

産業技術総合研究所 情報セキュリティ研究センター (RCIS) 紹介

2011年2月1日

情報セキュリティ研究センターとは

■ 産総研の研究分野

- 環境・エネルギー、ライフサイエンス、情報通信エレクトロニクス、ナノテク・材料・製造、標準・計測、地質

■ 設置期間：2005年4月～2012年3月

■ ハード、ソフト、理論系の5チーム構成

■ 人員構成：

常勤研究員	34(13)
招聘研究員	5
顧問	4
ポスドク	3
テクニカルスタッフ	8
産学官・国際連携来所者	10
事務系	7
合計	71

- 消費者の情報や権利を保護するための情報**セキュリティ対策**技術
 - ネットワーク社会において消費者の情報や権利を保護するため、バイオメトリクスやパスワード等の認証情報が漏えいした際にも、認証情報更新を容易にすることにより、被害を最小限に抑えることができる個人認証技術や、ユーザがサーバと相互に認証することで、ユーザがフィッシング詐欺を認知可能とする技術等のプライバシー情報保護及びユーザ権限管理技術を開発する。さらに、開発した技術を、ウェブブラウザのプラグイン等の形で5つ以上実装、公開し、10以上のウェブサービス等での採用を目指す (II-3-(1)-④)。
- 情報システム**製品のセキュリティ評価**技術
 - ICカードに代表されるハードウェアや基幹ソフトウェア等、情報システムの中核をなす製品の脆弱性分析や安全性評価に関して、現行の制度、標準や新たな評価制度を見据えた技術を開発する。また、当該技術等について、我が国の電子政府推奨暗号評価等での活用を実現する。さらに、それらの技術等を実システムに組み込み可能な暗号ライブラリに適用し、安全性検証済みライブラリとして公開する (III-3-(5)-①)。
- センター終了後も、引き続き研究が続けられる予定

各チームの研究分野

- セキュリティ基盤技術研究チーム
 - 暗号技術（暗号、デジタル署名、プライバシー保護他）
 - 社会科学等の他分野との融合領域
- 物理解析研究チーム
 - 量子情報セキュリティ
 - 符号理論ベースのセキュリティ技術
 - ハードウェアのセキュリティ解析
- ソフトウェアセキュリティ研究チーム
 - 脆弱性を防ぐプログラム作成技術
 - プログラムの安全性検証・保証技術
- ハードウェアセキュリティ研究チーム
 - ハード暗号モジュール評価ボード SASEBO の開発
 - 安全性評価環境の整備
- ICSS 技術チーム
 - IC チップセキュリティ評価体制構築に向けた産官連携による技術開発