SIP（戦略的イノベーション創造プログラム）
重要インフラ等におけるサイバーセキュリティの確保
研究開発計画（案）

平成 27 年 9 月

内閣府

政策統括官（科学技術・イノベーション担当）

研究開発計画の概要

1．意義・目標等

2020 年東京オリンピック・パラリンピック競技大会を迎える我が国にとって、サイバー攻撃の脅威は切実な問題であり、強固なサイバーセキュリティの確保による世界で最も安心・安全な社会基盤の確立が必達の課題である。

本研究開発では、重要インフラ等[1]におけるサイバーセキュリティを確保するために、重要インフラサービスの安定運用を担う制御ネットワークおよび制御ネットワークを構成する制御・通信機器（以下「制御・通信機器」という。）のサイバー攻撃対策として、制御・通信機器のセキュリティ確認[2]技術、制御・通信機器および制御ネットワークの動作監視・解析技術と防御技術を研究開発する。その成果を、2020 年東京オリンピック・パラリンピック競技大会をターゲットに、実証実験等を通して、通信・放送、エネルギー、交通などのインフラシステムに適用できることを確認する。また、今後普及・拡大が見込まれる IoT システムのセキュリティ確保に向けて前記技術を拡張するとともに、技術導入を支援する認証制度の設計、分野を超えた運用のための共通プラットフォームの実現、セキュリティ人材育成に取り組む。

2．研究内容

主な研究開発項目を以下に記す。

（a）制御・通信機器と制御ネットワークのセキュリティ対策技術の研究開発

（b）社会実装に向けた共通プラットフォームの実現とセキュリティ人材育成

3．実施体制

後藤厚宏がプログラムディレクター（以下「PD」という。）として研究開発計画の策定や推進を担う。PD が議長、内閣府が事務局を務め、関係省庁、技術や制度の専門家、重要インフラ事業者の有識者で構成する推進委員会が総合調整を行う。国立研究開発法人新エネルギー・産業技術総合開発機構（以下「NEDO」という。）交付金を活用して公募を実施する。同法人内に選考委員会を設置し、適切な評価のうえ、推進委員会と連携をしながら研究開発計画に基づき、最適な研究課題を状況に応じて選定し、大学、企業等によって構成される研究チームを構成し、研究開発を実施する。同法人のマネジメントにより、各課題の進捗を管理する。

4．知財管理

知財委員会を NEDO に置き、各受託機関で出願される知的財産の動向を把握・管理し、産業利用する際の利便性向上につながるよう、各受託機関と調整を行う。

---

[1]「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（改訂版）」が特定している 13 分野に代表される重要な社会基盤システム。

[2] セキュリティ確認とは、機器やソフトウェアの真正性、完全性を確かめること。

5．評価

ガバニングボードによる毎年度末の評価の前に、研究主体による自己点検及び PD による自己点検を実施する。

6．出口戦略

出口指向の研究推進として、重要インフラ等におけるサイバーセキュリティ確保の研究開発を推進し、研究開発段階から社会実装を最短で実現する研究開発体制と仕組みを構築する。当初の社会実装として 2020 年東京オリンピック・パラリンピック競技大会設備を支える主要な重要インフラ等に導入し実証する。引き続き、高度化するサイバー攻撃に対抗できるサイバーセキュリティ確保の研究開発を継続するとともに、その成果普及に際しては、利用される分野に応じた標準化・規格化・評価手法およびそれらに基づく認証制度の設計を進め、分野に応じた規制・基準等による導入促進策に貢献する。

1．意義・目標等

(1) 背景・国内外の状況

国民生活及び経済活動は、様々な社会インフラによって支えられており、その機能、サービス等を実現するために多数の情報システムが運用されている。特に、重要インフラは、サービスが停止又は低下した場合に多大なる影響を及ぼしかねない。政府においても「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」を策定し、ＩＴ障害の発生を可能な限り減らすとともにＩＴ障害発生時の迅速な復旧を図ることで重要インフラを防護することを目的として、諸施策を実施しているところである。

しかし近年、重要インフラへのサイバー攻撃の脅威が現実のものとなり、その対策は全世界的に急務である。ある調査によれば、サイバー犯罪による世界経済の損失は年間 53 兆円、インターネットによる価値創造の 15%から 20%に相当する[3]。特に、2020 年東京オリンピック・パラリンピック競技大会を迎える我が国にとっては、強固なサイバーセキュリティの確保による世界で最も安心・安全な社会基盤の確立が必達の課題である。

また、IoT(Internet of Things)を活用して経済の活力を向上させようとする時代を迎え、これまでにない多種多様な機器等がネットワークで接続されると共に、今後は重要インフラにおいても IoT の活用が進展することが予想される。このような状況下において、新しいサイバー攻撃の脅威が生まれることや攻撃の影響が広範にわたることが懸念されるため、重要インフラ事業者はそれぞれに対策を講じているが、個々の重要インフラ事業者が単独でセキュリティ対策を行うだけでは脅威への対応に限界がある。

一方、現在、我が国のサイバーセキュリティ対策に関する製品等は海外事業者に大きく依存しているが、重要インフラで取り扱われる情報の重要性を鑑み国産技術のレベルを高め活用していく必要もある。加えて、重要インフラで活用が進む機器においても海外依存度は高まっており、それらのセキュリティ認証制度も端緒についたばかりである。さらには、セキュリティ人材も不足している状況である。

我が国の重要インフラ等のサイバーセキュリティ確保に向けた取り組みは、安全な社会基盤作りと産業活性化の両面で極めて重要であり、国の最重要施策として推進する必要がある。

(2) 意義・政策的な重要性

｜ 重要インフラ等へのサイバー攻撃対策

重要インフラ等にサイバー攻撃が行われると、情報通信の麻痺や交通機関の混乱など、社会に重大な損害をもたらす恐れがある。図表 1 に、これまで発生した重要インフラ等への具体的なサイバー攻撃事例を示す。

従前から重要インフラ等へのサイバー攻撃は懸念されており、内閣官房内閣サイバーセキュ

[3] Center for Strategic and International Studies, “Net Losses: Estimating the Global Cost of Cybercrime”, 2014 年 6 月

リティセンター（NISC）を中心とした各府省庁の取り組みにより、重要インフラ事業者は一義的には自らの責任においてサイバーセキュリティ対策に取り組み、重要インフラ事業者、または重要インフラ分野間の情報共有の仕組みとしてセプター等様々な情共有体制も整備されているが、年々高度化するサイバー攻撃の脅威へ対抗するためには対策技術の抜本的な見直しと継続的な強化が欠かせない。

図表１　重要インフラ等へのサイバー攻撃事例

	発生国	インシデント	被害
電力	ブラジル	製鉄所内発電所の制御システムのワーム感染	発電所の数ヶ月停止
ガス	米国	制御システムのマルウェア感染	制御システムへアクセスする資格情報等の漏えい
鉄道	米国	内部システムのマルウェア蔓延	鉄道運行の 6 時間停止
石油化学	サウジアラビア	制御システムの PC30,000 台がマルウェア感染。	内部ネットワークの 1 週間以上停止、PC データの全削除

- **制御ネットワークの安全な運用がインフラサービスの鍵**

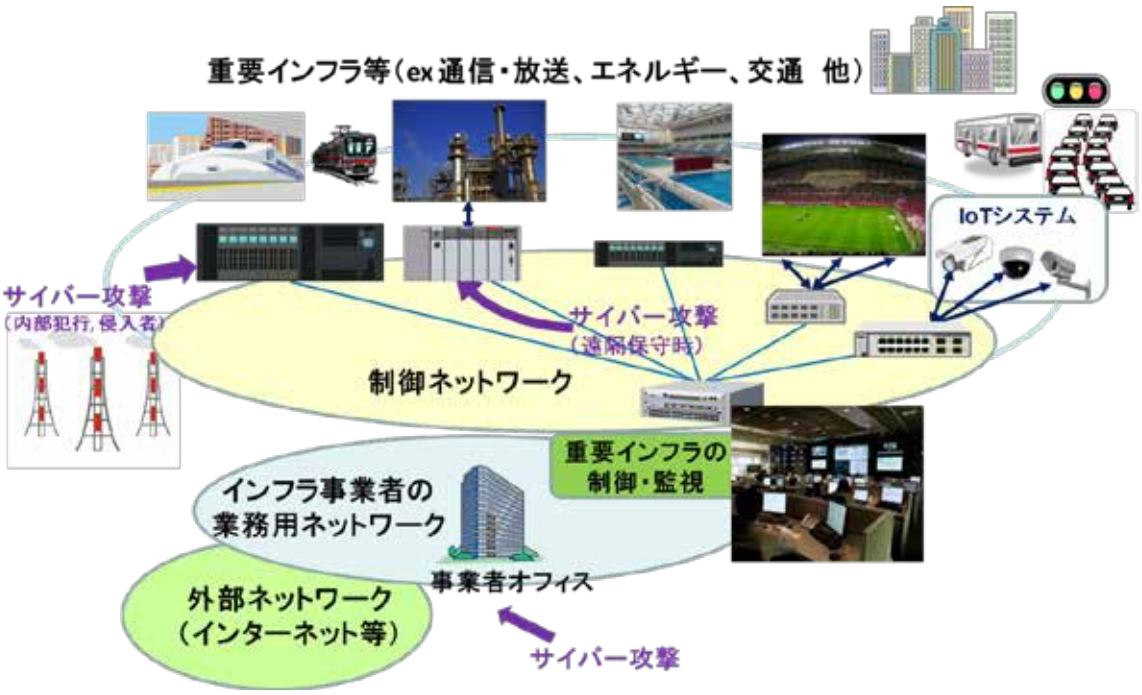
重要インフラにおいては、設備ごとの監視・制御に留まらず、広域に散在する各設備がネットワークにより接続され重要インフラ全体として監視・制御されている（図表２）。また、設備を長期に運用するためのシステムソフトウェアの保守や更新もネットワークが利用されている。この監視・制御・保守のためのネットワークを、以降、「制御ネットワーク」と呼ぶ。制御ネットワークを構成する制御・通信機器の形態は多様であり、企業の業務ネットワークと同様のルータやスイッチ、セキュリティアプライアンス、サーバー、端末等に加え、PLC 等[4]の制御機器や設備に組み込まれる場合もある。また、インフラによっては、監視・制御・保守の目的毎に制御ネットワークを構成する場合もある。このように重要インフラの監視・制御・保守を担う制御ネットワークのセキュリティがインフラサービスの安定した提供を大きく左右することは明らかである。

- **オープン化が必然な制御ネットワークをサイバー攻撃から守る**

一方、重要インフラサービス事業者は、事業者の業務用ネットワークをインターネットに接続して利用者に様々な付加サービス提供することで競争力を高めるようになってきている。具体的な付加サービスとしては、運行・運転状況通知サービスや座席予約サービスなどがある。さらに、重要インフラの制御ネットワークは、限定的であっても事業者の業務ネットワークに接続されており、システムソフトウェアの遠隔更新作業や USB 等を用いたオンサイトのメンテナンスを含めると、もはや制御ネットワークも完全な閉域環境とはなりえず、事業者の業務用ネ

[4] PLC Programmable Logic Controller. 機械制御等に用いられる小型コンピュータ。

ットワークと同じく、サイバー攻撃の脅威は高まっている。また、内部犯行や侵入者による制御ネットワークへのサイバー攻撃の脅威にも備える必要がある。したがって、重要インフラ事業者が保有する設備だけを様々なリスクから保護するだけでは不十分であり、この重要インフラの制御ネットワークを構成する制御・通信機器も含めてサイバー攻撃の対象になるとみなして保護すべきである。



図表２　重要インフラとサイバーセキュリティ

- **IoT システムの普及拡大に先行したセキュリティ確保**

さらに自動走行などの将来型交通システムや広域医療システムとして加速する IoT システムの普及、電力自由化など環境の変化にともない、重要インフラサービスや社会サービスの高度化・効率化・多様化に向けて複数の事業者が他の社会インフラサービスと相互連携する必要性が高まってくることで、重要インフラの制御ネットワークが相互接続される状況になっている。このため、将来にわたって、重要インフラの制御ネットワークが何等かのオープン性を有するという前提のもとで、重要インフラの設備及び制御・通信機器を健全な状態に保つことが、各重要インフラ分野のサイバーセキュリティの確保において共通的に重要な課題である。特に重要インフラ等のサービスにおいて普及・拡大が見込まれる IoT システムのセキュリティ確保については、その普及に先んじた対策が必要である。

- **システムとしてのサイバー攻撃対策**

中間とりまとめが報告された第 5 期科学技術基本計画では、「未来の産業創造と社会変革に向けた取組」において、個別製品や要素技術のみならず、個々の機能を組み合わせ、一つの統合体として機能させる「システム化」によって新たな価値が生み出されるとの考えが示されている。重要インフラ等のサービスを支える設備や制御ネットワークも「システム化」されていると

認識できるが、当該システムのセキュリティ機能を導入時だけでなく運用中も確認できることは新たな価値に相当すると考えられる。したがって、重要インフラ等の設備や制御ネットワーク、その制御・通信機器からなるシステム全体が健全な状態にあることを監視・解析することが重要である。これらの環境整備は 2020 年オリンピック・パラリンピック東京大会や事業環境、ＩＴ環境の変化を見据え、一日も早く実現されることが望ましく、国として支援することが重要である。

ｌ　サイバーセキュリティ強化を梃に国際競争力強化

本研究開発の成果を適用することにより重要インフラ等を構成する様々な設備・機器等がシステムとしてセキュリティが向上することで、国産機器・システムの市場競争力が高まるばかりでなく、それを梃子にしてインフラシステム全体の付加価値を高められる。これにより、IoT による新たな事業分野を含め、産業全体の国際競争力の向上も狙うことができる。

以上により、本研究開発は、我が国の重要インフラのサイバーセキュリティ確保に貢献すると共に、国産の機器やシステムの市場競争力を高め、さらにはインフラ産業の国際競争力向上も狙うことが出来る極めて重要なものである。

(3) 目標・狙い

①社会的な目標

- 日々、大規模化、巧妙化していくサイバー攻撃への耐性を根本から高め、世界で最も安全な社会基盤を確立する。
  - Ø 社会基盤の中でも特に国民生活の根幹を支える重要インフラ等については、サイバー攻撃を受けた場合の影響が広範にわたることから、重要インフラ事業者が単独で実施する対策だけに頼らず、重要インフラ全体の防護能力の維持・向上にも資することを目標とする。
  - Ø IoT 機器や IoT システムが社会に浸透する前にセキュリティ対策を先行させ、安全な IoT 機器や IoT システムを利用するビジネス等の普及に貢献する
- 2020 年東京オリンピック・パラリンピック競技大会を支え、世界に向けて日本の重要インフラシステムの優位性をアピールする
  - Ø ロンドンオリンピックでは電力インフラと公式 Web サイトがサイバー攻撃の標的にされたにも関わらず、その影響を受けることなく大会を終了したが、IT 環境の変化やサイバー攻撃の巧妙化が想定される 2020 年においても、重要インフラ等を防護し大会の運営に支障をきたさない実績を積み上げる。

②産業面の目標

- 重要インフラ等へのサイバー攻撃による損失を低減する「守り」のセキュリティと、インフラ産業の付加価値として産業競争力強化[5]並びにインフラシステムの輸出額増につなげる「攻め」のセキュリティの両軸を狙う。

[5] 第６回経協インフラ戦略会議における 2020 年目標は約 30 兆円

- **2020 年東京オリンピック・パラリンピック競技大会の運営に関わる主要な重要インフラサービスの設備から実証を始め、国内の他の重要インフラ等への展開、政府系システムへの展開などを図る。**
  - Ø **日本国内で重要インフラにおける運用実績を積み、重要インフラに関わる設備と合わせてシステムとして海外への展開を図る。**
- **セキュリティ強化された機器製品（大規模システムや重要インフラのセキュリティを支える製品等に重点を置く）の自給率向上と海外展開を狙う。**
  - Ø **サイバーセキュリティ対策に関する製品等は海外事業者に大きく依存しているが、重要インフラ保護の観点から国内技術力を高め活用していく必要があり、先導的に技術開発を進め、その技術の標準化もあわせて海外に展開することにより市場の競争優位性を備えて、先行的に開発した技術を競争力として海外展開を図る。**
  - Ø **技術の標準化と合わせてセキュリティ技術導入時の認証制度についても海外展開を図る。**
- **民生機器分野でも今後益々の普及が予測される IoT システムのセキュリティを確保することにより、安全な IoT システムによる新たなビジネス拡大を加速させる。**
  - Ø **重要インフラ等の小型端末、センサー網、防犯カメラ網などの IoT 機器や IoT システムに加え、社会生活で重要な役割を果たしている自動車など、ネットワークに接続することで活用が見込まれる様々なシステムを安全に保つための技術開発に、本研究開発成果を提供し、IoT を活用したビジネスの拡大に寄与することを目指す。**
  - Ø **セキュリティ対策の導入は、平常時の運用コストを多少なりとも上昇させるため、事業者にとっては優先度が下がってしまうことがしばしばあるが、対策の弱い企業ほど攻撃される可能が高く、その観点から、事後のセキュリティ対処の影響が社会的に大きい分野では、自主的な対策導入ではなく、社会的責任の下に、対策導入が適切にマネージできることを目指す。**

③技術的目標

- **機器の製造に組み込まれたセキュリティ機能により、システム構築時とシステム運用時に制御・通信機器のセキュリティ確認[6]ができ、その確認結果を理論的、又は実用的に担保できる技術を世界に先んじて実現**
  - Ø **暗号など理論に基づき安全性が担保される技術を活用することに加え、耐タンパーモジュールなど実用的な安全性を確保できる構成部品を用いて、最大限の安全性を確保するとともに、重要インフラ等において長期間の運用にも耐えられる実用性を目指す。**
  - Ø **上記の技術の適用が難しい超小型センサー等の IoT 機器（小型 IoT 機器）に向けて、複数の小型 IoT 機器を収容してネットワーク接続するサブシステムを想定して実用的なセキュリティ確認に基づいたセキュリティ対策ができる制御・通信機器技術を目指す。**
- **システムの運用時に、システムとして健全な状態であることを制御・通信機器および制御ネットワークの動作監視・解析から確認できる技術の実現**

[6] セキュリティ確認とは、機器やソフトウェアの真正性、完全性を確かめること。

- Ø 将来にわたり高速大容量化するネットワークトラヒックに追従できる先進的なリアルタイムのログ収集技術、および将来の重要インフラ等において普及が予想される革新的な監視技術を目指す。
- Ø それぞれの重要インフラの分野固有知識に基づく解析と、分野間にまたがる共有知を統合できる革新的な解析モデルを構築し、継続的に適用可能な動作監視・解析技術を目指す。

・ 上記の主な技術を社会実装するための認証制度の設計、共通プラットフォームの実現とセキュリティ人材育成

- Ø それぞれの重要インフラ等の特性を踏まえて新技術を円滑に導入するための認証制度を設計する。
- Ø セキュリティ対策に必要な情報や、脅威情報などを、重要インフラ分野共通、さらに分野間にまたがって共有し、活用できる共通プラットフォーム技術に取り組み、複数の重要インフラに対する同時サイバー攻撃へのセキュリティを確保する。
- Ø 重要インフラシステムにセキュリティ対策技術を適用する上での安全性検証を容易に実施するための評価検証技術を確立する。
- Ø 重要インフラ事業者、機器・システムの製造事業者、認証制度に係る団体、共通プラットフォームの運営に係る者等、重要インフラのステークホルダー全般に対して人材の育成を図る。

2．研究開発の内容

（1） 研究開発計画の全体像

① セキュリティ対策技術についてのシステムの要件

本研究開発にあたってのシステム要件は以下の通りである。

重要インフラ等で利用する設備や機器においては、情報システムとしての一般的要件に加えて、可用性の重視や十年以上の長期利用を前提とする特徴的な運用がなされている。このため、重要インフラ等のサイバーセキュリティ確保に向け、新たな技術を段階的に導入可能とすること、計画的なシステム改善が可能であること、システムソフトウェア等を安全に更新するための機能を具備することが必要である。特に、システムを構成する機器が多種かつ多数であるため、新規技術を一斉に導入することは困難であるため、新技術は部分的に導入され、新旧設備が混在しても、導入の効果が発揮できるものである必要がある。

今後、インフラシステムにも普及が期待される小型 IoT 機器のように搭載可能な処理性能が大幅に制限される場合が多いため、単独では十分なセキュリティ対策を実装できない機器がある。これらの機器に対しても有効な対策を講じる必要がある。

② 研究開発の取り組みの考え方

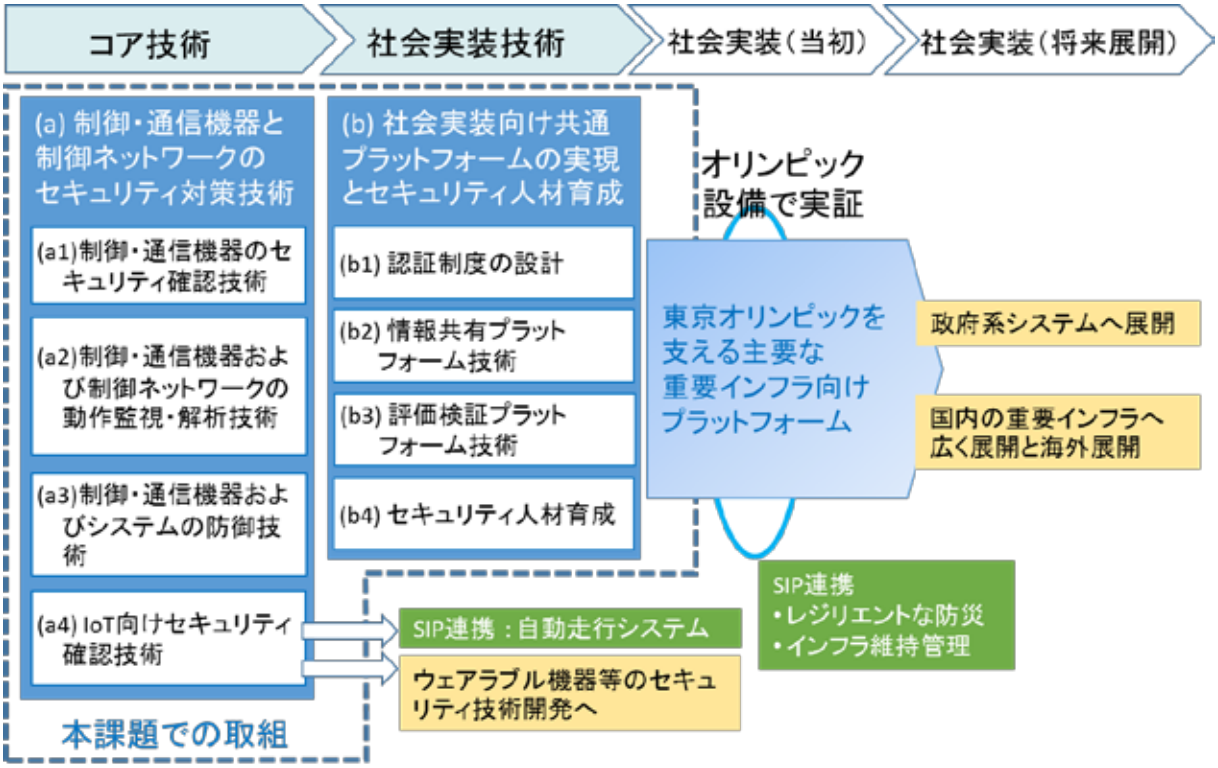
本研究開発は、図表３に示すように、コア技術として

（a）制御・通信機器と制御ネットワークのセキュリティ対策技術の研究開発

と、上記(a)技術の出口となる社会システムにおいて実装する社会実装技術として

（b）社会実装に向けた共通プラットフォームの実現とセキュリティ人材育成

を密に連携して進め、当初の社会実装として 2020 年東京オリンピック・パラリンピック競技大会設備を支える主要な重要インフラに導入し実証する。



図表３　計画の全体像

本研究開発の取り組みの考え方は次の通りである。

- 構築時の作り込みと運用時の監視・対処の双方が連結する取り組み

運用時のサイバーセキュリティ対策として、システム全体の監視・分析能力や組織としての緊急対処能力の強化が求められている。一方、それらのインシデントの原因（脆弱性）をもたらさないために、構築（企画・設計・製造）時のセキュリティの作り込み（SBD: Security By Design）が重要であることは言うまでもない。ただし、構築時または運用時の片方の対策のみでは、実用的なサイバーセキュリティ対策が見込めないことは明白である。このため、本研究開発では、構築時と運用時の双方を連結する技術によって経済的かつ効果的なセキュリティ対策を目指す。

- サイバー攻撃側の技術・手段の進化や狙いの変化への対応

サイバー攻撃側の技術や手段が常に進化し続けていることや、攻撃の目的そのものが年々変化していることは周知の事実である。本研究開発では、運用時の監視・解析にも重点を置き、得られた攻撃側の進化・変化の情報を分野間で共有するとともに、対策手段の研究開発に活かすことを目指す。

- 適切な社会的マネジメントに必要な制度設計と技術への取り組み

インターネットに代表される近年の ICT は、オープンかつ制約の少ない技術開発競争により急速に発展してきているが、サイバーセキュリティの側面では、社会的な問題が顕著になってから、事後対処として社会的なマネジメント（制度やガイドライン等）が導入され、結果として社会的コストが増大してしまう場合もある[7]。重要インフラ 13 分野だけでなく、事後のセキュリティ対処の社会的な影響が大きい分野では、制度設計やガイドラインを先行させ、サービスや利用される機器の導入を適切にマネージすることが社会的な要請となる。このため、本研究開発では、そのような制度の実装に必要となる技術（適合性評価技術等）と制度の枠組み設計を目指す。

l　重要インフラ等のセキュリティオペレーション体制強化への取り組み

重要インフラの制御ネットワークがサイバー攻撃を受けても安全に運用し続けるためには、制御ネットワークを構成する制御・通信機器に対するサイバー攻撃を防ぐ対策を講じることだけではなく、サイバー攻撃が発生した場合にいち早く検知すること、被害が発生した場合に素早く発生箇所を特定して応急対策・復旧をはかることが大切である。このため、本研究開発では、セキュリティオペレーションの共通プラットフォーム化と重要インフラ等の特性に応じた実装の両面から、セキュリティオペレーション体制の強化とその社会実装に必要となる技術を目指す。

さらに、重要インフラ等のセキュリティ対策技術の開発からセキュリティオペレーションにおいて、それぞれの分野知識・スキルとサイバーセキュリティの共通知識・スキルを併せ持つ人材育成に取り組む。

③　研究開発技術の概要

重要インフラのサイバーセキュリティ確保のためには、インフラシステムの制御ネットワークを構成する制御・通信機器が、仕様通りの構成であり改変されバックドア等の不正な機能が作り込まれていないこと（完全性）が構築時・運用時に確認でき、また運用中に不正な機器にすり替えられていないこと（真正性）が運用時に確認できる必要がある。この完全性と真正性の両観点で制御・通信機器の信頼性を確認するためのコア技術として(a1) 制御・通信機器のセキュリティ確認技術を研究開発する。さらに、制御・通信機器による信頼性確認方法が正当であることを含めて制御・通信機器の安全性を第三者が認証するための(b1)認証制度を設計する。これら構築時から運用時までが連結した技術により、機器の信頼性に関わるリスクを最小化することができる。なお、この技術を IoT システムの急速な普及に合わせ、小型 IoT 機器に対しても適用できるよう(a4)IoT 向けのセキュリティ確認技術を研究開発する。

このような予防的対策に加えて、本研究開発では、構成する制御・通信機器が仕様通りの動作をしているか（振る舞い正当性）のチェックを行う機能を新旧の設備が混在する制御ネットワークに対して実現する。そしてこの動作確認のためのログ分析は制御ネットワークに対しても行う。この技術によって、サイバーセキュリティ対策における検知プロセスを重要インフラの制御・通信機器と制御ネットワークにログ分析機能としてはじめから具備させることができる。この技術を(a2)制

[7] 2012 年から脆弱性のあるホームルータが原因となるサイバーインシデントが発生。2014 年、対策のために通信事業者への指針(H26 年 4 月 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ)。

御・通信機器および制御ネットワークの動作監視・解析技術とする。この技術によって、重要インフラ等の大規模システムの制御・通信機器と制御ネットワークのサイバーセキュリティ耐性を順次強化することが可能となる。さらに、機器の異常を検知した場合、制御システムの可用性を重視する(a3)制御・通信機器およびシステムの対策技術に取り組む。

この監視・解析結果により異常が発見された場合は、その状況をいち早く関係のインフラシステムのステークホルダーに共有する。例えば、各セキュリティオペレーションセンターSOC（Security Operation Center）へ共有することを想定した場合、重要インフラ事業者の意向を踏まえたSOCの判断に基づき、該当制御・通信機器等の停止等の制御を行うことも可能とする。(a1)～(a4)で開発したコア技術をそれぞれ具備した異なる重要インフラ分野の事業者間で円滑に情報共有を行うための(b2)情報共有プラットフォーム技術を研究開発し、サイバーセキュリティ対策における分野間連携の促進に貢献する。本技術により、発見された情報の緊急性や普遍性等に応じ、営業秘密等にも配慮しながら、同一分野のインフラ事業者間や、内容によってはインフラ分野をまたいで情報共有することが可能となる。重要インフラシステムに(a)技術を適用する上での安全性検証を容易に実施するために（b3）評価検証プラットフォーム技術を研究開発する。この情報共有プロセスや評価検証においては、情報の目利きができる優秀な人材の存在が不可欠である(b4)セキュリティ人材育成を行う。

これらの成果は、来る2020年東京オリンピック・パラリンピック競技大会関連の設備や大会を支える代表的な重要インフラへの適用をすすめ、それぞれのインフラシステムのサイバーセキュリティ確保に貢献する。これらのインフラはその制御ネットワークを構成する制御・通信機器の数が比較的限定でき、投資効果も予想がしやすく、ターゲットとしての合理性がある。また、これらの成果は政府系システムや他のインフラシステムへの展開が可能である。

さらに、重要インフラ向けのセキュリティ対策技術をさらに洗練もしくは簡素化を行うことにより、IoT向けの機器への適用が可能になる。IoT向けの成果は、並行して研究開発が進められているSIP課題「自動走行システム」やウェアラブル機器等において利便性とセキュリティの両立を可能とし、産業規模拡大に貢献できると考える。

（２） 研究開発項目

（a）制御・通信機器と制御ネットワークのセキュリティ対策技術の研究開発

（a1）制御・通信機器のセキュリティ確認技術

機器の製造に組み込まれる不正機能の混入を想定したセキュリティ機能により、システム構築時とシステム運用時に制御・通信機器のセキュリティ（真正性・完全性）確認ができ、その確認結果を理論的、又は実用的に担保することにより、安全なシステム更新を実現する。

① 制御・通信機器の信頼の起点を確保する技術。

② 機器を製造する段階で不正機能の混入有無を確認する機器テスト技術。

③ 運用時に制御・通信機器のソフトウェアの真正性・完全性を確認するための技術を実現する。

なお、ここでの技術開発においては、共通技術と、インフラ分野固有のシステム構造（階層的な制御ネットワーク構造等）に対応する技術を考慮する必要がある。

（a2）制御・通信機器および制御ネットワークの動作監視・解析技術

システムの運用時に、システムとして健全な状態であることを確認するために制御・通信機器および制御ネットワークに対する効率的なログ収集、ログ解析による動作監視、さらには、バックドア解析、重要インフラ分野で共通化可能な知識の解析モデル等の先端的な機能を実現する。なお、現在稼働中の重要インフラ等では、従来から稼働している制御・通信機器との混在を念頭に置くことが重要である。

① 個々の制御・通信機器および制御ネットワークとしての動作を監視し、バックドアの有無などを解析するために、制御・通信機器のログ分析を機器内で行う機能、もしくはネットワーク経由で処理を集約する設備で行う機能。本機能では(a1)技術による機器の真正性確認を活用することにより、新旧の機器が混在する大規模システムのセキュリティ耐性強化を可能とする。

② 将来にわたり高速大容量化するネットワークトラヒックに追従できる先進的なリアルタイムのログ収集機能、および将来の重要インフラ等において普及が予想される革新的な監視機能、および制御機能。

③ 重要インフラにおける制御システムの分野固有知識と、分野間にまたがる共有知を統合できる革新的な解析モデルを構築し、継続的に進化可能な動作監視・解析技術。

④ IoT 機器の動作監視・解析を可能にする IoT 機器向けゲートウェイ機能。

（a3）制御・通信機器およびシステムの防御技術

防御策については、重要インフラ分野ごとに判断基準が異なることから、本研究開発では、各重要インフラに対する攻撃の発生と被害を迅速に検知・通知することを重点に置くが、先行的に防御策を検討することも必要である。

具体的には、制御・通信機器の状態を監視し、機器の異常を検知した場合、制御システムの可用性を重視し、安全な機器のみで処理を継続するホワイトリスト協調技術を実現する。

（a4）IoT 向けセキュリティ確認技術

重要インフラに加え、広く社会生活の中で普及が見込まれる IoT に向けて、大小さまざまな種類の IoT 機器があることを考慮し、小型 IoT 機器までに適用可能な効率的な機器の具体化に向けて、制御・通信機器の信頼の起点を確保する技術を実装し、安全な IoT システムの普及に貢献する。

具体的には、高信頼な暗号処理や通信により IoT 機器の成り済ましおよびセンシングデータの改ざんを防止する技術、IoT 機器上のソフトウェアの完全性・真正性を確認する技術、製造段階での不正機能の混入を確認する機器テスト技術を開発する。

（b）社会実装に向けた共通プラットフォームの実現とセキュリティ人材育成

（b1）認証制度の設計

重要インフラシステムの制御ネットワークや政府系システムの制御・通信機器の製造者とその機器に対して、上記(a1)および(a4)の技術に基づく機能が正しく実装されていることを確認（技術適

合検査）する認証制度を設計する。本成果を活用した認証制度の実現においては、重要インフラ分野毎の特性や、既存技術との関係、国際標準戦略への取り組みから総合的に検討を進める。また、機器やシステムのセキュリティ設計や実装が適切に実施されていることを確認する既存の取り組み（制御機器認証プログラム(EDSA)、暗号モジュール試験及び認証制度(JCMVP)、情報セキュリティ評価及び認証制度(JISEC)等）や情報通信分野の安全性やセキュリティに関する各種基準（「情報通信ネットワーク安全・信頼性基準」、「電気通信分野における情報セキュリティ確保に係る安全基準」等）を利活用するなど、関連する制度・組織との間で緊密な連携を行う。

（b2）情報共有プラットフォーム技術

ログ分析・バックドア解析、モデル解析の結果を、発見された情報の緊急性や普遍性等に応じ、営業秘密等にも配慮しながら、同一インフラ事業者間や、内容によってはインフラ分野をまたいで情報を安全に共有する機能を実現する。その際、重要インフラ分野における横断的情報共有のための既存の取り組みや組織(サイバー情報共有イニシアティブ(J-SCIP)、重要インフラ事業者等の情報共有・分析機能（CEPTOAR)、テレコム・アイザック推進会議（Telecom-ISAC Japan）等)を利活用する等、関連する制度・組織との間で緊密な連携を行う。

この情報共有プラットフォーム技術は、インフラ事業者内のセキュリティオペレーションセンターSOC(Security Operation Center)等における情報共有機能（ISAC Information Sharing Analysis Center 機能）として導入し、重要インフラ分野をまたがる情報共有および連携を実現する。

また、情報共有機能に関連する法制度等を調査し、日本におけるあり方を検討する。

（b3）評価検証プラットフォーム技術

重要インフラシステムに(a)技術を適用する上での安全性検証を容易に実施できるように、試験・評価機能、評価手順および適用ガイドラインなどを共通プラットフォーム技術および検証環境として整備する。

（b4）セキュリティ人材育成

前述(a)の制御・通信機器の製造事業者や認証制度に係る組織におけるセキュリティ人材の育成については、セキュリティ機能の作り込み、テスト、および評価を実施できる人材を育成する。セキュリティに関する分野共通の知識・スキルとともに、分野固有の知識・スキルを有する人材育成のフレームワーク、カリキュラム、OJT による実践的教育の設計を実施する。

上記に当たっては、大学や公的セキュリティ機関、および様々な先行する取り組みとの連携を活用していく。

（３） 研究開発目標

【中間目標（2017 年末)】

(a) 制御・通信機器と制御ネットワークのセキュリティ対策技術の研究開発

制御・通信機器のセキュリティ確認技術については、2020 年東京オリンピック・パラリンピック競技大会の大会運営設備に関わる重要インフラシステムを対象として、技術の有効性をプロトタイ

プ実装によって評価する。本確認技術により、導入・運用時に管理対象でない制御・通信機器が繋げられたり、制御・通信機器に悪意のある機能が意図せず仕込まれることを防止する。

制御・通信機器および制御ネットワークの動作監視・解析技術と対策技術については、2020 年東京オリンピック・パラリンピック競技大会の大会運営設備に関わる重要インフラシステムを対象とし、インフラシステム毎の SOC に集約して解析するアーキテクチャを前提に、ログ分析・バックドア解析技術の有効性を評価する。本監視・解析技術と対策技術により、前述の確認技術が導入されていない制御・通信機器が混在する（移行段階の）制御ネットワークにおいても、仕様に準じない動作を検出することで、システム全体のセキュリティ向上を図ることができる。

IoT 向けのセキュリティ対策技術については、前述の確認技術並びに、監視・解析技術をそのまま適用できない小型 IoT 機器に対し、両セキュリティ技術相当のセキュリティ機能を具備させるべく方式設計と評価を行う。あわせて、多数の小型 IoT 機器を対象としてセキュリティ担保ができるシステムのプロトタイプを実現する。

（b）社会実装に向けた共通プラットフォームの実現とセキュリティ人材育成

制御・通信機器のセキュリティ確認技術の活用を促進するための認証制度に必要な国際標準化を準備する。

重要インフラシステムへの(a)技術適用の安全性検証を容易に実施できるように、試験・評価機能、評価手順および適用ガイドラインなどを整備し、2020 年東京オリンピック・パラリンピック競技大会の大会運営設備に関わる重要インフラシステムのセキュリティ運用で活用できる準備を行う。

機器の製造事業者や認証制度に係る組織や重要インフラシステムのオペレーションを担当する組織において、その管理者や機械、制御等のインフラ分野毎の技術者を対象に、本 SIP で整備する共通プラットフォームを有効活用できるセキュリティ人材を育成する体制と環境を設計する。

【最終目標（2019 年末）】

（a）制御・通信機器と制御ネットワークのセキュリティ対策技術の研究開発

制御・通信機器のセキュリティ確認技術については、2020 年東京オリンピック・パラリンピック競技大会に関連する運営設備として導入し、本番環境におけるシステム評価を実施する。

制御・通信機器および制御ネットワークの動作監視・解析技術については、2020 年東京オリンピック・パラリンピック競技大会の大会運営設備に関わる重要インフラシステムの SOC に導入し、プレ大会などを通して、ログ分析・バックドア解析技術の有効性を評価する。

制御・通信機器およびシステムの対策技術については、制御システムの可用性を重視し、安全な機器のみで処理を継続する技術を確立する。

IoT 向けのセキュリティ対策技術においては、前述の両セキュリティ技術を制御・通信機器に具備させる場合と比べ、ハードウェアとソフトウェアを併せて大幅なコスト削減を実現する。また、多数の小型 IoT 機器を対象としてセキュリティ担保ができるシステムを実用化する。

（b）社会実装に向けた共通プラットフォームの実現とセキュリティ人材育成

制御ネットワークの制御・通信機器（制御機器に内蔵されるものを含む）のセキュリティ確認技

術の活用を促進するために、適合性検査に必要な機器テストを含めた検査手順や手続きなど、認証制度を設計し、それらの認証基準についての国際標準化を行う。

情報共有および評価検証の共通プラットフォーム技術を活用して、重要インフラシステムへの(a)開発技術適用の事前検証を行うと共に、2020 年東京オリンピック・パラリンピック競技大会の大会運営設備に関わる重要インフラシステムのセキュリティ運用において、監視・解析結果を、適切に、インフラ分野をまたいで情報を安全に共有する機能を実現する。

機器の製造事業者や認証制度に係る組織や重要インフラシステムのオペレーションを担当する組織において、その管理者や機械、制御等のインフラ分野毎の技術者を対象として、適切な規模のセキュリティ人材を育成し、各重要インフラシステムを安定稼働させる。

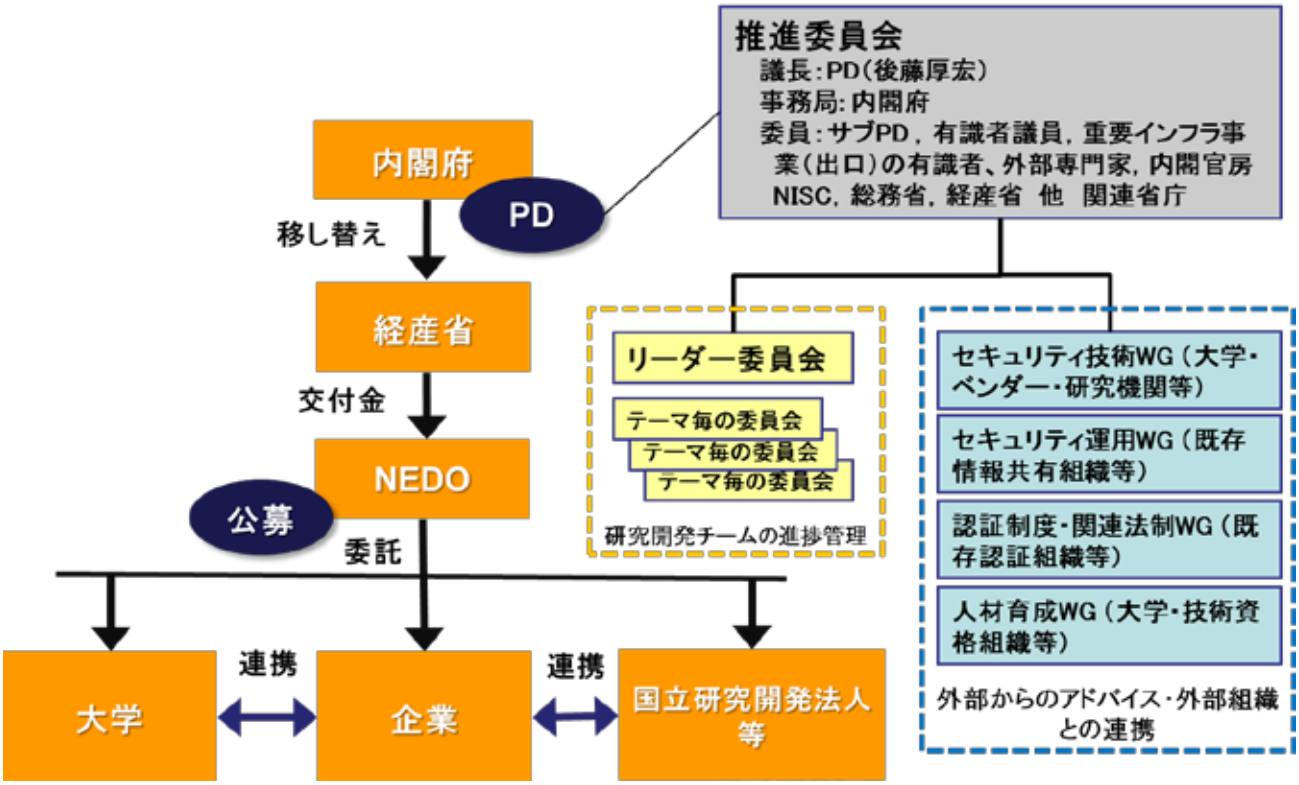
3．実施体制

(1) 国立研究開発法人新エネルギー・産業技術総合開発機構の活用

本件は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）への交付金を活用し、下図のような体制で実施する。NEDO は PD や推進委員会を補佐し、研究開発の進捗管理、自己点検の事務の支援、評価用資料の作成、関連する調査・分析などを行う。

(2) 研究主体の選定

NEDO は、本計画に基づき、研究課題、および研究課題を実施する研究主体を公募により選定する。選考に当たっての審査基準や審査員等の審査の進め方は、NEDO が PD 及び内閣府及び推進委員会と相談したうえで、決定する。審査には原則として PD 及び内閣府の担当官、外部有識者が参加する。応募課題に参加する研究者の利害関係者は当該課題の審査には参加しない。利害関係者の定義は NEDO が定める。選考により研究課題が決まった後、本計画に研究課題、および研究主体、研究参加者を記載する。



図表４　実施体制

(3) 研究主体を最適化する工夫

PD は、研究課題の進捗状況、および関係機関等で実施する技術調査等の調査結果や、社会情勢の変化に応じ、研究課題の変更、追加、研究主体の入れ替え、追加等を検討していく。

また、一部の研究課題については「ステージゲート方式」を採用し、多種多様なアイデアを選定して一定期間推進した後に、研究主体の絞り込みを行い、最適な体制で本プロジェクトを推進することも検討する。

それぞれの研究課題に取り組む研究主体同士の連携を図るために、リーダー委員会を設け、定期的な情報交換を通して、本課題の目標を共有する。

(4) 外部からのアドバイス・外部組織との連携の工夫

推進委員会の配下に、セキュリティ技術、事業者による運用、認証制度と関連法制度、人材育成など、主要な研究課題に対応した WG を設け、国内外の有識者からのアドバイスを得るとともに、既存の関連組織や活動との密な連携を図る。

4．知財に関する事項（P）

(1) 知財委員会

知財委員会を NEDO に置く。

知財委員会は、研究開発成果に関する論文発表及び特許等（以下「知財権」という。）の出願・維持等の方針決定のほか、必要に応じ知財権の実施許諾に関する調整などを行う。

知財委員会は、PD または PD の代理人、主要な関係者、専門家から構成する。

知財委員会の詳細な運営方法等は、知財委員会を設置する機関において定める。

(2) 知財権に関する取り決め

NEDO は、秘密保持、バックグラウンド知財権（研究責任者やその所属機関等が、プログラム参加する前から保有していた知財権）、フォアグラウンド知財権（プログラムで発生した知財権）の扱い等について、予め委託先との契約等により定めておく。

(3)バックグラウンド知財権の実施許諾

他のプログラム参加者へのバックグラウンド知財権の実施許諾は、当該知財権者が定める条件に従い、知財権者が許諾可能とする。

当該条件などの知財権者の対応が、SIP の推進に支障を及ぼすおそれがある場合、知財委員会において調整し、合理的な解決策を得る。

(4) フォアグラウンド知財権の取扱い

フォアグラウンド知財権は、原則として産業技術力強化法第 19 条第 1 項を適用し、発明者である研究責任者の所属機関（委託先）に帰属させる。

再委託先等が発明し、再委託先等に知財権を帰属させる時は、知財委員会による承諾を必要とする。その際、知財委員会は条件を付すことができる。

知財権者に事業化の意志が乏しい場合、知財委員会は、積極的に事業化を目指す者による知財権、実施権の保有を推奨する。

参加期間中に自らの意志で脱退する者は、当該参加期間中に SIP の事業費により得た成果（複数年度参加していた場合には、参加当初からの全ての成果）の全部または一部に関して、脱退時に NEDO が指定する機関に無償譲渡させること及び実施権を設定できることとする。

知財権の出願・維持等にかかる費用は、原則として知財権者による負担とする。共同出願の場合は、持ち分比率、費用負担は、共同出願者による協議によって定める。

(5)フォアグラウンド知財権の実施許諾

他のプログラム参加者へのフォアグラウンド知財権の実施許諾は、知財権者が定める条件に従い、知財権者が許諾可能とする。

第三者へのフォアグラウンド知財権の実施許諾は、プログラム参加者よりも有利な条件にはしない範囲で知財権者が定める条件に従い、知財権者が許諾可能とする。

当該条件などの知財権者の対応が、SIP の推進に支障を及ぼすおそれがある場合、知財委員会において調整し、合理的な解決策を得る。

(6) フォアグラウンド知財権の移転、専用実施権の設定・移転の承諾について

産業技術力強化法第 19 条第 1 項第 4 号を準拠し、フォアグラウンド知財権の移転、専用実施権の設定・移転の承諾には、合併・分割により移転する場合や子会社・親会社に知財権の移転、専用実施権の設定・移転の承諾をする場合等（以下、「合併等に伴う知財権の移転等の場合等」という。）を除き、NEDO の承認を必要とする。

合併等に伴う知財権の移転等の場合等には、知財権者は NEDO との契約に基づき、NEDO の承認を必要とする。

合併等に伴う知財権の移転後であっても NEDO は当該実施権にかかる再実施権付実施権を保有可能とする。当該条件を受け入れられない場合、移転を認めない。

(7) 終了時の知財権取扱いについて

プログラム終了時に、保有希望者がいない知財権については、知財委員会において対応（放棄、あるいは、NEDO 等による承継)を協議する。

(8)国外機関等（外国籍の企業、大学、研究者等）の参加について

当該国外機関の参加が課題推進上必要な場合、参加を可能とする。

適切な執行管理の観点から、研究開発の受託等にかかる事務処理が可能な窓口または代理人が国内に存在することを原則とする。

国外機関等については産業技術力強化法第 19 条第 1 項を適用せず、知財権は NEDO と外国機関等の共有とする。

5．評価に関する事項

(1) 評価主体

PD と NEDO 等が行う自己点検結果の報告を参考に、ガバニングボードが外部の専門家等を招いて行う。この際、ガバニングボードは分野または課題ごとに開催することもできる。

(2) 実施時期

○事前評価、毎年度末の評価、最終評価とする。
○終了後、一定の時間（原則として 3 年）が経過した後、必要に応じて追跡評価を行う。
○上記のほか、必要に応じて年度途中等に評価を行うことも可能とする。

(3) 評価項目・評価基準

「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）」を踏まえ、必要性、効率性、有効性等を評価する観点から、評価項目・評価基準は以下のとおりとする。評価は、達成・未達の判定のみに終わらず、その原因・要因等の分析や改善方策の提案等も行う。

①意義の重要性、SIP の制度の目的との整合性。
②目標（特にアウトカム目標）の妥当性、目標達成に向けた工程表の達成度合い。
③適切なマネジメントがなされているか。特に府省連携の効果がどのように発揮されているか。
④実用化・事業化への戦略性、達成度合い。
⑤最終評価の際には、見込まれる効果あるいは波及効果。終了後のフォローアップの方法等が適切かつ明確に設定されているか。

(4) 評価結果の反映方法

○事前評価は、次年度以降の計画に関して行い、次年度以降の計画等に反映させる。
○年度末の評価は、当該年度までの実績と次年度以降の計画等に関して行い、次年度以降の計画等に反映させる。
○最終評価は、最終年度までの実績に関して行い、終了後のフォローアップ等に反映させる。
○追跡評価は、各課題の成果の実用化・事業化の進捗に関して行い、改善方策の提案等を行う。

(5) 結果の公開

○評価価結果は原則として公開する。
○評価を行うガバニングボードは、非公開の研究開発情報等も扱うため、非公開とする。

(6) 自己点検

①研究責任者による自己点検

PD が自己点検を行う研究責任者を選定する（原則として、各研究項目の主要な研究者・研究機関を選定）。

選定された研究責任者は、5.(3)の評価項目・評価基準を準用し、前回の評価後の実績及び今後

の計画の双方について点検を行い、達成・未達の判定のみならず、その原因・要因等の分析や改善方策等を取りまとめる。

②PD による自己点検

PD が研究責任者による自己点検の結果を見ながら、かつ、必要に応じて第三者や専門家の意見を参考にしつつ、5.(3)の評価項目・評価基準を準用し、PD 自身、NEDO 及び各研究責任者の実績及び今後の計画の双方に関して点検を行い、達成・未達の判定のみならず、その原因・要因等の分析や改善方策等を取りまとめる。その結果をもって各研究主体等の研究継続の是非等を決めるとともに、研究責任者等に対して必要な助言を与える。これにより、自律的にも改善可能な体制とする。

これらの結果を基に、PD は NEDO の支援を得て、ガバニングボードに向けた資料を作成する。

6．出口戦略

①出口指向の研究推進

○先行すべき重要インフラへの導入を目標とした研究開発を推進

- **3 年目～4 年目に政府系システム及び 2020 年東京オリンピック・パラリンピック競技大会に向けて先行すべき重要インフラ等（通信・放送、エネルギー、交通システム等）への導入を目標として研究開発を推進する。**
- **4 年目～5 年目に分野横断の共通プラットフォームにより重要インフラ等（金融、化学、石油等）への導入を目標として研究開発を推進する。**
- **重要インフラ事業への導入を円滑に進めるために、研究開発当初から、技術のユーザとなる企業と連携した要件定義行程を実施する。**
- **平行して技術と認証評価制度に関わる国際標準化活動を実施する。**

○研究開発段階から社会実装を最短で実現する研究開発体制を構築

・社会実装先として想定される各重要インフラ分野の所管省庁や民間事業者の知見や技術を有効活用可能な研究開発体制を構築する。

・重要インフラ分野のセキュリティ対策を推進するNISCと連携した分野横断的な取り組みによって、本研究開発成果の社会浸透を図る。

②普及のための方策

○2020 年東京オリンピック・パラリンピック競技大会での実績作り

○強靭なセキュリティ機能を日本全体の重要インフラや政府系システムへ順次展開

○利用される分野に応じ、標準化・規格化・安全評価手法やその認定手法の策定を推進し、開発成果の利用を促進

○本研究開発成果を活用した機器の認証評価サービスを諸外国に先んじて開始することによって、その実績をもとにした国際標準化を進める。これによって民間事業者による重要インフラビジネスの海外展開を促進し、迅速な社会実装を実現

○研究開発した技術や仕組みを世界へ輸出展開し、グローバルビジネスに貢献

○分野に応じた規制、トップランナー基準等によるユーザーサイドでの適切な導入を促進

○今後の社会動向に合わせて、中長期的に産業界で求められるサイバーセキュリティ対策やセキュリティ人材のあり方を展望し、必要に応じて研究課題の変更等を実施

・メーカーや、有識者へのヒアリング、内外の技術動向の調査等を行い、最適な研究が実施されるようなマネジメントを遂行

7．その他の重要事項

(1) 根拠法令等

本件は、内閣府設置法（平成 11 年法律第 89 号）第 4 条第 3 項第 7 号の 3、科学技術イノベーション創造振興費に関する基本方針（平成 26 年 5 月 23 日、総合科学技術・イノベーション会議）、科学技術イノベーション創造振興費に関する実施方針（平成 26 年 5 月 23 日、総合科学技術会議・イノベーション会議）、戦略的イノベーション創造プログラム運用指針（平成 26 年 5 月 23 日、総合科学技術・イノベーション会議ガバニングボード）に基づき実施する。

(2) 弾力的な計画変更及び計画変更の履歴

本計画は、成果を最速かつ最大化させる観点から、PD の判断で状況に応じて見直すこととする。