資料３

経済産業省の研究開発関連の取組

令和4年9月

経済産業省商務情報政策局サイバーセキュリティ課

産業サイバーセキュリティ研究会とWGの設置による検討体制

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
アクションプランを加速化する３つの指針を提示
第４回：令和2年　　4月17日　開催（電話開催）
産業界へのメッセージを発信
第５回：令和2年　　6月30日　開催
サイバーセキュリティ強化運動の展開
第６回：令和３年　　４月２日　開催
アクションプランの持続的発展と、新たな課題へのチャレンジへ
第７回：令和４年　　４月11日　開催
産業界へのメッセージを発信

WG１（制度・技術・標準化）

１．サプライチェーン強化パッケージ

WG２（経営・人材・国際）

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３(サイバーセキュリティビジネス化)

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する~Proven in Japan~
３．『中小企業・地域』まで展開する

泉澤　清次　三菱重工業株式会社取締役社長
遠藤　信博　日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社取締役会長等
大林　剛郎　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長
櫻田　謙悟　経済同友会代表幹事、ＳＯＭＰＯホールディングスグループＣＥＯ取締役　代表執行役会長
篠原　弘道　日本電信電話株式会社取締役会長
東原　敏昭　株式会社日立製作所取締役会長代表執行役
船橋　洋一　一般財団法人アジア・パシフィック・イニシアティブ理事長
村井　純(座長)慶應義塾大学教授
渡辺　佳英　日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

産業サイバーセキュリティ研究会構成員　（2022年4月11日現在）

サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取組

- **「サイバー・フィジカル・セキュリティ対策フレームワーク」では、Society5.0における産業社会でのセキュリティ対策の全体枠組みを提示。** https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html
- 全体の枠組みに沿って、対象者や具体的な対策を整理し、『サイバーセキュリティ経営ガイドライン』や産業分野別のガイドラインなどの実践的なガイドラインを整備。

＜各種取組の大まかな関係＞

経営層 ／ 実務層（共通） ／ 実務層（産業分野個別）

コンセプト

サイバー・フィジカル・セキュリティ対策フレームワーク（2019年4月）

第I部　サイバー空間とフィジカル空間が融合した産業社会におけるサイバーセキュリティの在り方

第II部　リスク源の洗い出し

第III部　対策要件と対策例集

サイバーセキュリティ経営ガイドライン（Ver2.0：2017年11月）

活用

3層：協調的なデータ利活用に向けたデータマネジメント・フレームワーク（2022年4月）

2層：IoTセキュリティ・セーフティ・フレームワーク（2020年11月）

中小企業の情報セキュリティ対策ガイドライン（IPA）（第3版：2019年7月）

支援ツール

- **経営プラクティス集（IPA）**（第３版：2022年3月）
- **サイバーセキュリティ体制構築・人材確保の手引き**（第1.1版：2021年4月）
- **可視化ツール**（web版：2021年8月）

- ビル分野のガイドライン（第１版：２０１９年６月）
- 自動車分野のガイドライン（第１．０版：２０２０年12月）
- スマートホーム分野のガイドライン（第１．０版：２０２１年４月）
- 工場分野のガイドライン（２０２２年４月パブリックコメント募集）
- …
- 電力分野の取組

具体的対策

ソフトウェアタスクフォースにおけるSBOM実証について

- 令和3年度は、ソフトウェア製品のサプライチェーン（サプライヤー、ベンダー、ユーザー企業）において、SBOMの作成、共有、活用（脆弱性管理、ライセンス管理）の一連の実証を行い、**主なコスト・効果の項目を特定**。
- 令和4年度は、SBOMに関して**「規制や推奨化が見込まれる分野」や「効果が大きいと思われる分野」等を候補**に、実証参加企業の選定、実証内容の設計を進め、**実証結果や民間で進められているSBOM活用の取組について、知見等を共有し、実際の活用方法を検討**。

令和3年度の結果

SBOMを導入するための初期工数※1は大きいが、ツールを活用することで運用工数※2は小さくなった。

SBOMツールにより脆弱性発表から特定までのリードタイムを短縮可能。

OSSの依存関係を解析することで、構成ファイルからでは特定できない他のOSSの再利用も検知可能。

※1初期工数：ツール導入等の環境整備や使用方法習得のための学習等
※2運用工数：SBOM作成、活用等

令和4年度の取組

SBOMに関する規制や推奨化が見込まれる分野

自動車業界
（OEM/部品サプライヤー等）

医療機器業界
（医療機器メーカー等）

- 規制等において定められるSBOMへの要求事項を満たしつつ、効率的にSBOMを作成、活用していくモデルを検討。
- 米国NTIAにおける既存のPoCについて得られる情報を確認、活用。

知見を共有

SBOMの効果が大きいと思われる分野

ソフトウェア業界
（ITベンダーとそのサプライチェーン等）

- システム／サービスを多く管理し、SBOMを多様なサプライヤーやユーザーと共有するうえで、メリットを最大限享受できる活用モデルの検討。
- 開発環境や構成管理ツール等に関する知見や課題の整理。

サイバーセキュリティお助け隊サービス

- 2019年度・2020年度実証事業で得られた知見に基づき、実証参加事業者がサービスを開発。
- サービス普及に向け、2021年度よりサービスブランドを設立。2022年８月時点で18サービスが登録。
  サービス審査登録制度の運営とともに、中小企業の意識啓発・サプライチェーンによる普及などの施策と一体となった普及施策の展開を開始。

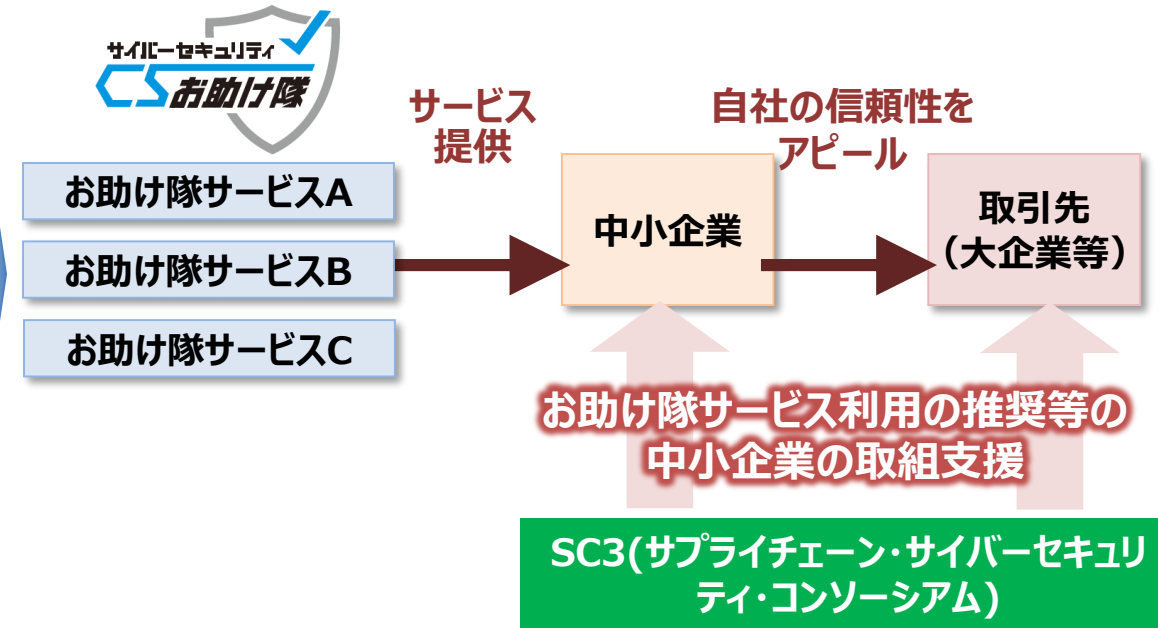
中小企業のサイバーセキュリティ対策に不可欠な各種サービス

- EDR・UTM等による異常監視
- 緊急時の対応支援・駆付けサービス
- 相談窓口
- 簡易サイバー保険
- 簡単な導入・運用

中小企業でも導入・維持できる価格でワンパッケージで提供

IT導入補助金により
最大2年間分のサービス利用料を
50%補助

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊マークの商標利用権を付与



SC3(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（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。

包括的なサイバーセキュリティ検証基盤を構築し、『Proven in Japan』を促進

- 「**Proven in Japan**」では、2つの方向を追求し、**セキュリティビジネスの成長を促進**。

① 有効性確認等を通じ、日本発のサイバーセキュリティ製品のマーケット・インを促進

② IoT機器等の信頼性を高度に検証するハイレベル検証サービスの拡大

⇒2021年度は新たに開発段階の製品・設計書等の検証も実施。

1.セキュリティ製品の有効性検証

ベンチャー等のセキュリティ製品

有効性検証

検証環境

2.実環境における試行検証

ベンチャー等

お試し製品提供と検証

実環境

民間事業者等のオフィス

3.攻撃型を含めたハイレベルな検証サービス

検証サービス事業者

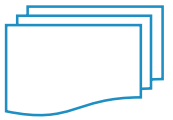
攻撃型検証等

IoT機器・システム等

4.セキュリティ・バイ・デザインを実現する開発段階検証

検証サービス事業者

開発段階検証



設計書・ソースコード等

New

信頼できるセキュリティ製品・サービス

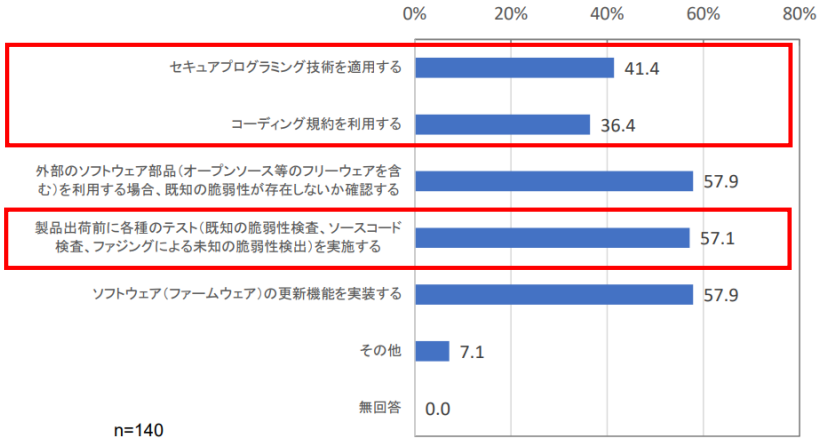
世界に貢献する高水準・高信頼の検証サービス

IoT機器に対するセキュリティの取組状況・開発段階検証事業

- IoT機器に対するセキュリティの取組においては、「**セキュリティ・バイ・デザイン**」の考えに基づき、設計・開発段階で**セキュリティ対策が適切に導入されていることが必要**。
- 他方で、**開発段階でセキュリティ対策を行っている企業は現状限定的**であり、十分な脆弱性対策が実施されていないことにより、**1,000万円以上の損害に繋がった企業も存在**する。
- 本事業は、セキュリティ・バイ・デザインの考えに立脚し、**開発段階からの脆弱性検証を試験的に実施することで効果的な検証手法を整理する**とともに、**その効果を可視化**し、**中小企業による発売前のIoT機器の脆弱性検証を促進する**ことを目的とする。

IoT機器に対するセキュリティの取組状況

（開発段階の脆弱性対策の考慮内容）



- **4割以上の企業が機器出荷前に検証を実施していない。**
- **6割程度の企業が開発段階のセキュリティ対策を行っていない。**

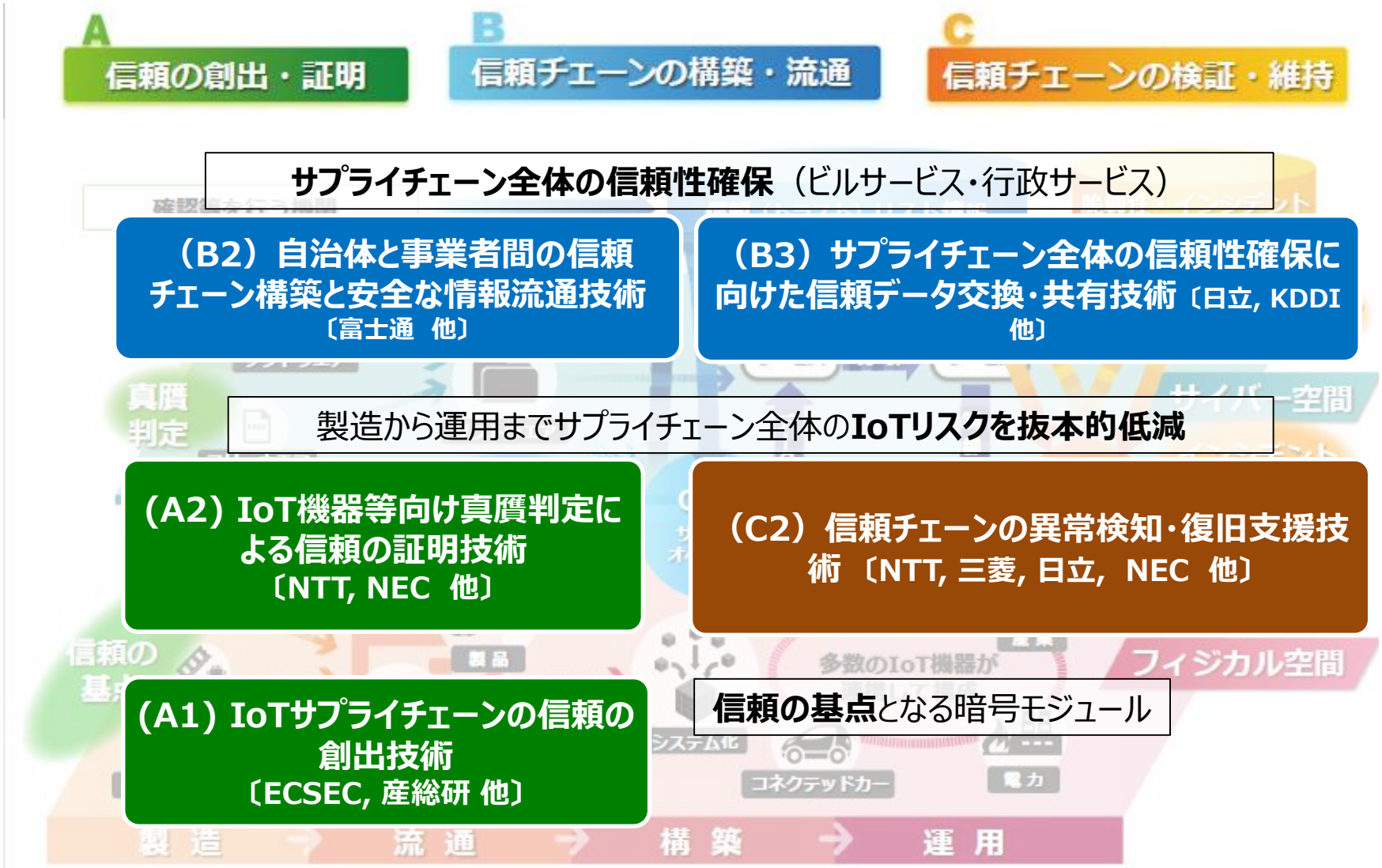
IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」
https://www.ipa.go.jp/files/000065094.pdf
※調査実施：2017年11月、調査対象：国内企業205社

中小企業が開発するIoT機器本体や、
当該IoT機器に関するものの一部を提供いただく

IoT機器の開発段階で実施すべきセキュリティ対策を示唆し、
発売前のIoT機器の脆弱性検証を促進する。

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

研究開発サブテーマと分担（2021年度から）

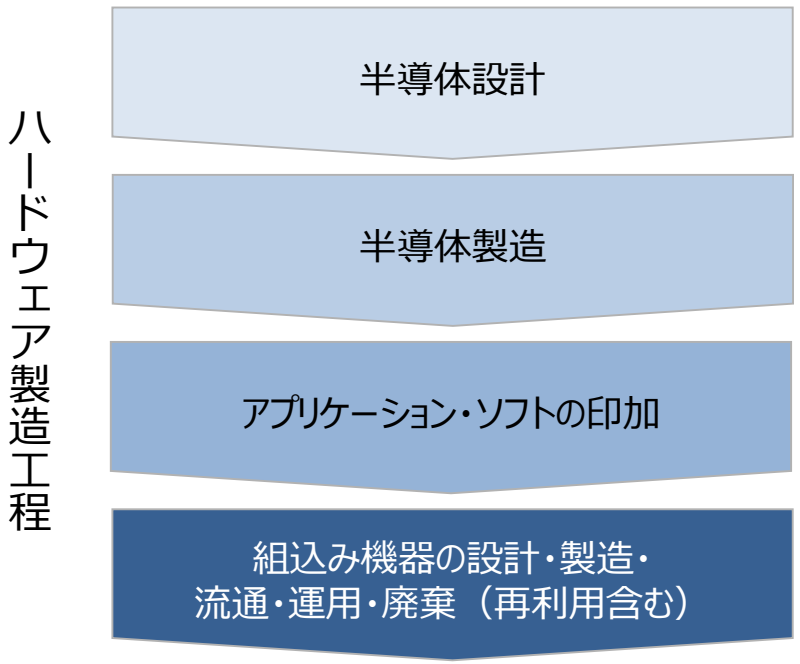


サイバーセキュリティ領域における研究開発テーマ例

【ハードウェア検証】
- 半導体等のハードウェアに本来期待される機能以外の回路が仕込まれることで、情報漏洩などの意図しない動作を引き起こすハードウェアトロージャンを特定するための検証技術。

【秘密計算】
- データの秘匿性を確保しながらAIによる分析等の計算を実現する秘密計算技術が有望であり、高速かつ多様な計算を実現することが可能。

ハードウェア検証技術



秘密計算技術