情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2009-SE-164 No.4
Vol.2009-EMB-13 No.4
Vol.2009-CSEC-45 No.4
2009/5/28

情報セキュリティ対策状況の評価手法の提案

武曽徹[†]　　飯田茂[††]

情報システムのセキュリティ対策の実施強度を評価する手法として，対策の強度を対策実施の有無とその運用実施水準で指標化し，この２つの指標を対策箇所とセキュリティ脅威を軸とする二次元マップ上に可視化して対策の弱点を分析する手法について提案する．

A Proposal of Method to Evaluate Information Security Measures

Toru Muso[†]　and　Shigeru Iida[††]

In this paper, a method to evaluate effectiveness of current security measures on an information system is proposed. In the method, the effectiveness of the security measures is expressed as indicators to show not only whether if the measures are taken, but also how effectively they are operated. And the indicators are visualized on a two-dimensional map which has axes of where the measures are taken, and security threat.

1. はじめに

企業での情報システムの導入範囲が拡大する中，個人情報や機密情報の漏洩，ウィルス感染などの情報セキュリティ事故による被害を抑えるために実施する，情報セキュリティ対策の重要性が高まっている．

従来の情報セキュリティ評価では，例えば個々のシステムに対して質問表を使った診断を行い，決められた対策を実施しているかどうかのみで評価しているが，それだけでは対策の実施強度を正しく把握して現状の弱点の分析や的確な強化施策の策定を実施することはできない．情報セキュリティ対策の実施強度を定量的に測り，弱い部分がどこにあるかをわかりやすく可視化して分析可能な手法の確立が必要である．

本稿では，対策の運用実施水準を測る５段階の運用レベル定義を導入して，対策実施率と対策の運用レベル充足率の２つの指標で評価を行うこととした．収集した診断結果データからこれらの指標を算出し，対策箇所と脅威を軸とした二次元マップ（ドメインリスクマップ）上に可視化することにより，現状の情報セキュリティ対策の実施強度を分析・評価する．

2. 課題

情報セキュリティ対策を成熟度により評価する手法[1]があるが，成熟度は実施強度（どれだけ効果的な対策になっているか）を直接的に示すものではない．対策の実施強度を評価する場合，組織のセキュリティポリシーをもとに対策のベースラインを定め，それらの対策を実施しているかどうか（実施の有無）を調べて，対策実施率により評価する方法が一般的である．しかしこの方法には以下のような課題がある．

(1) **対策強度を正しく把握できない**

実施有無のみの評価では対策を実施していれば“有”となり，その対策をどのように実施しているかが考慮されない．例えば，ウィルス対策ソフトのパターンファイル更新を，毎日自動的に更新されるようにしているのか，月に 1 回程度手動で更新しているのでは，ウィルス侵入に対する対策の効果は異なるが，どちらも同じ“有”と評価されてしまう．

(2) **的確な施策の策定が困難**

また，評価結果からセキュリティ強化のための施策を考える場合に，何の目的に，システムのどの部分に対策すればよいかがわからないため,的確な施策の策定が難しい．

[†] 三菱電機株式会社
Mitsubishi Electric Corporation
[††] 三菱電機インフォメーションシステムズ株式会社
Mitsubishi Electric Information Systems

Vol.2009-SE-164 No.4
Vol.2009-EMB-13 No.4
Vol.2009-CSEC-45 No.4
2009/5/28

本稿では，情報セキュリティ対策をどのように実施しているかという要素を含めた対策実施強度の評価手法と，現状の対策の弱点を明確にして，強化のための施策をより的確に策定できるようにする手法について提案する．

3. 解決のための手法

課題を解決するための手法として，対策の運用水準を表す運用レベルによる対策実施強度の評価手法と，対策箇所とセキュリティ脅威を軸とした二次元マップ（ドメインリスクマップ）上に現状の情報セキュリティ対策の実施強度を可視化する手法について記述する．

3.1 運用レベルによる評価

対策の実施強度には，従来までの対策実施の有無を表す機能強度の他に，その対策をどのように運用しているかを表す運用強度がある．運用強度を評価する手法として，運用レベルによる評価を導入する．まず，表 1 に示すように，運用レベル項目を定義する際の視点を４つに整理した．これらの視点に基づいて，各情報セキュリティ対策に対して運用レベル項目を設定する．

表 1　運用レベル項目例

視点	意味	運用レベル項目例
①技術的な強度	対策を実施する際に適用する技術によるレベル	暗号化や認証の技術的な強度 対策の自動化の度合い システム構成要素の冗長度，など
②時間的な強度	対策を実施する時間間隔や，期間によるレベル	監視や分析のインターバル アクセス権限等の見直しの間隔 不正検知のリアルタイム性，など
③距離的な強度	対策を実施する際の分離の度合いによるレベル	バックアップの保管場所 代替処理拠点の場所，など
④管理的な強度	実施する対策の範囲，網羅度や，制限の厳しさ，統合の度合いなどによるレベル	対象範囲の網羅度合い 管理の一元化の度合い，など

設定した運用レベル項目に対して，公開されているガイドライン[2]などを参考に，対象組織の基準に合せて５段階の運用レベル定義を行う．表 2 に運用レベル定義例を示す．

表 2　運用レベル定義例

対策	運用レベル項目	運用レベル定義
ウィルス対策ソフトの定期的なパターン更新	更新のインターバル	5　リアルタイム
		4　１日以内
		3　１週間以内
		2　１ヶ月以内
		1　それ以上
システムへのアクセス時の主体認証	認証方式	5　－
		4　生体認証
		3　OTP/乱数表
		2　ID/PW
		1　共通 ID/PW

評価するときには，各対策を実施しているかどうかの評価とともに，実施している場合は，どの運用レベルで実施しているのかを１～５から選択する．

3.2 ドメインリスクマップによる分析

情報セキュリティ対策の実施強度を評価する場合，その対策が，どのセキュリティ脅威に対して（Why），どの対策箇所に実施するものなのか（Where）がわかると，評価結果をもとにした新たな対策を立てやすい．ドメインリスクマップは，情報セキュリティ対策を網羅的に表現するもので，セキュリティ脅威と対策箇所を軸とした二次元のマップである．図 1 にドメインリスクマップの概観図を示す．

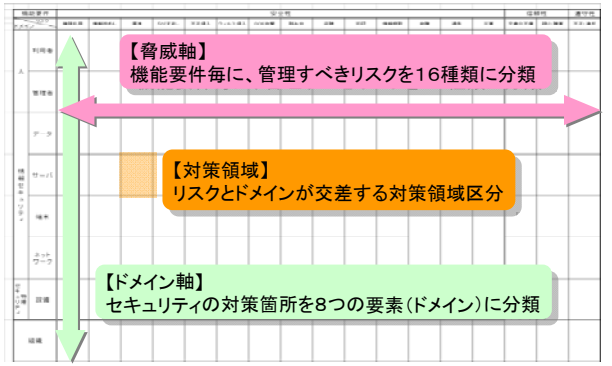

図 1　ドメインリスクマップの概観図

Vol.2009-SE-164 No.4
Vol.2009-EMB-13 No.4
Vol.2009-CSEC-45 No.4
2009/5/28

横軸には，情報改ざん，漏洩などのセキュリティリスクの要因となる脅威を定義する．また，縦軸には，対策を実施する対象（利用者，端末，ネットワーク，サーバなどの情報システムが提供する業務の構成要素）を対策箇所（ドメイン）として定義する．図 2 に，各ドメイン間の関係を示す．

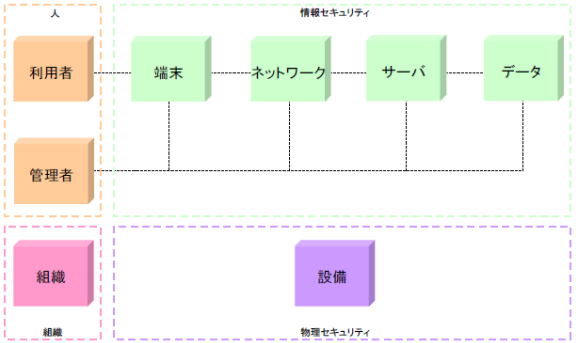

図 2　対策箇所（ドメイン）間の関係

ドメインリスクマップ上で，それぞれの脅威と対策箇所が交わる領域を対策領域と呼び，この対策領域ごとに，４．１節で記述する２つの指標値を表示する．これにより，どの脅威に対する，どの対策箇所への対策が不足しているのかを示すことができる．

4.　評価方法

4.1　評価指標

対策の機能強度，運用強度について，それぞれ対策実施率，運用レベル充足率を使って評価を行う．それぞれの指標の計算方法は以下の通りである．

$$\text{対策実施率}(\%) = \frac{\text{実施している対策項目数}}{\text{実施すべき全ての対策項目数}} \times 100$$

$$\text{運用レベル充足率}(\%) = \frac{\text{実施している運用レベル合計}}{\text{要求されている運用レベル合計}} \times 100$$

業務やシステムによって実施する対策項目や運用レベルへの要求は異なる．あらかじめ要求されている対策項目と運用レベルをベースラインとして設定しておき，その要求に対して実施している対策がどの程度実現されているかを表す指標として，運用レベル充足率を用いる．表 3 に，算出の例を示す．

表 3　指標の算出例

脅威	No	対策	実施有無	運用レベル	
				要求	実施
情報漏洩	1	対策項目 A	○	4	2
	2	対策項目 B	○	3	3
	3	対策項目 C	×	4	－
		・・・・・			
	12	対策項目 X	○	4	1
		実施項目数	10		
		運用レベル合計		40	20

この例の場合，対策実施率は，12 項目中 10 項目実施なので 83%となるが，運用レベル充足率は要求 40 に対して実施 20 なので，50%となり，情報漏洩に対する対策は実施されているが運用強度が弱いことがわかる．

4.2　評価の手順

現状の情報セキュリティ対策の実施強度の評価は，以下のように①～⑥の手順で行う．

(1)　評価の準備

①実施すべき対策項目の決定

組織で定められたセキュリティポリシーや，実施手順などの規程から，対象となるシステムで実施すべき情報セキュリティ対策項目を洗い出し，その対策項目が実施されているかどうかを確認するためのセキュリティ診断リストを作成する．

②対策項目の属性設定

①で作成した対策項目の属性として，どの脅威に対する対策なのか，どの対策箇所への対策なのか，の分類を行う．

③運用レベルの設定

対策項目ごとに，運用レベル定義の４つの視点に基づいて運用レベル項目と，１～５の各レベルでの実施内容を設定し，セキュリティ診断リストに追加する．セキュリティ診断リストの構造の一例を図 3 に示す．

Vol.2009-SE-164 No.4
Vol.2009-EMB-13 No.4
Vol.2009-CSEC-45 No.4
2009/5/28

対策	実施有無	運用レベル						
		項目	1	2	3	4	5	実施
対策項目A		インターバル	リアルタイム	1日以内	1週間以内	それ以上	問題発生時のみ	
対策項目B		…	…	…	…	…	…	
対策項目C		…	…	…	…	…	…	
·····		…	…	…	…	…	…	

↑ 実施有無（○／×）　　↑ 実施レベル（1～5）

図 3　セキュリティ診断リストの構造例

(2) 評価の実施

④現状の対策状況の調査

対象システムの運用担当者に，セキュリティ診断シートへの回答を依頼する．回答結果をもとに，詳細の運用レベル等についてヒアリングを行う．

⑤ドメインリスクマップの作成

ヒアリングの結果から，対策実施率と運用レベル充足率を脅威と対策箇所ごとに集計して，ドメインリスクマップ上へ表示する．

⑥対策実施強度の分析・評価

ドメインリスクマップから，どの脅威に対するどの対策箇所への対策が不十分なのかを分析する．

5. 有効性の検証

有効性の検証として，実システム（電子メールシステム）を対象に３章および４章で記述した評価手法を適用して，現状のセキュリティ対策の実施強度の評価を行った．既存のセキュリティ対策項目を利用してセキュリティ診断リストを作成し，リストへのシステム運用者からの回答とインタービューにより，現状の対策状況を調査した．調査結果データから対策実施率と運用レベル充足率を求め，ドメインリスクマップによる可視化を行った．評価の対象となった対策項目の総数は 172 項目であった．

5.1 検証結果

図 4 にドメインリスクマップによる検証結果（抜粋）を示す．

各対策領域で，対策実施率を○印で上段に，運用レベル充足率を□印で下段に表示している．また，その数値によって５段階に色分けをした．黒に近い方が各指標の低い数値，白に近い方が高い数値を示している．また，運用レベルの乖離が２段階以上の対策項目が含まれる対策領域には，「！」のマークを表示した．

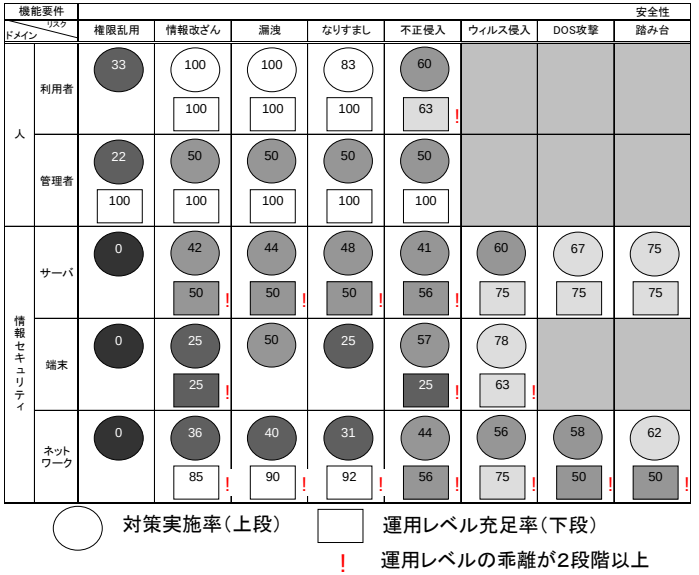

図 4　検証結果（ドメインリスクマップ抜粋）

5.2 検証結果の分析

図 4 のドメインリスクマップを全体的に俯瞰することにより，以下のことを読み取ることができる．

- 権限乱用の脅威に対する対策が不足している．
- 情報改ざん，なりすましに対する，端末，ネットワークへの対策が不足している．
- 利用者，管理者への対策の運用レベルはほぼ確保されている．
- 情報改ざん，不正侵入に対する，端末への対策の運用レベルが低い．
- 情報改ざん，漏洩，なりすましに対する，ネットワークへの対策の運用レベルは概ね確保されているが，運用レベルがベースラインから乖離している対策項目が存在する．
- サーバ，端末，ネットワークには，運用レベルがベースラインから乖離している対策項目が存在する．

ドメインリスクマップにより判明した対策不足や運用レベルの弱点から，詳細分析すべき対策領域（脅威／対策箇所）の絞り込みを行い，次に絞り込んだ各対策領域において不足している対策項目，運用レベルを抽出・整理することにより，強化のため

Vol.2009-SE-164 No.4
Vol.2009-EMB-13 No.4
Vol.2009-CSEC-45 No.4
2009/5/28

に必要な施策を表 4 のように導出した．

表 4　実施すべき施策（抜粋）

実施すべき施策	対策箇所	脅威
共通 ID でなく，運用担当者ごとに特権 ID を割り当てる	管理者	権限乱用
アクセスログの取得と定期的な分析	サーバ 端末	権限乱用 情報改ざん 漏洩
セキュリティホールへの対応迅速化	端末	情報改ざん 不正侵入
ネットワークの不正アクセス監視	ネットワーク	権限乱用 情報改ざん 漏洩
外部ネットワーク接続時の主体認証の強化	ネットワーク	漏洩 なりすまし 不正侵入

5.3 考察

指標として運用レベル充足率を導入することにより，従来の評価ではわからなかった運用強度が不足している部分が明確になった．例えば，情報改ざんや不正侵入の脅威に対する端末への対策では，運用レベルが不足していることがわかり，セキュリティホールへの対応の迅速化が実施すべき施策として導き出された．また，ベースラインから乖離した運用レベルが抽出され，外部ネットワークから接続する際の主体認証方式の強化という施策が導き出された．

また，ドメインリスクマップ上に可視化することにより，セキュリティ脅威と対策箇所が交差する対策領域単位で，現状の弱点分析と実施すべきセキュリティ強化策の策定が可能となった．例えば，検証結果では権限乱用の脅威に対する対策に弱点が明確に示されており，運用担当者の特権 ID 付与方法の改善，アクセスログの定期的な分析，不正アクセス監視が実施すべき施策として導き出された．

本稿で提案した手法は，現状のセキュリティ対策の実施強度を把握し，より的確なセキュリティ強化策を策定するのに有効な手法であると考える．

6. まとめ

本稿では，情報セキュリティ対策の運用実施水準を表す運用レベルを含めて実施強度を評価する手法，及びどの脅威に対する，どの対策箇所への対策が不足しているのかをドメインリスクマップ上に可視化する手法について提案した．これにより，現状を把握して，強化のための施策をより的確に策定することが可能である．

しかしながら，検証を進める過程で，一部の運用レベルのベースライン設定が高すぎると思われるものが見つかった．要求される運用レベルは，業務が扱う情報の機密度や，システムのネットワーク接続形態などにより異なる．業務種別やシステム形態などの条件から，対象の組織や業務に応じたベースラインを設定する手法が必要である．また，今回の検証は全て自己申告による調査をベースにしているため，調査データに回答者の主観による誤りや漏れが入りやすい．システムの構成要素から直接取得したデータを併用して，回答内容の確認をすることで評価の信頼性が向上すると考えられる．今後は，これらの課題を解決するべく，手法の改善を図っていく．

参考文献

1) IPA 情報セキュリティ対策ベンチマーク，http://www.ipa.go.jp/security/benchmark/index.html
2) 総務省, ASP・SaaS の情報セキュリティ対策ガイドライン（2008/1/30）