第６章　関西地情報セキュリティ対策の状況

本章では、まず「情報セキュリティ」の定義を行ったうえで、2005 年度から 2007 年度の 3 ヵ年に渡って実施した関西情報化実態調査による企業及び自治体の事業継続計画への対応によるリスク対応状況（可用性）と情報資産などに対する機密性、完全性を担保するための情報セキュリティ対策状況について分析を行う。

また、関西以外における我が国全体の情報セキュリティの現状と中央省庁による情報セキュリティに関する対応状況について整理し、今後の情報セキュリティ対策のあるべき姿について、所見を述べる。

→ 関西の情報セキュリティ対策の状況と今後の情報セキュリティ対策のあるべき姿のポイント

◆ 情報セキュリティ対策とリスク分析・リスクマネジメントの重要性

- ユビキタス社会の進展に伴い、ネットワーク利用の高度化、社会基盤などの IT への依存が高まっているが、これと並行して情報セキュリティの脅威が増している。
- 国では、このような状況を鑑み、「内閣官房情報セキュリティセンター（NISC）」を 2005 年 4 月に設置し、「セキュア・ジャパン 2006／2007」等を策定し、情報セキュリティ対策に関するさまざまな施策を展開している。
- 情報セキュリティ対策を検討するうえで、自社・自組織のリスクを洗い出し、どのような危険が潜でいるのかを分析し、状況に応じた事業継続計画を策定、マネジメントを行うことが非常に重要である。

◆ 関西の企業・自治体における情報セキュリティ対策の実態

- 2006 年度の調査結果では、事業継続計画の策定状況は、大きくは進んでいない。
- しかし、全国調査結果と 2007 年度の関西情報化実態調査の結果比較すると、中小企業、自治体でそれぞれ全国平均値を上回る結果が得られた。
- この要因としては、1995 年 1 月 17 日発生した「阪神・淡路大震災」の経験が活かされているものと考えられる。
- 上場企業の 2006 年度調査では、情報セキュリティ対策におけるマネジメント面で弱い傾向がみられたが、2007 年度調査結果では、改善された傾向がうかがえた。
- この要因としては､2008 年 4 月より運用が開始される日本版 SOX 法に関連した IT 全般による内部統制の見直しに伴った情報セキュリティ対策の見直しが影響していると思われる。
- 自治体でも、2006 年度調査結果では上場企業同様、マネジメント面において弱い傾向がみられたが、2007 年度調査結果では、徐々に改善されてきている傾向がうかがえる。
- 中小企業では、上場企業や自治体と比較すると、情報セキュリティ対策は遅れ気味の調査結果であるが、「情報セキュリティ上の事故対応状況」については、全国調査結果を大きく上回る結果が得られており、これも「阪神・淡路大震災」の経験が活かされている結果と考えられる。
- なお、2006 年度の調査結果では、上場企業・自治体ともに情報セキュリティ対策を担う人材が不足していることをうかがわせる回答が多くを占め、今後の課題と考えられる。

◆　今後の取り組み

- 今後は、国などが示す指針などを参考にしながら、IT を利活用する情報利用主体者が、より積極的に情報セキュリティ対策は必要不可欠なことであることを認識するとともに、電気通信事業者等、サービス提供事業者そのものが、情報利用者に代わって脅威を排除した環境でサービスを提供するなどの工夫も必要である。
- さらに、産学官連携による、より実践的な情報セキュリティ対策のあり方について検討を行い、利用者、サービス提供事業者が共生できる IT 社会モデルを構築していくことが重要である。

１．情報セキュリティと危機管理

１．１　情報セキュリティとは

「情報セキュリティ」とは、さまざまな脅威から企業や組織の重要な財産（資産）である情報（情報資産）のセキュリティを確保し、維持することである。情報資産のリスクを評価し、情報資産の価値に見合った適切な対策を実施することが情報セキュリティ対策の基本的なアプローチである。この情報セキュリティを構成する代表的な要素には、次の 3 つが挙げられる。

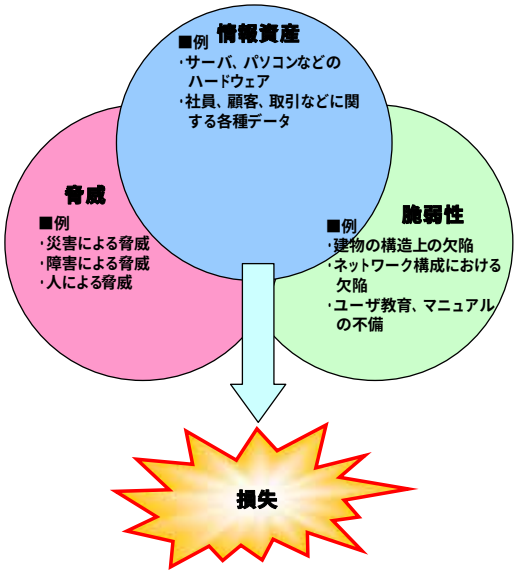
要素		主な脅威	主な対策
機密性	ネットワーク上で扱う情報が外部に漏れることなく、許可されたユーザのみが確実に情報にアクセスできること	侵入、盗聴	アクセス制御、デジタル暗号化
完全性	情報が改ざんなどされず、正確、完全である状態を維持すること	改ざん	デジタル署名、データの整合性チェック
可用性	いつでもシステムの情報に確実にアクセスできること	障害、妨害	二重化、保守

上記の 3 要素はいずれも重要であり、高いセキュリティを確保し、維持するためには必要不可欠なものである。なお、後述の事業継続計画（Business Continuity Management　BCP）は、上記の「可用性」に関する事項である。

１．２　情報セキュリティにおける危機（リスク）管理対策について

情報セキュリティ対策におけるリスク分析、リスクマネジメントは「何らかの事態が発生することに関する不確実性」と言える。リスク分析を行うことにより、組織に内在するさまざまなリスクを洗い出し、その発生頻度や影響度を分析する必要がある。リスクを構成する要素は、「情報資産」、「脅威」、「脆弱性」の 3 つから構成されている。これらの要素が結びつくことで、リスクが顕在化し、どのような損失が発生するのかが明らかになる。

図表．情報セキュリティにおけるリスクの 3 要素



（出典：「情報セキュリティアドミニストレータ 2005 年度版　株式会社翔泳社資料　をもとに作成）

２．関西の企業・自治体における情報セキュリティ対策の取り組み状況

ネットワークの利用環境などの進展などに伴い、業務効率や利便性は格段に向上しているが、一方で、コンピュータへの不正な侵入、ウィルス感染などによる攻撃、あるいは個人情報の漏えいなどにより、企業や自治体における重要な情報資産が危険に晒される頻度も高くなっている。このため、組織において情報セキュリティ対策を行うことは、非常に重要になっている。

関西情報化実態調査では関西の企業及び自治体が、情報セキュリティ対策を実施するにあたって、自組織のリスク分析を行ったうえで適切な対策が行えているのか、また、対策マニュアルなどを策定するだけでなく、マネジメントが適切に実施されているのかといった視点により、調査を実施した。以下、2005 年度から 2007 年度の 3 ヵ年で実施した調査結果の概要について述べる。

２．１　関西の企業・自治体における危機管理対策の取り組み状況

（1）調査結果のポイント

先述のとおり情報セキュリティ対策では、リスクを分析し、適切な対策を講じておく必要がある。情報管理だけでなく、災害発生などによる影響度を認識し、発生時の事業継続を確実にするため、必要な対応策を策定する必要がある。これを「事業継続計画（Business Continuity Plan BCP）」と呼ぶ。また、これの運用・訓練・継続的改善の取り組みを事業継続マネジメント（Business Continuity Management BCM）という。

2006 年度の関西情報化実態調査において、企業及び自治体における事業継続計画に関する取り組み状況について調査を実施した。調査結果の概要は次のとおりである。

◆上場企業の場合

- 多くの企業で、大規模災害対策を想定した防災計画作成を検討している段階である。
- しかし、従業員用行動マニュアルについては、4 割弱の企業が作成済みである。
- IT の視点から大規模災害対策の事業復旧にかかわるガイドラインの策定は、5 割弱存在した。
- 大規模災害を想定した訓練は、約 8 割の企業では実施できていない。
- 大規模災害対策を進める上での課題・問題点は、人員・資金の不足と、認識の低さである。
- CIO の能力や機能が充実している企業ほど、大規模災害対策状況も充実している。

◆中小企業の場合

- 大規模災害時における事業継続性に関する意識が低い。
- CIO を設置している企業では、設置していない企業よりも、対策状況はよい傾向にある。

◆自治体の場合

- 大規模災害を想定した防災計画や職員の行動マニュアルの策定は、比較的進んでいる。
- IT の視点による策定は低い。
- 大規模災害を想定した訓練は、約 8 割の自治体では実施できていない。
- 大規模災害対策を進める上での課題・問題点は、人員・資金不足である。
- 一部の自治体では、1995 年 1 月 17 日に発生した「阪神・淡路大震災」の教訓により、かな

り先進的な取り組みを行っている。

- CIO の能力や機能の実現度と大規模災害対策の実施状況には、大きな関係は認められない。
- 人口規模が大きくなる程、実施状況は高い。

上記のように、上場企業、中小企業では事業継続性に対する取り組みは、あまり進んでいないが自治体では、防災計画や行動マニュアルの策定は比較的進んでいるという結果が得られた。これは、1995 年 1 月 17 日に発生した「阪神・淡路大震災」が影響していると考えられる。

先進的な取り組み事例として西宮市では、「阪神・淡路大震災において情報システムを駆使した震災業務支援システムを構築したことで、被災者・市民はもちろん庁内においても計数的に計り知れないほど絶大な効果を発揮し、市民生活など住民サービスに語りつくせないほど寄与した。」とある。また、こうした動きは、「情報システム課員自身が被災しながらも、使命感と責任感により、被災者支援第一次主義と現場至上主義により得た体験である。」（いずれも、西宮市　電子自治体担当理事　吉田稔氏　掲載コラムより（※所属・役職は 2006 年度当時））とも記されており、現場での体験が実際の対策に反映された例と言える。

企業においても、同様の経験をしているはずであり、今後は西宮市同様、実体験をもとに対策を拡げていくことが重要である。

２．２　関西の企業・自治体における情報セキュリティ対策の取り組み状況

（1）調査結果のポイント

情報資産を守り、情報管理を適切に実施するために必要な対策の内容を整理すると、次の 3 つに分類される。

取り組みの分類	内容の例
物理的なセキュリティ対策	ウィルス対策、不正アクセス対策など
組織的なセキュリティ対策	推進体制、セキュリティポリシーの策定や従業員・職員に対する教育など
事故対応に関する取り組み	情報漏えいなどのセキュリティ事故が発生した際の対応

関西情報化実態調査では、このような視点において、2005 年度～2007 年度の３ヵ年で、企業及び自治体に対して情報セキュリティ対策の取り組み状況に関する調査を実施した。[1]

主な調査結果概要は次のとおりである。

◆上場企業の場合

- 2006 年度調査結果では、「情報セキュリティに関する組織・体制」、「セキュリティポリシーにもとづいた対策状況」、「業務見直し状況」などのマネジメント面に関する項目が弱い傾向がみられた。
- 2007 年度調査結果では、「組織的な取り組み状況」、「物理的セキュリティの対策状況」、「情報セキュリティ上の事故対応状況」のいずれの項目においても、2005 年度に経済産業省が実

[1] ただし、各年度の調査ではそれぞれ異なる内容での調査を実施しているため、同様の項目における厳密な経年変化による比較を行うことはできない。

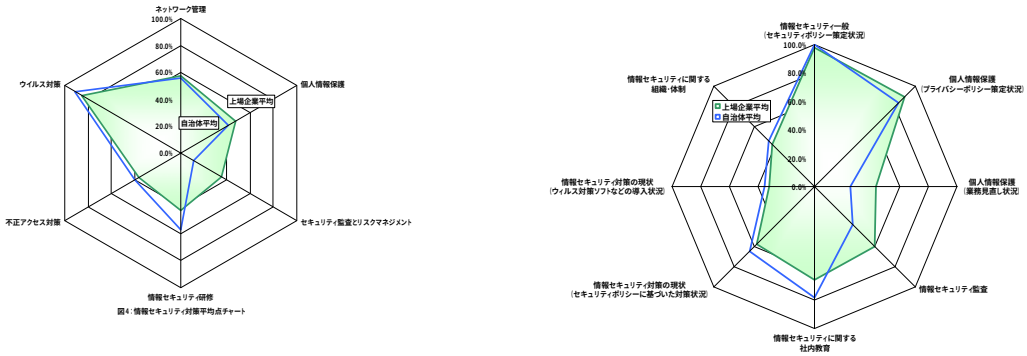
施した全国調査結果の平均値を上回っており、マネジメント面が改善している結果が得られた。

- この要因としては、2008 年 4 月より運用が開始される日本版 SOX 法に関連した IT 全般による内部統制の見直しに伴った情報セキュリティ対策の見直しが影響しているものと思われる。
- 情報セキュリティ対策の取り組み状況と CIO の関係をみると、CIO として必要とされている能力や機能が充実している企業ほど、情報セキュリティの対策状況も充実していることがうかがえる。
- なお、2006 年度の調査結果では、情報セキュリティ監査を実施しない理由として「担当者の確保が難しい」とする回答が 40.0%と占めており、情報セキュリティ対策を担う人材が不足していることがうかがえる結果であった。

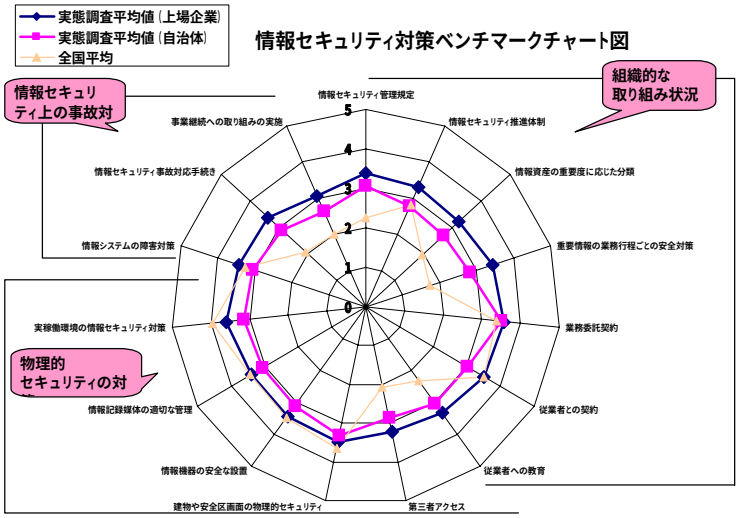
◆自治体の場合

- 2006 年度の調査結果では、セキュリティポリシーは概ね策定されているが、情報セキュリティ監査の実施状況については、セキュリティポリシーの策定状況と比較すると、それほど進んでおらず、マネジメント面が弱い傾向がみられた。
- 2007 年度の調査結果では、「組織的な取り組み状況」、「物理的セキュリティの対策状況」、「情報セキュリティ上の事故対応状況」のいずれも、2005 年度に経済産業省が実施した企業向けの全国調査結果の平均値を上回るものであったが、「情報セキュリティ上の事故対応状況」の詳細項目である「情報セキュリティ上の事故対応状況」については、全国調査結果の平均値を大きく上回る結果が得られた。
- この要因としては、中小企業の結果と同様、「阪神・淡路大震災」の経験が活かされているものと考えられる。
- 情報セキュリティ対策の取り組み状況と CIO の関係をみると、CIO として必要とされている能力や機能が充実している自治体ほど、情報セキュリティの対策状況も充実していることがうかがえる。
- なお、自治体においても上場企業と同様に、情報セキュリティ監査を実施しない理由をたずねたところ、「担当者の確保が難しい」とする回答が 63.6%と上場企業より、多くを占める結果が得られた。人材不足は自治体ではより深刻な状況であることがうかがえる。

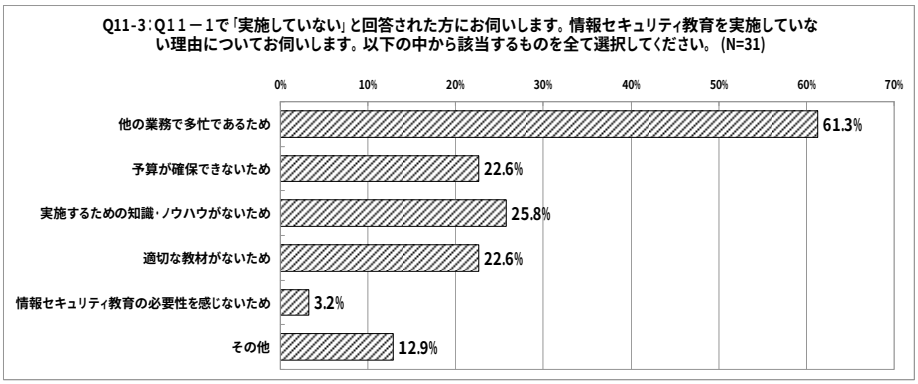
図表．情報セキュリティ対策の取り組み状況（左側：上場企業・自治体（2005 年度）　右側：上場企業・自治体　（2006 年度）

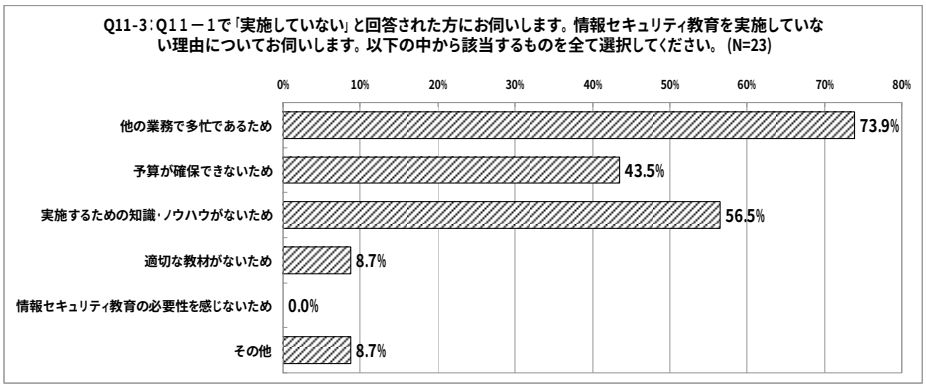


図表．情報セキュリティ対策の取り組み状況（上場企業・自治体　2007 年度）

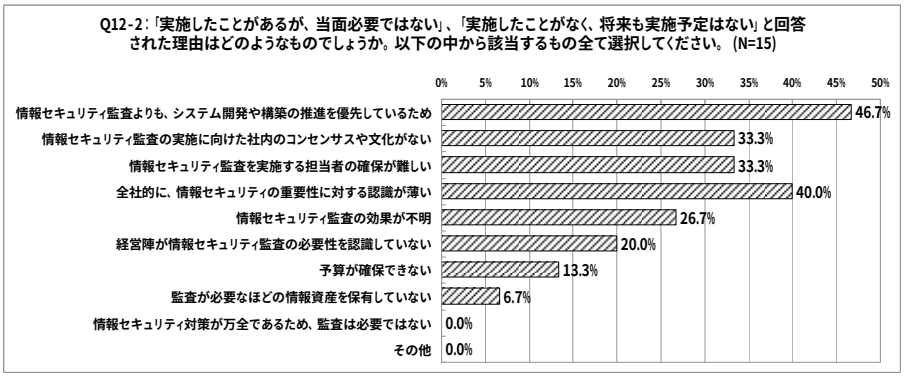


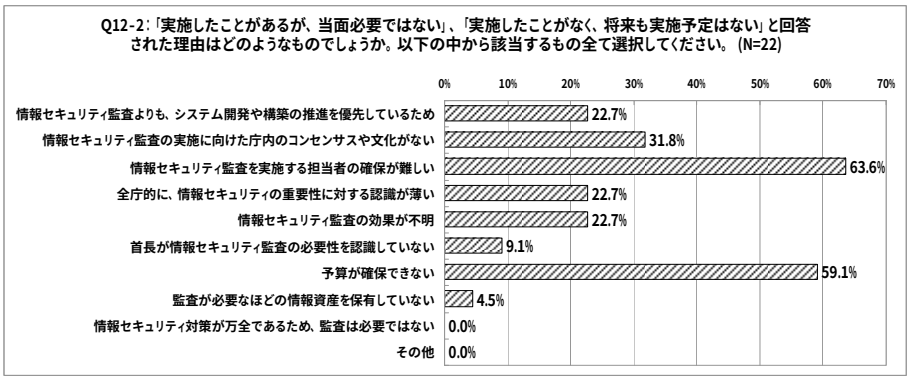
図表．情報セキュリティ教育を実施していない理由（上段：上場企業　下段：自治体　いずれも 2006 年度）





図表．情報セキュリティ監査を実施していない理由（上段：上場企業　下段：自治体　いずれも 2006 年度）

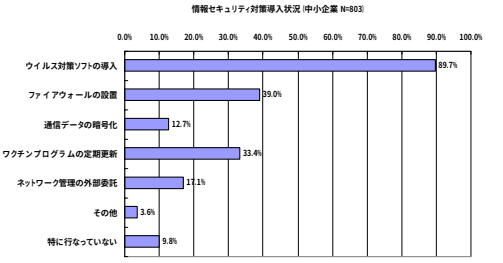


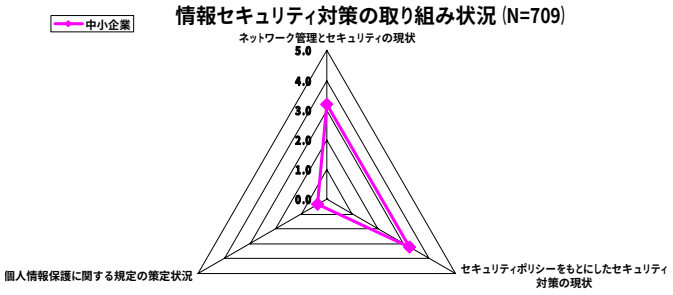


◆中小企業の場合

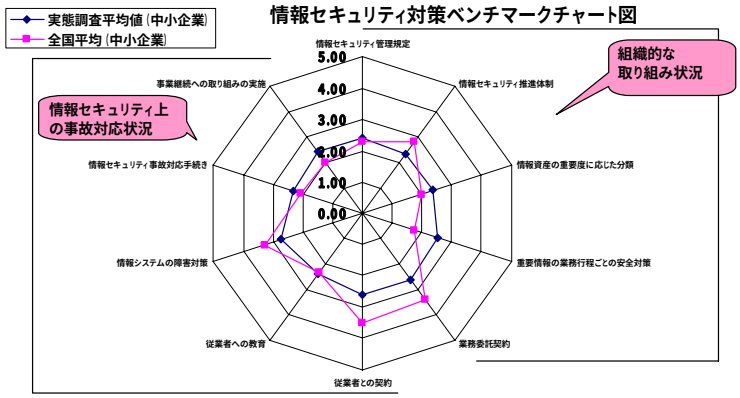
- 2005 年度及び 2006 年度調査結果では、ウィルス対策ソフト、ファイアウォールの導入といったシステム面に関する対策が比較的高いポイントを示した。
- しかし、情報セキュリティ関連認証取得コンサルティングや情報セキュリティポリシーコンサルティングといった運用・評価面に関する対策は、そもそもこれらの対策の存在があまり知られていないという結果であった。
- これに伴って、「個人情報保護に関する規定の策定状況」は非常に低いポイントであった。
- 2007 年度調査結果をレーダーチャート図で表すと、上場企業同様、「組織的な取り組み状況」、「情報セキュリティ上の事故対応状況」ともに、突出して弱い面はみられず、比較的真円に近い図になったが、多くの項目で 2005 年度に経済産業省が実施した全国調査結果の平均値を下回る結果となった。
- ただし、「情報セキュリティ上の事故対応状況」の詳細項目をみると、「事業継続への取り組みの実施」や「情報システムの障害対策」などの BCP に関連する項目については、全国調査結果を上回った。
- この要因としては、1995 年 1 月 17 日に発生した「阪神・淡路大震災」の経験が活かされているものと考えられる。
- 情報セキュリティ対策の取り組み状況と CIO の有無の関係をみると、CIO を設置している企業の方が設置していない企業より、実施状況が良好となる傾向がみられた。

図表．情報セキュリティ対策の取り組み状況（中小企業　左側：2005 年度　右側：2006 年度）





図表．情報セキュリティ対策の取り組み状況（中小企業　2007 年度）



３．今後の情報セキュリティ対策のあるべき姿

３．１　我が国の情報セキュリティの現状

IT 利用の急速な普及は、今後も続くものと考えられる。特に、かつて経験をしたことのない少子高齢化社会に直面している我が国において持続的な経済成長を実現するためには、これまで以上に IT が果たすべき役割は重要なものになると考えられる。

しかしながらその一方で、IT 利用の負の側面である情報セキュリティに対する問題や利用者における不安感が顕在化してきている。例えば、「社会基盤等におけるサービスの停止や機能低下」、「我が国におけるサイバー犯罪の状況」、「情報漏えい」、「インターネット利用における不安感」及び「利用者のセキュリティ対策実施状況」については、次に示すようなことが指摘されている。

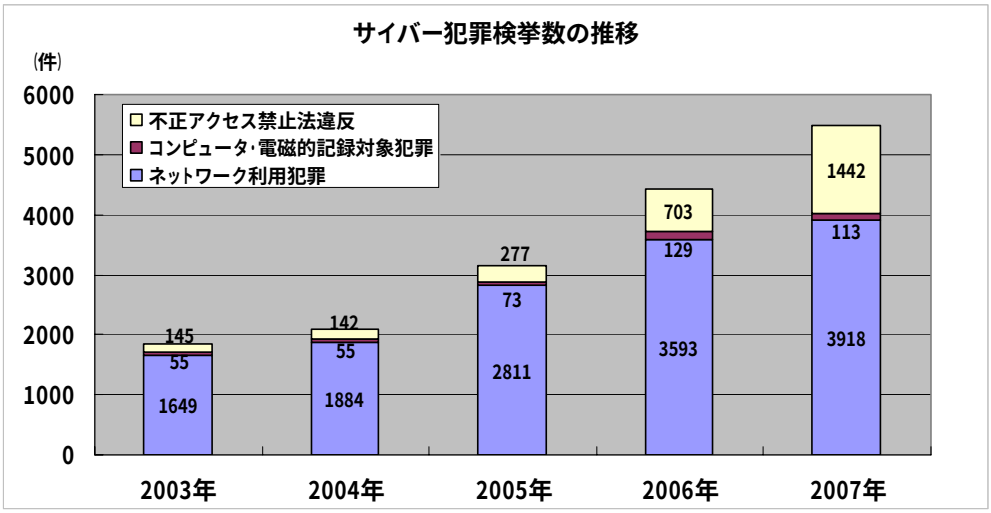
（1）社会基盤等に置けるサービスの停止や機能低下

社会生活の基盤である重要インフラ（他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下または不可能な状況に陥った場合に、我が国の国民生活または社会経済活動に多大なる影響を及ぼす恐れが生じるものであり、「重要インフラの情報セキュリティ対策に係る行動計画（情報セキュリティ政策会議決定　2005 年 12 月）においては、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流の 10 分野とされている」）における IT 利活用が進展するにつれて、重要インフラにおける IT 障害の発生が増加している。

（2）我が国におけるサイバー犯罪の状況

我が国における 2007 年中のサイバー犯罪の検挙件数は、5,473 件であり、2006 年（4,425 件）より 23.7%の増加となっている。これは 2003 年から 5 年間で約 3 倍に達している状況である。このうち、不正アクセス禁止法違反は 1,442 件で前年の 2.1 倍に増加するとともに、児童買春及び青少年保護育成条例違反や著作権法違反などの増加によりネットワーク利用犯罪の件数（3,918 件）も、2006 年比 9.0%の増加となっている。また、2007 年の主なサイバー犯罪検挙事例のひとつとして、中学生の被疑者がオンラインゲーム上のアイテムを収集する目的で、キーロガーをダウンロードさせて他人のユーザ ID とパスワードを入手して同オンラインゲームを運営する会社のコンピュータに不正アクセス行為を行う事例が取り上げられており、コンピュータ犯罪の低年齢化の傾向が指摘されているところである。

図表．サイバー犯罪検挙数の推移



（出典：警察庁調べ　2008 年 2 月）

（3）情報漏えい

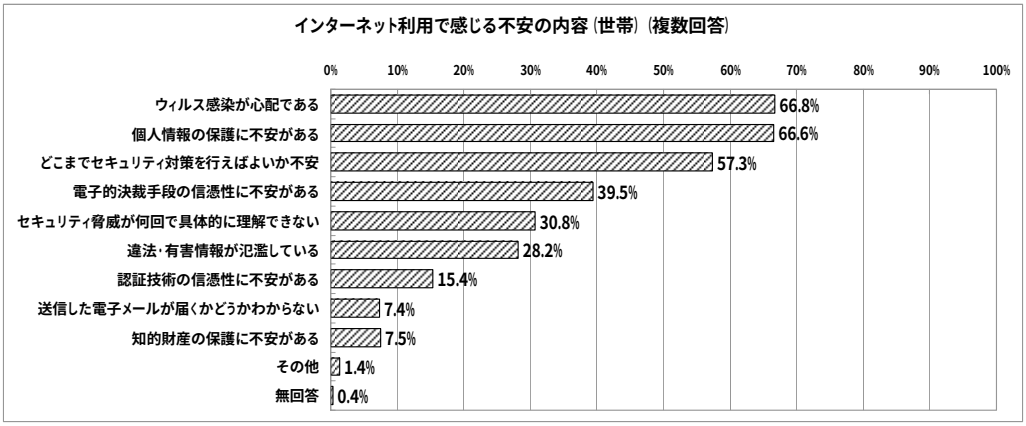
企業や官公庁における情報漏えいは、ここ数年来、継続して発生しており、2007 年 10 月に公表されている「2006 年情報セキュリティインシデントに関する調査報告書 Ver.0.2.00」（NPO 日本ネットワークセキュリティ協会）によると、2006 年の個人情報漏えいの公表件数は 993 件となり、2005 年の 1,032 件と同規模の件数となっている。また、同年の情報漏えいの特徴としては、情報漏えいの対象となった人の数が 2005 年は約 880 万人であったのに対し、2006 年ではその 2.5 倍に相当する 2,200 万人に増加し、1 件あたりの被害が大幅に増大していることを示している。

情報漏えいの原因としては、紛失・置忘れ（29.2%）、盗難（19.0%）、誤動作（14.7%）、ワーム・ウィルス（12.2%）の順となっており、2006 年と同様の傾向を示しているが、特にワーム・ウィスルが原因とされる情報漏えいに関しては、2006 年が 1.1%であったのに対して急増している。これは、Winny や Share といった自動転送型ファイル共有ソフトを介して拡散する暴露型ウィスルによる個人情報漏えいによるものと分析されている。

（4）インターネット利用における不安感

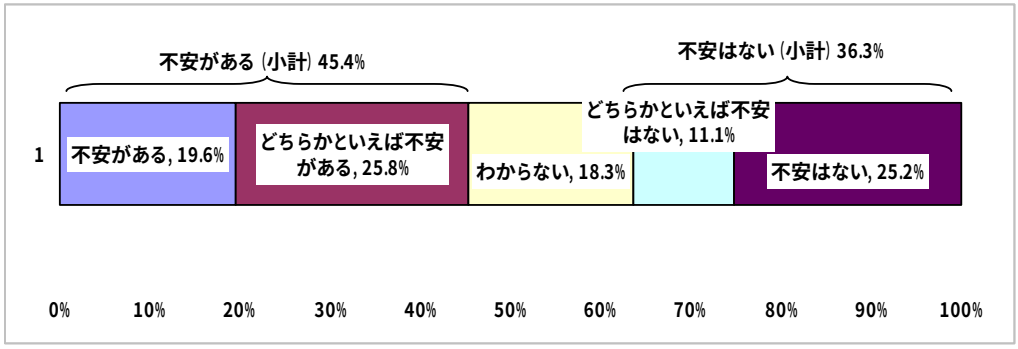
2006 年末現在、インターネット利用世帯の 4.0%以上は、その利用に何らかの不安を抱えている状況であり、その主たる要因としては、「ウィルスの感染が心配である」が 66.8%、「個人情報の保護に不安がある」（66.6%）、「どこまでセキュリティ対策を行えばよいか不明」（57.3%）の順となっている。このインターネット利用に対する不安感については、内閣府が 2007 年 11 月に実施した調査においても 40%を超える結果となっており、依然として、不安感は解消されていない状況にあることを示している。

図表．インターネット利用で感じる不安の内容



（出典：平成 18 年度通信利用動向調査　総務省）

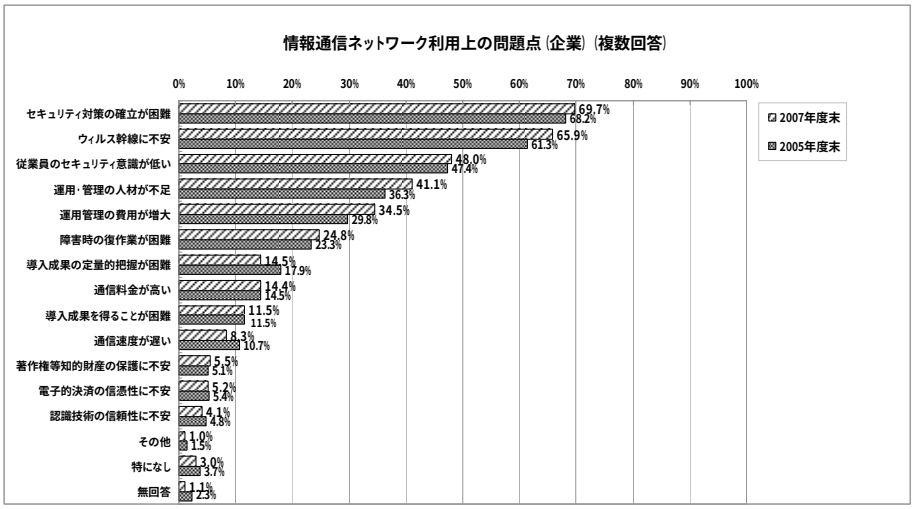
図表．インターネット利用に対する不安感



（出典：内閣府調べ　2007 年 11 月）

また、2006 年末現在、企業における企業通信網、インターネットなどの情報通信ネットワークの利用上の問題点として、「セキュリティ対策の確立が困難」が 69.7%、次に「ウィルス感染に不安」が 65.9%と「セキュリティ関連」が上位を占めている。

図表．情報通信ネットワーク利用上の問題点（企業）（複数回答）



（出典：平成 18 年情報利用動向調査　総務省）

（5）利用者のセキュリティ対策実施状況

最も基本的な情報セキュリティ対策のひとつであるパスワード管理の国際比較において日本は、パスワードを頻繁に変更する利用者の割合が、わずか 13%にとどまっており、調査を実施した 8 カ国中最下位となっている。日本以外の調査対象国においてパスワードを頻繁に変更すると回答した利用者の状況は、ブラジル 51%、中国 39%、オーストラリア 38%、イギリス 30%、ドイツ 25%、アメリカ 22%、フランス 21%となっている。

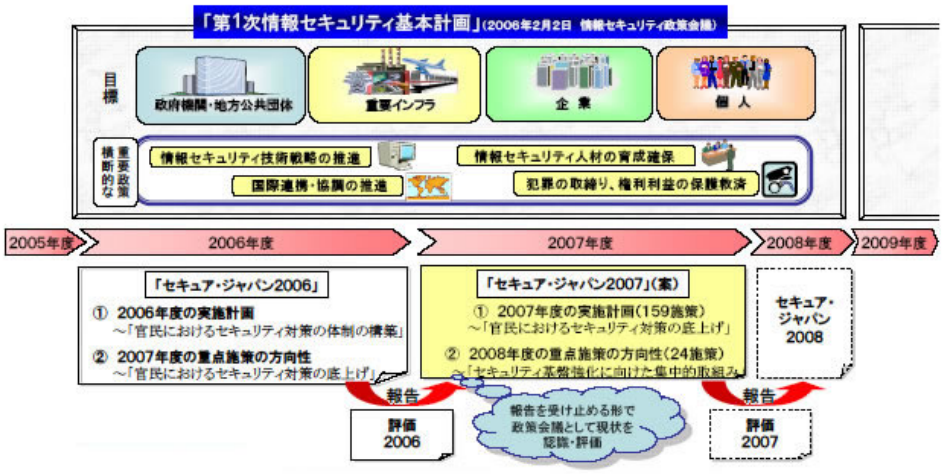
また、子どもがインターネットで何をしているかを、親子でオープンに話す家庭の割合においても日本は 22%と最下位となっており、他の調査対象国では、中国 71%、オーストラリア 59%、ブラジル 59%、フランス 54%、アメリカ 50%、ドイツ 45%、イギリス 44%となっている（出典：シマンテック「ノートン・オンライン生活リポート」2008 年 2 月）。

３．２　我が国の情報セキュリティ対策に関する取り組み

我が国では、ネットワーク利用の高度化に伴う負の側面への対応として、次のような対応を行っているところである。

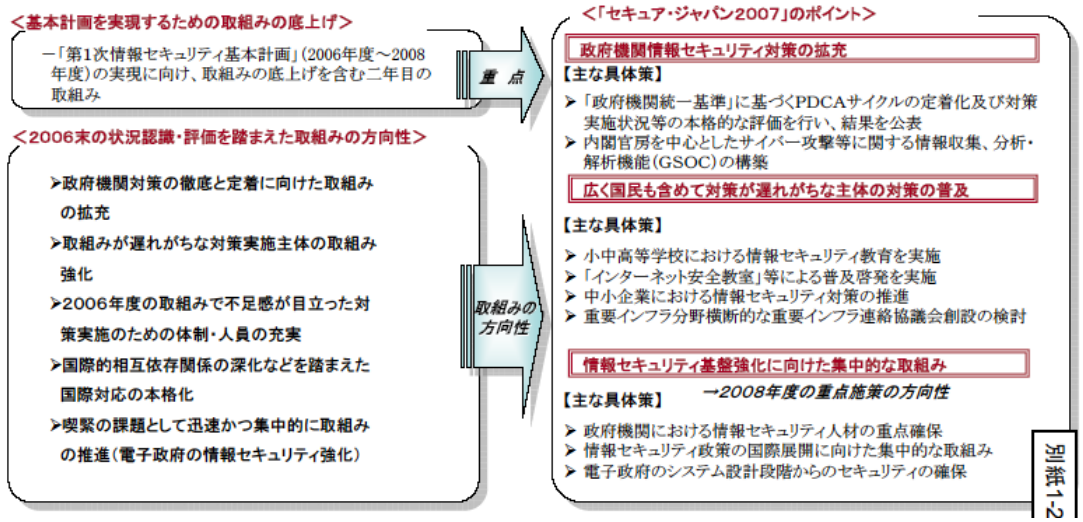
		主な国の取り組み	
2004 年 (平成16年)	7 月	「情報セキュリティ基本問題委員会」の設置	内閣官房セキュリティ推進室
	11 月	「第 1 次提言」の発表	
	12 月	「国会情報セキュリティセンター」設置の検討	
		「情報セキュリティ政策会議」の設置	
2005 年 (平成17年)	4 月	「内閣官房情報セキュリティセンター (NISC)」の設置	内閣官房セキュリティセンター
	7 月	第 1 回情報セキュリティ政策会議の開催	
2006 年 (平成18年)	2 月	第 1 次情報セキュリティ基本計画決定	
	6 月	「セキュア・ジャパン 2006」決定	
2007 年 (平成19年)	6 月	「セキュア・ジャパン 2007」決定	

図表．「第 1 次情報セキュリティ計画」の概要と「セキュア・ジャパン 2007」の位置づけ



（出典：「セキュア・ジャパン 2007」事務局説明資料　2007 年 6 月 14 日　内閣官房情報セキュリティセンター）

図表.「セキュア・ジャパン 2007」のポイント



(出典:「セキュア・ジャパン 2007」事務局説明資料　2007 年 6 月 14 日　内閣官房情報セキュリティセンター)

このように国では、情報セキュリティ対策に関する専門の組織を設置するなど、積極的な取り組みを実施しており、今後、情報セキュリティ政策は 3 カ年計画の実施最終年である 2008 年度に向けて、年度ごとに推進計画を策定・推進していくことになっている。

３．３　情報セキュリティ対策におけるマネジメントの重要性

（1）情報セキュリティガバナンスとは

情報セキュリティガバナンスとは、「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」（平成 17 年 3 月　経済産業省）によると、「社会的責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義されている。ところで、コーポレート・ガバナンス、内部統制、リスク管理とは、経済産業省の「企業行動の開示・評価に関する研究会」の報告書では、次のように定義されている。

■ **コーポレート・ガバナンス**
「企業経営を規律するための仕組み」とする。

■ **リスク管理**
「企業経営者が企業経営を行い、利益を追求していくうえで、企業を取り巻くさまざまな事象が抱えている不確実性（企業経営にマイナスの影響を与える不確実性だけでなく、プラスの影響を与えるそれも含む）というリスクに個々に対応するのではなく、経営理念、事業目的等に照らして経営に重大な影響を及ぼすリスクを企業経営者が認識・評価し対応していくマネジメントの一つ」とする。

■ **内部統制**
「企業経営者の経営戦略や事業目的等を組織として機能させ達成してくための仕組み」とする。

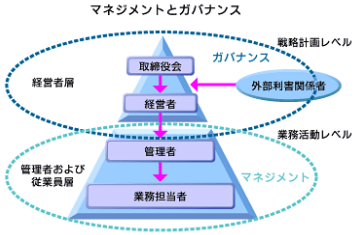
（出典：「企業行動の開示・評価に関する研究会中間報告書」平成 17 年 8 月　経済産業省）

一方、情報セキュリティにおけるマネジメントについては、ISMS（情報セキュリティマネジメントシステム）において、次のように定義されている。

■ **情報セキュリティのマネジメント**
マネジメントシステム全体の中で、事業リスクに対する取り組みにもとづいて、情報セキュリティの確立、導入、運用、監視、見直し、維持および改善を担う部分

つまり、情報セキュリティマネジメントを確立する前提条件として、情報セキュリティガバナンスは位置づけられると解釈でき、両者には密接な関係があると理解できる。

図表．ガバナンスとマネジメントの関係



（出典：「情報セキュリティのガバナンスとマネジメント」@IT 情報マネジメント）
URL：http://www.atmarkit.co.jp/im/cop/serial/secgov/06/01.html

（2）情報セキュリティガバナンスの必要性

企業・自治体といった組織が、自身の被害の局限化や法令遵守の観点に加え、社会的責任の観点も踏まえた形で情報セキュリティ対策に積極的に取り組むようになるためには、「情報セキュリティに絶対はなく、事故は起こり得るもの」との前提に立ち、対策をその場しのぎの対処療法的対応で済ませるのではなく、自律的・継続的に改善・向上する仕組みを導入することが必要となる。つまり、社会的な責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを情報セキュリティの観点から企業内に構築・運用すること、すなわち「情報セキュリティガバナンス」の確立が求められる。内部統制の仕組みを適用することで情報セキュリティ対策の自律的・継続的な推進が効率的に実現できると考えられる。

具体的には、コーポレート・ガバナンスの整備に合わせて情報セキュリティガバナンスを確立していくというアプローチもあるが、情報セキュリティガバナンスの確立を契機として、コーポレート・ガバナンスの本格的な整備を促進していくというアプローチもあり得る。

なお、情報セキュリティガバナンスの確立に際しては、IT 事故の影響を懸念するあまり、IT の利便性を犠牲にするのではなく、リスクを需要範囲内に入るようにマネジメントし、利便性と安全・安心の両立を目指していくことが重要である。

（3）情報セキュリティガバナンスの確立に向けた施策ツール

企業・自治体における情報セキュリティに係る取り組みは、さまざまな内容で行われているものの、情報セキュリティに関する事故はあとを絶たない。また組織として、どういったところに対して、どのような対策を行えば良いのかの判断しにくい問題もある。このような問題点を克服し、情報セキュリティガバナンスの確立を促進するための施策ツールとして、「企業における情報セキュリティガバナンスのあり方に関する研究会報告書[2]」（平成 17 年 3 月　経済産業省）では、「情報セキュリティ対策ベンチマーク」、「情報セキュリティ報告書モデル」、「事業継続策定ガイドライン」の 3 種類が提示されている。

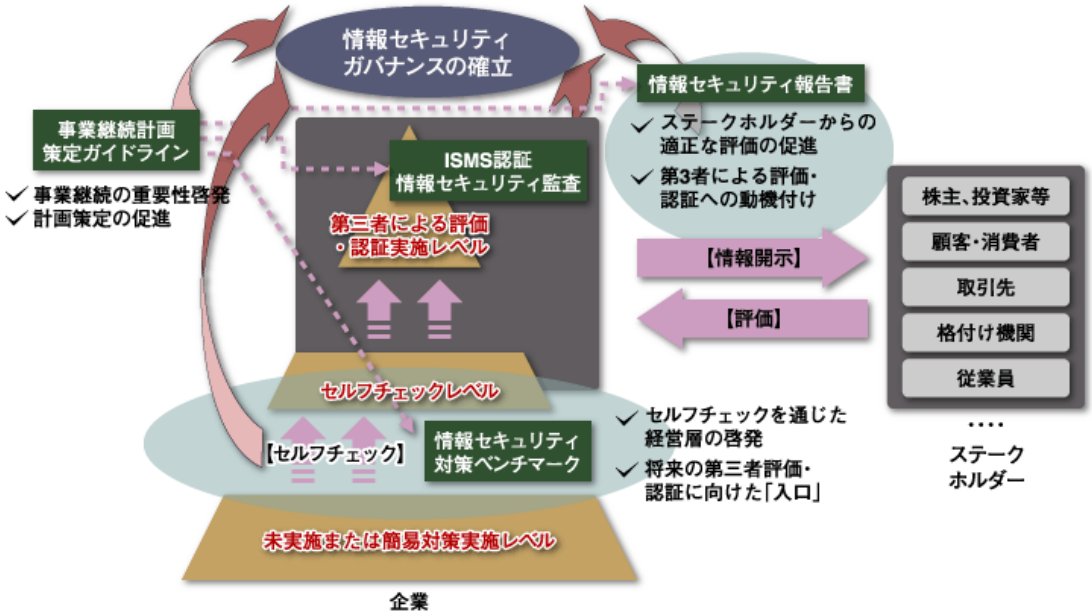
図表．情報セキュリティガバナンスの確立を促進するための施策ツール

施策ツール	概　要
情報セキュリティ対策ベンチマーク	企業の業態や保有する情報資産等の属性をもとに企業等の組織を分類し、それぞれの組織グループの望まれる水準と組織の現状を比較できる自己診断ツール
情報セキュリティ報告書モデル	企業の情報セキュリティの取組の中でも社会的関心の高いものについて情報開示することにより、当該企業の取組が顧客や投資家などのステークホルダーから適正に評価されることを目指すもの
事業継続計画策定ガイドライン	企業・自治体に対し、BCP の概念自体の認知度向上を図りつつ、IT 事故発生時にも事業運営を継続的に維持するのに有効な BCP の普及に寄与すべく、IT 事故を想定した BCP の策定手順や検討項目等を解説する「事業継続計画策定ガイドライン」を策定する

（出典：「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」平成 17 年 3 月　経済産業省などをもとに作成）

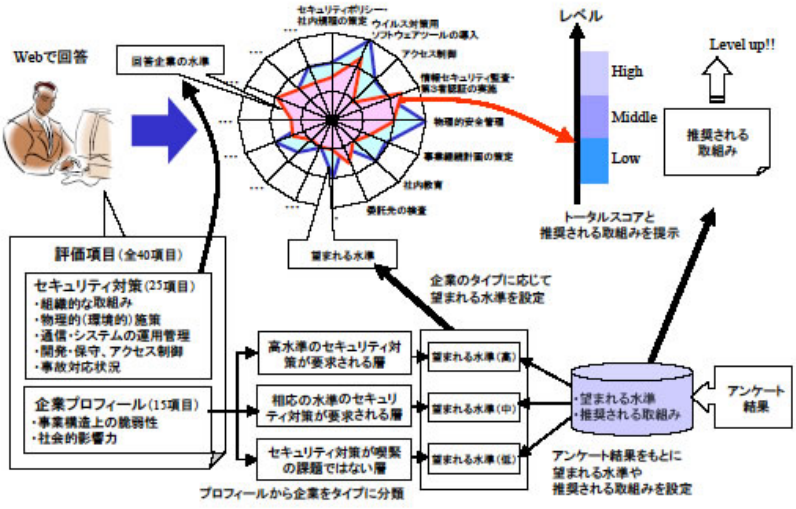
[2] 平成 19 年 8 月 24 日に改訂版として「情報セキュリティガバナンス施策ツールの改訂について」が新たに公表されている。

図表．施策ツールと ISMS 認証などとの基本的関係



（出典:「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」平成 17 年 3 月　経済産業省）

図表．情報セキュリティ対策のベンチマークのイメージ



（出典:「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」平成 17 年 3 月　経済産業省）

（4）情報セキュリティマネジメントの実践

このような情報セキュリティガバナンスにもとづくマネジメントを組織全体で推進していくためには、情報セキュリティ管理(マネジメント)体制を確立し、継続的な活動を行っていく必要がある。この管理（マネジメント）体制に関する要件は JIS X 5080 で規定されている。

図表．情報セキュリティ管理体制に関する JIS X 5080 の要求事項

4．組織のセキュリティ		
4.(1)情報セキュリティ基盤 **管理目的：組織内の情報セキュリティを管理するため。**		
管理策		
4.(1)①	**情報セキュリティ運営委員会**	**セキュリティを主導するための明りょうな方向付け及び経営陣による目に見える形での支持を確実にするために、運営委員会を設置すること。運営委員会は適切な責任分担及び十分な資源配分によって、セキュリティを促進すること**
4.(1)②	**情報セキュリティの調整**	**大きな組織では、情報セキュリティの管理策の実施を調整するために、組織の関連部門からの管理者の代表を集めた委員会を利用すること**
4.(1)③	**情報セキュリティ責任の割当て**	**個々の資産の保護に対する責任及び特定のセキュリティ手続の実施に対する責任を、明確に定めること**
4.(1)④	**情報処理設備の認可手続**	**新しい情報処理設備に対する経営陣による認可手続を確立すること**
4.(1)⑤	**専門家による情報セキュリティの助言**	**専門家による情報セキュリティの助言を内部又は外部の助言者から求め、組織全体を調整すること**
4.(1)⑥	**組織間の協力**	**行政機関、規制機関、情報サービス提供者及び通信事業者との適切な関係を維持すること**
4.(1)⑦	**情報セキュリティの他者によるレビュー**	**情報セキュリティ基本方針の実施を、他者がレビューすること**

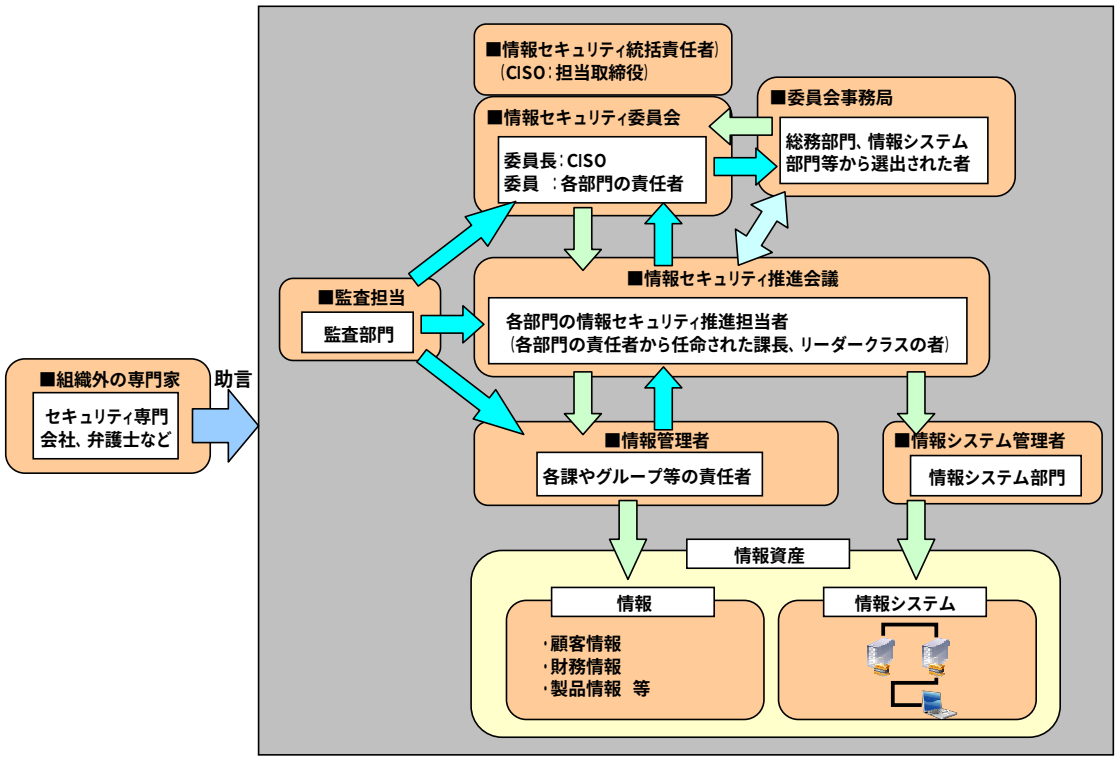
（出典：財団法人日本情報処理開発協会「ISMS 認証基準 Ver2.0」）

これらの中で特に重要といえるのは、「4.(1)③情報セキュリティ責任の割当て」とされている。

（5）情報セキュリティ管理(マネジメント)体制と役割の例

次に、実際に情報セキュリティを管理（マネジメント）するために必要な体制と各役割の例を示す。

図表．情報セキュリティ管理（マネジメント）体制と役割の例



（出典：「情報セキュリティアドミニストレータ 2005 年度版」株式会社翔泳社）

役職	役割
情報セキュリティ統括責任者	当該組織の情報セキュリティマネジメントを統括する最高責任者（CISO：Chief Information Security Officer）であり、社長もしくは社長から権限を以上された取締役（経営責任をもつ者）が担当する
情報セキュリティ委員会	当該組織における情報セキュリティマネジメントに関する意思決定を行う最高機関であり、CISO が委員長を務める。委員は各部門の責任者（本部長、あるいは部長クラスの者）が務める。具体的には次のような事項を決定／承認する役割を担う
情報セキュリティ委員会事務局	総務部門、情報システム部門など、組織内の情報セキュリティ関連部門から選出された担当者が事務局となり、情報セキュリティ委員会の開催、討議事項の取りまとめ、決定事項の周知等の事務作業を行う
情報セキュリティ推進会議	情報セキュリティ委員会の下部組織として、各部門における情報セキュリティマネジメントを実際に推進する役割を担う。同会議への参加者（情報セキュリティ推進担当者）は、各部門の責任者から任命された課長やリーダークラスの者であり、情報セキュリティアドミニストレータの資格保持者であることが望ましい
情報管理者	各課やグループ等の責任者（課長、リーダー等）が、各課やグループ内で取り扱う情報の管理者
情報システム管理者	情報システム部門が情報システムに対するセキュリティ対策の実施・管理等

役職	役割
	の責任者となる。各部門が独自に管理している情報システムについては、当該部門の責任者が管理者となる場合もある
監査担当	情報セキュリティマネジメントの適切性において監査する役割を務めるため、内部監査部門が担当する。内部監査部門がない場合には、ISMS 審査員、システム監査技術者、情報セキュリティアドミニストレータなどの有資格者からなる監査担当チームを編成して対応することもある。その場合には、各監査担当者は自分が所属する部門の監査を行うことがないようにする必要がある
組織外の専門家	必要に応じて、情報セキュリティや法律等の専門知識や技術を有する専門家から、自組織の情報セキュリティマネジメントに対する助言を受ける。セキュリティ専門会社の場合には、外部監査人として監査担当と同様の業務を依頼する場合もある

（出典：「情報セキュリティアドミニストレータ 2005 年度版」株式会社翔泳社資料　をもとに作成）

このように、組織の情報セキュリティマネジメントを推進するためには、情報セキュリティ管理（マネジメント）体制を整備し、その責任や役割を明確にする必要がある。

３．４　今後、情報セキュリティ対策で重点的に検討・実施すべき項目

情報セキュリティ対策の重要さは、これまで述べてきたとおりであるが、関西情報化実態調査の結果や各方面で実施されているアンケート結果などを見ると、情報セキュリティ対策の必要性（教育を含む）は認識しているものの、実態としてそれほど重要視されていない（あるいは、費用や人的資源をかけられない）等の現実も見られる。さらに中堅・中小企業などの小規模な組織体では、そもそも情報セキュリティ対策の重要性についての認識が低いという実態も見られる。

ここでは、このような現実を踏まえて、今後もより一層、情報化社会が安全・安心に進展していくために重点的に検討・実施すべき項目について、所見を述べる。

（1）情報利用主体者を取り巻く環境における情報セキュリティ対策の徹底

情報利用主体者における情報セキュリティ対策の徹底は、最も基本的な対策である。

サービス提供事業者や機器製造事業者、電気通信事業者等のITサービス提供者側が事前に想定し得る対策を講じた製品・サービス等を提供しなければならない責任を有していることは、そもそもの前提であるが、適切な情報セキュリティ対策を行わない情報利用主体者が、ボット等のマルウェア[3]に感染すること等によって、自らが被害者となるだけでなく、情報利用主体者が気づかないうちに他人に被害を及ぼす加害者になってしまうことを鑑み、「利用者は、インターネットをはじめとしたITを利用する際の社会的責任として、必ず一定程度の基本的な情報セキュリティ対策を講じなければならない」と考えること、また、このような考えを持つ社会的な土壌を醸成する必要があると考える。

しかしながら、小規模事業者や個人ユーザなどの必ずしも情報セキュリティ対策をはじめとする情報セキュリティが高くない利用者もインターネット等を利用することを考慮し、IT サービス提供側で、情報主体利用者間や情報主体利用者と IT サービス提供者側との間で生じた問題（紛争等）を迅速に解決する体制、電気通信事業者や IT サービスを利用する企業等における情報セキュリティ対策コスト負担のあり方、サイバー犯罪等に関連する法制度の検討・執行状況、電気通信事業者や IT サービスを利用する企業等における事業継続性等を勘案した実効性のある対策のあり方等については、継続的に検討を進めることが必要である。

（2）産学官連携による先進的な研究開発の実施

官の取り組みは、先述のとおり 2005 年 4 月に内閣官房情報セキュリティセンター（NISC）が設立され、同センターが中心となり、各種の情報セキュリティ対策に関する研究や指針などについて取りまとめている。

一方、平成 18 年度より文部科学省で実施されている「先導的 IT スペシャリスト育成推進プログラム」では、平成 19 年度に採択された通称「IT Keys（奈良先端科学技術大学院大学、大阪大学、京都大学、北陸先端科学技術大学院大学）において、情報セキュリティ対策の立案・遂行を実施する実務者の育成を目標とする研究を行っている。この中で、サイバークリ

[3] マルウェア：ウィルスやスパイウェアを含めた「悪意のあるソフトウェア」の総称。他人のパソコンやネットワークにウィルスを感染させる、パソコン内の個人情報を盗む、フィッシング詐欺ページに移動させるなど、被害をもたらすように作られたソフトウェア全般をマルウェアと呼ぶ。

ーンセンターでは、情報処理学会と連携し、業務において取得したマルウェア検体や攻撃が含まれた通信データを活用して、ネットワークインシデント解析、可視化技術等に関するコンテストを行うワークショップの開催を計画している。

このような産学官が連携した人材育成の取り組みが、より活性化することが重要である。

（3）ユビキタスネットワーク社会における情報セキュリティ対策に関する業界横断的な検討体制の整備

ユビキタスネットワーク社会において、利用者が安心・安全にさまざまな情報通信機器・端末を駆使し、多様なサービスを利用できるようになるには、電気通信事業者、OS/アプリケーション/サービス提供事業者、今後普及が予想される情報家電を含む情報通信機器・端末の製造・販売事業者、情報セキュリティ関連事業者等が、それぞれ独自に情報セキュリティ対策を実施するだけでなく、お互いに協調・連携することが重要である。

このため、上記のようなすべての関係者が参加し、継続的に情報セキュリティに関連する課題や、その対策等について検討する業界横断的な検討体制を整備する必要がある。

（4）利用者、情報通信環境、情報セキュリティが共生するIT社会モデルの検討

将来の情報通信環境では、複数の関係者が関連してサービスが提供され、またネットワークに接続される端末や利用者数、情報量が爆発的に増加することが予想されており、こうした複雑化が進む状況において、情報セキュリティを検討するにあたっての参照モデルが確立されていないことの指摘がある。

このため、ITサービスの多様性・利便性を確保しつつ、あわせて情報セキュリティ対策が施されている環境を、「利用者（利便性）、情報通信環境（多様なサービス）、情報セキュリティが共生するIT社会モデル」として実現することについて、具体的な実証モデルを構築して、その有効性や課題の検証を進めることが重要である。