第１１回評価ワーキンググループ
補足資料 － ２

情報セキュリティ分野に係る技術に関する施策・事業評価の概要について

平成26年4月16日

商務情報政策局情報セキュリティ政策室

目次

1. 技術に関する施策の概要

1. 施策の概要
2. 目的・政策的位置付け
3. 評価
4. 提言及び提言に対する対処方針

１．施策の概要

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

これを実現するため、以下を実施する（今回の評価対象は②及び③のみ）。

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

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

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

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

２．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

（＊）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）

課題に対応する
新戦略の必要性

「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

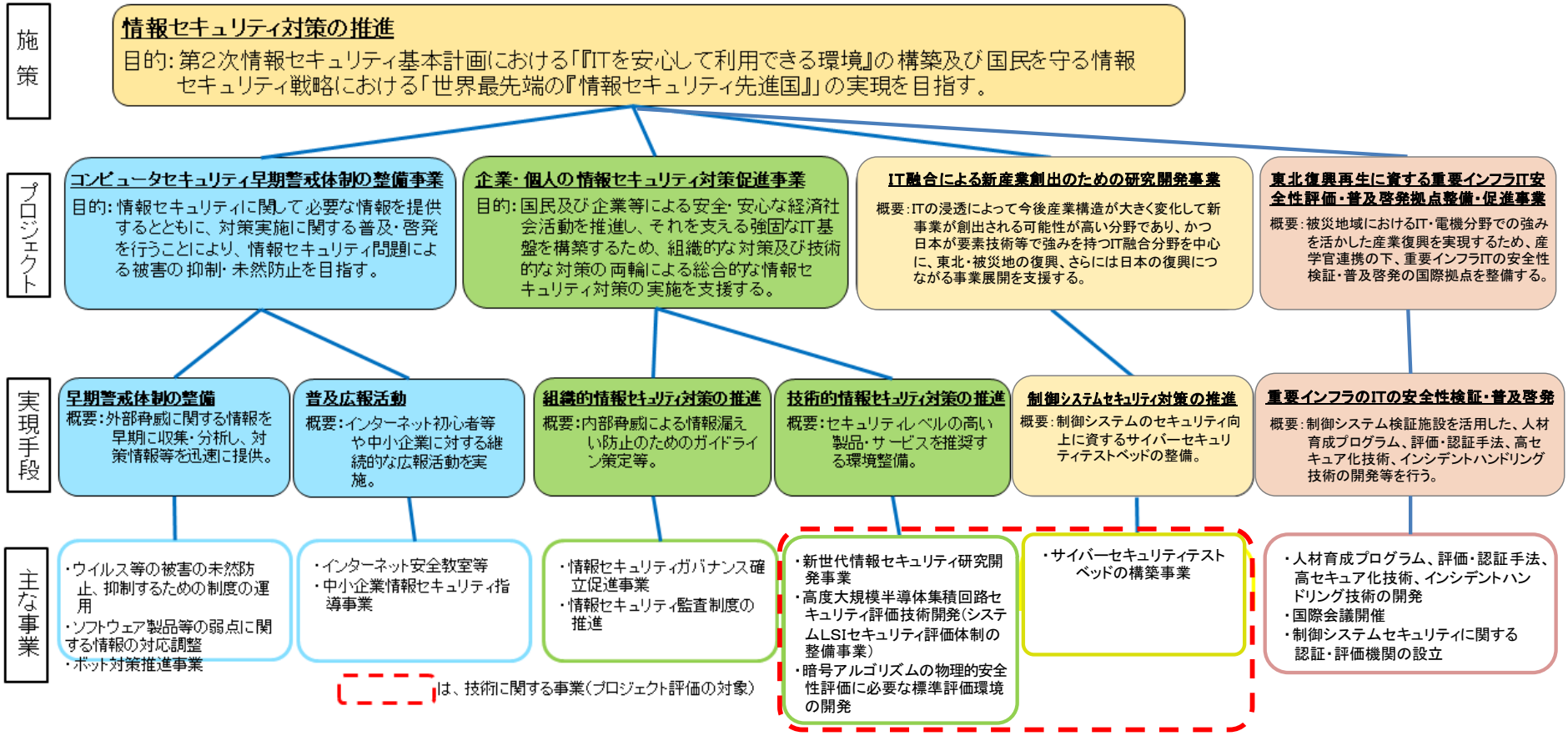
➢情報セキュリティガバナンスの確立
- ・情報セキュリティガバナンスの経営としての位置付け
- ・事業継続計画（BCP）の策定、情報セキュリティ監査　等

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

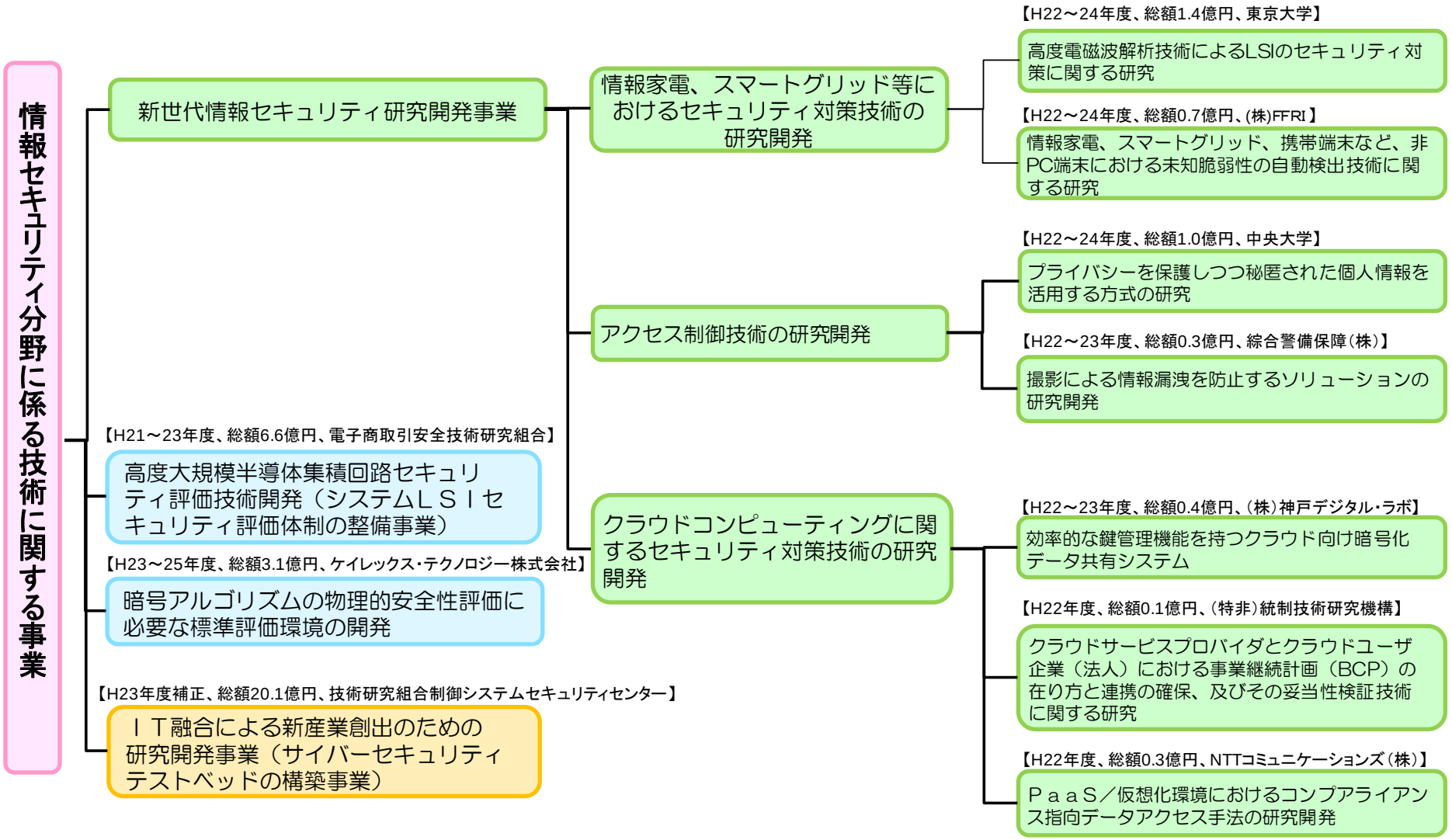
➢各国の情報セキュリティ制度の比較検討
- ・各国間の法制度等の相違について分析し、情報セキュリティ関連の国際連携のための課題抽出・連携方策の検討を実施

図1－3　情報セキュリティ対策の体系図

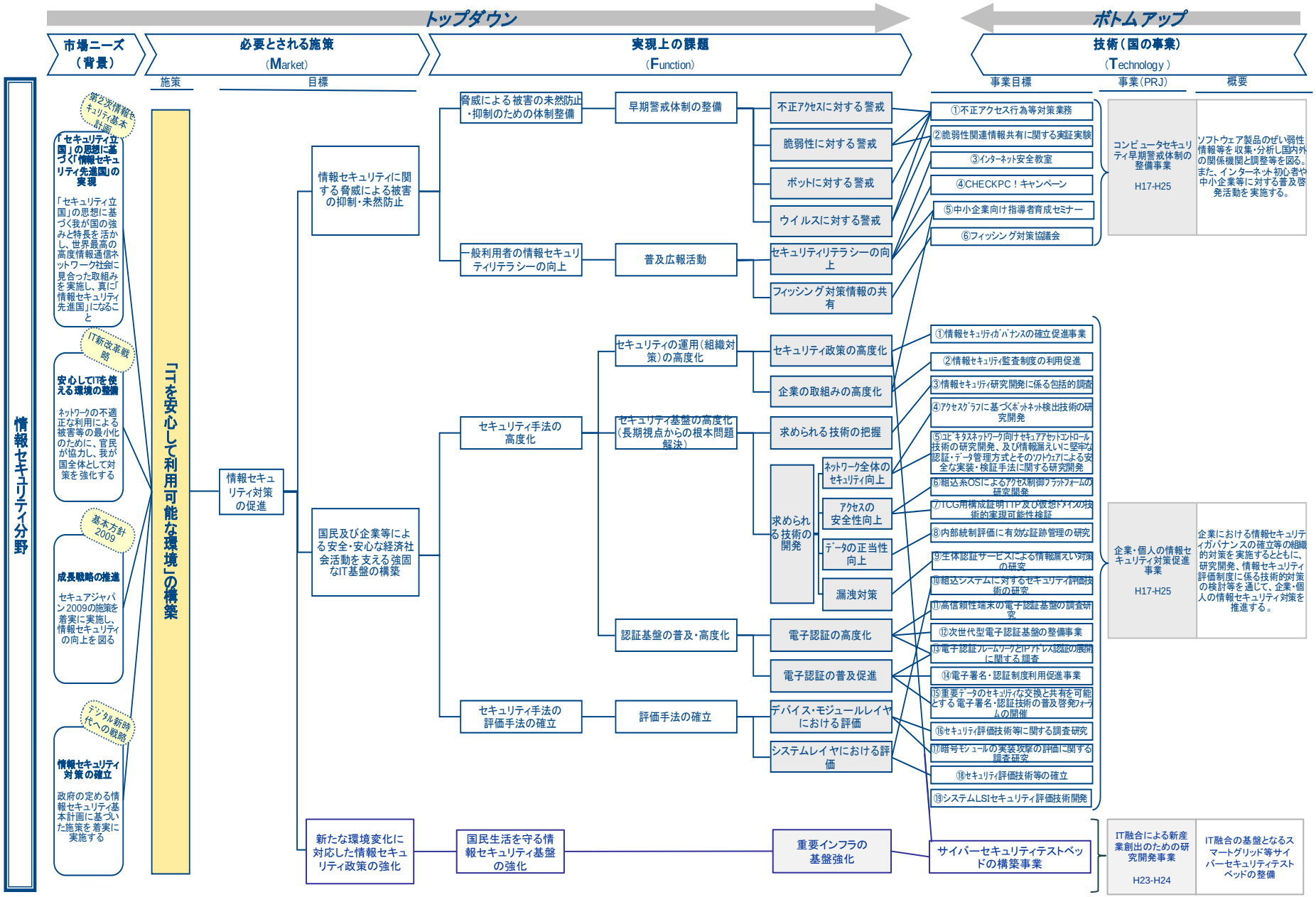


（注）平成24年度より、「コンピュータセキュリティ早期警戒体制の整備事業」と「企業・個人の情報セキュリティ対策促進事業」は統合され、「情報セキュリティ対策推進事業」となった。

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
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
データの正当性向上
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
重要インフラの基盤強化
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
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。
①情報セキュリティガバ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アクセスグラフに基づくボットネット検出技術の研究開発
⑤ユビキタスネットワーク向けセキュアセットコ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・データ管理方式とそのソフトウェ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プラットフォームの研究開発
⑦TCG用構成証明TTP及び仮想ド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生体認証サービ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アド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重要デ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暗号モジ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
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。
サイバーセキュリティテストベッドの構築事業
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。

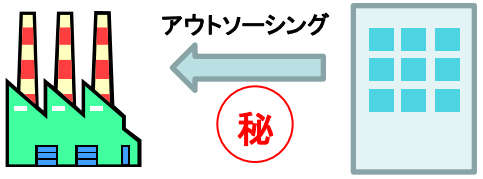
条件（対象者、対象行為、補助率等）

国 → 委託 → 民間企業等

事業イメージ

組織的対策の推進

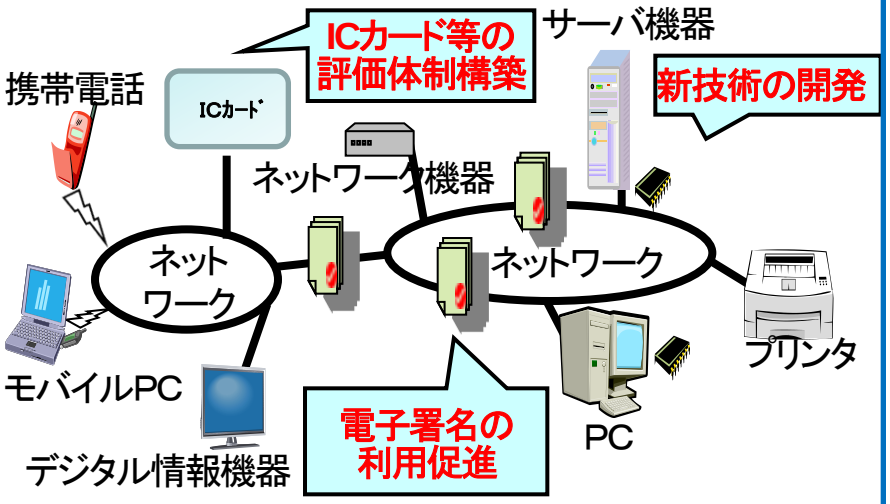
企業が情報セキュリティ対策を講じる際に参考とできるようなガイドラインを作成



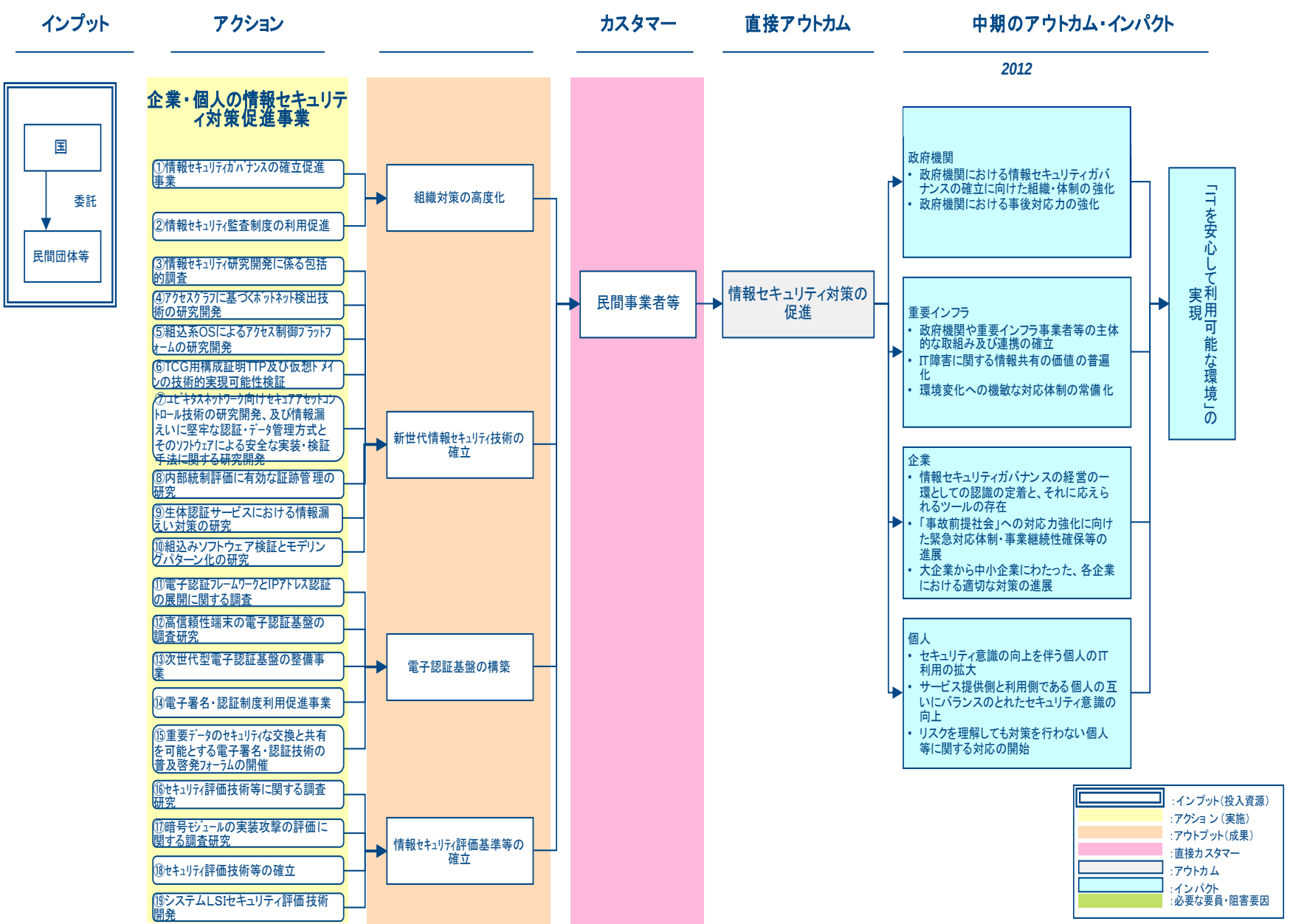
リスクを把握した上で、戦略的にアウトソーシング先を選定

技術的対策の推進

セキュリティ評価の推進　　技術開発の実施



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

3. 評価

3-1. 評価検討会

評価検討会名称		情報セキュリティ関連分野に係る技術に関する施策・事業評価検討会
評価検討会委員	座長	徳田　英幸 慶應義塾大学大学院 政策・メディア研究科委員長 教授
	委員	後藤　厚宏 情報セキュリティ大学院大学 情報セキュリティ研究科　教授 関口　和一 株式会社日本経済新聞社　論説委員 兼 編集委員 田辺　孝二 東京工業大学大学院 イノベーションマネジメント研究科　教授 西村　敏信 公益財団法人金融情報システムセンター 監査安全部長

3-2. 総合評価（コメント）（１）

施策の目的・政策的位置付けの妥当性

- 近年クラウドや携帯情報端末の普及が進む一方で、マルウェアの広がりに加え、国境を越えた組織的なサイバー攻撃が増えており、国民生活及び日本経済のセキュリティを確保する観点から、情報セキュリティ対策への需要は近年、非常に高まっている。情報セキュリティ対策は官民が一致協力して対応すべき課題であり、その意味において、中長期的視点に立ち、新たな脅威や既存脅威の巧妙化に対応するための情報セキュリティ技術の研究開発に国が積極的に関わることは極めて重要である。
- こうした中、当該事業の目的及び政策的位置付けは、「第2次情報セキュリティ基本計画」、「国民を守る情報セキュリティ戦略」に基づき、施策の目的、技術的課題を具体的に整理した上で実施され、さらに社会的ニーズへ適合していることから妥当である。
- なお、施策の目的を定める際には、産業・企業の情報セキュリティに関する技術的課題を総合的に検討し、中長期的な「情報セキュリティ研究開発戦略」を構築した上で、事業化に配慮した戦略的な研究開発として推進することが望ましい。また、公募案件として施策を実施していく場合、セキュリティ技術研究開発のポートフォリオを十分意識して、公募案件を設定すべきである。さらに、情報セキュリティ対策は各省庁横断的に重要な課題となっており、今後は各省庁連携のもとに有機的に機能する施策を共同して構築していくべきである。

3-2. 総合評価（コメント）（２）

施策の構造及び目的実現見通しの妥当性

- 本施策に配置された技術に関する事業は、施策の構造から必要なプロジェクトであり、スケジュール等も妥当である。また、各事業の技術開発のフェーズが異なるが、それぞれのフェーズにおいて妥当な成果が得られ、目標が達成されていることから、一定の成果を上げていると評価できる。
- なお、中間審査で成果があがっていない事業を中止した点は高く評価できる一方で、セキュリティ脅威に対する技術開発のポートフォリオに配慮することが望まれる。民間におけるクラウド技術開発は低コスト化競争にならざるを得ないため、国の事業として高信頼でセキュアなクラウド技術開発を進めるべきである。また、プロジェクトの配置に際しては、それぞれの事業ごとにPDCAサイクルを回し、全プロジェクトの中で適切なポートフォリオが描けているか、さらに注視する必要がある。

3-2. 総合評価（コメント）（３）

総合評価

- 中長期計画である「国民を守る情報セキュリティ戦略」などとの関係が明確であり、いずれの事業も重要な課題に取り組んでいる上に、認証機関の実現や普及に向けた活動のように、国の施策として価値ある波及効果も得られるなど、目的実現の見通しもあり、妥当であると評価する。
- なお、施策の構造及び技術に関する事業の配置の検討に際しては、日本の状況から必要な研究開発かのプライオリティとポートフォリオをより明確にするともに、他の関係機関や産官学の連携を意識したものとすべきである、また、認証機関に関わるものや、サイバーセキュリティテストベッドについては、構築だけでなくオペレーションについても支援すべきである。

4. 提言及び提言に対する対処方針

今後の研究開発の方向等に関する提言	提言に対する対処方針
● 技術開発の事業と、その事業化など、連携する施策間の関係を明確にした上で、事業の継続性を意識した枠組みを設けるとともに、中長期的な視点からその評価、検証を行うことが重要である。その中で、事業全体としての費用対効果を考えるべきである。 ● 技術に関する施策を公募案件で実施する場合、特に、情報セキュリティ技術開発に関しては、産官学間での信頼の輪を確立することが重要であり、申請チームの構成に関しても、配慮すべきである。事業化に関しても、適切なチーム編成を促進するような形の公募とすべきである。 ● さらなるクラウド普及促進のため、クラウド利用者が預けた個人情報等のデータに関して管理監督すること等を可能とする施策は重要であると考える。クラウド利用者が安全にクラウドを利用することに資する施策について、今後の課題とし継続検討されることを期待したい。	● 新世代情報セキュリティ研究開発事業については、事業の採択や事業の継続を審査する情報セキュリティ分野の学識経験者を中心とした有識者委員会を設け、事業実施者に対する各種アドバイスの実施、研究開発の方向性及びプロジェクト運営・管理・評価のあり方の検討、事業実施による成果についての評価についても、議論・検証しながら進めてきた。 ● ご指摘のとおり、技術に関する施策の実施にあたっては、産官学の連携や事業化を視野に入れたチーム編成といった視点は重要であり、今後の事業の実施の際には、十分に配慮してまいりたい。 ● クラウドに関する施策については、平成２３年４月、情報セキュリティ確保のためにクラウド利用者自ら行うべきことと、クラウド事業者に対して求めるべきことをまとめたガイドラインを公表した。また、クラウドサービスを取り巻く環境が著しく変化したため、本年４月には、現状に合わせた内容の追加、見直しを行い、改定版を公表したところ。

２．技術に関する事業の概要

Ａ　新世代情報セキュリティ研究開発事業

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

Ｃ　暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発

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

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・活用モデルのコンソーシアムでの事業化
			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
			クラウドサービスプロバイダとクラウドユーザ企業におけるBCPの在り方と連携の確保、及びその妥当性検証技術	特定非営利活動法人統制技術研究機構	（※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、当該テーマについては継続実施が不適切との判断がなされ、初年度のみの実施にて打切りとなった）
			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	NTTコミュニケーションズ株式会社	
(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

A

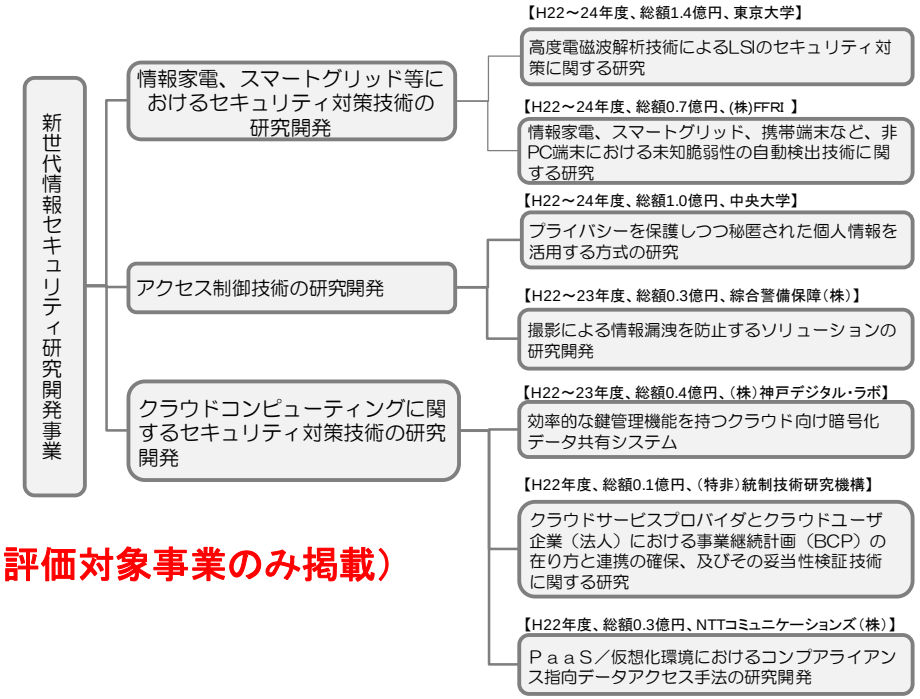
新世代情報セキュリティ研究開発事業

商務情報政策局情報セキュリティ政策室

目　次

1. 事業の概要
2. 目的・政策的位置付け
3. 目標
4. 成果、目標の達成度
5. 事業化、波及効果
6. 研究開発マネジメント、体制等
7. 中間評価に係る対処状況
8. 評価
9. 提言及び提言に対する対処方針

A-1. 事業の概要

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	

A-2. 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。

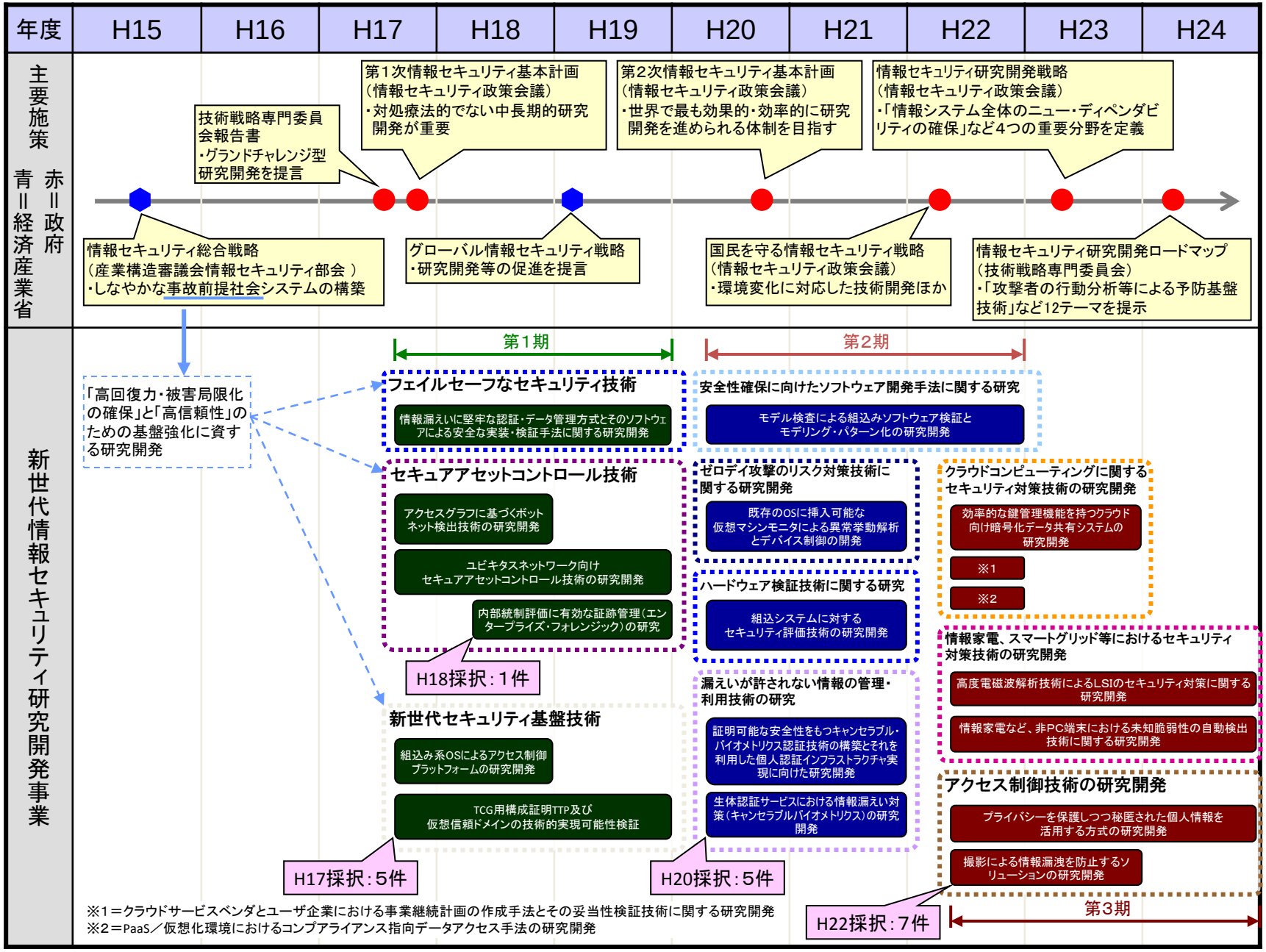
政策的位置づけ

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-3. 目標

新世代事業の目的を踏まえ、個別事業について以下の目標を設定した。

個別事業	目標・指標	妥当性・設定理由・根拠等
高度電磁波解析技術によるLSIのセキュリティ対策に関する研究	サイドチャネル攻撃を中心とする電磁波解析実験を通じて、電磁波中の情報取得に特化したマクロ磁界プローブの開発、磁界プローブをLSI上で移動しながら磁界計測を行う高精度スキャナの開発、高性能磁界プローブを実装した高精度スキャナの有効性を検証する評価実験用セキュリティ回路の開発、高精度磁界スキャナによって計測したデータを解析するツールの開発及び評価実験用セキュリティ回路による有効性の検証等を実施する。	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μ mオーダーの微少プローブを開発し、暗号回路上の局所情報の測定を可能にする。またこ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アクティブ振動制御システムを備えた高精度スキャナが必要。
情報家電、スマートグリッド、携帯端末など、非PC端末における未知脆弱性の自動検出技術に関する研究	攻撃モデルの変化と攻撃技術の進歩を長期的視点に立って分析し、将来に渡り適用可能である抜本的対策の仕組みとして、情報家電など、非PC端末における未知脆弱性の自動検出を行うことが可能なファジング方式のセキュリティ検査ツールの開発・評価を行うとともに、ツールで検査可能な機器と脆弱性の対象範囲の拡張を図る。	特別な知識を有しない一般的な技術者でも利用できる、モバイル機器で用いられるAndroid OSやWindows Phone7、ならびに制御機器で用いられているプロトコルに対応したファジングツールの開発を行うとともに、社会的ニーズに応え制御システムにも対応する。
プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究	「個人情報を秘匿化したまま収集、処理、活用する医療・介護連携ネットワーク」を実現するため、医療機関が保管する医療や介護における患者の記録などの機微な個人情報について、秘匿性を保ったまま、有効活用するために必要なプライバシー保護方式及び情報処理方式等の開発、オンラインで患者等から医療、介護等の機微な情報に関するアンケートを行う際に、回答者の匿名性を担保し、アンケート回答に対する心理的な障壁を低減するとともに、有効な統計情報を抽出して活用するために必要な暗号方式の開発及び性能評価等を実施する。	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。これを解決する暗号技術についても、これまでの方式ではアクセス権限毎の暗号化が必要であるなど、管理が必要な情報量の増加、利便性の低下、情報流出のリスクの増大が懸念される状況にある。

A-3. 目標

個別事業	目標・指標	妥当性・設定理由・根拠等
撮影による情報漏洩を防止するソリューションの研究開発	現状において十分な対策が講じられていない、「ディスプレイ上に表示されている情報の撮影」による情報漏えいを防止する手段として赤外線を活用するため、透明赤外線光源と赤外線遮断対抗技術の2種類の開発を行う。	人間の資格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与え、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。
効率的な鍵管理機能を持つクラウド向け暗号化データ共有システム	「鍵失効機能付き属性ベース暗号方式」の実用化を実現させ、安全・安心なクラウドコンピューティングサービスを提供する基盤を構築するため、鍵管理機能の構築、モデルシステムの構築、モデルシステムの実証実験、普及活動及び意見収集を実施する。	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を、クラウド環境上で属性ベース暗号を用いて構築可能かどうかの評価を行う。
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	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。	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。
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	ケーパビリティインジェクション機能とペアリング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。	ケーパビリティインジェクション機能により、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。ペアリング機構により、本来その機器及びシステムへの正しいアクセス権をもたない利用者による使用・管理を防止することができる。

A-4. 成果、目標の達成度

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

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

A−4. 成果、目標の達成度

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

A-5. 事業化・波及効果

事業化

- 本事業については、自社での製品化、受託開発における活用、公的実証における活用などの形で事業化が進められており、さらに連携先との交渉中のものもある。

波及効果

- 攻撃や不正の検知技術の開発を通じた攻撃や不正行為の抑止、暗号技術の活用による安全と利便性の両立、情報セキュリティ対策の効率化などの波及効果が期待できる。

個別事業	事業化	波及効果
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	• 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。 • 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おり、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。 • 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。 • 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。 • 自動車関連企業と車載部品の真贋判定について共同研究を検討中。 • 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。	• 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。 • 本成果を通じて低周波帯(MHz)の微弱な電磁波の分析が可能となったことが、電磁波の研究分野における新しいテーマを創出している。 • 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。現在未実現の機能の実装が実現した際には、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見込まれる。

A-5. 事業化・波及効果

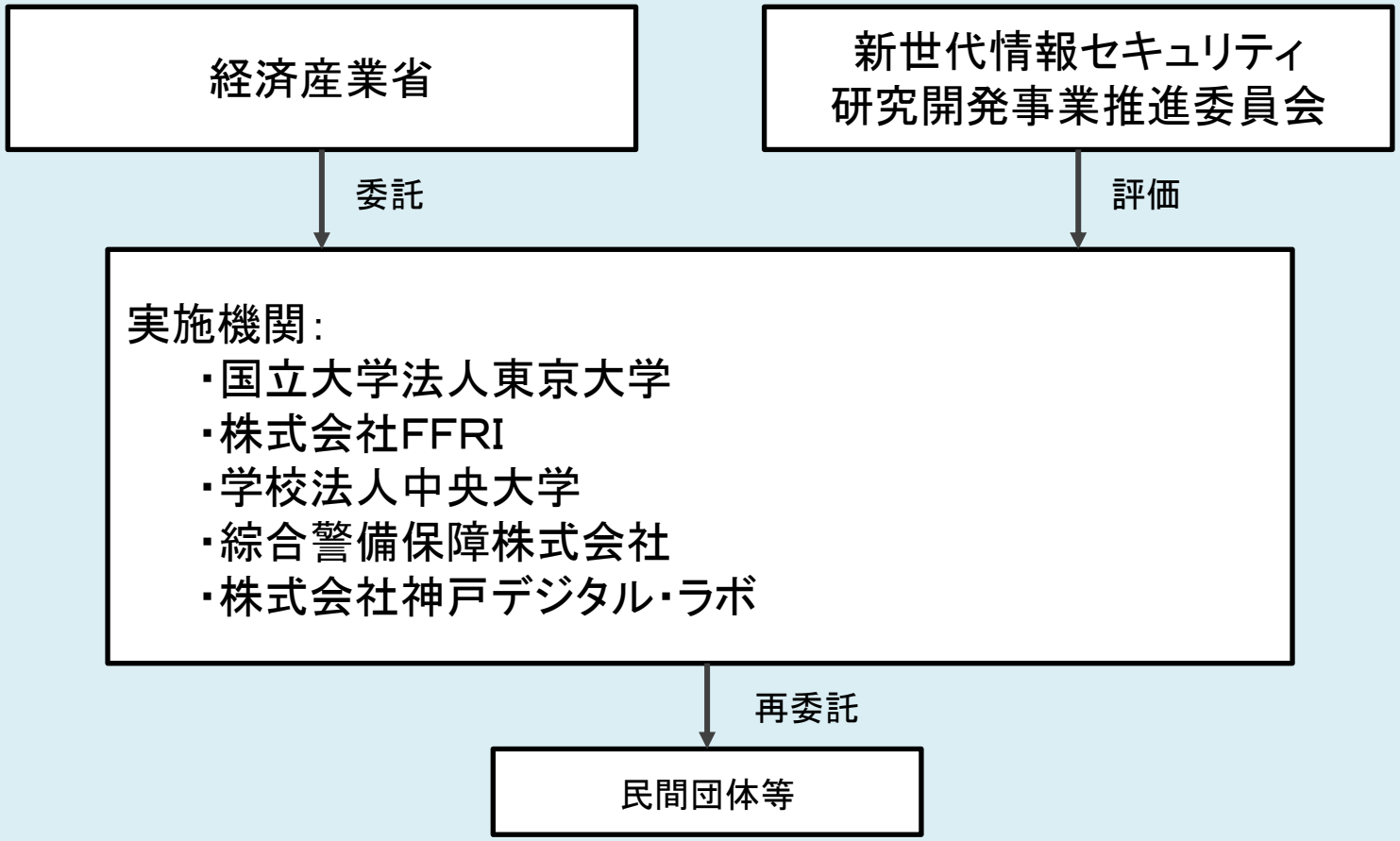
個別事業	事業化	波及効果
情報家電、スマートグリッド、携帯端末など、非PC端末における未知脆弱性の自動検出に関する研究	• 実施機関が自ら企業向けに提供する製品（FFR Raven）及びサービス（Android端末セキュリティ分析サービス）において活用中である。 • このほか、制御システム向け検査ツールに関しても、FFR Raven for ICSとして製品化が完了している。 • EDSA認証取得プロセスも完了予定である。	• 本成果を反映した製品は、従来のファジング用ツールと比較して安価であり、ユーザは低コストで脆弱性評価を行うことが可能。 • 海外の類似製品と比較して、今後も日本で用いられる情報家電、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。 • 国際会議での発表を通じて、我が国の脆弱性検査能力を国際的にアピールした。 • 研究開発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）を通じて報告を実施した。 • EDSAに準拠する検査機能の研究開発を行うことを通じて、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。
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	• 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。	• 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。

A-5. 事業化・波及効果

個別事業	事業化	波及効果
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	・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。ただし、低価格有機ELがまだ市場に存在しないほか、撮影者検知における誤検知防止のための精度向上、撮影防止ソリューションへのニーズが未だ不明確な点などが課題である。	・派生的成果として、開発した蛍光体ガラスを高級ガラス・陶磁器の真正性判定に利用することが可能（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り、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。
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	・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。	・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。
クラウドサービスプロバイダとクラウドユーザ企業（法人）における事業継続計画（BCP）の在り方と連携の確保、及びその妥当性検証技術に関する研究	（平成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ため、事業化・波及効果は無い）	
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		

A-6. 研究開発マネジメント・体制等

実施体制：



A-6. 研究開発マネジメント・体制等

【資金配分】

（単位：百万円）

個別事業	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
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に関する研究	24.7	23.1	20.5
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
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	
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	
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		
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		

A-6. 研究開発マネジメント・体制等

【費用対効果】

- 現在事業化されている成果を通じた売上は、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、売上以外で以下の効果が期待できる。
  - ハードウェアレベルの脆弱性への攻撃や、ＬＳＩ偽造の抑止
  - 脆弱性検査作業における生産性向上
  - 介護事業者への指示や記録類の電子化による省力化、転記誤り防止
  - 店舗バックヤードにおける防犯カメラの適切な管理による犯罪抑止

【変化への対応】

- **（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に関する研究）**
  脆弱性評価対象機器として、最新のAndroid OSやWindows Phone 7を追加したほか、制御システムに関する研究開発の比重を高めた。
- **（プライバシーを保護しつつ秘匿された個人情報を活用する方式の研究）**
  平成22年3月に発生した東日本大震災を受け、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。
- **（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）**
  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た。

A−7. 中間評価に係る対処状況

中間評価の結果	中間評価に係る対処状況
● 各テーマについて、当初予定の定性的目標は達成し、成果として社会に還元されているものもある等、波及効果を含め、国家、グローバルに貢献できていると思われる。 ● なお、国が行う事業として方向性、目的、予想される成果を設定する段階で、正しく現在の社会の問題と解決する課題を定義することで、もっと明確に事業目標を達成できたか否かを評価することが望ましい。 ● また、技術的な研究開発に重点が置かれていることから、開発された技術成果の事業化などに対しても注力することが望ましい。	● 第3期の公募分野の設定に際しては、情報家電、スマートグリッド、クラウドコンピューティング等における情報セキュリティ対策を対象とするなど、現在の社会の問題に対応した課題を選んでいる。一方で、達成状況については、本事業が中長期的な視点に立った課題解決を目指していることもあり、現時点では評価することは難しく、引き続き成果に基づく事業化の推進と、波及効果の把握に努めてまいりたい。 ● 開発された技術成果の事業化に関しては、事業の実施状況の適切性を審議する有識者委員会（新世代情報セキュリティ研究開発事業推進委員会）が、事業期間中から実施者に対して事業化に向けた活動状況の報告を求める等、積極的な取組みを行ってきた。その結果もあって、第3期において所定期間の研究開発を行った5テーマのうち、3事業で事業化の見通しが立つなど、事業化の達成率は第1期、第2期と比較して良好なものとなっている。

A−8. 評価

A−8−1. 評価検討会

評価検討会名称		情報セキュリティ関連分野に係る技術に関する施策・事業評価検討会
評価検討会委員	座長	徳田　英幸 慶應義塾大学大学院 政策・メディア研究科委員長 教授
	委員	後藤　厚宏 情報セキュリティ大学院大学 情報セキュリティ研究科　教授 関口　和一 株式会社日本経済新聞社　論説委員 兼 編集委員 田辺　孝二 東京工業大学大学院 イノベーションマネジメント研究科　教授 西村　敏信 公益財団法人金融情報システムセンター 監査安全部長

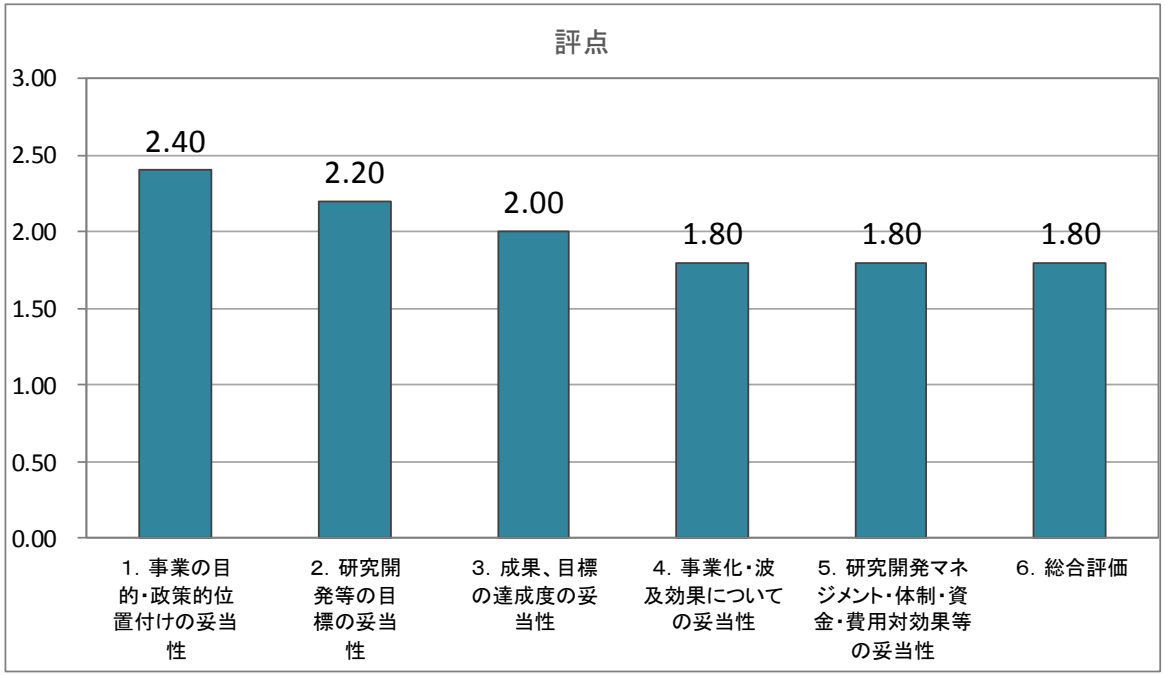
A-8-2. 総合評価（コメント）

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

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

A-8-3. 評点結果

- 「経済産業省技術評価指針」に基づき、プロジェクト事後評価において、評点法による 評価を実施した。
- 「事業化、波及効果についての妥当性」「研究開発マネジメント・体制・資金・費用対効果等の妥当性」：一部事業化に至っていない点に課題があったという評価から。
- 「総合評価」：結果的にクラウドコンピューティングに関する研究開発の比率が減るなど、セキュリティ技術研究開発のポートフォリオとして改善すべき課題があったとの評価から。



【評価項目の判定基準】
評価項目1.～5.
3点：非常に重要又は非常によい
2点：重要又はよい
1点：概ね妥当
0点：妥当でない

6. 総合評価
（中間評価の場合）
3点：事業は優れており、より積極的に推進すべきである。
2点：事業は良好であり、継続すべきである。
1点：事業は継続して良いが、大幅に見直す必要がある。
0点：事業を中止することが望ましい。

（事後評価の場合）
3点：実施された事業は、優れていた。
2点：実施された事業は、良かった。
1点：実施された事業は、成果等が今一歩のところがあった。
0点：実施された事業は、成果等が極めて不十分であった。

A-9. 提言及び提言に対する対処方針

今後の研究開発の方向等に関する提言	提言に対する対処方針
● 中長期的な視点に立ち、IT技術の進化に先回りした情報セキュリティ技術の研究開発を目指すべきである。多様な要素技術を基盤として統合する際の技術課題については国の施策として取り組む必要がある。 ● 国際的な開発競争が激しくなってきているIoT（Internet of Things）技術、サイバーフィジカルシステム、連携された重要生活機器（車やスマートフォン）に対する新たな脅威に関して、根本的な問題解決を目指す情報セキュリティ技術開発や標準化対応を考慮すべきである。 ● クラウドコンピューティングの高信頼化、セキュア化に関する事業は、我が国の競争力強化において重要である。特に、ビッグデータ向けのクラウド基盤技術は、そのセキュリティにおいて技術的に未解決の重要課題が多い。	● 新世代技術セキュリティ対策推進事業における第3期の事業公募にあたっては、「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）等の政府関連施策を踏まえつつ、情報セキュリティに係る技術の進歩に伴う新たな脅威の出現、既存脅威の一層の巧妙化が続いている情勢を受けて、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、②アクセス制御技術の研究開発、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、を重要なテーマと設定して実施してきたところ。 ● 引き続き、国の施策との整合性、経済社会、技術の進展への対応について、ご指摘を踏まえつつ、重点分野を見極め、効果的な事業の実施に努めてまいりたい。

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

目　次

B−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

B-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

B−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。

B-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

B-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	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）

B-5. 事業化・波及効果

事業化

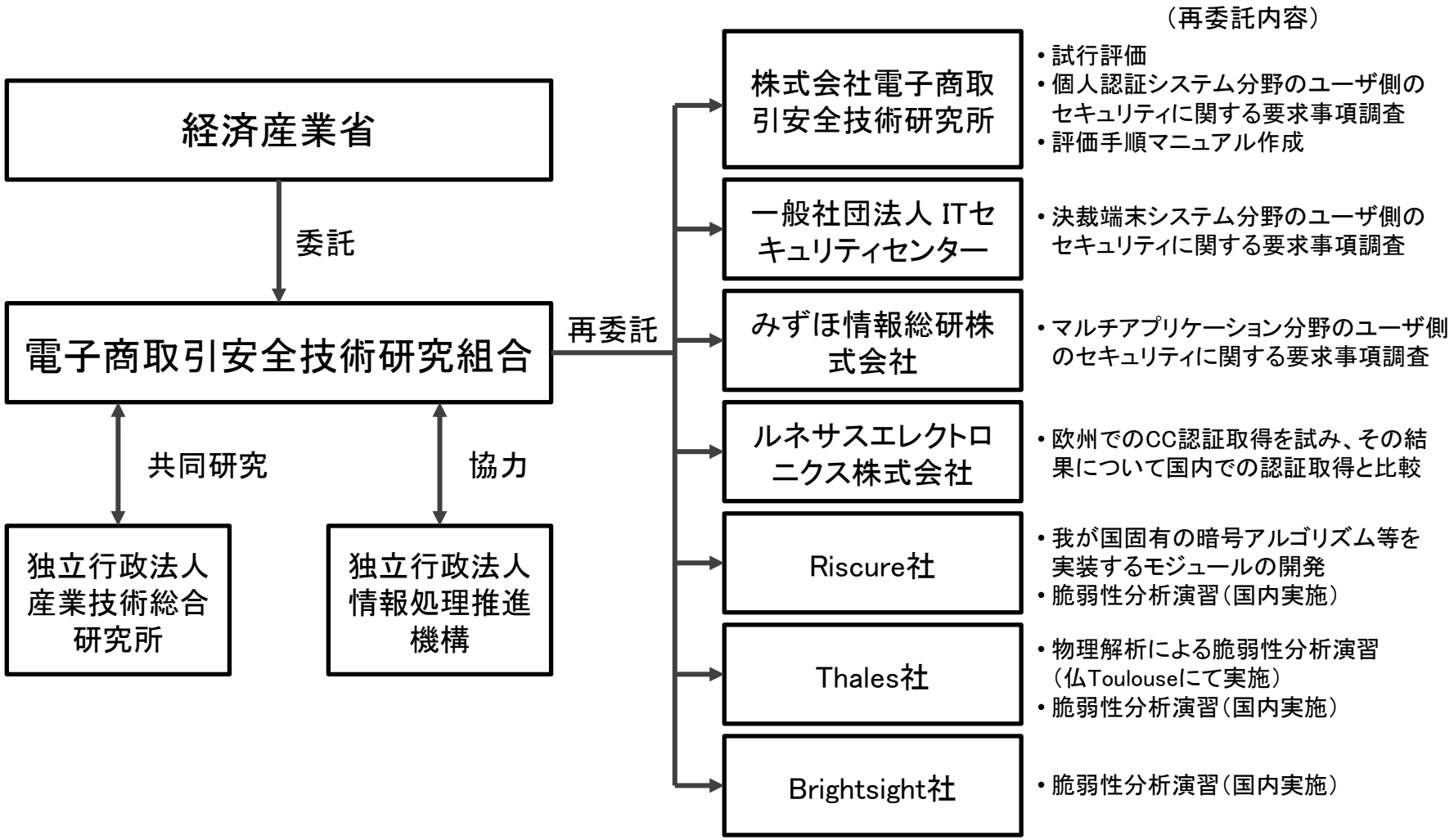
- 本事業で構築した共同利用設備をはじめとする成果は、現在の株式会社ECSEC Laboratory（旧社名：株式会社電子商取引安全技術研究所）に引き継がれ、平成24年9月、国内におけるICカード等ハードウェアのセキュリティ評価体制が確立した。
- 同社はハードウェア侵入テスト機関を内包して運用している。当該ハードウェア侵入テスト機関は、同社内のCC（Common Criteria）評価機関だけでなく、他社のCC評価機関に対してハードウェアCC評価における侵入テストサービスを提供することを可能とした。これは、国内における他のCC評価機関が個別に設備を保有することは資金面を考慮すると難しいため、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

B-6. 研究開発マネジメント・体制等

実施体制



B-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）	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。

B−7. 評価

B−7−1. 評価検討会

評価検討会名称		情報セキュリティ関連分野に係る技術に関する施策・事業評価検討会
評価検討会委員	座長	徳田　英幸 慶應義塾大学大学院 政策・メディア研究科委員長 教授
	委員	後藤　厚宏 情報セキュリティ大学院大学 情報セキュリティ研究科　教授 関口　和一 株式会社日本経済新聞社　論説委員 兼 編集委員 田辺　孝二 東京工業大学大学院 イノベーションマネジメント研究科　教授 西村　敏信 公益財団法人金融情報システムセンター 監査安全部長

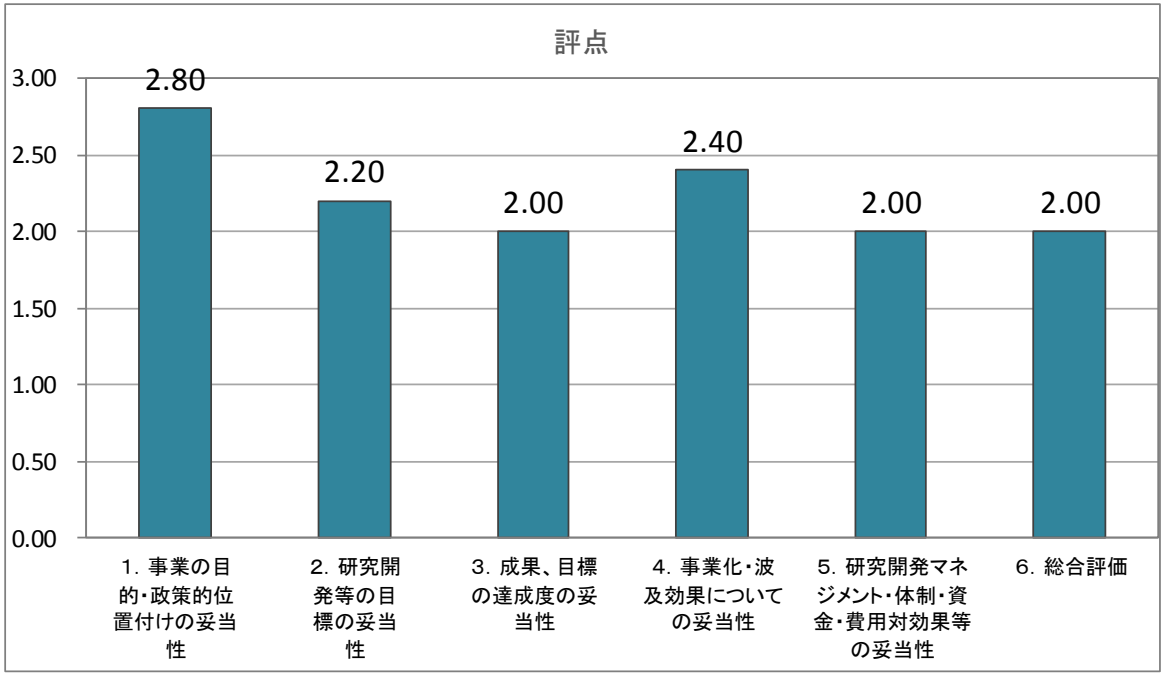
B-7-2. 総合評価（コメント）

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

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

B-7-3. 評点結果

- 「経済産業省技術評価指針」に基づき、プロジェクト事後評価において、評点法による 評価を実施した。
- 国内初のICカードセキュリティ評価環境の実現を目指す事業目的と、その波及効果について評価されている。



【評価項目の判定基準】
評価項目1.～5.
3点：非常に重要又は非常によい
2点：重要又はよい
1点：概ね妥当
0点：妥当でない

6. 総合評価
（中間評価の場合）
3点：事業は優れており、より積極的に推進すべきである。
2点：事業は良好であり、継続すべきである。
1点：事業は継続して良いが、大幅に見直す必要がある。
0点：事業を中止することが望ましい。

（事後評価の場合）
3点：実施された事業は、優れていた。
2点：実施された事業は、良かった。
1点：実施された事業は、成果等が今一歩のところがあった。
0点：実施された事業は、成果等が極めて不十分であった。

B-8. 提言及び提言に対する対処方針

今後の研究開発の方向等に関する提言	提言に対する対処方針
● 中長期的な視点に立ち、IT技術の進化に先回りした情報セキュリティ技術の研究開発を目指すべきである。多様な要素技術を基盤として統合する際の技術課題については国の施策として取り組む必要がある。	● 本事業は、中長期的な視点に立ち、我が国の産業競争力強化等の観点から、これまで欧州の評価認証に依存してきた、ICカード等のハードウェアセキュリティを評価する環境を我が国に整備するため、①セキュリティ評価を行うために必要な技術の開発、②共同利用設備の整備、③人材育成、④海外技術動向調査等を実施したもの。本事業の成果をもとに、平成24年9月、株式会社ECSEC Laboratoryが国内初のハードウェアセキュリティ評価機関としてスタートした。 ● 本事業は平成23年度で終了し、一定の成果を得たが、引き続き、欧州におけるハードウェアセキュリティに関する協議体であるJHASとの交流を継続し、欧州における最新の脆弱性情報等を国内にフィードバックしていく。 ● また、育成した人材の定着と継続的なキャリアサイクルを回すための活動については、個々の評価機関単位ではなく、産業界全体で考えていくべき重要な課題であると認識しており、引き続き検討してまいりたい。

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

C-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

C-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。

C-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

C−5. 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

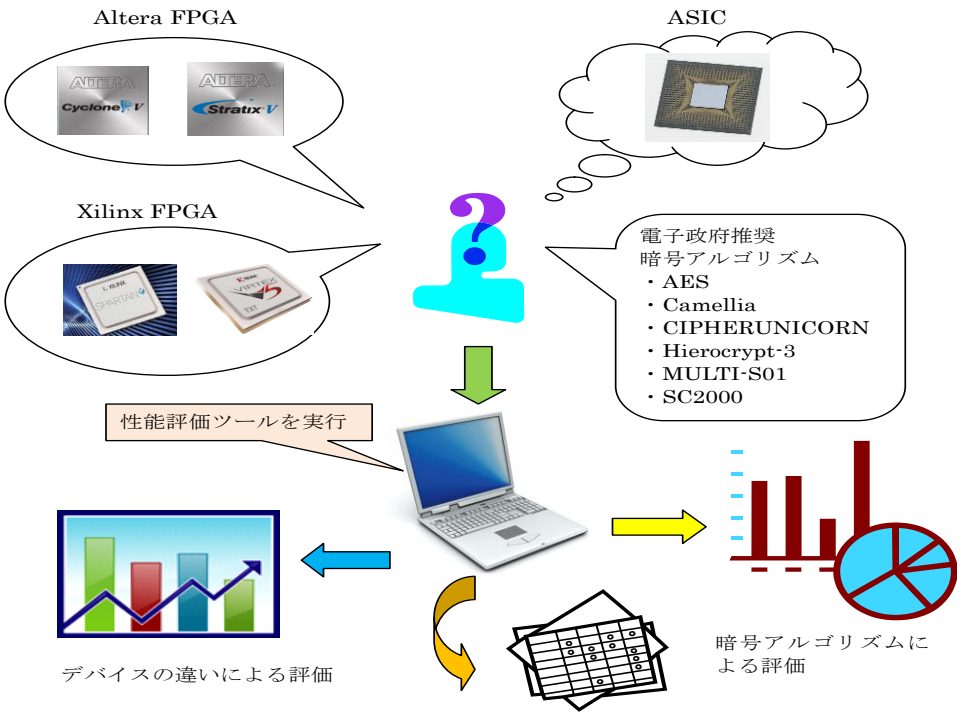
	要素技術	目標・指標	成　果	達成度
課題3	フォールト攻撃耐性評価ツール及び試験装置の開発	クロックや電源にグリッチを挿入してエラーを発生させる試験環境を構築する	・クロック信号、リセット信号、電源それぞれに非常に細いパルスを混入するグリッチ機能を開発した ・その環境を使用して評価実験を行い、検証のため解析プログラムを開発した	達成
課題4	侵襲攻撃耐性評価環境の構築	パッケージを開封してLSI内部の動作を直接操作する侵襲攻撃評価を行う環境を構築する	・外乱誘発装置としてレーザー照射装置と電磁界照射装置を開発した ・LSIのCADデータを用いて照射座標を制御したり、フォールトの発生状況を描画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

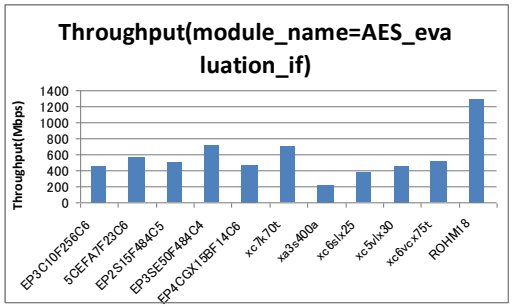
課題1:暗号ハードウェア実装性能評価ツールの開発

・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。



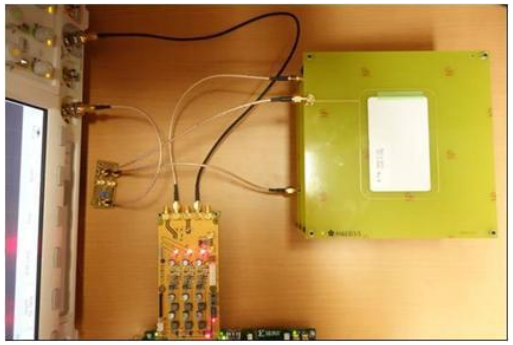
module	vender	familiy	device	slice	area	max clock frequency[MHz]	power [mW]	input blocks[bits]	cycle	throughput [Mbps]
AES_evaluation_if	Altera	Cyclone3	EP3C10F256C6	6721		87.4	59.76	512	100	447
AES_evaluation_if	Altera	Cyclone5	5CEFA7F23C6	2638		109.56	129.81	512	100	561
AES_evaluation_if	Altera	Stratix2	EP2S15F484C5	2825		97.04	325.1	512	100	497
AES_evaluation_if	Altera	Stratix3	EP3SE50F484C4	2767		138.48	435.66	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		73.196	72.18	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	504
AES_evaluation_if	ROHM		ROHM18	429676		252.525	2.5834	512	100	1293

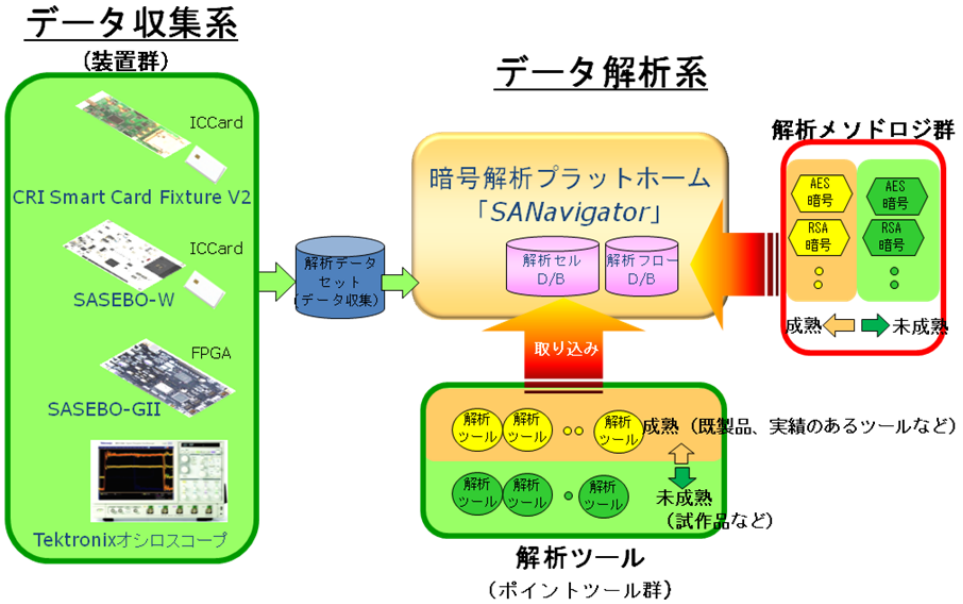


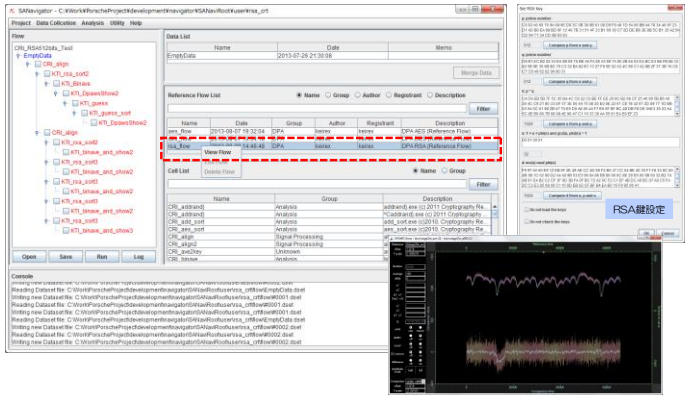
課題2:サイドチャネル攻撃耐性評価ツールの開発

・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。



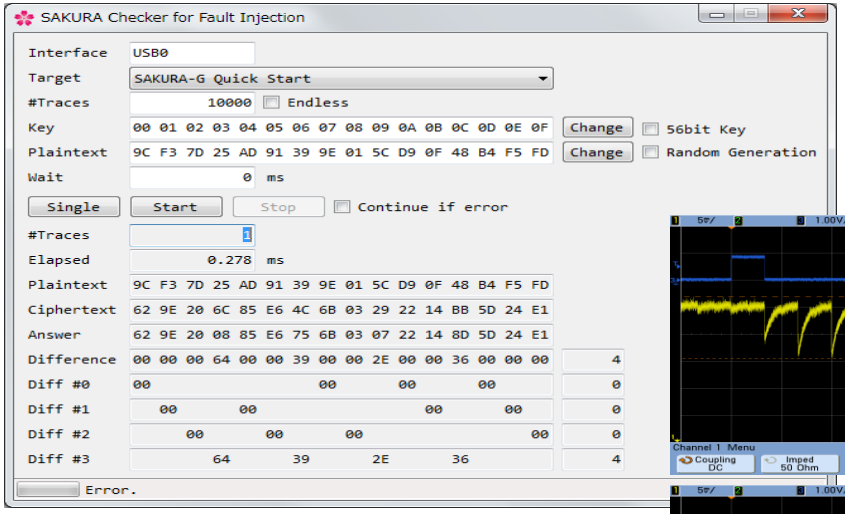


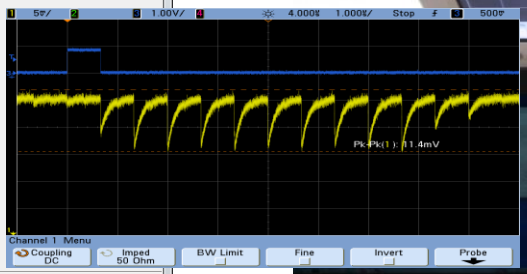


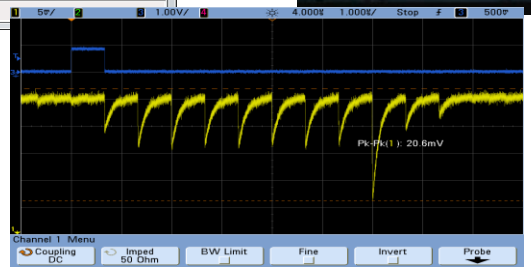
課題3:フォールト攻撃耐性評価ツール及び試験装置の開発

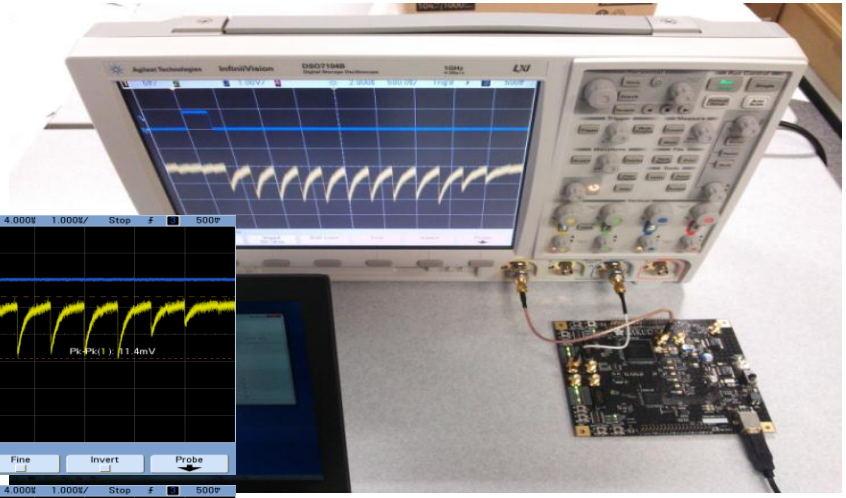
・グリッチ機能の開発
標準評価ボードであるSASEBO-GIIやSAKURA-Gを用いてFPGAをターゲットとしたフォールト評価環境を、SASEBO-Wを用いてICカードをターゲットとしたフォールト評価環境を構築した。

・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。





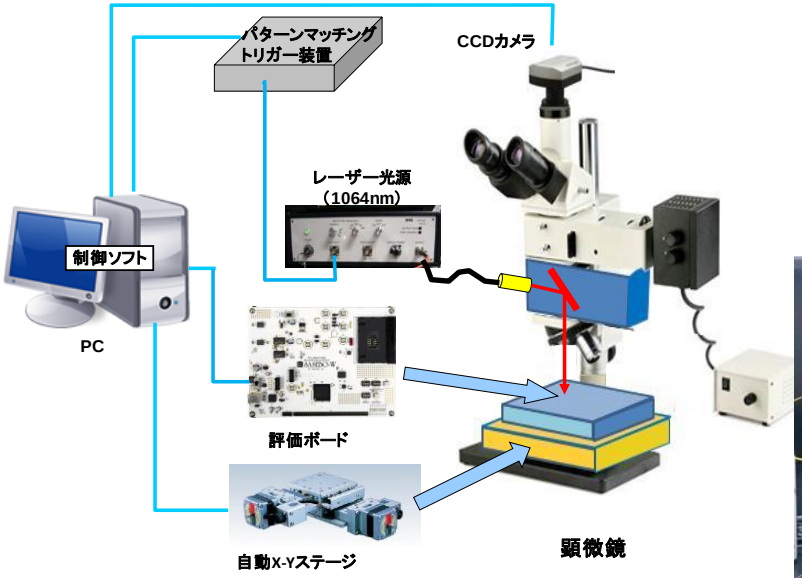


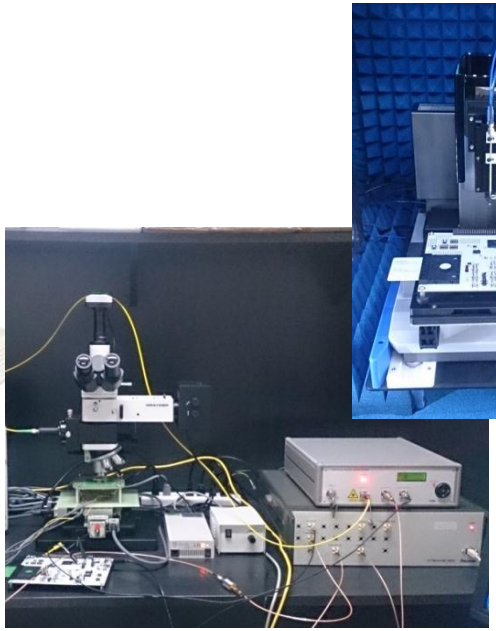


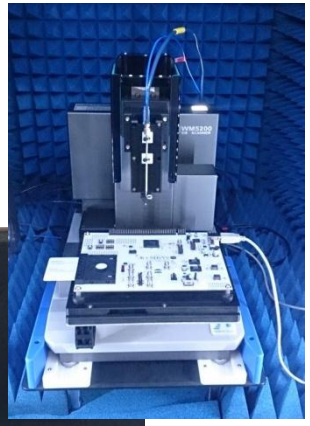
課題4:侵襲攻撃耐性評価環境の構築

・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。



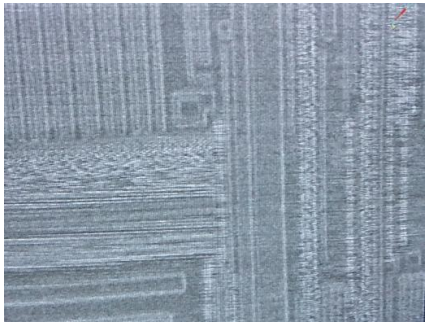




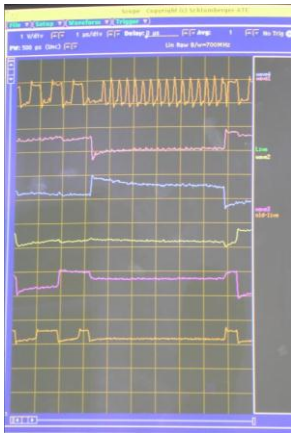
課題5:集積回路解析技術によるLSI内部動作解析及び先端技術調査

・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。

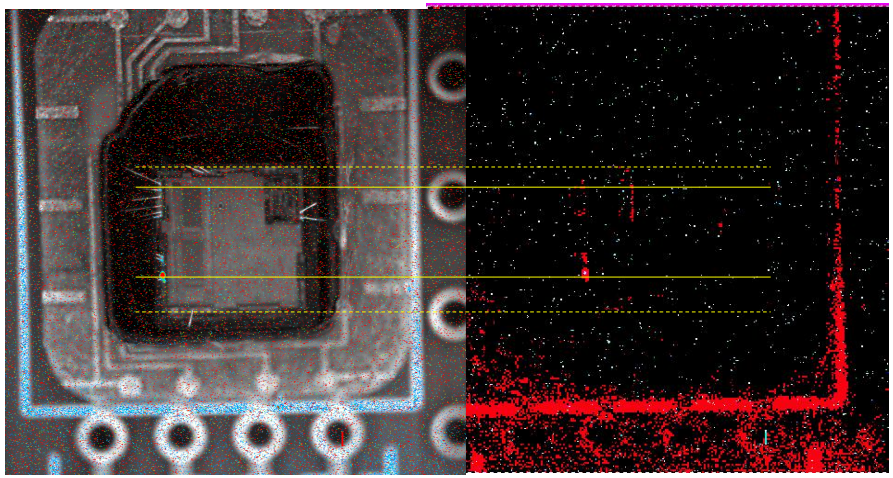
・発光解析と電子線プローブ観測結果との対比
同一のチップに対して発光解析を行ったところ、電子線プローブでの観測結果とよい対応関係を示していることを確認した。この結果から、電子線プローブ及び表面発光解析技術を用いることにより、ある程度のLSI 動作解析が可能であることが示された。



(a)



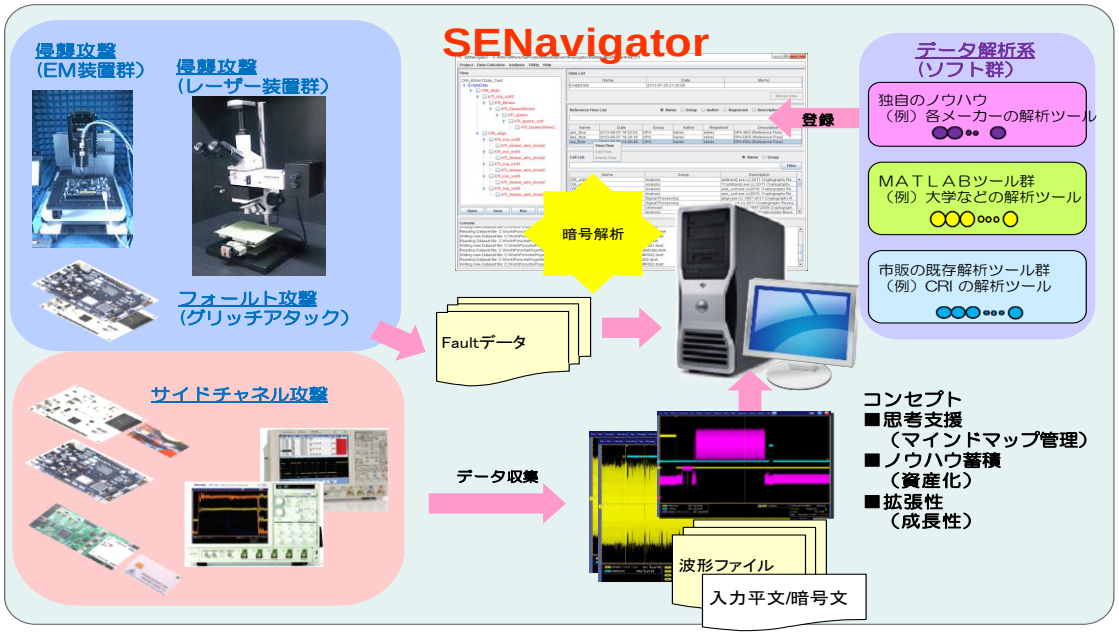
(b)



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

C-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。平成25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。

C-6. 研究開発マネジメント・体制等

実施体制：

平成25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：畑田　智子

・統合ハードウェア評価プラットフォームの開発
・サイドチャネル攻撃評価パッケージの開発及び統合化・実用化検証
・実装性能評価パッケージの統合化・実用化検証

↓ 再委託

森田テック株式会社

・フォールト・侵襲攻撃評価パッケージの開発及び統合化・実用化検証
・レーザー及び電磁波照射装置の開発

↓ 再委託

電子商取引安全技術研究組合

・統合ハードウェア評価プラットフォームの構築サポートと評価

↓ 再委託

デバイス・アナリシス株式会社

・フォールト攻撃評価用チップ加工

↓ 再委託

のぞみ株式会社

・フォールト攻撃評価機構（パターンマッチングトリガ装置）の開発

実施体制：

経済産業省（METI）

委託

平成24年度

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

C-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。

C−7. 評価

C−7−1. 評価検討会

評価検討会名称		情報セキュリティ関連分野に係る技術に関する施策・事業評価検討会
評価検討会委員	座長	徳田　英幸 慶應義塾大学大学院 政策・メディア研究科委員長 教授
	委員	後藤　厚宏 情報セキュリティ大学院大学 情報セキュリティ研究科　教授 関口　和一 株式会社日本経済新聞社　論説委員 兼 編集委員 田辺　孝二 東京工業大学大学院 イノベーションマネジメント研究科　教授 西村　敏信 公益財団法人金融情報システムセンター 監査安全部長

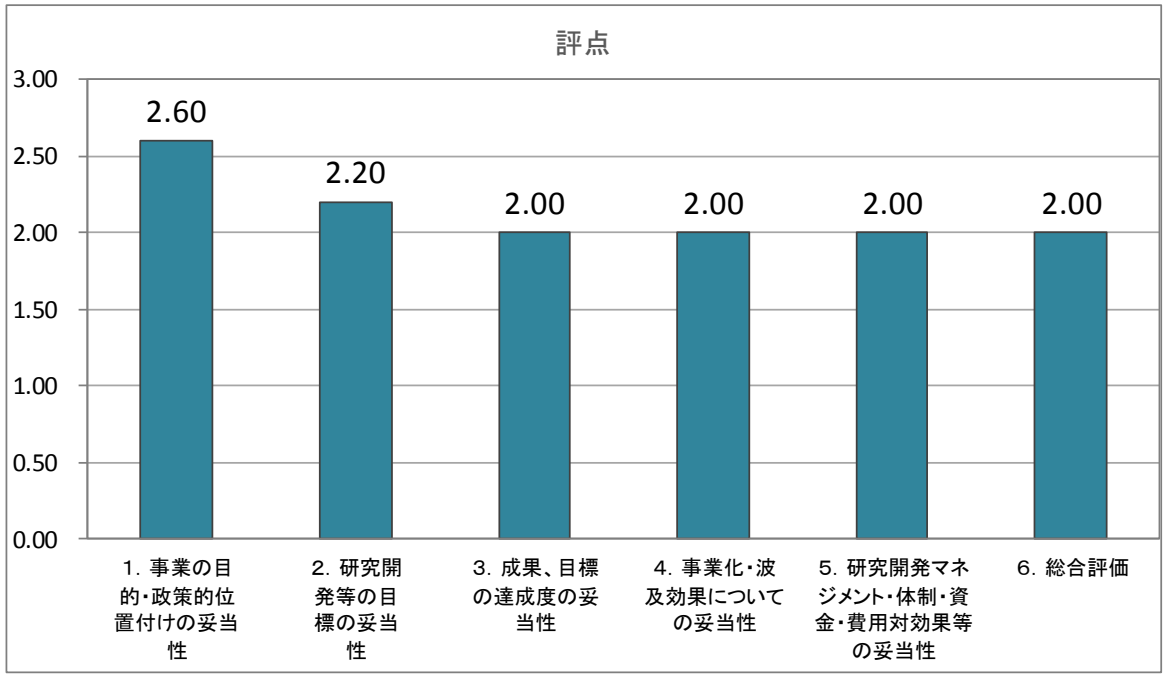
C-7-2. 総合評価（コメント）

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

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

C-7-3. 評点結果

- 「経済産業省技術評価指針」に基づき、プロジェクト事後評価において、評点法による 評価を実施した。
- 暗号アルゴリズムの物理的安全性評価に関する社会的な必要性に応える事業であることが、事業目的及び政策的値位置付けにおいて評価されている。



【評価項目の判定基準】
評価項目1.～5.
3点：非常に重要又は非常によい
2点：重要又はよい
1点：概ね妥当
0点：妥当でない

6. 総合評価
（中間評価の場合）
3点：事業は優れており、より積極的に推進すべきである。
2点：事業は良好であり、継続すべきである。
1点：事業は継続して良いが、大幅に見直す必要がある。
0点：事業を中止することが望ましい。

（事後評価の場合）
3点：実施された事業は、優れていた。
2点：実施された事業は、良かった。
1点：実施された事業は、成果等が今一歩のところがあった。
0点：実施された事業は、成果等が極めて不十分であった。

C-8. 提言及び提言に対する対処方針

今後の研究開発の方向等に関する提言	提言に対する対処方針
● 中長期的な視点に立ち、IT技術の進化に先回りした情報セキュリティ技術の研究開発を目指すべきである。多様な要素技術を基盤として統合する際の技術課題については国の施策として取り組む必要がある。	● 本事業は、ハードウェアセキュリティ評価体制の整備に関して、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、その成果を統合ハードウェア評価プラットフォームとして統合し、評価環境の効率化を図るもの。 ● なお、事業化にあたっては、評価機関やICベンダ等を対象とした、統合ハードウェア評価プラットフォーム全体としての販売に加え、レーザー照射装置、電磁波照射装置といった、各要素技術ごとの装置単体での販売も計画している。

D

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

D−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

D−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。

D−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。

D−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。

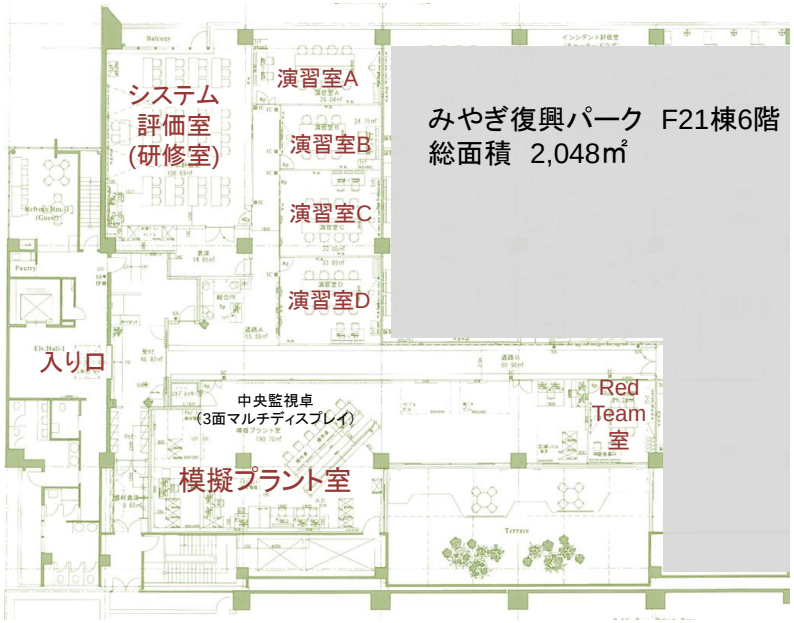
①化学プラント

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

D−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：

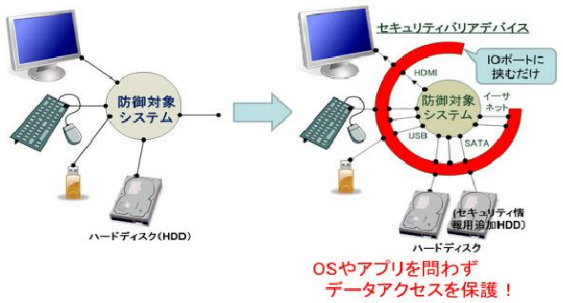
- ホワイトリスト型対策技術の開発
- 制御システム機器のセキュリティの評価・認証

【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。



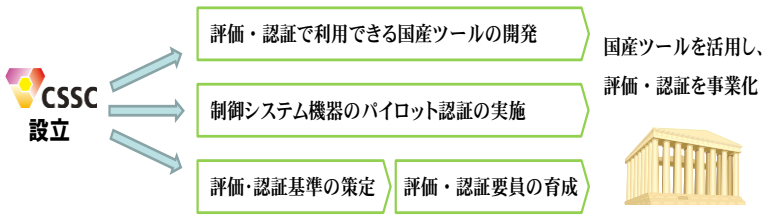
【制御システム機器のセキュリティの評価・認証】

✓ 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。

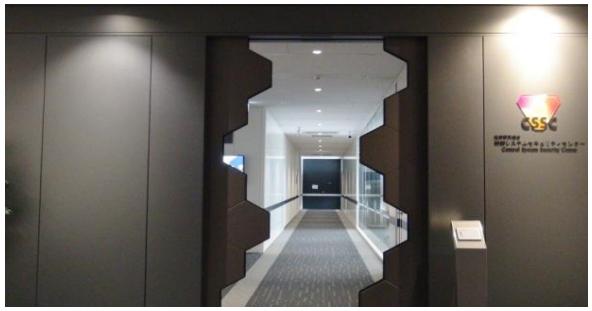
✓ 認定機関(JAB)は、米国ANSIと国際交互承認を締結済み。



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

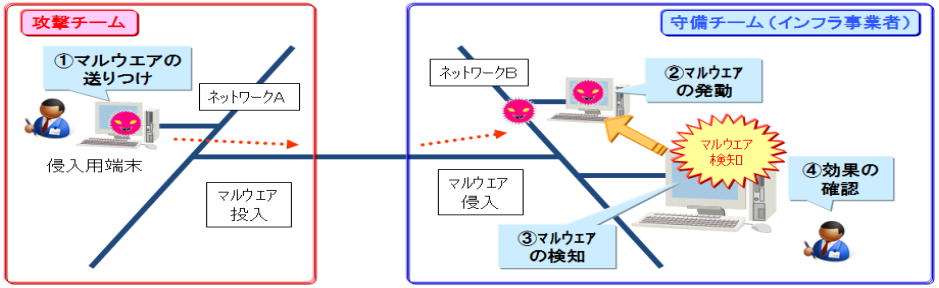


波及効果②：サイバーセキュリティ演習による普及啓発・人材育成

○ 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。

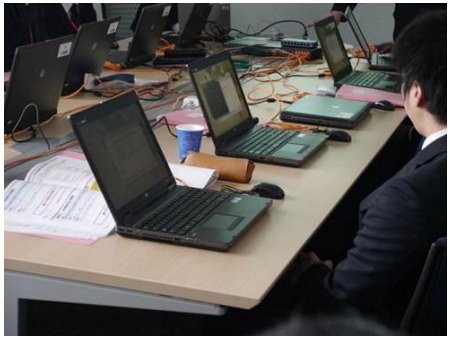
電力	実際に発生しているセキュリティインシデントを模擬体験。電力事業者とベンダが参加して、3/6-7に実施。
ガス	インシデント対応演習と最新対策技術の体験。参加者多数のため2回に分割実施。ガス事業者とベンダが参加して、1/21-22（1回目）、2/24-25(2回目)に実施。
ビル	攻撃・守備型の実践的演習と最新対策技術の体験。ビル事業者と計装事業者が参加して、1/29に実施。
化学	インシデント体験が主。3/4に実施。



サイバーセキュリティ演習の概要

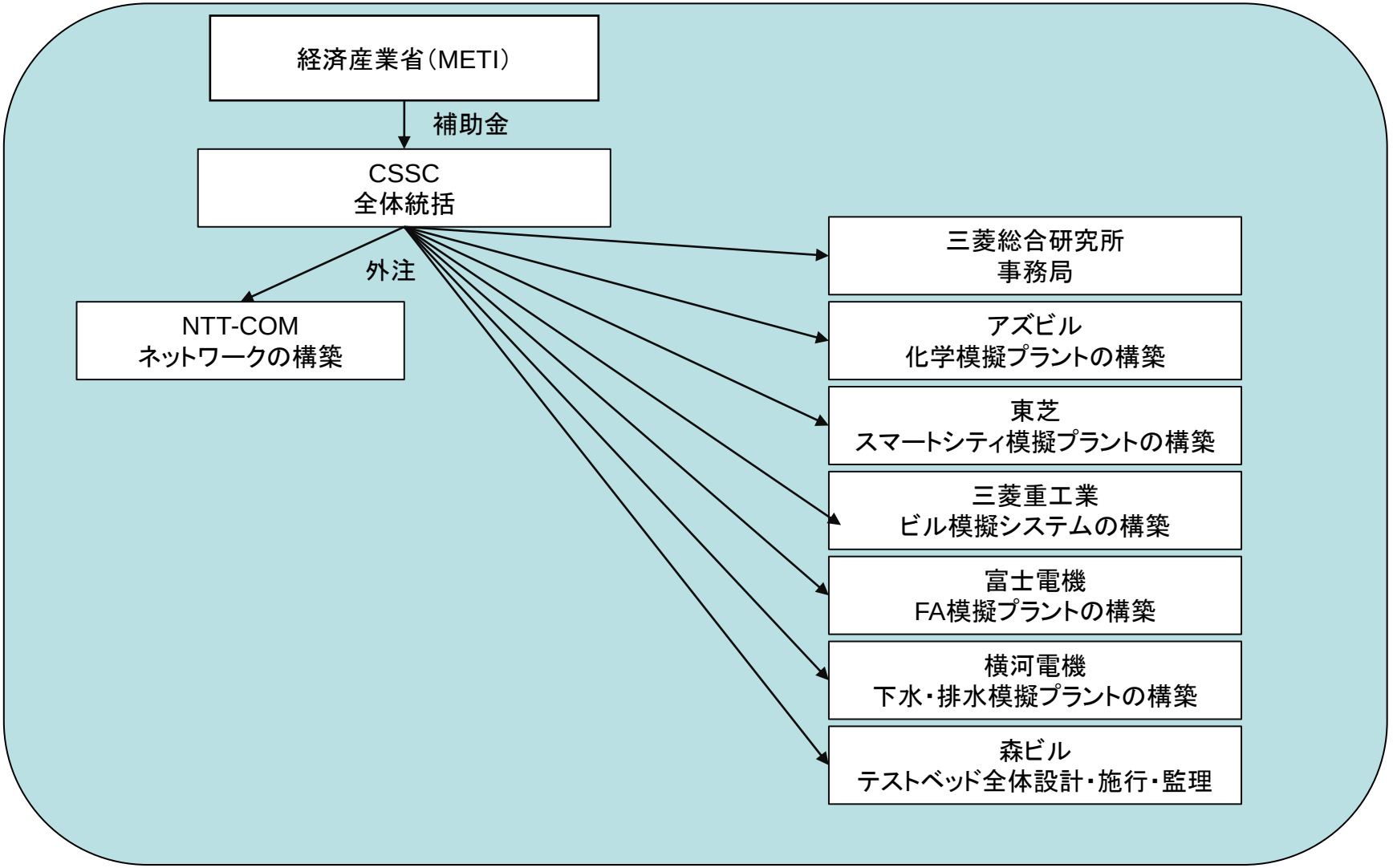
机上演習

機能演習（実機演習）



機能演習（対策技術の演習）

D−6. 研究開発体制、マネジメント体制



D−6. 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

D−7. 評価

D−7−1. 評価検討会

評価検討会名称		情報セキュリティ関連分野に係る技術に関する施策・事業評価検討会
評価検討会委員	座長	徳田　英幸 慶應義塾大学大学院 政策・メディア研究科委員長 教授
	委員	後藤　厚宏 情報セキュリティ大学院大学 情報セキュリティ研究科　教授 関口　和一 株式会社日本経済新聞社　論説委員 兼 編集委員 田辺　孝二 東京工業大学大学院 イノベーションマネジメント研究科　教授 西村　敏信 公益財団法人金融情報システムセンター 監査安全部長

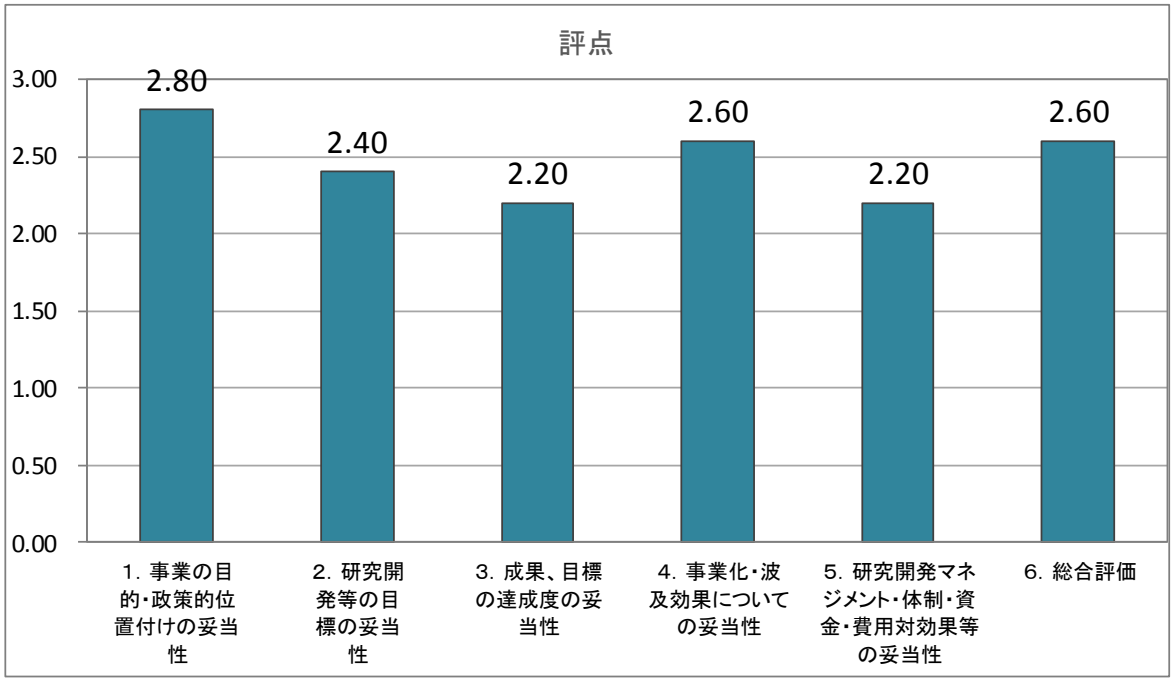
D-7-2. 総合評価（コメント）

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

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

D-7-3. 評点結果

- 「経済産業省技術評価指針」に基づき、プロジェクト事後評価において、評点法による 評価を実施した。
- 我が国初の制御システムセキュリティの拠点を設置した点と、高い波及効果が期待できる点において、高い評価を得ている。



【評価項目の判定基準】
評価項目1.～5.
3点：非常に重要又は非常によい
2点：重要又はよい
1点：概ね妥当
0点：妥当でない

6. 総合評価
（中間評価の場合）
3点：事業は優れており、より積極的に推進すべきである。
2点：事業は良好であり、継続すべきである。
1点：事業は継続して良いが、大幅に見直す必要がある。
0点：事業を中止することが望ましい。

（事後評価の場合）
3点：実施された事業は、優れていた。
2点：実施された事業は、良かった。
1点：実施された事業は、成果等が今一歩のところがあった。
0点：実施された事業は、成果等が極めて不十分であった。

D-8. 提言及び提言に対する対処方針

今後の研究開発の方向等に関する提言	提言に対する対処方針
● 中長期的な視点に立ち、IT技術の進化に先回りできるような情報セキュリティ技術の研究開発を目指すべきである。多様な要素技術を基盤として統合する際の技術課題については国の施策として取り組む必要がある。	● 本事業は、情報セキュリティ政策会議において決定された「情報セキュリティ2012」に位置づけられた事業であり、国が行うべき施策として重点的に実施してきた。 ● 本事業の終了後も引き続き、重要インフラ等に利用される制御システムに関する研究開発の推進と併せて、本事業で得た成果を活用したサイバー演習、制御システムセキュリティに係る国際標準化の推進とそれをベースとした国際的な相互認証制度を本年4月からスタートさせるなど、継続的な取組を行っている。