第34回評価ワーキンググループ
補足資料－2

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 プロジェクト終了時評価 補足資料

平成28年12月21日

商務情報政策局サイバーセキュリティ課

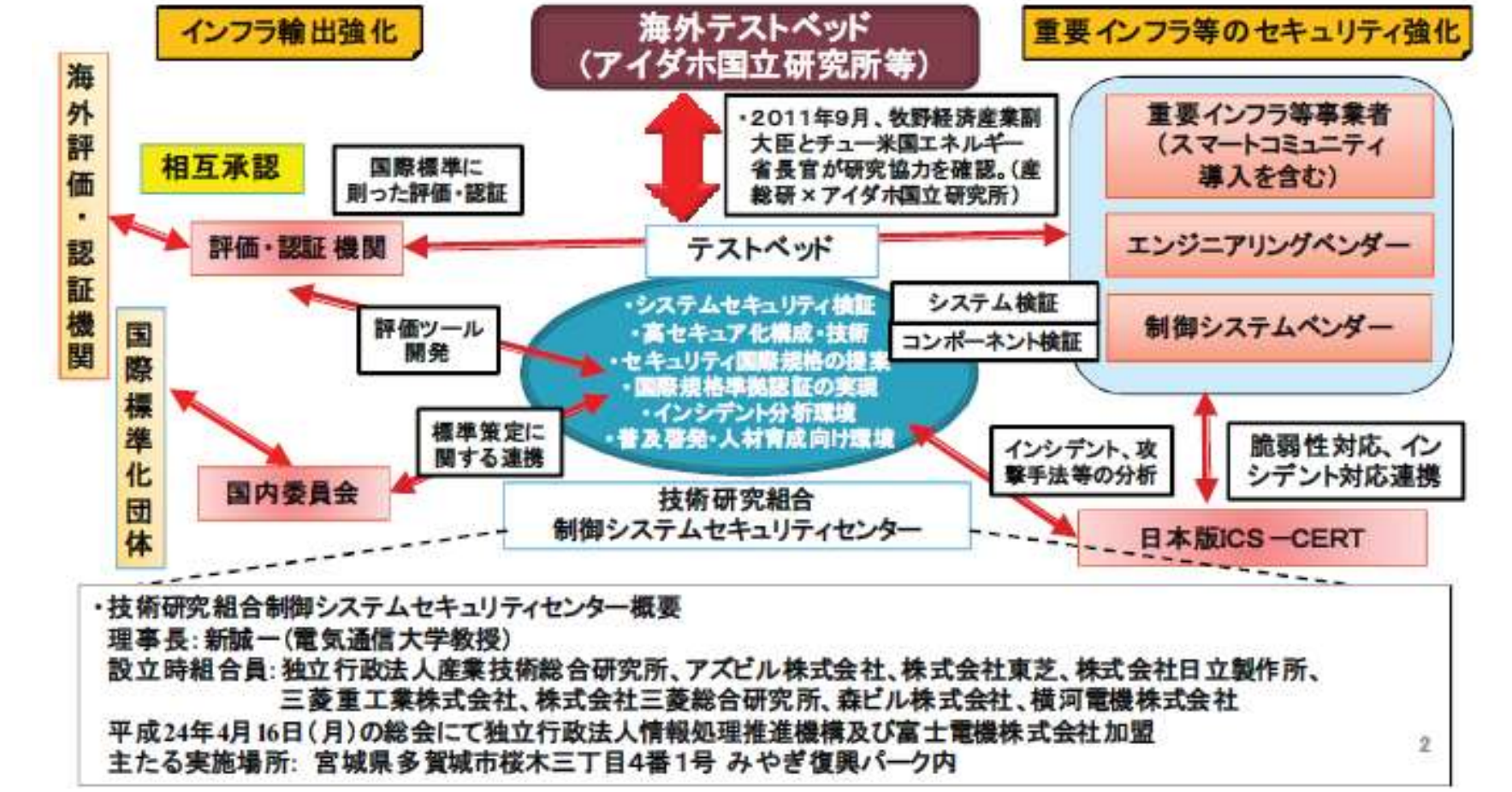
目　次

1．事業の概要　（1）事業の全体像

概　　要	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。
実施期間	平成25年度～平成27年度　（3年間）
実施形態	国からの直執行（民間企業への委託事業）
予算総額	14．5億円 （平成25年度：5.35億円　平成26年度：5.15億円　平成27年度：4.00億円）
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
プロジェクトリーダー	新　誠一　　制御システムセキュリティセンター　理事長 電気通信大学　教授

1. 事業の概要　（2）研究開発の概要

- 東北地方のセキュリティ検証施設（テストベッド）を活用し、評価・認証機関を確立。
- 制御システム・機器に関する「評価・認証」「高セキュア化の研究開発」「普及啓発・人材育成」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及びインフラ輸出強化を図る。

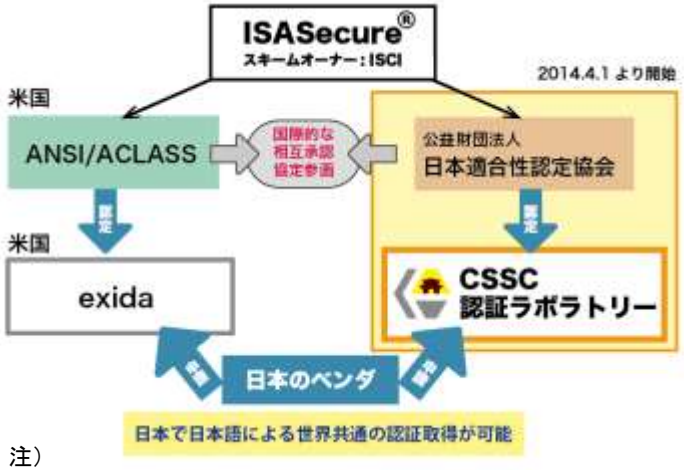


注）・ICS-CERT：Industrial Control System – Computer Emergency Response Team
（産業制御システム緊急対応チーム、米国はDHS（国土安全保障省）に設置

1. 事業の概要　（2）研究開発の概要　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。

制御システムセキュリティの日米相互承認



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
- 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

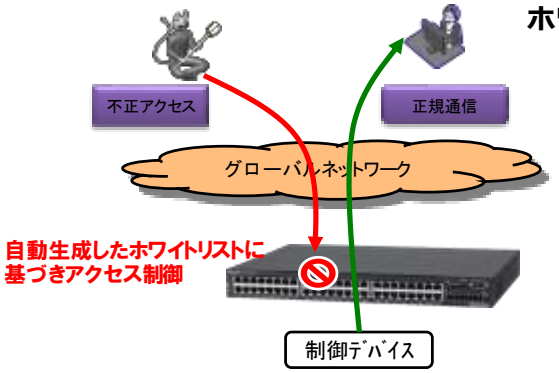
CSSC認証ラボラトリーの活動

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

1. 事業の概要　（2）研究開発の概要　②制御システムの高セキュア化

- 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。（ホワイトリストは実用化済）

ホワイトリストの学習機能に関する研究



ホワイトリスト自動設定と手動作成の効率検証

種別	85行の作成時間
手動作成	85分
自動設定	30分

65%削減

サイバー攻撃の早期認識支援技術

オンライン情報(1)
オンライン情報(2)
オフライン情報

・化学プラントで異常診断ロジックを製作
・プロトタイプの開発
・特定のサイバー攻撃の原因弁別が可能

サイバー攻撃を含む異常仮説の絞り込み

・オンライン情報(1):リアルタイムで常にモニターしている情報
・オンライン情報(2):必要に応じてオンラインで獲得する情報
・オフライン情報：現場情報を獲得し人間がシステムに入力する情報

CSSCにおけるサイバー攻撃に対する対策技術の研究

[機器]

・ISCI/EDSA評価認証技術（7）
・CSSC独自の検証項目策定
・ホワイトリストスイッチ（2）
・ホワイトリスト（端末・サーバ向け）（1）
・セキュリティバリアデバイス(SBD)

[システム、プラント]

・システムの評価認証技術（1）
・セキュアな制御システム構築ガイド(IEC62443)（1）
・セキュアなログ集約技術（1）
・ログの横断的分析技術（1）
・早期認識支援技術（CAeRS）（1）
・多層防御および多重防御技術（1）
・CSSC独自の検証ツール

[テストベッド]

・セキュアな実験環境構築運用（5）
・OPCによる相互接続環境の構築
・対策機器の評価環境構築運用
・サイバーセキュリティ演習を中心とした普及啓発

新規環境　6件
新規/既存環境　15件　で利用

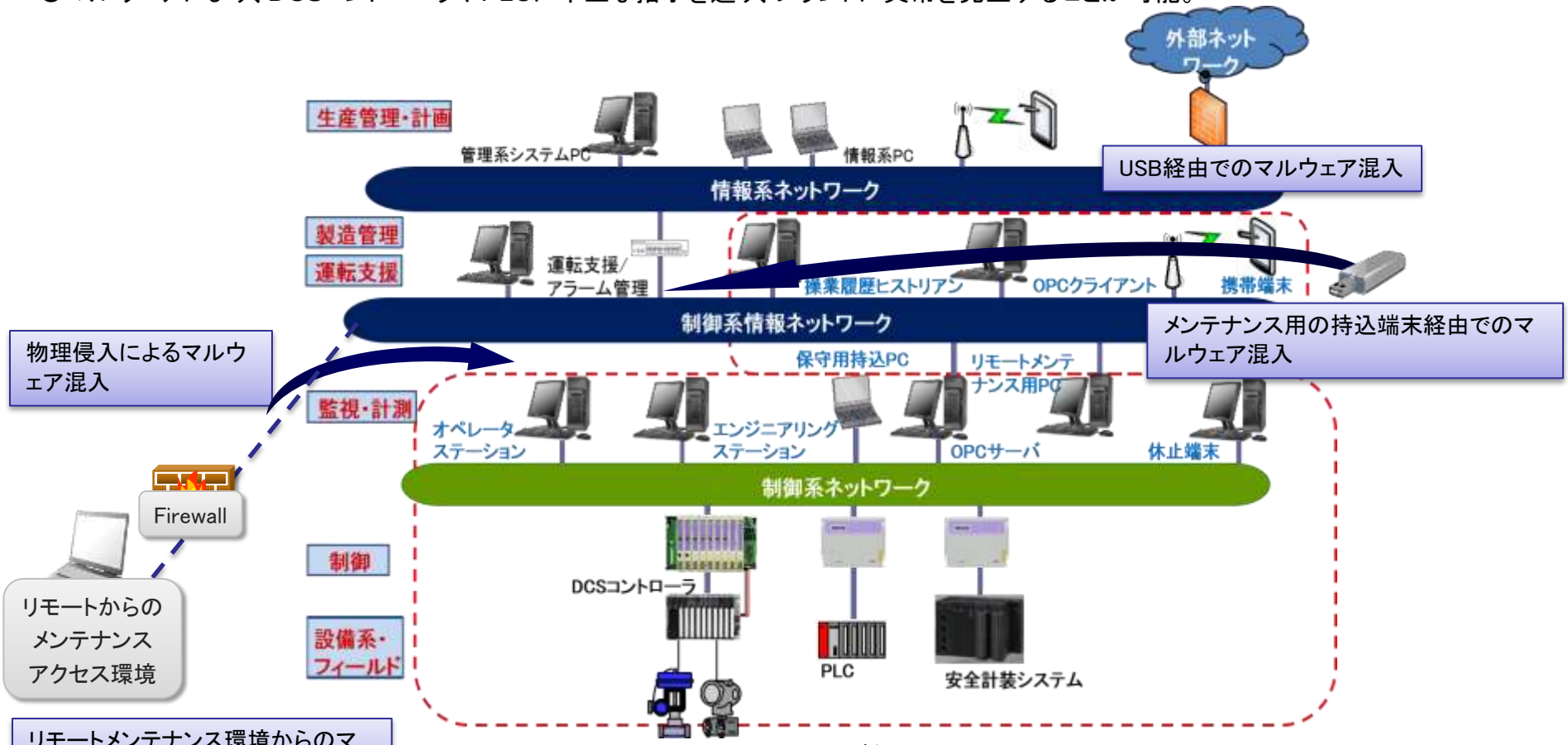
※（ ）は成果の利用件数。下線の技術は新規環境で利用可能、それ以外の技術は新規/既存環境とも利用可能。

1. 事業の概要　（2）研究開発の概要　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。3年間で合計4,940名がセンターに来所し、964回のデモを実施。

普及啓発のための演習シナリオの一例

●クローズと思われている制御システムにも、USBやリモートメンテナンス等、外部との接続点を経由したマルウェア混入等のリスクあり。
●マルウェアにより、DCSコントローラやPLCに不正な指示を送り、プラントに異常を発生することが可能。



注）
PLC　：　Programmable Logic Controller　：　プログラム可能なシーケンス制御装置
DCS　：　Distributed Control System　：　分散制御システム

1. 事業の概要　（3）政策的位置付け

- 「サイバーセキュリティ戦略」（平成25年6月、27年9月）「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）に位置付け。

サイバーセキュリティ戦略

■重要インフラを守るための取組

- 重要インフラ分野の範囲及び各分野内での「重要インフラ事業者」の範囲の継続的な見直し
- 情報提供によって不利益が生じない環境の構築、より効果的かつ迅速な官民の情報共有（ホットライン構築、情報共有の様式・手順の改良、処理の自動化等）、政府機関内での必要な連携、訓練・演習の実施の推進
- マイナンバー導入等の環境変化も見据え、地方公共団体に対し、政府として必要な支援を実施
- 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

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

行動計画期間中の施策

（1） 広報公聴
- 行動計画及びその取組について、広く認識・理解を得るための公報広聴活動の充実

（2） 国際連携
- 欧米、ASEAN、Meridian等二国間、地域間、多国間の枠組みの積極的な活用を通じた国際連携

（3） 規程類の整備
- 重要インフラ防護に係る関連規程集の発行
- 国際基準等の適用の際の手引書等の整備
- 情報セキュリティに関する評価・認証制度の拡充の支援

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する。

2. 事業アウトカム

- 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。

事業アウトカム指標 （妥当性・設定理由・根拠等）	目標値 （計画）	達成状況 （実績値・達成度）	原因分析 （未達成の場合）
制御システムセキュリティ人材の育成 （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	（事業開始時） **1,000**	**1,483** **（148.3%）**	（達成）
	（中間評価時）	**ー**	ー
	（事業終了時） **1,800**	**1,730** **（96.1%）**	26年度～27年度は1,700～1,800人／年の受講者が来訪し、目標をほぼ達成。
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 （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	（事業開始時） **3**	**3** **（100%）**	（達成）
	（中間評価時）	**ー**	ー
	（事業終了時） **4**	**2** **（50%）**	EDSA認証取得予定事業者が、製品開発の遅れにより受審できず、さらに市場動向を踏まえSSA認証の開始を見合わせたため、審査件数は目標を下回った。
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	（事業開始時） **10**	**9** **（90%）**	研究開始の早期の段階から技術の活用が進展。
	（中間評価時）	**ー**	ー
	（事業終了時） **20**	**21** **（105%）**	（達成）

3. 事業アウトプット

- 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。

事業アウトプット指標 （妥当性・設定理由・根拠等）	目標値 （計画）	達成状況 （実績値・達成度）	原因分析 （未達成の場合）
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	（事業開始時） －	－	－
	（中間評価時）	－	－
	（事業終了時） **1**	**1** **（100%）**	（達成）

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

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	ライセンス付与数	国際標準への寄与※	プロトタイプの作成
32	32	1	0	0	306	50

※IEC62443に準拠したEDSA認証規格に対する意見提出数

●受賞：1（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

＜参考＞論文リスト①

	種別	タイトル	著者	掲載誌
1	寄稿	制御システムセキュリティの国内動向（2013）	新　誠一	信頼性シンポジウム発表報文集 2013_春季(21), 7-32, 2013-06-12
2	寄稿	制御システムセキュリティセンターの活動 (特集 制御システムセキュリティ)	小林偉昭	日本工業出版
3	寄稿	増加する社会インフラを標的としたサイバー攻撃　Increasing Number of Cyber Attacks against Social Infrastructure	松崎和賢	情報処理 55(7), 636-637, 2014-06-15
4	寄稿	国民生活の要(かなめ)、産業インフラが標的に	新　誠一	OHM 101(3), 35-38, 2014-03
5	寄稿	制御システムセキュリティセンター活動紹介 : セキュアな制御システムを世界へ未来へ	小林偉昭	SEC journal 9(4), 202-205, 2014-01
6	寄稿	増加する社会インフラを標的としたサイバー攻撃:1. 社会インフラへのサイバー攻撃に対する課題と取り組み	新　誠一	情報処理 55(7), 640-646, 2014-06-15
7	寄稿	コントローラ,それはネットワーク機器 (特集 制御システムセキュリティの現状と課題)	新　誠一	計測と制御 53(10), 885-888, 2014-10
8	寄稿	工場の設備制御システムユーザによる現状の再認識と課題整理	新　誠一	計測と制御 53(10), 889-894, 2014-10
9	寄稿	情報機器化する制御装置とセキュリティ対策	新　誠一	日本原子力学会誌アトモス
10	寄稿	原子力分野における制御システムセキュリティ	村瀬　一郎	日本原子力学会誌アトモス
11	寄稿	制御システムセキュリティテストベッドについて	澤部直太	日本原子力学会誌アトモス
12	国際会議	A study of the asset discovery scheme using SCAP for IACS	N.Matsumoto, N. Saito, T.Yamada, S.Takemoto and T. Kamiwaki	SICE Annual Conference 2014
13	国際会議	ICSでのホワイトリスト制御	K. Suzaki, M. Kiuchi, H. Seki, Y. Komoriya	ICSJWG2014-Fall
14	座談会記事	人間とシステムの協調で社会インフラにレジリエンスを（座談会記事）	高橋 信	日立評論2014年3月号
15	論文	制御システムセキュリティセンターの紹介	小林偉昭	電子情報通信学会技術研究報告. ICSS, 情報通信システムセキュリティ 114(340), 1-6, 2014-11-20

＜参考＞論文リスト②

	種別	タイトル	著者	掲載誌
16	国際会議	Follow-up on Japan's Control Systems Security Center (CSSC) Efforts Since 2012	K. Matsuzaki, S. Watanabe, H. Kobayashi	ICSJWG Fall Meeting
17	寄稿	スマートグリッドとセキュリティ (特集 ビッグデータの技術動向)	新 誠一	Smart grid : technical journal 5(3), 21-27, 2015-07
18	寄稿	社会インフラにおけるサイバーセキュリティ課題の全体像	新 誠一	安全工学 54(6), 407-411, 2015
19	寄稿	制御システムのセキュリティ標準・認証とその活用状況	小林偉昭	電気評論 100(615夏季増刊), 49-55, 2015-06
20	寄稿	IEC 62443-2の紹介	奥村 剛	Sysmac Global Clubメールニュース（オムロン）
21	寄稿	EDSA認証の紹介	奥村 剛	Sysmac Global Clubメールニュース（オムロン）
22	寄稿	制御システムセキュリティの現状と認証制度の概要	奥村 剛	計装12月号
23	国際会議	A prototype of a cyber incident diagnosis mechanism for an early recognition support system against cyber attacks	S. Hosokawa, M. Enomoto, K. Matsumoto, M. Takahashi	ASCC 2015
24	国際会議	A Fallback Control Study of Networked Control Systems for Cybersecurity	K. Sawada, T. Sasaki, S. Shin and S. Hosokawa	ASCC 2015
25	国際会議	Model Based Fallback Control for Networked Control System via Switched Lyapunov Function	T. Sasaki, K. Sawada, S. Shin and S. Hosokawa	IEEE IECON
26	論文	CSSC、CAeRSの紹介	高橋信	ヒューマンインタフェース学会誌
27	寄稿	社会インフラとセキュリティ (社会インフラシステムにおけるセキュリティ対策)	新 誠一	標準化と品質管理 69(7), 2-6, 2016-07
28	寄稿	日本発 スマートものづくり(第12回)IoTを生かすためのセキュリティー	新 誠一	日経ものづくり (744), 106-110, 2016-09
29	寄稿	制御システムセキュリティに係わる評価認証について	小林偉昭	計測技術 44(1), 1-6, 2016-01
30	寄稿	制御システムの標準と認証の詳細	小林偉昭	標準化と品質管理 69(7), 14-21, 2016-07
31	寄稿	日本のエネルギーサービスとセキュリティ対策のあり方	吉松健三	単行本（電気学会）
32	国際会議	Rule Based Fallback Control System via Kalman Decomposition	T. Sasaki, K. Tsukada, K. Sawada, S. Shin, S. Hosokawa	ISA PCS2016

4．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。

5. 事業アウトカム達成に至るまでのロードマップ

CSSCの研究開発の特徴

- 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た研究開発
- 組合員・有識者による知見の結集による研究開発
- 攻撃者目線での検証シナリオによる防御技術の研究開発

本事業の成果

2015年

- 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

今後の研究開発の方向性

国の次期研究開発に沿った研究開発	重要インフラ事業者のセキュリティ確保に貢献する研究開発	東北地域の振興のための研究開発
2016年 • 稼働中特定の動きのみをさせるホワイトリスト技術の確立 • IoT化しつつある制御システムにおける異常の検知と予測、および高可用性確保技術の確立	• 評価認証による重要インフラのセキュリティ確保の底上げ • 重要インフラに対する侵入テスト等によるセキュリティ検証の実施 • 重要インフラ人材育成のためのコンテンツ開発	• 東北地域の企業（TOiNX等）との連携による研究開発 • 東北地域の大学・研究機関（東北大学等）との研究開発 • 自治体（宮城県・多賀城市等）との連携による研究開発
2020年 • IoT化へのさらなる対応 • 攻撃技術の蓄積	• 検証を踏まえた評価認証への対応 • 人材育成の強化 • 先導的な重要インフラ分野から他の重要インフラ分野への展開	• 東北地方への技術移転
制御システムセキュリティ技術の向上	重要インフラ事業者のセキュリティ向上	東北地方における制御セキュリティの産業化

東北多賀城本部を中心とした制御システムセキュリティ技術の世界的中核拠点

＜参考＞組合員における成果の実装状況

- 本事業を通じ、制御システムセキュリティ関連の製品化、自社製品のセキュリティ強化、新規事業の開始・強化等の成果実装が進展。
- 組合員の自主的な取り組みや情報収集においても、同様の成果実装。

成果展開方法	主な事例			
	製品化・販売、特許出願	自社製品等のセキュリティ強化	新規事業開始、事業強化	自組織の対策への反映
本事業による委託案件を通じた成果の実装	• ホワイトリストスイッチを製品化（2組織） • ホワイトリスト製品を販売（2組織） • セキュリティバリアデバイスを特許出願中 • セキュアなログ蓄積手法の製品化検討中（2組織） • ホワイトリスト技術の製品化検討中	• 制御機器の検証結果を製品に反映（2組織）	• 制御システムセキュリティ事業立ち上げ（3組織）	• 自社のセキュリティ対策に実装
組合員独自の取り組みによる成果の実装	• データダイオード、パスワード管理ツール、内部犯行検証ツール等の販売 • ホワイトリスト製品の販売	• 制御機器の検証結果を製品に反映（8組織） • 自社製品・サービスのセキュリティ強化（3組織） • 制御機器の検証結果の開発プロセス反映検討	• 制御システムセキュリティ事業立ち上げ	• 自社のセキュリティ対策に実装
認証取得に関わる実装	• 認証取得を念頭に対応機能を開発	―	• 認証取得により海外ビジネス展開（3組織）	―
情報収集からの実装	• デコイサーバを製品化 • ホワイトリスト製品を販売（2組織） • ホワイトリスト制御LAN装置を製品化 • 制御システム向けセキュリティ監視技術の製品化検討中	• 自社製品・サービスのセキュリティ強化（10組織） • 制御関連製品のセキュリティ機能の検討	• 制御システムセキュリティ事業立ち上げ（8組織） • 評価認証関連事業検討中（2組織） • 関連事業確立に向け検討中	• 自社のセキュリティ対策に実装（2組織）

6. 研究開発の実施・マネジメント体制等

- 「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。

経済産業省

委託

技術研究組合制御システムセキュリティセンター

理事長　新誠一
（電気通信大学 教授）

東北多賀城本部長　高橋信
（東北大学 教授）

委託

民間企業等

株式会社三菱総合研究所、東北インフォメーション・システムズ株式会社
イーヒルズ株式会社、株式会社MHPSコントロールシステムズ、
アラクサラネットワークス株式会社、アズビル株式会社、
株式会社日本環境認証機構　等

役職	氏名	所属等
理事長	新　誠一	国立大学法人電気通信大学　教授
理事	伊東　忠義	アズビル株式会社　執行役員 アドバンスオートメーションカンパニー ソリューション・サービス事業統括長
理事	渡部　宗一	イーヒルズ株式会社　取締役
理事	石井　秀明	株式会社東芝　社会インフラシステム社 統括技師長
理事	阿部　淳	株式会社日立製作所 サービス＆プラットフォームビジネスユニット 制御プラットフォーム統括本部 統括本部長
理事	関口　智嗣	国立研究法人産業技術総合研究所 情報・人間工学領域長
理事	中川　正也	三菱重工業株式会社　執行役員 ICTソリューション本部長
理事	近藤　賢二	三菱電機株式会社 専務執行役　開発本部長
理事	森　浩生	森ビル株式会社 取締役副社長　執行役員
理事	浦　直樹	横河電機株式会社IAPF事業本部　システム 事業センター長
顧問	高橋　信	東北多賀城本部長 東北大学　教授
顧問	渡辺　研司	名古屋工業大学　教授
顧問	澤田　賢治	国立大学法人電気通信大学　准教授
監事	稲垣　隆一	弁護士
事務局長	村瀬　一郎	技術研究組合制御システムセキュリティ センター

6. 研究開発の実施・マネジメント体制等

名称	**技術研究組合 制御システムセキュリティセンター** （英文名）Control System Security Center （略称）　CSSC ※経済産業大臣認可法人	**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）**
設立日	2012年3月6日（登録完了日）		
所在地	【東北多賀城本部（TTHQ)】 宮城県多賀城市桜木3-4-1 （みやぎ復興パーク F-21棟 6階）	**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。

（2016年10月1日時点）

7. 費用対効果

■ 活動指標及び活動実績（アウトプット）
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（単位当たり1.8億円/件）。
審査受審企業は、審査を通じ、製品のセキュリティ向上、認証取得に加え、セキュアな製品開発プロセス・体制の構築、評価技術に関わる知見の獲得が、他の製品のセキュリティ向上にも寄与。
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。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あり。

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。
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、事業化を検討している。

■ 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。

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。

８．外部有識者の評価等

８－１．評価検討会

評価検討会名称		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
評価検討会委員	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
	委員	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

８－２．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。

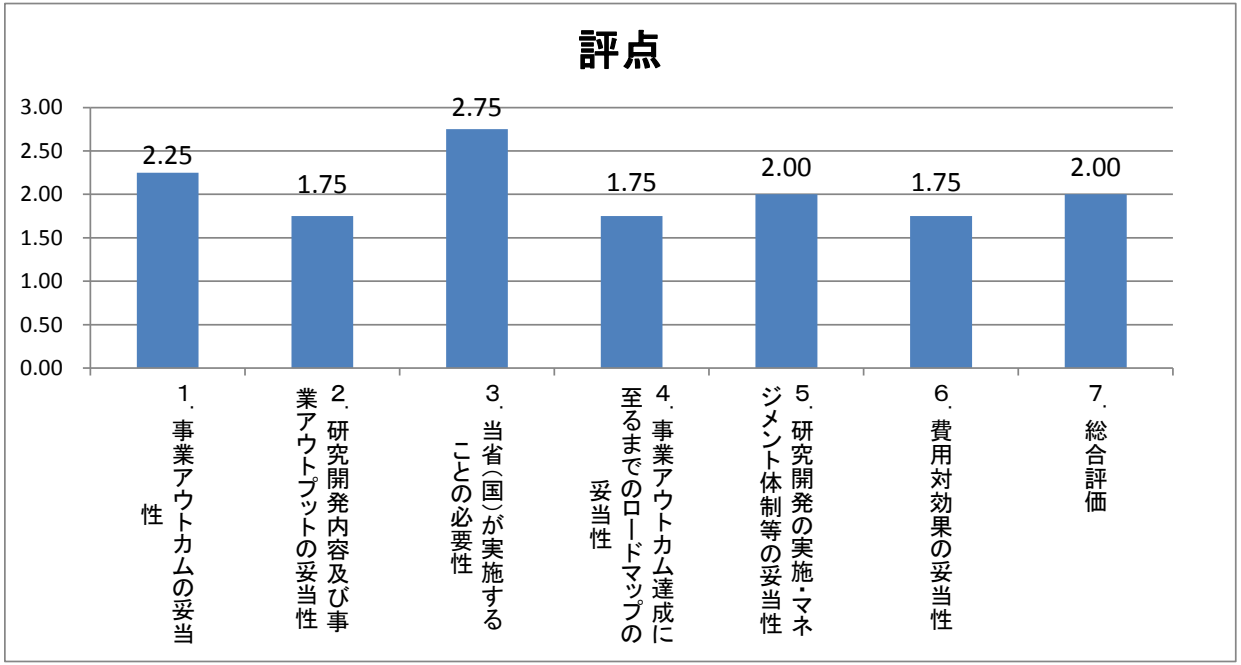
8－3. 評点結果

○「経済産業省技術評価指針」に基づき、プロジェクト終了時評価において、評点法による評価を実施した。

○「研究開発内容及び事業アウトプットの妥当性」については、高セキュア化技術開発の目標設定も必要、総合的なセキュリティ対策立案能力の育成も重要、さらに特許の速やかな審査請求や国際特許としての出願等、組合員の活用促進と国際競争力の強化を目指すべきとの意見があった。

○「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」については、ロードマップの積極的な見直しや具体化の必要性が指摘された。

○「費用対効果の妥当性」については、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、との指摘があった。



【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

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。

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

○ 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。

９．提言及び提言に対する対処方針

提言に対する対処方針

○ 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。