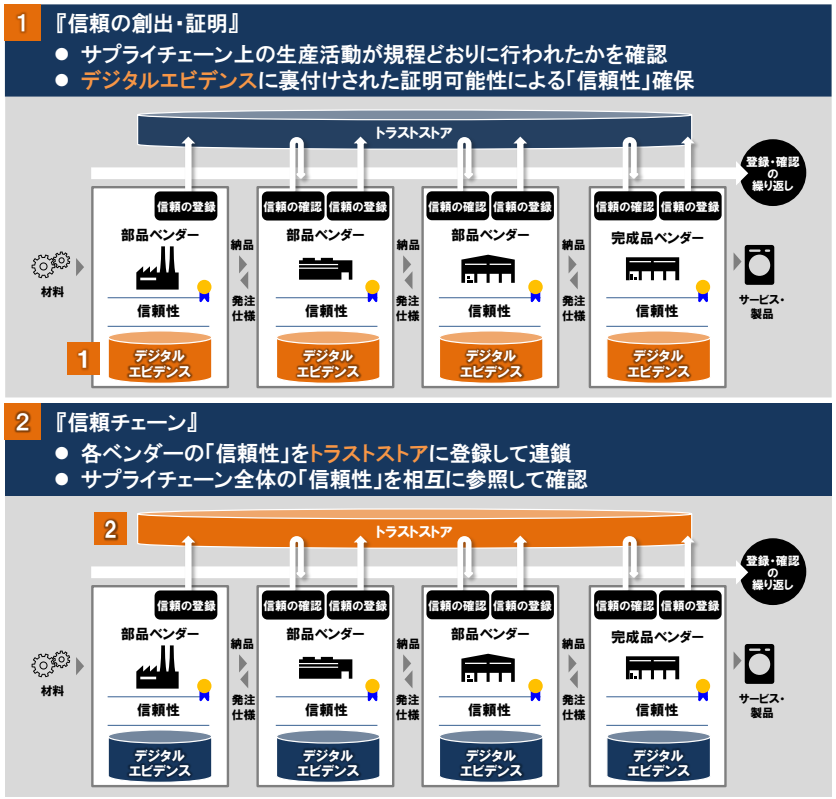
（8） 出口戦略 【再掲】

(1)技術開発トピックス

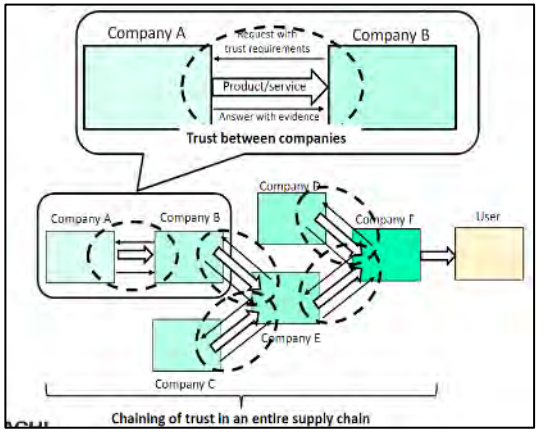
2020年暗号と情報セキュリティシンポジウム(SCIS2020)での「サプライチェーンセキュリティ」セッションにおいて、日立、KDDI総研、NEC、産総研で計5件の発表を実施し、開発技術の必要性・有用性をアピール。

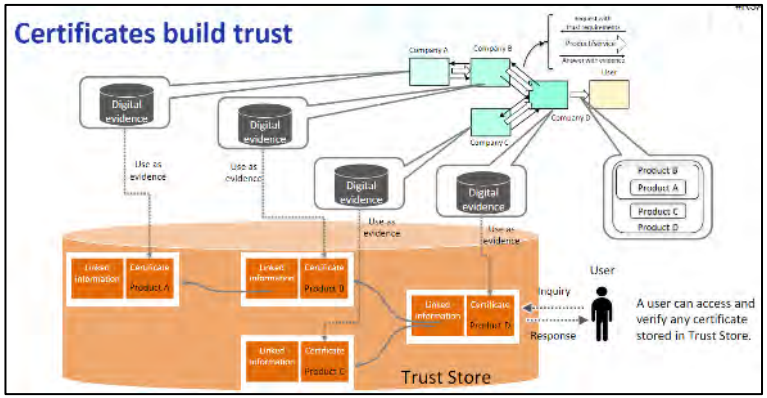


http://www.iwsec.org/scis/2020/program.html

(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

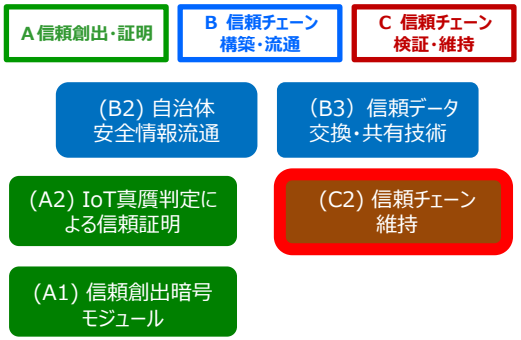
その他 対外発表リスト一覧

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

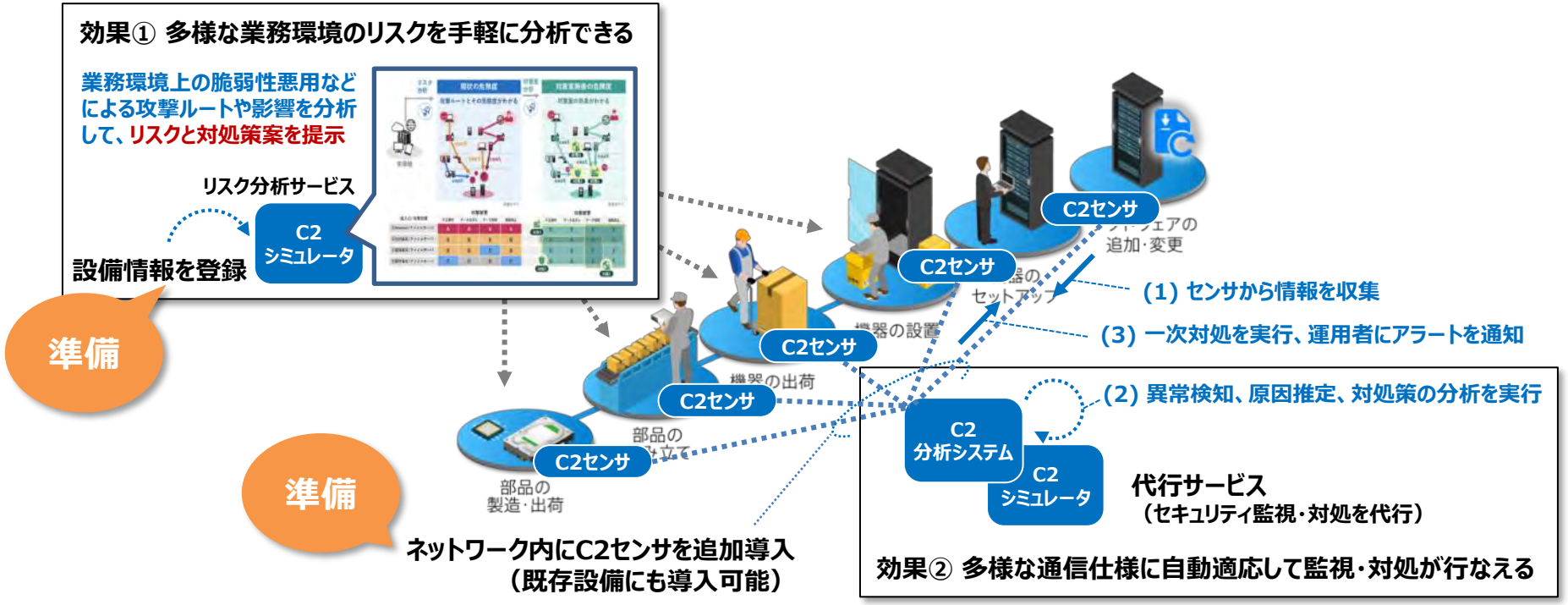
(1)通信プロトコルに対する自動適応によって、多様なCPSのセキュリティ異常検知を可能とするセンシング及び分析技術

(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

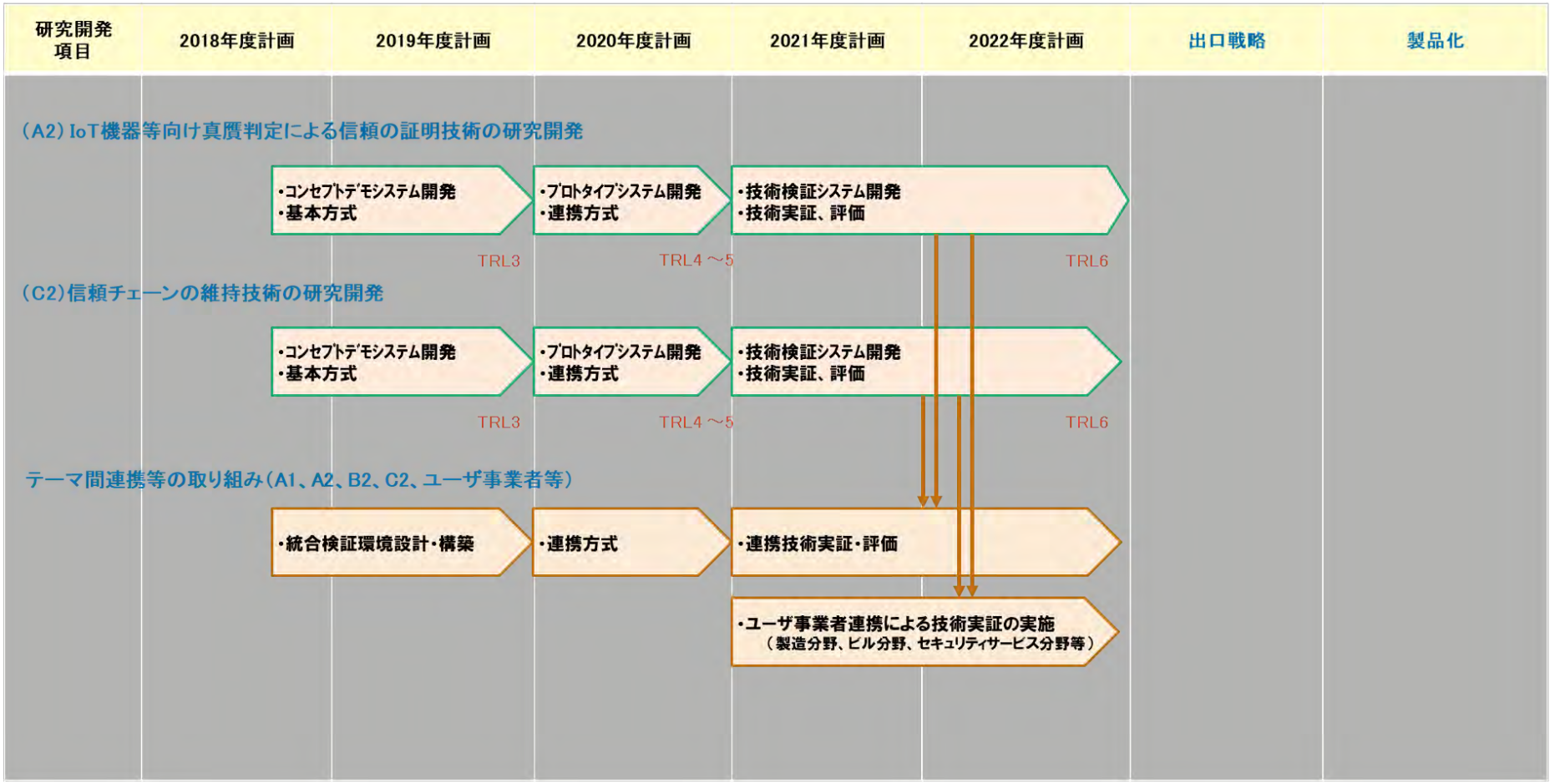
2021年度に開始した実証実験の延長をユーザ事業者と合意して拡充するとともに、新たな実証実験先にも拡大し、研究開発への技術課題フィードバックをさらに充実化させて当初目標の技術を確立するとともに、SIP終了時に当初計画していた「商用化の技術的見通しの獲得」を2022年度上期までに達成した。

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



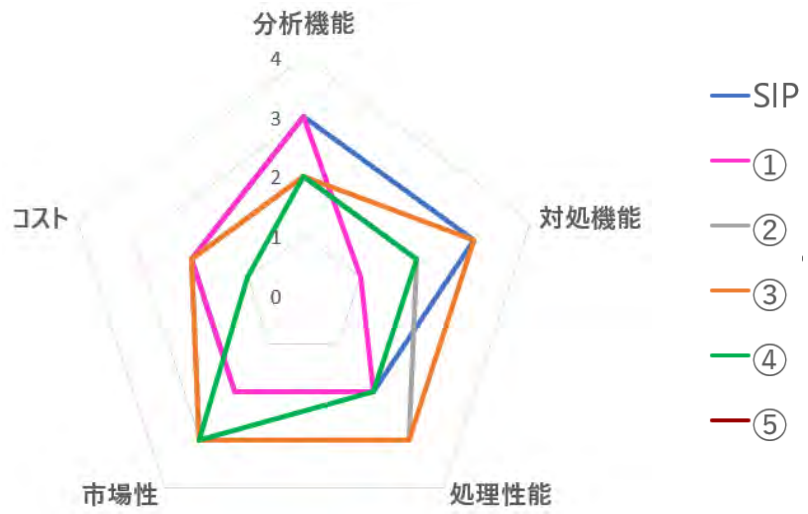
（5） グローバルベンチマーク ①国際競争力

(C2) 信頼チェーン維持

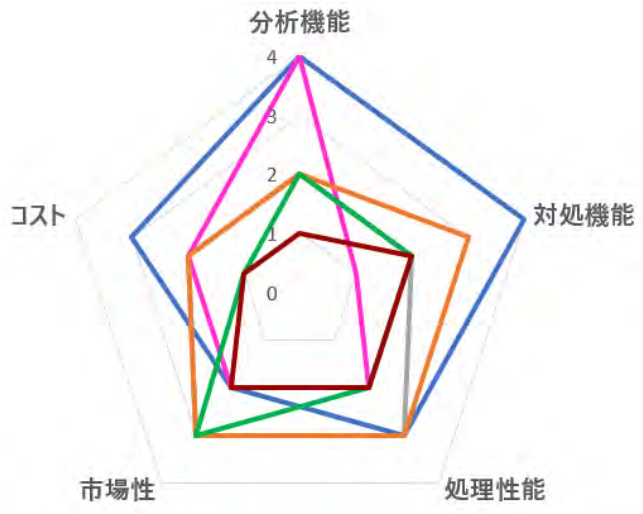
本技術の特長である「分析機能」及び「対処機能」を競争戦略の基軸に据え、他の「システムのセキュリティ分析・対処を自動的に行なう技術」とのベンチマークを実施した。

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

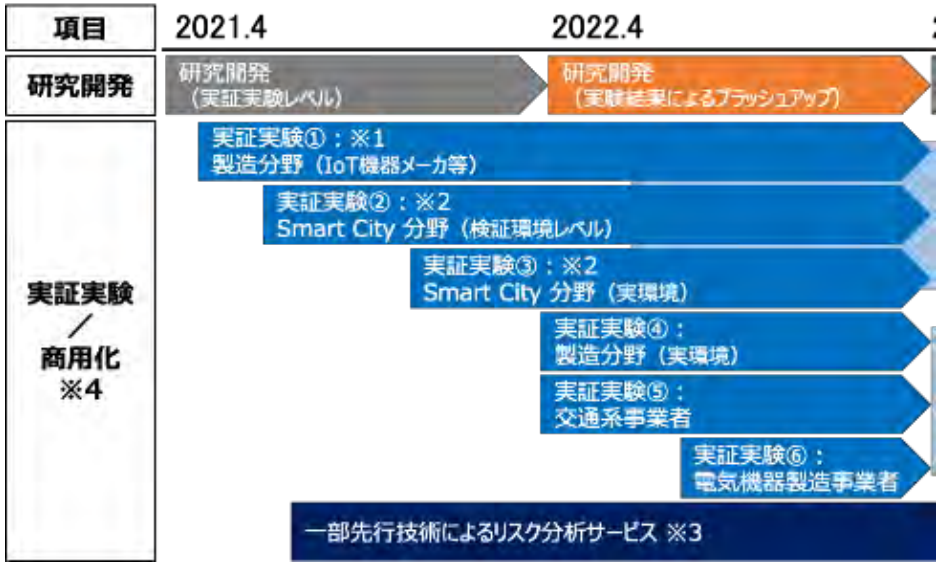
トピック②： サービス提供及び実用化実績に対する表彰の受賞

- 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

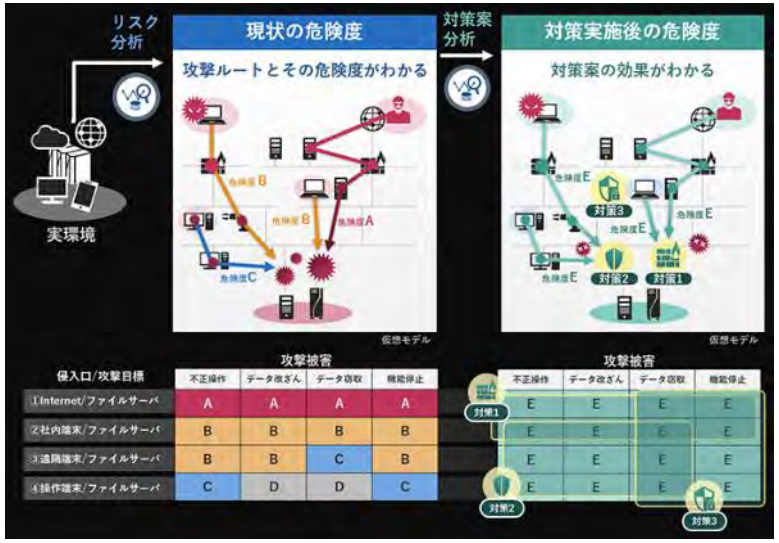
※1「NEC、システムのセキュリティリスクとその対策効果を可視化するサービスを提供開始」
（ https://jpn.nec.com/press/202106/20210629_01.html ）
※2 https://www.scat.or.jp/awards/file/2022awards.pdf

（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。