資料2

NISC National Information Security Center

情報セキュリティ研究開発戦略の策定に係わる検討

2010年11月25日

内閣官房情報セキュリティセンター（NISC）
http://www.nisc.go.jp/

背景

「国民を守る情報セキュリティ戦略」
情報セキュリティ政策会議　第23回会合（平成22年5月11日）決定

技術戦略

（4）技術戦略の推進等
①情報セキュリティ関連の研究開発の戦略的推進等
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。

「情報セキュリティ2010」
情報セキュリティ政策会議　第24回会合（平成22年7月22日）決定

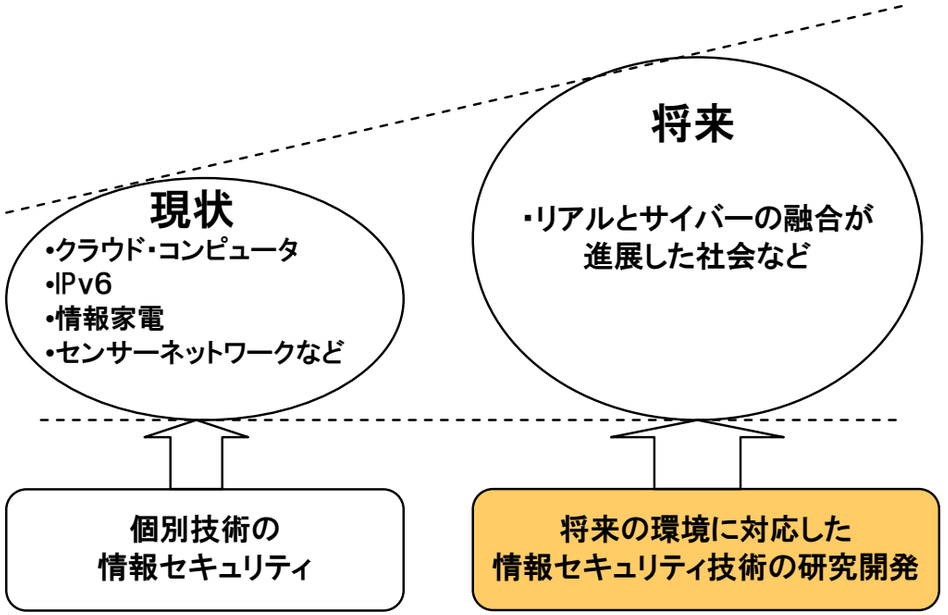
技術戦略

ア）新たな情報セキュリティ研究開発戦略の策定（内閣官房）
米国のサイバーセキュリティ強化法案等の動向を踏まえ、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、2011 年6 月を目処に新たな情報セキュリティ研究開発戦略を策定する。

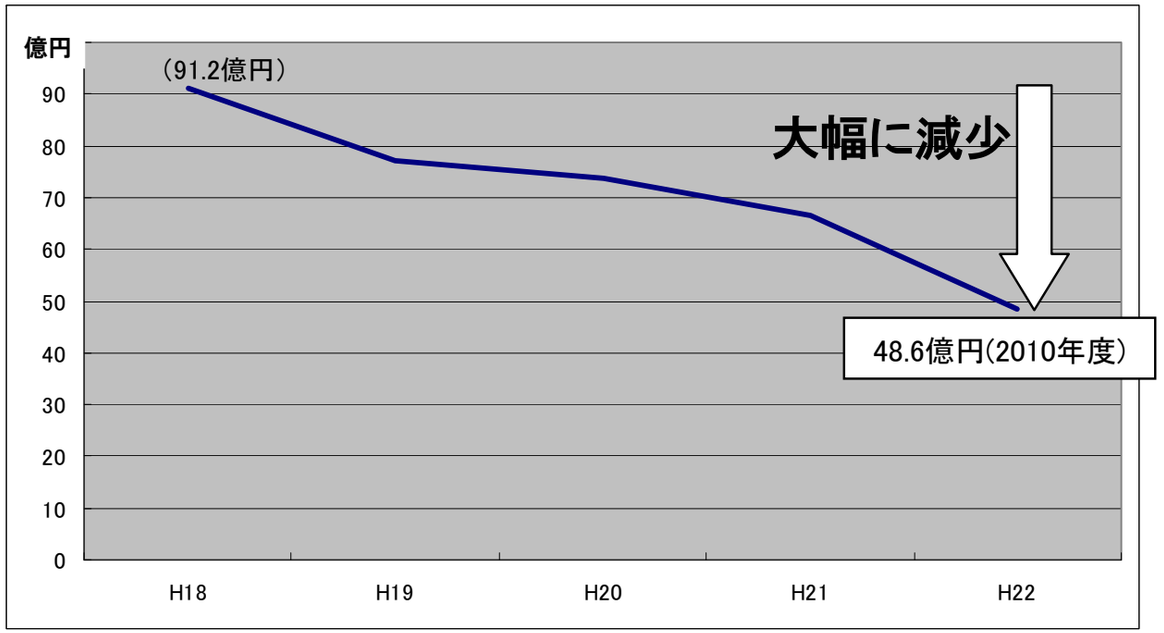
（略）

情報セキュリティ研究開発を取り巻く状況

①情報セキュリティの研究開発の必要性



②情報セキュリティ研究開発費の推移



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

③諸外国の情報セキュリティ研究開発戦略

	米国	EU	韓国
情報セキュリティの研究開発、技術開発に係わる戦略	サイバーセキュリティと情報保証のための米国連邦政府研究計画 （Federal Plan for Cyber Security and Information Assurance Research and Development）	セキュアな情報社会のためのEU戦略 （A strategy for a Secure Information Society - “Dialogue, partnership and empowerment”）	国家情報化基本計画
戦略の概要	今後10年間に必要となる研究開発の戦略を定めたもの。政府・民間の各分野で新たな活用法を創造するなどイノベーションを促進することを目的としている。	複数の利害関係者による取組みを強化するため、相互運用性と多様なソリューション開発を推進し、革新的かつ競争力を有する「欧州情報システム産業界」を育成することを目標とする。	サイバー攻撃に対する対応能力の向上、情報セキュリティに関する基盤技術の拡充、産業や人材の育成等を目的としている。
期間	2008年～2017年	研究開発フレームワーク（FP7）は 2007年～2013年	2009年～2012年

検討事項

問題意識

○　新たな環境変化に対応した研究開発戦略が必要

○　「いたちごっこ」の状況から脱却できる研究開発戦略の可能性の追求

検討内容

- 情報セキュリティを取り巻く環境変化と研究開発のあり方
- 科学技術分野における情報セキュリティ分野のあり方
- 我が国において重点的に推進すべき研究開発のあり方（分野、工程表等）
- 国際連携のあり方　など

問題意識

1. 今日まで、コンピュータウィルス対策ソフトなど「守り」の発想に基づく研究開発が行なわれてきたが、今後は、根本的な解決を目指す「攻め」の発想による研究開発を推進すべきではないか。

2. 今後の科学技術のイノベーションを促進するためには、情報通信技術を汎用的基盤技術として活用することが不可欠であり、その観点から情報セキュリティ技術の研究開発を位置付けることが重要ではないか。

3. 研究開発のみならず、日本の情報産業及び情報セキュリティ産業を活性化させるとの視点も重要ではないか。

4. 大規模サイバー攻撃事態が、今後我が国においても発生する可能性があることを踏まえ、我が国の情報システムや情報通信基盤の安全性を向上させるべきではないか。

5. 研究開発に関して、政府が負担する情報セキュリティ研究費は大幅な減少傾向にあることに、どのように対応すればよいのか。

我が国において重点的に推進すべき研究開発分野について

重点化して推進すべき研究対象分野（案）

攻撃者

攻撃の解析

- 攻撃者を特定する技術
- マルウェアの挙動分析技術
- DoSアタックの影響分析技術
- Spamを中継しているISPの判定技術など

情報システム

・ソフト
・ハード
（ネットワーク）

ディペンダブルな情報システムの開発

- 組み込みデバイスのセキュアなソフトウェア更新技術
- ディペンダブルなクラウドの構成技術
- 無線アドホックネットワークのセキュアな利用技術など

利用者

利用者の対応力（マネジメント技術等）

- ICT環境の変化に対応した情報セキュリティ指針
- セキュリティ投資に対す効果の定量化技術
- 社会科学的側面を考慮したマネジメント技術など

調査結果(意見の整理　その1)

攻撃の解析

No	研究対象分野	概要	技術分類
1	トレースバックのための国際観測拠点の設置とデータ解析	広義トレースバック(発信元の特定だけでなく、マルウェアの挙動分析、DoSアタックの影響分析、Spamを中継するISPの判定など)のためのデータ解析、国際的な観測データ収集スキームの構築	攻撃の解析
2	高度に重要な情報の管理技術	機微情報の管理技術及び重要情報の漏えい事案の対処(トレースバック等)方法	
3	悪意の利用者のゲーム理論	攻撃者及び協力者(無意識の協力者を含む)の行動要素(悪事への投資規模と期待する効果など)の分析、悪意の利用者の全貌把握(比較制度分析のような、全体の見取り図を知るためのモデル手法)	

調査結果(意見の整理　その2)

ディペンダブルな情報システムの開発

No	研究対象分野	概要	技術分類
4	ディペンダブル情報システムの構築	ディペンダブル(可用性だけでなく、セキュリティやプライバシー面の信頼性を合わせ持つ)ソフトウェア開発技術、ソフトウェアの柔軟性・拡張性とディペンダブルを両立するセキュアなソフトウェア更新フレームワーク	ディペンダブルな情報システムの開発
5	ネットワーク化された組み込みデバイス(センサー、アクチュエータ)のセキュリティパッチ適応スキーム	組み込みデバイスに対する統一的かつ安定的にセキュリティ向上の機能(ソフトウェア)を安全に書き換える技術及びフレームワーク	
6	組み込みシステムにおけるセキュリティ	組み込みシステムの脆弱性対処としてのソフトウェア更新フレームワーク	
7	無線ブロードバンド環境におけるセキュリティ技術	端末相互間のリンクが不確実な無線アドホックネットワークのセキュアな利用技術及び、無線周波数帯の効率的な利用技術	
8	クラウド化、大規模化に伴うセキュリティ	セキュリティ及びプライバシー面の信頼性を備えたクラウドの構成方法、クラウドセキュリティの可視化	

調査結果(意見の整理　その3)

利用者の対応力(マネジメント技術等)

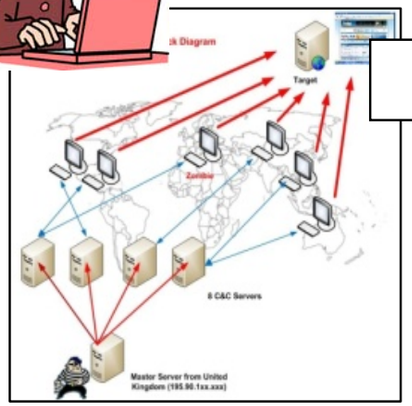
No	研究対象分野	概要	技術分類
9	レジリエントな高信頼性組織体制の構築	セキュリティ・インシデントのコーディネーション(意思疎通、情報共有のあり方)体制、社会科学的な側面(人的・組織的な側面)を考慮したマネジメント技術	利用者の対応力(マネジメント技術等)
10	BCM (Business Continuity Management)における情報セキュリティ対応策の策定	BCPのベストプラクティス(脅威に対する事前対策、脅威が顕在化した場合の対応、脅威を排除し正常化するベストプラクティスなど)の明示化	
11	新しい社会システムにおける情報セキュリティのあり方	ICT環境の変化(クラウドコンピューティング、利用端末の多様化、個人情報などの社会意識問題など)に対応した情報セキュリティ指針の策定	
12	文書中の重要事項の公開/非公開手法	文書が漏出することも想定し、例えば文書ファイルを多重レイヤー構造として、重要文書中の重要事項のレイヤーを暗号化しておくなど、公開／非公開を部分的にコントロールできる技術	
13	ROSI (Return On Security Investment)の可視化	セキュリティ投資対効果の定量化及び標準策定	

昨年度の検討（今後の研究開発課題の例）

- 昨年度は、現在の情報セキュリティの潮流を踏まえて、技術リスト（約150項目）の中から研究開発課題が残っているテーマを抽出

情報セキュリティ課題の根本的解決

- 情報漏洩検出技術（量子情報通信技術）
- **個人情報の安全な利用を可能とする情報管理技術**
- システムの相互影響評価・リスク分析技術
- セキュア・ソフトウェア構築技術
- **社会心理学に基づく情報セキュリティ対策技術**



IT技術の発展・普及に伴う情報セキュリティ

- **分散環境におけるプライバシー保護技術**
- **個人情報の安全な部分開示・管理技術**
- センシング情報の利活用におけるプライバシー保護
- クラウドサービスを想定した脅威分析・検出技術
- セキュア・ネットワーク・プロトコル技術

IT利用者の対応力向上

- **ユーザによる個人情報の制御**
- ユーザの意図に沿った操作支援技術
- セキュリティ投資対効果の評価技術
- 仮想環境上の情報セキュリティ確保技術

脅威の全体像の把握及び対抗スキーム

- データマイニングによる異常検知技術
- 大容量トラフィック監視技術
- サイバー攻撃のトレースバック技術
- 未知プロトコル・不正コンテンツ検出技術
- **社会的な合意形成技術**

セキュリティを高めたITの実現

- **システムの安全性・信頼性確保技術**
- 社会的な安全性・信頼性の確保技術
- 情報セキュリティの自動検証技術
- **IT障害の自動復旧技術**
- 情報セキュリティ対策の定量評価技術
- HW/OS/SWの信頼性確保技術
- **高速通信暗号化技術**

※赤太字は、重要度及び緊急性が高いと判断した研究テーマ

「科学技術に関する基本政策について」における記述

「第４期科学技術基本計画（2011～2015）」の素案

科学技術に関する基本政策について

目次

Ⅰ．基本認識

Ⅱ．成長の柱としての２大イノベーションの推進

Ⅲ．我が国が直面する重要課題への対応

1．基本方針
2．重要課題達成のための施策の推進
　（1）豊かで質の高い国民生活の実現
　（2）我が国の産業競争力の強化
　（3）地球規模の問題解決への貢献
　（4）国家存立の基盤の保持
　（5）科学技術の共通基盤の充実、強化
3．重要課題の達成に向けたシステム改革
4．世界と一体化した国際活動の戦略的展開

Ⅳ．基礎研究及び人材育成の強化

Ⅴ．社会とともに創り進める政策の展開

4）国家存立の基盤の保持
研究開発課題によっては、我が国が国際的な優位性を保持し、国民生活の安全を確保していくため、国自らが長期的視点に立って、継続的に、広範囲かつ長期間にわたって研究開発を推進し、成果を蓄積していくべき課題がある。このような研究開発課題については、国として、国家存立の基盤に関わる研究開発と位置づけて強力に推進する。＜途中略＞

ⅰ）国家安全保障・基幹技術の強化
有用資源の開発や確保に向けた海洋探査及び開発技術、情報収集をはじめ国の安全保障にもつながる宇宙輸送や衛星開発及び利用に関する技術、独自のエネルギー源確保のための新エネルギーに関する技術、高速増殖炉サイクルや核融合等の原子力に関する技術、世界最高水準のハイパフォーマンスコンピューティング技術、さらに地理空間情報や**情報セキュリティに関する技術の研究開発を推進**する。

科学技術に関する基本政策について（パブリックコメント募集文書、平成22年10月18 日）より抜粋

（参考）米国における情報セキュリティ研究開発戦略の策定の取組み

米国　NITRD CSIA IWG Cybersecurity Game-Change Research&Development Recommendations※ 概要

- NITRD (Networking and Information Technology R&D) Program と CSIA IWG (Cyber Security Information Assurance Interagency Working Group) により、2010年5月に策定
- Cybersecurity の現状の課題を、以下の３点に整理
  - ✓Attackのcostは攻撃者にとって圧倒的有利である
  - ✓全てのセキュリティ要件を同時に満たすような理想的システムの構築は、コストがかかり過ぎて事実上不可能である
  - ✓セキュリティに関する有効な指標や経済的に妥当な意思決定の欠如のため、適切な資源配分が妨げられている
- 上記の現状認識を前提とし、それを覆す“Game-Change”を実現するための initial R&D themes として、以下の3つのテーマを提唱
  - ◆**Moving Target**：動的に「変化」することで攻撃の困難さやコストを増加させ、攻撃にさらされても悪影響を受けにくいシステムの実現
  - ◆**Tailored Trustworthy Spaces**：ユーザの context に応じた適切なセキュリティ要件が実現される trust environment の実現
  - ◆**Cyber Economic Incentives**：Cybersecurity への適切な投資判断を可能にする、科学的な指標等の提供
- 各テーマについて、vision, milestone, critical supporting technologies などを提示。3つのテーマはそれ自体が重点研究課題という訳ではなく、研究課題を設定する際の方向性(initial focus)を示すものと位置づけられている

※原文は、添付の「CSIA_IWG_Cybersecurity_Game-Change_%20RD_Recommendations_20100513.pdf」を参照のこと

（参考）米国における情報セキュリティ研究開発戦略の策定の取組み

米国　NITRD CSIA IWG Cybersecurity Game-Change Research & Development Recommendationsについての技術戦略専門委員会委員のご意見

- 「Cyber Economic Incentive」は、制度・市場への参加者に適切なインセンティブを付与することの重要性を指摘したものであり、経済学的にみても妥当なもの。市場設計（market design）という観点は、市場参加者に適切なインセンティブを付与しつつR＆Dを推進する政策を検討するうえで重要なポイントになる。

- 「Cyber Economic Incentive」に述べられているように、対策側にインセンティブを与えて投資させることは、もちろん大切である。しかし、同時に悪者を「discourage」することを考えるべきである。ここで悪者という範囲に、意識的あるいは無意識のうちに悪者に協力している人、サイト、事業者を含めて考えると、従来から提案されている要素技術の意味が総合的な配置の中で明らかになる。同時に攻撃者の費用を直接に増大させる方法が現在は手薄であることが分かる。

情報セキュリティ研究開発戦略検討スケジュール（案）

平成22年11月25日
　　第16回　技術戦略専門委員会（研究開発戦略の検討キックオフ）

平成23年1月（予定）
　　第17回　技術戦略専門委員会（骨子案決定）

平成23年6月（予定）
　　第18回　技術戦略専門委員会（戦略案決定）