経済産業省　NISC

資料３

サイバーインフラ事業者に求められる役割等の検討の方向性

２０２５年2月１８日

サイバーインフラ事業者に求められる役割等の検討会

事務局

1. 本検討会の趣旨・取組の全体像の確認
2. 前回以降の各種ご意見を踏まえたガイドライン（案）の更新内容
3. ガイドライン（案）の全体像
4. ガイドライン（案）の活用促進に向けた取組の方向性
5. 来年度本検討会での検討事項
6. ご意見を頂きたい事項

1. 本検討会の趣旨・取組の全体像の確認

本検討会の趣旨の確認

第1回検討会資料の再掲

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

第２回検討会資料から一部変更

「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

本検討会開催の背景

参考　第1回検討会資料の再掲

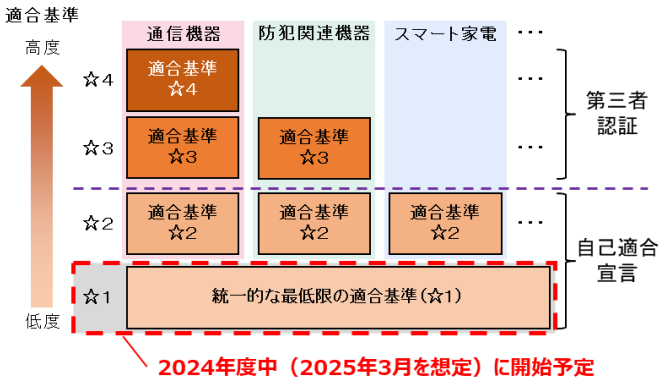
ガイドライン等の実効性の強化
（セキュアなIoT製品及びソフトウェアの流通に向けた取組等）

実効性強化

- セキュリティ対策レベルを評価し、それを可視化する取組の**先行例として、IoTセキュリティ適合性評価制度を検討中**。**米欧等の諸外国との制度調和を図るための議論も継続中**。
- また、**SBOM（ソフトウェア部品構成表）**導入時の課題検証のための実証や企業向けの手引書を策定。
- IoTセキュリティ適合性評価制度の実効性強化やSBOMの導入促進に向けては、**産業界との連携のほか、政府調達等の要件化等に向けて関係省庁と議論も開始**。
- さらに、米国が策定し、我が国政府も共同署名をしたセキュア・バイ・デザインのガイダンスも踏まえ、**ソフトウェア開発者が行うべき取組整理**や**安全なソフトウェアの自己適合宣言の仕組みの検討**を行っていく。

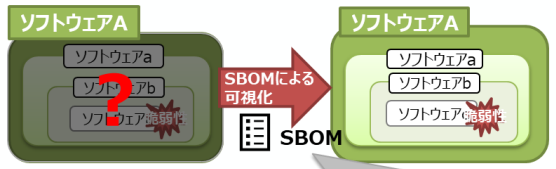
IoTセキュリティ適合性評価制度

- 幅広い**IoT製品を対象**として、一定のセキュリティ基準を満たすものを認証し、ラベルを付与する制度の整備に向けて、検討を実施。その結果を2024年３月に取りまとめ、**2024年度中に一部運用を開始**予定。



SBOMのイメージ

- **SBOM（ソフトウェア部品構成表）がソフトウェアのセキュリティの脆弱性を管理する手法の一つとして着目。**



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	……	…

セキュアバイデザイン・セキュアバイデフォルト

- **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。

（出典：国際共同ガイダンス「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」）（2023年10月28日署名）

出所：　経済産業省　第８回　産業サイバーセキュリティ研究会　事務局説明資料　（2024年4月）より

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との役割分担(案)

委員限り

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	成果物例
• 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	• 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

今年度の検討会における各回の検討内容および議事事項

検討内容

- サイバーインフラ事業者と顧客に求められる責務の考え方
- サイバーインフラ事業者と顧客が責務を果たすための要求事項
- 政府機関・重要インフラ事業者をはじめ、顧客となる事業者等によるガイドラインの活用を促す枠組み等、サイバーインフラ事業者のレジリエンス向上の実効性を強化する施策全般

検討スケジュール

検討会および開催時期	主な議題	備考
第１回検討会 （令和6年9月24日）	• 責務と要求事項について • 検討の進め方について • その他	• 追加調査すべき文献とヒアリング方針、ガイドライン（案）の活用方法と構成
第２回検討会 （令和6年12月17日）	• 文献調査およびヒアリング結果を踏まえたガイドライン（案）の審議 • ガイドライン附属書方針の審議	• 更新したガイドライン（案）の詳細 • ガイドライン（案）の出口の在り方の検討材料としてご意見頂く。
第３回検討会 （令和7年2月18日）	• ガイドライン（案）の承認 • 今後の普及方針の検討	• コストを含む実効性の確保のための施策等

2. ガイドライン（案）の更新内容

ガイドライン（案）の更新概要

- 検討会でのご意見、2024年12月に追加実施したクラウド事業者へのヒアリング結果等を踏まえ、①～⑤の更新を実施。

①事業者と顧客の位置付けの整理

項目	主なご意見	事務局対応案
顧客の責務	【有識者・検討会】 • 事業者も顧客への情報提供について学び顧客に働きかけ、顧客も対策に努めるべきである。 • サイバーインフラ事業者が顧客に説明し理解いただいた上で、顧客側にもコストを負担いただくための努力が必要という意味合いを記載するのがよい。　等	• 一定の責務（事業者への働きかけ、投資等）の必要性を補足　等
想定される関係者の責務と役割分担	【有識者・検討会】 • クラウドサービスを連携しているサービスサプライチェーンについても本ガイドラインの対象となることを明確にするのがよい。 • 契約形態に応じて、顧客自身が開発、運用になりうると書くとよい。　等	• クラウドサービス提供のサブ事業者の例示を追加 • 顧客自身が開発、運用になりうることを補足　等
事業者の範囲	【有識者・検討会】 • 「インフラ事業者（ネットワーク事業者）」を入れたほうが良い。	• インフラ事業者（ネットワーク事業者）が含まれることを補足

ガイドライン（案）の更新概要

②分かりやすさのための記載の充実・明確化

項目	主なご意見	事務局対応案
ソフトウェア範囲の明確化	【有識者・検討会】 • 脆弱性対策にはEOSもEOLも含めるべきである。等	• EOSが含まれることを補足　等
その他	【有識者・検討会】 • リスクの洗い出しの際に、脅威、対象、利益として何を洗うかがわからないと、実務者が困る状況になる。 • セキュリティバイデフォルトは、わかりやすく解説してほしい。 • クラウドサービスでは、「契約」ではなく、「利用規約」や「SLA（サービスレベルアグリーメント）」という表記が一般的である。　等	• 脅威モデリングの概要説明追加 • セキュアバイデフォルトの説明追加 • クラウドにおける利用契約の表記を更新　等

③関連文書との関連の整理

項目	主なご意見	事務局対応案
関連文書との関連整理	【有識者・検討会】 • 附属書はユーザとしては便利である。ガイドラインが発行されれば、政府統一基準との関係を明文化しておくと使う側にも良い。	• ガイドライン（案）と、「政府統一基準群」・「重要インフラのサイバーセキュリティに係る安全基準等策定指針」との関係を整理し、参考情報として掲載。

ガイドライン（案）の更新概要

④要求事項の整理

項目	主なご意見	事務局対応案
パッケージ定義の見直し	【有識者・検討会】 • サイバーインフラ事業者が採択するパッケージについて、ミニマム要求パッケージを選ぶか標準要求パッケージを選ぶかの判断材料（個人情報がどの程度あるかなどリスクに応じた例）があるとよい。 • 最低限の要求事項がミニマムということであれば、日本語で表記してはどうか。	• パッケージの判断材料を補足。 • 「最低限要求パッケージ」と「標準要求パッケージ」に名称変更。
要求事項の明確化	【ヒアリング】 • S(2)-3.1「セキュリティ要件の合意」、S(2)-3.2「サプライチェーンセキュリティ要求への対応」について、クラウドサービスのセキュリティ要件は供給者が決定するため、対応への配慮が必要である。 • S(1)-3.3「テスト実施」について、テストは自動化されている場合は、自動化したテストの証跡が残っていればよいのではないか。 • S(6)-2.2「セキュリティ慣行の要求開示」について、画一的なものを示すのではなく、リスクやソフトウェアの種類に応じて適切なものを示してほしいというのが事業者側の要求である。 【有識者・検討会】 • 組織の外部から調達する前提でソフトウェアを構築することを前提としているように見える。	• S(2)-3「関係者間のセキュリティ要件の確立」：再委託先とプライム事業者間でサプライチェーンセキュリティ要件が合致しない場合を考慮。 • S(1)-3「テスト実施」：　自動化を含め実施形態に応じて適切な証跡や環境を整えることを補足。 • S(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」：　事業者にリスクやソフトウェアの種類に応じて適切な慣行を要求することを明確化。 • S(2)-1「セキュアなソフトウェアコンポーネントの手配」：　外部調達を推奨するものではないことを補足。

ガイドライン（案）の更新概要

⑤本文書の位置付け整理

項目	主なご意見	事務局対応案
ガイドラインをセキュリティ取組の整理物と位置づけ	【有識者・検討会】 • サイバーインフラ事業者が顧客に提供するサービスについても、サイバーセキュリティの確保に努める対象に入ると基本法を解釈した上で、ガイドライン（案）が基本法やNISCの基本方針に対するより詳細な解釈を示すものであるのか、単に参考として資料を提供するものなのか、位置づけを明確にするとよい。	• ガイドライン（案）自体が義務を課すものではなく、参考となる考え方を示すものである旨を明確化。 • 上記位置づけを踏まえ、原則として、「責任」を「責務」とし、「義務」の表記を見直し。「望ましい」は、解説部分においてまさに「望ましい」ことの内容を説明するものとして限定的に使用。 • 「推奨パッケージ」は、「要件パッケージ」に変更。 • 現時点では検討会名義とし、パブコメ等を踏まえた成案化の際に経済産業省と内閣サイバーセキュリティセンターとの共同名義とする予定。 • ガイドライン（案）の中で「検討体制」として本検討会の情報を追加。

ガイドライン（案）の全体構成と更新箇所

※①～⑤は前頁の更新箇所を示す

1. 総論 ②⑤	1.1 背景と目的	諸外国の取組の動向、およびソフトウェアサプライチェーン上でのセキュリティ対策の必要性を簡潔に説明。インシデント事例を追加。
	1.2 ガイドライン（案）の位置付け	顧客と事業者に求められる責務と、責務を満たすための要求事項を整理することを説明。
	1.3 適用対象	「サイバーインフラ事業者」の範囲、対象ソフトウェア、本文書が想定するリスク概要を説明。
	1.4 役割分担の考え方	ソフトウェアの特性、開発・供給体制、契約形態による役割分担モデルを説明。
	1.5 代表的なユースケース例 ①	複数のサイバーインフラ事業者による役割分担について例示し説明。
2. サイバーインフラ事業者と顧客の責務と役割分担	2.1 責務と役割分担の考え方	事業者と顧客が協調しつつそれぞれの責務を果たす必要があることを説明。
	2.2 責務	事業者の5つの責務と、顧客の1つの責務を整理。
3. 責務を果すための要求事項	3.1 要求事項の全体像	要求事項（6カテゴリ、21要求事項）の全体像を説明。
	3.2 要求事項	個別要求単位の説明。
4. 要求事項の利活用	4.1 要求事項の要求パッケージ化 ④	要求事項を、その目的・目標に応じて２分類し、パッケージとして整理。
	4.2 役割分担に応じた要求事項の適用に関する注意点 ④	要求事項を適用する際のポイントを説明。
5. 参考情報 ②③	5.1 要求事項チェックリスト	自己適合宣言の様式を考慮したチェックリストを別紙として整理。
	5.2 セキュリティインシデントと要求事項の対応関係例	インシデント事例に対して、要求事項がどのようにリスクを軽減するのか、対応関係を説明。
	5.3 システムライフサイクルにおける脅威と要求事項の対応関係	脅威と要求事項の対応関係を参考情報として説明。
	5.4 要求事項に対する取組例	要求事項（個別要求）を実現するために対応すべき実施事項の例を参考情報として説明。
	5.5 統一基準群と本ガイドライン（案）との関係	統一基準群と本ガイドライン（案）の対応関係を整理。
	5.6 策定指針と本ガイドライン（案）との関係	策定指針と本ガイドライン（案）の対応関係を整理。
	5.7 参照情報	関連文書リスト、関連文書との対応関係を整理。
	5.8 用語	用語説明。
6. 本ガイドライン（案）の検討体制 ⑤		検討体制を説明。

3. ガイドライン（案）の全体像

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

4. ガイドライン（案）の活用促進に向けた取組の方向性

普及施策に関する要望

- 検討会、有識者および事業者からのヒアリングを通じて普及施策に関する意見を収集した。
- 主なご意見は以下の通り。

事業者

■ガイドラインの普及
- 各種テンプレートの整備
- 格付け制度や補助金の整備、入札要件化
- ベストプラクティス、チェックリストの整備
- インセンティブ設計
- ガイドラインの効果測定（統計的な情報、アンケート）

等

■自己適合宣言
- 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

■広報施策
- 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

有識者・検討会

■ガイドラインの普及
- 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
- 税制優遇の制度検討
- 調達時の加点要素化
- 地方公共団体等でのガイドラインの活用
- 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

■自己適合宣言
- 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

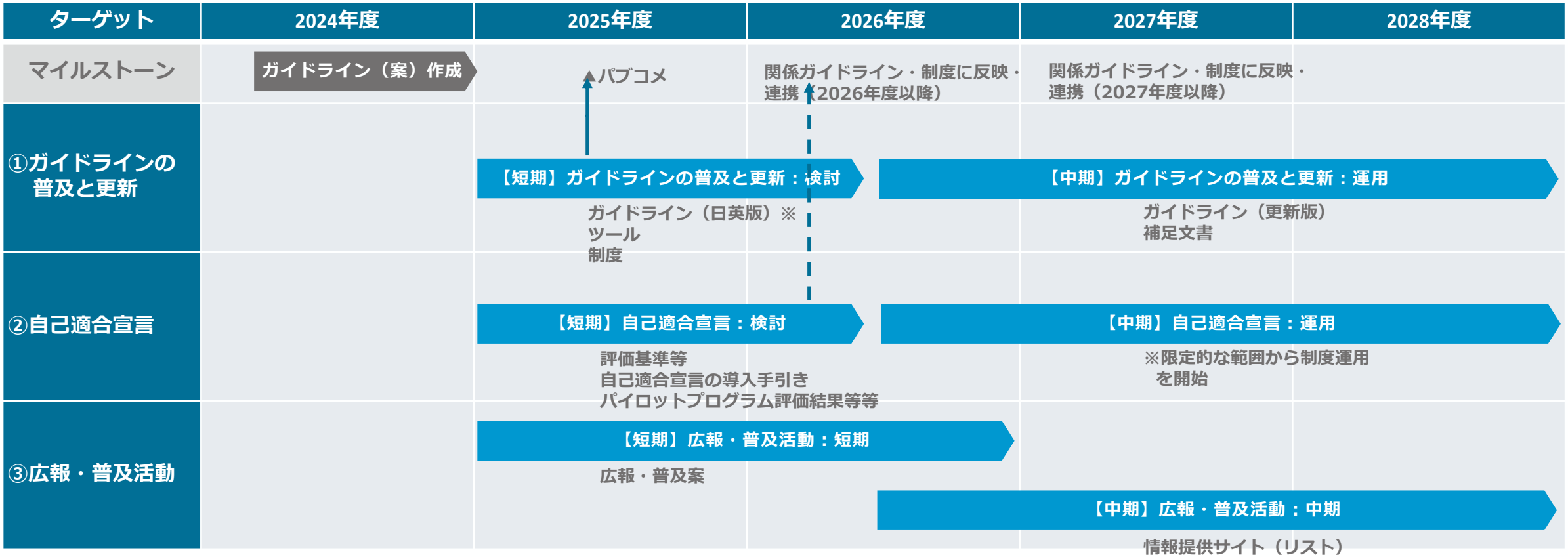
等

■広報施策
- 業界団体を通じた普及

等

普及施策のロードマップ案

- ご意見を、ガイドラインの普及と更新、自己適合宣言、両者に共通する広報・普及活動の3点に整理。
- 短期と中期の時間軸別に取組を進め、関連ガイドライン・制度とも整合を取る。



※本検討会はガイドラインの成案化をもって終了し、以降の自己適合宣言の制度などについては別途検討会の立ち上げ検討

施策① ガイドラインの普及と更新

- 短期：ガイドラインの具体的な適用方法など事業者の負担に配慮するツール整備を先行する。
- 中期：事業者からの意見収集などを通じて、ガイドライン自体の普及と更新を進める。

【短期】ガイドラインの普及と更新：検討

実施項目	概要	考えられる普及施策の例
ガイドラインの成案化	• 英語版とあわせてパブコメを行い意見を収集する。	・実施事項：英語版を作成し、パブコメを実施する。 ・成果物　：ガイドライン（日本語版・英語版）
関連文書類の整備	• ガイドラインの利用を後押しする関連文書類を整備する。	・実施事項：民間企業での利用を想定したモデル契約書、政府調達時のモデル調達仕様書等を優先度を踏まえてテンプレートとして整備する。 パイロットプログラム（後述）を通じ、コストや難易度の高い要求事項を特定し、優先度を踏まえ要求事項の実装を支援するフレームワークを整備する。 関係機関と連携して整備する。 （案）ユーザとベンダーが議論のたたき台となるような保守の考え方、契約面での論点を整理する。 要求事項単位で、フェーズ毎の具体的な取組事項と脅威を説明する文書を整備する。例えば、「リスクベース分析」の要求事項において、OS、ミドルウェア等のリスクを評価し、取るべき緩和策の手引きを整備する。 ・成果物　：モデル契約書、モデル調達仕様書テンプレート、実装フレームワーク等
制度設計	• ガイドラインの普及に繋がるインセンティブを設計する。	・実施事項：事業者の自主的な契約を中心とした取組を促すインセンティブを設計する。 ・成果物　：政府調達での活用、他制度との関連の整理、他制度と連携した一部評価免除、レーティング等の制度

施策① ガイドラインの普及と更新

【中期】ガイドラインの普及と更新：運用

実施項目	概要	考えられる普及施策の例
関連文書類・制度の運用	• 関連文書類・制度を運用する。	・実施事項：短期施策として整備した関連文書類を公開し、制度を運用する。 関係機関と連携して配布する。 ・考慮事項：対象範囲、文書類、制度に優先順位を設定し、運用する。
効果検証と更新	• 施策の効果を検証するフェーズを設ける。 • 事業者および顧客の現状を踏まえたガイドラインの更新を進める。	・実施事項：サンプリングによる実態調査、アンケート等を実施し、ガイドライン、制度、ツールの効果を収集し、更新に活用する。 ・成果物　：ガイドライン（更新版）
国内他制度等との連携	• 他のガイドライン類との関係を整理の上で、連携する。	・実施事項：分野別に他のガイドラインとの平仄・関係性の補足情報を附属書等を通じて提供する。 他のガイドラインと連携する。 （案）外部機関と連携し、要求事項の実装方法に関するガイドを整備する。 ISO 27002との対応関係を示すことで、顧客に気づきをもたらす。 ・成果物：　補足文書 ・考慮事項：政府調達・重フラの関連文書を優先して整理する。関係機関、業界団体の取組、経済産業省の関連取組（地場ベンダー手引等）も想定する。 下請法を踏まえた、サプライチェーンの取組強化の関連文書の検討も必要。
海外他制度との連携	• 関連する外国のガイドライン類に対して、本ガイドラインを順守すれば十分になるような制度設計と運用を行い、海外での対応が求められる事業者のインセンティブとする。	・実施事項：制度設計、海外向けの情報発信。 ・成果物　：制度 ・考慮事項：事業者ヒアリングなどを通じて、連携すべき海外のガイドラインを選定する。

施策② 自己適合宣言

- 短期：政府調達での活用を目指し、評価基準整備やパイロットプログラム試行を通じ、実効性の高い制度を検討する。
- 中期：分野別に自己適合宣言制度の普及を進める。

【短期】自己適合宣言：検討

実施項目	概要	考えられる普及施策の例
制度検討	• 自己適合宣言の範囲、評価基準等を含む制度を整理する。	・実施事項：各種文献を参照しつつ、実効性と事業者負担軽減を考慮した制度を検討する。 ・成果物　：評価基準等 ・考慮事項： ー宣言範囲：プロジェクト単位での宣言を可能とする。 ー評価基準：例えば、SWタスクフォースのSSDFの検討内容等も活用しうる。 ー宣言主体：米国事例等を参考にしつつ、我が国の商習慣を踏まえる。 ー更新期間：事業者負担、技術進展を考慮する。1～2年程度。 ー保証方法：内部監査を中心とする。クラウド事業者やオフショア先の保証は、プライム事業者に宣言を求め、サブ事業者に間接的に対応を求める。 ー情報開示：NDAに基づく個別検討、監査法人を活用する。テンプレートとして開示範囲とエビデンス例を整理する。 ー例外事項：自己適合が満たされていないことが判明した場合の取扱を整理する。損害賠償等に直結するため別枠で精緻に検討する。
関連文書類整備	• 自己適合宣言を活用するためのツールを整備する。	・実施事項：事業者の負担軽減と効果的な宣言に資する関連文書類を整理する。 ・成果物　：自己適合宣言の導入手引き等 ・考慮事項：宣言を行うことに伴う法的責任の検討が必要等の考慮点を盛り込む。
制度の実効可能性調査	• パイロットプログラム、ヒアリングを実施する。	・実施事項：本調査の初期ターゲットである政府調達の実績を有するプライム事業者などを対象に自己適合宣言の試行、および事業者へのヒアリングを実施する。 ・成果物　：パイロットプログラム評価結果等

施策② 自己適合宣言

【中期】自己適合宣言：運用

実施項目	概要	考えられる普及施策の例
制度の拡大・普及	• 制度の拡大・普及を促進する方法と対象を検討し、実施する。	・実施事項：普及の端緒（イノベーターの獲得）とするため、特に政府調達を対象とし、制度の活用を推奨するとともに、活用事例としてアナウンスする。 その後、さらに普及を拡大（アーリーアダプター獲得）するため、重要インフラ事業者や地方公共団体等の調達での制度の活用を推奨するよう働きかける。
制度の効果・効率の向上	• （施策③ご参照）	（施策③ご参照）

施策③　広報・普及活動

- 短期：自己適合宣言やガイドラインの活用を広めるための広報活動を進める。
- 中期：サイバーインフラ事業者の取組を支援する活動を進める。

【短期】広報・普及活動

実施項目	概要	考えられる普及施策の例
ガイドラインおよび制度自体の啓発活動	• サイバーインフラ事業者への啓発活動を行う。 • 広く社会認識の醸成を図る。	・実施事項：イベント開催、キャンペーンサイトや関連機関を通じたアナウンスを行う。 ・成果物　：広報・普及案 ・考慮事項：リソースの限られる事業者も想定する。 経営者へのアプローチも想定する。 事業者と顧客のコスト分担についての社会認識の醸成を図る。 事業者がガイドラインを2度、3度と利用することによるメリットを周知する。

【中期】広報・普及活動

実施項目	概要	考えられる普及施策の例
ガイドライン・制度を活用する事業者の間接的な支援	• サイバーインフラ事業者の活動・取組を周知することで間接的に支援する。	・実施事項：自己適合宣言や取組結果を公表するサイト（リスト）を整備する。 自己適合宣言のマークの利用を許可し、事業者のモチベーション向上を促す。 ・成果物　：情報提供サイト（リスト） ・考慮事項：情報の開示範囲を検討する。必要に応じて関連機関と連携する。
ガイドライン・制度を活用する事業者の直接的な支援	• 特にリソースの乏しいサイバーインフラ事業者の取組を支援する。	・実施事項：知見を有する事業者が、サイバーインフラ事業者を支援できる仕組みを整える。「サイバーセキュリティお助け隊サービス」などを参考に制度を整える。 ・成果物　：支援取組案

施策イメージ　－自己適合宣言と実装フレームワーク－

- 自己適合宣言の評価基準は、エビデンスと対応する評価方法の観点で詳細化し、信頼性と有効性を高める。
- 実装フレームワークは、要求事項を実現する具体的な取組を実装手順と入出力の点で整理し、実行可能性を高める。

要求事項例	自己適合宣言の評価基準イメージ	実装フレームワークのイメージ
S(1)-1.1 リスクベースのセキュリティ要件の定義 開発するソフトウェア、あるいはソフトウェアで構成されるシステム・サービスに対して、リスクベースの分析・評価を実施し、緩和策となるセキュリティ要件を定義する。	**エビデンス** リスク分析の結果、分析結果に基づくセキュリティ要件の一覧 **評価方法** 特定されたリスク分析方法にしたがった分析結果を確認する。必要なセキュリティ要件が網羅されていることを確認する。	**実装手順** リスクモデリングの事前準備、リスク分析手順（STRIDE等） **入出力** 分析対象とすべき脅威、守るべき機密データの例、セキュリティ要件（個人情報、認証、アクセス制御、クレデンシャル管理）、対象別（OS、ミドルウェア等）の取るべき緩和策例
S(3)-1.3 脆弱性情報の収集 公知情報の探索、ソフトウェア取得者からの通知、外部脅威情報の取得、システム構成データのレビュー、その他の方法を通じて、新たな脆弱性情報を収集する。	**エビデンス** 脆弱性情報を収集する手続き文書、収集した脆弱性情報 **評価方法** 手続き文書中の情報源が公知情報源を含むことを確認する。顧客からの通知を処理する手続きが含まれていることを確認する。	**実装手順** 収集方法、収集データの管理方法（SSVC等のツールの活用、自組織の資産管理と一体の取組方法） **入出力** 具体的な公知情報源

5. 来年度本検討会での検討事項

今年度の検討会における成果物と来年度の検討事項

今年度の検討結果

- ガイドライン（案）の整理
  - サイバーインフラ事業者と顧客に求められる責務の考え方と責務を果たすための要求事項を整理
- 普及施策の方針検討
  - ガイドラインの普及施策の検討
  - ガイドラインを活用する施策として、自己適合宣言の方針を検討

来年度の検討事項

- 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
- 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、他制度との関連を整理した上での連携、海外展開等）の具体的検討

※本検討会はガイドラインの成案化をもって終了し、以降の自己適合宣言の制度などについては別途検討会の立ち上げ検討

ご意見をいただきたい事項

1. ガイドライン（案）（更新版）について

- 第2回検討会のご意見、ヒアリング結果を踏まえた、ガイドライン（案）の修正内容は適切か
  - 事業者と顧客の役割分担
  - 要求事項
- 要求事項の内容について、考慮すべき事項はないか

2. 普及施策、今後の事業などについて

- ガイドラインそのものの普及、自己適合宣言制度等についてのご意見
  - ガイドラインを普及するための施策
  - 自己適合宣言の実効性を高めるための考慮点
- 本検討会で議論すべき点・課題があるか（トレンド情報等に基づき意見があればお願いいたします）