

情報セキュリティ対策マップ検討 WG

WG リーダー 富士通株式会社 奥原 雅之
WG サブリーダー 富士通株式会社 長谷川 喜也

■ 発足の背景

情報セキュリティ対策マップ検討 WG は、技術部会に所属する WG です。組織にとって最適な情報セキュリティ対策を系統的に検討する場面においては、対策すべき情報セキュリティの全体像を正確に把握できるドキュメントがあると大変便利です。そこで、「組織が持つ情報セキュリティの対策を正確に描ける地図」がもしあるとしたら、それは一体どういうものかということを検討し、作成するための手法、記述モデル、および汎用的な標準情報セキュリティ対策マップ案を開発することを目的に 2009 年 1 月より活動を開始、今年で 4 年目を迎えました。

■ 「情報セキュリティ対策マップ」は何故必要か

以下の様な悩みを的確に解決する方法を皆様はお持ちでしょうか？

『A さんの会社では、ファイアウォールを導入してから大分経ったので入れ替えを検討している。

新しいファイアウォールの選定をする担当になった A さんは、情報セキュリティ製品ベンダを呼んで話を聞いたところ、そのベンダは「当社では、価格の高いファイアウォールと、価格の安いファイアウォールの二種類を扱っている。価格の高いファイアウォールには、価格の安いファイアウォールに搭載されていない UTM（統合脅威管理）の機能があり、特にアンチウイルス機能が自慢だ。ここにあるガイドラインにも、『複数ベンダが提供する不正プログラム対策ソフトの利用を検討するように』と書いてある。」とあるガイドラインを提示しながら説明した。

この話を上司にしたところ、「当社では全てのパソコンにアンチウイルスソフトウェアを導入してウイルス対策を行っているから、いまさらファイアウォールの所にアンチウイルス機能はいらなと思うが、それが必要だというガイドラインがあるのであれば、その有効性を良く検討しなさい。」との回答が返ってきた。

A さんは困った。「確かにファイアウォールと個々のパソコンの二箇所ですウイルス対策をした方が、セキュリティは高い気がする。しかし、パソコンのウイルス対策だけでは足りない、とも言い切れない。ベンダが提示したこのガイドラインは、当社のリスクに対応する対策として適切なのだろうか。』

この悩みを解決するためには、A さんの会社のリスクと取り得る対策の関係を正確に記述する方法が必要です。それがあって初めて「当社のこのリスクは、この対策で対応する」と決定することができるのです。そのための拠り所となるのが、世の中の全ての対策の関係を表した地図「情報セキュリティ対策マップ」なのです。この WG ではこの「情報セキュリティ対策マップ」の開発を目指しています。

■ 検討の様子

2008 年 12 月に準備会を開催し、2009 年 1 月より正式に WG として活動を開始しました。これまで、ほぼ二週間ごとに活動をおこない、4 年目となった 2012 年 8 月現在、通算 79 回の WG を開催しています。2011 年には長期にわたり活動した事を評価され、JNSA 表彰を受賞しました。

これまでの活動では、世の中のガイドラインに載っている、情報セキュリティ対策といわれる物をたくさん収集してきて、それを分類するところから検討を始め、集まった対策をグループ分けしてグループ間の構造を表した「対策構造図」(図 1) や、2 つの対策間の関係を繋げていってツリー構造で表した「川図法(仮称)」(図 2) などを開発してきました。

現在は、情報セキュリティ対策そのものの構造に着目して、オブジェクト指向を取り入れた、「対策オブジェクトモデル V3」(図 3) を創案し、その有効性を JIS Q 27002 (ISO/IEC 27002) を使って検証中です。

図 1. 対策構造図

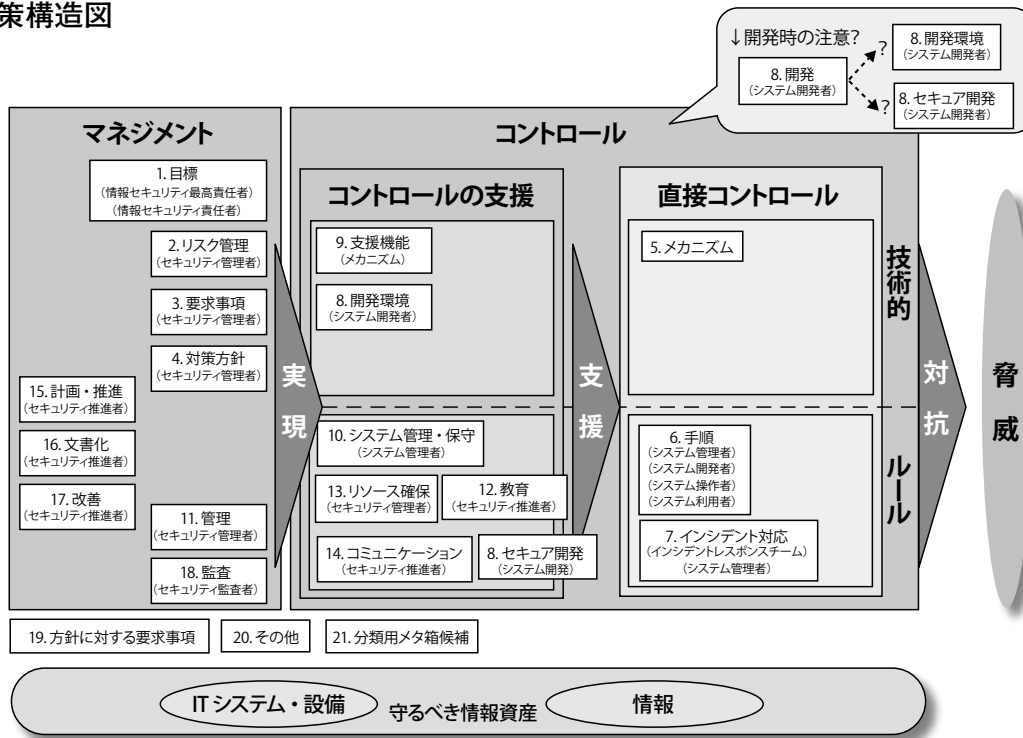
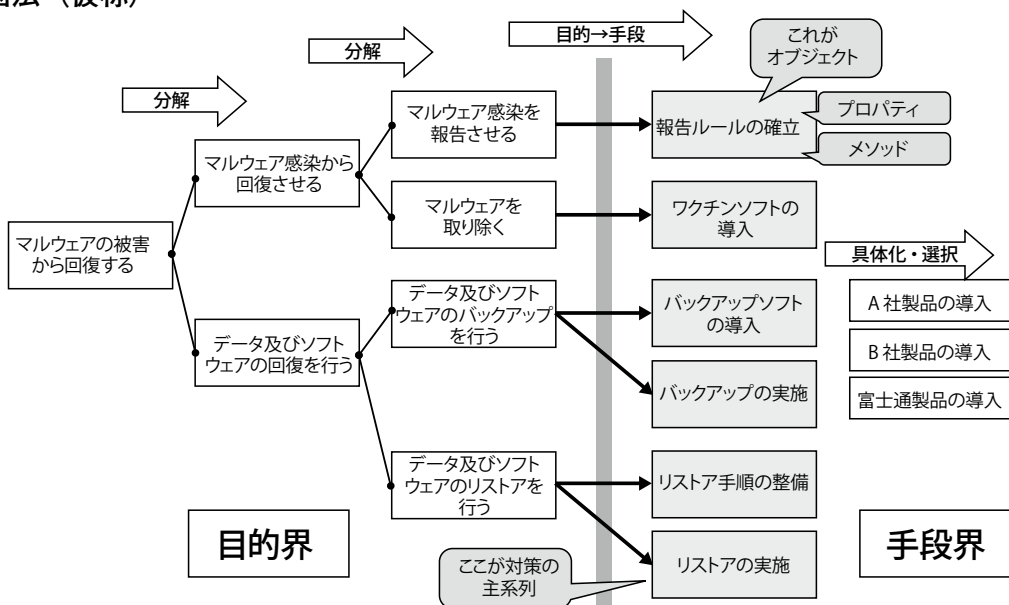


図 2. 川図法 (仮称)



JNSA ワーキンググループ紹介

図 3. 対策オブジェクトモデル V3

オブジェクト	「管理策」。			
プロパティ	方針 目的 機能 要求事項 場所 条件 時間 実施者 対象者・対象物			
メソッド	計画	検討する 計画する	コストを算定する 文書化する	方針を確立する 有効性の測定方法を決める
	準備	責任者を明確化する 機能を明確化する 導入条件を明確化する リソースを確保する 手順を確率する	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	

WG 発足当初は、3年で結果を出す予定でしたが、はからずも4年目に突入してしまい、今年こそは皆様にお披露目できる成果物を完成させたいと思い活動をしています。

グループのメンバーは「来る物は拒まず、去る者は追わず」の方針で募集しているため、登録者数は30名を超えていますが、コアとなって活動をしているのは、7名程度です。ご興味のある方は、いつでも歓迎をしておりますので、是非ご参加ください。

