2008－CSEC－42（39）
2008 / 7 / 25

セキュリティ対策の統合評価における個々の対策についての評価技法の提案

重松 孝明† 周 秉慧† 堀 良彰‡ 櫻井 幸一‡

†九州大学大学院システム情報科学府 〒819-0395 福岡市西区元岡 744
‡九州大学大学院システム情報科学研究院 〒819-0395 福岡市西区元岡 744
E-mail: †tk-shigematsu@wind.ocn.ocn.ne.jp, chou@itslab.csce.kyushu-u.ac.jp
‡{hori, sakurai}@csce.kyushu-u.ac.jp

あらまし 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する解を，相互に整合性のあるものにするためには，さまざまな評価を相互に連携させる統合評価技法の確立が必要となる．このセキュリティ対策の統合評価における，個々の対策についての評価の位置付けを示し，統合評価技法の要となるセキュリティ対策の基本単位の評価についての要件を示すとともに，その実務的な評価方法を提案し，その課題を論じる．

キーワード セキュリティ対策の統合評価，対策個々の評価技法，セキュリティ対策の階層構造

A Methodology for Evaluating Each Measure in the Integrated Evaluation of the Security Measures in a System

Takaaki SHIGEMATSU† Bin-Hui CHOU† Yoshiaki HORI‡ and Kouichi SAKURAI‡

† Graduate School of Information Science and Electrical Engineering, Kyushu University 744 Motooka, Nishi-ku, Fukuoka, 819-0395 Japan
‡ Faculty of Information Science and Electrical Engineering, Kyushu University 744 Motooka, Nishi-ku, Fukuoka, 819-0395 Japan
E-mail: †tk-shigematsu@wind.ocn.ocn.ne.jp, chou@itslab.csce.kyushu-u.ac.jp
‡{hori, sakurai}@csce.kyushu-u.ac.jp

Abstract For covering various requirements for the evaluations of security measures for a system with good coordination among the solutions of different evaluations, it is required to establish a methodology for integrated evaluation of security measures for a system which can satisfy such requirement. In this paper we show the positions of the evaluations for individual security measures in the integrated evaluation and propose a practical approach to evaluate a basic unit of security measures which will link total evaluation of all security measures in a system with the issues to be solved for making proposed approach practical and being widely used.

Keyword Integrated evaluation of security measures, Methodology for evaluating each security, Layer structure of security measures

1 はじめに

セキュリティ対策の評価は，セキュリティ対策全体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．“セキュリティ対策の統合評価技法についての考察” [1]で示したように，前者は，セキュリティ対策が全体として，どの程度その期待に応えられるものかを判断するためのものであり，セキュリティ対策が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込むことができるかを計る”キュリティ事故の抑止効果の評価“と，”事故による被害の抑制効果の評価“の２つの評価がある．一方，施策個々についての評価は，施策単位に，その必要十分性をチェックするとともに，実践上の問題点を把握し，事故が発生する前に必要な改善措置を講じることができるようにすることに加え，セキュリティ対策全体の総合評価に必要となるデータを提供することがその役割となる．

セキュリティ対策は，図１に示すように，セキュリティ

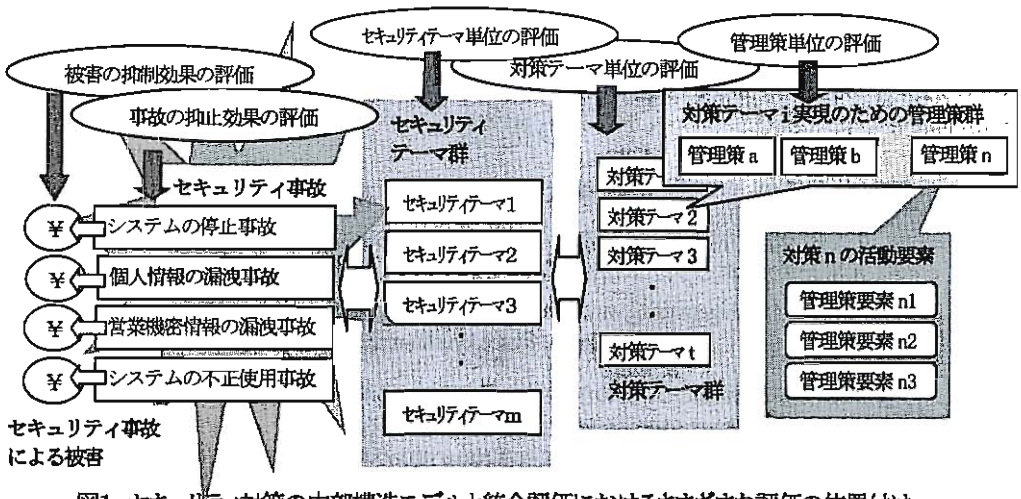

図1 セキュリティ対策の内部構造モデルと統合評価におけるさまざまな評価の位置付け

対策を目的単位に纏めたセキュリティテーマ，セキュリティテーマの実現のために必要となる施策を対策テーマ，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管理策(注)，および一つの管理策を構成する諸活動等を管理策要素の 4 層構造で捉えることができる．図 2 は，この階層構造のイメージをより明確にするため，上位 3 層の具体例を示したものである．

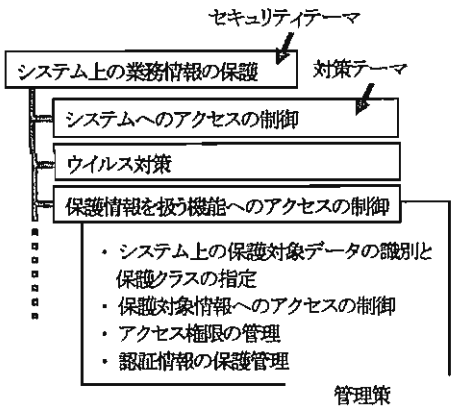

図2 各層の具体事例

セキュリティ対策をこのような階層構造で捉えると，対策の個別評価は，セキュリティテーマ単位，対策テーマ単位と対策テーマの構成要素である管理策単位のそれぞれに行わなければならないことが判る．

セキュリティテーマ単位の評価は，セキュリティ対策全体についての総合評価に必要なデータを与えるのに用いられる．対策テーマ単位の評価は，セキュリティ対策を比較的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，管理策単位の評価は，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必要となる．セキュリティテーマ単位の評価は，関係する対策テーマの評価の積上げで，対策テーマの評価は関係する管理策に対する評価の積上げで求まる．また，個々の管理策についての評価は，当該管理策を構成する管理策要素個々についての評価の積上げで求まる．

本稿では，さまざまな評価の原点となる管理策単位での評価に焦点を当て，統合的に対応できる統合評価技法の一環としてのその要件を示すとともに，客観的で，かつ対策全体としての総合評価につながるような評価を実現するための技法を提案するとともに，その課題を述べる．

(注) 本稿で言う管理策は，セキュリティマネジメントの対象としてのセキュリティ対策の要求を示した ISO/IEC27000 シリーズ(ISMS)で言う管理策(Control)とは，概念が異なる．

2 管理策単位の評価についての要件

管理策単位の評価が，適切な評価結果を提供し，統合評価技法の構成要素の一つとして十分にその役割を果たすためには，以下が求められる．

- セキュリティ対策の欠陥を具体的に指摘でき，必要な改善点を明確にできること
- 対策テーマ単位の評価に必要なデータを提供でき，対策全体としての総合評価に結びつけることができる

こと

- 評価者の主観の入る余地を極力少なくし，客観的の高い評価ができること
- 評価の実施に大きな手間を必用としないこと
- セキュリティ環境に左右されずすべてのシステムに共通して適用できること

3 管理策単位の評価についてのコンセプト

前節に示した要件に応えるためには，評価対象としての管理策の適切な括りだし，評価結果の表し方，評価の方法についての議論が重要となる．提案する評価技法おけるこれらについての考え方は，以下の通りである．

3.1 評価対象としての管理策の組立て

提案する評価技法における評価対象としての管理策は，セキュリティ対策を形作る技術やさまざまな活動で，計画，実装，実践の管理を一体として考えなければならない最小単位とする．これは，セキュリティ対策の実効性は、個々の施策における計画の妥当性，その実装の的確性，当該施策に関し要求される活動の要求通りの的確な実践に依存しているため，これらをワンセットでチェックしなければ，実効性の評価にはならないと言う考えによる．

また，最小単位とするのは，評価対象が複数の目的が絡むと，管理策の内部構造のモデル化が困難となり，統一的な評価基準の設定を困難なものにするためである．このような考え方による，管理策の具体的例を，対策テーマとの関連付けて示したものが，表1である（“セキュリティ対策の統合評価技法についての考察”［1］から引用）．

3.2 管理策単位での評価結果の表し方

管理策単位での評価結果は，それをセキュリティ対策全体についての総合評価につなげる，一般には複数の管理策がかかわる対策テーマ単位の評価に結びつけるためには，数値で表現することが望ましい．このため，管理策単位での評価尺度には，対象となる管理策がどの程度期待に応えられるかを示す対策強度と言う尺度を導入する．そして，セキュリティ対策についての信頼性は，対策のレベルにより大きく異なることから，高い精度は必要ではなく，そのレベル差が把握できれば，十分にその役割を果たせると考えることができる．このことと，評価に無用の手間がかからないようにするため，管理策単位の評価においては，その対策強度を，表2に示すようなイメージによる 5 段階に分けたレベルのどれに該当するかを把握する方法を採用する．この方法を用いれば，管理策単位の評価を，数値表現することが可能となる

強度レベル 5 は，信頼性は高いものの，その実践にはコストも現場の負担も大きく，その適用は，絶対的な信頼性が求められるシステムにおいてのみに限定されよう．この強度レベル 5 は，最強の手段を網羅した，当該対策における究極の姿を示すものとも考えることができる．強度レベル 4 は，レベル 5 ほどではないにしろ，それなりのコストや少なからぬ手間を必要とするが，高いセキュリティレベルが要求されるシステムで，万全を期したいところについては，その採用は検討対象とな

表1 対策テーマと管理策の組み立て例

対策テーマ	関係管理策
アプリケーションレベルでの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
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＊

表2 管理策単位の対策強度のレベル基準

強度レベル	当該強度レベルの主観的
レベル5 （非常に強）	最高に厳格なルール，厳格な管理，2 重化，最強の技術の使用等で，これ以上の対策は望めないレベルで，その信頼度は 100%に近いと見ることができる
レベル4 （強）	ベースラインと呼ばれるレベル 3 に比べて，より厳格なルールと管理，より精度の高い技術の使用や，必要に応じた対策や管理の 2 重化等で，脅威がつけ入る隙はほとんど潰しており，信頼性は平均より数段高い
レベル3 （ベースライン）	一般的に必要最小限とされる対策レベルと定義する．ルール，管理，使用技術は平均であっても最低限の PDCA サイクルは回っており，その信頼性は，一般的には一応十分と見られるレベル
レベル2 （弱）	ベースラインに対する要求を満たしてなく，隙が残されており，当該対策単独に見れば不十分と言えるが，対策は相当に機能しており，その弱点は他の対策で十分にカバーされているか，ここで問題が生じてもシステム全体としては問題が生じないと判断されるか，リスクレベルが低く，発生した問題は許容できると判断される場合にのみ採用が可能なレベル
レベル1（不可）	レベル 2 の達成基準もクリアーできないレベルを指し，対策は機能していなく，改善が急がれる状態

る．ベースラインと呼ぶレベル 3 は，レベル 4 は必要ではではないが，リスクが低かったり他の対策でカバーされているため，当該対策については，ある程度手を抜いても，問題が生じる可能性が低かったり，問題が生じても全体しては問題とならないと判断できるレベル 2 でも構わないと判断できる管理策以外に適用されるレベルとなる。

3.3 固有強度レベルと実効強度レベル

管理策の個々に対する評価においては，固有強度レベルと実効強度レベルの概念の導入が必要となる．管理策の個々についての固有強度とは，当該管理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対策のセキュリティ対策全体の中で割り当てられた役割を全うできる程度を示す尺度と定義する．

また，管理策個々についての実効強度レベルとは，実践上の問題に起因する，対策の固有強度の低下を考慮した現実の強度レベルと定義する．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．

4 管理策要素の評価を用いた固有強度レベルと実効強度レベルの評価方法

4.1 各強度レベル評価のアプローチ

管理策個々の固有強度は，当該管理策を構成する管理策要素のうち，固有強度にかかわる要素の強度レベルにより決定される．一方，実効強度レベルは，当該管理策の固有強度レベルと，当該管理策における要求事項の実践がかかわる管理策要素個々の実践度から定まる当該管理策の実践レベルに依存する．このアプローチを図 3 に示す．

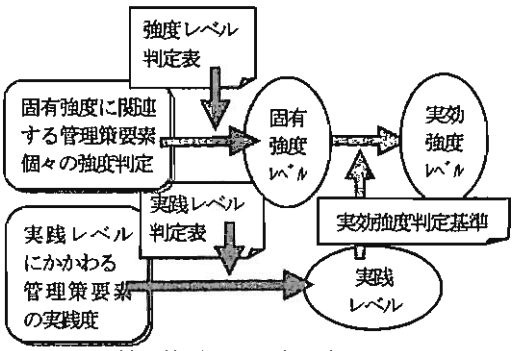

図3 管理策単位の固有強度レベルおよび実効強度レベルの評価のアプローチ

このため，管理策の強度レベルを知るためには，管理策における管理策要素の構成を分析し，管理策要素単位での強度の評価方法を確立するとともに，構成管理策要素個々の強度を用いた管理策の固有強度と実効強度の判定方法の確立が必要となる．

以下に，管理策要素の構成についての分析と，管理策要素ごとの強度レベルの判定方法，ならびにこの管理策要素の強度レベルを用いた管理策の固有強度レベルならびに実効強度レベルの判定の考え方を示す．

4.1 管理策要素についての分析

一つの管理策は，管理策構成要素と呼ばれる技術の使用や業務現場へのさまざまな要求とその実践等から構成される．

セキュリティ対策の評価において，評価の対象となる管理策は，150 は下らない数に達するものの，そのすべては図 4 に示すような構成モデルで表すことができる．管理策によっては不要なものもあるが，技術の使用がかかわる管理策同士，および管理的な対応だけで技術の使用はない管理策同士では，その構成はほぼ同じパターンとなる．

管理策単位に定義されるポリシーは，当該管理策に期待されること，すなわちセキュリティ対策全体の中での役割とその遂成についての期待のレベルを明確にするとともに，その実現への方向付けを示すものである．対策要件の定義は，当該管理策が前提とすべき環境と，当該管理策が実現すべきことを具体的に定義するものである．管理策の基盤とも言えるこの 2 つの要素は，当該管理策の枠組みを示すもので，これらにおける曖昧さは，当該管理策の対策そのものの的確性を危うくする．

管理的対応とは，業務の実践現場におけるセキュリティ対策にかかわる要求や，技術的な対応の運用にかかわる活動についての要求や，要求に対する実践群を指す．関係ルールの確立とは，情報の保護におおける保護レベルの設定基準や情報の作成，保管，閲覧についてのルール等，当該管理策が機能するためルールとして制定すべき事項をルールとして明確にするものである．また，関係手順の確立とは，当該管理策にかかわる現場の実務や，セキュリティ対策にかかわる活動の実施にあたって守るべき手順を示すものである．

ルールや手順がいかに的確なものとして策定されていても，それらが対策現場に十分に徹底されていなくては機能しない．ルールや手順の対策現場への展開とは，マニュアル化や教育等により，関係者の全員が業務活動でかかわるルールや手順を正しく周知させ，日々の活動に反映されるようにすることを指す．また，対策現場における実践は，日々の業務活動において，これらのルールや手順を遵守し，セキュリティ面で隙を残さないようにするためものである．また，要求事項の実践を追及するための管理の実践とは，業務活動一般におけるセキュリティ対策にかかわるルールや手順の遵守や，セキュリティ対策に関係して必要とされる活動等が適切に行われるよう，その実践レベルの維持向上するための管理的な活動を指す．

一方，技術的対応とは，技術の使用を前提とする管理策における，使用する技術，使用する技術の適用基準の確立，技術の実装についての設計，システムへの技術の組み込み等の要素で構成される．技術の使用が関係しない管理策においては，これらの要素は存在しない．技術を使用する管理策においても，技術使用の運用等で管理的な対応も存在する．使用する技術とは，当該管理策がその役割を果たすために使用するハードウエアやソフトウエアやシステム化されたツールやシステムアーキテクチャ面での方式や処理方式を指す．使用する技術の適用基準は，使用する技術をシステムにどのように組み込み，どのように使用するかを明確にするもので，使用する技術の配置場所，設定機能の指定等がこれに含まれる．使用する技術固有の信頼性とその使用法は，管理策の強度に大きくかかわる．使用技術の実装についての設計は，関係する技術のシステムへの組込みについての細かい指定や，アプリケーションソフトに要求されるセキュリティ関連機能の詳細設計を指す．これらにおける齟齬は，使用する技術の

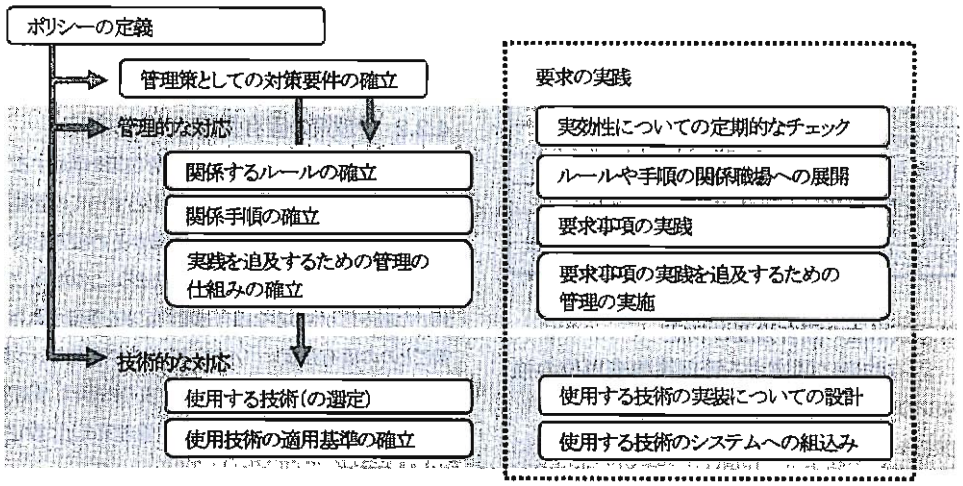

図4 管理策構成要素の構成モデル

実効性を大きく削ぐことにつながる．また，使用する技術のシステムへの組込みとは，使用する技術を設計に沿って的確にシステムに組み込むことを指す．この実装上の齟齬も，使用する技術の実効性を危ういものとする．対象とする脅威の阻止に十分な技術を使用しながらセキュリティ事故に見舞われる多くは，この使用技術の適用基準の不備や，実装設計やシステムへの組込みにおける不備がその原因となっている．

また，実効性についての定期的なチェックは，当該管理策が期待される役割を果たしているかどうかを定期的に確認するものである．管理策の固有強度は組織の運営形態や関係するITシステムの変化によって影響を受けるほか，その実効強度は，要求事項の実践レベルにも左右されるため，管理策の強度レベルを維持するためには，このチェックも欠かせない．

また，管理策構成要素の構成は，管理策としての具体的な要求に類するものと，その実践に類するものに分かれ，管理策の固有強度を左右する前者を固有強度関連要素，管理策の実効強度を左右する後者を実践レベル関連要素と呼ぶ．表3に，管理策構成要素の構成とそのタイプを示す．

表3 管理策を構成する管理策要素

管理策要素	管理策タイプ		要素区分	
	技術の使用		固有強度関連要素	実践度関連要素
	あり	なし		
ポリシーの定義	○	○	○	
対策要件の定義	○	○	○	
関係ルールの確立	○	○	○	
関係手順の確立	○	○	○	
ルールや手順の展開	○	○		○
要求事項の実践	○	○		○
管理の仕組みの確立	○	○	○	
実践についての管理の実施	○	○		○
技術的な対応手段	○		○	
使用技術の適用方法の確立	○		○	
使用技術の実装設計	○		○	
使用技術の実装	○		○	○
定期的な実効性の確認	○	○	○	○

4.2 管理策単位の固有強度の判定

4.2.1 固有強度に関連する管理策要素単位の強度レベルの判定

管理策個々の固有強度レベルは，表2に示す固有強度にかかわる管理策要素個々の強度レベルと管理策の強度レベルへの関与の重みから求める．管理策要素により決まる．

この管理策要素ごとの強度レベルとは，それぞれの信頼度を示す尺度で，提案評価技法では，表4に示すように4段階に分ける．

表4 固有強度関係管理策要素の強度レベルの定義

レベル	管理策要素単位での強度レベルのイメージ
強	十分で齟齬が生じる可能性はゼロに近い
中	おおむね十分と言えるが，齟齬が生じる余地は少しながら残されている
弱	十分とは言い難く，齟齬が生じる可能性は少なくない
不可	齟齬が生じる可能性が高く，信頼できない．

この管理策要素単位での強度レベルの判定要素には，以下があげられる．

- 検討における組織的な取り組みのレベル
- PDCAサイクルの循環状況
- 対策対象の網羅性
- ルールや手順，管理の仕組みの厳格さ
- 技術の設計や実装の的確性の保証のレベル
- 文書化のレベル

これら個々についての評価は，強，中，弱の3段階で十分であろう．これらについての評価は，ある程度主観的にならざるを得ないが，標準的な判定基準を確立しておき，これをベースに判定するようにすれば客観性を高めることができる．

また，これらの個々についての評価値と，管理策要素内での重みをパラメータとした表5に示すような判定表を設けておけば，容易に管理策要素単位の強度レベルを求めることができる．この管理策要素単位の強度レベルの判定表は，すべての管理策の管理策構成要素ごとに，その特性を反映するよう個別に設定しなければならない．

4.2.2 管理策の固有強度レベルの判定

管理策の固有強度レベルは，当該管理策を構成する管理策要素の中の固有強度の決定にかかわるすべての管理策要素の個々の強度レベルと，当該管理策がその役割を果たす上での各管理策要素の重みによって決まる．このため，これらを用いた表6に示すような固有強度判定表を準備すれば，管理策ごとのの固有強度レベルは，相当に客観的にかつ簡単に判定することが可能となる．この判定表の内容は，管理策の特性を反映しなければならないため，管理策ごとに設定しなければならない．

表5 固有強度関係要素の強度レベルの判定基準

判定要素	その他の要素(注1)				管理的対応関係要素				技術的対応関係要素			
	重み	レベルと達成基準(注2)			重み	レベルと達成基準(注2)			重み	レベルと達成基準(注2)		
		強	中	低		強	中	低		強	中	低
検討における組織的な取り組みのレベル	大	強	中	中	大	強	強	低	中	強	中	低
PDCAサイクルの循環状況	中	強	強	中	大	強	強	低	弱	強	中	低
対策対象の網羅性	−	−	−	−	大	強	中	中	大	強	中	中
ルールや手順，管理の仕組みの厳格さ	−	−	−	−	大	強	強	低	中	強	中	低
技術の設計や実装の的確性の保証レベル	−	−	−	−	−	−	−	−	大	強	中	低
文書化のレベル	大	強	強	中	大	強	中	低	中	強	中	低

(注1) セキュリティ対策全体としてのポリシーの確立や対策要件の確立等，セキュリティ対策の基盤整備にかかわる管理策群
(注2) 達成基準は，当該レベルの達成するために必要となる各判定要素についての評価の最低値を表示

表6 関係する管理策要素の強度レベルを用いた管理策の固有強度レベル判定表のイメージ

管理策要素	その他の管理策					技術の使用しない管理策					技術を使用する管理策				
	重み	各レベルの達成基準				重み	各レベルの達成基準				重み	各レベルの達成基準			
		5	4	3	2		5	4	3	2		5	4	3	2
ポリシーの定義	大	強	強	中	低	大	強	中	中	低	中	強	中	中	低
対策要件の定義	大	強	強	中	低	大	強	中	中	低	大	強	強	中	低
関係ルールの確立	−	−	−	−	−	大	強	強	中	低	中	強	強	中	低
関係手順の確立	−	−	−	−	−	大	強	強	中	低	中	強	強	中	低
管理の仕組みの確立	−	−	−	−	−	大	強	強	中	低	中	強	中	中	低
使用する技術	−	−	−	−	−	−	−	−	−	−	大	強	中	中	低
使用技術の適用方法の確立	−	−	−	−	−	−	−	−	−	−	大	強	強	中	低

(注1) セキュリティ対策全体としてのポリシーの確立や対策要件の確立等，セキュリティ対策の基盤整備にかかわる管理策群
(注2) 達成基準は，当該レベルの達成するために必要となる各管理策要素の強度レベルの最低値を表示，またこれらの条件に達しないものを強度レベル1とする

4.3 管理策単位の実効強度の判定

4.3.1 管理策要素単位の実践度の判定

実践レベルに関連する管理策要素の個々についての実践度は，表6に示すような基準で4段階に分ける．実践度の基準も実践度の判定要素も，管理策要素ごとに異なるが，代表的な判定要素は表7に示すようなものとなる．

表7 管理策要素単位の実践度の基準

実践度	当該レベルにおける実践度のイメージ
徹底	十分に徹底されており，実践率は100%と見てよい
高	おおむね十分ではあるが，漏れが生じる余地が残されている．実践率は98%以上
中	実践はされてはいるが徹底はされていない．実践率は95%～98%のレベル
低	不十分の領域で，実践率は95%以下

4.3.2 管理策単位の実践レベルの判定

管理策単位の実効強度レベルの判定に必要となる管理策単位での実践レベルは，表8に示すように5段階のレベルに分ける．関係管理策要素の実践度のよって決まるこの実践レベルの判定には，関係する管理策要素の実践度と，各管理策要素の当該管理策の強度レベルへの影響の重みをパラメータとした表9に示すような判定表を準備すれば，客観性の高い判定が可能になろう．この判定表は，管理策の特性を反映するよう管理策単位に設定しなければならない．

表8 管理策要素単位の実践度の判定要素

管理策要素種別	判定要素
ルールや手順の展開	・展開の仕組みの適切性 ・関係者への周知活動の徹底度 ・関係者におけるルールや手順の認知度
要求事項の実践	・関係者における要求事項の認知度 ・関係者におけるルールや手順等の要求事項の遵守についての意識のレベル ・日々の活動にける要求事項の遵守状況
実践についての管理の実施	・決められたルールや手順の遵守についての指導の実施度 ・要求事項の実践いついての管理監督の徹底度

表 9 管理策単位の実践レベル判定表のイメージ

関係管理策要素	重み	管理策の実践レベルと各レベルの達成基準			
		5	4	3	2
ルールや手順の展開	中	徹	徹	高	中
要求事項の実践	大	徹	徹	高	中
実践についての管理の実施	中	徹	高	高	中

4.3.3 管理策単位の実効強度の判定

管理策単位の実効強度レベルは，その固有強度レベルを，管理策単位の実践レベルにより決まる強度レベルの補正値で補正したものである．

この実践レベルによる固有強度レベルの補正値も，管理策の特性にも依存するため，厳密には管理策単位に設定すべきではあるが，表10に示す値をその目安におくことができると考える．

表 10 実践レベルによる固有強度の補正値

実践レベル	要求事項の実践率の尺度	実践レベルによる強度レベルの補正値
5	100%	−0
4	98%～100%	−1
3	95%～98%	−2
2	90%～95%	−3
1	90%未満	−4

5 まとめ

本稿で提案した，セキュリティ対策の基本要素である管理策についての評価方法は，手間のかかる手法ではあるものの，以下のような特長を持つことから，その有用性は高いと考えられる．

- 細かい点まで統一的な基準を用いた評価を行うため，多岐にわたる管理策についての評価を、客観的でばらつきのないものできる
- 評価は，管理策構成要素レベルからの評価の積み上げによるため、対策上の欠陥を，計画面と実践面に分けて具体的に指摘できる
- 管理策ごとにその強度レベルが示されるため，対策の過不足の判断が容易で，評価を対策の最適化に結びつけることができる
- 評価が統一的な基準をもととした強度レベルで表現されるため，他システムとの比較を容易にする

しかし，その実用化には課題が少なくない．実用化の鍵を握る課題としては，以下があげられる．

- セキュリティ対策の計画，実装，実践の管理の基本単位であり，評価の原点となる管理策の構成の標準の確立
- 管理策ごとに設定しなければならない表 4，表 5，表 8 に示すような管理策の固有強度レベルや実効強度レベルを判定するために必要となる各種の判定表作成作業の労力を低減するとともに，管理策間での判定基準のバラツキを小さくするための，管理策の特性タイプごとのこれらの判定表のテンプレートの確立
- 細かい評価の積上げとなる評価作業の労力を低減するために必須となる評価支援ツールの整備

提案する評価技法について議論すべきことは少なくないが、これらの議論は，セキュリティ対策の評価における本質的な課題の解決につながると確信する．このため，ISO/IEC27003 や ISO/IEC 27004 の検討動向や，セキュリティ対策の評価についてのさまざまな取り組みを参照しながら，実用化に向けた本評価技法のブラッシュアップに加え，実証モデルの開発も今後の研究課題としたい．

文 献

[1]重松孝明，周秉慧，堀良彰，櫻井幸一，“情報セキュリティ対策の評価技法についての考察，” 情報処理学会研究報告，CSEC-41，pp.91-96，2008.

[2]Takaaki Shigematsu, Bin-Hui Chou, Yoshiaki Hori, Kouichi Sakurai, “Methodology for Evaluating Information Security Countermeasures of a System,” 2008 International Conference on Information Security and Assurance,” pp. 433-438, 2008.