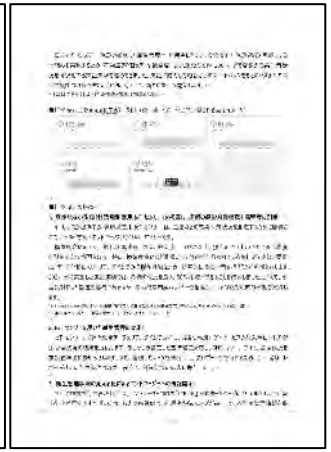
# （B3）サプライチェーン全体の信頼性確保に向けた信頼データ交換・共有技術

## （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、<br>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、<br>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、<br>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、<br>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、<br>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、<br>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、<br>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<br>欧州<br>ドイツ<br>イギリス | US17/191821<br>EP21160695A<br>21160695.9<br>21160695.9 | DIGITAL SIGNATURE MANAGEMENT METHOD AND DIGITAL SIGNATURE MANAGEMENT SYSTEM | 2021/4/9<br>2021/4/9<br>2022/11/11<br>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

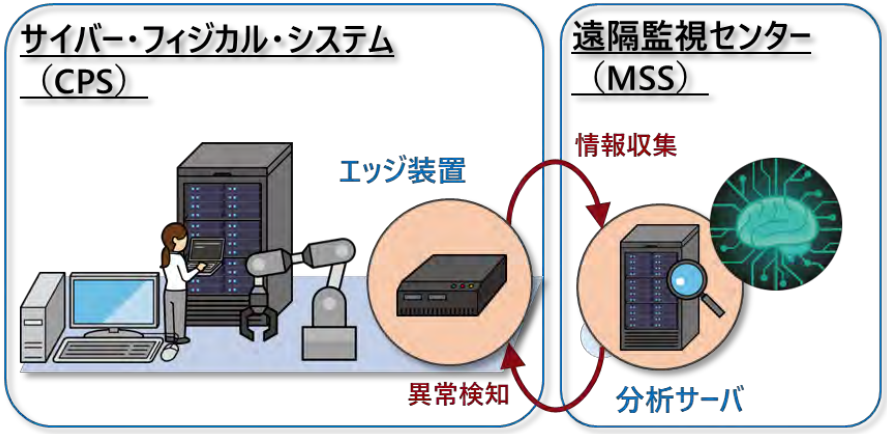
## トピック②：サービス提供及び実用化実績に対する表彰の受賞

- 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

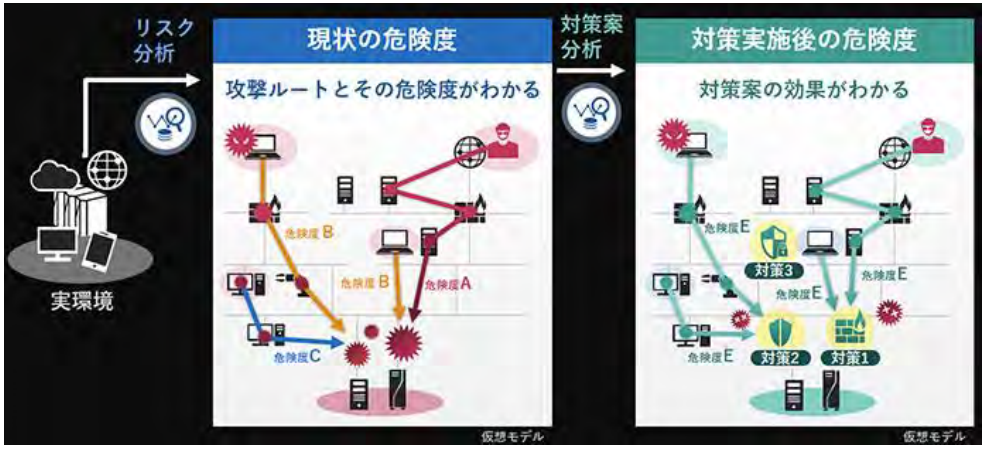
※1「NEC、システムのセキュリティリスクとその対策効果を可視化するサービスを提供開始」（ https://jpn.nec.com/press/202106/20210629_01.html ）

※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）

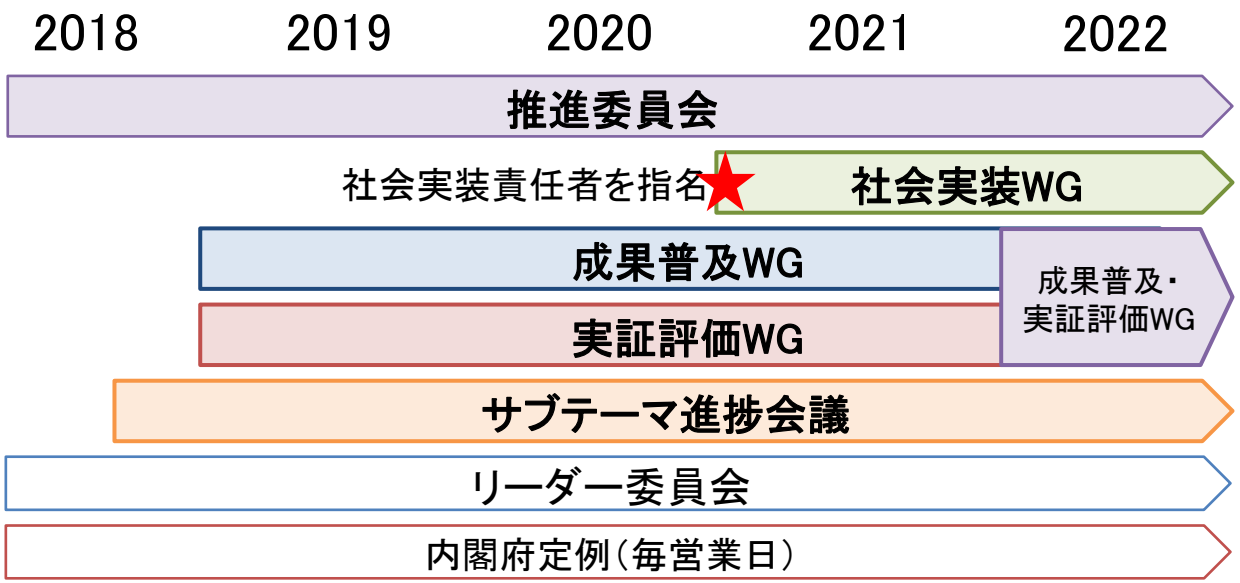
**A.信頼の創出・証明**

**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。



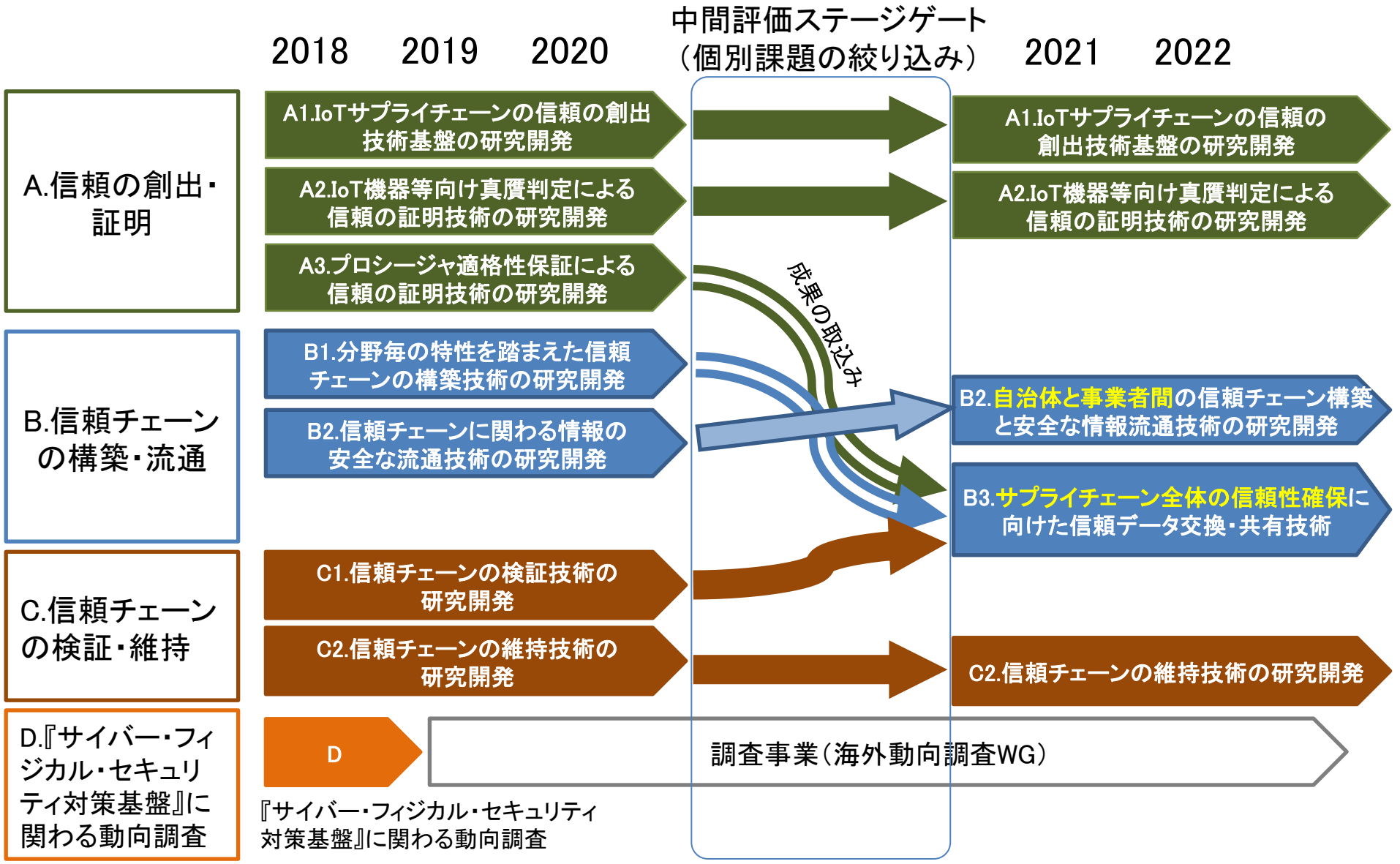

推進委員会、WG等参加者

▽ 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]<br>➢米NIST 所長 Dr. C.Romine |
| 2019 | ● シンポジウム　2019年10月31日（木）<br>➢米NTIA アラン・フリードマン　（SBOM）<br>➢ NISC 山内智生（CS戦略）<br>SBOM議論、プロトタイプ展示<br>  | ● 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]<br>➢ 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）<br>➢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）<br>➢ CYR3CON Paulo Shakarian　（ダークウェブ分析）<br>➢経団連産業技術本部　吉村隆<br>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）<br>➢BitSight Mr.Stephen Boyer（ソフトウェアサプライチェーン）<br>➢トヨタ自動車　村田賢一　（次世代モビリティ）<br>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）<br>2023年2月9日（木）<br>➢米MITRE Robart A Martin（Systems of Trust）<br>**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<br>技術研究組合が営利法人化 |

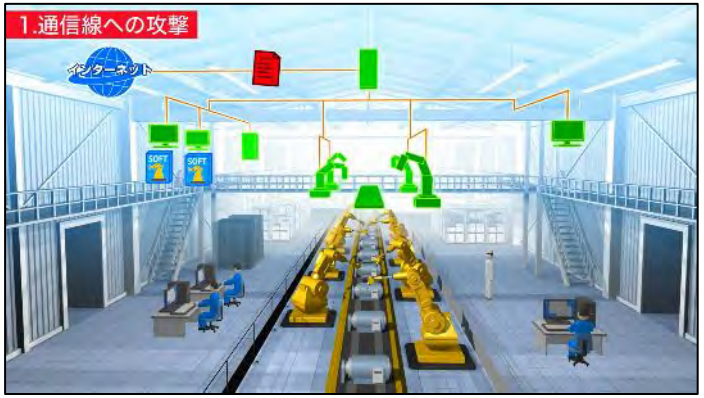
# 5年間の成果まとめ：シンポジウム2022

- 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<br>◆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<br>◆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）<br>◆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<br>（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<br>◆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。

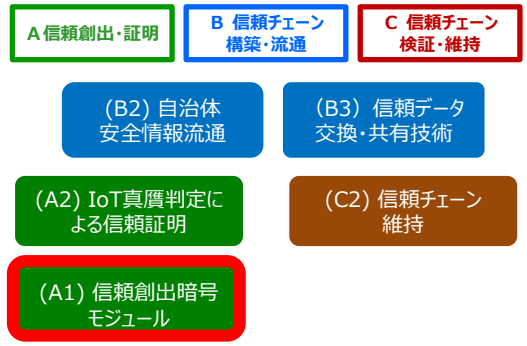
◆ 課題マネジメント

- 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。