２０１９年度成果報告書

戦略的イノベーション創造プログラム（SIP）第２期

IoT 社会に対応したサイバー・フィジカル・セキュリティ

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実証実験計画に向けた動向調査

２０２０年２月

国立研究開発法人　新エネルギー・産業技術総合開発機構
委託先　株式会社サイバー創研

目次

まえがき

IoTは、Society 5.0[1] の基盤技術であり、社会インフラ、産業システム、生活環境、自然環境等のフィジカル空間に埋め込まれた IoT 機器が、多様なネットワークを介してクラウド等のサイバー空間と連結され、AIに代表される高度な知識処理やビッグデータとしての分析・解析処理と連携することにより、様々な付加価値やサービスを創出し、フィジカル空間である経済社会に多大な恩恵をもたらすと期待されている。一方、サイバー攻撃の対象は急激に拡大し、攻撃の手法も著しく高度化している。特に、産業社会や家庭生活に新たな価値創造をもたらす IoT の普及・拡大に伴い、サイバー攻撃の脅威は、サイバー空間だけでなくフィジカル空間を合わせた、あらゆる産業活動に潜むようになっている。また、製品やサービスを製造し流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題も顕在化しつつあり、グローバルなサプライチェーンにおいてサイバーセキュリティ対策の強化が求められている。今後は一定の水準のセキュリティ要件を満たさない事業者、製品、サービスがグローバルな調達要件からはじき出される恐れがあり、輸出の大部分を占める製造業の参入機会を確保することが重要な課題となる。

このため、セキュアな Society 5.0 の実現に向け、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、IoT システム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証が行われている。

本調査事業の目的は、セキュアな Society 5.0 の実現に向けて取り組んでいる「戦略的イノベーション創造プログラム（SIP）第2期／IoT社会に対応したサイバー・フィジカル・セキュリティ」（以下、CPS プロジェクト）において、研究開発成果の実用化・事業化を促進するために、研究開発成果の利用者であるサプライチェーンの各ステークホルダを含めた実証実験を次年度以降に効果的に行うための情報収集、及び実社会での実装における課題抽出を行うことである。

本調査事業では、実証実験において、各分野のサプライチェーン全体を通して効果が明確にアピールでき、さらに多数のステークホルダの参加が見込まれ、かつ実証実験後に実用化・事業化にスムーズに移行できるような計画とすることを目標とし、下記の3項目を実施した。

1. 実証実験計画提案のための動向調査
2. 具体的な実証実験計画の提案
3. 実証実験の促進に係る課題の抽出と、調査結果の取りまとめ

---

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

調査実施にあたっては、CPS プロジェクトの実証評価ワーキンググループ及び実証評価サブワーキンググループに実施計画を提示し、調査の進捗状況を報告して確認いただくことにより実証実験の計画の参考となる調査とした。

1　動向調査の成果と達成状況

和文要約

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

一方、サイバー攻撃の対象は急激に拡大し、攻撃の手法も著しく高度化している。特に、産業社会や家庭生活に新たな価値創造をもたらす IoT の普及・拡大に伴い、サイバー攻撃の脅威は、サイバー空間だけでなくフィジカル空間を合わせた、あらゆる産業活動に潜むようになっている。また、製品やサービスを製造し流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題も顕在化しつつあり、グローバルなサプライチェーンにおいてサイバーセキュリティ対策の強化が求められている。今後は一定の水準のセキュリティ要件を満たさない事業者、製品、サービスがグローバルな調達要件からはじき出される恐れがあり、輸出の大部分を占める製造業の参入機会を確保することが重要な課題となる。

このため、セキュアな Society 5.0 の実現に向け、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、IoT システム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証が行われている。

本調査事業の目的は、セキュアな Society 5.0 の実現に向けて取り組んでいる「戦略的イノベーション創造プログラム（SIP）第２期／IoT 社会に対応したサイバー・フィジカル・セキュリティ」（以下、CPS プロジェクト）において、研究開発成果の実用化・事業化を促進するために、研究開発成果の利用者であるサプライチェーンの各ステークホルダを含めた実証実験を次年度以降に効果的に行うための情報収集、及び実社会での実装における課題抽出を行うことである。本調査事業では、実証実験において、各分野のサプライチェーン全体を通して効果が明確にアピールでき、さらに多数のステークホルダの参加が見込まれ、かつ実証実験後に実用化・事業化にスムーズに移行できるような計画とすることを目標とし、下記の3項目を実施した。

1. 実証実験計画提案のための動向調査
2. 具体的な実証実験計画の提案
3. 実証実験の促進に係る課題の抽出と、調査結果の取りまとめ

調査実施にあたっては、CPS プロジェクトの実証評価ワーキンググループ及び実証評価サブワーキンググループに実施計画を提示し、調査の進捗状況を報告して確認いただくことにより実証実験の計画の参考とすることができる調査とした。

セキュアなサプライチェーンの構築は拡大と発展の途上にあり、サイバー・フィジカル・セキュリティに関する市中の認識と期待は、本プロジェクトの活動を通じて一層高まり、今後具体的な課題も明らかになってくると予想される。このため CPS の研究開発と並行して今後も動向調査を継続することが必要であり、動向調査を有用なものとするための課題を報告した。

英文要約

IoT is the fundamental technology of Society 5.0. Through the connection with cyberspace such as clouds via various networks and the collaboration with advanced knowledge processing and analysis processing as big data, IoT devices which are embedded in the physical spaces such as social infrastructure, industrial system, living environment and natural environment, are expected to create various values added and services . They are also expected to bring great benefits to our economy society.

On the other hand, the scope of the targets of cyberattacks is rapidly expanding, and attack techniques are becoming more advanced. In addition, the risks of illegal programs being embedded, and programs being altered in an unauthorized manner during the processes of production and distribution of products and services, are becoming more prevalent within supply chains.

For this reason, for the purpose of protecting various IoT devices, and ensuring safety and security in society as a whole, we are engaging to develop and verify ″Cyber Physical Security Infrastructure″ which can be utilized to protect IoT system/services and large-scale supply chains including SMEs as a whole.

″Strategic Innovation Promotion Program (SIP) Phase 2 / ″Cyber Physical Security″ for IoT Society (hereinafter CPS Project), is working towards realization of a secure Society 5.0. The purpose of this trend survey is to collect information and to extract issues in implementing the R&D results in the real world in order to conduct the experimental demonstration after the next year efficiently. The experimental demonstration involves stakeholders in the supply chains and aims to promote their practical realization and commercialization of the R&D results.

In this survey of trend, we have conducted following three items.

1. Conduct trend survey in order to propose demonstration experiment plan
2. Propose concrete demonstration experiment plan
3. Extract issues related to the promotion of demonstration experiments and to summarize survey results

In conducting the survey, we presented the implementation plan, and reported and confirmed the progress of the survey to the demonstration and evaluation working group of CPS project so that it could be used as a reference for the experimental demonstration plan.

As the construction of secure supply chains is on a way of developing and expansion, the importance of CPS projects will be recognized increasingly further in the future. The survey of the trends should be continued in parallel with research and development of CPS project and we will report the issues that could the trend survey useful.

2　動向調査の目的

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

本調査事業は、セキュアな Society 5.0 の実現に向けて取り組んでいる「戦略的イノベーション創造プログラム（SIP）第 2 期／IoT 社会に対応したサイバー・フィジカル・セキュリティ」（以下、CPS プロジェクト）において、研究開発成果の実用化・事業化を促進するために、研究開発成果の利用者であるサプライチェーンの各ステークホルダを含めた実証実験を次年度以降に効果的に行うための情報収集、及び実社会での実装における課題抽出を行うことを目的とした。

3　実施内容

3.1　概要

本調査事業では、実証実験において、各分野のサプライチェーン全体を通して効果が明確にアピールでき、さらに多数のステークホルダの参加が見込まれ、かつ実証実験後に実用化・事業化にスムーズに移行できるような計画とすることを目標とし、下記の3項目を実施した。

1. 実証実験計画提案のための動向調査
2. 具体的な実証実験計画の提案
3. 実証実験の促進に係る課題の抽出と、調査結果の取りまとめ

調査実施にあたっては、CPS プロジェクトに設置された実証評価ワーキンググループ及び実証評価サブワーキンググループに調査計画を提示し、その進捗状況を報告して確認いただくことにより実証実験の計画の参考となる調査とした。

3.2　実証実験提案のため動向調査

3.2.1 サプライチェーンの調査

CPS プロジェクトにおいては、中小企業も参加するサプライチェーンの信頼性が課題となると認識されている。CPS プロジェクトが取り組んでいるテーマがフィットするサプライチェーンを確認し実証実験提案の検討資料とするために、調査対象とするサプライチェーンを限定することなく公開情報から調査可能な一般的なサプライチェーンを複数抽出して一次調査を行った。サプライチェーンの一次調査においては、対象とするサプライチェーンの網羅性や調査の完全性よりも、現在のサプライチェーンの概要の把握を優先させて調査することを実証評価ワーキンググループにおいて確認した。

一次調査における調査項目の選定にあたっては、5 件のサプライチェーンをサンプル調査し、各サプライチェーンで公開されている情報の確認を行なったのち、表 3-1 に示す調査項目を設定した。また、サプライチェーンを特徴づけるための分類モデルとして表 3-2 の検討を行ない、今回のサプライチェーンの一次調査では表 3-3 の 5 項目の分類でサプライチェーンを特徴づけることを実証評価ワーキンググループにおいて確認した。

一次調査の対象として抽出した 16 件のサプライチェーンを付表 A 一次調査対象のサプライチェーンに示す。

表 3-1 一次調査項目

項番	調査項目
1	推進主体者
2	サプライチェーンで流れるもの
3	実際のサプライチェーンの流れ・工程
4	サプライチェーンの範囲
5	サプライチェーンのリスクが記述されているか
6	サイバーセキュリティリスクに関して意識されているか
7	リスクはサプライチェーンの仕組みか、サプライチェーンで流れる対象か
8	市場規模
9	現在の進捗度合い
10	中小企業が関与するか

表 3-2 サプライチェーンの分類検討モデル

モデル		サプライチェーンが固定・系列化		各サプライチェーンが独立 複数のサプライチェーンが柔軟に構成され併存		規制	その他
	サブ分類	大企業が強い	中小企業が強い	中核企業あり	中核企業なし		
分野	もの：製造	自動車 建設		衣料品 IoTデバイス・組込機器 （ネットワークカメラ等）		防衛装備品	
	もの：食料品	ビール 生協		食品加工	生鮮食料品		ハラール
	ソフトウェア	業務系ソフトウェア		スマートフォンアプリ			
	サービス	金融（銀行・証券・保険）		ビルメンテナンス ヘルスケア		公共 通信・放送 電力・ガス	

IPAの分類†	垂直型		水平型		ユーザ組合せ型
	調達者仕様決定型	供給者仕様決定型	調達者仕様決定型	供給者仕様決定型	

† ソフトウェアサプライチェーン における変化と課題 https://www.ipa.go.jp/files/000040879.pdf の図表を加工

表 3-3 サプライチェーンを流れるものの分類

項番	分類		
1	もの	製造	食料品
2			食料品以外
3		流通	
4	ソフトウェア		
5	サービス		

3.2.2 実証実験の実用性や効果測定をするための評価軸と手法の調査

(1) 他の実証実験プロジェクトにおける評価項目の調査

CPS プロジェクトの実証実験の結果が、CPS プロジェクト関係者以外にも納得感があるものとするために、実証実験の実用性や実効性を効果測定するための手法の検討を行う。この検討の一環として、実証実験を実施して報告書を公開しているプロジェクトを選定し、そのプロジェクトの評価軸や評価項目の調査を行なうこととし、実証評価サブワーキンググループにおいて調査対象とする実証実験プロジェクトとして表 3-4 の 4 件を選定した。

調査対象とした 4 件の実証実験プロジェクトの評価項目を付表 B 1～4 に示す。

表 3-4 評価軸・評価項目を調査した実証実験プロジェクト

プロジェクト		概要	参照先
1	データ利活用型スマートシティ推進事業	地域が抱える様々な課題の解決や地域活性化・地方創生を実現する。	https://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000261.html https://www.soumu.go.jp/main_content/000563431.pdf"
2	横浜スマートシティプロジェクト(YSCP)	H24 年度半ばを目処に CEMS を中心とした地域エネルギーマネジメントシステムを技術的に確立し、デマンドレスポ ンス(DR)などの運用モデルの確立した。H25,H26 年度には、各種 DR 実証を実施し効果を検証した。	https://www.city.yokohama.lg.jp/kurashi/machizukuri-kankyo/ondanka/etc/yscp/yscp01.html
3	「戦略的イノベーション創造プログラム(SIP)自動走行システム ／大規模実証実験 ／情報セキュリティ実証実験」 （自動走行システム実証実験プロジェクト）	自動走行におけるセキュリティ脅威の調査/分析 を行い、国際標準化も見据えた車両レベルでのセキュリティ評価手法・プロトコルを策定し、本実 証実験を通して募る参加者の実車両システムを用いて対ハッキング性能検証のためのブラックボッ クステストを実施する。	https://app5.infoc.nedo.go.jp/disclosure/SearchResultDetail
4	スマート農業加速化実証プロジェクト	生産者の生産性を飛躍的に向上させるためには、近年、技術発展の著しいロボット、AI、IoT 等の先端技術を活用した「スマート農業」の社会実装を図ることが急務であるため、現在の技術 レベルで最先端の技術を生産現場に導入・実証する。	https://www.affrc.maff.go.jp/docs/smart_agri_pro/smart_agri_pro.htm

(2) システム評価モデルの調査

前項の実証実験を行っているプロジェクトの調査から得られた評価項目は、各プロジェクトの実証実験内容を強く反映したものとなっており、その研究開発内容は CPS プロジェ

クトの研究開発内容と重なる要素は少ない。また、実証実験の報告書には評価項目の設定における基本方針などについての情報がなく、他の実証実験プロジェクトの今回の調査結果を CPS の実証実験の評価の参考とすることは困難であった。

CPS の実証実験の成功を判断することができる CPS の各テーマ共通の評価軸を検討するための次の調査として、システムや製品の品質を評価する手法の調査を行った。SQuaRE[2]（スクウェア）はシステム及びソフトウェアの品質を評価するための国際規格であることから、その基本となる品質モデルを調査した。

つながる世界のソフトウェア品質ガイド[3]によれば、SQuaRE はシステム及びソフトウェアの利用者、受注者、開発者などの多岐にわたるステークホルダが持つ多様な品質要求を定義し、その実装を評価するための共通の考え方の基準の一つである。品質を定義し評価するために用いられる属性の集合である品質特性を最も重複が少なくなるように定義しており、品質を客観的かつ定量的に評価することができる。品質の観点や基準には、唯一無二の正解がある訳ではないことから、SQuaRE は観点に抜け漏れがないことや理解しやすいこと、基準が実用的かつ客観的な判断につながることなどの基本要件を充足するという立場から制定されている。

SQuaRE の品質モデルの品質特性を図 3-1 と図 3-2 に示す。また、システム／ソフトウェアの品質特性と利用時の品質特性との間には図 3-3 の関係が示されている。

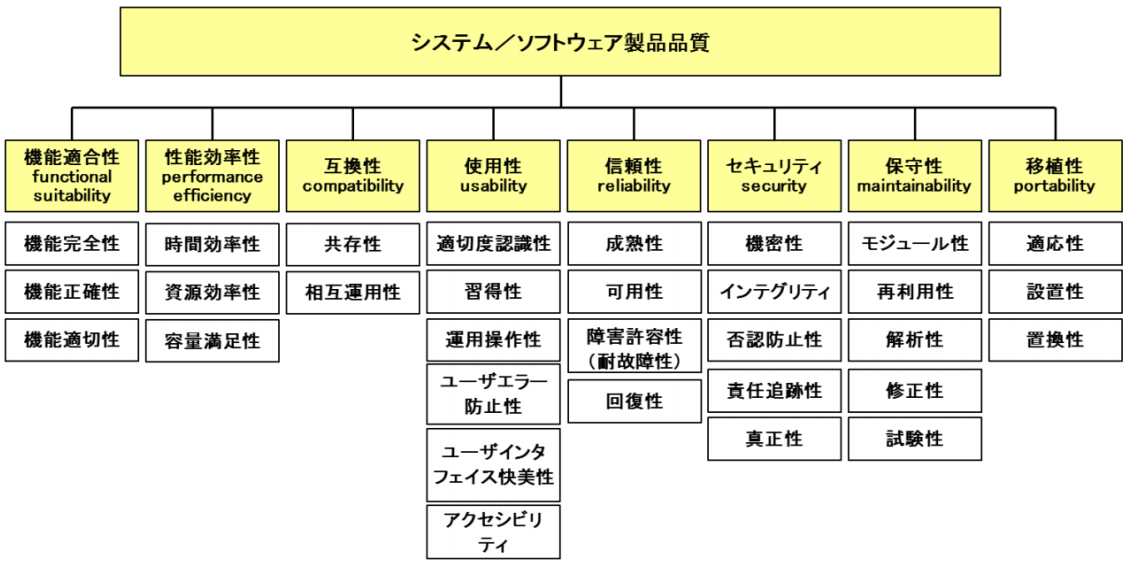


図 3-1 システム／ソフトウェア製品の品質特性 [3]

[2] SQuaRE:ISO/IEC 25000, JIS X 25000 シリーズ
[3] つながる世界のソフトウェア品質ガイド https://www.ipa.go.jp/files/000044964.pdf

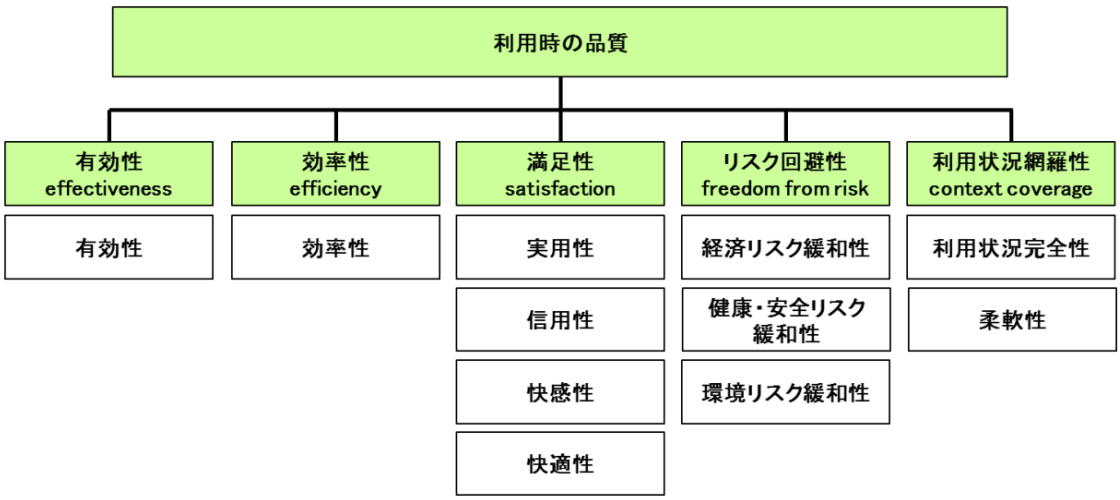


図 3-2 利用時の品質特性[3]

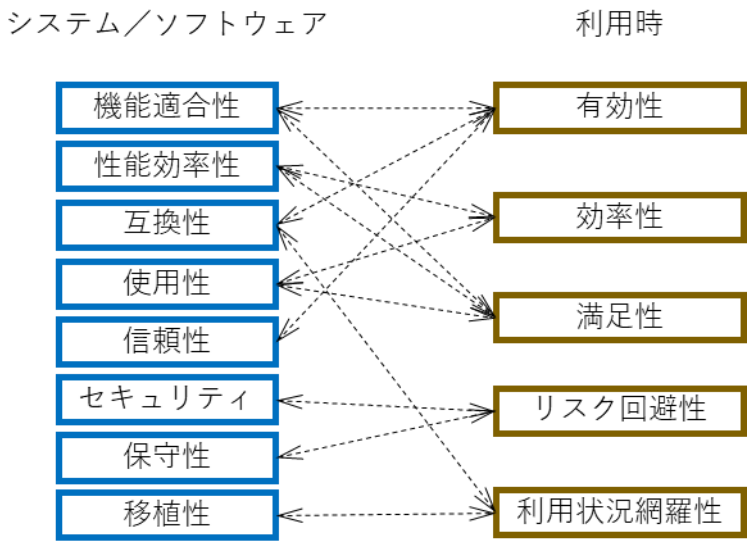


図 3-3 システム／ソフトウェアの品質特性と利用時の品質特性間の関係

3.2.3 CPS が目指すゴールと関係するシステム、認定制度、標準等の調査

CPS に関係する海外の情勢、サプライチェーンや製品認定に関する制度、標準化の動きなどの状況を CPS の研究開発及び実証評価の検討に反映するために、CPS プロジェクトが目指すゴールと関連する活動等の概要を短期間で把握し、結果を研究開発テーマに提供するための調査を行った。以下の 5 件の調査結果を、実証評価サブワーキンググループを通じて CPS のテーマ担当者と共有した。

(1) MS Azure Sphere（調査情報を表 3-5 に示す）

- マイクロソフトが提供するIoTデバイスのセキュリティ強化を目的とした総合的プラットフォームで 2018/04 に発表。
- 次の3つのコンポーネントで構成される。
  a) セキュリティで保護されたコネクテッドクロスオーバーマイクロコントローラーユニット（MCU）
  b) カスタムの高レベル Linux ベース オペレーティングシステム（OS）
  c) 継続的で更新可能なセキュリティを提供するクラウドベースのセキュリティサービス（Azure Sphere Security Service）
- 上記3つのコンポーネントが 2031 年までの更新サポートを含んで一括販売される。

(2) PSA Certified : Building trust in IoT（調査情報を表 3-6 に示す）

- Arm が 2019 年 2 月に発表した IoT 機器のセキュリティを第三者が認定する制度。世界的に有名なテストラボ 4 社とセキュリティコンサルタント、及び Arm が実施。
- Arm が提唱する IoT 機器のセキュリティフレームワーク「Platform Security Architecture（PSA）」に基づき、チップや OS、デバイスが開発されているかどうかを第三者がテストし認定する。
  PSA Certified は PSA の 4 つのステップの4番目に該当する。
- IoT チップ、OS、装置のための独立した評価スキームと、3 段階の認証レベルがある。
  認証には次の 2 種類がある。
  a) PSA certified Functional API ：PSA 開発 API に対する API 準拠を評価
  b) PSA certified ： 堅牢性に対する 3 段階のセキュリティテスト

(3) IETF CBOR（調査情報を表 3-7 に示す）

- IETF で標準化が進められている IoT 機器など計算リソースに制約がある環境に適したデータ表現形式。JSON フォーマットをバイナリ形式で表現したもの。RFC7049 で規定。
- 現在、Standards Track の PS(Proposed Standard)であるが、既にセンサ等 IoT 機器ネットワークの開発プラットフォームや、各種クラウドサービスにおける IoT ネットワークサービス、各種認証システム等において実装が進んでいる。
  a) Apache 2.0 や MIT ライセンスのオープンソースのライブラリが存在
  b) AWS、Alibaba Cloud での IoT 向けクラウドサービスで、CBOR 形式のデータをサポート
  c) Chrome（Android 含む）、Edge 等のブラウザや SNS アプリ等で FIDO 認証関連技術の実装が進行中

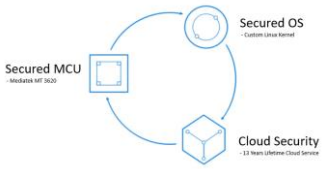
(4) RRI による日独間連携活動

- RRI（Robot Revolution & Industrial IoT Initiative）はロボット新戦略を推進するために次の活動を目的として民間主導で設立。
  a) 世界のロボット・イノベーション拠点としての日本―ロボット創出力の抜本的強化
  b) 世界一のロボット利活用社会
  c) IoT時代の到来を見据えたロボット新時代への世界の中でのイニシアティブの発揮
- 活動の一部として RRI は ドイツ Plattform Industrie 4.0 と IoT・インダストリー4.0 の分野における共通の挑戦への取組みについての情報交換を通じ、シナジーの創出並びに両国の企業及び研究機関の間における協力の促進をめざす。日独間で国を超えたサプラ

イチェーンを構成するパートナ間での信頼を確立してつなげるための具体的方策をNDA に関わらない範囲で検討している。
- 電子調達にメーカの期待する Trustworthiness と、サプライヤの提供できるTrustworthiness をマッチングさせる。
- ドイツ側では EU の標準化を目指してはいない。ドイツ側メンバは必要なものを定め調達に使うというスタンスで、eIDAS（EU の電子取引のための規則）は使える部分のみを使用する。
- 本年 4 月の HANNOVER MESSE でこれまでの検討結果を反映した White Paper を発表する。そのデモシステムについての検討も行われている。

（5） OpenChain Project
- Open Source Software（OSS）を活用するにあたりライセンスの順守が必要である。OpenChain Project は、OSS コンプライアンスをより簡単に、より一貫性のあるものにすることで、サプライチェーン全体にわたる OSS への信頼を築くことを目的として、仕様、カリキュラム、自己認証プログラムを提供する。
- Linux Foundation 傘下の公式プロジェクトであり、国内からはプラチナ会員として富士通、日立、パナソニック、ソニー、東芝、トヨタ自動車が参加。
- 2017 年 12 月にソニー、日立、トヨタが OpenChain Japan WG を設立。
- OpenChain 仕様の中核となる SBOM（Software Bills Of Materials）の第一人者であるアメリカ NTIA（National Telecommunications & Information Administration)のアラン・リードマン氏が 2019 年 10 月の CPS シンポジウムで招待講演を実施している。

表 3-5 MS Azure Sphere

名称	MS Azure Sphere
概要	Azure Sphere とは、IoT（モノのインターネット）デバイスのセキュリティー強化を目的とした総合的プラットフォームである。2018/04発表 Azure Sphereはクラウドサービス「Azure」の一部で、「Azure」と「Azure Sphere」で異なるのはセキュリティである。 Azure Sphereは、次の①～③で構成される。 ①セキュリティで保護されたコネクテッドクロスオーバーマイクロコ ントローラーユニット（MCU） ②カスタムの高レベルLinuxベース オペレーティングシステム（OS） ③継続的で更新可能なセキュリティを提供するクラウドベースのセキュリティサービス(Azure Sphere Security Service) このサービスを使用して、Azure Sphere MCU は安全かつ確実にクラウドや Web に接続する。(802.11 b/g/n Wi-Fiを実装)
	Azure Sphereのソリューションは右図のように三位一体で、構成されている。 ①MCUにはAzure Sphere 認定チップに Microsoft のセキュリティテクノロジが組み込まれ、信頼の高いハードウェアルートが提供される。 ②Azure Sphere OS は、何層もの保護と継続的なセキュリティ更新により、信頼できるプラットフォームとなる。 ③Azure Sphere Security Service は、deviceとクラウドの通信を仲介し、新しい脅威を検出し、デバイスのセキュリティを継続的に更新する。 Azure Sphereのインタフェースボードを実装したIoT機器は、下図のようにインタフェースボードを介し、クラウドに接続したPCを通じてAzure Sphere Security Serviceのサービスを利用する。 インタフェースボードにはMCUとAzure Sphere OSが搭載されている。  https://www.avnet.com/wps/portal/japan/manufacturers/microsoft/azure-sphere/attack-and-security/ 
推進主体・体制等	「Project Sopris」プロジェクトソプリス　2017年3月31日設立 マイクロソフトソプリス委員会
機能	Azure Sphere プラットフォームの主要目的は、マイクロコントローラーを利用した価格重視のデバイスで安全性と信頼性を確保してインターネットに接続できるように、高度なセキュリティを低コストで提供することにある。 Azure Sphere プラットフォームの特徴 1.信頼のハードウェアベースのルート 2.信頼済みの小規模なコンピューティングベース 3.多層防御 4.コンパートメント化 5.証明書ベースの認証 6.更新可能なセキュリティ 7.障害の報告 Azure Sphere Security Service の3つのコンポーネント　別紙＊3参照 1.証明書ベースの認証 2.更新 3.障害の報告
適用分野	新設、既存を問わずクラウド（Azure）に接続可能なデバイスを持つIoT企業。 マイクロソフトのHPで紹介されている企業　→ https://azure.microsoft.com/ja-jp/overview/iot/#trends

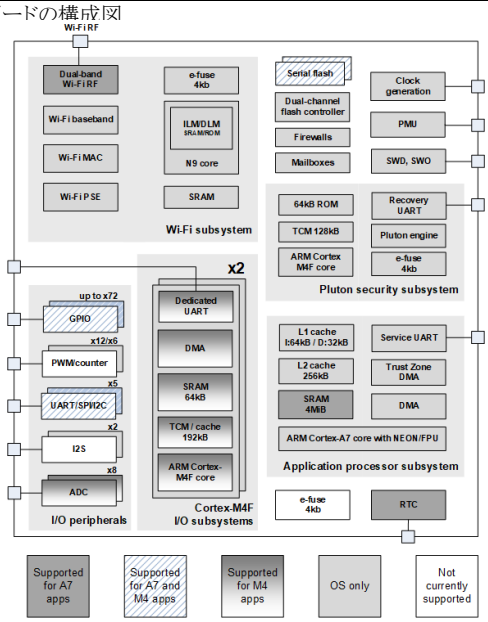
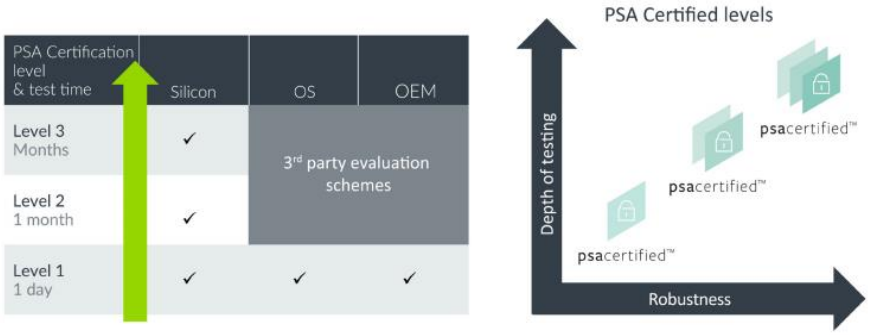
社会実装状況	●現在Azure Sphereの導入事例としてMicrosoftがプッシュしているのは、Starbucks Coffeeのケース。 現在世界80以上の市場に3万店、米国内だけでも1万4000店を抱える。店舗の大きさの大小はあるが、1店舗あたり各種装置が10台単位で存在し、夜間を除く1日16時間体制で稼働している。同チェーンはMicrosoftと提携し、これらマシンにAzure Sphereを導入していくことで合意した。 各店舗には、コーヒーマシン、グラインダー、ブレンダーなどの機器があり、それらが適切に機能していることを確認することが重要である。店舗機器全体で接続されたモノのインターネット(IoT)デバイスにAzure Sphereをデプロイすることで、クラウドに接続されたデバイスのマシンのメンテナンスに費やす時間を短縮している。 コーヒーマシンの稼働状況リアルタイム監視では、8時間で5MB程度のデータが収集される。 ●ドイツの自動車用電線メーカーのLEONI(レオニ)がAzure Sphereを利用したインテリジェント充電システムのデモをCOMPUTEX TAIPEI 2018(6/5～9)で行なった。 ●E.ON は、2019 年の E.ON Home ソリューションのリリースに向けてマイクロソフトと連携し、エコシステム内のすべてのデバイスを Azure Sphere で保護している。
その他	「Azure Sphere 認定 MCU」、「Azure Sphere OS」、「Azure Sphere Security Service」の 3つのコンポーネントが、Azure Sphere の1 つのソリューションとして一括販売される。 Azure Sphere MCU モデル MT3620AN は、968円。 2031年7月までサポートされるOSとセキュリティサービ スの更新プログラムのサポートが含まれる。
MT3620開発キット	Azure Sphereは日本国内ではMT3620開発キットとして販売されている。 国内での販売価格は¥9,800程度。(SKU 102991100 84.90ドル) インタフェースボードは85mm x50mm x16mm, 110g MT3620のアプリケーションは、Windowsパソコン上のVisual Studio 2017を使って開発する。
	開発キット  ボードの構成図  https://docs.microsoft.com/ja-jp/azure-sphere/hardware/mt3620-product-status
	MT3620は、台湾のMediaTek社が開発したAzure Sphere対応に認定されたMCU。 MT3620には、ユーザアクセス可能な最大500MHzで動作するARM Cortex-A7メインプロセッサと、 I/Oサブシステム用の最大200MHzで動作する2つのARM Cortex-M4Fプロセッサが搭載。 さらに、セキュリティとWi-Fi用としてエンドユーザーアプリケーションから分離された ARM Cortex-M4FプロセッサによるPlutonと呼ばれるサブシステムがある。 周辺機能は、GPIO、UART、I2C、SPI、I2S、PWM、ADC、IEEE802.11b/g/n(2.4/5GHz)Wi-Fiを内蔵。 Azure Sphere OSは、あらかじめインストールされており、Azure Sphere Security Serviceと連携してセキュアなIoTプラットフォームを作成するように設計されている。 Azure Sphere Security Serviceの利用が前提となるので、アカウントを取得する必要がある。

表 3-6 PSA Certifed

名称	PSA Certified
概要	Armが2019年2月25日に発表したIoT機器のセキュリティを第三者が認定する制度。Armが提唱するIoT機器のセキュリティフレームワーク「Platform Security Architecture（PSA）」に基づき、チップやOS、デバイスが開発されているかどうかを第三者がテストし認定する。 PSA認定は、Platform Security Architecture framework(PSA)の4番目の「Certify」に該当。 PSAには次の4ステップがある。 1.Analyze ／ 2.Architec ／ 3.Implement ／ 4.Certify
推進主体・体制等	下記の6社（PSA Joint Stakeholder Agreementの構成メンバー） Arm（英）：半導体開発、関連ソフトウェア、IoTプラットフォーム Brightsight（蘭），CAICT（中），Riscure（蘭），UL（米）：世界的に有名なテストラボ Prove&Run（仏）：セキュリティコンサルタント https://www.psacertified.org/about/who-created-psa-certified/
機能 （PSA認定）1/2 https://www.arm.com/why-arm/architecture/platform-security-architecture	PSA認定は、Platform Security Architecture framework(PSA)の4番目の「Certify」に該当。 PSAには次の4ステップがある。 
	PSA認証は、PSAベースのIoTチップ／OS／デバイスのための独立した評価スキーム。 3段階の認証レベルがある。 マルチレベル保証スキームは、デバイスメーカーと企業がユースケースに必要なセキュリティレベルを取得するのに役立つ。  2種類の認証がある。 ・PSA certified Functional API ：PSA開発APIに対するAPI準拠を評価 ・PSA certified ： 堅牢性に対する3段階のセキュリティテスト

機能 (PSA認定)2/2 https://www.arm.com/why-arm/architecture/platform-security-architecture	**PSA certified Functional API** テストキットを使用する個別の認定。PSAベースのソリューションに不可欠なセキュリティ機能の一貫したAPIセットがあり、一貫した実装がなされていることを保証する。 IoT機器に必須のセキュリティサービスの標準化されたアクセスを提供することで、セキュアなアプリケーション開発を容易にする。チップベンダー／RTOSプロバイダー／機器メーカーに対し、最新のハードウェアセキュリティ機能を利用するためのテスト群を無償で公開する。
	PSA certified IoTプラットフォームの一般的な3つの構成要素の第三者検証を行う。 3つの構成要素：ROT(Root of Trust)／RTOS(リアルタイムOS)／ デバイス本体 ・psacertified level one チップベンダ／OSサプライヤ／OEM向け 重要なセキュリティの質問のセット。開発者が回答し、テストラボで確認する。 PSAアーキテクチャドキュメントの10のセキュリティモデル目標を使用し、セキュリティ機能の評価を通じて一般的なセキュリティ問題をキャッチすることを目的としている。 アンケートをダウンロードして記入し、パートナーのテストラボに連絡してインタビュースタイルの評価を行う。 ・psacertified level two チップベンダー向け PSA-RoTと呼ばれるチップ内の信頼できるドメインのラボベースの評価。リモートソフトウェア攻撃やライトウェイト・ハードウェア攻撃の一般的なIoT脅威から保護する必要があるシステム向けに設計されている。PSA-RoT保護プロファイルに対する25日間のラボベースの評価が含まれ、この期間限定の評価によりスキームは手頃な価格で効率的になる。 ・psacertified level three チップベンダー向け PSA-RoTのラボベースの評価(開発中)、ソフトウェアおよびハードウェア攻撃からの保護。かなりのレベルの堅牢性と保証を提供。サイドチャネルや物理的な改ざんなどのより広範な攻撃をサポートする予定。 
適用分野	IoTソリューション開発、デバイスメーカ:さまざまな組織に、適切なセキュリティレベルを持つシリコンやデバイスを購入しているという保証を提供 IoT向けの安全なチップとデバイスの構築は簡単ではない。 PSA Certifiedのドキュメント、成果物、およびテストスキームは、エレクトロニクス業界にとってより簡単で迅速かつ手頃な価格になるように設計されている。
社会実装状況	Level Oneの認定:Cypress、Express Logic、Microchip、Nordic Semiconductor、 Nuvoton、NXP、STMicroelectronics、Silicon Labs Level One ＋ PSA Functional API Certification :Nuvoton、ZAYA、Arm
その他	PSA Certified https://www.psacertified.org/ PSA Certified Overview https://www.psacertified.org/about/ PSA Certified: Building Trust in IoT – arm https://www.arm.com/company/news/2019/02/psa-certified-building-trust-in-iot

表 3-7 IETF CBOR

名称	CBOR (Concise Binary Object Representation)
概要	IETFのART (Applications and Real-Time Area) のWGで標準化が進められている、IoT機器など計算リソースに制約がある環境に適したデータ表現形式。JSONフォーマットをバイナリ形式で表現したもの。RFC7049で規定。現在、Standards Track のPS(Proposed Standard)であるが、既にセンサ等IoT機器ネットワークの開発プラットフォームや、各種クラウドサービスにおけるIoTネットワークサービス、さらには各種認証システム等において社会実装が進んでいる。
推進主体・体制等	・IETFで策定。RFC作成の中心人物はブレーメン大学Center for Computing Technologies (TZI)のCarsten Bormann氏(CoRE WGのChairでもある) ・どこか特定のベンダ等の企業が中心的に推進しているということはなさそうな模様
機能	・CBORの目的 1. インターネット標準で一般に利用されているデータフォーマットを明確にエンコード 2. メモリ、CPUパワー、命令セットに制約のあるシステムでの実行をサポートするために、エンコーダ/デコーダをコンパクトに実装可能 3. JSONと同様にエンコードされたデータは自己記述的であり、スキーマ記述なしにデコード可能で、バージョンネゴシエーション等を必要としない 4. シリアライゼーションを合理的にコンパクト化。なおデータサイズのコンパクト性よりもエンコーダ/デコーダのコードのコンパクト性の方がより重要 5. 制約のあるノードと、大量のデータを扱うアプリケーションの両方に適用可能 6. JSONで扱う全てのデータ型を変換可能 7. データフォーマットは拡張性かつ下位互換性を保有 ・CBORデータフォーマット - CBORで表現可能なデータは、整数、バイナリ、テキスト(ASCII, UTF-8)、Array/Map、浮動小数点/多倍長整数、true/false/null/undefined、日付日時等、一通りのデータフォーマットをサポート - 最初の1byteが型を示し、それに続く0～N byteが実際の値を表現 - 型は、Major Type0～7の大きく8種類あり、さらに各Major Typeが細かく分類 Major type 0: 符号なし整数(unsigned integer) Major type 1: マイナス数値(negative integer) Major type 2: バイト文字列(byte string) Major type 3: テキスト文字列(text string) Major type 4: 配列(array) Major type 5: マップ(map, JSONだとobject) Major type 6: 拡張用のオプション領域、日時型、多倍長整数、固定小数点等 Major type 7: 浮動小数点(floating-point numbers)、真偽値、Null、Undefinedも定義
適用分野	・CPU、メモリ等限られた計算リソースのIoT機器での処理に適している。また計算リソースの効率的利用に加え、IoT通信費用の削減にも寄与する。 ・また、パスワードレス認証技術の策定を進めるFIDO(Fast IDentity Online)アライアンスで検討されている認証に関する技術、COSE(CBOR Object Signing and Encryption)、CTAP(Client-to-Authenticator Protocol)、CWT(CBOR Web Token)にも鍵情報やメッセージデータのバイナリエンコード方式としてCBORが採用されている。
社会実装状況	・Python, Javaなど様々な言語で、Apache 2.0 やMITライセンスのオープンソースのライブラリが存在する。また、IoT機器に対する開発キット等(ex. AllThingsTalk)でもCBORのサポートが進んでいる。 ・AWS、Alibaba CloudでのIoT向けクラウドサービスで、AWSではMQTT、AlibabaではCoAP, MQTTの双方でCBOR形式のデータをサポート済。なお、Google、AzureではMQTTをサポートしているが、CBORデータ形式については未サポート。 ・FIDO認証関連技術については、現在、Chrome(Android含む)、Edge等のブラウザやSNSアプリ等で実装が進行中 ・oneM2Mでも2016年8月公開のリリース2より、シリアライゼーション方式にCBORが追加
その他	IETF RFC7049(CBOR) https://tools.ietf.org/html/rfc7049 CBOR http://cbor.io/

3.3　具体的な実証実験計画の提案

3.3.1 実証実験と社会実装に向けたパートナ調査

CPS の研究開発成果の実用化・事業化を促進するための新たな実証実験の場の開拓を行うために、研究開発成果の利用者と位置付けられるサプライチェーンの調査を行い、中小企業を含む CPS の適用先の拡大と実証実験の実施の検討に用いる情報収集を行った。情報収集のために、産業分野、サプライチェーンの形態、研究開発テーマとの関連性、中小企業の存在、調査可能性を重視することとして、サプライチェーンの一次調査の結果に対するサブワーキンググループの検討において４件のサプライチェーンを、面談調査を前提とした深堀調査の対象として選定した。面談調査における深堀調査項目については、深堀対象として選定した各サプライチェーンに対して研究開発テーマが求める確認項目を確認し集約することによって表 3-8 に示す内容を定めた。

表 3-8 サプライチェーンの調査項目

サプライチェーンの特徴	ビジネス内容／活動目的	サプライチェーンの目的
		サプライチェーンが扱うもの（流通しているもの）
		サプライチェーンの構成、ビジネスの工程とフロー
	サプライチェーンシステム	サプライチェーンの利用者、利用形態
		サプライチェーンの管理者／運営者／活用推進主体者
		サプライチェーンで取引されている金額
		サプライチェーンの運用コストとその負担者
	その他	
サプライチェーンの課題とサプライチェーンを取り巻く状況の変化		現在の運用状況、今後の計画
		サプライチェーンのリスクの有無、リスクの所在
		解決したい課題
実証実験と研究成果の適用に関する項目		CPS の成果と CPS 基盤への期待
		CPS 実証実験が行われる際の参加希望と条件

また、初回の直接訪問となる面談調査時に SIP 及び CPS の活動目的と研究開発内容の紹介に用いる資料として表 3-9 の資料を準備した。付図 C に示すサプライチェーンにおけるサイバーセキュリティリスクの資料はサイバー・フィジカル・セキュリティの重要性を具体的に説明するために、公開されているセキュリティインシデントの例を含むものとした。

表 3-9 深堀調査用説明資料

目的	資料	
SIP 紹介	戦略的イノベーション創造プログラム（ＳＩＰ） 概要 ／ 内閣府 政策統括官（科学技術・イノベーション担当）	https://www8.cao.go.jp/cstp/gaiyo/sip/sipgaiyou.pdf
	SIP（第 2 期）研究開発計画の概要　平成 30 年 8 月 内閣府政策統括官（科学技術・イノベーション担当）	https://www8.cao.go.jp/cstp/gaiyo/sip/kenkyugaiyo2.pdf
	SIP とは	https://sip2019.go.jp/about/
CPS 紹介	戦略的イノベーション創造プログラム（SIP） IoT 社会に対応したサイバー・フィジカル・セキュリティ	https://www8.cao.go.jp/cstp/gaiyo/sip/keikaku2/3_iot.pdf
	SIP「IoT 社会に対応したサイバー・フィジカル・セキュリティシンポジウム」 プログラムの概要紹介（プレゼン資料）	SIP「IoT 社会に対応したサイバー・フィジカル・セキュリティシンポジウム」 https://www.sip2-cyberphysicalsecurity.org/
	同上 展示内容紹介リーフレット	
解説	サプライチェーンにおけるサイバーセキュリティリスク（ホラーストーリ）	付図 C サプライチェーンにおけるサイバーセキュリティリスク

深堀調査の対象としたサプライチェーンとの面談調査を通じて得られた情報を以下に示す。

(1) CPS プロジェクトが目指す研究開発の背景や目的について各サプライチェーンの認知を得ることができた。しかし、各サプライチェーンにおいて CPS の研究開発成果を活用する方法や時期等についてのイメージを持っていただくまでには至っていない。

(2) 各サプライチェーンの概要についての情報を入手することができた。しかし、サプライチェーンの現在の運用状況、セキュリティ上の課題、計画などに関するより詳細な情報の入手については不十分である。

(3) 各サプライチェーンやそれらのシステムにおいて情報セキュリティの重要性は認識されている。しかし、その対処が十分であるとは考えていない。

(4) システムやサプライチェーン全体にわたる CPS のリスクについての認知は十分ではない。

(5) ビジネスの拡大のきっかけとするため、サプライチェーンのシステム化やセキュリティ強化に関する施策等に対しての期待がある。

(6) 実証実験の実施時期や参加方法について興味をもっているサプライチェーンがある。

上記は各サプライチェーンに対する 1 回の面談による深堀調査の状況であり、実証実験の検討と社会実装に向けた参考となるより詳細な情報の入手には調査の継続が必要である。

調査においてサプライチェーンから情報を入手するには、CPS からもより具体的な情報の提供が必要であり、次の点についての準備を整えることにより、継続調査をより効果的なものとすることができると考えられる。

- サプライチェーンに合わせた研究開発テーマ内容の紹介
- 深堀調査への研究開発テーマの担当者の参加
- 研究開発テーマ担当者によるサプライチェーンの課題確認
- 実証実験計画の具体化
- サプライチェーンに提供する情報と、情報交換のためのルール作り

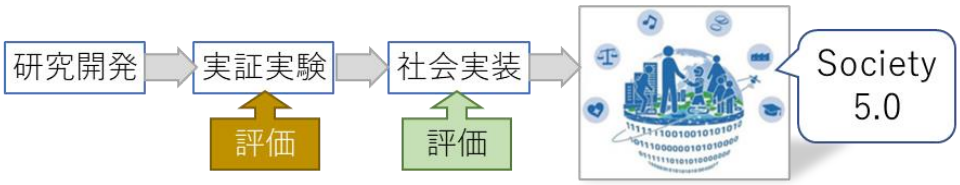
3.3.2 実証実験の評価軸

CPS プロジェクトの研究計画では研究目標として下記の面からの目標を掲げている。研究目標には研究開発成果の直接的なアウトプットではなく、研究成果が社会に展開されたときの、アウトカムとして達成されるものが含まれていることから、実証実験を通じて直接的な評価を行うことは難しい。

- 社会面
- 産業面
- 技術面
- 制度面
- グローバルベンチマーク
- 自治体等との連携

図 3-4 に示す研究開発成果の実証実験の着手前の現段階においては、CPS プロジェクト目標に対する活動として、目標を実現するためのロードマップを研究開発のビジョンとして示すこととする。そして実証実験の評価項目は、実証実験への参加者となるサプライチェーンが利用者の視点で実証実験に求める評価観点から定めることとし、実証実験においては評価観点に対する技術的目標の達成度合いを測るものとした。また、CPS プロジェクトでは多様な研究開発テーマを含むことから、実証実験においてテーマ間で共通的に使うことのできる評価観点を評価軸として定めた。このため、CPS の採用を判断する際の経営者の立場からの CPS に対する評価観点を各研究テーマに問い合わせて抽出し、SIP 1 期の開発とその実証実験で得られた知見に基づき 5 項目の評価軸に再編した。

実証実験の評価においては、各テーマの研究開発内容と開発フェーズに応じて、共通の評価軸に対応する評価項目を定めるものとした。各研究開発テーマが実証実験において確認を行う技術的目標によって、評価軸に対する評価項目の詳細化レベルが異なってもよい。また、各研究テーマの実証実験の内容によって、評価軸に対する評価項目の設定を行わない理由を明らかにして評価項目を定めないことも可能とした。



Society 5.0 - 科学技術政策 （内閣府）
https://www8.cao.go.jp/cstp/society5_0/ を加工して作成

図 3-4 CPS の研究開発ステップ

3.3.3 動向調査の実施と情報共有のための環境整備

今年度調査を開始した CPS と関連するシステム、およびサプライチェーンについては調査の継続が必要である。これらの動向は短期間で状況が変化することが想定されるため、動向調査状況等を把握し、実証評価ワーキンググループのメンバ間でタイムリーに情報を共有して CPS の実証実験の実施計画の検討に反映する必要がある。このためには実証評価ワーキンググループの全メンバ間で情報を共有し、適宜 CPS 関係者も参照することができる環境構築が有効である。また、調査に伴って入手した資料についても、情報共有のための環境に格納して一元管理することにより、情報への参照を効率化する。

情報共有のための環境整備にあたり、情報共有サービスを利用する場合には以下を考慮する必要がある。

- セキュリティの担保：アクセス権設定・管理等の機能が充実し、実績のある企業向けサービスから選定
- 実際に利用する人数（ID 数）、管理するファイル容量の見積り：適した料金体系のサービスを選定
- ワーキンググループメンバ各組織の組織内ネットワークからのアクセス可能性の担保：各組織内ネットワークにおいてアクセス制限されていないことの事前確認
- 契約形態、契約の引継ぎの可否等の確認：長期的な利用が想定されることから、情報の移管、もしくはサービス契約者の変更の可否

3.3.4 NEDO 主催の会合への参加と体制の構築

CPS プロジェクトの実施者との具体的な実証実験の計画を協議するために、NEDO 主催の成果普及ワーキンググループと、そのサブワーキンググループにオブザーバとして参加して検討状況の確認を行った。成果普及ワーキンググループで 2019 年 10 月 31 日に開催され

た CPS シンポジウム[4]の開催と運営、CPS に関するアンケート調査に協力した。また、成果普及ワーキンググループで設計を行っている CPS の成果普及のためのロードマップの具体化のために、実証評価ワーキンググループで深堀調査を継続し、その結果を参考情報として成果普及ワーキンググループに提供することを提案した。

PD との会合を通じで実証評価ワーキンググループの開催と、そのサブワーキンググループの体制と運営について確認を行い、実証評価ワーキンググループの主査を通じてサブワーキンググループに展開を行なった。この一環として 3.2.3 に述べた CPS 関連活動の調査を実証評価サブワーキンググループに提案して結果を実証評価ワーキンググループに報告した。

3.3.5 実証評価ワーキンググループの運営

実証実験計画についての議論の場として CPS プロジェクトに設置された実証評価ワーキンググループと、実証実験の検討のための動向調査の方針を定め実証実験に向けての検討を行う実証評価サブワーキンググループの運営を行った。両ワーキンググループの開催にあたっては、事前に実証評価ワーキンググループ主査に会議開催の準備状況を報告して議事進行等を確認することにより、会議開催が実効的なものとなるようにした。

実証評価ワーキンググループとサブワーキンググループの開催状況を表 3-10 に示す。

表 3-10 実証評価ワーキンググループの活動

会議	開催日	議題
第1回 実証評価 WG†	2019/7/21	WG 開催目的、参加者との役割
実証評価サブ WG 第 1 回	2019/8/20	WG の活動目標 調査方法(評価軸、サプライチェーン) 先行調査状況
第2回 実証評価 WG	2019/8/29	WG の活動目標、調査内容と進め方
実証評価サブ WG 第 2 回	2019/9/25	サプライチェーンの一次調査状況 CPS 関連活動調査状況報告 今後の調査の進め方
第3回 実証評価 WG	2019/10/3	サプライチェーンの一次調査報告 CPS 関連活動調査報告 調査の進め方
実証評価サブ WG 第 3 回	2019/11/5	サプライチェーンの深堀調査対象の選定 深堀調査項目の設定

[4] SIP 「IoT 社会に対応したサイバー・フィジカル・セキュリティ」 シンポジウム 2019 https://www.nedo.go.jp/events/IT_100048.html

実証評価サブ WG 第 4 回	2019/11/18	サプライチェーンの深堀調査項目 深堀調査用の CPS 説明資料 深堀調査状況 実証実験の評価軸調査状況と今後の調査方針
実証評価サブ WG 第 5 回	2019/12/18	CPS 関連の追加調査(RRI, OpenChain) 深堀調査実施状況と追加調査 評価軸の設定 実証評価 WG の活動報告の作成
実証評価サブ WG 第 6 回	2020/1/17	CPS 関連活動の追加調査(RRI)
実証評価サブ WG 第 7 回	2020/1/27	CPS 関連の追加調査報告(RRI, OpenChain) 深堀調査の追加調査 実証評価 WG の活動報告
実証評価サブ WG 第 8 回	2020/2/3	深堀調査(ビルシステム)
実証評価サブ WG 第 9 回	2020/2/12	実証評価 WG の活動報告について
第4回 実証評価 WG	2020/2/20	動向調査状況報告と今後の進め方 実証実験の評価軸の設定

† WG:ワーキンググループ

3.4 実証実験の促進に係る課題

3.4.1 動向調査の実施と情報共有のための環境整備

今年度調査を開始した CPS と関連するシステム、およびサプライチェーンについては、実証実験の検討のためにより詳細な情報を入手するために調査を継続することが必要である。また、これらの動向は短期間で状況が変化することが想定されるため、動向調査状況等を実証評価ワーキンググループのメンバ間でタイムリーに共有し、CPS の実証実験の実施計画の検討に活用する必要がある。このためには 3.3.3 で述べた動向調査の管理と調査情報を共有するための環境を早期に整備することが重要である。

3.4.2 実証実験計画の具体化

今年度調査を開始したサプライチェーンの動向については、より詳細な情報の入手に調査の継続が必要であり、継続調査においてサプライチェーンから情報を入手するには、CPS からも具体的な情報の提供の必要となる。このためには実証実験の計画の具体化と、CPS の公開情報に加え調査のためにサプライチェーンに提供する情報の準備と、提供情報の守秘管理のためのルール作りが求められる。

3.4.3 ワーキンググループ間の連携強化

CPS プロジェクトの研究開発のために表 3-11 の 3 つのワーキンググループが設定され、研究開発と並行してテーマ横断的な課題の解決を図るための活動をワーキンググループで行ってきた。また、ワーキンググループ間の連携活動として、成果普及ワーキンググループの CPS シンポジウム開催への協力と動向調査情報を活用する提案を行った。

ワーキンググループ間の連携を一層推進することにより、CPS プロジェクトの成果普及方針を実証実験の計画に反映させ、他国のプロジェクト等を含めた実証実験計画を拡充し、実証実験の評価結果を成果普及において有効に活用する活動を、セキュアな Society 5.0 の実現に向けて提案する。

表 3-11 CPS に設置されたワーキンググループ

1. 実証評価ワーキンググループ ・ 実証実験において実用性や実効性を効果測定する手法を調査・検討するとともに、実証実験パートナ候補と共同検討し、実証実験を進めるテーマ間で共有する。 ・ SIP 課題間、他の国プロ等と連携した実証実験を検討（外部向け窓口の役割）する。
2. 成果普及ワーキンググループ ・ 参画企業による事業化(製品化)と各産業分野へ導入推進する(知財委員会と連携)。 ・ 共用検証センター（自主評価用）等、中小企業などが成果を活用し易い環境を立上げる。 ・ 本取り組みの海外発信のために、国際シンポジウムを企画・開催する。
3. 海外動向調査ワーキンググループ ・ 各テーマで実施する国内内外の関連動向調査状況を集約し、プロジェクト全体で共有する。 ・ 国際連携活動として米国 NIST，欧州 ENISA 等へ積極的な提言活動をとりまとめる。

結び

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会である Society 5.0 をセキュアに実現するための研究開発プロジェクト「IoT 社会に対応したサイバー・フィジカル・セキュリティ」を実施している。この研究開発成果の実証事実験を効果的に行うための情報収集、及び実社会での実装における課題抽出として、①実証実験計画提案のための動向調査、②具体的な実証実験計画の提案、③実証実験の促進に係る課題の抽出を行った。

動向調査としては、実証実験の評価軸設定のための調査、サプライチェーンの状況把握のための調査、サイバー・フィジカル・セキュリティの関連活動調査を実施し、調査の途中経過を含めて実証評価ワーキンググループに報告することにより、調査の方向性の確認と有効活用を行った。

実証実験計画の提案とその関連活動としては、実証実験の評価軸の設定、サプライチェーンの深堀調査の実施継続、動向調査の管理と調査結果の活用のための情報共有環境を提案した。また、実証評価ワーキンググループとその作業部会である実証評価サブワーキンググループの開催に係る運営を行った。

実証実験の促進に係る課題としては、動向調査の管理と調査結果の活用を行う情報共有環境の構築、サプライチェーンの深堀調査のための実証実験の具体化、サイバー・フィジカル・セキュリティ・プロジェクトに設置されたワーキンググループ間の連携の強化の 3 件の課題を抽出し、これらの必要性を述べた。本年度の調査事業で入手した情報を活用し、実証実験の計画検討をより具体的に推進するために、次年度において調査事業を継続し進展させることを提案する。

付表・付図

付表 A 一次調査対象のサプライチェーン

ID	サプライチェーン	概要	出典
a.	自動走行ビジネス	トラックの隊列走行、ラストマイル自動走行、自動バレーパーキング等を含む自動走行技術を適用したMaaSを実現するためのサプライチェーン。 車両関連やセンサ等のハードウェア、認識・判断・制御等のソフトウェア、ダイナミックマップ等のデータ、通信機能、インフラ側機能等非常に多種多様な構成要素に対するサプライチェーンが必要となる。	(a1)https://www.meti.go.jp/shingikai/mono_info_service/jido_soko/pdf/20190626_02.pdf (a2)https://www.meti.go.jp/shingikai/mono_info_service/jido_soko/pdf/sanko_03.pdf (a3)https://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/pdf/001_05_00.pdf (a4)https://www.shinnihon.or.jp/corporate-accounting/industries/basic/automotive/2010-07-05-01.html
b.	エッジコンピューティングを用いたスマート工場	製造業のサプライチェーンにおいて、エッジコンピューティング技術を核としたFA-IT 連携による工場のスマート化に関する実証事業。複数工場にまたがる「生産管理・設備稼働監視」(部品加工～サブ組立～最終製品組立の 3 工場にまたがるサプライチェーンを想定)のユースケースを想定し、エッジと IT システムを連携した設備の「予兆保全」による稼働ロス低減効果を確認。	(b1)https://prtimes.jp/main/html/rd/p/000000007.000031239.html (b2)https://www.jmfrri.gr.jp/content/files/Open/2019/20190807_SWG7/20190807_WG1-SWG7.pdf
c.	医薬品関連 5 社によるサプライチェーンでの RFID 活用	医薬品に関する、資材メーカー～製薬メーカー工場～物流センター/卸～調剤薬局/病院～医薬品服用者の一連のサプライチェーンにおいて、RFID 技術を活用し、在庫管理業務等の効率化や偽造防止のためのサプライチェーン全体に渡るトレーサビリティの確保等の実現に向けた取り組み。2020 年度の実用化が目標。	(c1)https://www.microtechnica.co.jp/dcms_media/other/医薬品のサプライチェーンを RFID で変える仕組みを 5 社で共同開発.pdf

d.	防衛装備品に関するサプライチェーン	防衛省・自衛隊が運用する防衛装備品におけるサプライチェーン。防衛産業は多種多様な産業分野を含む複合産業であり、また防衛省と直接契約を結ぶプライム企業及び当該プライム企業と契約を結ぶ多数のサプライヤ企業からなる多層構造を形成。 近年、このサプライチェーンにおいて、グローバルな調達が進み、それに応じて情報流出リスクの高まり、また外国資本による日本企業の買収に伴う粗悪品・スパイウェア等の混入リスクの高まり等の懸念が発生	(d1)https://www.mod.go.jp/j/approach/agenda/meeting/bouei_gijutsu/sonota/03_a.pdf
e.	ファームコンプレックス研究開発プラットフォーム	施設型第1次産業の技術?新と、様々なデータベースを統合活活用する高度な情報の連携を進めることにより、①国内の第1次産業の生産効率化、②バリューチェーンの整備・強化による海外収益の拡大、③技術ライセンスやコンサルティング等の新ビジネスの創出（第6次産業化）などを推進するための Society 5.0 に基づく研究開発活動	(e1)https://www.knowledge.maff.go.jp/platform-case-2018/02.html (e2)https://www.knowledge.maff.go.jp/uploads/casebook_rev1808el.pdf
f.	ハラール製品に関するサプライチェーン	ハラール製品に関する原材料から小売事業者まで流通全体におけるサプライチェーン。ハラールとは、イスラム法上で「合法的なもの」を意味し、食品、薬、化粧品等多岐に渡り、最終製品がハラールであることを認証するためには、原材料は当然ながら、流通経路のサプライチェーン全体においてハラール準拠が必要。	(f1)https://www.murc.jp/wp-content/uploads/2017/03/global_1703.pdf (f2)http://www.maff.go.jp/j/shokusan/export/e_kikaku/pdf/5c01.pdf (f3)https://www.j-smeca.jp/attach/kenkyu/honbu/h26/halalshokuhin.pdf (f4)http://www.maff.go.jp/tohoku/kihon/yusyutu/kyougikai/pdf/tanaka-siryou.pdf
g.	大手ビール４社の共同輸配送	ビール大手4社でのビールの共同輸配送による効率化の取り組み。ビール配送において鉄道コンテナの相乗りなど共同配送を全国各地で推進。規格化されているパレットの回収も 4 社で協力し全体最適化することで、トラック輸送に伴う CO2 削減やドライバの労働時間削減を実現。	(g1)https://www.sankeibiz.jp/business/news/181029/bsd1810290500002-n1.htm (g2)http://cargo-news.co.jp/cargo-news-main/464 (g3)https://www.dsri.jp/forum/pdf/2018_beergroup.pdf

h.	食品製造加工6社の共同輸配送	大手加工食品メーカが連携し、主に共同配送の実現による物流の生産性向上を推進。従来の各社系列のロジスティクス会社を統合し、共同輸配送のための会社を設立。	(h1)http://www.t-renmei.or.jp/info/pdf/forum_1th_01.pdf
i.	直接販売等の新たな流通経路	水産物の流通に ICT を活用し、サプライヤである漁業者とバイヤである飲食店等を直接仲介するサービス。全国の漁業者の情報を集約し、スマホ等を介して飲食店にタイムリーで分かりやすい情報提供を実現。	(i1)https://foodison.jp/service/
j.	全コンビニ商品への無線タグの取り付け	大手コンビニ5社において、基本的に全ての商品に RFID を取り付け、商品の個品管理を実現するとともに、RFID により取得した情報の一部をサプライチェーン全体で利用可能とすることで、製品製造や物流の効率化を目指す取り組み。	(j1)https://www.meti.go.jp/press/2017/04/20170418005/20170418005-1.pdf (j2)https://www.meti.go.jp/press/2017/04/20170418005/20170418005-3.pdf (j3)https://www.meti.go.jp/press/2017/04/20170418005/20170418005-2.pdf
k.	OSS を含むソフトウェア管理手法	CSPF に基づくセキュリティ対策の具体化・実装の推進の一環として、検討が開始された OSS を含むソフトウェア管理手法。 CPSF では、機器の正規品確認を目的としたソフトウェアの真正性の確認や、脆弱性の確認を実施することを要求する一方、ソフトウェアの複雑化、OSS の利用拡大などに伴い、ソフトウェアそのもののセキュリティをどのように維持し続けるのか、それをどのように確認するかについての明確化は未実施	(k1)https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/001.html (k2)https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/001_02_00.pdf (k3)https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/001_04_00.pdf
l.	スマートホームサービスにおけるサプライチェーン	IoT や AI 技術等を駆使し、様々なライフスタイルの住人に対し、安心/安全/快適な暮らしを実現するスマートホームサービスを提供するためのサプライチェーン。住宅デベロッパー、住設機器メーカ、家電・ヘルスケア機器メーカ、通信事業者、サービス事業者及び情報連携事業者(プラットフォーマー)からなる多層的なサプライチェーンを構成	(l1)https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/003_03_02.pdf (l2)https://www.jeita.or.jp/japanese/pickup/category/doc/190314_item_definition_v1.0_201903r.pdf (l3)https://www.fcr.co.jp/pr/18096.htm

m.	ビルシステムのサプライチェーン	ビルシステムサービスを提供するためのサプライチェーン。ビルシステムにおいては、設計/施行から運用保守に渡るライフサイクル全般において、ビルオーナー、ゼネコン/サブコン、設計事務所、個別システム事業者(ビル管理システム、空調、エレベーター、ビデオ監視、電力・熱供給 等)、ビル管理会社、テナント、サービスプロバイダといった多様な事業者からなるサプライチェーンを形成。従来は各システムが非 IP ネットワークで独立していたが、近年 IP ネットワークによるシステム間連携等が進み、これにより従来になかったようなサイバーセキュリティリスクの懸念が発生	(m1)https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/pdf/001_gijiyoshi.pdf (m2)https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/pdf/20180903_01.pdf (m3)https://www.fuji-keizai.co.jp/market/detail.html?cid=16081&view_type=2
n.	個人への健康医療情報管理プラットフォーム	個人によって管理された健康医療情報を、本人の意思に基づき活用できるようにして、健康的な生活を支える新たなヘルスケアサービスの創出を支援するためのプラットフォーム	(n1)https://tech.nikkeibp.co.jp/dm/atcl/feature/15/327441/021400611/?ST=health (n2)https://pr.fujitsu.com/jp/news/2019/02/13.html
o.	Daigas グループ（大阪ガス）のバリューチェーン	都市ガスにおいて、原料調達などの上流側から、販売先を含めた下流側までを含めた一連の流れ。都市ガスの安定供給、お客様の安心安全の確保、事業領域の拡大などの取り組みを強化。	(o1)https://www.osakagas.co.jp/company/csr/charter01/safety01.html#1 (o2)https://www.osakagas.co.jp/company/csr/beginning/valuechain.html (o3)https://www.osakagas.co.jp/company/csr/charter01/safety03.html#0
p	ニアショア開発	ニアショア開発とは、オフシュア開発のデメリットを補うため、同じ日本国内で比較的人件費が安価な地方都市の事業者に委託しソフトウェア開発を行う形態	(p1)https://www.nce.co.jp/service/near-shore/

付表Ｂ１ データ利活用型スマートシティ推進事業の評価項目

評価項目	
経済	・失業率 ・一人当たり付加価値額
教育	・初等教育におけるプログラミング教育履修者数 ・課題発見／解決型の学習にICT活用が有効と実感す る教師の割合
エネルギー	・住民1人当たり電力の年間消費量 ・公共施設における再生可能エネルギー導入割合
環境	
消防・非常 事態対応	・住宅火災による死者（高齢者数） ・土砂災害から保全される流域人口
行政	・オープン化しているデータセット数 ・オープンデータを活用した行政サービス数 ・住民サービスに対する住民満足度の向上度
医療療・健康	・平均寿命 ・10万人当たりの病床数 ・要介護度別の人数
レクリ エーション	・無料公衆無線LANの利用可能面積 ・訪日外国人旅行者がコミュニケーションで困難を感じる割合
安全	・犯罪発生件数 ・安心して子育てができる環境が整っていると考える 住民の割合
通信	・Wi-Fiの整備状況 ・10万人当たりのスマートフォン加入者数 ・LTE不感地域
交通	・渋滞による損失時間 ・交通事故死傷者数 ・後期高齢者の年間外出回数
都市計画	・住民一人当たりの緑地面積 ・30分以内に中心市街地にアクセス可能な居住人口の 割合
上下水処理	・スマート水道メーターの導入率 ・漏水による損失の削減 ・浄水施設の耐震化 ・震災時の運転管理

付表Ｂ２ 横浜スマートシティプロジェクト（YSCP）の評価項目

評価項目／結果		
CEMS	・需給調整用蓄電池群を仮想電源とした LFC(周波数制御)機能の実証	・北米 PJM 市場の周波数調整（FR）指令値で一カ月以上 LFC 連続試験実施
	・多くの蓄電池の余力だけを仮想電源として電力利用制約不要の DR 実証	・蓄電池余力だけでピークシフト、PV 余剰電力対策の DR 計画 97%以上実現
	・需給調整用蓄電池群を仮想電源とした瞬動予備力機能の実証	・系統緊急時に需給調整用蓄電池が瞬動予備力供給を実証
EMS	・太陽電池・蓄電池の自動制御によるデマンドサイドマネジメント(DSM)	・48 戸での DSM 実証にて電力削減：平均 14%／自家消費率：平均 75%を実現
	・太陽電池・蓄電池の自動制御によるデマンドサイドマネジメント(DSM)	・約 2,100 戸へ B ルートを構築、DR 実証にてピークシフト効果 15%を実現
	・HEMS と CEMS の連携による地域エネルギーマネジメント	・CEMS からの DR に連動した蓄電池の自動制御によるピークカットを実証
	・HEMS 機器・サーバ機能の開発・実証	・戸建住宅向け蓄電池最適充放電制御 蓄電池スケジュール制御に対する電気料金収支向上（冬季）PV 設置宅 4 円／日 PV,FC 設置宅 11 円/日
	・集合住宅向け MEMS の開発・実証	・CO2 削減効果（H24 年度から H26 年度 共用部）JXE 所有社宅：平均 25.3±1.7 %、 パークホームズ大倉山：平均 18.4±1.3 % ・DR 効果（DR が行われた時間帯の共用部電力量の、DR が行われない日との比較）JXE 所有社宅： 夏季 平均 21.2% 冬季 平均 20.2%の電力削減、 パークホームズ大倉山： 夏季 平均 5.0% 冬季 平均 8.2%の電力削減
	・専有部（各住戸）エアコン ADR 実証	・ADR 実証結果（パークホームズ大倉山 2013 夏,冬, 2014 夏,冬 専有部エアコン消費電力）DR 効果 最大 23.0%、応答性 最大 29.9%（DR 開始前後の DR 効果の変化）
	・集合住宅において①再生可能エネルギー（PV、太陽熱）、燃料電池、蓄電池（充放電 EV 含む）を複数戸で シェアし、②電力・熱エネルギーの住戸間融通、③HEMS 等居住者の行動変化を促す手法を試行し、省エネ・ ピークカット貢献等	・住棟全体で約 38%の CO2 削減を達成し、HEMS による省エネ行動では 7%の一次エネ削減を達成 燃料電池を活用したデマンドレスポンスへの対応で最大 58%の系統負荷抑制を実現 ・EV・蓄電池の充放電状況など各種フィールドデータを取得し、集合住宅における EV 急速充電器利用時のデマンド抑制効果を確認
	・複数の蓄電池を一元管理し、複数の需要家で共同利用する「蓄電池シェアリングシステム」を開発・運用し、 蓄電池の可用性向上・長寿命化の観点で評価	・蓄電池の一元管理および共同利用を実現し、共同利用による蓄電池の可用性向上および長寿命化を確認
	・省エネ効果の実証 ※HEMS 導入により、各家庭で本実証前よりも省エネ効果 10%、DR 効果 5%の目標を達成する	・2013 年夏季・冬季 2014 年夏季ともに、本実証前に比べ、目標とした省エネ効果を達成 ・実証を通し 14.5pt の割合で節電意識が向上、継続により「常に節電を意識している」が 11.4pt 増加
BEMS	・フェーズ 1：ビル部門における最大限のピークカット効果を実証 ・フェーズ 2：安定した目標達成効果を実証	・フェーズ 1：PTR 方式によるデマンドレスポンスで、最大ピークカット 22%達成 ・フェーズ 2：削減目標に対して各拠点毎の平均で 9 割超の削減を達成
	・蓄熱と給電を連携させて十分な調整余力を備えたビル向け実証システムを構築し、デマンドレスポンスを含めたエ ネルギー利用の全体最適化。 ピークシフト/ピークカット効果率目標 最大 20%（ベースライン比）	・フェーズ 1：ＰＴＲ方式：冬期 22.9%, 夏期 28.7% ・フェーズ 2：ＣＣＰ方式：冬期 23.2%, 夏期 23.3%
	・スマート BEMS の開発 ・定置用大型リチウムイオン蓄電システムの開発	・複合エネルギーシステムの構築 ・スマート BEMS による統合制御によってエネルギー供給設備運転の適正化が図られ従来制御方式に比してエネルギー利用効率が向上 ・DR 応答に伴う需要家の負担を定量的に判断した上でインセンティブとの見合いによって最終的な反応度が自動決定されることを確認。冬季 DR 実証では、平均 25～30%程度の受電電力抑制を達成
	・商用施設向けエネルギー消費量 25%削減（2005 年度比）の実現 ・商用施設ピーク時の消費電力に対し、統合 BEMS の定めるベースラインに対して、6%のピークシフト/カットの実現	・2005 年度比で 38.6%の省エネが達成可能と試算、店舗データを活用した BEMS に基づく店舗運用改善の実施、提案 ・蓄電池活用 BEMS を利用した、デマンドレスポンス実証の結果、 統合 BEMS の定めるベースラインに比べて、夏季最大 15.5%、 および冬季最大 9.9%を達成 統合 BEMS 設定 DR 実施時間帯 30 分間単位における実績
FEMS	・個別導入・運用されてきた電力設備の統合制御 ・従来の工場等の事業所で、各々個別に導入・運用されてきた、蓄電システム、発電機、PV を統合最適制御する事により、省エネ、CO2 削減を実施。また最適制御の効果として契約電力を削減 ・地域レベルのエネルギー効率化向上のため、デマンドレスポンスに対応 ・夏季、冬季の電力需要の最大時期に、CEMS や統合 BEMS とインターネットを介して接続し、デマンド レスポンス実証し、電力需要をピークカットによるエネルギー効率化	・電力設備を統合最適計画、制御するスマートＦＥＭＳを開発 ・発電量予測データ並びに需要予測データに基づき、CGS（ガスエンジン：6 台）と RF 蓄電池（3 台の 電池構成）を統合最適計画、制御する事により、20%以上のピークカットと契約電力を 10%削減。 ・OpenADR2.0b の VEN 機能により統合 BEMS の VTN 機能と相互接続 ・デマンドレスポンスにおける世界標準規格である OpenADR2.0b の VEN 機能を開発し、アグリゲータ である統合 BEMS と、CCP による実証試験を実施。スマート FEMS により全自動でデマンドレスポンスに対応出来る事を確認。
EV	・太陽光発電電力を EV に蓄電し有効利用する V2H システムの効果 ・CEMS と連携可能な DR 対応した蓄電池と太陽光発電を利用した充電スタンドのエネルギーマネジメントシステムの効果 ・EV を活用したデマンドレスポンスによる電力需要調整の有効性	・EV の蓄電機能を活用することで、再生可能エネルギーの地産地消の 促進による CO２削減及び電力の需給調整において高い可能性を示した。①V2H：太陽光発電の自家消費率 25%向上、CO2 排出量を 25%低減 ②エコ充電スタンド：太陽光発電利用率が 30%となり、CO2 を 30%低減 ③EV を利用した DR：地域の電力需給調整に利用できることを確認
	・複数台の EV への同時・短時間充電を可能とするシステム ・EV 普及に資する社会インフラ	・蓄電・充電統合システムを開発、設置し、実証環境を構築 ・ピークカット８５％（１００ｋW⇒１５ｋW）でも、運用可能なことを確認 ・同時並列充電の必要条件と国内普及規模を定量的に評価 ・CEMS 連携により、地域の電力逼迫時、受電電力を抑制して運用 ・ピークカット時でも従来の充電器と遜色の無い充電時間を実現 ・必要な蓄電池容量と蓄電池の地域貢献能力を定量的に評価

付表Ｂ３ 自動走行システム実証実験プロジェクトの評価項目

評価項目				
a. 脅威分析調査	将来の自動走行モデルの全体像脅威	1 運転・駐車支援	1-3 車間距離制御（V2V型）	ITSと協調し先行車両との車間距離を制御する機能
			1-4 隊列走行（V2V型）	先頭車両と通信を行うことで後続車が無人で先頭車両を追従する機能（トラックなど商用車向け）
			1-5 自動運転（ITS協調型）	TSと協調することで人間に代わりあらゆる運転タスクを実施する機能
			1-9 自動駐車（スマホ連携）	スマートフォンにインストールされたアプリケーション経由で車両の操作指示を行うことで、遠隔からの車両の自動駐車を実施する機能
		2 安全走行支援	2-2 歩行者検知（V2P型）	歩行者の所有するスマートデバイスと連携し、車両の近くにいる歩行者を検知することで、必要に応じて車両を制御し歩行者との衝突を回避する機能
		4 ソフトウェアアップデート	4-1 OTA	無線通信を利用した電子制御システムのソフトウェア更新サービス
		5 故障検知	5-1 故障検知	自動車に備わる自己診断機能を活用し、故障を予知・検知するサービス
		8 車両遠隔操作	8-1 遠隔からのドアロック・アンロック	スマートデバイスなどと連携し、遠隔地より車両のドアのロック・アンロックを制御する機能
			8-3 充電制御	スマートデバイスと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能
			8-4 充電制御（音声認識AI連携）	音声認識AIエージェントと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能
			8-5 エアコン制御	スマートデバイスと連携し、遠隔地よりエアコンのオン・オフを制御する機能
			8-6 エアコン制御（音声認識AI連携）	音声認識AIエージェントと連携し、遠隔地よりエアコンのオン・オフを制御する機能
			8-7 エンジン再駆動・ステアリングロック解除禁止	オーナーの要請に基づき、エンジンの再始動・ステアリングロックの解除の禁止を実施する機能
b.情報セキュリティ評価ガイドラインドラフトの作成 (1/2)	評価ガイドラインドラフト（初版および第2版）	1.偵察	1.1 HW 調査	1.1.1 デバイス取り出し前 I/F 調査
				1.1.2 デバイス取り出し後 I/F 調査
				1.1.3 チップ取り外し後 I/F 調 査
				1.1.4 隠れたインターフェースからの調査
				1.1.5 インターフェース接続
				1.1.6 バイナリ抽出
				1.1.7 バイナリ保護機能確認
				1.1.8 リバースエンジニアリング
			1.2 SW 調査	1.2.1 アプリケーションの通信経路の調査
				1.2.2 WiFi（車両外部）の通信傍受
				1.2.3 WiFi（車両内部）の通信傍受
				1.2.4 Bluetooth の通信傍受
				1.2.5 BluetoothLE の通信傍受
				1.2.6 TCU の通信傍受
				1.2.7 ブラウザ、HTML エンジンの調査
				1.2.8 CAN メッセージ通信傍受
				1.2.9 アプリケーションの通信 傍受

b.情報セキュリティ評価ガイドラインドラフトの作成 (2/2)	評価ガイドラインドラフト（初版および第2版）	2.侵入	2.1 ユーザー介在型の受動的攻撃	2.1.1 DrivebyDownload 攻撃
				2.1.2 ファイル添付攻撃
			2.2 ユーザー非介在型の受動的攻撃	2.2.1 外部WiFiへの自動接続を利用した攻撃
				2.2.2 偽サーバー誘導による攻撃
				2.2.3 残存開発環境を用いた攻撃
			2.3 脆弱性を利用した能動的攻撃	2.3.1 Bluetooth 経由の攻撃
				2.3.2 BluetoothLE 経由の攻撃
				2.3.3.TCU 経由の攻撃
				2.3.4 WiFi（車両内部）経由の攻撃
			2.4 通信傍受した情報を用いた能動的攻撃	2.4.1 成りすまし攻撃
				2.4.2 リプレイ攻撃
		3. 権限昇格	3.1 保護機能の回避	3.1.1 コード実行防止機能の回避
				3.1.2 サンドボックス機構の回避
			3.2 高権限の奪取	3.2.1 既知の攻撃を試行することによる権限昇格
				3.2.2 強制アクセス制御（MAC）の機構の回避
		4.目的の実行	4.1 情報漏えい	4.1.1 機密情報の漏えい（外部送信）
			4.2 サービスの停止	4.2.1 車両のサービス（機能）の停止
			4.3 不正操作（制御系）	4.3.1 制御系ファームウェアの改ざん
				4.3.2 制御系機能の悪用
			4.4 不正操作（情報系）	4.4.1 情報系アプリケーションの改ざん
				4.4.2 情報系機能の悪用
c.情報セキュリティ評価の試行調査	・評価ガイドラインを用いた実車両システム評価 ・評価ガイドラインの妥当性評価および見直し	評価結果	評価結果の内容を記載	
		危険度	下記の判定基準に項目の危険度を記載	
		評価内容	評価により確認する内容を記載	
		評価手順	具体的な評価実施手順を記載	
		想定されるリスク	問題が見つかった場合、想定されるリスク（被害）の内容を記載	
		攻撃成立条件	問題が見つかった場合、攻撃が成功するための前提条件を記載	
		改善案	問題が見つかった場合、攻撃を防ぐための改善案を記載	
d.実証実験の運営準備	・実証実験実施計画（スケジュール） ・実証実験参加プロトコル（フローチャート等） ・参加者募集要領（要領、規約、申込書、契約書類） ・参加者募集説明実施要領、説明資料 ・実証実験情報管理手法、体制案			

付表Ｂ４ スマート農業加速化実証プロジェクトの評価項目

実証課題名	評価項目
関東平坦部における栽培管理支援システムとスマート農機の連携による大規模水稲作営農体系の実証	・ロボット農機や水管理システム導入による対象作業の作業時間20%減 ・ICTや収量コンバインを活用したデータ駆動型農業により生産性10% 向上 ・上記等の達成により、従事者一人当たりの労働報酬を40%向上
促成イチゴ栽培における圃場内環境および作物生育情報を活用した局所適時環境調節技術による省エネ多収安定生産と自動選別・パック詰めロボットを活用した調製作業の省力化による次世代型経営体系の検証	・10%の増収と本ぽ管理作業の20%の省力化、20%の省エネ(省資源)化を実現 ・ほ場内栽培環境、作物生育情報の収集技術の確立とスマホ等の活用による可視化アプリの提供 ・生育特徴量計測精度90%以上、収量予測精度80%以上の検出予測精度を達成 ・共同選果施設での自動選別ロボットの活用で、出荷調製コストを10%程度低減
輸出に対応できる「超低コスト米」生産体制の実証	・水稲の生産コスト「7,000円/60kg」(現況値(H29)から25%削減) ・スマート農業機械を汎用利用した最大限のコスト低減と、リモートセンシングによるデータの活用 ・単収・品質の向上を図り、輸出米に対応した「超低コスト米」の生産に取り組む体制と経営の実証

付図 C サプライチェーンにおけるサイバーセキュリティリスク

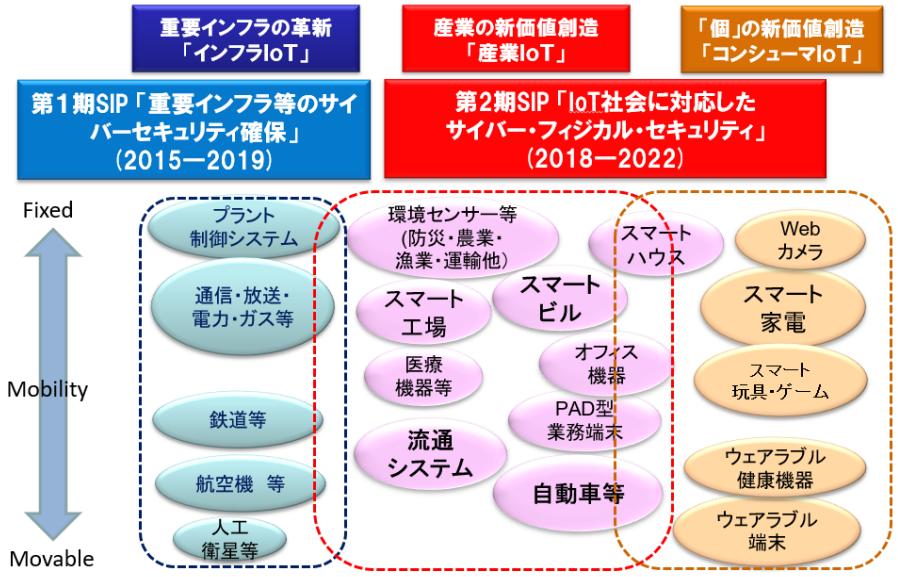
●●●●●●●様

サプライチェーンにおける
サイバーセキュリティリスク

●●年●●月●日
実証評価サブワーキング事務局

1

広義IoTがもたらす価値創造の多様性



2

IoTリスクとサプライチェーンリスクは喫緊の課題

IoTリスク：サイバー攻撃の脅威が、あらゆる産業活動に潜む

世界のサイバー犯罪による経済損失は6,000億米ドル（世界のGDPの0.8%相当
⇒日本では**約3兆円**）

IoTによるフィジカルとサイバーの融合により、サイバー攻撃がフィジカル空間まで到達し、**経済損失がさらに拡大**するリスク

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なる動き

米国：サイバーセキュリティフレームワークv1.1に、『サイバーサプライチェーンリスクマネジメント』を明記。
防衛調達の全参加企業にセキュリティ対策（SP800-171の遵守）を義務化

欧州：ネットワークに繋がる機器の認証フレームの導入検討。
EUの顧客データに新たな義務（GDPR）2018年から

3

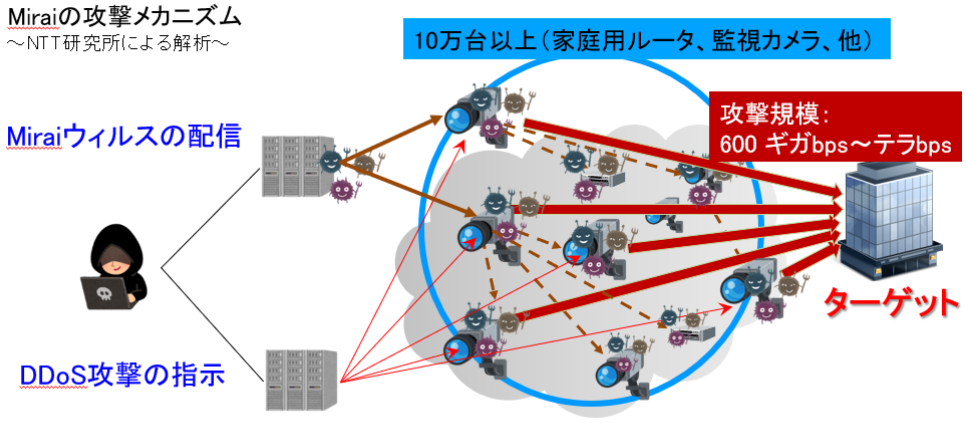
IoTリスク：IoT機器が社会インフラへサイバー攻撃

■ Miraiの事案：脆弱性のあるIoT機器が大規模DDoS攻撃の踏み台

【事例1】 DDoS攻撃（2016/10）により約6時間にわたりインターネットサービスが不安定（Twitter, Amazon, Netflixが使えない！）

【事例2】 ドイツテレコムのホームルータをマルウェア感染させる攻撃（2016/11）により、90万人が影響を受ける

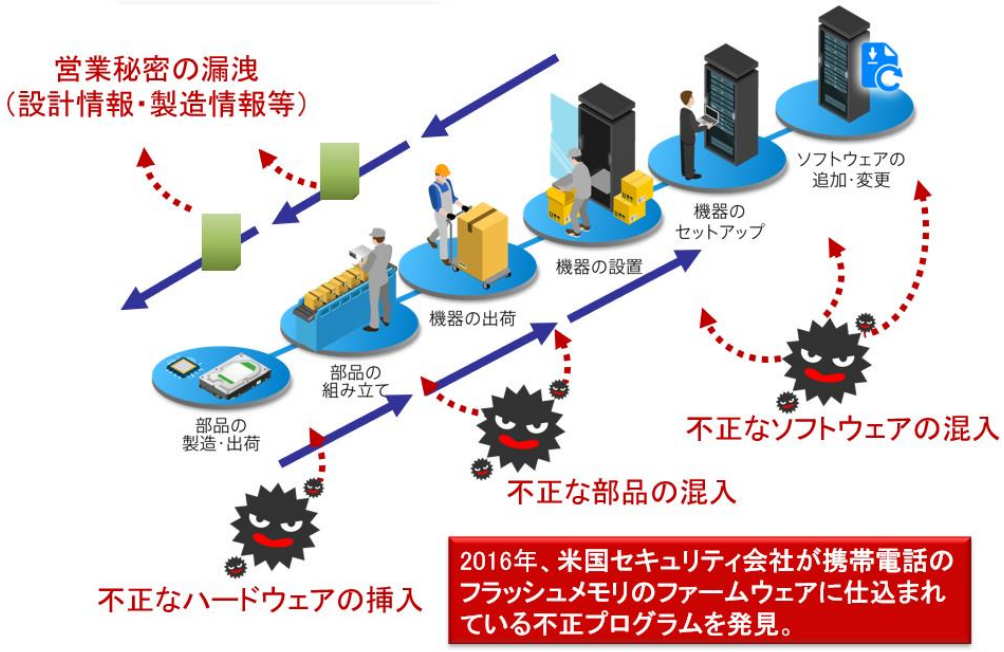
Miraiの攻撃メカニズム
～NTT研究所による解析～



同様の脆弱性を持つ多数の機器が感染し、一斉に遠隔操作される

4

サプライチェーンリスク:「混入」「改ざん」「漏洩」



5

サプライチェーンに関する問題発覚事例

事例	時期	場所	分野	工程	原因	被害	被害、信頼への影響
サーバーマザーボードへの攻撃用チップ組込み報道	'18/10	米国	IT	製造	規程違反	秘密情報流出(疑惑)	企業、製品への信頼棄損
ルーターへのバックドアツールの追加疑惑	'15/4	世界各国	IT	流通	規程不備	秘密情報流出(疑惑)	企業、製品への信頼棄損
WannaCryによるチップ製造ライン停止	'18/8	アジア	半導体製造	製造	規程違反(作業誤り)	製造ライン停止による納期遅延、売上減	企業やそのセキュリティ対策への信頼棄損
新幹線車両台車枠の仕様外製品の納入	'18/2	日本	車両製造	製造	規程不備	新幹線車両台車枠に亀裂発生、運行へ影響	製品、サービスの安全性への信頼棄損
産業用ゴム製品の検査不正	'17/3	日本	産業用部品製造	試験	規程違反	納入済製品の取り換え費用の発生	規程に則った検査実施、製品の安全性への信頼棄損
ディーゼル車排気ガス不正	'15/9	ドイツ	自動車製造	設計・製造・試験	規程違反	罰金、違反車の買戻し、企業の市場価値低下	環境基準適合、法令遵守への信頼棄損
「ハラール認証製品」のハラール不適合問題	'00/9	インドネシア	食品製造	設計	規程不備	製品回収	食品の宗教戒律への適合に対する信頼棄損
航空機副操縦士の乗務前過剰飲酒	'18/11他	英国、日本	旅客輸送	運用	規程違反(過剰飲酒)	-	安全運航への信頼棄損

6

サーバーマザーボードへの攻撃用チップ組込み報道

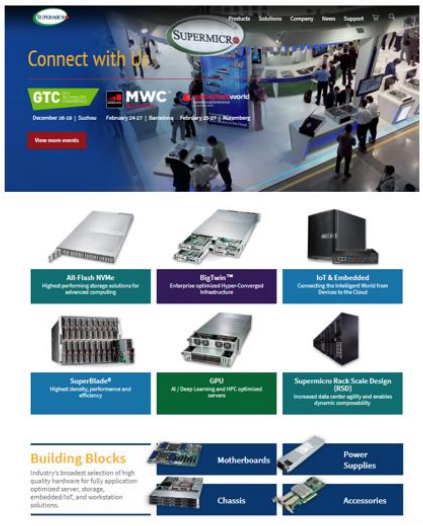
- Bloombergが2018年10月4日の記事で、AppleとAmazonが自社製サーバに採用しているSupermicro製のマザーボードにデータを盗み出すためのスパイチップが埋め込まれていたと報道
  https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

出展: 上記Bloomberg社記事より

- Bloombergの報道によると、Supermicro社の製造下請業者の一社である中国の業者の工場において、中国人民解放軍のスパイにより当該チップが埋め込まれたとのこと
- ただし、Apple、Amazonさらに米国土安全保障省(DHS)もこのBloombergの報道を否定しており最終的な真偽は不明の状況
- 真偽不明の状況ではあるが、現実問題として、報道された当時Supermicro社は株価下落といった実害を受けており、このような不正が行われないようにするための仕組みに加え、不正が行われていないということを客観的に証明できるための仕組みが必要と考えられる

【参考】Supermicro社

https://www.supermicro.com/en



株式会社アスク　製品情報
https://www.ask-corp.jp/products/supermicro.html

Supermicroとは？

Super Micro Computer, Inc.は、1993年に米国カリフォルニア州サンノゼにて設立された、サーバー/ワークステーション及びHPC関連製品などを開発・提供しているハードウェアベンダーです。設立以後、世界的な事業拡大を続けており、高性能・高効率サーバ技術及び世界中のHPC、IDC、クラウドコンピューティング、エンタープライズIT、Hadoop/ビッグデータ、組込システムへグリーンコンピューティングを提供する革新的グローバルリーダーとしてお客様からの幅広いご要望・要求仕様に対応出来る製品を供給しています。

産業用ゴム製品の検査不正

- 旧東洋ゴム（現TOYO TIRE）において、産業用ゴム製品の検査における不正が発覚
  - 事例1：2015年3月　免震ビルに適用される高減衰ゴム（免震ゴム）において、国交省が認定する性能評価基準を満たさない製品を検査データを改ざんし、出荷
  - 事例2：2017年2月　船舶向け配管バルブの「シートリング」において、必要な検査を実施せず、過去の検査データを流用するなどし、出荷

出展：https://www.sankei.com/west/news/170207/wst1702070094-n1.htmlより

- いずれの事例もそれぞれ一人の検査担当者による不正。事例1は、10年間一人で担当していた検査担当者が交代し、業務を引き継いだ担当者が発見。事例2は、事例1等を受け、検査体制を強化したさいに、過去データと酷似した検査データが発見されたことで判明
- 担当者の自己申告に頼るのではなく、検査作業等が正しい手順に則り実施されたかどうか、検査データ等が改ざんされていないかどうかを客観的に保障するための仕組みが必要と考えられる

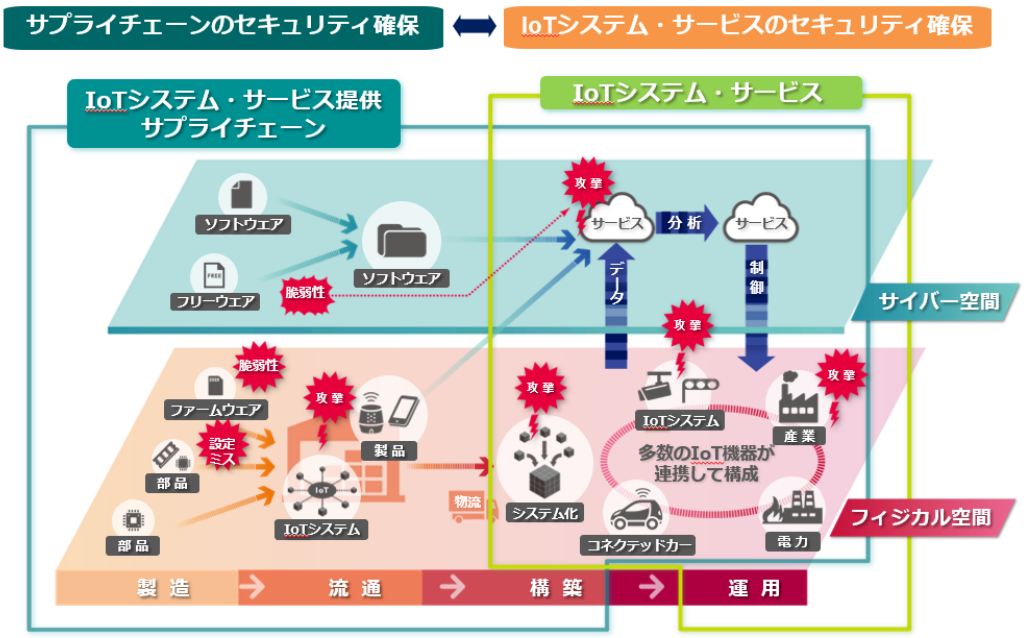
9

【参考】TOYO TIRE株式会社（旧 東洋ゴム）

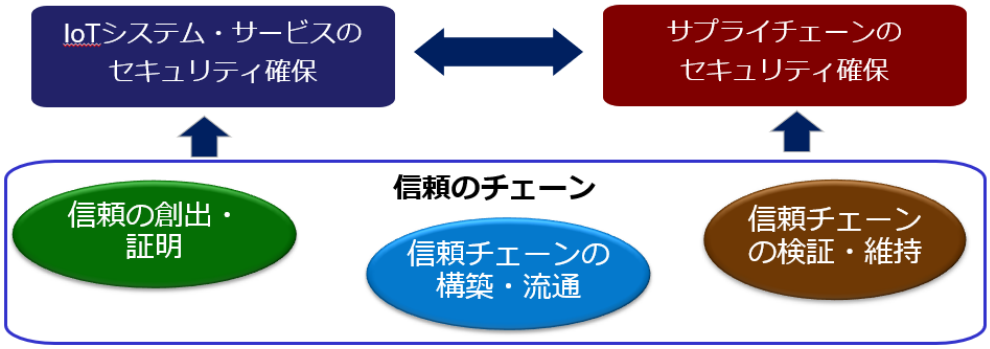
https://www.toyotires.co.jp/responsibility/

10

サイバー・フィジカル・システムのセキュリティ課題



「信頼のチェーン」によるセキュリティ確保



- ◆ 社会全体の安全・安心を確立し、Society5.0がもたらす**約90兆円の価値創出**を支える
- ◆ 幅広い産業分野の国際競争力を高め、輸出主体の製造業の**参入機会を確保**する
- ◆ 2030年までにサプライチェーン対策が求められる**中小企業の50%**に成果導入を目指す

契約管理番号：１９１０１５３５－０