令和４年度

戦略的イノベーション創造プログラム（ＳＩＰ）第２期

最終成果報告書（公表版）

課題名：IoT 社会に対応したサイバー・フィジカル・セキュリティ

2023 年　３月　２日

目次

1　課題全体の概要と課題目標の達成度

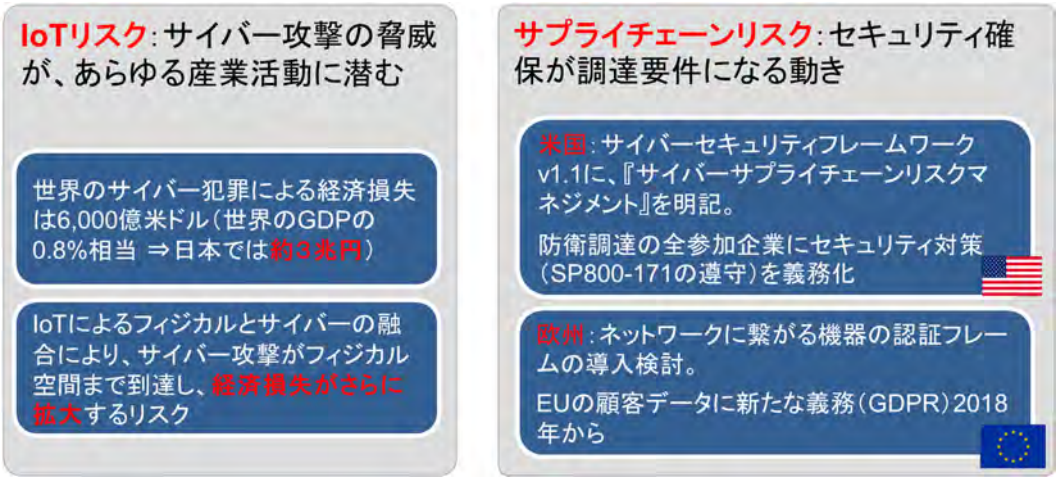
（1）課題全体の概要・目標

【ポイント】

- ✓ Society5.0[1]においては、サイバー攻撃の被害はフィジカル空間に及ぶ
- ✓ セキュリティ確保は「個々の組織が守る」だけでなく「サプライチェーン全体を守り、かつ証明する」ことが世界的ルールとして求められている
- ✓ 簡便に解決する手段が存在しないため、その『サイバー・フィジカル・セキュリティ対策基盤』技術を開発し、社会実装する
- ✓ 本基盤は、極小暗号モジュールを信頼の基点として信頼チェーンを構築し、IoT システムのソフトウェアの真贋判定・異常検知、さらにサプライチェーンの全組織の信頼性確保まで、IoT サプライチェーンのサイバーセキュリティ確保を実現する。
- ✓ 本基盤の強靭化により、Society5.0 がもたらす約 90 兆円の価値創出を支えるものであり、本技術が創出するグローバル市場規模は 10 年後に 3.5 兆円と期待される

【2018 年の状況】

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ため、IoT[2]社会では、サイバー攻撃の脅威は、あらゆる産業活動に潜むと認識しなければならない（図表 1-1）。2017 年における世界のサイバー犯罪による経済損失は 6,000 億米ドル、66 兆円（世界の GDP の 0.8%相当 ⇒日本では約３兆円）と報告されており、将来の IoT 社会では、IoT によるフィジカルとサイバーの融合により、サイバー攻撃がフィジカル空間まで到達し、経済損失がさらに拡大するリスクを抱えている。



図表 1-1 IoT リスクとサプライチェーンリスク

[1] https://www8.cao.go.jp/cstp/society5_0/

[2] IoT　Internet of Things

サプライチェーンのセキュリティリスクの拡大も懸念されている。米国ではサイバーセキュリティフレームワーク v1.1 に、『サイバーサプライチェーンリスクマネジメント』が明記され、防衛調達の全参加企業にセキュリティ対策（SP800-171 の遵守）を義務化されることになった。また、欧州では、ネットワークに繋がる機器の認証フレームの導入が検討され、2018 年５月から GDPR が施行され、顧客データの扱いに新たな義務が明確になるなど、サプライチェーンにおけるセキュリティ確保が調達要件になる動きが活発化している。

【本課題の狙い】

本課題では、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、多様な IoT システムやサービスからなる大規模サプライチェーン全体を守り、自治体の行政サービスや中小企業でも活用できる『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。

サイバー脅威に対する IoT システム・サービスの強靭化に向けた対策基盤のコア技術を開発する。製造・流通・ビルサービス・自治体サービス等のサプライチェーンでの実証を通じて対策基盤の有効性を確認する。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を有する産業分野において本対策基盤の社会実装を推進する。

【事業終了時点のアウトプット目標（技術的達成目標）】

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、それがもたらす信頼（トラスト）情報をサプライチェーン全体で流通・共有できる『サイバー・フィジカル・セキュリティ対策基盤』を確立する。

本対策基盤は、センサ等の末端の IoT 機器に内蔵可能な極小の暗号モジュールを信頼の基点とし、リソース消費率が 10%以内の高効率かつ実時間の真贋判定機能と、大規模ＩｏＴシステム（10,000 台規模）かつ多様なプロトコルにおいても異常を検知できる機能を有する。また、自治体などの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ほか、世界的に進む組織面でのルール形成に対し、サプライチェーン全体でルールを共通解釈し、準拠していることを対外的に証明できる技術を実現する。

この対策基盤を、技術実証を通じて機能面と性能面の有効性を確認し、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 社会の強靭化を図り、我が国のセキュアな Society5.0 実現に寄与することを目指す。

【アウトカム目標（社会的波及効果、市場規模等経済的波及効果）】

IoT 社会の強靭化（サイバー犯罪による経済損失回避と急速に拡大するデジタル社会のト

ラスト確保）により、Society5.0 の実現がもたらす約 90 兆円の価値創出を支える。具体的には、グローバルなサプライチェーンに参画する要件となるセキュリティ確保を適切なコストで実現することにより、日本の製品・サービスの国際競争力を強化（輸出主体の製造業の参入機会の確保）する。また、多様なサービスが複合的に連携する社会サービス・行政サービスにおいて、サービスのサプライチェーン全体のトラスト確保を支援する。

本課題では、国主導で進めて社会全体に貢献するとともに、当初から課題認識のある製造・流通・ビル等のユーザ企業と連携した研究開発と実証実験を進め、研究開発実施者（参画企業）も主体的に製品化・事業化を行う。欧米の基準とすり合わせながら府省による制度整備と連携して IoT システム・サービスやサプライチェーンへの導入を促進し、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%に成果の導入を目指す。

図表 1-2　期待されるグローバル市場規模　（2020 年）

信頼の基点となる暗号モジュール

- **適用産業**:**IoT 末端デバイス分野**
- **産業規模 : 25 兆円**/現在 **→ 40 兆円**/10 年後（出典 IDC IoT 全体の楽観的グローバル市場見込みの内、端末は 10%と想定）
- **適用分野のセキュリティ被害: 5.2 兆円**/10 年後（対策無の場合 10%の成長鈍化を想定）
- **本技術が担うセキュリティ産業規模: 2,600 億円**/10 年後（本技術貢献額 5%想定）
- **アジア展開と国際競争力**:米国、欧州の PC 向け競合技術（TPM 他）との競合が小さい極小 IoT デバイス向けセキュリティ技術としての競争力あり。

サプライチェーン全体の IoT リスクを抜本的低減

- **適用産業**:**スマート X 分野**（X = 工場、ビル、モビリティ、物流、シティ等）及び上記のインフラとなる 5G（特に各事業向けローカル 5G 等）
- **産業規模 : 10 兆円**/現在 **→ 98 兆円**/10 年後（内ローカル 5G: 0.1 兆円 → 10.8 兆円）（楽観的グローバル市場見込み）
- **適用分野のセキュリティ被害: 8.8 兆円**/10 年後（対策無の場合 10%の成長鈍化を想定）
- **本技術が担うセキュリティ産業規模: 4,400 億円**/10 年後（本技術貢献額 5%想定）
- **アジア展開と国際競争力**:米国の「クリーンネットワーク構想」の潮流により、「スマートインフラや通信インフラを信頼可能」とできる本技術は国際的な競争力に資する

サプライチェーン全体の信頼性確保

- **適用産業**:製品が人命に影響を及ぼすと想定される**既存の産業分野**（自動車、医療機器等）、およびビルサービス。自治体などの信頼に関わる情報などの業務関連データを取り扱う分野。
- **産業規模: 600 兆円**/現在 **→ 930 兆円**/10 年後（国内:54 兆円→78 兆円, 年 4%成長の楽観的見込み）
- **適用分野の信頼低下の影響: 55.8 兆円**/現在（対策無の場合の売上げ成長低下: -9.3%、EBIDTA 低下: －16.2%）
- **本技術が担うセキュリティ産業規模: 2,8 兆円**/現在（本技術貢献を 5%と想定）
- **アジア展開と国際競争力**:サプライチェーン全体でルールへの対応を示す仕組みは国際競争力あり。

2020 年に市場について再調査を行った（図表 1-2）。『サイバー・フィジカル・セキュリティ対策基盤』に見込まれる市場規模は、基盤を構成する

- 信頼の基点となる暗号モジュール技術
- サプライチェーン全体の IoT リスクを抜本的低減技術
- サプライチェーン全体の信頼性確保技術

が、それぞれ新たな市場を開拓することが期待でき、その合計は概算で 10 年後において 3.5 兆円/グローバルである。

【2022 年の状況】

近年、サプライチェーンのセキュリティリスクは急激に拡大している。

例えば 2020 年 12 月に SolarWinds 社のネットワーク管理ソフトウェアがサーバ攻撃の被害を受けていたことが明らかになった。同社の製品の更新ファイルに不正なコードが埋め込まれたまま顧客に配布され、当該ソフトウェアを利用していた米国政府機関や大手企業の内部情報が流失したと言われている。

そのほか、2021 年 6 月には米コロニアル・パイプライン社がランサムウェアの攻撃を受け、石油パイプラインが停止し市民がパニックに陥ったのは記憶に新しい。

これらのサイバー攻撃の増大を踏まえ、バイデン大統領は 2021 年 5 月に大統領令(EO 14028)を発行。連邦政府及び政府と契約する事業者のサーバーセキュリティ強化を命じた。この中には IoT 製品の安全にも言及されている。

また、国内においても、病院や、部品製造会社へのランサムウェア攻撃により、業務停止などフィジカル空間への影響が起きている。

欧州ネットワーク・情報セキュリティ機関（ENISA）では 2021 年 7 月にプレスリリースを行い、攻撃の増加を予測するとともに、対抗するために全体で協調して共通のセキュリティレベルに到達することが必要と述べた。

米国では大統領令を受け、SBOM[3]の本格採用の動きが出ているほか、MITRE 社より、サプライチェーンを健全化する”System of Trust”（SoT）の枠組みが示された。

本課題で開発してきた『サイバー・フィジカル・セキュリティ対策基盤』の各研究開発成果は、これらの対策を現実化させる技術となっており、本課題の先進性が改めて示された。

[3] SBOM　Software Bill of Material

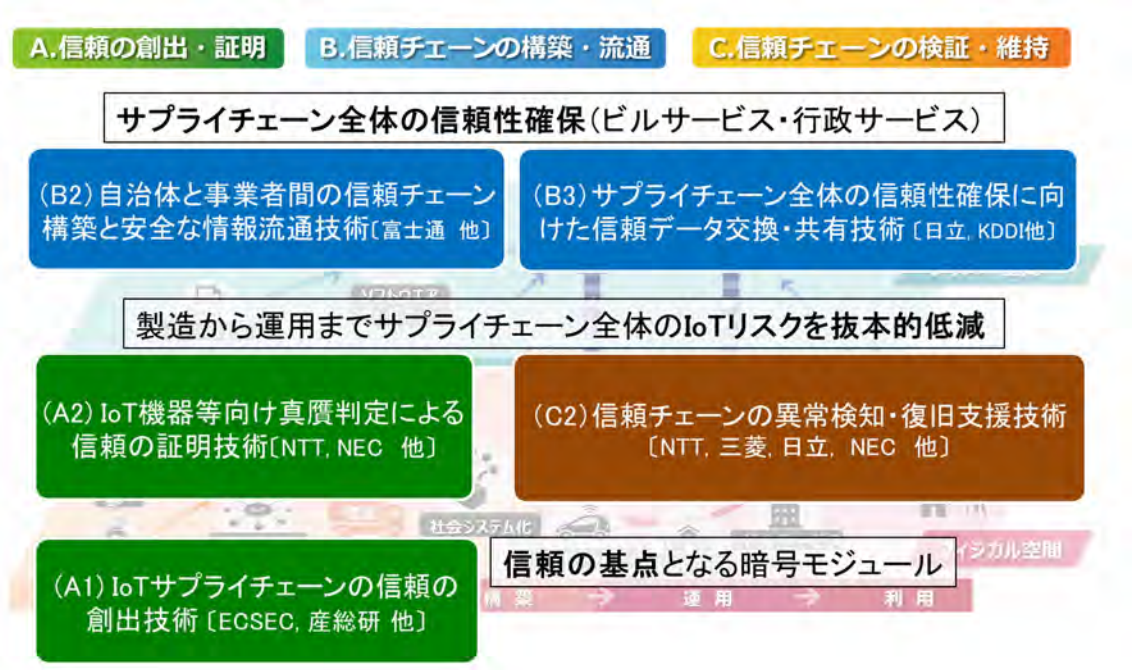
（２）課題目標の達成度

①国際競争力

【ポイント】

- ✓ 信頼の起点となる「暗号モジュール」、それを用いた IoT システムのリスク低減技術、その信頼性をサプライチェーン全体で証明する技術、の 3 階層からなる対策基盤を開発しており、世界的にも例がない取り組み
- ✓ グローバル市場で需要が高まる「国際標準 SBOM」へ、いち早く対応
- ✓ MITRE の提唱する System of Trust を、現実化させるための多くの技術を先行して開発済み
- ✓ 対策基盤を構成する個々のコア技術は、グローバルベンチマークにより、世界をリードできる見込みがしめされている

本課題は、“信頼の基点”として極めて小さい IoT デバイスにも搭載可能な暗号モジュール､その基点に立脚し､“製造から運用までサプライチェーン全体の IoT リスク抜本的低減”を可能するソフトウェアの真贋判定、高度な異常検知機能、および情報の安全な流通機能の実現、さらに、組織や人間系の行動、国際的なルール形成への対応を可能とする“正しい手順保証を基点にサプライチェーン全体の信頼性確保”の 3 階層の技術開発より『サイバー・フィジカル・セキュリティ対策基盤』を構成する（図表 1-3）。これは世界的にも例がなく、新規性は極めて高い。



図表 1-3　『サイバー・フィジカル・セキュリティ対策基盤』の技術開発

米国をはじめとしたグローバル市場で需要が高まる「国際標準 SBOM」へいち早く対応。A2 ソフトウェアを導入することで、構成機器の証明情報を SBOM に対応した形式で出力が可能となる。また、MITRE の提唱する System of Trust を現実化させる多くの技術（図表 1-3）を先行して開発。国際標準の動きも始まっており世界をリードしている。

本課題を構成する５つの研究テーマ毎に、そのテーマが目標とする技術の特性からグローバルベンチマークを実施している。

“信頼の基点”となる暗号モジュールは、世界的にも新規市場開拓となる極小組込み機器分野において、IoT 末端機器向けセキュリティチップが満たすべき要件を８項目設定し分析した。いずれも競争品に対して優位であるが、特に超小型機器で唯一のセキュリティ性能を有する。

“製造から運用までサプライチェーン全体の IoT リスク抜本的低減”を可能する真贋判定、高度な異常検知機能、および情報の安全な流通機能は、グローバルに評価されている技術との比較において、技術面と市場・コスト面から多角的に比較した結果、世界をリードできる見込みである。

“正しい手順保証を基点にサプライチェーン全体の信頼性確保”の技術については、企業や製品・サービスの信頼性の保証を目指す取組みを広く集めて分析した結果、対象要素数と対象フェーズ（検証可能内容）において優れるだけでなく、実現時の性能においても、優れていることを示すことができている。

②研究成果で期待される波及効果

【ポイント】
- ✓ サイバー犯罪による経済損失の回避により、Society5.0 の実現を支える
- ✓ 製品・サービスのセキュリティ品質向上・コストの削減・国際競争力強化に貢献する
- ✓ 多様なサービスが複合的に連携する社会サービス・行政サービスにおいて、サービスのサプライチェーン全体のトラスト確保を通してデジタル社会に貢献する

課題全体としては、本基盤技術の普及により、サイバー犯罪による経済損失の回避により Society5.0 の実現によりもたらされる価値創出約 90 兆円/2025 年を支える。また、製品・サービスのセキュリティ品質向上・コストの削減・国際競争力強化への貢献により製造業等の国際調達参入機会の確保につながる。

研究テーマ毎の波及効果は次の通りである。

- “信頼の基点（A1)”となる暗号モジュール、SCU 搭載チップは極小の IoT 機器に搭載可能であることから、あらゆるサプライチェーンの末端までセキュリティ機能を届けることが可能であり、セキュアな Society5.0 に必須の技術である。この成果により IoT 末端機器分野におけるセキュリティ市場の創出・活性化にとどまらず、製品に関わる多くのステークホルダーへのセキュリティ意識の向上、セキュリティ確保による IoT システムの総コストの低減が見込まれる。また同時に開発した耐タンパー機能は SCU 搭載チップに留まらず、多くの集積回路に展開可能な技術であり、セキュリティ対策技術へ貢献し安全安心の社会を実現する。
- “製造から運用までサプライチェーン全体の IoT リスク抜本的低減”を可能する真贋判定（A2）および高度な異常検知機能（C2）は、サプライチェーン攻撃が現実化し社会に実害を及ぼし始めている中、主要な米国政策の一つであるソフトウェアサプライチェーンセキュリティリスク対応の取組み（SBOM）に適用可能であるとともに、国内外の標準等が規定するサプライチェーンセキュリティリスク要件をより高いレベルで満たして、社会の安心・安全に貢献できる。また、この状況を商機として IoT/OT[4]機器メーカ向けビジネス、及び当該 IoT 機器を活用したセキュリティ監視サービスをそれぞれ創出して、セキュリティ産業を活性化し、継続的にセキュリティ人材を産み出すことで、日本の IoT 社会の進展を支えることができる。
- 情報の安全な流通機能（B2）は、分散・協調型の接続プラットフォーム実現により、データサプライチェーンのセキュリティ対策を均質化し、データ利活用にかかる社会的費用の削減に貢献する。加えて官民データ連携を促進する。自治体への展開に加えて、自治体業務に関わる中小事業者に展開することも想定し、本技術の導入や運用に関する支援サービスを企画・提供することで、地域経済の活性化にも貢献する。
- 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（B3）は、世界

[4] OT　Operational Technology

のルール形成に向けた動き（WP29, DFARS, GDPR 等）に呼応して、説明責任を果たすための仕組みを実現し、国内産業の製品・サービスのセキュリティ品質向上、コストの削減等の国際競争力強化へ貢献する。これにより国内製造業等の国際調達参入機会の増大が見込まれる。さらに、さまざまなモノ、コト、価値の繋がりによる新たな価値創出をめざす Society 5.0 において、『規程通り行ったことを示す』ことの価値を高め、信頼のエコシステム形成による国内産業競争力強化をめざす。同様の取組み（SoT）は米国でも始まったが、先行して開発してきた本技術では実用レベルになっており、今後は SoT 他と連携して世界をリードすることが期待される。

③達成度（１）SIP 第２期５年間の設定目標に対する達成度について

【ポイント】

- ✓ [A1] 世界最小、最小消費電力のセキュア暗号ユニット（SCU）の LSI チップ開発に成功
- ✓ [A1] ケーブルコネクターにも搭載可能とし、幅広い実用化に目途
- ✓ [A2] サプライチェーン攻撃から製品を守る IoT/OT 向け軽量かつリアルタイム性に優れた真贋判定システムを実現
- ✓ [A2] SBOM 対応のソフトウェアサプライチェーン対策で先行
- ✓ [B2] 信用情報流通、合意形成、分散セキュリティ制御を可能とする精選接続技術(TFC)を開発
- ✓ [B2] 自治体と地域コミュニティ組織間での住民サービスのサプライチェーンにおける実証評価により実用性を検証
- ✓ [B3] 複合サービスのサプライチェーンにおいて信頼構築フレームワークを実現する VCP モデル、デジタルエビデンス、トラストストアを開発
- ✓ [B3] 都心の大規模ビルのテナント衛生管理サービスとビルファシリティのサプライチェーンで機能実証に成功
- ✓ [C2] 大規模サプライチェーン上の事業者を守る異常検知・統合分析システムを実現
- ✓ [C2] AI を活用による幅広い FA/BA プロトコルに対応
- ✓ [C2] 運用現場での対策を自動立案できるリスク分析を実用化

- “信頼の基点”となる暗号モジュール（A1）は、セキュリティ、高性能・省リソース、セキュリティ保証の揃った SCU 搭載チップ試作の成功により、低リソースの末端までセキュアな IoT システムの技術を実証した。また、これを活用したセキュアかつ実用的なコネクターシステムを確立し、コネクターシステムへの実装を想定した鍵管理運用システムの開発を完了した。
- “製造から運用までサプライチェーン全体の IoT リスク抜本的低減”を可能する真贋判定（A2）および高度な異常検知機能（C2）では、軽量かつ実時間での真贋判定と高度な異常検知技術の技術開発に目途をつけ、“技術検証システム”への実装および、それを利用しての IoT ベンダとの実証実験完了。商用化に向けた技術的見通しを獲得した。A2 技術の判定基準（機器構成の証明情報）を SBOM に対応させた新方式を 2022 年度の実証実験に導入。C2 の異常検知・統合分析システムは既に一部の商用化を開始。「OT/IoT 機器のプロトコルカバー率」は、通信プロトコルの超多様性に対して独自の分析方式を創出し計画通りのカバー率を達成。
- 情報の安全な流通機能（B2）は、不特定多数の組織からビジネスなどで協働するパートナーを精選し接続する「精選接続技術」を確立し、開発技術を搭載したソフトウェアモジュール：Trustworthy Field Constructor(TFC)として実装を完了。自治体業務に関わ

る情報を信用情報として扱えるよう適応させ、実証を通じて自治体業務における安全なデータ流通環境として実用レベルに到達。

- サプライチェーン全体の信頼性確保技術(B3)は、複合サービスのサプライチェーンにおいて信頼構築フレームワークを実現する VCP モデル、デジタルエビデンス、トラストストアを開発。加えて、期待を上回る技術導入コスト低減を達成。都心の大規模ビルのテナント衛生管理サービスとビルファシリティのサプライチェーンにおいて社会実装実現に向けた方針と計画に従い、現在 TRL7 を達成。一部成果について、SIP 期間中に事業化を完了（サービス提供開始）した。

④達成度（２）社会実装の実現可能性について

【ポイント】

- ✓ [A1] 今後の社会実装の中核事業を担う株式会社ＳＣＵを設立（技組から営利法人へ転換）
- ✓ [A1] 設備更新をしなくてもレガシーな機器に装着可能なコネクターシステムを開発、比較的安価に提供することで普及を促す
- ✓ [A2/C2] Smart City 等に向けて事業展開を推進
- ✓ [A2/C2] 複数の IoT 機器ベンダと連携し十分なセキュリティが難しい中小事業者に展開（サプライチェーン・サイバーセキュリティ・コンソーシアム SC3 連携）
- ✓ [A2/C2] 中小事業者が導入しやすい支援サービス（MSS）としてサプライチェーンの異常検知機能を提供予定。リスク分析サービスは先行してサービス化済
- ✓ [B2] ソフトウェアモジュール TFC が自治体に採用されることで、自治体事業に関わる多様な中小企業を含む民間企業の安全な情報流通が可能に
- ✓ [B2] 自治体実証実験で実用性を確認済。総務省の実証事業に提言予定
- ✓ [B3] 大企業が主体となるサプライチェーンや大規模スマートビルで採用されることにより、サプライチェーンを構成する多数の中小企業の信頼データ交換・共有を可能とする
- ✓ [B3] ビル衛生管理サービスとして事業化済
- ✓ [B3] グローバル事業に向けた欧米への提言活動と国際標準化に着手

- “信頼の基点”となる暗号モジュール（A1）では、すでに民間投資もふまえて社会実装に着手しているものが 4 件。2022 年 8 月、技術研究組合法　第 7 章第 1 節（組織変更）を適用し ECSEC 組合を改組、株式会社化。当該法人（株）ＳＣＵが責任を持って社会実装を推進する。市場分析とフィジビリティスタディーの結果、「IP ビジネス」、「SoC ビジネス」、「システムインテグレーション・コンサルティングビジネス」を並行して行うこととした。
- “製造から運用までサプライチェーン全体の IoT リスク抜本的低減”を可能する真贋判定（A2）および高度な異常検知機能（C2）では、社会実装部門と一体となった社会実装推進体制を構築して取り組みを推進している。具体的には本技術の特長を踏まえ、「IoT 機器のベンダや開発部門」「IoT 機器活用事業者」「情報通信サービス」等に広く提案中である。また、2023 年度以降はスマート化ニーズが高まる Smart City 等の IoT 機器（建物関連デバイス等）を 1st ターゲットとする。

  実証実験ではフィードバックループを回し、導入の容易化や対象ＯＳの拡充といった対応を進めたほか、先行技術による「リスク診断サービス」[5]を 2021 年に提供開始。

[5] https://jpn.nec.com/press/202106/20210629_01.html

また、SIP と同様に「中小事業者を含むサプライチェーンのセキュリティ向上」をめざす SC3（サプライチェーン・サイバーセキュリティ・コンソーシアム）について、経産省を通じて調整を進め、 2021 年 10 月 19 日（SC3 中小企業対策強化 WG）から連携を開始している。

- 情報の安全な流通機能（B2）では、研究開発成果の自治体への適用を目標に、自治体ビジネスを担うフィールド部門と社内外との連携強化を担う渉外部門との連携体制により自治体への SIP 成果普及に向けた社会実装推進体制を確立しており、以下の取り組みを推進する。

  実証を行った自治体への導入を目指すとともに、フィールド実証結果をもとに策定したリファレンスアーキテクチャを活用し、他の自治体への SIP 成果普及を行う。

- サプライチェーン全体の信頼性確保技術(B3)は社会実装に向け、サービスプラットフォーム BU（ビジネスユニット）に社会実装責任者を立て、事業化に向けた事業部横断での社内体制構築とリソースの割り当て含め、全体を統括して推進している。

  2022 年 8 月に衛生管理に関するビルサプライチェーンの実証の成果を活用し、日立・イーヒルズにて「T*Plats」[6]として事業化。

  グローバル事業に向けた欧米への提言活動と国際標準化に着手。ISO/TC 292 において諸外国と連携して ISO22373 を立ち上げ、標準化議論を開始したほか、PI4、ITU-T での議論も進めている。

⑤知財戦略、国際標準化戦略、規制改革等の制度面の出口戦略

特許出願は 64 件。各社知財戦略に従い、情報公開、知財化およびノウハウ化を選択。

本取組みは、個別省庁の政策の他、サイバーセキュリティ戦略、データ戦略など政府全体の戦略における重要項目。SIP 終了後も関係省庁と協力して長期的に取り組む。

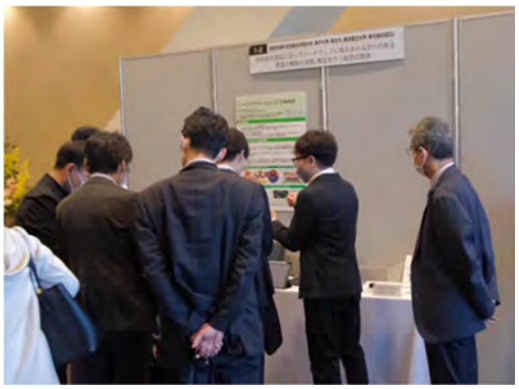
B2 では総務省「郵便局等の公的地域基盤連携推進事業」に向けた提案を実施。

[6] https://www.hitachi.co.jp/New/cnews/month/2022/08/0803.pdf

⑥成果の対外的発信

調査研究の結果を NEDO ページ[7]に掲載し、広く共有している。毎年シンポジウムを開催しているが、講演を海外のキーパーソンに依頼することで技術トレンドを確認し、研究開発に反映している。最終年度の 2023 年 2 月は 5 年間の成果を報告、宣伝するシンポジウムをハイブリッドで開催した（図表 1-4）。

図表 1-4　SIP-CPS　個別シンポジウム、その他イベント

2018	● SIP 第1期/重要インフラ等におけるサイバーセキュリティの確保[東京:、大阪] **➢米 NIST 所長 Dr. C.Romine**
2019	● シンポジウム 2019 年 10 月 31 日（木） **➢米 NTIA アラン・フリードマン （SBOM）** ➢NISC 山内智生（CS 戦略） SBOM 議論 ● SIP 第1期/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[東京、大阪] **➢ スイス連邦 フロリアン・シュッツ（ｻｲﾊﾞｰｾｷｭﾘﾃｨ Top）** ➢のうえノバ（株） 井上友二 プロトタイプ展示
2020	● ONLINE シンポジウム 2020 年 10 月 30 日（金） **➢CYR3CON Paulo Shakarian （ダークウェブ分析）** ➢経団連産業技術本部 吉村隆 成果普及に向け参加者とグループディスカッション
2021	● ONLINE シンポジウム 2021 年 10 月 22 日（金） **➢BitSight Mr.Stephen Boyer （ｿﾌﾄｳｪｱｻﾌﾟﾗｲﾁｪｰﾝ）** ➢トヨタ自動車 村田賢一 （次世代モビリティ） 成果普及に向け参加者とグループディスカッション
2022	● シンポジウム（リアル開催） 2023 年2月9日（木） **➢米 MITRE Robart A Martin（Systems of Trust）** **最終成果展示、デモンストレーション**  

[7] https://www.nedo.go.jp/activities/ZZJP2_100123.html

さらに成果普及を促す、社会課題と技術成果を紹介するビデオとガイドブックを作成した。動画は NEDO の Youtube チャネルで見ることができる。ガイドブックはシンポジウムで配布したほか、アドバイザの協力を得て、中小企業団体、厚生労働省領域、国土交通省領域などの関係者に配布している（図表 1-5)。

ガイドブック

社会課題と技術成果を紹介するビデオ

QR コードから NEDO の WEB ページ（https://www.nedo.go.jp/activities/ZZJP2_100123.html）を参照いただくと、ビデオの鑑賞とガイドブックのダウンロードができます。

図表 1-5　ガイドブックと成果紹介ビデオ

個別のテーマにおいても、積極的に対外発表を実施（学会・論文発表 102 件、講演・セミナー・展示・ニュースリリース 69 件)。

Web サイトにおける情報発信も日本語・英語の双方で実施している。

⑦国際的な取組・情報発信

国際標準化を目指して情報の収集および発信に努めている。

[A1] ISO/IEC15408 に準拠した設計開発過程を踏むことにより、セキュリティ保証面からの国際標準化を図る

[B3] ISO/TC 292/WG 4 において、ISO22373 として標準化プロジェクトを開始

[B3] Plattform Industrie 4.0 への提案、発行文書への盛り込み

[B3] ITU-T SG17 で X.509 属性証明書のユースケースを提案し、新規検討課題として設立完

2　各研究テーマの概要と課題目標の達成度

（1）研究テーマ（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

1）研究内容

第 1 期 SIP の研究成果を基礎として、市場に実在するアプリケーション分野を想定しつつ、以下の通り、信頼の基点としてのセキュア暗号ユニット「SCU」を実装した各種モデルシステムの技術実証等を行おうとするものである。これにより、IoT におけるセキュリティを飛躍的に向上させ、安全・安心な社会の実現に貢献することができる。

ア．先進的な暗号モジュールを信頼の基点として用い、これを活用したセキュアな IoT システム／サプライチェーンの社会実装めざす。具体的には、

（ア）SCU を搭載したシステム LSI チップを開発する。

（イ）上記を用いて、市場でのアプリケーションに密接した、実用的なモデルシステムを研究開発し、技術実証を行う。

上記暗号モジュールは SIP 第 1 期の成果である SCU をベースとする。

プロジェクト後半には、高機能暗号を実装した SCU の開発とモデルシステムでの技術実証も行う。

上記研究成果の社会実装を可能とするため、

イ．耐タンパー技術、対ハードウェアトロージャン（HT）技術等の研究開発を行う。

ウ．SCU を対象とするセキュリティ保証スキームを構築する。

そのための脆弱性分析技術の集約と IoT 各アプリケーション分野でのセキュリティ要求仕様のまとめ等を行う。

2）技術的目標

① SCU 搭載チップ SC01（4㎜×6㎜）、SC02（4㎜×4㎜～サイズを縮小、セキュリティを向上）、SC02ver.2（通信性能向上、データ様式に依拠しない署名検証）を開発する。

② モデルシステムによる技術実証（監視カメラ、コネクターシステム等）を行う。

3）課題目標の達成度

①国際競争力

グローバルベンチマーク 8 項目を設定。

いずれの項目においても、プロジェクト終了時に、競争品に対して優位を確立することを目標とする。SCU 搭載チップは、とくにセンサノード等の超小型末端機器への活用において優位性がある。

次の項目が、プロジェクト終了後も継続する。

【第 3 者認証スキーム】

（評価・）認証母体、技術 WG の体制確立と（SCU 搭載）実認証製品を普及するための
エコシステム構築

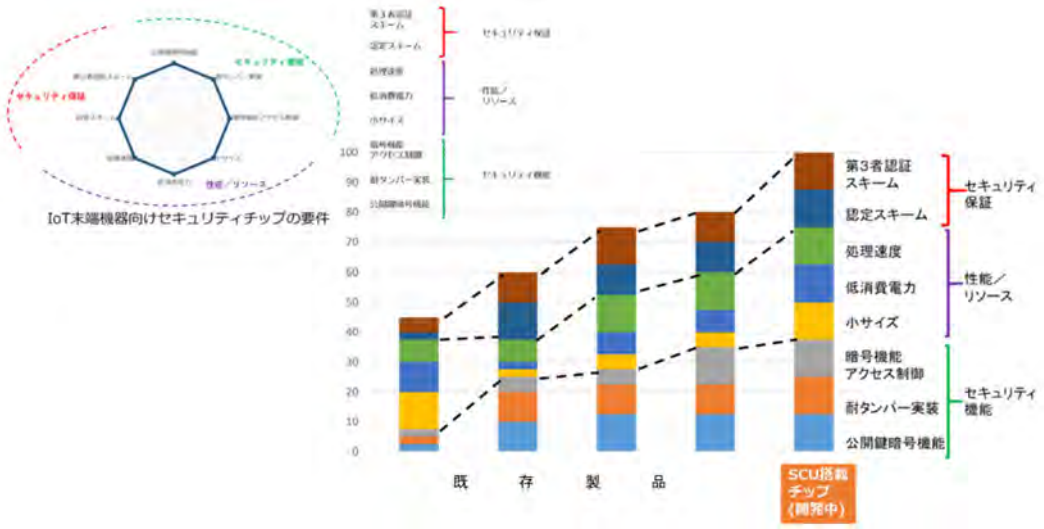
【認定スキーム】

SCU 搭載製品の開発と評価の効率化のためのツール開発と評価認定手順に関する
文書の保守

＜グローバルベンチマーク 8 項目に関する分析と注記＞

比較対象の様態が、チップ製品、IP 等異なるので、計量的な比較は困難である。

また、本研究開発完了時には、研究成果が全ての項目において優位に立てることを目標にしているが、それぞれの対象に個別の優位性があるので、それを以下に注記する。（優位性の分析等はあくまで当方の責任によるもので一部は想定を含んでいる。）



図表 2-(1)-1　サブテーマ A1　グローバルベンチマーク

②研究成果で期待される波及効果

開発された SCU 搭載チップは極小の IoT 機器に搭載可能であることから、あらゆるサプライチェーンの末端までセキュリティ機能を届けることが可能であり、セキュアな Society5.0 に必須の技術である。

この成果により IoT 末端機器分野におけるセキュリティ市場の創出・活性化にとどまらず、製品に関わる多くのステークホルダーへのセキュリティ意識の向上、セキュリティ確保による IoT システムの総コストの低減が見込まれる。

また、同時に開発した耐タンパー機能は SCU 搭載チップに留まらず多くの集積回路に展開可能な技術であり、セキュリティ対策技術へ貢献し安全安心の社会を実現する。

図表 2-(1)-2　期待される波及効果

＜新技術・市場の創出＞	
新製品・新機能への展開	公開鍵暗号を装備した IoT 用極小組込機器が可能 高機能暗号実装にもチャレンジ
科学技術の進展や新技術の確立	裏面配線パッケージングによる新しいセキュリティ対策技術の確立
新たな市場創出の可能性	IoT 末端機器分野におけるセキュリティ市場の創出
生産性向上への貢献	末端機器分野のセキュリティが確保されることによる IoT システム総コストの低減
海外展開への可能性	末端機器用のセキュリティカーネルの市場は未形成で、IoT の普及とともに地球規模で有望な分野
＜社会貢献＞	
IoT 社会の安全安心	末端のリソースに乏しい組込みデバイスに「軽く、速く、強い」「信頼の基点」を実装できるようになり、Society5.0 におけるセキュリティの実現に大きく貢献した。
経済安全保障上の貢献	宇宙分野等新たな情報セキュリティが必要とされる分野への活用の道を拓いた。 我が国半導体産業の復興に不可欠の HW セキュリティ技術のコアを確立した。

③ 達成度（1）

技術的目標は全て達成した。

図表 2-(1)-3　研究開発項目

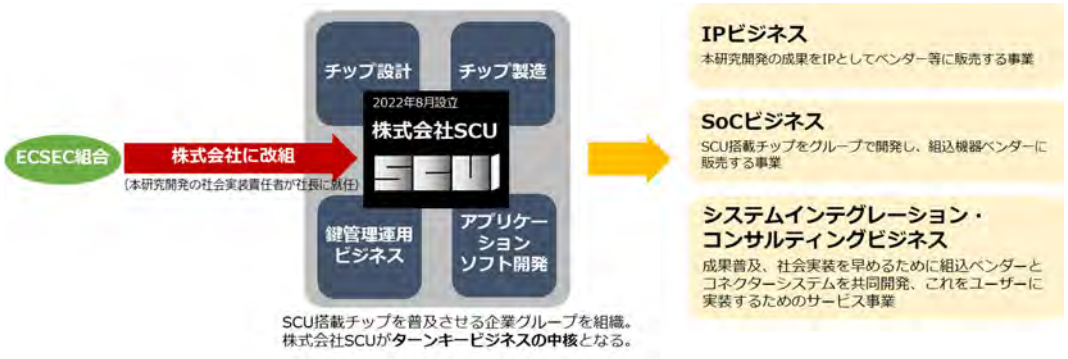
研究開発項目		研究開発目標	達成時期	備考
1.1 社会実装につながる SCU アプリケーションモデルシステムの構築と実用化技術の実証	1.1.1 一般組込み機器用 SCU アプリケーションモデルシステム	SCU を用いたアプリケーションシステムの技術実証	2021 年度	監視カメラシステムにて技術実証完了。
	1.1.2 極小組込み機器用 SCU アプリケーションモデルシステム	SCU を用いたアプリケーションシステムの技術実証	2022 年度	SCU 搭載チップ SC01・SC02・SC02ver.2 の開発・評価完了。 実用コネクターシステムの技術実証完了。
	1.1.3 高機能暗号の SCU 搭載に関する検討	1.1.4、1.1.5 のフィジビリティ検証	2020 年度	高機能暗号の SCU 搭載仕様案を策定。 1.1.5 に移行。
	1.1.4 秘匿検索用 SCU アプリケーションモデルシステム	SCU を用いたアプリケーションシステムの技術実証	選択集中により中止	2021 年実施計画変更：研究対象から削除。
	1.1.5 集約署名用 SCU アプリケーションモデルシステム	SCU を用いたアプリケーションシステムの技術実証	2022 年度	追跡機能付き集約署名アルゴリズムを FPGA 実装した試作品の開発・実証完了。
	1.1.6 IoT 向け公開鍵暗号運用システム	SCU を用いたアプリケーションシステム運用のための社会基盤技術実証	2021 年度	2021 年度までにコネクターシステムへの実装を想定した鍵管理運用システムの開発を完了。
	1.1.7 IoT 向け高機能暗号運用システム	SCU を用いたアプリケーションシステム運用のための社会基盤技術実証	2022 年度	高機能暗号鍵管理システム開発完了。
2.1 セキュリティ対策技術研究	2.1.1 SCU への脅威と対策	SCU のセキュリティ対策実装	2022 年度	裏面配線対策技術を対象としたサイドチャネル、レーザーフォールト等の攻撃の実験・評価完了。
	2.1.2 SCU の国際標準化と事業化、知財運用	SCU の認定基準の公開	2022 年度	3.1.3 と連携し、標準化戦略を完成。 ECSEC 組合の事業会社（株）SCU への移行完了（2022 年 8 月）。
2.2 ハードウェアトロージャン(HT)対策技術	2.2.1 ボード上の HT 検知技術	トロージャンセンシング技術の実現	2022 年度	技術実証用のチップ開発・デモシステム開発完了。
	2.2.2 LSI 設計 IP の HT 形式検証技術	形式検証による対 HT 技術基礎理論の構築	2020 年度	外部発表完了。
3.1 SCU のセキュリティ保証スキーム	3.1.1 組込製品用チップの脆弱性分析技術の集約	脆弱性リストの公開とメンテナンス体制の 構築、維持	2021 年度	脆弱性リスト最終版リリース。
	3.1.2 SCU アプリケーション分野別セキュリティ要求のまとめ	セキュリティ要求仕様公開	2021 年度	SCU 搭載組込機器用ワンチップの PP の ISO/IEC15408 認証取得。
	3.1.3 セキュリティ保証スキーム運用の技術的支援と SCU 認定	セキュリティ保証スキーム運用 SCU 認定スキーム運用	2022 年度	セキュリティ保証スキーム、SCU 認定スキームのための仕様設計完了。

④ 達成度（２）

ア．社会実装に向けた具体的な計画

2022 年 8 月、技術研究組合法　第 7 章第 1 節（組織変更）を適用し ECSEC 組合を改組、株式会社化。当該法人（株）SCU が責任を持って社会実装を推進する。

当初のもくろみでは、当該法人のビジネスは、研究成果知財のハンドリングが主であったが、その後の市場分析とフィジビリティスタディーの結果、「IP ビジネス」、「SoC ビジネス」、「システムインテグレーション・コンサルティングビジネス」を並行して行うこととした。



図表 2-(1)-4　社会実装に向けた戦略

イ．社会実装に向けた計画進捗状況

すでに、民間投資もふまえて社会実装に着手しているものが 4 件。

図表 2-(1)-5　社会実装に向けた取り組み状況

連携先	対象	技術実証の狙い	時期	状況
組込機器ベンダー ハイテクインター	コネクターシステム	コネクターシステムのキーデバイスであるセキュリティーアダプター（共同開発）の実証	2021 年　SC01 ボード 2022 年 5 月　SC02 ボード 2022 年 12 月 SC02ver.2 ボード試作開始	合意済み 実験開始
大手非鉄メーカ NDA により社名秘匿	工場用ロボット	ロボット制御にコネクターシステムを実装、アクチュエーターのセキュリティを実証（データファイル形式の定まった署名検証）	2022 年 5 月頃 SC02 ボードによる実験開始 2022 年 12 月頃 SC02ver.2 による実験へ移行	実証実験中
CPS テーマ A2 窓口 NTT（社会情報研究所）	真贋判定システム	A2 真贋判定システムに SCU 搭載チップを実装	2022 年 8 月 SC02 ボードを先方へ提供、A2 側で接続仕様検討中	実証実験中
SIP2 フィジカル空間デジタルデータ処理基盤 窓口 モバイルテクノ	工場オートメーションシステム（一般）	先方の工場内無線（秘密分散）通信システムと当方の有線コネクターシステムの連携による汎用的な工場制御セキュリティシステムの実証	2022 年 4 月 SC01 ボードにて接続成功 2022 年 10 月 監視カメラシステムを用いた接続実験を完了	実証実験中

⑤ 知財戦略、国際標準化戦略、規制改革等の制度面の出口戦略

＜知財戦略＞

本プロジェクトの成果を ECSEC 組合の後継会社（株）SCU が IP として普及させる。

（株）SCU は、従来予定の IP ビジネスだけではなく、いわゆるターンキービジネス（SCU 搭載ワンチップの製品販売）も視野に入れる。2022 年 8 月新会社発足。

＜国際標準化戦略＞

ISO/IEC15408 に準拠した設計開発過程を踏むことにより、セキュリティ保証面からの国際標準化を図る。

SCU のセキュリティ保証スキーム構築を研究。ICSS-JC/SWG11（Low resource chip 分科会）との連携。

同分科会をセキュリティ保証スキームの母体として活用することも検討中。

＜特許出願＞

8 件（三菱電機（株）×4、（株）SCU（発明は神戸大学）×4）

⑥ 成果の対外的発信

プレス/アウトリーチ活動など：7 件

（SIP-CPS シンポジウム×4（2019-2022）、産総研 Website、SCU 技術発表会（2022/1）、SCU 事業発表会（2022/11））

論文受理/学会採択、講演など：44 件

（e.g.国際論文誌で発表：Tsutomu MATSUMOTO, Makoto IKEDA, Makoto NAGATA, Yasuyoshi UEMURA, “Secure Cryptographic Unit as Root-of-Trust for IoT Era,” IEICE Transactions on Electronics, Vol. E104.C, No. 7. pp. 262-271, 2021.）

⑦ 国際的な取組・情報発信

ISO/IEC15408（コモンクライテリア CC）に準拠した設計開発過程を踏むことにより、セキュリティ保証面からの国際標準化を図る。本研究開発においてはSCU搭載シングルチップマイクロコントローラのセキュリティ要求仕様（PP）を作成した。本PPは、日本においてCCに基づく「ITセキュリティ評価及び認証制度（JISEC）」を運営する独立行政法人情報処理推進機より、認証を取得している（JISEC-C0764）。この認証は、国際的承認アレンジメント（CCRA）加盟国でも通用する。SCU搭載組込み機器向けマイコンが ISO/IEC 15408 に基づく認証を取得する際には、このPPが要求するセキュリティ仕様を満たすことを示せば良いこと、またそれにより取得した認証が国際的にも通用することから、本 PP の認証取得は、今後の国内マイコンベンダーの国際市場競争力の確保の点においても大変意義のあるものである。

なお、2021年4月よりTCG（Trusted Computing Group）に加入し、TCGの一員として技術情報の収集を開始すると共に、現在TCG内部で検討中のIoT版TPM規格と、本研究成果SCUとの接点がないかを検討中。

また、2020年度より、Arm社の主導する、ARM-PCI規格を調査、その提供するAPIと本研究成果SCUのAPIとの共通化の可能性を検討中。

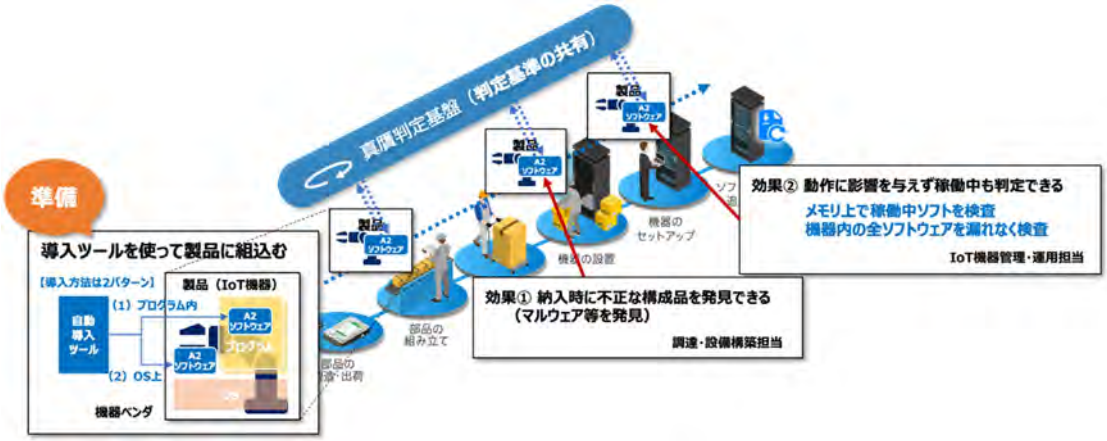
（２）研究テーマ(A2) IoT 機器等向け真贋判定による信頼の証明技術の研究開発

１）研究内容

Society 5.0 に向けてサイバー・フィジカルシステム（CPS）を構成する機器及びサービスにおけるサプライチェーンへの依存性が増大している。汎用ハード・ソフトを利用した機器開発、及びプラットフォームを活用したクラウドサービスの開発・提供が活発になり、機器調達時の「不正ソフトウェアの混入」や運用開始後の「アップデート作業及び稼働中ソフトウェアにおける改ざん」のリスクが顕在化している。サプライチェーン攻撃による実害も発生しており、サプライチェーン及び運用の全体にわたるセキュリティ強化を図る技術が必要である。

このような状況に対して本研究テーマでは、① IoT 機器のサプライチェーン全体及び大規模 IoT システムに対する真贋を判定する技術、② IoT 機器において稼働中のソフトウェアに対しても精密に真贋を判定する技術を確立した。（※新規の IoT 機器には本技術、既存の IoT 機器にはテーマ C2 によって対応する）

なお、サプライチェーン攻撃リスクは当初懸念どおり現実化し、SIP 開始時と比較してそのリスクが急速に顕在化していることから、各国政府もその対策を強化中である。本テーマでは当初より上記の懸念や課題認識を持ち、その対応策として「構成の証明」に着目した研究を進めるとともに、IoT 機器ベンダや関連事業部門の協力を得て実製品の要件を取り入れることによって、効果的な技術を先行確立することができた。



図表 2-(2)-1　ユースケースと創出効果

2）技術的目標

上記課題に対応可能な以下の新技術を IoT システム向けに確立し、従来の IT 向け技術にもない高い優位性を創出する。

(1) IoT 機器のサプライチェーンや機器の多様性、リソース制限、大規模性に対応可能な真贋判定技術

(2) IoT 機器における稼働中ソフトウェアプログラムの改ざん検知も可能な軽量性を備え、改ざん検知時の復旧も可能とする技術

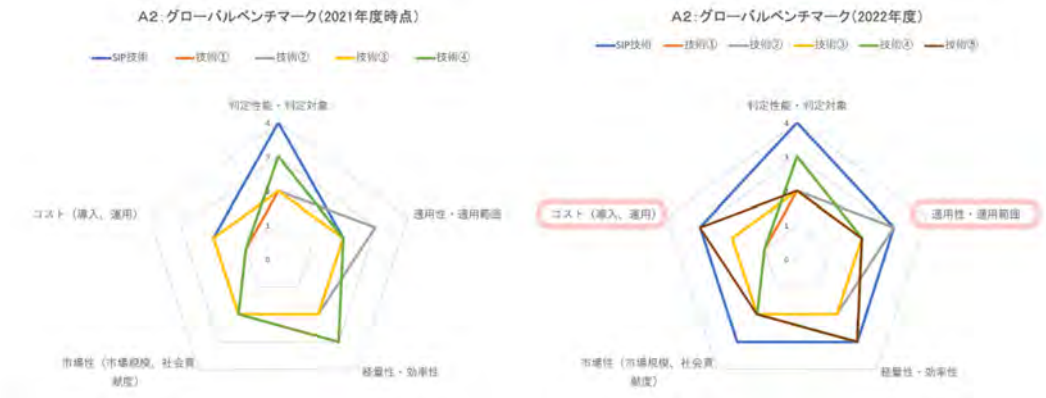
(3)

3）課題目標の達成度

① 国際競争力

- 本技術の主要な特長である「判定性能・判定対象」を競争戦略の基軸とし、当該項目における優位性を確実に確保し続けた上で、他評価項目は少なくとも他と同水準まで引き上げる方針で研究開発を進めた。
- 2022 年度は、「対応機器及び OS の拡大」によって適用性・適用範囲を向上させるとともに、「導入支援機能の実装」によってコスト（導入・運用）に関する改善を図り、優位性を高めることができている。

図表 2-(2)-2　グローバルベンチマーク（レーダーチャート）



② 研究成果で期待される波及効果

・ 新技術・市場創出
  - サプライチェーンリスクの顕在化によって、米国は大統領令を発行、日本は経済安全保障推進法の公布など、対策の義務化も視野に入れた取り組みが世界的に加速している。本技術は、上記に含まれるソフトウェアサプライチェーンセキュリティリスクへの対応に応用可能であり、各国の標準等が新たに規定するリスク対応要件を高いレベルで満たす特長も備えている。
  - また、従来技術が想定済みのリスク対応要件に対しても適合性がより高い。上記によって高まるニーズをタイムリーに捉え、サプライチェーンセキュリティリスク対応ビジネスを創出し、IoT/OT 関連事業部を通じて IoT 機器メーカを対象とした事業を展開するとともに、当該 IoT 機器を活用した IoT/OT 向けセキュリティ監視サービスを、海外を含む MSS 事業等として提供する。

・ 社会貢献
  - セキュリティリテラシが十分ではない中小事業者に展開することも想定して支援サービスを企画・提供し、IoT 社会の進展にも貢献する。
  - 特に以下の効果によって、今後急発展する日本の IoT 社会を支え、その導入実績をショーケースとして輸出ビジネスを活性化し、経済面にも貢献する。
    - ✧ コロナ禍で進む社会のリモート化において「モノの確かさ」を直接触れることなく確認する手段を社会に提供
    - ✧ Society5.0 時代に想定される IoT 機器の多様化と大規模化によるセキュリティ懸念を払拭
    - ✧ 国産IoTシステムにおいてセキュリティを付加価値とした安心安全ブランドを確立

③ 達成度（1）

- 当初5年計画時の外部情勢
  - Society 5.0 実現に向けて、従来の IT 向け技術では対応できないサイバー・フィジカルシステムを構成する IoT 機器の配送、導入、運用に至るライフサイクル全体にわたって、改造やすり替えといったサプライチェーンセキュリティリスクが懸念されていた。
- 現在の外部情勢
  - 研究開発開始当初は机上のリスクを捉えられていた印象もあるサプライチェーンセキュリティリスクであったが、ソフトウェアサプライチェーンをねらう攻撃が現実化して実害が発生している。米国政府はサプライチェーンセキュリティ対策を含む米国大統領令が発行するなど、各国が対策に動き出している。技術面ではソフトウェア構成の記述形式として SBOM が注目されている。
- 上記を踏まえた対応状況
  - 当初の設定目標については、対象機器を拡大しつつ当初目標以上の優位性を確保することができた。
  - さらに、上記の情勢変化に先立ち、リスク対応策として「機器構成に関する可視化の有効性」に着目し、技術検討とグローバル動向の監視を実施していたため、SBOM 対応ニーズの高まりにタイムリーに対応する研究開発を 2021 年度に開始することができた。
  - 本技術の判定基準(機器構成の証明情報)を SBOM に対応させた新方式を 2022 年度の実証実験に導入した。
- 5年計画に対する達成状況
- 統合検証環境
  - 実製品・実設備の模擬：
    - FA/BA 分野における実事業者へのヒアリングに基づいて実設備の模擬環境を設計・構築した。
    - A2、B2、C2 の実証先やターゲット顧客の条件（IoT 製品仕様、ベンダ設備条件など）が得られる都度、追加要件として反映した。
  - SIP 成果創出における意義：
    - 事業者と合意に至る前から実証実験相当の検証を実施し、技術課題の洗い出しを先行実施した。
    - 実証実験開始後は、顧客影響を避ける必要性から実フィールドでは実施困難な検証を実施した。
  - SIP 期間後の予定：
    - 上記を通じて蓄積した知見を、本テーマから派生する新規課題の研究開

発、SIP 成果による商用プロダクト開発に活用する予定である。

・ 実証実験を通じた技術のブラッシュアップと商用化の技術的見通し獲得
  - 2021 年度に開始した実証実験を継続・拡大して有効性を実証するとともに、これにより得られる技術課題を反映した「技術検証システム（完成版）」の実装を完了した。以上を通じて、各要素技術のブラッシュアップを完了して、商用化に向けた技術的見通しを獲得した。

・ 統合検証環境を活用したテーマ間連携技術の実現
  - テーマ（A2）（B2）及び（C2）の各技術単体では達成できない価値を生む連携技術を創出し、統合検証環境において検証を行なって有効性を実証した。

・ テーマ A1 連携
  - 2021 年 3 月に A2 技術における SCU の活用をめざした連携を開始した。2021 年度中に SCU による判定方式の机上検討を完了している。2022 年度は、A1 担当から SCU（評価ボード）の提供を受け、SIP 期間終了までに実機による試作及び検証を完了させる予定である。

④ 達成度（２）

・ 計画と進捗状況
  - 実施項目 1
    - ✧ 計画

      スマート化ニーズが高まる Smart City 等（建物関連機器等）をターゲットとしてセキュリティ脅威が顕在化するタイミングでタイムリーに提供し、事業展開を推進していく。
    - ✧ 進捗状況

      一部先行成果による商用化検討を事業部門にて開始した。
  - 実施項目 2
    - ✧ 計画

      既存のセキュリティ製品は小型の IoT 機器に適用できず、セキュリティの観点からは懸念事項である。これを事業機会と捉え、工場等で利用される IoT 機器や通信機器をターゲットとし、軽量型真贋判定技術を強みとして事業展開を推進していく。
    - ✧ 進捗状況

      一部先行成果による商用化検討を事業部門にて開始した。

・ 社会実装推進体制の構築と運営

  2021 年度当初から社会実装部門と一体となった社会実装推進体制を構築して取り組みを推進している。具体的には本技術の特長を踏まえ、「IoT 機器のベンダや開

発部門」「IoT 機器活用事業者」「情報通信サービス」等に広く提案中である。研究開発に協力可能なパートナーを早期に獲得し実証を進め、社会ニーズの高い要素技術／機能から先行確立・技術実証に投入して技術課題を着実に抽出・反映し、ユーザに受け入れられる技術を確立している。

・ 想定事業

本技術を搭載する IoT 機器、及び本技術を搭載する IoT 機器を活用するサービスに関する各事業を展開する。上記事業の実現に向け、IoT 機器ベンダ及びユーザ事業者と実証実験に取り組み、ニーズを研究開発に反映している。

・ 実証実験による課題フィードバック状況

- 導入の容易化
  開発・製造コストに影響を与える「導入作業の難易度」を抑え、自動化等により「時間短縮」する導入支援機能を実装した。
- 対象 OS の拡充
  製造現場や自社事業部門の意見を取り入れ、従来の組込み系 Linux に加えて「Android OS」にも対応した。

・ 中小事業者に向けた社会実装の取り組み

SIP と同様に「中小事業者を含むサプライチェーンのセキュリティ向上」をめざす SC3（サプライチェーン・サイバーセキュリティ・コンソーシアム）について、2021 年 10 月 19 日（SC3 中小企業対策強化 WG）から連携を開始した。これまでに複数の中小企業関連団体と、技術紹介セッション、ニーズ調査、技術セミナー等を実施し、結果を研究開発に反映した。

⑤ 知財戦略、国際標準化戦略、規制改革等の制度面の出口戦略

・ 今後、普及する IoT 機器のアーキテクチャにおいて広く活用可能なコア技術について優先的に知財の確保を行なっている。これによって、国産 IoT 製品の競争力を向上させるセキュリティ技術の権利を確保する。

・ 本技術の普及に向けて、IoT 向けのプロセッサ、セキュアエレメント、OS、及びソフトウェア構成の記述形式（SBOM）等の本技術を確立するにあたり不可欠となる要素技術は、原則、標準仕様を採用している。並行して、ゴール実現に必要となる標準、制度整備の監視や働きかけも行なっている。

⑥ 成果の対外的発信

・ 技術的内容については、研究発表・論文投稿等（国内 4 件）、展示会・シンポジウ

ム等（9 件）の対外発表を実施している。技術実証先のさらなる拡大に向けて、国内外の学会及び業界や各社の展示イベント等を活用して知名度を向上及び連携関係を構築中である。

⑦ 国際的な取組・情報発信

・ 海外向け技術紹介資料を作成するとともに、自社グループ内の海外販売チャネルを通じた提案、及び自社展示イベントにおいて海外顧客への技術紹介を実施中である。

（３）研究テーマ (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

１）研究内容

様々なモノがオンラインにつながりデータが活用されるデジタル社会に向け、「検証された組織間のみで構成する安全なデータ流通環境を迅速に構築」することによって、データ利活用の安全性を効率的に確保することを目的に、フィジカル空間-サイバー空間の組織検証の連続性と組織間の公平性を確保した接続検証・合意形成技術(精選接続技術)の研究開発を行った。

信頼性・公平性が強く求められる自治体業務へ開発技術を適用することで官民データ活用による自治体業務の効率化や住民サービスの利便性向上の実現に貢献する。

２）技術的目標

従来技術ではできていない以下の技術的目標を達成する。

- 不特定多数の組織がつながるインターネット上において、迅速かつ安全に接続相手を精選する手法(精選のための審議プロセス、審議過程で組織の信用を確認する属性情報の共有により、実世界の精選プロセスをサイバー空間に写像する技術)を確立する
- 中小企業への導入ハードルを下げるための導入・運用効率化手法(セキュリティ対策の共通化および自動制御)を補助技術として確立する
- 多数重層化するデータサプライチェーンの規模に対応するため、上記技術を実装したソフトウェアゲートウェイ(TFC(*))を10,000TFC接続したシステム構成を可能とするスケーラビリティに対応する

(*)Trustworthy Field Constructor

３）課題目標の達成度

① 国際競争力

ネットワーク仮想化技術(SD-WAN技術、ex. Cisco SD-WAN)により広域ネットワーク上のシステム間接続が柔軟になり、更に、ソフトウェア化されたネットワークとサーバ仮想化技術を合わせ、ネットワーク自身でデータ主権の確保やデータ提供条件保証など、本技術開発が目指すデータのサプライチェーンを制御するネットワークプラットフォーム(ex. IDSコネクタ)への進化が始まっている。

ここ1～2年においては、上記ネットワークプラットフォーム機能として、データを提供する人、組織の信用性(Credibility)を検証・保証する研究(ex. GAIA-X、Social IoT、 System of Trust、など)が始まってきている。

データのサプライチェーンを制御するプラットフォーム技術は今だ黎明期にあり、目的別に技術開発が行われている。利用者間の合意に基づき接続先を制御する汎用性

を持ち、既存システムへのボルトオンが可能な本技術は他に無く、データのサプライチェーン市場の創出が可能と考える。

国際的に通用する技術とするため、国際的な技術動向を元にグローバルベンチマークの対象を選定し、比較を行った結果を図表 2-(3)-1 に示している。

・比較対象技術の選定

本技術に関連する基本技術 (SD-WAN: 仮想ネットワーク技術)をベースに、データ流通基盤として現在急速に EU において研究開発が進められている IDS コネクタを比較対象とした。

・比較項目

本研究開発が対象とする①サイバー空間における接続制御、②ガバナンス（ルール統制)、③セキュリティ対策を比較項目とし、さらに、社会実装を観点に、④市場性、⑤導入・運用コストを比較項目に選定。

本技術の主要な特長である「サイバー空間における接続制御(接続先保証)」「ガバナンス(ルール統制)」「セキュリティ対策(脅威対策適用範囲、方法)」を競争戦略の基軸とし、当該項目における優位性を確保済み。

データ流通環境における接続先検証は、今後競争が激しくなる領域であり、他技術とも共通の弱点と言える導入コストの改善に SIP 終了後も取り組み、中小規模に受け入れられる技術をめざす。

図表 2-(3)-1：グローバルベンチマーク（レーダーチャート）

②研究成果で期待される波及効果

・新技術・市場創出

データを連携させることでデジタル化による行政効率化・地域活性化に対する高いニーズ・意欲を持つ自治体が複数あり、本技術適用による安全に行政事業関連データの連携による効率化・サービサビリティ向上が期待されている。特に、コロナ禍を契機として、柔軟かつ安全なデータ連携のニーズは高まっており、既存システムへのボルトオンが可能な本技術は、自治体を中心に市場に受け入れられると考える。

自治体以外の事業者(製造業等)においては、パートナーを含めたサプライチェーンのリスク管理としてのニーズは確認できており、Society5.0 の進展にあわせて需要が拡大すると想定している。

・社会貢献

分散・協調型の接続プラットフォーム実現により、データサプライチェーンのセキュリティ対策を均質化し、データ利活用にかかる社会的費用を削減することで官民データ連携が促進され、自治体が住民に提供する行政サービスの円滑化や高度化が期待される。

自治体への成果普及を通じて、データ利活用による地域課題解決・住民サービス向上に貢献するとともに、データ活用を妨げる法令・規則等の課題を抽出・提言し、データを活用しやすい環境づくりにも貢献する。

③ 達成度（1）

- **当初5年計画時の外部情勢**

  データ利活用の進展によってサプライチェーンは「サイバー・フィジカル・システム」により様々な業種プレイヤーが参加するエコシステムへと変化し、プレイヤーの多様化によってサプライチェーンが複雑化することで、サプライチェーンの構築・運用負担の増加や、個社依存のセキュリティ対策では防げないサイバー攻撃被害の増大が想定される。このネガティブな状況を回避するため、多様なプレイヤーが柔軟かつ効率的にサプライチェーンを構築し、かつサプライチェーン全体の安全性を維持する仕組みの確立が求められた。

- **当初5年計画時の設定目標**

  サイバー空間上で組織がサプライチェーンの変化の起点となれるデータ流通環境の構築、および、持続的に安全性を維持するための下記技術を確立することで、サプライチェーンの複雑化に伴う運用負担増大の回避やセキュリティリスクの低減を目指した。

  - 信用情報をもとにサプライチェーンに参加する組織の信頼性を評価し参加組織間で共有するとともに、組織間で公平性を持った合意形成を行うことに安全に情報流通が可能な「信用できる場」を形成する技術
  - セキュリティ脅威への対処を共通化し、自律的に適用することで「信用できる場」に参加する組織の安全性を均質に維持する技術

- **現在の外部情勢**

  製造業等では、IoT活用による自社生産現場の作業効率化など、自社内・グループ内の生産性向上がデータ活用の主目的となっており、パートナー間でデータ連携することによるリスク管理や新たなパートナーとのビジネス協創など、サプライチェーンの高度化・次世代化にまでは手が届いていない状況である。

  一方、行政においては、官民のデータを連携させることでデジタル化による行政効率化・地域活性化に対する高い意欲を持つ自治体が複数あり、データ連携を行う多数の任意組織と安全かつオンデマンドに接続する環境のニーズがあることが確認できた。

- **上記をふまえた対応状況**

  行政事業関連データと民間データの連携による効率化・サービサビリティ向上を目指している地方自治体への社会実装に注力することとした。2022 年度に実証実験に取り組み、その結果に基づいて商用化開発を推進している。

- **精選接続技術の確立と実証を通じた実用性の確認**
  - 不特定多数の組織からビジネスなどで協働するパートナーを精選し接続する「精選接続技術」を確立し、開発技術を搭載したソフトウェアモジュール：Trustworthy Field Constructor(TFC)として実装を完了した。精選接続技術を構成する主要技術は以下の通り。

    1. 参加者自身が開示した実世界の組織情報の開示・相互検証・合意形成を可能とする信用形成３層モデルをサイバー空間に実装し、他技術にはないサイバー空間と実世界における組織の実態検証に基づいた一意性検証を可能とした。[8][9][10]

    2. 検知したセキュリティインシデントを分析し、脅威の侵攻レベルを脅威リスクレベルとして算定(見える化)、実被害がある脅威リスクレベルに関する脅威情報を全 TFC で共有および 1 次対策の自律適用により、信用形成 3 層モデル全体の安全性を維持可能な優位性を確立した。

    3. 脅威リスクレベルの算定値に基づいた TFC 横断の統計分析による不断の状態監視により、セキュリティ脅威の脅威発生状況や予兆、利用者が行うべき対処をリコメンデーションとして通知する技術を確立することで、セキュリティ専門家に依存しない安全性維持の実現について見通しを得た。[11][12]

  - 精選接続技術を自治体業務に関わる情報を信用情報として扱えるよう適応させることで、自治体事業への適用を可能とし、実証を通じて自治体業務における安全なデータ流通環境として実用レベルに到達した。

  - 最大 10,000TFC 接続の拡張性について、実機環境およびシミュレーショ

---

[8] 2022－109030、”ネットワーク構築プログラム及びネットワーク構築方法、並びに通信装置”

[9] デジタルサービス・プラットフォーム技術特別研究専門委員会 第７回 DPF 研究会、”SIP 信用でつなぐネットワーク”

[10] IEEE 8th World Forum on Internet of Things、”Trusted Network Connection Control by Sharing Attributed Information”

[11] The 8th International Conference on Information Systems Security and Privacy (ICISSP 2022)、“Cyber Attack Stage Trace System Based on Attack Scenario Comparison”

[12] The 5th International Conference on Information Science and Systems (ICISS 2022)、” A Resource Importance Estimation Method Based on Proximity of Hierarchical Position”

ン環境を組み合わせた検証を行い、実用面・性能面において十分に動作可能な結果が得られ、大規模・複数業種の実運用システムへ適用できるスケーラビリティを達成した。

- **統合検証環境を活用したテーマ間連携技術の実現**

テーマ（A2）（B2）及び（C2）の各技術単体では達成できない価値を生む連携技術を創出し、統合検証環境において検証を行い、その有効性を実証した。

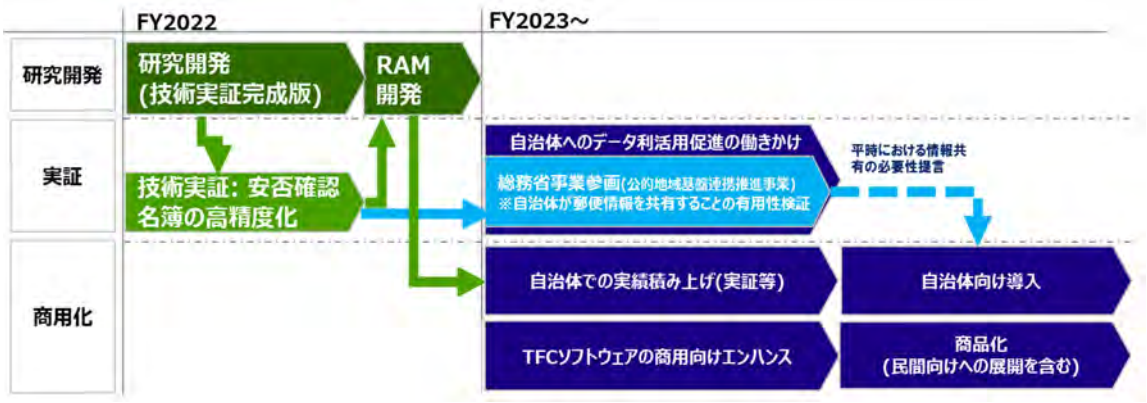
具体的には、C2 システムより検知・予測された情報を B2 システムに インプットすることで、最低限の不正通信のみが制限され、B2 システムを介して通信が行われる端末や機器などによる事業/業務の継続性の向上を達成した。

④ 達成度（２）

- **社会実装に向けた戦略と計画**

データを活用した地域活性化に取り組む自治体において、ステークホルダー間で安全にデータ交換できるデータ流通基盤のニーズがあることから、データ流通基盤のインフラとして製品化、および、導入支援事業の確立を目指す。

図表 2-(3)-2 に示すとおり、自治体をフィールドとした実証実験を通じて開発技術の実用性を実証するとともに、安全なデータ流通環境構築のリファレンスアーキテクチャを開発し、実証業務以外の住民・事業者等が直接関わる業務への適用拡大などでの実績積み上げ、更なるユースケースの拡大を図る。



図表 2-(3)-2：社会実装の推進計画

- **事業化に向けた体制整備状況**

自治体ビジネスを担うフィールド部門と社内外との連携強化を担う渉外部門との連携体制により自治体への SIP 成果普及に向けた社会実装推進体制を確立しており、以下の取り組みを推進する。

・ 実証を行った自治体への導入を目指すとともに、フィールド実証結果をもとに策定したリファレンスアーキテクチャを活用し、自治体への SIP 成果普及を行う。

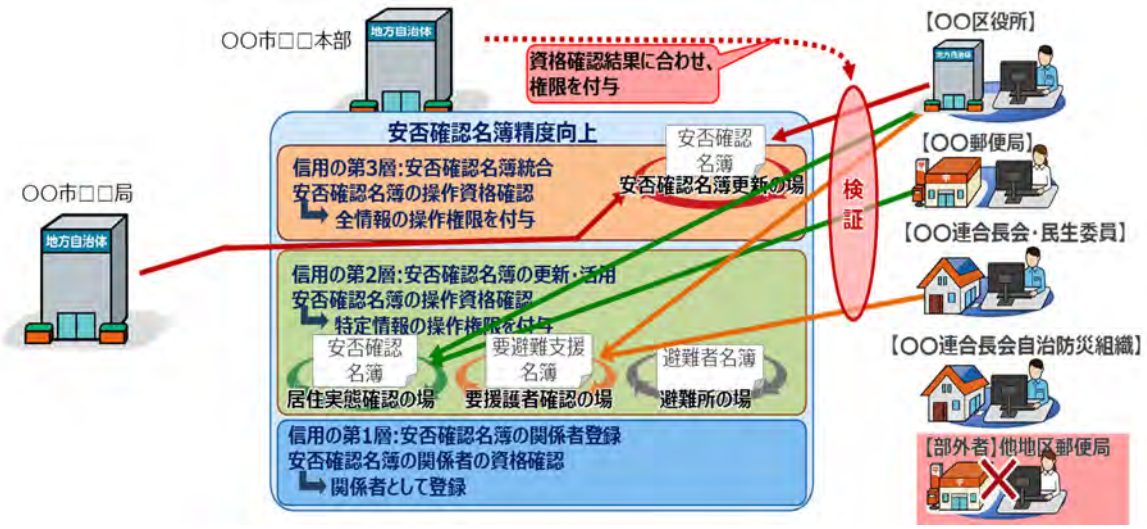
・ 渉外担当部門と連携し、自治体への展開を進めるために必要となる標準化や実装促進に取り組む。

- **成果**

1. **実証実験を通じた開発技術の実用性確認**

自治体・郵便局・民間が持つ情報を、TFC を介して安全に共有可能とすることで、情報連携による安否確認名簿の精度向上、および、個人情報を含むデータの

活用において、現行の法令やセキュリティポリシーが目指す情報漏洩対策に有効な技術であることを実証した。(図表 2-(3)-3)



図表 2-(3)-3：実証実験の概要

実証の結果、以下に示すとおり使い勝手など実適用に向けてはシステムとして対応すべき項目はあったものの、技術的には適用可能であることを確認した。

- 技術評価
  - 自治体・郵便局・民間(連合町会)が持つ情報への操作資格(誓約書, 同意書, 教育履歴等の信用情報)を検証することで信用できる場に保持される情報への操作権限を統制し、現行法令が目指す情報漏洩対策に有効な技術であることを確認した。
- 実適用に向けた課題
  - 業務フローを一括表示できるダッシュボードや処理内容にあわせたデータ加工などのツール群の提供、利用者自身による拡張可能なローコード開発機能の提供など、操作の簡単化が実適用時には重要である。
    - ➢ 商品化に向けて改善検討していく
  - 広く使っていくには、技術的な裏打ちと、自治体のシステムとしてのお墨付きが必要である。
    - ➢ 府省庁への働きかけを継続する

2. 総務省の実証事業参画に向けた提案

総務省「郵便局等の公的地域基盤連携推進事業」の令和 5 年度概算要求獲得に向けた提案を実施。日本郵便と自治体が連携し、大規模災害や事故等の緊急時に自治体へ「郵便物に関して知り得た他人の秘密」を提供することの有用性を、実

証成果を活用して検証する。(図表 2-(3)-4)

本実証事業参画を前述した課題(技術的な裏付けとお墨付き)への対応策と位置付け、平時における災害情報の精度向上による効果を実証し、郵便法における配達原簿情報の第三者提供範囲の規制緩和の必要性、規制緩和に向けた本技術の有効性を実証・提言していく。

図表 2-(3)-4：総務省「郵便局等の公的地域基盤連携推進事業」への SIP 成果展開

- **社会実装に向けた今後の課題と対処方法**

データ連携をするうえで法令や規則(とくに個人情報保護法) が障壁となり、本技術適用による業務フロー変更が実際には適用が難しいというケースが出てきている。総務省の実証事業への参画を通じてデータ連携に関する課題の提示など、データ連携がしやすい環境づくりに貢献していく。

本研究開発技術を自治体へ広く適用する上で、政府・デジタル庁などの各種計画への組み込みや標準仕様への準拠が必要不可欠であり、渉外担当部門と連携し、SIP 終了後も継続して取り組む。

⑤ 知財戦略、国際標準化戦略、規制改革等の制度面の出口戦略

- **知財戦略**

今後普及するサイバー・フィジカル・セキュリティ対策システムの　アーキテクチャを見極め、当該アーキテクチャ上で汎用的に活用可能な本技術コア技術を中心に国産セキュリティ技術としての競争力確保に取り組み、本テーマの各要素技術に関する特許出願済み(1 件)。

社会実装を通じて得られる活用技術については、リファレンスアーキテクチャを整備することで社内ノウハウとして確立し、事業化に向けた競争力を確保する。

- **国際標準化戦略／規制改革などの制度面の戦略**

社会実装においては、国内・諸外国との調和等を含めた信頼を担保する仕組みとルール形成が重要であり、府省庁や関係団体との連携により、本技術の普及を推進する。

⑥ 成果の対外的発信

研究開発期間において、展示会・シンポジウム等（4 件）、研究発表・ 論文投稿等（9 件、うち 5 件は海外学会発表）を通じて対外発表（計 13 件）を実施した。

⑦ 国際的な取組・情報発信

自治体への社会実装のため国内取り組みに注力しているが、海外動向 調査 WG を通じた海外動向の把握、自社グループ内の海外関係会社との情報交換など、将来的なグローバル展開に向けた情報収集を行っており、SIP 終了後も継続して取り組む。

（4）研究テーマ(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

1）研究内容

製品・サービスが、サプライチェーン全体で規程に従って生成、運用されたことを確認可能な、CPSF(Cyber Physical Security Framework) ※1に基づく仕組みをITにより構築し、サプライチェーン全体の『トラスト』提供を以下の技術で実現する。

※1：サイバー・フィジカル・セキュリティ対策フレームワーク[経産省]

①VCPモデル/共通VCPモデル：

規程を記述するためのプロセスモデル記法

②デジタルエビデンス：

データをセキュアに保存検索・確認可能な管理技術

③トラストストア：

サプライチェーンを辿って実施内容を共有する仕組み

④信頼構築フレームワーク：

上記の技術を適用するための作法を定めたもの

また、上記SIP技術をビル分野に適用して技術実証と価値実証を推進するとともに、研究開発の成果を国際社会へ発信し、社会実装へつなげる。

2）技術的目標

①VCPモデル/共通VCPモデル：

事業者横断で活用可能な証明方法カタログの構築、サプライチェーン全体を対象とした共通VCPモデルから個別VCPモデル作成の一連の手順構築、分野横断で活用可能な共通信頼性要件カタログの構築、共通VCPモデル作成手順の構築

②デジタルエビデンス：

製品・サービスが規程に従い生成されたことの根拠を改ざんできない形で保存し、トラストストアと連携して関連する根拠を検索するデジタルエビデンス管理を実現。

③トラストストア：

製品・サービス(付随するデータも含む)がサプライチェーン全体で規程に従い生成、運用されたことを第三者が確認・検索可能とする信頼のチェーンの構築。

サプライチェーン全体で規程に従ってデータを取り扱っていることを確認し、サプライチェーンの上流から下流に向かって原因の特定を容易に検索可能とする仕組みを実現。

④信頼構築フレームワーク：

国際社会での議論醸成を目的に、開発技術適用の作法をフレームワークとしてまとめ、情報発信とともに関係する業界団体や国際標準化団体へ提案。

研究項目との位置づけは以下の通り。

(A) 研究項目１

→①～④の技術開発に相当する。

ⅰ)信頼構築フレームワーク

国際/異業種間で信頼性を構築・評価・保証するフレームワーク

ⅱ)共通 VCP モデル構築技術

サプライチェーン全体での規格、ガイドラインなどへの準拠状況を確認可能とする共通 VCP モデルを構築する手順

ⅲ)データ適合性検証の範囲拡大と階層化した検証等への機能拡張

動的データにも適用可能な汎用的で適用範囲の広い適合性検証技術

(B)研究項目２

→①～④の実証に相当する。

ⅰ) 信頼構築フレームワークを用いた CPSF の実証

開発技術の有効性と実現性の評価に加え、技術利用時の効果の立証

(C)研究項目３

→①～④の国際連携に相当する。

ⅰ)信頼構築フレームワークの普及啓発

信頼構築フレームワークの業界団体への提案と、それによる合意形成と普及啓発

ⅱ)信頼構築フレームワークの国際標準化提案

サプライチェーンの信頼性を構築・評価・保証するフレームワークの合意形成に向けた国際標準化団体へ提案

ⅲ)信頼構築フレームワークの適用に向けた課題の整理と提言

信頼構築フレームワーク適用に必要な、制度や運用の改革を促すための提言

３）課題目標の達成度

①国際競争力

サプライチェーンに関するグローバルでの類似技術を調査、ヒアリングを行い、社会実装に必要な観点で評価を実施し、国際的な 4 つの技術動向(※)と比較してベンチマークを行った。

その結果、SIP(22 年度)技術は、対象要素と対象工程の点で、多くの要素を広いライフサイクルでカバーしており、過去の不祥事へのカバー範囲がもっとも広い。また、スループットの点では、SIP(22 年度)技術は、規模が比較対象に匹敵するスループットを備える。さらに、SIP(22 年度)技術は、共通 VCP モデルにより他にはない比較容易性を実現する。市場性やコストは他社と同等の点もあるが、サイバー・フィジカル・セキュリティ対策フレームワーク適用により技術がカバーする範囲（課題解決の効果を得る事例、業種)、サプライチェーン内の比較容易性について優位性があると考えられる。

社会実装に向けては、国際連携活動を通じて上記技術優位性をアピールすることにより認知度向上に取り組んでいく。

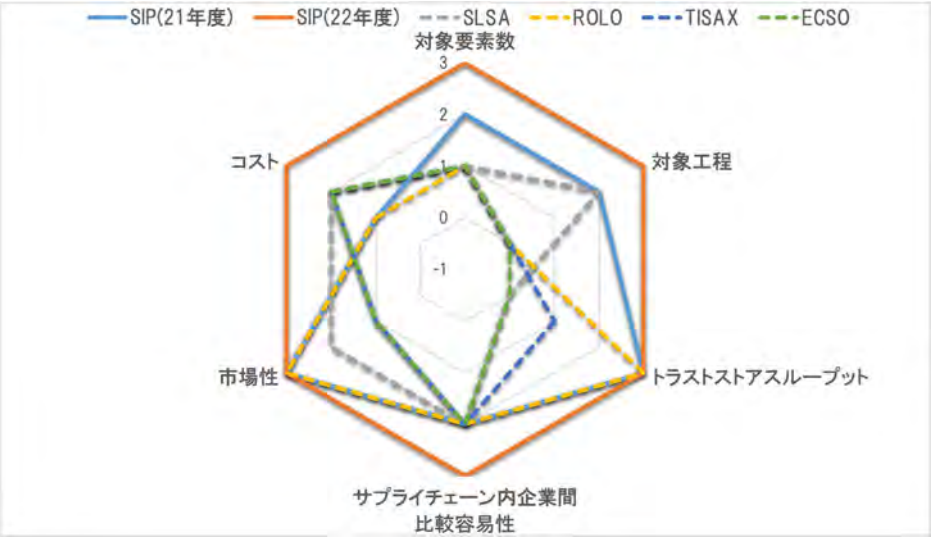
※：比較した国際技術

SLSA: Supply-chain Levels for Software Artifacts

ROLO: Register of Legal Organizations

TISAX: Trusted Information Security Assessment Exchange

ECSO: European Cyber Security Organization



図表 2-(4)-1 グローバルベンチマークのレーダーチャート

②研究成果で期待される波及効果

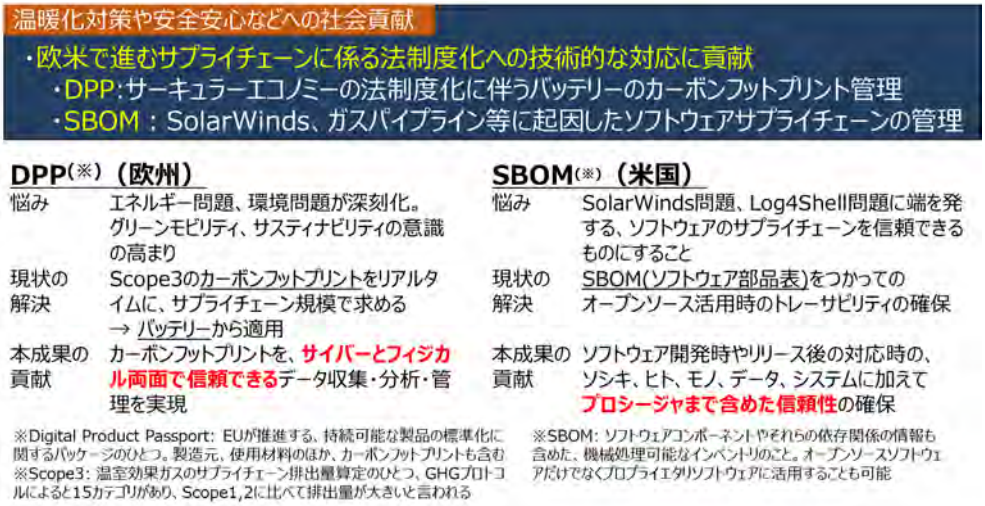
グローバルに進むルール形成に対して説明責任を果たすための仕組みを実現し、国内産業の製品・サービスのセキュリティ品質向上、コストの削減等の国際競争力強化へ貢献する。

これにより国内製造業等の国際調達参入機会の増大が見込まれる。

さらに、さまざまなモノ、コト、価値の繋がりによる新たな価値創出をめざす Society 5.0 において、以下の波及効果を得ることが期待される。

- 『規程通り行ったことを示す』ことの価値が高まり、流通することによる新市場創出、新技術創出の可能性
- 『規程通り行ったことを示す』ことに企業が積極的になり、ビジネスレジリエンス向上、信頼のエコシステム形成による国内産業競争力強化

更に、欧米で制度として具体化した DPP(Digital Product Passport)や SBOM(Software Bill of Materials)で必要とされるサプライチェーンのトラストを、日本発の信頼構築フレームワークの国際標準化および技術の確立により、諸外国よりも先行して実現し貢献する。



図表 2-(4)-2 欧米で進むサプライチェーン係る法制度への技術的な貢献

③ 達成度（1）

以下の点で目標達成が前倒しできるほどの成果を上げた。

・4 つの技術について技術目標を達成して開発完了の見込み

・開発したカタログを活用した技術導入コスト 1/20 達成（期待を上回る）

・開発技術はビル分野のトップ企業と組んで実環境における実証実施、計画を半年以上前倒して TRL7 を達成（期待を上回る）

・国際標準化に向け、予定を 1 年以上前倒して 2022 年度内に ISO/TC 292 委員会へ提案済（期待を上回る）

・証明書の X.509 拡張による実装に向けて、当初目標に追加して ITU-T SG17 で新規プロジェクトを立上げ（期待を上回る）

(A)技術：

・開発済の基本技術をサプライチェーンの現場への実装や運用のための手順書の作成完

・共通 VCP モデル構築に必要となる共通信頼要件カタログや証明方法カタログの構築および構築手順書の作成完

・信頼構築フレームワーク第 2 版の完成

・セキュリティ要件の自動・遠隔検証技術完

(B)実証

・ビルサービスのうち衛生管理とビルファシリティへの適用について実証を実施、そのうち、衛生管理については SIP 実施期間中に事業化

・技術の社会実装に向けて、現時点ですでに終了時目標である TRL7 を達成済み

(C)国際連携

・信頼構築フレームワークの国際標準化に向け、独 Plattform Industrie 4.0(以下 PI4 とする)と関係構築を行い、ISO/TC 292(セキュリティとレジリエンス)での標準化の道筋を 1 年前倒しで確立

・デジタルトラスト協議会の委員会においてホワイトペーパーを公開済

・ITU-T SG17 で証明書形式の X.509 属性証明書対応に関する技術検討を起案し新規プロェクト立ち上げ完

(D)研究項目毎の達成度

下記に研究項目毎の達成度を示す。

図表 2-(4)-3 研究項目毎の終了時達成目標に対する状況と見込み

研究項目	設定目標	状況	達成度
1-1	• サプライチェーン全体が適切な規程に従っていることを、容易にかつ効率的に確認できる仕組みの確立 • カタログ整備による技術適用コスト1/10	• 容易にかつ効率的に確認できる仕組みとして、信頼構築フレームワークを開発し、信頼構築を一般化したプロセスを定義済 • カタログ整備による技術適用コスト約1/20を達成見込み	目標を上回る
1-1(1)	• 共通VCPモデルを用いた個別VCPモデル構築手順(ガイドライン)を含む信頼構築フレームワークの完成 • 実証結果や標準化活動等のフィードバックを踏まえてブラッシュアップされた証明方法カタログや個別VCPモデル構築手順、信頼構築フレームワーク完成	• 信頼構築フレームワーク第1版、個別VCPモデル構築手順完 • 実証に向けて証明方法カタログのブラッシュアップ完。実証等のフィードバックを受けて、信頼構築フレームワーク第2版の完成見込み	予定通り
1-1(2)	• 共通信頼性要件を解説する共通信頼性要件ガイドラインの完成 • 共通信頼性要件を作成可能な共通信頼性要件カタログと、共通信頼性実施項目カタログの開発完了、ならびに両カタログの整備手順確立	ファシリティ実証に向けて、共通信頼性要件カタログ、共通信頼性要件カタログおよび共通信頼性実施項目カタログ作成完。準備や結果のフィードバックを得て、両カタログのブラッシュアップならびに整備手順を確立見込み。併せて、共通信頼性要件ガイドラインを完成見込み。	予定通り
1-2	• フィジカル空間の証跡を利用した検証技術の確立 • 証明書の拡張手法の確立	• ビル分野における実証として、エレベーター保守業務を対象とした実証を完了、検証技術確立 • 証明書拡張設計の実装評価完了、拡張手法確立	予定通り
2	・研究項目1-1の研究開発技術の有効性確認と実運用を踏まえた課題を抽出するために共通VCPモデルの策定と実証で検証 ・社会実装に必要な項目について実証結果報告に盛り込む	・衛生管理：飲食店他、公共施設や病院等、実証参加数200店舗以上で実施 ・セキュリティルーム：机上検討を完了、フィールドと実証・評価完 ・ファシリティ：VCPモデル：ビルファシリティに関わる共通VCPモデル、個別VCPモデルの策定、実証完了 顧客システムとの連接による適合性検証（プロシージャ）、デジタルエビデンス、証明書によるサプライチェーンの実証済 適合性検証（ヒト、モノ）の実証完（2022.12）、 全体検証（2022.12）、 報告書（2023.2）	予定を上回る
3-1	信頼構築フレームワークの国際的な業界団体への国際展開と、それによる合意形成と普及啓発を促進、国際提案の道筋を確立	・信頼構築フレームワークのISO提案に向け、PI4.0と関係構築し、ISO/TC292(セキュリティとレジリエンス)の道筋を1年前倒しで確立 ・サプライチェーンのトラストに関して、デジタルトラスト協議会の委員会で国内議論をリードし、ホワイトペーパを公開済 ・ドイツのフラウンホーファー研究所と共著ホワイトペーパを作成済、2023ハノーバーメッセ公開予定のPI4.0ペーパにインプット中	目標を上回る
3-2	研究・開発した信頼構築フレームワークを関係する国際標準化団体へ提案するための提案内容を作成	・RSA Conference 2021でBuilding Trust in Supply Chainsを講演 ・ISO/TC 292/WG 4議長（シーメンス）と面談、ドイツ提案プロジェクトを信頼構築フレームワークが補完で意見一致、協力合意。同プロジェクトに信頼構築フレームワークを組み込むべく提案文書作成中	目標を上回る
3-3	研究・開発した信頼性フレームワーク適用に必要な、制度や運用の改革を促すための提言を作成	・(21年度で完了）非技術分野を含めた課題を整理し、社会実装に向けた提言を整理完 ・(22年度の成果活用）デジタル庁での制度設計の検討に活用	予定通り
追加	当初研究開発項目に無し	・証明書のX.509拡張による実装に向け、ITU-Tへの提案と新規プロジェクトの立ち上げ完了、技術文書案の作成（2024年発行目標）	目標を上回る

対象技術：①VCP モデル/共通 VCP モデル②デジタルエビデンス③トラストストア④信頼構築フレームワーク

④ 達成度（２）

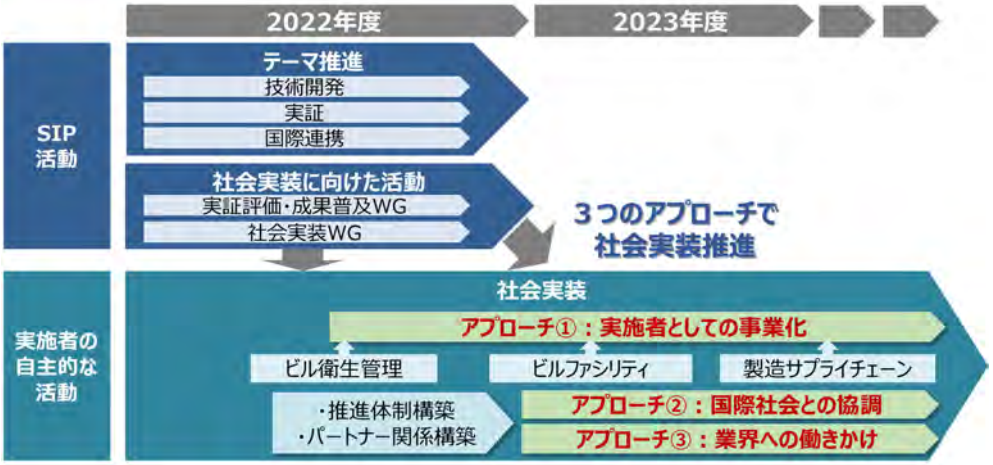
以下の点で目標達成を前倒しして社会実装に向けた成果を上げた。

・社会実装実現に向けた方針と計画に従い、社会実装責任者のもとで推進、現在 TRL7 を達成。一部成果について、SIP 期間中に事業化を完了。

(A)社会実装に向けた計画

22 年度の SIP 活動においては、23 年度以降に自走して社会実装を推進するための土台作りを推進。技術開発・実証・国際連携のテーマ推進とともに、各 WG において他の実施者と連携して社会実装に向けた活動を推進。

23 年度以降も実施者として、自主的な活動を 3 つのアプローチで継続的に活動を実施。



図表 2-(4)-4 社会実装に向けたスケジュール

(B)社会実装に向けた進捗状況

実施者による自主的な活動として、社会実装を３つのアプローチで実施し、以下の進捗を得られた。

アプローチ①：実施者としての事業化

■ 研究成果を実用化し、2022 年 8 月に「T*Plats」サービス提供開始
- ビル業界を巻き込み普及拡大を推進
- 大手デベロッパ数社、飲食業界他が参加予定。他業界との協業も模索中

■ 日立社内の事業部門と連携し、他の業界への適用を拡大

■ SBOM について、サプライチェーンでの活用を見越して、データ適合性検証技術の適用を検討中

アプローチ②：国際社会との協調

■ ISO/TC 292 において諸外国と連携して ISO22373 を立ち上げ、標準化議論を開始できた
  - サプライチェーンの信頼構築フレームワークを 9 月に提案済み
  - 産総研、日立、KDDI 総研が国内委員会メンバとして推進、独国内委員会メンバとも協力関係構築済み

■ 欧州で加速するサーキュラーエコノミーの法制度化に対し、トラストストア等を PI4 へ提案済み
  - バッテリーの CO2 排出のフットプリントの信頼性確保について提案推進体制構築済み、提案済み

■ ITU-T SG17 において日本からの提案で立ち上げた証明書形式の技術検討に関する新規課題の議論を主導する予定
  - 技術文書案を 8 月に提案し課題成立済み

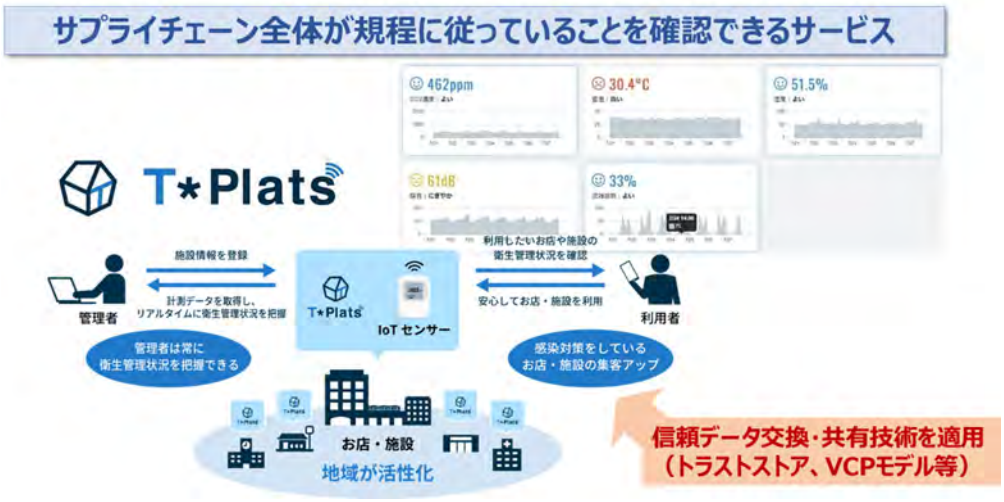
アプローチ③：業界への働きかけ

■ (一社)デジタルトラスト協議会(JDTF)でサプライチェーンの信頼性実現に向けた課題、解決策（トラストストア等）をまとめたホワイトペーパーを 2022 年 7 月に発行
  - JDTF サプライチェーン改革委員会メンバー(製造、IT、金融等)との議論を通じて、仲間作り、合意形成の枠組みを構築済み
  - 取り纏めた検討内容を各業界団体へ働きかかけ実施（10 月 CSA ジャパン、11 月 JEITA）

■ (一社)沖縄オープンラボ　Trusted Network PJ で、ワークショップ、価値検証を通じて業界へ働きかけを開始できた

(C)成果の事業化

衛生管理に関するビルサプライチェーンの実証の成果を活用し、日立・イーヒルズにて「T*Plats」として事業化。サービス開始に関してプレスリリースを行うとともに、TV3 局、ラジオ 1 局、新聞 5 紙、ネット記事 45 件で報道あり。現在、新サービスは約 200 箇所の施設が参加、主に、飲食、教育機関、医療機関、公共施設、オフィス等で活用中。



図表 2-(4)-5 事業化したサービス「T*Plats」の概要

⑤ 知財戦略、国際標準化戦略、規制改革等の制度面の出口戦略

研究開発の中で得たノウハウについて、公開すべきところと非公開とすべき技術を明確にて推進した。

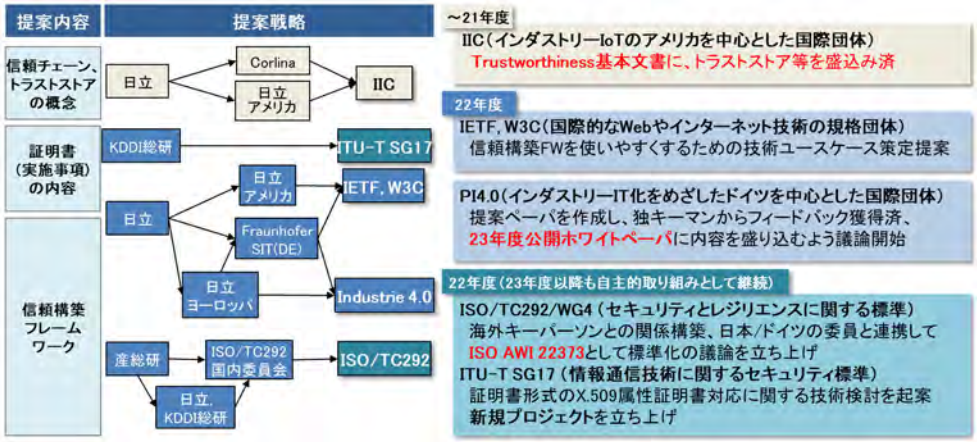
（例）成果の知財について、実装技術は非公開、「信頼構築フレームワーク」や実現技術に関するコンセプトや基本的な仕様は公開して標準化

(B)国際標準化戦略、出口戦略

国際標準化は、CPSF の取り組みや連携し、関連する国際団体へ成果をインプットするとともに、標準化団体での標準化を推進した。

国際標準化に向けた最初のステップとして以下の成果をあげており、達成度は十分と判断する。

- ISO/TC 292/WG 4 において、ISO22373 として標準化プロジェクトを開始
- ITU-T SG17 において、技術文書発行に向け議論開始。2024 年に技術文書を発行し、グローバルな技術の普及拡大を促進



図表 2-(4)-6 国際標準化に向けた提案戦略と状況

⑥ 成果の対外的発信

これまでに ISO における標準化を目的に、国際連携において推進した。ISO 以外にも IETF、PI4、IIC、ITU-T 等の国際団体に対して SIP の成果である信頼構築フレームワークや、トラストストアなどを提案し、議論を推進した。また、RSA Conference や CEATEC、IEEE 等において 20 件(内国際 8 件)以上の対外発信を実施済み。

- 2020 年暗号と情報セキュリティシンポジウム(SCIS2020)での「サプライチェーンセキュリティ」セッションにおいて、日立、KDDI 総研、NEC、産総研で計 5 件の発表を実施。
  http://www.iwsec.org/scis/2020/program.html
- セミナーや展示会で広く発信し、サプライチェーンに関する新たな仕組みの実現に向けて、解くべき社会課題、価値やコンセプトを共有する目的を達成
- 発信をきっかけとして、産業 IoT の主要団体である IIC との関係構築につなげ、彼らとのディスカッションを通じて、最終的には IIC の成果物である Trustworthiness Framework Foundations に SIP の技術成果を織り込み済み
  https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf

⑦ 国際的な取組・情報発信

国際的な情報発信と連携について以下の進捗と成果があり、現時点での達成度は十分と判断する。

【情報発信】

・セキュリティ分野世界最大の会議 RSA Conference 2021 で講演他全 8 件の国際発表を実施
https://www.rsaconference.com/Library/presentation/USA/2021/building-trust-in-supply-chains
・IEEE ICE-IAMOT Conference で論文発表、ITU-T SG17 で標準化寄書、電子情報通信学会　安全・安心な生活と ICT 研究会(ICTSSL)で論文発表
・T*Plats 事業化発表
https://www.hitachi.co.jp/New/cnews/month/2022/08/0803.pdf
・デジタルトラスト協議会ホワイトペーパー公開
https://jdtf.or.jp/report/whitepaper/file/JDTF_SCWG_%E3%83%9B%E3%83%AF%E3%82%A4%E3%83%88%E3%83%9A%E3%83%BC%E3%83%91%E3%83%BC1.0%E7%89%88.pdf

【国際連携】
・SIP の成果を織り込んだ成果物(Trustworthiness Framework Foundations)が 2021 年 4 月に大手産業 IoT 団体である IIC から正式に公開
https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf
・提案資料(New Work Item Proposal)ドラフト化、当初 2022 年度実施予定していたものを半年以上前倒して、2021 年度中の ISO 国内委員会への提案開始
・2022 年中の PI4 への提案に向け、欧州の組織と連携体制構築について合意済み
・信頼構築フレームワークがグローバルなサプライチェーンで利用可能な環境を整備
・各種団体と議論を活性化、ISO/TC 292 での信頼構築フレームワークの標準化に見通しを獲得
・ITU-T SG17 において証明書形式の技術検討に関する新規プロジェクトの立ち上げを完了

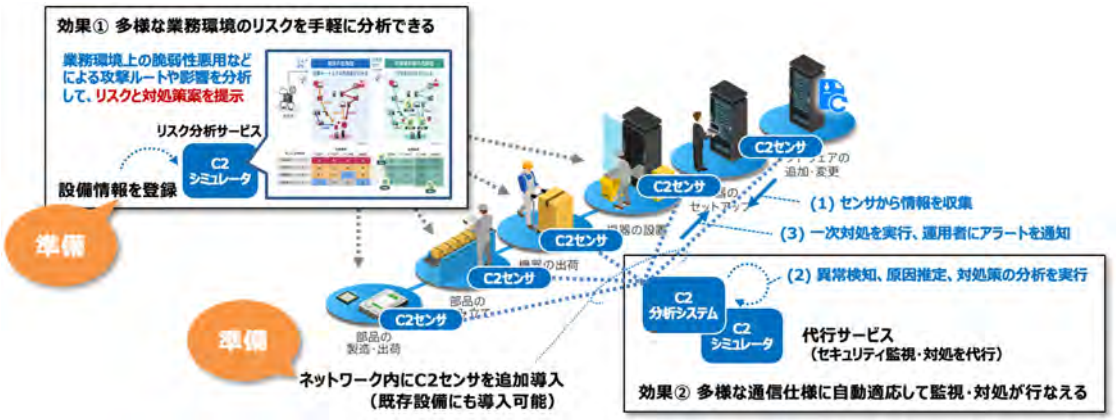
（５）研究テーマ(C2) 信頼チェーンの維持技術の研究開発

１）研究内容

Society5.0 時代のシステムは IT システムから「サイバー・フィジカルシステム(CPS)」に変化し、ゼロにならない脆弱性リスクによる影響が物理空間にも広がりさらに深刻化する。CPS では、特に構成機器の多様性と、「止められない（可用性)」「遅れや失敗が許されない(確実性)」といった特性に対応可能なセキュリティ技術が必要である。さらに、つながるシステムの急拡大による運用人材の不足が想定されるため、セキュリティオペレーションに不慣れな人材でも運用可能な技術が必要になる。

このような状況に対して本研究テーマでは、(1) サイバー・フィジカルシステムの物理事象を含む分析により高い即時性を備えた監視を実現する技術、(2) システム特性を考慮した不正データの検知・排除によりサービス継続性を確保する技術、(3) システムの仮想モデルを用いた対処策選定・影響評価により対処の安全確実な実施を可能にする技術を確立した。

なお、コロナ禍や DX で進むリモート化やサプライチェーン攻撃により、脆弱性の脅威が深刻化しており、特に OT/IoT システムでは脆弱性が放置された無防備な状態も少なくない。当該分野に関わる事業部門や顧客の生の声をもとにした研究開発によって、セキュリティオペレーションを強化する新機能を実現することができた。



図表 2-(5)-1　ユースケースと創出効果

2）技術的目標

上記課題に対応可能な以下の新技術を IoT システム向けに確立し、従来の IT 向け技術にもない高い優位性を創出する。

(1) 通信プロトコルに対する自動適応によって、多様な CPS のセキュリティ異常検知を可能とするセンシング及び分析技術

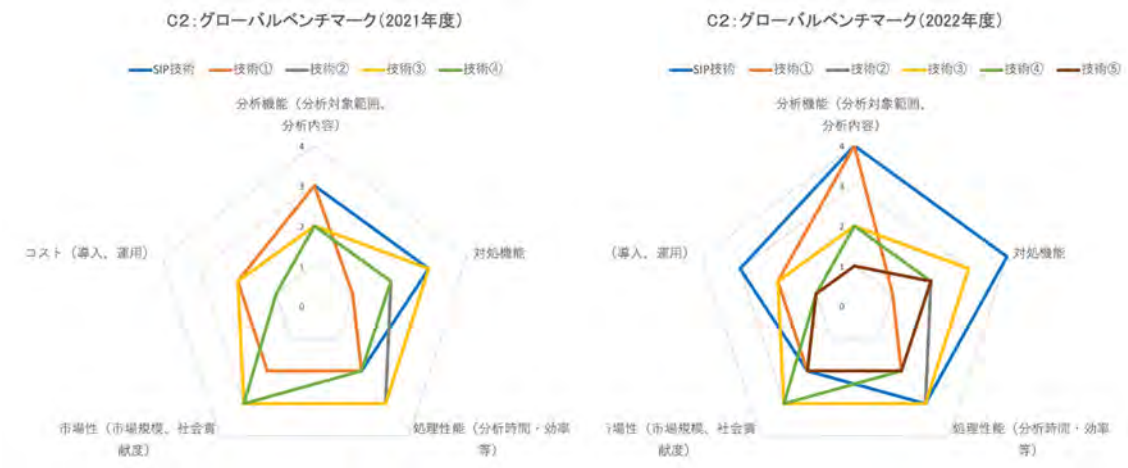
(2) システム特性情報に基づく解析によって、サービス影響を考慮した不正データ検知・対処を可能にする技術

(3) システムの仮想モデル構築と攻撃・対処シミュレーションによって、対処策の選定・実行を支援する技術

3）課題目標の達成度

①国際競争力

- 本技術の特長である「分析機能」については異なるアプローチをとる強力な製品（技術①）が存在することから高いレベルで競争しつつ、もうひとつの特長である「対処機能」も合わせた総合力で優位性を確保する方針とした。
- 2022 年度は、上記戦略に基づき「分析機能」「対処機能」について特に強化して当初目標性能を達成するとともに、中小事業者に対応する技術とするとため、実証実験や事業部門の知見を活用して「コスト」及び「処理性能」も改善を図った。
- 分析機能については、継続的に高度化している技術①と同等レベルと考えられるが、「プロトコルごとの個別開発が不要な低コスト性」と「閉域環境に対応しやすい」という点から本技術が総合力では優位と評価している。



図表 2-(5)-2 グローバルベンチマーク（レーダーチャート）

② 研究成果で期待される波及効果

・ 新技術・市場創出

- IoT/OT 機器の高機能化に伴って、汎用ハードをベースとした製品開発やソフトウェア化が進んでいる。必然的に、IoT/OT 機器においても脆弱性悪用が容易となり、攻撃側にとっては、物理空間にも影響を及ぼすことが可能という点から魅力的な標的となる可能性がある。また、IoT/OT 分野ではその事業特性上、設備を閉域環境で構築・運用するケースが少なくなく、このことがセキュリティの「隙」を生み出している。
- 上記の状況を踏まえ、本研究開発が確立する技術は、セキュリティ人材が潤沢ではない中小事業者にも活用可能な運用性と、従来製品では対応が難しい閉域環境への対応力を特長としている。この特長を最大限活かした IoT/OT 向けセキュリティ監視サービスを、海外を含む MSS 事業等として展開する。

・ 社会貢献

- セキュリティリテラシが十分ではない中小事業者に展開することも想定して支援サービスを企画・提供し、IoT 社会の進展にも貢献する。
- 特に以下の効果によって、今後急発展する日本の IoT 社会を支え、その導入実績をショーケースとして輸出ビジネスを活性化し、経済面にも貢献する。
  - コロナ禍によって利用が進むリモート化システム（生産ラインの遠隔操業、事業設備の遠隔管理等）のサイバーセキュリティリスクを大幅に低減
  - Society5.0 時代に想定される IoT 機器の多様化と大規模化によるセキュリティ懸念を払拭
  - 国産 IoT システムにおいてセキュリティを付加価値とした安心安全ブランドを確立

③達成度（1）

- 当初5年計画時の外部情勢
  - サイバー・フィジカルシステム（CPS）のインシデント対応に求められる高レベルの「即時性」「可用性」「確実性」を備えた低コストの技術がなく、Society 5.0 に向けたCPSの普及が、サイバー攻撃による回復困難な事態の頻発を招くことが懸念されていた。
- 現在の外部情勢
  - CPSに影響を及ぼすインシデントは発生し始めているものの、CPSのITシステム領域を侵害する手口が主である。また、CPS分野の事業者ではITセキュリティの導入を未だ推進している段階にあり、CPSセキュリティにまで手が回っていない。
- 上記を踏まえた対応状況
  - 上記を踏まえ、2021年度に実証実験先の意見を取り入れ、ITシステムとOTシステムが混在する環境を新たにターゲットに加えた研究開発に着手した。2022年度先行成果による実証実験を実施した。
- 5年計画に対する達成状況
-
- 統合検証環境
  - 実製品・実設備の模擬：
    - FA/BA分野における実事業者へのヒアリングに基づいて実設備の模擬環境を設計・構築した。
    - A2、B2、C2の実証先やターゲット顧客の条件（IoT製品仕様、ベンダ設備条件など）が得られる都度、追加要件として反映した。
    - 対応プロトコルの拡大を図るための環境として、EtherNet/IP、PROFINET等の産業用プロトコルを用いる機器を組込んだ。
  - SIP成果創出における意義：
    - 事業者と合意に至る前から実証実験相当の検証を実施し、技術課題の洗い出しを先行実施した。
    - 実証実験開始後は、顧客影響を避ける必要性から実フィールドでは実施困難な検証を実施した。
  - SIP期間後の予定：
    - 上記を通じて蓄積した知見を、本テーマから派生する新規課題の研究開発、SIP成果による商用プロダクト開発に活用する予定である。
- 実証実験を通じた技術のブラッシュアップと商用化の技術的見通し獲得
  - 2021年度に開始した実証実験を継続・拡大して有効性を実証するとともに、これにより得られる技術課題を反映した「技術検証システム（完成版）」の実

装を完了した。以上を通じて、各要素技術のブラッシュアップを完了して、商用化に向けた技術的見通しを獲得した。

・ 統合検証環境を活用したテーマ間連携技術の実現

- テーマ（A2）（B2）及び（C2）の各技術単体では達成できない価値を生む連携技術を創出し、統合検証環境において検証を行なって有効性を実証した。

④達成度（２）

・ 計画と進捗状況

➢ 実施項目 1

✧ 計画

スマート化ニーズが高まる Smart City 等（建物関連機器等）をターゲットとしてセキュリティ監視サービスを提供する。さらに、多様な現場設備やそのニーズに広く対応可能な高速エッジ処理装置を提供して事業展開する。

✧ 進捗状況

一部先行成果による商用化検討を事業部門において開始した。

➢ 実施項目 2

✧ 計画

品質・生産性向上を目的に適用が加速しているスマートファクトリー/流通システムの生産設備を 1st ターゲットとし、対象システム個別の特性に基づいた最適な一次対処案の提示・業務影響の評価を実施する。さらに、自動対処の機能を提供することにより各事業者のニーズに応えた利便性の高い機器を提供して事業化を推進する。

✧ 進捗状況

製品・サービス開発部署メンバが研究員として参画しており、本研究成果をもとに製品化を進めるべく準備中である。

➢ 実施項目 3

✧ 計画

サイバー攻撃は日々進化し、IoT/OT システムに対するサイバー攻撃の被害も増加している。サイバー攻撃発生時の運用者に対する対処策実行支援技術を創出すると共に、ニーズに合わせた技術の切り出しを行って段階的に早期社会実装を進め、実用化・事業化の取組みを推進する。2021 年にセキュリティリスクアセスメントサービスの提供を開始（当初計画 2023 年から 2021 年に前倒して実施）し、セキュリティリスクアセスメントのツール提供をめざす。

✧ 進捗状況

サービスのフィードバックを基に対処策自動立案機能の開発など、専門家でなくても利用可能なツールとしての提供に向けた機能開発を実施中である。

・ 社会実装推進体制の構築と運営

2021 年度当初から社会実装部門と一体となった社会実装推進体制を構築して取り組みを推進している。具体的には本技術の特長を踏まえ、「IoT 機器のベンダや開発部門」「IoT 機器活用事業者」「情報通信サービス」等に広く提案中である。研究開発に協力可能なパートナーを早期に獲得し実証を進め、社会ニーズの高い要素技術／機能から先行確立・技術実証に投入して技術課題を着実に抽出・反映し、ユーザに受け入れられる技術を確立している。

・ 想定事業

本技術を搭載するネットワーク機器、及び本技術を活用するサービスに関する各事業を展開する。上記事業の実現に向け、ユーザ事業者との実証実験を通じてニーズを分析し、技術課題を研究開発に反映している。

・ 実証実験及び商用化による課題フィードバック状況。

- 実サービスとの親和性向上
  MSS 型の監視代行サービスの現場意見を重視し、異常検知結果のレポーティング機能を改善している。
- 実運用との親和性向上
  検知事象がセキュリティ起因か別の障害起因かの切り分けを行う技術を特許化見込みである。
- 対策支援の強化
  顧客ニーズに基づき、分析結果からシステムへの推奨される対策の提示機能を新規開発、可視化機能を改善している。

・ 中小事業者に向けた社会実装の取り組み

SIP と同様に「中小事業者を含むサプライチェーンのセキュリティ向上」をめざす SC3（サプライチェーン・サイバーセキュリティ・コンソーシアム）について、2021 年 10 月 19 日（SC3 中小企業対策強化 WG）から連携を開始した。これまでに複数の中小企業関連団体と、技術紹介セッション、ニーズ調査、技術セミナー等を実施し、結果を研究開発に反映した。

⑤知財戦略、国際標準化戦略、規制改革等の制度面の出口戦略

- 今後、普及する IoT 機器のアーキテクチャにおいて広く活用可能なコア技術について優先的に知財の確保を行なっている。これによって、国産 IoT 製品の競争力を向上させるセキュリティ技術の権利を確保する。
- 通信プロトコル、外部連携インタフェース等の本技術の確立において重要となる既存要素技術は、原則、標準仕様を採用している。並行して、ゴール実現に必要となる標準、制度整備の監視や働きかけも行なっている。

⑥成果の対外的発信

- 技術的内容については、研究発表・論文投稿等（国内 16 件、うち表彰受賞 4 件※）、展示会・シンポジウム等（15 件）の対外発表、及び報道発表（2 件）を実施している。技術実証先のさらなる拡大に向けて、国内外の学会及び業界や各社の展示イベント等を活用して知名度を向上及び連携関係を構築中である。
- ※表彰受賞歴：

  ［監視技術関連］

  「第 91 回情報処理学会コンピュータセキュリティ研究会 CSEC 優秀研究賞」

  「第 24 回情報処理学会コンピュータセキュリティシンポジウム CSS2021 学生論文賞」

  ［リスク分析技術関連］

  「情報処理学会 2020 年度山下記念研究賞」

  「第 69 回電気科学技術奨励賞」

  「テレコム先端技術研究支援センター SCAT 表彰」

⑦国際的な取組・情報発信

- 海外向け技術紹介資料を作成するとともに、自社グループ内の海外販売チャネルを通じた提案、及び自社展示イベントにおいて海外顧客への技術紹介を実施中である。

３　課題マネジメント

① Society5.0 の実現を目指すもの

IoT は、Society 5.0 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。

さらに、急速に拡大するデジタル社会では、多様なサービスが複合的に連携する社会サービス・行政サービスにおいて、サービスのサプライチェーン全体のトラスト確保が必須である。

本研究開発課題は、上記の社会的課題を解決してセキュアな Society 5.0 の実現するために必要となる、『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ものであり、多様な IoT システムやサービスからなる大規模サプライチェーン全体を守り、自治体の行政サービスや中小企業でも活用することにより Society5.0 の実現を目指すものである。

② 社会実装を実現するためのマネジメント体制が構築されているか。

- 全てのサブテーマに社会実装責任者を指名するとともに、事業主体となる部門との連携を取り、ユーザのフィードバックを得られる体制を構築した。
- 特にサブテーマ A1 については、研究主体の ECSEC 技術組合が 2022 年 8 月に営利法人化。株式会社 SCU として、社会実装活動を行う。
- 社会実装 WG では、主査のもと各サブテーマの社会実装責任者が参加し、事業としての社会実装をどのような体制で進めていくべきかの議論を進め、業界団体、推進委員会専門家メンバ、関係省庁と意見を交わした。

- 『サイバー・フィジカル・セキュリティ対策基盤』の全体像を理解して貰うために「ガイドブック」を作成した。メディアミックスとして成果動画も作成。プログラム期間終了後の活動ツールとして使用する。

ガイドブック

社会課題と技術成果を紹介するビデオ

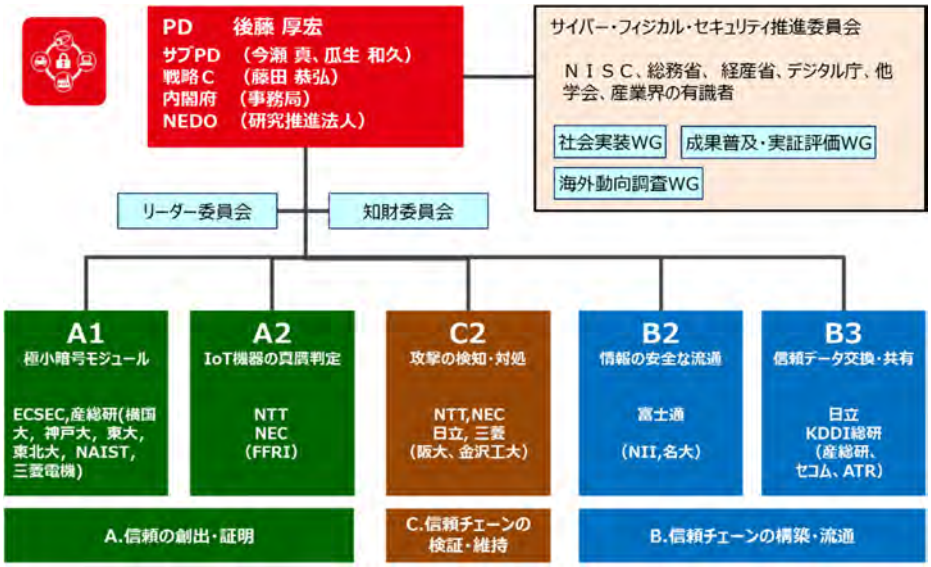
QR コードから NEDO の WEB ページ（https://www.nedo.go.jp/activities/ZZJP2_100123.html）を参照いただくと、ビデオの鑑賞とガイドブックのダウンロードができます。

図表 3-1　（再掲）ガイドブックと成果紹介ビデオ

③ **研究テーマに対する評価、マネジメントが適切に実施されているか。**

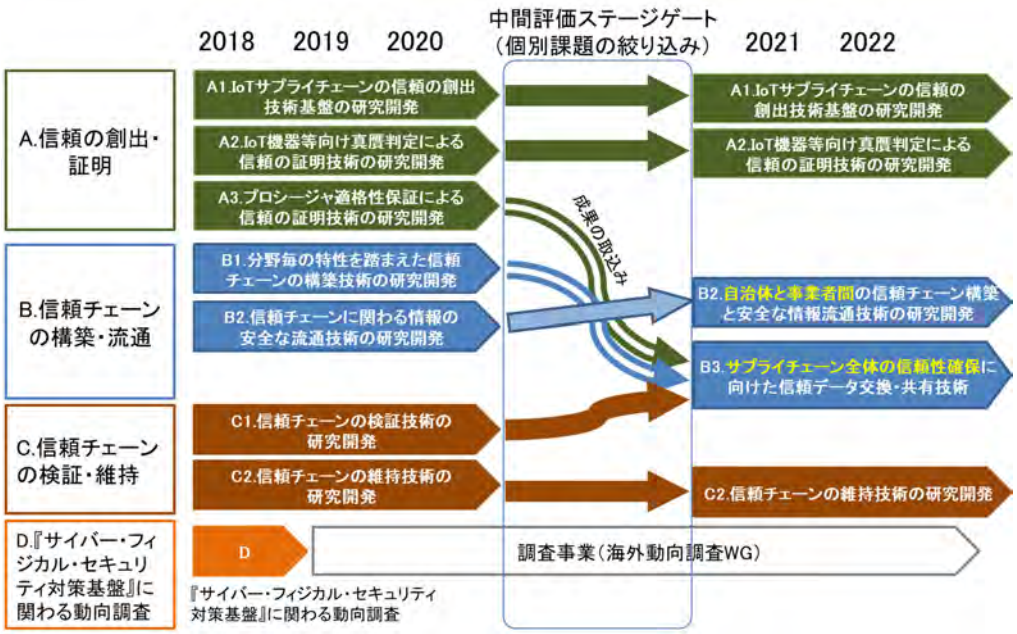
ＰＤは、サブＰＤ、戦略Ｃ、内閣府担当者、NEDO 担当者などとＰＤチームを構成し、本プロジェクトの密なマネジメントを実施。各実施者、調査事業受託者、各省庁と連携体制を構築している。（図表 3-2）

図表 3-2　課題実施体制



- 2020 年に中間評価ステージゲートを実施、社会実装を加速するためサブテーマ B3 を立ち上げた。（図表 3-3）

図表 3-3　中間評価ステージゲート



- 実証評価 WG において、グローバルベンチマークの評価軸、評価対象を精査した。
- サブテーマ別進捗会議、知財委員会、海外動向調査 WG、推進委員会などを通じて、専門家や省庁の意見、社会情勢を取り入れて方向性を定期的に確認した。
- 本プロジェクトの出口となる産業分野と関連府省庁、および、本プロジェクトが目標とする技術分野や産業活動や法制度などの有識者から構成する推進委員会を設置し、全体の方向性を検討・確認を行った。
- 実証評価のための情報共有、成果普及の施策相談、社会実装への課題共有のための各 WG を立ち上げ。府省庁、推進委員専門家、業界団体等に適宜参加いただき、御意見をいただいた。
- 研究テーマ間の連携を図るために、ＰＤチームと全研究責任者によるリーダー委員会を設け、目標を共有するとともに定期的な情報交換を実施。また、研究成果（知財等）の相互活用を円滑に進めるための知財委員会を設けた。
- サブテーマごとに進捗会議を定期的に実施（府省庁関係者　陪席）。各テーマが、研究開発計画書に沿って、適切に進捗していることを確認した。

④　民間から適切な負担を求めているか。官民の役割分担が適切になされているか。

セキュリティ技術は、未だに投資ではなくコストとみなされがちで、導入のインセンティブは低い。この社会課題解決のための技術開発を国主体で行うことにより、昨今急激に高ま

ってきたサプライチェーンセキュリティの要求に対して適用可能な技術をタイムリーに準備することができている。

各実施者はマッチングファンドによる投資も合わせて研究開発を加速し技術を確立することで、個別に関係のある企業、団体から多くの実証協力先を確保し社会実装を進めることができている。

以上から官民の適切な役割分担ができていると判断する。

⑤ マッチング額が十分に計上されているか。

年を追うごとに、マッチング率が向上しており、全体では国費と同額以上に到達。2022年度は、技術組合（8月に改組）・大学・国研からなるサブテーマA1を除く民間主体のサブテーマ（A2,B2,B3,C2)のマッチング率は2/3程度となり、目標を大幅に超える達成状況。なお民間負担額には、経費として算出できない「実証フィールドの提供コスト」などは含まれておらず、委託先による実質的な貢献は更に大きいことに留意さ

⑥ 府省連携が不可欠な分野横断的な取り組みとして実施されているか。

本ＳＩＰの取組は、PDがサイバーセキュリティ戦略本部員の観点から、政府全体のサイバーセキュリティ戦略に反映（戦略推進の前提条件となっている)。このような観点から、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の連携が重要であるため、NISC、警察庁、デジタル庁、総務省、文部科学省、厚生労働省、経済産業省、防衛省等、府省連携が不可欠であり、各省庁の担当部署のメンバに推進委員会/WGに参加いただき連携を行っている。

図表 3-4　府省連携状況

A1	厚生労働省	厚労省担当部局を通じて医療衛生分野への展開を推進中
A2C2	経産省、IPA、SC3	中小企業を含めた各主体の標準的なセキュリティ手法へ反映をめざす
B2	自治体、総務省郵政行政部	避難要支援者名簿作成に住民基本台帳外の情報を随時反映する仕組みの構築（個人情報保護法上のガイドラインを含む）
B3	経産省 CPSF ビルSWG	サプライチェーンセキュリティ上の標準的なセキュリティ手法への反映をめざす

⑦　ＳＩＰ第２期で実施する他の課題との連携が適切に図られているか。

サブテーマ A1 が「フィジカル空間デジタルデータ処理基盤」課題との連携を行っており、本年度中に連携システムに関する基礎的な実験結果が得られた。

図表 3-5　フィジカル空間デジタルデータ処理基盤との連携

連携テーマ	連携内容	状況
A1-SIP第2期「フィジカル空間デジタルデータ処理基盤」	当該研究ティームが開発中の無線機にSCU搭載ワンチップを実装することに合意した。2021年度末より技術実証開始。	2022年度監視カメラシステムを用いた実証実験を完了。

以上