制御システムセキュリティ評価手法等研究開発事業
事前評価報告書

平成２４年５月

産業構造審議会産業技術分科会

評　価　小　委　員　会

（注）「制御システムセキュリティ評価手法等研究開発事業」は、事業名「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」で概算要求されている。

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20年10月31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21年3月31日改正）を定め、これに基づいて研究開発の評価を実施している。

今回の評価は、制御システムセキュリティ評価手法等研究開発事業の事前評価であり、評価に際しては、当該研究開発事業の新たな創設に当たっての妥当性について、省外の有識者から意見を収集した。

今般、当該研究開発事業に係る検討結果が事前評価報告書の原案として産業構造審議会産業技術分科会評価小委員会（小委員長：平澤　泠　東京大学名誉教授）に付議され、内容を審議し、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24年5月

産業構造審議会産業技術分科会評価小委員会

産業構造審議会産業技術分科会評価小委員会
委 員 名 簿

委員長	平澤　泠	東京大学　名誉教授
	池村　淑道	長浜バイオ大学 バイオサイエンス研究科研究科長・学部学部長 コンピュータバイオサイエンス学科　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
	太田　健一郎	横浜国立大学　特任教授
	菊池　純一	青山学院大学法学部長・大学院法学研究科長
	小林　直人	早稲田大学研究戦略センター　教授
	鈴木　　潤	政策研究大学院大学　教授
	中小路　久美代	株式会社ＳＲＡ先端技術研究所　所長
	森　　俊介	東京理科大学理工学部経営工学科　教授
	吉本　陽子	三菱ＵＦＪリサーチ＆コンサルティング株式会社 経済・社会政策部　主席研究員

（委員敬称略、五十音順）

事務局:経済産業省産業技術環境局技術評価室

制御システムセキュリティ評価手法等研究開発事業の評価
に当たり意見をいただいた外部有識者

越島　一郎　　名古屋工業大学大学院　ながれ領域　教授

佐藤　吉信　　東京海洋大学　海洋工学部　教授

関　　宏也　　東京工業大学　資源化学研究所　准教授

山下　善之　　東京農工大学　工学部　教授

（敬称略、五十音順）

事務局：経済産業省商務情報政策局情報セキュリティ政策室

制御システムセキュリティ評価手法等研究開発事業の評価に係る省内関係者

【事前評価時】

商務情報政策局情報セキュリティ政策室長　上村　昌博（事業担当室長）

産業技術環境局　産業技術政策課　技術評価室長　　岡本　繁樹

制御システムセキュリティ評価手法等研究開発事業事前評価
審 議 経 過

〇新規研究開発事業の創設の妥当性に対する意見の収集（平成２４年５月）

〇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）
・事前評価報告書(案)について

目　次

第1章　技術に関する施策及び新規研究開発事業の概要

1. 技術に関する施策の概要

本事業については、以下の政府等の方針に基づいて実施することとしている。

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、議長：官房長官）においては、世界最先端の「情報セキュリティ先進国」を目標として、重要インフラの基盤強化を実施することとしている。

また、今後の情報セキュリティ政策を検討するため経済産業省において開催した「サイバーセキュリティと経済研究会」（委員長：村井純慶應義塾大学教授）において、制御システムのセキュリティを確保する取組として、セキュリティ検証施設の構築、国際標準化、評価認証スキームの構築、インシデント対応体制の構築等について提言された。

制御システムのセキュリティの確保は、ITの基盤技術であり、東日本大震災からの復興基本方針（平成23年7月東日本大震災復興対策本部）における「新産業創出の拠点整備等」を行う上でも不可欠な要素である。

これらのセキュリティに関する研究開発については、平成23年9月に、牧野経済産業副大臣とチュー米国エネルギー省長官との間において、研究協力の深化について確認した。

加えて、本年4月の日米首脳会談においては、制御システムセキュリティに関する協力について発表した。

上記を踏まえ、米国の協力も得つつ、制御システムのセキュリティ確保を推進していくこで、東日本大震災からの復興にも役立てるとともに、我が国を世界最先端の「情報セキュリティ先進国」を目指す。

2. 新規研究開発事業の創設における妥当性等について

①事業の必要性及びアウトカムについて（研究開発の定量的目標、社会的課題への解決や国際競争力強化への対応等）

イ)事業の必要性（どのような社会的課題等があるのか？）

重要インフラ等に活用されている機器をコントロールする制御システムについては、従来、インターネット等の外部ネットワークと切り離されているとともに、独自の OS 等が利用されていることから、サイバー攻撃の影響は受けづらいと考えられてきた。

しかしながら、平成22年9月に発生したイランの核施設に対する「Stuxnet」を利用したサイバー攻撃を契機として、制御システムへのサイバー攻撃が認知されるようになった。

また、制御システムの外部ネットワークとの接続や利用されている OS 等の汎用化が進んでおり（※1）、従来の情報システムと同様にサイバー攻撃への脅威が増している。

こうした脅威は、スマートコミュニティの進展とともに、より一層増すこととなる。

こうした中、欧米においては、制御機器の納入に際し、セキュリティについて一定の証明、検査結果等の評価・認証を求める事例がある（※2）。

他方、我が国においては、セキュリティ検証施設がないことに加え、このような評価・認証を行う機関が存在しない（※3）ことから、海外での認証取得に数年かかるケースもあるなど輸出の障害となりつつある。

このため、本年度構築予定のセキュリティ検証施設を利用し、以下の制御システムのセキュリティ確保に向けた取組を推進し、制御システムのセキュリティ及び輸出の強化を目指す。

（1）制御システムの高セキュア化のための研究開発を行う。さらに、スマートコミュニティのように複数の制御システムが広域に連携したコミュニティレベルにおける高セキュア化のための研究開発を行う。

（2）また、制御システムのセキュリティに関する評価・認証手法に関する研究開発を行う。

（3）（1）及び（2）の研究開発から得られた成果を我が国の競争力強化に資する国際標準化を推進する。

（4）制御システムに対するサイバー攻撃が発生した際の攻撃手法の分析方法や対応方法の研究開発を実施する。

（5）我が国に評価・認証機関を設立するとともに、評価・認証機関同士の国際相互承認実現に向けた取組を推進する。

（6）なお、上記（1）～（5）の実施に必要となる人材育成プログラムについても合わせて研究開発を実施する。

※1 我が国の制御システムの約3割が外部ネットワークと接続。また、約7割がWindowsを利用（平成23年度経済産業省委託調査）

※2 約51%の日本の制御システムベンダが輸出に際し、評価・認証を求められた。（平成22年度経済産業省調査）

※3 米国においては、セキュリティ検証施設及び評価・認証機関の双方が存在。

ロ)アウトカム（目指している社会の姿）の具体的内容とその時期

昨今、サイバー攻撃の脅威は、スマートコミュニティの進展とともに高まることが予想され、この脅威に対応した制御システムの高セキュア化が必要である。

他方、我が国は制御システムにおいて強みをもっている（※4）が、欧米への輸出にあたっては、セキュリティに関する評価・認証を求められる事例がある。

本事業を今後5年間の期間で集中的に取り組むことで、ITの基盤である制御システムのセ

キュリティを強化するとともに、制御システムの輸出における障害を取り除く。
　合わせて、インシデント分析手法及び対応手法を確立し、サイバー攻撃が発生した際の対応支援につなげる。

※4　日本ベンダの世界シェアは PLC 約 25%、DCS 約 14%。

ハ)アウトカムが実現した場合の経済や競争力、問題解決に与える効果の程度

　昨今、我が国においても制御システムに対するサイバー攻撃が発生しており、生産活動が一時停止する事例もでてきている。加えて、現在、制御システムについては、国際的に確立された評価・認証手法が存在しないことから、制御システムの輸出先の求める基準ごとに評価・認証を受ける必要がある。
　このため、制御システムを高セキュア化する研究開発を行うとともに、サイバー攻撃発生時のインシデント分析手法及び対応手法を確立することで、サイバー攻撃に対し強固な体制を構築する。加えて、各国が統一した評価基準に基づく評価・認証を行うよう、国際標準化を推進するとともに、国際相互承認を実現することで、輸出の障害を取り除く。
　これにより、制御システムを引き続き我が国の強みとしていく。

ニ)アウトカムに至るまでに達成すべきいくつかの中間段階の目標（技術的成果等）の具体的内容とその時期

　制御システムの高セキュア化、セキュリティに関する評価・認証手法等の研究開発を進めるのに合わせて、ここから得られた成果を活用し、我が国の競争力強化に資する国際標準化を推進し、2014年度目途に成立を目指す。
　この上で、この国際標準を踏まえた更なる研究開発に取り組み2017年度を目途に、研究開発を終了させ、我が国に評価・認証機関の設立を目指す。合わせて、評価・認証機関同士の国際的な相互承認実現に向けた取組を推進する。
　また、高セキュアな制御システムを市場投入するとともに、国際連携によるインシデント分析・対応手法の確立につなげる。

② アウトカムに至るまでの戦略について

ｲ)アウトカムに至るまでの戦略（研究開発のみならず、知財管理の取扱、実証や国際標準化、性能や安全性基準の策定、規制緩和等を含む実用化に向けた取組）

本事業の実施にあたっては、評価・認証手法の研究開発を行うための設備環境が必要となる。この点については、平成23年度3次補正予算において、現在構築を進めているセキュリティ検証施設を有効に活用し、研究を進めることとする。

また、本事業の主目的である制御システムの高セキュア化や評価・認証手法、インシデント分析・対応手法等の研究開発にあたっては、ここから得られる成果を国際標準へ反映や認証機関同士の国際相互承認や国際連携の実現を目指すことを念頭におくことが重要である。

このため、既に制御システムに関するセキュリティの研究が進んでいる米国と連携することが必要である。この点については、独立行政法人産業技術総合研究所が米国アイダホ国立研究所と高セキュア化及び評価手法等の研究について協力関係を構築しているとともに、独立行政法人情報処理推進機構が米国の国際計測制御学会と標準についての連携を進めている。

なお、本事業の実施にあたっては、産学官が連携による制御システムセキュリティ分野におけるオールジャパンの体制で研究開発を想定している。

また、研究開発の成果である高セキュア化や評価・認証手法については、スマートコミュニティにおける各種制御システムへの反映やこれらのものによって設立される評価・認証機関に引き継がれることを想定している。

加えて、インシデント分析手法等については、インシデント対応機関において活用されることを想定している。

ﾛ)成果のユーザーの段階的イメージ・仮説 （技術開発成果の直接的受け手や社会的インパクトの実現までのカギとなるプレイヤーは誰か）

本事業の実施体制としては、我が国において制御システムセキュリティに関する研究の第一人者である新誠一電気通信大学教授をプロジェクトリーダーとし、高セキュア化及び評価手法等の研究開発として独立行政法人産業技術総合研究所、国際標準化の推進として独立行政法人情報処理推進機構が参加することを想定している。また、これらの研究を加速するとともに、研究開発成果の利用が期待できるアズビル株式会社、株式会社東芝、株式会社日立製作所、富士電機株式会社、三菱重工業株式会社、森ビル株式会社、横河電気株式会社等の制御システムのベンダ等を体制に加えることによる研究体制を想定している。

③次年度に予算要求する緊急性について

制御システムのセキュリティについては、米国が先行しており、既に独自の評価・認証手法等が開発されつつある。加えて、国際的には、2014 年度を目途に制御システムのセキュリティに関する国際標準の成立が進められている。

したがって、これらの国際的な流れに遅れをとらず、国際競争力を維持していくためにも早急に研究開発を実施し、我が国が国際競争上優位となるように評価・認証の枠組みを構築していく必要がある。

④国が実施する必要性について

ｲ)科学技術的価値の観点からみた卓越性、先導性（我が国が強みを持ち、世界に勝てる技術分野か、また、他の研究分野等への高い波及効果を含む）

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、前述のとおり、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。

ﾛ) 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省内又は他省庁の事業との重複について

重複する事業はない。

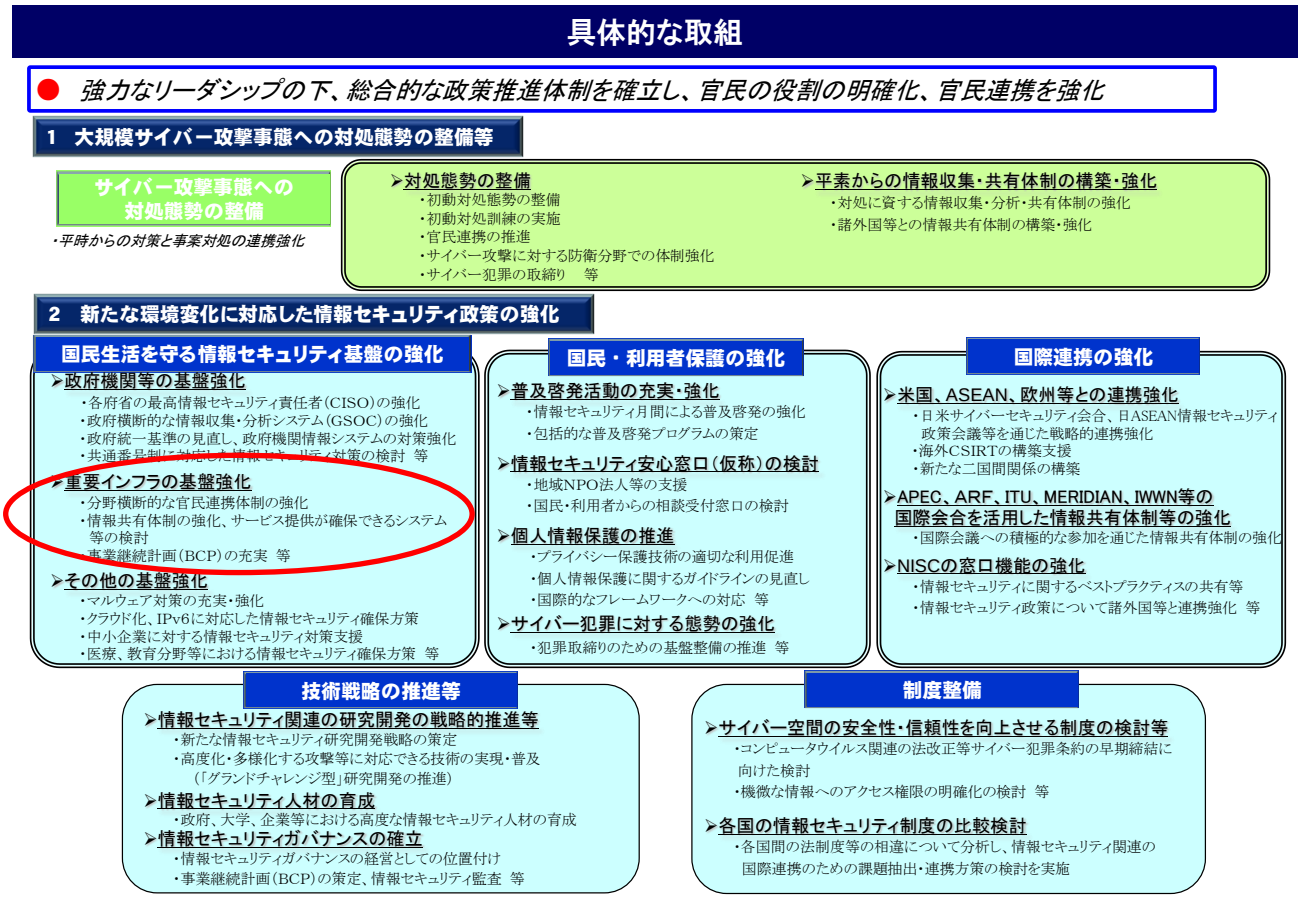
なお、本事業については、内閣官房情報セキュリティセンターを中心としたセキュリティに関する連携体制の下、経済産業省が実施すべき業務であることが、年次計画である「情報セキュリティ2012骨子（案）」等の各省協議の実施の上、位置付けられている。

3. 新規研究開発事業を位置付けた技術施策体系図等

〇国民を守る情報セキュリティ戦略

http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf

○国民を守る情報セキュリティ戦略の具体的な取組



(参考)

○サイバーセキュリティと経済 研究会
http://www.meti.go.jp/press/2011/08/20110805006/20110805006.html

○東日本大震災からの復興の基本方針
http://www.reconstruction.go.jp/topics/110811kaitei.pdf

○日米クリーンエネルギー協力ファクトシート(牧野経済産業副大臣と米国チューエネルギー省長官との確認事項)
http://www.meti.go.jp/press/2011/09/20110914004/20110914004-4.pdf

○日米イニシアティブ(日米首脳会談における発表)
http://www.mofa.go.jp/region/n-america/us/pmv1204/pdfs/Fact_Sheet_en.pdf

第2章　評価コメント

新規研究開発事業の創設の妥当性に対するコメント

①政策的位置付けの妥当性について

「情報セキュリティ先進国」を実現する上で、制御システムは最も重要なインフラの1つであり意義の深い事業であるとともに、国際動向とも一致している。

また、重要インフラの運用に不可欠な制御システムに対するITセキュリティ問題は、その発生原因の特定や対応には国際的協調が必要であり、民間で対応することは困難であることから、国全体の施策として意義が高い。

さらに、制御システムのセキュリティ確保に関する研究開発を推進することは、我が国として、安全で安定した社会生活及び生産活動、成果を反映した制御システムを海外にも流通させるために、時宜を得たものである。

なお、東日本大震災からの復興にどの程度貢献するのかが不明確であり、復興に貢献するためのより明確な筋道を示す必要があると考える。

また、これまで培ってきた「安全」と本事業で高める「制御システムセキュリティ」の同時達成によって、世界最先端の「情報セキュリティ先進国」となると考えられる。

〇肯定的意見

・これまでの政府等の方針に沿ったものであり、国策として意義は高い。また、国際的動向とも一致している。

・「情報セキュリティ先進国」を実現する上で、制御システムは最も重要なインフラの1つであり、意義の深い事業であると考える。国際標準化の構築の動きが進んでいることを考えると、乗り遅れてはならない。

・重要インフラの運用に不可欠な制御システムに対する IT セキュリティ問題は、その発生予測の困難性と、発生時には同時多発性を有することに特徴がある。更に、その発生原因の特定や対応には国際的協調がなければならないことから、民間で対応することは困難な問題である。この視点から、国全体の施策として意義が高い。

・情報セキュリティに関する施策として、制御システムのセキュリティ確保に関する研究開発を推進することは、我が国として、安全で安定した社会生活及び産業活動を行うために、さらには、成果を反映した制御システムを海外にも流通させるために、非常に時宜を得たものと評価できる。

国際的動向としては、国際電気標準会議(IEC)が、現在、産業用制御システムのセキュリティに関する規格 IEC 62443 を策定中であり、この動向とも一致していると評価できる。

〇問題点・改善すべき点

・セキュリティ検証設備を東北地方に構築するとしても、その波及効果がわかりづらく、東日本大震災から

の復興にどの程度貢献するのか不明である。復興に貢献するためのより明確な道筋を示す必要があると考える。

・「新産業創出の拠点整備等」を掲げている。「セキュリティ検証施設の構築」は拠点整備となることは理解できるものの、「国際標準化、評価認証スキームの構築」によって創出される「新産業」の具体的イメージが付かない。

制御システムがエネルギーや資源の最大活用を可能とし、「使用するモノ」への投資ではなく「使用するプロセス」への投資を通した「スマートな復興」＝「スマートシティーの創造プロセス」こそが、総体として「新産業」であり、他国が真似のできないオリジナリティとなることを示す必要がある。

これまで培ってきた「安全」と本事業で高める「制御システムセキュリティ」の同時達成によって、初めて世界最先端の「安心できる情報セキュリティ先進国」となると考える。

②事業の目的及び実施によるアウトプット、アウトカムの妥当性について

事業の目的は明確かつ妥当である。アウトカムに至るまでの戦略や中間段階の目標も適切に設定されており、アウトカムの設定は妥当である。

また、制御システムのセキュリティを強化することは、国内のセキュリティ環境の向上、我が国製品の輸出のための競争力の向上のいずれにも寄与でき、スマートコミュニティを実現するための重要な技術の1つであると考えられ、この観点からも妥当である。

さらに、この分野における人材の育成は、セキュリティレベルを将来にわたって維持する上で不可欠な取組であると考える。

なお、事業目的として、「予防」並びに「早期検知」を加えるべきである。アウトカムには、サイバー攻撃に対応する機関及び人材育成プログラムによって輩出される人材も示すべきである。アウトカムに至る戦略には、実施体制に制御システムユーザ企業の関与や制御システムセキュリティ分野に研究者を引き付ける施策の実施が必要である。加えて、米国だけではなく、EUの研究機関との連携も必要である。

また、セキュリティの問題が制御システムを介在して安全の問題に関わる可能性がある場合、ハザード分析及びリスクアセスメント手法の研究開発も必要である。

さらに、制御システムセキュリティ分野のみを考えるのではなく、より広い情報セキュリティ分野での位置付けを明確にしながら戦略をたてることが重要である。

〇肯定的意見

・事業目的:

（1）－（6）の取組みは妥当であると考える。

アウトカム:

「評価・認証機関の設立」は、事業目的の（2）、（3）、（5）に沿ったアウトカムであると考える。

アウトカムに至るまでの戦略:

新教授を中心とした実施体制でスタートすることは妥当であると考える。

・事業として、（1）制御システムの高セキュア化の研究開発など、（2）制御システムのセキュリティの評価・認証手法に関する研究開発、（3）成果の国際標準化の推進、（4）制御システムへのサイバー攻撃対策の研究開発、（5）評価・認証機関の設立と国際相互承認の推進、（6）上記の目的を達成するための人材育成プログラムの研究開発、を実施することを企図しているが、いずれも妥当であると評価できる。

上述の成果により、国内の情報セキュリティ環境の向上、我国の製品の輸出のための競争力の向上のいずれにも寄与できるとする事には十分な妥当性があると評価できる。

・事業の目的は明確かつ妥当である。アウトカムに至るまでの戦略や中間段階の目標も適切に設定されており、アウトカムの設定は妥当である。

・制御システムのセキュリティを強化することは、世界的な流れであり、制御システムの輸出ビジネスの競争力を維持することは、事業目的として妥当であると考える。

また、来たるべきスマートコミュニティを実現するための最重要な技術の1つであると考えられ、この

観点からも妥当な目的だと考える。

また、この分野における人材の育成は、セキュリティレベルを将来にわたって維持する上で不可欠な取り組みであると考える。

〇問題点・改善すべき点

・事業目的:

（4）に示された発生してからの対応に加えて、「予防」並びに「早期察知」を加えるべきであると考える。

（5）のみ「機関を設立」を目的としており、他が研究開発に関係することと比べると違和感が在る。

アウトカム:

スマートコミュニティを議論する場合は、モバイル機器や通信も含まれることから、スマートコミュニティに必要となるセキュリティと制御システムのセキュリティを同列で議論することは出来ない。

（4）のサイバー攻撃に対応する「機関」をアウトカムとして考えるべきである。

（6）の人材育成プログラムによって輩出された人材も重要なアウトカムとして示すべきであり、これらの人材を具体的に遇する「仕掛」もアウトカムとして用意するべきである。

アウトカムに至るまでの戦略:

新教授を中心とした本事業の実施体制に、制御システムのユーザ企業（現、森ビル株式会社のみ）の関与が望まれる。更に、ほとんど研究されていない制御システムセキュリティ分野に、研究者を引き付ける施策の実施が必要である。

Stuxnet の発見者はベラルーシの VirusBlokAda 社とされている。早期警戒のためには、米国だけでなく EU の研究機関とも連携することが必要であると考える。

・特に、セキュリティの問題が制御システムを介在して安全の問題に関わる可能性がある場合、それがどのように関わり想定外の最悪の結果を招くかなどを系統的に同定・分析・評価するための、ハザード分析及びリスクアセスメント手法の研究開発も必要となろう。

・技術革新の著しい分野であるため、事業終了後も継続的な研究開発を維持する体制の整備が重要である。

・スマートコミュニティの実態がまだはっきりしない現時点では、まずは、産業界における生産活動が安全に行われることを最重要課題とするべきである。スマートコミュニティに関しては、長期的な展望をもって取り組むべきだと考える。制御システムセキュリティ分野のみを考えるのではなく、より広い情報セキュリティ分野での位置づけを明確にしながら戦略をたてることが重要である。

③事業の優先性について

制御システムをターゲットとした標的型マルウエアは、今後ますます出現頻度が上がるものと考えられ、国際標準の制定や相互承認に積極的に関与するにも、独自の研究成果が不可欠であり、緊急度は大変高いと考える。

また、米国の当該分野における先行状況及び国際的動向に鑑み、我国が本研究開発を推進することは、早過ぎもせず、遅すぎもせず、時宜を得たタイミングであると評価できる。

なお、5年間の集中的な取組のあとの事業継続のことも考えることが必要である。

〇肯定的意見

・Stuxnetの亜種が発見されている事（Stuxnet発見から約1年4カ月）を考えると、制御システムをターゲットとした標的型マルウエアは、今後ますます出現頻度が上がるものと考えられる。また、国際標準の制定や相互承認に積極的に関与するにも、独自の研究成果が不可欠であり、緊急度は大変高いと考える。
・米国の当該分野における先行状況及び国際的動向に鑑み、我国が本研究開発を推進することは、早過ぎもせず、遅すぎもせず、時宜を得たタイミングであると評価できる。
・国際的な流れに後れを取らないためには、緊急に枠組みを構築する必要がある。
・2014年を目途に国際標準が成立される動きがあるなか、早急に事業を開始する必要があると考える。

〇問題点・改善すべき点

・セキュリティはそのレベルを恒久的に維持すべきものであるから、5年間の集中的な取り組みのあとの事業継続のことも考えることが必要である。

④国が実施することの必要性について

制御システム全体をカバーするセキュリティ基盤技術はボトムラインとしてしたがうべき規格等を定め、それを底上げするための技術であって、民間企業が競争優位のために開発する技術ではないことから国の関与が必要である。

また、米国における制御システムのセキュリティに関する技術の研究開発が国立研究所を中心として実施されているように、先ずは公的機関の国際的連携が必要である。

加えて、サイバー攻撃等は常に進化していく可能性があり、これに対応していくためには、長期的計画・戦略に基づく対応組織の運営が必要となり、この観点からも国が強く関与する必要性がある。

さらに、スマートコミュニティを視野にいれるとステークホルダーが広範囲におよぶことなどを考えると、国が実施することが必要である。

なお、「国際競争上優位」とするには、民間企業側も自社の優位性を担保するために、本事業を起点として独自の研究を推進するべきである。そのための、施策も盛り込むべきである。

また、国が実施するからには、できるだけ広い産業分野をカバーした取り組みが期待される。

〇肯定的意見

・米国防総省が2011年7月に発表した「サイバー戦略」では、サイバー空間を陸、海、空、宇宙に次ぐ第5の新たな「戦場」と定義している。したがって、米国アイダホ国立研究所との連携はこの「戦場」に関与することを意味し、どの様な形であれ国が前面に立つ必要がある。

　また、制御システム全体をカバーするセキュリティ基盤技術は、ボトムラインとして従うべき規格等を定め、それを底上げするための技術であって、民間企業が競争優位のために開発する技術ではないことから、国としての関与が必要である。

・米国における制御システムのセキュリティに関する技術の研究開発が国立研究所を中心として実施されているように、先ずは公的機関の国際的連携が必要である。

　また、サイバー攻撃等は常に進化していく可能性があり、これに対応していくためには、長期的計画・戦略に基づく対応組織の運営が必要となり、この観点からも国が強く関与する必要性がある。

・今後の基盤となる技術分野であるにもかかわらず、未だ世界的に確立されていない分野であり、先行する米国と協力しながら研究や相互承認を進めるためにも、国が実施する必要性は高い。

・制御システムのセキュリティは直接的に利益に結びつきにくいので民間で取り組むインセンティブが得られにくい、スマートコミュニティを視野にいれるとステークホルダーが広範囲におよぶことなどを考えると、国が実施することが必要である。

〇問題点・改善すべき点

・「国際競争上優位」とするには、民間企業側も自社の優位性を担保するために、本事業を起点として独自の研究を推進するべきである。そのための、施策も盛り込むべきである。

・国が実施するからには、できるだけ広い産業分野をカバーした取り組みが期待される。

⑤省内又は他省庁の事業との重複について

省内又は他省庁の事業と重複する事業はないとすることは妥当であると評価できる。
なお、サイバー空間で、「米国と研究を実施」する場合、「攻撃的」要素も当然含まれることとなる。この対応を、他省庁と擦り合わせる必要性を明記すべきである。
また、制御システム単体ではなく、より広範囲の情報システムの中で制御システムを捉え、セキュリティを考えるべきである。その意味で他省庁との連携があってもよいのではないか。

〇肯定的意見
・省内又は他省庁の事業と重複する事業はないとする事は妥当であると評価できる。

〇問題点・改善すべき点
・「戦場」と定義したサイバー空間で、「米国と研究を実施」する場合、「攻撃的」要素も当然含まれることとなる。この対応を、他省庁と擦り合わせる必要性を明記すべきである。
国として、「重複する事業はない」のみならず、「専門とする省庁が存在しない」ことが問題である。
・制御システム単体ではなく、より広範囲の情報システムの中で制御システムを捉え、セキュリティを考えるべきである。その意味で他省庁との連携があってもよいのではないか。

第3章　評価小委員会のコメント及びコメントに対する対処方針

本研究開発事業に対する評価小委員会のコメント及びコメントに対する推進課の対象方針は、以下のとおり。

【制御システムセキュリティ評価手法等研究開発事業】

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。

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。

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（復興特会）

商務情報政策局　情報セキュリティ政策室
03-3501-1253

事業の内容

事業の概要・目的

○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を整備します。

○エネルギー等のインフラを制御するITシステムの安全性確保に対する関心は、急速に高まっています。被災地域においても、震災の教訓を生かし、災害等に強く、エネルギー効率の高いインフラの整備を進めていく上でITシステムの安全性確保は、極めて重要な課題です。

○国際的にも、エネルギー等のインフラ市場はアジアを中心に更なる拡大が見込まれる成長分野であり、成長するアジアの活力を、被災地復興に活かしていく上で、安全性検証・普及啓発の国際拠点整備が期待されます。

○平成２５年度は、拠点整備へ向け、人材育成プログラムの開発や、システム安全性評価・認証手法の開発、国際シンポジウムの開催等を実施します。

条件（対象者、対象行為、補助率等）

国 → 委託 → 民間事業者等

事業イメージ