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

はじめに

今日、わが国企業は、情報開示（ディスクロージャー）や法令遵守（コンプライアンス）、企業の社会的責任（Corporate Social Responsibility：CSR）等といった世界的潮流の渦中で、日々熾烈な競争を繰り広げている。このように企業の経営に対する社会的要請が急速に変容し、拡大しつつある中、企業は、株主をはじめとするステークホルダーのため、永続的な発展と自らの価値の最大化を同時に追求することが求められている。

また、わが国では、e-Japan 戦略に基づく世界最高水準の IT 社会が実現しつつあり、企業においても IT の利活用が飛躍的に高度化し、ビジネスの効率化・高付加価値化をもたらしている。今や我々の経済活動や社会生活はＩＴによって支えられていると言っても過言ではない。

このように IT が企業、ひいては社会の「神経系」を担う一方、コンピュータウイルスやワームの感染拡大、機密情報の流出、システムダウン等、新しいタイプのリスクも顕在化しており、各企業は先に述べた競争の中で、このような新次元の事業リスクにも対応すること、つまり情報セキュリティ対策を適切かつ十分な形で推進することが必要不可欠となってきている。しかしながら、企業の情報セキュリティ対策は、上記のような事故が発生した後に場当たり的に対応するなど、適切になされているとは言い難い状況である。

こうした現状を踏まえ、企業が、このような対症療法的な対策から脱却し、自律的・継続的な取組みを推進していくには、情報セキュリティ対策を、単なるコストではなく、企業価値を高めるために積極的に取り組むべき投資対象として位置付けることが重要であり、そのための新たな環境の整備が不可欠である。同時に、自身の被害の局限化や法令遵守の観点に加え、IT 社会の一員としての社会的責任という観点も踏まえた形で情報セキュリティ対策に取り組む推進力を企業内に構築・運用していくことも重要である。これはすなわち「情報セキュリティガバナンス」という新たな概念を企業経営に組み込んでいくことに他ならない。

このような認識から、経済産業省では、平成 16 年９月より、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、その具体的な実現手段について、内部統制や財務報告といった観点にわたり、幅広く精力的な議論を重ねてきた。本報告書は、本研究会における検討の成果をとりまとめたものであり、情報セキュリティガバナンス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」を策定するとともに、それらの効果的な普及方策について提言したものである。

本報告書において示した情報セキュリティガバナンスの考え方が、企業の経営層はもとより、社会全体に浸透することによって、企業において IT の利活用が信頼性を担保した形で推進され、競争力が強化されるとともに IT 社会の一員としての社会的責任が全うされること、ひいては世界最高水準の「高信頼性社会」の実

現や、「セキュリティ文化」の醸成に寄与することを願ってやまない。

平成 17 年 3 月
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
座長　　土居　範久

目　　次

【参考資料】

１.検討の背景と方向性

１.１.社会の「神経系」を担う情報技術

情報技術（Information Technology：IT）は急速に普及が進展し、今や我々の社会を支えるインフラとして、必要不可欠な役割を担っている。特に企業活動においては、事業活動における IT への依存度が急速に高まっているだけではなく、EC/EDI[1]、SCM[2]、ERP[3]、CRM[4]に代表されるように、その利活用の形態も著しく高度化・複雑化しつつある。

（１）電子商取引市場の拡大

IT 革命を契機として本格化した企業活動における IT の利活用や、ネットワークユーザの急速な増加・多様化を背景として、電子商取引（EC）の市場は急成長を遂げている。企業間取引（BtoB）については、過去５年間で約９倍（1998 年：8.6 兆円 → 2003 年：77.4 兆円）、企業・消費者間取引（BtoC）については、同じ５年間で約 69 倍（1998 年：0.06 兆円→2003 年：4.4 兆円）と、それぞれ急激に成長している（図 １-１及び図 １-２参照）。さらに、ネットオークションのような CtoC の取引量も着実に拡大しており、こうした EC 市場拡大の流れは、経済分野における IT 依存の高まりの一端を示していると言えよう。

図 １-１　BtoB EC の市場規模の推移

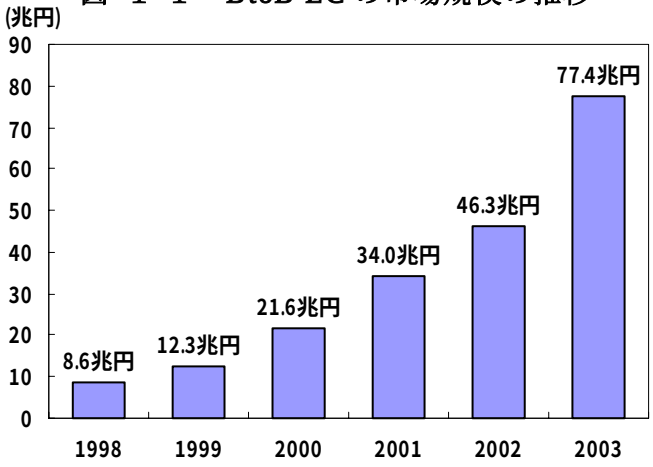
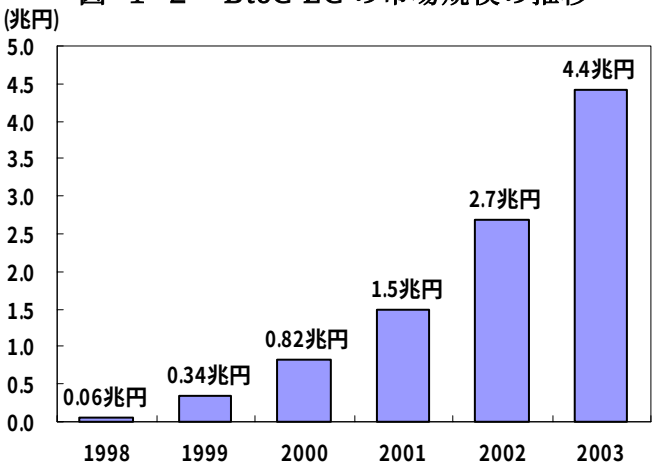


図 １-２　BtoC EC の市場規模の推移



注：1999 年は BtoB EC 調査を行っていないため、1998 年調査による予測値を使用。
出所：経済産業省「電子商取引に関する実態・市場規模調査」(2003 年 6 月)

[1] EC（Electronic Commerce）：ネットワークを介して契約や決済等を行う電子化された商取引の形態。EDI（Electronic Data Interchange）：商取引情報を標準化し、企業間で電子的に交換する仕組み。
[2] SCM（Supply Chain Management）：資材の調達から在庫管理、製品の配送・販売までの事業プロセス全体を総合的に管理し、在庫の削減や市場ニーズへの迅速な対応を実現する手法。
[3] ERP（Enterprise Resource Planning）：企業の基幹業務（会計、人事、給与、販売、生産等）の情報を一元管理し、業務プロセスを効率化する手法。
[4] CRM（Customer Relationship Management）：顧客情報をデータベース化して、顧客満足度の改善や営業の効率化、市場分析、品質改善等に活用する手法。

（２）IT の利活用と企業業績

IT の利活用度と企業業績の見通しに関する調査（図　1-3 及び図　1-4 参照）によると、情報システムの組織的な利活用が進んでいる企業ほど、業績の向上が予想される傾向が見受けられた。現時点では、IT の利活用により個別部門ごとの効率化を図る企業（ステージ 2）が大半であるが、企業組織全体のプロセスの最適化（ステージ 3）や、複数の企業で構成するバリューチェーンマネジメント[5]の最適化（ステージ 4）へと進化を遂げた企業も少数ではあるが存在しており、企業経営における IT のより効果的な利活用が、各分野・業種においてさらに進展していく可能性もある。

図　1-3　IT の利活用度と企業業績の見通し

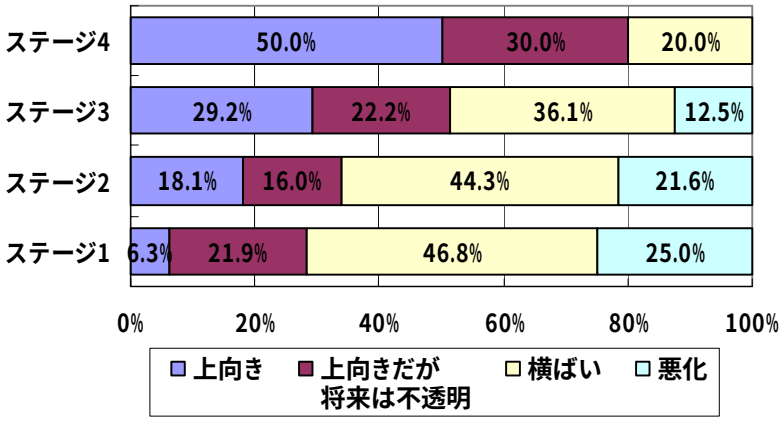
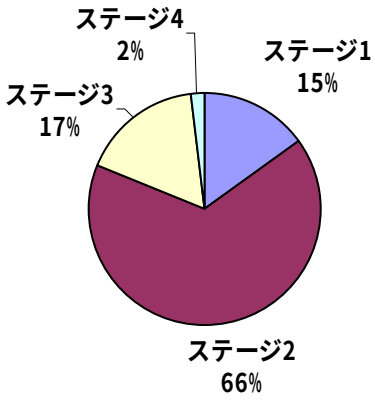


図　1-4　IT 利活用段階の分布



ステージ 1：単に情報技術を導入しただけで、その活用がなされていない企業群（「IT 不良資産化企業群」）
ステージ 2：情報技術の活用により、部門ごとの効率化を実現している企業群（「部門内最適化企業群」）
ステージ 3：企業組織全体におけるプロセスの最適化を行い、高効率と顧客価値の増大を実現している企業群（「組織全体最適化企業群」）
ステージ 4：単一企業組織を超えて、バリューチェーンを構成する共同体全体の最適化を実現している企業群（「共同体最適化企業群」）

出所：経済産業省「情報技術と経営戦略会議報告書」（2003 年 10 月）

１．２．企業や組織の情報セキュリティ対策の現状認識

（１）IT 事故[6]の影響の増大

近年、コンピュータウイルス・ワームの感染拡大、企業の保有する機密情報・個人情報の流出、システムダウンによる業務の停滞等の「IT 事故」が相次ぎ発生している。情報流出のケースでは金銭的被害も生じており、企業経営への影響が顕在化しつつある（表　1-1 参照）。

---

[5] 多国籍企業などが開発から資材調達・製造・販売に至る業務の全過程を，世界全体で最も効率的に行う経営手法。価値連鎖経営。

[6] 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（ソフトウエア（アプリケーション、システムソフトウエア、ユーティリティ）、ハードウエア（コンピュータ装置、通信装置、メディアなど）等）を指す。

また、社会全体が高度にネットワーク化されてきた結果、IT 事故の影響が個別企業内の問題に留まらず、社会全体に波及する事例も発生している（表 1-2 参照）。

このように、IT 事故は企業経営に直結することから、企業自らが情報セキュリティ対策を行うことが基本であるものの、企業における IT 事故が社会全体に波及する傾向もあることから、企業における情報セキュリティ対策の実施は、株主、消費者、取引先のみならず、社会全体から求められていると言っても過言ではない。

表 1-1　IT 事故による情報流出事例

企業名	事案の概要
大手 通信事業者A	・加入者、無料体験キャンペーン申込者、解約者などの数百万の個人情報（氏名、住所、電話番号、メールアドレス）が大量流出。代理店の経営者などが顧客情報を入手し、恐喝。 ・二次流出、悪用は確認されていない。 ・全会員を対象にお詫び料として1人当たり500円を支給。総額31億円を特別損失として計上。 ・事件直後、サービス新規加入者数が通常の半分に落ち込み。
大手 流通業者B	・会員カードの数十万の顧客情報（氏名、住所、性別、生年月日、自宅電話番号、携帯電話番号）の流出が発覚。 ・一部会員に不審なダイレクトメールが送られた。 ・全会員を対象に、お詫び料として1人当たり500円の商品券を支給。数億円の特別損失。
大手 メーカーC	・自衛隊の情報データ通信システムのIPアドレスやシステムの経路図などの重要資料が、システム開発を請け負ったメーカーCの孫請け会社を通じて外部に流出。 ・この資料を入手した複数の人物からC社へ買い取り要求があったことから事件が発覚。 ・一部の下請け企業名の報告を怠った契約不履行を理由に、一定期間の指名停止処分。 ・同システムの全面刷新をC側の費用負担で実施することで合意。

出所：各種報道資料を基に作成

表 1-2　IT 事故が及ぼす社会的影響の事例

○航空管制システム障害による影響

・2003年3月、航空機の飛行計画などを管理する「飛行計画情報処理システム」に障害発生。原因はプログラムの不具合。
・欠航215便、大幅な遅延1500便以上、約30万人の利用者に影響。
・2004年4月にも航空路レーダー処理システムのトラブルでメインシステムを停止。国内便約１３０便が遅延などの影響を受けた。

○金融ネットワークの障害による影響

・2004年1月、金融機関同士のATMをネットワークで結ぶ「統合ATMスイッチングサービス」に障害発生。原因は通信制御プログラムの不具合。
・全国約20の金融機関のATMで他行カードを利用した取引が不可に。

○医療現場のネットワーク障害による影響

・2004年3月、大学病院の学内ネットワークが「SQL Slammer」というワームに感染、これに接続する電子カルテシステムなどが利用できなくなり、完全復旧まで1日半外来患者が受け付けられない状態が続いた。
・システムを利用する外来患者数は1日平均4,000人、ピーク時には1時間で1,400人。

出所：各種報道資料を基に作成

（2）IT 事故を巡る社会情勢

①国内の状況

我が国では、法令遵守と企業の社会的責任（Corporate Social Responsibility：CSR）[7]の両面から、企業における情報セキュリティ対策が問われつつある。

前者についての代表例は、「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）である。個人情報保護法は、IT 化の進展に伴う個人情報の利用の増加と個人情報の取扱いに対する社会的な不安感の広がりを背景として 2003 年５月に成立したものであり、2005 年４月から全面施行される。本法によって、個人情報取扱事業者[8]に該当する企業は情報セキュリティ対策を中心とした「安全管理措置」が義務付けられるため、該当する企業には早急な対応が求められている（表 1-3 参照）。

表 1-3　個人情報保護法における安全管理措置関連箇所

（安全管理措置）
第二十条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。
（従業者の監督）
第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。
（委託先の監督）
第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

出所：「個人情報の保護に関する法律」（平成十五年法律第五十七号）より抜粋

また、法令に基づく情報開示という観点では、証券取引法に基づく、有価証券報告書の継続開示企業に対する投資家の判断に重要な影響を及ぼす可能性のあるリスク情報（IT リスクを含む）を有価証券報告書に記載することの義務付け、各事業法に基づく、金融業界（銀行業、保険業）に対する業務及び財産の状況に関する説明書類におけるリスク管理体制に関する記載の義務付けが挙げられる（表 1-4 参照）。

一方、CSR の観点から情報セキュリティを捉える動きも顕在化しつつある。社団法人日本経済団体連合会「企業行動憲章 ―社会の信頼と共感を得るために―」（最新版：2004 年５月 18 日改訂）では、企業の遵守すべき行動 10 原則の中で「社会的に有用な製品・サービスを安全性や個人情報・顧客情報の保護に十分配慮して開発、提供し、消費者・顧客の満足と信頼を獲得する。」との方針を示している。また、企業の CSR に係る取組みを開示する CSR 報告書において、情報セキュリティ対策の方針や実施状況を取り上げる事例（表 1-4 参照）も出てきている。現在の CSR を巡る議論[9]では情報セキュリティを正面

---

[7] 企業の責任を，従来からの経済的・法的責任に加えて，企業のステークホルダー（社内外の利害関係者。従業員や株主、消費者、取引先に加え、地域社会まで含める場合が多い）にまで広げる考え方。

[8] 5 千件を超える個人情報を、コンピュータなどを用いて検索することができるよう体系的に構成した「個人情報データベース等」を事業活動に利用している事業者。

[9] 近年、環境・エネルギー問題、製品・サービスの安全性、雇用のあり方などに対する意識の高まり、企業不祥事によるブランド価値の崩壊、社会的責任投資（SRI：Socially Responsible Investment）の拡大、国際標準化機構（ISO：International Organization for Standardization）での検討などを背景に、各国において CSR の定義や基本的考え方、規格化等に関する議論が行われてきた。ISO では、2004

から取り上げる動きは見られないが、IT 事故による社会的影響の増大を踏まえれば、将来的に情報セキュリティが CSR の重要な一要素となる可能性もある。

表 1-4　情報セキュリティの状況に関する企業の情報開示

情報開示手法	概　要
有価証券報告書におけるリスク情報の開示	投資家への説明責任として、有価証券報告書の継続開示企業には有価証券報告書におけるリスク情報の開示が義務づけられている(対策の取組状況等は対象外)。投資家の判断に重要な影響を及ぼす可能性のある事項を記載することで正確な投資判断を促すことを目的とする。一部の企業は情報システムのリスクを明示している。
銀行業及び保険業におけるディスクロージャー誌	銀行及び保険業は、事業法において「業務及び財産の状況に関する説明書類」の作成・公表が義務づけられており、その開示項目に「リスク管理の体制」がある。記載するリスク情報のうち、オペレーショナルリスクには、コンピュータシステムの停止や誤作動、不正利用等により金融機関が損失を被るリスクを想定したシステムリスクが含まれている。
CSR 報告書	これまで環境報告書を公表する企業が多かったが、近年、雇用、人権、コンプライアンス、社会貢献なども含めた CSR（企業の社会的責任）報告書、サステナビリティ（持続的可能性）報告書を公表する企業が徐々に増加している。これら報告書の中で「情報セキュリティ」「個人情報保護」を個別テーマとして取り上げるケースも存在している。
対策実施報告	個人情報流出等の IT 事故を経験した企業が、信頼性を回復するため、事故の経緯や情報セキュリティ対策の実施状況、改善項目などについて公表を行うもの。具体的な対策内容が記載されているが、公表事例は少ない。

②米国の状況

米国では、企業の不正会計対策やテロ対策の波及効果として、情報セキュリティへの取組みが進展しつつある。

2001 年以降、大手企業の不正会計事件が相次ぎ発覚し、失墜した株式市場の信頼性を回復するため、米国ではコーポレート・ガバナンス[10]の徹底を企業に求める Sarbanes-Oxley 法（企業改革法）[11]が 2002 年７月に制定された。同法では、財務諸表の正確性の保証を米株式市場に株式を公開している企業の CEO（Chief Executive Officer：最高経営責任者）及び CFO（Chief Financial Officer：最高財務責任者）に義務付けていること、また、財務報告プロセスに関わる内部統制については情報システムの有効性の評価も求められていることから、対象企業は結果的に情報セキュリティ対策を強化する必要に迫られている。

また、1993 年のワールドトレードセンター爆破事件を契機に、テロ対策の必要性が叫ばれ、企業においても事業継続計画（Business Continuity Plan：BCP）[12]への関心が高まった。さらに、2001 年の同時多発テロ事件以来、米国のリスク管理に対する意識が大きく変わり、BCP をより実践的に策定・運用する傾向が見られる。特に、事業の IT 依存度が高まっていることから、BCP の策定・運用においては IT の継続性も考慮した検討がなさ

年 6 月、CSR のガイドラインを策定することを決定。

[10] 企業の健全な経営のための意思決定の仕組み。ステークホルダーの利害調整、経営への反映、健全な経営に向けて経営者の規律付け、監視・監督等を表す。

[11] 同法の対象は、米国の株式市場に株式を公開している企業であり、時価総額が 7500 万ドル以上の米国企業には 2004 年度 11 月 15 日以降終了する事業年度から、それ以外（米国で上場している日本企業のような外国企業を含む）の企業には 2006 年 7 月 15 日以降終了する事業年度から適用される。

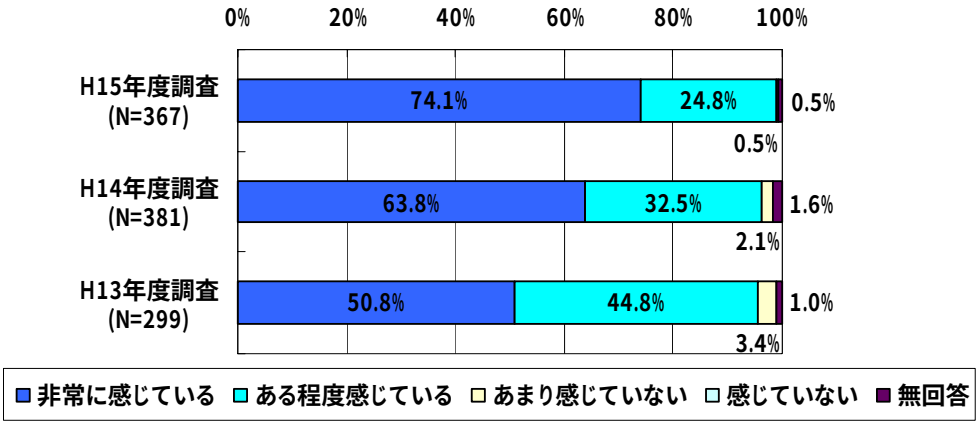
[12] 災害や事故等の発生に伴って通常の事業活動が中断した場合に、可能な限り短い期間（時間）で事業活動上最も重要な機能を再開できるように、事前に準備する計画。

れているものと推測される。

（３）情報セキュリティ対策の現状

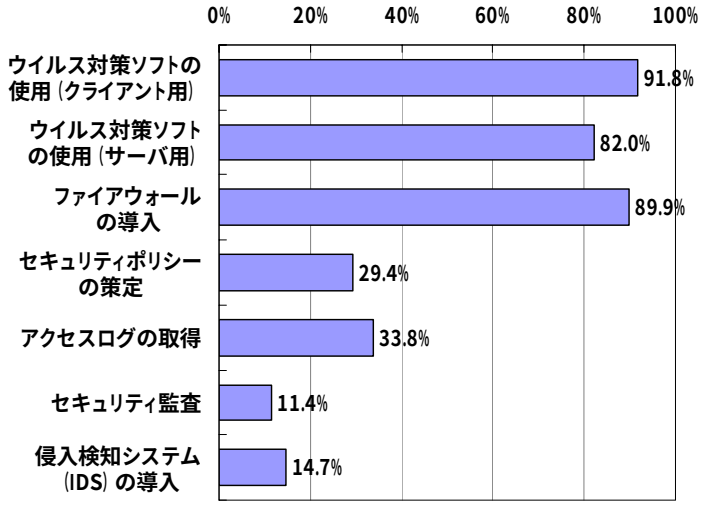
情報セキュリティ対策の必要性は、我が国の企業においても共通認識となりつつある（図１-５参照）。しかしながら、実態としては、コンピュータウイルス対策ソフトやファイアウォールといった製品の導入による対策が中心であり、組織的な対策（セキュリティポリシーの策定、セキュリティ監査、アクセスログの取得・解析等）は十分に行われていない状況にある（図　１-６参照）。

図　１-５　大手・中堅企業における情報セキュリティの必要性（重要インフラ業種を除く）



出所：警察庁「不正アクセス行為対策等の実態調査」（2003 年 12 月）

図　１-６　大手・中堅企業における情報セキュリティ対策の導入状況
（重要インフラ業種を除く）

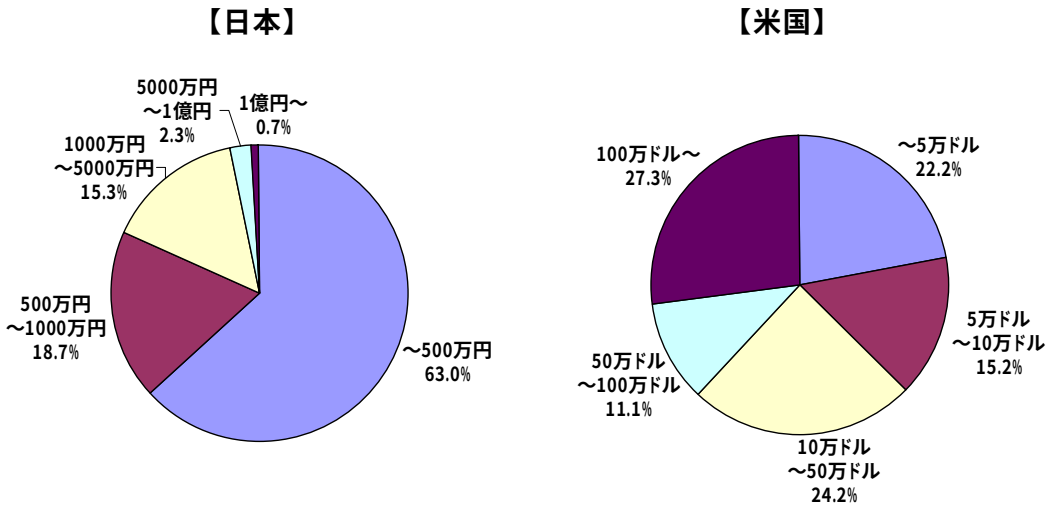


出所：警察庁「不正アクセス行為対策等の実態調査」（2003 年 12 月）

なお、日米の情報セキュリティ投資額を比較すると、日本企業に比べて、米国企業は投資額が多様化している。これは、日本企業の対策が製品の導入に偏っているのに対し、米

国企業では組織的な対策も含めた多面的な取組みがなされているためではないかと推測される（図　1-7参照）。

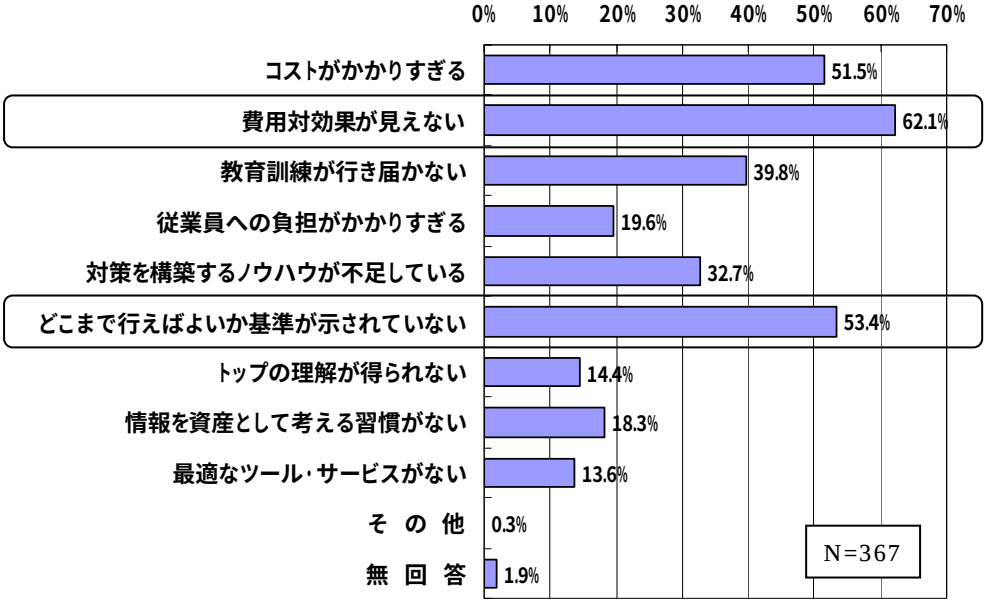
図　1-7　日米の情報セキュリティ投資額の比較（2001年）



・日本のデータは総務省「情報セキュリティ対策の状況調査」(平成14年5月発表)より引用。東証一部・二部上場企業2063社中541社が回答（回収率26.2%）、うち当該設問の未回答分31社を除く510社。
・米国のデータはInformation Security Magazine "2001 Information Security industry survey"（2001年10月発表）より引用。同誌のニューズレター会員45,000人中2545人が回答（回収率5.7%）、うち当該設問の回答者1746件。

このように国内企業の情報セキュリティ対策が十分に進んでいない原因として、①投資効果が見えない、②どこまで行えばよいか基準が示されていない、③コストがかかりすぎる等を挙げる調査結果も存在する（図　1-8参照）。③の経済的負担については、各企業の業種業態、経営方針、業績等との兼ね合いもあり、一概に情報セキュリティ投資に対する負担の多寡を論じることはできないが、①及び②については、情報セキュリティ投資の費用対効果が曖昧で、何をどこまで行うべきか判断が難しいという企業の悩みがうかがえる。

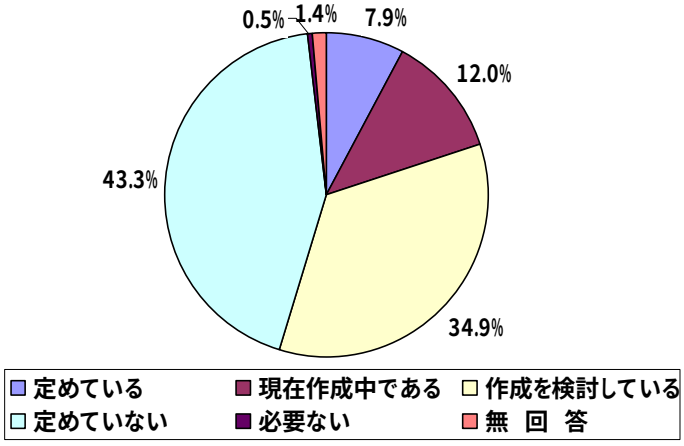
図 1-8　大手・中堅企業における情報セキュリティ投資の障害（重要インフラ業種を除く）



出所：警察庁「不正アクセス行為対策等の実態調査」（2003 年 12 月）

IT 事故が発生した場合の対応計画を作成済もしくは作成中の企業は、国内では 2 割にとどまる（図 1-9 参照）。米国では、BCP を作成済もしくは作成中の企業は 9 割超との調査結果[13]もあり、我が国企業の IT 事故に対する備えは米国に比べ脆弱と考えられる。

図 1-9　大手・中堅企業における非常事態発生時の対応計画の策定状況
（重要インフラ業種を除く）



出所：警察庁「不正アクセス行為対策等の実態調査」（2003 年 12 月）

[13] 米 KPMG “ KPMG 2002 BUSINESS CONTINUITY STUDY ”（2002 年）によると、米国では BCP 策定済みの企業は 67%、策定中の企業は 29%であり、未対応企業は 4 %に過ぎない。

２.情報セキュリティガバナンスの確立に向けて

２.１.情報セキュリティガバナンスの必要性

（１）企業[14]のあるべき姿と政府の役割

高度にネットワーク化されたIT社会においては、企業一社のIT事故によるトラブルが社会全体に波及する可能性がある。したがって、企業は、自身の被害の局限化や法令遵守への対応に留まらず、IT社会を構成する一員としての立場からも情報セキュリティ対策に取り組む責務があると考えられる[15]。また、平成15年10月に産業構造審議会情報セキュリティ部会が策定した「情報セキュリティ総合戦略」において掲げられているように、こうした取組みを通じて、世界最高水準の「高信頼性社会」の構築を目指していくことが極めて重要である。

なお、こうした企業の取組みを支えるためには、企業の情報セキュリティに対する努力を企業価値として評価するとともに、そうした取組みを促進していく、環境の整備が重要となる。政府の果たすべき役割は、企業による自主的な情報セキュリティ対策の取組みを促す環境の整備を支援することにある。

（２）情報セキュリティガバナンスの必要性

企業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、事故は起こりうるもの」との前提に立ち、対策をその場しのぎの対症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[16]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」[17]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

---

14 主に情報システムのユーザ企業とする。ただし、いわゆる重要インフラ業種（特に制御系）は、特別なリスクを有し、別途高いレベルのリスク管理策を検討する必要があると思われる。

15 OECD（Organization for Economic Cooperation and Development：経済協力開発機構）は「情報システム及びネットワークのセキュリティのためのガイドライン ― セキュリティ文化の普及に向けて ―」（2002年7月）に示した9原則の中で、情報社会のすべての参加者が「情報システム及びネットワークのセキュリティに責任を負う」ことについて言及している。

16 企業がその業務を適正かつ効率的に遂行するために、社内に構築され、運用される体制及びプロセス。「企業が事業目的の達成に係るリスクを低減させ、持続的に発展するためにも不可欠」（経済産業省「リスク新時代の内部統制」（2003年6月））とされる。なお、情報セキュリティの重要性は高まっているが、情報セキュリティが内部統制の必須要素となっているわけではない。

17 米National Cyber Security Partnership（NCSP）のコーポレート・ガバナンス・タスクフォースが発表した「Information Security Governance A CALL TO ACTION」（2004年４月）では、情報セキュリティガバナンスをITガバナンスの一部に位置づける見方が提唱されている。NCSPは、2003年12月に開催された全米サイバーセキュリティサミットを受けて結成された、国家の情報セキュリティレベルを高めるための官民連携の事業。同タスクフォースは「情報セキュリティの推進は、品質保証の取組みと同様、ビジネスコストの増加につながると多くの企業が考えているが、将来的には生産性の向上、顧客満足度の向上、ブランド力の強化が大いに期待できる」としている。

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、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。

２.２.企業の取組みを阻害する問題点

2.1.に示したとおり、企業による情報セキュリティガバナンスの確立に向けた自主的な取組みが期待されるが、実際にはそうした取組みが進んでいないのが実情である。そこで、1.2.(3)の現状分析から、企業の情報セキュリティに係る取組みを阻害する問題点を整理すると、次の項目が挙げられる。

①IT 事故発生のリスクが明確でなく、適正な情報セキュリティ投資の判断が困難

情報セキュリティ対策の難しさは、実際に情報システムやネットワークに係るトラブルが発生して、初めてその重要性に気づかされることにある。つまり、「情報システムは正常に稼働するもの」「企業の機密情報は漏洩しないもの」という思いこみがあるため、事故発生に伴う経済的損失やステークホルダーからの信頼喪失等といった企業経営に対するリスクを冷静に把握することが難しい。

さらに、企業経営者の視点から情報セキュリティ対策を考えると、具体的にどのようなリスクに対してどこまでセキュリティ対策を行えばよいか、また、どの程度セキュリティ投資を行えばよいかという判断基準がないという理由から、利益に直結しない情報セキュリティ投資を躊躇するケースも多く存在すると考えられる。

②既存の情報セキュリティへの「対策」「取組み」が企業価値に直結していない

情報セキュリティの確保は、企業活動におけるいわば「裏方」の位置にあり、その必要性はトラブルの未然防止の観点からある程度理解されつつあるものの、対策によるリスク低減の効果がわかりにくいこともあって、事業上のリスク回避策として積極的に情報セキュリティ対策に取り組む企業がステークホルダーから相応に評価されていない。

このため、企業戦略の観点から、情報セキュリティの取組みを同業他社との差別化を図る上での一要素として採り上げるケースや、説明責任の一環として積極的に開示しているケースはまだ少ない状況にある。

③事業継続性確保の必要性が十分に認識されていない

企業における IT 依存度が高まり、その利活用の形態も高度化しつつある中、自然災害等による情報システムのダウンや重要情報の流出等、企業の情報システムやネットワーク、情報資産に関連する突発的な事故が発生した場合であっても、事業を中断せず維持することは、企業にとって重要な課題となっている。しかしながら、国内の企業においては、個々

の事業形態・特性などを考慮した上で、自らの存続の生命線である事業継続を確保することの必要性が十分に認知されていないと思われる。

２.３.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

以上のとおり、企業における情報セキュリティに係る取組みは依然として進んでいない状況にあるが、以上の問題点を克服し、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、本研究会は以下の３つを提示する。

①情報セキュリティ対策ベンチマーク

企業においては、情報セキュリティに係る必要な対策や適正と考える水準について、目安となる指標が求められている。このため、ISMS 評価基準[18]に基づく評価項目を策定し、個々の評価項目に関する平均的なレベルや改善のための推奨される取組みなどを提供する。

②情報セキュリティ報告書モデル

企業が社会から適正に評価されるためには、社会が必要としている項目についての情報開示が不可欠である。このため、企業の IR（Investor Relations）[19]などの一環として、情報セキュリティポリシーやそれを実現する内部統制の仕組み、第三者評価等、社会的関心の高い項目について対外的に公表する「情報セキュリティ報告書」のモデルを提唱する。

③事業継続計画策定ガイドライン

事業の IT 依存度が高まる昨今、企業においては IT 事故を想定した BCP の策定が急務と考えられる。しかしながら、我が国における BCP の取組みは十分進んでいないのが現状である。このため、企業に対し 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。

これらの施策ツールの狙いは情報セキュリティガバナンスの確立にある。

それを実現する方向の一つとして、自社の情報セキュリティの取組みを客観的に検証し、改善を図る ISMS 認証や情報セキュリティ監査等の第三者評価・認証は効果的と考えられる。しかし、現状ではそうした第三者評価・認証の活用は十分でなく、製品の導入でとどまっている企業が多い。そこで、情報セキュリティ対策ベンチマークのセルフチェックを通じて、まず、対策を実施していない、あるいは簡易な対策しか行っていない企業に対し必要な取組みに関する理解を促すとともに、継続的な活用によるさらなるレベルアップを支援し、第三者評価・認証の実施へとつながる「入口」となることを目指す。

また、情報セキュリティ報告書を通じて、ISMS 認証や情報セキュリティ監査等を含む情報セキュリティへの取組みを公表することによって、透明性を高め、企業に対するステ

---

[18] 情報セキュリティマネジメントシステム（ISMS）適合性評価制度（脚注 20 参照）において、第三者である審査登録機関が本制度の認証を希望する事業者の適合性を評価するための基準。

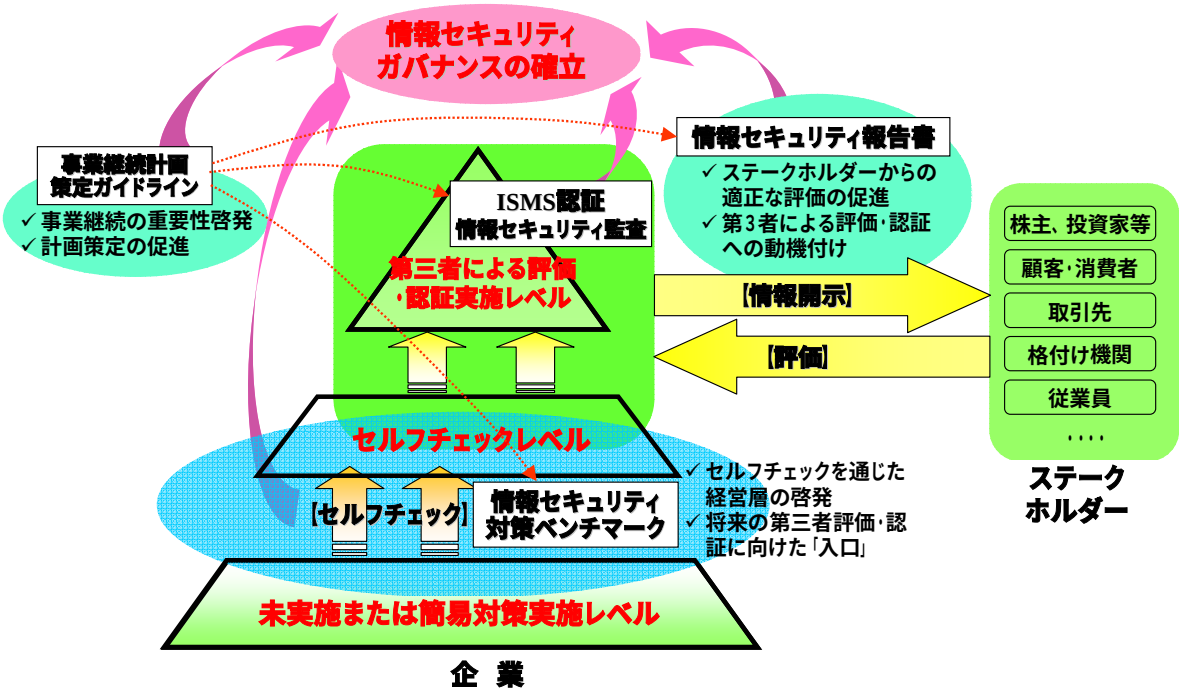
[19] 資金調達などのために、株式・社債等の発行体が株主・社債保有者等投資家に対し行う広報活動。

ークホルダーからの適正な評価を促す環境を整え、情報セキュリティガバナンスの自律的な確立を目指す。その際、セルフチェックレベルの企業が情報開示を通じて客観的な評価・認証の重要性を認識し、第三者による評価・認証の実施に着手する効果も期待できる。

さらに、事業継続は ISMS 認証や情報セキュリティ監査、情報セキュリティ対策ベンチマークにおいても言及される要素の一つであり、事業継続計画の策定は、そうした情報セキュリティ対策の強化に寄与する効果が期待される。加えて、計画の策定を情報セキュリティ報告書に記載することも考えられる。

これらの施策ツールと ISMS 認証等との基本的な関係を図 2-1 に示す。

図 2-1 施策ツールと ISMS 認証等との基本的関係



次章以降において、これらの施策ツールの概要について解説する。

３.情報セキュリティ対策ベンチマーク

３.１.概要

企業は、適正と考える水準、すなわち株主、消費者、取引先のみならず社会全体から「望まれる水準」において情報セキュリティに取り組むことが求められている。しかし、その水準は一様ではなく、企業の業態や保有する情報資産等の属性によって異なると考えられる。そこで、情報セキュリティ対策ベンチマークでは、これらの属性をもとに企業を分類し、それぞれの企業群に対して「望まれる水準」を提示することとした。

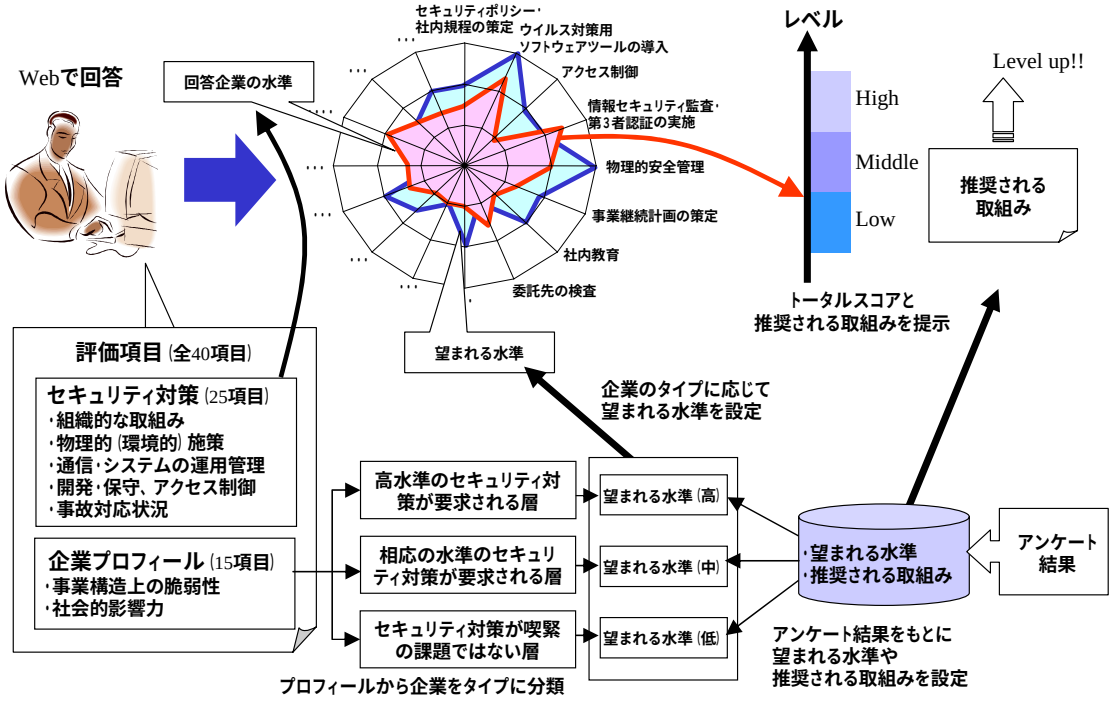
（１）情報セキュリティ対策ベンチマークの基本構成

情報セキュリティ対策ベンチマークの評価項目は、対策の取組状況を把握するための評価項目（25 項目）と、企業プロフィールに関する評価項目（15 項目）で構成される。

対策ベンチマークのシステムは、企業プロフィールに基づき回答企業を分類（分類の考え方は(2)参照）した上で、該当する企業群において「望まれる水準」を設定する。この「望まれる水準」とは、事前に実施した企業に対するアンケート（参考③参照）の結果をもとに、企業群ごとに導出したものである（16 頁及び参考①参照）。

また、対策の取組状況を把握するための評価項目に対する回答値から、企業のトータルスコアを算出し、回答企業の水準をレーダーチャート等で表示する（図　3-1 参照）。これは、回答企業の水準と望まれる水準を同時に提示し、その差分を可視化することにより、各社が優先的に取り組むべき項目を明確にするためである。さらに、推奨される取組みも併せて提示することにより、具体的な改善策実施へとつながるように促す。

図　3-1　情報セキュリティ対策ベンチマークのイメージ



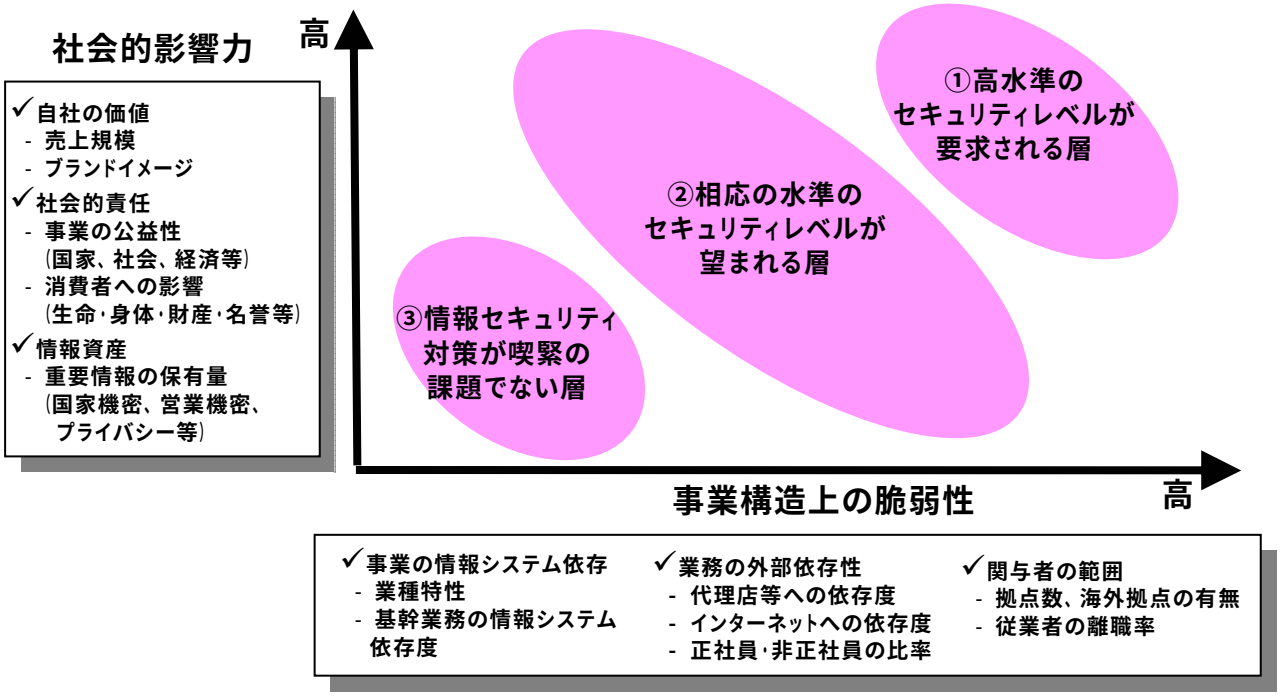
（2）企業分類

企業分類に際しては、「事業構造上の脆弱性」と「社会的影響力」に基づき企業群を分類する。「事業構造上の脆弱性」とは、事業の情報システム依存、業務の外部依存性、関与者の範囲などを考慮することによって、自社の情報資産がさらされている事業構造上の脆弱性の高さを評価するものと定義する。また、「社会的影響力」とは、自社の価値、社会的責任、保有する情報資産の性質などを考慮することによって、IT 事故が発生した場合に企業価値や社会に与える影響度の高さを評価するものと定義する。

具体的には、「事業構造上の脆弱性」、「社会的影響力」の２つを分類軸として、回答者の企業プロフィールの内容からこれらの値を算出し、いずれの値も高い層を「高水準のセキュリティレベルが要求される層」、いずれかの値が高い層を「相応の水準のセキュリティレベルが望まれる層」、いずれの値も低い層を「情報セキュリティ対策が喫緊の課題でない層」として、３グループに分類する（図　3-2 参照）。

なお、企業プロフィールの内容から「事業構造上の脆弱性」、「社会的影響力」を算出する計算式は、企業アンケートの結果の統計的分析（参考①参照）に基づき設定した。

図　3-2　要求される情報セキュリティの水準に基づく分類



３.２.位置付け

情報セキュリティ対策ベンチマークの目的として、情報セキュリティ対策を実施していない、あるいは簡易な対策しか行っていない企業に対し、セルフチェックを通じて情報セキュリティの取組みを活性化させることを想定しているが、こういった企業は、中堅・中

小企業が中心になると思われる。このため、中堅・中小企業における利活用を促進すべく、可能な限り評価項目の数を抑えている。なお、アンケート結果によれば、大企業にも、一部取組みが十分でない項目があることが判明している(参考③参照)ことから、中堅・中小企業のみならず、大企業も本ベンチマークを積極的に活用することが重要である。

今後は、さらに利用しやすくするためのツールの開発を行い、これを Web 上で公開して、企業によるセルフチェックを促していくことが望ましい。

また、第三者認証制度を始めとする高次のレベルを目指して向上していくことも重要であることから、ISMS 適合性評価制度[20]や情報セキュリティ監査との整合に配慮し、情報セキュリティ対策ベンチマークの評価項目は ISMS 認証基準（Ver.2.0）の詳細管理策[21]をベースに構成している。

なお、情報セキュリティガバナンスの確立という観点からすれば、情報セキュリティの実務担当者ではなく、経営層の担当責任者がセルフチェックを通じて対策の必要性に気づくことが望ましい。このため、経営層向けに平易な言葉を使用するとともに、単に対策を「行っている」／「行っていない」ではなく、ガバナンスの観点から見た対策の取組み方（成熟度）を評価の基準としている。

３.３.想定される効果

①経営層に対する目標の明確化と意識の啓発

自社の情報セキュリティの水準に不安を抱く企業の経営層が、本ベンチマークに基づくセルフチェックを通じて自社の現状と望まれる水準との差を把握し、目標を明確に理解することができる。企業にとっては、自社と同じタイプの企業群の取組状況に基づく指標が示されるため、実際の対策を検討する上で有用である。また、経営層が自らセルフチェックを行うことにより、自身に求められる役割を発見し、企業としての取組みのあるべき姿を理解するという啓発効果も期待できる。

②共通の尺度によるグループ内統制の実現

企業が株式の持ち合いや子会社・関連会社などと企業群を形成して事業活動を行っている場合、社会からはグループ全体としての一共同体とみなされるため、中核企業はグループ内企業に対する統制を確保し、グループ全体としての信頼性を確保する必要がある。そこで、グループの中核企業がグループ内各社のレベルを把握する共通の尺度として本ベンチマークを利用することにより、グループにおいて一定水準の情報セキュリティレベルの確保を確認することができる。

③受注者の信頼性の把握

---

[20] 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/）

[21] ISMS 評価基準の付属書であり、JIS X 5080：2002（国際標準 ISO/IEC 17799）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。

企業間の取引において、取引相手から本ベンチマークに基づくセルフチェックの結果の提出を受け、取引先の情報セキュリティレベルを確認することができる。例えば、個人情報保護法には委託先の監督義務が明記されているが、この観点から本ベンチマークの評価項目を利用して、委託先に対する評価を行うことも可能である。

④ISMS 認証取得等に向けた対策レベルの向上

情報セキュリティ対策の第三者認証取得を目指す企業が、まず本ベンチマークに基づくセルフチェックから始めて、それを繰り返し活用することで、徐々にレベルを上げていくことが可能となる。

ISMS の認証取得には、事前準備を含めて相応の取組みが必要であるが、本ベンチマークは ISMS 認証基準（Ver.2.0）の詳細管理策をベースに構成しているため、準備段階として有用である。

＜「望まれる水準」について（参考①参照）＞

企業の「望まれる水準」を設定する際の目安を明らかにするため、2005 年 1 月に企業約 6,000 社にアンケートを郵送し、1,633 件の回答を得た。

この 1,633 件のうち、すべての設問に回答した 885 件について「高水準のセキュリティレベルが要求される層」「相応のセキュリティレベルが望まれる層」「情報セキュリティ対策が喫緊の課題ではない層」に 3 分類した上で、対策の取組状況についてのトータルスコア（設問当たり最高 5 点で 125 点満点）を算出した。

このアンケートによって、以下のことが言える。

・各層のトータルスコアの平均を比較すると、要求されるセキュリティレベルが高い（さらされているリスクが高い）ほどトータルスコアの平均は高く、全体として対策が進んでいると言える。

・ただし、各層ともトータルスコアのばらつきは大きく、例えば、高水準のセキュリティレベルが要求される層の中にも、低いトータルスコアに留まる企業がある。

【望まれる水準】

以上のアンケート結果に加え、

①ISMS 認証を取得するに至るレベルは 4.0 であるが、部門別の ISMS 認証取得の場合は、企業全体として 3.0～4.0 の間に位置するのではないかと考えられること

②「情報セキュリティ対策が喫緊の課題ではない層」についても、「経営層の承認のもとに方針やルールを定め、全社的に周知・実施する(＝3.0)」のレベルを求めていくことが妥当と考えられること

③しかしながら、全体平均値を下回る企業が多数存在するため、直ちに①及び②のレベルを求めることは困難と考えられること

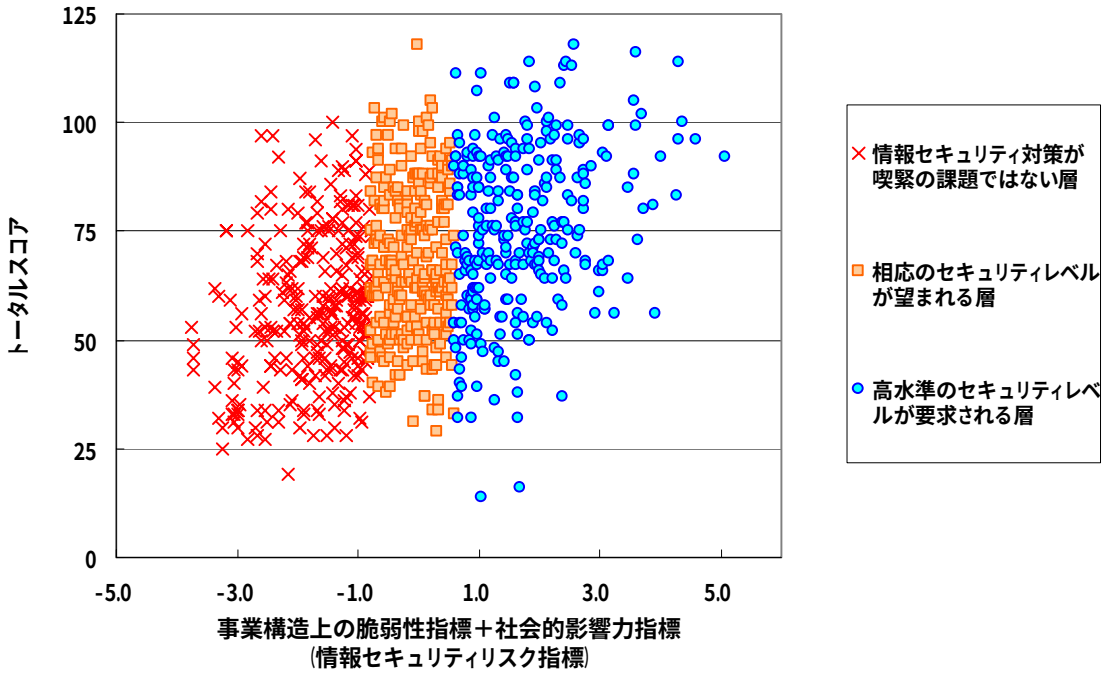
等を踏まえれば、

望まれる水準としては、「各層の上位１／３における平均値を目標としつつ、各層にお

ける全体平均値に達していない企業については、各層における全体平均値を、早期に達成すべき暫定的目標として設定する」ことが適当である。(具体的目標値については、下記参照)

ただし、この「望まれる水準」は、企業の業務内容・IT 依存度の変化といった内的要因だけではなく、社会全体のネットワーク化の更なる進展といった外的要因によっても変動していくものであることに十分な留意が必要である。

なお、「望まれる水準」の設定に当たっては、検討の過程で、「相対基準ではなく絶対基準が望ましい」との意見もあったが、情報セキュリティ対策が十分に進んでいない国内企業のレベル向上を目指すに当たり、絶対基準の設定が適当かは慎重な検討が必要であること、また、既に ISMS 認証基準のような絶対基準もあること等から、現段階で対策ベンチマークに係る絶対基準は設定しないこととした。この点については、利用者のニーズも踏まえ、対策ベンチマークの運用を担う機関を中心に、更なる検討を期待する（6.2①参照)。



	全体	高水準のｾｷｭﾘﾃｨﾚﾍﾞﾙが要求される層	相応のｾｷｭﾘﾃｨﾚﾍﾞﾙが望まれる層	情報ｾｷｭﾘﾃｨ対策が喫緊の課題ではない層
上位 1/3 の平均値	88(3.5)	96(3.8)	87(3.5)	76(3.1)
全体平均値	67(2.7)	75(3.0)	68(2.7)	57(2.3)

注：(　) 内の数値は、企業における取組みの成熟度に換算したもの。

４.情報セキュリティ報告書モデル

４.１.概要

情報セキュリティ報告書は、企業の情報セキュリティの取組み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、当該企業の取組み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である。

情報セキュリティ報告書モデルの基本構成を表 ４-１に示す(詳細は参考⑤参照)。なお、表 ４-１では、記載項目や内容のフルセットの例を提示しているが、企業はこれらの項目のうちから必要なものを選択できるものとする（4.2.参照)。

表 ４-１　情報セキュリティ報告書モデルの基本構成

①基礎情報

報告書の発行目的、利用上の注意、対象期間、責任部署等

②経営者の情報セキュリティに関する考え方

企業の情報セキュリティに関する取組み方針、対象範囲対象範囲、報告書におけるステークホルダーの位置付け、ステークホルダーに対するメッセージ等

③情報セキュリティガバナンス

情報セキュリティマネジメント体制（責任の所在、組織体制、コンプライアンス等)、情報セキュリティに関わるリスク、情報セキュリティ戦略等

④情報セキュリティ対策の計画、目標

アクションプラン、数値目標等

⑤情報セキュリティ対策の実績、評価

計画に対する実績、評価、事故報告等

⑥情報セキュリティに係る主要注力テーマ

個人情報保護や事業継続計画など特に強調したい取組み、テーマの紹介等

⑦第三者評価・認証

ISMS 適合性評価制度、情報セキュリティ監査、プライバシーマーク制度等

４.２.位置付け

情報セキュリティ報告書については、ステークホルダーへの説明責任遂行や新たな事業付加価値創出等、企業それぞれの目的に応じた策定を許容しつつ、企業にとって過度な負担を避けるという観点から、以下のように位置付ける。

・ 記載項目の選択や記載内容のレベルは、企業が自社の事情に応じて選択可能とする

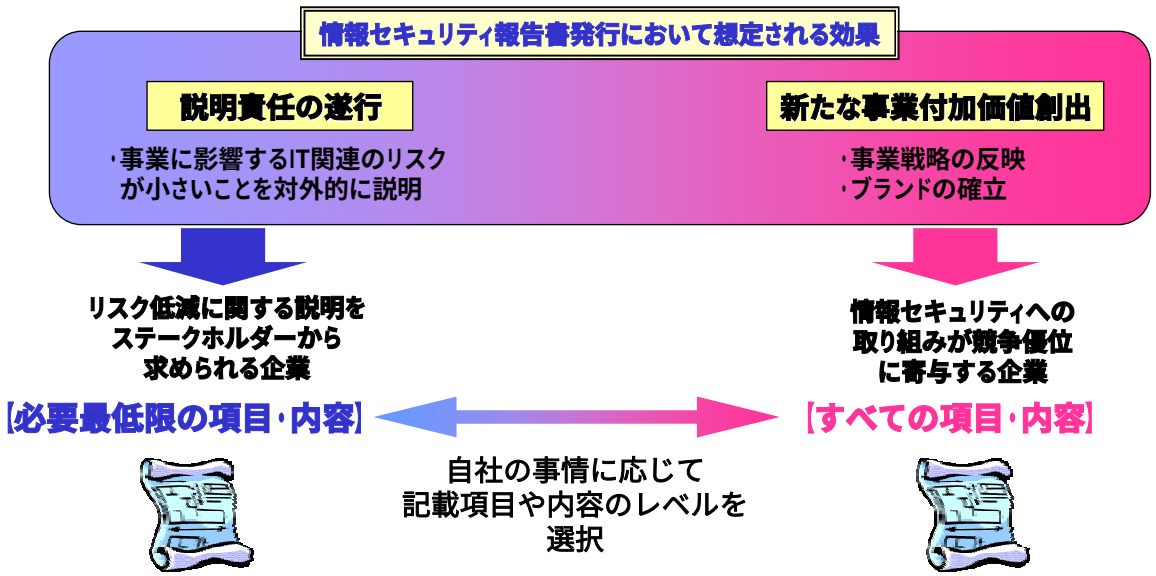
・ 情報開示の方法については、CSR 報告書等の一部として組み込むことも、単体の報告書として公表することも可能とする

4.3.想定される効果

（1）発行主体にとっての効果

情報セキュリティ報告書の発行主体にとって期待される効果としては、その立場やビジネスモデル等により図 4-1 のように想定される。

図 4-1 情報セキュリティ報告書発行において想定される効果



①説明責任の遂行

事業の IT 依存度が高まり、IT 事故が事業の存続すら脅かすリスクとなりつつある中、企業のステークホルダーは、今後 IT 事故に関するリスクに一層高い関心を示すものと見込まれる。このような状況の下、企業としては、情報セキュリティ報告書を通じて、当該リスクが小さいことをステークホルダーに対して説明していくこと等が、その発展のために重要となってくると考えられる。

特に、業界トップランナーと呼ばれる企業は、ステークホルダーからの信頼を獲得し、業界全体の健全な発展を先導するという立場から、情報セキュリティ報告書を率先して開示していくことが強く期待される。

②新たな事業価値の創出

主な商品やサービスが「IT」や「セキュリティ」に関連する企業や、収集した個人データをマーケティングなどに有効に活用する個人情報取扱事業者にとっては、提供する製品やサービスにおいてセキュリティを確保しておくことは当然のことながら、自社のセキュリティレベルの高さを対外的にアピールすることで、顧客からの支持を得て、企業価値の向上、競争優位の確保を狙うことができる。

このような効果を期待できる企業は、IT ベンダやセキュリティ関連企業、またネットビジネスやデータセンター等、ビジネスモデルが個人データや IT に強く依存している企業が想定される。

（2）ステークホルダーにとっての効果

情報セキュリティ報告書の読み手であるステークホルダーにとっての効果は、以下のように想定される。

①顧客・消費者　－　購買活動の判断

製品やサービスの購入者である顧客・消費者の最大の関心事の一つは、「顧客情報・個人情報の保護」である。情報流出事件を起こした企業には実際に売上げ減などの影響が見られることから、顧客・消費者は購買活動を判断するに当たって、企業の情報セキュリティ対策を重視する可能性があり、情報セキュリティ報告書による情報セキュリティの取組状況の開示は、こうしたニーズに合致するものと考えられる。

②取引先　－　取引相手の信頼性の把握

取引先は、調達等における相手企業の安定的な事業継続や情報管理の状況に対し高い関心を寄せており、取引条件として第三者認証の取得を求めるケースも見られる。したがって、情報セキュリティ報告書による情報セキュリティの取組状況の開示は、こうしたニーズに合致するものと考えられる。

③投資家、アナリスト　－　投資対象の評価

投資家やアナリストは、対象企業の業績や将来成長性を評価する上で、リスク情報やその対策に関する情報を活用する傾向がある。現在は、情報セキュリティの取組状況に対する投資家やアナリストの関心は必ずしも高くないが、今後、IT 事故による影響が拡大すると、そうした情報への関心が急速に高まる可能性がある。

④格付け機関　－　分析材料の充実

企業の格付けは、一般に公開資料、企業への面接、業界内の情報、取引先からの情報、カントリーリスク等を格付け機関が分析して行うもので、市場にも大きな影響力を持つ。IT リスクが経営に及ぼす影響が今以上に大きくなれば、将来的にリスクマネジメントの視点から格付け機関が情報セキュリティ関連の開示情報を積極的に活用する可能性がある。

⑤従業員　－　意識・理解の向上

情報セキュリティ報告書を開示することによって、従業員の情報セキュリティに対する意識･理解を高める効果が期待される。また、企業の情報セキュリティ担当者は、多くの場合、社内的に業績をアピールする機会に恵まれていないが、情報セキュリティ報告書の発行により、社内に対して自らの取組みをアピールすることが可能となり、業務へのモティベーションを高める効果が期待できる。

５.事業継続計画策定ガイドライン

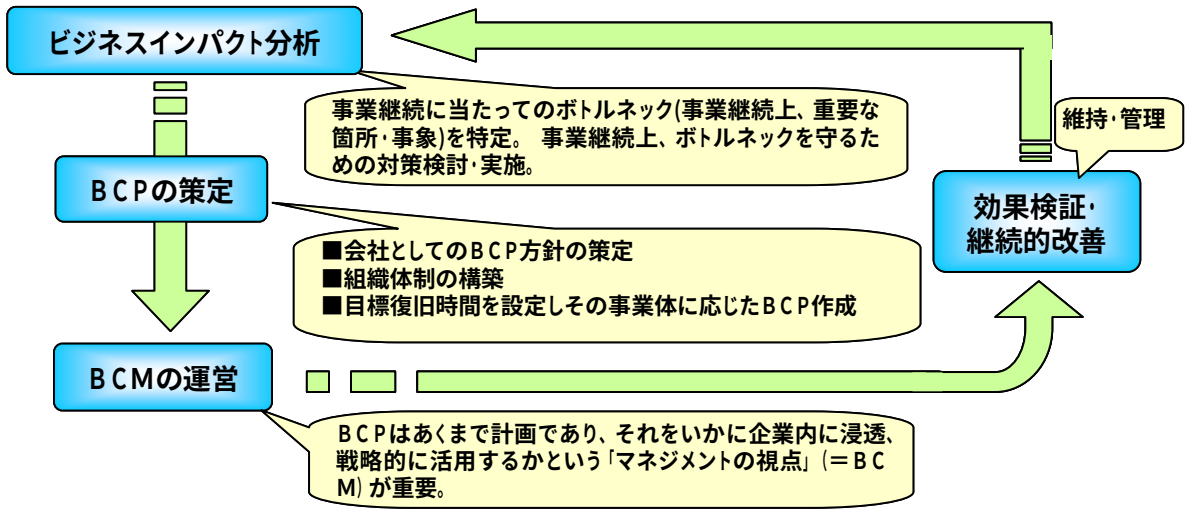
５.１.概要

本ガイドラインは、IT 事故を想定した事業継続計画（BCP）についての基本的考え方、総論、策定に当たっての検討項目、個別計画の４つの章と、参考資料から構成される（参考⑥参照）。BCP の構築を検討する企業にとって、考え方の理解を促すガイドラインという位置付けであり、基本的な考え方から具体的な計画の構築手順を説明するものである。参考資料やベストプラクティス事例などは、企業内での説明にも有用と考えられる。

①第Ⅰ章　基本的考え方

BCP の必要性や定義、一般的な構築の流れなどの概要を記載するとともに、BCP が求められる社会的背景やその特性、国内外の関連動向など、BCP の理解を深めるための基本的な説明を行う。阪神・淡路大震災やコンピュータ西暦 2000 年問題など過去の教訓やサプライチェーンマネジメント（SCM）との関係、諸外国の動向などについても説明を行う。

図　5-1　BCP の構築・運用の PDCA[22]サイクル



②第Ⅱ章　総論（フレームワーク）

Ⅰ章で紹介した BCP 構築と運用の一般的な流れについて、ステップ・バイ・ステップで説明し、BCP 策定プロジェクトの開始に当たって考慮すべき事項に言及する。BCP 策定に当たっての基礎分析となるビジネスインパクト分析や、組織体制、導入・教育、見直しなど、第Ⅰ章で示した BCP の構築・運用のサイクルについて詳細な説明を行う。

[22] 事業活動を「計画（Plan）」「実施（Do）」「監視（Check）」「改善（Action）」のマネジメントサイクルとして捉え、組織運営を通じて継続的な改善を図る取組み。

図 5-2　ビジネスインパクト分析

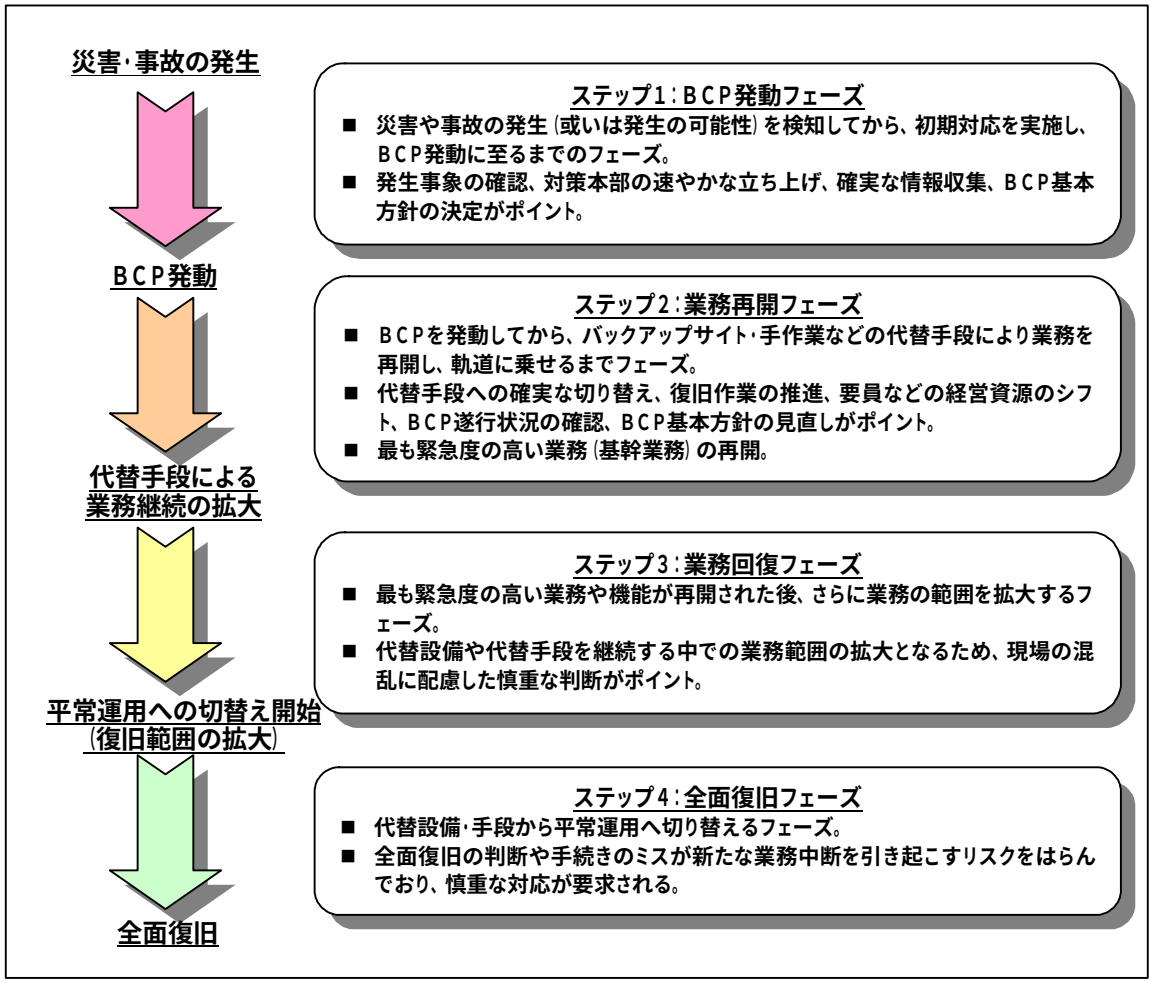
業務名			主管部署	関連部署	業務遂行上必要となるリソース				影響度分析結果			復旧優先度	RTO
区分	業務名	業務概要			業務遂行場所	利用システム名	必要人員数	その他必要資源	顧客影響度	収益資産影響度	社会的影響度		
管理	経営企画業務	経営計画の策定	経営企画部	－	本社	社内LANシステム（PC5台）	5名		3	3	1	低い	1W
管理	法務関連業務	監督官庁対応	総務部	－	総務別棟	－	3名	電話、FAX	2	3	1	中位	24H
システム	顧客照会業務	顧客情報の照会、DBメンテナンス	情報システム部	営業部	コンピュータセンター	顧客照会システム、顧客情報DB	本社2名、センター2名	－	5	4	5	高い	2H
：	：	：	：	：	：	：	：	：	：	：	：	：	：

③第III章　BCP 策定に当たっての検討項目

前章「Ⅱ　総論（フレームワーク）」のビジネスインパクト分析やリスク評価の結果を踏まえて構築された BCP について、実際の展開場面をイメージしながら策定に当たっての検討項目を記載したものである。

具体的には、情報システムを対象とした事故や災害の発生を想定し、BCP の基本的な項目について、BCP の発動から全面復旧に至るまでの各フェーズにおけるポイントを例示的に挙げている。

図 5-3　BCP の実施手順



④第Ⅳ章　個別計画（ケーススタディ）

企業を取り巻く災害・障害は多様であり、またその対応手順についても各企業で異なるのが自然である。本章においては、第Ⅲ章の基本的な対応手順に沿って、以下の３つのケースにおける具体的対応手順につき、それぞれの障害の特徴や考慮事項を説明する。

１．大規模なシステム障害への対応
２．セキュリティインシデントへの対応
３．情報漏えい、データ改ざんへの対応

⑤参考資料集（ベストプラクティス事例集等）

BCP 構築に当たり、企業がより具体的な導入のイメージを把握できるよう他社のベストプラクティス（構築事例）や、参考資料などを記載する。

５．２．位置付け

本ガイドラインは、BCP の重要性や基本的な考え方、要点等を紹介するとともに、計画の具体的イメージでは IT 事故を想定し、情報システムや IT 部門の観点から検討すべき事項を紹介するものである。

例えば、本ガイドラインにおいて、BCP 発動の契機となるダメージとしては、以下のケースが想定される。

①地震等による大規模なシステム障害
②システムセンター被災
③停電、通信回線事故
④ウイルス感染、社内ネットワーク障害などのセキュリティインシデント
⑤情報の漏えい（営業秘密情報、個人情報等）、データ改ざん

なお、内閣府中央防災会議では、「民間と市場の力を活かした防災力向上に関する専門調査会」[23]の企業評価・業務継続 WG において、自然災害を主な対象リスクとする BCP ガイドラインの検討が進められているが、このガイドラインと本ガイドラインは相互に補完する関係になるものと考えられる。

５．３．想定される効果

①事業活動の変化への対応

企業は、現在、効率化を追求し徹底的なコスト削減を行うため、生産拠点や物流拠点、取引先等を集約する方向にある。このことは一方で、その拠点や取引先に障害が発生した場合、代替拠点や取引先の手配を困難にし、基幹事業の停止に直結する確率が増加していることを意味する。こうした事業活動の変化を踏まえた上で、事業活動上のリスクや、その事業に与えるインパクトについて分析して対応策を準備しておくことは、企業価値を守るだけでなく、企業価値の向上につながるものである。

②信頼性確保による競争優位

BCP による事業継続性確保のための方策は、短期的に見てコスト要因になる。しかしながら中長期的に見れば、顧客やビジネスパートナーの信頼を得ることとなり、他社と比較して競争優位性を確保することができる。

③取引先からの要請への対応

産業構造の変革と企業活動のグローバル化により、企業は、事業活動を行う上で国内外の企業へのアウトソーシングを行い、高度なサプライチェーンを構築している。サプライチェーンでは相互依存性が高く、このうちの一企業が事業中断した場合でも連鎖的に多く

[23]内閣府中央防災会議「民間と市場の力を活かした防災力向上に関する専門調査会」
http://www.bousai.go.jp/MinkanToShijyou/

の企業に様々な影響が及ぶことから、事業継続性の確保のため、取引先からＢＣＰ策定を求められることがある。

特に日本企業が海外企業のサプライチェーン上の重要な要素となっている場合には、今後、事業継続性確保に係る意識が高い海外の企業から日本企業に対して、地震をはじめとする様々なリスクに対する BCP を求めてくることが想定される。

６.各主体に求められる取組み

情報セキュリティガバナンスの確立を促進するためには、ISMS 認証や情報セキュリティ監査へとつながる「入口」としての情報セキュリティ対策ベンチマーク、企業の情報セキュリティへの取組みを開示し透明性を高めることでステークホルダーによる評価を促す情報セキュリティ報告書モデル、IT 事故に対する企業の回復力を高める事業継続計画策定ガイドラインの各ツールが多様な企業活動の場面で有効に活用されるよう、関係者が様々な形で取組みを進める必要がある。

すなわち、これらのツールを直接活用する立場の企業において積極的な取組みが望まれるとともに、こうした取組みを支援・促進する環境を関係機関・業界及び政府が整えていくことが望まれる。

以下に、企業、関係機関・業界及び政府に求められるこれらの取組みを提言する。

６.１.企業に求められる取組み

企業には、情報セキュリティガバナンスの確立に向けて、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、事業継続計画策定ガイドラインの積極的な活用が望まれる。

①情報セキュリティ対策ベンチマークの活用

情報セキュリティガバナンスの確立に寄与する ISMS 認証取得や情報セキュリティ監査の実施を目指しつつ、まず、企業には「望まれる水準」達成に向け、情報セキュリティ対策ベンチマークのセルフチェックへの積極的な活用が望まれる。また、3.3 に例示したように、企業には、自社の現状把握や取引先の信頼性の確認等を含む様々な形で情報セキュリティ対策ベンチマークを活用することも望まれる。例えば、商取引の場面において、取引先の信頼性を評価する一つの材料として、情報セキュリティ対策ベンチマークを活用することが考えられる。特に、調達する製品・サービスが情報セキュリティの観点を必要とするものであれば（例：メンテナンスを含む IT 製品の調達、重要情報の取扱業務委託等）、発注者側に、納入者・受託者の信頼性について評価するニーズがあるものと推測される。

②情報セキュリティ報告書の発行

ステークホルダーによる適正な企業評価により情報セキュリティガバナンスの自律的な確立を促すため、企業には、情報セキュリティ報告書の発行が望まれる。具体的には、単体の報告書や CSR 報告書などの情報開示ツールを通じて、情報セキュリティ報告書モデルの記載項目を反映した情報開示に取組み、ステークホルダーに説明責任を果たしていくこと等が考えられる。特に、各業界のトップランナー企業や、セキュリティで競争優位を狙う IT ベンダ、セキュリティ関連企業、ネットビジネス、データセンター等の企業による積極的な取組みが期待される。

さらに、そうした開示情報について広くステークホルダーに知らしめるために、説明会

等を開催したり、情報セキュリティ報告書の収集・開示を行う機関（6.2 参照）に報告することも考えられる。

③IT 事故を想定した BCP の策定

企業の IT 事故に対する回復力を高め、情報セキュリティガバナンスの確立を目指すため、企業には、事業継続計画策定ガイドラインを踏まえ、自社の BCP 策定に取り組むことが望まれる。さらに、最近では、取引先が相手企業の BCP の有無を確認する動きが顕在化していることから、BCP の整備状況が受注に影響する可能性も考慮し、特に、IT 依存度が高い企業には、当ガイドラインを活用し、IT 事故に適切に備えておくことが有益と考えられる。

④企業グループセキュリティの実現

近年の企業セキュリティにおいては、企業グループ全体としてのセキュリティをどのように維持するかという問題が顕在化している。同一グループであっても、グループ内の個々の企業の事業構造上の脆弱性や社会的影響力が異なるケースが数多く存在しており、一義的に対応策を定めることは困難である。このため、本報告書が策定した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等も活用しつつ、グループ内への内部統制とグループ外への情報開示を効率的・効果的に進めていくための検討を、各企業グループにおいて、それぞれの状況を勘案しつつ進めていくことが望まれる。

６.２.関係機関・業界に求められる取組み

関係機関・業界には、施策ツールの開発・維持・改善、リスク定量化ツールの提供などを通じて、企業の情報セキュリティガバナンスに向けた取組みを支援・促進していくことが望まれる。

①施策ツールの開発・維持・改善

今回提示した各施策ツール（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）については、セルフチェックのための Web サイトの構築・運用を含む普及促進活動、普及状況の把握も含めたフォローアップ、アンケート等による指標データの定期的な更新、内容の改訂や対策ベンチマークにおける絶対基準の導入可能性に係る検討といった実務レベルの運用業務が発生することから、これら業務を適切な関係機関が実施することが望まれる。

②セルフチェックと連動するリスク定量化ツールの提供

企業においては、自社の情報セキュリティの水準や取組みが不足している分野を明らかにするだけでなく、その取組みの要否を判断するための参考情報が求められる。そこで、情報セキュリティ対策ベンチマークのセルフチェックツールと連動して、その企業がどれだけの情報セキュリティリスクを抱えているかを定量的に示すツール（リスク定量化ツール：参考④参照）を適切な関係機関において開発し、情報セキュリティ対策ベンチマーク

を公開するサイトにおいて提供することが望まれる。

③損害保険に係る評価・料率算定への適用

損害保険業界には、情報セキュリティ対策ベンチマークを活用して損害保険に加入を希望する企業の情報セキュリティ対策の状況を評価し、その水準に応じて損害保険の料率を調整する取組みが望まれる。このような対策ベンチマークの活用は、共通の評価尺度に基づくデータ収集につながり、企業の情報セキュリティ水準をより合理的・客観的に評価できることによって、保険引受(アンダーライティング）上のリスクを軽減できるという点で損保業界にとってもメリットがあると考えられる。

また、リスク評価に当たって、情報セキュリティ報告書の内容や BCP の策定状況を参考とすることも考えられる。

④情報セキュリティ報告書の発行事例の収集･開示

情報セキュリティ報告書（単体の報告書だけでなく、CSR 報告書の一部として記載するケースを含む）の発行事例を関係機関が収集・開示する等、発行企業の取組みをステークホルダーに広く知らしめる取組みが望まれる。例えば、情報セキュリティ報告書の普及促進を担う関係機関が、自身の調査や発行企業からの届出をもとに情報セキュリティ報告書の事例を集約・整理し、Web サイトなどを通じてその情報を公開する形が考えられる。

こうした取組みを通じて、個人投資家や消費者、取引先等のステークホルダー、さらに発行主体である企業自身が各社の情報セキュリティへの取組状況に関する開示情報を比較するようになり、それによって積極的に情報開示に取り組む企業が高く評価されるようになることが期待される。

⑤第三者機関による情報セキュリティ報告書格付け

将来的には、評価専門機関やマスコミ、非営利活動団体（NPO）等の第三者機関が、独自の視点・評価軸を持って情報セキュリティ報告書を評価し、その結果を格付けの形で公表することにより、ステークホルダーの関心が高まり、発行企業側も格付け向上に向けてさらに努力するという展開が期待される。

例えば、環境報告書の場合、株式会社トーマツ審査評価機構や日本格付研究所等の評価専門機関、日本経済新聞社やダウ･ジョーンズ社等のマスコミ、環境経営学会等の NPO が格付けを行っている他、日本政策投資銀行でも「環境配慮型企業活動支援事業」において、環境への配慮に対する取組み度合いを環境格付けし、ランクに応じて適用金利を適用している。

⑥情報セキュリティ報告書に関する表彰制度の整備

情報セキュリティ報告書の発行やその内容の充実を促進するため、そうした取組みに積極的な企業を表彰する制度を整備することが考えられる。例えば、情報セキュリティ報告書の普及促進を担う関係機関が、その年に発行された情報セキュリティ報告書（単体の報告書だけでなく、CSR 報告書の一部として記載するケースを含む）を審査し、何らかの賞を設定して表彰することもあり得る。例としては、上場会社のディスクロージャーの充実

を促進する観点から、その内容のわかりやすさも含め、ディスクロージャーに積極的に取り組んでいると認められる会社を表彰する東京証券取引所の「ディスクロージャー表彰制度」、優れた IR 活動を実施している企業を会員企業の中から選定し発表する日本インベスター・リレーションズ（IR）協議会の「IR 優良企業賞」、企業情報開示の向上を目的とした日本証券アナリスト協会企業の「リサーチ・アナリストによるディスクロージャー優良企業選定」制度が挙げられる。

⑦関係機関・関係者による啓発

企業が、ビジネスプロセス上の多様な場面で情報セキュリティ対策ベンチマークを活用し、情報セキュリティ報告書の発行や BCP の策定に取り組むように、各種業界団体を含む関係機関、IT コーディネーター等を通じて、企業の啓発を進めることが望まれる。その場合、セミナー等による啓発活動だけでなく、情報セキュリティガバナンスの確立に不可欠な人材の育成についても、企業との連携の下、積極的に取組みがなされることが期待される。例えば、企業の CIO（Chief Information Officer）／CISO（Chief Information Security Officer）のための人材や、情報セキュリティガバナンスの整備状況を客観的に評価・保証するための人材（ISMS 認証、情報セキュリティ監査等を含む）が各方面で求められると予想される。

⑧国際標準化への対応

ISO（国際標準化機構）では CSR ガイドラインの策定が決定しており、2005 年からその活動が本格化する。また、BCP についても、英国規格協会（BSI：British Standards Institution）が「PASS56」を、米国標準協会（ANSI：American National Standard Institute）が「NFPA-1600」をベースとして国際標準化を進めると予想される。こうした動きを踏まえ､我が国として情報セキュリティの文脈から貢献すべき部分があるか､また､どのように対応していくべきかを産業界を中心に検討していくことが望まれる。

６.３.政府に求められる取組み

政府には、必要に応じて関係機関・業界における取組を支援しつつ、施策ツールの政府調達への活用などを通じて、企業の情報セキュリティガバナンスに向けた取組みを支援・促進していくことが望まれる。

①情報セキュリティ対策ベンチマーク等の政府調達への活用

政府機関等には、調達における応札者の信頼性を評価する指標として、情報セキュリティ対策ベンチマークを活用することが望まれる。例えば、応札企業に、情報セキュリティ対策ベンチマークによるセルフチェックデータの提出を要求し、一定の目標値を示して、入札企業のセルフチェックデータが目標に到達もしくはそれに近いほど加点する構造を採り、信頼性の高い企業にメリットのある形とすることが考えられる。さらに、その際の評価対象は受託主体だけでなく再委託先等も含めた形で行うこと、情報セキュリティ報告書が発行されている場合には加点すること、必要に応じて調達元の政府機関等が応札企業に

おける対策実施状況を確認することなどによって、より強い効果を持たせることが望まれる。

このような政府調達への適用は、入札企業への情報セキュリティ対策を促進するだけでなく、将来的に民間企業間の受発注時の適用に波及する効果も期待できる。

②内閣府中央防災会議の事業継続計画策定ガイドラインとの連携

内閣府中央防災会議においても企業の防災に係る観点から、事業継続計画策定ガイドラインの検討作業に着手している。当該ガイドラインが対象とする事象はより広範な災害とそれに伴う事業継続の危機的状況であることから、本研究会で取りまとめた事業継続計画策定ガイドラインは、中央防災会議のガイドラインの一部を詳細化等した位置づけとなるものと考えられる。両ガイドラインが相互に補完し、整合的に BCP に係る取組を促進していくことを通じて、企業における防災担当者と情報システム担当者の協力・連携を醸成し、真の意味で企業における BCP の実装が進展していくことが期待される。

「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」委員名簿

【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　副学長

【委員】

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	IBM ビジネスコンサルティングサービス株式会社 チーフ・セキュリティ・オフィサー（CSO）
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
小林　一彦	社団法人電子情報技術産業協会　情報システム部会長 （日本電気株式会社　取締役　執行役員常務）
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
棚橋　康郎	社団法人日本経済団体連合会　情報化部会長 （新日鉄ソリューションズ株式会社　代表取締役会長）
中村　直司	社団法人情報サービス産業協会　副会長 （株式会社エヌ・ティ・ティ・データ　代表取締役副社長）
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
松尾　明	中央青山監査法人　代表社員　公認会計士
望月　純	社団法人日本損害保険協会　情報システム委員会 委員長 （株式会社損害保険ジャパン　執行役員兼事務・IT 企画部長）

「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

【主査】

大木　栄二郎　IBM ビジネスコンサルティングサービス株式会社　チーフ・セキュリティ・オフィサー（CSO）

【委員】

大久保　和孝　新日本インテグリティアシュアランス株式会社　取締役

加賀谷　哲之　一橋大学大学院　商学研究科　助教授

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

重松　孝明　電子商取引推進協議会（ECOM）　主席研究員

清水　恵子　監査法人中央青山監査法人　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

長嶋　潔　東京海上日動火災保険株式会社　情報産業部　e-リスクプロジェクトリーダー

保科　剛　日本ユニシス株式会社　最高技術責任者　兼　ビジネスイノベーション本部　副本部長

松尾　正浩　株式会社三菱総合研究所　情報環境研究本部　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　ISO マネジメント事業部　課長

【オブザーバ】

大西　富美子　ソフトバンク株式会社 グループ情報セキュリティ対策室 マネージャー

「事業継続計画策定ガイドラインワーキンググループ」委員名簿

【主査】

喜入　博　KPMG ビジネスアシュアランス株式会社　常勤顧問

【委員】

太田　岳志　株式会社損害保険ジャパン　情報通信産業室　企画グループ　課長代理

小林　偉昭　株式会社日立製作所　情報･通信グループ　セキュリティソリューション推進本部　統括主査

篠原　雅道　株式会社インターリスク総研　総合リスクマネジメント部　上席コンサルタント

近森　健三　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　主任研究員

堀越　繁明　KPMG ビジネスアシュアランス株式会社　シニアマネージャー

【オブザーバ】

渡辺　研司　長岡技術科学大学工学部経営情報系　助教授

活動記録

【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】

2004 年９月１日	第１回会合	論点整理について
2004 年 12 月８日	第２回会合	ワーキンググループの検討状況について
2005 年２月 21 日	第３回会合	報告書（案）について
2005 年３月 25 日	第４回会合	報告書のとりまとめについて

【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】

2004 年９月 13 日	第１回会合	目標・活動方針の意識合わせについて
2004 年 10 月 13 日	第２回会合	アウトプットの考え方、論点について
2004 年 11 月１日	第３回会合	アウトプットイメージについて
2004 年 12 月１日	第４回会合	研究会向け報告案について
2004 年 12 月 15 日	第５回会合	アンケートについて
2005 年１月 26 日	第６回会合	成果物のとりまとめについて
2005 年２月２日	第７回会合	成果物のとりまとめについて
2005 年３月 15 日	第８回会合	成果物のとりまとめについて

【事業継続計画策定ガイドラインワーキンググループ】

2004 年 9 月 17 日	第１回会合	目標、活動方針の意識合わせについて
2004 年 10 月 5 日	第２回会合	基本構成案の検討について
2004 年 11 月 18 日	第３回会合	詳細構成案の検討について
2005 年１月 24 日	第４回会合	ガイドライン案について
2005 年３月 15 日	第５回会合	ガイドライン案について