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　活動の概要

情報セキュリティ対策マップ検討WG

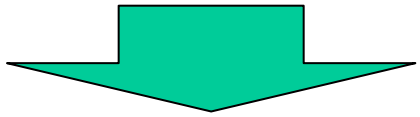
奥原　雅之（富士通株式会社）

2010 年 1 月 27 日

問題提起

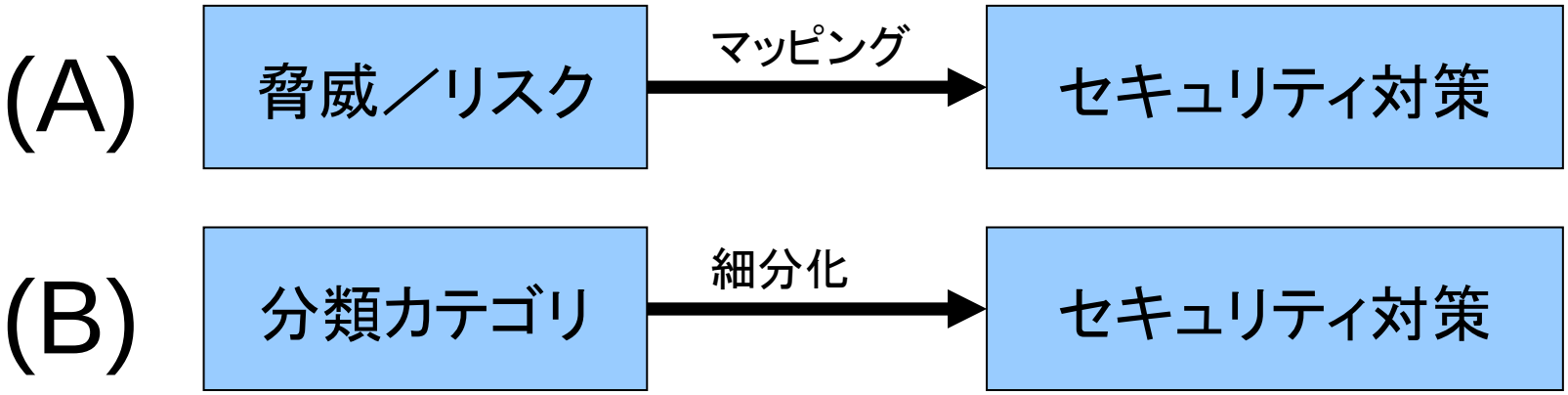
既存のセキュリティ対策マップ例

- 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



今さら何をやるの？

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

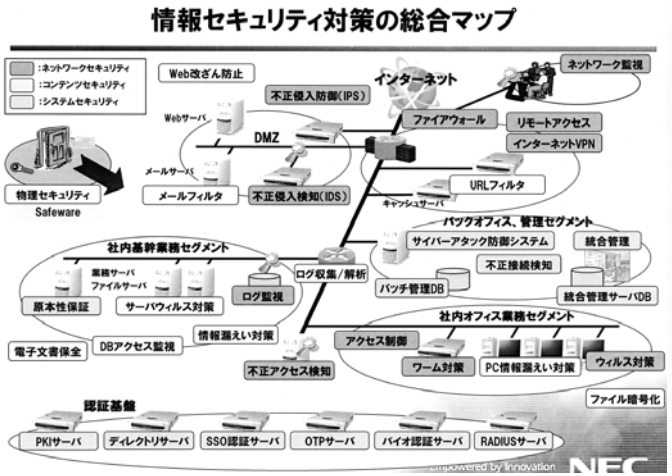
- 「情報セキュリティ対策マップ」を作る
  - 組織全体の情報セキュリティ対策の状況を確認することができる「情報セキュリティ対策マップ」のコンセプト
  - これを作成するための手法や記述モデル
  - 実例としての汎用的な標準情報セキュリティ対策マップ案

活動経過

これまでの主な活動

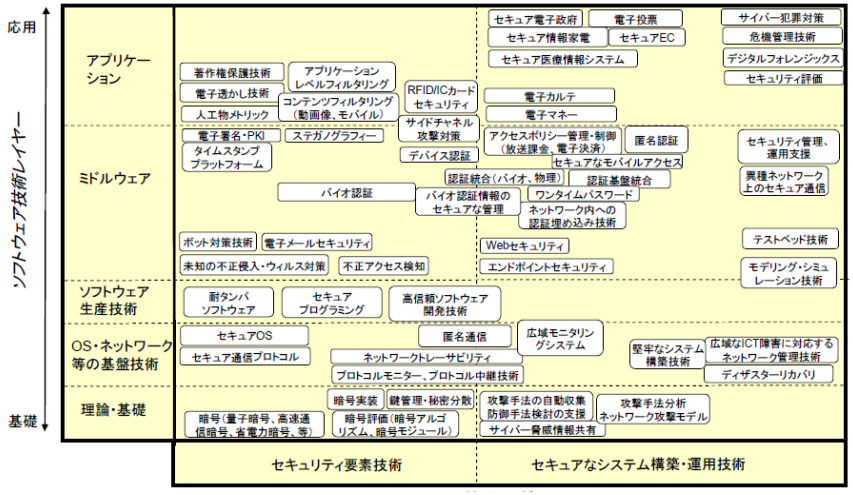
- 世の中の「マップ」の事例収集（～2009/2）
- 分類のための「軸」の検討（～2009/5）
- 世の中の「セキュリティ対策」の収集（昆虫採集）（～2009/8）
- 対策を分類する目安とする「対策構造図」の検討（～2009/12）
- 対策を客観的に記述する「標準構文」の検討（～現在）
- その他色々な提案、検討（オブジェクト指向、構文解析、とにかく地図を描いてみる、他）

マップの収集



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

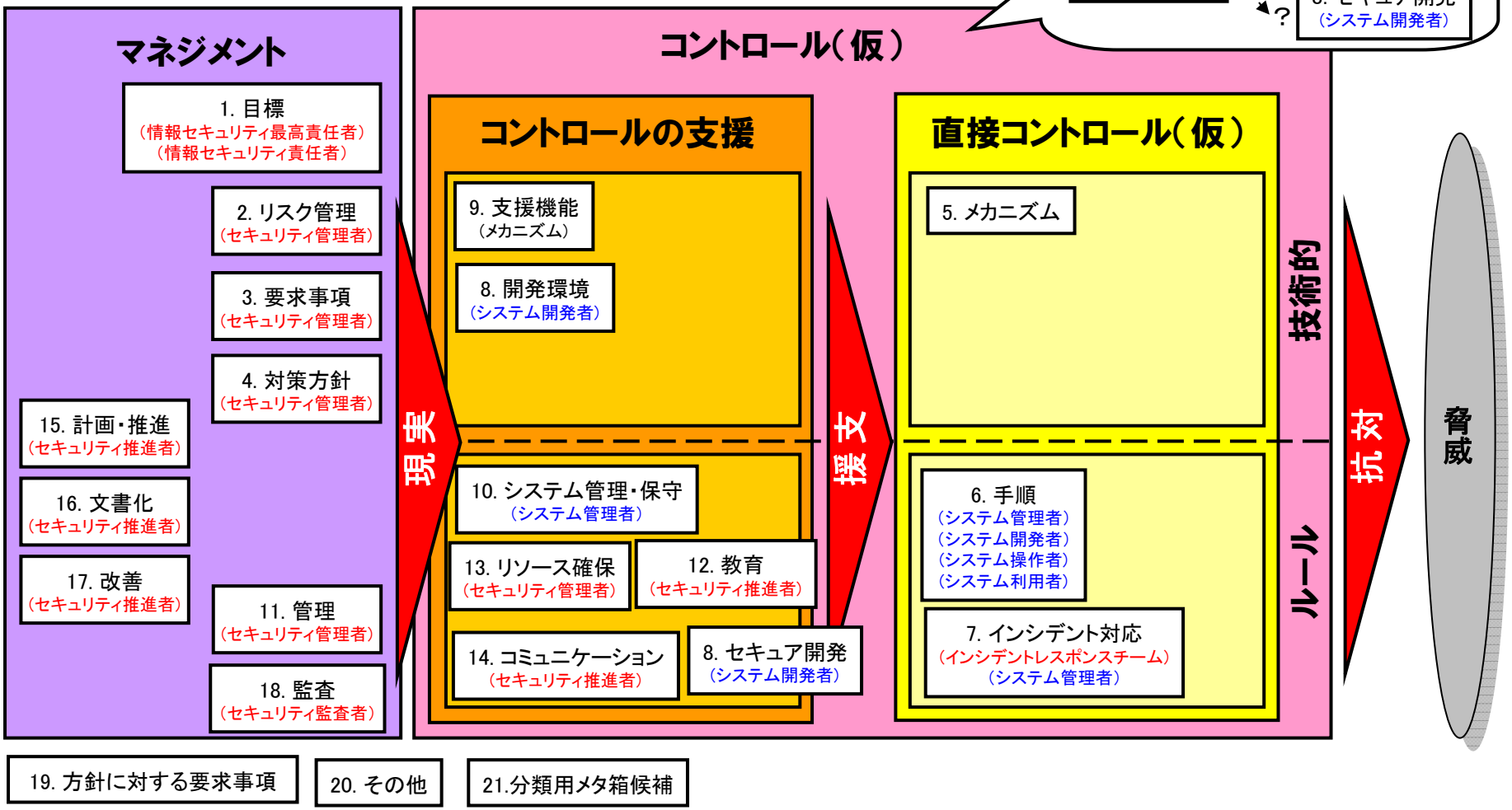
分類軸の検討

- マップを「2軸（あるいはそれ以上の次元）による対策のマッピング」と考えたとき、何が軸の候補となるか。
  - 軸の候補は「マップを読む人の目的」に依存する
  - その前に読む人を定義する必要がある
  - 「うれしさ」のような指標があってもよいかも
  - 軸の片方は対策の分類そのものなのでは
  - 分類するならMECE（網羅性と排他性）について考慮すべき

セキュリティ対策の収集（昆虫採集）

- ISO/IEC 27002
- ISO/IEC 27001
- その他ISO/IEC27000シリーズ
- ISO/IEC 15408
- NIST 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

対策構造図(開発中)


↓開発時の注意？
8. 開発
(システム開発者)
?
8. 開発環境
(システム開発者)
?
8. セキュア開発
(システム開発者)
マネジメント
1. 目標
(情報セキュリティ最高責任者)
(情報セキュリティ責任者)
2. リスク管理
(セキュリティ管理者)
3. 要求事項
(セキュリティ管理者)
4. 対策方針
(セキュリティ管理者)
15. 計画・推進
(セキュリティ推進者)
16. 文書化
(セキュリティ推進者)
17. 改善
(セキュリティ推進者)
11. 管理
(セキュリティ管理者)
18. 監査
(セキュリティ監査者)
現実
コントロール(仮)
コントロールの支援
9. 支援機能
(メカニズム)
8. 開発環境
(システム開発者)
10. システム管理・保守
(システム管理者)
13. リソース確保
(セキュリティ管理者)
12. 教育
(セキュリティ推進者)
14. コミュニケーション
(セキュリティ推進者)
8. セキュア開発
(システム開発者)
支援
直接コントロール(仮)
5. メカニズム
6. 手順
(システム管理者)
(システム開発者)
(システム操作者)
(システム利用者)
7. インシデント対応
(インシデントレスポンスチーム)
(システム管理者)
技術的
ルール
抗対
脅威
19. 方針に対する要求事項
20. その他
21.分類用メタ箱候補
ITシステム・設備
守るべき情報資産
情報

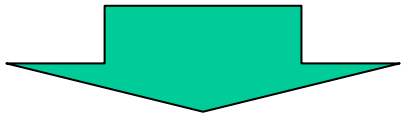
試しにマルウェア対策の洗い出し（挫折中）

行	No.	出典	要件	分類
1	1	27002 10.4	ソフトウェア及び情報の完全性を保護する。	01.《目標》
2	2	27002 10.4	悪意のあるコード及び認可されていないモバイルコードの侵入を防止し、検出する。	01.《目標》
3	55	SP800-53 SI-3	情報システムは、悪意のコードから、情報システムを保護する。	01.《目標》
4	85	SP800-53 SI-3	組織は、悪意のコードの検知や根絶のプロセスにおけるフォルスポジティブ（false positives：正常な通信なのに不正と判断する誤検知）を容認するか否かについて検討する。	02.《リスク管理》
5	86	SP800-53 SI-3	組織は、悪意のコードの検知や根絶のプロセスにおけるフォルスポジティブがもたらす情報システムの可用性への潜在的影響を受け入れるか否かについて検討する。	02.《リスク管理》
6	3	27002 10.4	管理者は、悪意のあるコードを防止するための管理策を導入すること。	03.《要求事項》
7	4	27002 10.4	管理者は、悪意のあるコードを検知するための管理策を導入すること。	03.《要求事項》
8	5	27002 10.4	管理者は、悪意のあるコードを取り除くための管理策を導入すること。	03.《要求事項》
9	6	27002 10.4	管理者は、モバイルコードを管理すること。	03.《要求事項》
10	7	27002 10.4.1	悪意のあるコードから保護するために、検出、予防及び回復のための管理策を実施すること	03.《要求事項》
11	8	27002 10.4.1	悪意のあるコードから保護するために、利用者に適切に意識させるための手順を実施すること	03.《要求事項》
12	9	27002 10.4.1	悪意のあるコードからの保護は、悪意のあるコードに対する検知・修復ソフトウェアに基づくこと。	04.《対策方針》

…以下マルウェア対策だけで100項目以上

標準構文

- 中心となる管理策は「何かを」「どうする」という単純な構文になる（期待を込めた仮定）。
- 「誰が」「何のために」「何を使って」などは修飾節（バリエーション）として扱う。
- 「を確実にする」などの表現上の語句は切り落とす（多少無理を承知）。
- 「どうする」の動詞と管理策の性質（分類）に関係が出る（期待）。



- 対策（管理策）を一意に表現できる構文ができるのでは。（地図を作るための記法となる）

今後の活動予定

- 本WGの実施を3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

ご期待ください。(￣ー￣)