

# 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(概要)

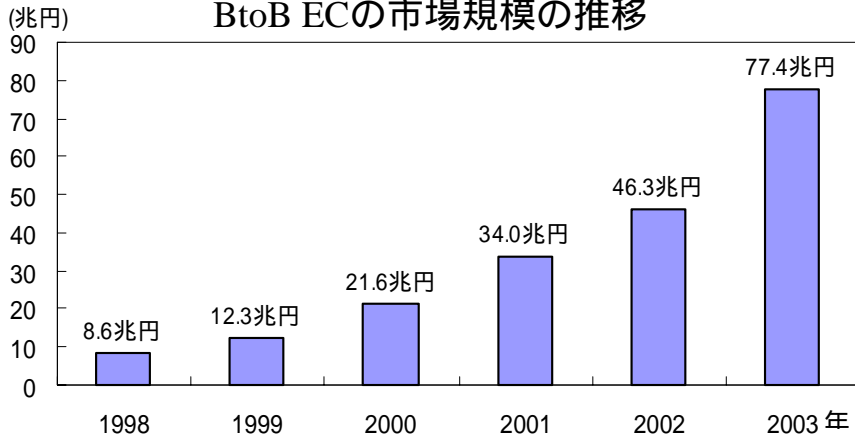
2005年3月

経済産業省 商務情報政策局  
情報セキュリティ政策室

# 1.1 背景～社会の「神経系」となったIT

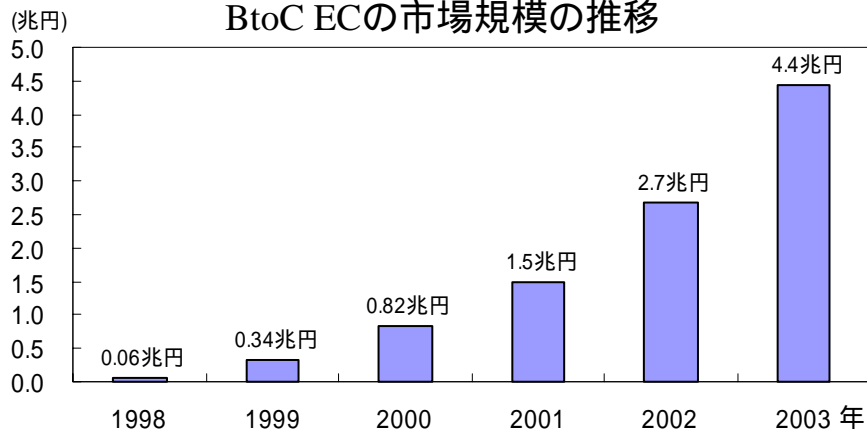
- 電子商取引（EC）市場は着実に拡大、経済分野におけるIT依存の高まりが顕在化。
- さらに、ITの組織的な利活用が企業業績にも影響を及ぼす傾向。現在は個別部門ごとの効率化を図る企業（ステージ2）が大半だが、企業組織全体のプロセスの最適化（ステージ3）や、複数の企業で構成するバリューチェーンの最適化（ステージ4）へと進化を遂げた企業も存在。

BtoB ECの市場規模の推移

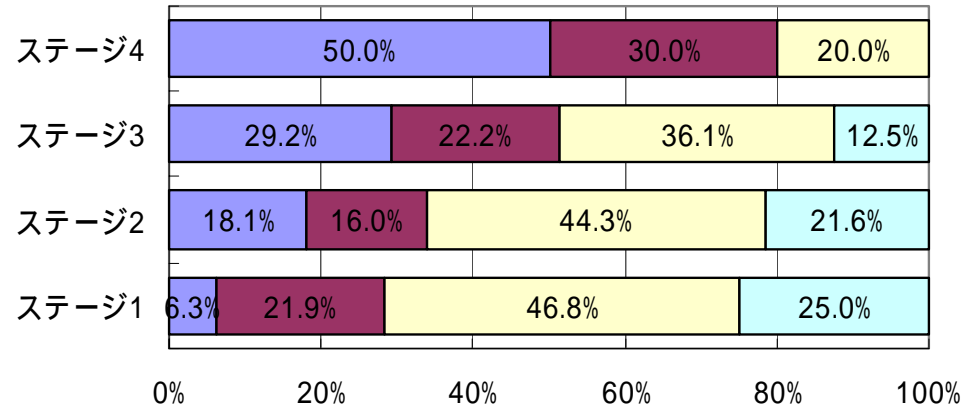


注：1999年はBtoB EC調査を行っていないため、1998年調査における予測値を使用。

BtoC ECの市場規模の推移



情報技術の利活用度と企業業績の見通し



n=436  
■ 上向き ■ 上向きだが将来は不透明 ■ 横ばい ■ 悪化

- 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7日）

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11日）

# 1.2 現状認識(1) ~ IT事故の影響の増大

- ▶ 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。
- ▶ 情報流出事案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。
- ▶ さらに、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。

\*) 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。

## IT事故による情報流出事例

## IT事故が及ぼす社会的影響の事例

大手 通信事業者 A	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 全会員を対象にお詫び料として1人当たり500円を支給。事件関連で2004年3月期に総額31億円を特別損失として計上。</li> <li>• 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。</li> </ul>
大手 流通業者 B	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
大手 メーカー C	<ul style="list-style-type: none"> <li>• 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C社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男からC社へ買い取り要求があったことから事件が判明。</li> <li>• 一部の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社側の費用負担で実施することで合意。</li> </ul>

航空	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 欠航215便、大幅な遅延1500便以上、約30万人の利用者に影響。</li> <li>• 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。</li> </ul>
金融	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
医療	<ul style="list-style-type: none"> <li>• 2004年3月、大学病院内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。</li> <li>• 外来患者は1日平均4,000人、ピーク時は1,400人/h。</li> </ul>

## コンプライアンスとCSR (Corporate Social Responsibility : 企業の社会的責任)

- ▶ 平成17年4月1日の個人情報保護法全面施行により、個人情報取扱事業者に課せられる「安全管理措置」義務について、企業は早急な対応を求められている。
- ▶ 法令に基づく情報開示として 有価証券報告書におけるリスク情報の記載（証券取引法）、金融業界のディスクロージャー誌におけるリスク管理体制の記載（事業法）がある。
- ▶ 社団法人日本経済団体連合会「企業行動憲章」では「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。
- ▶ 企業のCSRに係る取組みを開示するCSR報告書でも、情報セキュリティ対策の方針や実施状況を採り上げる事例が出てきている。

### 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)

#### 〈抜粋〉

#### (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。

### 企業行動憲章(抜粋)

企業は、公正な競争を通じて利潤を追求するという経済的主体であると同時に、広く社会にとって有用な存在でなければならない。そのため企業は、次の10原則に基づき、国の内外を問わず、人権を尊重し、関係法令、国際ルールおよびその精神を遵守するとともに、社会的良識をもって、持続可能な社会の創造に向けて自主的に行動する。

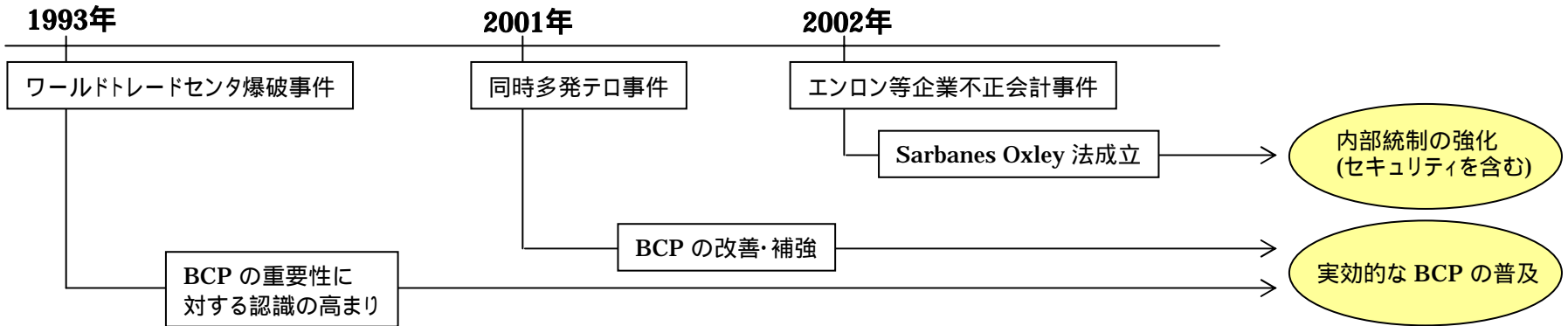
#### (以下抜粋)

- 1.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。
- 3.株主はもとより、広く社会とのコミュニケーションを行い、企業情報を積極的かつ公正に開示する。

出所：(社)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」  
(2004年5月18日改定)

## 米国では企業の不正行為やテロへの対策が情報セキュリティにも波及

- 米国では、不正会計事件を契機としたコーポレートガバナンスに対する法的規制の強化が、情報セキュリティ対策の取り組みにも影響。
- 事業継続計画 (BCP) についても、2001年のテロ事件を契機に改善・補強する方向へ。



### ◆ Sarbanes-Oxley 法 (2002年7月成立)

CEO および CFO が内部監査の結果について責任を負うことを規定し、コーポレートガバナンスの徹底を明確化した法律。情報セキュリティ対策の徹底について直接言及はしていないが、法律に準拠するためには情報セキュリティ対策が必須となる。IT との関連性が高いのは Section 404 であり、CEO・CFO・監査官に対して、会計報告書の作成プロセスが正確であることおよび一般的基準を満たすことを保証しなければならないと規定している。これによって企業は、会計報告書の作成に関わる全ての情報システムについて、法律が規定する基準を満たす事を保証しなければならないため、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ることになる。

### ◆ その他のセキュリティ関連の法律

米国では、あらゆる業種を対象とした情報システムのセキュリティ強化を規定する法律は存在しないが、金融機関や医療保険業界といった特定の業界を対象として、情報セキュリティの強化を規定する法律が存在する。

➤ 金融業界 : Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA)

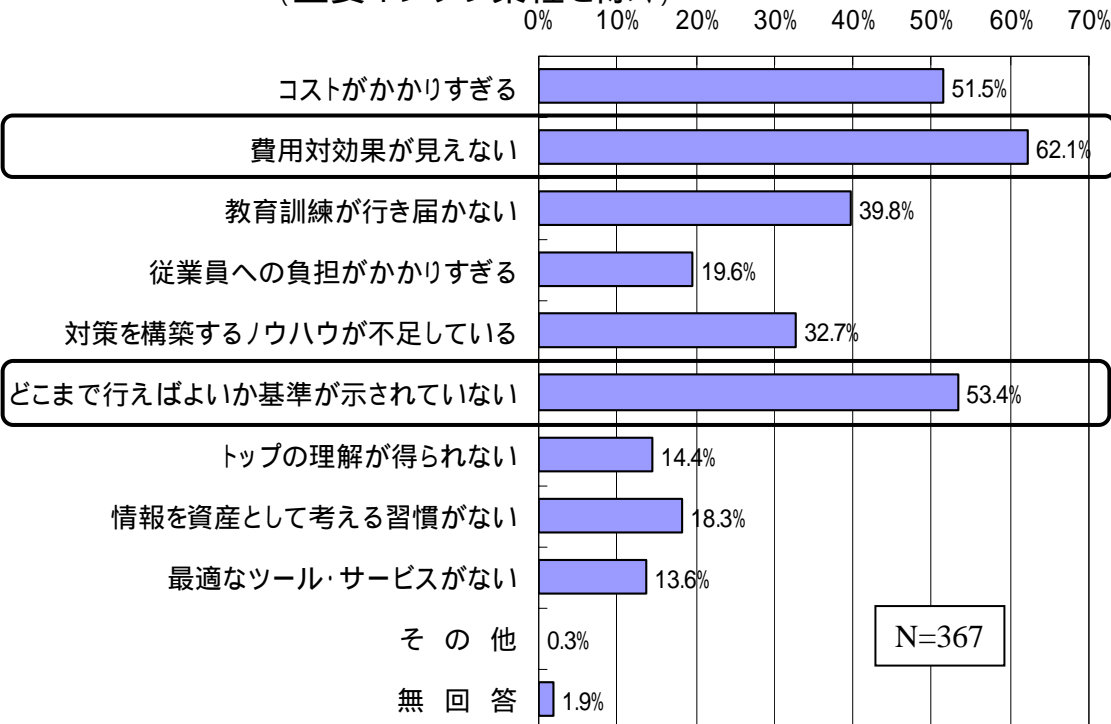
金融機関に対し、包括的セキュリティプログラムの策定やセキュリティ対策の実施を義務づけ。

➤ 医療保険業界 : Health Insurance Portability and Accountability Act of 1996 (HIPAA)

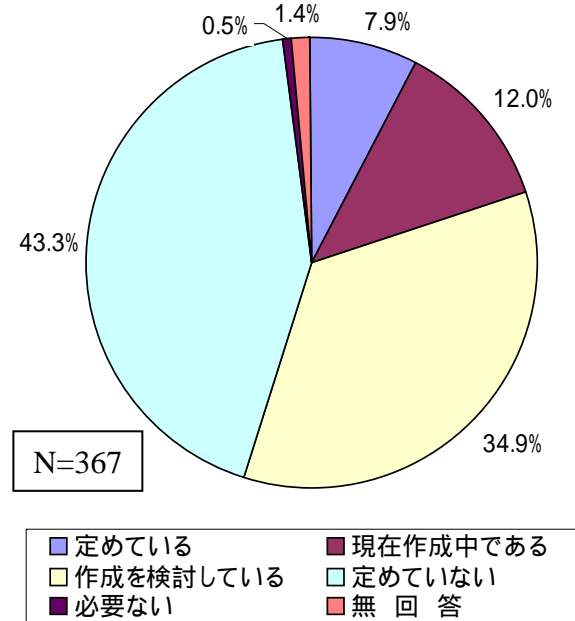
個人の電子的な医療情報に対するセキュリティ対策の実施や電子署名の使用等包括的なセキュリティ対策の実施を義務付け。

- ▶ 我が国企業が情報セキュリティ投資を行う上で障害と感じる主な要因は、費用対効果が見えない(62.1%)  
どこまで行えばよいか基準が示されていない(53.4%)
- ▶ 我が国企業の緊急事態対応計画は、策定済が7.9%、現在作成中が12.0%にとどまる。
- ▶ IT事故の発生可能性を無くすことはできない以上、企業は本来、IT事故発生時の被害局限化と早期復旧が重要であり、そのための事業継続計画(BCP)を策定すべき。

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)



大手・中堅企業における緊急事態対応計画の策定状況(重要インフラ業種を除く)



米KPMG「KPMG 2002 BUSINESS CONTINUITY STUDY」の調査(2002年)によると、米国では、BCP策定済の企業は67%、策定中の企業は29%であり、未対応企業は4%に過ぎない。

## 企業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社会では、企業<sup>\*1</sup>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。したがって、企業の情報セキュリティ確保は、自身の被害<sup>\*2</sup>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のではないか。
- ▶ 政府の果たすべき役割は、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す環境の整備を支援することにあるのではないか。

## 情報セキュリティガバナンスの必要性

- ▶ 企業が、上記の「あるべき姿」に向かうためには、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。
- ▶ 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。
- ▶ 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。

### 「情報セキュリティガバナンス」の確立

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

### 政府の役割

企業の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す環境の整備支援

### 企業のあるべき姿

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

OECDガイドライン  
「セキュリティ文化」

情報セキュリティ総合戦略  
「世界最高水準の『高信頼性社会』」

- \*1) 検討対象は主に情報システムの「ユーザ企業」。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。
- \*2) 株主等の損害も含む。

問題

**(1) IT事故発生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**

✓ **投資判断のための指標**が求められているのではないか。

**(2) 既存の情報セキュリティへの「対策」「取組」が企業価値に直結していない**

✓ 情報セキュリティに係る取組みが、**企業価値向上**に寄与する仕組みが必要ではないか。

**(3) 事業継続性確保の必要性が十分に認識されていない**

✓ IT事故発生時の対応手続きを**事業継続の観点**から定めておくことが必要ではないか。

## 問題点を克服し、企業が情報セキュリティガバナンスの確立を促進するツール

### 情報セキュリティ対策ベンチマーク

- 情報セキュリティ対策のセルフチェック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

### 企業・社会への普及方策

- ・情報セキュリティ格付け
- ・政府調達への活用
- ・損害保険との連携 等

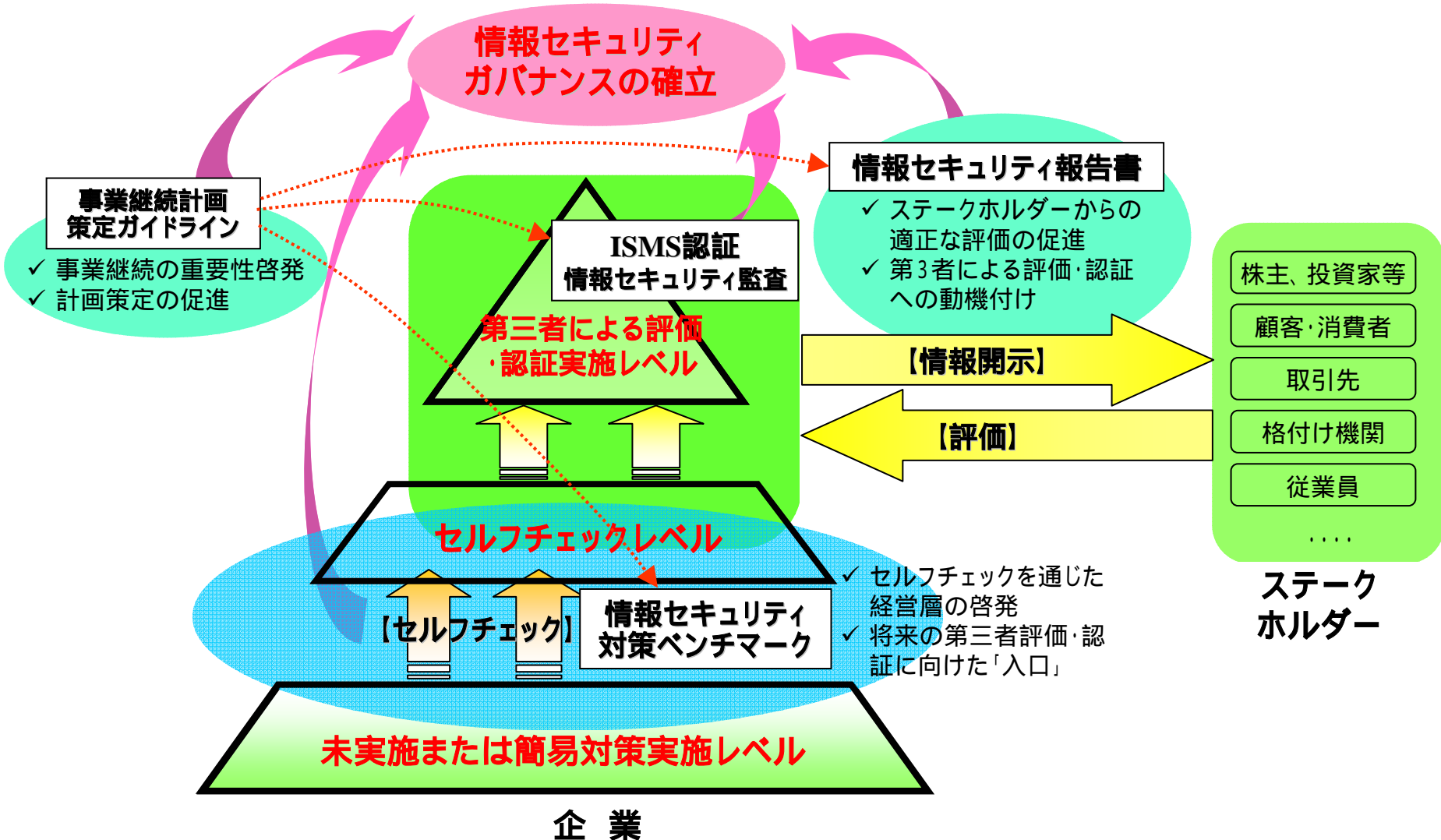
### 既存施策との連携

- ・ISMS認証や情報セキュリティ監査の「入口」としての活用
- (セルフチェック 第三者認証・評価へ) 等

**企業における情報セキュリティガバナンスの確立**

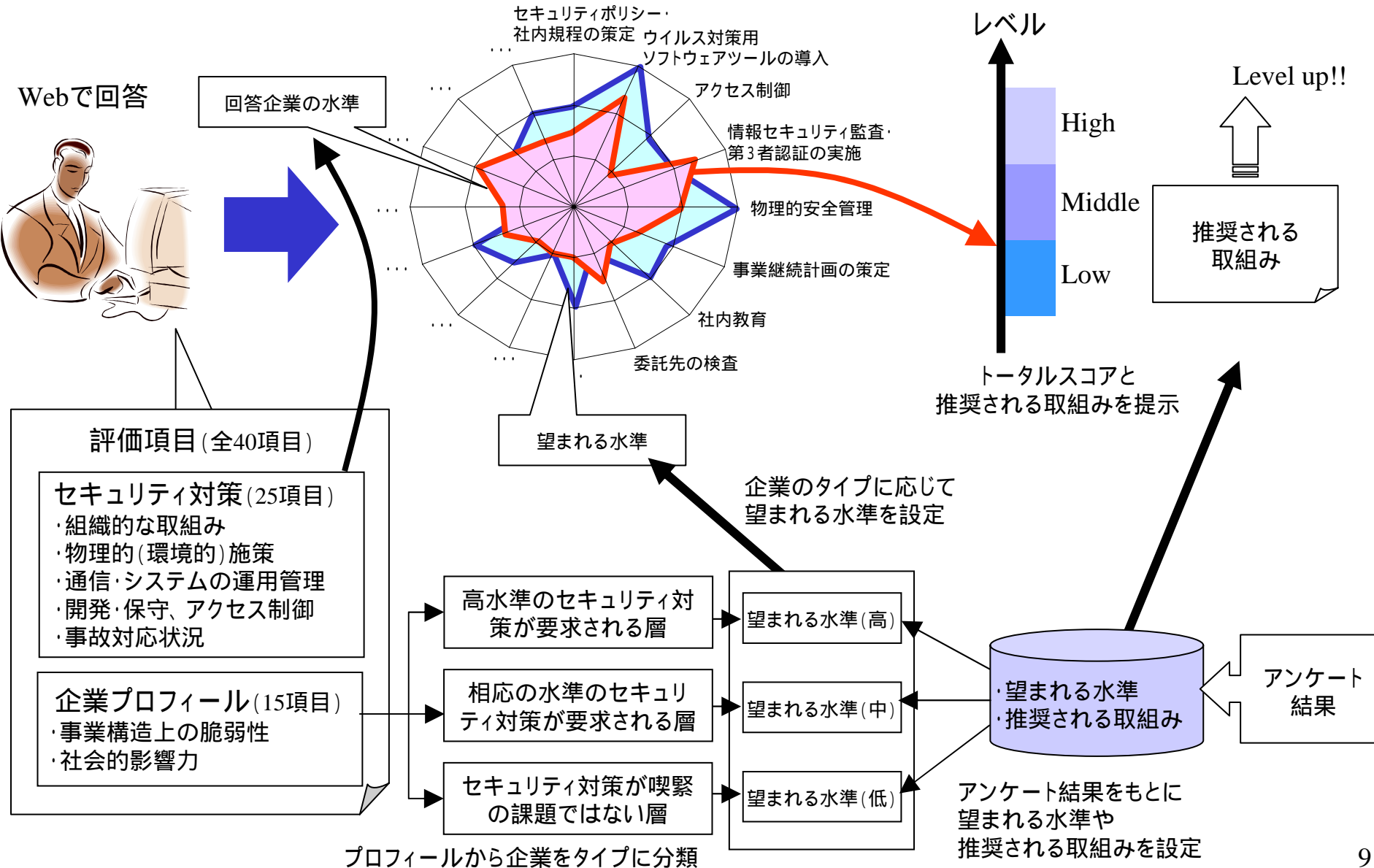
## 2.3 施策ツールとISMS認証等との基本的関係

- 対策ベンチマークは、第三者評価・認証の実施へとつながる「入口」の役割を担う。
- 情報セキュリティ報告書は、情報開示における客観的な評価・認証の重要性を啓発する。
- 事業継続計画の策定は、ISMS認証等で評価される情報セキュリティ対策の強化や、情報セキュリティ報告書の充実に寄与する。



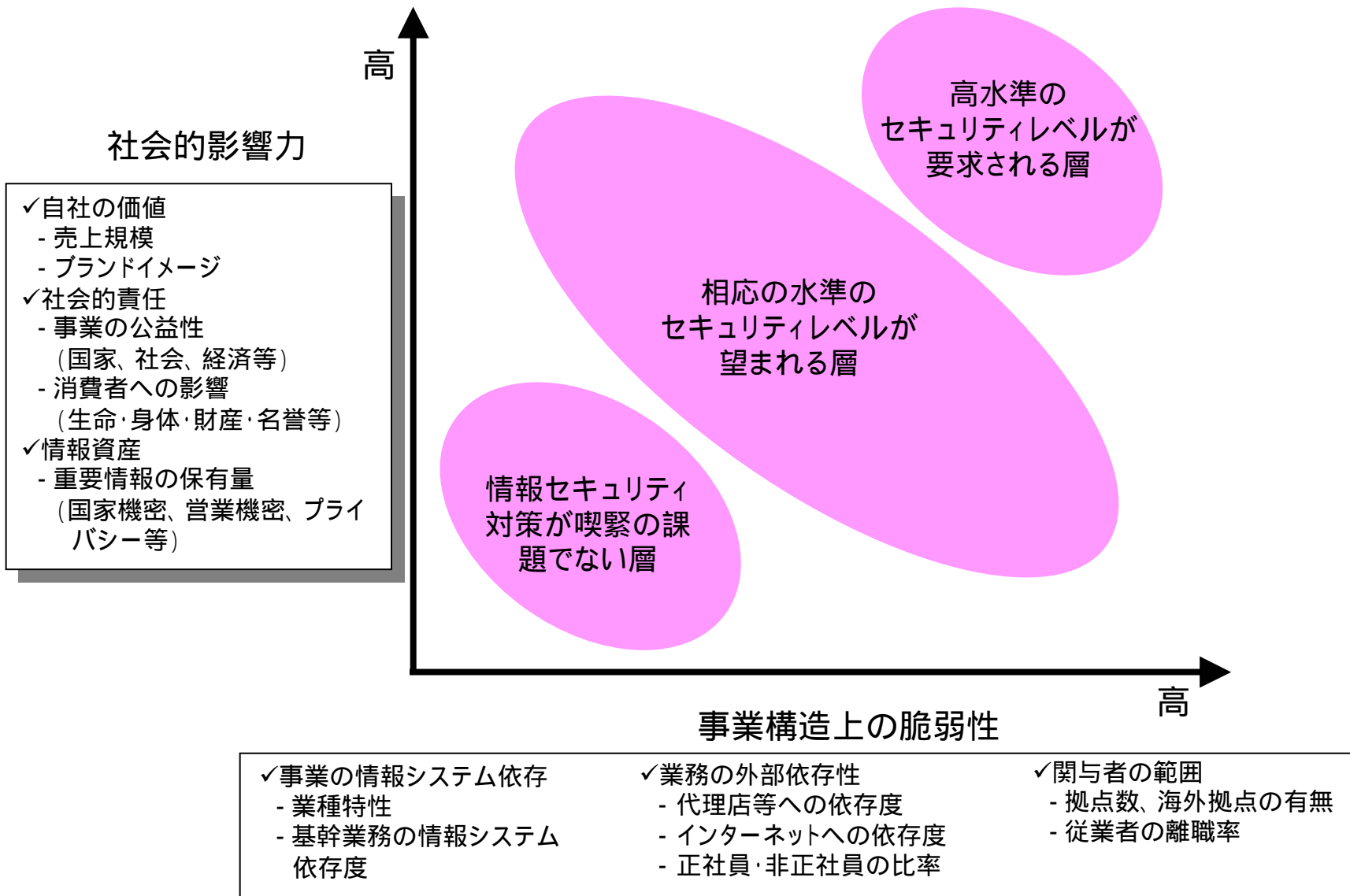
# 3.1 対策ベンチマーク～構成

- 何をどこまで実施すべきかわからない企業に、セルフチェックによる「気づき」を促しつつ、一定の目標を提示。
- 情報セキュリティ対策の取り組み状況の結果から、レーダーチャートや全体のスコアを算出。



## 3.2 対策ベンチマーク～企業の分類イメージ

- 「事業構造上の脆弱性」と「社会的影響力」を分類軸として、回答者のプロフィール項目の内容からこれらの値を算出。
- 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はない層」として、3グループに分類。



- 大手企業・中小企業各約3,000件、計6,024社にアンケート調査を実施。全回収票1,633件中、すべての設問に回答があった885件(大手企業474件、中小企業411件)について、事業構造上の脆弱性と社会的影響力から3つのグループに分類。
- 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(内在するリスクが高い)ほど、トータルスコアの平均も高く、より積極的に対策に取り組んでいることがわかる。ただし、各層ともトータルスコアのばらつきが大きい。

## 成熟度の構成

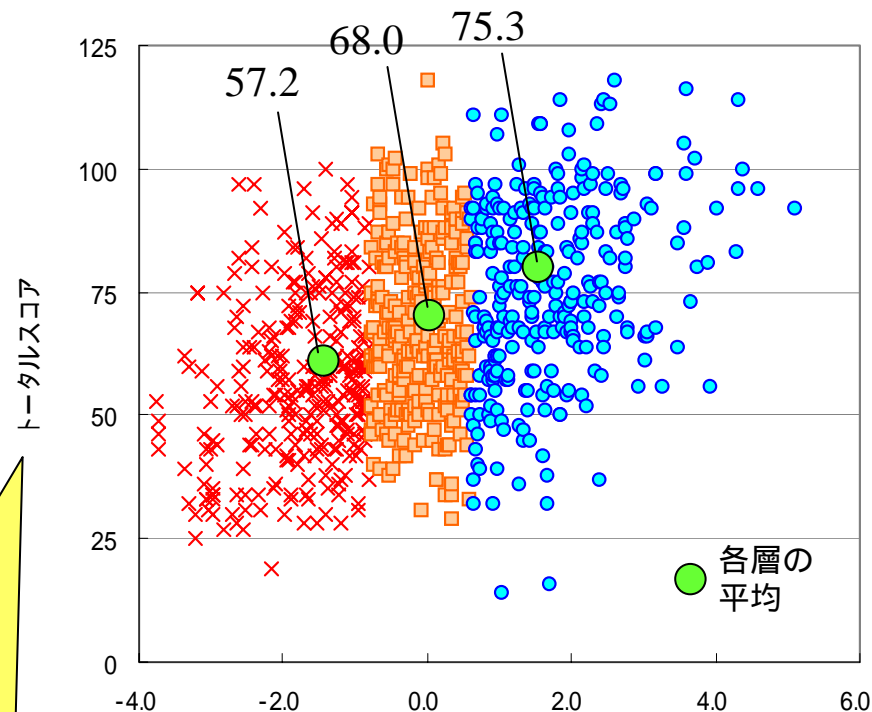
- 1) 経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
- 2) 経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
- 3) 経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
- 4) 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
- 5) 4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

## セキュリティ対策の状況の評価項目(25項目)

- ・組織的な取組み(7項目)
- ・物理的(環境的)施策(5項目)
- ・通信・システムの運用管理(5項目)
- ・開発・保守、アクセス制御(5項目)
- ・事故対応状況(3項目)

トータルスコア = 情報セキュリティ対策の状況  
25項目の成熟度の合計  
(125点満点)

## 回答企業とトータルスコアの分布



事業構造上の脆弱性指標 + 社会的影響力指標  
(情報セキュリティリスク指標)

- × 情報セキュリティ対策が喫緊の課題ではない層
- 相応のセキュリティレベルが望まれる層
- 高水準のセキュリティレベルが要求される層

ISMS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

「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

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「及び」のレベルを求めることは困難と考えられること

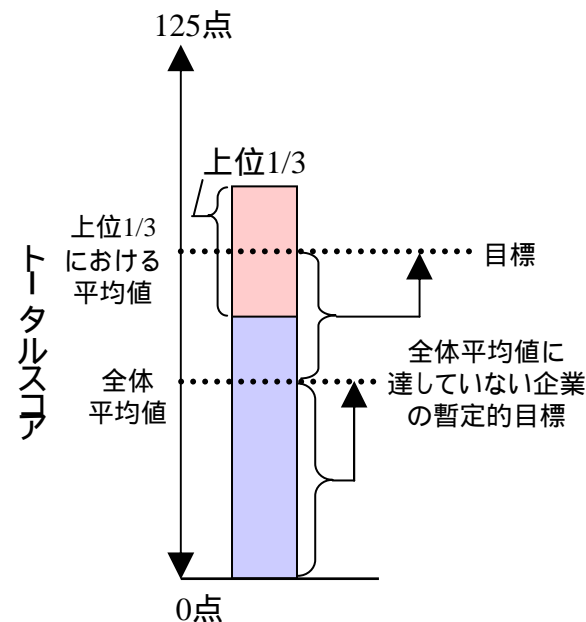
等を踏まえ、「望まれる水準」\*を次のように設定。

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する

\*) 「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

「望まれる水準」の具体的数値

	全体	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要求される層	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)



- 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。
- 不要な情報まで開示してしまうことがないよう若干の配慮が必要。

## 情報セキュリティ報告書の記載項目(フルセット)

### 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

### 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り組み方針
- ✓ 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

### 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

### 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(対策ベンチマークのスコア等)

### 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

### 情報セキュリティに係る主要注力テーマ

- ✓ 特に強調したい取組み、テーマを選択し、その状況を紹介(例:個人情報保護、事業継続計画等)

### 第三者評価・認証

- ✓ 第三者評価・認証に係る取組み
  - 認証の取得状況(ISMS認証、プライバシーマーク)
  - 情報セキュリティ監査の実施状況 等



- ✓ 情報セキュリティ報告書の基本的な位置づけは、その発行が企業の期待に応じた効果を持ちうるよう、「任意」「自由選択」の方向を指向すべき
- ✓ 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
- ✓ 他の報告書の一部として組み込む形もありうるし、単体の報告書という形もありうる

## 発行主体にとっての効果

### 説明責任の遂行

- ・事業に影響するIT関連のリスクが小さいことを対外的に説明

### 新たな事業付加価値創出

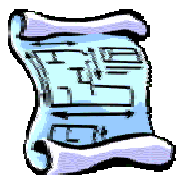
- ・事業戦略の反映
- ・ブランドの確立

リスク低減に関する説明を  
ステークホルダーから  
求められる企業

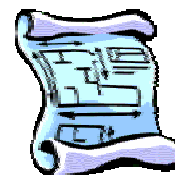
情報セキュリティへの  
取り組みが競争優位  
に寄与する企業

【必要最低限の項目・内容】

【すべての項目・内容】



自社の事情に応じて  
記載項目や内容のレベルを  
選択



## ステークホルダーにとっての効果

### 顧客・消費者

購買活動の判断

### 取引先

取引相手の信頼性の把握

### 投資家、アナリスト

投資対象のリスク評価

### 格付け機関

格付けの分析材料として活用

### 従業員

情報セキュリティに対する意識・理解の向上

## 利害関係者からの要求

- 取引先  
サプライチェーンの一員として、  
継続的な製品・サービスの提供
- 顧客・消費者  
継続的な製品・サービスの提供
- 地域社会  
継続的な雇用機会の提供
- 株主  
事業に係るリスク対策の説明

新たな社会からの要求

- ✓ビジネスに与える影響度を分析し、優先事項と対策を決定
- ✓リスクマネジメントへの組み込みが重要
- ✓実効的な計画とするため、導入後の訓練や改善が重要
- ✓経営層の最終的な承認が重要

## ビジネスの継続性確保が最重要課題



## IT事故への的確な対応が重要



既存の事前対策の限界



災害復旧計画、  
防災マニュアル等

## 事業継続計画 (BCP)

潜在的損失によるインパクトの認識を行い、実行可能な継続戦略の策定と実施、事故発生時の事業継続を確実にする継続計画。  
事故発生時に備えて開発、編成、維持されている手順及び情報を文書化した事業継続の成果物。

BCP策定後、実効的に企業内に浸透させ、マネジメントに組み込むことが重要

## 事業継続マネジメント (BCM)

事業継続計画 (BCP) の策定から運用、見直しまでのマネジメントプロセス。

## IT依存度の高まりとIT事故リスク

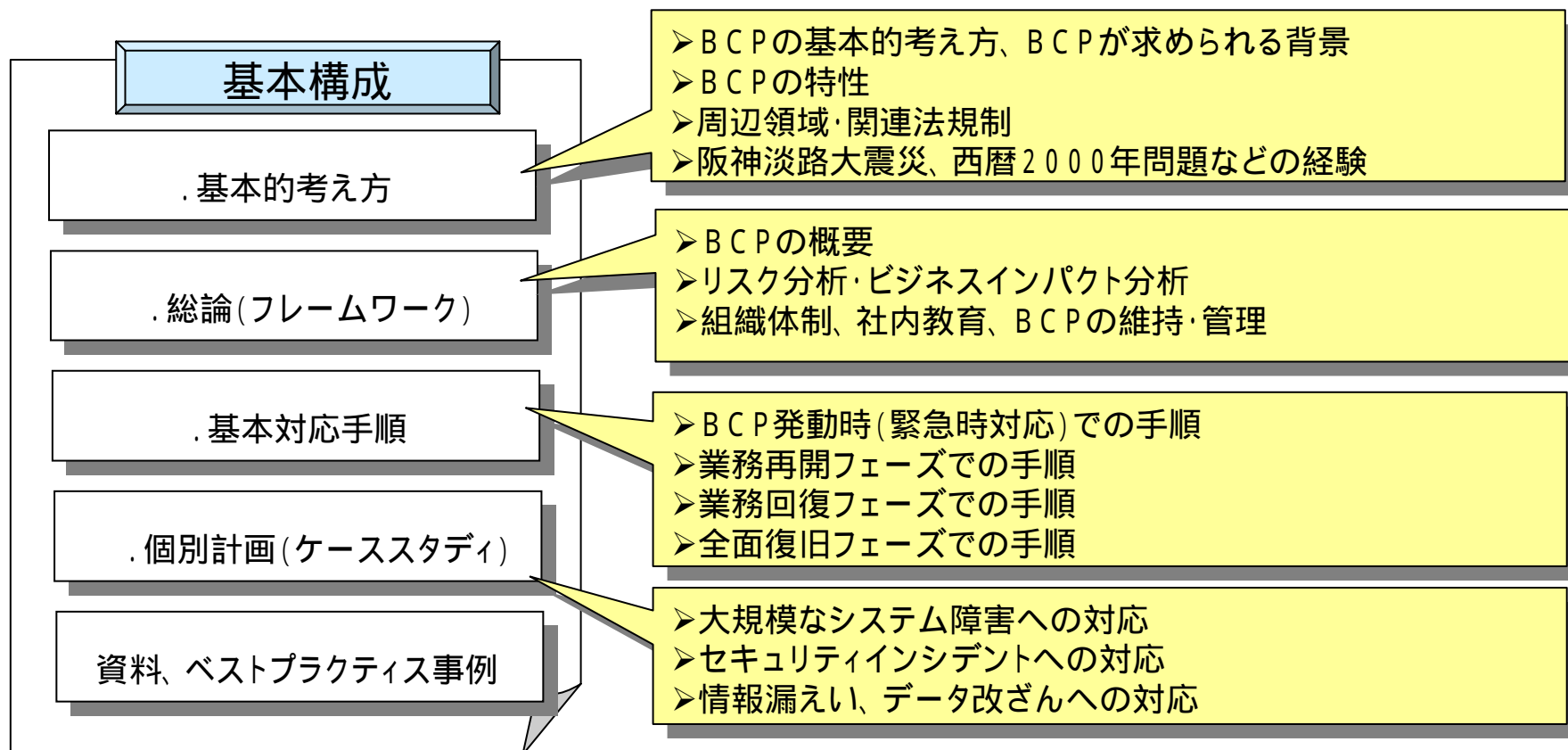
- 事業のIT依存度の高まり
- IT事故のリスク増大  
サイバー犯罪、システムダウン、  
西暦2000年問題の教訓、  
情報漏えい事故の多発

IT依存度の高まり

## 自然災害リスク

- 地震  
阪神・淡路大震災、新潟県  
中越地震の教訓
- 台風  
水害等による広域災害の教訓

- 事業継続計画(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
- 基本的な考え方から、具体的な計画の構築手順を説明
- 事業のIT依存度が高まっていることから、具体的計画はIT事故を想定
- 参考資料やベストプラクティス事例など、企業内での説明にも有用



## (1) 企業に求められる取組み

- **情報セキュリティ対策ベンチマークの活用**(例:自らの現状把握、取引先の信頼性確認)
- **情報セキュリティ報告書の発行**(例:モデルの記載項目を反映したCSR報告書等の情報開示)
- **IT事故を想定したBCPの策定**(例:取引先への説明責任としての対応)
- **企業グループセキュリティの実現**(施策ツールを活用しつつ企業グループごとに検討すべき)

## (2) 関係機関・業界に求められる取組み

- **施策ツールの開発・維持・改善**(適切な運用をめざし関係機関で役割分担)
- **セルフチェックと連動するリスク定量化ツールの提供**(対策ベンチマークの活用促進策として)
- **損害保険に係る評価・料率算定への適用**(対策ベンチマークを用いた対策推進の動機付けとして)
- **情報セキュリティ報告書の発行事例の収集・開示**(情報開示に係る取組み状況の比較を可能に)
- **第三者機関による情報セキュリティ報告書の格付け**(評価専門機関、マスコミ、NPO等に期待)
- **情報セキュリティ報告書に関する表彰制度の整備**(ディスクロージャーに関する表彰制度を例に)
- **関係機関・関係者による啓発**(関係機関やITコーディネーター等による啓発、CIO/CISOの育成等)
- **国際標準化への対応**(CSRガイドラインやBCPの国際標準化につい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)

## (3) 政府に求められる取組み

- **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**  
(例えば、応札企業にセルフチェックデータの提出を要求し、加点方式で評価する形を検討)
- **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**(相互に補完し、統合的に促進)

## 「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 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」

### 【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」

### 【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