第1回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
資料5

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・促進事業の概要

平成28年11月15日

商務情報政策局サイバーセキュリティ課

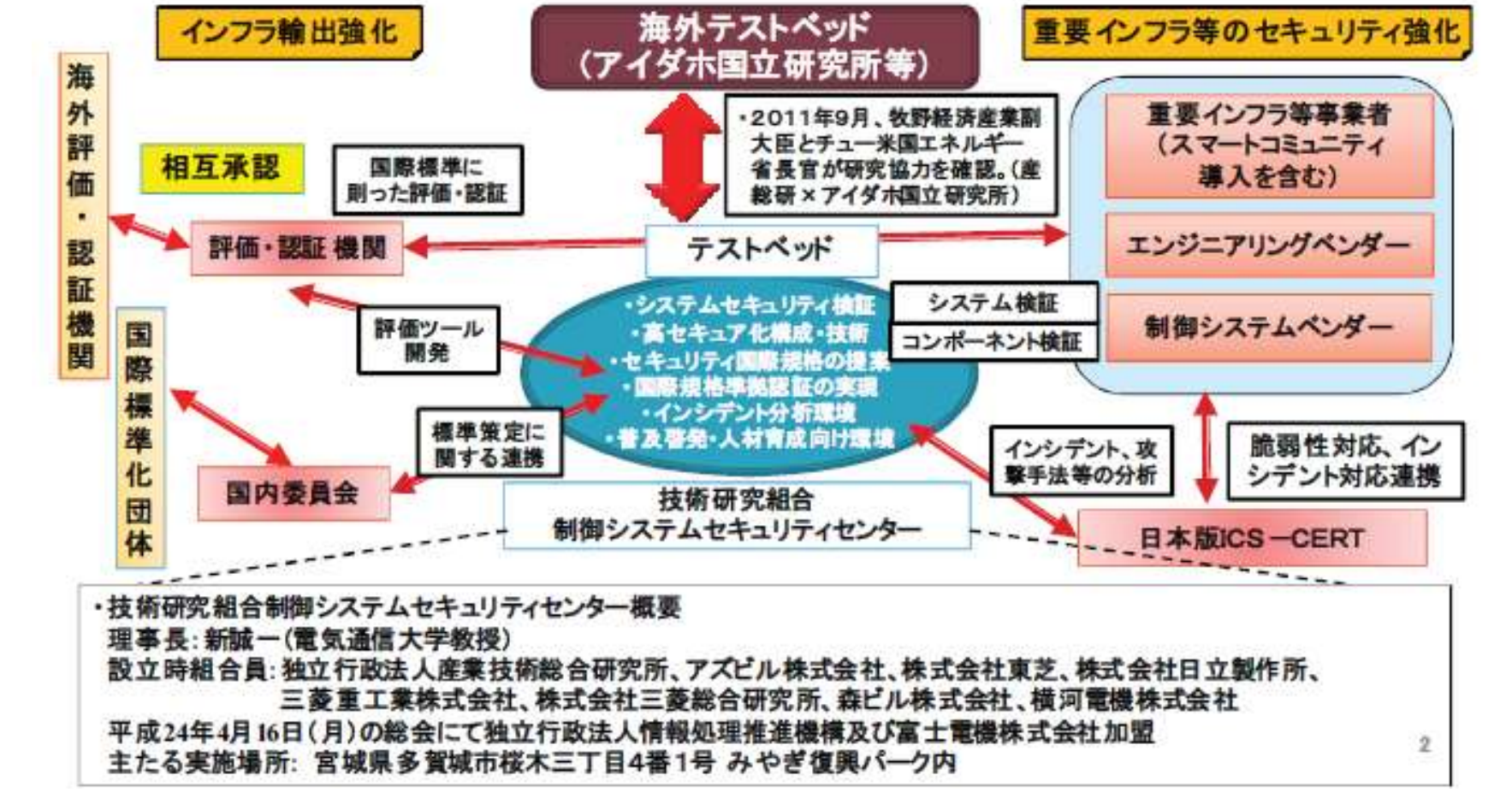
目　次

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。

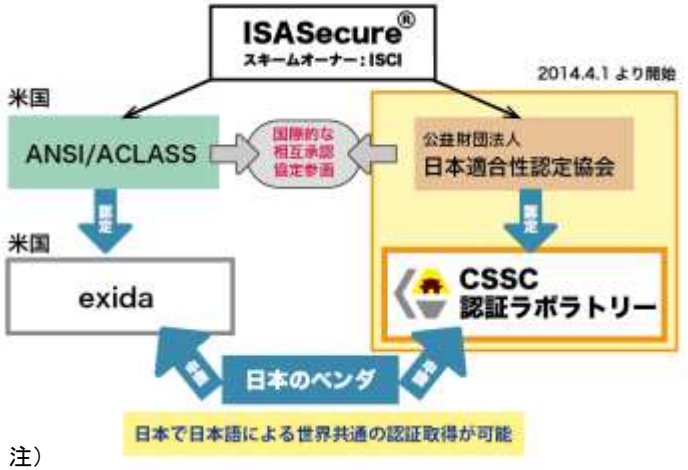


注）・ICS-CERT：Industrial Control System – Computer Emergency Response Team
（産業制御システム緊急対応チーム、米国はDHS（国土安全保障省）に設置

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

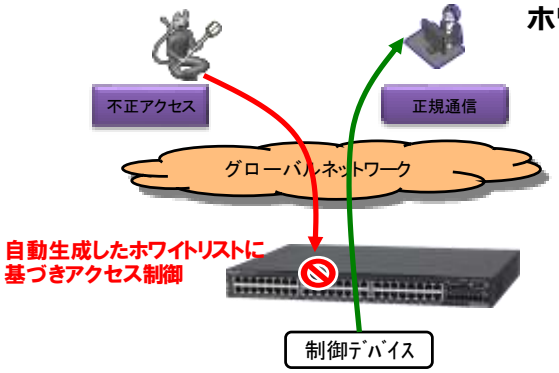
CSSC認証ラボラトリーの活動

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
- CSSC独自の検証項目策定
- ホワイトリストスイッチ
- ホワイトリスト（端末・サーバ向け）
- 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
- セキュアな制御システム構築ガイド(IEC62443)
- セキュアなログ集約技術
- ログの横断的分析技術
- 早期認識支援技術（CAeRS）
- 多層防御および多重防御技術
- CSSC独自の検証ツール

[テストベッド]

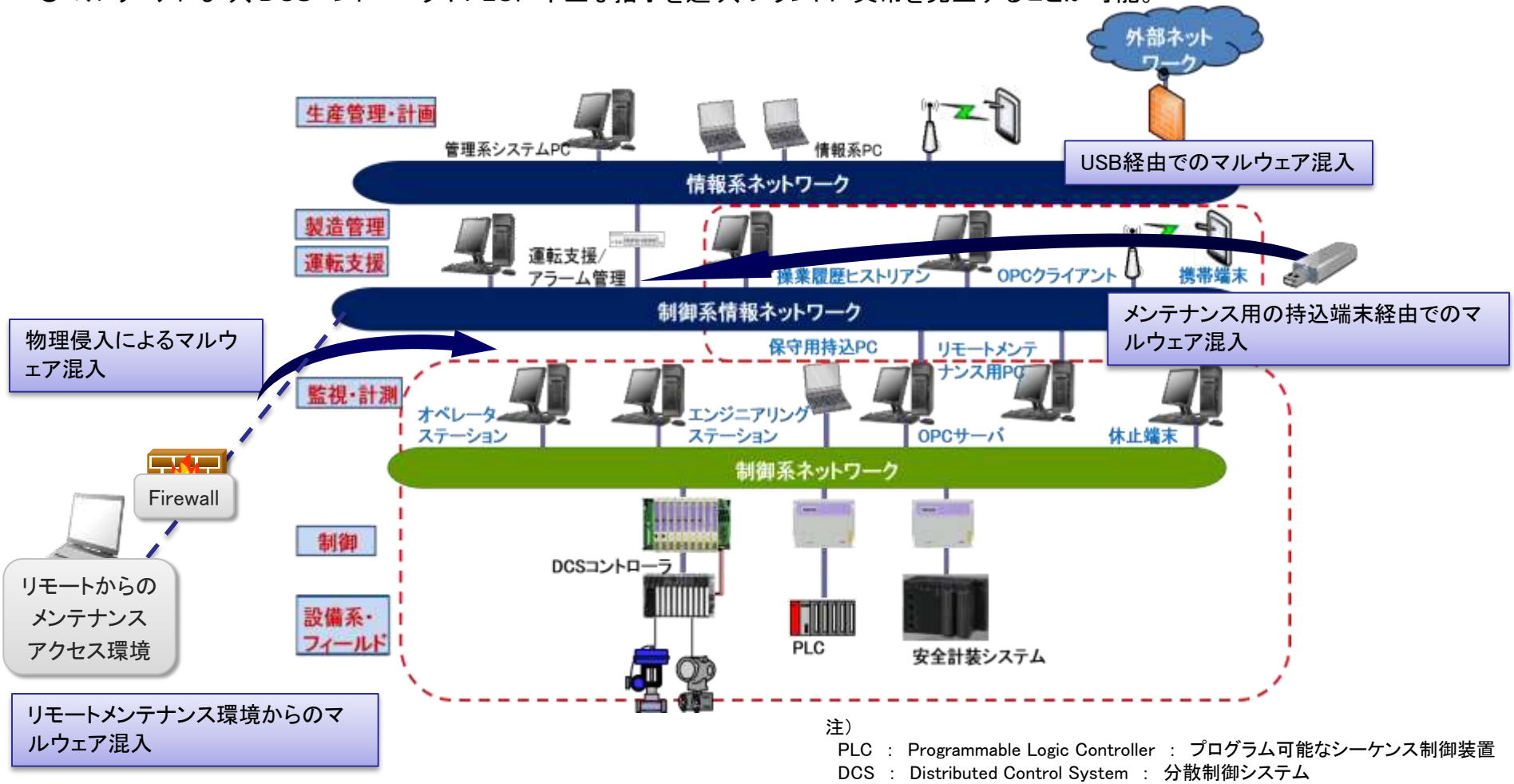
- セキュアな実験環境構築運用
- OPCによる相互接続環境の構築
- 対策機器の評価環境構築運用
- サイバーセキュリティ演習を中心とした普及啓発

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
30	32	2	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

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

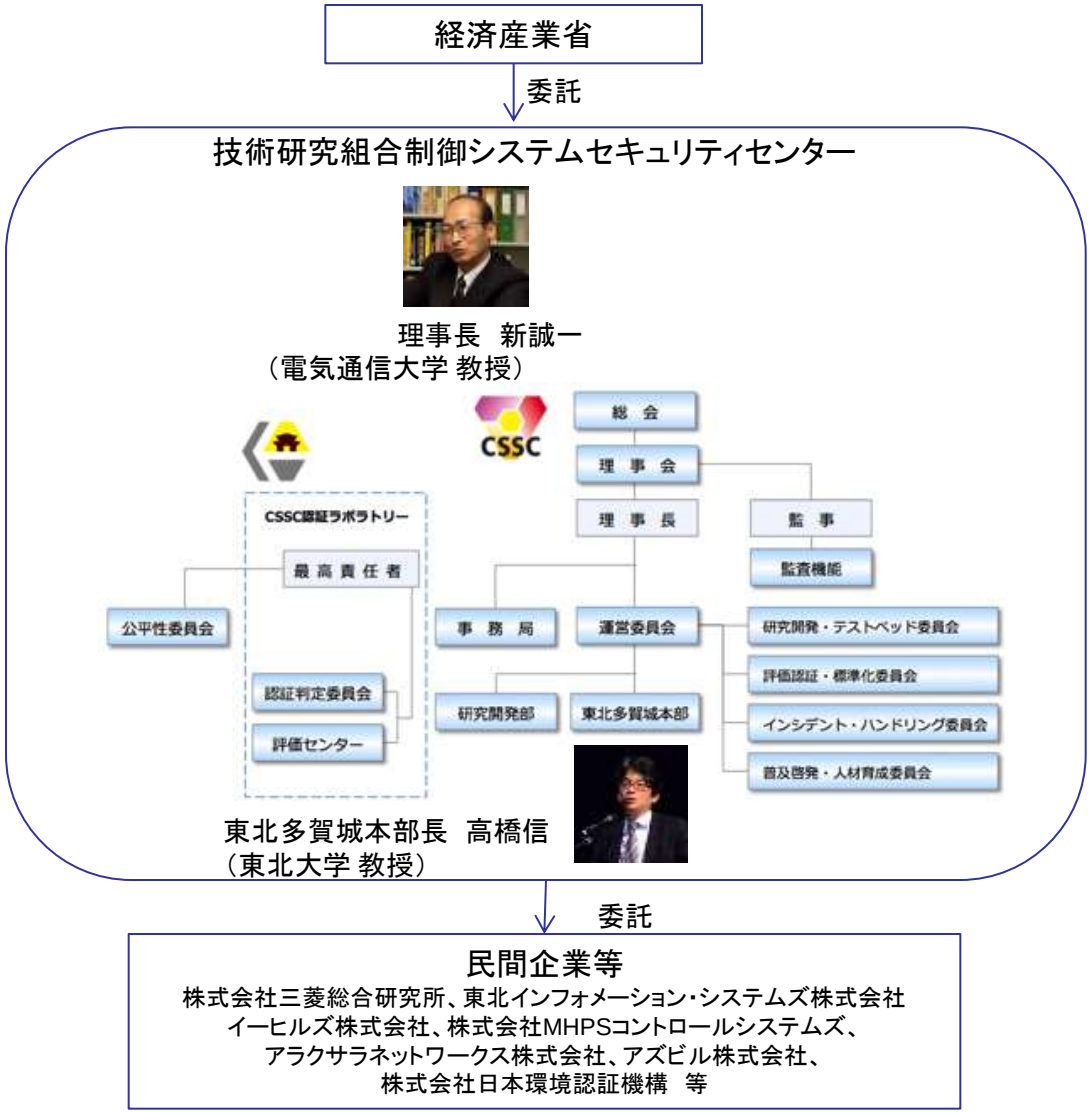
今後の研究開発の方向性

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

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。



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**	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	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	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）**

（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）。

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. 事前評価の結果

■評価小委員会コメント

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。

8. 事前評価の結果

■対処方針

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。