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最終活動報告

―目的の島、彼岸の川。究極のセキュリティ対策地図を追い続けた者たちが最後に見たものは―

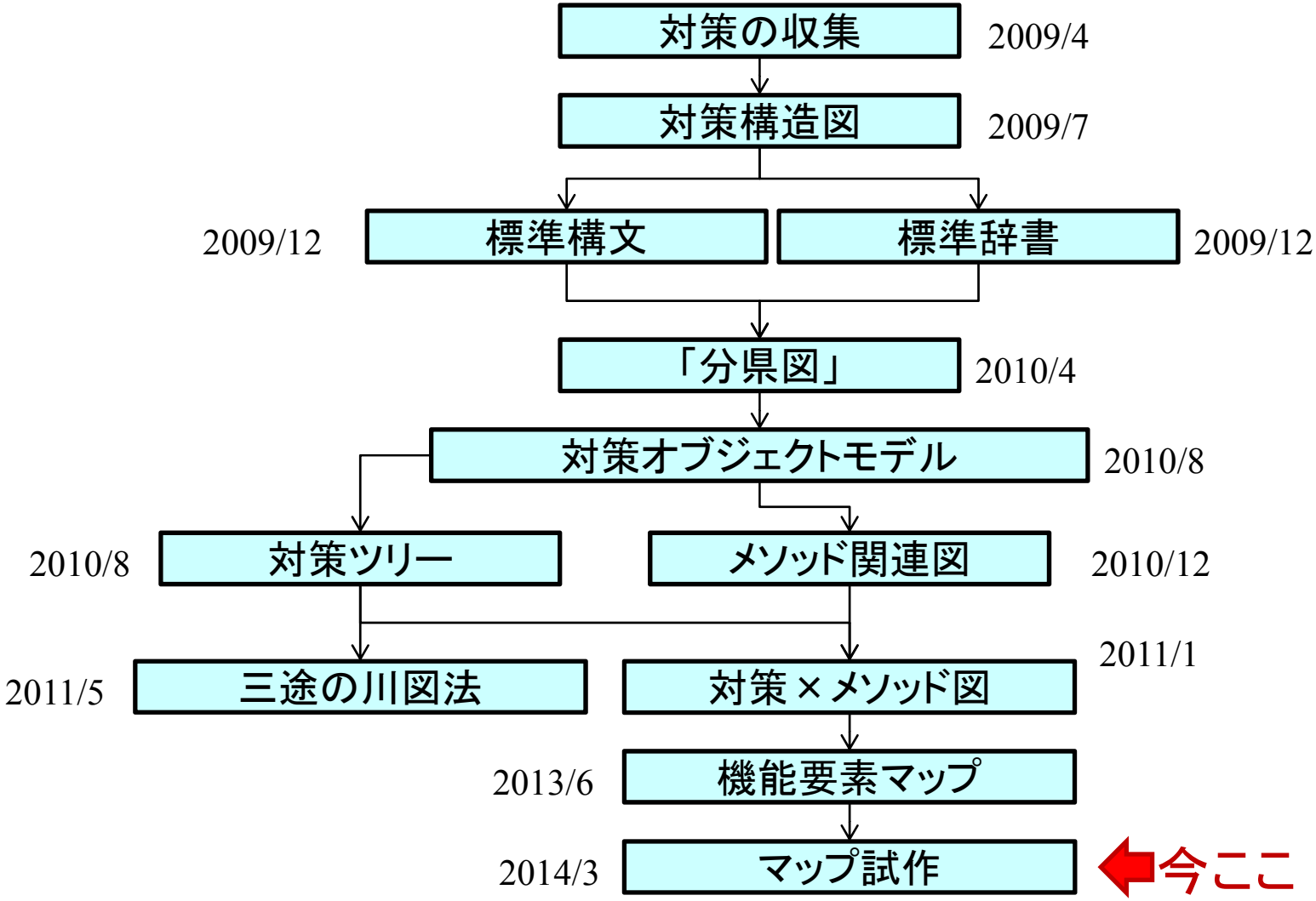
奥原　雅之
JNSA 情報セキュリティ対策マップ検討WG

2014 年 6 月10日

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

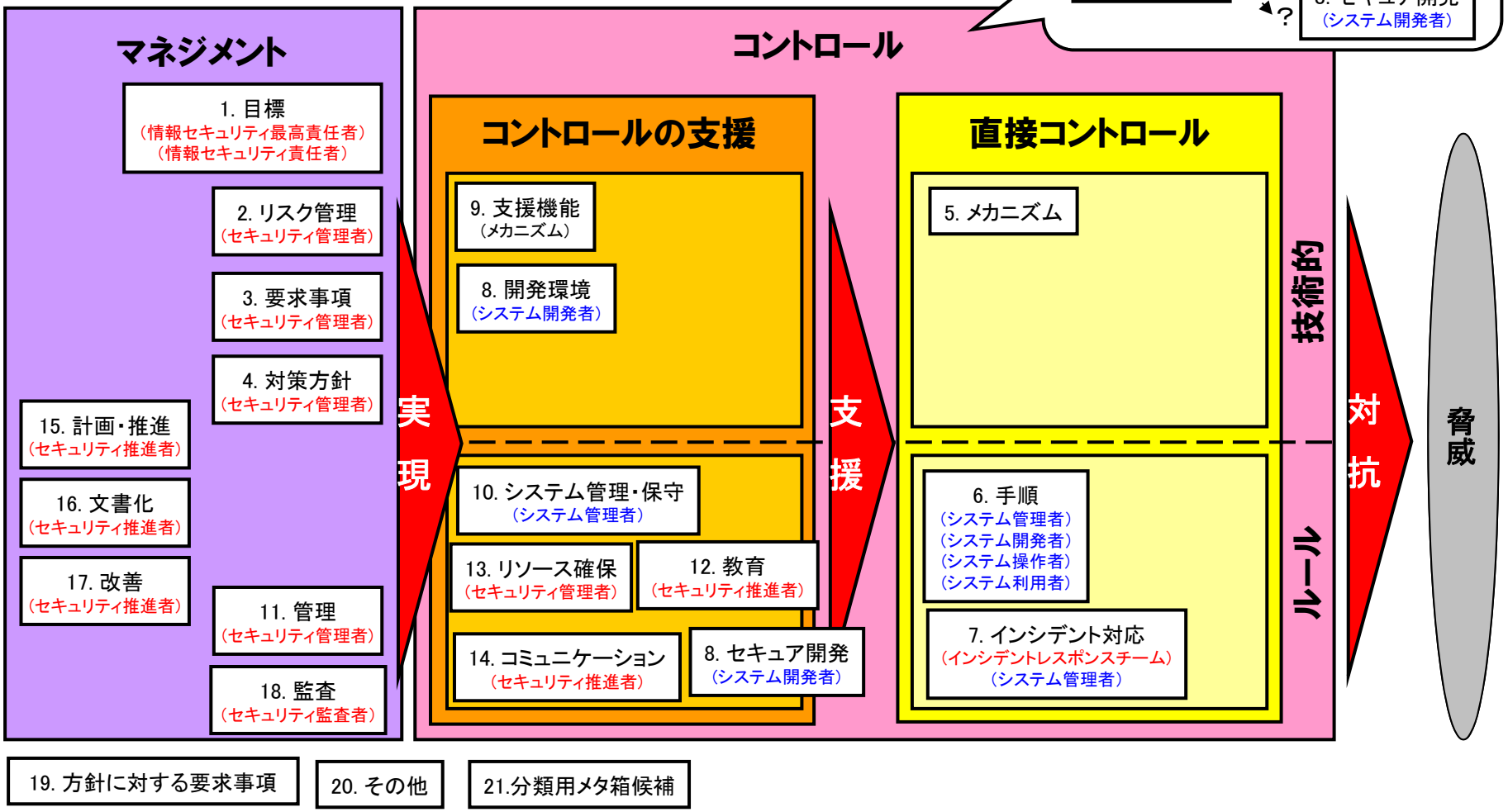
大まかな流れ



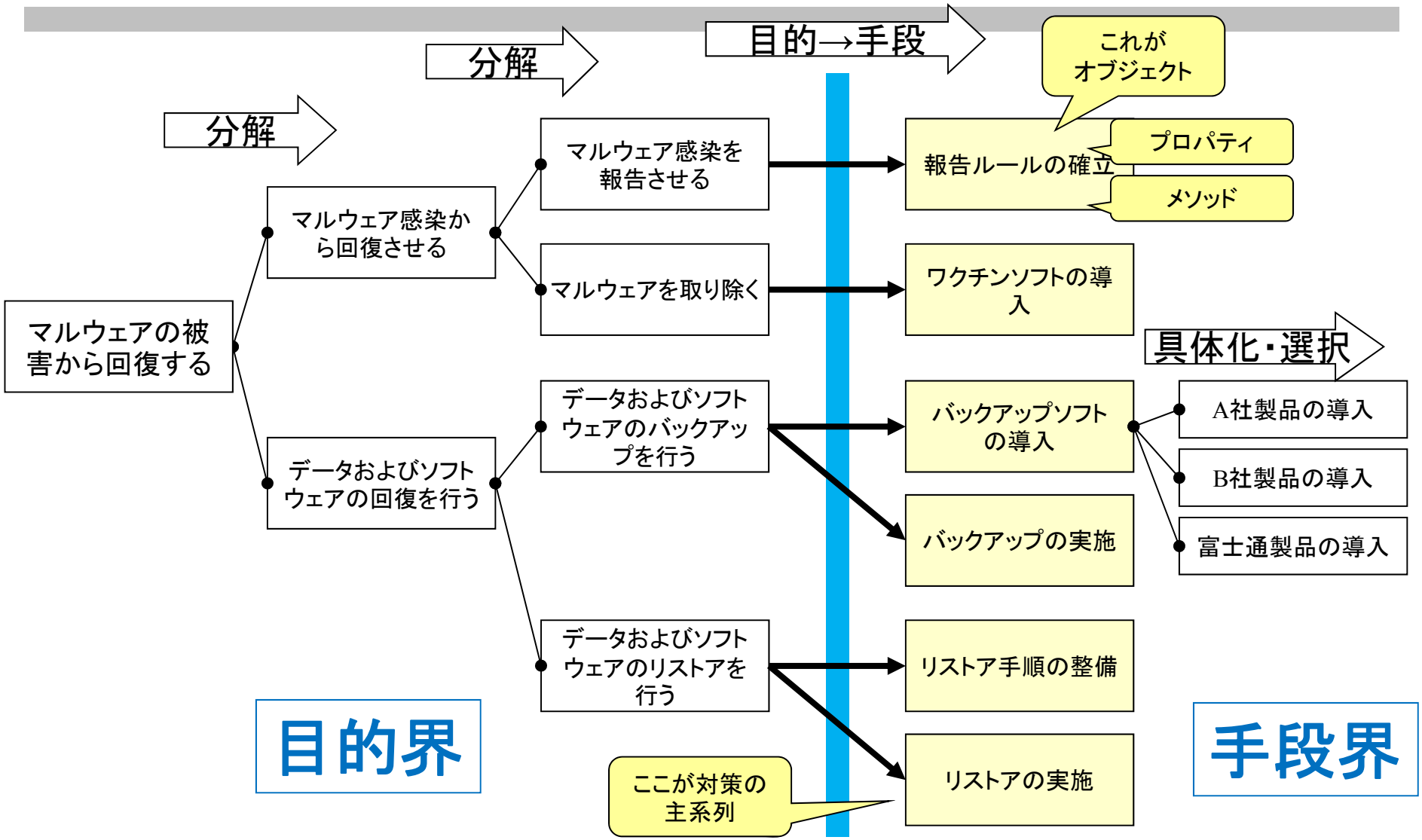
セキュリティ対策の収集

- 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
- NIST 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



三途の川モデル



対策オブジェクトモデルの提言

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
  - 色々なものが混じっている（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「極限まで具体化されたレベル」を定義する
- 対策のリポジトリの作成
  - 構造が正規化された対策の集合を一種の「データベース」としてまとめる

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

プロパティ

【目的・脅威】 のために 【実施者】 は

【条件】 のときに 【場所】 で

オブジェクト

【対策】 を

メソッド

【動詞】 する

修飾

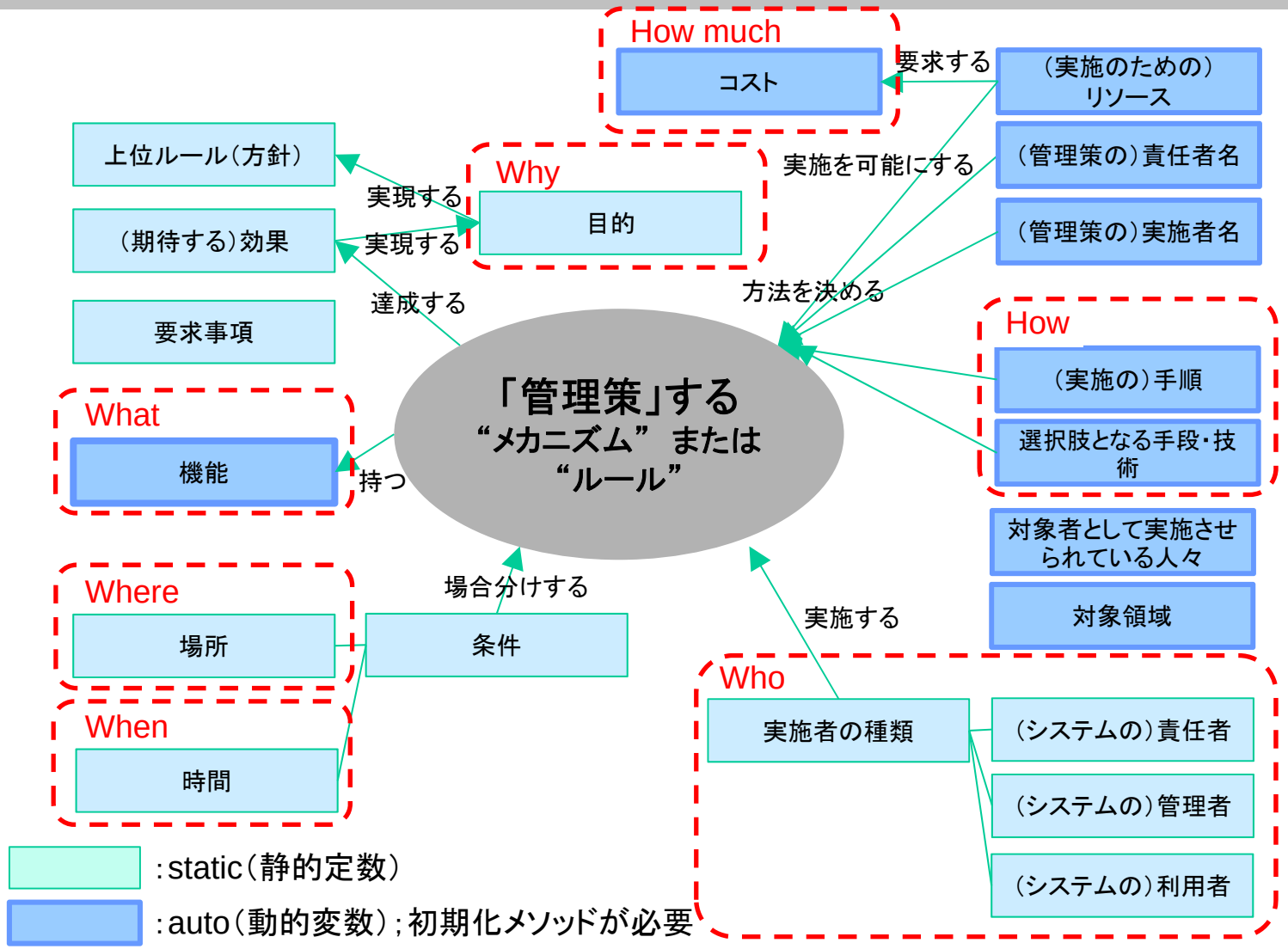
【副詞】
管理策の実施に関する修飾。
例:「もれなく」、「早く」

【結句】
管理策の要求の強度など。
例:「ことがのぞましい」、「べきである」

対策オブジェクトモデル

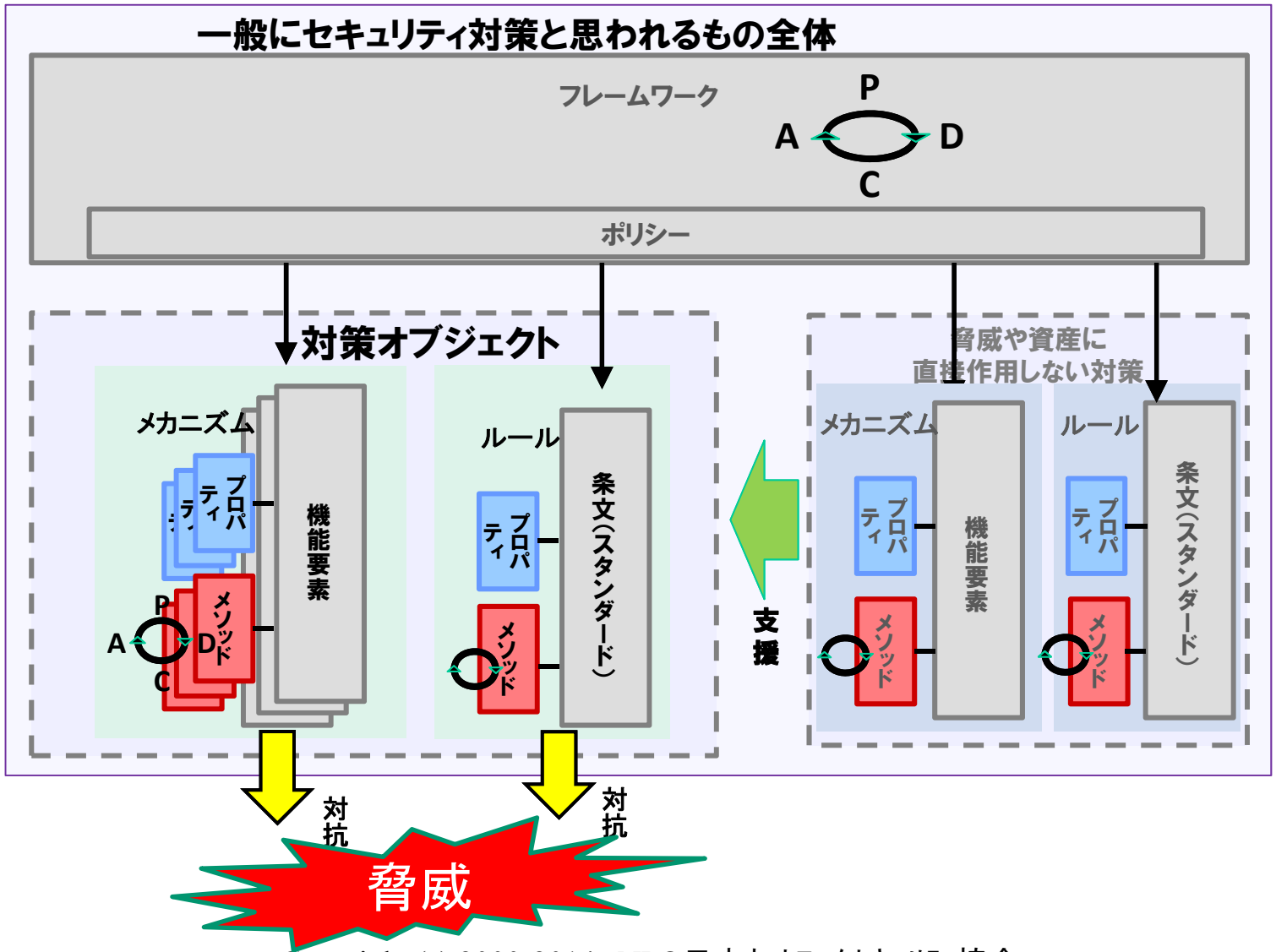
オブジェクト		「管理策」する。		
プロパティ	静的	上位ルール（方針） 要求事項 責任者 時間	目的 機能 管理者 場所	（期待する）効果 条件 利用者
	動的	リソース （実施の）手順 対象領域	責任者名 手段・技術 対象者	実施者名 コスト
メソッド	計画	検討する 計画する	コストを算定する 文書化する	方針を確立する 有効性の測定方法を決める
	準備	責任者を明確化する 機能を明確化する 導入条件を明確化する リソースを確保する 手順を確立する	利用者を明確化する 要求事項を明確化する 導入する時を明確化する 導入する 手順を文書化する	実施者を明確化する 導入場所を明確化する 手順を明確化する 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	

プロパティの構造

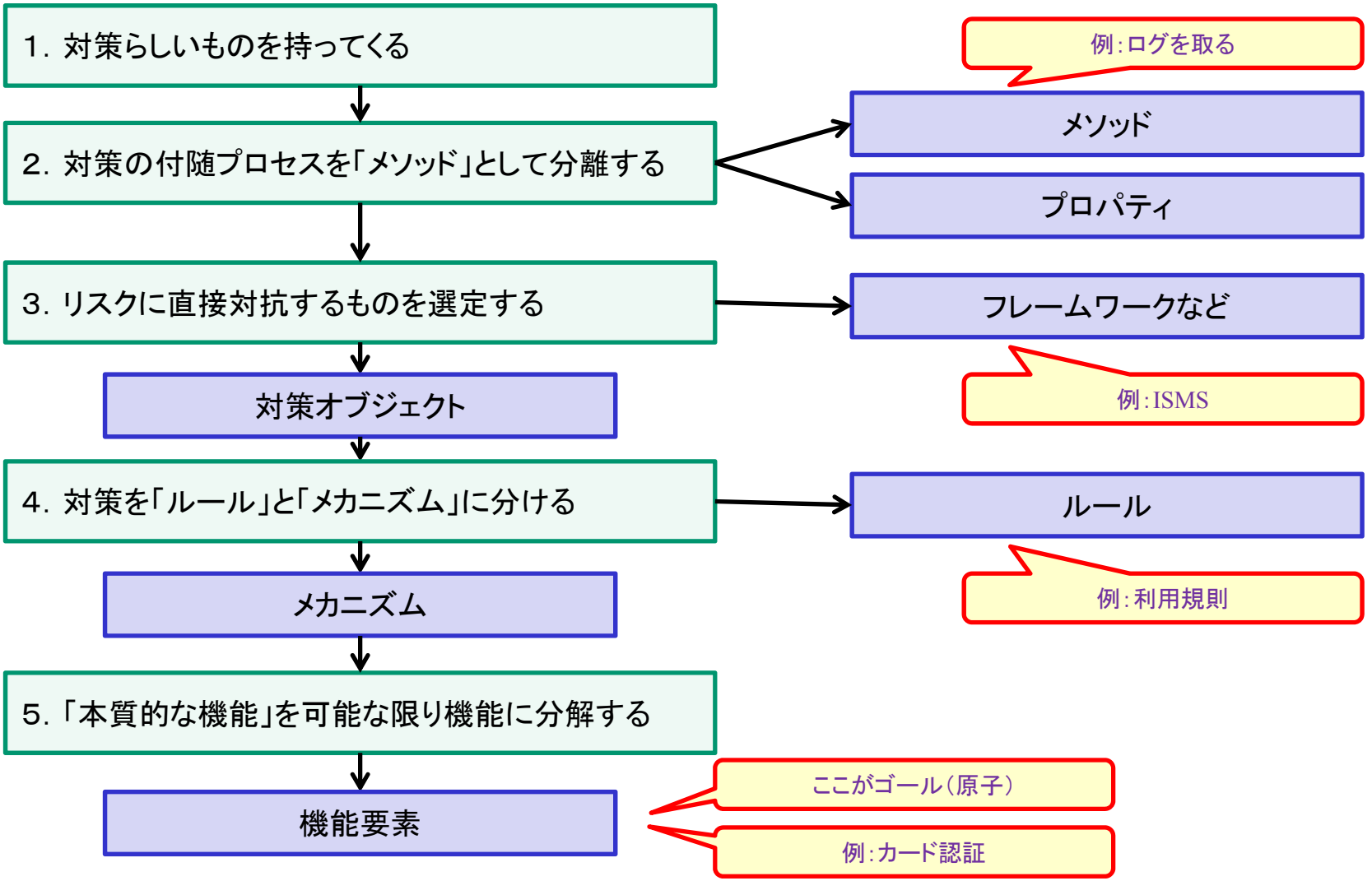


対策の原子化

セキュリティ対策の全体構造



対策の原子化



対策リポジトリの作成

標的型攻撃対策リポジトリ

2012年度セキュリティ市場調査報告書P57 http://www.jnsa.org/res	大分類	中分類	仮No.	機能	仮No.	バリエーション	機能要素表現	一般化されたオブジェクト表現	機能オブジェクト表現	製品例	備考
情報セキュリティツール	ネットワーク脅威対策製品	ファイアウォールアプライアンス	1	ファイアウォール（狭義）			ルールに基づくパケットフィルタ機能（必要な通信のみ通す、「すべてを拒否」）	[メカニズムにより]ルールに基づきパケットをフィルタリングする。	[メカニズムにより]ルールに基づきパケットをフィルタリングする。		【参考】 昨今、FWの定義として、パケットフィルタのみではなく、UTMの要素も含まれる。 http://www.hitachi-solutions.co.jp/paloalto/sp/history/history1.html
		同上	2	ステートフルインスペクション			動的パケットフィルタ機能（セッションと紐付け）	セッションと紐付けて動的にパケットをフィルタリングする。	セッションと紐付けて動的にパケットをフィルタリングする。	Cisco iMPERVA Juniper	
		同上	3	NAT機能			NAT機能	NATする。	NATする。		既出
		同上	4	データベースファイアウォール			Webサーバ、DBサーバ間において特定のルールに基づきDBMSへの通信を遮断する機能	Webサーバ、DBサーバ間において特定のルールに基づきDBMSへの通信を遮断する。	Webサーバ、DBサーバ間において特定のルールに基づきDBMSへの通信を遮断する。	Imperva SecureSphere Database Firewall Oracle Audit Vault and Database Firewall	
		VPNアプライアンス／ソフトウェア	5	VPN	1		カプセリング技術によるパケットの暗号化機能	（なし）	伝送路を暗号化する。		
		同上	5	VPN	2	SSL-VPN	SSLによる伝送路暗号化機能 [利点]IPSecより普及率が高い。様々なプロトコルにも対応。リモートアクセスだけに絞って考えると、特定のクライアントソフト等のインストールが必要なく、ファイアウォール越しでの接続性が高い為、IPsecよりも幅広い環境で利用可能。	（なし）	SSLにより伝送路を暗号化する。	IPCOM（富士通） SSLアクセラレータ（一般）	
		同上	5	VPN	3	IPSec-VPN	IPSecによる伝送路暗号化機能 [利点]ハードウェア制御なので、トネリングではSSLより早い。企業間（専用線等）の暗号化通信のみでは、SSLより優れている。	（なし）	IPSecにより伝送路を暗号化する。	IPCOM（富士通）	
		同上	5	VPN	4	PPTP-VPN	PPTPによる伝送路暗号化機能	（なし）	PPTPにより伝送路を暗号化する。	IPCOM（富士通）	ほぼWindows環境のみ
		IDS/IPSアプライアンス／ソフトウェア	6	IPS（狭義）			シグネチャあるいは挙動判断による不正／異常パケットの遮断・防御機能（パケット破棄、アラート、リセットパケット送信によるコネクション切断）	（なし）	シグネチャあるいは挙動判断により不正／異常パケットを遮断する。	IPCOM（富士通） Proventia（IBM） Juniper	
		同上	7	シグネチャ型IDS			シグネチャによる不正／異常パケットの検知機能	（なし）	シグネチャにより不正／異常パケットを検知する。	IDS/IPS製品一般	最近の傾向としては、両方の利点を活かした製品が多い。
		同上	8	アノマリ型IDS			RFCに準拠しないパケットなど不正／異常パケットの検知機能	（なし）	パケットの異常な特性・性質により不正／異常パケットを検知する。	IDS/IPS製品一般	
		同上	9	振る舞い検知型IDS			挙動判断による不正プログラムの検知機能	（なし）	挙動判断により不正プログラムを検知する。	FireEye	

セキュリティ対策マップの試作

アプローチ

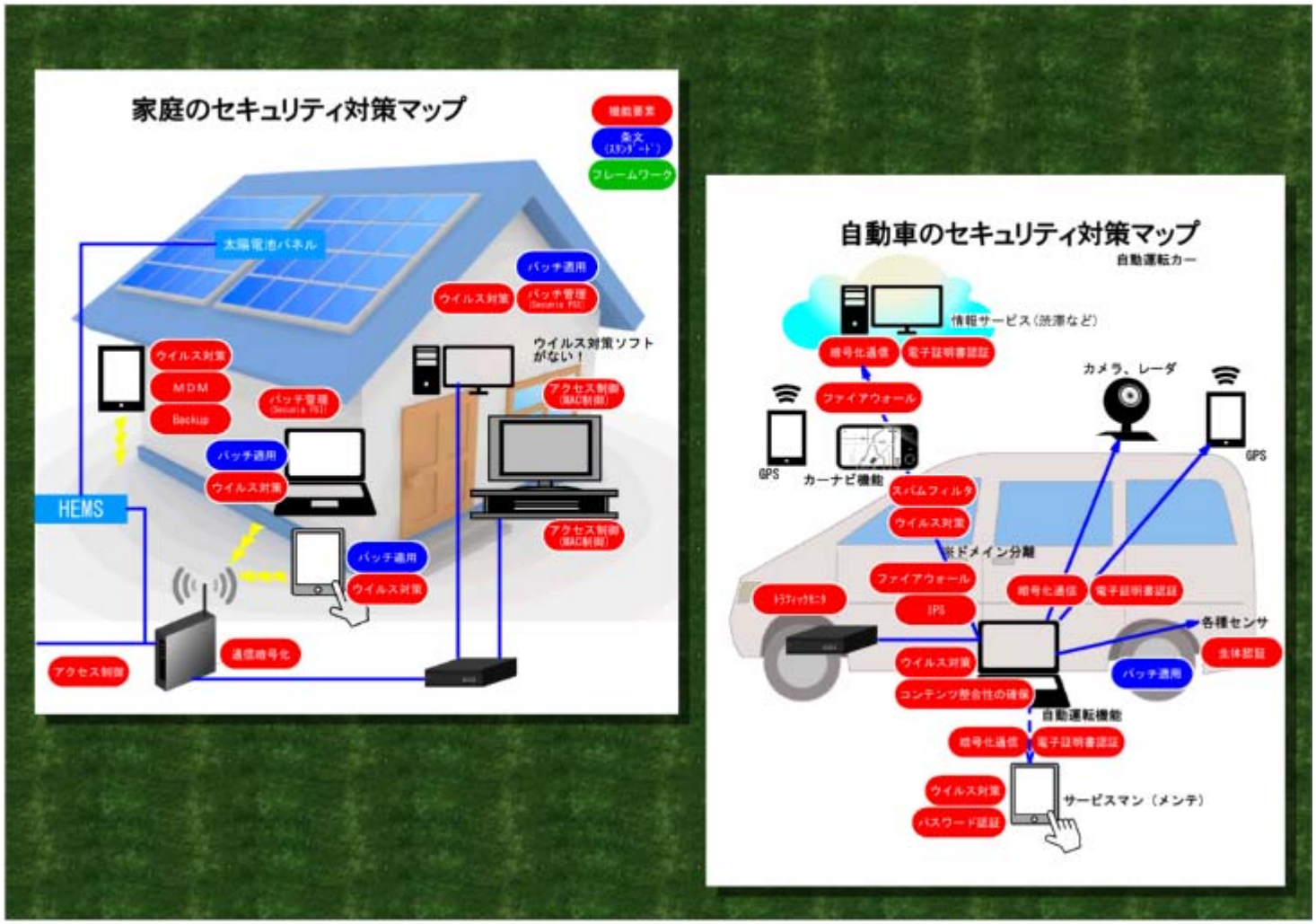
- 標的型攻撃の対策を対象領域に、小さなリポジトリを作ってみた
- そのリポジトリから、メンバーの独創性に基づいた「地図作成コンテスト」を実施
- 上位作品を地図としてブラッシュアップ

マップ作成例　その１（１）

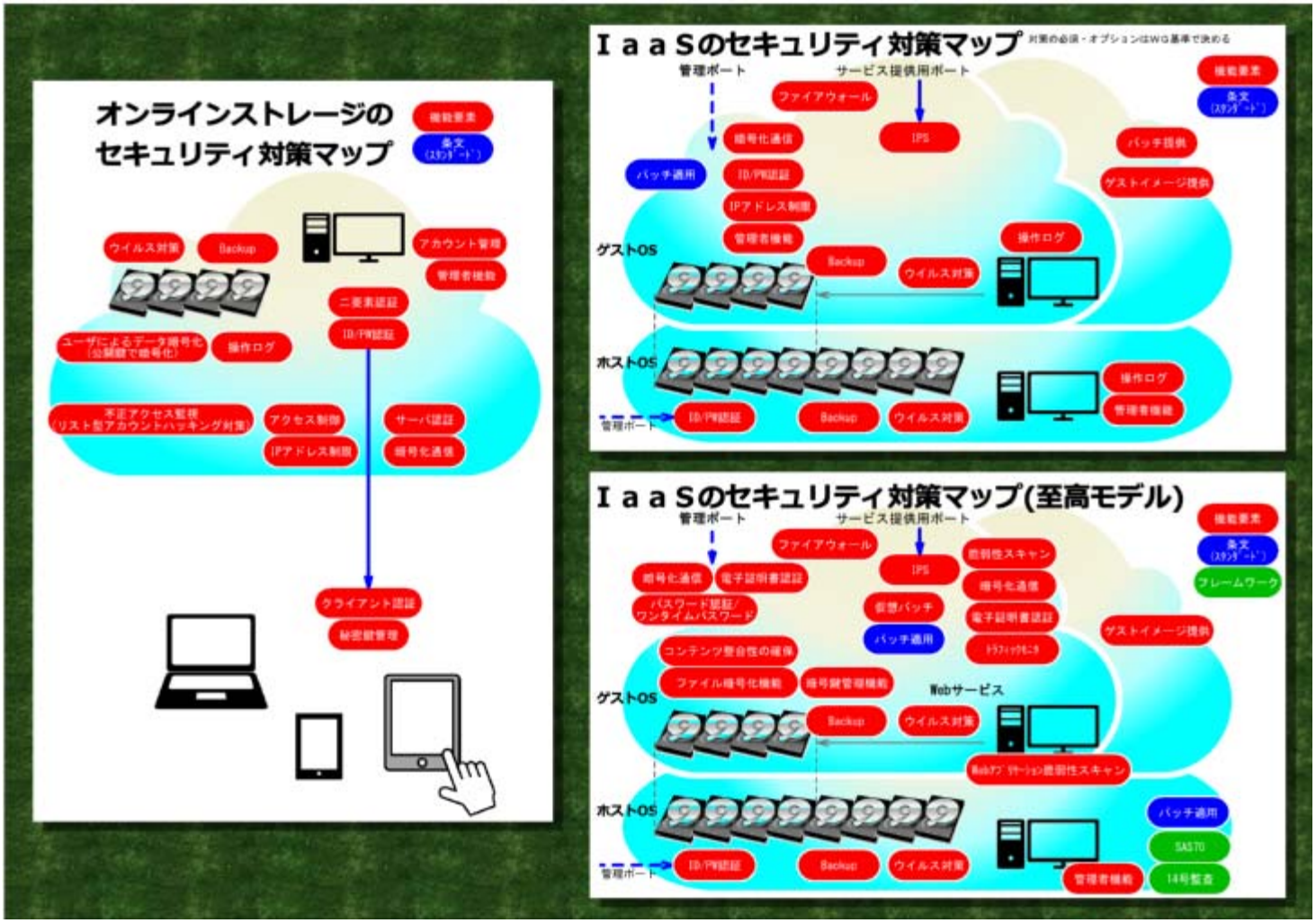
- セキュリティ対策を、それが配置される空間に配置したわかりやすい「地図」

- 家庭、自動車、オンラインストレージ、IaaSなどさまざまな「場面」で地図を描いてみた

マップ作成例　その1（1）



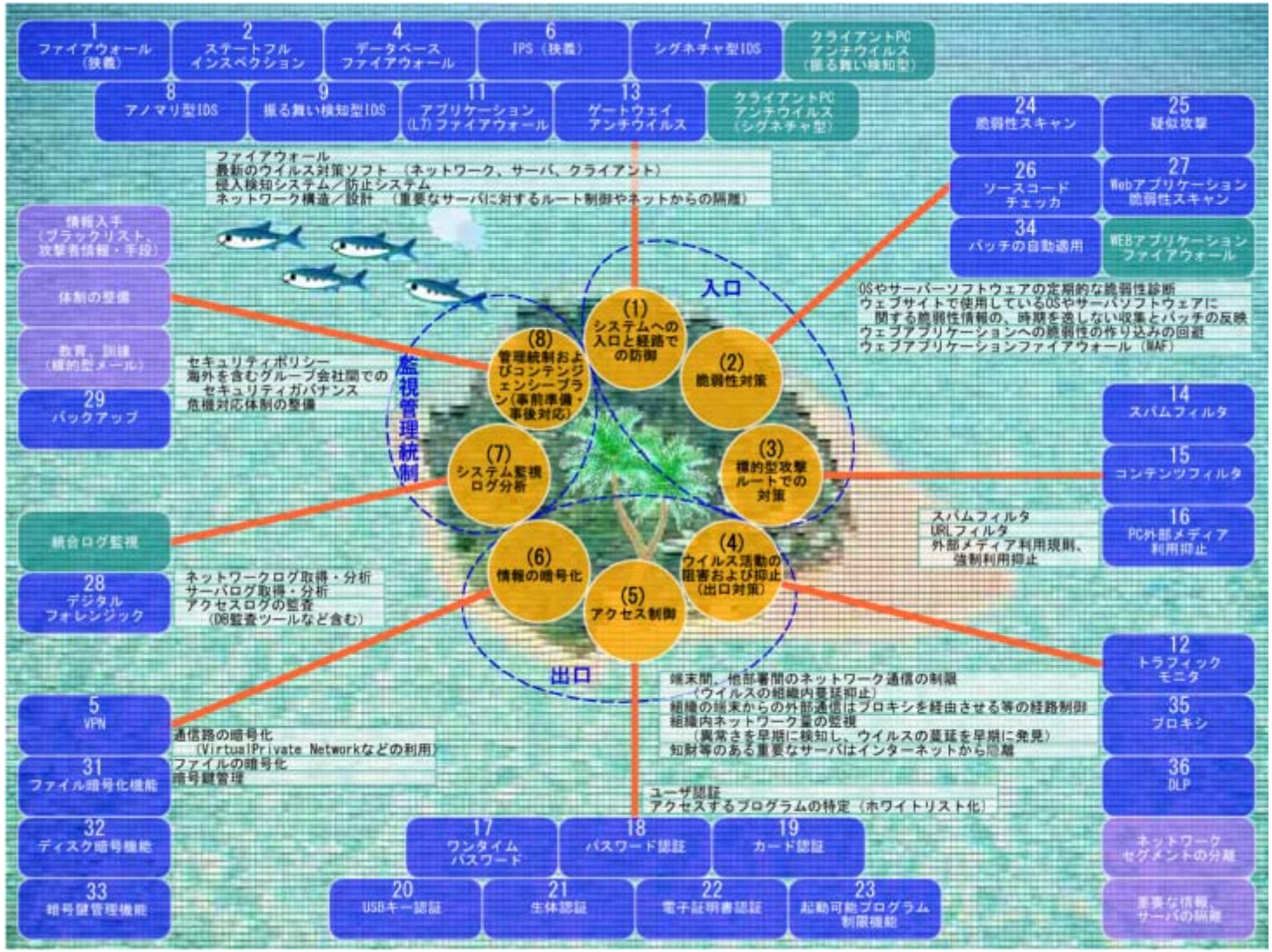
マップ作成例　その1（2）



マップ作成例　その２

- セキュリティ対策の目的を図の中心に配置し、宝がある「島」に見立ててみた
- そこからセキュリティ対策の「手段」をマインドマップのように展開し、「海」に見立てる
- 冒険心をくすぐる詩的な一枚

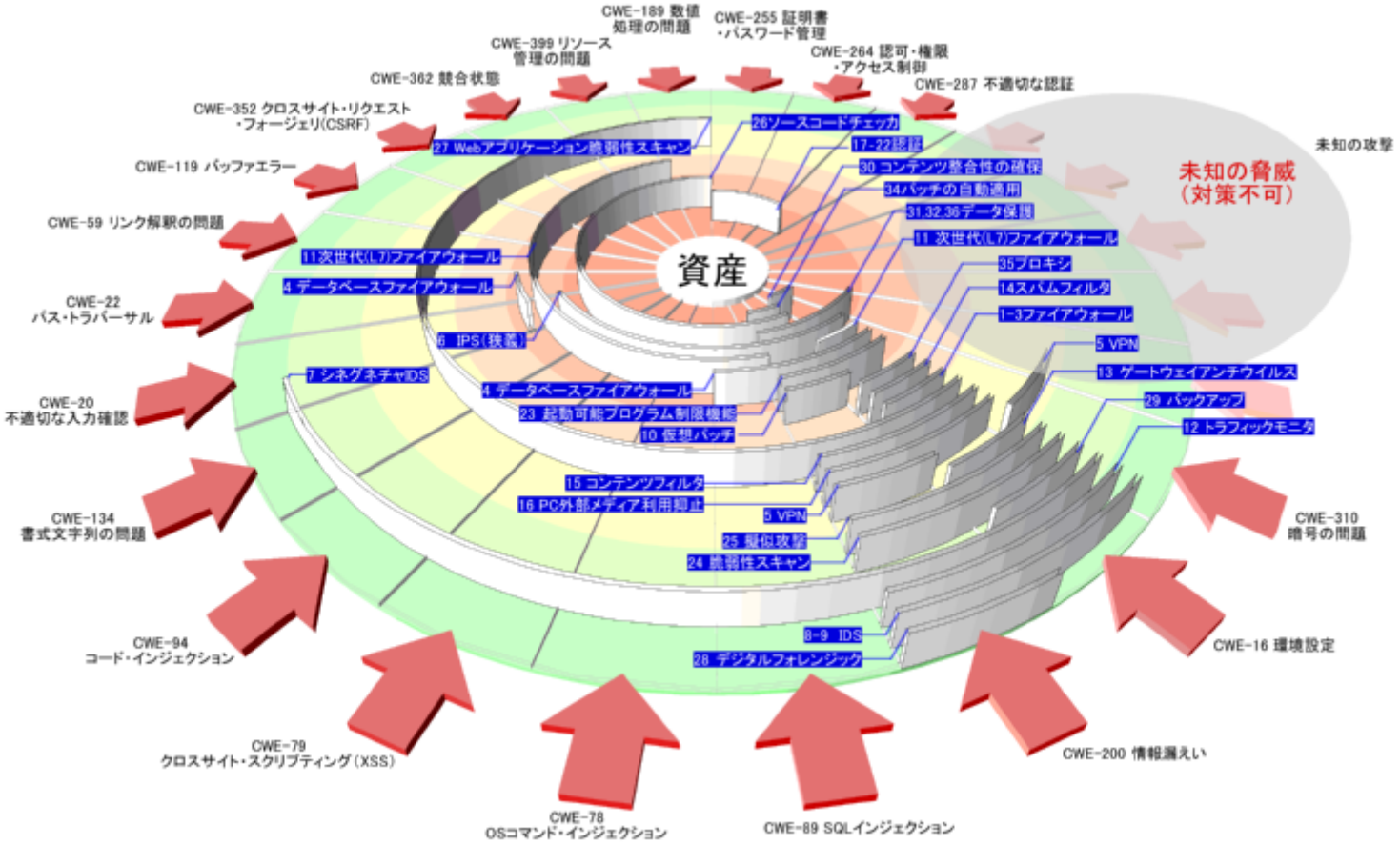
マップ作成例　その2



マップ作成例　その３

- ISOの技術文書「GMITS」の絵をリアルに描いてみた
- 真ん中に資産があり、それを対策が壁となって周りの脅威から守っている
- 壁１枚１枚が具体的な対策を示している

マップ作成例　その3



評価

評価

- 客観的に対策の最小単位を記述できる「対策オブジェクト」のモデルを提言した。
- 「対策オブジェクト」に基づいた地図の作成が可能であることを、作成例を用いて示した。

目的の達成

- 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

いずれも達成　か？

今後の課題

- すべての対策を系統的に記録した情報セキュリティ対策リポジトリの整備とライブラリ化。
- すべての対策を網羅した情報セキュリティ対策のマップ、いわば「世界地図」の完成。

そんなわけで

- 本WGは本報告を持って活動終了します。
  - ご支援、ご声援ありがとうございました。
    m(_ _)m
- 次は「情報セキュリティ対策マップ完成WG」

  か？

WGメンバー

ワーキンググループリーダー

奥原　雅之	富士通株式会社

ワーキンググループサブリーダー

長谷川　喜也	富士通株式会社

メンバー（登録順）

塚田　孝則	株式会社日立ソリューションズ
渡邊　浩一	株式会社日立ソリューションズ
田中　建次郎	ドコモ・システムズ株式会社
本川　祐治	株式会社日立システムズ
松井　康宏	日本アイ・ビー・エム株式会社
大谷　尚通	株式会社NTTデータ
藤井　裕一	富士ゼロックス株式会社
佐藤　一章	富士ゼロックス情報システム株式会社
菊地　正人	日本オラクル株式会社
戸田　勝之	NTTデータ先端技術株式会社
土屋　日路親	（サブスクライバ）
西谷　健二	株式会社インテリジェントウェイブ

（公表の許可をいただいた方のみ。載っていない方はご一報を）