戦略的イノベーション創造プログラム（SIP）

IoT 社会に対応したサイバー・フィジカル・セキュリティ

研究開発計画

2022年4月 25 日

内閣府

科学技術・イノベーション推進事務局

目次

＜添付資料＞

〇資金計画及び積算

研究開発計画の概要

1. 意義・目標等

IoT は、Society 5.0[1]の基盤技術であり、社会インフラ、産業システム、生活環境、自然環境等のフィジカル空間に埋め込まれた IoT 機器が、多様なネットワークを介してクラウド等のサイバー空間と連結され、AI に代表される高度な知識処理やビッグデータとしての分析・解析処理と連携することにより、様々な付加価値やサービスを創出し、フィジカル空間である経済社会に多大な恩恵をもたらすと期待されている。

一方、サイバー攻撃の対象は急激に拡大し、攻撃の手法も著しく高度化している。特に、産業社会や家庭生活に新たな価値創造をもたらす IoT の普及・拡大に伴い、サイバー攻撃の脅威は、サイバー空間だけでなくフィジカル空間を合わせた、あらゆる産業活動に潜むようになっている。

また、製品やサービスを製造し流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題も顕在化しつつあり、グローバルなサプライチェーンにおいてサイバーセキュリティ対策の強化が求められている。今後は一定の水準のセキュリティ要件を満たさない事業者、製品、サービスがグローバルな調達要件からはじき出される恐れがあり、輸出の大部分を占める製造業の参入機会を確保することが重要な課題となる。

このため、セキュアな Society 5.0 の実現に向け、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、IoT システム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証を行う。実証を通じて有効性を確認し、実稼働するサプライチェーンに組み込み実用化する。本基盤の社会実装を推進することで、サイバー脅威に対する IoT 社会の強靭化を図り、Society 5.0 の実現によりもたらされる約 90 兆円の価値創出[2]を支える。

2. 研究内容

中小企業を含む大規模サプライチェーンが多数重層構造となるスケール（構成組織数が1万以上）に対応でき、IoT システム・サービス（多様な IoT 機器数が数千以上）及びサプライチェーンの各構成要素（人、組織、製品、システム、サービス、データ等）のセキュリティ確保を実現する『サイバー・フィジカル・セキュリティ対策基盤』の研究開発を進める。本基盤は、IoT 機器やサプライチェーンの各要素について、セキュリティ確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーン（連鎖）を構築することで、IoT システム・サービス及びサプライチェーン全体のセキュリティを実現するものであり、その主な研究開発項目は、以下の 3 つである。

（A）「信頼の創出・証明」技術の研究開発

個々の IoT 機器やサービスのセキュリティを強化し、多様な IoT システム・サービスやサプライチェーン全体のセキュリティ確保を実現する上で必要な信頼創出・証明技術の多角的な研究開発を行う。

（B）「信頼チェーンの構築・流通」技術の研究開発

---

[1] Society 5.0 とは、第 5 期科学技術基本計画（2016 年 1 月 22 日閣議決定）で提唱された概念であり、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）のこと。

[2] 経済産業省 産業構造審議会 新産業構造部会『新産業構造ビジョン』より。
https://www.meti.go.jp/shingikai/sankoshin/shinsangyo_kozo/pdf/017_05_00.pdf

多様な社会インフラやサービス、幅広いサプライチェーンのセキュリティを確保するため、IoT システム・サービスや調達・構築に関わるサプライチェーンで「信頼チェーン」を構築し、必要な情報をセキュアに流通させる技術を研究開発する。

（C）「信頼チェーンの検証・維持」技術の研究開発

「信頼チェーン」を構築した IoT システム・サービス及びサプライチェーンにおいて、その「信頼チェーン」が安全に運用されていることを検証し、維持する技術を研究開発する。

3. 実施体制

後藤厚宏[3]プログラムディレクター（以下「PD」という。）は、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、専門家・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。）を活用し、公募により選定した研究責任者により研究開発を推進する。同法人のマネジメントにより、各研究テーマの進捗を管理する。PD は必要に応じてサブ PD をおき、研究開発の内容や進捗状況の管理について、PD を補佐させるものとする。また、本プロジェクトの活動状況や成果を広く周知し、産業への周知・浸透の促進を図るための取組を企画し、実施する委員会やワーキンググループ（WG）等を適宜設置する。

4. 知財管理

知財委員会を NEDO または選定した研究責任者の所属機関（委託先）に置き、各委託先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、調整を行う。

5. 評価

ガバニングボード[4]による毎年度末の評価の前に、研究責任者による自己点検、及び、必要に応じ外部有識者の意見を参考にして、PD と管理法人による自己点検を実施する。

6. 出口戦略

技術開発や実証実験にユーザの要求事項を反映できるよう、研究開発チームと課題認識のあるユーザ企業との連携体制をプロジェクト当初から構築し、参画企業による主体的な製品化・事業化を推進する。中小企業を含むサプライチェーン全体及びその構成企業の IoT システム・サービスへの導入を促進し、2030 年までに中小企業の 50%に本基盤の成果の導入を目指す。

本プロジェクトは、SIP 資金と参画企業の主体的な貢献により推進する。研究開発成果については、参画企業が主体となって製品化を進め、各産業分野への導入を推進する。一部の成果は、IP（知的財産権）化して関連するベンダにライセンス供与し、その普及を目指す。また、より広く本プロジェクトの成果を普及させるため、一般の認知、理解を高めるイベント（シンポジウムやセミナー、国際会議など）にも取組む。

本プロジェクトに関連するプロジェクトとしては、SIP 自動運転（システムとサービスの拡張）、SIP スマート物流サービス、等を想定する。

---

[3] 情報セキュリティ大学院大学 学長・教授

[4] ガバニングボードは、SIP の着実な推進を図るため、その重要事項を審議・検討することを目的として開催される。

1. 意義・目標等

(1) 背景・国内外の状況

Society 5.0 とは、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステム（以下「サイバー・フィジカル高度融合システム」という。）により、経済発展と社会的課題の解決を両立する、人間中心の社会であり、IoT や AI 等の先端技術を用いて全ての人とモノがつながり、様々な知識や情報が共有され、新たな価値観が生まれる社会をさす。

さらに、Connected Industries[5]を始めとするネットワーク化の進展は、従来とは異なる、より柔軟で動的なサプライチェーンの構成を可能とし、新たな付加価値を生み出す機会を増大させる。反面、サイバーセキュリティの観点では、攻撃の対象点が増加し、防御すべき範囲が拡大することになる。サイバー攻撃には、セキュリティが脆弱なポイントを一か所見つけるだけで侵入することが可能という特徴があるため、攻撃者の視点で見ると、今まで以上に侵入が容易になりつつあると考えられる。

加えて、サイバー攻撃の脅威は日々増大しており、今後、IoT 機器の爆発的な普及・拡大[6]を伴って発展することが想定される Society 5.0 の社会では、その脅威はサイバー空間のみならず、フィジカル空間に対しても深刻な影響を及ぼしうる。これまでも、脆弱な IoT 機器を踏み台とした大規模な DDoS 攻撃により重大なネットワーク障害が発生するなど、実際に甚大な被害を招く事例が散見されている。

あるセキュリティベンダーの調査では、世界のサイバー犯罪による経済損失は6000億米ドル（世界の GDP の 0.8%相当）[7] にも上ると言われている。

また、サプライチェーンの観点では、スマートフォンのファームウェアに、ユーザの個人情報等を国外に送信する機能が埋め込まれる等、製品やサービスを製造し流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題が顕在化しつつある。

サプライチェーンリスクに対して、米国では、国防総省の調達に NIST SP800-171 への遵守が求められるなど、サイバーセキュリティ対策の強化が進められている。日本のサプライチェーンに対しても同様のサイバーセキュリティ対策が求められつつあり、今後は一定の水準を満たしていなければ取引ができなくなるなど、セキュリティ要件を満たさない事業者、製品、サービスは、グローバルなサプライチェーンにおいて淘汰されるといった影響も懸念される。

Society 5.0 の社会においては、その実現段階から中小企業を含むサプライチェーンと多様な IoT システム・サービスで構成されるサイバー・フィジカル高度融合システム全体に高いサイバー攻撃耐性を備えることが必要となる。そのためには、Society 5.0 を構成する各要素（人、組織、製品、システム、サービス、データ等）が複雑に繋がり、多様化した社会が構成されたとしても、 設計・製造・運用といった各段階において、未知のサイバー攻撃が発生することも想定した上で、それらに備える高度なセキュリティ対策を組み込むことが、サイバー・フィジカル高度融合システム全体のセキュリティ確保の中で不可欠となる。

(2) 意義・政策的な重要性

Society 5.0 や Connected Industries を推進するに当たり、しかるべきセキュリティ対策を施し、安全・安心

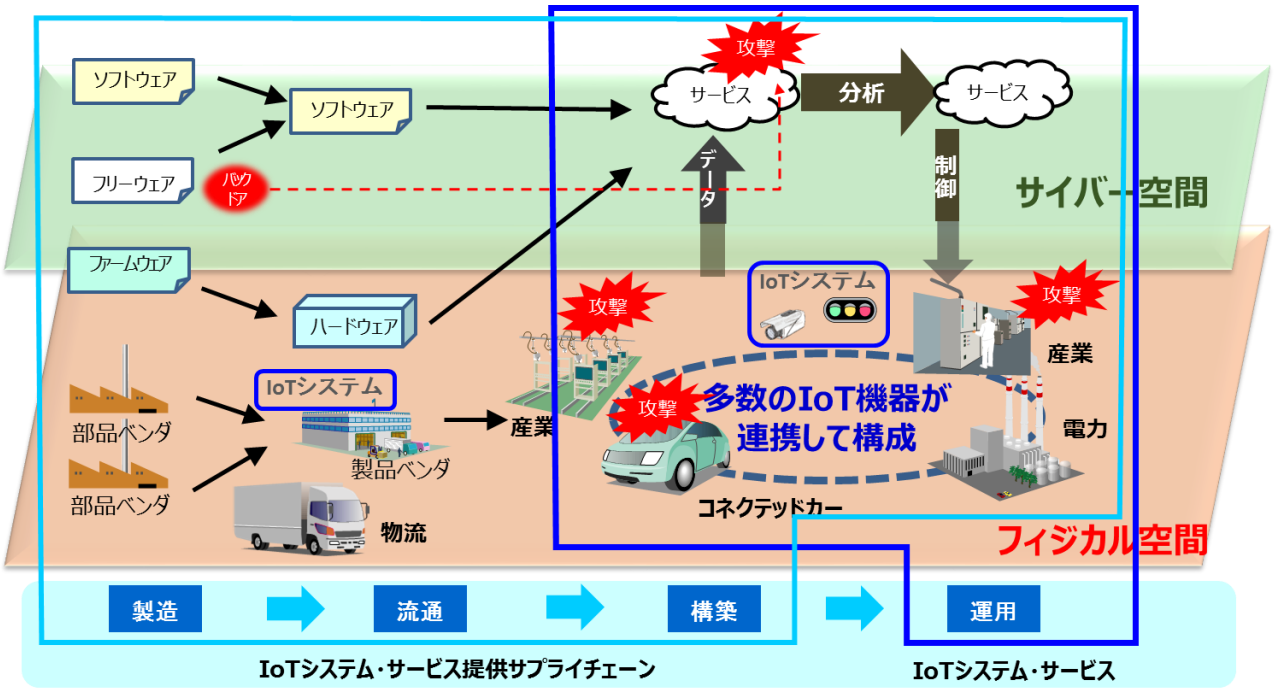
---

[5] Connected Industries とは、2017 年 3 月に経済産業省が発表した日本の産業が目指す姿を示すコンセプトであり、様々なつながりにより新たな付加価値が創出される産業社会のこと。

[6] IHS Technology の推定では、インターネットにつながる機器は、2016 年時点で 173 億個であり、その後も 15.0%の年平均成長率で増大し、2020 年は約 300 億となる見通しである

[7] 2018 年 2 月に発表された McAfee LLC と CSIS の共同レポートより。

を確保することが重要であるが、このような社会は、多様な要素（人、組織、製品、システム、サービス、データ等）が相互に連携・融合して構成されることから、一企業として取組むセキュリティ対策だけでは限界がある。すなわち、各企業が個別に、各製品・サービス等において企画・設計段階からセキュリティバイデザインの観点を踏まえてサイバーセキュリティ対策を考慮したとしても、それだけでは十分とは言えない。こうした対策に加え、多種多様な IoT 機器で構成される IoT システム・サービス全体、関連企業、取引先等、製造や流通を含むサプライチェーン全体として、ビジネス活動のレジリエンスまで考慮に入れ、セキュリティ対策に取組むことや、個々の主体が厳格に管理することが難しいデータの流通のセキュリティも含めて、サイバーセキュリティを確保する必要がある（図表 1-1）。



図表１－１．　Society 5.0 実現に向けたサイバー・フィジカル高度融合システムの課題

また、前述の世界のサイバー犯罪による経済損失の調査から、同割合の損失が日本市場で発生すると仮定した場合、現在の GDP の 0.8%は3兆円規模になると見込まれるため、日本の経済発展の観点からも、サイバー攻撃を未然に防ぐサイバーセキュリティ対策は重要である。

一方、2017 年 12 月 8 日に閣議決定された「新しい経済政策パッケージ」では、3 章のサイバーセキュリティ対策の強化において、IoT セキュリティ強化と中小企業のサイバーセキュリティ対策の必要性が示されている。本プロジェクトは、IoT 時代において IoT システム・サービスや中小企業を含むサプライチェーン全体のサイバーセキュリティ強化を推進する重要な取組である。

このように、サイバー空間とフィジカル空間を高度に融合させたシステムによって実現する Society 5.0 において、世界で最も安全な社会基盤として、スマート家電等の一般消費者向けの機器から産業用システムまで、多様な IoT 機器・システム・サービスのセキュリティを確保できる『サイバー・フィジカル・セキュリティ対策基盤』を確立することは、ICT 産業の高度化とそれに伴う社会の発展に不可欠である。

このため、『サイバー・フィジカル・セキュリティ対策基盤』の実現に必要となる世界最先端のコア技術の開発を行って、IoT システム・サービスの調達・構築に関わる中小企業を含むサプライチェーン全体のセキュリティを確保し、多様なサービスのセキュリティ維持を実現する。その効果を各産業分野[8]で実証することで、製品・サービスのライフサイクル全体のセキュリティ確保に要するコストの削減とセキュリティ品質の向上を通じて、当該産業の国際競争力強化に貢献する。

『サイバー・フィジカル・セキュリティ対策基盤』の確立により、Society 5.0 の実現によりもたらされる約 90 兆円の価値創出を支える。

(3) 目標・狙い

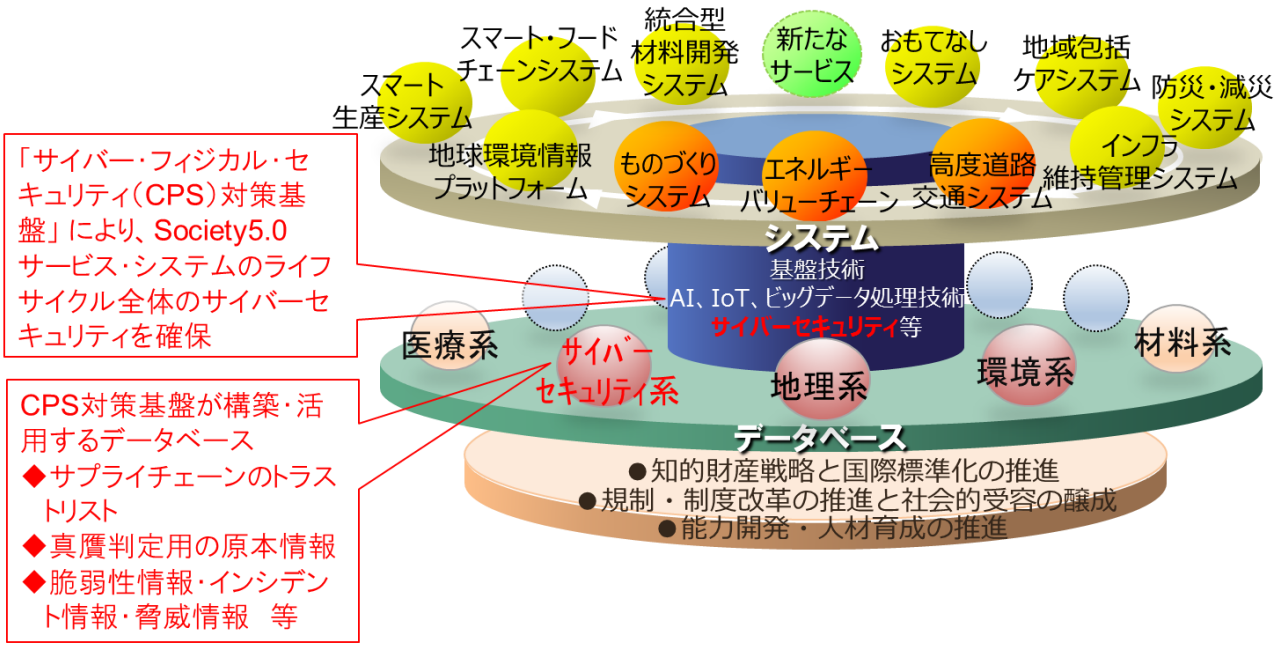
① Society 5.0 実現に向けて

- サイバー空間とフィジカル空間を高度に融合させたシステムによって実現する Society 5.0 において、本プロジェクトでは、世界で最も安全な社会基盤『サイバー・フィジカル・セキュリティ対策基盤』により、Society 5.0 サービス・システムのライフサイクル全体のサイバーセキュリティを確保する(図表 1-2)。
  - Society 5.0 の社会を構成する各要素(人、組織、製品、システム、サービス、データ等)が多様化し、サプライチェーンに重層的に多数の企業が関わる状況であっても、漏れなくセキュリティを行き届かせることを目標とする。
  - サイバー攻撃の進化は留まることがなく、Society 5.0 の社会ではその脅威はサイバー空間のみならず、フィジカル空間に対しても深刻な影響を及ぼしうる。この状況を見据え、製品、システム、サービスの運用・提供段階において未曾有のサイバー攻撃が発生することも想定し、サイバー・フィジカル高度融合システム全体に高いサイバー攻撃耐性を備えることを目標とする。
- 未来投資戦略 2017[9]では、Society 5.0 の実現により、製造業全体の労働生産性について年間2%以上の向上を目指しており、この実現のためには中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策強化が必須となることからこの実現に寄与する技術開発と社会実装を進める。
- 『サイバー・フィジカル・セキュリティ対策基盤』に必要となる情報は、従前の情報セキュリティ関連のデータベース(脆弱性情報やインシデント情報、脅威情報等)に加え、サプライチェーンにおける信頼性情報となる「トラストリスト」や構成製品の真贋判定用の原本情報などのデータベースを融合・拡張したものを想定する。
- 『サイバー・フィジカル・セキュリティ対策基盤』の実証を通じて有効性を確認し、実稼働するサプライチェーンに組み込み実用化する本基盤の社会実装を他国に先駆けて推進することで、サイバー脅威に対する IoT 社会の強靱化を図り、我が国のセキュアな Society5.0 実現に寄与する。

---

[8] Society 5.0 において更なる経済発展が期待される分野としては、自動車の自動運転、スマートホームやスマートビル、5G ベースの新しい通信サービス、日本の防衛力を支える防衛産業、医療機器分野、等が考えられる。

[9] 2017 年 6 月 9 日閣議決定。
https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf



図表１－２．　Society 5.0 における本プロジェクトの役割

② 社会面の目標

・　サイバー攻撃の起点が急激に拡大し、攻撃の手法も高度化する中、IoT システム・サービスの調達・構築に関わる中小企業を含むサプライチェーン全体のセキュリティを確保し、運用される多様な IoT システム・サービスのセキュリティ維持を実現することにより、製造・流通分野やスマートビル等の IoT 機器・システム・サービスを守り、社会全体の安全・安心を確立し、Society 5.0 がもたらす約 90 兆円の価値創出を支える。

③ 産業的目標

・　社会インフラや社会の基盤となるサービス、大規模なサプライチェーンを構成する特定産業分野において技術の実証に取組み、技術を確立した後、国内に水平展開して実績を積み重ねることによって、技術の有効性について市場での良好な評価を獲得する。その結果として、高いセキュリティが求められ、Society 5.0 の実現により更なる経済発展が期待される自動運転やスマートライフ産業、5G ベースの新しい通信サービス、日本の防衛力を支える防衛産業、医療機器分野などにおける国際競争力を高める。

・　我が国の産業が国際展開を図る上での阻害要因を回避するため、欧米が実施するサイバーセキュリティ施策との整合性を確保し、2030 年には、高いものづくり品質をもつ我が国の中小企業の 50%に導入を進め、グローバルサプライチェーンへの対応を推進する。

・　従来の IT 機器向けセキュリティ製品では海外事業者に大きく依存している実情があるが、本研究開発を通じて IoT 向けセキュリティ基盤製品における先導的な技術開発を進め、また当該技術の標準化やデファクト化にも取組むことなどによって、海外市場における優位性確保を目指す。

④ 技術的目標

- 個々の IoT 機器やサービスのセキュリティを強化し、多様な IoT システム・サービスやサプライチェーン全体のセキュリティ確保を実現する上で必要な(A)「信頼の創出・証明」技術、すなわち、多種・大量の小型 IoT 機器にコスト性能面で適用可能な信頼の基点実装（信頼の創出）技術と IoT 機器の真贋判定（信頼の証明）技術、及び、その製造プロセスの適格性保証（信頼の証明）技術の多角的な研究開発を行う。
- 多様な社会インフラやサービス、幅広いサプライチェーンのセキュリティを確保するため、IoT システム・サービスや調達・構築に関わるサプライチェーンで「信頼チェーン」を構築し、必要な情報をセキュアに流通させる(B)「信頼チェーンの構築・流通」技術、すなわち、信頼チェーンを構築・活用できるプロトコル技術と情報流通技術の研究開発を行う。
- 「信頼チェーン」を構築した IoT システム・サービスやサプライチェーンにおいて、その「信頼チェーン」が安全に運用されていることを検証し、維持することを可能とする(C)「信頼チェーンの検証・維持」技術の研究開発に取組む。
- 上記の(A)信頼の創出・証明、(B)信頼チェーンの構築・流通、(C)信頼チェーンの検証・維持は、単なる要素技術の開発ではなく、一貫して担保できる技術群として開発する。
- 具体的目標として、中小企業を含む大規模サプライチェーンが多数重層構造となるスケール（構成組織数が1万以上）に対応でき、IoT システム・サービス（多様な IoT 機器数が数千以上）及びサプライチェーンの各構成要素（人、組織、製品、システム、サービス、データ等）のセキュリティ確保を可能とする、信頼の創出・証明技術、信頼チェーンの構築・流通技術、信頼チェーンの検証・維持技術を確立する。
- 技術成熟度レベル（Technology Readiness Level、以下「TRL」という。）[10]として、プロジェクト全体では TRL6 を目標とし、部分的には TRL7 を目指す。

⑤ 制度面等での目標

- サイバー攻撃は、国境を越えて行われるものであるから、国内だけの取組では十分ではなく、欧米各国等との連携を強化し、産学官が連携して我が国の取組を積極的に国際標準に提案するなど、国際ハーモナイゼーションを確保していくことを常に視野に入れた取組を進める。具体的には、国際動向も踏まえながら、電力、防衛、自動車、スマートホーム／ビル、公共交通、通信・放送などの各産業分野（Industry by Industry）において取組が進むセキュリティポリシーの策定活動と連携する。
- サイバーセキュリティタスクフォース（総務省）、産業サイバーセキュリティ研究会（経済産業省）、

10 ここでは、U.S. Department of Defense (DoD)が定義する TRL を用いる。TRL 1：基本原理の提唱／研究開発論文レベル、TRL 2：基本原理の確認と評価／研究開発論文レベル、TRL 3：基本原理の分析と実験室での評価、TRL 4：研究開発した技術要素または試作品の実験室での評価レベル、TRL 5：研究開発した技術要素の関連した環境での評価ができるレベル、TRL 6：研究開発した技術の関連した環境でデモンストレーションできるレベル、TRL 7：システムプロトタイプの運用環境でのデモンストレーションができるレベル、TRL 8：実システム連動での動作実証、TRL 9：実システム／商用システムに適用可能なレベル。

IoT セキュリティ WG（総務省・経済産業省・IoT 推進コンソーシアム）の政府施策（以下「主要 3 政府施策[11]」という。）等と緊密に連携して、産業界の個別ニーズに応じて具体的な対策にかかる制度整備に貢献[12]する。

⑥ グローバルベンチマーク

- 米国では、管理された非格付け情報（CUI）[13]を管理するためのサイバーセキュリティ対策の基準として NIST SP800-171 が示されており、既に防衛調達において、下請け企業まで含めたサプライチェーン単位で NIST SP800-171 の遵守等が求められている（DFARS Clause 252.204-7012）。また、政府がサイバーセキュリティのリスク評価の枠組みを示した『サイバーセキュリティフレームワーク（NIST Cybersecurity Framework）』の中で、サイバーサプライチェーンリスクの評価を明確に位置づける方針を示している。
- 欧州では、2017 年 9 月に発表した政策パッケージの中で、『サイバーセキュリティ認証フレームワーク（The EU cybersecurity certification framework）』を今後整備していく旨表明しており、各機器の特性や認証方法も考慮に入れた上で、今後、サプライチェーンまで含めたサイバーセキュリティ対策を求めていく可能性が高い。
- 本プロジェクトでは、『サイバー・フィジカル・セキュリティ対策基盤』によってセキュリティを確保したサプライチェーンと IoT システム・サービスが、主要 3 政府施策に加え、上記の海外の要件にも適用できるかの検証を行い、世界に対する優位性を確認する。

⑦ 自治体等との連携

- 自治体、各省庁、業界団体等との情報交換により、自治体が現在保有する IoT 関連システム及び今後保有することが想定されるシステム、並びにそのサプライチェーンも視野に、安全な構築と運用に必要となるセキュリティ要件を明らかにする。

---

11 我が国では、2017 年 12 月、経済産業省に産業サイバーセキュリティ研究会を設置し、国際動向も踏まえたサプライチェーン全体のサイバーセキュリティ対策について検討を始めたところであり、総務省・経済産業省・IoT 推進コンソーシアムの IoT セキュリティ WG においても、2017 年 12 月から、上記諸外国の動向も踏まえながら、一定のセキュリティ要件を満たした IoT 機器の認証を含む、IoT 機器のセキュリティ確保策の検討等を行っている。また、総務省のサイバーセキュリティタスクフォースにおいても、IoT 機器の脆弱性対策に係る体制の整備等の『IoT セキュリティ総合対策』を 2017 年 10 月に公表し、施策を推進している。

12 日本企業では欧米企業に比べ、委託先等の取引先への対応が大幅に遅れている。
https://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/pdf/001_05_00.pdf
このため、経済産業省が策定を進める『サイバー・フィジカル・セキュリティ対策フレームワーク』と連携して包括的なセキュリティ対策についての指針を示し、各分野での詳細なセキュリティ要件の定義と本 SIP 成果の社会実装により取組みに関する共通的な指標を定めることで、IoT システム・サービスやサプライチェーンのセキュリティ対策の把握状況が現状の倍増となる欧米並みとなることを期待する。

13 高度な機密性を有するものではないが、共有が必要な関係者間のみで管理すべき情報(Controlled Unclassified Information)のこと。

2. 研究開発の内容

本プロジェクトでは、製造・流通分野やスマートビル等の分野における IoT 機器を守り、セキュアな Society 5.0 の実現に向けた社会全体の安全・安心を確立するため、①個々の IoT 機器のセキュリティ強化から、②IoT システムの調達・構築に関わる中小企業を含むサプライチェーン全体でのセキュリティ確保、さらに③IoT システムとして運用される社会インフラや多様なサービスのセキュリティの維持、といった要件を実現する『サイバー・フィジカル・セキュリティ対策基盤』の技術開発に取組む。

○ 信頼のチェーン（連鎖）によるセキュリティ確保

本研究開発における基本的な考え方は、サプライチェーンと IoT システム・サービスの双方において、構成要素間の信頼のチェーン（連鎖）を構築・維持することで、セキュリティ耐性を高めることである。

サプライチェーンにおいては、各構成要素（人、組織、製品、システム、サービス、データ等）のいずれかに信頼の基点を置き（信頼を創出）、そこを起点とする信頼のチェーン（連鎖）によって、各構成要素の信頼を創出し、証明を可能とする。これを繰り返すことにより、サプライチェーン全体にわたる「信頼のチェーン」を構築し、その検証・維持によって、サプライチェーンのセキュリティを確保する。

同様に、IoT システム・サービスにおいては、IoT 端末機器等に信頼の基点を置き、そこを起点として各構成要素（IoT 機器、IoT ネットワーク、クラウド等）の信頼を創出し、証明を可能とすることにより、構成要素の改ざん等を防ぐ。そのような構成要素に跨る「信頼チェーン」を構築し、検証・維持することで IoT システム・サービス全体のセキュリティ確保を実現する。

また、サプライチェーンと IoT システム・サービスは相補的な関係にある。例えば、サプライチェーンの一部である製造プラントや物流システムは IoT システムであるとともに、製造業や ICT 産業のサプライチェーンが提供する製品は IoT システム（または IoT 機器）・サービスである。このため、IoT システム・サービスのセキュリティ確保には、その調達・製造に関わるサプライチェーンのセキュリティ確保（信頼チェーンの構築等）が必要であり、サプライチェーンのセキュリティ確保には、その構成要素（製造ライン等）である IoT システム・サービスのセキュリティ確保が必要と言える

○ 主な研究開発項目

この『サイバー・フィジカル・セキュリティ対策基盤』の研究開発においては、信頼の創出、信頼の証明、信頼のチェーンの構築と維持が重要[14]であり、その主な研究開発項目は以下の 3 つである。

（A）「信頼の創出・証明」技術の研究開発

（B）「信頼チェーンの構築・流通」技術の研究開発

（C）「信頼チェーンの検証・維持」技術の研究開発

また、研究開発を進める上で必要となる

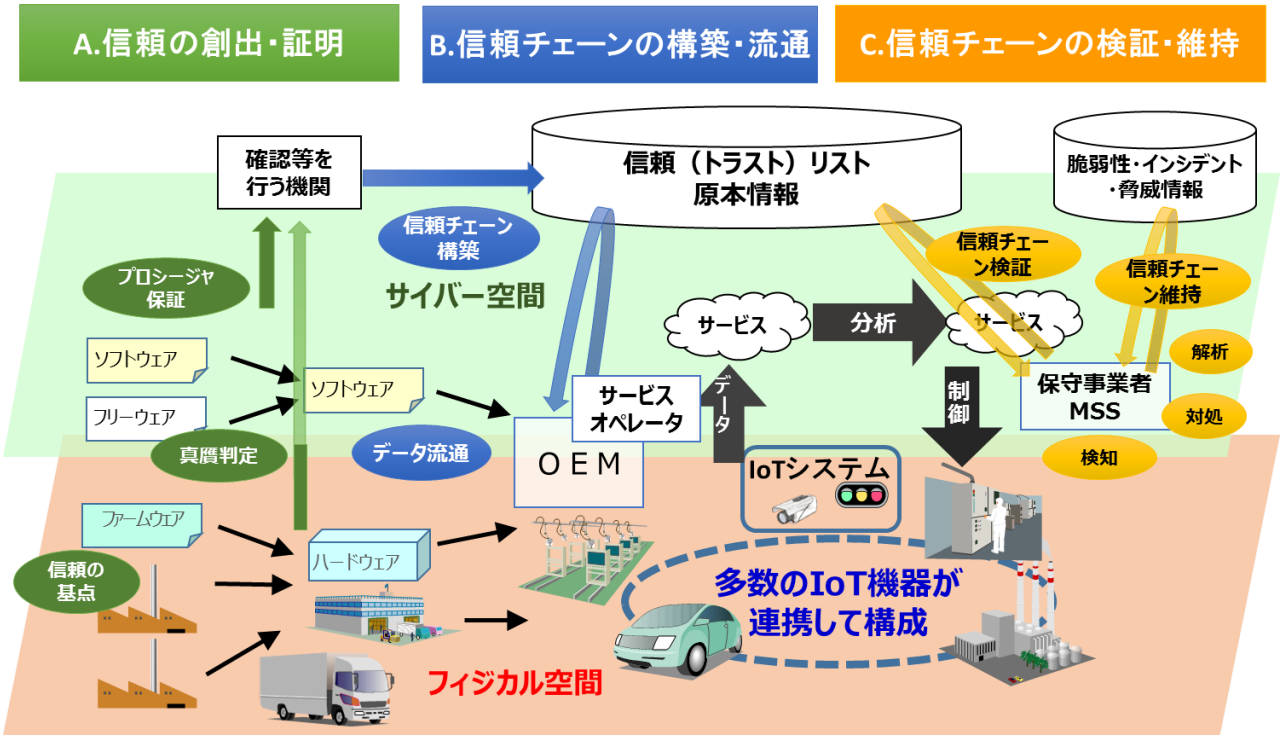
（D）『サイバー・フィジカル・セキュリティ対策基盤』に関わる動向調査

を行う。

---

14 経済産業省で策定を進める『サイバー・フィジカル・セキュリティ対策フレームワーク』においても、それぞれの構成要素についてのセキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーンを構築、維持していくことで価値創造過程全体のセキュリティを実現するものとしている。

図表２－１に、サプライチェーンの各構成要素についてのセキュリティ確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーン（連鎖）を構築することで、製品・サービスのライフサイクルにわたるサプライチェーン全体のセキュリティを社会実装するために必要となる技術開発項目の全体像を示す。



図表２－１．　信頼チェーンで構築されるサイバー・フィジカル・セキュリティ対策基盤のイメージ

（A）「信頼の創出・証明」技術では、個々の IoT 機器やサービスのセキュリティを強化し、多様な IoT システム・サービスやサプライチェーン全体のセキュリティ確保を実現する上で必要な信頼の創出・証明技術の多角的な研究開発を行う。また、（B）「信頼チェーンの構築・流通」技術では、多様な社会インフラやサービス、幅広いサプライチェーンのセキュリティを確保するため、IoT システム・サービスや調達・構築に関わるサプライチェーンにおいて「信頼チェーン」を構築し、必要な情報をセキュアに流通させる技術を研究開発する。さらに、（C）「信頼チェーンの検証・維持」技術では、「信頼チェーン」を構築した IoT システム・サービス及びサプライチェーンにおいて、「信頼チェーン」が安全に運用されていることを検証し、維持することを可能とする技術を研究開発する。加えて、技術成果の社会実装に必要な導入・運用マニュアルや組織・人材開発の取組みも併せて行う。

本基盤の研究開発にあたり、開発技術の実証実験を幅広く行い、有効性と課題の効果測定調査を実施して研究開発にフィードバックするとともに、海外の取組みと相互評価できる国際会議への参画などの普及活動を実施する。

また、（D）関連する技術の研究開発動向や政策動向などの海外動向調査を並行して実施し、（A）（B）（C）それぞれで実施する個別技術の動向調査と併せ、研究開発に随時反映する。

以下、3つの研究開発項目と動向調査項目について説明する。

(A)「信頼の創出・証明」技術

多様な IoT システム・サービス及びサプライチェーン全体のセキュリティ確保は、個々の IoT 機器やサービスのセキュリティを強化し、その信頼を創出できる起点から始まる。そのために、

・(A1) IoT サプライチェーンの信頼の創出技術基盤の研究開発

を進める。

また、対象機器及びその製造プロセス、対象サービスの提供プロセスの信頼を証明するために、

・(A2) IoT 機器等向け真贋判定による信頼の証明技術の研究開発

・(A3) プロシージャ適格性保証による信頼の証明技術の研究開発

を実施し、製品とプロセスの両面から、対象機器・サービス等が要件を満たした形で生成されたことを確認し、あるいは、対象機器・サービス等を生成する過程に関与した組織・責任者の信頼を証明するなどの枠組みを実現する。

本研究開発を進めるにあたり、信頼の創出・証明技術に関連する動向調査を行う。

上記の技術をベースに、「モノ」、ハードウェア、ソフトウェア、サービス、プロシージャ等に関する認証の仕組みを準備し、実サービスを提供するシステムに導入してその効果を実証する。さらに、本研究開発の成果である(B)信頼チェーンの構築・流通、(C)信頼チェーンの検証・維持が、一貫性ある技術群であることを検証する。実証実験は効果測定を含めて実施し、その結果を踏まえて、普及活動に取組む。

なお、「(A3) プロシージャ適格性保証による信頼の証明技術の研究開発」については、当該技術そのものの開発には一定の目途がついたことから、上記の方針及びステージゲート審査の結果を踏まえ、2021年度からは「(B)信頼チェーンの構築・流通」における実証実験及び普及に向けた取り組みへと統合した上で、一貫性のある技術群としての確立を目指す。

(A1) IoT サプライチェーンの信頼の創出技術基盤の研究開発

Society 5.0 時代に求められる大規模 IoT システム・サービス及び IoT サプライチェーンの信頼性の礎として、IoT の末端を構成する機器(末端ノード)に信頼の基点[15](セキュリティ保証)を配置し、それを起点として IoT 機器の真贋判定やプロシージャ適格性保証による信頼チェーンの構築を可能とするための技術基盤が強く求められている。その技術基盤として以下の技術等の研究開発を実施する。

① IoT 機器等に組込み可能な暗号モジュールをベースに、それを信頼の基点として活用するための基盤技術

② 信頼の基点に対するサイバー攻撃とフィジカル攻撃の双方に対処するために、耐タンパー性の向上、及び、サプライチェーンの各フェーズにおいて供給者の意図に反してハードウェアに組込まれる恐れのある悪意の機能に対抗する技術等

③ 信頼の基点に対するセキュリティ保証スキームの整備／構築。具体的には、信頼の基点に対する攻撃類型を調査、信頼の基点に関わるシステムの脆弱性評定技術の確立と脆弱性評定基準の策定

15 実社会では、パスポートや運転免許証を礎（信頼の基点）として、銀行口座や携帯電話の所有者が本人であることを担保している（信頼の基点を起点とした信頼チェーン構築の例)。

等を実施するとともに、保証スキームとしての枠組を構築する。

小型 IoT 機器に導入可能で世界トップ水準の暗号実装技術に基づく信頼の基点基盤技術の実現と、多種多様な小型 IoT 機器製品に搭載可能な耐タンパー性能の低廉な実現が、本テーマの技術的チャレンジポイントである。

参画機関:

電子商取引安全技術研究組合(共同実施:横浜国立大学、神戸大学、東京大学、東北大学、奈良先端科学技術大学院、三菱電機株式会社)、国立研究開発法人産業技術総合研究所

(A2) IoT 機器等向け真贋判定による信頼の証明技術の研究開発

IoT 機器は大量、無人かつ自動運用といった特性から管理の目が行き届かず、改造やすり替えといった改ざんに気づきにくいため、被害が長期にわたって発生し続けるおそれがある。このため、サイバー・フィジカル高度融合システムを構成する各 IoT 機器の真贋判定を可能とし、不正な IoT 機器の混入、及び混入時の即時検知によって被害の発生を回避するために以下の技術の研究開発を実施する。

① 現状ではセキュリティ対策機能を搭載することが困難な IoT 機器に対応可能な軽量性と、極めて多様な IoT 機器のアーキテクチャと対象機器の特性に対応可能な真贋判定技術

② IoT 機器単体の多様性に加え、IoT システムの構成の多様性、サービス提供時及び運用時のサプライチェーンの多様性に対応でき、構成する IoT 機器数が膨大になったとしても、システム全体の真贋を確実かつ効率的に判定可能にする技術

IoT 機器が用途・目的別に多様化する中、IoT 機器が膨大に存在する IoT システムであっても、高いサイバー攻撃耐性とレジリエンスを確保した上で真贋判定可能な技術を実現する。また、同時に、小型 IoT 機器にも対応可能な軽量性と多様な構成の IoT システムに対応可能な柔軟性を備えることも、本テーマの技術的チャレンジポイントである。

参画機関:日本電信電話株式会社(再委託:株式会社 FFRI)、日本電気株式会社

(A3) プロシージャ適格性保証による信頼の証明技術の研究開発

セキュアな Society 5.0 を実現するにはサプライチェーン全般にわたる信頼確保が必要である。プロシージャは、サプライチェーンにおいて価値を創造するプロセスそのものであり、信頼チェーンを構築するために、プロシージャに対する信頼を証明できる適格性保証技術が必要である。このため、プロシージャに関わる人、組織、製品、システム、サービス、データ等の信頼に加え、手順が追加/省略されずに正しい順序で実行することを保証するために、以下の技術を研究開発する。

① プロシージャが既定の手順通りに実行されていることを、外部観測可能なイベント(人の操作、システムのログ、ネットワークパケット等)などから確認可能とする技術

② 複数組織が連携する場面で活動する人の信頼についてオーソリティーを用いることなく証明する技術

③ データの創造者（所有者）が定めたポリシーに基づいてデータを取り扱い、組織を跨がってデータを授受する際にデータの漏えいや破壊が行われていないことを担保する技術

④ 人、組織、製品、システム、サービス、データ、プロシージャ等が信頼できるものであったことを後日確認可能とするためにデジタル化されたエビデンスを保存する技術

フィジカル空間、サイバー空間双方にある多様な要素情報を統合化して第三者に提示できる適格性保証の実現と、大規模サプライチェーンが多数重なり合う環境下でのデジタル化されたエビデンスによるトレーサビリティ確保が、本テーマの技術的チャレンジポイントである。

なお、本サブテーマについては、2021 年度より B1 及び C1 と統合の上で、新たに B3 として効果検証及び社会実装に向けた取り組みを行うものとする。

参画機関:

株式会社日立製作所、日本電気株式会社、

株式会社 KDDI 総合研究所（再委託:株式会社国際電気通信基礎技術研究所、早稲田大学）

(B)「信頼チェーンの構築・流通」技術

大規模プラント産業や自動車産業などでは、OEM企業のサプライチェーン規模は数万社におよび、その大部分は中小企業が占める。そのようなサプライチェーンによって IoT システム・サービスが提供され、一方で、そのサプライチェーンの一部は IoT システムで構成される。このように、日本の産業全体としては、IoT システム・サービスとサプライチェーンが重層構造になっている。

このような IoT システム・サービス及び大規模サプライチェーンにおいては、信頼の創出と証明を繰り返すことで「信頼チェーン」を構築し必要な情報を流通させる環境が必要となり、そこでは、対象機器・サービス等が正常に生成されたものであることを効率良く確認できる信頼（トラスト）リストの作成・管理と、信頼に関する情報などの業務関連データのセキュアな流通環境の整備と実現が重要となる。このために、

（B1） 分野毎の特性を踏まえた信頼チェーンの構築技術の研究開発

（B2） 信頼チェーンに関わる情報の安全な流通技術の研究開発

などを進める。

本研究開発を進めるにあたり、信頼チェーンの構築・流通技術に関連する動向調査を行う。

上記の技術をベースに、信頼チェーンの構築・流通の仕組みを準備し、実サービスを提供するシステムに導入してその効果を実証する。

さらに、複数の適用先分野の実証フィールドでの検証を繰り返すことにより、信頼チェーンの構築・流通技術を確立するとともに、本研究開発の成果である(A)信頼の創出・証明、（C)信頼チェーンの検証・維持が、一貫性ある技術群であることを検証する。実証実験は効果測定を含めて実施し、その結果を踏まえて、普及活動に取組む。

なお、「(B1)分野毎の特性を踏まえた信頼チェーンの構築技術の研究開発」については、当該技術そのものの開発には一定の目途がついたことから、上記の方針及びステージゲート審査の結果を踏まえ、2021 年度からは「(A)信頼の創出・証明」及び「(C)信頼チェーンの検証・維持」の関連技術とともに、「(B3)サプライチェーン全体の信頼性確保に向けた信頼データ交換・共有技術」として、実証実験及び普及に向けた取り組みへと統合した上で、一貫性のある技術群としての確立を目指す。

(B1) 分野毎の特性を踏まえた信頼チェーンの構築技術の研究開発

本研究開発成果の適用先となる様々な事業分野において、そのサプライチェーンの信頼確保において重要となる要素(人、組織、製品、システム、サービス、データ、プロシージャ等)が異なるため、以下の技術等を研究開発する。

① 事業分野毎のセキュリティ対策として、適用先分野の特性に応じたサプライチェーンのセキュリティを実現するための要件(「分野別プロファイル」)の開発
② その分野別プロファイルに沿ったトラストリストの構築技術(トラストリストの構成、管理技術等)
③ 価値を創造するために関わった人、組織、製品、システム、サービス、データ、プロシージャ等が信頼できることを証明するトラストリスト技術とサプライチェーンを構成する事業者によるトラストリストの利活用技術(トラストリストの登録・更新、参照技術、プロトコル技術、調達システムとの連携 等)

実際のサプライチェーンでの実証実験により、その実運用者の業務との整合性を確認できるトラストリストの構築・活用技術の実現、及び、実事業に即したトラストリストの運用コストの低廉化と堅牢性の両立が、本テーマの技術的チャレンジポイントである。

なお、本サブテーマについては、2021 年度より A3 及び C1 と統合の上で、新たに B3 として効果検証及び社会実装に向けた取り組みを行うものとする。

参画機関:

株式会社日立製作所(再委託:国立研究開発法人産業技術総合研究所、セコム株式会社)、
日本電気株式会社、株式会社 KDDI 総合研究所(再委託:株式会社国際電気通信基礎技術研究所)

(B2) 自治体と事業者間の信頼チェーン構築と安全な情報流通技術の研究開発

IoT システム・サービスの提供/運用時及びサプライチェーンにおいて信頼チェーンを形成するため、信頼に関わる情報などの業務関連データについて、その安全な流通を実現するデータ流通技術を実現する。具体的には、データ流通に関するセキュリティを監視・管理し、異常を検知した場合にはシステムに対する影響を極小化しつつセキュアかつスケーラブルなデータ流通を可能にする以下を満たす技術を実現する。

① データ流通時の信頼関係構築に必要となる認証及びトレーサビリティの確保技術
② データ流通に関わるサイバー攻撃の影響範囲可視化技術
③ サイバー攻撃に対するシステム影響の極小化技術
④ 上記 ②③の統合実施による安全なデータ流通に関するレジリエンシーの確保技術

広域かつ大規模なサプライチェーンが多数、重なり合う情報流通環境において、スケーラビリティ及びトレーサビリティを備えた技術を実現し、実装の軽量化や運用コストの低廉化により、優れた導入容易性も備えた情報流通環境を実現することが、本テーマの技術的チャレンジポイントである。

参画機関:富士通株式会社(再委託:情報・システム研究機構国立情報学研究所、名古屋大学)

(B3) サプライチェーン全体の信頼性確保に向けた信頼データ交換・共有技術

本研究開発では、2021 年度より A3、B1 及び C1 の研究開発成果を引き継ぎ、サプライチェーン全体でルールを守っていることを相互に確認可能な仕組みの実現に向け、以下の技術等を研究開発する。

① サプライチェーン全体の信頼性確保に向けた信頼性フレームワークの研究開発、及びそれに必要な VCP モデル構築技術と信頼データ交換・共有技術の研究開発

② A3、B1 及び C1 の研究開発成果を含めた、①の信頼性フレームワークに基づくサイバー・フィジカル・セキュリティ対策基盤の統合技術実証、価値実証

③ ①の信頼性フレームワークの国際連携と普及啓発、及び普及に向けた課題抽出と提言

加えて、上記技術の社会実装を果たすために、多様なエンティティーが関与するとともに、サプライチェーン全体での信頼性確保が制度等で求められていない「ビルサービス」の領域において、実証実験を通じて、本技術により生み出される価値の実証を行うとともに、社会実装を促す。

これらにより、実運用者の業務との整合性を確認できるトラストリストの構築・活用技術の実現、及び、実事業に即したトラストリストの運用コストの低廉化と堅牢性の両立、サプライチェーン全体でルールを守っていることを相互に確認可能な仕組みの実現に向け、分野横断で適用可能な実現手順を確立させることが、本テーマの技術的チャレンジポイントである。

参画機関:

株式会社日立製作所(再委託:国立研究開発法人産業技術総合研究所、セコム株式会社)、

株式会社 KDDI 総合研究所

(C) 「信頼チェーンの検証・維持」技術

サイバー・フィジカル高度融合システム上で「信頼チェーン」構築を実現した場合も、その「信頼チェーン」が安全に運用されていることを検証し、維持することが重要である。このために、

(C1) 信頼チェーンの検証技術の研究開発

(C2) 信頼チェーンの維持技術の研究開発

を進める。また、運用時における機能復旧やレジリエンスを確保・向上する技術、データの流通を制御する技術なども研究開発範囲として考慮する。

本研究開発を進めるにあたり、信頼チェーンの検証・維持技術に関連する動向調査を行う。

上記の技術をベースに、信頼チェーンの検証・維持の仕組みを準備し、実サービスを提供するシステムに導入してその効果を実証する。さらに、本研究開発の成果である(A)信頼の創出・証明、(B)信頼チェーンの構築・流通が、一貫性ある技術群であることを検証する。実証実験は効果測定を含めて実施し、その結果を踏まえて、普及活動に取組む。

なお、(C1) 信頼チェーンの検証技術の研究開発」については、当該技術そのものの開発には一定の目途がついたことから、上記の方針及びステージゲート審査の結果を踏まえ、2021 年度からは「(B)信頼チェーンの構築・流通」における実証実験及び普及に向けた取り組みへと統合した上で、一貫性のある技術群としての確立を目指す。

(C1) 信頼チェーンの検証技術の研究開発

サプライチェーン全体での信頼確保のためには、サプライチェーンを構成する複数の事業者間で、サイバー・フィジカル高度融合システム上に構築された信頼チェーンの検証技術の開発が必要である。特に、異なる事業者間であること、異なる事業分野間であること、分野別プロファイル、トラストリストの構成・運営等も異なること、また、事業分野によっては、サプライチェーンの一部を秘匿したいというニーズもあることを考慮し、以下の技術開発を実施する。

① 異なる事業者間、異なる事業分野間での信頼チェーンの検証技術、及び複数の異なるトラストリスト間で連携した検証を可能とする技術(プロトコル技術、調達システムとの連携　等)

② 具体的な組織名・モノの構造等は非開示なままでも、信頼できる人、組織、製品、システム、サービス、データ、プロシージャ等からのみ成り立っていることを確認することで信頼チェーンの検証を可能とする技術

複数事業者間での運用環境における検証プロトコルを確立し、サプライチェーンに関する業務の整合性評価、運用コスト評価を行うこと、及び、情報を秘匿化したまま信頼の検証を可能とする技術を実現することが、本テーマの技術的チャレンジポイントである。

なお、本サブテーマについては、2021 年度より A3 及び B1 と統合の上で、新たに B3 として効果検証及び社会実装に向けた取り組みを行うものとする。

参画機関:

株式会社日立製作所(再委託:国立研究開発法人産業技術総合研究所)、日本電気株式会社、
株式会社 KDDI 総合研究所(再委託:株式会社国際電気通信基礎技術研究所)

(C2) 信頼チェーンの維持技術の研究開発

サイバー空間及びフィジカル空間を構成する多様な機器の連動によって、サイバー攻撃の対象は現在の IP 通信を行う比較的シンプルな IoT 機器から、より多様かつ特殊な IoT 機器にも拡大していくと想定される。また、IoT 機器自体の性能制限や運用者のスキル不足等によって、セキュリティ対策が不十分かつ搭載困難な機器の利用は今後も続くと見込まれる。

このような状況に対して、サイバー・フィジカル高度融合システムにおける信頼チェーンの安全な運用を維持するため、システム上で発生するセキュリティ異常の検知・解析から対処までを含むプロセス全体を支援する以下の 3 つの技術を確立し、セキュリティインシデントへの確実かつ早期対処を可能にする。

① サイバー空間及びフィジカル空間における両事象を効率的かつ正確に収集し、統合解析することによって、両空間を跨がり発生するセキュリティ異常をも高精度に検知可能とする検知技術

② サイバー・フィジカル空間を跨って流れる不正なデータ(フィジカルデータ、制御データ)を検知及び排除する技術

③ サイバー・フィジカル高度融合システムにおけるサイバー攻撃発生時の影響評価及び対処策決定をシミュレーションにより実施可能にするとともに、当該対処策の実環境に対する実行を支援する技術

フィジカルとサイバー両空間の事象を統合的に解析することによって検知可能な異常事象を拡大し、異常発生から検知・対処までの即時性を大幅に高める。また、サイバー攻撃の直接的な影響と対処策による副作用をシミュレーション技術により事前評価可能にし、実システムへの影響を抑えながら最適な対処策を即時決定可能にする点が、本テーマの技術的チャレンジポイントである。

参画機関:
日本電信電話株式会社(再委託:大阪大学)、三菱電機株式会社(再委託:金沢工業大学)、
株式会社日立製作所、日本電気株式会社

(D)『サイバー・フィジカル・セキュリティ対策基盤』に関わる動向調査

本研究開発の出口戦略実現に向け、『サイバー・フィジカル・セキュリティ対策基盤』に関連する研究開発動向や政策動向など、以下の 4 項目について、海外を中心とした動向調査を実施する。調査にあたっては、(A)(B)(C)の研究開発テーマで個々に実施する調査を含め全体をコーディネートする。本テーマは 2018 年度のみ実施する。

① 欧米やアジアにおける類似の法制度や民間活動
② IoT システム・サービスに関連する技術の進展を踏まえた評価技術の動向
③ サプライチェーン全体から見たベンダー評価の動向と関連技術
④ 調査結果に基づく、本研究課題が取組むべき方向性の提言

参画機関:日本電気株式会社

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

本プロジェクトは、NEDO への交付金を活用し、図表３－１のような体制で実施する。NEDO は PD や推進委員会を補佐し、予算の管理、研究開発の進捗管理（知財管理を含む）など、必要な協力を行う。

(2) 研究責任者の選定

本プロジェクトでは、研究開発の成果を主体的に実用化・事業化できる企業を中心に、先進技術を有する大学やベンチャーを含む産学連携のプロジェクト実施体制を構築する。この考え方と本研究開発計画に基づき、NEDO は、研究テーマ、及び研究テーマを実施する研究主体とその研究責任者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 及び内閣府と相談したうえで決定する。審査には原則として PD 及び外部有識者が参加する。応募テーマに参加する研究者の利害関係者は当該テーマの審査には参加しない。利害関係者の定義は NEDO が定める。選考により研究テーマが決まった後、本計画に研究テーマ、及び研究主体、研究参加者を記載する。

(3) 研究体制を最適化する工夫

PD は、研究テーマの進捗状況、及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、研究テーマの変更、追加、研究主体の入れ替え、追加等を検討していく。必要に応じてサブ PD をおき、研究開発の内容や進捗状況の管理について、PD を補佐するものとする。

また、一部の研究テーマについては「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。

それぞれの研究テーマに取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、本プロジェクトの目標を共有する。

(4) 成果の普及推進体制の強化

PD 主導で、本プロジェクトの活動状況及び成果を、参画している企業や組織による実証だけでなく、より広く産業界に周知・理解してもらうための委員会やワーキンググループ(WG)等を適宜設置し、シンポジウムやセミナー、ビジネスイベントでの取組内容の発表、そして国際会議などを企画し、実施していく。

ワーキンググループ(WG)等として計画しているものは次の通り。2019 年度より、研究開発に並行して具体的に WG 活動を開始してテーマ横断的な課題の解決を図る。

実証評価 WG:

- 実証実験において実用性や実効性を効果測定する手法を調査・検討するとともに、実証実験パートナー候補と共同検討し、実証実験を進めるテーマ間で共有する。
- SIP の課題間、他国プロ等と連携した実証実験を検討(外部向け窓口の役割)する。

成果普及 WG:

- 参画企業による事業化(製品化)と各産業分野へ導入推進する(知財委員会と連携)。
- 共用検証センター(自主評価用)等、中小企業などが成果を活用し易い環境を立上げる。

・　本取り組みの海外発信のために、国際シンポジウムを企画・開催する。

海外動向調査 WG:

・　各テーマで実施する国内内外の関連動向調査状況を集約し、プロジェクト全体で共有する。
・　国際連携活動として米国 NIST, 欧州 ENISA 等へ積極的な提言活動をとりまとめる。

加えて、2020 年度においてはWG活動と連携して、「サプライチェーンセキュリティにおける製造者側と利用者側の連携強化」の取組を進める。本取組では、新型コロナ感染症対策等の緊急事態への対処に伴うサプライチェーンの再構築時においても、我が国における複雑なサプライチェーンの安全性を確保できるようにするため、サイバーセキュリティ上の情報交換と共同検証の仕組みを検討し、多様な分野に跨る製造者側と利用者側の相互連携を強化する。

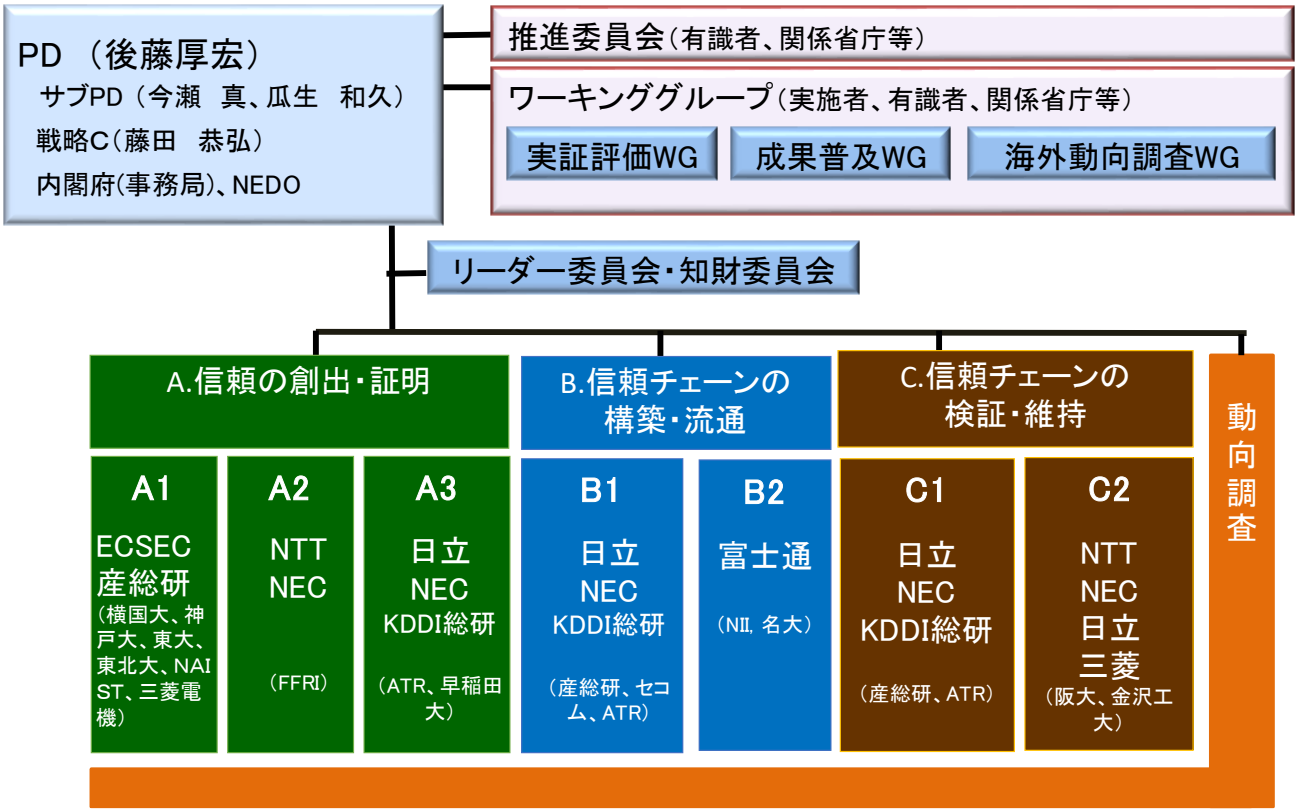
(5) 府省庁連携

本プロジェクトが目指す『サイバー・フィジカル・セキュリティ対策基盤』は、多様な社会サービスや製造業のサプライチェーン及び運用連携のセキュリティ確保を目指すものであり、総務省、経済産業省、NISC、IT総合戦略室、警察庁、防衛省、厚生労働省など幅広い府省連携が不可欠な分野横断的な取組である。このため、本プロジェクトの推進にあたっては、推進委員会のほか前述の主要 3 政府施策等と連携しつつ、IoT 社会に対応したシステム・サービス及びサプライチェーン全体のセキュリティ確保に必要な『サイバー・フィジカル・セキュリティ対策基盤』の構築等を図る。

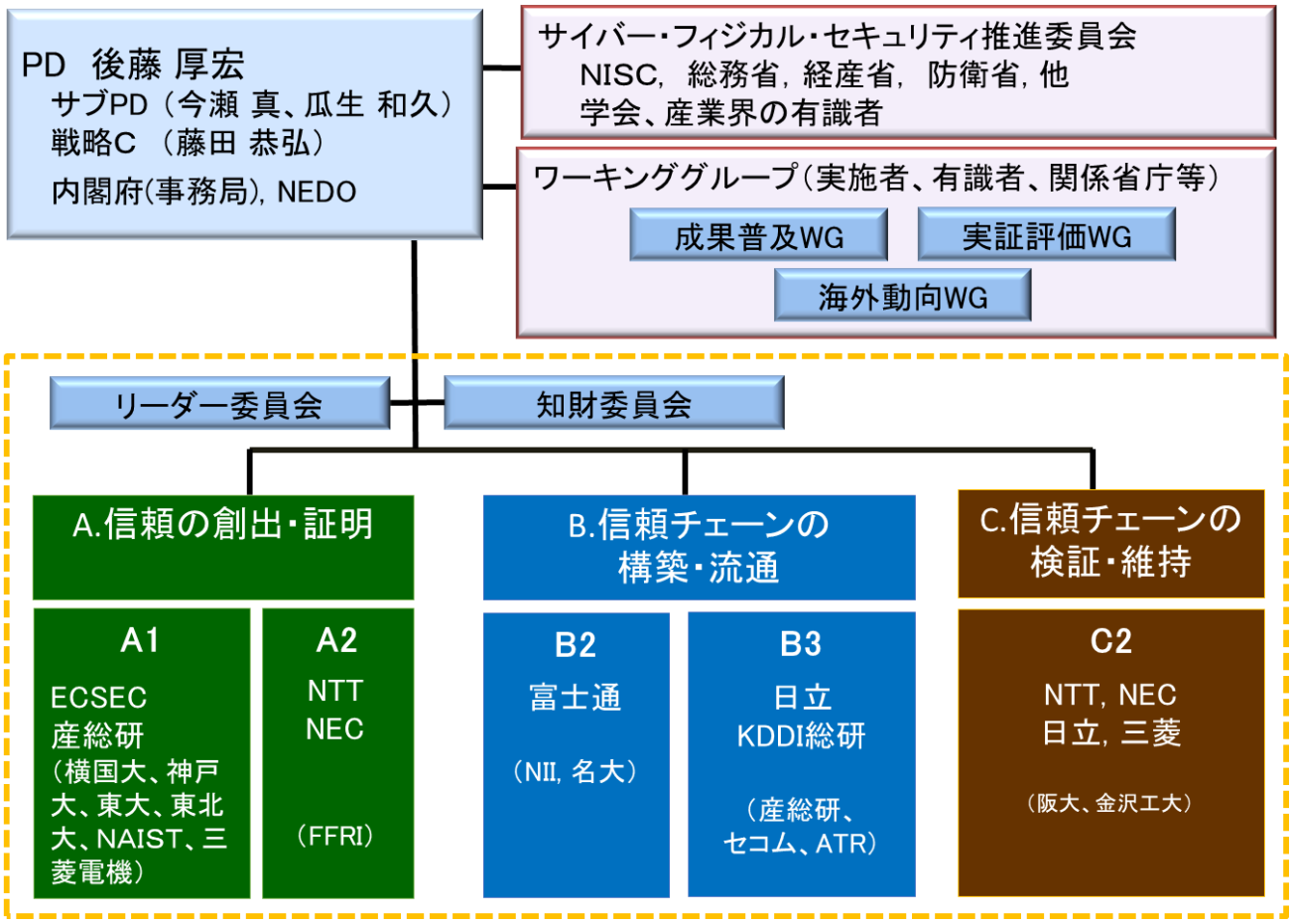
(6) 産業界からの貢献

本プロジェクトでは、参画企業の主体的な貢献による研究開発成果の実用化・事業化を想定する。また、技術成果の社会実装に向けた実証実験において、実フィールドをもち、課題認識のある事業者やベンダーが主体的に取組めるように、本プロジェクトの当初から研究開発チームと密に連携し、社会実装の観点からの要求事項を共有できる体制を構築する。研究開発を担う企業と実証実験に参画する事業者には、それぞれ、人的・事業的なリソースを主体的に投入するように促す。今後の産業界からの貢献(人的、物的貢献を含む。)は、研究開発費の総額(国と産業界からの貢献との合計)の 15%～35%程度を期待している。

また、2021 年度以降については、実施者がマッチングファンド対象外の組織のみからなる A1 を除き、産業界からの貢献が 50%以上となるよう取り組む。



図表3-1. 実施体制（2020 年度まで）



図表3-2. 実施体制（2021 年度から）

4. 知財に関する事項

(1) 知財委員会

○研究テーマまたは研究テーマを構成する研究項目ごとに、知財委員会を管理法人等または選定した研究責任者の所属機関(委託先)に置く。

○知財委員会は、それを設置した機関が担った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・維持等の方針決定等のほか、必要に応じ知財権の実施許諾に関する調整等を行う。

○知財委員会は、原則として PD または PD の代理人、主要な関係者、専門家等から構成する。

○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

○管理法人等は、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、プログラム参加前から保有していた知財権及びプログラム参加後に SIP の事業費によらず取得した知財権)、フォアグラウンド知財権(プログラムの中で SIP の事業費により発生した知財権)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、知財権者が定める条件に従い(あるいは、「プログラム参加者間の合意に従い」)、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(研究開発のみならず、成果の実用化・事業化を含む)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の保有、積極的に事業化を目指す者への実施権の設定を推奨する。

○参加期間中に脱退する者に対しては、当該参加期間中に SIP の事業費により得た成果(複数年度参加の場合は、参加当初からの全ての成果)の全部または一部に関して、脱退時に管理法人等が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(あるいは、「プログラム参加者間の合意に従い」)、知財権者が許諾可能とする。

〇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。
〇当該条件などの知財権者の対応が SIP の推進（研究開発のみならず、成果の実用化・事業化を含む）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

〇産業技術力強化法第 19 条第 1 項第 4 号に基づき、フォアグラウンド知財権の移転、専用実施権の設定・移転には、合併・分割による移転の場合や子会社・親会社への知財権の移転、専用実施権の設定・移転の場合等（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、管理法人等の承認を必要とする。
〇合併等に伴う知財権の移転等の場合等には、知財権者は管理法人等との契約に基づき、管理法人等の承認を必要とする。
〇合併等に伴う知財権の移転等の後であっても管理法人は当該知財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

〇研究開発終了時に、保有希望者がいない知財権等については、知財委員会において対応（放棄、あるいは、管理法人等による承継）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

〇当該国外機関等の参加が課題推進上必要な場合、参加を可能とする。
〇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。
〇国外機関等については、知財権は管理法人等と国外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

〇事前評価、毎年度末の評価、最終評価とする。
〇終了後、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。
〇上記のほか、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 28 年 12 月 21 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

〇事前評価は、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。
〇年度末の評価は、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。
〇最終評価は、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。
〇追跡評価は、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

〇評価結果は原則として公開する。
〇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

研究責任者は、担当する研究テーマについて、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。

③管理法人による自己点検

NEDO による自己点検は、予算執行上の事務手続を適正に実施しているかどうか等について行う。

6. 出口戦略

(1)出口指向の研究推進

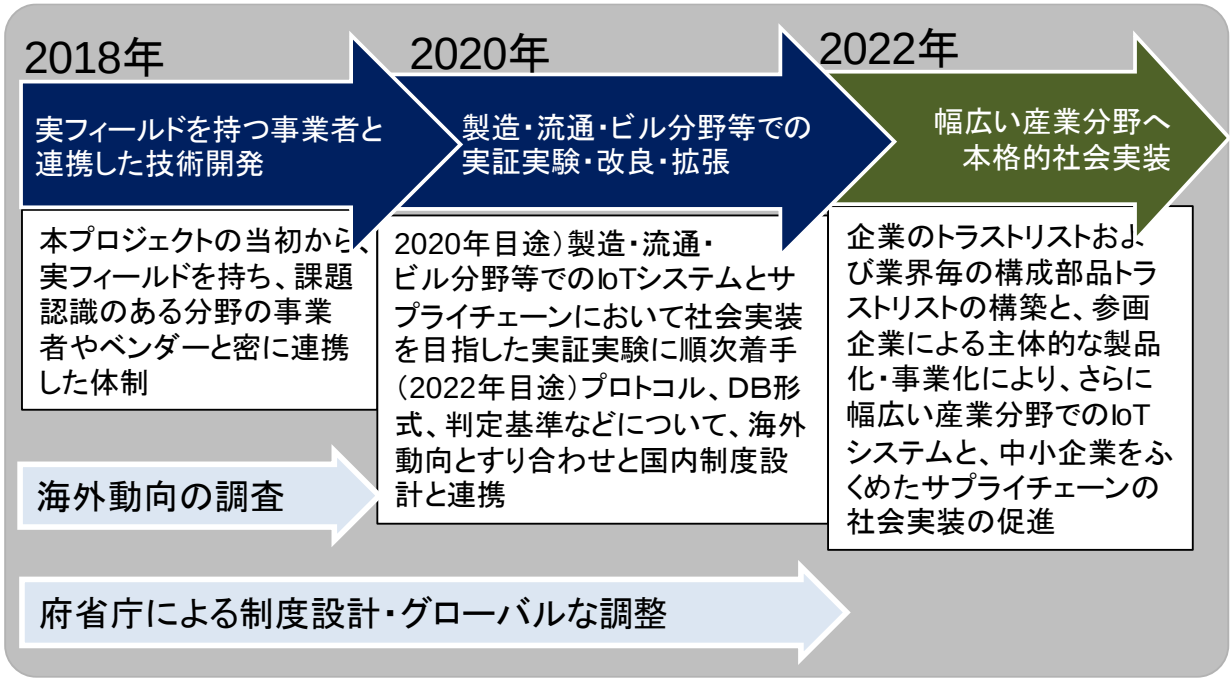
本研究テーマの社会実装の実現には、各テーマで実証した技術について民間企業への普及だけではなく、サプライチェーン全体での信頼チェーンの構築、検証、維持に向けた体制構築が必要となる。

サプライチェーンの各構成要素が真にセキュリティ要件を満たしているかいなかの確認（信頼の証明）は、求められるセキュリティ要件やその水準が産業分野毎に異なり、各産業の知見を踏まえる必要があることから、例えば、業界団体や独立行政法人を主体として構築することを想定している。

また、証明された信頼の情報の原本を保管し、第三者に照会可能とするためのリストやデータベースの構築・管理においては、業界団体や独立行政法人だけではなく、企業などの業種横断的な情報を扱う既存の信用情報データベースを活用していくことも考えられる。

信頼チェーンの維持に活用するための脆弱性・インシデント・脅威等の情報については、既存の情報共有の枠組や公的な組織と連携する前提で検討を進める。

2020 年を目途に、製造・流通分野やビル分野等、実証実験パートナー環境での IoT システム・サービスまたはサプライチェーンにおいて『サイバー・フィジカル・セキュリティ対策基盤』の社会実装を目指した実証実験に順次着手し、その他大規模なサプライチェーンを保有している社会インフラ産業への応用展開を図る。また、2021 年度以降は、単なる技術実証に留まらず、研究開発成果の価値を実証し、社会実装に直結する実証実験に取り組む。



図表６－１．社会実装に向けた取組み

本プロジェクトが終了する 2022 年までに、実証実験を行った産業分野について、実証実験の結果を踏まえ確認等を行う機関、トラストリストの構築・管理をする機関、脆弱性・インシデント・脅威等の情報管理をする機関の体制検討を完了し、サプライチェーン全体のセキュリティ確保を実施可能な体制を構築する。

本プロジェクトでは、技術開発に加え実証実験まで取組み、その研究開発成果については、参画企業が主体となって製品化を進め、各産業分野への導入を推進する。一部の成果は、IP（知的財産権）化して関連するベンダにライセンス供与することで、その普及を目指す。

また、中小企業を含むサプライチェーン全体及びその構成企業の IoT システム・サービスへの導入を促進し、2030 年までにサプライチェーン対策が求められる中小企業の 50%に本基盤の成果の導入を目指す。

(2)普及のための方策

国際動向も踏まえながら策定した各分野に求められるセキュリティポリシーや信頼チェーンなどの研究開発成果である基盤を、例えば、自動車、スマートビル、さらに通信・放送、電力、公共交通、防衛などの各分野でそれぞれ適用の実証を行いながら各分野での浸透を図る。また基盤導入の促進策として、政府や地方自治体、あるいは IoT サービス提供者に対して当該基盤の活用による信頼確認を推進し、IoT 機器やサービスのサプライヤー、調達側双方で当該基盤の有益性の認識を高めていく。その認識を高める方法として、最終の成果に至る途中の段階での取組状況を、各種イベント（シンポジウムやセミナー、ビジネスイベントでの発表、国際会議など）を通じて公開し、国内外の産業分野の IoT サービス関係者への理解を促進するとともに、国際的な解決を目指す取り組みに発展させるコーディネーションの場として活用し、我が国の取組み成果の国際貢献につなげる。また、2021 年度以降は、研究開発成果が安心して社会に実装されるよう、認証制度に向けた取り組みや、国際標準や業界合意への反映への取り組みを強化する。

加えて、総務省・経済産業省・IoT 推進コンソーシアムの IoT セキュリティ WG において検討されている IoT 機器の認証や IoT 機器のセキュリティ確保策に連携する。これにより、米国や欧州のサイバーセキュリティフレームワーク整備と伍することができる制度作りに貢献する。

〇規制・制度改革等のシナリオ

研究開発した技術の実証と、その結果のフィードバックを繰り返すことで、早期の社会実装を目指すとともに、中小企業を含むサプライチェーン全体での本基盤の活用を促し、日本発の高いセキュリティ品質を備えた製品・サービス・システムの普及を目指す。

このために、前述の主要 3 政府施策等と連携し、国際動向も踏まえながら、自動車、スマートホームやビル、さらに通信・放送、電力、公共交通、防衛などの各分野（Industry by Industry）に求められるセキュリティポリシー、IoT 機器の認証や IoT 機器のセキュリティ確保策の策定に貢献する。これらを果たすべく、2021 年度からは、安心・安全にかかわる認証制度確立に向けた取り組みを強化する。

〇国際連携のシナリオ

サイバー攻撃は、国境を越えて行われるものであるため、国内だけの取組では十分ではない。また我が国の IoT 機器・サービスの海外展開においても、米国、欧州各国等と考え方を統一することは重要で、各国との連携を強化するなど、常に国際ハーモナイゼーションを視野に入れた取組を進める。

具体的には各省庁と連携して、国際シンポジウムなどを活用し、世界各地域の有識者との積極的な意見交換を行い、我が国／本プロジェクトの取組への理解を得るとともに、各地域の取組の理解と比較などを行うなどにより、国際的な交流を推進する。特に、本プロジェクトの取組や成果が、欧米で加速しているサイバーセキュリティのフレームワークの動き（下記）と整合しているかの検証を行い、国際競争力が確保され

ることを確認しつつ研究開発を進めるとともに、2021 年度からは、国際標準や業界合意への反映への取り組みを強化する。

- 米国 NIST SP800-171：「管理された非格付け情報（CUI）」を管理するためのサイバーセキュリティ対策基準。既に防衛調達のサプライチェーンにおいて NIST SP800-171 の遵守等が求められている（DFARS Clause 252.204-7012）。
- 欧州サイバーセキュリティ認証フレームワーク： 2017 年 9 月に発表した政策パッケージの中でフレームワークの整備を表明。

○SIP の課題間、他の国プロとの連携

SIP 第 2 期の基盤技術課題(サイバー空間、フィジカル空間）とは、コア技術についての相互連携に取組む。また、Society 5.0 システムの応用課題（自動運転、物流他）とは、共同の実証実験実施などについて相互連携を調整する。

これらの取組により、Society 5.0 実現で更なる経済発展が期待される自動運転やスマートビル、5G 通信サービス、防衛産業等のセキュリティ品質を確保し、国際競争力を高めることを目指す。

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推進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）、戦略的イノベーション創造プログラム（SIP）第 2 期（平成 29 年度補正予算措置分）の実施方針（平成 30 年 3 月 29 日、総合科学技術・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）、国立研究開発法人新エネルギー・産業技術総合開発機構法第 15 条第 2 号に基づき実施する。

(2) 弾力的な計画変更

本計画は、成果を最速かつ最大化させる観点から、臨機応変に見直すこととする。

(3) PD 及び担当の履歴

① PD

後藤　厚宏　（2018 年 4 月～）

② サブ PD

今瀬　真　（2019 年 4 月～）
瓜生　和久　（2019 年 4 月～）

③ イノベーション戦略コーディネーター

藤田　恭弘　（2020 年 3 月～）

④ 担当参事官（企画官）

新田　隆夫　参事官　（2018 年 4 月～2019 年 7 月）
福島　千枝　企画官　（2018 年 4 月～7 月）
近藤　玲子　参事官　（2018 年 7 月～2020 年 7 月）
高村　信　　参事官　（2020 年 7 月～）

⑤ 担当

岡崎　皓広 （2018 年 4 月～2020 年 6 月）
丸山　英治 （2020 年 7 月～2021 年 3 月）
八木　寛雄 （2021 年 4 月～）

添付資料　資金計画及び積算

2018 年度　合計　2,500 百万円

（内訳）

1.研究費等（一般管理費・間接経費を含む）	2,350 百万円
（研究開発項目毎内訳）	
（A）「信頼の創出・証明」技術の研究開発	850 百万円
（B）「信頼チェーンの構築・流通」技術の研究開発	750 百万円
（C）「信頼チェーンの検証・維持」技術の研究開発	670 百万円
（D）『サイバー・フィジカル・セキュリティ対策基盤』に関わる動向調査	80 百万円
2.事業推進費（人件費、評価費、会議費等）	150 百万円

2019 年度　合計　2,200 百万円

（内訳）

1.研究費等（一般管理費・間接経費を含む）	2,050 百万円
（研究開発項目毎内訳）	
（A）「信頼の創出・証明」技術の研究開発	750 百万円
（B）「信頼チェーンの構築・流通」技術の研究開発	600 百万円
（C）「信頼チェーンの検証・維持」技術の研究開発	700 百万円
2.事業推進費（人件費、評価費、会議費等）	150 百万円

2020 年度　合計　2,255 百万円

（内訳）

1.研究費等（一般管理費・間接経費を含む）	2,050 百万円
（研究開発項目毎内訳）	
（A）「信頼の創出・証明」技術の研究開発	800 百万円
（B）「信頼チェーンの構築・流通」技術の研究開発	550 百万円
（C）「信頼チェーンの検証・維持」技術の研究開発	700 百万円
2.事業推進費（人件費、評価費、会議費等）	205 百万円

2021 年度　合計　1,980 百万円

（内訳）

1.研究費等（一般管理費・間接経費を含む）	1,889 百万円
（研究開発項目毎内訳）	
（A）「信頼の創出・証明」技術の研究開発	866 百万円

（B）「信頼チェーンの構築・流通」技術の研究開発　610 百万円
（C）「信頼チェーンの検証・維持」技術の研究開発　413 百万円

2.事業推進費（人件費、評価費、会議費等）　91 百万円

2022 年度　合計　2,007 百万円
（2022 年度配分額 1,822 百万円と前年度までの事業推進費繰越額の計）
（内訳）
1.研究費等（一般管理費・間接経費を含む）　1,828 百万円
（研究開発項目毎内訳）
（A）「信頼の創出・証明」技術の研究開発　788 百万円
（B）「信頼チェーンの構築・流通」技術の研究開発　623 百万円
（C）「信頼チェーンの検証・維持」技術の研究開発　417 百万円

2.事業推進費（人件費、評価費、会議費等）　179 百万円