2008－CSEC－41（16）
2008／5／23

情報セキュリティ対策の評価技法についての考察

重松孝明 周秉慧
九州大学大学院 システム情報科学府

櫻井幸一 堀良彰
九州大学大学院システム情報科学研究院

セキュリティ対策をより実効性あるものにするためには、セキュリティ対策の適切かどうかや、問題点の所在を判断が欠かせない。この判断を的確なものにするためには、セキュリティ対策の計画や実態についての的確な評価は不可欠となる。しかし、セキュリティ対策の評価についてのさまざまな要求に対応できる総合的な評価技法の確立はこれからの課題となっている。そこで、本稿は、今後、確立が求められるセキュリティ対策についての総合的な評価技法についての考察と課題を述べる。

Methodology for evaluation of information security measures of a system

Takaaki Shigematsu, Bin-Hui Chou
Graduate School of Information Science and Electrical Engineering
Kyushu University, Japan
tk-sgmt@guitar.ocn.ne.jp
chou@itslab.csce.kyushu-u.ac.jp

Yoshiaki Hori, Kouichi Sakurai
Faculty of Information Science and Electrical Engineering,
Kyushu University, Japan
{hori, sakurai}@csce.kyushu-u.ac.jp

For increasing the security level of a system, it is indispensable to have the appropriate evaluation about effect of current security measures which provide useful information for judging the adequacy and finding defects of a plan and present status of the deployments and practices of planned security measures. But the methodology for evaluating the effect of security measures for a system which can provide solution for various requirements is in a stage of just beginning. In this paper, we discuss the required integrated methodologies for evaluating effect of security measures of a system and issues to be solved for these this methodologies being accepted and applied widely.

1 はじめに

セキュリティ対策にかかる要求についての議論は、ISMS 等の国際規格の確立に見られるように、大きな進歩を見せてきた。しかし、IT システムや業務現場における実務への展開も含む組織の全領域へのセキュリティ対策の実装と、展開しているセキュリティ対策の実効性の評価についての議論は、いくつかの試みが見られる他は、ISO/IEC27001 および ISO/IEC27002 の要求を前提とした、ISMS シリーズとしての ISO/IEC27004 の規格化の議論が、未だ作業中であるように、まだ、これからと言った段階にある。また、特に、体系的な論議はあまり見かけない。

そこで、本稿では、セキュリティ対策の評価には、相互に関連するさまざまなタイプがあることを示し、そのそれぞれについての考え方を紹介するとともに、これらを体系化して一つの方法論として纏めるための課題を示す。

2 セキュリティ対策の評価技法についての要件

セキュリティ対策の評価には、セキュリティ対策のすべてを対象とした総合評価と、セキュリティ対策の構成要素である個々の施策についての評価に分けられる。セキュリティ対策全体を対象とした総合評価には、セキュリティ事故の発生や、事故による被害をどの程度に抑えることができる

かを計るセキュリティ事故の抑止効果と、事故による被害の抑制効果の評価の２つがある。一方、施策個々についての評価には、対策テーマ(後述)単位、管理策(後述)単位に、その固有強度レベルと実効強度レベルの評価が考えられる。総合評価は、経営レベルでのセキュリティ対策の妥当性のチェックに用いられる。施策個々についての評価は、セキュリティ対策の責任者や計画担当者が、計画の妥当性のチェックや、対策の現状のチェックを行い、実践上の課題を把握し、必要な是正措置を実施するために必要となる。対策テーマ単位の評価は、セキュリティ対策としての施策群を大きな管理単位で見たときの、その妥当性や実践上の課題を把握するのに用いられる。管理策単位の評価は、対策テーマ単位での評価や、セキュリティ事故の阻止効果や、被害の抑制効果の評価に必要なデータを与えるとともに、管理策単位に、計画の妥当性や実践上の課題を把握するのに用いられる。

施策個々の固有強度レベルとは、施策が要求していることが 100%的確に実践され、期待通りに機能した時に期待できる当該施策のセキュリティ対策全体の中での役割りを全うできる尺度を意味する。また、施策個々の実効強度レベルとは、実践上の問題に起因する、施策の固有強度の減衰を考慮した、対策現場における実際の強度レベルを指す。施策の個々について、固有強度と実効強度の概念を導入するのは、すべての施策には、業務現場やセキュリティ対策の実施現場の多くの活動がかかわっており、そのすべてが常に完全に機能していると考えるのは現実的でなく、要求事項の実践レベルが、各施策の実効性を大きく左右することを反映させるためである。

ここで、対策テーマとは、セキュリティ対策全体の中での役割り分担を指し、管理策とは、対策テーマの実現を支える活動等を、計画・実施・管理を一体として考えなければならない単位で束ねたものを言うものとする。また、管理策を構成する諸活動等を管理策要素と呼ぶと、セキュリティ対策の内部構造モデルと、セキュリティ対策の評価テーマとの関連を図１に示すように表すことができる。

また、表１に、セキュリティ事故と対策テーマ、およびこの対策テーマにかかわる管理策の関係のイメージを、“システム上の業務情報の漏洩事故”を例に示す。

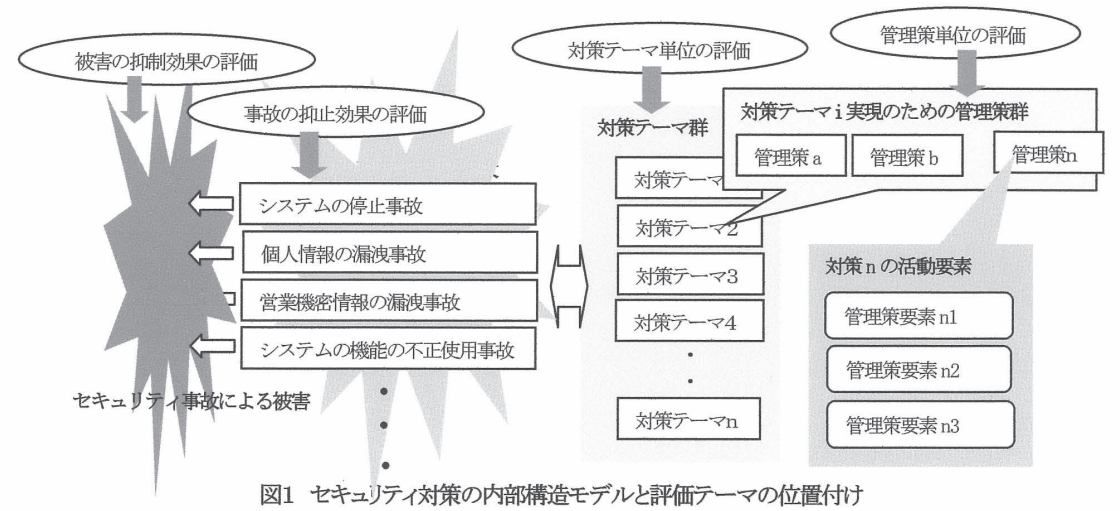

図1　セキュリティ対策の内部構造モデルと評価テーマの位置付け

表1 対策テーマ“システム上の保護情報の保護”にかかる対策テーマと関係管理策(注1)

対策テーマ	関係管理策
システム上の保護対象情報へのアクセス管理	・保護対象情報の識別と保護レベルの指定 ・当該情報へのアクセス権の管理 ・アクセス権の認証データの保護の徹底 ・アプリケーションへの保護対象情報へのアクセス制御機能の適切な組み込み ・記録媒体へのダウンロードの阻止 ・システム上の保護対象情報へのアクセス記録の確保と定期的なチェックの実施＊
ウイルス対策	・関係機器へのウイルス対策ソフトのインストール ・ウイルス検疫システムの導入 ・関係 OS の脆弱性対策の徹底 ・ウイルスチェックファイルの更新の徹底 ・関係者に対するウイルス感染阻止に向けた意識の徹底
システムへのアクセス管理	・さまざまなレベルのアクセス制御機能の適切なインストール ・システムへのアクセス権の管理の徹底 ・アクセス権認証データの保護の徹底 ・システムへのアクセス履歴の確保と定期的なチェックの実施＊
情報媒体の管理	・保護対象媒体の識別と保護レベルの指定 ・保護対象媒体の取り扱い規程の策定 ・保護対象媒体のルールに沿った取り扱いの実施 ・保護対象媒体の取り扱い記録の確保と定期的なチェックの実施＊

(注1)本表は、個別セキュリティ対策と関係管理策の対応概念を説明するための例示で、本表であげた対策テーマや関係管理策は、その一部にしか過ぎない。
(注2)＊を付した管理策は、当該対策テーマに関係する管理策ではあるが、事故による被害の抑制には寄与するが、事故の阻止には直接は寄与しない管理策であることを示している。

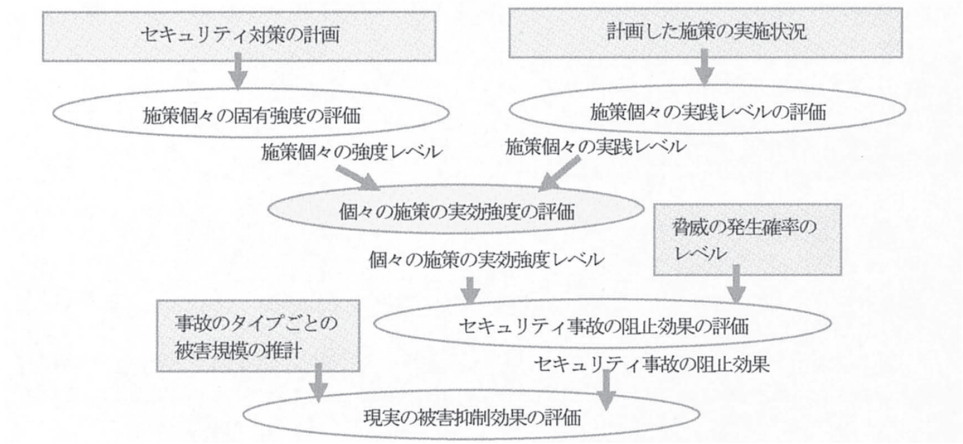

図1 セキュリティ事故による被害の抑制効果

図2 セキュリティ対策についての評価の全体像

3 セキュリティ対策の総合評価についての考察

3.1 セキュリティ事故による被害の抑止効果の評価

被害抑制効果の評価においては、一定期間内にセキュリティ対策をかいくぐって発生が想定されるセキュリティ事故による被害額の規模がその尺度となる。同じ情報漏洩事故であっても、個人情報と営業機密情報では、漏洩情報一件当たり被害額は大きく

異なる。また、一事故当たりの漏洩件数も、データファイルの不正な持ち出しと、外部からの不正アクセスによる情報の閲覧では、その規模は大きく異なる。この事例から判るように、事故による被害額の算定は、算定根拠が異なる、事故の種類、影響業務、事故の規模の組み合わせ(事故タイプと呼ぶ)別に行わなければならない。

一定期間における事故タイプ別の被害額は、当該タイプの事故の発生頻度、単位規模当たりの被害額と、事故の規模の相乗となる。単位規模当たりの被害額とは、システムの停止事故ではシステム停止一時間当たり被害額、情報の漏洩事故では、一件当たりの被害額と言ったような、事故の規模単位ごとの被害額の算定基準額を言う。また、事故の規模の尺度も、システムの停止事故では停止時間、情報の漏洩事故では漏洩件数と言い、事故の種類によって異なる。被害額の算定を大きく左右する事故の規模は、当該事故にかかわるセキュリティインシデント発生の検知機能、問題部位の切り離し等の事故の影響範囲の拡大を防ぐための機能、被害範囲の特定機能、事故からの復旧機能等の事故処理に当たる機能の能力に左右されるため、事故タイプごとに、関係するこれらの機能にかかわる施策についての評価にもとづいて決めることになる。

これらのことから、タイプ a の一定期間内における想定される事故の発生頻度を FA_a、タイプ a の事故の特性に対応する被害抑制策の効果から決まるタイプ a の事故における被害規模レベルを SA_a、タイプ a の事故の業務上の影響範囲から決まる単位規模当たりの被害額 DU_a とすると、一定期間内でのタイプ a の事故による想定される被害額 DA_a、は、式(1)で表すことができる。

$$DA_a = f(FA_a, SA_a, DU_a) \qquad (式1)$$

事故タイプごとの事故発生頻度は、3.2 節に示す事故の抑止効果の評価から求めることができる。また、すべての事故を対象とした被害の総額は、事故タイプごとの想定被害額の総和となる。

3.2 セキュリティ事故の抑止効果の評価

セキュリティ事故につながる脅威の発生頻度も、対応するセキュリティ対策の組み立ても、阻止したいセキュリティ事故の種類により異なること、および評価結果は、事故による被害の抑制効果の算定に結び付けなければならないため、セキュリティ事故の阻止効果の評価も、脅威に対応した事故のタイプごとに行わなければならない。

対策の現状を反映した、事故タイプごとの事故の阻止率は、関係する管理策個々の、実効強度レベルと対象事故の阻止への寄与率によって決まる。また、事故タイプごとの事故の発生頻度は、当該事故を引き起こす脅威の発生頻度と、対象となる脅威に対応するセキュリティ対策の事故阻止効果の相乗となる。

この関係は、一定期間内におけるタイプ a の事故を引き起こす脅威の発生頻度を FT_a、タイプ a の事故の阻止にかかわる管理策 i の寄与率を w_{ai}、タイプ a の事故の阻止にかかわる管理策 i の実効強度レベルを ER_{ai} とすると、事故タイプ a の阻止効果を EM_a、、および一定期間内におけるタイプ a の事故の発生頻度 FA_a は、式(2)および式(3)であらわすことができる。

$$EM_a = f(w_{ai}, ER_{ai}) \qquad (式2)$$

$$FA_a = FT_a \cdot EM_a \qquad (式3)$$

4 個々の施策に対する評価についての考察

施策単位での評価には、対策テーマ個々に対する評価、管理策の個々に対する評価があるが、紙面の都合から、本稿では、管理策の個々に対する評価についての考察にのみ触れる。

4.1 管理策単位での固有強度の評価

管理策個々の固有強度レベルは、当該管理策を形成する管理策要素の個々の固有の強度レベル、すなはち、使用する技術の信頼性、および当該技術の実装や運用、関係する業務活動におけるセキュリティにかかわるルールや手続きの緻密さや厳格さや正確性、およびセキュリティの確保にかかわる要求の実践や不手際の排除についてのマネジメント努力の程度に依存する。したがって、管理策 c に

おける管理策要素ｅの、管理策Ｃの目的達成についての寄与率をw_{ce}、管理策ｃ における管理策要素ｅの固有の強度レベルをRL_{ce}とすると、管理策Ｃの固有強度レベル RC_o は、式(4)で表されることになる。

$$RC_C = f(w_{ce}, RL_{ce},) \quad (式4)$$

管理策要素の当該施策の目的達成への寄与率は、管理策の役割りや管理策要素の組み立ての特性によって異なる。多くの管理策のすべてについて、管理策要素の寄与率を適切に決めることは、手間はかかるが困難ではないと考える。

4.2 管理策単位での実効強度の評価

管理策単位での実効強度レベルは、管理策要素と呼ばれる当該管理策を形成する諸活動等の固有の強度レベルと、管理策要素個々における要求事項の実践の正確性や徹底度の程度を示す実践レベルと、管理策要素の当該管理策の強度への寄与率により決まる。

この関係は、管理策ｃにおける管理策要素 ｅ の管理策ｃの目的達成への寄与率をw_{ce}、管理策ｃにおける管理策要素ｅの実践レベルをEL_{ce}、管理策ｃにおける管理策要素 ｅ の固有強度レベル $0L_c$ とすると、管理策Ｃの実効強度レベル ER_c は、式(5)で表すことができる。

$$ER_C = f(w_{ce}, EL_{ce}, OL_{ce},) \quad (式5)$$

管理策要素単位の実践レベルの評価は、管理策要素が活動を対象としたものに対してのみ必要となる。実践レベルは、表2に示すような基準で十分にその役を果たすと考える。管理策要素単位での実践レベルと、その固有強度と実効強度の関係のイメージを表２に示す。なお、管理策要素が使用技術である場合、実践上の問題による減衰はありえないため、その実践レベルは5相当とする。

表2 管理策要素単位での実践レベルと管理策要素の実効強度との関係

実践レベル	実施率	管理策要素単位での実践レベルの実効強度への影響
レベル5 ： 完全	100%	管理策要素単位の実効強度レベル＝管理策要素固有の強度レベル
レベル4 ： ほぼ完全	98%以上	管理策要素単位の実効強度レベル＝管理策要素固有の強度レベル－1
レベル3 ： 許容レベル	95%～98%	管理策要素単位の実効強度レベル＝管理策要素固有の強度レベル－2
レベル2 ： おおいに問題	90%～95%	管理策要素単位の実効強度レベル＝管理策要素固有の強度レベル－3
レベル1 ： 不可	90%未満	管理策要素単位の実効強度レベル＝管理策要素固有の強度レベル－4

(注) この表に示す実践レベルの設定基準や、その固有強度の減衰率は、評価方法の概念の説明のための事例である、実用のためには、さらなる議論が必要となる。

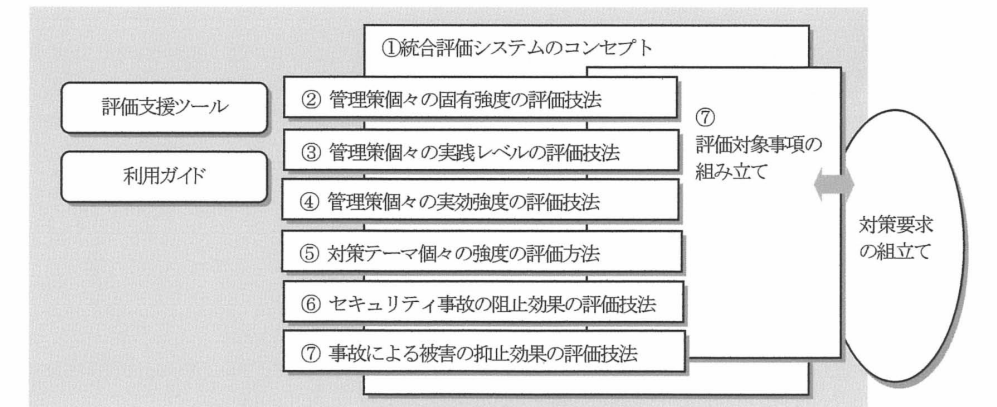

図3 セキュリティ対策の統合評価システムのフレームワーク

表3 セキュリティ対策の評価技法の確立に向けた課題

課題区分	課題
事故による被害の抑止効果の評価	・この評価の対象となる事故タイプの選定方法と事故タイプの標準モデルの確立 ・事故による被害抑止にかかわる管理策の被害規模の抑制効果の算定方法の確立 ・事故タイプごとの単位規模当たりの標準被害額の算定方法の確立
セキュリティ事故の阻止効果の評価	・この評価の対象となる事故タイプの選定方法と標準モデルの確立 ・代表的な事故タイプごとの関連管理策の寄与率の考え方の確立と参考値の設定
対策テーマ単位の強度評価技法	・評価対象とする対策テーマの選定方法と標準モデルの確立 ・対策テーマ個々における関係管理策の寄与率の考え方の確立と参考値の設定 ・関係管理策の強度レベルと対策テーマへの寄与率を用いた対策テーマの強度レベルの算定方法の確立
管理策個々の固有強度の評価	・管理策要素の構成モデルの確立 ・管理策要素ごとの管理策の固有強度への寄与率の考え方の確立と参考値の設定
管理策個々の実践レベルの評価	・管理策要素の強度レベルの定義と判定基準の確立
管理策個々の実効強度の評価	・管理策要素の強度レベルの定義の確立 ・管理策要素の強度レベルと管理策の固有強度への寄与率を用いた管理策の実効強度レベルの算定アルゴリズムの確立
評価対象事項の組み立て	・対策テーマの組み立てと対策テーマごとの関係管理策の構成モデルの確立 ・管理策構成要素の構成モデルの確立
その他	・評価事項の体系の I ISO/IEC2700 1 および 27002、および検討中の ISO/IEC27004SMS との整合性の確保 ・これらの評価をサポートするツールの開発

5 セキュリティ対策の評価技法確立に向けた課題

以上述べてきたようなさまざまなセキュリティ対策についての評価が、整合性のあるものにするためには、図 3 に示すような、セキュリティ対策についての評価技法のフレームワークを確立する必要があろう。このフレームワークの確立には、多くの課題が残されている。表 3 にその課題を一覧する。

6 まとめ

以上、まだ技法が確立しているとは言い難いセキュリティ対策の統合評価技法についての考察を述べてきた。最後に、本稿が、特に指摘したい点を纏めると、以下のようになる。

- セキュリティ対策の評価には、その使用場面により異なるニーズに対応するためさまざまなタイプがある
- セキュリティ対策の評価は、これらのすべてに対し整合性のある回答をだせるものでなければならない
- このためには、一つのフレームワークに体系化できる統合的な評価技法の確立が必要となる
- 統合評価技法の構成要素となるさまざまな視点の評価にも、評価を客観的なものにし、組織間での比較も可能にするためには、算定方法の確立のみならず、標準モデルや、判定基準の確立が随所に必要となる
- 定のアルゴリズムや、強度の評価基準等の確立が必要である

本稿では、セキュリティ対策の総合的な評価についての考え方を述べたに止まっているが、今後は、これらの考察を踏まえ、統合評価技法の確立に向けた研究を進めたい。セキュリティ対策の評価のベースとなる、本稿で述べた考察について多くのご意見を頂ければ幸いである。

6 参考文献

[1]重松孝明 “セキュリティ対策評価技法の提案” コンピュータセキュリティシンポジウム 2003 論文集、pp.337-342,2003

[2] “セキュリティ対策評価モデル” 電子商取引推進協議会 2005 年

[3]経済産業省報告書 2007 年 “情報セキュリティベンチマーク” http://meti.go/policy/netsecurity/downloadfiles/07824benchimark.pdf