JNSA

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

セキュリティ対策のモデル化と可視化への取り組み

奥原　雅之
JNSA 情報セキュリティ対策マップ検討WG

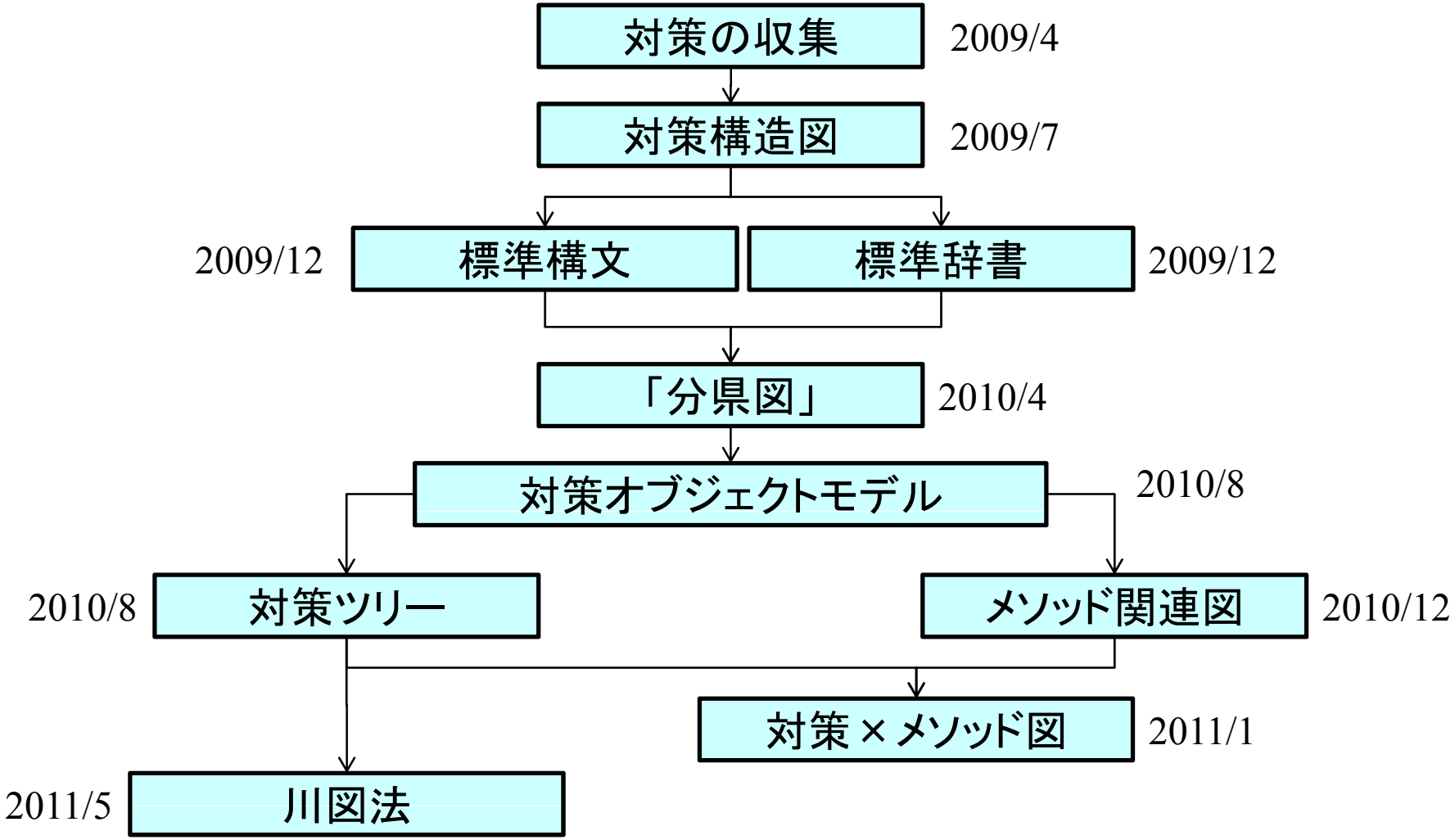
2012 年 6 月8日

WG活動の概要

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

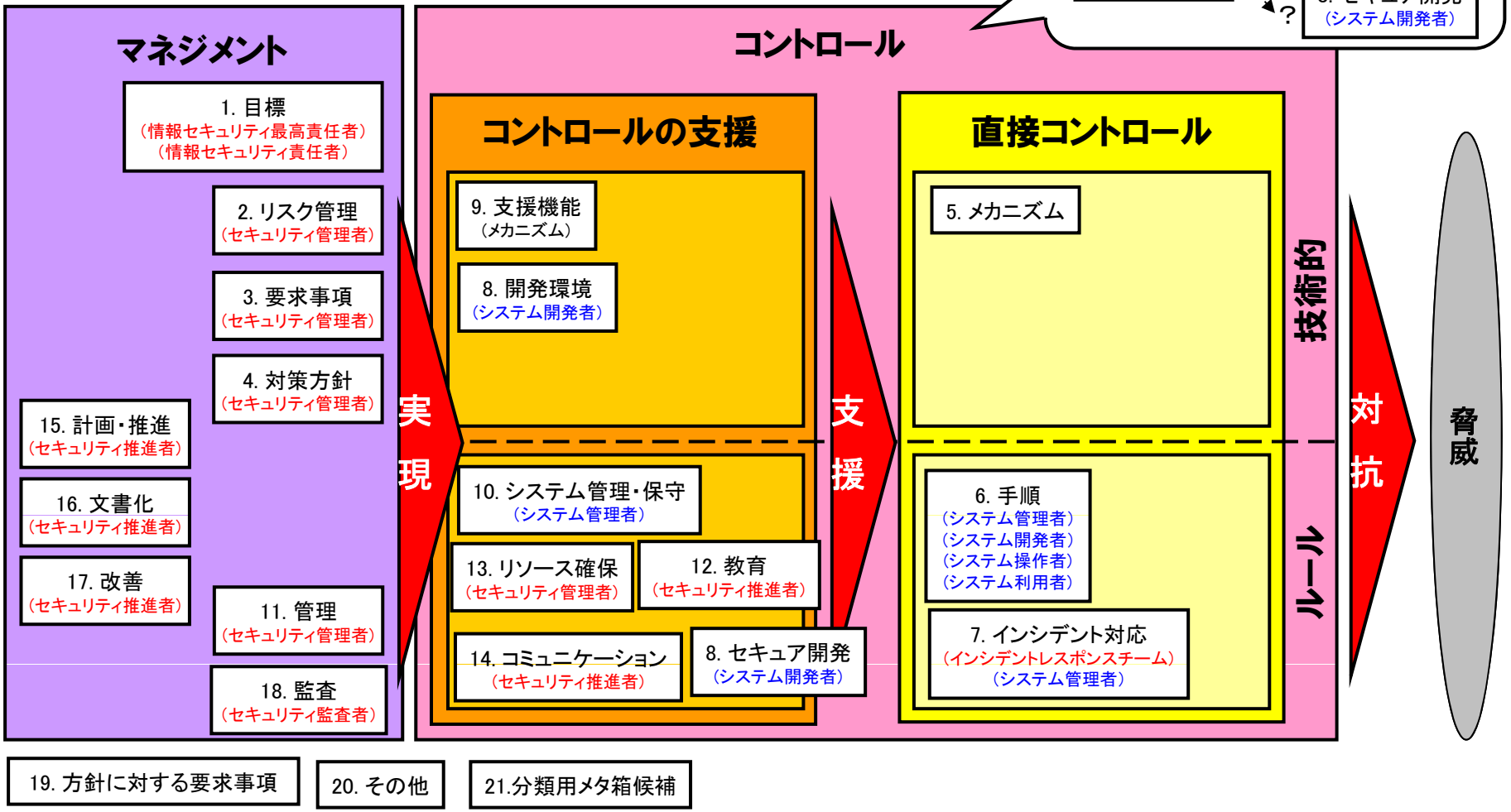
大まかな流れ



セキュリティ対策の収集

- 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
- HIPAA
- 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）
実現
コントロール
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
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
対抗
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

標準構文

【目的・脅威】 のために 【実施者】 は

【条件】 のときに 【場所】 で

管理策

【対策】 を 【動詞】 する

【結句】
管理策の外にある要求の強度など。
例:「ことがのぞましい」、「べきである」、「ことを徹底する」

標準辞書

標準用語	よみ	同義語(is)	含まれる概念(has)	概要
対策マップ上の対策毎に登場する単語	よみかた	標準用語と同じ意味の用語	標準用語に含まれる次レベルの用語	標準用語の意味するところ

モバイルコード	もばいるこーど		悪意のモバイルコード	モバイルなコード
ソフトウェア	そふとうぇあ		マルウェア モバイルコード プログラム	
マルウエア	まるうえあ	悪意のコード(SP800) 悪意のあるコード(27002) 悪意のソフトウェア 不正プログラム(FISC)	ウイルス ワーム スパイウェア トロイの木馬 悪意のモバイルコード 混合攻撃 攻撃ツール	被害者のデータ、アプリケーション、またはオペレーティングシステムの機密性、完全性、可用性を損なう目的や、被害者を困らせたり混乱させたりする目的で、通常は気づかれないようにシステムに挿入されるプログラム
ウイルス	ういるす	コンピュータウイルス(FISC)	コンパイル型ウイルス インタプリタ型ウイルス	自己複製、つまり、自分自身のコピーを作成し、そのコピーをほかのファイルやプログラム、またはコンピュータに配布するように設計されている

「マルウェア分県図」の試作

NSF2010にて成果ご紹介した分県図（部分）

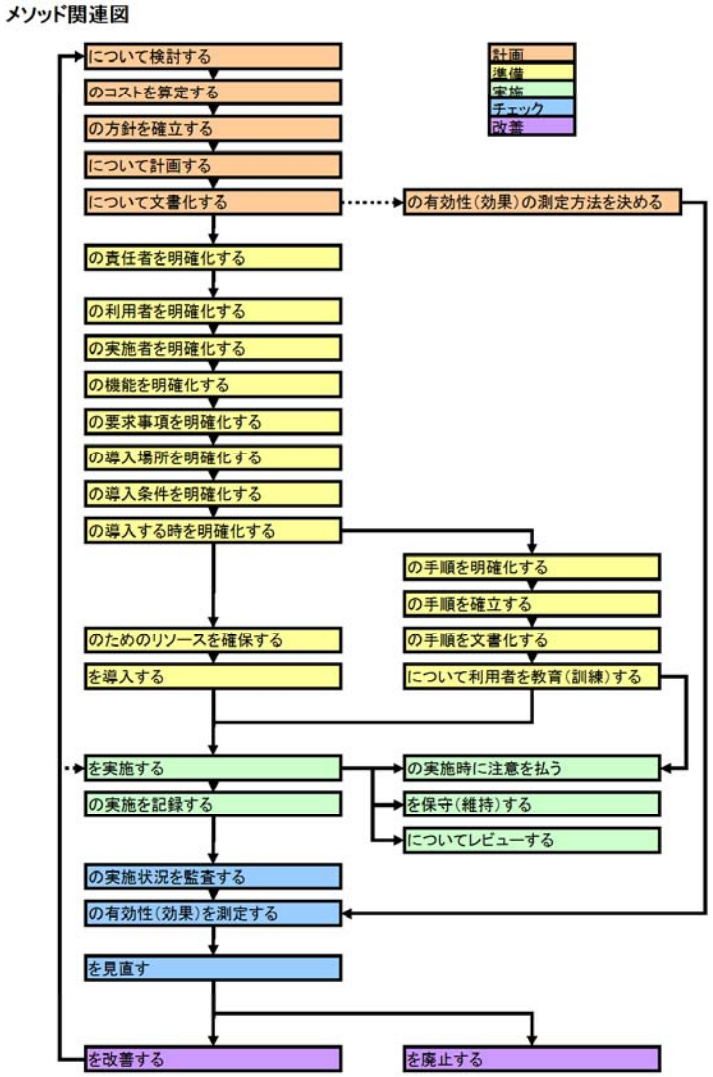
ID	名称	分類	内容
MAL.1	マルウェアからの防御	03.《要求事項》	マルウェアから保護するために、【防御対策の種類のリスト:｛予防｝、｛発見｝、｛回復｝】の防御対策を実施する。
MAL.2	マルウェアの検知	04.《対策方針》	【実施者のリスト:｛組織は｝】【条件のリスト:｛データの送受信の都度｝】【場所のリスト:｛外部ネットワークと内部ネットワークを接続するゲートウェイ等｝】に【使うツールのリスト:｛不正プログラム対策メカニズム｝】を利用して、【媒介物のリスト:｛電子メール｝、｛電子メールへの添付ファイル｝、｛インターネットアクセス｝、｛取り外し可能な記録媒体（｛USB デバイス｝、｛ディスケット｝,｛コンパクトディスク｝,｛など｝）｝、｛そのほかの一般的な手段｝、｛情報システムの脆弱性｝、｛など｝】を介して送り込まれた悪意のコード（（｛ウイルス｝、｛ワーム｝、｛トロイの木馬｝、｛スパイウェア｝、｛など｝）の不正プログラム）を【動作のリスト:｛検知｝,｛根絶｝｛チェック｝】する。
MAL.3	ウイルス対策ソフトウェアの導入	05.《メカニズム》	【目的のリスト:｛マルウェアインシデントを防止するため｝、｛【保護対象のリスト:｛ATM等の専用端末｝】にメンテナンス時にウイルスが混入しないよう｝、｛予防又は定常作業として、コンピュータ及び媒体を走査するため｝】【実施者のリスト:｛各組織は｝】【場所のリスト:｛要求を満たすウイルス対策ソフトウェアが利用可能なすべてのシステム｝、｛悪意のあるソフトウェアの影響を受けやすいすべてのシステム｝、｛情報システムの入口点および出口点｝、｛メンテナンス用パソコン等｝、｛ネットワーク上のワークステーション｝、｛端末｝、｛パーソナルコンピュータ｝、｛サーバー｝、｛ネットワーク上のサーバ｝、｛ネットワーク上のモバイルコンピューティング機器｝、｛境界デバイス｝】ウイルス対策ソフトウェアを導入する
MAL.4	複数ベンダーの採用	04.《対策方針》	【目的のリスト:｛マルウェアからの保護の効果を改善するため｝｛シグネチャを早く入手するため｝】組織は【設置場所のリスト:｛境界デバイス｝、｛サーバ｝、｛ワークステーション｝】にウイルス対策ソフトを導入する際には複数ベンダーが提供する、不正プログラム対策ソフトを利用する。
MAL.5	定義ファイルなどの最新化	04.《対策方針》	マルウェアの検出精度を向上させるために組織は定義ファイルおよびスキャンエンジンを【最新に保つ方法のリスト:｛正しい設定により自動的に更新する｝｛新しいリリースが入手可能な場合はすぐに入手し定めに従って更新する｝】。

対策オブジェクトモデル

標準文法による表記	「目的」「脅威」「実施者」「条件」「場所」「管理策」する。

オブジェクト名	「管理策」する。（リスクの大きさを直接修正する手段、一般的にはメカニズム　または　ルール）	
プロパティ	固定	方針、目的、機能、要求事項、場所、条件（トリガ）、時間、本質的な関係者（責任者、管理者・実施者、利用者）
	可変	手順、リソース、コスト、効果、本質的でない関係者
メソッド	検討する、計画する、コストを算定する、効果を見積る、確立する、リソースを確保する、導入する（機材の場合は「設定する」を含む）、保守（維持）する、文書化する、手順を確立する、手順を明確化する、手順を文書化する、（本質的でない）責任者を明確化する、実施する、実施を記録する、実施時に注意を払う、利用者を教育（訓練）する、レビューする、見直す、実施状況を監査する、有効性（効果）の測定方法を決める、有効性（効果）を測定する、改善する、廃止する	

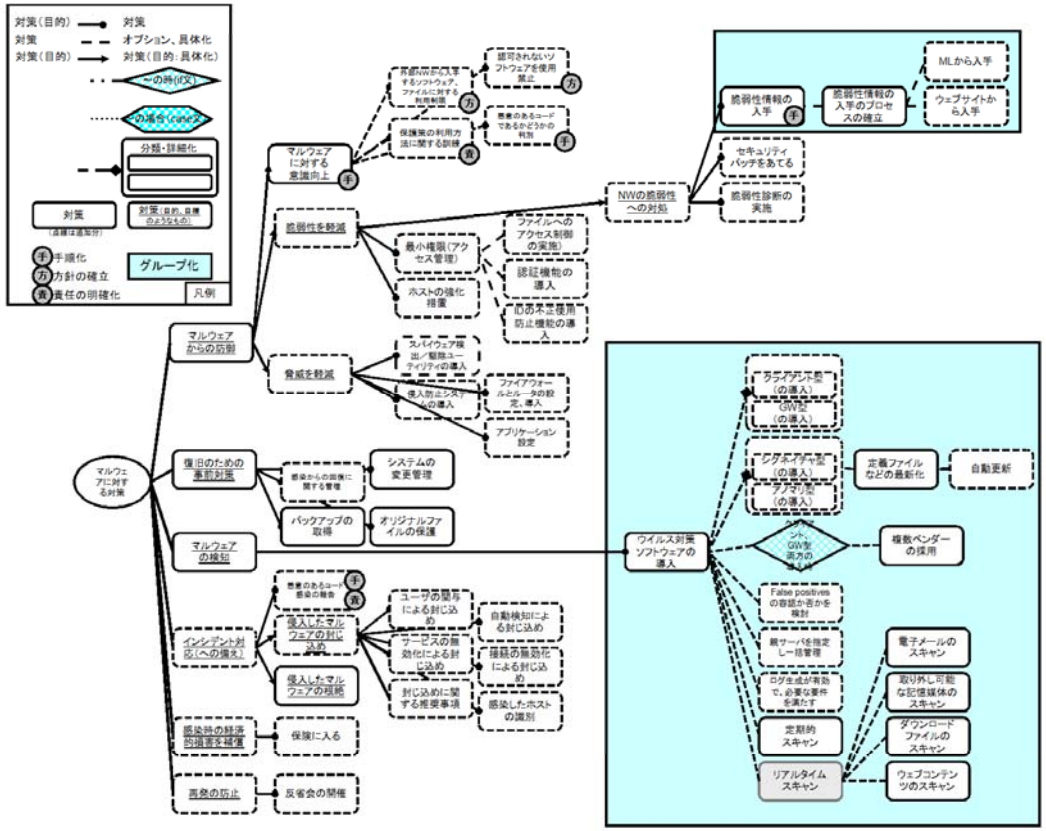
メソッドの構造



- メソッドは対策のライフサイクル(PDCA)と関係が深いように見える
- メソッドを使うフェーズに着目して整理するとメソッドの関係が可視化できるのでは
- どのような図になるかを現在検討中(左はその一例)

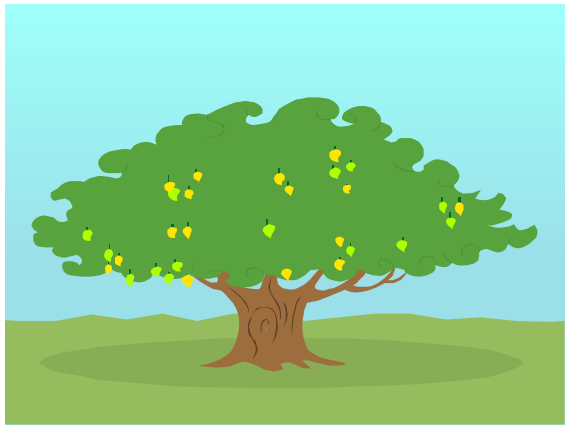
分県図のツリー化

- 「対策構造」その他の成果と組み合わせることで、ツリーにする。

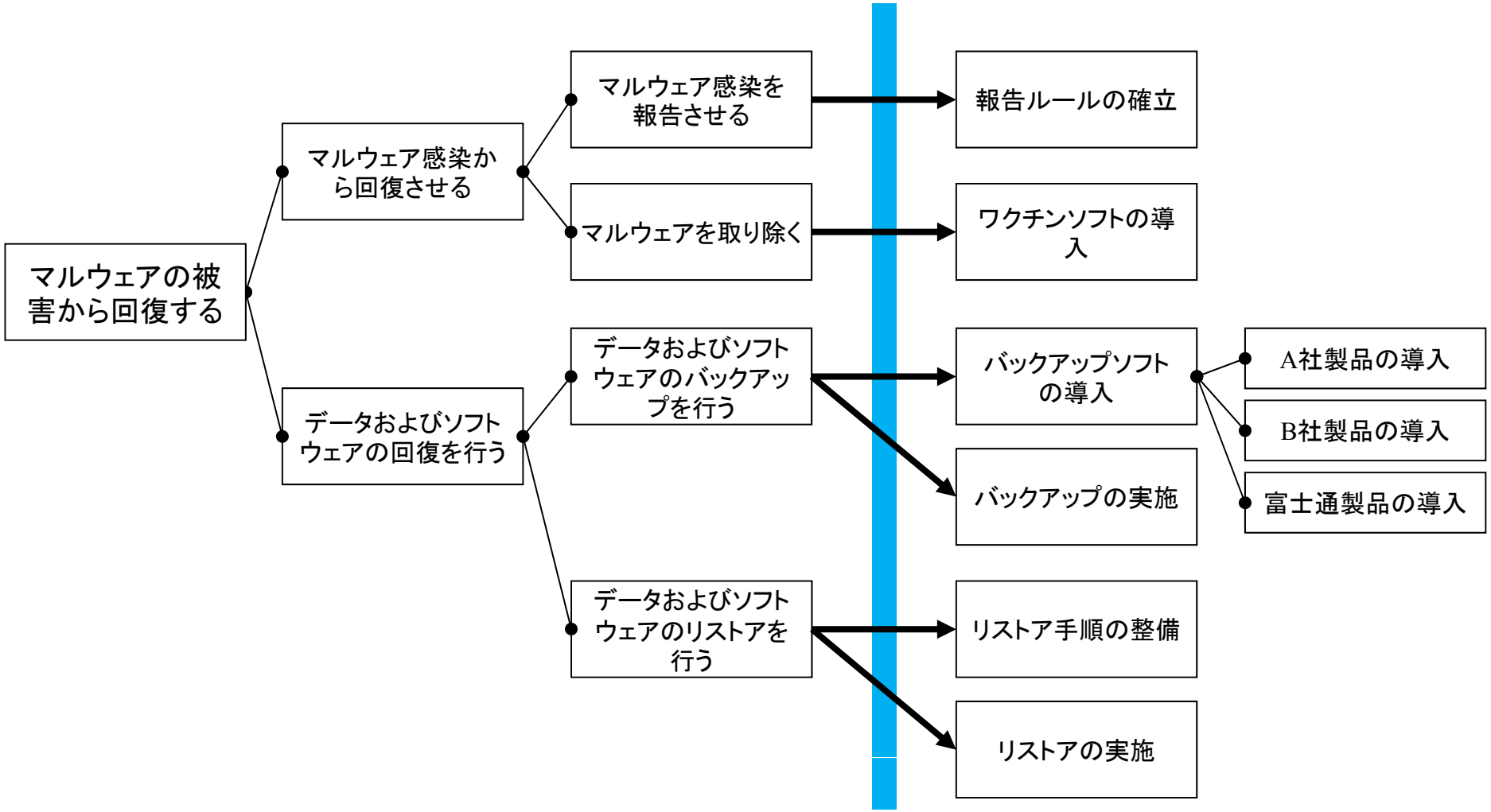


ツリー化の課題

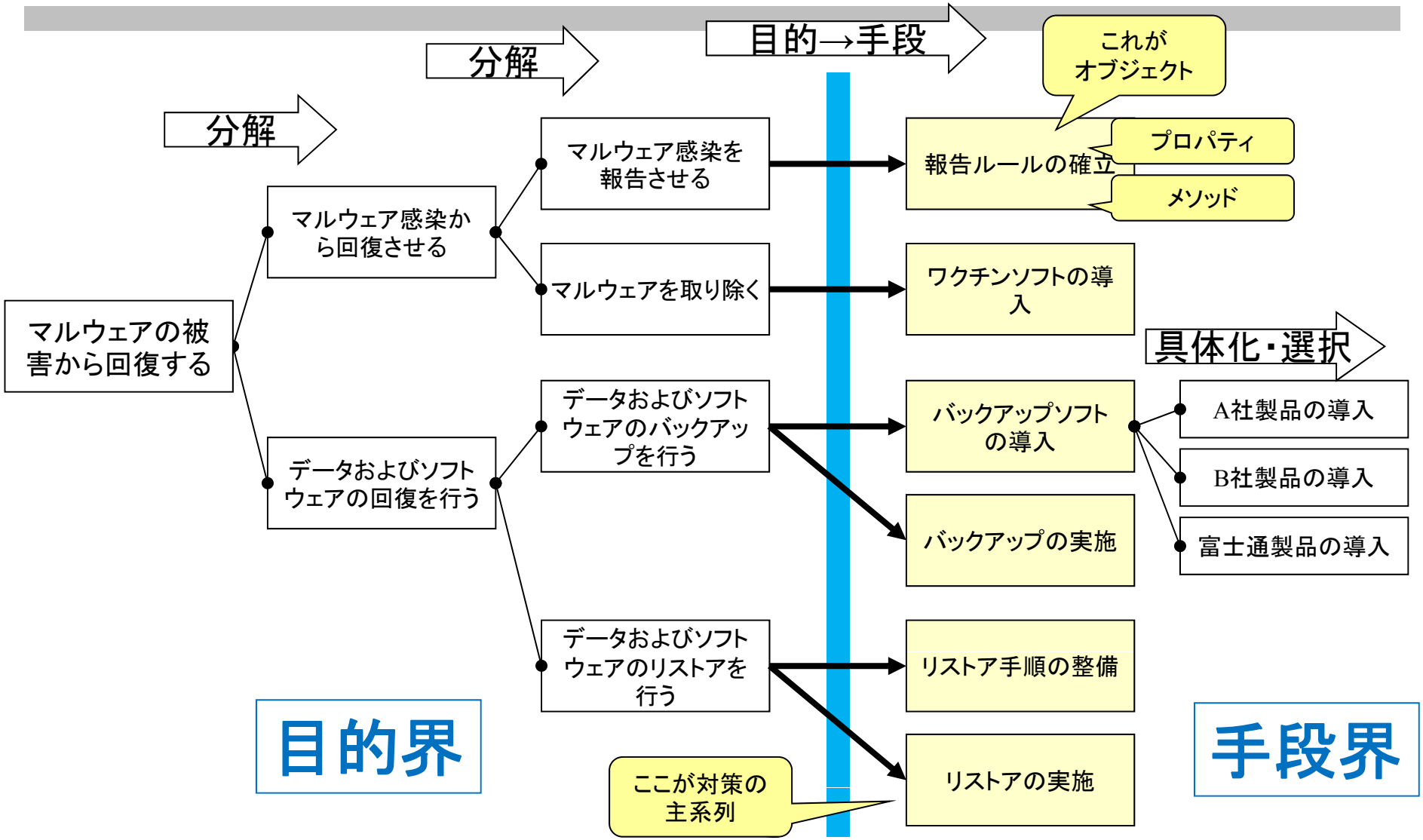
- 描く人によってツリーの形が変わってしまう（自由度が高すぎる）
- 何回描いてもこれでよいという納得感がいまひとつ得られない
- …orz



川モデル（旧称「三途の川モデル」）



川モデル（旧称「三途の川モデル」）



最新の活動

対策オブジェクトモデル V2

オブジェクト		「管理策」する。		
プロパティ		方針 目的 機能 要求事項 場所 条件 時間 実施者 対象者・対象物		
メソッド	計画	検討する 計画する	コストを算定する 文書化する	方針を確立する 有効性の測定方法を決める
	準備	責任者を明確化する 機能を明確化する 導入条件を明確化する リソースを確保する 手順を確立する	利用者を明確化する 要求事項を明確化する 導入する時を明確化する 導入する 手順を文書化する	実施者を明確化する 導入場所を明確化する 手順を明確化する 利用者を教育（訓練）する
	実施	実施する レビューする	実施時に注意を払う 実施を記録する	保守（維持）する
	レビュー	実施状況を監査する	有効性を測定する	見直す
	改善	改善する	廃止する	

オブジェクト化の例（１）

JIS Q 27002:2005 10.7.2

媒体が不要になった場合は，正式な手順を用いて，セキュリティを保ち，かつ，安全に処分することが望ましい。

媒体が不要になった場合は	→	プロパティ（条件、対象物）
正式な手順を用いて	→	メソッド（手順の明確化）
セキュリティを保ち、安全に処分する	→	オブジェクト（本体）
ことが望ましい	→	修飾節　（無視）

オブジェクト化の例（2）

JNSA

オブジェクト		セキュリティを保ち安全に処分する。		
プロパティ		方針 目的 機能 要求事項 場所 条件：　不要になった場合 時間 実施者 対象者・対象物：　媒体		
メソッド	計画	検討する 計画する	コストを算定する 文書化する	方針を確立する 有効性の測定方法を決める
	準備	責任者を明確化する 機能を明確化する 導入条件を明確化する リソースを確保する 手順を確立する	利用者を明確化する 要求事項を明確化する 導入する時を明確化する 導入する 手順を文書化する	実施者を明確化する 導入場所を明確化する 手順を明確化する 利用者を教育（訓練）する
	実施	実施する レビューする	実施時に注意を払う 実施を記録する	保守（維持）する
	レビュー	実施状況を監査する	有効性を測定する	見直す
	改善	改善する	廃止する	

何がうれしいのか

- 自然言語（日本語、英語など）で書かれたセキュリティ対策の構造が明確になる
- 「違う表現だけど同じ対策」を同じと認識できる
- 何言っているかわからない対策の意味が明確になる

次の仕事

- 世の中のセキュリティ対策を集める
- 集めた対策をオブジェクトモデルに基づいて標準化する
- それを何とか地図にする

たとえば標的型攻撃対策

- 複数の対策を網羅的に実施するのがよいと言われている
- どの対策を選び、どこに配置すればいいのか、実態は手探り
- やはり「地図」があった方がよいのでは

参考：IPA「新しいタイプの攻撃」の対応策
http://www.ipa.go.jp/about/press/20110920.html

【対策1】：入口（ネットワーク経路）をしっかり守る
【対策2】：ファイアウォールを抜けてもシステムにつけ入られる隙（脆弱性）を与えない
【対策3】：ウイルスの活動（組織内蔓延（まんえん）や外部通信）を阻害、抑止する。
＜出口対策＞
【対策4】：重要な情報はその利用を制限（アクセス制御）する
【対策5】：情報にアクセスされても保護するための鍵（暗号）をかける
【対策6】：操作や動き（ログ証跡）を監視・分析し不審な行為を早期に発見する
【対策7】：万一被害が発生したら早急な対応（ポリシーと体制）をとる

本日のBoFへの期待

- どんな地図があるといいと思いますか
- 地図があったら何に使いますか
- 地図は何かの役に立ちそうですか

忌憚ないご意見お願いします

ディスカッション

コメンテーターご紹介

（五十音順）

加藤　雅彦氏

JNSA 幹事／調査研究部会長

二木　真明氏

JNSA 2011年 リスク評価検討WG リーダー

やすだ　なお氏

株式会社ディアイティ／JNSA主席研究員

テーマ1
「ここが変だよ、このセキュリティ対策」

テーマ1

- 皆さんが出会った「変なセキュリティ対策」はありませんか
- 変な（矛盾する）対策の例
  - キングファイルはわかりやすいところに情報種別のラベルを付ける V.S. 秘密情報は見えると狙われやすくなる
  - 携帯電話の電話帳はイニシャル化する V.S. 誤送信や誤発信が多くなる
  - メールの暗号化をする V.S. メールのチェックをサーバで行う
  - パスワードを複雑にする V.S. 覚えきれなくて付箋に書く
  - ノートPC持出禁止 V.S. BYOD推進
  - 暗号化ファイル添付メールの後追いパスワードメール

テーマ2
「今までの情報セキュリティマップ・カタログの不満な点は？」

セキュリティ対策マップ・カタログらしきものの例（再掲）

- 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
- HIPAA
- 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

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？」

テーマ２

- 皆様はどう思いますか。

テーマ３
「標的型攻撃時代に求められる情報セキュリティマップってどんなもの？」

テーマ3

- セキュリティ対策の地図に何を期待しますか
  - セキュリティ対策カタログとは違うもの？

- 標的型攻撃やAPTなどの現代のセキュリティ脅威に対抗するにはどんなセキュリティの地図が必要になるでしょうか

JNSA

ご参加ありがとうございました。