第１１回評価ワーキンググループ
資料４（概要版）

情報セキュリティ分野に係る
技術に関する施策・事業評価報告書
（案）

平成２６年４月

産業構造審議会産業技術環境分科会

研究開発・評価小委員会評価ワーキンググループ

技術に関する施策・事業評価報告書概要

技術に関する施策

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

技術に関する施策の目的・概要

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

これを実現するため、以下を実施。

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

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

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

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

事業一覧

① コンピュータセキュリティ早期警戒体制の整備事業

② 企業・個人の情報セキュリティ対策促進事業

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

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

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

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

の４つである。

（企業・個人の情報セキュリティ対策促進事業）

Ａ．新世代情報セキュリティ研究開発事業

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

Ｃ．暗号アルゴリズムの物理的安全性評価に必要な標準評価環境の開発

（ＩＴ融合による新産業創出のための研究開発事業）

Ｄ．サイバーセキュリティテストベッドの構築事業

技術に関する施策評価の概要

１．施策の目的・政策的位置付けの妥当性

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

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

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

２．施策の構造及び目的実現の見通しの妥当性

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

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

は、それぞれの事業ごとに PDCA サイクルを回し、全プロジェクトの中で適切なポートフォリオが描けているか、さらに注視する必要がある。

３．総合評価

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

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

今後の研究開発の方向等に関する提言

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

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

技術に関する事業

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

事業の目的・概要

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

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

なお、技術に関する事業として、評価対象となるプロジェクトは以下の通り。

① 情報家電、スマートグリッド等におけるセキュリティ対策技術の研究開発

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

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

② アクセス制御技術の研究開発

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

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

③ クラウドコンピューティングに関するセキュリティ対策技術の研究開発

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

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

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

予算額等（委託）　（単位：千円）

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

※予算額、総予算額、総執行額の欄は、直近 3 年間の額である。

目標・指標及び成果・達成度

(1) 全体目標に対する成果・達成度

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

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

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

(2) 目標及び計画の変更の有無

なし

＜共通指標＞

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

総合評価概要

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

なお、今回はクラウド環境に関するセキュリティ技術開発案件が２つ打ち切りとなったことで、クラウド関連の技術開発がやや遅れる結果となっており、追加の技術開発の公募について検討すべきであった。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。

今後の研究開発の方向等に関する提言（各事業共通）

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

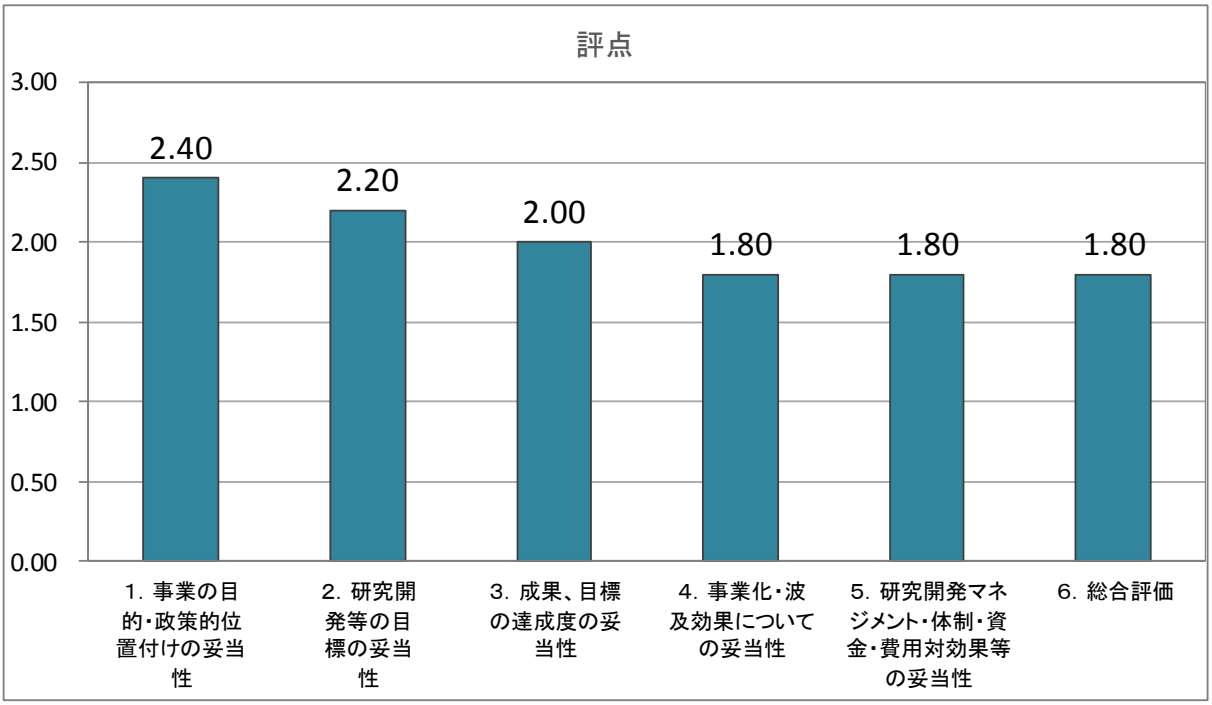
国際的な開発競争が激しくなってきている IoT (Internet of Things)技術、サイバーフィジカルシステム、連携された重要生活機器（車やスマホ）に対する新たな脅威に関して、根本的な問題解決を目指したセキュリティ技術開発や標準化に対する対応を考慮すべきである。

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

そのセキュリティにおいて技術的にも未解決課題が多く、重要な課題である。

評点結果

	評点	A 委員	B 委員	C 委員	D 委員	E 委員
1. 事業の目的・政策的位置付けの妥当性	2.40	2	2	3	2	3
2. 研究開発等の目標の妥当性	2.20	2	2	3	2	2
3. 成果、目標の達成度の妥当性	2.00	1	2	3	2	2
4. 事業化、波及効果についての妥当性	1.80	1	2	2	2	2
5. 研究開発マネジメント・体制・資金・費用対効果等の妥当性	1.80	1	2	2	2	2
6. 総合評価	1.80	1	2	2	2	2



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

事業の目的・概要

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

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

予算額等（委託）　（単位：千円）

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

目標・指標及び成果・達成度

(1) 全体目標に対する成果・達成度

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

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

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

(2) 目標及び計画の変更の有無

なし

＜共通指標＞

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

総合評価概要

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

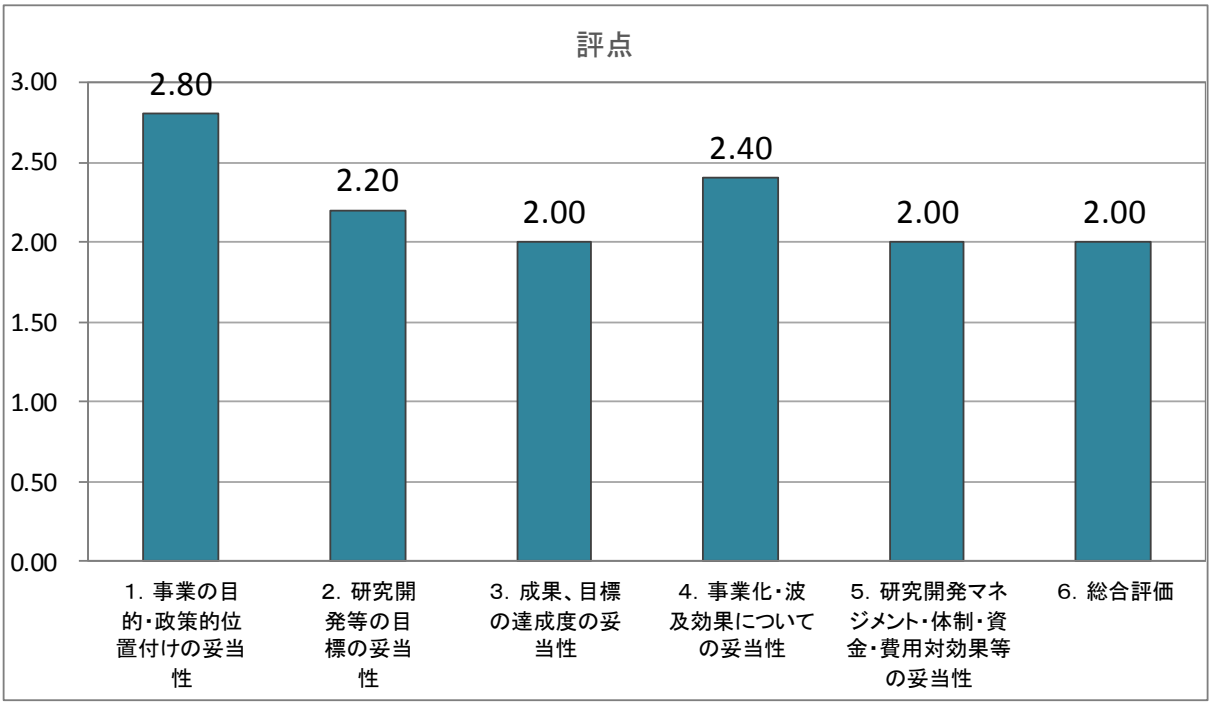
なお、本事業で構築した評価環境を持続的に運用するための人材育成方策として、育成した人材の定着と継続的なキャリアサイクルを回すための活動を明確にすることが重要である。

今後の研究開発の方向等に関する提言

（Ａ．新世代情報セキュリティ研究開発事業を参照）

評点結果

	評点	A 委員	B 委員	C 委員	D 委員	E 委員
1. 事業の目的・政策的位置付けの妥当性	2.80	2	3	3	3	3
2. 研究開発等の目標の妥当性	2.20	2	2	3	2	2
3. 成果、目標の達成度の妥当性	2.00	2	2	2	2	2
4. 事業化、波及効果についての妥当性	2.40	2	3	2	2	3
5. 研究開発マネジメント・体制・資金・費用対効果等の妥当性	2.00	2	2	2	2	2
6. 総合評価	2.00	2	2	2	2	2



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

事業の目的・概要

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

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

予算額等（委託）　（単位：千円）

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

※総執行額は、未確定である平成 25 年度の執行額を含まない。

目標・指標及び成果・達成度

(1) 全体目標に対する成果・達成度

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

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

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

(2) 目標及び計画の変更の有無

なし

＜共通指標＞

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

総合評価概要

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

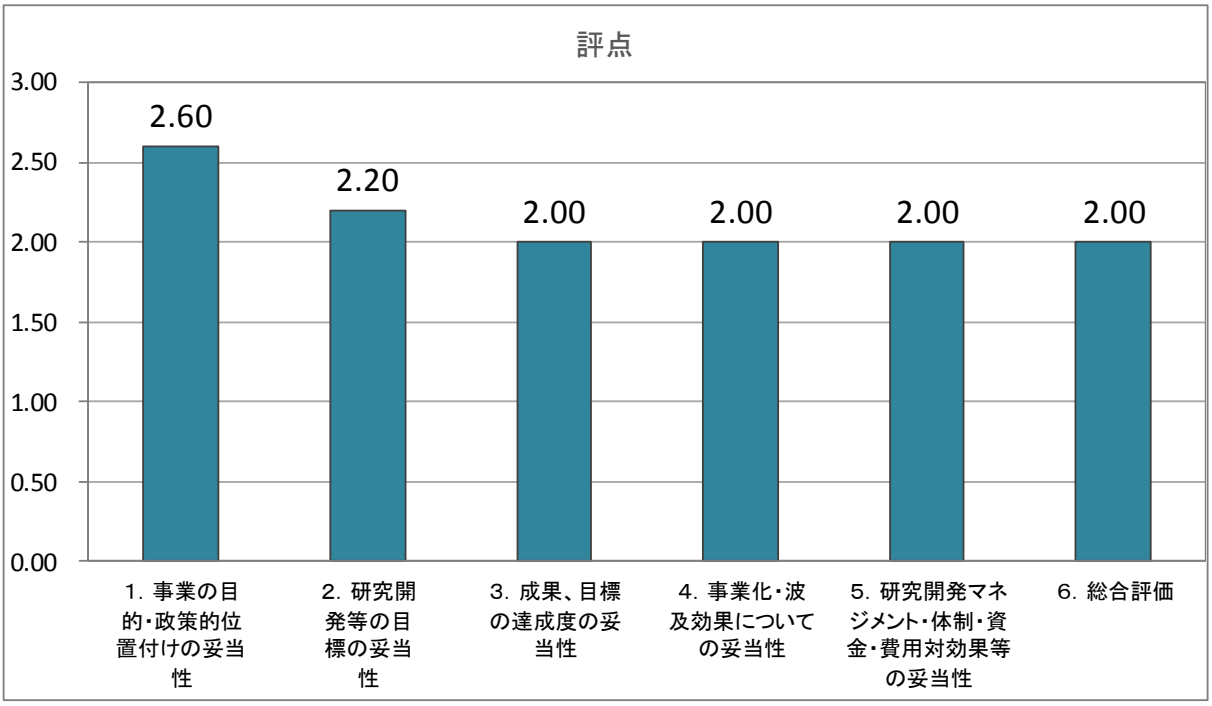
なお、攻撃手法や評価ノウハウの一部は、悪意ある利用につながらないように、適切に管理されるべきものである。事業全体としての管理や運用方針を明確にすべきである。

今後の研究開発の方向等に関する提言

（A．新世代情報セキュリティ研究開発事業を参照）

評点結果

	評点	A 委員	B 委員	C 委員	D 委員	E 委員
1. 事業の目的・政策的位置付けの妥当性	2.60	3	2	2	3	3
2. 研究開発等の目標の妥当性	2.20	3	2	2	2	2
3. 成果、目標の達成度の妥当性	2.00	2	2	2	2	2
4. 事業化、波及効果についての妥当性	2.00	2	2	2	2	2
5. 研究開発マネジメント・体制・資金・費用対効果等の妥当性	2.00	2	2	2	2	2
6. 総合評価	2.00	2	2	2	2	2



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

事業の目的・概要

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

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

予算額等（補助）　（単位：千円）

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

目標・指標及び成果・達成度

(1) 全体目標に対する成果・達成度

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

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

(2) 目標及び計画の変更の有無

なし

＜共通指標＞

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

総合評価概要

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

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

今後の研究開発の方向等に関する提言

（Ａ．新世代情報セキュリティ研究開発事業を参照）

評点結果

	評点	A 委員	B 委員	C 委員	D 委員	E 委員
1. 事業の目的・政策的位置付けの妥当性	2.80	3	3	2	3	3
2. 研究開発等の目標の妥当性	2.40	2	2	3	2	3
3. 成果、目標の達成度の妥当性	2.20	2	2	2	2	3
4. 事業化、波及効果についての妥当性	2.60	2	3	2	3	3
5. 研究開発マネジメント･体制･資金･費用対効果等の妥当性	2.20	2	2	2	2	3
6. 総合評価	2.60	2	3	2	3	3