft （個人情報窃盗）	被保険企業のネットワーク侵害により、顧客や取引企業の個人情報が盗まれた場合の賠償責任を補償する。また、被保険企業は 24 時間体制の AIG Identity Theft Call Center も利用できる。
７）	Extra Expense （追加費用）	セキュリティ侵害による妨害を受けた後、迅速な復旧を行うために必要な追加費用を補償。また、コンピュータ攻撃後、科学捜査分析のための費用（最高 10 万ドル）を提供
８）	Cyber Extortion （サイバー恐喝）	被保険企業がサイバー上の恐喝を受けた場合、調査や問題の解決に関する費用を補償
９）	Cyber Terrorism （サイバー・テロリズム）	「テロ行為」による被害の補償。テロ行為の定義は幅広く、サイバーテロ行為による当事者および第三者の損失、データの損害、ビジネス妨害、第三者への賠償責任をカバーする。
10）	Criminal Rewards 犯罪対策報酬）	コンピュータ攻撃やその他特定の犯罪の犯人（または犯そうとした者）の逮捕や有罪につながる情報を提供した人への報酬用資金（最高 5 万ドル）。
11）	Crisis Communication Fund （危機時のコミュニケーション基金）	コンピュータ攻撃でダメージを受けた企業の信用を回復するための PR 資金を提供（最高 5 万ドル）。
12）	Punitive, Exemplary and Multiple Damages （懲罰的損害賠償金補償）	法律によって認められる範囲で懲罰的賠償金を補償。
13）	Physical Theft of Data （データの物理的窃盗）	情報資産を含むコンピュータ・ハードウェアやファームウェアの物理的窃盗に伴う賠償責任を補償。

同社は、自社の情報セキュリティ保険商品の売り込みの特徴として、以下の点を挙げている。

- オンライン・セキュリティ評価の無料実施サービス。
- 補償限度額は最大 2500 万ドル。保険料は 5000 ドル～。
- 顧客のリスクに応じてカバー内容を変更することが可能。
- カバー内容は基本的に世界規模、システムワイドで提供される。
- AIG の Technology Panel Counsel（AIG による法律サービス）の利用が可能。

(2) CNA Pro

米国保険会社大手、CNA Pro は、情報セキュリティ保険として CNA NetProtect を販売している。NetProtect では、当事者および第三者を対象として、以下のような補償を提供している。

＜当事者補償＞
- 外部者の不正アクセスによる、資金や証券、モノ、サービス、無形資産の電子窃盗。
- 悪意を持った意図的行為によるデータやソフトウェアの損失。
- これらの行為によって発生した事業妨害および収入損失のための追加費用。

＜第三者補償＞
- コンテンツおよび電子出版における損害（名誉毀損や誹謗中傷）。
- プライバシー侵害および機密情報の漏洩。
- ネットワーク・セキュリティの賠償責任。
- 業務責任。

NetProtect では、前述のように、保険が適用される企業の優先条件として、（a）3 年以上、事業をしていること、（b）収益があること、（c）米国に本社があること、（d）収入が 5000 万ドル～10 億ドルであることを挙げているほか、一部の事業（アダルト・コンテンツ、ゲームやギャンブル、アルコール・タバコ・武器などの販売、オンライン証券取引）を行っている企業との契約は認めていない。

さらに、補償を全面的に得るために、被保険企業は、最低限のリスク・コントロールとして、以下の 13 点を実施する必要があると定めている。

CNA Pro が求めるリスク・コントロール策

(1) アンチウィルス ・全てのコンピュータ機器にアンチウィルス・ソフトウェアを導入すること。

	・アンチウィルス・ソフトウェアは少なくとも 1 日 1 回、自動的にアップデートすること。 電子メールの添付ファイルを開く前に、自動スキャンを行うこと。
(2)	CERT やその他の類似機関からウィルスや脅威に関する情報配信を自動的に受信すること。
(3)	使用しているファイアウォールはデフォルト以外の設定にし、確実に確認すること。
(4)	インターネット用のシステムとバックオフィス業務用のネットワークを別にし、複数のファイアウォールを利用すること。
(5)	全ての従業員および契約者にセキュリティ方針を広めること。
(6)	データ・センターにおける緊急事態からの復旧計画を含め、緊急時対応計画を作成し、テストすること。
(7)	ネットワーク上の直接的攻撃（ハッキングなど）および間接的攻撃（ウィルスなど）に対するセキュリティ事故対応計画を作成し、テストすること。
(8)	ネットワーク・データとコンフィギュレーション・ファイルのバックアップを毎日取ること。
(9)	バックアップ・ファイルはオフサイトに保管すること。
(10)	リモート・アクセスは、VPN またはそれに類似する技術を使ったアクセスの場合のみ、許可すること。
(11)	セキュリティ・パッチやアップグレードを入手するため、ネットワーク・プラットフォームのベンダを少なくとも 1 日 1 回、モニターすること。
(12)	セキュリティ・パッチやアップグレードは、利用可能日から 30 日以内にテスト、導入すること（理想は 7 日以内）。
(13)	サーバ室は常に施錠し、許可を与えられた者のみ入手するよう、制限すること。

NetProtect の場合、保険損害に対して支払われる限度額は 1000 万ドル。保険料については明らかになっていない。

(3) Safeonline

サイバー保険の製品やサービスを開発し、英国保険市場ロイズ・オブ・ロンドンのシンジケート保険会社である ACE グローバル・マーケット（ACE Global Markets）を引受人として情報セキュリティ保険を販売する Safeonline は、1998 年に設立された。本社は英国にあり、米国でも各種のサイバー保険を販売している。

同社の主要な米国市場向け商品は、SafeBusiness、SafeCommerce、SafeEnterprise の 3 種類である。

Safeonline の情報セキュリティ保険

SafeBusiness	
対象機関	電子メールシステムやウェブサイト、データをコンピュータ・ネットワークに保管しているあらゆる企業。
カバー範囲	・ 利用電子メールが 100 件未満。 ・ 当事者および第三者のサイバー保険を別個に購入することも可。 ・ データの損失（コンピュータ・ウィルス、従業員の過失、内部および外部によるハッキング、物理的損失、自然災害、停電、窃盗を理由とする） ・ 賠償責任（ウィルス感染、名誉毀損、誹謗中傷、プライバシー侵害、盗用、ウェブサイト、HIPAA 遵守）
保険料	750 ドル～。
免責金額	当事者：100 ドル～。第三者：1000 ドル～。
限度額	当事者：2 万ドル～7 万 5000 ドル。 第三者：25 万ドル～100 万ドル。
SafeCommerce	
対象機関	ウェブサイトを有する企業。従業員や顧客のデータをコンピュータに保管している企業。インターネットを使って電子商取引を行っている企業。
カバー範囲	・ 個人や広告による賠償責任を補償。 ・ 著作権やドメインネーム、デザイン、タイトル、スローガンの侵害や、商標、サービスマーク、サービスネーム、トレードネームの侵害または希釈。 ・ アイデアの盗用や不正流用。 ・ インターネット・コンテンツの賠償責任。 ・ ネットワーク・セキュリティの賠償責任（ハッキングやウィルスによる賠償責任も含む）。 ・ 機密情報の漏洩または機密情報や法規制の対象となる情報の不正使用。
保険料	2750 ドル～。
免責金額	5000 ドル～。
限度額	最高 500 万ドル。
SafeEnterprise	
対象機関	アプリケーション・サービス・プロバイダ、B2B ウェブサイト、コンピュータ・システム管理企業、コンピュータ・コンサルティング企業、ソフトウェア・デベロッパー、クレジットカード処理企業、CRM 企業、B2C ウェブサイト、ポータル企業、他。
カバー範囲	・ 職業賠償責任（errors and omissions）。 ・ 知的財産リスク、広告や個人による損害（名誉毀損、誹謗中傷、製品への誹謗中傷、プライバシーや著作権の侵害なども含む）。 ・ インターネット・コンテンツの賠償責任。 ・ ネットワーク・セキュリティの破損。

	・　ウィルスや悪質コードの意図的でない感染。 ・　機密情報の漏洩または情報の不正使用。
保険料	2250 ドル～。
免責金額	5000 ドル。
限度額	50 万ドル～1000 万ドル。

（参考資料）

David Bank “Retailers rush to secure data against theft” Wall Street Journal, April 25, 2005
http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf
http://www.khlaw.com/index.cfm?fuseaction=publications.showPubDetail&pubID=834
http://subscript.bna.com/SAMPLES/ctl.nsf/0/59805394d21e746485256fb9007c8fa0?OpenDocument
http://www.post-gazette.com/pg/05202/541454.stm
J. Wylie Donald “New Jersey Takes On Identity Theft” New Jersey Law Journal. October 31, 2005.
http://www.colliershannon.com/documents/SenateJudiciaryCommittee.pdf
http://www.swissre.com/INTERNET/pwsfilpr.nsf/vwFilebyIDKEYLu/MBAR-4VFJQ3/$FILE/sigma5_2000_e.pdf
http://infosecon.net/workshop/slides/weis_5_1.pdf
http://www.businessweek.com/bwdaily/dnflash/apr2002/nf2002042_8163.htm
Brian Kerbs “White House pushing cybersecurity insurance” Washington Post June 27, 2002
http://www.iii.org/media/hottopics/insurance/computer/
http://www.isalliance.org/
http://www.us-cert.gov/reading_room/CSG-small-business.pdf
http://www.computerworld.com/news/2000/story/0,11280,48721,00.html
http://www.aignetadvantage.com/content/netad/NetAdvantage_FI_brochure.pdf
Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail “A framework for using insurance for cyber-risk management” Communications of the ACM March 2003 p.83
http://www.agentandbroker.com/default.cfm?page=287
http://www.itworldcanada.com/a/News/8d3d2211-f322-4f51-9204-82e4dfc34e2c.html
http://www.aignetadvantage.com/content/netad/netadvantage_assessment.doc
Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail “A framework for using insurance for cyber-risk management” Communications of the ACM March 2003 p.83-85
http://www.lloyds.com/index.asp?ItemId=7269
http://www.isalliance.org/
http://www.aignetadvantage.com/content/netad/Coverage.pdf
http://www.cnapro.com/pdf/TechNetProtect.pdf
http://www.cnapro.com/pdf/NetProtAppetite-MinControls.pdf
http://www.safeonline.com/

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。