## 3.2　評価

### 3.2.1　意義の重要性、SIP の制度の目的との整合性

#### (1)サイバーセキュリティの社会的・経済的意義

重要インフラ等へのサイバー攻撃の脅威は現実のものとなる中で、重要インフラ等に関わるサイバーセキュリティ対策技術は、安全保障の観点から、海外ベンダに依存するのではなく、一部のコアな技術だけでも日本国内だけで対応できるようにすることが重要である。本課題は、我が国の重要インフラ等の安定運用に貢献するとともに、我が国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にも貢献することが期待できる。

研究開発に取り組んだ研究開発者も、研究責任者等のアンケートで「課題が社会的・経済的に意義を持っていたか。」という問いに対して社会的意義については「とてもそう思う」が 93%・「そう思う」が 7%、経済的意義については「とてもそう思う」が 86%・「そう思う」が 14%と高く認識されている。

#### (2)重要インフラ等事業者との連携

サイバーセキュリティ技術のユーザーとなる重要インフラ等事業者と密に協議する体制を実現できたため、重要インフラ等事業者がサイバーセキュリティ技術を導入するに際してのニーズを的確にフィードバックできた。

通常はサイバーセキュリティ技術を有する企業において研究開発がある程度進み、製品化段階となって初めて重要インフラ等事業者とコミュニケーションを深めることができるため、社会実装に時間を要する。しかし、本課題では研究開発当初より推進委員会等で重要インフラ等事業者のニーズを直接確認でき、適宜研究開発にフィードバックできた。例えば、可用性を重視する重要インフラ等への導入に必要とされるリードタイム等を早い段階で把握でき、オリパラまでの先行導入につなげられた。また、長期運用されている機器ゆえの性能面の制約に対応するための仕様変更も行われた。重要インフラ等事業者が人材育成やランニングコストに関心を持つことがわかり、早い段階から対応できた。さらに、重要インフラ等事業者から提供された設備仕様をもとに有効な共用検証環境を構築できた。

#### (3) サイバーセキュリティ技術を有する企業間の連携

本課題を主導した企業は通常事業において互いに競合する面があるが、今回は適切な分担で協力する体制が構築できたため、その中で情報交換ができた。具体的には、互いに得意領域を基に研究テーマを分担し、全体として高度な研究開発を実現できた。また、各企業それぞれが従来関係を持つ重要インフラ等事業者が存在することから、互いにそのネットワークを共有し、社会実装をうまく進めることができた。

また、大規模予算であることを活用して、重要インフラ等事業者の設備を再現した共用検

証環境を作り、各企業が持ち込み検証を行う仕組みも実現できた。

### (4) 省庁連携

省庁連携が実現されたことで、複数分野の重要インフラ等における展開を効果的・有効に実行できた。

各種重要インフラ等は、各々所管官庁が異なり、サイバーセキュリティに係る政策の取り組み状況に差があるが、SIP では、推進委員会、WG の場に省庁、重要インフラ等事業者等も参加し、一堂に会して議論した。その結果、各省庁でのサイバーセキュリティに関する意識が共通的に醸成されたとともに、各種重要インフラ等事業者に関してもサイバーセキュリティ意識や取組のレベル差を埋めようとする動きが活発化した。

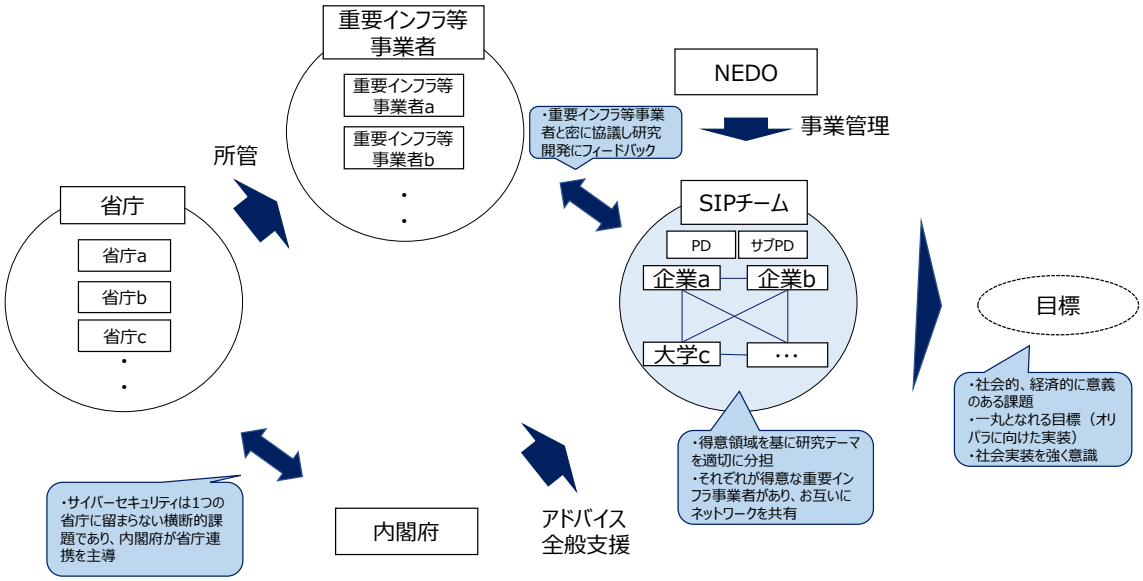


図 3-5　「意義の重要性、SIP の制度の目的との整合性」に関わる事項のまとめ

（注）「意義の重要性、SIP の制度の目的との整合性」に係るポイントを「吹き出し」に記載

## 3.2.2 目標・計画・戦略の妥当性

アウトカム目標として、SIP 期間内で、開発したサイバーセキュリティ技術を重要インフラ等に実装し、オリパラに貢献することを掲げている。こうした目標は時期も含めて明確であり、セイバーセキュリティ技術を有する企業だけではなく、重要インフラ等事業者も含めた多様なステークホルダーが問題意識を共有し、一丸となることができる適切な設定だった。

本課題の計画についても、PD によってコア要素技術（セキュリティ（真正性・完全性）確認、動作監視・解析技術等）から社会実装（適合性評価、人材育成等）まで、体系的に設定されていた。前半の 3 年間でコア要素技術開発を重点的に行い、後半の 2 年間で社会実装やコア要素技術の実証試験を行う点は概ね妥当であったと考えられる。計画通りのアウトプットが現時点で出そろっており、かつ出口のタイミングを的確に見定めて先行リリー

スを実施した点を加味すると妥当であったと考えられる。

研究責任者対象のアンケート調査においても、計画に対する評価は高い。「アウトプット目標(技術達成目標等)は、適切だったか」で「とてもそう思う」が 79%となっており、同様に「とてもそう思う」が「必要十分な研究テーマがそろっていた」は 64%、「研究テーマは体系的に整理されていた」は 71%、「具体的な内容を示した工程・計画だった」は 64%、「アウトカム目標は適切な設定だったか」は 64%といずれも高くなっている。

ただし、重要インフラ等事業者がサイバーセキュリティ技術を導入するに際しては、技術の実証試験、一部導入等、調達に至るまでのリードタイムが必要であった。こうしたことが明らかになったのは、本課題で重要インフラ等事業者と連携できたからこそであり、結果として新たに研究開発した技術の導入という面からは、非常に短期的で厳しい目標となったが、研究計画の変更を行って先行版の導入を達成している。

### 3.2.3 課題のマネジメント（適切なマネジメントがなされているか。）

#### (1) PD による強力で細やかなリーダーシップ

研究開発テーマ毎の頻回の進捗会議に PD、サブ PD 両名が参加する等、PD 自ら積極的に関与しており、各研究責任者の取り組みを十分にサポートした。具体的には、研究開発テーマ毎に開催される定期的な進捗会議（月 1 回程度）に PD 自ら参加し、研究開発の進捗状況、方向性の検討、問題点の共有、社会実装先の候補となる重要インフラ等事業者との調整方法の相談等、研究開発進捗状況のモニタリングを定期的に行って PD と研究責任者間とで友好な関係を構築した。その一方で、PD に係る負担は非常に大きかったものとみられる。

サブ PD は、特定の研究開発テーマを担当するのではなく、PD 補佐的役割として事業に全面的に関わり、PD とともに進捗会議等に参加した。このことは、事業を円滑に遂行するためのリスク管理としても有効に機能した。

#### (2) テーマ横断的な議論の場としての推進委員会・WG

推進委員会は主要な重要インフラ等事業者の経営層、各重要インフラ等分野の所管省庁、情報連携組織、学識経験者等により構成され、研究開発の進め方や方向性、迅速な社会実装実現に向けての議論を行い、議論内容を研究開発に適宜フィードバックした。さらに、この推進委員会に加えて、「セキュリティ技術 WG」、「セキュリティ運用 WG」、「認証・法制 WG」、「人材育成 WG」を設置[5]し、社会実装に向けたテーマ横断的な課題解決を議論する場を設けた。

さらに、これらの会議体に重要インフラ等事業者の経営層等が参加したことで、重要インフラ等事業者側が抱えるニーズを事業者が適切に把握することができたことに加えて、決定事項が重要インフラ等事業者内でトップダウン式に浸透した。

[5] 令和元年度（2019 年度）は社会実装 WG 及び人材育成 WG に再編して事業者アンケート・ヒアリングを実施することでより幅広い社会実装向けての議論を実施した。

SIP では様々な重要インフラ等（電力、放送等）事業者が関与しており、業界団体ごとにセキュリティへの認識に対する温度差もあったが、他のトップランナーや業界として意識的に進めたことでこの異業種間の認識格差を埋めて、取り組みを推進した。事業者間連携の推進に当たっては、必要に応じて NDA を締結する等、研究マネジメント面における適切な対応を行ったことも有効に機能した。

その他、シンポジウムも他の研究開発テーマとの情報共有に有効であったとの意見もあった。

なお、推進委員会や WG については参加者が多すぎるために深い議論がしにくかったとの意見もあった。

### (3) ICT の有効な活用

一部の研究開発テーマ（(a1) 制御・通信機器のセキュリティ確認技術、(a2)制御・通信機器および制御ネットワークの動作監視・解析技術の研究開発、(b5) IoT セキュリティ社会実装技術(IoT 機器向けゲートウェイの社会実装に関する研究開発)）では、各社窓口を明確にし、さらにファイル共有やチャットツール等のクラウド環境を整備し、このことが円滑な作業環境につながった。通常、こうしたツールは各社のセキュリティポリシーの観点で導入が円滑に進まないことがあるが、各社で NDA を締結しているため、それをもとに各社のセキュリティポリシーをクリアして活用することができた。

その他の(a3)制御・通信機器およびシステムの防御技術、(a4-2) IoT 機器向け評価検証プラットフォーム技術、(b5-1) IoT セキュリティ社会実装技術でも Web 会議システムが活用され、(b4)セキュリティ人材育成では遠隔地にある慶應義塾大学、情報セキュリティ大学院大学、名古屋工業大学がテレビ会議システムを利用して意思疎通をとる工夫も行われた。

### (4) スケジュール・内容の柔軟な見直しの実施

当初の研究開発計画も適切であったが、外部状況の変化や研究開発の状況に応じて PD 主導による柔軟なテーマの見直し・追加検討の判断を実施したことで社会実装に向けてより効果的・効率的に研究開発が進められた。例えば、もともと研究開始当初時点で b5（IoT セキュリティ社会実装）は存在しなかったが、途中段階で、SIP が目標とする「社会実装」には b5 の枠組みが必須との判断から組み込まれ、これにより社会実装に向けて更なる加速につながった。

前述のように PD と研究責任者とで定期的に開催される進捗会議等でコミュニケーションが密であったことも計画の見直しを円滑に進める上で有効に機能した。

全般として、事業遂行上で常に見直しと最適化を意識して進めたことは、セキュリティ等トレンドが非常に速い ICT 分野においては特に有効であった。そして、途中段階で成果を出しながら研究を進める方策は効果的であった。開発優先度の変更や検討自体の中断、予算配分先の見直し（技術開発から社会実装に配分を変更）等が行われたが、PD の強力なリーダーシップの采配によって計画変更による課題全体の進捗への影響・問題は生じなかった。

### (5) 管理法人による手続面に対する研究者の意見

管理法人（NEDO）が予算管理面で厳格に管理を実施したことで、着実に研究開発を推進できたが、一方で、SIP の特徴を活かした柔軟な対応も期待されていた。管理法人である NEDO との「契約」のもとに研究開発が遂行されていることから、管理法人側では実施計画書上の記載が重視される。事業の方向性の修正に合意しても認識の齟齬（そご）が生じたり、書類による手続が求められたりすることがあり、それを煩雑とする研究者の意見が研究責任者向けアンケート・インタビューから挙がっている。

## 3.2.4 直接的な研究成果（アウトプット）

研究開発活動の目標の達成状況と、得られた直接的な研究成果（アウトプット）は以下である。

### (1) 目標の全般的な達成状況

令和元年度の研究開発計画における技術的目標は、以下のとおりである。
【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
- 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
- 上記の主な技術を社会実装するための認証のあり方と仕組みの検討、共通プラットフォームの実現とセキュリティ人材育成

本課題では、コア技術・社会実装技術それぞれの研究テーマで概ね当初の計画通り目標は達成し、オリパラにおける導入に向けた「先行版」及び本格的な社会実装に向けた「拡大版」の社会実装の取組を並行して進めている。

### (2) コア技術の研究開発成果

本課題では、設備内部のセキュリティ耐性を高める真贋判定技術／動作監視・解析技術／防御技術／IoT 向け暗号実装技術を「コア技術」として研究開発した。主要な成果の内容を以下に示す。

#### 1）きめ細かな完全性証明、大規模システム全体の監視を実現する真贋判定技術（a1）

1 台あたり数十万の大量ファイルからなる数百～数千台レベルのサーバ機器に対応し、機器・ソフトウェアの真正性・完全性の確認を効率的に実現するセキュリティ確認基盤を確立した。これは、きめ細やかな完全性証明を可能とする「信頼の基点」の構成技術及び大規模システム全体の完全性確認を可能とする基盤技術（「信頼の連鎖」）を確立したことによる。また、内部不正や作業誤りによる改変に対しても有効な技術を開発できた。

真贋判定技術における「信頼の基点」「信頼の連鎖」のイメージを図 0-6 に示す

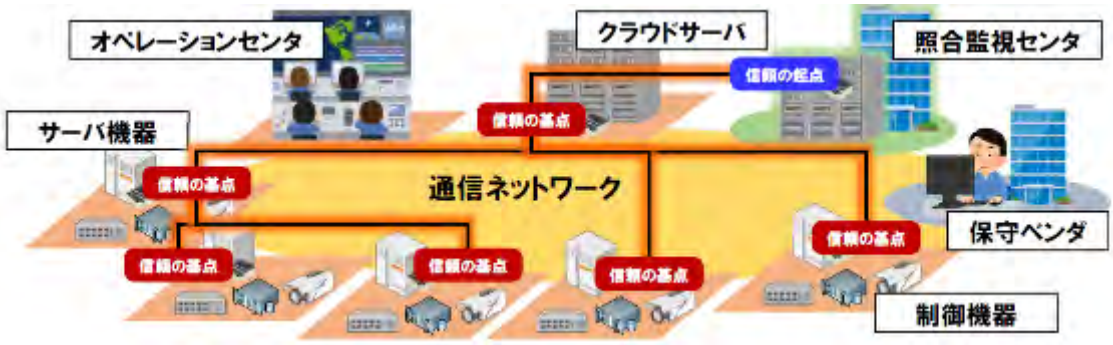


図 3-6　真贋判定技術「信頼の基点」「信頼の連鎖」のイメージ
（出典）内閣府プログラムディレクター　後藤厚宏「SIP 第 1 期令和元年度課題評価 WG PD 自己点検説明資料　重要インフラ等におけるサイバーセキュリティの確保（令和元年 12 月 20 日）」

### 2）仮想ネットワーク、IoT ネットワーク、制御ネットワークに対応した動作監視・解析技術（a2）

動作監視・解析のコア技術となる「①収集・蓄積・分析技術」「②IoT-ゲートウェイと深層学習による監視・分析技術」「③制御 NW センサ技術及び統合解析技術」を確立した。①は物理・仮想合計 100Gbps で収集・蓄積、10Gbps までの通信の解析性能を実現している。NII の実証評価環境において 20Gbps の大容量環境を構築し、不審な通信の検知に成功している。①②③のいずれにおいても不正通信検知率 90%を目標としていたが、達成している。また、情報通信事業者等の実環境にて有効性が確認されている。

①　②③全体像のイメージを図 0-7 に示す。

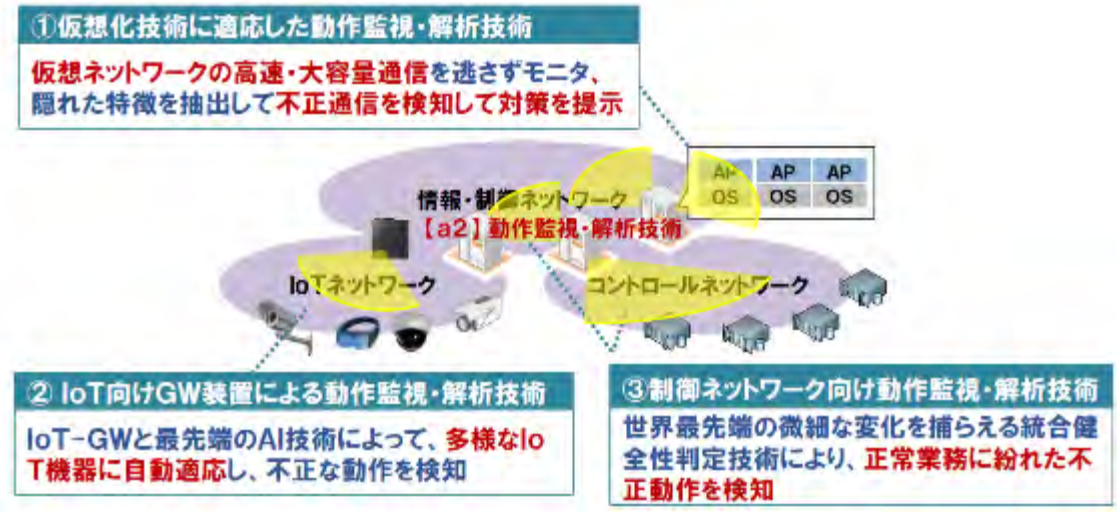


図 3-7　動作監視・解析技術のイメージ
（出典）内閣府プログラムディレクター　後藤厚宏「SIP 第 1 期令和元年度課題評価 WG PD 自己点検説明資料　重要インフラ等におけるサイバーセキュリティの確保（令和元年 12 月 20 日）」

### 3）異常検知時においても安全な運用継続を可能とするシステム防御技術（a3）

攻撃から制御機器を防御しつつ、安全な運転継続を可能とするホワイトリスト技術を開

発した。3 層のホワイトリストを協調動作させることにより、監視端末（HMI）、通信機器、コントローラの異なるレイヤーを監視し、各機器が協調的に動作することで階層防御を可能とした。検知性能を高精度化するとともに影響局所化による運転継続を実現した。ビル・ガスプラントを模擬した環境で評価を行い、その有効性を確認している。

#### 4）世界最小、世界最小消費電力、世界最速の IoT 向け暗号実装技術（a4）

「末端ノードでも公開鍵暗号の自在な活用を可能とし IoT セキュリティ実現に貢献する超低電力暗号実装技術」、「安全な IoT 機器選択を容易に実現可能とするため、暗号鍵生成実装方式の正しさを確認する乱数生成評価技術」を開発した（前倒しで性能目標を達成）。楕円曲線暗号円陣を実装したセキュア暗号ユニット（SCU を開発。末端ノード向けでは 1 ミリワット級の超低電力及び 10 キロゲート級の小面積・低コスト、中間ノード向けでは 10,000 回/秒以上の超高速動作を達成した。

SCU 内蔵マイクロコントローラーの例、及び SCU を搭載する IoT 機器や応用システムの開発向けに提供される開発ツールで、SCU のセキュリティプラットフォームを利用してアプリ開発・評価を行うことが可能な「SCU 評価ボード」を図 3-8 に示す。

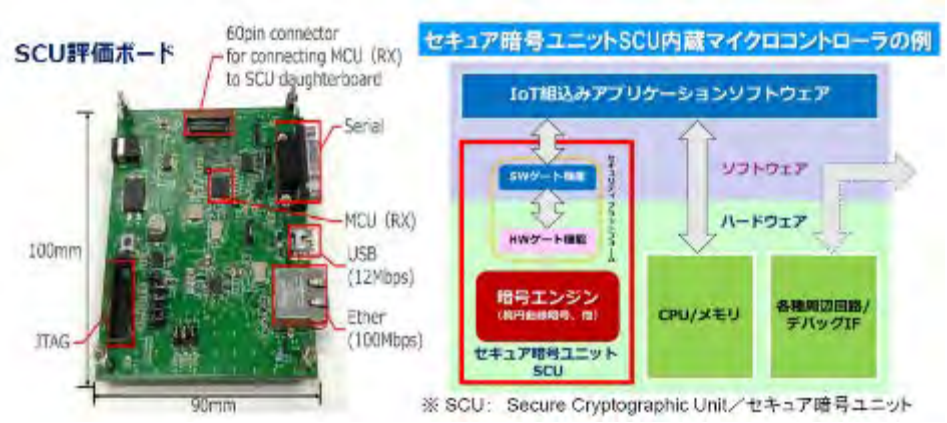


図 3-8　SCU 内蔵マイクロコントローラーの例及び SCU 評価ボード
（出典）内閣府プログラムディレクター　後藤厚宏「SIP 第 1 期令和元年度課題評価 WG PD 自己点検説明資料　重要インフラ等におけるサイバーセキュリティの確保（令和元年 12 月 20 日）」

継続して幅広い分野への実装を目指すため、普及に向けたガイダンス文書を作成している。

### (3) 社会実装技術の研究成果

本課題では、コア技術の社会実装を促進するため、研究開発技術の適合性確認のあり方と仕組みの調査検討／情報共有プラットフォーム技術の整備／評価検証プラットフォーム技術開発／サイバーセキュリティ人材育成／IoT セキュリティ社会実装技術開発を実施した。主要な成果の内容を以下に示す。

#### 1）研究開発技術の適合性確認のあり方と仕組みの調査検討（b1）

欧米のセキュリティ技術調査に基づき、(a)技術と海外規程類とのマッピングを実施した。研究開発技術の適合性を確認し、国際普及に向けた検討等を実施し、コア技術開発の側面

支援を実施した。

### 2）緊急度の高い脅威情報を迅速に配信する情報共有プラットフォーム技術（b2）

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、ログ分析・バックドア解析、モデル解析の結果を、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情報共有プラットフォーム技術を開発した。なお、プラットフォーム技術は日立システムズ社が国際標準 STIX/TAXII 準拠の国内事業者向けサービス「SHIELD」として 2018 年に商用化している。重要インフラ等関連組織が協力し、長期間の試行運用を実施している。

### 3）評価検証プラットフォーム技術の整備（b3）

コア技術として開発した「動作監視・解析技術(a2)」を重要インフラ等事業者に早期適用するための評価手順、検証環境等を整備し、評価検証を実施した。なお、動作監視・解析技術(a2)のうち特に「③制御 NW センサ技術及び統合解析技術」と協力して製品開発を行い、日立製作所が HAD（Hitachi Anomaly Detector）として 2017 年に製品化した。

### 4）重要インフラ等での実践力を養うサイバーセキュリティ人材育成（b4）

重要インフラ等における OT（制御技術）運用者がサイバーセキュリティの方策検討やインシデント対応等を適切に実施するための講義・演習教材やシステムを開発した。具体的には、セキュリティ人材育成のためのカリキュラム・講義・演習教材・e-learning 環境を開発し、既に 40 を超える組織（電事連、NTT-ME、日立等多数）に配布され、人材育成を推進している。重要インフラ等事業者に対しても配布し、育成試行をしており、事業者のニーズを確認の上フィードバックを行った。また、経営者への重要インフラ等へのセキュリティの理解と意識啓発も必要との観点から、新たに経営者向けの教材も作成している。

また、セキュリティインシデント対応を PC 上で疑似的に体験できる演習システムを開発し、企業に PC を持ち込んでクローズな環境で演習を利用することを可能とした。

人材育成のための取組イメージを図 3-9 に示す。教材を更新するための仕組み、と指導者コミュニティの整備が進んでいる。

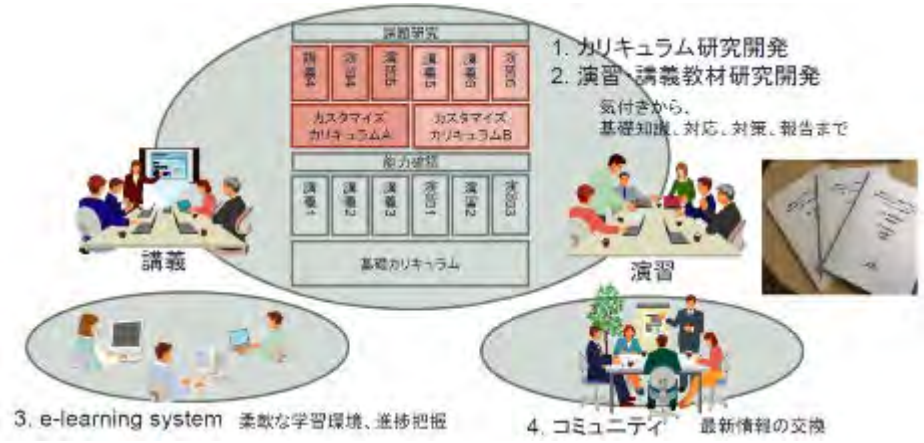


図 3-9　人材育成のための取組イメージ

（出典）内閣府プログラムディレクター　後藤厚宏「SIP 第 1 期令和元年度課題評価 WG PD 自己点検説明資料　重要インフラ等におけるサイバーセキュリティの確保（令和元年 12 月 20 日）」

なお、令和元年度に東京（令和 2 年 1 月 24 日）、大阪（令和 2 年 2 月 7 日）に実施された「SIP／重要インフラ等におけるサイバーセキュリティの確保　シンポジウム 2019」においても、来場者向けに人材育成基礎講座（情報セキュリティ人材育成トライアルコース（ProSec））を開講している。

#### 5）IoT セキュリティ社会実装技術（b5）

IoT 技術活用ニーズの急速な高まりを踏まえ、IoT 機器から出力されたログを利用した攻撃検知アルゴリズムを確立した。また、a4 及び a2②の社会実装促進のため、社会実装促進シナリオの策定、個別適用・SI 導入・IoT 向けセキュリティ監視サービスの実現に向けた評価・課題抽出を実施した。また、当初計画にない、工場の生産ラインにおける IoT セキュリティ監視の社会実装を達成している。

### (4) 情報発信

2016 年度より毎年プロジェクト全体でのシンポジウムを開催し、プレゼンスの向上とともに成果の情報発信に努めた。また、PD 自らが海外訪問した際に積極的に SIP 活動をプレゼンし、国際的にアピールした（イスラエル、シンガポール、北欧、米国等）。

本課題の情報発信活動として、令和元年度に開催したシンポジウムを表 3-16 に示す。

表 3-16　重要インフラ等におけるサイバーセキュリティの確保に関する情報発信
（令和元年度のシンポジウム）

| 年月日 | 名称 | 主催等 | 概要 |
|---|---|---|---|
| 令和 2 年 1 月 24 日（東京） | SIP／重要インフラ等におけるサイバーセキュリティの確保シンポジウム 2019（東京）<br>―世界で最も安心・安全な社会基盤の確立を目指して― | 内閣府、NEDO | 本課題を推進する各研究機関・企業から、研究テーマ別の技術成果の講演の他、成果を分かりやすく説明したデモ展示、サイバーセキュリティ技術知識を高める人材育成基礎講座等（無料）を実施した。 |
| 令和 2 年 2 月 7 日（大阪） | SIP／重要インフラ等におけるサイバーセキュリティの確保シンポジウム 2019（大阪）<br>―世界で最も安心・安全な社会基盤の確立を目指して― | 内閣府、NEDO | 本課題を推進する各研究機関・企業から、研究テーマ別の技術成果の講演の他、成果を分かりやすく説明したデモ展示、サイバーセキュリティ技術知識を高める人材育成基礎講座等（無料）を実施した。 |

### (5) 論文・知的財産

過去 5 年間の論文数は全 132 件（うち査読あり 85 件）である。

対外発表ルールを整備し、実施者による自発的・積極的な対外発表を促すとともに、研究

開発成果の早期切り出しを行い製品化とそれに伴う報道発表を推奨しており、講演（50 件)、展示（11 件)、発表（26 件）等成果の普及に努めている。

社会実装技術についてはオープン戦略とし、開発した情報共有デザインガイド（b2)、適用ガイドライン（b3[6])、人材育成教材（b4）は広く公開し普及を図った。

表 3-17　サイバーセキュリティに関する論文数

| | | | 発表年 | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 5 年合計 | | | | | |
| | | | | 2015 | 2016 | 2017 | 2018 | 2019 |
| 合計 | | | 132 | 13 | 22 | 30 | 42 | 25 |
| | 査読あり合計 | | 85 | 13 | 13 | 23 | 25 | 11 |
| | | 英文 | 73 | 10 | 10 | 22 | 22 | 9 |
| | | 和文 | 12 | 3 | 3 | 1 | 3 | 2 |
| | | その他 | − | − | − | − | − | − |
| | 査読なし合計 | | 47 | − | 9 | 7 | 17 | 14 |
| | | 英文 | 6 | − | 1 | 1 | 2 | 2 |
| | | 和文 | 41 | − | 8 | 6 | 15 | 12 |
| | | その他 | − | − | − | − | − | − |

（注 1）令和元年 12 月末実績。発表年は年度ではなく暦年である。
（注 2）「査読あり」については学術誌での発表論文以外に学会発表・予稿集等も一部含んでいるが、「査読なし」については学会発表・予稿集等は原則として除いている。

本課題における知財戦略として、特許に関しては、知財委員会を通じてチームごとの知財管理状況を把握・確認し、関連組織でアウトプット（技術）を活用しやすい管理・連携方法を常時検討して整理を実施した。本課題の研究開発技術の特性上、知財戦略は念入りに検討を行い、セキュリティのコア技術はクローズ戦略を基本とし、個々の技術の特徴を精査しながら各社にて出願、SIP 終了後は各者の製品開発で活用することとした。

みなし取下げを除いた出願年度別の特許出願件数及び登録件数（ファミリー単位で集計）は表 3-18 のとおりである。7 件の国内出願と、6 件の海外を含む出願がある。うち、1 件が国内で登録に至っている。

表 3-18　サイバーセキュリティに関する特許数

| | | 出願年度 | | | | | |
|---|---|---|---|---|---|---|---|
| | | 5 年合計 | | | | | |
| | | | 2015 | 2016 | 2017 | 2018 | 2019 |
| 出願 | 合計 | 13 | − | − | 5 | 3 | 5 |
| | 国内のみ | 7 | − | − | − | 3 | 4 |
| | 海外含む | 6 | − | − | 5 | − | 1 |
| | PCT | 7 | − | − | 2 | 4 | 1 |
| | 米国 | 2 | − | − | 1 | 1 | − |
| | 欧州 | 2 | − | − | 2 | − | − |

[6] セキュリティ対策適用ガイドラインとして「サイバー攻撃から重要インフラを守る-セキュリティ製品導入のための手引き-」（令和 2 年 1 月）を広く公開している。

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 中国 | 1 | － | － | 1 | － | － |
| | 韓国 | － | － | － | － | － | － |
| 登録 | 日本 | 1 | － | － | － | － | 1 |
| | 米国 | － | － | － | － | － | － |
| | 英国 | － | － | － | － | － | － |
| | ドイツ | － | － | － | － | － | － |
| | フランス | － | － | － | － | － | － |
| | 中国 | － | － | － | － | － | － |
| | 韓国 | － | － | － | － | － | － |

（注）令和元年 12 月末実績。みなし取下げを除いた出願年度別の特許出願件数及び登録件数をファミリー単位で集計。

## 3.2.5　現在・将来の波及効果（アウトカム）

研究終了時である現時点の目標の達成状況と波及効果、将来（短期・中期・最終）に期待できる波及効果については次のとおりである。

### (1) 目標の全般的な達成状況

令和元（2019）年度の研究開発計画における社会的な目標及び産業面の目標は、以下のとおりである。

【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
- 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等システムの優位性をアピールする

【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。
- 2020 年東京オリンピック・パラリンピック競技大会の運営を支える主要な重要インフラ等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。
- 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等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。
- 民生機器分野でも今後ますます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。

重要インフラ等事業者への展開を先行版として、2020 年東京オリンピック・パラリンピック競技大会の安全な開催に貢献するために首都圏近郊の主要インフラへの社会実装を先行して実施した。2020 年東京オリンピック・パラリンピック競技大会における貢献が期待されている。

2020 年東京オリンピック・パラリンピック競技大会の開催後、「拡大版」の取組の先において、国内の他重要インフラ等事業者等への展開を推進し、重要インフラ等輸出の競争力強化、セキュリティ強化された機器製品の自給率工場と海外展開、IoT システムのビジネス拡大が期待されている。

先行版・拡大版の取組イメージを図 3-10 で示す。

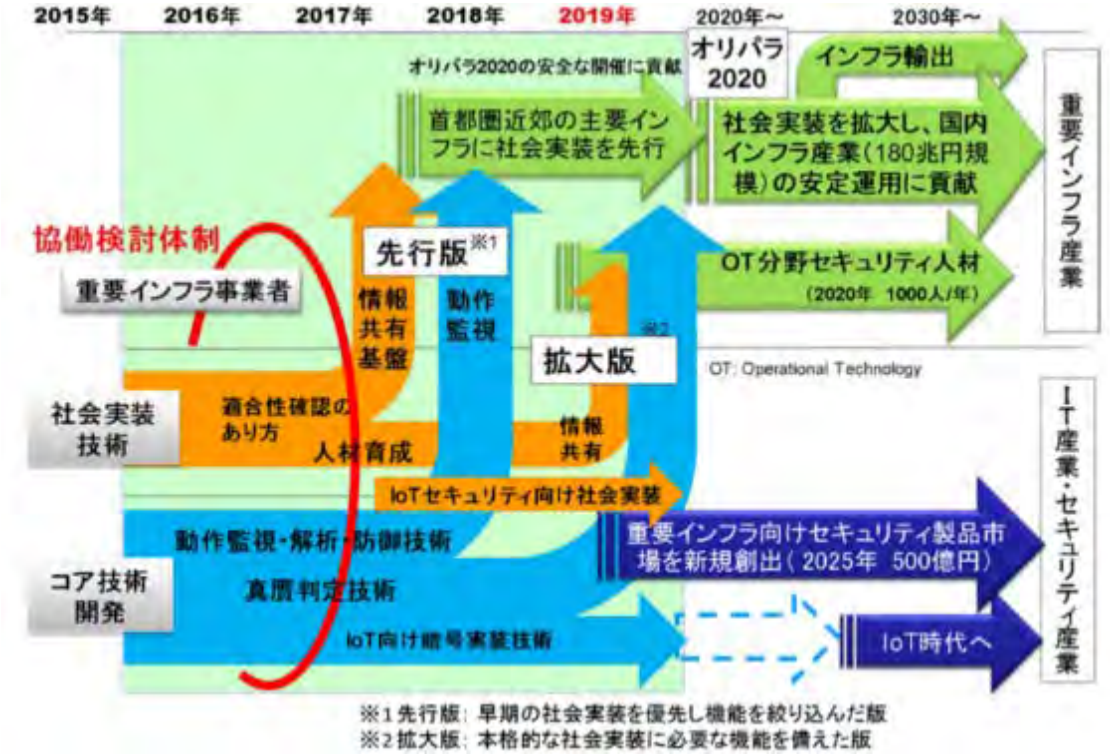


図 3-10　先行版・拡大版の展開イメージ

（出典）内閣府プログラムディレクター　後藤厚宏「SIP 第 1 期令和元年度課題評価 WG PD 自己点検説明資料　重要インフラ等におけるサイバーセキュリティの確保（令和元年 12 月 20 日）」

## (2) 国内重要インフラ等の安定運用

本課題の成果は国内のインフラ産業（180 兆円規模）の安定運用に貢献することが期待されている。

まずは「先行版」として首都圏近郊の主要インフラに社会実装が実施されており、2020 年開催の東京オリンピック・パラリンピック競技大会の安全な開催を支える重要インフラのサイバーセキュリティ確保に貢献することが見込まれる。ただし、本課題の成果は、重要インフラ等のネットワークの全てのセキュリティをカバーできているわけではないことには留意する必要がある。

## (3) 重要セキュリティ製品市場の新規創出

重要インフラ等向けセキュリティ製品市場の新規創出に向けて、表 3-19 に示すように、既に一部で導入、製品化が進められている。

表 3-19　導入・製品化の状況

| 研究開発成果 | 状況 |
|---|---|
| (a1)真贋判定技術 | 商用製品化を行い、2018 年度末までに情報通信分野において初の商用導入に成功。 |
| (a2)①動作監視・解析技術（仮想 NW） | 情報通信事業者の重要インフラ等設備のオペレーションシステムに導入検討開始。 |
| (a2)②動作監視・解析技術（IoT 機器）+(b5) | 情報通信事業者の重要インフラ等設備のオペレーションシステムに導入開始。<br>三菱電機の自社工場での試行を経て、工場向けサービスとしての検討開始。 |
| (a2)③動作監視・解析技術（制御 NW）+(b3) | 日立製作所が HAD（Hitachi Anomaly Detector）として製品化(2017/10/2)。<br>重要インフラ等事業者の重要オペレーションシステムに導入決定。 |
| (a3)防御技術 | アラクサラ社が通信機器部分を製品化し、電力事業者へ導入。 |
| (a4-2) IoT 向け乱数生成技術+(b5) | パナソニックの自社工場での試行を経て、工場向けサービスを検討開始。 |
| (b2)情報共有プラットフォーム | 国際標準 STIX/TAXII 準拠の国内事業者向け情報共有ツールを開発（日立システムズ社が SHIELD 情報共有サービスとして商用化(2018/5/30)。<br>重要インフラ等関連組織での長期間の試行運用・評価実施により、情報共有組織強化に貢献。 |

### (4) インフラ輸出への貢献

コア要素技術（a1~a4）は重要インフラシステムをパッケージとして海外輸出する際にサイバーセキュリティ技術も付加価値として貢献することを想定している。

海外展開は国内での社会実装・普及後に期待され、特にオリパラの安心・安全な開催終了後、その実績を基に重要インフラ等輸出の競争力強化を目指している。

他にもサイバーセキュリティ人材育成のための成果を活かし IEC62443（制御システムのセキュリティ）、NICE Cybersecurity Workforce Framework （NIST. SP.800-181）を整合させ、内容をより具体化・英語化の上でアジア諸国（インドネシア　ミャンマー、タイ等）へ展開することが検討されている。

### (5) サイバーセキュリティの社会実装を促進する人的ネットワーク形成

推進委員会や WG、進捗会議等の会議体は、各府省庁、重要インフラ等事業者、情報連携組織、学識経験者等により構成されており、今後の社会実装を進めていく中で必要となるステークホルダーが参加した。これにより、SIP 終了後も継続してネットワークを活用し社会実装を円滑に進めていくことを可能とする人的ネットワークが構築された。また、これらの

会議体を通じて、新聞社、放送事業者との新たな関係性を構築したことにより、将来的なユーザーの拡大可能性確保にも繋がることが期待できる。

## (6) 重要インフラ等事業者における人材の育成

### 1) 人材育成プログラムの展開

本課題で開発した人材育成プログラム（運用技術者向けのセキュリティ人材育成のためのカリキュラム及び講義・演習教材）は、今後、大学においてエクステンションコースとして人材育成の実施や教材を配布した組織においても社内教育等が実施すること等に活用されることが期待される。また、経営者向けのテキストも作成中であり、経営者のセキュリティへの意識と理解が高まることで企業内での広まりも期待される。

また、並行して、教材を更新するための手順と指導者によるコミュニティの整備も進めており、SIP 終了後も継続的に定常的にカリキュラム・教材開発が行われることで、今後は年間 1000 人程度規模のセキュリティ人材育成がなされることが想定されている。

### 2) セキュリティ意識の向上

本課題を通して重要インフラ等事業者と連携をすすめる中で、重要インフラ等事業者側のサイバーセキュリティに対する意識が大きく変化した。SIP 開始当初と比較してセキュリティに対する認識が格段に向上したことは本課題における大きな成果であると言える。

従来の IT 人材以外にも、重要インフラ等事業者内の OT 人材へとサイバーセキュリティの関心が広まり、さらにユーザー企業（新聞社、ゼネコン、プラントメーカー）へも波及しつつある。重要インフラ等事業者としては、オリパラのタイミングでオペレーションの混乱は絶対に避けたいというニーズもあったほか、所管省庁等への説明の必要性等、サイバーセキュリティへの関心が高まっていた。

## (7) SIP 他課題との連携

SIP 他の課題間連携としては、本課題と SIP「自動走行システム」との連携がある。本課題でダイナミックマッププラットフォームのセキュリティ要求事項・プラットフォームの有用性に関する検討・評価を実施したことで、SIP「自動走行システム」の研究開発にも貢献していた。この課題間連携による成果は、今後のインフラ維持管理などにおいても広く活用される可能性がある。

SIP「自動走行とシステム」の課題間連携のイメージを図 3-11 に示す。

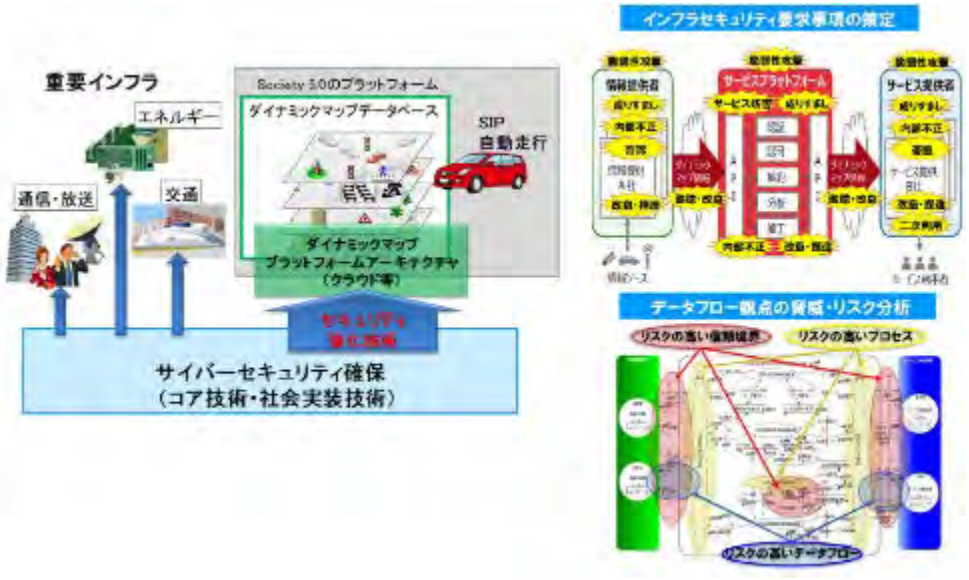


図 3-11　SIP 自動走行との課題間連携のイメージ
（出典）内閣府プログラムディレクター　後藤厚宏「SIP 第 1 期令和元年度課題評価 WG PD 自己点検説明資料　重要インフラ等におけるサイバーセキュリティの確保（令和元年 12 月 20 日）」

## 3.2.6　改善すべきであった点と今後取り組むべき点

### (1) 改善すべきであった点

容易に結論が出ないとは思われるものの、公的資金を活用した研究開発として、どのように取り組みや成果を開示することが適切かは課題であった。本課題は、サイバーセキュリティ技術を取り扱っているという特性上、サイバーアタックを行う者（クラッカー等）からの攻撃を避けるため、参画あるいは導入先である重要インフラ等事業者が公開されておらず、外部からの評価が困難であった。SIP のような外部有識者を評価者として予算配分を決定するような技術開発に関して、管理法人と各社の間には NDA が締結されているが、その中に評価関係者に限定した開示事項を定めておくことも考えられた。

また、開始当初の研究開発計画の段階から、あるいはその後も段階的に、重要インフラ等事業者の巻き込みをさらに進めた体制を構築することも考えられた。本課題においてはユーザーとなる重要インフラ等事業者が当初から会議体（推進委員会、WG 等）に参画していることが特徴であり、研究開発が行われたコア要素技術を重要インフラ等事業者において実証試験の打診までは円滑に行うことができた。しかし、重要インフラ等事業者は、会議体には参画していたものの、研究開発体制に参画していないこともあり、研究開発実施体制に含まれるサイバーセキュリティ技術を有する企業からみて責任分界の交渉が難しくなった面がある。

また、人材育成は研究開発テーマの 1 つとして挙げられているが、これにとどまらず、研究開発をしながら人材育成を強化するという視点をもっと取り入れることも考えられた。国内にサイバーセキュリティ分野の専門的な人材が不足しており、我が国としてやや弱い領域となっている。

なお、本課題に固有ではないと思われるが、SIP の次年度予算確定時期と民間企業内での

次年度計画の決定時期とに乖離があるため、企業側でのリソース確保が困難であるという意見もあった。多くの民間企業において次年度の社内計画は年内～1 月に決定されるが、SIP で次年度の予算の大枠が判明するのは 1 月頃、最終的な確定は 3 月である。さらに、SIP での次年度予算決定において全体予算が増額された場合の検討は年度明け 4 月からとなる。このため、民間企業の年度計画スケジュールと整合しておらず、主に人員配置等リソース確保の面での困難が生じた。

### (2) 今後取り組むべき点

技術的な目標を達成し、一部導入も実現することができたが、今後は、国内重要インフラ等事業者や海外展開に向けてビジネスモデルを構築し、マーケットの評価を高めていくことが必要となる。サイバーセキュリティについては継続的な研究開発が必要であり、導入するだけではなく、その後の継続的な維持管理や運用も重要である。また人材育成についても、教育カリキュラム、演習教材やシステム等の維持管理や運用についても継続的に取り組んでいく必要がある。

国内重要インフラ等事業者に対して、どのようなインセンティブやルール（法令文書・業界のガイドラインの改定、セキュリティ技術の品質、イニシャル・ランニングコスト等）でサイバーセキュリティ技術を売り込んでいくかについて、ユーザー視点かつ具体的に議論していく必要がある。国内重要インフラ等事業者は、既に一定レベルのサイバーセキュリティ技術を導入していると考えられるため、本課題の研究開発成果が、いかに高精度でサイバーアタックを検知可能なものなのか、事業者側の認知・理解を進めていくことが重要である。また、業界ガイドラインの勧告事項に本課題の研究成果に関する機能を追記するといった方策も考えられる。セキュリティのような分野では事前に関係省庁で出口について協議して、例えば調達要件等を含めて検討すべきである。

まずは国内インフラ事業者への導入を進めていくことにより、海外展開として、重要インフラ等とサイバーセキュリティをパッケージ化して輸出することにつながると期待される。本課題の研究開発成果が、重要インフラ等向けに製品化・事業化され、重要インフラ等事業者に導入されているのか、あるいは導入される動きがあるのかについては、内閣府による追跡的なフォロー及び評価・フィードバックが必要である。

国際展開については、重要インフラ等とサイバーセキュリティ技術について、人材育成も加えて、パッケージ化して輸出するなどの具体的な方針を検討する必要があり、企業・個社を超えた取り組みが必要である。この点についても内閣府による追跡的なフォロー及び評価・フィードバックが必要である。