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（マップ化）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
富士通株式会社

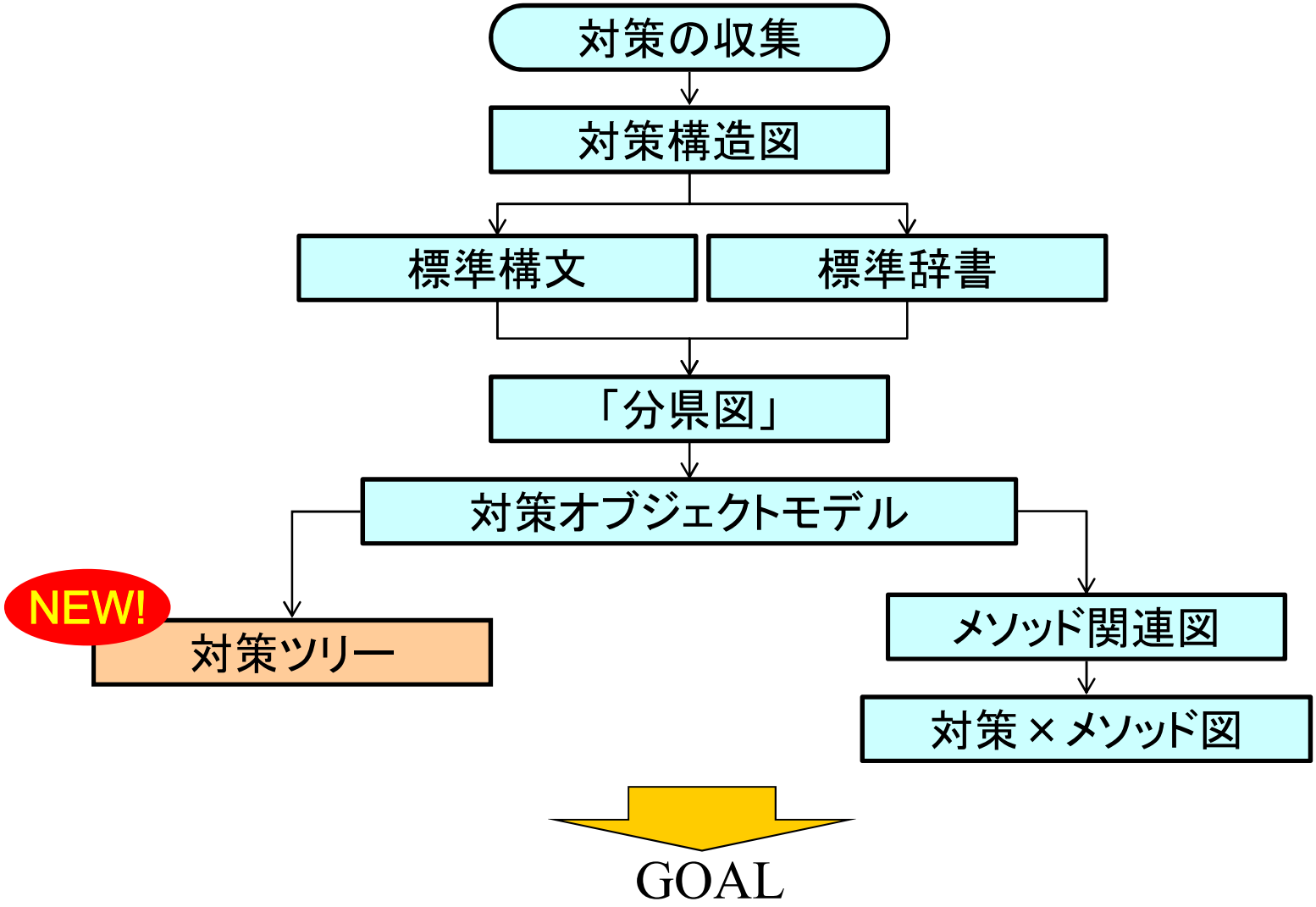
2011 年 6 月8日

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

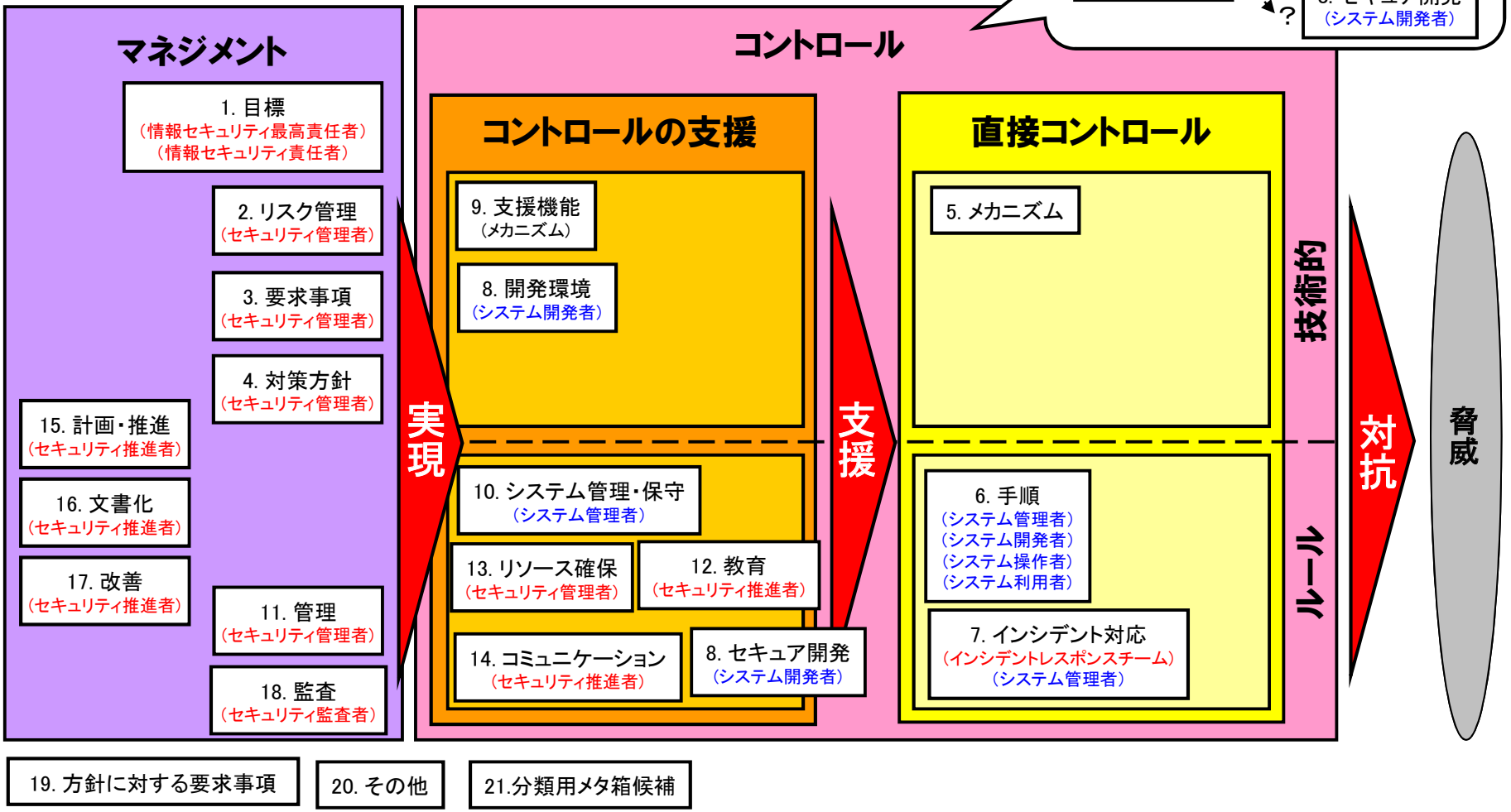


前回までのあらすじ
（2009年度～2010年度）

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）

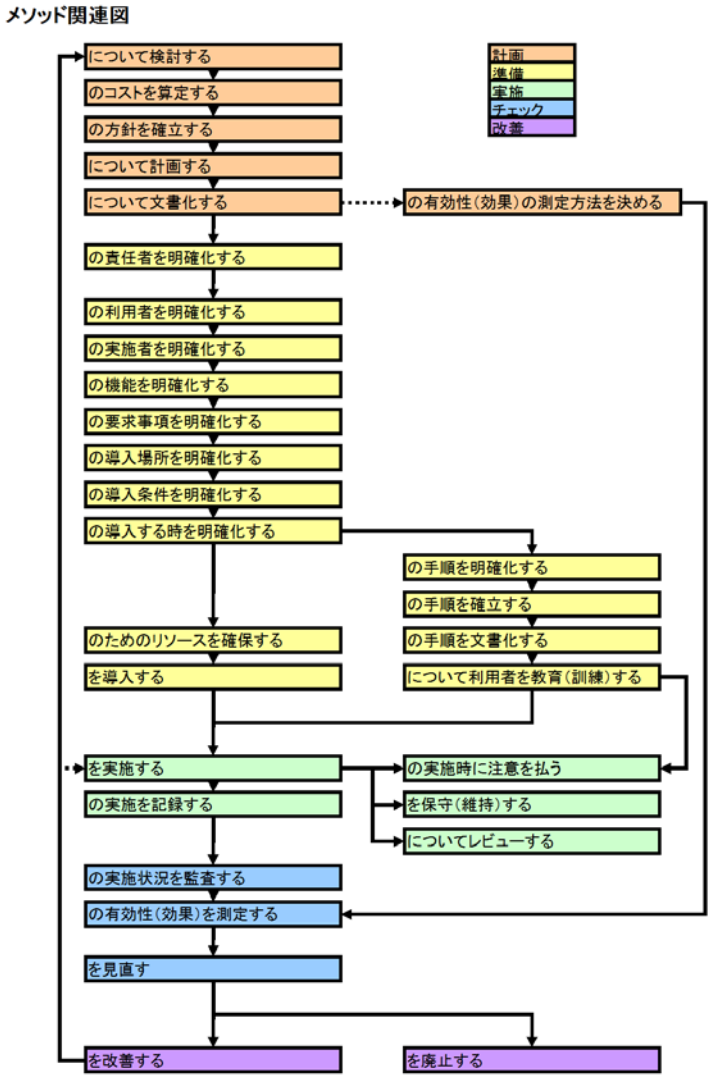
ID	名称	分類	内容
MAL.1	マルウェアからの防御	03.《要求事項》	マルウェアから保護するために、【防御対策の種類のリスト:｛予防｝、｛発見｝、｛回復｝】の防御対策を実施する。
MAL.2	マルウェアの検知	04.《対策方針》	【実施者のリスト:｛組織は｝】【条件のリスト:｛データの送受信の都度｝】【場所のリスト:｛外部ネットワークと内部ネットワークを接続するゲートウェイ等｝】に【使うツールのリスト:｛不正プログラム対策メカニズム｝】を利用して、【媒介物のリスト:｛電子メール｝、｛電子メールへの添付ファイル｝、｛インターネットアクセス｝、｛取り外し可能な記録媒体（｛USB デバイス｝、｛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

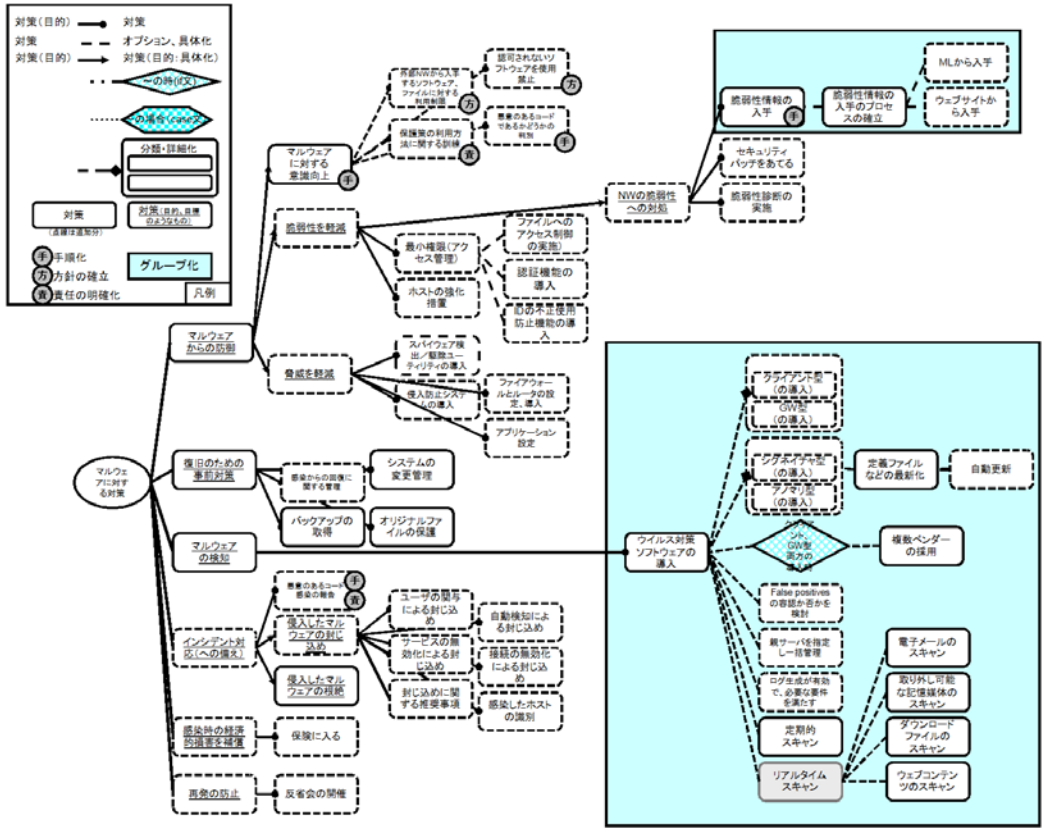


- メソッドは対策のライフサイクル（PDCA）と関係が深いように見える
- メソッドを使うフェーズに着目して整理するとメソッドの関係が可視化できるのでは
- どのような図になるかを現在検討中（左はその一例）

対策のツリー化の試行
（2011年度成果）

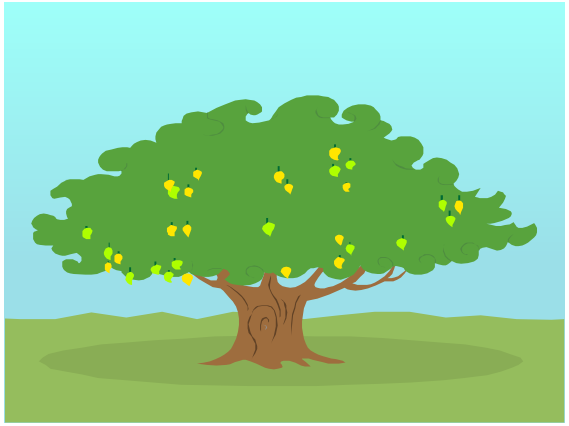
分県図のツリー化

- 「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



寄り道：CRAMMを調べてみた

- 対策の分類の仕方に何かヒントはないか
- そういえばリスク分析ツールは対策のDBを持っている

- 著名なリスク分析ツール「CRAMM」が対策をどう扱っているかを調査してみた

CRAMMとは

- イギリス発祥のリスク分析手法とツール
- シーメンス社が製品として販売
- 30日間無料ライセンスで試してみました

CRAMM V

If you‘re responsible for information security within an organisation, you’ll quickly appreciate the value that CRAMM could bring to every aspect of assessing, designing and managing your information security strategy.

CRAMMのWebサイトより http://www.cramm.com/

CRAMMの対策分類

- 5段階の階層化した対策データベース
  - 階層１：グループ（81項目）
  - 階層２：サブグループ（283項目）
  - 階層３：セキュリティ目的（Security Objectives）（425項目）
  - 階層４：機能（Functions）（1622項目）
  - 階層５：実例（Examples）（1274項目）
- 上位層が目的に応じた分類、下位層が具体的な対策
- 「目的」と「機能」の分類は一見よくできているが、詳しく見てみると釈然としない部分もある　→　ブレークスルーのヒント

ブレークスルー

- 実は「目的」と「対策」の区別はあいまい
  - 「○○（という目的のため）の対策を実施する」という形の対策ガイドラインの存在（これは目的か、それとも対策か）
  - 対策の表現には「目的型対策表現」と「手段型対策表現」がある
  - もしかすると「目的型対策表現」と「手段型対策表現」は一つの対策の裏表なのでは
- 真ん中に線（「川」）を引いて、目的と手段で対策を分けてみよう

「目的」と「手段」の分別

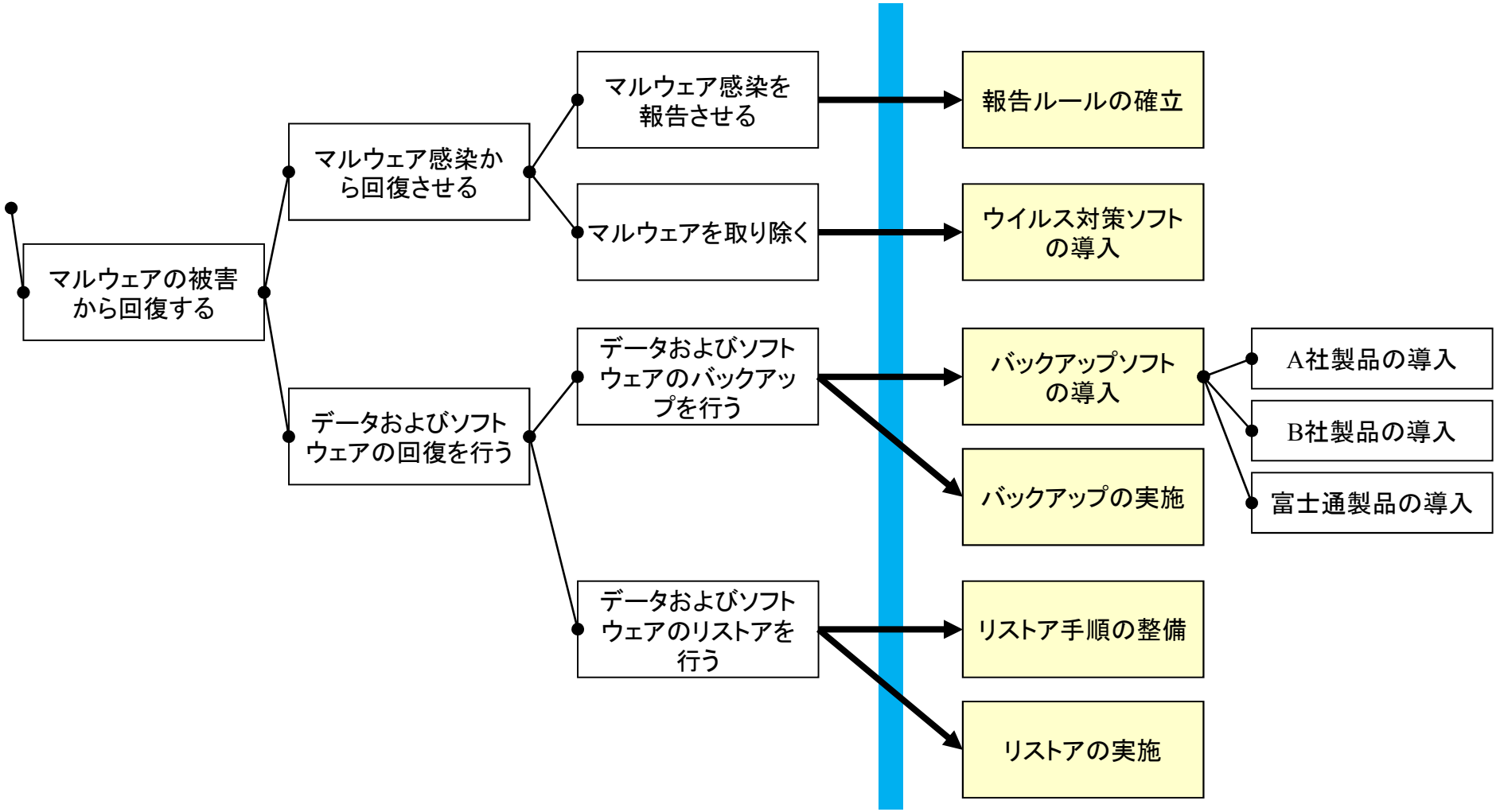
ひとつの目安として:

- 「〇〇したい」と表現して違和感がないときは、これを目的型と判断することした。
- 「〇〇したい」と表現すると何か違和感があるときは、これを手段型とした。

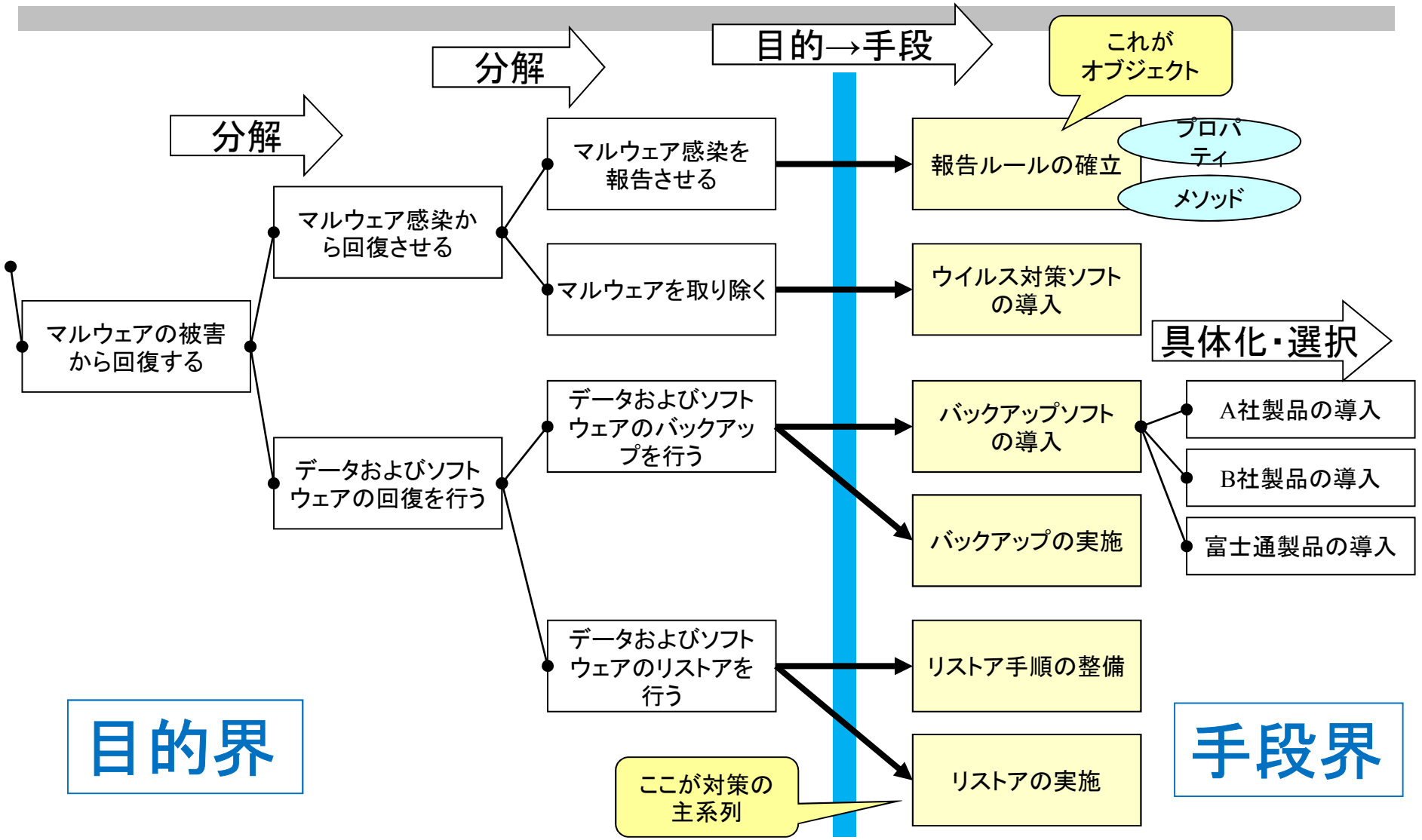
例:

- 「マルウェアの拡散を防止する」→目的型
- 「マルウェアの感染を報告する」→手段型

「三途の川（仮称）」モデル



「三途の川（仮称）」モデル



まとめ

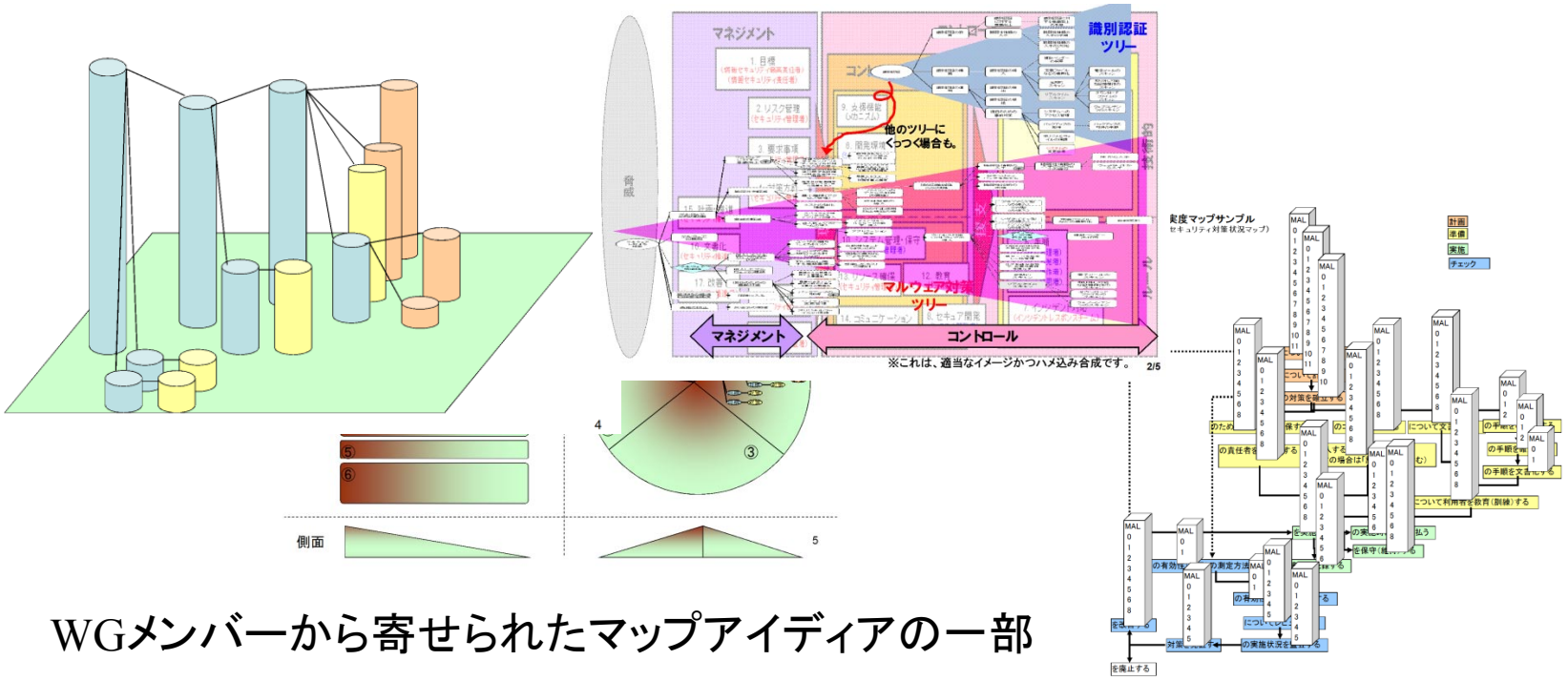
- ツリーについて、ある程度作成の方法を標準化できた。
- マルウェア対策のツリーの試作図が完成した。（本日配布）
- 他の分野についてのマップ化への道筋が少しずつ見えてきた（あと80分野？）

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

今年の抱負

- 最後の一年なので、これまでの知見を生かし、夢のある「マップ」を描いてみたい！



WGメンバーから寄せられたマップアイディアの一部