第34回評価ワーキンググループ
資料３

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
（プロジェクト）
技術評価結果報告書（終了時評価）

（案）

平成２８年１２月

産業構造審議会産業技術環境分科会

研究開発・イノベーション小委員会評価ワーキンググループ

はじめに

研究開発の評価は、研究開発活動の効率化・活性化、優れた成果の獲得や社会・経済への還元等を図るとともに、国民に対して説明責任を果たすために、極めて重要な活動であり、このため、経済産業省では、「国の研究開発評価に関する大綱的指針」（平成２４年１２月６日、内閣総理大臣決定）等に沿った適切な評価を実施すべく「経済産業省技術評価指針」（平成２６年４月改正）を定め、これに基づいて研究開発の評価を実施している。

経済産業省において実施している「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」は、宮城県において、インフラを制御するIT システムのセキュリティの国際的な評価・認証機関を確立し、被災地域のIT・電機分野等の地元企業とともに、産学官連携のサイバーセキュリティ国際拠点の整備を図るため、平成２５年度から平成２７年度まで実施したものである。

今般、省外の有識者からなる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・促進事業終了時評価検討会（座長：越島一郎　名古屋工業大学大学院工学研究科ながれ領域教授）における検討の結果とりまとめられた、「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・促進事業技術評価結果報告書（終了時評価）」の原案について、産業構造審議会産業技術環境分科会研究開発・イノベーション小委員会評価ワーキンググループ（座長：小林　直人　早稲田大学研究戦略センター副所長・教授）において、審議し、了承された。

本書は、これらの評価結果を取りまとめたものである。

平成２８年１２月

産業構造審議会産業技術環境分科会

産業構造審議会産業技術環境分科会

研究開発・イノベーション小委員会　評価ワーキンググループ

委員名簿

座長	小林　直人	早稲田大学研究戦略センター副所長・教授
	大島　まり	東京大学大学院情報学環教授 東京大学生産技術研究所教授
	亀井　信一	株式会社三菱総合研究所政策・経済研究センター長
	齊藤　栄子	三菱ＵＦＪリサーチ＆コンサルティング株式会社 政策研究事業本部主任研究員
	高橋　真木子	金沢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
	津川　若子	東京農工大学大学院工学研究院准教授
	西尾　好司	株式会社富士通総研経済研究所主任研究員
	浜田　恵美子	元・名古屋工業大学大学院教授
	森　　俊介	東京理科大学理工学部経営工学科教授

（敬称略、座長除き五十音順）

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

終了時評価検討会

委員名簿

座長	越島　一郎	名古屋工業大学大学院 工学研究科ながれ領域　教授
	阿部　克之	電気事業連合会　情報通信部長
	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長　教授
	山下　善之	東京農工大学 工学部化学システム工学科　教授

（敬称略、座長除き五十音順）

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

技術評価に係る省内関係者

【終了時評価時】

（平成２８年度）
商務情報政策局　サイバーセキュリティ課長　　師田　晃彦（事業担当課長）

大臣官房参事官（イノベーション推進担当）
産業技術環境局　研究開発課　技術評価室長　　竹上　嗣郎

【事前評価時】（事業初年度予算要求時）

商務情報政策局　情報セキュリティ政策室長　　上村　昌博（事業担当課長）

産業技術環境局　産業技術政策課　技術評価室長　　岡本　繁樹

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

中間（終了時）評価の審議経過

【終了時評価】

◆産業構造審議会産業技術環境分科会研究開発・イノベーション小委員会評価ワーキンググループ（平成２８年１２月２１日）

・技術評価結果報告書（終了時評価）について

◆「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」評価検討会

第１回評価検討会（平成２８年１１月１５日）

・事業の概要について

・評価の進め方について

第２回評価検討会（平成２８年１１月２９日）

・技術評価結果報告書（終了時評価）について

【事前評価】

◆産業構造審議会産業技術分科会評価小委員会（平成２４年５月２９日）

・技術評価書（事前評価）について

目　　次

目次

ページ

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
技術評価結果報告書（終了時評価）

プロジェクト名	東北復興再生に資する重要インフラＩＴ安全性検証・普及啓発拠点整備・促進事業
行政事業レビューとの関係	平成２８年度　０１６２
上位施策名	○「サイバーセキュリティ戦略」（平成 25 年 6 月情報セキュリティ政策会議決定） ○「サイバーセキュリティ 2014」（平成 26 年 7 月情報セキュリティ政策会議決定） ○「重要インフラにおける情報セキュリティ対策に係る行動計画」（平成 26 年 5 月情報セキュリティ政策会議決定） ○「日本再興戦略」（平成 25 年 6 月閣議決定）
担当課室	統括官付参事官（予算・会計担当）

プロジェクトの目的・概要

本事業は、宮城県において、インフラを制御する IT システムのセキュリティの国際的な評価・認証機関を 3 年以内に確立させ、被災地域の IT・電機分野等の地元企業とともに、産学官連携のサイバーセキュリティ国際拠点の整備を図ることを目的とする。

宮城県多賀城市に構築した国内唯一の「制御システム検証施設」を活用して、インフラを制御する IT システムの安全性検証・普及啓発のための、人材育成プログラム、評価・認証手法、高セキュア化技術、インシデント分析技術の開発等を行う。

本事業において、制御システムのセキュリティに関する国際的な評価・認証機関を確立することは、「サイバーセキュリティ戦略」（平成 25 年 6 月　情報セキュリティ政策会議決定、平成 27 年 9 月閣議決定）で示される重要インフラを守るための取組としての「スマートメーター等の制御系について、国際標準に即した第三者認証制度の活用等を推進」や、「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成 26 年 5 月、27 年 5 月改訂）」で示される「防衛基盤の強化」としての「内閣官房は（中略）制御系機器・システムの第三者認証制度の拡充を支援」等の方針に則ったものである。

予算額等（委託 or 補助（補助率：　　））　（単位：百万円）

開始年度	終了年度	中間評価時期	終了時評価時期	事業実施主体
平成２５年度	平成２７年度	―	平成２７年度	技術研究組合制御システムセキュリティセンター
H25FY 執行額	H26FY 執行額	H27FY 執行額	総執行額	総予算額
535	481	375	1391	1450

Ⅰ．研究開発課題（プロジェクト）概要

１．事業アウトカム

本事業では、国際標準に則った審査と共に、攻撃者視点の検証技術を人材育成コンテンツや高セキュア化技術の開発に展開し、セキュリティの普及啓発や技術利用促進に寄与した。事業アウトカム指標として、以下を設定した。

(1) 制御システムセキュリティ人材の育成（制御システム検証施設訪問者数）

検証施設を普及啓発・人材育成としても活用することで、ユーザ企業の意識喚起による対策が進展すると共に、国内外の受講者が集積することで産学官連携のサイバーセキュリティ国際拠点の地位を確立可能である。

(2) 我が国における制御システムのセキュリティに関する評価・認証機関の確立（評価・認証の審査件数）

国際基準に則った評価・認証機関を東北に設置し、受審企業が集積することで、知見共有や地元企業への技術移転が可能である。

(3) 制御システムの高セキュア化（制御システムの高セキュア化技術の利用件数）

攻撃者視点の検証技術を、防御側の視点で制御システムの高セキュア化技術開発に活かし、組合員で迅速に共有することで、オールジャパンの防御力を高めるために有効である。

なお、(1)制御システムセキュリティ人材の育成については、平成 26 年度～27 年度は年間 1,700～1,800 人の受講者が検証施設に来訪し、平成 27 年度の目標である年間 1,800 人をほぼ達成した。

(2) 我が国における制御システムのセキュリティに関する評価・認証機関の確立については、平成 25 年度は計画通りの 3 社が受審したものの、平成 27 年度は計画の 50%である 2 件の審査に留まった。EDSA 認証（Embedded Device Security Assurance：制御システムコンポーネントのセキュリティ認証）取得予定事業者が、製品開発の遅れにより受審できなかったこと、さらに国際市場動向を踏まえ SSA 認証（System Security Assurance： 制御システム（商用製品）のセキュリティ認証）の開始を見合わせたことが原因である。

(3)制御システムの高セキュア化については、研究開始段階から技術の活用が進展し、平成 27 年度は 21 件の利用申請があり、目標である 20 件の技術利用を達成した。

事業アウトカム指標		
制御システム検証施設訪問者数。（東北を中心として国内外からも参加が見込まれる。）		
指標目標値 制御システムセキュリティ人材の育成のため、平成 27 年度の制御システム検証施設訪問者を 1,800 人とする。		
事業開始時（25 年度）	計画：1,000	実績：1,483（148.3%）

中間評価時（ー）	計画：ー	実績：ー
終了時評価時（27 年度）	計画：1,800	実績：1,730（96.1%）
目標最終年度（27 年度）	計画：1,800	

事業アウトカム指標		
評価・認証の審査件数		
指標目標値 我が国における制御システムのセキュリティに関する評価・認証機関を確立し、平成 27 年度の評価・認証の審査件数を 4 件とする。		
事業開始時（25 年度）	計画：3	実績：3（100%）
中間評価時（ー）	計画：ー	実績：ー
終了時評価時（27 年度）	計画：4	実績：2（50%）
目標最終年度（27 年度）	計画：4	

事業アウトカム指標		
制御システムの高セキュア化技術の利用件数		
指標目標値 制御システムの高セキュア化技術を開発し、平成 27 年度の技術の利用件数を 20 件とする。		
事業開始時（25 年度）	計画：10	実績：9（90%）
中間評価時（ー）	計画：ー	実績：ー
終了時評価時（27 年度）	計画：20	実績：21（105%）
目標最終年度（27 年度）	計画：20	

２．研究開発内容及び事業アウトプット

（１）研究開発内容

本事業では、技術研究組合制御システムセキュリティセンター（Control System Security Center：CSSC）において、重要インフラサービスを支える制御システムのセキュリティを高めるための、人材育成プログラム、評価・認証手法、高セキュア化技術の開発等を行った。

これらの研究で得られたシステムやコンポーネントの検証技術により、プラント等を活用する重要インフラ等のセキュリティ強化を図るとともに、海外で活用されつつある国際標準に則った評価・認証や国際標準策定に対する貢献を通じて、国内プラントベンダのインフラ輸出力の強化を図るものである。

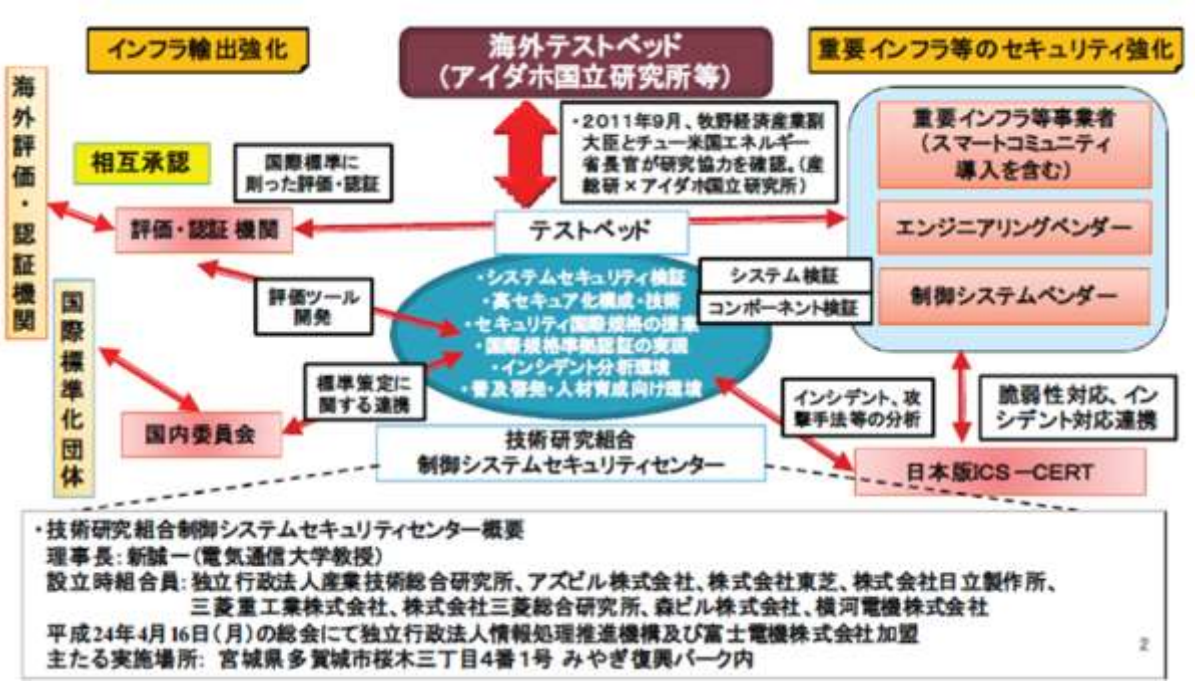


図 1 技術研究組合制御システムセキュリティセンターの機能

1） 評価・認証

制御システムセキュリティに関する国際標準である IEC 62443 をベースに、それに準拠する EDSA（Embedded Device Security Assurance：制御システムコンポーネントのセキュリティ）認証の実証実験を通じた認証制度の設立、及び制御システムセキュリティ評価・認証のための環境整備を実施した。

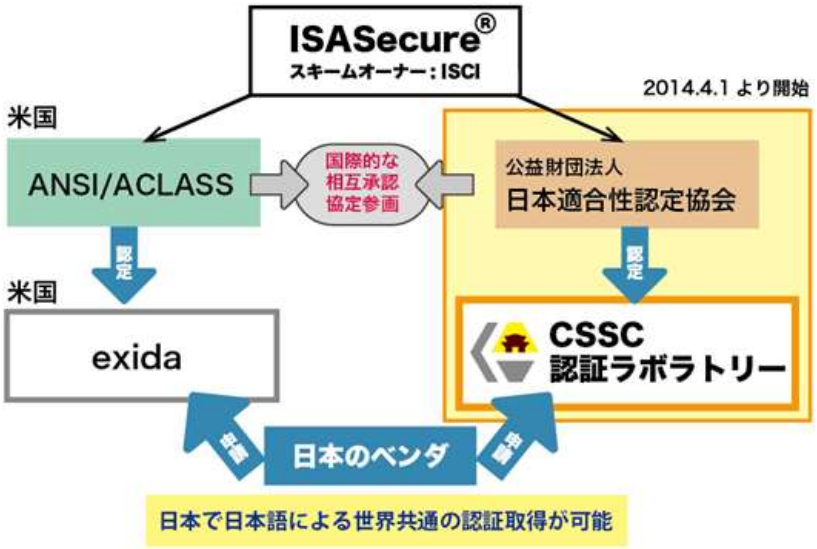


図 2 制御システムセキュリティ認証の日米相互承認

注）
・ISCI ： ISA Security Compliance Institute
国際計測制御学会 ISA(International Society of Automation)における認証推進組織
ISA Secure のスキームオーナ
・ISA Secure ： 制御システムセキュリティ認証機関(EDSA 認証、SSA 認証、SDLA 認証を推進)
・EDSA 認証:制御機器セキュリティ認証
・SSA 認証:制御システム(商用製品)セキュリティ認証
・SDLA 認証:制御機器開発ライフサイクルプロセス認証

表 1 CSSC 認証ラボラトリーの活動

項目	平成 25 年度	平成 26 年度	平成 27 年度
認証機関 ステータス	PCLS	Certification Body	Certification Body
試験所認定	ISO/IEC 17025 認定	ISO/IEC 17025 認定	ISO/IEC 17025 認定
製品認証 機関認定	審査途中(Step1 まで)	ISO/IEC Gide65 認定	ISO/IEC 17065 認定
認証業務	CRT テストおよび FSA/SDSA 評価まで実施(パイロットプロジェクト)	EDSA 認証 3 件	EDSA 認証 1 件(他に 1 社 1 製品仕掛中)
委員会	公平性委員会 1 回 (キックオフ) 認証判定委員会 1 回 (キックオフ)	公平性委員会 1 回 認証判定委員会 2 回	公平性委員会 1 回 認証判定委員会 1 回
認証書発行	なし	国内 3 社 3 製品	国内 1 社 1 製品(他に 1 社 1 製品仕掛中)
人材	CISSP 保持者 2 名	CISSP 保持者 3 名	CISSP 保持者 2 名 GICSP 保持者 1 名
試験環境	Achilles	Achilles Defensics	Achilles Defensics NESSUS
認証 プログラム	EDSA 2010.1	EDSA 2010.1	EDSA 2010.1
講演会/研修	講演会 1 回	なし	講演会 2 回 研修：1 回

注）
・PCLS:Provisional Chartered Laboratory Status(認証可能な状態)
・CRT ： Communication Robustness Test （通信ロバストネス試験）
・FSA ： Functional Security Assessment（機能セキュリティ評価）
・SDSA ： Software Development Security Assessment
（ソフトウェア開発セキュリティ評価）
・CISSP ： Certified Information Systems Security Professional
・GICSP ： Global Industrial Cyber Security Professional
・Achilles、Defensics、NESSUS ： 商用試験ツールの名称

2) 高セキュア化技術

制御システムのセキュリティ確保のために、「機器」「システムやプラント」を対象としたセキュリティ技術を開発し、実システムと同様の制御機器を使ったテストベッドを利用して、開発技術の有効性を検証した

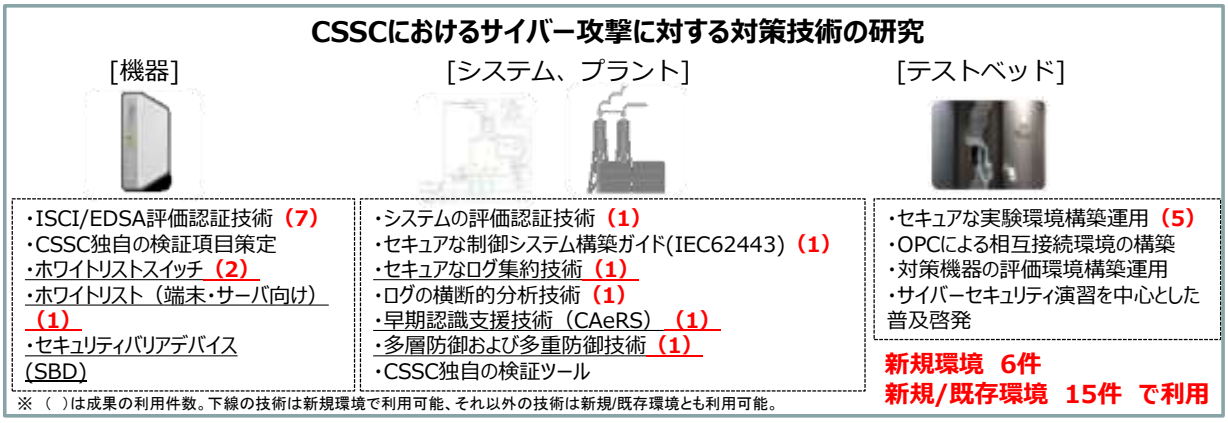


図 3 CSSC におけるサイバー攻撃に対する対策技術の研究

制御システムのホワイトリストを効率的に運用する学習機能に関する研究や、制御システムのサイバー攻撃を早期に発見するための技術等、制御システムを高セキュア化するための技術を開発した。なお、本事業によって研究された制御システムのホワイトリストが実用化されている。

ホワイトリスト機能とは、ネットワークスイッチに正常な通信フローを登録し、それ以外の通信はすべてシャットアウトするが、大規模・複雑なネットワークでは設定等の運用負荷が大きい。そこで、通信フローを一定期間監視・学習することで、通信の許可リストを自動で生成・登録する技術を開発・検証した。本技術では、ある環境において手動リスト生成に 85 分要していたものが、自動設定では 30 分でリスト生成可能となり、65%の作業時間を削減できた。

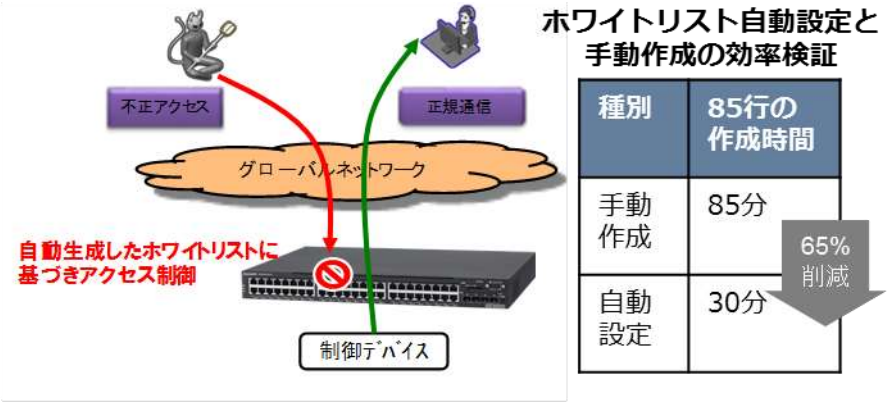


図 4 ホワイトリストの学習機能に関する研究

また、従来の制御システムでは、異常発生時、ユーザ自身あるいはベンダへ依頼しての原因究明を行っているが、機器故障や操作ミス等、全ての異常の可能性を否定してからサイバー攻撃の可能性を考えると、サイバー攻撃と認識できるまでの時間が長期化して対処が遅れたり、そもそもサイバー攻撃と認識ができなくなる恐れがある。そこで、異常発生時に現場情報等、様々な情報をインプットしサイバー攻撃の可能性を系統的に絞り込むことで、短時間でサイバー攻撃と認識可能とし、早期の対処を実現する技術を開発した。本技術は、化学（水位一定制御）のプラントにプロトタイプを実装し、特定のサイバー攻撃については原因弁別を可能とした。

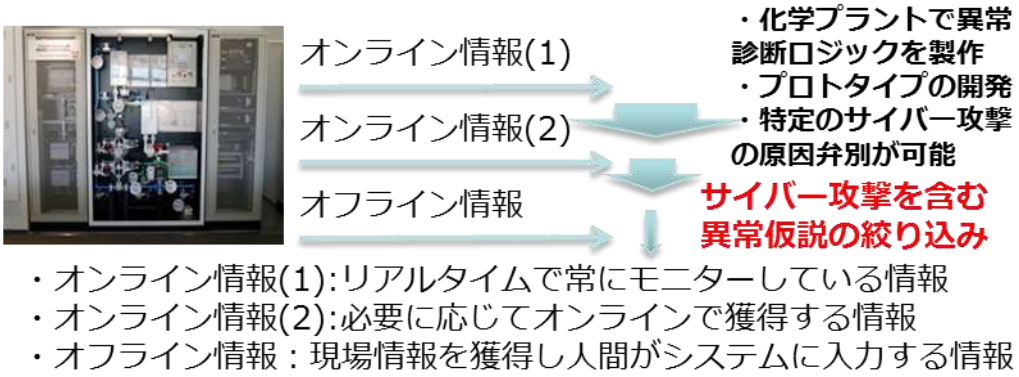


図 5 サイバー攻撃の早期認識支援技術

3) 普及啓発・人材育成

研究開発成果を活用し、普及啓発・人材育成のためのコンテンツを開発した。3 年間で合計 4,940 名が来所、964 回のデモを実施した。

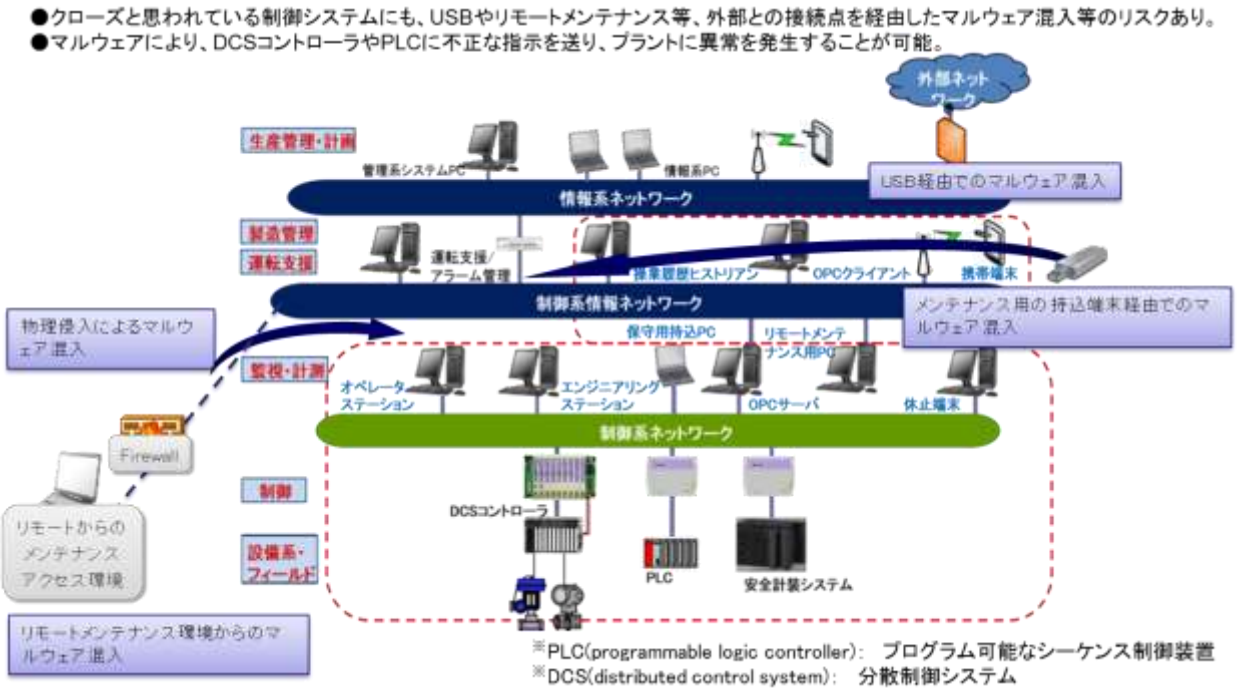


図 6 普及啓発のための演習シナリオの一例

（２）事業アウトプット

本事業では、IEC62443 に準拠したセキュリティ評価・認証機関を確立することを目標とした。事業アウトプット指標として、以下を設定した。

制御システム機器の評価・認証機関の確立（認証機関の確立件数）

国際基準に則った評価・認証機関を東北に設置することで、国際的なブランド力の向上が期待できる。

なお、IEC62443 に準拠した制御機器のセキュリティ認証（EDSA 認証）を 2014 年 4 月 1 日より開始。国内 3 社 4 製品が認証取得し、国内の制御セキュリティ及び輸出競争力の強化に貢献するとともに、米国との相互承認体制により国際認知度も向上した。

事業アウトプット指標		
制御システム機器の評価・認証機関の確立 ※平成 26 年 4 月 1 日から EDSA 認証（機器の認証）を開始		
指標目標値（計画及び実績）		
事業開始時（25 年度）	計画：ー	実績：ー
中間評価時（ー）	計画：ー	実績：ー
終了時評価時（27 年度）	計画：1	実績：1
目標最終年度（27 年度）	計画：1	

＜共通指標実績＞

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	国際標準への寄与※	プロトタイプの作成
32	32	1	0	0	306	30

※IEC62443 に準拠した EDSA 認証規格に対する意見提出数

受賞： 1 件（アジア・パシフィック ISLA 受賞）

メディアによる報道： 49

講演： 70

注）

・ISLA ： CISSP 認定資格の試験運営、認定を行う（ISC）2 が定める
情報セキュリティ・リーダーシップ・アチーブメント

表 2 日本におけるEDSA認証取得製品

サプライヤー	タイプ	モデル	バージョン	レベル
アズビル株式会社	DCS コントローラ	Harmonas/Industrial-DEO/Harmonas-DEO システム プロセス・コントローラ DOPCⅣ (冗長タイプ)	R4.1	EDSA2010.1 Level1
株式会社日立製作所	DCS コントローラ	HISEC 04/R900E	01-08-A1	EDSA2010.1 Level1
横河電機株式会社	DCS コントローラ	CENTUM VP	R5.03.00	EDSA2010.1 Level1
横河電機株式会社	DCS コントローラ	CENTUM VP	R6.01.00	EDSA2010.1 Level1

３．当省(国)が実施することの必要性

■科学技術的価値の観点からみた卓越性、先導性

制御システムに関するセキュリティは、スマートコミュニティが進展することで増していくサイバー攻撃への脅威へ対応するための基盤となる技術である。また、我が国のＩＴ基盤を強固とするためには、高まる脅威に対応した制御システムの高セキュア化に向けた取組が必要となる。

しかしながら、制御システムのセキュリティに関する技術や標準、評価・認証手法については、未だ世界的に確立されたものは存在しない。このような中で、既に制御システムのセキュリティについては、米国アイダホ国立研究所が先行して研究を実施している。我が国においては、米国との研究協力について政府レベルで合意しており、国が主導して米国と研究を実施していくことが、将来的な国際標準化や評価・認証機関同士の国際相互承認を目指す上で近道である。

■未来開拓研究、民間とのデマケの整理等

本事業は、我が国において強みを持つ制御システムについて、輸出の障害となりつつある世界的なセキュリティ意識の高まりに対応するもの、本事業の研究内容については我が国で未だ実施されていない、研究にあたってはオールジャパンの体制に加えて米国の協力も得ること等から、未来開拓研究へ位置付けられる。また、民間企業において本研究開発と同様の研究開発は行われていない。

４．事業アウトカム達成に至るまでのロードマップ

本事業では、模擬プラントや検証ツールを用いた制御システムの現場を模した実証環境を用いて、国内の主要なプラントベンダ・システムインテグレータ・セキュリティベンダ等の組合員・有識者が知見の結集し、攻撃者目線での検証シナリオや防御技術の研究開発を行った。

事業 3 年間の成果として、「制御システムセキュリティ人材育成・普及啓発」「制御システムセキュリティ評価・認証機関の確立」「制御システムの高セキュア化技術開発」において目標を達成した。

今後も、IoT 化等、技術の発展を踏まえた国の次期研究開発に沿った研究開発を進めるとともに、重要インフラ事業者のセキュリティ確保に向け、重要インフラ分野への対策実装や人材育成に資する研究開発を進める。また、多賀城市に確立した評価・認証機関を活用することで、人材育成拠点としての活性化や地元企業への技術移転等、東北地域における制御セキュリティの産業化を目指す。

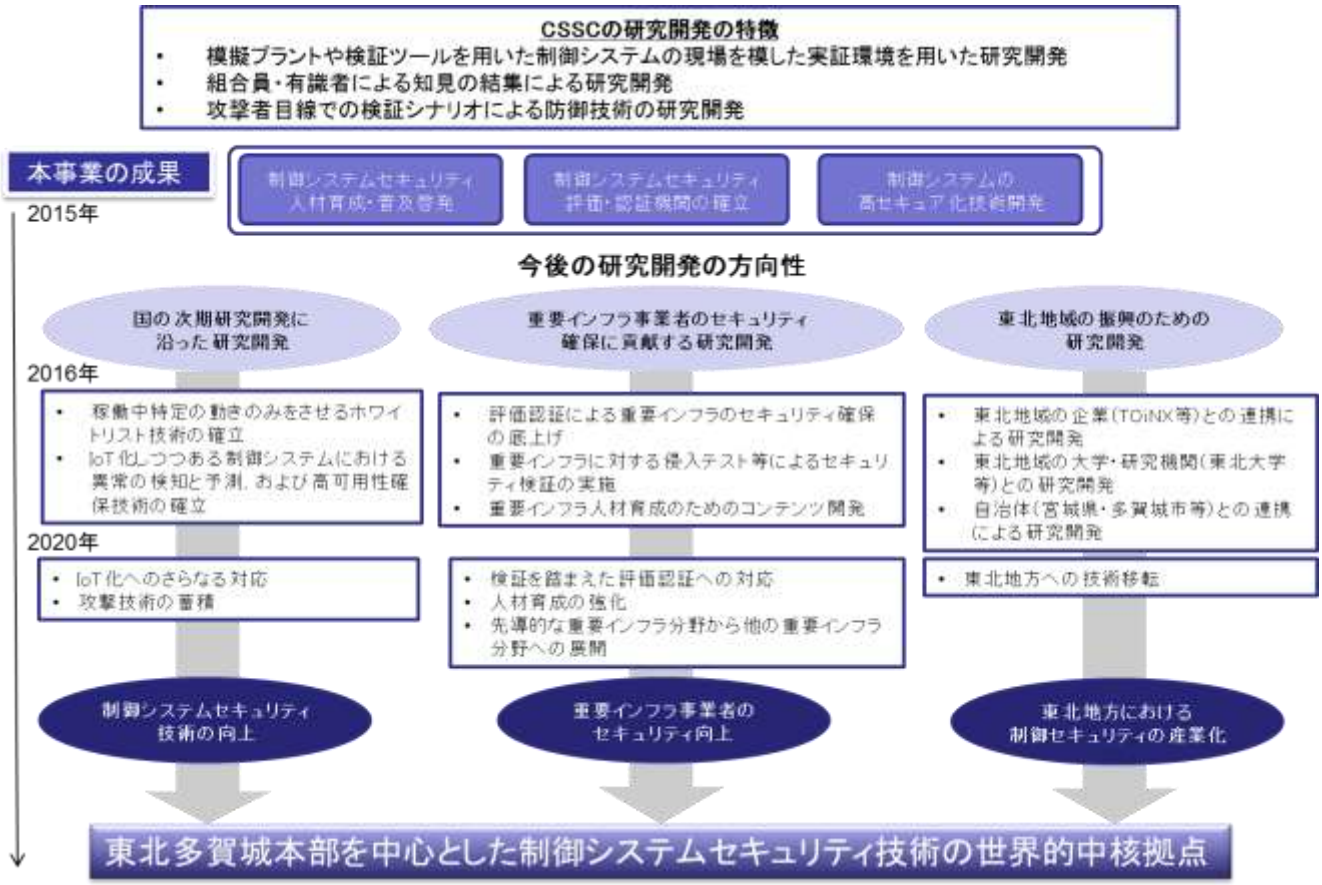


図 7 事業アウトカム達成のためのロードマップ

５．研究開発の実施・マネジメント体制等

本事業の委託先である CSSC は、組合員による「研究開発・テストベッド委員会」「評価認証・標準化委員会」「インシデント・ハンドリング委員会」「普及啓発・人材育成委員会」の 4 つの委員会を軸に研究開発を推進しており、各委員会で議論された内容は、全組合員が参加する「運営委員会」において審議されることで、組合員の意向を踏まえた研究テーマや実施内容が決定されている。研究は、CSSC 研究員他、民間企業への委託によって遂行された。顧問である学識経験者から適宜研究内容に関する助言を得る形で研究内容の向上を図っている。

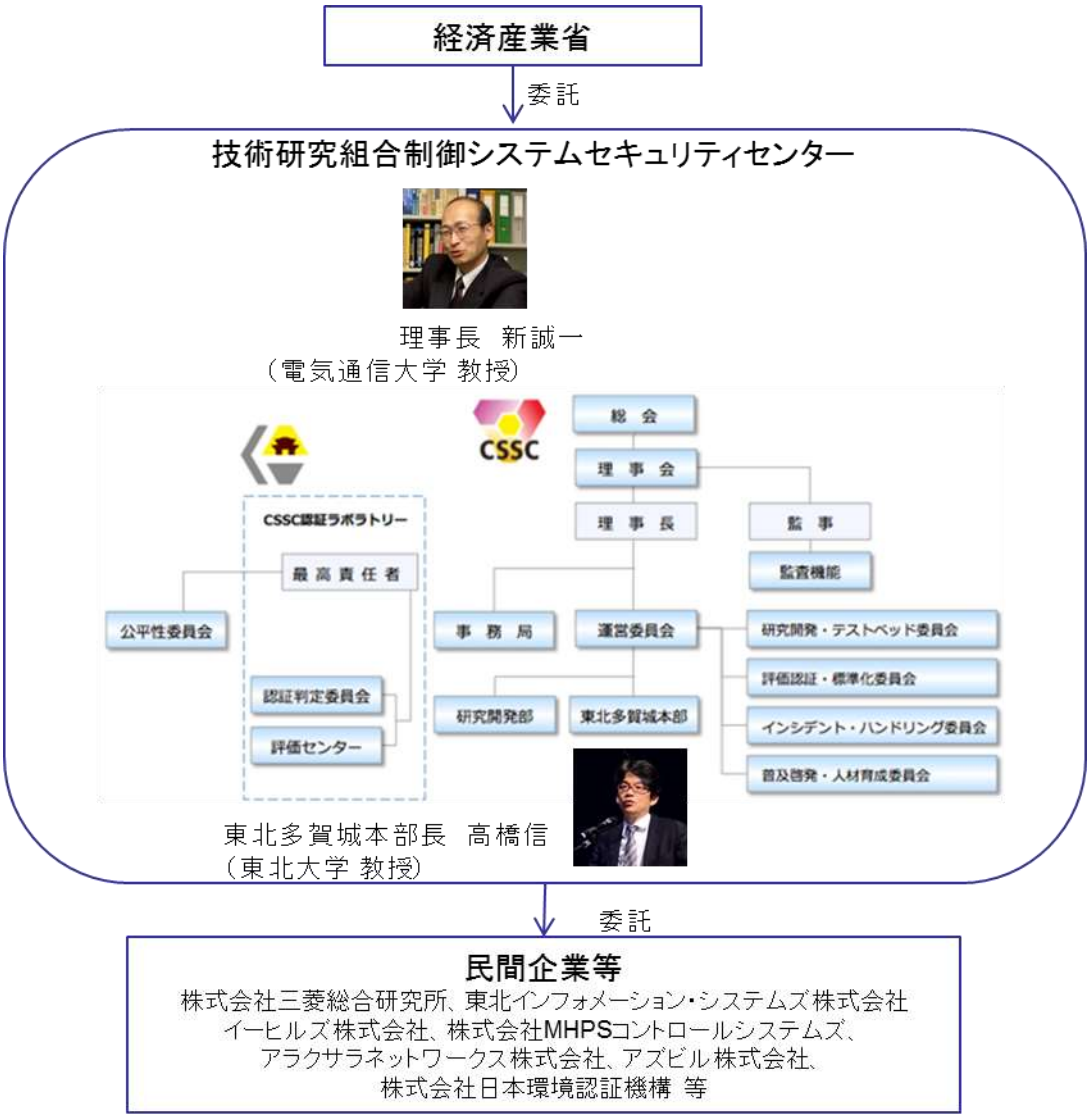


図 8　技術研究組合制御システムセキュリティセンターにおける研究開発体制

表 3　技術研究組合制御システムセキュリティセンター　組合員等一覧

組合員 (50 音順)	株式会社 IHI、アズビル株式会社*、アラクサラネットワークス株式会社、エヌ・アール・アイ・セキュアテクノロジーズ株式会社、エヌ・ティ・ティ・コミュニケーションズ株式会社、オムロン株式会社、国立研究開発法人産業技術総合研究所*、シスコシステムズ合同会社、独立行政法人情報処理推進機構、綜合警備保障株式会社、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、国立大学法人東北大学、トレンドマイクロ株式会社、株式会社日本環境認証機構、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*、株式会社日立システムズパワーサービス、富士通株式会社、富士電機株式会社、パナソニック株式会社、マカフィー株式会社、マクニカ・富士エレホールディングス株式会社、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、株式会社明電舎、森ビル株式会社*、横河電機株式会社*、株式会社ラック（**全 32 組織**）

特別賛助会員（岩手県、宮城県、福島県に本社を置く中小企業・自治体。無料）	宮城県、多賀城市、株式会社アイシーエス、株式会社イーアールアイ、株式会社サイバーソリューションズ、株式会社システムロード、株式会社高山、通研電気工業株式会社、テクノ・マインド株式会社、東杜シーテック株式会社、株式会社戸崎通信工業、トライポッドワークス株式会社、株式会社東日本計算センター、株式会社福島情報処理センター（**全 14 組織**）
賛助会員（成果報告会参加、会員向けウェブサイト閲覧可能な会員。有料）	株式会社アルチザネットワークス、イクシアコミュニケーションズ株式会社、株式会社インタフェース、株式会社インフォセック、株式会社 OTSL、KPMG コンサルティング株式会社、株式会社原子力エンジニアリング、日本原子力防護システム株式会社、日本ダイレックス株式会社、千代田計装株式会社、株式会社 TTK、株式会社東陽テクニカ、一般社団法人 日本ガス協会、フォーティネットジャパン株式会社、株式会社ロックインターナショナル、三菱スペース・ソフトウエア株式会社（**全 16 組織**）
連携団体（組合と連携し、研究開発を実施する団体）	一般社団法人 JPCERT コーディネーションセンター、一般社団法人 日本電機工業会、公益社団法人 計測自動制御学会、一般社団法人 電子情報技術産業協会、一般社団法人 日本計装工業会、一般社団法人 日本電気計測器工業会、一般財団法人 製造科学技術センター、電気事業連合会、一般社団法人 日本化学工業協会、一般社団法人 東北経済連合会、一般社団法人 宮城県情報サービス産業協会、多賀城・七ヶ浜商工会、一般社団法人ビルディング・オートメーション協会（**全 13 組織**）

※ 本表は技術研究組合の組合員等を示したもので、本事業に関わる組織の記載ではない。

６．費用対効果

本事業においては、評価・認証の審査件数 1 件につき 1.8 億円の国費が投入され、審査を通じた製品そのものやプラントベンダの開発体制のセキュリティ向上に寄与している。

また、東北地方への普及啓発・産業化の推進や、認証取得によるインフラ輸出力の強化など、研究成果の活用を通じた社会効果が期待できる。

■ 活動指標及び活動実績（アウトプット）

本事業は、国費総額 14.5 億円に対し、制御機器セキュリティ認証審査件数 8 件であり、単位当たりでは、審査件数 1 件につき 1.8 億円であった。

審査受審企業は、日本の主要プラントベンダであり、認証取得のための審査を通じて、単に製品のセキュリティを向上させ、認証を得るだけではなく、セキュアな製品開発プロセス・体制の構築、認証取得のためのセキュリティ評価技術に関わる知見の獲得ができたことで、他の製品開発におけるセキュリティ向上にも寄与している。

国内のセキュリティ認証機関は、企業間の機密情報の保護に関する体制整備や運用を実現するノウハウが重要であり、管理コストを踏まえると、国費の単位当たりの費用以上の効果があると言える。

表 4 認証審査件数の国費総額に対する単位当たりコスト

	25 年度	**26 年度**	**27 年度**
単位当たりコスト（百万円）	178	172	200
計算式（億円/件）	5.35/3	5.15/3	4/2

■ 東北地方の企業への普及啓発・産業化

CSSC の特別賛助会員（岩手県、宮城県、福島県に本社を置く中小企業、または同3県の自治体）に対して、研究開発に関する成果を無償で情報提供を行っている。また、公益財団法人みやぎ産業振興機構復興パークを通した見学受け入れ（平成 27 年度に 22 回）、東北大学・カタールサイエンスキャンパス（県内の小中高生を対象としたものづくりや科学実験に関するイベント）、多賀城高校への出張授業等、東北地域の関係組織や教育機関と連携した研究成果の普及啓発を図っている。

また、東北地方の企業において、平成 28 年 4 月以降、国内重要インフラ事業者向けの制御セキュリティ検証事業を立ち上げるべく、事業化を検討開始しており、東北企業への技術移転を徐々に進めているところである。

■ インフラ輸出強化

EDSA 認証は世界的に石油・化学分野を中心に調達要件の中で指定される場合があり、日本ベンダの海外展開に効果が出始めている。さらに、日本の企業からも徐々に問い合わせが出ており、一定レベルのセキュリティが確保された制御製品は、日本のベンダの競争力強化につながることが期待されている。

＜EDSA 認証製品を巡る状況＞

EDSA 認証製品に対して、石油・化学分野を中心にニーズが高まっている。

中近東や南米のインフラ・プロジェクトは、EDSA 認証を指定する件数が増えている。

＜導入事例と効果＞

日本の EDSA 認証製品の導入事例

某重要インフラ分野プラントに EDSA 認証済コントローラを 100 台規模で導入。

EDSA 認証済コントローラに対して、大手化学会社数社から問合せ、提案中。

日本ベンダの EDSA 認証取得による効果

- 海外展開、特にサウジアラビア向け石油プラント、米国・英国・オランダ（BP、ロイヤル・ダッチ・シェル等）石油メジャーに対する効果あり。
- 今後、水・発電関連において、東南アジア、北米、中東をターゲットとした訴求も期待している。

Ⅱ．外部有識者（評価検討会等）の評価

１．事業アウトカムの妥当性

普及啓発、認証機関確立、高セキュア技術の利用に関する指標については明確かつ妥当であり、当初目標をほぼ達成したことは評価できる。ユーザ企業に対する意識喚起、評価・認証に関する知見や攻撃者視点から開発した防御技術の組合員間での共有など、制御システムセキュリティの重要性の認識や普及を早期に進めた意義は大きい。

なお、認証審査件数が開発遅れ等の理由から目標を下回った点は課題である。また、人材育成指標として普及啓発が主となる訪問者数ではなく別の指標を定めるか、訪問者の目的別に価値を図るべきである。さらに、認証機関の確立を目指すのであれば、認証に関わる人材の育成や認証確立までの準備期間の短さ等も評価した方がよい。今後は、国が推進する他の人材育成プログラムに対しても、本研究における成果や知見の活用がなされることが期待される。

【肯定的所見】

・（Ａ委員）国際標準に則った評価・認証機関の確立、セキュリティの普及啓発、技術利用促進のいずれも事業終了時において当初の目標をほぼ達成している．日本の国際競争力を維持するために、制御システムセキュリティを担う人材育成は急務であり、本事業が与えた効果は評価できる.

・（Ｂ委員）本事業の３つのアウトカムである⑴啓発・人材育成　⑵認証機関確立　⑶高セキュア技術は、我が国の重要インフラを支える制御システムセキュリティを先導する役割を担うものであり、明確かつ妥当である。特に、ユーザ企業を中心に、制御システムセキュリティの重要性の意識喚起を早期から進めることができたことは高く評価できる。

・（Ｃ委員）（１）検証施設の活用によるユーザ企業を含む制御システムセキュリティ人材育成への寄与、評価・認証機関の確立と実働による知見共有、（２）攻撃者視点からのセキュリティ防御技術を開発し参加組合委員間での共有など、何れも妥当と評価できる。

【問題あり・要改善とする所見】

・（Ａ委員）制御システムセキュリティの審査件数については、受審側の開発遅れなどもあり、事業終了時においては目標を下回った.

・（Ｂ委員）本事業の⑴啓発・人材育成のアウトカム指標として、施設訪問者数は啓発活動の指標として適切であるが、人材育成の指標は別に設けるべきである。

・（Ｃ委員）ＳＩＰプログラムで推進するサイバーセキュリティ確保や、サイバーセキュリティ推進センター構想における人材育成プログラムに対しても、本研究における実環境を考慮した成果や知見の活用が期待される。

・（Ｄ委員）訪問人数だけでは、施設の持つ価値を計れない。施設を訪問者の目的別に人数を集計し、さらに滞在時間を掛け合わせることで、より具体的に価値が図れるのではないか？見学者と技術開発者では、訪問の意味も変るはずである。

・（Ｄ委員）ICS セキュリティの重要性の啓蒙と対応人材の育成も重要であるが、認証機関としては、認証に関わる人材の育成に重きをおくべきではないか。

・（Ｄ委員）評価・認証機関は、本邦初の立ち上げである。このため、準備期間->実施期間とフェーズも分かれるはずであり、全期間の結果として認証数を示すのではなく、準備期間では立ち上げが如何に短期間に行われたかを評価し、実施期間では実施数が評価されるべきではないか。

２．研究開発内容及び事業アウトプットの妥当性

国際標準に準拠した制御機器のセキュリティ認証を開始し認証取得実績もある点や、国際標準への意見提出、論文発表やメディア報道等、普及啓発につながる指標を明確にしたことは評価できる。技術的優位性を目指す制御システムの高セキュア化技術の開発、経済的優位性を目指す評価・認証手法の確立は、我が国の重要インフラの安心・安全と経済基盤の確立の両面で妥当である。

なお、高セキュア化技術開発の目標設定も必要であり、制御システムのみならず情報システムも含めた総合的なサイバーセキュリティ対策の立案能力の育成も重要である。研究成果については、特許の速やかな審査請求や国際特許としての出願等、組合員における活用促進と国際競争力の強化を目指すべきである。

【肯定的所見】

・（Ａ委員）国際標準に準拠した EDSA 認証を開始し、すでに４製品が認証を取得している。30 報の論文発表と 2 件の特許出願、国際標準への多くの意見提出などが実施されており評価できる

・（Ｂ委員）研究開発要素は、技術的優位性を目指す制御システムの高セキュア化技術、経済的優位性を目指す評価・認証手法として明確であり、我が国の重要インフラの安心・安全と経済基盤の確立の両面で妥当である。

・（Ｂ委員）アウトプット指標として論文、特許、国際標準への寄与などに加え、メディア報道など、社会啓発につながる指標を明確にしている。

・（Ｂ委員）事業アウトプットの目標値として認証機関の確立が設定されており、達成されていることは妥当である。

・（Ｃ委員）（１）国際標準をベースとしたＥＤＳＡ認証機関の設立と国内製品の認証取得による国際認知度の向上、（２）既存制御システムの構成変更難易度を考慮したホワイトリスト運用に対する効率化の研究、（３）サイバー攻撃の早期検知技術開発とプロトタイプ実装・評価、研究開発成果のコンテンツ化・普及啓発デモなど、何れも妥当と判断される。

【問題あり・改善とする所見】

・（Ｂ委員）事業アウトプットの目標値として、認証機関の確立に加え、高セキュア技術開発における目標値を設定し、達成状況を示すと良い。

・（Ｃ委員）標的型攻撃においては巧妙さ、複雑さが増す一方であり、人材育成面では、制御システムのみならず情報システムの利用環境も念頭に置いたリスクアセスメントを踏まえ、総合的なサイバーセキュリティ対策を立案する更なる応用力も重要と考えられる。

・（Ｄ委員）研究論文のリストを示すべきではないか。

・（Ｄ委員）組合員に使用させるためには、速やかに特許の審査請求を行うべきではないか。

・（Ｄ委員）国際競争力強化を考えると、国際特許として出願したかを示すべきではないか。

３．当省(国)が実施することの必要性

制御システムセキュリティに対してはユーザ企業や一般社会の認識が不足しており、ベンダ企業による積極投資が難しかったことから、国が研究開発を推進する意義は大きい。また、国際標準化を見据えた技術開発や評価認証手法の確立、国際相互承認などグローバルな取り組みは、国が主導

する必要がある。
　なお、民間では困難な認証機関設立の時期は終え、今後は民側への費用負担を求めるべきである。
規制緩和やオープン化の流れを受けて、他の作業分野も幅広く

【肯定的所見】
・（Ａ委員）将来的な国際標準化や評価・認証機関同士の国際相互承認を目指すための技術や標準、評価認証手法を確立するために不可欠な取り組みである.
・（Ｂ委員）重要インフラの安心・安全は我が国の産業基盤、社会基盤として必須でありながら、そのインフラを支える制御システムのセキュリティは、ユーザ企業や一般社会における認識が不足していたため、ベンダ企業自身による積極投資が難しかった。このような状況において、国が率先して研究開発事業を立ち上げ、民間企業や大学と協働で推進したことは高く評価できる。
・（Ｃ委員）制御システムのセキュリティに関して一律の技術、標準、評価・認証手法が確立していない中、民間企業個社が情報システムも含めてグローバルなサイバー空間へ立ち向かうには経営資源面からも限界があり、国際標準化をも見据えた国の役割は大きいと考える。
・（Ｄ委員）海外の機関、特に政府機関と真の連携をとるには、より一層国の機関としての位置付けを明らかとする必要がある。

【問題あり・要改善とする所見】
・（Ｃ委員）規制緩和やオープン化の流れの中では、他の産業分野も幅広く国がリードすべきと考える。
・（Ｄ委員）民間では難しい、機関設立の時期は終えた。このため、実際に利を得る民側にもっと費用負担を求めるべきである。

４．事業アウトカム達成に至るまでのロードマップの妥当性

2015 年度までの本事業の目標、制御システムセキュリティ人材育成・普及啓発、評価・認証機関の確立、高セキュア化技術開発は、重要かつ明確である。また、今後の方向性として、セキュリティ技術向上、重要インフラのセキュリティ確保、東北振興による産業化は妥当である。
　なお、３つの目標（人材育成、認証、高セキュア技術）を目指して得られた成果をさらに発展・活用することが重要であるが、そのためのロードマップは積極的に見直すことも重要である。さらに、東北地方における産業化や世界的中核拠点の整備に向けては、ロードマップの具体化が必要である。認証についても、認証制度や実施機関体制作りは国際的な競争領域であり、それに則した計画・体制、およびロードマップを再検討し、ビジネス的な視点も積極的に取り入れた活動を期待する。

【肯定的所見】
・（Ａ委員）「制御システムセキュリティ人材育成・普及啓発」、「制御システムセキュリティ評価・認証機関の確立」、「制御システムの高セキュア化技術開発」において目標を達成しており評価できる.
・（Ｂ委員）2015 年度までの本事業の成果は重要かつ明確である。
・（Ｃ委員）制御システムのセキュリティ技術の向上、重要インフラ分野から優先した取り組み、東北地方の振興のための産業化など、方向性として妥当と考える。

【問題点・改善とする所見】

・（Ａ委員）今後の EDSA 認証については、ビジネス的な視点も積極的に取り入れた活動が期待される.

・（Ｂ委員）本事業が目指す３つの目標（人材育成、認証機関、高セキュア技術）は、いずれも重要であり、事業アウトカムの達成に向けて、得られた成果をさらに発展・活用することが重要である。ただし、そのためのロードマップは積極的に見直すことも重要である。例えば：

－　高セキュア化技術としてホワイトリスト技術は重要であるが、制御システムセキュリティとしては一つの要素技術である。本事業の成果としてのホワイトリスト技術と、関連するセキュリティ技術を連携するための計画が重要である。

－　認証機関の取組みは重要であるが、認証制度や実施機関体制作りそのものが国際的な競争領域であり、その位置づけに則した計画・体制、およびロードマップを再検討すべきである。

・（Ｃ委員）東北地方における産業化や世界的中核拠点の整備に向けては、今後の推進体制の中でロードマップのより具体化が必要と想定される。

・（Ｄ委員）本事業の成果と今後の方向性の関連性を明記すべきである。

５．研究開発の実施・マネジメント体制等の妥当性

本事業の実施者は、我が国の制御システムの主要ベンダ企業、自治体や研究機関等の産官学からなる適切な研究開発実施体である．組合員の意向を重視した研究開発計画となっており、適切な学識経験者より助言を受けて内容を見直すなど、実施体制は妥当である。

なお、事業終了後における研究開発の実施・マネジメント体制については、必ずしも明確ではなく、今後の展開を考え、利用者となる重要インフラ事業者などが主体となれる組織体制または連携体制が必要である。さらに、防護側の技術は攻撃側の技術と表裏一体であり、研究開発成果の知財管理体制についても明示すべきである。

【肯定的所見】

・（Ａ委員）産官学からなる適切な研究開発実施体制となっている.

・（Ｂ委員）本事業の実施者であるＣＳＳＣは、我が国の制御システムの主要ベンダ企業、業界団体に加え、自治体や学会が連携しており、本事業の委託先として妥当である。

・（Ｃ委員）参加組合員の意向を重視した研究開発計画となっており、適切な学識経験者より助言を受けて内容を見直すなど、実施体制は妥当と考える。

【問題あり・要改善とする所見】

・（Ａ委員）事業終了後における研究開発の実施・マネジメント体制については、必ずしも明確ではない.

・（Ｂ委員）本事業成果に基づくアウトカム達成に向けて、制御システムセキュリティの利用者となる重要インフラ事業者などが主体となれる組織体制または連携体制が必要である。

・（Ｃ委員）セキュリティにおける防護側の技術は攻撃側の技術と表裏一体であり、研究開発成果の知財管理について体制図にも明示しておくべきと考える。

・（Ｄ委員）現状の運営委員会は設立検討時の構成である。今後の展開を考えると、プラントオーナ

一企業が組合員として参加しやすい組織運営体制を考慮すべきである。

６．費用対効果の妥当性

審査１件当たりのコストは、今後、認証普及により回収可能と想定され、日本のベンダの競争力強化という意味でも妥当な費用対効果である。認証によりベンダのセキュリティ向上やインフラ輸出力の強化の今後の社会効果に期待が持て、認証製品への投資全体および今後の事業規模全体における効果を指標とすることが望ましい。さらに、東北復興再生の観点から東北地方の企業等に研究成果を積極的に展開していることが評価できるため、復興再生への貢献額の概算が見積もられることが望ましい。

なお、本事業における人材育成、認証機関、高セキュア技術への取組毎に、費用対効果の評価がなされるべきである。国費全てを認証機関設立に費やしたわけではなく、企業からの認証取得費用を除外し、実際に要した費用でコストを示すべきである。

【肯定的所見】

・（Ａ委員）認証審査１件当たりのコストとすると高額にも思えるが、今後、EDSA 認証が普及するにつれて回収できるものである．また、日本のベンダの競争力強化という意味でも妥当な費用対効果である.

・（Ｂ委員）東北復興再生の観点からの取組として東北地方の自治体を拠点とする企業等に研究成果を積極的に展開していることが評価できる。さらに、復興再生への貢献額の概算が見積もられることが望ましい。

・（Ｂ委員）認証審査件数あたりの費用効果を指標としていることは重要である。さらに、認証を受けた製品への投資全体および今後の事業規模全体における効果（特にレバレッジ効果）を指標とすることが望ましい。

・（Ｃ委員）東北振興、産業化の具体的なプロセスが見えず定量的な評価は難しいが、製品の認証取得実績に伴い、プラントベンダのセキュリティ向上、インフラ輸出力強化の先駆けとなっており、今後の社会効果に期待が持て、妥当と考える。

【問題あり・要改善とする所見】

・（Ｂ委員）本事業における人材育成、認証機関、高セキュア技術への取組毎に、費用対効果の評価がなされるべきである。

・（Ｄ委員）15.4 億全てを認証機関設立に費やしたわけではない。実際に要した費用でコストを示すべきである。また、認証を受けた企業から得た認証料があれば、それを差し引くべきではないか。

・（Ｄ委員）東北企業での啓発・産業化は、アウトカムに謳われていない。

７．総合評価

我が国の重要インフラを支える制御システムセキュリティの重要性について、本事業が社会的な先導役としてその重要性を強くアピールでき、普及啓発および人材育成において重要な貢献をし、国際標準に則った評価・認証機関を確立、関連分野における我が国の国際競争力を保つために重要な役割を果たした．技術研究のみに特化せず、人材育成への取り組みも合せた実効的な研究成果を上げた。

一方、事業終了後も、継続的に研究開発や普及啓発および人材育成が不可欠な分野であるため、長期的なアウトカムの達成に向けたロードマップおよび実施体制については､ステークホルダーを考慮し、随時適切に見直しながら、具体的な内容を策定し推進することが望まれる。さらに、継続的な人材育成については費用対効果や他機関での育成との役割分担の点からの見直しが望まれる。

【肯定的所見】

・（Ａ委員）本事業は、日本の制御システムセキュリティの普及啓発および人材育成において重要な貢献をした. また、国際標準に則った評価・認証機関実施し、関連分野における我が国の国際競争力を保つために重要な役割を果たした.

・（Ｂ委員）本事業の開始前において、我が国の重要インフラを支える制御システムセキュリティの重要性について、その利用者であるユーザ企業や一般社会においては、十分に理解されているとは言えなかった。そのような状況において、本事業が立ち上がり、社会的な先導役として、技術開発、人材育成、認証評価の重要性を強くアピールできたことは高く評価できる。

・（Ｃ委員）制御システムの取り巻く社会状況や、サイバー攻撃の実態を踏まえ、対策技術の研究のみに特化せず、人材育成への取り組みも合せた実効的な研究成果と判断される。

【問題あり・要改善とする所見】

・（Ａ委員）事業終了後も、継続的に研究開発や普及啓発および人材育成が不可欠な分野であるが、今後の実施体制については必ずしも明確ではない.

・（Ｂ委員）認証機関の確立に向けた取組は挑戦的なものとして評価できるが、長期的なアウトカムの達成に向けたロードマップおよび実施体制については、随時適切に見直しながら推進することが望まれる。

・（Ｂ委員）同様に、人材育成・啓蒙活動のうち、実環境に近い制御システム設備を用いた活動は経営者を含めたユーザ企業の意識喚起や政策担当者への動機づけの面で評価できるが、継続的な人材育成については費用対効果や他機関での育成との役割分担の点からの見直しが望まれる。

・（Ｃ委員）今後のロードマップとして方向性は妥当と考えるが、実現に向けてはステークホルダーの調整なども考慮し、実施計画の具体化が必要と想定される。

【評点を付けるに当たり、考慮した（重要視した）点】

・（Ａ委員）EDSA 認証環境を整備し、テストベッドを構築し、3 年間で 4940 名が来所し、964 回のデモを実施したという実績.

・（Ｂ委員）制御システムセキュリティのユーザとなる重要インフラ事業者へのインパクト。意識づけができたことは高く評価するが、技術面での貢献度については更なる分析が必要である。

・（Ｃ委員）研究成果が実際の制御システムの構築、運転等に結び付いく結果となっているか、将来的なアウトカム達成へ向けたロードマップが具体的に可視化できているかの観点で評価を行った。

８．今後の研究開発の方向等に関する提言

巧妙化・複雑化するサイバー攻撃に対し、規制緩和やオープン化、IoT 化に伴い、制御システムセキュリティに関する研究開発、普及啓発、人材育成へは継続して取り組む必要がある。

本事業では、既存の運用中の制御システムを考慮した技術対策が考案され、プロトタイプ実装も

されており、成果・課題を踏まえた今後の展開が期待される。

技術開発においては、重要インフラシステムの特性（長い更改ライフサイクル、運用体制・手順を重視する風土、等）を踏まえ、ユーザ組織と密に連携できる研究開発の体制が必須である。また、「日本発の国産プログラム」の開発では、開発プロセス自体のセキュア化する公募・発注方法も運用すべきであり、コア部分は内製化も不可欠である。

人材育成は、そのプロセスが多岐にわたることから、産学官において社会的な分担を議論し、それぞれの得意領域を活かしながら、役割にそった取組を進め、相互連携により効果的に進めることが重要である。また、IT と制御等、各々部門の専門家がリスクアセスメントなどを通して相互に技術的な特徴を理解できる人材を育成していく事が望まれる。マネジメント、技術対策の両面を含む人材育成カリキュラムの指針整備が有効である。

認証については、ビジネス的な視点も積極的に取り入れた活動が期待される。

本事業は、地域の復興再生、産業活性化、研究開発でのアウトカムを目指す取り組みであるが、これらを同時に達成するために、今後の研究開発において目標とするアウトカムの絞り込みと達成時期を明確にし、具体的な実施計画に基づいた事業マネジメント（体制とロードマップ）が重要である。

事業者各々での対策は限界があり、国際標準化や攻撃情報と応急対処策の速やかな情報共有など、ルール整備や運用面においても、国が主体となったグローバルな取り組みが望まれる。今後は、本拠点の活用に加え、国内の様々な活動を柔軟にネットワーク化したコミュニティ体制を形成していくことが重要である。

【各委員の提言】

・（Ａ委員）制御システムセキュリティについては、制御システムの IoT 化の流れの中で、今後も継続的な研究開発と普及啓発、人事育成が必要である.

・（Ａ委員）今後の EDSA 認証については、ビジネス的な視点も積極的に取り入れた活動が期待される.

・（Ｂ委員）本事業は、地域の復興再生、産業活性化、研究開発という３分野でのアウトカムを目指す取組みであることに加え、それぞれにおいて、短期的成果（貢献）と中長期的成果（貢献）が期待される意欲的な取り組みである。ただし、それらの目標を同時に達成するための事業マネージメント（体制とロードマップ）は容易ではないことも明らかである。今後の研究開発においては、目標とするアウトカムの絞り込みと達成時期を明確にした事業マネジメントが重要である。

・（Ｂ委員）制御システムセキュリティの技術開発においては、そのターゲットとなる重要インフラシステムの特性（システムは機器の長い更改ライフサイクル、運用体制・手順を重視する風土、等）とのすり合わせが重要である。そのためには、ユーザ組織と密に連携できる研究開発の体制が必須である。

・（Ｂ委員）人材育成は、セキュリティ強化における共通課題である。その人材育成プロセスは、経営者や技術者に気付きをあたえる啓蒙活動（イベント的取組）から、数カ月から 1 年をかけてし

っかりとしたスキルを身に付ける育成活動まで多岐にわたる。今後の取組では、産学官において人材育成に関わる社会的な分担をしっかりと議論し、産官学がそれぞれの得意領域を活かしながら、役割にそった取組を進め、相互に連携することにより、効果的な人材育成を進めることが重要である。

・（Ｂ委員）制御システムのセキュリティ技術開発や人材育成の推進には、上記の観点での組織体制が重要であるが、箱物主体の組織は、その組織維持が重荷になりかねない。国が主体となって推進するためには、国内の様々な活動を柔軟にネットワーク化したコミュニティ体制を形成していくことが重要である。

・（Ｃ委員）巧妙化・複雑化するサイバー攻撃に対し、長期的なセキュリティへの取り組みが必要であり、規制緩和やオープン化に伴う制御システムセキュリティへの取り組みは継続する必要がある。また、これまでＩｏＴ技術を担ってきた人材と、制御システム技術を扱う人材は、各々部門の専門化として育成している事業分野もある中、リスクアセスメントなどを通して相互に技術の特徴を理解できる人材を育成していく事が望まれる。セキュリティ推進においてはマネジメント、技術対策面双方を含む指針となる人材育成カリキュラムの整備が有効と考えられる。

・（Ｃ委員）サイバー空間におけるセキュリティは事業者各々での対策は限界があり、グローバルな枠組みでの取り組みは国の役割が欠かせないと考えられる。国際標準化や、攻撃情報と応急対処策の速やかな共有など、ルール整備や運用面においても並行した取り組みが望まれる。

・（Ｃ委員）本研究においては、既存の運用中の制御システムを考慮した技術対策が考案されプロトタイプ実装もされており、成果・課題を踏まえた今後の展開が期待される。

・（Ｃ委員）評価・認証機関の活性化、研究成果の技術移転による東北地域振興など、今後のロードマップを実現するための具体的な実施計画も重要と考える。

・（Ｄ委員）ホームページの公募情報を見ると、重要なアウトカムである高セキュア化技術も公募されている。しかし、今後の研究開発を進める「日本発の国産プログラム」の開発では、開発プロセス自体のセキュア化を図る必要がある。このため、全体像がわからない様な公募・発注方法を開発して運用すべきである。また、コア部分は外部発注ではなく内製化も不可欠である。このため、組合各社により多くの人材派遣を求めるべきである。

＜上記提言に係る担当課室の対処方針＞

深刻化するサイバー攻撃に対して、重要インフラ等の稼働を支える制御システムセキュリティの確保は重要な課題である。
本事業では、制御システム機器・システムの製造・提供組織を中心に、研究開発を実施してきた。

今後は、制御システムのユーザ組織への人材育成への取り組みを強化し、ユーザ組織自らがサイバー攻撃の脅威を認識し、自組織のシステムリスクを適切に評価することで、セキュリティ対策への投資を促すエコシステムを構築すべく、平成 29 年度より、（独）情報処理推進機構（IPA）に産業系サイバーセキュリティ推進センター（仮称）を設置する。

技術開発においては、本センターの枠組みを活用し、ユーザ組織と研究機関・大学等との連携を一層深めながら推進する。

人材育成では、本事業で整備した演習コンテンツも活用しながら、情報系から制御系までの模擬プラントを用いた演習や対策立案等を行い、IT と制御等の人材が専門家と共に実施するリスク分析等を通じて、相互の理解を深め、実効的な対策を立案可能となることを目指す。

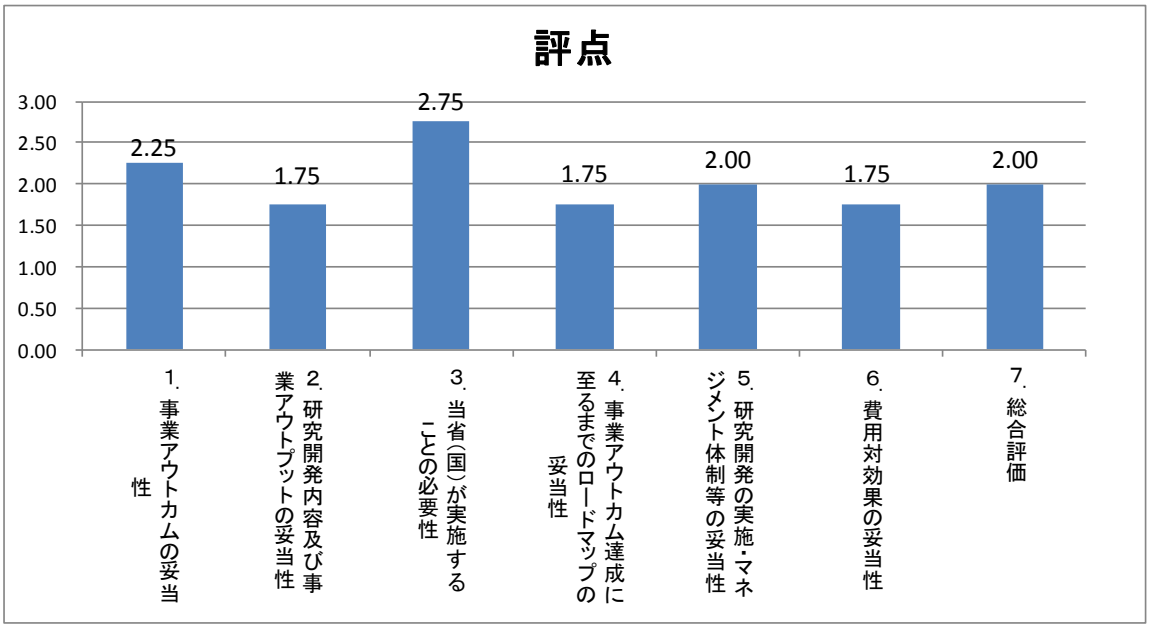
認証については、IoT 化を見据えた、制御システム全体のセキュリティ評価・認証の仕組みや、第三者評価のあり方について検討を行い、関係主体の事業性を考慮した持続可能な制度構築に向けて取り組む。

本事業の研究開発テーマは、平成 28 年度以降、国が実施する研究開発事業に引き継がれ、具体的な実施計画の下、推進する。また、地域の復興再生や産業活性化等においては、引き続き地元自治体と連携しつつ、新たなセンターにおける人材育成施策や認証事業の方向性を踏まえ、実現を図る。

新たなセンターでは、本事業で整備した拠点を活用しつつ、海外の政府機関・研究機関との連携を強化する。また、国際標準化や情報共有等、サイバーセキュリティ対策の推進に向け、内閣官房サイバーセキュリティセンター（NISC）や関係省庁と連携しつつ、官民協調した取り組みを推進する。

Ⅲ．評点法による評価結果

	評点	A委員	B委員	C委員	D委員
1．事業アウトカムの妥当性	2.25	2	2	3	2
2．研究開発内容及び事業アウトプットの妥当性	1.75	2	2	2	1
3．当省（国）が実施することの必要性	2.75	2	3	3	3
4．事業アウトカム達成に至るまでのロードマップの妥当性	1.75	2	1	2	2
5．研究開発の実施・マネジメント体制等の妥当性	2.00	2	2	2	2
6．費用対効果の妥当性	1.75	2	2	2	1
7．総合評価	2.00	2	2	3	1



【評価項目の判定基準】
評価項目１．～６．
３点：極めて妥当
２点：妥当
１点：概ね妥当
０点：妥当でない

評価項目７．総合評価
（終了時評価の場合）
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、不十分なところがあった。
０点：実施された事業は、極めて不十分なところがあった。

Ⅳ．評価ワーキンググループの所見及び同所見を踏まえた改善点等

評価ワーキンググループの所見【終了時評価】 ※評価ＷＧの指摘を記載する。 （（「所見」に該当する評価項目を記載する）） ・ ・ ・
所見を踏まえた改善点（対処方針）等【終了時評価】 ※評価ＷＧの指摘を踏まえ、各原課において記載する。 ・ ・ ・ ・

評価ワーキンググループの所見【事前評価】 ①情報セキュリティに係るプログラムの進め方等 ・情報セキュリティに係る本プログラムの目指しているところは重要であり、その内容をより強化して進めて欲しい。どのようなサイバー攻撃があり得るのか、想定されているよりもより広くその範囲をとって、それに対応できるようなプログラムにしてほしい。セキュリティというのはエンドレスになるので、体制として常に追いかけっこをしていくことを想定した上で、人材育成の問題、総務省を含めた体制全体の問題など、どのように展開していくのかというダイナミクスをプログラムの中で考えて欲しい。 ・ＥＩＡ（米国電子工業会）の動きや米国の状況（軍事等のリスク回避の事例など）を考えると、日本の場合、対象として化学プラントを想定してもよいのではないか。 ・現在の制御システムに加えたり変更していくことになると思うが、２０００年問題でもあれだけ大騒ぎした。新しい認証評価の制度が導入されると認証できない工場がでるなどいろいろな問題がでてくると思うが、どんな順序で、また、どんな体制で国民の安心感を保持しつつ巨大なレガシーシステムをアップデートしていくのか、もう少し考慮しておかないといけない。 ②その他 情報セキュリティの標準化を進めている人たちからは大変だという意見があるため、いろいろなことが動かないのであれば経済産業省に動いていただく必要がある。
所見を踏まえた改善点（対処方針）等【事前評価】 ①情報セキュリティに係るプログラムの進め方等 ・標的型攻撃に関する対策としては、インシデント発生前において、想定外の攻撃に対しても対処できるような、マルウェア対策を実装するための日本発の国産プログラムを設計・開

発し、既存の制御システムに適用し、新しい制御システムには標準装備するように対処する。また、このような技術構成要素が、外国や悪意を持った者に漏えいしないよう開示範囲を明確に絞りながら、国内制御ベンダ・ユーザに限定して広く普及することを目指す。
・ガス協、日化協などの業界団体が、技術研究組合制御システムセキュリティセンター（CSSC）の組合員として加入する予定で前向きに検討中であり、まずは、このような業界団体を通して、制御システムセキュリティ向上のための普及啓発を行っていく。次の段階において、必要となるセキュリティ人材像を明確にし、調達者・責任者・オペレータの各担当において到達すべきスキル標準を明確にし、必要な研修コンテンツを活用して人材育成を行っていく。各制御ベンダ・ユーザ企業内においても同様に、人材育成を行う。また、大学やセキュリティキャンプ事業とも連携した人材育成を行っていく。
・総務省とは、NICT の新世代通信網テストベッド StarBED（大規模エミュレーション基盤）と経産省の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）とを将来的にはつなぐことで連携を図っていく。両施設を相互に利用して、経産省と総務省で連携してセキュリティ検証を実施する。
・セキュリティ検証の対象分野としては、まずは、重要インフラ（電力、ガス）分野及び化学プラントに優先的に焦点を当て、その後、通信、自動車、半導体、造船等にも対象範囲を広めていく。
・産業用制御システムの標準化動向について調査し、戦略的に対応する標準を IEC62443（制御システムセキュリティ）に絞り込んだ。今後、国内ベンダ等への影響度合いを勘案しつつ、我が国の優位な技術や特徴（高品質・高信頼のシステム等）を活かした戦略的な国際標準化推進を図る。

②その他
・IEC62443（制御システムセキュリティ）の国際標準化推進の取り組みについては、国内委員会（JEMIMA）を母体として、政策と連携して経済産業省主導で取り組みたい。2014 年度中の国際標準化を目指して取り組む。
策定中の IEC62443 への日本要求の提言、基準反映として、現在、IEC で策定が進められているドラフトに対して、「国内ベンダへの影響度の大きさ」、「国内ベンダの国際競争力強化」を考慮した寄書の提案を実施する。
New Work Item の提案推進として、日本の優位な技術や特徴を活かし汎用的な標準を各業界や各コンポーネント向けに最適化した標準(3-4,4-3)の策定や、汎用的な制御システムに対して現時点で標準化されていない日本として強みとなる技術の標準化を目指す、なお、その際には、その主体者(ベンダーや業界団体等)とともに検討を実施する。また、CSSC で開発する先行技術(インターロック機能保護、バッチ検証他)や、日本式ビジネスモデルに適応するための標準化を目指す。
標準の普及啓発推進として、既に標準化されているパートに関する調査や分析を利用促進の観点で実施し、結果の普及啓発を行っていく。特に、2-1 は、国内重要インフラのセキュリティ強化に活用していく。