情報セキュリティ会計に関する検討報告書

～ガイドライン策定に向けて～

２００５年７月

特定非営利活動法人　日本ネットワークセキュリティ協会

目　次

ＪＮＳＡ　政策部会　セキュリティ会計ガイドライン検討ワーキンググループ

ワーキンググループリーダー

佐野　智己	凸版印刷株式会社

ワーキンググループメンバー（１３名）

蛭間　久季	株式会社アークン
村主　俊彦	ＮＲＩセキュアテクノロジーズ株式会社
小宮山　靖裕	ＮＴＴコムウェア株式会社
勝見　勉	グローバルセキュリティエキスパート株式会社
若井　順一	グローバルセキュリティエキスパート株式会社
大久保　和孝	新日本監査法人
宮原　潤	新日本監査法人
下村　武史	セコム株式会社
木村　章展	中央青山監査法人
清水　惠子	中央青山監査法人
井上　吉隆	日本電信電話株式会社
安藤　信之	株式会社ヒューコム
佐久間　敦	みずほ情報総研株式会社

はじめに

NPO 日本ネットワークセキュリティ協会（JNSA）では、近年、重要性の高まる情報セキュリティ分野において、技術・政策・マーケティング・教育という観点で幅広いワーキンググループ活動が行われている。

各ワーキンググループにおいて情報セキュリティにかかる諸問題を解決すべく活動する中で、大きな懸案として存在した共通認識が、対象が守られていることを可視化し、比較対象可能な形で情報セキュリティガバナンスを執行することであった。

そこで、JNSA 政策部会「セキュリティ会計ガイドライン検討ワーキンググループ」では、この懸案解決への一つのプログレスのために、企業における情報セキュリティ確保の取り組みを会計的視点から認識・評価・伝達（ディスクローズ）する仕組みとして、『環境会計』に倣い、『セキュリティ会計』を定義し、その基本的な考え方を取りまとめることを試みた。

背景と目的

情報セキュリティ事故の被害が顕在化し、企業に於ける情報セキュリティ対策への意識が変わりつつある。今日、情報技術（Information Technology ： IT）が企業活動における重要なインフラとして浸透する反面、個人情報や機密情報の漏洩、コンピュータウィルス・ワームへの感染などによる情報セキュリティ事故が社会的な事件として取り沙汰されるようになった。

このような社会状況の変化により、企業経営者は情報セキュリティにかかるリスクが企業の事業継続にとって大きな影響を及ぼす事と、情報セキュリティ事故による被害が当該組織に収まらず情報通信ネットワーク社会の秩序維持と発展に対して甚大な影響を与えるという 2 つの事実を強く認識させられた。そして、これらの認識をもとに、情報セキュリティ事故の「発生頻度」、「被害の範囲・大きさ」、「復旧に要する時間・費用」など、多様な事業リスクを保有することを意識し、情報資産にかかるリスクを「新たな事業リスク」として積極的に対策を講じる必要がある。

ところが、企業における情報セキュリティ対策の現状を眺めると、経営者主導の自発的な施策として向上・継続しているとは言い難く、情報セキュリティ対策は法整備への適応や情報セキュリティ事故から誘発される「受身の投資」となっている。

このような状況を生む理由としては、主に２点考えられる。

第一に、通常、情報セキュリティ対策は脅威と脆弱性に対して根拠ある判断の上に成立させるべきであり、意志決定者はその投資効果を比較対照可能な形で評価することが求められる。しかし、この根拠の算出に応えるツールが十分には開発されていない。

第二に、情報セキュリティ対策は技術的対策・物理的対策・人的対策・組織的対策と広範かつ多額の投資が必要となるため、近年のコーポレートガバナンスの観点から鑑みたとき、株主をはじめとする各種ステークホルダ（利害関係者）へのアカウンタビリティ（説明責任）が発生する。現在、ステークホルダにむけたセキュリティ投資を説明するツールに関しても十分には成熟しておらず、市場のメカニズムを断絶する結果となっている。

これら企業の情報セキュリティへの取り組み背景を踏まえ、本ワーキンググループでは情報セキュリティ対策に向けた動きが企業の自主的な活動として実装される事を目指し、「環境会計ガイドライン」[1]に倣い、「情報セキュリティ会計ガイドライン」の策定を試みた。

本ガイドラインが完成した暁には、企業の情報セキュリティ投資が本来の目的に沿って再検討されるきっかけとなり、これまで見えなかったリスクへの投資(過少投資の是正)と適切なリスクアセスメントによるコスト削減(過剰投資の是正)が実現される事を願ってやまない。また、事業活動に関わるステークホルダが企業価値を比較・評価するための指標となり、ＩＲコミュニケーションが円滑になることを目指したいと考える。

---

[1] 「環境会計ガイドライン 2005 年版」（環境庁：平成 17 年 2 月）

1．　情報セキュリティ会計とは

1.1　情報セキュリティ会計の定義

本報告書では、「情報セキュリティ会計」を以下のように定義する。

- 企業等が自身の企業価値を維持し、さらに向上させていくことを目指して、情報セキュリティに関する取り組みを効率的かつ効果的に推進していくことを目的として、事業活動における情報セキュリティのためのコストとその活動によって得られた効果を認識し、可能な限り定量的に測定し伝達する仕組み
- ここで、「情報セキュリティ」とは、企業等が自身の情報資産を各種の脅威から保護し、その機密性、完全性、可用性を確保し、維持するための取り組みのことをいう
- 加えて、企業等が自身の事業活動を通じて、情報通信ネットワーク社会の秩序の維持と発展に資する取り組みを含む

1.2　情報セキュリティ会計の機能と役割

情報セキュリティ会計の機能は内部機能と外部機能に分けられる。

（1）内部機能

企業等において、情報セキュリティのコストの管理やコスト対効果の分析を可能にし、適切な経営判断を通じて効率的かつ効果的な情報セキュリティへの取り組みを促す機能である。

（2）外部機能

企業等の情報セキュリティへの取り組みを定量的に測定した結果を開示することによって、消費者や投資家、ネットワーク社会の参加者等の外部の利害関係者（ステークホルダ）の意思決定に影響を与える機能である。

内部機能は、企業等の内部において、情報セキュリティ対策に要したコストとその効果を評価して情報セキュリティ対策をより効率的、効果的なものにするために、また、情報セキュリティが事業活動に与える影響を把握するために有効である。すなわち、経営者や関係部門等が、経営管理ツールとして情報セキュリティ会計を利活用することが期待される。

外部機能は、CSR 報告書や独立した情報セキュリティ報告書等の手段を通じて情報セキュリティへの取り組み姿勢や具体的な対応などを公表することによって、企業等の情報セキュリティへの取り組みを利害関係者に伝達するために有効である。公表は企業等の社会的信頼を高め、社会的評価を確立していくことにつながる。すなわち、外部の消費者、投資家、地域住民等に対して説明責任を果たすと同時に、情報セキュリティの観点も含めた、より適切な企業評価に結びつく役割が期待される。

1.3 情報セキュリティ会計に求められる要件

企業等における情報セキュリティ会計にかかわる取り組みがその目的（内部機能・外部機能）を充足するためには、下記のような原則的な要件を満たすことが求められる。

（1）目的適合性

情報セキュリティ会計は、企業等の情報セキュリティ対策のためのコストとその活動により得られた効果に関して、利害関係者の意思決定に資する有用な情報を提供すべきである。

ア　重要性： 目的適合性については、重要性を考慮すべきである。

（2）信頼性

情報セキュリティ会計は、情報の重大な誤り及び偏りを排除し、利害関係者から信頼を得るべきである。

ア　正当性：情報セキュリティ会計情報を開示する場合は、正確かつ妥当に記述すべきである。
イ　実質性： 単に形式的な開示に従うにとどまらず、情報セキュリティ活動の実態に即して情報開示の必要性を判断すべきである。
ウ　中立性： 公正不偏の態度で記述すべきである。
エ　網羅性： すべての情報セキュリティ対策活動について、重要な情報を漏れなく対象とすべきである。
オ　慎重性： 不確実性を伴う情報は、慎重に取り扱い、その性質、対象範囲、判断根拠を明らかにすべきである。

（3）明瞭性

情報セキュリティ会計は、利害関係者に対し、必要な情報セキュリティ会計

情報を明瞭に表示し、企業等の情報セキュリティへの取り組み状況に関する判断を誤らせないようにすべきである。

（4）比較可能性

情報セキュリティ会計は、企業等の各期を通じて比較可能であり、かつ異なる企業間を通じて比較可能である情報を提供すべきである。

（5）検証可能性

情報セキュリティ会計情報は、客観的立場から検証可能であるべきである。

1.4　情報セキュリティ会計の構成要素

情報セキュリティ会計は、事業活動における情報セキュリティのためのコストとその活動により得られた効果より構成される。

（1）情報セキュリティ対策コスト

情報セキュリティインシデントの発生の防止、抑制または回避、影響の除去、発生した被害の回復またはこれらに資する取り組みのための投資額及び費用額とし、貨幣単位で測定する。

投資額とは、対象期間における情報セキュリティを目的とした支出額で、その効果が数期にわたって持続し、その期間に費用化されていくもの（財務会計における償却資産の当期取得額）とする。

費用額とは、情報セキュリティを目的とした財・サービスの費消によって発生する財務会計上の費用又は損失とする。

（2）情報セキュリティ対策効果

情報セキュリティインシデントの発生の防止、抑制または回避、影響の除去、発生した被害の回復またはこれらに資する取り組みによる効果とし、物量単位で測定する。情報セキュリティ対策効果の測定のアプローチとして、年間損失予測を積み上げてコスト対効果を算定する方法がある。もう１つは、重要業績評価指標（KPI： Key Performance Indicator）を設定して、管理する方法である。

1.5 「情報セキュリティ会計キューブ」のコンセプト

本報告書では、費用と効果の考え方を整理するために図１に示す「情報セキュリティ会計キューブ」のコンセプトを導入する。

情報セキュリティ会計キューブは、「目的」「対策」「対象」の３つの軸から構成される。それぞれの軸の意味は以下の通りである。

（ａ）目的

企業の個別の事業活動と対応づけられ、ブレークダウンされた、情報セキュリティのカテゴリ。本報告書では、例として以下の 5 項目を設定した。

- 個人情報保護
- 企業機密情報保護
- 事業継続
- ネットワーク秩序維持
- その他

（ｂ）対策

情報セキュリティのために行う各種対策（コントロール）の項目。本報告書では、例として以下の 9 項目を設定した。

- セキュリティ基本方針
- 組織のセキュリティ
- 資産の分類および管理
- 人的セキュリティ
- 通信および運用管理
- アクセス制御
- システムの開発および保守
- 事業継続管理
- 適合性

（ｃ）対象

情報セキュリティの対象となる組織単位。全社レベルから各部門、あるいは個別の事業活動といった単位が想定される。

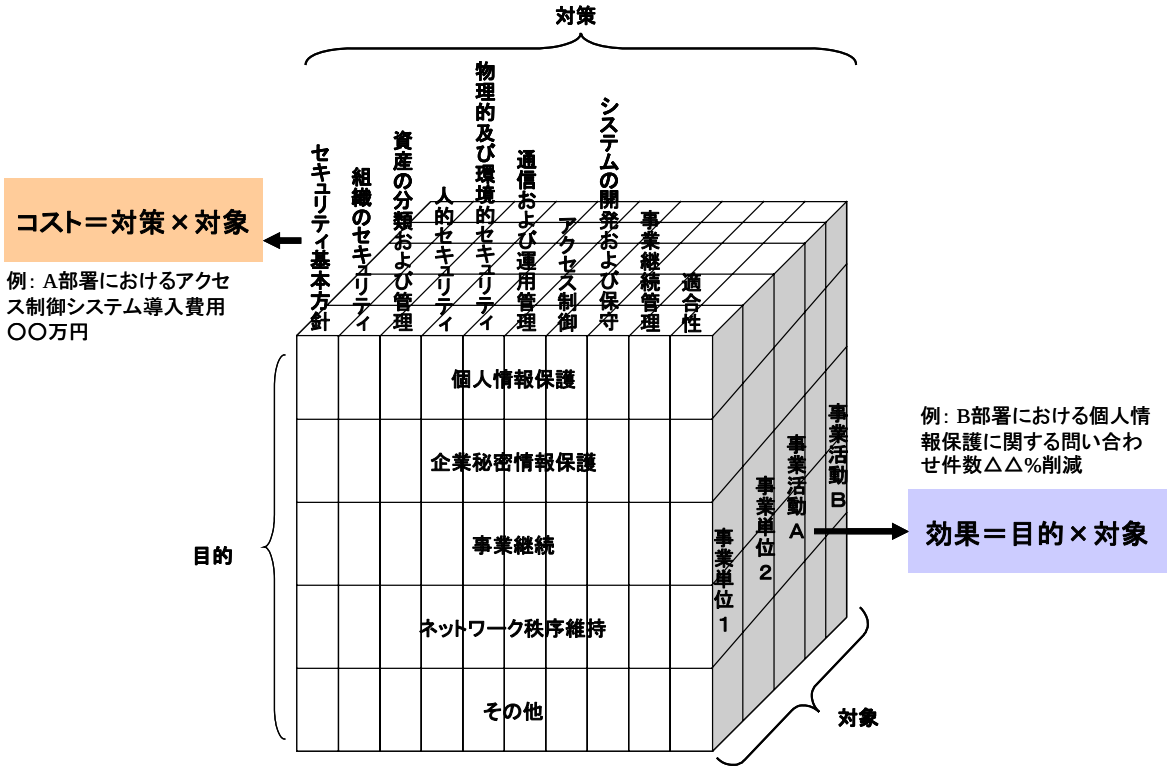


図１　「情報セキュリティ会計キューブ」におけるコストと効果の考え方

上記の３軸とコスト・効果との関係は以下のようになる。

- コスト ＝ 対策 × 対象 ： どの対象（全社、部署等）において、どのような対策にどれだけお金を掛けたか？
- 効果 ＝ 目的 × 対象： 各対象ごとに、設定された目的に対して、金銭的・非金銭的な効果はどの程度あったか？

「目的」「対策」「対象」に設定した各項目は、本報告書の検討にあたって、一例として抽出したものである。実際の企業等では、それぞれの背景事情やセキュリティポリシーに応じて、適宜設定することを想定している。「３．コストと効果の算定」では、上記の例に基づくコスト・効果の算定の方法について説明する。

「1.2　情報セキュリティ会計の機能と役割」で述べたように、情報セキュリティ会計の目的は内部機能と外部機能の 2 つの側面がある。情報セキュリティ会計の機能と情報セキュリティ会計キューブの関係を図２に示す。

企業等は守るべき情報資産を特定し、情報セキュリティの目的を設定して、対象となる部署や組織単位においてセキュリティ対策を実施する。

このセキュリティ対策の適正性と効果は、一定期間ごとに評価される。内部機能の観点からは、現状のセキュリティ対策を維持または是正し、必要な投資を判断するための資料として使用される。一方、外部機能においては、上記の評価を外部のステークホルダに対して開示できる形に取りまとめて提供される。これにより、ステークホルダは、企業等が企業価値を維持・向上させるために、情報セキュリティの観点からどのような取り組みを行い、どの程度の効果が見込まれるのかが判断できるようになる。

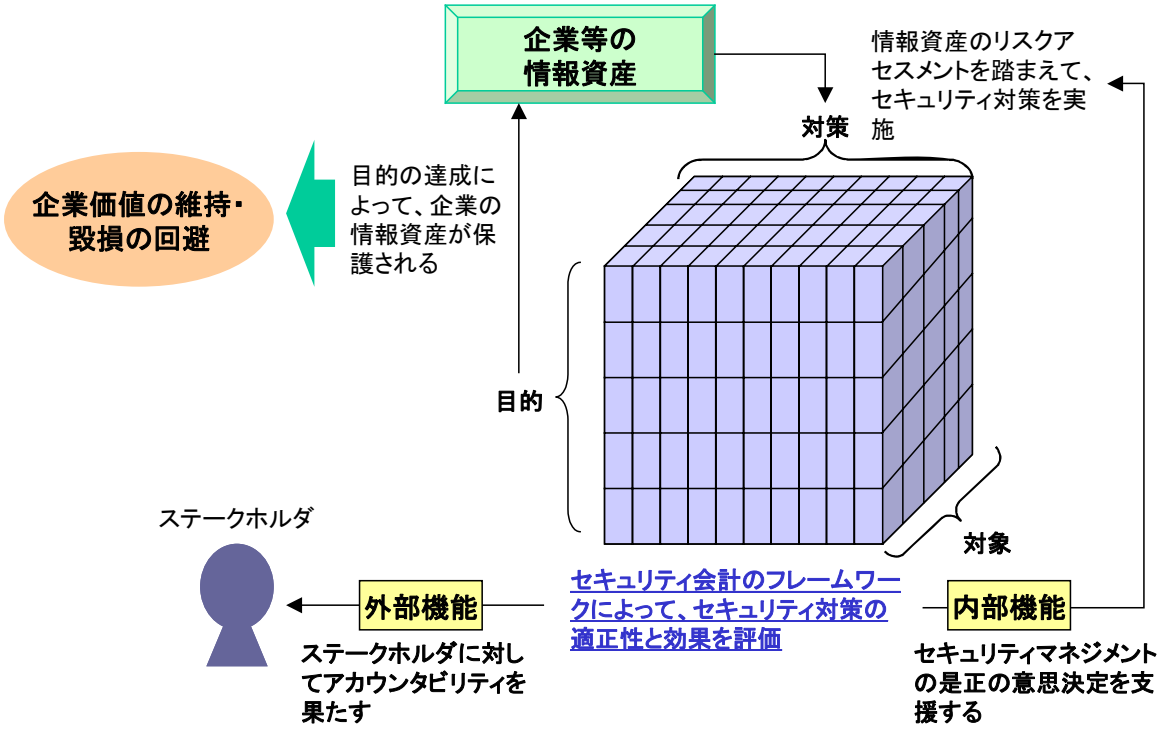


図２　情報セキュリティ会計の機能と役割

2．　情報セキュリティ会計の基本事項

2.1　情報セキュリティ会計において基本となる重要な事項

情報セキュリティ会計を実施する前提として、まず、情報セキュリティ会計に取り組む目的を明確にしておくべきである。情報セキュリティ会計の目的は、企業等の情報セキュリティに関する経営方針や目標と適合したものとすることが必要である。

次に、情報セキュリティ会計の実施に際しては、

・対象期間

・集計範囲

・情報セキュリティ対策のコストの算定基準

・情報セキュリティ対策の効果の算定基準

について定めておく必要がある。また、情報セキュリティ会計の公表に際しては、上記の事項について開示するとともに、変更があった場合には、変更した旨、内容、理由及び影響を記載するものとする。

2.2　対象期間と集計範囲

（1）対象期間

対象期間は、原則として情報セキュリティ報告書と同一とする。基本的には、企業等の財務会計情報と情報セキュリティ対策の活動及び情報セキュリティ会計情報とが整合するように当該企業等の事業年度と一致させるべきである。

（2）集計範囲

集計範囲は、原則として情報セキュリティ報告書（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」において情報セキュリティ報告書モデルが策定、平成 17 年 3 月公表）と同一とする。基本的には、全社とすべきである。

また、必要に応じて、全社、情報処理の委託の子会社及び関連会社を含めたグループ、事業所、ISMS 認証制度適用範囲といった範囲での集計を行うことも有効であり、企業等の実態に即して順次集計範囲が拡がることが望まれる。

ア　全社

企業等の財務会計情報と情報セキュリティ対策の活動及び情報セキュリティ会計情報とが整合するように、原則として財務会計上の会計単位と同一の企業等の全体を対象とする。

イ　情報処理の委託の子会社及び関連会社を含めたグループ

情報処理の委託の子会社及び関連会社等からなるグループを対象とする。

情報のサプライチェーンが形成されている企業等の情報セキュリティ対策の活動では単一企業等だけではなく、子会社等を含めて当該企業等の情報セキュリティ対策の活動の実態を把握するためには、情報処理の委託の子会社及び関連会社を含めたグループ企業集団全体で情報セキュリティ会計を集計する必要がある。

ウ　事業所

個別の事業所を対象とする。

エ　ISMS 認証制度適用範囲

ISMS 認証制度適用範囲は、企業等において ISMS 認証制度の適用範囲を宣言している範囲のことであり、ISMS 認証制度のコストや効果を測定することが比較的容易であるといえる。

2.3　コストと効果の考え方

情報セキュリティ対策のコストを算定するに当たり、以下の事が重要である。

・算定に含める情報セキュリティ対策の範囲を明確にすること

・もれなく重複なく計上すること

2.3.1 コスト範囲の明確化

情報セキュリティ対策の範囲には複数の考え方がある。これは企業により情報セキュリティの目的の範囲が異なっているためと考えられる。本 WG では、企業の情報セキュリティ対策目的として考えられるものを４つ挙げた。

企業により情報セキュリティ目的の集合の部分集合を、集計範囲として捉えることは可能である。ただしそのような場合には、よりいっそうコスト範囲を明確化する必要がある。

2.3.2 もれなく重複なく計上する

コストの範囲を明確にし、その範囲内に該当するコストをもれなく重複なく計上するように心がける必要がある。

情報セキュリティを直接的に担当する従業員だけでなく、間接的に情報セキュリティ対策にかかわる従業員についてもコストが発生していると考えるのが自然である。例としてはウイルスソフトのパターンファイルの更新等がある。これらの時間も計上したほうがより正確なコストが把握できる。

2.3.3 対策コストと効果の関係

1 章で述べたように、情報セキュリティ対策のコストと効果は一対一に対応するものではない。特定の目的、例えば個人情報保護に対するコスト対効果だけを知りたい場合であっても、関連するすべての対策コストを算出する必要があ

る。

情報セキュリティ対策のコストと効果の因果関係は複雑である。同じ効果を得るために必要となるコストは、企業の提供するサービス、保有する情報資産、対策の組み合わせ等により異なる。対策に費やしたコストを記録し、効果を算出することで、総合的な情報セキュリティの成果を把握でき、対策の効率性を認識することができる。企業等は、情報セキュリティの成果を総合的に考慮できるよう、情報セキュリティ対策の効果の指標を選択する必要がある。

2.3.4 過去の情報セキュリティ対策活動の考慮の必要性

情報セキュリティ対策の効果は、情報セキュリティ対策を進めるにつれて、同額の追加的対策コストを費やしてもその効果は逓減していく場合もある。このため、情報セキュリティ対策の取り組みが進んだ企業等ほど、効果が生じにくくなる可能性がある。

従って、企業等のセキュリティの取り組みを評価する際、単一の対象期間におけるコスト対効果のみでなく、過去の情報セキュリティ対策活動も考慮し、現在の取り組みの水準を理解する必要がある。

3．　コストと効果の算定

3.1　情報セキュリティ対策コスト

情報セキュリティ対策コストは、情報セキュリティ事故の発生の防止、抑制又は回避、影響の除去、発生した被害の回復又はこれらに資する取り組みのための投資額及び費用額とし、貨幣単位で測定する。

3.1.1 情報セキュリティ対策コストの内容

（1）投資額及び費用額

投資額は、企業等の償却資産への設備投資額のうち、情報セキュリティ対策を目的とした支出額を計上する。これは、情報セキュリティ対策に係る効果が長期間にわたって及ぶ情報セキュリティ対策への資金投入に関する情報を得るためのものである。例えば、情報機器を購入すれば、有形固定資産勘定に計上され、ソフトウェアの開発や購入であれば、無形資産勘定に計上される。物件費として費用計上される場合もある。導入対応のための人件費も含められる。

費用額は、企業等の費用のうち、情報セキュリティ対策を目的とした発生額を計上する。

これは、当期の情報セキュリティ対策に係る効果に対応する発生費用に関する情報を得るためのものである。例えば、固定資産計上により発生する減価償却費、設備リース費用、対応のための人件費があげられる。

（2）目的基準

各々のコストが情報セキュリティ対策コストに該当するかどうかの判断は、目的基準による。目的基準とは、情報セキュリティ対策の目的で投下されたコストを抽出する基準である。

3.1.2 情報セキュリティ対策コストの分類

主たる事業活動とは、財・サービスの購入から製造、流通を経て、販売又は提供に至る一連の事業活動のうち、管理活動、研究開発活動、社会活動を除いた部分とする。

表１　分類内容

(1)事業エリア内コスト：主たる事業活動により事業エリア内で生じる情報セキュリティ確保（情報ネットワークシステムを外部からの攻撃、内部からの不正使用、誤使用から保護するための）に係るコスト
(2)取引先・委託先等に対する情報セキュリティ対策コスト：取引先・委託先等との情報のやり取りに伴って生じる情報セキュリティ確保に係るコスト、並びに取引先・委託先等の情報セキュリティのレベル向上に係るコスト
(3)管理活動コスト：情報セキュリティ確保のための管理活動に伴うコスト
(4)研究開発コスト：研究開発活動における情報セキュリティ対策のコスト
(5)社会活動コスト：社会活動における情報セキュリティ対策のコスト
(6)情報セキュリティ事故対応コスト：情報セキュリティ事故に対応するコスト
(7)その他コスト：その他情報セキュリティ対策に関連するコスト

（１）事業エリア内コスト

企業等の主たる事業活動により事業エリア内で生じる情報セキュリティ事故を低減する取り組みのためのコストとする。例えば、物理的設備の導入、ファイアウォール等の機器の導入、セキュリティソフトウェアの導入などである。事業エリアとは、企業等が直接的に情報セキュリティ対策を実施できる領域とする。

（２）取引先・委託先等に対する情報セキュリティ対策コスト

企業の取引先・委託先等との情報のやり取りに伴って生じる情報セキュリティ確保に係るコスト、並びに取引先・委託先等の情報セキュリティのレベル向上に係るコストとする。

（３）管理活動コスト

企業等の情報セキュリティ対策のための管理活動であって、事業活動に伴い発生する情報セキュリティ事故の抑制に対して間接的に貢献する取り組みのためのコストや、情報セキュリティ情報の開示等、企業等が社会とのコミュニケーションを図る取り組みのためのコストとする。

①情報セキュリティマネジメントシステムの整備、運用のためのコスト

②情報セキュリティ情報の開示及び情報セキュリティ広告のためのコスト

③情報セキュリティ監視のためのコスト

④従業員への情報セキュリティ教育等（セキュリティリテラシーの向上）のためのコスト

（４）研究開発コスト

企業等の研究開発活動のためのコストのうち、情報セキュリティ確保や情報資産保護・保全のための対策に関するコストとする。例えば、情報セキュリテ

ィ対策に資する製品等(暗号技術)の研究開発コストである。事業の性質を有するものはここでは除く。

（５）社会活動コスト

企業等の事業活動に直接的には関係のない社会活動における情報セキュリティ対策に関する取り組みのためのコストとする。例えば、脆弱性情報流通のための枠組みに参画するコストである。ISAC[2]、JNSA などへの参加活動コストである。

（６）情報セキュリティ事故対応コスト

企業等の事業活動に影響を与える情報セキュリティ事故に対応して生じたコストとする。

①情報セキュリティ対策に関する損害賠償等のためのコスト

（例）個人情報漏洩時の補償・善後策のコスト

②情報セキュリティの事故に対応する引当金繰入額及び保険料

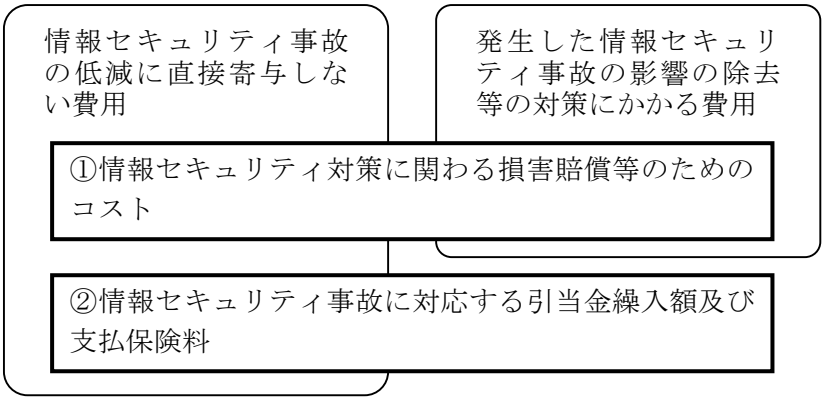
（例）個人情報漏洩に備えた損害保険料のコスト

情報セキュリティ事故対応コストの性格

引当金繰入額や支払保険料は、事後的にかかる情報セキュリティ事故対応コストの企業負担を平準化又はリスク転嫁させるための費用であり、直接的には情報セキュリティ事故の低減には寄与しない。

損害賠償のためのコストは事後的に発生する費用であると同時に、情報セキュリティ事故の低減に直接的には寄与しない費用である。

なお、情報セキュリティ事故対応コストは、発生しない方が望ましいコストである。



[2]情報システムに対する各種インシデントには業界毎に特徴があり、発生したインシデントに関する情報を業界内で分析・共有することが情報セキュリティ対策の上で非常に有効と考えられている。このような考え方に基づき、米国においては、通信、金融などの重要インフラ業界において ISAC（Information Sharing and Analysis Center）の活動が存在し、日本においても Telecom-ISAC Japan が設立されている。

（7）その他コスト

情報セキュリティ対策コストのうち、これまで列挙した項目には当てはまらないコストである。例えば、企業外での情報セキュリティ事故や脆弱性情報の収集コストなどである。

なお、その他情報セキュリティ対策に関連するコストを開示する場合には、その内容、対象範囲、分類の根拠を明記することとする。

ところで、上記の分類は絶対的なものではなく、

(a) 組織的コスト、人的コスト、物理的コスト、技術的コストによる分類

(b) 外部調達を伴うもの、内部コストとなるものによる分類

(c) 情報システム系部門に関わるコスト、その他の部門に関わるコストによる分類

(d) 技術的・直接的にシステムを設置・運用するコスト、間接的に付随するコストによる分類

などが考えられる。

さらにコストの詳細な分類にあたっては、JISX5080 や情報セキュリティ管理基準との対応づけを図ることにする。これにより、情報セキュリティ対策として、ISMS 認証制度を取得し推進している企業や情報セキュリティ監査を受けている企業等にとっては、現在の情報セキュリティ確保のための活動の延長線上に「情報セキュリティ会計」を位置づけることができるため、一貫性があり、会計情報や効果の測定に多いにメリットがある。さらに、自己の活動を開示していくための手がかりにもなる。

具体的には、事業エリア内コストは JISX 5080 の 7 物理的及び環境セキュリティ、8 通信及び運用管理、9 アクセス制御、10 システムの開発及び保守と主に対応する。取引先・委託先等に対する情報セキュリティ対策コストは 4.3 外部委託と主に対応する。管理活動コストは 3 セキュリティ基本方針、4 組織のセキュリティ、5 資産の分類及び管理、6 人的セキュリティ、11 事業継続管理、12 適合性と主に対応する。

表２　JIS X 5080 の分類とコスト分類との対応

JISX 5080 の分類	コスト分類
セキュリティ基本方針	管理活動コスト
組織のセキュリティ	管理活動コスト、取引先・委託先等に対する情報セキュリティ対策コスト
資産の分類および管理	管理活動コスト
人的セキュリティ	管理活動コスト
物理的及び環境的セキュリティ	事業エリア内コスト
通信および運用管理	事業エリア内コスト
アクセス制御	事業エリア内コスト
システムの開発および保守	事業エリア内コスト
事業継続管理	管理活動コスト
適合性	管理活動コスト

3.1.3 情報セキュリティ対策コストの集計方法

情報セキュリティ対策コストの把握は、直接識別できる場合と複合コストとして認識される場合がある。複合コストとは、情報セキュリティ対策コストとそれ以外のコストとが結合した投資額及び費用額とする。

（１）直接識別できる場合は、当該額を情報セキュリティ対策コストとして集計する。

（２）複合コストの場合は、次のとおりの優先順位に従い、いずれかの方法で集計する。

ア　差額集計

情報セキュリティ対策コスト以外のコストを控除した差額を集計する。

イ　合理的基準による按分集計

差額集計できない情報セキュリティ対策コストについては、支出目的による合理的な按分基準を定めて按分集計する。

合理的な基準による按分比率の設定方法

（１）人件費の場合

実際の職務内容と情報セキュリティ対策との関係を考慮して、例えば兼務職員の場合に一定期間の労働時間配分比率等を用いる。

（２）減価償却費の場合

情報セキュリティ対策のための特定の機能の取得価額が、当該設備全体の取得価額に占める割合や面積比等を用いる。

ウ　簡便な基準による按分集計

差額集計も合理的基準による按分集計もできない情報セキュリティ対策コ

ストについては、簡便な按分比率を定めて按分集計する。

簡便な基準による按分比率の設定方法

（1）複合コストの主たる部分が情報セキュリティ対策コストであると認められる場合は、全額を集計することができる。

（2）情報セキュリティ対策コストの全体に占める割合が僅少であると認められる場合は、当該コスト項目の集計額をゼロとすることができる。

（3）情報セキュリティ対策コストが相当の割合で含まれていると認められる場合は、例えば、10%、50%のように一定割合を集計すべき額とみなすことができる。これらにより設定した比率は、その根拠とともに基本となる重要な事項として記載する。

3.2 情報セキュリティ対策効果

3.2.1 情報セキュリティ対策効果に関する基本的な考え方

情報セキュリティの取り組みは、組織にとって何らかの利益を生じさせる他の組織活動とは異なり、情報資産に対する問題を生じさせないことが最大の目的である。情報セキュリティの目的をその定義[3]からなぞると、「情報資産の機密性[4]、完全性[5]、可用性[6]を維持すること」であり、情報セキュリティの取り組みを通じて当該組織の使命と事業目標を達成可能にすることであるといえる。

情報セキュリティ対策の効果を考える場合、情報セキュリティの取り組みが間接的ではあるが組織の事業目標の達成に寄与するとはいえども、直接的な効果は情報資産の問題をどの程度発生させなかったか、つまり、機密性、完全性、可用性の損失をどの程度減少させたかという点で把握することが合理的である。

近年、米国の研究機関等において情報セキュリティにおける投資回収率（ROI：Return On Investment）、いわゆる ROSI の算定に関する研究が進められており、セキュリティ対策の効果算定も「困難ではあるが不可能ではない」といわれはじめている。ROSI の算定方法は各研究機関等によって異なるが、多くはセキュリティ対策コストと年間損失予測（ALE：Annual Loss Expectancy）[7]に基づいており、セキュリティ対策の効果を算定することは、すなわち、損失を減少させた程度を算定することを意味する。

---

[3]『情報セキュリティポリシーに関するガイドライン（内閣官房情報セキュリティ対策推進会議、2000 年）』より引用。

[4] 情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

[5] 情報及び処理方法の正確さ及び完全である状態を安全防護すること。

[6] 許可された利用者が、必要なときに情報にアクセスできることを確実にすること。

[7] 1977 年に米国連邦標準技術局（NIST：National Institute of Standards and Technology）が推奨した定量的リスク分析手法のこと。

3.2.2 情報セキュリティ対策効果の算定基準

情報セキュリティ会計において情報セキュリティ対策の効果を明らかにする場合、2 つのアプローチが考えられる。1 つは、情報資産の価値や脆弱性、脅威の発生可能性を定量化し、ALE として損失額を積み上げて情報セキュリティ対策効果を算定するホワイトボックス型のアプローチである。もう 1 つは、情報漏洩事故やシステム障害の発生件数等を情報セキュリティにおける重要業績評価指標（KPI：Key Performance Indicator）[8]として設定し、事故発生件数等の減少度合いを数値化するブラックボックス型のアプローチである。

組織において情報セキュリティ対策が進展しない理由の一つとして、情報セキュリティ問題が発生した場合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であるという指摘がある。経営者の視点から情報セキュリティ対策を考えると、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曖昧な状況である。

組織にとって「適切な水準」での情報セキュリティ対策を実施するためには、指標となるべくリスクの定量化が必要である。上記のいずれのアプローチも、国内外の機関等にて算定基準が研究されている一方で、まだ「決定打」や「万能薬」となるような案は発表されていないのが現実である。本報告においても新たな研究結果や推奨案を示すには至らないが、算定基準の基本的な考え方について以下にご紹介する。

（1）ホワイトボックスアプローチ

ホワイトボックス型のアプローチとは、組織が保有する情報資産の各々の価値や情報資産における脆弱性、情報資産の機密性、完全性、可用性を脅かす脅威の発生可能性を定量化し、ALE として損失額を算出することにより、情報セキュリティ対策効果を算定する方法である。一般的な算定式は以下の通りである。

$$\text{ALE} = \frac{\text{〔1 回の予想損失額：SLE〕} \times \text{〔損害の年間予想発生回数：ARO〕}}{\text{SLE} = \text{〔資産価値：AV〕} \times \text{〔起こりうる損害の可能性：EF〕}}$$

1 回の予想損失額（SLE：Single Loss Expectancy）は資産価値（AV：Asset Value）と起こりうる損害の可能性（EF：Exposure Factor）の積から算出する。資産価値（AV）は、当該情報資産における固定資産としての価値ではなく、当該情報資産に対するビジネス上の重要度から判断する。また、起こりうる損害の可能性（EF）

[8] 企業目標やビジネス戦略を実現するために設定した具体的な業務プロセスをモニタリングする指標の 1 つであり、どの程度実行されているかを定量的に計測するもの。

は、機密性、完全性、可用性が損なわれたことによる直接的な損害額（機会損失による逸失利益、機密情報の漏洩や誤報による賠償額など）と通常の管理状態に回復させるための復旧コストから算出する。

一方、損害の年間予想発生件数（ARO：Annualized Rate of Occurrence）は、脅威そのものの発生可能性と情報資産における脆弱性より算出される年間予想発生件数（固有リスクに基づく発生件数）から、情報資産に施されたコントロールにより抑止される数を減算することで算出した件数（残余リスクに基づく発生件数）とする。例えば、Web サーバーに対してファイアウォール等のアクセス制御措置を施すことによって年間の不正アクセス件数が減った場合は、その減った後の件数が ARO になる。

ホワイトボックス型のアプローチには、上記のほか、平成 17 年 3 月に経済産業省の商務情報政策局情報セキュリティ政策室より公表された『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 報告書』の参考資料④『リスク定量化に関する検討資料』においても、「リスク定量化に関する検討事例」として以下のような方法が紹介されているほか、当該ワーキンググループにおける検討結果として「停止リスク曲線による被害量算定モデル」[9]が掲載されている。

- ■コンピュータウイルス被害総額（独立行政法人情報処理推進機構）[10]
- ■インシデント被害額・情報漏えい被害額（NPO 日本ネットワークセキュリティ協会）[11]
- ■新 BIS 規制に伴う「オペレーショナルリスク」定量化[12]

前述の通り、組織の経営者における投資判断に必要なリスクの定量化手法は、未だ確立した手段というものがない状況である。組織におけるセキュリティ会計導入に際して、ホワイトボックスアプローチを採用する場合は、ALE の算定を含めた、上記のようなリスク定量化手法について自組織への適合性を十分に検証す

---

[9] 情報システムがある時点で停止している確率を各種調査等から各事故事象でのシステム停止時間の項目を入手して求め（停止リスク曲線）、これに企業毎の 1 日の利益に与える影響度、事故の年間発生確率、セキュリティ対策を講じることにより低減されるリスクの比率を掛け合わせて、年間の被害量を概算する算定モデル。

[10] 独立行政法人情報処理推進機構（IPA）より 2004 年 4 月に公表された『国内･海外におけるコンピュータウィルス被害状況調査 被害額推進報告書』にて掲載された算出方法。我が国におけるコンピュータウィルス被害総額を推計する方法であり、インシデント被害額を「表面化被害額」と「潜在化被害額」の和から算出する。推計に必要なパラメータは、事業者アンケートから得られたデータを用いている。

[11] JNSA より 2004 年 3 月に公表された『2003 年度情報セキュリティインシデントに関する調査報告書』にて掲載された算出方法。インシデント被害額はＩＰＡ被害算出モデルをベースに策定しているが、情報漏えいによる被害想定として、損害賠償額を基礎情報価値、機微情報度、本人特定容易度、情報漏えい元組織の社会的責任度、事後対応評価の積から算出する。

[12] 国際決済銀行（BIS：Bank for International Settlements）が定めた、国際業務を行う民間銀行の自己資本比率に関する国際統一基準のこと。バーゼル合意とも呼ばれ、達成できない銀行は、国際業務から事実上の撤退を求められる。新 BIS 規制は、リスクの計測方法として、オペレーショナルリスクを損失分布手法等により定量化することが挙げられている。

る必要がある。

（２）ブラックボックスアプローチ

ブラックボックス型のアプローチとは、情報漏洩事故やシステム障害の発生件数といった情報セキュリティ問題の発生を対象にした評価指標（KPI）を設定し、事故発生件数等の減少度合いを数値化することにより、情報セキュリティ対策効果を算定する方法である。

評価指標としては、通常のシステム運用にて集計・管理しているような障害発生件数や稼働率（平均回復時間（MTTR：Mean Time To Repair)、平均故障間隔（MTBF：Mean Time between Failure）より算定)、不正アクセス件数、コンピュータウイルスの感染件数はもちろんのこと、ユーザーによる情報セキュリティポリシー違反（未許可の情報資産の持ち出し等）の件数や、個人情報保護における顧客からの苦情・問合せ件数といった非技術的な指標も有効である。

また、上記のような「脆弱性の減少」というマイナス面の減少の観点から抽出された評価指標のほか、下記の図３のように、「損害検知性能の向上」や「情報資産の許容保有量の増加」といった、副次的なプラスの効果の観点からの評価指標の抽出も可能である。

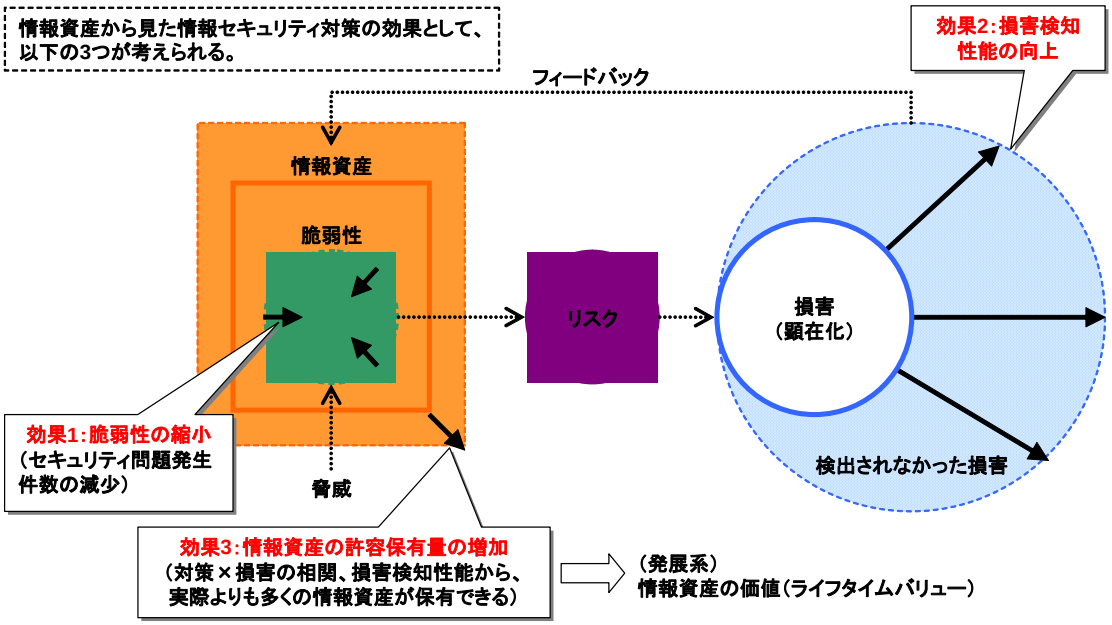


図3　情報セキュリティ対策の効果の考え方

いずれにせよ、ブラックボックスアプローチにおける評価指標は、客観的な視点で定量データとして測定が可能な項目や自動的に測定可能な項目、測定した結

果の保存や収集が容易な項目等を選択し、評価作業を効率化できるよう工夫することが望まれる。

3.2.3 情報セキュリティ対策効果の報告モデル

本節の最後に、本報告書第 1 章にて提示した「情報セキュリティ会計キューブ」に従い、ブラックボックス型のアプローチによる情報セキュリティ対策効果の報告モデルの考え方を説明する。

前述の通り、情報セキュリティにおける本来の目的は「情報資産の機密性、完全性、可用性を維持すること」であるが、ブラックボックス型のアプローチによって情報セキュリティ対策効果を算定する場合には、事業単位や事業活動ごとの単位で把握可能な明確な目標に沿って算定することが、経営者や顧客などの「報告を受ける者」にとっての理解のしやすさの面で効果的である。

本報告書 1.5 節で挙げた情報セキュリティ会計キューブにおける目的と、目的毎の評価指標の例を表 3 に示す。

最後に、組織において情報セキュリティ対策効果を算定する場合には、ホワイトボックス型、ブラックボックス型のいずれのアプローチを採用するにも関わらず、その前提として、組織におけるセキュリティ上の問題の発生件数や対処にかかったコストなど、自組織における効果算定に必要な数値を日々蓄積し管理していくことが重要であることを留意していただきたい。

表3　本報告における情報セキュリティ対策効果の評価指標

No.	目的	対象	評価指標
1	個人情報保護	特定部署／特定事業活動／全社レベル	個人情報に関する苦情・問合せ件数
			個人情報漏洩事故発生件数
			個人情報への不正アクセス件数　など
2	企業機密情報保護	特定部署／特定事業活動／全社レベル	機密情報漏洩事故発生件数
			機密情報への不正アクセス件数
			機密情報保管場所への不正な入退室件数など
3	事業継続	全社レベル	緊急対策本部設置に要した時間
			事業再開（暫定復旧）までに要した時間
			事態の収束までに要した時間　など
4	ネットワーク秩序維持	特定部署／特定事業活動	外部に発信した不正パケットの量
			Web ページの改竄被害件数　など
5	その他	特定部署／事業活動	特定システムの障害発生件数
			特定システムの稼働率
		特定部署／特定事業活動／全社レベル	コンピュータウイルスの感染件数
			ユーザーによる情報セキュリティポリシー違反件数　など

※　評価指標については、今後、本ワーキンググループにて、より網羅的に抽出することが課題となる。

４．　今後の展望

情報セキュリティに対する社会全般の意識が向上し、顧客や取引先などのステークホルダに対する説明責任を果たすため、企業は自らの情報セキュリティへの取り組みを積極的に情報開示することが求められるだろう。さらに、こうした企業の取り組みを第三者機関が適正に評価するための仕組みも必要になってくるだろう。一方、情報セキュリティレベルの維持・向上に継続的に取り組んでいくためには、社会的な後押しやある種のインセンティブの供与なども検討すべきであろう。

これらを支えるのが、情報セキュリティ会計であると考える。

以下に、想定される情報セキュリティ会計の導入イメージ、並びに波及効果を示す。

(1)内部管理への適用

米国では、連邦情報セキュリティ管理法（FISMA：Federal Information Security Management Act）により、各省庁が毎年、自省庁における情報セキュリティ対策の状況を分析・評価し、その結果を行政管理予算局(OMB：Office of Management and Budget)に報告することになっており、セキュリティ対策に係る内部管理の仕組みが既にできている。

ところで、上記はまさに好例であるが、その本質は自身の情報セキュリティ対策の金額把握を行っている点にある。種々の既発表の調査報告書を見ても、情報セキュリティ対策に係る費用・投資額の定義が未だ曖昧なようである。

当ＷＧが取り組む情報セキュリティ会計は外部に対する伝達を目指しているが、そのレベルに到達するにはまだまだ障壁がある。そのため、まずは内部管理のためのツールとしてお役立ていただきたいと思う。また、ISMS 認証制度では費用対効果の検証が規定されており、既取得事業所等にも利用していただきたい。

(2)情報セキュリティ監査の利用促進

情報セキュリティ会計の導入による波及効果として、情報セキュリティ監査の利用促進が考えられる。今後、多くの企業で情報セキュリティ会計が導入され、積極的に公開する環境が構築されるようになると、それが適正に作成されたものであるかの第三者による評価・承認が求められるであろう。さらには、そのデータの真性を保証すべく、情報セキュリティ監査が実施され、その監査結果を情報セキュリティ報告書や有価証券報告書などに記載する企業が現れてくることも予想される。将来的には、情報セキュリティ会計＋情報セキュリティ監査が証券取引所における上場基準になるかもしれない。

(3)情報セキュリティ確保に向けた取り組みに係る報告書との連携

近年、企業にとって情報セキュリティ対策は、企業が果たすべき社会的責任(CSR)の１つとして捉えられている。既に、自社の情報セキュリティ確保に向けた取り組みを、個人情報保護と併せて、CSR 報告書や社会環境報告書などに記載する日本企業の事例も出て来ている。また、経済産業省は、「企業における情報セキュリティガバナンスのあり方に関する研究会」にて、情報セキュリティ報告書を提唱し、そのモデルを策定した。こうして企業の情報セキュリティの取り組みを情報開示するための環境が整いつつある。

当ＷＧが取り組む情報セキュリティ会計は、これらの報告書と密接に連携するものである。コーポレートコミュニケーションの観点から、情報セキュリティに積極的に取り組む企業において、情報セキュリティ会計が自発的・戦略的に導入されることを期待する。

(4)情報セキュリティ融資に係る優遇金利の適用

ネットワークでつながった IT 社会の一員として、環境同様、企業はネットワーク秩序維持という社会的責任を担っている。すなわち、企業が情報セキュリティ対策に取り組むとき、その目的は広くネットワーク秩序維持にも及ぶと言える。そこで、これを支援する仕組みが必要になってくる。

ところで、日本政策投資銀行は、「環境配慮型経営促進事業」として、環境に配慮した経営を推進する企業に対して、その企業の環境配慮の度合いに応じた金利による融資制度を行っている。

このスキームを情報セキュリティにも展開させることができないだろうか。すなわち、情報セキュリティに積極的に取り組む企業に対して、融資を行う制度である。このとき、当該企業の取り組み度合いを評価する“ものさし”として、情報セキュリティ会計が利用できるものと考えられる。

(5)情報資産の価値評価

情報セキュリティの真髄は、まさに“情報資産の適正な活用と保護（守ること）”にある。

多くの企業は日常的に大量の顧客情報を保有し、それを事業活動に活用している。ダイレクトマーケティングの観点から言うと、顧客の属性などに応じたセールスプロモーションを行い、顧客一人一人のライフタイムバリューの最大化を追及しているということになる。そして、顧客価値はセールスプロモーション費用などのマーケティングコストに対するリターンで評価できる。ただし、このときのマーケティングコストには、顧客情報を守る、あるいは顧客に「安全・安心」を訴求するための情報セキュリティコストはほとんど考慮されていない。

情報セキュリティ会計を導入することにより、情報セキュリティコストが把握でき、顧客情報の資産価値が評価できる。さらに、リスクの定量化などが実現できれば、現在保有する情報資産の割安・割高が評価できるようになるだろう。近い将来には、情報資産の証券化も実現するかもしれない。

さいごに

情報セキュリティ会計は、未だ完成された研究・開発テーマではない。今後も、果敢にチャレンジし、「情報セキュリティ会計ガイドライン」を策定したいと考えている。

併せて、JNSA 内の他ワーキンググループや外部機関などとも積極的に連携していくことも必要であると考えている。将来的には、情報セキュリティ会計の普及や社会環境整備など、これを起点に、種々の波及テーマにも取り組んでいきたいと考えている。

初年度にあたる 2004 年度は、多くの方々から貴重なご助言をいただいた。この場を借りて、厚くお礼を申し上げたい。

当ワーキンググループのチャレンジが、企業における情報セキュリティ対策のレベルの向上、さらには企業価値の向上につながれば幸いである。

付属資料

Ａ．情報セキュリティ対策コストの公表用フォーマット

情報セキュリティ対策コストの公表用フォーマットを以下に例示する。

	取り組み内容	投資額	費用額	計
(1)事業エリア内コスト				
(2)取引先・委託先等に対する情報セキュリティ対策コスト				
(3)管理活動コスト				
(4)研究開発コスト				
(5)社会活動コスト				
(6)情報セキュリティ事故対応コスト				
(7)その他コスト				
合計				

B．情報セキュリティ対策における詳細コスト集計表

情報セキュリティ対策におけるコストを詳細に管理・把握する際に活用していただけるよう、詳細コスト集計表を例示する。

この詳細コスト集計表は、当該企業の実態に即して、どのような取り組みを対象とするのかを検討した上で、対象とする事業活動や事業単位ごとに利用していただきたい。

(1) セキュリティ基本方針

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	（合計）
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費（他物件費）	内部人件費	その他		
情報セキュリティ基本方針 (3.1)										
情報セキュリティ基本方針文書 (3.1.1)										
見直し及び評価 (3.1.2)										

(2)組織のセキュリティ

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	（合計）
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費（他物件費）	内部人件費	その他		
情報セキュリティ基盤 (4.1)										
情報セキュリティ運営委員会 (4.1.1)										
情報セキュリティの調整 (4.1.2)										
情報セキュリティ責任の割り当て (4.1.3)										
情報処理設備の認可手続き (4.1.4)										
専門家による情報セキュリティの助言 (4.1.5)										
組織間の協力 (4.1.6)										
情報セキュリティの他者によるレビュー (4.1.7)										
第三者によるアクセスのセキュリティ (4.2)										
第三者のアクセスから生じるリスクの識別 (4.2.1)										
第三者との契約書に記載するセキュリティ要求事項 (4.2.2)										

(3)資産の分類および管理

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	（合計）
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費（他物件費）	内部人件費	その他		
資産に対する責任 (5.1)										
資産目録 (5.1.1)										
情報の分類 (5.2)										
分類の指針 (5.2.1)										
情報ラベル付け及び取り扱い (5.2.2)										

(4) 人的セキュリティ

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	(合計)
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費(他物件費)	内部人件費	その他		
職務定義及び雇用におけるセキュリティ (6.1)										
セキュリティを職責にふくめること (6.1.1)										
要員審査およびその個別方針 (6.1.2)										
機密保持契約 (6.1.3)										
雇用条件 (6.1.4)										
利用者の訓練 (6.2)										
情報セキュリティの教育及び訓練 (6.2.1)										
セキュリティ事件・事故および誤動作への対処 (6.3)										
セキュリティ事件・事故の報告 (6.3.1)										
セキュリティの弱点の報告 (6.3.2)										
ソフトウェアの誤動作の報告 (6.3.3)										
事件・事故からの学習 (6.3.4)										
懲戒手続き (6.3.5)										

(5) 物理的及び環境的セキュリティ

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	(合計)
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費(他物件費)	内部人件費	その他		
セキュリティが保たれた領域 (7.1)										
物理的セキュリティ境界 (7.1.1)										
物理的入退管理策 (7.1.2)										
オフィス、部屋および施設のセキュリティ (7.1.3)										
セキュリティが保たれた領域での作業 (7.1.4)										
受渡し場所の隔離 (7.1.5)										
装置のセキュリティ (7.2)										
装置の設置および保護 (7.2.1)										
電源 (7.2.2)										
ケーブル配線のセキュリティ (7.2.3)										
装置の保守 (7.2.4)										
事業敷地外における装置のセキュリティ (7.2.5)										
装置の安全な処分または再利用 (7.2.6)										
その他の管理策 (7.3)										
クリアデスクおよびクリアスクリーンの個別方針 (7.3.1)										
資産の移動 (7.3.2)										

(6) 通信および運用管理

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	(合計)
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費(他物件費)	内部人件費	その他		
運用手順および責任 (8.1)										
操作手順書 (8.1.1)										
運用変更管理 (8.1.2)										
事件・事故管理手順 (8.1.3)										
職務の分離 (8.1.4)										
開発施設および運用施設の分離 (8.1.5)										
外部委託による施設管理 (8.1.6)										
システム計画の作成および受入れ (8.2)										
容量・能力の計画作成 (8.2.1)										
システムの受入れ (8.2.2)										
悪意のあるソフトウェアからの保護 (8.3)										
悪意のあるソフトウェアに対する管理策 (8.3.1)										
システムの維持管理 (8.4)										
情報のバックアップ (8.4.1)										
運用の記録 (8.4.2)										
障害記録 (8.4.3)										
ネットワークの管理 (8.5)										
ネットワーク管理策 (8.5.1)										
媒体の取扱いおよびセキュリティ (8.6)										
コンピュータの取外し可能な附属媒体の管理 (8.6.1)										
媒体の処分 (8.6.2)										
情報の取扱い手順 (8.6.3)										
システムに関する文書のセキュリティ (8.6.4)										
情報およびソフトウェアの交換 (8.7)										
情報およびソフトウェア交換契約 (8.7.1)										
配送中の媒体のセキュリティ (8.7.2)										
電子商取引のセキュリティ (8.7.3)										
電子メールのセキュリティ (8.7.4)										
電子オフィスシステムのセキュリティ (8.7.5)										
公開されているシステム (8.7.6)										
情報交換のその他の形式 (8.7.7)										

(7)アクセス制御

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	（合計）
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費（他物件費）	内部人件費	その他		
アクセス制御に関する業務上の要求事項 (9.1)										
アクセス制御方針 (9.1.1)										
利用者のアクセス管理 (9.2)										
利用者登録 (9.2.1)										
特権管理 (9.2.2)										
利用者のパスワードの管理 (9.2.3)										
利用者アクセス権の見直し (9.2.4)										
利用者の責任 (9.3)										
パスワードの使用 (9.3.1)										
利用者領域にある無人運転の装置 (9.3.2)										
ネットワークのアクセス制御 (9.4)										
ネットワークサービスの使用についての個別方針 (9.4.1)										
指定された接続経路 (9.4.2)										
外部から接続する利用者の認証 (9.4.3)										
ノードの認証 (9.4.4)										
遠隔診断用ポートの保護 (9.4.5)										
ネットワークの領域分割 (9.4.6)										
ネットワークの接続制御 (9.4.7)										
ネットワーク経路を指定した制御 (9.4.8)										
ネットワークサービスのセキュリティ (9.4.9)										
オペレーティングシステムのアクセス制御 (9.5)										
自動の端末識別 (9.5.1)										
端末のログオン手順 (9.5.2)										
利用者の識別および認証 (9.5.3)										
パスワード管理システム (9.5.4)										
システムユーティリティの使用 (9.5.5)										
利用者を保護するための脅迫に対する警報 (9.5.6)										
端末のタイムアウト機能 (9.5.7)										
接続時間の制限 (9.5.8)										
業務用ソフトウェアのアクセス制御 (9.6)										
情報へのアクセス制御 (9.6.1)										
取扱いに慎重を要するシステムの隔離 (9.6.2)										

(8)システムの開発および保守

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	（合計）
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費（他物件費）	内部人件費	その他		
システムのセキュリティ要求事項 (10.1)										
セキュリティ要求事項の分析及び明示 (10.1.1)										
業務用システムのセキュリティ (10.2)										
入力データの妥当性確認 (10.2.1)										
内部処理の管理 (10.2.2)										
メッセージ認証 (10.2.3)										
出力データの妥当性確認 (10.2.4)										
暗号による管理策 (10.3)										
暗号による管理策の使用に関する個別方針 (10.3.1)										
暗号化 (10.3.2)										
ディジタル署名 (10.3.3)										
否認防止サービス (10.3.4)										
鍵管理 (10.3.5)										
システムファイルのセキュリティ (10.4)										
運用ソフトウェアの管理 (10.4.1)										
システム試験データの保護 (10.4.2)										
プログラムソースライブラリへのアクセス制御 (10.4.3)										
開発及び支援過程におけるセキュリティ (10.5)										
変更管理手順 (10.5.1)										
オペレーティングシステムの変更の技術的レビュー (10.5.2)										
パッケージソフトウェアの変更に対する制限 (10.5.3)										
隠れチャネル及びトロイの木馬 (10.5.4)										
外部委託によるソフトウェア開発 (10.5.5)										

(9)事業継続管理

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	（合計）
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費（他物件費）	内部人件費	その他		
事業継続管理種々の面 (11.1)										
事業継続管理手続 (11.1.1)										
事業継続及び影響分析 (11.1.2)										
継続計画の作成及び実施 (11.1.3)										
事業計画作成のための枠組み (11.1.4)										
事業継続計画の試験、維持及び再評価 (11.2)										
計画の試験 (11.2.1)										
計画の維持及び再評価 (11.2.2)										

(10)適合性

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	(合計)
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費(他物件費)	内部人件費	その他		
法的要求事項への適合 (12.1)										
適用法令の識別 (12.1.1)										
知的所有権(IPR) (12.1.2)										
組織の記録の保護 (12.1.3)										
データの保護及び個人情報の保護 (12.1.4)										
情報処理施設の誤用の防止 (12.1.5)										
暗号による管理策の規制 (12.1.6)										
証拠の収集 (12.1.7)										
セキュリティ基本方針及び技術適合のレビュー (12.2)										
セキュリティ基本方針との適合 (12.2.1)										
技術適合の検査 (12.2.2)										
システム監査の考慮事項 (12.3)										
システム監査管理策 (12.3.1)										
システム監査ツールの保護 (12.3.2)										

(11)研究開発コスト

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	(合計)
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費(他物件費)	内部人件費	その他		

(12)社会活動コスト

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	(合計)
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費(他物件費)	内部人件費	その他		

(13)情報セキュリティ事故対応コスト

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	(合計)
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費(他物件費)	内部人件費	その他		

(14)その他コスト

	取り組み内容	投資額(初期構築時)			費用額(ランニング費用)				廃棄費用	
		無形又は有形固定資産勘定	物件費	内部人件費	減価償却費	設備リース費（他物件費）	内部人件費	その他		（合計）