JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

情報セキュリティ対策マップ検討 WG　中間報告

情報セキュリティ対策マップ検討WG
奥原　雅之　／　長谷川　喜也
富士通株式会社

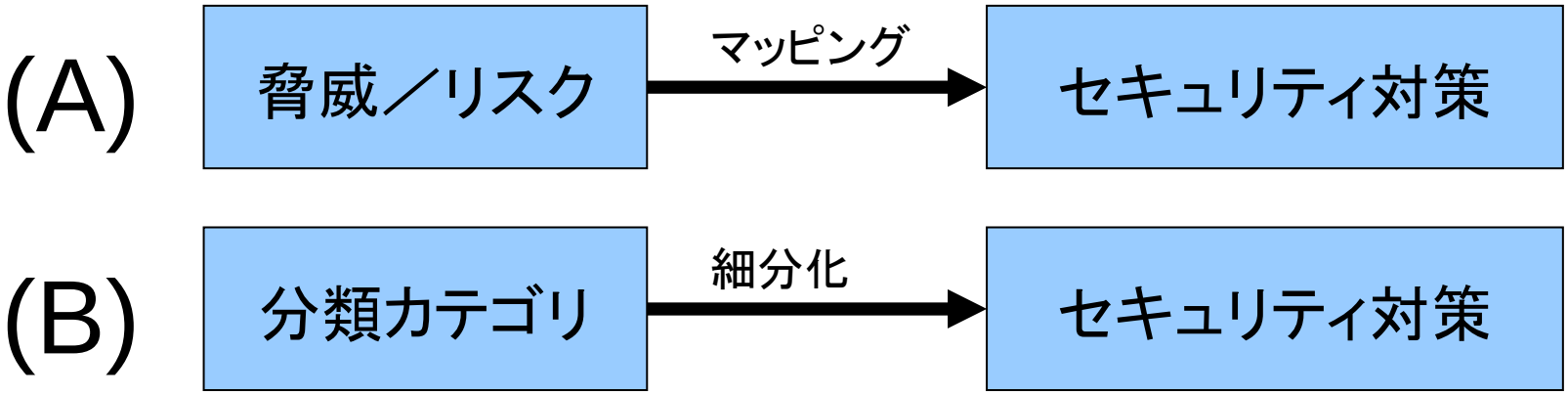
2009 年 6 月 3 日

問題提起

既存のセキュリティ対策マップ例

- ISO/IEC 27002
- NIST SP800-53
- 情報セキュリティ管理基準
- ベンダーのセキュリティソリューションリスト
- 他

既存対策マップの一般的な構造



- 一般に上記のいずれかの構造
- 概念としては理解できるが、実際のセキュリティ対策実施の有効性・網羅性を記述するのにはどうにも力不足

どんなときに困るかというと

- （1）対策の有無しか記述できない。
  - 特定のリスクに対策されているかどうかしか見えない（0か1かの世界）
  - 「高価な機材」を入れる理由の説明に使えない

どんなときに困るかというと

- （2）2個以上の対策の関係や対策の十分性を正確に記述できない。
  - 二つの対策が相互に補完するとき
  - ある対策が別の対策に依存するとき
  - 二つの対策が排他関係にあるとき
  - 二つ以上の対策に相乗効果があるとき

どんなときに困るかというと

- （3）組織内のどの部分にどのような対策を配備すればよいかというようなプランニングには使えない。
  - どの組織に配備するか
  - どのシステムに配備するか
  - 最強の逃げ口上：「リスクアセスメントすれば？」

活動目的

最終目的

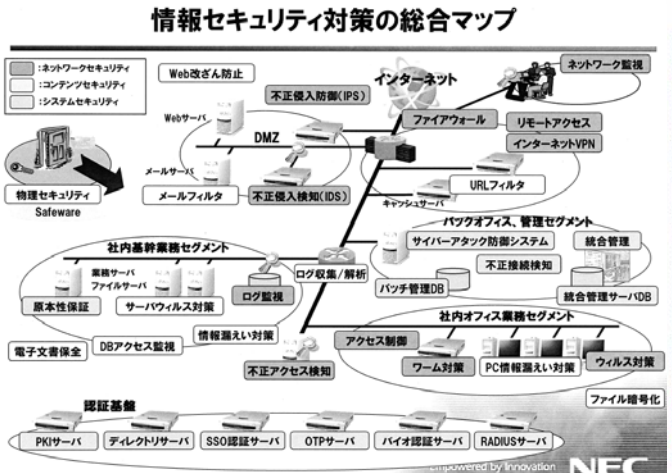
- 組織全体の情報セキュリティ対策の状況を確認することができる「情報セキュリティ対策マップ」のコンセプト
- これを作成するための手法や記述モデル
- 実例としての汎用的な標準情報セキュリティ対策マップ案

活動経過

私が情報セキュリティマップだと思うもの

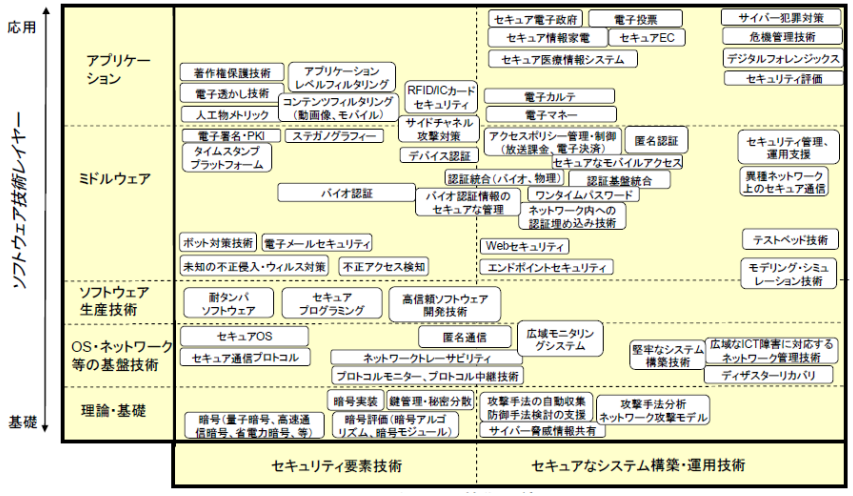
- お客さん自身が、自社のセキュリティ的に弱いところを簡単にチェックできるような物が欲しい
- マップに投資効果も表現できる余地がほしい
- これだけやれば大丈夫という90%くらいをカバーしたJNSAお墨付きのマップがほしい
- マップに期待しているのは網羅性
- 良い物を集めてくると結果として網羅したことになるというアプローチもある、世界中のガイドラインを集めてスーパーガイドラインを作るというというのもありかもしれない
- 心理的なリスクに対する投資効果も表現できるといい

集まったマップの例



対策カテゴリー一覧

セキュリティ統制	
認証・アイデンティティマネジメント	コンプライアンス対応統合IDM
	大規模向け統合IDM
	中小規模向け統合IDM
アクセスコントロール	クライアントのアクセスコントロール
	サーバのアクセスコントロール
	ファイルのアクセスコントロール
証跡管理	証跡管理
	PCログ分析
	ログ分析サービス
集中管理	セキュリティ統合サービス
	プロセス管理
不正アクセス対策	ファイアウォールアプライアンス／UTM
	セキュリティ最適化
セキュリティコンサルティング	
セキュリティポリシー	組織ポリシー策定支援
	ポリシー定着支援ツール
	セキュリティ対策支援
セキュリティ対策	セキュリティ可視化
セキュリティ監査	セキュリティ監査
セキュリティ認証取得支援	BS7799 / ISO17799 / ISMS
	ISO27000取得支援ツール
	ISO15408
	プライバシーマーク
エンドユーザ教育	ユーザ教育支援
不正アクセス対策	
ファイアウォール	ファイアウォール
	アプリケーションファイアウォール



セキュリティ対策マップ（正面装備編・部分）　2009/1/7

脅威	場面	対策名	対策の概要	対策の限界	必要な資源 I 訓練された管理者	必要な資源 II 運用手順	必要な資源 III セキュリティ方針	必要な資源 IV 教育された利用者	必要な資源 V 定期的な更新	必要な後方支援 A IDM管理基盤	必要な後方支援 B 証跡管理基盤	必要な後方支援 C アクセス管理基盤	必要な後方支援 D 集中管理基盤
ネットワーク外部からの侵入および攻撃	ネットワーク接続点（DMZ）	ファイアウォール	他の機器とDMZを形成し、内部ネットワークに外部の脅威が直接到達することを防ぐ。	許可されたアクセス経路を経由する攻撃には対応できない。	◎	○	○	–	○	○	○	○	○
		侵入検知システム（IDS）	ネットワークを経由する攻撃を意図した通信を検知し、警報を発信する。	一般に検知できない攻撃が存在する。	○	○	◎	–	◎	–	○	–	○
		侵入防御システム（IPS）	ネットワークを経由する攻撃を意図した通信を検知し、その通過を阻止する。	一般に検知できない攻撃が存在する。また、誤検知により正常な業務を阻害する可能性がある	○	○	◎	–	◎	–	○	–	○
	ネットワークサーバ	脆弱性アセスメントツール	各サーバの脆弱性の有無について外部から調査し、結果を報告する。	一般に検出できない脆弱性が存在する。診断後対処を行わないと攻撃に対抗できない。	◎	○	–	–	◎	–	○	–	–

出典：独立行政法人 情報処理推進機構
「情報セキュリティ分野における技術ロードマップ策定～ IC カードシステムにおける情報セキュリティ ～報告書」 より

「セキュリティマップ」に求めるもの

- 目標
  - 利用者にとって有益で、使えるものであること
    - ベンダ側：製品を売り込む上での妥当性を提示できる
    - ユーザ側：対策をすることの責任説明を提示できる
- 目標を達成するための必要条件
  - 要素（カテゴリ）はMECEであること
    - 網羅性は必須
    - 重複していないほうがよい（気分的な問題か？）
  - 5W1Hを明確にすること
    - **Who（誰が→対象組織、職種）** **What（何を→対象資産）** When（いつ→PDCAサイクル） Where（どこで） **Why（どうして→脅威）**
- 目標を達成するための十分条件
  - 対策のレベルがわかること（「集団の知恵」を活用できるような仕組みも）
  - 多くの軸が入っていること
  - 見やすいこと
  - 使いやすいこと

「昆虫採集班」のアプローチ

- 世の中でセキュリティ対策と呼んでいるものを遍く集めてきて分類し、セキュリティ対策の巨大な辞書をつくる。
  → まず初めに、「昆虫採集」をするフィールドを決めよう
  → 次に、どこのフィールドにも必ず「生息」しているであろう「認証」と「ウィルス・マルウェア対策」の採取を通して、各フィールドの特性を知ろう

「昆虫採集」のフィールド候補

- ISO/IEC 27002
- ISO/IEC 27001
- その他ISO/IEC27000シリーズ
- ISO/IEC 15408
- SP800-53
- PCI DSS
- COBIT
- COBIT for SOX
- BS25999-1
- ITIL
- ISO20000
- 情報セキュリティ管理基準
- システム管理基準
- システム管理基準追補版
- 個人情報の保護に関するガイドライン
- 政府機関の情報セキュリティ対策のための統一基準
- 安全なウェブサイトの作り方
- 安心して無線LANを利用するために（総務省）
- 小規模企業のための情報セキュリティ対策
- 金融機関等コンピュータシステムの安全対策基準
- 中小企業の情報セキュリティ対策チェックシート
- 不正プログラム対策ガイドライン
- Webシステム セキュリティ要求仕様
- セキュリティ・可用性チェックシート
- データベースセキュリティガイドライン
- HIPPA
- 中小企業の情報セキュリティ対策ガイドライン（IPA）
- SAS70
- IPAのリンク集にあるガイドライン
- SP800の53以外（64他）
- FIPS
- COSO
- 共通フレーム2007（SLCP-JCF）／ISO/IEC 12207
- 高等教育機関の情報セキュリティ対策のためのサンプル規程集
- RFC2196 サイトセキュリティハンドブック
- 地方公共団体における情報セキュリティポリシーに関するガイドライン

「コンセプト班」のアプローチ

- マップの目的、どんな形で書くのがいいか、等コンセプチュアルな議論を進める
  - 「対策」を正確に記述するにはどうするか？（MECEを含む）
  - マップ作成のための「軸」の候補になるものは何があるか？
  - マップの「目的」は何か？

→ まず初めに、マップの「目的」を決めるために、「誰が」「何のために」使うか整理しよう

→ マップの「目的」として「投資判断」が多いので、「投資判断」に使うマップから検討しよう

マップは誰が何ために使うのか？

使用者	用途
情報セキュリティ担当者	対策の評価
	脅威の影響の評価
	次に強化する分野の特定
	購入製品の選定
	事故が起こったときの言い訳
	他社との比較
	ベンダーの比較
情報セキュリティ担当管理職	対策の評価
	脅威の影響の評価
	事業継続への影響
	コストパフォーマンスの評価・投資効果
	経営者層への答申(稟議)
	他社との比較
経営者・CISO	安全がひと目でわかる
	事故が起こったときの言い訳
	うれしさ・安心感
	コストパフォーマンスの評価・投資効果
	コンプライアンス
	説明責任(CSR)・セキュリティ報告書
	他社との比較
	業種平均との比較(偏差値)
	対策のバランス

使用者	用途
ベンダー	製品の有効性のアピール
	新製品開発のマーケティング
	製品ラインアップの網羅性のアピール
	お客様への対策必要性の訴求
	お客様ヒアリングシート
開発者	要件定義期間の短縮
	システム設計の有効性評価
	開発過程のチェック
	セキュリティテスト
	システムの安全性確保
コンサルタント	コンサルティングの素材
	状況可視化
	対策アドバイス
エキスパート・研究者	各種調査(基礎資料)
	分析
	立法などの参考資料
その他のコンピュータ利用者	教育・啓発
	製品・サービスの評価

今後の活動予定

- 本WGの実施を三カ年とすると。
  - １年目：先行事例の調査研究、
    対策マップの方向性検討
  - ２年目：対策マップ記述モデルの検討、
    作成手法の検討、
    標準対策マップ案の作成
  - ３年目：標準対策マップの検証、
    最終報告書作成

予定成果物

- 先行事例調査結果報告書（１年目）
- 情報セキュリティ対策マップモデル（２年目）
- 標準情報セキュリティ対策マップ案（２年目）
- 標準情報セキュリティ対策マップ（３年目）

JNSA

ありがとうございました。