経済産業省

ソフトウェアセキュリティに関する経済産業省の施策について

2025年2月

商務情報政策局サイバーセキュリティ課

見次　正樹

目次

サイバー攻撃を行う主体について

①国家の支援を受けたグループ（APT（Advanced Persistent Threat）攻撃グループ）

- 執拗に高度で継続的な攻撃を行うことが特徴（つまり、ミッション達成優先でコスト度外視の攻撃集団）。インテリジェンス企業によれば、攻撃グループのバックについている国として中国、ロシア、北朝鮮、イラン、ベトナムが挙げられている。

②サイバー犯罪組織（クライム（Crime）系）

- 情報等を盗んで現金化するグループ。2018年の被害総額は60兆円に達したという調査結果もあるようで、既に一大市場となっており、攻撃用ツール制作・販売、攻撃起点の時間貸しなど、様々な犯罪サービスの分業化が進展。

③ハクティビスト

- 「アクティビスト（社会活動家）」と「ハッカー」を掛け合わせた言葉で、サイバー攻撃を通じて社会的・政治的メッセージを発信していくことを主眼とした活動を行うグループ。アノニマスもハクティビストと捉えられることが多い・

④悪意のある個人（愉快犯、腕試し等）

- 趣味や研究の延長として個人が行う攻撃で、子供が行っているケースも少なくない。ただし、②の攻撃用ツールを使ったりしているうちに犯罪グループの活動に取り込まれているようなことも。

⑤産業スパイ

- 知的財産の窃取を目的とした攻撃グループ。

※実態は、上記のようにきれいに分類することは困難。例えば、普段はクライム系として活動しているグループが、要請に応じて“傭兵”となってAPT攻撃グループとして働いている可能性が指摘されている。

主なサイバー攻撃事案

①個人情報や機微技術情報などが情報窃取される

- **米国SolarWinds事案（2020年12月）**主要政府機関等のシステムが2019年9月から不正アクセスを受けていたことが発覚。極めて高度な攻撃手法を用いて検知体制をすり抜けていたが判明。

②ランサムウェア攻撃やBEC (Business E-mail Compromise)などにより金銭等資産が奪われる

- **JALビジネスメール詐欺被害公表（2017年12月）**ビジネスメール詐欺で3.8億円の被害を被る。

③データ改ざんやフェイク情報拡散などによって意思決定・指示が歪められる

- **米国大統領選挙に対するロシアの干渉疑惑（2016年）**ロシア攻撃集団がサイバー攻撃やSNSを使ったプロパガンダを展開したとして、オバマ政権はロシア外交官３５人国外退去処分等の制裁を実施。

④事業活動が停止に追い込まれる

- 自動車部品メーカーが、ランサムウェア攻撃を受けサーバがダウン。同社と連係関係にある自動車メーカーは、**国内全工場の稼働を１日間停止**。（2022年３月）

⑤社会インフラの誤作動・機能停止により社会全体に被害が発生する

- ウクライナでは、**サイバー攻撃による大規模な停電が複数発生**（2015年12月、2016年12月、2022年10月）
- **名古屋港のコンテナターミナル**において、ランサムウエア攻撃によるシステム障害が発生し、**約3日間コンテナの搬入・搬出が停止**。（2023年７月）

デジタル技術の発展とサイバーリスクの増加

- 社会のデジタル化は進展する一方、AI等のデジタル技術の発展や地政学情勢の不安定化の影響もあり、**サイバー攻撃は今後ますます増加するとともに高度化・複雑化していくおそれ。**

デジタル技術の発展によるサイバーリスクの増加の例

■ 情報システムの利用拡大やクラウド等の活用拡大、インターネットに接続されるIoT製品の急増（2019年：231億台 ⇒ 2024年：399億台）など**サイバー空間の利用拡大**等に伴い、サイバー攻撃を受ける**システム側の侵入口が増加**。

■ スピアフィッシングやビジネスメール詐欺等の実行を支援する**サイバー犯罪用の生成 AI ツールも登場**。

□ NICTER において2023年に観測した**サイバー攻撃関連通信数は増加傾向**であり、約6,197億パケット（2018年の約３倍）。中でも、**IoT機器を狙った攻撃関連通信が多い**。

□ フィッシング対策協議会によると、2023年における**フィッシングの報告件数は100万件超**（2019年の約20倍まで増加）。

（出典）総務省「令和 5 年度版情報通信白書データ集」、(独)情報処理推進機構（IPA）「情報セキュリティ10大脅威 2024」解説書、(国研)情報通信研究機構「NICTER観測レポート2023」、フィッシング対策協議会「月次報告書」 等

サイバー攻撃の現状

- 企業等の情報を暗号化して金銭をゆすり取る「**ランサムウェア攻撃**」やセキュリティ対策に弱点のある取引先等が攻撃経路として狙われ、被害が拡大する「**サプライチェーンの弱点を悪用した攻撃**」により、甚大な影響が生じている。また国家支援型の攻撃集団等が特定の企業を執拗に狙う「**標的型攻撃**」も大きな課題。
- 社会のデジタル化は進展する一方、AI等のデジタル技術の発展や地政学情勢の不安定化の影響もあり、**サイバー攻撃は今後ますます増加するとともに高度化・複雑化していく**おそれがある。
- 相対的にセキュリティの弱い**中小企業の対策強化**を我が国全体で進める必要がある。

情報セキュリティ10大脅威 2024	
順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	内部不正による情報漏えい等の被害
4位	標的型攻撃による機密情報の窃取
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6位	不注意による情報漏えい等の被害
7位	脆弱性対策情報の公開に伴う悪用増加
8位	ビジネスメール詐欺による金銭被害
9位	テレワーク等のニューノーマルな働き方を狙った攻撃
10位	犯罪のビジネス化（アンダーグラウンドサービス）

中小企業の被害が全体の約6割を占める

相対的にセキュリティ対策の弱い中小企業を起点に、大企業含むサプライチェーンを共有する企業を攻撃

<出典：(独)情報処理推進機構(IPA)、2024.1.24>

国家のサイバーセキュリティの改善に係る米国大統領令の署名

- 2021年5月12日、バイデン大統領は、連邦政府機関におけるサイバーセキュリティ改善に係る大統領令に署名。
- 官民での脅威情報の共有、**ソフトウェアサプライチェーンセキュリティ対策**の強化、ゼロトラストアーキテクチャへの移行等を通じて、連邦政府機関のサイバーセキュリティ対応能力の向上を図っている。

1. 官民の脅威情報共有における障害の除去 (Section 2)
2. 連邦政府におけるより強力な標準の近代化と導入 (Section 3)
3. **ソフトウェア・サプライチェーンのセキュリティ向上 (Section 4)**
4. サイバー安全審査委員会の創設 (Section 5)
5. インシデント対応のための標準プレイブックの策定 (Section 6, 7)
6. 調査及び修復能力の向上 (Section 8)

- NISTを通じて**政府が調達するソフトウェアの開発に関するセキュリティ基準**(安全な開発環境の確保や構成要素に関する詳細**（SBOM）の開示等を含む)を確立**し、特に**重要なソフトウェアに対して一定の対策を義務づける。**
- 商務省は、既存のラベル表示などを参考にして、消費者向けの情報提供に関するパイロット制度を開始する。

- 大統領令では、**ソフトウェア・サプライチェーンの確保に向け、NISTが中心となりガイドラインを策定する**旨を指示しており、この**ガイドラインには製品購入者に対するSBOM提供に関する項目も含まれる。**
- 将来的には、公開されたソフトウェア・サプライチェーンに関するガイダンスの要求事項に基づき、**連邦政府のソフトウェア調達に関するFAR（連邦調達規則）が改正される予定**である。

国際動向①：重要インフラ事業者等への義務

- 欧米を中心に、**重要インフラ事業者等のサイバーセキュリティ対策を義務化する動きが加速。**

重要インフラ事業者等（各国定義）

重要インフラに係るサイバーインシデント報告法案
（Cyber Incident Reporting for Critical Infrastructure Act of 2022）

- 米国の16の「重要インフラ」セクターに対し、**①重大なサイバーセキュリティインシデント**について発生を認知後**72時間以内**、**②ランサム支払い**について支払い後**24時間以内に米CISAに報告すること等を義務付け**。
- 2022年3月に成立、2024年4月に規則案公表。施行は2025年秋を想定。

NIS 2指令
（Directive (EU) 2022/2555）

- **2016年NIS指令から対象セクターを拡大**の上、対象「主要エンティティ」、「重要エンティティ」に対し、**①サイバーセキュリティ・リスクマネジメントの強化**、**②重大なサイバーセキュリティインシデントについて**発生を認知後**24時間以内に早期警告、72時間以内にインシデント通知をCSIRT又は管轄省庁に報告すること等を義務付け**。
- **2023年1月発効、2024年10月18日より執行予定**、それまでに加盟国が国内法に反映予定。

その他事業者

米国証券取引委員会開示規則（SEC Form 8-K）

- 登録企業に対し、①サイバーセキュリティインシデントに重要性があると判断してから**4営業日以内に、当該インシデントの性質、影響等の開示**、**②リスク管理、戦略、ガバナンスの年次開示等を義務付け**。
- 2023年7月に採択、2023年12月18日より運用開始。

国際動向②：製造者・製品へのセキュリティ要件

- **セキュア・バイ・デザイン*1の概念が国際的に支持*2を集める**など、企業は自社をサイバー攻撃から守ることのみならず、**自社が提供する製品のサイバーセキュリティ対策についても問われる時代に**なりつつある。

*1 IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていることを指す。
*2　日米含む13か国の政府機関等が2023年10月にセキュア・バイ・デザイン等の実践に向けた推奨事項をまとめたガイダンスに共同署名。

IoT製品等

サイバーレジリエンス法案
（Cyber Resilience Act）

- **デジタル要素を備えた全ての製品（ソフトウエア含む）の製造者に対し、**①セキュリティ特性要件に従った**上市前の設計製造**、② **上市後に積極的に悪用された脆弱性・インシデントの報告等を義務付け。**
- 2024年後半に発効見込み。**報告義務の運用開始は2025年秋～冬、その他は2027年夏頃運用開始を想定。**

米国サイバー・トラスト・マーク
（U.S. Cyber Trust Mark）

- **消費者向け無線IoT製品を対象とした、任意のラベリング制度。**消費者向けルータ、スマートメーター等**一部製品については、個別のセキュリティ要件が定義される見込み。**
- 2024年7月に最終規則公表。**2024年中に制度運用開始**を予定。

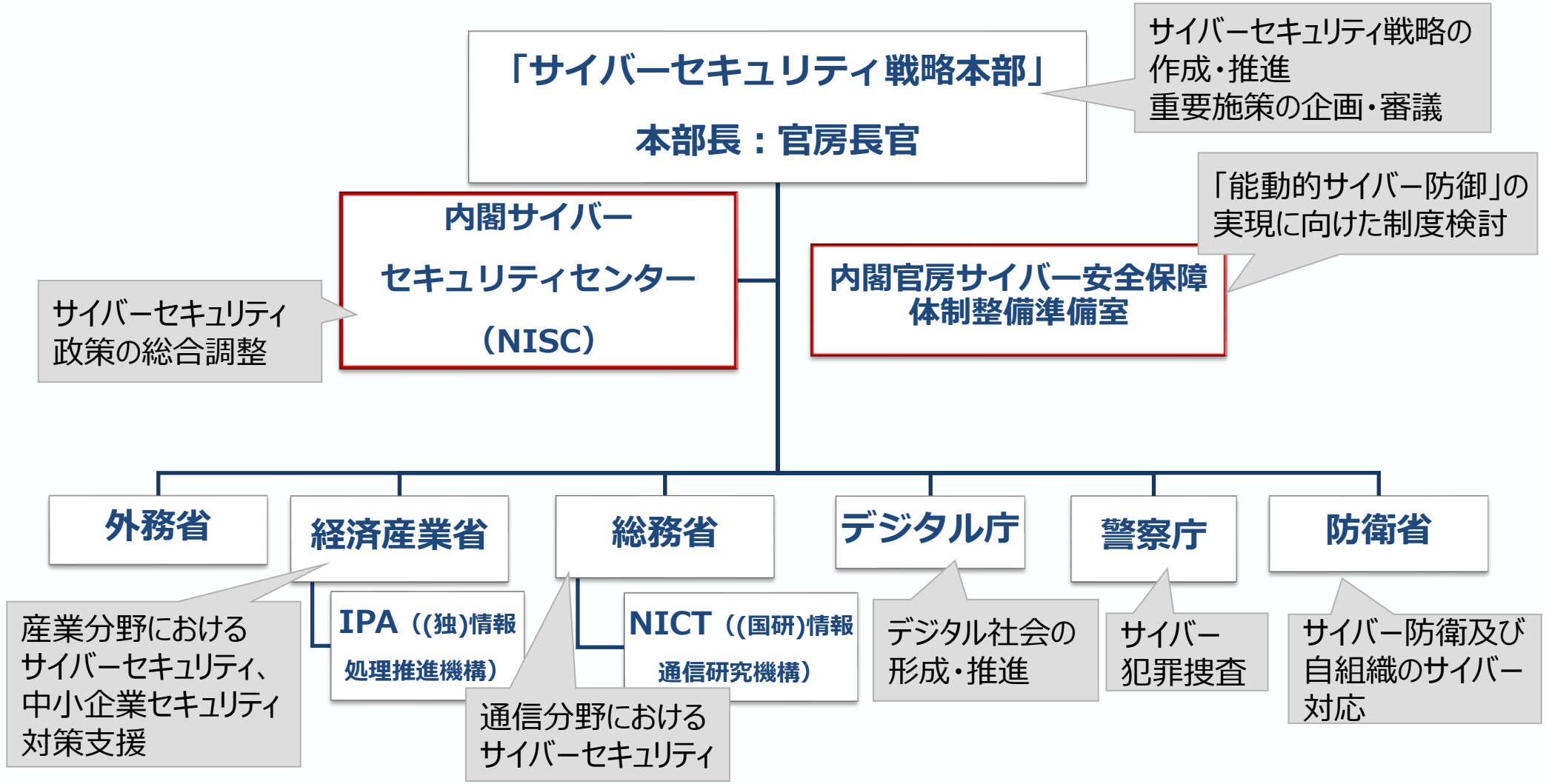
PSTI法
（Product Security and Telecommunication Infrastructure Act）

- **消費者向けIoT機器の製造者に対し**、デフォルトパスワードを使用しない等の**最低セキュリティ基準への自己適合宣言を義務化。**
- 2022年12月に国王裁可し、下位法制定を経て**2024年4月に施行された。**

目次

サイバーセキュリティ政策の推進体制

- サイバーセキュリティ戦略本部（本部長：官房長官）の下、内閣サイバーセキュリティセンター（NISC）が総合調整を行い、各省が所管分野におけるサイバーセキュリティ政策を担う。



サイバー安全保障の確保に向けた法制度整備（内閣官房）

- 国家安全保障戦略を踏まえ、重大なサイバー攻撃を防ぐために未然に攻撃者のサイバー等への接続・無害化を行うなどの「**能動的サイバー防御**」の導入に向けた制度整備に向けた検討を、内閣官房中心に継続。
- **昨年6月7日に「サイバー安全保障分野での対応能力の向上に向けた有識者会議」での検討を開始**し、**11月29日に「サイバー安全保障分野での対応能力の向上に向けた提言」をとりまとめ。**
- **本年2月7日に「サイバー対処能力強化法案及び同整備法案」※が閣議決定。** ※重要電子計算機に対する不正な行為による被害の防止に関する法律案及びその施行に伴う関係法律の整備等に関する法律案

国家安全保障戦略（令和４年12月16日閣議決定）の概要

- 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれを未然に排除、または攻撃が発生した場合に被害の拡大を防止するために**能動的サイバー防御を導入**する。このため以下の必要な措置の実現に向け検討を進める。

ア）官民連携の強化

：重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への支援等の強化

イ）通信情報の利用

：国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するための取組

ウ）アクセス・無害化

：国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限を付与

→上記取組を実現・促進するために、NISCを発展的に改組　等

サイバー安全保障の有識者会議の提言概要①

提言の概要

（１）官民連携の強化

- 政府から**基幹インフラ事業者等に**、事業者の**サイバー攻撃対処に必要な情報を提供**
- 基幹インフラ事業者に政府への**サイバー攻撃被害の報告を義務付け**
- 基幹インフラ事業者に対し、インフラ停止等につながる**重要コンピュータ等の届出を義務付け**
- 重要な事業者に被害情報の提供を促す**「情報共有会議（仮称）」を新設**
- 脆弱性情報の提供やサポート期限の明示など、**ベンダが利用者とリスクコミュニケーションを行うべき旨を法的責務**として位置づけ

（２）通信情報の活用

- 一定の条件下での**通信情報の利用を検討。**国外が関係する通信は分析の必要が特に高い（①外外通信に加えて、②外内通信(国外から国内への通信）及び内外通信(国内から国外への通信)についても分析）。
- **コミュニケーションの本質的内容に関わる情報は分析せず**に、機械的に絞る等の工夫。
- **独立機関が取得・情報処理のプロセスを監督**
- なお、**通信当事者の有効な同意**がある場合の**通信情報の利用**は、同意がない場合とは**異なる内容の制度により実施も可能**（制度により、基幹インフラ事業者の同意を促す）

サイバー安全保障の有識者会議の提言概要②

提言の概要

（３）侵入・無害化措置

- **サイバー攻撃元のコンピュータにアクセス・無害化等できる権限を整備**
- 内閣官房（新組織及び国家安全保障局）の総合調整の下、**まずは警察がアクセス・無害化等を実施**
- 公共の秩序維持の観点から**特別の必要がある場合に自衛隊と共同で対処**　等

（４）横断的課題

- **サイバーセキュリティ戦略本部の構成等の見直し**とともに、政府の司令塔として機能すべく**NISCの発展的改組**
- **重要インフラのレジリエンス強化のため、セキュリティ水準の提示**とともに、政府機関等についても**国産技術を用いたセキュリティ対策を推進**
- **セキュリティ人材の定義の可視化**を行い人材育成・確保の各種方策を自ら実践しながら、**官民の人材交流を強化**
- サプライチェーンを構成する**中小企業等のセキュリティについて、意識啓発や支援拡充、対策水準等を検討すべき**。

重要電子計算機に対する不正な行為による被害の防止に関する法律案
及び　その施行に伴う関係法律の整備等に関する法律案　　の概要

趣　旨

- 国家安全保障戦略（令和４年12月16日閣議決定）では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④***NISC*の発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置**　等の実現に向け検討を進めるとされた。
- 国家安全保障戦略に掲げられたこれら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、サイバー安全保障分野での対応能力の向上に向けた有識者会議を開催（令和６年６月７日～11月29日）、「サイバー安全保障分野での対応能力の向上に向けた提言」を取りまとめ。

→　これらを踏まえ、「新法」及び「整備法」として必要な法制度を整備。

概　要

官　民　連　携　（新法）

- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告
- 情報共有・対策のための協議会の設置
- 脆弱性対応の強化

通信情報の利用　（新法）

- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得
- （同意によらない）通信情報の取得
- 自動的な方法による機械的情報の選別の実施
- 関係行政機関の分析への協力
- 取得した通信情報の厳格な取扱い
- 独立機関による事前審査・継続的検査　等

→ 分析情報・脆弱性情報の提供等 ←

アクセス・無害化措置　（整備法）

- 重大な危害を防止するための警察による無害化措置
- 独立機関の事前承認・警察庁長官等の指揮 等
  （警察官職務執行法改正）
- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・在日米軍が使用するコンピュータ等の警護（権限は上記を準用）　　等
  （自衛隊法改正）

組織・体制整備等　（整備法）

- サイバーセキュリティ戦略本部の改組　（サイバーセキュリティ基本法改正）
- サイバーセキュリティ戦略本部の機能強化　（サイバーセキュリティ基本法改正）
- 内閣サイバー官の新設　（内閣法改正）　　等

施行期日

公布の日から起算して１年６月を超えない範囲内において政令で定める日　　等

サイバーセキュリティ戦略本部第42回会合資料2-1

サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項について

社会全体へのDXの浸透や、AI・量子技術等の進展により、急速に変化するサイバー空間をめぐるリスクに対応するため、「サイバーセキュリティ戦略」（特にサイバーセキュリティ2024における「特に強力に取り組む施策」）及び「サイバー安全 保障分野での対応能力の向上に向けた提言」等を踏まえ、現行制度下において喫緊に取り組むべき事項について検討 し、対処方針を示す。

サイバーセキュリティ2024（特に強力に取り組む施策）

- 政府機関や重要インフラ等の対処能力の向上
- サプライチェーン・リスクへの対応強化
- DXを推進・支援する取組の強化
- 欧米主要国をはじめとする関係国との連携の一層の強化　等

サイバー安全保障分野での対応能力の向上に向けた提言（横断的課題等）

- 政府機関や重要インフラ事業者等の対策強化
- サイバーセキュリティ人材の育成・確保
- 中小企業や地域における対策強化
- 国産セキュリティ製品・サービスの供給強化
- 被害組織の負担軽減（報告様式一元化）

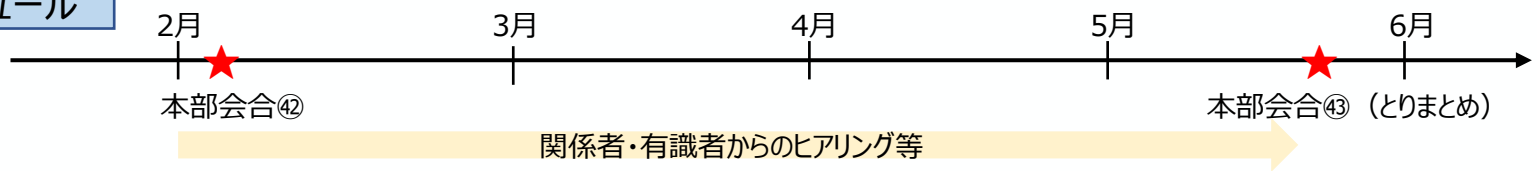
等

検討事項（案）

- 政府機関・重要インフラ事業者等の対応能力の向上
- 社会全体のサイバーセキュリティ確保
  - 官民連携の強化
  - セキュアバイデザイン・セキュアバイデフォルト原則等を踏まえた対策強化
  - 中小企業のサイバーセキュリティ対策の促進
- 国際連携の一層の強化
- 横断的施策の推進
  - サイバーセキュリティ人材の育成・確保
  - 我が国のサイバーセキュリティ技術の研究開発・活用及び産業振興・育成（研究開発・社会実装の推進等）

年次計画への反映
中長期的課題の整理

今後のスケジュール



経済産業省におけるサイバーセキュリティ政策の全体像

- サイバー攻撃の高度化・多様化が生じている現状を認識しつつ、我が国**産業界へのサイバー攻撃を抑制・防御**し、事業活動への影響を最小化する。そのための政策を企画・実行する。
- その上で、各種の取組を、**我が国産業競争力の強化**につなげる。

①サプライチェーン全体での対策強化

- 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・実装
- 経営ガイドラインの活用促進
- サイバーセキュリティお助け隊サービスの普及促進
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）
- 日米欧によるインド太平洋地域向けの能力構築支援

サイバーセキュリティ お助け隊

IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

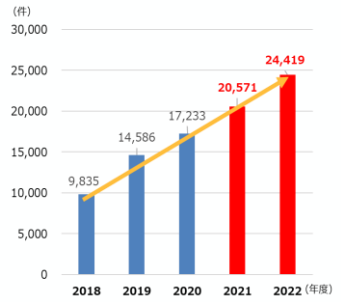
②国際連携を意識した認証・評価制度等の立上げ

- IoT適合性評価制度の検討、国際制度調和に向けた調整
- SBOM（Software Bill of Materials）の活用促進
- QUAD上級サイバー会合、G7等を通じた各国間連携

③政府全体でのサイバーセキュリティ対応体制の強化

- 国境を越えて行われるサイバー攻撃へのJPCERT/CCの対処能力の向上
- 重要インフラ事業者等での事案発生時の初動支援を行うJ-CRATの体制強化
- 改正保安３法を踏まえた事故調査体制の構築
- サイバー攻撃被害情報の共有促進に向けた検討

サイバー攻撃事案の調整件数（年度集計）



④新たな攻撃を防ぎ、守るための研究開発の促進（サイバーセキュリティ産業振興）

- 先進的サイバー防御機能・分析能力の強化
- セキュリティ産業の成長加速化、製品/サービスの国内自給率向上に向けた政策検討

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月に「Society5.0」によって柔軟化・拡張するサプライチェーンに求められる**セキュリティへの対応指針**として、「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**）を策定。

※「Society5.0」においては、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**。

「Society5.0」以前

個々の企業主体の定型的なつながりで価値を生み出す

<3層構造>

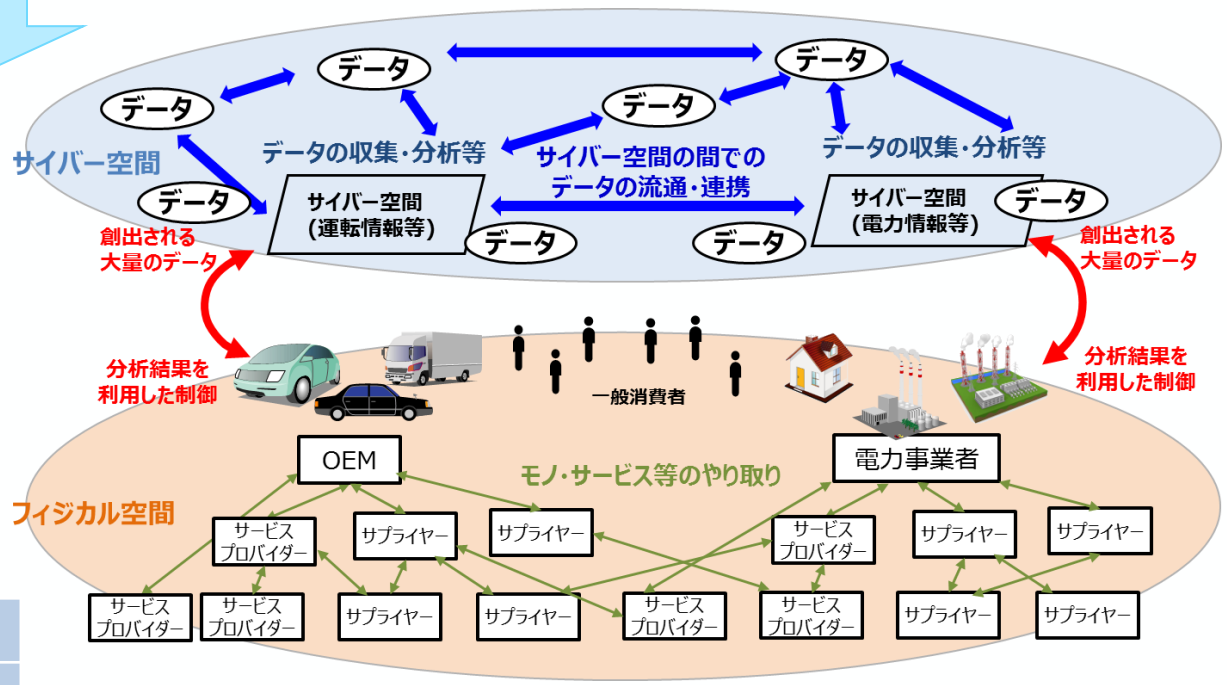
【第３層】
サイバー空間におけるつながり

【第２層】
フィジカル空間とサイバー空間のつながり

【第１層】
企業間のつながり

<6つの構成要素>

ソシキ	ヒト	モノ
データ	プロシージャ	システム



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

CPSFを軸とした各種取組

- CPSFに沿って、**対象者や具体的な対策を整理**し、実践的なガイドラインを整備。

主なガイドラインや対策ツール

産業分野別での具体化と分野横断的な検討

- **７つの産業分野別サブワーキンググループ（SWG）**を開催し、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設置した、３つのタスクフォース（TF）のうち、**ソフトウェアTF**にて、**企業によるSBOMの利活用を推進するための検討を実施**。
- ソフトウェアTFの配下にて、サイバーインフラ事業者に求められる役割等の検討会(*)を実施。

※NISCと経産省の共同事務局

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**

ビルSWG	ガイドライン第２版（2023.4）
電力SWG	小売電気事業者ガイドライン（2021.2）
防衛産業SWG	防衛産業サイバーセキュリティ基準改訂（2022.4）
自動車産業SWG	ガイドライン2.1版（2023.9）
スマートホームSWG	ガイドライン1.0版（2021.4）
宇宙産業SWG	ガイドライン2.0版（2024.3）
工場SWG	ガイドライン拡充版（2024.4）
・・・	

サプライチェーン強化に向けたセキュリティ対策評価制度に関するSWG

分野横断SWG

『第３層：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TF

- ✓ OSSの管理手法に関する事例集の策定
- ✓ **SBOM導入手引の策定**
- ✓ **セキュアソフトウェア開発フレームワーク(SSDF)実証**

サイバーインフラ事業者に求められる役割等の検討会

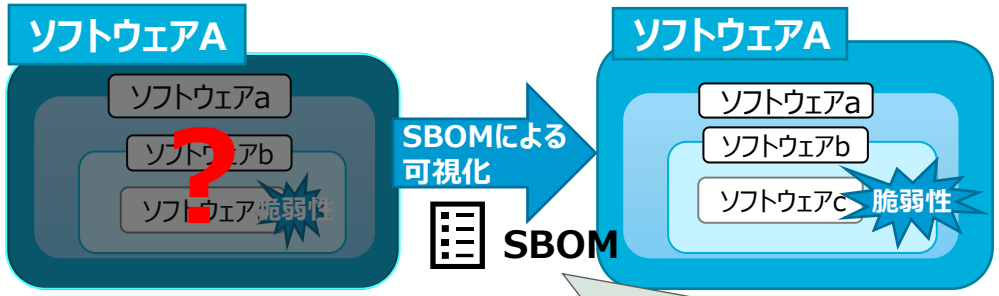
『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討TF

目次

SBOMとは

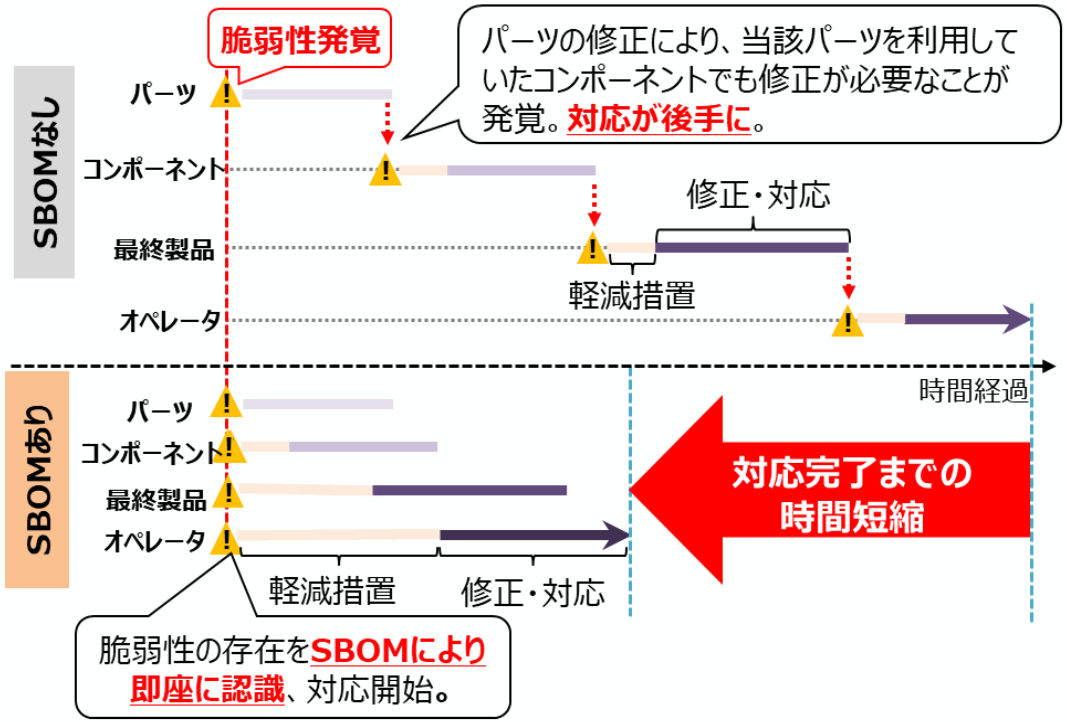
- SBOM（Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。ソフトウェアを構成する各コンポーネントを誰が作り、何が含まれ、どのような構成となっているか等を示す。
- SBOMによりソフトウェアの構成情報の透明性を高めることで詳細を把握することができ、ライセンス管理や脆弱性対応への活用が期待される。

<SBOMイメージ>



サプライヤ名	コンポーネント名	バージョン	製品URLなど	…
A会社	ソフトウェアA	Ver1.0	……	…
A会社	|…ソフトウェアa	Ver2.1	……	…
B会社	|…ソフトウェアb	Ver5.3	……	…
C会社	|…ソフトウェアc	Ver1.2	……	…

<SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮>



ソフトウェア管理に向けたSBOMの導入に関する手引

- 2023年7月、SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示した**「ソフトウェア管理に向けたSBOMの導入手引」を公表。**
- **2024年８月に改訂版を公表。**主な改定ポイントは、**①脆弱性管理プロセスの具体化、②「SBOM対応モデル」の追加、③「SBOM取引モデル」の追加。**

サイバー攻撃への備えを！「SBOM」（ソフトウェア部品構成表）を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引を策定しました

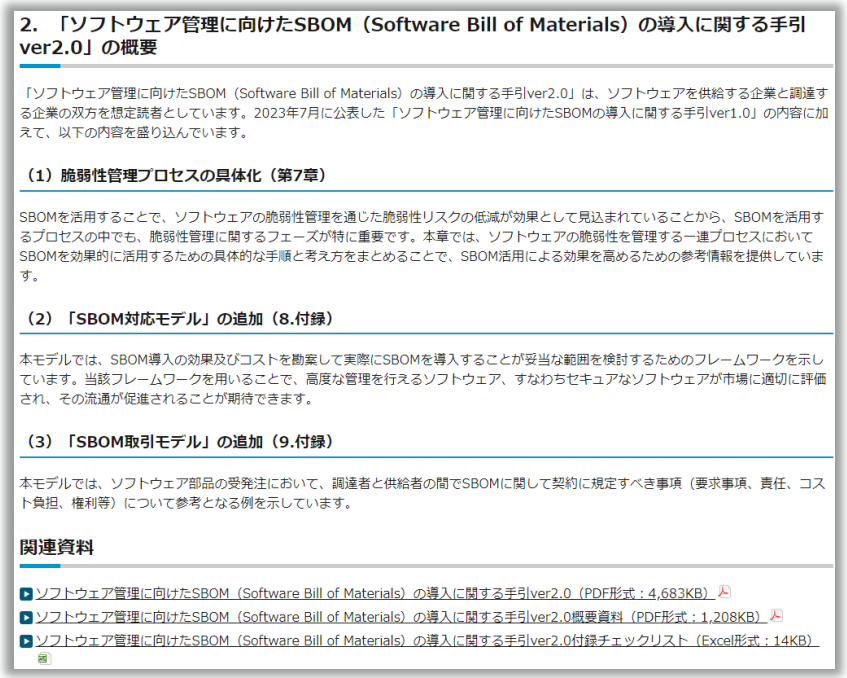
2024年8月29日

▶ 安全・安心

経済産業省は、2023年7月に、ソフトウェアを供給する企業と調達する企業の双方を想定読者として、SBOM（ソフトウェア部品表）を導入するメリットや実際に導入するにあたって認識・実施すべきポイントをまとめた手引書を策定しました。
その後も中小企業を含むあらゆる企業にとってSBOMをより効率的に活用できる方法等の検討を継続し、今般、今年4月26日から5月27日に実施した意見公募で頂いた御意見を踏まえて本手引書の改訂版を策定しましたので、公表します。
具体的には、（1）ソフトウェアの脆弱性を管理する一連プロセスにおいてSBOMを効果的に活用するための具体的な手順と考え方、（2）SBOM導入の効果及びコストを勘案して実際にSBOMを導入することが妥当な範囲を検討するためのフレームワーク、（3）委託先との契約等においてSBOMに関して規定すべき事項（要求事項、責任、コスト負担、権利等）を追加しています。

1．背景・趣旨

近年、ソフトウェアの脆弱性管理に関し、ソフトウェアの開発組織と利用組織双方の課題を解決する一手法として、「ソフトウェア部品表」とも呼ばれるSBOM（Software Bill of Materials）を用いた管理手法が注目されています。米国サイバーセキュリティ・インフラ安全庁（CISA）等が策定し、我が国政府も共同署名をしたセキュア・バイ・デザイン（IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていること）の考え方においては、ソフトウェアの製造業者が製品ごとにSBOMを構築・管理し、ユーザーがSBOMを利用できるようにすることが奨励されています。
経済産業省では、SBOMの企業による活用を推進しており、企業がSBOMを導入するメリットや実際に導入するにあたって実施すべきポイントをまとめた手引書を「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ver1.0」として2023年7月に公表しました。
中小企業も含め、あらゆる企業にとってSBOMをより効率的に活用できる方法等について、「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）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」において検討を進め、今年4月26日から5月27日に実施した意見公募で頂いた御意見を踏まえ必要な修正を行い、同ソフトウェアタスクフォースで了承を得た上で、今般、「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ver2.0」を策定しました。



2．「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ver2.0」の概要

「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ver2.0」は、ソフトウェアを供給する企業と調達する企業の双方を想定読者としています。2023年7月に公表した「ソフトウェア管理に向けたSBOMの導入に関する手引ver1.0」の内容に加えて、以下の内容を盛り込んでいます。

（1）脆弱性管理プロセスの具体化（第7章）

SBOMを活用することで、ソフトウェアの脆弱性管理を通じた脆弱性リスクの低減が効果として見込まれていることから、SBOMを活用するプロセスの中でも、脆弱性管理に関するフェーズが特に重要です。本章では、ソフトウェアの脆弱性を管理する一連プロセスにおいてSBOMを効果的に活用するための具体的な手順と考え方をまとめることで、SBOM活用による効果を高めるための参考情報を提供しています。

（2）「SBOM対応モデル」の追加（8.付録）

本モデルでは、SBOM導入の効果及びコストを勘案して実際にSBOMを導入することが妥当な範囲を検討するためのフレームワークを示しています。当該フレームワークを用いることで、高度な管理を行えるソフトウェア、すなわちセキュアなソフトウェアが市場に適切に評価され、その流通が促進されることが期待できます。

（3）「SBOM取引モデル」の追加（9.付録）

本モデルでは、ソフトウェア部品の受発注において、調達者と供給者の間でSBOMに関して契約に規定すべき事項（要求事項、責任、コスト負担、権利等）について参考となる例を示しています。

関連資料

- 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ver2.0（PDF形式：4,683KB）
- 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ver2.0概要資料（PDF形式：1,208KB）
- 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ver2.0付録チェックリスト（Excel形式：14KB）

「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 ver2.0 」（2024年8月29日 経済産業省）
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

ソフトウェア管理に向けたSBOMの導入に関する手引　～全体概要～

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活用の効果が確認できた。一方、SBOM導入・活用に際しては様々な課題(例：脆弱性管理の効率化、分野や用途に応じたSBOMの適切な範囲、ソフトウェアの調達者と供給者の立場間の取り決め）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「誤解と事実」を提供し、**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認識しておくべきポイント**を示す。(ver1.0)
- 加えて、ソフトウェアの脆弱性を管理する一連プロセスにおいて**SBOMを効果的に活用するための具体的な手順と考え方**、SBOM導入の効果及びコストを勘案して**SBOMを導入することが妥当な範囲を検討するためのフレームワーク**、ソフトウェアの受発注において、**調達者と供給者の間でSBOMに関して契約に規定すべき事項（要求事項、責任、コスト負担、権利等）について参考例**を示す。(ver2.0)

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

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(ver1.0)

フェーズ1	環境構築・体制整備	● 1-1. SBOM適用範囲の明確化 ● 1-2. SBOMツールの選定 ● 1-3. SBOMツールの導入・設定 ● 1-4. SBOMツールに関する学習
フェーズ2	SBOM作成・共有	● 2-1. コンポーネントの解析 ● 2-2. SBOMの作成 ● 2-3. SBOMの共有
フェーズ3	SBOM運用・管理	● 3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施 ● 3-2. SBOM情報の管理

脆弱性管理プロセスの具体化(ver2.0)

- SBOMを活用することで、ソフトウェアの脆弱性管理を通じた脆弱性リスクの低減が効果として見込まれていることから、**SBOMを活用するプロセスの中でも、脆弱性管理に関するフェーズが特に重要**。
- 脆弱性管理の一連プロセスにおいてSBOMを効果的に活用するための**具体的手順と考え方をまとめることで、SBOM活用による効果を高めるための参考情報**を提供。

SBOMを活用した脆弱性管理プロセス

フェーズ1　脆弱性特定
- マッチング手法区分選択
- 利用可能なSBOMデータ特定
- 脆弱性DBの選択
- マッチング手法の選択・作成

フェーズ2　脆弱性対応優先度付
- 予備フィルタリング
- 優先度付情報の選択・取得
- 判断ツリーに基づくカテゴリ判定
- 優先度スコア評価

フェーズ3　情報共有
- 共有情報と共有相手の特定
- 共有方法の特定と実施

フェーズ4　脆弱性対応
- 脆弱性の暫定対応
- 脆弱性の根本対応

SBOM対応モデル(ver2.0)

- SBOM導入の効果及びコストを勘案してSBOMを導入することが**妥当な範囲を検討するためのフレームワーク(5W1Hを網羅するよう体系化)**。
- 実証を通じて、**医療機器、自動車、ソフトウェア製品等の分野**において、コスト・効果を考慮して妥当な対応範囲の参考例を提示。
- 当該フレームワークを用いることで、高度な管理を行えるソフトウェア、すなわちセキュアなソフトウェアが市場に適切に評価され、その流通が促進されることが期待できる。

SBOM取引モデル(ver2.0)

- ソフトウェア部品の受発注において、調達者と供給者の間でSBOMに関して**契約に規定すべき事項（要求事項、責任、コスト負担、権利等**）について参考となる例を示す。
- 既存のソフトウェアに関するモデル契約書と組合せることで、**SBOMに対応した契約書を作成する際の項目案を提示**するもの。

目次

セキュアなソフトウェアを開発するためのフレームワーク（SSDF)

- 2022年2月、NISTは、**ソフトウェアの脆弱性を軽減するためのソフトウェア開発者向けの手法**をまとめたフレームワークであるSSDF（Secure Software Development Framework）のVer. 1.1を公開。
- **各手法は4つに分類**され、**手法を実践するためのタスクが体系化**。各手法の実践により、**脆弱性を低減する**とともに、**未対処の脆弱性が悪用された場合の影響を軽減**し、**脆弱性の再発を防ぐ根本原因に対処可能**。

セキュアなソフトウェアを開発するための手法をまとめたフレームワーク（SSDF）

分類（カテゴリ）	手法
1. 組織の準備（PO） ソフトウェアを開発する組織は、組織レベルで安全なソフトウェアの開発を行うために、適した人材、プロセス、技術を準備する必要がある。	• ソフトウェア開発におけるセキュリティ要件を定義する（PO.1） • ソフトウェア開発における役割と責任を明確化する（PO.2） • ソフトウェア開発を支援するツールチェーンを明確化する（PO.3） • ソフトウェアのセキュリティを確認するための基準を定義し、活用する（PO.4） • ソフトウェア開発のための安全な環境を導入し、維持する（PO.5）
2. ソフトウェアの保護（PS） ソフトウェアを開発する組織は、ソフトウェアのすべてのコンポーネントを、改ざんや不正アクセスから保護する必要がある。	• あらゆる形態のコードを不正アクセスや改ざんから保護する（PS.1） • ソフトウェアリリースの完全性を検証する仕組みを提供する（PS.2） • 各ソフトウェアのリリースをアーカイブ化し、保護する（PS.3）
3. 安全なソフトウェアの開発（PW） ソフトウェアを開発する組織は、脆弱性を最小限に抑え、十分なソフトウェアを備えたソフトウェアをリリースする必要がある。	• セキュリティ要件を満足するとともにセキュリティリスクを軽減できるよう、ソフトウェアを設計する（PW.1） • ソフトウェア設計をレビューし、セキュリティ要件やリスクへの適合性を検証する（PW.2） • 実現可能な場合、機能を重複させずに既存の保護されたソフトウェアを再利用する（PW.4） • セキュアコーディングのプラクティスを遵守してソースコードを作成する（PW.5） • 実行可能なセキュリティを向上させるために、コンパイル、インタプリター及びビルドプロセスを構築する（PW.6） • コードをレビュー・分析することで、脆弱性を特定し、セキュリティ要求事項への準拠を検証する（PW.7） • 実行コードをテストして脆弱性を特定し、セキュリティ要求事項への準拠を検証する（PW.8） • ソフトウェアをデフォルトで安全な設定とする（PW.9）
4. 脆弱性への対応（RV） ソフトウェアを開発する組織は、リリースするソフトウェアに残存する脆弱性を特定し、適切に対応する必要がある。	• 脆弱性に対する継続的な把握と確認を実施する（RV.1） • 脆弱性の評価、優先順位付け及び修正を実施する（RV.2） • 脆弱性を分析することで、その根本原因を特定する（RV.3）

実証を含む取組の全体像

- SSDF活用のための考え方等をまとめた**国内事業者向けの文書**(ガイドライン等)を策定するとともに、**自己適合宣言の仕組み**を構築し、**政府調達等への要件化**を通じて実効性を強化することにより、QUAD共通原則を履行することが目標。
- 今年度は、SSDFと国内ガイドラインのマッピング、実ソフトウェアに対する実証等を通じて、国内ガイドラインの不足事項や課題・対応方法の具体化等について整理し、国内事業者向けの文書(ガイドライン等)の初版案を作成。
- 来年度以降は、残課題の整理・対応、国内事業者向けの文書の初版案の成案化、初版改訂に向けた検討と改訂案策定、自己適合宣言の仕組みの検討・構築、政府調達等への要件化などを検討。

今年度実施予定の内容

- SSDFと国内ガイドラインの対応関係を示すマッピング
- マッピング表を用いたSSDF活用方法・対応フローの整理
- 実ソフトウェアに対する実証、課題・対応方法の具体化等の整理
- 国内ガイドラインの不足事項の明確化と対応方針案の検討
- 事業者のSSDF自己適合宣言文書作成に関する参考情報等の提示、など

＜成果物例＞

国内事業者向け文書(ガイドライン等)の初版案
- SSDFと国内ガイドラインのマッピング表
- SSDF活用の考え方等をまとめた文書
  - ✓ マッピング表を用いたSSDF活用方法
  - ✓ 課題・対応方法の具体的内容
  - ✓ 国内ガイドラインにおける不足事項・対応方針案
  - ✓ 事業者のSSDF自己適合宣言文書作成に関する参考情報、など

来年度以降実施予定の内容

① 残課題(不足項目の対応方法の更なる具体化等)への対応

② 国内事業者向け文書の初版案の成案化

③ 初版改訂に向けた検討と改訂案作成

④ 自己適合宣言の仕組み検討・構築

⑤ 政府調達等への要件化の検討、 など

実証の目的

- サイバーセキュリティを確保する上で、システムの構成要素であるソフトウェア、ハードウェア、人のセキュリティ確保が必要となる。その中でも、ソフトウェアは重要な基盤であるため、ソフトウェアのセキュリティ確保は、極めて重要である。
- そのようなことから、 SAFECode Secure Software Development Practice, OWASP Software Assurance Maturity Model, BSA Framework for Secure Softwareなどのセキュアソフトウェア開発の実践ガイドラインが多数策定されてきた。それらを**包括するセキュア・ソフトウェア開発フレームワークと共通言語の役割**を果たすものとしてSSDFが取りまとめられた。SSDFは開発プロセス全体を対象としており、要求・設計工程に重点を置くSecure by DesignやSecure by Defaultを包含する。
- QUAD共同原則においては、**セキュア・ソフトウェア開発プラクティスを政府調達方針とすることに合意**している。そのベースとしてSSDFが主要なフレームワークとして活用することができる。
- 一方で、SSDFは、幅広い分野で適用できるように、汎用的で、抽象度の高い、包括的なフレームワークを提供するものであるため、組織において**実践導入する上で具体的な方法や達成基準が明確ではない**といった課題がある。
- このようなことから、本事業では、実ソフトウェアを対象に、SSDFの導入実証を行い、実証を通じて得られた**具体的な導入方法、達成レベル、課題の解決策**等の整理を行う。また、SSDF導入の参考情報として、SSDFと国内ガイドラインの対応関係を整理(マッピング)した情報を整理することで、すでに対応済みの国内ガイドラインを参考とした導入方法について考え方を整理する。

実証の進め方

- 目的に基づき、実証項目の具体化、実践、評価、整理を行う。

①実証の要件定義	問題認識の整理、成果物の構成内容、実施項目の定義を行う。
②マッピング対象ガイドラインの選定	SSDFと国内ガイドラインの対応関係を整理(マッピング)するため、マッピング対象の国内ガイドラインを選定する。
③実証項目の具体化	SSDFタスクについて、対象ソフトについて実践する項目、机上評価する項目を特定し、それぞれ実践する内容を定義する。
④実証項目の実践	③に従い実践、机上評価を行う。具体的には、SSDFタスク項目と選定した国内ガイドラインのマッピングの妥当性の評価、 SSDFのレベル分け案（3段階）作成、SSDFタスクの達成度（3段階）評価、SSDFタスクと選定した国内ガイドラインの包含関係（４区分）の特定など。
⑤SSDFx国内ガイドラインのマッピング表整理	①～④の結果をもとに、SSDF×国内ガイドラインのマッピング表を整理する。
⑥SSDFx国内ガイドラインのマッピング表の活用方法整理	⑤のSSDF×国内ガイドラインのマッピング表の活用方法として、国内ガイドラインへの対応状況からSSDFに対応するためのギャップ分析の手順を整理する。

本実証で予定する成果物

成果物の概要と構成

① **SSDF Task 達成レベル（暫定版作成）**(p.23 成果物例：SSDF活用の考え方等をまとめた文書)
SSDFは網羅性高く体系化されているが、抽象的であり具体的に実施すべきことが明確ではなく、実施主体により実施内容に大きな差が出ることが想定される。SSDF Task項目ごとに達成レベルを３段階に分け、プラクティス案として判断指針と具体例を示すことで、実施事項が明確で具体的なものにする。

② **Task実証の具体例(ケーススタディ)と達成評価（暫定版作成）**(p.23 成果物例：SSDF活用の考え方等をまとめた文書)
本実証において実施した具体的な内容をケーススタディとして示し、セキュリティ向上の効果、達成レベルとその評価、SSDF導入企業に対して参考情報を提供する。

③ **SSDF・国内ガイドラインマッピング表（案作成）** (p.23 成果物例：SSDFと国内ガイドラインのマッピング表)
国内ガイドラインを実践する企業の参考となるように、国内の関連ガイドラインの項目とSSDFのTaskの対応関係、包含関係とその説明を整理したマッピング表を整理する。また、NIST AI版SSDF, CISA SBD[2]とのマッピングも示す。

④ **SSDF Taskの課題（整理中）** (p.23 成果物例：国内ガイドラインにおける不足事項・対応方針案、課題・対応方法の具体的内容)
SSDF Task自体の課題（Task過不足、運用フェーズなど）、Task実施上の課題を整理し、課題に対する対応策、今後期待される施策を整理する。

⑤ **SSDF導入ガイダンス基礎編（整理中）** (p.23 成果物例：国内事業者向け文書(ガイドライン等)(マッピング表を用いたSSDF活用方法、事業者のSSDF自己適合宣言文書作成に関する参考情報を含む))
成果物①②③④を活用してSSDFを導入するための手順を示すガイダンスを整理する。本年度は、1つのケーススタディに基づき、成果物①②③④をどのような順序でどのように活用するか基礎的な流れを示す。

③SSDF・国内ガイドラインマッピング表(全体イメージ)

SSDF Taskと国内ガイドラインの章項目最小単位を対象に対応関係を整理する。これにより、各組織が対応済みの国内ガイドラインを起点に、SSDFの対応Task、未対応Taskを特定し、未対応Taskについては、他の国内ガイドラインで関連する事項を特定し、自社の導入における参考情報として活用できるようにする。

対象の国内ガイドライン

発行者	ガイドライン名
METI	SBOM導入手引き　Ver.1.0，Ver.2.0
Software-ISAC	情報システムにおけるセキュリティコントロールガイドライン
デジタル庁	政府情報システムにおけるセキュリティ・バイ・デザインガイドライン
METI	サイバーセキュリティ経営ガイドライン
NISC	政府機関等のサイバーセキュリティ対策のための統一基準群
METI	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）
MIC	クラウドサービス提供における情報セキュリティ対策ガイドライン

対応項目の包含関係区分

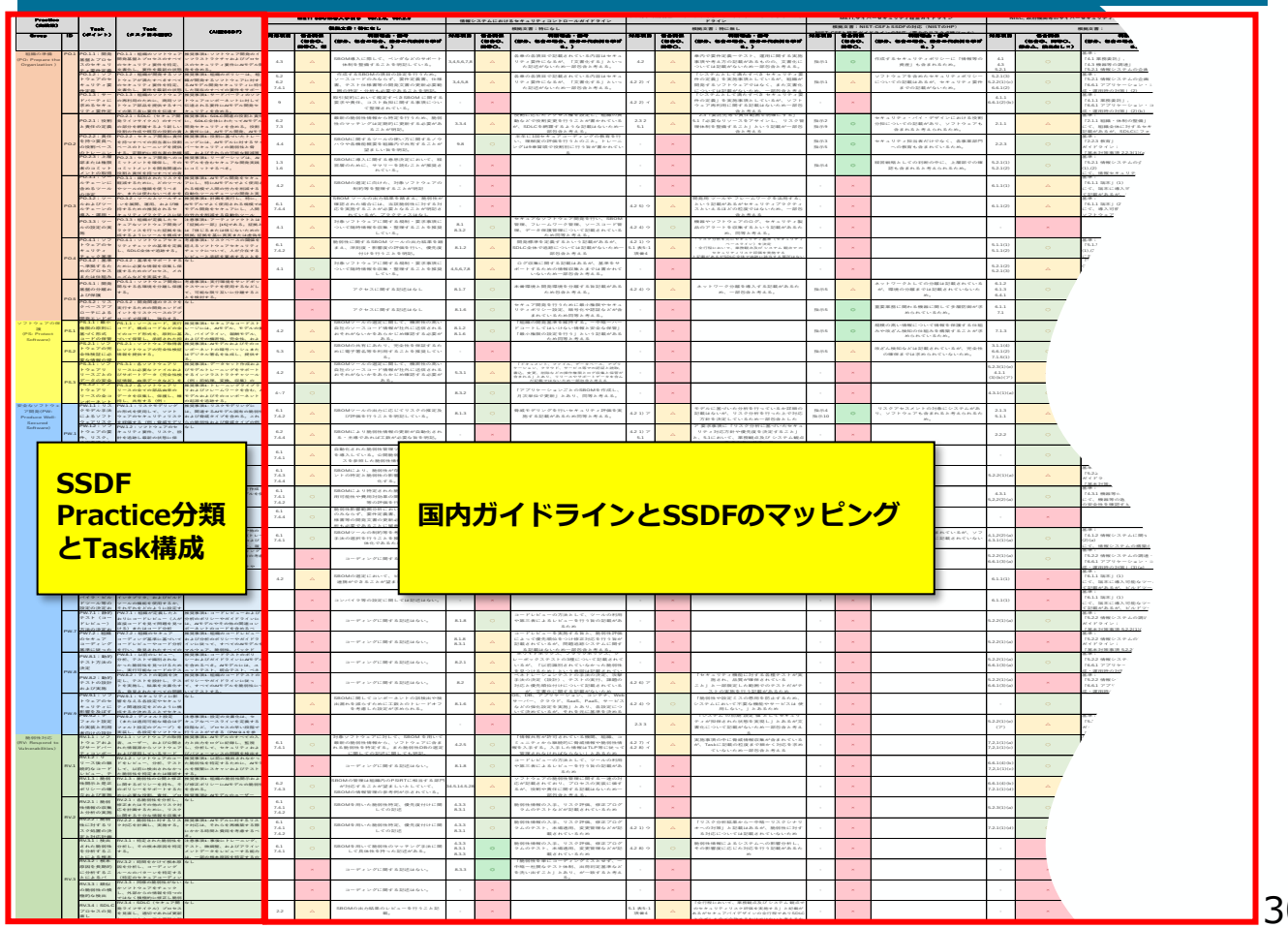
対応項目は以下の包含関係に分類しその判断理由を示す。

◎:包含	ガイドライン該当章は、SSDF taskを含みより広い
○:同等	ガイドライン該当章は、SSDF taskと同等の範囲
△:部分	ガイドライン該当章は、SSDF Taskの部分のみ
×:該当なし	SSDF Taskに該当する章は含まれない

凡例：SSDF　Taskカテゴリ

組織の準備 (PO: Prepare the Organization)
ソフトウェアの保護 (PS: Protect Software)
セキュアソフトウェアの開発 (PW: Produce Well-Secured)
脆弱性対応 (RV: Respond to Vulneravilities)

SSDF Taskと国内ガイドラインのマッピング表（全体イメージ）

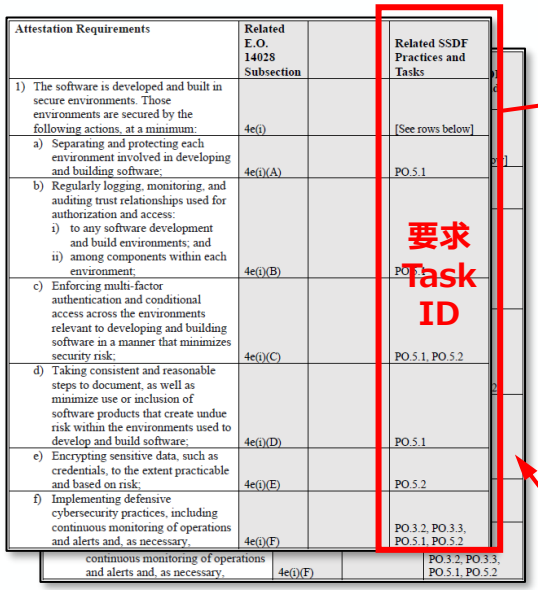


⑤SSDF導入ガイダンス基礎編（整理中）
成果物を活用したSSDF導入ガイダンス（導入プロセス）

SSDF導入プロセスの手順

SSDF導入にあたり、SSDFと国内ガイドラインのマッピング表（成果物）を活用し、対応済項目、未対応項目について参考にできる国内ガイドラインの項目を特定する。SSDF Task毎に、自社にとって必要なプラクティス案を特定し、実施すべき事項の具体例等を参考に、カスタマイズを加えて実践する。必要に応じて、CISA SSDF自己適合証明フォームに示される対応項目との関係を元に、自己適合証明書を作成する。
SSDF導入プロセスの流れを以下に示す。

CISA SSDF自己適合証明フォーム



Attestation Requirements	Related E.O. 14028 Subsection		Related SSDF Practices and Tasks
1) The software is developed and built in secure environments. Those environments are secured by the following actions, at a minimum:	4e(i)		[See rows below]
a) Separating and protecting each environment involved in developing and building software;	4e(i)(A)		PO.5.1
b) Regularly logging, monitoring, and auditing trust relationships used for authorization and access: i) to any software development and build environments; and ii) among components within each environment;	4e(i)(B)		PO.5.1
c) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk;	4e(i)(C)		PO.5.1, PO.5.2
d) Taking consistent and reasonable steps to document, as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	4e(i)(D)		PO.5.1
e) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk;	4e(i)(E)		PO.5.2
f) Implementing defensive cybersecurity practices, including continuous monitoring of operations and alerts and, as necessary,	4e(i)(F)		PO.3.2, PO.3.3, PO.5.1, PO.5.2
continuous monitoring of operations and alerts and, as necessary,	4e(i)(F)		PO.3.2, PO.3.3, PO.5.1, PO.5.2

要求 task ID

SSDF導入プロセス

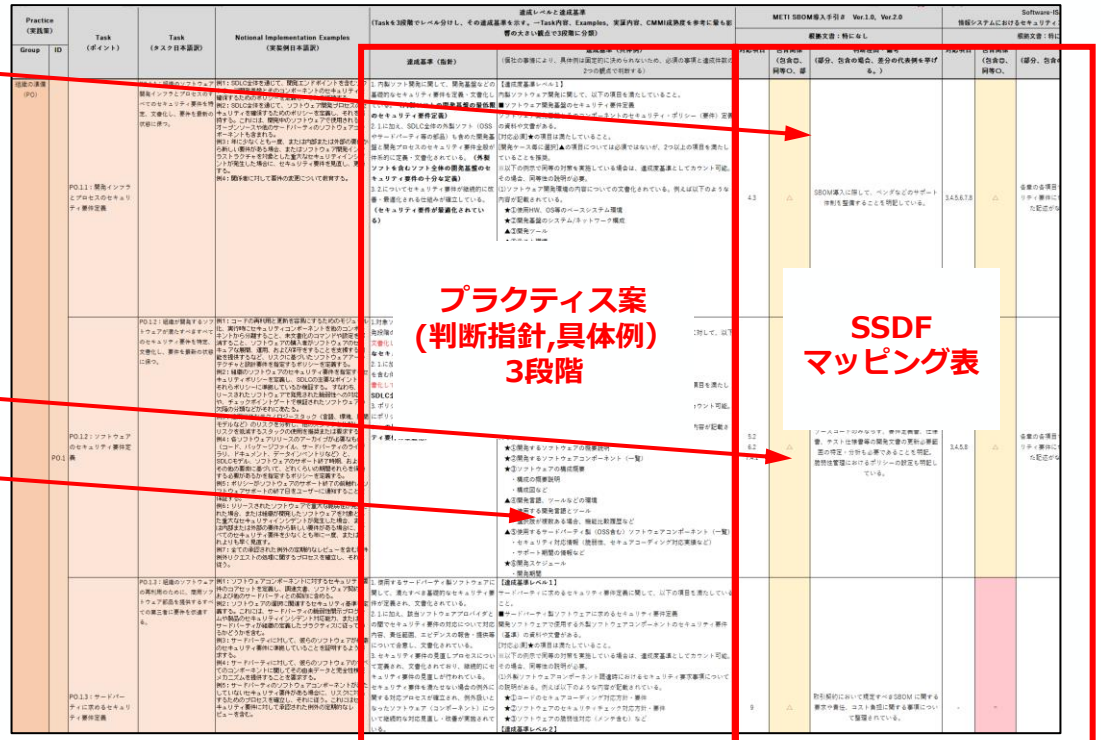
自社の国内ガイドライン対応状況、SSDFマッピング表を参考に自社のSSDF対応項目を特定

Task不足項目の特定

Task不足項目への対応
① SSDFマッピング表を基に参考となる国内ガイドラインを活用
② 実証SSDF実施内容、プラクティス案を参考に対応

SSDF自己適合証明の作成
① 妥当なプラクティス案を選択
② プラクティス案を参考に適合基準を定義し、理由説明を作成

本実証SSDF Taskのプラクティス案



プラクティス案（判断指針,具体例）3段階

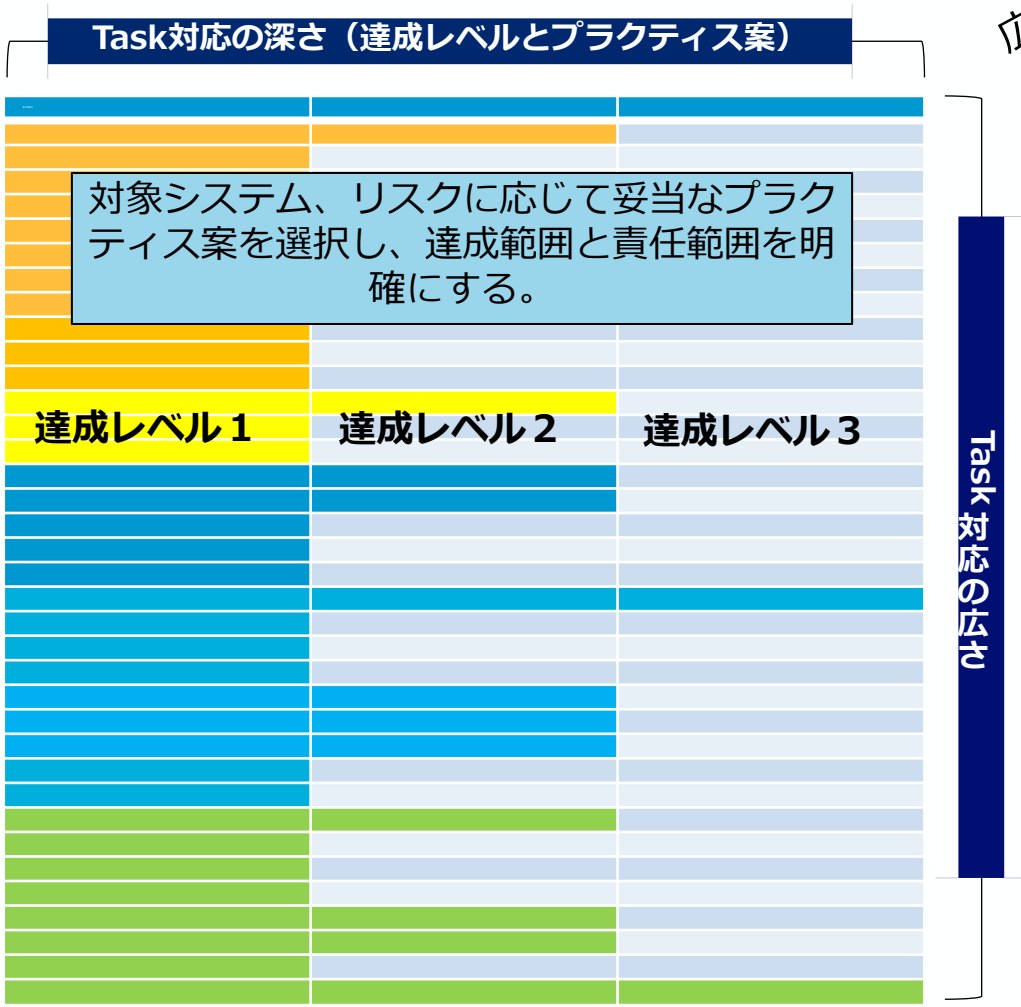
SSDF マッピング表

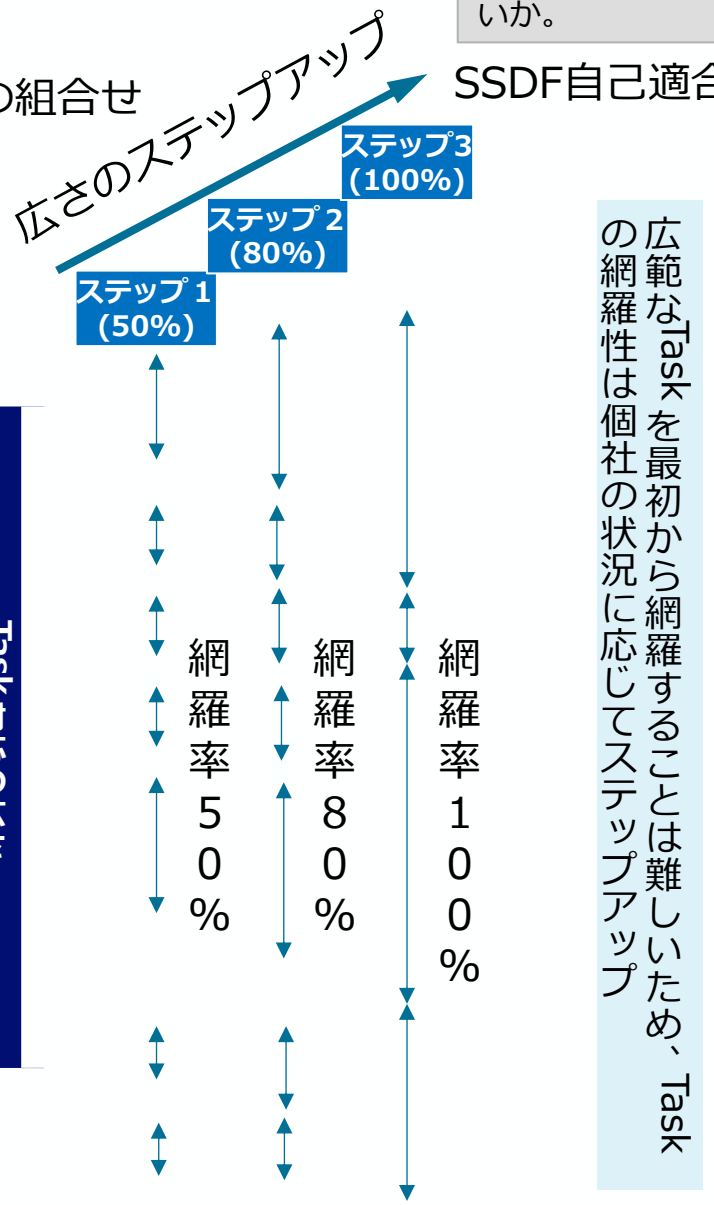
⑤SSDF導入ガイダンス基礎編（整理中）
SSDF導入ガイダンス（基礎編）使い方

ステップアップアプローチ（イメージ）

SSDFの達成度は、Task対応項目の範囲（広さ）と各Taskの達成レベル（深さ）の組合せで決まる。現場に導入する際は、Task項目は段階的に拡大することが想定される。

SSDF Task一覧





Task難易度をベースに５０%、８０%、１００%に暫定分類できないか。

SSDF自己適合証明

広範なTaskを最初から網羅することは難しいため、Taskの網羅性は個社の状況に応じてステップアップ

（参考）SSDF導入の効果（中間整理）

セキュリティ・アシュアランス全体の向上

個別効果（例）

1. **体系的なフレームワークによる弱点の網羅的なチェックと解消**
   SSDF Taskは、セキュアソフトウェア開発プラクティスについて体系的、網羅的に実施すべきことを整理したものであり、本実証でそれらを適用することにより、多数の弱点やリスクを解消することができた。例えば、静的解析、動的解析などの対策においては新たな脆弱性を特定することができた。

2. **組織・ツール環境の整備によるプロセスの効率化**
   SSDFプラクティスのうち、「**組織の準備 (PO: Prepare the Organization)**」においては、組織体制やツール環境のリスクに関わる対策が示されている。これらの取組は、**「ソフトウェアの保護 (PS: Protect Software)」、「セキュアソフトウェアの開発 (PW: Produce Well-Secured Software)」、「脆弱性対応 (RV: Respond to Vulnerabilities)」**を効率的に確実に実施する上で基盤となり開発プロセスの効率化につながった。

3. **組織間の共通言語としての効果**
   SSDFにおいては、実施すべき対策について、包括的な整理を通じて共通言語を整理しているため、開発部署、品質・セキュリティ管理部署などにおける技術者と管理者のコミュニケーションを円滑に行い、対策を効率的に確実なものとすることに有効であった。

4. **（本事業の成果活用）セキュリティレベルの可視化**
   SSDFのプラクティスカテゴリおよびタスクに関して、セキュリティレベルを可視化することができ、取引相手やユーザなどの他のステークホルダに対してセキュリティレベルに関する確信を与えることができる。

5. **OSS等のサードパーティ部品の脆弱性の特定と解消（テクニカルな効果の例）**
   本実証では、OSSサードパーティ部品についても検査を行い、多数の不具合を発見することができた。このようなテクニカルな対策により脆弱性の解消など具体的なセキュリティ向上に効果が確認できた。

目次

「サイバーインフラ事業者に求められる役割等の検討会」の趣旨

趣旨

現代社会において、ソフトウェアは社会活動の基盤となっており、その重要性は増大してる。そのため、ソフトウェアの脆弱性を悪用するサイバー攻撃は社会インフラに甚大な影響を及ぼす可能性がある。ソフトウェアを提供・運用する事業者の責任は、その重要性から従来と変わらないものの、役割の変容に伴い、特に大規模システムを提供する事業者にはより一層の責任が求められている。

また、諸外国では、内閣サイバーセキュリティセンターも共同署名したセキュア・バイ・デザイン／デフォルトに関する文書である「Shifting the Balance of Cybersecurity Risk」や、「ソフトウェア・セキュリティに関する日米豪印共同原則」などが公表され、ソフトウェアサプライチェーン（※1）のレジリエンス向上の取組が急速に進展している。我が国においても、こうした時代の変化を踏まえ、諸外国の取組と整合した、ソフトウェアを提供・運用する事業者の責任に対する対応を整理することが求められている。

我が国のサイバーセキュリティ基本法第７条においては、サイバー関連事業者（※2）その他の事業者の責務が規定されている。このうち、**一定の社会インフラの機能としてソフトウェアの開発・供給・運用を行っている事業者**（※3）（以下、「**サイバーインフラ事業者**」という。）に関しては、官民が連携した取組の在り方や、コストとのバランスを踏まえたソフトウェアサプライチェーンセキュリティ確保のための取組の体系的な整理に関する調査・検討が求められている。

本件に関してはこれまで経済産業省及びNISCにおいてサイバーインフラ事業者に求められる役割等につき調査研究を実施してきたところ、これを踏まえ、**サイバーインフラ事業者と顧客に求められる責務**と、**責務を果たすための要求事項（役割別の具体的な取組の在り方）**を含むガイドライン（以下「ガイドライン（案）」という。）の策定及びその普及策（自己適合宣言の仕組み化等）の検討を目的として本検討会を開催する。

※1 ソフトウェアの開発、供給、運用のすべてに関わるライフサイクルと、関連する組織およびソフトウェアの相互依存関係
※2 インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者
※3 政府機関及び重要インフラ事業者をはじめ広く社会で活用される情報・通信システム、ソフトウェア製品及び ICT サービスを開発し提供する事業者並びに当該情報・通信システム等のソフトウェアのライフサイクルとサプライチェーンに関わる事業者

「サイバーインフラ事業者に求められる役割等の検討会」の概要

- **ソフトウェア・サプライチェーンのサイバーセキュリティ対策強化**のため、令和６年９月から重要インフラ専門調査会及び、経済産業省 産業サイバーセキュリティ研究会の下に共同開催として、産学の有識者からなるワーキンググループを立ち上げ、ソフトウェアを利用する顧客等の保護を目的とした**サイバーインフラ事業者に求められる役割等**について検討。
- 本年度中に、ガイドライン（案）としてとりまとめ、来年度に成案化。その後、自己適合宣言の仕組み化、政府機関や重要インフラの調達等での参照といった普及策等を検討予定。

背景・課題

・ソフトウェアの脆弱性を悪用するサイバー攻撃の脅威が増加

⇒ ソフトウェアの開発・供給・運用を行う「サイバーインフラ事業者」のそれぞれがより一層の責任をもって対応する必要性

⇒ セキュア・バイ・デザイン／デフォルトに関する国際文書にNISCも共同署名

・他方、サイバーインフラ事業者に求められる役割等を整理した国内のガイドラインなし

検討中のガイドライン（案）のイメージ

・サイバーインフラ事業者と顧客に求められる責務、責務を果たすための要求事項（具体的取組）を整理※

サイバーインフラ事業者

○ソフトウェア（クラウド上のものを含む）の
- 開発者
- 供給者
- 運用者

顧客

○顧客（政府機関、重要インフラ 等）

(1) セキュリティ品質を確保したソフトウェアの開発・供給・運用

(2) ソフトウェアサプライチェーンの管理

(3) 残存脆弱性への速やかな対処

(4) ソフトウェアに関するガバナンスの整備

(5) ステークホルダー間の情報連携・協力関係の強化

(6) 顧客経営層のリーダーシップによるリスク管理とソフトウェア調達・運用

※諸外国の関連ガイドライン等を参照

取組の全体像

- ソフトウェアの開発・供給・運用に関わる**サイバーインフラ事業者と顧客に求められる責務**、および**責務を果たすための要求事項**（役割別の具体的な取組の在り方）をまとめたガイドライン（案）を策定すると共に、その普及策（自己適合宣言の仕組み化等）の検討を通じて、ソフトウェアサプライチェーンのレジリエンス向上を図ることが目標。
- 今年度は、関連する諸外国の取組の調査、サイバーインフラ事業者へのヒアリング等を通じて、責務および責務を果たすための要求事項を整理し、**ガイドライン（案）**を作成。
- 来年度は、**ガイドライン（案）の成案化**を行う。その後、経済産業省・NISCそれぞれにおいて**自己適合宣言の仕組み化検討、残課題への対応、普及施策**（政府機関や重要インフラ事業者での調達等での参照・推奨等）を検討予定。

今年度実施予定の内容

実施事項

- 関連する諸外国の取組の調査
- サイバーインフラ事業者へのヒアリング
- サイバーインフラ事業者と顧客に求められる責務の整理
- 責務を果たすための要求事項の整理
- ガイドライン（案）の作成

成果物例

- ガイドライン（案）
  - サイバーインフラ事業者と顧客に求められる責務
  - 責務を果たすための要求事項
  - 参考情報　など

※ 参照の容易性などを踏まえ、附属書の内容をガイドライン（案）に統合。

来年度以降実施予定の内容

実施事項

- ガイドライン（案）の成案化
- 自己適合宣言の仕組み化の検討
- 残課題への対応
- 普及施策（政府機関や重要インフラ事業者での調達等での参照・推奨、関連機関との連携、海外展開等）の検討　など

サイバーインフラ事業者に求められる役割等に関するガイドライン（案）の全体概要と今後の取組例

ガイドライン（案）の背景

- ソフトウェアとそのサプライチェーンに潜む脆弱性を悪用するサイバー攻撃が増加
- NISC等も共同署名したセキュア・バイ・デザイン／デフォルトなどデジタル製品・サービスにおけるサイバーセキュリティ対策の強化に関する制度整備が加速

ガイドライン（案）の趣旨

- 諸外国の取組と整合した、ソフトウェアを利用してサイバーインフラを提供する「サイバーインフラ事業者」の対応を整理することが求められているところ、事業者及び関係者がサイバーセキュリティ対策の実効性を確保するために参考となる考え方を示すもの

今後の取組例

- 活用促進に向けた自己適合宣言等の制度検討、ツール類の整備、広報活動などを検討

ガイドライン（案）の概要

6つの責務 サイバーセキュリティに関するレジリエンス向上のため、サイバーインフラ事業者と顧客が認識すべき基本理念	6つの要求事項 サイバーセキュリティに関するレジリエンス向上のため、共通して取組むべきサイバーセキュリティ対策	対象組織
セキュリティ品質を確保したソフトウェアの開発・供給・運用	セキュアな開発・供給・運用	サイバーインフラ事業者（ソフトウェア開発ベンダー、ソフトウェア販売会社、ソフトウェア運用ベンダー　等） ＋ 関係機関（行政機関、関連業界団体）
ソフトウェアサプライチェーンの管理	ライフサイクル管理、透明性の確保※	
残存脆弱性への速やかな対処	残存する脆弱性の速やかな対処	
ソフトウェアに関するガバナンスの整備	人材・プロセス・技術の整備	
サイバーインフラ事業者・ステークホルダー間の情報連携・協力関係の強化	サイバーインフラ事業者・ステークホルダー間の関係強化	
顧客経営者のリーダーシップによるリスク管理とソフトウェア調達・運用	顧客経営層によるリスク管理とセキュアなソフトウェアの調達・運用	顧客

※「ライフサイクル管理、透明性の確保」のうちSBOM関連の内容については、経済産業省の「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ver2.0」を参考とすることができる。

(参考) ガイドライン（案）の要求事項の概要

- 要求事項はカテゴリとして整理する。複数の個別要求（要求事項の具体的な取組の在り方）から構成する。

	要求事項のカテゴリと概要	要求事項
サイバーインフラ事業者	(1) セキュアな開発・供給・運用 脆弱性を抑え、セキュリティを備えたソフトウェアを開発・供給・運用する	(1)-1 設計時のリスク評価と対策の追跡 (1)-2 セキュアなビルド (1)-3 テスト (1)-4 サービスのモニタリング
	(2) ライフサイクル管理、透明性の確保 ソフトウェア管理の透明性をライフサイクル全体で確保しサプライチェーンを含むリスク管理を行う	(2)-1 セキュアなコンポーネントの手配 (2)-2 リリースファイルやデータのセキュアなアーカイブ (2)-3 関係者間のセキュリティ要件の確立 (2)-4 利用者への適切な情報提供
	(3) 残続する脆弱性の速やかな対処 リリースしたソフトウェアに残存する脆弱性を特定し、速やかに対応する	(3)-1 継続的な脆弱性調査 (3)-2 検知した脆弱性への対処 (3)-3 対処結果を組織のプロセス改善に活用
	(4) 人材・プロセス・技術の整備 組織レベルでソフトウェアに関わる人材・プロセス・技術を整備する	(4)-1 人材：経営層のコミットメントと人員の整備 (4)-2 プロセス：開発ポリシーの確立と法令順守 (4)-3 プロセス：運用ポリシーの確立と法令順守 (4)-4 プロセス：開発運用基準の策定 (4)-5 技術：セキュアな開発ツールの整備 (4)-6 技術：セキュアな開発環境の整備
	(5) サイバーインフラ事業者・ステークホルダー間の関係強化 サイバーインフラ事業者・ステークホルダー間の情報連携・協力体制を強化する	(5)-1 情報連携のための組織体制 (5)-2 協力体制の強化
顧客	(6) 顧客によるリスク管理とセキュアなソフトウェアの調達・運用 顧客経営層のリーダーシップによるリスク管理とセキュアなソフトウェア調達、運用を行う	(6)-1 顧客経営層のリーダーシップによるリスク管理 (6)-2 顧客経営層のリーダーシップによるソフトウェアの調達、運用

目次

新たなサイバーセキュリティ政策の方向性

- サプライチェーン全体での対策強化に向け、これまでソフトロー・アプローチとして、経営層の意識改革の促進、各種のフレームワーク・ガイドライン等の策定を実施。
- 今後、関係省庁と連携し、**政府調達等への要件化を通じた実効性の強化、国産製品の開発・普及促進や高度人材の育成・確保**、サイバー安全保障の実現に向け**官民のサイバー状況把握力・対処能力向上に向けた取組**を進める。　※十分なリソースの確保が困難な中小企業等に対しては、支援策を一層強化。

サイバーセキュリティ対策の実効性強化

<これまでの取組：フレームワーク・ガイドライン等の整備>

サイバー・フィジカル・セキュリティ対策フレームワーク

経営ガイドライン　工場ガイドライン　●●ガイド・・・etc

政府調達に関する基準／民間企業における調達要件（政府機関等のサイバーセキュリティ対策のための統一基準群等）

<今後目指すべき取組：調達要件化等を通じた実効性の強化>

IPA

策定・連携

サイバー・フィジカル・セキュリティ対策フレームワーク

経営ガイドライン　工場ガイドライン　●●ガイド・・・etc

政府調達に関する基準／民間企業における調達要件（政府機関等のサイバーセキュリティ対策のための統一基準群等）

認証基準策定

認証製品の調達要件化等の連携（例：IoTセキュリティ適合性評価制度）

認証制度（新設）

セキュリティ市場の拡大に向けたエコシステムの構築

需要側：工場　電力

・セキュアな製品の調達
・事案対処能力強化
・・・etc

需給の相互連関を通じたエコシステムの構築・セキュリティ産業の発展

供給側

研究開発促進・SU創出

検証・市場化支援・信頼性確保

高度人材の育成・確保（情報処理安全確保支援士の活用促進等）

サイバー情勢分析能力の強化

官民の情報ハブとしてのIPAの強みを活かし、地政学等の情勢と産業界（エンドポイント）から得られるサイバー攻撃情報の集約・分析を一層推進。攻撃者の意図を把握し、攻撃の対象や手法を予見して効果的な防御策を講じる。

J-CSIP　サイバーセキュリティCS赤助け隊

情報集約

IPA 情報集約・分析・トリアージ

初動対応支援　情報提供　被害組織　政府機関等

（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

SBOMの普及促進とSSDFに関する取組の方向性

- SBOM導入手引ver2.0(英語版)を国際文書から参照させることにより、国際的な成果の普及を図る。
- 実証の結果を踏まえ、SSDFに関する導入ガイダンスを整備する。また、自己適合宣言の仕組みの検討、政府調達などにおける要件の国際調和を図る。

(1)国内事業者向けSSDF導入ガイダンスの整備

- 次年度以降、国内事業者向けにSSDFを導入するためのガイダンスの整備を進める。
- さらに、今年度の実証と異なる分野等の実践例を通じて、SSDF導入方法に関する内容を拡充し、具体性を高める。
- 国内ガイドラインの不足事項（残課題）の特定を行い対応方針を検討する。

(2)自己適合宣言の仕組みの検討

- 次年度以降、SSDF導入の実効性を高めるための自己適合宣言の仕組みの検討・構築を行う。
- その際には、特にSSDFの達成レベル識別と可視化をベースとした仕組みについても考慮し検討する。
- 策定した自己適合宣言の仕組みについては、政府調達等との連携についても検討する。

(3)要件の国際調和の検討

- QUAD共同原則をベースにセキュア・ソフトウェア開発に関する要件の国際調和、産業競争力強化や国際戦略を意識した国際連携の方策を検討する。
- 具体的には、SBOM導入手引2.0(英語版)が国際文書から参照されるよう調整し、国際的な成果の普及を図る。また、QUAD共同原則においては、政府調達要件の整合性が求められるため、（２）で検討する内容と関連付けて進める。

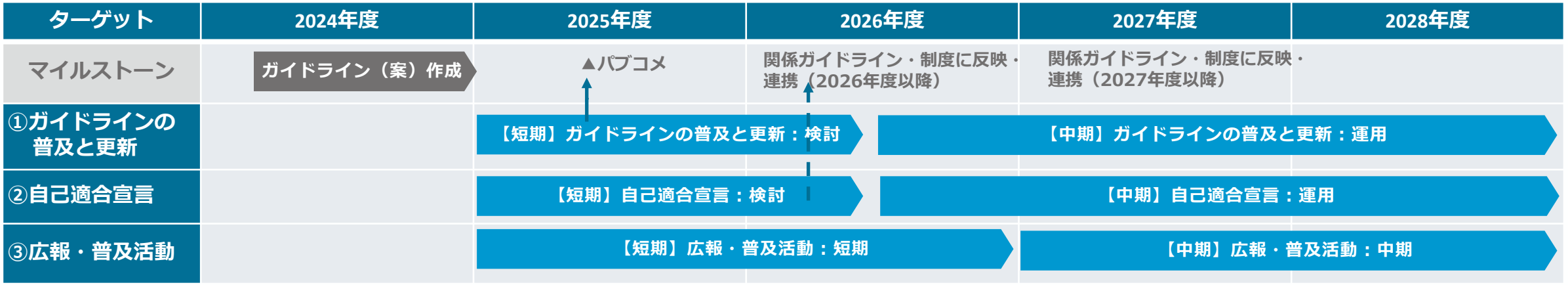
サイバーインフラ事業者に求められる役割等に関するガイドライン（案）の活用促進に向けた取組の方向性

- 検討会の有識者、事業者からのヒアリングを通じて普及施策に関する要望を抽出。
- 要望を踏まえ、ガイドラインの普及と更新、自己適合宣言、広報・普及活用の3点に整理し、短期・中期軸別に取組を進める。

普及施策に関する要望

	ガイドラインの普及	自己適合宣言	広報施策
事業者	• 各種テンプレートの整備 • ベストプラクティス、チェックリストの整備 • ガイドラインの効果測定　等	• 自己適合宣言による免責や責任の軽減制度の検討 • 保証の在り方の整理 • 妥当な更新期間の設定	• コスト、経営層の取組に関する広報 • 取組実施企業のリスト整備　等
検討会の有識者	• モデル契約書、英語版ガイド、リスクベースのセキュリティ要件ガイドの整備 • 主要な文献との関連の整理 • 本ガイドラインの活用状況の調査　等	• 事業者が客観評価できる基準の整備 • 宣言状況を確認できるサイトの整備 • 政府調達、重要インフラ事業者自身の調達での実績の蓄積 • 普及開始前の制度の実証　等	• 業界団体を通じた普及　等

普及施策のロードマップ



※普及施策等については「サイバーインフラ事業者に求められる役割等の検討会」以外の検討会の立ち上げも検討

METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html