経済産業省

資料４

事務局説明資料

産業サイバーセキュリティ研究会
WG１・分野横断SWG　合同会議

令和６年３月１４日

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

構成員

※　2022年4月開催時の構成員・役職

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　代表執行役社長
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

オブザーバー　NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省、デジタル庁

WG１（制度・技術・標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日
第６回　令和2年3月（書面開催）
第７回　令和2年10月（書面開催）
第８回　令和3年３月15日
第９回　令和4年4月4日
第10回　令和6年3月14日

１．サプライチェーン強化パッケージ

WG２（経営・人材・国際）

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日
第５回　令和2年1月15日
第６回　令和2年8月25日
第７回　令和3年2月18日
第８回　令和4年3月23日
第９回　令和5年3月27日

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）

第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日
第５回　令和2年3月(書面開催)
第６回　令和3年3月10日
第７回　令和4年4月6日

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

分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化 と テーマ別TFにおける検討

- **<u>7つの産業分野別サブワーキンググループ（SWG）</u>**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、**<u>3つのタスクフォース（TF）を設置</u>**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
(分野ごとに検討するためのSWGを設置)

ビルSWG
- ガイドライン第2版の策定(2023.4)

電力SWG
- 小売電気事業者ガイドライン策定(2021.2)

防衛産業SWG
- 防衛産業サイバーセキュリティ基準の改訂を公表(2022.4)

自動車産業SWG
- ガイドライン2.1版を公表(2023.9)

スマートホームSWG
- ガイドライン1.0版を公表(2021.4)

宇宙産業SWG
- ガイドライン1.1版を公表(2023.3)

工場SWG
- ガイドライン1.0版を公表(2022.11)

・・・

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
データの信頼性確保に向け「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク」を策定。

ソフトウェアTF：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

検討事項：
OSSの管理手法に関するプラクティス集を策定、SBOM活用促進に向けた実証事業（PoC）を実施。「ソフトウェア管理に向けたSBOMの導入に関する手引」を策定。

『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。このIoT-SSFをわかりやすく理解するためのユースケースを策定。

前回ＷＧからの主な進捗

①セキュアバイデザイン・セキュアバイデフォルトについての国際的な議論の加速

⇒SBOMの活用促進

②サプライチェーン全体におけるセキュリティ強化の必要性

⇒産業分野別ガイドラインの策定・普及促進（業界横断的分野も含め）

③デジタル技術の進展に伴う新たなサイバー攻撃のリスク

⇒経済安全保障重要技術育成プログラムを活用した、先進的サイバー技術の開発

目次

【米日他】セキュアバイデザイン・セキュアバイデフォルト

- **セキュリティの責任は製造者等が追うべきである（「責任のリバランス」）**、という**欧米諸国を中心に提唱されている概念**。
- 2023年4月に米CISAが一部有志国と共に**セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項をまとめたガイダンスを作成**し、**ソフトウェア開発者に対し、安全な製品を出荷するために必要な措置を講じるよう**促した（法的拘束力なし）。同年10月に本文書が改訂され、**日本含む13か国が共同署名**。*
- 文書では**ソフトウェア開発者**に対し、**セキュリティ実現のための3つの基本原則と各原則を実現するためのプラクティス**が示されている。一部のプラクティスでは、**経産省の文書（OSS事例集及びSBOM導入手引）が参考文書として引用**されている。
- また、ソフトウェア開発者に対して**セキュアバイデザイン・セキュアバイデフォルトを実践するための手法を示している**ほか、**ソフトウェア利用者に対する推奨事項**も示している。

*共同署名者：米CISA、米NSA、米FBI、米OAS/CICTE、豪ACSC、加CCCS、英NCSC-UK、独BSI、蘭NCSC-NL、諾NCSC-NO、新CERT NZ、新NCSC-NZ、韓KISA、以INCD、日NISC、日JPCERT/CC、星CSA、捷NÚKIB

文書の概要

1. 定義

- セキュアバイデザイン：IT製品（ソフトウェア等）が、設計段階から安全性を確保されていること。
- セキュアバイデフォルト：ユーザーが、追加のコストや手間をかけることなく購入後すぐにIT製品（ソフトウェア等）を安全に利用できること。

2. ソフトウェア開発者等への提言

- セキュアバイデザイン手法の導入（安全なプログラミング言語の採用、SBOMの採用等）、セキュアバイデフォルト手法の導入（デフォルトパスワードの排除、多要素認証の導入等）、顧客のセキュリティの結果に責任を持つ等の基本原則の遵守　等

3. ユーザー組織への提言

- セキュリティ結果の責任をソフトウェア開発者に問うこと
- セキュアバイデザインやセキュアバイデフォルトを導入している製品の購入を優先すること　等

【英日他】「セキュアAIシステム開発のためのガイドライン」

- **英NCSC(国家サイバーセキュリティセンター）を中心に、**AIの「開発」等におけるセキュアバイデザインの実現に向け、**AIプロバイダー向けの指針（「セキュアAIシステム開発のためのガイドライン」文書）を作成**（法的拘束力なし）。**日本を含む17か国*が共同署名**。2023年11月28日公表。
- AIプロバイダーはセキュアバイデザイン原則に沿って、ユーザーのセキュリティ結果に責任を負うべきであるとした上で、**AI開発ライフサイクルを４つのステップに沿って整理**する内容。

*共同署名者：英NCSC-UK、米CISA、米NSA、米FBI、豪ACSC、加CCCS、新NCSC-NZ、智CSIRT、捷NÚKIB、エストニアRIA、エストニアNCSC-EE、仏ANSSI、独BSI、以INCD、伊ACN、日NISC、日CSTI、ナイジェリアNITDA、諾NCSC-NO、ポーランドMC、ポーランドNASK、韓NIS、星CSA

文書の内容（抜粋）

（ア） セキュアな設計

- システムに対する脅威をモデル化する。AI特有の脅威の影響を評価し、意思決定を文書化する。
- システム設計に際し、機能性やパフォーマンスと同等に、セキュリティを考慮する。

（イ） セキュアな開発

- サプライチェーンのセキュリティを確保する。
- 関連アセットを保護し、SBOM等によりデータ、モデル、プロンプトを文書化する。

（ウ）セキュアな導入

- システムのライフサイクルを通じて、使用するインフラのセキュリティを確保する。
- あらかじめインシデント管理手順を定め、適切かつ効果的なテスト後にAIシステム等をリリースし、ユーザに適切な使用方法等を明示する。

（エ） セキュアな運用とメンテナンス

- システムの挙動を監視し、潜在的な侵入、侵害等を検知できるようにする。
- デフォルトで自動化アップデートを実装し、モデル等の変更による挙動の変化につき、ユーザが評価できるようサポートする。

【豪日他】「AI使用に関する国際ガイダンス」

- **豪州サイバーセキュリティセンター（ACSC）を中心に**、AIの「使用」に着目し、**「AI使用に関するガイドライン(“Engaging with Artificial Intelligence”)」を作成**（法的拘束力なし）。**日本を含む11か国*が共同署名**。2024年1月24日公表。
- AIシステムに対する**６つの脅威を特定の上、これに対する12の緩和策を注意喚起**する内容。

*共同署名者：豪ACSC、米CISA、米NSA、米FBI、英NCSC-UK、加CCCS、新NCSC-NZ、独BSI、以INCD、日NISC、日CSTI、諾NCSC-NO、星CSA、スウェーデンNCS

６つの脅威

①データポイズニング
②インプット改ざん攻撃
（プロンプトインジェクション・敵対的サンプル）
③生成AIハルシネーション
④プライバシー・知的財産に関する懸念
⑤モデル窃取攻撃・学習データ漏えい
⑥匿名化データの再特定

12の緩和策

①サイバーセキュリティ枠組みの実施
②プライバシー・データ保護義務への影響評価
③多要素認証の実装
④特権アクセスの管理
⑤バックアップ
⑥試行
⑦サプライチェーンを含むセキュアバイデザイン確保
⑧限界や制限の理解
⑨関係スタッフの能力・資格
⑩検査・ヘルスチェック
⑪ログ監視
⑫インシデント対応

【米】安全、セキュアで、信頼できるAIに関する大統領令

- 2023年10月30日、バイデン大統領は「**安全、セキュアで信頼できるAIに関する大統領令**」を発表。
- 従前から米国が進めてきたAI開発者向けの自主的コミットメント等に基づきながら、**米国がAIの便益を確保しながら、リスクを管理することを目的**とするもの。
- AIの安全性、セキュリティに関する新たな基準の策定から労働者支援、政府機関によるAIの活用まで、広範な政策パッケージを**８つの柱に従って提示。**（以下一部抜粋）

AI技術の安全性とセキュリティの確保　（セクション4）

4.1. AIの安全性とセキュリティに関するガイドライン、標準、ベスト・プラクティスの策定

(a) 本大統領令の発令日から**270日以内に、安全、安心かつ信頼できるAIシステムの開発を確実にするため**、商務長官は、**国立標準技術研究所（NIST）所長を通じて、**エネルギー省長官、国土安全保障省長官、商務長官が適切と考えるその他の関連機関の長と連携して、以下のことを行う：

(i) 業界標準のコンセンサスを促進する目的で、**以下を含む安全、安心、信頼できるAIシステムを開発及び展開するためのガイドラインとベストプラクティス**を確立する：

（略）

(B) **生成AIおよびデュアルユース基盤モデルのための安全な開発プラクティスを組み込んだ、安全なソフトウェア開発フレームワーク（SSDF）の付属資料の開発**

【米英】AIセーフティ・インスティテュートに関する主要国動向

	AI Safety Institute NIST（商務省）	AI Safety Institute DSIT
概要	• 2023年10月31日米AI大統領令に規定、翌日11月１日に正式発表。 • 産官学の200以上の組織からなるAISIコンソーシアムをAISI配下に設置したことを2024年2月8日に公表（今後、レッドチーミング、安全性・セキュリティ等の５つのテーマ別ワーキンググループで作業予定。）。	• 2023年11月1日-2日に英が主催したAIサミットにて正式発表。 • 2023年4月から活動していた首相直下の「フロンティアAIタスクフォース」を発展改組。
主な機能	• **AIシステムの安全性評価の評価方法の策定** ➢ 開発者におけるAIの市場導入前の安全性評価のためのガイドライン、ツール等を米AISIが整備。 ➢ 対象事業者がそのツールを用いて自己評価を実施し、結果及び対策を米政府に報告する義務が課せられる見込み。	• **AIシステムの安全性評価の評価方法の策定及び実施** ➢ 開発者におけるAIの市場導入前の安全性評価のためのガイドライン、ツール等を整備。重点項目は、①デュアルユース能力を有するAI、②社会的インパクトの大きなAI、③システムの安全性とセキュリティ、④統御不可能性（人間の思いもよらない挙動） ➢ 英AISI が対象事業者の技術評価を実施。 • **AIの安全性に関する基礎研究の推進** AIガバナンスのためのツールの開発、評価技術の向上等について、米仏等の外部研究者と連携して取り組む。

（参考）米連邦調達規則案　FAR 2021-0017

- 大統領令14028を受け、米政府調達局（GSA）、米国防省（DoD）、米NASAが、**米連邦調達規則（FAR）の改正案**について、2023年10月3日から2024年2月2日まで**パブコメを実施**（既にパブコメは終了）。
- 本改正案では、**政府が調達するICT製品・サービス（例：通信サービス、電子メディア、IoTデバイス、運用技術）の請負業者**に対して、**SBOMの作成・維持、SBOMへの政府機関のアクセスの許可、サイバー脅威の調査やインシデント対応に関連するCISAへの協力、インシデントに関する報告**（発見時から8時間以内にCISAに報告、その後72時間ごとに更新）等を求めている。

SBOM箇所抜粋

- セキュリティインシデント発生の有無に関わらず、**契約の履行において連邦政府が使用するすべてのソフトウェアについて、SBOMを作成・維持**し、**SBOM に対する連邦政府機関のアクセスを許可**すること。
  注：大統領令14028は、「政府が調達するソフトウェア」のSBOMを想定していたため、本改正案はより広範囲
- 請負業者は、**ソフトウエアの更新に伴い、SBOMを更新**しなければならない。

（2024年2月2日付コメント）

The Software Alliance
BSA

- **SBOMの作成・使用を指示しているものの**、未熟の手法であり、且つその標準化が議論されている中で、**準備が整っていない**。
- SBOMの議論を米国内で牽引している、**米サイバーセキュリティ庁（CISA）との連携が必要**。

目次

前回のWG1・分野横断SWG合同会議における主なご指摘

【ソフトウェアタスクフォース、SBOMについて】

- 米国においては、SBOMは特にヘルスケアとファイナンスに取り組んでいる。米国とのインターオペラビリティを確保するためにファイナンシャル、例えばクレジットの領域などで実証をトライしてみるとよいのではないか。
- SBOMは各国で、規制などのエコシステムができあがってくると、日本の産業がついていくのは大変。今後、SBOMの脆弱性の対応の実証を進める際には、それを有効に活かしていくような、**日本ならではの官民の連携や共助の仕組み**など議論できるとよい。
- SBOMについて、現在、米国や海外含めて足並みを揃えて進めているところと理解。その際、SBOMのフォーマットが、**日本独自にならないように留意することが必要**。また、エンドユーザ企業と話をしていると、ベンダー側からSBOMの情報を出してもらえないと、進められないという姿勢で静観しているという企業が多いように感じているので、**SBOMを使うことのメリットや、使わないことのデメリットを普及啓発**していく必要がある。
- SBOMに関して、どこまで深堀して追いかけていくかということを、そろそろ真面目に考えないといけないの。Log4Jの件でも明らかなように、ほとんどのところが使っていることすら意識していないものがこれからたくさん出てくると思う。**一個一個のOSやプログラムのモジュールまで全部追いかけていくのか**、それを**誰が管理していくのか**、またそもそもその**モジュールを使っていることを公表するのか**しないのか、**公表できないものをどのように扱っていくのか**など、色々な検討すべきハードルが出てくる。
- 自社でSBOMの取り組みを行う中で、今まで独自で作っていた部分がリプレースされて、OSをインストールするようなユースケースも増えてきているなかで、どこまで管理するのか、どこまで深掘りできるのか、悩んでいる。また、課題だと思っていることは、**SBOMを作るプロセス**と、作った後に、**脆弱性情報とマッチングすることができる技術者が足りない点**。その影響は何かというところについて、ソフトウェアのサーバや情報システムで、それを解釈する人材不足、力不足を感じている。使う部分でも新しい課題が出てくると思うので、どういう仕掛けが必要か、検討が必要。
- プロダクトを提供するプロバイダー側としてもOSSを始めとしたソフトウェアの脆弱性の早期検知と、ひいては対応という意味で、プロダクトSIRTとしての活動として、構成情報のデジタルでの把握は喫緊の課題となっていて、非常に重要な取り組みだと捉えている。これを実現するために、データをどこまで管理するのか、コストや運用のフィージビリティなども重要。また、フォーマットの標準化なり、運用の定型化が課題になってくるが、そのためにインダストリーごとの実証を行うことが実践的な活動。一方で、今、各種製品形態での提供というのみならず、クラウド上であらゆるソフトがさまざまなサービスに組み込まれてきている時代であるので、**インダストリーのプラクティスが、業種を超えたサービサーにとって有効な事例になってくるのではないか**と期待している。
- 実体であるソフトウェアとSBOMで管理しているものが乖離してしまわないように管理していかないといけないが、その管理体系の仕方についても、**運用規則、あるいは運用ガイドラインとしてまとめるとよい**。それをやっていなければ調達しない等が言えるガイドラインであれば、各社としてもSBOMを取り入れていくトリガーになる。

SBOM導入・活用に向けた課題

- SBOM活用による効果が想定される一方で、**導入コスト等が障壁となり、活用が進んでいない**。
- **実証事業において、どうSBOMを活用すれば、導入効果が大きくなり、普及に繋がるか**を確認。

SBOM導入にかかるコスト

– 効果に対してどの程度のコストをかけるべきか判断に必要な情報が少ない。

– 多数のSBOMを手動で管理するとコストが膨大になるためツールによる自動化が考えられるが、下記のような課題が存在。

- ツールの導入コスト・ランニングコストが発生。
- ソフトウェアIDやSBOM形式が統一されていないなど、自動化の障害が存在。

SBOM生成・情報開示に対するサプライヤーの強い抵抗感

実証事業を踏まえた検討

- 企業がSBOMを活用するにあたって抱いている課題感を解決すべく、**2021年度から実証事業を開始**。
- 実証事業では、**SBOMの実際の効果やコストを算出**するとともに、**実際の活用方法についても検討**。この中で得られた**SBOM作成・導入のノウハウ**を踏まえて、**2023年7月にSBOM導入手引きを策定**。

	FY21	FY22
実証概要	• SBOM作成手段、作成者の条件を設定し、脆弱性管理やライセンス管理における**効果やコストを比較**し、今後の検討事項を整理 • 対象ソフトは、OSSの自動運転システム開発向け検証基盤ソフト • 中小企業への普及も考慮し、**無償ツールと有償ツール間も比較**	• 民間におけるSBOM活用の取組について、実際の**SBOM活用の方法等を検討** • SBOMに関して「規制や推奨化が見込まれる分野(**医療・自動車**)」や「効果が大きいと思われる分野(**ソフトウェア**)」を候補に、実証参加企業の選定、実証実施
成果	• SBOM作成・活用の工数感明確化 • 脆弱性特定における効果を確認	• **SBOM作成・導入のノウハウ** • SBOM活用の方法（対応範囲・取引状況等）
抽出課題	• SBOM**導入における初期工数**が発生 • 無償ツールにおける**ノウハウ不足** • ソフトウェア全体のうち**SBOM対応の範囲や責任の所在が不明瞭**	• SBOMを活用した**脆弱性管理の効率化** • **脆弱性マッチング**の高度化

2023年7月　手引きを策定・公開

ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引　～全体概要～　（2023年7月策定）

手引の背景・目的

- ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、ソフトウェアにおける脆弱性管理やライセンス管理の重要性が高まっている。
- ソフトウェア管理の一手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。
- 複数の産業分野における実証を通じ、SBOMを活用することで効率的なソフトウェア管理を実施できることが確認できた一方で、実際のSBOM導入に際しては様々なハードルが存在することが明らかとなった。
- 本手引では、**SBOMに関する基本的な情報やSBOMに関する誤解と事実を提供**するとともに、企業のSBOM導入を支援するために、**SBOM導入に向けた主な実施事項及び導入にあたって認識しておくべきポイント**を示す。

対象読者

- 主に、パッケージソフトウェアや組込みソフトウェアに関するソフトウェアサプライヤー※
  - ✓ ソフトウェア開発・設計部門
  - ✓ 製品セキュリティ担当部門（PSIRTなど）
  - ✓ 経営層
  - ✓ 法務・知財部門

※ このうち、以下に示すようなSBOM初級者を特に対象としている。

- ソフトウェアにおける脆弱性管理に課題を抱えている組織
- SBOMという用語は聞いたことがあるが具体的な内容やメリットは把握できていない組織
- SBOMの必要性は理解しているが、導入に向けた取組内容が認識できていない組織　など

SBOM導入の主なメリット

- **脆弱性管理のメリット**
  - ✓ 脆弱性残留リスクの低減
  - ✓ 脆弱性対応期間の低減
  - ✓ 脆弱性管理にかかるコストの低減
- **ライセンス管理のメリット**
  - ✓ ライセンス違反リスクの低減
  - ✓ ライセンス管理にかかるコストの低減
- **開発生産性向上のメリット**
  - ✓ 開発遅延の防止
  - ✓ 開発にかかるコストの低減
  - ✓ 開発期間の短縮

SBOM導入に向けたプロセス

フェーズ1　環境構築・体制整備フェーズ

- **1-1. SBOM適用範囲の明確化**
  - ✓ SBOMを作成する対象ソフトウェアに関する情報（言語、開発ツール、構成図、契約形態・取引慣行、規制要求事項、SBOM導入に関する組織内の制約等）を整理する。
  - ✓ 整理した情報を踏まえて、SBOM適用範囲を明確化する。
- **1-2. SBOMツールの選定**
  - ✓ SBOMツールの選定の観点を整理し、当該観点に基づきSBOMツールを評価・選定する。
    （選定観点の例：機能、性能、解析可能な情報・データ形式、コスト、対応フォーマット、解析方法、サポート体制、他ツールとの連携、ユーザーインタフェース、対応する言語、日本語対応等）
- **1-3. SBOMツールの導入・設定**
  - ✓ SBOMツールが導入可能な環境の要件を確認し、整備する。
  - ✓ 取扱説明書等を確認して、SBOMツールの導入・設定を行う。
- **1-4. SBOMツールに関する学習**
  - ✓ 取扱説明書等を確認して、SBOMツールの使い方を習得する。
  - ✓ ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する。

フェーズ2　SBOM作成・共有フェーズ

- **2-1. コンポーネントの解析**
  - ✓ SBOMツールを用いて対象ソフトウェアのスキャンを行い、コンポーネントの情報を解析するとともに、コンポーネントの解析結果について、コンポーネントの誤検出や検出漏れが無いかを確認する。
  - ✓ SBOMツールを用いることで、手動の場合と比較して効率的にコンポーネントの解析及びSBOMの作成を行うことができる。
  - ✓ パッケージマネージャーを用いることで、SBOMツールでは特定できない粒度の細かいコンポーネントを特定できる場合がある。
- **2-2. SBOMの作成**
  - ✓ 作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定し、当該要件を満足するSBOMを作成する。
- **2-3. SBOMの共有**
  - ✓ 対象ソフトウェアの利用者及びサプライヤーに対するSBOMの共有方法を検討した上で、当該方法に基づきSBOMを共有する。

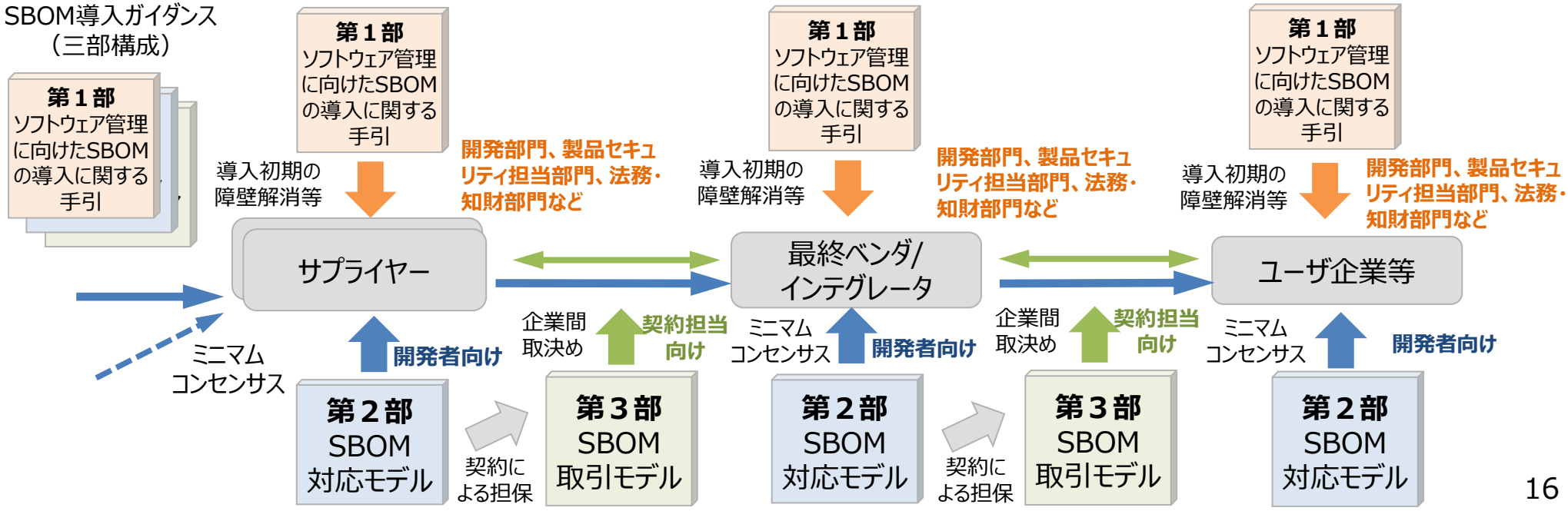
フェーズ3　SBOM運用・管理フェーズ

- **3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施**
  - ✓ 脆弱性に関するSBOMツールの出力結果を踏まえ、深刻度の評価、影響度の評価、脆弱性の修正、残存リスクの確認、関係機関への情報提供等の脆弱性対応を行う。
  - ✓ ライセンスに関するSBOMツールの出力結果を踏まえ、OSSのライセンス違反が発生していないかを確認する。
- **3-2. SBOM情報の管理**
  - ✓ SBOMに含まれる情報やSBOM自体を適切に管理する。
    ※ SBOMの管理は、組織内のPSIRTに相当する部門が対応することが効果的
  - ✓ 自動で脆弱性情報が更新・通知されるSBOMツールを用いることで、新たな脆弱性に関する情報を即座に把握することができる。ツールを用いた自動管理ができない場合、担当者を別途設置するなど運用面でカバーする。

今年度の実証結果等を踏まえた検討について

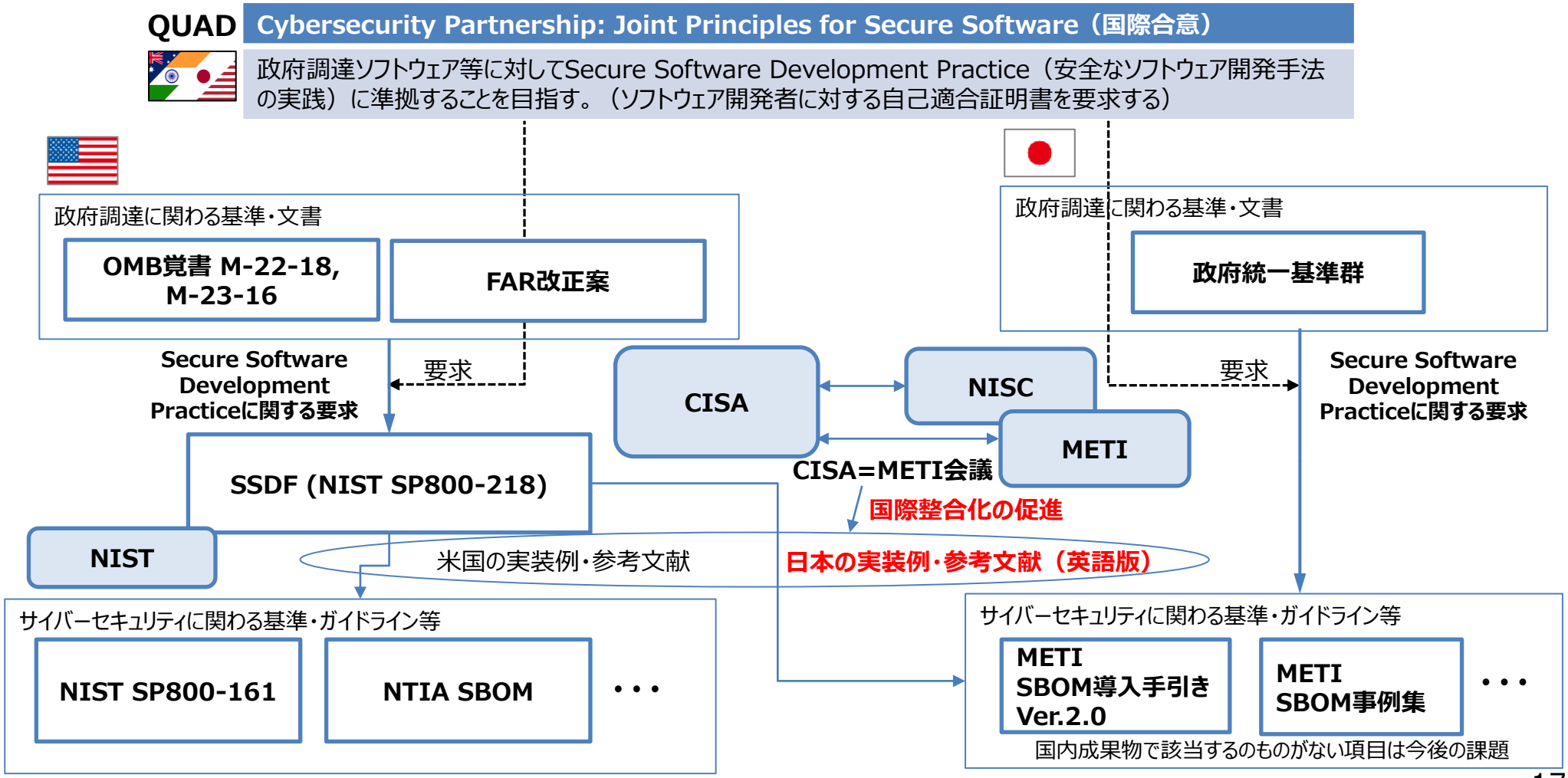
- 2023年度の実証事業では、**中小企業含む企業が活用**できるよう、**SBOMを活用した脆弱性管理の効率的な方法を検討**。また、SBOMのさらなる活用を促すべく、**SBOMを用いた部品の特定・脆弱性管理における対応範囲の可視化**や**契約における担保のあり方**についても検討。
- これらの実証結果については、SBOM導入手引きを改訂すべく、**本年2月に素案を提示**。今後、**パブリックコメントを経て、正式に公表予定**。

SBOM導入ガイダンスは、以下の３部から構成する。
第１部　ソフトウェア管理に向けたSBOMの導入に関する手引：導入初期の課題、阻害要因を解消するための開発者向けのヒント・TIPS等
【2023年7月公表済】。
さらに脆弱性管理プロセスの具体的な内容を取り込む予定**【今後公表予定】**。
第２部　対応モデル：業界として期待される開発者向けのSBOM対応レベル（ミニマム・コンセンサス）**【今後公表予定】**。
第３部　取引モデル：対応モデルを契約でどのように担保するか契約担当向けの例示。要件・責任関係の明確化**【今後公表予定】**。
※【今後公表予定】の内容は、Ver2.0に盛り込む予定。



SBOMの普及展開に向けて①

- **CISAとの会議を通じて**、**作成・改訂する参照文書・ガイドラインの国際的な整合化を図る**。
- QUAD国際合意に基づき、政府調達ソフトウェア等に対して、Secure Software Development Practiceの先行例である**SSDF(NIST SP800-218)に準拠**するため、**日本におけるSSDFの実装例・参考文献**として、**SBOM成果物、国内の基準・ガイドラインのマッピングを行う**。



SBOMの普及展開に向けて②

- **QUADで要求されるSSDF**のうち、プロセス・手法の例示と参考文献については、**各国の検討が必要に応じて求められる**。手法・プロセスの例示と参考文献のうちSBOMや脆弱性管理に係るものについて、**SBOM手引き、対応モデル、事例集等を対応づける**ことで、**日本企業にとっての負担を解消**するとともに、**SBOMの普及促進**を図る。

SSDFにおける各プラクティスの構成と日本におけるカスタマイズ取組の方向性

プラクティス(実践項目)	タスク(要件)	米国の実装例（手法・プロセス等）	参考文献
Practices	**Tasks**	**Notional Implementation Examples**	**References**
Provide a Mechanism for Verifying Software Release Integrity (PS.2): Help software acquirers ensure that the software they acquire is legitimate and has not been tampered with.	**PS.2.1**: Make software integrity verification information available to software acquirers.	**Example 1**: Post cryptographic hashes for release files on a well-secured website. **Example 2**: Use an established certificate authority for code signing so that consumers' operating systems or other tools and services can confirm the validity of signatures before use. **Example 3**: Periodically review the code signing processes, including certificate renewal, rotation, revocation, and protection.	**BSAFSS**: SM.4, SM.5, SM.6 **BSIMM**: SE2.4 **CNCFSSCP**: Securing Deployments—Verification **EO14028**: 4e(iii), 4e(ix), 4e(x) **IEC62443**: SM-6, SM-8, SUM-4 **NISTCSF**: PR.DS-6 **NISTLABEL**: 2.2.2.4 **OWASPSAMM**: OE3-B **OWASPSCVS**: 4 **PCISSLC**: 6.1, 6.2 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-8 **SP800161**: SA-8 **SP800181**: K0178
Archive and Protect Each Software Release (PS.3): Preserve software releases in order to help identify, analyze, and eliminate vulnerabilities discovered in the software after release.	**PS.3.1**: Securely archive the necessary files and supporting data (e.g., integrity verification information, provenance data) to be retained for each software release.	**Example 1**: Store the release files, associated images, etc. in repositories following the organization's established policy. Allow read-only access to them by necessary personnel and no access by anyone else. **Example 2**: Store and protect release integrity verification information and provenance data, such as by keeping it in a separate location from the release files or by signing the data.	**BSAFSS**: PD.1-5, DE.1-2, IA.2 **CNCFSSCP**: Securing Artefacts—Automation, Controlled Environments, Encryption; Securing Deployments—Verification **EO14028**: 4e(iii), 4e(vi), 4e(ix), 4e(x) **IDASOAR**: 25 **IEC62443**: SM-6, SM-7 **NISTCSF**: PR.IP-4 **OWASPSCVS**: 1, 3.18, 3.19, 6.3 **PCISSLC**: 5.2, 6.1, 6.2 **SCSIC**: Vendor Software Delivery Integrity Controls **SP80053**: SA-10, SA-15, SA-15(11), SR-4 **SP800161**: SA-8, SA-10, SA-15(11), SR-4
	PS.3.2: Collect, safeguard, maintain, and share provenance data for all components of each software release (e.g., in a software bill of materials [SBOM]).	**Example 1**: Make the provenance data available to software acquirers in accordance with the organization's policies, preferably using standards-based formats. **Example 2**: Make the provenance data available to the organization's operations and response teams to aid them in mitigating software vulnerabilities. **Example 3**: Protect the integrity of provenance data, and provide a way for recipients to verify provenance data integrity. **Example 4**: Update the provenance data every time any of the software's components are updated.	**BSAFSS**: SM.2 **BSIMM**: SE3.6 **CNCFSSCP**: Securing Materials—Verification, Automation **EO14028**: 4e(vi), 4e(vii), 4e(ix), 4e(x) **NTIASBOM**: All **OWASPSCVS**: 1.4, 2 **SCSIC**: Vendor Software Delivery Integrity Controls **SCTPC**: MAINTAIN3 **SP80053**: SA-8, SR-3, SR-4 **SP800161**: SA-8, SR-3, SR-4

QUAD内で共通項目として期待されると想定

米国における例示。必要に応じて各国の検討が求められる。

タスクに対する確立された手法の文献例。必要に応じて各国の検討が求められる。

- SBOMについては、PW4.1に部品のリスク評価のためSBOM等を取得すると抽象的に書かれている。
- 脆弱性対応についてプラクティスは3件、タスクは9件

SBOM手引き、対応モデル等をもとにプロセス・手法のカスタマイズ、具体化

SBOM手引き、対応モデル等で代替できるものを例示し、日本企業の対応の負担を軽減する。

SBOMの普及展開に向けて③

- **業界団体と連携**し**SBOM成果物を普及展開**することで、ソフトウェア管理の浸透を図る。
- **SSDFの適用**について、**実証事業を通じて妥当性評価等の検討**を行う。

各分野のステークホルダーとの連携を通じたSBOM普及促進

リスク区分※		分野等	規制・制度等	社会実装アプローチ（方針案） ステークホルダーとの連携等
規制・業法あり				
I	人命に影響	医療機器	薬機法，基本要件基準，JIS規格，手引書	基準・ガイドラインに関連付いた業界の解説文書、業界セミナーなどでSBOMガイダンスの参照・推奨を受けデファクト化を推進。(規制当局・認証機関におけるSBOMガイダンスの活用促進)
		自動車	保安基準、告示、協定規則	業界団体と連携し、会員向けにSBOM手引き、対応モデルの活用・推奨など働きかけを依頼。
		人命に係る重要インフラ（ガス等）	有り（一部自主規制）	—
II	社会・経済への波及的影響が大きい（重要インフラ）	電力等（重要インフラ）	有り（業法、自主規制）	関係省庁と連携を行う
		政府・行政	政府調達基準	関係省庁と連携を行う
		通信機器	技適・認証等	関係省庁と連携を行う
		重要ソフトウェア(OS,NW等)	任意、CC等	関係省庁と連携を行う
規制等なし				
III	社会・経済への影響が限定的 (波及範囲が狭い)	波及的影響が限定的なインフラ（B2B EC等）	自主規制等	関係団体と連携し、SBOM活用の方策についての検討を行う。
		セキュリティソフト	任意、CC等	関係団体と連携し、関連業界の普及を促進する。
IV	影響が個人・個社に限定	パッケージソフト、業務ソフト、SaaS	任意・認証等	業界団体と連携し、会員企業へのSBOM手引き・対応モデルの推奨、活用の働きかけを図る。パッケージ分野については、SSDF適用の実証事業を行い、適用可能性、マッピング妥当性の評価、国内文書類の不足等について検討を行う。
		コンシューマIoT機器	任意・ラベリング	既存制度の中でSBOMを促進すべく検討を行う

※高信頼化ソフトウェアのための開発手法ガイドブック(IPA)におけるリスク分類に基づき設定

（参考）産業界における自主的な取組

- **NTT・NECをはじめとした民間企業10社**が、「**セキュリティ・トランスペアレンシー・コンソーシアム**」を立ち上げ。**SBOM等の可視化データの活用**によって、セキュリティの透明性を高めることを目指す。その**活用過程での課題**に対して、**民間企業としての対処策をとりまとめ**、順次公表予定。
- こうした産業界における自主的な取組を慫慂しつつ、今後も引き続きSBOMの活用促進に向けた政策を進めていく。

【コンソーシアムの活動概要】

✓ **SBOMなどの可視化データの活用**によってサプライチェーンを通じてセキュリティの透明性を高め、製品・システム・サービス等に関する**サプライチェーンセキュリティリスクの低減**を目指す。

✓ その過程で**障害となる課題**（※）に対して、今後、コンソーシアムを通じた事業者によって、SBOMを含む可視化データ活用における各問題に関する対処策をまとめ、**「可視化データ活用に関する知見集（仮称）」としてとりまとめ**、2024 年春以降、順次公表。

（※）**社会的認知の不足、フォーマット・データの未整備技術・ツールの不足、活用コスト負担** 等

【参画企業】

アラクサラネットワークス株式会社／NRI セキュアテクノロジーズ株式会社／株式会社NTTデータグループ

株式会社FFRIセキュリティ／シスコシステムズ合同会社／東京エレクトロン株式会社

日本電気株式会社／日本電信電話株式会社／株式会社日立製作所／三菱電機株式会社

（出典）公開情報より作成。

目次

前回のWG1・分野横断SWG合同会議における主なご指摘

【産業分野別SWGについて】

- 中小企業対策について、例えば自動車業界はすそ野が広く、サプライチェーンに対するリスクを負っている。経産省が行っているサイバーセキュリティお助け隊サービスもあるが、なかなか普及が進んでいかないので、**国家レベルと業界とが補い合って相乗効果を出していけるような取組**を強化していきたい。また、中小企業もセキュリティ対策をやるのが当たり前というような相場観を、業界として醸成していくとともに、国としても、**法的、あるいはガイドラインのような形で強制力のある形でやらないといけないのではないか**。もしくは**セキュリティ対策をやったら得するといった宣伝活動も強化する必要**があるのではないか。
- 今回の資料では**経済面**としてどうなるという点がなかったが、そうした点もう少し**整理することが非常に重要**。また、デジタル臨調で全ての監視や管理をデジタル化するということを国の戦略として進めていくとされたが、サイバーセキュリティは当然、その前提として入ってくるというところを、デジタル臨調との整合性から**経産省として押し出していくことが必要**。そのとき経済面がKPIとしてKGIの１つとして入っていて、その際にどのような目標値となるかといった具体的な数字の議論ができるとよい。
- **工場ガイドライン**は、**一業界だけではなく産業界を横断する形で取り組まれることを期待**する。業界としても、サイバーセキュリティに関する相場作りのようなものや、標準化などに取り組んでいきたいという意識でいる。
- 工場ガイドラインは、ベースラインの部分は共有のナレッジという形にできればコストダウンに繋がるし、**業界ごとに特化した部分については業界ごとに定めていくという形で運用していければ非常に効率的**。

分野別SWGにおけるサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化

- **産業分野別サブワーキンググループ**を設置。CPSFに基づくセキュリティ対策の具体化を推進。
- 今後は、政府と産業界の協業を進めつつ、国際的なルール形成の推進に向けた取組や、**サプライチェーン全体のセキュリティ向上に向けた取組の実装**を進める。

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

ビルSWG

- 事前対策が中心の第1版にインシデントレスポンスを追加した**ガイドライン第2版を公開（2023年4月）**。
- **個別編(空調システム)ガイドライン第1版を公開（2022年10月）**。

防衛産業SWG

- 米国の新標準と同程度まで強化した**新情報セキュリティ基準を策定（2022年４月１日）**。

スマートホームSWG

- シンプルな対策ガイドから、具体的な対策要件や他の標準との対比まで、セキュリティ対策を階層的に整理し、**ガイドライン1.0版を公開（2021年4月）**。

宇宙産業SWG

- 宇宙分野における民間事業者の役割拡大や、米国等における官民の取組を踏まえ、2021年１月に立ち上げ。
- **ガイドライン1.1版を公開（2023年３月）。**

標準モデル（CPSF）

Industry by Industryで検討
（分野ごとに検討するためのSWGを設置）

電力SWG

- 電力分野のサイバーセキュリティを取り巻く現状、諸外国の状況を分析し、官民が取り組むべき課題と方向性について広く検討。**小売電気事業者ガイドラインを策定（2021年2月）**。

自動車産業SWG

- エンタープライズ領域（会社全体のベースとなるOA環境）対象とした**「自工会／部工会サイバーセキュリティガイドライン1.0版」を策定（2020年12月）し、サプライチェーンへの展開を実施**。**ガイドライン2.1版を公開（2023年9月）。**
- 工場領域や販売領域セキュリティの課題対応についても検討中。

工場SWG

- 業界団体や企業が自ら対策を企画実行するに当たり参照すべき考え方やステップを手引きとして**ガイドラインVer1.0版を公開（2022年11月）。**
- 工場をスマート化する際に留意すべき点や対策のポイント等についてまとめた**ガイドライン 別冊：スマート化に向けた対策ポイントを公開（2024年4月）。**

自動車産業SWG (一般社団法人　日本自動車工業会)

- 日本の自動車業界として対象のセキュリティフレームワーク・ガイドライン・実現レベルを定め、活用を推進することで、適切なセキュリティ対策の実施を図る。
- **2023年度は「自工会／部工会サイバーセキュリティガイドライン 2.1版」をサプライチェーンへ展開し自己評価の依頼**等を実施。

＜開催状況＞
- 2019年4月16日 第1回 電子情報委員会／サイバーセキュリティ部会を開催。
- 2020年12月4日 第1回 総合政策委員会／ICT部会／サイバーセキュリティ分科会を開催。
  （自工会の組織体制変更に伴い名称変更）
- 2021年度以降　**月1回の会合を継続して開催**し、自動車業界のサイバーセキュリティ対応を推進。

＜2022年度進捗＞
- 2022年３月に公開した**「自工会／部工会サイバーセキュリティガイドライン2.0版」をサプライチェーンに展開**し適用状況を集約。
- **21年度(1.0版)の回答2,300社に対し、22年度(2.0版)は約4,000社に増加。**
- 集計データ最終結果、自動車業界平均比較テンプレート活用方法の公表

＜2023年度進捗＞
- 自己評価結果の提出方法のシステム化に伴う入力項目追加と誤記修正を実施した**「自工会／部工会サイバーセキュリティガイドライン2.1版」を公開**。
- 2023年度の自己評価を実施のための自工会・部工会合同の説明会開催
- データ集計中であり、最終結果は例年通り３月末に公表予定
- 部工会と連携したサプライヤー向けの相談会やインシデント実例をもとにしたセミナーも開催

https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

工場SWG （座長：江崎 浩　東京大学 教授）

- 2022年1月6日に工場SWGを設置し、これまでに計7回開催。委員、オブザーバー、ヒアリング対象など、主な関係団体・企業も広く参画し、工場セキュリティガイドラインの策定に向けて活動。
- 2022年11月16日に**ガイドラインを公表**。**工場のスマート化に伴う対策のポイントをまとめた拡充版を、別冊として策定予定（現在パブコメ中）**。

開催実績

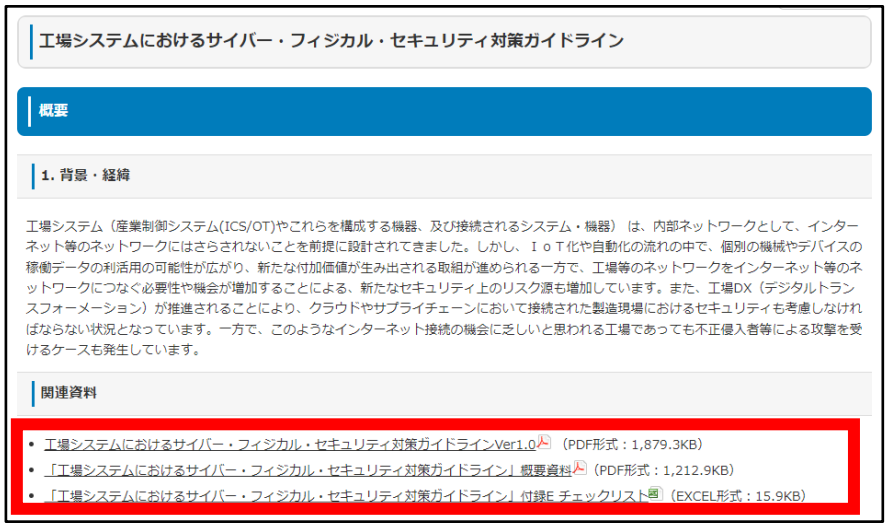
第１回　工場SWG設置について
第２回　主な産業界団体・企業からのヒアリング
第３回　パブコメに向けたガイドライン案の審議
第４回　パブコメ意見を踏まえたガイドライン案の審議
第５回　ガイドラインの普及に関する取組等について
第６回　ガイドラインの拡充版について

【拡充版 作業部会】
- 第1回：2023年10月30日
- 第2回：　〃　11月22日
- 第3回：　〃　12月6日
- 書面レビュー：〃 12月28日～翌年1月12日

第７回　ガイドライン拡充版 別冊(案) について

委員名簿

江崎 浩（座長）	東京大学 教授
岩﨑 章彦	電子情報技術産業協会
榎本 健男	日本工作機械工業会
桑田 雅彦	日本電気株式会社
斉田 浩一	ファナック株式会社
佐々木 弘志	フォーティネットジャパン株式会社
斯波 万恵	株式会社東芝
高橋 弘宰	トレンドマイクロ株式会社
中野 利彦	株式会社日立製作所
市岡 裕嗣	三菱電機株式会社
藤原 剛	ビー・ユー・ジーDMG森精機株式会社
松原 豊	名古屋大学　准教授
村瀬 一郎	技術研究組合制御ｼｽﾃﾑｾｷｭﾘﾃｨｾﾝﾀｰ
渡辺 研司	名古屋工業大学　教授


工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

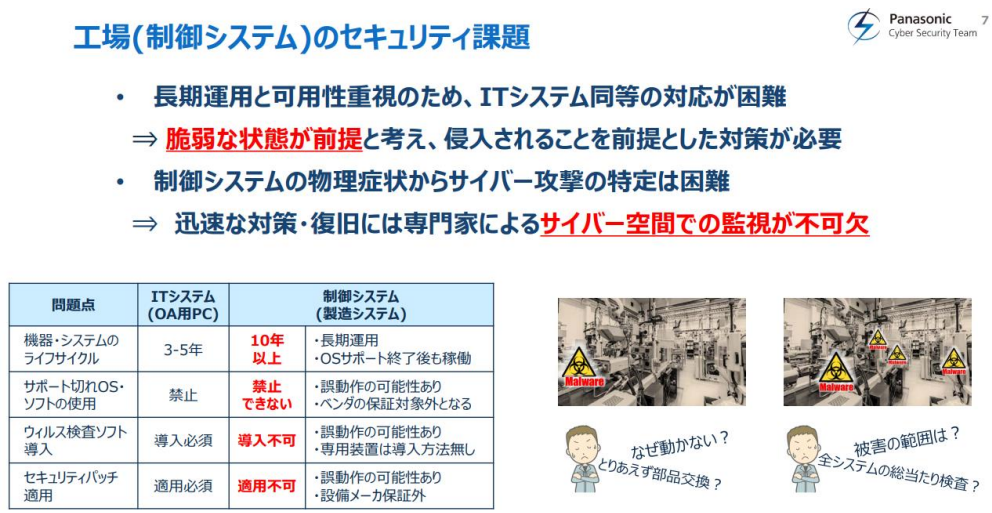
概要

1. 背景・経緯

工場システム（産業制御システム(ICS/OT)やこれらを構成する機器、及び接続されるシステム・機器）は、内部ネットワークとして、インターネット等のネットワークにはさらされないことを前提に設計されてきました。しかし、ＩｏＴ化や自動化の流れの中で、個別の機械やデバイスの稼働データの利活用の可能性が広がり、新たな付加価値が生み出される取組が進められる一方で、工場等のネットワークをインターネット等のネットワークにつなぐ必要性や機会が増加することによる、新たなセキュリティ上のリスク源も増加しています。また、工場DX（デジタルトランスフォーメーション）が推進されることにより、クラウドやサプライチェーンにおいて接続された製造現場におけるセキュリティも考慮しなければならない状況となっています。一方で、このようなインターネット接続の機会に乏しいと思われる工場であっても不正侵入者等による攻撃を受けるケースも発生しています。

関連資料

- 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインVer1.0（PDF形式：1,879.3KB）
- 「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」概要資料（PDF形式：1,212.9KB）
- 「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」付録E チェックリスト（EXCEL形式：15.9KB）



第2回 産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化） 工場サブワーキンググループ 資料4-2,4-4より抜粋
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/002.html

工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（概要）

ガイドラインの背景・目的

- 工場の**IoT化やクラウド活用によるネットワーク接続機会の増加**に伴いサイバー攻撃リスクが増加。また、ネットワークの接続が少ない工場であっても不正侵入者等による攻撃の可能性あり。
- 意図的な攻撃の場合もあれば、たまたま攻撃される場合もある。

→**いかなる工場でもサイバー攻撃のリスクあり**。

- 本ガイドは業界団体や個社が自ら対策を企画・実行するに当たり、**参照すべき考え方やステップを示した「手引き」**。

→**各業界・業種が自ら工場のセキュリティ対策を立案・実行**することで、**工場のセキュリティの底上げを図ることが目的**。

想定する読者の方

- ITシステム部門
- 生産関係部門（生産技術部門、生産管理部門、工作部門等）
- 戦略マネジメント部門（経営企画等）
- 監査部門
- **機器システム提供ベンダ、機器メーカ**
  （サプライチェーンを構成する調達先を含む）

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。
※事務系の情報システム（IT）は対象外。

対策に取り組む効果

- **工場のBC／SQDC※の価値がサイバー攻撃により毀損されることを防止**。
- **経営目標(事業伸長、継続の観点等)**との連関
- セキュリティが担保されることで**IoT化や自動化が進み、多くの工場から新たな付加価値**が生み出されていくことを期待。

※ 安全確保(S：Safety)、
事業／生産継続(BC：Business Continuity)
品質確保(Q：Quality)
納期遵守・遅延防止(D：Delivery)
コスト低減(C：Cost)

セキュリティ対策企画・導入の進め方

ステップ 1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
  セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2**　業務の整理
- **ステップ1-3**　業務の重要度の設定
- **ステップ1-4**　保護対象の整理
- **ステップ1-5**　保護対象の重要度の設定
- **ステップ1-6**　**ゾーン**の整理とその業務、保護対象の結びつけ
  （生産管理・監視、制御系、自動搬送、自動倉庫、リモートメンテナンス等）
- **ステップ1-7**　ゾーンと、セキュリティ脅威の影響の整理
  （**俯瞰化、別ゾーンへの影響の抑止、被害の抑制**）

ステップ 2　セキュリティ対策の立案

- **ステップ2-1**　セキュリティ対策方針の策定
- **ステップ2-2　(高・中・最低限)**
  想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策
① ネットワークにおけるセキュリティ対策
② 機器におけるセキュリティ対策
③ 業務プログラム・利用サービスにおけるセキュリティ対策

(2)物理面での対策
① 建屋にかかわる対策
② 電源／電気設備にかかわる対策
③ 環境(空調など)にかかわる対策
④ 水道設備にかかわる対策
⑤ 機器にかかわる対策
⑥ 物理アクセス制御にかかわる対策

ステップ 3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策

(1)ライフサイクルでの対策
① 運用・管理面のセキュリティ対策
A) サイバー攻撃の早期認識と対処
（OODAプロセス）
B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
C) 情報共有

②維持・改善面のセキュリティ対策
・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
・組織・人材のスキル向上（教育、模擬訓練等）

(2) サプライチェーン対策
・**取引先や調達先に対するセキュリティ対策の要請、対策状況の確認**

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」拡充版（案）

- 「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」に記載した実施事項と整合を取りつつ、**各ステップにおいてスマート化の際に留意すべき点や対策のポイント等について、別冊で整理**（**現在パブコメ中**）。

ドキュメントの目的・読み方

- 先進的な事業者が臆することなく工場のスマート化を進め、工場の価値創造を促進することを後押しする。
- 主に工場のスマート化を進める企業を読者に想定。**スマート工場の概要を示すとともに、ガイドライン本編に示した各ステップの対策におけるスマート化を進めるにあたっての留意点や具体例を示す**。

スマート工場で想定されるセキュリティリスク

- スマート工場では、**外部ネットワーク接続の増加**と**サプライチェーンの広がり**、これによりセキュリティリスクが増加することが想定される。

スマート工場でのセキュリティ対策のポイント

- スマート化に伴い留意すべき点に基づき、セキュリティ対策にあたっては、特に以下の点を考慮する。
  - **ゾーン設定の考え方：**
    スマート化では、目的に応じて業務の追加・高度化を行うため、**業務視点での詳細なゾーン（※）設定がより重要**である。ガイドライン本編では、ゾーンの重要性を示していたが、別冊では、**業務視点に基づいたより詳細なゾーン設定における考え方と留意点を記載**する。
  - **サプライチェーンの広がりに伴う責任分界や役割分担の考え方**
    スマート化では、外部機器やサービスの導入、自社の工場間や自社・他社間でのデータ流通が促進され、**自社のみで管理できない対象が増える可能性**が高いため、**対策の責任分界や役割分担がより重要**である。ガイドライン本編では、サプライチェーン対策を進める上でのポイントを示していたが、別冊では、**取引先・調達先に求めるセキュリティ要件における考え方を具体的に例示**する。

（※） 業務の内容や重要度が同等である領域を指すものであり、同じゾーンに存在する保護資産に対しては、同等の水準のセキュリティ対策が必要。

ビルSWG （座長：江崎 浩　東京大学 教授）

- **2023年4月にガイドライン第2版を策定し**、当該SWG内外を問わず**ガイドラインの拡張・充実化**が進んでいるため、**業界の自主的取組への移行が期待**される。
- 現在、IPAを中心に設置が検討されている**スマートビルアソシエーション(仮称)下のセキュリティWGへの合流**を検討中。

時期	内容
2018年2月	**ビルSWG設置** ：ビルオーナーを始め、建設会社、設計事務所、ビルに係わる各種設備機器のベンダ、制御システムセキュリティの有識者など、多数のステークホルダーが一堂に会し、ビルシステムに関するサイバーセキュリティ対策のガイドラインを議論。
2019年6月	**ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版の策定** ：CPSFに基づいてビルシステムに対するサイバーセキュリティ対策についてまとめた共通編ガイドラインとして策定。 ＜背景＞ 近年のサイバー攻撃技術の高度化や、様々なシステムが益々ネットワークに繋がっていく状況の中、制御システムへのサイバー攻撃リスクも高まってきている一方で、ビルシステムに関するサイバーセキュリティ対策は遅れていた。
2022年10月	**ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（個別編：空調システム第1版の策定）** ：共通編ガイドラインに加え、ビルの個別のサブシステムに特化した内容をまとめた個別編ガイドラインとして策定。 ＜背景＞ ガイドラインは共通編及び個別編の2階建てで作ることとしていた。共通編が出来上がったことを受け、個別編の議論に入り、当初より要望のあった空調分野でまず検討が開始された。
2023年4月	**ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第2版の策定** ：インシデントレスポンスに係る内容を共通編ガイドラインに組み込む形で策定。 ＜背景＞ スマートビル化の進展により、ビルシステムがサイバー攻撃を受ける可能性はより高まっている。事前対策でサイバー攻撃を受ける可能性を抑止するとともに、それでもサイバー攻撃（サイバーインシデント）を受けてしまった場合に、その損害を最小限に抑え、復旧にかかる時間とコストを削減するための取組（インシデントレスポンス）が重要。

ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第2版の構成

目次

主に教育・啓発的内容
・なぜビルのサイバー対策が必要か？
・誰が考えるべきか？

第2版で**インシデントレスポンス**のエッセンスを追加

主にガイドラインの作り／考え方
・対象システムのモデル
・対策を導き出す思考アプローチ

対象ごとの考え得る**インシデント、リスク源、対策（ポリシー）**をワンセットで記載

さらに詳細な対応を、**ビルのライフサイクルのそれぞれの場面にブレークダウン**（別表としてインデックス化）

サイバー攻撃（インシデント）の発生時に、その損害を最小限に抑え、復旧にかかる時間とコストを削減するための取組を記載

実装レベルの対策（対策の具体的解説や、実際の対策事例）は、関係者のみで共有

宇宙産業SWG（座長：坂下 哲也 JIPDEC 常務理事）

- **<u>2023年3月にガイドライン1.1版を公開</u>**。2023年度は2.0版への改訂に向けてスコープの拡大、セキュリティ関連規程雛形の追加、具体的な対策内容の追記等について議論。
- また、宇宙事業者が抱える情報共有に関する課題・ニーズを踏まえ、国内の宇宙分野における**<u>情報共有体制のあり方について検討。</u>**

「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン」に関する取組

産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化）宇宙産業サブワーキンググループ 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1

経済産業省では、産業サイバーセキュリティ研究会ワーキンググループ1（制度・技術・標準化）宇宙産業SWGの下で、「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1」を策定しましたので、公表します。

本ガイドラインは、民間宇宙事業者のビジネス振興及びサイバー攻撃による倒産等の経営リスク軽減の観点から、
- 宇宙システムに係るセキュリティ上のリスク
- 宇宙システムに関わる各ステークホルダーが検討すべき基本的セキュリティ対策
- 対策の検討に当たり参考になる参考文献、活用可能な既存施策 等

について分かりやすく整理して示し、民間事業者における自主的な対策を促すことを目的としています。

和文

- 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver1.1（PDF形式：4,464KB）
- 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.1 概要資料（PDF形式：1,788KB）
- 【添付資料1】対策要求事項チェックリスト（Excel形式：16KB）
- 【添付資料2】NIST CSFと宇宙システム特有の対策との対応関係（Excel形式：20KB）

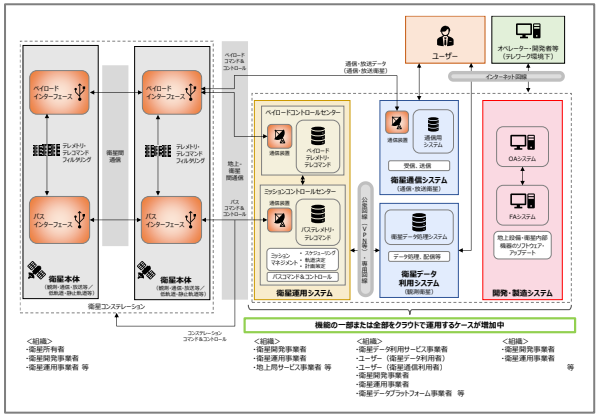
英文

- Cybersecurity Guidelines for Commercial Space Systems Ver 1.1（PDF形式：2,846KB）
- Cybersecurity Guidelines for Commercial Space Systems Ver 1.1 (Summary)（PDF形式：665KB）
- 【Attachment 1】Checklist of Requirements and Measures（Excel形式：15KB）
- 【Attachment 2】Correlation between NIST CSF and Specific Measures for Space Systems（Excel形式：18KB）

- 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0

～2022年度：
ガイドライン1.0版/1.1版に関する議論、公開

民間宇宙システムの標準的なモデル



セキュリティ関連規程雛形

2023年度：
ガイドライン2.0版への改訂に向けた議論
（スコープの拡大、セキュリティ管理規程雛形の追加、具体的な対策内容の追記等）

目次

前回のWG1・分野横断SWG合同会議における主なご指摘

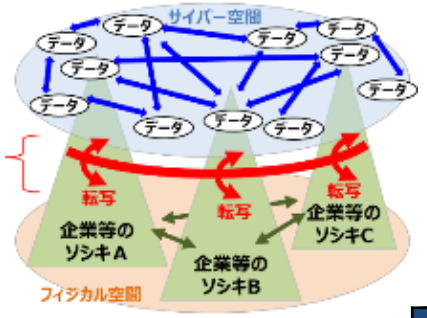
【CPSFの国際規格化について】

- サイバーフィジカルシステムの概念モデルに基いた海外の考え方も吸収した形で全体の規格にしていこうとしている。今後、ユースケースを具体的に入れていくなどのフレームワークを具現化していくアプローチで進めていく予定。今後このような国際基準を進めていく中で、具体的に標準を作る時に、**経済産業省で行っている事業の成果やガイドライン等を標準に入れていくのがよい**。

サイバー・フィジカル・セキュリティ対策フレームワークが盛り込まれた国際規格の策定

- ISO/IECの国内エキスパートの協力のもと、**CPSFのモデル等を盛り込んだ国際規格（TS:技術仕様書）策定**を推進。現在、**ISO/IEC JTC1/SC27**にてTS 5689としてプロジェクトが進行中。
- 2023年10月に**NP投票（提案段階）**が行われ、賛成27票(内、積極参加8カ国)、反対1票、棄権27票となり、棄権除く2/3以上賛成および積極参加5カ国以上を満たして**可決**。
- **WD（作成段階）へ移行**し、**最終的な投票にかけるTS原案(DTS)を策定中**。**2024年度中にDTS投票を行う予定**で2/3以上の賛成を得た場合**TSが成立し**、**2025年度早々の発行を目指す**。

CPSFのモデル



CPSFのモデル
・「3層構造」
・「6つの構成要素」
を盛り込んだドラフトを提案

国際標準化団体へ提案

ISO / IEC
JTC 1
SC 27
WG 4

※ 下図において、「会合」とは、SC 27/WG 4で通常4月周辺、10月周辺に年2回開催される定期会合を指す。「中間会合」とは、上記に示す定期的な会合とは別に、アドホックに開催されるプロジェクト単位の会合を指す。

区分	2023年度		2024年度				2025年度
国際標準化提案先イベント	2023/4 会合 ★	2023/10 会合 ★	2024/4 会合 ★	2024/7 中間会合 ★	2024/10 会合 ★	2025/2 中間会合 ★	
CPSFをベースとした国際標準化ステップ	**NP(再)** PWI(再)で検討した内容をベースに再度投票を実施する。		**作成段階** ・担当する委員会の指名するエキスパートが作業原案(WD)を作成する。		**承認段階** ・委員会メンバーの2/3以上の賛成を得ることで、原案を技術仕様書として発行するよう要請できる。		▲ **国際規格(TS等)発行**

目次

先進的サイバー防御機能・分析能力強化のための研究開発

- 深刻化するサイバー攻撃に対して、サイバー防御機能や分析能力の強化につながる技術を確保することが重要。
- 経済安全保障重要技術育成プログラムにおいて、経済安全保障の確保・強化の観点から、「サイバー空間」を支援すべき重要技術とし、**サイバー空間の状況把握力や防御力の向上に資する技術**や、**セキュアなデータ流通を支える暗号関連技術**等の研究開発を実施予定（320億円を超えない範囲／5年）。
- 2023年10月に具体的な研究開発の構想を決定。これに基づき、同年12月に公募を開始し、外部有識者による審査等も踏まえた上で、実施事業者を採択。**本年5月頃から研究開発を開始予定**。

目　的

- サイバー空間において提供される多様なサービスが複雑化するに伴い、サイバー空間内やサイバーとフィジカルの垣根を超えた主体間の「相互連関・連鎖性」が一層深化。近年では、**人工知能（AI）**を活用した攻撃に代表される**新たなサイバー攻撃のリスク**や、**量子計算機の活用**の広がりに伴う**既存暗号の危殆化によりデータが漏洩するリスク**が顕在化。
- **サイバー空間の状況把握力や防御力の向上に資する技術**や、**セキュアなデータ流通を支える暗号関連技術**等を開発し、我が国のサイバー領域における状況把握力・防御力を飛躍的に向上させることを目的とする。

実施内容

（１）サイバー空間の情報を収集・調査する状況把握力の向上

- アーティファクト分析技術／攻撃者からより多くの情報を獲得するための技術／高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

（２）サイバー攻撃から機器やシステムを守る防御力の向上

- AIを活用した脆弱性探査技術／AI等を活用した防御能力の評価・向上技術／AIを活用したOTペネトレーションフレームワーク技術
- 耐量子計算機暗号技術／耐タンパー性向上技術

（３）共通基盤の整備

- 情報の効果的な連携に関わる技術
- 高度サイバー人材の評価・管理に関する技術

（４）セキュアな量子情報通信技術の開発

- Y-00のデジタルコヒーレントの開発／Y-00の高速光ファイバ通信の開発／Y-00の高速光ワイヤレス通信の開発