2013年度
情報セキュリティ対策マップ検討WG
活動報告書

2014 年 6 月 10 日

NPO 日本ネットワークセキュリティ協会
情報セキュリティ対策マップ検討ワーキンググループ

目次

著作権・引用について

本報告書は、NPO 日本ネットワークセキュリティ協会(以下、「JNSA」とする) 情報セキュリティ対策マップ検討ワーキンググループが作成したものです。本報告書の著作権は JNSA に帰属します。本報告書は JNSA の公式サイトより公開情報として提供されます。本報告書より引用される場合は、「JNSA 2013 年度情報セキュリティ対策マップ検討ワーキンググループ成果報告書より引用」と記述してください。また、引用の範囲を越えて書籍、雑誌、セミナー資料などに利用される場合は、JNSA のホームページ上にある問い合わせフォームをご利用ください。

JNSA 情報セキュリティ対策マップ検討ワーキンググループ

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

＊このリストは報告書作成時にメーリングリストで連絡が取れた方で、かつ掲載を承諾された方のみ掲載しています。もし本 WG 活動に参加された方で掲載が漏れている方がおられましたら JNSA までご一報ください。

1 WG の概要

1.1 WG の設立趣旨

あらゆる技術がそうであるように、情報処理・通信技術（ICT）にも光と陰の二つの面がある。ICT が発達し、その可能性が拡大するとともに、それを悪用できる可能性も同様に広がっていく。その結果として、これまでに膨大な種類のセキュリティ対策技術やセキュリティ対策手法が開発され、普及してきた。これらの「セキュリティ対策」は、さまざまな目的のためにさまざまな場面でカタログ化されている。例えば ISO/IEC 27002 [1]は非常によく知られたセキュリティのガイドラインのカタログである。同様なセキュリティ対策のカタログとしては、米国 NIST の SP800-53 [2]、経済産業省の情報セキュリティ管理基準 [3]などが挙げられる。

これらのセキュリティ対策のカタログは (A)脅威またはリスクを列挙し、それに対応するセキュリティ対策を記述したもの、(B)作成者の考える分類カテゴリに従ってセキュリティ対策を分類したもの、のいずれかの構成を取ることが一般的である。これらの構造に従ったセキュリティ対策カタログはセキュリティ対策立案の参考とする目的などには十分であるが、例えばリスク分析を形式的に行おうとすると、その構造が自然言語に依存しているため、厳密な分析には不都合を生じることが多々あった。

これらのセキュリティ対策カタログでは困る状況として以下のような状況が挙げられる。

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
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
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

これらの問題を解決するためには、従来の「セキュリティ対策カタログ」ではなく、ある程度の客観性と正確性があり、セキュリティ対策の構造を明確に提示できる「情報セキュリティ対策マップ」を作成する必要があると考え、NPO 日本ネットワークセキュリティ協会の技術部会 WG として 2008 年から有志を募り、活動を開始した。

1.2 WG の目的

「情報セキュリティ対策マップ」の作成に関する以下のアウトプットを作成する。

- 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

1.3 WG の活動概要

2008 年度 2009 年度	・ 準備会開催（2008 年 12 月） ・ WG 開催（通算 1 階から 28 回まで、28 回） ・ 2008 年度活動報告会にて報告（2009 年 6 月） ・ 第 1 回定量的リスクアセスメントについて考える BoF 参加（2009 年 8 月） ・ 第 2 回定量的リスクアセスメントについて考える BoF 参加（2009 年 12 月） ・ Network Security Forum 2010 にて報告（2010 年 1 月）
2010 年度	・ WG 開催（通算 29 回から 50 回まで、22 回） ・ 2009 年度活動報告会にて報告（2010 年 6 月） ・ Network Security Forum 2011 にて報告（2011 年 1 月）
2011 年度	・ WG 開催（通算 51 回から 70 回まで、20 回） ・ 2010 年度活動報告会にて報告（2011 年 6 月） ・ Network Security Forum 2012 にて報告（2012 年 1 月） ・ 2011 年度 JNSA 賞受賞
2012 年度	・ WG 開催（通算 71 回から 93 回まで、23 回） ・ 2011 年度活動報告会にて報告（2012 年 6 月）
2013 年度	・ WG 開催（通算 94 回から） ・ 2012 年度活動報告会にて報告（2013 年 6 月） ・ 活動報告書作成

詳細は第 2 章および第 8 章を参照。

2 WG 検討の歩み

2.1 2009 年度

・プロローグ －2008 年 12 月 10 日－

その日、工学院大学における JNSA 活動拠点の 570 号室は、WG の準備会にしては多くの参加者であふれかえっていた。「情報セキュリティ対策マップ」という、このときはまだ形ないものに、みんな想い想いにイメージを膨らませ、期待と情熱持って集まった 19 名。

当初 3 年の活動予定にもかかわらず、5 年という長きにわたり苦闘を続けることになる、「情報セキュリティ対策マップ検討 WG」の華々しい船出である。

・マップ検討のスタート －情報セキュリティ対策マップを作るとは？－

「情報セキュリティ対策マップを作る」というテーマで検討を開始したものの、目標とすべき「情報セキュリティ対策マップ」というものが、どのようなものなのか、想い想いにイメージを膨らませて WG に参加した参加者の中には統一したイメージは無く、これを合わせるところから検討は始まった。

参加者がそれぞれイメージする、情報セキュリティ対策マップに求めるイメージを集めたところ、世の中のベンダーが提供しているソリューションを全て集めた「スーパーソリューションマップ」のようなものや、情報セキュリティ対策として採用している企業が多いほど高くなるような「山岳地図モデル」、刻々と移り変わる世の中の情報セキュリティの状況を天気予報のように表現する「天気予報モデル」など多くのイメージが集まった。

このようにして集まったイメージを整理していく中で、「情報セキュリティ対策マップ」は、やはり「マップ」なので情報セキュリティ対策と「何か」をマッピングするものであるということ、この情報セキュリティ対策とマッピングする「何か」がわかれば情報セキュリティ対策マップの方向性も見えてくるのではないかということ、がわかってきた。そこで、私たちの検討は情報セキュリティ対策とマッピングする「何か」を見つけるという次のフェーズに入った。

情報セキュリティ対策とマッピングする「何か」の候補は、「脅威」や「リスク」、「対策を実施する場所」や「対策を実施する目的」、「対策を実施するレイヤ」など、数多く見つかった。また、「経営者」や「管理者」の「うれしさ・安心感の度合い」など、斬新な意見もあった。

しかし、これらの中に絶対的にこれ、という候補は無いこと、そしてそれは情報セキュリティ対策マップを使う人やその目的によって「何か」が異なるからだということがわかった。これは実際の地図が、世界地図や日本地図、道路地図や路線図など、使う人の目的によって、縮尺やそこに記載されているものが変わっていくのに似ている。実際の地図は、例えば合コンのお店を仲間に知らせるときに簡単に描いて送るように、使う人が必要に応じて簡単に作成する事ができ、また、受け取った相手もそれを読み取ることができる。これは地図を作る手法が統一されていて、さらにそれがみんなに共有されているからであり、普段地図を使

っている上では気にすることは無いが、実はすごいことである。

ここまできて、私たちが目指す「情報セキュリティ対策マップを作る」という作業は、既存の手法を使ってある特定の一つの情報セキュリティ対策マップを作る事ではなく、「情報セキュリティ対策マップを描くための統一した手法を確立すること」なのだ、ということがわかってきた。

・マップ素材の持ち寄りと整理（昆虫採集アプローチ） －フィールドに出てみよう－

「新しい手法を確立する」ためには、今ある情報セキュリティ対策がどのようなものなのかを知らなければならない。

そこで、私たちは既存の情報セキュリティ対策を広く集めることにした。この作業が、あたかも昆虫学者がフィールドに出て、昆虫を採取して分類していく作業に似ているということで、私たちはこの作業を昆虫採集と呼ぶことにした。昆虫学者が行き当たりばったりで適当に昆虫を採取するのではなく、採取するエリアを決め、採取する種を決めて行うように、情報セキュリティ対策を採集するエリアと種類を決めることにした。採集するエリアの候補としてあがったのは、以下のような物である。

- ISO/IEC 27001
- ISO/IEC 27002
- 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

私たちはこの中で、「JIS Q 27002（ISO/IEC 27002）」、「NIST SP800-53」、「FISC」の三つを採集エリアとして選択した。また、採集する種類は、だれもがイメージしやすい「マルウェア対策」とすることにした。

「JIS Q 27002（ISO/IEC 27002）」、「NIST SP800-53」、「FISC」から「マルウェア対策」を抽出してくる作業は簡単なように思えた。しかし、これは実際には一筋縄で行くものでは無かった。

例えば、「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、検出するために予防対策が必要となる。」という情報セキュリティ対策がある。一見、一つながりの文書であるため、一つの情報セキュリティ対策の様にも思えるが、見方によっては「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するために予防対策が必要となる」と「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検出するために予防対策が必要となる」の二つの情報セキュリティ対策であるようにも思える。

私たちはこれを「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するために予防対策が必要となる」と「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検出するために予防対策が必要となる」の二つに分けて採集することにした。

この結果、この三つのフィールドだけであっという間に 133 個を超える情報セキュリティ対策が採集できた。以下に採取した情報セキュリティ対策の抜粋を示す。

表 1 採集されたセキュリティ対策(部分)

No.	出典	要件	分類
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	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》
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》
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》
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》
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》
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》
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》
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》
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》
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》
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》

・「対策構造」の提言　―情報セキュリティ対策間には構造がある？―

採集した情報セキュリティ対策を眺めてみると、「コンピュータウイルス対策を講ずること」のように抽象的なものや「悪意のあるコードに対する検知・修復ソフトウェアを導入する」のようにより具体的・直接的なもの、「保護策の利用方法に関する訓練に関する管理の手順の明確化」のように間接的なものなどいくつかのグループに分けられることがわかる。

これらのお互いの関係を整理していくと、情報セキュリティ対策の間には一つの構造があることが見えてきた。これを図示する案が「対策構造図」である(図 1)。

一般的にこのような図は、「マネジメント」のような物を上位概念として図の上の方に描き、実装に近い「メカニズム」のような物を下位概念として図の下の方に描く事が多い。

私たちも当初そのような構造図を模索していた。しかし、情報セキュリティ対策の関係をよくみてみると、情報セキュリティ対策には上位下位という関係ではなく、リスクから遠いか近いかという関係があることがわかってきた。そこで、向かって右側にいる敵(リスク)に対して前線で直接的に対策する「直接コントロール」、その後方で支援する「コントロールの支援」、さらにその後方で指示をする「マネジメント」という図 1のような横展開をする図が出来上がったのである。

この「対策構造図」の案であるが、2011 年度の JNSA 成果報告会で発表以降、今日まで各方方面で根強い評価をいただいている、当WG初期における代表的な成果の一つで

ある。

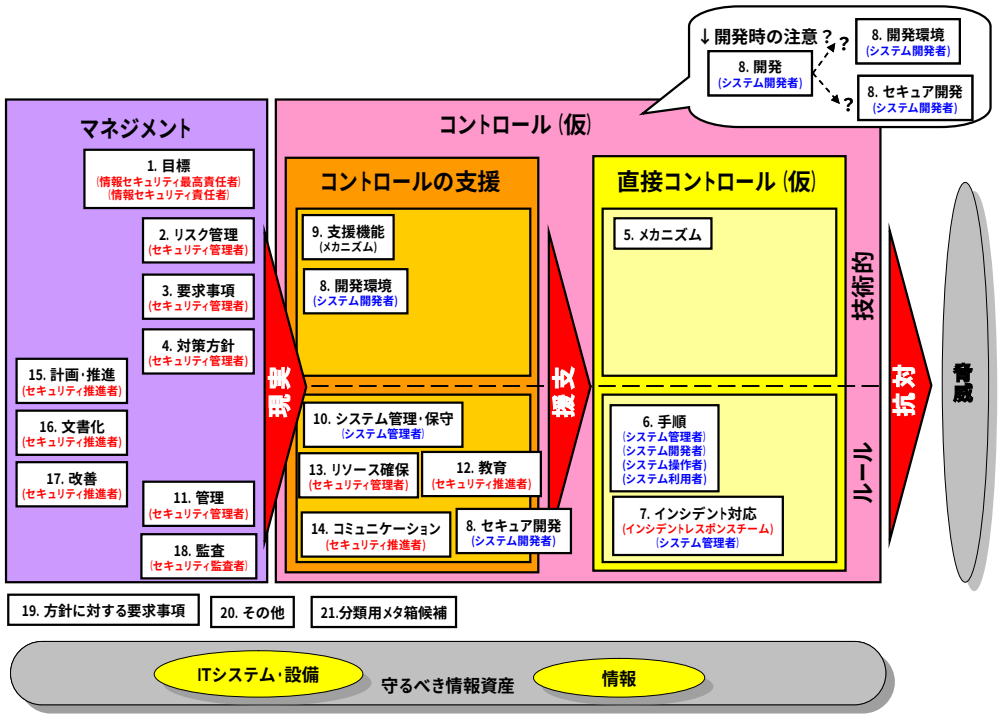


図 1 対策構造図

・「標準構文」と「標準辞書」の提言

さて、採取してきた情報セキュリティ対策を整理・分類する過程で、私たちは最初の大きな壁に突き当たった。それは、「二つの情報セキュリティ対策は同じなものなのか、それとも違うものなのか」という問題である。

例えば、次の二つの情報セキュリティ対策は同じ物だろうか？

・情報セキュリティ対策1：

ファイルをスキャンし、既知のウイルスがないかを調べる。ファイルシステムの感染を特定できるように、すべてのハードディスクドライブを定期的にスキャンするよう、また任意で、ほかのストレージメディアについても同様にスキャンするようにウイルス対策ソフトウェアを設定する。

・情報セキュリティ対策2：

悪意のあるソフトウェアの影響を受けやすいすべてのオペレーティングシステムタイプを含む、システムコンポーネントのサンプルについて、定期スキャンが有効になっていることを確認する。

情報セキュリティ対策間の関係を整理していくためには、昆虫採集で集めてきた沢山の情報セキュリティ対策に対して、同じものなのか、異なるのか、異なるとしたら、どこがどのように異なるのか、そして異なるのであればそれらの情報セキュリティ対策間の関係はどのようなものであるか、これらを評価していかなければならない。

さらに、私たちが目指しているのは、「情報セキュリティ対策マップを描くための統一した手法を確立すること」、すなわち誰が行っても二つの情報セキュリティ対策間の関係を正しく評価できるようにしなければならない。

しかし、採集してきた情報セキュリティ対策の書き方は、集めてきた元のガイドラインによって様々であり、また、同じガイドラインの中でさえ統一されていない物もある。いったい何を統一したら評価が可能になるのであろうか。ここで私たちは「用語」と「文の構造」の二点に注目をした。

まずは、用語の統一である。

「マルウェア」、「ウイルス」、「悪意のあるソフトウェア」、「不正プログラム」、「ワーム」、「スパイウェア」そして「悪意のコード」。情報セキュリティ対策の中に出てくるこれらの用語は同じ物を表しているのであろうか？それとも異なる物を表しているのであろうか？もし、同じ物を表しているのであれば、「マルウェアに感染しないために○○対策をする」という情報セキュリティ対策と、「ウイルスに感染しないように○○対策をする」という情報セキュリティ対策は同じ物だということができる。また、もし、違う物を表すのであれば「マルウェア」と「ウイルス」の関係がそのままこの二つの情報セキュリティ対策間の関係になる。

きちんと使い分けている人もいるが、多くの場合、普段はあまり意識して使い分けていないこれらのような用語を厳密に整理してみると、「マルウェア」と「悪意のあるソフトウェア」のように、意味が同じでそのまま置き換えることができる同義語の関係にあるものと、「マルウェア」の中で特に意図的に何らかの被害を及ぼすように作られたものを「ウイルス」と呼ぶように包含関係にあるものがあることがわかる。また、「ウイルス」と「ワーム」、「スパイウェア」のように、お互いに「マルウェア」に含まれながら、それぞれが並立の関係にあるものもある。こうした関係を一覧表として整理したものを私たちは「標準辞書」呼ぶことにした（図 2）。

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

図 2 標準辞書（抜粋）

「標準辞書」では、同義語の関係にある物の中からもっとも一般的に使われていると思われる語を「標準用語」として選び出す。そして情報セキュリティ対策を比較する時には、まず

「標準用語」に置き換えることが出来るものは、置き換えてから評価を行う事とした。

次に、文の構造の整理である。

上記の「情報セキュリティ対策1」の「既知のウイルスがないかを調べる」と「ファイルシステムの感染を特定できるように」の部分は、この情報セキュリティ対策全体の中で「目的」を表していると見ることができる。また、「すべてのハードディスクドライブ」と「ストレージメディア」は共にこの情報セキュリティ対策を実施する「場所」を表していると見ることができる。一方、「情報セキュリティ対策2」の「システムコンポーネント」の部分はやはり、この情報セキュリティ対策を実施する「場所」を表していると見ることができる。

この二つの情報セキュリティ対策から、これらの枝葉を取り除くと、中心となる「定期的にスキャンする」という部分だけが残る。この結果、この二つの「情報セキュリティ対策1」と「情報セキュリティ対策2」は同じ対策であると言うことができるようになる。

この例のように、情報セキュリティ対策の文の構造を見ていくと、その中心となる部分は「何かを」「どうする」という単純な構文になることがわかる。これ以外の「誰が」や「何のために」「何を使って」などは要求事項の具体化や詳細化の要素として扱うことができ、また、情報セキュリティ対策の強度を要求するために、文の最後に付けられる「～を確実にする」などの表現上の語句は、切り捨ててしまっても情報セキュリティ対策としては影響が無いことがわかる。これらを整理すると以下のようになる（図 3）。

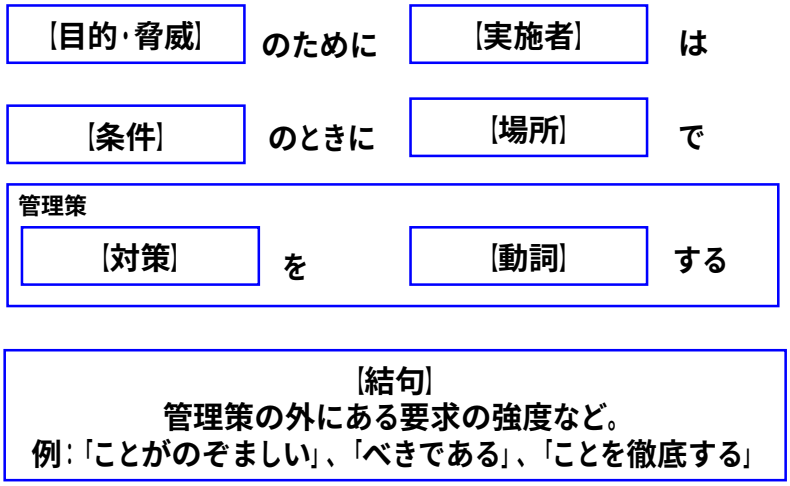


図 3 標準構文

私たちはこれを「標準構文」と呼ぶことにした。世の中の全ての情報セキュリティ対策をこの「標準構文」で表すことができれば、情報セキュリティ対策間の関係を容易に評価する事ができるようになり、さらに、全ての情報セキュリティ対策を表すことができる「標準構文」は、「情報セキュリティ対策マップを描くための統一した手法」になるとも考えている。

2.2 2010 年度

・「マルウェア分県図」の試作

2010 年度の WG は、「標準構文」と「標準辞書」を使ってみる事から始まった。

昆虫採集で集めた、マルウェアに関する情報セキュリティ対策の中で、複数のガイドラインに記載があった対策について「標準構文」の検証と、「標準辞書」の試作を行ってみた。

「標準構文」は、対策の幹となる「何かを」「どうする」を中心に、「誰が」や「何のために」「何を使って」などの枝葉となる修飾節を【○○のリスト:{リスト項目1}{リスト項目2}】のような書き方で変数として添えていく。以下は、「ウイルス対策ソフトウェアを正しく設定して、定期的にスキャンする。」という幹に、「目的のリスト」と「場所のリスト」という枝葉がついた例である。

ID	MAL.6
名称	定期的スキャン
情報セキュリティ対策	【目的のリスト:{既知のウイルスがないかを調べるために}{ファイルシステムの感染を特定できるように}】【場所のリスト:{すべてのハードディスクドライブ}{ストレージメディア}{システムコンポーネント(悪意のあるソフトウェアの影響を受けやすいすべてのオペレーティングシステムタイプを含む)}】ウイルス対策ソフトウェアを正しく設定して、定期的にスキャンする。

私たちはこうして作成した「標準構文」で記述されたマルウェア対策を使って、「マルウェア県」の地図作りを行った。これは、情報セキュリティ対策全体を日本地図に見立て、そして対策の大分類を一つの県に見立てた地図作成の第一歩である。以下に作成中当時の「マルウェア県」の地図を示す。

表 2 マルウェア分県図

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}】。
MAL.6	定期的スキャン	04.《対策方針》	【目的のリスト:{既知のウイルスがないかを調べるために}{ファイルシステムの感染を特定できるように}】【場所のリスト:{すべてのハードディスクドライブ}{ストレージメディア}{システムコンポーネント(悪意のあるソフトウェアの影響を受けやすいすべてのオペレーティングシステムタイプを含む)}】ウイルス対策ソフトウェアを正しく設定して、定期的にスキャンする。
MAL.7	電子メールのスキャン	05.《メカニズム》	組織は電子メールの送受信のたびに【場所のリスト:{電子メールサーバ}{電子メールクライアント}】ですべての電子メールの添付ファイルをスキャンし、疑わしい電子メールの添付ファイルを特定し、【処理のリスト{電子メールから添付ファイルを削除}、{電子メールそのものをブロック}】する。
MAL.8	取り外し可能な記憶媒体のスキャン	05.《メカニズム》	組織は取り外し可能な【記録媒体のリスト:{電子的媒体}{光学的媒体}】上のファイルに対する、マルウェア検出のための使用前スキャンをする。
MAL.9	ネットワーク使用時のスキャン	05.《メカニズム》	ユーザがファイルを【行為のリスト:{ダウンロードする}{ネットワーク経由で入手する}{開く}{実行する}】ときに、【場所のリスト:{*}】でマルウェア検出のための使用前スキャンをする。
MAL.10	ウェブページ閲覧時のスキャン	05.《メカニズム》	組織は、【ユーザアクセスのリスト:{インターネットアクセス}{ウェブページへのアクセス}】のときにマルウェア検出のための【対策のリスト:{スキャン}{コンテンツフィルタリング}】をする。
MAL.11	マルウェアに対する意識向上	12.《教育》	マルウェアから保護するために組織内部のすべてのユーザに、【意識させることのリスト:{マルウェアの侵入、感染、および拡散の方法}、{マルウェアがもたらすリスク}、{技術的管理策ではすべてのインシデントは防げないこと}、{インシデントを防ぐうえでユーザが重要な役割を果たすこと}】を意識させる。
MAL.12	マルウェアに対する意識向上の手順	06.《手順》	マルウェアから保護するために【MAL.11】のための手順を実施する。
MAL.13	脆弱性情報の入手	14.《コミュニケーション》	【入手する情報のリスト:{Os 等のセキュリティホール}、{Web アプリケーションの脆弱性}】に関する最新情報を入手する。
MAL.14	脆弱性情報の入手手順	06.《手順》	【MAL.13】のための手順を実施する。
MAL.15	脆弱性情報の入手プロセス	15.《計画・推進》	【MAL.13】のプロセスを確立する。
MAL.16	マルウェア侵入の検知	03.《要求事項》	マルウェアから保護するために、組織はマルウェアが侵入した場合には組織全体で【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}、{そのほかの一般的な手段}】または【手段のリスト:{情報システムの脆弱性}】で送り込まれたマルウェアを検知する。
MAL.17	マルウェア感染時の対策	03.《要求事項》	マルウェアの拡散の阻止と、システムのさらなる被害の防止のためマルウェアに感染した場合、【発見後の対策のリスト:{被害の拡大防止}、{マルウェアの拡散防止}、{システムの復旧}、{再発の防止のための事後対策}】を行う
MAL.18	システムへのアクセス管理	03.《要求事項》	システムへの適切なアクセスを実現する【アクセス管理策のリスト:{ファイルに対するアクセス制限機能}、{本人確認機能}、{ID の不正使用防止機能}】を導入する
MAL.19	マルウェアの根絶	03.《要求事項》	組織は【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}、{そのほかの一般的な手段}】または【手段のリスト:{情報システムの脆弱性}】でマルウェアが送り込まれ感染したときに【根絶作業のリスト:{感染しているシステムからマルウェアを駆除する}、{原因となった弱点を除去または軽減する}】を行いマルウェアを根絶する。
MAL.20	復旧のための事前対策	03.《要求事項》	マルウェアに感染した場合に備えるため速やかな復旧・回復が行えるように事前の対策を行う。
MAL.21	バックアップの取得	10.《システム管理・保守》	マルウェアに感染した場合に備えるためプログラムやデータのバックアップを取得する
MAL.22	バックアップの手順	06.《手順》	マルウェアに感染した場合に備えるため【MAL.21】の手順を策定する。
MAL.23	バックアップの保護	10.《システム管理・保守》	バックアップを保護するためにプログラムのオリジナルファイルにはライトプロテクトを施して保管する。
MAL.24	変更管理	10.《システム管理・保守》	マルウェアから保護するためにシステムの変更管理を行う。

・「対策オブジェクト」概念の導入

採集した 24 項目の中で、対策と、その対策の手順を確立する、という内容の項目が対となって出てくるのは、「MAL.11 マルウェアに対する意識向上」と「MAL.12 マルウェアに対する意識向上の手順(を確立する)」、「MAL.13 脆弱性情報の入手」と「MAL.14 脆弱性情報の入手の手順(を確立する)」、「MAL.21 バックアップの取得」と「MAL.22 バックアップの(取得の)手順(を確立する)」の三つだけであるが、その他の、例えば「MAL.2 マルウェアの検知」に対して「マルウェアの検知の手順を確立する」という対策は昆虫採集で採集されていないだけで、実際には存在する。また、この対策に意味があるのか問われると微妙ではあるが、「MAL.12 マルウェアに対する意識向上の手順(を確立する)」に対して「マルウェアに対する意識向上の手順を確立する方法の手順を確立する」というのも考えられる。すなわち、採集した24項目全てに「～(の)手順(を確立する)」という項目を追加することが出来そうなのである。

これは、～(の)手順(を確立する)」だけではない。「～の教育を実施する」を付加した項目も追加できるし、「～の導入をする」や「～の(手順の)文書化をする」、「～の保守をする」というものを付加した項目も追加出来そうである。

このように見ていくと、「～の対策をする」の語尾(述部)を少し変化させるだけで、「対策構造図」に出てくる 21 種類の分類全てに対する項目が、自動的に生成できそうである。単

純に計算をするとこれだけで 504 項目の対策のツリー図を書く必要がでてくる。

一方、ツリー図を作成する時のノードとして使用している各対策の名称は、「標準構文」の「何かを」「どうする」の「幹の部分」を取り出した物である。「標準構文」にはこの他に「枝葉の部分」である、「目的・脅威」や「実施者」、「条件」、「場所」といったパラメータが存在する。例えば、「～の教育を実施する」という対策も、管理者に対して実施する場合と、一般社員に対して実施する場合では、その内容や方法が一般的には異なるように、実施する「目的」ごとに対策が付加される。同様に「脅威」によっても「実施者」、「条件」、「場所」によっても、それぞれのパラメータに応じた対策が追加されていく。

こう考えていくと、対策の関係を整理しなければならない個数が爆発的に増えていくことになる。私たちは途方に暮れることになった。

ここで私たちは「情報セキュリティ対策マップ」には何を書くべきなのか、を検討することになった。すなわち、今まで漠然と捉えてきた、何を「情報セキュリティ対策」として扱うのか、についてきちんと定義をする事に迫られたのである。

議論の結果、「情報セキュリティ対策マップ」に書くべき「情報セキュリティ対策」は、『リスクの大きさを直接修正する手段、一般的には「対策構造図」の「メカニズム」または「ルール」に属する物』と定義する事とした。

ただし、これにより、上記の定義から外れる多くの「情報セキュリティ対策」達はどう扱っていけばよいのだろうか、という課題が発生する。

これを解決するために、「標準構文」の「枝葉の部分」をプロパティに、「語尾の変化（＝対策によく出現する述語）」をメソッドにしたオブジェクト指向を導入したモデルを考えてみた（図 4）。このモデルの導入により、「標準構文」の「幹の部分」を「対策構造図」の中の「メカニズム」または「ルール」の表現であらわしたオブジェクト名の下に、「標準構文」の「枝葉の部分」により追加される対策や、「語尾の変化」によって追加される対策をたたみ込むことが出来るようになる。

さて、たたみ込んだ対策の取り扱いであるが、これは細かい対策まで表現する必要がある場合などに必要に応じて展開をする。これは実際の地図が縮尺を大きくしていくと建物などの位置関係は変わらずに、細かいところまで見えるようになるのと同じ考え方である。

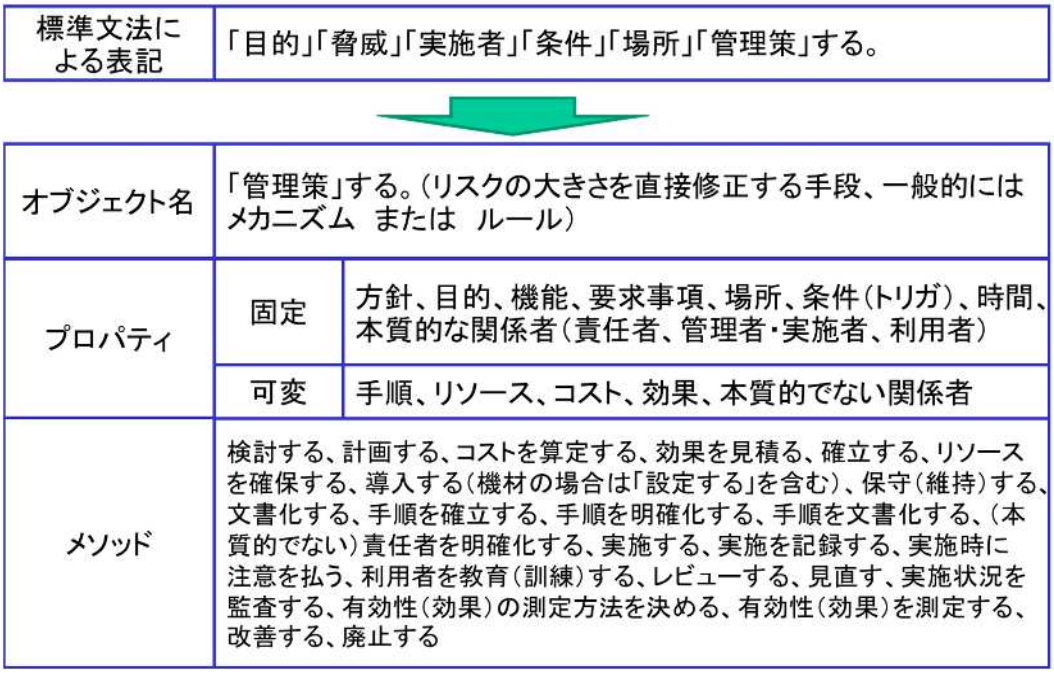


図 4 対策オブジェクトモデル

「マルウェア対策」を「対策オブジェクトモデル」で書き直した。その結果、「MAL.14 脆弱性情報の入手手順」は、「MAL.13 脆弱性情報の入手」にたたみ込まれることとなった。また、「マルウェア対策」を追加採集し、全部で 44 項目とした(表 3)。

表 3 「対策オブジェクトモデル」で書き直したマルウェア対策一覧

ID	正式表現	簡易表現
0	マルウェアに対する【対策{*}】を実施する。	マルウェアに対する【対策】の実施
1	マルウェアの被害発生のリスクを包括的に軽減するための【対策】を実施する。	マルウェアの被害発生のリスクを包括的に軽減するための【対策】の実施
2	【色々な場面において:{ファイルやソフトウェアを入手するとき}、{*}】マルウェアの被害発生を防止する【対策】を実施する。	【色々な場面において】マルウェアの被害発生を防止する【対策】の実施
3	マルウェアの被害拡大を防止する【対策】を実施する。	マルウェアの被害拡大を防止する【対策】の実施
4	マルウェアの被害からの回復のための【対策】を実施する。	マルウェアの被害からの回復のための【対策】の実施
5	【感染時の経済的損害の補償:{保険}】を適用する。	【感染時の経済的損害の補償】
6	再発の防止のための事後対策を行う。	再発の防止のための事後対策
7	マルウェアが侵入しにくくする。	マルウェアの侵入の防止
8	脆弱性をなくす。	脆弱性の除去
9	マルウェアの拡散防止を行う。	マルウェアの拡散防止
10	【ツール:{マルウェア対策メカニズム}】を利用して、【媒介物:{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}、	【ツール】を利用して、【媒介物】を介して送り込まれた【マルウェア】の検知

	{スパイウェア}、{その他の不正プログラム}】を検知する。	
11	速やかな復旧・回復が行えるように事前の対策を行う。	速やかな復旧・回復が行えるような事前の対策
12	【根絶作業：{感染しているシステムからマルウェアを駆除する}、{原因となった弱点を除去または軽減する}】を行いマルウェアを根絶する。	駆除によるマルウェアの根絶
13	【入手経路：{外部ネットワーク}、{＊}】から入手した許可されない【資産：{ソフトウェア}、{ファイル}】の使用を禁止する。	【入手経路】から入手した許可されない【資産】の使用禁止
14	組織内部のすべてのユーザに、【意識すべきこと：{マルウェアの侵入、感染、および拡散の方法}、{マルウェアがもたらすリスク}、{技術的管理策ではすべてのインシデントは防げないこと}、{インシデントを防ぐうえでユーザが重要な役割を果たすこと}】を意識させる。	組織内部のすべてのユーザに、【意識すべきこと】を意識させること
15	事態収束後にマルウェアの感染について報告する。	事態収束後にマルウェアの感染についての報告
16	再発防止のため、【振り返りの会議：{反省会}、{レビュー}、{その他の取り組み}】を開催する。	再発防止のための【振り返りの会議】の開催
17	ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】をする。	15B:ウェブ閲覧時にマルウェア感染防止のための【フィルタリング対策】
18	【侵入防止】のため、ウイルス対策ソフトウェアを導入する	【侵入防止】のためのウイルス対策ソフトウェアの導入
19	【各種アプリケーション：{メーラー}、{ブラウザ}、{ビジネスソフト}、{＊}】のセキュリティ設定を適切に行う。	【各種アプリケーション】の適切なセキュリティ設定
20	ホストの【強化措置：{ハードニング}、{セキュリティ機能強化}】を行う。	ホストの【強化措置】
21	【情報：{Os 等のセキュリティホール}、{Web アプリケーションの脆弱性}、{マルウェアに対する情報}】に関する最新情報を入手する。	【情報】に関する最新情報の入手
22	正しい情報とデマ情報を識別する	正しい情報とデマ情報の識別
23	【色々な対象：{Web アプリケーション}、{ネットワーク}、{サーバ}】の脆弱性診断を実施する。	【色々な対象】の脆弱性診断の実施
24	【色々な対象：{Web アプリケーション}、{ネットワーク}、{サーバ}】の脆弱性を【適切に対処：{除去}、{セキュリティパッチの適用}、{軽減}】する。	【色々な対象】の脆弱性の【適切な対処】
25	システムへの適切なアクセスを実現する【アクセス管理策：{ファイルに対するアクセス制限機能}、{本人確認機能}、{ID の不正使用防止機能}】を導入する	システムへの適切なアクセスを実現する【アクセス管理策】の導入
26	マルウェアの感染後に報告する。	マルウェアの感染報告
27	【導入目的：{マルウェアの侵入の防止}、{スパイウェアの検出}、{スパイウェアの駆除}】のため、ウイルス対策ソフトウェアを導入する	【検出】のためのウイルス対策ソフトウェアの導入
28	ウイルス対策ソフトウェアを正しく設定する。	ウイルス対策ソフトウェアの正しい設定
29	ウイルス対策ソフトウェアでスキャンする。	ウイルス対策ソフトウェアによるスキャン
30	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。	複数ベンダーが提供するウイルス対策ソフトの利用
31	定義ファイルおよびスキャンエンジンを【最新に保つ：{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}、{最新に保つための管理サーバを置く}】。	ウイルス対策ソフトの定義ファイルおよびスキャンエンジンを【最新に保つ】こと

32	プログラムやデータのバックアップを取得する	プログラムやデータのバックアップの取得
33	プログラムのオリジナルファイルにはライトプロテクトを施して保管する。	プログラムのオリジナルファイルにライトプロテクトを施して保管
34	システムの変更管理を行う。	システムの変更管理の実施
35	【駆除】のため、ウイルス対策ソフトウェアを導入する	【駆除】のためのウイルス対策ソフトウェアの導入
36	保険を適用する。	保険の適用
37	【IP フィルタリングデバイス:{ファイアウォール}、{ルータ}】を導入する。	【IP フィルタリングデバイス】の導入
38	マルウェア検出のための【対策:{スキャン}{コンテンツフィルタリング}】をする。	ウェブ閲覧時にマルウェア検出のための【スキャン対策】
39	ウイルス対策ソフトウェアを正しく設定して、定期的にスキャンする。	ウイルス対策ソフトウェアでの定期的なスキャン
40	ウイルス対策ソフトウェアを正しく設定して、リアルタイムにスキャンする。	ウイルス対策ソフトウェアでのリアルタイムスキャン
41	マルウェア検出のための使用前スキャンをする。	ダウンロードファイルに対するマルウェア検出のための使用前スキャン
42	すべての電子メールの添付ファイルをスキャンし、疑わしい電子メールの添付ファイルを特定し、【処理:{電子メールから添付ファイルを削除}、{電子メールそのものをブロック}】する。	すべての電子メールの添付ファイルをスキャンし、疑わしい電子メールの添付ファイルを特定し【処理】すること
43	取り外し可能な【記録媒体:{電子的媒体}{光学的媒体}】上のファイルに対する、マルウェア検出のための使用前スキャンをする。	取り外し可能な【記録媒体】上のファイルに対するマルウェア検出のための使用前スキャン
44	【使うツールのリスト{マルウェア対策メカニズム}】を利用して、【場所のリスト:{ローカル}】の【資産のリスト:{ファイル}】を定期的にスキャンする。	ウイルス対策ソフトウェアでのローカルファイルの定期的スキャン

・「ツリー図」から「三途の川図法」への展開

先に作成した「マルウェア県」の地図は、単なる表であり、あまり地図らしくは無い。いわば「マルウェア対策」地図に書かなければならない部品、例えば実際の地図における「家」や「学校」、「病院」、「田んぼ」、「畑」のような物、の一覧である。

これを地図にするためには、各部品がどのような位置関係で、どのように繋がっているのかを見つけ出していかなければならない。「マルウェア県」として採集した「マルウェア対策」の名称を眺めてみた。

「MAL.2 マルウェアの検知」と「MAL.3 ウイルス対策ソフトウェアの導入」の二つ対策を見ていると、なんとなく「MAL.2 マルウェアの検知」をするための対策の具体的な対策として、「MAL.3 ウイルス対策ソフトウェアの導入」があるように見えてくる。そこで、この二つの対策繋いでみた（図 5）。

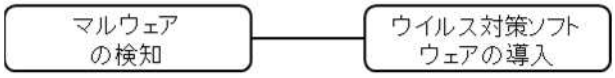


図 5「マルウェア検知」と「ウイルス対策ソフトウェアの導入」の関係

また、「MAL.3 ウイルス対策ソフトウェアの導入」と、「MAL.4 複数ベンダーの採用」の

二つの対策を見ていると、なんとなく「MAL.3 ウイルス対策ソフトウェアの導入」を検討する時（導入前）の選択肢として「MAL.4 複数ベンダーの採用」という対策があるように見えてくる。そこで、この二つの対策を繋いでみた（図 6）。

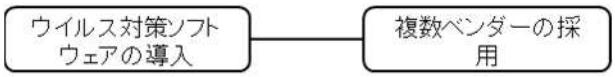


図 6「MAL.3 ウイルス対策ソフトウェアの導入」と「MAL.4 複数ベンダーの採用」の関係

「MAL.5 定義ファイルなどの最新化」、「MAL.6 定期的スキャン」の二つの対策は、なんとなく共に「MAL.3 ウイルス対策ソフトウェアの導入」という対策を実施する時（導入後）の選択肢に見えてくる。そこで、この三つの対策を以下のように繋いでみた（図 7）。

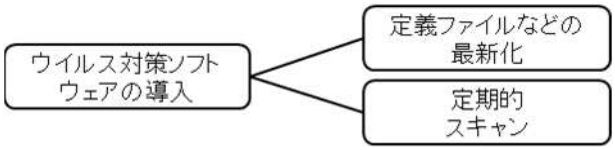


図 7 三つの対策の関係

そして、これらの結果を一つにまとめると、以下のようなツリー図ができあがる（図 8）。

図 8 ツリー構造

このように二つの対策間の関係を繋いだ物を一つにまとめていくと、なんとなく「マルウェア対策のツリー図」ができあがった（図 9）。なお、この図では採集した 24 項目の対策には含まれていない「リアルタイムスキャン」という対策が含まれているが、二つの関係を繋いでいくためにはこの対策を補った方がスムーズであるために追加したものである。この事は、この 24 項目だけでは「マルウェア対策」は全てでない可能性を示唆している。

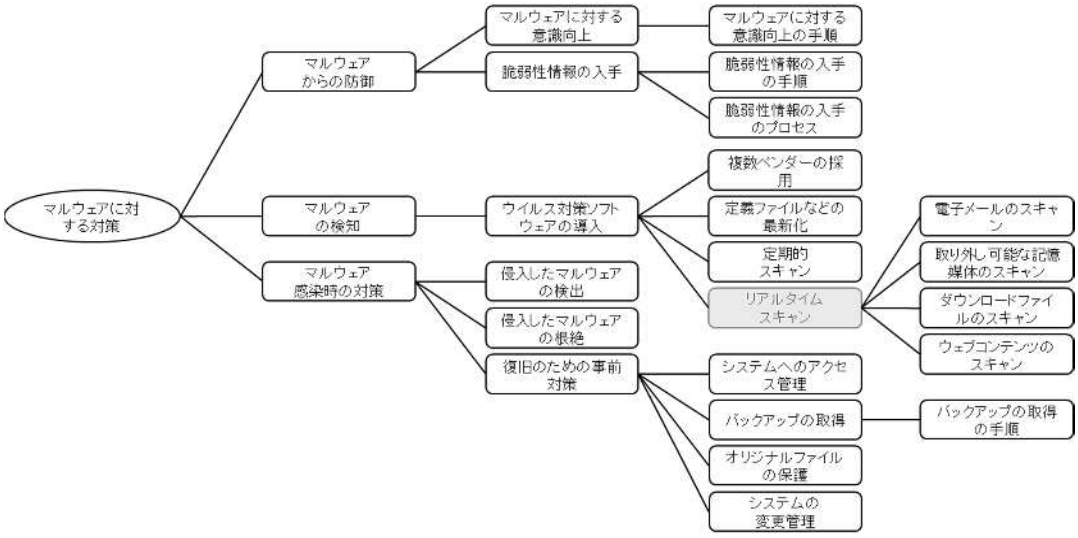


図 9 マルウェア対策のツリー図

地図という物が、そこに表される物の位置関係と、その繋がりを表す物であるとすると、このなんとなく出来たツリー図も、一つの地図であるといえる。後は、このツリー図作成の過程で示唆された、24 項目では全てではないという事象を解消するために、まだ採集できていない対策を採集して追加すればマルウェア対策の地図は完成する、かに思えた。

この、なんとなく出来上がった「マルウェア対策のツリー図」は、最初の内、なんとなくそれぞれのノードの据わりが悪いと感じはするものの、具体的にどこに問題点があるのかわからなかった。しかし、ノードの位置を変えてみたり、ノードの繋がりを変えてみたり、試行錯誤を繰り返す中で、各ノードを繋ぐルールは明確になっているのか、という問題があることに気づく事になる。

左から右へ、抽象が高い物から抽象度が低い具体的な対策へと並んでいっているように見えるが、同じレイヤ（ツリーの縦軸）で見た時に、それを揃えるルールは明確なのだろうか、また、分岐しているところが複数あるが、その分岐のルールは明確だろうか、という問題である。

ツリー図という表現は非常に自由度が高いため、どのノードをどこに付けるか、というルールが明確で無いと、作成する人によって、さまざまなツリー図が出来てしまう。

例えば、「マルウェアに対する【対策】の実施」という対策をルートにした時、第二レイヤ目には、「抑止のための対策」、「予防のための対策」、「検知のための対策」、「回復のための対策」のような「目的」をキーとして分類したノードを繋げていく事も考えられるし、「感染前の対策」、「感染後の対策」のような「フェーズ」をキーとして分類したノードを繋げていく事も考えられる。第二レイヤ目がこのように変わってくれば、当然それ以降のツリー図は全く異なった物となってしまう。

さらに、上位レイヤのノードが排他でない場合、それ以降のレイヤで複数の上位レイヤを持つノードが発生してしまい、ルートからきれいに分かれていく本来のツリー図にならなくな

ってしまう事もある。

ノードを繋げていくための何らかのルールが必要だが、そのルールの制約が強すぎるとプロットできないノードが発生してしまうし、逆に自由すぎるとマインドマップになってしまう。ノードを繋げていく適度なルールとはどのような物なのか、何回描いてみてもこれでいいという納得解がなかなか得られなかった。

・CRAMM の調査と理解の共有

ツリーを作成するという事は、対策の分類をしようとしているということであり、私たちはその分類のキー、分類指標を巡って、色々なところをグルグル廻っている感じから抜け出せないでいた。メソッドやプロパティを導入する事により扱わなければならない対策の数を減らすことはできたが、本質となる分類学というのは、2 年やってみたがコレというものがまだ見つかっていなかった。

行き詰まったので、寄り道をしてみる事にした。

対策の分類の仕方に何かヒントになるものはないかということを考えたとき、リスク分析ツールというのが世の中にあり、それらは対策のデータベースを持っているだろう、ということで、著名なリスク分析ツールとして、CRAMM が対策をどう扱っているか調べてみる事にした。

CRAMM の対策のデータベースを調べたところ、項目数は 3400 項目余りであり、5 段階で対策を階層化した非常に洗練された物であった。階層が上に行くほど目的に近く、下に行くほど具体的な対策になっていた。

目的と機能の分類は良くできていたが、詳しく見ていくと釈然としない部分があった。例えば、CRAMM では目的として出てきた物の中に、我々は対策そのものとしていた物がたくさん出てきた。結局、CRAMM の整理の方法は、目的と機能はわかりやすいのだが、我々の対策分類をこの通りにやってもうまくいかないな、という感想になった。

ただ、CRAMM の調査を行った結果、ブレークスルーのヒントを得ることができた。実は、普段我々が使っている目的と対策の区別は曖昧だということに気がついたのだ。具体的には、「～という目的のための対策を実施する」というものがよく対策のガイドラインに出てくるが、そもそもこれは目的を書いているのだろうか、それとも対策を書いているのだろうか、どちらにも読める、というのがきっかけだった。

対策の表現には、「目的型」というべき対策の表現と、「手段型」というべき対策の表現がある、ということである。内容は同じようなことなのだが、表現として二通り書けそうなのである。そうすると、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ないか、必ずペアになった「目的型」と「手段型」というのは出てくるのではないか、そして、これらの表現が混ざっているから、上手く整理できないのではないか、ということで、これらを分けてから整理してみることにした。

こうして、後に「三途の川図法」と呼ばれるマップ作成図法の緒に就く事ができたのである。

2.3 2011 年度

・「三途の川図法によるマルウェア地図」の試作

2011 年度は、CRAMM の調査から得られたヒントに沿って、実際に「マルウェア対策」の 44 項目を使って「目的型」の対策と「手段型」の対策を分けて整理してみる事から始まった。

まず真ん中に一本線を引いて、左側に「目的」に近いカードを配置し、右側には「手段」のカードを配置する。そして、それらを線で結んでいくと、ちょうど真ん中の線のところが「目的」から「手段」に変わっていくところになり、「目的」と「手段」が一対一になるポイントがここに出てくることになる。

実際にやってみると、きれいに一対一になるわけではなく、一つの「目的」に複数の「手段」が対応する一対 N になっているところも出てくる。しかし、だいたい同じ数の「目的」と「手段」が真ん中に集まった。残った、より概念的な目的や、より詳細化した対策を左右にだんだん広げていくという作りにしてみた（図 10）。

私たちは、真ん中に引いた物をとりあえず「三途の川」と呼び、左を「目的界」、右側を「手段界」と呼んでみることにした。真ん中の「三途の川」で「目的界」と「手段界」を分けるところがこの図法の特徴であるため、この図法を「三途の川図法」と呼ぶこととした。

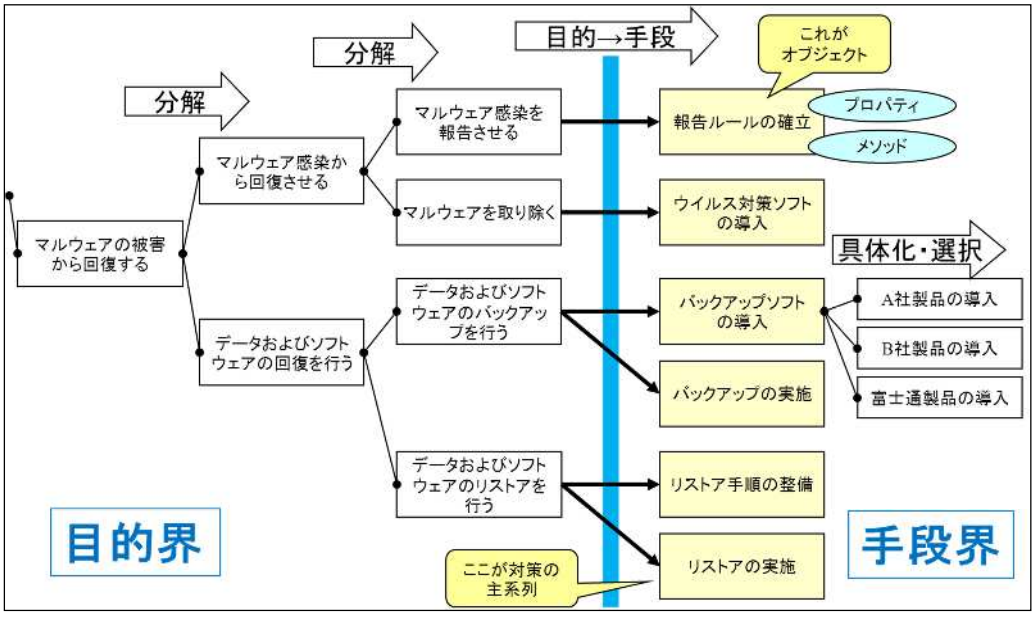


図 10 「三途の川図法」による「マルウェア対策」マップ（一部抜粋）

画が描き上がったマップを見てみると、左から順に「目的」を分解するようなイメージになっている。そして、真ん中の青い川のところで、「目的」から「手段」に変わっていき、「手段」に変わってから右へは、例えば、「具体化」であったり、「複数の対策の選択」であったり、と

いう観点で「手段」を細分化していく。

「三途の川」を挟んだ「目的界」側の岸には一番細分化された「目的」を並べ、「手段界」側の岸には一番粗い「手段」を並べる、というルールを設けることで、描く人によってツリー図が変わってしまうという問題はある程度防ぐことが出来たのではないかと思う。

「三途の川」の両岸から離れていく時の「目的」を抽象化していく方法や、「手段」を細分化していく方法についてまだ検討の余地が残ってはいるが、このアプローチが、私たちの一つの回答である。

また、「目的界」には「目的」のみを書く、というルールを設けることで、純粋に「目的」だけを集めていくと、その細分化はある程度のところで終わりが見える事が予想できる。これは「どこまで採集したらこれで全部だと思えるのか」の一つの解になるのではなかと思っている。

「三途の川」を挟んで左側に「目的界」、右側に「手段界」に分けて作成する「三途の川図法」では、「三途の川」を渡って最初の「手段界」に出てくる「手段」のリストが、「情報セキュリ対策」のリストとして完成度が高いのではないかと思う。それは、「目的」から「手段」に最初に落ちたところなので、一つ上に行けば必ず「目的」があり、そして「手段」として一番粒度が荒いところで、粒がそろっている。しかも、「目的」が網羅しているのであれば、きっと「手段」も網羅している、と考えると非常によいリストになっているはずである。

今回作成した「マルウェア対策」のマップには 44 個のノードがあるが、「手段界」の最初の列には 24 個のノードが並んでいる。それ以外のノードは、そこから派生して出てくる「手段」であったり、その「目的」であったりするので、マルウェアの対策はいくつあるのか、と聞かれたら「24 個です」と言って、このリストを見せても異論はないのではないかと思っている。

この 24 個の粒度の揃ったリストを得る方法がわかったことが、「三途の川図法」の大きな成果であると思う。

「マルウェア対策」マップの一部抜粋であった上記の図1には描かれていないが、「マルウェア対策」のマップの「手段界」の 1 列目に、「ウイルス対策ソフトウェアでスキャンする。」というノードがある。このノードには 6 項目の詳細化した「手段」が紐づけられているが、これは「マルウェア対策」のマップの中では一番多い（図 11）。

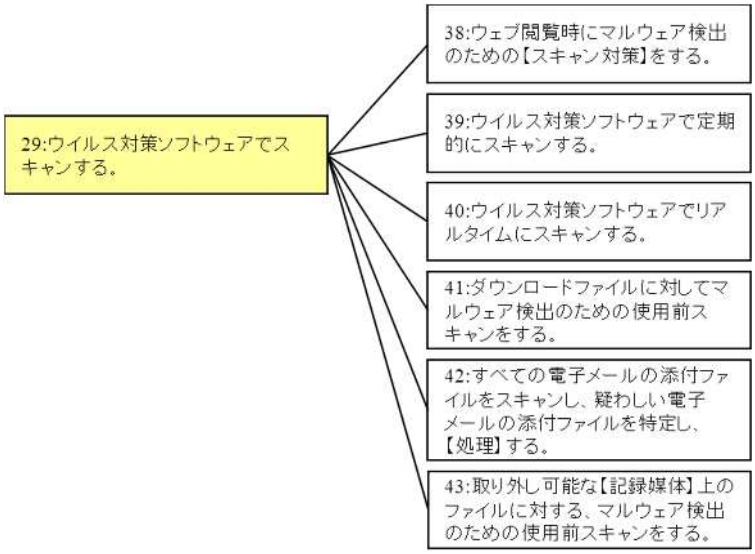


図 11 多くのノードが紐づく「ウイルス対策ソフトウェアでスキャンする。」

これは「マルウェア対策」が、現実世界ではスキャンに依存してしまっているからだと思われる。「マルウェア対策」がスキャンに大きく依存しているため、色々なガイドラインは、そこを細かく分類してしまう傾向にあり、また、逆に使い手からも、ここを細かく描いて欲しいというニーズもあるのではないだろうか。世の中のガイドラインは所詮ノウハウ集なので、どこのノウハウが求められているのか、というのが均一ではない、と言うこともできるかもしれない。そういうことが解るのも、こういったツリーのおもしろさの一つではないかと思う。

・「対策オブジェクト」モデルの詳細化

「マルウェア対策」の「三途の川図法」によるマップ作成の成功に気をよくした私たちは、次に、SP800-53 から採取した「アクセス制御」の対策を使った「アクセス制御地図」の作成に着手した。

対策を「対策オブジェクトモデル」を使って採取し、採取した対策を「目的」と「手段」に分けて「三途の川」の両側に配置していく。多少の試行錯誤は予想されるものの、順調に進んでいくものと、誰もが思っていた。

ところが、である。採取した対策の中に「目的」にあたる対策が無いのである。どれもが「手段」の対策なのだ。私たちは困惑した（図 12）。

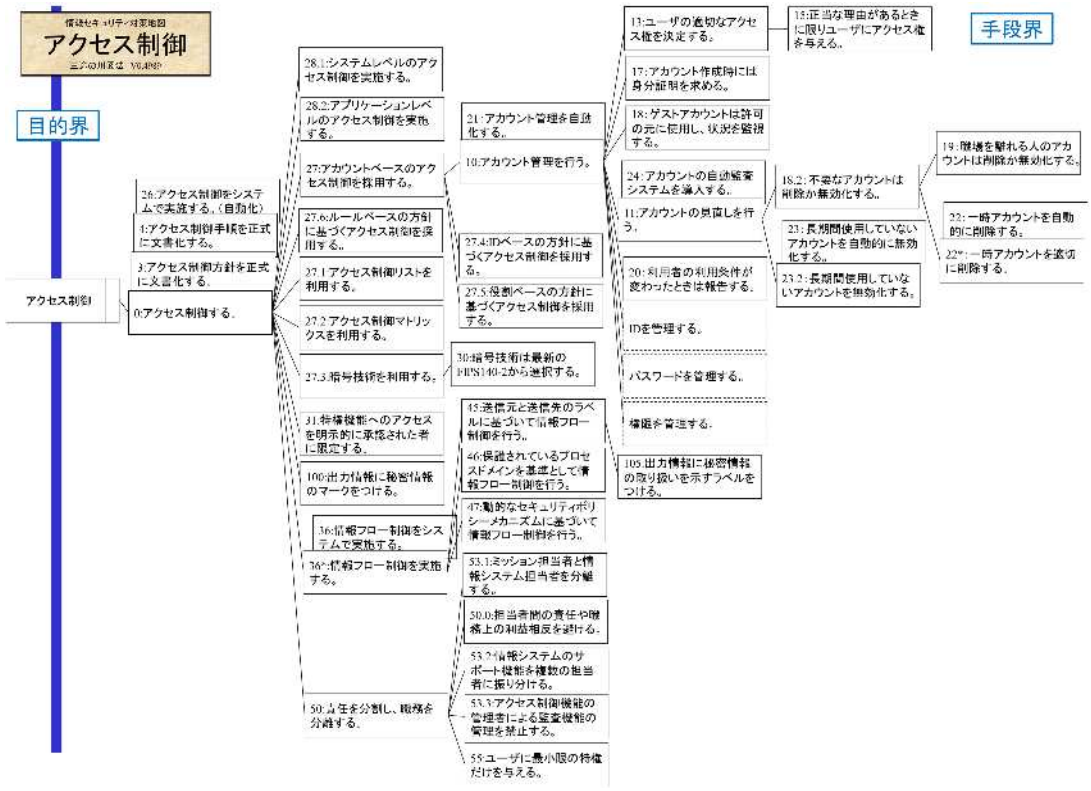


図 12 三途の川図法による「アクセス制御」のマップ

「マルウェア対策」は、マルウェアという脅威に対する対策である。そのため、少なくとも「マルウェアの脅威を無くしたい」という「目的が」存在する。一方、「アクセス制御」は、対応する脅威というのが明確には無い。「アクセス制御」は、セキュリティ技術の名前であり、「アクセス制御」自身が「手段」である。

アクセス制御自身が手段なのであれば、「アクセス制御」だけを「三途の川図法」で表すことはできず、もっと大きな何か他の対策を「三途の川図法で」表したときの一部分を作っていることになる。この「アクセス制御」のツリーは、「手段」の一つのライブラリのような形にしておいて、今後、「手段」として「アクセス制御」を使う「目的」が出てきたら、必ず、このサブルーチンを呼ぶ、そのような使い方にするのが正しいのではないか、ということになり、「アクセス制御」のツリーを「アクセス制御ライブラリ」と呼ぶことにした。

情報セキュリティ対策というのは、目的ベースで書ける物と、それ自身が手段であって目的を明確に定義できない物とが混在しており、後者の例としては、アクセス制御や暗号、識別認証など、技術要素の名前を使った情報セキュリティ対策カテゴリがあたると考えられる。

「三途の川図法」を使ってマップを作成するためには、「目的」が存在する情報セキュリティ対策を対象である必要がある。「目的」が存在する情報セキュリティ対策とはどのようなものだろうか。

そこで私たちは「対策構造図」に立ち返ることにした。ただし、2009 年度に作成した「対策

後続図」は、その後導入したメソッドやプロパティの概念が反映されていないため、それを反映する作業を、まず行うことになった。この作業の中で、これまで決めてきたメソッドやプロパティの要素が妥当であるのかも一緒に見直しを行った。

まずはメソッドの見直しである。

メソッドは、「標準構文」の「語尾の変化」を集めたもの（対策の述語の典型例）であるため、「～を計画する」や「～の手順を明確にする」、「～を実施する」、「～の効果を測定する」、「～を改善する」、「～を廃止する」などのように、一つの情報セキュリティ対策を機能させるために必要な一連の作業項目になっている。対策というのは、何か一つの機能だけなのではなく、これらの運用まで含めて管理して、はじめて機能するある一定の存在（オブジェクト）である、ということだ。したがって、これらは、一つの PDCA サイクルを持っている。

対策を機能させるのに必要な項目が揃っているか、という観点で見直し、これらの関係を整理した（図 13）。

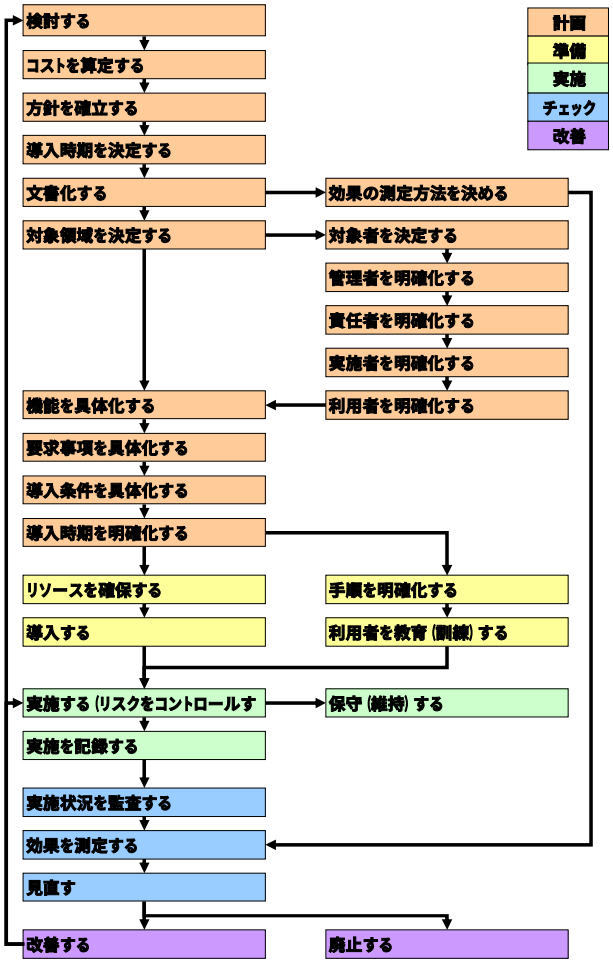


図 13 メソッドの関係整理

しかし、現実には、これらの一部が実施されていなかったり、そもそも情報セキュリティ対策として認識されていなかったりするために、本来その対策が持っている有効性が下がっ

ている場合があるのでは無いかと思う。

このメソッドという概念を取り入れたのは、本 WG で一番大きな成果ではないかと思う。対策の本質と周辺を上手く分離できるというのはとても良いことであり、多くのベストプラクティスやガイドラインが、これを混ぜて書いてしまっているため、リスクアセスメントに使おうと思ったときにこの部分で苦労しているのでは無いだろうか。

次はプロパティである。

プロパティは、「標準構文」の「枝葉の部分」を集めたものだ。「標準構文」の「枝葉の部分」とは、対策を実施するために、決めなければならないこと全て、もしくは用意しなければいけないこと全て、の事である。

そのため、「いつ」、「誰が」、「どこで」、「なぜ」、「何を」、「どのように」といった、所謂 5W1H の観点で整理する事ができる。整理にあたっては、人を中心としたモデリングや、条件を中心としたモデリングを行ってみた（図 14）。

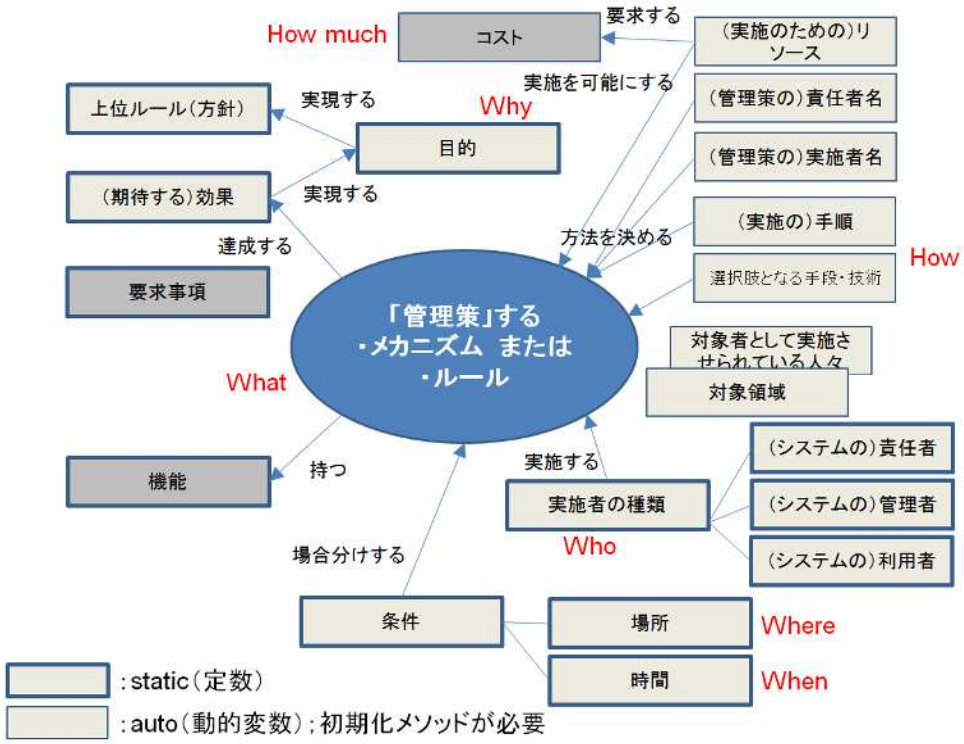


図 14 プロパティの整理

こうして見直した、メソッドとプロパティを合わせて完成させたのが、以下の「対策オブジェクト」である（図 15）。

オブジェクト		「管理策」		
プロパティ	静的	上位ルール(方針) 要求事項 時間	目的 機能 場所	期待する効果
	動的	リソース 実施者 実施手順 対象領域	責任者 利用者 手段・技術 導入時期	管理者 対象者 コスト 効果　実施記録
メソッド	計画	検討する 導入時期を決定する 対象領域を決定する 責任者を明確化する 機能を具体化する 導入場所を明確化する	コストを算定する 文書化する 対象者を決定する 実施者を明確化する 要求事項を具体化する	方針を確立する 効果の測定方法を決める 管理者を明確化する 利用者を明確化する 導入条件を明確化する
	準備	リソースを確保する 利用者を教育(訓練)する	手順を明確化する	導入する
	実施	実施する(リスクをコントロールする) 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	効果を測定する	見直す
	改善	改善する	廃止する	

図 15 対策オブジェクト

・エピソード　－2012 年 1 月 25 日－

その日、Network Security Forum 2012 の会場で、私たち WG のメンバーは多くの人から祝福を受けていた。栄えある JNSA 表彰を受賞したのである。

ひな壇で記念写真に収まる私たち WG のメンバーは、大きな喜びと、成果が出ていないのにもかかわらず表彰される事への少しの後ろめたさを感じていた。そして、皆心の中で強く誓っていた。「2012 年度こそ成果を出す」と。

しかし、2012 年度末、皆の強い誓いはもろくも崩れていた。成果が出るまでには、さらに一年が必要だったのである。

写真 1 JNSA 賞受賞

2.4 2012 年度

・「対策オブジェクト」に基づく地図作図手法の検討

今年度中に成果を出す、という強い意気込みで 2012 年度の WG は始まった。

「対策構造図」を、新たに導入されたオブジェクト指向を導入したモデルで書き直す目的で始めた、メソッドやプロパティ、「対策オブジェクト」の見直しであるが、新しい「対策オブジェクト」ができたため、これを使って、再度「マルウェア対策」の「三途の川図法」で作成したマップを見直してみることにした。

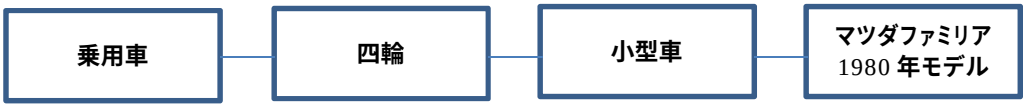
すると私たちは何となく違和感を覚えるようになった。その違和感の原因はなかなか見つからなかったが、実はその違和感の原因を探るヒントは、2011 年度に「三途の川図法」を完成させたときに思った、『この 24 個の粒度の揃ったリストを得る方法がわかったことが、「三途の川図法」の大きな成果であると思う。』という言葉の中に潜んでいた。

『24 個の粒度の揃ったリストを得る方法』、言い換えれば、「マルウェア対策」の「三途の川図法」にのっている粒度の揃った 24 個以外の対策は、粒度がバラバラであるということだ。本物の地図で考えれば、一つの地図の上に 1/2500 の縮尺の場所と、1/12500 の縮尺の場所が混在しているような物だ。これではゆがんだ地図になってしまう。

『対象物の「表現の抽象度」が上がると、対象物の「粒度」は荒くなる』。

これは、どちらも大雑把な方向に進んでいるように感じさせるため、一見正しいことを言っているように思える。でも本当だろうか？

例えば車で考えてみよう。



上記は、左に行くに従って対象物の「表現の抽象度」は上がっている。しかし、一方、対象物はいずれも「車一台」であり、その粒度は変化していない。そうなのである。『対象物の「表現の抽象度」が上がると、対象物の「粒度」は荒くなる』、は必ずしも正しいわけでは無いのである。いや、むしろマップ作成という作業においては、対象の「表現の抽象度」が上がっても、対象の「粒度」は変えてはいけないのだ。

では、どうしたら粒度を揃えることができるのか。

「三途の川図法」では、対象の「表現の抽象度」の高い「目的」を、どんどん分類して抽象度を下げていって、あるところから手段になっていくという作り方をしていた。そこで発想を逆転して、世の中の製品や、サービスという具体物から、それらをグループ化していくというボトムアップで対象の「表現の抽象度」を上げていく方法により考えてみる事にした。

世の中の製品やサービスを、JNSA の他の WG の成果の中から採取しよう、ということで市場調査 WG の報告書から採取することにした。

しかし、ここから採取した製品やサービスを分類して見てみると、1 つの製品やサービスでも、複数の機能を持っているものが多いという事がわかった。確かに、ファイアウォールと UTM は、それぞれ物理的に筐体が一個という意味では粒度が揃っているが、機能としては粒度が異なる。そして、ファイアウォールと UTM の横にはセキュリティコンサルティング、というのが同列に並ぶ事になってしまったりする。機能としての粒度が同じでは無い。さらに、MECE の確保ができない。

そこで、MECE の確保を、ISO/IEC 27002 の管理策に求めることにした。ISO/IEC 27002 に載っている管理策であれば、MECE は確保されているはずである。ISO/IEC 27002 に載っている 133 の管理策を一度バラバラにして、再度分類し直し、そこにラベルを貼る。さらにそのラベル同士で近い物を分類し、また新しいラベルを貼る、という作業を繰り返すことで、「表現の抽象度」を上げていく事ができないか、と考えたのである。

・ISO/IEC 27002 管理策の再分類試行（かるた取り）

ISO/IEC 27002 の 133 の管理策を見ていると、離れた項番に書いてあるが、内容が近い物がある事がわかる。

管理策とはなんぞや、を考えるために、今回は、「『管理策』を実施する」のモデルで書ける物が情報セキュリティ対策である、として検討を進める事とした。今までは、「実施する」に限定しないで、「標準構文」で切り出してしまったために、メソッドも混ざってしまった可能性があったが、「実施する」に限定することで、その可能性を取り除こうと言うことである。

ISO/IEC 27002 の 133 の管理策を短冊状に切り分け、分担をして、各管理策の中心となる「『管理策』を実施する」の部分にマークをして持ち寄った。そして短冊の「『管理策』を実施する」の内容を見て直感的に内容が近いと思えるものを近い場所に、遠いと思えるものを遠い場所に並べていき、ISO/IEC 27002 の 133 の管理策を新しく分類しなおした。この結果、15 の島に分類でき、出来た島にラベルを付けた。

短冊を分類する作業は、一人が適当に短冊を取り上げ、その内容を読み上げ、その内容に近い物を探す、という方法をとったため、あたかもかるた取りをしているようである、ということから私たちは、この作業を「ISO/IEC 27002 のかるた取り」と呼ぶことにした。（写真 2）

写真 2 かるた取り

・「機能要素」の導入

分類した ISO/IEC 27002 の 133 の管理策は、そのほとんどが要求事項[1]であることがわかった。そもそも、ISMS の本質に従えば、ISO/IEC 27002 に載っているのは組織が実現すべき要求事項で、その実装をルールにするかメカニズムにするかは組織が決めることである。その組織が意思決定するための仕組みが ISMS であって、その意思決定の結果を明文化した物が、ポリシーである。セキュリティポリシーでは、具体的な手順の詳細まで記述されることは一般にはないだろう。したがって、ISO/IEC 27002 には要求事項レベルのことしか書いてないと言っても何の違和感も無い。

ここで問題なのは、要求事項を情報セキュリティ対策と呼ぶべきなのか、それとも実際に

[1] ここでは、マネジメントシステム適合性評価のための要求事項ではなく、管理策として求められるセキュリティ要件という意味でこの言葉を使っている。

導入される、ルールやメカニズムを情報セキュリティ対策と呼ぶべきなのか、という事である。この二つはレイヤが異なるので、要求事項と、ルールおよびメカニズムの両方を情報セキュリティ対策と呼ぶのは、難しい。もし、ルールとメカニズムが情報セキュリティ対策で、要求事項は情報セキュリティ対策では無い、といってしまうと、ISO/IEC 27002 はほとんど情報セキュリティ対策が書いていないということになってしまう。一方、要求事項のレイヤで議論を打ち切ってしまったら、世の中に UTM という情報セキュリティ対策があるよね、という議論が出来ない。

議論を重ねる中で、私たちは、本 WG の設立趣旨の中で謳った解決したいことの一つとして『「高価な機材」を入れる理由の説明をできるようなマップが作りたい』というものがあったことを思い出した。UTM で解決できる出来る要求事項を明らかにして、A 社の UTM なら一台でまかなえるが、B 社の UTM だと機能が足りないね、という議論が出来るようにするべきなのでは無いか、と。

しかし、世の中にある全ての要求事項を洗い出し、実際の製品と結びつける作業を行うことは現実的では無い。ISO/IEC 27002 だけでも 133 項目もあるのだ。

そこで、一つの要求事項があった場合、ある製品がこの要求事項を満たしているかどうかは、何を持って判断しているのか、このことを考える事から検討を始めた。製品が持っているのは、「機能」である。要求事項を満たすために必要となる「機能のリスト」を作ることができれば、この「機能のリスト」と、製品が持っている「機能」を付け合わせて、製品が要求事項を満たしているのか、いないのか判断することができるのでは無いか。

そこで、各要求事項を実現するために必要となる「機能のリスト」を洗い出してみた。

「機能のリスト」の項目は、複数の要求事項で共通の物も多く、また、ISO/IEC 27002 以外の要求事項でも共有できる。そして、このリストの項目一つ一つは「標準構文」の「『管理策』を実施する」という形で書くことができ、メソッドやプロパティも定義できそうである。すなわち、「対策オブジェクトモデル」として扱う事ができるのである。また、粒度は、洗い出す「機能」の定義を「特定のリスクと1対1になるもの」とする事で、ある程度揃えることができる。

私たちは、このリストの一つ一つの項目を「機能要素」と呼ぶことにし、これを対策のルールやメカニズムから抽出することにした。

この「機能要素」の項目を介して、要求事項と世の中の製品を結びつけることで、機能の豊富な「高価な UTM（機材）」と、機能を絞った「安価な UTM（機材）」とを選び分ける説明をする事ができるようになる。さらに進めて言えば、情報セキュリティ対策製品のスペックシートを作るときに、「機能要素」の欄を設けることを標準化しておけば、各製品同士を比較できるようになる。

これでようやく情報セキュリティ対策として書くべき最小単位が見つかった。

・市販技術の整理試行（標的型攻撃対策分野）

私たちは、「機能要素」の有用性を検証するために、「IPA の標的型メール攻撃対策」の中のメカニズムが「機能要素」に分解できるか試してみた。

「機能要素」に分解していると、例えば、同じ SSL を使った暗号化でも、HTTP をカプセリングしたら HTTPS であるが、シェルをカプセリングしたら SSH になる、ように同じ技術ではあるが、使われるシチュエーションによって名前が変わるような物が出てきた。私たちはこれを「コンテキストバリエーション」として整理することにした。

この「コンテキストバリエーション」の導入は、現実世界に存在する「機能要素」を整理するためには必要ではあるが、「機能要素」を「特定のリスクと1対1になるもの」とする定義には、若干の見直しを要求することになる。リスクベース考えると、HTTPS も SSH も共に「暗号化機能」になってしまい、コンテキストとして並べる事はできない。

「コンテキストバリエーション」を導入することにより、「機能要素」の取り扱いは、脅威とかリスクとかにあまり縛られずに、純粋に技術的に何が出来るか、というかなり哲学論で分類していくことが求められる、一方、それがセキュリティ対策かどうかと判断するには、それが何かのリスクを消しているというエビデンスは必要なため、その微妙なバランスを取りながらやらないといけないことになった。

IPA の標的型メール攻撃対策の中のメカニズムを「機能要素」に分解して整理した結果を見ると、ゲートウェイ型アンチウイルスと IPS が実は仲間だったり、IPS と IDS のようにいつもひとまとめで語っていたものが、別物だったり、今まで明らかに違うだろうと思っていたものが、案外近いとか、今まで仲間にして当然だと思っていたものが、案外遠いとか言うのが見えてきた（図 16）。

図 16 標的型メール攻撃対策の機能要素（部分）

2.5 2013 年度

・既存製品カテゴリとの整合性検討（市場調査 WG の結果との突合せ）

「機能要素」の導入で前途が開けた感じを得られた私たちは、2013 年度こそ成果を出す

べく、年度の初めからラストスパートをかけた。

「三途の川図法」の時に、「マルウェア対策」のマップは作成できたにもかかわらず、「アクセス制御」では期待通りの結果が得られなかった経験に学んだ私たちは、「IPA の標的型メール攻撃対策」を「機能要素」に分解する作業で得た知見を使って、「2012 年度の JNSA セキュリティ市場報告書」のメカニズムを「機能要素」に分解できるか試してみることにした。

作業をしてみると、「JNSA セキュリティ市場報告書」の分類の目指しているところは、我々のマップの目指しているものと似ていた。この JNSA セキュリティ市場報告書の分類を、我々のポリシーで分類しなおしたらどうなるか、というかたちでアプローチをしてみることにした。

「JNSA セキュリティ市場報告書」では、実際に売っている製品を分類するために、「○○システムとそれに使用するデバイス」、のように記述されている。このシステムとデバイス両方併せて一つの「機能」を実現しているのであるが、この「JNSA セキュリティ市場報告書」の分類を、私たちの分類で分類し直すとき、「JNSA セキュリティ市場報告書」の分類の表現のどこの部分を「機能」としてとらえたら良いのだろうか。

何かが「機能」するというのは、「機能」する前と後とで何か変化があるということである。

この変化がはっきりわかる物であれば、効果を評価することが出来る。そこで効果を評価することができる単位を「機能」としたらよいのではないか、ということになった。各分類の「○○システムとそれに使用するデバイス」という表現で、どのようなリスクを消しているのか、という事を定性的に評価し、その内容と、「2012 年度の JNSA セキュリティ市場報告書」の「機能要素」を対比させながら、「2012 年度の JNSA セキュリティ市場報告書」の「機能要素」一覧表に加えていった（図 17）。

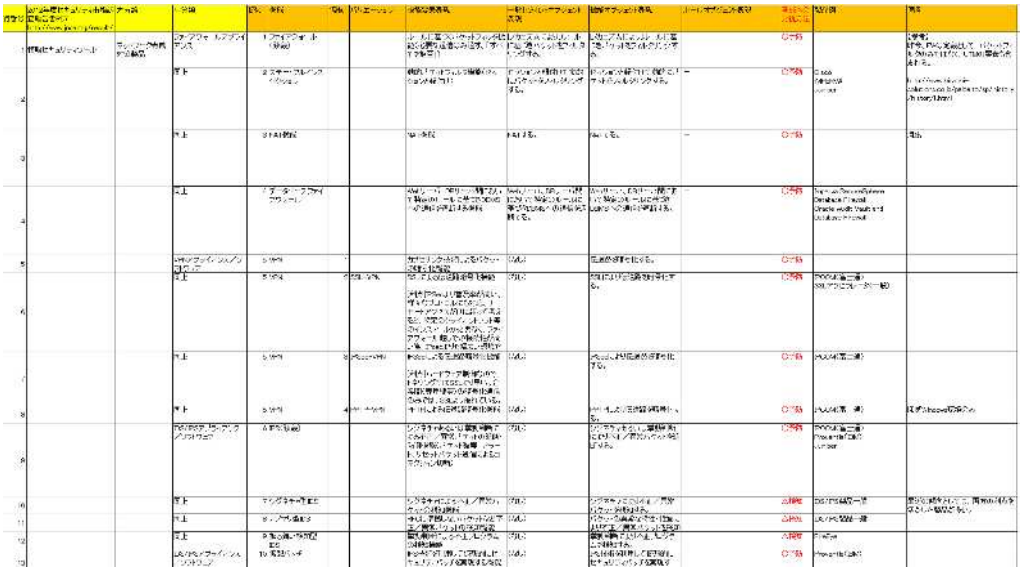


図 17 分類を考慮した標的型メール攻撃対策の機能要素（部分）

さらに、各「機能要素」にそれを実装している製品を付け合わせてみた。付き合わせた製品の選定は、WG に参加しているメンバーの会社の取り扱い製品、オープンソース、極メジャーな製品とした。将来的に、この一覧と金額をマッピングすることにより、『「高価な機材」を入れる理由の説明をできるようなマップが作りたい』、が実現できるのでは無いかと思う。

結果は成功であった。「JNSA セキュリティ市場報告書」も「機能要素」で分解できたのである。

・非技術的対策（フレームワーク、ルールなど）の取扱いの決定

これまで、世の中に該当する製品があってわかりやすい、メカニズムに注目して議論してきた。このメカニズムの整理が一段落したため、私たちはそれ以外の要素について整理を行うことにした。

まずは用語の定義である。

- ✧ 対策オブジェクト：強制力を持って実施させることで脅威に直接対応する物または事
- ✧ メカニズム：対策オブジェクトの内、自然法則を用いて人の意思に関わりなく強制力を実現する物
- ✧ ルール：対策オブジェクトの内、メカニズムでは無い物または事
- ✧ フレームワーク：コントロールが適切にその効果を発揮するために組織が行うマネジメント活動の要素（フレームワーク自身は脅威に直接は対応しない）

ここで、ルールは、脅威に対策オブジェクトの中で、メカニズムではないもの、と定義したため、ルールとメカニズムは並列かつ排他の関係になる。

ところで、ルールには、似ている物として、ポリシー、スタンダード、ガイドライン、プロシージャという物がある。これらの関係を整理するために調査を行ったが、実はこれらの関係について、標準化された定義が無いことがわかった。

しかし、何の根拠もなくこれらの関係を議論することは難しいため、CISA のサイトに記述されている以下の定義を採用することにした。

『ポリシーは経営者がサインしたハイレベルなドキュメント、スタンダードはポリシーを統一した適用を可能にするためのミドルレベルのドキュメント、ガイドラインは標準が無いときでも正しい行動が出来るように判断基準を与えるもので、必ずしも作らなくてもよいもの、プロシージャはスタンダードを実現するためにステップバイステップ形式で書かれている手順となっている』 [4]

この定義をベースに整理を行うと、私たちがこれまでルールといっていた物は、スタンダードに近い物だということがわかる。そして、ポリシーはその上位にあって、経営者が実施することを定めた物で、ルールでは無い。また、プロシージャは、どう実現するか、という How to なので、ルールより一階層下であり、「手順を作る」は既にメソッドに入っている。さらに、ガイドラインはこのモデル図には出てこない、ということになる。なお、ポリシーはメカニズムの上位にもあり、メカニズムおよびルールとフレームワークを繋ぐ役割をしている。

また、これまで対策オブジェクトの定義を、直接脅威に対抗する物または事、としていたが、この概念を拡張して、直接もしくは間接に脅威に対抗する物または事、としてしまうことで、「間接的対策」や「支援的対策」と呼んできた脅威に直接対応しない対策も、対策オブジェクトの中に取り込むことにした。これにより、たくさんある情報セキュリティ対策全体の中から、フレームワークを除いた物は全て対策です、と言えるようになる（図 18）。

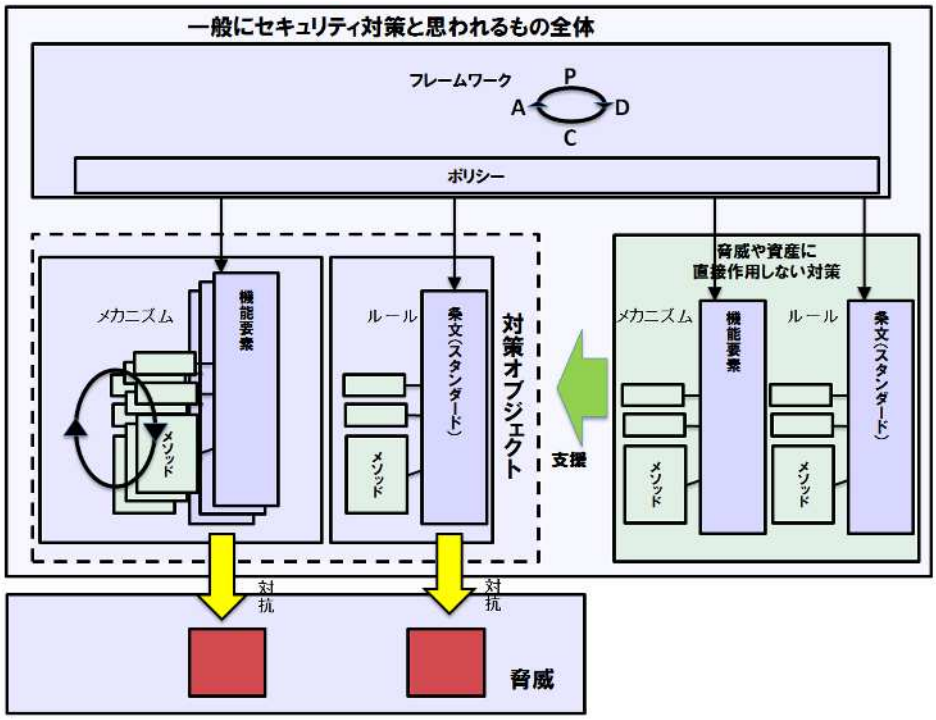


図 18 セキュリティ対策の全体構造

・「対策オブジェクト」に基づく地図の提言

このWGがこれまで行ってきたのは、ISO/IEC 27002やSP800-53など色々な情報セキュリティガイドラインから対策を集めてきて、それを「標準構文」で表した後、メソッドやプロパティとなる対策をたたみ込んで、「対策オブジェクト」を作成する。そして、「対策オブジェクト」を「機能要素」まで分解して、それらを分類してみる。こういった作業であった。

ここで得られた「機能要素」間には、構造を定義することができるが、この構造は「機能」間の関係を整理するための構造であり、何らかの目的を持ったものではない。

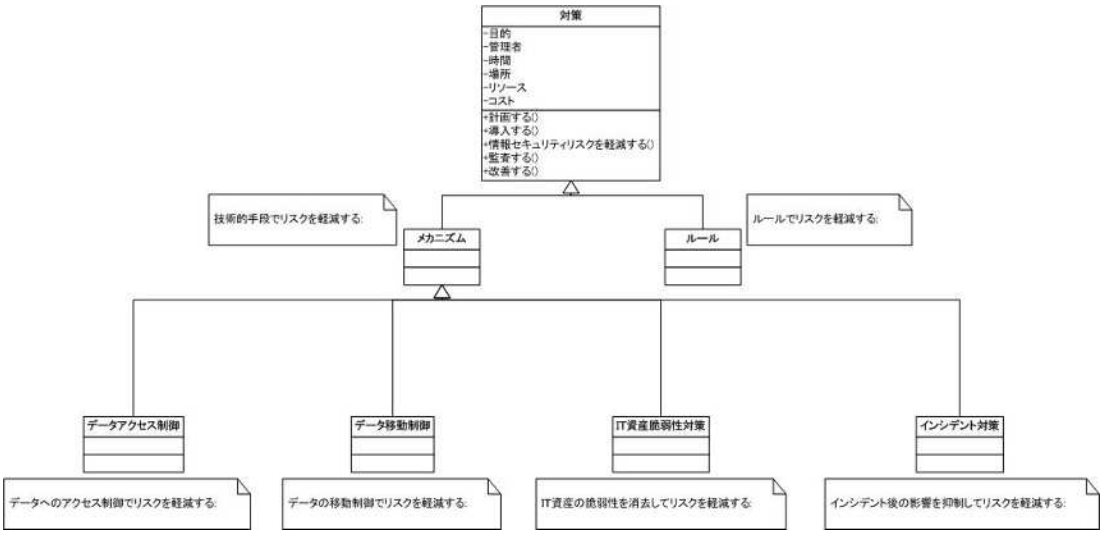


図 19 セキュリティ対策のオブジェクトツリー(その1)

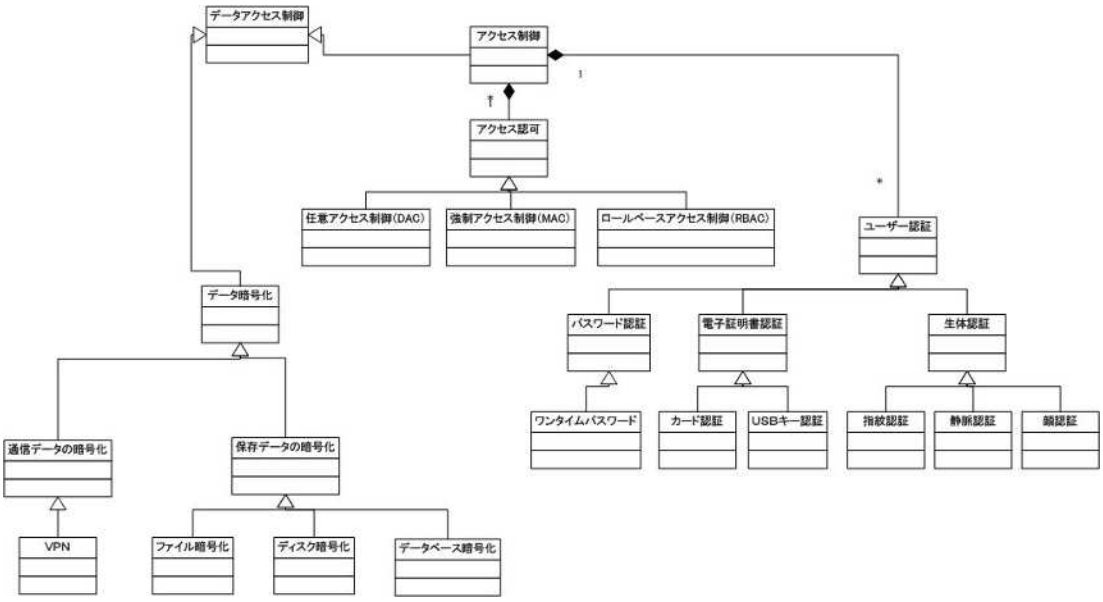


図 20 セキュリティ対策のオブジェクトツリー(その2)

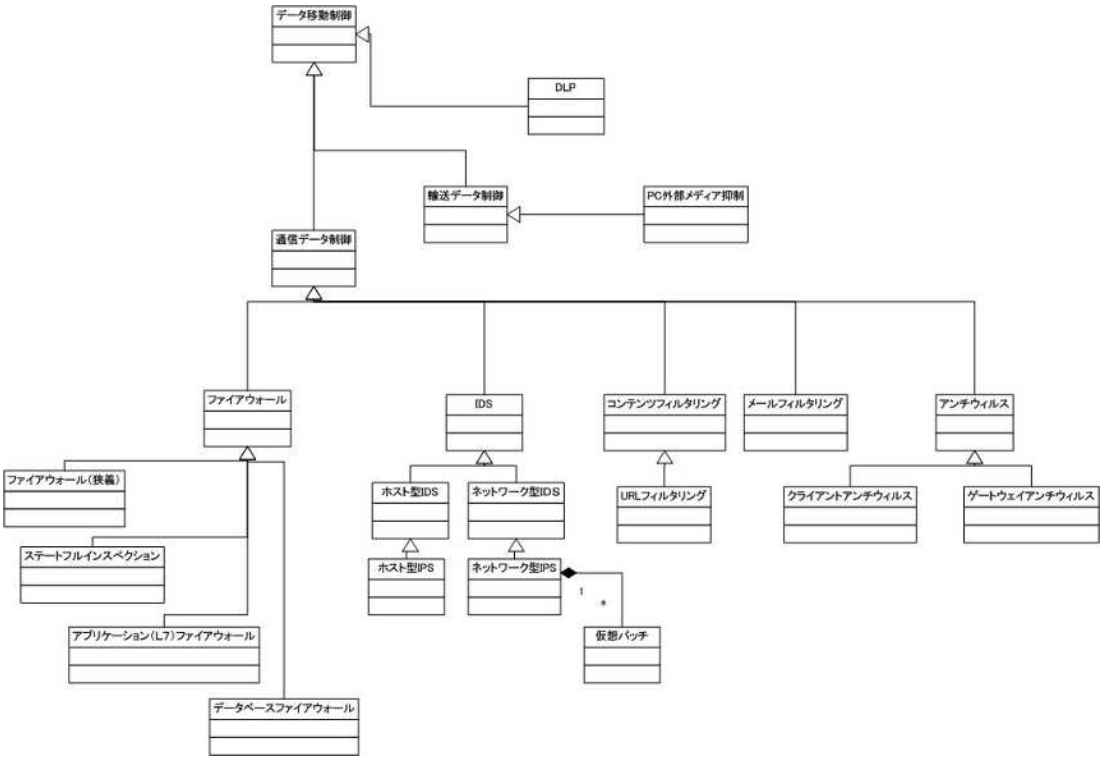


図 21 セキュリティ対策のオブジェクトツリー(その3)

すなわち、これらの「機能要素」は、「情報セキュリティ対策マップを作成するための部品」であり、いわばリポジトリのようなものである。この「機能要素」の構造を表す構造図はあくまでも構造図であって、情報セキュリティ対策マップでは無い。使用する目的や、誰が使用するのか、といった、何らかの観点のもとに組み合わせて初めて情報セキュリティ対策マップになる。

私たちは、どのような観点のマップを作ったら、楽しいか、有用であるか、という意見を出し合った。このときに出てきた意見を以下に列挙する。この中から最終的に三つの案について本 WG の成果とすることになった。しかし、最後の三つに残らなかった案も、いずれも秀作であり、今後機会があれば作成してみたいものばかりである。

- ◆ 朝出社してから帰るまでの情報セキュリティ対策
- ◆ ネットワーク図に対して各ポイントに対策を紐付けたマップ
  (対策に CVSS スコア付き)
- ◆ ユーザの観点で、ユーザの意識を高める事を目的としたマップ
  (ユーザが使うものを対象にそれぞれに対する脅威を縦軸にして、それらを使う場所を横軸に並べてみた)
- ◆ レポジトリの中から、脅威に対する対策、資産という観点の対策、場所に関連した対策、といった切り口で作成するマップ
- ◆ 戦いにおける城を守るイメージで、城を情報資産に見立てて、その城を守るための城壁やトラップとして対策を配した地図

◆ 家やストレージ、車など色々な場面を想定してそこのセキュリティ対策を同じ要素で考えるとどうなるかを考えたマップ

◆ 真ん中に目的を置き、これを島ととらえて、その周りを囲むように対策を並べていったマップ

◆GMITS のモデルを正確に書いた地図
直接的な対策ほど真ん中にくるようにもってきた
外側から、抑止・回復、ネットワークの上で防御するもの、資産そのものに直接作用するもの、の三ランクに分けて配置して、そこに建つ壁の長さにも何等かの意味を持たせる
なお、脅威は CWE の脆弱性から持ってきている

◆ 各対策を路線図で表したマップ

・最終報告

五年間の長きにわたって検討してきた、本 WG の成果は、次章以降に詳しく記載する。本報告書をもって本 WG の最終報告とさせて頂きたい。

・エピローグ　－2014 年 3 月 7 日、そして 3 月 8 日－

春まだ浅い葉山町の山の上は穏やかに晴れて、遠くに富士山がきれいに望めた。

時折、カラスとトンビが縄張り争いの空中戦を繰り広げる以外は、非常に穏やかな時間が流れていた。

WG の最終成果である「情報セキュリティ対策マップ」を作成するために合宿に集まったメンバーは 9 名。みんな想い想いに作成したいマップの案を持って集まっていた。五年前と異なるのは、みんなが持ち寄っている物が、マップのイメージでは無く、目に見える案という形になっている点である。

持ち寄った案の中から、WG の成果として報告書に載せる三点を投票で選び、そして、その三点を参加者みんなでブラッシュアップしていった。合宿の最終日、完成した三点のマップの出来映えはみんなの満足のいく物であった。

合宿所を出たみんなの顔は晴れ晴れとしていた（特にリーダー）[2]。それは、約束の三年間で成果が出せず、成果が出ないままに JNSA 表彰を受賞してしまった後ろめたさから解放されたせいかもしれない。

次章以降では、本 WG 活動によって得られた知見を、テーマごとに整理して記述する。本報告書執筆過程において、最終的に整合性が取れたモデルとなるように図などを調整しているため、次章以降の図などは 2 章で記述したものとは必ずしも同一ではない。

[2] 事実無根である。

3 対策オブジェクトモデル

3.1 対策オブジェクトモデル導入の背景

最初に当 WG では、世の中にすでに存在する各種のセキュリティ対策のガイドラインを収集し、そこに記載されているセキュリティ対策をカタログ化しようと試みた。この試みは WG 活動期間全体を通じて何回か行われたが、最終的な成果物を得ることはできなかった。しかしながら、この試みを通じて、世の中に存在する「対策」を客観的に扱う上で障害となる、様々な問題が見えてきた。

- 対策が自動的に実施されるメカニズムと、運用によって対策が実施される規則やルールが混在している。
- 対策を行う時の注意事項や工夫点など、対策ではないものも記述されている。
- 対策の記述の粒度がずれている。抽象的な対策から具体的な対策が混在している。
- ある対策を採用すると必然的に別の対策も必要となる相補関係や、二つ以上の対策は同時に実施できない背反関係などの複雑な関係が明確に記述されていない。
- 元になったガイドラインごとに表現が異なるため、異なる文書間でよく似ている対策があった場合に本当に同じかどうか客観的に判断できない。

これらの問題のほとんどは、世の中のセキュリティ対策のほとんどが日本語や英語などの、いわゆる「自然言語」で記述されていることに由来している。自然言語はその強力な表現力ゆえに、どのような内容の要求事項でも「対策」として記述できてしまう。極端な例として、「セキュリティ事故を起こさないようにする」という対策すら記述できる。これは本質的にセキュリティ対策の目的そのものであり、事実上すべてのセキュリティ対策を包含している。

この問題を解決するためには、まず自然言語で記述されている世の中のセキュリティ対策に対して、自然言語に特有の記述のあいまいさ、記述の多様性などを排除し、さらにその対策で要求している内容を、誰が見ても同じ理解ができる程度の客観性をもって正確に記述できる方法が必要になる。

上記の問題を解決するために、本 WG ではセキュリティ対策に対してオブジェクトモデルの概念を導入し、これを対策オブジェクトモデルと呼ぶこととした。この対策オブジェクトモデルの導入により、世の中のセキュリティ対策の記述が整理できて、マップ化しやすくなった。次節以降で、この対策オブジェクトの概念の詳細について説明する。

3.2 対策オブジェクトとは

対策オブジェクトは、セキュリティ対策をオブジェクト指向モデルの考え方を準用して記述す

る試みであり、情報セキュリティリスクをコントロールする識別できる対策の属性や振る舞いをカプセル化したものである。対策の属性は“プロパティ”と呼び、対策の振る舞いは“メソッド”と呼ぶ。このアイディアの中心になるのは、多くのセキュリティ対策の記述に共通して登場する要件を、共通の「メソッド」および「プロパティ」として分離することにより、取り扱う対策の数を抑制し、かつ網羅性の議論を進めやすくすることにある。

例えば、特定の対策の「責任者を明確にする」や「実施の記録を取る」といった要求事項は、多くのセキュリティ対策に付随する要求事項としてよくガイドラインに現れる。これらをそれぞれ独立したセキュリティ対策として取り扱うと、取り扱う対象のセキュリティ対策は膨大なものになってしまう。また、個別に取り扱っていると、A という対策には「責任者を明確にする」という要求事項があるのに、B という対策にはその要求事項がないといった、網羅性の不完全さを生み出す可能性もある。

そこで、まずセキュリティ対策をオブジェクト指向で扱われる「オブジェクト」として取り扱うことを考える。例えば「ファイアウォールを導入する」は一つの対策オブジェクトとなる。そして様々なセキュリティ対策に共通して登場する要求事項を、対策オブジェクトの「メソッド」として定義する。例えば「ファイアウォールを導入する」という対策オブジェクトに対して、「(ファイアウォール導入の) 責任者を明確にする」というメソッドを定義する。同様に、「対策の実施責任者」のように、多くの対策で共通して登場する場面や人などの属性を「プロパティ」として定義する。

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	

図 22 対策オブジェクト

対策オブジェクトは、一般的なクラスの性質を持つと考える。ある対策オブジェクトはより抽象度が高い上位の対策オブジェクトを持ち、上位の対策オブジェクトからメソッドとプロパティを継承する。最上位には最も抽象度が高い「セキュリティ対策」の対策オブジェクトがあり、ここ

に定義されたメソッドとプロパティは、そこから派生するすべての対策オブジェクトに継承される。この考え方により、多数のセキュリティ対策で共通して持つ「メソッド」と「プロパティ」を一つのオブジェクト内にカプセル化することができ、それぞれを個別に扱う煩わしさから解放される。

従来のセキュリティ対策を記述するアプローチと比較した利点をまとめると以下になる。

- カプセル化： 属性や振る舞いをまとめて対策オブジェクトにすることで、個々の対策が独立性を増すため、複数の対策の関係や連携を把握しやすい。
- 継承と構成： 今ある対策がどの他の対策を継承しているか、もしくは含むかの関係を把握することができ、新たな対策も既存の対策を継承したり、含んだり、また、発展させて生み出すことができる。

3.3 メソッドとプロパティ

メソッドは、対策オブジェクトで記述される対策に対する、付随的な要求事項であり、対策オブジェクトが対策としてその機能を十分発揮するために必要となる作業項目である。対策の振る舞いは、“メソッド”を利用して実行することができる。本 WG では、一般的にどの対策オブジェクトにも定義できる標準メソッドとして、次表のとおりメソッドを定義した。ここではわかりやすくするために、対策の導入段階にあわせてメソッドを分類している。また、「実施」の段階にある「実施する（リスクをコントロールする）」は、対策オブジェクトの機能そのものを表す特別なメソッドである。

表 4 メソッドの一覧

段階	メソッド
計画	検討する コストを算定する 方針を確立する 導入時期を決定する 文書化する 効果の測定方法を決める 対象領域を決定する 対象者を決定する 管理者を明確化する 責任者を明確化する 実施者を明確化する 利用者を明確化する 機能を具体化する 要求事項を具体化する

	導入条件を明確化する 導入場所を明確化する
準備	リソースを確保する 手順を明確化する 導入する 利用者を教育（訓練）する
実施	実施する（リスクをコントロールする） 保守（維持）する 実施を記録する
レビュー	実施状況を監査する 効果を測定する 見直す
改善	改善する 廃止する

プロパティは、対策を実施するために必要となる資源、対策の適用場面など、対策の実行時の属性またはパラメータとなる項目である。本 WG では、これを「静的プロパティ」と「動的プロパティ」に分類した。静的プロパティは、その対策をセキュリティ管理策として採用することを確定した段階で定義される情報を示しており、「動的プロパティ」はその対策が現場にて実施に移されるときに定義されるべき情報を示している。これらの「プロパティ」の内容 は「メソッド」を利用してアクセスしたり変更したりすることができる。本 WG で定義したプロパティは次表の通りである。いわゆる「5W1H」に相当する情報はこのプロパティの構成要素となっている。

表 5 プロパティの一覧

分類	プロパティ
静的	上位ルール（方針） 目的 期待する効果 要求事項 機能 時間 場所
動的	リソース 責任者 管理者 実施者

	利用者 対象者 実施手順 手段･技術 コスト 対象領域 導入時期 効果 実施記録

いくつかのプロパティは、メソッドと関連を持つ。例えば、プロパティ「実施記録」は、メソッド「実施を記録する」によって作成される情報そのものである。

さらに、「メソッドに対する共通修飾子」として、以下の用語を定義した。これらはセキュリティ対策の機能そのものには本質的な変化は与えないが、各種セキュリティのガイドラインによく出てくるため、確認の意味で定義している。例えば、「(対策を) もれなく実施する」という表現は一般のガイドラインによく現れるが、これは「(対策を) 実施する」という要求事項のバリエーションに過ぎない。このバリエーションを与える表現が共通修飾子である。

表 6 共通修飾子の一覧

共通修飾子	をもれなく を早く を安く を利便性を損なわずに を楽に

なお、メソッドはある対策を実施するために必要となる関連プロセスの全体像であるとも言える。この点に着目して、メソッドをその実施する順番に並べて図示することにより、次のような対策の実施フロー図を描くことができる。この構造が、いわゆる PDCA ループに類似であることは興味深い。

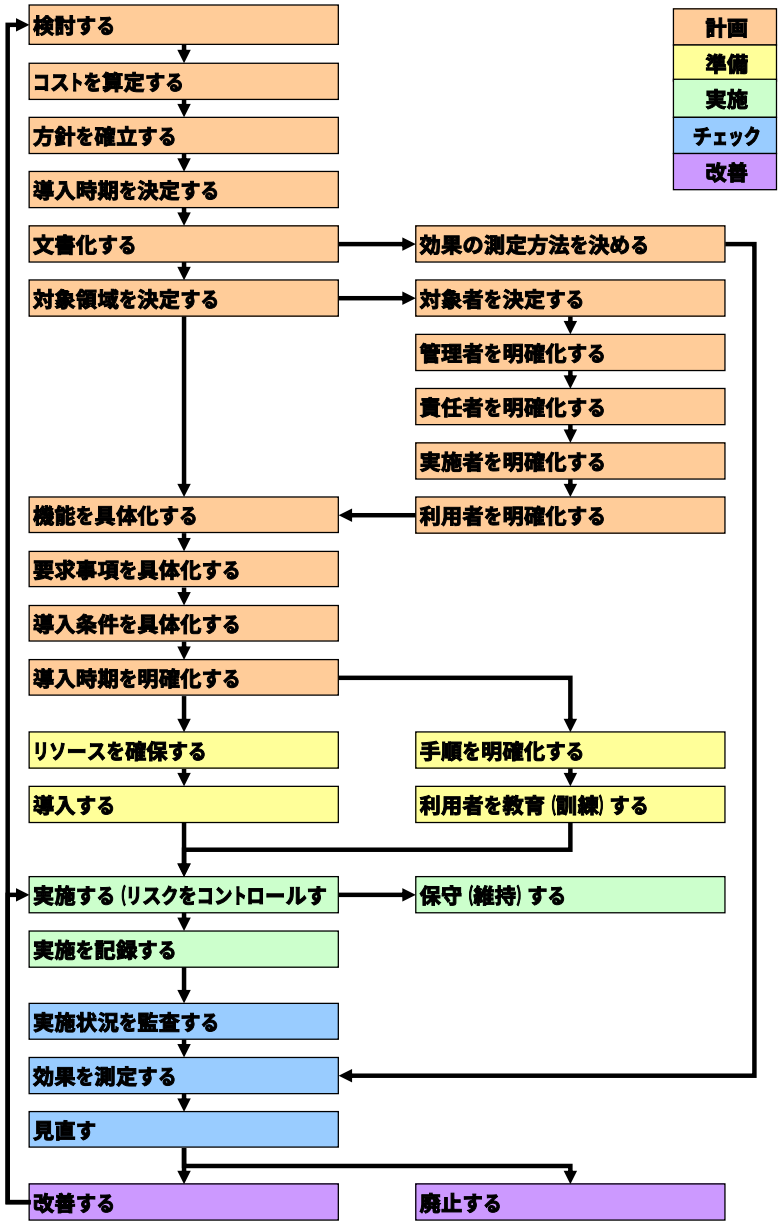


図 23 メソッドの関連図

一方、プロパティはそのセキュリティ対策を実施に移すために必要となる各種のパラメータ（変数）と言える。これらは、対策の実施場面と密接に関係を持つ。そして、一部のメソッドは、これらのプロパティを適切に設定するための活動だと理解することもできる（図 24）。

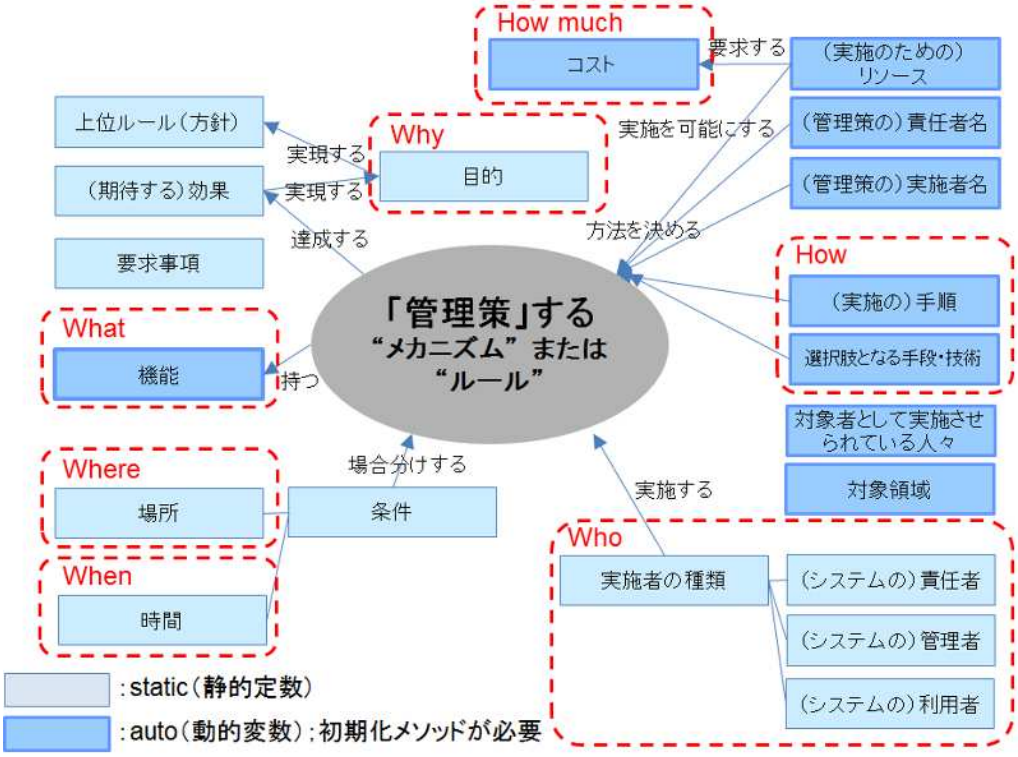


図 24 プロパティの位置付け

このように、セキュリティ対策（あるいは管理策）をオブジェクトととらえ、付随的な属性を「メソッド」や「プロパティ」として位置付けることで、従来は別個の対策として扱われていたものを統合整理することができる。次の図（図 25）は、マルウェア対策に関連する 34 個の対策オブジェクトを抽出して縦軸に配置し、それぞれに対するメソッド（この検討当時は 23 個）との組み合わせを横軸として、マトリックスとして配置したものである。それぞれの交点のセルは、ある対策オブジェクトに対するあるメソッドを表現しており、すべてのセルは異なる内容を持っている。従って、特定のメソッドで記述できる要件を一つのセキュリティ対策として認めるなら、マルウェア対策はこの表に登場する 782 個のセルの分だけセキュリティ対策が存在するということができる。

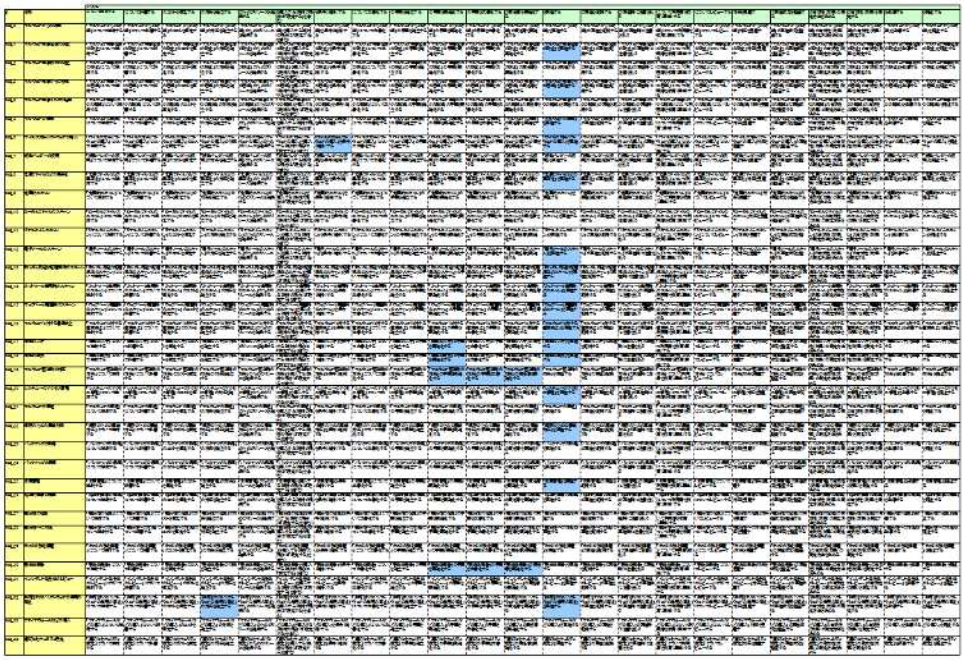


図 25 マルウェア対策に関する対策×メソッド表

（原寸大の資料は別冊資料編を参照）

表の中に 25 か所だけセルが青色に塗られた部分がある。これは、該当するセルで記述されたセキュリティ対策とメソッドの組み合わせが、ISO/IEC 27002 のマルウェアに対する管理策の記述の中で明に言及されていることを示す。このことから、ISO/IEC 27002 はマルウェア対策について、理論上は 782 個存在するセキュリティ対策の全体集合から、特に重要な 25 個を選択して採用したと理解することができる。逆に言えば、ISO/IEC 27002 の 25 個の要求事項の裏側には、明に記述されない 757 個のセキュリティ対策が潜在しているとも言える。このことから、本セキュリティ対策オブジェクトの考え方は、対策の網羅的な洗い出しのための非常に強力な武器になることがわかる。

3.4 機能と機能要素

前節で述べた通り、セキュリティ対策にオブジェクト指向的な概念を導入してモデル化することで、扱うべきセキュリティ対策の全体量を劇的に減らせるとともに、客観的にセキュリティ対策の要求事項を表現できる見通しが立った。次の目標は、セキュリティ対策ごとに異なる「抽象度」をそろえることである。

一般のガイドラインに記述されているセキュリティ対策は、広範囲な対象を取り扱うものから、非常に狭い、具体的な領域だけを取り扱うものまで、その対象領域や具体性には大きな幅がある。前節で例示した「セキュリティ事故を起こさないようにする」というセキュリティ対策は、おそらく最大の適用領域と抽象度を持つ対策だと言える。一方で、特定の機器に特定のソフトを入れる、さらにはその設定項目の在り方といった非常に限られた場面での具体性の高いセ

キュリティ対策も存在する。

セキュリティ対策を網羅したマップを作成しようとすると、どのように世の中のセキュリティ対策を洗い出せば網羅したことになるかという問題に必ず直面する。いわゆる MECE (Mutually Exclusive and Collectively Exhaustive) 性を持って重複なく、漏れなくセキュリティ対策を数え上げるには、対象を正確に分類することが最もよい方法である[3]。しかし、抽象度が異なるセキュリティ対策が存在すると、対策の分類がうまくできなくなる。だれもが納得できる分類を完成させるには、いかにして抽象度が均一にそろったセキュリティ対策のセットを作れるかが鍵になる。

そこで、本 WG では、「これ以上具体化または細分化できない、もっとも具体性の高いセキュリティ対策」の集合を作り出し、これを分類の基準とすることを考えた。抽象度の高いセキュリティ対策は、より具体性の高いいくつかのセキュリティ対策に分解できる。例えば、一般的なセキュリティ機能の名称である「ファイアウォール」は、より具体的な「侵入防御システム (IPS)」「ウェブアプリケーションファイアウォール (WAF) などのセキュリティ対策機能に細分化できる。このように抽象度の高い対策から、より具体的な対策への具体化、細分化を続けていき、これ以上進めることができなくなった段階で、最も細分化されたセキュリティ対策を確定する。これは、あたかも物質を細かく分割していき、最終的には原子を得ることによく似ている。このようにして、セキュリティ対策の「原子」が得られないかと考えたのである。

本 WG では、セキュリティ対策のうち、何等かの技術的な方法で対策を実施する「メカニズム」型の対策にまず着目し、その「原子化」が可能かどうかを試みた。最終的に、これ以上細分化できないレベルになったメカニズム型の対策を「機能要素」と呼び、これによって実現されるより抽象度の高い対策を包括して「機能」と呼ぶことにした。「機能要素」が原子に相当し、機能は複数の原子が集まってできる「分子」となるイメージである。

本 WG では、独立行政法人 情報処理推進機構 (IPA) が発行している「「標的型メール攻撃」対策に向けたシステム設計ガイド」 [5]などからいわゆる「標的型攻撃対策」を抽出し、この「機能要素」への展開を試みた、最終的に、36 種類の「機能要素」を得た (表 7)。

表 7 標的型攻撃対策の機能要素

No.	機能要素名
1	ファイアウォール (狭義)
2	ステートフルインスペクション
3	NAT 機能
4	データベースファイアウォール
5	VPN
6	IPS (狭義)

[3] 身近なところでは生物学がこの方法を取っている。本 WG の活動は、生物学の分類から多くのヒントを得ている。

7	シグネチャ型 IDS
8	アノマリ型 IDS
9	振る舞い検知型 IDS
10	仮想パッチ
11	次世代(L7)ファイアウォール
12	トラフィックモニター
13	ゲートウェイアンチウイルス
14	スパムフィルタ
15	コンテンツフィルタ
16	PC 外部メディア利用抑止
17	ワンタイムパスワード
18	パスワード認証
19	カード認証
20	USB キー認証
21	生体認証
22	電子証明書認証
23	起動可能プログラム制限機能
24	脆弱性スキャン
25	疑似攻撃
26	ソースコードチェッカー
27	Web アプリケーション脆弱性スキャン
28	デジタルフォレンジック
29	バックアップ
30	コンテンツ整合性の確保
31	ファイル暗号化機能
32	ディスク暗号機能
34	パッチの自動適用
35	プロキシ
36	DLP

この機能要素の洗い出し作業で、次のような議論があった。

- UTM など、一部のセキュリティ対策機能は、複数の機能を併せ持つ。このような複合対策を表現できるように工夫する必要がある。
- 暗号化、識別/認証/許可などは、機能要素としたが、これらのように機能要素単独ではリスクをコントロールできないものもある。

さらに、あまりに適用領域を限定しているため、機能要素として分類することが正当かどうか難しい詳細な機能要素のグループがあった。例えば、サーバ型ウイルス対策ソフトで、適用プロトコルごとに「HTTP 向けウイルス対策ソフト」「SMTP 向けウイルス対策ソフト」「POP3 向けウイルス対策ソフト」といった形で羅列される対策の一群が抽出された。これらを別の機能要素として取り扱うことは労力のわりには効果が少ないと考え、「機能要素のバリエーション」とい

う考え方を取り入れることとした[4]。

3.5 用語の標準化

セキュリティ対策のモデル化を実施する上で、もう一つ重要な作業が用語の標準化である。セキュリティ用語の標準化はそれそのものが非常に大きなテーマであり、本 WG では多くの時間を割くことはできなかったが、マップを試作するために必要がある最小限の部分での用語については WG にて標準化を試み、標準辞書としてまとめた（表 8）。

表 8 マルウェア対策領域の標準辞書

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
コンパイル型ウイルス	こんぱいるがたういるす		ファイル感染型ウイルス ブートセクタ感染型ウイルス	オペレーティングシステム (OS) によって実行される
[脅威に] 対策する	たいさくする			
[資産を] 保護する	ほごする			
防止する	ぼうしする			
検知する	けんちする	検出する、チェックする (FISC 技49)		
ウイルス対策ソフトウェア (SP800)	ういるすたいさくそふとうぇあ	悪意のあるコードからの対策ソフトウェア製品 (27002) 悪意のコードから保護するためのメカニズム (SP800) 不正プログラム対策メカニズム (SP800) 悪意のあるコード検知及び修復ソフトウェア (27002) ウイルス対策ソフトウェア (SP800) 抗ウイルスソフト (FISC) ワクチンソフト (FISC) アンチウイルスプログラム (PCIDSS) アンチウイルスメカニズム (PCIDSS)	スパイウェア検出／駆除ユーティリティ (SP800)	
スキャンエンジン	すきゃんえんじん	アンチウイルスソフトウェア (PCIDSS)		
スキャン	すきゃん	走査 (27002) 点検 (27002)		
定義ファイル	ていぎふぁいる	ウイルスパターンファイル (FISC) 定義 (PCIDSS)		
[対策を] 導入する	どうにゅうする	[対策を] 採用する (SP800-53)		
境界デバイス	きょうかいでばいす			境界に置かれるデバイス (ファイアウォールなど) ?
*	さまざま			
[対策] する	する	[対策] する対策を実施する		

[4] この「機能要素のバリエーション」の導入により、「機能要素はこれ以上細分化できない」という定義が少し危うくなってしまったのも事実である。

3.6 対策のオブジェクト化プロセス

ここまでの知見に基づいて、世の中にある一般的な「セキュリティ対策」を、セキュリティ対策のオブジェクトモデルに変換しつつ、最終的に機能要素の集合を得るまでのプロセスを検討した。その結果、以下のプロセスによって機能要素まで分類できることが WG の試行で確認できた（図 26）。

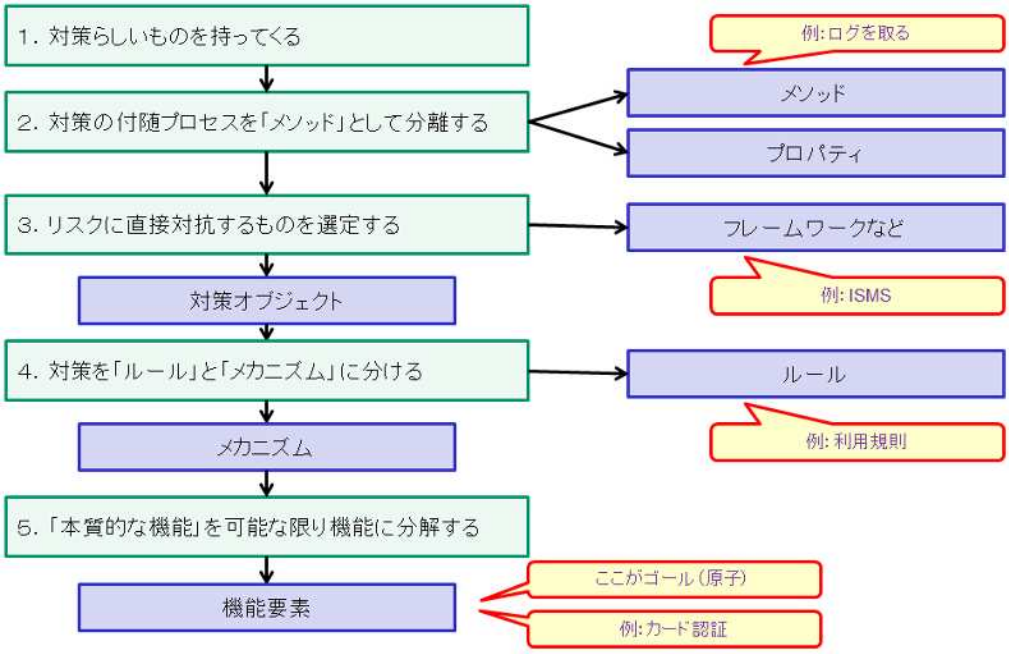


図 26 対策のオブジェクト化プロセス

1. 一般的なガイドラインから「セキュリティ対策らしいもの」を持ってくる。これ以降のプロセスでセキュリティ対策の正確な分類を行うので、ここではセキュリティ対策として読める可能性があるものなら何でもプロセスのインプットとしてよい。
2. 対策の付随プロセスを「メソッド」として分離する。例えば対象となるセキュリティ対策が、何かの「ログを取る」という表現であったなら、これは独立のセキュリティ対策ではなくて、他のセキュリティ対策のメソッドとして分類されるべきものである。同様に、「プロパティ」に言及しているものがあれば、同様に他のセキュリティ対策に包含されるものとして扱う。
3. その対策が直接「リスクに対抗しているか」を判断する。これに該当しないものとして、フレームワークの要求事項がある。フレームワークは例えば ISO/IEC 27001 [6]に記述されているような要求事項であり、セキュリティ対策を効果的に維持するための組織の取り組みに対する要求をまとめたものである。いわゆる「PDCA」に関わるものだと理解してもよい。
4. 対策を「ルール」と「メカニズム」に分ける。

5. 「本質的な機能」を可能な限り機能要素に分解する。ここの方法は 3.4 節にて述べた通りである。

これらのプロセスから逆算して、セキュリティ対策全体の分類図を描いたのが次の図（図 27）である。

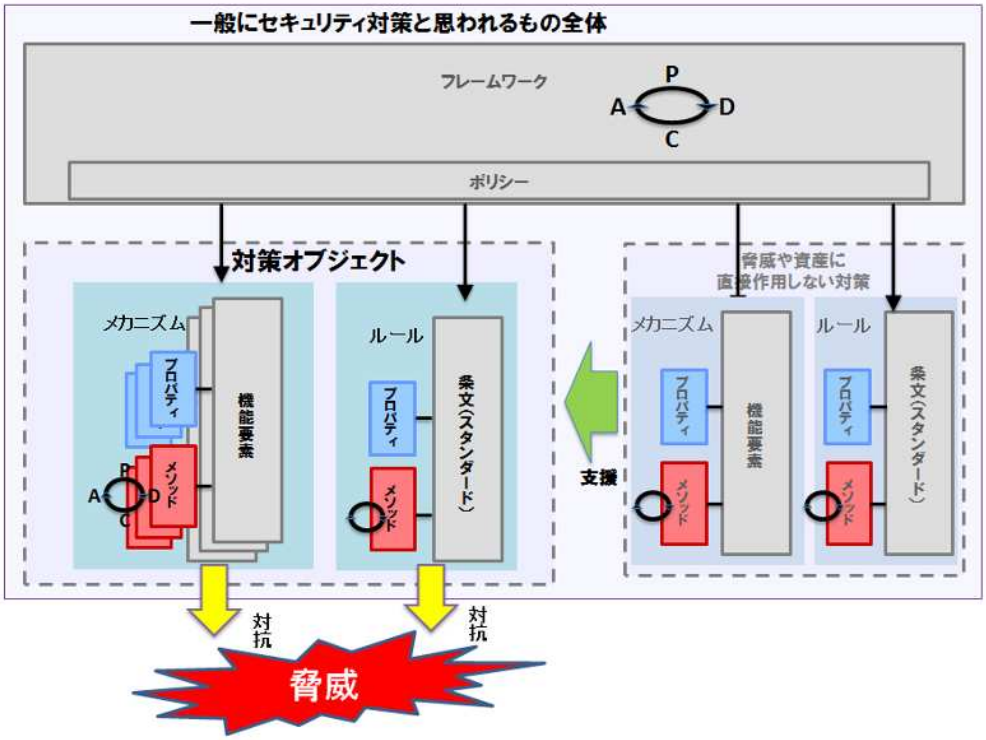


図 27 セキュリティ対策の全体構造

プロセス内の手順 3 で分離されたフレームワークは、その他のセキュリティ対策全体をコントロールする位置にある。その基幹文書として、セキュリティポリシーが定められている。

手順 4 でルールとメカニズムが分離される。これらの対策は、直接脅威に対抗する性質のものと、それを支援する性質のものにさらに分けることができる。これらすべての対策は「対策オブジェクト」でモデル化されており、それぞれ固有のメソッドとプロパティを持つ。特に、メソッドはそれ自身が小さな PDCA ループと見做せる構造を持ち（図 23 を参照）、そのセキュリティ対策自身の維持･改善に役立つ。

最後にメカニズムとして脅威に対抗する「機能」から「機能要素」が抽出される。機能要素は複数の要素が協調･連携して脅威に対抗する。

4　セキュリティ対策マップの作成

4.1　セキュリティ対策リポジトリ

セキュリティ対策マップとは、その利用目的によって、どのような表現形態がふさわしいかが左右される。その対策マップの利用者として誰を対象に想定しているかによって、様々な異なる種類の「対策マップ」が考えられる。「対策マップ」は、その対象となる利用者が経営者か、情報セキュリティマネジャーか、IT セキュリティ技術者かによって、そのあるべき形態が大きく違うであろう。例えば、ISO/IEC 27002 [1]などの世界的に普及しているセキュリティのガイドラインは、世の中で一番有名なセキュリティ対策マップということもできる。

セキュリティ対策マップがどのような形態のものであれ、そのマップを構成するものはセキュリティ対策そのものである。これらの様々な「対策マップ」に共通な対策の構成要素（元）を前章の対策オブジェクトモデルに基づいて記述することする。本章では対策オブジェクトを抽象的なクラスとして扱うため「対策クラス」と呼ぶ。

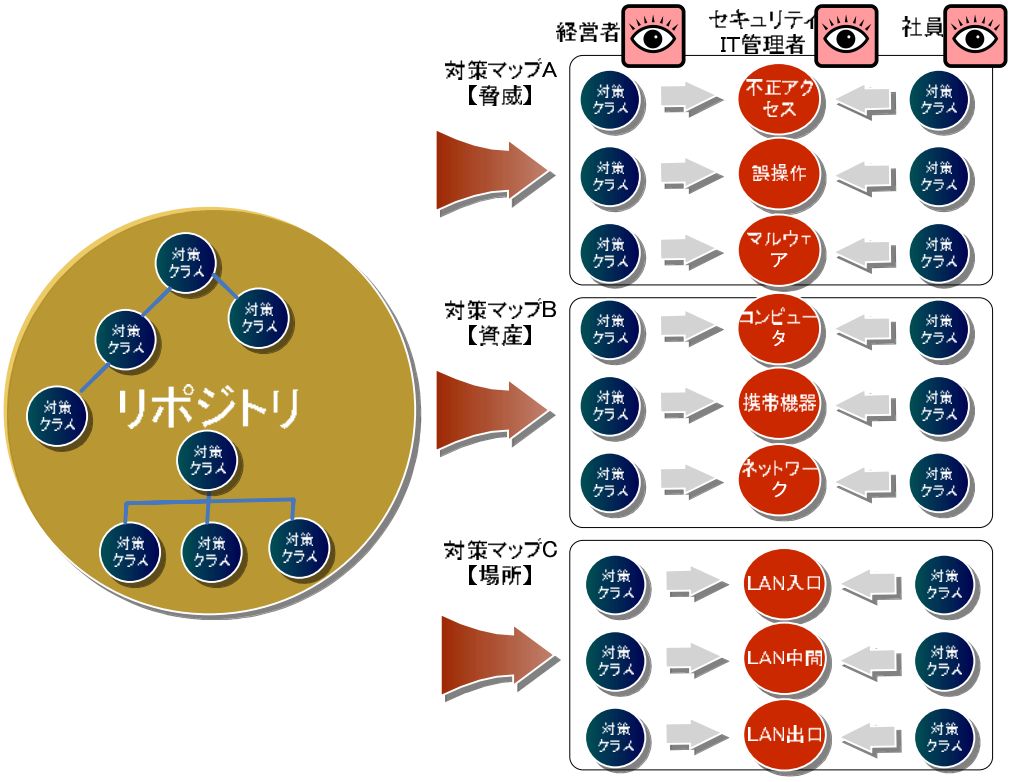


図 28 リポジトリからの対策マップ作成

対策マップを作る作業として、最初に行わなければならないことは、そのマップを構成する対策クラスを収集し、その対策クラスの集合を構造化することである。これは対策クラスのデー

タベースを作成する作業と考えるとわかりやすい。この作業で作成された、構造化された対策クラスの集合を「リポジトリ」と呼ぶことにする。リポジトリは、対策クラス間の構成や継承の関係に関する情報を内部に保持する。このように対策クラスをリポジトリとして整備することにより、様々な利用目的のための異なる種類の対策マップを客観的手法により生成する基盤を得ることができる。すなわち、これら“対策クラス”は利用目的が異なる様々な”対策マップ”に描かれることによって、対策対象の脅威、資産、場所などの観点を軸にその関係が並び変えられる。

4.2 セキュリティ対策の目的と手段

セキュリティ対策を日本語や英語などの自然言語で記述する場合は、その「目的」か、あるいはその「手段」かのいずれかを明示する形を取るのが普通である。例えば「メール送信時の情報漏えいを防止する」という表現は「目的」に重きを置いた記述であり、「メール送信のときに本文を暗号化する」という表現は「手段」に重きを置いた表現である。しかし、この分類は必ずしも常に明確なものではない。それは、場合によってはある「手段」が別の対策の「目的」となるケースが存在するからである。

例として、「ウイルス対策ソフトを導入する」というセキュリティ対策を考えてみる。ここで、もし仮に「ウイルス感染を予防する」というセキュリティ対策が別にあったとすれば、「ウイルス対策ソフトを導入する」は、「ウイルス感染を予防する」という「目的」を実現する「手段」と考えることができる。従って、「ウイルス対策ソフトを導入する」はここでは「手段」を記述していることになる。

一方、「特定のウイルス対策ソフトをクライアントにインストールする」という別の対策があったとしよう。この対策は「ウイルス対策ソフトを導入する」という「目的」を達成する「手段」と考えることができる。この場面では、「ウイルス対策ソフトを導入する」は「目的」を記述していることになる。このように、一般に一つの対策は「目的」→「手段」の関係のどちら側にでも現れることができる。さらにこの「目的」→「手段」の関係を鎖のようにつないでいくことで、対策のチェーンを生成できる。このようにして作成されたものが、当 WG の試作成果物の一つである「三途の川[5]」図法である。

[5] 三途の川はこの世とあの世を分ける境目にあるとされる川。渡り方が三通りあるためこの名がついた。本 WG では、二つの世界を分ける境界という概念からこの名を図法として採用した。

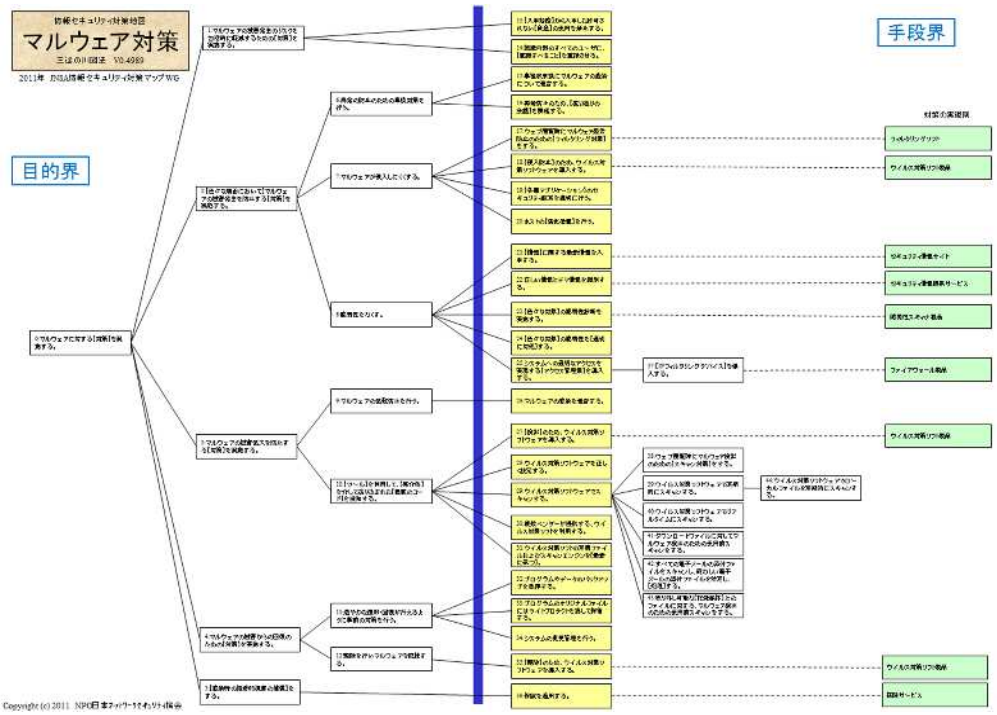


図 29 三途の川図法によるマルウェア対策のマップ

（原寸大の資料は別冊資料編を参照）

この図法では、長い対策のチェーン（実際には一つの目的を複数の手段で実現できるためツリー状の形状になる）が形成され、上流側がより目的に近く、下流側がより手段に近い表現が配置される。このことから、ちょうどその中心付近に「目的」と「手段」の境界があると想定することができる。本 WG では、この仮想的な「目的」と「手段」の境界線を「三途の川」と呼ぶことにした。さらに、三途の川の上流側に配置された対策の領域を「目的界」、下流側に配置された対策の領域を「手段界」と名付けた。

経営者には法令や株主の意向などの外的要因の「目的」があり、その目的を適える手段の集まりが「対策マップ」という形になる。経営者が決めた対策が、今度は情報セキュリティマネジャーにとっては外的要因の「目的」となり、その目的を適える手段の集まりが情報セキュリティマネジャーにとっての「対策マップ」という形になる。これら目的と手段の境が、それぞれの対策マップの「三途の川」となる。（図 30）

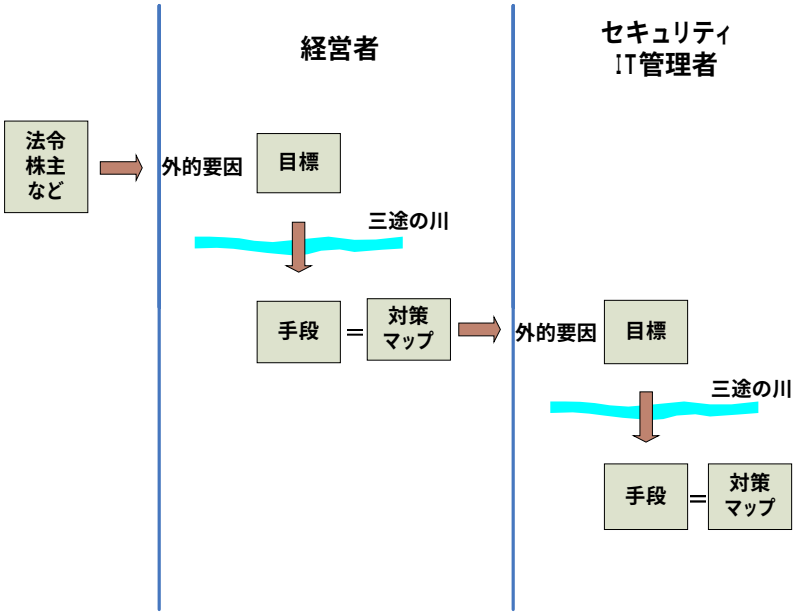


図 30 利用者視点による目標と手段の位置付け

4.3 セキュリティ対策マップの作成プロセス

本 WG が検討したモデルに従って、セキュリティ対策マップを作成するためのプロセスを整理すると以下のようになる。

1. 対策マップの対象者の識別
   (ア) 対策マップの対象者を特定する。
2. 対策マップの対象者の要望分析
   (ア) 対策マップの対象者の目的を特定する。
   (イ) 上記目的を達成するための手段（対策クラス）を特定する。その時、リポジトリを参照して、どの対策クラスを利用するか検討する。
3. 対策マップの描画
   (ア) 対策対象の脅威、資産、場所などの観点を軸に、個々の対策クラスを並べる。

なおこのプロセスは、2.（イ）の対策クラスの選定の部分で、リポジトリを用いる代わりにリスク分析を用いて対策を選定するプロセスを採用すると、各種マネジメントシステムで定義している一般的なセキュリティ管理策策定のプロセスとほとんど同一となる。別の言い方をすれば、各組織でのセキュリティ管理策策定とは、その組織専用の「セキュリティ対策マップ」を描くことだと言い換えることもできる。

5　セキュリティ対策マップ作成例

3.4 節で、標的型攻撃対策の機能要素の洗い出しを行い、36 種類のセキュリティ対策機能要素を抽出した。これを元にセキュリティ対策リポジトリを表形式で暫定的に作成し、いくつかのアイディアに基づき、実際にセキュリティ対策のマップができるかどうかを試行した。本章にて、その試行の例を紹介する。

表 9　標的型攻撃対策リポジトリ（部分）

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NP	機能	仮NP	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。	Cisco IMPERVA Juniper	[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。		
		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より速い。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	

（原寸大の資料は別冊資料編を参照）

5.1　マップ作成例その1

最初のマップ作成例は、セキュリティ対策をそれが実装される場所にプロットしたものである。特に物理的なメカニズムを持つセキュリティ対策は、それが配置される物理的な場所を特定することができる。従って、一つの企業の事務所やデータセンターなど、物理的な空間にセキュリティ対策をプロットすれば、利用者にわかりやすいセキュリティの地図となる。

図 31 は試作した「家庭のセキュリティ対策マップ」と「自動車のセキュリティ対策マップ」の例である。「家庭のセキュリティ対策マップ」では、一般的な家庭内に存在する IT 機器を想定し、そのどの場面にセキュリティ対策が必要になるかを図示している。また、「自動車のセキュリティ対策マップ」では、比較的近未来に実現するであろう、高度に IT 化された自動車を想定してそこに配置されうる各種のセキュリティ対策をプロットしている。

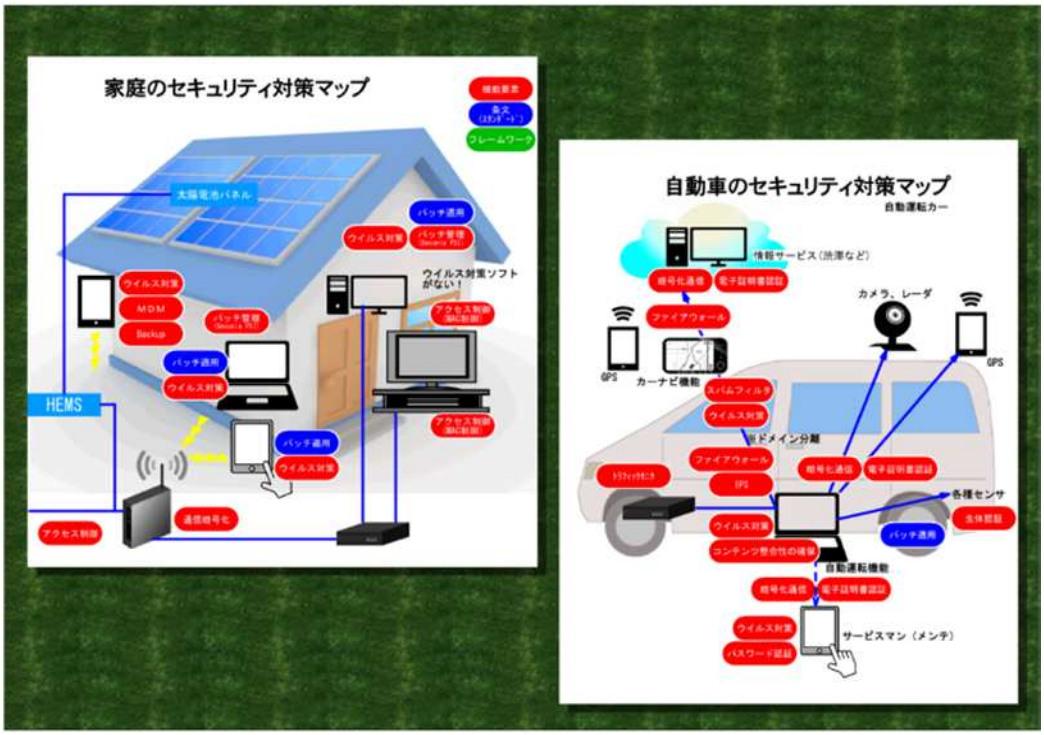


図 31 マップ作成例その1の1 「家庭と自動車のセキュリティ対策マップ」

（原寸大の資料は別冊資料編を参照）

図 32 は、「オンラインストレージのセキュリティ対策マップ」と「IaaS のセキュリティ対策マップ」の例である。いずれも実体は遠く離れたデータセンターにあり、利用者はその物理的配置を通常意識することはできない。そこで、これらのサービスに対しては正確な物理配置ではなく、むしろ利用者にイメージしやすい論理的な空間にセキュリティ対策を配置する方がわかりやすいと考えた。

IaaS については、現在一般的に実施されていると思われるセキュリティ対策をプロットした「一般モデル」と、現段階で想定されるセキュリティ対策を考えられる限り実装した「至高モデル」の2種を作成した。

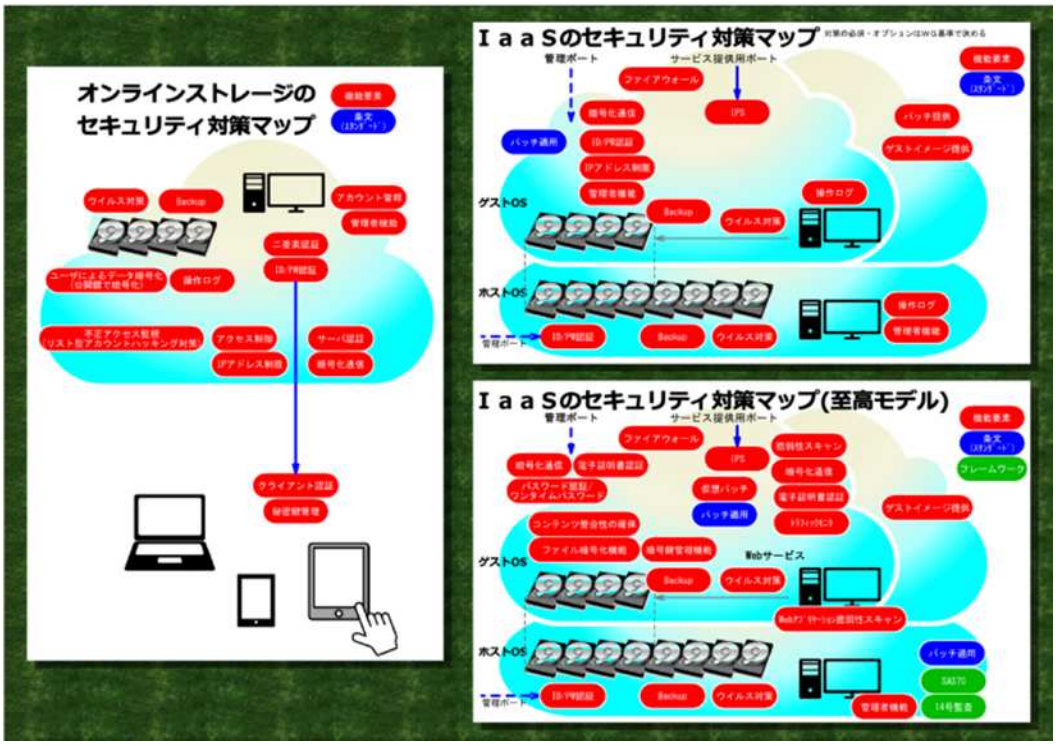


図 32 マップ作成例その1の2 「オンラインストレージと IaaS のセキュリティ対策マップ」

(原寸大の資料は別冊資料編を参照)

5.2 マップ作成例その2

「手段の海、目的の島」モデルは、ある目的のために適用可能な対策を俯瞰するモデルである。ある目的から情報セキュリティ対策を引き出すマインドマップであるといってもよい。

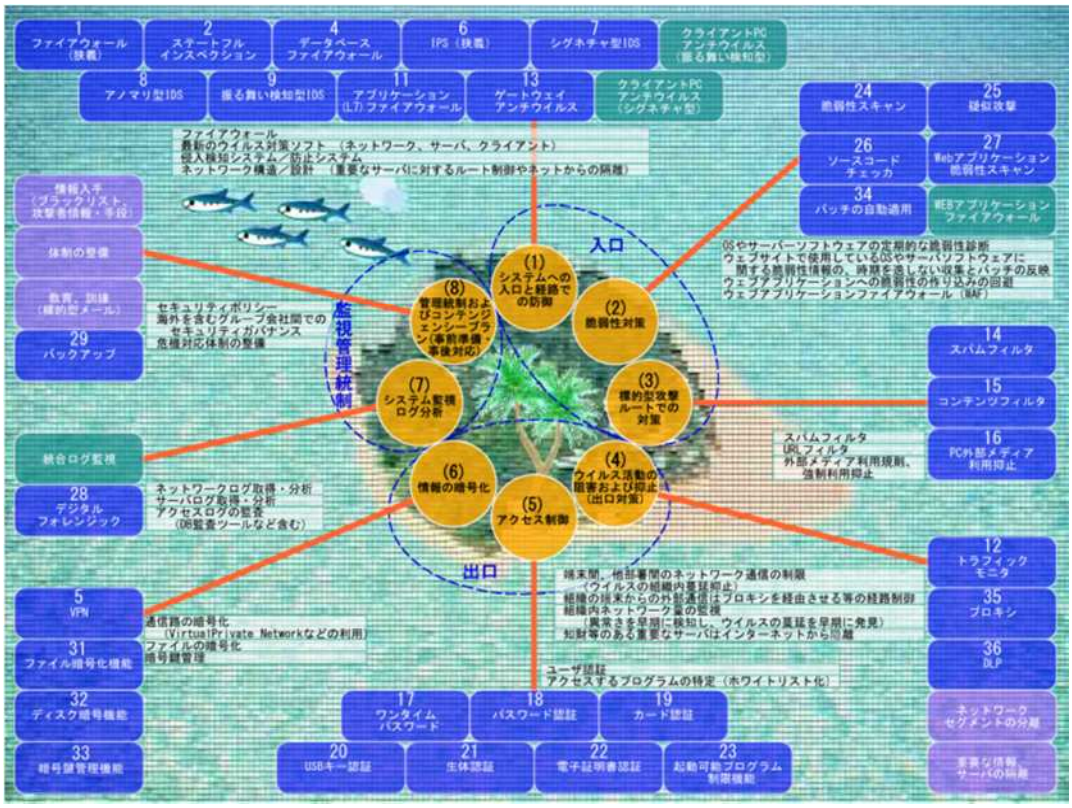


図 33 マップ作成例その2 「手段の海、目的の島」

（原寸大の資料は別冊資料編を参照）

このモデルでは、あまたある対策の「海」から、ある目的のために有用な対策が選ばれて利用されている様子が示される。目的を実現するための対策はひとつとは限らないので、その「島」の目的からいくつもの対策が分岐枝分かれしながら、さらに対策のための対策が数珠繋ぎに海の中にぶら下がる。それらは対策の選択肢であったり、結合あるいは協調であったりする。

図 34 目的の島と手段の海

「手段の海」では対策が生成と消滅を繰り返す。「目的の島」では、海蘊(もずく)のように海にたゆたう網状の手段を岸辺から引き上げている。海岸で引き上げた網に多種多様の海草が絡みついてくるように、対策は互いに関連し、繋がっている。

「海」には、ISO/IEC 27002 [1] や NIST ST800 [7]、PCI DSS [8]、FISC 基準 [9]、FIPS [2]、GMITS [10]、P マークなどといった、多くの対策を産み、育む海洋や海域、海峡、湾、海流などの編成が公に知られている。

また、このモデルでは、海の底から「脅威」が海底火山のように隆起し、海面に現われたところで、それが目的に固まるイメージを思い描いている。即ち、そこに、まさに噴煙を上げながら新たな脅威に対抗する「目的の島」が誕生する図絵である。

「目的の島」の中心にあるのは「脅威に対抗する」という最終目的である。島の中心の目的

の周りには、さらにいくつかの目的が取り囲む。それらは対策の方向性や方針を示すものである。マインドマップでいえば、セントラルイメージと BOI (Basic Ordering Idea) に当たるものだろう。

「手段の海、目的の島」モデルでは、「目的の島」の海岸線が目的と手段の境界線である。これは「三途の川」図法における「川」に当たる。

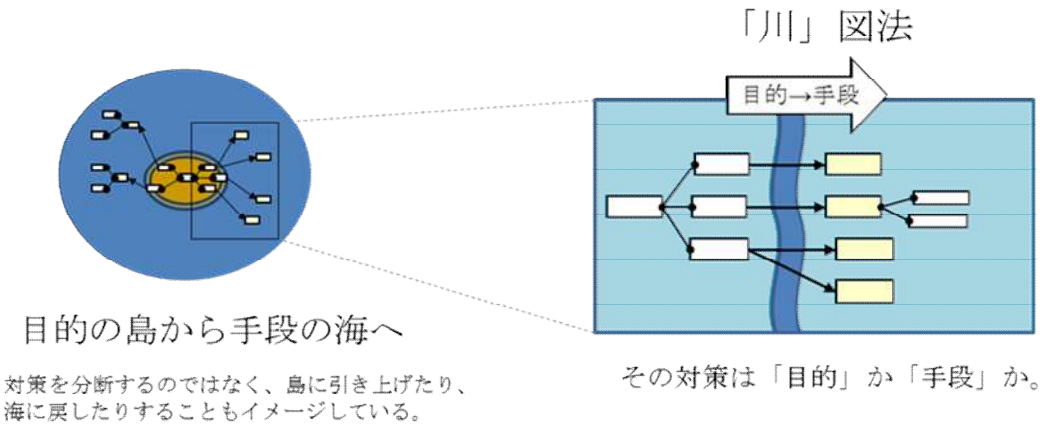


図 35 手段の海、目的の島と川

ただし、このモデルでは、波打ち際での「島」の境界は曖昧である。それが目的であるか手段であるかは確定できない。寄せる波によって、あるいは、潮の満ち引きによって、実際には海岸線が止まってはいられないのと同様に、それは静止した境界線ではない。対策は、ときには目的であり、ときには手段である。目的と手段の関係は相対的で、対策は目的と手段の両面を重ね合わせて持つ。

「手段の海、目的の島」モデルは、対策の連鎖が目的と手段に分化していない、という意味では、「三途の川」図法よりもいくらか原始的である。情報セキュリティ対策を分類するために、さらに進化したのが「三途の川」図法であるといえる。

5.3 マップ作成例その3

ここでは、既存の IT セキュリティ関係の文献を調べ、それらをベースにして対策マップ作成にたどり着いた例を示す。ここでのマップは、情報資産と脅威との位置関係および対策の有無や重なり具合を図示することを目的としている。

まず、前章で示した制作手法に則って、特定された対象を具体的に示す。

1. マップの対象者の識別

(ア) 対策マップの対象者を特定する。

⇒対象者は、この対策マップをもってセキュリティ対策を検討する立場の人である。たとえば、セキュリティ管理策全体を提案するコンサルタント、実際に企画する立場にある組織のリーダー等である。

2. 対策マップの対象者の要望分析

(ア) 対策マップの対象者の目的を特定する。

⇒対象者が知りたいことの一つに、現状把握がある。それは、対策の過不足を認識するため、そして他者に説明できるようにするためである。さらには、把握できた事実から新たな建策をするツールにも使用する。

(イ) 上記目的を達成するための手段（対策クラス）を特定する。その時、リポジトリを参照して、どの対策クラスを利用するか検討する。

⇒WG で作成したリポジトリ(表 9)を用いて対策クラス(図 37)を整理した。この中で対策がどのように配置(つまりマップ)されるか分かることが、得るところとなる。

3. 対策マップの描画

(ア) 対策対象の脅威、資産、場所などの観点を軸に、個々の対策クラスを並べる。

⇒描画には、GMITS [10](図 36)で用いられている資産、脅威、Safeguard(対策)の関係図をベースにした。円形での表現は、各の位置関係が分かりやすいからだ。GMITS は古典の部類に入る文献ではあるが、現在でも活きていると言える。ただし、全く同一ではなく、下記の解説において、その点含めて述べる。

脅威については、CWE [11]の階層構造図に倣って作成された JVN iPedia が使用する脆弱性タイプ [12] から、逆算するようにして想定(代用)した。対策が WG 由来なのに対して、客観性を担保するために脅威は、あえて WG 外から用意した。

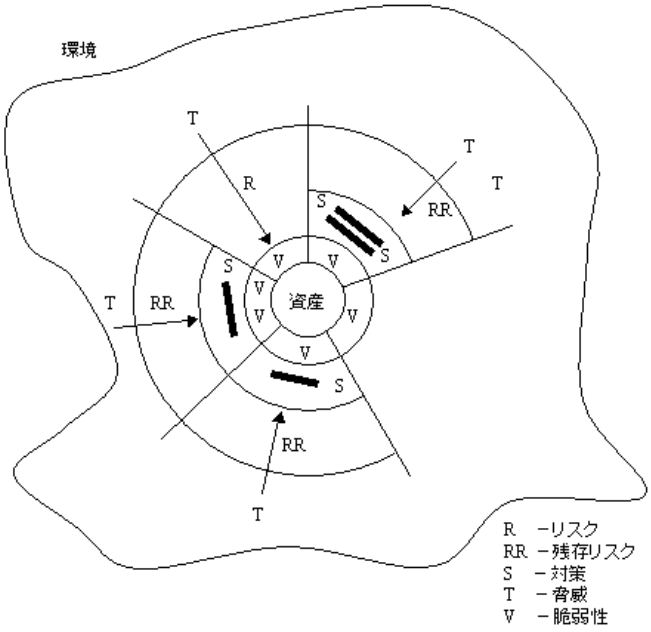


図 36 GMITS のリスク概念図

GMITS [10]より引用

JVN iPedia ベースの脅威と WG で整理した対策クラスの関係を、紐付けするために作成したのが下表である。これにより、資産価値を損なうリスクをもたらす脅威と呼応する対策との関係が結び付けられた。

図 37 脅威と対策の関係整理表

（原寸大の資料は別冊資料編を参照）

「次世代ファイアウォール」のように脅威への対応能力の高いものや、逆に「情報漏えい」の

ように、広汎な対策が求められるものが浮き彫りになった。なお、「JVN iPedia が使用する脆弱性タイプ」は、あくまで脆弱性のリストなので、脅威として捉え直しにくいもの(「情報不足」など)は省いてある。結果として、作成された対策マップが下図である。資産を中心に、外周に脅威があり、その間に対策が同心円上に挟み込まれた形になっている。

以下に解説をする。

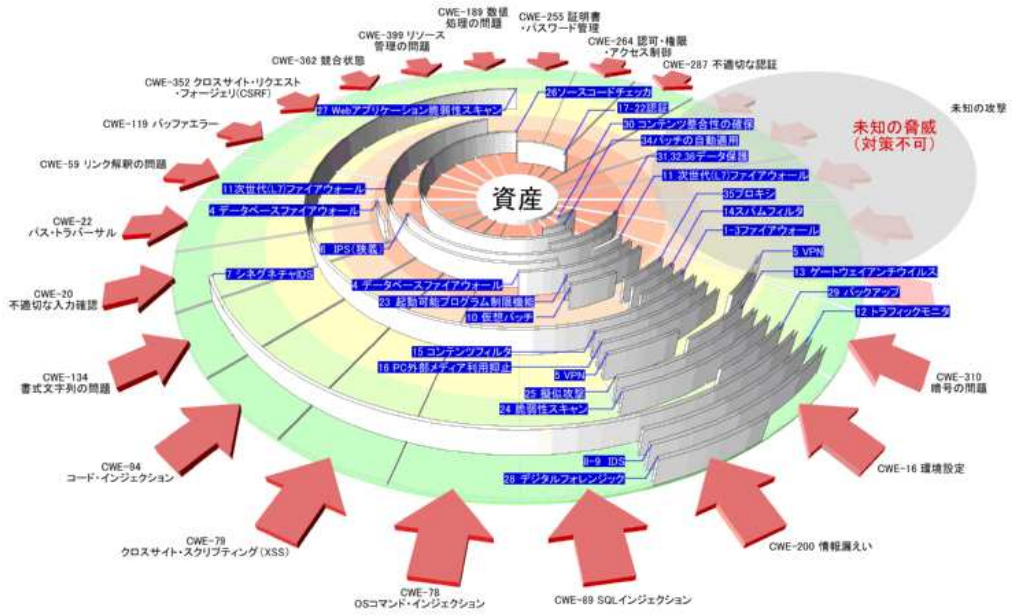


図 38 マップ作成例その3 「脅威に対抗するセキュリティ対策マップ」

（原寸大の資料は別冊資料編を参照）

<u>各パーツ</u>

資産：中心にある通り、対策を検討する起点である。ここでは特定せずに汎用的な資産とした。また中心からの距離により対策には意味を持たせたのが特徴である。

脅威：円の外周に配置されている脅威は、「JVN iPedia が使用する脆弱性タイプ」 から脆弱性をリストして、それを脅威に見立て直したものである。

並び方に絶対的な意味は無いので、外周部の位置は調整可能である。つまり、対策マップ利用者が、脅威の位置関係で意味を持たせたければ、資産との位置関係を侵すことなく操作可能である。

対策：

描画中、円弧のブロックで表記されている。弧の長さは守備範囲を意味する。また中心に

近いものほど、資産に直接対応している対策である。仮に中心点から遠い順に、緑系、黄色系、赤系に色分けしたゾーンとすると描画中では、次の 3 ゾーンと実際の内容がある。

ゾーン:

緑系. 抑止･回復系

黄色系. ネットワークでの制御

赤系. 資産に直接的に作用

ここでの対策マップの見方

資産と脅威の間に、どれだけの対策が施されているかを見ることが第一歩となる。上図は、典型的な配置であり、対策の疎密が明らかだろう。多重防護の観点から、複数の対策が資産と脅威の間にあるべきである。問題はバランスである。密であれば当然強固であるわけだが、場合によっては見直しの対象にもなる。疎であれば十分性に視察を入れた方が良いと言える。

WG では、スイスチーズモデル[12]と比較する意見が出た。このモデルは、穴の空いたスイスチーズを並べた時、全てのチーズの穴が通貫しうる偶発性から、リスクが現実化する可能性を示唆するものである。

図 38 で、緑系、黄色系、赤系の各ゾーンは、独立しているためスイスチーズのように扱えるだろう。仮に、各ゾーンの予算枠が一定のような制約があれば、用意できる対策枠にも制限があるはずである。たとえば未知の脅威が特定された時、対策を追加すると、どこかが手薄になることが予想される。また対策クラスの大きさを変えず、ゾーンの円弧を回して対応すると、外周から見て空隙が生ずるか、をシミュレーションするようなことが可能となる。

今後の余地:

変数として、対策である円弧の幅、厚さ、面積、色、3D にした場合の高さ表現、さらに外周に配置した脅威の角度幅に拡張の余地があると WG では議論になった。脅威には発生頻度も変数になるので、このマップ上でシミュレーションする案もあった。また図 38 は報告上きれいなイラストになっているが、WG では描画にプレゼンテーション･ツール(Power Point)を用いたため、表現には限界があったのも事実である。図 37 の作表から、図 38 に自動展開するツールの作成には時間が足らなかった。これらは、今後の課題である。

6 結論

本 WG で得られた成果を要約すると以下の通りである。

・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。

これにより、本 WG の設立目的であった

- 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

の作成はいずれも達成することができた。

なお、以下のテーマは本 WG でコンセプトは提示されたものの、時間制約などの関係でなし得なかった。今後の課題として次世代に期待したい。

・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（図 39）。

・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。

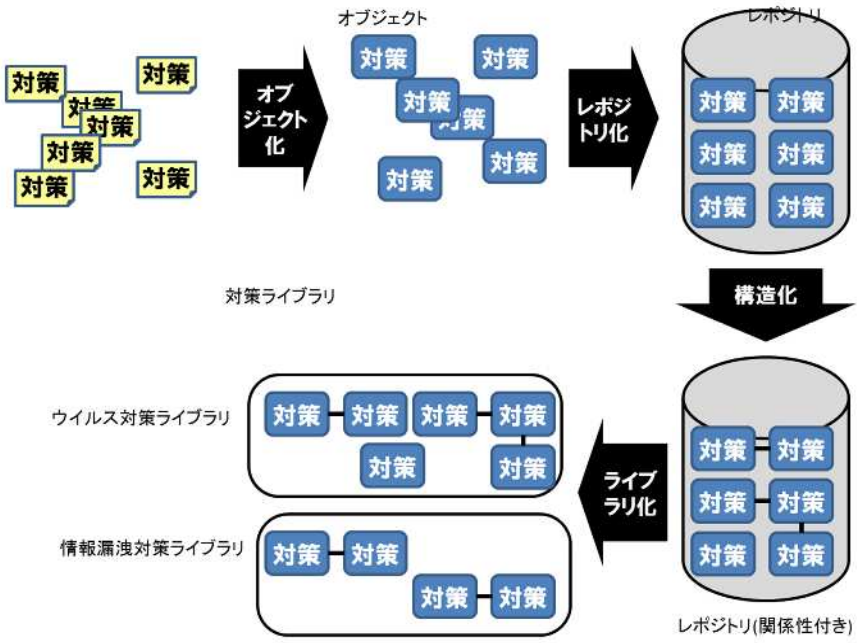


図 39 情報セキュリティ対策のリポジトリ構築とライブラリ化

7 謝辞

「だからたとえば、ファンタージエンの地図をつくることはまったく不可能なことだ。」

― ミヒャエル・エンデ『はてしない物語』

本 WG が成果をまとめるにあたり、数多くの皆様のご協力をいただきました。

まず当初3年といいながら大幅に活動年限を超過しながら、その間暖かい目で活動を許可していただいた NPO 日本ネットワークセキュリティ協会（JNSA）の田中英彦会長、下村正洋事務局長、中尾康二標準化部会長始め役員の方々に御礼とお詫びを申し上げます。すみません、やっと出来上がりました。

また、活動中有形無形さまざまなご協力をいただいた JNSA 事務局の皆様にも厚く御礼申し上げます。いただいた差し入れは決して公平とは言えない形でメンバーで分け合っていただきました。

今回の WG の成果であるサンプル地図をすばらしい形に仕上げていただいたアーバンアンドの田川澄恵様、おそらく他ではありえない不可解なお仕事にお付き合いいただき、本当にありがとうございました。

本 WG の活動場所として新宿キャンパスの JNSA プロジェクトルームをご提供いただいた工学院大学様にも感謝の言葉を述べさせていただきたいと思います。ありがとうございました。あの無数の機材が詰め込まれ、四六時中ファンの音が響き渡る愛すべきプロジェクトルームを私たちは生涯忘れないでしょう。

活動にあたりさまざまな助言をいただいた JNSA の許先明様、二木真明様始め各 WG のリーダーおよびメンバーの皆様にもこの場を借りてお礼申し上げます。

JNSA の会議室にていつも私たちの活動をじっと見守ってくれた経済産業省のしえな様とせりな様にもありがとうと言いたいと思います。今度クリアファイルください。

IPC 生産性国際交流センター様には成果物作成合宿のための大変快適な場所をご提供いただきました。湘南の豊かな自然の中で、成果物作成が大変捗りました。しらす海鮮丼おいしかったです。コンビニが近くにあるともっとよかったです。

最後に、長い間活動にお付き合いいただいた本 WG のメンバー全員に心よりお礼を言いたいと思います。お疲れさまでした。誰か世界地図作ってください。

8 WG 活動の軌跡

準備会

日時：2008 年 12 月 10 日(水) 18:00～20:00
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者（順不同、敬称略。以下同じ）：佳山、永沼、秋山、酒井、関取、井出、古村、本川、鈴木、大橋、浅尾、田中、小橋、渡邉、塚田、北村、やすだ、長谷川、奥原
検討内容
・設立趣旨説明、参加者自己紹介
・事例紹介（SANS）
・「情報セキュリティマップとは何か」についてブレインストーミング
・リーダー・サブリーダー選出

2009 年度活動

第 1 回 WG

日時：2009 年 1 月 7 日(水) 18:00～20:00
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：佳山、松井、古村、酒井、田中、やすだ、勝見、宮永、北村、若林、浅尾、小橋、本川、谷口、鈴木、服部、馬場、渡邉、塚田、長谷川、奥原
検討内容
・「私が情報セキュリティマップと思うもの」資料の持ち寄りと紹介（13 種類）
・資料に対する意見交換
・「情報セキュリティマップとは何か」について再度ブレインストーミング
・WG に提供された情報の取扱いルールについての合意

第 2 回 WG

日時：2009 年 1 月 28 日（水） 18:00～20:00
場所：JNSA 西新橋 JC ビル 1F 大会議室
参加者：佳山、北村、宮永、馬場、酒井、本川、塚田、渡邊、大谷、吉村、松井、古村、田中、やすだ、長谷川、鈴木、奥原
検討内容
・前回のセキュリティマップの分析についての資料、および情報セキュリティマップ例の追加資料持ち寄り（11 種類）
・持ち寄り資料の紹介、質疑応答
・MECE（mutually exclusive, collectively exhaustive）という概念の紹介
・マップの分類についての提案と意見交換

第 3 回 WG

日時：2009 年 2 月 10 日（火） 18:00～20:00
場所：JNSA 西新橋 JC ビル 1F 大会議室
参加者：北村、渡邉、塚田、小橋、酒井、田中、本川、宮永、安達、宍戸、井出、長谷川、奥原
検討内容
・WG の運営についての取り決め
・マップの分類についてのコンセプト提言
・マップに MECE をどの程度求めるべきかについての議論
・天気図をセキュリティマップに応用できないか

第 4 回 WG

日時：2009 年 2 月 26 日（木） 18:00～20:00
場所：JNSA 西新橋 JC ビル 1F 大会議室
参加者：北村、田中、井出、安達、本川、吉村、松井、馬場、長谷川、鈴木、奥原
検討内容
・セキュリティ対策分類の先行調査事例の紹介
・マップを作成する「軸」についての検討
・セキュリティ対策を集めてから考える「昆虫採集アプローチ」の検討

第 5 回 WG

日時：2009 年 3 月 11 日（水） 18:00～19:30
場所：富士通本社 第 10 応接室
参加者：吉村、大谷、佳山、井出、北村、古村、宍戸、安達、本川、塚田、渡邉、酒井、小橋、田中、宮永、鈴木、松井、長谷川、奥原
検討内容
・対策を正確に記述するための方法
・マップを構成する軸の候補
・マップの目的の整理
・「セキュリティ対策収集」の試行結果の紹介

・第1回懇親会実施（3 月 11 日）、新橋、参加 19 名。
・JNSA Press Vol.25（2009 年 3 月発行）に WG 活動が掲載される。

第 6 回 WG

日時：2009 年 4 月 8 日（水） 18:00～20:00
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：北村、古村、田中、宍戸、大谷、井出、やすだ、

松井、浅尾、塚田、佳山、長谷川、奥原
検討内容
・これまでの検討の整理
・「経営者の安心感」とセキュリティ対策指標化
・SANS「What Works」の分析
・「セキュリティ対策整理」の試行結果紹介

第 7 回 WG

日時：2009 年 4 月 28 日（火） 18:30～20:30
場所：富士通本社 第 14 応接室
参加者：春山、大谷、古村、井出、佳山、田中、北村、塚田、宍戸、松井、酒井、安達、鈴木、浅尾、渡邊、長谷川、奥原
検討内容
・「昆虫採集」の進め方／対象となるガイドライン候補の整理
・「コンセプト」の進め方／地図の目的・使い方の整理

第 8 回 WG

日時：2009 年 5 月 19 日（火） 18:30～20:30
場所：富士通本社 第 10 応接室
参加者：田中、北村、本川、塚田、渡邊、松井、浅尾、長谷川、奥原
検討内容
・「昆虫採集」対象場所のグルーピング、位置付け整理
・「コンセプト」地図の使い方、目的についての討論

2009 年度活動報告会

日時：2009 年 6 月 3 日（水） 11:25～11:40
場所：ベルサール神田 room3+room4
報告内容
・WG 活動の目的、問題提起
・これまでの活動内容

第 9 回 WG

日時：2009 年 6 月 10 日（水） 18:00～20:00
場所：JNSA 西新橋 JC ビル 1F 大会議室
参加者：塚田、渡邊、酒井、鈴木、大谷、田中、宮永、宍戸、安達、小橋、北村、長谷川、奥原
検討内容
・活動報告会および総会の状況報告
・昆虫採集チーム
・「認証」「ウイルス対策」のテーマで、各ガイドラインの記述の比較検討
・「対策」「要件」「管理策」の意味の違いについての議論
・コンセプトチーム
・「被害」「コスト」の考え方についての議論
・IPA ベンチマークの紹介

第 10 回 WG

日時：2009 年 7 月 1 日（水） 18:00～20:20
場所：JNSA 西新橋 JC ビル 1F 大会議室
参加者：塚田、渡邊、安達、佳山、田中、宍戸、井出、北村、大谷、松井、長谷川、奥原
・検討内容：
・マップをテーマとしている他 WG との調整状況報告
・昆虫採集チーム
・各ガイドラインの記述の比較検討（前回の続き）
・「対策」の部品と登場人物の整理
・コンセプトチーム
・IPA ベンチマークの内容分析
・ここまでの課題の整理

第 11 回 WG

日時：2009 年 7 月 15 日（水） 18:00～20:00
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大津、宍戸、宮永、渡邊、田中、松井、北村、鈴木、長谷川、奥原
検討内容：
・「対策構造」について各自アイディアの持ち寄りと検討
・FISC の要求項目分析

第 12 回 WG

日時：2009 年 7 月 29 日（水） 18:00～20:00
場所：西新橋 JC ビル 1 階 大会議室
参加者：佳山、藤井、佐藤、鈴木、塚田、渡邊、田中、松井、宍戸、北村、やすだ、長谷川、奥原
検討内容：
・やすださんよりスキルマップのご紹介
・セキュリティ対策の構造についての検討

第 1 回定量的リスクアセスメントについて考える BoF

日時：2009 年 8 月 19 日（水） 15:00～17:00
場所：西新橋 JC ビル 1 階 大会議室
・主催：JNSA 標準化部会＋情報セキュリティ対策マップ検討 WG
・企画担当：住商情報システム株式会社 二木真明

第 13 回 WG（ISOG-J WG1 合同開催）

日時：2009 年 8 月 19 日（水） 18:00～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：
ISOG-J WG1：許、齋藤、武智、川崎、ももい
マップ検討 WG：北村、松井、大谷、藤井、宍戸、佳山、鈴木、酒井、安達、渡邊、佐藤、菊地、塚田、長谷川、奥原
検討内容：
・ISOG-J WG1 の皆様との意見交換（セキュリティサービスッップ）

第 14 回 WG

日時：2009 年 9 月 3 日（木） 18:15～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室

参加者：北村、藤井、佐藤、宍戸、安達、本川、小橋、渡邊、塚田、大谷、長谷川、奥原
・検討内容：
・対策構造図の検討
・対策構造に基づく各種ガイドラインの分類試行
・アクター（登場人物）の整理

第 15 回 WG

日時：2009 年 9 月 16 日（水） 18:15～20:15
場所：西新橋 JC ビル
参加者：藤井、佐藤、鈴木、松井、宍戸、酒井、菊地、田中、塚田、渡邊、大谷、やすだ、長谷川、奥原
検討内容：
・対策構造図の検討
・対策構造に基づく各種ガイドラインの分類試行

第 16 回 WG

日時：2009 年 10 月 1 日（木） 18:15～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：北村、本川、藤井、大谷、田中、塚田、長谷川、奥原
検討内容：
・対策構造図の検討（継続）
・対策構造に基づく各種ガイドラインの分類試行（継続）

第 17 回 WG

日時：2009 年 10 月 14 日（水） 18:15～21:00
場所：西新橋 JC ビル 大会議室
参加者：藤井、松井、田中、大谷、塚田、安達、宍戸、北村、やすだ、長谷川、奥原
検討内容：
・対策構造図の検討（継続）
・対策構造に基づく各種ガイドラインの分類試行（継続）
・この日は大雨（参考）

第 18 回 WG

日時：2009 年 10 月 29 日（木） 18:15～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：松井、宍戸、安達、本川、田中、菊地、北村、塚田、佐藤、藤井、大谷、長谷川、奥原
検討内容：
・対策構造図の検討（継続）
・対策構造に基づく 27002 の分類試行

第 19 回 WG

日時：2009 年 11 月 11 日（水） 18:15～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、北村、田中、宍戸、本川、藤井、松井、塚田、長谷川、奥原
検討内容：
・対策構造図の検討（継続）
・対策構造に基づく 27002（つづき）と SP800-53 の分類試行

第 20 回 WG

日時：2009 年 11 月 25 日（水） 18:15～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：北村、大谷、松井、渡邊、安達、田中、藤井、本川、菊地、塚田、長谷川、奥原
検討内容：
・対策構造の検討（継続）、地図化の方向の検討
・対策構造に基づく FISC の分類試行

第 2 回定量的リスクアセスメントについて考える BoF

日時：2009 年 12 月 9 日（水） 15:00～17:00
場所：西新橋 JC ビル 1 階 大会議室
主催：JNSA 標準化部会＋情報セキュリティ対策マップ検討 WG

第 21 回 WG

日時：2009 年 12 月 9 日（水） 18:15～20:15
場所：西新橋 JC ビル 大会議室
参加者：大谷、塚田、菊地、田中、佐藤、藤井、やすだ、長谷川、奥原
検討内容：
・対策構造の検討（継続）
・標準文法の検討

第 22 回 WG

日時：2009 年 12 月 21 日（月） 18:15～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：安達、宍戸、田中、菊地、藤井、長谷川、奥原
検討内容：
・対策構造の検討（継続）
・標準文法の検討（継続）

第 23 回 WG

日時：2010 年 1 月 13 日（水） 18:15～20:15
場所：西新橋 JC ビル 大会議室
参加者：藤井、宍戸、田中、やすだ、大谷、松井、北村、長谷川、奥原
検討内容：
・標準文法の検討（27002 の分類試行、典型的動詞の洗い出し）

第 24 回 WG

日時：2010 年 1 月 25 日（水） 18:15～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：松井、田中、本川、藤井、大谷、長谷川、奥

原
検討内容:
・標準文法の検討(27002 への適用再試行)

Network Security Forum 2009

日時:2010 年 1 月 27 日
場所:ベルサール神田
内容:リスク定量化 BoF、セキュリティ被害調査 WG などと合同でパネルディスカッション

第 25 回 WG

日時:2010 年 2 月 10 日(水) 18:15〜20:15
場所:西新橋 JC ビル 大会議室
参加者:塚田、宍戸、藤井、菊地、北村、やすだ、長谷川、奥原
検討内容:
・標準文法の検討(前回提案の構文規則による分解と分類の試行)

第 26 回 WG

日時:2010 年 2 月 24 日(水) 18:15〜19:45
場所:工学院大学 新宿校舎(中層棟) 5 階 570 号室
参加者:松井、北村、藤井、田中、大谷、宍戸、菊地、塚田、長谷川、奥原
検討内容:
・標準文法の検討(FISC の分解試行の持ち寄りと分析)
・久しぶりに懇親会を実施

第 27 回 WG

日時:2010 年 3 月 10 日(水) 18:15〜20:15
場所:西新橋 JC ビル 大会議室
参加者:田中、宍戸、安達、松井、本川、大谷、北村、やすだ、長谷川、奥原
検討内容:
・標準文法の検討(マルウェアの整理、アトムの検討)
・辞書の考え方の整理

第 28 回 WG

日時:2010 年 3 月 24 日(水) 18:15〜20:15
場所:工学院大学 新宿校舎(中層棟) 5 階 570 号室
参加者:大谷、田中、北村、菊地、長谷川、奥原
検討内容:
・辞書の考え方の整理(用語の構造など)

2010 年度活動

第 1 回(通算 29 回)WG

日時:2010 年 4 月 7 日(水) 18:30〜20:15
場所:工学院大学 新宿校舎(中層棟) 5 階 570 号室
参加者:北村、松井、藤井、大谷、田中、長谷川、奥原
検討内容:
・「マルウェア分県図」の試作(その1)

第 2 回(通算 30 回)WG

日時:2010 年 4 月 21 日(水) 18:30〜20:15
場所:西新橋 JC ビル 大会議室
参加者:田中、大谷、藤井、北村、長谷川、奥原
検討内容:
・「マルウェア分県図」の試作(その2)
・標準構文のあり方について

第 3 回(通算 31 回)WG

日時:2010 年 5 月 12 日(水) 18:30〜20:15
場所:工学院大学 新宿校舎(中層棟) 5 階 570 号室
参加者: 北村、松井、田中、本川、藤井、菊地、大谷、長谷川、奥原
検討内容:
・「マルウェア分県図」の試作(その 3)
・地図の作り方(方向性検討)

第 4 回(通算 32 回)WG

日時:2010 年 5 月 27 日(木) 18:30〜20:15
場所:西新橋 JC ビル 大会議室
参加者:藤井、本川、大谷、田中、北村、長谷川、奥原
検討内容:
・「マルウェア分県図」のクリーンアップ、分類の試行
・報告会資料の簡単なレビュー

第 5 回(通算 33 回)WG

日時:2010 年 6 月 9 日(水) 18:30〜20:15
場所:工学院大学 新宿校舎(中層棟) 5 階 570 号室
参加者:松井、北村、田中、本川、菊地、藤井、長谷川、奥原
検討内容:
・報告会資料のレビュー
・今後の WG の活動方向についての意見交換

2009 年度活動報告会

日時:2010 年 6 月 11 日(金) 12:50〜13:05
場所:ベルサール神保町

第 6 回(通算 34 回)WG

日時:2010 年 6 月 23 日(水) 18:30〜20:15

場所：西新橋 JC ビル　大会議室
参加者：大谷、藤井、松井、田中、北村、長谷川、奥原
検討内容：
・活動報告会の結果報告
・地図の構造について田中さんの資料ベースに検討（ツリー表現の考え方など）
・懇親会（新橋「わん」、B 級グルメフェア実施中）

第 7 回（通算 35 回）WG

日時：2010 年 7 月 7 日（水）18:30～20:15
場所：工学院大学　新宿校舎（中層棟）5 階　570 号室
参加者：藤井、田中、松井、菊地、長谷川、奥原
検討内容：
・地図の構造について（オブジェクト指向な書き方の導入など）
・「～のとき」の解釈の仕方（前提なのか、タイミングなのか）

第 8 回（通算 36 回）WG

日時：2010 年 7 月 21 日（水）18:30～20:15
場所：西新橋 JC ビル　大会議室
参加者：松井、田中、藤井、大谷、北村、長谷川、奥原
検討内容：
・地図の構造について（オブジェクト指向な書き方の導入など）の続き

第 9 回（通算 37 回）WG

日時：2010 年 8 月 11 日（水）18:30～20:15
場所：工学院大学　新宿校舎（中層棟）5 階　570 号室
参加者：北村、藤井、田中、本川、大谷、菊地、長谷川、奥原
検討内容：
・地図の構造について（ツリー構造の検討）
・従来の「分県図」と現在の「ツリー図」の関係の整理

第 10 回（通算 38 回）WG

日時：2010 年 8 月 25 日（水）18:30～20:15
場所：西新橋 JC ビル　大会議室
参加者：松井、藤井、大谷、長谷川、奥原
検討内容：
・対策オブジェクトのメソッドの整理
・従来の「分県図」と現在の「ツリー図」の関係の整理の続き

第 11 回（通算 39 回）WG

日時：2010 年 9 月 8 日（水）18:30～20:15
場所：西新橋 JC ビル　大会議室
参加者：松井、藤井、大谷、北村、長谷川、奥原
検討内容：
・「対策構造図」と「ツリー図」の関係の整理
・「ツリー図」の描き方の方針整理

第 12 回（通算 40 回）WG
日時：2010 年 9 月 29 日（水）18:30～20:15
場所：工学院大学　新宿校舎（中層棟）5 階　570 号室
参加者：田中、松井、藤井、大谷、菊池、長谷川、奥原
検討内容：
・「ツリー図」における対策のオブジェクト化の検討
・「ツリー図」のカテゴライズの方針の検討

第 13 回（通算 41 回）WG

日時：2010 年 10 月 21 日（木）18:30～20:15
場所：西新橋 JC ビル　大会議室
参加者：松井、藤井、大谷、本川、北村、田中、長谷川、奥原
検討内容：
・「マルウェア分県図」のアップデート

第 14 回（通算 42 回）WG

日時：2010 年 11 月 4 日（木）18:30～20:15
場所：工学院大学　新宿校舎（中層棟）5 階　570 号室
参加者：松井、藤井、大谷、菊地、北村、田中、長谷川、奥原
検討内容：
・ツリー図から地図への展開方法
・マルウェアツリー図の見直し

第 15 回（通算 43 回）WG

日時：2010 年 11 月 17 日（水）18:30～20:15
場所：西新橋 JC ビル　3 階会議室
参加者：松井、藤井、大谷、北村、田中、長谷川、奥原
検討内容：
・ツリー図から地図への展開方法（継続）
・マルウェアツリー図の見直し（継続）

第 16 回（通算 44 回）WG

日時：2010 年 12 月 8 日（水）18:30～20:15
場所：工学院大学　新宿校舎（中層棟）5 階　570 号室
参加者：菊地、北村、藤井、大谷、本川、田中、渡邉、塚田、長谷川、奥原
検討内容：
・ツリー図から地図への展開方法（継続）
・メソッドの再整理

第 17 回（通算 45 回）WG

日時：2010 年 12 月 22 日（水）18:30～20:15
場所：西新橋 JC ビル　3 階会議室
参加者：北村、藤井、大谷、松井、長谷川、奥原
検討内容：
・メソッドの再整理・可変なメソッドの抽出
・メソッド構造図の再整理

第 18 回（通算 46 回）WG

日時：2010 年 1 月 6 日（木） 18:30～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：北村、藤井、大谷、松井、本川、田中、菊地、長谷川、奥原
検討内容：
・マップの方向性についての振り返り
・ツリー図の整理方法についての振り返り
・認証ツリーの試作

第 19 回（通算 47 回）WG

日時：2010 年 1 月 19 日（水） 18:30～20:15
場所：西新橋 JC ビル 3 階会議室
参加者：北村、藤井、大谷、松井、奥原、岡谷（NISC、ゲスト）
検討内容：
・NSF2011 資料レビュー
・WG 活動についての意見交換
・対策オブジェクトモデルの仕様凍結

Network Security Forum 2011

日時：2011 年 1 月 25 日（火） 16:00～16:30
場所：ベルサール神田

第 20 回（通算 48 回）WG

日時：2010 年 2 月 2 日（水） 18:30～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：北村、田中、藤井、本川、大谷、菊地、松井、長谷川、奥原
検討内容：
・NSF2011 結果報告
・今後の WG の進め方について

第 21 回（通算 49 回）WG

日時：2010 年 2 月 16 日（水） 18:30～20:15
場所：西新橋 JC ビル 3 階会議室
参加者：北村、松井、大谷、奥原
検討内容：
・マルウェア分県図の再構成

第 22 回（通算 50 回）WG

日時：2010 年 3 月 2 日（水） 18:30～20:15
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：松井、田中、大谷、藤井、菊地、長谷川、奥原
検討内容：
・脅威、リスクと対策の関係と取り扱い
・リスク分析ツール CRAMM の情報共有
・2011 年度の検討方向性

2011 年度活動

第 1 回（通算 51 回）WG

日時：2011 年 4 月 6 日（水） 18:30～20:30
場所：西新橋 JC ビル 大会議室
参加者：田中、松井、藤井、大谷、菊地、奥原
検討内容：
・リスク分析ツール CRAMM の評価
・2011 年度の検討方向性

第 2 回（通算 52 回）WG

日時：2011 年 4 月 20 日（水） 18:30～20:30
場所：西新橋 JC ビル 大会議室
参加者：藤井、田中、菊地、大谷、松井、奥原
検討内容：
・CRAMM の対策モデル評価
・「目的由来の対策」と「機能由来の対策」の分離

第 3 回（通算 53 回）WG

日時：2011 年 5 月 11 日（水） 18:30～20:30
場所：西新橋 JC ビル 大会議室
参加者：藤井、田中、奥原
検討内容
・「目的」「手段」の分離モデル（三途の川モデル）によるツリー作成の試行

第 4 回（通算 54 回）WG

日時：2011 年 5 月 25 日（水） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室

第 5 回（通算 55 回）WG

日時：2011 年 6 月 1 日（水） 18:30～20:30
場所：西新橋 JC ビル 大会議室
参加者：大谷、菊地、田中、藤井、松井、奥原
検討内容：
・三途の川モデルによるマルウェア対策全体マップの試作

2010 年度活動報告会

日時：2011 年 6 月 8 日（水）10:30～10:45
場所：アルカディア市ヶ谷
内容：活動中間報告（15 分）

第 6 回（通算 56 回）WG

日時：2011 年 6 月 22 日（水） 18:30～20:30

場所：工学院大学　新宿校舎（中層棟）　5 階　570 号室
参加者：大谷、田中、松井、長谷川、奥原
検討内容：
・活動報告会発表の振り返り
・今後の方向性の検討（地図を広げていくか、新しい地図を考えるか）

第 7 回（通算 57 回）WG

日時：2011 年 7 月 6 日（水）　18:30～20:30
場所：西新橋 JC ビル　大会議室
参加者：大谷、近藤、田中、藤井、長谷川、八鍬、奥原
検討内容：
・川モデルの表現についての検討
・認証のツリーの作成試行について
・アクセス制御のツリー作成の進め方について

第 8 回（通算 58 回）WG

日時：2011 年 8 月 3 日（水）　18:30～20:30
場所：工学院大学　新宿校舎（中層棟）　5 階　570 号室
参加者：大谷、菊地、田中、藤井、長谷川、松井、奥原
検討内容：
・アクセス制御のツリーの正規化

第 9 回（通算 59 回）WG

日時：2011 年 8 月 24 日（水）　18:30～20:30
場所：西新橋 JC ビル　大会議室
参加者：大谷、菊地、田中、藤井、長谷川、松井、奥原
検討内容：
・アクセス制御の項目の正規化（つづき）

第 10 回（通算 60 回）WG

日時：2011 年 9 月 7 日（水）　18:30～20:30
場所：工学院大学　新宿校舎（中層棟）　5 階　570 号室
参加者：大谷、藤井、長谷川、松井、本川、奥原
検討内容：
・アクセス制御の項目のツリー化（その1）

メモ：9 月 21 日の WG は台風のため中止

第 11 回（通算 61 回）WG

日時：2011 年 10 月 5 日（水）　18:30～20:30
場所：工学院大学　新宿校舎（中層棟）　5 階　570 号室
参加者：大谷、藤井、長谷川、松井、奥原
検討内容：
・アクセス制御の項目のツリー化（その2）

第 12 回（通算 62 回）WG

日時：2011 年 10 月 19 日（水）　18:30～20:30
場所：西新橋 JC ビル　大会議室
参加者：大谷、長谷川、藤井、松井、奥原
検討内容：
・アクセス制御の項目のツリー化まとめ

第 13 回（通算 63 回）WG

日時：2011 年 11 月 2 日（水）　18:30～20:30
場所：富士通本社（汐留）
参加者：大谷、菊地、田中、塚田、長谷川、藤井、松井、奥原
検討内容：
・ツリーマップ振り返り
・シンガポールチキンライスの集い

第 14 回（通算 64 回）WG

日時：2011 年 11 月 16 日（水）　18:30～20:30
場所：工学院大学　新宿校舎（中層棟）　5 階　570 号室
参加者：大谷、長谷川、藤井、奥原
検討内容：
・マップモデルの構造検討

第 15 回（通算 65 回）WG

日時：2011 年 11 月 30 日（水）　18:30～20:30
場所：西新橋 JC ビル　3 階会議室
参加者：大谷、菊地、田中、長谷川、藤井、奥原
検討内容：
・対策オブジェクトの構造検討（特にプロパティの取り扱いについて）
・スマートフォンによるピザの注文方法について

第 16 回（通算 66 回）WG

日時：2011 年 12 月 14 日（水）　18:30～20:30
場所：工学院大学　新宿校舎（中層棟）　5 階　570 号室
参加者：菊地、藤井、長谷川、奥原
検討内容：
・対策オブジェクトの構造検討（特にプロパティの取り扱いについて、のつづき）
・2011 年度の検討方向性
・辞書の考え方の整理（用語の構造など）

第 17 回（通算 67 回）WG

日時：2012 年 1 月 11 日（水）　18:30～20:30
場所：西新橋 JC ビル　3 階会議室
参加者：大谷、長谷川、藤井、松井、奥原
検討内容：
・NSF 資料レビュー
・対策オブジェクトの構造検討（特にプロパティの取り扱いについて、のつづき

Network Security Forum 2012

日時：2012 年 1 月 25 日（水）
場所：ベルサール神田
内容：パネルディスカッション参加

第 18 回（通算 68 回）WG

日時：2012 年 2 月 1 日（水） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、菊地、藤井、長谷川、奥原
検討内容：
・地図の書き方について
・2012 年度の検討方向

第 19 回（通算 69 回）WG

日時：2012 年 2 月 15 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、田中、藤井、松井、長谷川、奥原
検討内容：
・2012 年度の検討方向（つづき）
・APT とか

第 20 回（通算 70 回）WG

日時：2012 年 2 月 29 日（水） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、菊地、田中、藤井、長谷川、奥原
検討内容：
・2012 年度の検討方向（つづき）

2012 年度活動

第 1 回（通算 71 回）WG

日時：2012 年 4 月 11 日（水） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、菊地、田中、藤井、松井、長谷川、奥原
検討内容：
・2011 年度活動報告会の方向性検討
・ISO27002 かるた取り大会

第 2 回（通算 72 回）WG

日時：2012 年 4 月 25 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、田中、藤井、松井、長谷川、奥原
検討内容：
・ISO27002 かるた取り大会の振り返り

第 3 回（通算 73 回）WG

日時：2012 年 5 月 9 日（水） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、菊地、長谷川、奥原
検討内容：
・2011 年度活動報告会の BoF プラン検討
・宿題持ち寄り（27002 正規化）
・ISO27002 かるた取り大会（その 2）

第 4 回（通算 74 回）WG

日時：2012 年 5 月 23 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
＊JNSA 賞受賞記念パーティー併催
参加者：大谷、菊地、田中、藤井、松井、長谷川、奥原
検討内容：
・2011 年度活動報告会の BoF プラン検討
・ISO27002 かるた取り大会の振り返り

第 5 回（通算 75 回）WG

日時：2012 年 6 月 6 日（水） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、菊地、藤井、松井、長谷川、奥原
検討内容：
・2011 年度活動報告会の BoF 事前打ち合わせ
・ISO27002 分析振り返り

2011 年度活動報告会

日時：2012 年 6 月 8 日（金）13:05
場所：ベルサール神田
タイトル：「標的型攻撃時代に必要な情報セキュリティ対策マップとは」

第 6 回（通算 76 回）WG

日時：2012 年 6 月 27 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：菊地、戸田、藤井、松井、長谷川、奥原
検討内容：
・2012 年度活動報告会の BoF 振り返り
・ISO27002 再分析

第 7 回（通算 77 回）WG

日時：2012 年 7 月 11 日（水） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、菊地、戸田、藤井、奥原
検討内容：
・27002 の管理策の標準化

第 8 回（通算 78 回）WG

日時：2012 年 8 月 1 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、戸田、藤井、松井、長谷川、奥原
検討内容：
・27002 の管理策の標準化（つづき）

第 9 回（通算 79 回）WG

日時：2012 年 8 月 20 日（月） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、菊地、戸田、藤井、松井、長谷川、奥原
検討内容：
・27002 の管理策の標準化（その3）

第 10 回（通算 80 回）WG

日時：2012 年 9 月 5 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、田中、藤井、松井、長谷川、奥原
検討内容：
・27002 の管理策の標準化（その4）

第 11 回（通算 81 回）WG

日時：2012 年 9 月 29 日（水） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、菊地、戸田、長谷川、奥原
検討内容：
・27002 の管理策の標準化（その 5）

第 12 回（通算 82 回）WG

日時：2012 年 10 月 3 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：菊地、田中、戸田、長谷川、藤井、松井、奥原
検討内容：
・マップの方向性について（振り返りと今後の方針討議）

第 13 回（通算 83 回）WG

日時：2012 年 10 月 24 日（水） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、菊地、田中、長谷川、藤井、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（ISO/IEC 27033 ベース）

第 14 回（通算 84 回）WG

日時：2012 年 11 月 7 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、長谷川、藤井、松井、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（SP800-53 ベース）

第 15 回（通算 85 回）WG

日時：2012 年 11 月 21 日（水） 18:30～20:30
場所：工学院大学 新宿校舎（中層棟） 5 階 570 号室
参加者：大谷、菊地、戸田、藤井、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（市販製品ベース）

第 16 回（通算 86 回）WG

日時：2012 年 12 月 5 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、田中、戸田、長谷川、藤井、松井、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（市販製品ベースその2）

第 17 回（通算 87 回）WG

日時：2012 年 12 月 19 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、田中、戸田、長谷川、藤井、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（市販製品ベースその2）

第 18 回（通算 88 回）WG

日時：2013 年 1 月 9 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、田中、戸田、長谷川、藤井、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（市販製品ベースその3）

第 19 回（通算 89 回）WG

日時：2013 年 1 月 23 日（水） 18:30～20:30
場所：日本オラクル 会議室
参加者：大谷、菊地、松井、長谷川、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（IPA 出口対策ベースその1）

第 20 回（通算 90 回）WG

日時：2013 年 2 月 6 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、田中、戸田、松井、長谷川、藤井、奥原
検討内容：

・「機能要素」に着目した要件の整理の試行（IPA 出口対策ベースその2）

第 21 回（通算 91 回）WG

日時：2013 年 2 月 20 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、田中、長谷川、藤井、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（IPA 出口対策ベースその2）

第 22 回（通算 92 回）WG

日時：2013 年 3 月 6 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、田中、戸田、松井、長谷川、藤井、しえな（経済産業省）、せりな（経済産業省）、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（IPA 出口対策ベースその3）

第 23 回（通算 93 回）WG

日時：2013 年 3 月 27 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、塚田、松井、長谷川、藤井、奥原
検討内容：
・ 地図を書くプロセスの整理（その1）

2013 年度活動

第 1 回（通算 94 回）WG

日時：2013 年 4 月 10 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、土屋、戸田、藤井、松井、長谷川、奥原
検討内容：
・ 地図を書くプロセスの整理（その2）

第 2 回（通算 95 回）WG

日時：2013 年 4 月 24 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、佐々木、田中、戸田、藤井、西谷、長谷川、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（IPA 出口対策ベースその4）

第 3 回（通算 96 回）WG

日時：2013 年 5 月 8 日（水） 18:30～20:30
場所：富士通本社会議室
参加者：大谷、佐々木、田中、戸田、藤井、西谷、長谷川、奥原
検討内容：
・「機能要素」に着目した要件の整理の試行（IPA 出口対策ベースその5）

第 4 回（通算 97 回）WG

日時：2013 年 5 月 22 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、佐々木、土屋、藤井、松井、長谷川、奥原
検討内容：
・ モデルの整理
・ 活動報告会内容検討

第 5 回（通算 98 回）WG

日時：2013 年 6 月 5 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、土屋、戸田、西谷、藤井、松井、右松、長谷川、奥原
検討内容：
・ いままでの活動振り返り
・ 活動報告会プレゼンレビュー

2012 年度活動報告会

日時：2013 年 6 月 7 日（金） 10:50-11:20
場所：秋葉原 UDX NEXT1
タイトル：「情報セキュリティ対策マップ検討 WG 活動報告 －セキュリティ対策の構造と戦った4年間－」

第 6 回（通算 99 回）WG

日時：2013 年 6 月 19 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：土屋、戸田、西谷、藤井、松井、奥原
検討内容：
・ 活動報告会の結果分析
・ 今後の活動方向検討
・ WG100 回記念パーティー検討

第 7 回（通算 100 回）WG

日時：2013 年 7 月 3 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、土屋、西谷、長谷川、藤井、松井、右松、奥原
検討内容：
・ 対策分類ルールの見直し（付帯的対策の扱いの見直し）
・ WG100 回記念祝賀パーティー

第 8 回（通算 101 回）WG

日時：2013 年 7 月 17 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、戸田、長谷川、藤井、奥原
検討内容：
・JNSA 市場調査のカテゴリとのマッチングについての検討（その1）

第 9 回（通算 102 回）WG

日時：2013 年 7 月 31 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、西谷、長谷川、藤井、奥原
検討内容：
・JNSA 市場調査のカテゴリとのマッチングについての検討（その2）

第 10 回（通算 103 回）WG

日時：2013 年 8 月 21 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：土屋、田中、戸田、西谷、長谷川、藤井、堀江（ウォッチガード）、松井、奥原
検討内容：
・JNSA 市場調査のカテゴリとのマッチングについての検討（その3）
・メソッドの整理、「フレームワーク」の位置付けの再検討

第 11 回（通算 104 回）WG

日時：2013 年 9 月 4 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、土屋、長谷川、藤井、松井、奥原
検討内容：
・「ルール」の扱いについての検討
・フレームワークの位置付けの整理

第 12 回（通算 105 回）WG

日時：2013 年 9 月 18 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、戸田、西谷、長谷川、松井、奥原
検討内容：
・「ルール」の扱いについての検討（その2）

第 13 回（通算 106 回）WG

日時：2013 年 10 月 2 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、戸田、西谷、長谷川、松井、奥原
検討内容：
・「ルール」の扱いについての検討（その3）

（中止）

日時：2013 年 10 月 16 日（水） 18:30～20:30
台風 26 号接近のため開催中止

第 14 回（通算 107 回）WG

日時：2013 年 10 月 30 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：菊地、戸田、西谷、長谷川、藤井、松井、奥原
検討内容：
・検討結果のマップ化について

第 15 回（通算 108 回）WG

日時：2013 年 11 月 13 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、田中、土屋、西谷、長谷川、藤井、松井、奥原
検討内容：
・JNSA 市場調査のカテゴリとのマッチングについての検討（その4）
・検討結果のマップ化について（その2）
・活動報告書の目次検討（その1）

第 16 回（通算 109 回）WG

日時：2013 年 11 月 27 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、西谷、長谷川、藤井、奥原
検討内容：
・検討結果のマップ化について（その3）

第 17 回（通算 110 回）WG

日時：2013 年 12 月 11 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：菊地、土屋、戸田、西谷、長谷川、藤井、松井、奥原
検討内容：
・「セキュリティマップ」の概念について（その1）

第 18 回（通算 111 回）WG

日時：2013 年 12 月 25 日（水） 18:30～20:30
場所：富士通本社会議室
参加者：大谷、菊地、田中、土屋、戸田、西谷、藤井、奥原
検討内容：
・「セキュリティマップ」の概念について（その2）
・標的型攻撃対策マップの整理

第 19 回（通算 112 回）WG

日時：2014 年 1 月 8 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、土屋、西谷、藤井、松井、奥原
検討内容：
・機能要素表のブラッシュアップ
・報告書1章レビュー

第 20 回（通算 113 回）WG

日時：2014 年 1 月 22 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、西谷、藤井、松井、長谷川、奥原
検討内容：
・これまでの検討シナリオの振り返り
・報告書レビュー（5 章）
第 21 回（通算 114 回）WG
日時：2014 年 2 月 5 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、藤井、松井、長谷川、奥原
検討内容：
・これまでの検討シナリオの振り返り（その 2）

第 22 回（通算 115 回）WG

日時：2014 年 2 月 19 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、田中、戸田、藤井、西谷、長谷川、奥原
検討内容：
・これまでの検討シナリオの振り返り（その 3）

第 23 回（通算 116 回）WG

日時：2014 年 3 月 5 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、田中、戸田、藤井、西谷、長谷川、松井、米原、奥原
検討内容：
・マップ作成の方針検討
・成果物完成合宿の進め方検討

第 1 回成果物完成合宿

日時：2014 年 3 月 7 日（金）～8 日（土）
場所：IPC 生産性国際交流センター
参加者：大谷、菊地、田中、土屋、藤井、西谷、長谷川、松井、奥原
検討内容：
・サンプルマップ作成
・報告書執筆プロセスの確認

第 23 回（通算 117 回）WG

日時：2014 年 3 月 19 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、戸田、長谷川、藤井、松井、米原、奥原
検討内容：
・成果物完成合宿アウトプットの確認
・報告書執筆状況確認

2014 年度活動

第 1 回（通算 118 回）WG

日時：2013 年 4 月 2 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：大谷、菊地、田中、土屋、長谷川、藤井、松井、奥原
検討内容：
・報告書執筆状況確認
・オブジェクトモデルの検討

（中止）

日時：2013 年 4 月 16 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室

第 2 回（通算 119 回）WG

日時：2013 年 5 月 7 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：菊地、田中、戸田、長谷川、藤井、松井、奥原
検討内容：
・報告書レビュー
・報告会までのスケジュール確認

第 3 回（通算 120 回）WG

日時：2013 年 5 月 21 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：菊地、田中、戸田、長谷川、藤井、松井、奥原
検討内容：
・報告書レビュー

第 4 回（通算 121 回）WG

日時：2013 年 6 月 5 日（水） 18:30～20:30
場所：西新橋 JC ビル 3 階会議室
参加者：菊地、田中、戸田、長谷川、藤井、松井、奥原
検討内容：
・報告書レビュー
・報告会資料レビュー

2013 年度活動報告会

日時：2013 年 6 月 10 日（火） 14:00～14:30
場所：ベルサール神田
タイトル：「情報セキュリティ対策マップ検討 WG 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―」

9 参考文献

[1] ISO/IEC, *ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security management,* 2013.

[2] NIST, "Federal Information Processing Standards Publications," [Online]. Available: http://csrc.nist.gov/publications/PubsFIPS.html.

[3] 経済産業省, "情報セキュリティに関する政策、緊急情報," [Online]. Available: http://www.meti.go.jp/policy/netsecurity/audit.htm.

[4] CISA, "CISA: Certified Information Systems Auditor Study," [Online]. Available: http://cisacertified.blogspot.jp/2011/04/understanding-policies-standards.html.

[5] IPA, "「標的型メール攻撃」対策に向けたシステム設計ガイド," [Online]. Available: http://www.ipa.go.jp/security/vuln/newattack.html.

[6] ISO/IEC, *ISO/IEC 27001 － Information security management systems － Requirements.*

[7] NIST, "SPECIAL PUBLICATIONS (800 SERIES)," [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html.

[8] PCI SSC, "PCI SSC Data Security Standard Overview," [Online]. Available: https://www.pcisecuritystandards.org/security_standards/.

[9] FISC, "『金融機関等コンピュータシステムの安全対策基準・解説書』第 8 版," [Online]. Available: https://www.fisc.or.jp/publication/disp_target_detail.php?pid=225.

[10] ISO/IEC, *ISO/IEC TR13335 Guidelines for the Management for IT Security.*

[11] MITRE, "CWE: Common Weakness Enumeration," [Online]. Available: http://cwe.mitre.org/data/pdfs.html.

[12] IPA, "表 2. JVN iPedia が使用する脆弱性タイプ," [Online]. Available: http://www.ipa.go.jp/security/vuln/CWE.html.

[13] R. J, "Human error: models and management. BMJ 2000, 320:768-70," [Online]. Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117770/.