経済産業省　NISC

資料４

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9月２４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. 諸外国の取組
3. ガイドライン案
    ① ガイドライン案の位置付け
    ② ガイドライン案の構成案
    ③ ガイドライン案の対象
    ④ 責務の整理
    ⑤ 要求事項の整理
    ⑥ 要求事項と責務の対応関係
    ⑦ 要求事項の概要
4. 検討の進め方
    ① 文献調査
    ② ヒアリング先
    ③ 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

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

検討会開催の背景

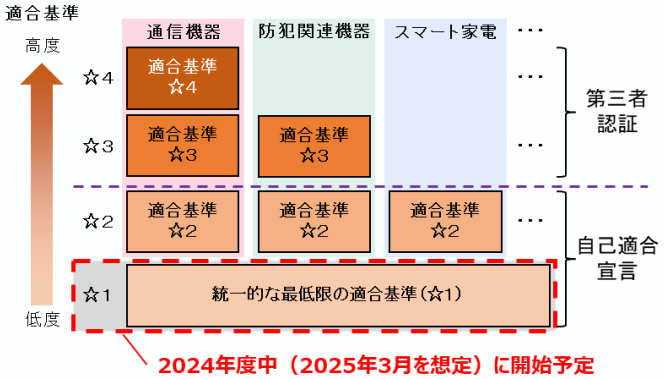
ガイドライン等の実効性の強化
（セキュアなIoT製品及びソフトウェアの流通に向けた取組等）

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。

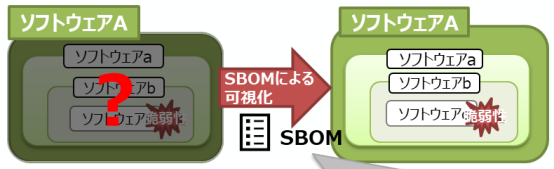
IoTセキュリティ適合性評価制度

- 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

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。

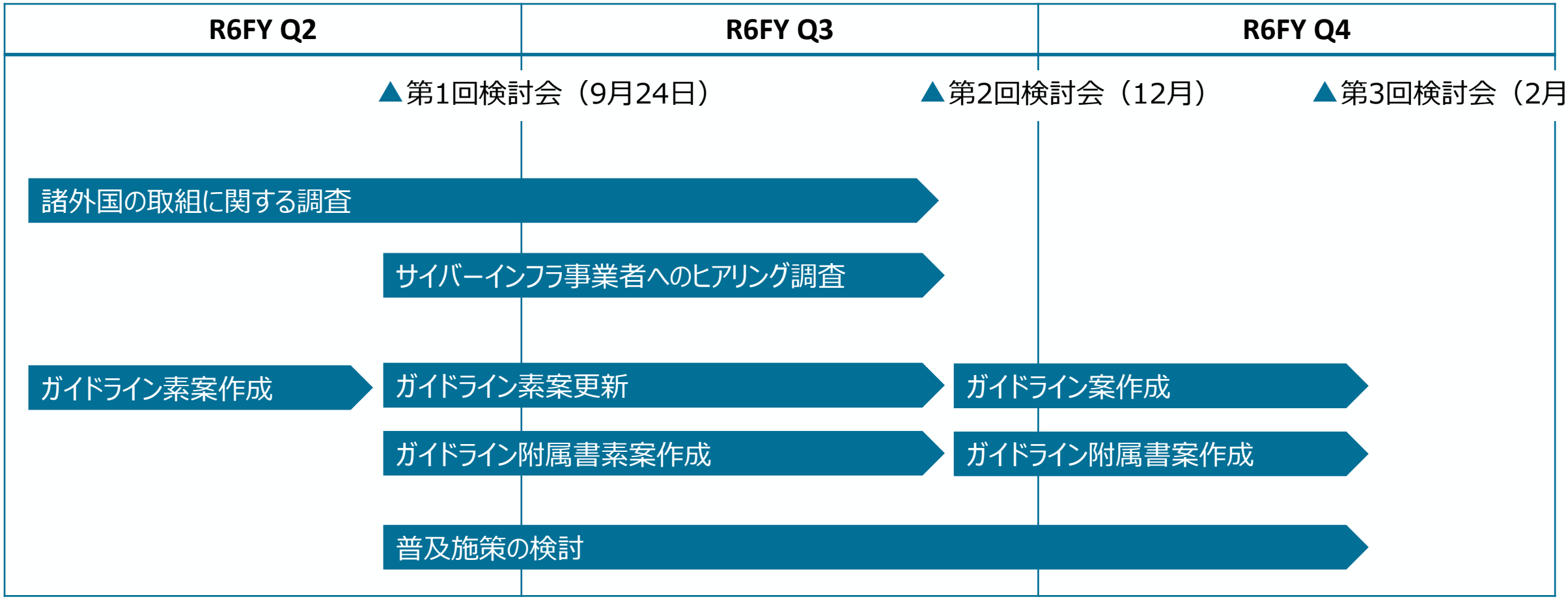
今年度実施予定の内容

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での調達等での参照・推奨等）の検討　など

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素案作成
ガイドライン附属書案作成
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のご報告 • ガイドライン案（更新版）の審議 • ガイドライン附属書案の審議	• ガイドライン案、ガイドライン附属書案の詳細
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. 諸外国の取組

ソフトウェアサプライチェーンに関わる諸外国の取組

- 欧米を中心に、ソフトウェアサプライチェーンにおける脆弱性対策に関わる制度、ガイドライン類の整備が進む。
- セキュア・バイ・デザイン／デフォルトの概念が広まっており、サイバーインフラ事業者には、顧客との適切な役割分担のもと、自社が提供するソフトウェア製品のサイバーセキュリティ対策が求められている。

欧州	
EU 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、**セキュリティを考慮した設計、開発の評価や適合証明書を義務化**。 • 2024年後半に発効見込み。**報告義務を除き、2027年夏頃運用開始を想定。**
英国	
Code of Practice for Software Vendors	• ソフトウェアサプライチェーン攻撃等のリスクに対処するためのソフトウェアベンダー向けの行動規範。**セキュアな設計開発、セキュアな開発環境、セキュアな導入と保守、顧客とのコミュニケーション**の原則から構成。 • 2024年公表。
Guidelines for secure AI system development	• **セキュアバイデザインの観点**から、ソフトウェアのうち AI に焦点を当て、Aセキュアな AI システムの構築を支援するための指針を整理。 • 2023年発表。内閣府科学技術・イノベーション推進事務局及び内閣サイバーセキュリティセンターも署名。

ソフトウェアサプライチェーンに関わる諸外国の取組（つづき）

米国	
NSA SECURING THE SOFTWARE SUPPLY CHAIN / Recommended Practices Guide	• **供給者、開発者、顧客**の3部構成となっており、セキュアなソフトウェアサプライチェーンを確保するために各主体に推奨されるプラクティスを整理。 • 2022年発行。
NIST SP800-218	• ソフトウェア開発者向けに、**ソフトウェアライフサイクル全体で**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**（Secure Software Development Framework：SSDF）。 • 2022年発行。
OMB M-22-18 （M-23-16に更新）	• 政府機関が、ソフトウェアベンダーに対して、**SSDFの実装の適合性を証明する自己適合宣言書**の取得を要求することを定める文書。自己適合宣言書では、SP800-218から抽出した最低限とするセキュアなソフトウェア開発プラクティスに従っていることを宣言。 • 2023年発行。
Supply Chain Cybersecurity Principles	• 米国のエネルギー事業者とそのサプライヤー向けのサプライチェーン・サイバーセキュリティ原則。 • 2024年公表。
Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default	• ソフトウェア開発事業者が脆弱なソフトウェアを商品化しないよう、そして**顧客にセキュリティ確保の負担をできるだけ負わせない**ようにすることを目指し、**セキュア・バイ・デザイン／デフォルトの概念**に基づき、ソフトウェア開発事業者に求められる3つの原則を整理。 • 2023年発行。内閣サイバーセキュリティセンターとJPCERTも署名。

ソフトウェアサプライチェーンに関わる諸外国の取組（つづき）

その他	
日米豪印サイバーセキュリティ・パートナーシップ：共同原則	• 政府間及び産業界のパートナーとの間で**脅威情報を迅速かつ時宜を得た形で共有**すること、政府が調達するソフトウェアに対して**最低限のソフトウェアセキュリティ標準を実施**すること等を求める。 • 2022年公表。
ソフトウェア・セキュリティに関する日米豪印共同原則	• 政府のためのソフトウェアの開発、調達及び利用の指針となる最低限のサイバーセキュリティ・ガイドライン。 • 2023年公表。

3. ガイドライン案

ガイドライン案の位置付け

- ソフトウェアサプライチェーンのセキュリティ確保のため、サイバーインフラ事業者と顧客の自主的な取組を促す。
- サイバーインフラ事業者と顧客が、自組織の取組を振り返り、将来的な政府調達等の要求事項への準拠についての準備を進める際の参考情報となり得るもの。

目的	● これまでの調査結果を踏まえ、**サイバーインフラ事業者と顧客に求められる責務（基本理念に類する事項）**をガイドライン案として示し、サイバーインフラ事業者と顧客によるソフトウェアサプライチェーンのセキュリティ確保の取組を促す。 ● 国内にはサイバー関連事業者を直接規制する法律がない中で、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整理するものである。
成果物	● 具体的なHow（セキュリティ対策の方法・手順）よりも、Shifting the Balance of Cybersecurity Riskなどの諸外国の取組を参考に、**責務として何を求めていくか（What）について、以下の2部構成で整理**する。 **本体：ガイドライン案** 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。 将来的な政府機関や重要インフラ事業者の調達等において、サイバーインフラ事業者向けの要求事項（自己適合宣言相当）として活用することも念頭に置く。 **附属書：ガイドライン案の活用方法** 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、普及の端緒として政府機関や重要インフラ事業者の調達時に参考となる枠組みを提供することを検討中。サイバーインフラ事業者が、目的に応じて参照できるプラクティスを含む。活用例毎に作成。

ガイドライン案の構成案

- サイバーインフラ事業者と顧客に係わる責務と責務を果たすための要求事項をまとめる。

1. 総論	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、本ガイドの提供目的を簡潔に説明。
	1.2　位置付け	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を整理するという位置付けと利用方法を説明。
	1.3　適用対象	サイバーインフラ事業者の範囲、対象とするソフトウェア、想定するリスク概要を説明。
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	サイバーインフラ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	サイバーインフラ事業者の5つの責務と、顧客の1つの責務を整理。
	2.3　ユースケース	ITシステム、パッケージ・IoT製品、クラウドサービス（SaaS）におけるサイバーインフラ事業者と顧客の関係を説明。
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ステートメント）の全体像を説明。
	3.2　要求事項	ステートメント単位の説明。
	3.3　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. 参考情報	4.1　要求事項チェックリスト	要件事項に関する情報を一覧で確認できるチェックリストを 別紙として提示。
	4.2　要求事項に対するプラクティス例	要求事項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整理。
	4.3　参照情報	関連文書リスト、関連文書との対応関係を整理。
	4.4　用語	

ガイドライン案の対象

- 顧客に提供されたソフトウェア製品、情報・通信システムまたはICTサービスを構成するソフトウェア、OTやIoT機器に組み込まれるファームウェアなど、**ソフトウェアライフサイクル上で開発・保守されるソフトウェア**を対象とする。
- 広くソフトウェアに関わるサイバーインフラを提供する**「サイバーインフラ事業者」**と**「顧客」**を含むステークホルダーを対象とする。

ソフトウェアの範囲

名称	説明
ソフトウェア製品	クラウドサービスを含む
IT/OTシステムまたはICTサービスを構成する構成ソフトウェア	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などのソフトウェア製品も含む
OT/IoT機器などのハードウェア製品組込みソフトウェア	ファームウェアも含む

想定する事業者

分類	名称	説明
サイバーインフラ事業者	開発者	システム・サービス開発に従事する事業者・人員
	供給者	顧客に、システム・サービスを提供する事業者・人員
	運用者	顧客に、システム・サービス運用を提供する事業者・人員
ステークホルダー	顧客	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
	その他関係機関	サイバーレジリエンス向上の支援を担う組織

責務の整理

整理方針	• 事業者と顧客に対して、責務として何が求められるかを広く調査し、整理する。 • 各種文献から、共通的およびポイントとされている概念を抽出し、整理する。
参照文献とベンチマーク	• ソフトウェア開発とそのサイバーサプライチェーンを主要なテーマとした先行文書である日米豪印サイバーセキュリティ・パートナーシップ, NIST SP800-218, Shifting the Balance of Cybersecurity Risk, NSA SECURING THE SOFTWARE SUPPLY CHAIN等を主な対象とする。 （文献については、別紙ご参照）

サイバーインフラ事業者

- 文献調査結果から、強靭なソフトウェアサプライチェーンに必要な要素として、**サイバーインフラ事業者の責務（基本理念に類する事項）**に相当すると考えられる概念を抽出し、５つに集約した。

顧客

- 文献調査結果から、強靭なソフトウェアサプライチェーンに必要な要素として、**顧客（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）の責務（基本理念に類する事項）**に相当すると考えられる概念を抽出し、１つに集約した。

要求事項の整理

- 行政機関・重要インフラ事業者をはじめ顧客となる事業者等のソフトウェアサプライチェーンに関わる民間事業者（サイバーインフラ事業者）を念頭に、文献調査に基づき、**<u>責務を果たすための要求事項</u>**を責務と一対に整理する。

整理方針	• 昨年度までの検討結果を踏まえつつ、サイバーインフラ事業者と顧客に対して、責務として何を求めていくかを広く調査し、整理する。 • （実施が望まれる）責務を果たすための要求事項（概念レベル）を責務と一対に整理する。 • 先行する米国、欧州の取組をベンチマークとしつつ、サイバーインフラ事業者の取組状況が異なる点については、要素の追加削除を行う。
参照文献とベンチマーク	• ソフトウェア開発とそのサイバーサプライチェーンを主要なテーマとした先行文書である NIST SP800-218, Shifting the Balance of Cybersecurity Risk, NSA SECURING THE SOFTWARE SUPPLY CHAINを主な対象とする。
整理手順	• ガイドライン本体には、ベンチマークに加えて、その他の文献情報から、共通的な事項を抽出し整理。文献によっては、方針だけではなく、プラクティスや実施例が整理されているところ、これらからも要求事項の実効性確保のために必要なベンチマークしたものは、本書の参考情報として示す。 • 附属書には、普及の端緒として政府機関と重要インフラを念頭に、利用者の利便性を考慮し、本ガイドラインの責務が関連する統一基準と重要インフラ策定指針のプラクティス例を整理する。
分類	• サイバーインフラ事業者と顧客の実行可能性に配慮するため、要求の目的・目標に応じて分類する。（後述）

要求事項と責務の対応関係

- 責務を果たすための要求事項を責務と1対1の関係でカテゴリとして整理。

	責務	要求事項のカテゴリ
サイバーインフラ事業者	(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 • セキュアなソフトウェアの提供と対策評価 • ソフトウェアのライフサイクル全体でのサイバーセキュリティの考慮	セキュアな開発・供給・運用 (1) 脆弱性を抑え、セキュリティを備えたソフトウェアの開発・供給・運用する
	(2)ソフトウェアサプライチェーンの管理 • セキュリティ管理策の実施状況の共有 • ソフトウェア構成情報の共有 • サプライチェーンを含むリスクマネジメントの推進	ライフサイクル管理、透明性の確保 (2) 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
	(3)残存脆弱性への速やかな対処 • 脆弱性と脅威情報の共有と対処	残続する脆弱性の速やかな対処 (3) 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
	(4)ソフトウェアに関するリスク管理の高度化 • サイバーサプライチェーンリスク管理を企業のリスク管理に統合	人材・プロセス・技術の整備 (4) 組織レベルで(人材・プロセス・技術を整備する)
	(5)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 • 関係者間での脅威・脆弱性情報の共有と対処 • サイバーセキュリティに関わる関係者の協働	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 (5) 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
顧客	(6)顧客の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 • 顧客の経営者のリーダー シップによるリスク管理 • 顧客の経営者のリーダーシップによるソフトウェア調達・運用	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 (6) 顧客の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

要求事項の概要

- 要求事項のカテゴリは、複数のステートメント（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	ステートメント
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：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 顧客の経営者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 顧客の経営者のリーダーシップによるリスク管理 (6)-2 顧客の経営者のリーダーシップによるソフトウェアの調達、運用

要求事項の概要　―分類―

- 諸外国の取組との整合、脅威への効果、実行の難易度を踏まえ、2段階に分類する仮説を設定した。

標準要求パッケージ

標準的に実施が求められる共通的な要求事項。組織的な取組を必要とする事項を含む**全ての**要求事項から構成される。

ミニマム要求パッケージ

全てのサイバーインフラ事業者が最低限参照すべき要求事項。**セキュリティ対策の実施と脆弱性の対処**に関する要求事項のみから構成される。

諸外国の取組との整合	脅威への効果	実行の難易度
諸外国の取組に合致 参照する諸外国の取組の要求内容と合致する	**直接的・即効性あり** 脅威への直接的な対策効果が期待できる	**比較的高い** 採算面で懸念があり、技術的にも難易度が高い
諸外国の取組にない 参照する諸外国の取組が求めていない	**能力をより高める** 持続的な取組により対策効果が得られる	**比較的低い** 採算性があり、技術的にも対応が比較的容易

全ての要求事項

【諸外国の取組に合致】	：	諸外国の取組に含まれる要求事項
【直接的・即効性有】 ＋【比較的低い】	：	諸外国の取組に含まれないが、国内の取組として着手すべきと考えられる要求事項 （効果の観点で積極的な取組が求められ、負担が限定的と見込まれる要求事項）

標準要求パッケージ

ミニマム要求パッケージ

要求事項の概要　―分類―

諸外国の取組との整合性

■ **仮説**

- 参照する取組は、実務適用に動き出している知見として有効である。ハーモナイズは現時点では不明確であるものの、特に政府調達にプライム対応するサイバーインフラ事業者には、取組の整合性は海外展開時の負担軽減につながる。
- 米国OMB M-23-16では、SP800-218から抽出した**最低限とされるセキュアなソフトウェア開発プラクティスに従って開発**されていることの宣言を要求している。また、EU Cyber Resilience Actでは、**製品開発においてサイバーセキュリティ**を考慮し、**脆弱性対処**、**サイバーセキュリティの透明性**を要求している。
- **先行する取組の要求仕様は、優先して取組を求める**ことが望ましい。

■ **分類基準案**

諸外国の取組に合致：　参照する諸外国の取組と合致する要求事項
諸外国の取組にない：　それ以外のもの。

諸外国の取組に合致	**サイバーインフラ事業者**	OMB M-23-16, Cyber Resilience Actの要求内容と合致する要求事項 • 委託先との要件合意、セキュアコーディング、コードの要件確認と出所管理、コードのアクセス制御、開発環境の保護、テスト、開発・運用ポリシーの制定、脆弱性対応、顧客への情報提供等
	顧客	Shifting the Balance of Cybersecurity Riskと合致する要求事項 • 調達時のリスク評価、リソースの整備、サイバーインフラ事業者への要求提示
諸外国の取組にない	**サイバーインフラ事業者**	上記以外の要求事項 • 脅威モデリング、設計の追跡、標準セキュリティ機能のサポート、セキュアな代替コンポーネントの開発、組織体制の整備（トレーニング、経営層のコミットメント）、脆弱性の根本対策等
	顧客	

要求事項の概要　―分類―

脅威への効果

■ **仮説**

- 脅威に対する対抗策として重要かつ直ちに取組むべき要求事項とそのような緊急性の高くない要求事項とを整理することが有効である。
- ソフトウェア調達の計画段階から廃棄までのサプライチェーン上のライフサイクル全体の脅威シナリオを検討し、**脅威への直接的な対策効果が期待できる取組**を優先する。

■ **分類基準案**

直接的・即効性有　：脅威への直接的・即効性のある効果が期待できる要求事項
能力をより高める　：脅威への対応能力をより高めるための踏み込んだ対策に関する要求事項
（組織としての持続的な取組により対策効果が得られる）

直接的・即効性有	**サイバーインフラ事業者**	• 委託先との要件合意、セキュアコーディング、コードの要件確認と出所管理、コードのアクセス制御、開発環境の保護、テスト、開発・運用ポリシーの制定、脆弱性対応、顧客への情報提供等
	顧客	• 調達時のリスク評価、事業者への要求提示
能力をより高める	**サイバーインフラ事業者**	• リスクモデリング、要件のトレース、組織としてのソフトウェアセキュリティ要件の確立、人員教育、脆弱性を根本的に削減する組織プロセスの整備、外部組織との情報連携等
	顧客	• 外部組織との情報連携、予算確保

要求事項の概要　―分類―

実行の難易度

■ **仮説**

- ソフトウェアサプライチェーン上のセキュリティ確保するという観点で、必要かつ妥当なコストであり、責務と役割分担に照らして十分実行可能性のある要件かどうかを整理することが有効である。
- サイバーインフラ事業者における実行可能性に配慮するため、**コスト的にも採算性があり、技術的にも対応が容易な要求事項**は取組を求める。

■ **分類基準案**

比較的高い：　技術的およびコスト面で懸念があり、実行難易度が比較的高い要求事項。
特に、個社で費用負担が増大することが想定されるもの。

比較的低い：　コスト的にも採算性があり、技術的にも対応が比較的容易である、実行難易度が比較的低い要求事項。

比較的高い	サイバーインフラ事業者	• リスクモデルの整備、セキュアな開発プロセスの維持と更新、役割の整備、人員教育、経営層によるコミットメント等
	顧客	• 全ての要求事項
比較的低い	サイバーインフラ事業者	• テスト、脆弱性の対処、コードのアクセス制御、コンポーネントのサポート期間の確認、利用者への情報提供、脆弱性情報の委託先への提供、脆弱性情報の通知サービスの利用等
	顧客	―（なし）

4. 検討の進め方

文献調査

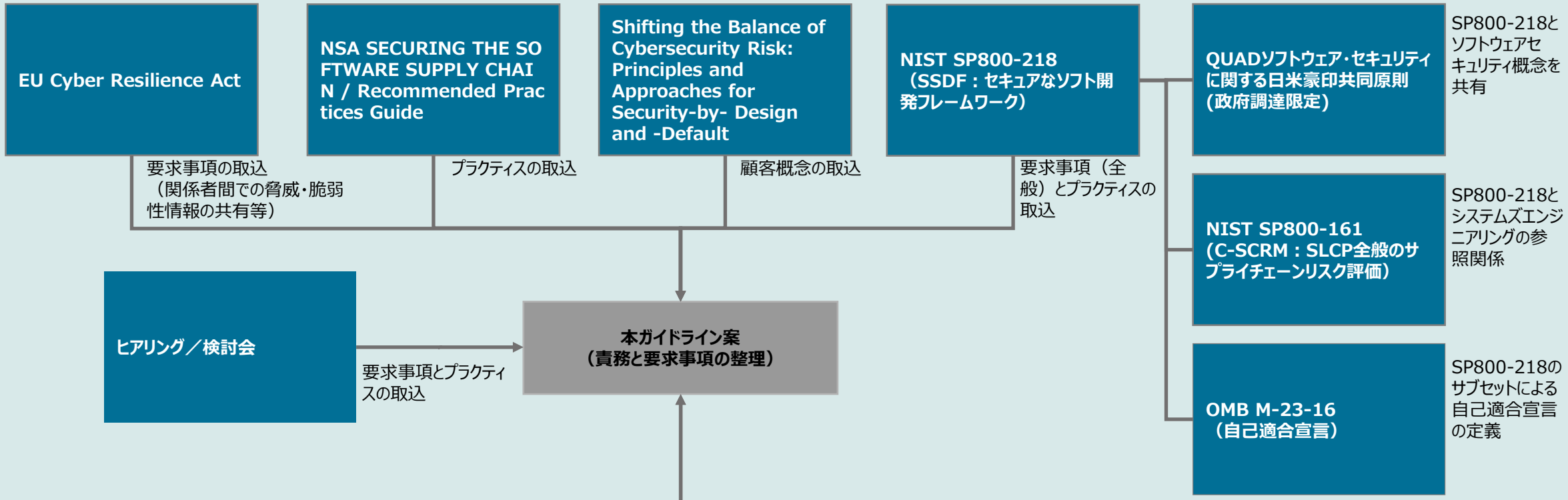
- 主な調査対象は以下の通り。

- 注目する文献
  - OMB M-23-16
  - CISA Shifting the balance of Cyber Security Risk, Secure by Demand Guide
  - NIST SP800-218, SP800-218A, SP800-161
  - EU Cyber Resilience Act
  - NSA Securing the Software Supply Chain
  - QUAD ソフトウェア共同声明
  - DoE Supply Chain Cybersecurity Principles
  - DSIT Code of Practice for Software Vendors
  - ISO27036, ISO27002（JISQ27002）、ISO27017
  - NCSC Guidelines for secure AI system development
  - NISC 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，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，サイバーセキュリティ基本計画，重要インフラ行動計画
  - 経済産業省 IoTセキュリティ適合性評価制度，情報セキュリティサービス審査登録制度

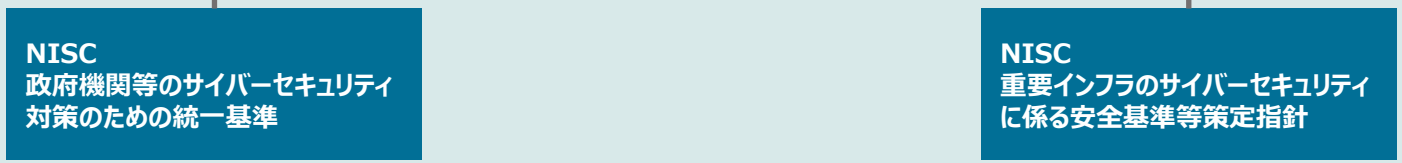
※昨年度有識者からご提供頂いた文献については、調査したうえで、本年度のガイドライン案の構成に対して必要に応じて適用する。

文献調査

ガイドライン案と主な参考文献との関係



ガイドライン案と既存の国内の取組との整合も確認



ヒアリング

- ガイドライン案の調査や参考となる事例や内容に関する意見等を収集するため、サイバーインフラ事業者や顧客にヒアリングを実施する。

- ヒアリング先：
  - ソフトウェアセキュリティに関わる主要なサイバーインフラ事業者業界団体
  - 実効性を確保するため、ソフトウェアサプライチェーンを構成する2次請け以降のサイバーインフラ事業者
- ヒアリング項目：
  - 過年度のヒアリング先を中心に、ガイドライン案の更新内容への意見
  - 要求事項の分類の妥当性への意見
  - ソフトウェアサプライチェーンの実態に関わる事項（サイバーインフラ事業者と顧客との要件調整、役割分担、商流、対策例等）

ご意見をいただきたい事項

1. 責務と要求事項について

- 責務と要求事項の内容は適切か
  - 検討対象は適切か。
  - 責務の内容は調査背景・意図に照らして適切か
  - 責務の内容について、考慮すべき事項はないか
  - 要求事項の内容は調査背景・意図に照らして適切か
  - 要求事項の内容について、考慮すべき事項はないか
  - 要求事項の分類は適切か

2. 検討の進め方について

- 責務と要求事項の整理に向けて、追加の文献調査・ヒアリングを実施して明らかにすべきことがあるか
- ガイドライン案本体の構成が妥当か（詳細については、第2回検討会にてお願いいたします）

3. その他　今後の事業などについて

- 来年度以降、自己適合宣言を検討する場合に、考慮すべき事項があるか
- 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）