情報セキュリティ対策の効果測定

Effectiveness Measurement of Information Security Measures

柏　浦　謙　一

要　約　昨今の情報セキュリティ・インシデント（事件事故）を受け，個々の情報システムだけでなく，企業が保有する情報資産の保護を含め全般的な活動に対しても情報セキュリティ（エンタープライズ・セキュリティ）水準を向上させることが求められている．

政府としても国家全体の情報セキュリティ水準の底上げを目指し，様々な政策や戦略を提示することで，官民一体となった対応に乗り出しているが，新たな脅威の出現や社会情勢の変化，技術の進歩に対応すべく，企業の現場では様々な努力が払われている一方で，対策を実施することが目的化している実情が見て取れる．

また，どこまで対策を実施すれば十分なのかという迷いとあいまって，担当者は利便性への要求と高セキュリティ化の要求の狭間で悩んでいる．

こういった状況から脱却するためにも，現状の情報セキュリティ対策の効果を認識し，その妥当性の検証と改善のためのプロセスを確立することで，各組織で必要とされる情報セキュリティ対策を見極める必要がある．

Abstract　In response to recent information security incidents, it is expected to improve levels of information security (Enterprise security) for overall activities including information assets possessed by not only individual information systems but also the enterprise.

The Japanese government has presented also various policies and the strategies, and launched activities hand-in-hand with private sectors, aiming at raising levels of the information security of the nation as a whole, however, it shows facts that the various efforts have been made by the operational level within a company in order to respond to the occurrence of the new types of threat and changes in of social conditions, and the technological advances, while their efforts are geared principally to implementation of security measures.

In addition, information security staff members are torn between the demand for convenience and one for the high security, as well as they have the hesitation whether the extent to which they implement security measures is adequate.

To get rid of such a situation, the enterprise should ascertain the information security measures needed in various departments by recognizing the effectiveness of current information security measures, and establishing the process for validating effectiveness and improving security measures.

1. は　じ　め　に

顧客やプロジェクト関係者から「情報セキュリティ対策をどの程度まで実施すれば十分か」という問いかけを多く受ける．

これに答えることは，情報セキュリティを担保できると考えられる水準（対策レベル）が，顧客や組織，情報システムによってまちまちであり，対象が変わるたびにその都度検討しなけ

ればならないという点で難しい．また，業務を遂行する上で求められる機能が顧客や開発者との間で共有しやすいのにくらべ，非機能要件に分類される情報セキュリティ要件は，ステークホルダー間での合意形成に手間取り，ともすれば検討が後回しにされかねない．結果的にITセキュリティ製品を適用するだけとなり，それが適切であり必要な対策かどうかという評価が疎かになる．

一方，個々のシステムに限らず企業全体を俯瞰すると，個々人の意識や職種，組織の業務，社内業務システムの違いにより対策の実施方針が異なる．ある組織では必要な対策が，他では不要だという場面である．例えば，製品化前の設計図を持つ設計部門は，外部とは隔絶された状態の独立した区画で，厳格な入退管理や情報の持ち出し制限，情報の暗号化対策を実施しているかもしれない．情報セキュリティ対策は，その部門が取り扱う情報の価値に応じて行われるが，それが果たして必要であったか，という評価を行なっている組織はどの程度あるか疑問である．

本稿では，個々の情報システムにとらわれることなく，企業全体における情報セキュリティ対策（エンタープライズ・セキュリティ）の実施プロセスのうち，有効性と妥当性を評価するための判断指標について検討を行なう．これは，PDCAサイクル（Plan－Do－Check－Act）の“Check”で必要とされるものである．

2. 企業に求められる情報セキュリティ対策

2006年2月に内閣官房情報セキュリティセンター（NISC；National Information Security Center）は，「第1次情報セキュリティ基本計画」[1]を公表した．その中で，現代の高度情報化社会を構成する主体として四領域（政府機関・地方公共団体，重要インフラ，企業，個人）に分類し，各領域別に重点施策を示している．四領域のうち「企業」に対して掲げられている目標は，「2009年度初めに，企業における情報セキュリティ対策の実施状況を世界トップクラスの水準にすることを目指す」というもので，官民一体となって情報セキュリティ対策の強化が進められている．

2.1 政府が示す情報セキュリティ対策への取り組み

企業に対して掲げた目標を実現させるため，政府が示した重点施策は，次の四点である[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
- 質の高い情報セキュリティ関連製品及びサービスの提供促進
- 企業における情報セキュリティ人材の確保・育成
- コンピュータウイルスや脆弱性等に早期に対応するための体制の強化

このうち，「質の高い情報セキュリティ関連製品及びサービスの提供促進」において，政府は企業における情報セキュリティ対策への取り組みの実情を，次のように分析している[1]．

- 情報セキュリティ対策は，本来業務を達成するために必要な機能とは異なる機能を，リスクに応じて講じていく性質のものである
- 対策そのものを可視化しにくい特性を持つことから，企業が情報セキュリティ対策を講ずる際には，理解のしやすい形で必要な対策を選択できる環境が整備される必要がある

これらは，各企業の経営層・上位マネジメント層から現場の情報セキュリティ担当者に至る

まで，共通した認識であろうと想像できる．政府は現状の課題を解決するための方向性を，重点施策として次のように示している[1]．

- 情報セキュリティ関連リスクに対する定量的評価手法の研究を推進する
- IT セキュリティ評価及び認証制度，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，情報セキュリティ監査といった第三者評価の活用を推進する

特に，定量化の問題については「セキュア・ジャパン 2006」[2]，「セキュア・ジャパン 2007」[3]で，具体的施策として「組織における情報セキュリティのリスクの定量化，情報セキュリティ対策に関する費用対効果の測定等の研究開発」を行うとしており，現在でもさまざまな定量化に関する考えが示されている*1．

2. 2　情報セキュリティ対策における定量化の意味

情報セキュリティ対策の分野で定量化について考える場合，リスクの視覚化を目的として，発生率やそれによって生じる損害額等を数値で表すことが多い．ISMS 適合性評価制度においても，情報資産に対する脅威や情報資産が潜在的に持つ脆弱性を見極め，リスクの特定・分析（リスクアセスメント）結果に基づいた対応を求めている．しかし，このリスクアセスメントの過程では，実施している対策がどのように効果（パフォーマンス）を発揮しているか，それが投資に見合ったものなのかが明確になりにくい．これは，一般的に機密性，完全性，可用性の視点から見て価値が損なわれる可能性のある情報資産を洗い出し，その価値が保全されるに十分な対策が実施されているか否かという評価・分析に重きがおかれているためである．情報資産の保護度合いを見極めるには重要な手法であるが，情報セキュリティ対策自体の実効性を把握したい人々（経営層や上位マネジメント層）には別の指標を提示する必要がある．

3.　企業における情報セキュリティ対策の取り組み

ISMS 認証を取得する組織は図 1 で示すように増加傾向にあるが，認証を受けるに至った各組織の動機は様々であろう．情報セキュリティ対策実施体制の構築や対策の実施状況の把握の

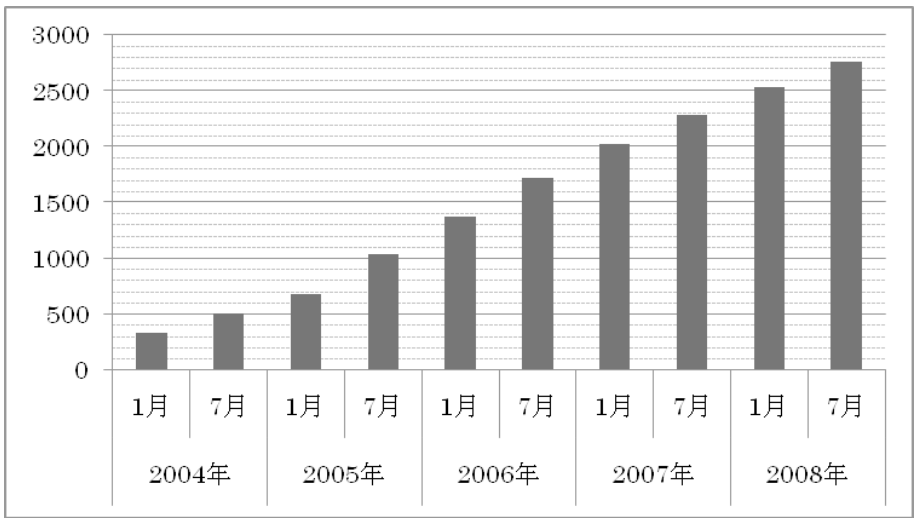

図 1　ISMS 認証取得組織数
（財団法人日本情報処理開発協会情報マネジメントシステム推進センターのデータ[4]を一部加工）

ため，顧客への対外的アピールのため，もしくは，取引先からの要求/入札要件として必要，といった例もあるかもしれない．ただ，動機は何であれ，ISMS認証取得のための作業を通して，情報セキュリティ対策の重要性や，その対策が軽視された状態であることが企業活動の根幹に関わる問題に発展しかねないことを認識するきっかけになったのではなかろうか．

3.1　情報セキュリティ対策と事業継続

そもそも企業の本質的な意義を考えた場合，企業・組織の存続や事業の継続は，企業の取り組むべき最優先事項の一つである．それは，リスクマネジメント，すなわち企業の危機管理能力なしに実現することはできない．他稿で紹介されているように，新型インフルエンザや地震等の自然災害対策と同様に，情報セキュリティ対策への要求はリスクマネジメントのための手段の一つと捉えることができる．ただし，対策の必要性や重要性は認識されているものの，その実施度合いは組織により異なっているだろう．

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報告書」[5][6]の中で，「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る」ことを目的に情報セキュリティガバナンスの必要性を説いているが，その確立を阻害する要因に次の課題を列挙している．

- IT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
- 既存の情報セキュリティへの「対策」「取り組み」が企業価値に直結していない
- 事業継続性確保の必要性が十分に認識されていない

いずれも上位マネジメント層が持つ悩みであろうと想像できる．研究会は報告書の中で，これらを克服する手段として，三つのツールを使うことを提案している．

- 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

詳細は報告書を参照すべきであるが，情報セキュリティ対策ベンチマークで自組織の対策度合いの自己評価を行い，情報セキュリティに係る推進体制や実績，今後の計画といった組織の取り組みを外部に向け発信・アピールする道具として情報セキュリティ報告書を活用するよう述べている．また，災害時や不慮の事故が発生し制約された環境下であっても企業活動を継続することを目標とする事業継続計画は，情報セキュリティ報告書と同様に企業の市場価値を高める効果も得られる，としている．

情報漏洩等により企業活動に多大な影響を及ぼしかねない状況において，事業継続計画は不可欠なものとなりつつあり，策定過程で情報セキュリティ対策の検討は避けては通れない．ISMS認証基準（JIS Q 27001: 2006）に対応した「情報セキュリティ対策ベンチマークVer.3.1」の中で，組織的，人的，物理的，技術的対策の実施状況の確認に加え，事件事故発生時の対応を問う構成になっていることからも，組織として存続するための方策・計画の立案が重要視されていることが推測できる．

情報セキュリティガバナンスを確立するため，三つのツールを活用するよう提言されているが，報告書や計画書を策定するプロセスを通して，情報セキュリティガバナンスの確立を促進する狙いもあるだろう．

3.2　情報セキュリティ管理者・担当者が求める対策評価指標

企業や各組織の情報セキュリティ管理者・担当者の多くは，何のために対策を実施すべきかを正しく認識している．ただし，それを具体化させていく過程でどの水準まで行うべきか，どのように運用していくべきか，新技術にどう取り組むか，といった上位マネジメント層とは異なった視点で悩みを抱えている．場合によっては，明確な基準がないまま目的と手段を取り違え，IT セキュリティ製品だけを導入して満足する状況であったり，過剰な対策を継続し効率性や利便性を犠牲にすることで，業務遂行能力を低下させてしまうのではと危惧している．それは総じて次の問題に起因していると考えられる．

- 情報セキュリティ対策の目標設定が曖昧
- 情報セキュリティ対策の効果を定量的に計測，継続的に評価する手段・手法が不足

この二つの問題のうち，目標設定については保護すべき情報資産やその組織のおかれている状況（業務内容を含む）によって目標とする姿が異なるため，独自に設定する必要がある．例えば，インターネットと物理的に遮断されている環境において，外部ネットワークからの不正侵入件数をゼロ件にするという目標は意味をなさない．

一方，計測・評価する手法については，実施・実装方法に差異があったとしても，それが果たす機能，若しくは求められる役割は共通しており，何らかの基準や尺度があれば，有効に機能しているか否かの識別は可能である．

次章では，企業活動の永続性を支えるために，情報セキュリティ対策がどのように貢献できるかという点を考慮しつつ，その貢献度（実効性/有効性）を確認するための評価指標を具体的に検討する．合わせて，IT セキュリティを含む情報セキュリティ対策の実効性を計る評価指標を導くことを試みる．

ISO/IEC2700 シリーズ，NIST SP800 シリーズ，COBIT 等情報セキュリティに関係した規格や規範が既に公開されているが，対策評価指標とすべき項目を検討する際に参考になる．

4.　情報セキュリティ対策評価指標

情報セキュリティ対策は実施したものの，果たしてそれが組織の情報セキュリティ評価の向上に寄与しているか判断が難しいというのは前述のとおりであり，拠り所となる定量的な指標や基準が求められる．この指標や基準を KGI（Key Goal Indicator；重要目標達成指標）や KPI（Key Performance Indicator；重要業績評価指標）として，各組織が目標とする数値を設定し，到達度を確認するとともに実績値の傾向を探ることで実効性/有効性の評価に利用する．

COBIT4.1 では，従来 KGI，KPI と表現していたものが，それぞれ，事実として認識された後に計測されるものとして“lag indicators”（結果指標）に，成果が事実として確定する前の状態でも計測できるものとして“lead indicators”（先行指標）に置き換えられた．厳密には KGI，KPI と異なった意味で用いられるが，本稿では情報セキュリティ目標の達成度と対策実施度のための評価指標を検討する趣旨で KGI，KPI を使用する．

4.1　企業を支える情報セキュリティ対策

企業が自身の活動を継続的に展開するために実践している，若しくは実践するのが望ましい次の五つの行動を企業を支える基本要素と捉え，企業の構成員が取り組むべき目的に設定す

る．

- 事業継続
- 営業利益拡大/コスト削減
- 人材育成
- 情報資産保護
- 法令遵守

それの達成度を計るために，数値表現可能な表現への展開過程の概要を図2に示す．情報セキュリティ対策がどのように貢献できるかという視点から，本章で述べる対策評価指標としてのKGI，KPIを導く過程を表現したものである．一部すでに数値表現される項目があるが，これはそのまま対策評価指標として利用できる．

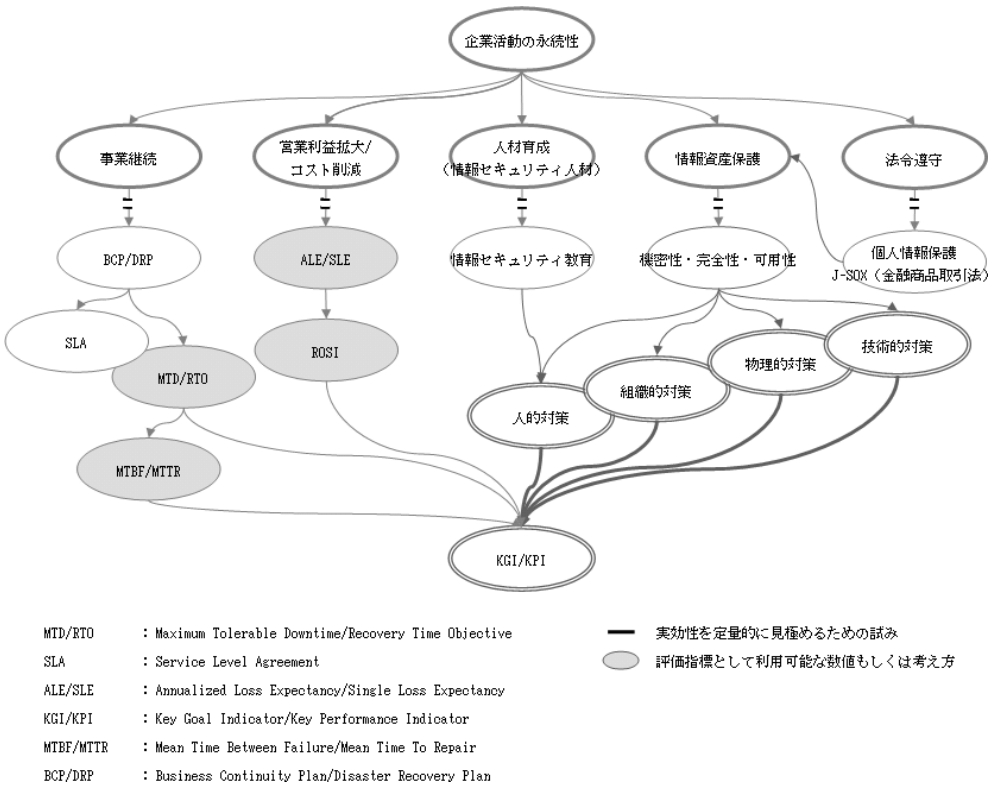

図2　情報セキュリティ対策評価指標導出概要図

4.2　情報セキュリティ対策評価項目の検討

4.1節で示した企業の永続的活動を支える五つの基本目的（事業継続，営業利益拡大/コスト削減，人材育成，情報資産保護，法令遵守）と，情報セキュリティの視点から見た目標及びその達成度を数値として表現可能な項目を表1に例示する．

表1　情報セキュリティ目標達成確認項目一覧

	目的	情報セキュリティ目標	情報セキュリティ対策評価指標項目
企業活動の永続性確保	事業継続	事業継続計画立案	最大許容事業停止時間（MTD）
			通常業務再開時間（RTO）
			緊急対策本部設置時間
	営業利益拡大/コスト削減	情報システムが貢献する利益/コスト削減	年間損失予想被害額（ALE）
			単一損失予想被害額（SLE）
			情報セキュリティ投資利益率（ROSI）
	人材育成	継続的な情報セキュリティ人材育成実施	情報セキュリティ関連資格取得者
			情報セキュリティポリシー、ISMS管理策等遵守率
			情報セキュリティポリシー違反者，違反回数
	情報資産保護	企業情報の機密性の確保	機密情報漏洩回数
			機密情報への権限外アクセス回数
		業務システムの可用性の確保	平均故障間隔（MTBF）
			平均復旧時間（MTTR）
			情報システムの障害回数
			情報システムの稼働率
			不正侵入・アクセス回数
			外部公開サーバ改竄回数
			ウィルス感染回数
	法令遵守	適切な個人情報保護の取り扱い	個人情報漏洩回数
			個人情報問い合わせ回数

表1は，対策評価指標として使用できる可能性がある項目を目標別に分類しただけであって，目標値に対して評価指標の実績値がどのような場合に目的が実現したのか，若しくは目標地点まで到達したのか，ということを識別することが難しい．それを可能にするために，KGI，KPIとして一段階細分化したものが表2である．表1，表2ともに，対策評価指標はこうあるべき，というものではなく，各組織において目標やそこに到達するまでの手段・プロセスが異なるように，それに合わせた評価項目を設定すればよい．

表2　情報セキュリティ対策評価指標分類表

目的　：情報資産保護				
情報セキュリティ目標　：企業情報の機密性確保				
KGI		KPI		
評価項目	目標値	対策種別	評価項目	目標値
モバイルPCの紛失・情報漏洩を防ぐ	−50%（計3件）	人的対策	モバイルPC運用細則教育	受講率 100% 理解率 90%
		技術的対策	HDDの暗号化SWの導入	導入率 90%
		物理的対策	モバイルPCの施錠管理	実施率 100%
機密情報への不許可のアクセスを防ぐ	−100%（計0件）	技術的対策	アクセス権の設定	実施率 100%
		組織的対策	アカウントの定期棚卸し 未使用アカウント数	実施率 100% アカウント数 0個
		物理的対策	サーバ室の入退室管理	実施率 100%

4.3　情報セキュリティ対策評価指標の妥当性確認

「情報セキュリティ目標」ごとにKGI，KPIを設定し実績値を測定することで，達成度や経年変化の傾向を見ることができる．情報セキュリティ対策も企業が存続する限り継続的に行うことが重要であるため，この傾向を追跡することは，効果を視覚化するという意味で有効である．

継続的な対策評価指標の計測から，KGI，KPIが高水準を維持でき，情報セキュリティ目標

が達成され，目的が実現されていると判断できることもあれば，期待通りに実績値が向上しないこともあろう．KPI とそれの上位目標である KGI の実績値が目標値に到達していない場合は，KPI の向上に努めるべきだが，KPI の実績値が目標値に到達しているにも関わらず，KGI の実績値が目標値に及ばないという状況では次の要因が考えられる．

- KGI と KPI の組み合わせが正しくない
  モバイル PC の紛失による情報漏洩防止を目標とする KGI を達成するのに，モバイル PC のスクリーンロック実施を行いその実施率を計測している．むしろ，KPI としてモバイル PC の施錠管理率を評価するのが合致している．
- KPI で対象としている情報セキュリティ対策が機能していない
  IC カードによる入退室管理を実施しているが，共連れがあとを絶たず，保護区画のシステムにアクセスできている．新たな情報セキュリティ対策の適用を検討し，KPI の設定・計測を行う．

漠然とした不安から過剰な対策を実施し，例えばまったく使用されなくなった，本来不要な IT セキュリティ製品を適用し続ける状況や，運用負荷の増大により利便性を損なう結果を生じさせているような状況に苦労を強いられている組織があるのではないか．「セキュア・ジャパン 2008」[7]では，「対策疲れ」という表現を用いており的を射ていると考えるが，しかし，そのような状況に陥らざるを得ない環境の変化や技術の変化を考慮すれば同情の余地がある．

上記のような例を克服するために，対策評価指標を利用することで，有効に機能していない対策を把握し，より効果が期待できる対策を見出すことに貢献できると考える．

4.4　情報セキュリティ対策評価指標の運用プロセス

1 章でも述べたように，対策評価指標は情報セキュリティ対策における PDCA サイクルの Check で使用するものと定義した．使用範囲は限定されるものの，実施している対策の妥当性を検証するために必要な評価指標であるため，刻々と現れる新たな脅威や日々登場する新しい技術に対応できるよう，対策自体を見直すことと同様に，評価指標そのものを見直すプロセ

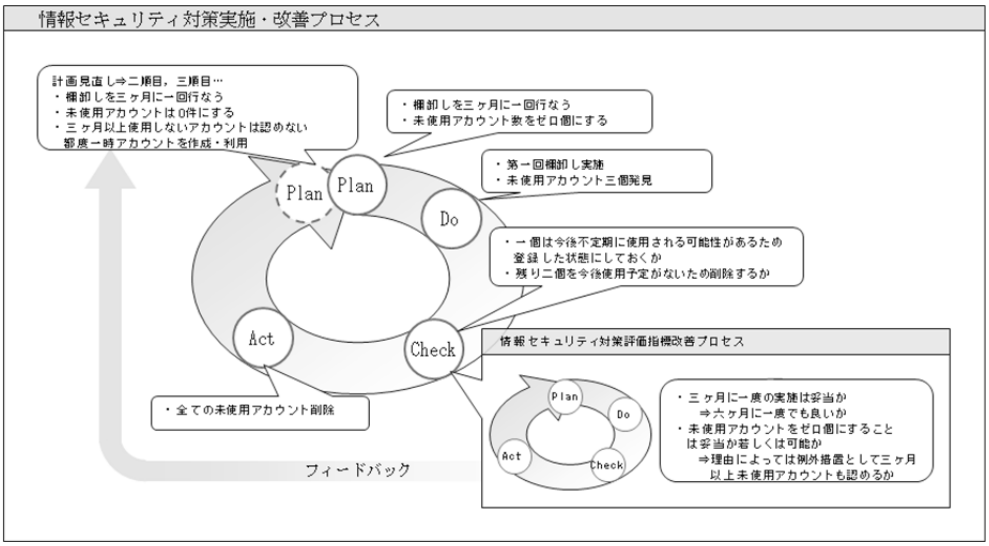

図 3　情報セキュリティ対策評価指標 改善プロセスの位置づけ

スも重要である．すなわち，対策評価指標の数値自体の妥当性を検証・改善し，Check 工程の硬直化を防ぐためのプロセスが必要になる．

図 3 に，表 2 における「アカウントの定期棚卸し」を例として，対策評価指標自体の評価・改善プロセスの位置づけを示した[*2]．Check 工程の結果を二順目以降の Plan 工程にフィードバックを行なう表現にしているが，Plan 工程内で対策評価指標の妥当性の検証と見直しを制限するものではない．

5. 情報セキュリティ対策の投資対効果

ここまで情報セキュリティ対策の実効性/有効性確認の考えを示したが，それに加え，投資に見合った効果の度合いを確認するための指標も考慮する必要がある．投資判断を下す経営層や上位マネジメント層にとって重要な指標となるものである．

5. 1　ROSI（Return On Security Investment）

ROSI という考え方があるが，まだ研究段階のため広く定着するには至っていないとみられている[8][9]．情報セキュリティ対策自体が，リスクの顕在化や損害の発生を防止するために行われるため，マイナス志向にならざるを得ず積極的な投資行動に結び付かないと考えられる．損害発生時に予測される被害額と損害発生率，それらを低減させるための対策費用，そして，損害を受けた時の対応費用を総体的に比較する考え方が一般的であろう．米国国立標準技術研究所（NIST；National Institute of Standards and Technology）の年間予想損失額（ALE；Anuual Loss Expection）が代表的な算出手法である[*3]．

しかし今後は，単なるコストという考えから脱却し，「利益を生み出す情報セキュリティ対策投資」という視点で ROSI を算出する方式が求められるはずである．

6. お　わ　り　に

高度情報化社会の中にあって，様々な情報を取り扱う企業にとり，情報セキュリティ対策を実施することは社会に対しての責務となりつつある．しかし，防衛本能が過度に働き，過剰な情報セキュリティ対策により，本来の業務遂行に支障をきたしかねない状況というのもまた一方で見られる．経営層・上位マネジメントから情報セキュリティ担当者まで含め，情報セキュリティ対策の「あるべき姿」や「最適な解」を求めている作業に終わりはないかもしれない．しかし，現状を改善するプロセスを継続的に実践することで，よりバランス感のある情報セキュリティ対策が行なわれることを願ってやまない．

最後に，本稿の執筆において協力を頂いた関係各位に感謝の意を表する．

＊ 1　独立行政法人 情報処理推進機構は，「2003 年度 IPA ソフトウェア開発支援事業一括公募」の研究成果である「定量的セキュリティ測定手法および支援ツールの開発」（http://www.ipa.go.jp/security/fy15/development/metrics/）を公開している．また，NPO 日本ネットワークセキュリティ協会　脆弱性定量化に向けての検討 WG は，「脆弱性定量化に向けての検討報告書」（http://www.jnsa.org/result/2006/tech/vulnera/report_tv070518.pdf）を公開している．

＊ 2　「アカウント定期棚卸し」プロセスとして PDCA サイクルを表現しているが，これよりも上位のプロセスとして「アカウント管理プロセス」が想定されるが割愛している．

＊ 3　経済産業省も，最近の報告書「企業・個人の情報セキュリティ対策促進事業プロジェクト評

価（中間）報告書（案）」（http://www.meti.go.jp/committee/materials2/downloadfiles/g80703a07j.pdf）で，同様の算出方法を示している．

参考文献 ［1］ 情報セキュリティ政策会議，「第1次情報セキュリティ基本計画 「セキュア・ジャパンの実現に向けて」」，内閣官房情報セキュリティセンター，2006年2月2日，http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf
［2］ 情報セキュリティ政策会議，「セキュア・ジャパン2006 ―セキュア・ジャパンへの第1歩―」，内閣官房情報セキュリティセンター，2006年6月15日，http://www.nisc.go.jp/active/kihon/pdf/sjf_2006.pdf
［3］ 情報セキュリティ政策会議，「セキュア・ジャパン2007 ―ITを安全・安心に利用できる環境づくりのための情報セキュリティ対策の底上げ―」，内閣官房情報セキュリティセンター，2007年6月14日，http://www.nisc.go.jp/active/kihon/pdf/sjf_2007.pdf
［4］ 情報マネジメントシステム推進センター，「ISMS認証取得組織数推移」，財団法人日本情報処理開発協会，2008年10月24日，http://www.isms.jipdec.jp/lst/ind/suii.html
［5］ 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，「企業における情報セキュリティガバナンスのあり方に関する研究会 報告書」，経済産業省，2005年3月，http://www.meti.go.jp/policy/netsecurity/downloadfiles/sec_gov-report.pdf
［6］ 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，「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 参考資料 リスク定量化に関する検討資料」，経済産業省，2005年3月，http://www.meti.go.jp/policy/netsecurity/downloadfiles/4_risk.pdf
［7］ 情報セキュリティ政策会議，「セキュア・ジャパン2008 ―情報セキュリティ基盤の強化に向けた集中的な取組み―」，内閣官房情報セキュリティセンター，2008年6月19日，http://www.nisc.go.jp/active/kihon/pdf/sjf_2008.pdf
［8］ 商務情報政策局 情報セキュリティ政策室，「「企業・個人の情報セキュリティ対策促進事業」の概要」，経済産業省，2008年3月26日，http://www.meti.go.jp/policy/tech_evaluation/c00/C0000000H20/080326_secu/secu_9.pdf
［9］ 商務情報政策局 情報セキュリティ政策室，「評価資料「企業・個人の情報セキュリティ対策促進事業」」，経済産業省，2008年3月26日，http://www.meti.go.jp/policy/tech_evaluation/c00/C0000000H20/080326_secu/secu_10.pdf

執筆者紹介 柏 浦 謙 一（Kenichi Kashiura）
1991年日本ユニシス(株)入社．情報セキュリティ・コンサルティング業務の担当を経て，地銀 勘定系システムの共同アウトソーシング事業におけるITセキュリティ基盤の設計・構築・保守に携わる．現在，共通利用技術部に所属．CISSP．