

平成 24 年度「戦略的国際連携型研究開発推進事業」情報セキュリティに関する
研究開発課題の公募 委託先候補一覧

研究開発課題	研究機関 (下線は代表研究機関)	研究開発期間	研究開発概要
オープン環境におけるプログラム保護技術の研究開発	<u>株式会社 KDDI 研究所</u>	平成 24 年度	クラウドやオープンプラットフォームなどの比較的信頼性の低い環境で実装されるプログラムを保護するための技術を確立する。これに加えて、プログラム保護技術を応用してソフトウェアでトラストアンカーを構築することで、サーバに保存されたデータの管理状況をユーザがセキュアに検証できる技術やサーバ上で実行するプログラムを保護する技術を検証する。これらの実現のために、従来とは異なる基礎技術を使用し、性能低下を最小限とするセキュリティ対策を提案する。 (FP7 SecFutur と連携。)
情報流通連携のためのオープンな ID 連携プラットフォームにおけるプライバシー保護機能の高度化	<u>国立情報学研究所</u> 東京大学 京都大学 株式会社野村総合研究所	平成 24 年度	現在、広く用いられている ID 連携プラットフォームでは、個々のユーザの認証を行った後、そのユーザに関する属性情報を ID 管理側からサービス提供側に提示し、それに基づいて認可判断を行う形態をとる。属性情報には個人情報が含まれるので、その提示には本人同意が前提となるのは当然として、その開示範囲が必要最小限となるように配慮すべきである。 また、誰がどのようなサービスにアクセスしたかという情報もプライバシー情報として保護されるべきものであり、開示範囲を最小化する必要がある。 本研究開発では、これらの属性情報を適切に暗号化、仮名化（スードニマイズ, pseudonymize）した上で流通させる仕組みを標準化することにより、たとえば、ユーザがどのサービスにアクセスしたかが ID 管理側に分からない、あるいは、どのユーザがアクセスしてきたかがサービス提供側に分からない（しかし正しいユーザであることは保証され、インシデント発生時には関係者の協力によりユーザの特定可能）、といった機能を持つオープンなプラットフォームを開発し、ユーザのプライバシー保護を担保した上での自由な情報の流通・連携を実現する。 (FP7 GÉANT と連携。)

<p>医療等社会システムのセキュリティ・デペンダビリティを確保維持するマルチレイヤ ICT の研究開発</p>	<p>横浜国立大学 中央大学 株式会社日本ジー・アイ・ティー</p>	<p>平成 24 年度</p>	<p>医療、エネルギー、交通などのライフラインとなる命に関わる Life Critical な社会システムに対する意図的な攻撃や干渉妨害に必要なセキュリティ、デペンダビリティの条件やレベルを定義、設定し、処理能力・消費電力に制約がある医療用ボディアエリアネットワーク（BAN）などでもその条件やレベルを満たす物理層から上位層の要素技術とマルチレイヤ垂直統合技術を、フィンランドのCWCとCWC日本などの既に確立されたEU-日本の共同体制を活用して研究開発する。さらに、本年2月に国際標準化を達成したBAN（IEEE802.15.6）のセキュアシステムの試作、治験や技術基準適合証明などの法的認証や社会実験を短期間で実現し、車両制御用ハーネスなどの Life Critical システムへ水平展開し、国際ビジネスをEU-日本共同で展開する。</p>
---	---	-----------------	---