

# 情報セキュリティ研究開発戦略

2011年7月8日

情報セキュリティ政策会議



# 目次

1	はじめに	2
2	これまでの取り組み	3
	(1) 経緯	3
	(2) これまでの情報セキュリティ技術の開発モデル	3
3	情報セキュリティに係る環境変化	5
	(1) 我が国の情報セキュリティを取り巻く環境の変化	5
	(2) 情報セキュリティ研究開発予算の推移	6
	(3) 研究開発戦略の諸外国における取組	8
4	情報セキュリティ研究開発戦略	9
	(1) 基本的考え方	9
	(2) 研究開発戦略のコンセプト	12
	(3) 研究開発の投資タイプ	15
5	情報セキュリティの研究開発における重要分野	17
	(1) 情報通信システム全体のニュー・ディペンダビリティの確保	17
	(2) 攻撃者の行動分析に基づくゼロデイ・ディフェンス	20
	(3) 個人情報等の柔軟管理の実現	21
	(4) 研究開発の促進基盤の確立と情報セキュリティ理論の体系化	23
6	東日本大震災を踏まえた重点分野	26
	(1) 耐災害性に強い情報通信システムの構築	26
	(2) 「リスク・マネジメント」等	27
	(3) 個人情報等の柔軟管理の実現	28
	(4) 「ニュー・ディペンダビリティ」	29

## 1 はじめに

我が国の情報セキュリティ政策は、「国民を守る情報セキュリティ戦略」（平成 22 年 5 月 11 日 情報セキュリティ政策会議決定、以下「情報セキュリティ戦略」という。）及びその年度計画である「情報セキュリティ 2010」（平成 22 年 7 月 22 日 情報セキュリティ政策会議決定、以下「年度計画」という。）に基づき、官民が連携して推進しているところである。

情報セキュリティに係る研究開発については、「情報セキュリティ戦略」において、「米国等の動向も踏まえ、情報セキュリティに係る研究開発を戦略的に推進するため、新たな情報セキュリティ研究開発戦略を策定する」と規定され、年度計画において、「情報セキュリティに係る研究開発を戦略的に推進するため、2011 年 6 月を目途に新たな情報セキュリティ研究開発戦略を策定する」とされている。「情報セキュリティ研究開発戦略」（以下、「研究開発戦略」という。）は、これに基づき策定するものである。

また、情報セキュリティに係る研究開発は、我が国の科学技術戦略とも密接に関係する。我が国の科学技術戦略については、今後 5 年間（2011 年度から 2015 年度）を対象とした「第 4 期科学技術基本計画」（以下、第 4 期基本計画）という。）の基となる「諮問第 11 号『科学技術に関する基本政策について』に対する答申」（平成 22 年 12 月 24 日 総合科学技術会議決定）において、「重要課題達成のための施策の推進」の中の「国家存立の基盤の保持」のための施策として、「能動的で信頼性の高い（ディペンダブルな）情報セキュリティに関する技術の研究開発の推進」が謳われている。本研究開発戦略は、これを具体化するためのものであると位置づけられる。

本研究開発戦略の対象期間は、情報セキュリティ戦略や第 4 期基本計画との整合性を図るため、基本的には 2011 年度～2015 年度とするが、研究開発を戦略的に推進するため、中長期的な課題も盛り込んでいる。

なお、研究開発戦略を推進するため、「技術戦略専門委員会」において官民連携、国際連携を含め各施策の評価を定期的に行い、必要に応じて取組内容の見直しを行うものとする。

## **2 これまでの取り組み**

### **(1) 経緯**

2005年に総合科学技術会議における第3期科学技術基本計画（以下、「第3期基本計画」という。）の策定が進められる中、情報セキュリティに焦点を当てた技術戦略の在り方を検討し、2005年11月に「技術戦略専門委員会報告書」を取りまとめた。

2006年3月に閣議決定された「第3期基本計画」における情報通信分野に係る分野別推進戦略では、報告書で提示した様々な方策が取り入れられるとともに、情報セキュリティが「戦略重点科学技術」の一つとして位置づけられた。

その後、最新の動向を反映させたフォローアップ作業や、我が国における情報セキュリティに係る研究開発・技術開発の実施状況の俯瞰などを行い、2007年6月には「技術戦略専門委員会報告書 2006」、2009年4月には「技術戦略専門委員会報告書 2008」を取りまとめ、それらに基づき研究開発・技術開発を推進しているところである。

### **(2) これまでの情報セキュリティ技術の開発モデル**

これまでの情報セキュリティに係る研究開発・技術開発では、大きく二つの目標設定が行われてきている。

一つは、現在運用されている情報システムにおけるリスクを把握し、そのリスクを低減し、かつ、ゼロに限りなく近づけるための技術開発である。

もう一つは、脅威をモデル化し、情報処理システムとネットワークにおけるリスクをゼロにするための新たなアーキテクチャを実現する、中長期的な目標設定を行った研究開発である。

また、「高度情報通信ネットワークを安心して利用可能」な環境を

- ① そもそも「高度情報通信ネットワークが安全である」こと
  - ② 利用者が、「高度情報通信ネットワークが安全である」と分かる（認識・体感できる）こと
  - ③ 万が一事故が起こった場合でも、その被害の局限化や救済等が図られるとともに業務の継続性が保たれること
- と定義し、それらに寄与する研究開発・技術開発を推進してきたところである。

しかしながら、これらの研究開発・技術開発を推進する中においても、年々、新たに取り組むべき課題が出現しているのが現状である。

例えば、

- ① 情報機器やデバイスの急速な普及と高機能化及び、サービスの多様化などに

伴って、国民の情報通信技術への依存度が高まり、情報セキュリティに係る課題として扱うべき範囲が大幅に拡大している。また、急速に拡大する情報通信技術の利活用に、情報セキュリティ技術の開発が対応できていない。

- ② マルウェアの増加に加え、新たな脆弱性の発見や攻撃手法の開発スピードが加速化していることから、従来の情報セキュリティ対策では対応しきれないケースが増加してきている。
- ③ 既存の情報セキュリティ技術の限界を補完する組織・人間系の管理手法とのバランスが確保できていないことや、高齢化など世代構成変化に対応し、サービスや製品の設計・開発に際して、使い方が簡単で利用者のミスがリスクにつながらないための改善策なども十分ではない。

「情報システムのライフサイクルから捉えると、ある世代の情報システム・アーキテクチャから次の世代の情報システム・アーキテクチャへとシームレスに進化させていくための情報セキュリティに係る課題解決は、“moving target”型課題解決とも言える。具体的には、

- ・新しい世代のアーキテクチャに移行することによりリスクが変容し、システム可用性や事業継続性などの目標値も動的に変化する
- ・新たな技術やシステム構成要素の導入によって、リスクの変容が発生する
- ・攻撃側は、絶えず新しい技術を利用し、ターゲットシステムを攻撃することが可能という防御側との非対称性が存在する
- ・上記の原因が複合的に働くことで、課題を取り巻く環境は、常に変化しているといえる。このような状況の中で、これらの課題を克服できる情報システム・アーキテクチャや、開発・運営・保守プロセスを確立し、最終的には、①情報資産と情報処理の保護、②事業継続性の円滑な確保を実現しなければならない。

2005 年以降、これらの課題を解決するため、情報セキュリティに係る研究開発の推進の重要な柱として、「グランドチャレンジ型研究開発・技術開発」を掲げ推進してきたところである。グランドチャレンジ型研究開発・技術開発とは、近年の科学技術研究の問題として、研究領域の細分化や先鋭化が進んだことにより、研究実施の目標設定が短期的なものになったり、他の研究領域との連関性を意識しない研究実施になったりするケースが増加していることを踏まえ、これらを解決する方策の一つとして、10 年程度の長期間にわたる持続的な研究開発を念頭に置いて、特定の大目標を設定し、その大目標の実現に向けて各種要素技術全体の統合的開発を行う研究開発・技術開発である。

基本的には、この考え方を包含するとともに、先述した新たな課題が今後益々複雑化・多様化する傾向にあることを踏まえ、新たな研究開発戦略を策定することとする。

### 3 情報セキュリティに係る環境変化

#### (1) 我が国の情報セキュリティを取り巻く環境の変化

##### ① 情報通信技術の変革

近年、コンピュータ・リソースの仮想化によるクラウド・コンピューティング（以下、「クラウド」という。）の活用や、端末のユビキタス化、高度な組み込みソフトウェアのシステム化などが目覚ましく進展しており、今後、更に加速化すると思われる。また、家庭やオフィスなどに様々なセンサーが設置され、リアルタイムセンシング機能の強化や位置情報やユーザー情報を活用したコンテキストウェアネス化（Context Awareness）<sup>1</sup>の動きなども加速化すると予想される。さらにスマートフォンの飛躍的な発展やソーシャル・ネットワーク・サービス（SNS：Social Network Service）といった新しいコミュニケーションサービスが急速に普及している。

技術革新の著しい情報通信技術の動向を予測することは、困難な面もあるが、今後益々、ユビキタス化やリアルとバーチャルを融合する技術などが発展すると思われる。これらの新たな情報通信技術を支える情報セキュリティ技術が求められている。

##### ② 情報セキュリティの脅威の高度化・多様化

大規模サイバー攻撃の発生、大規模なシステム障害の発生、大規模な個人情報の漏えいなど情報セキュリティに係る脅威は、ますます大規模化・高度化・複雑化してきている。コンピュータウイルスの種類が増加状況だけを見てもその増加傾向は顕著である。

最近の新しいタイプの攻撃として、「Operation Aurora」<sup>2</sup>と呼ばれる攻撃や、「Stuxnet」<sup>3</sup>ウイルスによる攻撃を代表例として挙げることができる。これらは、一般的な防護システムを回避するように、既存の攻撃手法を巧みに組み合わせ、さらに攻撃目標に合わせて設計されており、APT（Advanced Persistent Threats<sup>4</sup>）と呼ばれる新たな脅威が出現している。また、普及が目覚ましいス

<sup>1</sup> コンピュータがセンサーやネットワークを介して様々な事柄に関する状況の変化を自動的に認識し、状況の変化に応じて対応することができるという概念。

<sup>2</sup> Internet Explorer の脆弱性を狙うゼロデイアタックによってエンドユーザーのコンピュータを乗っ取り、遠隔操作によって特定企業のシステムに侵入し、スパイ行為や知的財産の窃取などを行うサイバー攻撃。

<sup>3</sup> 複数の脆弱性を悪用して Windows PC に感染し、原子力発電所の制御システムへ侵入して、その制御システム上にある装置に攻撃を加えるコンピュータウイルス。独シーメンス社の PLC（プログラマブルロジックコントローラ）向けソフト「WinCC/Step7」の脆弱性を狙い、PLC に悪質なコードを書き込むことで、原子力発電所の制御システムに悪影響を及ぼすよう仕組まれていた。

<sup>4</sup> 情報窃取や組織の重要な局面に関する弱体化又は妨害、あるいは将来においてこれらの目的を実現するための準備行為を目的として、標的とした組織の IT インフラ中に足場を構築し利用し続けることを目的に、

スマートフォンを狙った脅威や、新しいビジネスモデルとして注目を集めているクラウドに係わる脅威なども新しい脅威として挙げることができる。

更に、マルウェアを簡単な操作だけで作成できるツールの売買や搾取した認証情報やクレジットカード情報を換金する仕組みがアンダーグラウンド市場で成立しており、営利目的と思われる攻撃主体が台頭しているという問題もある。

このような状況を見ると、サイバー空間においては、防御側よりも攻撃側が有利という状況は変化していないのみならず、攻撃側が優位な状況が加速化しているとも言える。このような状況をどう改善、克服するか大きな課題である。

### ③ 東日本大震災の発生

東日本大震災（以下、「大震災」という。）は、大規模な地震、津波、原発事故など、これまで経験したことのない複合的な大災害であり、東日本のみならず我が国の社会・経済に甚大な損害をもたらした。既存の情報通信インフラも壊滅的な被害を受け、情報の途絶が救助・救援、復旧を遅らせるとともに人々の不安を増大させた。また、社会経済活動の基盤となる情報が円滑に流通しないことにより、様々な活動が停滞を余儀なくされた。今般の大震災を踏まえ、バックアップシステム、非常用電源の強化、クラウドの活用などにより、耐災害性に強い情報通信システムを検討し、再構築するとともに、事業継続計画（BCP：Business Continuity Plan）についても抜本的な見直しを行う必要がある。

また、大震災が発生し、状況がダイナミックに変化することで、リスクに対する社会の捉え方や許容できるリスクレベルも大きく変容する。災害時には、最適な対応を行うための「ダイナミック・リスク対応」の観点を持つことが必要である。「リスク・コミュニケーション」、「リスク・マネジメント」の重要性が改めて認識されたところであるが、これらの分野における知見は現時点で必ずしも確立されておらず、早急に検討する必要がある。

#### （２）情報セキュリティ研究開発予算の推移

我が国の情報セキュリティ研究開発予算は、2006年度は91.2億円であったが、2010年度は48.6億円となっており、この5年間に約47%の大幅な減少を示している。

一方、米国の研究開発予算は、2007年度から2011年度まで増加傾向にあり、5年間で91%程度増加し、2010年度は366億円（4.07億ドル）<sup>5</sup>である。

日米の予算を比較すると、2007年度には、米国192億円（2.13億ドル）、日

---

複合的な攻撃手法を用いることにより、目的達成の機会を作出することができる、高度な専門的知識と莫大なリソースを有する攻撃主体（NIST SP800-39 “Managing Information Security Risk: Organization, Mission, and Information System View” 【Appendix B GLOSSAR Y】）

<sup>5</sup> 為替レート1ドル=90円で換算。

本 77.1 億円であり、GDP 比では日米ほぼ同程度の予算規模であったが、2010 年度には、米国は 366 億円へと増加し、日本は 48.6 億円へと減少しているため、GDP 比で比較すると 3.02 倍の格差となっている。

諸外国が情報セキュリティに係る研究開発に力を入れている中、我が国の状況は、憂慮すべき状態にあると言わざるを得ない。

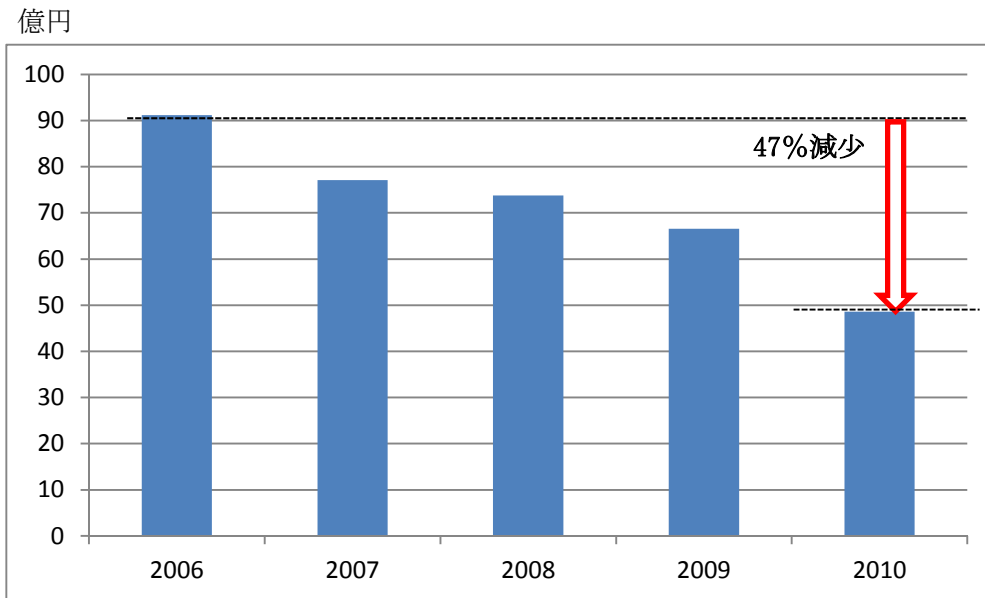


図 1 日本の情報セキュリティ研究開発予算の推移<sup>6</sup>

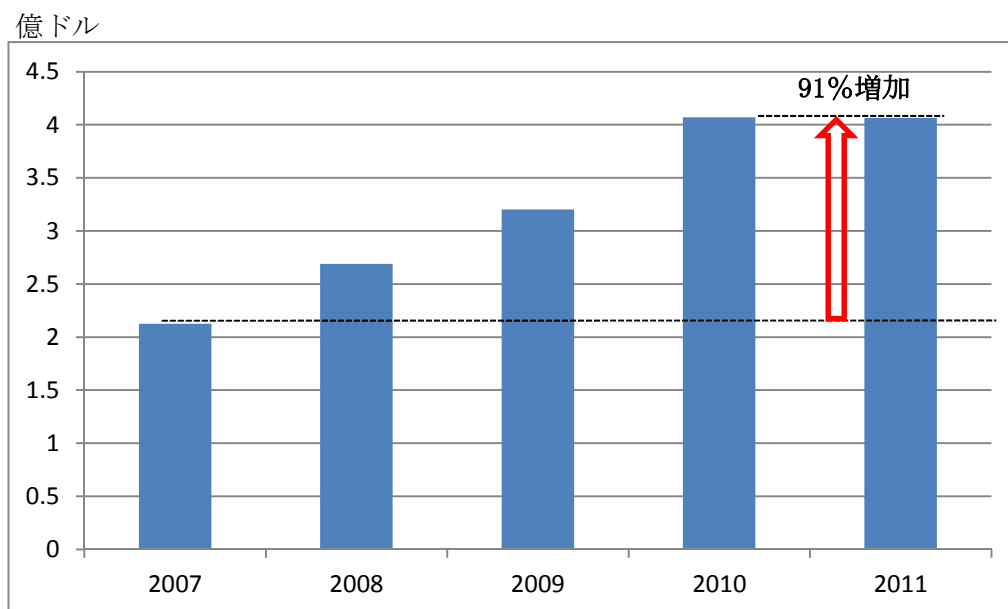


図 2 米国の情報セキュリティ (NITRD CSIA) 研究予算の推移<sup>7</sup>

<sup>6</sup> 総合科学技術会議 基本政策専門調査会平成 21 年度フォローアップ調査票を元に作成

<sup>7</sup> NITRD 大統領予算教書補足資料を元に作成

	2007 年	2010 年
GDP の比率（米国／日本）	2.12	2.49
研究開発予算の比率（米国／日本）	2.48	7.53
研究開発予算の GDP 比率（米国／日本）	1.17	3.02

図 3 日米の研究開発予算の GDP 比率

### (3) 研究開発戦略の諸外国における取組

#### ①米国の研究開発動向

米国の情報セキュリティの研究開発は情報通信産業の競争力強化や国家安全保障等の側面から、様々な省庁によって実施されており、それぞれの省庁が対象とする研究分野・予算スキームが異なる。そこで、連邦政府全体で効果的な研究開発戦略を策定するために各省庁間の調整が図られている。

また、トップダウンの方針に基づく予算措置と、実際に研究開発を実施するための技術的な根拠に基づく予算措置、実際に研究開発を実施するための技術的な根拠に基づく研究分野の整理、各組織間の調整や実施計画の策定等のボトムアップの検討が相互に繰り返されることで、現場のニーズに根ざした研究を拾い上げるとともに、ダイナミックな社会の変化に対して迅速に対応する機能を持たせている。(参考資料 4.(1) 参照)

#### ②EU の研究開発動向

EU では、情報通信分野の研究開発の目的は、欧州の情報通信産業の競争力強化及び、情報通信技術の欧州域内での普及とされており、社会・経済的側面に重点を置いたプログラムが設定されている。そのため情報セキュリティに関わる研究テーマもツールや標準、メトリクス、評価手法、ベストプラクティス等の実用化を前提としたものが重視されている。また、研究スキームにも、欧州以外の地域との戦略的連携関係構築や、中小企業の研究開発支援、一般に向けた成果のアピール等、競争力強化及び情報通信技術の普及を推進する仕組みが取り入れられている。(参考資料 4.(2) 参照)

## 4 情報セキュリティ研究開発戦略

### (1) 基本的考え方

情報セキュリティに係る研究開発・技術開発は、「技術戦略専門委員会報告書」等に基づき、推進してきたところであるが、最近の環境変化や諸外国の動向などを踏まえ、新たに研究開発戦略を策定する。一方、研究開発戦略は、中長期的に推進すべきテーマであることから、研究開発戦略では、基本的に、従来推進してきた考え方を包含するとともに、新たな環境変化に的確に対応するため、新たな研究開発テーマを掲げるとともに一層の重点化を図ることとした。

従来の研究開発・技術開発に係る取組においても「リスクをゼロにするための新たなアーキテクチャを中長期的に実現する」という目標を掲げてきたところであるが、昨今の情報セキュリティを取り巻く環境の変化を見ると、攻撃側と防御側の非対称性が顕在化している傾向にある。分かりやすく表現すれば、攻撃側が優位な状況が改善できていないと言える。そこで、研究開発戦略の最大の特徴として、攻撃側が優位な状況から防御側が優位な状況に「ゲーム・チェンジ」するための革新的な取組に重点を置くこととした。換言すれば、情報セキュリティに係る研究開発は、「攻め」と「守り」（発生したサイバー攻撃の被害を最小化する）の分野に大別できるが、研究開発戦略では、「攻め」（サイバー攻撃を無効化するとともに、攻撃者の経済的負担を増大させることなど）に重点を置き、より安心・安全で、新しい価値を創造でき、社会を支える情報通信システムを実現するための研究開発を促進することとした。

研究開発を促進するにあたっては、先導的研究開発、高度情報セキュリティ人材育成、情報セキュリティ産業の活性化の好循環構造が構築できるよう積極的に取り組むことが重要である。

また、大震災は、科学技術の在り方にも大きな問題を提起した。震災からの復旧・復興、そして新たな成長に寄与する観点から、情報セキュリティと密接に関連する「ニュー・ディペンダブルな情報通信システム」、「リスク・マネジメント」、「リスク・コミュニケーション」など災害時における安全性向上に資する研究開発に重点を置くこととする。

研究開発戦略の基本的考え方は以下のとおりである。

- ① 「能動的で信頼性の高い（ディペンダブルな）情報セキュリティ」（以下、「ニュー・ディペンダビリティ」<sup>(注)</sup>という。）に係る研究開発を推進し、情報セキュリティ上の脅威の後追いとなる受動的な研究から、サイバー攻撃の非対称性を解消する能動的な研究に変えること等により、サイバー攻撃を無効化させるとともに、攻撃者の経済的負担を増大させるなど革新的な取組（いわ

ゆる、ゲーム・チェンジ) を促進することにより、世界を先導する。特に、情報システム全体の「ニュー・ディペンダビリティ」を確保することは、極めて重要である。

(注) 情報セキュリティは、従来、人間の不正行為に基づく事象を主な対象としていたが、情報通信技術への社会の依存度の増大に伴い、自然現象や経年劣化、ヒューマンエラー等も含めた事象への総合的対応が必要になり、従来のディペンダブルの概念を拡張するとともに、サイバー攻撃を無効化するなど「能動的」な情報セキュリティの要素を追加したものを「ニュー・ディペンダビリティ」という。

- ② 災害からの安全性向上に寄与するため、情報セキュリティの観点から耐災害性に強い情報通信システムの構築や「リスク・マネジメント」、「リスク・コミュニケーション」等に係る研究開発を促進する。
- ③ 我が国が将来にわたり持続的な成長を遂げるため、「グリーン・イノベーション」及び「ライフ・イノベーション」が成長の柱と位置付けられている。社会的なレベルでこれらのイノベーションを起こすためには、情報通信技術の活用は必要不可欠であり、特に、高度な情報セキュリティ基盤の構築は極めて重要である。社会的イノベーションを支える研究開発と連携を図り、高度な情報セキュリティ基盤の構築に寄与する研究開発を促進する。
- ④ 上記①とも関連するが、情報セキュリティについての課題を抜本的に解決するために、情報通信技術のパラダイムシフトを実現する次世代インターネットなどの革新的研究開発との連携を図る。また、情報セキュリティについての課題を抜本的に解決する観点から、科学技術分野の新たな研究テーマについても積極的な貢献を行う。
- ⑤ 情報セキュリティに係る研究開発を促進し、我が国の情報セキュリティ産業のグローバル展開に貢献する。
- ⑥ 情報が国境を越えて自由に流通する中、各国とも戦略的に情報セキュリティに係る研究開発を進めており、一国だけでは解決できない課題も増加していることから、一層の国際連携を促進する。
- ⑦ 研究開発戦略の推進にあたり、官民の役割分担を明確化するとともに、市場メカニズムを活用しつつ官民連携の促進を図る。また、研究開発の評価を適切に行うとともに、必要な予算の確保や研究開発の各段階における動機づけに努める。

## 基本的な考え方

- ①サイバー攻撃の非対称性を解消する(サイバー攻撃を無効化させ、攻撃者の経済的負担を増大させる)能動的研究に変える革新的取り組みの推進
- ②情報セキュリティの観点から耐災害性に強い情報通信システムの構築や「リスク・マネジメント」、「リスク・コミュニケーション」に係る研究の推進
- ③社会的イノベーションを支える研究開発と連携し、高度な情報セキュリティ基盤の構築に寄与する研究開発の促進
- ④次世代インターネットなどの革新的研究開発との連携
- ⑤我が国の情報セキュリティ産業のグローバル展開へ貢献
- ⑥研究開発における国際連携の推進
- ⑦官民の役割分担を明確化し、官民連携を推進。また、必要な予算の確保、研究開発の各段階における動機付けに努力

図 4 情報セキュリティ研究開発戦略の基本的な考え方

## **(2) 研究開発戦略のコンセプト**

研究開発戦略では、サイバー攻撃の無効化など「攻め」の発想によって、攻撃者の経済的負担を増加させる「ゲーム・チェンジ」に重点を置き、社会を支える基盤として、より安全・安心で、新しい価値を創造できる情報通信システムを実現するための研究開発を促進する。このため、図4に示すように、研究開発の対象を攻撃者、情報システム、利用者、それらを支える基盤に大別し、それぞれに必要な技術をマッピングしている。さらに従来のサイバー攻撃から情報システムを守るという狭義の情報セキュリティに、次世代インターネット環境を支える広義の情報セキュリティの観点を加えることとした。すなわち、後者が①情報システム全体のニュー・ディペンダビリティを確保するための技術であり、前者が②攻撃者の行動分析に基づくゼロデイ・ディフェンスである。また、組織・人間系の管理手法として利用者の観点で、③プライバシー情報等の自律管理性の向上技術がある。さらに、研究開発戦略は情報セキュリティの研究自体を活性化することも目的としているため、④研究開発を促進するための基盤の確立も重要なコンセプトとしている。

以下に、これらの4つのコンセプトについて説明する。

### **①情報システム全体のニュー・ディペンダビリティの確保**

能動的で信頼性の高い情報システムを実現するために必要な技術を明確にするためには、情報システムに係わる環境変化を考慮する必要がある。次世代インターネットを基盤として実現される社会システムでは、クラウド化、仮想化、端末のユビキタス化が進展し、リアルタイムセンシング機能の強化、位置情報等を活用したコンテキスト・アウェア化（センサーを用いてリアル空間の状況をコンピュータ内に能動的に収集・処理を行う）が進んだ CPS (Cyber-Physical-System) が実現すると考えられている。CPS では、リアルとサイバーの結びつきが今まで以上に強まったシステムになる。このため、実世界とコンピュータを繋ぐセンサーや制御機器を構成要素とするシステムには高い信頼性が求められるため、ニュー・ディペンダブルな情報通信システム構築技術の確立が必要となる。

### **②攻撃者の行動分析に基づくゼロデイ・ディフェンス（先読みの防御）**

社会経済活動における「情報」の役割が増大している中であって、国家の機密情報や企業の知的財産の漏えい事態が発生しており、情報漏えいの要因は多様化・複雑化している。また、サイバー攻撃の手法が複雑化・巧妙化する傾向

にあるが、サイバー攻撃への対応は後追いとなっており、現状を打破するための根本解決を目指す必要がある。このため、情報漏えいを起こす内部攻撃者やネットワークを介した外部攻撃者の行動観測によるプロファイリング、インセンティブやゲーム理論に基づく行動モデルの分析により、攻撃者の行動予測モデルから脅威を洗い出し、対策の最適化を行う先読みのディフェンス技術が求められている。

### **③個人情報等の柔軟管理の実現**

今後、位置情報やライフログなどのプライバシー情報の活用が拡大すると考えられるが、現在はプライバシー情報を提供するか、提供しないかという二者択一しかできないため、プライバシー情報を有効活用することが難しい。さらに、情報システムに係わるステークホルダーが多様化しており、利用者やベンダーの情報セキュリティに対する意識やスキルレベルの違いが問題となっている。このため、プライバシー情報等の積極活用と保護のバランスなど、多様性に対応した自律管理性を向上する技術が求められている。

### **④研究開発の促進基盤の確立と情報セキュリティ理論の体系化**

現在の情報セキュリティの研究開発は、個々のリスクに対応する対策のノウハウ集になっており、情報セキュリティ技術が理論的に体系化されていないため、これ以上の進展を期待することが難しい状況にある。研究を客観的に評価することにより、より優れた研究や適切な普及方法を明らかにすることが可能となる。

また、理論研究が正しいことを確認するためには、実証研究のためのデータが必要になる。このため、実証研究のためのデータの共通化・整備、研究の効率化のための評価体系の確立、実証研究の基盤となる暗号技術等の開発が求められている。

## 【コンセプト全体像】

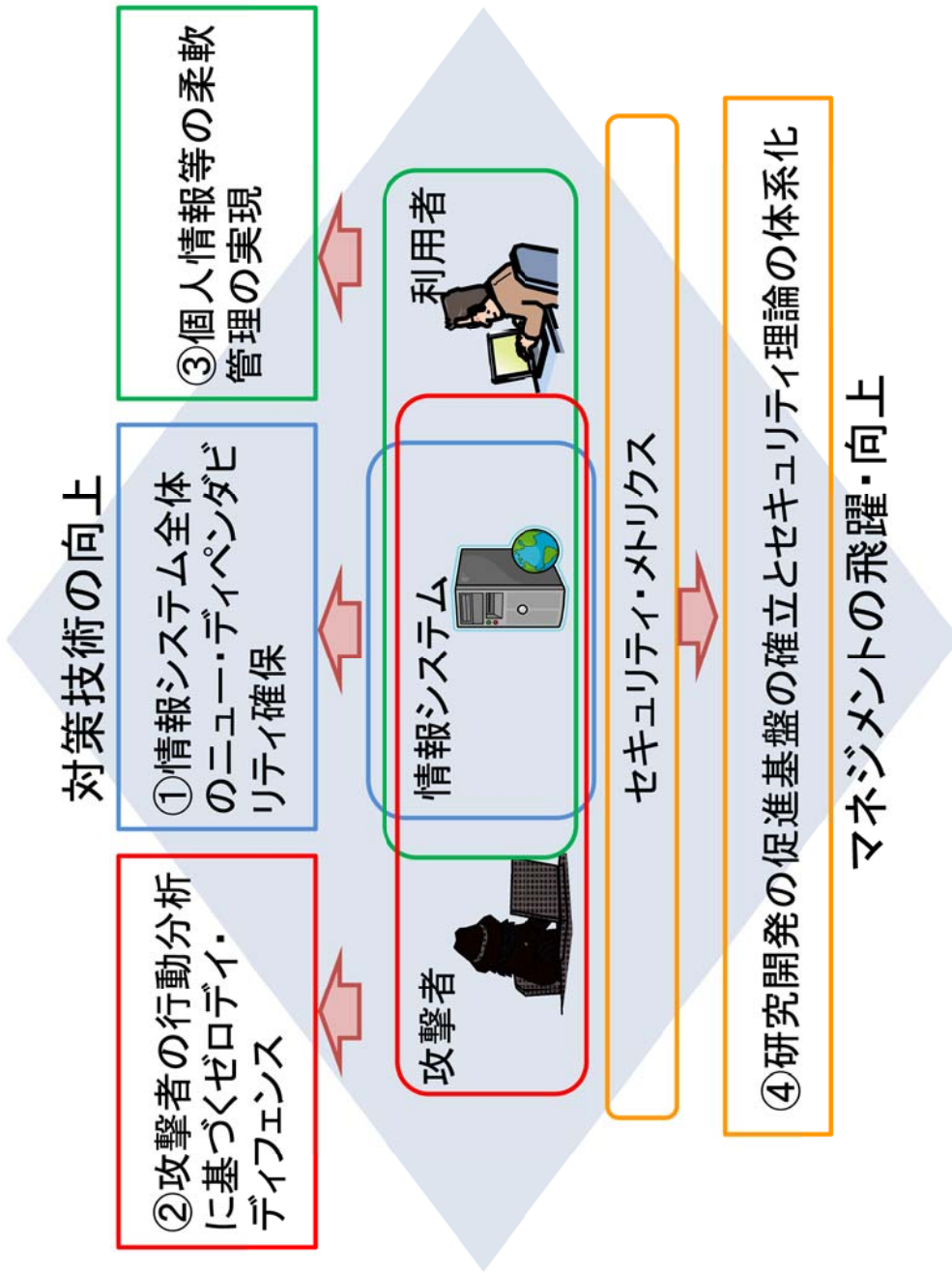


図 5 重要分野のコンセプト

### **(3) 研究開発の投資タイプ**

政府による研究開発投資においては、欧米においても①プロジェクトの成功率と②研究開発期間との観点で検討がなされている。これらの観点は、研究開発予算とも関連性が高い。2つの観点を使って、政府の支援が必要な研究開発の投資タイプを以下の3つに分類することとした。後述する情報セキュリティの研究開発における重点分野を3つに分類することにより、タイムフレームを伴った戦略的な研究開発の推進が可能になると考えている。

#### **①緊急対応型投資**

環境変化に伴う新たなニーズや脅威に、早急に対応する必要がある研究開発である。ニーズが明確なので、プロジェクトの成功率は高く、研究期間も一般的に短期であるが、大規模なトライアルが必要なものがあり、研究開発の推進に当たり政府の支援が必要になる。

#### **②イノベーション型投資**

従来 of 延長ではなく、革新的なアイデアやテーマに係る研究開発である。革新的なアイデアに関する研究であるため、プロジェクトの失敗リスクもあるが、成功した場合には大きな効果が期待できることから、研究の多様性を確保する点でも政府の支援が必要である。

#### **③長期基盤型投資**

国力の維持や国として人材やコミュニティの維持が必要であり、プロジェクトの失敗リスクは低くないが、波及効果が広範な基盤的研究開発である。一般的に、基盤的研究は投資から収益回収までの期間が長いから、政府の支援が必要である。

# 研究開発の投資タイプ

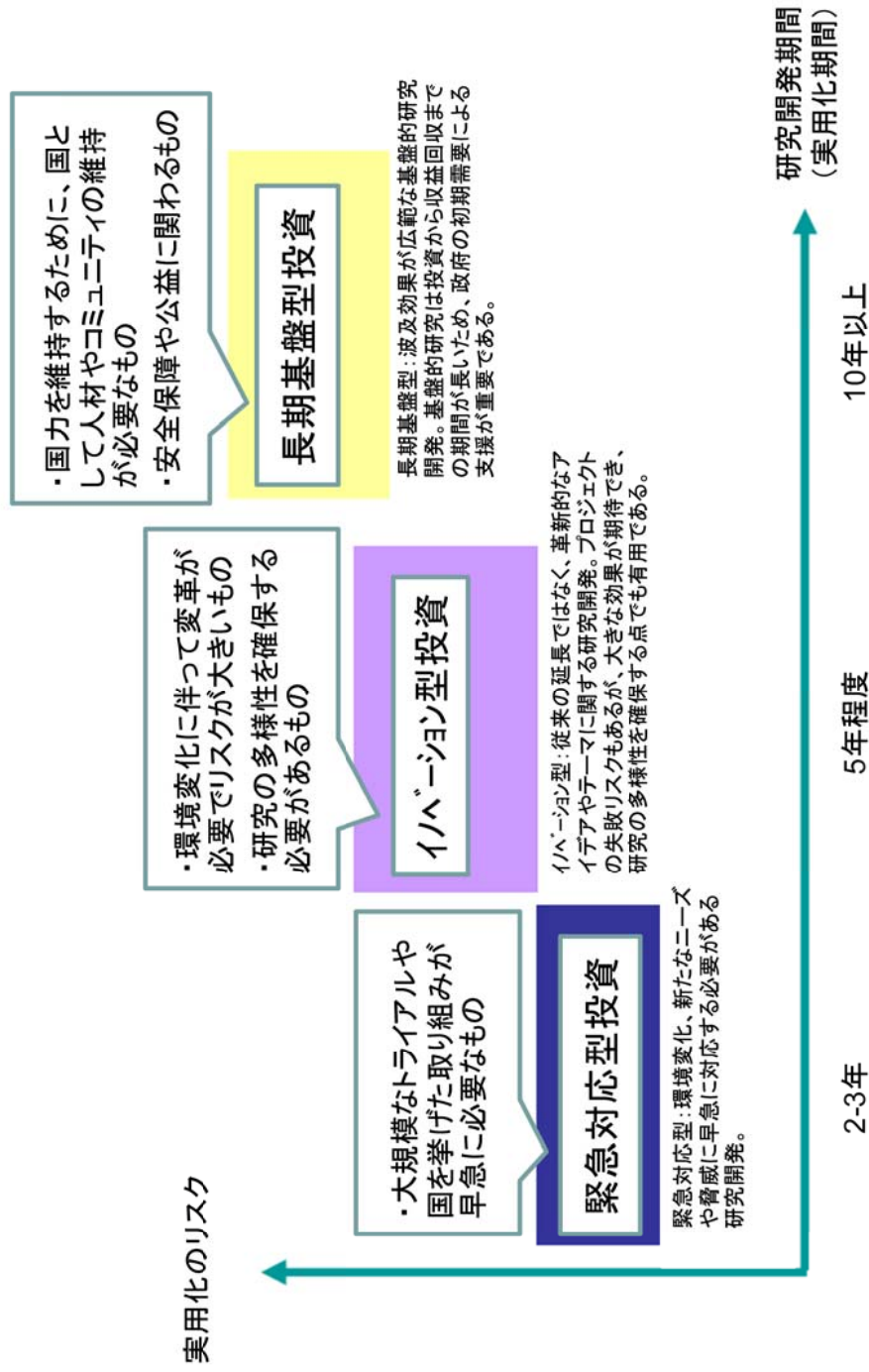


図 6 研究開発の投資タイプ

## 5 情報セキュリティの研究開発における重要分野

研究開発戦略の基本的考え方にに基づき、今後重要となると考えられる研究課題を抽出した。

重要分野の全体像を、図6に示す。

情報通信システム全体のニュー・ディペンダビリティの確保	
①	実世界とコンピュータ内のモデル世界が融合した次世代ネットワークにおける情報セキュリティ基盤技術
②	システムのセキュリティ設定を上位から下位まで自動保証する技術
③	障害に対する自動回復可能なコンピュータネットワーク構築技術
④	生体情報をコンピュータで管理するためのID管理と生体情報を統合するシステム設計構築技術
攻撃者の行動分析に基づくゼロデイ・ディフェンス	
⑤	攻撃者の行動分析等による予防基盤技術
⑥	大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合
個人情報等の柔軟管理の実現	
⑦	個人情報等の利活用を促進する自己情報の統制技術
⑧	フォレンジック等を支援するためのデータ管理・追跡技術
⑨	ITリスクに関する理論から実務までの体系化
研究開発の促進基盤の確立とセキュリティ理論の体系化	
⑩	情報セキュリティ研究の基盤体系化
⑪	セキュリティ部品が正しく実装されていることを保証する製品評価認証技術
⑫	情報理論的安全性を備えた暗号技術

図7 情報セキュリティの研究開発における重要分野

### (1) 情報通信システム全体のニュー・ディペンダビリティの確保

次世代インターネットを基盤として実現される社会システムは、リアルとサイバーの結びつきが今まで以上に強まったシステムになる。すなわち、私たちの身の回りに様々なセンサーが配置され、実社会の様々な状況がセンシングされて情報空間に取り込まれるようになると同時に、情報空間のデータが制御システムを介して実社会に反映されるようになる。このため、実世界とコンピュータ内のモデルを繋ぐセンサーや制御機器を構成要素とする情報通信システムには高い信頼性が求められるため、ニュー・ディペンダブルな情報通信システム構築技術の確立が必要となる。

さらに、このセンサーネットワーク及びアクチュエータネットワークは大規模になるため、その協調動作を集中管理することは困難になる。すなわち、大規模なセンサーネットワークを維持するためには、ローカルネットワークを自律的に構築・運用管理するとともに、これらのローカルなネットワークを相互接続する自己変革能力が必要となる。また、そのネットワーク上の情報を自由かつ自律的に伝送し、共有・加工する自律分散的な協調動作機能も必要となる。

そこで、①実世界とコンピュータ内のモデル世界が融合した次世代ネットワークにおける情報セキュリティ基盤技術、②システムのセキュリティ設定を上位から下位まで自動保証する技術、③障害に対する自動回復可能なコンピュータネットワーク・アーキテクチャの構築技術、④生体情報をコンピュータで管理するための ID 管理と生体情報を統合するシステム設計構築技術が重要テーマとなる。

以下、個別のテーマについて説明する。

### **①実世界とコンピュータ内のモデル世界が融合した次世代ネットワークにおける情報セキュリティ基盤技術**

前述のリアルとバーチャルが融合した社会システムにおいては、様々なセンサーが家庭や職場に設置され、エネルギー効率の高い社会が実現されると考えられているが、同時に災害発生時の状況把握にも威力を発揮し、安全・安心な社会の実現に寄与することが期待できる。一方、個人が持つスマートフォン等の発信者情報やセンサーからの身体健康情報の漏えいが懸念されるため、それらを保護する仕組みの構築が求められる。なお、スマートフォンに係る情報セキュリティ課題は、端末からのプライバシー情報の漏えい以外にも、端末識別子のなりすましによるスマートフォン用のウェブサイトへの不正アクセスなども想定されるため、スマートフォンの情報セキュリティ基盤の開発を早期に行う必要がある。

また、このようなセンサーネットワークにおいては、バックボーンを介さないアドホックネットワークの利活用が見込まれるが、無線通信の物理レイヤ以下の階層の情報セキュリティ技術は未だ確立されておらず、利便性と安全性のバランスを考慮した情報セキュリティ基盤の確立が必要である。

このため具体的には、(a)センサーネットワークの情報セキュリティ基盤技術、(b)アドホックネットワークにおける利便性と安全性のバランスを考慮した情報セキュリティ基盤技術等の研究開発を推進する。

## ②システムのセキュリティ設定を上位から下位まで自動保証する技術

システムのコンポーネント化が進む中、システムの上位層から下位層まで、情報セキュリティの整合性を系統的に保証する情報システムの構築技術が求められている。このため、システムのアーキテクチャに基づいて、情報セキュリティ・ポリシーやコンフィグレーションを管理するフレームワークを開発する。さらに、このフレームワークに基づいて、ポリシーやコンフィグレーションが守られていることを保証するために、形式手法等の技術を活用した自動検証技術の研究開発を推進する。自動検証技術については、米国の情報セキュリティ・オートメーション等の研究動向を踏まえ、海外の成果を活用して研究を進めることが求められる。

また、IPv6 への移行に伴う情報セキュリティ面の懸念は、ネットワーク層の問題だけではなく、上位アプリ層まで含めたトータルの整合性を取ることが必要であり、情報セキュリティ・ポリシーやコンフィグレーションを管理するフレームワークの一環として研究開発を推進する。

## ③障害に対する自動回復可能なコンピュータネットワーク・アーキテクチャの構築技術

緊急に対応が必要な局面において指示系統を構成する通信基盤が失われると壊滅的な状況が生じることになる。一方、想定を超える災害、様々な脅威や障害からネットワークを完全に守るために必要なコストは膨大であり、ネットワークの障害をゼロにすることはできないという前提に立ちつつ、ネットワークサービスを止めないようにする為の仕組み（自己治癒型ネットワークの構築技術）を開発する必要がある。

具体的には、ネットワークの仮想化技術などを用いて、ネットワーク通信方式の多様性や冗長性を高めることで、サイバー攻撃などによる障害への耐性を高めたダイバーシティ・ネットワーク・アーキテクチャの研究開発を推進する。

また、ネットワークの多様性や冗長性を活用して、障害が発生した場合の自己治癒機能の研究開発を推進する。この研究には、他の重要テーマである「大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合」の成果も活用し、攻撃に対しても即応できる治癒機能を開発する。

## ④生体情報をコンピュータで管理するための ID 管理と生体情報を統合するシステム設計技術

リアルとバーチャルが融合した社会システムにおいて、リアルの間人をコンピュータ内に取り込む場合、バイオメトリクス情報と ID 管理の統合が必要にな

る。バイオメトリクス分野の要素技術は性能面で成熟しており、これからの研究開発テーマとしては、バイオメトリクスを含むオープンな ID 管理システム・アーキテクチャの設計及び、当該システム・アーキテクチャの標準化、SAML (Security Assertion Markup Language) 等による認証システムとの統合技術が求められている。これは、例えば入国審査システム等にも適用されうるものである。

また、日本はバイオメトリクスの要素技術に強みを持っており、この強みを維持するためにも、統合システムの部品となるバイオメトリクス認証技術の適合性評価を行う国際的なフレームワークにおいて、イニシアチブを取ることが望ましい。

具体的には、OpenID<sup>8</sup>をベースとしたミドルウェア・アーキテクチャの開発、SAML 等を活用してバイオメトリック・デバイスとのインタフェースやプロトコルを開発する必要がある。また、統合システムの部品となるバイオメトリクス認証技術の適合性評価を行う国際的なフレームワークを構築する。さらに、ISO の国際標準化を想定し、事前に国内の関係者などとの調整及び新作業項目 (NP: New Work Item Proposal) の提案取りまとめを行う。

## (2) 攻撃者の行動分析に基づくゼロデイ・ディフェンス

近年、注目されている APT 攻撃は、特定のターゲットに対して持続的に攻撃・潜伏を行い、様々な手法を駆使して執拗なスパイ行為や妨害行為などを行う攻撃である。サイバー攻撃の手法は、ますます複雑化・巧妙化する傾向にあるが、サイバー攻撃への対応は後追いとなっており、根本解決を目指した研究開発を推進する必要がある。このため、情報漏えいを起こす内部攻撃者やネットワークを介した外部攻撃者の行動観測を広域で行い、攻撃者のプロファイリングや行動モデルの分析により対策の最適化を行う、先読みのディフェンス技術が求められている。

そこで、⑤攻撃者の行動分析等による予防基盤技術、⑥大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合が重要テーマとなる。以下、個別のテーマについて説明する。

### ⑤攻撃者の行動分析等による予防基盤技術

現在のインターネット環境は攻撃者に有利な状況であり、攻撃に対する後追

---

<sup>8</sup> ウェブサイトによらず使用できる認証システムの標準、およびそこで使用される識別子

い対策では、対策コストの増大を抑えることができない。このため、米国においては、攻撃者に有利な状況を打開するための研究開発を緊急の課題として進めており、我が国においても早急に取り組むことが期待されている。

具体的には、情報漏えいを起こす内部攻撃者やネットワークを介した外部攻撃者の行動観測によるプロファイリング、インセンティブやゲーム理論に基づく行動モデルの分析により、攻撃の公算や影響を予測し、対策の最適化を行う技術の研究開発を推進する。

## ⑥大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合

スマートフォンの爆発的な普及やスマートフォンを狙ったウイルスの登場、更には Web や SNS 等を用いた新たなサイバー攻撃の増加によって、パンデミックなネットワーク障害のリスクが高まっている。このため、従来行われてきた「人」による監視と対応には限界がくるため、Web 等の観測・分析技術、マルウェアの自動検知技術及び自動対処技術（トラフィックの制御など）が必要不可欠になってくる。これには、IPv6 に対応した広大なアドレス空間を効率的に観測する技術の研究開発が必要である。

また、異常を検知した際に、自動的にトラフィックを制御する技術の開発も必要となる。

なお、近年のサイバー攻撃は、防護システムを回避するように巧みに設計されたものとなっているため、マルウェアの挙動分析においては、攻撃者から観測ネットワークの存在を察知されないシステムの開発も必要となる。

### （3）個人情報等の柔軟管理の実現

情報システムに係わるステークホルダが多様化しており、利用者やベンダーの情報セキュリティに対する意識やスキルレベルの違いが問題となっている。このため、プライバシー情報等の積極活用と保護のバランスなど、多様性に対応した自律管理性を向上する技術が求められている。また、大きな災害等が発生すると、プライバシー情報の扱いやそれに伴うリスクに対する社会のとらえ方が変化することもあり、許容されるリスクを調整するリスク・コミュニケーションの仕組み等が必要となる。

そこで、⑦個人情報等の利活用を促進する自己情報の統制技術、情報のコントロールに関連して⑧フォレンジック等を支援するためのデータ管理・追跡技術、⑨IT リスクに関する理論から実務までの体系化が重要テーマとなる。

以下、個別のテーマについて説明する。

## ⑦個人情報等の利活用を促進する自己情報の統制技術

現在は、プライバシー情報を提供するか、提供しないかという二者択一であるため、プライバシー情報を有効活用することが難しい。プライバシー情報を適切にコントロールすることができれば、情報の有効活用によるメリットを享受することが可能になる。

例えば、位置情報やライフログなどのプライバシー情報を適切に利用するためには、利用者ごとにプライバシー保護レベルやポリシーを柔軟に設定するシステムの開発、プライバシーを保護したまま有用なデータを計算するための秘密計算、プライバシー保護データマイニング等の基礎的研究を行う必要がある。

また、医療情報など特に機微な情報の活用については、社会環境に即した法制度の検討、業界における合意の形成や、医療情報システムと連携したデータ活用の技術開発を進める必要がある。

なお、新しいビジネスモデルとして注目を集めているクラウドにおいてもプライバシー情報の漏えいが情報セキュリティ上の大きな課題であり、クラウドに係わる他の情報セキュリティ課題についても研究開発を推進する。

## ⑧フォレンジック等を支援するためのデータ管理・追跡技術

個人にとってプライバシー情報の漏えいが大きな問題であると同じように、政府にとっては、国家機密の情報漏えいや知的財産の国外流出が発生することは大きな問題であり、これらを防止するために早急な技術開発が求められている。ネットワークを介した情報漏えい事件が増加傾向にあることから、漏えい先を突き止めるためのネットワーク・トレースバックや、情報の改ざんや情報漏えいに関与したものを特定するための証拠データの収集技術が必要とされている。

具体的には、(a)リアルタイムの証拠データの保全・調査、(b)ネットワーク・フォレンジック(c)証拠データの信頼性評価などの研究課題がある。ネットワーク・フォレンジックで扱うデータ量は極めて大きくなるため、データの収集・解析を効率的に行うための研究が必要となる。

## ⑨IT リスクに関する理論から実務までの体系化

大きな災害が発生すると、リスクに対する社会のとらえ方が変化する（例えば、平常時にプライバシー情報がネットに公開されると問題であるが、災害時には安否確認が優先される）。さらに、災害復興に向かう過程では、多様な価値観が混在するため、許容されるリスクを調整するリスク・コミュニケーション

の仕組み等が重要となる。

また、社会基盤を支える重要インフラシステムの中核にはリスク・マネジメントが不可欠であるが、リスクは益々複雑化しており、1つのリスク対策が別のリスクを生む原因になることがある。

このため具体的には、(a)リスク対リスクを回避するための手段の研究、(b)複数の関係者間で合意を得るためのコミュニケーション手段の研究、(c)対策の最適な組み合わせを求めるシステムを開発する必要がある。

#### **(4) 研究開発の促進基盤の確立と情報セキュリティ理論の体系化**

現在の情報セキュリティの研究開発は、個々のリスクに対応する対策のノウハウ集になっており、情報セキュリティ技術が理論的に体系化されていないため、これ以上の進展は期待できない。研究として評価できるようにすることで、より良い研究や適切な普及方法を明らかにすることが期待される。また、理論研究が正しいことを確認するためには、実証研究のためのデータが必要になる。

さらに、情報セキュリティ全体の研究開発を促進するうえで、研究の前提となる共通基盤技術の開発は必須である。

このため、実証研究のためのデータの共通化・整備、研究の効率化のための評価体系の確立、共通基盤技術の開発等が求められている。

そこで、⑩情報セキュリティ研究の基盤体系化、⑪セキュリティ部品が正しく実装されていることを保証する製品評価認証技術、⑫情報理論的安全性を備えた暗号技術、が重要テーマとなる。

以下、個別のテーマについて説明する。

#### **⑩情報セキュリティ研究の基盤体系化**

情報セキュリティの研究開発を対策のノウハウ集ではなく、研究として評価するためのサイエンスとする必要がある。また、理論研究が正しいことを確認するためには、実証研究のためのデータが必要となり、データを継続的に観測する仕組みも必要になる。

サイバーセキュリティ研究の活性化の基盤として、(a)サイバーセキュリティ研究の科学的な評価フレームワークの確立、(b)実証研究のためのデータ基盤の整備が必要になる。(a)については、脅威やリスクの評価手法、技術の効果の評価手法、科学的に評価体系を研究開発する必要がある。(b)については、データ整備が必要なものの洗い出し、各データ構成の設計、データ提供システムの研究開発が必要になる。

## ⑩セキュリティ部品が正しく実装されていることを保証する品質評価認証技術

ソフトウェアの品質評価手法、及びソフトウェア品質の属性（セキュリティ、安全性、信頼性等）に与える影響に基づいた欠陥の特性解析が必要である。情報システムの構成要素であるセキュリティ部品の品質評価の基準が標準化されていれば、セキュリティの要求に合った適切なセキュリティ製品を使ってシステムを構成することが可能になる。これは、セキュリティ対策の費用対効果を改善する上でも有用である。また、品質評価に基づく認証制度とそのための基盤を世界に先駆けて具体化することは、我が国の産業競争力の向上にもつながる。

具体的には、(a)セキュリティ製品のセキュリティレベルを評価するための基準設計、(b)セキュリティ製品の組み合わせ方の正当性を評価する手法、(c)評価プロセスの標準化などが必要になる。

## ⑪情報理論的安全性を備えた暗号技術

情報理論的に安全な暗号技術は、従来主流の計算量的暗号技術に対比される技術である。近年、重要インフラの制御システムを狙ったマルウェアが登場しており、制御システムのセキュリティ対策の必要性が高まっている。DES,RSAなどの計算量的な暗号技術の場合、計算機の処理速度の向上に伴う危殆化の問題が付きまとう為、制御システムの稼働期間（十数年の長期）に渡って、安全性を保障することはできない。

また、センサー機能を持った組み込み機器が家庭やオフィスに配置され、ネットワークに接続されるようになってきており、組み込み機器のセキュリティ対策が求められている。情報理論的な暗号は、線形演算で構成でき高速処理が可能となるため、計算資源の小さい組み込みシステムへの適用が可能と考えられる。

情報理論的に安全な暗号技術を実用化するためには、組み込みシステムへの導入に関する研究も重要となる。車載コンピュータ、制御系コンピュータ、電力システムなど、システムごとにリソースやリアルタイム性の制約を考慮した方式の研究開発が必要である。

また、情報理論的に安全な暗号技術の1つである量子暗号技術では、大きな秘密鍵を事前に共有する仕組みが重要となり、その手段として量子通信等が有望とされている。特定環境における量子通信の実現は、10～20年程度の研究課題とされており、国際的な成果も活用して推進することが効率的である。

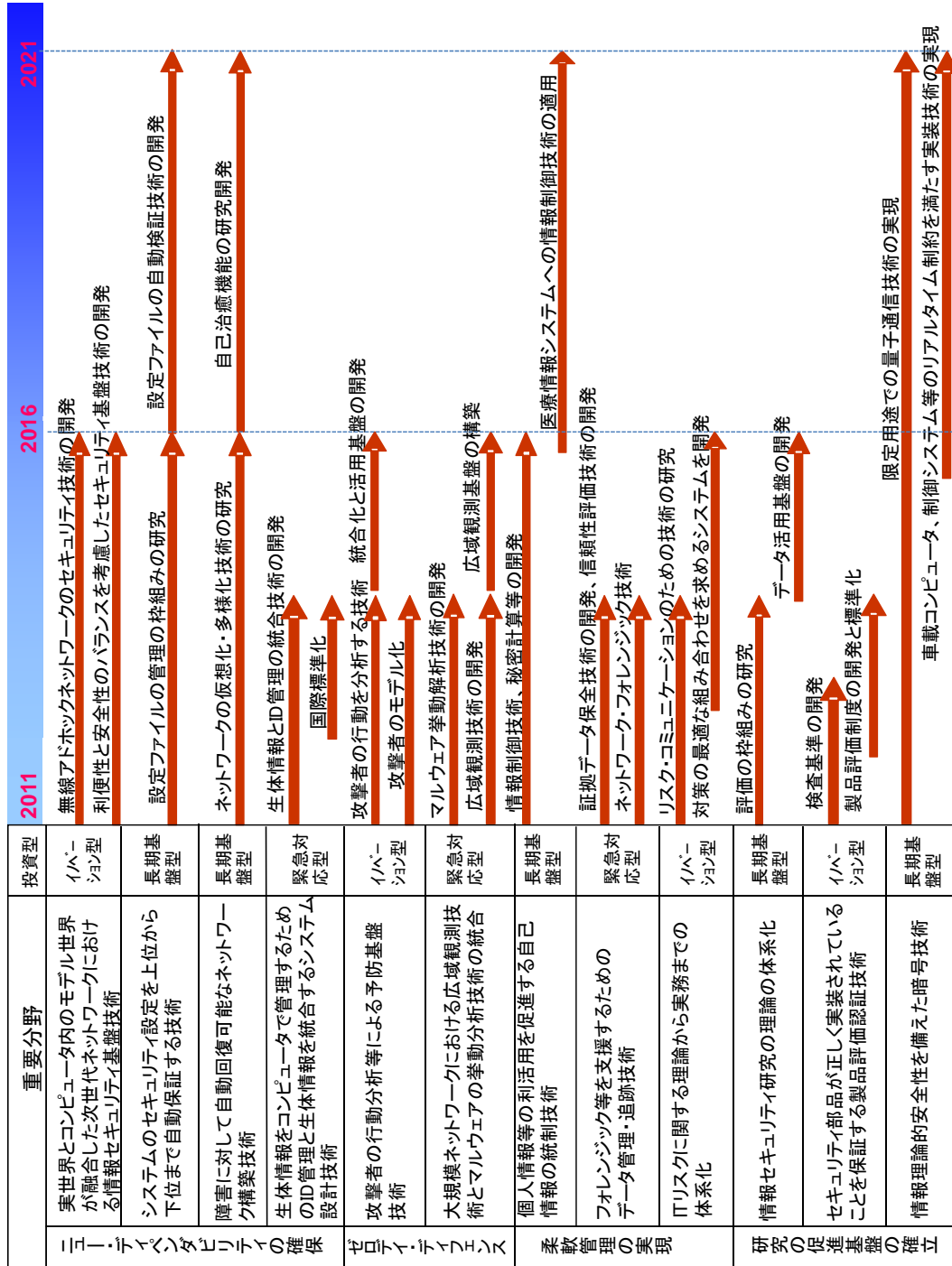


図8：重要テーマの技術ロードマップ

## 6 東日本大震災を踏まえた重点分野

情報セキュリティについては、「機密性」（許可された者に限って情報にアクセスできること）、「完全性」（情報が変化せずに完全に維持されていること）、「可用性」（必要な時に情報やサービスが利用できる）の確保に重点をおいて推進しているところであるが、大規模な災害発生時には、特に「可用性」の確保が重要になると考えられる。

本章では、今回の大震災を踏まえ、情報セキュリティの観点から重点的に取り組むべき分野を抽出するが、復旧・復興に寄与するために早急に対応すべき分野と、中長期的視点から「ニュー・ディペンダビリティ」の確保など、より高い耐災害性を実現するために必要な分野を峻別して、研究開発を促進することが重要である。

### （1）耐災害性に強い情報通信システムの構築

今回の震災では、災害発生時における迅速な情報連絡、情報共有の困難化、長時間の停電や複合的なインフラの供給停止による情報通信システムの停止、サプライチェーンの崩壊、市町村に保管されている詳細な住民基本台帳や戸籍データの一時消失などが問題となった。このため、耐災害性に強い情報通信システムを検討、再構築するとともに遠隔地への情報のバックアップや分散化などに対応した BCP の見直しが不可欠である。サイバーセキュリティとフィジカルセキュリティは表裏一体の関係にあるので、複合的な災害が発生することを前提とした BCP の見直しが必要となっている。

#### ①耐災害性のある情報通信インフラ

災害時に強い、有線・無線の有機的なネットワークシステム、非常用電源設備の強化などに取り組む必要がある。

#### ②災害時の情報システム

災害時には、早急に、迅速な情報連絡、情報共有体制を確立する必要がある。

- ・今般の震災において、SNS の極めて有効な活用事例が明らかになった。SNS は、情報の信頼性が懸念されるとの指摘もあるが、社会のリテラシーが向上しており、データに基づく中立的な情報が選択される傾向にあると考えられる。情報セキュリティに配慮しながら、更なる SNS の活用方策<sup>9</sup>を検討する

<sup>9</sup> 内閣官房（情報セキュリティセンター、情報通信技術（IT）担当室）、総務省、経済産業省において、「国、

必要がある。

- ・住民登録、医療記録等の個人情報、資産・負債関係（緊急時の預金引き出しの円滑化）、緊急避難指定地域と住民 ID のデータ照合、緊急時のロジスティックを容易にするための交通管制情報、外国人・留学生等の所在情報などについて、適切に情報の共有を可能とする情報システムの構築が重要である。緊急時に情報を収集・管理・運用するため、情報セキュリティに配慮した制度設計を検討する必要がある。
- ・今般、災害関連情報を提供しているミラーサイトが次々と立ち上がり、情報提供に重要な役割を果たしたが、短時間での対応が求められるため、災害発生時のミラーサイトのセキュリティ確保方策について予め検討しておく必要がある。
- ・また、災害時に災害情報等を届けるための機動的なルート構成方策、災害復旧の為の動的ネットワークの組み替え技術などについて検討しておく必要がある。

### ③情報通信システムのバックアップ、分散化

災害発生に備え、情報通信システムのバックアップ、分散化を図っておくことは極めて重要である。今般の大震災を踏まえ、クラウドなど新たな技術を活用したバックアップ、分散化の方策を検討する必要がある。

- ・情報のバックアップや分散化を比較的低コストで実現する方法として、クラウドの活用に注目が集まっているが、情報セキュリティ上の課題が大きな阻害要因の一つとして指摘されている。研究開発面、運用面などからこれらの課題を克服する取り組みを加速化する必要がある。
- ・システムの分散化を図った場合、災害時における遠隔認証の問題についても検討する必要がある。大学間では Shibboleth 認証などが活用されているが、災害が発生した場合には、システムが利用できない可能性があるため、それを回避する方策も検討する。また、災害時に、暗号化や認証が使えなくなった時のリスクについても検証しておく必要がある。

## (2) 「リスク・マネジメント」等

今般の大震災により、「リスク・マネジメント」、「リスク・コミュニケーション」の重要性が認識された。

前述したように、大きな災害が発生すると、リスクに対する社会のとらえ方が変化する（例えば、平常時にプライバシー情報がネットに公開されると問題

であるが、災害時には安否確認が優先される)。さらに、災害復興に向かう過程では、多様な価値観が混在するため、許容されるリスクを調整するリスク・コミュニケーションの仕組み等が重要となる。

このとき、情報セキュリティの確保といった従来の狭義の情報セキュリティの視点ではなく、社会全体のリスクの低減に寄与するといった広義の情報セキュリティの確保に重点をおいて対策を検討することが重要である。

また、社会基盤を支える重要インフラシステムの中核にはリスク・マネジメントが不可欠であるが、リスクは益々複雑化しており、1つのリスク対策が別のリスクを生む原因になることがある。

社会を取り巻くリスクに関する正確な情報を様々なステークホルダ間で共有し、相互に意思疎通を図ることがリスク・コミュニケーションであり、さらに評価し対策を講じること、またリスクを受容できるレベルまで低減するプロセスがリスク・マネジメントである。

大災害が発生し、状況がダイナミックに変化することにより、リスクに対する社会の捉え方や許容できるリスクレベルも大きく変容する。災害時においては、このような状況変化の中で、最適な対応を行うための「ダイナミック・リスク対応」の観点を持つことが必要である。また、一つのリスクへの対応が従来存在しなかった新たな別のリスクを引き起こすことがあり、リスクとリスクを比較考慮しながら（「リスク対リスク」）最適な施策を模索（「リスク・マネジメント」）する必要がある。

我々は「ゼロリスク願望」を持ちがちであるが、この発想に固執する限り、むしろ適切なリスク・マネジメントから遠ざかることになる。組織が持つリスクを明確にし、評価・対処することによりシステムトータルとしてセキュリティの確保が可能になると考えられる。

また、リスク・コミュニケーションの観点からは、災害時においてどのような形で国民に情報を伝達すべきか、企業においては危機管理の観点からどのように情報を伝達、コントロールすべきかなど検討すべき課題は多い。

更に、BCPや事業継続マネジメント（BCM）の概念を持ち、想定外の事象に対する応用力を身につける必要がある。そのためには、より厳しい状況を想定してシミュレーションを実施することなども有用である。

具体的には、⑨「ITリスクに関する理論から実務までの体系化」で述べたように、(a)リスク対リスクを回避するための手段の研究、(b)複数の関係者間で合意を得るためのコミュニケーション手段の研究、(c)対策の最適な組み合わせを求めるシステムを開発することが求められている。

### **（3）個人情報等の柔軟管理の実現**

個人情報等の積極活用と保護のバランスなど、多様性に対応した情報の自律管

理性を向上する技術の重要性は、5章の(3)「個人情報等の柔軟管理の実現」で記述したとおりであるが、災害時には、安否確認のための情報公開が優先されるなど、社会のプライバシー情報に対する考え方やリスクの捉え方は変化する。一度インターネットに流出した情報を回収することは極めて困難であることから、平時から災害時に備えて、個人情報を適切にコントロールする技術、個人情報保護レベルやポリシーを柔軟に設定するシステムの研究開発を進めておくことが望ましい。

具体的には、5章の(3)「個人情報等の柔軟管理の実現」で述べた研究開発を推進するに当たり、災害時の視点を十分に考慮して、進める必要がある。

#### **(4)「ニュー・ディペンダビリティ」**

既に述べたように、我々の社会は、高度に発達した情報システムへの依存度を増しており、特に災害時には情報システムが提供するサービスは、より良質で信頼できるものでなければならない。また、そこで扱われる情報は正確で一貫性があり、その機密性が規定通りに守られる必要がある。今回の震災を踏まえ、今後の社会システムはこのような「ニュー・ディペンダビリティ」の要件を満たすシステムとすべきである。

情報システムのニュー・ディペンダビリティを確保するにあたり、情報システムの構成要素であるソフトウェアのコンポーネント化が進んでおり、システムの上位から下位層まで、トータルにセキュリティの整合性を系統的に保証する情報システム構築技術が求められている。また、想定を超える災害、様々な脅威や障害からネットワーク等を完全に守るために必要なコストは膨大になるため、ネットワークサービスを止めないようにする為のダイバーシティ・ネットワークなどの仕組みの研究開発の重要性も増すと考えられる。

このような災害時の観点を重視して、5章の(1)「情報通信システム全体のニュー・ディペンダビリティの確保」で述べた研究開発を推進する必要がある。

## 【参考資料】

1. 情報セキュリティに係る環境変化に関する資料等

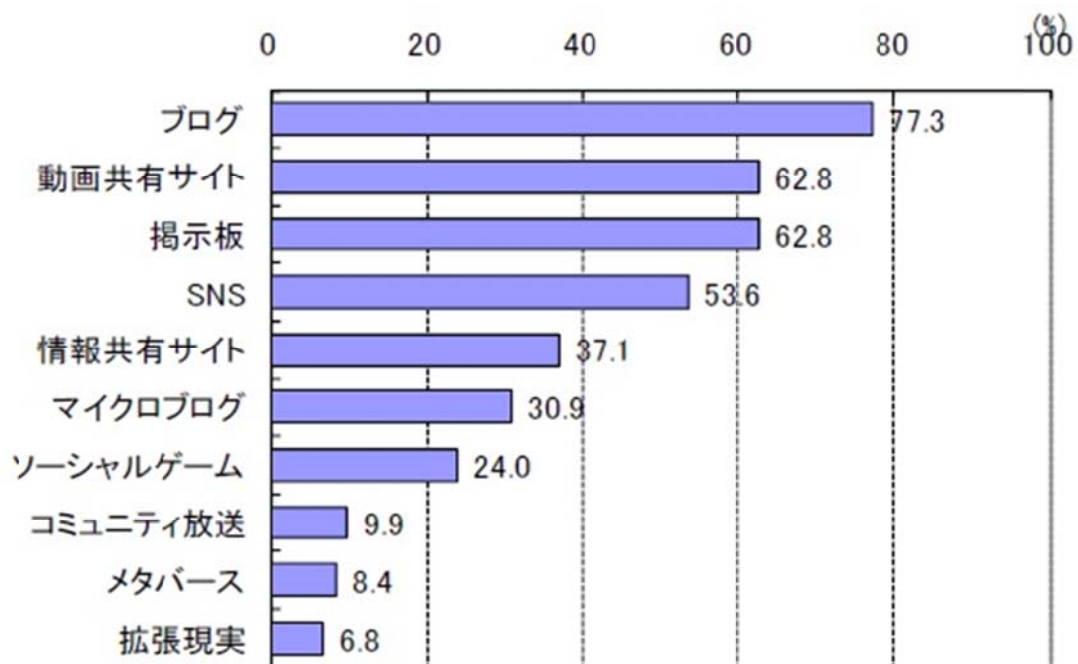


図1：新しいコミュニケーションサービスの普及状況

【出典】総務省「ソーシャルメディアの利用実態に関する調査研究」（平成22年3月）

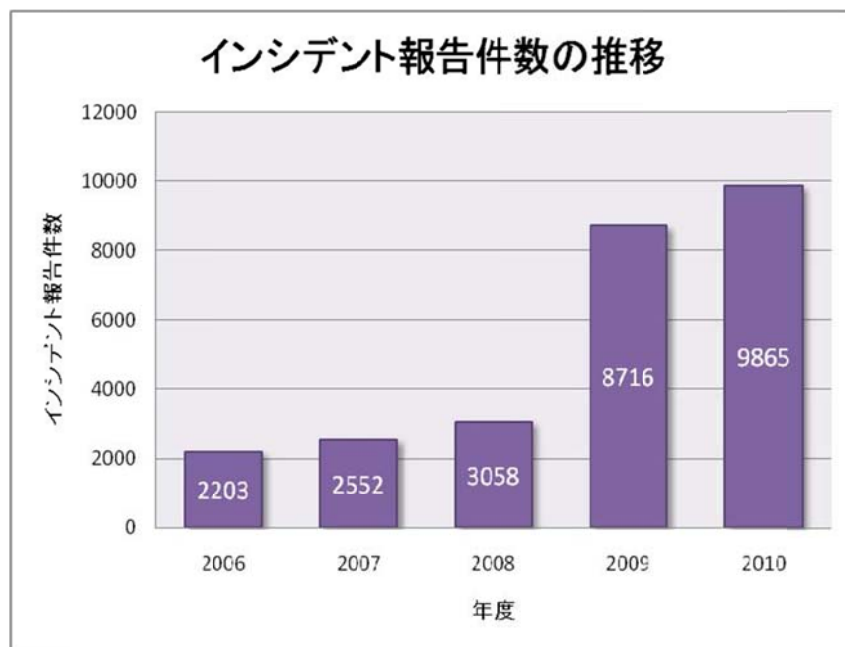


図2：情報セキュリティ上のインシデントとしてJPCERT/CCに報告された件数の推移

【出典】JPCERT/CC インシデント報告対応レポート[2011年1月1日～2011年3月31日]

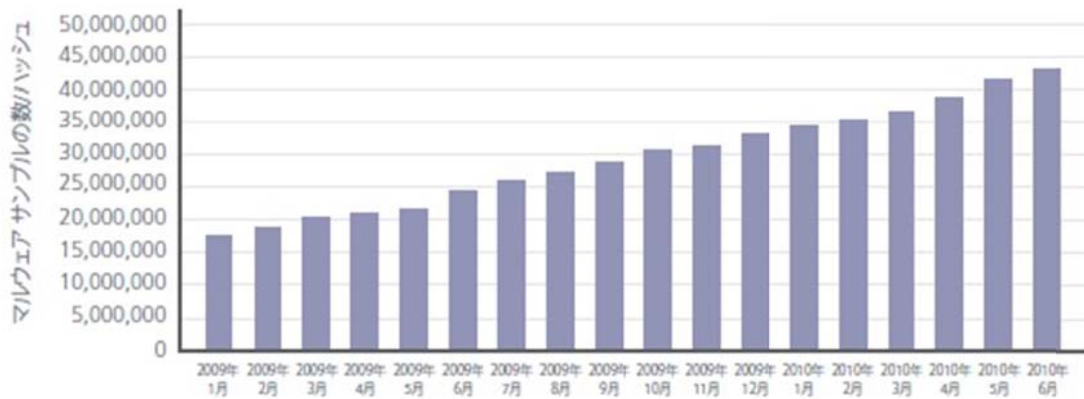


図3：マルウェアの種類増加状況

【出典】マカフィー社 McAfee 脅威レポート:2010 年第2四半期

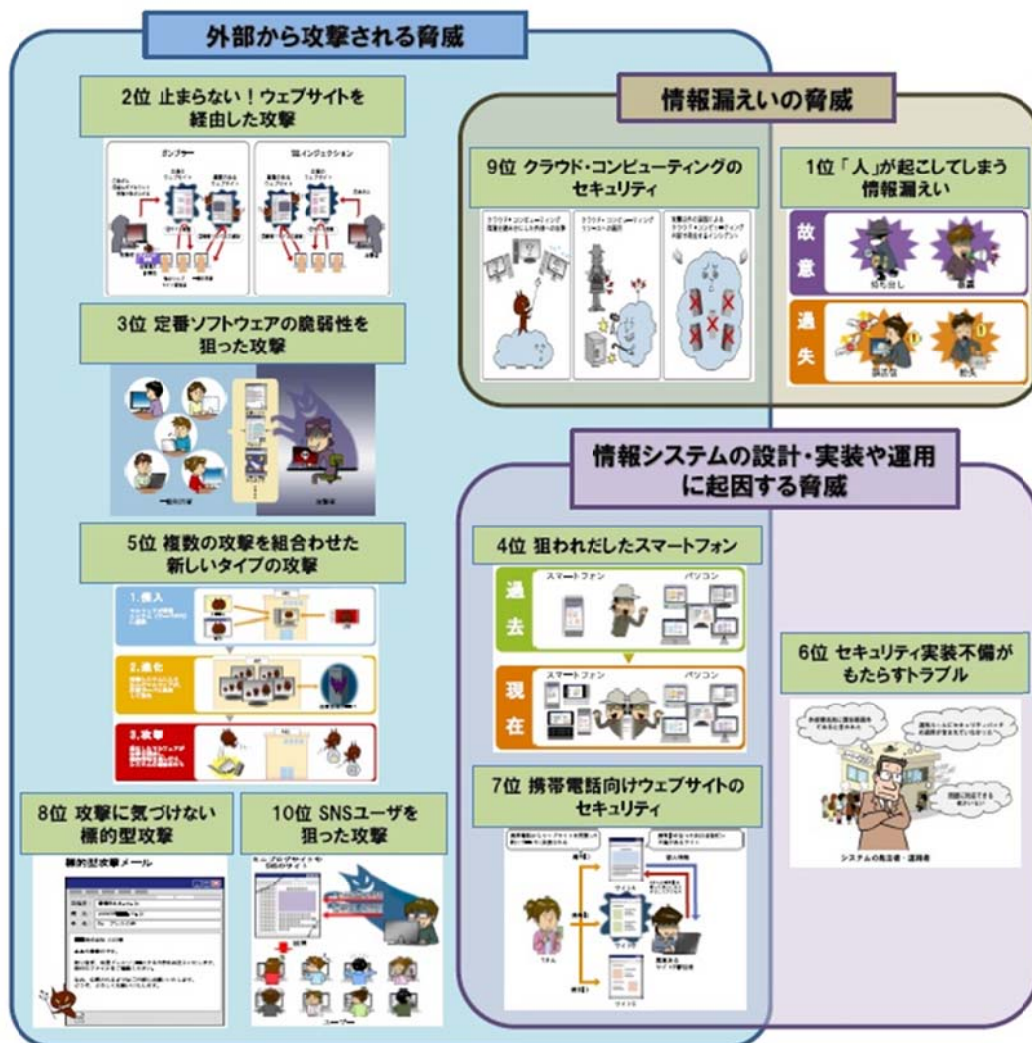


図4：多様化・複雑化する脅威

【出典】IPA 「2011年版 10大脅威 進化する攻撃... その対策で十分ですか?」(平成23年3月)

## 2. 米国の情報セキュリティ R&D の状況に関する資料等

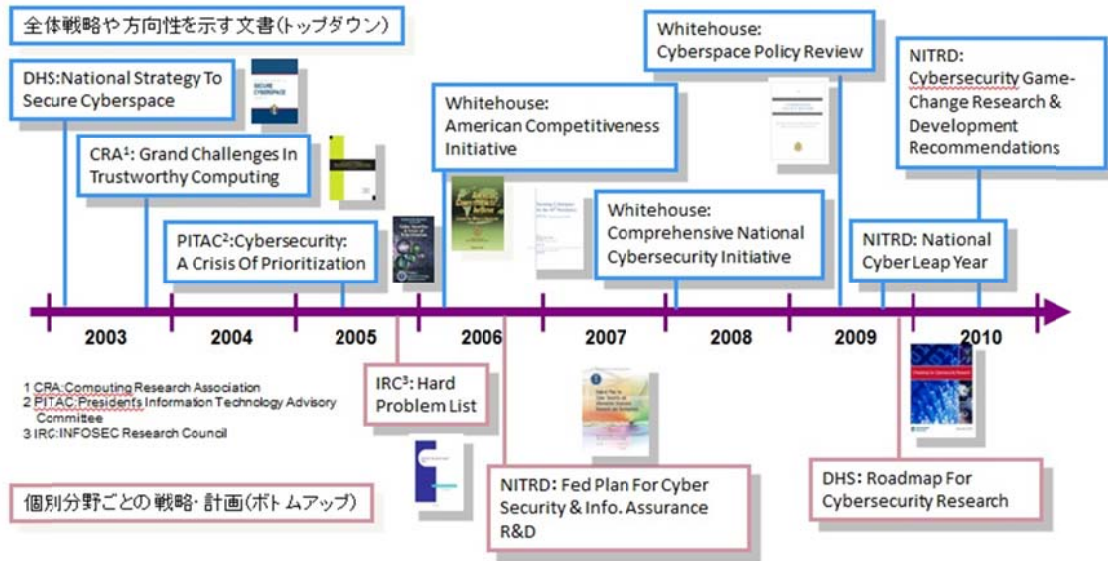


図5：米国の情報セキュリティ R&D 戦略の変遷

【出典】 NITRD: Toward a Federal Cybersecurity Research Agenda: Three Game-changing Themes ([http://www.nitrd.gov/CSThemes/NITRD\\_Cybersecurity\\_RD\\_Themes\\_20100519.ppt](http://www.nitrd.gov/CSThemes/NITRD_Cybersecurity_RD_Themes_20100519.ppt))等から作成

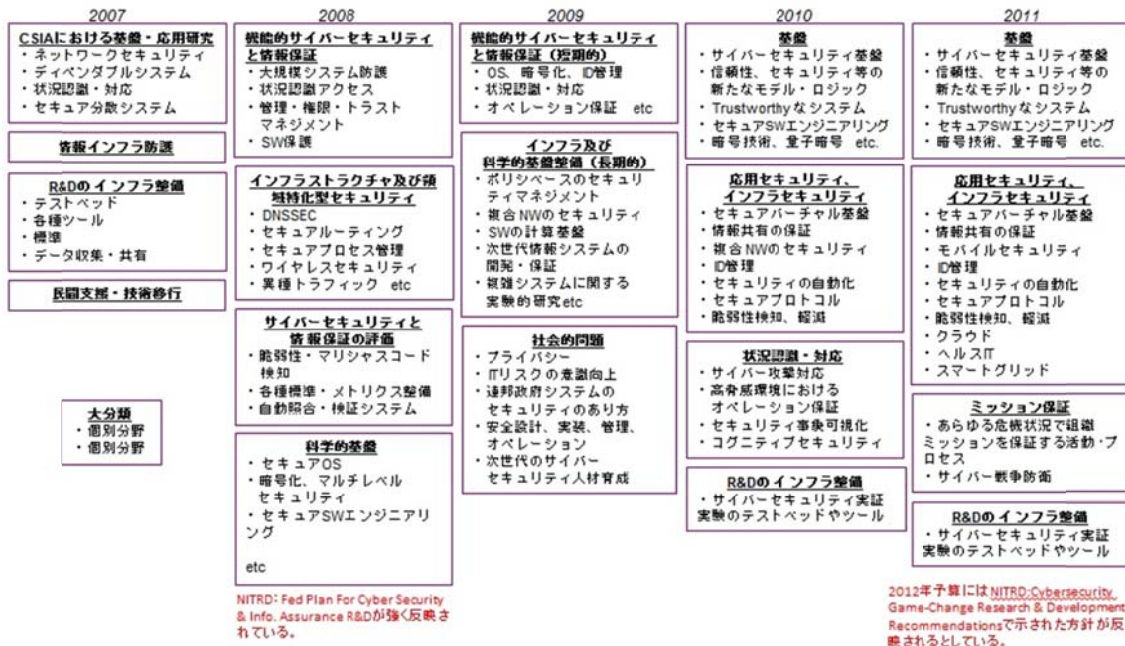


図6：米国（NITRD CSIA）における優先分野の推移

【出典】 NITRD: <http://www.nitrd.gov/pubs/bluebooks/index.aspx> 等から作成

### 3. 重要テーマの具体例

No.	重要テーマ	技術ロードマップ	関連施策の一例	必要額
①	リアルとバーチャルが融合した次世代ネットワークにおける情報セキュリティ基盤技術	コンテキストアウェアネス(センサーを用いてリアル空間の状況をコンピュータ内に能動的に収集・処理を行う)を実現するため、セキュアでディペンダブルな情報システム構築技術の研究が必要。		20億円 ×5年＝ 100億円
②	システムのセキュリティ・コンプライアンス向上から下位まで自動保証する技術	米国のセキュリティ・オートメーションの研究動向も踏まえ、ポリシーに基づいてレイヤ間の整合性を自動検証する形式手法の基礎研究も必要。  <b>(a) IPv4アドレスの枯渇によりIPv6の普及が見込まれ、IPv6環境の実践的なセキュリティ検証と防御技術の確立が必要。</b>	適材適所にセキュリティ技術を自動選択し、セキュアなネットワークを最適に構成するためのセキュリティアーキテクチャの研究開発(NICT)	5億円 ×10年＝ 50億円
③	障害に対する自動リカバリー可能なネットワーク・アーキテクチャの構築技術	自己治癒型のネットワークの研究開発の前提として、ネットワークの仮想化・多様化に係わる基礎研究が必要。 		5億円 ×10年＝ 50億円
④	ID管理とバイオメトリクスを統合するシステム・アーキテクチャの設計・構築	生体情報を用いたIDマネジメントを国際的に行うためには、国際標準化のプロセスに沿った取り組みが必要。 		10億円 ×3年＝ 30億円

図7：情報セキュリティの研究開発における重要分野（情報システム全体のニュー・ディペンダビリティの確保）

【出典】情報セキュリティ政策会議 技術戦略専門委員会第17回会合資料（平成23年4月）

No.	重点テーマ	技術ロードマップ	関連施策の一例	必要額
⑤	攻撃者の行動分析等による予防基盤技術	<p>(a) 攻撃者のプロファイリングは、セキュリティ研究の全般に有益な情報となるため、研究成果を活用する基盤構築が必要。</p> <p>攻撃者のプロファイリング等に基づくモデル構築(3年) → 活用基盤の設計・構築(2年)</p> <p>(b) WebやSNS等を利用した新たな脅威の観測・分析・対策技術や、先行的防御の実現を目指した予防基盤技術の確立が必要。</p>		5億円 ×5年＝ 25億円
⑥	大規模ネットワークにおけるマルウェア収集挙動分析と広域攻撃観測の統合技術 (a) サイバー攻撃観測網の構築	<p>(a) 海外を含めた広域観測には、マルウェアの挙動分析の研究及び海外のステークホルダとの調整が必要。</p> <p>広域観測に向けた海外の関係者との調整(3年) → 広域観測基盤の構築(2年)</p> <p>(b) 能動的なディフェンスを実現するためには、その前段としてサイバー攻撃を能動的に観測するメカニズムの確立と観測網構築が必要。</p>	広域の攻撃観測とマルウェアの解析、さらにそれらを統合するサイバーセキュリティ技術の研究開発(NICT)	15億円 ×5年＝ 75億円

図8：情報セキュリティの研究開発における重要分野（攻撃者の行動分析に基づくゼロデイ・ディフェンス）

【出典】情報セキュリティ政策会議 技術戦略専門委員会第17回合会資料（平成23年4月）



No.	重点テーマ	技術ロードマップ	関連施策の一例	必要額
⑦	プライバシー情報の活用を促進する自己情報コントロール技術	<p>医療情報への適用を行うための実用化研究の前提として、秘密計算やプライバシー保護データマインギング技術等の基礎研究が必要。</p> 	<p>適材適所にセキュリティ技術を自動選択し、セキュアなネットワークを最適に構成するためのセキュリティアーキテクチャの研究開発(NICT)          新世代情報セキュリティ研究開発事業(アクセス制御、クラウド)(METI)</p>	<p>50億円          × 10年 =          500億円</p>
⑧	フォレンジック等を支援するためのデータ管理・追跡技術	<p>技術的な要件が法制度と関連するため、技術的な研究開発は法制度の整備と並行して進めることが必要。</p> 		<p>10億円          × 3年 =          30億円</p>
⑨	セキュリティ部品が正しく実装されていることを保証する製品評価技術	<p>適切なコストで実現できるシステムの評価技術が求められており、標準化のプロセスに沿った研究が必要。</p> 	<p>適材適所にセキュリティ技術を自動選択する技術の一端として、セキュリティ技術の組み合わせ方の正当性を評価する手法の研究開発及びプロセスのISOにおける標準化(NICT)          高度大規模半導体集積回路セキュリティ評価技術開発事業(METI)</p>	<p>10億円          × 3年 =          30億円</p>

図9：情報セキュリティの研究開発における重要分野（個人情報等の柔軟管理の実現）  
 【出典】情報セキュリティ政策会議 技術戦略専門委員会第17回会合資料（平成23年4月）




No.	重点テーマ	技術ロードマップ	関連施策の一例	必要額
⑩	サイバー・セキュリティ技術を評価する体系の確立、および実証研究のためのデータ基盤の構築	<p>セキュリティをサイエンスとして評価する方法の研究と理論研究の実証のためのデータ基盤の構築が必要。</p>  <p>データ収集制度の整備 データ形式の統一、評価方法の体系化の研究(3年) データ基盤の構築(2年)</p>	マルウェア検体や攻撃トラフィック等のセキュリティ情報を安全に研究利用するためのサイバーセキュリティ研究基盤の研究開発(NICT)	10億円 × 5年 = 50億円
⑪	情報理論的安全性を備えた暗号技術	<p>(a)情報理論的な暗号では、大きな秘密鍵を事前に共有する仕組みが重要。その手段として量子通信が有望。</p>  <p>量子通信の特定環境における実現(10年) 組込システムへの導入</p> <p>(b)量子計算機が実現されても安全性が低下しない、長期に渡って安全性を保証できる暗号技術が必要。</p>  <p>安全性評価手法(5年) 数学的アルゴリズムの開発(2年) 次世代PKI・電子署名試験環境構築(3年)</p>	現代暗号と量子ICTを組み合わせて新たな秘匿通信システムを実現する量子セキュリティ技術の研究開発(NICT)	5億円 × 10年 = 50億円

図10：情報セキュリティの研究開発における重要分野（研究開発促進のための基盤の確立）

【出典】情報セキュリティ政策会議 技術戦略専門委員会第17回会合資料（平成23年4月）

## 4. 米国・欧米の取組

### (1) 米国の研究開発動向

米国の情報セキュリティの研究開発は ICT 産業の競争力強化や国家安全保障等の側面から様々な省庁で実施されるが、それぞれの省庁が対象とする研究分野・予算スキームが異なるため、連邦政府全体で効果的な研究開発戦略を策定するために各省庁間の調整が図られてきた。2006 年には NITRD<sup>10</sup> CSIA<sup>11</sup>の組織横断的な検討グループ CSIA IWG<sup>12</sup>によって、連邦政府全体の情報セキュリティ技術分野を整理して優先分野を示した『Federal Plan For Cyber Security and Information Assurance Research and Development』が取りまとめられた。これにより、機能的サイバーセキュリティと情報保障、インフラのセキュリティ確保、次世代システムとアーキテクチャなど 8 つのコンセプトに係る約 50 の重点分野がボトムアップに抽出された。

一方、2008 年にブッシュ大統領から示された『CNCI<sup>13</sup>』や 2009 年にオバマ大統領による『Cyberspace Policy Review』では、情報セキュリティに関する連邦政府の研究開発体制を強化するとともに、画期的な (lead-ahead) 技術や環境変化に対応する (game-changing) 考えに基づく新たな研究開発を推進するトップダウンの方針が示された。その結果 DARPA<sup>14</sup>や NSF<sup>15</sup>などを中心に情報セキュリティの研究開発予算が増額され、NITRD CSIA 全体の 2011 年の予算 (推定) は 4.06 億ドルに上り、2007 年の予算 2.13 億ドルの 2 倍近い規模となった。

このように米国の情報セキュリティの研究開発においては、トップダウンの方針に基づく予算措置と、実際に研究開発を実施するための技術的な根拠に基づく予算措置と、実際に研究開発を実施するための技術的な根拠に基づく研究分野の整理、各組織間の調整や実施計画の策定等ボトムアップの検討が相互に繰り返されることで、現場のニーズに根ざした研究を拾い上げるとともに、ダイナミックな社会変化に対して迅速に対応する機能を持たせている。

### (2) EU の研究開発動向

EU の ICT 分野の研究開発は基本的に欧州首脳理事会で採択された『リスボン戦略』や欧州委員会によって策定された『i2010』などの上位戦略で示された方針に従い推進される。FP7 (第 7 期フレームワークプログラム) はこのような上位戦略の実施プログラムとして、EU の研究機関や企業に対して研究開発の助

<sup>10</sup> NITRD:Networking and Information Technology Research and Development

<sup>11</sup> CSIA:Cyber Security and Information Assurance

<sup>12</sup> CSIA IWG:Interagency Working Group on Cyber Security and Information Assurance

<sup>13</sup> CNCI:Comprehensive National Cybersecurity Initiative

<sup>14</sup> DARPA:Defense Advanced Research Projects Agency

<sup>15</sup> NSF:National Science Foundation

成を行う。バルセロナ会議や『新リスボン戦略』における研究開発への投資増加の方針を受け、FP7の予算は533億ユーロとFP6の191億ユーロから大きく増額されている（1年あたりの予算では約2倍の増額）。また、EUでは情報化社会の形成を見据えてICT分野の研究開発に力を入れており、FP7の国際連携研究では10の研究分野のうち、ICT分野のみで全体の予算の3割を占めている。中でも情報セキュリティはICTの安全性や信頼性を支える基盤的な技術として重視されている。FP7では情報セキュリティに関わる研究テーマはChallenge1:Pervasive and Trusted Network and Service Infrastructuresに分類され、情報セキュリティ技術に特化したものはObjective1.4:Trustworthy ICTの枠組みの中で実施されている。2011-2012年次計画ではChallenge1に6.25億ユーロの予算が割り当てられており、これは8つあるChallengeの中で最も多く、ICT分野全体予算の25%を占める（その内Trustworthy ICTは0.8億ユーロが割り当てられている）。

FP7の国際連携研究におけるICT分野の研究開発の目的は欧州のICT産業の競争力強化及び、ICT技術の欧州域内での普及とされており、社会経済的側面に重点を置いたプログラムが設定されている。そのため情報セキュリティに関わる研究テーマでもツールや標準、メトリクス、評価手法、ベストプラクティス等の実用化を前提としたものが重視されている。また、FPの研究スキームにも、欧州以外の地域との戦略的連携関係構築や、中小企業の研究開発支援、一般に向けた成果のアピール等、競争力強化及びICT技術の普及を推進する仕組みが取り入れられている。