ネットワークセキュリティ対策の最適化

ー　経営視点×担当視点×PDCA＝最適化　ー

アブストラクト

１．研究の背景と目的

ネットワークの利便性が向上した反面、複雑化したネットワークの脆弱性をついた不正アクセスによる被害件数も増加している。個人情報保護法に代表される社会的なセキュリティ意識の高まりに伴い、不正アクセスによる被害は営業機会損失という企業経営そのものを揺るがしかねない問題となっている。

当分科会では、具体的なレベルで自社のネットワークセキュリティ対策状況を把握すること、および経営層の合意のもとにバランスのとれた対策を最適なレベルで維持することを研究の主題に据えた。

２．ネットワークセキュリティレベル評価表の作成

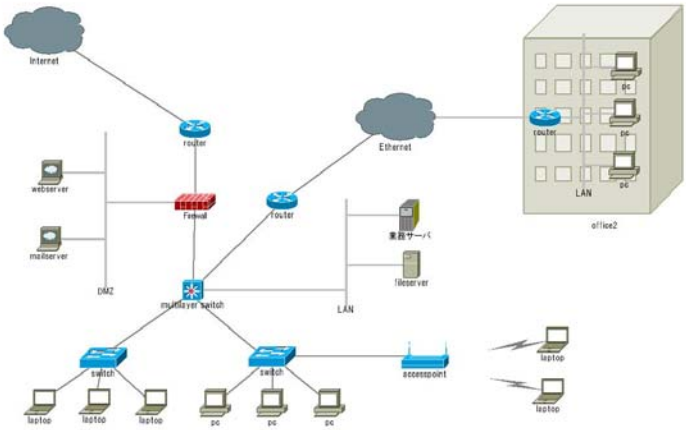
複雑化したネットワークに対し、以下のアプローチによりセキュリティ対策レベルの計測対象を絞りこんだ。

（１）典型的なネットワークの企業モデルを考察する。

（２）考察した企業モデルにて利用する機器をリストアップする。

（３）機器の重複を省き、最小構成のネットワーク「標準ネットワーク構成図（図表１）」を作成した。

図表１　標準ネットワーク構成図



構成図上の「ネットワークの経路」に着目して、以下の手法によりネットワークセキュリティを定義した。

（１）リスクが発生する｢始点｣と「終点」を探す。

（２）｢始点｣から「終点」に至るまでの経路をリストアップする。

（３）各経路での対策を列挙し、「リスク経路分析表（図表２）」を作成した。

図表２　リスク経路分析表（抜粋）

リスク名（大項目）	リスク名（小項目）	始点	経路1	経路2	経路3	経路4	経路5	終点
		インターネット	ルータ	FW	DMZ	メールサーバ	スイッチ	PC／サーバ
マルウェア／スパム	メールウィルス	プロバイダのウイルス対策サービスに加入している		ウイルスフィルタ機能付きFW導入	①GW型アンチウイルスソフトを導入 ②GW型アンチウイルスハードを導入	メールサーバ用アンチウイルスソフト導入		①PC用ウイルス対策ソフトの導入 ②最新のセキュリティパッチを適用したOSの導入
		インターネット	ルータ	FW	DMZ	メールサーバ	スイッチ	PC／サーバ
	スパムメール/フィッシング	プロバイダのウイルス対策サービスに加入している		スパムメールフィルタ機能付きFWを導入	GW型スパムメール対策ハードを導入	メールサーバ用スパムメール対策ソフトを導入		①PC用スパムメール対策ソフトを導入 ②最新のセキュリティパッチを適用したOSを導入
		インターネット	ルータ	FW	DMZ	サーバ	スイッチ	PC／サーバ
	ファイル共有ソフトを経由するウイルス			ウイルスフィルタ機能付きFWを導入				①PC用ウイルス対策ソフトを導入 ②最新のセキュリティパッチを適用したOSを導入
		PC	スイッチ	FW	ルータ	サーバ	スイッチ	PC／サーバ
	持ち込みPC・媒体から感		検疫機能付きのスイッチを導入	ウイルスフィルタ機能付きFWを導入		Active Directory（ないし、それに準ずるユーザ管		①PC用ウイルス対策ソフトを導入

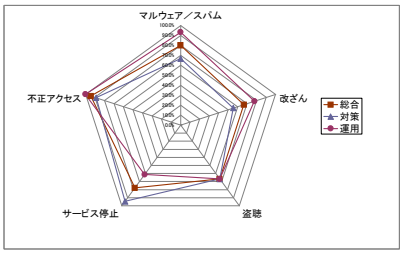
リスク経路分析表を元にセキュリティ対策実施レベル、および運用レベルをまとめた「ネットワークセキュリティレベル評価表（図表３）」を作成した。

図表３　ネットワークセキュリティレベル評価表（抜粋）

リスク名（大項目）	リスク名（小項目）	経路	脅 威		対策内容		実施状況 対策レベル 3	2	1	0	対策得点	運用レベル 3	2	1	0	運用得点	小項目得点（対策得点＋運用得点）
マルウェア／スパム	メールウィルス	インターネット～PC	①多数のPCが感染し利用できない場合がある ②業務PCがウイルスに感染し、機密データなどの情報が漏洩する				Aor ((C1orC2)or(BorD)andE1 andE2	Aor (B1orB2)or CorD	E1andE2	無	3点	状況に応じて見直しが行われている	状況が把握され記録している	担当者レベルで管理されている	全く管理されていない	3点	6点
				サービス	プロバイダのウイルス対策サービスに加入している	始点(A)		○					3				
				ハード	ウイルスフィルタ機能付きFWを導入している	経路(B)											
				ソフト	GW型アンチウイルスソフトを導入している	経路(C1)		○					3				
				ハード	GW型アンチウイルスハードを導入している	経路(C2)											
				ソフト	メールサーバ用アンチウイルスソフトを導入している	経路(D)		○					3				
				ソフト	PC用ウイルス対策ソフトを導入している	終点(E1)		○					3				
				ソフト	最新のセキュリティパッチを適用したOSを導入している	終点(E2)		○					3				
	スパムメール／フィッシング	インターネット～PC／サーバ	①大量のメールを受信することによりサーバ・ネットワークのリソースが枯渇する				AorBorCor D)andE1and E2	AorBorCorD	E1andE2	無	2点	状況に応じて見直しが行われている	状況が把握され記録している	担当者レベルで管理される	全く管理されていない	2点	4点

セキュリティレベル評価表に自社の対策レベルを入力すると、自動的に各リスクのセキュリティ対策評価バランスがレーダーチャート（図表４）でわかりやすく求めることができる。

図表４　レーダーチャート



３．リスクコスト総括表の作成

ネットワークセキュリティ対策は直接売り上げに結びつくものではないため、予算確保が困難である。対策内容を経営層と話し合うため、対策コストを考慮した「リスクコスト総括表（図表５）」を作成した。

図表５　リスクコスト総括表（抜粋）

			見直し前		見直し後		補足
変更箇所		対策	標準契約 Internet router Firewall multilayer switch		標準契約＋オプション Internet router Firewall multilayer switch プロバイダのウイルス対策サービスに加入		<オプション：メールゲートウェイサービス> （対象） 社内メールサーバにおけるインターネットとの送受信メール （動作） 社内メールサーバを経由する送受信メールにおける感染を検出し、感染した場合はウィルスを駆除もしくは削除する。
		運用	運用レベル3		運用レベル3		
リスク評価	マルウェア／スパム		15点	ウィルス対策ソフトに問題がある場合(パターンファイルの更新など)、ウィルスに感染したメールを送受信する可能性がある。	22点	左記の場合でも既知のウィルスであれば、感染を防ぐことができる。	
	改ざん		20点		20点		
	盗聴		20点		20点		
	サービス停止		20点		20点		

４．評価の繰り返し実施と PDCA

制度改正による企業を取り巻く環境の変化、新たなリスクの発生などコストに関わらず、セキュリティ対策を見直す機会がある。セキュリティレベルを維持するためには、PDCA サイクルによる取り組みが不可欠である。

定期的な評価の実施、ネットワーク環境の変化、およびリスク発生時の評価見直しを手順としてまとめた。

５．まとめ

従来ある評価基準ではネットワークセキュリティ対策を概略レベルでしか測ることが出来なかったが、「リスク経路分析表」「ネットワークセキュリティレベル評価表」により、自社のネットワークセキュリティ対策レベルが容易に具体的に把握できる。また「リスクコスト総括表」は経営層との合意を得るための有用な「ものさし」となる。加えて PDCA サイクルによりバランスのとれた対策を最適レベルに維持できるものとなる。ネットワークセキュリティ対策の最適化のために、ぜひ活用していただきたい。