産業構造審議会情報セキュリティ基本問題委員会

中間とりまとめ

～企業における戦略的な情報セキュリティガバナンスの確立に向けて～

平成 20 年6月

目　次

はじめに

平成 15 年 10 月、産業構造審議会情報セキュリティ部会では、「世界最高水準の『高信頼性社会』実現による経済・文化国家日本の競争力強化と総合的な安全保障向上」という基本目標を掲げ、「しなやかな『事故前提社会システム』の構築」を始めとする「情報セキュリティ総合戦略」をとりまとめた。同戦略の実現に向けて、平成 17 年 3 月、経済産業省に設置された「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」は、企業が対症療法的な対策から脱却し、自律的・継続的な取組を推進していくため、「情報セキュリティガバナンス[1]」の考え方を企業経営に組み込むことの重要性を掲げ、その実現を促すツールとして「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」及び「事業継続計画策定ガイドライン」を策定した。従来から経済産業省が促進してきた情報セキュリティマネジメントシステム適合性評価及び情報セキュリティ監査と併せ、企業の自律的な対策を支援する環境の充実を図ったものである。

こうした中、今後 IT が、我が国だけではなく世界の経済社会の隅々に行き渡り、経済社会システムに融合した密接不可分のものと化していくことを見据え、平成 19 年 5 月、情報セキュリティ基本問題委員会は「グローバル情報セキュリティ戦略[2]」と題した報告書をとりまとめた。同報告書では、「情報セキュリティ総合戦略」で掲げられた基本目標に加えて、「我が国経済社会が直面し続ける『変化と挑戦』を支える情報セキュリティの実現」という基本目標を設置し、目標達成に向けた戦略を示している。

同報告書において、「企業」の領域に関しては、中小企業に対してより細かく配慮しつつ、情報セキュリティガバナンスの概念の更なる普及、業務効率化・知財管理強化といった競争力強化の視点から企業が戦略的に情報セキュリティ対策を実施していくための基盤醸成の必要性について提言した。特に、企業活動が国境を越えてグローバルに展開されている現状に合わせ、世界に向けた情報セキュリティに係るジャパンモデル、ジャパンクオリティの発信を通じて、豊かで強く魅力ある日本経済の実現を情報セキュリティの側面から支援することが重要であると指摘した。

これらの指摘、提言に基づき、経済産業省では、「グローバル情報セキュリティ戦略」で提言された事項をグローバルなビジネス環境にインプリメントすべく、平成 19 年度から、競争力強化の視点に沿った企業における情報セキュリティガバナンスの確立・普及のための施策の検討に取り組んでいる。当委員会は、経済産業省にお

[1] 情報セキュリティガバナンス：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。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」経済産業省、平成 17 年 3 月

[2] http://www.meti.go.jp/press/20070510001/20070510001.html

ける検討の進捗状況を踏まえつつ、企業の経営者が情報セキュリティガバナンス確立のために考慮すべき事項とそれを支援するために必要な施策について審議を行い、ここに、戦略的かつ適正な情報セキュリティガバナンスの確立のための環境整備に関する提言を行うべく中間とりまとめを行った。

なお、「グローバル情報セキュリティ戦略」では、企業以外の領域についても提言を行っている。政府機関・重要インフラの領域については、原則として、情報セキュリティ政策会議及び内閣官房情報セキュリティセンターを中心に適切かつ着実に政策が推進されるべきであることを指摘した。また、個人の領域に関しては、万全を期していても事故は発生し得るものであるという事故前提社会の中で安全にＩＴを利活用することができるよう、情報提供を通じてリテラシーの向上を図るとともに、社会的・国民的運動を強力に展開し、セキュリティ文化を実現するための基盤醸成の必要性を指摘したところである。企業以外の領域及び研究開発等の横断的基盤の領域についても、継続的に経済産業省等の取組状況を点検することとする。

第1章　企業戦略における情報セキュリティの位置づけ

（１） 情報資産の利活用と管理

近年、IT を企業基盤として利活用することで組織横断的な情報の共有化を図り、更に業務及び企業全体構造の最適化を図り競争力強化につなげるといった IT ガバナンスの必要性が重要視されている。そこで、我が国企業における IT 投資実態を明らかにするため、平成 15 年、経済産業省「情報技術と経営戦略会議」は、我が国企業の IT 投資実態について検討を行い、企業の情報技術利活用を４段階に分類した（図 1)。全体最適化段階にある企業では、IT 導入と業務改革が一体化することで、現場に散逸している知見や情報を有効に活用し、競争力向上に取り組んでいることを示した 。また、その後の調査で、全体最適化に向け利活用の段階が高まるほど、企業の業績も向上していること、米国では、全体最適化段階の企業比率が高いことなどが確認された[3]。引き続き、平成 17 年、平成 18 年と同様の調査を行ったが、我が国上場企業では全体最適段階と部分最適段階の企業群の比率は 3:7 から大きく変化していない。この現状を踏まえ、経済産業省では部分最適段階からの脱却方策について集中的に討議を実施するため、平成 19 年 11 月から、全体最適段階にある企業の CIO を中心に、その他専門家などから構成される CIO 戦略フォーラムを開催し、IT 経営の改善に向けロードマップの策定に取り組んでいるところである。

さらに、経済産業省「産業構造審議会情報経済分科会」では、「情報経済・産業ビジョン概論」（平成 17 年 4 月）において、情報を「つなぐ」ことの意義及び情報を「つなぐ」状態にする仕組みの構築の重要性を指摘した。同分科会では、引き続き、個人や現場に散逸している知見や情報が本来生み出すべき付加価値を最大化するためのバリューチェーンの再構築に向けた検討を行っているところである。

図 1 で示されるように、企業が最適化されたバリューチェーンの形成及びグローバル市場への展開といった、より高いステージへ上るためには、企業が所有する情報の価値を正しく把握し、適切に扱うことが必要要件となる。ステージを上がると、情報を保有する形態、範囲等が変化することから、企業の抱えるリスク要因にも変化が生じ、それまで存在していたリスクが解消される可能性がある一方で、新たなリスクが生じる可能性もあることに注意が必要である。企業が価値を有すると考える情報等（情報資産）の利活用範囲が拡大するほど、情報資産管理の成否の鍵とし

[3] 部門や企業の壁を越えて IT を最適に活用している企業の割合は、米国が 54%であるのに対し、日本では 26%にとどまっている（平成 19 年 3 月)。企業内で IT を最適に活用している企業（第 3 段階)、企業を越えて IT を最適に活用している企業（第 4 段階）は、部門内で IT を活用している企業（第 2 段階）よりも、企業レベルでの全要素生産性の成長率が、それぞれ 3%、5%高くなっている。(「IT による生産性向上の加速化に向けて」 産業構造審議会情報経済分科会 平成 19 年 6 月）

て、情報の所有者が当該情報資産をどのような範囲でどう共有するかを定めておくことの重要性が高まる。こうした取組は、企業戦略に直結することから、経営層が積極的に関与することが必要である。

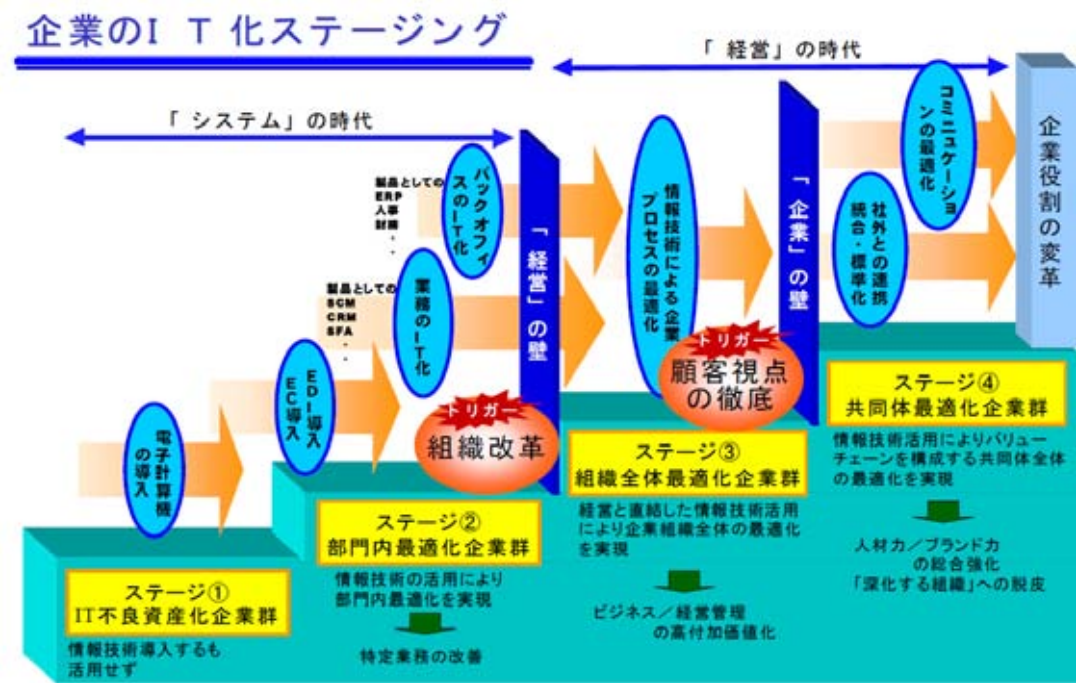


図 1 IT 投資のステージング

（出典：経済産業省 情報技術と経営戦略会議＜提言＞平成 15 年 10 月）

情報共有は、ただ無目的に全社ベースで行っても効果を伴わない。経営戦略から得た視点に基づき、その情報の意味・役割と使い方を徹底的に検討した上で必要な範囲で行うことが不可欠であり、必要な情報の品質を維持・向上し続けることが重要である。そのためには、それぞれの情報について、IT ベンダや情報システム部門だけではなく、関係する業務現場自らがしっかりと責任を持って正しいデータを設計・開示すること、あわせて、その目的に即した情報セキュリティ管理（情報システムのみならず情報そのものの管理を含む。）を導入することが不可欠となる。

IT 投資効果がより厳しく問われるようになった結果、企業の情報セキュリティ管理も、企業内 IT インフラにおける技術的な基盤の強化に重点投資する時代から、情報利活用の目的に照らして、業務現場と柔軟に協力していけるような IT ガバナンスの能力そのものが問われる時代へと、変化しつつある。

（２） 適法性と適正性

企業における情報資産の効率的・効果的利活用は企業価値向上の観点において極めて重要であるが、企業が保有する情報の中には法令や契約で利用が制限されてい

るものが含まれ、取扱にリスクが伴うケースもあることに注意が必要である。例えば、個人情報取扱事業者[4]は、個人情報の保護に関する法律（以下「個人情報保護法」という。）により、顧客等から預かった個人情報を管理する上で安全管理措置を実施することが義務付けられている[5]。上場企業は、その財務情報の取扱にあたり、金融商品取引法により正確性の確保が求められる。また、業務上の取引先の営業秘密を保有する企業には、取引先との間の機密保持契約上、対象となる情報を適切に管理することが求められる。

会社法では、内部統制システム構築の基本方針の決定を、大会社・委員会設置会社の取締役の義務と定めており[6]、会社法施行規則では、決定すべき基本方針の対象として「損失の危険の管理に関する規程その他の体制」すなわちリスク管理体制が挙げられている[7]。対象となるリスクには、会社が保有する情報や事業に活用されている IT に係るリスクも含まれると考えられるため、企業の経営層は情報資産に係る必要なリスク管理体制（法令遵守体制を含む。）、すなわち情報セキュリティへの取組が求められることとなる。特に、企業の業種、規模等によっては、情報セキュリティ対策の実施が取締役の善管注意義務とみなされる場合もあることから、企業は、適法性を意識した情報セキュリティを考慮しなければならない。

また、我が国の社会や顧客等は、企業に対して適法性のみならず適正性を期待することがあることへの配慮も必要と考えられる。情報セキュリティの分野では、適切な対策を実施していたとしても事故を完全に防ぐことは難しい。しかし、実際に事故が発生した場合、企業が適法な範囲で事故に対処したとしても、適法というだけでは社会や顧客等から評価されないことがある。過去の事故対応事例においては、企業がより徹底した情報開示と被害者への対応を実施し、さらに、被害が及んでいるかもしれない利用者への対応に積極的に取り組むことで、初めて社会や顧客等から高い評価を受けたという状況が見られる。

ただし、情報セキュリティ対策を過剰に優先することが、業務プロセスの円滑な進行を必要以上に阻害してしまう事態や、必ずしも適法性が認められるわけではない事態も招く可能性のあることに留意すべきである。例えば、全ての顧客からの問い合わせメールを社長自ら確認した後回答することとしたため、回答までに長時間を要し、顧客からの苦情が大幅に増加したケース、情報セキュリティ対策を理由に、

---

[4] 個人情報保護法第二条３項で、「この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。一 国の機関 二 地方公共団体 三 独立行政法人等 四 その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者」と定義される。四は政令で「個人情報が数の合計が過去六月以内のいずれの日においても五千を超えない者とする。」とされており、個人情報を 5,000 件以上保有する事業者はすべて該当する。

[5] 個人情報保護法第 20 条

[6] 会社法第 348 条・第 362 条・第 416 条

[7] 会社法施行規則第 98 条、第 100 条及び第 112 条

技術供与ライセンスを与えた者に対して開示した技術情報を基に当該者が新たに創出したノウハウ等までも利用制限を課すといった適法性に疑義があるケース[8]などである。企業は、社会等からの情報セキュリティへの要求と企業活動としての取組との間で合理的な調和を図りつつ対応することが望まれるが、情報セキュリティの分野では、どこまで行えば十分かわからず、全体最適化を考慮せずに過重な対策を行ってしまう場合があることへの対応も求められている。

（３） 社会的責任と情報セキュリティ

企業に対して、顧客、社会等の利害関係者による透明性や情報開示を求める声が高まる今日、企業によるリスクなどの情報の開示、説明責任が求められている。

この社会的責任について、米国の代表的な経営学者であるマイケル・ポーター[9]は、「『受動的 CSR[10]』を超えて『戦略的 CSR』を推し進めることで、新たな競争優位を築き、持続的成長への道を拓く」ことを提唱し、「事業上の判断を下す場合と同じフレームワークに基づいて、企業の社会的責任への対応を判断することができれば、CSR はコストでも制約でも、また慈善行為でもなく、ビジネスチャンスやイノベーション、そして競争優位につながる有意義な事業活動である[11]」と指摘している。すでに欧州では「市場での事業活動を通じた CSR の実践」が企業戦略に根付きつつあることから、我が国においても、CSR を企業価値の向上に資するための戦略的な活動ととらえ、CSR を通じた企業の持続的な成長を意識することが重要であるとの意見もある[12]。

平成 18 年度に実施された警察庁の調査[13]によると、企業の情報セキュリティ対策の方針・目的（複数回答）について、「個人情報保護のため」という回答が 84.4%と最も高く、次いで「社会的責任を果たすため」（72.0%）、更に「リスクマネジメントの一環として取り組んでいるため」（62.2%）、「セキュリティ事故がブランドイメージや業績に与える影響を避けるため」（58.7%）、「法律に従う必要があるため」（51.8%）などの回答が続いている。このように、我が国企業において、情報セキュリティ対策の目的は、社会的責任を果たすためのもの、すなわち、情報セキュリティの向上が社会的責任の一つとして高く認識されていると考えられる。

---

8 鈴木満,「独占禁止法からみた企業の秘密情報保護活動の問題点」桐蔭論叢,第 15 号,2006 年 12 月

9 Michael E. Porter、Bishop William Lawrence University 教授

10 Corporate Social Responsibility、企業の社会的責任

11 マイケル・ポーター「戦略と社会：競争優位と CSR のつながりについて」, Harvard Business Review 平成 18 年 12 月号

12 経済同友会「CSR イノベーション-事業活動を通じた CSR による新たな価値創造-日本企業のグッド・プラクティス 2007」平成 19 年 5 月

13 警察庁「不正アクセス行為対策等の実態調査報告書」平成 18 年 1 月

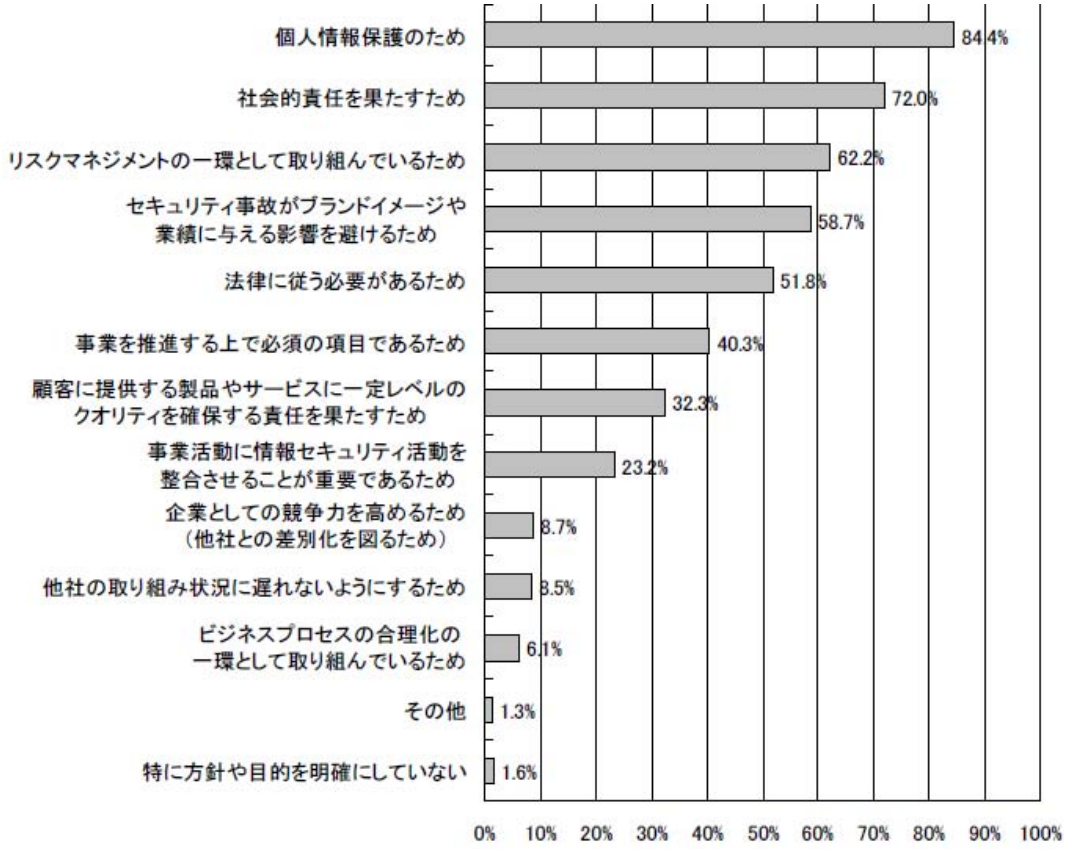


図 2 情報セキュリティ対策の方針・目的（複数回答可、N=1024）

（出典：警察庁「不正アクセス行為対策等の実態調査報告書」）

一方で、例えば、同調査において「企業としての競争力を高めるため」という回答が 8.7%にすぎないとの結果も出ている。多くの企業が守備的、受動的な意味で情報セキュリティ対策を行っており、情報セキュリティの向上が社会から求められる状況を「機会（Opportunities）」として捉える戦略的な取組、すなわち戦略的 CSR として取り組んでいる企業はまだ少ないのではないかと考えられる。

また、企業は、事業目的達成の観点から事業継続は不可欠であるが、顧客や取引先を含むサプライチェーン全体から見た事業継続に対しても重要な責任を有している。特に、IT が事業の基盤として利用されている場合には、IT サービス[14]の観点も含めた事業継続管理への適切な対応も求められる。「情報セキュリティ総合戦略[15]」では「しなやかな『事故前提社会システム』の構築」を掲げたが、まさにこれは「情報セキュリティに絶対はなく事故は起こりうるもの」との前提に立って、事前・事後のバランスが取れたリスク管理を提唱したものである。企業が、こうしたリスク

14 IT サービスとは、組織における業務の遂行に際して必要となる IT 等によって提供される機能をいう。

15 経済産業省「産業構造審議会情報セキュリティ部会」報告書 平成 15 年 10 月

管理の一つとして、IT サービスの観点も含めた事業継続管理を行うことは、取引先、顧客、株主等に対する責任のみならず社会的責任としても求められることがあると考えられる。

環境報告書の例[16]などに鑑みると、社会的責任を果たす重要な手段の一つとして、社会、顧客、市場等に対して情報セキュリティに対する取組状況の開示・説明が考えられる。例えば、上場企業において有価証券報告書におけるリスク情報開示の一環等として情報セキュリティに係る取組を予め開示している企業の場合、情報流出などの情報セキュリティ関連事故が発生した直後に株価は一旦下落するものの、その後、上昇基調に転じている現象が見られる一方で、開示に消極的な企業の場合、情報セキュリティ関連事故発生後、株価が下落し、一定期間をおいても下落に歯止めがかからないとの研究[17]もある。この現象は、自社に内在している情報資産に係るリスクを開示するという企業の姿勢が社会や市場によって高く評価された結果であるとも考えられる。

（４） 情報セキュリティへの取組と企業戦略を整合させることの重要性

企業は、適法性と適正性、社会的責任を考慮しつつ、情報資産の利活用と管理の高度化に取り組む必要がある。そのためには、経営層が情報セキュリティを企業戦略の中に整合的かつ明確に位置づけて推進することが重要である。次に示す事例は、リスク管理の一環としての情報セキュリティに係る取組を、企業の事業目的追求のために効果を発揮させる積極的な活動として、経営層の意志の下で、企業戦略の一部に位置づけているものであると考えられる。

16 例えば、環境報告書に関し、事業者は環境に関する情報を公開していく社会的責務があるとの考え方も広まりつつあると説明されている。http://www.env.go.jp/policy/j-hiroba/04-4.html
17 伊藤邦雄「コーポレートブランド価値向上のための情報セキュリティガバナンス」, 情報セキュリティガバナンスシンポジウム 2008 特別講演（平成 20 年 3 月 5 日）

［戦略的に情報セキュリティ対策を行っている事例］

あるドキュメント・ソリューションを提供する企業では、同社の情報セキュリティガバナンスの社内実践経験を、同社が提供するソリューション・サービスに取り込んで、顧客に実践可能なソリューションとして捉えてもらうという戦略をもっている。また、自社でソリューションを実施するので、その結果は社内の情報セキュリティ対策にフィードバックできるという PDCA サイクルも確立されている。

ある OA 機器・ソリューションのメーカーでは、グローバルの顧客へ提供する商品・サービスのセキュリティレベルを向上させるため、国内外の主要なグループ会社・事業所全体で ISO/IEC 27001 に基づく統一認証を取得。さらに独自の実施基準を用いた活動を展開し、グループ内の情報セキュリティレベルを向上させると共に、蓄積したノウハウ・実践事例に基づいたビジネス展開を図っている。

ある情報システムを用いたサービスを提供する企業では、IT を用いた新たな価値を提供するために、情報を適切に取扱い、顧客に信頼される情報システム構築をすべく、自ら企業グループ全体で情報セキュリティ対策を実践する戦略を持っている。このため、グループ企業間での情報共有を積極的に行うための統一セキュリティポリシーを策定し、グループ企業間で平等に監査をしあう体制を整備している。

あるエレクトロニクス製造・販売企業では、技術情報管理サーバのセキュリティの実態を調査し改善していく過程で、台数を大幅に削減することに成功した。また、個人情報についての実態把握と不要な情報を削減することで、データ数を適正規模に抑制することができた。結果的にリスクを減らすとともに、管理コストや電力消費量を画期的に削減することに成功した。

ある食品製造・販売企業では、新鮮な商品を全国の消費者に提供するためには、一部地域の被災によるリスクを最小化するための全社的な事業継続計画が必要で、そのために実現可能な IT 継続計画が求められた。このため、データセンターのある地域との同時被災確率の極めて低い地域に、バックアップセンターを構築。将来的にはこれをメインセンターとして、国際的 HUB 拠点とした海外グループ企業間との効率的なネットワークを構築していくことも検討している。

今後、情報資産の共有化・最適化が進展していくにつれ、これらのような情報セキュリティの目標を、事業目的等と整合的なものとし、情報資産の利活用とそのリスク管理を同時に達成するような戦略的な取組が増加していくことが期待される。

第2章　情報セキュリティガバナンスの確立とその実現に向けた課題

（１） 情報セキュリティガバナンスとは

企業内及び企業間における情報資産の利活用及び共有が付加価値向上の源泉となっている。一方、適切な管理を行わずに利活用の範囲を拡大することは、技術情報、営業情報といった競争力に影響を与える情報の流出、消失といったリスクを増大させることにもつながりかねない。この現状に鑑み、経営層においては情報資産に係る機密性、完全性、可用性の観点からのリスク管理を、自らの経営課題の一つとして捉え直すことが重要である。

経済産業省では、企業における情報セキュリティ対策を、対処療法的なものから、企業価値を高めるための投資対象として位置づけることの重要性を示すため、平成16年度に「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」を開催して、情報セキュリティガバナンスの考え方を示した。そして、平成17年度、平成18年度と、情報セキュリティガバナンス確立実現の促進ツールとして、「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」及び「事業継続計画策定ガイドライン」の活用事業を推進してきた。

情報セキュリティガバナンスの概念について、「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」では、次のように位置づけている。

> 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

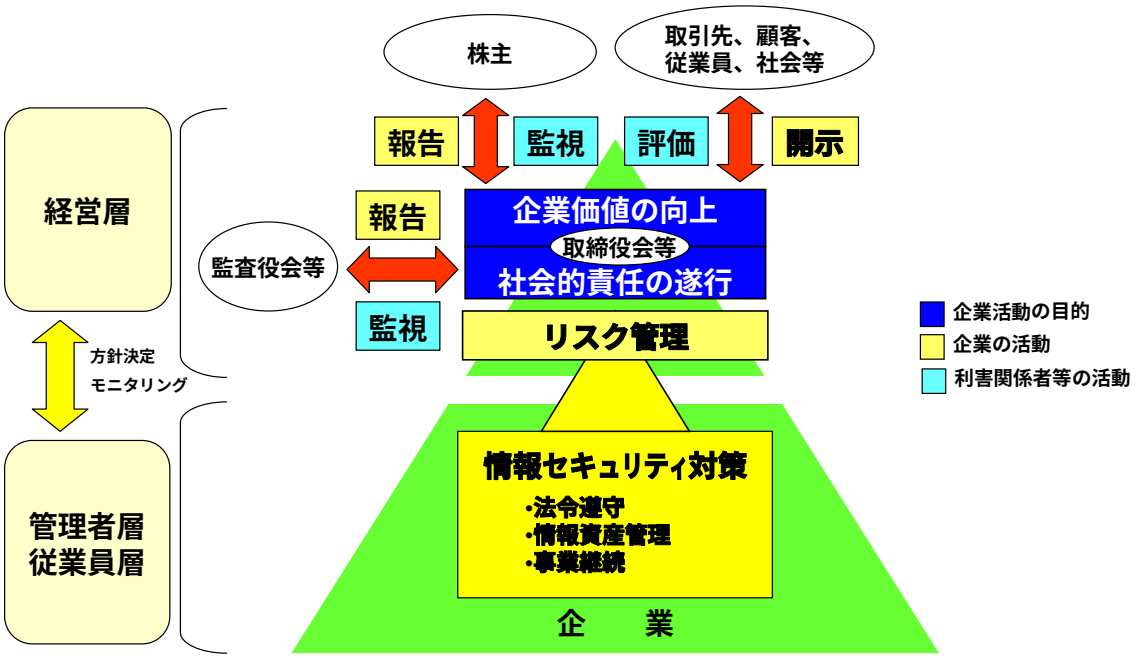
（出典：経済産業省「企業における情報セキュリティガバナンスのあり方に関する研究会」平成17年3月）

当委員会では、第1章の考え方を踏まえた企業戦略に整合的な情報セキュリティガバナンスの普及に資するため、以下のように情報セキュリティガバナンスの概念について一層の明確化を図った。

企業経営の主目標は、株主、顧客、取引先、従業員、社会等の利害関係者に対して責任を果たすこと、つまり、「企業価値の向上」及び「社会的責任の遂行」にあり、これを支える重要な取組の一つにリスク管理が位置づけられる。

様々なリスクの内、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み*を構築・運用することを情報セキュリティガバナンスと位置づける。(*経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組みを指す)

この概念を企業の構造と対比した形で図 3 に示す。



※経営層が取り組む「情報資産に係るリスク管理」を、管理者層・従業員層が取り組む実務的な管理策に詳細化すると、情報資産に係る「法令遵守」、「情報資産管理」、「事業継続」に収斂する構造。
※「監査役会等」、「取締役会等」には、委員会設置会社等の場合を含む。
※「評価」の対象には、顧客からの要望への対応を含む。
※「情報資産管理」には、責任者の設置、情報資産資産の利活用及び漏えい／改ざん防止策等を含む。
※「リスク管理」のリスクには法令違反から生じるリスクを含み、図中の「法令遵守」は管理策を指す。

図 3 企業における情報セキュリティガバナンスの概念イメージ

経営層が自らの経営課題として、情報セキュリティガバナンスの確立を目指すときに考慮すべき情報資産に係るリスクとしては、機密性に係るリスク（法令等で保護が要求される情報や企業価値向上に重要な営業秘密などの情報の漏えいなど）や完全性に係るリスク（法令等で正確性確保が要求される情報を含む情報の改ざんなど）、可用性に係るリスク（IT サービスの事業継続に障害が生じることなど）が考

えられる。経営層は、これらのリスクを管理するために、管理者層・従業員層における対策が着実に実施されるための仕組みを構築し、運用することになる。

その際、経営層は、適法性、適正性、社会的責任、企業戦略等と情報セキュリティとの間のバランスについて合理的に判断すべきである。経営の一環として情報セキュリティガバナンスを捉え、企業及び企業グループにおける一連の統制活動に情報セキュリティガバナンスの確立を組み込むことが、全体最適化への有効な手段である。

ただし、このように情報セキュリティガバナンスを構築しようとした場合に、以下に挙げるいくつかの課題が存在する。

（２） 情報セキュリティガバナンスの確立に向けた課題

①明確な経営層の意志とその徹底の必要性

経営層が情報セキュリティを戦略的なものとして位置づけている事例はまだ多くなく、情報資産に係るリスクの管理を情報システム部門等の現場の判断に任せている企業も少なくないと考えられる。

「情報セキュリティガバナンスシンポジウム 2008[18]」における来場者アンケート（図 4）によると、「情報セキュリティガバナンス確立に係る課題」としては、「社員の意識・理解度」を挙げる回答が最も高く（66.1%）、「効果測定・評価方法」（40.4%）、「経営トップの意思」（38.7%）、「担当部署の体制・権限」（35.1%）といった項目がそれに続く。

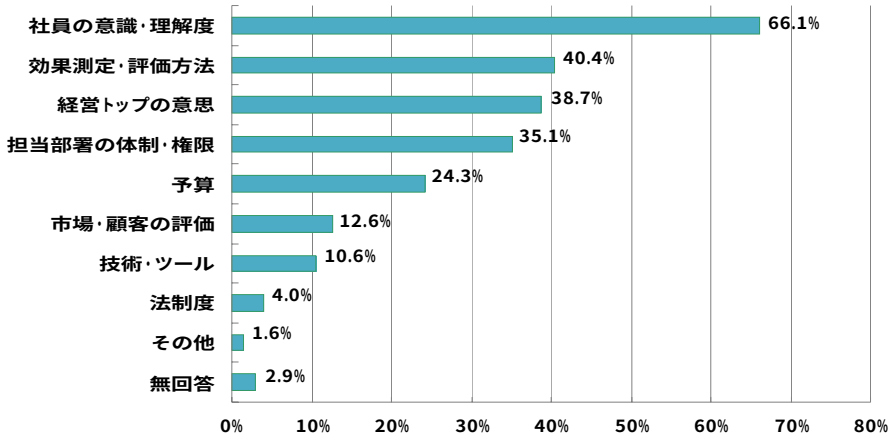


図 4 情報セキュリティガバナンス確立に係る課題（複数回答可）[19]

[18] 主催：経済産業省、日本経済新聞社、2008 年 3 月 5 日開催

[19] 情報セキュリティガバナンスシンポジウム 2008 アンケート結果。回収数 445 件（回収率 52.3%）

この結果から、現場における情報セキュリティ対策の推進が難しいことに加え、経営層が意志決定を行う際に必要な情報セキュリティ対策の効果測定、数値化がうまくできていない、経営層の意志も明確にされていないといった、経営層による情報セキュリティ上の統制の欠如という課題も大きいと考えられる。これは、経営層による企業戦略の一環のリスク管理としての明確な意志と、現場レベル（管理者層・従業員層）で対応する方策との間にギャップが生じていること、及びこのギャップを埋める方法に関する情報が不足していることによるものと考えられる。

また、自然災害、IT 障害等、企業で発生しうるリスク管理の観点から見た事業継続計画の策定率は、海外企業（米国）が約 6 割であるのに対して[20]、我が国の大企業（資本金 10 億円以上）は、約 1 割に満たない状況であり、必ずしも十分とは言えない（図５）。企業において、財務会計システム、生産管理システム、電子メールシステム等の業務の遂行等に必要となる IT の利活用が浸透するにつれ、これら情報システムの中断、停止によって企業の活動全体に影響が生じるリスクが高まっている。情報セキュリティの観点からの事業継続への取組は、現場での対応のみならず、経営層の判断の下での対応が求められている[21]。

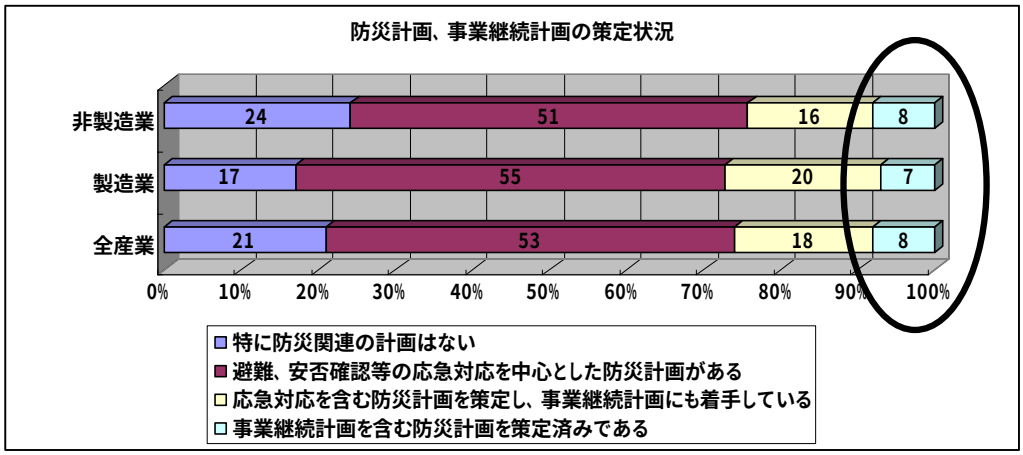


図 5 事業継続計画の策定状況[22]

②安全な情報資産の共有

[20] KPMG Japan「事業継続マネジメント（BCM）サーベイ 2006」
[21] 例えば、国境を越えて組織や職員の心理面のぜい弱性を悪用してコンピュータウイルスを侵入させ、当該コンピュータウイルスにより情報漏えいを招くおそれのある事象の例が散見される。このような事業が発生したときに、情報漏えいの防止のためにネットワークを用いた事業の継続を自ら中断するかどうかの判断が求められる場合が考えられるが、その場合に、法令遵守（個人情報保護法）の観点から個人情報の漏えい防止を優先する場合、自ら開発した技術情報などの一部の漏えいを覚悟しても事業継続を優先する場合など、異なる経営判断をする可能性が考えられる。このような組織面、技術面等が複合した問題が発生する現状がみられる。
[22] 日本政策銀行「企業の防災への取り組みに関する特別調査」平成 19 年 9 月（大企業から 1,530 件の回答を集計）

グローバルな競争が激しさを増す中、各企業は市場の要請に応じて柔軟に企業内外の業務取引の形態を変えていくことが求められるようになっている。その中で、“上手に”情報の利活用を進めようとすると企業内のみならず、企業グループ内での情報資産の適切な管理が必要となる。法人格が異なるため、連結子会社を含めて、企業グループ内での統制が難しいという現状が見られる。

業務アウトソーシング等から進展し、企業の 3 割から 4 割が情報処理関連業務を外部委託する状況[23]にある中で、委託先からの情報漏えい等も発生している。しかしながら、例えば、ソフトウェアのオフショア開発において、開発ベンダの選定基準に情報セキュリティ対策を考慮している割合は、米国企業では約 9 割に上がるのに対して、我が国企業では、約 3 割にとどまっている[24]。また、内閣府の報告によると、2006 年における個人情報の漏えい事案のうち、事業者から直接漏えいしたケースが約 7 割を占める一方、委託先から漏えいしたケースも約 3 割に達する（表 1）[25]。

表 1 個人情報の漏えいに関する漏えい元・漏えいした者

漏えいした者 / 漏えい元	従業者				第三者				その他	不明	合計
	意図的	不注意	不明	計	意図的	不注意	不明	計			
事業者	6 (0.7%)	492 (55.1%)	5 (0.6%)	503 (56.3%)	101 (11.3%)	0 (0.0%)	1 (0.1%)	102 (11.4%)	4 (0.4%)	7 (0.8%)	616 (69.0%)
委託先	37 (4.1%)	164 (18.4%)	1 (0.1%)	202 (22.6%)	50 (5.6%)	3 (0.3%)	2 (0.2%)	55 (6.2%)	5 (0.6%)	4 (0.4%)	266 (29.8%)
不明	－	－	－	－	－	－		－	－	11 (1.2%)	11 (1.2%)
合計	43 (4.8%)	656 (73.5%)	6 (0.7%)	705 (78.9%)	151 (16.9%)	3 (0.3%)	3 (0.3%)	157 (17.6%)	9 (1.0%)	22 (2.4%)	893 (100.0%)

（注）（ ）内は、漏えい事案全体（893 件）に対する割合。

警察庁の調査[26]によると、過去 1 年間にファイル共有ソフトの利用に伴う被害が生じている事案のうち、情報漏えいが生じた際の経路・状況としては、「私物である PC などから漏洩」（60.5%）に続いて、「業務委託先から漏洩」とする割合も 31.6%に達している（図 6）。このように、委託先における情報資産管理は重要な課題となっている。

23 ＩDC「2007 年 国内アウトソーシング市場」
24 JEITA「海外・国内企業におけるソフトウェアのオフショア開発について調査・分析と提言」
25 内閣府「平成１８年度個人情報の保護に関する法律施行状況の概要」平成 19 年 9 月
26 警察庁「不正アクセス行為対策等の実態報告書」平成 19 年 1 月

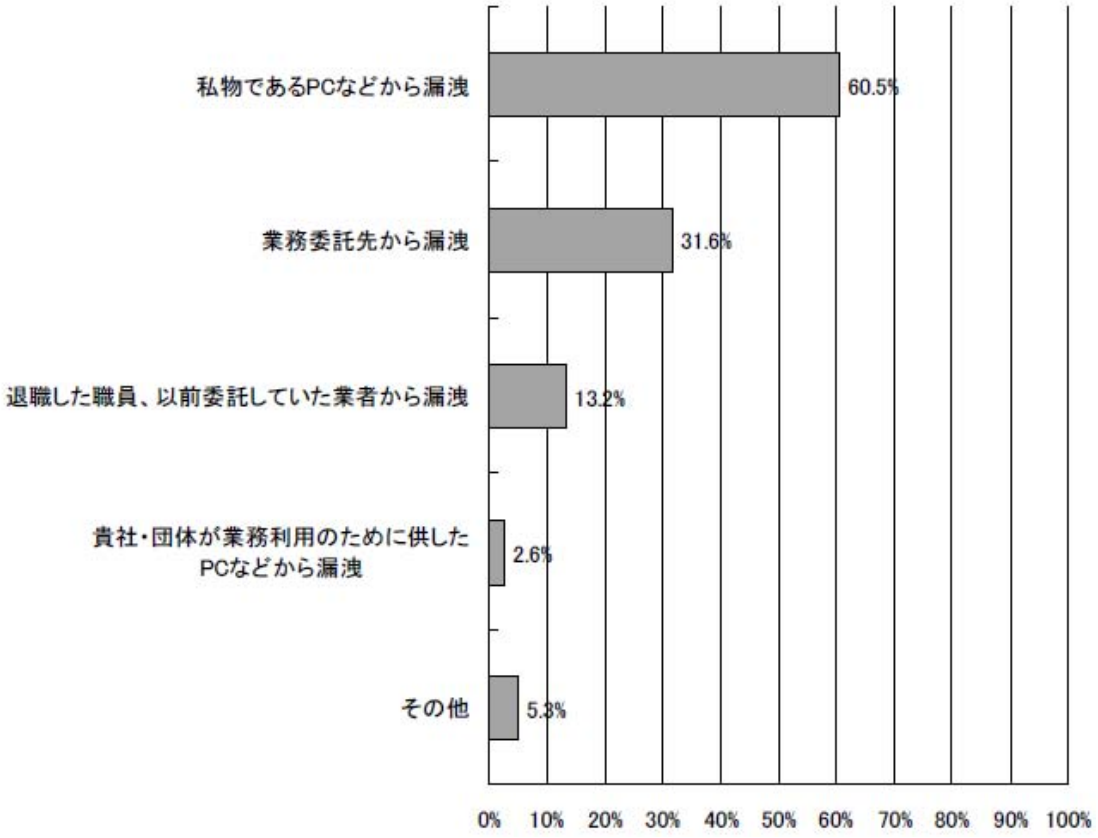
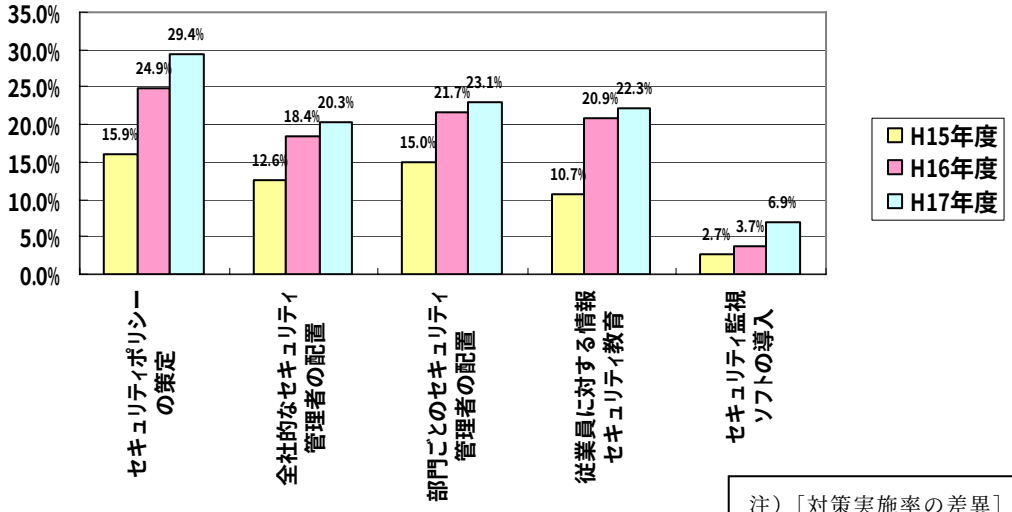


図 6 情報漏えいが生じた際の経路・状況（MA, N=38）

また、大企業と比較して、中小企業においては、人員が少ないというそもそもの構造に起因して、情報セキュリティ管理者の設置や社内情報セキュリティ教育の実施等の情報セキュリティ対策に関する取組に遅れが生じ、大企業との格差が拡大する傾向にある（図 7）。企業グループ内や委託先の取引企業に中小企業が含まれるが、これら中小企業における適切な情報資産管理の推進は今後の重要な課題である。



注）［対策実施率の差異］
＝［大企業における対策実施率］
－［中小企業における対策実施率］

図 7 大企業と中小企業の格差[27]

さらに、情報処理に関わらず、業務外部委託については、国内のみならず、海外へのアウトソース、いわゆるオフショアアウトソーシングも行われている。今後、バリューチェーンの拡大、企業活動のグローバル化が引き続き進展することが予想され、その結果として海外を含めた複数の企業間での情報共有範囲、共有方法が問題になると考えられる。従って、我が国企業のグローバルな活動を支援するため、企業にとって安全なビジネス環境を実現するべく情報セキュリティガバナンスへの取組の必要性と具体的な確立方法を国際的に浸透させていく必要がある。

③異なる目的の法令の遵守の必要性

近年、個人情報保護法や金融商品取引法の施行等に伴い、企業は、法令により要求される情報セキュリティ対策の実施に一層注力するようになってきている。企業では、情報セキュリティ対策は IT 担当部署によって推進されることが多いが、IT 担当部署は、こうした法令を遵守するための担当部署と連携した対応が求められるようになってきている。一方、IT 担当部署が、情報セキュリティ対策を実施していくにあたり、企業の情報資産の保護等とは別の目的の法令との関係も注意する必要がある。例えば、情報セキュリティ対策を従業員が確実に実施することを保証するための措置を推進しようとするときには、労働者の勤労条件について一定の基準を定めた労働基準法等を遵守しなければならないこと[28]に IT 担当部署は気づかなけ

[27] 平成 16、17、18 年情報処理実態調査から作成
[28] 情報セキュリティ事故を発生させた従業員に対する懲戒処分などについては、労働契約法等との関係で効力が判断されると考えられる。

ればならない。適切な方法をとらない場合には、実効ある情報セキュリティ対策を取り得なくなる可能性もある。法令を遵守できていない場合に、企業にとっては大きなリスクとなるものであり、こうした課題を明らかにして欲しいという要請が高まりつつある。

④説明責任への適切な対応

顧客、従業員、社会等の利害関係者が透明性や情報開示を求める声が高まる今日、企業によるリスク等についての情報開示、説明責任が求められている。企業が実施した情報セキュリティ対策について、利害関係者から適性に評価されるためには、利害関係者が求める内容の情報開示が重要である。2007 年度に実施した調査[29]では、国内の上場企業（3,920 社）のうち、CSR 報告書、サステナビリティレポート、環境報告書等に情報セキュリティに係る記載のある企業は、11.8%（463 社）であり、近年上昇傾向にあるものの、依然として高い水準とは言えない（図８）。消費者の 38.9%が情報セキュリティに関する被害をイメージできていない現状等（図９）も踏まえ、今後、情報セキュリティに対する取組状況の開示の促進が重要であると考えられる。

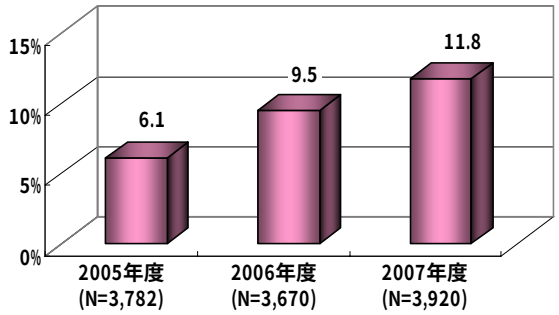


図 8 情報セキュリティに対する取組状況の開示の推移

[29] 経済産業省「情報セキュリティガバナンス研究会報告書」平成 20 年 3 月

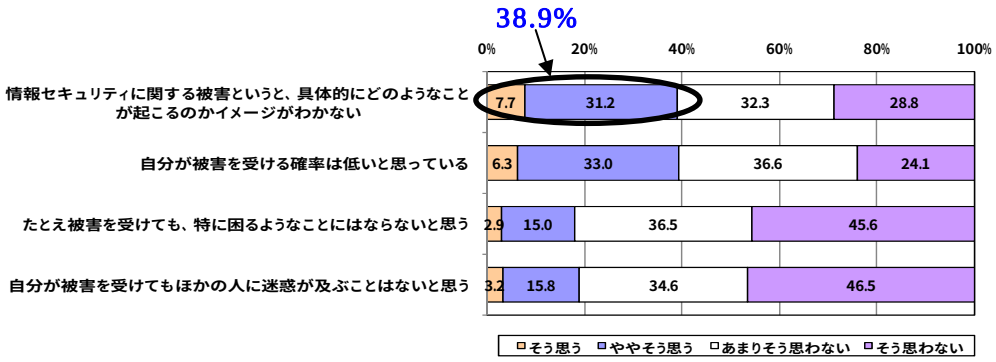


図 9 情報セキュリティに関する被害に対する意識[30]

[30] (独)情報処理推進機構「情報セキュリティに関する脅威に対する意識調査」平成 19 年 12 月

第3章　情報セキュリティガバナンスの確立に向けた今後の取組

（１） 今後の取組の基本方針

今後、企業における情報資産の利活用を支える情報セキュリティに関しては、万全を期していても事故は発生し得るものであるという事故前提型の社会の中で、適正なレベルの取組が実施される社会の実現を目指すべきである。

このため、経営層による企業戦略と整合的な情報セキュリティに係る取組と、高度化が求められている管理者層・従業員層における管理策を有機的に結合して、適正な対策の実施を実現する情報セキュリティガバナンスの確立・促進、中小企業における情報セキュリティ対策の促進及び我が国における取組の成果を国際的に共有し、グローバルに活動する企業にとってセキュアな事業環境整備の促進を目指し、必要な施策を以下に示す。

（２） 明確な経営層の意志とその徹底のための取組

（ア）IT 経営協議会における戦略的な情報セキュリティに係る議論の場の形成

企業価値向上等に資する戦略的な情報セキュリティガバナンス確立の取組を促すため、本年６月に正式に発足した「ＩＴ経営協議会」において、情報資産の利活用とそれを支える適正なリスク管理に係る先進的な取組に関する情報交換、意見交換等を行う。

（イ）情報システム・情報セキュリティに係る内部統制ガイダンス（仮称）の策定

今後、経営層が企業戦略に基づく情報セキュリティ方針や実施計画の策定方法、法令遵守、情報管理、事業継続に係る管理策の構築、各管理策の実施状況を経営層に報告するメカニズムの構築方法[31]、利害関係者への開示・説明方策等を記述した「情報システム・情報セキュリティに係る内部統制ガイダンス」（仮称）の検討を行う。その際、最近の情報セキュリティに係る脅威が技術面、組織面などで複合化している状況に鑑み、情報セキュリティ事象が発生した場合に、管理者層が、経営層に対して事業目的に照らした判断等を求めるときの方法論についても検討する。

（ウ）情報セキュリティガバナンスポータルサイトの整備

「情報セキュリティガバナンス」を切り口として、企業の情報セキュリティに係る各種基準、「SaaS 向け SLA ガイドライン」や「医療情報を受託管理する情報処

[31] 情報セキュリティの効果測定などに関する国際的な検討状況についても適切に対応していき、その成果などの活用も検討。

理事業者向けガイドライン」を含む各種情報セキュリティ関連のガイドライン、事例集等や関連の論文、各種資料、事象事例分析結果、関係公的機関のイベント等の情報提供等を行う総合的な情報セキュリティガバナンスポータルサイトを開設する。その内容は技術や管理策のみならず、経営層や経営企画部門の社員等が経営課題としての情報セキュリティに関する知識を得ることのできるサイトを目指す。また、企業の情報セキュリティに係る情報開示事例や開示情報を集積し、本サイトで提供することなども考えられる。我が国の取組を国際的にも発信できるよう、英語版の整備も検討する。

（エ）情報セキュリティガバナンス事例集の策定

現在調査中の情報セキュリティガバナンス（企業戦略との整合事例、企業グループ内統制の事例等）を先行して実施している企業の取組を踏まえて、事例集を策定・公表する。今後、事例の収集にあたって公募方式の採用を検討する。策定にあたっては、事前準備段階・取組段階、運用段階などの事例、これらの取組に要した期間、可能な場合に事例に関する具体的な問い合わせ先に関する情報等を含むよう努めるものとする。

（オ）IT サービス事業継続向上のための情報提供

2005 年に経済産業省が公表した「事業継続計画策定ガイドライン」と対になるガイダンスとして、IT サービスの可用性等を確保するための具体的なガイダンスを、適切な手順をもって IT ユーザ企業が参照可能な形にとりまとめ、公表する。また、特に国民生活に影響の大きい重要インフラ事業者向け情報システムについて、信頼性向上等の取組事例や事故情報の共有を図るための環境整備が重要であり、事業者の自発的な情報共有ネットワークの形成に対し、専門的・技術的観点から独立行政法人情報処理推進機構ソフトウェア・エンジニアリングセンターが必要な支援を行う。

（カ）情報セキュリティガバナンス確立に向けたインセンティブ

先進的な情報セキュリティガバナンス確立に取り組む企業に対して、情報セキュリティ関連シンポジウム等における講演機会を提供するとともに、情報セキュリティに関する開示状況等をもとにした表彰などを検討する。

（キ）情報セキュリティ、ガバナンス関連の実施主体との連携

「情報セキュリティ管理基準」、「情報システム・情報セキュリティに係る内部統制ガイダンス（仮称）」をはじめ、各種ガイドライン等が、必要な者に必要なときに参照される機会を増やすべく、既存の情報セキュリティやガバナンス、内部統制等に関する実施主体等との連携を強化する。また、顧客、取引先等の利害関係者に

対する情報セキュリティへの取組を示すことにも用いられる ISMS[32]適合性評価制度や情報セキュリティ監査制度等における活用についても検討する。

（３） 安全な情報資産共有に係る取組

（ア）情報セキュリティガバナンス事例集の策定（再掲）

（イ）中小企業が情報セキュリティ対策に取り組む環境の改善

今後、中小企業が保有する情報のセキュリティ対策を推進するために有効となる管理策のチェックリストとして、現在、独立行政法人情報処理推進機構において検討が進められている中小企業向け情報セキュリティ標準フォーマットを作成するとともに、その活用推進策についても検討を行う。また、IT 経営応援隊の活用や、例えば商工会議所等を通じて情報セキュリティの重要性を中小企業に伝える仕組みの構築によって、中小企業による情報セキュリティ対策の促進を図る。

（ウ）海外アウトソーシング時のリスクチェック手法の検討

現在、海外アウトソーシング時のリスクに係る企業の関心事項に関して調査を行っていることから、今後、当該調査結果を踏まえた海外アウトソーシング時のリスクチェック手法について検討を行う。

（エ）アジアにおける情報セキュリティ確保の推進・貢献

アジアなど我が国企業の事業活動で関係の深い国・地域における企業の情報セキュリティレベルを一層醸成させるための活動等、我が国の情報セキュリティ施策の経験を共有するための国際的な議論の場などを通じた取組を実施する。例えば、企業の情報セキュリティレベルの向上に寄与する情報セキュリティ対策ベンチマークの共通化の研究、我が国が世界の認証件数の 50%以上を占める実績を有している ISMS の普及支援などを検討する。

（オ）アジアにおける企業内緊急時対応組織構築支援の協力

取引先において発生した情報セキュリティ上の問題が自社に影響することを考慮すれば、国内外を問わず取引先における緊急対応の仕組みが稼動し、被害を局限化し再発を防ぐ対処がなされることが望まれる。したがって、国内での取組に加えて、アジア諸国に情報セキュリティに係る企業内緊急時対応組織を構築支援する取組を提示し、その協力を進める。

（４） 異なる目的の法令の遵守に係る取組

（ア）情報セキュリティ関連法律上の要求事項の公表

[32] Information Security Management System

我が国企業が、法令を遵守し、着実に情報セキュリティ対策を実施していくためには、情報セキュリティ対策実施部門を含め企業における関係者により情報セキュリティ関連法律上の要求事項に関する理解を深める必要がある。このため、これまでの調査結果をとりまとめた報告書を可及的速やかに公表する。さらに、今後、利用者の利用場面を勘案した形式・記述に編集し、公表に向けて取り組む。公表文書は、継続的に必要な改訂・拡充を図る。

（５） 説明責任への適切な対応を促す取組

（ア）「情報セキュリティ情報開示イニシアティブ（仮）」の実施

戦略的な情報セキュリティ対策による企業価値向上に加え、予め企業の取組やリスクを利害関係者に開示することにより説明責任を果たすなどの取組も促すため、「IT 経営協議会」における情報セキュリティに係る活動の一環として、情報セキュリティ報告書の発行など、情報セキュリティ関連の情報開示推進活動「情報セキュリティ情報開示イニシアティブ（仮）」の実施も検討する。当該活動を通じて、情報セキュリティ報告書の策定・開示を促進する各種啓発活動を行う。

（イ）情報セキュリティガバナンスポータルサイトの整備（再掲）

（ウ）事故前提社会における消費者への情報提供方法の検討

情報セキュリティ対策に万全を期していても情報セキュリティ事故は根絶できないものである。こうした事故前提社会のもとで、企業が提供するウェブサービスなどを消費者が適切に利活用できるようにするためには、消費者自ら IT や自己の情報を適切に管理することが重要であり、そのための方法について分かりやすい情報提供等による啓発活動を推進することが重要である。このため、企業が消費者等に対して情報提供をするときの適切な手法について調査し、推奨事項等をとりまとめる。こうした取組成果は、消費者以外の利害関係者にも分かりやすい情報提供という観点から有益であるため、これらの者に対する啓発活動についても検討する。

（エ）民間における情報セキュリティ格付けの取組の促進

企業の情報セキュリティに対する取組が、顧客、取引先、株主など主要な利害関係者から適切に評価されるためには、各企業の取組が比較可能な形式で提示されることが必要であり、企業の情報開示を進展するような環境醸成に資するものの一つとして、情報セキュリティ格付けが考えられる。民間の組織による情報セキュリティ格付けの信頼性を高めるため、情報セキュリティに関する格付けを実施する機関が満たすべき要件について、適切な手順をもってとりまとめ、情報セキュリティ格付機関が参照可能となるよう公表する。その際、海外の情報セキュリティ格付けに関連する機関との連携などの可能性を踏まえた観点から、必要に応じて、国際標準

化を視野に入れた要件とするよう努める。

（オ）情報セキュリティ、ガバナンス関連の実施主体との連携（再掲）

産業構造審議会 情報セキュリティ基本問題委員会 委員名簿

【委員長】

寺島　実郎	財団法人日本総合研究所会長／株式会社三井物産戦略研究所所長

【委員】（５０音順）

池上　徹彦	独立行政法人産業技術総合研究所特別顧問／宇宙開発委員会委員
和泉　法夫	新潟大学脳研究所統合脳機能研究センター特任教授
今井　秀樹	中央大学教授／ 独立行政法人産業技術総合研究所情報セキュリティ研究センター長
江崎　浩	国立大学法人東京大学大学院教授
大木　栄二郎	工学院大学教授
岡村　久道	弁護士
黒川　博昭	富士通株式会社代表取締役社長
古池　進	松下電器産業株式会社代表取締役副社長
志方　俊之	帝京大学法学部教授
関口　和一	日本経済新聞社産業部編集委員兼論説委員
田島　優子	弁護士
土居　範久	中央大学教授
野原　佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
藤山　知彦	三菱商事株式会社国際戦略研究所所長
細川　泰秀	社団法人日本情報システム・ユーザー協会専務理事
山口　英	奈良先端科学技術大学院大学教授
山下　徹	株式会社ＮＴＴデータ代表取締役社長