セキュリティポリシー（基本方針と管理策）

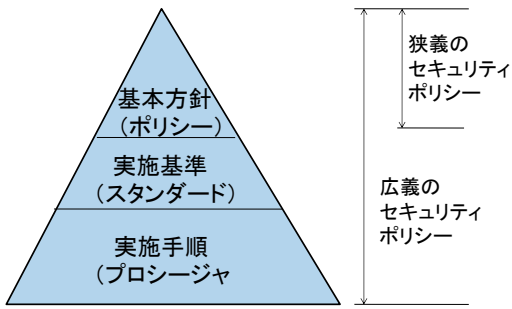
2013年12月17日

後　保範

情報セキュリティマネジメントの必要性

- 企業は自身の顧客や取引先に対し、情報が安全に管理されていることを示す責任がある
- ISMSとは情報セキュリティマネジメントシステム（Information Security Management System)の略で、組織における個別のセキュリティ技術に加え、組織ノマネジメントとしてリスク評価を行い、必要なセキュリティレベルを定めてシステムを運用する
- 情報は企業にとって重要な「資産」であり、情報漏洩や不正アクセス、自然災害による利用停止から情報資産を適切かつ継続的に守る必要がある

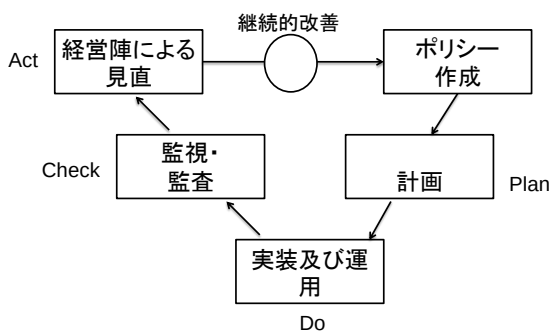
情報セキュリティポリシーの概念



セキュリティポリシーの構成

- 基本方針（基本ポリシー）
  一番上の階層で、具体的な規定の前に方針や目的、範囲、義務、罰則などを記載
- 実施基準（スタンダード）
  実際に守るべき規定を具体的に記述。適用範囲や、対象者を明確にし、具体的に分かりやすく記述
- 実施手順（プロシージャ）
  スタンダードで実施するための詳細な手順を記載。マニュアルに相当し、特定の部署の固有な作業も

情報セキュリティポリシーのマネジメントサイクル



情報セキュリティポリシー策定の組織

- 情報セキュリティポリシーを策定するには、各部門の代表者からなるセキュリティ委員会、実際の作業を行う策定チームといった横断的な組織が必要
- 経営層による承認
- 情報セキュリティ委員会の役割
- ポリシー策定チーム
- 事務局の設置
  継続的に各部門の調整や調整、社内窓口を担当

情報資産の価値

- グループ化した情報資産の価値を機密性、完全性、可用性のセキュリティの3要素の観点から評価
  次のいずれかの方法により資産価値を決める
- 機密性、完全性、可用性のいずれかの最高値を持って資産価値とする
- 資産価値が何点以上の要素がいくつあったら情報資産の価値をいくつにする
- 機密性、完全性、可用性の平均値（切り上げ）を用いる

機密性の基準

資産価値	クラス	説　明
1	公開	一般に公開する内容
2	社外秘	機密情報を含まない、標準的な社内文書や管理記録
3	秘密	関係部署の未開示、漏洩発生時に顧客影響が発生する情報
4	極秘	極一部にのみ公開、漏洩発生時に経営に深刻な影響

完全性の基準

資産価値	リスク	説　明
1	低	情報の内容が改ざんされても、業務への影響が少ない
2	中	情報の内容が改ざんされた場合、業務への影響が大きい
3	高	情報の内容が改ざんされた場合、業務への影響が深刻かつ重大
4	超高	情報の内容の改ざんは新聞記事となり、社会的にも大問題

可用性の基準

資産価値	リスク	説　明
1	低	1日以上の利用停止が許容される
2	中	1時間程度の利用停止が許容される
3	高	1分未満の停止まで許容される
4	超高	1秒の停止も許容できない

情報資産の洗い出しの結果の例

所属	情報資産	機密性	完全性	可用性
業務	預貯金マスターファイル	4	4	4
全社	NW及びNW機器	3	3	3
全社	公開Webサーバ	1	2	2
全社	公開メールサーバ	3	3	3
全社	社内ファイルサーバ	4	2	2
経理	資産情報、会計情報	4	3	2
営業	顧客情報	4	3	3
設計	製品情報	4	3	3

リスク評価

- リスク評価は情報資産を適切に管理するため
- リスク評価では以下の事項を明確にする
  個々の情報資産の管理状況
  情報資産を脅かす脅威
  脅威に対して情報資産に内在する脆弱性
  問題が発生した場合の事業への影響度

ギャップ分析

- 一般に推奨される管理レベルに対し、企業の管理レベルと比較しギャップを分析する
- 大きな差があったり、明らかに不足している箇所を発見したら、その情報資産の詳細リスク分析をする
- ギャップ分析は情報資産すべてを対象にする
- ギャップ分析を行った上で詳細リスク分析を行うのは、詳細リスク分析を行うのは労力が大きく現実的でない
- ギャップが大きい部分及び企業に特に重要な情報資産に対してのみ詳細リスク分析をするのが現実的

リスク分析の手順

情報資産の価値を求める
↓
情報資産に対する脅威を分析
↓
内在する脆弱性を分析
↓
情報資産の価値、脅威、脆弱性からリスク値を算出

脅威分析

- 人為的・意図的な脅威の例
  SQLインジェクション、不正アクセスによる個人情報の漏洩
  サーバの脆弱性を狙った攻撃によるサービス停止
  コンピュータ・ウィルス感染による業務停止・停滞
  社員による意図的な不正アクセス、情報持ち出し
- 人為的・偶発的な脅威の例
  社外に持ち出したPCや機密文書の紛失による情報漏洩
  入力ミスによる誤った出力結果、誤操作による消去
  通信機器やサーバの設定もれ、ソフトウェアのバグ、不具合
- 非人的・偶発的な脅威の例
  火災、地震、水害
  ハードディスク、通信機器の故障、ケーブルの断線と停電

脆弱性分析

- 脆弱性の計算式
  脆弱性レベル ＝攻撃難易度×管理レベル
- 攻撃難易度と現状の管理レベル

攻撃難易度

容易	普通	困難
3	2	1

現状の管理レベル

低い	普通	高い
3	2	1

- 脆弱性のレベル分け
  攻撃難易度×管理レベル＝1～3 ---- 脆弱性レベル1
  4～6 ---- 脆弱性レベル2
  7～9 ---- 脆弱性レベル3

リスク値の算出

- リスク値＝情報資産の価値×脅威×脆弱性

資産価値	脅威レベル								
	1			2			3		
	脆弱	性レ	ベル	脆弱	性レ	ベル	脆弱	性レ	ベル
	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

セーフガードの選択

- 算出したリスク値を元に、適切なセーフガードを選択
- リスク管理から下記の4つに区分

許容　低減　移転　回避

- リスクコントロールの観点から下記の4つに区分

抑止　予防　検知　回復

セーフガードの選択例(公開Webサーバ)

脅威	リスク	リスク管理	コントロール	セーフガード
情報漏洩	大	低減	予防	安全なWebアプリ開発
		低減	検知	ファイアウォール
		低減	予防	最新のパッチの適用
		移転	予防	外部ホスティングサービス
改ざん	大	低減	予防	最新のパッチの適用
			検知	ハッシュ値で改ざん検知
			回復	バックアップ
		移転	予防	ホス外部ティングサービス
不正アクセス	大	低減	予防	最新のパッチの適用

情報セキュリティポリシーの記述例（基本方針）

- 目的
  情報セキュリティの必要性と組織における目的を宣言
- 適用範囲
  情報セキュリティを適用する範囲を定義
- 組織と責任
  情報セキュリティを維持するための組織と、その責任
- 管理
  情報資産の管理の必要性と管理方法
- 監査
  業務の責任から独立した監査部による監査
- 教育
  全社員に対し教育の義務があることを明確にする
- 罰則
  強制力を持たすため、責任と義務を怠った場合の罰則

情報セキュリティポリシーの記述例（管理策）

- 目的
  管理策の目的や主旨、目標を記載
- 適用範囲
  対象とする業務、システム、情報資産を具体的に記載
- 対象者
  管理策を遵守すべき対象者を記載
- 規定事項
  ここが本文。具体的に遵守すべき規定を記載
- 例外
  実施基準に例外事項がある場合、ここに補足を記載
- 関連事項
  関連する他の規定がある場合は、ここに記載
- 改訂記録
  実施基準が改定になった場合の履歴を時系列で列挙