ITリスク対策策定ガイドラインの開発

背　景

企業活動のITシステムへの依存度の高まりとともに、サイバー攻撃によるシステム停止等の影響を防止・軽減するITリスク対策が重要になってきている。適切なリスク対策を実現するには、リスクの規模・頻度を適切に評価し、その結果に基づいて対策を選定することが必要となる。しかし、従来手法（ISO/IEC 27005:2008）では、大規模なITシステムのリスク評価に多大なコスト・時間がかかるため、新たな概念に基づく実施方法が求められている。

目　的

大規模ITシステムにおけるITリスク対策策定を簡便に実施するための具体的な手順をとりまとめる。

主な成果

大規模ITシステムを複数のセキュリティゾーン*1に分割し、セキュリティゾーン毎の評価結果を積み上げて、全体システムのITリスク評価と対策選定を行う手法を開発し、ガイドライン化した。本ガイドラインでは、脅威・脆弱性や資産影響度*2等のレベル評価基準（対数指標）と評価結果のテンプレート、ITリスク対策と効果の一覧等を整備し、具体的な作業手順とその支援ツールを用意することで、コスト・時間の削減を図っている。ITリスクの評価結果と、それに基づく対策選定の例を図1に示す。ガイドラインに基づく具体的な作業手順は以下の通りである。

(1) 資産の特定：ITシステムをセキュリティゾーンに分割し、各セキュリティゾーン内に存在する機器ユニット（サーバやPC、通信機器等）や情報、セキュリティゾーン間の境界を特定する。
(2) 資産影響度の評価：業務における情報の重要性に基づいて、その情報を蓄積・利用する機器ユニットの資産影響度レベルを、3種類の被害タイプ毎に評価する。（図1 (a)【1】）。
(3) インシデント発生可能性の評価：① 各セキュリティゾーンでの脅威源（攻撃者や作業ミス等）の発生し易さと、② セキュリティゾーン間の境界の通過し易さ、③ 機器ユニット毎の脅威の実現し易さ／脆弱性の発生し易さを評価することで、①、②、③を合成したインシデント発生可能性レベルが算定される（図1 (a)【2】）。
(4) リスクレベルの算定：(2)、(3) の結果に基づいて、想定した脅威・脆弱性に対する機器ユニットのリスクレベル（被害規模の期待値の対数指標に相当）が算定される（図1 (a)【3】）。
(5) 対策候補の選定：企業が定める許容リスクレベルを逸脱するものを特定し（図1 (a)【4】）、それらに対する対策群を、対策一覧から選定する。たとえば、図1 (b) に示す対策群により、各リスクレベルは許容リスクレベルである7以下となる（図1 (c)）。複数の候補群がある場合は、導入・運用コストが最も小さなものを選定する。

今後の展開

実際のITシステムでの適用事例を増やし、ガイドラインおよび支援ツールの改良を進める。

主担当者　　システム技術研究所　情報数理領域　上席研究員　二方　厚志

関連報告書　「大規模ITシステムの簡便なITリスクアセスメント手法の開発」電力中央研究所研究報告：R08020（2009年6月）
「ITリスク対策の費用対効果評価手法の開発（その1）―簡便な評価手法の提案―」電力中央研究所調査報告：R07024（2008年6月）

＊1：必要とされるセキュリティレベルに応じて分割された部分ネットワーク。外部公開用Webサーバ等が設置されている区画や、基幹業務用サーバが設置されている区画、基幹ネットワークの区画等に分割される。
＊2：インシデント発生による業務への被害の想定規模。

（a）ITリスク評価結果の例（DMZの外部向けWWWサーバ）

セキュリティゾーン	機器ユニット	資産影響度レベル 機密性喪失（C）	完全性喪失（I）	可用性喪失（A）	脅威 内容	脅威 レベル	脆弱性 内容	脆弱性 レベル	インシデント発生可能性レベル	機密性リスクレベル	完全性リスクレベル	可用性リスクレベル	リスクレベル
DMZ	外部向けWWW	3	3	3	盗難	5	機器の（一部の）取り外し、持ち出し可能	4	1	9	9	9	9
					破壊	5	物理的にアクセス可能	5	2	-	-	10	10
					外部機器の接続による盗聴	4	外部機器、外部記憶媒体が接続可能	4	0	8	-	-	8
					外部機器・メディアの接続による不正なソフトウェア起動、改ざん	3	外部記憶媒体などからOSが起動可能	3	-2	6	6	6	6
					外部機器・メディアの接続による不正なソフトウェア起動、改ざん	3	外部記憶媒体接続時にソフトウェア自動起動	3	-2	6	6	6	6
					タッピングによる盗聴	3	物理的にアクセス可能	5	0	8	-	-	8
					タッピングによる改ざん	1	物理的にアクセス可能	5	-2		6		6
					コンソールからの不正操作	3	コンソールでの認証が不十分	3	-2	6	6	6	6
					出入力装置からの情報漏洩	3	コンソールでの認証が不十分	3	-2	6	6	6	6
					不正機器インライン接続による盗聴	3	外部機器、外部記憶媒体が接続可能	4	-1	7	-	-	7

最終結果
脅威・脆弱性毎の外部向けWWWのリスクレベル

【4】
リスクレベルが許容リスクレベルを逸脱（＞ 7）

【1】
DMZの外部向けWWWの支障が業務に与える影響を，被害タイプ（C, I, A）毎に資産影響度レベルとして評価

【2】
本文 ①, ② から算定する脅威源から DMZ への侵入し易さと，③ の侵入後の脅威・脆弱性レベル（発生し易さ）からインシデント発生可能性レベルを算定

【3】
【1】,【2】の結果から，被害タイプ毎のリスクレベルを算定 し，最大のものをリスクレベルに

※ 各レベルが小さいほど可能性・被害規模は小さい。

評価結果に基づいてITリスク対策を選定

（b）ITリスク対策群の例

セキュリティゾーン	機器ユニット	対策 内容	対策 効果
DMZ	外部向けWWWサーバ	部屋・収容ロッカー等への施錠	サーバの設置場所への侵入を防ぐことで，盗難や破壊，外部機器の接続等を防止
		外付け機器や記憶媒体の接続禁止	外部機器の接続による盗聴や情報漏えい，不正ソフトウェアの持ち込み等を防止
		通信の暗号化	タッピングによる盗聴や通信改ざんを防止

機器ユニットやセキュリティゾーン境界での対策によってリスクレベルが低下

（c）対策群の効果例（許容リスクレベル7）

DMZ	外部向けWWW	3	3	3	盗難	5	機器の（一部の）取り外し、持ち出し可能	4	-1	7	7	7	7
					破壊	5	物理的にアクセス可能	5	-1	-	-	7	7
					外部機器の接続による盗聴	4	外部機器、外部記憶媒体が接続可能	2	-2	6	-	-	6
					タッピングによる盗聴	3	物理的にアクセス可能	2	-3	5	-	-	5

リスクレベルを 7 以下に低減

図1　ガイドラインの基づくITリスク対策策定の例 （一部）