第３回 情報セキュリティ分野に係る
技術に関する評価検討会
資料２

情報セキュリティ分野に係る
技術に関する施策・事業

評価報告書

（案）

平成２６年３月

情報セキュリティ関連分野に係る
技術に関する施策・事業評価検討会

はじめに

研究開発の評価は、研究開発活動の効率化・活性化、優れた成果の獲得や社会・経済への還元等を図るとともに、国民に対して説明責任を果たすために、極めて重要な活動であり、このため、経済産業省では、「国の研究開発評価に関する大綱的指針」（平成２０年１０月３１日、内閣総理大臣決定）等に沿った適切な評価を実施すべく「経済産業省技術評価指針」（平成２１年３月３１日改正）を定め、これに基づいて研究開発の評価を実施している。

また、第２５回産業構造審議会評価小委員会（平成２１年１月）において、新たな評価類型として「技術に関する施策評価」が審議・了承された。技術に関する施策評価は、当該技術分野全体の方向性等を勘案しつつ、当該施策の下に位置付けられる技術に関する事業のまとまりを俯瞰する形で、各事業の相互関係等に着目し、個々の事業に係る評価結果を踏まえて行うこととしている。経済産業省において実施している技術に関する施策「情報セキュリティ分野」は、ＩＴが経済社会に浸透する中で、安全・安心な国民生活、企業活動のためには、情報セキュリティの確保が不可欠となっている状況のもとで、国民を守る情報セキュリティ戦略（平成２２年５月情報セキュリティ政策会議決定）における「世界最先端の『情報セキュリティ先進国』」を目指すため、以下の事業から構成される施策である。

（１）技術的情報セキュリティ対策推進事業

Ａ　新世代情報セキュリティ研究開発事業

①情報家電、スマートグリッド等におけるセキュリティ対策技術の研究開発

ａ 高度電磁波解析技術によるLSIのセキュリティ対策に関する研究（平成２２年度から平成２４年度まで）

ｂ 情報家電、スマートグリッド、携帯端末など、非PC端末における未知脆弱性の自動検出技術に関する研究（平成２２年度から平成２４年度まで）

②アクセス制御技術の研究開発

ｃ プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究（平成２２年度から平成２４年度まで）

ｄ 撮影による情報漏洩を防止するソリューションの研究開発（平成２２年度から平成２３年度まで）

③クラウドコンピューティングに関するセキュリティ対策技術の研究開発

ｅ 効率的な鍵管理機能を持つクラウド向け暗号化データ共有システム（平成２２年度から平成２３年度まで）

ｆ クラウドサービスプロバイダとクラウドユーザ企業（法人）における事業継続計画（BCP）の在り方と連携の確保、及びその妥当性検証技術に関する研究（平成２２年度）

ｇ ＰａａＳ／仮想化環境におけるコンプアライアンス指向データアクセス手法の研究開発（平成２２年度）

Ｂ 高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業）（平成２１年度から平成２３年度まで）

Ｃ 暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発（平成２３年度から平成２５年度まで）

（２）ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築事業）（平成２３年度）

今回の評価は、技術に関する施策「情報セキュリティ分野」、及びこの構成要素である技術に関する事業評価であり、実際の評価に際しては、省外の有識者からなる情報セキュリティ関連分野に係る技術に関する施策・事業評価検討会（座長：徳田英幸　慶應義塾大学大学院 政策・メディア研究科委員長　教授）を開催した。

本書は、これらの評価結果を取りまとめたものである。

情報セキュリティ関連分野に係る技術に関する施策・事業評価検討会
委員名簿

座　長	徳田　英幸	慶應義塾大学大学院 政策・メディア研究科委員長　教授
	後藤　厚宏	情報セキュリティ大学院大学 情報セキュリティ研究科　教授
	関口　和一	株式会社日本経済新聞社　編集委員 兼 論説委員
	田辺　孝二	東京工業大学大学院 イノベーションマネジメント研究科　教授
	西村　敏信	公益財団法人金融情報システムセンター　監査安全部長

（敬称略、五十音順）

事務局：経済産業省 商務情報政策局 情報セキュリティ政策室

「情報セキュリティ分野」に係る技術に関する施策・事業評価に係る
省内関係者

１．技術に関する施策

商務情報政策局　情報セキュリティ政策室　上村　昌博（事業担当室長）
産業技術環境局　産業技術政策課　技術評価室長　飯村　亜紀子

２．技術に関する事業

Ａ．新世代情報セキュリティ研究開発事業

商務情報政策局　情報セキュリティ政策室　上村　昌博（事業担当室長）
産業技術環境局　産業技術政策課　技術評価室長　飯村　亜紀子

Ｂ．高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業）

商務情報政策局　情報セキュリティ政策室　上村　昌博（事業担当室長）
産業技術環境局　産業技術政策課　技術評価室長　飯村　亜紀子

Ｃ．暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発

商務情報政策局　情報セキュリティ政策室　上村　昌博（事業担当室長）
産業技術環境局　産業技術政策課　技術評価室長　飯村　亜紀子

Ｄ．ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築事業）

商務情報政策局　情報セキュリティ政策室　上村　昌博（事業担当室長）
産業技術環境局　産業技術政策課　技術評価室長　飯村　亜紀子

「情報セキュリティ分野」に係る技術に関する施策・事業評価

審　議　経　過

〇第１回評価検討会（平成２６年２月１８日）
・評価の方法等について
・技術に関する施策事業の概要ついて
・評価の進め方について

〇第２回評価検討会（平成２６年３月１４日）
・技術に関する施策事業の概要ついて
・評価の進め方について

〇第３回評価検討会（平成２６年３月２７日書面開催）
・評価報告書（案）について

〇産業構造審議会技術分科評価小委員（平成２６年４月予定）
・評価報告書（案）について

目　　次

第１章　評価の実施方法 26
１．評価の目的 27
２．評価者 28
３．評価対象 28
４．評価方法 29

第２章　技術に関する施策の概要 31
１．施策の目的・政策的位置付け 32
２．施策の構造及び目的実現の見通し 37

第３章　技術に関する事業の概要 42
〇情報セキュリティ分野に係る技術に関する事業について 43
Ａ　新世代情報セキュリティ技術開発事業 44
①　情報家電、スマートグリッド等におけるセキュリティ対策技術の研究開発 45
Ａ－ａ　高度電磁波解析技術による LSI のセキュリティ対策に関する研究 ... 45
Ａ－ｂ　情報家電、スマートグリッド、携帯端末など、非 PC 端末における未知脆弱性の自動検出技術に関する研究 68
②　アクセス制御技術の研究開発 82
Ａ－ｃ　プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究 82
Ａ－ｄ　撮影による情報漏洩を防止するソリューションの研究開発 106
③ クラウドコンピューティングに関するセキュリティ対策技術の研究開発 128
Ａ－ｅ　効率的な鍵管理機能を持つクラウド向け暗号化データ共有システム 128
Ａ－ｆ　クラウドサービスプロバイダとクラウドユーザ企業（法人）における事業継続計画（BCP）の在り方と連携の確保、及びその妥当性検証技術に関する研究 146
Ａ－ｇ　ＰａａＳ／仮想化環境におけるコンプアライアンス指向データアクセス手法の研究開発 150
Ｂ　高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業） 156
Ｃ　暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発 172

２．２　ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築事業） 189

第４章　技術に関する施策評価 201
１．施策の目的・政策的位置付けの妥当性 202
２．施策の構造及び目的実現見通しの妥当性 205
３．総合評価 207

第５章　技術に関する事業評価 209
(1) 技術的情報セキュリティ対策推進事業 210
Ａ　新世代情報セキュリティ研究開発事業 210
Ｂ　高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業） 212
Ｃ　暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発 213
(2) ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築事業） 214

第６章　今後の研究開発の方向等に関する提言 216

第７章　評点法による評点結果 219

技術に関する施策・事業評価報告書概要

技術に関する施策

技術に関する施策名	情報セキュリティ分野
担当課	商務情報政策局　情報セキュリティ政策室

技術に関する施策の目的・概要

第２次情報セキュリティ基本計画（平成２１年２月情報セキュリティ政策会議決定）における「『IT を安心して利用できる環境』の構築」及び国民を守る情報セキュリティ戦略（平成２２年５月情報セキュリティ政策会議決定）における「世界最先端の『情報セキュリティ先進国』」を目指す。

これを実現するため、以下を実施。

① コンピュータウイルス等による被害の抑制・未然防止を図る早期警戒体制の整備やインターネット利用者への普及啓発等

② 企業等の情報セキュリティ対策の実施に役立つガイドラインの整備等の組織的対策及び情報セキュリティに係る研究開発等の技術的対策

③ 災害被害により経済活動が停滞し、民間による積極的な投資が望めない状況にある被災地における、今後の産業活動の基盤となるサイバーセキュリティテストベッドの環境整備

④ 被災地域におけるＩＴ・電機分野での強みを活かした産業復興を実現するため、産学官連携の下、重要インフラＩＴの安全性検証・普及啓発の国際拠点の整備

事業一覧

① コンピュータセキュリティ早期警戒体制の整備事業

② 企業・個人の情報セキュリティ対策促進事業

③ ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築）

④ 東北復興再生に資する重要インフラＩＴ安全性評価・普及啓発拠点整備・促進事業

（注）平成２４年度から①コンピュータセキュリティ早期警戒体制の整備事業と②企業・個人の情報セキュリティ対策促進事業が統合され、「情報セキュリティ対策推進事業」となった。以下の項同じ。

※これらの事業のうち、本年度に実施するプロジェクト評価の対象となる技術に関する事業は以下の４つである。

（企業・個人の情報セキュリティ対策促進事業）

Ａ．新世代情報セキュリティ研究開発事業

Ｂ．高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業）

Ｃ．暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発

（ＩＴ融合による新産業創出のための研究開発事業）

Ｄ．サイバーセキュリティテストベッドの構築事業

技術に関する施策評価の概要

１．施策の目的・政策的位置付けの妥当性

近年クラウドや携帯情報端末の普及が進む一方で、マルウェアの広がりに加え、国境を越えた組織的なサイバー攻撃が増えており、国民生活及び日本経済のセキュリティを確保する観点から、情報セキュリティ対策への需要は近年、非常に高まっている。情報セキュリティ対策は官民が一致協力して対応すべき課題であり、その意味において、中長期的視点に立ち、新たな脅威や既存脅威の巧妙化に対応するための情報セキュリティ技術の研究開発に国が積極的に関わることは極めて重要である。

こうした中、当該事業の目的及び政策的位置付けは、「第 2 次情報セキュリティ基本計画」、「国民を守る情報セキュリティ戦略」に基づき、施策の目的、技術的課題を具体的に整理した上で実施され、さらに社会的ニーズへ適合していることから妥当である。

なお、施策の目的を定める際には、産業・企業の情報セキュリティに関する技術的課題を総合的に検討し、中長期的な「情報セキュリティ研究開発戦略」を構築した上で、事業化に配慮した戦略的な研究開発として推進することが望ましい。また、公募案件として施策を実施していく場合、セキュリティ技術研究開発のポートフォリオを十分意識して、公募案件を設定すべきである。さらに、情報セキュリティ対策は各省庁横断的に重要な課題となっており、今後は各省庁連携のもとに有機的に機能する施策を共同して構築していくべきである。

２．施策の構造及び目的実現の見通しの妥当性

本施策に配置された技術に関する事業は、施策の構造から必要なプロジェクトであり、スケジュール等も妥当である。また、各事業の技術開発のフェーズが異なるが、それぞれのフェーズにおいて妥当な成果が得られ、目標が達成されていることから、一定の成果を上げていると評価できる。

なお、中間審査で成果があがっていない事業を中止した点は高く評価できる一方で、セキュリティ脅威に対する技術開発のポートフォリオに配慮することが望まれる。民間におけるクラウド技術開発は低コスト化競争にならざるを得ないため、国の事業として高信頼

でセキュアなクラウド技術開発を進めるべきである。また、プロジェクトの配置に際しては、それぞれの事業ごとに PDCA サイクルを回し、全プロジェクトの中で適切なポートフォリオが描けているか、さらに注視する必要がある。

３．総合評価

中長期計画である「国民を守る情報セキュリティ戦略」などとの関係が明確であり、いずれの事業も重要な課題に取り組んでいる上に、認証機関の実現や普及に向けた活動のように、国の施策として価値ある波及効果も得られるなど、目的実現の見通しもあり、妥当であると評価する。

なお、施策の構造及び技術に関する事業の配置の検討に際しては、日本の状況から必要な研究開発かのポートフォリオをより明確にするともに、他の関係機関や産官学の連携を意識したものとすべきである、また、認証機関に関わるものや、サイバーセキュリティテストベッドについては、構築だけでなくオペレーションについても支援すべきである。

今後の研究開発の方向等に関する提言

技術開発の事業と、その事業化（例えば認証機関の立ち上げ）など、連携する施策間の関係を明確にした上で、事業の継続性を意識した枠組みを設けるとともに、中長期的な視点からその評価、検証を行うことが重要である。その中で、事業全体としての費用対効果を考えるべきである。

技術に関する施策の実施に際しては、産官学での信頼の輪の確立に配慮することが望ましい。

技術に関する事業

技術に関する事業名	Ａ．新世代情報セキュリティ研究開発事業
上位施策名	企業・個人の情報セキュリティ対策促進事業
担当課	商務情報政策局　情報セキュリティ政策室

事業の目的・概要

情報セキュリティに係る技術の進歩に伴い新たな脅威の出現、既存脅威の一層の巧妙化が続いており、安全・安心なＩＴ社会を確保するためには変化に素早く対応し、かつ先手を打った研究開発を継続的に行っていくことが重要である。

このような観点から、対症療法的な対策だけではなく、中長期的な視点に立って、根本的な問題解決を目指した研究開発を実施する。

なお、技術に関する事業として、評価対象となるプロジェクトは以下の通り。

① 情報家電、スマートグリッド等におけるセキュリティ対策技術の研究開発

ａ 高度電磁波解析技術による LSI のセキュリティ対策に関する研究（平成 22 年度～平成 24 年度）

ｂ 情報家電、スマートグリッド、携帯端末など、非 PC 端末における未知脆弱性の自動検出技術に関する研究（平成 22 年度～平成 24 年度）

② アクセス制御技術の研究開発

ｃ プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究（平成 22 年度～平成 24 年度）

ｄ 撮影による情報漏洩を防止するソリューションの研究開発（平成 22 年度～平成 23 年度）

③ クラウドコンピューティングに関するセキュリティ対策技術の研究開発

ｅ 効率的な鍵管理機能を持つクラウド向け暗号化データ共有システム（平成 22 年度～平成 23 年度）

ｆ クラウドサービスプロバイダとクラウドユーザ企業（法人）における事業継続計画（BCP）の在り方と連携の確保、及びその妥当性検証技術に関する研究（平成 22 年度）

ｇ ＰａａＳ／仮想化環境におけるコンプアライアンス指向データアクセス手法の研究開発（平成 22 年度）

予算額等（委託）　（単位：千円）

開始年度	終了年度	中間評価時期	事後評価時期	事業実施主体
平成 17 年度	平成 24 年度	平成 22 年度	平成 25 年度	民間団体等
H22FY 予算額	H23FY 予算額	H24FY 予算額	総予算額	総執行額
154,930	148,059	110,390	413,378	385,499

※予算額、総予算額、総執行額の欄は、直近 3 年間の額である。

目標・指標及び成果・達成度

(1) 全体目標に対する成果・達成度

個別事業について、所定の研究開発期間にわたって実施された全ての事業が目標を達成している。さらに、これら５事業のうち３事業において事業化が実現し、１事業で派生研究に活用されるなど優れたアウトプットを産み出しており、今後民間産業における幅広いアウトカムが期待できる。

個別要素技術	目標・指標	成果	達成度
高度電磁波解析技術による LSI のセキュリティ対策に関する研究	サイドチャネル攻撃を中心とする電磁波解析実験を通じて、電磁波中の情報取得に特化したマクロ磁界プローブの開発、磁界プローブを LSI 上で移動しながら磁界計測を行う高精度スキャナの開発、高性能磁界プローブを実装した高精度スキャナの有効性を検証する評価実験用セキュリティ回路の開発、高精度磁界スキャナによって計測したデータを解析するツールの開発及び評価実験用セキュリティ回路による有効性の検証等を実施する。	1. 従来比およそ 10 倍の出力振幅を実現する高性能磁界プローブの開発に成功した。 2. 従来比約 10 倍の位置決め精度を有する高精度スキャナを開発し、世界初の 12μm ピッチでの高解像度の画像取得に成功した。	達成
情報家電、スマートグリッド、携帯端末など、非 PC 端末における未知脆弱性の自動検出技術に関する研究	攻撃モデルの変化と攻撃技術の進歩を長期的視点に立って分析し、将来に渡り適用可能である抜本的対策の仕組みとして、情報家電など、非 PC 端末における未知脆弱性の自動検出を行うことが可能なファジング方式のセキュリティ検査ツールの開発・評価を行うとともに、ツールで検査可能な機器と脆弱性の対象範囲の拡張を図る。	1. 情報家電、モバイル端末、スマートメーター等に対応する国産初のファジングツールを開発し、未知脆弱性を発見する成果を得た。 2. EDSA 認証対応の制御システム検査ツールを開発した。	達成
プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究	「個人情報を秘匿化したまま収集、処理、活用する医療・介護連携ネットワーク」を実現するため、医療機関が保管する医療や介護における患者の記録などの機微な個人情報について、秘匿性を保ったまま、有効活用するために必要なプライバシー保護方式及び情報処理方式等の開発、オンラインで患者等から医療、介護等の機微な情報に関するアンケートを行う際に、回答者の匿名性を担保し、アンケート回答に対する心理的な障壁を低減するとともに、有効な統計情報を抽出して活用するために必要な暗号方式の開発及び性能評価等を実施する。	1. 秘密分散保存法による個人情報の統計処理方式を提案し、実験でその優位性を確認した。 2. 論理学暗号を用いた自然言語による秘匿検索技術を開発した。 3. 多変数公開鍵暗号による受信組織対応暗号方式を開発し、派生研究を通じた事業化を実現した。	達成

撮影による情報漏洩を防止するソリューションの研究開発	現状において十分な対策が講じられていない､｢ディスプレイ上に表示されている情報の撮影」による情報漏えいを防止する手段として赤外線を活用するため、透明赤外線光源と赤外線遮断対抗技術の２種類の開発を行う。	1. 波長 880nm で発光する透明蛍光体ガラスの開発に成功した。 2. 画面に設置されたフィルタのカットを検知する透明センサを開発した。 3. 撮影行為を検知する技術開発に成功した。	達成
効率的な鍵管理機能を持つクラウド向け暗号化データ共有システム	「鍵失効機能付き属性ベース暗号方式」の実用化を実現させ、安全・安心なクラウドコンピューティングサービスを提供する基盤を構築するため、鍵管理機能の構築、モデルシステムの構築、モデルシステムの実証実験、普及活動及び意見収集を実施する。	属性ベース暗号を用いたクラウド向け鍵管理システムと携帯端末用クライアントを開発し、実証実験を通じて実用的性能が得られることを確認した。	達成

(2) 目標及び計画の変更の有無

なし

＜共通指標＞

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
39	0	3	0	0	0	0

総合評価概要

中長期的視点に立って、新たな脅威や既存脅威の巧妙化に対応するための情報セキュリティ技術の研究開発が実施され、それぞれが目標を達成し、有用な成果を上げている点は評価できる。

なお、今回はクラウド環境に関するセキュリティ技術開発案件が２つ打ち切りとなったことで、クラウド関連の技術開発がやや遅れる結果となっており、追加の技術開発の公募について検討すべきである。また、公募によるテーマ選定においては、最も優先度の高いセキュリティ課題への取組かどうか、国の施策としての優先度を考慮することが重要である。

今後の研究開発の方向等に関する提言（各事業共通）

中長期的な視点に立ち、IT 技術の進化を先回りした情報セキュリティ技術の研究開発をめざすべきである。個々の要素技術への取組みではなく、多様な要素技術を基盤として統合する際の技術課題については国の施策として取り組む必要がある。

国際的な開発競争が激しくなってきている IoT (Internet of Things)技術、サイバーフィジカルシステム、連携された重要生活機器（車やスマホ）に対する新たな脅威に関して、根本的な問題解決を目指したセキュリティ技術開発や標準化に対する対応を考慮すべきである。

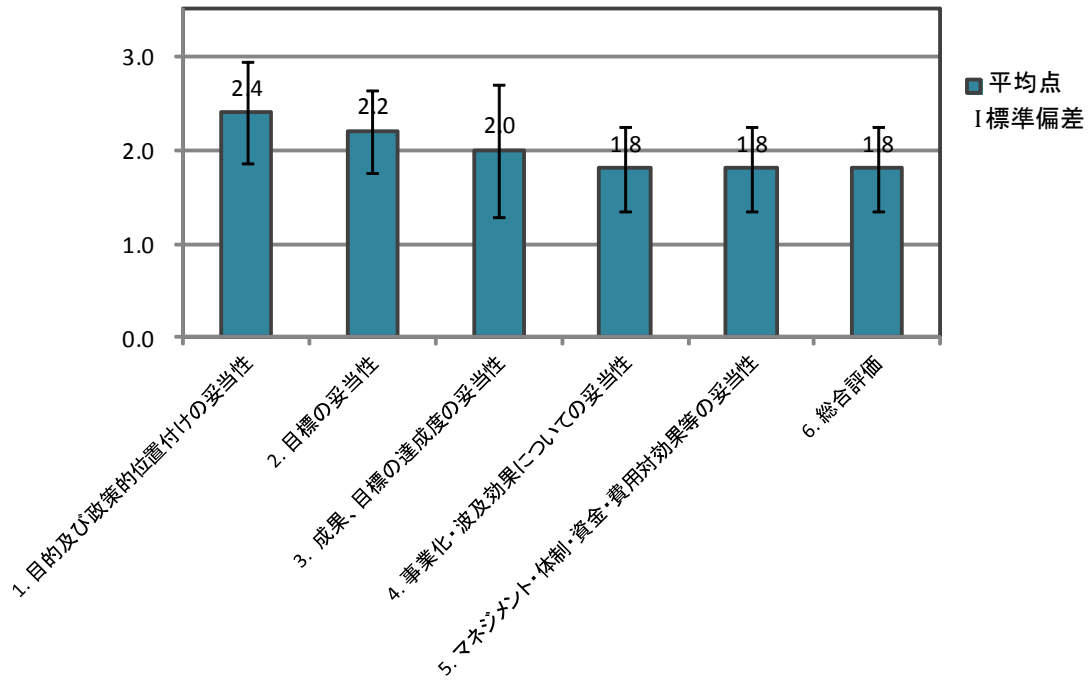
クラウドコンピューティングの高信頼化、セキュア化は、我が国の競争力強化において重要であり、事業として推進すべきである。特に、ビッグデータ向けのクラウド基盤技術は、

そのセキュリティにおいて技術的にも未解決課題が多く、重要な課題である。

評点結果

評 点 法 に よ る 評 価 結 果

評価項目	平均点	標準偏差
1. 目的及び政策的位置付けの妥当性	2.4	0.55
2. 目標の妥当性	2.2	0.45
3. 成果、目標の達成度の妥当性	2.0	0.71
4. 事業化・波及効果についての妥当性	1.8	0.45
5. マネジメント・体制・資金・費用対効果等の妥当性	1.8	0.45
6. 総合評価	1.8	0.45



技術に関する事業名	B．高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業）
上位施策名	企業・個人の情報セキュリティ対策促進事業
担当課	商務情報政策局　情報セキュリティ政策室

事業の目的・概要

システムLSI が使用されているIC カードは、金融や交通等、生活の様々な場において用いられており、既に企業や個人の財産・商取引を支える重要な基盤となっている。しかしながら、当時の国内では、IC カードのセキュリティについての評価体制が構築できていなかった。IC カード等のIT 製品のセキュリティに関する評価は、国際的に国際標準（ISO/IEC 15408）などに基づく評価・認証が行われていることから、海外の関係機関と連携しつつ、日本国内で IC カードのセキュリティ評価を行うことができるよう、必要な体制整備を進めることが重要である。

そこで本事業では、国内外の関係機関と連携しつつ、国内でICカードのセキュリティ評価を行うために必要な技術開発や環境整備等を行う。具体的には、我が国におけるICカードのセキュリティ評価認証体制のすみやかな構築、海外先進事例と等価な評価技術の確立、我が国における評価技術の深化と独自ノウハウの蓄積を図る。

予算額等（委託）　（単位：千円）

開始年度	終了年度	中間評価時期	事後評価時期	事業実施主体
平成 21 年度	平成 23 年度	―	平成 25 年度	電子商取引安全技術研究組合
H21FY 予算額	H22FY 予算額	H23FY 予算額	総予算額	総執行額
255,000	300,000	100,000	655,000	646,044

目標・指標及び成果・達成度

(1) 全体目標に対する成果・達成度

下表の技術開発を通じて我が国国内においてICカードのセキュリティ評価を可能とする体制の構築を実現した。これによる国内 IC カードベンダにおける製品競争力の向上や、海外への評価依頼を通じた情報漏えいリスクの防止等の効果が期待されている。

個別要素技術	目標・指標	成果	達成度
セキュリティ評価を行うために必要な技術の開発	新規・既知の攻撃方法に関する評価手法の開発を実施するとともに、評価ツールの開発を行う。	1. 約 600 件の攻撃事例データベースを作成して欧州 JHAS と共有。 2. 産業技術総合研究所との共同研究成果をもとに電力解析、故障利用解析技術等の研究開発を実施した。	達成

システムLSIセキュリティ評価に関する共同利用設備の整備	システム LSI セキュリティ評価のための共同利用設備の整備を実施する。また、委託事業終了後の共同利用設備の運営に関する検討を行う。	1. 都内に施設を設置し、ASNITE-IT 及び ISO/IEC 17025 の認定を取得。 2. 事業終了後の継承者として、株式会社電子商取引安全技術研究所（現：株式会社 ECSEC Laboratory）を選定。	達成
セキュリティ評価を行うために必要な人材育成	セキュリティ評価を行うために必要な人材の育成を行うとともに、育成した人材による試行評価を実施する。	1. 要員 3 名を対象とした各種演習、評価者育成のための IC チップ脆弱性分析技術指導を実施。 2. 日欧共同評価による二国認証を前提とした試行評価を実施。	達成
セキュリティ評価体制の構築に必要な調査	海外技術動向調査を行うとともに、IC カードを利用するユーザ側のセキュリティ要求仕様ならびにチップセキュリティ評価のための手順に関するの調査を実施する。	1. 海外の企業訪問、専門家会合参加等を通じてセキュリティ評価に関する情報収集・交換を実施。 2. 個人認証システム、決裁端末システム、マルチアプリケーションシステムについてセキュリティ要求仕様に関する調査を実施。 3. チップセキュリティ評価のための手順についての調査を実施。	達成

(2) 目標及び計画の変更の有無

なし

＜共通指標＞

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
0	0	0	0	0	0	0

総合評価概要

国民の生活にとって必需品となっているICカード等のIT製品のセキュリティを評価する体制整備が遅れている中、国内外の関係機関と連携し、IC カードのセキュリティ評価に資する技術開発、環境・体制の整備を行い、国内での評価が可能となったことは評価できる。本事業は国際競争戦略の観点から重要な取り組みであり、費用対効果は、関連産業全体の競争力強化へのインパクトから考えるべきである。

なお、本事業で構築した評価環境を持続的に運用するための人材育成方策として、育成した人材の定着と継続的なキャリアサイクルを回すための活動を明確にすることが重要である。

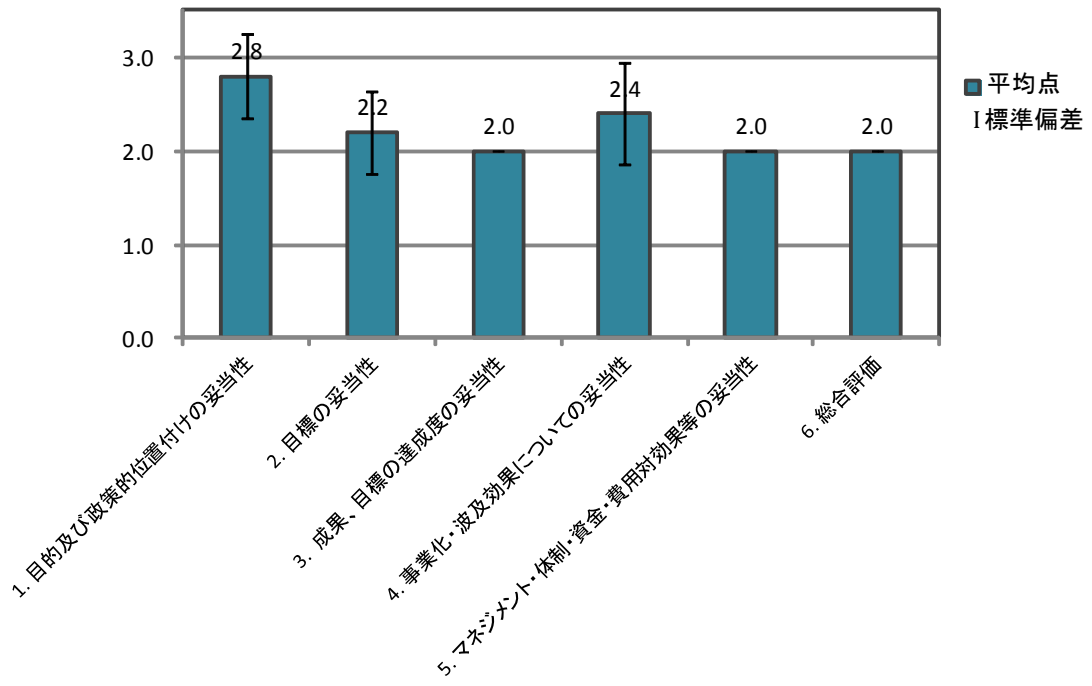
今後の研究開発の方向等に関する提言

（Ａ．新世代情報セキュリティ研究開発事業を参照）

評点結果

評 点 法 に よ る 評 価 結 果

評価項目	平均点	標準偏差
1. 目的及び政策的位置付けの妥当性	2.8	0.45
2. 目標の妥当性	2.2	0.45
3. 成果、目標の達成度の妥当性	2.0	0.00
4. 事業化・波及効果についての妥当性	2.4	0.55
5. マネジメント・体制・資金・費用対効果等の妥当性	2.0	0.00
6. 総合評価	2.0	0.00



技術に関する事業名	C．暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発
上位施策名	企業・個人の情報セキュリティ対策促進事業
担当課	商務情報政策局　情報セキュリティ政策室

事業の目的・概要

暗号製品の実装技術は公開されることがほとんどないため、実装性能評価においても評価手法により大きな差が出たとしても第三者検証ができない、また物理的安全性評価においても評価手法の標準化と公正な評価が難しいという問題がある。これに対して、ハードウェア設計・解析の高い技術力を背景としながらも、極めて高い専門性を有する一部の研究者やエンジニアだけが利用できる特殊な環境ではなく、評価制度として第三者が実施可能な統合システムを構築し、かつ民間の活力を利用したビジネスとして成立させるレベルにまで落とし込むことが大きな課題である。

本研究開発は、このような背景にあって、暗号アルゴリズムの危殆化に伴う標準アルゴリズムの選定作業等において、ハードウェアの実装性能評価及び物理的な安全性の評価を統合的に行うシステムを開発し、さらに LSI 解析技術の進歩による将来的な脆弱性の検討を行い、これらの技術開発の成果を、ISO/IEC 19790/24759 に則した JCMVP(Japan Cryptographic Module Validation Program)等の暗号モジュール試験認証制度や、ISO/IEC 15408 Common Criteria における IC カード評価等にインプットすることで、国際標準規格の改定に貢献することと、国内企業の技術の底上げと国際競争力の向上に貢献することを目的とする。

予算額等（委託）　（単位：千円）

開始年度	終了年度	中間評価時期	事後評価時期	事業実施主体
平成 23 年度	平成 25 年度	―	平成 25 年度	ケイレックス･テクノロジー株式会社
H23FY 予算額	H24FY 予算額	H25FY 予算額	総予算額	総執行額
119,749	125,000	61,502	306,251	243,687

※総執行額は、実施中につき平成 25 年度の執行額を含まない。

目標・指標及び成果・達成度

(1) 全体目標に対する成果・達成度

暗号アルゴリズムの物理的安全性評価に必要な評価環境を開発し、計画に基づいて順調な成果が得られた。成果である統合ハードウェア評価プラットフォームを研究者などが利用可能な場所への設置が実現されることにより、国内企業、大学等の研究団体の技術の底上げと国際競争力の向上への貢献が期待できるほか、レーザー照射装置、電磁波装置に関する成果についても、より安価な提供を通じた攻撃手法の研究促進への貢献が期待できる。

個別要素技術	目標・指標	成果	達成度
暗号ハードウェア実装性能評価ツールの開発	暗号アルゴリズムや構成法そして実装プラットフォームに対する各種性能指標の比較を、表やグラフで自動的に表示する評価ツールを開発する。	1. 暗号モジュールとデバイスの複数の組み合わせから性能レポートを出力する性能評価を自動化。 2. 評価レポートから暗号モジュールの回路規模、処理速度などを可視化するツールを開発。	達成
サイドチャネル攻撃耐性評価ツールの開発	各種サイドチャネル攻撃に対する網羅的な評価ツールを開発する。	1. 各種サイドチャネル攻撃の耐性評価のためのデータ収集・解析、及び評価結果の表示等、各種機能を統括するツールを開発。 2. サイドチャネル攻撃の耐性評価に適した非接触 IC カード評価プラットフォームを設計し、解析実験を実施。	達成
フォールト攻撃耐性評価ツール及び試験装置の開発	クロックや電源にグリッチを挿入してエラーを発生させる試験環境を構築する。	1. クロック信号、リセット信号、電源それぞれに非常に細いパルスを混入するグリッチ機能を開発。 2. 開発した環境を用いた評価実験を実施するとともに、検証のため解析プログラムを開発。	達成
侵襲攻撃耐性評価環境の構築	パッケージを開封して LSI 内部の動作を直接操作する侵襲攻撃評価を行う環境を構築する。	1. 外乱誘発装置としてレーザー照射装置と電磁界照射装置を開発。 2. LSI の CAD データを用いて照射座標を制御したり、フォールトの発生状況を描画する CAD ナビゲーションシステムを開発。	達成
集積回路解析技術によるＬＳＩ内部動作解析及び先端技術調査	先端の集積回路解析装置を用いて LSI の内部動作解析を実施し、LSI の局所的な動作情報を取得する技術の研究開発を行う。	1. 暗号 LSI、接触型 IC カード内のチップに対して、電子線プローブによる内部信号の観測を実施。 2. 接触型 IC カード内のチップに対して発光解析を行い、電子線プローブでの観測結果とよい対応関係を示していることを確認。	達成

統合ハードウェア評価プラットフォームの構築	これまでの研究開発成果を統合ハードウェア評価プラットフォームに集約する。	1. これまでの評価技術の成果の商品化を想定したパッケージングを実施。 2. ひとつの評価対象に対して、サイドチャネル攻撃、フォールト攻撃および侵襲攻撃の解析評価を一貫して行うことができるツールを開発。	達成

(2) 目標及び計画の変更の有無

なし

＜共通指標＞

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
3	0	0	0	0	0	0

総合評価概要

本事業は暗号の実装攻撃対策技術として重要な取り組みであり、開発成果を基に「統合ハードウェア評価プラットフォーム」が構築され、設定された開発目標を達成するとともに、実用化に向けた準備が進められていること、及び国内企業等の技術の底上げと国際競争力向上への貢献が期待できる点などから評価できる。

なお、攻撃手法や評価ノウハウの一部は、悪意ある利用につながらないように、適切に管理されるべきものである。事業全体としての管理や運用方針を明確にすべきである。

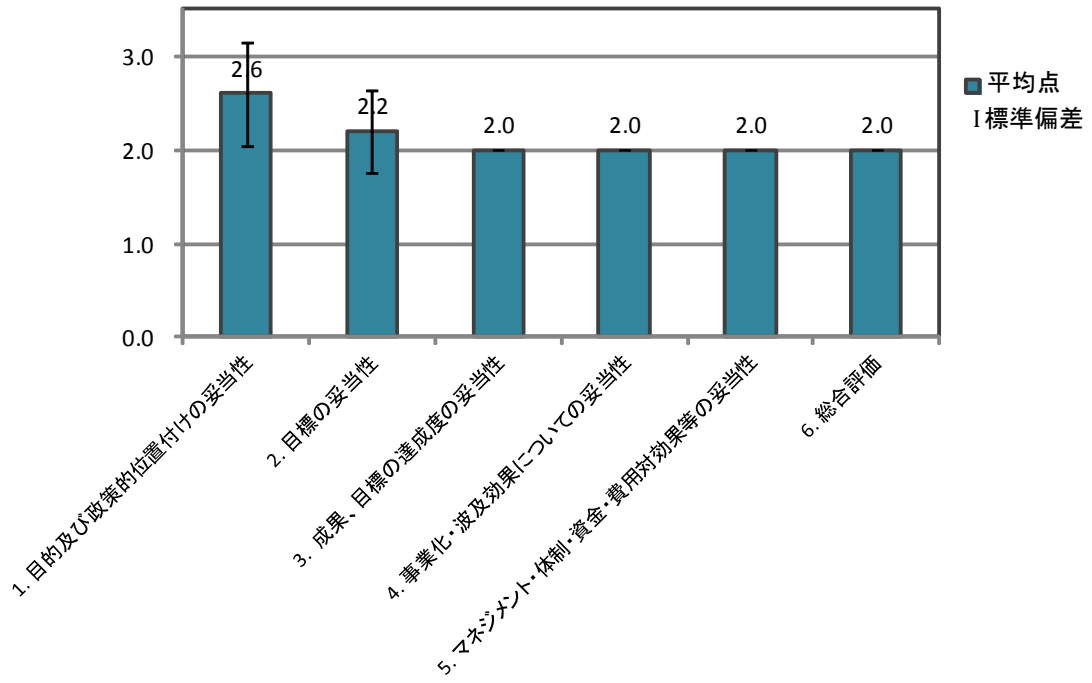
今後の研究開発の方向等に関する提言

（A．新世代情報セキュリティ研究開発事業を参照）

評点結果

評 点 法 に よ る 評 価 結 果

評価項目	平均点	標準偏差
1. 目的及び政策的位置付けの妥当性	2.6	0.55
2. 目標の妥当性	2.2	0.45
3. 成果、目標の達成度の妥当性	2.0	0.00
4. 事業化・波及効果についての妥当性	2.0	0.00
5. マネジメント・体制・資金・費用対効果等の妥当性	2.0	0.00
6. 総合評価	2.0	0.00



技術に関する事業名	D．サイバーセキュリティテストベッドの構築
上位施策名	ＩＴ融合による新産業創出のための研究開発事業
担当課	商務情報政策局　情報セキュリティ政策室

事業の目的・概要

電力・ガス・ビル等の社会インフラや工場のプラントの「制御システム」は、サイバー攻撃の対象となりづらいとされていた以前の状況から一変し、現在では重大なインシデント源となると考えられている。制御システムの障害は、インフラのサービスレベル低下やプラント操業停止等に直結するため、制御システムのセキュリティ強化やセキュリティ強度の検証が急がれている。

本事業では、制御システムを高セキュア化するための設計方法、セキュリティ検証方法及び第三者による評価認証方法の研究開発、制御システムのセキュリティの国際標準化に係る活動及び被災地における評価認証・普及啓発・人材育成を行うための環境整備に対して補助を実施し、これらを通じて、被災地におけるスマートグリッド導入促進、重要インフラ等のセキュリティ向上、インフラシステムの輸出強化を目的とする。

予算額等（補助）　（単位：千円）

開始年度	終了年度	中間評価時期	事後評価時期	事業実施主体
平成 23 年度	平成 23 年度	―	平成 25 年度	技術研究組合制御システムセキュリティセンター
H23FY 予算額	―	―	総予算額	総執行額
2,007,990	―	―	2,007,990	1,986,422

目標・指標及び成果・達成度

(1) 全体目標に対する成果・達成度

本事業では、下表に示すように所定の目標を達成している。この成果をもとに、技術研究組合制御システムセキュリティセンター（CSSC）は、本事業で構築したサイバーセキュリティテストベッド（CSS-Base6）を設置する「みやぎ復興パーク」内の CSSC 東北多賀城本部に主要な機能を移した。東北多賀城本部では、CSSC-Base6 を活用した研究開発を継続し、組合員の研究成果を活用した製品化が進められている。また、セキュリティの認証に必要な試験装置を CSSC-Base6 施設内に設置し、国際基準に準拠した評価認証の事業化を進めている。普及啓発・人材育成の活動も活発化し、CSS-Base6 の模擬プラントシステムを利用した事業の検討を行っている。こうした取組の結果、技術研究組合に加入する事業者が急拡大するなどの波及効果も得られている。

個別要素技術	目標・指標	成果	達成度
制御システムのためのサイバーセキュリティテストベッド構築技術	本事業では、制御システムのセキュリティに関する次の活動を行うための施設・設備の構築に関する研究開発を行い、以後の活動に必要な基盤環境を整備する：制御システムを高セキュア化するための設計方法の研究開発、セキュリティ検証方法の研究開発、第三者による評価認証方法の研究開発、及び被災地における評価認証・普及啓発・人材育成。	1. みやぎ復興パーク（多賀城市）に、国内唯一のサイバーセキュリティテストベッド（CSS-Base6）を構築した 2. 産業用制御システムの特徴的な機能を模擬システムとして実現するための研究開発を行い、５種（化学、スマートシティ、ビル制御、組立、下水・排水）の模擬プラントシステムをCSS-Base6 に設置した。 3. インシデントの再現、電力・ガス等インフラ事業者向けのサイバー演習、制御システムのセキュリティの評価・検証が実施できる普及啓発、人材育成及び評価・認証のための環境を整備した。	達成

(2) 目標及び計画の変更の有無

なし

＜共通指標＞

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
8	0	3	0	0	0	0

総合評価概要

サイバーセキュリティテストベッドの構築により、制御システム系に対するセキュリティ向上を実現するための設計方法、検証方法、第三者による評価認証方法の研究開発、ならびに被災地における評価認証、普及啓発、人材育成を実現した点が評価できる。我が国の制御システムセキュリティ拠点として重要であり、産業インフラや都市インフラを担う制御システムのセキュリティの重要性に対応するタイミングとしても適切である。また、認証機関の見込みがついたことの価値は高い。

なお、制御システムセキュリティの技術や運用体制に関わる人材育成については、更なる取組みが必要である。本センターを活用しながら、関連する企業等と共同で、人材育成を促進できる事業を国の施策として立ち上げるべきである。単年度ではなく、オペレーションの軌道がのるまでの数年は支援すべき事業である。

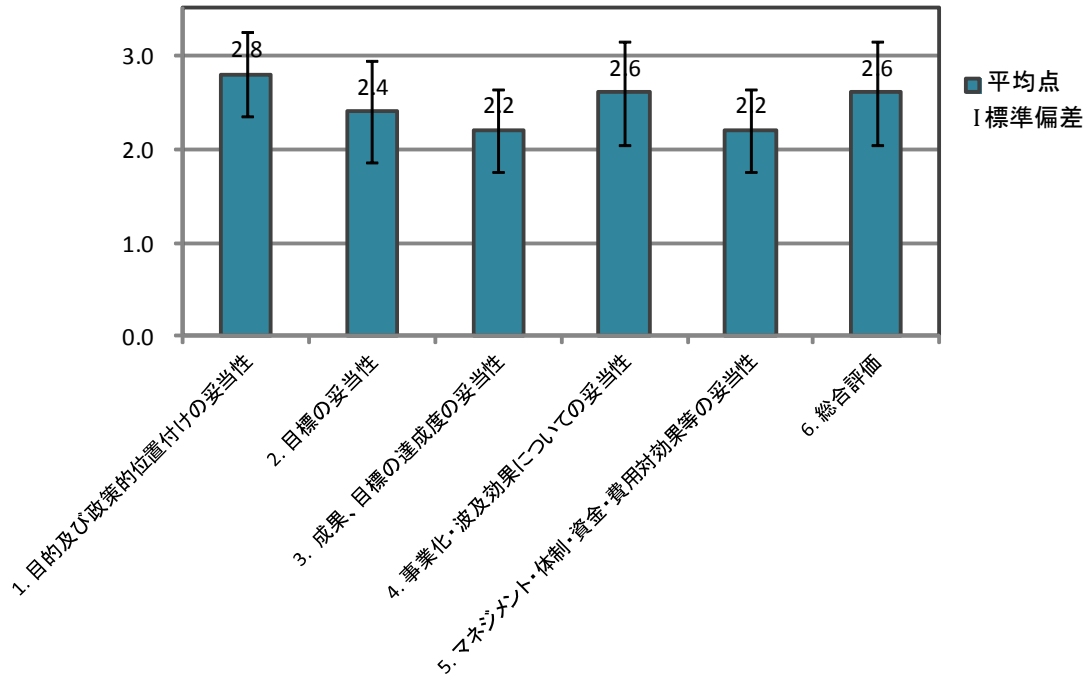
今後の研究開発の方向等に関する提言

（Ａ．新世代情報セキュリティ研究開発事業を参照）

評点結果

評 点 法 に よ る 評 価 結 果

評価項目	平均点	標準偏差
1. 目的及び政策的位置付けの妥当性	2.8	0.45
2. 目標の妥当性	2.4	0.55
3. 成果、目標の達成度の妥当性	2.2	0.45
4. 事業化・波及効果についての妥当性	2.6	0.55
5. マネジメント・体制・資金・費用対効果等の妥当性	2.2	0.45
6. 総合評価	2.6	0.55



第１章　評価の実施方法

第１章　評価の実施方法

本プロジェクト評価は、「経済産業省技術評価指針」（平成２１年３月３１日改定、以下「評価指針」という。）及び第２５回産業構造審議会産業術部会評価小委員会（平成２１年１月２８日）において審議・了承された「技術に関する施策の評価」に基づき、実施した。

１．評価の目的

以下の（１）～（４）を目的として評価を実施した。

(1) より良い政策・施策への反映

評価を適切かつ公正に行うことにより、研究者の創造性が十分に発揮されるような、柔軟かつ競争的で開かれた研究開発環境の創出など、より良い政策・施策の形成等につなげること。

(2) より効率的・効果的な研究開発の実施

評価を支援的に行うことにより、研究開発の前進や質の向上、独創的で有望な優れた研究開発や研究者の発掘、研究者の意欲の向上など、研究開発を効果的・効率的に推進すること。

(3) 国民への技術に関する施策・事業の開示

高度かつ専門的な内容を含む技術に関する施策・事業の意義や内容について、一般国民にわかりやすく開示すること。

(4) 資源の重点的・効率的配分への反映

評価の結果を技術に関する施策・事業の継続、拡大・縮小・中止など資源の配分へ反映させることにより資源の重点化及び効率化を促進すること。また、研究開発をその評価の結果に基づく適切な資源配分等通じて次の段階に連続してつなげることなどにより、研究開発成果の国民・社会への還元の効率化・迅速化に資すること

また、評価の実施に当たっては以下の①～④を基本理念として実施した。

① 透明性の確保

推進課、主管課及び研究開発機関においては、積極的に成果を公開し、その内容について広く有識者等の意見を聴くこと。評価事務局においては、透明で公正な評価システムの形成、定着を図るため、評価手続、評価項目・評価基準を含めた評価システム全般についてあらかじめ明確に定め、これを公開することにより、評価システム自体を誰にも分かるものとするとともに、評価結果のみならず評価の過程についても可能な限り公開すること

② 中立性の確保

評価を行う場合には、被評価者に直接利害を有しない中立的な者である外部評価の導入等により、中立性の確保に努めること。

③ 継続性の確保

技術に関する施策・事業においては、個々の評価がそれ自体意義を持つだけではなく、評価とそれを反映した技術に関する施策・事業の推進というプロセスを繰り返していく時系列のつながりにも意義がある。したがって、推進課及び主管課にとって評価結果を後の技術に関する施策・事業の企画立案等に反映させる際に有用な知見を抽出し、継続性のある評価方法で評価を行うこと。

④ 実効性の確保

政策目的に照らし、効果的な技術に関する施策・事業が行われているか判断するための効率的評価が行われるよう、明確で実効性のある評価システムを確立・維持するとともに、技術に関する施策・事業の運営に支障が生じたり、評価者及び被評価者双方に過重な負担をかけることのない費用対効果の高い評価を行うこと。

２．評価者

評価を実施するにあたり、評価指針に定められた「評価を行う場合には、被評価者に直接利害を有しない中立的な者である外部評価者の導入等により、中立性の確保に努めること」との規定に基づき、外部の有識者・専門家で構成する検討会を設置し、評価を行うこととした。

これに基づき、評価検討会を設置し、技術に関する施策、技術に関する事業（プロジェクト等）の目的や研究内容に即した専門家や経済・社会ニーズについて指摘できる有識者等から評価検討会委員名簿にある５名が選任された。

なお、本評価検討会の事務局については、指針に基づき経済産業省商務情報政策局情報セキュリティ政策室が担当した。

３．評価対象

技術に関する施策「情報セキュリティ分野」

技術に関する事業

(1) 技術的情報セキュリティ対策推進事業

Ａ　新世代情報セキュリティ研究開発事業

①情報家電、スマートグリッド等におけるセキュリティ対策技術の研究開発

ａ 高度電磁波解析技術によるLSIのセキュリティ対策に関する研究

ｂ 情報家電、スマートグリッド、携帯端末など、非PC端末における未知脆弱性の自動検出技術に関する研究

②アクセス制御技術の研究開発

ｃ プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究

ｄ 撮影による情報漏洩を防止するソリューションの研究開発

③クラウドコンピューティングに関するセキュリティ対策技術の研究開発

ｅ 効率的な鍵管理機能を持つクラウド向け暗号化データ共有システム

ｆ クラウドサービスプロバイダとクラウドユーザ企業（法人）における事業継続計画（BCP）の在り方と連携の確保、及びその妥当性検証技術に関する研究

ｇ ＰａａＳ／仮想化環境におけるコンプアライアンス指向データアクセス手法の研究開発

Ｂ　高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業）

Ｃ　暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発

(2) ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築事業）

４．評価方法

第１回評価検討会においては、担当課、研究開発実施者からの資料提供、説明及び質疑応答が行われた。

第２回評価検討会においては、それらを踏まえて、第２５回産業構造審議会産業技術部会評価小委員会（平成２１年１月）において審議・了承された「技術に関する施策」「技術に関する事業（プロジェクト）」の評価項目に従い評価を実施し、今後の研究開発の方向等に関する提言をいただいた。技術に関する事業評価については、加えて３段階評点法により評価を行い、評価報告書（案）を審議・確定した。

また、評価の透明性の確保の観点から、知的財産保護、個人情報で支障が生じると認められる場合等を除き、評価検討会を公開として実施した。

５．評価項目

【技術に関する施策】

〇施策の目的・政策的位置付けの妥当性

・施策の目的の妥当性

・施策の政策的位置付けの妥当性

・国の施策としての妥当性、国の関与が必要とされる施策か。

〇施策の構造及び目的実現見通しの妥当性

・現時点において得られた成果は妥当か

・施策の目的を実現するために技術に関する事業が適切に配置されているか。

〇総合評価

【技術に関する事業】

〇事業の目的・政策的位置付けの妥当性

・事業の目的は妥当で、政策的位置付けは明確か。

・国の事業として妥当であるか、国の関与が必要とされる事業か。

〇研究開発等の目標の妥当性

・研究開発等の目標は適切かつ妥当か。

〇成果、目標の達成度の妥当性

・成果は妥当か。

・目標の達成度は妥当か。

〇事業化、波及効果についての妥当性

・事業化については妥当か。

・波及効果は妥当か。

〇研究開発マネジメント・体制・資金・費用対効果等の妥当性

・研究開発計画は適切かつ妥当か。

・研究開発実施者の実施体制・運営は適切かつ妥当か。

・資金配分は妥当か

・費用対効果は妥当か。

・変化への対応は妥当か。

〇総合評価

第２章　技術に関する施策の概要

第２章　技術に関する施策の概要

１．施策の目的・政策的位置付け

１－１　施策の目的

IT が経済社会に浸透する中で、安全・安心な国民生活、企業活動のためには、情報セキュリティの確保が不可欠である。情報処理基盤の安全性を確保するための対策、企業・個人における情報セキュリティ対策を促進することを通じて、第２次情報セキュリティ基本計画（平成２１年２月情報セキュリティ政策会議決定）における「『IT を安心して利用できる環境』の構築」及び国民を守る情報セキュリティ戦略（平成２２年５月情報セキュリティ政策会議決定）における「世界最先端の『情報セキュリティ先進国』」を目指す。

１－２　政策的位置付け

・　政府の情報セキュリティ対策に関する戦略である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（議長：官房長官））において（図１－１及び図１－２）、示されているように、安全・安心な国民生活を実現させるため、①マルウェア対策の充実・強化、②普及啓発活動の充実強化、③情報セキュリティガバナンスの確立、④情報セキュリティ関連の研究開発の戦略的推進等が位置づけられている。
・　これらの事項は、図１－３にも示されるように、当施策においても明確に位置づけており、直近の政府全体の取組とも合致している。

図１－１　国民を守る情報セキュリティ戦略概要

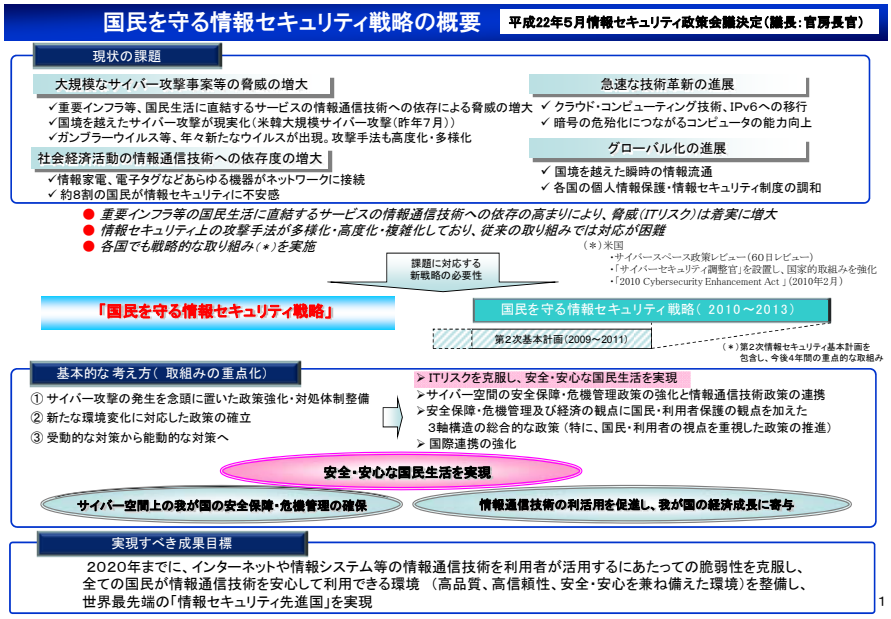


図１－２　国民を守る情報セキュリティ戦略の具体的な取組

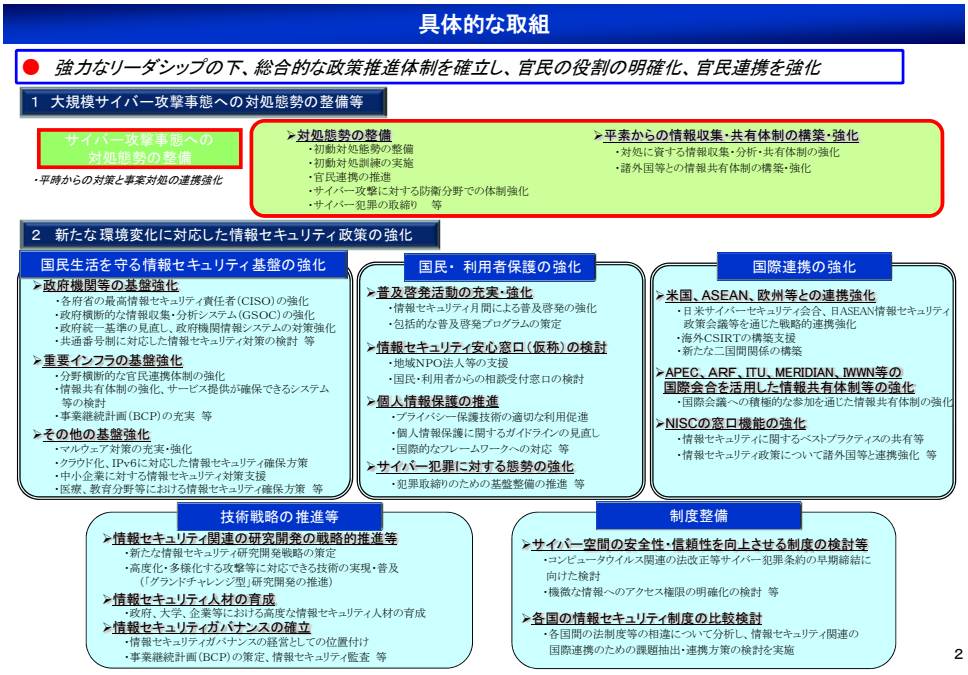


図１－３　情報セキュリティ対策の体系図

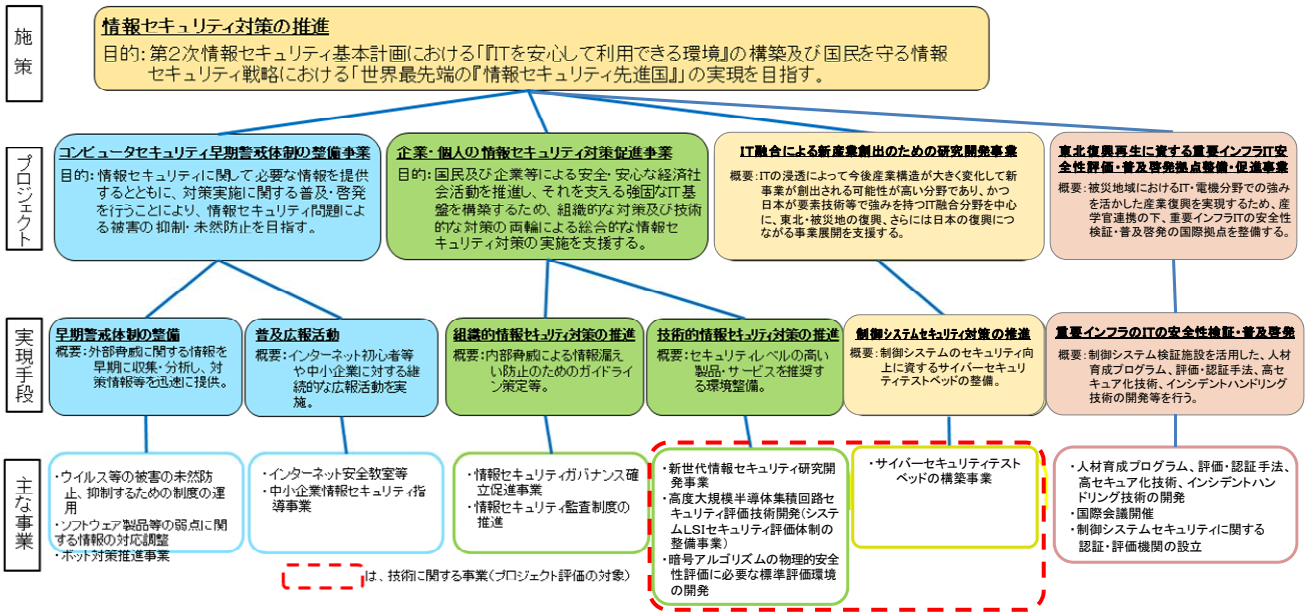
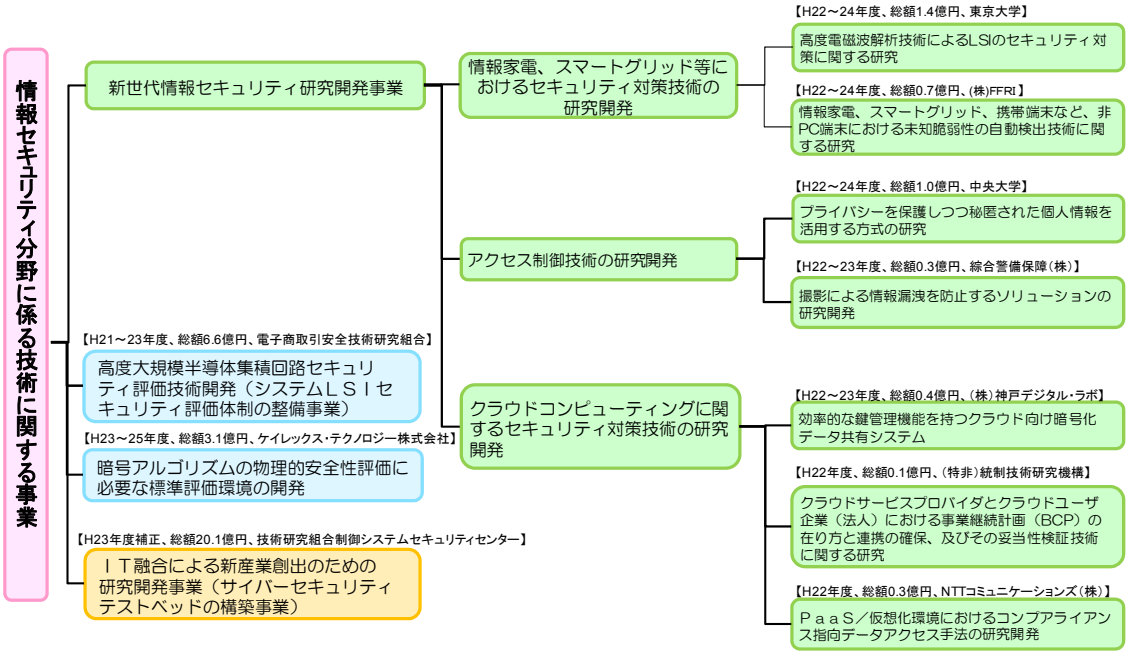


図１－４　情報セキュリティ分野に係る技術に関する事業



１－３　国の関与の必要性

情報セキュリティ対策として、以下の４事業・６項目を実施。

（１）コンピュータセキュリティ早期警戒体制の整備事業
　① 早期警戒体制の整備
　② 普及啓発事業

（２）企業・個人の情報セキュリティ対策促進事業
　① 組織的情報セキュリティ対策の推進
　② 技術的情報セキュリティ対策の推進

（３）ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築）

（４）東北復興再生に資する重要インフラＩＴ安全性評価・普及啓発拠点整備・促進事業

（１）コンピュータセキュリティ早期警戒体制の整備事業

本事業は、コンピュータウイルスによる被害やソフトウェア製品のぜい弱性情報について、関係機関（国際連携を含み）と情報共有するとともに、対応策を調整し、対策情報を公表することで、被害の拡大や未然防止を図っている。また、インターネット初心者等や中小企業を対象とした情報セキュリティレベルの向上を目指す普及・啓発を実施している。

脆弱性等への対応は製品開発者の利益に直結しない上に、そもそも製品開発者が脆弱性等に気付きにくいこと等から、本分野については民間の自主的な取組だけでは十分な効果が期待できない。情報セキュリティ対策を民間の自主的な対応のみに委ねた場合、民間における情報セキュリティ対策は不十分なものとなり、結果として、経済社会活動の基盤となっているIT 全体の安全性・信頼性が大きく損なわれ、我が国経済社会活動全体にも及ぼしうることから、情報システムの安全性の確保を担当する経済産業省が実施する必要がある。

（２）企業・個人の情報セキュリティ対策促進事業

①　組織的情報セキュリティ対策の推進

本事業は、企業からの機密情報の漏洩等を防止するため、情報セキュリティポリシーの策定支援や情報セキュリティ監査の実施を支援するための環境整備（ガイドラインの策定等）を実施している。

企業の内部統制に係る情報セキュリティ対策は、その体制構築、展開、国際標準化等を推進しているところであり、これらの環境整備については、上記の対策を所掌する経済産業省が主導して実施していく必要がある。

②　技術的情報セキュリティ対策の推進

本事業は、新たな脅威等への対応や情報セキュリティ対策の環境を整備するための研究開発等を実施している。具体的には、ＩＴ製品のセキュリティ評価・認証基盤の整備、電子署名及び認証業務に関する法律に基づく調査・相談業務等、新たな脅威に対応するための技術開発を実施している。

IT 製品の安全性評価については、国際的な相互認証制度があり、各国政府等によって実施されている。我が国においては、経済産業省が政策立案・実施者として本制度に加盟しており、政策立案・実施者である経済産業省が、評価を行える環境整備を実施する必要がある。

また、電子署名の利用促進は、電子署名及び認証業務に関する法律に基づき、国が実施することとされていることから、これを実施する必要がある。

さらに、新たな脅威に対応するための技術開発については、国の情報セキュリティ政策を踏まえた情報セキュリティ対策として、共通に利用できるような標準化や規格化等を目指している。こういった環境整備は、我が国産業のセキュリティ技術の向上とそれによる安全・安心な国民生活の実現のため、国が実施すべき事項である。

（３）ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築）

本事業は、ＩＴの浸透によって今後産業構造が大きく変化して新事業が創出される可能性が高い分野であり、かつ日本が要素技術等で強みを持つＩＴ融合分野を中心に、東北・被災地の復興、さらには日本の復興につながる事業展開を支援する。

本事業は、災害被害により経済活動が停滞し、民間による積極的な投資が望めない状況にある被災地において、今後の産業活動の基盤となるサイバーセキュリティテストベッドの環境整備を行うものであり、全国的な調整や海外政府との調整等が必要となることから、国が実施すべき事項である。

（４）東北復興再生に資する重要インフラＩＴ安全性評価・普及啓発拠点整備・促進事業

本事業は、被災地域におけるＩＴ・電機分野での強みを活かした産業復興を実現するため、産学官連携の下、重要インフラＩＴの安全性検証・普及啓発の国際拠点を整備する。

本事業は、（３）と同様、災害被害により経済活動が停滞し、民間による積極的な投資が望めない状況にある被災地において、制御システム検証施設を活用した、人材育成プログラム、評価・認証手法、高セキュア化技術、インシデントハンドリング技術の開発等を行うものであり、全国的な調整

や海外政府との調整等が必要となることから、国が実施すべき事項である。

２．施策の構造及び目的実現の見通し

２－１　得られた成果

（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－H25）

①早期警戒体制の整備

【アウトプット】

コンピュータウイルス等による被害やソフトウェア製品のぜい弱性情報について、関係機関（国際連携を含み）と情報共有するとともに、対応策を調整し、対策情報を公表することで、被害の未然防止や軽減対策を実施。具体的には、以下の通り。

・コンピュータウイルス・不正アクセス等によるインシデント対応
・ソフトウェア製品のぜい弱性情報についての国際調整・公表
・国内外の企業・組織内のコンピュータインシデント対応チーム（CSIRT）の構築支援

【アウトプットからアウトカムへの展開】

コンピュータウイルス被害やソフトウェア製品のぜい弱性情報に対応するための早期警戒体制を整備。

【アウトカム】

コンピュータウイルス等による被害やソフトウェア製品のぜい弱性情報を狙ったサイバー攻撃による被害の未然防止や軽減。

②普及啓発事業

【アウトプット】

インターネット初心者や中小企業等の情報セキュリティリテラシーの向上を目的とした普及啓発活動を実施。具体的には以下の通り。

・インターネット初心者等を対象としたインターネット安全教室の開催。
・中小企業の経営者やシステム管理者を指導する指導者を育成する中小企業向け指導者育成セミナーの開催。

【アウトプットからアウトカムへの展開】

普及啓発活動により、インターネット初心者や中小企業等の情報セキュリティリテラシーの向上。

【アウトカム】

安心なインターネットの利用や適切な情報セキュリティ対策の確保。

（２）企業・個人の情報セキュリティ対策促進事業（H17－H25）

①組織的情報セキュリティ対策の推進

【アウトプット】

企業からの機密情報の漏洩等を防止するためのガイドラインの策定・推進を実施。具体的には以下の通り。

・情報セキュリティガバナンス導入ガイドラインの策定

・アウトソーシングに関する情報セキュリティ対策ガイダンスの策定

・情報セキュリティ監査の推進

【アウトプットからアウトカムへの展開】

ガイドライン等を策定することにより、企業が情報セキュリティ対策を実施するための環境を整備。

【アウトカム】

企業における組織的な情報セキュリティ対策の確保

②技術的情報セキュリティ対策の推進

【アウトプット】

新たな脅威等への対応や情報セキュリティの環境を整備するための研究開発等を実施している。具体的には以下の通り。

・ＩＴ製品のセキュリティ評価・認証基盤の整備

・電子認証基盤の構築

・新たな脅威に対応するための技術開発

【アウトプットからアウトカムへの展開】

情報セキュリティ対策を実施する上での基盤となる技術開発等を実施し、情報セキュリティの技術的な対策を推進。

【アウトカム】

情報セキュリティ対策が施された製品の利用による技術的な情報セキュリティ対策の確保。

（３）ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築）（H23）

【アウトプット】

制御システムのセキュリティ向上に資するサイバーセキュリティテストベッドを整備する。

【アウトプットからアウトカムへの展開】

整備されたサイバーセキュリティテストベッドに設けられた模擬プラントを用いて、重要インフラ事業者を対象とするサイバーセキュリティ演習を実施するとともに、制御システムの情報セキュリティ対策のための製品開発等を実施する。

【アウトカム】

重要インフラ事業者における情報セキュリティ対策の充実を通じた、

サイバー攻撃への対処能力の向上、ならびに国内情報セキュリティ産業における競争力の向上。

（４）東北復興再生に資する重要インフラ IT 安全性評価・普及啓発拠点整備・促進事業（H25－）

【アウトプット】

制御システム検証施設を活用して、以下の施策を実施する。

・人材育成プログラム、評価・認証手法、高セキュア化技術、インシデントハンドリング技術の開発
・国際会議開催
・制御システムセキュリティに関する認証・評価機関の設立

【アウトプットからアウトカムへの展開】

制御システムを対象とする情報セキュリティに関する高いスキルを持った人材を輩出するとともに、施設を活用する事業者における制御システムの高セキュア化に関する技術力の向上、評価・認証事業を通じた高い性能を備えた製品の普及を促進する。

【アウトカム】

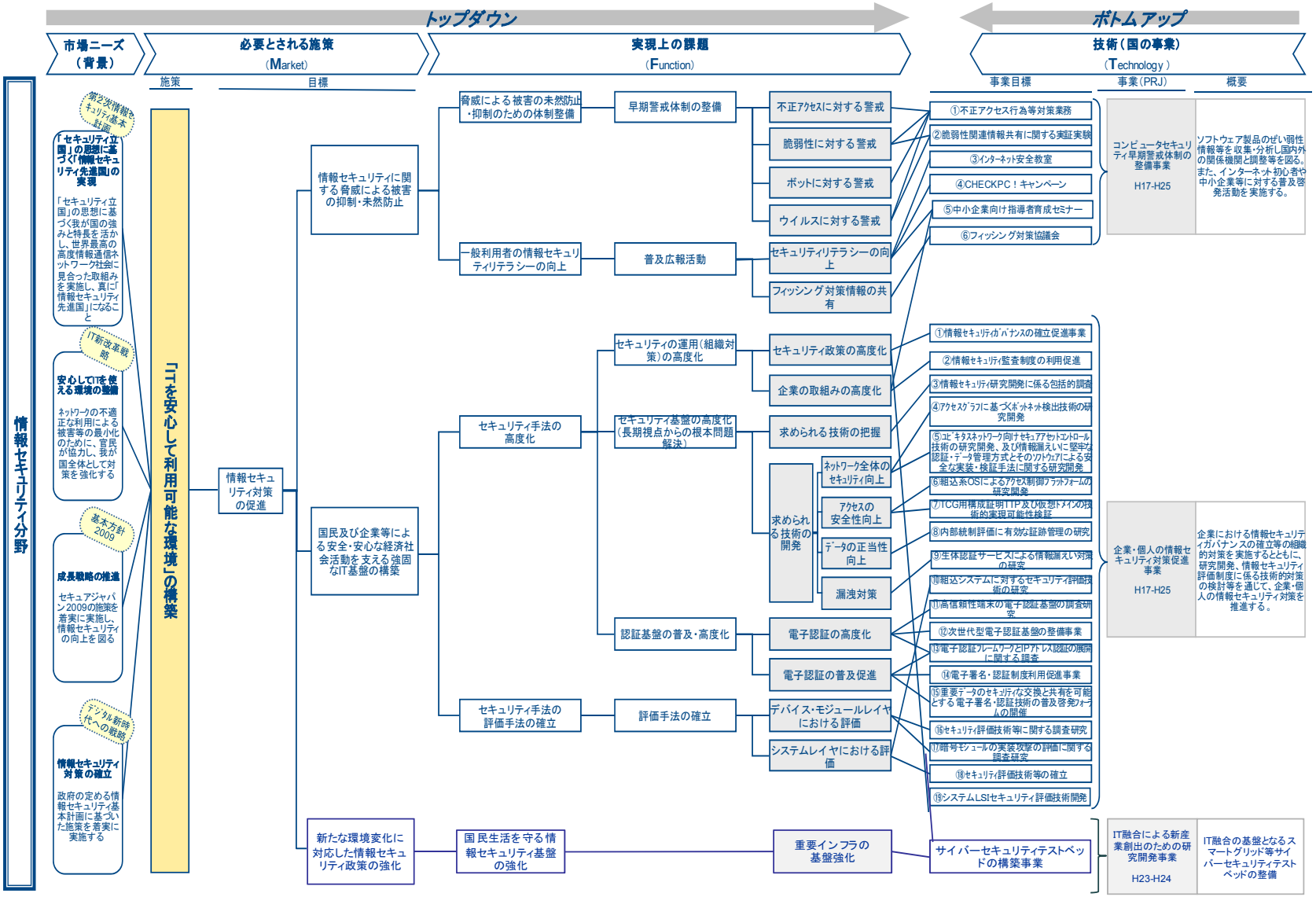
制御システム分野における情報セキュリティ対策の充実による、製造業や重要インフラ分野におけるサイバー攻撃への対処能力の向上、ならびに制御システムセキュリティに関する市場創出。

２－２　施策の構造

別紙２－２－１～２－２－２参照

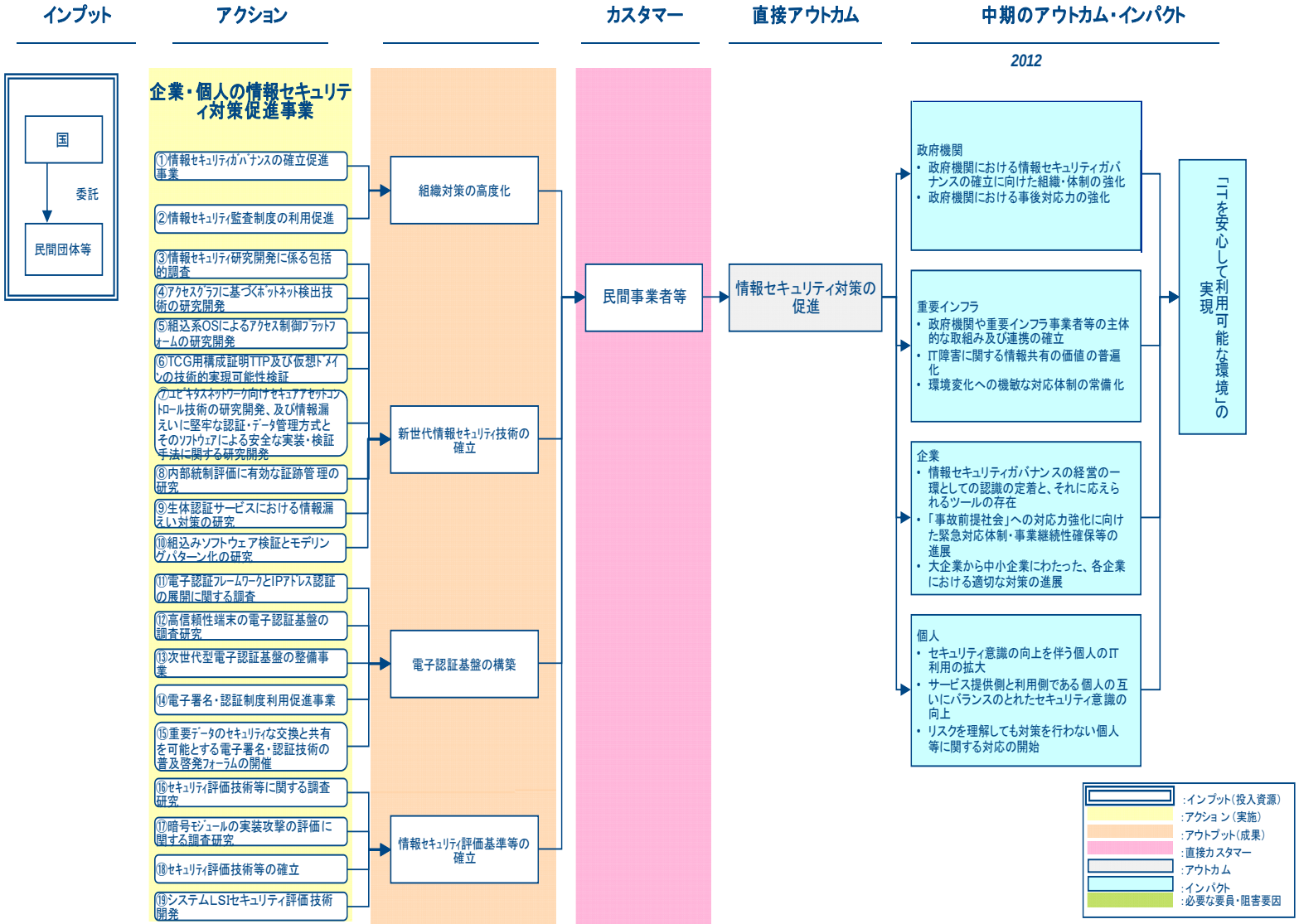
別紙２－２－１

情報セキュリティ分野



別紙２－２－２

企業・個人の情報セキュリティ対策促進事業（H17－H25）



第３章　技術に関する事業の概要

第３章　技術に関する事業の概要

〇情報セキュリティ分野に係る技術に関する事業について

技術に関する事業は、本施策中、企業・個人の情報セキュリティ対策促進事業及びＩＴ融合による新産業創出のための研究開発事業の一部として実施されている。評価検討会の目的は、研究開発事業についての評価を行うことにあるため、プロジェクト評価の対象事業は技術開発に係るもののみとする。具体的には、以下の事業が対象となる。

＜企業・個人の情報セキュリティ対策促進事業＞

Ａ　新世代情報セキュリティ研究開発事業

①情報家電、スマートグリッド等におけるセキュリティ対策技術の研究開発

ａ 高度電磁波解析技術による LSI のセキュリティ対策に関する研究

ｂ 情報家電、スマートグリッド、携帯端末など、非 PC 端末における未知脆弱性の自動検出技術に関する研究

②アクセス制御技術の研究開発

ｃ プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究

ｄ 撮影による情報漏洩を防止するソリューションの研究開発

③クラウドコンピューティングに関するセキュリティ対策技術の研究開発

ｅ 効率的な鍵管理機能を持つクラウド向け暗号化データ共有システム

ｆ クラウドサービスプロバイダとクラウドユーザ企業（法人）における事業継続計画（BCP）の在り方と連携の確保、及びその妥当性検証技術に関する研究

ｇ ＰａａＳ／仮想化環境におけるコンプアライアンス指向データアクセス手法の研究開発

Ｂ　高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業）

Ｃ　暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発

＜ＩＴ融合による新産業創出のための研究開発事業＞

Ｄ　サイバーセキュリティテストベッドの構築事業

Ａ　新世代情報セキュリティ技術開発事業

１－Ａ　事業の目的・政策的位置付け

１－１－Ａ　事業の目的

情報技術の社会基盤化に伴い、情報システムに起因する事故が、経済活動全体の停滞や国民全体の生命・財産そのものに関わるリスクをもたらしかねない状況が生まれつつある。また、情報セキュリティに係る技術の進歩に伴い新たな脅威の出現、また既存脅威の一層の巧妙化が続いており、安全・安心なＩＴ社会を確保するためには変化に素早く対応しかつ先手を打った技術開発を継続的に行っていくことが重要である。このような観点から、対症療法的な対策だけではなく、中長期的な視点に立って、根本的な問題解決を目指して、研究開発を行う。

１－２－Ａ　政策的位置付け

本事業は政府全体の情報セキュリティ政策の中長期計画である「第１次情報セキュリティ基本計画」（平成１８年度２月情報セキュリティ政策会議決定）、「第２次情報セキュリティ基本計画」（平成２１年２月情報セキュリティ政策会議決定）に基づき毎年度策定されている「セキュア・ジャパン」に位置づけられている。また、これらのものは「国民を守る情報セキュリティ戦略」においても、引き続き、推進することとされている。

＜国民を守る情報セキュリティ戦略（抜粋）＞

インターネットを始めとする情報通信技術を利用者が活用するにあたっての脆弱性の克服や、IPv6 や、クラウドコンピューティング、情報家電、携帯端末、センサーネットワーク等の情報通信技術の環境の変化に対応した情報セキュリティ技術の開発、高度化・多様化する攻撃等に対応できる情報セキュリティ技術（「グランドチャレンジ型」研究開発・技術開発）の実現・普及の実現を目指す。

１－３－Ａ　国の関与の必要性

情報技術の進歩や社会情勢の変化に伴い、情報セキュリティに係る脅威は急速に高まっている。こうした中、本事業では、対処療法的な対策だけでなく、長期的な視点から、情報セキュリティ上の問題を根本的に解決するための技術を、国の情報セキュリティ政策を踏まえて、開発し、共通に利用できるような標準化や規格化等を目指している。こういった環境整備は、我が国産業のセキュリティ技術の向上とそれによる安全・安心な国民生活の実現のため、国が実施すべき事項である。

① 情報家電、スマートグリッド等におけるセキュリティ対策技術の研究開発

Ａ－ａ 高度電磁波解析技術によるLSIのセキュリティ対策に関する研究

１－ａ 事業の目的

あらゆる情報家電の安全性と信頼性の確保に対して重要となる、LSIの偽造、改ざん、情報漏えいなど、様々な脅威への対策として、高度化された電磁波計測技術を確立することにある。このため、電磁波解析攻撃耐性評価技術の高度化、不正に挿入された回路の検出、異常動作の検出、偽造LSIの非破壊検査を通じて、LSIの放射電磁波を高精度で取得する装置及び解析手法を開発する。

２－ａ 研究開発目標

LSIの微細加工技術が進み、ますます高集積化する情報家電のハードウェア側からのセキュリティ評価技術として、世界最高水準の高精度電磁波解析システムを開発し、電磁波への情報漏えい解析、不正回路の混入検出、異常動作検知技術の確立を目指した。本事業では、次の４種類のサブテーマに分けて高度電磁界計測・解析技術の開発・研究を進め、各結果を応用して目的を達成するための電磁界解析システムを構築した。

表ａ－１ 個別要素技術の目標

要素技術	目標・指標	妥当性・設定理由・根拠等
高性能磁界プローブの開発	・コイル・アンプの設計 ・プローブ加工技術の開発 ・プローブの開発・改良 ・プローブによるLSIの性能評価 ・プローブ筐体の改良 ・マクロプローブ開発	現在の電磁波解析攻撃で利用される直径0.5～5mm程度のコイルによる磁界プローブに対し、LSIプロセスによる直径数十μmオーダーの微小磁界プローブを開発し、暗号回路上の局所情報の測定を可能にする。なお異常動作にはLSI 全体で検知されるマクロ的なものも含まれるため、高利得プローブを併用して動作解析を行う。
高精度スキャナの開発	・スキャナ基本機構の開発 ・高精度制御機構の開発 ・プローブ筐体実装・改良 ・磁界計測・解析ツールの開発	高空間分解能のマイクロプローブによるμmオーダーの精度での自動計測を可能とするためには、レーザー測定による制御と、周囲の振動の影響を除去するアクティブな振動制御システムを備えた高精度スキャナが必要。
実験用セキュリティ回路の開発	・暗号回路の実装 ・回路制御ツールの開発 ・真贋判定回路の開発 ・Trojan混入ツールの開発 ・Trojan回路実装 ・電力解析手法の開発	開発するマイクロ／マクロプローブおよび高精度スキャナの性能評価およびセキュリティ対策の有効性の検証のためには、電磁波解析実験の対象とするセキュリティ回路が必要。
電磁波解析ツールの開発	・LSIのレイアウトデータと漏洩電磁波を表示するGUI等の開発 ・局所磁界計測 ・評価実験用プラットフォーム開発	開発した磁界プローブと高精度スキャナを用いて、実験用セキュリティ回路の電磁波計測を行い、取得した電磁波を解析してLSIを様々なセキュリティ上の脅威から防御する手法と評価ツールを開発する。

各年度の詳細な目標は次の通りである。

① 平成２２年度

【高性能磁界プローブの開発】

- 現在製品化している近磁界プローブを本事業の目的に合わせて改良し、設計・試作の後にオシロスコープおよびスペクトル解析機能付きネットワークアナライザーを用いて基本性能評価を行う。マイクロプローブは、超高精細な磁界ノイズマップを取得するため、ピックアップコイルとそこで発生する誘導起電力を増幅するための低ノイズ増幅器を単一 LSI 上に実装する方式を検討し、回路設計を行う。設計したインダクタンスと増幅器の利得と周波数応答の評価には、次元電磁界解析ソフトウェアを用い、被測定対象からの磁場放出およびピックアップコイル端での磁界の様子などをモデリングする。所望の性能が得られたならば、物理レイアウトを行い、精細な配置・接続を検討・検証する。
- 上述の LSI の実装方式を具体的に検討する。測定感度を上げるためにはアンテナ部を出来るだけ LSI の表面に近接させ、かつ、ノイズ発生要因を除去する必要があるので、LSI チップを裏面研磨により 50μm 程度まで薄くするとともにアンテナ領域下のシリコン基板厚さを 5μm 程度まで薄くする加工技術の検討を行う。更に、加工した LSI チップを BGA(Ball Grid Array)法で厚さ 0.4mm のフレキシブル基板に実装する方法を検討する。

【高性能スキャナの開発】

- 高精度スキャナの試作・実験に向けて、まず高精度レーザー距離測定器、X-Y-Z ステージ、アクティブ微小震動制御システム等の主要部材の調査・選定を行い、それらを用いたシステムの基本設計をまず行う。実施期間が短いため、この基本設計を基に試作・組立の役務調達を行い、それと並行しての詳細設計を行う。試作スキャナの納品時には基本動作の検証を行い、次年度以降、調整および改良を継続する。

【実験用セキュリティ回路の開発】

- セキュリティ回路としてまず暗号回路を SASEBO-GII 上に実装し、PC から制御する簡単なソフトウェアの開発も行う。FPGA はユーザーが外部から回路構成情報(ビットストリーム)を書き込むことによって動作可能となるため。Trojan 回路はこのビットストリームを一部書き換えることによって実装を行う。しかし、FPGA はビットストリームに付加された誤り訂正符号によってエラーのないことを検証しており、勝手に一部を書き換えるとエラーで FPGA が起動しなくなる。そこで、ビットストリームの解析を行い、FPGA によってエラーが検出されない回路の書き換え手法を構築する。
- 真贋判定用の電磁波を発生する専用回路としては、インバータ(NOT 回路)を数珠繋ぎにしてフリーランさせるリングオシレータなど、プロセスに大きく依存して特性（この場合は発振周波数）が変化する方式を検討し、SASEBO-G および SASEBO-GII に実装して真贋判定に利用可能かどうかの検証を行う。

【電磁波解析ツールの開発】

- 実験用セキュリティ回路の開発作業において開発する評価実験用セキュリティ回路を用いた基礎実験として、既開発のプローブとスキャナを用いて電磁波解析攻撃や磁界強度マップ作成を行う。また、高精度スキャナに関しては、レーザー距離測定器および X-Y-Z ステージの制御ドライバと、電磁波計測のためのオシロスコープとスペクトルアナライザのドライバを開発する。

② 平成２３年度

【高性能磁界プローブの開発】

- （近磁界測定用マクロ磁界プローブの開発）市販の磁界プローブは、情報家電等が発生する電磁波が基準を下回っているかといった計測（EMC/EMI 試験）を目的としており、情報が電磁波から漏えいしているかどうかといった解析は対象外である。また、情報家電全体が発する電磁波を計測するため、今回の目的である LSI のごく近傍の電磁波解析には特化していない。そこで、LSI 全体からの電磁波などによる情報漏えいの検査に適したマクロ的な計測のためのプローブに必要な条件を明らかにするため、LSI 近傍の電磁波解析実験を行い、これに特化した「マクロ磁界プローブ」の開発を行う。
- （LSI プロセルを用いたマイクロ磁界プローブの作成）通常の磁界プローブは直径が mm オーダーの巻きコイル等を用いているが、本プローブは、LSI プロセスの金属配線層を用いて作成されたμm オーダーの微小コイルを用いる。通常のプローブはコイルで捉えた信号をアンプに入力する線路で外部のノイズを拾ってしまい、ノイズごと増幅されるため、プローブのヘッド以外が余計な信号を拾わないようにシールドを施す。また、本マイクロ磁界プローブで捉える信号のレベルは極めて小さいため、シールドだけでは不足であるため、微小コイルに隣接し、同じ LSI プロセスでプリアンプを構成し、信号を増幅してから後段のアンプへと送る方式をとる。なお、観測対象とする周波数帯が MHz 帯であり、かつコイル径もμm と微小なため、コイルで計測できる信号は極めて小さく、それを増幅するプリアンプの設計は、解析対象の信号の特性や周波数帯、利用する LSI プロセス等、様々な要素を考慮しながら複数設計し、また試作による性能評価をフィードバックしていく。微小プローブを用いて取得した波形はデジタルデータに変換し、PC 等を用いて信号解析を行う。このため、微小プローブにプリアンプだけでなく、チップ上に信号処理機能を実装し、周波数帯域を選択した高感度測定を可能とする技術を開発する。
- （プローブ加工による高空間分解能マイクロ磁界プローブの試作）LSI プロセスを用いた微小プローブはシリコンウエハー上に形成されるだけなので、そのままで計測に用いることはできず、解析対象物である LSI 上の磁界を走査できる形状に加工する必要がある。このとき、以下のような条件を考慮する必要がある。

- 測定対象 LSI の配線を流れる電流が発生する磁束を効率よく検出するため、測定対象に対してコイル断面が垂直となるよう固定する。
- 測定対象 LSI とコイルとの距離を極限まで狭めながら、両者が多少接触しても破損しない構造とする。
- 磁界測定の空間分解能を上げるため、プローブの先端を可能な限り小さくする（プローブの先端幅の目標はコイル幅の 3 倍以下）。

これらをもとにガラスエポキシ基盤を用いてプローブを構成するが、さらなる空間分解能の向上を目的に、LSI の加工装置である収束イオンビーム (FIB: Focused Ion Beam) を用いたプローブの先端部の微細加工技術の可能性を探り、製造コストも考慮しながら試作の検討を行う。

【高性能スキャナの開発】

- 開発したマイクロ磁界プローブによる計測のため、ステージの XYZ 方向の精度として±1μm を目標に、新たな制御機構、特にレーザー測距を用いた位置測定・キャリブレーション機構の開発に主眼を置いた、高性能スキャナの開発を行う。また、磁界プローブも一本一本、その形状および特性に微小なばらつきがあるので、それらの磁界を計測しながらキャリブレーションする技術も開発する。
- 現在の計測では磁界の強度分布を調べることが目的であるが、内部の動作状態を解析して情報漏えいがないかを検証するには、磁界の時間波形および情報が漏洩している周波数帯を同定する必要があり、これらの分析も同時に進める。

【実験用セキュリティ回路の開発】

- 高性能磁界プローブの開発ならびに高性能スキャナの開発によって得られる技術の有効性の検証のためには､電磁波解析実験を行うためのターゲット LSI が必要となる。磁界プローブおよびスキャナの基本性能評価および電磁波解析攻撃は、独立行政法人産業技術総合研究所（以下､「産総研」という｡）が開発したサイドチャネル攻撃用標準評価ボード SASEBO-R を利用して行う。一方、Trojan 回路等の悪意のあるハードウェアのサンプル実装については、論理回路をユーザが手元で書き換えることができる FPGA ボードである SASEBO-B/-G/-GII を用いて評価実験を行う。
- LSI の真贋判定に用いる偽物の LSI は入手することが困難であるため、異なる FPGA 上に同じ論理回路を実装して、その違いが磁界プローブによって判別可能かどうかについて検証する。また、この真贋判定は、LSI が持つアプリケーションとしての論理回路が発生する電磁波を解析する必要はないことから､真贋判定用の電磁波を発生する専用回路による判定方式の開発も行う。この専用回路としては、インバータ（NOT 回路）を数珠繋ぎにしてフリーランさせるリングオシレータなど、プロセスに大きく依存して特性（この場合は発振周波数）が変化するものが挙げられる。このほか、トランジスタのス

イッチング確率が高く疑似乱数生成器としても利用される LFSR(Linear Feedback Shift Register)などによって、放射電磁波を増幅させる回路による非破壊検査手法の開発を行う。さらに、検査用の電磁波を効率的に生成する専用のアンテナを金属配線で構成することも検討する。ここではアンテナを電磁波を放射するパーツとしてだけでなく、プロセスによって大きく変化する特性により、真贋判定のための電磁波の差異を増幅するコンポーネントとして研究する。

【電磁波解析ツールの開発】

- 開発された磁界プローブと新たな計測技術を用いて、前項のセキュリティ回路の電磁波計測を行い、その取得した電磁波を信号処理や暗号理論を用いて解析することで、LSI を様々なセキュリティの脅威から防御するための評価ツールを開発する。本研究では LSI 上の 2 次元の局所的な電磁波を計測し、これまで観測できなかった微小な情報を含むと考えられる大量のデータを解析する必要があることから、電磁波解析攻撃に対する安全性評価と Trojan 回路の情報漏えいの研究においては、これまでのツール開発で培った信号処理・解析の技術を発展させるのと同時に、新規に、LSI のレイアウトデータと漏洩電磁波の重ね合わせ表示、正常動作と異常動作の比較・差分表示等、グラフィカル・ユーザ・インタフェース等の開発も行う。さらに、真贋判定のためのパターンマッチング技術についても様々な評価実験を行い、LSI からの電磁波を用いた識別に適した手法の検討と実装を行う。また、これらの解析・評価技術を必要に応じてスキャナの制御・データ表示ツールにも組み込むことで、計測・解析実験の効率化を図る。

③ 平成２４年度

【高性能磁界プローブの開発】

- 前年度に開発した第１世代のマイクロ磁界プローブのアンプ特性を改良し、その実装と性能評価を行いながら、同時に第２世代プローブの開発を進め, 実験から実用化へ向けたプローブの実装方式と筐体の改良を行う。またその性能評価の計測対象の LSI を加工しその内部動作解析を進める。第１世代のプローブは、一つの広帯域アンプで計測する全周波数帯をカバーする方式を採用していた。しかしながら、アンプの周波数帯域を広くとると、全周波数に渡って均一に分布する熱雑音の影響が大きくなり、測定対象からの電磁放射に含まれる極微小な成分を高い SN 比で測定することが困難となる。そこで、次年度に開発する第２世代の高機能磁界プローブは、ミキサ回路を使用することで所望の周波数の信号をダウンコンバートし、極狭帯域のアンプで増幅することで熱雑音の影響を抑え、高い SN 比の実現を目指す。第２世代のプローブ LSI の回路構成におけるアンプの段数は 3 段を想定するが、ミキサ及び最終段のアンプによって十分な利得が得られれば、適宜段数を削減する。ダウンコンバートされた信号は、LPF(Low Pass Filter)によって帯域を制

限し、熱雑音の影響を抑える。ミキサ回路には参照信号となる周波数入力が必要となるが、LSI 上で低ノイズの周波数信号を作るには大きな発振器が必要なため、プローブ LSI 内に実装することは難しく、外部の信号発生器を用いることとする。

- 以上の目的を達成するため、マイクロ磁界プローブ用 LSI のオンチップアンプ・ミキサ回路の実装・計測技術についての調査のため、European Solid-State Circuits Conference (ESSCIRC) 2012 に参加する。同時に磁界プローブ回路の新たな構成についても調査を行い、海外の技術者とも同技術について議論を行う。さらに国内の集積回路研究会ＬＳＩとシステムのワークショップに出席し、国内の研究動向を調査するとともに国内の技術者との議論を行いさらに知見を深める。本研究で設計した磁界プローブを用いた磁界計測法及びその応用方法・応用アプリケーションの調査と最新の研究動向の調査、同時に国外の技術者と議論を行うため、International Solid-State Circuits Conference (ISSCC) 2013 に参加する。

【高性能スキャナの開発】

- 前年度に行った高精度スキャナを用いたマイクロ磁界プローブの評価実験において、外来ノイズの影響が非常に大きいことが明らかとなっている。そこで、高精度スキャナへの外来ノイズを遮蔽するシールドボックスを作成する。また、第 1 世代のプローブボードは、強度を重視した比較的大きな筐体におさめたが、より計測が容易となるよう小型化を進める。前年度に研究を終了した産総研の異常や不正品等の検出技術の開発を行う。

【電磁波解析ツールの開発と評価実験】

- 開発したプローブと高精度スキャナを用いて、効率的に電磁波を計測・解析するツールの改良を続ける。LSI の正常動作と異常動作の比較・差分表示などのグラフィカル・ユーザ・インタフェースを向上させる。Trojan 回路の実験では、磁界強度マップを利用して漏洩情報の大きい場所を特定するなど攻撃の効率化を行う。また前年度に電力波形に対して実施した Dual-round attack を電磁波形へ適用し、また 2 つの S-box の動作の類似性を利用した新しい攻撃手法の実験も行う。

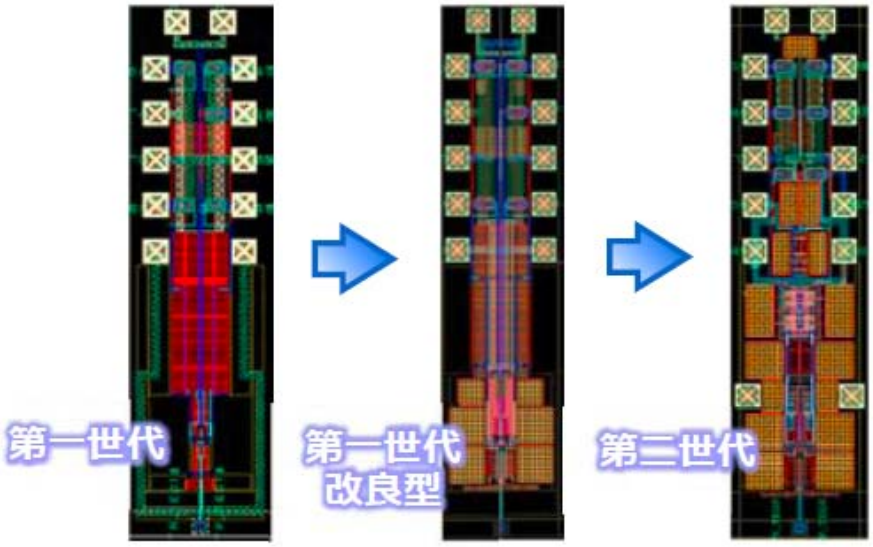
３－ａ　成果、目標の達成度

３－１－ａ　成果

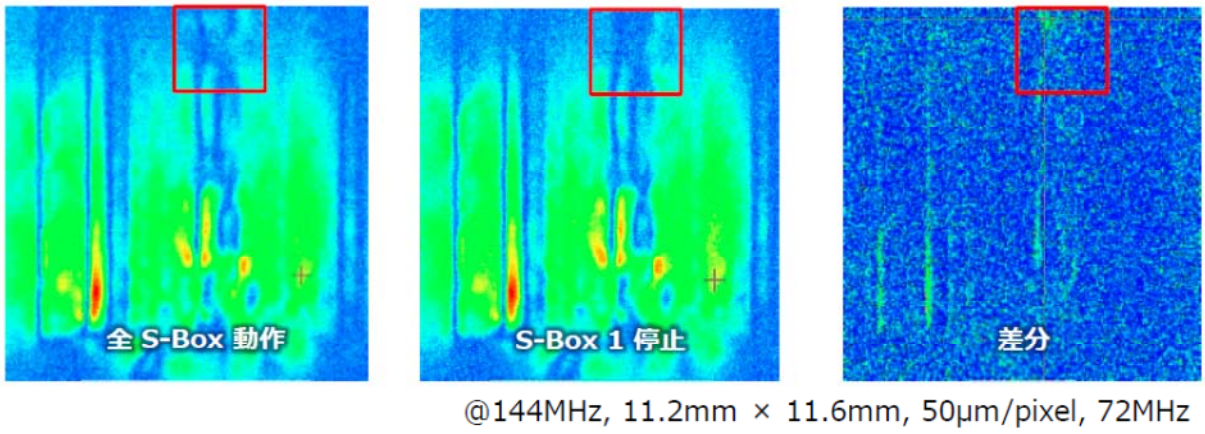
（１）成果

開発したマイクロ磁界プローブは従来比およそ 10 倍の出力振幅を達成した。同様に、高精度スキャナシステムでは従来よりもおよそ10倍の位置決め精度を達成した。

開発したマイクロ磁界プローブは、従来のようにコイルを巻いてアンプで増幅する磁界プローブではなく、マイクロプローブLSI のワンチップ上に磁界検出用ループアンテナと増幅用アンプ、そして周波数ダウンコンバータを実装するなど先進的な設計を行うとともに、集積イオンビーム装置を用いたアンテナ下のシリコン基板除去など、加工成型プロセスにおいても大きなチャレンジを行った。



図ａ－１　開発したマイクロプローブの内部基板



図ａ－２　マイクロ磁界プローブを用いた差分磁界マップによる解析の例

開発したマイクロ磁界プローブを用いた差分磁界マップでは、従来のマクロプローブでは見えなかった局所的な構造が詳細に観測可能となった。上図では差分画像においてメッシュ構造などが明らかとなっており、マイクロ磁界プローブを用いることで、LSI のフロアプランとの比較による解析が可能と期待される。このように、本成果を入力データを制御して磁界強度を制御できることから、ホワイトボックス評価における大きな可能性をもたらすだけでなく、従来のような観測結果に基づく統計解析を行うことなく、磁界マップから直接情報漏洩を目視できる潜在性も有している。

（２）特許・論文等の状況

本研究開発の成果をもとに出願した特許、発表した論文等は次の通りである。

表ａ－２　特許・論文等件数

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
2	0	0	0	0	0	0

論文のリストは以下のとおりである。このほか、International Solid-State Circuits Conference（ISSCC 2013）にて発表を行った。

- Nguyen Ngoc Mai-Khanh, Tetsuya Iizuka, Makoto Yamada, Osamu Morita, and Kunihiro Asada, ``An Integrated High-Precision Probe System for Near-Field Magnetic Measurements on Cryptographic LSIs," in Proceedings of IEEE Sensors 2012, pp. 2074 - 2077, Oct. 2012.
- Nguyen Ngoc Mai-Khanh, Tetsuya Iizuka, Makoto Yamada, Osamu Morita, and Kunihiro Asada, “An Integrated High-Precision Probe System in 0.18-um CMOS for Near-Field Magnetic Measurements on Cryptographic LSIs,” IEEE Sensors Journal, vol. 13, no. 7, pp. 2675 - 2682, Jul. 2013.

３－２－ａ　目標の達成度

マイクロ磁界プローブLSIの製造は数ヶ月の単位の綿密なスケジュール管理が必要であったが、設計→試作→評価→改良というサイクルを回しながら、同時に高精度スキャナの改良、制御ソフトウェアの開発、セキュリティ回路を用いた実機評価、等の複数の作業と協調しながら、各年度の目標と課題をクリアした。マイクロ磁界プローブおよびスキャナの性能は目標通りの性能が得られ、またセキュリティ回路を用いた不正回路混入検知、情報漏えい検出技術も開発し、技術的には計画を達成できた。しかしながら、期間内に事業成果を産業へ展開するには至らなかった。目標の達成度を分野別に示すと、次ページ表のようになる。

表ａ－３　目標に対する成果・達成度の一覧表

要素技術	目標・指標	成果	達成度
高性能磁界プローブの開発	•コイル・アンプの設計 •プローブ加工技術の開発 •プローブの開発・改良 •プローブによるLSIの性能評価 •プローブ筐体の改良 •マクロプローブ開発	• 低雑音アンプにより実装した第1世代、増幅率を調整するとともにバイアス電源を単一化し、最大増幅率を63dBから76dBに改善した第1世代改良型、微小磁界を周波数選択することで高S/N比を実現した第2世代の3種類のマイクロ磁界プローブを開発した。 • 従来比およそ10倍の出力振幅を実現。	達成
高精度スキャナの開発	•スキャナ基本機構の開発 •高精度制御機構の開発 •プローブ筐体実装・改良 •磁界計測・解析ツールの開発	• 初期の実験において外来電磁ノイズの影響を受けていたのをシールドの変更により改善。 • 磁界強度マップの自動生成、ジョイスティックによる操作性向上、誤操作防止機構などを実装した電磁波計測・解析ツールを開発・改良。 • 位置決めにおいて、従来比約10倍の精度を実現。 • 12μmピッチでの高解像度の画像取得に成功。	達成
実験用セキュリティ回路の開発	•暗号回路の実装 •回路制御ツールの開発 •真贋判定回路の開発 •Trojan混入ツールの開発 •Trojan回路実装 •電力解析手法の開発	• サイドチャネル攻撃実験用AES暗号回路をSASEBO-GIIに実装 • 真贋判定用電磁波強調用のAES発振回路を設計しSASEBO-GIIに実装 • 3種類の攻撃手法を適用 ・2ラウンド攻撃（電力解析用手法の適用） ・クロック間衝突を用いた攻撃 ・回路の類似性を用いた攻撃 • AES回路のレイアウトをもとに磁界強度分布の分散と平均値を調査	達成
電磁波解析ツールの開発	•LSIのレイアウトデータと漏洩電磁波を表示するGUI等の開発 •局所磁界計測 •評価実験用プラットフォーム開発	• 実験用回路とオシロスコープを制御し、自動的に電磁波測定するソフトウェアを開発 • Trojan回路に対する磁界スキャナによる評価環境を整備 • ジョイスティックとGUIによる計測・解析の効率化	達成

各年度の詳細な成果は次の通りである。

① 平成２２年度

【高性能磁界プローブの開発】

- （近磁界測定用マクロ磁界プローブの開発）マクロプローブは、計測対象に応じて特性が選択できるよう高利得と低ノイズの 2 種類を開発した。高利得プローブは増幅器とのマッチングを最適化した既開発の 10 巻きの磁界プローブに対して、さらに下記の改良を行ったプローブを作成した。低ノイズプローブは利得は低いもののノイズが低いため、SASEBO-GII 上の AES 回路に対する電力解析攻撃実験では、既開発の高利得プローブよりも高い精度での鍵推定に成功している。
- （高空間分解能マイクロ磁界プローブの開発）マイクロプローブはコイルを小さくすることで空間解像度が向上する半面、測定対象からの磁場による誘導起電力が減少する。そこで来年度の試作に向け ROHM 社の 0.18um CMOS プロセスを用い、サイズ・巻き数を変更した 4 種類のオンチップ微小コイルをレイアウトし、その特性シミュレーションを行った。コイルをプローブヘッドとして実装する際には、シリコン基板の裏面研磨を行う予定で、これに

よってコイルの Q 値が向上することを確認した。微小コイルに誘起される電圧は極めて小さいため、同じ LSI 上に実装するアンプの熱雑音の影響を検討する必要がある。基本的な構造のアンプの熱雑音を理論的に計算したところ、単一の広帯域アンプでは熱雑音レベルが大きく、低周波側の信号の S/N 比が 1 を下回り検出が困難となることがわかった。そこで、計測する周波数帯域を分けて複数のアンプを切り替える構成を引き続き検討した。

- （高空間分解能マイクロ磁界プローブの加工）来年度に試作予定のオンチップコイルおよび低雑音増幅器 LSI を、プローブの先端へ実装するための加工・実装試験として、サンプル LSI の裏面研磨とダイシングを行った。裏面研磨でチップの厚みのばらつきが大きいと、圧力のかかり方や熱の放散に違いが生じ、プローブ化のためのそれに続く加工の問題やプローブの性能差が起こるため、LSI のリバースエンジニアリング用の高精度な裏面研磨装置を使用した。その結果 100μm±10%、150μm±10%という高い精度での加工を実現することができた。研磨の次に、LSI のプローブヘッドの形状への高い精度でのダイシングと、Si 基板部の局所的除去に対して FIB(Focused Ion Beam)法を用いた。アンテナ先端部として、LSI を荒れのない状態で確実に仕上げることができた。

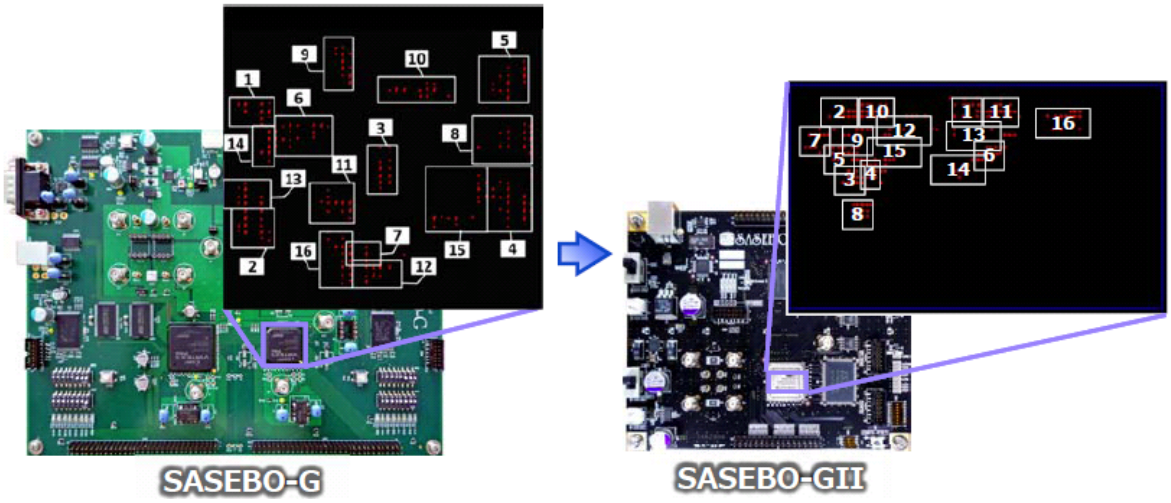
【高性能スキャナの開発】

- 測定対象の LSI 上をμm の精度で走査する高精度スキャナの開発・実験に向けて、まず高精度レーザー距離測定器、X-Y-Z ステージ、アクティブ微小震動制御システム等の主要部材の調査・選定を行い、それらを用いたシステムの基本設計を行なった。高空間分解能のマイクロプローブでは、LSI 上で数～数十万ヶ所の観測をするため、自動計測が可能なスキャナが必要である。そして、測定対象が発生する磁界によってプローブ上のコイルに生じる起電力は、それらの距離の 2 乗に反比例することから、水平方向よりも垂直方向の精密制御がより重要となる。そこで、距離の計測には高精度レーザー距離測定器を用いた。さらに、周囲の振動による測定系への影響も除去する必要があるため、アクティブ微小震動制御システムを導入している。そして、スキャナシステムを制御するためのソフトウェアも開発し、マクロプローブと SASEBO-GII を用いた基本動作試験を行った。

【実験用セキュリティ回路の開発】

- SASEBO-GII にサイドチャネル攻撃実験用 AES 暗号回路を実装し、また真贋判定用回路にそれをベースにリングオシレータのようにループを作って発信させる回路を開発した。リングオシレータはインバータチェインによるシンプルな発信回路で、その周波数はプロセスに極めてセンシティブなものの、波形が単純で発生する電力・電磁波も弱いという欠点がある。これに対して、AES を用いた発信回路は電力が大きく、デバイスによって特徴の異なる波形が得られ、真贋判定用回路としての大きな可能性が示された。

- Trojan 回路については、AES 暗号でラウンド処理ブロックを繰り返し使うループアーキテクチャの回路をベースに、バッファの挿入、ラウンド処理部の冗長化、レジスタの冗長化により、消費電力を増加させる Trojan 回路を考案し、SASEBO-GII に実装した。そして、各実装に対する電力解析攻撃実験を行なった結果、16 バイトの秘密鍵のうち解析対象の 1 バイトにだけバッファを挿入した方式が、他に比べて数倍高い精度が得られた。他方式は解析対象バイト以外の部分にも冗長回路を付加したことで全体の消費電力は増加したものの、解析対象の漏洩情報とその他のノイズの両方が増幅されたため S/N 比が向上しなかったものと考えられる。この結果から、電磁界の局所的な解析を可能とするマイクロプローブの開発による解析精度の向上が期待される。



図ａ－３　実験用セキュリティ回路としての２種類のボードにおける AES 暗号化の実装箇所

【電磁波解析ツールの開発】

- 評価環境のとして、SASEBO-GII 上に実装した AES 回路とオシロスコープを制御し、自動的に電磁波測定するソフトウェアの開発を行った。また、AES 回路の暗号処理に応じた電磁波の変動から秘密鍵を抽出できることを確認し、その実験結果を通じて高性能なマクロプローブを開発した。さらに、100μm 単位の位置操作による自動測定や、測定を再現する電動ステージによる実験環境も構築した。解析ツールの開発と実験環境の構築において、SASEBO-GII を解析対象として用いた。SASEBO-GII は暗号回路用と制御回路用にそれぞれ Xilinx 社製 Virtex-5 および Spartan-3 の 2 つの FPGA を実装している。この Virtex-5 は放熱のため金属カバーを有しており、電磁波が漏れにくく実験には不都合であった。そこで、カバーを剥離し導熱接着材を除去するという加工を施し、また、プローブの位置合わせを行うためのマーキングを行った。計測した波形を用いて電磁波解析攻撃の一手法である Correlation Electro Magnetic Attack を実施した結果、いずれのプローブにおいても秘密鍵の抽出に成功した。

- 電磁波解析実験を効率よく進めるために、測定対象のデバイスやオシロスコープを制御して数万～数十万の波形を自動的に計測するソフトウェアの開発を行った。
- チップサイズがが 2~5mm 角の SASEBO-R 上の暗号 LSI を用いた評価実験には、精度の高い位置決めが不可欠である。また、LSI の電磁界強度マップ作成には、測定を自動で行うステージが必要となる。携帯機器などの EMC 評価向けに販売されている電動ステージは、数百万円と高価であったため、組立型電動ステージを利用して簡易環境を構築することとした。制御装置により 100μm ステップの連続移動が可能で、プローブの位置を USB 経由で PC より観測することを可能とした。

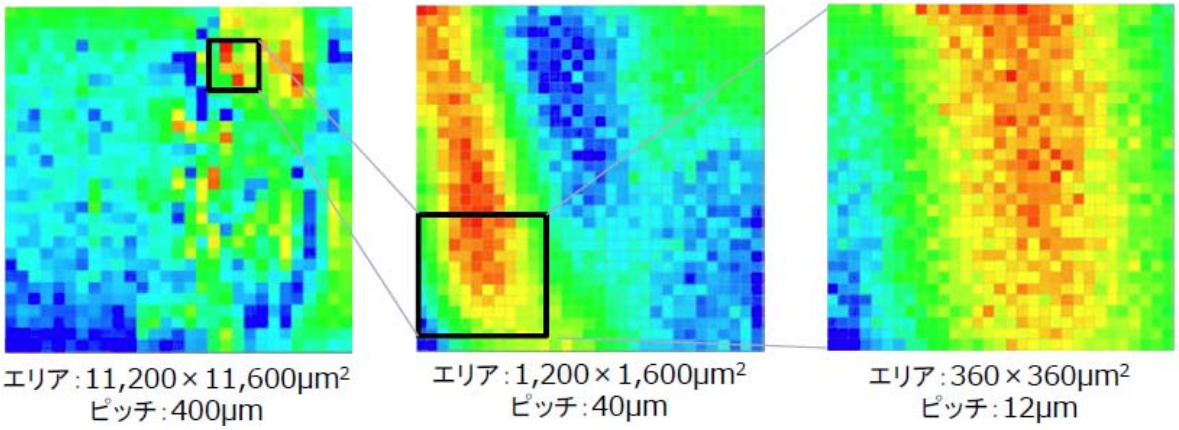
② 平成２３年度

【高性能磁界プローブの開発】

- マイクロ磁界プローブに搭載する微小コイルとアンプを実装したＬＳＩを、ローム社の 180nmCMOS プロセスを用いて設計・製造した。微小コイルで得られる 50uV という微小な信号を 50mV まで増幅する必要があるため、図 2.1 に示すようにアンプ構成は低ノイズ性を考慮した初段から高い増幅率を持つ最終段までの 3 段とした。図 2.1 中央のこちらのグラフはアンプ利得の周波数特性で、最終段の動作電圧を外部から調整することで利得を制御することができるようになっている。この構成で広帯域と狭帯域の 2 種類のアンプを、5 種類の形状のコイルと組み合わせ、短冊状のレイアウトを 10 種類作りＬＳＩ上に実装した。試作した LSI を評価用基板に実装し、アンプ利得の周波数特性を計測した。計測機器の 50Ω終端抵抗の影響により、シミュレーションよりも利得が低くなったもの、期待する特性が得られた。この結果を踏まえて、高い利得が得られるように改良を施したアンプを設計・レイアウトした。
- 予算の制約から 10 種類全てのアンプを、プローブ化することができないため、このうちの 3 つを選んで実装を行った。LSI からプローブチップを短冊状に切り出した後に、裏面研磨等の加工を行い、プローブ用基板に実装、コネクタを接続した。このプローブ基板を用いて、マイクロストリップラインに電流を流し、そこに発生する磁界を観測する実験により、その動作確認と基本性能評価を行った。

【高性能スキャナの開発】

- 前年度に制作したスキャナの基本ハードウェアに、高精度な制御を行うためのレーザーによる距離計測や、顕微鏡カメラによる校正機構を実装することで、μｍのオーダーの位置精度で制御し、観測対象の電磁波を計測可能とした高精度スキャナを開発した。
- プローブ筐体及び保持機構にも、万がープローブ先端が計測対象に接触した場合に、ヘッドが逃げられるようバネで固定するなどの工夫を施した。



図ａ－４　マイクロ磁界プローブを用いた高空間分解能磁界計測の例

【実験用セキュリティ回路の開発】

- 本研究では、平均化された電力波形では見えないＬＳＩの局所的な情報を電磁波でとらえることが重要な課題の一つである。マイクロ磁界プローブだけでなく、直径数 mm のマクロ磁界プローブでもそれが可能であることを検証するための評価用回路として、AES の S-box 回路が発生する局所電磁界を利用する Trojan 回路を開発した。レイアウトに制約を与え、攻撃対象の S-box1 を分離配置して計測すると 7,000 波形で攻撃に成功した。このように、マクロプローブでの局所電磁波の情報取得が可能であることが示され、マイクロプローブではさらに高精度なＬＳＩ内部の解析が期待される。前年度までは、回路のロジックを変更する Trojan の研究を行っていたが、ロジックにはまったく手を加えずにレイアウトを操作するだけでも Trojan となりうることが明らかとなった。また、この実験の局所電磁波解析技術は攻撃手法としてではなく、逆に Trojan の検出技術としても有効であることがわかった。
- FPGA では回路書き込み時に多重の CRC チェックが行われるため、Trojan 回路を挿入しようと単純に回路情報を書換えようとしてもエラーとなってしまう。そこで FPGA の回路情報のフォーマットを解析し、CRC を改ざんするツールを作成して実験を行った。その結果、FPGA に異常な発熱を生じさせることに成功した。
- 同じデジタル動作をする LSI であても製造プロセスが異なると、トランジスタデバイス等のアナログ的な性能が異なる。そこで、偽造対策を目的に、デバイスのばらつきから特異な動作波形が得られる LFSR 型発振回路を開発し、SASEBO-GII 上の FPGA に実装した。実験結果から、同じ Virtex-5 であってもグレードや製造国による個体の違いを識別が可能であることが示された。

【電磁波解析ツールの開発】

- 前年度は FPGA 上の Trojan 回路に対して電力解析を行ったが、同じ Trojan 回路に対して磁界スキャナによる評価環境を整備し、電磁波解析を行った。
- 新しいサイドチャネル解析手法の研究を進めた。従来の AES のサイドチャネ

ル攻撃では、暗号文出力の処理を行う最終 10 ラウンドの動作波形を利用していたが、暗号文出力から遡って 9 ラウンド目の内部状態を推定して波形を解析する手法を開発した。これにより、従来の 2/3 の波形数で秘密鍵の導出に成功し、サイドチャネル攻撃の技術を競う国際コンテスト DPAcontest において、最も優れた成績を収めた。

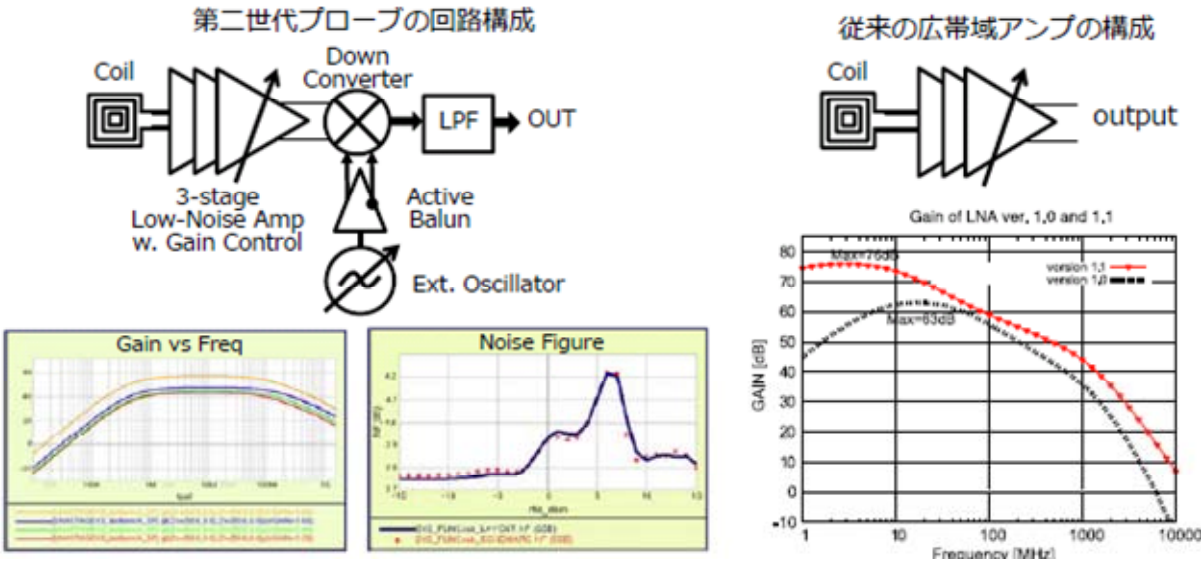
- マクロ磁界プローブとして様々な形状のものを開発し、その基本特性評価を行うとともに、FPGA 上の AES 暗号回路の他に、パッケージを剥離した IC カード上に AES 暗号ソフトウェアを実装し、計測ツールにより磁界強度マップを作製した。上述の Trojan 回路の実験では、レイアウト情報を基に、漏えい情報を多く含む場所にプローブを置いて磁界を計測していたのとは逆に、作成した磁界強度マップから漏洩情報を多く含む場所、たとえば Trojan が潜む場所を検出するといったことが可能となった。

③ 平成２４年度

【高性能磁界プローブの開発】

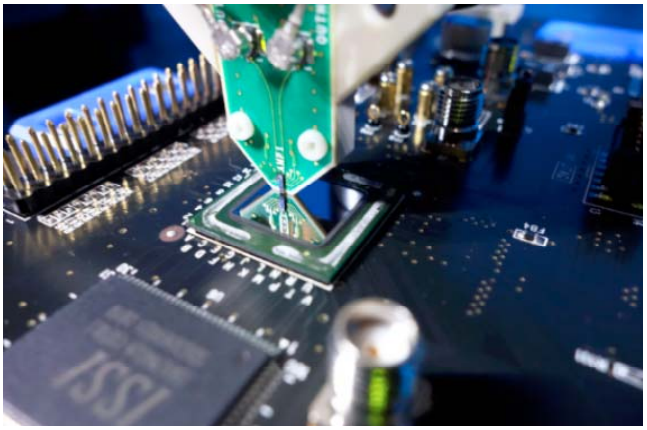
- 昨年度、設計・試作・検証を行った第 1 世代マイクロ磁界プローブの増幅率（ゲイン）を向上させるため、第 1 世代プローブを改良した第 1.5 世代プローブの回路設計と検証を行った。シミュレーションにより動作検証を行った広帯域および帯域制限型の第 1.5 世代アンプ回路を、Rohm 社の 0.18CMOS プロセスを用いて集積回路上に実装するレイアウトを作成した。これらのアンプ回路を５種類のサイズのコイルと組み合わせた 10 種のプローブ用 LSI と 2 種のアンプ単体テスト用回路を実装した 5mm×5mm サイズのチップの試作を行った。試作を行ったチップ中の単体テスト用回路を使用して、試作した第 1.5 世代プローブ用アンプ回路の実測による性能評価を行った。シミュレーションと比較して、測定で得られたゲインは大幅に小さくなったが、これは測定環境におけるバイアス入力等に重乗するノイズが原因と考えられている。これらの耐雑音性についてはプローブ形状への実装および X-Y ステージ上へのマウント時により詳細な対策を実施し、磁界マップ取得時には安定して高いゲインが実現できるように配慮した。
- 第 1 世代、第 1.5 世代のマイクロ磁界プローブにおいては、対象となる周波数を幅広くカバーすることを目標としていたが、こうした広い帯域にわたって高いゲインを持つアンプにおいては、回路内のトランジスタの熱雑音を主たる原因とする雑音が、測定対象からの放射性磁界によってプローブのピックアップコイルに誘起される電圧よりも大きくなり、測定時の十分な S/N 比（信号対雑音比）が確保できなくなる問題が明らかとなった。また、主な測定対象となるセキュリティを目的とした暗号回路などは、通常ある周波数のクロック信号を基準として動作しており、その周波数及び高調波成分が測定対象となる場合がほとんどである。そこで、アンプの周波数帯域を制限して熱雑音の影響を抑えるとともに、測定対象周波数の選択を可能とする第 2 世

代のプローブヘッド LSI の設計を行うこととした。ゲイン制御可能な 3 段アンプ、ダウンコンバーター、アクティブ Balance-Unbalance 回路、Low-Pass Filter を同一 LSI 上に実装した。また、ミキサ回路を用いて対象周波数を低周波数に変換することで、雑音帯域を抑制し、微弱な磁界を取得可能とするとともに、低帯域化による測定器のコスト削減も実現した。ただし、本事業の研究開発期間内ではプローブ用 LSI とプローブの製造段階までにとどまり、プローブによる性能測定までには至らなかった。



図ａ－５　マイクロ磁界プローブを用いた差分磁界マップによる解析の例

- 計測対象ハードウェアとして、劣化した LSI を意図的に作成するために、SAKURA-RII ボードを高温・高電圧で動作させる加速試験用ボードを開発し、3 ヶ月間動作させたものの、LSI の信頼性が高くエラーが発生しなかった。そこで、SASEBO-GII の FPGA を研磨することにより、仮想的なエラーを生じさせることに変更した。



図ａ－６　開発した第２世代マイクロ磁界プローブによるスキャンの状況

【高性能スキャナの開発】

- 前年度に明らかとなった放送電波や計測機器が発生する外来ノイズの影響を除去するため、電波暗箱及び、装置全体を収容する専用台の設計・試作を行った。電波暗箱設置時に、プローブアンプ用の精密 DC バイアス電源からスイッチング電源ノイズが発生しており、そのノイズが近接するプローブ出力の測定用 RF ケーブルに重乗していることがわかり、DC バイアスケーブルにノイズ対策としてシールド被服を実施した。さらに、高さ測定用のレーザー光源からもノイズの発生が認められ、そのノイズ対策のため高さ測定のルーチン終了後、高さ測定装置の電源を OFF にする装置を開発し、合わせてソフトウェアの実装も行った。
- 電波暗箱設置場所の制約及びプローブ交換作業の安全性確保の観点から、X-Y-Z スキャナ、ステージを 90 度回転して使用できるように改修を実施した。この改修により、プローブ交換作業、校正作業もスムーズに実施できる環境となった、さらに、電波暗箱設置場所の制約から X-Y-Z スキャナ、ステージ用ドライバ回路装置、校正用顕微鏡装置、高さ測定用装置本体などを収納する専用台を製作した。ステージ用ドライバ回路装置（マスター／スレーブ電源 ON のタイミング）をはじめ、全 12 台の装置の電源 ON/OFF の集中制御（電源投入の順番、タイマー機能）を有する装置も合わせて開発し実装した。
- マイクロ磁界プローブを高精度スキャナに実装するための、プローブ筐体の設計・実装を行った。昨年度試作した第 1 世代プローブ用筐体は金属製であったが、計測磁場への影響を考慮し、ポリフェニレンサルファイド（PPS）樹脂製への変更を行った。本年度開発の第 2 世代プローブに関しては、計測対象の LSI 上を走査しやすくするため第 1 世代のプローブよりも先端をより細くし、それに合わせた筐体の設計と実装を行う予定であった。しかし、LSI の納入と動作確認作業に時間を要したため、プローブボードの再設計には至らず、第 1 世代の基板形状を踏襲し、DC バイアスの印加コネクタやケーブル等の変更にとどめることとした。

【電磁波解析ツールの開発】

- 高空間分解能のマイクロ磁界プローブは、スキャナの水平方向をμmオーダーで制御する必要があることから、より安定して精度の高い磁界計測を可能とするために校正機構を改良した。
- スキャナの操作性向上のため、ジョイスティックの実装を行い、高精度スキャナとマイクロ磁界プローブを用いて、効率的に電磁波を計測・解析するツールの改良を行った。また、初期設定時のプローブの高さ校正において、校正面との接触によるプローブの破損を防止するため、顕微鏡カメラによる画像を PC 画面上に表示して、プローブヘッドと校正面の距離を正確に計測し、テンキーと数値入力によってその距離を設定する機構を開発した。
- 前年度に開発した電磁波解析ツールについて、入力データによる磁界の変化

の解析等を目的として、２つの磁界の比較・差分を表示する機能を追加した。
追加された機能は以下の通りである。
－比較画面を大きな別ウィンドウで開く
－磁界マップ上の十字カーソルにおいて周波数スペクトラムを表示
－計測範囲が異なる磁界データを比較するための比較エリアの調整機能
－画像データ及び CSV ファイルの出力

図ａ－７　電磁波解析ツールの整備による操作性の向上

４－ａ　事業化、波及効果について

４－１－ａ　事業化の見通し

従来よりも一桁高い高精度磁界スキャナシステムは、悪意のある攻撃による誤動作や情報漏えいの検知だけでなく、偶発的な故障による異常の検知へも応用が可能である。シリコンを透過する磁界の検出により、半導体メモリ等で実用化されロジックチップに対する技術開発が進んでいる積層チップ内部の故障検出への応用が期待される。そこで JEITA(電子情報技術産業協会)の故障解析関係の情報交換会などを通じて、メモリカードベンダや LSI 検査装置メーカーに技術の紹介を行っている。しかし、スキャナシステムの製品化と導入にはその性能だけでなく、操作性やコストなどの課題を今後クリアしていく必要がある。

研究開発終了後、以下の用途での事業化に向けた取り組みを実施している。これらのの実用化に向けて、開発した解析装置や技術のさらなる品質の向上、ユーザインタフェースの改良、コスト削減も重要な課題として、引き続き検討を重ねている。

（１）IC カードの安全性評価

従来の電磁波解析攻撃では平均化された暗号デバイス全体の電磁波を統計解析し、その安全性を数値として評価していたが、本事業で開発した高利得・高分解能・高精度な磁界計測により、漏えい情報を含む電磁波を直接、二次元イメージとして評価することが可能となる。また、それにより IC カードチップの中で脆弱な場所を特定し、対策を取ることが可能となる。暗号デバイスの物理安全性に関して標準化が進められて ISO/IEC17825（暗号モジュールに関するセキュリティ要求事項）では、鍵や入力データを自由に換作するホワイトボックス評価が導入される見込みである。この考えに基づいてレジスタのスイッチングを大きくするデータを入力し、それによる磁界強度の変化を観測・評価するための差分解析ツールの開発も行われている。さらに、新規の電磁波解析攻撃手法と高性能プローブを用いた局所磁解析手法は、IC カードの安全性解価において高いアドバンテージを有する日本の技術であり、海外からの期待も示されている。そこで海外の IC カードツールベンダーとも協議を行って事業化につなげていく予定である。

（２）故障解析

情報家電の安全性という意味ではセキュリティを含むシステムデバイスの信頼性の向上も重要な課題となる。高集積化が進むシステム LSI ではチップを積層する技術開発が進められているが、故障やエラーが発生したときにその物理的な原因を特定するにはチップを分解して内部を観測する必要がある。したがって従来のレーザーや電子ビームを用いた解析手法では、チップを動作させながら不具合を調べることが困難であった。これに対し、本事業で開発した故障解析技術はシリコンを透過する局所的な磁界を利用するため、積層 LSI を動作させながらの解析が可能となる。この技術に関しては、すでに国内半導体メーカーのメモリ開発部門とのコンタクトを実施してい

る。

（３）車載ネットワークのセキュリティ

システムのセキュリティに関しては、様々な制御 LSI や電子デバイスが接続される車載ネットワークへの利用が重要視され始めている。現在、電磁波解析技術に関してカーエレクトロエクスメーカーとの共同研究を実施中である。

（４）模造品対策

オプション部品、中古部品の模倣品被害が拡大しており、本事業で昨年度に産総研が開発した LSI のばらつきを利用した真贋判定技術を含めた研究を継続していく。しかしながら、模倣品対策を LSI 識別技術だけでカバーすることは困難である。また LSI だけでなく、食品、医薬品、そして様々な家電製品のコピー品が新興国から出回り、その対策としてトレーサビリティの国際標準化や RFID タグの利用が検討されている。そこで、半導体業界団体の semi や JIPDEC、そして RFID タグを製造・販売する IC カードベンダーと協力しながら、本事業の真贋判定技術を含めたトータルな模倣品対策技術に取り組んでいく予定である。これについてはデンソーと車載部品の真贋判定について共同研究を実施中である。

４－２－ａ　波及効果

本研究開発成果は、上述の通り、製品の安全性検証や不正回路の検出のみでなく、経年劣化による動作異常や模造品の検出にも応用可能であるなど、幅広い波及効果が期待できる。

図ａ－８　本研究開発成果による波及効果

また､本研究においてプローブLSIの開発は､時限の研究員が主に担当していたが､その成果が高く認められたことで東京大学の助教職に就いており､その研究の延長として本システムで得られた高精細データから回路の内部動作を推定する手法の研究を行っている｡電磁波の研究は従来､EMC/EMI を中心とする高周波帯(GHz)のノイズ解析が主体であった｡これに対して本研究は､低周波帯(MHz)の微弱な電磁波に注目し､それを情報として捉え解析するもので､電磁波の研究分野における新しいテーマとなっている｡

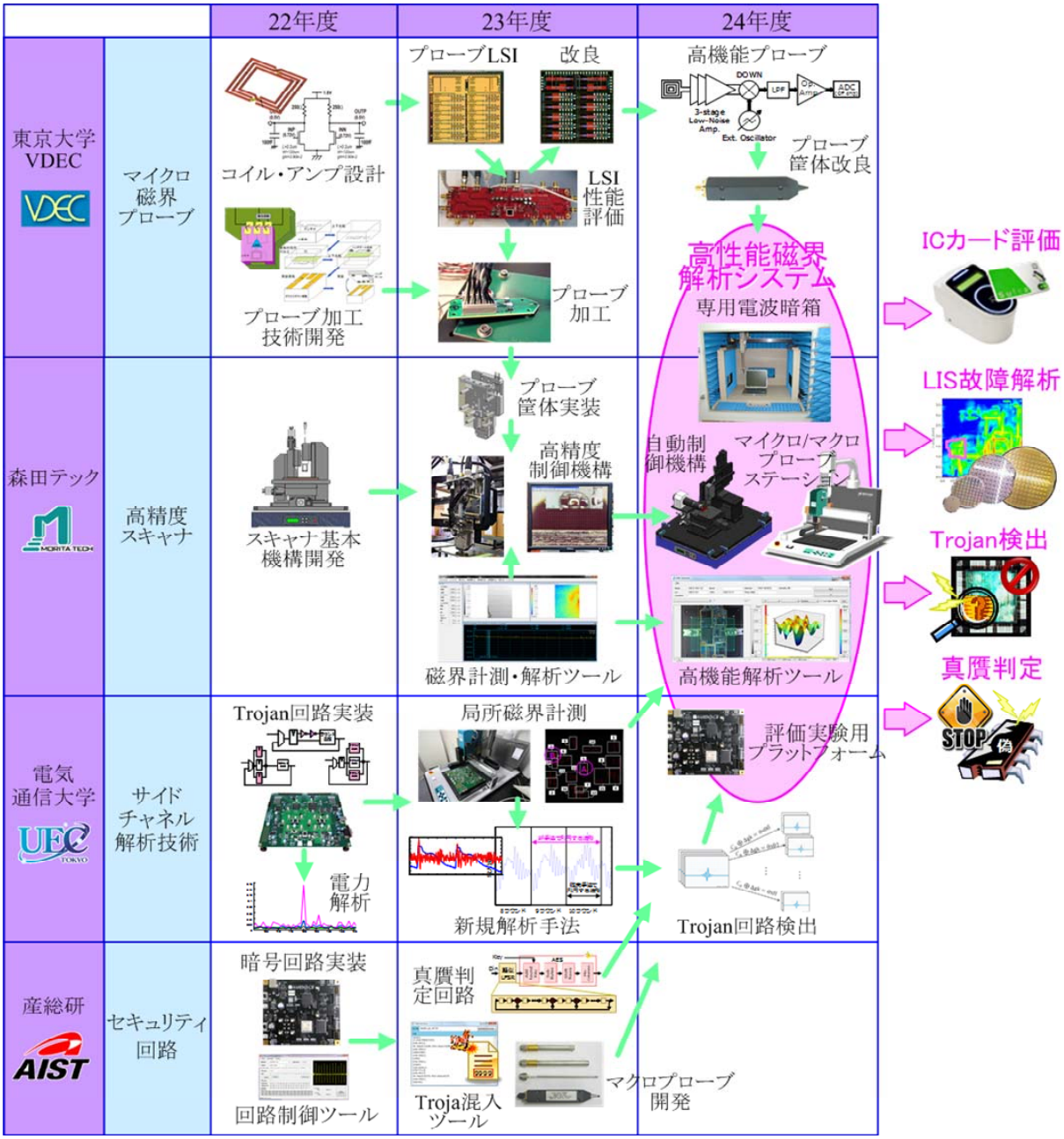
このほか､本研究を通じて改良を重ねた磁界計測システムにより､従来にない高詳細なLSI の磁界マップが得られ､不正回路や攻撃による異常の検知､情報漏えい検出だけでなく､LSI の故障解析､特に多層集積LSI の動作解析等の市場にも活用が期待される｡しかしながら､校正や操作に技術が必要とされ､GUI の改良､そして製造コストの削減などの課題を残している｡これらの課題が解決されたならば､得られる磁界マップはCAD レイアウト情報との高い一致性が確認されたことから､その情報を有するLSI 開発者は､セキュリティのリスクが高いであろう場所（たとえば暗号回路における鍵ストレージや､そのデータが入力されるゲート）を注視した電磁波計測が容易に行えるようになる｡これによりLSI をブラックボックスとして大きな径の磁界プローブで漏えい情報の有無を検査していた従来方法と比べ､数段高い精度でかつ短い検査時間でセキュリティのリスク評価が可能になると考えられる｡

５－ａ　研究開発マネジメント・体制・資金・費用対効果等

５－１－ａ　研究開発計画

本事業は、平成 22 年度から 24 年度までの 3 年計画で実施された。各要素技術の研究開発計画は次のとおりである。

表ａ－４　研究開発計画



実施にあたっては、数ヶ月ごとに事業者全員が集まって進捗状況の報告を行うだけでなく、メールや電話でも密にコンタクトを取りながら分担者間の歩調をそろえ、問

題が生じた場合には適宜アクションプランを取り、事業実施を円滑に進めるよう努めた。

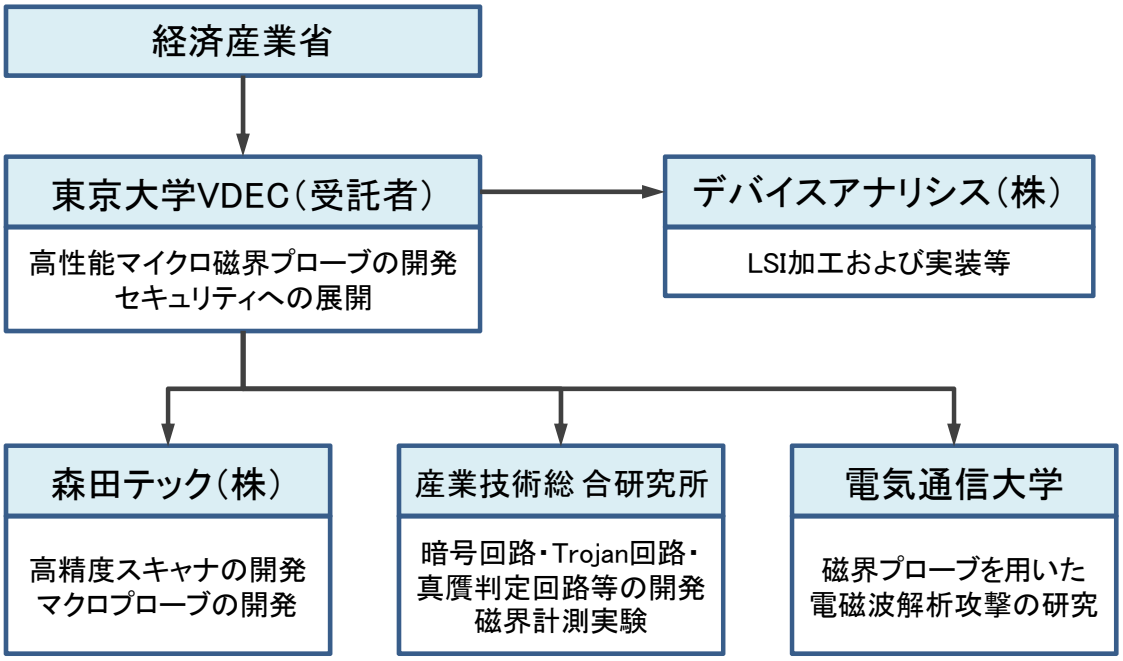
問題点としては特に初年度の予算執行の遅れから、機材や部品などの調達が間に合わないものがあった。そこでスケジュールを見直し、開発項目の順番の入れ替えを適宜行い、全体としての遅れや予算執行の無駄が生じないよう工夫を行った。

５－２－ａ　研究開発実施者の実施体制・運営

本事業は、平成２２年度から平成２４年度において、経済産業省から東京大学への委託により実施されている。また各年度につき、再委託先として以下の機関が事業に参加した。

各実施者は、マイクロ磁界プローブ、高精度スキャナ、解析技術、セキュリティ回路、とそれぞれの得意とする技術を分担し、それらを融合するために互いの役割を理解しながら適切な研究開発を行った。その結果、従来にない高精細な磁界計測システムを実現することができた。

また最終年度、産総研が組織変更により本事業を離脱することとなったが、産総研の研究代表者が東京大学の立場として継続参加するとともに、その研究を残りの実施者が責任を持って分担・継続することで適切な体制を維持することができた。



図ａ－９　研究開発実施体制

５－３－ａ　資金配分

産総研の離脱により、予算に関しても変更が必要となったが、当初の目標を達成するために計画を見直し、適切な再配分を行い、無駄のない執行を行った。また、LSIの開発・製造・試験には大きな予算と長い期間が必要となるが、この種の研究としては大幅なコスト削減と効率化に努めた。

表ａ－５　資金配分　　(単位百万円)

要素技術	平成22年度	平成23年度	平成24年度
高度電磁波解析技術によるLSIのセキュリティ対策に関する研究	32.9	52.7	52.7

５－４－ａ　費用対効果

現在のところ、本成果に基づく製品の販売には至っておらず、本成果に基づく直接的な売上等の発生はない。しかしながら、世界最高水準の高精度電磁波解析システムを開発し、高レベルの解析が可能であることを学会発表等を通じて公表したことは、ハードウェアレベルの脆弱性を悪用する攻撃やＬＳＩの偽造等の抑止に効果を発揮しているものと考えられる。このため、本事業終了後も、これらの実用化に向けて、開発した解析装置や技術のさらなる品質の向上、ユーザインタフェースの改良、コスト削減も重要な課題として、引き続き検討を重ねている。

５－５－ａ　変化への対応

本研究テーマに関連する論文発表について継続的な調査を行ったが、競合する発表は実施期間中になかったことから、大きな見直しを行っていない。

Ａ－ｂ　情報家電、スマートグリッド、携帯端末など、非 PC 端末における未知脆弱性の自動検出技術に関する研究

１－ｂ　事業の目的

近年インターネットに接続するデバイスの多様化が進んでおり、情報家電や制御システムなど様々なデバイスがインターネットに接続されるようになっている。しかし情報家電等はこれまでオープンなネットワークに接続してこなかったことから、情報セキュリティ対策が不十分な場合が多く、対策が急務となっている。

こうした状況を踏まえて、セキュリティ脆弱性を自動検出するための技術を研究開発する。未知のセキュリティ脆弱性を発見する技術は世界的にも研究途上であり、主にセキュリティ研究者の一部が保持する特殊な技術となっているが、研究成果をツール化することにより、一般の開発現場で手軽に脆弱性を発見することが可能となる。

２－ｂ　研究開発目標

情報家電など、非 PC 端末における未知脆弱性の自動検出を行うことが可能なファジング方式のセキュリティ検査ツールの開発・評価を行うとともに、ツールで検査可能な機器と脆弱性の対象範囲の拡張を図る。

これまで脆弱性発見技術は一部の専門家が有する特殊技術という扱いがなされているが、今後共通のアーキテクチャで構成されるパーソナルコンピュータ以外の機器として、情報家電や携帯端末、スマートデバイスや制御機器等、多様なアーキテクチャの製品がインターネットに接続されることを踏まえると、より多くの技術者が脆弱性を発見できるようにする必要があり、脆弱性検出の作業を容易にする技術には高いニーズが見込まれる。加えて、日本国内における技術開発であり、国内で将来的に登場・普及するプロトコルに対しても柔軟に対応できるため、脆弱性発見の技術を他国に依存するような状況が生ずるのを回避することができる。

各年度の目標は次の通りである。

① 平成２２年度

- 特別な知識を有しない一般的な技術者であっても、脆弱性発見のために必要な操作ができるようにするため、本研究開発で用いるファジングによる検査を行うためのデータ定義を行う言語仕様を開発するとともに、このデータを用いてファジングを行うエンジンを開発し、検査対象のプロトコルに対応したルールを作成することで、評価を行えるようにする。

② 平成２３年度

- エンジンの機能追加により、ミューテーションファジングを行えるようにするとともに、Android のアーキテクチャや制御システムで用いられるアルゴリズムを対象とした検査を行えるようにする。

- ルールの追加開発を行うことで、情報家電、モバイル端末、スマートメーターで利用されるプロトコルの検査を可能とする。

③ 平成２４年度

- エンジン群の追加開発として、前年度に開発したミューテーションファジング機能について、ブロックソート式、統計に基づくデータ生成方式、オートマトン方式及びバイナリツリー方式の４種類のアルゴリズムへの対応を行うとともに、Android 以外のモバイル OS や制御システムの脆弱性発見手法に関する調査を実施し、制御システム向けの情報セキュリティ機能に関する認証制度である EDSA 認証を取得する。
- 前年度にネットワーク機器及び情報家電を対象とするルールの作成と評価が進捗した一方で、スマートメーターや制御システム向けのルール作成及び評価が滞っていたことを踏まえ、スマートメーター及び制御システム向けのルール作成、及び評価を重点的に実施する。

表ｂ－１　個別要素技術の目標

要素技術	目標・指標	妥当性・設定理由・根拠等
ファジングベース開発	・ファジング定義言語の開発	特別な知識を有しない一般的な技術者であっても、ファジングデータを容易に定義できるようにするため、YAMLフォーマットベースのファジング定義言語を設計し、その定義言語を用いてルールファイルを作成することによって、ファジングデータを定義できるようにする。 （平成22年度）ファジング定義言語の開発
ファジング開発・実装	・基本エンジンの開発 ・エンジン群の追加開発	開発したベース技術をもとに、既存の機器を対象に評価を行い、有効性を検証する。さらに、海外で注目されているミューテーションファジング技術を利用するためのプロトタイプを作成し、効果測定を兼ねた評価を行う。 （平成22年度）基本エンジンの開発 （平成23～24年度）エンジン群の追加開発
ファジングルール追加実装	・ベースルールの開発 ・情報家電、モバイル端末、スマートメーター専用ルールの開発 ・EDSA認証の取得	モバイル機器で用いられるAndroid OSやWindows Phone 7、ならびに制御機器で用いられているプロトコル等に対応するとともに、制御システム機器及びその評価ツールを対象とするEDSA認証を取得し、制御システムベンダにおける活用性に配慮する。 （平成22年度）ベースルールの開発 （平成23～24年度）情報家電、モバイル端末、スマートメーター専用ルールの開発

３－ｂ　成果、目標の達成度

３－１－ｂ　成果

（１）成果

情報家電、モバイル端末、スマートメーターを対象にファジングによる自動検査を行う機能の開発を実施した。３年の開発期間中に、対象機器の拡大、ミューテーションファジングへの対応等の機能強化を実施している。さらに、社会的なニーズに対応するため、制御システム向けの検査機能を実現した。年度別の成果は以下の通りである。

① 平成２２年度

- 日本国産のファジング技術を用いた製品が、実施機関による組込機器向けの FFR Raven しか存在しない中、多様な検査対象に対応可能な本研究成果をファジング用エンジンとして実装し、FFR Raven への統合を実現した。
- 特別な知識を有しない一般的な技術者であっても、ファジングデータを容易に定義できるようにするため、YAML フォーマットベースのファジング定義言語を設計し、その定義言語を用いてルールファイルを作成することによって、ファジングデータを定義できるようにした。ファジング定義言語を利用したルールファイルを採用することにより、新しいプロトコルを追加する際にファジングパターンのコーディングや再コンパイルをする必要はなく、ルールファイルをテキストエディタで編集するだけで対応可能という利点がある。
- 実施計画書で定めたプロトコルに加え、GIF、Flash に対応するなど、以下に示す多様なプロトコルに対応するルールファイルを作成した。
  - IPv4
  - IPv6(ICMPv6 含む)
  - TCP
  - UDP
  - ICMP
  - IPsec
  - SMB
  - SSL
  - GIF
  - Flash
- 評価用機材の調達を行い、開発したファジング技術の評価を実施した。その結果、50 超のネットワーク機器の検査を実施し、うち 10 機種以上について機器の停止、リセット、通信障害の発生等の問題を発見した。このほか PC 向けの Windows 7 についても IPv6 に関する未知脆弱性を発見した。
- バンクーバー（カナダ）にて開催された CanSecWest にて研究成果の発表を

行った。その結果、海外の大手ソフトウェアベンダ、セキュリティベンダ等では、ルールによらず動的にファジングデータを生成するミューテーションファジングに関する研究開発が注目されていることを認識した。

② 平成２３年度

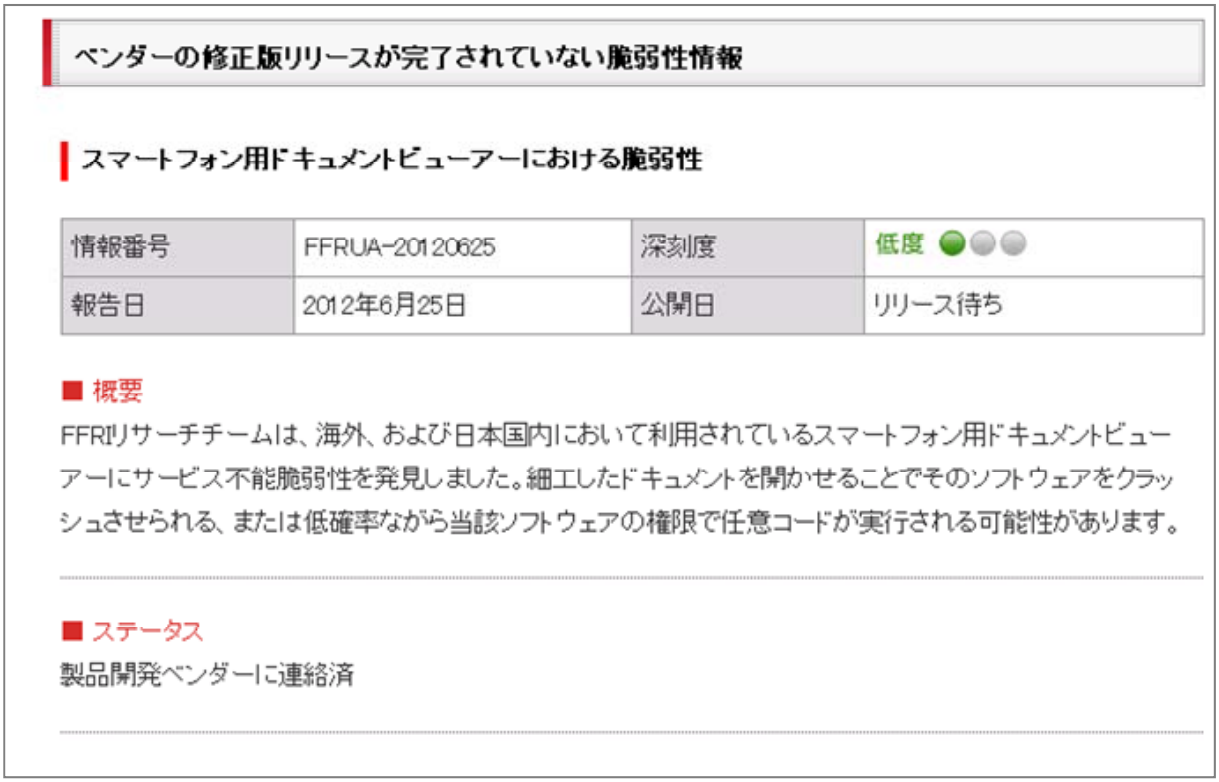
- ミューテーションファジングに関するプロトタイプの研究開発を実施した。17 種類のミューテーションアルゴリズムの実装を行い、効果測定を兼ねた評価を実施した。
- 従来のファジングがサーバアプリケーションを想定した検査手法であったのに対し、スマートフォン等の端末を主たるターゲットとして、ネットワーク越しに他の端末からの接続を待ち受け、その返信としてエラーの発生し得るパケットを送信するクライアントファジング機能を開発した。これは、Android2.1 及び iOS4.3 以降のスマートフォンに搭載されたウェブブラウザの検査を可能とするものである。
- 情報家電、モバイル端末向けファジングパターン用ルールとして、クライアントファジングパターンを開発した。一方で、スマートメーター向けについては当年度に評価を行うことができず、次年度に実施することとなった。
- Android 端末の脆弱性の発見手法の確立のため、そのシステムや現実に行われている脆弱性攻撃について調査研究を実施した。その結果、判明した Android 特有の構造上の弱さ等について国内外のセキュリティカンファレンスにて成果発表を行った（調査報告書３本、講演５回）。
- 平成 23 年度に経済産業省において実施された制御システムセキュリティタスクフォースにおいて求められていた検査ツールとして提案可能なツールの研究開発として、実現性の調査、検証の観点から制御システムで利用されているプロトコルである DNP3、Modbus/TCP について仕様を調査した上で、これらに対応するファジング機能を開発するとともに、横河電機、日立製作所の協力のもと、制御システム向けの検査パターンの開発を行った。
- 以下の自動検査機能を開発し、検査手順の短縮化を実現した。
  －ファジング対象プロトコル自動検出機能
  －問題を引き起こすパケットの自動特定機能
  －ファジングパケット再生機能
- これまでに開発した各種ファジング方式及び制御システム向けの検査機能を用いて、28 種類の評価機器を用意し、機能と効果についての評価を実施した。この結果、クライアントファジングにより 9 件、ミューテーションファジングにて 2 件の問題を発見した。制御システム向けの検査機能についても、1 件以上の問題を発見した。

③ 平成２４年度

- 前年度に開発したミューテーションファジングがゼロ知識ベースであったのに対し、ある程度フォーマットに依存した形式によるミューテーションファ

ジングの効果について検討を行った。

- Android 以外のスマートフォン向け OS として、Windows Phone 7 プラットフォームに対するセキュリティ評価を実施し、結果を BlackHatUSA 2012 にて発表[1]した。
- スマートフォン用ドキュメントビューアに脆弱性を発見し、ベンダに連絡済みである（下図）。



ベンダーの修正版リリースが完了されていない脆弱性情報

スマートフォン用ドキュメントビューアーにおける脆弱性

情報番号	FFRUA-20120625	深刻度	低度
報告日	2012年6月25日	公開日	リリース待ち

■ 概要

FFRリサーチチームは、海外、および日本国内において利用されているスマートフォン用ドキュメントビューアーにサービス不能脆弱性を発見しました。細工したドキュメントを開かせることでそのソフトウェアをクラッシュさせられる、または低確率ながら当該ソフトウェアの権限で任意コードが実行される可能性があります。

■ ステータス

製品開発ベンダーに連絡済

図ｂ－１　発見された脆弱性

https://www.ffri.jp/cgi-bin/advisory/advisory.cgi?type=upcoming&id=FFRUA-20120625

- 情報家電、モバイル端末向け専用ルールとして DLNA（Digital Living Network Alliance）でのデバイス探索プロトコルのルール作成及びファジングアルゴリズムの追加を行った。
- 新たに作成したファジングルールとアルゴリズムを用いて、情報家電（HDD 内蔵テレビ、ブロードバンドルーター）の検査を行った。
- 制御システム向けの検査機能として、EDSA に準拠したツールの研究開発を実施し、必要な機能を実装したツールの開発は完了したが、研究開発期間中に認証を取得することはできなかった。

[1] https://media.blackhat.com/bh-us-12/Briefings/Oi/BH_US_12_Oi_Windows_Phone_Slides.pdf

（２）特許・論文等の状況

本研究開発の成果をもとに出願した特許、発表した論文等は次の通りである。

表ｂ－２　特許・論文等件数

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
0	0	0	0	0	0	0

情報セキュリティ関連の対外発表を次の通り行った。

- Nicholas Green, GRAPE: Generative Rule-based Generic Stateful Fuzzing, CanSecWest 2011.
- Inside Android Security, ホワイトペーパー。 http://www.ffri.jp/research/research_papers.htm
- How Security Broken, PacSec2011.
- ～とびらの向こうに～ S10 スマートフォンセキュリティ, Internet Week 2011.
- Tsukasa Oi, Yet Another Android Rootkit, Black Hat Abu Dhabi 2011.
- Inside Android Security ～内部構造から探る Android のセキュリティ機構と脅威の実態～, ITPro EXPO 2011.
- Tsukasa Oi, Windows Phone 7 Internals and Exploitability, Black Hat USA 2012.

３－２－ｂ　目標の達成度

本研究開発に関する目標に対する達成度は次表の通りである。ファジング定義言語において、仕様で求められた以上の多様なプロトコルに対応したほか、情報家電、スマートフォン等で未知脆弱性を発見するなどの成果を得た一方で、制御システム向け検査機能において目標としていた EDSA 認証の取得を研究開発期間内に実現することはできなかった。

表ｂ－３　目標に対する成果・達成度の一覧表

	目標・指標	成果	達成度
ファジングベース開発	・ファジング定義言語の開発	・以下のプロトコルに対応するルールの作成と整備を実施した。 （一般ネットワーク機器向け）IPv4、IPv6、ICMPv4、ICMPv6、TCP、UDP、IPSec、SMB、SSL、GIF、Flash、UPnP等 （制御機器向け）DNP3、Modbus/TCP	達成
ファジング開発・実装	・基本エンジンの開発 ・エンジン群の追加開発	・評価用機材の調達を行い、上記ルールを用いた評価を実施した結果、50超のネットワーク機器の検査を実施し、内10以上の機器について機器の停止、リセット、通信障害の発生等の問題を発見した。 ・ミューテーションファジングのアルゴリズムとして、ゼロ知識ベースとフォーマットに依存するものの2種類を評価し、DNLA向けのルールを作成した。	達成
ファジングルール追加実装	・ベースルールの開発 ・情報家電、モバイル端末、スマートメーター専用ルールの開発 ・EDSA認証の取得	・AndroidとWindows Phone 7向けの検査手法を開発し、評価を実施した。この結果、未知脆弱性1件を発見し、製品ベンダに連絡した。 ・スマートメーター用専用ルールを開発した。 ・EDSA認証に対応する制御システム向け検査ツールを開発したが、研究開発期間中の認証取得には至らず。	概ね達成

４－ｂ　事業化、波及効果について

４－１－ｂ　事業化の見通し

本研究開発成果は実施機関が自ら企業向けに提供する製品・サービスにおいて活用している。以下にその例を示す。

（１）組込み機器向け脆弱性検査ツール：Ｒａｖｅｎ

http://www.ffri.jp/services/android/

図ｂ－２　FFR Raven

（２）Android 端末セキュリティ分析サービス

http://www.ffri.jp/services/android/

図ｂ－３　Android 端末セキュリティ分析サービス

（３）制御システム向け

制御システム向け検査ツールに関しても、FFR Raven for ICS として製品化が完了している。EDSA 認証取得プロセスも完了予定である。

４－２－ｂ　波及効果

本成果による波及効果は次の通りである。

- 本成果を反映した実施機関の製品は、従来のファジング用ツールと比較して安価な価格設定を行っており、ユーザは低コストで脆弱性評価を行うことが可能である。
- 実施機関は日本国内でサービスの開発と提供を行っているため、海外の類似製品と比較して、今後も日本で広く用いられている情報家電、モバイル端末、スマートメーター、制御システム等への対応が行われやすくなる効果が期待できる。
- 研究開発の結果を国際会議にて成果発表を行うことで、我が国における脆弱性検査能力を国際的にアピールすることができた。
- 本事業にて研究開発した検査機能の評価の過程にて脆弱性を発見し、独立行政法人情報処理推進機構（IPA）を通じて機器メーカーへの報告を実施した。
- 制御システムに対応し、EDSA に準拠する検査機能の研究開発を行い、日本における制御システムセキュリティの活動に貢献した。

５－ｂ　研究開発マネジメント・体制・資金・費用対効果等

５－１－ｂ　研究開発計画

本事業は、平成 22 年度から 24 年度までの 3 年計画である。各要素技術の研究開発計画は次のとおりである。平成 22 年度は契約締結後の年度内作業期間が短期となり、また震災の影響もあり研究開発に支障を生じたが、これについては柔軟に研究者のアサインを調整することで対応を行った。

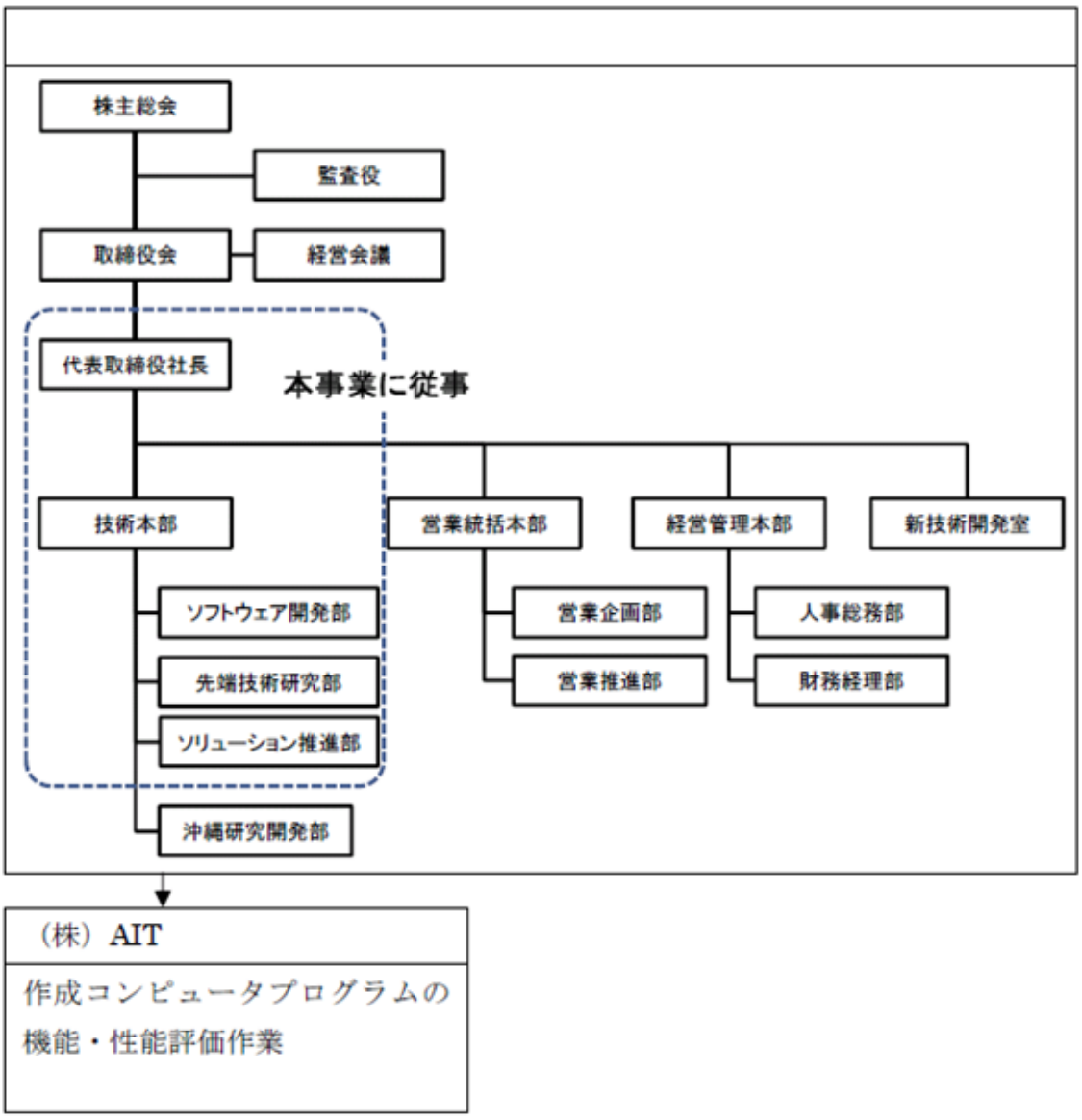
これ以外については、概ね予定通りの対応を行うことができた。

表ｂ－４　研究開発計画

年度	平成22年度	平成23年度	平成24年度
予算額	24.7百万円	23.1百万円	20.5百万円
ファジングベース開発	ファジング定義言語開発		
ファジング開発・実装	基本エンジン開発	エンジン群 追加開発	エンジン群 追加開発
ファジングルール追加実装	ベースルール開発	情報家電、モバイル端末、スマートメーター専用ルール開発	

５－２－ｂ　研究開発実施者の実施体制・運営

本事業は、平成 22 年度から平成 24 年度において、経済産業省から株式会社フォティーンフォティ技術研究所への委託により実施された。また再委託先として以下の機関が事業に参加した。



図ｂ－４　研究開発実施体制

５－３－ｂ　資金配分

本研究開発における資金配分の状況は下表の通りである。本研究開発においては、情報家電、携帯機器、スマートメーター、制御機器等の調査を行うにあたり、ベンダからの貸与が期待できないものについては資金内で調達を行う必要があり、多くの機器に対応しようとすると膨大なコストを要してしまう。そこで、研究開発成果の評価において妥当な評価を行うため評価対象機器について種別、開発ベンダ規模、OS、対応プロトコル等の様々なクライテリアに基づいて分類を行い、脆弱性発見の評価に最適と考えらえる機器構成とした。

表ｂ－５　資金配分　　(単位百万円)

要素技術	平成22年度	平成23年度	平成24年度
情報家電、スマートグリッド、携帯端末など、非PC端末における未知脆弱性の自動検出技術に関する研究	**24.7**	**23.1**	**20.5**

５－４－ｂ　費用対効果

成果を組み込んだ製品の売上は、研究開発への投入費用に達するものとはなっていない。しかしながら、本成果による効果は、成果を活かした製品・サービスを導入したベンダにおいて、少ないコストで効率的に脆弱性を発見できるという生産性の向上にある。

旧来のファジングツールでは、テストパターンの膨大な組み合わせについてデータを生成し、検査を行っていた。この場合、効率的なテストが実施できないだけでなく膨大な検査時間が必要となる状況であった。本研究開発では、脆弱性の発見手法から研究を行うことで、脆弱性が埋め込まれやすいパターンを精査することで、テストパターンを限定した。これにより、効率的な検査を短期間で実施することが可能となった。

５－５－ｂ　変化への対応

非 PC 端末の最新の状況に対応するため、対象機器として Android OS や Windows Phone 7 を用いるモバイル機器を追加し、評価を実施した。

さらに、制御システムに対するセキュリティ対策の機運の高まりから、それに関連した研究開発の比重を高めた。

② アクセス制御技術の研究開発

Ａ－ｃ　プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究

１－ｃ　事業の目的

情報セキュリティに深く関わる価値観としては、自由、安心・安全、プライバシー保護の三者が重要であるが、この三者は、互いに矛盾・相克する場合が多い。管理経営、倫理、法制度、技術、即ち Management、Ethics、Law and Technology（MELT）を密結合・強連結させ、融合（MELT）させて、自由、安心・安全、プライバシー保護という相克しがちな三者の関係を止揚することが要請されている。本研究開発は、クラウドに個人情報や機密情報が暗号化されて保管・預託される環境が増える中で、効率性、安全性の面から、暗号化した状態のままで、加算・乗算を含む統計処理や、サーバー管理者に知られることなく個人情報や機密情報の検索を行いたいという要請に応える。

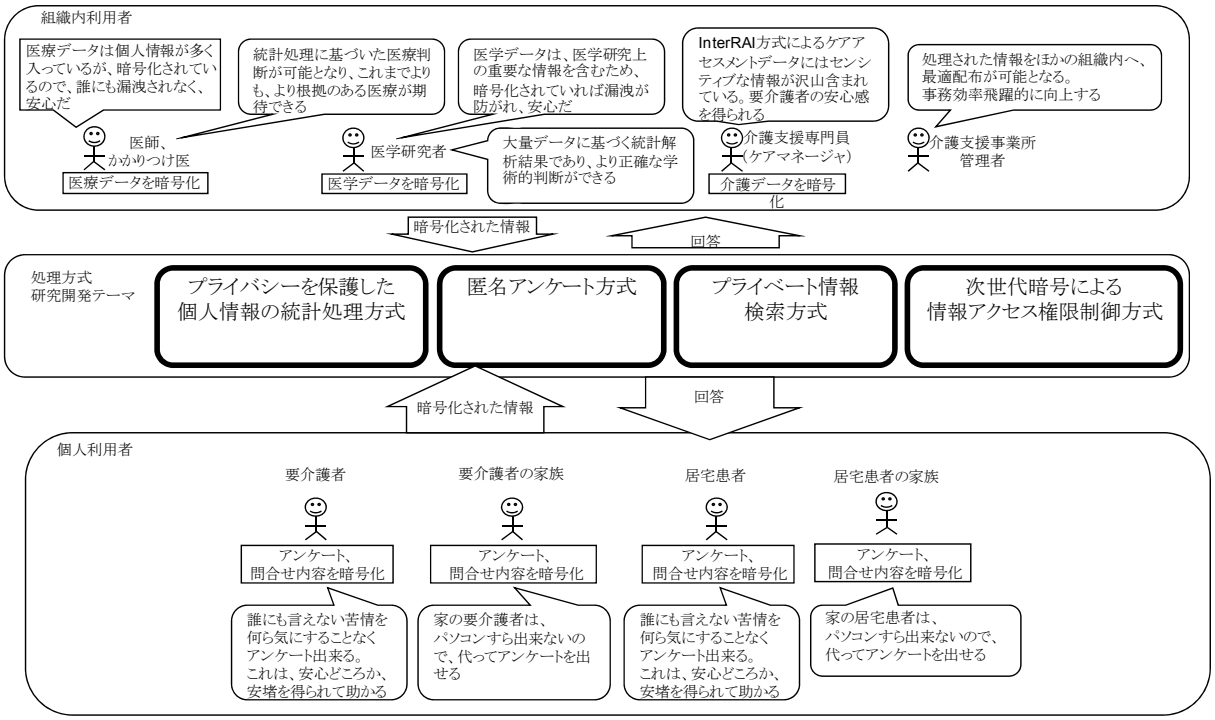
２－ｃ　研究開発目標

本事業では「個人情報を秘匿したまま収集、処理、活用する医療・介護連携ネットワーク」を実現するため、以下の研究開発テーマを実施する。

表ｃ－１　個別要素技術の目標

要素技術	目標・指標	妥当性・設定理由・根拠等
プライバシーを保護した個人情報の統計処理方式	・機微な個人情報について、秘匿性を保ったまま有効活用するために、必要なプライバシー保護方式及び情報処理方式等の研究開発を行う。	・医療機関が保管する医療や介護における患者の記録などは機微な個人情報であり、これまでプライバシー保護を理由に活用が妨げられた状況にある。
匿名アンケート方式	・オンラインでアンケートを行う際に、回答者の匿名性を担保し、アンケート回答に対する心理的な障壁を低減するとともに、有効な統計情報を抽出して活用するために必要な暗号方式の開発及び性能評価を行う。	・医療、介護等の機微な情報に関するアンケートを患者等に対して実施する場合、匿名性が担保されない可能性への不安などが心理的な障壁として機能してしまうため、アンケート調査を実施しても有効な回答を得にくい状況にある。
プライベート情報検索方式	・情報を検索する際に、当該検索者の個人情報及びその検索内容について秘匿したまま、必要な情報を取得できるシステムを構築するために必要な暗号方式、暗号プロトコル等の研究開発を行い、暗号プロトコル全体のセキュリティと性能を評価し、全体の評価を行う。	・医療・介護に関する情報について、患者や患者の家族が、関連する情報を検索する際に、当該検索者の個人情報及びその検索内容について、サービス提供側に把握されることが懸念されることで、サービスの利用を躊躇する可能性がある。
次世代暗号によるアクセス権限制御方式	・一括して暗号化した個人の様々な医療情報について、職能権限や資格ごとに複数の復号鍵を設定でき、アクセス権限がある情報のみを選択的に復号できる次世代の暗号方式を開発する。	・従来の暗号方式では、アクセス権限ごとに個人情報を複製、分割してそれぞれについて別途暗号化を行うなどが必要であり、管理が必要な情報量の増加、利便性の低下、複製による情報流出のリスクの増大などが懸念される。

これらの目標・指標は、本研究開発が対象とする医療・介護分野におけるニーズとの間に次の関係を有する。



図ｃ－１　本研究開発の目標と医療・介護分野におけるニーズとの関係

本研究開発では平成２２年度に、「平文へ戻すことなく加減乗除の演算が可能なセキュリティ方式を開発する」という、当時まだ現実的なシステムリソースで現実的な時間内に行うことは不可能とされていたことを、通常のサーバー程度のスペックで実現可能とすることを目標にした。これは当時の技術開発の状況では非常に野心的な目標であった。

各年度の詳細な目標は次の通りである。

① 平成２２年度

【プライバシーを保護した個人情報の統計処理方式の研究開発】

- 本研究開発で用いる暗号方式と個人情報の統計処理方式について、調査をもとに比較を実施し、採用すべき方式の選定を行う。また、複合化部分を IC カードに実装できるかどうかをシミュレーションと実験により決定するため、候補となる暗号化方式すべてについて試験と評価を行う。

【匿名アンケート方式】

- プライバシー保護のために用いる見込みの二重化暗号方式について、他方式に対する優位性があることを確認するとともに、医療・介護現場で実施するアンケート／サーベイにに適しているかを調査する。調査においては、暗号プロトコルとしての計算量、処理性能について、候補となる暗号方式を対象に比較評価する。
- 開発した匿名アンケート方式については、技術的安全性やコンセプト及び既

存手法に対する優位性などの外部評価を受けるため、国際学会での発表や査読付き論文への投稿を行う。さらに、２重化暗号方式において利用する暗号方式を、性能と安全性を比較することによって選定する。

【プライベート情報検索方式】

- 候補方式について、シミュレーションと実験による予備試験で構想通りの機能が期待できるかを確認した上で、検索指示内容秘匿方式の基本方式を決定する。開発した秘匿方式については、適宜、国際学科等への発表を行い、客観的にその安全性や実現性について、外部の専門家から評価を受け、その結果を基に見直しを行う。
- 求められるセキュリティ強度と処理を行う際の効率を判断基準として、検索指示内容秘匿方式について、暗号処理性能及び暗号プロトコル処理性能について比較し、基礎情報を決定する。

【次世代暗号によるアクセス権限制御方式】

- 情報アクセス権限制御基本方式について、多変数公開鍵暗号方式を秘匿に利用する基本構成方式を検討する。順序解法方多変数公開鍵の発展型であるSTS（Stepwise Triangular System）構造を基本とし、開発する暗号方式の安全性の検討を行うとともに、現在数多く提案されている類似の機能を有する暗号方式との安全性及び効率（鍵サイズや暗号・復号の性能など)、及び実装されたシステムの医療現場での運用可能性について比較検討を行う。開発した資格適応型暗号方式については、適宜学会発表や、査読付き論文への投稿などにより、産業界及び学会の外部の専門家から安全性評価の妥当性、及び実装上の問題などのコメントをいただき、方式案の見直しに活用する。

② 平成２３年度

【プライバシーを保護した個人情報の統計処理方式の研究開発】

- 昨年度絞り込んだ以下の３方式をもとに、基本方式を決定する。
  －準同型暗号関数を用いた情報秘匿方式（辻井方式）
  －中国人剰余定理を利用した秘密分散方式
  －第三者的監視機関の存在を前提とした秘密分散プロトコル方式
- 上述の方式で用いる第三者監視機関について、社会的必要性や社会的実装の可能性を悪鬼らかにするため、海外先行例の調査を行うとともに、第三者監視機関を前提とする個人情報取り扱い管理制度の案を作成する。また、他方式を用いる場合に必要な性能を得るために、方式とパラメータ、及び計算能力に関する検討を行う。具体的には Pailler 暗号、ElGamal、RSA について、実装性からの試験と評価を行う。
- 上記の実施を通じて、以下の成果を得る。
  －最終的に採用される個人情報保護方式（１つに定まるとは限らない)、及び条件に応じた方式選定基準
  －与えられた規模での実現に必要なシステム能力及びパラメータの一覧

－個人情報利用に関する管理機関（暗号鍵管理や個人情報利用ログ記録などを行う機関）に関する条件、及び実現可能性に関する調査報告

【匿名アンケート方式】

- 医療・介護における匿名アンケートに要求される秘匿強度とシステム性能の関連を考察する。
- 十分な暗号性能を得るために必要なシステム能力・容量・パラメータなどを検討する。

【プライベート情報検索方式】

- 検索指示内容秘匿方式における基本方式の決定を行うとともに、匿名通信路における各ミックスセンターの処理の正当性検証の方式を考察する。
- 医療分野での Semantic Computing System で実績を有する米国 Biomedical Objects, Inc.と協力して Semanntic 機能記述言語、Semantic 検索記述言語の機能、仕様ならびに Semantic Service Engine の研究を行う。
- 暗号処理性能（秘匿、関数演算等）の基礎情報の決定を行う。

【次世代暗号によるアクセス権限制御方式】

- 前年度に提案した多変数公開鍵暗号の１つである、STS（Stepwire Triangle System）構造を用いた組織対応暗号方式について、専門家が多数参加する国際会議 The Fourth International Workshop on Post-Quantum Cryptography に参加し、セキュリティ及び応用の可能性について議論を行う。
- 多変数公開暗号の解読計算量に関する研究として、様々な解読法に関して漏れなく検証を行う。
- 上記の取り組みを通じて、以下の成果物を得る。
  －組織対応暗号方式、及びそのプログラム実装（数式処理システムまたは汎用プログラム言語）
  －組織対応暗号の実装仕様案
  －多変数公開暗号一般の解読アルゴリズムと汎用解読方式の提案を論文にまとめ、国際的に評価を求めうる形にしたもの

③ 平成２４年度

【プライバシーを保護した個人情報の統計処理方式の研究開発】

- 前年度に引き続き、RSA 暗号によって暗号化状態での乗算を行い、Pailler 暗号によって暗号化状態での加算を行う方式を研究し、個々の個人情報を漏洩することなく、暗号化状態での加算、及び乗算を任意に行うことの可能な方式を完成させる。
- 本方式の発表に際して、電子情報通信学会、暗号とセキュリティシンポジウムで発表した際、個人情報活用期間のゴールが明確ではないとの意見を受けたので、個人情報活用期間の役割をより明確に設定する。この結果を電子情報通信学会の研究会に投稿し、方式及び組織体制について議論を行う。
- 前年度に発表した方式以外で､Oblivious Transfer を用いた別の方式を検討し、

論文誌及び国際学会 Seventh International Conference on Computing, Complexity and Randomness（CCR 2012）に投稿することで、国内外の研究者と方式案について議論し、検討を進める。

- 前年度に研究開発を行ったプライバシー保護条件付情報開示方式について、その発展形として、クラウド上のデータベースの機能を 3 個以上の一般的な場合に拡張するとともに、複数の病院の様々な内容の医療データベースをリンクする機能を実現する。さらに、本方式でプライバシーの保護を実現する基本要素技術において、中核技術になっている Oblivious Transfer を ElGamal 暗号と組み合わせることで、一層の効率化を図る。また、医療・介護連携ネットワークにとどまらず、情報連携基盤での本方式の本方式の本格運用を目指し、情報連携基盤で求められるプライバシー保護に関する様々な制約・要請を満足するよう、改良・効率化及び機能増強を図り、本方式の実用化を行う。実用化案は電子情報通信学会の情報セキュリティ研究会で発表し、広く暗号及び情報セキュリティの専門家からの意見を求める。
- プロトタイプで実装済みの中国人剰余定理による秘密分散保存方式について、実用レベルの運用に向けた性能評価を行う。

【匿名アンケート方式】

- 暗号化、復号処理の正当性検証を行うためのゼロ知識証明法を研究する。また、RSA、ElGamal 公開鍵暗号系の暗号化、復号処理性能、ならびにこれらの公開鍵暗号系を用いたゼロ知識証明法の処理性能をシミュレーションする。
- プロトタイプを作成し、基本論理の妥当性を吟味する。
- 国際会議 IEEE-ICIOS2012（IEEE International Conference of Internet Operating System）に投稿し、同会議において参加者と安全性及び性能について広く意見を求める。
- 本研究成果を医療、介護関係分野に適用、実用化を促すため、研究成果の紹介・意見徴収に努める。

【プライベート情報検索方式】

- システム構成要素の処理として、暗号化、復号処理の正当性検証のためのゼロ知識証明法を研究する。この検証方式案は、国際学会 ATLAS-2012（The Academy of Trans-disciplinary Learning and Advance Studies、於台湾）で発表し、国内外の研究者から広く意見を求め、討議する、また、匿名アンケート方式と組み合わせた全体方式提案を国際学会 The Society for Design and Process Science（SDPS2012）の年次総会で発表し、内容について国内外の研究者と議論する。

【次世代暗号によるアクセス権限制御方式】

- 前年度に多変数公開鍵暗号方式（Multivariable Public Key Cryptsystem, MPKC）が最適であるとの結論を得たのを受け、受信側の様々な組織構造に適応した同方式の階層構造の最適化を行う。

- 素因数分解の困難性に依拠する MPKC 落し戸を用いた暗号方式を国際学会 Third International Conference on Symbolic Computation and Cryptography（於スペイン）にて発表し、その安全性及び効率について議論を行う。
- MKPC を用いたアクセス制御方式について、情報通信及びセキュリティー般を対象とする国際学会で様々な専門を持つ研究者から意見を求めるため、International Symposium on Information Theory and its Applications（ISITA2012）での発表を予定する。
- アクセス制御方式に応用可能な新しい落し戸方式についｔ、安全性や暗号復号の性能評価などの検討を行う。

【プロトタイプ仕様の研究】

- これまで研究してきたプライバシーを保護したままでの統計計算方式やプライバシー保護条件付情報開示方式、アクセス制御方式などをもとに、医療情報システムで用いられる個人情報を保護するセキュリティシステムの仕様案を作成する。
- 検討に当たって、アルゴリズム及び運用方式など全体的な案について、暗号に関する国際会議である AsiaCrypt に参加し、出席者と内容に関する議論を行う。

３－ｃ　成果、目標の達成度

３－１－ｃ　成果

（１）成果

本事業による研究開発成果は次表のように整理される。

表ｃ－２　研究開発の成果

研究テーマ	具体的方式名	特徴	製品化計画	提携企業	学会発表	有識者評価	備考
プライバシーを保護した個人情報の統計処理方式	乱数付加による統計処理秘密分散	超高速、低コスト	YDKによって製品化	InterRAI Organization (ASPICを通して相談予定) YDK, スカパーJSAT(相談中), カナミック, ASPIC	ISITA2012など学会発表12件	山本隆一准教授・理事長「難病患者情報はこの方式が極めて有効」	早急に実用化すべくアプローチ中である。 また、「暗号の社会的利用」フォーラムで社会への提案及び研究開発を行ってゆく予定。
	Paillier暗号を用いた統計処理	高次数の処理も可能					
	プライバシー保護条件付き情報開示	市川市CIOが2010年に要望				堀部教授「電子行政が実現したらすぐ使える」	
プライベート情報検索(PIR)	論理学暗号を用いた自然言語による秘匿検索／Semantic Computing	ヒューマンフレンドリーな操作、自然言語に適した秘匿機能	UCIにてプロトタイプ作成、医学部、バイオ医学部に適用	米国Biomedical Object Inc.	IEEE-ICIOS2012など学会・論文誌発表9件	神戸大森井教授「このような方式は今までになく画期的」	
匿名アンケート方式						Ramamoorthy名誉教授「構造化自然言語機能が加わったことで飛躍的に利用者層が拡大する」	
次世代暗号によるアクセス権制御方式	多変数公開鍵(TSK)暗号による受信組織対応暗号	柔軟性非定常性	フォーラム活動を通じて展開	YDK	SCC2013など学会発表15件	井堀氏「組織暗号無くして電子行政無し」	属性・関数暗号は、固定的

平成２３年度は,「平文へ戻すことなく加減乗除の演算が可能なセキュリティ方式」をデモシステムに実装し、ノートブック PC 上で，かなり現実的な件数のデータの処理を実現した。また、研究課題としていた各テーマについて、計 4 つのデモシステム実装が実現された。これは計画以上の成果である。また、同年度は更に新しい個人情報保護方式「条件つきプライバシー情報開示」を提案している。

各年度の詳細な成果は次の通りである。論文及び学会発表の詳細は後述する。

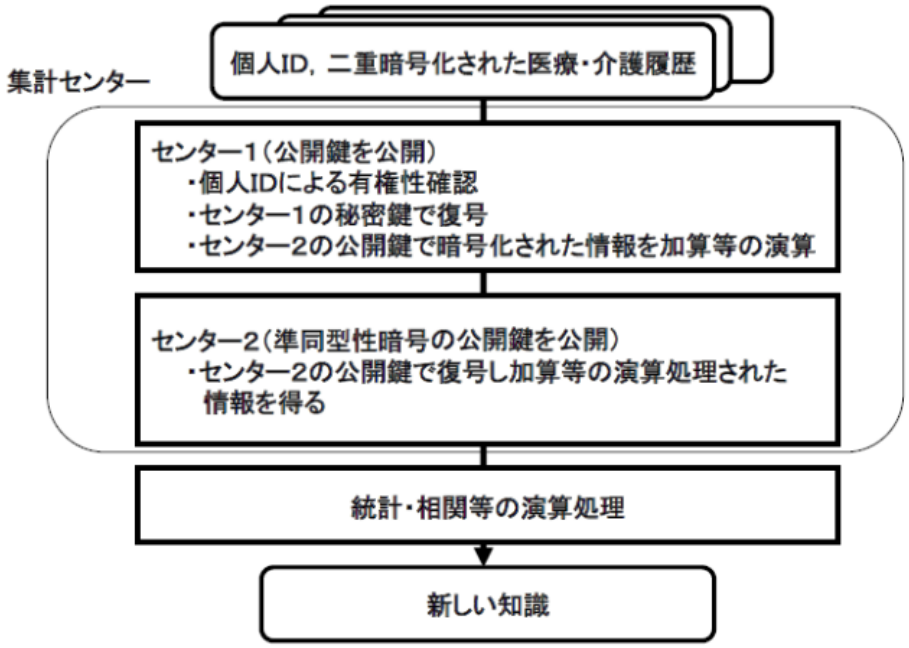
① 平成２２年度

【プライバシーを保護した個人情報の統計処理方式の研究開発】

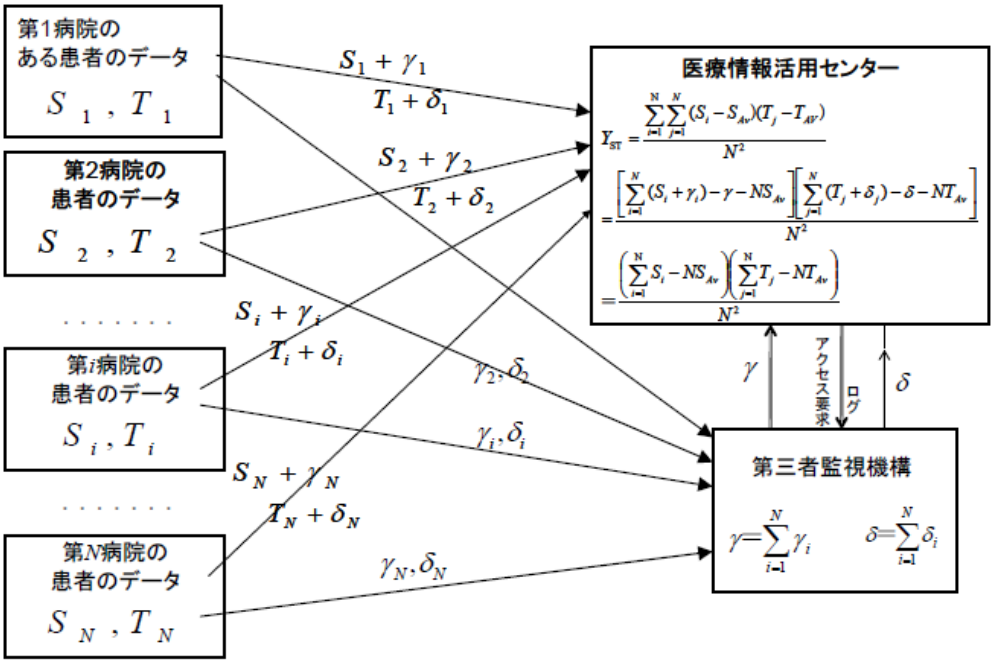
- プライバシーを保護しつつ、個人情報の活用を可能とする方式として、実施機関の研究者が 1998 年に提案した「二重化暗号プロトコル方式」と、「第三者機関を利用して個人情報の保護と活用を図る方式」の２方式について、双方の実現可能性を検証した上で、必要計算処理コスト、正当性照明プロトコ

ルの必要実行数、技術的な難易度等の観点から比較を実施した。

- 上記の２方式はそれぞれ異なる特長を有するため、本年度においてどちらか一方への絞り込みは実施せず、こうした技術の評価に実績を持つ国際医療福祉大学、UCIrvine に成果を紹介し、医療・福祉分野での実用面での評価を行うこととなった。



図ｃ－２　二重化暗号によるプライバシーを保護した個人情報の集計、統計、相関等の演算処理方式



図ｃ－３　第三者監視機構による秘密分散と保護されたままでの演算方式

【匿名アンケート方式】

- 二重化暗号方式について、過去に提案された匿名通信路を使用した方式とブラインド署名技術を利用した方式と比較し、センターの計算処理コストならびにセンターの処理正当性検証のための計算処理コスト、通信コストが少なく優位性があることを確認した。
- 平成２２年度内の国際学会での発表や査読付き論文への投稿は行われていない。

【プライベート情報検索方式】

- 現在のリレーショナルデータベース、XML データベースと同様の検索支持方式が可能でかつプライバシーを保護可能なアプローチとして、ミックスネットと呼ばれる匿名通信路を用いる方式を用いることとし、ビット単位、キーワード単位でのアプローチと比較して、新規性、革新性を満たし、既存論文発表に類似のものが存在しないことを確認した。
- 研究開発成果をもとに、国際会議で発表した。

【次世代暗号によるアクセス権限制御方式】

- 組織から組織への情報授受を意識した、多変数公開鍵暗号方式を用いる方式（組織暗号）を開発した。これは医療機関での実用化を考慮し、暗号化する側は組織の構造や役割分担を意識する必要が無く、組織内の管理者が復号鍵を配布するときにアクセス許可を設定するものである。
- 研究開発成果をもとに、国内研究会、シンポジウムで発表を行った。

② 平成２３年度

【プライバシーを保護した個人情報の統計処理方式の研究開発】

- データ数値を秘匿したままで統計演算処理を行う方法として、乱数を加える統計処理秘密分散方式について、実際に想定される医療情報の利用モデルをもとに必要となる計算量を評価した。また、本方式を Windows 上のデモプログラムとして実装するとともに、Java プラットフォームで動くプロトタイプシステムの構築に向けてライブラリの仕様をとりまとめた。
- 加法と乗法それぞれに同型性を持つ異なる暗号方式を用いることによる、データ数値を秘匿したままで統計演算処理を行うための別方式を考案した。
- 東日本大震災を契機に災害対策についての対応を行うこととし、中国人剰余定理を用いて情報を安全に分散保存できる手法を考案した。実証実験用のソフトウェアを開発して医療用画像の分散保存に要する時間を測定した結果、８秒程度で可能であることを確認した。
- 第三者監視機関による個人情報管理制度に代えて、クラウド対応型暗号化状態処理方式におけるデータセンター・個人情報活用センターの管理手法についての検討を行った。
- 行政の専門家の意見をもとに、プライバシー保護条件付きの情報開示の要件を実現可能な方式を検討した。

- 研究開発成果をもとに、研究会にて発表を行った。

【匿名アンケート方式】

- 意見提供者の意見をアンケートシステムに伝えつつ、しかもその意見提供者の匿名性を保護することが可能な上に、その意見に対する回答も返信できる特長を備えた、ミックスネット通信路に基づく匿名アンケート方式を考案した。
- ElGamal 公開鍵暗号を用いることとし、その処理性能を用いた暗号プロトコルの検討を行った。
- 暗号と暗号プロトコルの処理性能評価において、必要暗号化回数はミックスネット通信路上のセンタ数に依存せず、処理性能の向上が可能である方式を考察した。
- 研究開発成果をもとに、国際会議で発表を行った。

【プライベート情報検索方式】

- 本方式で利用するアルゴリズムを、匿名アンケート・返答方式のアルゴリズムに準じるものに決定した。
- アルツハイマー病患者のデータ検索に関するデモプログラムを開発した。
- 研究開発成果をもとに、国際会議で発表を行った。

【次世代暗号によるアクセス権限制御方式】

- 多変数公開鍵暗号をもとに、暗号化及びアクセス許可定義のプロセスを構築した。
- プロトタイププログラムにより、暗号化・復号速度を評価した。
- 研究開発成果をもとに、研究会にて発表を行った。

③ 平成２４年度

【プライバシーを保護した個人情報の統計処理方式の研究開発】

- 統計処理秘密分散方式を国際学会で発表した。
- Pailler 暗号を用いた方式を国際学会に投稿した。
- 中国人剰余定理による医療画像の分散保存方式について、秘密分散方式を商用レベルへ実装する際のスケーラビリティの検討を行うと共に、本方式の基となるコンセプトとアルゴリズムを整理し、体系立った理論として再構築を行った。
- プライバシー保護条件付き情報開示について、前年度の方式を改良し、マイナンバー精度施行時に効果を発揮する方式を開発し、論文発表した。
  東大情報学環、国際医療福祉大学へ本研究成果を紹介するとともに、スカパーJSAT、カナミックネットワーク、YDK などへ事業提携を提案した。

【匿名アンケート方式】

- プライベート情報検索システムと共通の部分をまとめ、アルゴリズム実装の効率化を図った。

【プライベート情報検索方式】

- 構造化自然言語による検索指示内容を保護するためのセキュリティ技術案を作成、検討した。
- 自然言語による検索内容を的確かつ効率的に保護するセキュリティ技術を検討し、従来のような数学に基づく方式とも言語学に基づく方式とも異なる「論理暗号」を考案した。この方式は、構造化自然言語に変換されたクエリを暗号化し、その内容を保護するものである。

【次世代暗号によるアクセス権限制御方式】

- 前年度に考案した方式案を国際学会で発表し、問題点について多変数公開鍵暗号の権威と議論した。
- 全体の方式案を構築、発表した。
- 組織暗号に応用可能な新しい暗号化方式として、素因数分解の困難性に依拠した秘匿方式を考案し、具体的に方式案を固め、論文として発表した。また、多変数公開鍵暗号だけでなく、既存のものも含めて様々な暗号方式から、組織暗号へ応用できるものを探索し、組織暗号方式の最適化を図った。

【プロトタイプ仕様の研究】

- 以下の機能・方式について、実プログラムへの実装を行った。
  1. プライバシーを保護した個人情報の統計処理方式
  2. 暗号化処理エンジン(性能測定用)
  3. 中国人剰余定理を用いた医療画像の分散保存システム
  4. Semantic Computing Engine による、自然言語を用いた患者データの検索システム
  5. プライベート情報検索方式
  6. 匿名性を維持したままで回答への返信が可能なアンケートシステム
  7. 次世代暗号によるアクセス権制御システム

（２）特許・論文等の状況

本研究開発の成果をもとに出願した特許、発表した論文等は次の通りである。

表ｃ－３　特許・論文等件数

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
37	0	0	0	0	0	0

その他関連する発表実績を次ページ表に示す。

表ｃ－４　発表実績

発表種別	発表件数
論文誌掲載	3 件
査読付国際会議論文	9 件
招待講演	4 件
学術論文（査読無し）	19 件
学会発表（査読無し）	6 件
その他	2 件

論文誌掲載論文

- 平成 24 年度

[1] Jennifer Kim, Phillip C.-Y. Sheu, and Hiroshi Yamaguchi, “Semantic computing and business intelligence,” International Journal of Semantic Computing, 07, 87 (2013).

[2] 只木孝太郎, 土居範久, 辻井重男, “プライバシー保護条件付き情報開示,”電子情報通信学会和文論文誌(A), A, 基礎・境界 J96-A(11), 735-744, 2013-11-01.

- 平成 22 年度

[1] 只木孝太郎, 辻井重男, “ランク攻撃の厳密解析 I,” 日本応用数理学会論文誌, Vol.21, No.1, pp.89-102, March 2011.

査読付国際会議論文

- 平成 24 年度

[1] Shigeo Tsujii, Hiroshi Doi, Ryo Fujita, Masahito Gotaishi, Yukiyasu Tsunoo, and Takahiko Syouji, “Privacy preserving data processing with collaboration of homomorphic cryptosystems,” Workshop on Applied Homomorphic Cryptography (WAHC ‘13).

[2] Charles C.N. Wang, David A. Hecht, Phillip C.-Y. Sheu, Hiroshi Yamaguchi, and Jeffrey J.P. Tsai, “BioFactory: Semantic integration of biomedical data and applications,” First IEEE International Conference on Internet Operating Systems and New Applications (ICIOS-2012), December 10-12, 2012, Irvine, California, USA.

[3] Hiroshi Yamaguchi, Masahito Gotaishi, and Shigeo Tsujii, “Privacy preserving problems, solutions, and semantic computing,” First IEEE International Conference on Internet Operating Systems and New Applications (ICIOS-2012), December 10-12, 2012, Irvine, California, USA.

[4] Shigeo Tsujii, Kohtaro Tadaki, Ryo Fujita, Hiroshi Yamaguchi, Masahito Gotaishi, Yukiyasu Tsunoo, Takahiko Syouji, and Norihisa Doi, “Scheme overcoming incompatibility of privacy and utilization of personal data,” 2012 International Symposium on Information Theory and its Applications (ISITA), pp.727-730, October 28-31, 2012, Honolulu, Hawaii, USA.

[5] Shigeo Tsujii, Kohtaro Tadaki, Masahito Gotaishi, and Ryou Fujita, “Construction of the

Tsujii-Shamir-Kasahara (TSK) type multivariate public key cryptosystem, which relies on the difficulty of prime factorization," Extended abstracts of the third Workshop on Mathematical Cryptology (WMC 2012) and the third international conference on Symbolic Computation and Cryptography (SCC 2012), pp.165-168, July 9-13, 2012, Castro Urdiales, Spain.

[6] Kohtaro Tadaki and Norihisa Doi, "Cryptography and algorithmic randomness," Conference Booklet of the Seventh International Conference on Computability, Complexity and Randomness (CCR 2012), pp.43-44, July 2-6, 2012, Cambridge, Great Britain.

- 平成 23 年度

[1] Hiroshi Yamaguchi, Phillip Sheu, Shigeo Tsujii, and Norihisa Doi, "Semantic PIR," Society for Design and Process Science (SDPS2011), June 12-16, 2011, Jeju Island, South Korea.

[2] Zhang, Xu, Sheu, and Yamaguchi, "Parallel processing of rule networks," Society for Design and Process Science (SDPS2011), June 12-16, 2011, Jeju Island, South Korea.

[3] Kitazawa, Zhang, Yao, Sheu, and Yamaguchi, "A query optimization model for object relational databases," Society for Design and Process Science (SDPS2011), June 12-16, 2011, Jeju Island, South Korea.

<u>招待講演</u>

- 平成 24 年度

[1] 辻井重男, "医療情報 PPDM の可能性," 医療情報のプライバシー保護と利活用に関するシンポジウム, 2013 年 3 月 25 日, 全社協・灘尾ホール.

[2] Shigeo Tsujii, "Cryptosystems for social organizations based on MPKC," Workshop on Solving Multivariate Polynomial Systems and Related Topics, March 2-3, 2013, Fukuoka, Japan.

[3] Ryo Fujita, "Piece In Hand concept for enhancing security of multivariate public key cryptosystems and its applications," Workshop on Solving Multivariate Polynomial Systems and Related Topics, March 2-3, 2013, Fukuoka, Japan.

[4] 只木孝太郎, "アルゴリズム的ランダムネスとランダムオラクルモデル," 第 4 回 暗号及び 情報セキュリティと数学の相関ワークショップ (CRISMATH 2012), 2012 年 12 月 26 日, 筑波大学東京キャンパス文京校舎.

<u>学術論文（査読無し）</u>

- 平成 24 年度

[1] Kohtaro Tadaki and Norihisa Doi, "Algorithmic Randomness and the Generic Group Model," Proceedings of the 30th Symposium on Cryptography and Information Security (SCIS2013), 3B3-1, January 22-25, 2013, Kyoto, Japan.

[2] 辻井重男, 山口浩, 森住哲也, 趙晋輝, "論理学暗号の提唱—自然言語から論理推論規則への変換による秘匿検索—," 2013 年暗号と情報セキュリティシンポジウム (SCIS2013) 講演予稿, 2B2-2, 2013 年 1 月 22 日～1 月 25 日,ウェスティン都ホテル京都.

[3] Kohtaro Tadaki and Norihisa Doi, “A secure instantiation of the random oracle by a computable function,” Proceedings of the 35th Symposium on Information Theory and its Applications (SITA2012), December 11-14, 2012, Beppu, Oita, Japan.

[4] 辻井重男, 山口浩, 森住哲也, “自然言語から論理推論規則への暗号化による秘匿回答文作成 ～ 論理学を基盤とする暗号方式の構築に向けて ～,” 電子情報通信学会技術研究報告, Vol.112, No.305, ISEC2012-65, LOIS2012-40, pp.53-60, 2012 年 11 月 21 日～11 月 22 日, 静岡市産学交流センター.

[5] 辻敏雄, 笠原正雄, “中国人剰余定理による秘密分散法とその応用,” 電子情報通信学会技術研究報告, Vol.112, No.306, ISEC2012-66, LOIS2012-41, pp.61-68, 2012 年 11 月 21 日～11 月 22 日, 静岡市産学交流センター.

[6] 只木孝太郎, 土居範久, “アルゴリズム的情報理論とランダムオラクルモデル,” 日本応用数理学会 2012 年度年会「数理的技法による情報セキュリティ」(FAIS) オーガナイズド・セッション, 日本応用数理学会 2012 年度年会講演予稿集, pp.29-30, 2012 年 8 月 29 日, 稚内.

[7] 辻井重男, 山口浩, 土井洋, 角尾幸保, 藤田亮, 庄司陽彦, “Paillier暗号とRSA暗号の連携による暗号化状態処理の一方式 — 第 2 報 ～電子行政・医療介護ネットワークにおける個人情報の保護と利用の両立を目指して～,” 電子情報通信学会技術研究報告, Vol.112, No.126, ISEC2012-33, SITE2012-29, ICSS2012-35, EMM2012-25, pp.175-179, 2012 年 7 月 19 日～7 月 20 日, 北海道工業大学.

[8] 辻井重男, 五太子政史, “整数環上の多変数多項式を用いた多変数公開鍵暗号,” 電子情報通信学会技術研究報告, Vol.112, No.126, ISEC2012-39, SITE2012-35, ICSS2012-41, EMM2012-31, pp.213-216, 2012 年 7 月 19 日～7 月 20 日, 北海道工業大学.

- 平成 23 年度

[1] 辻井重男, 山口浩, 只木孝太郎, 角尾幸保, “Paillier 暗号と RSA 暗号の連携による暗号化状態処理の一方式 -電子行政・医療介護ネットワークにおける個人情報の保護と利用の両立を目指して-,” 2012 年暗号と情報セキュリティシンポジウム (SCIS2012) 講演予稿, 3A1-3, 2012 年 1 月 30 日～2 月 2 日, 金沢エクセルホテル東急, 石川.

[2] 只木孝太郎, 土居範久, 辻井重男, “プライバシー保護条件付き情報開示,” 2012 年暗号と情報セキュリティシンポジウム (SCIS2012) 講演予稿, 3D2-1, 2012 年 1 月 30 日～2 月 2 日, 金沢エクセルホテル東急, 石川.

[3] Kohtaro Tadaki and Norihisa Doi, “Instantiating the Random Oracle Using a Random Real,” Proceedings of the 29th Symposium on Cryptography and Information Security (SCIS2013), 3B3-1, January 30 - February 2, 2012, Kanazawa, Japan.

[4] 辻井重男, 山口浩, 五太子政史, 只木孝太郎, 藤田亮, 井堀幹夫, 山本拓真, 土居範久, “電子行政・医療介護ネットワークにおける個人情報の保護と活用の両立のための情報連携システム-第 2 報,” 2012 年暗号と情報セキュリティシンポジウム (SCIS2012) 講演予稿, 2D1-4, 2012 年 1 月 30 日～2 月 2 日, 金沢エクセルホテル東急, 石川.

[5] 山口浩, P. C.-Y. Sheu, 辻井重男, “プライバシーを保護した問題 / 解決,意味計算方式,” 2012 年暗号と情報セキュリティシンポジウム (SCIS2012) 講演予稿, 2F3-4, 2012 年 1 月 30 日～2

月 2 日，金沢エクセルホテル東急，石川.

[6] 辻井重男，山口浩，五太子政史，角尾幸保，井堀幹夫，山本拓真，“電子行政における個人情報の保護と利用の両立を図る情報連携システムに関する研究 ～ 第 1 報 ～,” 電子情報通信学会技術研究報告, Vol.111, No.363, SITE2011-28, pp.19-24, 2011 年 12 月 17 日～12 月 18 日，島根大総合理工学部.

[7] 五太子政史，辻井重男, “多変数公開鍵暗号による署名方式 Hidden Pair of Bijection 第二報～セキュリティの検討 ～,” 電子情報通信学会技術研究報告，Vol.111，No.285，ISEC2011-42, LOIS2011-36 , pp.55-60, 2011 年 11 月 14 日～11 月 15 日，大阪電気通信大学.

[8] 五太子政史，辻井重男, “グレブナー基底計算の最適化に関する一考察 ～暗号解析のためのグレブナー基底計算～,” 電子情報通信学会技術研究報告，Vol.111，No.123， ISEC2011-15, SITE2011-12, ICSS2011-20, EMM2011-14, pp.79-83, 2011 年 7 月 12 日～7 月 13 日，静岡大学浜松キャンパス.

- 平成 22 年度

[1] 五太子政史，辻井重男, “相補型 MPKC 役割交代型署名の提案,” 電子情報通信学会技術研究報告, Vol.110, No.443, IT2010-126, ISEC2010-130, WBS2010-105, pp.383-388, 2011 年 3 月 3 日～3 月 4 日，大阪大学.

[2] 山口浩，只木孝太郎，辻井重男，土居範久, “医療・介護ネットワークにおける個人情報の保護と活用の両立に関する考察,” 電子情報通信学会技術研究報告, Vol.110, No.429, SITE2010-52, IA2010-88, pp.33-38, 2011 年 2 月 28 日～3 月 1 日，高知市文化プラザ かるぽーと.

[3] 辻井重男，五太子政史，“相補型 STS-MPKC 方式による組織対応型公開鍵暗号の提案,” 2011 年暗号と情報セキュリティシンポジウム (SCIS2011) 講演予稿, 2A4-2, 2011 年 1 月 25 日～1 月 28 日，リーガロイヤルホテル小倉，福岡.

国際学会発表（査読なし）

- 平成 24 年度

[1] Kohtaro Tadaki and Norihisa Doi, “The Generic Group Model and Algorithmic Randomness,” Computability Theory and Foundations of Mathematics (CTFM), February 18-20, 2013, Tokyo Institute of Technology, Tokyo, Japan.

[2] Kohtaro Tadaki, “The random oracle methodology and algorithmic randomness,” Fourth Workshop on Game-Theoretic Probability and Related Topics (GTP 2012), November 12-14, 2012, Hongo Campus, The University of Tokyo, Japan.

国内学会発表（査読なし）

- 平成 24 年度

[1] 只木孝太郎, “ジェネリック群モデルとアルゴリズム的ランダムネス,” 日本数学会 2013 年度年会, 2013 年 3 月 20 日～3 月 23 日，京都大学 吉田キャンパス.

[2] 藤田亮，辻井重男, “暗号化維持でのデータ処理技術・秘匿分散計算技術の実運用における一考察～医療・介護情報の利活用を推進する状況適応型組織暗号の実装を例として～,” 日本セキ

ュリティ・マネジメント学会第 26 回全国大会, 2012 年 6 月 23 日, 電気通信大学, 東京.

- 平成 23 年度

[1] 只木孝太郎, “暗号理論におけるランダムオラクルのランダム実数による具現化,” 日本数学会 2012 年度年会, 2012 年 3 月 26 日～3 月 29 日, 東京理科大学 神楽坂キャンパス.

[2] 藤田亮, “「攻め」の秘匿分散計算技術の普及を目指して～プライバシーを保護しつつ秘匿された個人情報の安心・安全な活用に向けて～,” 日本セキュリティ・マネジメント学会第 25 回全国大会, 2011 年 6 月 25 日～6 月 26 日, 長岡技術科学大学 , 新潟.

その他（プレプリント等）

- 平成 23 年度

[1] Shigeo Tsujii, Kohtaro Tadaki, Masahito Gotaishi, and Ryou Fujita, “Construction of the Tsujii-Shamir-Kasahara (TSK) type multivariate public key cryptosystem, which relies on the difficulty of prime factorization,” Cryptology ePrint Archive: Report 2012/145, March 2012.

[2] Masahito Gotaishi and Shigeo Tsujii, “Hidden Pair of Bijection signature scheme,” Cryptology ePrint Archive, Report 2011/353, July 2011.

３－２－ｃ　目標の達成度

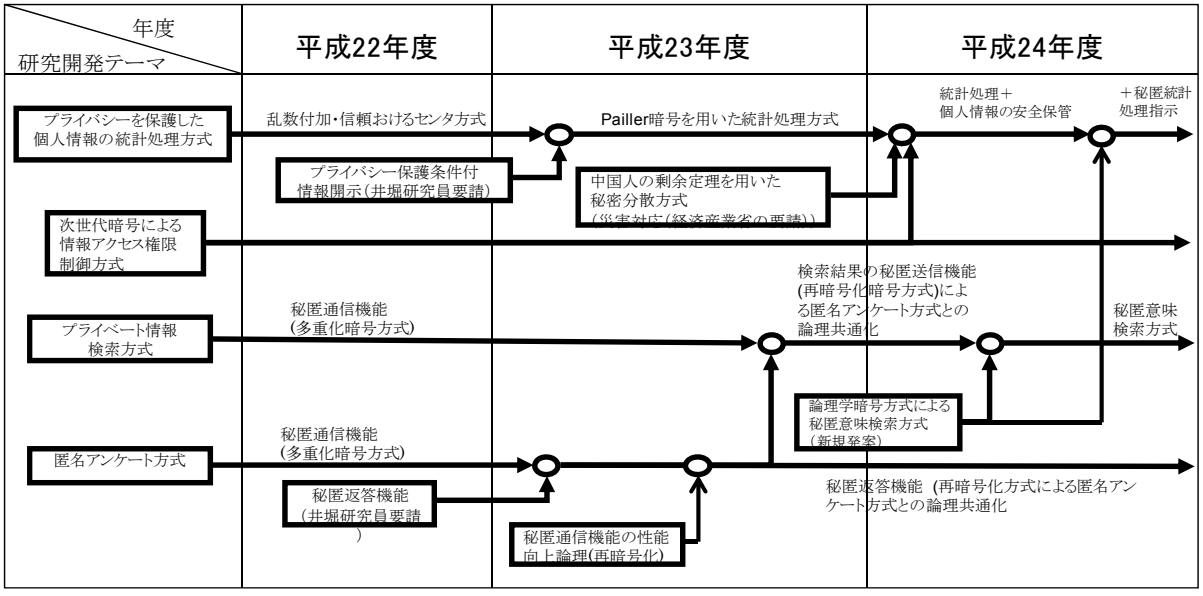
平成 22 年度は研究開発の方式の検討、他方式の優位性の考察、ならびに医療・介護分野におけるニーズ、シーズの調査を行った。平成 23 年度は方式実現のための暗号、暗号プロトコル手法の検討、ならびに一部、プロトタイピング、デモプログラムの作成を行った。平成 23 年度に「デモシステムへの実装」はテーマとしていたうち 4 方式について実現しており、計画以上の成果である。平成 24 年度はプロトタイピングによる性能評価、論文発表、ならびに報告書作成を行い、各テーマとも所定の目標を達成した。

さらに、研究開発の過程で把握したニーズをもとに、機能追加を実施している。この経緯を表ｃ－６に示す。

表ｃ－５　目標に対する成果・達成度の一覧表

要素技術	目標・指標	成果	達成度
プライバシーを保護した個人情報の統計処理方式	・機微な個人情報について、秘匿性を保ったまま有効活用するために、必要なプライバシー保護方式及び情報処理方式等の研究開発を行う。	・秘密分散保存法を提案し、必要な手法を完成の上デモプログラムに実装し、実験により本方式の優位性を確認した。	達成
匿名アンケート方式	・オンラインでアンケートを行う際に、回答者の匿名性を担保し、アンケート回答に対する心理的な障壁を低減するとともに、有効な統計情報を抽出して活用するために必要な暗号方式の開発及び性能評価を行う。	・Private Information Retrieval(PIR)の手法が利用できることを確認し、処理性能の比較から有用性を確認し、方式案を策定した。 ・策定した方式案をもとに、プロトタイプを作成した。	達成
プライベート情報検索方式	・情報を検索する際に、当該検索者の個人情報及びその検索内容について秘匿したまま、必要な情報を取得できるシステムを構築するために必要な暗号方式、暗号プロトコル等の研究開発を行い、暗号プロトコル全体のセキュリティと性能を評価し、全体の評価を行う。	・医療情報を対象とする自然言語による検索方法を考案、実装した。 ・Semantic Computingに関する研究結果をもとに、論理暗号を提案した。	達成
次世代暗号によるアクセス権限制御方式	・一括して暗号化した個人の様々な医療情報について、職能権限や資格ごとに複数の復号鍵を設定でき、アクセス権限がある情報のみを選択的に復号できる次世代の暗号方式（組織暗号）を開発する。	・新たな構成手法を検討し、そのセキュリティ上の性能を解明するとともに、デモプログラムを実装した。	達成

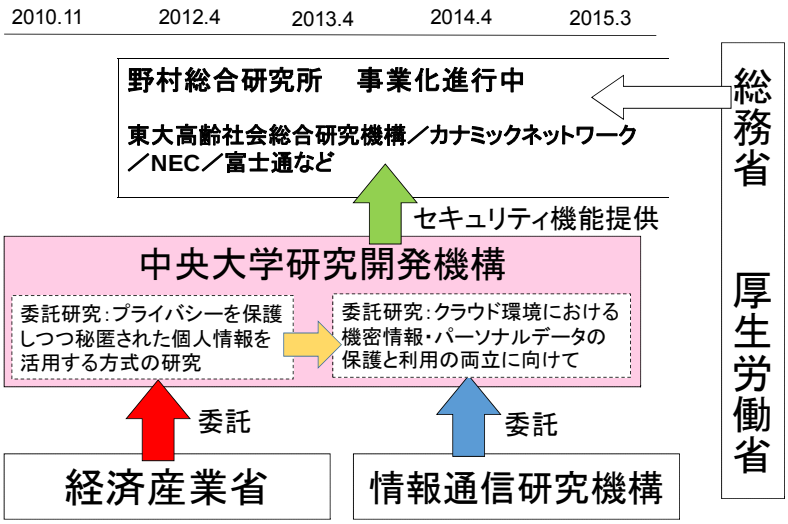
表ｃ－６　本テーマに関する機能追加等の状況



４－ｃ　事業化、波及効果について

４－１－ｃ　事業化の見通し

下図の体制にて事業化に向けた取り組みを実施している。



図ｃ－４　本テーマに関する機能追加等の状況

このうち、株式会社野村総合研究所による活動において利用されるセキュリティ機能は、本成果を拡張したものである。現在利用されつつあるセキュリティ機能は、本成果のうち「組織暗号」に関するもので、独立行政法人情報通信研究機構（NICT）の委託研究においてその機能・運用方法などが現場の事情に合うよう、アプリケーションとのインターフェースやユーザインターフェースなどを更に具体化したものである。

「組織暗号」の概念は本研究開発の事業期間中に実施機関において着想されていたものであるが、組織暗号は広い概念であって、組織の形態も多様であり、それに応じて、暗号にもいろいろな方式が考えられている。

典型的な階層型組織に対しては、多変数公開鍵方式が考えられ、これについての基礎的研究は本研究開発期間中に進められた。NICT 委託研究では、多変数公開鍵方式による組織暗号を発展させると同時に、平坦型組織を対象とする多受信楕円暗号についての研究が行われている。

以上の 2 点が NICT 委託研究において拡張された主要なポイントである。

このほか本テーマに関しては、事業化に向けて下表の活動が行われている。

表ｃ－７　事業化状況

区分	実用化計画	提携企業
実用化戦略	「インターライ方式ケアアセスメントクラウドサービス」への「プライバシーを保護した統計処理システム」の適用	ASPIC, カナミックネットワーク
	「プライバシーを保護した統計処理システム」「匿名アンケート方式」「プライベート情報検索方式」を用いて医療データの2次利用データベースから1次利用データの活用を図るシステムの実現	YDK, スカパーJSAT
	米国Biomedical Objects Inc. による臨床医学分野への適用を促進し、併せて国内における同分野における展開を行う	Biomedical Objects Inc.
実用化推進フォーラム戦略	「暗号の社会的利用研究」フォーラム設立によるITベンダー(日本電信電話、日立製作所、東芝、日本電気、富士通、三菱電機)と中央大学による共同研究	
次期実用化戦略	マイナンバー制に基づく電子行政システムや電子政府に関するシステムへの当プロジェクト研究成果の適用を提案してゆく	フォーラム活動を通して募集

上表における「暗号の社会的利用研究」フォーラムは、現在「MELT up フォーラム」[2]として活動している。そのウェブサイトの画面を次ページに示す。

[2] http://www.fuji-serv.com/chuo/index.html

図ｃ－５　MELT up フォーラム

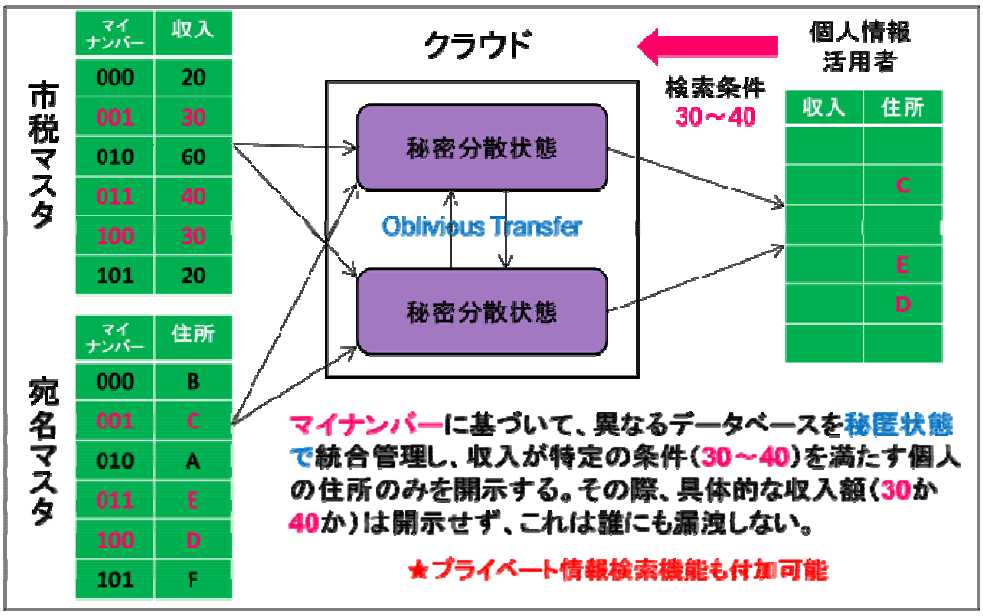
４－２－ｃ　波及効果

平成 23 年度は、当初想定していた「医療・介護」に加えて、「行政（主にマイナンバー精度関連）での個人情報の保護と活用」への応用が可能であるという評価を専門家から受けることができた。

平成 24 年度は、上記の評価に基づき、総務省及び厚生労働省の進めていた「地域の医療・介護組織間での情報共有方式」に適用することが提案された。これは翌年度に実現している。

乱数付加による統計処理秘密分散方式は、他の暗号化状態処理方式に比較して、数桁以上の高速性を有する実用性の高い方式であり、国際会議及び有識者からの高い評価の下に、現在、ＩＴ企業・クラウド事業者等と実用化へ向けて検討を進めている。

マイナンバー制導入後の電子医療・行政の進展に向けた本成果の活用に向け、暗号の有効性に対する社会の認識・信頼感を高めるためのフォーラムを立ち上げ、活動を開始した。その中で、間隔抽出方式や組織対応暗号等、本プロジェクトで得られた成果の導入を図る予定である。



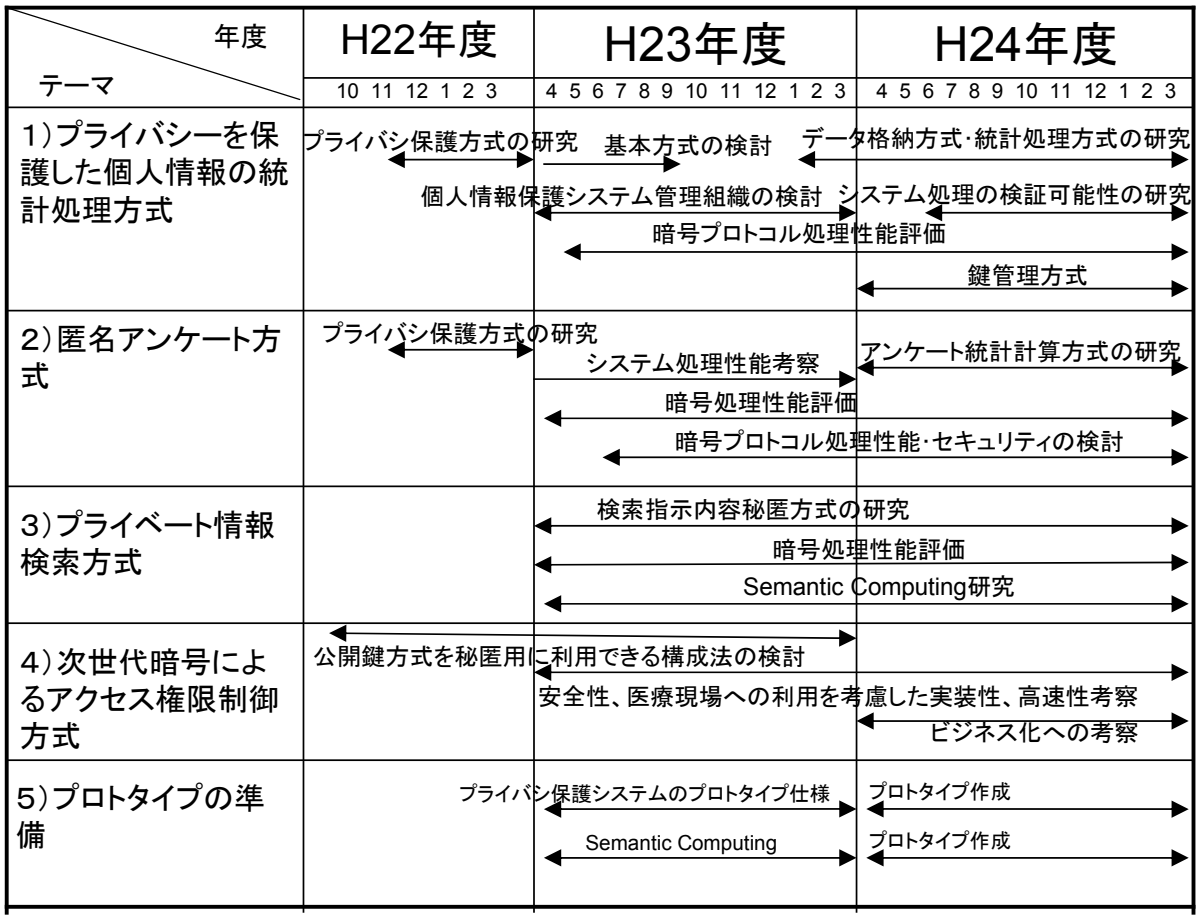
図ｃ－６　マイナンバー制度への応用

５－ｃ　研究開発マネジメント・体制・資金・費用対効果等

５－１－ｃ　研究開発計画

本事業は、平成 22 年度から 24 年度までの 3 年計画である。各要素技術の研究開発計画は次のとおりである。

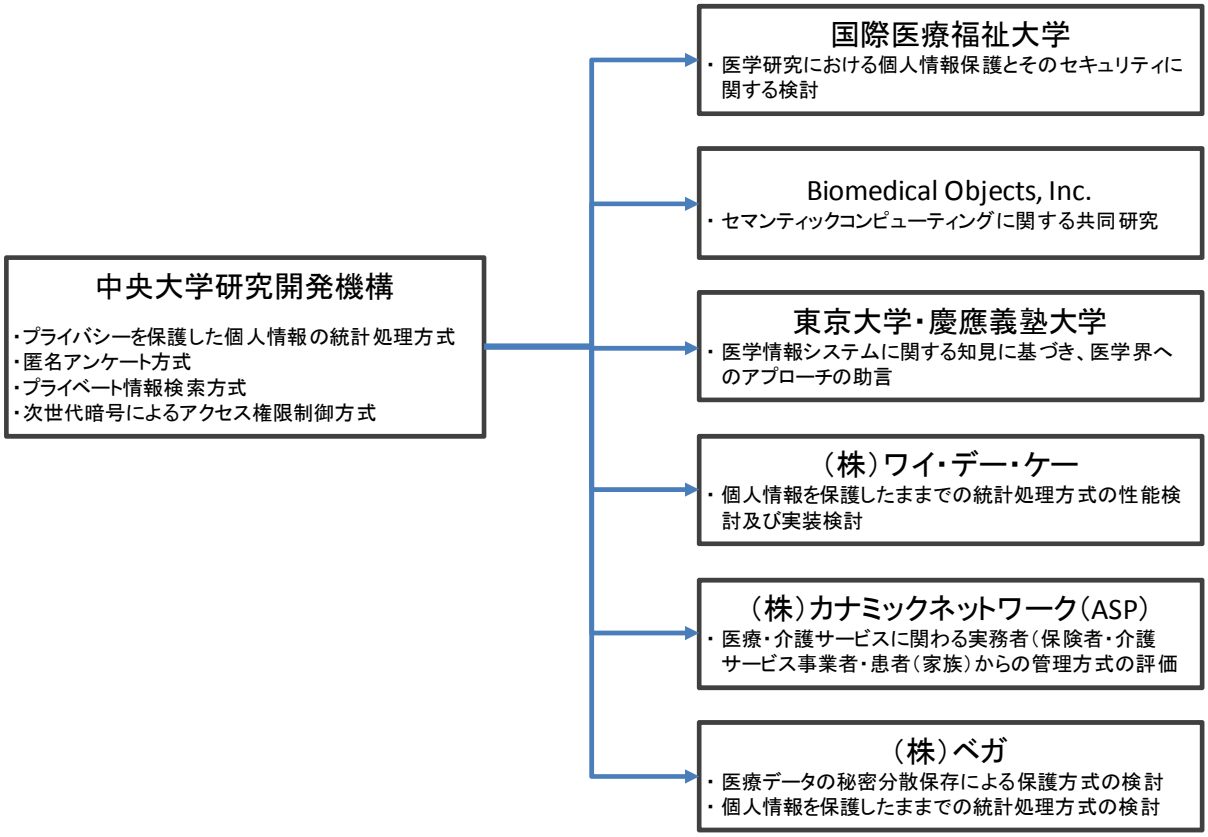
表ｃ－８　研究開発計画



５－２－ｃ　研究開発実施者の実施体制・運営

本事業は、平成 22 年度から平成 24 年度において、経済産業省から中央大学への委託により実施されている。また再委託先として以下の機関が事業に参加した。

平成 22 年度、平成 23 年度、平成 24 年度とも、実施計画書記載の体制には、医療分野、介護分野共に優れた実績を上げている組織、企業、及び研究者が参加しており、この体制が研究に有効に寄与している。



図ｃ－７　研究開発実施体制

５－３－ｃ　資金配分

表ｃ－９資金配分　　(単位百万円)

要素技術	平成22年度	平成23年度	平成24年度
プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究	**27.7**	**36.3**	**37.1**

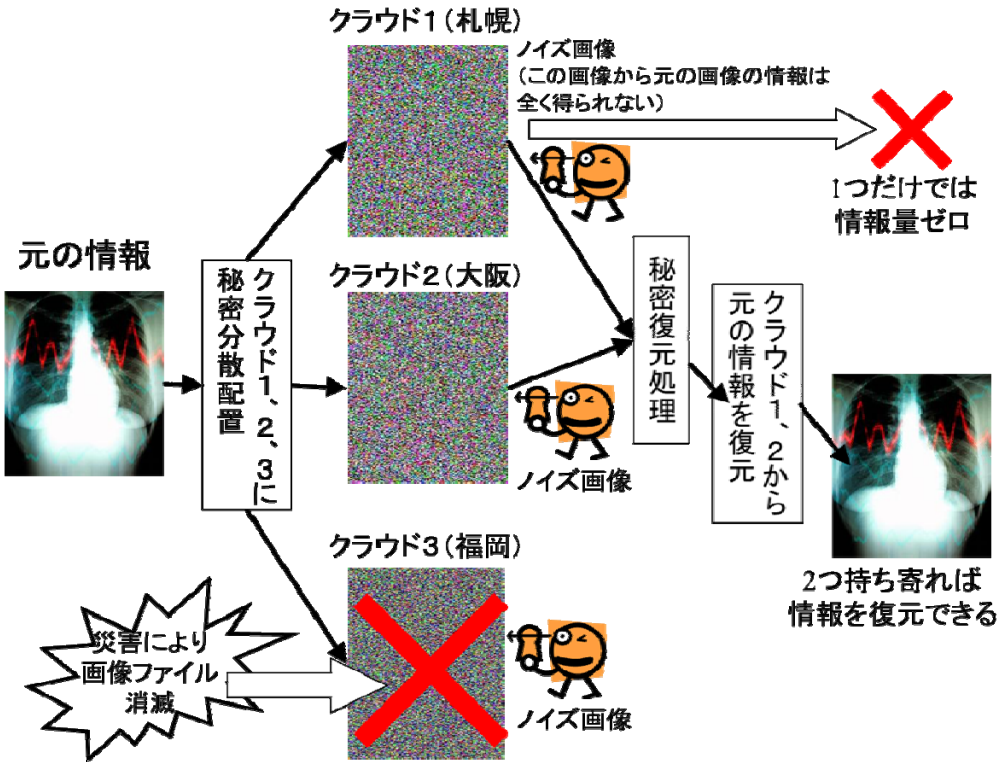
５－４－ｃ　費用対効果

評価時点において、事業化に向けた動きは進んでいるものの、本研究成果による売上等は発生していない。

しかしながら、本研究開発は、現在書面によって行われている介護事業者への業務指示やサービス記録、各種報告類の電子化を実現する要因としてとらえることができる。これらの作業の電子化は総務省及び厚生労働省により平成 23 年度から 24 年度にかけて実施された調査研究の結果をもとに、平成 25 年に認められることとなったが、こうした判断には本成果が提供するセキュリティ機能により、情報保護が可能であることが同調査研究の担当者に認知されていたことが影響している。したがって、これらの作業の電子化を通じて実現される、データ転記作業の省力化、転記誤りの防止やトレーサビリティの向上は本研究開発からの派生的効果としてとらえることが可能である。

５－５－ｃ　変化への対応

東日本大震災の発生を受け、本成果で機微情報の保護に用いている秘密分散方式に、中国人剰余定理を用いて一部の保存情報が消滅した場合の復元を可能とする機能を追加した。



図ｃ－８　東日本大震災を踏まえた見直し結果

Ａ－ｄ　撮影による情報漏洩を防止するソリューションの研究開発

１－ｄ　事業の目的

情報漏えい対策については、小型記憶媒体へのコピーを禁止するソフトウェアをパソコンにインストールしたり、ネットワークサービスの利用を禁止する通信機器等を導入したりするなどして、対策を整えているが、「ディスプレイ上に表示されている情報を撮影する」という持ち出し方法への対策は、ほとんどの情報表示端末において行われていない。

このため、デジタルな画像・映像を撮影できるビデオカメラ等により、パソコンやタブレットＰＣ等のディスプレイに表示されている静的・動的なコンテンツを撮影したとしても、品質が低下したコンテンツとして記録させることにより、持ち出しによるコンテンツのリークやコンテンツをコピーしたＣＤ・ＤＶＤの売買等を抑止できる手法の研究開発を行う。また、上記の手法を無力化する手段（赤外線カットフィルターを用いた撮影）に対抗するために、当該フィルターの存在を検知できる手法の研究開発を行う。

２－ｄ　研究開発目標

撮影による情報漏えいを防止する手段として赤外線を活用するため、２種類の技術開発を実施することとした。さらにこれまでに類似の手法が存在しない技術であるため、成果を普及させるための方策について、別途検討することとした。

表ｄ－１　個別要素技術の目標

要素技術	目標・指標	妥当性・設定理由・根拠等
透明赤外線光源の開発	・赤外線を発光するシートを開発することで、撮影されたコンテンツに光学的なノイズを含ませる（コンテンツの品質を低下させる）。	・人間の視覚では識別されないが、カメラによる撮影画像に影響を与える赤外線を用いて、コンテンツにノイズを加え、人間による利用に影響を及ぼさずに撮影の効果を失わせることを目指す。
赤外線遮断対抗技術の開発	・品質の高いコンテンツが記録されることを防止するため、IRカットフィルターがディスプレイの近傍にあることを検知できる手法を開発する。 ・撮影行為を検知できる手法の開発を目指す。	・IRカットフィルタを用いた撮影が行われると、上記の赤外線発光による効果が損なわれるため、IRカットフィルタを用いた撮影を検知する必要がある。 ・撮影行為そのものを検知することで、情報漏えい目的の撮影の抑止に資する。
成果の普及啓発	・成果に基づく特許を出願する。 ・国内および海外で開催される学術集会において研究発表を実施する。 ・当該集会等においてセンサーシステム等をデモ展示する。	・これまでにないアプローチであるため、成果に基づく事業化に先立ち、さまざまな視点からの意見を得るとともに、研究成果の普及にあたって克服すべき課題についての情報収集を行う。

各年度の詳細な目標は次の通りである。

① 平成２２年度

【透明赤外線光源の開発】

- 光励起により赤外線を発光し、かつその波長が 870nm 程度となる透明な蛍光体の生成を行う。具体的には、希土類イオン（「ネオジム、イッテルビウム）を少量ドープした「担持ガラスの粉末」を燃焼してガラス化する。希土類イオンと担持ガラスの配合量を調整することにより、可視光受光時に高い赤外線変換効率をもつ蛍光体を生成する。この素材を選んだ理由は、当該時点において直接的な電流・電圧の入力を必要とせずに赤外線を発光でき、薄いシート状の赤外線発光デバイスの開発が期待できる唯一の素材と考えられたためである。実施機関からは、後述のように結果的にガラス素材では目標を達成できなかった事実を踏まえ、今回採用した無機材料のみでなく、有機材料についても調査すべきであったとの反省が示されている。
- 赤外線を発光する透明なフィルム上の光源（以下、「ＩＲフィルム光源」という。）の生成を行う。具体的には、上項により生成された蛍光体を粉砕した後、溶媒（透明ポリマー）を用いて蛍光体を分散させる。そして、これを透明フィルム（アクリル）に塗布し、乾燥させることで成型を行う。フィルムに塗布する量や乾燥させる時間を調整することにより、透明なフィルム光源を生成する。
- ＩＲフィルム光源の取り外しを迅速に検知できるセンサの開発、及びプロトタイプの試作を行う。
- ＩＲフィルム光源を貼り付けたディスプレイに表示される情報を撮影した結果、当該映像・画像にノイズが含まれており、かつ、当該ノイズによって情報が読み取れないことを確認するための実証実験を行う。実験で使用するビデオカメラ・デジタルカメラのスペックは、プロフェッショナル向け（有効画素数が多く、高性能な撮像素子のもの）と一般向け（家電量販店で容易に入手できる程度のもの）を用意し、ひとつのカテゴリーに対して機能やスペックが異なる３つの機種を使用する。具体的には、一眼レフカメラを３台、コンパクトカメラを３台、デジタルビデオカメラを３台、それぞれ使用する。実験には、情報を表示するための「ディスプレイ」と、情報を送出するための「パソコン」、およびその両方を備えた「ノート型パソコン」を使用する。ディスプレイの種類は、「表面光沢有り」のものと「表面光沢無し」のものをそれぞれ使用する。
- ＩＲフィルム光源の材料である希土類の安全性、および赤外線の受光による目への影響について文献調査を行う。

【赤外線遮断対抗技術の開発】

- 赤外線を遮断する手段（赤外線カットフィルタ等）を用いてディスプレイを撮影したとしても、これを無効とする（たとえば、光学的なノイズを混在さ

せる、など）ための技術開発を行う。具体的には、光学に関する文献を用いて調査を行い、上記手段を無効化するためのアイデアを創出する。また、当該アイデアをもとにして「赤外線カットフィルタ」と「撮影用機器」を用いて実験を行い、その妥当性を検証する。

【成果の普及啓発】

- 平成２２年度の実施計画書には成果の普及についての目標設定は無いが、国内および海外で開催されるメジャーな学術集会で発表することで普及啓発を効果的に行うとともに、特許を出願することで実用化に向けた道筋を明確にすることが目標として想定されていた。

② 平成２３年度

【透明赤外線光源の開発】

- 光励起により赤外線を発光する素材として、波長を目標値である８７０nm に近づけるとともに、透明度及び赤外線への変換効率の高い蛍光体ガラスの開発を行う。この実現のため、たとえば、「酸化希土類（ネオジム、イッテルビウム等）」と「担持ガラス（ホウ酸等）」の配合量を調整したり、酸化希土類や担持ガラスの組成を変更したりするなどといった方法を実施する。
- 透明度が高く、励起光によって赤外線を発光するＩＲシート光源のプロトタイプを生成する。たとえば、蛍光体ガラスと樹脂との屈折率が同じになるように調整したあと、ある程度の粒径と厚みをもつ蛍光体ガラスを樹脂に封入する。そして、これをシート状に成形し、表面や側面から補助光源を照射する、という方法を実施する。
- ＩＲシート光源の切り取りを検知するセンサーシステムを開発する。たとえば、タッチパネルディスプレイに採用されている透明度の高いシート状の電極をＩＲシート光源に取り付けて、その抵抗値をパソコンでモニタリングする。そして、切り取りにより抵抗値が上がったときに、ディスプレイの電源をオフにしたり、撮影されても支障のない「無意味なコンテンツ」を表示したりする機能をもつ「コンテンツ保護機能」を付加する方法を実施する。また、上記のモニタリング及びコンテンツ保護機能を実現させるために、センサーと連動するソフトウェアを開発する。
- ＩＲシート光源のプロトタイプを用いた実証実験により、記録されたコンテンツに光学的なノイズを含ませることができる環境条件（必要な光の照度、強度など）の最適化を図る。つぎに、上記プロトタイプの光源よりも蛍光体ガラスの濃度を高めたものを用いて、上記の環境条件の最適化を図る試みも実施する（たとえば、蛍光体の板ガラスを生成し、可視光を照射しながら分光器等を用いて赤外線の発光スペクトルを測定したり、記録されたコンテンツに含まれるノイズを確認したりする）。また、上記で開発したセンサーシステムの動作を確認する。また、ＩＲシート光源とマイクロルーバーとを組み合わせることにより、ディスプレイの正面以外からの撮影に対抗できること

を検証する。

- 必要に応じて、赤外線の使用に関する安全性調査を実施する。

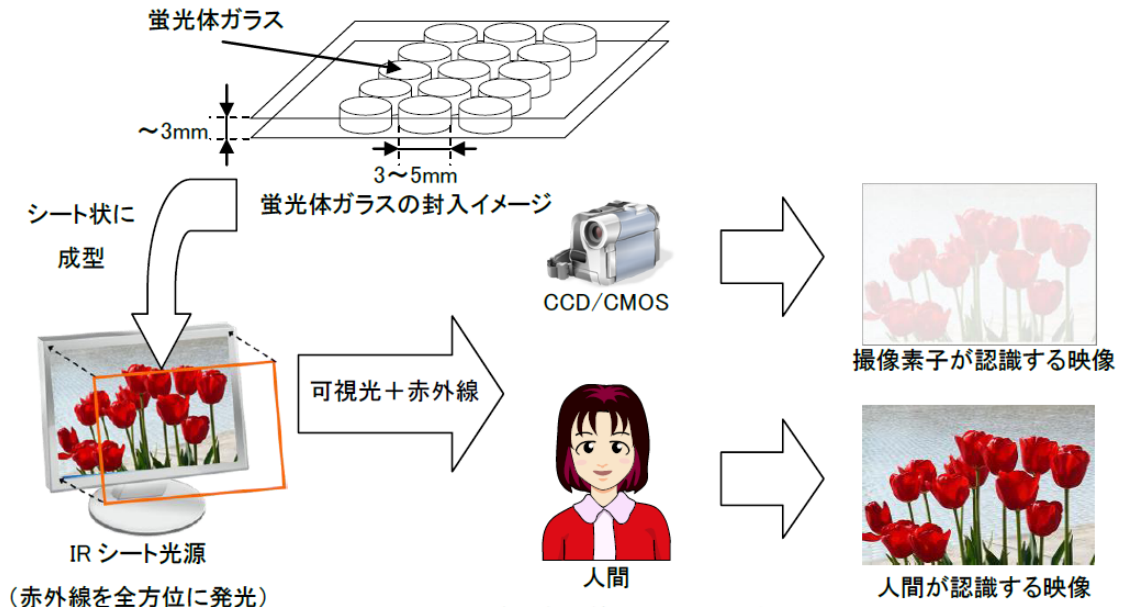
【赤外線遮断対抗技術の開発】

- ディスプレイの正面・近傍距離（３０cm～６０cm 程度）に存在する２種類の赤外線カットフィルターが検知できる手法を検討する。たとえば、ディスプレイの上枠部分からスポット状の近赤外線を、ディスプレイの正面・近傍領域に照射しながら、その様子を近赤外線イメージセンサーで撮影する。つぎに、得られた画像を分析・処理することよって、赤外線カットフィルターの存在を検知する方法を実施する。
- 赤外線カットフィルターが内蔵されているカメラを用いた撮影に対抗するために、カメラを構えてディスプレイを撮影していることを検知できる方法についても検討する。
- 前項により検討・創出されたアイデアをもとにして、ＩＲフィルターの存在を検知できるソフトウェアを開発する。また、当該フィルターの存在やカメラを構えてディスプレイを撮影していうことを検知したときに、ディスプレイの電源をオフにしたり、別の無意味なコンテンツを表示させたりするセキュリティ機能を付加することを検討する。
- 前項で開発したソフトウェアで構成されるシステムを用いて、ディスプレイの正面・近傍距離に存在する赤外線カットフィルター（反射型・吸収型）が検知できることを確認する。たとえば、ディスプレイから当該フィルターまでの距離を３０cm～６０cm の範囲で少しずつ変更したり、赤外線を吸収しやすい色の服を着用した人に当該フィルターを持たせたり、当該フィルターの大きさを変更したりするなどして、検知性能の評価を行う。また、カメラを構えてディスプレイを撮影していることを検知できるシステムができたときには、当該システムについても合わせて評価を行う。

【成果の普及啓発】

- これら研究成果の普及方法として、国内および海外で開催される学術集会において研究発表を実施する。また、当該集会等においてセンサーシステム等をデモ展示することを検討する。
- 国内では、具体的には情報処理学会・コンピュータセキュリティシンポジウム２０１１及び電子情報通信学会・情報セキュリティシンポジウム２０１２の２つの学術集会に参加する。２つの学術集会では、参加者層が異なり、普及啓発を効果的に行うことができるとともに、さまざまな視点からの意見を得る。
- 情報処理学会主催の学術集会では、企業からの参加者が多いため、事業化に向けたビジネスマッチングとともに、製品化に向けた具体的なアドバイスを得る。一方、電子情報通信学会主催の学術集会では、アカデミックな研究交流を通じ、研究開発の深化に向けた指導・助言を得る。

- 海外で開催される学術集会は研究成果に対する審査水準が日本国内よりも高く「良いものは良い」「悪いものは悪い」という判断が明確であり、国内における学術集会と併せて参加することで、研究成果の普及にあたって克服すべき課題等について明確に情報を収集することができるとともに、日本の技術力をアピールできる。海外学術集会への研究論文投稿にあっては、（１）研究成果に対する審査水準が高いもの（採択率が３０%程度)、（２）情報セキュリティの研究者に広く知られているもの、（３）ビジネスマッチングの機会があるもの、の３点をもとに選択することが必要である。２０１１年８月にオーストリアで開催されるＡＲＥＳ（可用性、信頼性とセキュリティに関する国際会議）は、当該３点の条件を満たしている（前年の採択率は２５%であり、ＩＥＥＥ等の国際的な機関のイベントカレンダーに掲載されており認知度が高い。また、企業の研究成果を発表できる Industrial Track を設けるなど、ビジネスマッチングの機会がある）ため、当該学術集会に参加する。
- 本事業終了後における研究成果の活用方法として、光源製品及びシート製品の製造・販売能力を有する事業者と共同して製品開発を行い、市場に投入することを検討する。



図ｄ－１　本研究開発で想定していた成果のイメージ

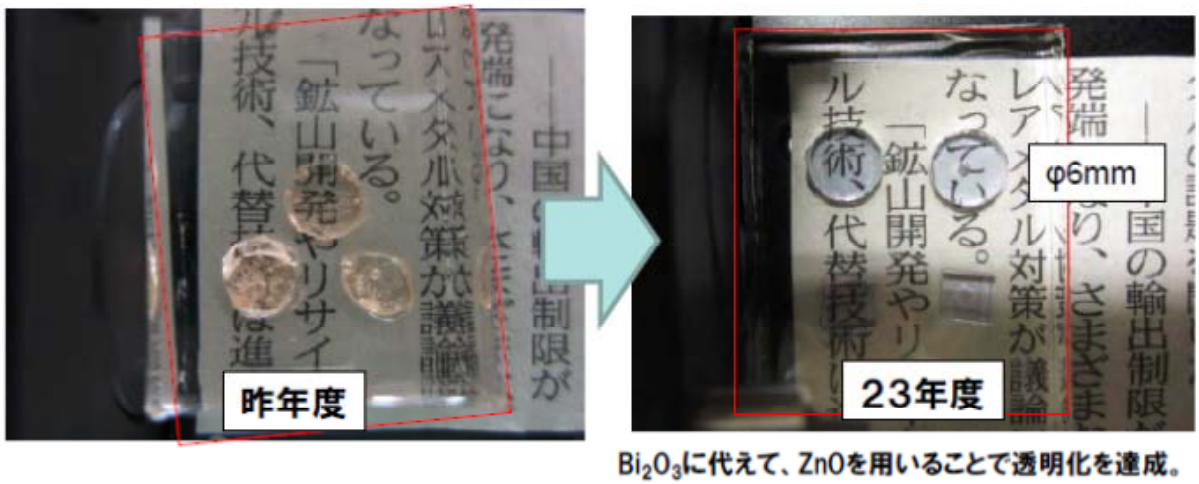
３－ｄ　成果、目標の達成度

３－１－ｄ　成果

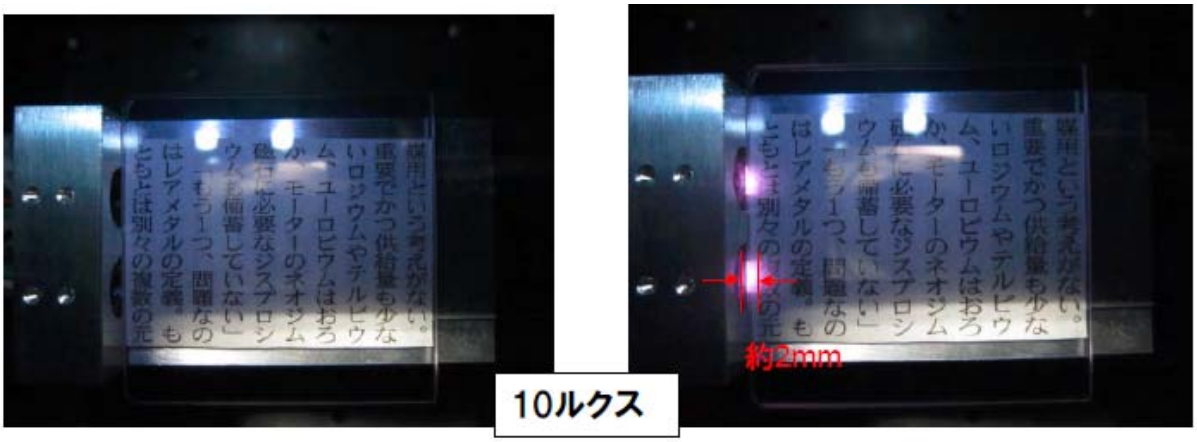
（１）成果

（１－１）透明赤外線光源の開発

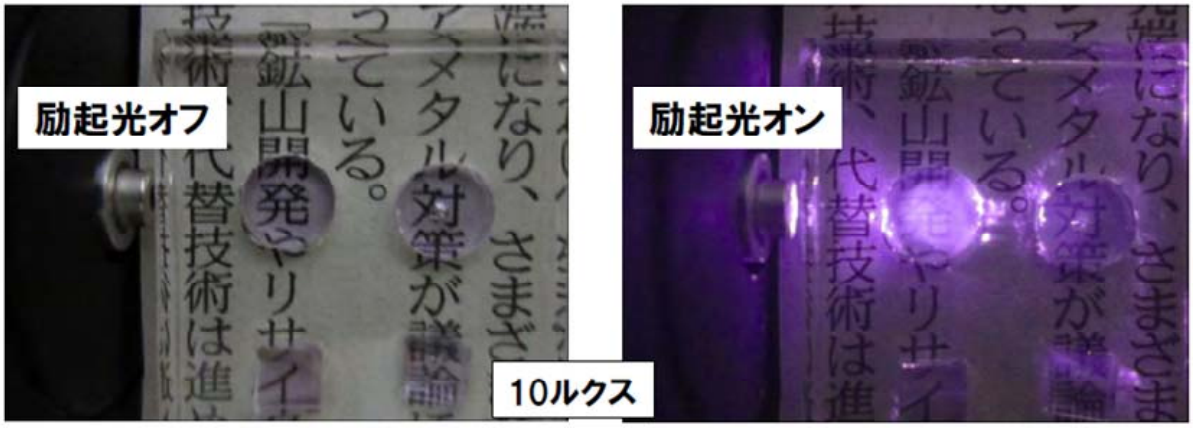
波長 880nm で発光する透明な蛍光体ガラスの開発に成功し、これをもとに工学的ノイズの発生を試みたが、コンテンツの識別性低下には至らなかった。板ガラスを用いる場合は発光するのはガラスの端部のみで、中央部での発光が得られず、粒ガラスの場合は複数並んだガラス粒のうち、別の粒ガラスを超えての励起が行われないため、いずれも本研究開発の目的に対して有効な効果を発揮しないことが確認された。



図ｄ－２　蛍光体ガラスにおける透明度の向上成果



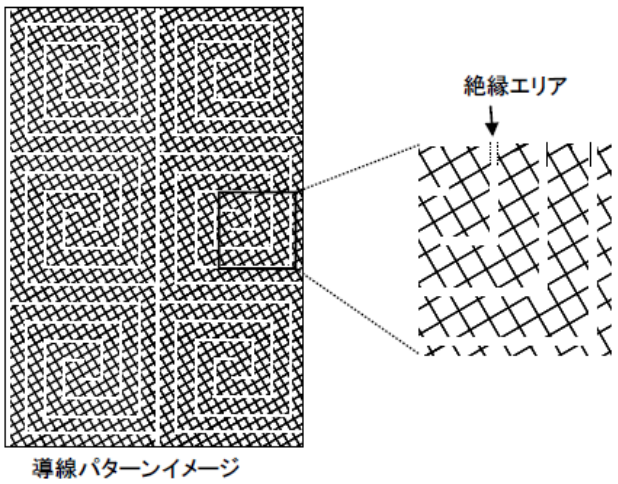
図ｄ－３　赤外線光源によるコンテンツの識別性低下に関する実験結果（板ガラス）



図ｄ－４　赤外線光源によるコンテンツの識別性低下に関する実験結果（粒ガラス）

このほか、本成果を実用化する際の回避防止策として、画面に設置されたフィルタがカットされたことを検知するセンサーの開発も実施した。こちらは実験の結果、フィルタのカットを検知することに成功している。

図ｄ－５　取り外し検知センサーシステムの概要



図ｄ－６　実験に成功したときの導線パターンのイメージ

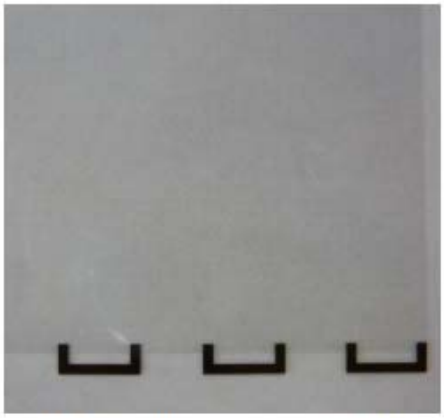
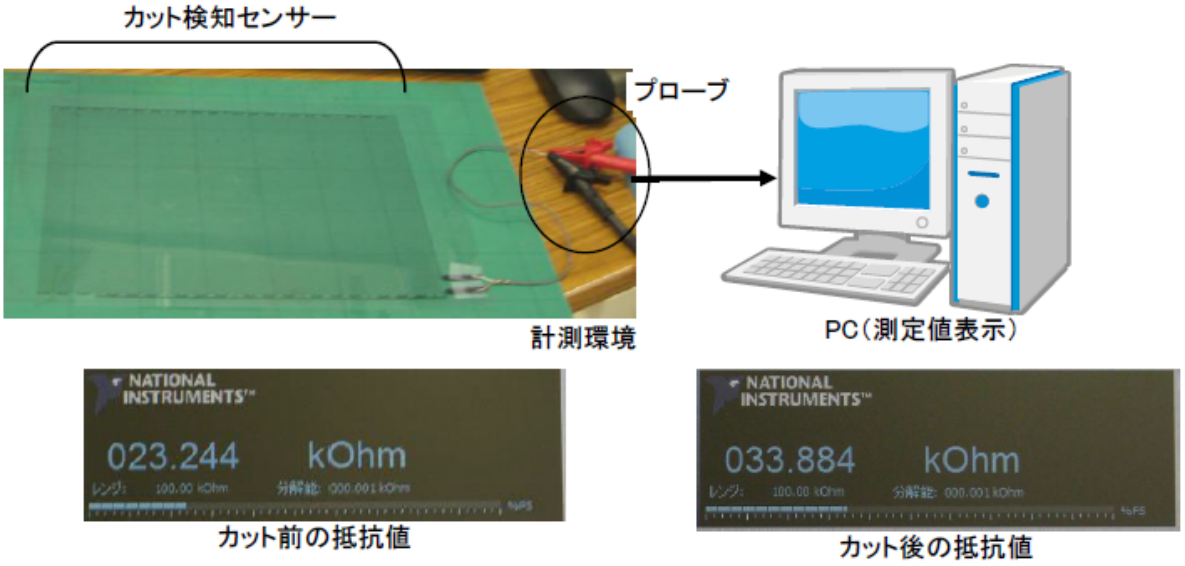


図 2.30　サンプル（一部拡大）

図ｄ－７　センサーを画面全面に設置してもモアレが発生しないことの確認画像



図ｄ－８　カット検知センサーのカットによる抵抗値の変化

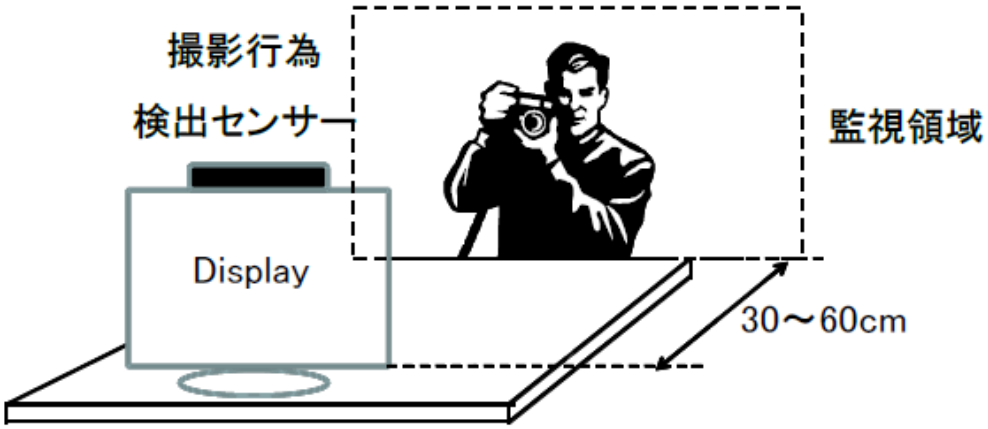
（１－２）赤外線遮断対抗技術の開発

画面に対する撮影行為を検知するため、カメラを片手や両手で構えたり、三脚等を用いたりする場合でも検知する技術開発を行った。（１－１）における赤外線光源による抑止を回避するために撮影時に赤外線カットフィルタの利用が想定されるため、この識別を可能とすることも目標とされた。実験の結果、次のような成果が得られた。

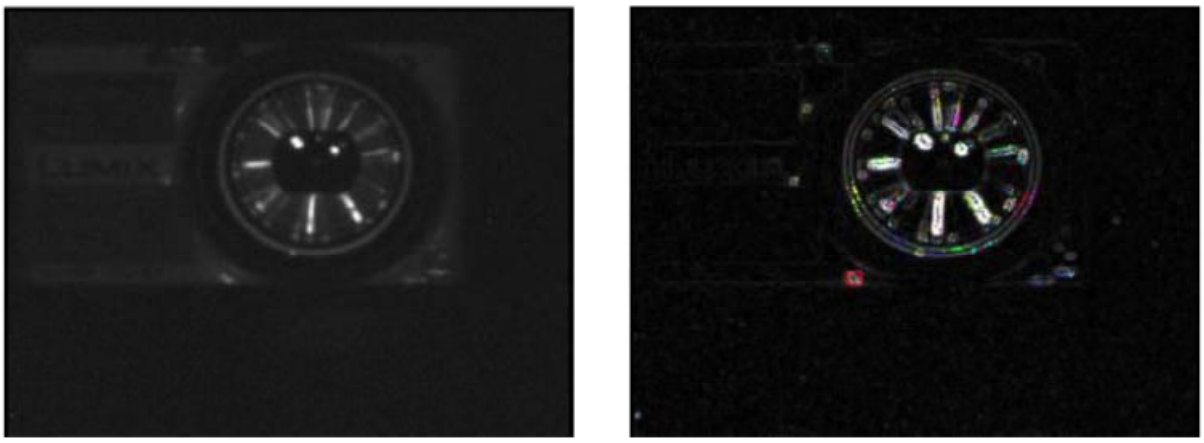
- 撮影機材のうち、デジタルカメラ、ビデオカメラ、一眼レフカメラ、スマートフォンについては、ディスプレイ側から照射する赤外線ＬＥＤの分光画像から、レンズ相当部分で生ずる反射の点状のハイライトをを円形のエッジとして抽出することができ、射影ヒストグラムを可変閾値法によって分析を行

うことで、レンズの検出に成功した。一方、カメラ機能付き携帯電話については、レンズの抽出ができず、検出に失敗した。

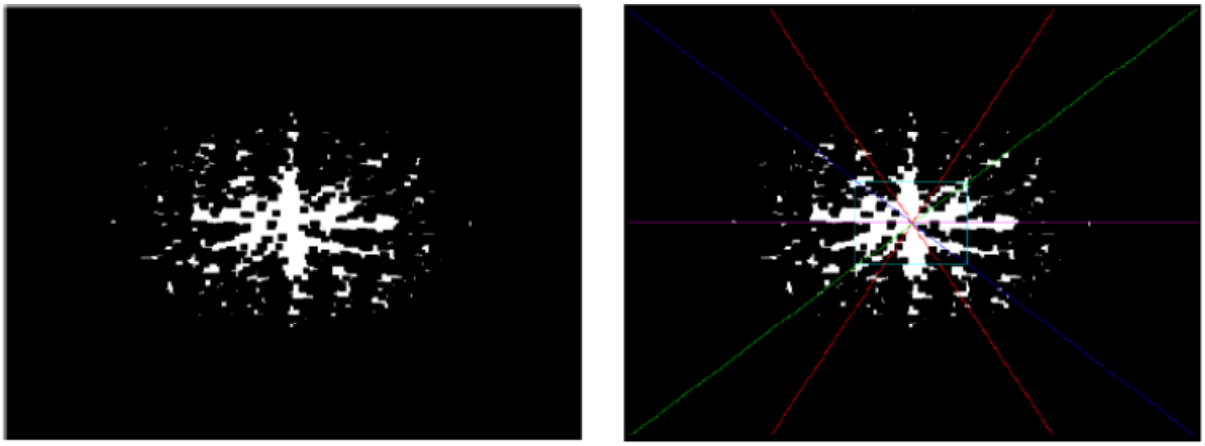
- 赤外線カットフィルタの識別に関しては、照射した赤外線が反射する反射型と吸収型（反射防止コーティングなし）のものについて、分光画像を処理することで検出に成功した。一方、吸収型赤外線フィルタ（反射防止コーティング有り）については検出できなかった。
- 人が撮影機材を操作する行為に関しては、両手、片手共に体の前面で撮影する行為を検出することができた。しかしながら、体の側面方向に手を伸ばした状態では撮影行為を検出することができなかった。当該行為を検出するために腕を側面方向に広げる行為も撮影行為とすることは誤報増加の原因となるため、分光画像による撮影機材の検出など、他の原理手法との組み合わせを検出する必要がある。



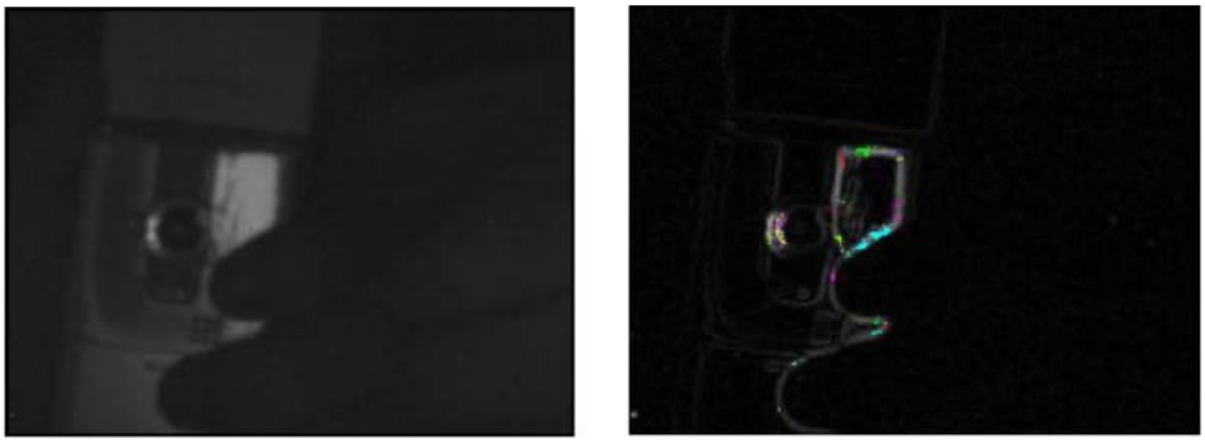
図ｄ－９　撮影者の識別技術のイメージ



図ｄ－１０　エッジ抽出による画像処理に基づくデジタルカメラの識別（成功例）

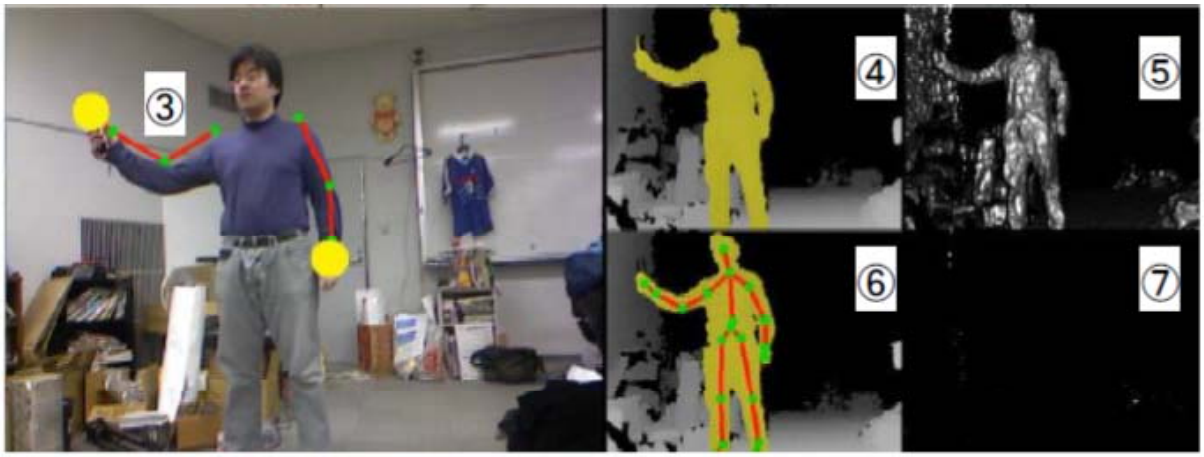


図ｄ－１１　可変閾値法による画像処理に基づくデジタルカメラの識別（成功例）



図ｄ－１２　エッジ抽出による画像処理に基づく携帯電話のレンズの識別（失敗例）

図ｄ－１３　撮影者の識別に関する実験結果（成功例）



図ｄ－１４　撮影者の識別に関する実験結果（失敗例）

（２）特許・論文等の状況

本研究開発の成果をもとに出願した特許、発表した論文等は次の通りである。

表ｄ－２　特許・論文等件数

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
0	0	3	0	0	0	0

① 特許出願

特許の詳細は次の通りである。

（ａ）認証媒体の製造方法、認証媒体、及び認証システム

本研究にて開発した蛍光体ガラスを用いて、陶磁器やガラスなどの製品の真正を判定する技術について特許を出願した。本技術では、蛍光体ガラスを認証媒体とし、励起光を照射した際に蛍光体ガラスが発する赤外線によって対象の真正を判定する。当該蛍光体ガラスは透明であるため、真正判定対象の外観を損なわずに真正判定が出来る。本特許情報を下記に示す。

【発明の名称】：認証媒体の製造方法、認証媒体、及び認証システム
【発明者】　：藤川　真樹（綜合警備保障株式会社）
村山　千明（ウシオ電機株式会社）
小田　史彦（ウシオ電機株式会社）
森安　研吾（ウシオ電機株式会社）
渕　真悟（国立大学法人名古屋大学）
竹田　美和（国立大学法人名古屋大学）

（ｂ）複写防止用紙

本研究にて開発した蛍光体を用いて、紙面上の機密情報などの複写を、当該紙面の外観を損なわずに防止する技術について特許を出願した。本技術では、可視光を励起光として赤外線（不可視光）を発光する蛍光体（紙面と同色）を紙面へ塗布するため、紙面の外観を損なわずに機密情報などの複写を防止することが出来る。本特許情報を下記に示す。

【発明の名称】：複写防止用紙
【発明者】　：藤川 真樹（綜合警備保障株式会社）
小田 史彦（ウシオ電機株式会社）
渕 真悟（国立大学法人名古屋大学）
竹田 美和（国立大学法人名古屋大学）

（ｃ）盗撮防止シート

本研究にて開発した蛍光体ガラスを用いて、表示画面に表示された画像の盗撮を防止する技術について特許を出願した。本技術では、可視光を励起光として赤外線（不可視光）を発光する透明な蛍光体ガラス（主に粒子状）を表示画面上に設置するため、表示される画像の視認性を阻害せずに当該画像の盗撮を防止することが出来る。本特許情報を下記に示す（なお、本特許は平成２２年度に出願しているが、権利化を確実にするために蛍光体ガラスの作成方法等を追加し、国内優先権主張を利用して平成２３年度に再度出願したものである）。

【発明の名称】：盗撮防止シート
【発明者】　：藤川 真樹（綜合警備保障株式会社）
小田 史彦（ウシオ電機株式会社）
渕 真悟（国立大学法人名古屋大学）
竹田 美和（国立大学法人名古屋大学）

② 論文作成、国際会議における発表等

詳細は次の通りである。

【原著論文】

[1] Masaki Fujikawa, Fumihiko Oda, Kengo Moriyasu, Shingo Fuchi & Yoshikazu Takeda : "Proposal for a New Artifact-Metrics Method (Application to Valuable Pottery, Porcelain and Glass Products)", International Journal of Information and Electronics Engineering (IJIEE), (to be published)

[2] Masaki Fujikawa, Hikaru Mori & Kenji Terada : “Study of the Detection System for Onscreen Contents Shooting (Countermeasure Against Information Leakage by Video Recording/Photo Shooting)”, International Journal of Information and Electronics Engineering (IJIEE), (to be published)

【国際会議】

[1] Masaki Fujikawa, Fumihiko Oda, Kengo Moriyasu, Shingo Fuchi and Yoshikazu Takeda : "The New Verification Method of Authenticity for Pottery and Porcelain Products", The 37th Annual International Computer Software and Applications Conference (COMPSAC 2013) (2013.07).
[2] Masaki Fujikawa, Fumihiko Oda, Kengo Moriyasu, Shingo Fuchi and Yoshikazu Takeda : "Proposal for a New Method of Authenticity of Pottery and Porcelain Products - Application of the Artifact-metrics Technology -", The International Conference on Information Society (i-Society 2012) (2012.06).
[3] Masaki Fujikawa, Ryosuke Kamai, Fumihiko Oda, Kengo Moriyasu, Shingo Fuchi, Yoshikazu Takeda, Hikaru Mori and Kenji Terada : "Development of Countermeasure Systems for Content Leaks by Video Recording/Camera Shooting", The International Conference on Information Society (i-Society 2012) (2012.06).

【技術報告】
[1] 藤川真樹、森輝瑠、寺田賢治："モーションキャプチャを用いた撮影検知システムの構築と評価"、情報処理学会コンピュータセキュリティシンポジウム 2013 (2013.10)
[2] 藤川真樹、小田史彦、森安健吾、渕真悟、竹田美和："有価陶磁器に対する人工物メトリクス適用のための研究"、情報処理学会コンピュータセキュリティシンポジウム 2013 (2013.10)

【受賞】
"有価陶磁器に対する人工物メトリクス適用のための研究"、情報処理学会コンピュータセキュリティシンポジウム 2013 優秀論文賞

３－２－ｄ　目標の達成度

本研究開発による目標の達成状況を下表に示す。

表ｄ－３　目標に対する成果・達成度の一覧表①

要素技術	目標・指標	成果	達成度
透明赤外線光源の開発	・赤外線を発光するシートを開発することで、撮影されたコンテンツに光学的なノイズを含ませる（コンテンツの品質を低下させる）。	・波長880nmで発光する透明な蛍光体ガラスの開発に成功。 ・発光効率25%を達成。 ・ノイズとしての赤外線の発光に成功したが、コンテンツの識別性低下には至らず。 ・画面に設置されたフィルタがカットされたことを検知するセンサーを開発。	概ね達成
赤外線遮断対抗技術の開発	・品質の高いコンテンツが記録されることを防止するため、IRカットフィルターがディスプレイの近傍にあることを検知できる手法を開発する。 ・撮影行為を検知できる手法の開発を目指す。	・赤外線カットフィルターをレンズの前面に設置した撮影、カメラ単体による撮影の検知に成功。 ・片手、両手でカメラを構えたり、三脚等を用いてカメラを構える行為の検知に成功。 ・実証実験では眼鏡のレンズの誤検知や、反射防止型フィルタや携帯電話による撮影などの検知漏れなどの問題が生じており、実用化には更なる精度向上が必要。	概ね達成
成果の普及啓発	・成果に基づく特許を出願する。 ・国内および海外で開催される学術集会において研究発表を実施する。 ・当該集会等においてセンサーシステム等をデモ展示する。	・特許出願3件 ・ARES 2011、SCIS2012にて口頭発表。 ・CSS2011にて口頭発表及びデモンストレーションを実施。 ・CSS2013における派生研究“有価陶磁器に対する人工物メトリクス適用のための研究”の発表において、優秀論文賞を受賞。	達成

各年度の詳細な成果は次の通りである。

① 平成２２年度

【透明赤外線光源の開発】

- 蛍光体ガラスの開発に関して、９００nm の赤外線を発光する蛍光体ガラスの生成に成功した。
- ＩＲシート光源として、蛍光体ガラス（粉末、丸い粒）を透明なポリマー樹脂（ＫＥ－１０６）に封入したり、屈折率を調整したりすることなどにより、高い透明度をもつ光源の実現可能性を検討した。これによって、封入するガラスと樹脂との屈折率を同じにすることにより、ガラスの粒を見えにくくすることが確認された。
- ＯＨＰシートをＩＲシート光源に見立てて、その長辺部分にセンサーを取り付けることにより、ＯＨＰシートの取り外しを検知できることを確認し、ＩＲシート光源の取り外しを検知するセンサーシステムを開発することができた。しかしながら、当該システムの組み込みを知った者は、センサーが取り

付けられている部分を避けるようにして光源をカッターナイフ等で切り取り、コンテンツを撮影するものと予想されるため、その対策の必要性が新たに確認された。

- 実証実験を通じて、次の３点の知見が得られた。
  - 人間の目は赤外線を認識しないが、ＣＣＤやＣＭＯＳ等のイメージセンサーは赤外線を白っぽい光として認識し、撮影されたコンテンツの品質を低下させることができる。
  - ディスプレイの表面光沢の有無が、コンテンツの品質低下具合に違いを出すことはない。
  - 一眼レフカメラは赤外線をノイズとして認識しなかったが、ビデオカメラ、コンパクトカメラ、小型カメラは赤外線をノイズとして認識した。
- 光が人体に与える障害の種類や、それぞれの障害に対する許容露光量、電気的光源から放射される光による障害の度合いを評価するための基準などを定めた文書（CIE S 009/E:2002）等の文献調査から、赤外線発光シートを生成するときには、当該シートがもつ放射照度と放射強度の値は、液晶ディスプレイにおけるそれぞれの値と同等かそれ以下に設定する必要がある成果が得られた。

【赤外線遮断対抗技術の開発】

- 簡易型の近赤外線・分光イメージャーを用いて４つの検体（吸収タイプカットフィルター、反射タイプカットフィルター、フェルト布、アルミ板）の分光画像を撮影した。この結果、画像処理とパターンマッチングによって分光画像からカットフィルターを切り出し、それが反射タイプか吸収タイプかを判定できる可能性があることを確認した。

【成果の普及啓発】

- 下記の２件の特許を出願した。
  - 【発明等の名称】盗撮防止シート
    【出願日】平成２３年２月１６日
    【出願番号】特願２０１１－０３１４４９
  - 【発明等の名称】複写防止用紙
    【出願日】平成２３年２月１６日
    【出願番号】特願２０１１－０３１４４８

② 平成２３年度

【透明赤外線光源の開発】

- 前年度開発した蛍光体ガラスを改良し、透明度を高めるとともに目標の８７０nm に近い８８０nm で発光する蛍光体ガラスの開発に成功した。ただし１ｋｇの材料で大型のガラス板を作成する計画は、複数回試みたもののいずれもアルミナ製の坩堝が割れてしまい、失敗に終わった。残った材料と白金製の坩堝を用いて５cm 角、２mm 厚の板ガラス２枚を生成し、以降の実験で使

用した。

- 粒ガラス状のプロトタイプで赤外線を発光させ、環境照度を変えながら撮影妨害効果を観測した結果、環境照度 103 ルクス以上ではプロトタイプからの赤外線発光を観測できず、撮影妨害効果を得られる環境照度は数十ルクス未満であることが確認された。ディプレイを用いた作業をを行うオフィスの照明基準は、水平面照度 750 ルクス、鉛直面照度 100～500 ルクスであり、さらにディスプレイ本体からの光が加わるため、現状性能ではディスプレイ上のコンテンツの撮影防止用のＩＲシート光源として使用することは困難である。ＩＲシート光源として使用するためには、赤外線の発光強度を現状の１０倍程度に向上させる必要があると考えられるが、蛍光体ガラスの発光効率の向上のみでは実現は難しく、蛍光体ガラスの個数や配置、励起光強度の向上が必要となる。
- 板ガラス状のプロトタイプで赤外線を発光させ、ディスプレイ上でノイズの発生について検証した結果、ガラスの端面部分で発光が観測されるものの、ガラスを通じて表示されるコンテンツを全面的に覆うほどの光学的ノイズは見られなかった。これは、蛍光体ガラスに照射された励起光が、光源からの距離に応じて指数関数的に減衰するため､光源から約 2mm 程度の範囲のみ赤外線の発光が観測される結果をもたらすことによると考察された。
- 前年度の取り外し検知センサに関する検討において、刃物等によるＩＲシートのカットの可能性に対応するため、カット検知センサの開発を行った。実用化時のシートの製造コストへの影響を考慮し、メッシュ形状の導線パターンを基本とし、カット検知のための格子状導線パターンを絶縁エリアとして適用する導線パターンを考案した。このサンプル版を作成し、ディスプレイ前面に設置したところ、画面上のモアレを発生させることなく表示が可能であり、かつシートのカットによりシート内の抵抗値が変化することが確認された。シートの設置による光量（照度）の低下は最大でも 15%程度にとどまるため、コンテンツの確認を十分な明るさのもとで視認できるものと判断した。これにより、カット検知センサシステムの要件を満たす、ハードウェア、ソフトウェア構成を実現した。

【赤外線遮断対抗技術の開発】

- 前年度よりも高スペックな分光イメージャーを用いて試料の分光画像を撮影したところ、表面に光反射防止コーティングを施していない吸収型赤外線カットフィルターや、カメラのレンズ部および筐体部は、照射した赤外線を反射することを確認した。これをもとに分光画像を用いた撮影行為の検出手法を開発した。実証実験の結果、､照射した赤外線が反射する反射型と吸収型（反射防止コーティングなし）の赤外線カットフィルターの分光画像は、各処理を行うことで赤外線カットフィルターの存在を検出することが出来た。しかしながら、赤外線の反射を検出出来ない吸収型赤外線カットフィルター（反

射防止コーティングあり）は検出することが出来なかった。当該赤外線カットフィルターを検出するためには、円状のハイライトの有無以外の検出手法の検討が必要であることが明らかとなった。

- 画像におけるエッジ抽出処理とパワースペクトル画像の特徴の分析により、当該分光画像中に赤外線カットフィルターまたは撮影機材が存在しないことを判断可能であることを確認した。撮影機材についてはデジタルカメラ、ビデオカメラ、一眼レフカメラ、スマートフォンの分光画像は、各処理を行うことで撮影機材の存在を検出することが出来た一方で、携帯電話の分光画像には円状のハイライトが無いため、撮影機材の存在を検出することが出来なかった。当該撮影機材を検出するためには、照射する赤外線 LED の強度を上昇させる等の手法を用いる必要がある。
- 距離画像センサ（Kinect）を用いることにより、両手、片手及び三脚を用いた撮影行為の検出の実証実験を実施した。その結果、両手、片手共に体の前面で撮影する行為を検出出来た。しかしながら、体の側面方向に手を伸ばした状態では撮影行為を検出することは出来なかった。当該行為を検出するために腕を側面方向に広げる行為も撮影行為とすることは誤報増加の要因となるため、分光画像による撮影機材の検出などの他原理手法との組み合わせを検討する必要がある。また、計測エリア内の三脚の設置とカメラのレンズの検出が出来た。これにより、遠隔操作による撮影を検出出来ることがわかった。

【成果の普及啓発】

- 可用性、信頼性とセキュリティに関する国際会議（International Conference on Availability, Reliability and Security）は、前年（2010 年）の採択率 25%であり、IEEE 等の国際的な機関のイベントカレンダーに掲載されており認知度が高い。また、企業の研究成果を発表できる Industrial Track が設けられており、ビジネスマッチングの機会があることから発表先として適切であると判断された。発表と共に試作した蛍光体ガラスとセンサーのプロトタイプを用いたデモンストレーションを行い、セッション終了後にディスカッションを行った中で、下記のような質問や意見を得た。
  - 同じ目的をもって研究を進めている団体は他にあるか。
  - 光励起により赤外線を発光する素材を用いることは興味深く、電気を用いないことは一種のクリーン＆グリーンエネルギーと言える。
  - 赤外線発光シートの開発だけでなく、当該シートの取り外しやカットを検知するセンサーを開発し、セキュリティ的にバランスが取れている。
  - 更にセキュリティを高めるために、配線の断線検知や、シートと同じ大きさの赤外線カットフィルターをシートの表面に貼り付けて赤外線を遮断させる攻撃に備えるべきである。
- コンピュータセキュリティシンポジウム（CSS）2011 にて研究発表を行うと

ともに、蛍光体ガラスのサンプル、試薬、各種センサー、システムの試作品やデモ映像を展示した。これにより、参加者の投票（１人２団体まで）によって選出される「最優秀デモンストレーション賞」を受賞した。研究発表後の質疑やデモ展示においてディスカッションを行った中で、下記のような質問や意見を得た。

- 撮影による情報漏洩の影響度が高いことが理解出来た。
- シャッター操作を遠隔で行った場合（ぶら下げた状態で撮影）は検知できるのか。
- 携帯電話（スマートフォン含む）のパスワード盗撮の防止に活用できる可能性がある。

● 暗号と情報セキュリティシンポジウム（SCIS）2012 にて研究発表を行い、研究発表後の質疑においてディスカッションを行った中で、下記のような意見を得た。

- 無機材料の限界：無機材料を用いた光源は高いエネルギー（励起光、電圧など）が必要であるため、小型化・薄型化・省電力化が難しい。
- 有機材料の可能性：有機材料は薄くて柔軟性があり、低いエネルギーで可視光を発光する有機 EL ディスプレイが存在しており、これを応用した赤外線発光シートの開発に見込みがある。

● ３件の特許を出願した（３－１－ｄ（２）に記載の通り）。

４－ｄ　事業化、波及効果について

４－１－ｄ　事業化の見通し

（１）撮影防止技術の事業化

本研究開発成果の製品化に向け、引き続き自己資金による研究開発が実施されている。しかしながら、研究開発を通じて実用化の手段として利用不可能であることが明らかとなったガラスの代替物となる、赤外線発光が可能な低価格有機 EL（エレクトロルミネセンス）が、まだ市場に存在しないことが障害となっている。また、撮影者検知については、依然として誤検知防止の精度向上が必要な状況になる。

このほか、実施機関において市場調査を実施したところ、撮影防止ソリューションへのニーズが未だ不明確なことが明らかになっている。

（２）派生的事業化の可能性

本研究開発の成果は、以下の各分野での応用による事業化が期待できる。

①蛍光体ガラスの応用

● 当該ガラスは、透明度が高く、光励起により赤外線を発光するため、陶磁器、ガラスなどの製品や紙面などの電源供給が出来ない対象物に設置し、外観を損ねることなく陶磁器などの対象物の真正性判定を行うことができる。当該

蛍光体ガラスの赤外線発光強度は低いが、真正性判定は赤外線の発光が常時必要な本事業の本来用途とは異なり、判定時のみ赤外線発光を得ることが出来れば良いため、蛍光体ガラスを用いた真正性判定への応用可能性がある。

- 具体的な蛍光体ガラスの設置・真正性判定方法の検討のため、現在、関連事業者（ブランド企業、窯元、問屋など）へのヒアリング等を通じたニーズ調査の段階にある。

②カット検知センサーの応用

- 当該センサーは、透明度および柔軟性が高いため、小売店などで陳列されている商品や美術館などの展示品を、外観を損ねることなく展示ケースに張り付けたり、箱状などに加工した当該センサーで包みこんだりすることが可能である。本特性を活かし、当該センサーをカット（破りを含む）して商品や展示品などの対象物を持ち出す行為や、商品などに取り付けられた盗難防止 IC タグの取り外す行為を検知する盗難防止センサーとしての応用が考えられる。また、同様にして対象物を包み、トレーサビリティにおいて対象物のすり替えなどを検知する開封検知センサーとしての応用も考えられる。
- カットと漏液を検知できる透明なセンシングデバイスは、現在のところ本成果が世界的にも唯一の存在である。
- しかしながら、当該センサーは、使用する透明導電シート内の導線を全て接続したり、導線に通電するための電源を供給したりする必要があるため、対象物を包む際の導線設計、電源や異常通知方法などの検討が必要である。

４－２－ｄ　波及効果

成果を継承した現在進行中の研究が３つある（人工物メトリクス、カットと漏液を検知できる透明なセンシングデバイス）。この事業化への取り組みを通じて、研究成果の普及拡大につながっている。

上記のうち、人工物メトリクスについては 2013 年に情報処理学会コンピュータセキュリティシンポジウムにおいて優秀論文賞を受賞した。このため、技術的に大きなインパクトをもたらしたものと評価される。

５－ｄ　研究開発マネジメント・体制・資金・費用対効果等

５－１－ｄ　研究開発計画

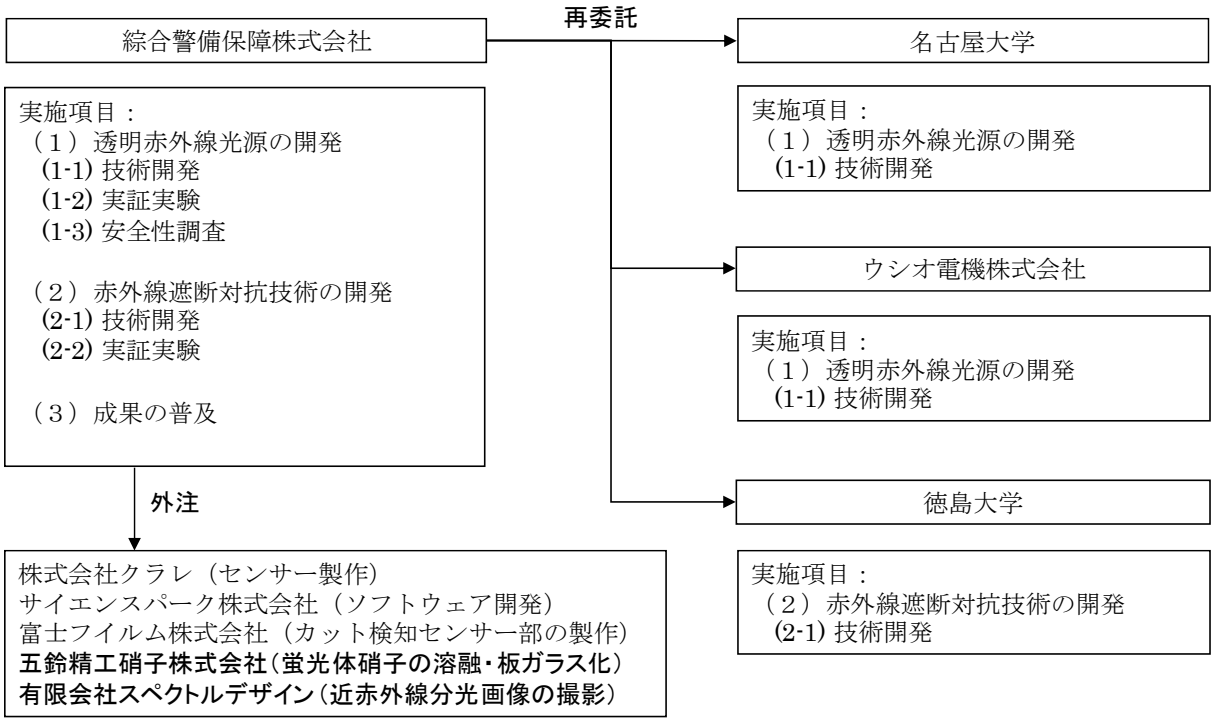
本事業は、平成 22 年度から 23 年度までの 2 年計画である。各要素技術の研究開発計画は次のとおりである。４－ｄにて記載の通り、研究開発の途上においてガラス蛍光体を用いたシート状の赤外線発光シートの開発が失敗したことが明らかになったが、これを早い段階で推進委員会に報告した。推進委員会委員からは、「失敗を糧として今後の研究に生かしてほしい」という励ましの言葉をいただいている。

表ｄ－４　研究開発計画

年度	平成22年度	平成23年度
予算額	12.2百万円	16.4百万円
透明赤外線光源の開発	技術開発 実証実験 安全性調査	技術開発 実証実験
赤外線遮断対抗技術の開発	技術開発	技術開発 実証実験
成果の普及啓発		成果の普及

５－２－ｄ　研究開発実施者の実施体制・運営

本事業は、平成 22 年度から平成 23 年度において、経済産業省から綜合警備保障株式会社への委託により実施されている。また各年度につき、再委託先として以下の機関が事業に参加した。なお、赤外線発光シートのカットを検知できるセンシングデバイスの開発にあたっては、オンスケジュールで研究開発を進めるために、綜合警備保障株式会社の社員３名の時限的な応援を得た。



図ｄ－１５　研究開発実施体制

５－３－ｄ　資金配分

表ｄ－５資金配分　　(単位百万円)

要素技術	平成22年度	平成23年度
撮影による情報漏洩を防止するソリューションの研究開発	12.2	16.4

５－４－ｄ　費用対効果

本成果に基づく事業化は未だ実現しておらず、成果を通じた売上は生じていない。将来的な事業化を通じては、撮影による情報の不正な持ち出し行為の防止による効果や、コンビニエンスストアのバックヤードにおける防犯カメラ映像の適切な管理による犯罪抑止効果等が期待できる。

５－５－ｄ　変化への対応

本調査研究の期間中の変化は、概ね当初予測されていた範囲内であり、計画の変更は不要であった。

③ クラウドコンピューティングに関するセキュリティ対策技術の研究開発
Ａ－ｅ　効率的な鍵管理機能を持つクラウド向け暗号化データ共有システム

１－ｅ　事業の目的

近年、脚光を浴びているクラウドコンピューティングは利用時に、プライバシー情報や機密性の高いデータをクラウドサービス提供者に渡して処理を行うため、データの機密性保護に関するセキュリティ上の問題が普及の妨げとなっている。

本事業は、利用の際に、企業が求める高度なプライバシー保護機能を持った暗号化データ共有システムの開発及び実証研究を行い、クラウドコンピューティングの上記の問題を解消した安全・安心なクラウドコンピューティングサービスを提供する基盤を構築することを目的とする。

２－ｅ　研究開発目標

上記の目的を達成するため、本事業において以下の項目を実施する。これらの目標の設定は、「属性ベース暗号方式」を使用した鍵発行システムの実用化を目指した際に懸案となる事項を解決し、事業化の際のハードルを今回の実証実験で洗い出し、それを取り除くということを主眼として設定された。

表ｅ－１　個別要素技術の目標

要素技術	目標・指標	妥当性・設定理由・根拠等
研究作業	・属性ベース暗号の理論検証 ・属性ベース暗号の運用モデルと失効リストのチェック機能の理論構築 ・実証環境下における問題の洗い出し	・属性ベース暗号の実用化にあたり、一度秘密鍵を発行すれば、鍵が消失しない限り利用者は復号を行い続けることが可能な問題の解決方法について検討する。
評価システム構築	・開発実験環境の構築 ・全体設計 ・評価システムの構築 ・評価の実施	・研究作業において追加された失効リストにより、属性ベース暗号の問題の解決が可能かどうかを検証するためのシステムを構築して、評価を行う。
鍵管理機能の構築	・設計、構築、動作検証	・上項の成果をもとに、鍵の発行や失効鍵の管理機能等を設計し、クラウド環境上に実装する。
モデルシステムの構築	・検討、設計、構築、動作検証	・属性ベース暗号方式の利用が最適と思われるサービスモデルをクラウド環境上に構築する。
モデルシステムの実証実験	・実証実験（1回目） ・中間レビュー ・実証実験（2回目）	・属性ベース暗号がクラウド環境上で有効に機能することを実証する。
普及活動及び意見収集	・準備 ・各種発表	・本成果を展示会、セミナー、論文発表の形で広く内外に告知する。

各年度の詳細な目標は次の通りである。

① 平成２２年度

【研究作業】

- 属性ベース暗号の実装をするにあたり、鍵生成、暗号化、復号それぞれに必要な理論について検証を行う。また、必要となるプログラミング処理の洗い出しを行い、システム全体の制御構造に関する設計の下調べを行う。
- 属性ベース暗号の運用モデルとして、鍵生成局、データ送信者、データ受信者の理論的な計算量や通信量を考慮し、属性ベース暗号方式実装において望ましいシステムの運用モデルの構成を検討する。
- 失効リストによるチェック機能を追加するにあたって、計算量や通信量の観点から望ましい方式の分析を行い、実装するにあたっての必要な処理を検討する。
- 上記の理論的な観点を考慮した上で望ましい属性ベース暗号方式の運用モデルを構築し、その上で、実証実験を実施機関の社内で行う上でのシステム全体の存在しうる問題点を洗い出す。
- 実証実験を行う上で必要なマシンスペックやネットワーク環境なども考慮し、理論的、実証的な観点から再度、問題を洗い出す。
- 設計をするにあたって理論的、実証的に望ましい「失効リストによるチェック機能付きの属性ベース暗号方式」の運用モデルをまとめ、評価システム構築時に参考とするようにする。

【評価システム構築】

- プロジェクト開発環境として、参加メンバ間の情報共有および知識の蓄積、進捗管理、問題点管理等を実施するためのグループウェア環境を用意する。
- 機能評価を実施するための仮想環境と各モジュールの性能評価を実施することにより、評価環境を構築する。
- 研究実施結果に基づいて、鍵生成モジュール、暗号モジュール、復号モジュール、失効モジュール等、モジュール単位の設計を実施する。
- 機能評価及び性能評価を実施するための条件や手順などの評価手法について設計を行う。
- 研究実施結果に基づいて、実証システムの設計を実施する。特に今回はクラウド環境に構築する実証実験環境であることを考慮した設計を行い、最終的な実証環境となるクラウドベンダの選定まで実施する。
- 鍵生成モジュール、暗号化モジュール、復号化モジュール、失効モジュー等、モジュール単位の構築を実施する。
- 機能評価環境、性能評価環境において、評価を実施する。評価を実施した結果、当初予定していた目標に達しない場合は、機能追加・チューニング等の作業を行い目標に近づけるよう努め、再度評価を実施する。
- 情報処理学会主催:第 73 回全国大会にて発表を行うため、研究作業結果と評価システムの構築内容を元にして、論文を作成する。評価システムの評価結

果については、論文発表原稿に追加資料としてまとめる。論文発表を実施し、有識者に研究作業結果に対する意見や評価を求める。

- 論文発表や質疑応答により収集した意見や評価をまとめる。まとめた内容は、実証環境構築の際に反映する。

② 平成２３年度

【鍵管理機能の構築】

- 前年度の成果である属性ベース暗号の各モジュール（セットアップ機能モジュール、鍵生成モジュール、暗号化機能モジュール、復号化機能モジュール、鍵管理機能モジュール）を使用して鍵管理機能を構築する。
  - 鍵管理機能として、利用者から「鍵の発行」の依頼を受けて鍵を発行する機能、失効鍵の管理などの機能を設計する。
  - 前項にて作成した内容をクラウド環境上に構築する。
  - 前項にて構築した機能が、設計内容どおりに動作することを検証する。

【モデルシステムの構築】

- 前年度の研究結果をもとに、鍵失効機能付き属性ベース暗号方式の利用が最適と思われるサービスモデルをクラウド環境上に構築し、システムの検討を行う。
  - モデルシステムとして、既存のクラウドサービスの中で、属性ベース暗号を応用することで、サービスとして広く普及することが見込まれる有用性の高いモデルの検討を行う。
  - 前項にて検討したモデルシステムを実現するために必要となる機能や現存のサービスを洗い出し、目的とするシステムが円滑に稼働するように設計する。
  - 前項にて設計した中で、前年度に製造をおこなったモジュールにはない機能やインタフェース部分について製造を行い、現存するモジュールと組み合わせて目標とするモデルシステムを構築する。また、構築したシステムに鍵管理機能を組み込んでモデルシステムを完成させる。
  - モデルシステムが設計通りに動作することを検証する。

【実証実験】

- 前項で構築したモデルシステムを使用して属性ベース暗号がクラウド環境にて有効に機能することを実証する。
  - 第１回目の実証実験として、実際の運用に近い環境での実証を行い、実用上問題がないか検証を行う。
  - 前項の結果を評価し、問題点があれば改善策を検討し、フィードバックを行う。
  - 第２回目の実証実験として、フィードバックを行った結果をもとに、再度実証実験を行う。
  - 実証実験で明らかになった有用性もしくは、発見された問題点・解決策

の反映結果等をまとめる。

【普及活動及び意見収集】

- 研究開発成果を展示会、セミナー、論文発表の形で広く内外に告知することで、広くクラウドサービス上で「属性ベース暗号」を利用することでクラウドサービスが安全に利用できることを認知させる。
  - 平成 23 年 7 月に、OSC 京都のセミナーおよびブース展示を行い、前年度の成果である属性ベース暗号の各モジュールの説明を行い、開発者向けに「属性ベース暗号」の普及を実施する。
  - 平成 23 年 10 月に、コンピュータセキュリティシンポジウム（CSS)2011 にて論文発表及びブース展示を行うことで、セキュリティの有識者に事業成果を報告し、意見を募集する。
  - 平成 23 年 10 月に､ITExpo もしくはセキュリティ EXPO 等の一般利用者向けの展示会に出展し、一般利用者向けの普及活動を行う。一般利用者には「属性ベース暗号」の認知度を向上させると伴に、クラウドサービス上で「属性ベース暗号」を使用することにより、利用者にセキュリティコントロールが取り戻せる点をアピールする。
  - 平成 23 年 11 月に、実施機関にて自社セミナーを開催し、弊社顧客に対して「属性ベース暗号」の認知度を向上させると伴に、クラウドサービス上で「属性ベース暗号」を使用することにより、弊社顧客にセキュリティコントロールが取り戻せる点をアピールする。また、セミナールーム内で展示も行う。

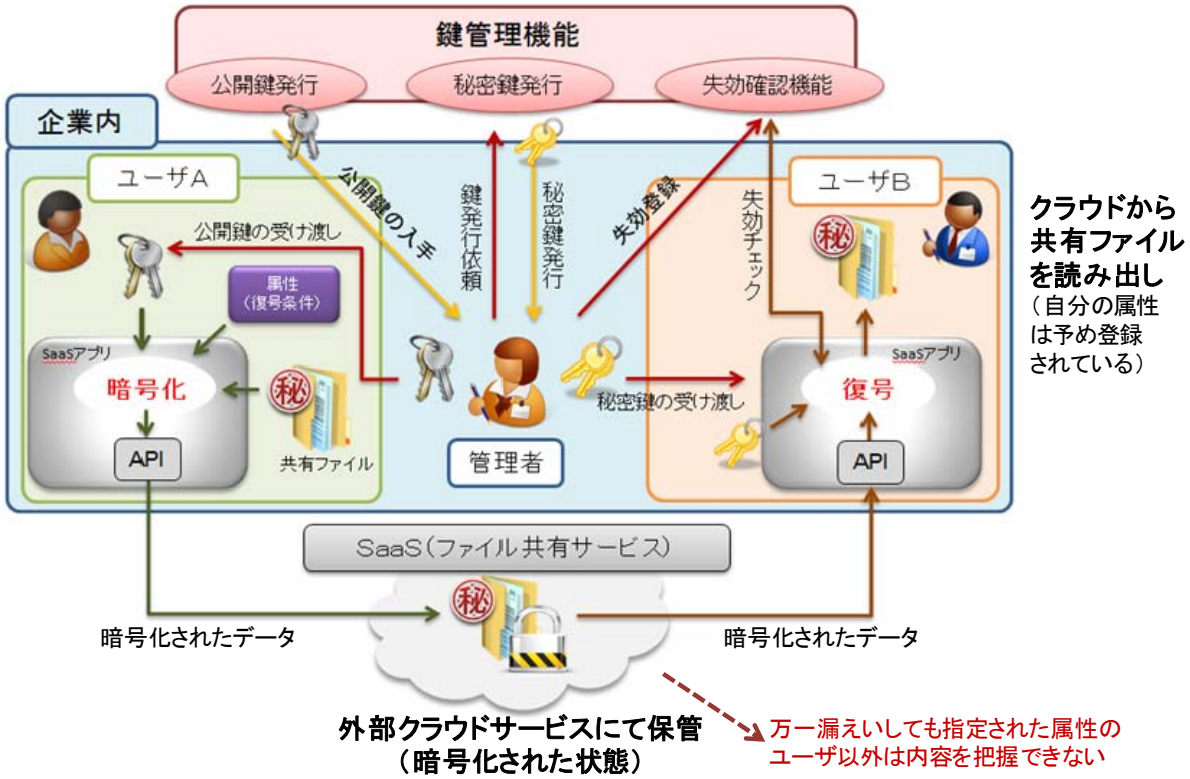
３－ｅ　成果、目標の達成度

３－１－ｅ　成果

（１）成果

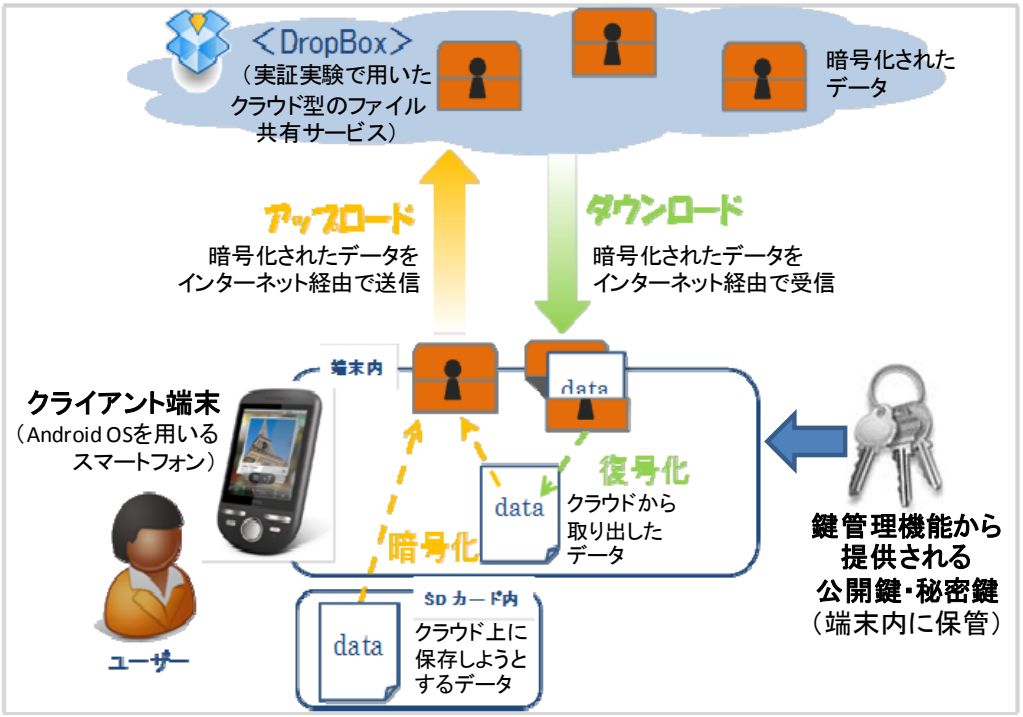
クラウド上のデータを安全に管理するための暗号化鍵の管理システムとして、次図に示すようなモデルシステムを設計し、この性能評価を行うためのプロトタイプを作成した。実験ではクラウドサービスとして DropBox を利用し、ユーザからは Android を OS とするスマートフォン端末でアクセスする環境を構築した。

属性ベース暗号方式を用いた鍵発行システムは、これまでの主流である PKI 方式に比べ、１つの暗号データを複数の人が復号することができるので、暗号データを大量に格納する必要があるシーンで有用と見込まれる。



図ｅ－１　モデルシステムにおける鍵管理機能の利用イメージ

（ユーザがクラウドに対して共有ファイルの保存、読み出しを行う場合に必要となる鍵の受け渡しの関係図）



図ｅ－２　実証実験で用いたクライアント端末とクラウドサービスの構成イメージ

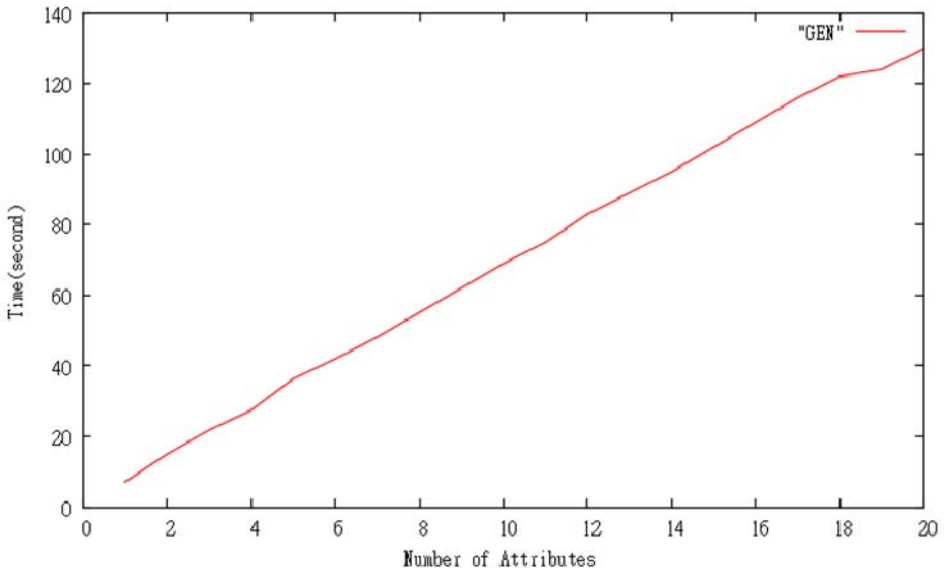
性能については、次の２回の実験で測定されている。

① 評価システムを対象とする性能測定

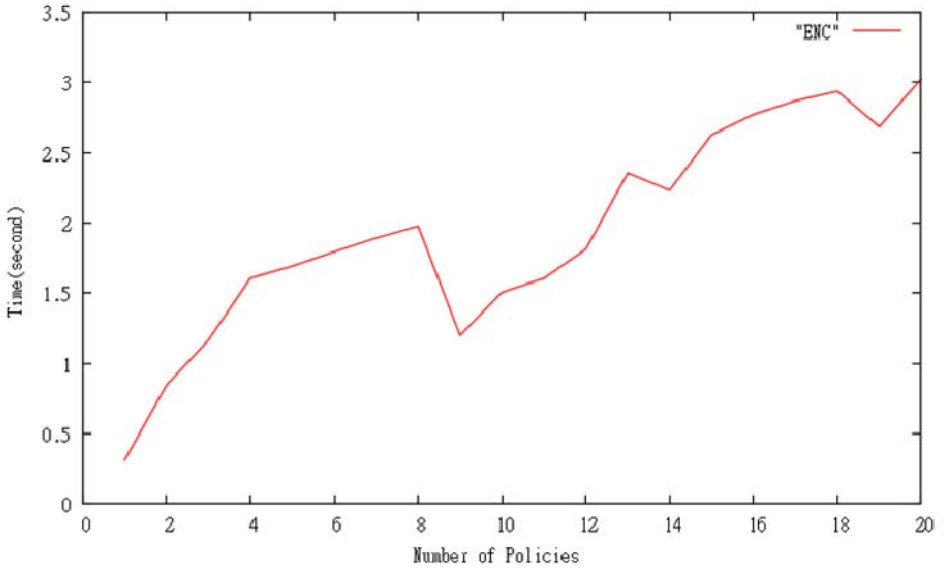
利用者 200 万人、失効者 50 万人、ユーザの属性が最大 20 種類、復号の条件が最大 20 条件のもとで評価を行った結果、それぞれ以下の結果を得た。

（評価システムの実行環境 : OS=CentOS 5.5、CPU=Celeron 1.3G、Memory=768M）

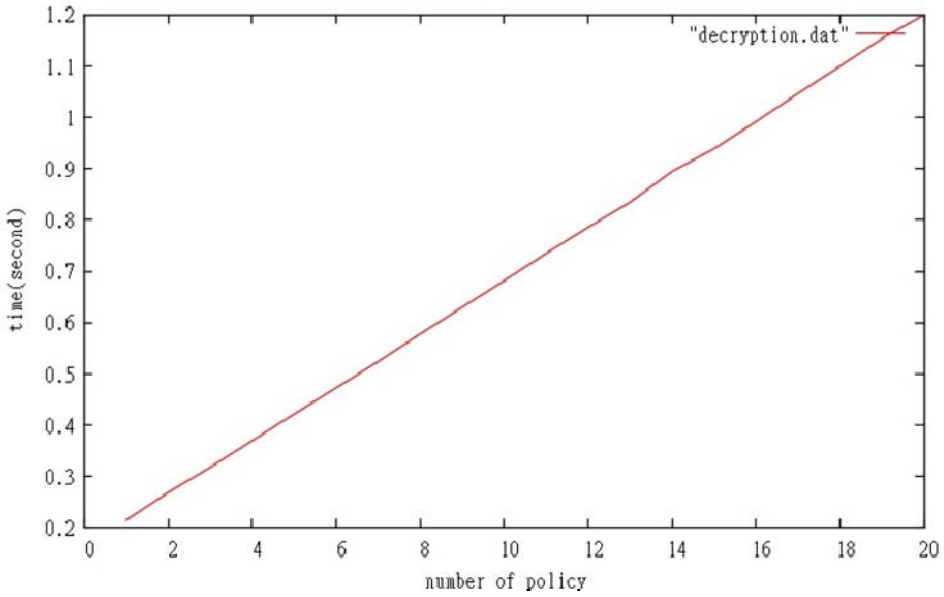
- 鍵生成時間：129.98 秒（属性数 20）
- 暗号化処理時間：3.14 秒（属性数 20）
- 復号処理時間：1.20 秒（属性数 20）
- 失効確認：0.29 秒（失効ユーザ数 50 万人）



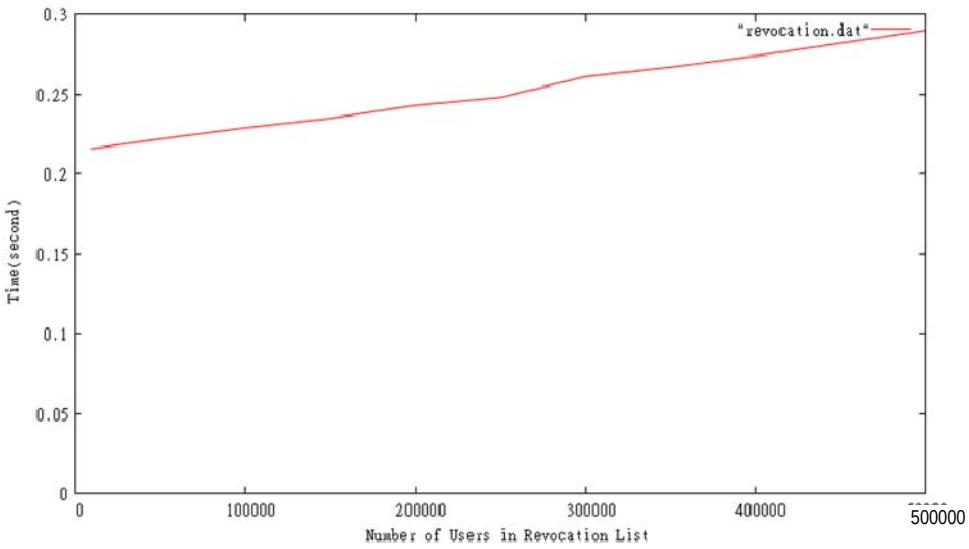
図ｅ－３　鍵生成処理時間の変化



図ｅ－４　暗号化処理時間の変化



図ｅ－５　復号処理時間の変化



図ｅ－６　失効ユーザ増加に伴う処理時間の変化

② モデルシステムを対象とする性能測定

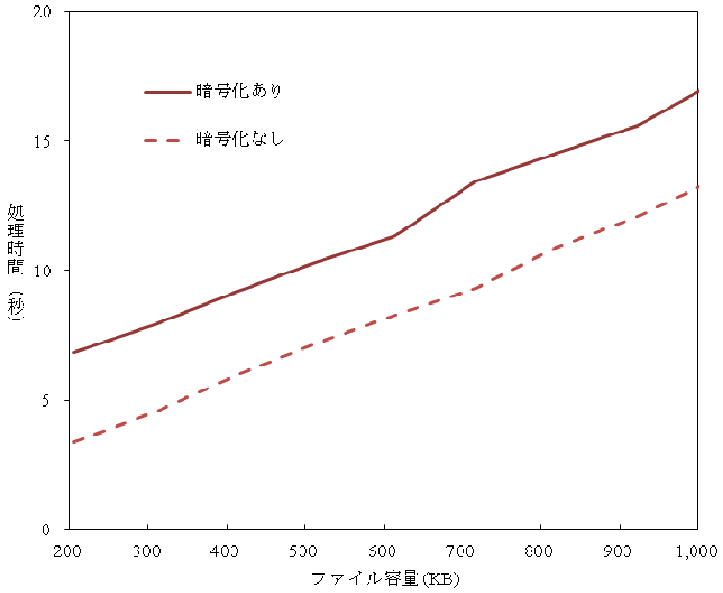
開発した Android 用アプリケーション「錠前屋」を用いたシステムの性能評価を実施し、次の結果を得た。これにより、属性ベース暗号において処理に影響を及ぼすと懸念されていた属性数に関して、数を増やしても処理時間には影響を及ぼさないことが確認された。

（測定環境）

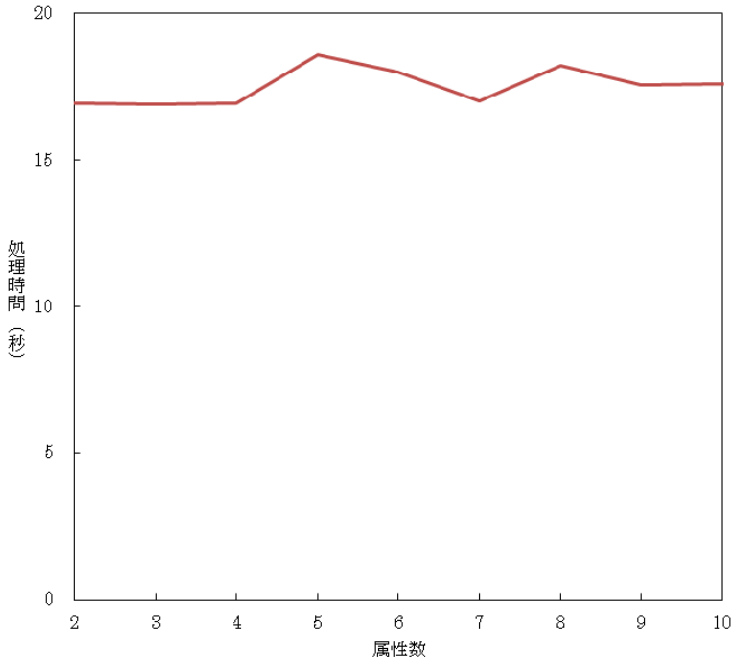
端末：OS=Android2.2、CPU=NVIDIA Dual Cortex-A9 1GHz、Memory=512M

回線：サーバ→端末=11Mbps／端末→サーバ=5.4Mbps

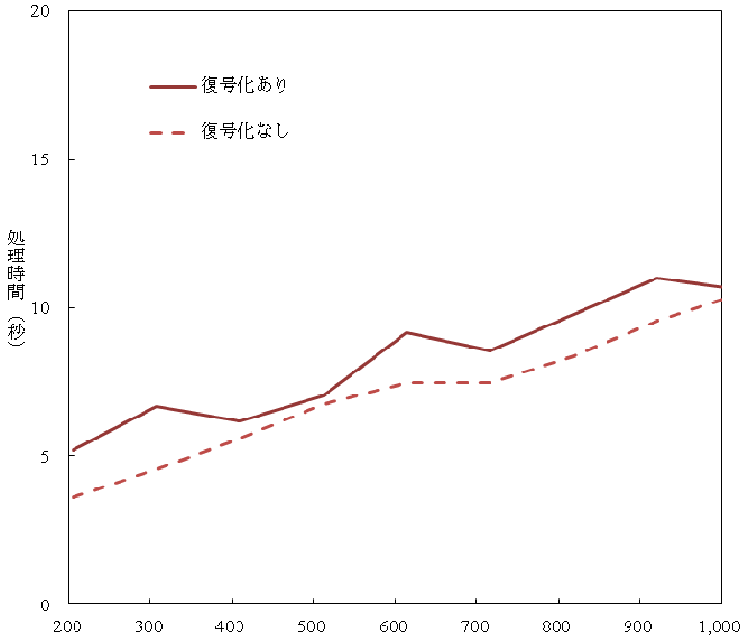
- 暗号化処理時間：約 3 秒（ファイル容量 1MBytes、属性数 10）
  （実際の操作にはこれに約 12 秒間の通信時間が加わる）
- 復号処理時間：1～2 秒（ファイル容量 1MBytes、属性数 10）
  （実際の操作にはこれに約 10 秒間の通信時間が加わる）



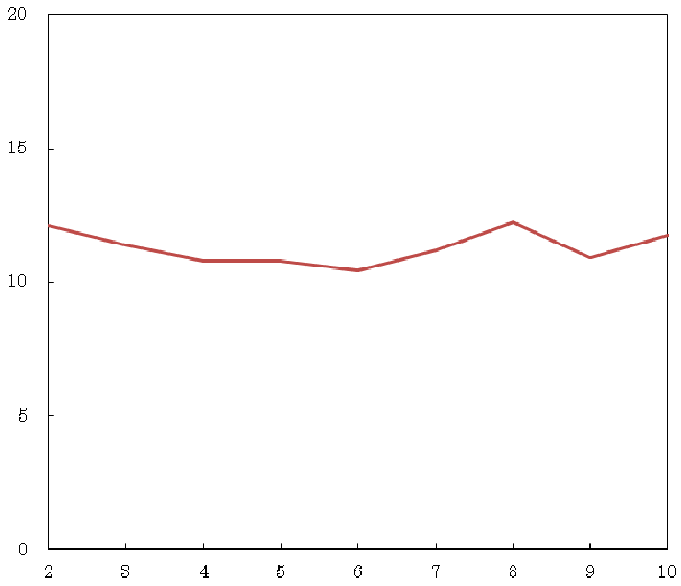
図ｅ－７　ファイル容量に対する暗号化処理時間



図ｅ－８　復号条件の属性数に対する暗号化処理時間



図ｅ－９　ファイル容量に対する復号処理時間



図ｅ－１０　復号条件の属性数に対する復号処理時間

なお、モデルシステムを用いた性能の限界テストについては、実施機関による当初の計画で想定していなかったこともあり、実施されていない。

（２）特許・論文等の状況

主要な対外発表内容を示す。本研究開発に基づく査読付き論文の掲載、特許出願等の実績はない。

表ｅ－２　特許・論文等件数

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
0	0	0	0	0	0	0

「情報処理学会 第 73 回全国大会」にて「鍵失効機能を持つ属性ベース暗号の実装評価」の論文発表、論文集に掲載
https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=76697&item_no=1&page_id=13&block_id=8

「コンピュータセキュリティシンポジウム 2011」にて「鍵失効機能を持つ属性ベース暗号の実装評価」の論文発表、論文集に掲載
https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=77929&item_no=1&page_id=13&block_id=8

「電子情報通信学会技術研究報告. ICM, 情報通信マネジメント」にて「属性ベース暗号を用いたオンラインストレージサービス用クライアントの実装評価」の論文発表、論文集に掲載
http://ci.nii.ac.jp/naid/110009480823

３－２－ｅ　目標の達成度

本研究開発に関する目標の達成度を次表に示す。「研究作業」、「評価システム構築」については、実用化の問題として、性能面がハードルとなることが洗い出され、それをクリアするために属性情報の判定条件を制限する解を導き出した。これにより、実施機関において目標を達成できたと判断されている。

「鍵管理機能の構築」「モデルシステムの構築」「実証実験」及び「普及活動及び意見収集」においては、実際に稼働するモデルシステムが構築でき、それを展示会で発表することにより大手機械メーカーからの問い合わせがあり、案件につながった点という成果から、同様に目標を達成できたと判断されている。

表ｅ－３　目標に対する成果・達成度の一覧表

要素技術	目標・指標	成果	達成度
鍵管理機能の構築	・設計、構築、動作検証	・これまでの成果をもとに、クラウド向け鍵暗号モジュールに必要な機能の構築を行った。	達成
モデルシステムの構築	・検討、設計、構築、動作検証	・クラウド向け鍵管理システムと携帯端末用クライアントについて、利用モデルをもとに必要な機能と仕様を定め、実装・動作検証を行った。	達成
モデルシステムの実証実験	・実証実験（1回目） ・中間レビュー ・実証実験（2回目）	・モデルシステムを用いて、ファイル容量、復号条件の属性数に基づく処理時間の変化について評価を実施し、属性数の増加が処理時間に影響を及ぼさないことを確認した。	達成
普及活動及び意見収集	・準備 ・各種発表	・学会等での発表とデモンストレーションを行った。 ・来場者にアンケート調査を実施した。	達成

各年度の詳細な成果は次の通りである。

① 平成２２年度

【研究作業】

- 属性ベース暗号の理論的背景を整理するとともに、本方式において重要となる受信者における復号の可否と、失効リストによるチェック機能について、求められる機能の内容を確認した。

【評価システム構築】

- 属性ベース暗号の運用モデルを設定した上で、以下の５種類の機能について、各機能を実装するモジュールの仕様の設計を行った。
  ① セットアップ機能
  ② 鍵生成機能
  ③ 暗号化機能
  ④ 復号機能
  ⑤ 鍵管理失効機能
- 前項で定義した各機能で想定される操作手順を定めるとともに、属性ベース暗号における役職グループ、部署グループのポリシ条件設定の条件について、機能設計を行った。
- 前項までの検討結果をもとに、評価システムの詳細設計を実施した。
- 評価環境をもとに、ユーザ数の増加に伴って負荷の増大が見込まれる「鍵生成時間」「暗号化処理時間」「復号処理時間」及び「失効者確認時間」の処理時間の計測を実施した。利用者 200 万人、失効者 50 万人、ユーザの属性が最大 20 種類、復号の条件が最大 20 条件のもとで評価を行った結果、それぞ

れ以下の結果を得た。

- 鍵生成時間：129.98 秒（属性数 20）
- 暗号化処理時間：3.14 秒（属性数 20）
- 復号処理時間：1.20 秒（属性数 20）
- 失効確認：0.29 秒（失効ユーザ数 50 万人）

● 情報処理学会主催:第 73 回全国大会のセッション、デモセッションに参加し、発表を行うとともに、本研究の有用性・実用性について客観的な意見収集を行うことを目的として、会場でアンケート調査を実施した。41 件の回答のうち、本研究は有効との回答が 37 件、実用性があるとの回答が 34 件と、概ね肯定的な評価を得た。

② 平成２３年度

【鍵管理機能の構築】

● 前年度の成果である属性ベース暗号の各モジュール（セットアップ機能モジュール、鍵生成モジュール、暗号化機能モジュール、復号化機能モジュール、鍵管理機能モジュール）を使用して、クラウド向け鍵暗号モジュールの仕様設計を行った。
● クラウド向け鍵管理システムとして、以下の３種類の機能仕様を定めた。
  - 鍵発行依頼システム
  - 鍵管理者システム
  - Web サービス
● ユーザが用いる携帯端末用クライアントについて、実用的なクラウドサービスの用途として DropBox を経由したデータのアップロード及びダウンロードを行うことを前提としたアプリケーションの仕様を設計した。

【モデルシステムの構築】

● クラウド向けデータ共有システムについて、以下の各サブシステムを対象に、実証実験で用いる具体的な利用場面とデータをもとに詳細設計を行った。
  - 鍵管理システムデータベース
  - 鍵発行依頼システム
  - 鍵管理者システム
  - Web サービス
● 携帯端末用クライアントについて、Android を利用するスマートフォンを対象に、設計された仕様に従って DropBox との通信を行うための詳細設計を行うとともに、開発済みの暗号化モジュールを Andoid に対応させるための変更に関する詳細設計を行った。完成したアプリケーションを「錠前屋」と命名。

【実証実験】

● 開発した Android 用クライアント（Android2.2 の端末とダウンロード 11Mbps／アップロード 5.4Mbps の回線を利用）を用いたシステムの性能評価を実施し、次の結果を得た。

- 暗号化処理時間：約 3 秒（ファイル容量 1MBytes、属性数 10）
  （実際の操作にはこれに約 12 秒間の通信時間が加わる）
- 復号処理時間：1～2 秒（ファイル容量 1MBytes、属性数 10）
  （実際の操作にはこれに約 10 秒間の通信時間が加わる）

【普及活動及び意見収集】

- 平成 23 年 10 月に新潟市で開催されたコンピュータセキュリティシンポジウム（CSS)2011 にて論文発表及びデモンストレーション展示を行った。デモンストレーション会場にて、来場者に約 60 枚のパンフレットを配布するとともに、研究開発成果についてのアンケート調査を依頼し、27 件の回答を得た。来場者はセキュリティを専門に研究している研究者および学生が多く、属性ベース暗号の認知度も高かったため、専門的な観点での意見交換を行った。
- 平成 23 年 10 月に開催されたクラウドコンピューティング EXPO に出展し、展示ブースにおいて、ポスターの展示、パンフレットの配布、プロジェクター投影にてデモビデオの再生、PC モニタおよび Android 端末でのデモンストレーション展示を行い、来場者に対して積極的な説明を行った。来場者にパンフレットを 500 枚配布するとともに、170 件のアンケートを回収した。

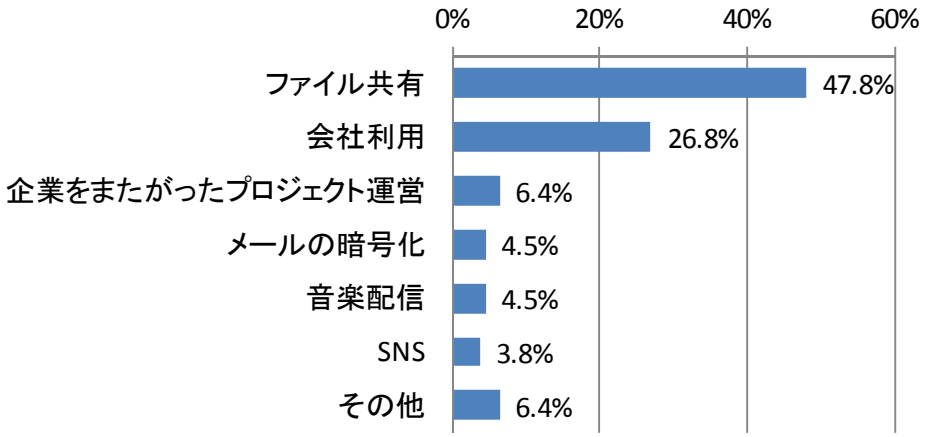
図ｅ－１１　本研究成果に関するデモンストレーションの状況
（左：CSS2011、右：クラウドコンピューティング EXPO）

- 平成 23 年 11 月に金沢工業大学にて開催された KITpro 勉強会にて、本研究開発成果に関する展示ブースを設置し、ポスターの展示、パンフレットの配布、PC モニタおよび Android 端末でのデモンストレーション展示を行った。

次ページに、CSS2011 およびクラウドコンピューティング EXPO にて実施したアンケートにおける本成果への関心や評価に関する設問の集計結果を示す。

表ｅ－４　アンケート集計結果

設問	回答
アプリケーションの性能（n=83)	よい＝25.3% ふつう＝73.5% わるい＝1.2%
アプリケーションの操作性（n=81)	よい＝21.0% ふつう＝79.0% わるい＝0.0%
サービスの利用意向（n=197）	利用したい＝66.5% 利用したいと思わない＝2.0% その他＝31.5%



図ｅ－１２　このサービスが有効と思う場面（複数選択、N=157）

４－ｅ　事業化、波及効果について

４－１－ｅ　事業化の見通し

本研究の成果は大手機械メーカー及び大手通信事業者に採用され、属性ベース暗号を用いた実際のサービスへの実装に向けて活動中である。

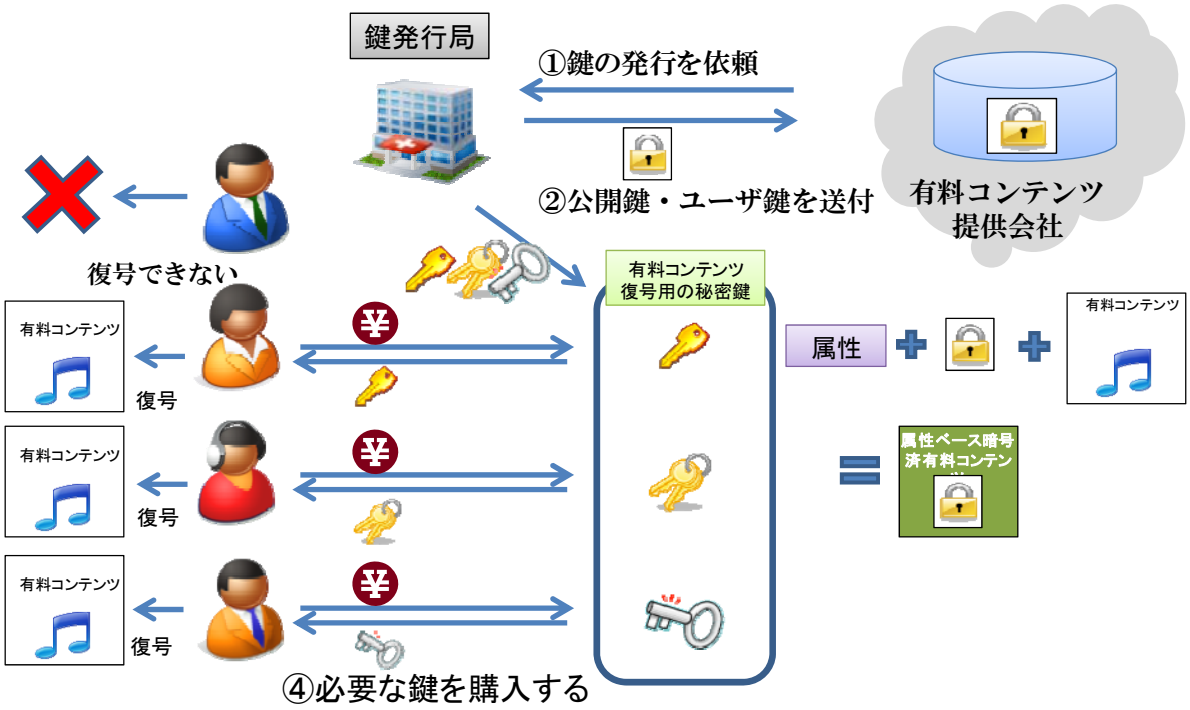
各社への鍵発行システムの組み込み案件として、下記の金額による開発・保守業務の委託を受けて実施している。

- 2012 年度（2012 年 4 月～2013 年 3 月）約 770 万円
- 2013 年度（2013 年 4 月～2014 年 3 月）約 1,500 万円

並行して、現在サービス実装を行っている案件を拡張し、企業内の属性ベース暗号基盤を構築・販売するモデルを確立し、営業展開を行うことが計画されている。

さらに、複数の企業を一括して１つの属性ベース暗号基盤で賄える仕組みを開発し、

中小企業にも普及できる廉価モデルの構築が検討されている。



図ｅ－１３　有料コンテンツ提供会社への鍵発行サービス例（事業化イメージ）

４－２－ｅ　波及効果

本研究開発成果に基づくシステムは前述の通り現在実装中であり、まだ実稼働はしていないことから、直接の波及効果は発生していない。

しかしながら、本成果を基に実施機関が「次世代セキュア情報基盤ワークショップ」にて広島大学の大東助教授に紹介されるなど、セキュリティ基盤業界への「属性ベース暗号」の認知が進んでいる。

５－ｅ　研究開発マネジメント・体制・資金・費用対効果等

５－１－ｅ　研究開発計画

本事業は、平成 22 年度から 23 年度までの 2 年計画である。各要素技術の研究開発計画は次のとおりである。

開発期間中、Android 対応にてコンパイル不能な問題が発生し、技術的な支援を実施機関の技術者が行うことで解決した。

また、当初段階で発生しうる問題点を洗い出し、解決することでモデルシステム構築時には、Android のコンパイル問題以外のほとんど大きな問題を出すことなく終えることができた。

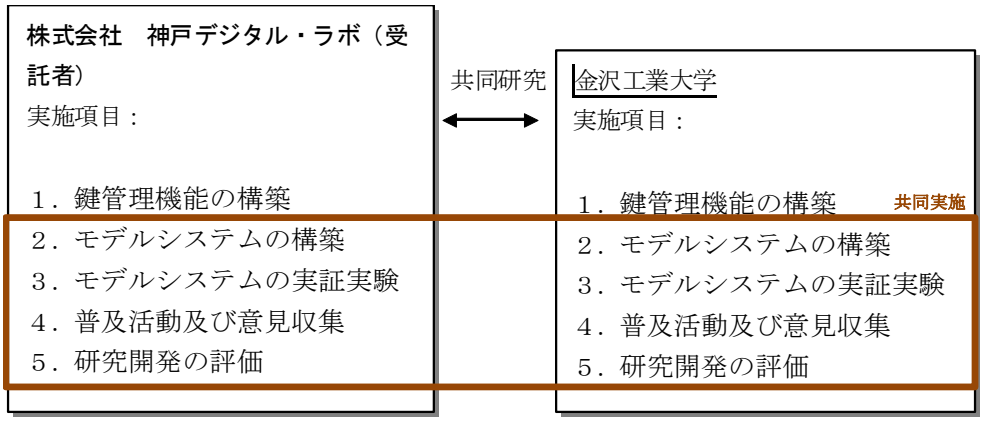
表ｅ－５　研究開発計画

年度	平成22年度	平成23年度
予算額	15.6百万円	19.6百万円
研究作業	→	
評価システム構築	→	
鍵管理機能の構築		→
モデルシステムの構築		→
実証実験		→
普及活動及び意見収集		→

５－２－ｅ　研究開発実施者の実施体制・運営

本事業は、平成 22 年度から平成 23 年度において、経済産業省から株式会社神戸デジタル・ラボへの委託により実施されている。

また各年度につき、再委託先として金沢工業大学が事業に参加した。



図ｅ－１４　研究開発実施体制

５－３－ｅ　資金配分

実施期間中の資金配分は次表の通りである。

表ｅ－６資金配分　　(単位百万円)

要素技術	平成22年度	平成23年度
効率的な鍵管理機能を持つクラウド向け暗号化データ共有システム	15.6	19.6

５－４－ｅ　費用対効果

本研究開発成果に基づくシステムは、前述の通り現在実装中である。

実施機関においてはこれまで本課題を通じて２３百万円の受注を実現しているが、この実装作業が成功した際には、属性ベース暗号を用いた初の実用的なアプリケーションとして、本成果の事業化による売上とみなせることになる。

なお、株式会社 KDDI 研究所では、属性ベース暗号と同様の原理からなる「ポリバレント暗号」による類似のサービス展開を計画しており、実施機関が本成果に基づく事業を拡大するためには、こうした今後予想される競合への対策を講じていく必要がある。

５－５－ｅ　変化への対応

当初のモデルシステムは PC 上で開発する予定であったが、スマートフォンやタブレットの普及に伴い、Android 上で稼働するモデルシステムに変更し、市場により有利にアプローチできるものとした。

Ａ－ｆ　クラウドサービスプロバイダとクラウドユーザ企業（法人）における事業継続計画（BCP）の在り方と連携の確保、及びその妥当性検証技術に関する研究

１－ｆ　事業の目的

最近のクラウドサービス市場規模の拡大に合わせて BCP の実効性を維持することは、クラウドベンダの信頼性を確保する上で重要であり、その信頼性を高めることはクラウドユーザ企業の事業展開上有効な委託関係を構築することになる。本研究では、クラウドサービスベンダ、クラウドユーザ双方の BCP のあり方、連携、妥当性の検証方法に焦点を当て、この知見を反映したクラウドベンダのための BCP 構築基準を策定することを通じて、クラウドサービス・ユーザの事業継続性の向上に資する。

２－ｆ　研究開発目標

上述の目的の達成のため、以下の目標を設定した。

表ｆ－１　個別要素技術の目標

要素技術	目標・指標	妥当性・設定理由・根拠等
クラウドユーザ企業における現実的なBCP（事業継続計画）の作成	「クラウドベンダのためのBCP構築基準」の作成	災害やサイバー攻撃に対するクラウドサービスの事業継続性を高めるために、クラウドベンダが自ら活用し、BCPを構築する過程でガイダンスとして用いる

３－ｆ　成果、目標の達成度

３－１－ｆ　成果

平成２３年３月に開催された事業継続の妥当性を審査する有識者委員会（新世代情報セキュリティ研究開発事業推進委員会）において、本テーマについては継続実施が不適切との判断がなされた結果、実施予定期間２年間のところ、初年度のみの実施にて中止となった。

よって、以下に初年度の成果を示す。

（１）成果

調査結果をもとに、「クラウドベンダのための BCP 構築基準」が作成された。

（２）特許・論文等の状況

本研究開発に基づく査読付き論文の掲載、特許出願等の実績はない。

表ｆ－２　特許・論文等件数

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
0	0	0	0	0	0	0

３－２－ｆ　目標の達成度

本研究開発による目標の達成度は下表の通りである。

表ｆ－３　目標に対する成果・達成度の一覧表

要素技術	目標･指標	成果	達成度
クラウドユーザ企業における現実的なBCP（事業継続計画）の作成	「クラウドベンダのためのBCP構築基準」の作成	調査結果をまとめて同基準を作成し、報告書として納入した。	－

４－ｆ　事業化、波及効果について

４－１－ｆ　事業化の見通し

平成２３年度以降の継続がなされなかったため、事業化の取り組みは行われていない。

４－２－ｆ　波及効果

本研究開発の成果は事業化しておらず、波及効果は発生していないが、こうした研究が実施されることで、クラウドサービスの提供と利用におけるＢＣＰ策定に関する意識の醸成を促す効果が期待される。

５－ｆ　研究開発マネジメント・体制・資金・費用対効果等

５－１－ｆ　研究開発計画

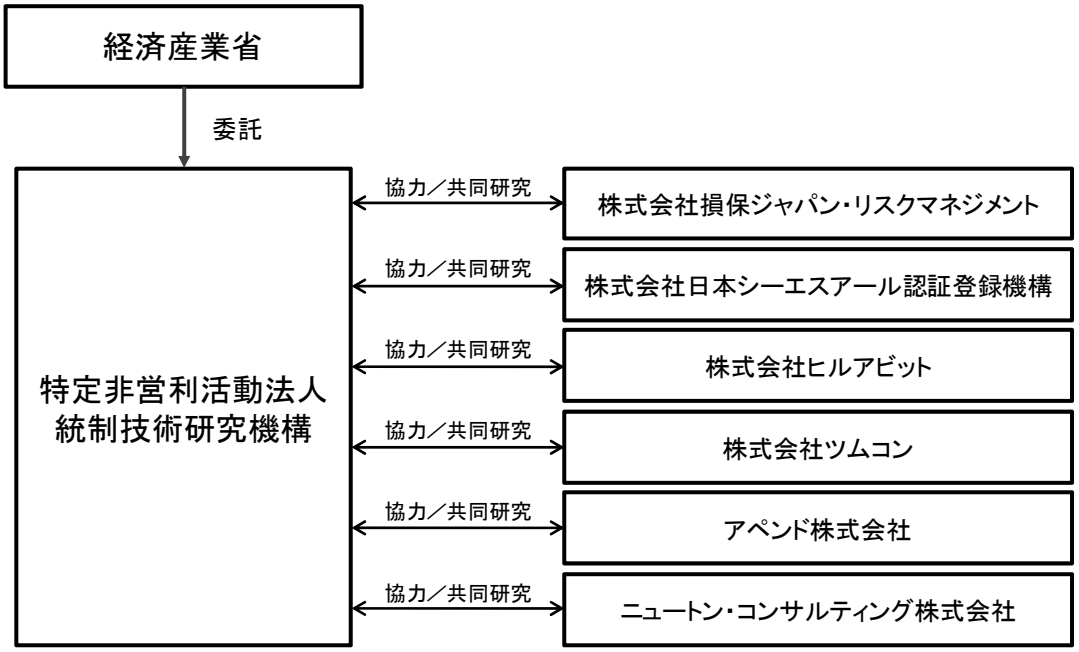
本事業の研究開発計画は次のとおりである。

表ｆ－４　研究開発計画

年度	平成22年度
予算額	12.5百万円
クラウドサービスベンダの実態調査	→
クラウドサービスベンダ側で起こり得る事故について、事件発生から収束までのシナリオを作成	→
事業継続に関わるリスク対応と、BCPに取り入れる管理策のベンチマークを決定	→
「BCP構築基準 サービスベンダ編」の開発	→

５－２－ｆ　研究開発実施者の実施体制・運営

本事業は、平成 22 年度に、経済産業省から特定非営利活動法人統制技術研究機構の委託により実施されている。



図ｆ－１　研究開発実施体制

５－３－ｆ　資金配分

表ｆ－５資金配分　　(単位百万円)

要素技術	平成22年度
クラウドサービスプロバイダとクラウドユーザ企業（法人）における事業継続計画（BCP）の在り方と連携の確保、及びその妥当性検証技術に関する研究	12.5

５－４－ｆ　費用対効果

本テーマを通じて、成果に基づく効果は生じていない。

５－５－ｆ　変化への対応

１年間の実施であり、変化への対応の必要は生じていない。

（参考）１年間で打ち切りとなった理由

平成２３年３月に開催された事業継続の妥当性を審査する有識者委員会（新世代情報セキュリティ研究開発事業推進委員会）において、本テーマについては継続実施が不適切との判断がなされた結果、実施予定期間２年間のところ、初年度のみの実施にて中止となった。

表ｆ－６　有識者委員会における主な意見

評価項目	委員からの意見
要素技術から見た成果の意義	・意義はあると思うが、方法論が正しいのか。
実用化の見通し	・実現性に疑念がある。 ・具体的な成果が予測できない。 ・今のままの進め方で行くと、具体的に活用できるものができるか疑問である。 ・基準を作成するだけでは普及するとは思えない。 ・現在のクラウドプロバイダの実状に合致しない。プロバイダは進化している。そのような変化を反映する取り組みが欲しい。
次年度の計画	・継続する意味はないのではないか。あるいは、同じ方法ではなく、目標は同じでも異なる事業者で行うほうがよいのではないか。
総合評価	・普及計画が曖昧であることから、継続は難しいのではないか。 ・次年度に継続する必要はない。

Ａ－ｇ　ＰａａＳ／仮想化環境におけるコンプアライアンス指向データアクセス手法の研究開発

１－ｇ　事業の目的

クラウド基盤サービスにおいては、一般にクラウド基盤提供者が特権アカウントを持ち、その不正利用が懸念されるため、個人情報保護法や SOX 法などの法令遵守の観点から利用を躊躇する例が多い。そこで、クラウド基盤利用者自身によるデータの管理・監督を可能にする機構に関する研究開発を通して、利用者の視点でのクラウド基盤サービスのコンプライアンス向上を図る。さらに、利用者から見たクラウド基盤サービスをよりコンプライアンス施策が利用しやすいものにすることにより、我が国のクラウド基盤サービス事業の発展に寄与する。

２－ｇ　研究開発目標

本研究開発で提案する以下の２つの機構を通じたコンプライアンス指向データアクセス手法を確立し、プロトタイプ開発とその評価により、提案手法が実現可能であることを確認する。

表ｇ－１　個別要素技術の目標

要素技術	目標・指標	妥当性・設定理由・根拠等
ケーパビリティインジェクション機構	・手順の検討 ・プロトタイプの設計 ・試験項目の設定 ・プロトタイプの評価 ・実環境向け実装仕様の検討 ・実環境向け実装による評価	ケーパビリティインジェクション機構により、利用者がクラウドに預けたデータにアクセスするために必要となる権限に関する情報を安全にクラウド内のゲスト環境のOSに通知することで、利用者自身による機密データの管理監督を行うことが可能となる。
ペアリング機構	・手順の検討 ・プロトタイプの設計 ・試験項目の設定 ・プロトタイプの評価 ・実環境向け実装仕様の検討 ・実環境向け実装による評価	ペアリング機能により、ハードウェア、仮想化機構、ゲスト環境に関して、規定されたペア以外での動作を防止することで、本来その機器及びシステムへの正しいアクセス権を持たない利用者による使用・管理を防止するコンプライアンス指向のデータアクセス手法の実現が可能となる。

３－ｇ　成果、目標の達成度

３－１－ｇ　成果

平成２３年３月に開催された事業継続の妥当性を審査する有識者委員会（新世代情報セキュリティ研究開発事業推進委員会）において、本テーマについては継続実施が不適切との判断がなされた結果、実施予定期間２年間のところ、初年度のみの実施にて中止となった。

よって、以下に初年度の成果を示す。

（１）成果

プロトタイプの構築を通じた実験により、クラウド利用者が、自ら預けたデータの管理・統制を行うことが可能であることが確認され、実施機関において提案されたペアリング機構及びケーパビリティインジェクション機構の有効性を明らかにした。

（２）特許・論文等の状況

本研究開発に基づく査読付き論文の掲載、特許出願等の実績はない。

表ｇ－２　特許・論文等件数

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
0	0	0	0	0	0	0

３－２－ｇ　目標の達成度

平成２１年度は、ペアリング機構、ケーパビリティインジェクション機構の両試験において、本プロトタイプ実装によって本件提案手法の二機構が実現可能であることが確認された。

表ｇ－３　目標に対する成果・達成度の一覧表

要素技術	目標･指標	成果	達成度
ケーパビリティインジェクション機構	･手順の検討 ･プロトタイプの設計 ･試験項目の設定 ･プロトタイプの評価 ･実環境向け実装仕様の検討 ･実環境向け実装による評価	・保護対象情報へのアクセスケーパビリティ(暗号鍵等)を、ゲスト環境内部（ファイルシステム上のファイル等）に永続的に保存させず、必要な時に動的かつ安全に、外部から注入する手法を確立した。 ・評価に必要な最低限の機能を模倣するプロトタイプの設計と実装を行った。 ・機能試験とケーパビリティインジェクション機構の項目を定めた。 ・プロトタイプが所定の動作を行うことを確認したが、実環境での実装の検討には至らなかった。	－
ペアリング機構	･手順の検討 ･プロトタイプの設計 ･試験項目の設定 ･プロトタイプの評価 ･実環境向け実装仕様の検討 ･実環境向け実装による評価	・ホスト環境とホスト仮想化機構とのペアリング、ホスト仮想化機構とゲスト環境とのペアリングの検査方法を確立した。 ・評価に必要な最低限の機能を模倣するプロトタイプの設計と実装を行った。 ・機能試験とペアリング機構試験の項目を定めた。 ・プロトタイプが所定の動作を行うことを確認したが、実環境での実装の検討には至らなかった。	－

４－ｇ　事業化、波及効果について

４－１－ｇ　事業化の見通し

平成 23 年度以降の継続がなされなかったため、事業化の取り組みは行われていない。

４－２－ｇ　波及効果

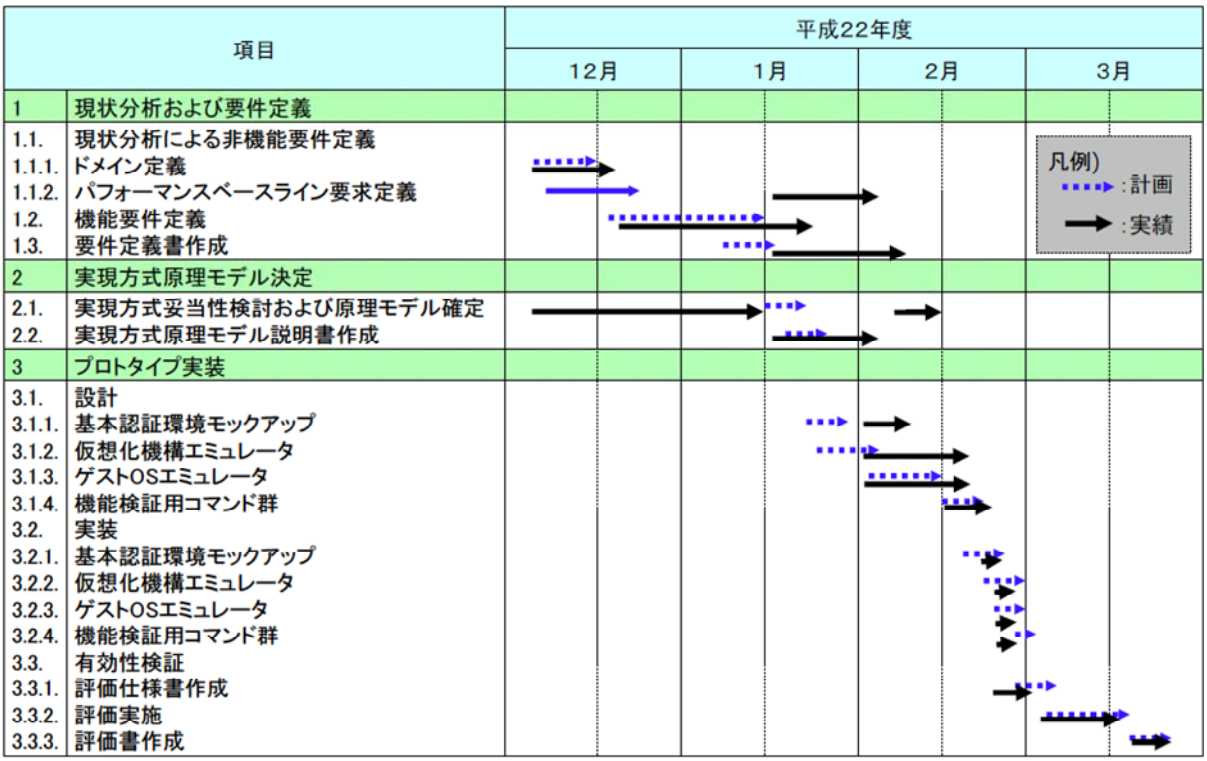
本研究開発の成果は事業化しておらず、波及効果は発生していないが、こうした研究が実施され、クラウドサービス利用時のコンプライアンス対応オプションが増えることにより、利用者が自ら情報をコントロールできない状況が削減される効果が期待できる。

５－ｇ　研究開発マネジメント・体制・資金・費用対効果等

５－１－ｇ　研究開発計画

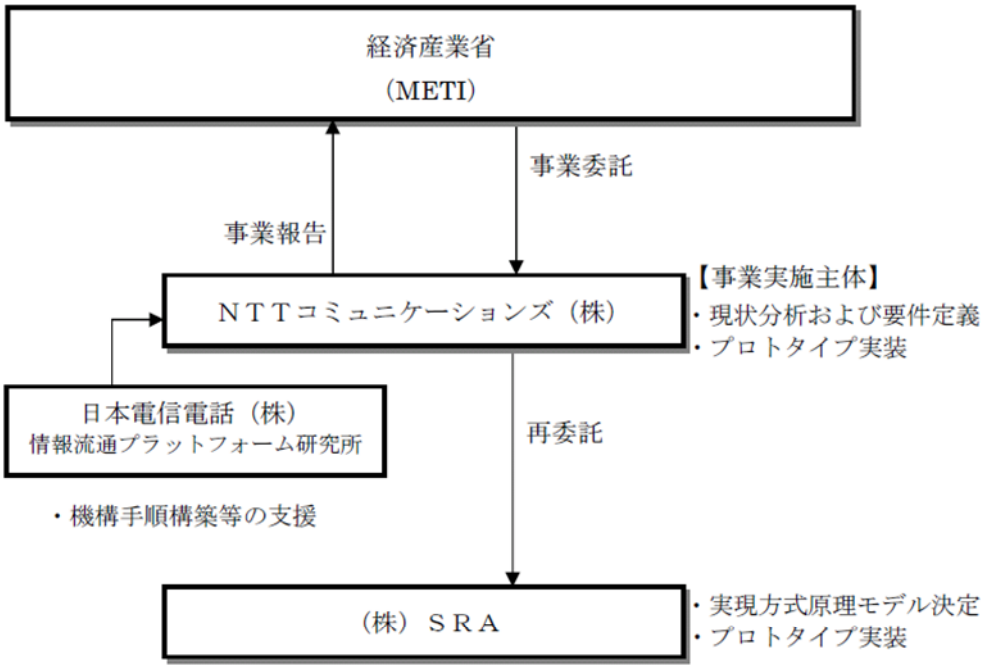
本事業は、平成 22 年度から 24 年度までの 3 年計画である。各要素技術の研究開発計画は次のとおりである。

表ｇ－４　研究開発計画



５－２－ｇ　研究開発実施者の実施体制・運営

本事業は、平成 22 年度において、経済産業省から NTT コミュニケーションズ株式会社への委託により実施されている。また再委託先として以下の機関が事業に参加した。



図ｇ－１　研究開発実施体制

５－３－ｇ　資金配分

表ｇ－５資金配分　　(単位百万円)

要素技術	平成22年度
PaaS／仮想化環境におけるコンプアライアンス指向データアクセス手法の研究開発	**29.4**

５－４－ｇ　費用対効果

本テーマを通じて、成果に基づく効果は生じていない。

５－５－ｇ　変化への対応

１年間の実施であり、変化への対応の必要は生じていない。

（参考）１年間で打ち切りとなった理由

平成２３年３月に開催された事業継続の妥当性を審査する有識者委員会（新世代情報セキュリティ研究開発事業推進委員会）において、本テーマについては継続実施が不適切との判断がなされた結果、実施予定期間２年間のところ、初年度のみの実施にて中止となった。

表ｆ－６　有識者委員会における主な意見

評価項目	委員からの意見
要素技術から見た成果の意義	・ 技術的難しさをどのように解決しているのかがわからない。 ・ 本方式でコンプライアンス指向が何故達成できるのか疑問である。
実用化の見通し	・ 効果的な開発が可能か疑問である。 ・ ゲスト OS における安全な領域の実現性に疑問がある。
総合評価	・ 社会的にどのように展開していくのかが不明である。 ・ 仮想コンピュータの技術は進歩が早いので、この手法がこれから数年後でも役立つのかがよくわからない。 ・ 重要な技術開発だと思うが、その方法について、投資価値があるかどうか疑問が残る。

Ｂ　高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業）

１－Ｂ　事業の目的

システム LSI が使用されている IC カードは、金融や交通等、生活の様々な場において用いられており、既に企業や個人の財産・商取引を支える重要な基盤となっている。しかしながら、当時の国内では、IC カードのセキュリティについての評価体制が構築できていなかった。IC カード等のＩＴ製品のセキュリティに関する評価は、国際的に国際標準（ISO/IEC 15408）などに基づく評価・認証が行われていることから、海外の関係機関と連携しつつ、日本国内で IC カードのセキュリティ評価を行うことができるよう、必要な体制整備を進めることが重要であった。

そこで本事業では、国内外の関係機関と連携しつつ、国内で IC カードのセキュリティ評価を行うために必要な技術開発や環境整備等を行う。具体的には、我が国における IC カードのセキュリティ評価認証体制のすみやかな構築、海外先進事例と等価な評価技術の確立、我が国における評価技術の深化と独自ノウハウの蓄積を図る。

２－Ｂ　研究開発目標

前述の目的を達成するため、本事業において以下の項目を実施する。

表Ｂ－１　個別要素技術の目標

要素技術	目標・指標	妥当性・設定理由・根拠等
セキュリティ評価を行うために必要な技術の開発	・新規・既知の攻撃方法に関する評価手法の開発 ・評価ツールの開発	・新しい攻撃（例：システムLSIのメモリ部に対する攻撃）や故障利用解析、ツールの統合による高度なデータ解析への対応が必要。 ・効率的にセキュリティ評価を行うため、新たな解析手法をサポートする標準的な評価ツールの開発が必要。
システムLSIセキュリティ評価に関する共同利用設備の整備	・共同利用設備の整備 ・委託事業終了後の共同利用設備の運営に関する検討	・システムLSIのセキュリティ評価を行う際に必要な装置等について、CC補助文書に規定される装置一覧を満たすように整備する必要がある。 ・共同利用設備については、事業終了後も有効活用できるように配慮する必要がある。
セキュリティ評価を行うために必要な人材育成	・人材育成 ・育成した人材による試行評価	・共同利用設備の装置等を用いて、チップの脆弱性分析を行う要員を育成するほか、こうした要員による脆弱性分析を監督する評価者を育成する。 ・育成した人材による評価が適切であることを確認するため、日欧共同評価による二国認証を行う。
セキュリティ評価体制の構築に必要な調査	・海外技術動向調査 ・ICカードを利用するユーザー側のセキュリティ要求仕様等に関する調査 ・チップセキュリティ評価のための手順の調査	・欧州の専門家会合等に参加し、最新技術動向を調査した上で、国内向けハードウェア評価手順書を策定する。 ・評価対象となるICカードの用途別のセキュリティ要求仕様を調査し、今後開発するセキュリティ評価技術等に反映する。 ・ICチップのセキュリティ評価に関して、CC補助文書に準拠したマニュアルを作成する。

個別の要素技術毎の目標は次の通りである。

【セキュリティ評価を行うために必要な技術の開発】

① 新規・既知の攻撃方法に関する評価手法の開発

１）海外の技術動向に対応する技術開発

- 欧州 JHAS（JIL Hardware Attack Sub working group）との技術交流を通じて、今後製造者がセキュリティ対策を実装する必要が出てくることが見込まれる新しい攻撃（例：システム LSI のメモリ部に対する攻撃など）について、評価技術の研究開発を行う。具体的には、後述の「海外技術動向調査」等により、抽出された技術課題について、研究開発を行い、年 1 回以上欧州に技術レポートを提示する。これは日欧の HW セキュリティに関するリエゾン関係を構築するに当たり、欧州側から単に情報収集するだけではなく、日本側からも何らかの技術貢献をする必要があったことによる。（平成 22 年度、23 年度）

２）ツール統合技術の開発

- システム LSI が発する電力、電磁波の微細な変異を観測しそれを解析して暗号鍵の推定等を行う電力解析（DPA, SPA）、電磁波解析（DEMA, SEMA）、暗号処理中のモジュールの電源・クロックに対するノイズ混入やレーザ照射等でモジュールに誤作動を起こさせ、通常の処理では得られない内部情報を出力させて暗号鍵の推定等を行う故障利用解析（DFA）等に用いる複数のハードウェアから得られたデータの様式を統一し、複数の解析ソフトを統合的に運用しデータを解析するツール統合技術の研究開発を行う。統合したツールを運用して、より高度なデータ解析技術を開発する。平成 22 年度末までに、ツール統合モデルを構築することとする。
- 統合モデルを用いた、より高度なデータ解析技術の実証を行う。（平成 23 年度末まで）

３）故障利用解析（DFA）技術等の研究開発

- 故障利用解析（DFA）について、チップ裏面へのレーザ照射等の最新の解析手法の研究開発を行う。また、本委託事業で整備する解析ソフトに、本成果を適用し最新解析手法を利用可能にする。具体的には、チップ裏面へのレーザ照射等最新解析手法の研究開発を行う。上記研究開発を円滑に進めるため、独立行政法人産業技術総合研究所等と連携し実施する。（平成 22 年度末まで）
- 本事業で整備する解析ソフトの高度化を行う。（平成 23 年度末まで）

② 評価ツールの開発

- 既知の攻撃について、効率的にセキュリティ評価を行うにあたり、脆弱性試験のベンチマークとなる評価対象（テストビークル）としての評価ツールの

開発を行う。具体的には、電磁波解析など新たな解析手法を順次サポートできる機能を実装し、かつ、評価結果の再現・追試を可能とする高い拡張性と汎用性のあるデータ構造の標準的な評価ツールを開発する。こうした目標設定は、現在欧州等海外で行われているハードウェア脆弱性試験の対象は、殆ど RSA,DES,AES 等のアルゴリズムであり、我が国がハードウェア評価認証体制を構築する上で、日本固有のアルゴリズムを対象とするテストビークルが必要であったことによる。本項は、CC 認証機関を運営する独立行政法人情報処理推進機構との協力の下に開発を推進することとする。

【システム LSI セキュリティ評価に関する共同利用設備の整備】

① 共同利用設備の整備

- システム LSI のセキュリティ評価を行う際に必要な装置等については、CC 補助文書（Application of Attack Potential to Smartcards March 2009 Version 2.7 Revision 1 の 3.7 項）に規定される装置一覧を満たすように整備する。具体的には、補助文書 3.7 項の Standard 及び Specialized に規定される装置については、特殊な設備（恒温槽）を除き購入又はリースにより整備する。補助文書 3. 7 項の Bespoke に規定される装置及び恒温槽については、本事業による購入又はリースの他に、独立行政法人産業技術総合研究所及び当組合の組合員企業が所持するものを借用する方法についても検討を行う。
- また、脆弱性分析の過程で取得したデータを解析し、演算過程と暗号鍵等の情報資産を推定するための解析ソフトについても、開発、購入またはライセンス等により併せて整備する。なお、解析ソフトについては、試験者要員が主導して、多様な解析、今後の攻撃技術の発展等に対応しうるように、必要な場合にカスタマイズし、実用試験を行う。
- 上記装置及び解析ソフトは、都内に整備する施設において使用するほか、独立行政法人産業技術総合研究所と協議が整った場合には、一部を同研究所つくばセンター施設内に置くことも検討する。

② 委託事業終了後の共同利用設備の運営に関する検討

- ①で整備する共同利用設備について、委託事業終了後に有効活用できるよう必要な検討を行う。具体的には、CC 評価機関、ベンダ等に対して脆弱性分析サービスを提供する試験機関（以下、「チップテストラボ」という）を設立し、この試験機関が、共同利用設備を保有し、活用する方法を中心に検討を進める。当該試験機関の組織形態、設立時期、運営方法について、早急に検討し、委託事業終了後の円滑な事業運営をはかる。

【セキュリティ評価を行うために必要な人材の育成】

① 人材育成

1）試験者の育成

- 本事業により整備した共同利用設備の装置等を用いて、チップの脆弱性分析を行う要員（以下、「試験者」という）を育成する。具体的には、チップテストラボの要員となることを前提として、組合研究員を本事業における評価技術の研究開発、共同利用設備の習熟に関する演習及び以下の各種研修・演習等に従事させることなどにより育成し、新たなハードウェア評価認証体制の基幹要員とする。

  a）ハードウェア評価研修：海外評価機関の支援を得て、最新のハードウェア CC 評価方法、JIL 文書等に関する研修を実施し、早期に習得を図る。

  b)評価用ボードによる演習：経済産業省委託事業により開発された評価用ボード SASEBO（G-Ⅱを想定）を用い、試験者要員により脆弱性分析演習を行う。SASEBO ボードは JHAS に対する日本の技術貢献の一環としても活用することも検討する。

  c）脆弱性分析演習：海外機関の支援を得て、共同利用設備等を用い、平成 21-22 年度を通じ故障利用解析と電磁波解析、可能であれば物理解析の演習を実施する。

  d）セキュリティ対策実装チップへの攻撃演習：脆弱性分析技術習得のため、様々なセキュリティ対策を実装したチップに対して繰り返し攻撃演習を行う。

2）評価者等の育成

- CC 評価機関に所属する要員で、チップテストラボの試験者に委託する脆弱性分析を監督し、テストプランの作成、脆弱性の評定と CC 評価報告書作成を行う者（以下、「評価者」という）を育成する。具体的には、CC 評価機関の評価者について、海外評価機関による上記 a)ハードウェア評価研修に従事させ、ハードウェア CC 評価の方法について習得をはかる。
- また、ハードウェア CC 評価に関する研修や脆弱性分析に関する各種研修・演習の一部には、試験者に加え、時宜により評価者、認証者、開発者各要員にも参加を求め、各要員の CC 評価・認証に関する共通理解の促進と所要のスキルの習得を図る。

② 育成した人材による試行評価

1）試行評価の実施

- 国内市場用途のアプリケーション搭載を想定したチップ製品の試行評価を行う。当組合の組合員企業等より評価対象（Target Of Evaluation; TOE）を募集し、育成した試験者要員が共同利用設備を活用して脆弱性分析を行い、国内 CC 評価機関に脆弱性分析レポートを提供する。評価機関はこの脆弱性分析レポートを用いて当該対象の試行 CC 評価を行う。この評価は、独立行政法人情報処理推進機構が運営するわが国 CC 評価・認証制度下での正規の評価として行い、ベンダはわが国 CC 認証を申請するものとする。評価対象を製造

するベンダは、同時に当該製品の欧州での CC 認証取得を試み、その結果について国内での認証取得と比較した報告書を提出する。日欧評価技術の等価性を検証し、育成した人材による評価が適切であることを確認するために、欧州で既に評価認証済みの TOE を我が国 JISEC 体制下で試行評価を行い、日欧の評価及び評価報告書の比較を、開発者が行うこととした。

２）評価技術の確認（日欧共同評価による二国認証）

- 日欧評価の等価性を検証し、育成した人材による評価が適切であることを確認するため、日欧共同評価による二国認証を行う。具体的には、欧州（英、仏、独、蘭、西いずれか一国）認証機関と評価機関の協力を得て、同一の製品を対象に、日本国内で本事業により整備した共同利用設備と育成した試験者要員を用いて、日欧の評価機関が、共同で CC 評価を行い、評価報告書（Evaluation Technical Report; ETR）を作成して、ベンダは両国で各々CC 認証を申請するものとする。

【セキュリティ評価体制の構築に必要な調査】

① 海外技術動向調査

- システム LSI のセキュリティ評価を行う上で必要な海外調査を行う。具体的には、欧州 JHAS 定期会合等に調査員を派遣し、欧州等の最新技術動向を調査するとともに、その結果も活用して日本の CC ハードウェア評価手順書をとりまとめる。必要であれば、JHAS 参加機関等の個別訪問や招聘により調査を補完する。また調査結果を本事業で構築する IC チップのセキュリティ評価体制の構築に活用する。本目標の設定は、とくに欧州 JHAS を中心とする HW セキュリティ評価方法・手順を我が国が共有することが、新たに発足する我が国 HW 評価認証体制にとって不可欠であったことによる。

②IC カードを利用するユーザー側のセキュリティ要求仕様等に関する調査

- IC カードを利用するユーザー側のセキュリティに関する要求事項等について調査を行う。また、セキュリティ評価技術等の開発を行うにあたり、当該調査結果を反映したものとする。具体的には、評価機関と連携して、①個人認証システム分野、②決済端末システム分野、③マルチアプリケーションシステム分野の３分野の IC カードについて、それぞれユーザー側のセキュリティ要求仕様を調査し、ユーザーと連携しつつ、セキュリティ保証のために必要な要件をまとめる。この調査結果をユーザー側に提供し、ユーザーの製品・システムの調達仕様作成に活用することを促す。また、必要に応じ、既製の認証済みセキュリティ要求仕様書等にアプリケーションノートを加える作業を行うことにより前記ユーザー側要求仕様へ対応する方法についても検討を行う。

③ チップセキュリティ評価のための手順の調査

- IC チップのセキュリティ評価方法について、評価のための手順を調査し、CC 補助文書及びその下位文書にのっとった評価手順マニュアルを作成する。当該評価手順は、欧州との整合をはかりつつ、本事業を通じた知見をとりいれてまとめる。作成したマニュアルを評価機関及び認証機関と共有し、脆弱性分析に関する理解を促進する。

３－Ｂ　成果、目標の達成度

３－１－Ｂ　成果

（１）成果

本研究開発の狙いは、我が国国内にＩＣカード等のハードウェアのセキュリティ評価を実施可能とする環境を整備することであり、この目的は達成されている。さらに、試験や評価を行う人材の育成や、評価手法の開発を同時に行うことで、我が国国内で質の高い評価を行うことが可能となった。

（２）特許・論文等の状況

本研究開発に基づく査読付き論文の掲載、特許出願等の実績はない。

表Ｂ－２　特許・論文等件数

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
0	0	0	0	0	0	0

３－２－Ｂ　目標の達成度

設定した目標について、以下の通り達成した。

表Ｂ－３　目標に対する成果・達成度の一覧表

要素技術	目標・指標	成果	達成度
セキュリティ評価を行うために必要な技術の開発	・新規・既知の攻撃方法に関する評価手法の開発 ・評価ツールの開発	・約600件の攻撃事例データベースを編集・作成・更新し、欧州JHASと共有。 ・産業技術総合研究所との共同研究の成果を活かし、電力解析、故障利用解析技術等の研究開発を実施。 ・オランダRescure社に対し、我が国固有の暗号アルゴリズムに対応する10件のモジュールの開発を委託。	達成
システムLSIセキュリティ評価に関する共同利用設備の整備	・共同利用設備の整備 ・委託事業終了後の共同利用設備の運営に関する検討	・都内オフィスビル内に試験室、評価室、研究室を設置し、試験施設としてASNITE-IT及びISO/IEC 17025の認定を取得した。 ・事業終了後の継承者として、株式会社電子商取引安全技術研究所を選定した。	達成
セキュリティ評価を行うために必要な人材育成	・人材育成 ・育成した人材による試行評価	・3名の要員を対象に、海外機関への再委託により脆弱性分析演習、セキュリティ対策実装チップへの攻撃演習等を実施した。 ・評価者育成に向け、ICチップ脆弱性分析技術指導を実施し、10名の参加を得た。 ・1社を対象に日欧共同評価による二国認証を前提とした試行評価を実施した。	達成
セキュリティ評価体制の構築に必要な調査	・海外技術動向調査 ・ICカードを利用するユーザー側のセキュリティ要求仕様等に関する調査 ・チップセキュリティ評価のための手順の調査	・海外の企業訪問、専門家会合参加等を通じてセキュリティ評価に関する情報収集及び情報交換を実施。 ・個人認証システム、決裁端末システム、マルチアプリケーションシステムについてセキュリティ要求仕様の調査を実施。 ・チップセキュリティ評価のための手順について、再委託による調査を実施し、報告書をとりまとめた。	達成

個別の要素技術毎の成果は次の通りである。

【セキュリティ評価を行うために必要な技術の開発】

① 新規・既知の攻撃方法に関する評価手法の開発

1）海外の技術動向に対応する技術開発

- 約 600 件の攻撃事例データベースを編集・作成・更新し、欧州 JHAS と共有した。なお成果は欧州側のカウンターパート JHAS との共有を目的とするものであって、公開用途ではない。

2）ツール統合技術の開発

- 産業技術総合研究所との共同研究成果を活用し、電力解析、故障利用解析技術等の研究開発を実施した。
- 本事業で取得した各種ツールの内、各分野の攻撃に用いるものを 1 つ以上ピックアップして統合運用を実証し、より高度なデータ解析を行った。
- 本事業で開発した運用技術は、設立された試験機関要員に引き継がれ、平成 24-25 年度ハードウェアセキュリティ評価において実際に活用され、現在に至っている。また、本事業で開発した運用技術とその知見は、別事業「暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発」（平成 23-25 年度）にインプットされ、同事業の成果物 “SENavigator”の開発に貢献した。

3）故障利用解析（DFA）技術等の研究開発

- DFA の一例として CryptoLSI の DES 実装に対して電源グリッチによる DFA を行い、一連の過程において以下の成果を得た。これらの成果は、他のデバイスにおける DFA の評価への応用にあたっても有用であると考えられる。
  - 高機能な DFA ツールの作成。
  - 共通入力ファイルによるツール間の統合。
  - 付随するデータ変換・可視化用スクリプトの作成。
  - SASEBO-R で外部クロック入力を可能にする FPGA デザインの作成。
  - DES 用フォールトエミュレーションツールの作成。
  - ツール・装置の操作に関する情報の収集。
  - SASEBO-R + CryptoLSI をターゲットとして作成したツールで DES DFA に成功。
  - 実験の再現性を確認。
  - 電圧・平文・クロック周波数の差によるグリッチ発生の変化について調査。
  - 電源電圧とフォールトの発生に関する考察。
  - 効率のよい解析方法について検討。
- 本事業で開発した運用技術とその知見は、別事業「暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発」（平成 22-24 年度）にインプットされ、平成 24 年度レーザ DFA 装置の開発に貢献した。

② 評価ツールの開発

- オランダ Rescure 社に対し、我が国固有の暗号アルゴリズムに対応する 10 件のモジュールの開発を委託し、所定の目標を達成した。再委託先オランダ Riscure 社への業務推進について、我が国 CC 認証機関 JISEC を運営する独立行政法人情報処理推進機構との協力を得て行った。
- 成果は我が国認証機関 JISEC に供用され同機関において利用されている。

【システム LSI セキュリティ評価に関する共同利用設備の整備】

① 共同利用設備の整備

- 都内オフィスビル内に試験室、評価室、研究室を設置し、試験施設とし、所要の設備を整備した。
- ASNITE-IT 認定体制下で、ハードウェア試験機関として必要十分と認められる試験施設設備を整備し､ASNITE-IT 及び ISO/IEC 17025 の認定を取得した。

② 委託事業終了後の共同利用設備の運営に関する検討

- 事業終了後の継承者として、株式会社電子商取引安全技術研究所（現社名：株式会社 ECSEC Laboratory）を選定した。
- 実施計画策定当初においては独立の試験機関を想定したが、試験機関の経営リスク等の問題があり、同一社内で CC 評価機関に併設される試験機関という形態となった。ただし、当該試験機関は併設される以外の他の評価機関の業務を請け負うことが出来るよう諸般の措置を講じることとした。
- 本事業で整備した施設と設備は、本項によって設立された試験機関に引き継がれ（設備は払い下げ)、平成 24-25 年度ハードウェアセキュリティ評価において実際に活用され、現在に至っている。
- 当初 22 年度中に検討を完了する予定であったが､東日本大震災により経済状況が不透明となる中で､試験機関の経営リスクを誰がとるか等の問題があり､検討を 23 年度に持ち越した。関係評価機関、ベンダ、認証機関等による公式の合意形成は ICSS-JC 代表者会議の場で行った。

【セキュリティ評価を行うために必要な人材の育成】

① 人材育成

1）試験者の育成

- 3 名の試験者要員を対象に、海外機関への再委託により脆弱性分析演習、セキュリティ対策実装チップへの攻撃演習等を実施した。但し、平成 23 年度末に試験者 1 名が病気のため出向元に帰任し、JISEC/HW 認証体制下の脆弱性分析試験者として 2 名が承認された。当初要員の選定にあたっては､ICSS-JC 内で参加企業に募集を行った。

- 本事業で育成した試験者 2 名は、設立された試験機関に引き継がれ、平成 24-25 年度ハードウェアセキュリティ評価その他の案件に実際に参加し、現在に至っている。
- 可能であれば、各種の試験に全要員が交代で取組みノウハウを共有する体制とすることが望ましかったが、平成 23 年度は試行評価スケジュールの遅れ、要員の病欠等により、やや専門分化せざるを得なかった。
- 平成 26 年 2 月の時点で、ハードゥエアの CC 評価だけでなく、こうした要員による脆弱性分析を単独で行う業務の引き合いが、数件試験機関に寄せられている。

2）評価者等の育成

- 評価者育成に向け、IC チップ脆弱性分析技術指導を実施、10 名の参加を得た。ICSS-JC を通じて技術指導参加者を募集した。
- 技術指導参加者 2 名が試行評価に参加、他 1 名がその後ハードウェア評価に参加している。これら 3 名の評価者が現在 JISEC 認証体制下のハードウェア評価者として承認を受けている。
- 本事業で育成した評価者は、試行評価、平成 24-25 年度ハードウェアセキュリティ評価において実際に参加し、現在に至っている。
- ハードウェア評価機関以外にも、ベンダ、他評価機関等より技術指導に参加した者が多数おり、知見を共有した。

② 育成した人材による試行評価

1）試行評価の実施

- ルネサスエレクトロニクス株式会社による製品評価依頼をもとに欧州の評価機関と本事業実施機関との試行評価を実施し、評価結果に関して、両者は同じ水準にあるものと報告された。評価依頼者は、実施機関による製品の脆弱性やバグの発見を評価した。

2）評価技術の確認（日欧共同評価による二国認証）

- 委託事業終了後、日仏二国の認証を取得した。開発者側の設計変更等の理由により、委託事業期間内に試行評価を完了できなかったが、委託事業終了後本件評価は、民間ベースの評価案件として日欧で継続され、評価完了、日仏で共に認証された。なお開発者側の希望により、前記認証は日仏ともに公開されていない（認証書によるエビデンスはある）。

【セキュリティ評価体制の構築に必要な調査】

① 海外技術動向調査

- 以下の調査を実施した。
  - ANSSI（フランス・パリ、平成 21 年 12 月）
  - Thales（フランス・パリ、平成 21 年 12 月）

- Brightsight（オランダ・Delft、平成 21 年 12 月）
- Renesas Europe（英国・Bone End、平成 22 年 1 月、平成 23 年 5 月）
- SiVenture（英国・Maidnhead、平成 22 年 1 月）
- JHAS（ベルギー・ブリュッセル、平成 22 年 1 月、3 月、5 月、7 月、9 月、11 月、平成 23 年 1 月、3 月、5 月、7 月、9 月、11 月、平成 23 年 1 月、3 月）
- Riscure（オランダ・Delft、平成 22 年 1 月、3 月、平成 22 年 6 月）
- Thales（フランス・ツールーズ、平成 22 年 6 月）
- SRC（ドイツ・ボン、平成 22 年 7 月）
- ICCC（トルコ・アンタルヤ、平成 22 年 9 月）
- ICCC（マレーシア・セランゴール、平成 22 年 9 月）

● 上記の調査は下記の目的で実施したものである。
- 我が国 ICSS-JC と欧州 JHAS との円滑なリエゾン関係構築による信頼関係の醸成
- 上記によるハードウェアセキュリティ全般（CC 評価方法・手順、脆弱性評定の方法等）に関する知見の共有
- 我が国ベンダのスマートカード製品、組込製品における開発力の向上
- 我が国ベンダの迅速なセキュリティ対策技術のキャッチアップ

● 欧州側に JHAS とは別に端末機に関するテクニカル・コミュニティである JTEMS が設立され、平成 22 年度以降日本との交流が開始されたので所要の対応を行った。

②IC カードを利用するユーザー側のセキュリティ要求仕様等に関する調査

● 再委託先により、以下の３種類の調査が実施された
- 国家公務員カード調査
- 決裁端末システム分野のユーザセキュリティ要求仕様調査
- マルチアプリケーションシステム分野のユーザセキュリティ要求仕様調査

● なお、上記 PP（セキュリティ要求仕様書）ドラフトを直接利用した CC 認証申請事例はない。理由は、本件成果が、PP ドラフトにとどまり CC 認証を得ていないため、ST 作成に際して直接利用できないことによる。実施計画策定時には、PP ドラフト作成後は、必要とするユーザ団体があれば、当該団体のコスト負担で CC 認証を取得する想定であった。しかしながら、そのようなユーザ団体が存在せず、コスト負担はなされなかった。これにより、事業化には結びつかなかった。

③ チップセキュリティ評価のための手順の調査

● IC チップのセキュリティ評価に関して、CC 補助文書に準拠したマニュアル

を作成した。本調査を通じて、フランス認証体制 ANSSI が我が国評価とほぼ同様の手順を共有した。このことにより、我が国ハードウェア評価機関の評価報告書の大部分が（フランス評価機関を通じてフランスの認証機関に提出された際に）ANSSI に承認されるようになった。

- 手順書は予定通り完成したが、試行評価の認証遅れにより手順の最終的に確認手続きが委託事業終了後となった。

４－Ｂ　事業化、波及効果について

４－１－Ｂ　事業化の見通し

本事業で構築した共同利用設備をはじめとする成果は、現在の株式会社 ECSEC Laboratory（旧社名：株式会社電子商取引安全技術研究所）に引き継がれ、平成２４年９月､国内におけるICカード等ハードウェアのセキュリティ評価体制が確立した。

同社はハードウェア侵入テスト機関を内包して運用している。当該ハードウェア侵入テスト機関は、同社内の CC（Common Criteria）評価機関だけでなく、他社の CC 評価機関に対してハードウェア CC 評価における侵入テストサービスを提供することを可能とした。これは、国内における他の CC 評価機関が個別に設備を保有することは資金面を考慮すると難しいため、本事業で構築した設備を実質的に共同で利用できるように配慮したためである。

４－２－Ｂ　波及効果

以下の３種類の波及効果が期待される。

（１）情報セキュリティ対策への効果

国内 IC カードベンダがこれまでよりも認証取得を積極的に行うことにより、IC カード等を利用する際の物理的脅威の減少が期待できる。

本事業を通じて、フランス認証体制 ANSSI が我が国評価とほぼ同様の手順を共有したことにより、我が国ハードウェア評価機関の評価報告書の大部分が（フランス評価機関を通じてフランスの認証機関に提出された際に）ANSSI に承認されるようになったことで、同国向けの製品開発を促す効果が期待できる。

なお、本目的をさらに推進するため、本事業を通じて「国家公務員カード調査」「決裁端末システム分野のユーザセキュリティ要求仕様調査」及び「マルチアプリケーションシステム分野のユーザセキュリティ要求仕様調査」の３件の調査により各用途についてのプロテクションプロファイル（PP）を作成したが、現時点においてそれらについての CC 認証が行われていないため、十分な効果発揮には至っていない。

（２）民間産業への波及効果

本事業における欧州 JHAS（JIL Hardware Attack Sub working group）との技術交流等を通じて、人脈が太くなり、欧州における最新の脆弱性情報を引き続き入手しやすくなり、国内企業にフィードバックすることが容易になる。

また、国内 IC カードベンダの製品における認証取得率の向上により、国際的な製品競争力の向上が期待できる。

（３）社会への波及効果

国内に IC カード等のハードウェアの物理的安全性を評価できる環境を有することによる、ナショナルセキュリティ面での効果が期待できる。

５－Ｂ　研究開発マネジメント・体制・資金・費用対効果等

５－１－Ｂ　研究開発計画

本事業は、平成 22 年度から 24 年度までの 3 年計画である。各要素技術の研究開発計画は次表のとおりである。

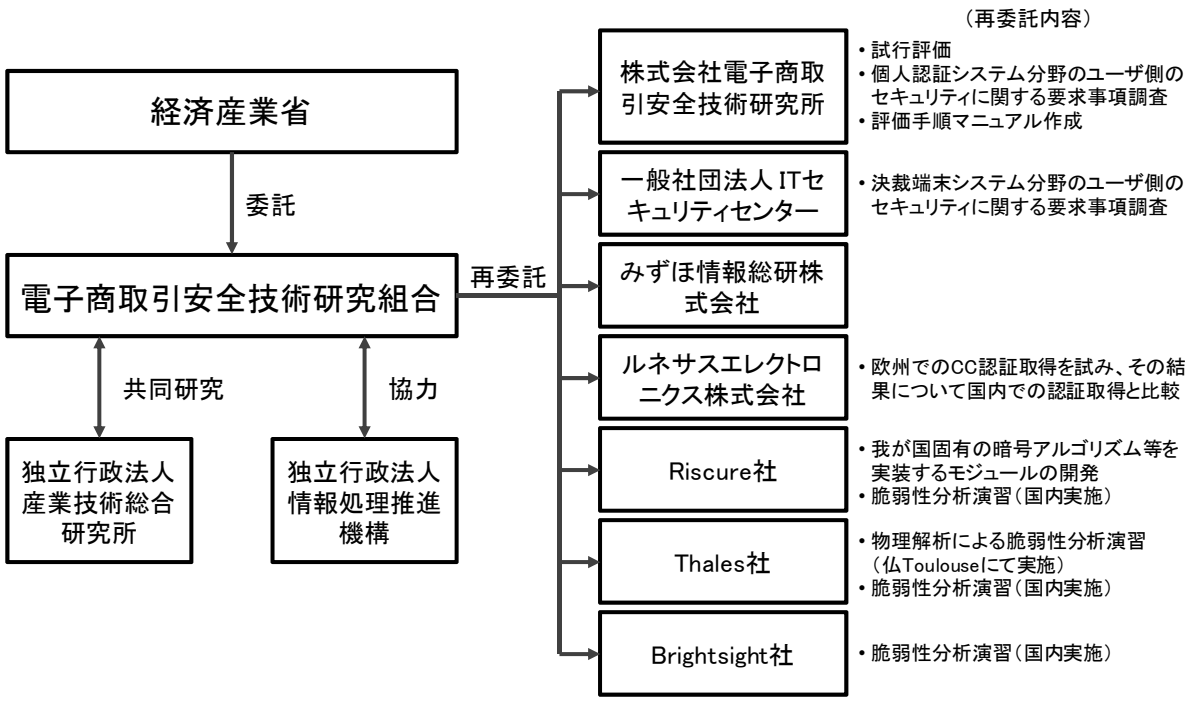
東日本大震災により平成 22 年度末から平成 23 年度前半にかけて、共同研究先である独立行政法人産業技術総合研究所の一部設備が使用不能となったが、本事業で購入した岩本町設備の範囲で研究を続行した。

表Ｂ－４　研究開発計画

年度	平成21年度	平成22年度	平成23年度
予算額	2.6億円	3.0億円	1.0億円
セキュリティ評価を行うために必要な技術の開発	新規・既知の攻撃方法に関する評価手法の開発 評価ツールの開発	新規・既知の攻撃方法に関する評価手法の開発 評価ツールの開発	新規・既知の攻撃方法に関する評価手法の開発
システムLSIセキュリティ評価に関する共同利用設備の整備	共同利用設備の整備	共同利用設備の整備 委託事業終了後の共同利用設備の運営に関する検討	共同利用設備の整備 委託事業終了後の共同利用設備の運営に関する検討
セキュリティ評価を行うために必要な人材育成	人材育成	人材育成 育成した人材による試行評価	人材育成 育成した人材による試行評価
セキュリティ評価体制の構築に必要な調査	海外技術動向調査 ICカードを利用するユーザー側のセキュリティ要求仕様等に関する調査 チップセキュリティ評価のための手順の調査	海外技術動向調査 ICカードを利用するユーザー側のセキュリティ要求仕様等に関する調査 チップセキュリティ評価のための手順の調査	海外技術動向調査 （成果物の英訳）

５－２－Ｂ　研究開発実施者の実施体制・運営

本事業は、平成 21 年度から平成 23 年度において、経済産業省から電子商取引安全技術研究組合への委託により実施されている。また各年度につき、再委託先として以下の機関が事業に参加した



図Ｂ－１　研究開発実施体制

５－３－Ｂ　資金配分

表Ｂ－５資金配分　　(単位百万円)

要素技術	平成21年度	平成22年度	平成23年度
高度電磁波解析技術によるLSIのセキュリティ対策に関する研究	**2.6**	**3.0**	**1.0**

５－４－Ｂ　費用対効果

本研究開発の成果をもとに、平成 24 年 9 月から、株式会社 ECSEC Laboratory が国内初の IC カード等ハードウェアセキュリティ評価機関としてスタート。これまでハードウェア認証 4 件が実施され、1 件が評価中となっている。また、これ以外に脆弱性試験のみの評価案件も複数件実施している。これまで欧州に依存していたハードウェアセキュリティ評価が自国で可能になったことは、認証を受ける者のコスト低減に資するとともに、我が国技術の流出を未然に防止する効果も期待される。

５－５－Ｂ　変化への対応

平成 22 年 3 月に発生した東日本大震災により、平成 22 年度末から平成 23 年度前半にかけて、共同研究先である独立行政法人産業技術総合研究所の一部設備が使用不能となったが、本事業で購入した岩本町設備の範囲で研究を続行した。

Ｃ　暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発

１－Ｃ　事業の目的・政策的位置付け

１－１－Ｃ　事業の目的

暗号製品の実装技術は公開されることがほとんどないため、実装性能評価においても評価手法により大きな差が出たとしても第三者検証ができない、また物理的安全性評価においても評価手法の標準化と公正な評価が難しいという問題がある。これに対して、ハードウェア設計・解析の高い技術力を背景としながらも、極めて高い専門性を有する一部の研究者やエンジニアだけが利用できる特殊な環境ではなく、評価制度として第三者が実施可能な統合システムを構築し、かつ民間の活力を利用したビジネスとして成立させるレベルにまで落とし込むことが大きな課題である。

本研究開発は、このような背景にあって、暗号アルゴリズムの危殆化に伴う標準アルゴリズムの選定作業等において、ハードウェアの実装性能評価及び物理的な安全性の評価を統合的に行うシステムを開発し、さらにLSI 解析技術の進歩による将来的な脆弱性の検討を行い、これらの技術開発の成果を、ISO/IEC 19790/24759 に則したJCMVP(Japan Cryptographic Module Validation Program)等の暗号モジュール試験認証制度や、ISO/IEC 15408 Common Criteria における IC カード評価等にインプットすることで、国際標準規格の改定に貢献することと、国内企業の技術の底上げと国際競争力の向上に貢献することを目的とする。

１－２－Ｃ　政策的位置付け

本事業は政府全体の情報セキュリティ政策の中長期計画である「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）に基づき推進するものである。また、サイバーセキュリティ２０１１（平成２３年７月８日情報セキュリティ政策会議決定）において提唱されている「システム LSI のセキュリティ評価・認証体制の整備」にも資する事業である。

＜国民を守る情報セキュリティ戦略（抜粋）＞

インターネットを始めとする情報通信技術を利用者が活用するにあたっての脆弱性の克服や、IPv6 や、クラウドコンピューティング、情報家電、携帯端末、センサーネットワーク等の情報通信技術の環境の変化に対応した情報セキュリティ技術の開発、高度化・多様化する攻撃等に対応できる情報セキュリティ技術（「グランドチャレンジ型」研究開発・技術開発）の実現・普及の実現を目指す。

＜サイバーセキュリティ２０１１（抜粋）＞

(ｲ) システム LSI のセキュリティ評価・認証体制の整備（経済産業省）

2011 年度までに、IC カード等に用いられるシステム LSI について、国内で ISO/IEC15408 に基づくセキュリティ評価・認証が行えるよう必要な体制整備を行うため、脆弱性評価用標準スマートカードの整備、人材育成、調査等を着実に実施する。

１－３－Ｃ　国の関与の必要性

本事業は、CAD ナビゲーションシステムや電磁照射プローブの開発など、既存製品がなく学術的にも新しい分野に取り組む内容である。また、5 項目の課題およびその研究成果を暗号ハードウェア評価システムへ統合し、評価環境を整えることは、経済産業省が同時並行的に実施していたハードウェアセキュリティの評価・認証体制の確立に資する事業である。これらの成果は、JCMVP 試験や CC 評価およびそれらに関する国際規格の改定に貢献するものと考えられる。また、国内企業の技術の底上げと国際競争力の向上への貢献にも大きな期待ができるため、国が関与することが適当である。

２－Ｃ　研究開発等の目標

２－１－Ｃ　研究開発目標

近年、実装の物理的な安全性評価が急務となっている。図１に示すように、アルゴリズムが実装された「暗号モジュール」が処理時に発生する電磁波や電力波形を解析して内部の秘密情報を盗み出す「サイドチャネル攻撃」の研究が発展し、それに対する安全性評価指針の国際標準化と試験認証制度の準備が進んでいる。さらに、レーザー等を使って誤動作を誘発するなど、より高度な攻撃方法の研究が進んでおり、急速に進歩するLSI 解析装置を利用した最先端の技術を用いた攻撃にも備える必要が出てきている。

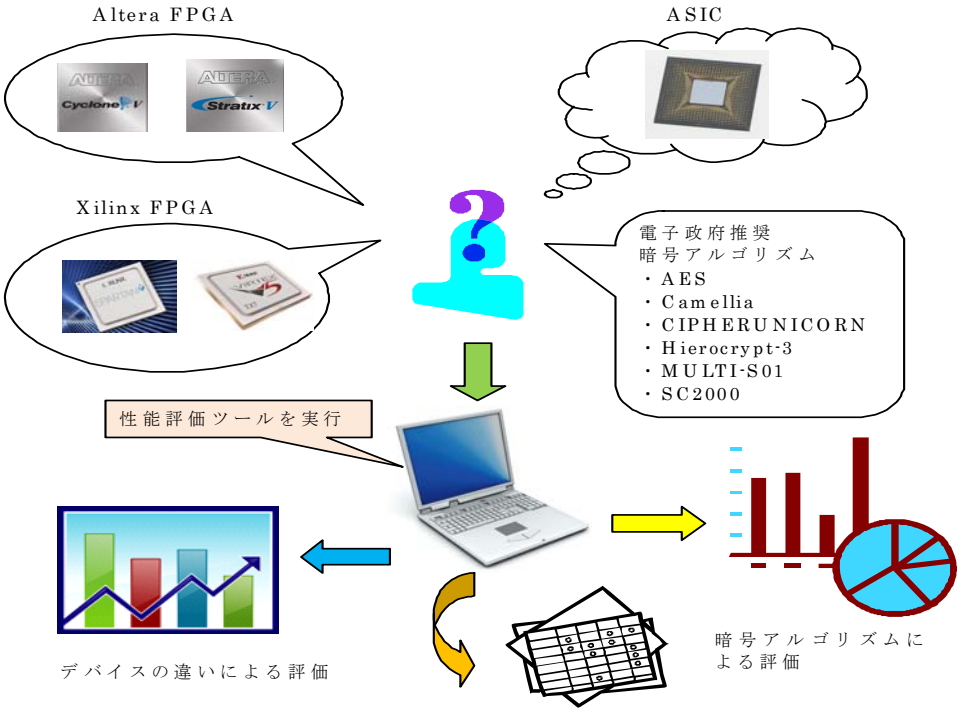
こうした状況に対応するため、暗号アルゴリズムの物理的安全性評価に必要な研究開発を実施し、その成果を暗号ハードウェア評価システムに統合する。

図Ｃ－１　暗号モジュールの安全性評価に関する研究開発

（１－１）暗号ハードウェア実装性能評価ツールの開発

暗号モジュールの回路規模、処理速度、消費電力などの実装性能を評価するためには、ターゲットとするハードウェアの開発ツールで暗号モジュールの HDL（Hardware Description Language：ハードウェア記述言語）をビルドし、性能の解析を行うことでレポート出力を得る。FPGA や ASIC の複数のハードウェアプラットフォームをターゲットとして評価を行うためには、複数の開発ツールでそれぞれビルドと解析を行う必要があり、複数の暗号モジュールを評価するためには、暗号モジュール毎にこれらの手順を繰り返す必要がある。また、性能評価指標を追加する場合や、性能評価方法を変更する場合には、すべての暗号モジュールについて解析をやり直さなければならないことがある。したがって、正しい性能評価を効率的かつ網羅的に行うためには、実装性能評価の自動化と評価結果の可視化が重要である。

そこで、HDL ソースを入力として論理合成を行い、アルゴリズムや構成法そして実装プラットフォームに対する各種性能指標の比較を、表やグラフで自動的に表示する評価ツールを開発する。



図Ｃ－２　FPGA 及び ASIC による性能評価

（１－２）サイドチャネル攻撃耐性評価ツールの開発

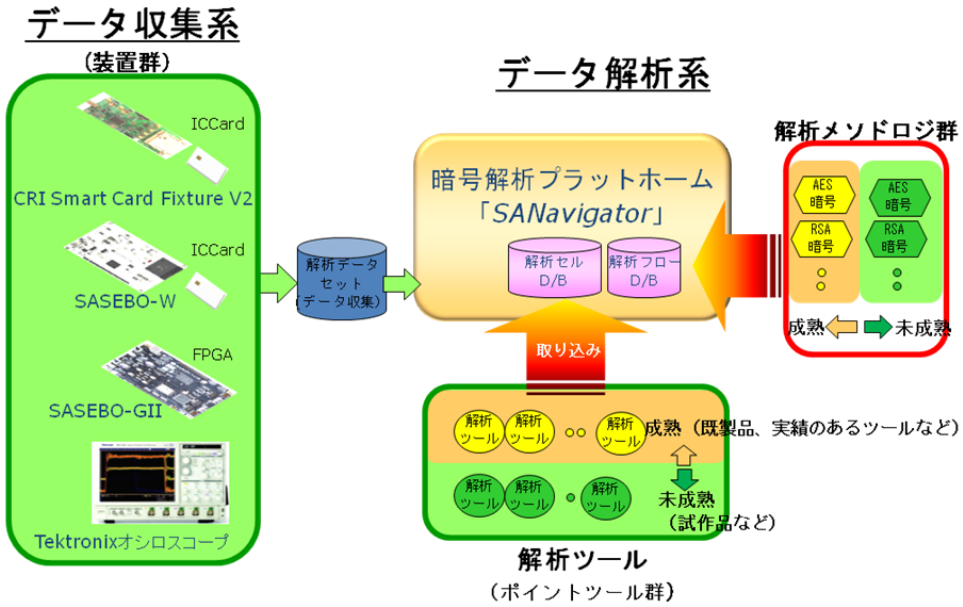
暗号アルゴリズムを実装したハードウェアモジュールの安全性を担保するために、各種サイドチャネル攻撃に対する網羅的な評価ツールを開発する。

サイドチャネル攻撃の耐性評価を行うためには、データの収集、データの解析、評価結果表示の処理が必要である。これらの処理を行う際の解析対象となる暗号モジュ

ールの実装形態は接触/非接触 IC カード・ASIC・FPGA などが考えられ、測定する漏洩情報は消費電力や電磁界などが考えられる。これらの組み合わせに対して、漏洩情報を測定するためのオシロスコープ等の計測機器を加えると膨大な組み合わせが存在することになる。しかし、従来のサイドチャネル攻撃の評価環境では特定の組み合わせのみがサポートされていることから、サイドチャネル攻撃の評価を行うためには、評価プラットフォーム一式を構築しなおす必要があり、このことが評価環境の導入を難しくしていると考えられる。

そのような複数のサイドチャネル攻撃手法、モジュールの実装形態、計測機器から選択された対象に対して、統合されたグラフィカル ユーザ インタフェースからデータの収集・解析・表示を可能とする、評価用ソフトウェアを開発する。

また、評価対象の暗号モジュールとして、銀行・クレジットカードや電子マネー、交通系等に広く用いられ、高い物理セキュリティが求められる IC カードが重要である。特に近年は、非接触の IC カードが用いられるようになってきているが、現在はまだ非接触 IC カードのセキュリティ評価に適した評価ボード等は見られない。そこで、非接触 IC カードの暗号処理中の消費電力及び放射電磁波の収集を容易に行える環境を構築する。

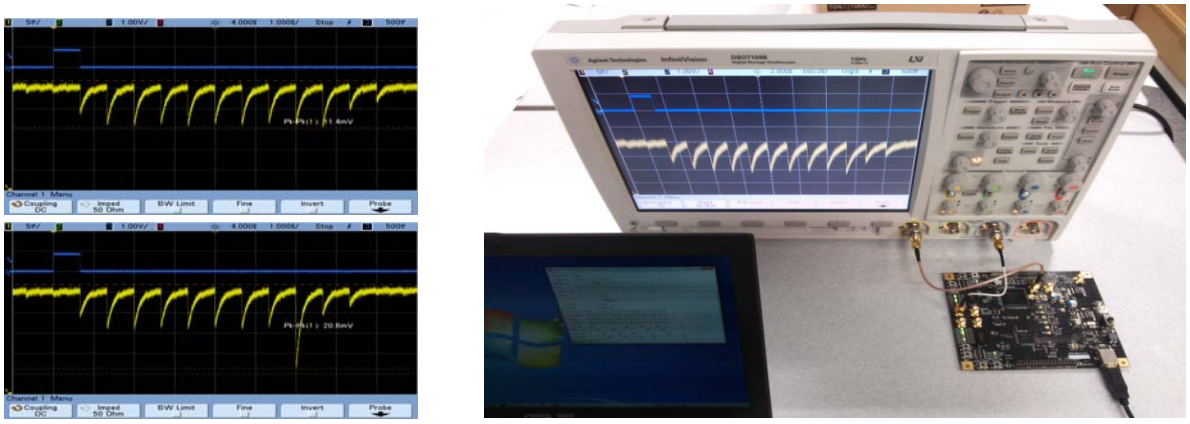


図Ｃ－３　サイドチャネル攻撃耐性評価ツールの機能

（１－３）フォールト攻撃耐性評価ツール及び試験装置の開発

暗号モジュールに対して外部から電圧やクロックを操作して異常動作を引き起こすことで、サイドチャネル攻撃では得られない情報を取得するフォールト攻撃の研究が活発化している。暗号モジュールにどのような異常動作が起こせるのか、解析に使える有用な情報を与ることができるのかといったことは、実装形態に大きく依存するため、サイドチャネル攻撃よりも強力な攻撃となりえる半面、解析も難しい。しかしながら評価においては、解析によって秘密鍵を盗み出せるかという以前に、再現性の

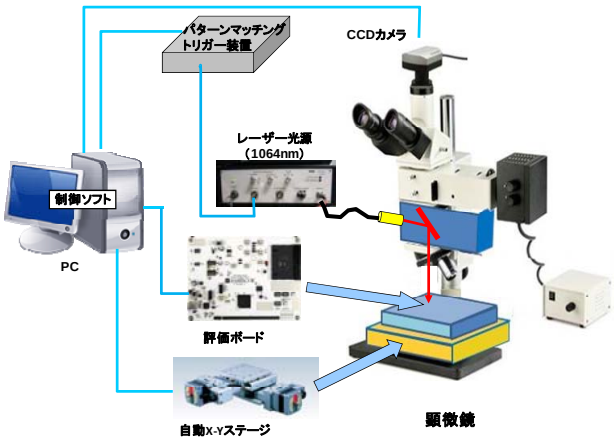
あるエラーを引き起こすことができない、あるいはエラーが発生したことを検出して暗号モジュールが何らかのアクションを取ることができるかといった観点で試験を行うこともできる。なお、再現性のあるエラーを引き起こせたとしてもそれが解析できるどうかは別の問題である。そこで、サイドチャネル攻撃評価ボード SASEBO の機能を拡張して、FPGA や、既開発の暗号 LSI、そして新規開発の IC カード評価装置にクロックや電源にグリッチを挿入して内部データやシーケンスにエラーを発生させる試験環境を構築する。



図Ｃ－４　SAKURA-G 上のオンボードグリッチ実験環境と実験結果

（１－４）侵襲攻撃耐性評価環境の構築

クロックや電源の操作といった外部からの能動的な攻撃からさらに積極的に、パッケージを開封してLSI内部の動作を直接操作する侵襲攻撃評価を行う環境を構築する。評価試験を行うものは、攻撃者と異なりLSIの設計情報にアクセスできるという仮定のもとに、レイアウト情報と連携し、所定の回路上を観察し、レーザーや電磁波を照射して誤動作を誘発する等のより高度な攻撃を実施する。そのために、レーザー照射位置をμmオーダーで制御可能な装置や制御ソフトウェアの開発、電磁波を照射して誤動作を誘発するための専用装置の開発等を行う。

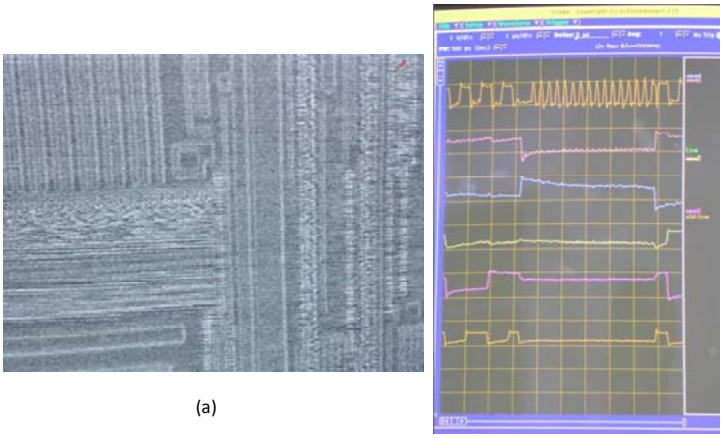


図Ｃ－５　レーザー照射システム構成図

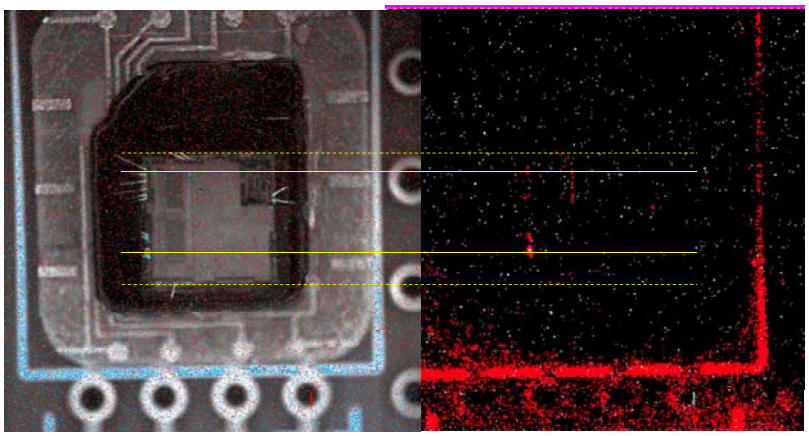
（１－５）集積回路解析技術によるLSI内部動作解析及び先端技術調査

FIB（収束イオンビーム）装置、EB（エレクトロンビーム）テスタ、LSIプローバなど、LSI加工装置や測定装置を用いて内部動作の解析を行い、サイドチャネル攻撃やフォールト攻撃では得られないLSIの局所的な情報を取得する技術の研究を行う。

暗号LSIの動作時に内部の挙動を直接観測し、かつLSIの設計情報を利用しながら取得したデータを詳細に解析することで、より精密な安全性評価が可能となる。現在は、ごく限られた研究者でしか実施できない攻撃法であっても、解析装置の価格対性能比は年々向上していることから、それが現実的な脅威となる前に先んじて研究を進め、対策について検討しておく必要がある。そこで、先端の集積回路解析技術を駆使して、暗号LSIを直接観測し、内部の秘密情報を取得する研究、実験、技術開発を行う。本課題においては、電子線プローブを使用してLSIチップの内部の動作解析する手法と、LSI表面又は裏面から先端の加工技術を用いてLSIを加工し、より内部の波形の可観測性を向上させる手法のふたつを用いて、LSIの内部動作の解析を行う。この課題に対して、先端LSI解析装置による暗号モジュールの動作解析と暗号LSI動作解析のための集積回路加工技術の開発を行う。



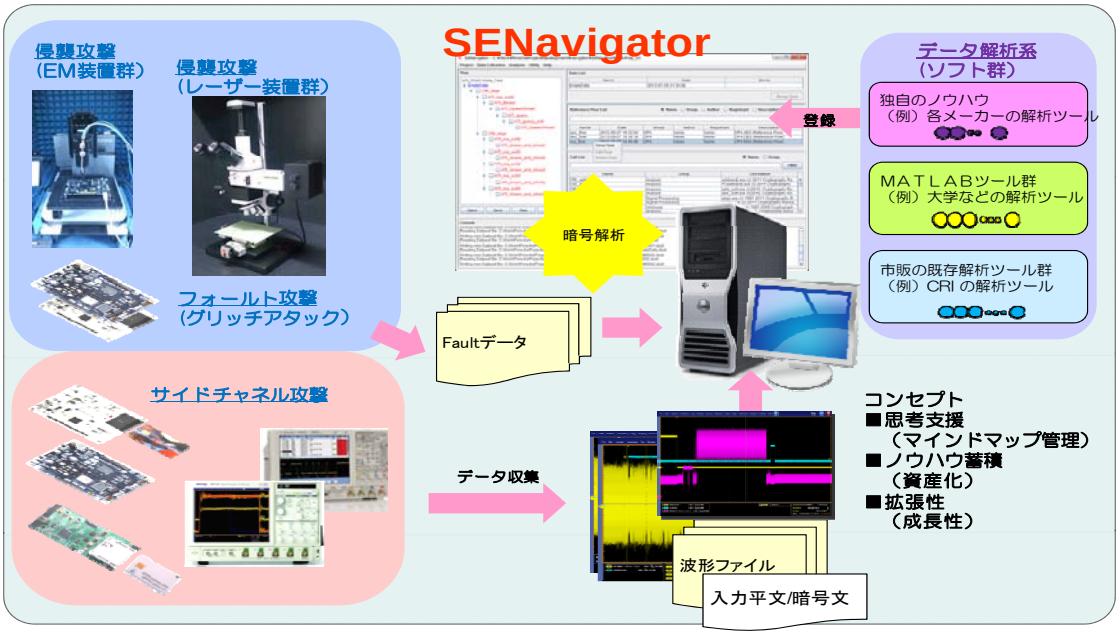
図Ｃ－６　ATMega IC Card Chip の(a)電位コントラスト像と(b)波形



図Ｃ－７　ATMega IC Card Chip の発光解析結果

（１－６）統合ハードウェア評価プラットフォームの構築

極めて高い専門性を有する一部の研究者やエンジニアだけが利用できる特殊な環境ではなく、評価制度として第三者が実施可能な、ハードウェアの実装性能評価及び物理的な安全性の評価を統合的に行うシステムの開発とその実用化に向けて、平成 25 年度は統合ハードウェア評価プラットフォームを構築し、それにプラグインして使用できる各種評価技術群をサブシステムとしてパッケージ化する。



図Ｃ－８　統合ハードウェア評価プラットフォームのシステム構成図

２－２－Ｃ　全体の目標設定

表Ｃ－１　全体の目標

目標・指標	設定理由・根拠等
上記１－１から１－５において得られた研究開発成果を統合ハードウェア評価プラットフォームに集約する	極めて高い専門性を有する一部の研究者やエンジニアだけが利用できる特殊な環境ではなく、評価制度として第三者が実施可能な、ハードウェアの実装性能評価及び物理的な安全性の評価を統合的に行うシステムを構築することにより、民間の活力を利用したビジネスの成立を目指す

２－３－Ｃ　個別要素技術の目標設定

表Ｃ－２　個別要素技術の目標

要素技術	目標・指標	設定理由・根拠等
暗号ハードウェア実装性能評価ツールの開発	暗号アルゴリズムや構成法そして実装プラットフォームに対する各種性能指標の比較を、表やグラフで自動的に表示する評価ツールを開発する	暗号アルゴリズムをハードウェアに実装した時の性能はハードウェアやパラメータ設定によって異なるが、その性能比較には多大な労力が必要となる そこで正しい性能評価を効率的かつ網羅的に行うために、実装性能評価の自動化と評価結果の可視化が重要である
サイドチャネル攻撃耐性評価ツールの開発	各種サイドチャネル攻撃に対する網羅的な評価ツールを開発する	サイドチャネル攻撃の耐性評価を行うためには、データの収集、解析、評価結果表示の処理が必要であるが、従来の環境では特定の組み合わせのみがサポートされているため、評価を行うためにはプラットフォーム一式を構築しなおす必要があり、このことが評価環境の導入を難しくしている そこで複数の攻撃手法、計測機器に対して統合されたグラフィカル ユーザ インタフェースから操作を可能とする、評価用ソフトウェアが必要である
フォールト攻撃耐性評価ツール及び試験装置の開発	クロックや電源にグリッチを挿入してエラーを発生させる試験環境を構築する	暗号モジュールに対して外部から電圧やクロックを操作して異常動作を引き起こすことで、サイドチャネル攻撃では得られない情報を取得するフォールト攻撃の研究が活発化している しかしながら評価においては、再現性のあるエラーを引き起こすことが難しい そこで研究者が扱い易い評価ボードを使用した試験環境を提供する
侵襲攻撃耐性評価環境の構築	パッケージを開封してLSI内部の動作を直接操作する侵襲攻撃評価を行う環境を構築する	レーザーや電磁波を照射して誤動作を誘発する等のより高度な攻撃環境はまだ市場に少なくかつ非常に高価である そこでレーザー照射位置をミクロンオーダーで制御可能な装置や制御ソフトウェア、

		電磁波を照射して誤動作を誘発するなどの機能を備えた安価を目指した専用装置の開発を行う
集積回路解析技術によるＬＳＩ内部動作解析及び先端技術調査	先端の集積回路解析装置を用いて LSI の内部動作解析を実施し、LSI の局所的な動作情報を取得する技術の研究開発を行う	暗号 LSI の動作時に内部の挙動を直接観測し、かつ LSI の設計情報を利用しながら取得したデータを詳細に解析することで、より精密な安全性評価が可能となる 現在は、ごく限られた研究者でしか実施できない攻撃法であっても、解析装置の価格対性能比は年々向上していることから、それが現実的な脅威となる前に先んじて研究を進め、対策について検討しておく必要がある

３－Ｃ　成果、目標の達成度

３－１－Ｃ　成果

３－１－１－Ｃ　全体成果

（１）成果

これまでの評価技術の成果をまとめ、個々の単位で商品化が可能なパッケージングを行った。レーザー、電磁波照射装置などは、統合環境に組み込まれた形の商品化だけでなく、それぞれの用途に応じた商品として販売を計画している。

また、ひとつの評価対象に対して、サイドチャネル攻撃、フォールト攻撃および侵襲攻撃の解析評価を、一貫して行うことができるツール(SENavigator)を開発した。この「統合ハードウェア評価プラットフォーム（SENavigator)」は、暗号モジュール試験認証制度に則った評価フローを実行するためのツールとして使用可能であると想定され、商品化に向けて準備を進めている。

上記のとおり、極めて高い専門性を有する一部の研究者やエンジニアだけが利用できる特殊な環境ではなく、評価制度として第三者が実施可能な、ハードウェアの実装性能評価及び物理的な安全性の評価を統合的に行うシステム「統合ハードウェア評価プラットフォーム」が構築でき、さらにそのシステムに対して日々進化する解析手法などに対応できるよう独自に解析手法などを追加できる、またその環境を活用することにより過去の資産を蓄積しさらに必要に応じて再現・再利用が可能、などの付加価値を付けることができた。

以下、個々の事業内容についてその成果と目標達成度をまとめる。

３－１－２－Ｃ　個別要素技術成果

（１－１）暗号ハードウェア実装性能評価ツールの開発

暗号モジュールとデバイスの複数の組み合わせから性能レポートを出力する性能評価を自動化した。また、評価レポートから暗号モジュールの回路規模、処理速度などを可視化するツールを開発した。

（１－２）サイドチャネル攻撃耐性評価ツールの開発

各種サイドチャネル攻撃の耐性評価のためのデータ収集、データの解析、および評価結果の表示等、各種機能を統括するツール(SANavigator)を開発した。また、サイドチャネル攻撃の耐性評価に適した非接触 IC カード評価プラットフォームを設計し、解析実験を行った。

（１－３）フォールト攻撃耐性評価ツール及び試験装置の開発

クロック信号、リセット信号、電源それぞれに非常に細いパルスを混入するグリッチ機能を開発した。その環境を使用して評価実験を行い、検証のため解析プログラムを開発した。

（１－４）侵襲攻撃耐性評価環境の構築

外乱誘発装置としてレーザー照射装置と電磁波照射装置を開発した。また、LSI の CAD データを用いた照射座標の制御、フォールトの発生状況を描画する CAD ナビゲーションシステムを開発した。

なお、電磁波照射装置は本事業が先鞭をつけた技術である。平成 23 年度においては、暗号回路に対して故障を誘発できることを確認するにとどまったが、平成 24 年度には、電磁波照射装置を使用した実験では世界で初めて再現性のあるフォールト攻撃評価環境を構築するとともに、実験版レーザー照射装置を使用した実験では、接触型 IC カードを用いて加工を一切行わずフォールト攻撃に成功し、それらの実験結果を ISEC 等にて論文発表を行った。

（１－５）集積回路解析技術によるＬＳＩ内部動作解析及び先端技術調査

暗号 LSI、接触型 IC カード内のチップに対して、電子線プローブにより内部信号を観測した。また、接触型 IC カード内のチップに対して発光解析を行い、電子線プローブでの観測結果とよい対応関係を示していることを確認した。

３－２－Ｃ　特許出願状況等

表Ｃ－３　特許・論文等件数

論文数	論文の被引用度数	特許等件数(出願を含む)	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
3	0	0	0	0	0	0

論文のリストは以下のとおり。また、本事業の開発成果と研究結果を、暗号と情報セキュリティに関する国内最大級の学会（SCIS）において技術展示をあわせて行い、普及促進を積極的に図った。

- 土屋 遊, 岸川 剛, 齋藤 翔平, 遠山 毅, 佐々木 明彦, 佐藤 証, 松本 勉, “電磁波照射を用いたフォールト攻撃による IC カードからの AES 鍵の抽出,” 電子情報通信学会技術研究報告　Vol.112, No.305, pp. 1-8, ISEC2012-57, 2012.

- 遠山 毅, 土屋 遊, 大野 仁, 岸川 剛, 齋藤 翔平, 佐々木 明彦, 佐藤 証, 松本 勉,“電磁波照射を用いたフォールト攻撃による IC カードからの AES 鍵の抽出(2),” 2013 年暗号と情報セキュリティシンポジウム, 予稿集 CD-ROM, 3E4-4, 2013.

- 大野 仁, 土屋 遊, 遠山 毅, 岸川 剛, 齋藤 翔平, 佐々木 明彦, 佐藤 証, 松本 勉,“非加工接触型 IC カードのレーザー照射によるフォールト攻撃,” 電子情報通信学会技術研究報告 Vol. 112, No. 460, pp. 195-202, ISEC2012-111, 2013.

３－３－Ｃ　目標の達成度

表Ｃ－４　目標に対する成果・達成度の一覧表

要素技術	目標・指標	成果	達成度
暗号ハードウェア実装性能評価ツールの開発	暗号アルゴリズムや構成法そして実装プラットフォームに対する各種性能指標の比較を、表やグラフで自動的に表示する評価ツールを開発する	・暗号モジュールとデバイスの複数の組み合わせから性能レポートを出力する性能評価を自動化した ・評価レポートから暗号モジュールの回路規模、処理速度などを可視化するツールを開発した	達成

要素技術	目標・指標	成果	達成度
サイドチャネル攻撃耐性評価ツールの開発	各種サイドチャネル攻撃に対する網羅的な評価ツールを開発する	・各種サイドチャネル攻撃の耐性評価のためのデータ収集、データの解析、および評価結果の表示等、各種機能を統括するツール(SANavigator)を開発した ・サイドチャネル攻撃の耐性評価に適した非接触 IC カード評価プラットフォームを設計し、解析実験を行った	達成
フォールト攻撃耐性評価ツール及び試験装置の開発	クロックや電源にグリッチを挿入してエラーを発生させる試験環境を構築する	・クロック信号、リセット信号、電源それぞれに非常に細いパルスを混入するグリッチ機能を開発した ・その環境を使用して評価実験を行い、検証のため解析プログラムを開発した	達成
侵襲攻撃耐性評価環境の構築	パッケージを開封してLSI内部の動作を直接操作する侵襲攻撃評価を行う環境を構築する	・外乱誘発装置としてレーザー照射システムと電磁波照射装置を開発した ・LSI の CAD データを用いた照射座標の制御、フォールトの発生状況を描画する CAD ナビゲーションシステムを開発した ・レーザー照射装置は当初の目標であったコストを下げた構成、複数回レーザーを照射できるシステムを目指したが、さらにレーザーパワーロスの削減、レーザー径縮小など計画以上の精度を出すことができた。	達成
集積回路解析技術によるＬＳＩ内部動作解析及び先端技術調査	先端の集積回路解析装置を用いて LSI の内部動作解析を実施し、LSI の局所的な動作情報を取得する技術の研究開発を行う	・暗号 LSI、接触型 IC カード内のチップに対して、電子線プローブにより内部信号を観測した ・接触型 IC カード内のチップに対して発光解析を行い、電子線プローブでの観測結果とよい対応関係を示していることを確認した	達成

４－Ｃ　事業化、波及効果について

４－１－Ｃ　事業化の見通し

本事業の開発成果と研究結果を暗号と情報セキュリティに関する国内最大級の学会（SCIS）にて技術展示および論文発表を行い、普及促進を積極的に図った。

また、開発成果を統合した環境「統合ハードウェア評価プラットフォーム（SENavigator)」は、暗号モジュール試験認証制度に則った評価フローを実行するためのツールとして使用可能であると想定され、商品化に向けて準備を進めている。今年度末までの事業であるため、具体的な販売実績はまだ出ていないが、既に４社に対してデモンストレーションを実施し、商談に向けて継続活動中である。

さらに、本事業で生まれた評価ボード SAKURA-G は世界で広く認知されている標準評価ボード SASEBO-GII が製造中止となったため、その後継として商品化し、世界に供給を開始した。

なお、レーザー照射装置、電磁波照射装置などは、統合環境に組み込まれた形の商品化だけでなく、それぞれの用途に応じた商品として販売を計画している。

４－２－Ｃ　波及効果

成果物である統合ハードウェア評価プラットフォームを研究者などが利用可能な場所への設置が実現できれば、国内企業、大学等の研究団体の技術の底上げと国際競争力の向上への貢献が期待できる。

レーザー、電磁波照射により誤作動を誘発する研究が進められているが、その設備を準備するには現時点では海外の装置を利用するか、自作するなど費用がかかる手段しかないと考えられる。これに対して本事業の開発成果であるレーザー、電磁波装置はそれと比較して安価で提供することが可能であり、最先端の技術を用いた攻撃手法の研究促進への貢献が期待できる。

５－Ｃ　研究開発マネジメント・体制・資金・費用対効果等

５－１－Ｃ　研究開発計画

本事業は、平成 23 年度から 25 年度までの 3 年計画である。現在、最終年度の研究開発を進めており、当初の予定の計画通り、H25 年度で事業を完了する予定である。

なお、本事業の申請段階では、実用化にはリスクのある技術開発として、LSI の高度な不良解析技術を応用した暗号解析技術の確立をも視野に置いていた。初年度の研究において、一部の汎用技術がデータ収集の手段として使えることは確認できたので、最終年度は新たな研究開発より、それまでの成果の実用化を優先し、開発項目の見直しを行った。

各要素技術の研究開発計画は次のとおりである。

表Ｃ－５研究開発計画

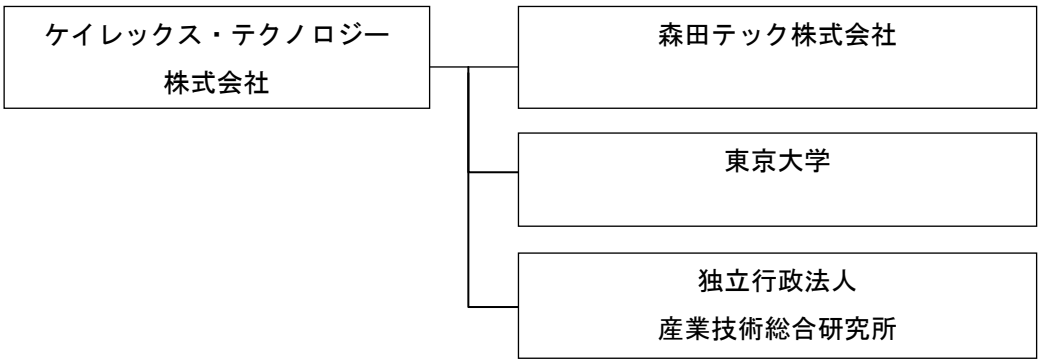
年度 要素技術	平成 23 年度	平成 24 年度	平成 25 年度
予算額	120 百万円	125 百万円	62 百万円
①暗号ハードウェア実装性能評価ツールの開発	開発・実験等		パッケージ化
②サイドチャネル攻撃耐性評価ツールの開発	開発・実験等		パッケージ化
③フォールト攻撃耐性評価ツール及び試験装置の開発	開発・実験等		パッケージ化
④侵襲攻撃耐性評価環境の構築	開発・実験等		パッケージ化
⑤集積回路解析技術によるＬＳＩ内部動作解析及び先端技術調査	解析・調査		
⑥統合ハードウェア評価プラットフォームの構築			統合化

５－２－Ｃ　研究開発実施者の実施体制・運営

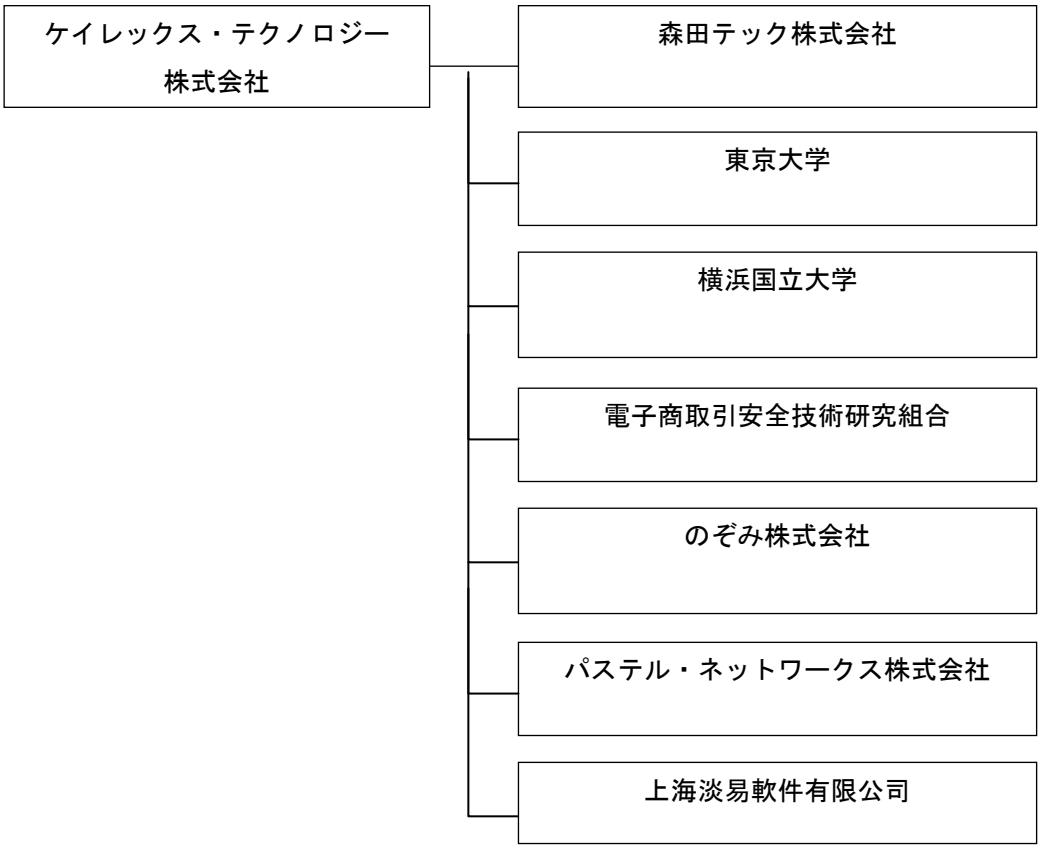
本事業は、平成 23 年度から平成 25 年度において、経済産業省からケイレックス・テクノロジー株式会社への直接委託により実施されている。また、下の図で示すとおり、再委託先として森田テック株式会社、電子商取引安全技術研究組合等が事業に参加した。事業の進捗状況を踏まえ、適切な体制を組んで実施したものと考えている。

なお、再委託先を中心に年度毎に体制の変更が生じたが、早めの引き継ぎ実施、各事業メンバーのフォローなどにより、体制変更による混乱は起きなかった。

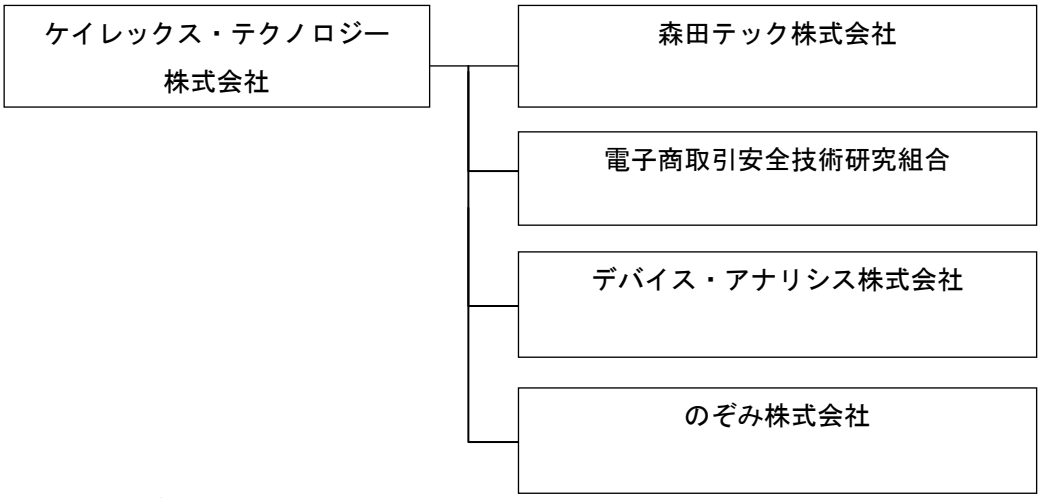
図Ｃ－９　研究開発実施体制（H23）



図Ｃ－１０　研究開発実施体制（H24）



図Ｃ－１１　研究開発実施体制（H25）



５－３－Ｃ　資金配分

表Ｃ－６　資金配分　　（単位：百万円）

年度 / 要素技術	平成 23 年度	平成 24 年度	平成 25 年度	合計
暗号ハードウェア実装性能評価ツールの開発	1.8	3.5	3.8	9.1
サイドチャネル攻撃耐性評価ツールの開発	34.2	20.8	7.5	62.5
フォールト攻撃耐性評価ツール及び試験装置の開発	23.7	40.0	16.6	80.3
侵襲攻撃耐性評価環境の構築	43.1	41.4	17.0	101.6
集積回路解析技術によるＬＳＩ内部動作解析及び先端技術調査	16.9	19.3	0	36.2
統合ハードウェア評価プラットフォームの構築	0	0	16.6	16.6
計	119.8	125.0	61.5	306.3

５－４－Ｃ　費用対効果

開発成果を統合した「統合ハードウェア評価プラットフォーム(SENavigator)」は、暗号モジュール試験認証制度に則った解析手法の実行が可能であり、制度の進歩にも対応できるよう解析手法などを独自に導入できるシステムとなっている。そのため進化への対応に必要となる新たな投資を押さえる事が可能となり、費用対効果は大きい。

製造中止となった標準評価ボート SASEBO-GII は現在も引き合いがあり、後継機種が望まれている。そのため本事業で生まれた評価ボード SAKURA-G の存在意義は大きい。

従来、レーザー照射装置、電磁波照射装置などを利用したフォールト評価環境は単体での販売がなく、サイドチャネル評価環境等と合わせたセキュリティ評価システムの一部として海外などで販売するケースはあるが非常に高価である。本事業の開発成果であるこれらの装置はシンプルな構成となっており、かつ単体での販売を計画しているため、比較的安価で提供することが可能である。

５－５－Ｃ　変化への対応

本調査研究の期間中の変化は、概ね当初予測されていた範囲内であり、計画の変更は不要であった。

２．２　ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築事業）

１－２　事業の目的・政策的位置付け

１－１－２　事業の目的

電力・ガス・ビル等の社会インフラや工場のプラントの「制御システム」は、サイバー攻撃の対象となりづらいとされていた以前の状況から一変し、現在では重大なインシデント源となると考えられている。制御システムの障害は、インフラのサービスレベル低下やプラント操業停止等に直結するため、制御システムのセキュリティ強化やセキュリティ強度の検証が急がれている。

本事業では、制御システムを高セキュア化するための設計方法、セキュリティ検証方法及び第三者による評価認証方法の研究開発、制御システムのセキュリティの国際標準化に係る活動及び被災地における評価認証・普及啓発・人材育成を行うための環境整備に対して補助を実施し、これらを通じて、被災地におけるスマートグリッド導入促進、重要インフラ等のセキュリティ向上、インフラシステムの輸出強化を目的とする。

１－２－２　事業の政策的位置付け

本事業は、「情報セキュリティ２０１２（2012 年７月４日付け情報セキュリティ政策会議決定）」にて、位置づけられている。

＜情報セキュリティ２０１２抜粋＞

平成２４年度中に主たる実施場所を東北地域とし、制御システムのサイバーセキュリティ検証施設を米国の協力を得つつ構築する。また、当該演習施設において、評価・認証手法に関する研究を行い、競争力強化に資する国際標準化を推進する。合わせて、評価・認証機関同士の国際相互承認の実現に向けた取組を促進する。

２－２　研究開発目標

本事業における目標を、下表のように設定する。

表２－１　個別要素技術の目標

要素技術	目標・指標	妥当性・設定理由・根拠等
制御システムのためのサイバーセキュリティテストベッド構築技術	本事業では、制御システムのセキュリティに関する次の活動を行うための施設・設備の構築に関する研究開発を行い、以後の活動に必要な基盤環境を整備する：制御システムを高セキュア化するための設計方法の研究開発、セキュリティ検証方法の研究開発、第三者による評価認証方法の研究開発、及び被災地における評価認証・普及啓発・人材育成。	・世界でも米国のアイダホ国立研究所（Idaho National Laboratory）しか、制御システムのセキュリティ検証施設を保有していなかった。 ・2009～2011年にICS-CERT（米国土安全保障省の下部組織）がインフラ事業者から受けたサイバー攻撃の報告件数が、9件→198件に急増し、重要インフラのセキュリティ強化の緊急性が生じた。 ・被災地における評価認証・普及啓発・人材育成を行うセキュリティテストベッドを構築して、IT障害やサイバー攻撃等の危機に対する減災技術をみやぎ復興パークに集積するという宮城県多賀城市の「減災リサーチパーク構想」に貢献できる。

こうした目標を設定した根拠は次の通りである。

- これまで国内には制御システムを対象とするテストベッドが存在せず、海外環境に依存せざるを得ないことは、我が国の情報セキュリティ確保の上で障害となる恐れがあるほか、国内の制御システム産業の発達の阻害要因となる可能性がある。
- 現在、我が国における制御システムセキュリティに関する技術は確立されておらず、将来のサイバー攻撃による被害が、我が国の重要インフラや製造業に深刻な影響を及ぼすことを防ぐために、我が国の制御システム分野における情報セキュリティ技術を早期に確立していくことが求められている。

３－２　成果、目標の達成度

３－１－２　成果

（１）成果

本事業の主たる成果は次の通りである。

- 制御システムにおけるサイバーセキュリティ対策の評価・認証を行うための設備として、国内唯一のサイバーセキュリティテストベッド施設（愛称：CSS-Base6）を宮城県多賀城市のみやぎ復興パーク内に構築した（平成 25 年 5 月 28 日）。この運営主体として、制御システムセキュリティセンター（CSSC）は同施設に「東北多賀城本部」を設置した。
- 産業用制御システムの特徴的な機能を模擬システムとして実現するための研究開発を行い、その成果をもとに次の５種の模擬プラントシステムを CSS-Base6 に設置した。
  ① 化学
  ② スマートシティ（広域制御）
  ③ ビル制御
  ④ 組立
  ⑤ 下水・排水
- サイバー攻撃によって発生したインシデントの再現、電力・ガス等インフラ事業者向けのサイバー演習及び制御システムのセキュリティの評価・検証が実施できる普及啓発、人材育成及び評価・認証のための基盤環境を整備した。
- 施設の開設から平成 26 年 2 月までの間に、制御システムセキュリティテストベッドを利用した製品は以下の通り。
  - アズビルセキュリティフライデー　ISUACT-V
    特徴：稼働中の制御システムでも安全に着脱できるウィルス検知システムを実装した。
  - マカフィ　McAfee Application Control
    特徴：不正なコードの実行を阻止する機能をリアルタイム性を確保しつつ実現した。
  - トレンドマイクロ　Trend Micro Safe Lock
    特徴：端末内のアプリケーション情報を自動収集し、許可リストを作成

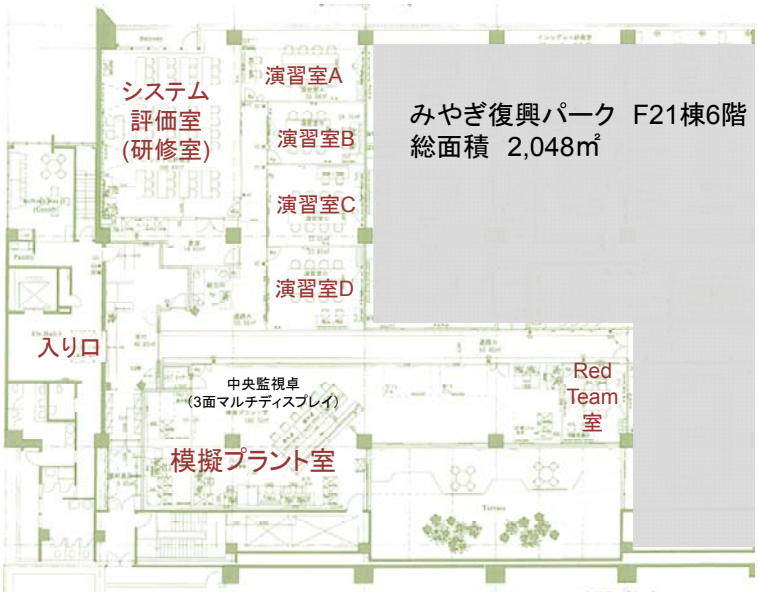


図２－１　サイバーセキュリティテストベッド見取図

①化学プラント

②スマートシティプラント

③ビル制御システム

④組立プラント

⑤下水・排水プラント

図２－２　分野別模擬プラントシステム

（２）特許・論文等の状況

本研究開発に基づく査読付き論文の掲載、特許出願等の次の通りである。

表２－２　特許・論文等件数

論文数	論文の被引用度数	特許等件数（出願を含む）	特許権の実施件数	ライセンス供与数	取得ライセンス料	国際標準への寄与
8	0	0	0	0	0	0

その他のパブリックリターンは次の通りである。

- 受賞： 1 件（情報セキュリティ文化賞）
- メデイアによる報道： 28 件
- 講演： 38 件

３－２－２　目標の達成度

サイバーセキュリティテストベッドが設置され、前述のように本施設を活用した制御システムを対象とする情報セキュリティ対策のための製品開発が実施されており、設定した目標は、次表のように全て達成されたものと判断する。

表２－３　目標に対する成果・達成度の一覧表

要素技術	目標･指標	成果	達成度
制御システムのためのサイバーセキュリティテストベッド構築技術	本事業では、制御システムのセキュリティに関する次の活動を行うための施設･設備の構築に関する研究開発を行い、以後の活動に必要な基盤環境を整備する：制御システムを高セキュア化するための設計方法の研究開発、セキュリティ検証方法の研究開発、第三者による評価認証方法の研究開発、及び被災地における評価認証･普及啓発･人材育成。	･みやぎ復興パーク（多賀城市）に、国内唯一のサイバーセキュリティテストベッド（CSS-Base6）を構築した ･産業用制御システムの特徴的な機能を模擬システムとして実現するための研究開発を行い、５種（化学、スマートシティ、ビル制御、組立、下水･排水）の模擬プラントシステムをCSS-Base6に設置した。 ･インシデントの再現、電力･ガス等インフラ事業者向けのサイバー演習、制御システムのセキュリティの評価･検証が実施できる普及啓発、人材育成及び評価･認証のための環境を整備した。	達成

４－２　事業化、波及効果について

４－１－２　事業化の見通し

本事業では、制御システムのセキュリティに関する施設・設備の構築に関する研究開発を行い、次の活動を行うための基盤環境を整備した：

- 制御システムを高セキュア化するための設計方法の研究開発
- セキュリティ検証方法の研究開発、第三者による評価認証方法の研究開発
- 被災地における評価認証
- 普及啓発・人材育成

技術研究組合制御システムセキュリティセンター（CSSC）は、本事業で構築したサイバーセキュリティテストベッド（CSS-Base6）を設置する「みやぎ復興パーク」内の CSSC 東北多賀城本部に主要な機能を移した。東北多賀城本部では、CSSC-Base6 を活用した研究開発を継続し、組合員の研究成果を活用した製品化が進められている。また、セキュリティの認証に必要な試験装置を CSSC-Base6 施設内に設置し、国際基準に準拠した評価認証の事業化を進めている。普及啓発・人材育成の活動も活発化し、CSS-Base6 の模擬プラントシステムを利用した事業の検討を行っている。

（１）現在までの事業化の状況

- ３－１－２（１）に示したように、サイバーセキュリティテストベッドを利用して開発された３製品（アズビルセキュリティフライデー　ISUACT-V、マカフィ　McAfee Application Control、トレンドマイクロ　Trend Micro Safe Lock）が存在する。ただし各製品の売上高は公表されていない。

（２）今後見込まれる事業化の内容

- 2014 年 4 月に CSSC が、IEC62443 に基づく EDSA 認証業務を開始する見込みである。
- アラクサラ（日立製作所と日本電気の子会社）が工業用ホワイトリストスイッチについて、2015 年度に製品化予定。

（３）事業化に向けての取り組み

- 開設されたサイバーセキュリティテストベッドでは、重要インフラのセキュリティ強化を目的とする以下の活動が平成 25 年度から開始されている。
  - 国際標準化
  - 評価・認証
  - 人材育成
  - 普及啓発

- 制御システムのセキュリティ検証

- CSSC の事業は､｢IT 障害やサイバー攻撃等の危機に対する強靭な情報システム・制御システムのセキュリティに関する技術を、みやぎ復興パークに集積を進める減災技術」として、多賀城市の減災リサーチパーク構想の一つに位置付けられている。
- CSSC では、制御システムを高セキュア化する設計方法、セキュリティ検証方法及び第三者による評価認証方法の研究開発、制御システムのセキュリティの国際標準化等を実施する。具体的には以下の活動が計画されている。
  - ホワイトリスト型対策技術の開発
    サーバや制御端末の記憶装置と本体の間に装着して、制御システム内部からのサイバー攻撃から重要データを防御する、セキュリティバリアデバイス（SBD）を開発する。SBD は、OS の種類を問わず、デバイスドライバー等のソフトウェアをインストールする必要がない利点を有する。今後記憶装置メーカと連携し、装置の小型化に取り組む予定。
  - 制御システム機器のセキュリティの評価・認証
    分野共通的な国産の評価･認証ツールを開発し、我が国初となる制御システムの評価･認証機関を設立する。民間事業者による当技術を通じて、評価･認証機関の自立運営を目指す。現在評価・認証機関のための認定審査中であるが、認定機関(JAB)はすでに米国 ANSI と国際交互承認を締結済みである。

４－２－２　波及効果

サイバーセキュリティテストベッド CSS-Base6 の波及効果は以下の通りである。

- CSS-Base6 の開所以来、現在までに見学者は 800 人を超え、マスコミ取材も 10 社を超えた。制御システムのセキュリティに対する社会の認識が高まり、CSSC に加入する事業者数は、設立時の８事業者から２３事業者まで増加した。
- 政府では、重要インフラの領域拡大の議論が進み、情報セキュリティ政策会議が指定する重要インフラ分野は、経済産業省所管の３分野（化学・石油・クレジット）が新たに追加された。
- 電力・ガス・化学・ビル分野の４分野でサイバーセキュリティ演習を、CSSC 東北多賀城本部の模擬プラントを用いて次ページ表の要領にて実施。演習内容や目標は分野毎に異なる。これによる波及効果は次の通り。
  - 模擬プラントを用いた演習を通じて、現場担当者、技術者、関連事業者等が、制御システムにおけるセキュリティ上の脅威を認識するとともに、セキュリティインシデント発生の検知手順や障害対応手順を検証することが可能であるなど、人材育成面での効果が期待できる。

- 経営層から現場レベルに至るセキュリティ対策の必要性が確認されるなど普及啓発効果が期待できる。特に、ガス分野では、セキュリティ対策に関するガイドライン見直しの検討が始まった。

- ビル分野においては、CSSC 組合員である森ビルを中心にビル業界にて対策の機運が高まっている。

表２－４　CSSC 加入事業者一覧（平成 26 年 3 月現在 23 事業者）

アズビル株式会社	一般財団法人日本品質保証機構
NRI セキュアテクノロジーズ株式会社	株式会社日立製作所
NTT コミュニケーションズ株式会社	富士通株式会社
オムロン株式会社	富士電機株式会社
独立行政法人産業技術総合研究所	マカフィー株式会社
独立行政法人情報処理推進機構	三菱重工業株式会社
国立大学法人電気通信大学	株式会社三菱総合研究所
株式会社東芝	三菱電機株式会社
東北インフォメーション・システムズ株式会社	森ビル株式会社
株式会社トヨタ IT 開発センター	横河電機株式会社
トレンドマイクロ株式会社	株式会社ラック
日本電気株式会社	（事業者名五十音順）

表２－５　各分野におけるサイバーセキュリティ演習の実施状況（平成 25 年度）

電力	実際に発生しているセキュリティインシデントを模擬体験。電力事業者とベンダが参加して、3/6-7 に実施。
ガス	インシデント対応演習と最新対策技術の体験。参加者多数のため2回に分割実施。ガス事業者とベンダが参加して、1/21-22（1 回目）、2/24-25(2回目)に実施。
ビル	攻撃・守備型の実践的演習と最新対策技術の体験。ビル事業者と計装事業者が参加して、1/29 に実施。
化学	インシデント体験が主。3/4 に実施。

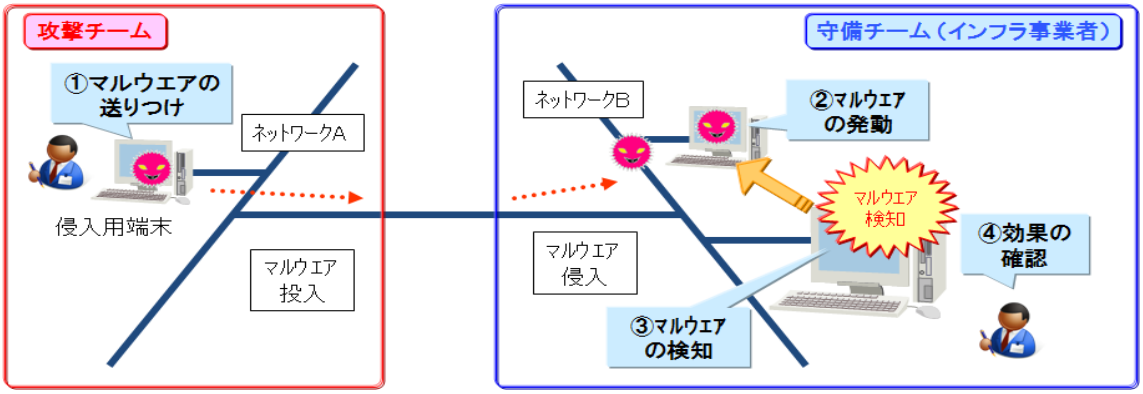


図２－３　サイバーセキュリティ演習の概要


政治の現場
見えない戦争
10
アジア唯一 ティアー1活用を
サイバー攻撃に立ち向かうには
基大な被害をもたらす脅威であると認識する
国際的なルール作りを急ぐ
インフラなどが攻撃された場合の対応を検討しておく
民間企業
重要インフラ
国家
サイバー攻撃
（犯罪から武力攻撃に等しいものまで多様）

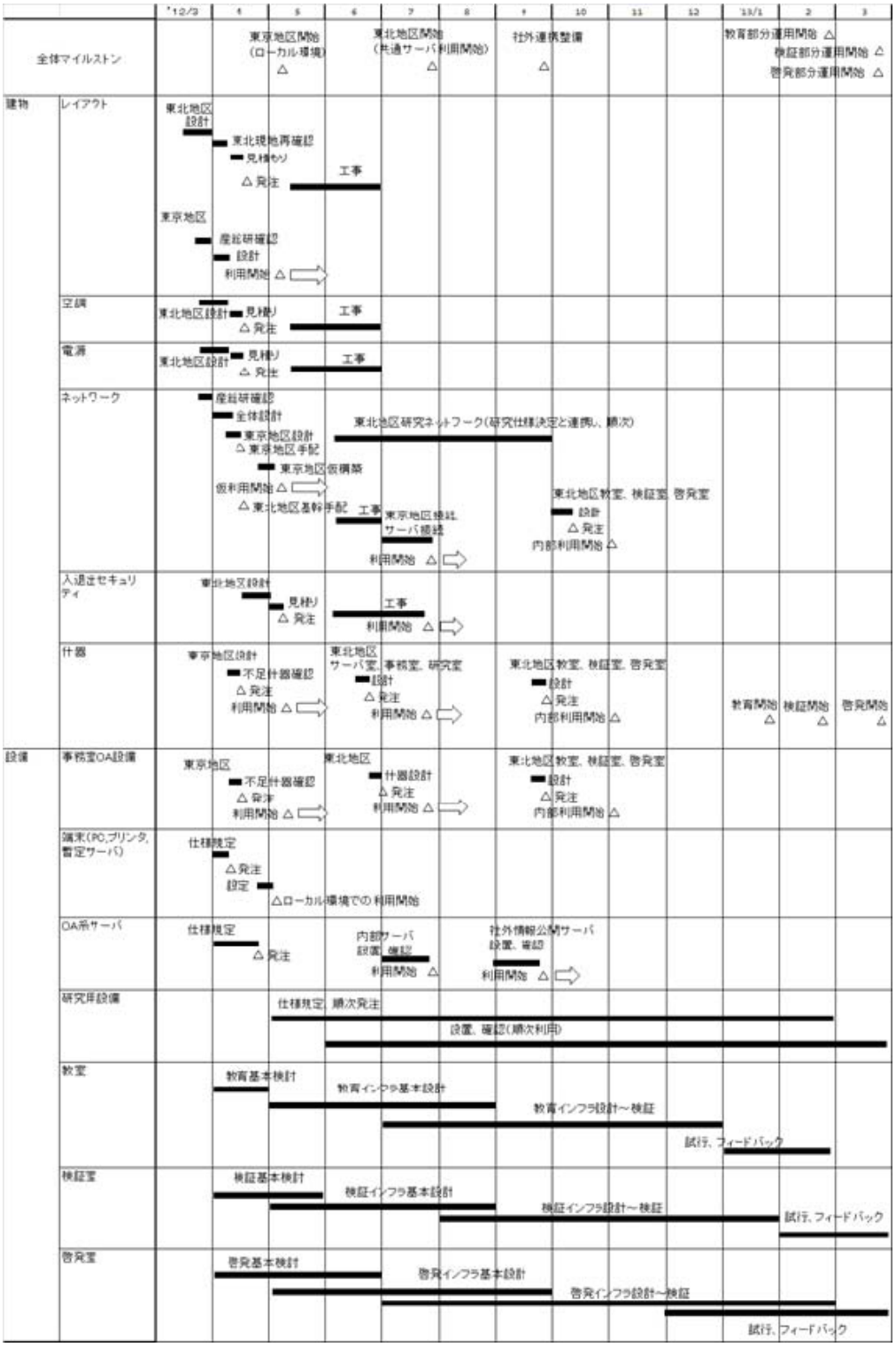
図２－４　新聞報道の例
（平成２５年１月２９日（水）　読売新聞　朝刊４面（抜粋）
サイバーセキュリティ演習について解説）

５－２　研究開発マネジメント・体制・資金・費用対効果等

５－１－２　研究開発計画

本事業は以下のスケジュールにて実施された。

表２－６　研究開発スケジュール



５－２－２　研究開発実施者の実施体制・運営

本事業は、平成２３年度の補正予算事業として、経済産業省から技術研究組合制御システムセキュリティセンターへの委託により実施されている。

制御ベンダ、建築設計監理業者、ネットワーク構築事業者、事務局から体制を構築し、それぞれ日本を代表する業者を選定した。

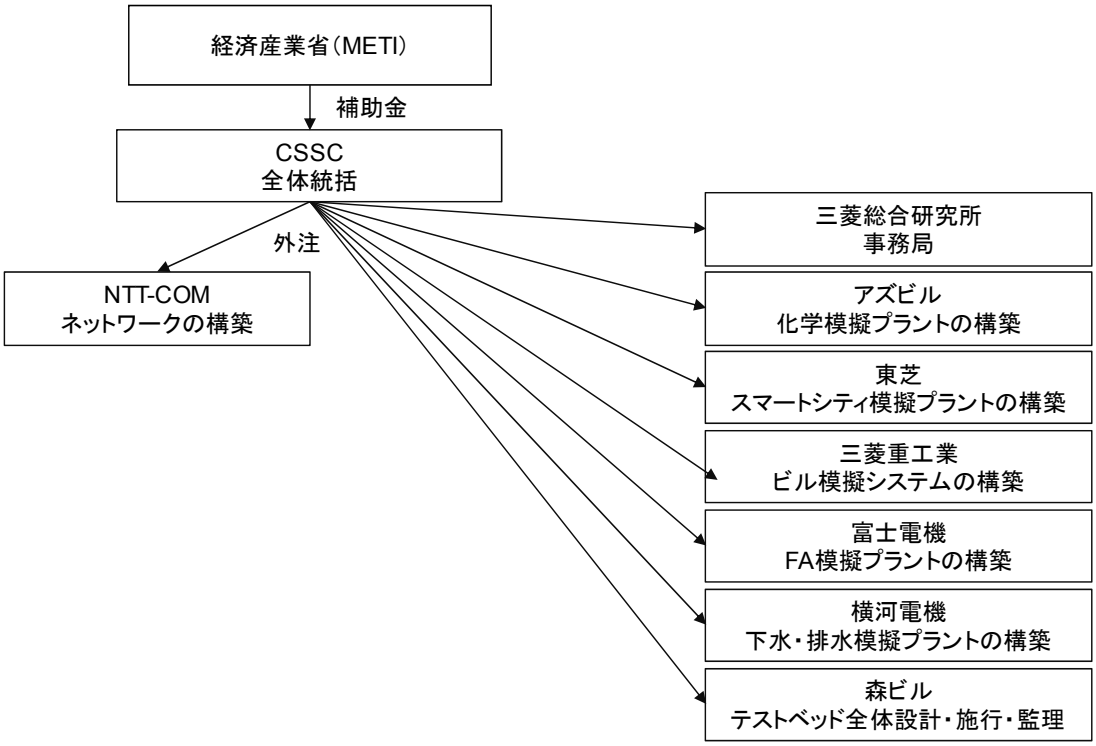


図２－５　研究開発実施体制

５－３－２　資金配分

本事業の資金は下表の通りである。

表２－７　資金配分　　(単位百万円)

年度	23補正	合計
制御システムのためのサイバーセキュリティテストベッド構築技術	2,008	2,008
合計	2,008	2,008

（１）実施計画の目標ごとの資金配分

① 評価認証・国際標準化・人材育成・普及啓発・インシデント分析に利用可能な制御システムセキュリティテストベッドを構築する：1500 百万円

② 制御システムを高セキュア化するための設計方法の研究とセキュリティ検証方法の研究開発を通して、制御システムセキュリティ技術を確立のための基盤を構築する：508 百万円

（２）資金配分に関しての工夫

上記 1)と 2)は共通部分もあり、その部分は支出を一元化し、支出を最適化した。

５－４－２　費用対効果

- サイバーセキュリティテストベッド CSS-Base6 を構築したことにより、制御システムを高セキュア化するための設計方法、セキュリティ検証方法及び第三者による評価認証方法の研究開発、被災地における評価認証・普及啓発・人材育成のための環境が整い、制御システムのセキュリティの研究推進における意義は大きい。
- 制御システムを高セキュア化するための研究基盤としては、平成 25 年度の研究開発を通して、組合員にてホワイトリスト技術の製品化が進められている。
- CSSC は、平成 25 年度において制御機器の評価・認証機関の認定審査中である。
- 組合員の数が、発足時の８者から約３倍（現在２３者）に増加している。

５－５－２　変化への対応

特になし。

第４章　技術に関する施策評価

第４章　技術に関する施策評価

１．施策の目的・政策的位置付けの妥当性

近年クラウドや携帯情報端末の普及が進む一方で、マルウェアの広がりに加え、国境を越えた組織的なサイバー攻撃が増えており、国民生活及び日本経済のセキュリティを確保する観点から、情報セキュリティ対策への需要は近年、非常に高まっている。情報セキュリティ対策は官民が一致協力して対応すべき課題であり、その意味において、中長期的視点に立ち、新たな脅威や既存脅威の巧妙化に対応するための情報セキュリティ技術の研究開発に国が積極的に関わることは極めて重要である。

こうした中、当該事業の目的及び政策的位置付けは、「第 2 次情報セキュリティ基本計画」、「国民を守る情報セキュリティ戦略」に基づき、施策の目的、技術的課題を具体的に整理した上で実施され、さらに社会的ニーズへ適合していることから妥当である。

なお、施策の目的を定める際には、産業・企業の情報セキュリティに関する技術的課題を総合的に検討し、中長期的な「情報セキュリティ研究開発戦略」を構築した上で、事業化に配慮した戦略的な研究開発として推進することが望ましい。また、公募案件として施策を実施していく場合、セキュリティ技術研究開発のポートフォリオを十分意識して、公募案件を設定すべきである。さらに、情報セキュリティ対策は各省庁横断的に重要な課題となっており、今後は各省庁連携のもとに有機的に機能する施策を共同して構築していくべきである。

【肯定的意見】

・中長期的視点に立って、新たな脅威や既存脅威の巧妙化に対応するための情報セキュリティ技術の研究開発が実施された点は、妥当である。
・「第 2 次情報セキュリティ基本計画」、「国民を守る情報セキュリティ戦略」に基づいて実施されており、戦略的な推進の観点から改善すべき点があるが、概ね妥当と考えられる。
・施策の目的、技術的課題が具体的に整理されていること、及び社会的ニーズへ適合していることから妥当である。
・クラウドや携帯情報端末の普及により、情報セキュリティ対策への需要は近年、非常に高まっており、施策の目的は妥当である。
・目的は妥当である。

・中長期計画である「国民を守る情報セキュリティ戦略」などとの関係が明確であり、妥当である。
・技術に関する施策である「技術的情報セキュリティ対策の推進」及び「IT 融合によ

る新産業創出のための研究開発事業」は、情報セキュリティ政策である「情報セキュリティ対策の推進」の主要項目として位置づけられており、政策的位置付けは妥当である。
・情報セキュリティ戦略にそった施策であり、政策的位置付けは妥当である。
・マルウェアの広がりに加え、最近は国境を越えた組織的なサイバー攻撃が増えており、情報セキュリティ戦略として、こうした分野に焦点を当てることは極めて有意義である。

・ハイリスクな研究開発、国際競争力の向上、国内初の認証機関の確立など、国として必要な技術開発、環境整備、標準化などを牽引しており、妥当である。
・情報セキュリティ対策は官民が一致協力して対応すべき課題であり、その意味において国が積極的に関わることは極めて重要である。
・（１B）（２）のように、我が国がグローバルに通用する認証機関作りにつながるものは、国の施策として担うべきテーマとして相応しい。認証機関のオペレーションが軌道に乗るように、継続した支援があるべきものと考えます。
・「技術的情報セキュリティ対策の推進」、「IT 融合による新産業創出のための研究開発事業」は、国民生活及び日本経済のセキュリティを確保する観点から、国の関与が必要であり、国の施策として妥当である。
・情報セキュリティ対策の推進に関する施策として位置付けられ、施策として妥当である。また、各施策は標準化や規格化等の推進を目指すものであり、国の関与が必要とされる施策である。

【問題点・改善すべき点】
・公募案件として施策を実施していく場合、セキュリティ技術研究開発のポートフォリオを十分意識して、公募案件を設定すべきである。
・産業・企業の情報セキュリティに関する技術的課題を総合的に検討し、中長期的な「情報セキュリティ研究開発戦略」を構築し、戦略的に情報セキュリティ関連の研究開発を推進する必要がある。
・情報セキュリティ対策は各省庁横断的に重要な課題となっており、今後は各省庁連携のもとに有機的に機能する施策を共同して構築していくべきである。

・公募案件として施策を実施していく場合、ある分野の技術開発を中止した際などは追加公募などを検討すべきである。
・新世代情報セキュリティ研究開発事業のプロジェクト数の拡大、委託金額規模の多様化（数億円規模の事業を可能とする等）を検討すべきである。

・公募案件として施策を実施していく場合、事業化に対する配慮をすべきである。特に、開発メンバー構成に関しては、産官学の連携を誘導すべきである。

・国の関与は極めて重要であり、さらに各省庁のさらなる協力が求められる。

２．施策の構造及び目的実現見通しの妥当性

本施策に配置された技術に関する事業は、施策の構造から必要なプロジェクトであり、スケジュール等も妥当である。また、各事業の技術開発のフェーズが異なるが、それぞれのフェーズにおいて妥当な成果が得られ、目標が達成されていることから、一定の成果を上げていると評価できる。

なお、中間審査で成果があがっていない事業を中止した点は高く評価できる一方で、セキュリティ脅威に対する技術開発のポートフォリオに配慮することが望まれる。民間におけるクラウド技術開発は低コスト化競争にならざるを得ないため、国の事業として高信頼でセキュアなクラウド技術開発を進めるべきである。また、プロジェクトの配置に際しては、それぞれの事業ごとに PDCA サイクルを回し、全プロジェクトの中で適切なポートフォリオが描けているか、さらに注視する必要がある。

【肯定的意見】

・クラウド関連のセキュリティ技術開発に遅れが生じているが、概ね妥当である。
・各事業は、技術開発のフェーズが異なるが、それぞれのフェーズにおいて妥当な成果が得られている。
・「技術的情報セキュリティ対策の推進」及び「IT 融合による新産業創出のための研究開発事業」から得られた成果は妥当と思われる。
・各事業において、目標が達成されていることから、得られた成果は妥当である。
・一定の成果は上げていると評価できる。

・中間審査で成果があがっていない事業を中止した点は高く評価できる一方で、補完すべき新しい事業も採択すべきであった。
・現行の制度・予算では、技術に関する事業（プロジェクト等）が適切に配置されている。
・配置された技術に関する事業は、施策の構造から必要なプロジェクトであり、スケジュール等も妥当である。
・プロジェクトの配置については、それぞれの事業ごとに PDCA サイクルをきちっと回し、全プロジェクトの中で適切なポートフォリオが描けているか、さらに注視する必要がある。

【問題点・改善すべき点】

・新しい分野におけるセキュリティ脅威に対する技術開発のポートフォリオを強く意識すべきである。
・すでに上記に述べた通り、PDCA サイクルの強化を図るべきである。

・全プロジェクトのポートフォリオをさらに明確にしてほしい。

・クラウド関連のセキュリティ技術開発の事業を補完すべきであった。
・（１A）のクラウドのセキュア化に向けた技術開発は我が国として大変重要である。今回、事業が縮小されたことは大変残念である。民間におけるクラウド技術開発は低コスト化競争にならざるを得ないため、国の事業として高信頼でセキュアなクラウド技術開発を進めるべきである。
・関連する技術項目(1Aa, 1C)などは、計画の途中でも、目標の統合など、陽な連携を推進すべきである。
・産業・企業の情報セキュリティ対策は極めて重要であり、技術的課題に対応する中長期的な「情報セキュリティ研究開発戦略」を構築し、必要な制度・予算を確保し、戦略的に情報セキュリティ関連の研究開発を推進することが望まれる。

３．総合評価

中長期計画である「国民を守る情報セキュリティ戦略」などとの関係が明確であり、いずれの事業も重要な課題に取り組んでいる上に、認証機関の実現や普及に向けた活動のように、国の施策として価値ある波及効果も得られるなど、目的実現の見通しもあり、妥当であると評価する。

なお、施策の構造及び技術に関する事業の配置の検討に際しては、日本の状況から必要な研究開発かのポートフォリオをより明確にするともに、他の関係機関や産官学の連携を意識したものとすべきである、また、認証機関に関わるものや、サイバーセキュリティテストベッドについては、構築だけでなくオペレーションについても支援すべきである。

【肯定的意見】

・総合的には、中長期計画である「国民を守る情報セキュリティ戦略」などとの関係が明確であり、概ね妥当である。
・情報セキュリティ対策に向けての技術開発や技術評価は引き続き力を入れていくべきである。
・いずれの事業も重要な課題に取り組んでおり、認証機関に向けた活動など、国の施策として価値ある波及効果も得られている。
・技術に関する施策について、目的、施策の政策的位置付け、国の施策として、妥当と考えられる。
・各施策は目的、政策的位置付け、目的の実現性の見通しがあり、妥当であると評価する。

【問題点・改善すべき点】

・公募案件として、技術開発を実施していく際には、技術開発のポートフォリオをより明確にする点と産官学の連携を意識した施策とすべきである。
・情報セキュリティ対策における技術研究については、警察庁も新たな組織を発足するところであり、技術リソースの有効活用を図る意味でも、外部との連携をもっと行うべきである。
・クラウドコンピューティングのセキュリティ対策など、重要なものについて、再度取り組むべきである。
・認証機関に関わるものや、サイバーセキュリティテストベッドについては、構築だけでなくオペレーションについても支援すべきである。
・施策の構造及び技術に関する事業の配置については、日本の状況から必要な研究開発が推進されている根拠が不明である。
・産業・企業の情報セキュリティ対策は極めて重要であり、技術的課題に対応する中長期的な「情報セキュリティ研究開発戦略」を構築し、必要な制度・予算を確保し、

戦略的に情報セキュリティ関連の研究開発を推進することが望まれる。

第５章　技術に関する事業評価

第５章　技術に関する事業評価

(1) 技術的情報セキュリティ対策推進事業
Ａ　新世代情報セキュリティ研究開発事業
（総合評価）

中長期的視点に立って、新たな脅威や既存脅威の巧妙化に対応するための情報セキュリティ技術の研究開発が実施され、それぞれが目標を達成し、有用な成果を上げている点は評価できる。 なお、今回はクラウド環境に関するセキュリティ技術開発案件が２つ打ち切りとなったことで、クラウド関連の技術開発がやや遅れる結果となっており、追加の技術開発の公募について検討すべきである。また、公募によるテーマ選定においては、最も優先度の高いセキュリティ課題への取組かどうか、国の施策としての優先度を考慮することが重要である。

【肯定的意見】
・中長期的視点に立って、新たな脅威や既存脅威の巧妙化に対応するための情報セキュリティ技術の研究開発が実施された点
・クラウド、ビッグデータ時代の情報セキュリティは、扱う情報の大きさと、個人のプライバシーに関わる情報を扱うという点で、従来とは異なる次元に来ており、その意味でもさらなる研究開発が必要である。
・実施された各事業は有用な成果を上げている。
Ａ－ａ：ＬＳＩ偽造等の脅威への対策は、重要な課題であり、本研究では電磁界解析システムの構築など成果を上げており評価できる。
Ａ－ｂ：情報家電等非ＰＣ端末における未知脆弱性検出は、昨今の社会環境において重要な課題であり、この脆弱性を評価するシステムを開発したこと等の成果は評価できる。
Ａ－ｃ：クラウドの普及に伴い、個人情報の安全面を考慮した活用は重要な課題である。本研究により、実用化に向けた検討も進められており評価できる。
Ａ－ｄ：撮影による情報漏洩対策のソリューションを開発し、特許出願も行い、成果を上げており評価できる。
Ａ－ｅ：重要課題であるクラウド向け暗号化に関して、鍵管理機能、モデルシステムの構築等の成果を上げており評価できる。
総合的に、各施策において目標達成しており評価できる。
・（1Ad）は挑戦的な取り組みで良い。
・応募案件の進捗状況や成果結果を評価し、１年間だけで２つの事業を打ち切った点

は、評価できる。

【問題点・改善すべき点】
・セキュリティ技術研究開発のポートフォリオを意識して、公募案件を募集すべきである。今回は、結果的にクラウド環境に関するセキュリティ技術開発案件が２つ打ち切りなったため、クラウド関連の技術開発がやや遅れてしまったように感じる。事業を打ち切った場合に、追加の技術開発を公募できないか、検討すべきである。
・中長期的な視点に立っているのであれば、公募時点でサイバーフィジカルシステムに対する新たな脅威やネットワークに接続された車などに対する脅威に関してもセキュリティ技術開発や標準化に対する対応を考慮すべきであった。
・クラウド時代の到来により、最近は海外のデータセンターを活用する例が増えており、セキュリティ対策についても海外ベンダーも視野に入れた対策が必要である。
・いくつかの事業は、当初の目標通りの事業化が進み、素晴しい成果が出ているものの、「撮影による情報漏洩を防止する技術」事業に関しては、一部の事業に関しては、成果とその事業化が今一歩であった。
・クラウドのセキュリティ技術は再度事業としてとりくむべき。
・（1Ac）は、波及効果として取り上げられている活動も含め、重要な課題への取組であるが、基礎技術としての成果と波及効果を狙う事業化体制との間の関係がわかりにくい。
・個々の事業は、企業・個人の情報セキュリティ対策促進にとって有益な成果に結びついているが、今後将来のセキュリティ課題に対処すべき最も優先度の高い課題への取組であったかどうかは再考が必要である。公募と選定段階で、国の施策としての優先度を考慮することが重要である。
・3 年間で 4.1 憶円の予算（委託額）で十分かの検討を行い、より大きな規模の研究開発も推進できるように、抜本的に拡充すべきと思われる。

Ｂ　高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業）

（総合評価）

国民の生活にとって必需品となっているICカード等のIT製品のセキュリティを評価する体制整備が遅れている中、国内外の関係機関と連携し、IC カードのセキュリティ評価に資する技術開発、環境・体制の整備を行い、国内での評価が可能となったことは評価できる。本事業は国際競争戦略の観点から重要な取り組みであり、費用対効果は、関連産業全体の競争力強化へのインパクトから考えるべきである。

なお、本事業で構築した評価環境を持続的に運用するための人材育成方策として、育成した人材の定着と継続的なキャリアサイクルを回すための活動を明確にすることが重要である。

【肯定的意見】

・国民の生活にとって必需品となっているICカード等のIT製品のセキュリティを評価する体制整備が遅れている中、国内外の関係機関と連携し、国内初となる IC カードセキュリティ評価技術の開発と環境整備を実現した点が評価できる。
・国内 IC カードベンダの製品における認証取得が容易になり、国際競争力の向上が期待できる。
・国際競争戦略の観点から重要な取り組みである。費用対効果は、狭く評価すべきではなく、関連産業全体の競争力強化へのインパクトから考えるべきである。
・本事業の成果を基に、システムＬＳＩセキュリティ評価体制が整備されており、目的を達成している。
・ＩＣカードのセキュリティ評価に資する技術開発、環境・体制の整備を行い、国内での評価が可能となったこと、また、共同利用設備の運用、国内ＩＣカードベンダーの認証取得の促進につながり、事業化も進められおり成果を上げている。

【問題点・改善すべき点】

・人材育成に関して、持続可能となるような人材育成プログラムが検討がされていない点。当初の立ち上げ時の要員が異動した場合は、どのように対処されるか明確になっていない。
・人材育成については、関連業界全体として、育成した人材の定着と継続的なキャリアサイクルを回す活動が明確になることが重要である。

C　暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発

本事業は暗号の実装攻撃対策技術として重要な取り組みであり、開発成果を基に「統合ハードウェア評価プラットフォーム」が構築され、設定された開発目標を達成するとともに、実用化に向けた準備が進められていること、及び国内企業等の技術の底上げと国際競争力向上への貢献が期待できる点などから評価できる。

なお、攻撃手法や評価ノウハウの一部は、悪意ある利用につながらないように、適切に管理されるべきものである。事業全体としての管理や運用方針を明確にすべきである。

【肯定的意見】

・設定した目標どおりの成果を達成できている点。特に、製造中止となった標準評価ボード SASEBO-GII の後継器として、SAKURA-G が商品化された点。
・暗号の実装攻撃対策技術として重要な取り組みである。
・開発成果を基に「統合ハードウェア評価プラットフォーム」が構築され、設定された開発目標を達成している。
・暗号アルゴリズムの物理的安全性評価に関する研究開発、及び暗号ハードウエア評価システムへの統合により、ハードウエアセキュリティ評価・認証体制の確立に貢献したことで成果を上げている。
・また、実用化に向けた準備が進められていること、国内企業等の技術の底上げと国際競争力向上への貢献が期待できることも評価できる。

【問題点・改善すべき点】

・事業(1Aa)との目標の統合など、陽な計画の見直しや、事業そのものの統合など、ダイナミックな事業運営が求めらえる。
・攻撃手法や評価ノウハウの一部は、悪意ある利用につながらないように、適切に管理されるべきものである。事業全体としての管理方針や運用が明確になっていたかどうかが課題である。

(2) ＩＴ融合による新産業創出のための研究開発事業（サイバーセキュリティテストベッドの構築事業）

サイバーセキュリティテストベッドの構築により、制御システム系に対するセキュリティ向上を実現するための設計方法、検証方法、第三者による評価認証方法の研究開発、ならびに被災地における評価認証、普及啓発、人材育成を実現した点が評価できる。我が国の制御システムセキュリティ拠点として重要であり、産業インフラや都市インフラを担う制御システムのセキュリティの重要性に対応するタイミングとしても適切である。また、認証機関の見込みがついたことの価値は高い。

なお、制御システムセキュリティの技術や運用体制に関わる人材育成については、更なる取組みが必要である。本センターを活用しながら、関連する企業等と共同で、人材育成を促進できる事業を国の施策として立ち上げるべきである。単年度ではなく、オペレーションの軌道がのるまでの数年は支援すべき事業である。

【肯定的意見】

・制御システム系に対するセキュリティ向上を実現するための設計方法、検証方法、第三者による評価認証方法の研究開発、ならびに被災地における評価認証、普及啓発、人材育成を実現した点が評価できる。
・特に、我が国初となる制御システムの評価・認証機関が確立された点は、タイムリーな施策として評価できる。また、電力分野、ビル分野、化学分野の関係者等が、制御システムのセキュリティ脅威に対するサイバーセキュリティ演習を実施するとともに、その重要性を認識させた点
・組合員数も順調に増加している点
・我が国の制御システムセキュリティ拠点として重要であり、産業インフラや都市インフラを担う制御システムのセキュリティの重要性に対応するタイミングとしても適切である。また、認証機関の見込みがついたことの価値は高い。
・本研究開発の成果を基に構築されたサイバーセキュリティテストベッドを活用して、インフラのセキュリティ強化に関する本格的な活動が実施されている。
・サイバーセキュリティテストベッドの構築により、制御系システムを高セキュア化するための各種研究開発、評価認証と普及開発環境整備を行い、大きな成果を上げている。

【問題点・改善すべき点】

・模擬プラントなどを継続的に更新していく仕組みや継続的な人材育成に対するプログラムが明確でない点
・単年度ではなく、オペレーションの軌道がのるまでの数年は支援すべき事業である。
・本事業の普及啓発と人材育成において、制御システムセキュリティの重要性を啓蒙することについては大いに役立つと思われるが、制御システムセキュリティの技術

や運用体制に関わる人材育成については、更なる取組みが必要である。本センターを活用しながら、関連する企業等と共同で、人材育成を促進できる事業を国の施策として立ち上げるべきである。

第６章　今後の研究開発の方向等に関する提言

第６章　今後の研究開発の方向等に関する提言

【技術に関する施策】

技術開発の事業と、その事業化（例えば認証機関の立ち上げ）など、連携する施策間の関係を明確にした上で、事業の継続性を意識した枠組みを設けるとともに、中長期的な視点からその評価、検証を行うことが重要である。その中で、事業全体としての費用対効果を考えるべきである。

技術に関する施策の実施に際しては、産官学での信頼の輪の確立に配慮することが望ましい。

【各委員の提言】

・技術に関する施策を公募案件で実施する場合、特に、情報セキュリティ技術開発に関しては、産官学間での信頼の輪を確立することが重要であり、申請チームの構成に関しても、配慮すべきである。事業化に関しても、適切なチーム編成を促進するような形の公募とすべきである。
・補正予算によるタイムリーな施策も重要であるが、同時に、継続性を意識した枠組みを当初より検討すべきである。
・技術開発の事業と、その事業化（例えば認証機関の立ち上げ）など、連携する施策間の関係を明確にし、中長期的な視点で評価、検証することが重要である。その中で、関係する技術項目の目標の統合や、技術開発から引き続く事業全体としての費用対効果を考えるべきである。
・さらなるクラウド普及促進のため、クラウド利用者が預けた個人情報等のデータに関して管理監督すること等を可能とする施策は重要であると考える。クラウド利用者が安全にクラウドを利用することに資する施策について、今後の課題とし継続検討されることを期待したい。

【技術に関する事業】

中長期的な視点に立ち、IT 技術の進化を先回りした情報セキュリティ技術の研究開発をめざすべきである。個々の要素技術への取組みではなく、多様な要素技術を基盤として統合する際の技術課題については国の施策として取り組む必要がある。

国際的な開発競争が激しくなってきている IoT (Internet of Things)技術、サイバーフィジカルシステム、連携された重要生活機器（車やスマホ）に対する新たな脅威に関して、根本的な問題解決を目指したセキュリティ技術開発や標準化に対する対応を考慮すべきである。

クラウドコンピューティングの高信頼化、セキュア化は、我が国の競争力強化において重要であり、事業として推進すべきである。特に、ビッグデータ向けのクラウド基盤技術は、そのセキュリティにおいて技術的にも未解決課題が多く、重要な課題である。

【各委員の提言】

・中長期的な視点に立ち、IT 技術の進化を先回りした情報セキュリティ技術の研究開発をめざすべきである。特に、国際的な開発競争が激しくなってきている IoT (Internet of Things)技術、サイバーフィジカルシステム、連携された重要生活機器（車やスマホ）に対する新たな脅威に関しても、根本的な問題解決をめざしたセキュリティ技術開発や標準化に対する対応を考慮すべきである。
・クラウドコンピューティングの高信頼化、セキュア化は、我が国の競争力強化において重要であり、事業として推進すべきである。民間では、低価格化競争にとらわれがちであり、国の施策として高信頼化、セキュア化が必要と考える。特に、ビッグデータ向けのクラウド基盤技術は、そのセキュリティにおいて技術的にも未解決課題が多く、重要な課題である。個々の要素技術への取組みではなく、多様な要素技術を基盤として統合する際の技術課題については国の施策として取り組むべきである。

第７章　評点法による評点結果

第７章　評点法による評点結果

「情報セキュリティ分野に係る施策・事業」に係る評価の実施に併せて、以下に基づき、本評価検討会委員による「評点法による評価」を実施した。その結果、「３．評点結果」のとおりである。

１．趣　旨

評点法による評価については、産業技術審議会評価部会の下で平成１１年度に評価を行った研究開発事業（３９プロジェクト）について「試行」を行い、本格的導入の是非について評価部会において検討を行ってきたところである。その結果、第９回評価部会（平成１２年５月１２日開催）において、評価手法としての評点法について、

(1) 数値での提示は評価結果の全体的傾向の把握に有効である、

(2) 個々のプロジェクト毎に評価者は異なっても相対評価はある程度可能である、

との判断がなされ、これを受けて今後のプロジェクト評価において評点法による評価を行っていくことが確認されている。

また、平成２１年３月３１日に改定された「経済産業省技術評価指針」においても、プロジェクト評価の実施に当たって、評点法の活用による評価の定量化を行うことが規定されている。

これらを踏まえ、プロジェクトの中間・事後評価においては、

(1) 評価結果をできる限りわかりやすく提示すること、

(2) プロジェクト間の相対評価がある程度可能となるようにすること、

を目的として、評価委員全員による評点法による評価を実施することとする。

本評点法は、各評価委員の概括的な判断に基づき、点数による評価を行うもので、評価報告書を取りまとめる際の議論の参考に供するとともに、それ自体評価報告書を補足する資料とする。

２．評価方法

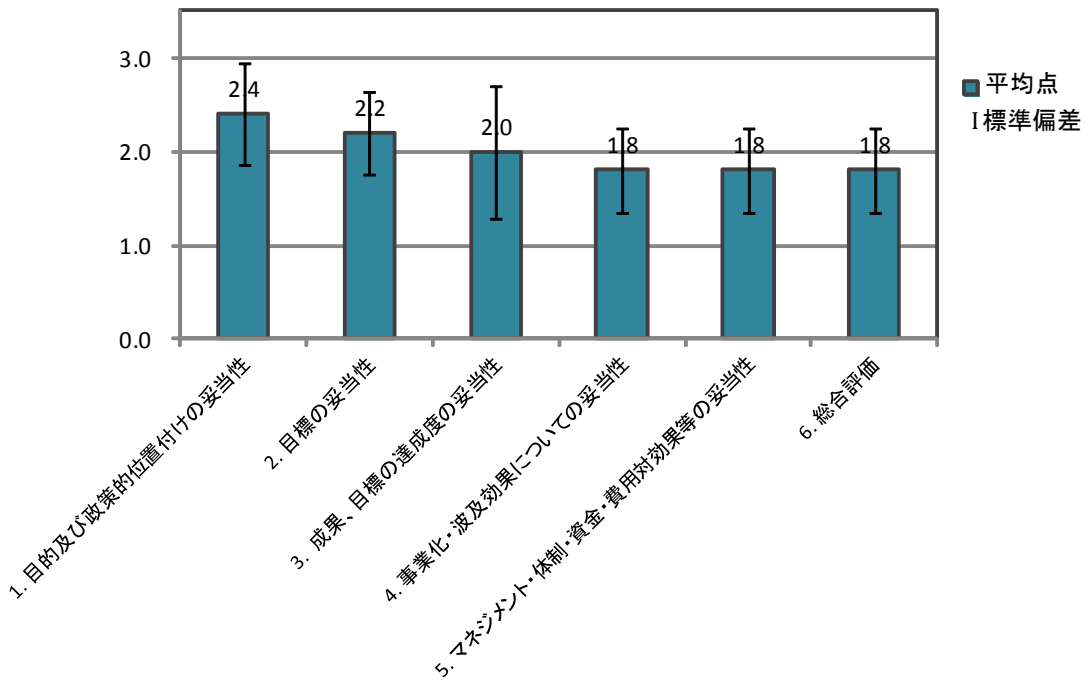
・各項目ごとに４段階（A(優)、B(良)、C(可)、D(不可)<ａ，ｂ，ｃ，ｄも同様>）で評価する。
・４段階はそれぞれ、A(ａ)＝３点、B(ｂ)＝２点、C(ｃ)＝１点、D(ｄ)＝０点に該当する。
・評価シートの記入に際しては、評価シートの《判定基準》に示された基準を参照し、該当と思われる段階に〇を付ける。
・大項目(A, B, C, D)及び小項目(a, b, c, d)は、それぞれ別に評点を付ける。
・総合評価は、各項目の評点とは別に、プロジェクト全体に総合点を付ける。

３．評点結果

（Ａ　新世代情報セキュリティ研究開発事業）

評 点 法 に よ る 評 価 結 果

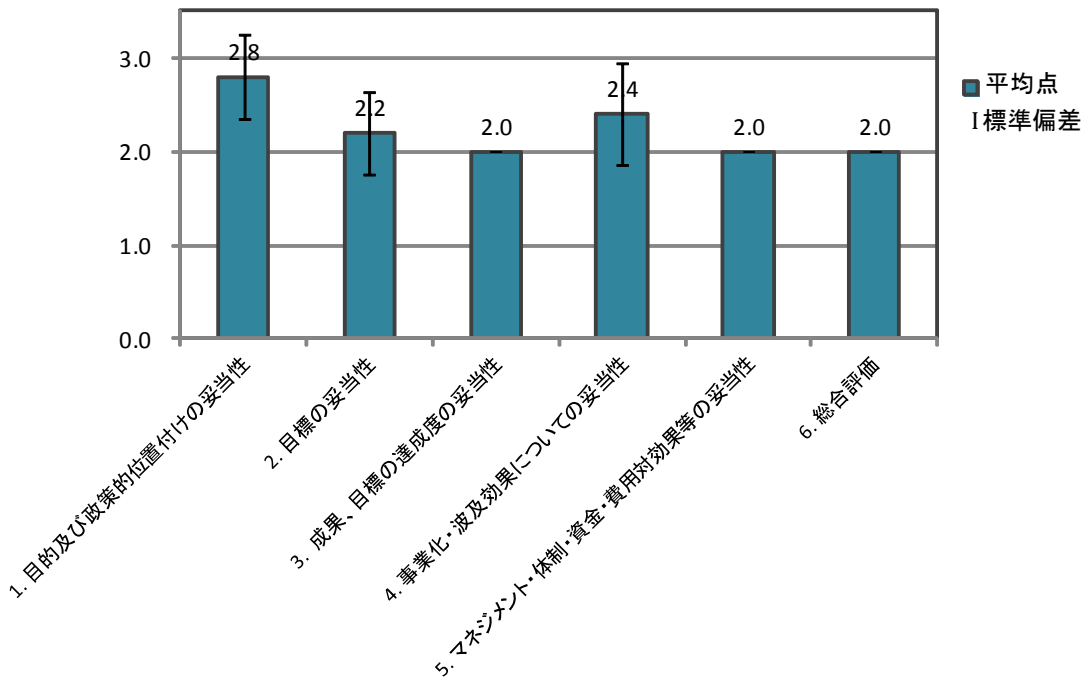
評価項目	平均点	標準偏差
1. 目的及び政策的位置付けの妥当性	2.4	0.55
2. 目標の妥当性	2.2	0.45
3. 成果、目標の達成度の妥当性	2.0	0.71
4. 事業化・波及効果についての妥当性	1.8	0.45
5. マネジメント・体制・資金・費用対効果等の妥当性	1.8	0.45
6. 総合評価	1.8	0.45



（Ｂ　高度大規模半導体集積回路セキュリティ評価技術開発（システムＬＳＩセキュリティ評価体制の整備事業））

評点法による評価結果

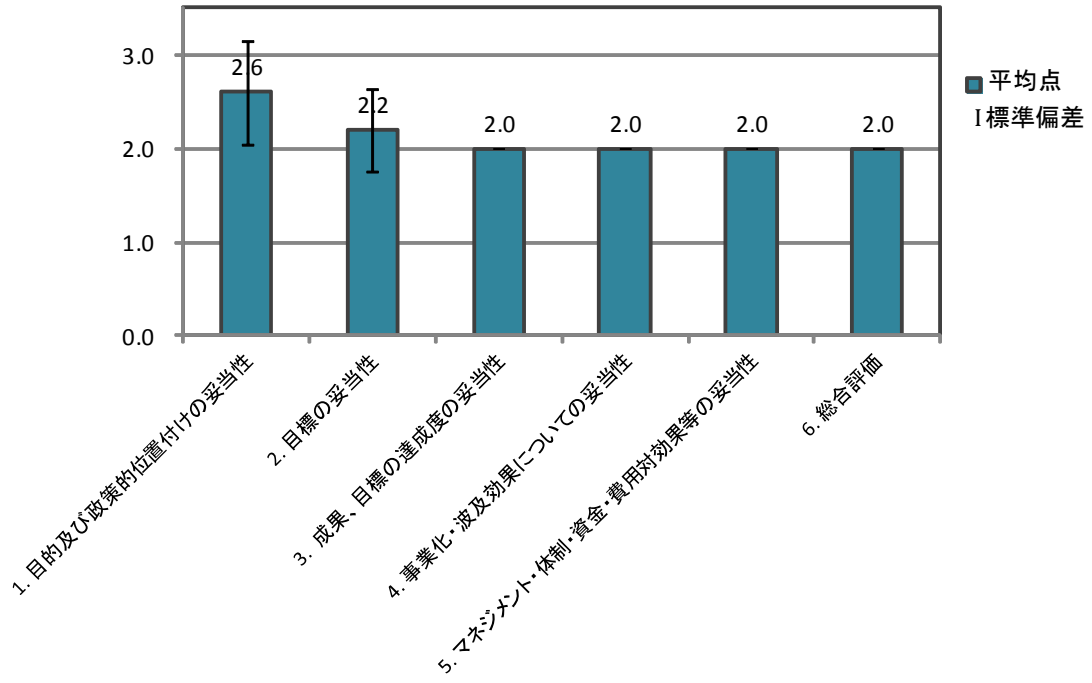
評価項目	平均点	標準偏差
1. 目的及び政策的位置付けの妥当性	2.8	0.45
2. 目標の妥当性	2.2	0.45
3. 成果、目標の達成度の妥当性	2.0	0.00
4. 事業化・波及効果についての妥当性	2.4	0.55
5. マネジメント・体制・資金・費用対効果等の妥当性	2.0	0.00
6. 総合評価	2.0	0.00



（C　暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発）

評 点 法 に よ る 評 価 結 果

評価項目	平均点	標準偏差
1. 目的及び政策的位置付けの妥当性	2.6	0.55
2. 目標の妥当性	2.2	0.45
3.　成果、目標の達成度の妥当性	2.0	0.00
4. 事業化・波及効果についての妥当性	2.0	0.00
5. マネジメント・体制・資金・費用対効果等の妥当性	2.0	0.00
6. 総合評価	2.0	0.00



（D　サイバーセキュリティテストベッドの構築事業）

評 点 法 に よ る 評 価 結 果

評価項目	平均点	標準偏差
1. 目的及び政策的位置付けの妥当性	2.8	0.45
2. 目標の妥当性	2.4	0.55
3.　成果、目標の達成度の妥当性	2.2	0.45
4. 事業化・波及効果についての妥当性	2.6	0.55
5. マネジメント・体制・資金・費用対効果等の妥当性	2.2	0.45
6. 総合評価	2.6	0.55