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活動報告

ーセキュリティ対策の構造と戦った4年間ー

奥原　雅之
JNSA 情報セキュリティ対策マップ検討WG

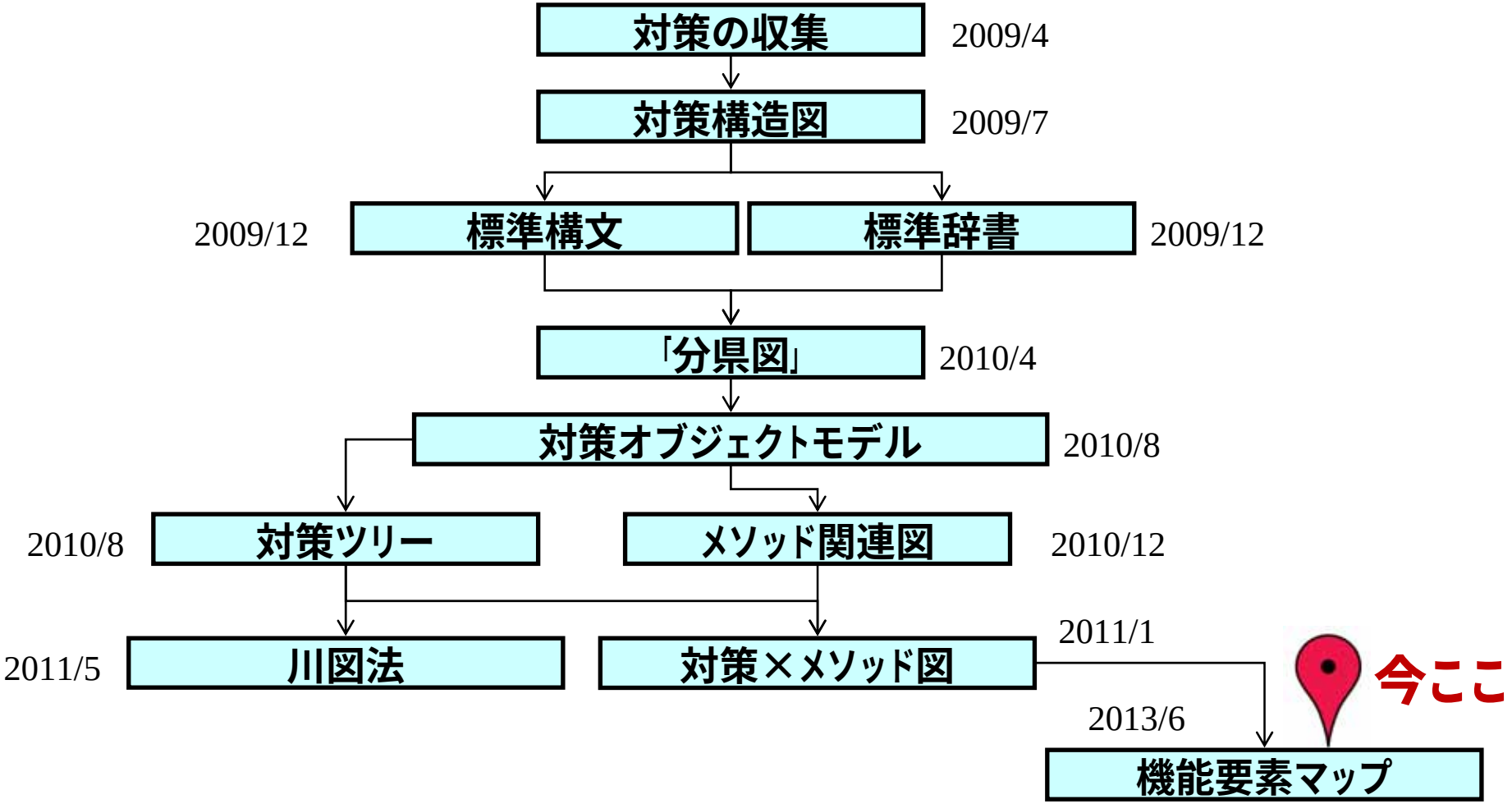
2012 年 6 月7日

WG活動の歴史

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

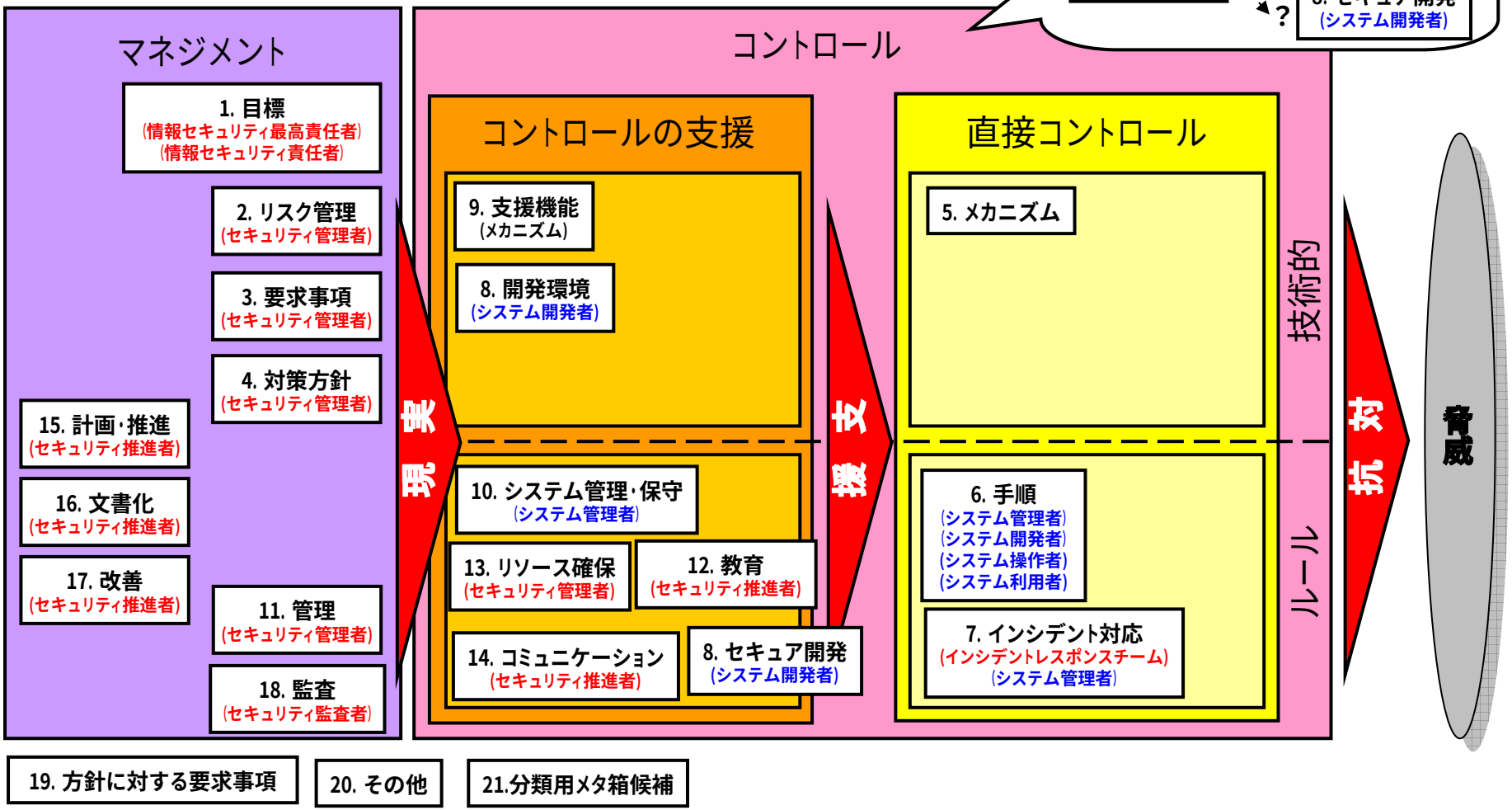
大まかな流れ



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)
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)
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
実現
支援
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

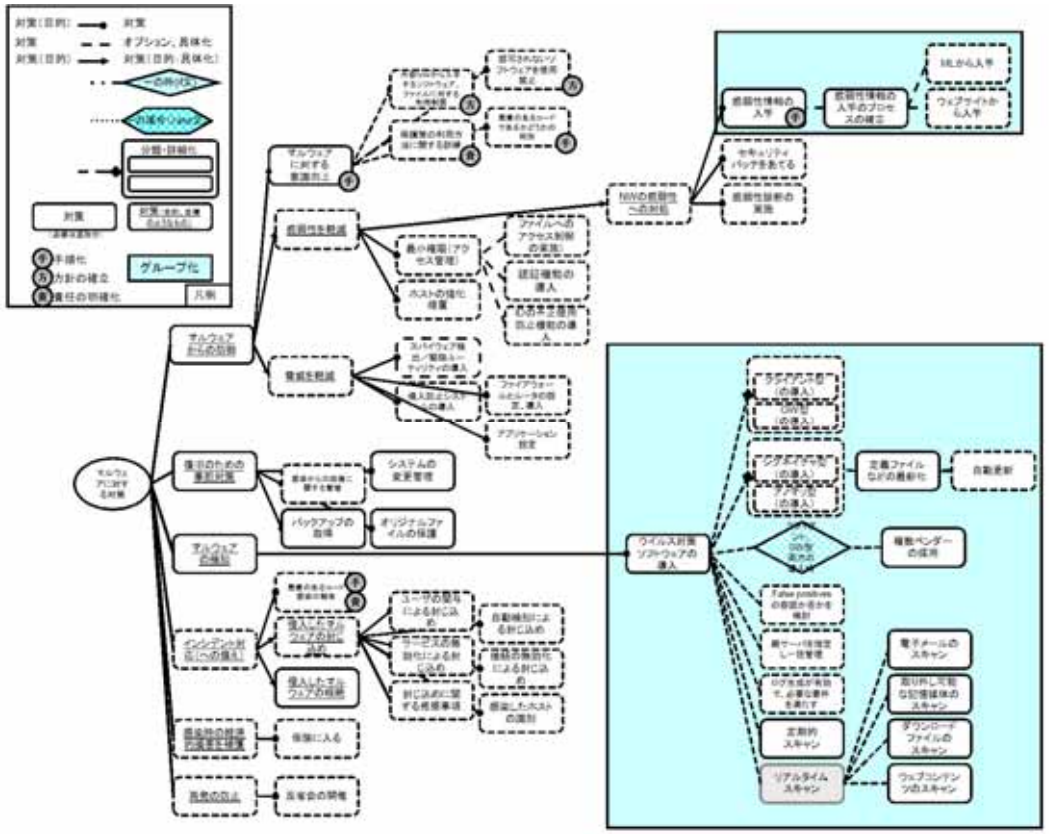
「マルウェア分県図」の試作

NSF2010にて成果ご紹介した分県図（部分）

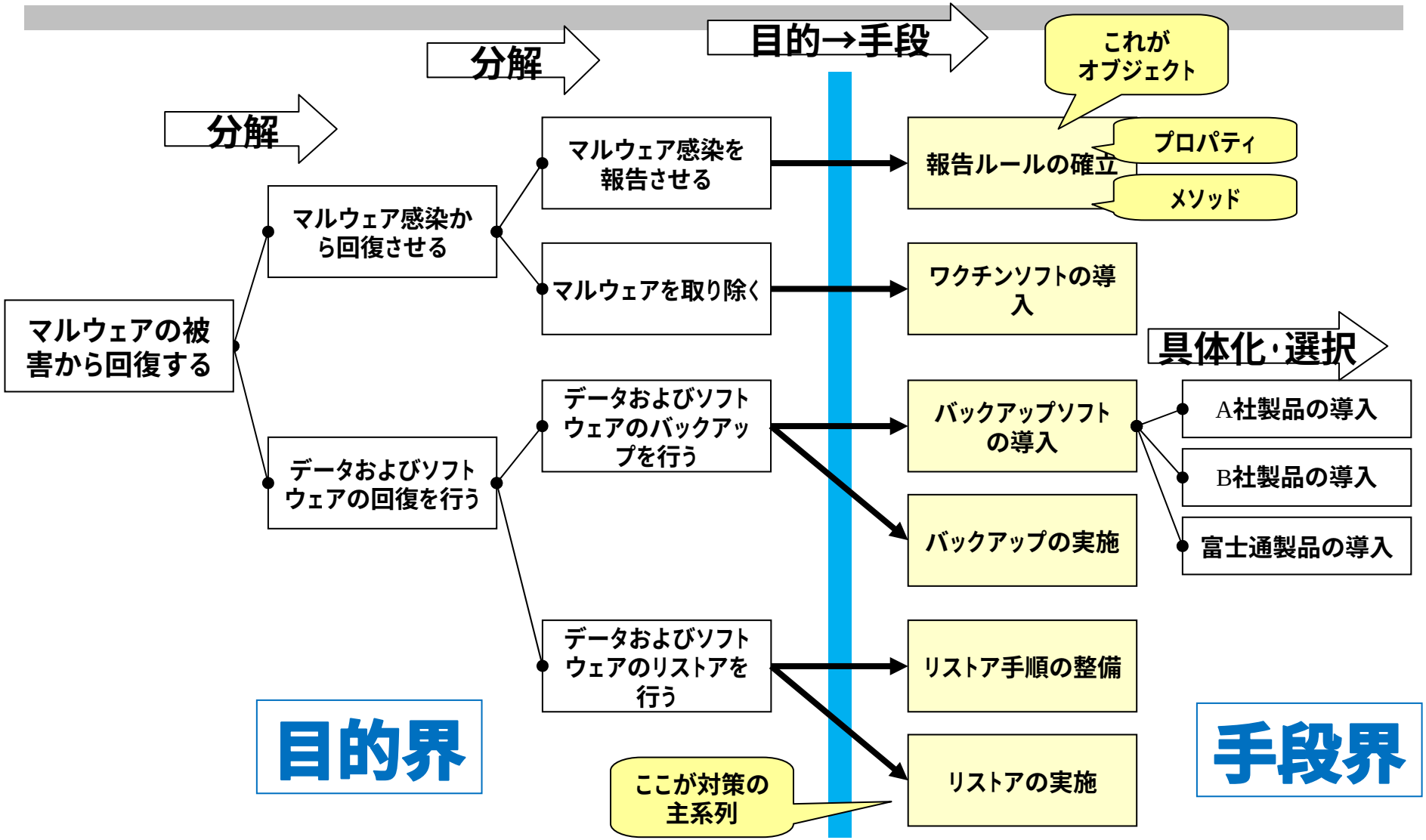
ID	名称	分類	内容
MAL.1	マルウェアからの防御	03.《要求事項》	マルウェアから保護するために、【防御対策の種類のリスト：{予防}、{発見}、{回復}】の防御対策を実施する。
MAL.2	マルウェアの検知	04.《対策方針》	【実施者のリスト：{組織は}】【条件のリスト：{データの送受信の都度}】【場所のリスト：{外部ネットワークと内部ネットワークを接続するゲートウェイ等}】に【使うツールのリスト：{不正プログラム対策メカニズム}】を利用して、【媒介物のリスト：{電子メール}、{電子メールへの添付ファイル}、{インターネットアクセス}、{取り外し可能な記録媒体（{USB デバイス}、{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

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



川モデル（旧称「三途の川モデル」）



見えてきた課題
ー何がマップ作成を阻むのかー

集めれば何とかなる？

- はじめはとにかく対策をたくさん集めて分類すれば地図が書けるに違いないと考えた
- 対策をたくさん集めてみた

- 全部違う…orz
  - 用語が違う
  - 細かい表現が違う
  - 粒度（抽象度）が違う
  - 色々なものが混ざっている（右図）
  - …そもそもセキュリティ対策って何？

アプローチ

- 対策の正規化
  - あらゆる対策を同じ表現で書けるようにする
- 対策の原子化
  - 対策を互いに比較できるように「これ以上分割できない極限まで具体化されたレベルの対策」を定義する

対策の正規化

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

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」

対策オブジェクトモデル

JNSA

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。

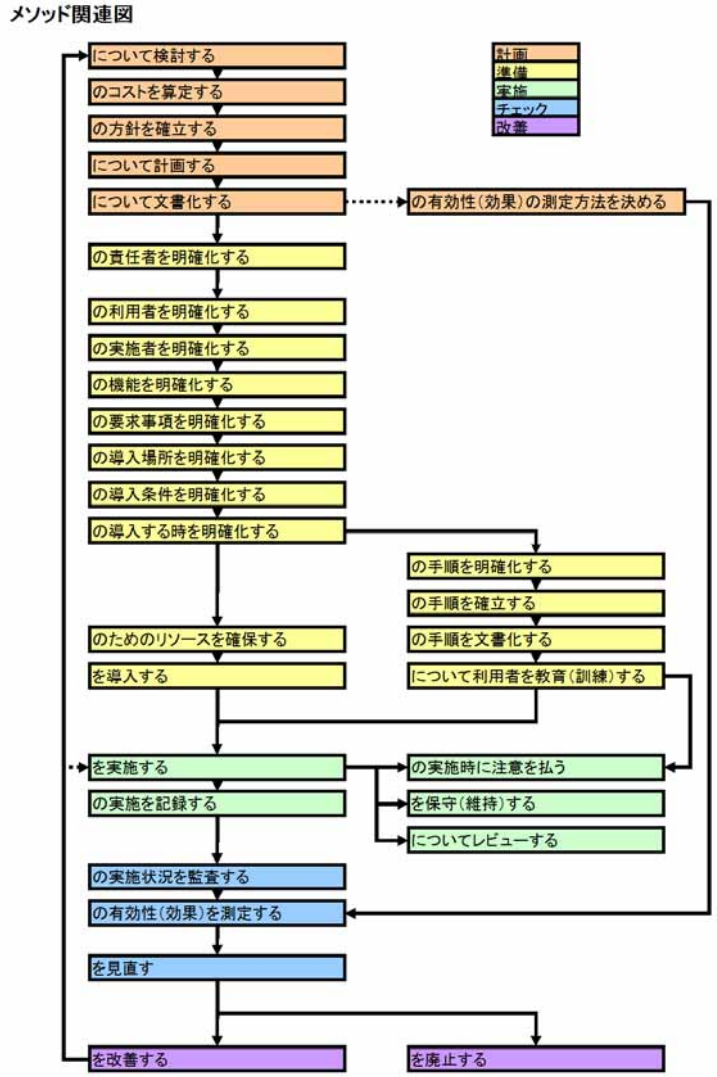
媒体が不要になった場合は	→	プロパティ (条件、対象物)
正式な手順を用いて	→	メソッド (手順の明確化)
セキュリティを保ち、安全に処分する	→	オブジェクト (本体)
ことが望ましい	→	修飾節　(無視)

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	

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

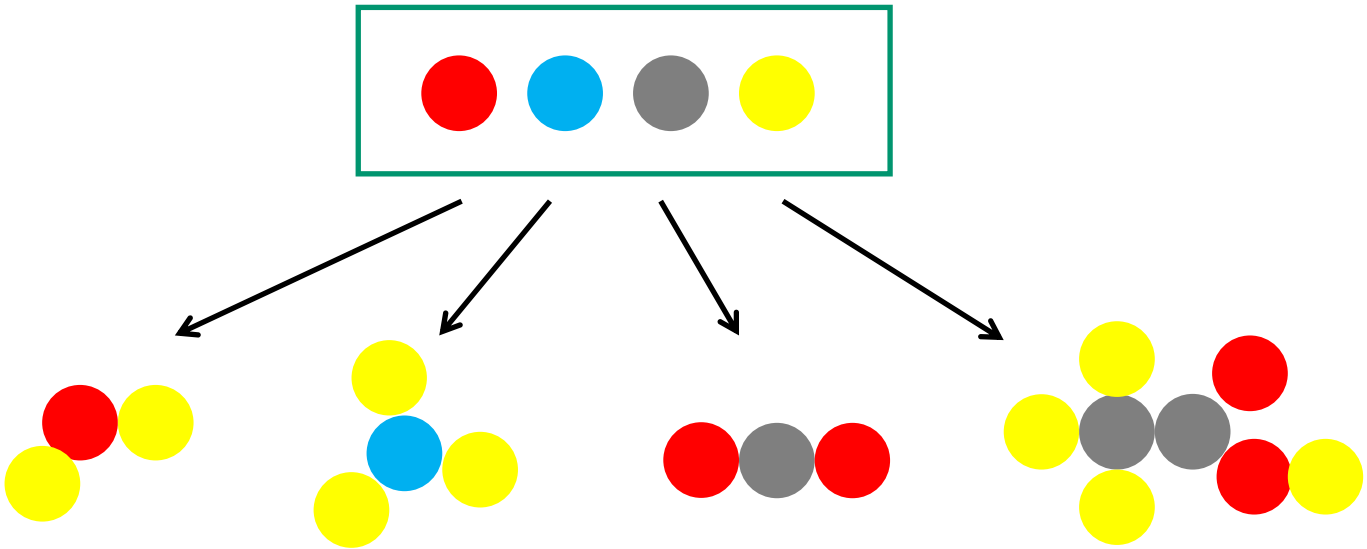
対策の原子化

方針

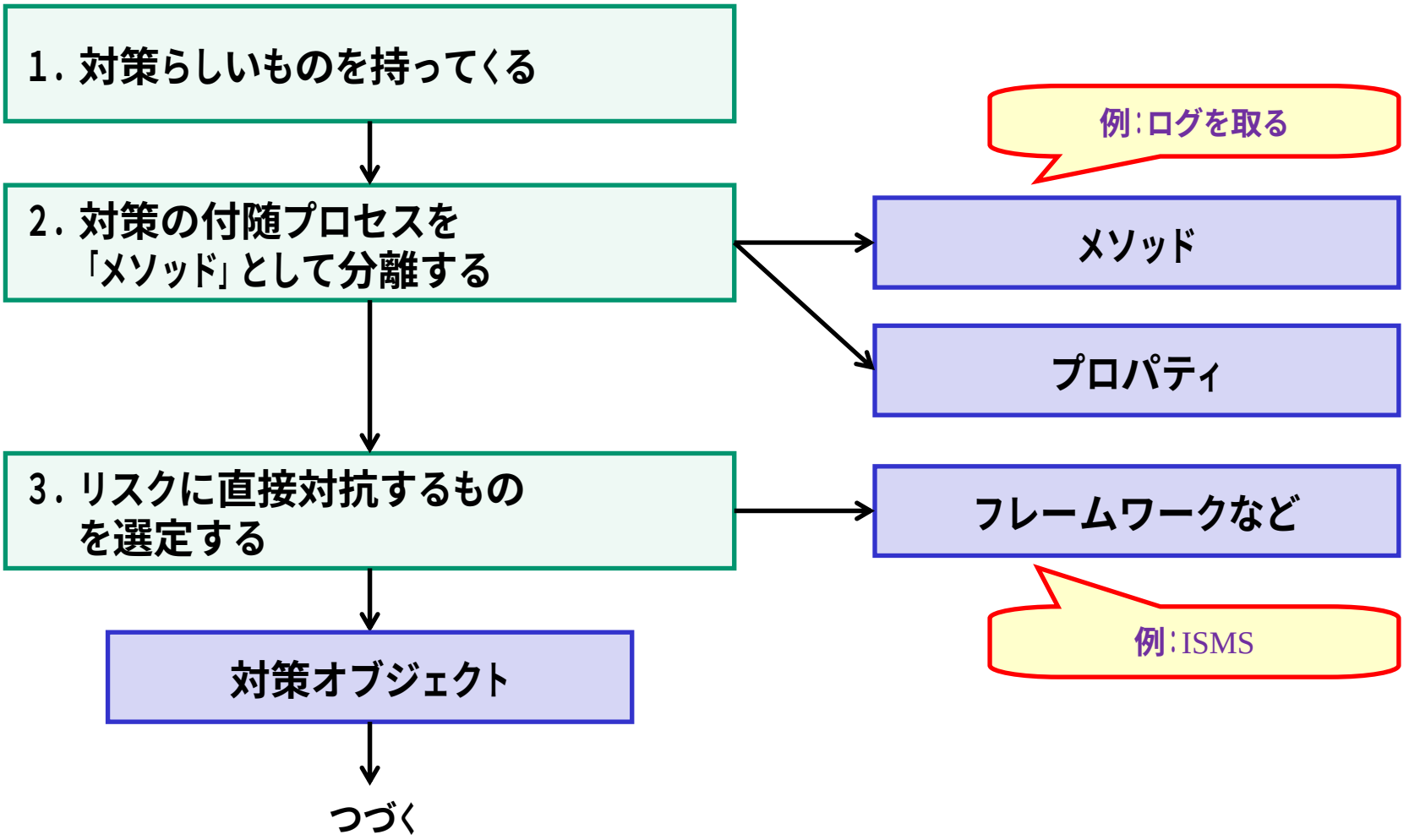
- 対策を「リスクに直接対抗する本質的な機能」と、それを支援するその他の機能に分ける
- それ以上は分解できない、原子のような対策の「機能要素」を抽出する

原子化の意味

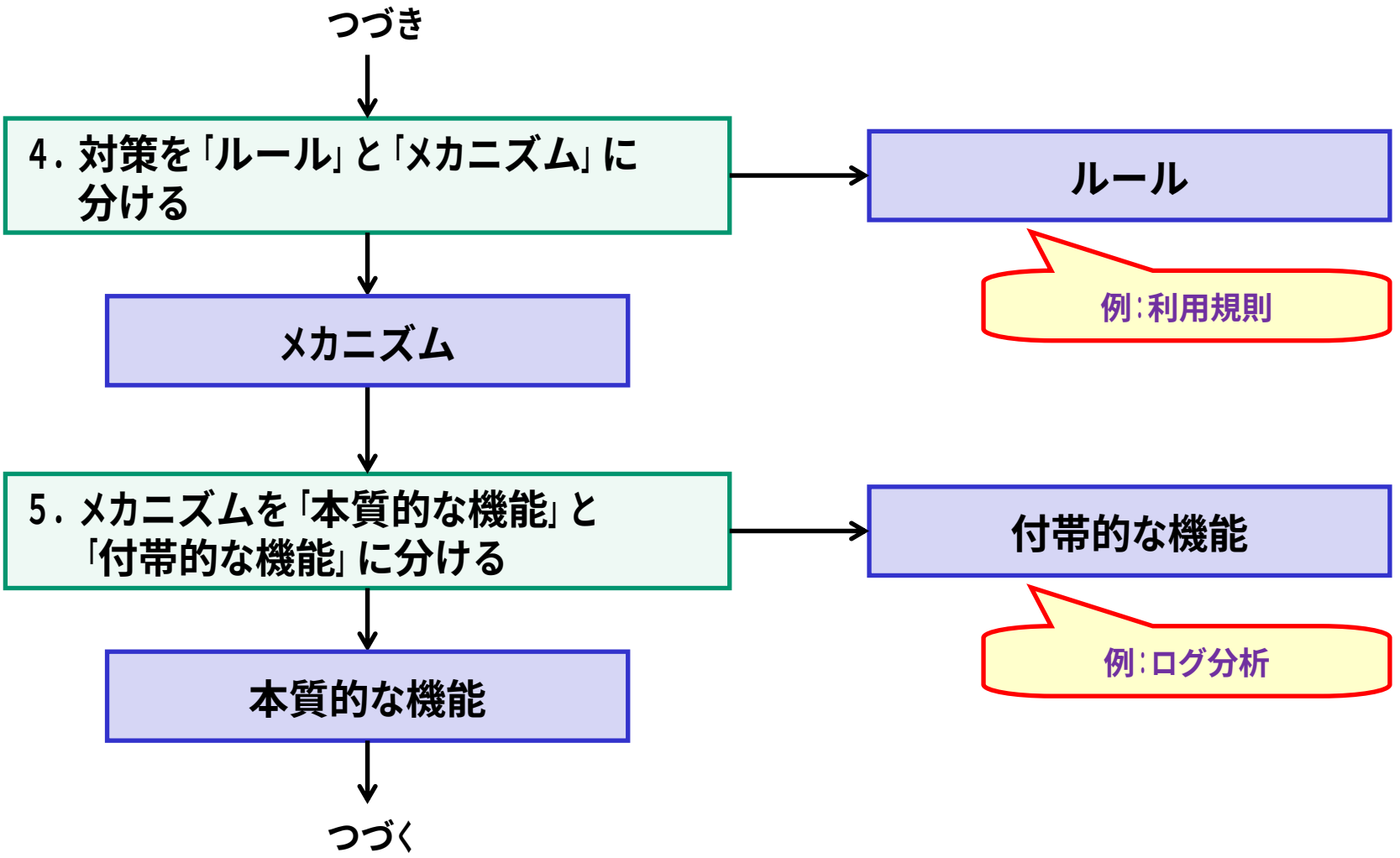
- 「機能の最小単位」が明確になれば、複雑なセキュリティ対策でも正確に記述できる
- 粒度が違う対策同士の分類が可能になる



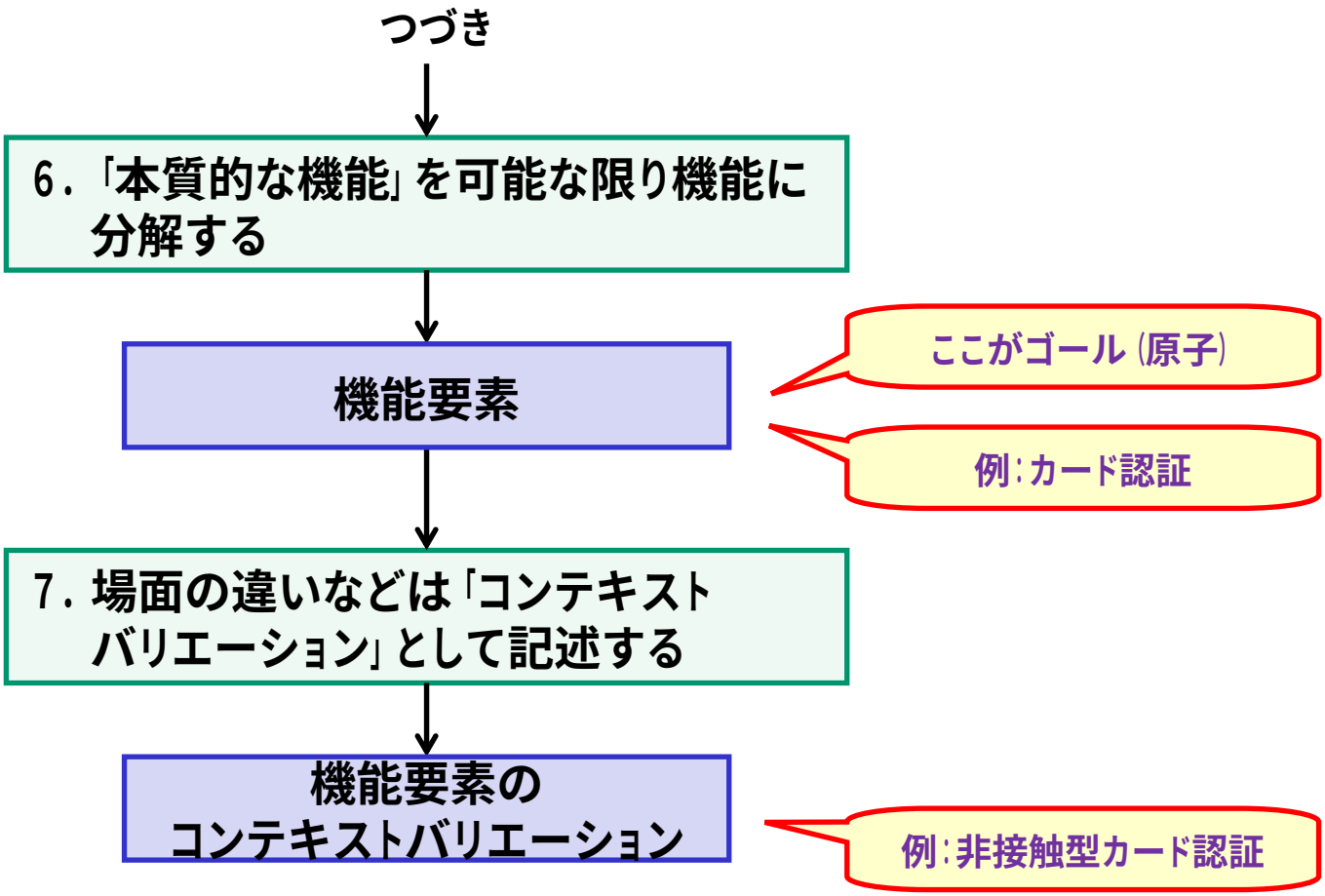
対策の原子化（1）



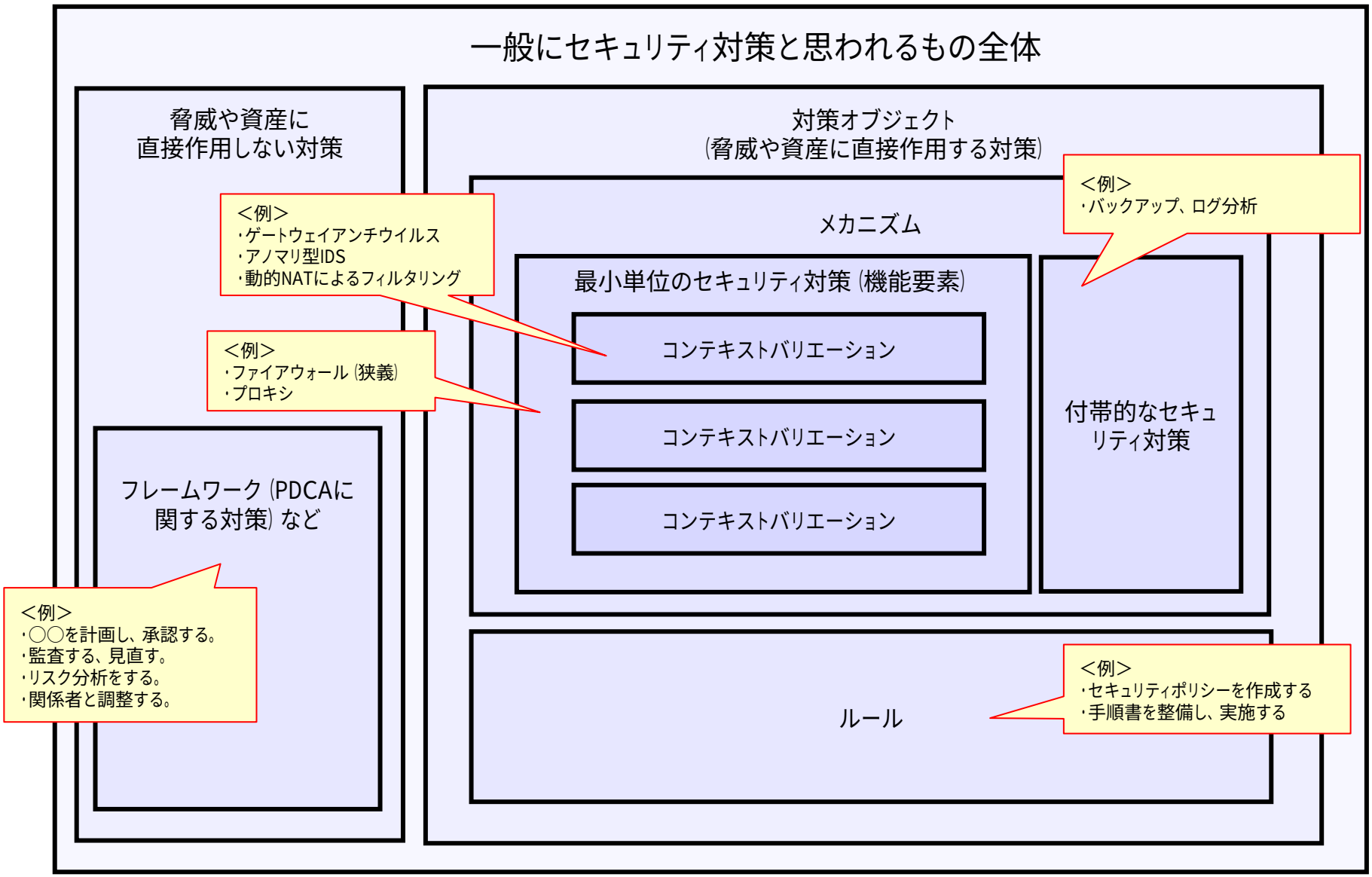
対策の原子化（2）



対策の原子化（3）



原子化に基づいた対策の構造（整理中）



評価

評価その１

- IPAの「標的型攻撃対策ガイド」のマップを作ってみた
- なんとなく整理できた
- 実在の製品と組み合わせるといい感じになりそう（現在試行中）

評価その2

- せっかくオブジェクト指向でモデル化しているので、オブジェクト指向の手法を使ってアクティビティ図を書いてみた
- 書いてみるとなんとなく納得できる
- オブジェクト指向の手法がそのまま使えるかも

今後の課題

今後の課題

- 「なんとなく」を「きちんと確かめる」
- 製品をプロットしたマップを作ってみる
- セキュリティ対策の可視化に役立つ図法を考える
- オブジェクト指向の手法との親和性も見てみる
- 詰めが甘いところをもう少し整理する

そんなわけで

- ２０１３年度も継続活動します　m(_ _)m
  - 今年度が最後です
- WG参加者募集します
  - 本当に今年度が最後です