別添1

NISC National Information Security Center

補足資料

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/

我が国の情報セキュリティ研究開発の状況（総務省・経済産業省）

総務省

No.	施策名称	期間	研究開発の目標
1	スパムメールやフィッシング等サイバー攻撃の停止に向けた試行	H18-22	情報システム、ソフトウェア又はネットワークに関して、新たな脅威に対応した情報セキュリティに係わる被害を未然に防止する技術及び、被害が発生した場合にもその被害を局限化できるような技術を開発する。 我が国の国民生活・経済活動・安全保障に密接に関連する情報セキュリティを適切に確保し、ITを安心して利活用できる環境を整備するため、適切な組織体制の確立、信頼性の高い情報システム、ソフトウェア又はネットワークの普及及び電子認証基盤の構築に関わる技術を確立する。 【総務省・経済産業省（連名）】
2	情報漏えい対策技術の研究開発	H19-21	
3	経路ハイジャックの検知・回復・予防に関する研究開発	H18-21	
4	ネットワーク環境の脆弱性レベルをリアルタイムで定量評価し、情報流通をセキュアに運用するための意志決定支援システムの研究開発	H16-18	脆弱性をリアルタイムに評価分析し、意志決定を支援するシステムの開発を目指す
5	スパムメールやフィッシング等サイバー攻撃の停止に向けた試行	H18-22	2010年までに、ボットを捕獲・解析・駆除するための技術の確立を目指す
6	IPパケットトレースバック技術に関する研究開発	H17-21	2009年度までに、アドレスを詐称した通信の正しい送出機器を探知しうるトレースバック技術の確立を目指す
7	情報セキュリティ技術に関する研究開発	H18-22	2010年頃までにネットワーク上のサイバー攻撃・不正通信などに耐え、それらを検知、排除する技術の実現を目指す
8	量子暗号実用化のための研究開発	H18-22	2010年度までに、100kbps程度の鍵配送レートを有する8～16ノードの都市内量子暗号網を実現するための量子暗号ネットワーク技術等を実現する
9	光・量子通信技術に関する研究開発	H18-22	2030年までに、情報通信の大容量化と高秘匿性を確保する量子通信技術を実現する

経済産業省

No.	施策名称	期間	研究開発の目標
1	コンピュータセキュリティ早期警戒体制の整備事業	H17-22	情報システム、ソフトウェア又はネットワークに関して、新たな脅威に対応した情報セキュリティに係わる被害を未然に防止する技術及び、被害が発生した場合にもその被害を局限化できるような技術を開発する。【総務省・経済産業省（連名）】
2	企業・個人のセキュリティ対策促進事業	H17-22	我が国の国民生活・経済活動・安全保障に密接に関連する情報セキュリティを適切に確保し、ITを安心して利活用できる環境を整備するため、適切な組織体制の確立、信頼性の高い情報システム、ソフトウェア又はネットワークの普及及び電子認証基盤の構築に関わる技術を確立する。【総務省・経済産業省（連名）】

我が国の情報セキュリティ研究開発の状況（文部科学省の科研費）

凡例　テーマ数：1～20　21～40　41～

ソフトウェア・アルゴリズム等

① H／W

耐タンパー性のあるH／W

・安全性と製造検査容易性の両立したLSI設計方法の研究（九州大学）　ほか計 **4テーマ**

② OS

セキュアなOS

・仮想マシンモニタのための安全性向上技術に関する研究（電気通信大学）　計 **1テーマ**

③ 認証

・大量の情報の機密性・完全性を保証する情報セキュリティ技術の研究（福井大学）　ほか計 **4テーマ**

減少傾向

④ 暗号

・大量の情報の機密性・完全性を保証する情報セキュリティ技術の研究（福井大学）　ほか計 **10テーマ**

⑤ プライバシ保護

プライバシ保護

・プライバシーデータマイニングのための暗号プロトコルの設計と安全性評価（九州大学）　ほか計 **7テーマ**

増加傾向

⑥ 機器セキュリティ

脆弱性対策

・仮想マシンモニタのための安全性向上技術に関する研究（電気通信大学）　ほか計 **3テーマ**

⑦ ネットワーク技術

ネットワークセキュリティ

・センサネットワークの安全・安心を保証する情報セキュリティ技術の研究（北陸先端科学技術大学院大学）ほか計 **17テーマ**

増加傾向

⑧ システム構築技術

セキュアシステム構築

・マルチビューに基づく安全なシステム設計法の研究（国立情報学研究所）　ほか計 **8テーマ**

⑨ 社会システム

人材育成

経済システム

防災

・情報セキュリティの相互依存性に関する経済分析（東京大学）　ほか計 **19テーマ**

⑩ 運用管理

評価システム

・セキュリティシステムの危殆化リスク評価とシステムSLAの提案（筑波大学）　ほか計 **2テーマ**

各国の情報セキュリティ研究開発プログラムの特徴

	米国	EU	韓国
国家戦略	Federal Plan for Cyber Security and Information Assurance Research and Development	A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"	国家情報化基本計画
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が促進されることを目的としている。	革新的かつ競争力を有する「欧州情報システム産業界」の育成	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。
プログラムや制度	Cyber Security and Information Assurance（CSIA）	ICT Work Programme Objective 1.4 および Objective 1.7	国家情報化基本計画
概要	基本的なインフラストラクチャと先進的なコミュニケーション機能を経済のあらゆる分野に提供することを目的とし、特に緊急通信網や金融システムなど重要インフラへのサイバー攻撃の対策技術、情報漏えいの検知や機密情報の保護に係わる技術の研究開発・技術開発を推進するためのプログラム。	ICTの信頼性や利便性向上、サイバー攻撃への対策能力向上や重要インフラの防護を目的とし、EU各国の関係機関や企業が連携して研究開発・技術開発を推進するためのプログラム。	韓国では、情報セキュリティに特化した制度は設けておらず、上記の「国家情報化基本計画」に情報セキュリティ分野を含むIT関連全般に対する内容を含んでいる。近年、韓国で増加している個人情報漏えいへの対策などの研究開発・技術開発を推進することにしている。
推進主体	CSIA IWG （大統領直属の科学技術諮問委員会NSTCの下部組織）	Information Society and media Directorate General （欧州委員会の部局のひとつ）	行政安全部
予算	3億4,250万ドル(2010年度) (約310億円)	4,300万ユーロ(2008年) (約53億7,500万円)	詳細不明
特徴	**(1)認知心理学等に重点をおいた研究開発 (2)情報セキュリティ関連の研究者への奨学金制度の拡充**	**ネットワークサービスにおける個人情報の取り扱い方法などはEU加盟国全体の問題として研究開発を推進**	**政府の研究開発と民間の製品化力のマッチングを組織化・制度化し、安全保障に関わる製品開発を効率的に推進**

米国CSIAのR&D計画

CSIAは、連邦政府のサイバーセキュリティ・情報保障R&D計画を策定しており、技術面、予算面での8つの優先領域を示している。

- 機能的なサイバーセキュリティ及び情報保障
（認証、承認、信頼管理、アクセス制御、特権管理、攻撃からの保護、攻撃の予防・先制、大規模サイバー攻撃の自動攻撃検出、警戒、レスポンス、フォレンジクス、トレースバック等）
- インフラの安全確保
（セキュアなプロセス制御システム）
- 領域特化型セキュリティ
（ワイヤレス・セキュリティ、集中型ネットワークと異種トラフィックのセキュリティ）
- サイバーセキュリティと情報保障の特性解析と評価
（ソフトウェア品質評価と障害特性解析、脆弱性と悪質コードの検知、ソフトウェア試験と評価ツール）
- サイバーセキュリティと情報保障基盤
（暗号学、セキュアなソフトウェア工学、ITシステムの工学ライフサイクルを通じたセキュリティ分析技術）
- サイバーセキュリティと情報保障R&Dの実現技術
（サイバーセキュリティと情報保障R&Dテストベット、ITシステムのモデリング、シミュレーション、および可視化）
- 高度な次世代システムとアーキテクチャ
（信頼コンピューティング・ベース・アーキテクチャ、セキュアかつ高保障なシステムおよびアーキテクチャ、拡張可能セキュアシステム、自律システム、次世代インターネット・インフラ・アーキテクチャ）
- サイバーセキュリティと情報保障の社会的側面
（プライバシー）

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

FP7 ICT Workprogramme 2007-2008 Objective 1.4 projects Secure, dependable and trusted Infrastructure 概要

プロジェクト名称	概要	分類	URL
MASTER	Business risk analysis, compliance engineering, security technology 特に、セキュリティ コンプライアンスの監査・粛正・監視を実現する方法論や基盤の提供を目指す。	管理技術、 ネットワーク技術、 社会システム	http://www.master-fp7.eu/
PRIME LIFE	Bringing sustainable privacy and identity management to future networks and services	プライバシ保護、 ID管理	http://www.primelife.eu/
TAS3	Trusted Architecture for Securely Shared Services	ID管理(ID連携)、 分散データ管理、 プライバシ保護	http://tas3.eu/
TECOM	Trusted Embedded Computing 組み込みプラットフォーム上での トラスト コンピュータ ソリューションの開発を目指す。(パソコンでのTPMの組み込み機器版)	HW、 機器セキュリティ	http://www.tecom-project.eu/
TURBINE	Trusted Revocable Biometric Identities To develop an innovative, privacy enhancing technology solution for electronic identity (eID) authentication through fingerprints biometrics	認証、 プライバシ保護	http://www.turbine-project.eu/

Objective 1.4 projects のうちの統合プロジェクト(比較的大規模なプロジェクト)として選定された5つのプロジェクトのうち、PRIME LIFE,TURBINEの2つはプライバシ保護がプロジェクトの主要な動機として明確に位置付けられている。また、TAS3においてもプライバシ保護が主要な要素に含まれている。

個別課題にとりくむ特定目的研究プロジェクトにおいても、12件のうち4件でプライバシ保護が主要な要素となっている。特定目的研究プロジェクトについては、別添の「」を参照のこと。