

情報セキュリティガバナンス研究会報告書

～ 情報セキュリティによる企業価値創造に向けて ～

平成 19 年 3 月

はじめに

会社法や金融商品取引法等による内部統制の強化、組織再編関連法制の整備、グローバル化・アウトソーシング化の進展、CSR（企業の社会的責任）に対する意識の高まりなど、わが国企業を取り巻く経営環境は急速に変貌しつつある。そのため、企業が抱える事業リスクも多様化・複雑化しており、経営層には多面的な観点から見たリスク管理が求められている。

IT リスクについても、個人情報や営業秘密等の流出、システムダウンによるサービスの停止といった IT 事故のもたらす損失や信用の失墜などの被害が企業経営にも深刻な影響を及ぼすことから、本来は、リスク管理の一環として経営層が正しく理解し、対策の必要性について判断することが望まれる。しかし、実際には、予算や人的資源の制約から十分な予防的対策を適用することが困難なケースや、事故発生時も場当たりの対応のみに終始し、改善が進まないケースが見られる。

こうした問題を踏まえ、経済産業省は、平成 16 年 9 月に商務情報政策局長の私的研究会として「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」を発足し、翌年 3 月にその検討成果を報告書にとりまとめた。同報告書では、情報セキュリティガバナンスを「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」と位置付け、その確立を促す施策ツールとして「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 3 つを提言した。

以降、現在まで、政府調達への適用やイベント、セミナー等の普及啓発活動を通じて、施策ツールの社会への実装に向けた動きは着実に広がりつつあると考えられる。

そこで、そうした動きをさらに加速し、情報セキュリティガバナンスの確立を促すべく、有識者や関係団体等により構成される「情報セキュリティガバナンス研究会」を発足し、社会動向や企業の現状を踏まえ、施策ツールの見直し・改善等に係る検討を行った。本報告書は、関係者のご尽力により得られた検討成果をとりまとめたものである。お忙しい中、研究会やワーキンググループの活動にご協力いただいた関係各位にこの場を借りて感謝したい。

本検討の成果をきっかけとして、施策ツールがこれまで以上に活用され、わが国の社会・経済活動の中に根付くことが期待される。さらに、その結果として、情報セキュリティガバナンスの確立に取り組む企業が正當に評価され、価値向上を果たすようなメカニズムを構築すべく、政府や関係機関が協力して取り組む必要があるだろう。情報セキュリティガバナンスの取組が環境問題のような社会運動として広がることを願ってやまない。

平成 19 年 3 月

情報セキュリティガバナンス研究会座長

土居範久

目 次

1. 背景	1
1.1. 検討の経緯	1
1.2. 平成16年度研究会以降の主な動き	3
1.3. 現状認識	12
2. 施策ツールに関する課題	17
2.1. 情報セキュリティ対策ベンチマークに関する課題	17
2.2. 情報セキュリティ報告書モデルに関する課題	18
2.3. 事業継続計画策定ガイドラインに関する課題	20
3. 情報セキュリティ対策ベンチマークの改訂	22
3.1. 基本方針	22
3.2. 作業方法	23
3.3. 改訂案	23
4. 情報セキュリティ報告書モデルの改訂	26
4.1. 基本方針	26
4.2. 改訂作業の概要	26
4.3. 改訂案	26
5. 施策ツールの普及方策案	28
5.1. 情報セキュリティ対策ベンチマークの普及方策案	28
5.2. 情報セキュリティ報告書モデルの普及方策案	29
別紙1 情報セキュリティ対策ベンチマーク改訂案	
別紙2 情報セキュリティ報告書モデル改訂案	

1. 背景

IT 事故¹による事業中断や重要情報の流出の頻発、個人情報保護法や企業の内部統制強化等コンプライアンスの要請などにより、情報セキュリティの確保は企業経営上も重要な課題になってきている。しかし、必要性を認識していてもどこまで行えばよいか目安がない、真摯に取り組んでもステークホルダーから評価を得られない等、多くの企業では対症的療法的対策に留まっている。

そこで、経済産業省では平成 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、同研究会報告書において企業における情報セキュリティガバナンスの確立を提唱するとともに、確立を促す 3 つの施策ツール（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、事業継続計画策定ガイドライン）を策定した。引き続き経済産業省では平成 17 年度情報セキュリティガバナンスの確立促進事業を実施し、シンポジウム等を通じた普及啓発や情報セキュリティガバナンスの実装に係る課題の抽出を行ってきたところである。また、平成 18 年 2 月に情報セキュリティ政策会議により策定された「第 11 次情報セキュリティ基本計画」においても、情報セキュリティガバナンスの確立促進が求められているなど、情報セキュリティガバナンスの重要性に対する認識も高まってきた。

このような状況の中、情報セキュリティガバナンス及び 3 つの施策ツールは社会への実装に向けた取組が進む一方、策定から 2 年が経過することで、例えば情報セキュリティ対策ベンチマークの JIS Q 27001:2006 への対応など、改善すべき課題も顕在化しつつある。これらの課題解決や高度化等の方策を明らかにするため、平成 18 年度情報セキュリティガバナンスの確立促進事業の一環として「情報セキュリティガバナンス研究会」を設置し、有識者による検討を実施した。

1.1. 検討の経緯

高度にネットワーク化された IT 社会では、企業一社の IT 事故によるトラブルが社会・経済全体にも影響する可能性がある。したがって、企業の情報セキュリティ確保は、自身の被害の局限化や法令遵守に留まらず、IT 社会を構成する一員としての企業の責務といえる。つまり、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、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。

一方、政府の果たすべき役割は、企業の情報セキュリティ対策に対する努力を企業価値として評価するとともに、そうした取組を促す環境の整備を支援することにある。そこで、

¹ ここでは、情報資産に係るリスク（コンピュータウイルス、不正アクセス、災害などの外部要因、従業員及び委託先の過失・犯行、システム障害などの内部要因）に起因する事件や事故を「IT 事故」と位置付ける。情報資産とは、企業にとって価値を有する情報そのもの（企画、製品開発や営業などの情報、顧客情報、知的財産などのデータベース、資料など）と、その情報を可用化する環境（ソフトウェア（アプリケーション、システムソフトウェア、ユーティリティ）、ハードウェア（コンピュータ装置、通信装置、メディアなど）等）を指す。

経済産業省では平成 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、同研究会報告書において企業における情報セキュリティガバナンスの確立を提唱するとともに、それを促す 3 つの施策ツール（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、事業継続計画策定ガイドライン）を策定した。

●情報セキュリティ対策ベンチマーク

- ・ 情報セキュリティ対策の自己診断等に有用なベンチマークの指標を開発
- ・ さらに、IT 事故データ収集のあり方や被害想定額算出手法について調査し、ベンチマークデータと連動したリスク評価の可能性を模索

●情報セキュリティ報告書モデル

- ・ 企業のコンプライアンスや社会的責任を説明する IR の一環として、自らの情報セキュリティポリシーやそれを実現する対策の実施状況について対外的に公表する「情報セキュリティ報告書」を提唱し、そのモデル案を策定

●事業継続計画策定ガイドライン

- ・ 企業が IT 事故発生時にも事業運営を継続的に維持するための事業継続計画（BCP）について、その策定手順や検討項目、事例等を紹介する「事業継続計画策定ガイドライン」を策定

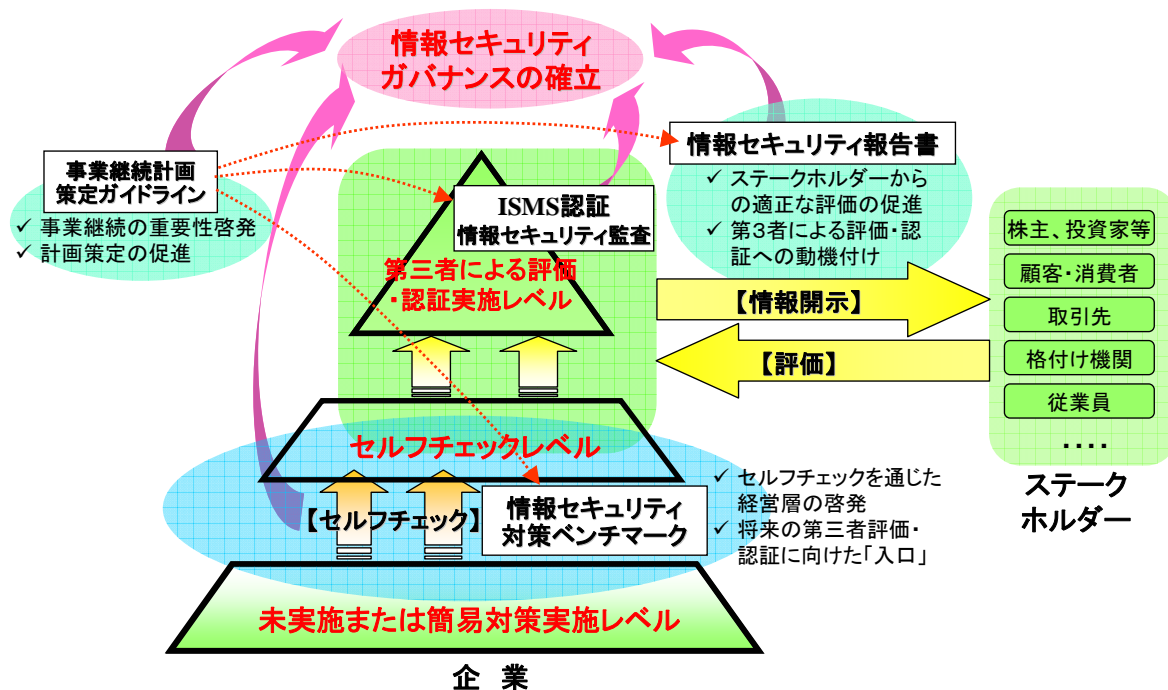


図 1-1 施策ツールと ISMS 等との基本的関係

1. 2. 平成 16 年度研究会以降の主な動き

(1) 政府における取組

情報セキュリティ政策会議では、我が国における情報セキュリティ政策の中期計画である「第 1 次情報セキュリティ基本計画」（2006 年 2 月策定）において、情報セキュリティガバナンスの確立を促進する方針を示し、その具体的施策として政府調達への導入を示唆している。

第 1 次情報セキュリティ基本計画【情報セキュリティ政策会議】（2006 年 2 月 2 日）

第 3 章第 1 節(3) 企業

①企業の情報セキュリティ対策が市場評価に繋がる環境の整備

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・運用することを推進する。このため、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普及・改善を図るとともに、情報システム等の政府調達の競争参加者に対して、必要に応じて、これらの制度や第三者評価の結果等を活用した情報セキュリティ対策レベルの評価を入札条件等の一つとする。

これを受けて、我が国における情報セキュリティ政策の年次計画に相当する「セキュア・ジャパン 2006」（情報セキュリティ政策会議、2006 年 6 月発表）では、外部委託先の候補者における情報セキュリティ対策の水準を確認する目的で、情報セキュリティ対策ベンチマークを政府調達における選定基準の一要素として活用することを明示した。

セキュア・ジャパン 2006 【情報セキュリティ政策会議】（2006 年 6 月 15 日）

第 2 章第 1 節ア① オ) 外部委託先等の情報セキュリティ対策の水準の確保

a) 情報セキュリティマネジメントシステム適合性評価制度等の活用(内閣官房及び全府省庁)
2006 年度に、外部委託先の候補者における情報セキュリティ対策の水準を確認するため、必要に応じて、政府調達における選定基準の一要素として情報セキュリティマネジメントシステム適合性評価制度及び情報セキュリティ対策ベンチマークを活用する。

これらの計画と呼応する形で、情報セキュリティ政策会議の決定文書「政府機関の情報セキュリティ対策のための統一基準」（2005 年 12 月）や、内閣官房情報セキュリティセンター（NISC：National Information Security Center）による外部委託関連の資料においても、外部委託先の評価などへ情報セキュリティ対策ベンチマークを利用することが提案されている。

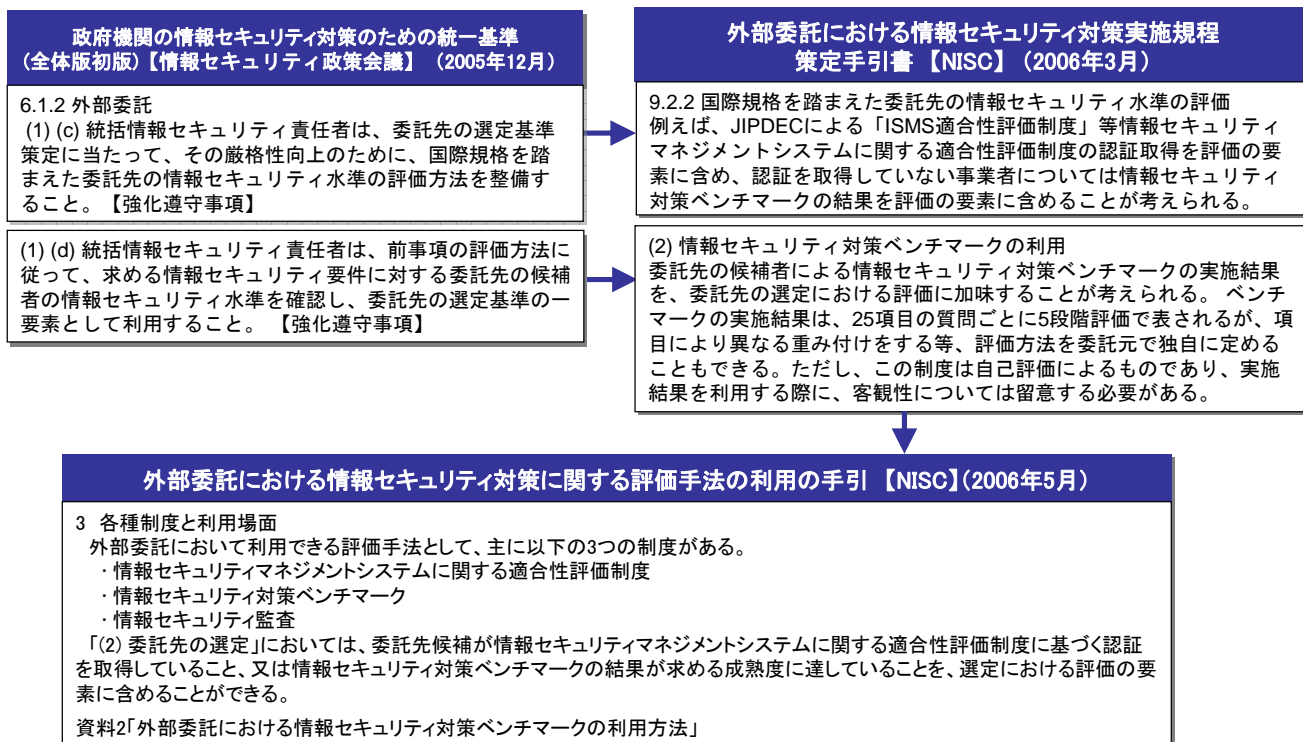


図 1-2 外部委託における情報セキュリティ対策関連の資料

(2) 確立促進事業の実施

情報セキュリティガバナンスの確立を一つの潮流として加速し、企業・社会に普及させていくためには、情報セキュリティガバナンスが環境問題のような「社会運動」として認知されることが重要であり、そのためには、「企業が情報セキュリティについて適切に取り組むことは社会的な責務」という社会意識の醸成が重要である。

ただし、環境問題では、消費者側からの要求が推進力として機能したが、情報セキュリティ問題の場合には、現時点ではそうした動きを期待することは難しい。そこで、例えばベストプラクティスの確保と共有、大手企業への浸透と中小企業への展開といったシナリオを念頭に置きながらそれを促す施策を展開し、政策的アプローチから情報セキュリティガバナンスの「社会運動」化を目指すことが考えられる。

そこで経済産業省は、平成 17 年度以降、情報セキュリティガバナンス確立促進事業を実施し、国の施策として情報セキュリティガバナンスの確立や施策ツールの普及啓発に取り組んでいる。

①情報セキュリティ対策ベンチマーク

a) 自己診断サイトの稼働

独立行政法人情報処理推進機構 (IPA) では、平成 16 年度の研究会報告を受けて情報セキュリティ対策ベンチマークに基づく自己診断サイトを構築し、2005 年 8 月から公開している。2007 年 2 月 25 日時点の利用件数は 7,802 件である。

当初は、中堅・中小企業向けの啓発ツールとしての役割を想定していたが、実際には大手企業等で部門毎に利用するケースや自治体など公的機関が利用するケースも見られた。

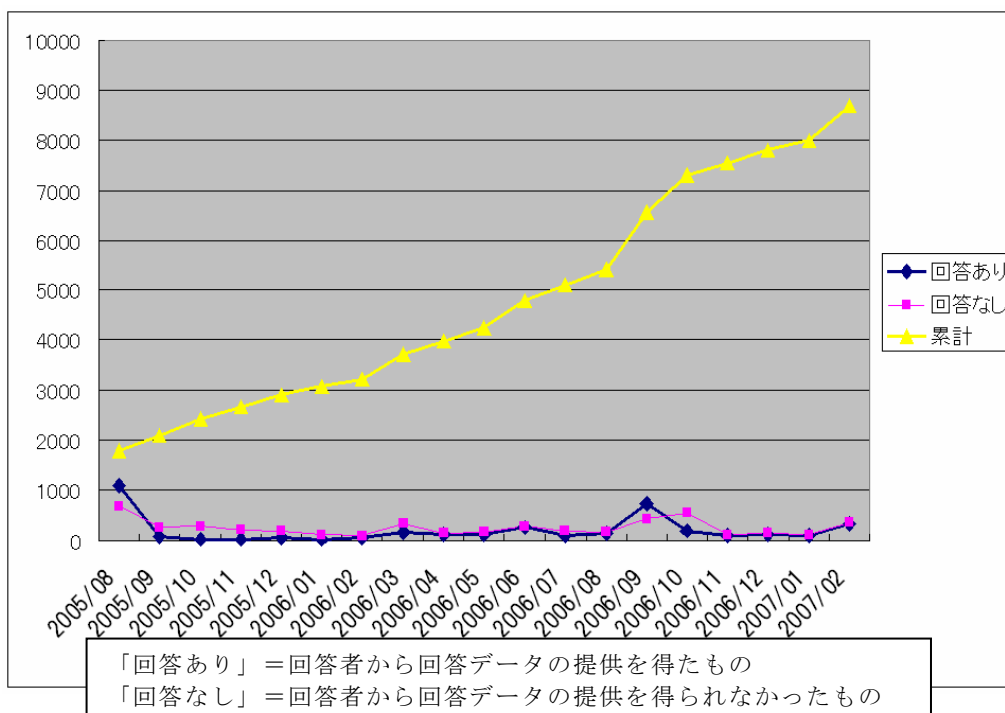


図 1-3 IPA 情報セキュリティ対策ベンチマーク 自己診断サイトの利用状況

(出所:「情報セキュリティ対策ベンチマークセミナー」IPA 講演資料)

b) セミナー

情報セキュリティ対策ベンチマークは、国内の大半を占める中堅・中小企業の利用を想定して策定されたが、中堅・中小企業にツールの存在を伝えるのは容易ではない。そこで、経済産業省では、中堅・中小企業の利用を促進するための方策として、特定非営利活動法人 IT コーディネータ協会、社団法人日本コンピュータシステム販売店協会の協力を得て、中堅・中小企業を顧客としている IT コーディネータやシステム販売事業者向けに、情報セキュリティ対策ベンチマークについての理解・活用を促すセミナーを開催した。

表 1-1 情報セキュリティ対策ベンチマークセミナーの実施状況

開催時期	開催地	受講者数
2006年3月2日	東京	97名
2006年3月7日	大阪	44名
2007年3月5日	東京	81名

2007年に実施したセミナーの受講者アンケートによると、「情報セキュリティ対策ベンチマークを貴社または貴方のお客様向けの情報セキュリティビジネスに活用したいか」という問いに対して「活用している」のは回答者のわずか1%と、まだビジネス利用されていない状況であるが、回答者の65%が「活用してみたい」と回答しており、今後の活用が期待できる。

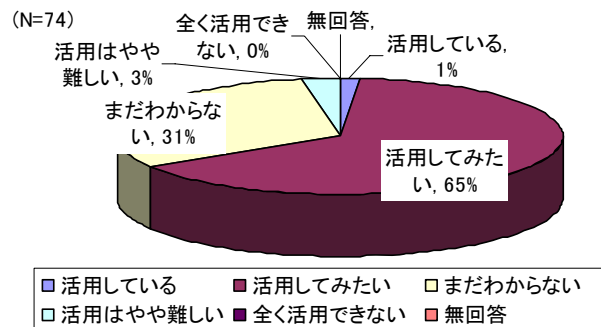


図 1-4 情報セキュリティ対策ベンチマークの活用意向

(出所：2006 年度「情報セキュリティ対策ベンチマークセミナー」受講者アンケート)

②情報セキュリティ報告書モデル

a) 情報セキュリティ報告書の発行事例

情報セキュリティ報告書については、平成 16 年度研究会で提案されたモデルに基づき、2006 年 6 月には富士ゼロックス²が、2006 年 8 月にはリコーグループ³が発行し、注目を集めている。

●事例 1：富士ゼロックス

富士ゼロックスは、情報セキュリティを同社の事業ビジョンである「オープン オフィス フロントティア」実現のための必須要件と位置付け、情報セキュリティガバナンスを通じて、内部統制の目的である業務の効率性・有効性、財務報告の信頼性、コンプライアンス、資産の保全を目指している。

2006 年 6 月に公表した情報セキュリティ報告書によると、同社では、情報セキュリティ戦略の立案・実施に当たり、1) 全社、2) 部門、3) 提供商品のそれぞれの情報セキュリティと、4) 情報セキュリティ機能・商品の提供という 4 つの視点から中期計画を策定している。また、「情報セキュリティ文化の醸成と定着」と「事業継続管理」の 2 つを主要注力テーマとして位置付けている点が特徴的である。

同社では、2005 年 7 月に情報セキュリティ戦略の立案、社内のガバナンス、営業支援の 3 つのミッションを負う情報セキュリティ部が本社に新設され、情報通信システム部(システムセキュリティを担当)や総務部(物理セキュリティを担当)と一体となって情報セキュリティガバナンスを推進する体制をとっている。

また、情報セキュリティを企業倫理活動の一環として位置付け、各種規程類を整備し、2003 年から情報倫理・情報セキュリティ教育を、2004 年には個人情報保護教育を開始、受講を義務付けたほか、ハンドブックやポスター、シールを作成して注意喚起している。

さらに、情報セキュリティ事故防止のための最も有効な手段として情報セキュリティ事故の管理を重視し、どのような軽微な事故でも 2 時間以内に緊急報告をした上で、さらに事態の進展の都度報告することを国内の全社員に義務付けるとともに、事故報告に基づくデータを集計・解析して、問題点や課題を抽出している。

² http://www.fujixerox.co.jp/release/2006/0629_secure.html

³ <http://www.ricoh.co.jp/about/security/report/index.html>

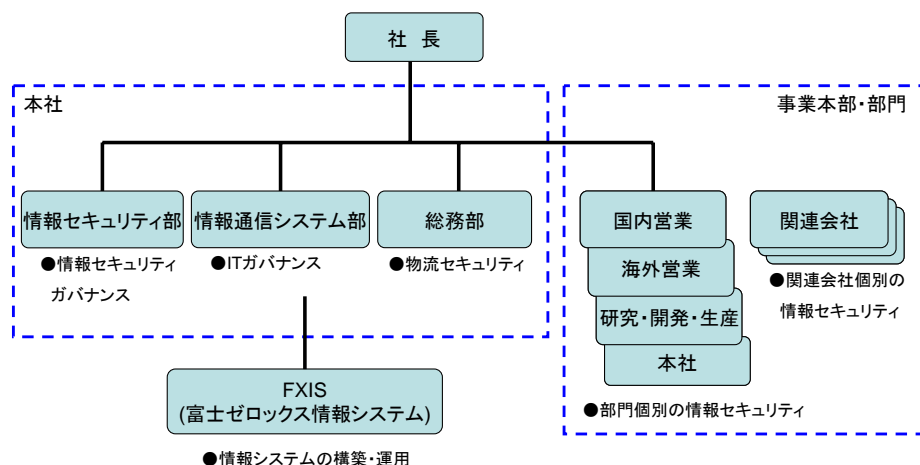


図 1-5 富士ゼロックスの情報セキュリティマネジメント体制（2005年7月1日付）

（出所：富士ゼロックス「情報セキュリティ報告書 2005」）

●事例 2：リコーグループ

リコーグループは、2006年8月、情報セキュリティ報告書を公表した。その中で、同グループは、情報セキュリティを企業の社会的責任と捉え、情報セキュリティの活動を通して、全従業員の行動規範であるリコーグループ CSR 憲章にある「誠実な企業活動」「社会との調和」を実践することを宣言している。

同グループの特徴は、グループ全体で ISMS の整備に取り組んでいる点である。2002年度から ISMS に基づくマネジメントシステムの構築に着手し、2004年12月には国内のグループ 91 社で国内 ISMS 統一認証を取得、さらに 2005年には海外主要生産会社 4 社が認証を取得した。このようにグループ一体となって取り組むことにより、一部の企業の立ち遅れがグループ全体のセキュリティレベルの低下を招く事態を防ぐ効果がある。

同グループの情報セキュリティ管理体制は、チーフ情報セキュリティオフィサー(CISO)を頂点として、グループ ISMS 統括部門を設置し、本社部門・事業本部・カンパニー、国内販売会社、生産関連会社、一般関連会社、海外販売関連会社の情報セキュリティ管理を推進している。

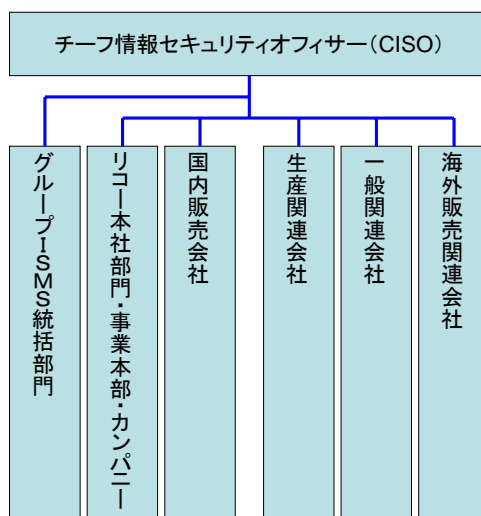


図 1-6 リコーグループの情報セキュリティ管理体制

（出所：リコーグループ「情報セキュリティ報告書 2006」）

今後の取組としては、CSR 本部における「情報セキュリティセンター」の新設、総合的な情報セキュリティガバナンスへの取組の推進、海外販売関連会社における ISMS の構築・認証、事業継続計画・管理の遂行、日本版 SOX 法等の法令順守等が挙げられている。

b) 情報セキュリティに関する開示

国内の上場企業 3,670 社について、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、9.5% (350 社) であった (2006 年 11 月時点)。このうち、326 社 (93.1%) は東証 1 部上場企業である。

また、調査対象社数に占める開示企業の割合を業種別で見ると、「銀行」(62.0%)、「保険」(60.0%)、「電気・ガス」(52.0%) 等の開示率が高い。ただし、銀行・保険業界は、事業法により「業務及び財産の状況に関する説明書類」の作成・公表が義務付けられており、その一環としての情報開示と考えられる。

その他、情報セキュリティに関連して「個人情報保護方針」「プライバシーポリシー」等が Web ページに記載されているのは 2,955 社 (80.5%)、セキュリティポリシーや ISMS 等、情報セキュリティに対する取組指針等に関する記載がされているのは 73 社 (2.0%) であった。

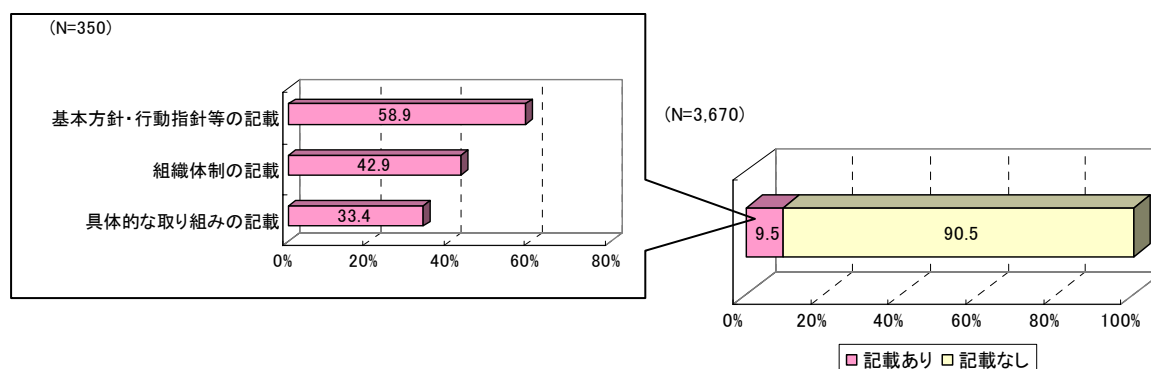


図 1-7 情報セキュリティに係る開示状況

表 1-2 情報セキュリティに係る開示状況 (業種別)

	調査対象	開示社数	開示率		調査対象	開示社数	開示率
情報・通信	141	8	5.7%	食料品	152	15	9.9%
通信	156	5	3.2%	石油・石炭	13	4	30.8%
電機	300	44	14.7%	繊維	87	6	6.9%
サービス	314	6	1.9%	化学	209	27	12.9%
銀行	92	57	62.0%	卸売	380	18	4.7%
保険	10	6	60.0%	ガラス・土石	71	8	11.3%
その他金融	52	9	17.3%	その他製品	110	14	12.7%
電気・ガス	25	13	52.0%	非鉄金属	39	8	20.5%
空運	6	1	16.7%	パルプ・紙	29	1	3.4%
陸運	64	1	1.6%	ゴム製品	21	3	14.3%
建設	223	10	4.5%	海運	18	5	27.8%
医薬品	49	10	20.4%	金属製品	97	4	4.1%
精密機器	48	9	18.8%	鉱業	8	0	0.0%
証券	36	3	8.3%	水産・農林	11	0	0.0%
小売	360	25	6.9%	倉庫	12	0	0.0%
機械	238	13	5.5%	倉庫・運輸関連業	30	0	0.0%
輸送用機器	105	12	11.4%	不動産	108	3	2.8%
鉄鋼	56	2	3.6%	合計	3670	350	9.5%

③事業継続計画策定ガイドライン

a) ガイドラインに関する広報活動

事業継続計画（BCP：Business Continuity Plan）策定ガイドラインは、書籍化とセミナーでの広報活動を実施した。書籍は2005年8月に発刊され、一般書店で販売されている。また、2005年度実施の情報セキュリティ対策ベンチマークセミナー（①参照）でも、その概要を紹介した。

b) BCPを巡る国内の動き

BCPについては、平成16年度研究会で策定された事業継続計画策定ガイドライン以外にも、内閣府中央防災会議が自然災害を想定した総合的なBCPの普及を促す「事業継続ガイドライン第一版」（2006年8月）を、中小企業庁が「中小企業BCP策定運用指針」（2006年2月）を策定するなど、政府の取組が進展している。

また、こうした政府の動きと連動する形で、日本政策投資銀行が企業のBCPに関する取組を評価しその結果に基づき金利を優遇する融資制度を創設⁴、さらに民間の損害保険会社でもその評価結果に応じて企業費用・利益総合保険の保険料割引を行う制度を創設する⁵など、BCPの整備を促進する制度的な動きが出てきた。

さらに、企業・団体の事業継続を推進するための団体として、2006年6月に特定非営利活動法人事業継続推進機構が設立された。

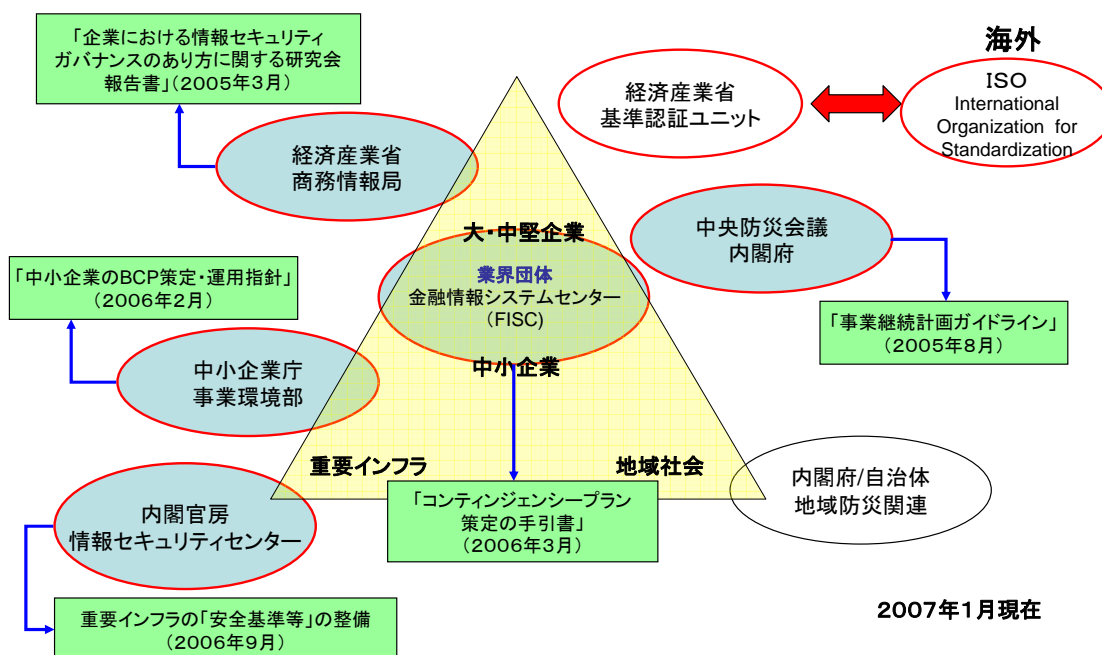


図 1-8 事業継続に係る標準化動向

(出所：渡辺研司「企業経営における事業継続マネジメント～その戦略的重要性～」(講演資料)，2007.01.23)

c) BCPを巡る海外の動き

海外の状況を見ると、テロや自然災害の脅威を背景に国際的にもBCPの重要性が認

⁴ <http://www.dbj.go.jp/japanese/environment/infrastructure/DP-rating.html>

⁵ <http://www.dbj.go.jp/japanese/release/rel2006/1005.html>

識されており、国際標準化機構（ISO : International Standards Organization）において国際標準化の策定に向けた検討が進展している。

英国では、BCI（Business Continuity Institute）と英国規格協会（BSI）が2003年に公開したガイドライン「PAS56」をベースに、2006年6月には産業界のフィードバックを反映した「BS25999」が公開された。また、ITに特化した事業継続マネジメントの規格についても、2006年8月に「PAS77」（IT Service Continuity Management）を公開している。

米国では、米国規格協会（ANSI : American National Standards Institute）と米国防火協会（NFPA : National Fire Protection Association）が制定したNFPA1600が標準化の中心となるフレームワークと位置付けられている。

ISOでは、企業や自治体などの危機管理体制に関する国際規格化を議論する国際会議を2006年4月に開催、米国・カナダ（NFPA1600）、英国（BS25999）、オーストラリア、イスラエル、日本から5カ国からあらかじめ提出されたドラフトを元に議論が進められた。さらにISOが設置したTC223委員会において統合案を策定、2006年11月の委員会総会の審議を経て、ISOの「PAS」として検討することが決定されている。

④イベント

情報セキュリティガバナンスという考え方を一つの潮流としてさらに加速し、企業・社会に普及・定着させていくきっかけとすべく、先進企業の事例や今後の展望等を紹介するイベントとして2005年度には「情報セキュリティガバナンスシンポジウム2005」（2005年12月、於東京）を、翌2006年度には「情報セキュリティガバナンスシンポジウム2007」（2007年2月、於東京）を開催し、2005年度には609名、2006年度には1,049名の来場者を得た。シンポジウムでは、経営課題としての情報セキュリティ対策の捉え方や情報、開示、社内体制・ルールの整備、事故対応や事業継続計画について、先進企業の具体事例が紹介され、企業における情報セキュリティガバナンスのあり方について議論がなされた。

2006年度の来場者アンケートによると、回答の約9割がシンポジウムを通じて「情報セキュリティガバナンスの理解が深まった」としており、同様なイベントが今後開催されれば「ぜひ参加したい」とする回答が48.4%、「興味はある」とする回答が46.4%を占めた。

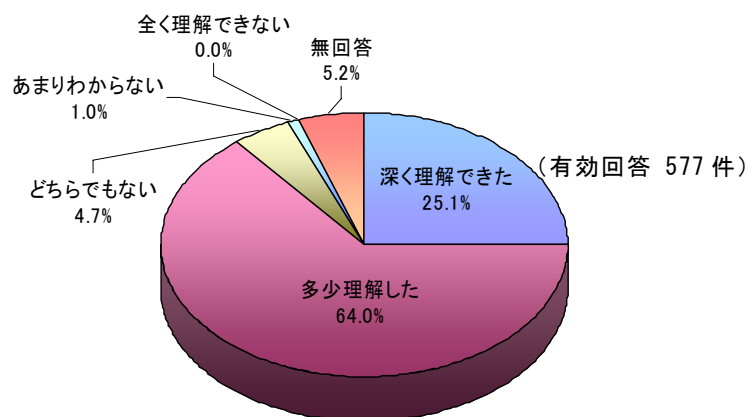


図 1-9 シンポジウム聴講後の情報セキュリティガバナンスに関する理解

(出所：「情報セキュリティガバナンスシンポジウム2007」来場者アンケート)

表 1-3 情報セキュリティガバナンスシンポジウム 2005 の構成

10:00-10:10	開会挨拶 経済産業省 経済産業大臣政務官 小林 温氏
10:10-10:40	基調講演「IT 社会に求められる情報セキュリティガバナンス」 内閣官房情報セキュリティセンター情報セキュリティ補佐官 山口英氏
10:40-11:20	講演「安心・安全なビジネスの創造を目指して」 ヤフー株式会社代表取締役社長 井上雅博氏
11:20-12:00	講演「企業価値創造のための情報セキュリティガバナンス」 一橋大学大学院商学研究科助教授 加賀谷哲之氏
13:30-15:30	先進企業における取組事例紹介 松下電器産業株式会社情報セキュリティ本部参事 長野數利氏 株式会社日立製作所情報・通信グループ CSO 山口光雄氏 富士ゼロックス株式会社情報セキュリティ部部長 関昭男氏 株式会社ジャパネットたかた常務執行役員 CPO 吉田周一氏
15:45-17:15	パネルディスカッション「情報セキュリティガバナンスの確立に向けて」 コーディネータ： 中央大学理工学部教授/慶應義塾大学名誉教授 土居範久氏 パネラー： 株式会社野村総合研究所理事長/ 社団法人日本経済団体連合会 IT ガバナンスに関する WG 座長 村上輝康氏 KPMG ビジネスアシュアランス株式会社常勤顧問 喜入 博氏 経済産業省商務情報政策局情報セキュリティ政策室室長 頓宮裕貴氏 独立行政法人情報処理推進機構セキュリティセンター長 三角育生氏 取組事例をご紹介いただいた先進企業より 山口光雄氏、関昭男氏、吉田周一氏

表 1-4 情報セキュリティガバナンスシンポジウム 2007 の構成

10:00-10:05	開会挨拶 経済産業省 経済産業大臣政務官 高木美智代氏
10:05-11:00	特別講演「日本の経済安全保障と情報セキュリティ」 財団法人日本総合研究所会長 寺島実郎氏
11:00-12:00	基調講演「社会が求める情報セキュリティとガバナンス」 内閣官房情報セキュリティセンター情報セキュリティ補佐官 山口英氏
13:00-14:00	講演「情報セキュリティガバナンスで築くコーポレート・シチズンシップ」 株式会社リコー取締役専務執行役員 遠藤紘一氏
14:05-14:20	講演「情報セキュリティガバナンスの必要性」 経済産業省商務情報政策局情報セキュリティ政策室長 頓宮裕貴氏
14:20-15:20	講演「内部統制確立に向けた情報セキュリティガバナンス」 日本大学商学部教授 堀江正之氏
15:35-17:30	パネル討論「情報セキュリティマネジメントで守る企業価値～ステップアップのヒントを収集する」 富士通株式会社経営執行役法務・知的財産権本部長 加藤幹之氏 川島汽船株式会社取締役常務執行役員 久保島暁氏 味の素株式会社執行役員情報戦略部長 山田裕美氏 株式会社ジャパネットたかた常務執行役員 CSO 吉田周一氏 日本経済新聞社産業部編集委員件論説委員 関口和一氏（コーディネータ）

1.3. 現状認識

(1) 依然として頻発する IT 事故

昨今の IT 事故が招く被害は、当該企業の金銭的損失や信用失墜はもちろん、ステークホルダーである株主や取引先、エンドユーザにまで影響が及ぶ、深刻かつ大規模なものとなりうる。特に、トラブルの事例を通じて、以下の点がさらに明確になったと考えられる。

- ・ 「Winny」などの情報共有ソフトを悪用したコンピュータウイルスによるトラブルが頻発しており、個人情報だけでなく原子力発電所の技術情報や空港施設の暗証番号といった機密情報まで流出していること
- ・ 外部委託先など、実質上統制が困難な領域から情報流出が多く発生していること
- ・ 事故のタイプによっては社会・経済全体に大きな影響を及ぼしうること

表 1-5 最近の IT 事故の事例

当事者企業	IT 事故の概要
印刷 A 社	A 社は、2007 年 2 月、預かっていた個人情報や業務委託先の元社員によって不正に持ち出されたことを公表した。持ち出された個人情報は 863 万件以上、その一部はネット経由で売買され、ネット通販詐欺に悪用されるなどの被害も発生した。
自動車 B 社	2006 年 12 月、最大約 538 万人分の顧客情報が社外に流出した可能性があると発表。社内調査では流出の事実や経路は特定できなかったが、流出したとされる情報の内容から「社内から流出した可能性を否定できない」と判断し、発表した。
証券 C 社	2006 年 11 月、C 社の Web サイトにおいて、外部からの不正アクセスが確認された。犯人は自作のプログラムで同社の顧客 ID26 人分を盗み出し、不正ログインを行ったとされる。
通信 D 社	2006 年 6 月、インターネット接続サービスの顧客情報を提示し、金銭を要求した 2 名が恐喝未遂容疑で逮捕・起訴された。流出した顧客情報は約 400 万件。D 社の委託先社員が 2003 年 12 月に当該データを持ち出したとされる。
証券 E 社	2005 年 12 月、誤って発行済み株式数を上回る売り注文を出し、407 億円もの損失を計上。E 社は証券取引所のシステムの問題で取消処理が遅れ損失が膨らんだとしており、約 400 億円の損失負担を求めている。
電力 F 社	2005 年 12 月、原子力発電所の耐震関係の技術資料などが流出したことを発表。業務情報を保存していた F 社社員の個人 PC がウイルスに感染し、Winny 経由で流出したとされる。流出時期は不明。
証券取引所 G 社	2005 年 11 月、株式売買システムのダウンにより全銘柄の取引停止という前代未聞の事態に陥った。システム更新時の作業指示に漏れがあったことが原因とされる。
EC サイト運営 H 社	2005 年 5 月、価格比較サイトが不正アクセスを受け、エンドユーザのメールアドレス約 22,500 件が流出、約 10 日間のサービス停止に追い込まれた。サイトを閲覧するとウイルスを感染させる改ざんがなされていたとされる。

(出所：各種報道を基に事務局作成)

(2) 技術流出の脅威

2006 年 12 月に公表された経済産業省「我が国製造業における技術流出問題に関する実態調査」によると、国内外に技術流出が発生したとする企業は 35%以上に達し、そのうち「技術データ（ワザ）を通じた流出（図面・製造データの流出等）」があったとする企業は 52.8%に達した。

調査時期：平成 18 年 8 月～10 月
 対象企業：製造業関係企業 625 社に
 アンケートを依頼。
 ・回収企業数 357 件
 ・回収率 57.1%

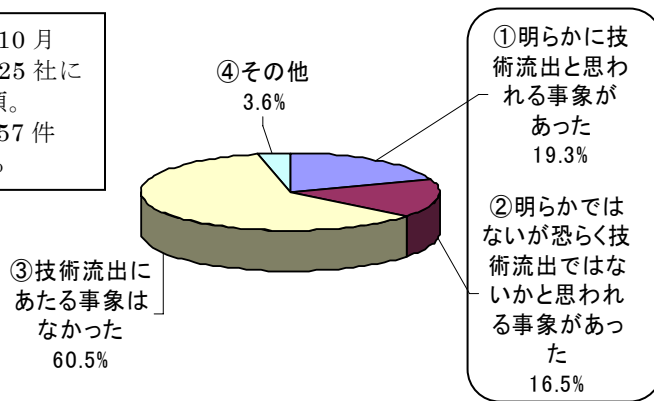


図 1-10 技術流出の実態

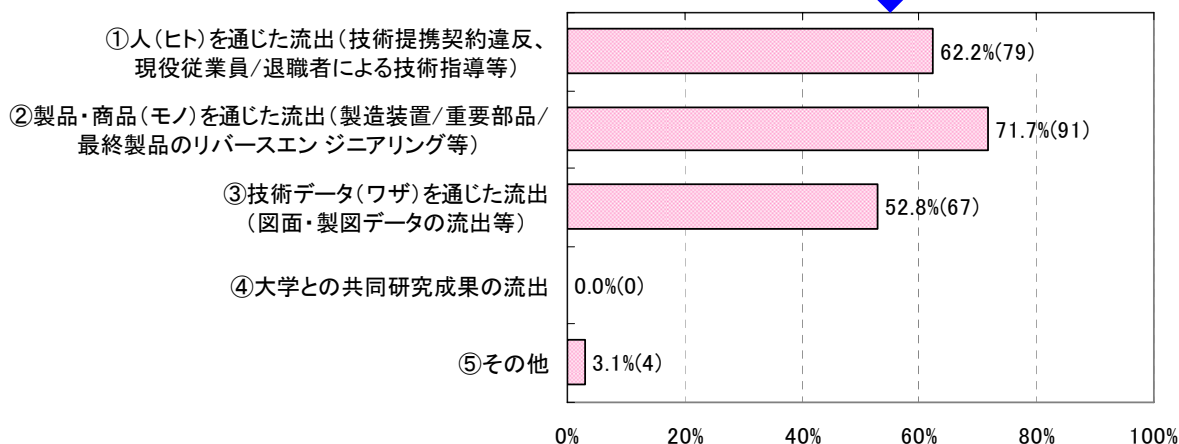


図 1-11 技術流出のパターン

(出所：図 1-10、図 1-11 とも経済産業省「我が国製造業における技術流出問題に関する実態調査」2006.12)

個別には、大手精密機器メーカーの研究者が同社の光通信に関する機密部品を盗み出し、ロシアの通商代表部員に渡した疑いで書類送検された事件(2006年8月)、大手自動車部品メーカーの社員が社内データベースから設計図等機密性の高いものを含む約13万件のデータをノートパソコンにダウンロードし無断で持ち出した疑いで逮捕された事件(2007年3月)などの事例も報道されている。

特に製造業において、重要技術に係る機密情報は生命線であり、その流出は競争力と付加価値の喪失を招きかねない。さらに、軍事転用の可能性から輸出規制品目に指定されている製品の場合には、その影響は国際的な平和及び安全の維持上の深刻な問題にまで及ぶことになる。

なお、不正競争防止法では、このような技術情報や法人顧客の名簿など、個人情報保護法の対象外である営業秘密を保護する法制度として改正されたが、その保護対象として認められるためには安全管理措置の適用が不可欠とされる。

(3) 内部統制強化を求める要求

相次ぐ不正会計や不祥事を背景に、企業に対し内部統制環境の整備を求める要求が急速

に高まっている。

2005年6月29日に成立し、2006年5月1日に施行された会社法⁶では、大会社⁷について「内部統制システムの構築」が義務付けられた点で大きな注目を集めている。会社法第362条4項6号を具体化した法務省令「会社法施行規則」(2006年2月7日公布)第100条1項では、「取締役の職務執行に係る情報の保存及び管理に関する体制」、「損失の危険の管理に関する規程その他の体制」、「取締役の職務の執行が効率的に行われることを確保するための体制」、「使用人の職務の執行が法令及び定款に適合することを確保するための体制」、「当該株式会社並びにその親会社及び子会社から成る企業集団における業務の適正を確保するための体制」の整備が求められており、そうした観点から情報セキュリティの確立に取り組む必要が生じるものと考えられる。

また、2006年6月7日に成立した金融商品取引法、いわゆる「日本版SOX法」では、上場企業の経営者が内部統制の状況を確認・評価し内部統制報告書を作成すること、公認会計士が内部統制の適正性をチェックし「内部統制監査報告書」を作成することが義務付けられており、2008年4月1日以後に開始する事業年度からの適用が予定されている。

企業に求められる内部統制の指針については、金融庁の企業会計審議会内部統制部会が「財務報告に係る内部統制の評価及び監査の基準のあり方について」⁸(2005年12月8日)において、内部統制の構成要素を「統制環境」「リスクの評価と対応」「統制活動」「情報と伝達」「モニタリング」「ITへの対応」と位置付けている。このうち「ITへの対応」は、国際的な内部統制議論のベースになっている米トレッドウェイ委員会支援組織委員会(COSO: The Committee of Sponsoring Organization of the Treadway Commission)の「内部統制の基本的枠組みに関する報告書」には記載のない項目であるが、多くの組織がIT抜きでは業務を遂行することができなくなっている現状を考慮し付加されたものである。さらに、同部会では、2007年2月15日に「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について(意見書)」⁹(以下、実施基準)を公開し、より詳細な実務上の指針を示した。実施基準では、ITに対する統制活動を「全般統制」と「業務処理統制」と位置付け、その具体例を示している。

⁶ 商法第2編、有限会社法、株式会社の監査等に関する商法の特例に関する法律等の各規定を再編成し、新たな法典として創設された。

⁷ 資本金5億円以上、負債額200億円以上の会社(会社法第2条6項)。

⁸ <http://www.fsa.go.jp/news/newsj/17/singi/f-20051208-2.html>

⁹ http://www.fsa.go.jp/singi/singi_kigyousin/20070215.html

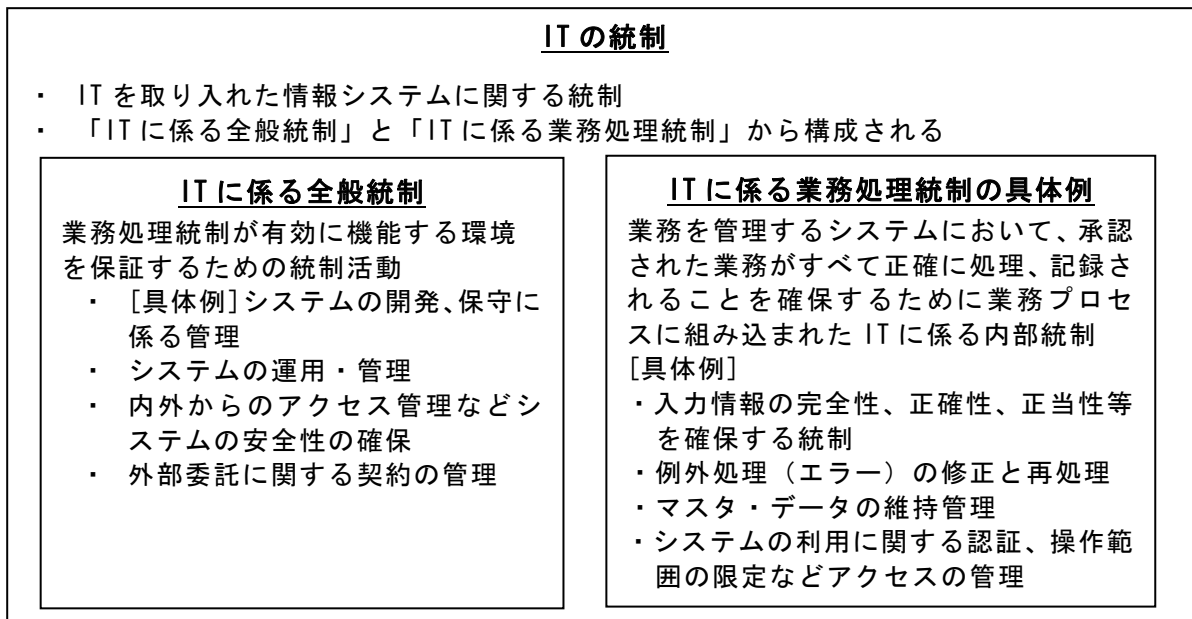


図 1-12 ITの統制のイメージ

（出所：金融庁企業会計審議会内部統制部会「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について（意見書）」（2007.02.15）をもとに事務局作成）

なお、経済産業省では、2007年3月30日、財務報告に係る内部統制を念頭に、主要なケースを想定しつつ、IT統制に関する概念、経営者評価、導入等について例示した「システム管理基準 追補版（財務報告に係るIT統制ガイダンス）」¹⁰を公開している。

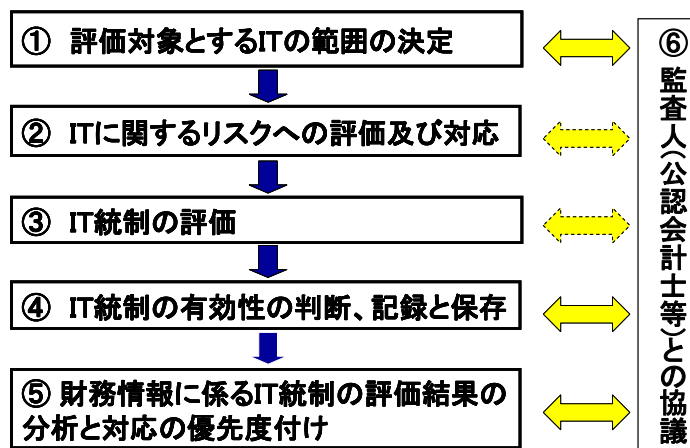


図 1-13 IT統制の評価のロードマップ

（出所：原田要之助「内部統制確立のための情報セキュリティ/経済省システム管理基準追補版について」（講演資料），2007.03.05）

(4) 米国の動向

米 IT Governance Institute は、2006年3月、「Information Security Governance - Guidance for Boards of Directors and Executive Management 2nd Edition」¹¹を公表している。このレポートは、発行元こそ異なるが、米 National Cyber Security Partnership

¹⁰ <http://www.meti.go.jp/press/20070330002/20070330002.html>

¹¹ <http://www.itgi.org/ContentManagement/ContentDisplay.cfm?ContentID=24384>

(NCSP)¹²の Corporate Governance Task Force が 2004 年 4 月に発表した「Information Security Governance: A CALL TO ACTION」¹³の”2nd Edition”として位置付けられている。

“2nd Edition”では、情報セキュリティガバナンスの定義を、「企業のガバナンスの部分集合で、それは戦略的方向性を示し、目的が達成するのを保障し、リスクを適切に管理し、責任を持って組織的資源を使用し、企業のセキュリティプログラムの成功または失敗をモニタするもの」としている。また、情報セキュリティガバナンスのフレームワークの構成要素として、以下の項目が挙げられている。

- ・ 情報セキュリティリスクマネジメント手法
- ・ ビジネスと IT の目的に関連した包括的なセキュリティ戦略
- ・ 効果的なセキュリティ組織的構造
- ・ 保護する情報の価値に関して言及したセキュリティ戦略の伝授
- ・ 戦略の個々の側面に関するセキュリティポリシー、コントロールと規制
- ・ 手続きとガイドラインがポリシーに合致するように個々のポリシーのセキュリティ基準のセット
- ・ コンプライアンスの確保とリスク低減のフィードバックをもたらす組織的なモニタリングプロセス
- ・ セキュリティポリシー、基準、手続き、リスクの継続的な評価と更新を保障するプロセス

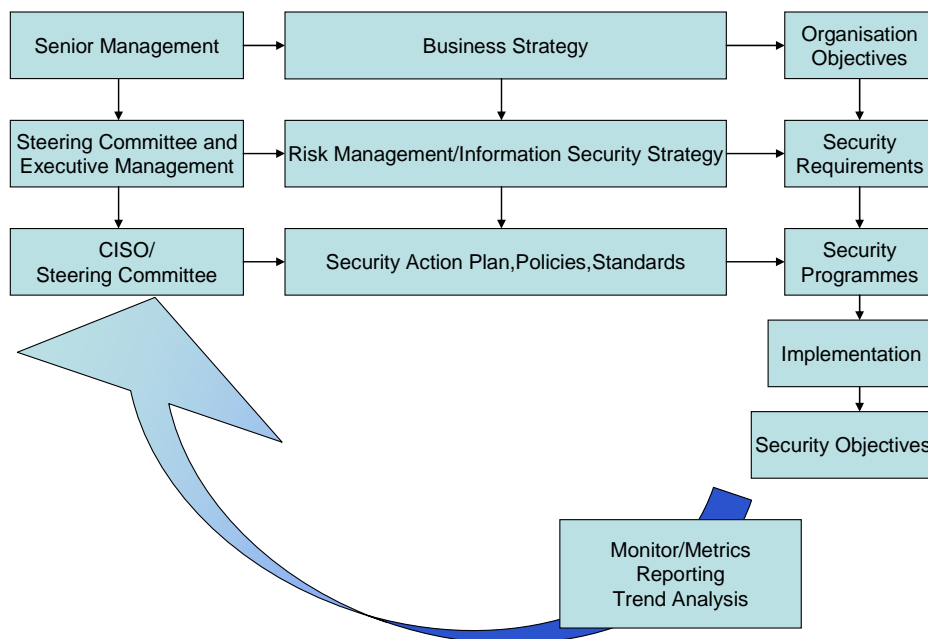


図 1-14 情報セキュリティガバナンスの概念

(出所：IT Governance Institute:” Information Security Governance – Guidance for Boards of Directors and Executive Management 2nd Edition” ,2006.03)

¹² <http://www.cyberpartnership.org/>

¹³ http://www.cyberpartnership.org/InfoSecGov4_04.pdf

2. 施策ツールに関する課題

情報セキュリティガバナンス及び3つの施策ツール（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、事業継続計画策定ガイドライン）は社会への実装に向けた取組が進む一方、策定から2年が経過することでいくつかの課題も顕在化してきた。そこで、本章ではそうした課題を踏まえ、各施策ツールの見直しの必要性について検討する。

2.1. 情報セキュリティ対策ベンチマークに関する課題

(1) JIS Q 27001:2006 との整合

情報セキュリティ対策ベンチマークは、ISMS 適合性評価制度¹⁴や情報セキュリティ監査との整合に配慮し、その評価項目を ISMS 認証基準（Ver.2.0）の詳細管理策¹⁵をベースに構成している。

ISMS の源流である英国規格 BS7799 は、BS7799-1（規範）と BS7799-2（仕様）に分かれる。このうち、BS7799-1 は、ISO/IEC17799:2000 として国際標準化されたが、その後、各国の ISMS 基準や関連規格を総合的に組み立て直す形で検討が進められ、2005 年に ISO/IEC 17799:2005 へ移行、さらに 2007 年には ISO/IEC 27002:2007 に番号変更される予定である（国内規格は先行して 2006 年に JIS X 5080:2002 から JIS Q 27002:2006 に移行）。ISO/IEC 17799:2005 は、ISO/IEC 17799:2000 に比べ、分類が 10 から 11 に、管理目的が 36 項目から 39 項目に、管理策が 127 項目から 133 項目に変更された（表 2-1 参照）。

一方、BS7799-2 は、ISMS 認証基準のベースとなった規格で、2005 年に ISO/IEC 27001:2005 として国際標準化され、2006 年には JIS Q 27001:2006 として JIS 規格化された。これに伴い、ISMS 認証基準も JIS Q 27001:2006 に移行され、管理目的及び管理策も JIS Q 27001:2006 の付属書 A（JIS Q 27002:2006 の管理策を参照している）に合わせることになる。

従って、情報セキュリティ対策ベンチマークの項目もこれらの変更に応じて、項目構成や内容を適切に見直す必要があると考えられる。

¹⁴ 財団法人日本情報処理開発協会（JIPDEC）が運営する、情報セキュリティ対策に関する国内での第三者評価制度（<http://www.isms.jipdec.jp/>）。2006 年 7 月からは財団法人日本適合性認定協会（JAB）でも、審査登録機関の認定申請の受付を開始している。

¹⁵ ISMS 評価基準の付属書であり、JIS X 5080:2002（国際標準 ISO/IEC 17799:2000）を参照して ISMS 構築に必要なセキュリティ対策を定義している。ISMS 評価基準では、詳細管理策から適切な管理目的及び管理策を選択することを求めている。

表 2-1 JIS X 5080:2002 と JIS Q 27002:2006 の構成

JIS X 5080:2002(ISO/IEC 17799:2000)			JIS Q 27002:2006(ISO/IEC 17799:2005)		
分類	管理目的	管理策	分類	管理目的	管理策
3. セキュリティ基本方針	1	2	5.セキュリティ基本方針	1	2
4. 組織のセキュリティ	3	10	6.情報セキュリティのための組織	2	11
5. 資産の分類及び管理	2	3	7.資産の管理	2	5
6. 人的セキュリティ	3	10	8.人的資源のセキュリティ	3	9
7. 物理的及び環境的セキュリティ	3	13	9.物理的及び環境的セキュリティ	2	13
8. 通信及び運用の管理	7	24	10.通信及び運用管理	10	32
9. アクセス制御	8	31	11.アクセス制御	7	25
10. システムの開発及び保守	5	18	12.情報システムの取得、開発及び保守	6	16
			13.情報セキュリティインシデントの管理	2	5
11. 事業継続管理	1	5	14.事業継続管理	1	5
12. 適合性	3	11	15.順守	3	10
計 10	計 36	計 127	計 11	計 39	計 133

(出所：JIS X 5080:2002 及び JIS Q 27002:2006 をもとに事務局作成)

(2) 多様な利用ニーズへの対応

前章で示したとおり、情報セキュリティ対策ベンチマークには、大企業等における部門単位の利用や公的機関の利用など、多様な需要があることが明らかになった。しかし、現在の評価項目は主に中堅・中小企業を想定して構成したため、表現や枠組みが部門単位の利用や公的機関の利用に適していない。

さらに、当初、リピーターが繰り返し使用し、レベルアップを目指すという利用形態を想定していたが、改善の度合い（全体の中での位置の変化）が見えにくいため、繰り返し利用する動機付けに乏しいという問題についても検討が望まれている。

2.2. 情報セキュリティ報告書モデルに関する課題

(1) 情報セキュリティ報告書発行の促進

企業がステークホルダーに対し自社の情報セキュリティの取組を開示することは、その取組について経営者がステークホルダーに「約束」する意味があり、企業の情報セキュリティレベルの向上を促すトップダウンアプローチとして有効である。したがって、企業の情報セキュリティに関する開示を促すことは効果的な政策といえる。

もちろん、ステークホルダーに説明する手段は情報セキュリティ報告書に限らない。例えば、会社全体のメッセージを総括した CSR 報告書の中に、情報セキュリティに関する情報が掲載されることは非常に重要である。たとえば、CSR 報告書を通じて、個人情報保

護や内部統制等のコンプライアンス（法令遵守）の流れで情報セキュリティの取組について説明するケースが多い。

ただし、CSR 報告書への掲載だけでは十分な情報開示とは言えない。使用できるスペースは限定的であり、そのメッセージも CSR が前提となるため、本来発すべき情報を適切に伝えきれない可能性が高いためである。

実際に情報セキュリティ報告書を発行した事業者における発行の動機や効果から、

- ・ 営業秘密に係る情報管理や事業継続性といった観点からの取引先への説明責任
- ・ 従業員やグループ会社・外部委託先に対する意思統一・意識啓発
- ・ お客様に対するマーケティング効果やブランドイメージの向上

といった効果を意図して情報開示を行うのであれば、情報セキュリティ報告書の発行が有効と考えられる。

表 2-2 情報セキュリティ報告書発行の動機と効果

発行の動機	<ul style="list-style-type: none"> ・ 会社としての情報セキュリティ活動の見える化（内外認知度の向上、言行一致、担当者の求心力向上） ・ 取引先や顧客に、自社の取組について説明するための資料の作成 ・ 従業員に情報セキュリティに取り組む理由を理解してもらうツールの確保
発行の効果	<ul style="list-style-type: none"> ・ CSR の一環としての、情報セキュリティガバナンスに関する説明責任の実現 ・ 営業活動への活用 ・ 社内の情報セキュリティ活動の活性化 ・ コーポレートガバナンス強化への寄与

（出所：発行者のコメントをもとに事務局作成）

また、「情報セキュリティガバナンスシンポジウム 2007」来場者アンケートによると、回答企業（もしくは取引先企業）の情報セキュリティガバナンス確立に係る課題として「社員の意識・理解度」が挙げられているが、情報セキュリティ報告書はこの課題を解決するツールとしても有効であることにも留意すべきであろう。

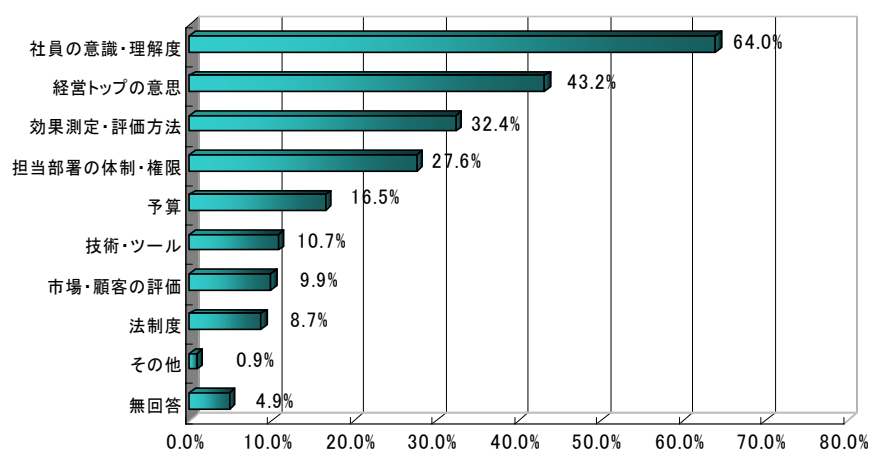


図 2-1 情報セキュリティガバナンス確立のための課題

（出所：「情報セキュリティガバナンスシンポジウム 2007」来場者アンケート）

つまり今後は、情報セキュリティに関する開示をより多くの企業に推奨すると同時に、情報開示の目的が合致する企業に対して情報セキュリティ報告書の発行を促すことが必要である。その場合、情報セキュリティ報告書が多数発行されジャンルが確立されることで、情報セキュリティに関する開示の一般化を促すことが可能と考えられる。

そこで、さらに多くの企業の情報開示を促すため、情報セキュリティ報告書の発行者の知見を踏まえ、導出が難しい項目の内容を改善するなど、情報セキュリティ報告書モデルの項目構成等を見直すこととする。

(2) 競争原理の導入

情報セキュリティ対策の推進や積極的な情報開示を促す方策として、格付けやランキングといった競争原理を導入することを念頭に、複数の情報セキュリティ報告書を比較評価できるような項目を適用することも考えられる。ただし、報告書は自己宣言型の開示情報であることから、想定すべき競争モデルは認証等が伴う公的な評価制度ではなく、民間機関が企業を対象に独自に実施する格付けやランキングと考えられる。

表 2-3 格付け、ランキングの例

格付け、ランキングの例	概要
防災格付融資「防災対策促進事業」 ¹⁶ (日本政策投資銀行)	企業の防災に対する取組を評価し、融資金利から最大 0.6% を割引く。
「2006 年版世界企業ランキング」 ¹⁷ (NewsWeek)	CSR を評価軸として、世界 500 社についてランキングを実施。
「CSR 総合ランキング 2005」 ¹⁸ (日経ビジネス)	東証 1、2 部上場企業が CSR を果たすための意思や能力、体制を総合的に評価。
「2006 年度優良企業ランキング」 ¹⁹ (日本経済新聞社)	NEEDS-CASMA (日経が開発した企業評価システム) を使って上場企業を総合的に評価。
「環境格付」 ²⁰ (トーマツ審査評価機構)	環境報告書やホームページによる公開情報等を基に環境格付けを実施。

(出所：各種資料より事務局作成)

2.3. 事業継続計画策定ガイドラインに関する課題

BCP を取り巻く環境は、2 年間で大きく変化している。従って、経済産業省のガイドラインも、新たなニーズへの対応や他のガイドライン等の整合を図ることは意味があると考えられる。

しかし、ISO/IEC では国際標準化の検討が始まっているが、現在は各国の提案をもとに統合案を策定している段階であり、その作業は 2009 年頃までかかる見込みであることから、ガイドラインの改訂にそうした国際標準との整合をとるのは困難なタイミングである。したがって、こうした国内外の動向を踏まえ、本年度は BCP 策定ガイドラインについての見直しを見送るが、引き続き注意深く国際標準化に係る動きを迫りかけるものとする。

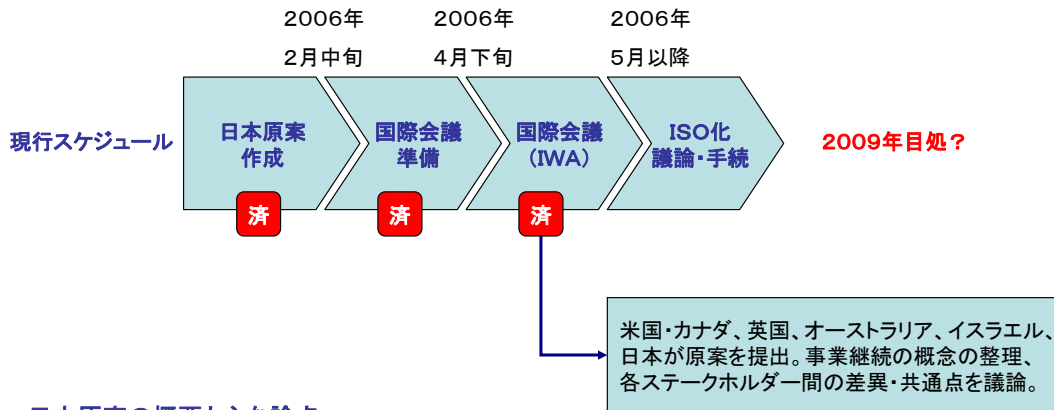
¹⁶ <http://www.dbj.go.jp/japanese/environment/infrastructure/DP-rating.html>

¹⁷ <http://www.newsweekjapan.hankyu-com.co.jp/cover/contents/20060621.html>

¹⁸ <http://nb.nikkeibp.co.jp/free/PROJECT/20050819/108139/>

¹⁹ <http://www.nikkei-ad.com/techo/2007/db/070102.html>

²⁰ <http://www.teco.tohatsu.co.jp/service/is022.html>



日本原案の概要と主な論点

- ・経済産業省、中央防災会議/内閣府のガイドラインの統合をベースに必要なに応じて内容を補記。
- ・第三者による認証制度を採用しない。
- ・災害発生直後における公的組織が第一義的行う活動は対象外。
- ・対象とするリスクは各組織が合理的な基準に基づき自主的に選択するものとする。
- ・広域災害においては、被災した地域の復旧計画との連携・調整に留意する。

図 2-2 ISO 化動向と日本の対応 (2007 年 1 月現在)

(出所：渡辺研司「企業経営における事業継続マネジメント～その戦略的重要性～」(講演資料), 2007.01.23)

3. 情報セキュリティ対策ベンチマークの改訂

本章では、前章で示した情報セキュリティ対策ベンチマークを巡る問題を踏まえ、見直した検討結果を示す。

3.1. 基本方針

情報セキュリティ対策ベンチマークの改訂に際しては、以下の基本方針を置いた。

(1) JIS Q 27001:2006 付属書 A 管理目的及び管理策との整合を前提とする

JIS Q 27001:2006 の付属書 A の管理目的及び管理策と整合した内容となるように、評価項目の構成や表現等を見直す。ベンチマークの評価項目 25 項目の本文で触れていない内容についても、解説文等でカバーし、管理策の 133 項目がベンチマーク 25 項目のいずれかに対応する形をとる。

(2) 継続性や既存の資産との整合性に配慮する

政府調達をはじめ情報セキュリティ対策ベンチマークが現在様々な形で活用されていることや、分析に利用可能なデータが約 3,800 件（利用者の提供データ及び平成 16 年度研究会における企業アンケートデータ）に達していることを踏まえ、継続性や既存の資産との整合性に配慮した変更とする。

(3) 変化や全体の中での位置が見えるようにする

利用者がベンチマークを繰り返し利用することを促進するため、過去から現在までのデータの推移を見たり、偏差値のように全体の中での位置を把握するためのデータを得られるようにして、利用者がレベルアップを実感できるようにすることを目指す。

(4) 平易な言葉を使用するとともに、曖昧な表現を排除する

IT についてあまり詳しくない経営層が利用することを想定し、可能な限り平易な言葉を使用する。また、USB や携帯電話の利用など、IT 環境の現状に合わせた内容にする。同時に、曖昧な表現を排し、該当・非該当の判別がつくような表現を用いることで、回答のブレを抑制する。

(5) 部門単位の利用や公的機関の利用を可能にする

利用者のニーズを踏まえ、企業における部門単位での利用や公的機関の利用が可能になるよう、属性の設問等における表現の改善や解説の補足を行う。

(6) 業務プロセスに沿った情報管理の視点を踏まえる

技術的対策ありきの説明ではなく、業務プロセスとそれに沿った情報管理が前提にあって、それに応じて対策を検討する必要があることを明確にする。

3.2. 作業方法

情報セキュリティ対策ベンチマークの改訂にあたっては、有識者、専門家、ユーザ企業、IPA等のメンバーによるワーキンググループを発足し、検討を行った。

検討作業は、3回の会合とメーリングリストによる討論等を経て実施した。

3.3. 改訂案

(1) 構成上の変更

構成上の主要な変更点と変更理由を以下に示す。

表 3-1 構成上の主要な変更点と変更理由

項目	構成上の主要な変更点	変更理由
全体	JIS Q 27001:2006 付属書 A 管理目的及び管理策に応じて評価項目の内容、[対策のポイント][説明][解説]を再構成	中堅・中小企業における実施上の制約に配慮しつつ、JIS Q 27001:2006 付属書 A 管理目的及び管理策との整合を実現
	企業単位の表現を変更 ・「自社」→「自組織」 ・「社内・社外」→「内部・外部」 ・「貴社における」を削除	部門単位の利用や公的機関の利用に配慮
1. 情報セキュリティに対する組織的な取組状況	組織、雇用に係る表現を改善 ・「業務プロセス」に基づく整理 ・従業者／従業員の使い分け ・退職に係る記載の充実 ・雇用に係る「機密保持」契約→「守秘義務」契約	より適切・丁寧な表現を選択し、誤解を避けるため
2. 物理的（環境的）セキュリティ上の施策	評価項目①と評価項目②を入れ替え	守るべき建物や区画を決めてから、人の出入りのルールを定める 内容が運用時の管理であるため、大項目3に入れるのが適当
	評価項目⑤を大項目3に移動	
3. 通信ネットワーク及び情報システムの運用管理	大項目2の評価項目⑤を①として追加	電子商取引の要素を補足するため
	評価項目⑤に保護の対象に「公開サーバのデータ」を追加	
4. 情報システムへのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策	タイトルの変更： 「情報システムの開発、保守におけるセキュリティ対策」と「情報システムへのアクセス制御」の前後を入れ替	ここでの「アクセス制御」は「開発、保守」時だけでなく「運用」時の場合も含むことを明確にするため
	アクセス制御の対象の分類を「情報／業務アプリケーション／ネットワーク」を「ID 識別・認証、ID 管理／アクセス権の付与／ネットワーク」に変更	ID 識別・認証とアクセス権の付与との違いについて理解を促すことが重要と判断したため
5. 情報セキュリティ上の事故対応状況	個人情報の漏えい時の対応について追記	個人情報保護法への適切な対応を促すため

具体的な改訂案を別紙 1 に示す。

(2) その他の改善点

(1)では評価項目の修正案を示したが、ワーキンググループではその他の改善すべき点についても議論がなされた。

①利用形態の多様化への対応

情報セキュリティ対策ベンチマークの用途として、たとえば、各部門の長に部門単位で回答させると、それぞれの意識のレベルやばらつきを明らかにして、全体の調整方針の検討に役立てることができる。そうしたニーズに対応するため、評価項目の修正に併せて行うべき自己診断サイトの改善策として、以下の案が挙げられた。

- ・自己診断に入る前に、評価の範囲（組織全体／部門単位）を選択させる。
- ・評価の対象とする事業を意識し、事業単位で適宜読み替えるように指示する。ただし、読み替えが難しい項目（例：人数）については必要に応じて解説を追記する。
- ・企業プロフィールについては全組織の単位で回答し、対策については該当部門の状況を回答する。

また、「部門ごとに何か作らなければならない」という誤解を与えることがないように留意する必要があるとの指摘も挙げられた。たとえば、部門単位で利用する場合、セキュリティポリシーを部門として独自に有する必要はなく、全社のものであれば十分であるという補足をすることが望ましい。

②偏差値の提示

サイトの利用者がベンチマークを繰り返し利用することを動機付けるため、全体の中での位置を把握するためのデータを得られるように、自己診断サイトにおいて偏差値を提示する機能を整備することが望まれる。

偏差値を算定する場合、その基礎データ（母数）については、情報セキュリティを巡る環境変化やレベルの変化を勘案し、ある程度古いデータは除外する仕組みを適用する必要がある。具体的には次の 2 つの案が得られた。

(案 1) 年度末で集計を区切り、過去 2 年間のデータを基礎データとする

たとえば、2007 年 4 月 1 日より 2008 年 3 月 31 日までの診断に対し、平均値や望まれる水準を出すための基礎データの集計期間は、当該年度を含めず前年度・一昨年度の合計、すなわち 2005 年 4 月 1 日²¹～2007 年 3 月 31 日とする。案 2 に比べ安定した基礎データを利用できると考えられる。

(案 2) 四半期ごとで集計を区切り、過去 8 四半期分のデータを基礎データとする

たとえば、2007 年 4 月 1 日より 2007 年 6 月 30 日までの診断に対する集計期間は 2005 年 4 月 1 日²¹～2007 年 3 月 31 日となる。同様に、2007 年 7 月 1 日より 2007 年 9 月 30 日までの診断に対する集計期間は 2005 年 7 月 1 日²¹～2007 年

²¹ ただし、情報セキュリティ対策ベンチマークの自己診断サイトは 2005 年 8 月 4 日から運用を開始したので、集計期間は 2005 年 8 月 4 日から開始する形となる

6月30日、2007年10月1日より2007年12月31日までの診断に対する集計期間は2005年10月1日～2007年9月30日となる。案1に比べ最新のデータを基礎データとして活用することができる。

なお、ワーキンググループでは、案1を実現した上で案2についても利用可能にすることが望ましいとの意見があった。

③利便性向上のための機能追加

その他、教育的効果を高めるため、画面上の評価項目の本文（質問）から自己診断中に「対策のポイント」等を直接参照できるようにしてはどうかとの意見があった。

4. 情報セキュリティ報告書モデルの改訂

本章では、2章で示した情報セキュリティ報告書モデルを巡る問題を踏まえ、見直した検討結果を示す。

4.1. 基本方針

情報セキュリティ報告書モデルの改訂に際しては、以下の基本方針を置いた。

(1) 短期的には情報開示企業の増加、長期的には企業間競争の本格化を促す

情報セキュリティ報告書には、情報セキュリティに係る情報開示の一般化と、情報セキュリティに係る企業間競争の本格化を促す役割が期待されている。これらを同時に実現することは困難であることから、短期的な目標として情報セキュリティに係る情報開示企業の増加、長期的な目標として情報セキュリティに係る企業間競争の本格化を設定する。

(2) 情報セキュリティ報告書の発行を容易にする

情報セキュリティに関する開示を一般化するためには、たとえば、情報セキュリティ報告書が多数発行されジャンルとして確立することが効果的である。情報セキュリティ報告書の発行を促す手段として、まず情報セキュリティ報告書の発行を容易にする方策を検討する。具体的には、記載内容を重要な項目に絞った簡易版の報告書イメージを明示し発行しやすさを訴求すること、また、情報セキュリティ報告書を実際に発行した企業の知見を踏まえ、導出が難しい項目の内容を改善することが挙げられる。

(3) 情報セキュリティ報告書に必要な項目を追加する

情報セキュリティに係る企業間競争の本格化を促すためには、報告書の記載項目中に、企業が訴求したいと考える項目や比較可能な項目が組み込まれていることが望ましい。そこで、発行経験者や有識者の意見を踏まえ、情報セキュリティ報告書の項目構成上、追加すべき項目を洗い出し、モデルに組み込むことが求められる。

ただし、「すべての項目をカバーしなければならない」との誤解を招かないようにする必要がある。

4.2. 改訂作業の概要

情報セキュリティ報告書モデルの改訂にあたっては、有識者、専門家、報告書発行企業等のメンバーによるワーキンググループを発足し、検討を行った。

検討作業は、3回の会合とメーリングリストによる討論等を経て実施した。

4.3. 改訂案

主要な変更点と変更理由を以下に示す。

表 4-1 構成上の主要な変更点と変更理由

項目	主要な変更点	変更理由
全体	記載することが望ましい「基本的な項目」の存在について補足	全項目を記載する必要はないことを明示し取組やすくするため
位置付け	「取引先への説明責任、関係者の意思統一・意識啓発、ブランドイメージの向上といった効果を意図として情報開示を行うのであれば、単体の報告書としての発行が効果的」というメッセージを追加	CSR 報告書等の一部とすると、分量の制約や読者層・テーマの違いから、本来発すべきメッセージを適切な相手に伝えきれない可能性が高いため
効果	[発行主体] 「準備や対外的な説明作業を通じて、経営者自身が情報資産とビジネスプロセスの関係を把握し説明責任を果たすことができる」ことを補足	経営者への啓発効果が期待できる点も情報セキュリティ報告書の重要な特長と考えられるため
	[ステークホルダー] 取引先、従業員・グループ会社・外部委託先、顧客・消費者、投資家、アナリスト、格付け機関・メディア・関連団体のそれぞれにとっての効果をより具体的に記載	ステークホルダーのそれぞれに訴求する有効性を明らかにして、理解を促すため
項目の変更・追加	[②経営者の考え方] 「対象となる情報」を追加	情報の種類により設定するセキュリティレベルが異なる可能性があるため
	[④情報セキュリティ対策の計画、目標] 「アクションプラン」を「基本的な項目」から外す	情報セキュリティ対策に関する行動計画を開示することが難しいケースもあると考えられるため
	[⑤情報セキュリティ対策の実績、評価] 「計画に対する実績」→「実績」	
	「実績に対する評価」を「基本的な項目」から外す	自己評価やその開示が難しいケースもあると考えられるため
	「実績に対する評価」に情報セキュリティ対策ベンチマークの自己診断結果等を提示することを追記	客観的な評価指標にニーズがあると考えられるため
	「情報セキュリティの品質改善活動」、「海外拠点の統制」、「外部委託」、「情報セキュリティに関する社会貢献活動」を追加	発行企業が訴求したい点や、社会的に共有すべき知見を取り上げやすくするため
	[⑥主要注力テーマ] キーワードとして「内部統制」を追加	内部統制を契機とした取組のケースもあると考えられるため
[⑦第三者評価・認証]	タイトルを「(取得している場合の) 第三者評価・認証等」に変更	第三者認証を取得していなくても報告できることを明示し、取組やすくするため
	「情報セキュリティ関連資格者数」、「格付け／ランキング」を追加	他社との比較の指標となりうる項目を加え、将来の競争への流れを確保するため
留意事項	情報開示の範囲や方向について誤ると、リスクを高める可能性もある点、トラブルが発覚すると報告書の内容の信頼性が問われるリスクもある点を明記	情報セキュリティ報告書の発行について客観的な判断を促すように補足

具体的な改訂案を別紙 2 に示す。

5. 施策ツールの普及方策案

情報セキュリティ対策ベンチマークや情報セキュリティ報告書モデルなどの施策ツールには、内容の改善だけでなく、社会に普及していくことで、情報セキュリティガバナンスの確立を促進するという重要な課題を抱えている。

「情報セキュリティガバナンスシンポジウム 2007」来場者アンケートによると、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のいずれも「利用したことがある」「内容を知っていた」人は2割前後にとどまり、4割以上が「知らなかった」と回答している。

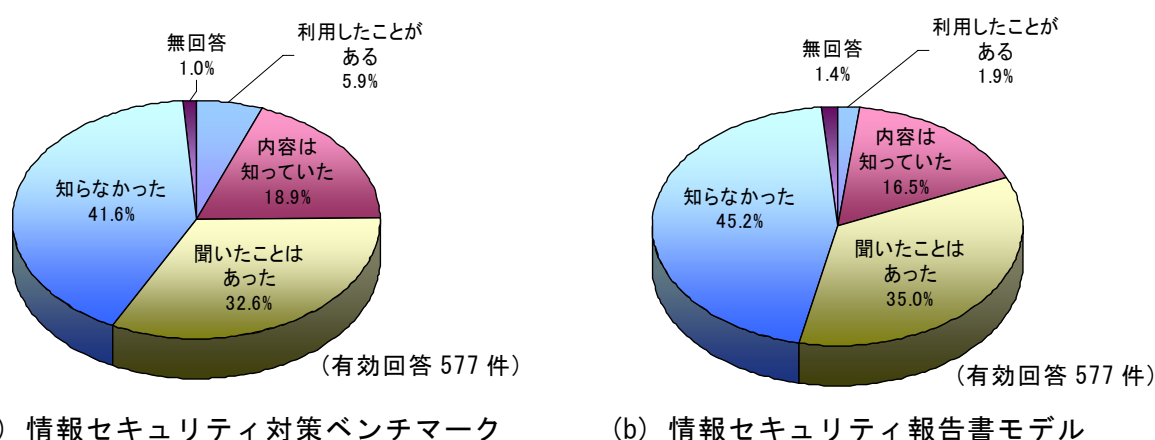


図 5-1 情報セキュリティガバナンスの施策ツールに関する認知度

(出所：「情報セキュリティガバナンスシンポジウム 2007」来場者アンケート)

したがって、これら施策ツールの普及のためには、シンポジウムやセミナー等イベントを中心とする啓発活動を通じて認知度向上を推し進めるとともに、実際の利活用につながる動機付けやきっかけを生み出す工夫が必要となる。そこで、本章では、このような施策ツールの普及方策に係るアイデアについて検討した結果を以下に示す。

5.1. 情報セキュリティ対策ベンチマークの普及方策案

(1) 活用事例の収集・公表

情報セキュリティ対策ベンチマークの普及方策の一つとして、どのように使いこなすと効果的かということ、具体的な活用事例を通じて周知し、利用を促すことが考えられる。

たとえば、関係団体等が主導する形で、ユーザ企業や IT コーディネータ、コンサルタント等から、社内での部署別利用や顧客への提案等の活用事例を募集し、その成果を公表してフィードバックする方向が期待される。

(2) 幅広い利用モデルの提案

事例が乏しいケースについても、情報セキュリティ対策ベンチマークの利用モデルを提

唱して、利用形態の幅を広げることを検討すべきである。たとえば、次のような方向について利用モデルを提示し、活用事例を広げていく取組が考えられる。

例 1) 企業グループ等への適用

系列や提携等によってブランドを共有する企業グループ等の場合、グループ内の一企業のトラブルがグループ全体に悪影響を及ぼすこともあるため、共通の方針で情報セキュリティ対策に取り組むことが望まれる。しかし、業種や文化の異なる企業間では意識や取組の水準に差があり、一社が他社を統制できる構造でなければ、グループ全体の足並みを揃えることは難しい。したがって、取組にどれだけの違いがあるのか、情報セキュリティ対策ベンチマークのような共通の尺度で計測した上で、望ましいレベルについて合意を形成していく必要がある。

例 2) 二者監査への適用

個人情報保護法の全面施行以降、受託企業では、委託元の要請に従って情報セキュリティ対策に関する対応状況の回答票（点検シート）を提出するケースが見られる。点検シートは委託元毎に異なるため、受託企業は類似作業を何度も行うことになる一方、委託元でも点検シートのバックデータがないため、委託先として適当か否かを判断することが難しい。このような委託元に対する情報開示の際に情報セキュリティ対策ベンチマークの自己診断シートを適用することで、

- ・受託企業は、作業の重複を省くことができる
- ・委託元は、多数のデータに基づくより客観的な指標を委託先選定に利用できる
- ・情報セキュリティ対策ベンチマークが共通の尺度として社会的に認知されるといった効果が期待できる。

例 3) 地方自治体への適用

地方自治体においては、近年の市町村合併の影響から、情報セキュリティの対応についての意思統一が十分でなく、部署間・地域間で混乱しているケースも少なくないと考えられる。そこで、自治体内の異なる部署間で意識や取組にどれだけ差があるのか、情報セキュリティ対策ベンチマークのような共通の尺度で計測した上で、望ましいレベルについて合意形成を図る展開が有効である。

5.2. 情報セキュリティ報告書モデルの普及方策案

(1) 業界別・事業者別の情報セキュリティ報告書発行の打診

当初、情報セキュリティ報告書の発行を広く呼びかける形で、まず 2 件の優れた事例を得ることができた。今後はこうした事例を一つの目標に置きつつ、できる限り多くの情報セキュリティ報告書の発行を促し、ジャンルを確立することを目指す。そのためには、業界・業種別に対象を明確化して、それぞれに適したアプローチで積極的な発行を働きかけることが重要である。以下に、発行が期待される業界や企業群の例を示す。

① IT 業界

システムベンダや情報サービス事業者等の IT ベンダ、通信キャリア及び ISP、EC

事業者などが挙げられる。IT 業界は、自身のビジネスの競争優位の確保という意味でも、また IT 利用のさらなる促進をユーザ企業に働きかける意味でも、本来は情報セキュリティに対する取組を積極的・先導的に説明すべき立場にある。IT 事業をビジネスの中心に据えているため、IT 事故が発生する可能性は他業種より高く、「安全宣言」としての説明はリスクが高いことも事実だが、その一方、情報セキュリティへの取組がサービスの高付加価値化につながる点、また事故発生後に何を説明しても伝わりにくい点に考慮すれば、日頃の適切な情報開示が重要であることは明らかである。

たとえば、業界団体を中心に、IT 企業に対して、情報セキュリティ報告書モデルとその具体事例に関する周知活動を推し進める取組が考えられる。

②金融業界

金融業は高度な情報管理が重視される業種であり、厳格なルールを用いた組織的対策や静脈認証等積極的な新技術の導入など、高レベルの情報セキュリティ環境の構築に注力している。そうした努力や姿勢を顧客等に適切に提示していくことで、業界内での競争優位を確保するだけでなく、社会の安心感・信頼感を高め、ステークホルダーとのより良い関係を形成することも可能である。また、そのような取組は、事業法に基づくコンプライアンスの一環としての開示にとどまらず、さらに踏み込んだ「攻め」の情報開示へとつながるものである。たとえば、業界を代表する事業者が報告書を活用して、情報セキュリティガバナンスの確立について説明することにより、そうした取組が業界全体に波及していく展開が想定される。

③IT 事故の経験企業

IT 事故を経験した企業、特に大手企業や社会的に影響の大きい企業では、顧客や消費者に対し、情報セキュリティへの取組についてどのように改善したか説明することは重要である。その際、情報セキュリティ報告書の枠組みを活用することで、効果的な説明を行うことができる。なお、情報セキュリティ報告書は「安全宣言」ではなく、改善に向けた真摯な姿勢、取組の適切性、妥当性を説明するものであることに留意すべきである。

(2) 情報セキュリティの開示状況の公表

情報セキュリティに関する情報開示は、経営層が自社の情報セキュリティレベルの向上に注力する動機付けとして有効である。したがって、企業に情報セキュリティ報告書の発行を促すとともに、報告書の発行が困難な企業に対しても、情報セキュリティに関する情報開示を促すことが重要である。

たとえば、上場企業を中心に、企業各社における情報セキュリティの開示状況を調査し、その結果を公表することによって、情報開示に対する抵抗感を緩和し、一般化を図る手法が考えられる。

さらに、そうした情報をもとに、ランキング等の形で比較評価したり、優れた情報開示事例に対する表彰等を行うことによって、企業の競争意識を刺激し、さらなる情報開示を促進する方策も考慮すべきである。

「情報セキュリティガバナンス研究会」委員名簿(2007年3月末現在)

【座長】

土居 範久 中央大学 理工学部 教授

【座長代理】

伊藤 邦雄 一橋大学大学院 商学研究科 教授

【委員】

岩間 研二 三菱電機株式会社 総務部情報セキュリティセンター担当部長
引頭 麻実 大和証券 SMBC 株式会社 事業調査部部長 シニアコーポレートアナリスト
大木 栄二郎 工学院大学 情報学部 教授
岡村 久道 弁護士法人英知法律事務所長 弁護士
喜入 博 KPMG ビジネスアシュアランス株式会社 常勤顧問
黒沼 悦郎 早稲田大学大学院 法務研究科 教授
佐藤 淑子 日本インベスター・リレーションズ (IR) 協議会 首席研究員
藤本 正代 富士ゼロックス株式会社 マネジメントイノベーションオフィス シニアマネージャー
松尾 明 青山学院大学 会計プロフェッション研究科 特任教授
松本 主計 株式会社リコー CSR 本部 情報セキュリティセンター 参与
三角 育生 独立行政法人情報処理推進機構 セキュリティセンター長
渡辺 研司 長岡技術科学大学 工学部 助教授

【オブザーバ】

経済産業省
社団法人日本経済団体連合会
社団法人情報サービス産業協会
社団法人日本情報システム・ユーザー協会
社団法人日本損害保険協会

【事務局】

株式会社三菱総合研究所

「情報セキュリティ対策ベンチマークワーキンググループ」委員名簿(2007年3月末現在)

【主査】

大木 栄二郎 工学院大学 情報学部 教授

【委員】

岩間 研二 三菱電機株式会社 総務部情報セキュリティセンター担当部長
河野 省二 株式会社ディアイティ セキュリティビジネス推進室 室長
菅野 泰子 独立行政法人情報処理推進機構 セキュリティセンター 調査役
重松 孝明 有限会社e社会研究所 代表取締役社長
長嶋 潔 東京海上日動リスクコンサルティング株式会社 リスクコンサルティング室 主席研究員
保科 剛 日本ユニシス株式会社 最高技術責任者
松尾 正浩 株式会社三菱総合研究所 コンサルティング事業本部 主席研究員
山本 匡 株式会社損害保険ジャパン・リスクマネジメント 情報セキュリティ事業部 上席コンサルタント

【オブザーバ】

経済産業省

【事務局】

株式会社三菱総合研究所

「情報セキュリティ報告書モデルワーキンググループ」委員名簿(2007年3月末現在)

【主査】

加賀谷 哲之 一橋大学大学院 商学研究科 助教授

【委員】

大久保 和孝 新日本監査法人 CSR担当パートナー
佐野 智己 凸版印刷株式会社 コーポレートコミュニケーション部 CSRソリューションチーム主任
清水 恵子 みすず監査法人 シニアマネージャー
田村 仁一 監査法人トーマツ エンタープライズリスクサービス部 ディレクター
藤本 正代 富士ゼロックス株式会社 マネジメントイノベーションオフィス シニアマネージャー
松本 主計 株式会社リコー CSR本部 情報セキュリティセンター 参与
三好 眞 株式会社格付投資情報センター 新規事業開発室長

【オブザーバ】

経済産業省

【事務局】

株式会社三菱総合研究所

活動記録

【情報セキュリティガバナンス研究会】

2007年1月26日	第1回会合	現状認識と論点について
2007年3月22日	第2回会合	報告書（案）について

【情報セキュリティ対策ベンチマークワーキンググループ】

2007年2月9日	第1回会合	目標、活動方針の意識合わせについて
2007年2月22日	第2回会合	ベンチマークの見直しについて
2007年3月6日	第3回会合	ベンチマークの見直しについて（とりまとめ）

【情報セキュリティ報告書モデルワーキンググループ】

2007年2月13日	第1回会合	目標、活動方針の意識合わせについて
2007年3月2日	第2回会合	モデルの見直しについて
2007年3月12日	第3回会合	モデルの見直しについて（とりまとめ）