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

２０２４年１２月１７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. 検討会について
2. 文献調査
3. ヒアリング結果
4. ガイドライン案
    ① 要求事項の概要
    ② ガイドライン案の更新概要
5. 普及施策
6. ご意見を頂きたい事項

1. 検討会について

検討会について

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

「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の下に※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、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。

※経済産業省 産業サイバーセキュリティ研究会のワーキンググループとして共同開催

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) 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

検討会開催の背景

参考　第1回検討会資料の再掲

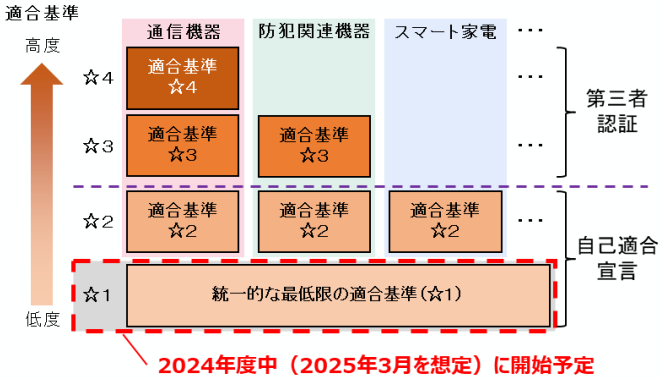
ガイドライン等の実効性の強化
（セキュアなIoT製品及びソフトウェアの流通に向けた取組等）

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。

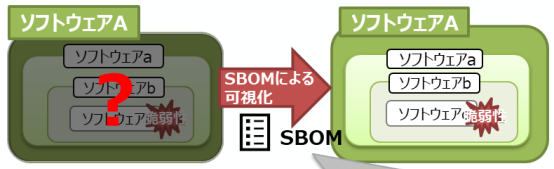
IoTセキュリティ適合性評価制度

- 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。
- 来年度以降は、**自己適合宣言の仕組み化検討、ガイドライン案の成案化、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

- ガイドライン本体案
  - 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
- ガイドライン附属書案
  - 本ガイドライン案の活用方法

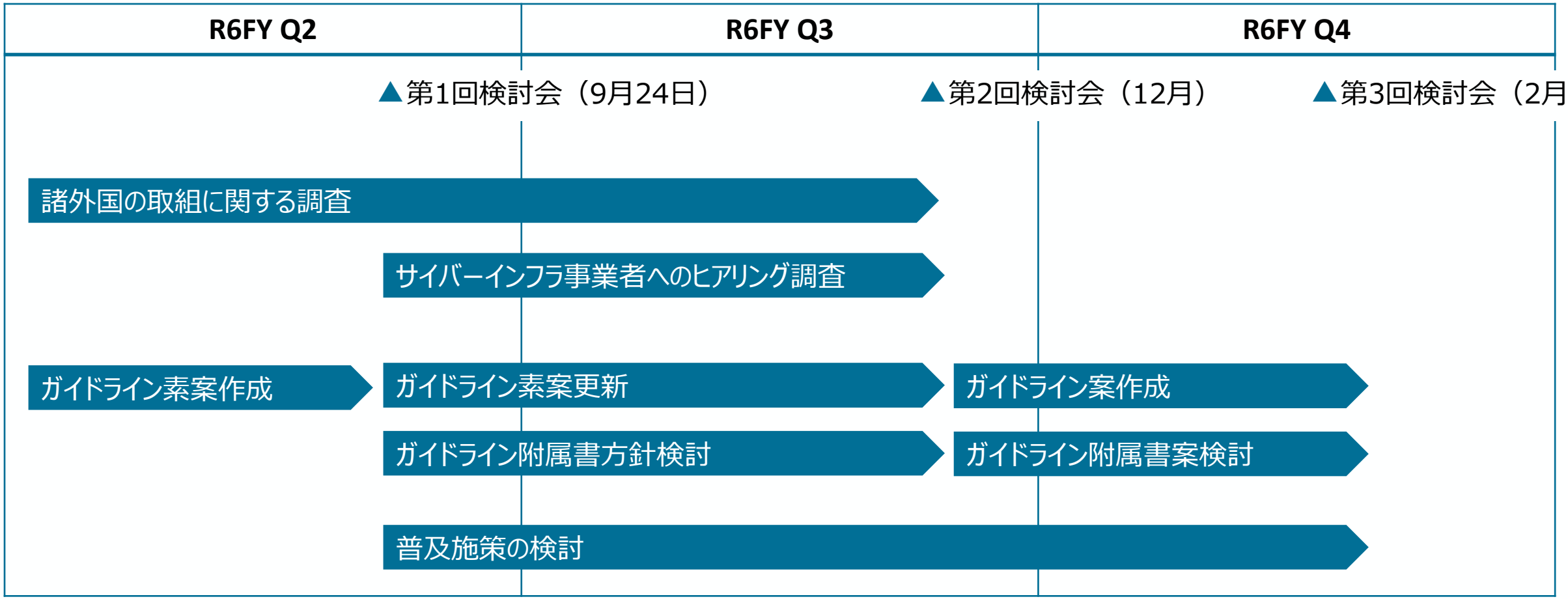
来年度以降実施予定の内容

実施事項

- 自己適合宣言の仕組み化の検討
- ガイドライン案の成案化
- 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

※ 第１回検討会から、来年度以降の取組を詳細化

今年度の取組の進め方


R6FY Q2
R6FY Q3
R6FY Q4
▲第1回検討会（9月24日）
▲第2回検討会（12月）
▲第3回検討会（2月）
諸外国の取組に関する調査
サイバーインフラ事業者へのヒアリング調査
ガイドライン素案作成
ガイドライン素案更新
ガイドライン案作成
ガイドライン附属書方針検討
ガイドライン附属書案検討
普及施策の検討

今年度の検討会について

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（本体）の活用方法と構成
第２回検討会 （令和6年12月中旬）	• 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）	• 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. 文献調査

ソフトウェアサプライチェーンに関わる諸外国の取組（追加）

- 欧米を中心に、セキュア・バイ・デザイン／デフォルトの概念に関連する文書の公開が進んでいる。また、ソフトウェアの導入組織向けの文書や高リスクとみなされるプラクティスも公開されている。

米国	
Secure By Demand	• **ソフトウェアの購入組織がソフトウェア・ベンダーに対してソフトウェア製品に関わるセキュリティを要求する**ために利用できるガイダンス。質問例が整理されている。 • 2024年発行。
Product Security Bad Practice	• ソフトウエア開発において、**高リスクと見なされるプラクティス**の概要を説明し、これらのリスクを軽減するための推奨事項を提供する。 • 2024年発行。

3. ヒアリング結果

ヒアリング

- 2024年11月11日から18日まで、ソフトウェアサプライチェーンを構成するサイバーインフラ事業者、サイバーインフラ事業者業界団体からご紹介いただいた有識者の計5組織にヒアリングを実施。
- 主に、ガイドライン全般、要求事項、要求パッケージ分類、普及施策に関するご意見を頂いた。

分類	ヒアリング先の概要
サイバーインフラ事業者	親事業者からの受託実績、自社ソフトウェアパッケージの開発実績を有する事業者。
サイバーインフラ事業者	2次請け以降のSI実績、自社ソフトウェアパッケージの開発実績を有する事業者。
有識者	セキュリティコンサルティングに従事されている有識者。
有識者	セキュリティコンサルティングに従事されている有識者。
有識者	セキュリティコンサルティング・運用に従事されている有識者。

ヒアリング　―ガイドライン案全般への主なご意見―

- 顧客の概念、用語等について、わかりやすさを求める意見が多い。

概要	主なご意見	事務局対応案
事業者と顧客別の参照箇所の明確化	• 自社が顧客の立場になるケースもあり、参照すべき箇所がわかりにくい。	• ガイドライン案1.4章で、サイバーインフラ事業者と顧客の役割分担の説明を拡充。
用語・説明の追加	• 「特定のシステム・サービスのソフトウェア」等の対象がわかりにくい。 • サイバーインフラ事業者視点での「顧客の責務」に対する考え方として、責務について顧客と合意形成を図るといったような補足説明があった方が良いのではないか。 • 1.3章の 適用対象、1.4章の役割分担の考え方、1.5章の代表的なユースケース例、3.1章の要求事項の全体像に示される図が複雑である。	• 本文中に説明を追加すると共に、必要な用語については、付録に用語定義を追加。 • 図をわかりやすく見直し。

ヒアリング　―要求事項への主なご意見―

- 要求事項に過不足があるとの意見はなく、運用の要求事項が盛り込まれていることの違和感の指摘はない。
- 自己適合宣言を念頭におくと、要求事項の達成度合いを判断できるよう、詳細な粒度を求める意見が多い。

概要	主なご意見	事務局対応案
要求事項に関する追加情報	• S(1)-1.1で、リスク分析やリスク評価をどのように行うか考えなければならないので、参考となる情報等を記載した方が良い。	• リスク分析の補足情報を追加。
誤解の少ない表記	• 主語の記載が省かれている要求事項は、解釈が難しい。 • 「組織」の表記は、複数の解釈が可能であり、具体的に記載した方が良い。	• 解釈に誤解を生むケースについては、記載を明確化。
記載粒度	• 要求項目を細分化して対応を求めた方が分かりやすい要求事項がある。例：S(4)-1.5の役割とトレーニングは、要求事項を分割し、レベル設定を行うのが望ましい。 • 要求事項の達成度合いを判断できるよう、詳細な粒度が必要。 例：S(4)-1,(4)-2：「定期的」、S(4)-2.1：「特定方法」、S(5)-1：「連携」、S(2)：体制、対象とする「脆弱性」	• 本ガイドライン案は広く実施が望まれる概念レベルの責務と責務を果たすための要求事項を整理することから、現状の記載レベルを維持する。 なお、自己適合宣言の枠組みに関連することから、第3回検討会の検討事項とする。

ヒアリング　―プラクティス例への主なご意見―

- 記載の充実を求める意見が多い。

概要	主なご意見	事務局対応案
記載の充実	• セキュアコーディング等、ソフトウェアサプライチェーンの契約形態に応じてセキュアな開発方法が変わるのであれば、その特性や気を付けておくべき事項を記載してほしい。 • プラクティス例において、特に重要と考えられる措置については、具体的な内容に踏み込んでほしい。	• 本ガイドライン案は、広く実施が望まれる概念レベルの責務と責務を果たすための要求事項を整理することから、現状の記載レベルを維持する。 なお、本ガイドラインの普及施策に関連することから、第3回検討会の検討事項とする。
表記の見直し	• プラクティス例の中に、「生産性向上」といった記載があるが、本ガイドラインの責務もしくは要求事項に相対する記載のみにすべき。	• 生産性向上を通じて、対策費用を間接的に捻出することを意図していたが、セキュリティに対する責務を実現するためのプラクティスという位置づけを明確にし、生産性向上の表現を見直し。

ヒアリング　―要求パッケージ分類への主なご意見―

- 対策の必要性の観点から、標準要求からミニマム要求への変更意見あり。（経営層の関与、予算確保等）
- 実効性の観点から、ミニマム要求から標準要求への変更意見あり。（セキュリティバイデフォルト等）

概要	主なご意見	事務局対応案
予算確保	• S(4)-2.3、S(6)-2.4の予算確保は、実施の前提であることから、ミニマム要求が望ましい。	• 前提として、ミニマム要求パッケージに変更。
経営層の取組	• (4)-1.2の経営者のコミットメントは、ミニマム要求ではないか。	• 予算確保には経営層の判断が必要であることから、あわせてミニマム要求パッケージに変更。
セキュリティ要求と設計との関係	• S(1)-1.1でセキュリティ要件を定義しないと、S(1)-1.2の設計レビューの実施は難しい。	• S(1)-1.1は、ソフトウエア設計の起点のなる事項であることから、ミニマム要求パッケージに変更。
セキュアバイデフォルト	• S(2)-4.1に示されるセキュリティバイデフォルトは、セキュリティバイデザインとセットとなる考え方である。企業の現状を踏まえると現段階でミニマムとすることは難しい。	• セキュリティバイデフォルトとセキュリティバイデザインを推進するという趣旨を踏まえ、ミニマム要求を維持。
運用中のレビュー	• S(3)-1.4の運用フェーズでの定期的なレビュー実施は、難しい。	• 開発終了後のレビューは、工数が高いものの、脆弱性の解消には有効であることから、ミニマム要求を維持。

ヒアリング　―要求パッケージ分類への主なご意見(続き)―

概要	主なご意見	事務局対応案
運用の要求事項	• S(1)-4の運用に関する個別要求事項が明確に判断できない。また、運用フェーズの取組は開発フェーズより進んでいる所感であり、基本的に考慮が必要である。	• S(1)-4.1, 4.4は、ミニマム要求に変更。S(1)-4.2, 4.3は要求事項の記載を明確化。
商用製品の出所管理	• S(2)-1.3のコンポーネントのリスク管理において、OSSと商用製品の対策は異なる。商用製品の出所管理は、現状の商慣行等をふまえると標準要求パッケージがよい。	• 本ガイドライン案は、広く実施が望まれる概念レベルの責務と責務を果たすための要求事項を整理する方針である。要求事項としては総合的なリスク判断を求めており、具体的な実施方法にまで詳細化せず、ミニマム要求を維持。
脆弱性の根本対応	• S(3)-3.1の脆弱性の根本原因の対応は、ミニマム要求が望ましい。	• 根本原因を特定し、プロアクティブに対応することは、比較的難易度が高く、標準要求を維持。

4. ガイドライン案

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調達 (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 顧客の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 顧客の経営層のリーダーシップによるリスク管理 (6)-2 顧客の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

ガイドライン案の更新概要

- 第1回検討会およびヒアリングのご意見を踏まえた主な更新内容は以下の通り。

① 事業者と顧客の位置付けの整理

② ソフトウェアの対象範囲の明確化

③ 要求事項の明確化
要求パッケージの適用方針、ライフサイクルが事業者と顧客で合致しないこと等の補足説明

④ 分かりやすさのための記載の充実
要求事項が脅威に対抗することの説明、脅威モデリングの説明、サイバーセキュリティ基本法との関係、用語説明等の追加

ガイドライン案の更新概要

1. 総論 ④ ② ①	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 位置付け	顧客と事業者に求められる責務（基本理念に類する事項）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	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. 顧客とサイバーインフラ事業者の責務と役割分担	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 ③	4.1 要求事項の推奨パッケージ	要求事項を、その目的・目標に応じて２分類し、要求事項の推奨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事項	要求事項を適用する際のポイントを説明。
5. 参考情報 ④ ④	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 要件事項に対するプラクティス例	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。
	5.4 参照情報	関連文書リスト、関連文書との対応関係を整理。
	5.5 用語	用語説明。

ガイドライン案の更新概要　ー①事業者と顧客の位置付けの整理ー

- ソフトウェアの特性、責任区分と役割分担、開発供給体制、契約形態などに基づいて、想定される関係者の責務と役割分担を例示。

対象とするソフトウェアの特性は

- 販売/利用するソフトウェア
  - ソフトウェア製品
  - ソフトウェアサービス
  - 組込みソフトウェア、など
- システム・サービスを構成するソフトウェア
  - 自社開発
  - 開発を請負委託
  - 各役割の契約による委託、など

責任区分と役割分類の分担は

- 責任区分
  - サイバーインフラ事業者
  - 顧客　（運用者を兼ねる/兼ねない）
- 役割分担
  - 開発者　（主体、支援）
  - 供給者　（主体、支援）
  - 運用者　（主体、支援、インフラ）
  - 顧客　（主体、支援）

役割分担に影響するその他の要因は

- 開発・供給体制を考慮した役割分担
  - 第三者ソフトウェアコンポーネント
  - 複雑な構成要素
  - セキュリティ欠陥への対応、など
- 契約に基づく役割分担
  - 販売契約
  - 運用契約
  - 準委任型契約、など

※他の要因も検討のうえ役割分担を特定する

ガイドライン案の更新概要　ー①事業者と顧客の位置付けの整理ー

ソフトウェア製品の場合

責任区分＼役割分担	開発者	供給者	運用者	顧客
ソフトウェア開発ベンダー	サイバーインフラ事業者	○			
販売会社	サイバーインフラ事業者		○		
購入者	顧客(運用者を兼ねる)			○	○

- 開発者と顧客は別の事業者であり、供給者はソフトウェア製品の販売代理店または開発者による直販（開発者が供給者を兼ねる）。
- 運用者は、ソフトウェア製品の利用者である顧客自身もしくは顧客の運用部門等が担当する。

■ソフトウェアサービスの場合

責任区分＼役割分担	開発者	供給者	運用者	顧客
サービスプロバイダ（プライム事業者）	サイバーインフラ事業者	○(主体)	○	○	
サービス開発支援（サブ事業者）	サイバーインフラ事業者	○(支援)			
インフラ事業者（サブ事業者）	サイバーインフラ事業者	○			
サービス利用者	顧客(運用者を兼ねる)			○	○

- サービスの開発・供給・運用は、サービス利用者とは別の事業者群が担当。
- サービスプロバイダが、開発者、供給者、及び供給するサービス階層の運用者を兼ねる。
- 責任共有の考え方に基づいて運用者としての各ステークホルダーの責任範囲を定める。

○　　：各々の責任区分において該当する役割
(主体)　　：一般的に主体的な立場で役割を分担する
(支援)　　：一般的に支援的な立場で役割を分担する
(インフラ)　　：システムが動作する基盤を提供する役割
(運用者を兼ねる)：顧客の役割分担に加え、サイバーインフラ事業者の「運用者」相当の責務を負う

ガイドライン案の更新概要　ー①事業者と顧客の位置付けの整理ー

■組込みソフトウェアの場合

役割分担 / 責任区分	開発者	供給者	運用者	顧客
機器開発ベンダー	サイバーインフラ事業者	○			
組込みソフトウェア開発部門	サイバーインフラ事業者	○			
販売会社	サイバーインフラ事業者		○		
購入者	顧客(運用者を兼ねる)			○	○

- 開発者はソフトウェアの開発部門を擁する機器の開発者。
- 組込みソフトウエアを含む機器の運用者は、顧客自身もしくはユーザである顧客の運用部門等が担当。

ガイドライン案の更新概要　ー①事業者と顧客の位置付けの整理ー

■システム（システムオーナーが企画、開発・運用、インフラサービスを調達するケース）

責任区分＼役割分担		開発者	供給者	運用者	顧客
開発運用請負業者	サイバーインフラ事業者	○(主体)	○(主体)	○(支援)	
開発支援	サイバーインフラ事業者	○(支援)	○(支援)		
ソフトウェアコンポーネント開発	サイバーインフラ事業者	○			
インフラ事業者	サイバーインフラ事業者	○	○(インフラ)	○(インフラ)	
調達者（システムオーナー）	顧客(運用者を兼ねる)			○(主体)	○

- システムの利用もしくは提供の主体となる事業者（一般にシステムオーナーと呼ばれる事象者）が、顧客の役割を担当。
- システムの開発・供給・運用は、システムオーナーとは別の事業者群が担当。
- システムオーナー（顧客）の運用部門が、運用者としての役割の全体または運用を外部もしくは引き入れ委託する事象者群の取りまとめを担当。
- 顧客側でセキュリティ要件を含む開発仕様が作成され、ソフトウェア開発を含むシステム開発の完成責任を負う請負型の契約では、請け側の事業者が開発者及び供給者の役割を担当する。
- システム化構想など仕様検討段階の役務提供などでは準委任型の契約を締結する場合、役割分担とその役割に応じた責務の認識と、契約において責務に応じた実施内容の明確化が必要。

ガイドライン案の更新概要　ー①事業者と顧客の位置付けの整理ー

■システム（自社開発、系列事業者が開発・供給・運用を支援するケース）

役割分担 / 責任区分	開発者	供給者	運用者	顧客
親事業者（開発部門）	サイバーインフラ事業者	○(主体)	○(主体)		
系列事業者	サイバーインフラ事業者	○(支援)	○(支援)	○(支援)	
親事業者（運用部門）	サイバーインフラ事業者			○(主体)	
親事業者（利用部門）	顧客				○

■システム（準委任型委託ケース。前提として調達者の利用部門、運用部門、開発部門が各役割に主体として取り組む場合の例）

役割分担 / 責任区分	開発者	供給者	運用者	顧客
調達者（開発部門）	サイバーインフラ事業者	○(主体)	○(主体)		
調達者（運用部門）	サイバーインフラ事業者			○(主体)	
調達者（利用部門）	顧客				○(主体)
コンサル（システム化構想）	顧客				○(支援)
調達事業者（PMO支援）	顧客				○(支援)
開発ベンダ（開発）	サイバーインフラ事業者	○(支援)	○(支援)		
運用ベンダ（運用保守）	サイバーインフラ事業者			○(支援)	○

ガイドライン案の更新概要 ―②ソフトウェアの対象範囲の明確化―

- Webプログラムやクラウドサービス等の対象範囲を明確化。
- OT、IoT機器の他、統一基準のソフトウェア対象に含まれる制御機器の範囲等も踏まえた記述を追加。

名称	説明
ソフトウェア製品	製品として顧客に提供されるソフトウェア
ソフトウェアサービス	クラウドサービスなど顧客が直接利用するITサービス
組込みソフトウェア	OT/IoT機器などのハードウェア製品として提供される組込みソフトウェア及びファームウェア （さまざまな接続機器が対象となる（IoT機器、制御装置、検査装置、輸送機器、医療機器等の各種接続機器など））
システム・サービスを構成するソフトウェア	IT/OTシステムまたはICTサービスを構成するソフトウェア。 専用に開発するソフトウェアのほか、パッケージソフトウェア、ソフトウェアライブラリ、オープンソースソフトウェア、Webプログラム など、システムの構成要素として提供されるソフトウェアを含む

ガイドライン案の更新概要　ー③要求事項の明確化ー

- 適切な要求事項の理解のため表記を見直し。

観点	更新内容
経営層が主体となった取組であることを明確化	• 要求事項(4)-1のタイトルを「経営層のコミットメントと人員の整備」に更新。
事業者と顧客間のライフサイクルについての認識統一	• 5.3章において、顧客のライフサイクル（利用期間）の認識と、事業者のライフサイクル（サポート期限）の認識に差異があることを補足。
運用フェーズに関わる要求事項の明確化	• 運用やモニタリングに関わる要求事項を設けると共に、4.1章において、運用者が関連する要求事項を明確化。
要求事項の必要性を脅威との関係から説明	• ライフサイクル別に、想定される脅威と、脅威に対抗するために要求事項が必要な理由を整理。

ガイドライン案の更新概要　ー④分かりやすさのための記載の充実ー

- 分かりやすさのために表記方法の見直し、記載を補充。

補充の観点	詳細
表記の見直し	• 「ステートメント」という用語の使用をやめ、「要求事項」、「個別要求」に変更。 • 本ガイドライン案はサイバーインフラ事業者と顧客に関する（広く実施が望まれる概念レベルの）責務と責務を果たすための要求事項を整理するため、「経営者」ではなく幅広い役割を意図する「経営層」を使用。 • サイバーセキュリティ基本法に基づく各関係者の「責務」を具体化した記述は「責務」で統一。サイバーセキュリティ戦略における任務保証の考え方に則り、任務の安全かつ持続的な提供に対する責任を具体化した記述は「責任」の用語を使用。 • 本検討会の趣旨および本ガイドラインの対象を踏まえ、「サイバーサプライチェーン」を「ソフトウェアサプライチェーン」に統一。
基本法との関係	• 事業者に対して一定の努力義務を示す第7条と関連することを注意書きとして補足。
用語定義	• ソフトウェアサプライチェーン等を追加。
具体的なインシデント事例の追加	• 自分ごととしてとらえられるようにインシデント事例とリスク要因を追記。 　• 病院のVPNにまつわるインシデント事例 　• SolarWinds 　• Log4J

5. 普及施策

普及施策

- 第1回検討会、ヒアリング、および委員からのコメントを通じて、ガイドライン案を活用した施策、およびガイドライン案そのものの普及等についてご意見を頂いた。
- 第3回検討会にて将来的に考えられる普及施策の骨子をご提示するため、コメント頂きたい。

①ガイドライン案を活用した制度を通じ、事業者の取組を誘導

観点	主なご意見	考えられる普及政策の例
インセンティブ	• 政府調達での優遇、補助金、税制優遇、免責、格付け等のインセンティブを設計してほしい。 • 要求事項を強制するためには法令や罰則を検討してほしい。	• 政府調達等での参照や他の制度等を検討する。 • 本ガイドライン案は、あくまで事業者の自主的な契約を中心とした取組を想定。
タイムスコープ	• ビジネスモデルの見直しが求められるケースもあるという観点も含めて、時間をかけて啓蒙すべきではないか。	• 中長期でのスケジュールを念頭においた普及施策を検討する。
費用負担	• 経営者へコスト配分の考え方を啓蒙すべきではないか。 • 顧客サプライヤーに要求する際の、事業者と顧客のコスト割合を整理すべきではないか。	• コスト配分の啓蒙のための取組みを進める。 • 事業者と顧客のコスト割合について調査した上で、整理を行う。
取組み状況の確認方法	• 契約前に顧客側で契約相手先の取組情報をWebなどで確認できるようにしてほしい。	• 取組み状況をWebで公開することを検討する。

普及施策

観点	主なご意見	考えられる普及政策の例
自己適合宣言時のサプラチェーン上での保証の在り方	• クラウド事業者やオフショア先の保証の在り方を検討してはどうか。	• プライム事業者による保証や、既存の認証制度等による代替策を整理する。
自己適合宣言時の範囲、粒度	• 宣言の範囲を定めるべきではないか。	• 全社、部門単位等の範囲とそのメリットとデメリットを整理した上で、範囲を設定する。
自己適合宣言時の適用先	• プライム事業者に要求するのか、サブ事業者（2層目以降の委託先）に要求するのかを検討すべきではないか。	• 適用先に応じたメリットとデメリットを整理した上で、適用先を設定する。
自己適合宣言の更新頻度	• 1年、2年、3～4年に1回等の複数の意見を頂いた。	• 事業者の負担、技術の進展などの要因を考慮した上で、更新頻度を定める。
自己適合宣言の開始タイミング	• 要求範囲に応じて、制度実施までのリードタイムを確保すべきではないか。	• 自己適合宣言制度開始までのリードタイムを確保する。

普及施策

観点	主なご意見	考えられる普及政策の例
自己適合宣言時の品質担保方法・宣言主体	• 責任限度を示してはどうか。 • プライムの経営者への要求が必要ではないか。 • プライム事業者がソフト開発委託先の更に先までガイドラインを守らせる場合の考え方が必要ではないか。（例えばCIS Benchmarksのバージョン等の具体的な定義が必要） • 取組のエビデンス、サーベイランス等に基づいて認定する。自己宣言とあわせて有識者を含める体制の定義を行った後に、外部からの評価を受ける等、段階的な進め方が考えられるのではないか。 • 経営者名でサインをすることも考えられるのではないか。 • 関連事業者と十分な意見交換が必要ではないか。 • 大手電機メーカーが、審査機関として経済産業省から委託を受け、チェックリストの適用状況を担保することも考えられるのではないか。	• 自己適合宣言の制度設計に際しては、その範囲とあわせて、宣言の主体、責任限度を定める。 • 制度が採用する適合性基準、評価方法等を整備する。

普及施策

②ガイドライン案そのものの普及を通じ、ノウハウ等を浸透

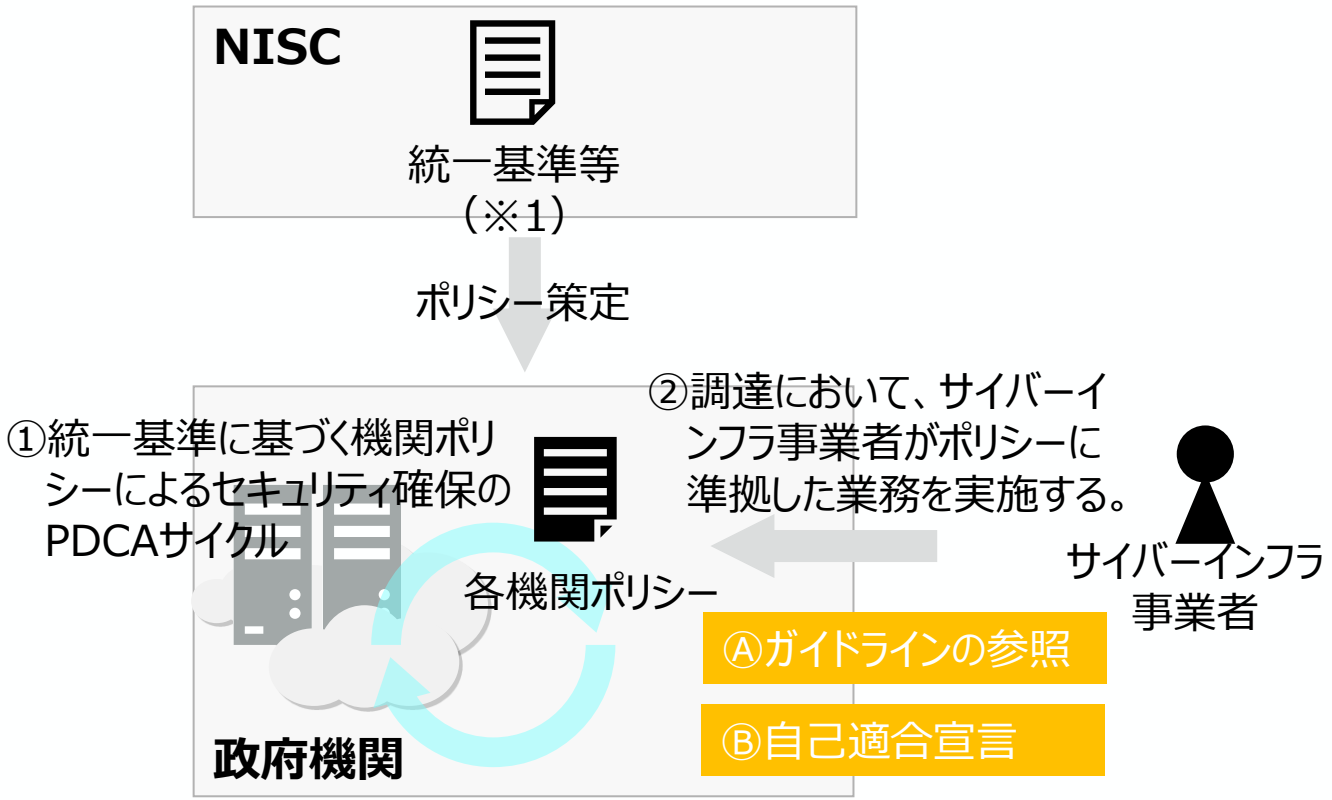
観点	主なご意見	考えられる普及政策の例
ツール、関連ドキュメントの整備	• モデル契約書、テンプレートやフレームワーク等を用意してはどうか。 • 将来、国際整合を意識して取組を行ってはどうか。	• モデル契約書、テンプレートやフレームワーク等を関係機関と連携して作成・配布することを検討する。 • 作成成果物の英語化し、普及展開に活用する。
広報施策	• 中小規模の事業者への広報施策を検討してはどうか。	• 関連組織と連携し広報イベント等を検討する。 • 別施策として検討中の地場事業者向けガイドライン等と連携する。
支援体制	• セキュリティに知見のある事業者が支援できる仕組みを検討してはどうか。	• サイバーインフラ事業者を支援する事業者をサポートする仕組みを検討する。
ガイドラインの継続的な改善	• ガイドラインの効果を検証するフェーズを検討してはどうか。	• ガイドライン公開の一定期間後に、過去に起きたインシデントをモデルケースとして、本ガイドラインの効果検証を検討する。
継続的な改善	• 継続的にガイドラインが利用できるような仕組みを用意してはどうか。	• 自組織がガイドラインの適用状況を継続的に評価・確認する仕組み（ツール）を検討する。
要求パッケージの在り方	• 最低限の要求事項＝ミニマムということだと認識するが、日本語で表記してはどうか。 • ミニマム要求が膨れ上がっており、標準と差がないように思う。見直さないと事業者は対応が難しいのではないか。 • 対応が難しいのではないか。	• 「ミニマム要求パッケージ」は、最低限の要求事項であることを明確にするため「必須要求パッケージ」に変更する。 • 一定の社会インフラの機能としてソフトウェアを対象としていることから、要求パッケージ分類は維持。

普及施策

③その他（本枠組み以外の取組）		
観点	**主なご意見**	**考えられる普及政策の例**
セキュアビルドの検討	• セキュアビルドの確保は重要である。	• 別途検討する。
顧客向けのガイドライン	• 顧客向けのガイドラインを整備してほしい。	• 顧客（幅広い民間事業者）が利用できる粒度の細かいガイドライン整備について検討する。

統一基準の将来的なユースケース

「①ガイドライン案を活用した制度」の将来像の一例として、将来的に政府統一基準等において本ガイドライン案の内容に準拠した自己適合宣言を活用することが考えられる。



本ガイドライン案の利用シーン（案）

Ⓐ最初は、事業者が自身のセキュリティを自主的に向上させるための指針と位置付ける。

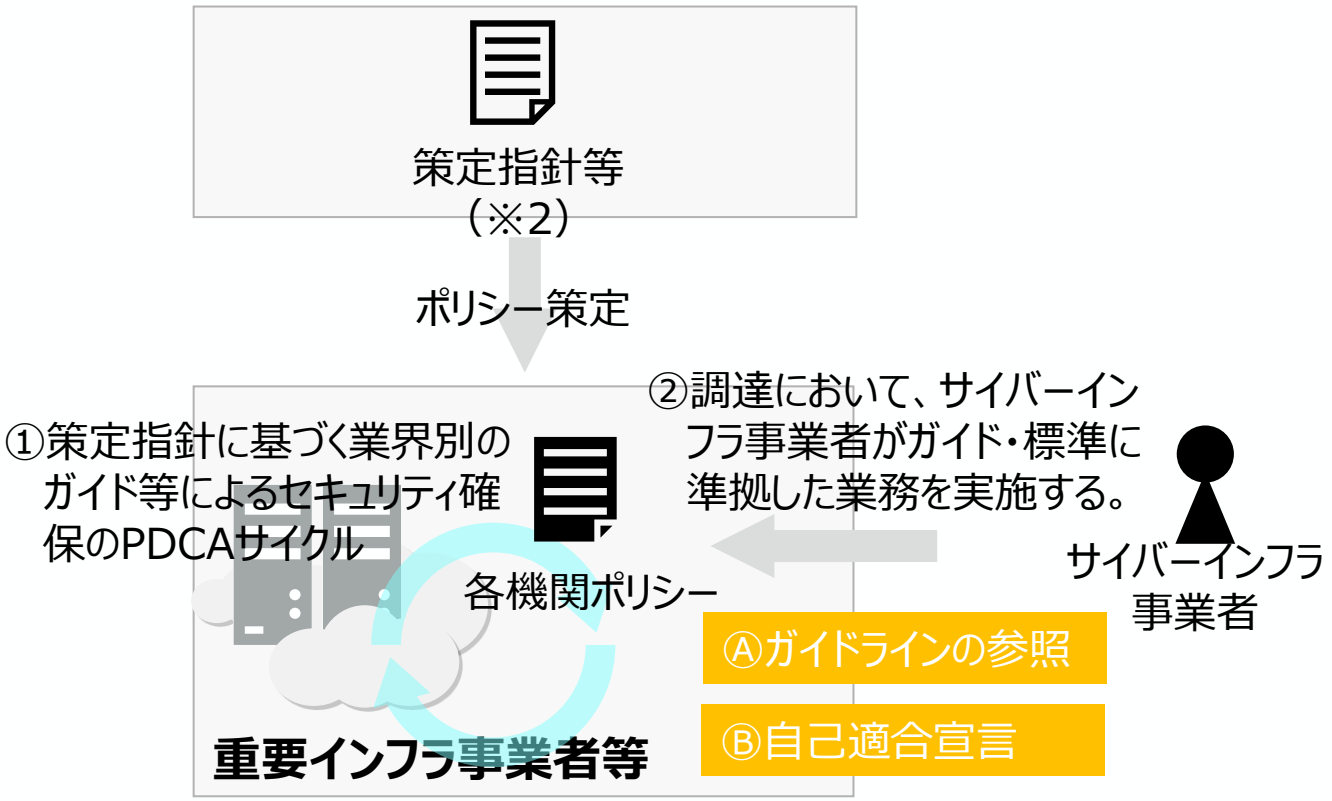
Ⓑ顧客が、事業者のソフトウェアライフサイクルの能力を客観的に把握するために、将来的に事業者の自己適合宣言を参照する。（ガイドの全ての要求事項を満たす必要がある）

事業者が、自身の能力を向上させることが、サプライチェーン全体のセキュリティ確保につながる。

※1　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等

策定指針の将来的なユースケース

「①ガイドライン案を活用した制度」の将来像の一例として、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等を通じて将来的に本ガイドライン案の内容に準拠した自己適合宣言を活用することが考えられる。



本ガイドライン案の利用シーン（案）

Ⓐ最初は、事業者が自身のセキュリティを自主的に向上させるための指針と位置付ける。本ガイドを策定指針を補足する資料として参照。

Ⓑ顧客が、事業者のソフトウェアライフサイクル全般の能力を客観的に把握するために、将来的に事業者の自己適合宣言を参照する。（ガイドの要求事項の中で分野に応じた適切な範囲を満たす必要がある）

事業者が、自身の能力を向上させることが、サプライチェーン全体のセキュリティ確保につながる。

※2　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等

ガイドライン案附属書（活用方法の提案）の作成方針

- 「②ガイドライン案そのものの普及」の将来像の一例として、ガイドライン案がデファクトスタンダートとして活用されるように、普及の端緒として本事業の初期ターゲット対象である政府機関や重要インフラ事業者の調達時の参考情報を提供することが考えられる。

概要	● 本ガイドライン案と、「政府統一基準」・「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」（「対象文書」）との関係を整理する。
読者	● サイバーインフラ事業者
利用方法	● 読者が「対象文書」を参照する際に、本ガイドライン案の関連箇所を参照し、ソフトウェアサプライチェーンセキュリティを向上させるための取組を自主的に進めることに活用する。 ● 将来的な調達において、セキュリティ取組に関する事業者の自己適合宣言を運用する際の参考情報を提供する。

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1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
  - 要求パッケージ分類
- 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

- 第1回検討会とヒアリングを通じて、ガイドライン案を活用した施策、およびガイドライン案そのものの普及等についてのご意見
- 来年度以降、普及を進めるにあたっての附属書の作成方針は適切か
- 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）