

平成 21 年度各専門分野情報共有スキームの連携性  
及び情報交換モデルの構築支援業務  
(リスク要件リファレンスモデルドキュメント集等の作成)  
総括報告書

平成 22 年 3 月

株式会社三菱総合研究所

## 目次

|  |    |
|--|----|
| はじめに.....                              | 3  |
| 1. 事業の目的と背景.....                       | 4  |
| 1.1. 問題認識.....                         | 4  |
| 1.1.1. 情報セキュリティに係る脅威と問題の変質.....        | 4  |
| 1.1.2. 専門分野間の役割分担と連携の必要性.....          | 5  |
| 1.2. 検討範囲.....                         | 6  |
| 1.3. 検討フレーム.....                       | 7  |
| 1.4. 検討体制.....                         | 10 |
| 1.5. 検討経緯.....                         | 14 |
| 2. 検討成果サマリ.....                        | 16 |
| 2.1. リスク要件リファレンスモデル作業部会.....           | 16 |
| 2.1.1. リスク要件リファレンスモデル開発の目的とモデルの構成..... | 18 |
| 2.1.2. 振る舞いモデル.....                    | 20 |
| 2.1.3. システムトポロジーモデル.....               | 23 |
| 2.1.4. 設計対策セット.....                    | 24 |
| 2.1.5. 運用解説書.....                      | 27 |
| 2.2. 組織リスク動的判断モデル作業部会.....             | 28 |
| 2.2.1. 組織とインシデント対応を巡る現状.....           | 28 |
| 2.2.2. 動的判断モデルチャート.....                | 30 |
| 2.2.3. まとめ.....                        | 32 |
| 2.3. 連携マップ作成作業部会.....                  | 33 |
| 2.3.1. 情報セキュリティに関する時系列俯瞰図(連携マップ).....  | 33 |
| 2.3.2. 組織連携成立要件のセオリー.....              | 34 |
| 2.3.3. 課題.....                         | 35 |
| 2.3.4. まとめ.....                        | 36 |
| 3. 今後の展開.....                          | 37 |
| 3.1. 普及方策検討計画(案).....                  | 37 |
| 3.2. リスク要件リファレンスモデル運用連携スキーム(案).....    | 37 |

## はじめに

情報セキュリティ分野は、対応すべき脅威や関連する技術など、様々な側面において環境の変化が早い。また、近年の攻撃手法の高度化やそれに対応する対策の深化に伴い、情報セキュリティに係る専門分化や分業化が生じつつある。刻々と変化する状況を適時適切に把握し、新たに生起する課題に対して的確な対応を行うためには、関係する専門分野の知見を有する各主体が、情報を共有し、かつ連携して対処していくことが重要である。

このため、「セキュア・ジャパン 2009」(平成 21 年 6 月 22 日情報セキュリティ政策会議決定。)に基づき、内閣官房情報セキュリティセンター(以下、「NISC」)において、システム設計分野、ウイルス解析分野、CSIRT<sup>1</sup>分野、ISP<sup>2</sup>分野等の各専門分野の情報共有スキームの役割と連携性を整理し、それぞれの目的・機能に応じた情報連携と情報交換モデルの検討を行い、この一環として「連携マップ」を作成した。社会・経済におけるITの役割が高度化・複雑化する中、ITセキュリティ上の問題の影響も従来の領域を超え広がりがつつある。そこで、そうした影響が生じている多様な事業分野を対象に、各専門分野間の情報共有スキーム及び連携モデルの在り方や実現に係る課題について検討した。

具体的には、各専門分野それぞれの目的・機能に応じた情報連携と情報交換モデルの構築を目指して、情報セキュリティ政策や業界動向に関する専門家・有識者及びシステム関連事業者等から構成される「情報セキュリティに係る各専門分野の情報共有・連携推進会議」や「リスク要件リファレンスモデル作業部会」や「組織リスク動的判断モデル作業部会」、「連携マップ作成作業部会」を設置し、それぞれの検討や調査、各種作業等の中で相互にフィードバックしながら、今後必要となる課題解決の手段やしくみを開発した。

本事業の実施にあたり、ご尽力いただいた関係各位に厚くお礼申し上げますとともに、本事業の成果が今後の我が国の情報セキュリティを巡る様々な局面で有効に活用されることを期待する。

平成 22 年 3 月

---

<sup>1</sup> Computer Security Incident Response Team

<sup>2</sup> Internet Service Provider

# 1. 事業の目的と背景

## 1.1. 問題認識

ICT 環境の変化や脅威の変質に伴い、情報セキュリティを取り巻く構造変化が生じつつある。そうした動きに伴い、既存の取組では対応が困難な課題について、問題対処を支援するための検討を行う。

### 1.1.1. 情報セキュリティに係る脅威と問題の変質

#### (1) 攻撃の多様化・高度化・複雑化

近年、botnet を悪用した DDoS 攻撃の ASP サービスや、ネットワーク経由で詐取した ID/パスワード等の認証情報やクレジットカード情報を換金するしくみなど、情報セキュリティに係る攻撃を活かした国際的なビジネスモデルが確立されている。そうした環境整備を背景に、営利目的と思われる攻撃主体が台頭し、攻撃手法の技術や手口がいつそう発展しつつある。

また、未公表の脆弱性を悪用するゼロデイ攻撃やターゲットを狙い撃ちする標的型攻撃も頻発しているが、これらの被害は発生してもそれが発覚しにくい上に、気づいても動きが複雑で分析が容易ではなく、状況の把握や適切な対応を行うことが非常に難しいと考えられる。そのため、以前のように被害が共通体験として認識され、一丸となって問題対処に取り組むことはなくなり、組織の内外においてこうした問題意識を共有することは難しい状況になっている。

#### (2) 責任分界点の曖昧化

ICT が今日、ビジネスインフラとして不可欠な役割を担っていることは言うまでもない。加えて、近年は、ビジネスプロセスの様々な局面で ICT の活用が浸透しており、その関与者も幅広く多様化・複雑化している。こうした状況では、仮にトラブルが発生した場合、責任の所在が曖昧する可能性がある。

また、今後、クラウドコンピューティングの到来を迎えるにあたり、管理・統制構造についての検討は不可避である。たとえば、クラウドコンピューティングの環境では、複数の事業者間でデータが扱われるため、トラブル発生時にどのような枠組みで責任を分担すべきなのか、明確ではない。

さらに、組込みシステムについては、汎用化・ネットワーク化が進むのに伴い、脆弱性の問題も顕在化しつつある。しかし、一般ユーザがコンピュータシステムにおける脆弱性対応のように、パッチを適用してくれる可能性は低く、問題解決には別の手立てが必要と考えられる。

### (3) 組織リスクにおける情報セキュリティ分野の影響の高まり

会社法等を背景に、企業はリスク管理の体制整備や方針の策定が求められており、そうしたリスク管理においては情報セキュリティに係るリスクも対象範囲とされる。

また、ビジネスプロセスが ICT に依存している場合、ICT トラブルの影響が事業に直結するという点にも配慮が必要である。これは特殊な業種・業界に限った話ではなく、たとえば EC サービスは決済機能も一種のインフラとしてサポートされており、すでに業種を問わず一般化していることが明らかである。

以上の傾向を踏まえると、ICT 環境の変化や脅威の変質に伴い、情報セキュリティを取り巻く構造変化が生じつつあると捉えることができる。中でも、攻撃の多様化・高度化・複雑化は、既存の取組では対応が困難であり、新しい対策とそれを支えるしくみが必要になると考えられる。

#### 1.1.2. 専門分野間の役割分担と連携の必要性

先に述べたとおり、高度化・複雑化する攻撃に対処するためには、情報管理だけでなく、サイバー攻撃防御の強化が不可欠である。そのために必要な情報セキュリティ対策の技術は、高度化に伴い、専門分化する方向にある。

したがって、高度化・複雑化する攻撃に対処するためには、情報セキュリティの様々な専門分野間の役割分担と連携が必要である。

こうした課題を踏まえ、「セキュア・ジャパン 2009 ～すべての主体に事故前提の自覚を～」では、対応する施策が提示されている。

## 第4章 政策の推進体制と持続的改善の構造について

政府は、2009 年度に、前章に示した重点政策に、以下に示す体制と持続的構造の下で総合的に取り組むこととする。

### 第1節 政策の推進体制

#### (3) 状況の変化の適時適切な把握と新しい課題への対応

情報セキュリティ分野は、脅威や技術など、様々な側面において変化が早い。このため、刻々と変化する状況を適時適切に把握するとともに、新たに生起する課題に対して迅速かつ的確な対応を行うことが重要となる。また、新たにトレンドとなる政策手法についても適切な検討を進めることが不可欠である。さらに、情報提供主体を対象とした新たな取組みを進めることも必要である。

このため、NISCをはじめとする様々な関係機関・関係者が連携し、また情報セキュリティ政策会議の下に適宜設置される専門委員会も活用し、法律、技術、啓発など政策に係る幅広い視点全

般から、検討を動的にかつ柔軟に進める体制を強化する。

**【具体的施策】**

**ア)各専門分野情報共有スキームの連携性及び情報交換モデルに関する検討  
(内閣官房、総務省及び経済産業省)**

昨今の高度化されたサイバー攻撃及び IT 障害対処等に関する適切な対処立案には、多様な専門性を有する情報収集・相関分析と各々の情報共有スキームの目的・機能に応じた連携対処が必要である。

このため、2010年3月末までに「システム設計分野・ウイルス解析分野・CSIRT 分野・ISP 分野」等の各専門分野の情報共有スキームの役割と連携性を整理し、それぞれの目的・機能に応じた情報連携と情報交換モデル(連携構図設計)の検討を行う。

図 1-1 本事業に関する施策の記載

(出典:「セキュア・ジャパン 2009 ～すべての主体に事故前提の自覚を～」)

## 1.2. 検討範囲

問題認識を踏まえ、対処に寄与する情報セキュリティに係る各専門分野の情報共有・連携を図る。具体的には、連携の基盤となる考え方や前提条件を明らかにするとともに、システムの企画・設計、運用の各段階における問題を探り上げ、対処を支援する検討を行う。

- (1) 情報セキュリティ専門家が有する情報を発注者と Sier がシステム企画・設計時に活用できるか。
- (2) トラブル発生時に組織を取り巻く多様なリスクをどのようにして把握し、対処判断すべきか。
- (3) 組織間連携が成立する要件は何か。情報セキュリティ分野を取り巻く環境変化(前提条件をどのように捉えるべきか。

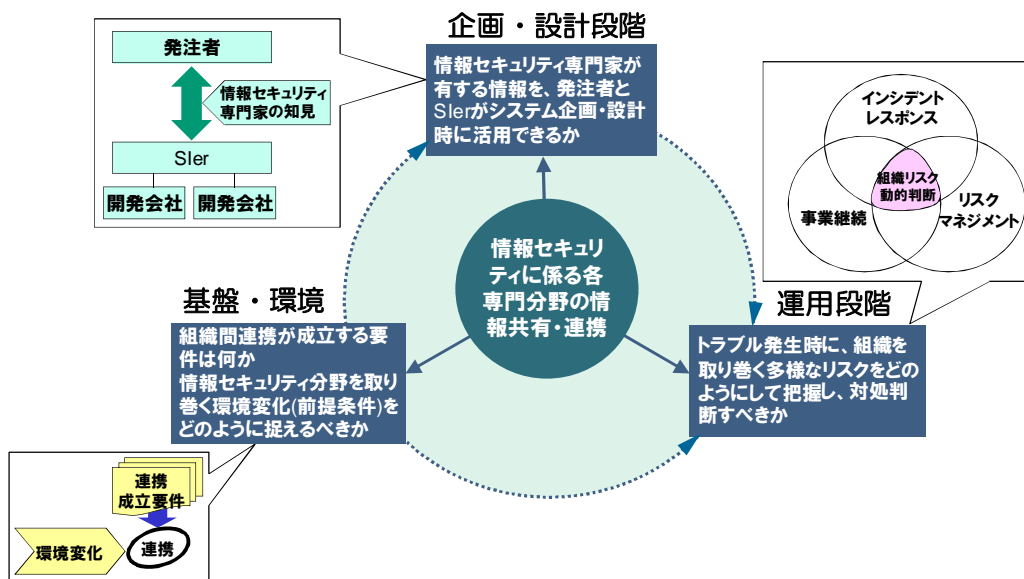


図 1-2 本事業の検討範囲

### 1.3. 検討フレーム

本事業の検討フレームは、検討成果をとりまとめ、全体の整合を図る「情報セキュリティに係る各専門分野の情報共有・連携推進会議」と、その下で個別の課題を検討する「作業部会」で構成する。

作業部会では、以下の検討課題を対象とする。

- (1) リスク要件リファレンスモデル及び標準対処法の検討
- (2) 組織リスク動的判断モデルの検討
- (3) 専門分野の情報共有スキームの役割と連携性に関する検討と連携マップの作成

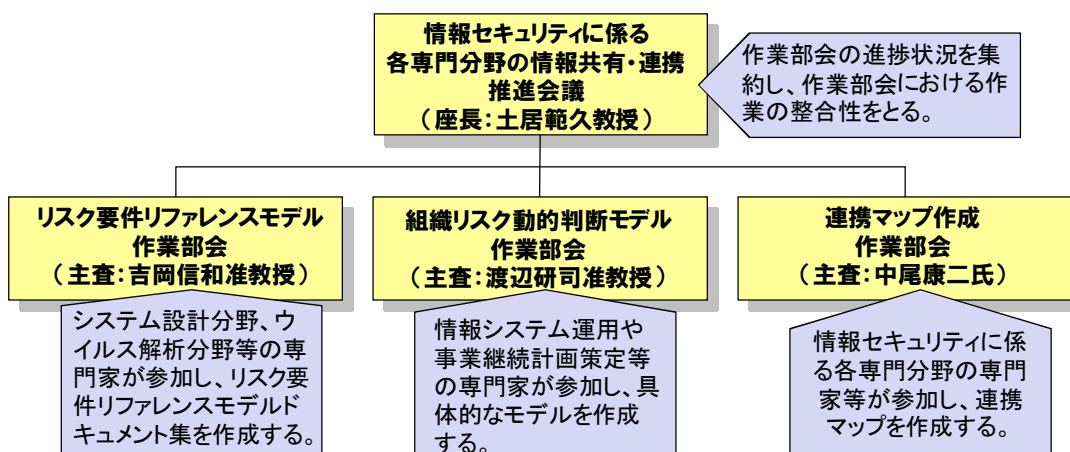


図 1-3 本事業の検討フレーム

さらに、リスク要件リファレンスモデルについては、作業部会の下に、多数のセキュリティ技術者やシステム技術者等で構成される「仮想作業場」を設置し、具体的な検討を行う体制を整えた。

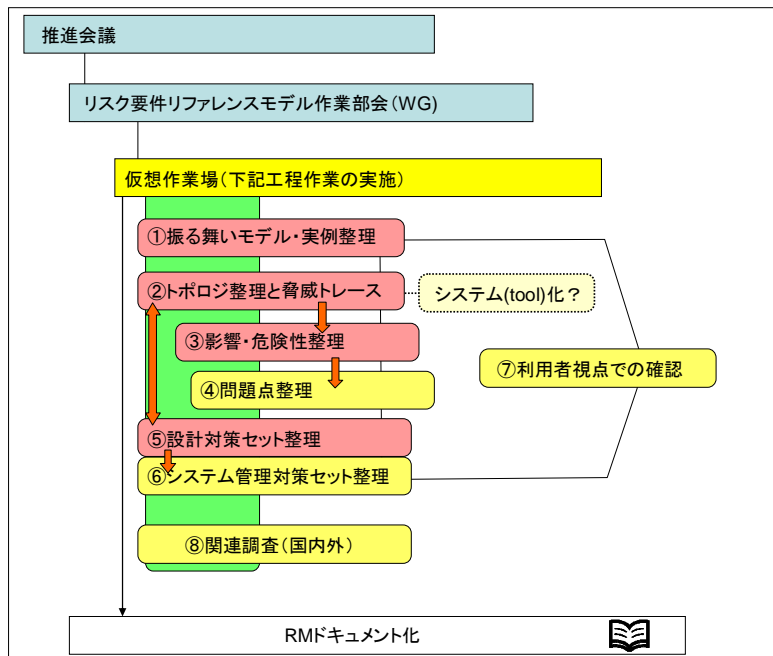


図 1-4 仮想作業場の位置づけ

リスク要件リファレンスモデルの作成には、各専門分野の相関で脅威分析～設計対策までを一連整理する必要がある。このため下記の各分野相関の場を儲けた（仮想作業場）。

- ・各専門分野の相関で設計対策までを整理。→RMは各分野相関でないと造れない。(通常、分野間の関係性は薄い)
- ・RM作成作業を通じて、各分野相関の場を構築。
- ・相互連携の一つのモデル事例。

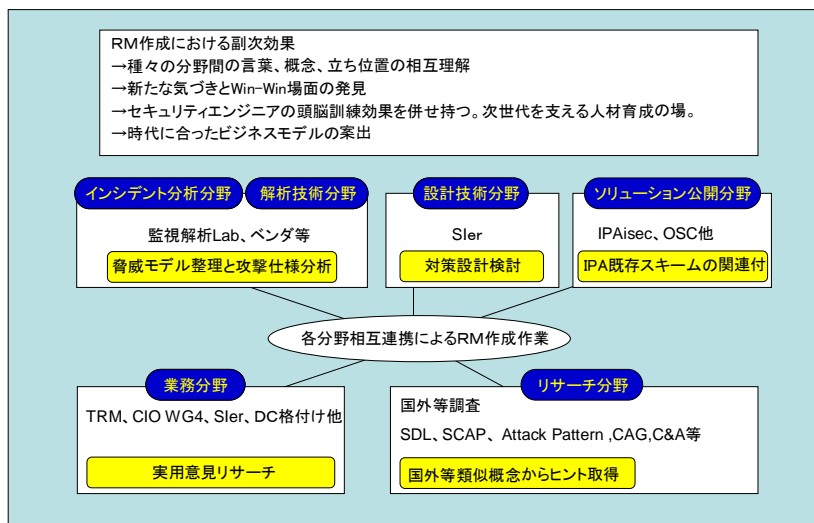


図 1-5 リスク要件リファレンスモデルの作成に関わる諸分野

各作業部会間の相互関係を下図に示す。

それぞれは、単独利用及びリスク要件リファレンスモデルの各コンテンツを参照する場合の理由付けとして使用される事を想定している。

- ◆ ICT環境・ビジネスモデルの変化や脅威の変質に伴い、情報セキュリティ(CND)を取り巻く構造変化が生じつつある。
- ◆ 既存の取組では対応が困難な課題について、問題対処を支援するための検討を行う。
- ◆ 本施策はサイバー攻撃対処(CND)に基本軸足を置き各課題を整理。

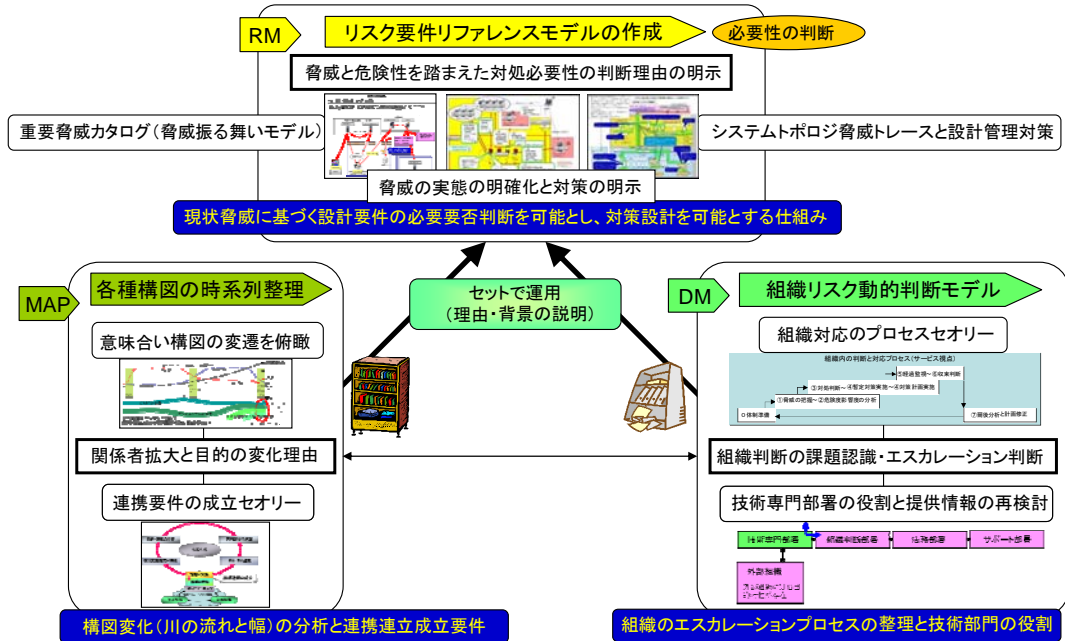


図 1-6 各作業部会の相互関係

## 1.4. 検討体制

本事業の検討体制を以下に示す(所属・肩書等は2010年3月23日現在)。

### (1) 情報セキュリティに係る各専門分野の情報共有・連携推進会議

#### 【座長】

土居 範久 中央大学 工学部 情報工学科 教授

#### 【構成員 (50音順)】

有村 浩一 Telecom-ISAC JAPAN 企画調整部部長  
伊藤 光恭 日本電信電話株式会社 情報流通プラットフォーム研究所  
セキュアコミュニケーション基盤プロジェクトグループリーダー  
高橋 正和 マイクロソフト株式会社 チーフセキュリティアドバイザー  
寺田 真敏 株式会社日立製作所  
Hitachi IRT チーフコーディネーションデザイナー  
徳田 敏文 日本アイ・ビー・エム株式会社 情報セキュリティ担当部長  
中尾 康二 KDDI 株式会社 運用統括本部 情報セキュリティフェロー  
吉岡 信和 国立情報学研究所 GRACE センター  
アーキテクチャ科学研究系 准教授  
渡辺 研司 長岡技術科学大学 大学院技術研究科 准教授

### (2) リスク要件リファレンスモデル作業部会

#### 【主査】

吉岡 信和 国立情報学研究所 GRACE センター  
アーキテクチャ科学研究系 准教授

#### 【構成員 (50音順)】

飯田 朝洋 トレンドマイクロ株式会社 サポートサービス本部  
コアテクノロジーサポートグループ Threat Monitoring Center 課長  
鵜飼 裕司 株式会社フォティーンフォティ技術研究所  
取締役副社長 最高技術責任者 (CTO)  
織茂 昌之 株式会社日立製作所 情報・通信グループ  
セキュリティ・トレーサビリティ事業部 Hitachi IRT センタ長  
加藤 雅彦 株式会社アイアイジェイテクノロジー 技術開発部  
IBPS 本部担当部長  
金谷 延幸 株式会社富士通研究所 ソフトウェア&ソリューション研究所

|       |   |
|-------|---|
|       | セキュアコンピューティング研究部 主任研究員                                |
| 高橋 正和 | マイクロソフト株式会社 チーフセキュリティアドバイザー                           |
| 谷川 哲司 | 日本電気株式会社 経営システム本部<br>セキュリティ技術センター シニアマネージャー           |
| 富樫 一哉 | 一般社団法人 JPCERT コーディネーションセンター<br>事業推進基盤グループ システム開発マネージャ |
| 徳田 敏文 | 日本アイ・ビー・エム株式会社 情報セキュリティ担当部長                           |
| 名和 利男 | 株式会社サイバーディフェンス研究所 上級分析官                               |
| 春山 智  | 株式会社NTTデータ 技術開発本部 シニアエキスパート                           |
| 前田 典彦 | 株式会社カスペルスキーラボスジャパン<br>エンタープライズ事業部 部長                  |
| 満塩 尚史 | 環境省 CIO 補佐官   |
| 三好 眞  | 株式会社アイ・エス・レーティング 執行役員調査研究部長                           |
| 矢島 秀浩 | 独立行政法人 情報処理推進機構 セキュリティセンター長                           |

【オブザーバ】

|       |                           |
|-------|---------------------------|
| 鈴木 律郎 | 社団法人情報サービス産業協会 企画調査部 技術課長 |
|-------|---------------------------|

(3)仮想作業場

【構成員（50音順）】

|        |  |
|--------|--|
| 有村 浩一  | Telecom-ISAC Japan 企画調整部部長   |
| 飯田 朝洋  | トレンドマイクロ株式会社 サポートサービス本部<br>セキュリティエンハンストサポートグループ<br>Threat Monitoring Center 課長 |
| 石丸 傑   | 株式会社カスペルスキーラボスジャパン 情報セキュリティラボ  |
| 伊藤 光恭  | 日本電信電話株式会社 情報流通プラットフォーム研究所<br>セキュアコミュニケーション基盤プロジェクトグループリーダー                    |
| 乾 奈津子  | 株式会社サイバーディフェンス研究所 分析官  |
| 岩村 誠   | 日本電信電話株式会社 情報流通プラットフォーム研究所<br>セキュアコミュニケーション基盤プロジェクト<br>セキュアネットワーク構成方式グループ      |
| 鵜飼 裕司  | 株式会社フォティーンフォティ技術研究所 代表取締役社長  |
| 大久保 隆夫 | 株式会社富士通研究所 ソフトウェア&ソリューション研究所<br>セキュアコンピューティング研究部                               |
| 大塚 紘史  | 株式会社NTT データ 技術開発本部<br>SI アーキテクチャ開発センタ  |

|         |  |
|---------|--|
| 小野寺 匠   | マイクロソフト株式会社 セキュリティレスポンスチーム   |
| 片山 昌憲   | エキサイト株式会社 テクノロジー&サービス本部<br>サービスマネジメント室   |
| 加藤 雅彦   | 株式会社アイアイジェイテクノロジー IBPS 本部 担当部長   |
| 金岡 晃    | 筑波大学大学院 システム情報工学研究科 助教授  |
| 金谷 延幸   | 株式会社富士通研究所 ソフトウェア&ソリューション研究所<br>セキュアコンピューティング研究部   |
| 佳山 こうせつ | 富士通株式会社 クラウドセキュリティセンター<br>インテグレーション部   |
| 金 賛愚    | トレンドマイクロ株式会社 サポートサービス本部<br>コアテクノロジーサポートグループ Threat Monitoring Center<br>Threat Research Engineer |
| 熊白 浩文   | 株式会社アイ・エス・レーティング 格付部 アナリスト   |
| 小林 偉昭   | 独立行政法人情報処理推進機構 セキュリティセンター<br>情報セキュリティ技術ラボラトリー長   |
| 小林 克巳   | NRI セキュアテクノロジーズ株式会社<br>テクニカルコンサルティング部  |
| 小松 優介   | トレンドマイクロ株式会社 サポートサービス本部コアテクノロジーサポートグループ Threat Monitoring Center 担当課長代理                          |
| 高橋 正和   | 株式会社マイクロソフト チーフセキュリティアドバイザー  |
| 田口 研治   | 国立情報学研究所 先端ソフトウェア工学・国際研究センター<br>NII アーキテクチャ科学研究系 特任教授  |
| 谷川 哲司   | 日本電気株式会社 経営システム本部<br>セキュリティ技術センター シニアマネージャー  |
| 丹京 真一   | 株式会社日立情報システムズ セキュリティリサーチセンタ 技師   |
| 辻 俊幸    | 株式会社アイ・エス・レーティング 企画部 マネジャー   |
| 寺田 真敏   | 株式会社日立製作所<br>Hitachi-IRT チーフコーディネーションデザイナー   |
| 富樫 一哉   | 一般社団法人 JPCERT コーディネーションセンター<br>事業推進基盤グループ システム開発マネージャ  |
| 徳田 敏文   | 日本アイ・ビー・エム株式会社<br>経営品質・情報セキュリティ推進室 情報セキュリティ担当部長  |
| 中川 彰男   | 株式会社アイ・エス・レーティング 格付部 アナリスト   |
| 鍋島 学    | 内閣官房情報セキュリティセンター 参事官補佐   |
| 名和 利男   | 株式会社サイバーディフェンス研究所 上級分析官  |
| 羽山 剛弘   | 株式会社アイ・エス・レーティング 格付部 グループ長   |

|       |  |
|-------|--|
| 春山 智  | 株式会社NTT データ 技術開発本部<br>SI アーキテクチャ開発センタ シニアエキスパート                                    |
| 前田 典彦 | 株式会社カスペルスキーラブスジャパン<br>エンタープライズ事業部部長  |
| 松川 博英 | トレンドマイクロ株式会社 サポートサービス本部<br>セキュリティエンハンストサポートグループ<br>Threat Monitoring Center 担当課長代理 |
| 松田 剛  | 株式会社アイ・エス・レーティング 格付部 アナリスト   |
| 真鍋 敬士 | 一般社団法人 JPCERT コーディネーションセンター 理事   |
| 宮坂 肇  | 株式会社NTT データ セキュリティ技術推進   |
| 宮本久仁男 | 株式会社NTT データ 技術開発本部<br>SI アーキテクチャ開発センタ シニアエキスパート                                    |
| 三好 眞  | 株式会社アイ・エス・レーティング 執行役員 格付部長   |
| 村上 純一 | 株式会社フォティーンフォティ技術研究所<br>技術本部 先端技術研究部長   |
| 本川 祐治 | 株式会社日立情報システムズ ネットワークサービス事業部<br>ネットワーク事業推進本部 セキュリティリサーチセンタ センタ長                     |
| 守屋 英一 | 日本アイ・ビー・エム株式会社 ISS 事業部 営業推進部   |
| 山岸 篤弘 | 独立行政法人情報処理推進機構 セキュリティセンター<br>情報セキュリティ技術ラボラトリー 研究員                                  |
| 山口 進  | 株式会社アイ・エス・レーティング 格付部 チーフアナリスト  |
| 吉岡 信和 | 国立情報学研究所 先端ソフトウェア工学・国際研究センター<br>NII アーキテクチャ科学研究系 准教授                               |
| 吉川 孝志 | トレンドマイクロ株式会社 人事総務部付  |
| 吉府 研治 | 日本電気株式会社 経営システム本部<br>(セキュリティ技術センター) マネージャー   |

#### (4) 組織リスク動的判断モデル作業部会

##### 【主査】

渡辺 研司 長岡技術科学大学 大学院技術研究科 准教授

##### 【構成員 (50 音順)】

|       |  |
|-------|--|
| 有村 浩一 | Telecom-ISAC JAPAN 企画調整部部長             |
| 片山 昌憲 | エキサイト株式会社 テクノロジー&サービス本部<br>サービスマネジメント室 |
| 篠原 雅道 | 事業継続協会日本支部代表                           |

|       |  |
|-------|--|
| 高橋 正和 | マイクロソフト株式会社 チーフセキュリティアドバイザー                |
| 寺田 真敏 | 株式会社日立製作所<br>Hitachi IRT チーフコーディネーションデザイナー |
| 徳田 敏文 | 日本アイ・ビー・エム株式会社 情報セキュリティ担当部長                |
| 名和 利男 | 株式会社サイバーディフェンス研究所 上級分析官                    |

#### (5) 連携マップ作成作業部会

##### 【主査】

中尾 康二 KDDI 株式会社 運用統括本部 情報セキュリティフェロー

##### 【構成員（50音順）】

|       |   |
|-------|---|
| 有村 浩一 | Telecom-ISAC JAPAN 企画調整部部長                                  |
| 伊藤 光恭 | 日本電信電話株式会社 情報流通プラットフォーム研究所<br>セキュアコミュニケーション基盤プロジェクトグループリーダー |
| 鵜飼 裕司 | 株式会社フォティーンフォティ技術研究所 代表取締役社長                                 |
| 片山 昌憲 | エキサイト株式会社 サービスマネジメント室                                       |
| 再起 和夫 | パナソニック株式会社 参事   |
| 杉浦 芳樹 | 日本シーサート協議会 運営委員会委員長   |
| 鈴木 律郎 | 社団法人情報サービス産業協会 企画調査部 技術課長                                   |
| 高橋 正和 | マイクロソフト株式会社 チーフセキュリティアドバイザー                                 |
| 名和 利男 | 株式会社サイバーディフェンス研究所 上級分析官                                     |
| 松並 勝  | ソニーデジタルネットワークアプリケーションズ株式会社<br>セキュリティテクノロジスト                 |
| 三好 眞  | 株式会社アイ・エス・レーティング 執行役員 格付部長                                  |

## 1.5. 検討経緯

本事業の検討経緯を以下に示す。

### (1) 情報セキュリティに係る各専門分野の情報共有・連携推進会議

|       |                     |          |
|-------|---------------------|----------|
| 第1回会合 | 1月29日（金）10:00-12:00 | 於三菱総合研究所 |
| 第2回会合 | 2月17日（水）15:00-17:00 | 於三菱総合研究所 |
| 第3回会合 | 3月17日（水）13:00-15:00 | 於三菱総合研究所 |

### (2) リスク要件リファレンスモデル作業部会

|       |                    |                   |
|-------|--------------------|-------------------|
| 第1回会合 | 12月22日（火）1600-1800 | 於内閣官房情報セキュリティセンター |
| 第2回会合 | 2月3日（水）10:00-12:00 | 於三菱総合研究所          |

第3回会合 3月12日(金) 10:00-12:00 於三菱総合研究所

(3) 組織リスク動的判断モデル作業部会

第1回会合 2月12日(金) 10:00-12:00 於内閣官房情報セキュリティセンター

第2回会合 3月3日(水) 14:30-17:00 於三菱総合研究所

第3回会合 3月8日(月) 10:00-12:00 於三菱総合研究所

(4) 連携マップ作成作業部会

第1回会合 2月5日(金) 10:00-12:00 於内閣官房情報セキュリティセンター

第2回会合 2月22日(月) 10:00-12:00 於三菱総合研究所

第3回会合 3月12日(金) 13:00-15:00 於三菱総合研究所

## 2. 検討成果サマリ

本事業を構成する、「リスク要件リファレンス作業部会」、「組織リスク動的判断モデル作業部会」、「連携マップ作成作業部会」における検討成果の概要を以下に示す。

### 2.1. リスク要件リファレンスモデル作業部会

「リスク要件リファレンスモデル」は、「現状脅威に基づく設計要件の要否判断に基づいた対策設計」を行うためのツールとして開発したもので、官公庁および民間の情報システム構築の際に、発注者と受注者が共通の理解に基づいた、情報システムへの情報セキュリティ対策設計の支援を目的としている。

「リスク要件リファレンスモデル」とは、高度化した現状脅威と組織への影響問題点の共通認識に基づき、対策の要否判断と実効性の有る対策設計を可能とする仕組みであり、その為の参照ドキュメント体系とその対策分析の連携スキーム構築から成る。

#### リスク要件リファレンスモデル(RM)を一言で言うと...

サイバー攻撃対処情報を共有

高度化したサイバー攻撃に対処する新たな防御モデルを開発

現状の高度化した脅威と組織への影響問題に対する共通認識に基づき、コスト対効果を勘案した対策の要否を判断し、実効性の有るシステム設計対策を可能とする仕組み。  
(参照ドキュメント体系とその分析スキーム構築)

- 何のためのセキュリティか？ (目的思考)
- 対策の理由は何か？ 何から何を守りたいのか？ その効果は？
- 組織ビジネス (業務) への影響はなんなのか？
- その上でやるべき事 (コストに見合う対策はどれか) を決める為の方法論？

- 昔は「1脆弱性=1攻撃」の個別攻撃モデルであり対処判断は単純。現在は多様な意図に基づく「複合多段型攻撃の組織攻撃モデル」のため、対処判断が困難。
- 脅威の全体像が判らないため、組織業務への影響、危険性が理解出来ない。このため、迅速な組織の対応判断と影響を極限化する有効な対策立案が行われない。
- 従来のサイバー攻撃解説は「攻撃手法に主眼」が置かれているため攻撃全容が判らない。現攻撃は各手法の組み合わせであり「攻撃戦術」と「防御対策戦術」の解説が必要。
- サイバー攻撃の全体像が見えにくくなっており、意味を伝えられないのが有効な対策立案と適正コストを判断出来ない原因。
- 一方、脅威の全体像は単一組織や単一分析分野では整理出来ないため、他分野連携が必須。
- 脅威全容と危険性影響の分析に基づく、情報システムの設計管理対策に関する整理や対策分析の連携スキームが存在しない。

脅威の全容を把握した上で脅威の意味を正確に理解し、組織への影響問題に軸足を置いて考えるための方法論と対策分析連携スキームが必要。

図 2-1 リスク要件リファレンスモデルとは

◆対処が必要なサイバ脅威を組織の影響問題視点で判断し有効な対抗策を考える仕組みを考えたい。

「現状脅威に基づく設計要件の必要要否判断を可能とし、必要な対策設計を可能とする仕組み」  
 →脅威・危険性分析を基に、セキュリティ設計管理対策の「理由」を定量定性的に明示。  
 →種々相互関係ポイントでの正確な検討調整に資する。  
 →必要性和効果を認識した上で、システム開発を行える手法の開発

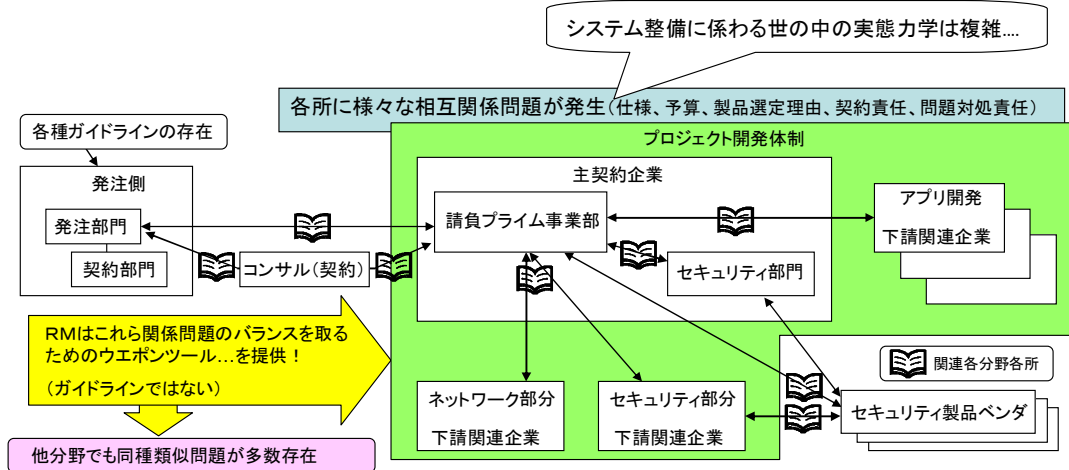


図 2-2 リスク要件リファレンスモデルの目的

また、リスク要件リファレンスモデルは、対象リスクにCND(サイバー攻撃対処)を主たる脅威として作成されている。

同分野は変化が激しく、かつ攻撃全容の把握と理解が困難であるため有効な対策立案が後手になりがちな「攻防非対称特性」を持つ。

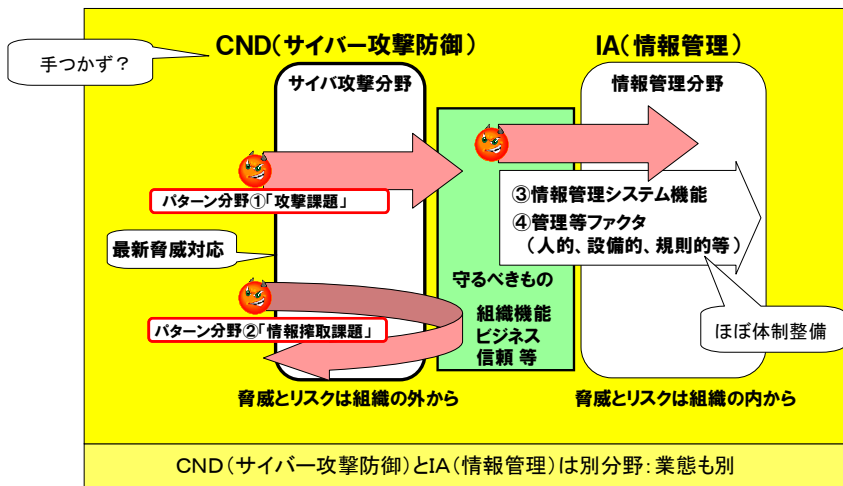


図 2-3 リスク要件リファレンスモデルにおける対象分野設定

### 2.1.1. リスク要件リファレンスモデル開発の目的とモデルの構成

「リスク要件リファレンスモデル」の開発は、これまで主要なセキュリティ対策と考えられてきた、セキュリティ製品を情報システム内に配置する手法が、標的型攻撃などの新たなサイバー攻撃手法の出現により、著しく有効性が低下していることが背景となっている。この状況を解決するため、脅威の実態に基づき、事業および業務への影響を評価し、必要とされる対策とコストを明らかにしする手法が必要とされている。

このため、脅威に対する影響と対応必要性を判断し、効果と必要コストを事前に机上確認した上で契約発注及びシステム設計開発に盛り込むための新たな手法方法論としてRMを作成した。

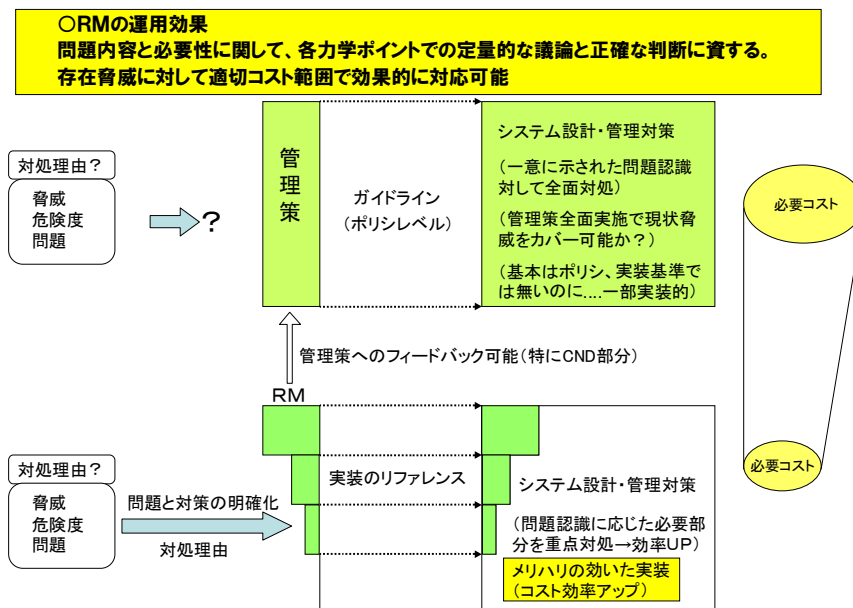


図 2-4 リスク要件リファレンスモデルにおける対象分野設定

リスク要件リファレンスモデルは、この課題に取り組んだもので、情報システムの納品後に問題になることの多い情報セキュリティ対策を、契約発注時やシステム設計時に、必要となるコストと共に明示的に組み入れることを目指している。なお、リスク要件リファレンスモデルは、設計手法や方法論の基本参照モデルであることから、各情報システムの特性を踏まえて利用することを前提としている。

リスク要件リファレンスモデルは、受発注時の共通の理解の形成に加え、攻撃の高度化・複雑化と、これに伴う被害の潜在化によって、部門間、組織間での連携が難しくなっている現状において、脅威に対する共通の理解を構築するための基盤となり、連携を円滑に進める上での有効なツールになるものと考えている。

RM ドキュメントは、手法方法論の参照基本モデルとして作成しており、各分野特性を踏まえて同種方法論が各分野組織毎に展開される事を前提としている。

また、RMドキュメントの一部である「重要脅威カタログ」はサイバー脅威の実像や影響を具体的

に定義できるため、混乱している問題整理を解きほぐす効果は高く、関連業界分野における情報連携スキームへと発展することを期待。

リスク要件リファレンスモデルの基本概念を図2-5に示す。これら概念に基づき分析された結果がセットとして整理されている。

リスク要件リファレンスモデルは、実際のサイバー攻撃の分析を通じて得られた脅威とその振る舞いをグループ化した「脅威振る舞いパターン」、情報システムをその構成と構造によってグループ化した「システムトポロジーモデル」、システムトポロジーモデル毎に現実の脅威に基づく対策をまとめた「対策セット」で構成される。

「脅威分析」で整理される各パターン毎の攻撃仕様は、攻撃解析情報の中から情報システムの設計管理に係わる部分を抽出して整理したものであり、脅威分析分野とシステム設計分野双方の視点が合致して始めて「机上模擬攻撃トレース」結果から分析される「設計管理対策」が整理可能となる。

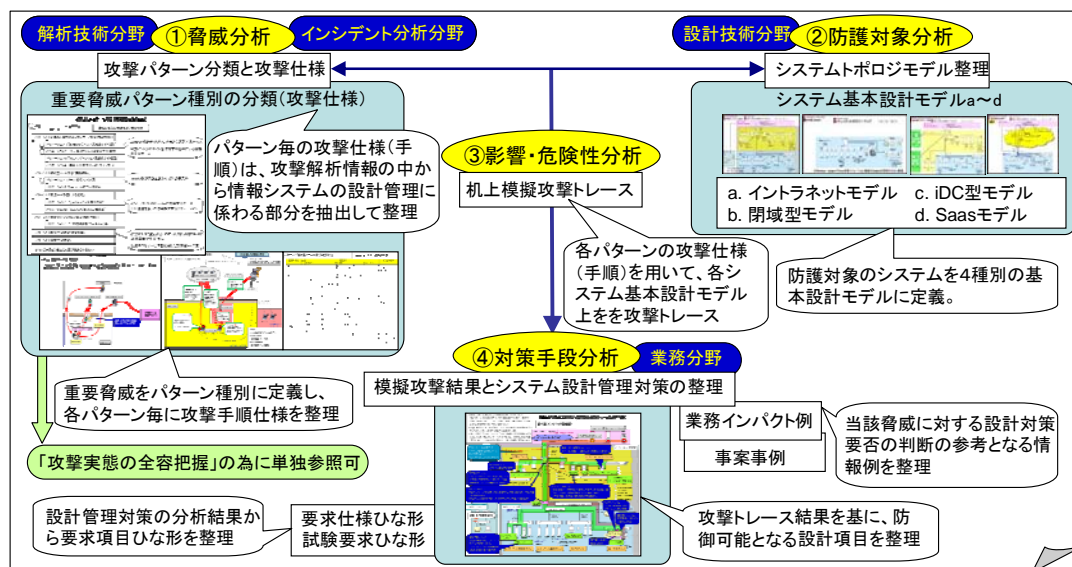


図 2-5 リスク要件リファレンスモデルの基本概念

リスク要件リファレンスモデルは、システム設計を理解し、サイバー攻撃防御(CND)の知見を持つ技術者(RMフルセット利用者)が利用することで、最大限の効果を発揮するが、各種調整場面や説明等を行う際に、それぞれの目的に応じて必要となる一部のコンテンツを抜き出して利用することも想定している。

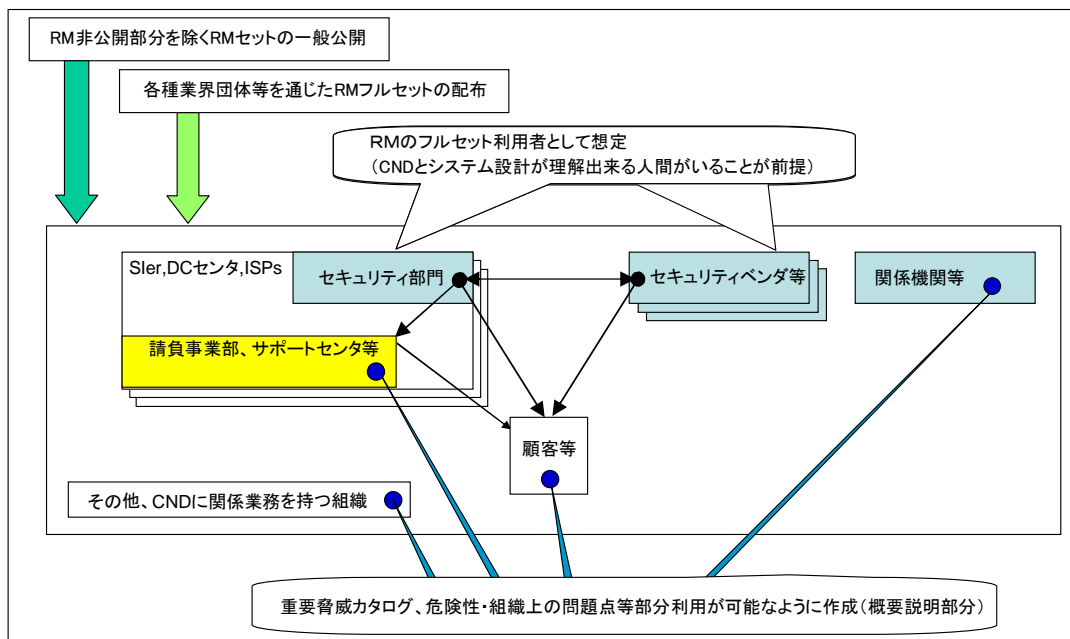


図 2-6 想定されるリスク要件リファレンスモデルセットの利用者

### 2.1.2. 振る舞いモデル

今日の脅威は、多様化・高度化・複雑化しているため、個別に対処を行っていたのでは、影響の分析や対策の立案が困難であり、契約段階や設計段階で対策を決定することは不可能である。このため、リスク要件リファレンスモデルでは、実際に確認された脅威の振る舞いを分析することにより、脅威を6つのパターンに分類し「重要脅威カタログ」として取りまとめ、これを分析したものを「振る舞いパターン」として整理した。

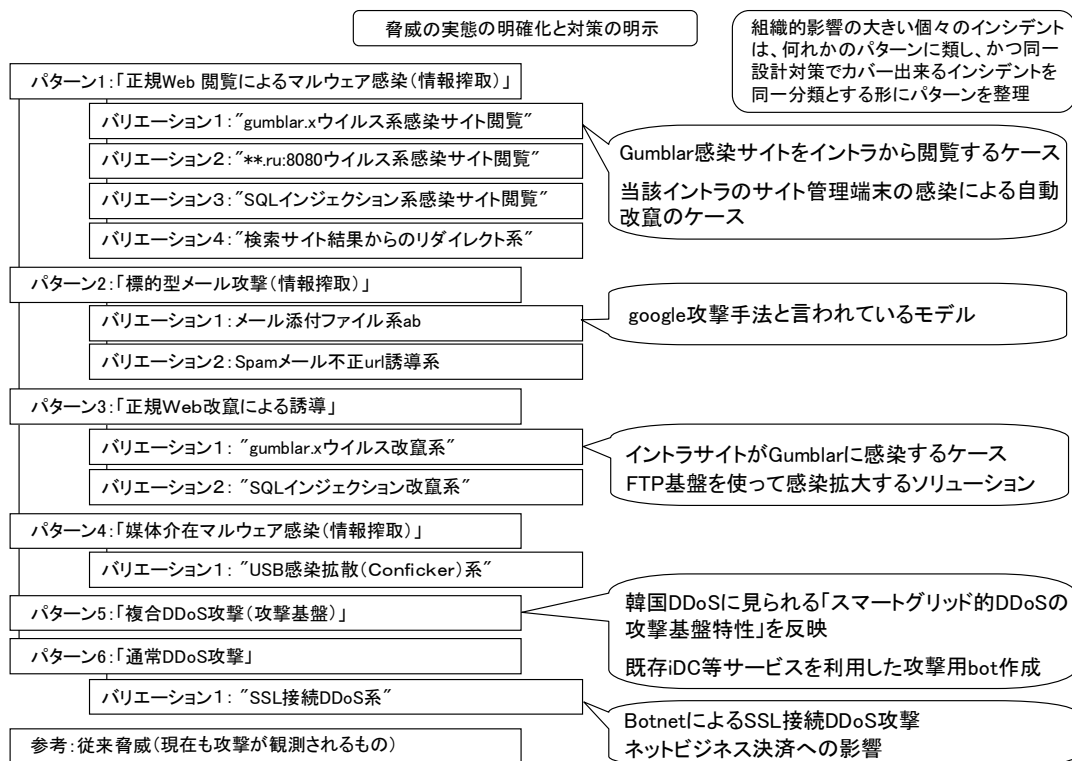


図 2-7 重要脅威カタログ

図 2-8 は、パターン1:「正規 Web 閲覧によるマルウェア感染(情報搾取)」の振る舞いパターンの概要図である。この図に見るように、「振る舞いパターン」は、攻撃のシーケンスと攻撃の機能仕様を中心に、分析整理した結果を記載している。

パターン1:「正規Web 閲覧によるマルウェア感染(情報搾取)」

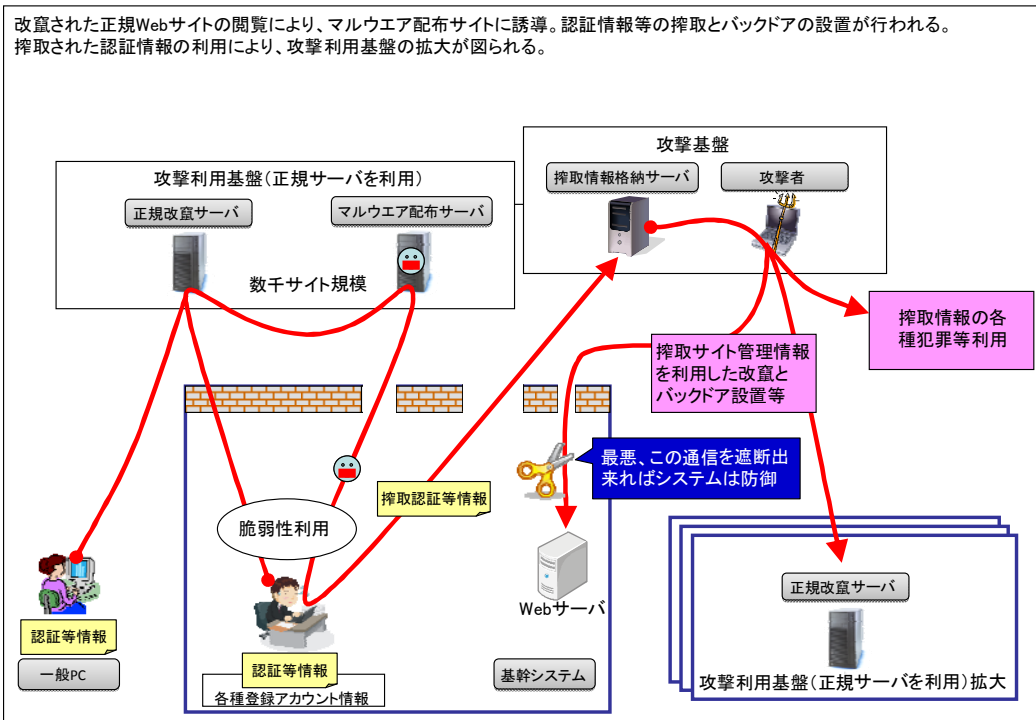


図 2-8 「正規 Web 閲覧によるマルウェア感染(情報搾取)」の振る舞いパターン概要図

「振る舞いパターン」で整理した攻撃シーケンスと攻撃の機能仕様は、後述する「トポロジーモデル」上でのトレース(机上での動作シミュレーション)を通じて、影響と危険性の評価と、対策のための設計要素を導くために利用する。

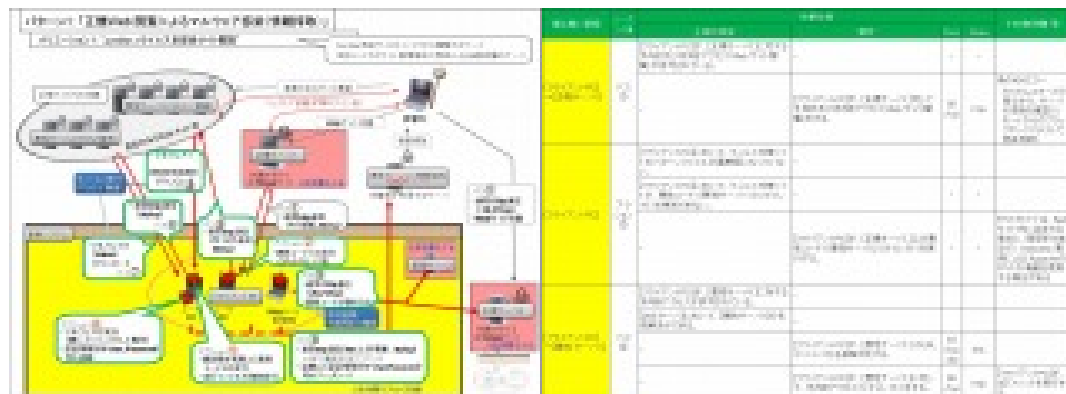


図 2-9 攻撃シーケンス及び攻撃仕様

### 2.1.3. システムトポロジーモデル

情報システムが攻撃を受けた際の脅威(ウイルス等)の振る舞いを分析するため、典型的な情報システムの構成例を4つの「システムトポロジーモデル」として整理した(表 2-1)。なお、クラウドコンピューティングや自動車・家電などの組み込みシステムは対象から外している。

各システムトポロジーモデルは、必ずしも単独で利用されるわけではなく、たとえば「イントラネットモデル」と「iDCモデル」の組み合わせなど、複数のモデルを組み合わせることも念頭に置いている。

表 2-1 システムトポロジーモデル

- |               |
|---------------|
| A. イン트라ネットモデル |
| B. 閉域型モデル     |
| C. iDCモデル     |
| D. SaaSモデル    |

図 2-10 は、A. イン트라ネットのトポロジーモデルである。実際に SI 業務を行っている設計者の視点から、典型的なシステム構成やセグメント構成を整理している。

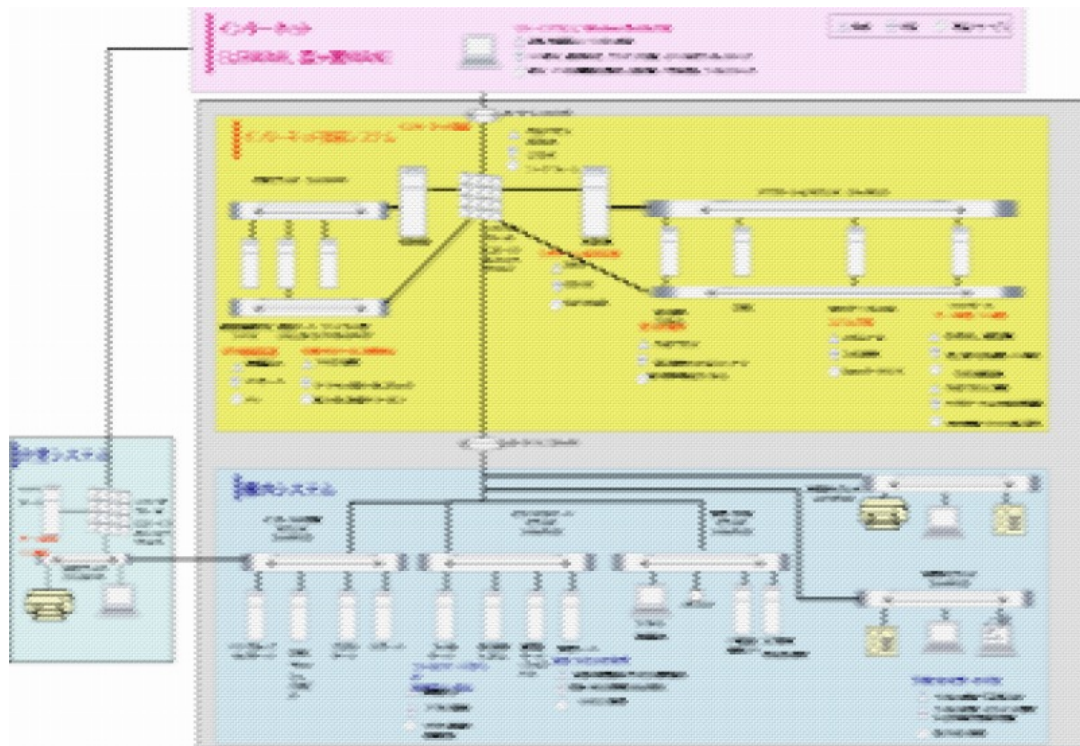


図 2-10 イン트라ネットモデルの構成図

## 2.1.4. 設計対策セット

「振る舞いモデル」で作成した「振る舞いパターン(攻撃シーケンス及び攻撃仕様)」の、各「システムトポロジーモデル」上での動作を分析するための「脅威トレース」(机上シミュレーション)により、トポロジー上に実装されたセキュリティ対策の効果を評価し、脅威を抑止するための技術的な手法をベストプラクティクスとして検討した。また、「脅威トレース」は、実攻撃事案の発生状況に即した状態で行った。

これらの結果をトポロジーモデル別・振る舞いパターン別にまとめ、「設計対策セット」とした(表2-2)。

表 2-2 対策セット一覧

|          |                                   | トポロジーモデル                |       |       |       |       |
|----------|-----------------------------------|-------------------------|-------|-------|-------|-------|
|          |                                   | A                       | B     | C     | D     |       |
| 設計対策セット  |                                   | インターネット                 | 閉域型   | iD C  | SaaS  |       |
| 振る舞いパターン | パターン1: 「正規Web閲覧によるマルウェア感染 (情報搾取)」 |                         |       |       |       |       |
|          | バリエーション1:                         | gumblar.xウイルス系感染サイト閲覧   | 1.1-A | 1.1-B | 1.1-C | 1.1-D |
|          | バリエーション2:                         | **..ru:8080ウイルス系感染サイト閲覧 | 1.2-A | 1.2-B | 1.2-C | 1.2-D |
|          | バリエーション3:                         | SQLインジェクション系感染サイト閲覧     | 1.3-A | 1.3-B | 1.3-C | 1.3-D |
|          | バリエーション4:                         | 検索サイト結果からのリダイレクト系       | 1.4-A | 1.4-B | 1.4-C | 1.4-D |
|          | パターン2: 「標的型メール攻撃 (情報搾取)」          |                         |       |       |       |       |
|          | バリエーション1:                         | メール添付ファイル系ab            | 2.1-A | 2.1-B | 2.1-C | 2.1-D |
|          | バリエーション2:                         | Spamメール不正url誘導系         | 2.2-A | 2.2-B | 2.2-C | 2.2-D |
|          | パターン3: 「正規Web改ざんによる誘導」            |                         |       |       |       |       |
|          | バリエーション1:                         | gumblar.xウイルス系改ざん系      | 3.1-A | 3.1-B | 3.1-C | 3.1-D |
|          | バリエーション2:                         | SQLインジェクション改ざん系         | 3.2-A | 3.2-B | 3.2-C | 3.2-D |
|          | パターン4: 「媒体介在マルウェア感染 (情報搾取)」       |                         |       |       |       |       |
|          | バリエーション1:                         | USB感染拡散 (conficker) 系   | 4.1-A | 4.1-B | 4.1-C | 4.1-D |
|          | パターン5: 「複合DDoS攻撃 (攻撃基盤)」          |                         |       |       |       |       |
|          | パターン6: 「通常DDoS攻撃」                 |                         |       |       |       |       |

図 2-11 は、脅威トレースの例で、振る舞いパターン1、バリエーション1を使い、イントラネットトポロジーモデル上で脅威トレースを行っている。青い吹き出しは、脅威トレースで明らかになった効果の高い対策を示している。

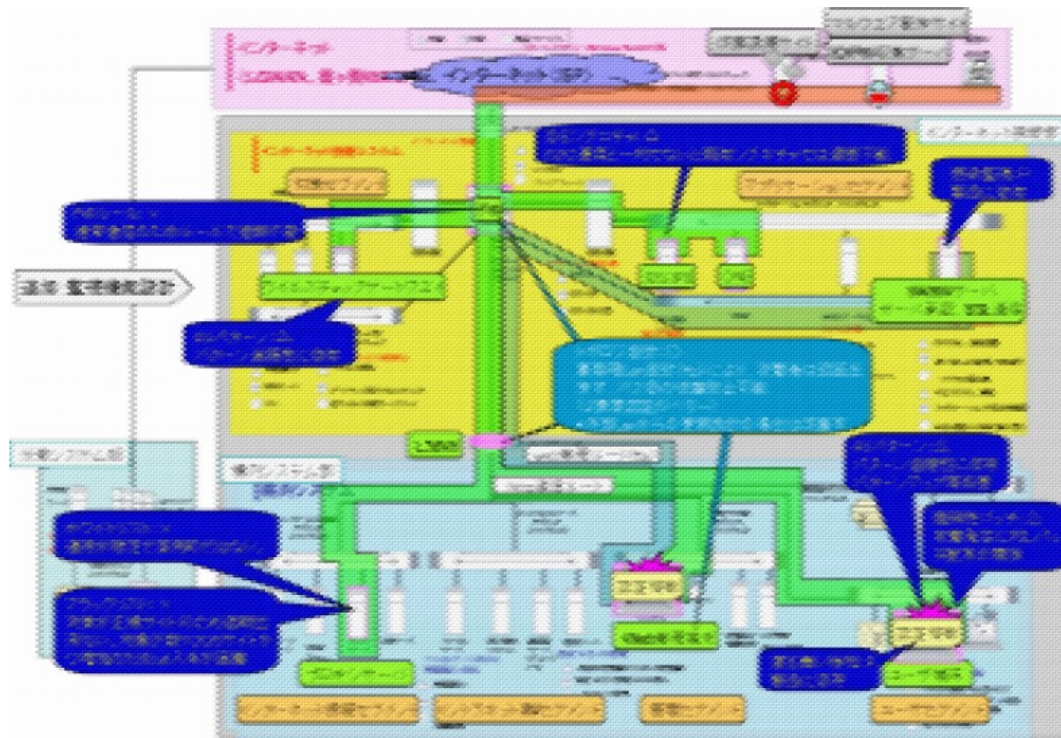


図 2-11 イン트라ネットモデル上での脅威トレース結果サマリ(パターン1・バリエーション1)

設計対策セットは、脅威トレースで得た分析結果に基づいて、本事業に参加した専門家が、具体的な設計対策として整理したものである。設計対策セットは、対策の必要性を検討し、必要と判断した対策については、システム発注要件や基本設計に具体的に組み入れるためのリファレンスとなるとともに、システム発注時に要求仕様項目ひな形や、試験要求項目ひな形として、利用することも想定している。

表 2-3 トポロジー別・振る舞いパターン別設計対策セットの例

| システム<br>脆弱性<br>基   | 振る舞いパターン                                      | 設計対策と運用管理対策 |          |
|--------------------|---|-------------|----------|
|                    |   | 対策番号        | 対策の内容及効果 |
| イントラ<br>ネット<br>サーバ | 振る舞いパターン1:<br>正規Web閲覧による<br>マルウェア感染<br>(情報搾取) | A010        | ...      |
|                    |   | A030        | ...      |
|                    |   | A040        | ...      |
|                    |   | A060        | ...      |
|                    |   | G010        | ...      |
|                    |   | G030        | ...      |
|                    |   | G050        | ...      |
|                    |   | G080        | ...      |

設計対策セットの実装要否を判断する上で必要となる、「組織上の問題点及び攻撃等事例」を検討する際の参考として、重要脅威カタログの各パターン毎に整理した。

リスク要件リファレンスモデルを参照する利用者自身の組織にとって、攻撃脅威が組織業務に与える影響問題点を確認する事により、対策実施可否及び優先度判断の資とするものである。

パターン1:「正規Web閲覧によるマルウェア感染(情報搾取)」

|  |
|--|
| <p>・業務委託先の管理問題</p> <p>ガンブラ等の認証情報搾取と悪用のケースでは、管理業務を委託又は再委託先での感染ケースで起こる事が多い。管理責任が多岐に跨り、その責任の所在が不明確な事による対処の困難性を生んでいる。(コンテンツの外部委託形態と管理責任と監督責任)</p> <p>サイト管理を委託(再委託先に表看板を預ける)している構図の中で、「表看板」を預けている再委託先での感染が非常に多いのが現状。管理責任の分散拡大が背景であり、盲点をつかれた形。</p> |
| <p>・契約責任問題</p> <p>サイト管理の委託構造が多層分散されている事により、事故発生時の賠償責任の所在と契約内容との関係が組織課題となる可能性がある。</p>   |
| <p>・信頼基盤を利用した攻撃拡散(前提の盲点)</p> <p>安全(な筈)として設計運用されているサービス網を攻撃基盤に使って脅威を拡散(安全の為に作った基盤の逆利用は想定外)は設計管理前提を崩す形になる。</p>   |
| <p>・共通基盤を介したリスクの伝搬</p> <p>今後、クラウド下に委託する事を考えると、共通管理セグメントを通じ一気に他社部分まで脅威が広がる事も有り得る。</p>   |

図 2-12 組織上の問題点の例

### 2.1.5. 運用解説書

リスク要件リファレンスモデルは、情報システムの発注者、受注者の双方が情報セキュリティ対策について検討するための枠組みである。すでに述べたように、実際に適用するシステムの特성에応じたカスタマイズが必要となることから、リスク要件リファレンスモデルの運用解説書を用意する。

具体的には、以下のステップを経て、発注者と受注者が、共通の認識を持つとともに、具体的な対策を必要なコストと共に、システム発注要件や基本設計に組み込んでゆく。

1. システムの特性に近い「トポロジーモデル」を選択し、必要な修正を加える
2. システム利用形態や特性から、検討が必要な「振る舞いパターン」を特定する
3. 特定した振る舞いパターンを、トポロジーモデル上で「脅威トレース」を行う
4. 脅威トレースの結果に基づき、対処すべき問題と脅威を特定する
5. 「設計管理対策セット」を参照し、対策設計項目を立案する

\* 組織(社)内のセキュリティ設計要件リストと照合して設計管理対策セットを確定する

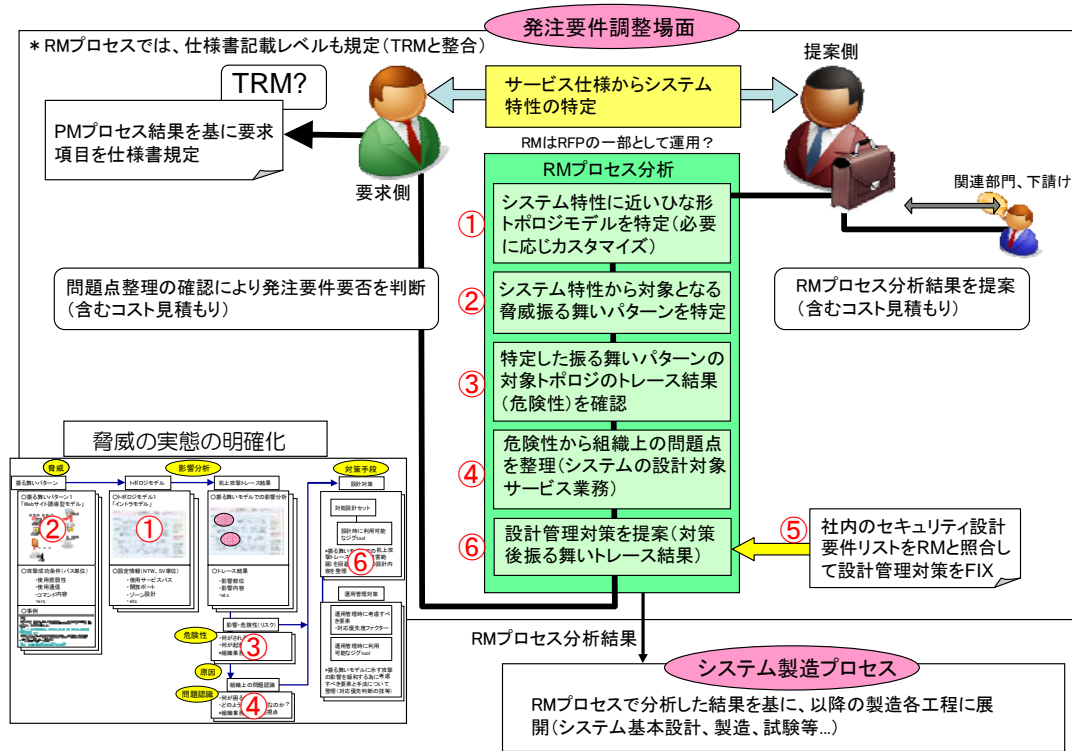


図 2-13 想定されるリスク要件リファレンスモデル運用形態(基本形態)

また、脅威実態の理解やインシデント発生場面での影響判断等リスク要件リファレンスモデル各コンテンツの一部を利用する運用についても整理している。

## 2.2. 組織リスク動的判断モデル作業部会

情報セキュリティ対策は、対応すべき脅威や関連する技術など、様々な側面において環境の変化が急速に進んでいる。また、近年の攻撃手法の高度化や、対策の深化に伴う情報セキュリティに係る専門分野の多様化により、分業化が進みつつある。刻々と変化する状況を適切に把握し、新たに発生する課題に対して的確な対応を行うためには、関係する専門分野の横断的な取り組みが必要であり、部門間で情報を共有し連携して対処していくことが重要である。

本作業部会では、環境そのものの変化の中で、各部門が連携しながら適切な判断を下すスキームを「組織リスク動的判断モデル」として定義した。また、具体的な進め方についても検討し「組織リスク動的判断モデルに関するチャート」としてまとめている。

### 2.2.1. 組織とインシデント対応を巡る現状

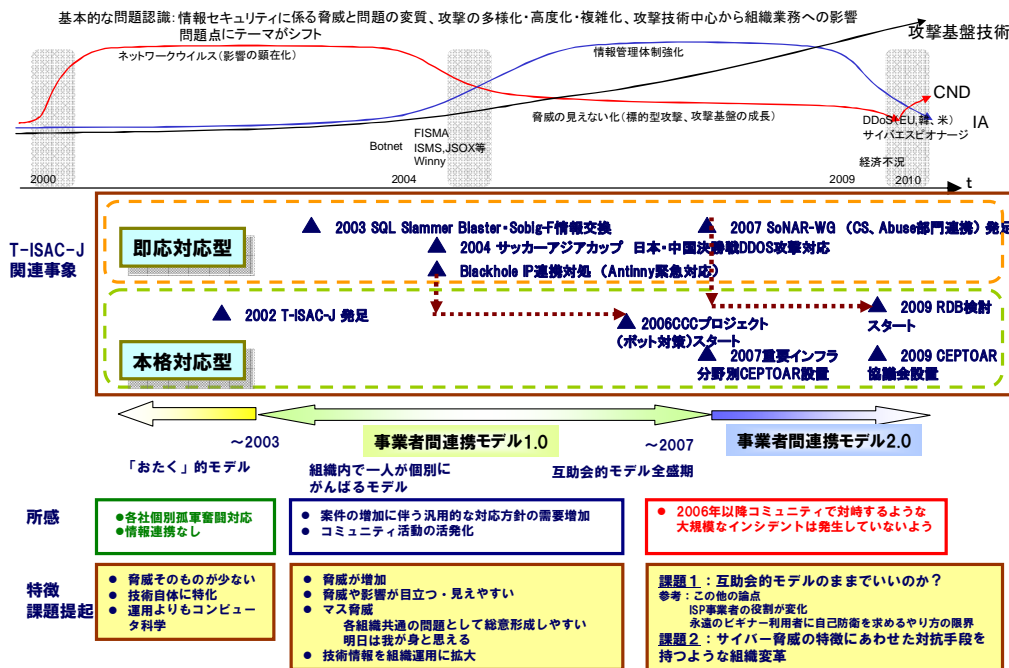
#### (1) 脅威の変化に伴って生じた課題

インターネットの普及に伴い、2000年頃からネットワークウイルスによる脅威の顕在化が進んできた。しかし、2004年頃から、攻撃の悪質化・複雑化が進み、特定のターゲットを狙った標的型攻撃へと移行し、ボットネットなどの攻撃基盤が構築されるに伴い、脅威そのものを認識することが難しくなった。

一方、やはり、2004年頃から、ISMS、個人情報保護法、J-SOX等に対するコンプライアンスを目的とした、情報管理体制の強化が求められるようになり、技術的な攻撃への対処という側面が強いサイバー攻撃防御(CND: Cyber Network Defence)から、組織における情報資産管理(IA: Information Assurance)が、情報セキュリティの中心的なテーマと考えられるように変化した。

一方で、攻撃手法は継続的に悪質化・複雑化が進んでおり、今日では、情報資産管理を中心とした対策だけでは対応が難しいと考えられるようになり、改め技術的な対策としてのサイバー攻撃防御の重要性が認識され、より本格的な対策としての発展が期待されるようになった。

このような変化に伴い、対応組織も変化も迫られている。社会を席卷するような大規模インシデント(マス脅威)が発生しにくい現状では、脅威が局所化することから、これを共有することは困難である。このため、「マス脅威」に対しては有効に機能していたインシデント対処手法が、効果的に機能しにくい状況にあることから、現状の脅威に即した新たな対応スキームが必要とされている。



資料: Telecom-ISAC Japan

図 2-14 脅威の変化と組織モデル

## (2) 技術専門部署の役割変化

ネットワークワームなどを前提とした、従来のインシデント対応は、脆弱性情報の入手、暫定的な対応の実施、パッチの適用、感染したウイルスやワームの駆除を中心としたもので、これらの作業を迅速かつ的確に行うことが重要視されていた。このため、均質性の高い、技術的な対策が中心であったことから、情報システム部門が中心的かつ指導的な立場で取り組む場合が多かったと考えられる。

今日においては、攻撃の手法や攻撃のターゲットとなるソフトウェアが多様化し、ソフトウェア、ハードウェアのマルチベンダ化、運用のアウトソース化が進んだことから、システムの全体像や依存関係を把握することが難しく、脅威と対策の一般化も困難な状況にある。このため、インシデント発生時に責任の所在が不明確になり、対応のたらい回しになってしまい、問題が解決しないという事態が起きやすい状況にある。

また、経済動向の変化や、経営スタイルの変化に伴い、情報システム部門が最適化＝スリム化する傾向も影響を与えている。この結果、インシデント発生時に必要とされる技術的な解析や検証作業を行うリソースの確保が難しく、問題の解決を長期化させるばかりでなく、再発防止策の実施などの事後対応にも予算が割けず、リスクを抱えたままで運用を続けるケースもあるものとみられる。

このような背景から、インシデント発生時に、情報システム部門が全体のバランスを取りながら、指導的な役割を果たすことが難しくなっており、単なる調整者という意味でのコーディネーションに終始する傾向が強まっている。

### (3) 組織風土に合った技術専門部署の概念

インシデント対処を行う組織としての CSIRT (Computer Security Incident Response Team) は、欧米的な組織構造と組織運営を前提としている部分があり、日本の組織にそのまま適用することが難しい面がある。たとえば、多くの欧米の企業では、各業務を執行する責任が明確であり、それぞれ執行役などの役職として割り当てられている。一般に CSIRT はこのようなライン型の組織には属さないが、インシデント対処を執行する責任と権限が明確に与えられ、各事業部門に対しても強制力を持った対処が行える場合が多い。

多くの日本の組織では、そもそも執行責任という概念で事業運営が行われていることは少なく、CSIRT も明確な執行権が与えられず、各事業部門への強制権を持たないことから、調整機関としての役割に終始する場合が多い。

一方で、日本は自然災害に対する緊急対応の経験が豊かであり、独自のノウハウを持ち、非常時に対応する仕組みや体制を有している事も少なくない。また、日本の企業運営においては、役割と責任が、欧米ほど明確ではない反面、各部門が専門部署に頼らずに自らの努力で解決を試みる姿勢が強い。日本におけるインシデント対応を考える上では、この姿勢は大きな強みとすべきである。

CSIRT の位置づけについて考えると、グローバル化が進んだといわれる現在においても、組織の特性や文化は、国や組織によって大きく異なっている。CSIRT が、インシデント対処時に有効に機能するためには、所属する組織の特性や文化を考慮した取り組みが必要である。

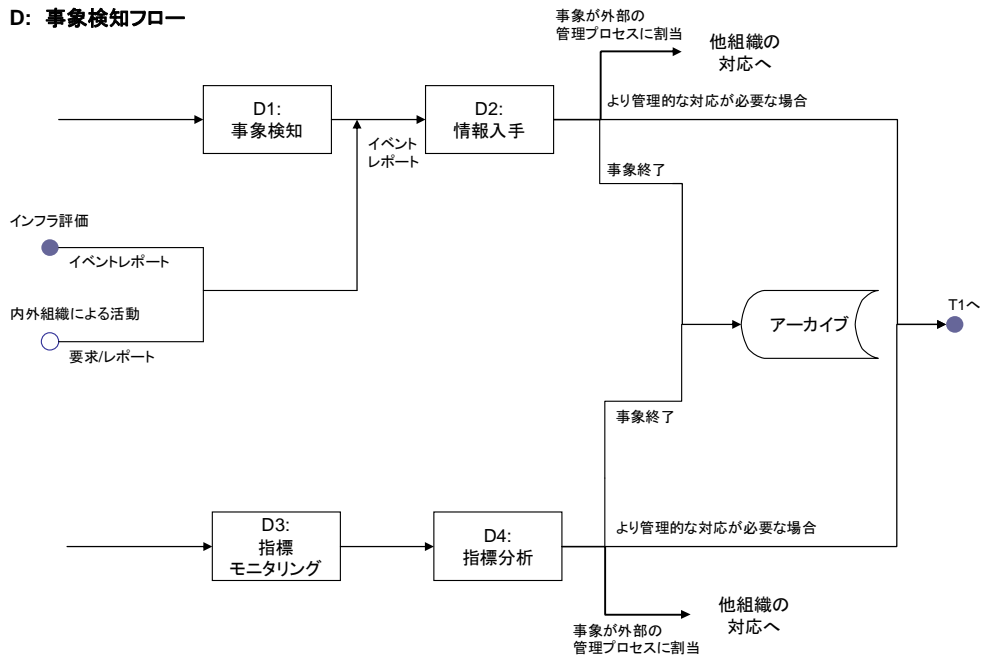
#### 2.2.2. 動的判断モデルチャート

米国型 CSIRT のモデルに基づき、インシデント発生時の組織における動的判断モデルチャートの例を示す。

図 2-15 は、事象を検知する際のフローで、事象の検知、モニタリングにおける指標の分析から、エスカレーションにいたるパスを例示している。

図 2-15 は、トリアージフロートと呼ばれるもので、事象を分析・分類し、適切な対応先へと割り当てを行うためのものである。

**D: 事象検知フロー**



資料: CMU-SEI-2004-TR-015 を基に MRI 作成

図 2-15 動的判断モデルチャートの例:事象検知フロー

**T: トリアージフロー**

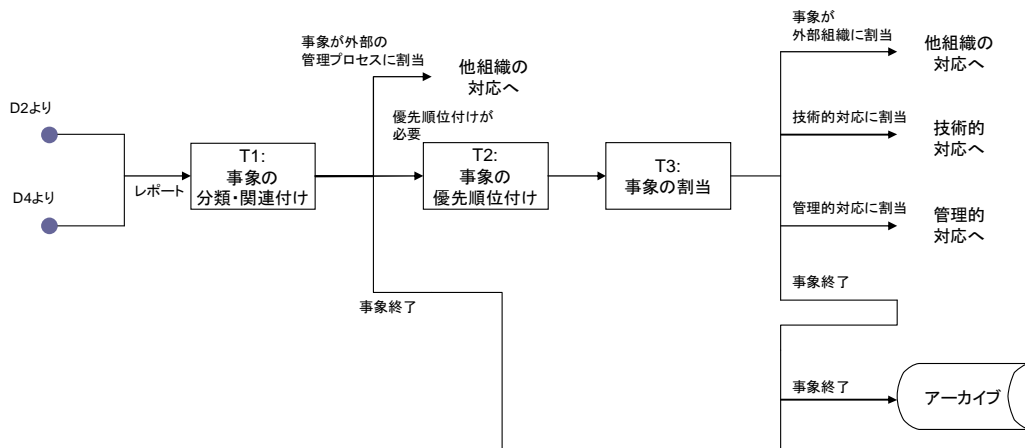


図 2-16 動的判断モデルチャートの例:トリアージフロー

動的判断モデルチャートが有効に機能するためには、インシデント発生時に「何が起きているのか」、「何を守らなければならないか」、「何を判断しなければならないか」、「何の情報をどう使うのか」について、組織間、部門間で共有していることが重要である。インシデント対応時の各部門

の目的と必要な情報の一例を、表 2-4 に示す。

表 2-4 インシデント対応時の各部門の協力体制と必要な情報

| 組織               | 個別の目的       | 協力阻害要因         | 必要な情報               |
|------------------|-------------|----------------|---------------------|
| 米国本社             | 信頼の回復       | 高コスト           | 何が問題なのか             |
| 法務               | 信頼の回復       | 高コスト           | 証拠となる事実・情報<br>勝てる方法 |
| RMO<br>リスクマネジメント | 再発防止        | 情報セキュリティ部門との重複 | 発生原因                |
| 広報               | 適切な情報公開     | 知らない人に知らせること   | 対策の進捗               |
| 情報セキュリティ         | 根本原因と真実の追及  | 真実を認めない        | 調査の技術               |
| 事故発生部門           | お客様との関係修復   | お客様の不利益        | 対応の進捗               |
| 購買               | -           | 契約書変更など        | 具体的な内容              |
| コールセンター          | -           | 判断を伴う対応        | 技術のサポート<br>情報の伝え方   |
| IT部門             | 効果的なシステムの導入 | 作業の発生          | 発生原因                |

資料:IBM資料(一部MRI変更)

### 2.2.3. まとめ

本調査においては、情報システムとビジネス環境の変化の現状の分析に基づき、情報セキュリティに関わるインシデント発生時の技術専門部署の課題と、企業形態に即した有効性の高いインシデント対応のあり方について検討を行った。また、情報セキュリティに関わるインシデントの発生時の動的判断について、各主体が状況に応じて最適な判断を行うための動的判断モデルチャートを作成し、効果的に運用するための条件について整理した。

情報システムが事業継続のための重要な基盤になると共に、情報セキュリティ上の脅威の質が変化している。企業においては事業継続の観点から、インシデント対処が再考されており、その結果、技術専門部署に求める役割が変化している。技術専門部署においても、従来の業務や役割の枠組みに留まっていたは、事業の経営・運営に即した効果的な対応を行うことが難しくなっている。

情報システム部門においても、企業における事業継続マネジメントの一環として情報セキュリティを捉えなおし、インシデント対応ばかりでなく、平常時の事前予防の活動も視野に入れ、組織内外における各部門・組織の効果的な情報共有・連携対処の方法を継続的に検討し、効果的な事後対応体制と手順を整備していく必要がある。

### 2.3. 連携マップ作成作業部会

「組織リスク動的判断モデル」では、組織内のインシデント対処を中心に取まとめたが、「連携マップ」は、関連する事業分野が各専門分野を活かした連携を行うために必要となる要素を分析し、この結果に基づいて「連携マップ」を作成する。連携マップは、情報セキュリティに係る関係者の特定と連携要件の分析、問題の時系列変化に基づいて作成した。

従来は、情報セキュリティに関する連携が想定されていなかった分野も含めて検討を行った結果、新たな連携手法と連携スキームについて整理することができた。

#### 2.3.1. 情報セキュリティに関する時系列俯瞰図(連携マップ)

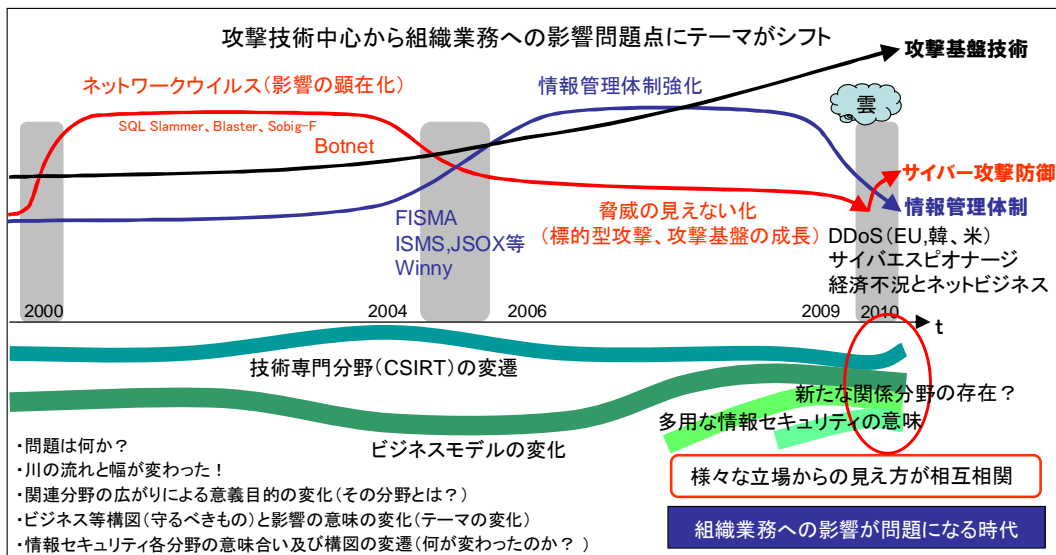


図 2-17 情報セキュリティ各分野の意味合い及び構図の変遷<sup>4</sup>

これまでの情報セキュリティに関する流れを俯瞰すると、2000 年前後のネットワークウイルスの蔓延により、サイバー攻撃防御(CND)注目されるようになり、2004-2005 年頃には、FISMA、ISMS、J-SOX 等の導入や、P2P 型ファイル共有ソフト(Winny 等)による機密性の高い情報流出事件の多発などに伴い、情報保証(IA)が情報セキュリティの中心的なテーマと考えられるようになった。2006 年頃から、サイバー攻撃の組織化と犯罪マーケットの融合を背景に、攻撃が経済的な目的へと移行し、攻撃の分析や対策が困難な状況におかれている。2009 年頃より Gumblar 被害、米韓への DDoS 攻撃、Google 問題などの事案の顕在化により、この状況が強く認識され、現在の攻撃手法に対応したサイバー攻撃防御(CND)が注目されるようになっている。

<sup>4</sup> 第 1 回 MAP—WG資料 MAP1-4 各作業部会の概要(P29)

一方で、情報セキュリティ対策のコーディネーションに着目すると、これまで脆弱性や動勢情報と言った、技術的な枠組みを中心としたCSIRTが主な役割を担ってきた。しかし、攻撃が経済的な目的へと移行し、デジタル家電のインターネット接続が一般化するなど、従来のCSIRTでは考慮されていない、経済分野などの幅広い分野での連携を考える必要に迫られている。

### 2.3.2. 組織連携成立のセオリー

異なる組織が連携するためには、それぞれの目的を相互に理解し、信頼関係を構築する必要がある。連携における具体的な活動(共同部分)は、この関係に基づいて決定される。活動がWin-Winの関係を実現することで連携が強化され、情報交換の活性化、信頼関係の強化へとつながり、価値の高い情報が共有されるようになる。このような情報の流通は、連携のネットワークを強化し、組織連携の価値を高めていくことになる。

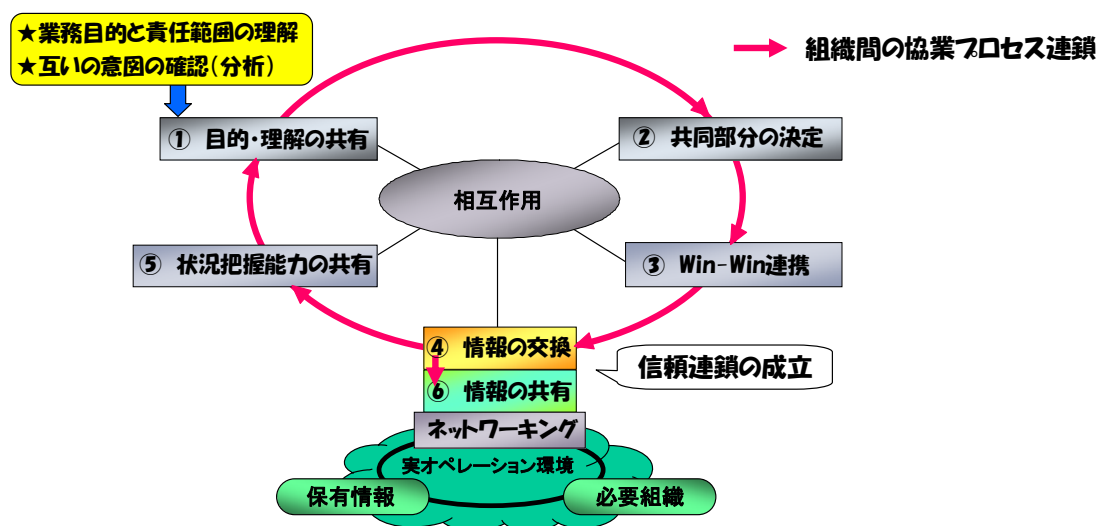


図 2-18 組織間連携の成立要件<sup>5</sup>

組織間連携においては、以下のような情報運用の原則がある。この原則に沿って組織間の連携が成立するのであり、情報共有だけを目的とした連携は成立し得ない。

- |                          |                  |
|--------------------------|------------------|
| 1. need to Know          | 必知事項である          |
| 2. Give & Take           | Take & Give ではなく |
| 3. Win-Win               | 相互に利益のある         |
| 4. Correlation analysis  | 情報見積             |
| 5. informational purpose | 情報目的             |
| 6. Reliability           | 信頼関係             |

<sup>5</sup>第1回MAP-WG資料MAP1-4 各作業部会の概要(P29)

加えて、運営の費用負担、共通の理念や利害関係、連携に係るマスタープラン、具体的な目標（当面、中長期）、定期的な活動の実施が必要である。

### 2.3.3. 課題

本作業部会では、これまで情報セキュリティにおいて考慮されてこなかった、広範囲な分野との連携の必要性について調査と分析を行った。しかし、このような連携は、まだ現実のものとなっていない。このため提案している連携スキームを実際に構築し、その有効性を確認していく必要がある。

本事業では、本事業の中核であるリスク要件リファレンスモデルの拡充・強化を軸にした「リスク要件リファレンスモデル運用連携スキーム」を仮構築し、他の作業部会の成果を活用しながら検証するとともに、ここで提案する連携スキームの有効性を明らかにすることを検討している。

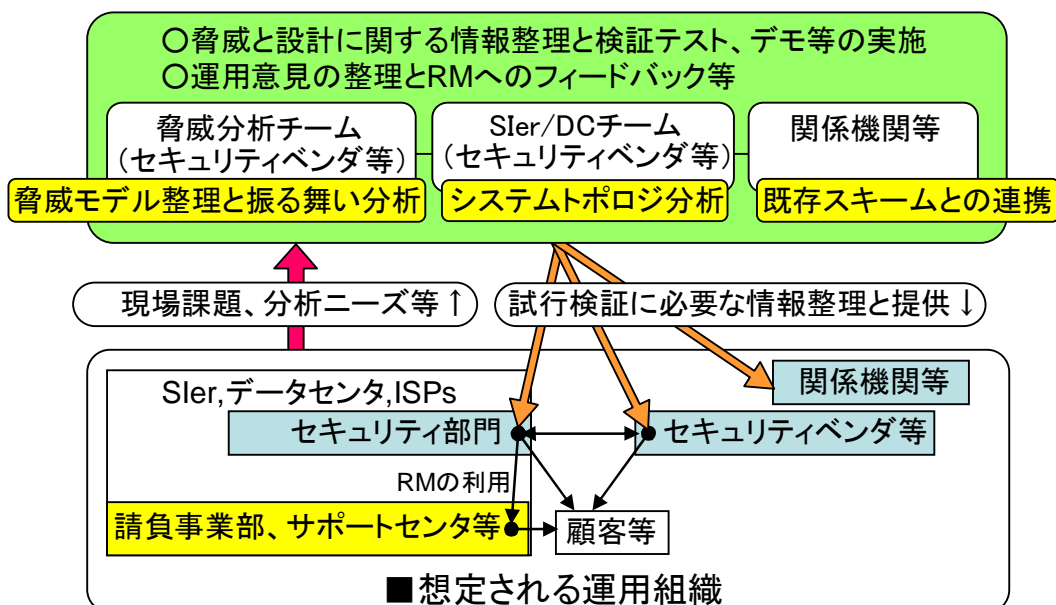


図 2-19 リスク要件リファレンスモデル作成時の連携スキーム

この運用連携スキームは、従来は必ずしも連携が十分でなかったセキュリティベンダ（専門家）と Sler のセキュリティ部門（実務家）の知見を融合し、変容する情報セキュリティの脅威に対抗するための有効なアプローチになると考えられる。こうした取組は ICT 分野が業界横断的な連携を行うための基盤としての側面も持つことになる。

#### 2.3.4. まとめ

インターネットの発展と共に利用目的も広がり、関係する業種・業態も多様化している。同様に、攻撃目的も愉快犯から金銭目的へと変化し、攻撃手法は組織化された高度化している。さらに、脅威の対象も、PCやサーバーから様々なデバイスまで拡大している。

これまでは技術的な問題と考えられていたインターネットの脅威は、インターネットのインフラ化やビジネスモデル変化により、事業に対して直接的な脅威を与えるようになっている。このため、情報セキュリティ対策は、ビジネス的な観点に基づいた施策が必要であり、従来の枠を超えた、幅広い業界・分野との連携を模索する必要性が高まっている。

しかしながら、業界・分野を横断した組織間連携は、参考になる前例もない上に、本質的に成果が見えにくい面がある。加えて、組織間連携として、単に情報交換を目的とした連携スキームは目標や意義が不明瞭であり、うまく機能しない場合が多い。幅広い業界・分野との組織連携を模索するに当たっては、共通の理念や利害関係を明らかにし、連携のマスタープランを策定した上で、具体化した短期的、長期的な目標を共有する必要がある。

### 3. 今後の展開

本年度を「リスク要件リファレンスモデル」、「組織リスク動的判断モデル」、「連携マップ作成」の基本部分の作成と位置付け、来年度は、情報セキュリティ脅威の実態を踏まえたシステム設計管理対策の強化・普及を図ることとし、仮にこれを「リスク要件リファレンスモデル Phase-2」とする。

強化・普及にあたっては、民間エリアを対象とした普及方策検討の為の新体制をセットし、継続的な運用と定着方策を検討する。

#### 3.1. 普及方策検討計画(案)

リスク要件リファレンスモデルの強化・普及を行うため、「リスク要件リファレンスモデル運用連携スキーム」を構築する。この体制は、試行検証によるニーズ調査及び発展拡張部分等の抽出、各種既存スキームを念頭にした普及方策の検討を行う為の調整機能として位置付けられるほか、「情報システム調達のための技術参照モデル (TRM) <sup>6</sup>」をはじめとした既存スキームや関係機関との協同普及展開の準備を行う。

なお、リスク要件リファレンスモデルの一般への公開については、組織が想定している脅威を露呈する危険性があることから、公開する範囲及び手段並びに提供内容についても検討を行う。

#### 3.2. リスク要件リファレンスモデル運用連携スキーム (案)

リスク要件リファレンスモデルの運用時に必要となる各種分析や新たなサイバー攻撃手法の出現等に即時対応するための場として、「リスク要件リファレンスモデル運用連携スキーム」を構築し、必要な情報等の提供交換の場とする。

同時に、各種運用場面において得られたシステム開発場面以外での副次効果等含む運用結果をリスク要件リファレンスモデルの強化改善にフィードバックし、リスク要件リファレンスモデルの実用性と実効性を向上させる。



図 3-20 リスク要件リファレンスモデル運用連携スキームの構造

<sup>6</sup> 情報システム調達のための技術参照モデル(TRM) 経済産業省、独立行政法人 情報処理推進機構  
<http://www.ipa.go.jp/software/open/osscc/download/trm20.pdf>