JNSA

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

情報セキュリティ対策マップ検討WG 活動報告

奥原　雅之（富士通株式会社）

2010 年 6 月 11 日

WG活動の概要

最終目的

- 「情報セキュリティ対策マップ」を作る
  - 組織全体の情報セキュリティ対策の状況を確認することができる「情報セキュリティ対策マップ」のコンセプト
  - これを作成するための手法や記述モデル
  - 実例としての汎用的な標準情報セキュリティ対策マップ案

これまでの主な活動

- 世の中の「マップ」の事例収集（～2009/2）
- 分類のための「軸」の検討（～2009/5）
- 世の中の「セキュリティ対策」の収集（昆虫採集）（～2009/8）
- 対策を分類する目安とする「対策構造図」の検討（～2009/12）
- 対策を客観的に記述する「標準構文」の検討（～現在）
- 「分県図」「標準辞書」の検討（～現在）
- その他色々な提案、検討（オブジェクト指向、構文解析、とにかく地図を描いてみる、他）

分類軸の検討

- マップを「2軸（あるいはそれ以上の次元）による対策のマッピング」と考えたとき、何が軸の候補となるか。
  - 軸の候補は「マップを読む人の目的」に依存する
  - その前に読む人を定義する必要がある
  - 「うれしさ」のような指標があってもよいかも
  - 軸の片方は対策の分類そのものなのでは
  - 分類するならMECE（網羅性と排他性）について考慮すべき

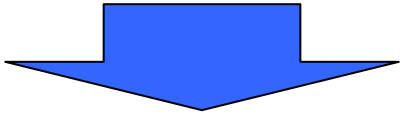
セキュリティ対策の収集（昆虫採集）

- 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
- HIPPA
- 中小企業の情報セキュリティ対策ガイドライン（IPA）
- SAS70
- IPAのリンク集にあるガイドライン
- SP800の53以外（64他）
- FIPS
- COSO
- 共通フレーム2007（SLCP-JCF）／ISO/IEC 12207
- 高等教育機関の情報セキュリティ対策のためのサンプル規程集
- RFC2196 サイトセキュリティハンドブック
- 地方公共団体における情報セキュリティポリシーに関するガイドライン

セキュリティ対策構造の検討

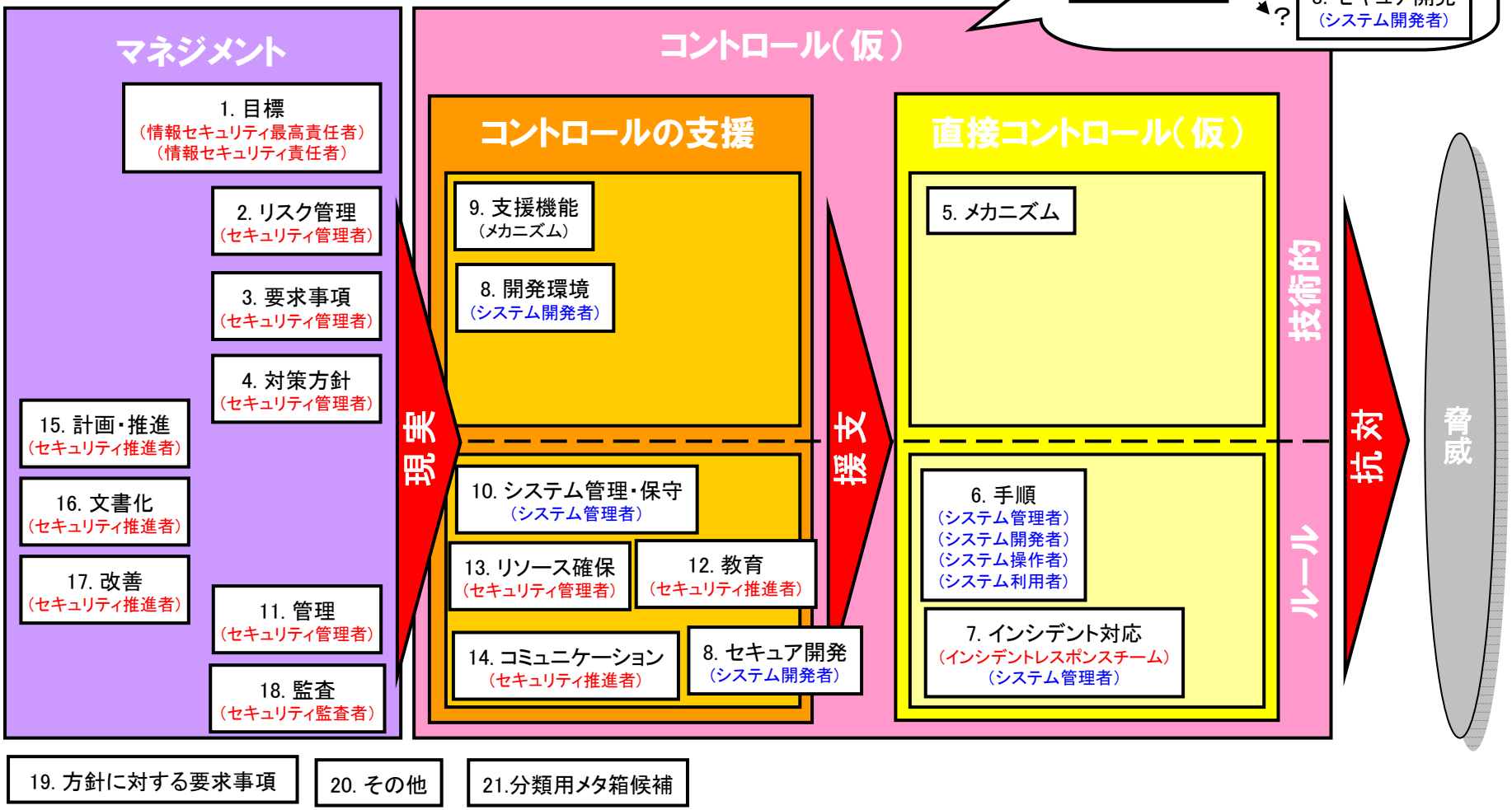
対策構造図のコンセプト

- 世の中にある多くの「管理策」を集めてみた（昆虫採集アプローチ）が、どうやって分類するか。
- 同じような目的を持つが、要求事項としては異なると思われる管理策の「グループ」「ファミリー」のようなものが存在するような気がしてきた。例えば:
  - 「○○すること」
  - 「○○する仕組みを導入すること」
  - 「○○するルールを確立すること」



- 要求している内容に着目して管理策を分類し、一般的な対策の構造を図にしてみる。

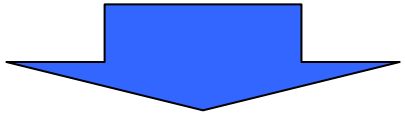
検討中の対策構造図


↓開発時の注意？
8. 開発
（システム開発者）
？
8. 開発環境
（システム開発者）
？
8. セキュア開発
（システム開発者）
マネジメント
1. 目標
（情報セキュリティ最高責任者）
（情報セキュリティ責任者）
2. リスク管理
（セキュリティ管理者）
3. 要求事項
（セキュリティ管理者）
4. 対策方針
（セキュリティ管理者）
15. 計画・推進
（セキュリティ推進者）
16. 文書化
（セキュリティ推進者）
17. 改善
（セキュリティ推進者）
11. 管理
（セキュリティ管理者）
18. 監査
（セキュリティ監査者）
現実
コントロール（仮）
コントロールの支援
9. 支援機能
（メカニズム）
8. 開発環境
（システム開発者）
10. システム管理・保守
（システム管理者）
13. リソース確保
（セキュリティ管理者）
12. 教育
（セキュリティ推進者）
14. コミュニケーション
（セキュリティ推進者）
8. セキュア開発
（システム開発者）
支援
直接コントロール（仮）
5. メカニズム
6. 手順
（システム管理者）
（システム開発者）
（システム操作者）
（システム利用者）
7. インシデント対応
（インシデントレスポンスチーム）
（システム管理者）
技術的
ルール
対抗
脅威
19. 方針に対する要求事項
20. その他
21.分類用メタ箱候補
ITシステム・設備
守るべき情報資産
情報

セキュリティ対策の標準記法（標準文法）の検討

標準構文のコンセプト

- 中心となる管理策は「何かを」「どうする」という単純な構文になる（期待を込めた仮定）。
- 「誰が」「何のために」「何を使って」などは修飾節（バリエーション）として扱う。
- 「を確実にする」などの表現上の語句も基幹部分の外に出す。



- 対策（管理策）を一意に表現できる構文ができる。（地図を作るための記法となる）
- 「どうする」の動詞と管理策の性質（分類）に関係が出る（期待）

検討中の標準構文

【目的・脅威】 のために 【実施者】 は

【条件】 のときに 【場所】 で

管理策

【対策】 を 【動詞】 する

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

セキュリティ対策の標準辞書の検討

検討中の標準辞書（一部）

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

標準構文によるガイドラインのマッピング（分県図）試行

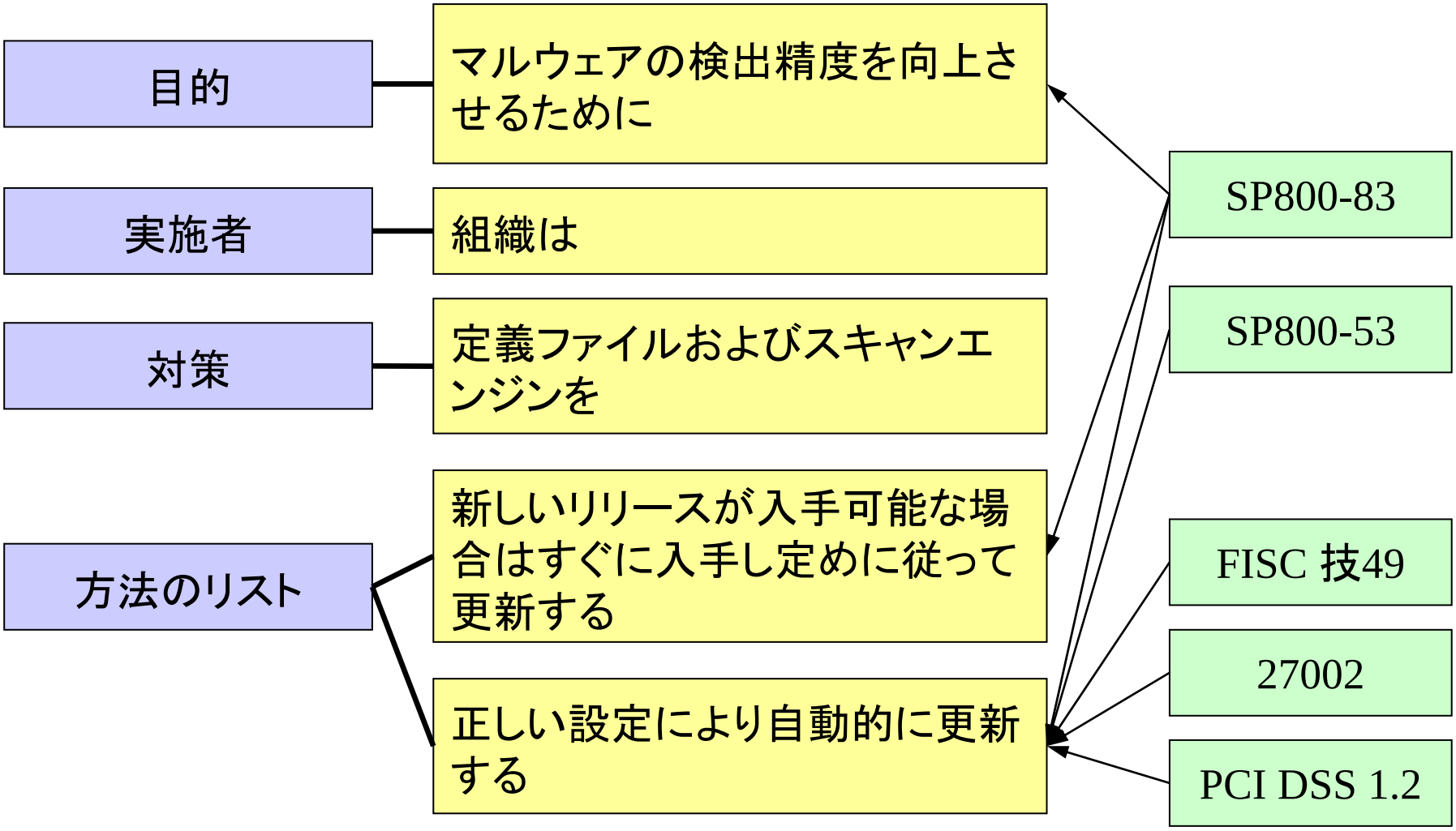
分県図の「作図」方法

- まずあるテーマに沿ってガイドラインをいくつか集める。
- 「標準文法」を使って、各ガイドラインの要求事項（管理策）の「幹の部分」を記述する。
- 「枝葉の部分」は「変数」として明確に分離できるように記述する。（ISO/IEC 15408に似たアプローチ）

分県図の記述例

ID	MAL.5
名称	定義ファイルなどの最新化
管理策	マルウェアの検出精度を向上させるために組織は定義ファイルおよびスキャンエンジンを【最新に保つ方法のリスト:{正しい設定により自動的に更新する}{新しいリリースが入手可能な場合はすぐに入手し定めに従って更新する}】。

分県図の「作図」方法

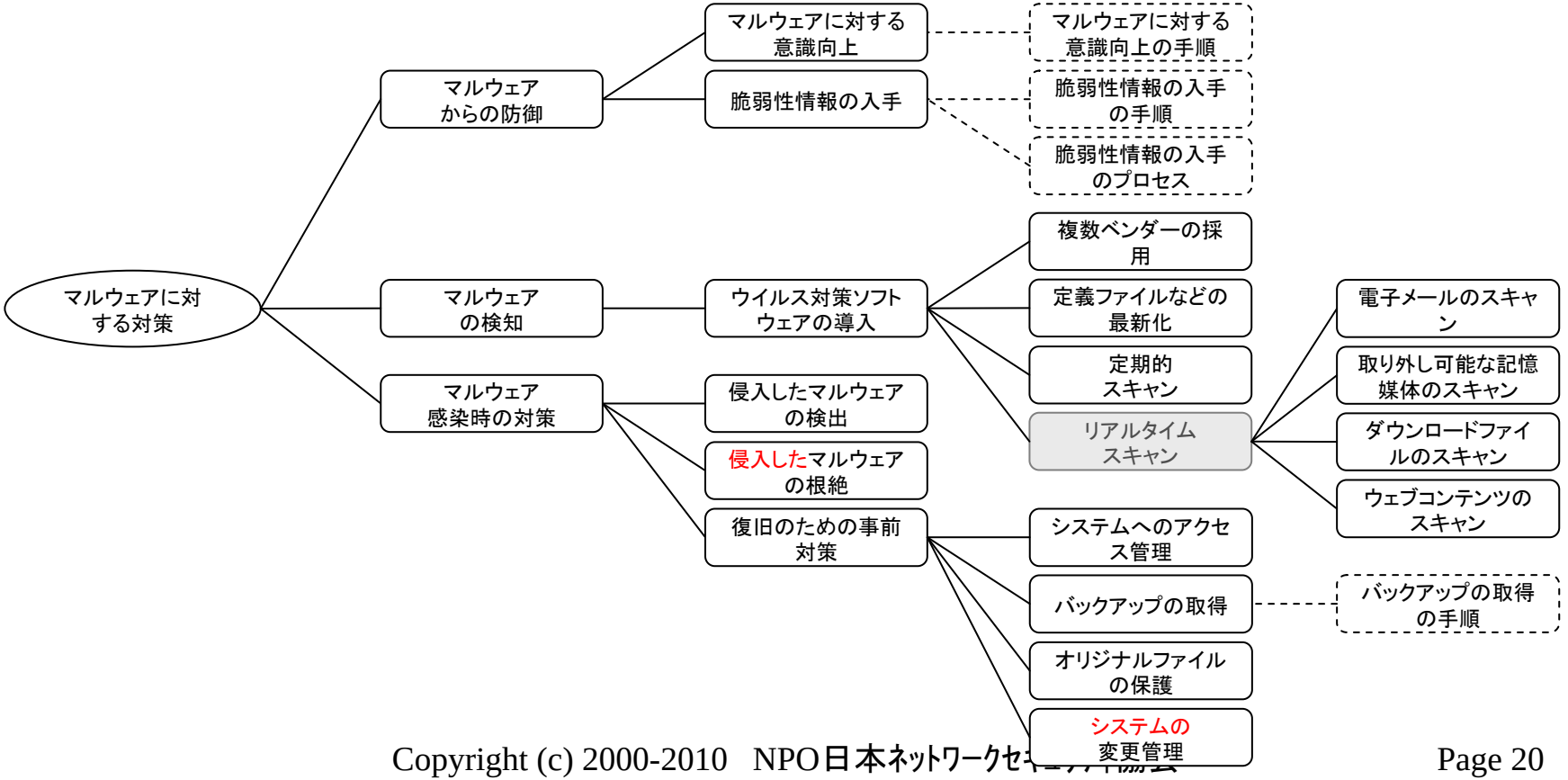


「マルウェア県　分県図」の試作

- 「マルウェア対策」をテーマに、分県図の作成を試みた。
- 並行して、標準構文の検証、標準辞書の試作を実施した。
- マルウェアの分県図として、24種類の標準的な管理策を抽出できた。（巻末に記載）
- 他の分野も何とかなりそうな気がしてきた。

分県図の「地図」化

- 「対策構造」その他の成果と組み合わせることで、「地図」にする。（現在検討中）



今後の活動予定

- 本WGの実施を3カ年とすると。
  - １年目：先行事例の調査研究、
    対策マップの方向性検討
  - ２年目：対策マップ記述モデルの検討、
    作成手法の検討、
    標準対策マップ案の作成
  - ３年目：標準対策マップの検証、
    最終報告書作成

【付録】マルウェア「分県図」

【付録】マルウェア分県図（1）

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}】。

【付録】マルウェア分県図（2）

ID	名称	分類	内容
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。

【付録】マルウェア分県図（3）

ID	名称	分類	内容
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。