第2回　情報セキュリティ分野に係る
技術に関する施策・事業評価検討会
資料3

情報セキュリティ分野に係る技術に関する施策・事業の概要について

平成26年3月14日

商務情報政策局

情報セキュリティ政策室

目次

1.1. 施策の目的・政策的位置付け

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。

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の概要

国民を守る情報セキュリティ戦略の概要

平成22年5月情報セキュリティ政策会議決定（議長：官房長官）

現状の課題

大規模なサイバー攻撃事案等の脅威の増大

✓重要インフラ等、国民生活に直結するサービスの情報通信技術への依存による脅威の増大
✓国境を越えたサイバー攻撃が現実化（米韓大規模サイバー攻撃（昨年7月））
✓ガンブラーウイルス等、年々新たなウイルスが出現。攻撃手法も高度化・多様化

社会経済活動の情報通信技術への依存度の増大

✓情報家電、電子タグなどあらゆる機器がネットワークに接続
✓約8割の国民が情報セキュリティに不安感

急速な技術革新の進展

✓クラウド・コンピューティング技術、IPv6への移行
✓暗号の危殆化につながるコンピュータの能力向上

グローバル化の進展

✓国境を越えた瞬時の情報流通
✓各国の個人情報保護・情報セキュリティ制度の調和

課題に対応する新戦略の必要性

（＊）米国
・サイバースペース政策レビュー（60日レビュー）
・「サイバーセキュリティ調整官」を設置し、国家的取組みを強化
・「2010 Cybersecurity Enhancement Act」（2010年2月）

「国民を守る情報セキュリティ戦略」

国民を守る情報セキュリティ戦略（2010～2013）

第2次基本計画（2009～2011）

（＊）第2次情報セキュリティ基本計画を包含し、今後4年間の重点的な取組み

基本的な考え方（取組みの重点化）

①サイバー攻撃の発生を念頭に置いた政策強化・対処体制整備
②新たな環境変化に対応した政策の確立
③受動的な対策から能動的な対策へ

➢ITリスクを克服し、安全・安心な国民生活を実現
➢サイバー空間の安全保障・危機管理政策の強化と情報通信技術政策の連携
➢安全保障・危機管理及び経済の観点に国民・利用者保護の観点を加えた3軸構造の総合的な政策（特に、国民・利用者の視点を重視した政策の推進）
➢国際連携の強化

安全・安心な国民生活を実現

サイバー空間上の我が国の安全保障・危機管理の確保

情報通信技術の利活用を促進し、我が国の経済成長に寄与

実現すべき成果目標

2020年までに、インターネットや情報システム等の情報通信技術を利用者が活用するにあたっての脆弱性を克服し、全ての国民が情報通信技術を安心して利用できる環境　（高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」を実現

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

具体的な取組

● *強力なリーダシップの下、総合的な政策推進体制を確立し、官民の役割の明確化、官民連携を強化*

1　大規模サイバー攻撃事態への対処態勢の整備等

サイバー攻撃事態への対処態勢の整備

・平時からの対策と事案対処の連携強化

➢**対処態勢の整備**
- ・初動対処態勢の整備
- ・初動対処訓練の実施
- ・官民連携の推進
- ・サイバー攻撃に対する防衛分野での体制強化
- ・サイバー犯罪の取締り　等

➢**平素からの情報収集・共有体制の構築・強化**
- ・対処に資する情報収集・分析・共有体制の強化
- ・諸外国等との情報共有体制の構築・強化

2　新たな環境変化に対応した情報セキュリティ政策の強化

国民生活を守る情報セキュリティ基盤の強化

➢**政府機関等の基盤強化**
- ・各府省の最高情報セキュリティ責任者（CISO）の強化
- ・政府横断的な情報収集・分析システム（GSOC）の強化
- ・政府統一基準の見直し、政府機関情報システムの対策強化
- ・共通番号制に対応した情報セキュリティ対策の検討　等

➢**重要インフラの基盤強化**
- ・分野横断的な官民連携体制の強化
- ・情報共有体制の強化、サービス提供が確保できるシステム等の検討
- ・事業継続計画（BCP）の充実　等

➢**その他の基盤強化**
- ・マルウェア対策の充実・強化
- ・クラウド化、IPv6に対応した情報セキュリティ確保方策
- ・中小企業に対する情報セキュリティ対策支援
- ・医療、教育分野等における情報セキュリティ確保方策　等

国民・利用者保護の強化

➢**普及啓発活動の充実・強化**
- ・情報セキュリティ月間による普及啓発の強化
- ・包括的な普及啓発プログラムの策定

➢**情報セキュリティ安心窓口（仮称）の検討**
- ・地域NPO法人等の支援
- ・国民・利用者からの相談受付窓口の検討

➢**個人情報保護の推進**
- ・プライバシー保護技術の適切な利用促進
- ・個人情報保護に関するガイドラインの見直し
- ・国際的なフレームワークへの対応　等

➢**サイバー犯罪に対する態勢の強化**
- ・犯罪取締りのための基盤整備の推進　等

国際連携の強化

➢**米国、ASEAN、欧州等との連携強化**
- ・日米サイバーセキュリティ会合、日ASEAN情報セキュリティ政策会議等を通じた戦略的連携強化
- ・海外CSIRTの構築支援
- ・新たな二国間関係の構築

➢**APEC、ARF、ITU、MERIDIAN、IWWN等の国際会合を活用した情報共有体制等の強化**
- ・国際会議への積極的な参加を通じた情報共有体制の強化

➢**NISCの窓口機能の強化**
- ・情報セキュリティに関するベストプラクティスの共有等
- ・情報セキュリティ政策について諸外国等と連携強化　等

技術戦略の推進等

➢**情報セキュリティ関連の研究開発の戦略的推進等**
- ・新たな情報セキュリティ研究開発戦略の策定
- ・高度化・多様化する攻撃等に対応できる技術の実現・普及（「グランドチャレンジ型」研究開発の推進）

➢**情報セキュリティ人材の育成**
- ・政府、大学、企業等における高度な情報セキュリティ人材の育成

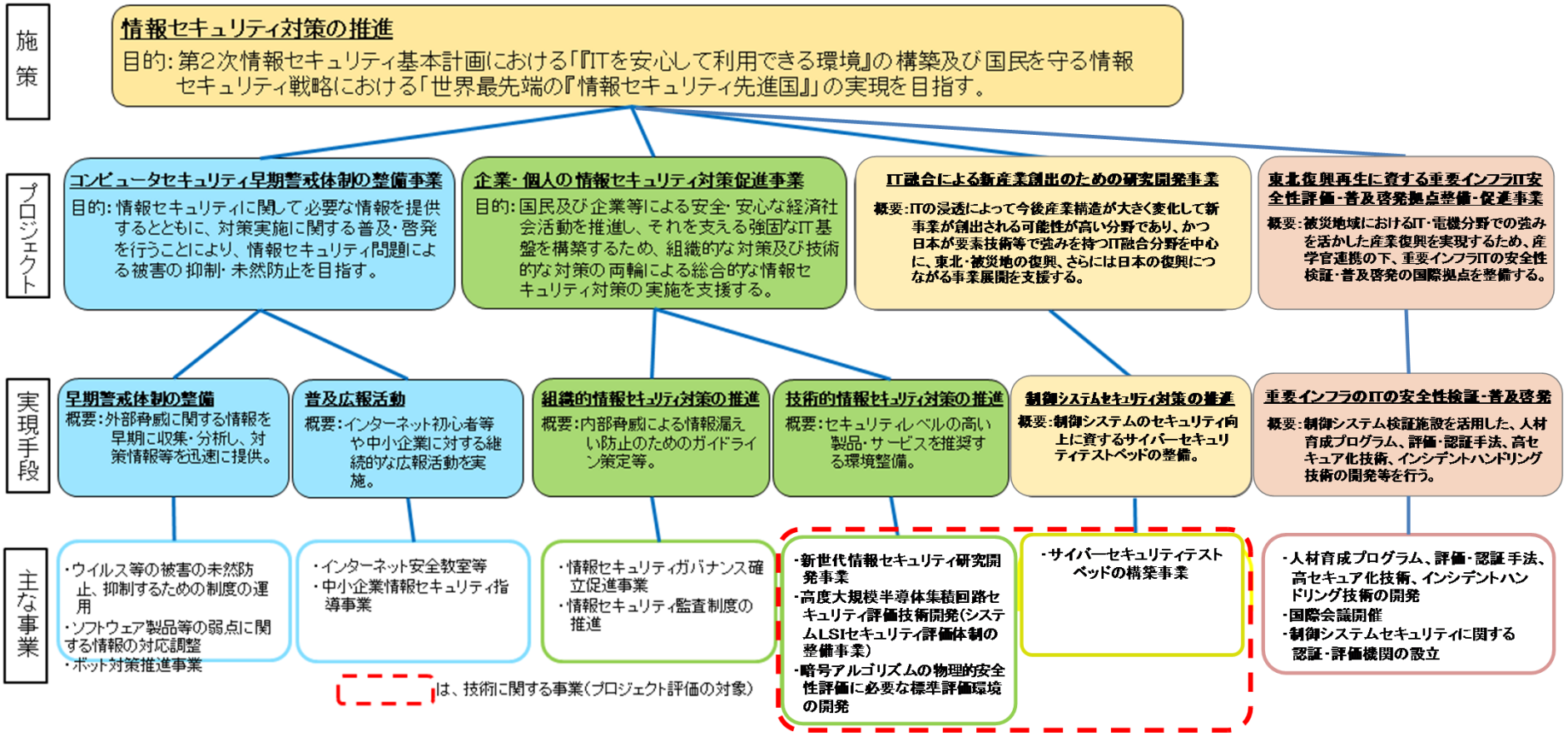
➢**情報セキュリティガバナンスの確立**
- ・情報セキュリティガバナンスの経営としての位置付け
- ・事業継続計画（BCP）の策定、情報セキュリティ監査　等

制度整備

➢**サイバー空間の安全性・信頼性を向上させる制度の検討等**
- ・コンピュータウイルス関連の法改正等サイバー犯罪条約の早期締結に向けた検討
- ・機微な情報へのアクセス権限の明確化の検討　等

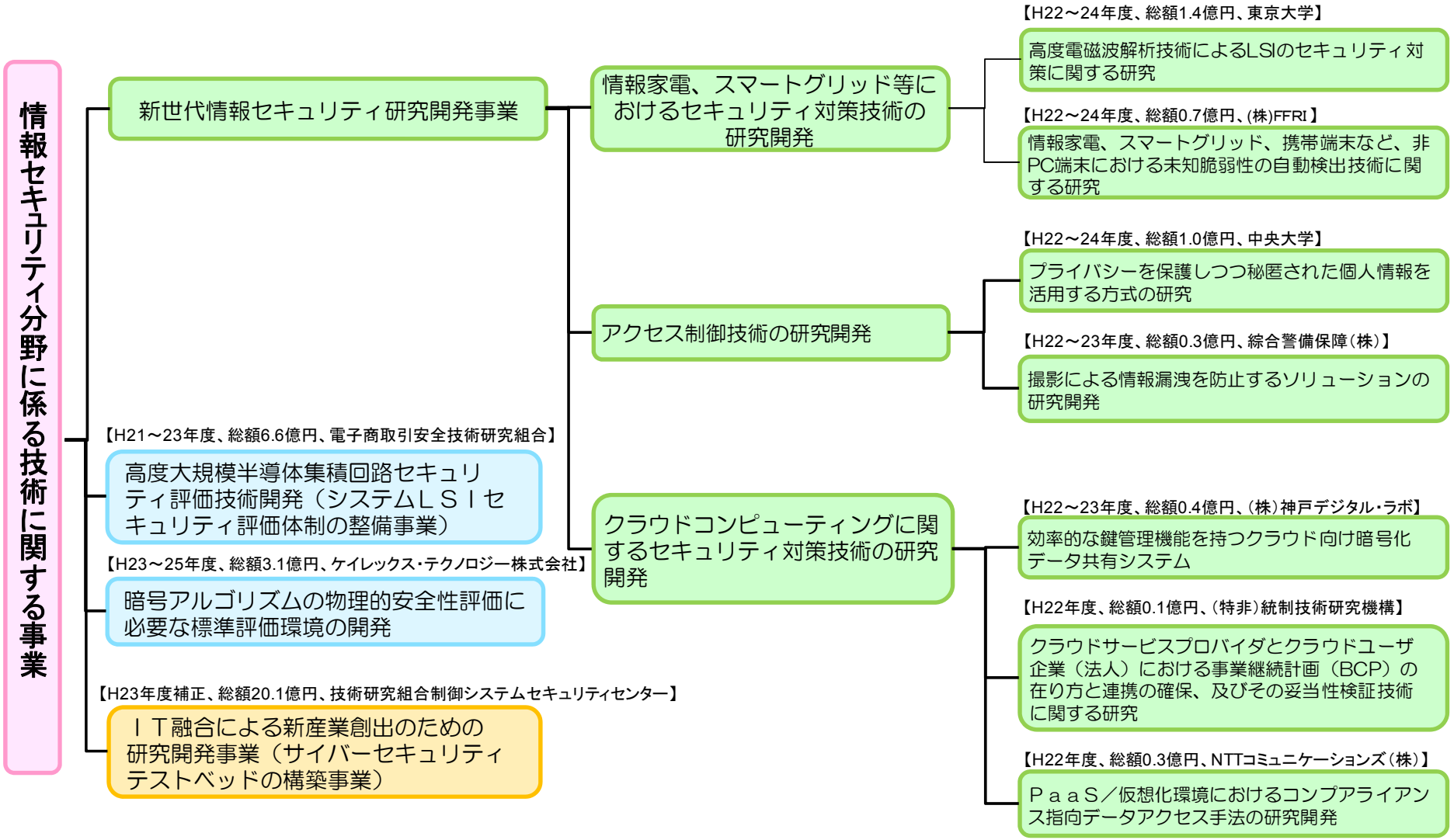
➢**各国の情報セキュリティ制度の比較検討**
- ・各国間の法制度等の相違について分析し、情報セキュリティ関連の国際連携のための課題抽出・連携方策の検討を実施

図1－3　情報セキュリティ対策の体系図

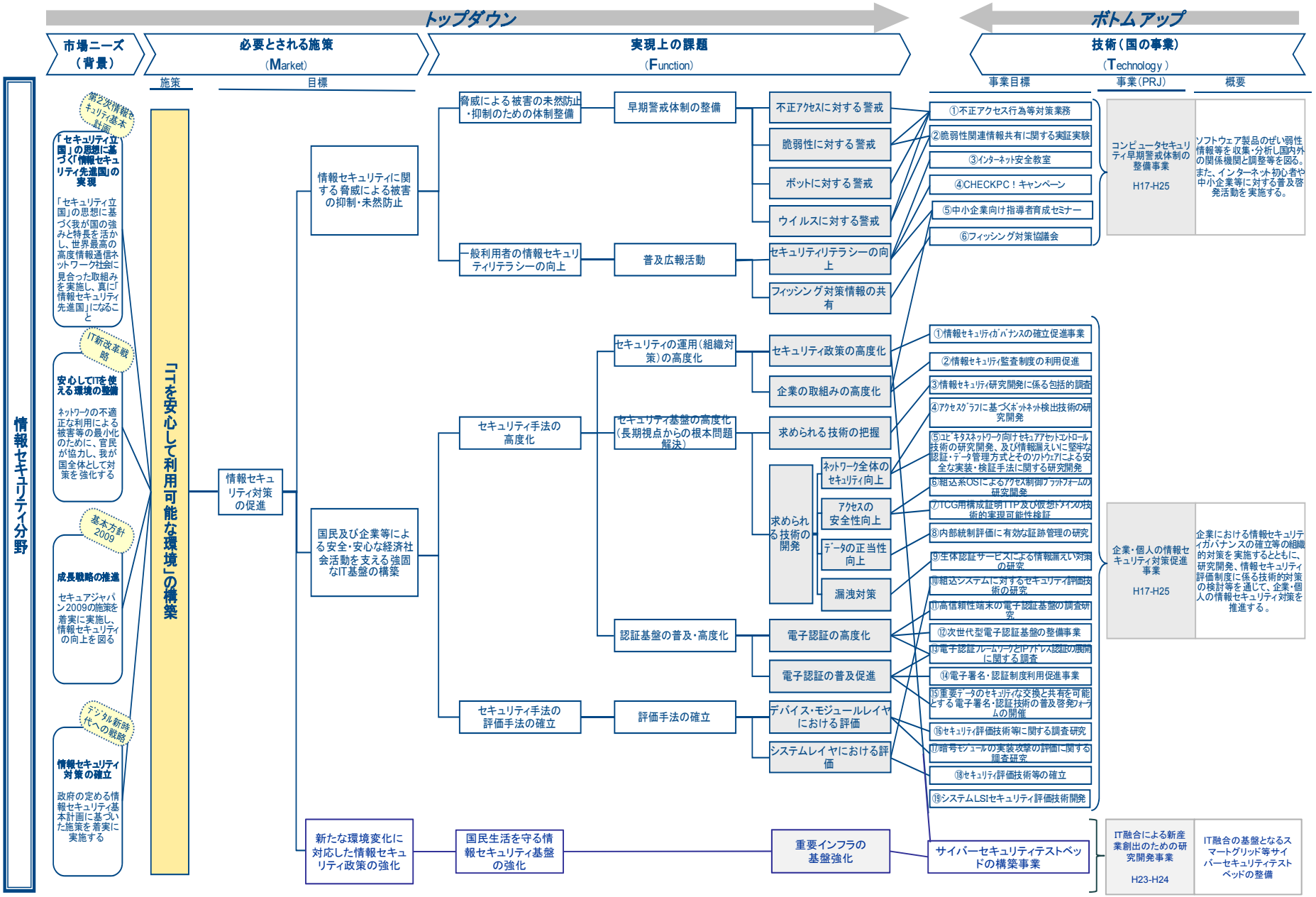


（注）平成24年度より、「コンピュータセキュリティ早期警戒体制の整備事業」と「企業・個人の情報セキュリティ対策促進事業」は統合され、「情報セキュリティ対策推進事業」となった。

図１－４　情報セキュリティ分野に係る技術に関する事業



1.2. 施策の構造


トップダウン
ボトムアップ
市場ニーズ（背景）
必要とされる施策（Market）
実現上の課題（Function）
技術（国の事業）（Technology）
施策
目標
事業目標
事業(PRJ)
概要
情報セキュリティ分野
第2次情報セキュリティ基本計画
「セキュリティ立国」の思想に基づく「情報セキュリティ先進国」の実現
「セキュリティ立国」の思想に基づく我が国の強みと特長を活かし、世界最高の高度情報通信ネットワーク社会に見合った取組みを実施し、真に「情報セキュリティ先進国」になること
IT新改革戦略
安心してITを使える環境の整備
ネットワークの不適正な利用による被害等の最小化のために、官民が協力し、我が国全体として対策を強化する
基本方針2009
成長戦略の推進
セキュアジャパン2009の施策を着実に実施し、情報セキュリティの向上を図る
デジタル新時代への戦略
情報セキュリティ対策の確立
政府の定める情報セキュリティ基本計画に基づいた施策を着実に実施する
「ITを安心して利用可能な環境」の構築
情報セキュリティ対策の促進
情報セキュリティに関する脅威による被害の抑制・未然防止
国民及び企業等による安全・安心な経済社会活動を支える強固なIT基盤の構築
新たな環境変化に対応した情報セキュリティ政策の強化
脅威による被害の未然防止・抑制のための体制整備
一般利用者の情報セキュリティリテラシーの向上
セキュリティ手法の高度化
セキュリティ手法の評価手法の確立
国民生活を守る情報セキュリティ基盤の強化
早期警戒体制の整備
普及広報活動
セキュリティの運用（組織対策）の高度化
セキュリティ基盤の高度化（長期視点からの根本問題解決）
認証基盤の普及・高度化
評価手法の確立
重要インフラの基盤強化
不正ｱｸｾｽに対する警戒
脆弱性に対する警戒
ボットに対する警戒
ウイルスに対する警戒
セキュリティリテラシーの向上
フィッシング対策情報の共有
セキュリティ政策の高度化
企業の取組みの高度化
求められる技術の把握
求められる技術の開発
ネットワーク全体のセキュリティ向上
ｱｸｾｽの安全性向上
ﾃﾞｰﾀの正当性向上
漏洩対策
電子認証の高度化
電子認証の普及促進
デバイス・モジュールレイヤにおける評価
システムレイヤにおける評価
①不正アクセス行為等対策業務
②脆弱性関連情報共有に関する実証実験
③ｲﾝﾀｰﾈｯﾄ安全教室
④CHECKPC！キャンペーン
⑤中小企業向け指導者育成セミナー
⑥フィッシング対策協議会
①情報ｾｷｭﾘﾃｨｶﾞﾊﾞﾅﾝｽの確立促進事業
②情報ｾｷｭﾘﾃｨ監査制度の利用促進
③情報ｾｷｭﾘﾃｨ研究開発に係る包括的調査
④ｱｸｾｽﾛｸﾞﾗﾌに基づくﾎﾞｯﾄﾈｯﾄ検出技術の研究開発
⑤ﾕﾋﾞｷﾀｽﾈｯﾄﾜｰｸ向けｾｷｭｱｱｾｯﾄﾄﾝﾄﾛｰﾙ技術の研究開発、及び情報漏えいに堅牢な認証・ﾃﾞｰﾀ管理方式とそのｿﾌﾄｳｴｱによる安全な実装・検証手法に関する研究開発
⑥組込系OSによるｱｸｾｽ制御ﾌﾟﾗｯﾄﾌｫｰﾑの研究開発
⑦TCG用構成証明TTP及び仮想ﾄﾞﾒｲﾝの技術的実現可能性検証
⑧内部統制評価に有効な証跡管理の研究
⑨生体認証ｻｰﾋﾞｽによる情報漏えい対策の研究
⑩組込システムに対するセキュリティ評価技術の研究
⑪高信頼性端末の電子認証基盤の調査研究
⑫次世代型電子認証基盤の整備事業
⑬電子認証ﾌﾚｰﾑﾜｰｸとIPｱﾄﾞﾚｽ認証の展開に関する調査
⑭電子署名・認証制度利用促進事業
⑮重要ﾃﾞｰﾀのｾｷｭﾘﾃｨな交換と共有を可能とする電子署名・認証技術の普及啓発ﾌｫｰﾗﾑの開催
⑯ｾｷｭﾘﾃｨ評価技術等に関する調査研究
⑰暗号ﾓｼﾞｭｰﾙの実装攻撃の評価に関する調査研究
⑱ｾｷｭﾘﾃｨ評価技術等の確立
⑲システムLSIセキュリティ評価技術開発
サイバーセキュリティテストベッドの構築事業
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
ソフトウェア製品のぜい弱性情報等を収集・分析し国内外の関係機関と調整等を図る。また、インターネット初心者や中小企業等に対する普及啓発活動を実施する。
企業・個人の情報セキュリティ対策促進事業
H17-H25
企業における情報セキュリティガバナンスの確立等の組織的対策を実施するとともに、研究開発、情報セキュリティ評価制度に係る技術的対策の検討等を通じて、企業・個人の情報セキュリティ対策を推進する。
IT融合による新産業創出のための研究開発事業
H23-H24
IT融合の基盤となるスマートグリッド等サイバーセキュリティテストベッドの整備

企業・個人の情報セキュリティ対策促進事業

実施期間：平成１７～２５年度

事業の内容

事業の概要・目的

○国民及び企業等による安全・安心な経済社会活動を推進し、それを支える強固なIT基盤を構築するべく、企業・国民による情報セキュリティ対策の実施を支援する。

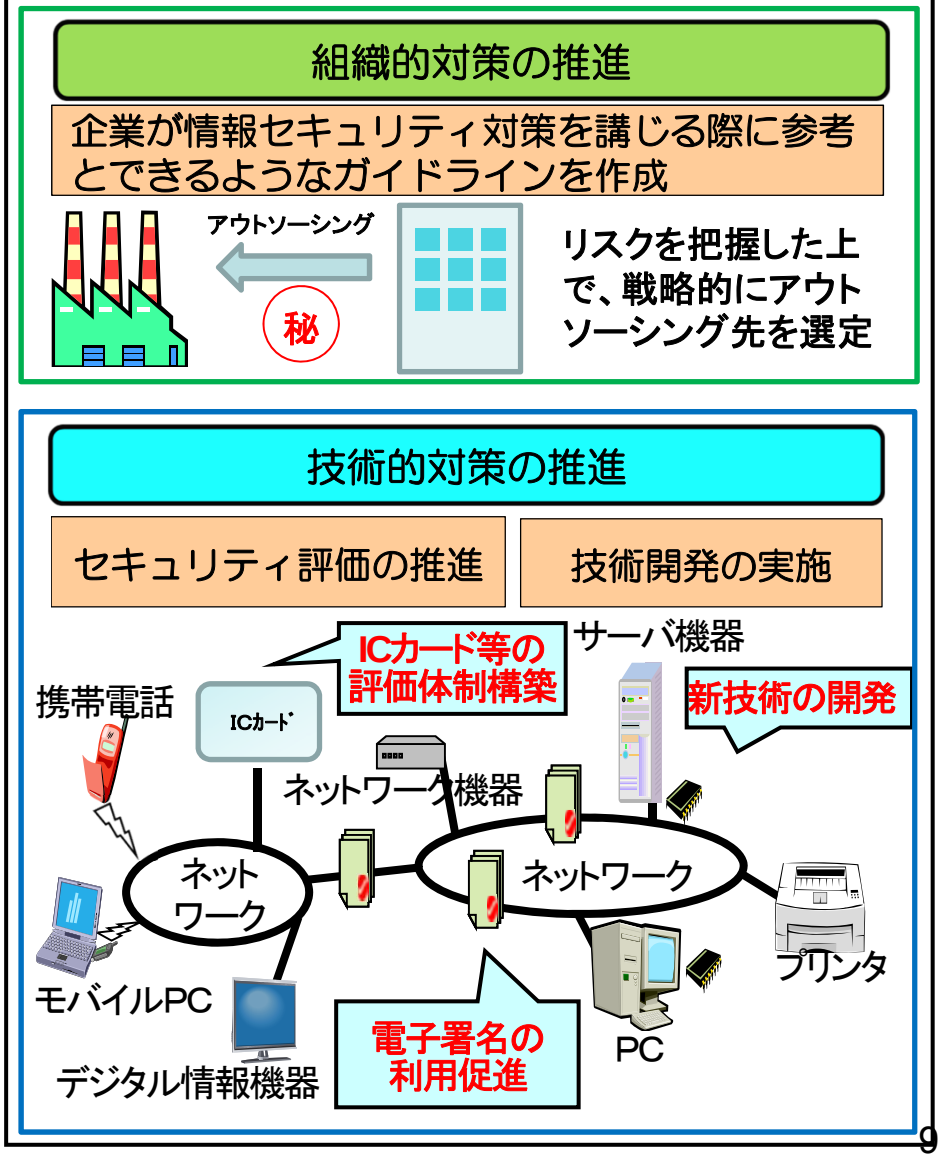
①企業等における技術ノウハウや顧客情報等の漏えいを防止するため、組織マネジメント強化のためのガイドライン等の整備等を行う。

②国民・企業が、情報家電や情報システム等を安心して利用できるように、情報セキュリティに関する革新技術の開発を行うとともに、電子署名法に基づく電子署名制度の運営等を行う。

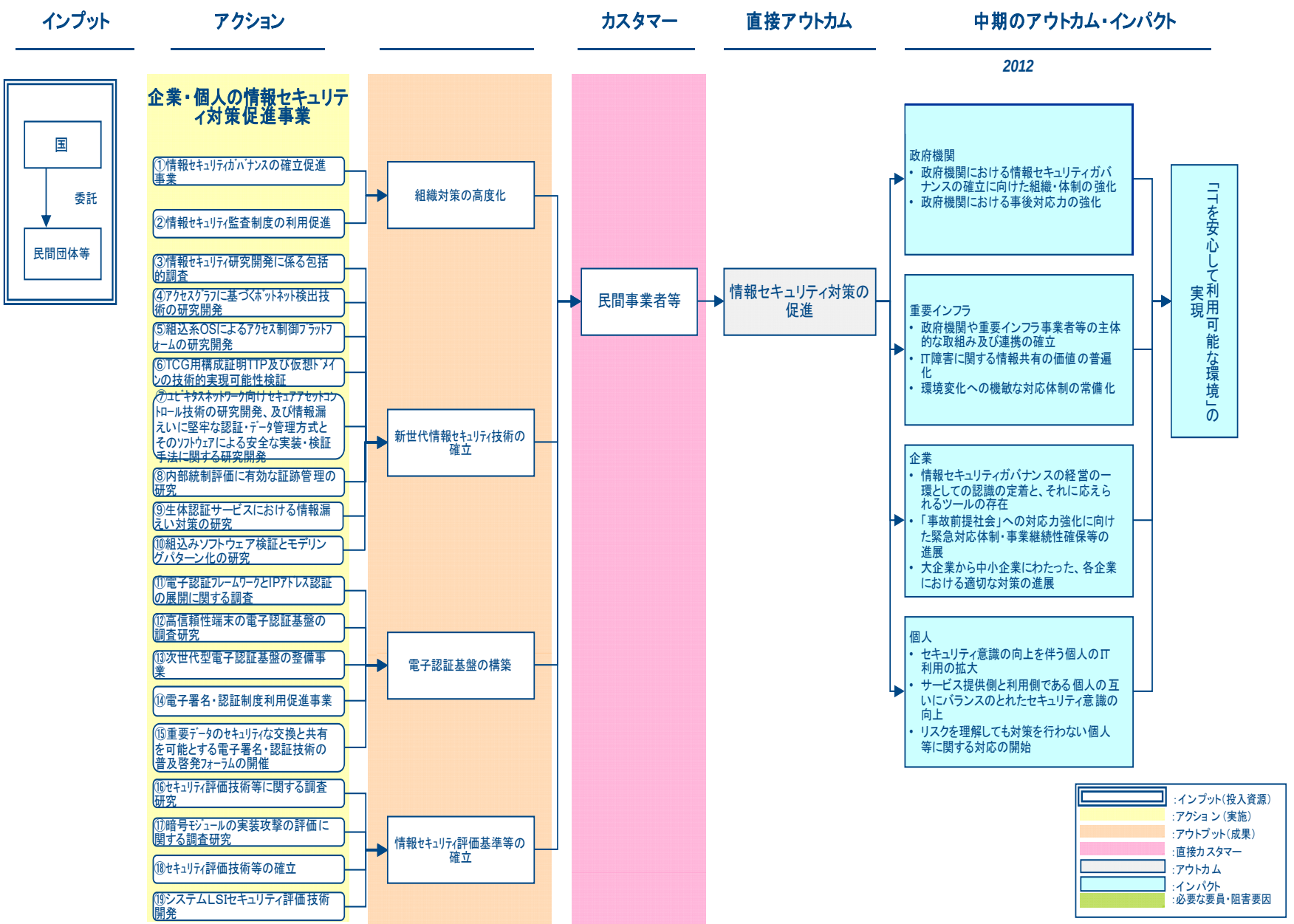
条件（対象者、対象行為、補助率等）

国 → 委託 → 民間企業等

事業イメージ



企業・個人の情報セキュリティ対策促進事業



ＩＴ融合による新産業創出のための研究開発事業

平成２３年度三次補正予算額　３９．７億円

※今回の評価対象である「サイバーセキュリティテストベッドの構築事業」は、本事業の中で実施された

事業の内容

事業の概要・目的

○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（エネルギー、医療・健康、農業、ロボット、自動車・交通等を想定）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します。

○そのために、IT融合分野の研究・システム開発の拠点整備及び拠点整備と一体化した研究・システム開発を補助します。

○研究・システム開発にあたっては、関係企業・団体で最適なコンソーシアムを組成します。

条件（対象者、対象行為、補助率等）

国 → 補助（定額・2／3） → 民間企業等

事業イメージ

分野毎にプロジェクトを推進

異業種・異分野の企業・大学等が連携して開発・実証プロジェクト等を推進

- スマート・ヘルスケア産業（IT×医療・健康）

- スマートアグリシステム（IT×農業）

- 社会システム対応ロボット（IT×ロボット）

- 情報端末化する自動車（IT×自動車・交通）

IT融合の基盤となるスマートグリッド等サイバーセキュリティテストベッドの整備

産学官連携サイバーセキュリティコンソーシアム

↓ 構築

サイバーセキュリティテストベッド（セキュリティ検証施設）

- 重要インフラ等のセキュリティ強化
- インフラ輸出強化
- スマートグリッド導入

2. 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、技術的情報セキュリティ対策推進事業及び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。

（1）技術的情報セキュリティ対策推進事業（旧事業名：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

（2）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

今回の評価対象事業の概要

事業名	期間・費用	概要		代表実施機関	主な成果とアウトカム
(1-A) 新世代情報セキュリティ研究開発事業（第3期抜粋）	H22～H24 4.1億円 （委託）	中長期的視点に立った根本的な問題解決を目指し、情報セキュリティに係る技術の進歩に伴う新たな脅威や既存脅威の巧妙化の変化に対応するための研究開発を行う。	高度電磁波解析技術によるLSIのセキュリティ対策	東京大学	開発した電磁波計測・解析ツールを再委託先で製品化
			情報家電など、非PC端末における未知脆弱性の自動検出技術	株式会社FFRI	情報家電、モバイル端末、スマートメータ向け脆弱性検査ツールの開発、自社利用
			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	中央大学	開発した医療・介護向け個人情報保護・活用モデルの医療機関での利用の働きかけ
			撮影による情報漏洩を防止するソリューション	綜合警備保障株式会社	撮影行為の検知手法を開発し、製品への応用可能性を検討
			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	株式会社神戸デジタル・ラボ	鍵失効機能付き属性ベース暗号方式を開発し、クラウドサービスでの事業化を検討
(1-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）	H21～H23 6.6億円 （委託）	ICカード等のIT製品のセキュリティを評価する体制が国内に存在しない状況を踏まえ、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。		電子商取引安全技術研究組合	ICカード等のハードウェアの物理的安全性を評価するための施設を東京都内に整備し、暗号モジュール試験を含む評価サービスを提供
(1-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	H23～H25 3.1億円 （委託）	暗号アルゴリズムに関するハードウェアの実装性能評価およ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、これをもとにLSI解析技術の進歩を踏まえた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、JCMVP等の暗号モジュール試験認証制度や、ISO/IEC 15408 によるICカード評価等に反映する。		ケイレックス・テクノロジー株式会社	暗号アルゴリズムの実装環境を対象とする物理的安全性を統合的に評価することを目的として、「サイドチャネルおよびフォールト攻撃耐性評価システム」を開発し、これを用いて、物理的な脆弱性に関する分析を実施中
(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）	H23補正 20.1億円 （補助）	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等を研究開発するとともに、これらの研究開発、国際標準化活動及び評価認証等のための施設・設備として、制御システムサイバーセキュリティテストベッドを構築する。		技術研究組合制御システムセキュリティセンター	宮城県多賀城市のみやぎ復興パーク内に実施機関の研究開発拠点を設置し、重要インフラ事業者や関係ベンダを対象に、システムセキュリティ検証、国際規格準拠認証等のサービスを提供

施策の波及効果について

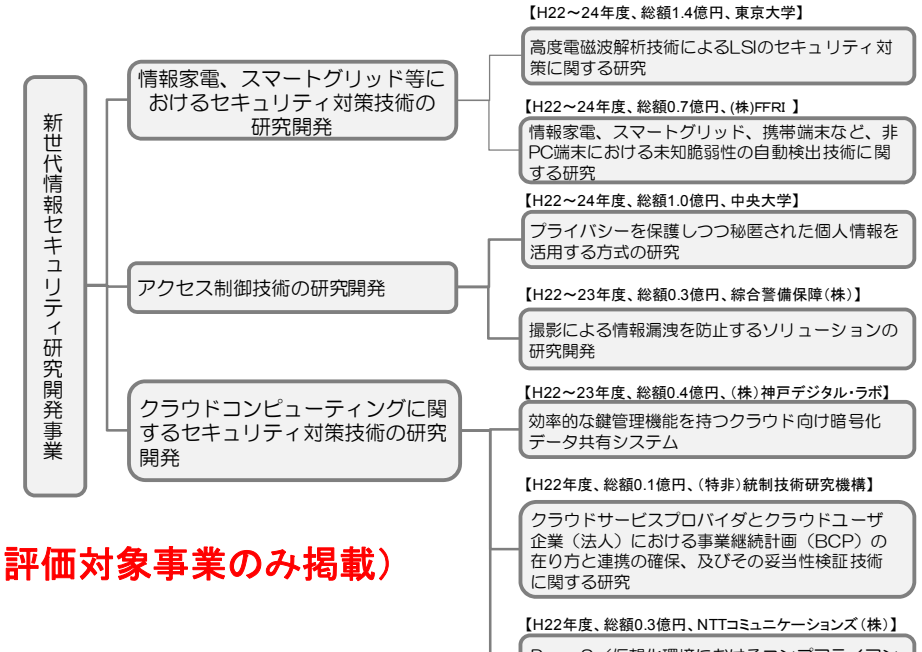
事業名	情報セキュリティ対策への効果	民間産業への波及効果	社会への波及効果
(1-A) 新世代情報セキュリティ研究開発事業（第3期）	• 脆弱性検出能力の向上 • プライバシーの保護の強化 • 情報漏洩機会の減少 • クラウドを安全に利用する手段の増加	• 開発されたユニークな成果に基づく事業化機会の増加	• 国内における情報セキュリティ分野の質の高い研究者の増加による研究開発力の強化
(1-B) 高度大規模半導体集積回路セキュリティ評価技術開発（システムLSIセキュリティ評価体制の整備事業）	• 国内ベンダによる認証取得製品の増加による、ICカード等利用時の物理的脅威の減少	• 国内ベンダ製品における認証取得率の向上による、国際的な製品競争力の向上	• 国内に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
(1-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	• ベンダにおいて簡単に物理的安全性を評価できる環境が普及することによる、コストに影響せずに実現可能な製品安全性向上	• 高度な評価を簡単に行う環境が普及することによる、製造コスト抑制による製品競争力の向上	• 物理的安全性に関する評価経験を有する人材の増加による、国内情報セキュリティ研究開発人材の質の向上
(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）	• 重要インフラ設備に用いられる制御システムの脆弱性検出を通じた、重要インフラシステムの安全性向上	• 高度な脆弱性検出を行う環境を簡単に利用できることによる、国内システムベンダの製品競争力の向上	• 国内重要インフラ設備に用いられているシステムを検査可能な環境を有することによる、新規脆弱性への対応能力向上によるナショナルセキュリティの向上

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

２．１．新世代情報セキュリティ研究開発事業

概　　要	情報技術の進展にともない、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いる。こうした脅威に対応するため、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、研究分野を再設定し、各分野毎に研究開発を行う。
実施期間	平成１７年度～平成２４年度
予算総額	22年度:1.5億円、23年度:1.5億円、24年度：1.1億円
実施体制	

２．１．事業の目的・政策的位置付け

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、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。

このため、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技術開発を行うことにより、安心・安全な国民生活の実現を目指す。

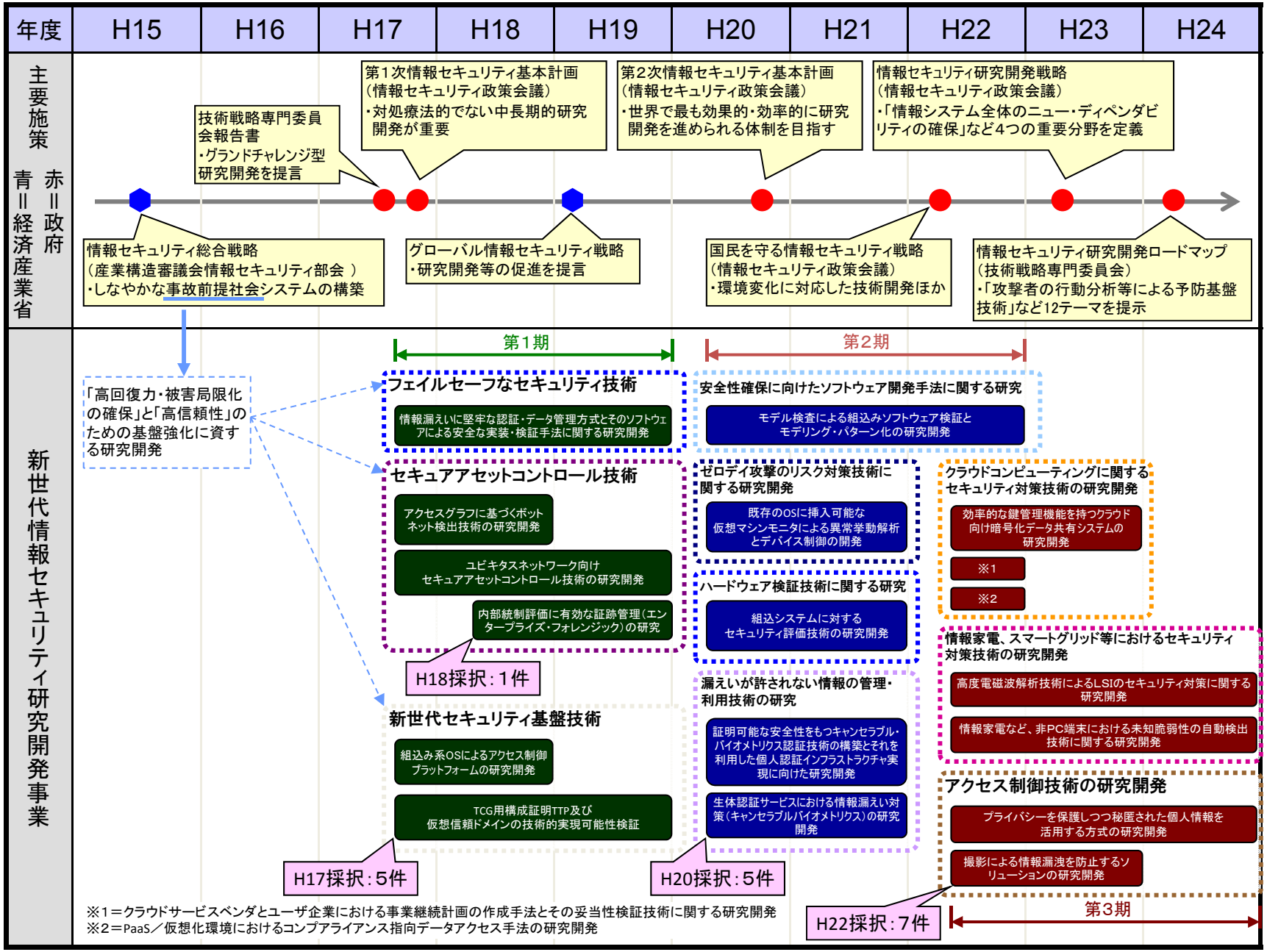
政策的位置づけ

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。

新世代情報セキュリティ研究開発事業：関連上位施策とテーマの変遷



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

商務情報政策局情報セキュリティ政策室

実施機関：国立大学法人東京大学

目　次

１．事業の概要

概　要	本研究では、高度電磁界計測・解析技術の開発・研究を進め、それを応用し、事業目的を達成するための電磁界解析システムを構築した。具体的には、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した。
実施期間	平成２２年度～平成２４年度（３年間）
予算総額	1.4億円（委託） 平成２２年度32.9百万円　平成２３年度52.7百万円　平成２４年度52.7百万円
実　施　者	国立大学法人東京大学　大規模集積システム設計教育研究センター
プロジェクトリーダー	国立大学法人東京大学　大規模集積システム設計教育研究センター センター長　浅田邦博

2. 事業の目的、政策的位置づけ

事業の目的

本事業は、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。

政策的位置づけ

本テーマは、事業公募に先立って公表された「国民を守る情報セキュリティ戦略」（平成22年5月11日公表）における以下の項目に対応する。

2. 新たな環境変化に対応した情報セキュリティ政策の強化

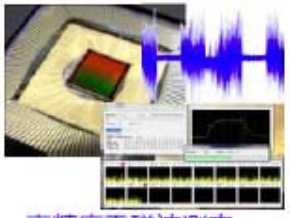
（1）国民生活を守る情報セキュリティ基盤の強化

③その他の基盤強化

情報家電、モバイル端末、電子タグ、センサーネットワークの情報セキュリティ確保方策

（4）技術戦略の推進等

①情報セキュリティ関連の研究開発の戦略的推進等


高精度電磁波測定
と信号解析


不正回路の
検出・混入防止


異常検出・対策

模造LSIの検出

3. 目標

本事業は、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・研究を進めることで、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す。

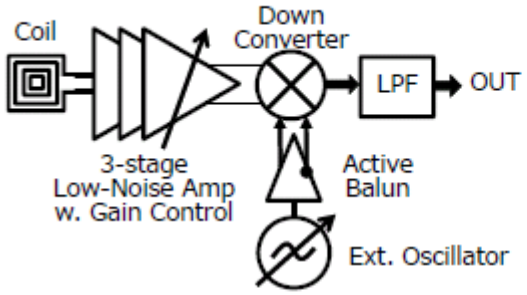
要素技術	目標・指標	妥当性・設定理由・根拠等
高性能磁界プローブの開発	• コイル・アンプの設計 • プローブ加工技術の開発 • プローブの開発・改良 • プローブによるLSIの性能評価 • プローブ筐体の改良 • マクロプローブ開発	現在の電磁波解析攻撃で利用される直径0.5～5mm程度のコイルによる磁界プローブに対し、LSIプロセスによる直径数十μmオーダーの微小磁界プローブを開発し、暗号回路上の局所情報の測定を可能にする。なお異常動作にはLSI 全体で検知されるマクロ的なものも含まれるため、高利得プローブを併用して動作解析を行う。
高精度スキャナの開発	• スキャナ基本機構の開発 • 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。

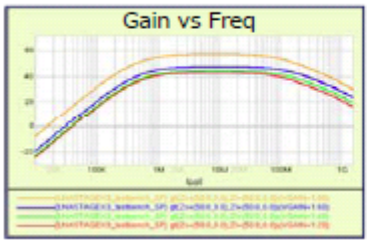
4. 成果、目標の達成度

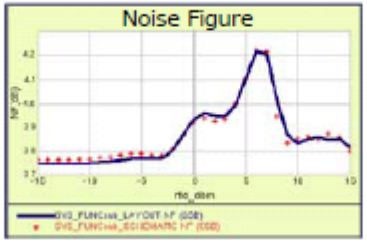
① 高性能磁界プローブの開発

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

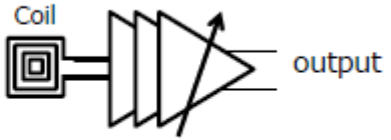
第二世代プローブの回路構成

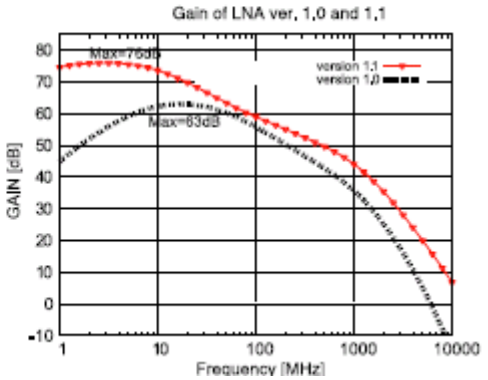






従来の広帯域アンプの構成

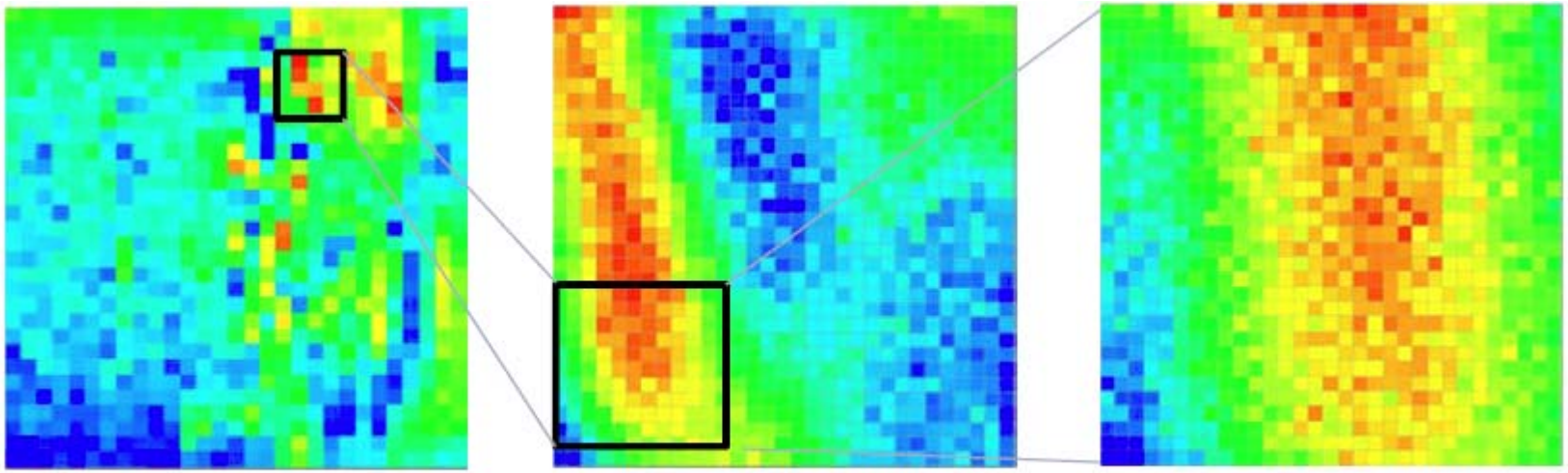




4. 成果、目標の達成度

② 高性能スキャナの開発

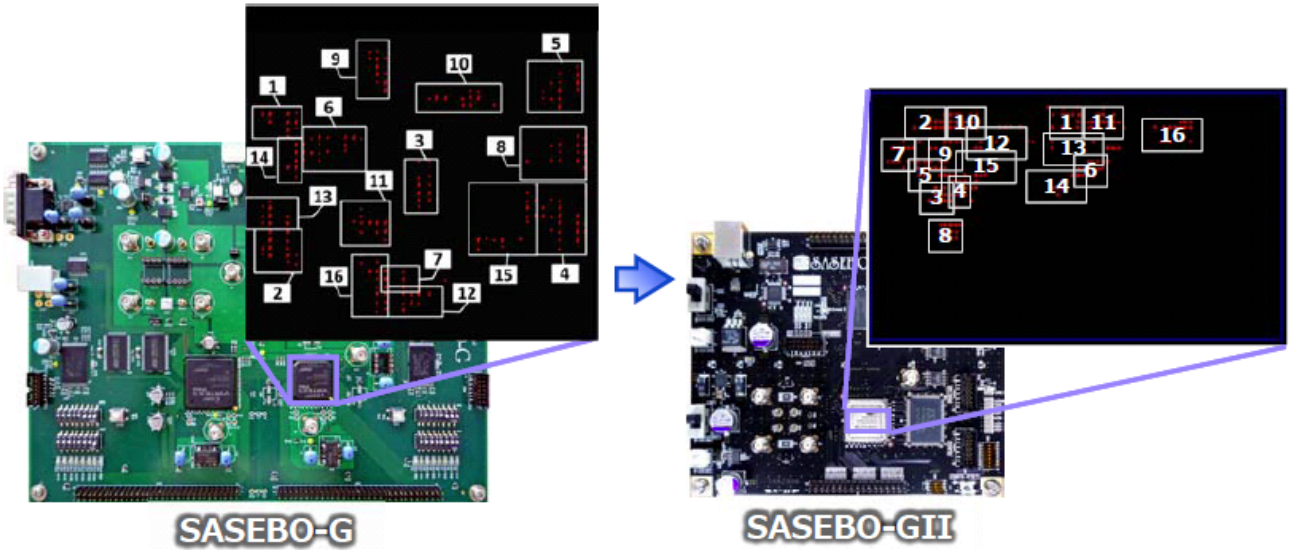
要素技術	目標・指標	成果	達成度
高精度スキャナの開発	• スキャナ基本機構の開発 • 高精度制御機構の開発 • プローブ筐体実装・改良 • 磁界計測・解析ツールの開発	• 初期の実験において外来電磁ノイズの影響を受けていたのをシールドの変更により改善。 • 磁界強度マップの自動生成、ジョイスティックによる操作性向上、誤操作防止機構などを実装した電磁波計測・解析ツールを開発・改良。 • 位置決めにおいて、従来比約10倍の精度を実現。 • 12μmピッチでの高解像度の画像取得に成功。	達成



4. 成果、目標の達成度

③ 実験用セキュリティ回路の開発

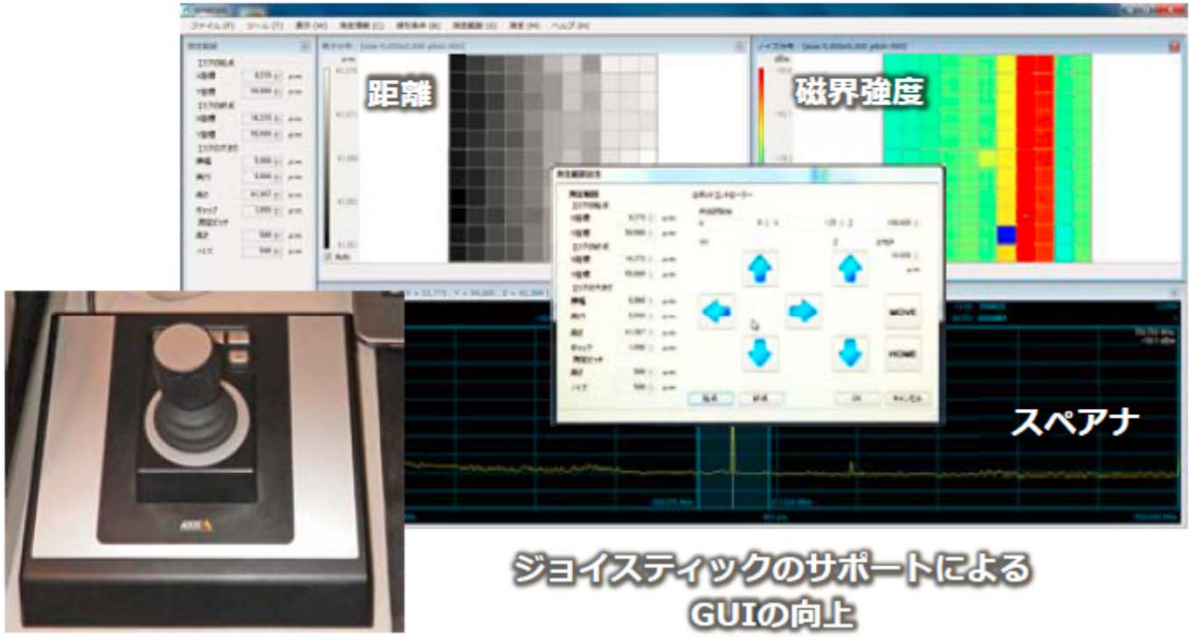
要素技術	目標・指標	成果	達成度
実験用セキュリティ回路の開発	• 暗号回路の実装 • 回路制御ツールの開発 • 真贋判定回路の開発 • Trojan混入ツールの開発 • Trojan回路実装 • 電力解析手法の開発	• サイドチャネル攻撃実験用AES暗号回路をSASEBO-GIIに実装 • 真贋判定用電磁波強調用のAES発振回路を設計しSASEBO-GIIに実装 • 3種類の攻撃手法を適用 • 2ラウンド攻撃（電力解析用手法の適用） • クロック間衝突を用いた攻撃 • 回路の類似性を用いた攻撃 • AES回路のレイアウトをもとに磁界強度分布の分散と平均値を調査	達成



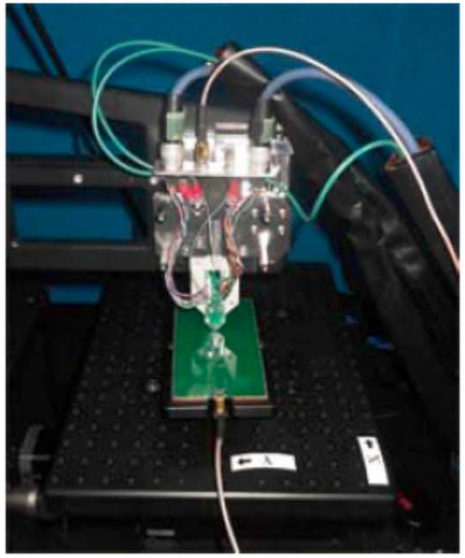
4. 成果、目標の達成度

④ 電磁波解析ツールの開発

要素技術	目標・指標	成果	達成度
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



ジョイスティックのサポートによる
GUIの向上

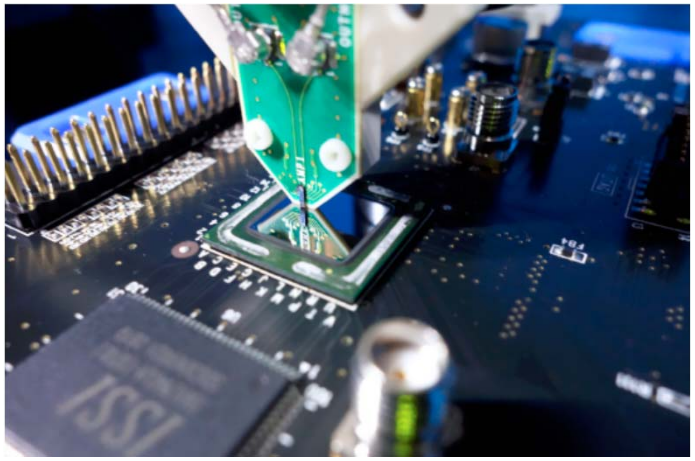


ストリップライン上の磁界計測

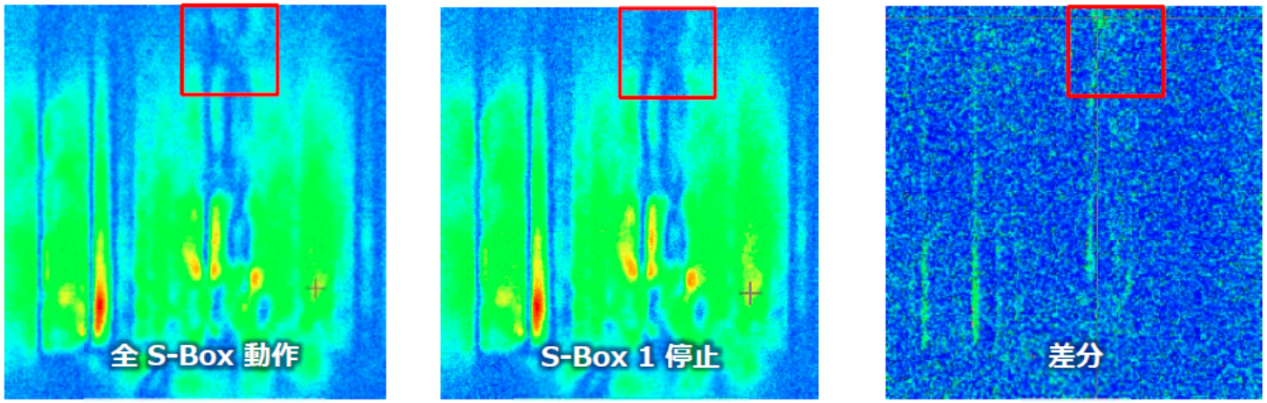
4. 成果、目標の達成度

マイクロ磁界プローブを用いた電磁波解析がもたらす効果：
- 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の大きな可能性
- 統計解析を行わずに磁界マップから直接的情報漏えいを目視できる可能性

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



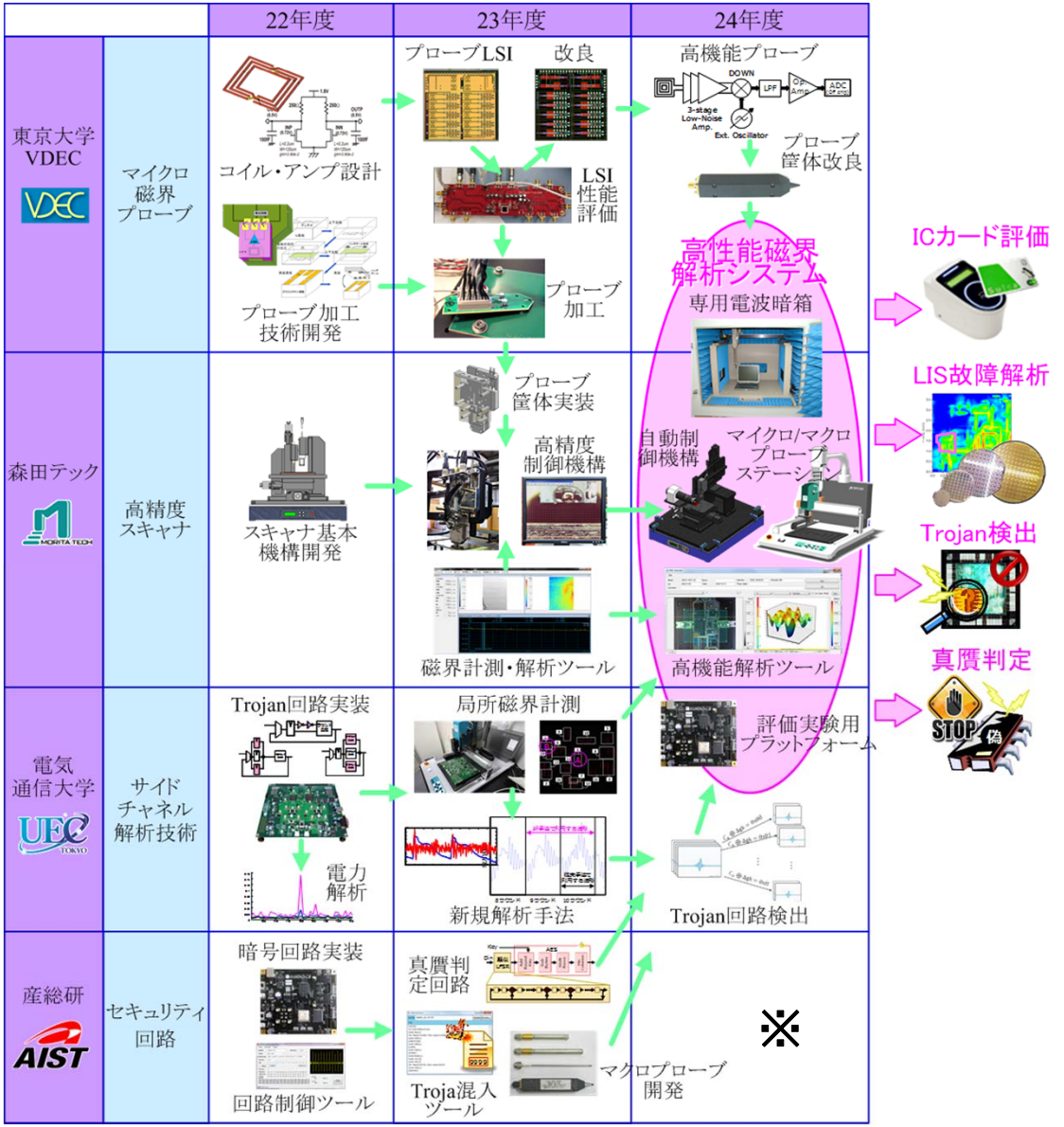
マイクロ磁界プローブを用いた差分磁界マップによる解析の例



@144MHz, 11.2mm × 11.6mm, 50μm/pixel, 72MHz

4. 成果、目標の達成度

研究開発スケジュール



※産総研が組織変更により平成24年度から本事業から離脱したが、産総研の研究代表者が東京大学の立場として研究を継続し、初期に計画した成果を得ている。

5. 事業化・波及効果

事業化状況

- 開発したスキャナの製品化等を通じた産業界への展開については実現していないが、本事業終了後の事業化に向けた取組を継続している。
  - 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
- ICカードの安全性評価への応用
  - ICカード評価において欧州にない日本の技術としてマイクロ磁界プローブが期待されている
  - ISO/IEC 17825（暗号モジュールに関するセキュリティ要求事項）に導入予定のホワイトボックス評価に有効
  - 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
- 車載ネットワークのセキュリティへの応用
  - 電磁波解析技術でカーエレクトロニクスメーカーと共同研究を実施
- 偶発的な故障による異常の検知への応用
  - 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
    →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実施
- 模造品対策への応用
  - 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
  - LSIの個体識別技術だけでなく、semiやJIPDECとトレーサビリティの標準規格化、ICカードベンダーとRFIDの活用等で協力

5. 事業化・波及効果

波及効果

- 本成果は、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。

5. 事業化・波及効果

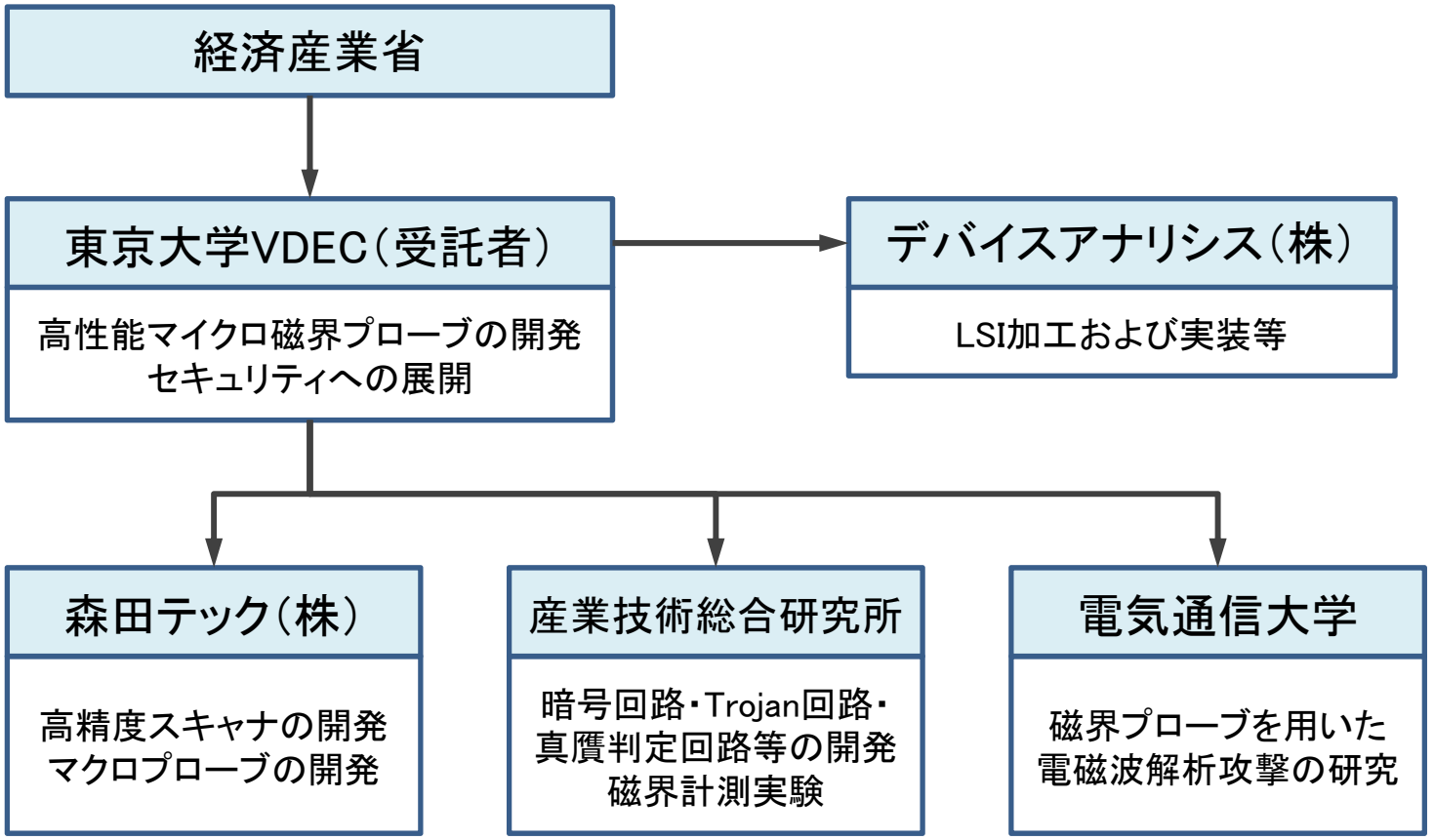
電磁界研究における波及効果

- 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。
- 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。

6. 研究開発マネジメント・体制等

実施体制

- 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。



６．研究開発マネジメント・体制等

【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

【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。

【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

商務情報政策局情報セキュリティ政策室

実施機関：株式会社FFRI

（事業実施時の社名は「株式会社フォティーンフォティ技術研究所」）

1．事業の概要

概　要	現在の情報セキュリティ技術は、ハッキングやコンピュータウイルスなどによる外部脅威においては、対策技術の研究が十分に進んでいるとは言い難い状況である。このため、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を研究開発することが極めて重要となっており、「情報家電など、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開発」を実施するとともに、制御システム向けのファジング技術として、EDSA（Embedded Device Security Assessment）認証に適合可能なファジングツールの研究開発を実施した。 ミューテーションファジング技術の様々な方式に関する研究開発を通じて、モバイルOS（Android、Windows　Phone 7）をはじめとする様々な機器の脆弱性発見手法について検討し、多数の未知脆弱性を発見したが、EDSA認証については、EDSAに規定された要件に適合するツールの開発を実施したが、研究開発期間中に認証を取得するには至らなかった。
実施期間	平成22年度～平成24年度（3年間）
予算総額	68.3百万円（委託） 平成22年度24.7百万円　平成23年度23.1百万円　平成24年度20.5百万円
実　施　者	株式会社フォティーンフォティ技術研究所（現：株式会社FFRI）
プロジェクト リーダー	株式会社フォティーンフォティ技術研究所（現：株式会社FFRI） 代表取締役社長　鵜飼祐司

２．事業の目的、政策的位置づけ

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。

政策的位置づけ

本テーマは、事業公募に先立って公表された「国民を守る情報セキュリティ戦略」（平成22年5月11日公表）における以下の項目に対応する。

（1）国民生活を守る情報セキュリティ基盤の強化

③その他の基盤強化

情報家電、モバイル端末、電子タグ、センサーネットワークの情報セキュリティ確保方策

（4）技術戦略の推進等

①情報セキュリティ関連の研究開発の戦略的推進等

３．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。

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

4. 成果、目標の達成度

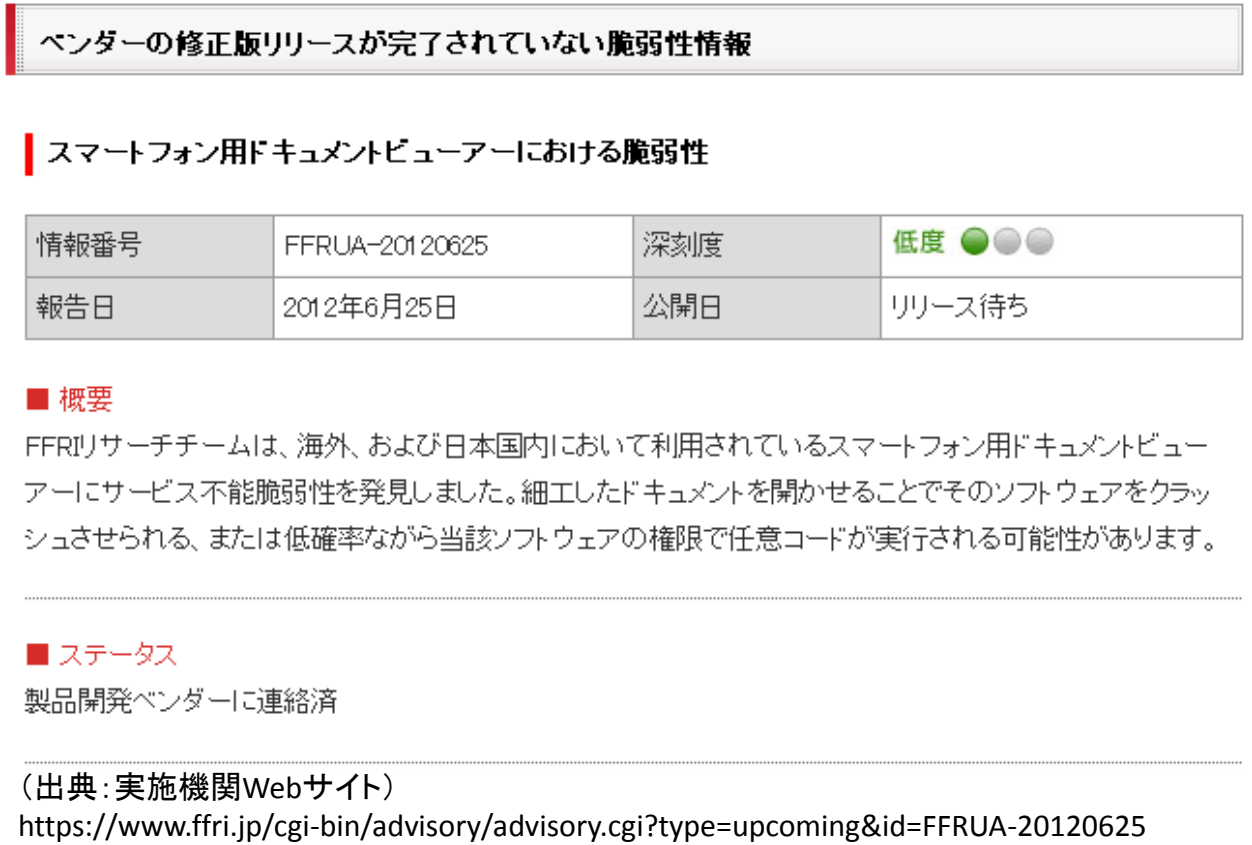
情報家電、モバイル端末、スマートメーター、制御機器等を対象とするファジング方式による脆弱性評価ツールを開発し、実際の機器の検査に適用した。

	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. 成果、目標の達成度

未知脆弱性の発見実績

- 本研究開発の実施過程において、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。
- その他、PC（Windows7）及びそれ以外のネットワーク機器で10件以上の未知の脆弱性を発見した。



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

FFRI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

（出典：実施機関Webサイト）
https://www.ffri.jp/cgi-bin/advisory/advisory.cgi?type=upcoming&id=FFRUA-20120625

4. 成果、目標の達成度

研究開発のスケジュール

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. 事業化・波及効果

事業化

- 実施機関が自ら企業向けに提供するサービスにおいて活用中。
- 下記製品・サービスのほか、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。

（出典：実施機関Webサイト）
http://www.ffri.jp/products/raven/index.htm
http://www.ffri.jp/services/android/

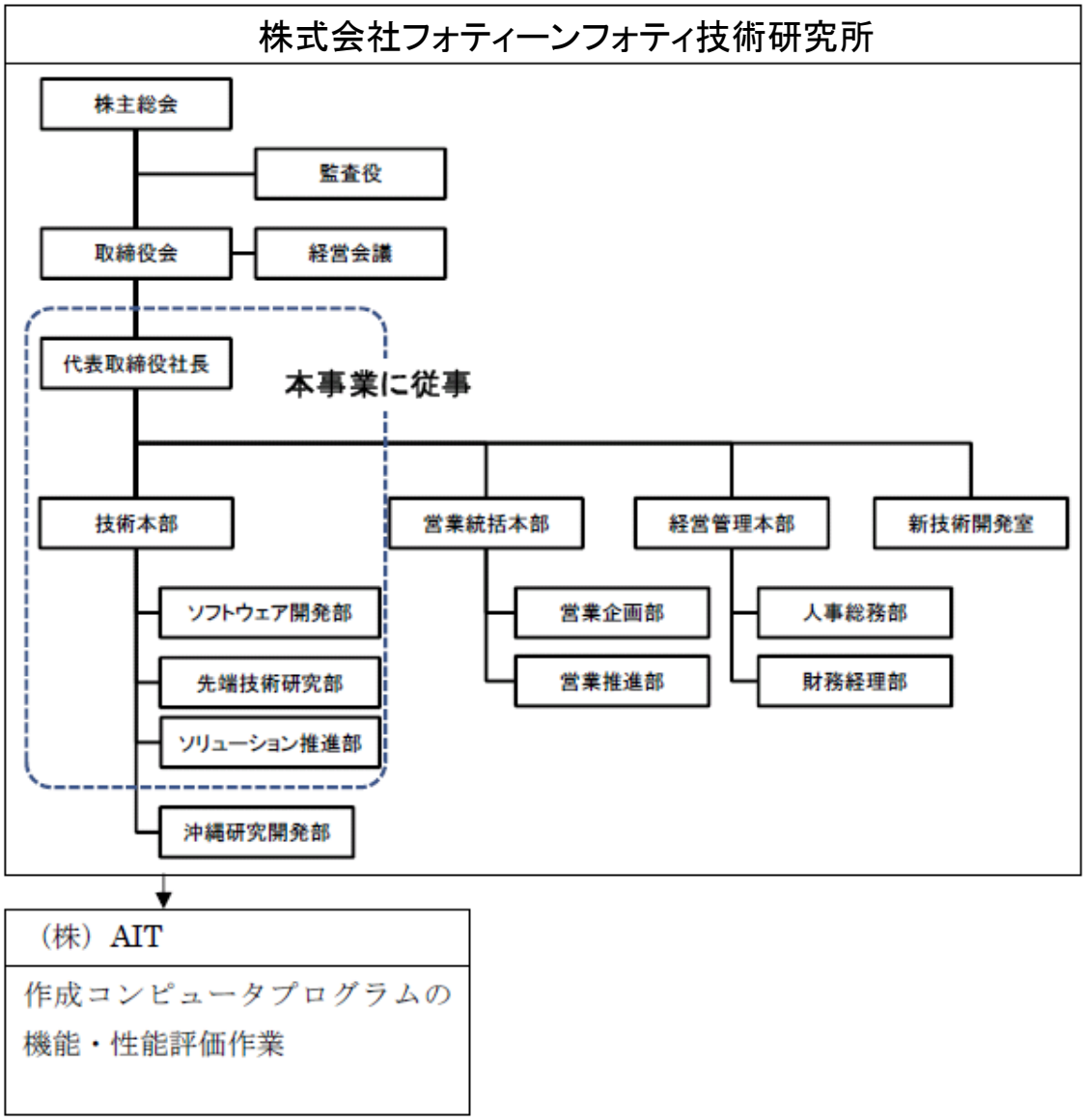
5. 事業化・波及効果

波及効果

- 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。
- 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。

6．研究開発マネジメント・体制等

実施体制



6. 研究開発マネジメント・体制等

【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

【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。

【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。

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

商務情報政策局情報セキュリティ政策室
実施機関：学校法人中央大学

１．事業の概要

概　要	コンピュータや通信ネットワークの発展に伴い、様々な業務に関するデータの集積が進んでいるが、それに伴い、個人情報の取扱いに関心が高まり、法制度の整備が行われている。一方、これら大量に蓄積された情報を分析することにより、利用価値の高い情報や知識を得られるという側面もある。このため、プライバシーを保護しつつ、個人情報を暗号により秘匿されたまま必要な情報処理を行うことにより、個人情報の有効な活用を可能とする方式の研究開発を行った。 具体的には、「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した。
実施期間	平成22年度～平成24年度（3年間）
予算総額	1.0億円（委託） 平成22年度　27.7百万円　平成23年度　36.3百万円　平成24年度　37.1万円
実　施　者	学校法人中央大学　研究開発機構
プロジェクトリーダー	学校法人中央大学　研究開発機構教授　土居範久

2. 事業の目的、政策的位置づけ

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。

政策的位置づけ

本テーマは、事業公募に先立って公表された「国民を守る情報セキュリティ戦略」（平成22年5月11日公表）における以下の項目に対応する。

2. 新たな環境変化に対応した情報セキュリティ政策の強化

（1）国民生活を守る情報セキュリティ基盤の強化

③その他の基盤強化

医療、教育分野等における情報セキュリティ確保方策

（2）国民・利用者保護の強化

③個人情報保護の推進

プライバシー保護技術の適切な利用促進

（4）技術戦略の推進等

①情報セキュリティ関連の研究開発の戦略的推進等

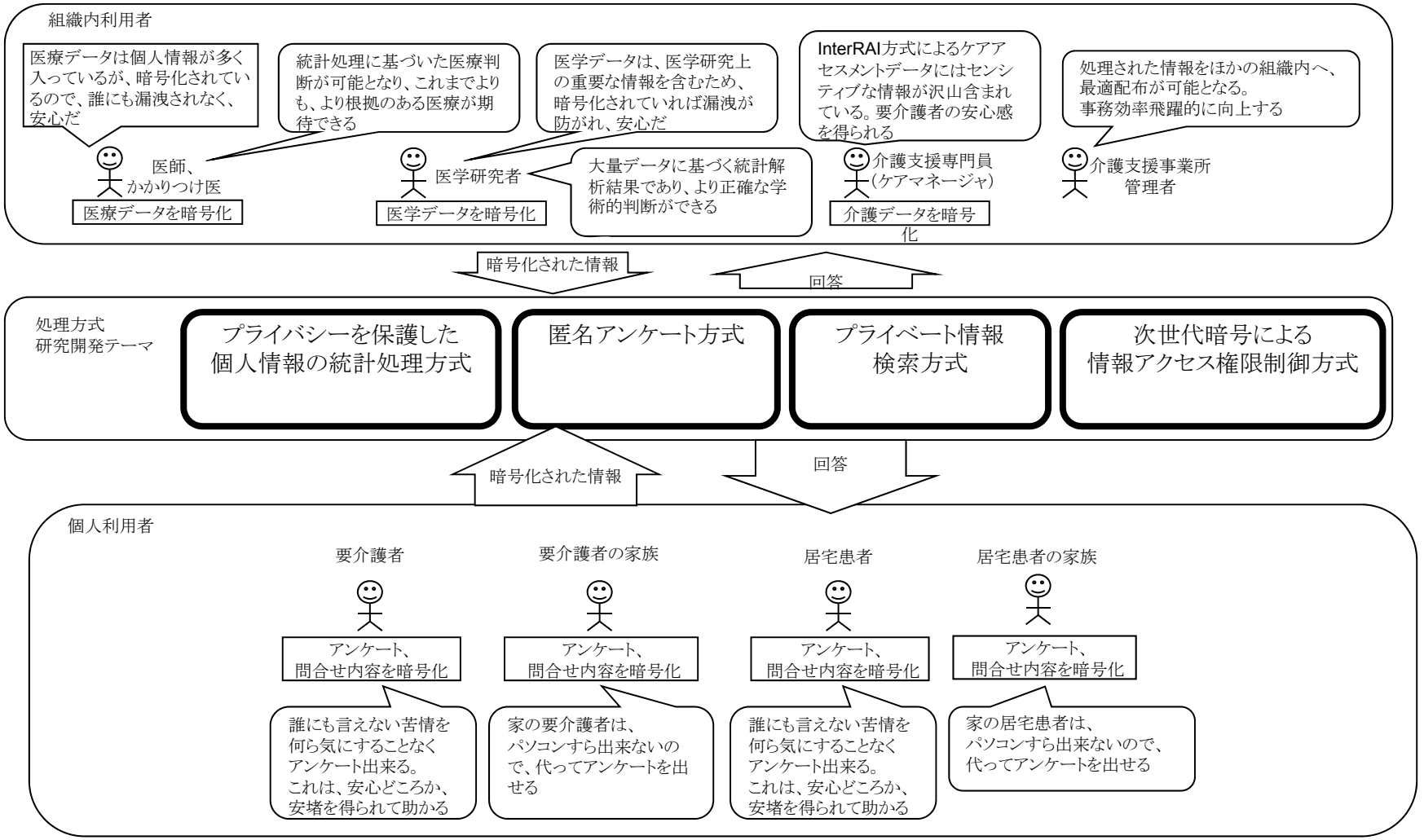
3. 目標

本事業ではプライバシーを保護しつつ、個人情報の有効な活用を図るため、「医療・介護分野」を対象とした、以下の研究開発テーマを実施する。

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（組織暗号）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。

3. 目標

研究開発テーマと医療・介護との関係は下図のとおり。



4. 成果、目標の達成度

下記に示す4種類の要素技術それぞれについて、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並びに医療・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並びに一部、プロトタイピング、デモプログラムの作成を行った。平成24年度はプロトタイピングによる性能評価、論文発表並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。

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

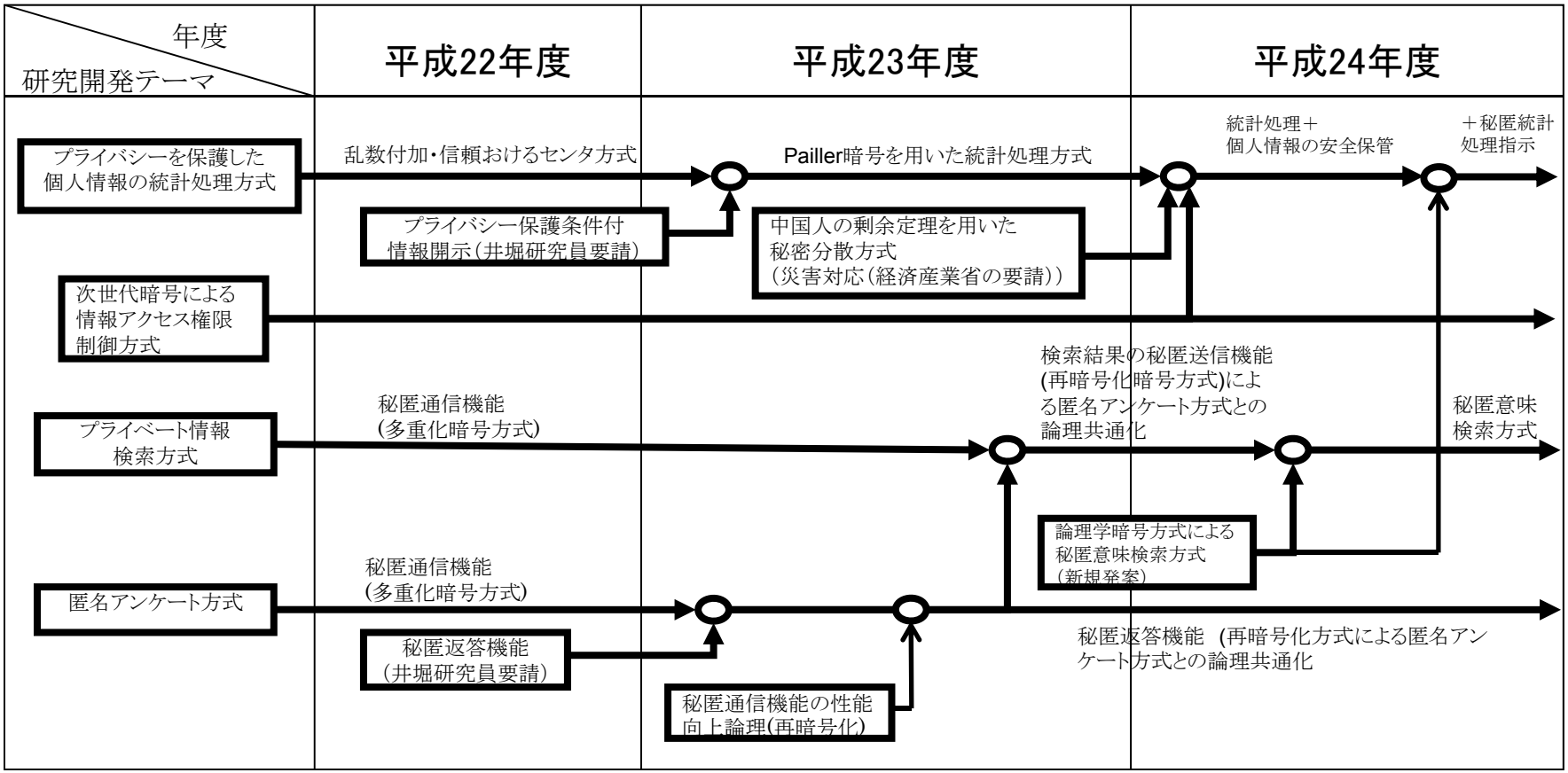
4. 成果、目標の達成度

本事業による研究開発成果は下表のように整理される。(2013年3月末時点の活動状況)

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

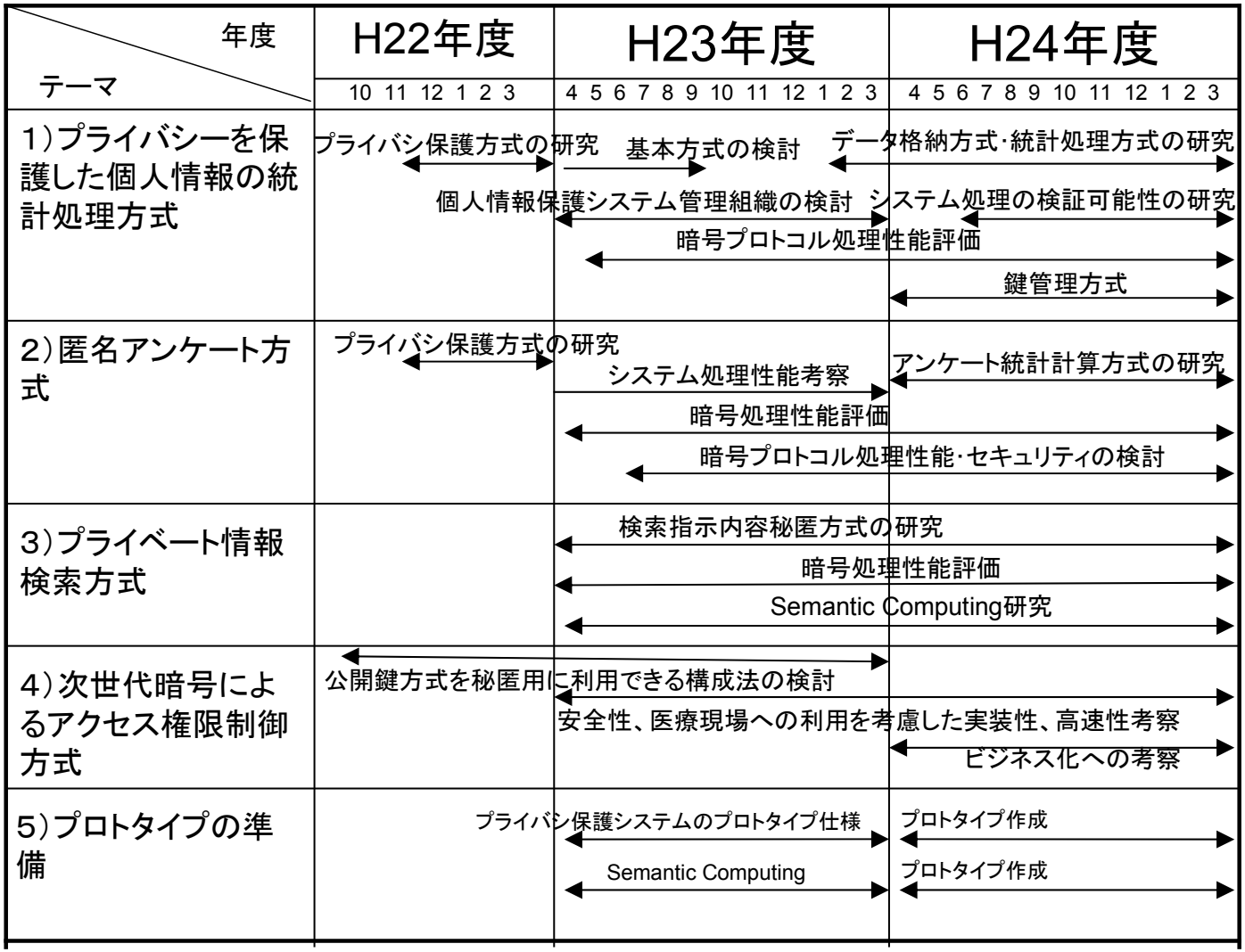
4. 成果、目標の達成度

本事業の実施過程において、社会等のニーズをもとに以下の機能追加を実施。



4. 成果、目標の達成度

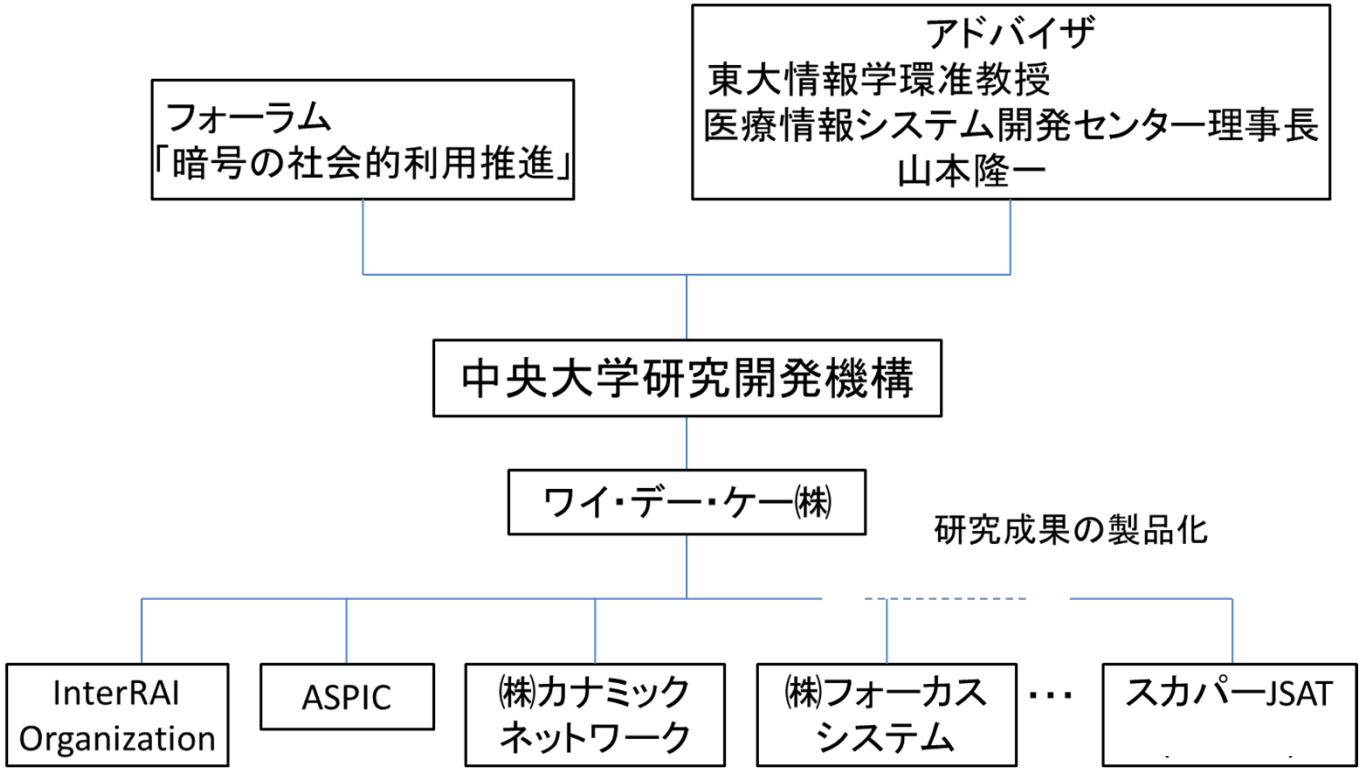
研究開発のスケジュール



5. 事業化・波及効果

事業化

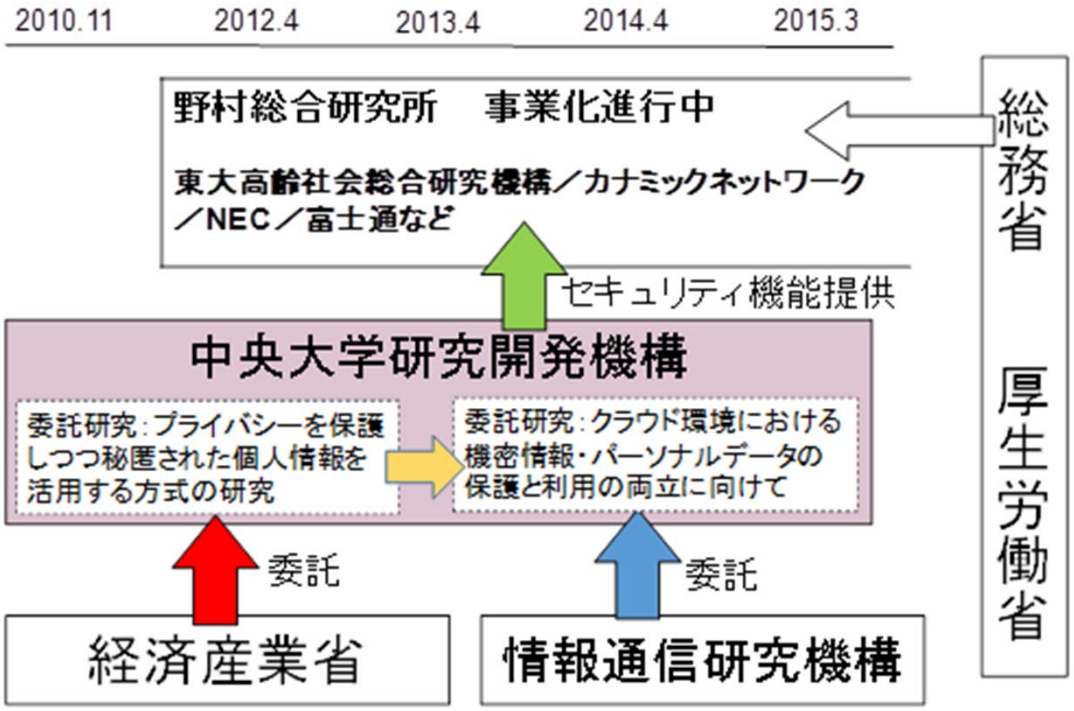
- 下図の事業化体制にて、事業化を目指している。



5. 事業化・波及効果

事業化

- 本成果のうち、「次世代暗号による情報アクセス制御方式」の成果である、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）は、平成25年度から開始された独立行政法人情報通信研究機構の委託研究「クラウド環境における機密情報・パーソナルデータの保護と利用の両立に向けて」において活用されている。
- 上記委託研究におけるインタフェースの具体化などを経て、株式会社野村総合研究所による事業化が現在進行中である。



5. 事業化・波及効果

その他の事業化

- 多様な事業化の実現に向け、下表の活動を実施中。

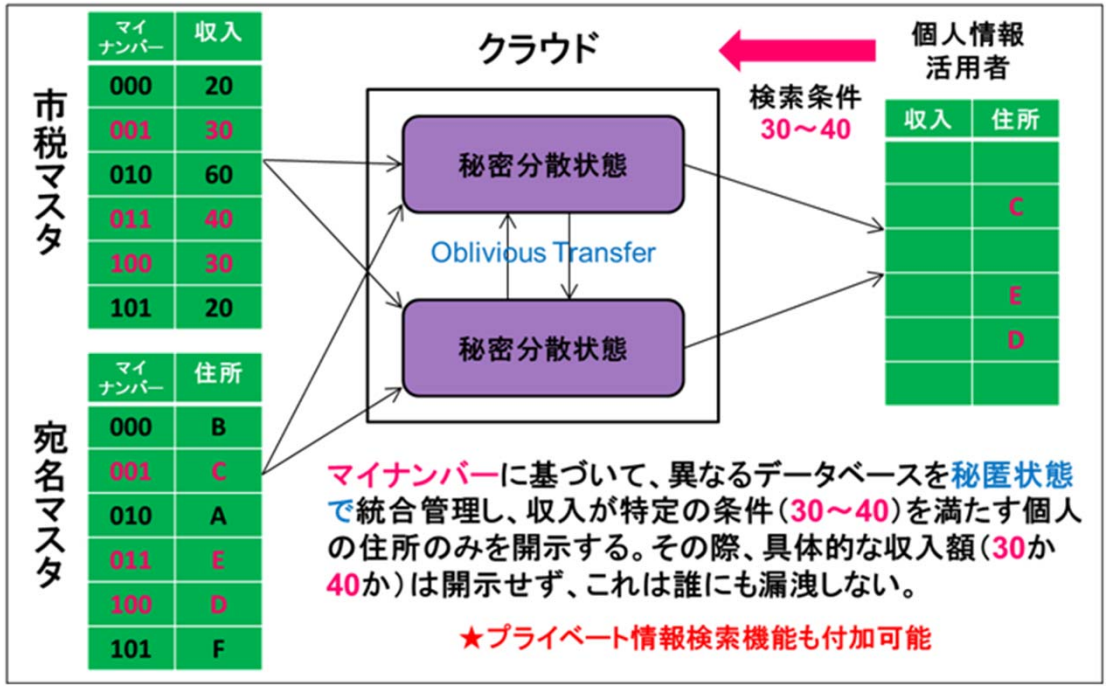
区分	実用化計画	提携企業
実用化戦略	「インターライ方式ケアアセスメントクラウドサービス」への「プライバシーを保護した統計処理システム」の適用	ASPIC, カナミックネットワーク
	「プライバシーを保護した統計処理システム」「匿名アンケート方式」「プライベート情報検索方式」を用いて医療データの2次利用データベースから1次利用データの活用を図るシステムの実現	YDK, スカパーJSAT
	米国Biomedical Objects Inc. による臨床医学分野への適用を促進し、併せて国内における同分野における展開を行う	Biomedical Objects Inc.
実用化推進フォーラム戦略	「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

左表内「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」として活動中。
http://www.fuji-serv.com/chuo/index.html

5. 事業化・波及効果

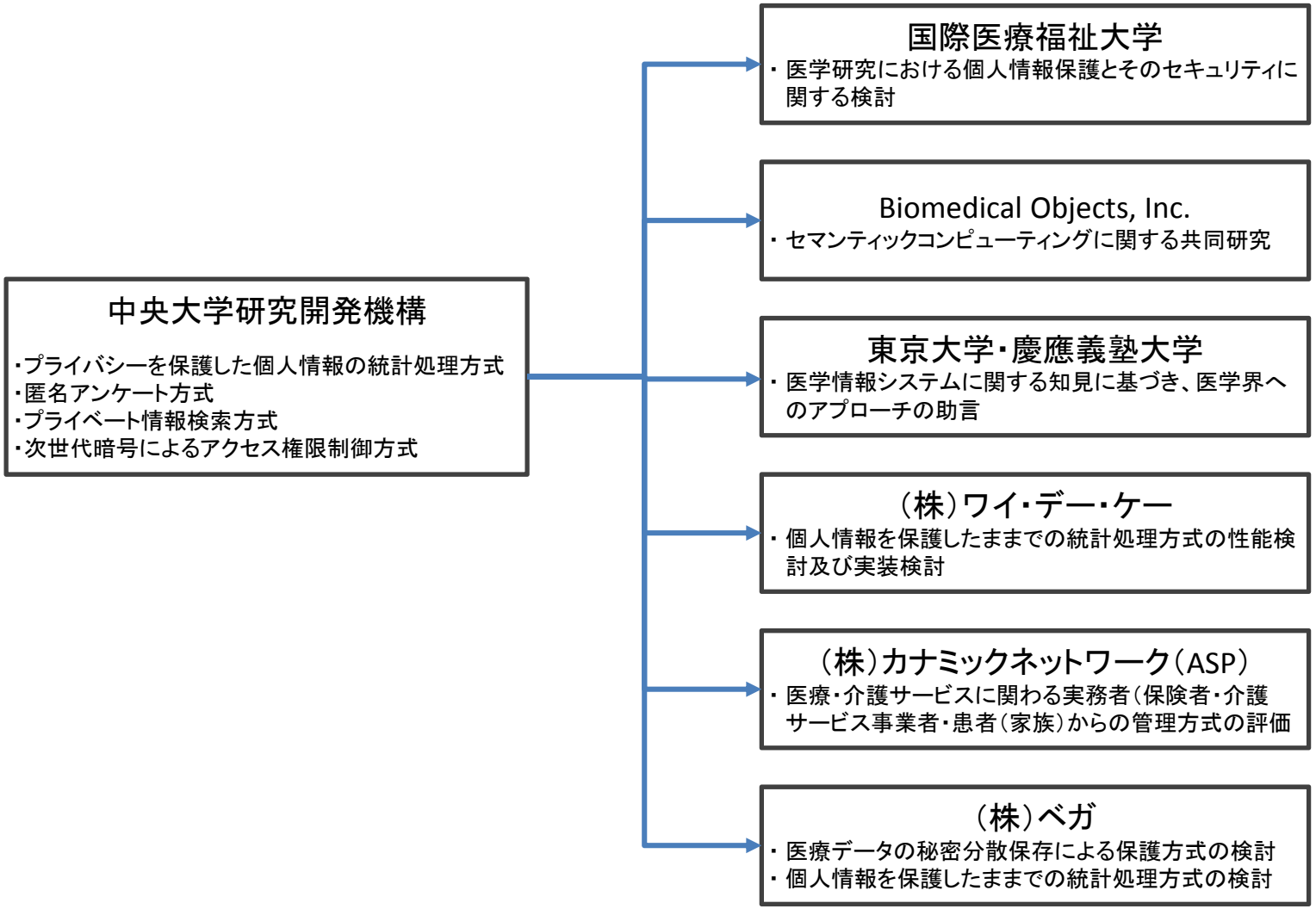
波及効果

- 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。



6．研究開発マネジメント・体制等

- 本実施体制に参加した組織、企業、及び研究者は、いずれも医療分野、介護分野で優れた実績を上げているとの観点から選定された。



６．研究開発マネジメント・体制等

【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

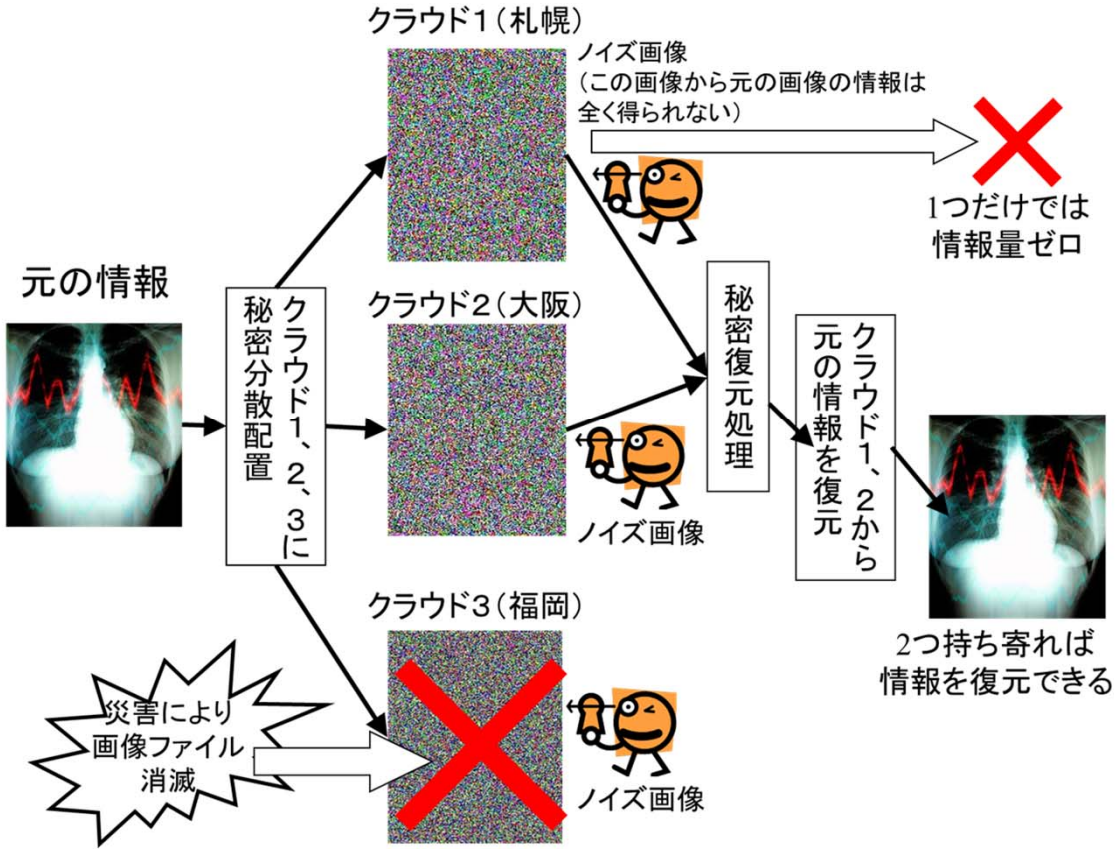
【費用対効果】

- 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。

6. 研究開発マネジメント・体制等

【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。



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

商務情報政策局情報セキュリティ政策室

実施機関：綜合警備保障株式会社

１．事業の概要

概　要	現状において十分な対策が実現できていない、撮影による情報漏洩について、以下の２種類の研究開発を実施した。 （１）透明赤外線光源の開発 透明度が高く、赤外線を発光するIRシート光源のプロトタイプの開発を行った結果、撮影にとってノイズとなる赤外線の発生に成功した。ただし実験に用いたガラス素材ではコンテンツの識別性の低下の実現は難しいことが確認された。 （２）赤外線遮断対抗技術の開発 画面に対する撮影行為の検知システムとして、カメラを構えている人物の識別技術を開発した。
実施期間	平成２２年度～平成２３年度（２年間）
予算総額	28.6百万円（委託） 平成２２年度12.2万円　平成２３年度16.4万円
実　施　者	綜合警備保障株式会社
プロジェクトリーダー	綜合警備保障株式会社　開発企画部 シニアエンジニア　藤川真樹

2. 事業の目的、政策的位置づけ

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。

政策的位置づけ

本テーマは、事業公募に先立って公表された「国民を守る情報セキュリティ戦略」（平成22年5月11日公表）における以下の項目に対応する。

2. 新たな環境変化に対応した情報セキュリティ政策の強化

（1）国民生活を守る情報セキュリティ基盤の強化

③その他の基盤強化

情報家電、モバイル端末、電子タグ、センサーネットワークの情報セキュリティ確保方策

（4）技術戦略の推進等

①情報セキュリティ関連の研究開発の戦略的推進等

3. 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。

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。

4. 成果、目標の達成度

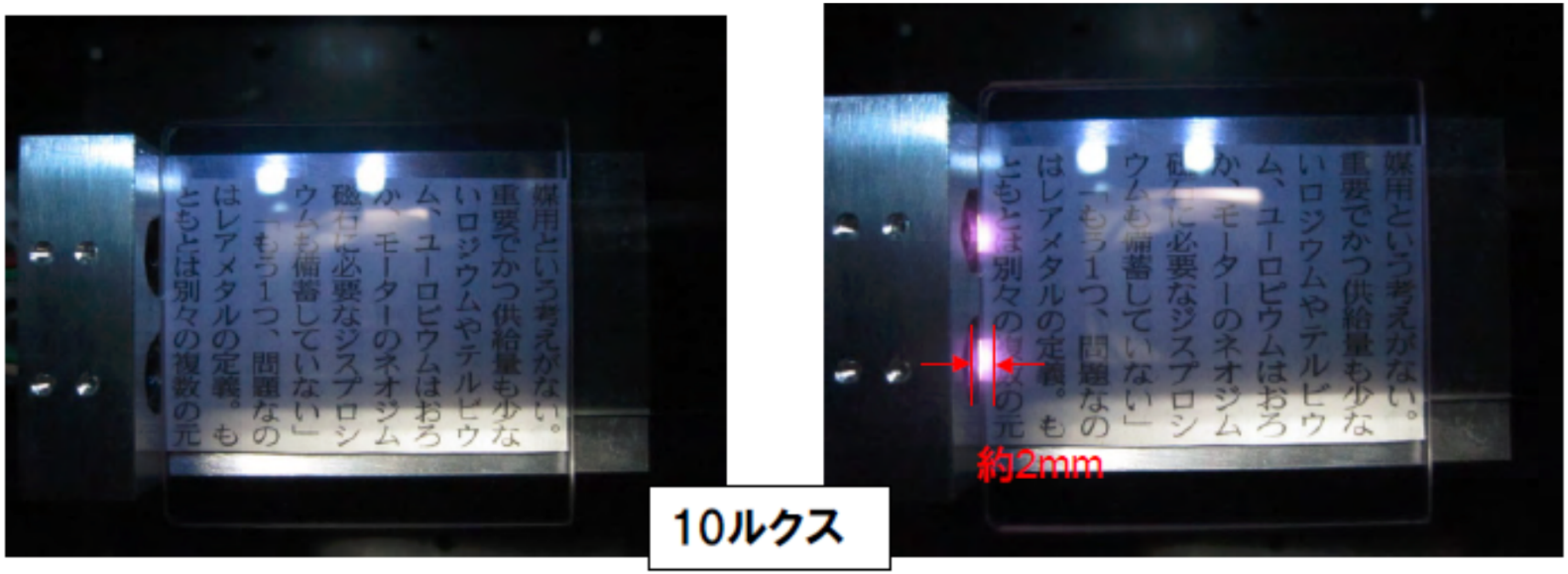
透明赤外線光源の開発

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

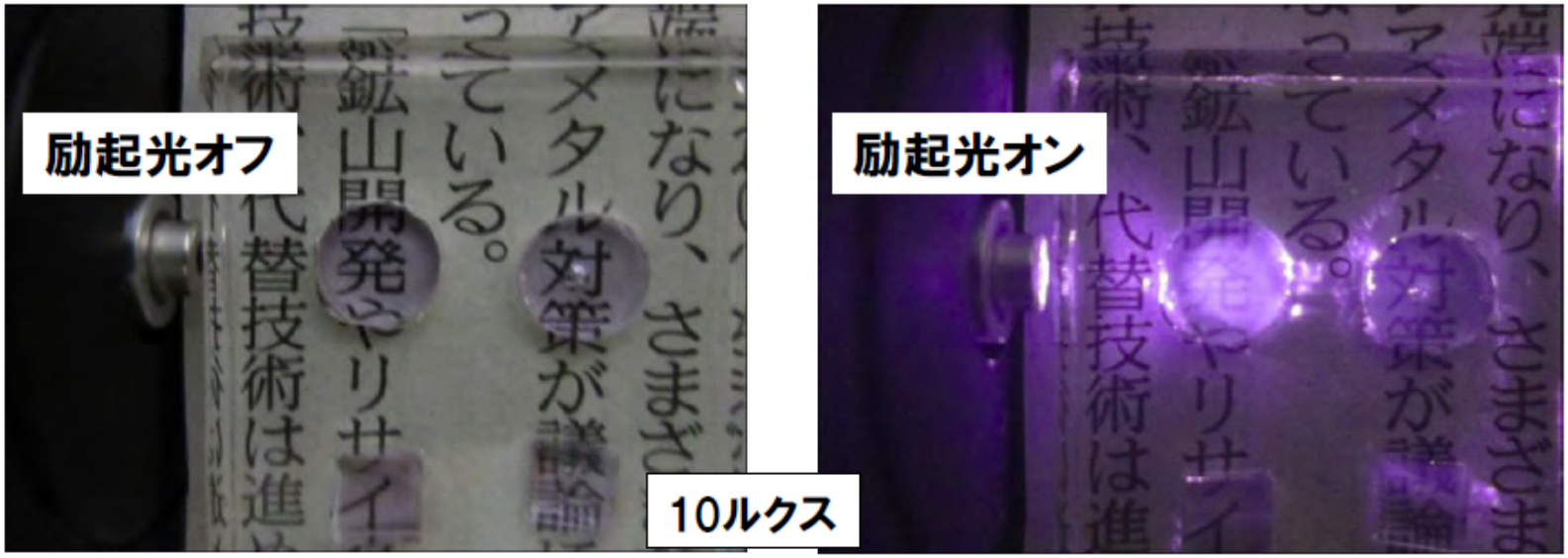
Bi_2O_3に代えて、ZnOを用いることで透明化を達成。

4. 成果、目標の達成度

板ガラス



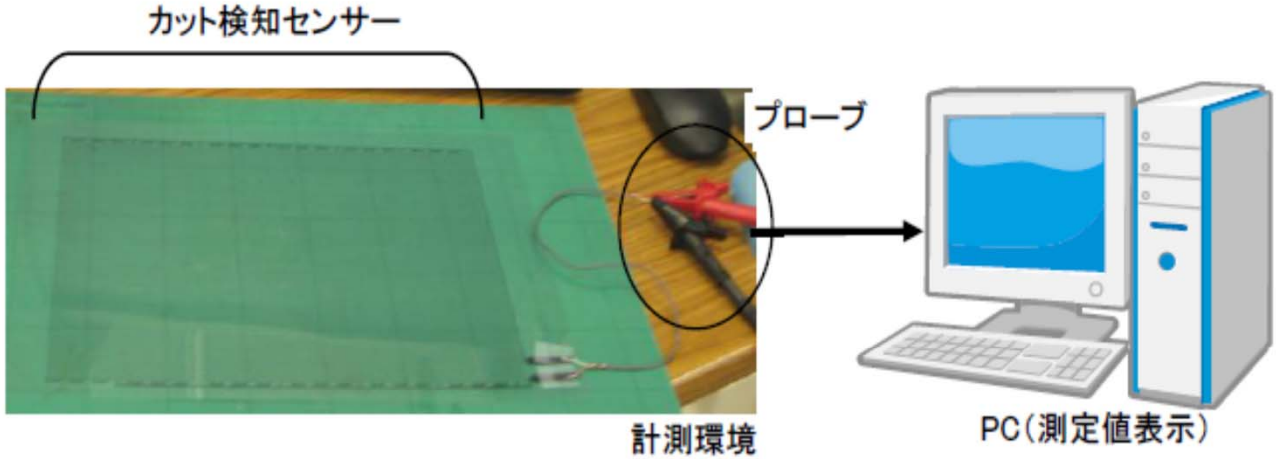
粒ガラス



いずれも発光によるノイズ発生効果は不十分

4. 成果、目標の達成度

カット検知センサ
（開発成功）



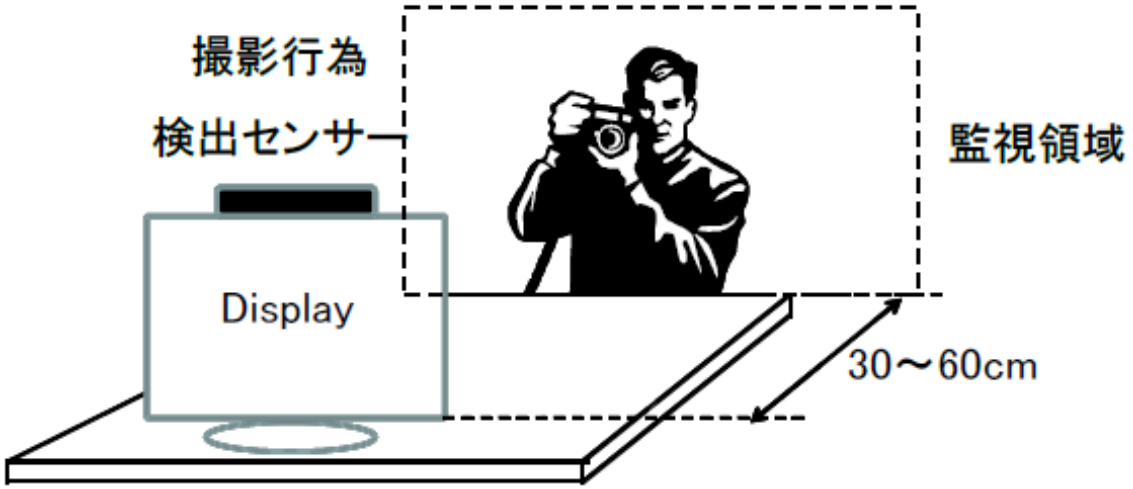
カット前の抵抗値

カット後の抵抗値

4. 成果、目標の達成度

赤外線遮断対抗技術の開発

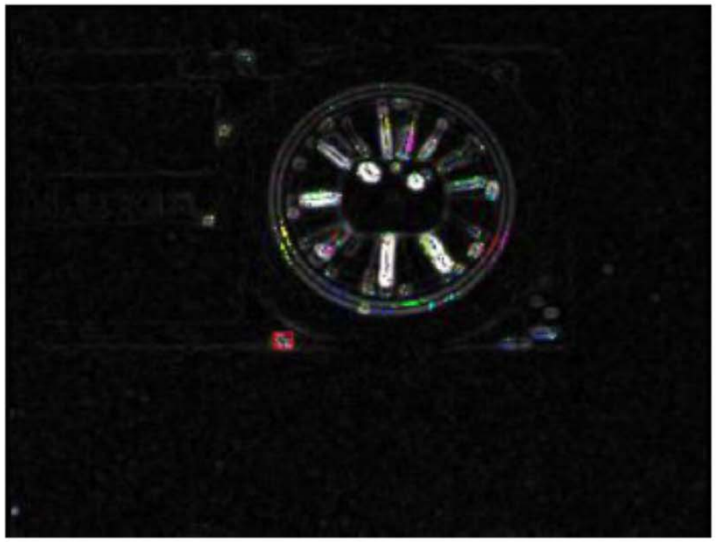
要素技術	目標・指標	成果	達成度
赤外線遮断対抗技術の開発	• 品質の高いコンテンツが記録されることを防止するため、IRカットフィルターがディスプレイの近傍にあることを検知できる手法を開発する。 • 撮影行為を検知できる手法の開発を目指す。	• 赤外線カットフィルターをレンズの前面に設置した撮影、カメラ単体による撮影の検知に成功。 • 片手、両手でカメラを構えたり、三脚等を用いてカメラを構える行為の検知に成功。 • 実証実験では眼鏡のレンズの誤検知や、反射防止型フィルタや携帯電話による撮影などの検知漏れなどの問題が生じており、実用化には更なる精度向上が必要。	概ね達成



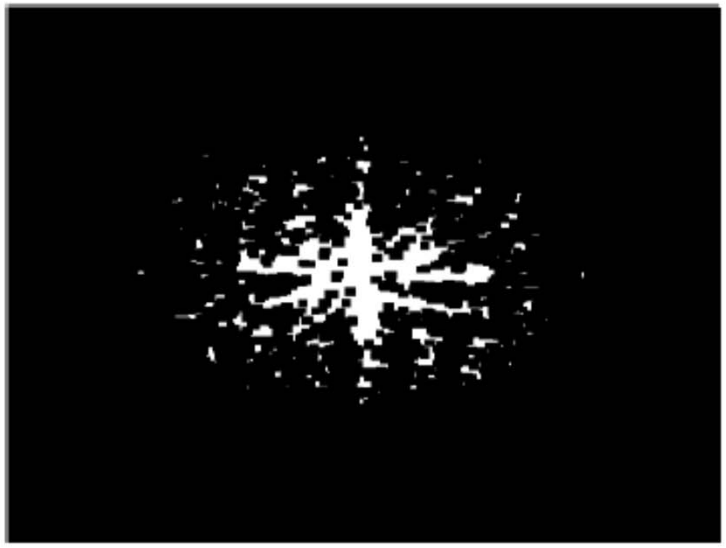
4. 成果、目標の達成度

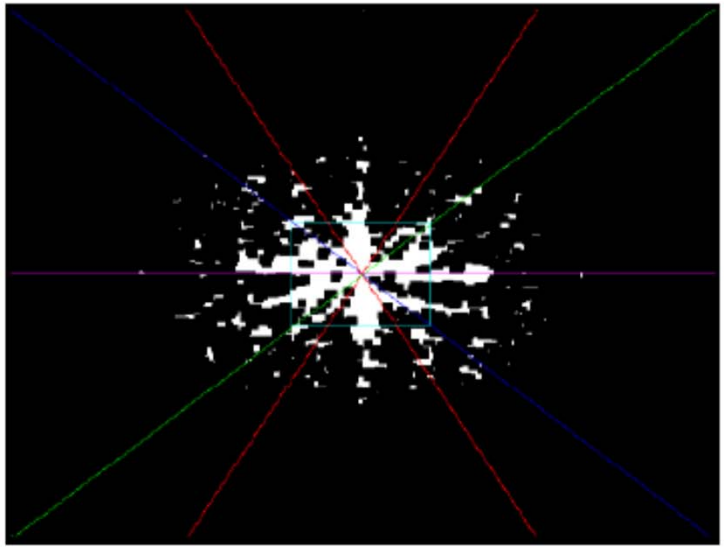
コンパクトデジタルカメラの識別（成功例）

レンズ部分のエッジ抽出



可変閾値法による識別



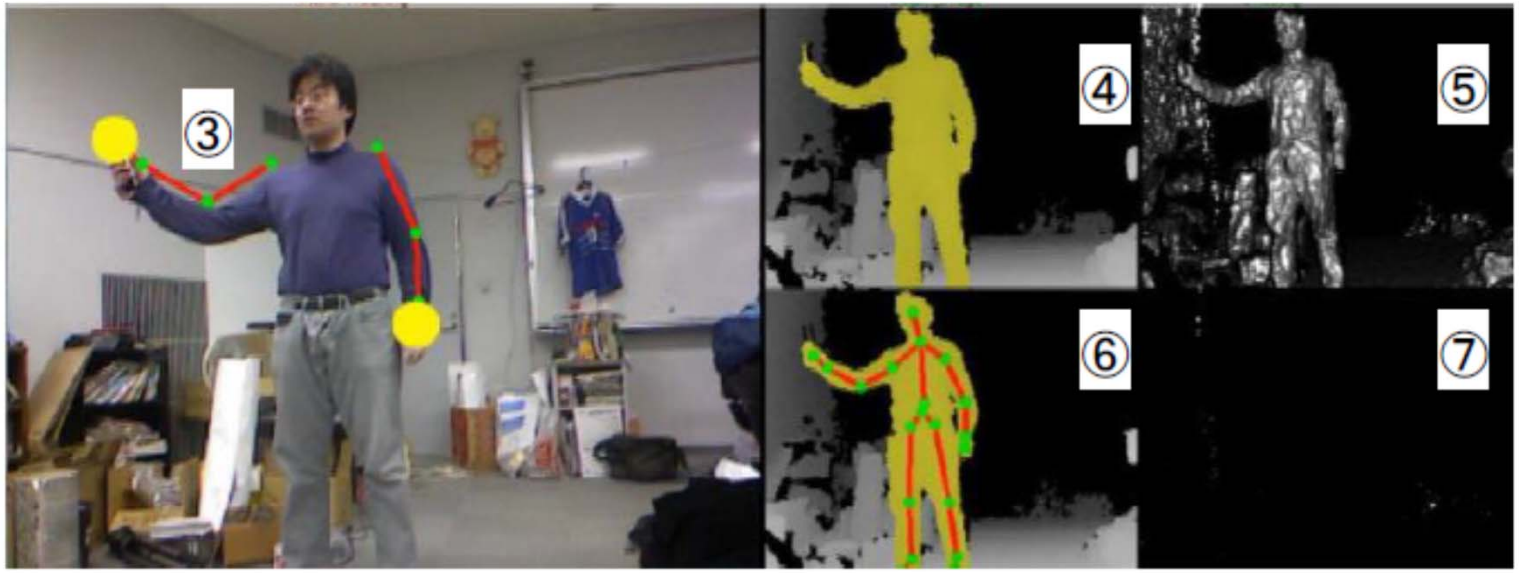


4. 成果、目標の達成度

撮影者の動作の識別手法

成功例

失敗例



4. 成果、目標の達成度

成果の普及啓発

要素技術	目標・指標	成果	達成度
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

Vienna university (ARES2011)


新潟 (CSS2011)

4. 成果、目標の達成度

研究開発のスケジュール

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

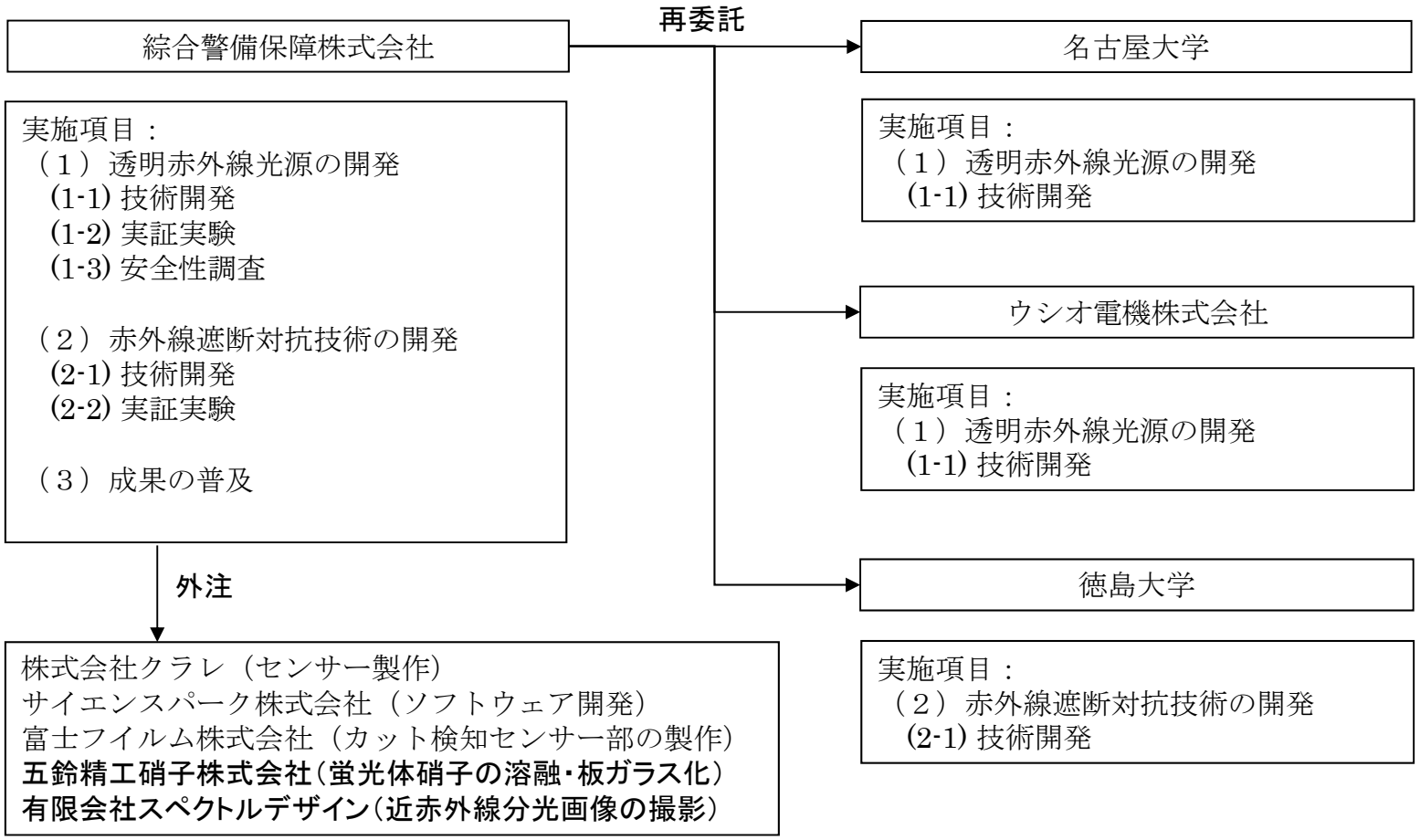
5. 事業化・波及効果

事業化に向けた取り組み

- 成果の製品化に向け、引き続き自己資金による研究開発を実施中。
  - 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が、まだ市場に存在しない。
  - 撮影者検知については、誤検知防止の精度向上が必要。
  - 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。
- 派生的事業化の可能性
  - 開発した蛍光体ガラスを利用することで、高級ガラス・陶磁器の真正性を判定することが可能（特許出願済み）。ブランド企業や窯元等へのヒアリングなどの市場調査を検討。
  - カット検知センサーは、流通過程におけるパッキングフィルムや結束バンドの不正な取り外しの検知に利用できる可能性がある。本件についても、特許を出願するとともに、流通事業者へのヒアリング等の市場調査を検討。

6. 研究開発マネジメント・体制等

実施体制



６．研究開発マネジメント・体制等

【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

【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。

【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。

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

商務情報政策局情報セキュリティ政策室
実施機関：株式会社神戸デジタル・ラボ

１．事業の概要

概　要	「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した。
実施期間	平成２２年度～平成２３年度（２年間）
予算総額	35.2百万円（委託） 平成２２年度15.6百万円　平成２３年度19.6百万円
実　施　者	株式会社神戸デジタル・ラボ
プロジェクトリーダー	株式会社神戸デジタル・ラボ　ICTソリューション部　セキュリティ部門　近藤伸明　チーフコンサルタント（主任研究員）

2. 事業の目的、政策的位置づけ

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。

政策的位置づけ

本テーマは、事業公募に先立って公表された「国民を守る情報セキュリティ戦略」（平成22年5月11日公表）における以下の項目に対応する。

2. 新たな環境変化に対応した情報セキュリティ政策の強化

（1）国民生活を守る情報セキュリティ基盤の強化

③その他の基盤強化

クラウドコンピューティング化に対応した情報セキュリティ確保方策、標準化

（4）技術戦略の推進等

①情報セキュリティ関連の研究開発の戦略的推進等

３．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。

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。

4. 成果、目標の達成度

- **前ページに設定した目標のうち、「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。**

要素技術	目標・指標	成果	達成度
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	• 属性ベース暗号の運用モデルと失効リストによるチェック機能について、具体例をもとに要件をとりまとめた。	達成
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	• 評価システムが備えるべき機能として、鍵生成、暗号化、復号、鍵管理失効の各機能の処理内容と操作手順を定め、これをもとに評価システムを構築した。 • 評価システムを用いて性能測定を行い、属性数や失効ユーザ数を増やしても、処理時間が実用的な範囲内に収まることが確認された。 • 情報処理学会会合参加者への本成果に関するアンケート調査を実施した。	達成

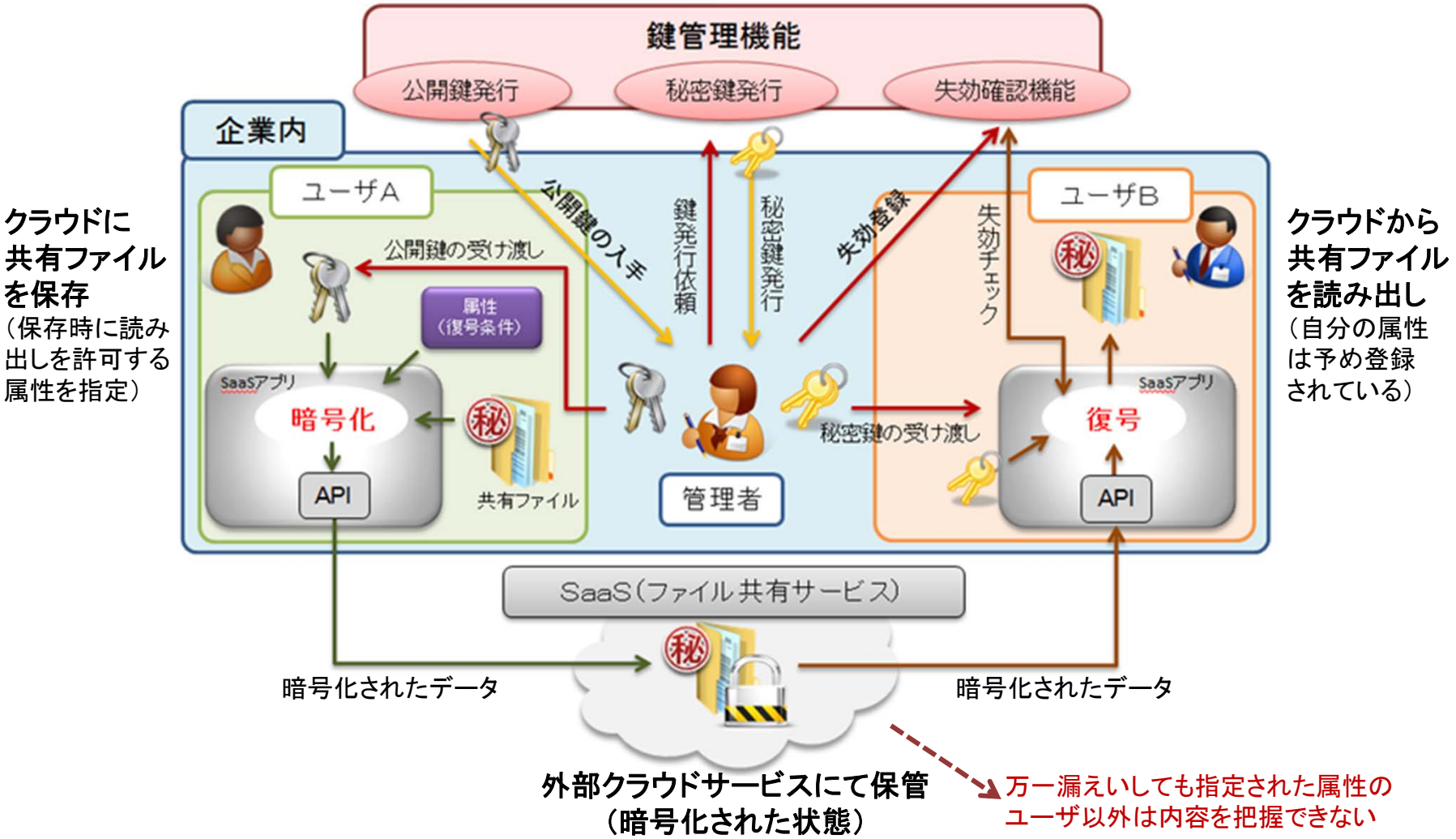
4. 成果、目標の達成度

- 「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。

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

4. 成果、目標の達成度

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）

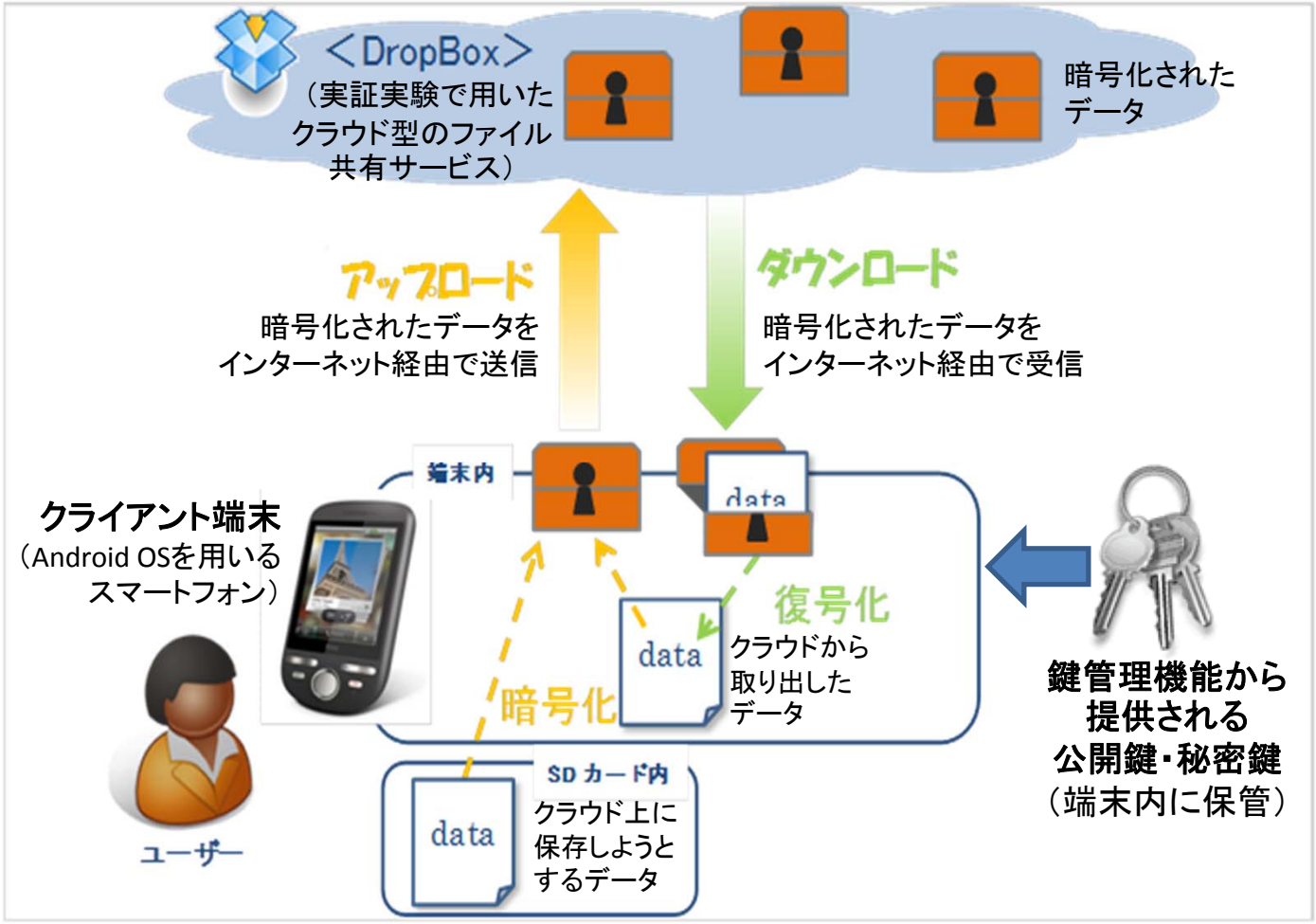


クラウドに共有ファイルを保存
（保存時に読み出しを許可する属性を指定）

クラウドから共有ファイルを読み出し
（自分の属性は予め登録されている）

4. 成果、目標の達成度

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



4. 成果、目標の達成度

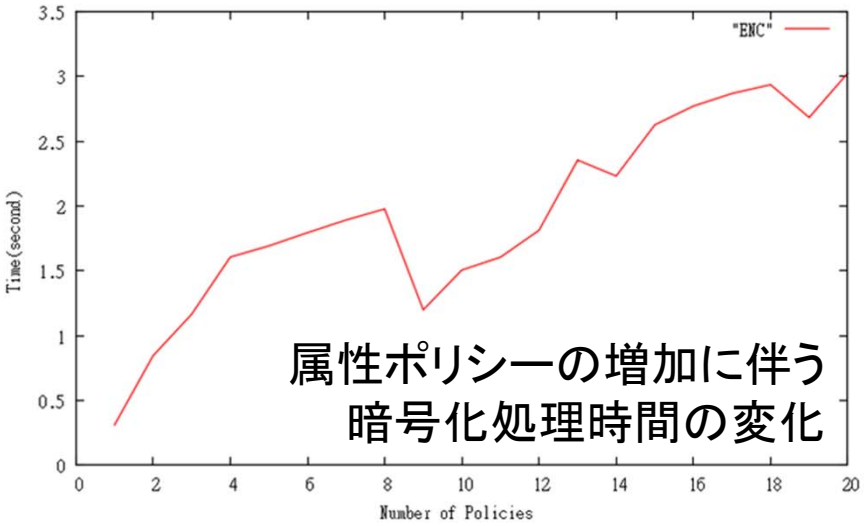
評価システムを対象とする性能測定結果

- 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。

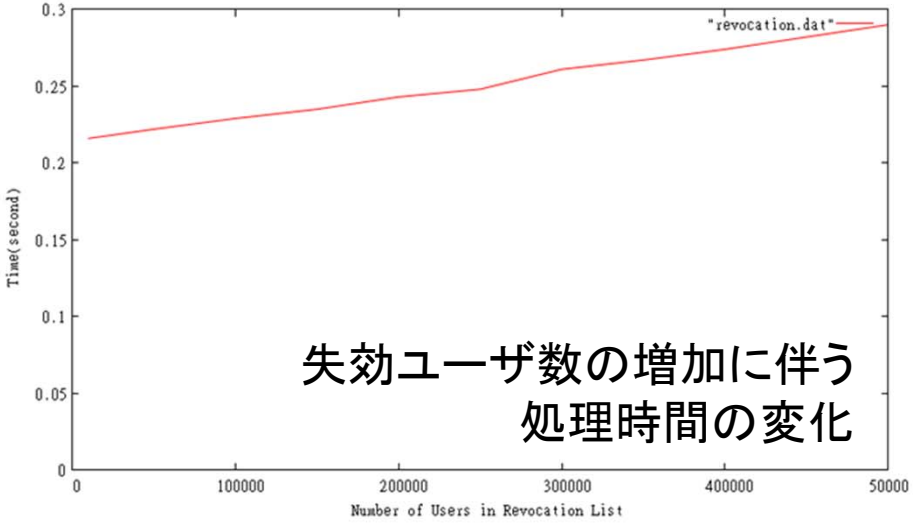
（評価システムの実行環境：OS=CentOS 5.5、CPU=Celeron 1.3G、Memory=768M）

- 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）

実用上問題がない性能を確保可能なことを確認



属性ポリシーの増加に伴う
暗号化処理時間の変化



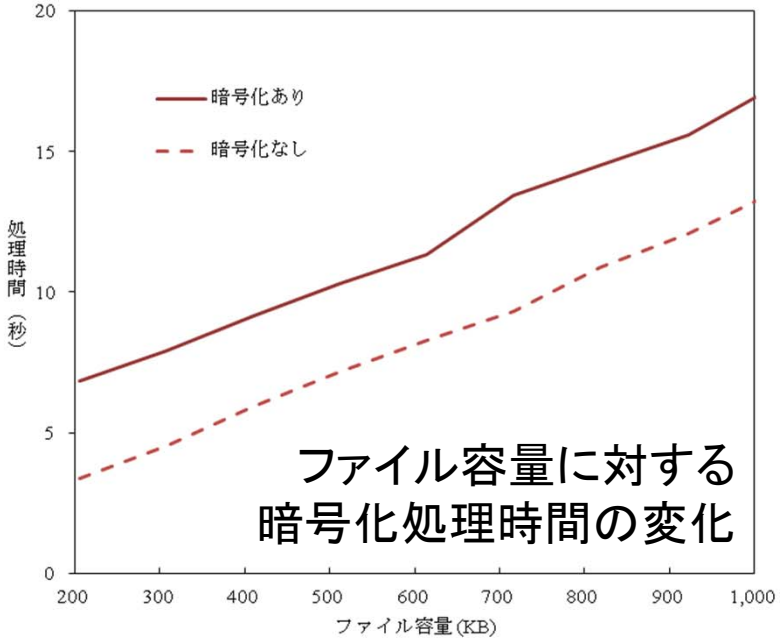
失効ユーザ数の増加に伴う
処理時間の変化

4. 成果、目標の達成度

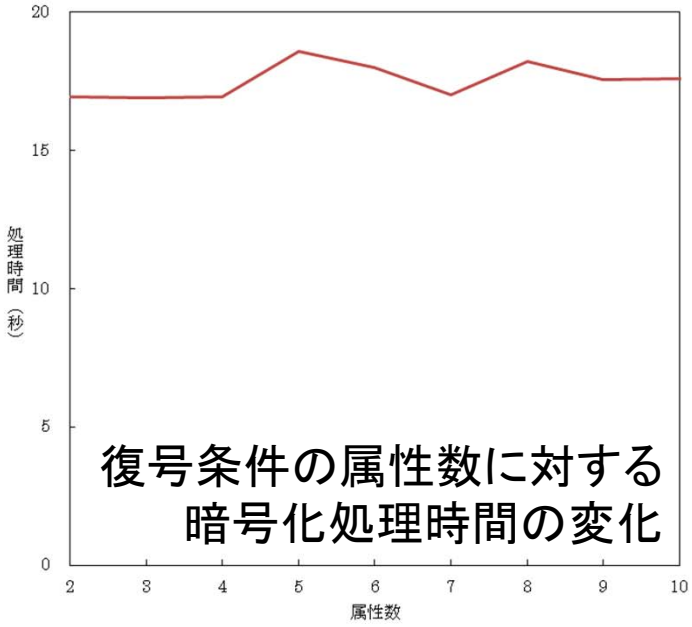
モデルシステムを対象とする性能測定結果

- 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。
  （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）

属性数が増えても処理に影響を及ぼさないことを確認



ファイル容量に対する
暗号化処理時間の変化



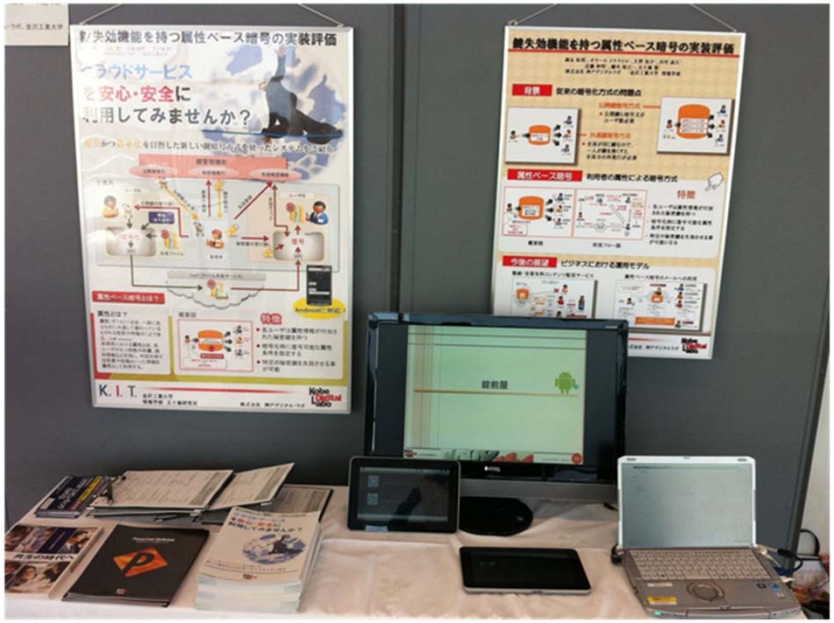
復号条件の属性数に対する
暗号化処理時間の変化

4. 成果、目標の達成度

成果に基づくデモンストレーションの実施

- コンピュータセキュリティシンポジウム（CSS) 2011（平成23年10月）
- クラウドコンピューティングEXPO（平成23年10月）

いずれもデモンステーションの会場にて、パンフレットを配布するとともに、成果の評価に関するアンケート調査を行い、一定の関心と評価を得ていることを確認した。

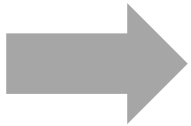


CSS 2011 におけるデモンストレーション

クラウドコンピューティングEXPOの
展示ブース

4. 成果、目標の達成度

研究開発のスケジュール

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. 事業化・波及効果

事業化計画

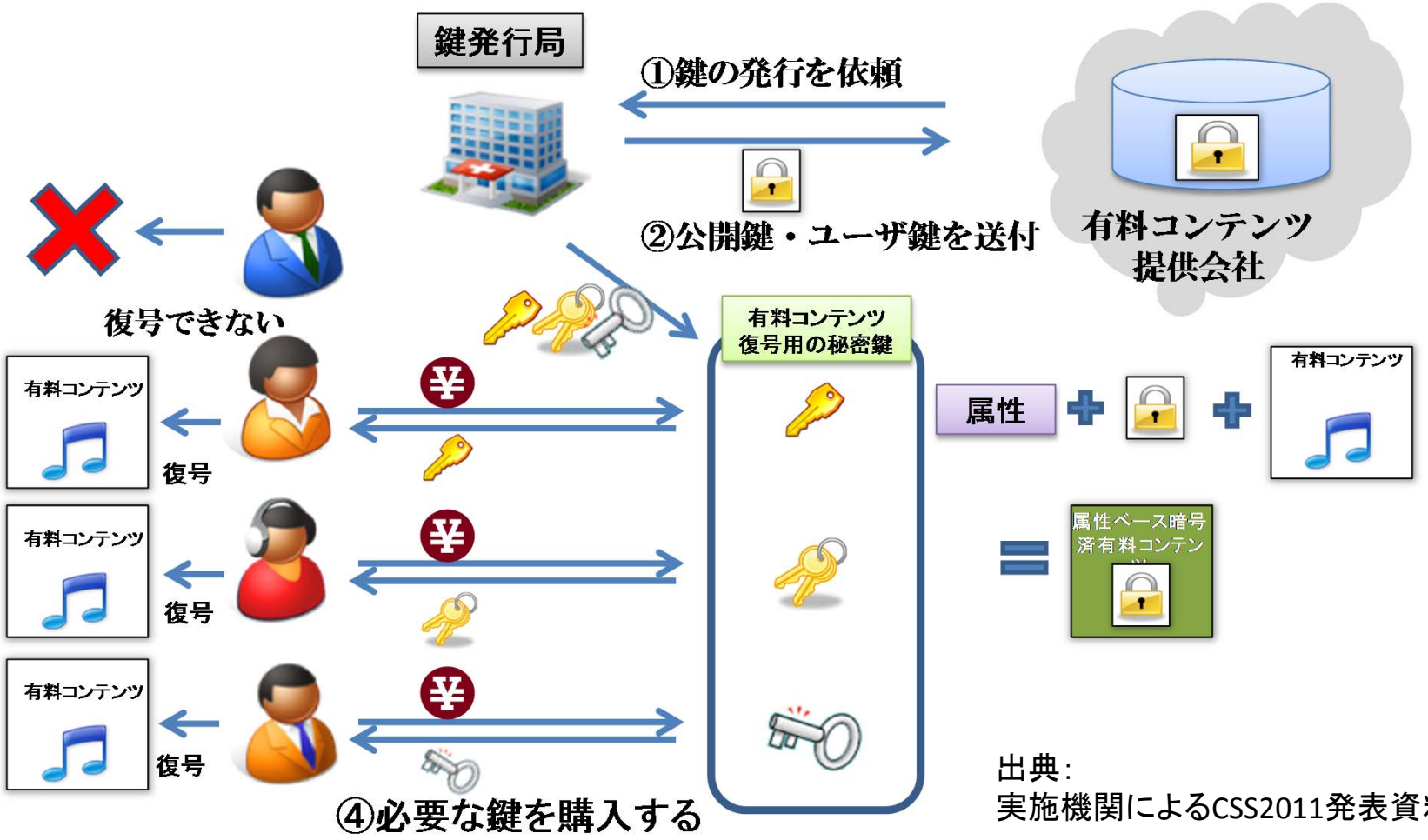
- 本研究の成果は大手機械メーカー及び大手通信事業者に採用され、属性ベース暗号を用いた実際のサービスへの実装に向けて活動中である。
- 各社への鍵発行システムの組み込み案件として、下記の金額による開発・保守業務の委託を受けて実施している。
  - 2012年度（2012年4月～2013年3月）約770万円
  - 2013年度（2013年4月～2014年3月）約1,500万円
- 並行して、現在サービス実装を行っている案件を拡張し、企業内の属性ベース暗号基盤を構築・販売するモデルを確立し、営業展開を行うことが計画されている。
- さらに、複数の企業を一括して1つの属性ベース暗号基盤で賄える仕組みを開発し、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。

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. 事業化・波及効果

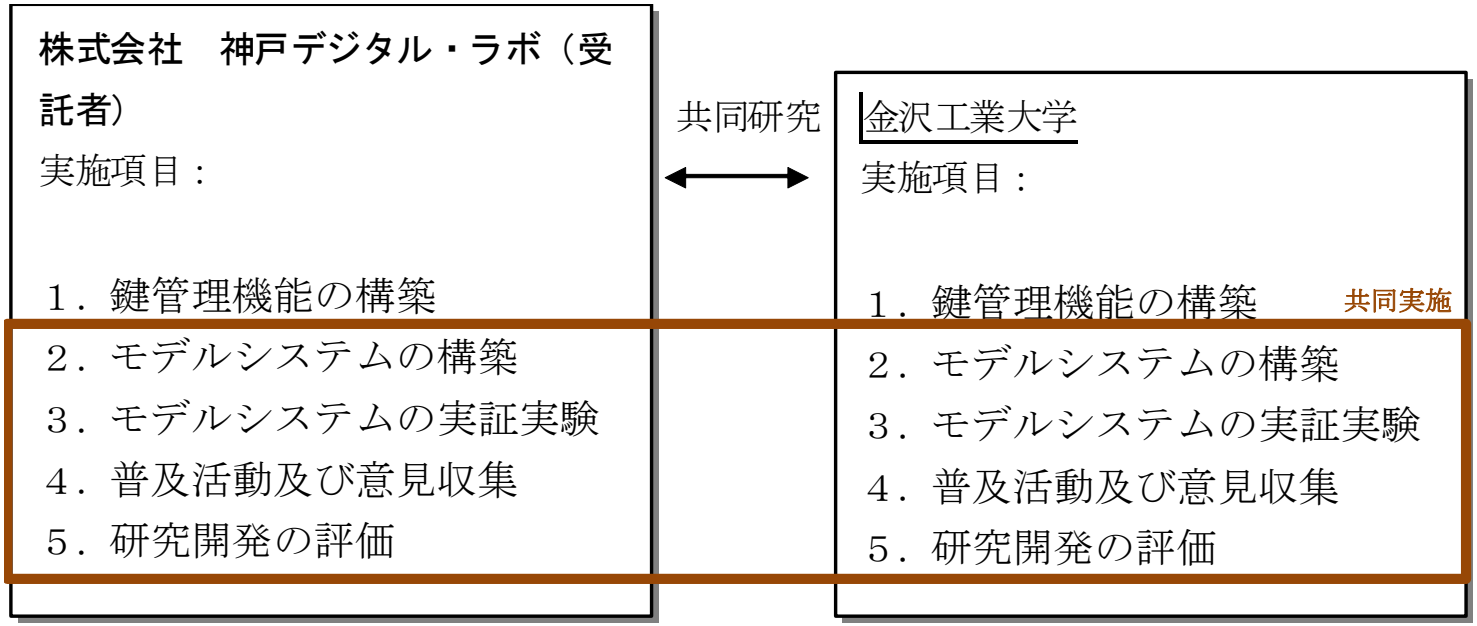
事業化イメージ（有料コンテンツ提供会社への鍵発行サービス例）



出典：
実施機関によるCSS2011発表資料

6. 研究開発マネジメント・体制等

実施体制



６．研究開発マネジメント・体制等

【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

【費用対効果】

- 本研究開発成果に基づくシステムは、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。
- 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。

【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

商務情報政策局情報セキュリティ政策室

実施機関：特定非営利活動法人統制技術研究機構

1．事業の概要

概　要	最近のクラウドサービス市場規模の拡大に合わせてBCP（事業継続計画）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。 本研究は、当初はクラウドコンピューティングサービスのBCPの妥当性検証の基準開発を第一の目標とし、「クラウドサービスベンダ並びにクラウドユーザ企業（法人）のためのBCP 妥当性検証基準」を2年間かけて開発することを目標とする計画であった。しかしながら、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、本研究の2年目への継続は適切ではないとの意見が示されたことを受けて、1年で事業を打ち切ることとなった。このため、成果物は平成22年度の完成を予定していた「クラウドベンダのためのBCP構築基準」の作成のみにとどまった。
実施期間	平成22年度 （当初の予定期間は2年間であったが、1年間で打ち切り）
予算総額	12.5百万円（委託）
実　施　者	特定非営利活動法人統制技術研究機構
プロジェクトリーダー	特定非営利活動法人統制技術研究機構　土屋慶三

2. 事業の目的、政策的位置づけ

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。

政策的位置づけ

本テーマは、事業公募に先立って公表された「国民を守る情報セキュリティ戦略」（平成22年5月11日公表）における以下の項目に対応する。

2. 新たな環境変化に対応した情報セキュリティ政策の強化

（1）国民生活を守る情報セキュリティ基盤の強化

③その他の基盤強化

クラウドコンピューティング化に対応した情報セキュリティ確保方策、標準化

（4）技術戦略の推進等

①情報セキュリティ関連の研究開発の戦略的推進等

３．目標

前述の目的の達成のため、以下の目標を設定した。

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

4. 成果、目標の達成度

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。

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	「クラウドサービスベンダ並びにクラウドユーザ企業（法人）のためのBCP 妥当性検証基準」の作成	左記の実現のために計画されていた4種類の基準のうち、平成22年度に実施された「クラウドベンダのためのBCP構築基準」が作成された。	－

（参考）1年間で打ち切りとなった理由

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。

4. 成果、目標の達成度

研究開発のスケジュール

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	

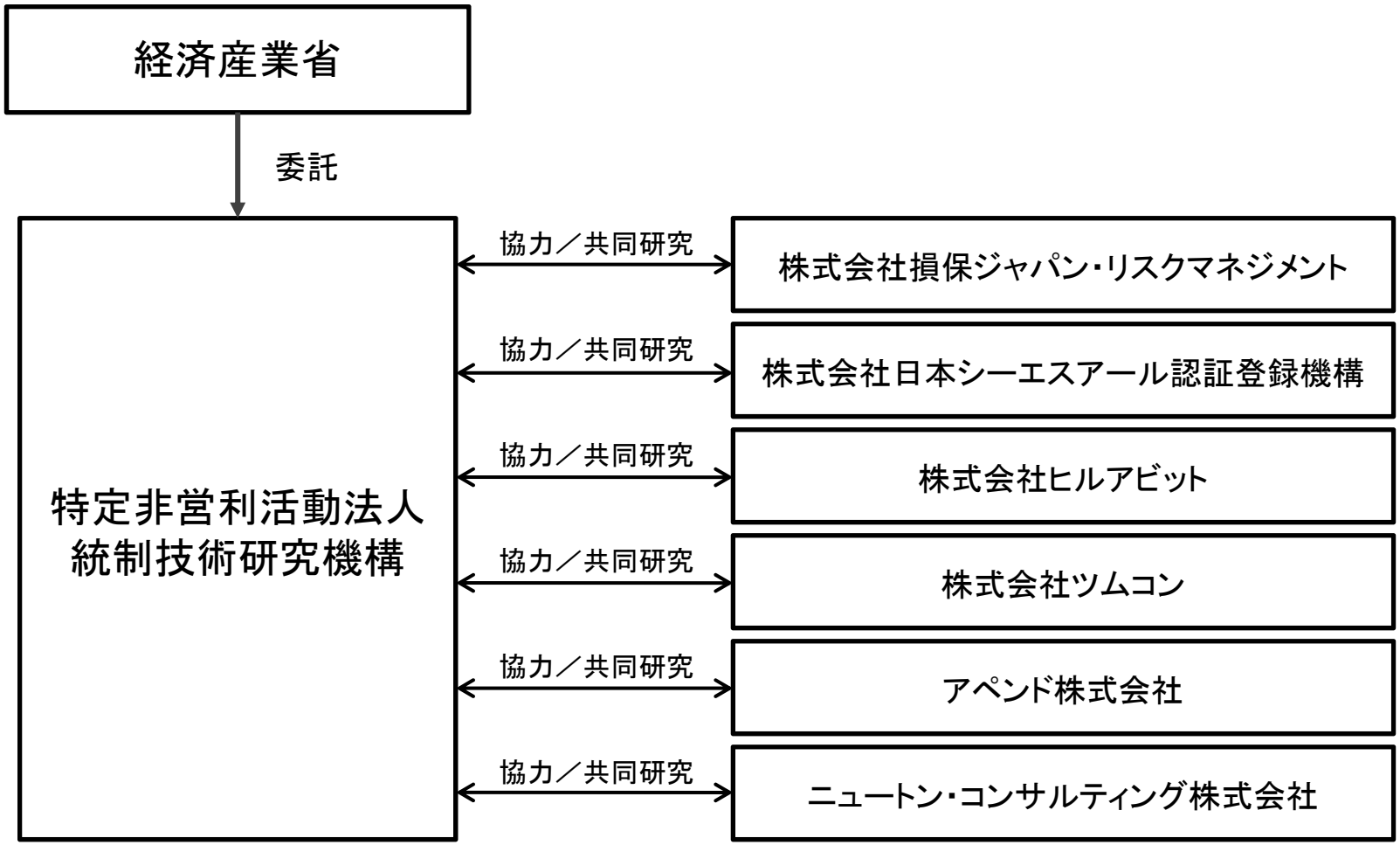
５．事業化・波及効果

事業化

- 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。

6. 研究開発マネジメント・体制等

実施体制



６．研究開発マネジメント・体制等

【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

【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。

【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。

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

商務情報政策局情報セキュリティ政策室

実施機関：エヌ・ティ・ティ・コミュニケーションズ株式会社

1．事業の概要

概　要	クラウドサービス利用時のコンプライアンス向上に向け、クラウド基盤利用者自身によるデータの管理・監督を可能にする下記の2つの機構についての研究開発を実施した。 a. ケーパビリティインジェクション機構：クラウドに預けたデータへのアクセスに必要となる権限を安全にクラウド内のゲストOSに通知することにより、利用者自身による機密データの管理・監督を可能とする機構 b. ペアリング機構：ゲスト環境とホスト環境とが予め許可された組み合わせで動作していることを保証することにより、クラウド事業者による不正なゲスト環境のコピーを防止する機構 しかしながら、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、本研究の2年目への継続は適切ではないとの意見が示されたことを受けて、1年で事業を打ち切ることとなった。このため、成果物は上記2つの機能のプロトタイプとその評価結果のみにとどまった。
実施期間	平成22年度 （当初の予定期間は3年間であったが、1年間で打ち切り）
予算総額	29.4百万円（委託）
実　施　者	エヌ・ティ・ティ・コミュニケーションズ株式会社
プロジェクトリーダー	エヌ・ティ・ティ・コミュニケーションズ株式会社　先端IPアーキテクチャセンタ　認証・セキュリティプロジェクト担当部長　森　直彦

2. 事業の目的、政策的位置づけ

事業の目的

PaaS型のクラウドコンピューティングサービス（以下、「クラウドサービス」という。）が普及しつつあるが、PaaSの基盤である仮想化環境では、クラウド事業者が特権ユーザであり、利用者が預けたデータを含め、あらゆるリソースにアクセス可能であることが、利用者の不安を増長している。こうしたデータ管理の実情を考慮すれば、個人情報の保護に関する法律において義務づけられている、個人情報取扱者による、個人情報の取扱の委託先への必要かつ適切な監督の実現性にも疑問が生ずる。そこで、クラウドサービスを利用しつつ、かつ利用者自身が個人情報や機密情報の管理監督を実施可能とするための機構を新規開発することで、クラウド利用者が預けたデータをクラウド利用者自身が管理監督することを可能とする。こうした研究開発を通じて、利用者から見たクラウドサービスをより安全で利用しやすいものにすることにより、我が国のクラウドサービス事業の発展に寄与する。

政策的位置づけ

本テーマは、事業公募に先立って公表された「国民を守る情報セキュリティ戦略」（平成22年5月11日公表）における以下の項目に対応する。

2. 新たな環境変化に対応した情報セキュリティ政策の強化

（1）国民生活を守る情報セキュリティ基盤の強化

③その他の基盤強化

クラウドコンピューティング化に対応した情報セキュリティ確保方策、標準化

（4）技術戦略の推進等

①情報セキュリティ関連の研究開発の戦略的推進等

3. 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。

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。

4. 成果、目標の達成度

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3年間のところ、初年度のみの実施にて中止となった。

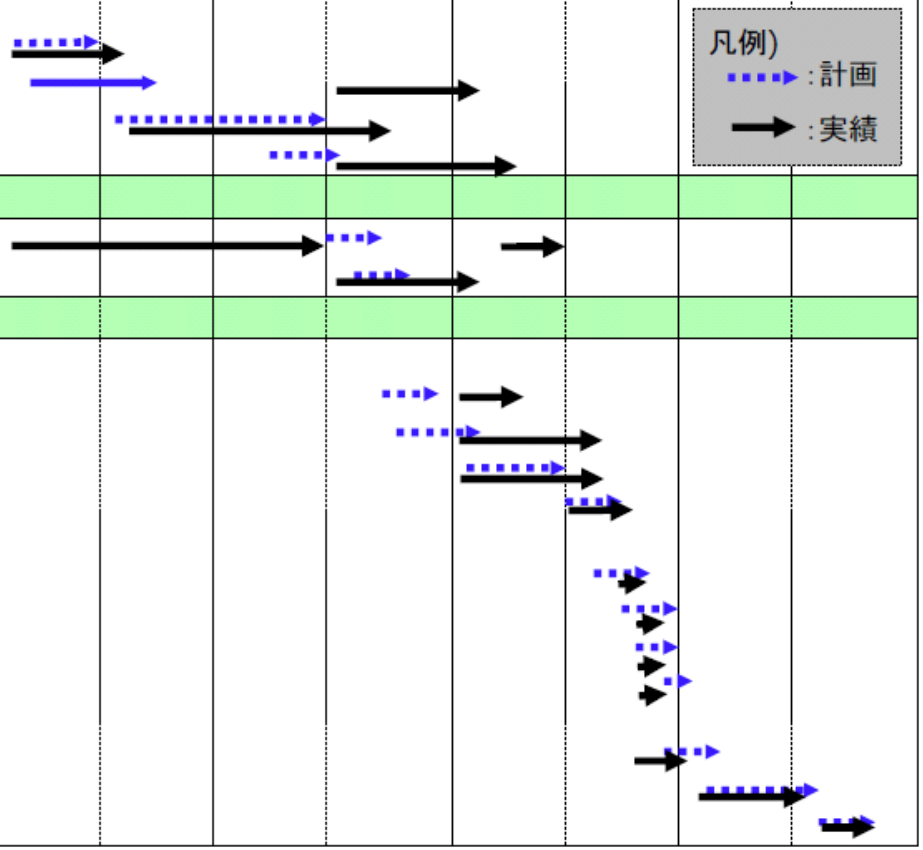
※ 1年間で打ち切りとなった理由については、5. 事業化・波及効果のページを参照

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. 成果、目標の達成度

研究開発のスケジュール

項目		平成22年度			
		12月	1月	2月	3月
1	現状分析および要件定義				
1.1.	現状分析による非機能要件定義				
1.1.1.	ドメイン定義				
1.1.2.	パフォーマンスベースライン要求定義				
1.2.	機能要件定義				
1.3.	要件定義書作成				
2	実現方式原理モデル決定				
2.1.	実現方式妥当性検討および原理モデル確定				
2.2.	実現方式原理モデル説明書作成				
3	プロトタイプ実装				
3.1.	設計				
3.1.1.	基本認証環境モックアップ				
3.1.2.	仮想化機構エミュレータ				
3.1.3.	ゲストOSエミュレータ				
3.1.4.	機能検証用コマンド群				
3.2.	実装				
3.2.1.	基本認証環境モックアップ				
3.2.2.	仮想化機構エミュレータ				
3.2.3.	ゲストOSエミュレータ				
3.2.4.	機能検証用コマンド群				
3.3.	有効性検証				
3.3.1.	評価仕様書作成				
3.3.2.	評価実施				
3.3.3.	評価書作成				



5. 事業化・波及効果

事業化

- 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。

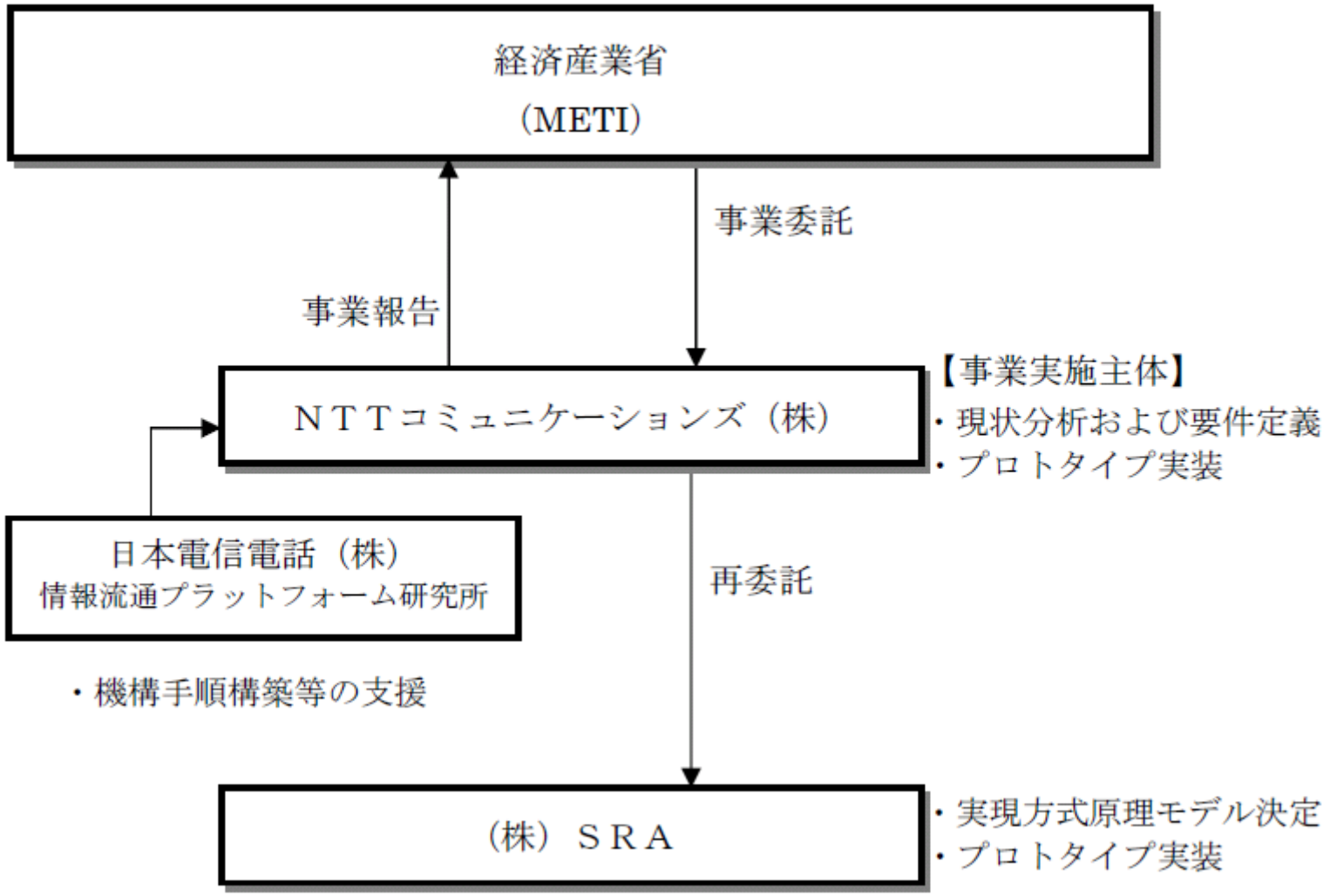
（参考）１年間で打ち切りとなった理由

- 平成２３年３月に開催し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、実施機関に対して以下の評価が行われたことによる。

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。

6．研究開発マネジメント・体制等

実施体制



6. 研究開発マネジメント・体制等

【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

【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。

【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。

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

実施機関：電子商取引安全技術研究組合

1．事業の概要

概　要	国内でICカードのセキュリティ評価を行う体制を構築するため、必要な技術開発や環境整備の取組として、以下を実施した。 (1) 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 ②評価ツールの開発 (2) 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 ②委託事業終了後の共同利用設備の運営に関する検討 (3) セキュリティ評価を行うために必要な人材育成 ①人材育成 ②育成した人材による試行評価 (4) 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 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 ③チップセキュリティ評価のための手順の調査
実施期間	平成21年度～平成23年度（3年間）
予算総額	6.6億円（委託） 平成21年度2.6億円　平成22年度3.0億円　平成23年度1.0億円
実　施　者	電子商取引安全技術研究組合
プロジェクト リーダー	電子商取引安全技術研究組合　専務理事　植村泰佳

2. 事業の目的、政策的位置づけ

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。

政策的位置づけ

本テーマは、事業公募に先立って公表された「国民を守る情報セキュリティ戦略」（平成22年5月11日公表）における以下の項目に対応する。

2. 新たな環境変化に対応した情報セキュリティ政策の強化

（1）国民生活を守る情報セキュリティ基盤の強化

③その他の基盤強化

安全な電子商取引の推進

（4）技術戦略の推進等

①情報セキュリティ関連の研究開発の戦略的推進等

3. 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。

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。

4. 成果、目標の達成度

前ページに設定した目標について、以下の通り達成した。

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（現：株式会社ECSEC Laboratory）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

4. 成果、目標の達成度

研究開発のスケジュール

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. 事業化・波及効果

事業化

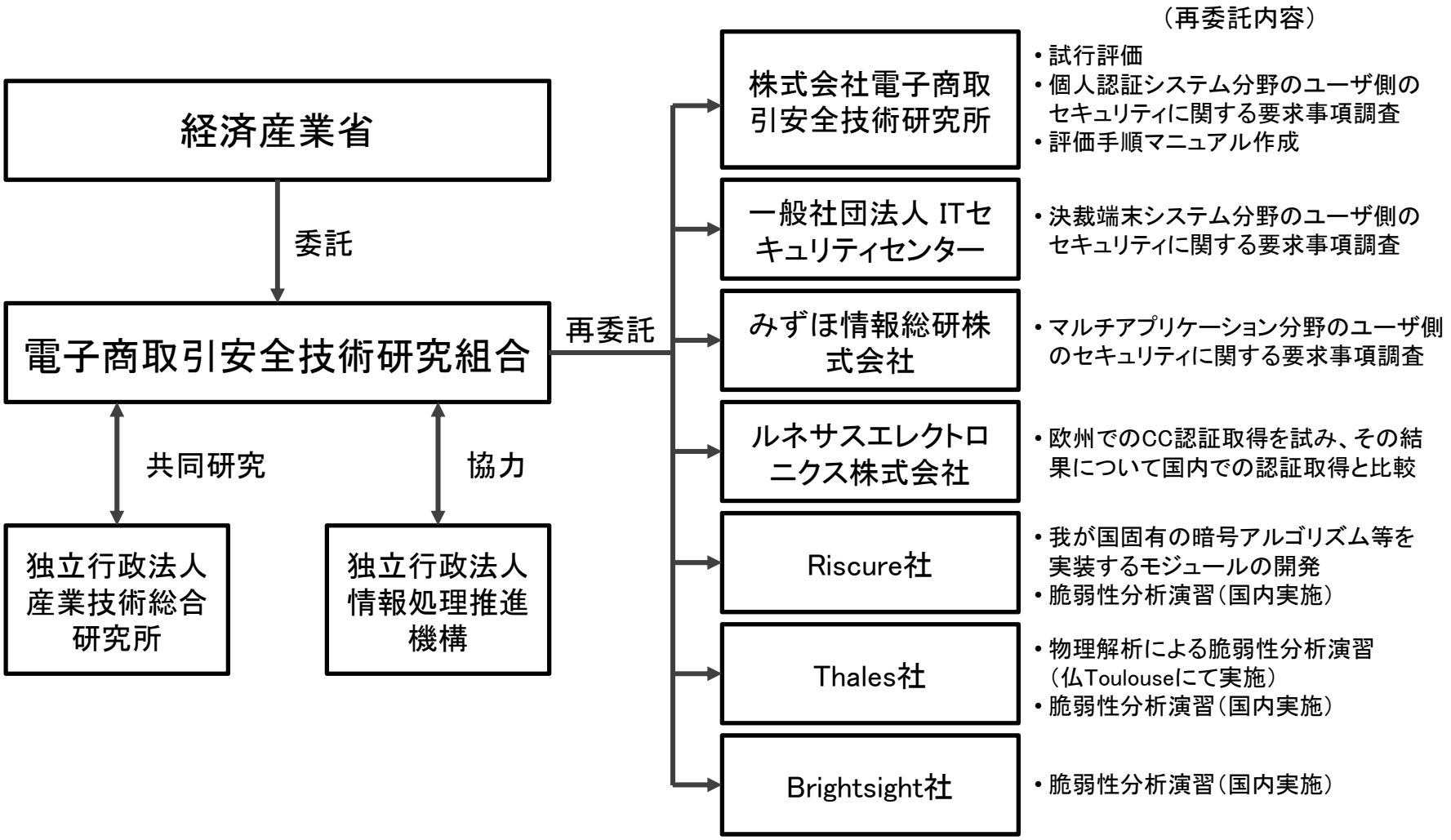
- 本事業で構築した共同利用設備をはじめとする成果は、現在の株式会社ECSEC Laboratory（旧社名：株式会社電子商取引安全技術研究所）に引き継がれ、平成24年9月、国内におけるICカード等ハードウェアのセキュリティ評価体制が確立した。
- 同社はハードウェア侵入テスト機関を内包して運用している。当該ハードウェア侵入テスト機関は、同社内のCC（Common Criteria）評価機関だけでなく、他社のCC評価機関に対してハードウェアCC評価における侵入テストサービスを提供することを可能とした。これは、国内における他のCC評価機関が個別に設備を保有することは資金面を考慮すると難しいため、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。

波及効果

- 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。
- 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。
- 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。
- 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。

6. 研究開発マネジメント・体制等

実施体制



６．研究開発マネジメント・体制等

【資金配分】

（単位：億円）

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

【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。

【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

商務情報政策局情報セキュリティ政策室

実施機関：ケイレックス・テクノロジー株式会社

目　次

1．事業の概要

概　　要	本研究開発は、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とともに、国内企業の技術の底上げと国際競争力の向上に寄与する。
実施期間	平成23年度～平成25年度　（3年間）
予算総額	306百万円（委託事業） （平成23年度：120百万円　平成24年度：125百万円　平成25年度：62百万円）
実 施 者	ケイレックス・テクノロジー株式会社
プロジェクトリーダー	畑田　智子　　ケイレックス・テクノロジー株式会社 システム開発部 プロジェクトマネージャ

2. 事業の目的

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。

事業の政策的位置付け

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。

３．目標

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。

	要素技術	目標・指標	妥当性・設定理由・根拠等
課題１	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エ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
課題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 ユーザー 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

	要素技術	目標・指標	妥当性・設定理由・根拠等
課題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
課題４	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

	要素技術	目標・指標	妥当性・設定理由・根拠等
課題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	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
課題６	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	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

4. 成果、目標の達成度

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。

	要素技術	目標・指標	成　果	達成度
課題1	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
課題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

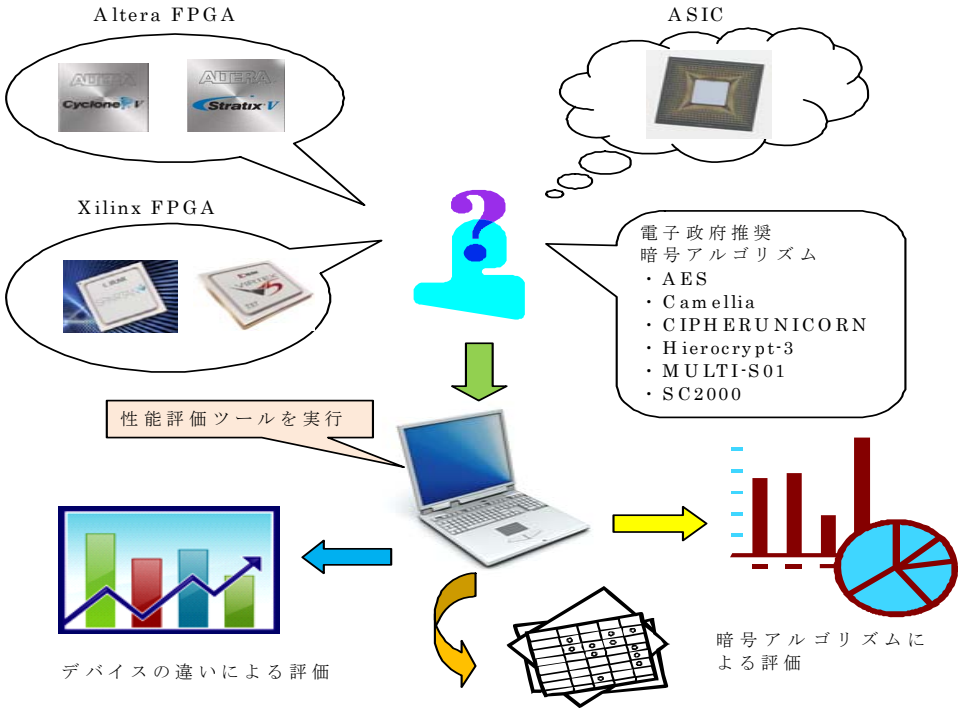
	要素技術	目標・指標	成　果	達成度
課題3	フォールト攻撃耐性評価ツール及び試験装置の開発	クロックや電源にグリッチを挿入してエラーを発生させる試験環境を構築する	・クロック信号、リセット信号、電源それぞれに非常に細いパルスを混入するグリッチ機能を開発した ・その環境を使用して評価実験を行い、検証のため解析プログラムを開発した	達成
課題4	侵襲攻撃耐性評価環境の構築	パッケージを開封してLSI内部の動作を直接操作する侵襲攻撃評価を行う環境を構築する	・外乱誘発装置としてレーザー照射装置と電磁界照射装置を開発した ・LSIのCADデータを用いて照射座標を制御したり、フォールトの発生状況を描画するCADナビゲーションシステムを開発した	達成

	要素技術	目標・指標	成　果	達成度
課題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	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
課題6	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	・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 ・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	達成

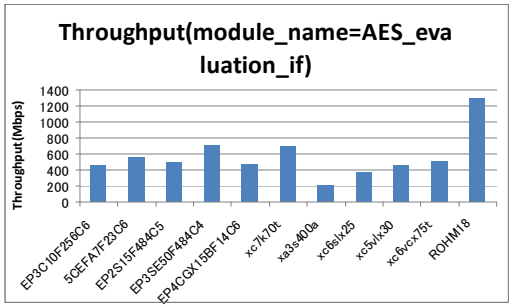
課題1:暗号ハードウェア実装性能評価ツールの開発

・性能評価の自動化
対象は、代表的な実装（Xilinx FPGA、Altera FPGA、ASIC）をターゲットとした。
性能評価項目は、回路規模、処理速度（スループット）、消費電力など。
電子政府推奨の暗号アルゴリズムを利用して動作実験を実施した。

・可視化ツールの開発
性能評価結果から自動的をグラフを出力。
同一の暗号アルゴリズムを異なるハードウエアに実装した場合の比較や、逆に同一のハードウエアに異なる暗号アルゴリズムを実装した時の比較など、評価内容に応じて出力するグラフの変更が可能。



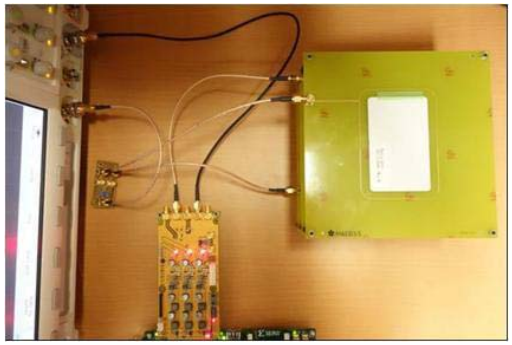
module	vender	familiy	device	slice	area	max clock frequency[MHz]	power [mW]	input blocks[bits]	cycle	throughput [Mbps]
AES_evaluation_if	Altera	Cyclone3	EP3C10F256C6	6721		87.4	59.76	512	100	447
AES_evaluation_if	Altera	Cyclone5	5CEFA7F23C6	2634		109.58	129.81	512	100	561
AES_evaluation_if	Altera	Stratix2	EP2S15F484C5	2825		97.04	325.1	512	100	497
AES_evaluation_if	Altera	Stratix3	EP3SE50F484C4	2767		138.48	435.68	512	100	709
AES_evaluation_if	Altera	Stratix5	EP4CGX15BF14C6	6490		91.28	66.92	512	100	467
AES_evaluation_if	Xilinx	Kintex7	xc7k70t	877		135.08	80.06	512	100	692
AES_evaluation_if	Xilinx	Spartan3a	xa3s400a	2983		41.764	68.39	512	100	214
AES_evaluation_if	Xilinx	Spartan6	xc6slx25	778		73.198	72.19	512	100	375
AES_evaluation_if	Xilinx	Virtex5	xc5vlx30	848		88.277	448.48	512	100	452
AES_evaluation_if	Xilinx	Virtex6	xc6vcx75t	886		98.532	1333.2	512	100	506
AES_evaluation_if	ROHM		ROHM18	429676		252.525	2.5834	512	100	1293

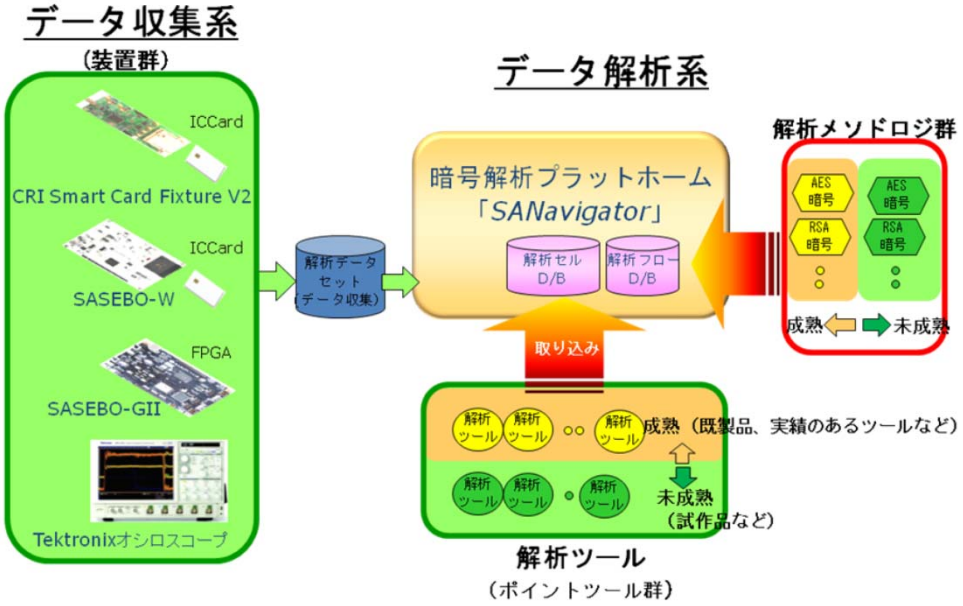


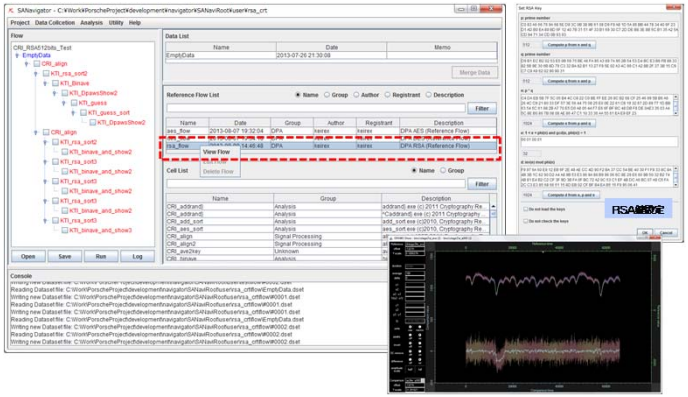
課題2:サイドチャネル攻撃耐性評価ツールの開発

・サイドチャネル攻撃耐性評価ツール(SANavigator)の開発
主に解析に必要なデータ収集を行う機能と、収集したデータを使用して暗号解析を行う機能で構成される。
複数の攻撃手法、実装形態、計測機器から選択されたターゲットに対して、統合されたグラフィカル
ユーザーインタフェースから操作可能とした。
次々と現れる新たな攻撃手法や対策手法に対応するために、実行履歴の管理、ノウハウの共有化が重要
であるため、評価者の思考支援、ノウハウの蓄積(資産化)、容易な機能拡張性の三つをコンセプトとした。

・非接触ICカード評価プラットフォームの設計
サイドチャネル攻撃の耐性評価に適した非接触IC カードを評価する
装置を作製し、その装置を使用して動作実験を行った。
その結果、歪みの少ない良好な電磁界波形を得ることができた。



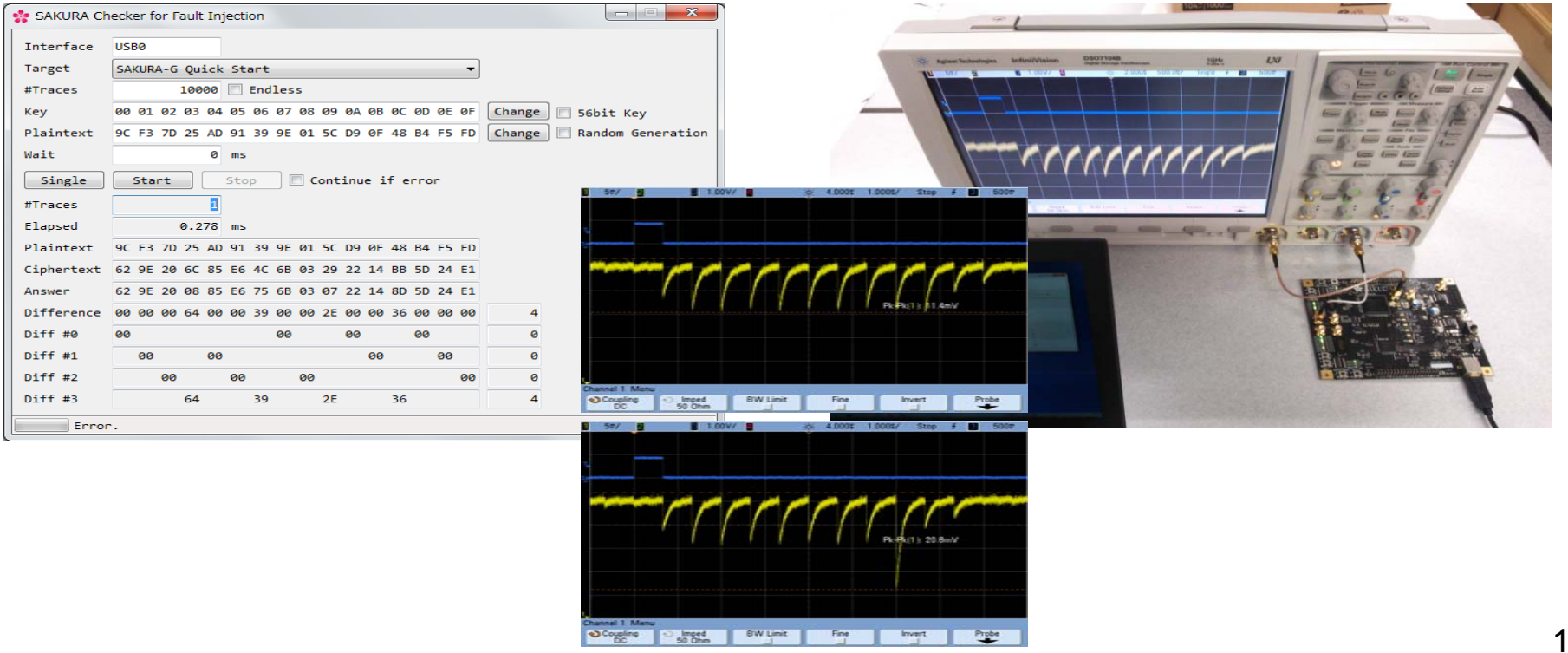




課題3:フォールト攻撃耐性評価ツール及び試験装置の開発

・グリッチ機能の開発
標準評価ボードであるSASEBO-GIIやSAKURA-Gを用いてFPGAをターゲットとしたフォールト評価環境を、SASEBO-Wを用いてICカードをターゲットとしたフォールト評価環境を構築した。

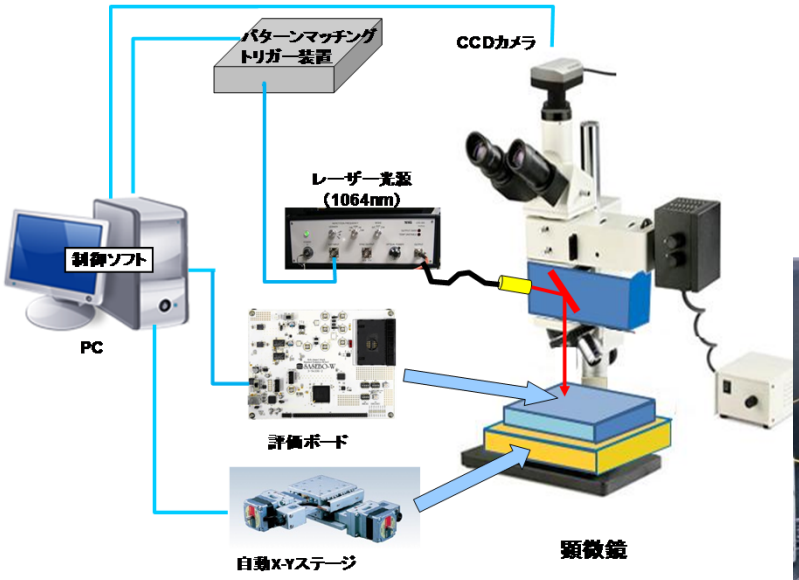
・クロックグリッチを与える評価実験の実施
構築したフォールト評価環境を使って実験を行い、グリッチを与えることにより誤動作を発生させる事ができた。また、誤作動した結果を使用して鍵を導出する解析プログラムを開発し、少ない処理数(約20組の暗号文)で鍵がすべて導出できることを実証した。

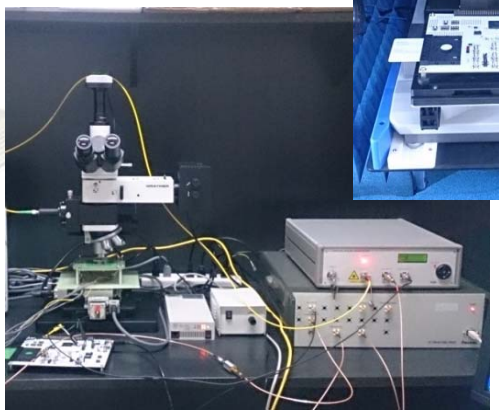


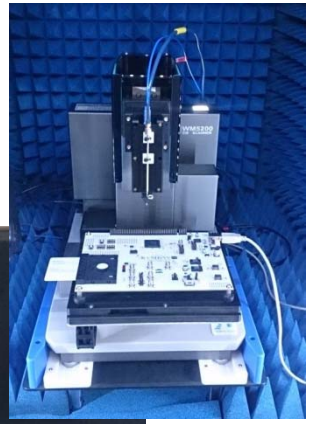
課題4:侵襲攻撃耐性評価環境の構築

・レーザー照射装置と電磁波照射装置の開発
レーザー照射装置は、商用化されている既存のレーザー照射装置の評価を行い、レーザー出力の安定度が低いことやステージの精度に問題があることを明らかにし、それらを改善した装置を作製した。
また、消費電力等の波形を連続的にモニタして特徴的な波形でトリガを発生させるパターンマッチングトリガ装置を開発し、侵襲攻撃中の基準時刻を合わせることを可能にした。
電磁波照射装置は、周波数を調整可能な装置を開発した。

・CADナビゲーションシステムの開発
評価対象の顕微鏡画像とそのレイアウト設計情報との対比を行い、照射座標を制御したり、フォールトの発生状況をカメラ画像に重ねて描画するCADナビゲーションシステムを開発し、評価の効率化を実現した。



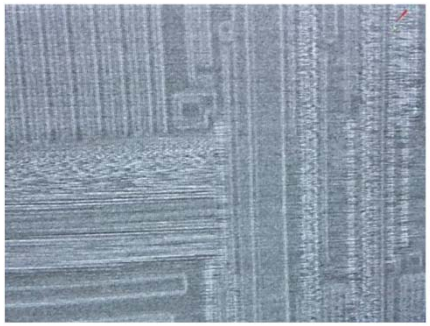




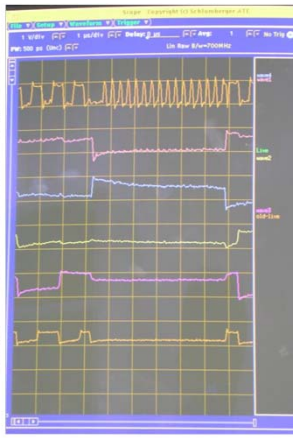
課題5:集積回路解析技術によるLSI内部動作解析及び先端技術調査

・電子線プローブにより内部信号の観測
130nm CMOSプロセスによる暗号LSIに対して、電子線プローブにより内部信号を観測した。
これにより、解析対象LSIを先端LSI解析装置で動作させることが可能となった。
また、接触型ICカード内のチップの動作を測定できる測定系を構築し、この測定系を使用して電子線プローブを用いた内部電位コントラスト像の観測と内部信号波形の観測を行い、動作中のICカードチップの波形を観測できることを示した。

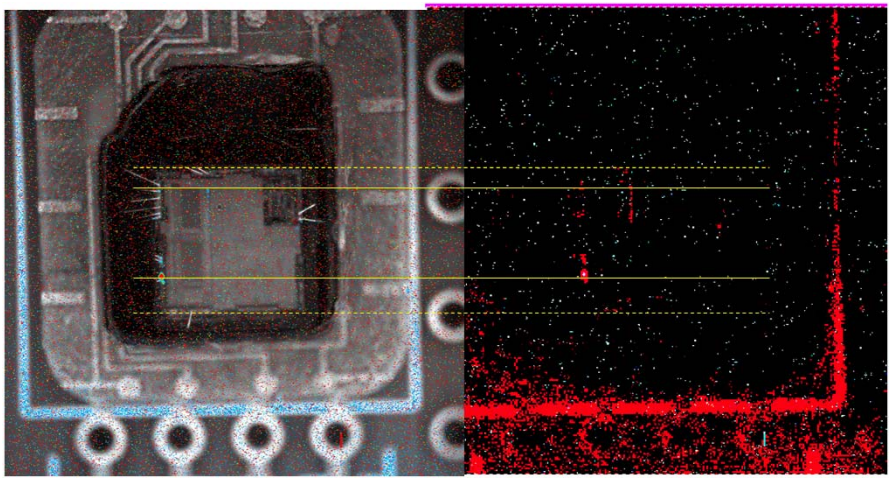
・発光解析と電子線プローブ観測結果との対比
同一のチップに対して発光解析を行ったところ、電子線プローブでの観測結果とよい対応関係を示していることを確認した。この結果から、電子線プローブ及び表面発光解析技術を用いることにより、ある程度のLSI 動作解析が可能であることが示された。



(a)



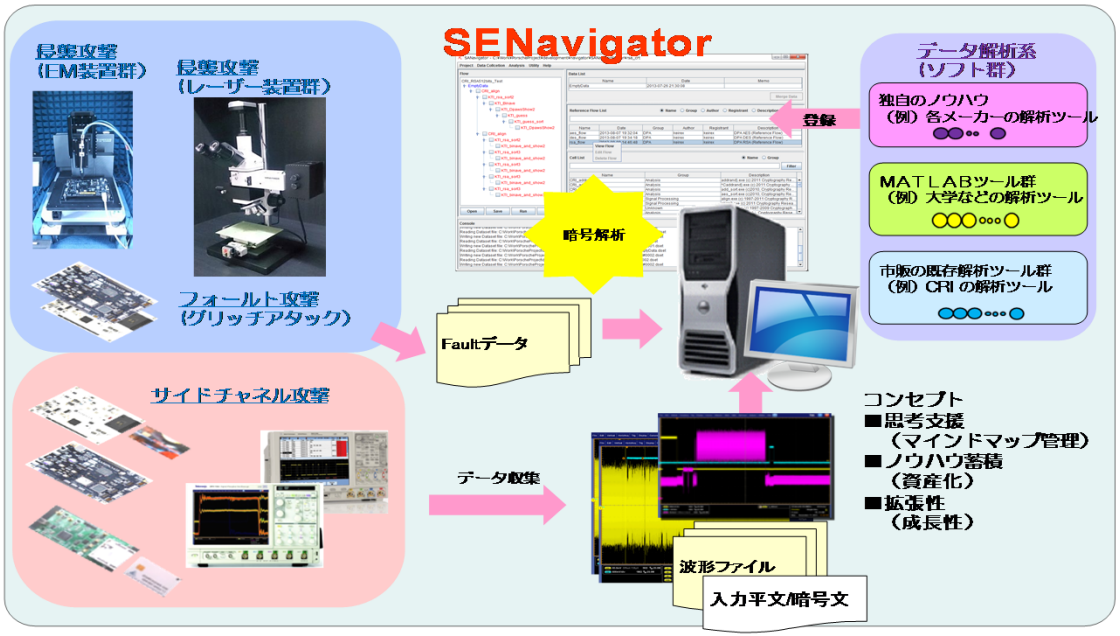
(b)

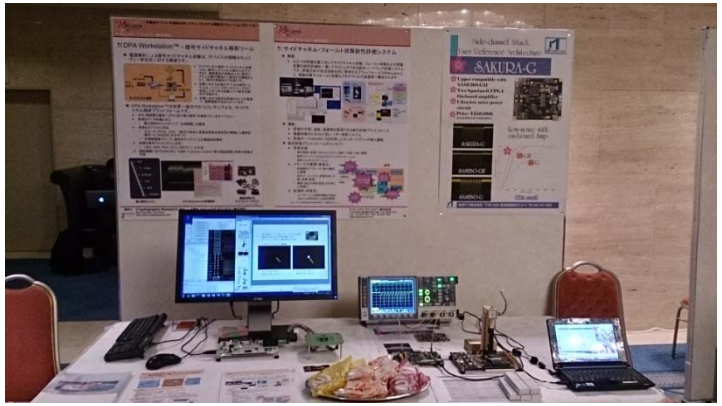


課題6:統合ハードウェア評価プラットフォームの構築

・評価技術のパッケージング化
　これまでの評価技術の成果をまとめ、サイドチャネル攻撃、フォールト攻撃など評価手法ごとに
　装置やツール類を整理・取りまとめ（パッケージング）を行い、使用用途に応じた販売を計画している。

・ひとつの評価対象に対して試行される複数の解析評価を統合するツール（SENavigator）の開発
　評価対象（TOE）毎にプロジェクト情報やユーザー情報、データ情報を保持したり、履歴を参照、検索する
　機構を開発することにより、統合ハードウェア評価プラットフォームを構築した。
　これにより、ひとつの評価対象に対して、サイドチャネル攻撃からフォールト攻撃、侵襲攻撃までを網羅した
　解析評価を統合して管理する事が可能となる。





研究開発のスケジュール

	年度	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
課題１	暗号ハードウェア実装性能評価ツールの開発	AES回路設計・SASEBO-GII上へ実装 Xilinx用論理合成スクリプト開発	実装性能評価ツールの開発 視覚化ツール開発・統合	評価技術のパッケージ化
課題２	サイドチャネル攻撃耐性評価ツールの開発	GUI開発・仕様策定等	統合解析環境GUIの初期開発 非接触ICカードRWボードの開発・実験	公開鍵暗号評価 MATLABでの解析 評価技術のパッケージ化

	年度	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
課題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・電源制御機構開発　等	グリッチ制御機能のGUIへの統合 フォールト攻撃解析プログラムの開発	パターンマッチング 評価ボード 評価技術のパッケージ化
課題４	侵襲攻撃耐性評価環境の構築	レーザー機構及び電磁照射装置の設計・制作 CADリンク仕様策定	ステージ調整機能の開発　等 ナビゲーション機能・フォールト注入機能の開発　等	EM・レーザー計測 評価技術のパッケージ化

	年度	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
課題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・EBテスタ試運　等 プロービングによる波形観測	LSI解析装置によるデータ収集・解析 ICカードデータ取得・解析	
課題６	統合ハードウェア評価プラットフォームの構築			統合プラットフォーム

5. 事業化、波及効果

（1）事業化

・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。

・開発成果を統合した環境「統合ハードウエ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。

・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。

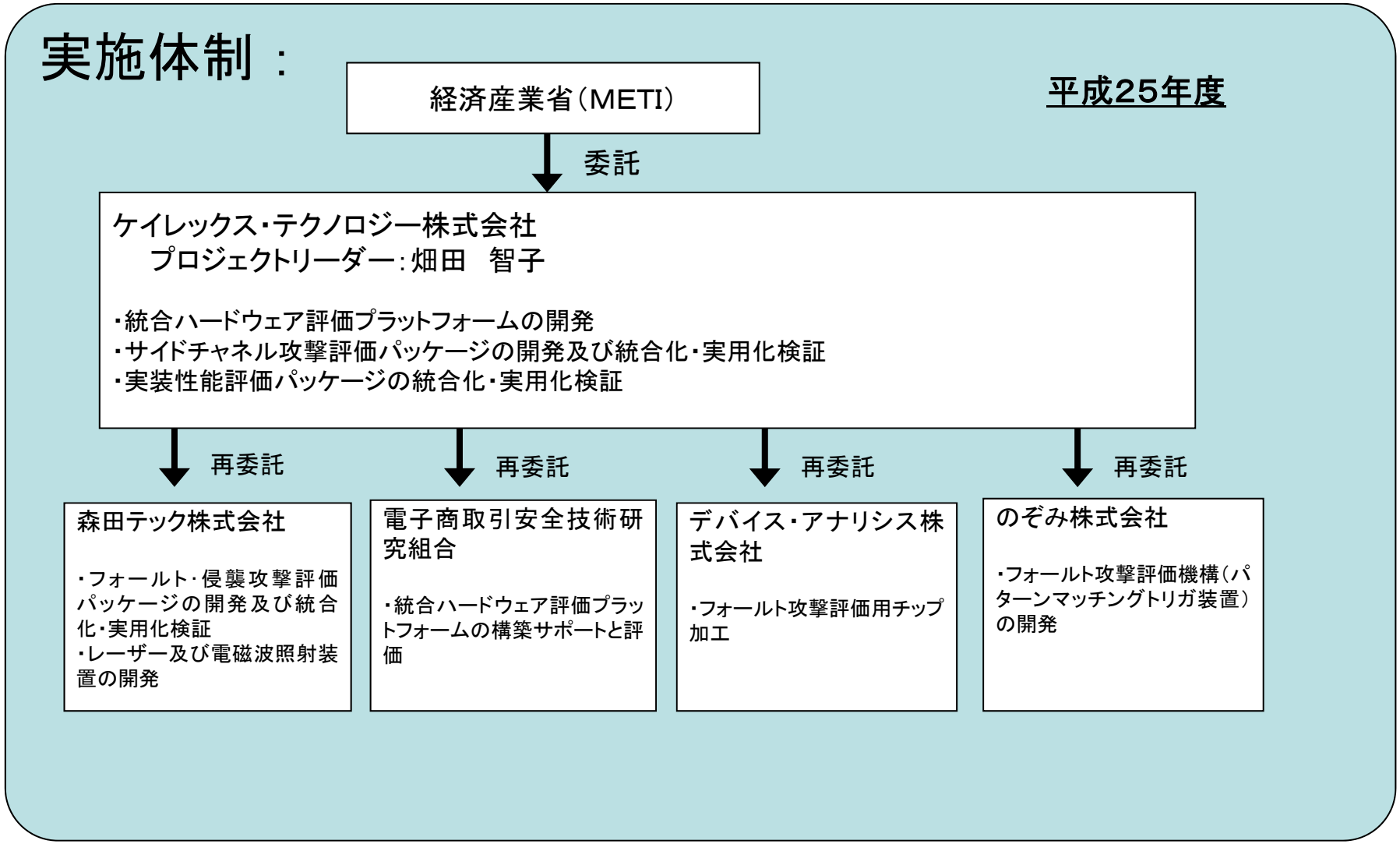
・レーザー照射装置、電磁波照射装置などは、統合環境に組み込まれた形の商品化だけでなく、それぞれの用途に応じた商品として販売を計画している。

（2）波及効果

・統合ハードウエ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。

・レーザー照射、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照射装置、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。

6. 研究開発マネジメント・体制等



実施体制：

経済産業省（METI）

平成24年度

委託

ケイレックス・テクノロジー株式会社
プロジェクトリーダー：札抜　宣夫

・サイドチャネル攻撃及びフォールト攻撃の統合解析環境GUIの開発

再委託

森田テック株式会社

・非接触ICカードR／Wボード開発及び評価
・レーザー及び電磁波照射装置開発
・フォールト攻撃用ステージ制御機構開発

再委託

東京大学

・先端解析装置によるLSI評価技術開発
・ICカード及びFPGAに実装したSW及びHW動作解析

再委託

横浜国立大学

・フォールト攻撃実験及びデータの解析

再委託

電子商取引安全技術研究組合

・解析ツール開発コンサルテーション
・ICカード解析作業

再委託

のぞみ株式会社

・フォールト攻撃評価機構開発

再委託

パステル・ネットワークス株式会社

・制御ソフトウェア等のコーディング

再委託

上海淡易軟件有限公司

・暗号LSI、FPGA実装加工

実施体制：

平成23年度

経済産業省（METI）

委託

ケイレックス・テクノロジー株式会社
プロジェクトリーダー：札抜 宣夫

・サイドチャネル攻撃及びフォールト攻撃用の統合解析ツールの開発

再委託

森田テック株式会社

・レーザー・ステーションの設計・試作
・電磁波照射装置の設計・試作
・制御ソフトウェア開発

再委託

東京大学

・先端LSI解析装置による安全性評価の研究

再委託

独立行政法人
産業技術総合研究所

・暗号ハードウェア性能評価
・非接触ICカード評価ボード開発

6. 研究開発マネジメント・体制等

【資金配分】

（単位：百万円）

年度	23	24	25	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
合計	119．8	125．0	61．5	306．3

【費用対効果】

・開発成果を統合した「統合ハードウエ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。

・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レーザー照射装置、電磁波照射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。

【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であり、計画の変更は不要であった。

新規産業創造技術開発費補助金
（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））

商務情報政策局情報セキュリティ政策室

実施機関：

技術研究組合制御システムセキュリティセンター

目　次

1. 事業の概要

概　　要	我が国の重要インフラのセキュリティ向上、インフラシステムの輸出強化、および東日本大震災からの復興を念頭に置いて、宮城県多賀城市とお台場にまたがるサイバーセキュリティテストベッド（セキュリティを評価検証する施設の意味、以下、CSS-Base6）を構築する。本事業では、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、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。
実施期間	平成24年度 （1年間）
予算総額	20.1億円（補助金） 平成23年度補正：20.1億円
実 施 者	技術研究組合制御システムセキュリティセンター （英語名称 Control System Security Center; 略称 CSSC）
プロジェクトリーダー	理事長　新 誠一

2. 事業の目的・政策的位置付け

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。

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、当該炎症施設において、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。

3. 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。

4. 成果、目標の達成度

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

事業の成果：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

◯みやぎ復興パークに、国内唯一のサイバーセキュリティテストベッドを構築した。

◯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。

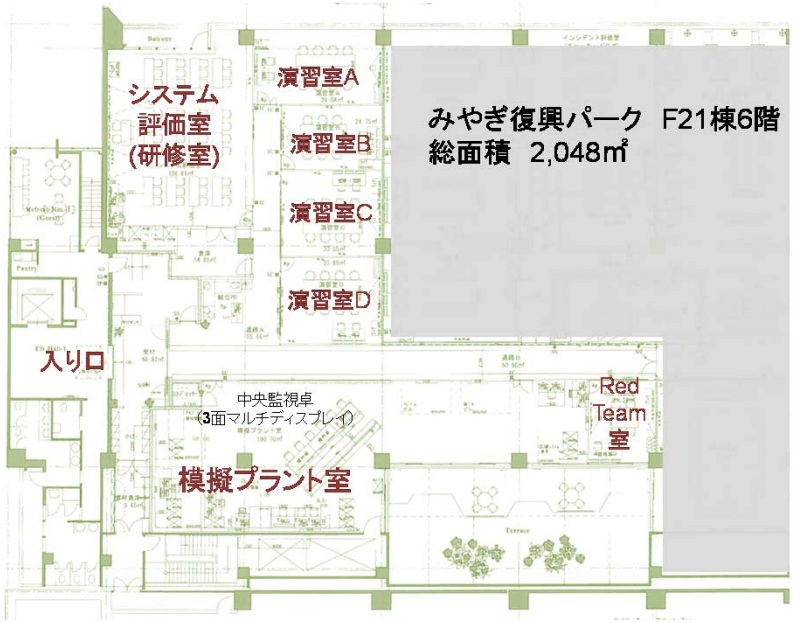
①化学プラント

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



サイバーセキュリティテストベッド見取図

5. 事業化、波及効果

事業化

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。

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。

① 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、8→23に増加した。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。

② 電力・ガス・化学・ビル分野のサイバーセキュリティ演習を、CSSC多賀城本部で実施して、経営層～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た。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。

事業化に向けての取組：インフラのセキュリティ強化を実現する各種事業

◯ 重要インフラのセキュリティ強化を目的として、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に資する本格的な活動をH25年度から開始。

◯ 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。

◯ 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。以下は、CSSCの活動例：

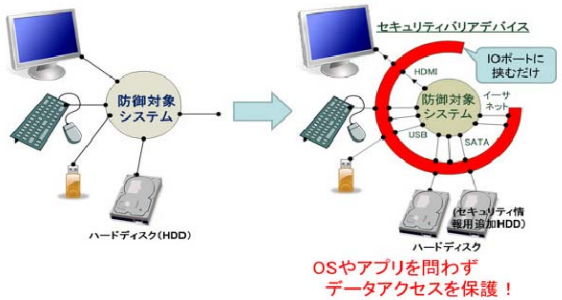
- ホワイトリスト型対策技術の開発
- 制御システム機器のセキュリティの評価・認証

【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）の開発。

✓ 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。

✓ 記憶装置メーカと連携し、今後小型化する課題に取り組む。



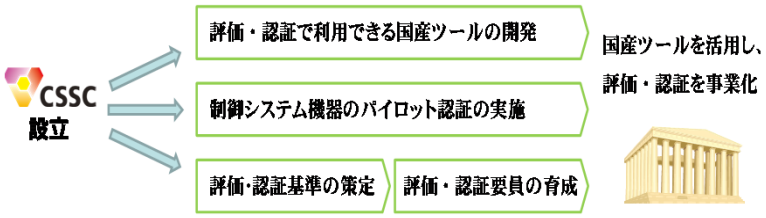
【制御システム機器のセキュリティの評価・認証】

✓ 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・認証機関を確立。

✓ 民間事業者による当技術を活用した評価・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。

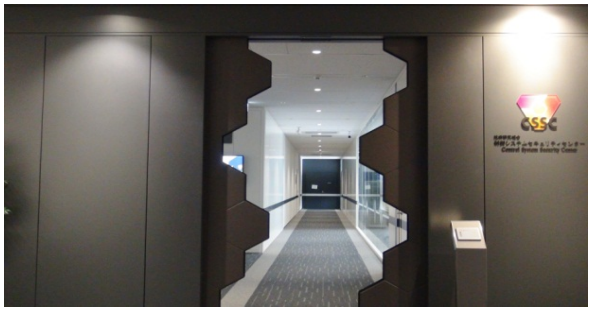
✓ 認定機関(JAB)は、米国ANSIと国際交互承認を締結済み。



波及効果①：技術研究組合に加入する事業者の急拡大

- ○ 技術研究組合制御システムセキュリティセンターは、2012年3月6日設立当時は、参加事業者は8。
- ○ 東北多賀城本部（宮城県多賀城市）を開所後、参加企業数は増加し、2014年3月現在、23事業者。
- ○ 理事長は、新 誠一（国立大学法人電気通信大学 教授）、今年3月に情報セキュリティ文化賞を受賞。

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

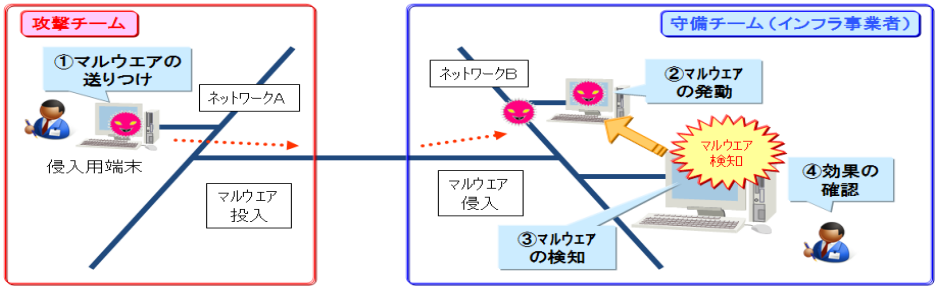


波及効果②：サイバーセキュリティ演習による普及啓発・人材育成

○ 電力分野、ガス分野、ビル分野、化学分野の現場担当者、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こと、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目的。

○ 各分野が実施するサイバーセキュリティ演習は、CSSCの模擬プラントを使用して以下の表の通り実施。演習内容や目標は、分野毎に異なる。

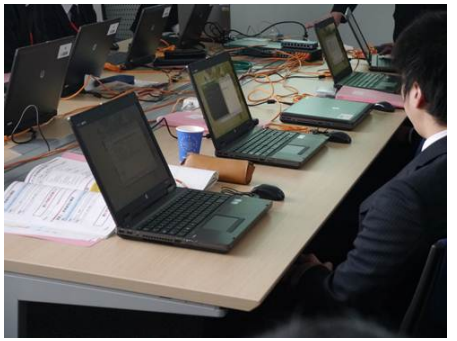
電力	実際に発生しているセキュリティインシデントを模擬体験。電力事業者とベンダが参加して、3/6-7に実施。
ガス	インシデント対応演習と最新対策技術の体験。参加者多数のため2回に分割実施。ガス事業者とベンダが参加して、1/21-22（1回目）、2/24-25(2回目)に実施。
ビル	攻撃・守備型の実践的演習と最新対策技術の体験。ビル事業者と計装事業者が参加して、1/29に実施。
化学	インシデント体験が主。3/4に実施。



サイバーセキュリティ演習の概要

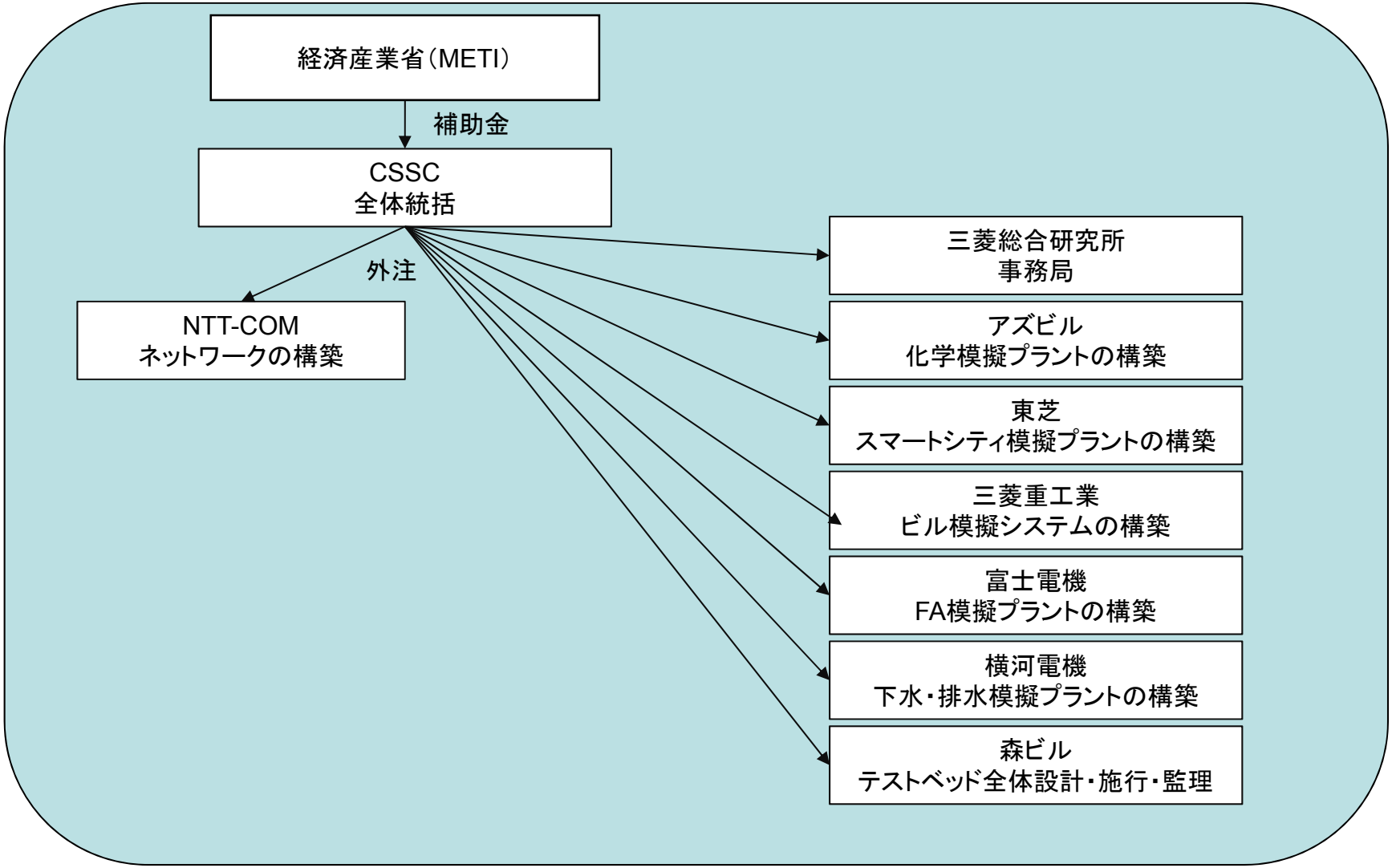
机上演習

機能演習（実機演習）



機能演習（対策技術の演習）

6. 研究開発体制、マネジメント体制



7. 費用対効果等

【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

【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。

【変化への対応】

特になし