社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－CSEC－41 (15)
2008／5／23

情報システムのセキュリティレベルを評価する手法の提案

橋本 和也　　小田原 育也
東芝ソリューション株式会社 IT技術研究所

あらまし 情報システムに関連したセキュリティ事故が報告されているが、これは現状のセキュリティレベルを把握できていないことが一因と考えられる。現状を把握するためには、まず情報システムのセキュリティレベルを可視化することが必要となる。しかし、現存の多くの評価基準が採用しているセキュリティ対策の実施件数のバランスで可視化する方法では、セキュリティ対策の質までは可視化されないため、現状の把握が不十分になってしまうと考えられる。本稿では、セキュリティ対策の実施件数と質の 2 つの観点でセキュリティレベルを表現しかつセキュリティに疎くとも理解しやすい指標と、利用者が観測可能な情報でセキュリティレベルを評価する手法を提案する。

The Proposal of Methodology for Evaluating Security Level of Information Systems

Kazuya Hashimoto　　Ikuya Odahara
Advanced IT Laboratory, Toshiba Solutions Corporation

Abstract We thought that being not able to grasp current security level of information systems contributes to security incident. To grasp the level, security level of information systems should be made visible. However, existing security evaluation methodology cannot show quality of security countermeasure because of evaluating only the number of security countermeasure. So it is thought that the grasp of current security level becomes insufficient. In this paper, we propose measures that show the number and quality of security countermeasure. we also propose a methodology for evaluating security level of information systems.

1 はじめに

情報システムの脆弱性をついた攻撃や誤操作や設定ミスなどの内部要因により、情報漏えいといったセキュリティ事故が報告されている。企業ではISMS (Information Security Management System) 認証の取得などの活動を通して、セキュリティ事故の発生を防止しようとしているが、それでもセキュリティ事故は後を絶たない。

この一因として、現状のセキュリティレベルを正しく把握できていないことが考えられる。これは、現状のセキュリティレベルの評価方法では、対策さえ実施されていれば評価が高くなるため、対策の質までも含めた形で評価できていないと考えられるためである。このような評価方法ではセキュリティが十分に確保されているとは言いがたい。

そこで、我々はセキュリティレベルを評価する

指標として、セキュリティ対策の実施件数と質の2つの観点が重要であると考えた。しかし、セキュリティレベルの質を扱うのは容易ではなく、システムの利用者、運用者には理解しづらい。

本稿では、前述の2つの観点を考慮し、かつ情報システムの利用者が得られる情報を利用することで、セキュリティの知識が少なくても理解しやすい指標で情報システムのセキュリティレベルを評価する手法を提案し、その試行結果について考察する。

2 課題

情報システムを運用していく上で必要とされるセキュリティ対策を評価する場合には、ISMSや情報セキュリティ対策ベンチマーク [1]、Common Criteria (ISO/IEC15408, 以後 CC)などの方法が存在する。

ISMS や情報セキュリティ対策ベンチマークは各セキュリティ対策の実施件数のバランスを可視化する方法であるため、必要なセキュリティ対策がどれだけ網羅されているかについては可視化することができるが、セキュリティ対策の質までは可視化できないと考えられる。そのため、セキュリティレベルを評価するためには、セキュリティ対策の実施件数だけではなく、セキュリティ対策の質を評価することが重要となる。

一方、CC はセキュリティ対策の質について評価する基準である。CC では、情報システムに必要なセキュリティ機能要件とセキュリティ保証要件に基づいて情報システムを評価する。CC の評価は厳密であり、その評価結果を理解するためにはセキュリティの知識が必要である。評価結果が利用者にわかりにくければ、セキュリティ対策の必要性を理解することが難しくなり、結果として利用者が本当に必要なセキュリティ対策を実施しないという可能性もある。このため、セキュリティの質を評価する際には、評価に利用する入力情報や評価結果をセキュリティの知識が少ない利用者でも理解できるものにする必要がある。

そこで本稿では、本来必要とされるセキュリティ対策がどこまで実現されているかとセキュリティ対策の質とを評価する指標でありかつセキュリティの専門知識が少ない利用者でも理解しやすい指標と、この指標で情報システムのセキュリティレベルを評価するための手法とを提案する。

3 セキュリティレベル評価手法

2章で提示した課題の解決策として、本章ではセキュリティ対策の実施件数とセキュリティ対策の質のそれぞれを表現する指標とこの指標で情報システムのセキュリティレベルを評価する手法について記述する。

3.1 セキュリティレベルの評価指標

本稿で提案する情報システムのセキュリティレベルを評価するための指標とその定義を図 1 に示す。

図 1 で示すように、セキュリティレベルは網羅性とアメニティ性の 2 つの観点を組み合わせて表現される。また、アメニティ性の質についてより詳細にするためにアメニティ性を表現する4つの指標を定義する。それぞれの指標に該当する具体的な例を表 1 に示す。

図 1 の定義と表 1 の例で示すように、視認性は利用者からセキュリティ対策が見えることで安心してシステムを利用できるかどうかを、必然性はセキュリティ対策を回避する手段が存在しないかを評価するものであり、いずれもセキュリティ対策の安全性を評価する指標である。また、透過性はセキュリティ対策が利用者に負荷を与えないどうかを、一貫性はセキュリティ対策の実

装方針によって利用者の誤操作を導かないかを評価するものであり、いずれもセキュリティ対策の利便性を評価する指標である。

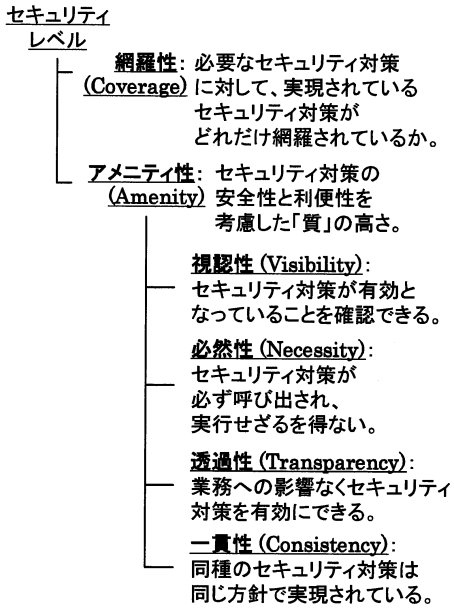

図 1　評価指標

表 1　アメニティ性の各指標を満たす例

視認性の定義を満たす例	暗号化機能において、暗号化通信されている状態がアイコン等で確認できる。
	アクセス制御機能において、利用者の権限で利用できるメニューしか画面に表示されない。
必然性の定義を満たす例	暗号化機能において、暗号化しなくてもデータを送信できるようになっている。
	認証機能において、正規の認証画面を利用する以外にログインする手段がない。
透過性の定義を満たす例	暗号化機能において、送信時に利用者が意識することなく暗号化される。
	認証機能において、認証に手間がかからない。
一貫性の定義を満たす例	認証機能において、業務機能を利用するための利用者認証機能と、利用者属性を変更するための利用者認証機能とが同じインタフェースで実現されている。
	パスワード認証機能において、パスワードポリシがどの認証でも統一されている。

3.2 評価手法の手順

情報システムの利用者が観測可能な情報を利用して、セキュリティレベルを評価する手順を以下に示す。この手順は、事前に行っておくべきことと、評価時に行うことの 2 種類に大別される。

- 事前に行う手順

手順 0：あるべき姿の定義

- 評価時に行う手順

手順 1：評価対象の具体化

手順 2：現状の情報収集

手順 3：評価結果の分析

以下の項では、各手順の要点について記述する。

3.2.1　あるべき姿の定義

手順 0 では、情報システムのあるべき姿を定義する。

網羅性を評価するためには、セキュリティの専門家が情報システムに必要なセキュリティ対策を検討した「あるべき姿」を用意する必要がある。これは、理想的な「あるべき姿」と評価対象とのギャップを測ることでセキュリティレベルが表現されるためである。このあるべき姿を基本モデルと呼ぶことにする。

本手法では、情報システムの機能やシステム構成を表す構成要素に対して「どのセキュリティ対策があるべきか」を、セキュリティの専門家が基本モデルとして事前に定義しておき、これと評価対象を比較できるようにする。この際、基本モデルの構成要素を抽象的にしておくことで、専門家のノウハウが入った基本モデルを他システムの評価に流用できる。基本モデルは表 2 のようなマトリクスで表現される。

表 2　基本モデルの一例

		セキュリティ対策			
		主体認証	権限管理	暗号化	・・・
構成要素	業務機能	○	―	○	・・・
	業務管理機能	○	○	○	・・・
	通信路	―	―	○	・・・
	・・・	・・・	・・・	・・・	・・・

表 2 の例において、「○」は当該行の構成要素に対して当該列のセキュリティ対策が必要であ

ることを示し、「－」は当該行の構成要素に対して当該列のセキュリティ対策が不要であることを示している。例えば、業務機能には主体認証が必要であることを示している。

3.2.2　評価対象の具体化

手順 1 では、基本モデルで抽象的に定義された構成要素に対して、評価担当者が実際に観測可能な画面や機能を決定することで、評価を行う範囲を定義する。

3.2.3　現状の情報収集

手順 2 では、情報システムの現状について情報収集する。この手順で、評価担当者はまず評価の際に利用する質問の一覧を作成し、次に作成された質問項目を見て情報システムの評価を行う。この質問の一覧を「質問リスト」と呼ぶこととする。

質問項目は、表 2 の基本モデルで「○」がついた項目ごとに作成される。その内容は、手順 1 で定義した画面や機能に対してセキュリティ対策がどうなっていればよいかを確認できるようにしておく。質問リストの例を表 3 に示す。表 3 では、個人情報管理機能で主体認証がどうなっていればよいかを確認するための質問を記述されている。また、質問ごとに「貢献度」を定義している。これは、3.1 節で定義した網羅性とアメニティ性の 4 つの指標に対して、質問内容を満たすことがどれだけ指標に貢献するかを定義したものである。質問内容を満たしている場合、当該質問の貢献度を加算していく。これにより、どの機能がどの指標をどれだけ満たしているかがわかるようになる。

例えば、表 3 において No.2 の質問内容を満たした場合、No.2 で定義された貢献度 1 が必然性に加算される。

質問リスト作成後、評価担当者が質問に対して回答する。

表 3　質問リストの例

No.	質問	貢献度
1	[個人情報管理機能]に[主体認証]が、存在しているか。	網羅性 1
2	[個人情報管理機能]の[主体認証]が、回避できないようになっているか。	必然性 1
3	[個人情報管理機能]の[主体認証]が、意識しなくとも有効になっているか。	透過性 1

3.2.4　評価結果の分析

手順 3 では、回答を集計し、評価結果を分析する。

まず、手順 1 で定義した評価範囲全体の網羅性とアメニティ性を求める。網羅性とアメニティ性を算出するイメージを図 2 に示す。

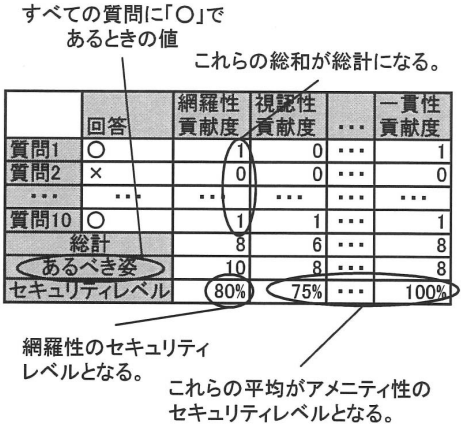

図 2　網羅性とアメニティ性の算出

質問リストに記載されたすべての質問に対して「○」と回答された質問の貢献度を図 2 のように指標ごとに加算していき総計を取る。この総計とあるべき姿を比較してどの程度ギャップが存在するかを算出する。具体的には、総計があるべき姿に占める割合を求める。網羅性についてはこの割合がセキュリティレベルとなる。アメニティ性については、アメニティ性の 4 つの指標ごとに算出した割合の平均値がセキュリティレベルとなる。

また、情報システムのどこが脆弱かをより詳し

く分析するために、構成要素ごと、セキュリティ対策ごとに網羅性、アメニティ性を求めておく。

最後に、算出された網羅性とアメニティ性から、情報システムのどこが脆弱かを分析する。評価範囲全体のセキュリティレベルを基準とし、これよりもセキュリティレベルが低かった構成要素やセキュリティ対策が情報システムの脆弱な部分であるとわかる。

図 2 で示すように指標ごとに貢献度を集計することで、あるべき姿とのギャップが可視化され、セキュリティ対策の実施件数と質のセキュリティレベルを評価できると考えられる。さらに、分析によりどのセキュリティ対策のどの指標のセキュリティレベルが低いかを具体的に示せるため、セキュリティの知識が少ない利用者にもわかりやすい評価結果を提示できると考えられる。

4 手法の試行と考察

4.1 試行の概要

今回の試行では、報告書を新規作成し、ワークフローに従って回覧し、コメントや承認をもらう報告書管理システム(試験環境)を評価対象とした。基本モデル作成時に必要な構成要素とセキュリティ対策を表 4 に示す。

表 4 基本モデルに関するデータ

構成要素	業務機能、業務管理機能、通信路
セキュリティ対策	主体認証機能、アクセス制御機能、権限管理機能、証跡管理機能、暗号化機能、電子署名機能

4.2 試行結果

本手法を試行して得られた評価結果の一部を表 5、図 3、図 4 に示す。

まず、セキュリティ対策の実施件数を示す網羅性を確認する。表 5 より、網羅性の値が 52%とあるべき姿(100%)の約半分となっていることがわかる。この原因を追究するため、セキュリティ対策ごとに網羅性を計算した図 3 を見ると、電子署名機能、暗号化機能、証跡管理機能が不足していることがわかる。これより、評価対象システムでは例えば、下記のようなセキュリティ対策を補うことでセキュリティレベルが向上すると考えられる。

- 証跡管理機能：ログを管理できる機能。
- 暗号化機能:取り扱うデータを暗号化して保存する機能。
- 電子署名機能：ワークフロー時に誰が申請、承認したかを示す電子署名を付加する機能。

表 5 評価対象のセキュリティレベル

	セキュリティレベル
網羅性	52%
アメニティ性	95%
視認性	81%
透過性	100%
必然性	100%
一貫性	100%

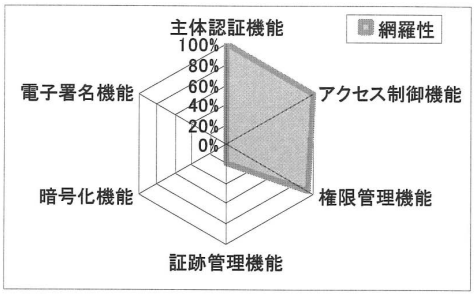

図 3 セキュリティ対策ごとの網羅性

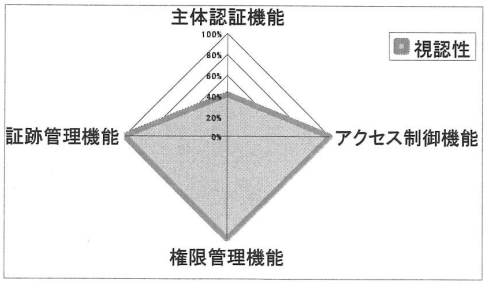

図 4 セキュリティ対策ごとの視認性

次に、情報システムで実現されているセキュリティ対策(52%)の質を示すアメニティ性を確認する。表 5 より、アメニティ性の値はあるべき姿(100%)に近いものの、視認性の値が低くなっていることがわかる。この原因を追究するため、セキュリティ対策ごとに視認性を計算した図 4 を見ると、主体認証機能の視認性が低いことがわかる。これより、評価対象システムでは例えば、下記のようにセキュリティ対策を改修することで、セキュリティレベルが向上すると考えられる。

- 認証機能が実行されていることが利用者に見えるように改修すること。

4.3 考察

今回の評価で視認性について、質問内容を満たさなかった質問項目は「報告書新規作成の主体認証機能が、視認性を満たしている。」であった。

このシステムでは、認証成功後に画面上で利用者 ID や利用者名が表示されていなかったため、誰がログインしているかがすぐにはわかりづらく、共用端末などでは間違って第三者がログインしている画面で操作してしまう可能性がある。これを防止するためには、図 5 のように画面上のわかりやすいところに誰がログインしているかを表示するように改修すべきである。図 5 のように改修することで、視認性に関する質問に対して質問内容を満たすため、視認性のセキュリティレベルを向上できる。

この例では、視認性が低い構成要素に対して、セキュリティ対策を実現・改修することで、視認性が向上することを示した。以上より、今回の試行では、網羅性によりセキュリティ対策の実施件数を表現できることと、セキュリティ対策の質が低い場合にも本稿で提案した指標を利用することでその質を表現できることを視認性についてだけであるが確認できた。

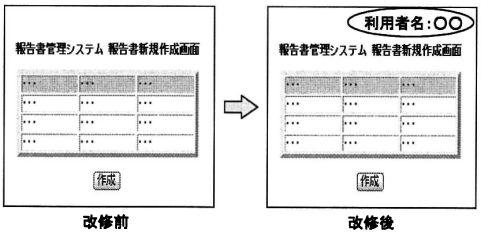

図 5 セキュリティ対策の改修例

5 まとめ

本稿では、本来必要なセキュリティ対策がどこまで実現されているかだけではなく、セキュリティ対策の質も合わせて評価するような指標および手法を提案した。また、試行により、提案した指標でセキュリティ対策の実施件数だけではなく、セキュリティ対策の質も表現できることを確認した。

今後は、今回の試行では確認できなかった視認性以外の指標についても質を表現できているかを検証するとともに、利用者にとって本当にわかりやすい指標や評価結果となっているかを客観的に確認していくことが課題である。

参考文献

1) 情報処理推進機構, 組織の情報セキュリティ対策自己診断テスト ～情報セキュリティ対策ベンチマーク～ http://www.ipa.go.jp/security/benchmark/
2) 政府機関の情報セキュリティ対策のための統一基準（2008 年 3 月版［第 3 版］）http://www.nisc.go.jp/active/general/pdf/k303-072.pdf