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

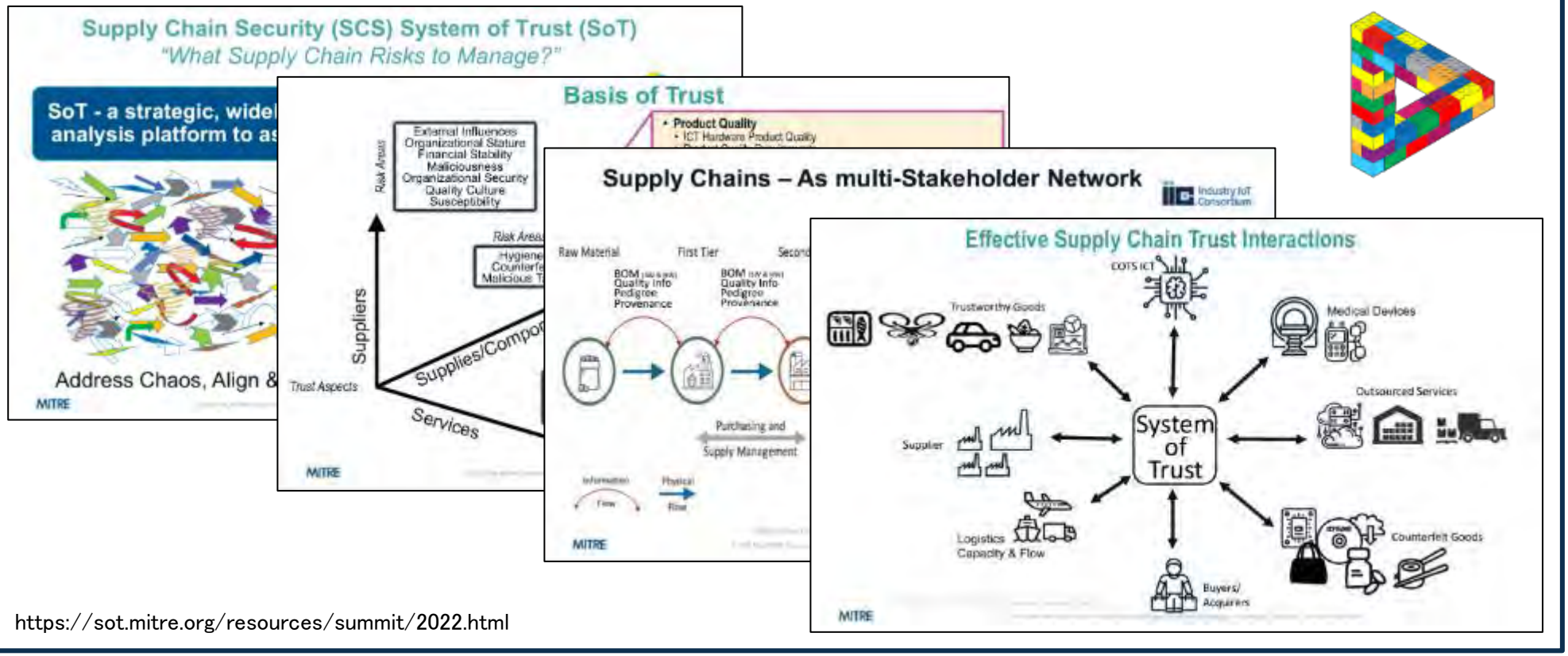
NIST National Institute of Standards and Technology U.S. Department of Commerce

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]

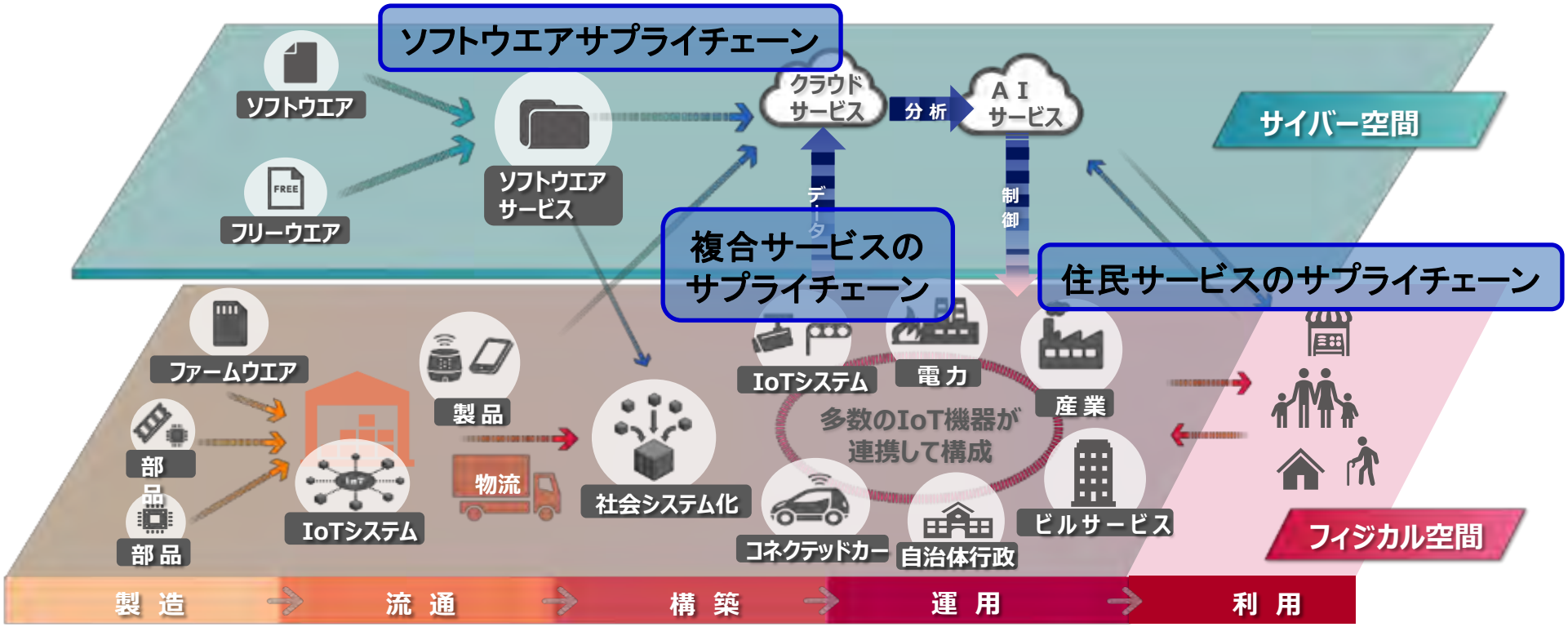
*1https://www.cisa.gov/uscert/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

*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

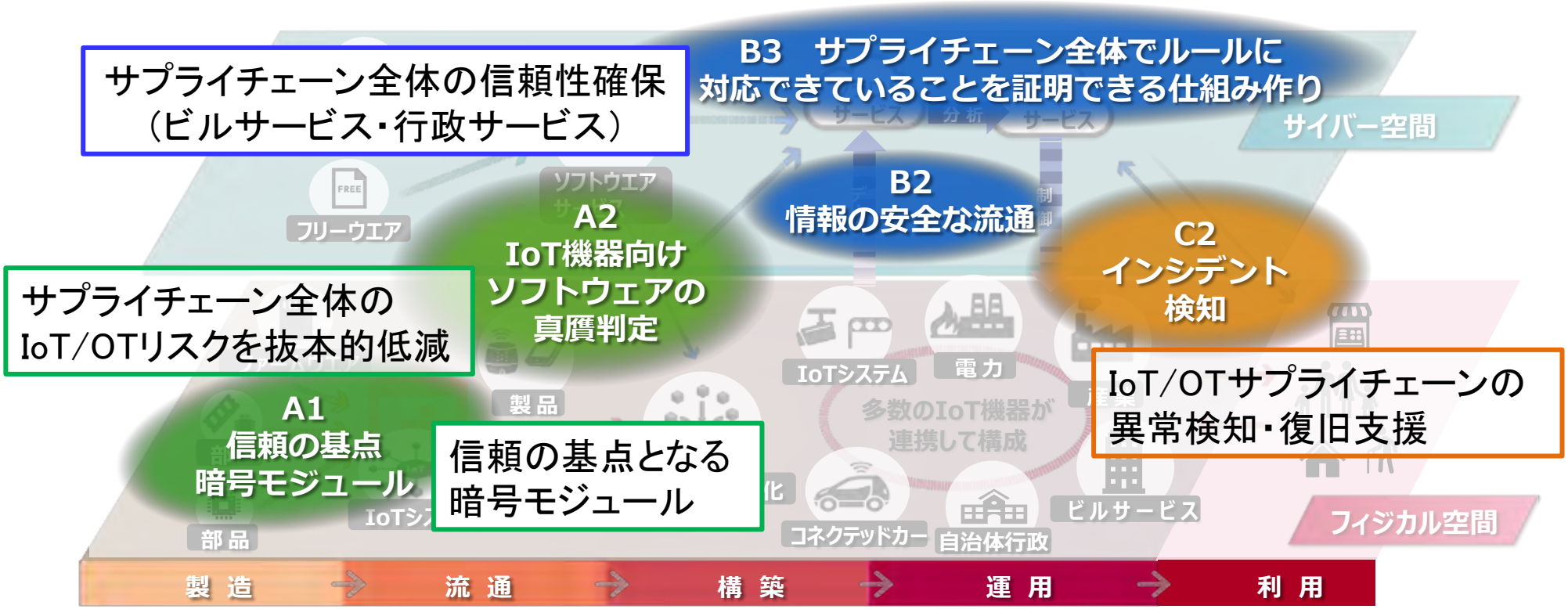
サイバー空間とフィジカル空間の双方に跨るIoT社会でのサプライチェーン



『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