

セキュリティマネジメント高度化サービス

要 旨

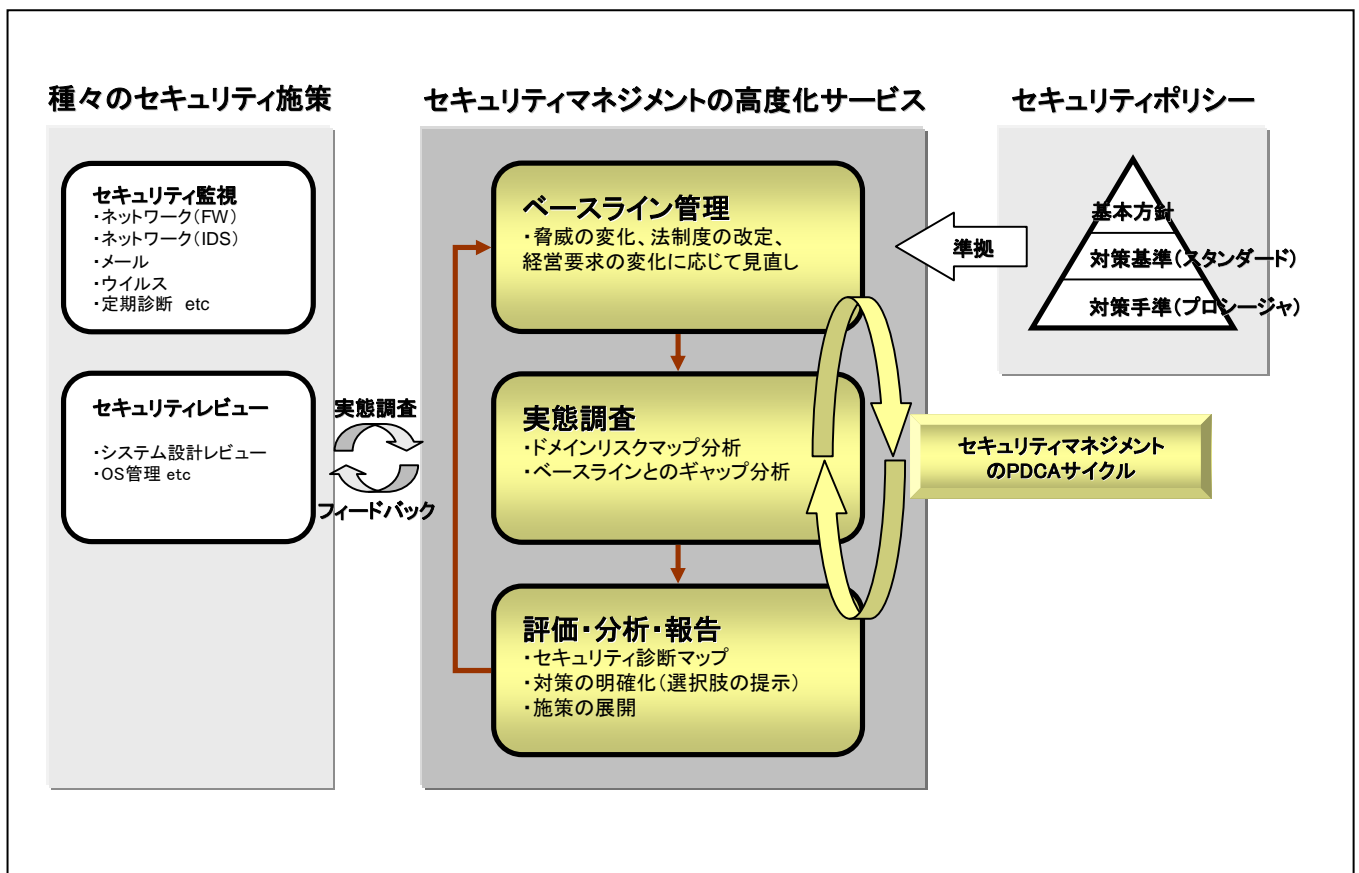
情報資産の安全性を脅かすセキュリティ脅威は年々複雑多様化しており、情報システム管理者には、セキュリティ対策を情報システム全体に漏れなく実施し、情報資産の安全性を維持管理して行く事が求められている。しかし、各種対策は情報システムの構成要素毎に個別管理されており、情報システム全体を俯瞰した対策の網羅性や妥当性を把握することができないという課題を抱えている。

三菱電機インフォメーションシステムズ株式会社(MDIS)では、本稿に記載するセキュリティマネジメント高度化サービスを三菱電機情報技術総合研究所と共同で創出し、大手金融機関を中心にこのサービスの導入を推進している。

このサービスは、情報システム全体のセキュリティ対策の網羅性、妥当性を評価・分析するためのマネジメントサ

ービスである。情報セキュリティ対策の実施強度を表す指標を、対策箇所と脅威を軸とした二次元マップを使って“見える化”して、システム全体を俯瞰した対策を評価・分析するところに特長がある。満たすべきセキュリティ水準をベースラインとして管理し、実態調査結果とベースラインとのギャップ分析に基づいて乖離する対策項目を漏れなく抽出することで、情報セキュリティ対策の実施強度を定量的に評価し、必要な施策を明確にしていく。

また、脅威の変化、法制度の改定、経営要求の変化に迅速に対応するために、セキュリティマネジメントのPDCAサイクルを確立することで、セキュリティ対策の実施水準を継続的に維持管理することができる。



セキュリティマネジメント高度化サービスの概念図

セキュリティマネジメント高度化サービスは、①セキュリティポリシーの基本方針、対策基準に準拠したセキュリティ水準をベースラインとして管理し、②種々のセキュリティ施策の実態調査結果とベースラインとのギャップ分析を行って、③対策箇所と脅威の二次元マップにより“見える化”して対策状況を評価・分析する。このPDCAサイクルを確立することで、セキュリティ対策の実施水準を継続的に維持管理する。

* 三菱電機インフォメーションシステムズ株式会社

** 三菱電機株式会社 情報技術総合研究所

1. ま え が き

情報資産の安全性を脅かすセキュリティ脅威が増大し、情報セキュリティ対策の重要性が益々高まっている。

一口にセキュリティ脅威と言っても、盗聴、改ざん、ウイルス等、様々な脅威が存在する。その対策も端末、サーバ、ネットワーク等のシステム構成要素全般、さらには、人的、組織的な側面にも及び、情報セキュリティ管理者には、広範囲で漏れのない対策の実施が求められている。

このためには、セキュリティマネジメントのPDCAサイクルを確立し、情報セキュリティ対策の実施強度を定量的に測り、システムの何処に弱い部分があるかを分りやすく俯瞰できるセキュリティ分析手法と、満たすべきセキュリティ水準の継続的な維持管理が必要である。

セキュリティマネジメント高度化サービスでは、セキュリティ対策の運用方法の強度を測る5段階の運用レベル定義を導入し、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。これらの指標は収集した診断結果データから算出し、脅威と対策箇所を軸とした二次元マップ上に可視化し、情報セキュリティ対策の状況を分析・評価する。

2. 従来の手法が抱える課題

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を実施の有無で評価して、その対策実施率で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、ウイルス対策ソフトのパターンファイル更新を、毎日自動的に更新しているのと、月に1回程度手動で更新しているのでは、ウイ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、何の目的で、システムのどの部分に対策を施せばよいかかわからないための的確な施策の策定が難しい。

3. 解決のための手法

セキュリティマネジメント高度化サービスでは、課題(1)を解決するため、対策をどのように実施しているかを表す運用レベルを含めた対策の実施強度の評価手法を導入した。また、課題(2)を解決するため、セキュリティ脅威と

対策箇所を軸とした二次元マップ（これをドメインリスクマップと呼ぶ）に評価結果を表示させ、現状の情報セキュリティ対策の弱点を可視化する手法を導入した。

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。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が、その際の視点は以下のような4つに整理できる。

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を表す。

② 時間的な強度

対策を実施する時間間隔や、期間によるレベルを表す。

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を表す。

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を表す。

これらの視点ごとに、各視点で設定される運用レベル項目を表1に示す。

表 1. 運用レベル項目例

視点	運用レベル項目例
① 技術的な強度	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	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	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	対象範囲の網羅度合い 管理の一元化の度合い、など

運用レベル項目に対して、公開ガイドライン⁽²⁾等を参考に、対象組織の基準に合わせて5段階のレベル定義を行う。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
個人情報へのアクセスのログ分析	分析のインターバル	5 リアルタイム
		4 1日以内
		3 1週間以内
		2 それ以上
		1 問題発生時
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状況を評価する場合、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（Where）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、セキュリティ脅威と対策箇所を軸とした二次元マップで、情報セキュリティ対策を網羅的に表現する。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

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。縦軸には、対策箇所（ドメイン）として、利用者、データ、サーバ、ネットワーク、端末などの業務を構成する要素を定義する。

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、それぞれ以下の指標を使って評価を行う。

機能強度： 対策実施率

運用強度： 運用レベル充足率

各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それに対する運用レベルを、ベースラインとして設定しておく。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、対策実施率と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	要求	実施
情報漏洩	1	通信路の暗号化	○	○	4	2
	2	個人データ暗号化	×	—	—	—
	3	ログ分析	○	×	3	—
	4	○	○	4	4
				
	15	○	○	4	1
		対策項目数	12	10		
		運用レベル合計			40	20

この例の場合、対策実施率は要求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%となる。このことから、情報漏洩に対する対策は実施されているが運用の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状況の評価は、以下のよう①～⑥の手順で行う。

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等の規程から、対象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す。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対策項目の分類

①で作成した各対策項目を、ドメインリスクマップの軸である、セキュリティ脅威と対策箇所で分類する。例えば対策項目が“通信路の暗号化”であれば、セキュリティ脅威：情報漏洩、盗聴、対策箇所：ネットワークとなる。

③運用レベルの定義

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表4.に示す。

表 4. セキュリティ診断リストの構造例

対策	実施有無	運用レベル					実施
		項目	1	2	3	4	
対策項目A		インターネット	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)

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現状の対策状況の分析・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. 評価手法の適用事例

5.1 評価結果

メール等のサービスを提供するイントラネットシステムを対象に、210項目の対策項目について運用レベル定義を行い、セキュリティ対策状況の評価を行った。図 2 にドメインリスクマップによる評価結果（抜粋）を示す。

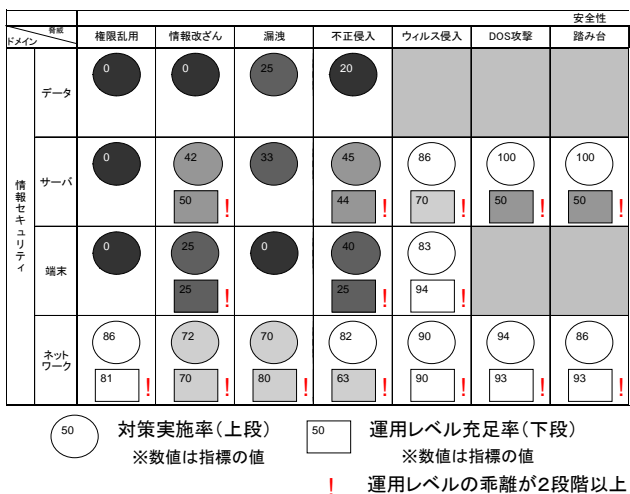


図 2. 評価結果（抜粋）

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おり（内部の数値は各指標の値）、その指標値によって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、対策の運用レベルがベースラインから乖離しているものを漏れなく抽出するため、2段階以上乖離している場合には、その対策領域に“!”マークを表示した。この結果から以下のことを読み取ることができる。

- ネットワークに対する対策は実施されているが、データや端末への対策が不足している。
- 権限乱用の脅威に対する対策が不足している。
- 権限乱用、情報改ざん、不正侵入に対するデータへの対策が不足している。

- 情報改ざんと不正侵入の脅威に対する端末への対策の運用レベルが良くない。
- DOS 攻撃や踏み台に対するサーバへの対策の実施はできているが、運用レベルが不足している。
- 全体として、運用レベルが乖離している対策項目が存在している。

5.2 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、従来の評価では隠れていた、対策が実施されていても運用強度が不足している部分が明確になった。例えば、DOS攻撃や踏み台に対するサーバへの対策の実施はできているが、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強化策として導き出された。

また、ドメインリスクマップ上に可視化することにより、セキュリティ脅威や対策箇所ごとに、より細かく対策の弱点を分析することができるようになり、よりの確なセキュリティ強化策を考えられるようになった。例えば、権限乱用、情報改ざん、不正侵入に対するデータへの対策ができていないことが示され、暗号化やデータアクセスログの分析が実施すべき強化策として導き出された。

このように本稿で述べた手法は、現状のセキュリティ対策状況を把握し、よりの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。

6. むすび

本稿では、情報セキュリティ対策をどのように運用しているかという要素（運用レベル）を含めて実施強度を評価する手法について述べた。また、どの脅威に対する、どの対策箇所への対策実施や運用レベル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ことで、よりの確に強化施策を策定できることがわかった。この手法は、セキュリティマネジメントのPDCAサイクルの C と A にあたり、ベースライン管理と組み合わせることによりセキュリティ水準の継続的な維持管理が可能となる。

今後は、評価支援ツールの整備により、セキュリティ診断シートの作成、データの集計・分析などの評価作業の効率化を図って行く。また、対策に不備がある箇所には、強化施策を具体的に提示できるように、対策のベストプラクティスを集積し、これを対策箇所に関連付けて行く。

参 考 文 献

- (1) IPA(独立行政法人 情報処理推進機構), 情報セキュリティ対策ベンチマーク
- (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)