第１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６

情報セキュリティ分野に係る
技術に関する施策・事業

評価用資料

平成２６年２月１８日

経済産業省　商務情報政策局
情報セキュリティ政策室

目　　次

第一章　技術に関する施策

１．施策の目的・政策的位置付け 1
　１－１　施策の目的 1
　１－２　政策的位置付け 1
　１－３　国の関与の必要性 3
２．施策の構造及び目的実現の見通し 5
　２－１　得られた成果 5
　２－２　施策の構造 8

第二章　技術に関する事業 11

○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 11
Ａ　新世代情報セキュリティ技術開発事業 12
　１－Ａ　事業の目的・政策的位置付け 12
　　１－１－Ａ　事業の目的 12
　　１－２－Ａ　政策的位置付け 12
　　１－３－Ａ　国の関与の必要性 12
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 13
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 13
　１－ａ　事業の目的 13
　２－ａ　研究開発目標 13
　３－ａ　成果、目標の達成度 14
　　３－１－ａ　成果 14
　　３－２－ａ　目標の達成度 15
　４－ａ　事業化、波及効果について 15
　　４－１－ａ　事業化の見通し 15
　　４－２－ａ　波及効果 16
　５－ａ　研究開発マネジメント・体制・資金・費用対効果等 17
　　５－１－ａ　研究開発計画 17
　　５－２－ａ　研究開発実施者の実施体制・運営 18
　　５－３－ａ　資金配分 18

５－４－ａ　費用対効果 18
５－５－ａ　変化への対応 19
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 20
１－ｂ　事業の目的 20
２－ｂ　研究開発目標 20
３－ｂ　成果、目標の達成度 20
３－１－ｂ　成果 20
３－２－ｂ　目標の達成度 22
４－ｂ　事業化、波及効果について 23
４－１－ｂ　事業化の見通し 23
４－２－ｂ　波及効果 24
５－ｂ　研究開発マネジメント・体制・資金・費用対効果等 25
５－１－ｂ　研究開発計画 25
５－２－ｂ　研究開発実施者の実施体制・運営 25
５－３－ｂ　資金配分 26
５－４－ｂ　費用対効果 27
５－５－ｂ　変化への対応 27
②　アクセス制御技術の研究開発 28
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 28
１－ｃ　事業の目的 28
２－ｃ　研究開発目標 28
３－ｃ　成果、目標の達成度 29
３－１－ｃ　成果 29
論文誌掲載論文 31
査読付国際会議論文 31
招待講演 32
学術論文（査読無し） 32
国際学会発表（査読なし） 34
国内学会発表（査読なし） 34
その他（プレプリント等） 35
３－２－ｃ　目標の達成度 35
４－ｃ　事業化、波及効果について 37
４－１－ｃ　事業化の見通し 37
４－２－ｃ　波及効果 38

５－ｃ　研究開発マネジメント・体制・資金・費用対効果等 39
５－１－ｃ　研究開発計画 39
５－２－ｃ　研究開発実施者の実施体制・運営 39
５－３－ｃ　資金配分 40
５－４－ｃ　費用対効果 40
５－５－ｃ　変化への対応 41
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 42
１－ｄ　事業の目的 42
２－ｄ　研究開発目標 42
３－ｄ　成果、目標の達成度 42
３－１－ｄ　成果 42
３－２－ｄ　目標の達成度 46
４－ｄ　事業化、波及効果について 46
４－１－ｄ　事業化の見通し 46
４－２－ｄ　波及効果 47
５－ｄ　研究開発マネジメント・体制・資金・費用対効果等 47
５－１－ｄ　研究開発計画 47
５－２－ｄ　研究開発実施者の実施体制・運営 47
５－３－ｄ　資金配分 48
５－４－ｄ　費用対効果 48
５－５－ｄ　変化への対応 49
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 .. 50
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 50
１－ｅ　事業の目的 50
２－ｅ　研究開発目標 50
３－ｅ　成果、目標の達成度 50
３－１－ｅ　成果 50
３－２－ｅ　目標の達成度 52
４－ｅ　事業化、波及効果について 52
４－１－ｅ　事業化の見通し 52
４－２－ｅ　波及効果 53
５－ｅ　研究開発マネジメント・体制・資金・費用対効果等 54
５－１－ｅ　研究開発計画 54
５－２－ｅ　研究開発実施者の実施体制・運営 54
５－３－ｅ　資金配分 55
５－４－ｅ　費用対効果 55

５－５－ｅ　変化への対応 55
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 56
１－ｆ　事業の目的 56
２－ｆ　研究開発目標 56
３－ｆ　成果、目標の達成度 56
３－１－ｆ　成果 56
３－２－ｆ　目標の達成度 57
４－ｆ　事業化、波及効果について 57
４－１－ｆ　事業化の見通し 57
４－２－ｆ　波及効果 57
５－ｆ　研究開発マネジメント・体制・資金・費用対効果等 58
５－１－ｆ　研究開発計画 58
５－２－ｆ　研究開発実施者の実施体制・運営 58
５－３－ｆ　資金配分 58
５－４－ｆ　費用対効果 59
５－５－ｆ　変化への対応 59
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 60
１－ｇ　事業の目的 60
２－ｇ　研究開発目標 60
３－ｇ　成果、目標の達成度 60
３－１－ｇ　成果 60
３－２－ｇ　目標の達成度 61
４－ｇ　事業化、波及効果について 61
４－１－ｇ　事業化の見通し 61
４－２－ｇ　波及効果 61
５－ｇ　研究開発マネジメント・体制・資金・費用対効果等 62
５－１－ｇ　研究開発計画 62
５－２－ｇ　研究開発実施者の実施体制・運営 62
５－３－ｇ　資金配分 63
５－４－ｇ　費用対効果 63
５－５－ｇ　変化への対応 64
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） 65

１－Ｂ　事業の目的 65
２－Ｂ　研究開発目標 65
３－Ｂ　成果、目標の達成度 66
３－１－Ｂ　成果 66
３－２－Ｂ　目標の達成度 66
４－Ｂ　事業化、波及効果について 67
４－１－Ｂ　事業化の見通し 67
４－２－Ｂ　波及効果 67
５－Ｂ　研究開発マネジメント・体制・資金・費用対効果等 67
５－１－Ｂ　研究開発計画 67
５－２－Ｂ　研究開発実施者の実施体制・運営 68
５－３－Ｂ　資金配分 69
５－４－Ｂ　費用対効果 69
５－５－Ｂ　変化への対応 70
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 71
１－Ｃ　事業の目的・政策的位置付け 71
１－１－Ｃ　事業の目的 71
１－２－Ｃ　政策的位置付け 71
１－３－Ｃ　国の関与の必要性 72
２－Ｃ　研究開発等の目標 72
２－１－Ｃ　研究開発目標 72
２－２－Ｃ　全体の目標設定 77
２－３－Ｃ　個別要素技術の目標設定 78
３－Ｃ　成果、目標の達成度 79
３－１－Ｃ　成果 79
３－３－Ｃ　目標の達成度 81
４－Ｃ　事業化、波及効果について 83
５－Ｃ　研究開発マネジメント・体制・資金・費用対効果等 83
５－１－Ｃ　研究開発計画 83
５－２－Ｃ　研究開発実施者の実施体制・運営 85
５－３－Ｃ　資金配分 86
５－４－Ｃ　費用対効果 87
５－５－Ｃ　変化への対応 87
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） 88
１－２　事業の目的 88

２－２　研究開発目標 88
３－２　成果、目標の達成度 88
３－１－２　成果 88
３－２－２　目標の達成度 89
４－２　事業化、波及効果について 89
４－１－２　事業化の見通し 89
４－２－２　波及効果 90
５－２　研究開発マネジメント・体制・資金・費用対効果等 90
５－１－２　研究開発計画 90
５－２－２　研究開発実施者の実施体制・運営 90
５－３－２　資金配分 91
５－４－２　費用対効果 91
５－５－２　変化への対応 91

第一章　技術に関する施策

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

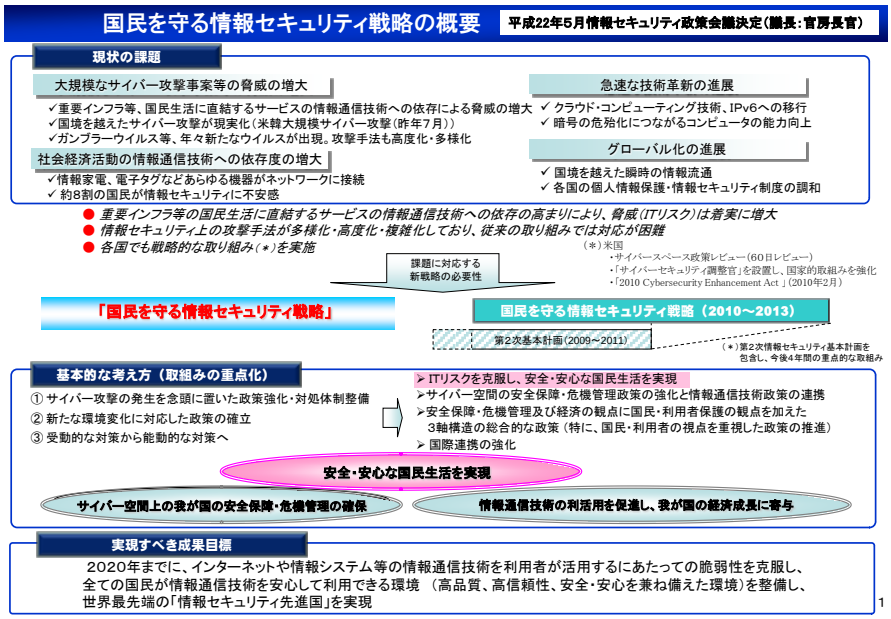


図１－２　国民を守る情報セキュリティ戦略の具体的な取組

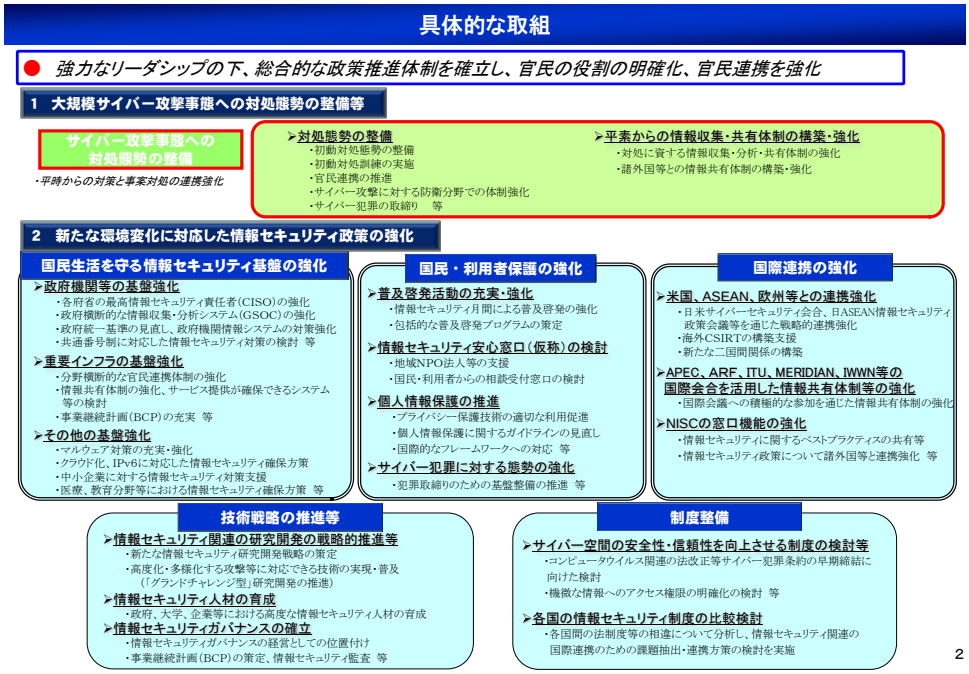


図１－３　情報セキュリティ対策の体系図

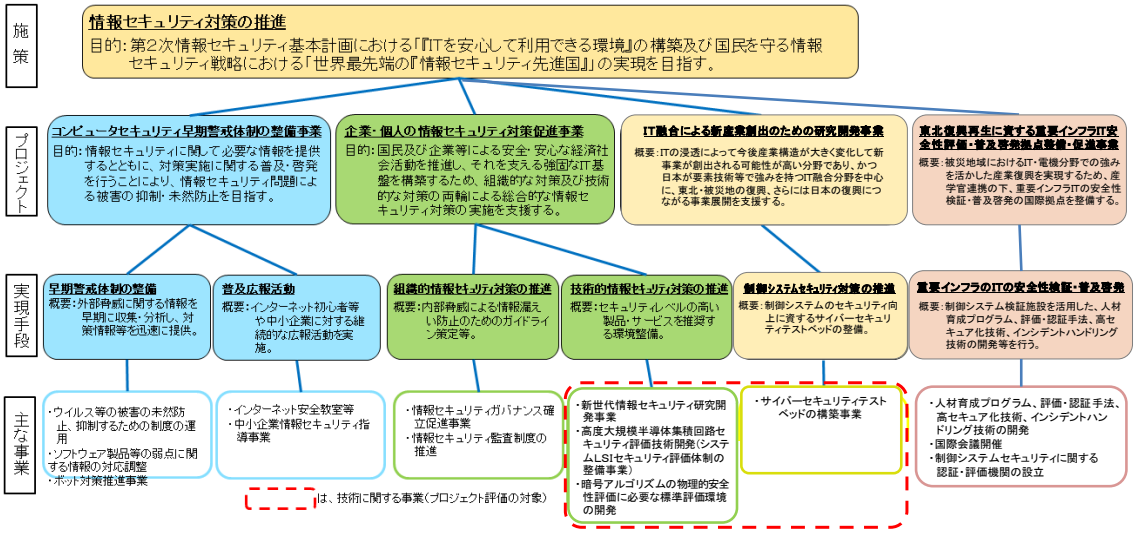
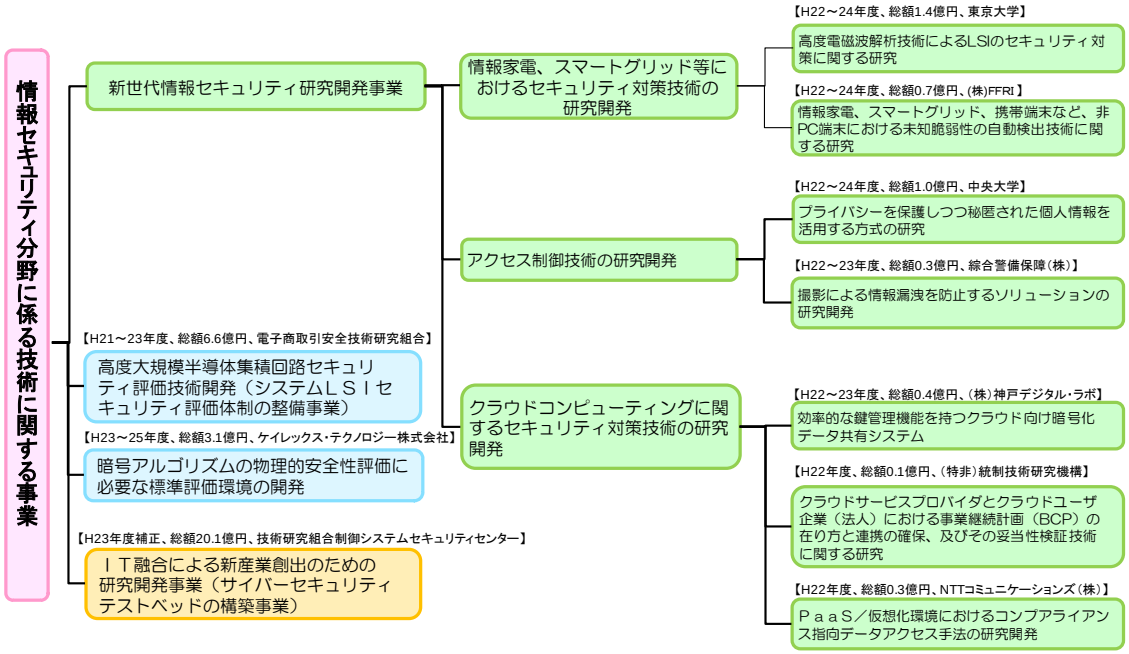


図１－４　情報セキュリティ分野に係る技術に関する事業



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。

（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。

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

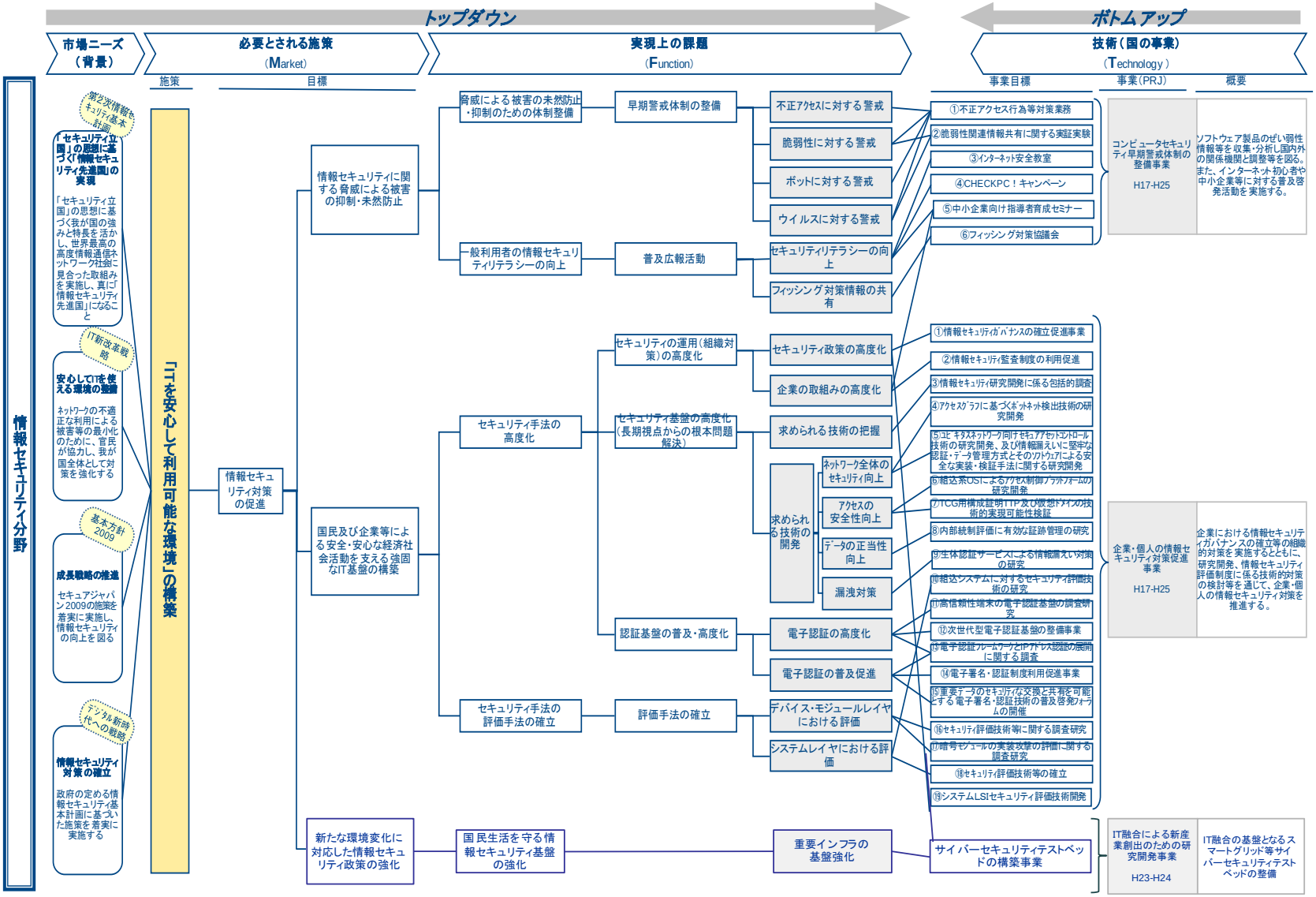
業や重要インフラ分野におけるサイバー攻撃への対処能力の向上、ならびに制御システムセキュリティに関する市場創出。

２－２　施策の構造

別紙２－２－１～２－２－４参照

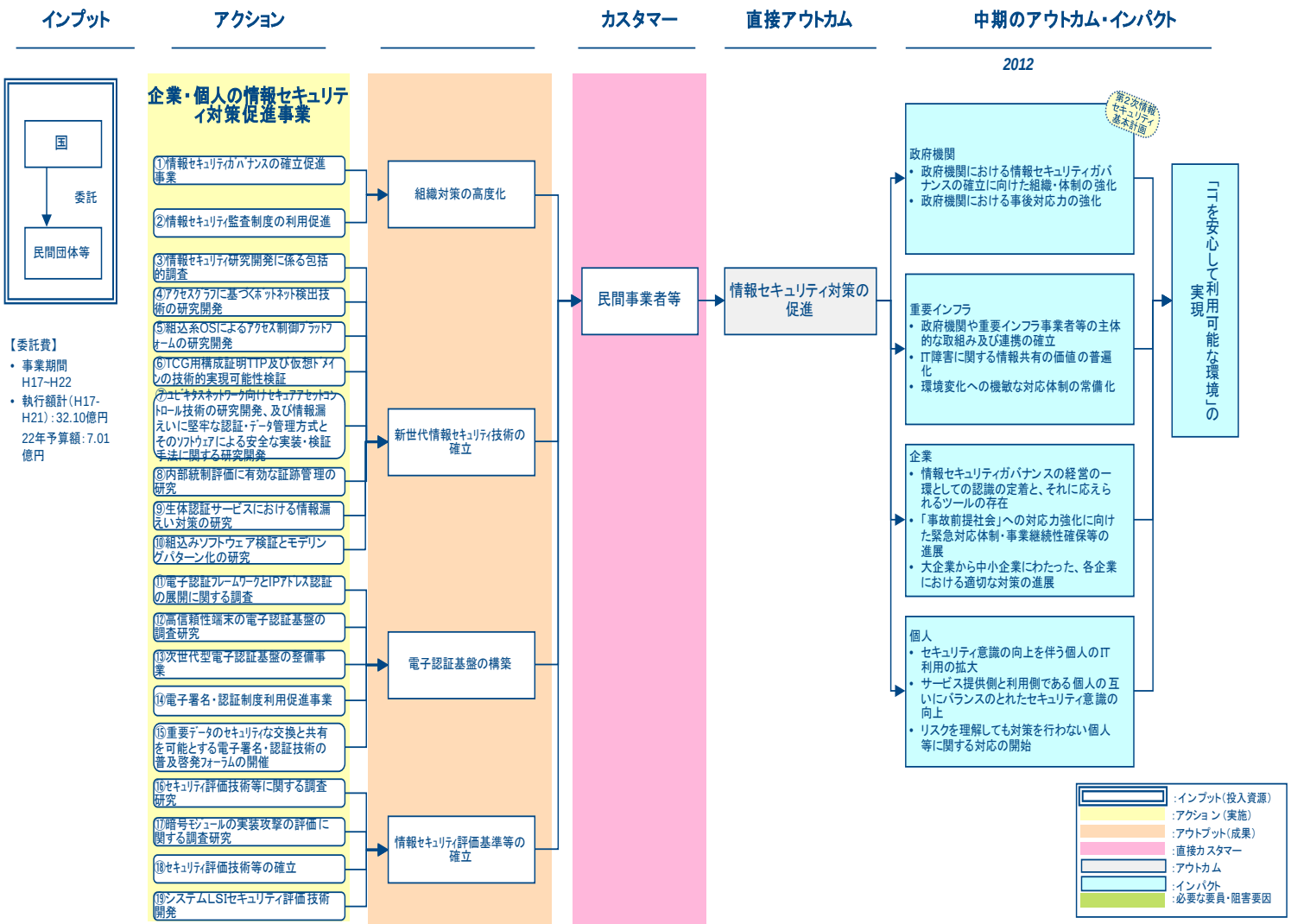
別紙２－２－１

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）



第二章　技術に関する事業

○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、技術的情報セキュリティ対策推進事業（平成２３年度までの事業名は企業・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。

＜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

＜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

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、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する。

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	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	•Trojan回路実装 •電力解析手法の開発 •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。

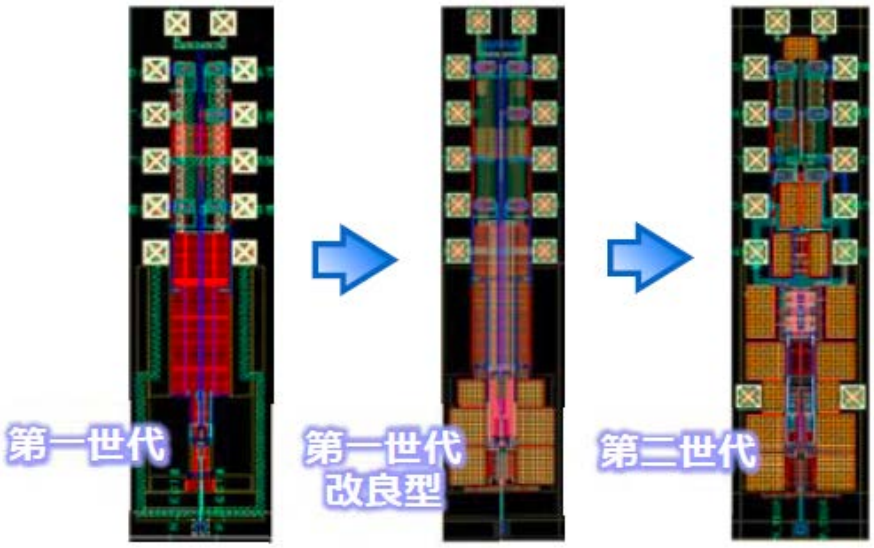
３－ａ　成果、目標の達成度

３－１－ａ　成果

（１）成果

従来製品と比較して空間解像度の高いマイクロプローブを開発し、磁界観測における効率の高い判別を可能とした。これは、単なる故障の検知でなく、恣意的に混入された不具合を検知することが可能な点において、トロイの木馬のような悪意のあるソフトウェアへの対策として有効である。

さらに、このプローブの機能を発揮するために必要となる高精度スキャナを並行して開発するとともに、観測した電磁波の解析ツールの開発も行うことで、高性能磁界解析システムを実現した。



図ａ－１　開発したマイクロプローブの内部基板

（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.

３－２－ａ　目標の達成度

目標の達成度を分野別に示す。

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、それぞれの性能評価を実施した。	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。 • 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	• 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	•Trojan回路実装 •電力解析手法の開発 •局所磁界計測 •評価実験用プラットフォーム開発	• サイドチャネル攻撃実験用AES暗号回路をSASEBO-GIII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-GIIIに実装 • 入力データに応じた特徴的な電磁波の発生可能性を実験を通じて検討	達成

４－ａ　事業化、波及効果について

４－１－ａ　事業化の見通し

以下の用途での事業化に向けた取り組みを実施。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。

（１）IC カードの安全性評価

- 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 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

（２）故障解析

- シリコンを透過する磁界計測により積層 LSI 内部の故障解析が可能
- フラッシュメモリメーカーとコンタクト実施

（３）車載ネットワークのセキュリティ

- 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

（４）模造品対策

- 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 カードベンダと RFID の活用等で協力。

４－２－ａ　波及効果

本研究開発成果は、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。

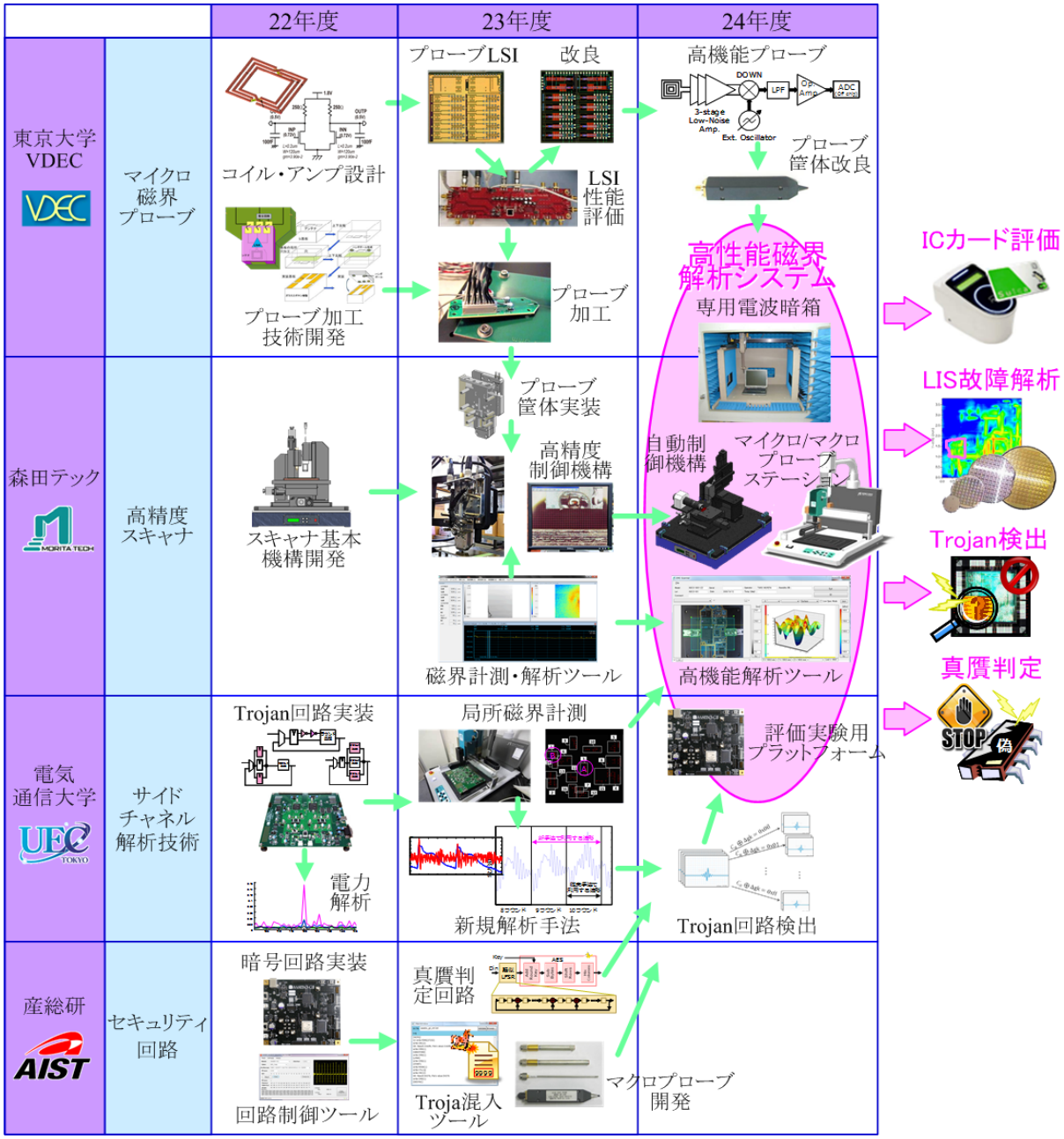
図ａ－２　本研究開発成果による波及効果

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

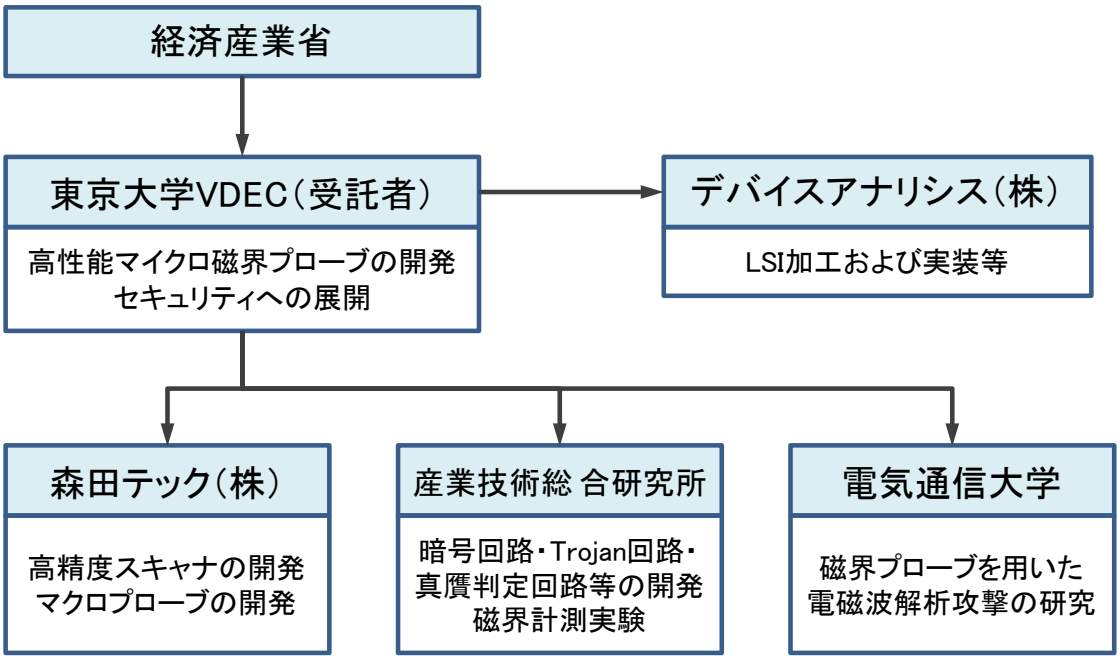
本事業は、平成 22 年度から 24 年度までの 3 年計画で実施された。各要素技術の研究開発計画は次のとおりである。

表ａ－４　研究開発計画



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



図ａ－３　研究開発実施体制

５－３－ａ　資金配分

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

IC カードは耐タンパ性があることを前提として認証手段などに用いられており、仮に IC カードに脆弱性が存在する場合、社会的な損害額が大きくなる。情報家電などと異なり、ネットワーク経由でアップデートを行うこともできないため、物理的に交換するコストは大きい。そうした条件を考慮すると、IC カードの安全性を高める効果

がある活動に対して投資可能な情報セキュリティ対策に関する投資額は、情報家電等と比較して大きくしても見合う可能性が高い。

５－５－ａ　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－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。

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。
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。
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。

３－ｂ　成果、目標の達成度

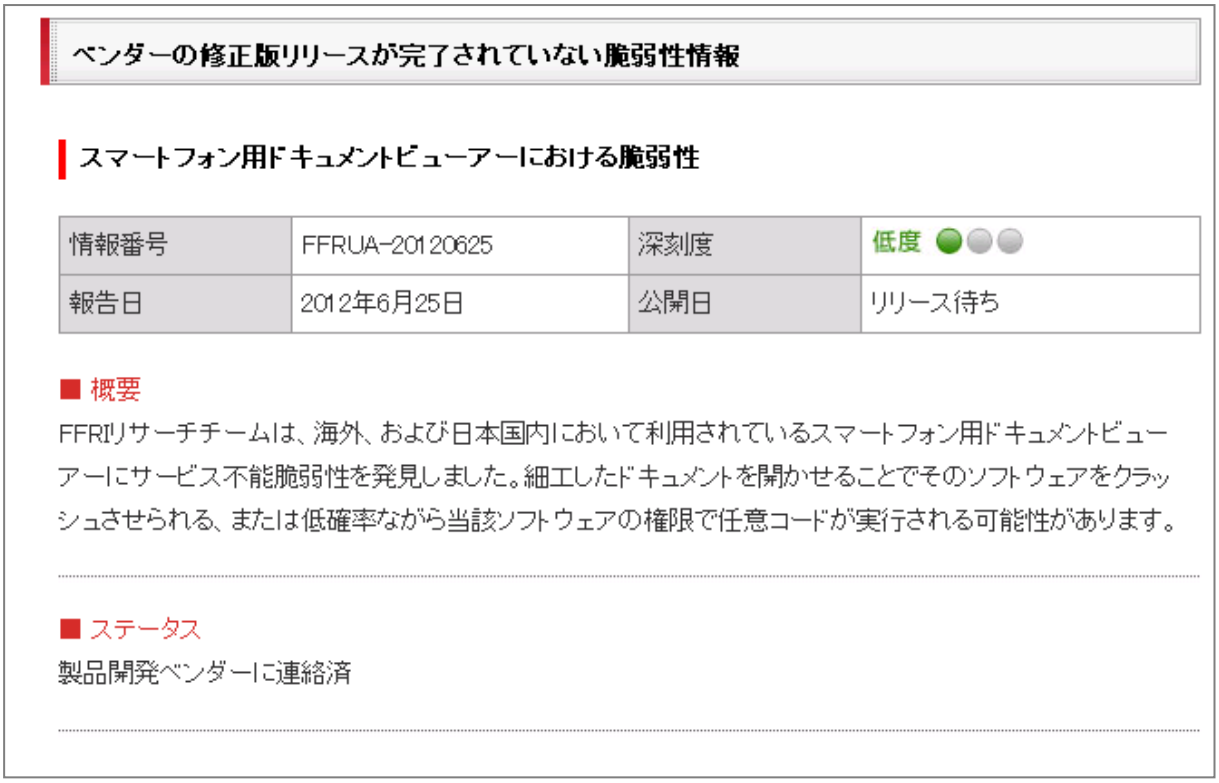
３－１－ｂ　成果

（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。

（２）未知脆弱性の発見

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、ベンダに連絡済みである。



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

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

（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。

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向けのルールとしての検討を行った。	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。 • 制御システム向け検査機能を開発し、検査ツールとしてEDSA認証を取得した。	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サービスにおいて活用している。以下にその２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

４－２－ｂ　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である。

また、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。

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

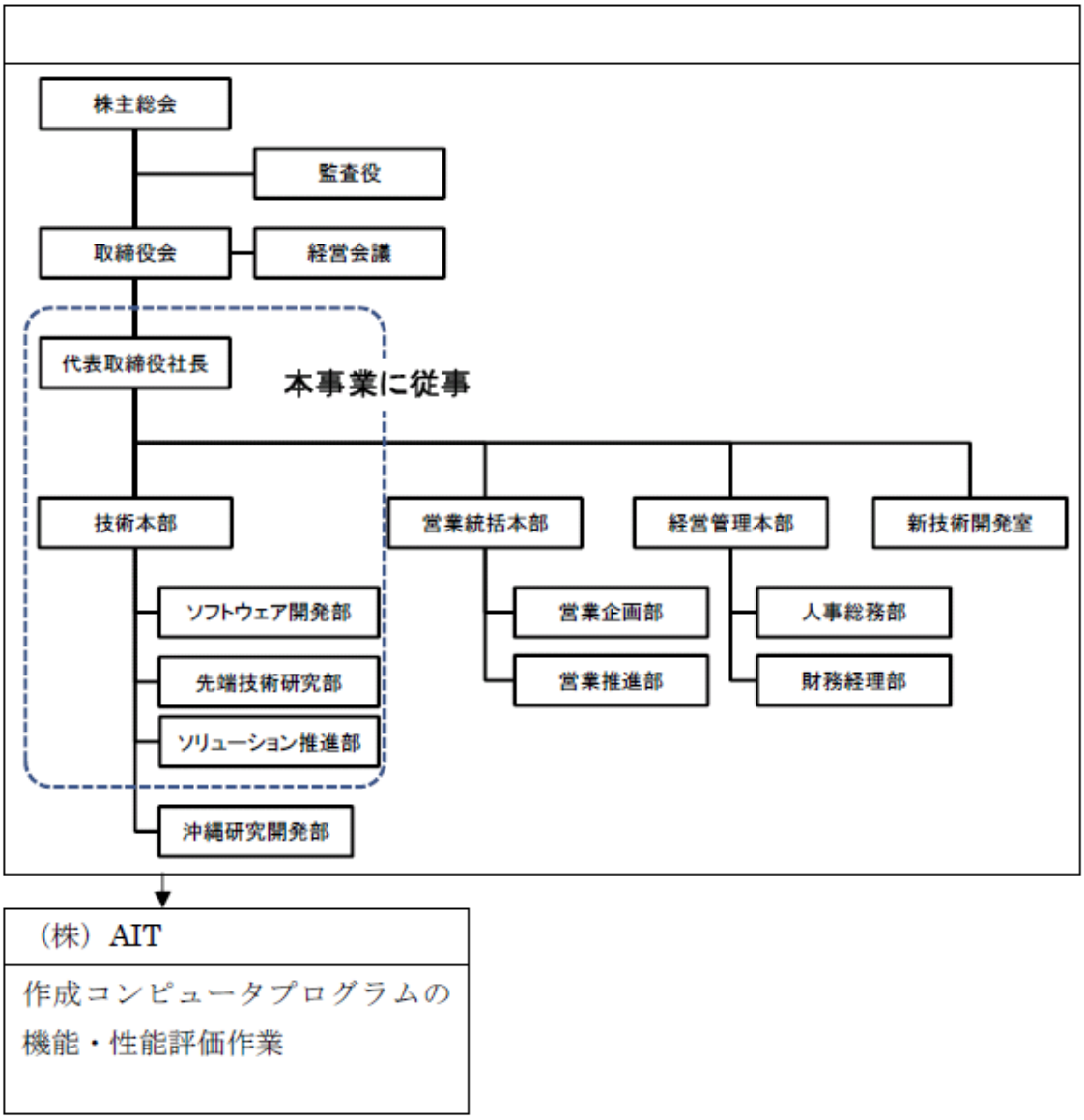
本事業は、平成 22 年度から 24 年度までの 3 年計画である。各要素技術の研究開発計画は次のとおりである。

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。

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

情報家電や組込機器における脆弱性は、今後こうした機器がネットワークに接続されることにより、脅威としての影響度が高まることが予想される。こうした脆弱性がユーザに脅威をもたらすものであった場合、不正利用による損失や、機器を利用できないことによる不利益等の損失は、PC 端末を上回る恐れもある。

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、制御システムの脆弱性が注目されたことを踏まえ、制御システム向けの検査機能の追加ならびに強化を実施した。

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

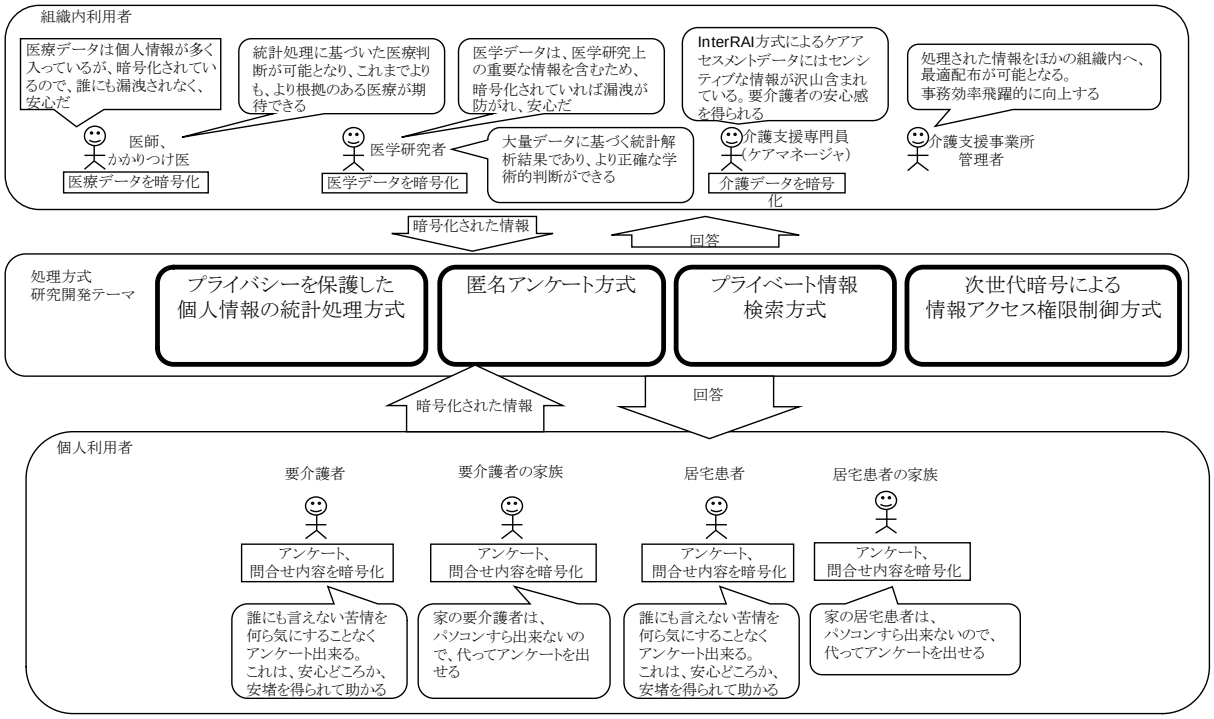
情報セキュリティに深く関わる価値観としては、自由、安心・安全、プライバシー保護の三者が重要であるが、この三者は、互いに矛盾・相克する場合が多い。管理経営、倫理、法制度、技術、即ち Management、Ethics、Law and Technology（MELT）を密結合・強連結させ、融合（MELT）させて、自由、安心・安全、プライバシー保護という相克しがちな三者の関係を止揚することが要請されている。本研究開発は、クラウドに個人情報や機密情報が暗号化されて保管・預託される環境が増える中で、効率性、安全性の面から、暗号化した状態のままで、加算・乗算を含む統計処理や、サーバー管理者に知られることな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



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

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下表のように整理される。当初の研究開発計画に追加した項目として将来における研究開発成果の製品をめざして YDK 株式会社にプロトタイピングを依頼したこと、ならびに米国 Biomedical Objects Inc. に University of California, Irvine における研究内容の評価を依頼したことが、医療・介護分野におけるニーズへの対応として有効に機能している。また医療・介護分野における有識者とへの研究開発内容の説明、デモ、ならびに意見を聞く機会を多くもったことも研究開発の方向の妥当性判断にきわめて役立ったと考えられている。

表ｃ－２　研究開発の成果

<table>
<tr><th>研究テーマ</th><th>具体的方式名</th><th>特徴</th><th>製品化計画</th><th>提携企業</th><th>学会発表</th><th>有識者評価</th><th>備考</th></tr>
<tr><td rowspan="3">プライバシーを保護した個人情報の統計処理方式</td><td>乱数付加による統計処理秘密分散</td><td>超高速、低コスト</td><td rowspan="3">YDKによって製品化</td><td rowspan="3">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</td><td rowspan="3">ISITA2012など学会発表12件</td><td>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」</td><td rowspan="4">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。</td></tr>
<tr><td>Paillier暗号を用いた統計処理</td><td>高次数の処理も可能</td></tr>
<tr><td>プライバシー保護条件付き情報開示</td><td>市川市CIOが2010年に要望</td><td>堀部教授「電子行政が実現したらすぐ使える」</td></tr>
<tr><td rowspan="2">プライベート情報検索(PIR)
匿名アンケート方式</td><td rowspan="2">論理学暗号を用いた自然言語による秘匿検索／Semantic Computing</td><td rowspan="2">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</td><td rowspan="2">UCIにてプロトタイプ作成、医学部、バイオ医学部に適用</td><td rowspan="2">米国Biomedical Object Inc.</td><td rowspan="2">IEEE-ICIOS2012など学会・論文誌発表9件</td><td>神戸大森井教授「このような方式は今までになく画期的」</td></tr>
<tr><td>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」</td></tr>
<tr><td>次世代暗号によるアクセス権制御方式</td><td>多変数公開鍵(TSK)暗号による受信組織対応暗号</td><td>柔軟性
非定常性</td><td>フォーラム活動を通じて展開</td><td>YDK</td><td>SCC2013など学会発表15件</td><td>井堀氏「組織暗号無くして電子行政無し」</td><td>属性・関数暗号は、固定的</td></tr>
</table>

（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

- 2012 年度

[1] Jennifer Kim, Phillip C.-Y. Sheu, and Hiroshi Yamaguchi, “Semantic computing and business intelligence,” International Journal of Semantic Computing. (査読受け中)

[2] Ke Hao, Phillip Sheu, and Hiroshi Yamaguchi, “An implementation of collaborative network operating system,” International Journal of Semantic computing. (査読受け中)

[3] 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). (投稿中)

[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,” IEICE Trans. Fundamentals. (投稿中)

- 2010 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

- 2012 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). (採録決定)

[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.

- 2011 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.

招待講演

- 2012 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.＜発表予定＞

[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.

学術論文（査読無し）

- 2012 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.

- 2011 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.

- 2010 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）

- 2012 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）

- 2012 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.

- 2011 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）

- 2011 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

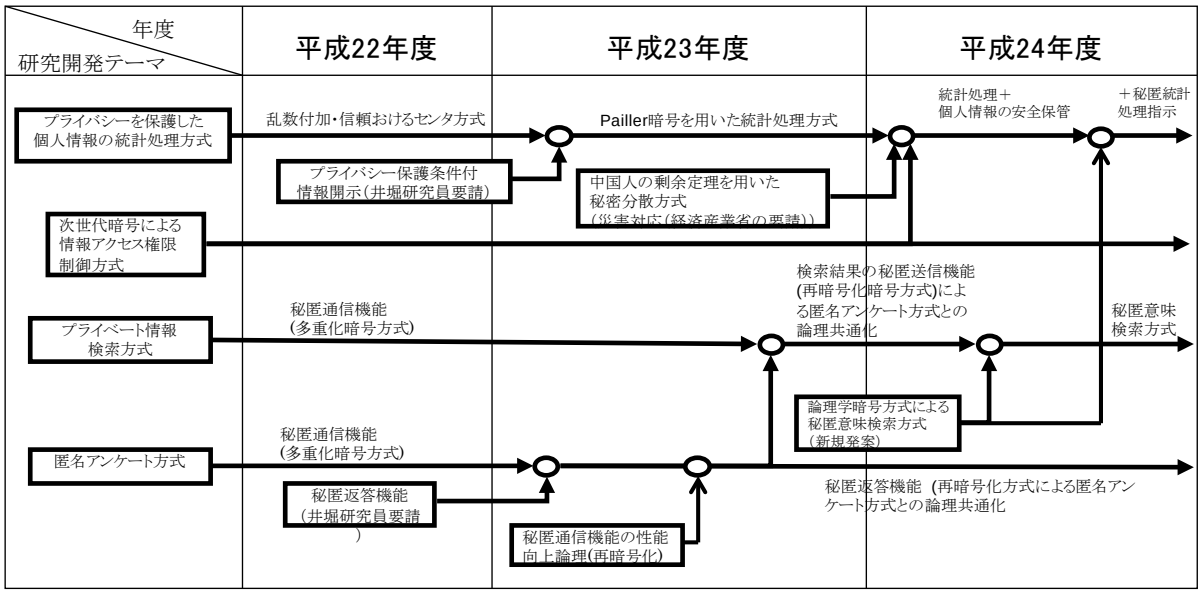
平成 22 年度は研究開発の方式の検討、他方式の優位性の考察、ならびに医療・介護分野におけるニーズ、シーズの調査を行った。平成 23 年度は方式実現のための暗号、暗号プロトコル手法の検討、ならびに一部、プロトタイピング、デモプログラムの作成を行った。平成 24 年度はプロトタイピングによる性能評価、論文発表、ならびに報告書作成を行い、各テーマとも所定の目標を達成した。

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、必要な手法を感性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公安、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

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」[1]として活動している。そのウェブサイトの画面を次に示す。

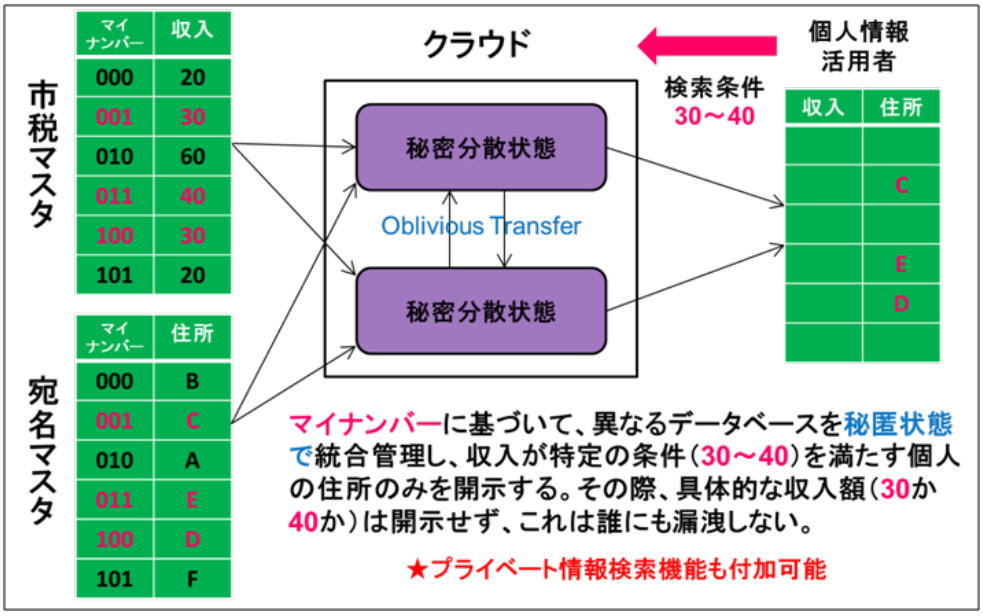
[1] http://www.fuji-serv.com/chuo/index.html

図ｃ－２　MELT up フォーラム

４－２－ｃ　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。



図ｃ－３　マイナンバー制度への応用

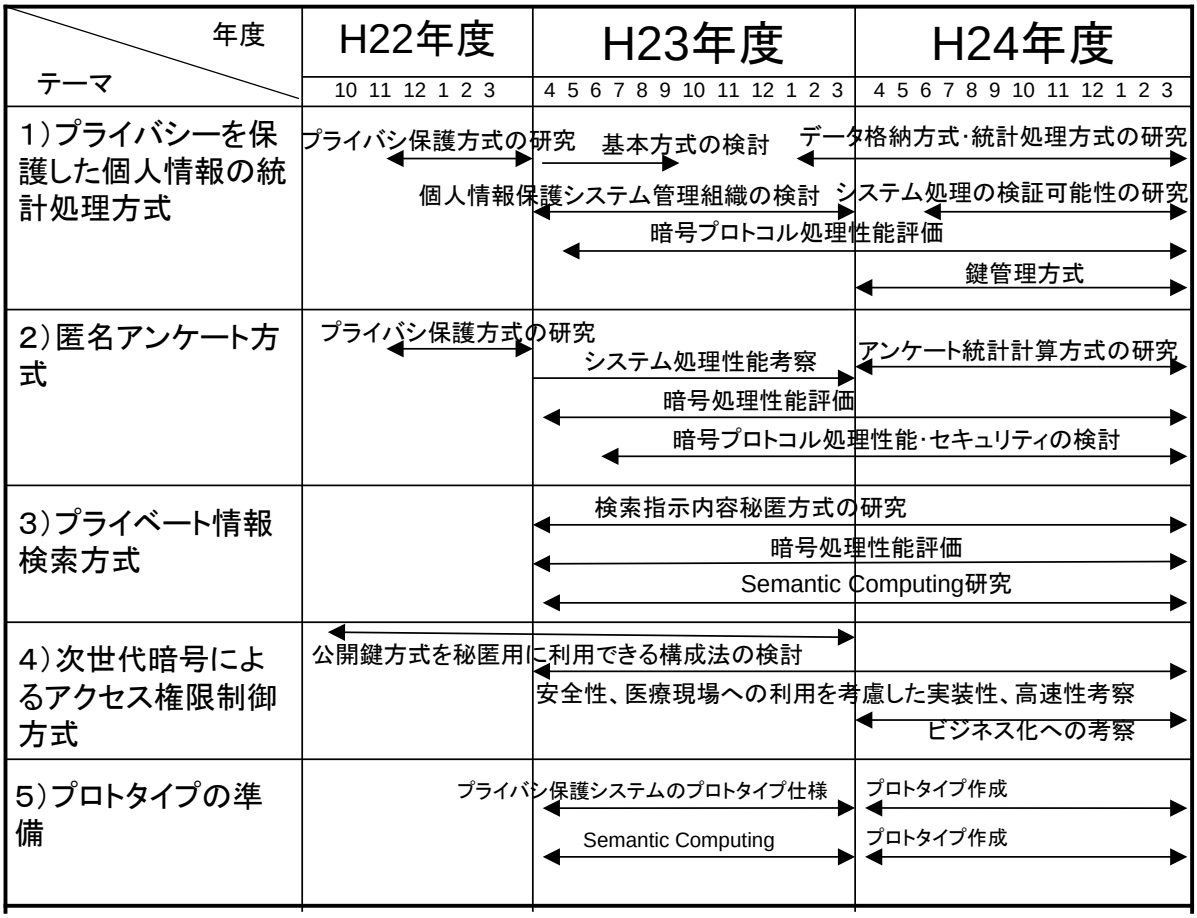
５－ｃ　研究開発マネジメント・体制・資金・費用対効果等

５－１－ｃ　研究開発計画

研究開発計画

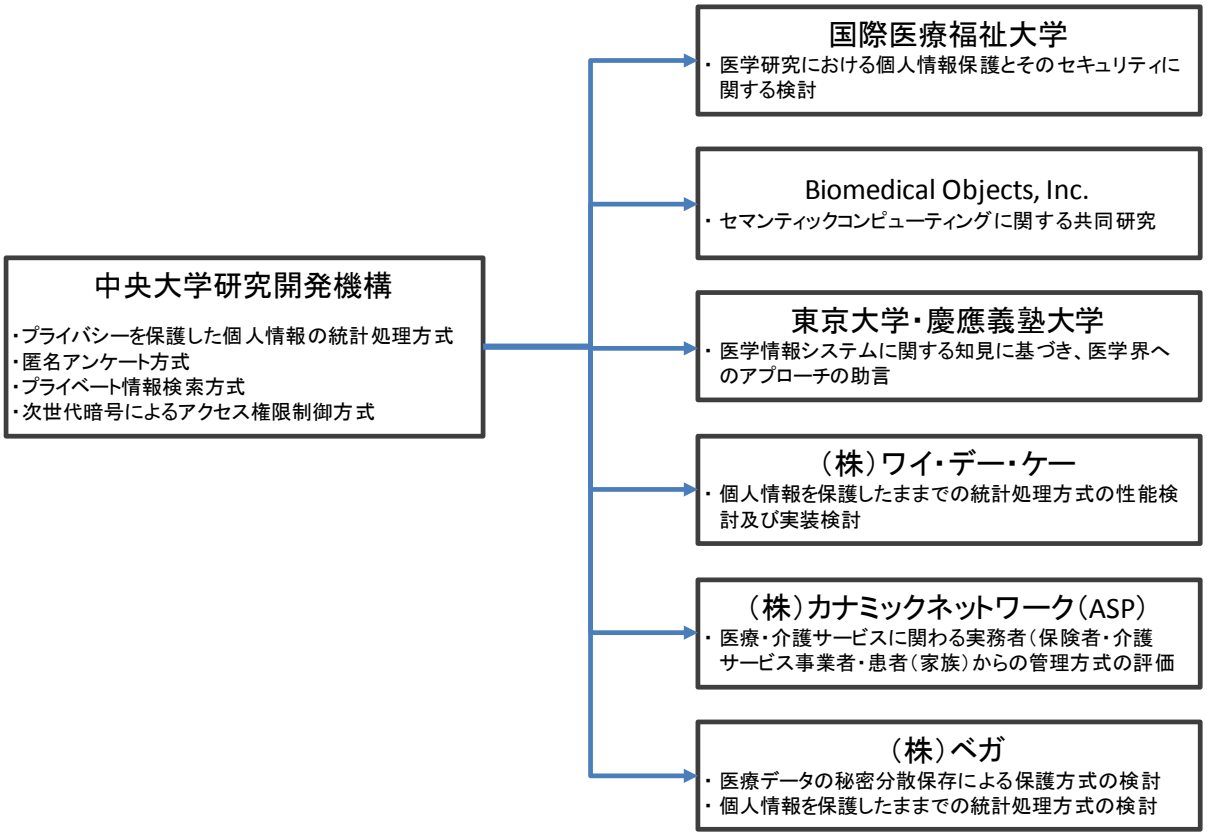
本事業は、平成 22 年度から 24 年度までの 3 年計画である。各要素技術の研究開発計画は次のとおりである。

表ｃ－８　事業化状況



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



図ｃ－４　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**

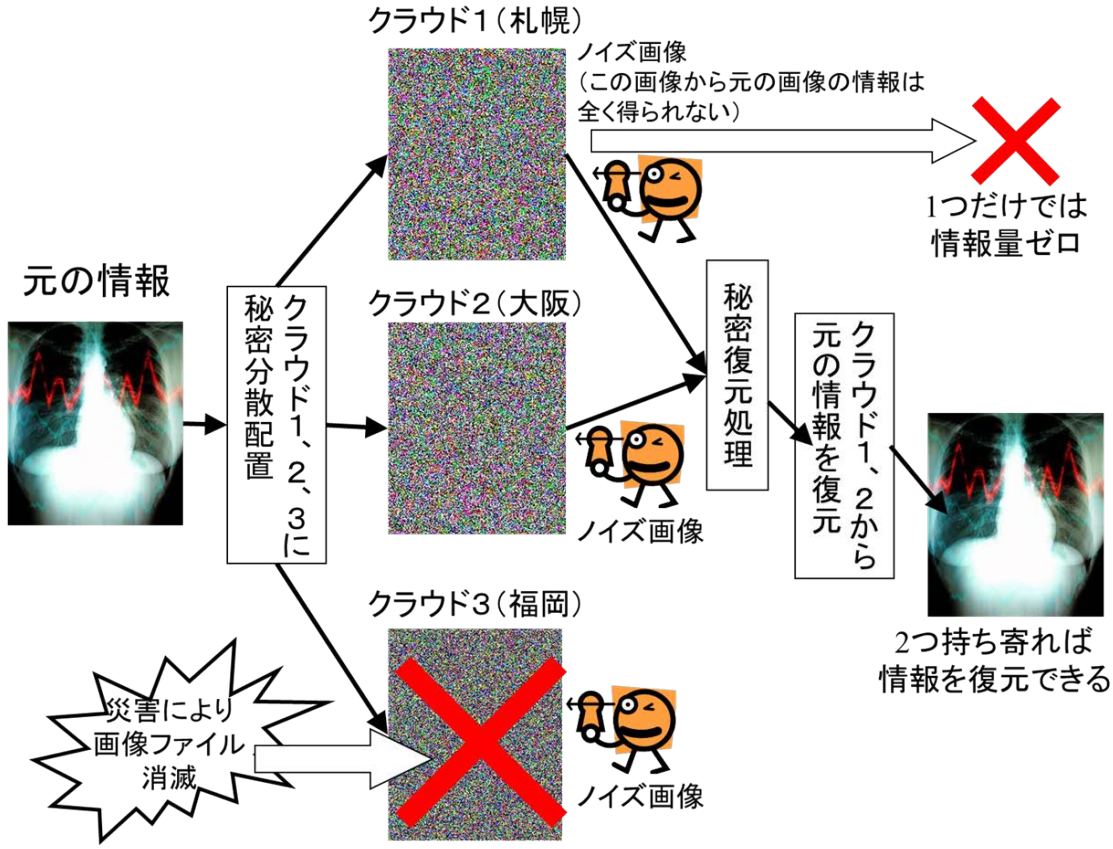
５－４－ｃ　費用対効果

日本ネットワークセキュリティ協会（JNSA)の報告書「２０１２年度 個人情報漏えいインシデント調査報告書【上半期 速報版】」によれば、情報漏えいに起因する 2012 年の想定損害賠償総額は約３４８億円であり、本事業成果の普及により、今後その１%の削減に貢献できたとすると、年間３億円の波及効果が得られることになる。米国 CERT 公表の"2011 Cyber Security Watch Survey"によれば、外部からの攻撃による被害よりも、内部不正による被害のほうが大きいとの回答が 33%を占めており、公表

されていない内部不正による損失を想定すると、本成果により機微な個人情報を保護することによる効果は、さらに大きくなることが想定される。
本成果による個人情報やプライバシーの保護方式は、特殊なハードウェアや専用の情報通信ネットワークシステムを必要とせず、クラウドサービスを含めてこれまでの情報通信システム基盤を利用することが可能であり、コスト面での優位性が高い。

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－５　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

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。

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。

３－ｄ　成果、目標の達成度

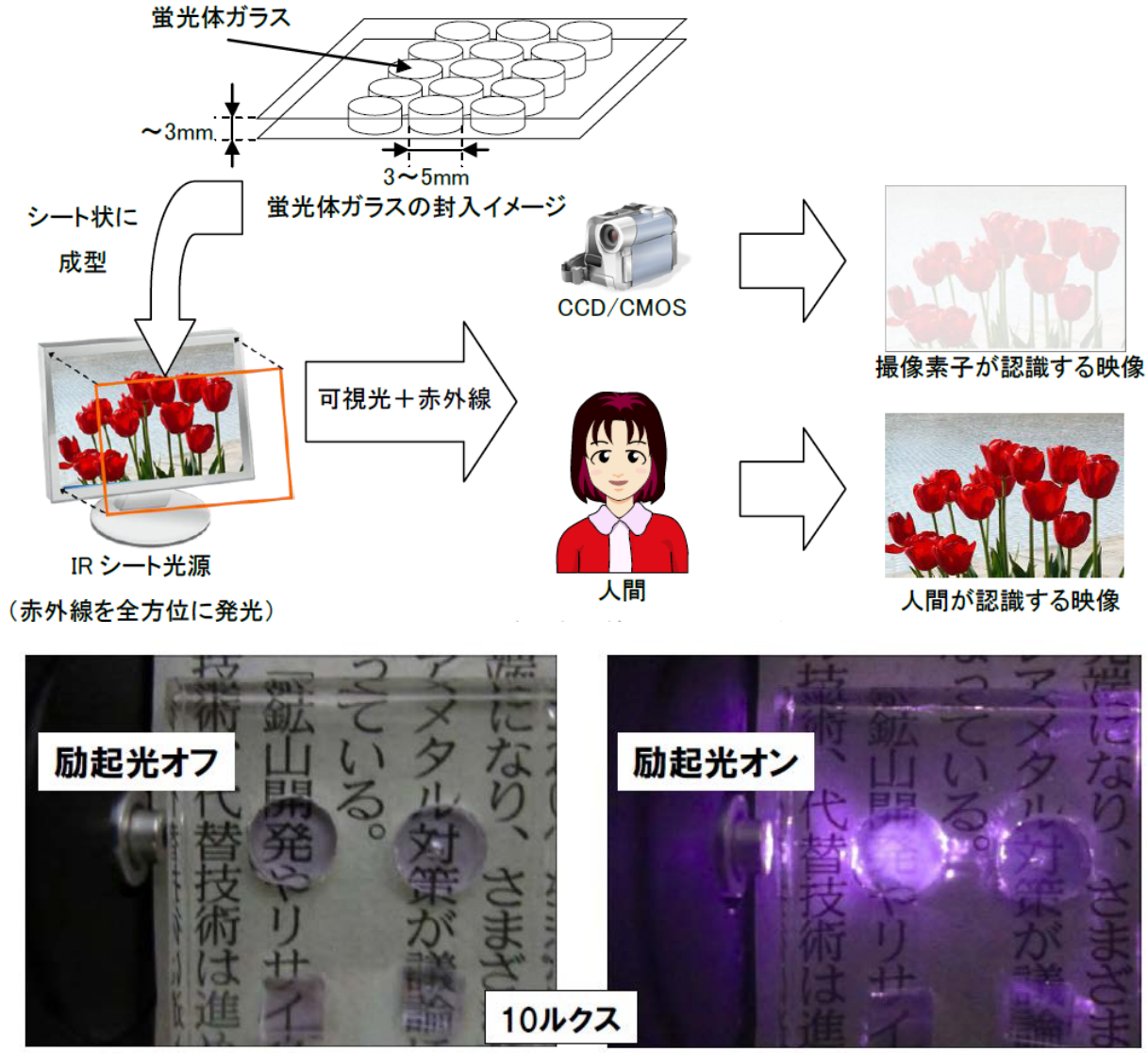
３－１－ｄ　成果

（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

る場合はガラス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。



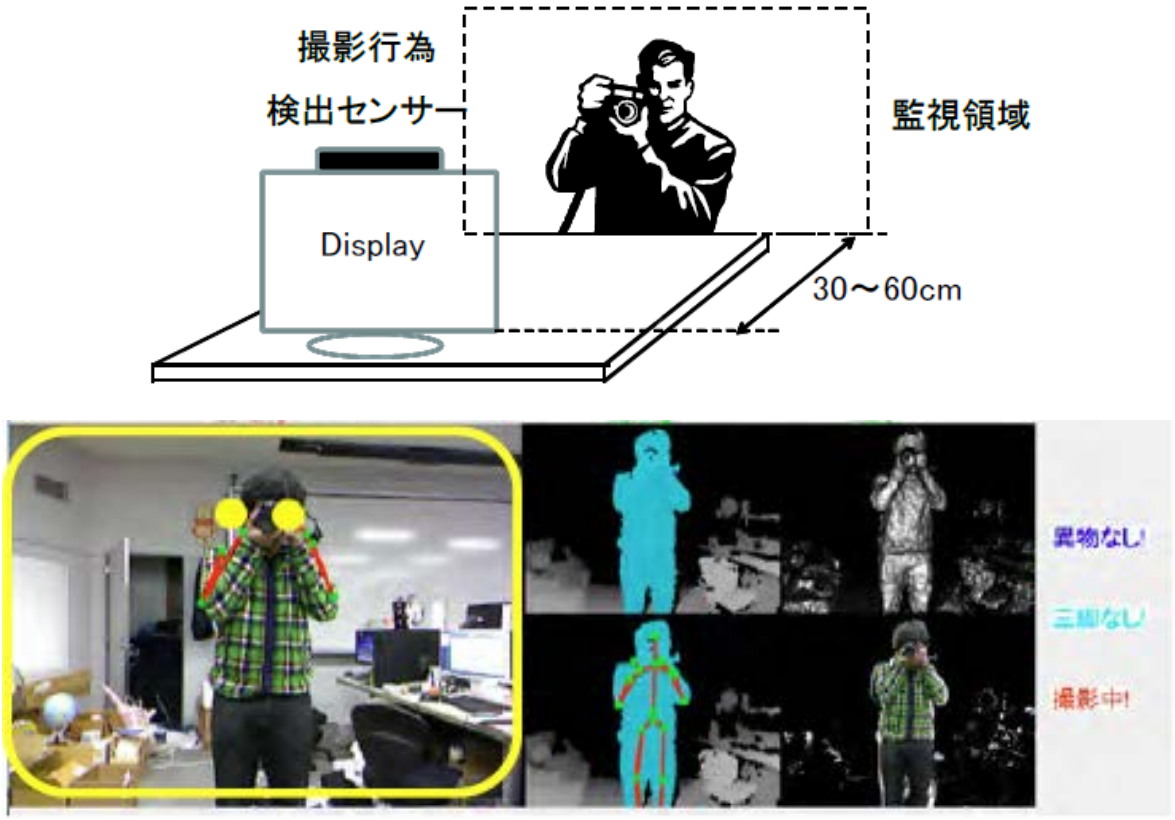
図ｄ－１　赤外線光源によるコンテンツの識別性低下に関する実験結果

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。

（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、撮影者の識別に成功した一方、眼

鏡フレームやネームプレートをカメラとして誤検知してしまうなど、精度上の改善の必要があることが明らかとなった。



図ｄ－２　撮影者の識別に関する実験結果

（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

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、本特許は昨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）

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。	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。 • 眼鏡フレームやネームプレートにも反応するため、更なる精度向上が必要。	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。	達成

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

一方、本研究開発で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でき、本件について特許を出願している。この事業化の可能性を探るため、ニーズがあると考えられるブランド企業や窯元等へのヒアリングな

どの市場調査が検討されている。
　このほか、同様に本研究開発において開発したカット検知センサー技術は、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している。

４－２－ｄ　波及効果

　本研究開発の成果はまだ事業化しておらず、直接の波及効果は発生していないが、こうした研究が継続され、派生的な技術が活用されていく中で、コンテンツの適切な保護と活用に関する社会的な意識の醸成効果が期待される。

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

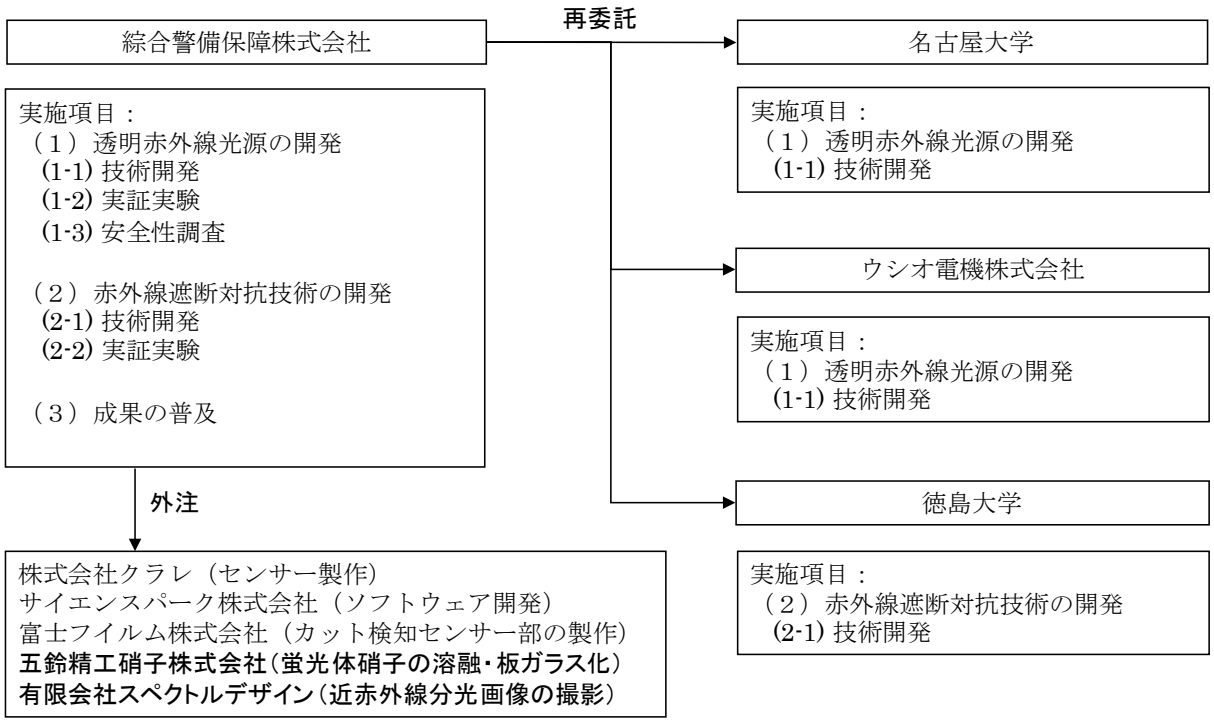
　本事業は、平成 22 年度から 23 年度までの 2 年計画である。各要素技術の研究開発計画は次のとおりである。

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



図ｄ－３　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

日本ネットワークセキュリティ協会（JNSA)の報告書「２０１２年度 個人情報漏えいインシデント調査報告書【上半期 速報版】」によれば、情報漏えいに起因する 2012 年の想定損害賠償総額は約３４８億円である。撮影を通じた情報漏えいの発生状況は明らかではないが、画面の撮影行為はテレワークや在宅勤務における情報漏えい防止

対策の効果を損なわせるものであり、この防止が可能となることで、上記の損害賠償総額の１%が抑制されると仮定すれば、約３億円の効果が想定される。

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

理論の分野では、属性ベース暗号、格子暗号、インテリジェント暗号等、次世代に向けた様々な方式が提案されている。一方で、実際のサービスとして提供されているのは Voltage Security Inc.の ID ベース暗号など、数少ない。近年、脚光を浴びているクラウドコンピューティングに適すると言われる属性ベース暗号方式に着目し、サービスとして提供できるレベルに引き上げるための研究開発を行い、サービスモデルの構築・評価を行い、サービス化を目指す。

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。

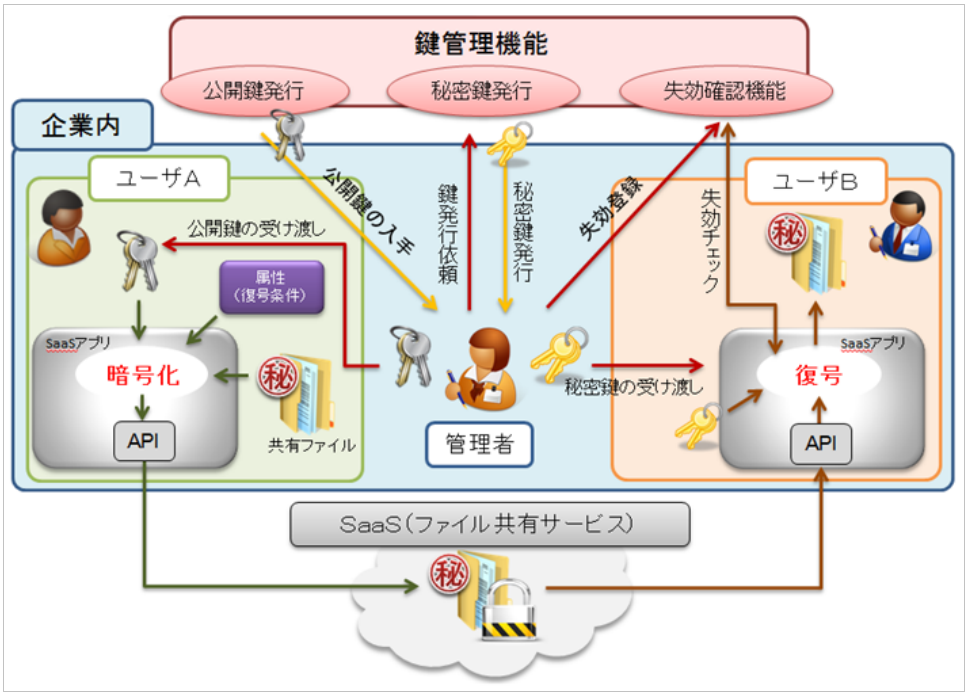
表ｅ－１　個別要素技術の目標

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。
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。

３－ｅ　成果、目標の達成度
３－１－ｅ　成果

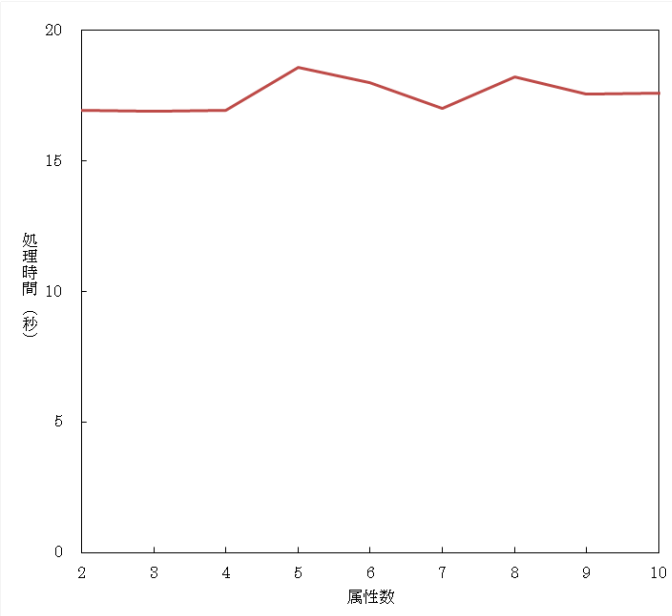
（１）成果
クラウド上のデータを安全に管理するための暗号化鍵の管理システムとして、次

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 端末でアクセスする環境を構築した。



図ｅ－１　開発したモデルシステムの概要

実験の結果、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。



図ｅ－２　復号条件の属性数に対する暗号化処理時間

（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

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。

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
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。 ・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
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
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また来場者にアンケート調査を実施した。	達成

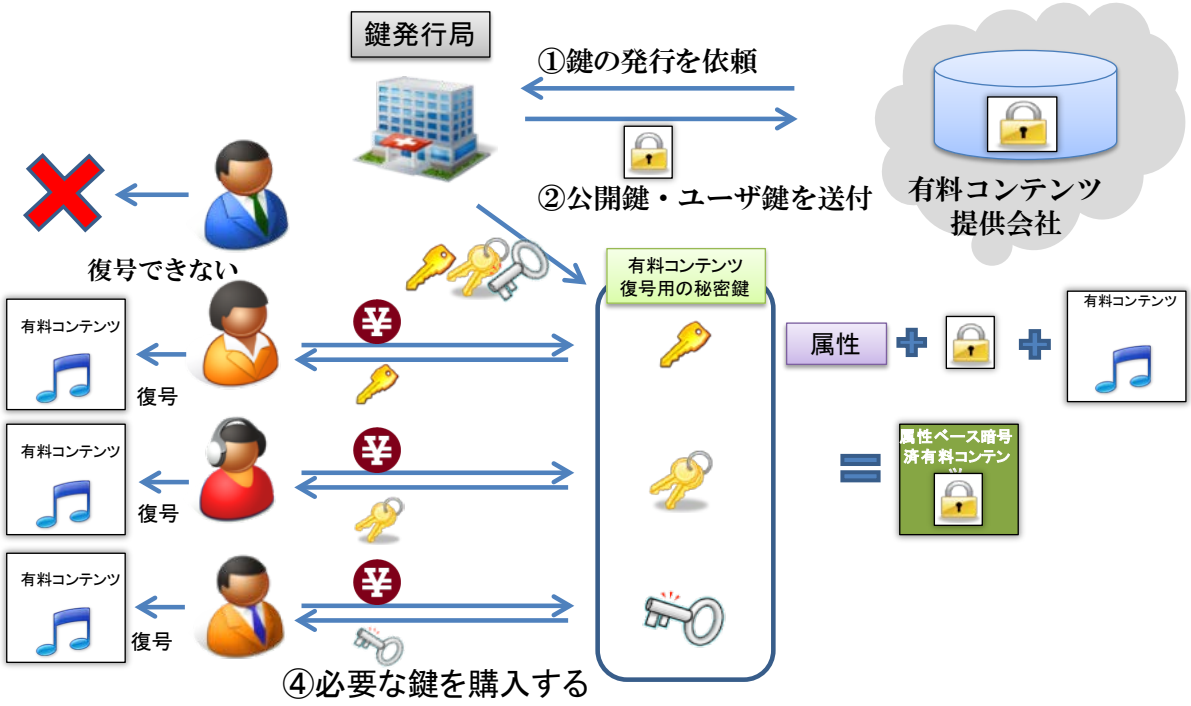
４－ｅ　事業化、波及効果について

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。

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－３　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

本研究開発の成果はまだ事業化しておらず、直接の波及効果は発生していないが、こうした研究が継続され、クラウドサービスにおける情報セキュリティ対策の選択肢が増えることが、利用者による多様な利用を促していく効果が期待される。

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

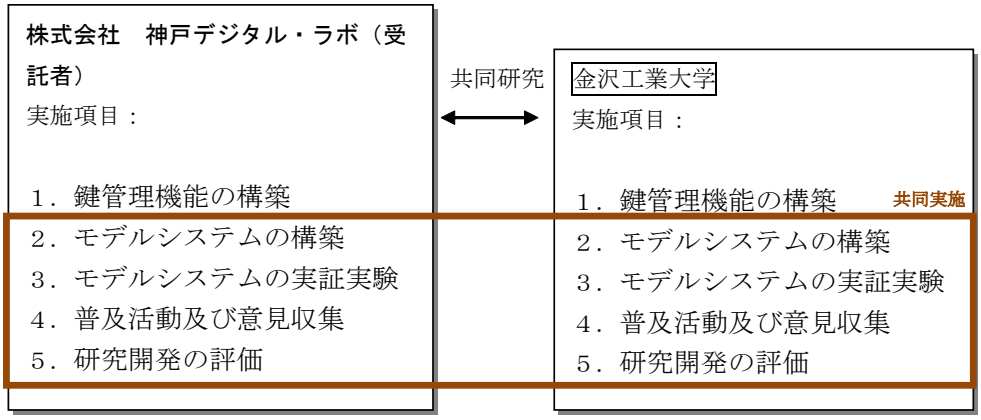
本事業は、平成 22 年度から 23 年度までの 2 年計画である。各要素技術の研究開発計画は次のとおりである。

表ｅ－４　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、再委託先として以下の機関が事業に参加した。



図ｅ－４　研究開発実施体制

５－３－ｅ　資金配分

表ｅ－５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	12.2	16.4

５－４－ｅ　費用対効果

IDC Japan の調査（2013 年 10 月 24 日公表）によれば、2013 年の国内パブリッククラウドサービス市場は 1,321 億円であり、2017 年には 3,376 億円まで成長すると見込まれている。市場の拡大に伴い、情報セキュリティ上の損害額も増大することが懸念されるが、本成果による安全な情報共有が行われることで、損害額を抑制する効果が期待できる。

５－５－ｅ　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－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

（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。	達成

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

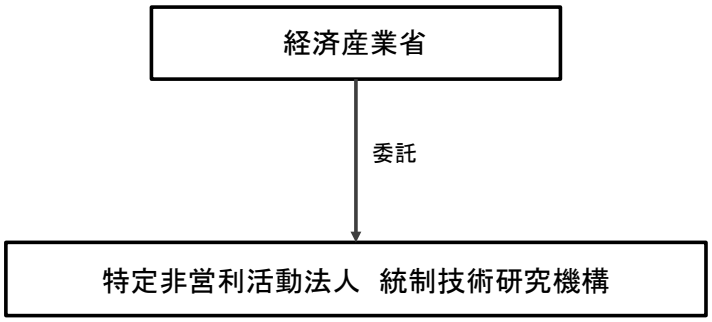
本事業の研究開発計画は次のとおりである。

表ｆ－４　研究開発計画

年度	平成22年度
予算額	12.4百万円
クラウドベンダの実態調査	→
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	→
「クラウドベンダのためのBCP構築基準」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	**12.2**

５－４－ｆ　費用対効果

2012 年 6 月に発生したファーストサーバによるデータ消失事故においては、親会社が特別損失として 12 億円を計上するなど、クラウドサービスにおける障害発生が社会的に大きな影響を及ぼすことを明らかにした。本成果が示すような事業継続計画に関する基準に基づいた対策をクラウドサービスベンダが実施することで、ユーザに影響を及ぼすような事故の発生や、ユーザに及ぶ被害を減少させる効果が期待できる。

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。

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
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	仮想化機構とゲスト環境のペアリングを実現するケーパビリティインジェクション機構と組み合わせることで、エンドユーザやクラウド基盤利用者が預けたデータをクラウド基盤利用者自身が管理・統制することが可能となる。
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	クラウド基盤サービスの利用者側、すなわちゲスト環境（OS）への外部からの権限移譲を可能とする。2つの機能を通じて、クラウド利用者が持つコンプライアンスへの懸念を軽減することができる。

３－ｇ　成果、目標の達成度

３－１－ｇ　成果

（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

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より、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
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	• 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。 • プロトタイプによる試験に合格したことを確認した。	達成
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	• 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。 • プロトタイプによる試験に合格したことを確認した。	達成

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。

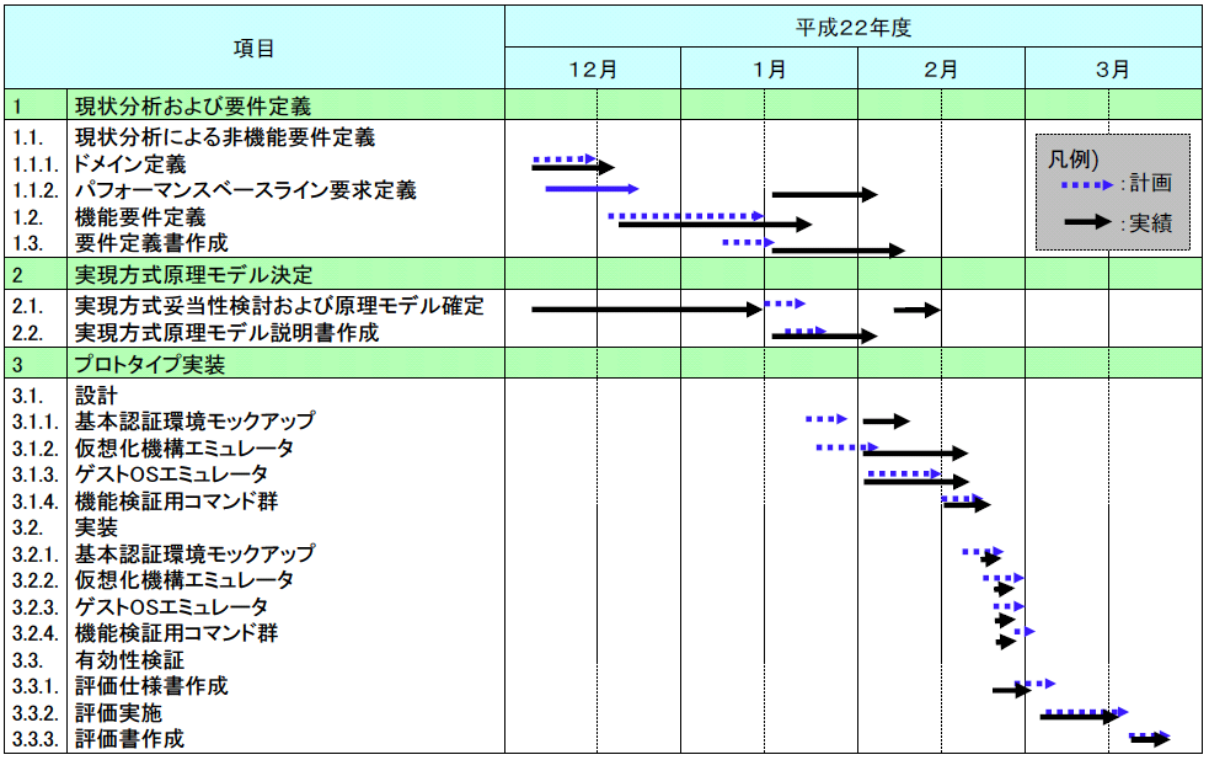
５－ｇ　研究開発マネジメント・体制・資金・費用対効果等

５－１－ｇ　研究開発計画

研究開発計画

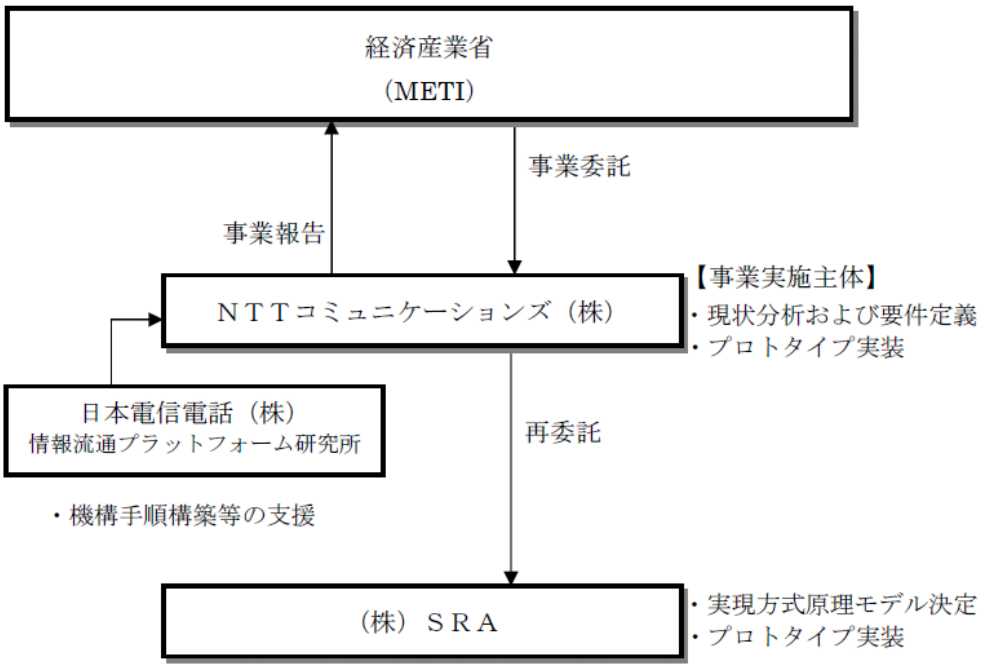
本事業は、平成 22 年度から 24 年度までの 3 年計画である。各要素技術の研究開発計画は次のとおりである。

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	**12.2**

５－４－ｇ　費用対効果

IDC Japan の調査（2013 年 10 月 24 日公表）によれば、2013 年の国内パブリッククラウドサービス市場は 1,321 億円であり、2017 年には 3,376 億円まで成長すると見込まれている。クラウド利用の拡大に伴い、コンプライアンスに抵触する恐れのある利用も増える可能性があるが、本成果による利用者自らがデータの管理・監督を行うことが可能な機構が普及することで、実態としてコンプライアンス違反となるようなクラウド利用の減少が期待できる。

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。

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、現在国内では、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い。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。

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。

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

４－Ｂ　事業化、波及効果について

４－１－Ｂ　事業化の見通し

事業で構築した共同利用設備は、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）が運用することと定められた。同社はハードウェア侵入テスト機関を内包して運用する。

当該ハードウェア侵入テスト機関は、自社内の 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ため、国内評価機関は、共同利用設備を引き続き共同利用することが可能である。

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。

（２）民間産業への波及効果

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

研究開発計画

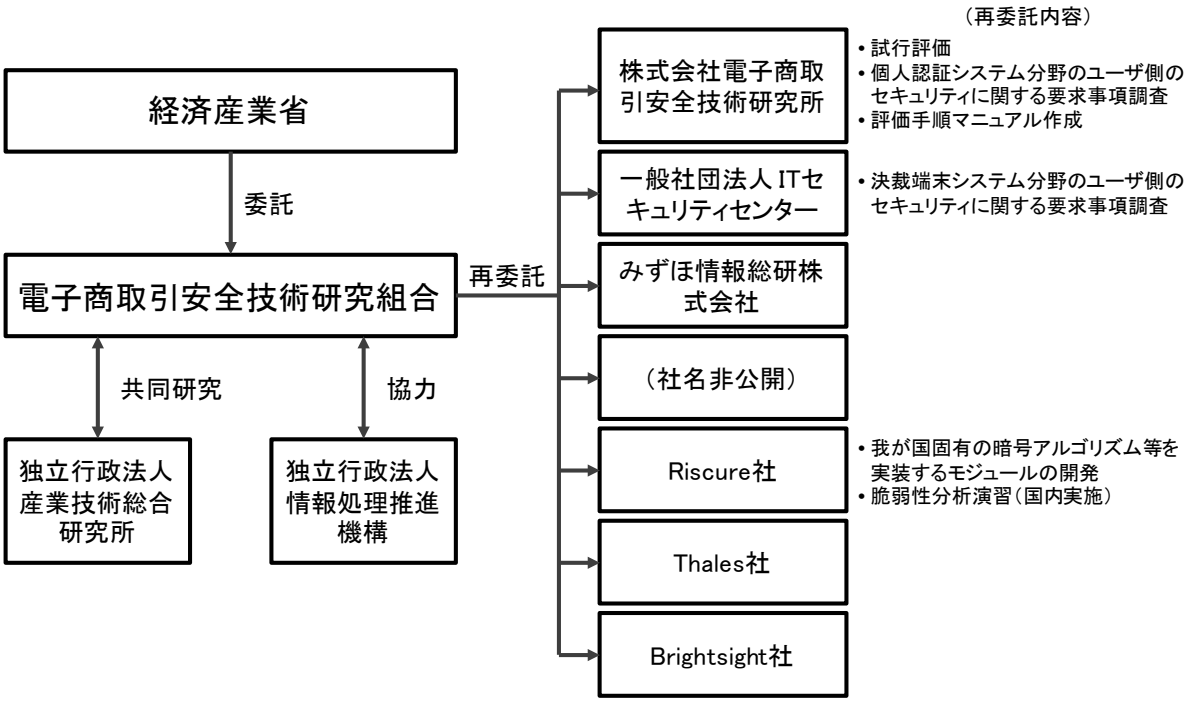
本事業は、平成 22 年度から 24 年度までの 3 年計画である。各要素技術の研究開発計画は次ページ表のとおりである。

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	評価ツールの開発	
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
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	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

鉄道における交通系 IC カードの導入状況に関する国土交通省の発表によれば、平成 25 年 3 月時点で交通系 IC カードの発行枚数は 8,700 万枚に及ぶ。このほか、金融庁の発表によれば、IC キャッシュカードが平成 25 年 3 月時点で約 1 億枚発行されるなど、IC カードは国民の社会生活に定着している。一方で、ひとたび IC カードのハードウェア部分に脆弱性が発見された場合、ソフトウェアのようにネットワーク経由でアップデートするような対策はとれず、交換を余儀なくされるため、対策コストは莫大なものとなる。本成果は、IC カードベンダにおいて、こうした脆弱性を出荷前に検出することを容易にするための取り組みであり、社会的な経済効果としても十分に

大きいものと見込まれる。

５－５－Ｂ　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。

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る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、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。

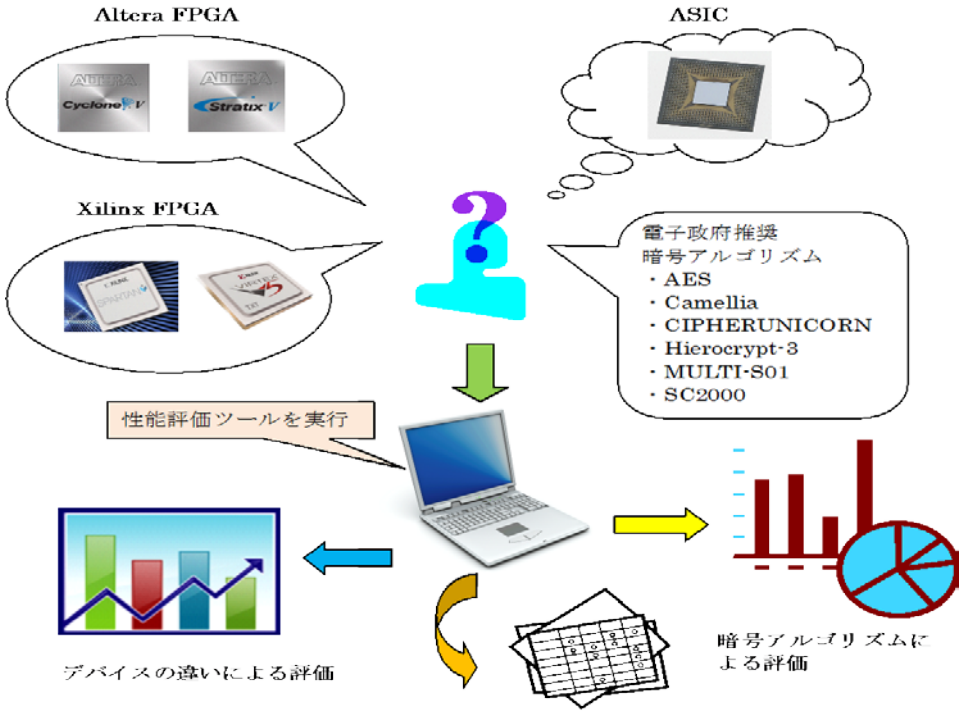
こうした状況に対応するため、暗号アルゴリズムの物理的安全性評価に必要な研究開発を実施し、その成果を暗号ハードウェア評価システムに統合する。

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

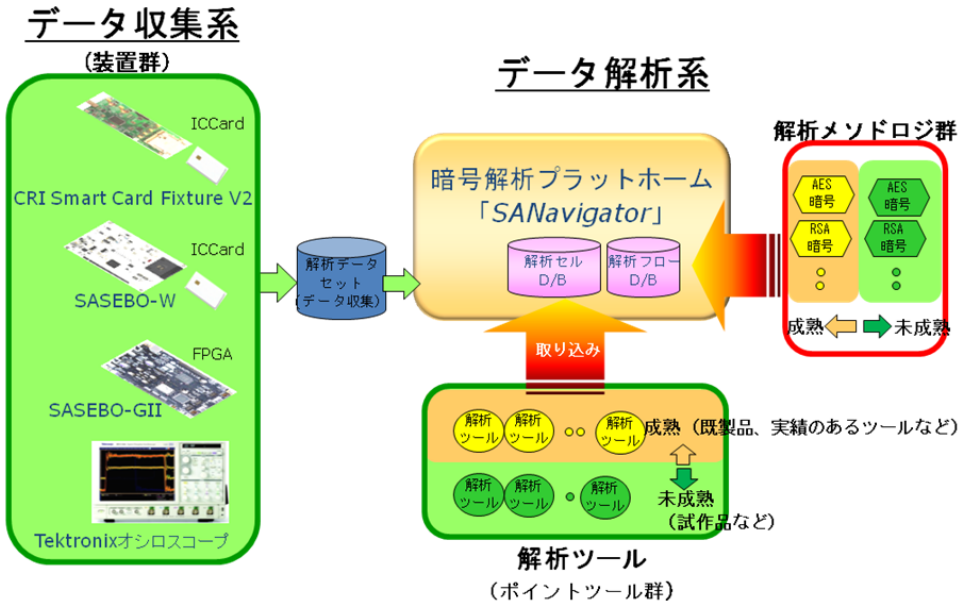
暗号アルゴリズムを実装したハードウェアモジュールの安全性を担保するために、各種サイドチャネル攻撃に対する網羅的な評価ツールを開発する。

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。

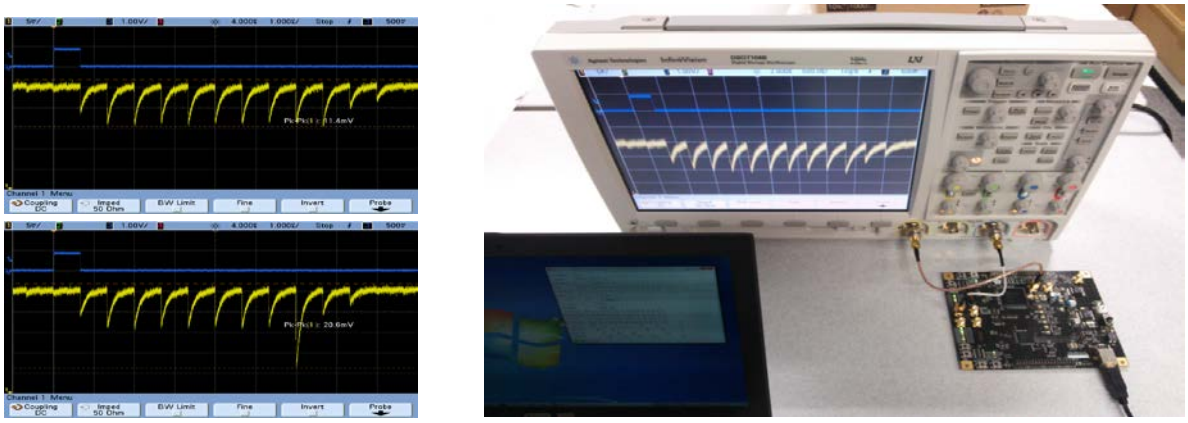


図Ｃ－３　サイドチャネル攻撃耐性評価ツールの機能

（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

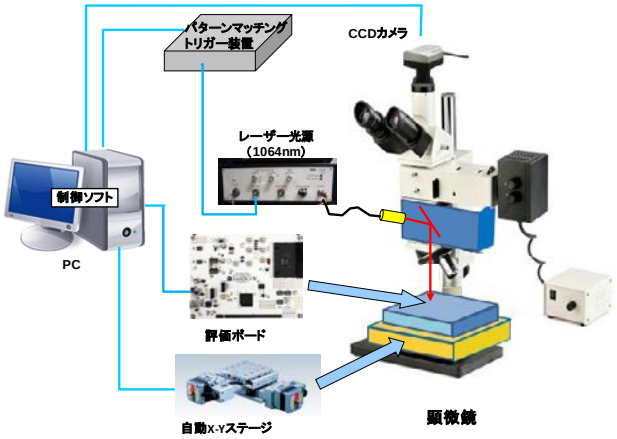
あるエラーを引き起こすことができない、あるいはエラーが発生したことを検出して暗号モジュールが何らかのアクションを取ることができるかといった観点で試験を行うこともできる。なお、再現性のあるエラーを引き起こせたとしてもそれが解析できるどうかは別の問題である。そこで、サイドチャネル攻撃評価ボード SASEBO の機能を拡張して、FPGA や、既開発の暗号 LSI、そして新規開発の IC カード評価装置にクロックや電源にグリッチを挿入して内部データやシーケンスにエラーを発生させる試験環境を構築する。



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。

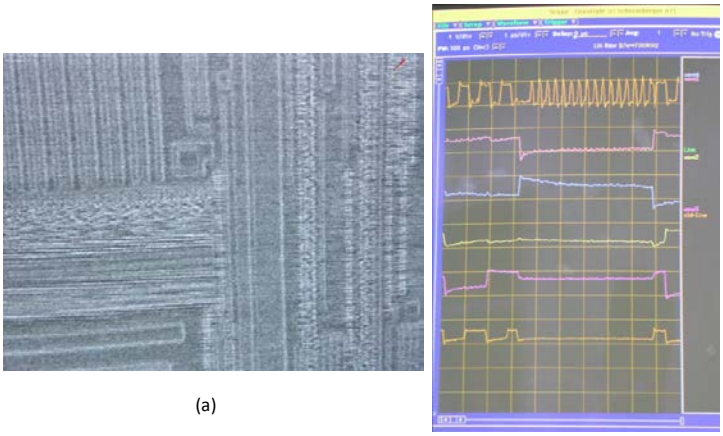


図Ｃ－５　レーザー照射システム構成図

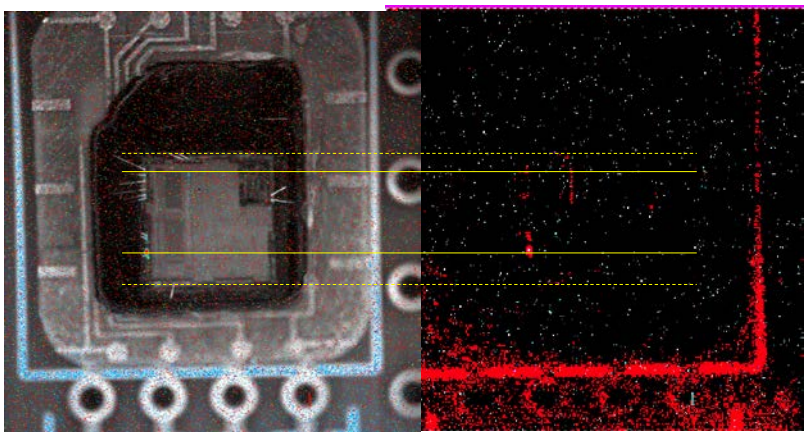
（１－５）集積回路解析技術によるLSI内部動作解析及び先端技術調査

FIB（集積イオンビーム）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。



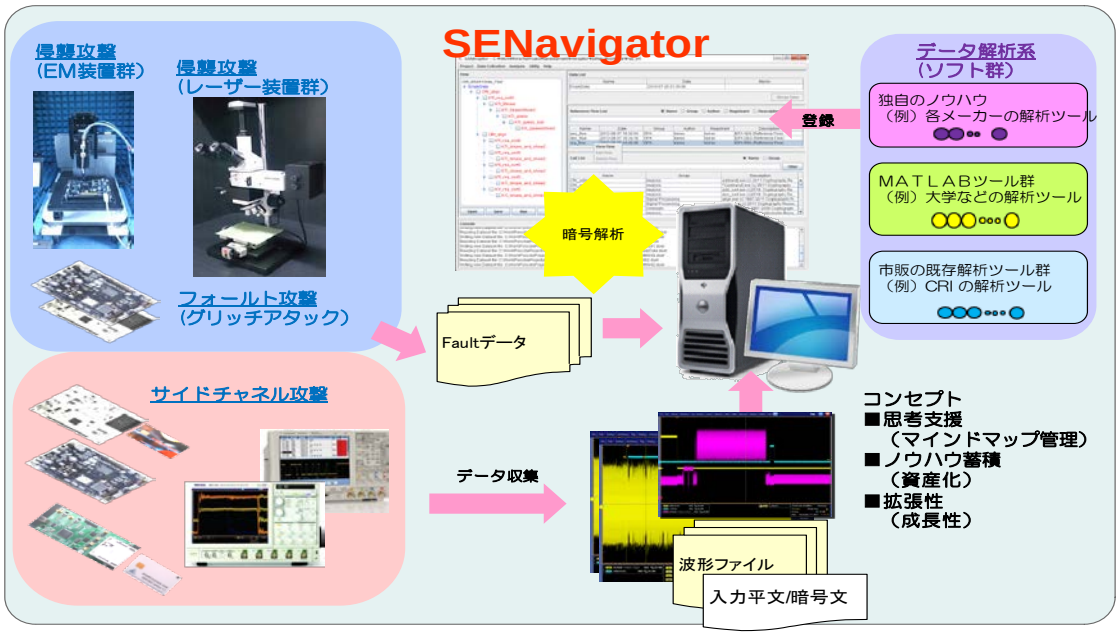
図Ｃ－６　ATMega IC Card Chip の(a)電位コントラスト像と(b)波形



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すすめている。

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システムと電磁界照射システムを開発した。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。

（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	・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

	ールを開発する		
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	・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界照射システムを開発した ・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	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。

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ト 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、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

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に設置することにより、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。

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。

各要素技術の研究開発計画は次のとおりである。

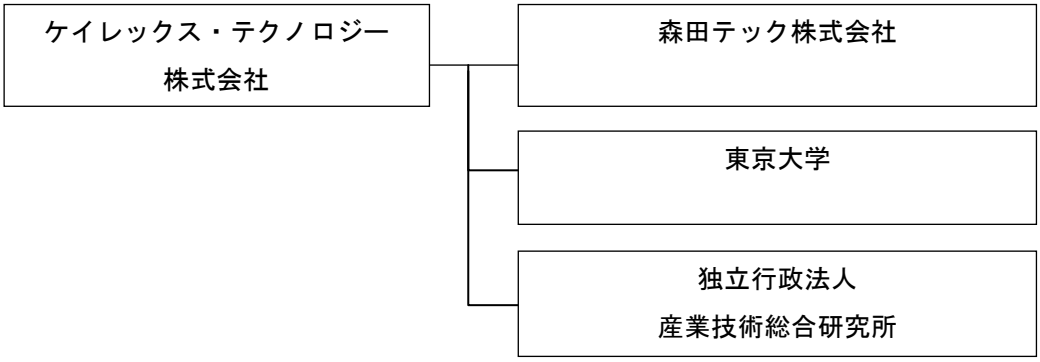
表Ｃ－５研究開発計画

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・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・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・パッケージ化		
④侵襲攻撃耐性評価環境の構築	開発・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

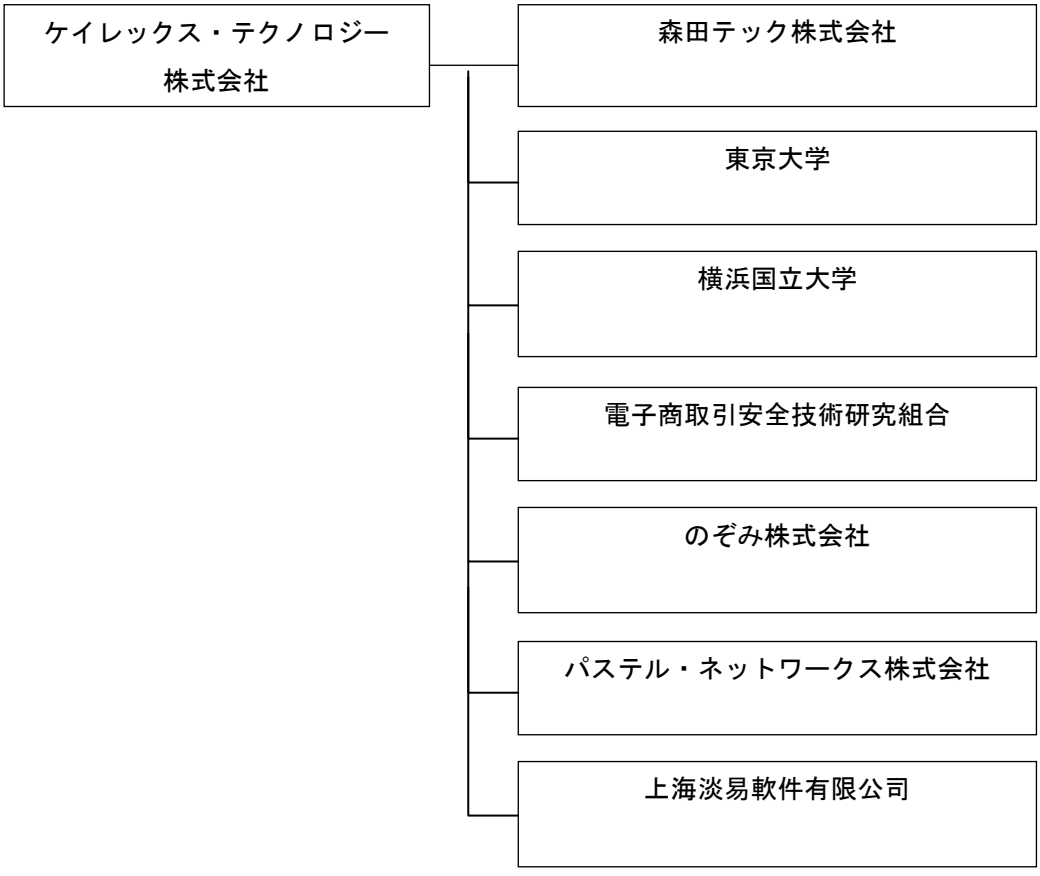
５－２－Ｃ　研究開発実施者の実施体制・運営

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。

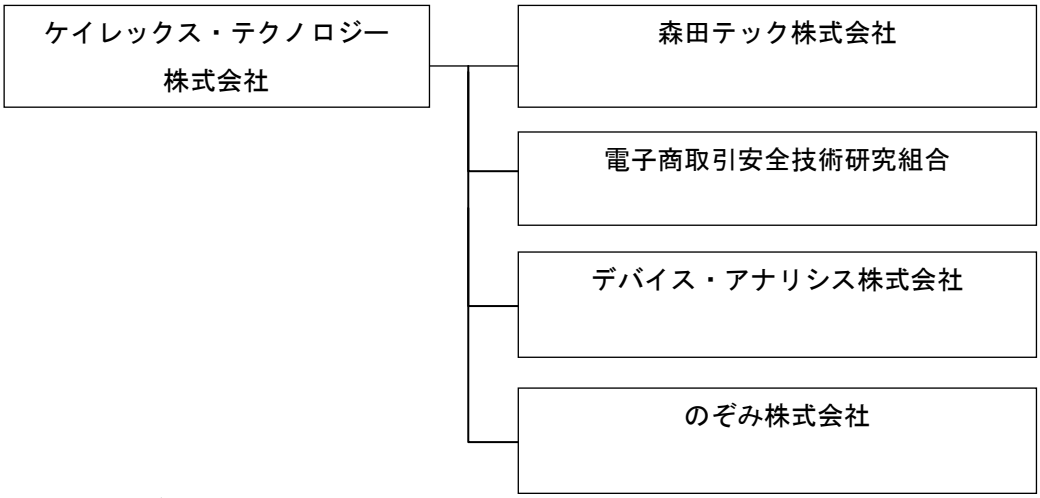
図Ｃ－９　研究開発実施体制（H23）



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。

レーザー、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、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。

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

本事業は、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、その国際標準化活動及び被災地における評価認証および普及啓発・人材育成の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及び重要インフラ等のセキュリティ強化、インフラ・システム輸出強化を目的とする。

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	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国際標準に準拠した第三者による製品認証方法の研究開発を実施する。また、被災地における評価・認証及び普及啓発・人材育成のための環境を整備する。	•世界でも米国のアイダホ国立研究所しか、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。 •重要インフラのセキュリティ確保、インフラ･システム輸出強化、復興支援の立場から被災地にてテストベッドを構築することは緊急性が高い。

３－２　成果、目標の達成度

３－１－２　成果

（１）成果

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、サイバーセキュリティテストベッドを宮城県多賀城市のみやぎ復興パークに構築した。さらにこの施設を活用するため、評価認証のためのツールの整備と環境構築を実施した。

（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

３－２－２　目標の達成度

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	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国際標準に準拠した第三者による製品認証方法の研究開発を実施する。また、被災地における評価・認証及び普及啓発・人材育成のための環境を整備する。	•みやぎ復興パーク（宮城県多賀城市）に、サイバーセキュリティテストベッド（CSS-Base6）を構築した。 •CSS-Base6には、模擬プラント7式を設置した。 •評価認証のためのツールの導入および環境構築を行った。	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、その国際標準化活動及び被災地における評価認証および普及啓発・人材育成のためのテストベッド CSS-Base6 を構築した。

平成 25 年度は、CSS-Base6 を活用した研究開発を継続しており、評価認証および普及啓発・人材育成に関しては CSS-Base6 を利用した事業の検討を行っている。高セキュア化に関しても、組合員にて研究成果を活用した製品化が進められている。

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。

1) CSS-Base6 の影響を受けて、オランダ ENCS にて類似施設構築がなされた

2) CSS-Base6 の見学者は 2013 年 5 月以降 2014 年 1 月までに 800 人を超えており、マスコミ取材も 10 社以上となっており、制御システムセキュリティに対する社会の認識が劇的に高まった

3)特に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。。

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、平成 23 年度の単年度の計画で実施された。

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。

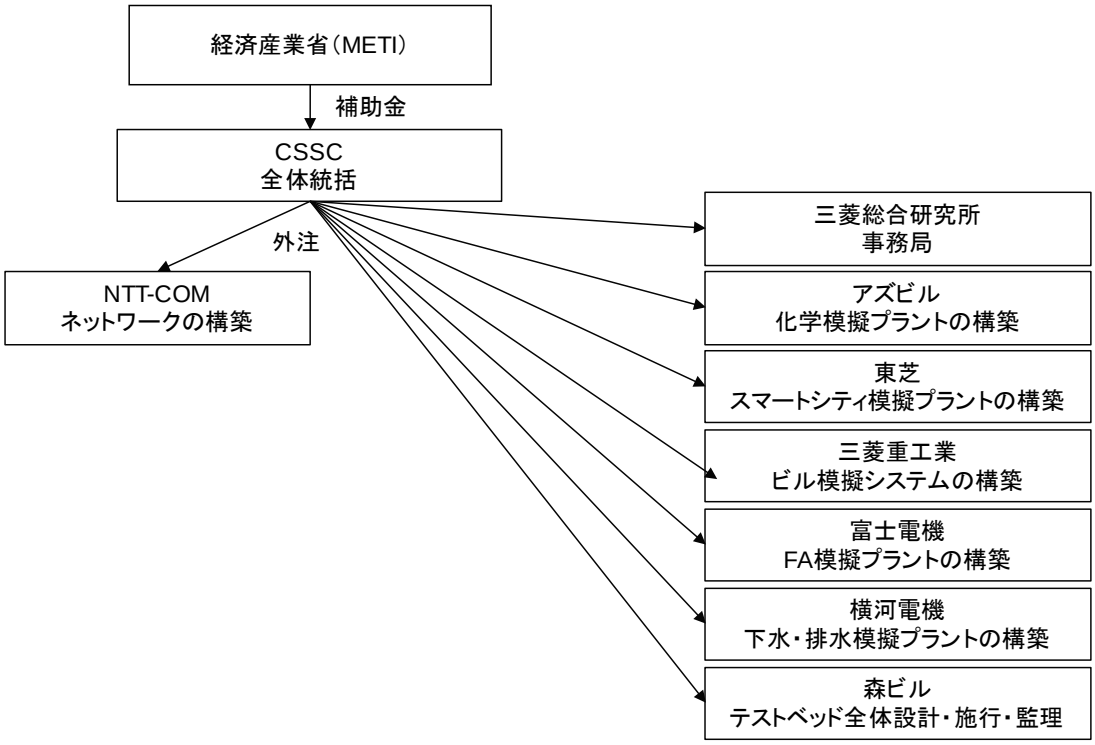


図２－１　研究開発実施体制

５－３－２　資金配分

表２－４　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

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、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国際標準に準拠した第三者による製品認証方法の研究開発、および評価認証と普及啓発人材のための環境が整い、制御システムセキュリティ研究推進の面から意義は大きい。

また、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。

このほか、組合員の数が、発足時の８者から約３倍に増加している。（平成２５年１２月現在２３者）

５－５－２　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。