資料1

「IoT社会に対応したサイバー・フィジカル・セキュリティ」推進委員会（第10回）

令和5年3月6日（月）

内閣府 プログラムディレクター
後藤　厚宏

公開用編集版

「IoT社会に対応したサイバー・フィジカル・セキュリティ」

令和5年2月3日（金）

内閣府 プログラムディレクター
後藤　厚宏

目次：SIP第2期　最終課題評価WG　PD自己点検結果説明資料

1　課題概要・目標

◆ SIP第2期開始時の状況：

–Society5.0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ため、今後のセキュリティ対策は「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」ことが必要になり、世界的ルールとして求められる

◆ SIP第2期での達成目標：

–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ができる『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

◆ アウトプット目標

–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プロダクトのサプライチェーンおよびサービスの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

◆ アウトカム目標

–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

SIP課題「IoT・サプライチェーンのセキュリティ確保」を取り巻く状況

SIPの開始時（2018年度）の「将来の想定リスク（懸念）」が、今日「現実の問題」として顕在化し、米国やEUにおいて対応策作りが急務に

SIPの開始時の将来の懸念

IoTリスク：サイバー攻撃脅威が、あらゆる産業活動に潜む

- IoT社会では、サイバー攻撃がフィジカル空間まで到達し、**経済損失が拡大**するリスク
- 欧州、米国等：ネットワークに繋がる**IoT機器のセキュリティ要件**の議論が活発に

サプライチェーンリスク：セキュリティ確保が調達要件に

- 米国：防衛調達の全参加企業にセキュリティ対策（SP800-171）を**義務化**

懸念が現実に

- 大規模ソフトウェアサプライチェーン攻撃 ⇒米国連邦政府の危機感
- コロナ禍でのグローバルサプライチェーンの分断
- 遠隔業務・在宅勤務等でのIoT機器活用の急増

SBOM：Software Bill of Materials

対応策が急遽検討

- 米国 Software Supply Chain 対策の指南書[*1] by U.S. NSA, CISA, ODNI（2022/9）とSBOM本格活用への動き ①
- 米国 MITRE社 サプライチェーンセキュリティの “System of Trust” の枠組み ②
- EU IoT類を含むネットワーク接続機器類への規制強化[*2]

*1https://www.cisa.gov/uscert/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

*2 https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

① 米国のIoT・サプライチェーンのセキュリティ確保に関する連邦政府動向

頻発するサイバーセキュリティ被害

ソフトウェアサプライチェーン攻撃の大規模被害

ランサムウェアによる事業継続攻撃の被害

重要インフラで多用されるOSSへの脆弱性への攻撃被害

LOG4J

国家のサイバーセキュリティ改善に係る大統領令（EO14028）2021/5/21

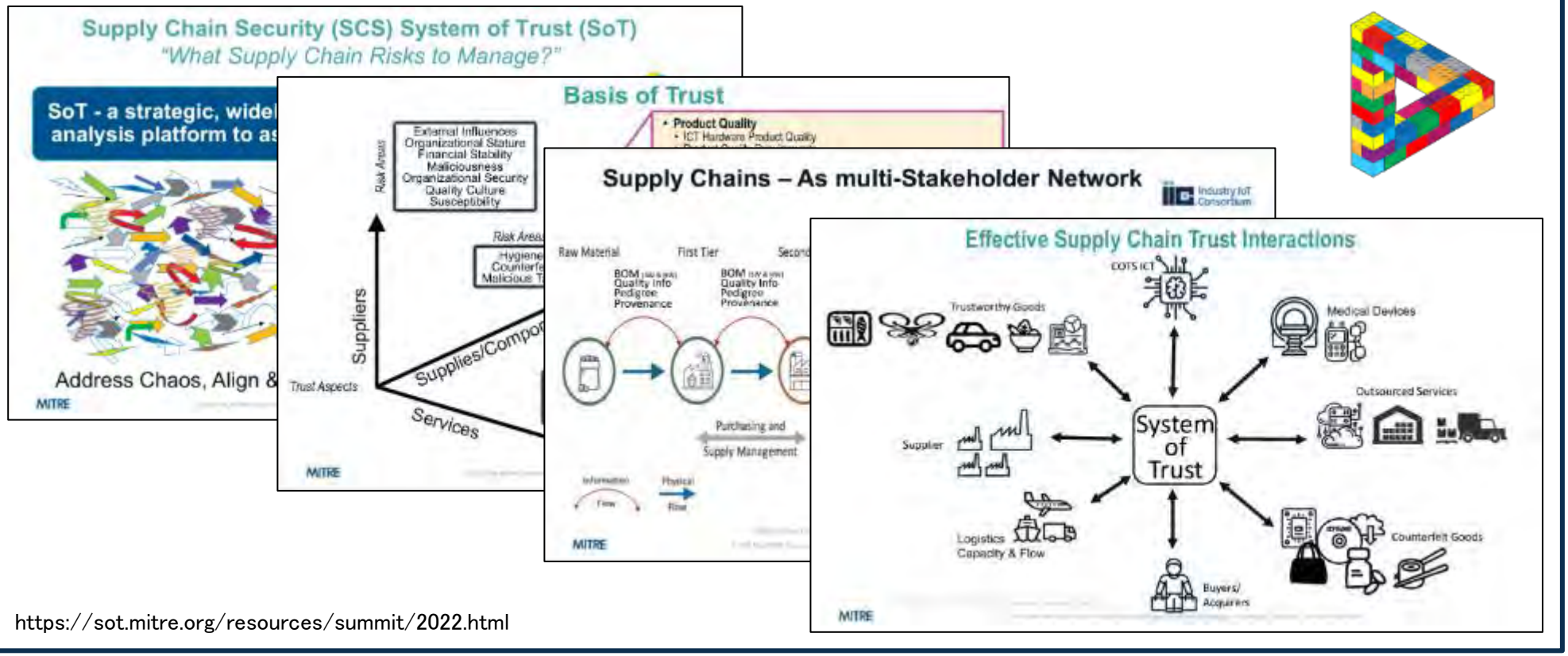
NIST National Institute of Standards and Technology U.S. Department of Commerce

2021.5.12	大統領令の署名	
2021.6.25	「重要なソフトウェア」の定義の公表	NIST DoD DHS
2021.7.9	「重要なソフトウェア」のセキュリティ対策に係るガイダンスの公開	OMB
	ソフトウェア検証の最低基準に関するガイドラインの公表	NIST DHS
2021.7.12	SBOMの最小要素の公表	OMB
2021.8.10	NISTが公開した重要なソフトウェアのセキュリティ対策に関するガイダンスを、各省庁が遵守することを求めるための措置を講じる	NIST DHS NIST NTIA
2021.11.17	ソフトウェア サプライヤー プレイブック: SBOM の作成と提供	OMB
	ソフトウェア コンシューマー プレイブック: SBOM の取得、管理、および使用	NTIA
2021.11.29	連邦政府各省庁を対象としたIoTを利用する際の手引書	NTIA
2022.2.4	消費者向けソフトウェア製品のサイバーセキュリティラベリング推奨基準	NIST
	消費者向けIoTソフトウェア製品のサイバーセキュリティラベリング推奨基準	NIST
2022.3.8まで	大統領令以降に調達されたソフトウェアに関して、各省庁がNISTによる指針を遵守するための適切な措置を講じる	NIST OMB
2022.5.5	サプライチェーン全体のサイバーセキュリティリスクを特定、評価、および軽減するためのガイダンス	NIST
2022.5.12まで	FAR審議会に対し、各省庁が購入可能なソフトウェアサプライヤーに対する上記ガイダンスに基づく要求事項の遵守と、遵守の証明を義務付ける契約文言を勧告	DHS

※経産省サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース資料等を参照

今後の輸出製品は、これらのガイドラインに対応必要

② 米国 MITRE社 サプライチェーンセキュリティの “System of Trust” の枠組み



https://sot.mitre.org/resources/summit/2022.html

2020年6月に米MITREにより、SIP-CPSと同様のコンセプト（サプライチェーン共通の安全性を確保するためのフレームワーク）が提唱されたが、その実現ツールはこれから。

⇔SIP-CPSでは当初（2018年度）から全体像を構想し、その実現技術を先行開発。

SIP課題「IoT・サプライチェーンのセキュリティ確保」を取り巻く状況

SIPの開始時（2018年度）の「将来の想定リスク（懸念）」が、今日「現実の問題」として顕在化し、米国やEUにおいて対応策作りが急務に ⇒ 先行開発してきたSIP-CPSの成果を活用（社会実装）

SIPの開始時の将来の懸念

IoTリスク：サイバー攻撃脅威が、あらゆる産業活動に潜む

- IoT社会では、サイバー攻撃がフィジカル空間まで到達し、**経済損失が拡大**するリスク
- 欧州、米国等：ネットワークに繋がる**IoT機器のセキュリティ要件**の議論が活発に

サプライチェーンリスク：セキュリティ確保が調達要件に

- 米国：防衛調達の全参加企業にセキュリティ対策（SP800-171）を**義務化**

（2018～2022） SIP-CPS の研究開発成果

- 信頼の起点（A1）からSBOM対応の真贋判定（A2）
- サプライチェーン全体でのトラスト確保（B3）と情報流通（B2）
- IoTサプライチェーンの異常検知（C2）

SBOM：Software Bill of Materials

必須のツール

懸念が現実に

- 大規模ソフトウェアサプライチェーン攻撃 ⇒米国連邦政府の危機感
- コロナ禍でのグローバルサプライチェーンの分断
- 遠隔業務・在宅勤務等でのIoT機器活用の急増

対応策が急遽検討

- 米国 Software Supply Chain 対策の指南書[*1] by U.S. NSA, CISA, ODNI（2022/9）とSBOM本格活用への動き ①
- 米国 MITRE社 サプライチェーンセキュリティの “System of Trust” の枠組み ②
- EU IoT類を含むネットワーク接続機器類への規制強化[*2]

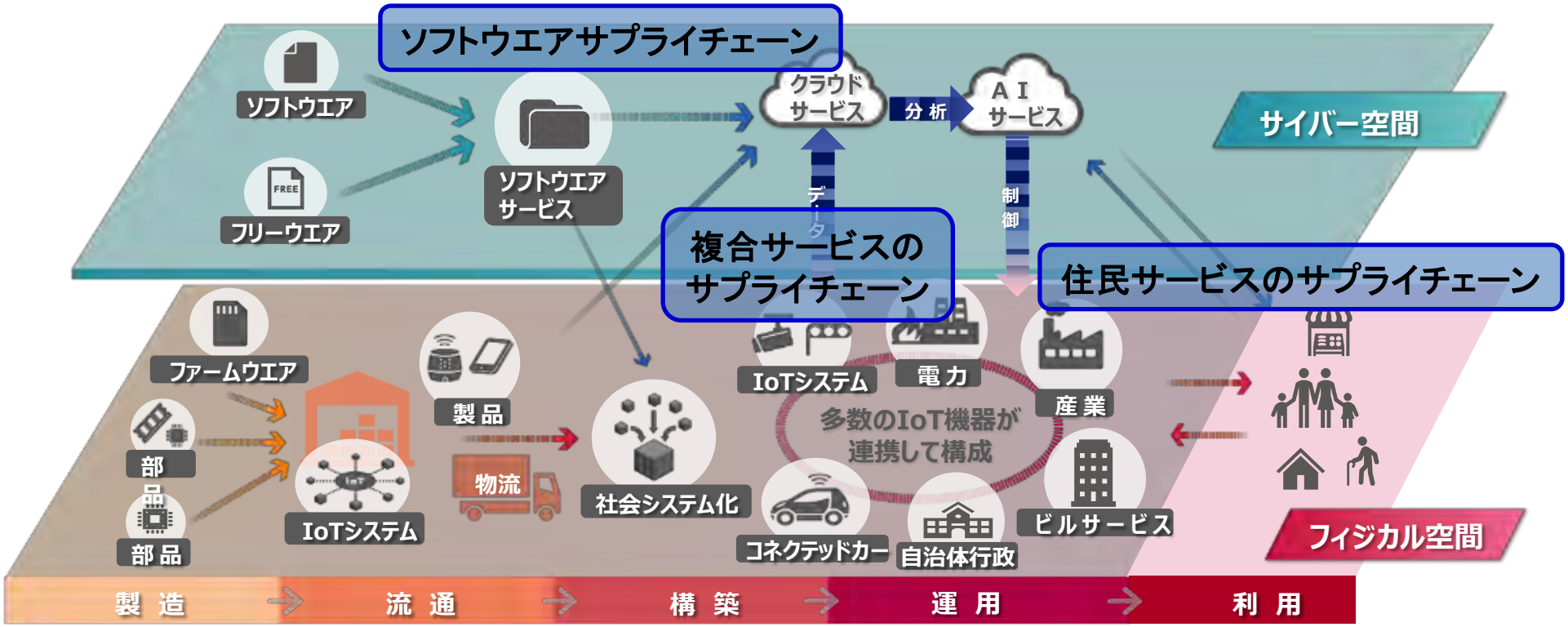
*1https://www.cisa.gov/uscert/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

*2 https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

『サイバー・フィジカル・セキュリティ対策基盤』の貢献領域

IoT機器やサプライチェーンの各構成要素について，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**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**を確保

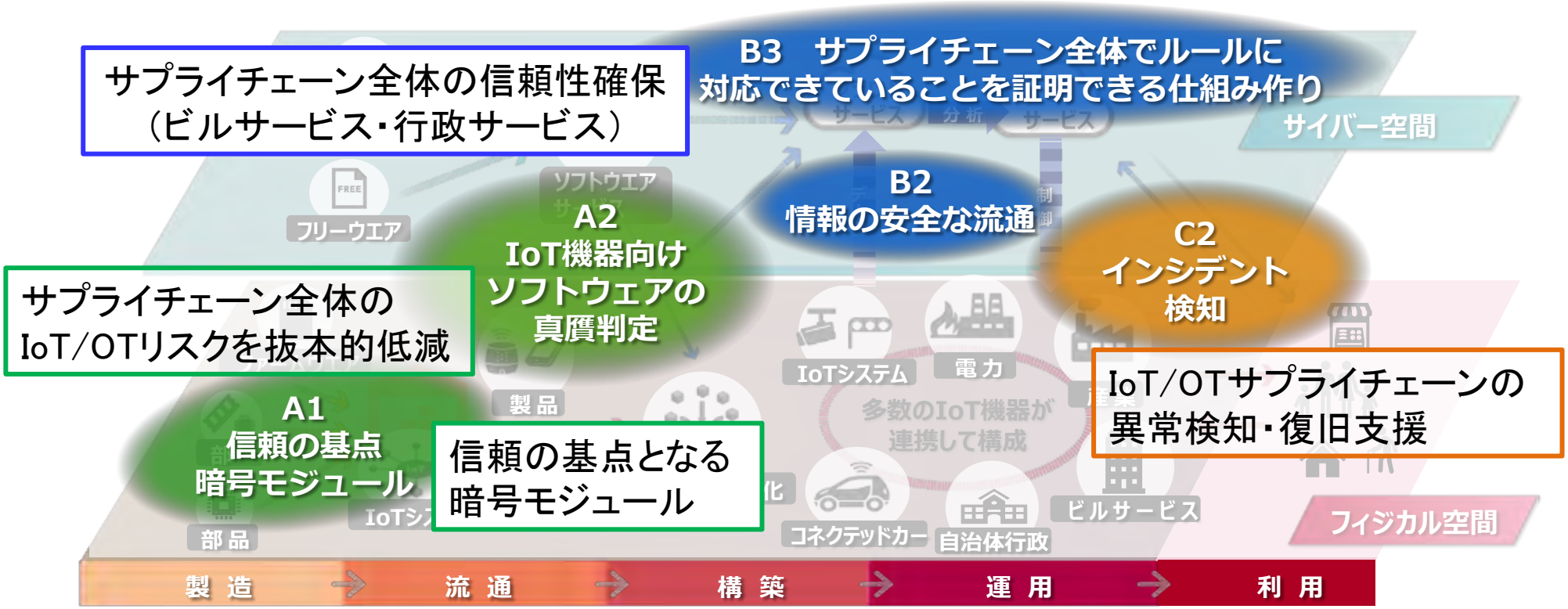
サイバー空間とフィジカル空間の双方に跨るIoT社会でのサプライチェーン



『サイバー・フィジカル・セキュリティ対策基盤』構築に向けた研究開発項目

IoT機器やサプライチェーンの各構成要素について，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**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**を確保

サイバー空間とフィジカル空間の双方に跨るIoT社会でのサプライチェーン



我が国の政策上の「IoT社会に対応したサイバー・フィジカル・セキュリティ」の位置づけ

IoTサプライチェーンセキュリティ確保は、サイバーセキュリティ戦略の重要事項の一つであり、内閣府SIPが府省庁（総務省、経産省等）を取りまとめて技術開発を進める。

サイバーセキュリティ戦略2021（戦略本部）

- 基本的な理念
  情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携、の5原則を堅持
- 「DXとサイバーセキュリティ同時推進」に向けた施策
  経営層の意識改革、地域・中小企業におけるDX with Cybersecurityの推進
  新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり
  誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

2020年度より：データ戦略（デジタル本部）

- データの信頼性（トラスト）を確保し、データ活用を促進できるプラットフォームを即急に実現（組織・人・機器のトラストアンカー、データ改ざん防止等）

経産省の施策

- “サイバーフィジカルセキュリティフレームワーク”の実現技術

総務省の施策

- “IoT・5Gセキュリティ総合対策2020”の推進技術
  （⇒“ICTサイバーセキュリティ総合対策2022”）

他　省庁

- 本SIPのWGには、NISC、デジタル庁、総務省、経産省に加え、警察庁、文部科学省、厚生労働省、防衛装備庁が参加

2 課題目標の達成度 課題全体について

① 国際競争力

- ✓ 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昨年度に引き続き確認された

② 研究成果で期待される波及効果

- ✓ 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

③ 達成度（1）5年間での目標に対する達成見込み （⇒p.13、pp.15～21）

- ✓ 全ての開発項目で目標を達成見込み（A1⇒p.43、A2⇒53、B2⇒p.63、B3⇒p.76、C2⇒p.89）

④ 達成度（2）社会実装の体制構築に向けた達成見込み （⇒ p.14 ）

- ✓ 事業化に向けた具体的な体制構築、計画策定を完了済み（A1⇒p.44、B2⇒p.65、B3⇒p.77）

③達成度（1）『サイバー・フィジカル・セキュリティ対策基盤』の研究開発成果

本SIP課題の研究開発課題（目標）	開発技術成果	
サプライチェーン全体でのセキュリティ対策と信頼性確保の「起点」 ⇒極小IoT機器に導入できる高性能・低消費電力の暗号機能	• 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 • 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	A1
製造から流通・運用・保守までIoT製品ライフサイクル全体での不正部品・不正機能の混入防止 ⇒サプライチェーン全体のIoT/OTリスクを抜本的低減と異常検知・復旧支援	• 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 • SBOM対応のソフトウェアサプライチェーン対策で先行	A2
	• 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 • AIを活用による幅広いFA/BAプロトコルに対応 • 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	C2
市民・民間・行政間サービスにおける多様なデータ流通の信頼確保 ⇒デジタル社会で安全な情報流通のためのトラスト機構	• 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 • 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	B2
グローバルサプライチェーン全体での企業責任の明確化 ⇒ SDGs, ESG, 企業不正対処、ルール形成対応の説明責任とトラスト	• 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 • 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	B3

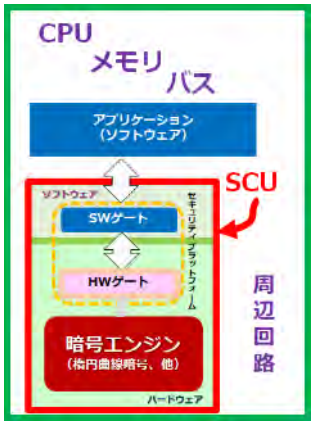
④達成度（2）
『サイバー・フィジカル・セキュリティ対策基盤』の社会実装と中小企業普及展開

	サブテーマ	施策
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	• 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）。 • 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	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	• Smart City 等関連サービスに向けて事業展開を推進。 • 複数のIoT機器ベンダー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）。 • 中小事業者も導入し易い支援サービス（MSS）としてサプライチェーンの異常検知機能の提供が可能に。リスク分析サービスは先行してサービス化済。 MSS：Managed Security Service
C2	信頼チェーンの維持技術の研究開発	
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	• 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。 • 横浜市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	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	• 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。 • ビル衛生管理サービスとして事業化済。 • 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

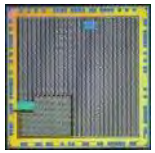
（A1）IoTサプライチェーンの信頼の創出技術基盤

IoTサプライチェーンの**信頼の基点**となる「軽く、速く、強い」セキュア暗号モジュールを開発

SIP1期の成果を継承
世界最小、世界最速の
楕円曲線暗号実装

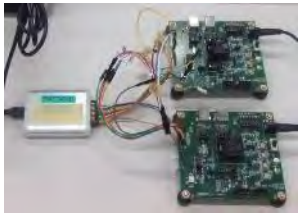


「軽く、速く、強い」セキュア暗号モジュール=SCUを搭載した半導体チップの試作開発



SC02チップ

SC02v.2チップ

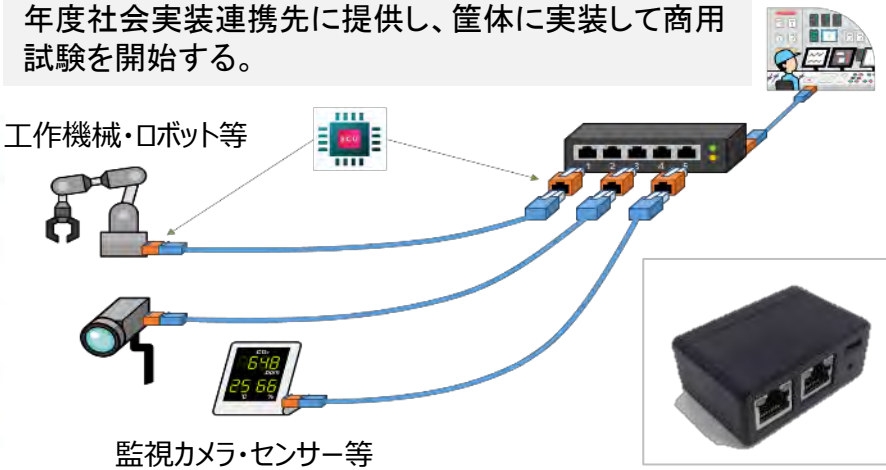


チップ評価完了

社会実装に向けて

レガシーシステムのIF部にアダプターを実装するだけで、システムのセキュリティを担保するコネクターシステムを開発

ネットワークケーブルの端末に**超小型のSCU機能を搭載**したチップを実装することで、システムのセキュリティを担保する**「セキュリティアダプター」**を開発。23年度社会実装連携先に提供し、筐体に実装して商用試験を開始する。



並列型セキュリティアダプターのイメージ

（A2）IoT機器等向け真贋判定による信頼の証明技術

トピック①：国際的な情勢変化へのタイムリーな対応

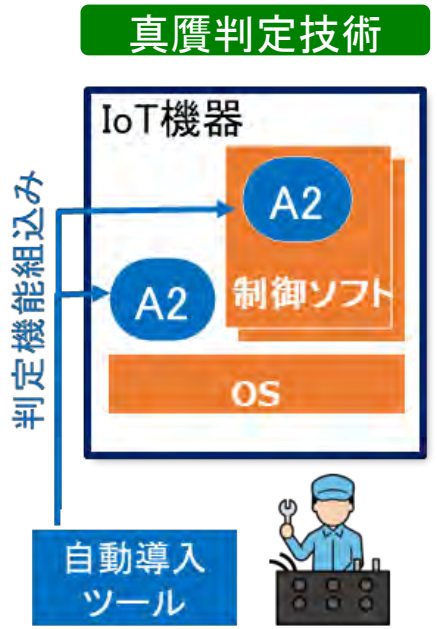
- サプライチェーンセキュリティに関する国際情勢の急速な変化に際し、研究当初より着目していた独自コンセプト（構成の証明）を活かして機動的に研究計画を強化
- 上記によりグローバル市場で需要が高まる「国際標準SBOM※」への対応を完了

※ SBOM: Software Bill of Materials（ソフトウェア部品表）

トピック②：複数の実証実験を相次いで前倒し開始

- IoT機器メーカ※の新製品開発に本技術を実適用するなどして、商用化の課題を効果的に抽出

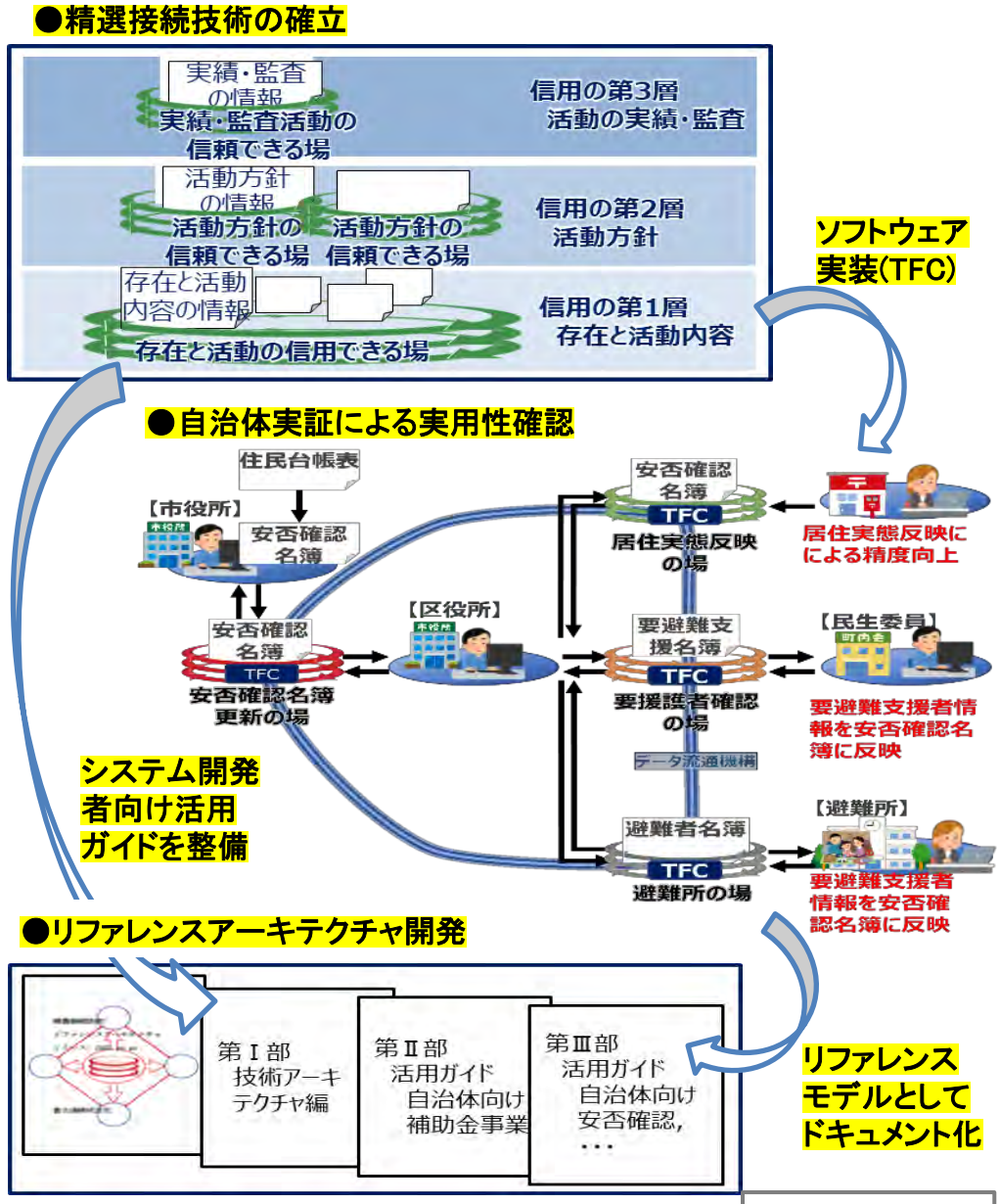
※ 連結従業員数約600名の国内中堅IoT機器ベンダ（主な商材：物理セキュリティ、無線、映像、音声デバイス等）



（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

■ 精選接続技術の確立、実証を通じた実用性の検証、および、成果普及に向けたツール（リファレンスアーキテクチャ)を開発し、当初目標を達成

- **精選接続技術**
  - ✓ 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する信用形成3層モデルを開発
  - ✓ セキュリティインシデントの脅威侵攻レベルを算定、1次対策を自律適用し、信用形成3層モデル全体の安全性を維持する分散セキュリティ技術を開発
- **技術の具現化**
  - ✓ 精選接続技術を仮想サーバシステム上のソフトウェアモジュールTFCとして具現化し、信用形成3層モデルの動作を実証
  - ✓ 動作実証されたシステムを自治体業務に適用し、自治体業務での有効性・実用性を評価
- **リファレンスアーキテクチャ**
  - ✓ 具現化実績をもとに自治体へのSIP成果普及を目指し、リファレンスモデルや活用ガイドを記載したリファレンスアーキテクチャ(ドキュメント)を開発



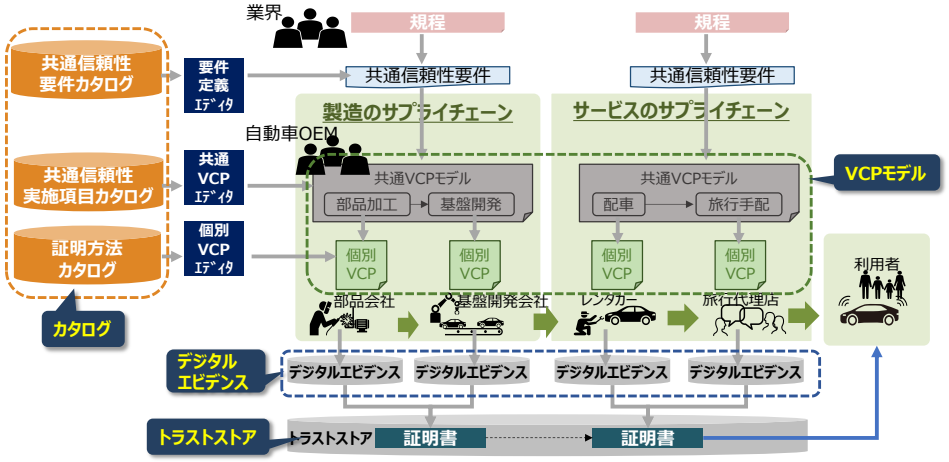
（B3）サプライチェーン全体の信頼性確保に向けた信頼データ交換・共有技術

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、容易かつ効率的に確認できる仕組みを実現し、以下の成果を獲得

(1)サプライチェーンの信頼性の構築技術確立と効率化
(2)標準化に向け日独米推進体制構築、提案前倒し
(3)SIP成果を活用したサービス提供開始

(1)技術開発

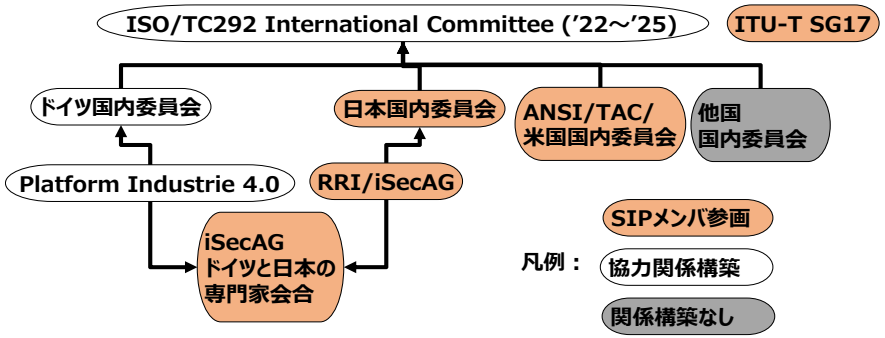
- 組織が規程に従っていることを確認する技術確立（VCPモデル、デジタルエビデンス、トラストストア）
- 適用方法を定義した**信頼構築フレームワーク策定**
- VCPモデル作成を効率化する**カタログを整備**、社会実装で課題となる**モデル構築コスト1/20達成**



技術開発全体概要

(2)標準化に向けた国際連携

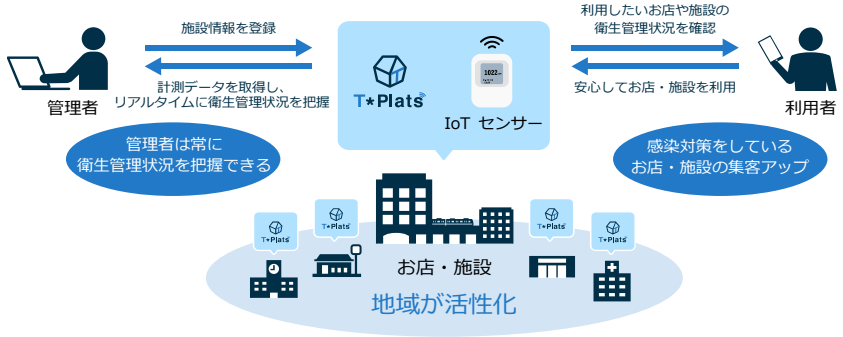
(1)の信頼構築フレームワークの標準化に向け、**RRI等を活用した日独米推進体制の構築に成功**し、日本単独提案と比べ、**ISO標準化提案1年前倒しを達成**



標準化に向けた国際連携体制

(3)SIP成果を活用した事業化

- 都心の大規模ビルのサプライチェーンで実証に成功
- 成果を活用し、2022年8月に㈱日立製作所、イーヒルズ㈱から**衛生管理可視化サービス「T*Plats」をサービスイン**

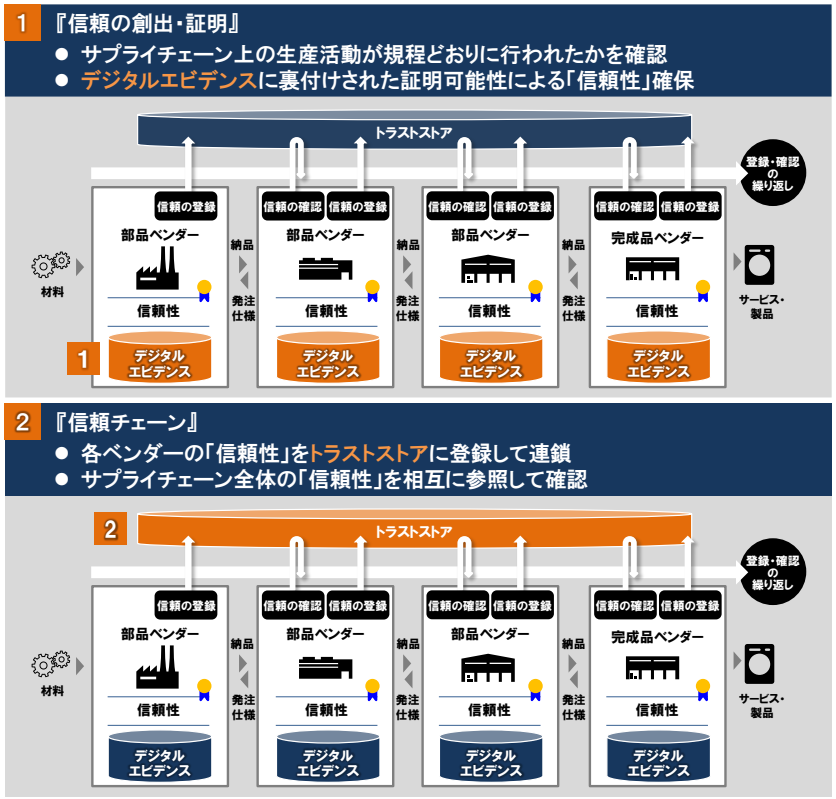


衛生管理可視化サービス概要

（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)技術開発トピックス

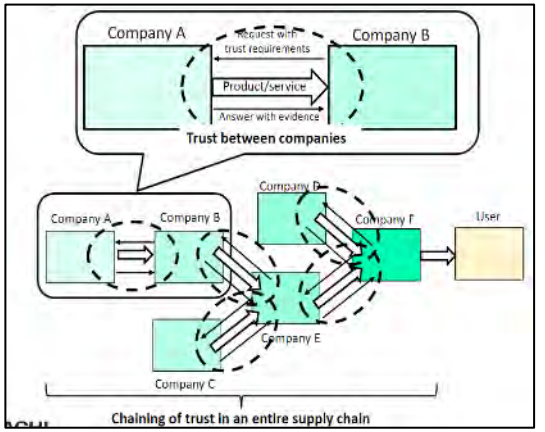
2020年暗号と情報セキュリティシンポジウム(SCIS2020)での「サプライチェーンセキュリティ」セッションにおいて、日立、KDDI総研、NEC、産総研で計5件の発表を実施し、開発技術の必要性・有用性をアピール。

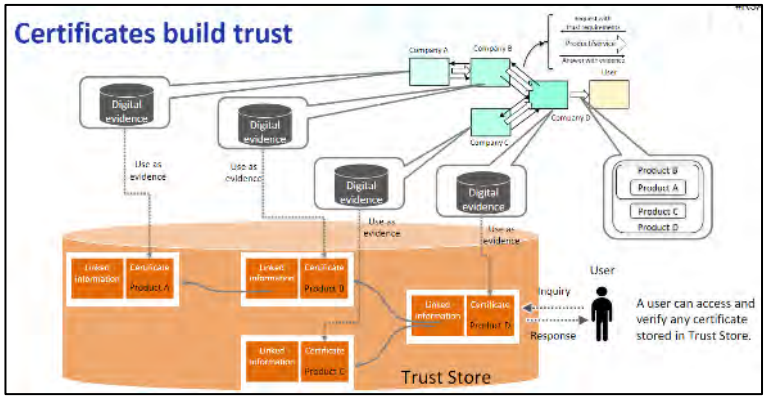


http://www.iwsec.org/scis/2020/program.html

(2)国際標準化トピックス

2021年RSA Conference(世界有数のセキュリティ専門家会議)において、サプライチェーントラストのコンセプトを発信。これをベースにISOで標準化活動を開始。



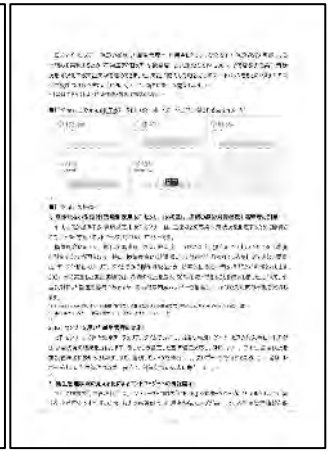


https://www.rsaconference.com/Library/presentation/USA/2021/building-trust-in-supply-chains

（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

（3）事業化のニュースリリース

ニュースリリースに対し大きな反響を獲得
（TV3社、新聞/ネット記事40件以上で報道）



サービス化発表のニュースリリース
https://www.hitachi.co.jp/New/cnews/month/2022/08/0803.pdf

NHK：おはよう日本：飲食店の感染リスク「見える化」安全な時間に来店を

フジテレビ：News Live α：飲食店などの感染対策見える化サービス　換気状況など

その他　対外発表リスト一覧

研究発表、講演；24件、プレス発表など：4件、特許：2件

年	月	学会名、イベント名など	タイトル	会社名
2019	3	情報処理学会・電子情報通信学会組込み技術とネットワークに関するワークショップ ETNET2019	周辺ネットの特徴量を考慮した二段階のニューラルネットワークによるハードウェアトロイ検出手法	早稲田大学
2019	6	日立セキュリティフォーラム	サプライチェーンセキュリティ ~超スマート社会における信頼を生み出す~	株式会社日立製作所
2019	7	The 16th International Conference on Mobile Web and Intelligent Information Systems	A Framework for Secure and Trustworthy Data Management in Supply Chain	KDDI総合研究所、 国際電気通信基礎技術研究所
2019	7	サイバーセキュリティ国際シンポジウム	今考える、超スマート社会を支えるこれからのサプライチェーンに必要なこと	株式会社日立製作所
2019	10	ATR オープンハウス2019	「Society 5.0」におけるサイバーセキュリティ ～全体像とATRの取り組み～ Cybersecurity for "Society 5.0" – Overview and ATR's activities –	国際電気通信基礎技術研究所
2019	10	ATR オープンハウス2019	サプライチェーンの信頼性を保証する先端セキュリティ技術	国際電気通信基礎技術研究所
2019	10	Hitachi Social Innovation Forum 2019 TOKYO	サプライチェーンの信頼性回復への挑戦 ～製品・サービス不正を防ぎ、信頼でつながる社会へ～	株式会社日立製作所
2019	11	International Workshop of Privacy Security Enhancement Forum 2019	Supply Chain Security for 5G and beyond 5G Era	KDDI総合研究所
2019	12	サイバーセキュリティ国際シンポジウム	サプライチェーン・サイバーセキュリティの社会実装に向けた課題ー官民の施策・課題ー	株式会社日立製作所
2020	1	SCIS2020	SIP委託・再委託者による合同セッション	株式会社日立製作所
2020	1	2020年 暗号と情報セキュリティシンポジウム（SCIS2020）	サプライチェーンの信頼構築に向けたデータの適合性に関する考察	国際電気通信基礎技術研究所、 KDDI総合研究所
2020	6	European Conference on Networks and Communications(EuCNC)	Consideratio on Data Conformance Toward Building Trust in Supply Chain	KDDI総合研究所、 国際電気通信基礎技術研究所
2020	7	日立セキュリティフォーラム 2020 ONLINE	「デジタルトラスト」が生み出す超スマート社会の信頼	株式会社日立製作所
2020	10	CEATEC	サプライチェーンのトラストが生み出す安心な超スマート社会	株式会社日立製作所
2020	10	サイバーセキュリティ国際シンポジウム	サプライチェーントラストに関する国際動向と日立の取り組み	株式会社日立製作所
2020	11	Hitachi Social Innovation Forum 2020 TOKYO ONLINE	サプライチェーンのトラストが生み出す安心な超スマート社会	株式会社日立製作所
2020	11	ATR オープンハウス2020	サプライチェーンの信頼性を保証する先端セキュリティ技術	国際電気通信基礎技術研究所
2021	2	報道発表	イチゴの出荷における温度データの検証に関わる実証実験の実施	KDDI総合研究所、 沖縄セルラー電話
2021	3	第2回 ATR-KDDI総合研究所セキュリティ技術セミナー	サプライチェーンの信頼確保技術	国際電気通信基礎技術研究所
2021	5	RSA Conference 2021	Building Trust in Supply Chains	株式会社日立製作所、 国立研究開発法人産業技術総合研究所
2021	6	日立セキュリティフォーラム 2021 ONLINE	トラストを構築してサプライチェーンをまもる、サプライチェーンにおける信頼の構築	株式会社日立製作所、 国立研究開発法人産業技術総合研究所
2021	6	18th IEEE/ACIS International Virtual Conference on Software Engineering, Management and Applications	Automatic Security Inspection Framework for Trustworthy Supply Chain	KDDI総合研究所、 国際電気通信基礎技術研究所
2021	6	ナノオプト・メディアオンライン セキュリティセミナー	サプライチェーンにおけるデータセキュリティ確保の取り組み – 証跡管理と検証技術 –	KDDI総合研究所
2021	7	報道発表	不正回路検出ツールの実行結果共有に関わる実証実験の実施	KDDI総合研究所、東芝情報システム
2021	10	Hitachi Social Innovation Forum	コロナ対策も安心、トラストが生み出す信頼の社会	株式会社日立製作所
2021	12	Keidanren SDGs	KDDIにおける安心安全なサプライチェーンの実現に向けた取り組み	KDDI総合研究所
2022	6	28th IEEE ICE & 31st IAMOT Conference IEEE	Security Inspection Framework and its Application to Use Cases	KDDI総合研究所
2022	8	ニュースリリース(日立製作所)	施設の衛生管理状況を見える化する「T★Plats」の提供を開始	株式会社日立製作所

出願人	出願国	出願番号	発明の名称	NEDOへの届出日
株式会社日立製作所	日本	特願2020-74817	デジタル署名の管理方法、デジタル署名の管理システム	2020/6/10
	米国 欧州 ドイツ イギリス	US17/191821 EP21160695A 21160695.9 21160695.9	DIGITAL SIGNATURE MANAGEMENT METHOD AND DIGITAL SIGNATURE MANAGEMENT SYSTEM	2021/4/9 2021/4/9 2022/11/11 2022/11/11
国立研究開発法人産業技術総合研究所	日本	特願2022-14066	検証装置、検証方法及び検証プログラム	2022/2/9

（C2）信頼チェーンの維持技術

トピック①：実証実験の拡大

- 2021年度に開始した実証実験3件（IoT機器ベンダ※、Smart City 事業者※×2件）に加えて、2022年度からさらに3件（製造系×2件、交通系）を開始して実施範囲を拡大
- IoTソリューション、IoTサービス等への展開に向けて事業化課題を広範囲から抽出

※ 連結従業員数約600名の国内中堅IoT機器ベンダの設備、最新スマートビル内設備など

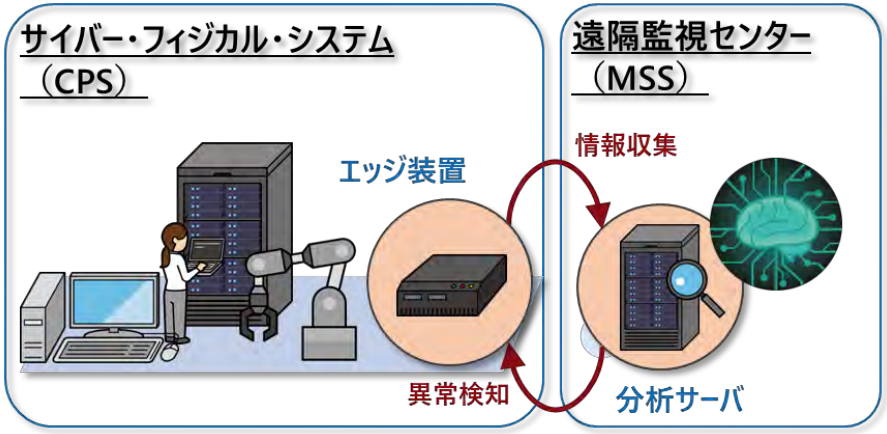
トピック②：サービス提供及び実用化実績に対する表彰の受賞

- 先行技術による「リスク診断サービス※1」を2021年に提供開始し、さらに機能を拡充
- この実用化が評価され、テレコム先端技術研究支援センターSCAT表彰※2を受賞

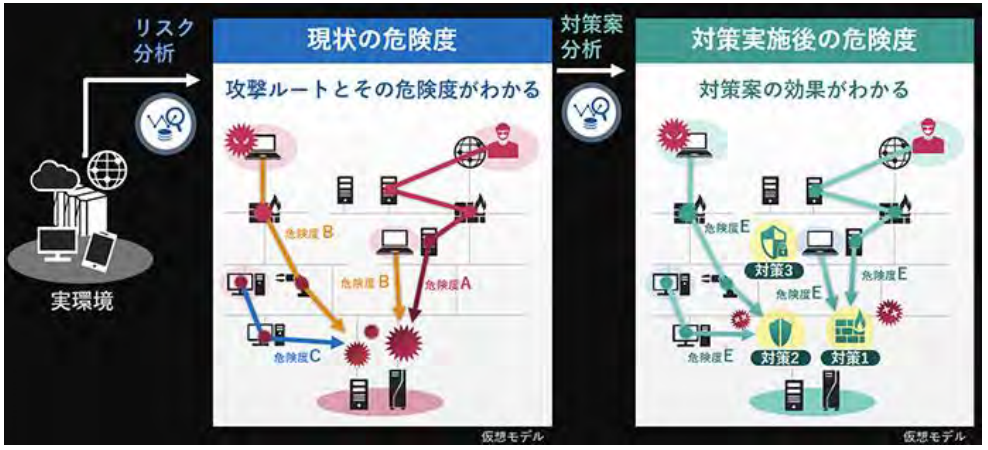
※1「NEC、システムのセキュリティリスクとその対策効果を可視化するサービスを提供開始」（ https://jpn.nec.com/press/202106/20210629_01.html ）

※2 https://www.scat.or.jp/awards/file/2022awards.pdf

検知技術の向上



リスク診断サービス



2 課題目標の達成度 課題全体について

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]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 成果の対外的発信

- ✓ 調査研究の結果をNEDOページに掲載し、広く共有。
- ✓ 5年間の成果を報告、宣伝するオンラインシンポジウムを実施予定（2023年2月）。
- ✓ 成果普及を促す、成果動画、ガイドブックを作成。シンポジウムで配布するほか、各県警（サイバー担当）、中小企業団体、厚生労働省領域、国土交通省領域の関係者に配布する。
- ✓ 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

- ✓ [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

3. 課題マネジメント

① Society5.0の実現を目指すもの

- 本課題は、IoTリスクおよびサプライチェーンリスク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、Society5.0の実現に必須のものである。

② 社会実装を実現するためのマネジメント体制（⇒p.25）

- 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、ユーザー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に、主査藤田戦略C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ー、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。

③ 研究テーマに対する評価、マネジメント（⇒p.26）

- PDは昨年度同様、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。
- 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。（⇒p.27）
- 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ている。

3. 課題マネジメント

④ 適切な民間の負担と官民の役割分担

- ✓ 社会課題解決のため国主導で実施しているが、産業界の研究開発実施者には、人的貢献や実証フィールドの主体的な提供や運用など、主体的な自己貢献を期待できる。

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、国費と同額以上に到達。

⑥ 府省連携が不可欠な分野横断的への取り組み（⇒p.34）

- ✓ 本SIPの取組は、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の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、総務省、経済産業省、NISC、デジタル庁、警察庁、防衛装備庁、厚生労働省等、府省連携が不可欠な分野横断的取組である。

⑦ SIP第 2期の他の課題との連携

- ✓ 「フィジカル空間デジタルデータ処理基盤」と連携し、実証を終えた。

社会実装を実現するためのマネジメント体制（2022年度）

PD　後藤 厚宏
サブPD　（今瀬 真、瓜生 和久）
戦略Ｃ　（藤田 恭弘）
内閣府　（事務局）
NEDO　（研究推進法人）

サイバー・フィジカル・セキュリティ推進委員会

ＮＩＳＣ、総務省、経産省、デジタル庁、他
学会、産業界の有識者

社会実装WG　成果普及・実証評価WG
海外動向調査WG

リーダー委員会　知財委員会

A1
極小暗号モジュール
ECSEC,産総研(横国大，神戸大，東大，東北大，NAIST，三菱電機)

A2
IoT機器の真贋判定
NTT
NEC
（FFRI）

C2
攻撃の検知・対処
NTT,NEC
日立，三菱
（阪大、金沢工大）

B2
情報の安全な流通
富士通
（NII,名大）

B3
信頼データ交換・共有
日立
KDDI総研
（産総研）

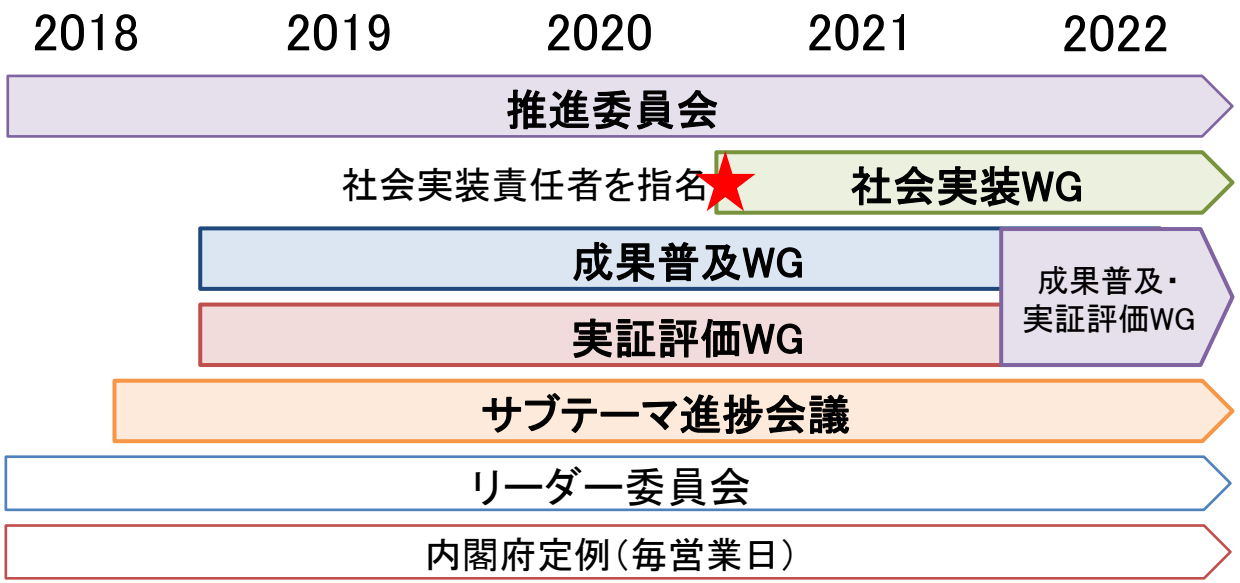
A.信頼の創出・証明

C.信頼チェーンの検証・維持

B.信頼チェーンの構築・流通

研究テーマに対する評価、マネジメント

- 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。
- 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ている。
- PDは、サブPD、イノベーション戦略C、内閣府担当者、NEDO担当者らとPDチームを構成、本課題の密なマネジメントを実施した。特にPDと内閣府担当者は、毎営業日に打ち合わせ、研究開発実施者への適時適切な介入に努めた。



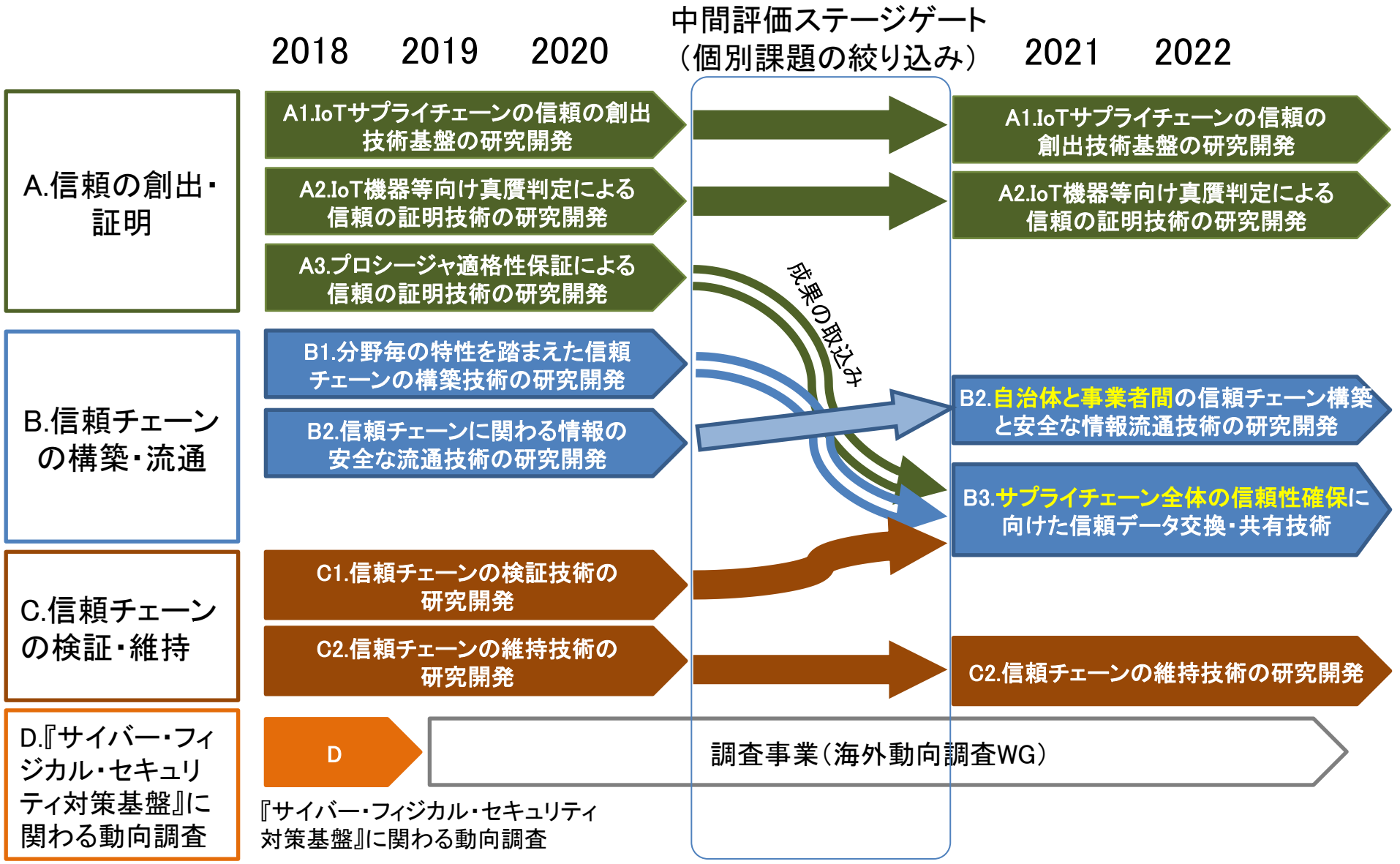
推進委員会、WG等参加者

▽ 推進委員会専門家
JPCERT/CC、IPA、NICT、大学教授等

▽ 府省庁
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、防衛装備庁

▽ 業界団体、産業界
SC3中小企業対策強化WG、（公社）神奈川産業振興センター、イーヒルズ（株）、（株）A-Digital

研究テーマの見直し（2018年度～2022年度）



外部動向の調査事業

国際的な情勢の変化を、現地の専門家により調査し、各国政府の法制度や技術標準、技術トレンドを把握。 リアルタイムに研究開発実施者と府省庁関係者に共有。

2019年度	IoT社会に対応したサイバーフィジカル・セキュリティに係る 標準化動向調査	情報通信総合研究所
2020年度	「IoT 社会に対応したサイバー・フィジカル・セキュリティ」に係る海外動向調査	サイバー創研
2021年度	IoT社会に対応したサイバー・フィジカル・セキュリティに係る海外動向調査	サイバー創研
2022年度	「IoT 社会に対応したサイバー・フィジカル・セキュリティ」に係る海外動向調査	サイバー創研

サプライチェーンおけるOSS活用状況や、その安全を担保する仕組みについて国内外調査を行い、その結果をPJ内で共有したほか、NEDOページにて広く公表。

2020年度	IoT社会に対応したサイバー・フィジカル・セキュリティに係るサプライチェーンにおけるOSSの活用状況調査	日本シノプシス合同会社
2020年度	IoT社会に対応したサイバー・フィジカル・セキュリティに係るOSSの技術検証、CSIRT・PSIRT連携等に関する調査	日本シノプシス合同会社
2021年度	IoT社会に対応したサイバー・フィジカル・セキュリティに係るOSSの技術検証のあり方等に関する調査	重要生活機器連携セキュリティ協議会
2022年度	「IoT社会に対応したサイバー・フィジカル・セキュリティ」に係るOSSの管理手法及びCSIRT・PSIRT連携等に関する調査	重要生活機器連携セキュリティ協議会

シンポジウム等の活用によるグローバル連携

海外のキーパーソンとコンタクトをとり、技術トレンドを研究開発に反映

	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、プロトタイプ展示 	● 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（サイバーセキュリティTop） ➢のうえノバ（株）　井上友二
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	コロナ禍により国際的なカンファレンス、出展等を取りやめ（イベント自体が中止）
2021	● ONLINEシンポジウム　2021年10月22日（金） ➢BitSight Mr.Stephen Boyer（ソフトウェアサプライチェーン） ➢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	オンラインで国際イベントに出展
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**	一部、技術成果を商用提供開始 技術研究組合が営利法人化

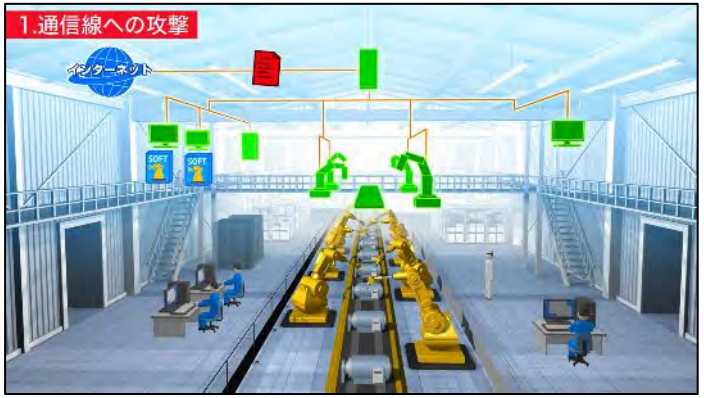
5年間の成果まとめ：シンポジウム2022

- SIP-CPSのシンポジウムは、2023年2月9日（木）開催
- 会場：御茶ノ水ソラシティ　sola city Hall（250名収容）
- 開催形態：展示会併設シンポジウム ＋オンライン配信
- 2/2現在、登録者　401名（現地+オンライン）

- 基調講演は、MITREのRobert Martin氏
  - MITRE’s System of Trust : Supply Chain Assessment Synergy Consistency and Evidence-Based

- 展示会場にサブテーマごとにブースを設け、研究実施者が、5年間の成果を報告する。
- 課題全体の共通ブースを構え（成果動画上映、ガイドブック配布）
- オンラインでの資料、動画の視聴も可能にする

ガイドブック（106頁）配布



成果動画（33分）上映

5年間の成果まとめ：ガイドブック

- ガイドブックの狙い
  - 経営層に、サイバーセキュリティ対策の必要性を気付いてもらう（4ページのエグゼクティブサマリ版も作成）
  - 対策を命じられた担当者が、自組織の状況に最適な対策イメージを作成できる
  - 各研究開発成果の社会実装（技術導入）につなげる（SIP期間終了後も利用可能）

ガイドブックの構成

はじめに
1. IoTやOTシステムの危険性
2. IoTやOTに関するサイバー・セキュリティ対策の現状
3. SIP技術を用いたサイバー・フィジカル・セキュリティの対策例
   - 3.1. 悪意ある人物による機器に対する直接攻撃への対策
   - 3.2. サプライチェーンフェーズでの悪意のあるソフトウェア混入への対策
   - 3.3. リモートメンテナンスの脆弱性への対策
   - 3.4. 自社で脆弱性を検討できないことによる放置リスクへの対策
   - 3.5. 不適正な組織・事業者の接続への対策
   - 3.6. サプライチェーン上で流通するデータ改ざんへの対策
4. 対策の企画・導入の進め方

付録：ソリューション説明
- ソリューション①：既存機器のIF部に外付け可能な 通信暗号化コネクタシステム
- ソリューション②：IoT機器向けの改ざん検知ソフトウェア(サービス)
- ソリューション③：IoT・OTシステムにおける セキュリティ異常対処支援サービス
- ソリューション④：信頼できる取引ネットワーク構築サービス
- ソリューション⑤：サプライチェーン・トラスト・ソリューション

5年間の成果まとめ：成果動画

- 成果動画の狙い
  - ホラーストーリーを軸に、わかりやすくIoTサプライチェーンのセキュリティリスクを伝える（トヨタ自動車と小島プレス工業に事例の利用をご承諾済）
  - 製造業（工場の生産ライン）への導入時の課題を考慮済
  - SIP期間終了後も成果の技術導入（社会実装）につなげる（SIP期間終了後も利用可能な権利処理済）

1．プロローグ
2．Chapter 1　サイバー攻撃の実例
　　（ソーラーウインズ、コロニアルパイプライン、国内事例）
3．Chapter 1　サプライチェーンの崩壊（ホラーストーリ）
4．Chapter 2　事業視点でのセキュリティ導入（インタビュー）
5．Chapter 3　サイバーフィジカルシステムへの攻撃方法
6．Chapter 4　SIPにより開発された安心、安全を実現する技術
　　A1：　セキュア暗号ユニット「SCU」
　　A2：　IoT機器等向け真贋判定による信頼の証明技術
　　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
　　B3：　サプライチェーンの信頼性を築くデジタルトラスト
　　C2①：　IoTの異常自動検知
　　C2②：　サイバー攻撃発生時の影響評価及び対処策実行支援
　　C2③：　不正なデータの検知・対処
7．最後に

（再掲）我が国の政策上の「IoT社会に対応したサイバー・フィジカル・セキュリティ」の位置づけ

IoTサプライチェーンセキュリティ確保は、サイバーセキュリティ戦略の重要事項の一つであり、内閣府SIPが府省庁（総務省、経産省等）を取りまとめて技術開発を進める。

サイバーセキュリティ戦略2021（戦略本部）

- 基本的な理念
  情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携、の5原則を堅持
- 「DXとサイバーセキュリティ同時推進」に向けた施策
  経営層の意識改革、地域・中小企業におけるDX with Cybersecurityの推進
  新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり
  誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

2020年度より：データ戦略（デジタル本部）

- データの信頼性（トラスト）を確保し、データ活用を促進できるプラットフォームを即急に実現（組織・人・機器のトラストアンカー、データ改ざん防止等）

経産省の施策

- “サイバーフィジカルセキュリティフレームワーク”の実現技術

総務省の施策

- “IoT・5Gセキュリティ総合対策2020”の推進技術
  （⇒“ICTサイバーセキュリティ総合対策2022”）

他　省庁

- 本SIPのWGには、NISC、デジタル庁、総務省、経産省に加え、警察庁、文部科学省、厚生労働省、防衛装備庁が参加

府省連携と課題連携

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。

◆ 府省連携

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

◆ 課題間連携

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。

府省庁へのSIP第2期終了後に向けた期待

経産省	◆産業サイバーセキュリティーの担当部署としてSIP CPS社会実装を推進 ◆IPA（セキュリティセンター），SC3（中小企業WG)を通した中小企業向けソリューション（A1，A2，C2）の展開支援 ◆CPSF を介したサプライチェーンソリューション（A1，A2，B2，B3，C2）の展開支援
厚労省	◆医療衛生分野に向けた通信暗号化コネクタシステム（A1）の展開支援
総務省	◆郵政行政部：　災害避難要支援者名簿作成に向けた郵便原簿の活用ガイドライン準備（B2　自治体向け安全な情報共有システム） ◆テレコム部門：　通信システムにおける通信暗号化コネクタシステム（A1）、真贋判定（A2）と異常検知（C2）の展開支援
内閣府 （SIP第3期）	◆SIP当初理念である「基礎研究から実用化」「テーマ 一丸となった取組み」に沿ったシンプルな評価体制 ◆上記理念に基づくPDへの権限と責任の集約、研究開発予算の制約の排除

まとめ :「IoT社会に対応したサイバー・フィジカル・セキュリティ」

Society 5.0 の安全・安心を確立するため，IoTシステムの製造・流通・運用から行政サービス・民間サービスのサプライチェーン全体を守ることができる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証を行い、2030年までの社会実装の目途をつけることができた。

◆ 取組みの狙いと概要

- SIPの開始時（2018年度）の「将来の想定リスク（懸念）」が、今日「現実の問題」として顕在化し、米国やEUにおいて対応策作りが急務になるなか、本SIPにて先行開発してきた成果は、必須ツールとして国内外で活用（社会実装）が期待できる。

◆ 課題目標の達成度

- 対策基盤のコア技術：高い国際競争力を内包するコア技術を開発完了した。その社会実装を促進するためのデモシステム・ガイドブック・広報ビデオをSIP終了後に向けて準備できた。
- 製造・ビル・自治体等での実証：SIPの外部企業・自治体の協力を得て研究成果の技術実証・価値実証を実施し、それを通して研究開発実施者の企業における事業化体制（社会実装推進体制）を整備できた。

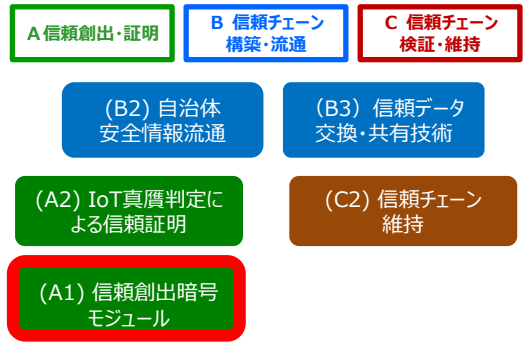
◆ 課題マネジメント

- 課題全体での連携体制と実施者による主体的な開発体制によりPJを推進できた。
- 官民での役割分担（マッチングファンド）は計画以上の実績であった。
- SIP終了後に向けて、政府施策としての長期的な取り組み関連府省庁と合意できた。

４　参考資料
各サブテーマ資料

(A1)　IoTサプライチェーンの信頼の創出技術基盤
(A2)　IoT機器等向け真贋判定による信頼の証明技術
(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
(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
(C2)　信頼チェーンの維持技術

（A1）IoTサプライチェーンの信頼の創出技術基盤 [㈱SCU（旧ECSEC組合），産総研 他]



（1） 研究開発概要

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。

例：SCU入り1チップマイクロコントローラ

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

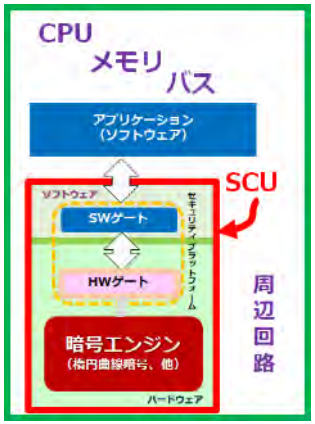
①SCU搭載チップSC01（4mm×6mm）、SC02（4mm×4mm～サイズを縮小、セキュリティを向上）、SC02ver.2（通信性能向上、データ様式に依拠しない署名検証）を開発する。

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。

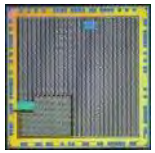
（3） 研究開発内容 （再掲）

IoTサプライチェーンの**信頼の基点**となる「軽く、速く、強い」セキュア暗号モジュールを開発

SIP1期の成果を継承
世界最小、世界最速の
楕円曲線暗号実装

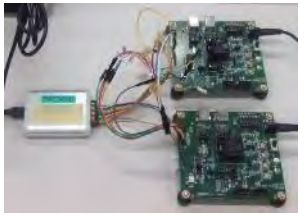


「軽く、速く、強い」セキュア暗号モジュール=SCUを搭載した半導体チップの試作開発



SC02チップ

SC02v.2チップ

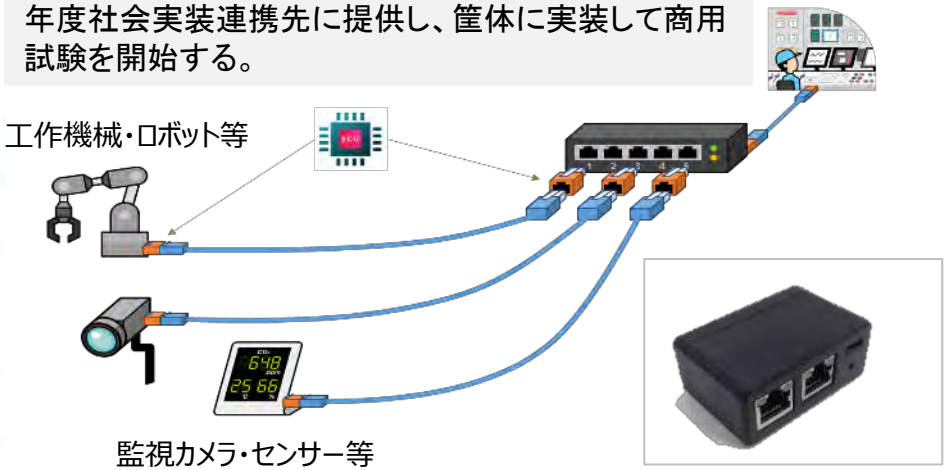


チップ評価完了

社会実装に向けて

レガシーシステムのIF部にアダプターを実装するだけで、システムのセキュリティを担保するコネクターシステムを開発

ネットワークケーブルの端末に**超小型のSCU機能を搭載**したチップを実装することで、システムのセキュリティを担保する**「セキュリティアダプター」**を開発。23年度社会実装連携先に提供し、筐体に実装して商用試験を開始する。



並列型セキュリティアダプターのイメージ

（4） 工程表

(A1) 信頼創出暗号モジュール

出口戦略・社会実装に向けて

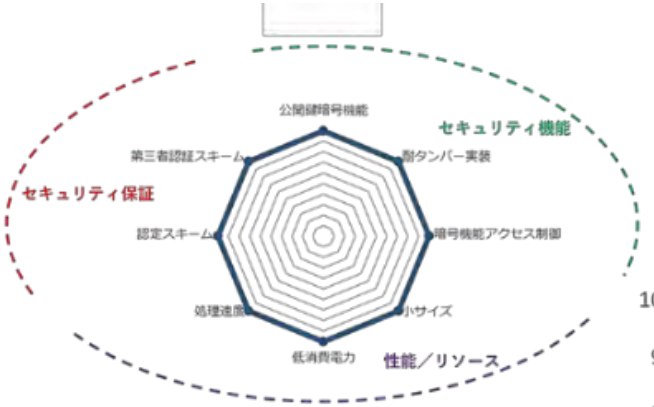
「IoT社会に対応したサイバー・フィジカル・セキュリティ」工程表

(A1) IoTサプライチェーンの信頼の創出技術

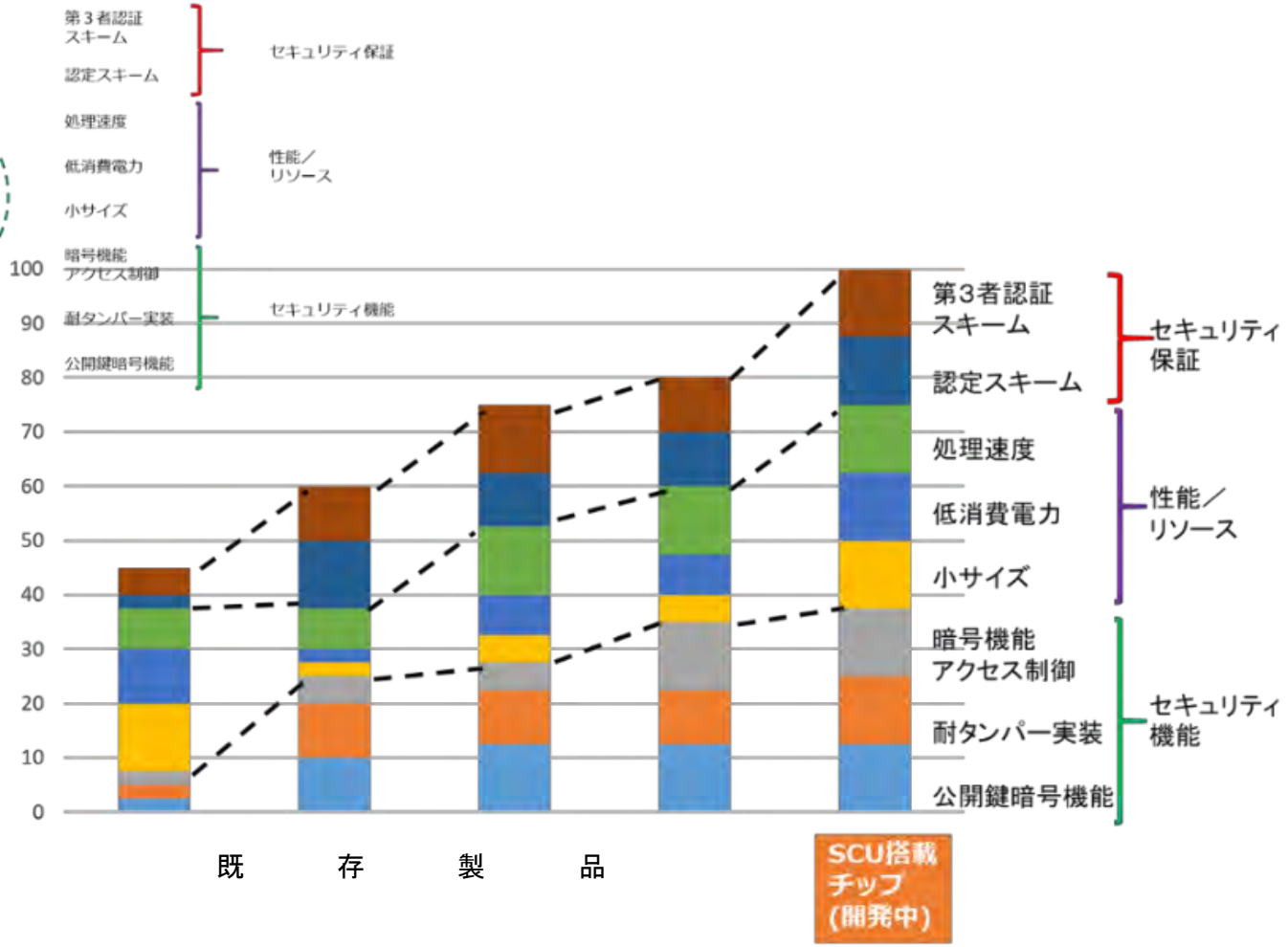
研究開発項目	2018年度実績	2019年度実績	2020年度実績	2021年度計画	2022年度計画	出口戦略	製品化
(A)「信頼の創出・証明」技術の研究開発							
(A1) IoTサプライチェーンの信頼の創出技術基盤の研究開発							
①IoT機器等に組込み可能な暗号モジュールをベースに、それを信頼の基点として活用するための基盤技術	• バランス型SCU(非ワンチップ)の一般組込み機器(監視カメラ)での実証実験 • ワンチップ化、鍵運用等検討 TRL2 → TRL4	• SCU搭載ワンチップ「α版」(SC01)完成 • コネクターシステム検討 TRL6	• SCU搭載ワンチップ「β版」(SC02)完成 • 工場・インフラ等向け「SCU搭載コネクターシステム」(鍵管理運用モデルを含む)の完成	• ECSEC組合組織変更 • 社会実装先開拓 • 事業資金調達 TRL7		● ECSEC組合の後継会社が、 ✓ 知財運用、 ✓ SCU搭載チップおよび活用システムの開発・販売、 ✓ 技術の標準化およびセキュリティ保証スキームの構築・運用 等、社会実装促進のための責務を担い、SCUを信頼の基点とする安全・安心なIoTシステム・サービスおよびサプライチェーンの確立を実現する。 ● SIP課題間連携	製品・サービス開発(2020～) 製品化・サービス化(2022～)
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の技術等	• 耐タンパー技術／ボードレベルHT検知技術／HT形式検証技術の技術実証 TRL2 → TRL4			• 実用化開発(比類なき耐タンパー性の実現) TRL5			
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	• セキュリティ保証スキーム先例調査 TRL2	• SCU搭載組込み製品用チップの脆弱性DB公開 • SCU搭載チップのセキュリティ要求仕様策定 TRL4	• TCGへの加入 • 「SCUコンソーシアム」組成 • 技術標準化 • SCU認定方式の提案 • SCU組込み製品のセキュリティ保証スキームの具体化 TRL6				
実証実験等 (A,B,Cの各テーマ毎、およびテーマを横断して実施)	• 一般組込み機器(監視カメラ)での実証実験			• 製造・流通・ビル分野等での実証実験 • 関連機関と一体での実証実験			
	・普及活動 ・提言活動 ・海外動向 との摺合わせ						
	• 府省庁による制度設計						

(5)グローバルベンチマーク 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。



IoT末端機器向けセキュリティチップの要件



次の項目は、プロジェクト終了後も継続。

【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

（6） ② 研究成果で期待される波及効果

(A1) 信頼創出暗号モジュール

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。

＜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。

（7）研究目標の達成状況・見込み　③ 達成度（1）

(A1) 信頼創出暗号モジュール

主な目標である、「SCU搭載チップSC01～SC02ver.2の開発」、「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）の実施」をはじめとして、技術的目標は全て達成した。

研究開発項目		研究開発目標	達成予定時期	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。

（8）出口戦略　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。

SCU搭載チップを普及させる企業グループを組織。
株式会社SCUが**ターンキービジネスの中核**となる。

IPビジネス
本研究開発の成果をIPとしてベンダー等に販売する事業

SoCビジネス
SCU搭載チップをグループで開発し、組込機器ベンダーに販売する事業

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
成果普及、社会実装を早めるために組込ベンダーとコネクターシステムを共同開発、これをユーザーに実装するためのサービス事業

（8）出口戦略　④ 達成度（2）

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。

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

（8）出口戦略

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）

(8)出口戦略

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.)

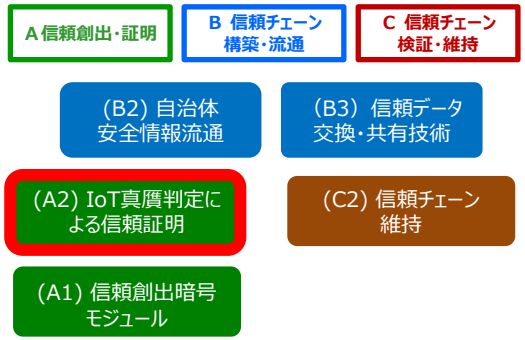
⑦ 国際的な取組・情報発信

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。

（A2）IoT機器等向け真贋判定による信頼の証明技術〔NTT, NEC　他〕



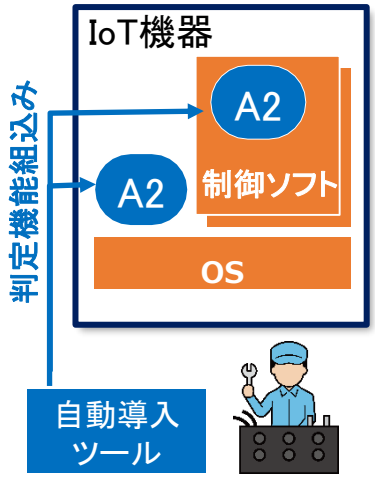
（1） 研究開発概要

Society 5.0 実現に向けて、従来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。

当初の上記懸念が現実化し、各国政府も対策に動き始める中、本テーマにおける先行的な研究開発が功を奏し、この動向にいち早く対応した技術を創出することができている。

具体的には、上記対策において米国政府等を中心に活用が進むSBOM(Software Bill of Materials)フォーマットに対応した、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、及び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ている。

機器内部に真贋判定技術を搭載



（2） 技術的目標

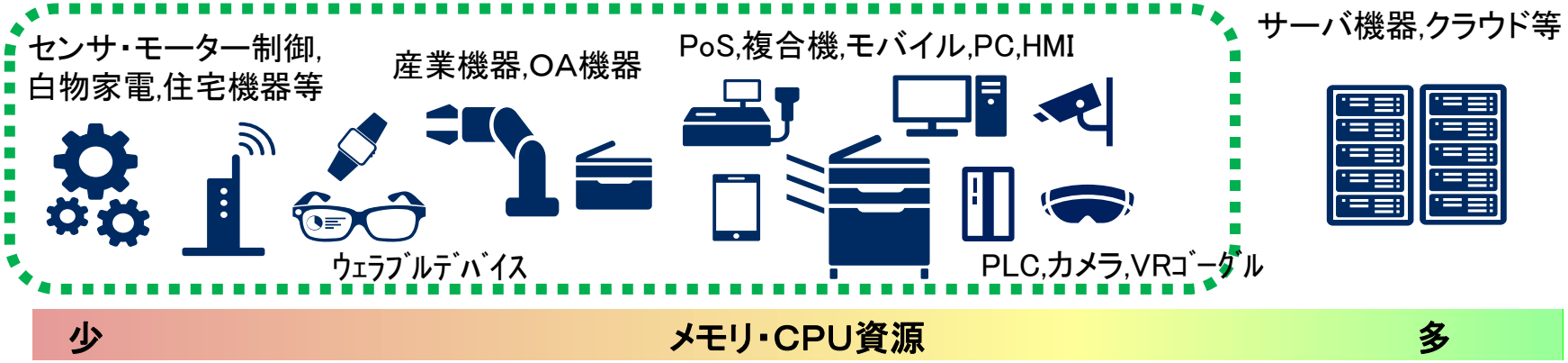
① 真贋判定技術は サプライチェーン上（多対多）での柔軟な開発活動を阻害することなく、高精度な構成保証が可能になるために、IoT機器の本来機能に影響を与えない軽量性（リソース使用率、判定効率）による常時監視を実現する。

② 稼働中の機器についても動作可能とするとともに、低機能機器（OSレス）への搭載、低い検査オーバヘッドを実現する。

（3） 研究開発内容

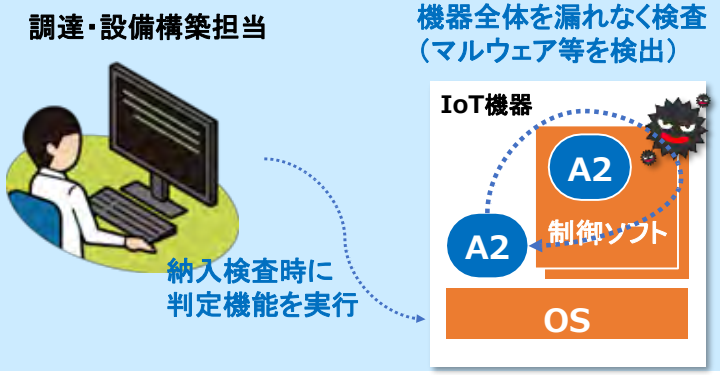
(A2) IoT真贋判定による信頼証明

ターゲットはメモリ・CPU資源の少ない「**中～低レベル機器**」であり、リソース制限等によって、従来は対策が困難であった多様なIoT機器の**構成を確認・証明**できる。

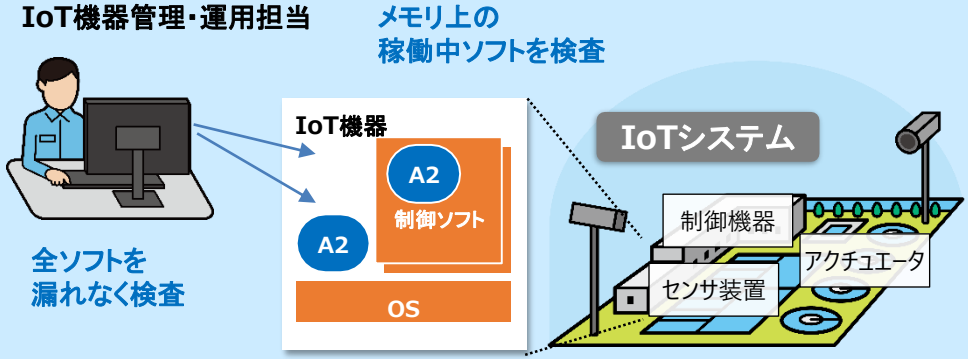


サプライチェーン上でIoT機器に不正な構成要素（マルウェア等）が混入する脅威、および運用中に遠隔制御や保守作業を介して汚染される脅威に対処できる

【効果①】
納入時に不正な構成要素を発見できる



【効果②】
本来動作に影響を与えず稼働中に判定できる



（4） 工程表

(A2) IoT真贋判定による信頼証明

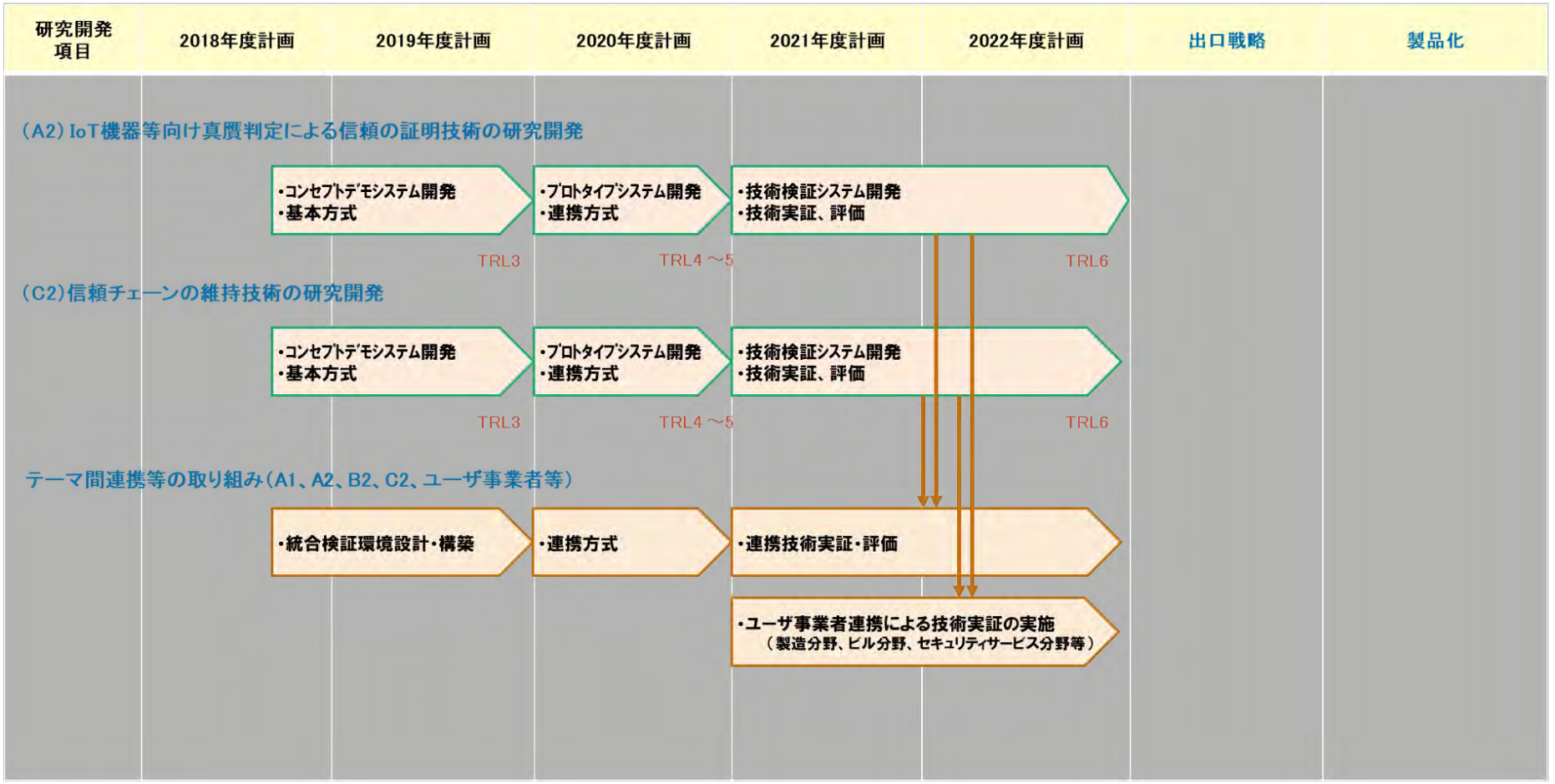
2021年度に開始した実証実験の延長をユーザ事業者と合意して拡充するとともに、新たな実証実験先にも拡大し、研究開発への技術課題フィードバックをさらに充実化させて当初目標の技術を確立するとともに、SIP終了時に当初計画していた「商用化の技術的見通しの獲得」を2022年度上期までに達成した。

出口戦略・社会実装に向けて

「IoT社会に対応したサイバー・フィジカル・セキュリティ」 工程表

(A2) IoT機器等向け真贋判定による信頼の証明技術

(C2) 信頼チェーンの異常検知・復旧支援技術



（5） グローバルベンチマーク ①国際競争力

(A2) IoT真贋判定による信頼証明

競争戦略の基軸である「判定性能・判定対象」の観点を中心に詳細な比較を実施
→「判定性能」の高さ、「判定対象」の広さにおいて明確な優位性を確認した

2022年度は、この優位性を保持したまま適用性をさらに向上させるとともに、他技術とも共通の弱点であるコスト改善について「技術導入の自動化及び支援機能」による導入障壁の低減を図った。

FY2021

FY2022

（6） ②研究成果で期待される波及効果

(A2) IoT真贋判定による信頼証明

・ 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本技術のライセンス販売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。

（7） 研究目標の達成状況・見込み ③達成度（1）

(A2) IoT真贋判定による信頼証明

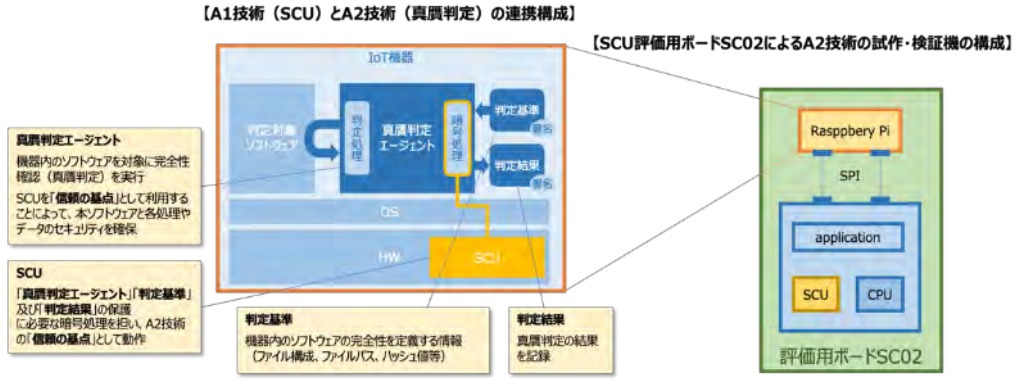
2022年度の目標

ア. 実証実験結果を研究開発にフィードバックして「技術検証システム(完成版)」の実装を完了する。

イ. 上記の取り組みを通じて、商用化の技術的見通しを獲得する。

進捗状況

- 当初の設定目標について、対象機器を拡大しつつ当初目標性能以上の優位性を確保。
- グローバルの情勢変化に先立って、リスク対応策として「機器構成に関する可視化の有効性」に着目していたことによって、タイムリーに研究計画を強化(2021年度)。その結果、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完成させて2022年度の実証実験に導入。
- 上記と並行して、実データを判定に用いる通常方式に加えて、属性情報（データ格納位置、サイズ等）を用いて判定する軽量方式を開発。CPU使用率及び監視間隔の当初目標を満たす判定効率を実証実験先の試作機でも確認完了。
- 稼働中機器のリアルタイム判定を行なう技術について当初計画の低レベル機器から中レベル機器へと適用範囲を拡大するとともに、当初目標の各性能値をいずれも達成。
- 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。2021年度中にSCUによる判定方式の机上検討を完了。
  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。



（7） 研究目標の達成状況・見込み ③達成度（1）【再掲】

(A2) IoT真贋判定による信頼証明

トピック①： 国際的な情勢変化へのタイムリーな対応

- サプライチェーンセキュリティに関する国際情勢の急速な変化に際し、研究当初より着目していた独自コンセプト（構成の証明）を活かして機動的に研究計画を強化
- 上記によりグローバル市場で需要が高まる「国際標準SBOM※」への対応を完了

※ SBOM: Software Bill of Materials（ソフトウェア部品表）

トピック②： 複数の実証実験を相次いで前倒し開始

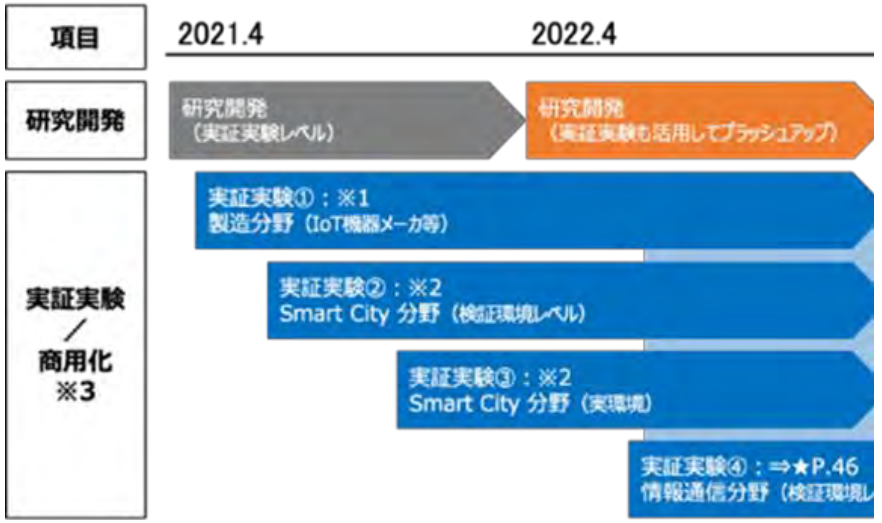
- IoT機器メーカ※の新製品開発に本技術を実適用し、商用化の課題を効果的に抽出

※ 連結従業員数約600名の国内中堅IoT機器ベンダ（主な商材：物理セキュリティ、無線、映像、音声デバイス等）

（8） 出口戦略 ④達成度（2）

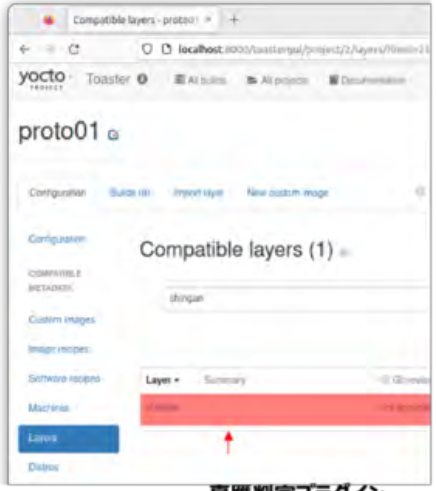
ウ. 実証実験の実施状況

- 2021年5月に1年前倒しで開始した実験①ではSTEP#3を実施中、実験③は本運用を開始
- 2022年6月にサプライチェーンやセキュリティ部門を含む全社的展開に着手（実験④を開始）



エ. 実証実験による課題フィードバック状況

■ ビルドツール画面



真贋判定プラグイン

■ 判定基準（SBOM形式）の構造

- 入退室管理向けIoT機器（新製品）を対象に実証実験を実施中
- ユーザの製品開発過程でOSがLinuxからAndroidに設計変更となったが、A2技術の対象OSを速やかに拡大して適用力を実証
- 世界的に重要性が増しているSBOM対応機能の実証も完了

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コア技術を中心に知財確保を実施中である。
  特許出願27件（フォアグラウンド知財6件、うち公開3件、バックグラウンド知財21件）
  - OT/IoT機器に対応可能な高効率な真贋判定判定方式
  - 軽量型真贋判定に関する判定基準リスト作成方式　など
- セキュアエレメント、IoT向けOS等の本技術の確立に不可欠となる既存要素技術は、原則、標準仕様を採用することによって本技術が広く普及しやすい状況を確保している。

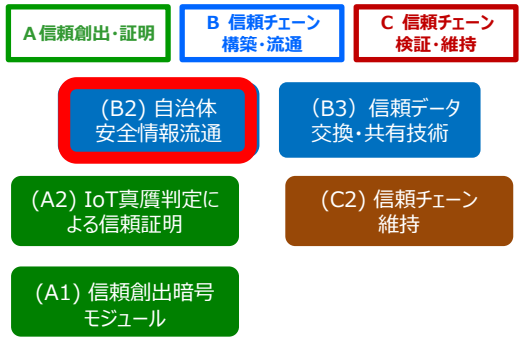
⑥成果の対外的発信

- 技術的内容については、研究発表・論文投稿等（国内9件）、展示会・シンポジウム等（13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。

（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〔富士通〕



（1） 研究開発概要

検証済み組織のみが参加する安全なデータ流通環境を柔軟・迅速に構築する。

これは「フィジカル空間(実世界)における相手組織の確認プロセス」と「サイバー空間で独立している接続相手検証プロセス」を統合し、フィジカル空間とサイバー空間の間で発生する検証プロセスの隙間を解消することにより、サイバー空間のみで組織検証から組織間ネットワーク接続までを可能とすることで達成される。

（2） 技術的目標

従来技術では達成できていない以下の技術的目標を達成する。

ア. フィジカル空間−サイバー空間の相手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)を開発する。

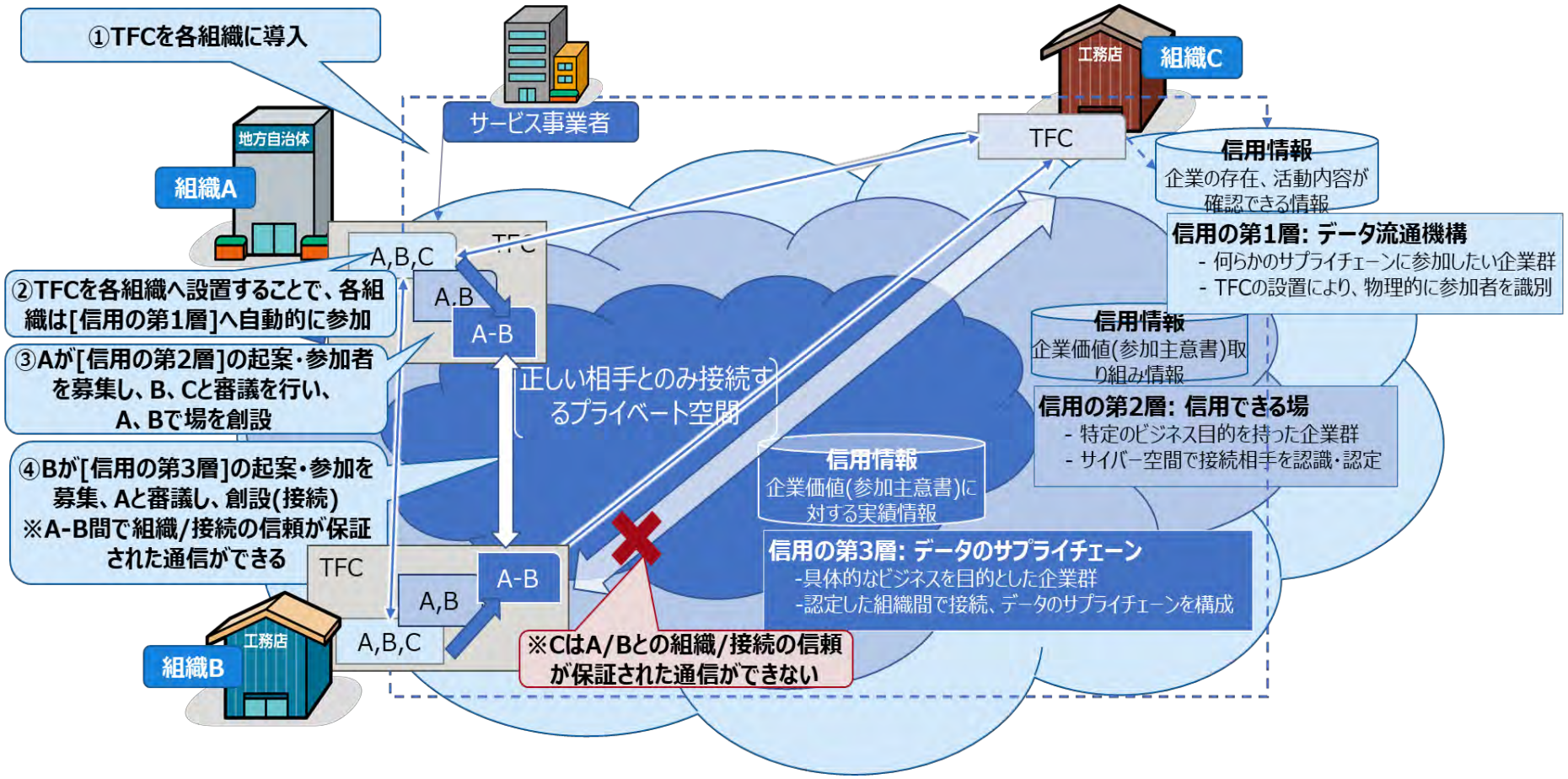
イ. 多数重層化するデータサプライチェーンの規模に対応するため、精選接続技術をソフトウェアゲートウェイ(TFC(*))として実装し、10,000TFC接続を可能とするスケーラビリティに対応するとともに、中小企業への導入ハードルを下げるための導入・運用効率化手法(セキュリティ対策の共通化および自律制御)も補助技術として確立する。

(*)TFC：Trustworthy Field Constructor　精選接続技術を実装したソフトウェアゲートウェイ

（3）研究開発詳細（TFCについて）

■ **データ・サプライチェーンの信用形成段階毎に情報流通範囲を統制する情報交換の「場」を構築し、検証済み組織のみが参加する安全なデータ流通環境を実現**

- 信用形成段階の**3層モデル**(事前審査、認定、取引・監査)　・信用情報流通における**共有範囲制限・改竄防止**
- 暗号メッセージ通信(ネットワークアドレス秘匿)による**情報漏洩防止**
- マルチステークホルダ間の合意形成による**信用情報の相互確認と完全性・真正性確保**



（4） 工程表

(B2) 自治体
安全情報流通

研究開発当初より以下のとおり研究開発ロードマップを策定し、2022年度の技術実証達成を目指した取り組みを実施。本ロードマップをテーマ間（A2、B2、C2）において共通化して取り組み、各テーマにおいて確立する技術の連携効果を創出することも重要方針として設定している。

出口戦略・社会実装に向けて

「IoT社会に対応したサイバー・フィジカル・セキュリティ」 工程表

(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

研究開発項目	2018年度計画	2019年度計画	2020年度計画	2021年度計画	2022年度計画	出口戦略	製品化
(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		・ｺﾝｾﾌﾟﾄﾃﾞﾓｼｽﾃﾑ開発 ・基本方式	・ﾌﾟﾛﾄﾀｲﾌﾟｼｽﾃﾑ開発 ・連携方式	・技術検証システム開発 ・技術実証、評価		・デジタル化による行政効率化・地域活性化に対するニーズ・意欲を持つ地方自治体を中心にデータ流通のインフラとして展開 ・実証実験の結果をもとにリファレンスアーキテクチャを整備し、自治体へのSIP成果普及を進めていく	・開発技術を搭載したTFCソフトウェアのライセンス販売事業、および、TFCソフトウェアを組み込んだ業務アプリケーションのシステム構築サービスを提供 ・2023年度は自治体での実証等で実績を積み上げ、2024年度以降の自治体への導入を目指す
		TRL3	TRL4 ～5		TRL6		
テーマ間連携等の取り組み（A2、B2、C2、ユーザ事業者等）		・統合検証環境設計・構築	・連携方式	・連携技術実証・評価			
				・ユーザ事業者連携による技術実証の実施 （自治体および自治体事業に関わる企業・団体を対象）			

（5） グローバルベンチマーク ①国際競争力

(B2) 自治体
安全情報流通

ネットワーク仮想化技術により、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の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への進化が始まっている。本ベンチマークは技術動向を踏まえ、本研究開発技術の主要技術を起点に、接続制御方式の異なる2つの技術と比較した。

SD-WAN技術:
管理者による集中型接続制御が可能な、主に企業内で用いられるネットワーク仮想化技術。

IDSコネクタ技術:
欧州International Data Spaces Association(IDSA)が提供するソフトウェアで、自己申告(Self-Description)にもとづき、各データへのアクセスを制御する技術。企業間のデータ交換に用いられる。

本技術の特長である「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、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目指す。

（6） ②研究成果で期待される波及効果

(B2) 自治体
安全情報流通

ア. 新技術・市場創出

デジタル化とともに、行政効率化・地域活性化を目指す自治体が複数あり、本技術適用により行政事業関連データが安全に連携可能となることで効率化・サービサビリティ向上が期待できる。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、 Society 5.0の進展にあわせて需要が拡大すると想定している。

イ. 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。

（7） 研究目標の達成状況・見込み ③達成度（1）

(B2) 自治体
安全情報流通

ア. 当初5年計画時の外部情勢と設定目標

データ活用の進展によってサプライチェーンは様々な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り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。

その解決策として、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。

- 信用情報によりサプライチェーン参加組織の信頼性を評価し、参加組織間で共有するとともに、組織間の公平な合意形成により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

イ. 現在の外部情勢と対応状況

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といった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。

このような状況を鑑み、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、実証実験の結果に基づいて商用化開発を推進している。

（7） 研究目標の達成状況・見込み ③達成度（1）

(B2) 自治体
安全情報流通

ウ. 5年計画に対する達成状況

■ 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」を開発し、ソフトウェアモジュール(TFC：Trustworthy Field Constructor)として実装が完了。自治体との実証実験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。
  - ✓ 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。※[1][2][3]
  - ✓ 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。
  - ✓ 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、セキュリティ脅威発生状況や予兆、利用者が行うべき対処をリコメンドとして通知する技術を開発し、セキュリティ専門家に依存しない安全性維持の実現見通しを得た。※[2][4][5]
- 大規模・複数業種の実運用システムに適用可能な10,000TFC接続のスケーラビリティを達成。

■ 統合検証環境を活用したテーマ間連携技術の実現

- C2システムが検知・予測した情報をB2システムにインプットすることでB2システムの検知・対処制度が向上し、B2システムを介して通信する端末や機器などによる業務継続性の向上を達成。

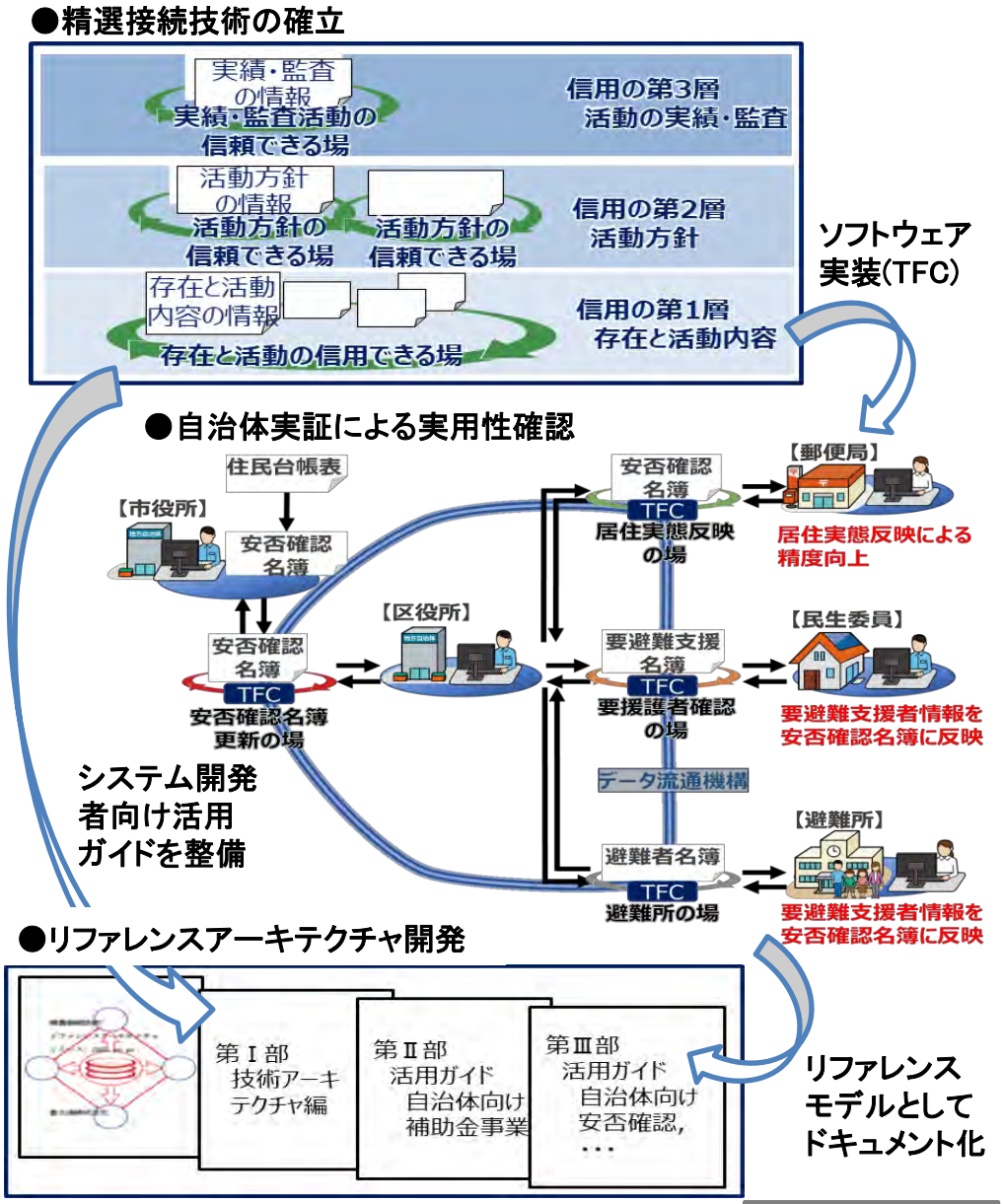
[1] 2022－109030、”ネットワーク構築プログラム及びネットワーク構築方法、並びに通信装置”
[2] デジタルサービス・プラットフォーム技術特別研究専門委員会 第7回DPF研究会、”SIP 信用でつなぐネットワーク”
[3] IEEE 8th World Forum on Internet of Things、”Trusted Network Connection Control by Sharing Attributed Information”
[4] ICISSP 2022、“Cyber Attack Stage Trace System Based on Attack Scenario Comparison”
[5] ICISS 2022、” A Resource Importance Estimation Method Based on Proximity of Hierarchical Position”

（7） 研究目標の達成状況・見込み ③達成度（1）【再掲】

(B2) 自治体
安全情報流通

■ 精選接続技術の確立、実証を通じた実用性の検証、および、成果普及に向けたツール（リファレンスアーキテクチャ）を開発し、当初目標を達成

- 精選接続技術
  - ✓ 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する信用形成3層モデルを開発
  - ✓ セキュリティインシデントの脅威侵攻レベルを算定、1次対策を自律適用し、信用形成3層モデル全体の安全性を維持する分散セキュリティ技術を開発
- 技術の具現化
  - ✓ 精選接続技術を仮想サーバシステム上のソフトウェアモジュールTFCとして具現化し、信用形成3層モデルの動作を実証
  - ✓ 動作実証されたシステムを自治体業務に適用し、自治体業務での有効性・実用性を評価
- リファレンスアーキテクチャ
  - ✓ 具現化実績をもとに自治体へのSIP成果普及を目指し、リファレンスモデルや活用ガイドを記載したリファレンスアーキテクチャ（ドキュメント）を開発



（8） 出口戦略 ④達成度（2）

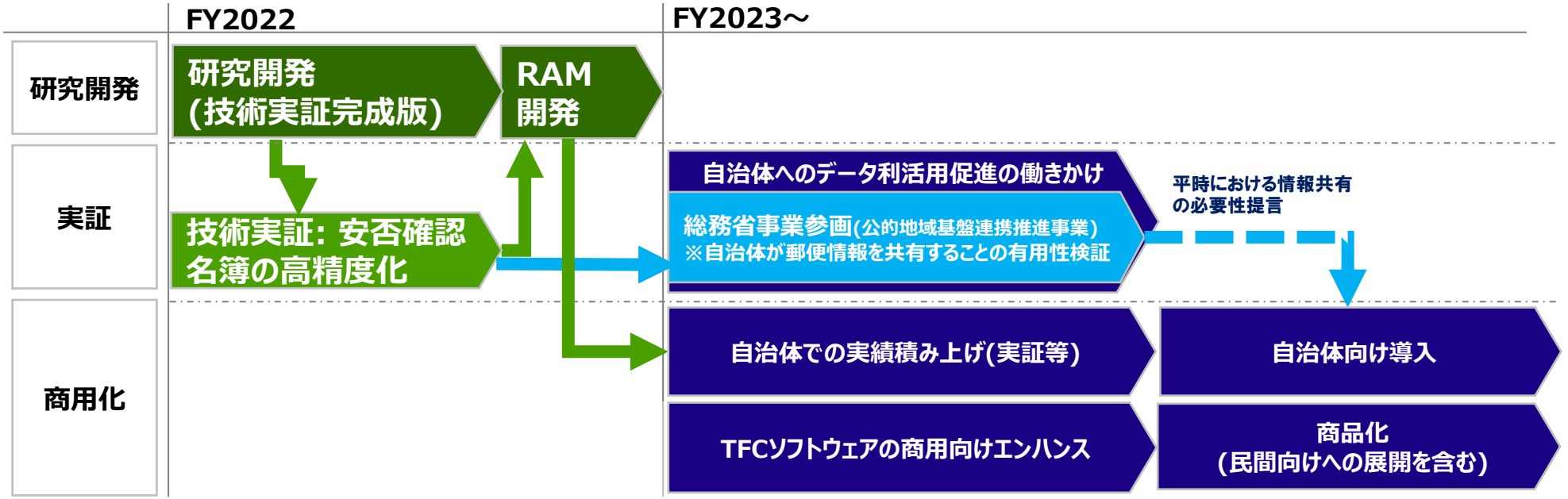
(B2) 自治体
安全情報流通

ア. 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等に取り組む自治体をターゲットに、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。開発したリファレンスアーキテクチャをもとに住民・事業者等が直接関わる業務への適用拡大による実績積み上げ、派遣人材を活用した更なるユースケースの拡大、社内関連サービスとの連携によるサービス提供範囲拡大に取り組む。

イ. 社会実装推進体制の構築と運営

自治体ビジネスを担うフィールド部門、および、社内外との連携強化を担う渉外部門との連携体制を確立済み。自治体での実績積み上げや実装促進の働きかけなどSIP成果普及に取り組む。

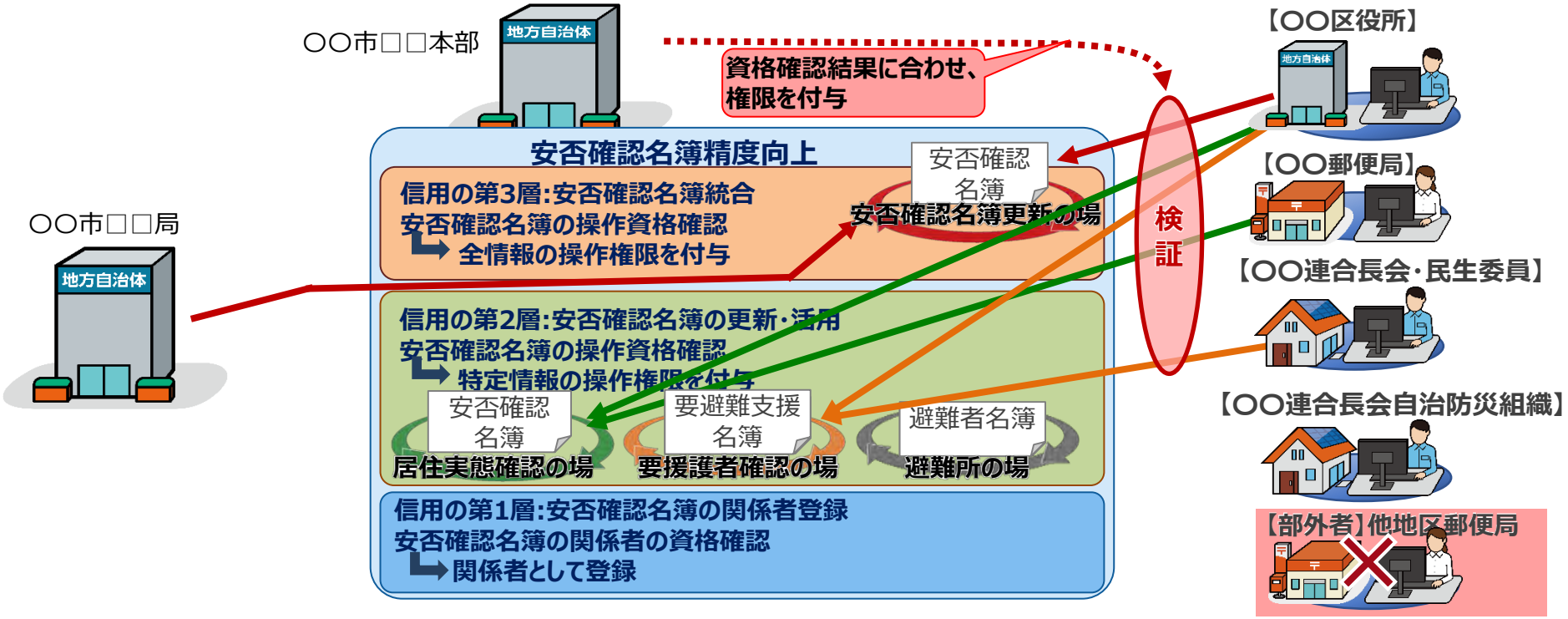


（8） 出口戦略 ④達成度（2）

ウ. 自治体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(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)を検証することで安否確認名簿の更新・活用に関わ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実証した。

また、従来技術では4つのシステム(安否確認名簿更新、居住実態確認、要援護者確認、避難所)で実現していた情報操作権限の制御を、同一システムの権限切り替えによって1システム、開発工数1/4で構築し、安全なデータ流通環境の迅速な構築が可能であることを実証した。



（8） 出口戦略 ④達成度（2）

エ. 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、自治体実証成果を活用して検証する。

本実証事業参画を前期課題(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。

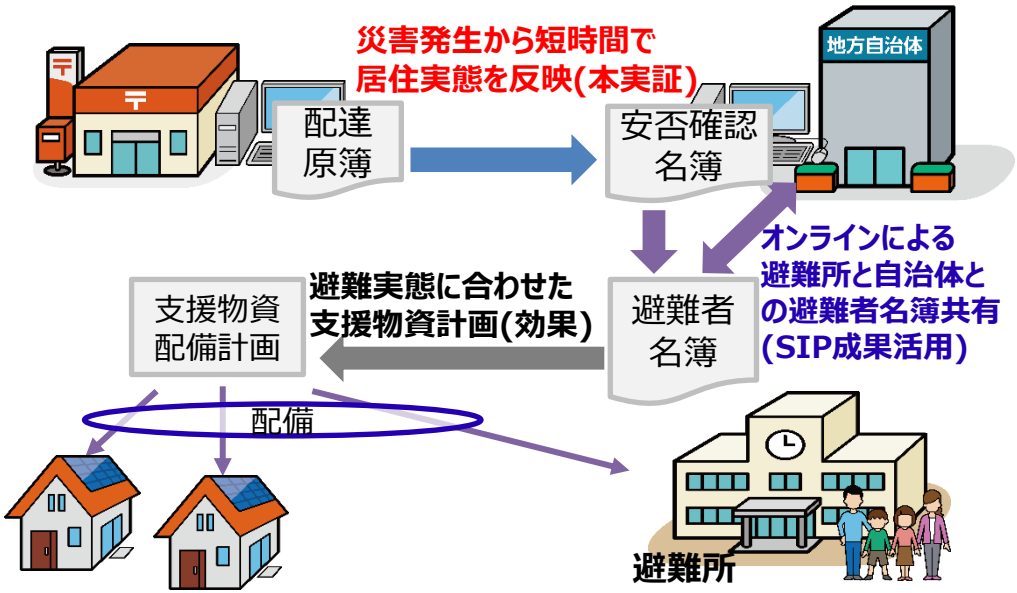
1. 本実証の目的

日本郵便が把握している居住実態を地方公共団体等に提供することで、より正確な安否確認名簿が作成でき、迅速な安否確認や救助等が可能となり、被災者の生命、身体又は財産の保護に質する。

日本郵便と地方公共団体等が連携し、災害時を想定した住民の安否確認名簿の居住実態に沿った精度向上に関わる課題解決に活用するモデルケースの創出を図る。

2. 具体的な実証内容等

日本郵便と地方公共団体が連携し、災害時を想定した住民の安否確認名簿の居住実態に沿った精度向上の実現性に関わる実証を行う。



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

本技術アーキテクチャ上で汎用的に活用可能なコア技術について特許出願済み(1件)。また、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保し、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、省庁や関係団体との連携により、本技術の普及にSIP終了後も継続して取り組む。

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

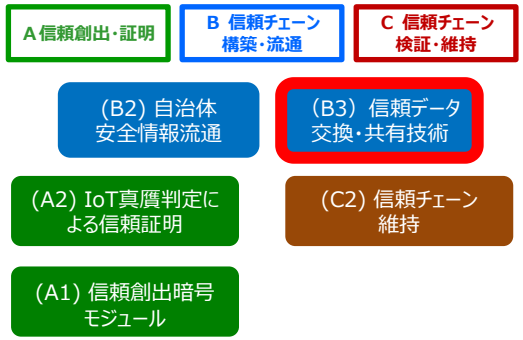
自治体への社会実装のため国内取り組みに注力している状況、海外動向 調査WGを通じた海外動向の把握、自社グループ内の海外関係会社との情報交換など、将来的なグローバル展開に向けた情報収集を行っており、SIP終了後も継続して取り組む。

（8） 出口戦略　出願特許の一覧

(B2) 自治体
安全情報流通

出願人	出願日	出願国	出願番号	発明の名称	NEDOへの届出日 (産業財産権出願通知書提出日)
富士通株式会社	2022/7/6	日本	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	2022/7/19

(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〔日立、KDDI総研〕



(1) 研究開発概要

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、技術的目標に掲げた4つの技術で実現する。

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。

※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]

(2) 技術的目標

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):事業者横断で活用可能な証明カタログの構築、要件カタログの構築、作成手順の構築を行う。

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):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する。

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):製品・サービス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を行う。さらに、サプライチェーンの下流から上流に向かって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(上記の技術を適用するための作法を定めたもの):国際社会での認知度向上を目的に、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する。

（3） 研究開発詳細

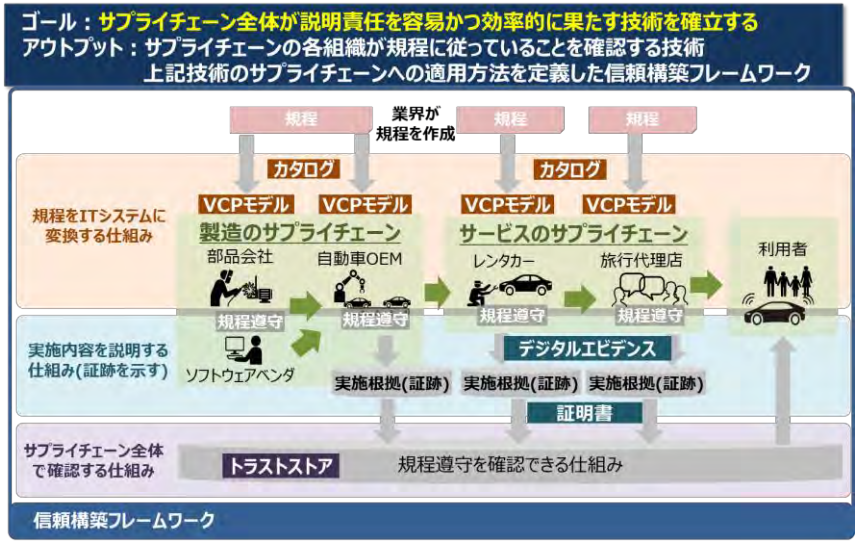


図 技術の全体像

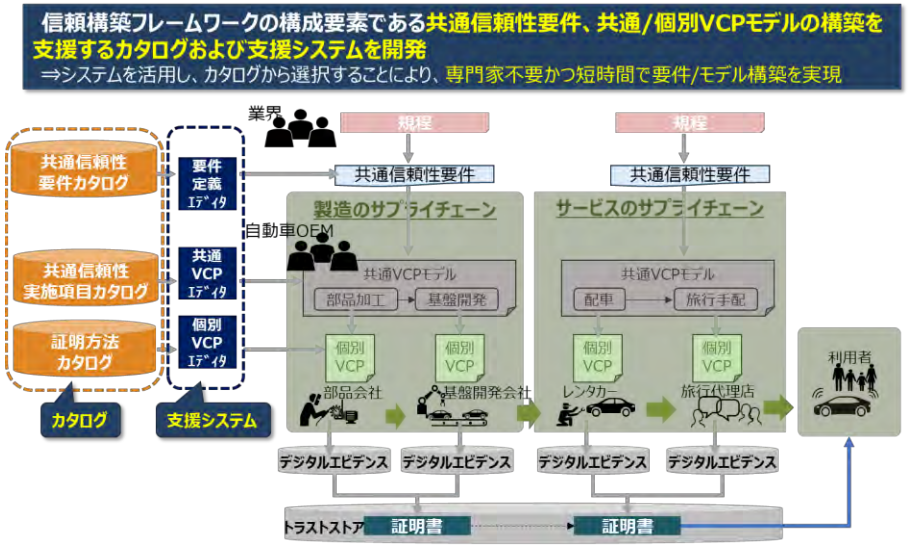


図 VCPモデル作成支援のためのカタログ類

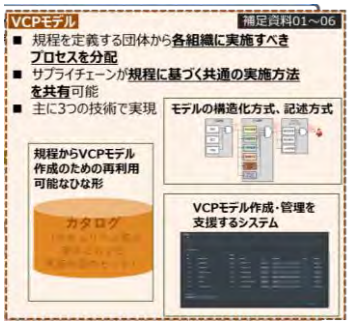


図 VCPモデル

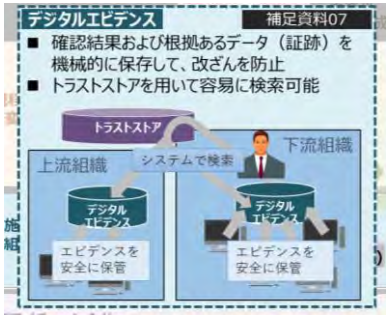


図 デジタルエビデンス

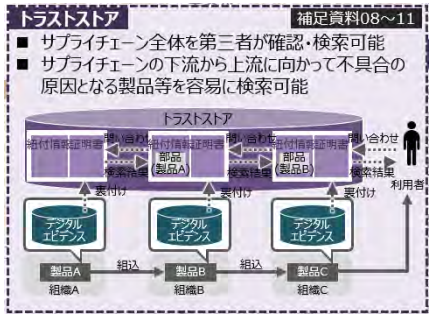


図 トラストストア

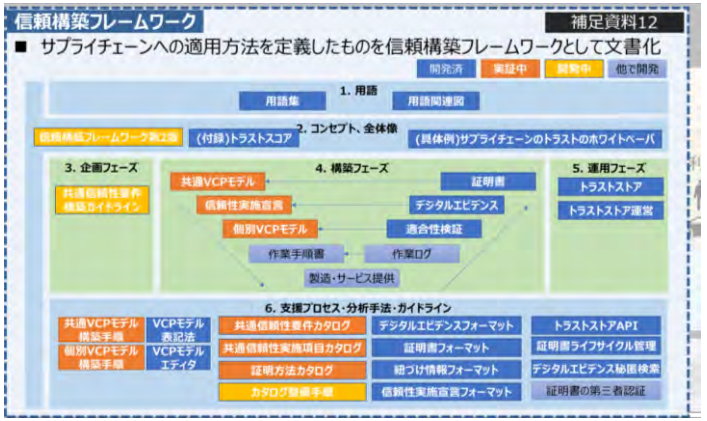


図 信頼構築フレームワーク

（4） 工程表

2022年度は、共通VCPモデル及び信頼構築フレームワークの研究開発を推進。開発した技術（共通VCPモデルやトラストストア)について、ビル分野（ファシリティ）で実証し、適応性を評価しフィードバックを獲得する。SIP成果をPI4等の関連団体へ提案、発信する。

出口戦略・社会実装に向けて

「IoT社会に対応したサイバー・フィジカル・セキュリティ」 工程表

（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

研究開発項目	2018年度計画	2019年度計画	2020年度計画	2021年度計画	2022年度計画	出口戦略	製品化
(A)「信頼の創出・証明」技術の研究開発	・要件定義 ・関連技術調査 ・プロファイル策定 TRL1～3	・基本設計(適合性検証他) ・VCPモデル検討 ・関連技術調査	・プロト開発 ・実証向けVCPモデル作成 ・実証環境構築 TRL5			技術、国際連携、国内の社会実装の3点で出口戦略を推進 【利用技術・運用技術】 ・実証を通じて利用技術、運用技術の課題抽出 ・ユーザ、有識者への提案とフィードバック 【国際連携】 研究成果の海外動向との整合性確保を目的に提案、発信 ・セキュリティの海外公的機関 ・Industryに関する国際団体 ・国際的なtrustworthinessの議論を進める関連団体 【国内の社会実装】 ・ビル分野 、公共分野への提案、事業性評価 ・他分野への適用拡大に向けた業界の巻き込みと適用性の評価 【その他】 ・SIP課題間連携 ・社会実装、普及に向けた提言	サービス開発 （ビル分野：2022年～ その他：2023年～） サービス化 （ビル分野：2022年～ その他：2024年～）
(B)「信頼チェーンの構築・流通」技術の研究開発	・要件定義 ・関連技術調査 ・プロファイル策定 TRL1～3	・信頼チェーンプロト開発 ・信頼チェーン構築と情報流通の要件定義と検証	・実証（企業間取引） ・課題のフィードバック ・関連技術調査 TRL5	・共通VCPモデル開発 ・関連団体への提案、発信 ・実証実験 TRL6	・実証実験 ・他分野への適応性評価 ・関連団体への提案・発信 TRL7		
(C)「信頼チェーンの検証・維持」技術の研究開発	・グランドデザイン ・関連技術調査 ・コンセプト発信 TRL1～3	・実証計画・環境構築 ・要件定義 ・対外発信	・実証(製造) ・実証(ビル分野) ・信頼性フレームワーク TRL5				
実証実験等	・実証実験に向けた体制検討／構築		・製造・流通・ビル分野等での実証実験	・ビル分野における技術実証、価値実証（対象：衛生管理）	・ビル分野における技術実証、価値実証（対象：ビルファシリティ）		
			・普及活動 ・提言活動		海外動向との摺合わせ		
			・府省庁による制度設計				

（5） グローバルベンチマーク ①国際競争力

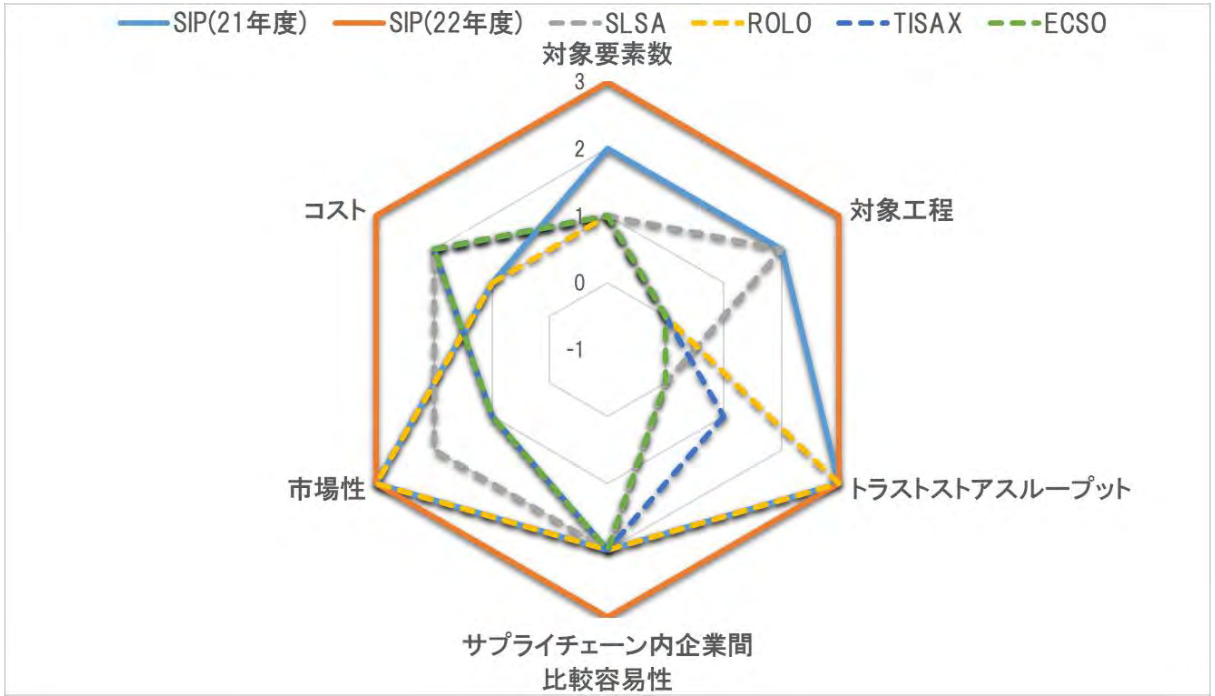
社会実装に必要な観点で評価、国際的な4つの技術動向(※)と比較してベンチマーク実施
・SIP(終了時)技術は、対象要素と対象工程の点で、多くの要素を広いライフサイクルでカバーしており、過去の不祥事へのカバー範囲がもっとも広い。
・共通VCPモデルにより他にはない比較容易性を実現する。

評価観点
(a)対象要素数　(d)企業間比較容易性
(b)対象工程　(e)市場性
(c)スループット（性能）　(f)コスト

対象フェーズの算出
・過去の不祥事事例を類型化
・検証可能事例数を元に、スコア化(30点満点)

過去の不祥事事例
（約100件）

	要素	類型	件数	重み
設計 製造	プロシージャ	不正	21	3
		不備	7	2
	データ	不正	2	1
		偽造	22	3
	ヒト	資格不備	7	2



※：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

（6） 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。

例：温暖化対策や安全安心などへの社会貢献

・欧米で進むサプライチェーンに係る法制度化への技術的な対応に貢献
　・DPP:サーキュラーエコノミーの法制度化に伴うバッテリーのカーボンフットプリント管理
　・SBOM：SolarWinds、ガスパイプライン等に起因したソフトウェアサプライチェーンの管理

DPP(※)（欧州）

悩み	エネルギー問題、環境問題が深刻化。 グリーンモビリティ、サスティナビリティの意識の高まり
現状の解決	Scope3のカーボンフットプリントをリアルタイムに、サプライチェーン規模で求める → バッテリーから適用
本成果の貢献	カーボンフットプリントを、**サイバーとフィジカル両面で信頼できる**データ収集・分析・管理を実現

※Digital Product Passport: EUが推進する、持続可能な製品の標準化に関するパッケージのひとつ。製造元、使用材料のほか、カーボンフットプリントも含む
※Scope3: 温室効果ガスのサプライチェーン排出量算定のひとつ、GHGプロトコルによると15カテゴリがあり、Scope1,2に比べて排出量が大きいと言われる

SBOM(※)（米国）

悩み	SolarWinds問題、Log4Shell問題に端を発する、ソフトウェアのサプライチェーンを信頼できるものにすること
現状の解決	SBOM(ソフトウェア部品表)をつかってのオープンソース活用時のトレーサビリティの確保
本成果の貢献	ソフトウェア開発時やリリース後の対応時の、ソシキ、ヒト、モノ、データ、システムに加えて**プロシージャまで含めた信頼性**の確保

※SBOM: ソフトウェアコンポーネントやそれらの依存関係の情報も含めた、機械処理可能なインベントリのこと。オープンソースソフトウェアだけでなくプロプライエタリソフトウェアに活用することも可能

（7） 研究目標の達成状況・見込み ③達成度（1）概要

・設定した全ての研究開発の目標を2022年度達成(見込み)。
・一部成果を事業化済みで目標のTR7以上を達成。以下特筆すべき達成度

研究項目１(技術開発): 信頼性確保に向けた信頼データ交換・共有技術の研究開発

・各種カタログ整備によるVCPモデル構築コストについて、実証フィールドに適用した条件において、当初目標の1/10に対して、1/20を達成

研究項目２(実証)　：信頼性フレームワークに基づくCPS対策基盤の実証

・日立・KDDI総合研究所で連携してビル関連サービス分野（衛生管理、ファシリティ）で実証を実施
衛生管理　：飲食店や公共施設等、目標以上の200施設以上が実証に参加し完了、前倒しで成果を事業化
ファシリティ：当初保守のプロシージャ、データを中心に実証予定に対し、ヒト（入退）、モノ(鍵)を追加して実証し、成果を今後の顧客の業務で使用継続していく見通しを得た

研究項目３(国際連携): 信頼性フレームワークの国際連携と普及啓発

・信頼構築フレームワークの国際標準化提案のため、日本が主体となりドイツと関係構築し、ISO/TC292(セキュリティとレジリエンス)国際提案の道筋(NP→AWI)を1年前倒しで確立
・セキュリティ分野で世界最大の会議RSA Conference 2021で講演、サプライチェーンのトラストの研究開発として世界に先駆けて情報発信
・証明書のX.509拡張による実装に向けて、2024年発行を目標にITU-T新規プロジェクト立上げ完(当初の目標に追加)

ISO提案のステップ：PWI→NP→AWI→WD→CD→DIS→FDIS→IS　AWI: Approved Work Item

（7） 研究目標の達成状況・見込み ③達成度（1）詳細

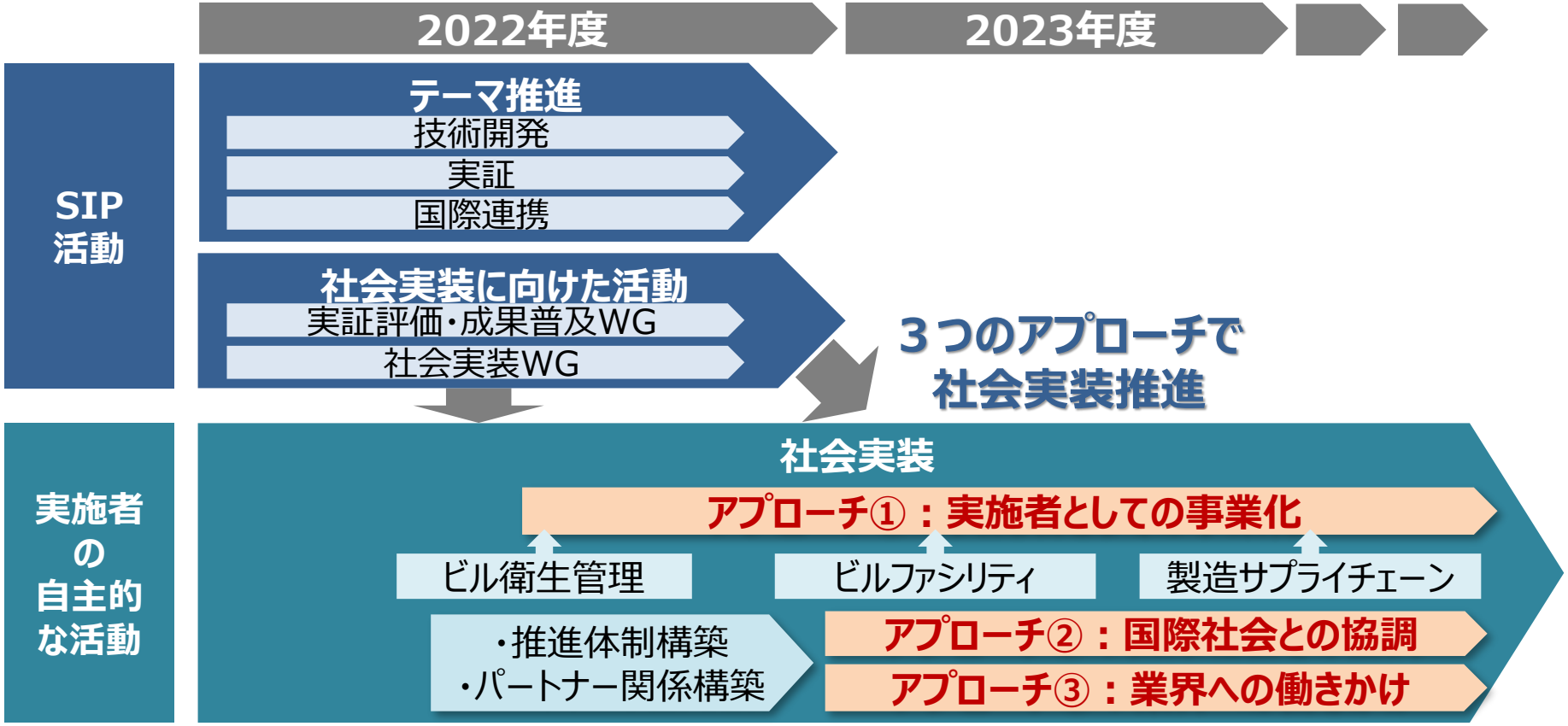
（B3）信頼データ交換・共有技術

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

（8） 出口戦略 ④達成度（2）

（A）社会実装に向けた計画

■ **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（2022年度完了）**
- **技術：**ヒト、モノ、データ、プロシージャが関与するサプライチェーンの信頼性構築技術の実用化
- **国際連携：**METIのCPSF標準化との連携、ISOにおける標準化、Industrie 4.0との関係構築
- **事業化：**SIP成果を活用した実施者としての事業化、事業推進体制構築



（8） 出口戦略 ④達成度（2）

（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、2023年度以降も社会実装を３つのアプローチで継続

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」サービスを提供開始
- 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

■ SIPで推進中のビルファシリティへの適用についても、事業化を検討中

アプローチ②：国際社会との協調

■ISO TC292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
- サプライチェーントラストのフレームワークに対してトラストストアやデジタルエビデンス等を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へ提案予定
- 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、11月提案済み

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発行済み
- 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
- 取り纏めた検討内容を各業界団体へ働きかけ実施済み（10月 CSAジャパン、11月 JEITA）

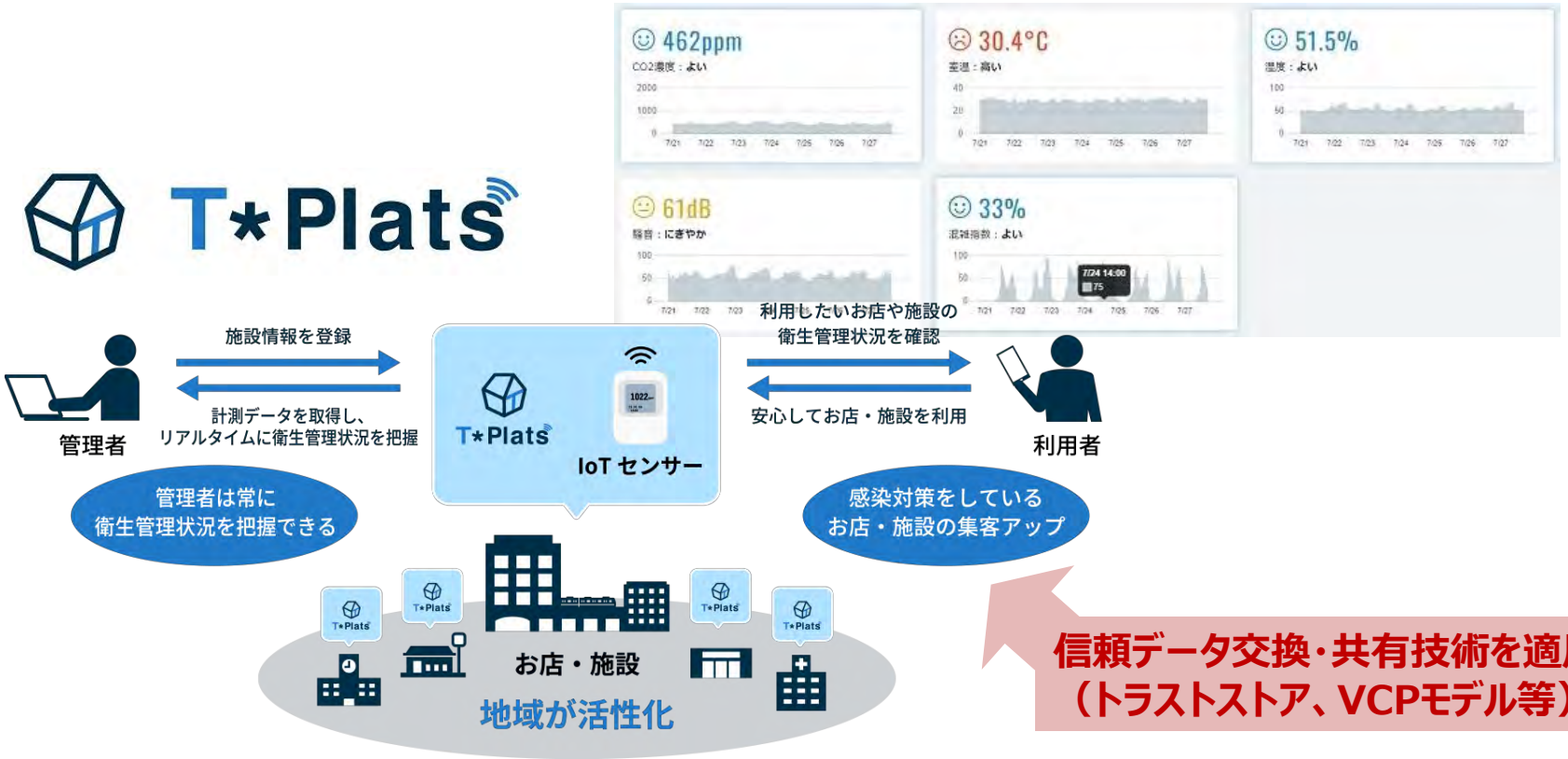
■ （一社）沖縄オープンラボ Trusted Network PJで、ワークショップ、価値検証を通じて業界へ働きかけ

（8） 出口戦略 ④達成度（2）

（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。TV3局、ラジオ1局、新聞5紙、ネット記事45件で報道
・約200箇所の施設が参加、飲食、教育機関、医療機関、公共施設、オフィス等で活用中

サプライチェーン全体が規程に従っていることを確認できるサービス



信頼データ交換・共有技術を適用（トラストストア、VCPモデル等）

（8） 出口戦略

⑥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

(ア)知財戦略

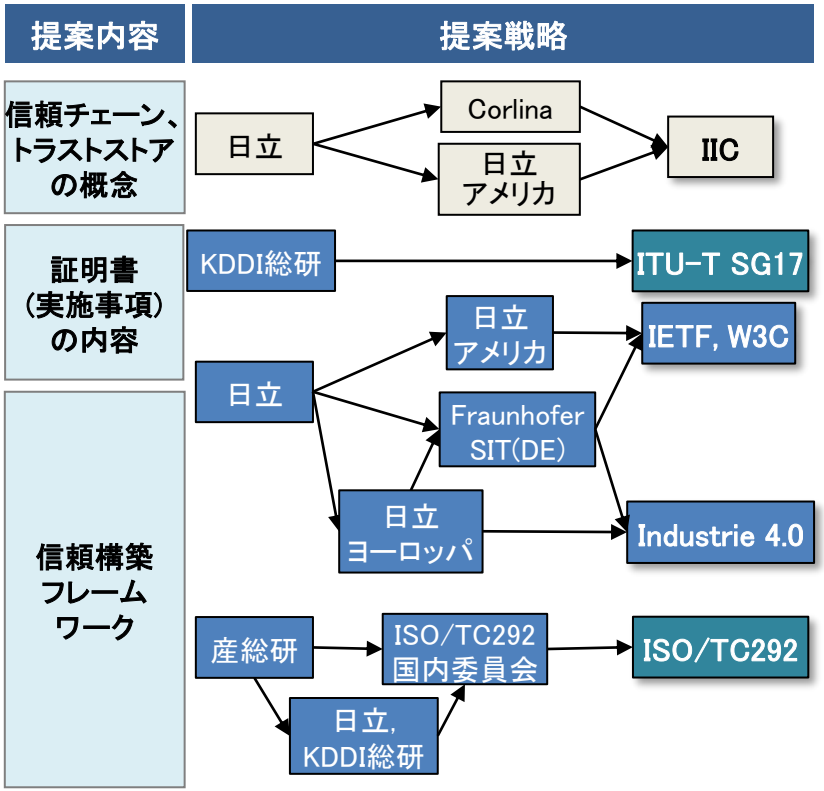
研究開発の中で得たノウハウについて、公開すべきところと非公開とすべき技術を明確にして競争力を確保する。

(イ)国際標準化戦略、出口戦略

国際団体へのインプットと、標準化団体での標準化を推進

・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



～21年度

IIC（インダストリーIoTのアメリカを中心とした国際団体）
Trustworthiness基本文書に、トラストストア等を盛込み済

22年度

IETF, W3C（国際的なWebやインターネット技術の規格団体）
信頼構築FWを使いやすくするための技術ユースケース策定提案

PI4.0（インダストリーIT化をめざしたドイツを中心とした国際団体）
提案ペーパを作成し、独キーマンからフィードバック獲得済、
23年度公開ホワイトペーパに内容を盛り込むよう議論開始

22年度（23年度以降も自主的取り組みとして継続）

ISO/TC292/WG4（セキュリティとレジリエンスに関する標準）
海外キーパーソンとの関係構築、日本/ドイツの委員と連携して
ISO AWI 22373として標準化の議論を立ち上げ

ITU-T SG17（情報通信技術に関するセキュリティ標準）
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
新規プロジェクトを立ち上げ

（8） 出口戦略

⑦成果の対外的発信

これまでに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。
・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は達成できた。
・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んだ。

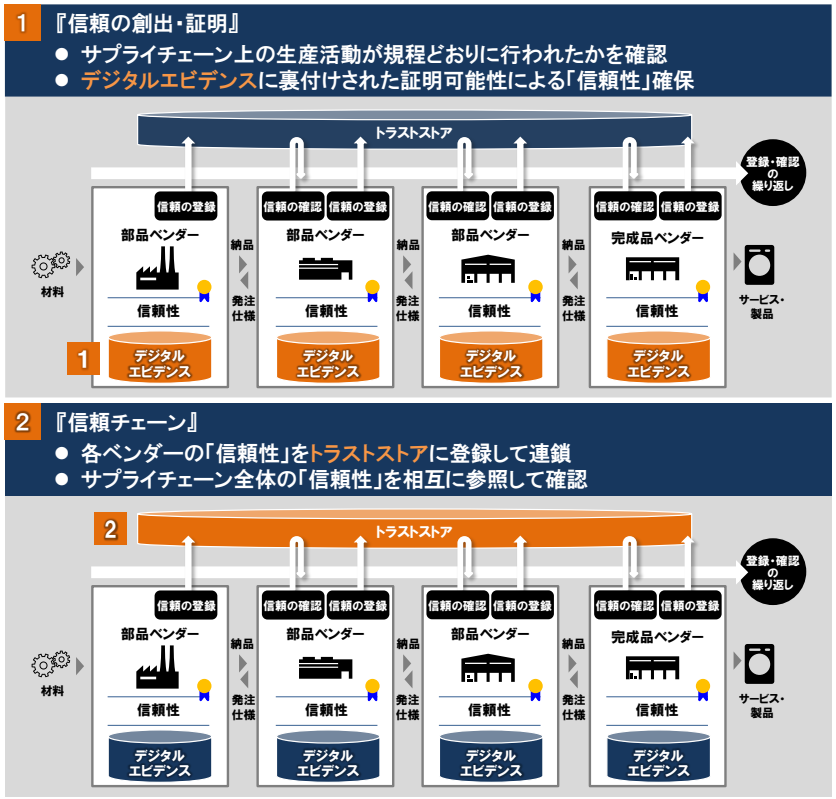
⑧国際的な取組・情報発信

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、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
・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
・デジタルトラスト協議会ホワイトペーパー公開
【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
・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

（8） 出口戦略 【再掲】

(1)技術開発トピックス

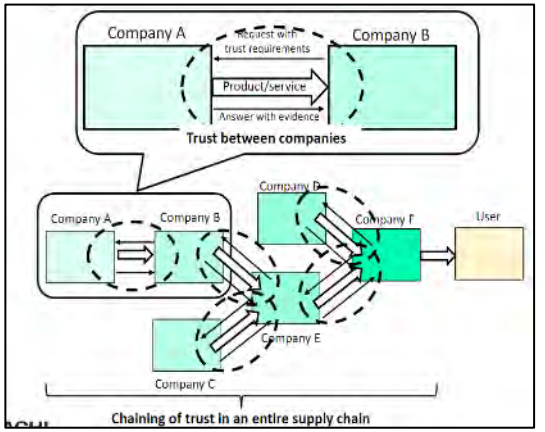
2020年暗号と情報セキュリティシンポジウム(SCIS2020)での「サプライチェーンセキュリティ」セッションにおいて、日立、KDDI総研、NEC、産総研で計5件の発表を実施し、開発技術の必要性・有用性をアピール。

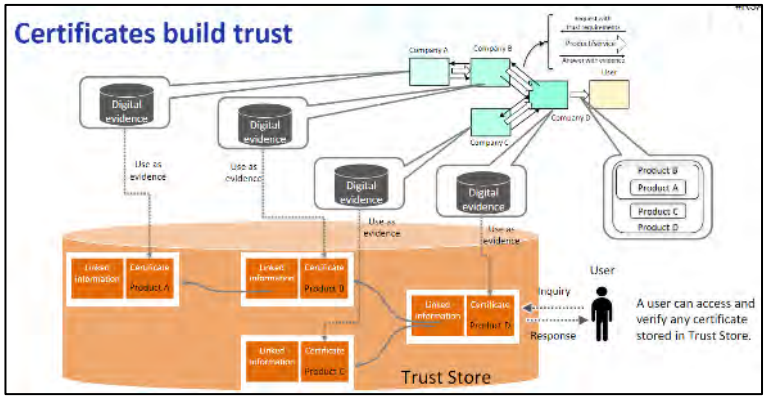


http://www.iwsec.org/scis/2020/program.html

(2)国際標準化トピックス

2021年RSA Conference(世界有数のセキュリティ専門家会議)において、サプライチェーントラストのコンセプトを発信。これをベースにISOで標準化活動を開始。





https://www.rsaconference.com/Library/presentation/USA/2021/building-trust-in-supply-chains

（3）事業化のニュースリリース

ニュースリリースに対し大きな反響を獲得
（TV3社、新聞/ネット記事40件以上で報道）

サービス化発表のニュースリリース
https://www.hitachi.co.jp/New/cnews/month/2022/08/0803.pdf

NHK：おはよう日本：飲食店の感染リスク「見える化」安全な時間に来店を

フジテレビ：News Live α：飲食店などの感染対策見える化サービス 換気状況など

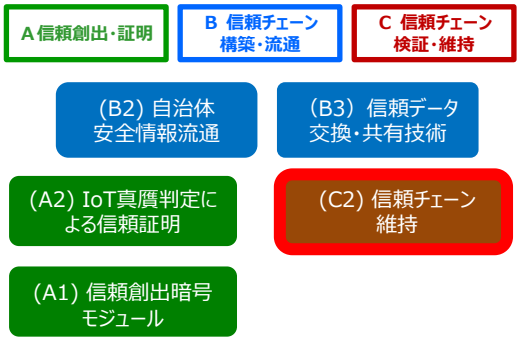
その他 対外発表リスト一覧

研究発表、講演：24件、プレス発表など：4件、特許：2件

年	月	学会名、イベント名など	タイトル	会社名
2019	3	情報処理学会・電子情報通信学会組込み技術とネットワークに関するワークショップ ETNET2019	周辺ネットの特徴量を考慮した二段階のニューラルネットワークによるハードウェアトロイ検出手法	早稲田大学
2019	6	日立セキュリティフォーラム	サプライチェーンセキュリティ ~超スマート社会における信頼を生み出す~	株式会社日立製作所
2019	7	The 16th International Conference on Mobile Web and Intelligent Information Systems	A Framework for Secure and Trustworthy Data Management in Supply Chain	KDDI総合研究所、 国際電気通信基礎技術研究所
2019	7	サイバーセキュリティ国際シンポジウム	今考える、超スマート社会を支えるこれからのサプライチェーンに必要なこと	株式会社日立製作所
2019	10	ATR オープンハウス2019	「Society 5.0」におけるサイバーセキュリティ ～全体像とATRの取り組み～ Cybersecurity for "Society 5.0" – Overview and ATR's activities –	国際電気通信基礎技術研究所
2019	10	ATR オープンハウス2019	サプライチェーンの信頼性を保証する先端セキュリティ技術	国際電気通信基礎技術研究所
2019	10	Hitachi Social Innovation Forum 2019 TOKYO	サプライチェーンの信頼性回復への挑戦 ～製品・サービス不正を防ぎ、信頼でつながる社会へ～	株式会社日立製作所
2019	11	International Workshop of Privacy Security Enhancement Forum 2019	Supply Chain Security for 5G and beyond 5G Era	KDDI総合研究所
2019	12	サイバーセキュリティ国際シンポジウム	サプライチェーン・サイバーセキュリティの社会実装に向けた課題ー官民の施策・課題ー	株式会社日立製作所
2020	1	SCIS2020	SIP委託・再委託者による合同セッション	株式会社日立製作所
2020	1	2020年 暗号と情報セキュリティシンポジウム（SCIS2020）	サプライチェーンの信頼構築に向けたデータの適合性に関する考察	国際電気通信基礎技術研究所、 KDDI総合研究所
2020	6	European Conference on Networks and Communications(EuCNC)	Consideratio on Data Conformance Toward Building Trust in Supply Chain	KDDI総合研究所、 国際電気通信基礎技術研究所
2020	7	日立セキュリティフォーラム 2020 ONLINE	「デジタルトラスト」が生み出す超スマート社会の信頼	株式会社日立製作所
2020	10	CEATEC	サプライチェーンのトラストが生み出す安心な超スマート社会	株式会社日立製作所
2020	10	サイバーセキュリティ国際シンポジウム	サプライチェーントラストに関する国際動向と日立の取り組み	株式会社日立製作所
2020	11	Hitachi Social Innovation Forum 2020 TOKYO ONLINE	サプライチェーンのトラストが生み出す安心な超スマート社会	株式会社日立製作所
2020	11	ATR オープンハウス2020	サプライチェーンの信頼性を保証する先端セキュリティ技術	国際電気通信基礎技術研究所
2021	2	報道発表	イチゴの出荷における温度データの検証に関わる実証実験の実施	KDDI総合研究所、 沖縄セルラー電話
2021	3	第2回 ATR-KDDI総合研究所セキュリティ技術セミナー	サプライチェーンの信頼確保技術	国際電気通信基礎技術研究所
2021	5	RSA Conference 2021	Building Trust in Supply Chains	株式会社日立製作所、 国立研究開発法人産業技術総合研究所
2021	6	日立セキュリティフォーラム 2021 ONLINE	トラストを構築してサプライチェーンをまもる、サプライチェーンにおける信頼の構築	株式会社日立製作所、 国立研究開発法人産業技術総合研究所
2021	6	18th IEEE/ACIS International Virtual Conference on Software Engineering, Management and Applications	Automatic Security Inspection Framework for Trustworthy Supply Chain	KDDI総合研究所、 国際電気通信基礎技術研究所
2021	6	ナノオプト・メディアオンライン セキュリティセミナー	サプライチェーンにおけるデータセキュリティ確保の取り組み – 証跡管理と検証技術 –	KDDI総合研究所
2021	7	報道発表	不正回路検出ツールの実行結果共有に関わる実証実験の実施	KDDI総合研究所、東芝情報システム
2021	10	Hitachi Social Innovation Forum	コロナ対策も安心、トラストが生み出す信頼の社会	株式会社日立製作所
2021	12	Keidanren SDGs	KDDIにおける安心安全なサプライチェーンの実現に向けた取り組み	KDDI総合研究所
2022	6	28th IEEE ICE & 31st IAMOT Conference IEEE	Security Inspection Framework and its Application to Use Cases	KDDI総合研究所
2022	8	ニュースリリース(日立製作所)	施設の衛生管理状況を見える化する「T*Plats」の提供を開始	株式会社日立製作所

出願人	出願国	出願番号	発明の名称	NEDOへの届出日
株式会社日立製作所	日本	特願2020-74817	デジタル署名の管理方法、デジタル署名の管理システム	2020/6/10
	米国 欧州 ドイツ イギリス	US17/191821 EP21160695A 21160695.9 21160695.9	DIGITAL SIGNATURE MANAGEMENT METHOD AND DIGITAL SIGNATURE MANAGEMENT SYSTEM	2021/4/9 2021/4/9 2022/11/11 2022/11/11
国立研究開発法人産業技術総合研究所	日本	特願2022-14066	検証装置、検証方法及び検証プログラム	2022/2/9

（C2）信頼チェーンの維持技術
〔NTT,三菱,日立,NEC 他〕



（1）研究開発概要

サイバー・フィジカルシステム（CPS）に求められる性能を備える低コストな対策技術がなく、攻撃による回復困難な事態の発生が懸念されていた。

当初の懸念どおりCPSをねらうサイバー攻撃は発生しているものの、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、攻撃の手口はCPSのIT領域を侵害する手口が主となっている。

そこで、本研究テーマではCPSにおけるITと非ITの混在を前提としながら、(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ている。

（2） 技術的目標

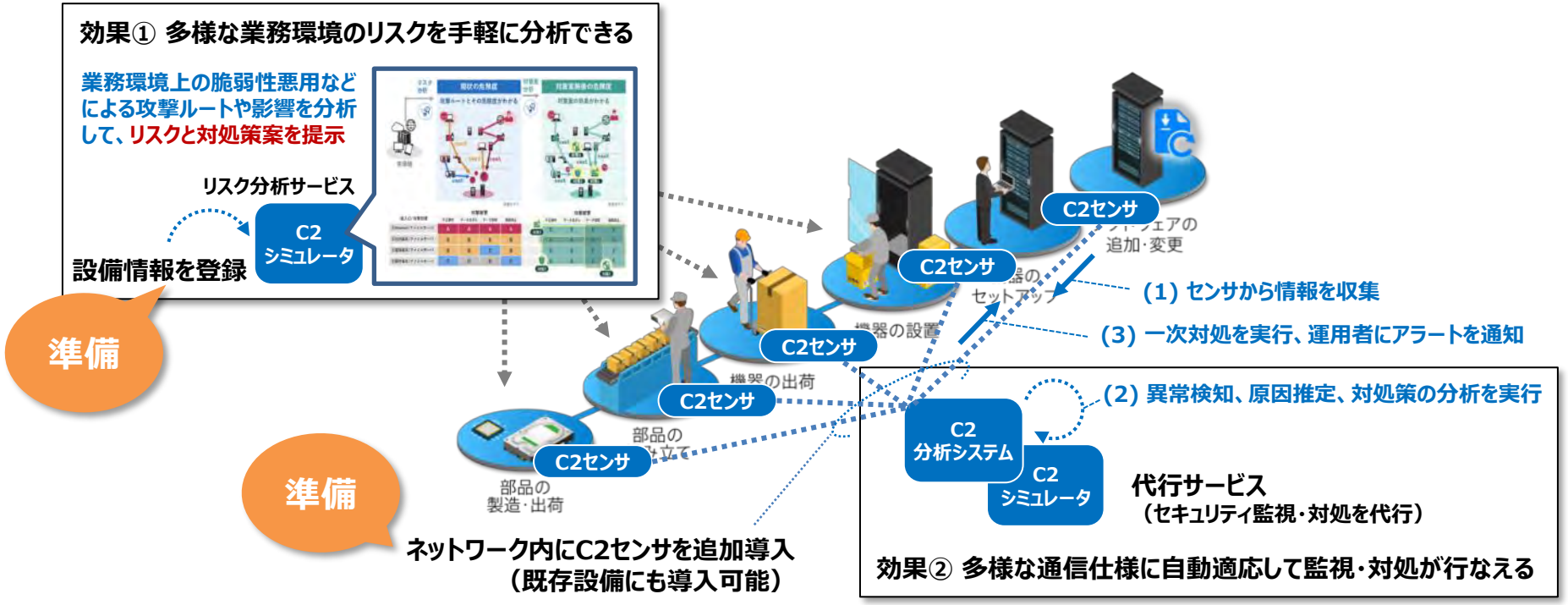
(1)通信プロトコルに対する自動適応によって、多様なCPSのセキュリティ異常検知を可能とするセンシング及び分析技術

(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） 研究開発内容

■ サプライチェーンはさまざまな事業者によって形成されていることから、**多様な業務環境に対応でき、かつ手軽に利用できるリスク分析サービス**を提供することによって侵害リスクを低減する。
■ さらに、通信トラフィックの**センサ追加のみで利用可能なセキュリティ監視・対処の代行サービス**により侵害を早期発見・対処する。



（4） 工程表

（C2）信頼チェーン維持

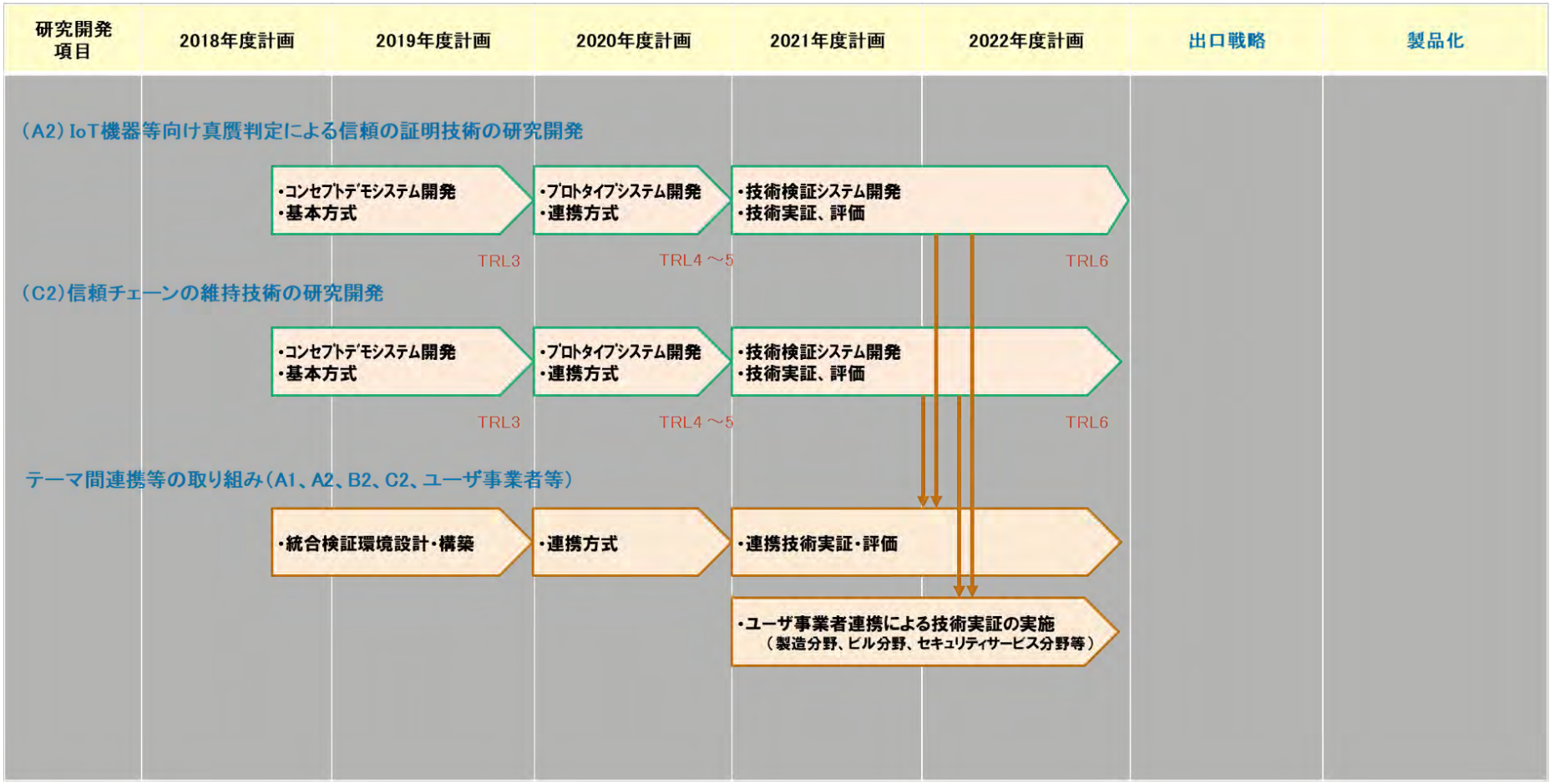
2021年度に開始した実証実験の延長をユーザ事業者と合意して拡充するとともに、新たな実証実験先にも拡大し、研究開発への技術課題フィードバックをさらに充実化させて当初目標の技術を確立するとともに、SIP終了時に当初計画していた「商用化の技術的見通しの獲得」を2022年度上期までに達成した。

出口戦略・社会実装に向けて

「IoT社会に対応したサイバー・フィジカル・セキュリティ」 工程表

（A2）IoT機器等向け真贋判定による信頼の証明技術

（C2）信頼チェーンの異常検知・復旧支援技術



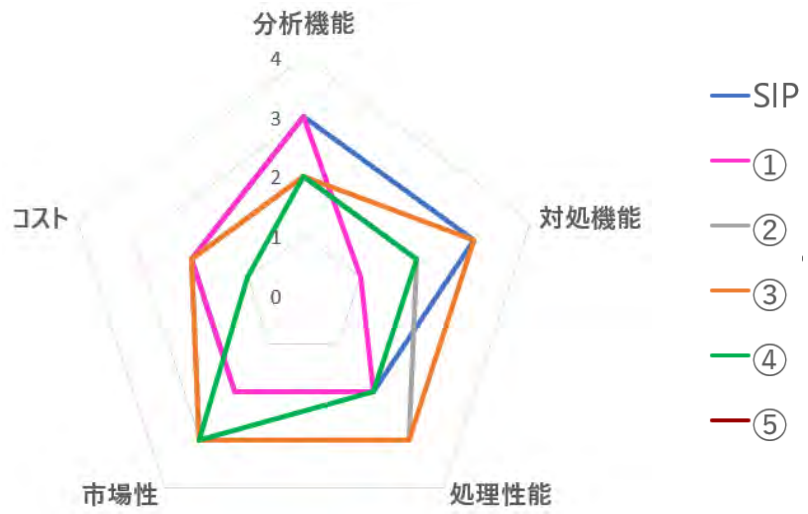
（5） グローバルベンチマーク ①国際競争力

(C2) 信頼チェーン維持

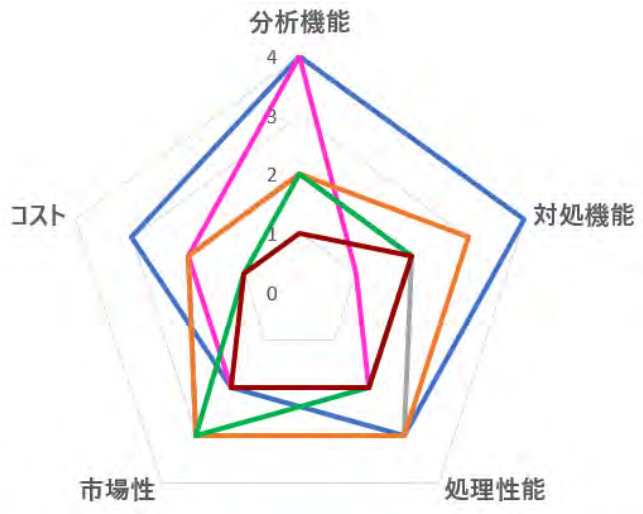
本技術の特長である「分析機能」及び「対処機能」を競争戦略の基軸に据え、他の「システムのセキュリティ分析・対処を自動的に行なう技術」とのベンチマークを実施した。

その結果、「分析機能」の面で優秀な他技術が存在するものの、本技術のプロトコル自動適応方式は他技術と競争状態が長く続くほど、プロトコルの追加対応開発コストの面で優位となることを確認した。「分析機能」の面では本技術独自の「高度な攻撃シミュレーション機能」も加えて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していく。

FY2021



FY2022



（6） ②研究成果で期待される波及効果

- 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。

（7） 研究目標の達成状況・見込み ③達成度（1）

（C2）信頼チェーン維持

2021年度の目標

ア. 本研究テーマの各技術を、実証実験に導入予定の「技術検証システム」へ実装完了する

イ. 実証実験実施に関するユーザ事業者との合意を取る

進捗状況

- 「検知技術」は、OTプロトコルのペイロードから制御コマンドや設定値などを抽出できるDPI特徴量生成技術と、プロトコル種別に依らず任意のペイロードを学習できる汎用プロトコル学習方式の組合せで、当初目標及びプロトコルの市場シェアベースにおける対応カバレッジ率を達成見込みである。
  また、異常原因箇所を自動特定する技術、多様な規模のBA模擬環境を自動構築可能な大規模評価環境技術を確立するとともに、「学習データ汚染対策」「学習モデル保護」を目的とした新たな基礎理論を発明した。
- 「対処技術」は、各IoTシステムにおける信頼性、継続性をシステム特性としてパラメータ化し、サイバー⇔フィジカル間を流れるデータの不正検知時に、不正対処の優先度を合わせて通知する技術をシステム実装を通じて確立し、複数の特許を創出・出願済みである。
- 「リスク分析技術」は、IT/OT領域含む1万台規模に対応したリスク分析及び対処策実行支援機能を開発、OT領域単体は目標規模の適用可能性を確認済である。IT領域は目標規模の適用に向けた高速化を図って適用可能性を2022年度中に確認見込みである。当該機能を先行的にサービス化し、顧客フィードバックを得てリスク分析結果の可読性及びユーザビリティ向上の機能も開発した。対処策実行を支援するための対処策自動立案機能の開発も2022年度中に完了予定である。
- 研究テーマA2、B2、C2の連携については、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（A2の検知結果をB2/C2の分析や制御に用いる等）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。

（7） 研究目標の達成状況・見込み ③達成度（1）【再掲】

(C2) 信頼チェーン維持

トピック①： 実証実験の拡大

- 2021年度に開始した実証実験3件 (IoT機器ベンダ※、Smart City 事業者※×2件)に加えて、2022年度からさらに3件(製造系×2件、交通系)を開始して実施範囲を拡大
- IoTソリューション、IoTサービス等への展開に向けて事業化課題を広範囲から抽出

※ 連結従業員数約600名の国内中堅IoT機器ベンダの設備、最新スマートビル内設備など

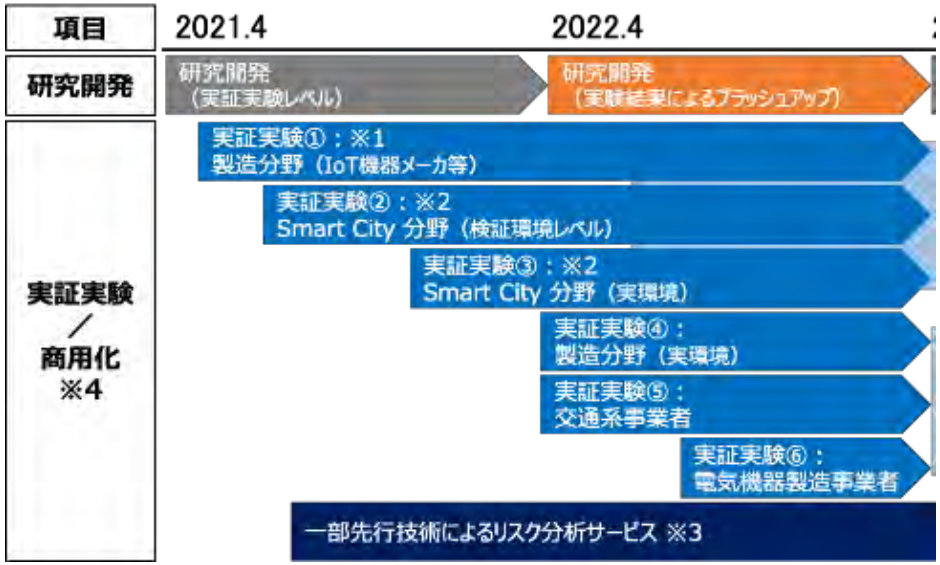
トピック②： サービス提供及び実用化実績に対する表彰の受賞

- 先行技術による「リスク診断サービス※1」を2021年に提供開始し、さらに機能を拡充
- この実用化が評価され、テレコム先端技術研究支援センターSCAT表彰※2を受賞

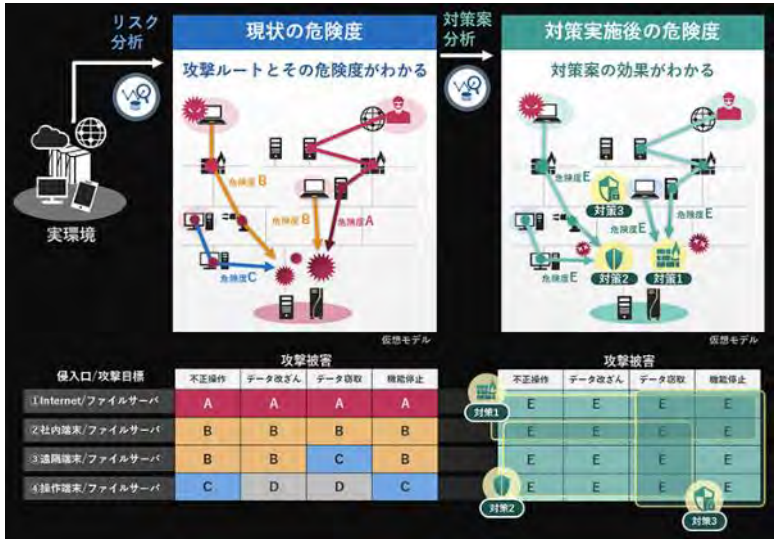
※1「NEC、システムのセキュリティリスクとその対策効果を可視化するサービスを提供開始」
（ https://jpn.nec.com/press/202106/20210629_01.html ）
※2 https://www.scat.or.jp/awards/file/2022awards.pdf

（ウ）実証実験及び商用化の実施状況

実証実験はA2と連携して進めているものの他、「交通系事業者」「電気機器製造事業者」における対処技術の実証を追加開始した。リスク分析技術は、データ自動収集の主要ツール対応によって先行提供中のサービスを機能強化。



サイバー攻撃ルート診断サービス（NEC）



https://jpn.nec.com/cybersecurity/professionalservice/vulnerability_diagnosis/attack_route.html

診断サービスの商用可に伴い、2021年に第69回電気科学技術奨励賞を受賞したリスク分析技術は、先行提供サービスにおける顧客フィードバックを元にして「分析結果の可読性改善」を予定どおり達成。

（8） 出口戦略

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コア技術を中心に知財確保を実施中である。
  特許出願26件（フォアグラウンド知財11件、うち公開6件、バックグラウンド知財15件）
- 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、標準仕様を採用することによって本技術が広く普及しやすい状況を確保している。

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（34件、うち表彰受賞4件※）、展示会・シンポジウム等（21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。