経済産業省　NISC

資料８

「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）

― ソフトウェアの開発、供給、運用におけるサイバーセキュリティ確保とレジリエンス向上のための顧客とサイバーインフラ事業者の適切な役割分担と責務の在り方について―」

の概要

「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。
- 令和６年度、ガイドライン（案）をとりまとめたところであり、令和7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。

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設計・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) 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

(6) 顧客の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

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）全体概要

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に求められる責務(基本理念に類する事項)、及び責務を果たすための要求事項を6つに整理。今後は活用促進に向けた自己適合宣言等の制度検討等の取組を実施予定。

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、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設計・開発・供給・運用	セキュアな設計・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）
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。

サイバーインフラ事業者及び顧客に求められる要求事項（一覧）

- 責務を果たすための要求事項は、責務と1対1の関係でカテゴリとして整理。
- サイバーインフラ事業者に求められる５つの要求事項、顧客に求められる１つの要求事項を以下に示す。

	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) セキュアな設計・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) 残存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

【サイバーインフラ事業者 要求事項 例】セキュアな設計・開発・供給・運用

セキュアなビルド

開発言語や開発環境に適したセキュアコーディング及びシステム構築のプロセスを定義し、これにしたがいコードを生成・ビルドする。設定を含むコードのレビュー及び分析を実施し、対応結果をプロセスにフィードバックする。

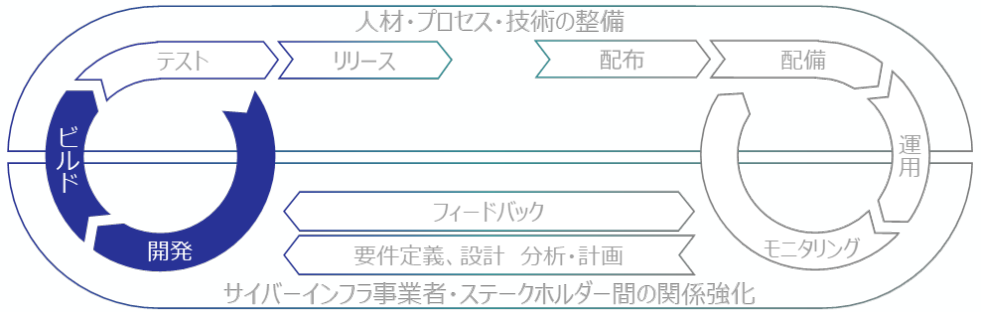
S(1)-2

開発者

供給者

運用者

顧客



個別要求

- ☐ **S(1)-2.1 セキュア開発プロセス定義**
  セキュアコーディングの観点、ビルド実施タイミングと方式、自動化ツールの利用、トレーニングなど、セキュアコーディング、セキュアビルド及びデフォルトセキュアに関するプロセスを定義する。
- ☐ **S(1)-2.2 セキュアビルド**
  実行可能形式のセキュリティを向上させる機能を提供するコンパイラ、インタプリタ、及びビルドツールを使用し、コードを生成・ビルドする。
- ☐ **S(1)-2.3 検証とフィードバック**
  レビュー及び分析による検証により発見された問題の根本原因を特定し、その対応結果をプロセスにフィードバックする。
- ☐ **S(1)-2.4 コードベース**
  レビュー及び分析の対象は、ソースコードのみでなく、可読性があると組織が決定したさまざまな形式のコード（設定ファイル等）も対象とする。

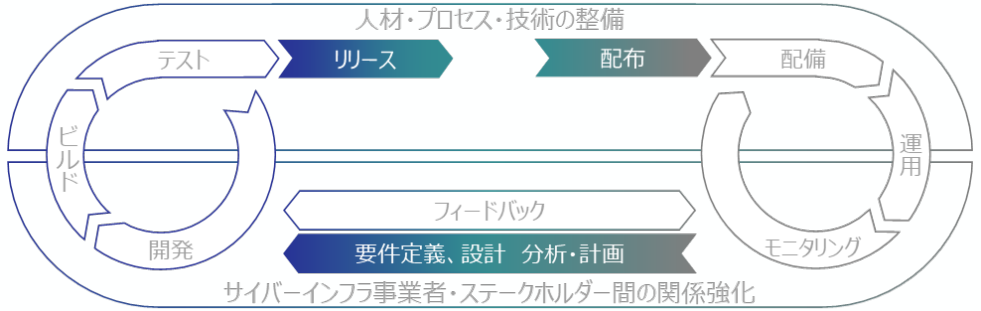
【サイバーインフラ事業者 要求事項 例】ライフサイクル管理、透明性の確保

リリースファイルやデータのセキュアなアーカイブ

ソフトウェアのリリースごとに保持すべき必要なファイルやデータをアーカイブし、必要な人員、ツール、サービスのみにアクセスを制限する。ソフトウェア部品表（SBOM）の段階的な採用などを通じて、各リリースの全てのコンポーネントについて、出所データを収集、保護、維持、共有する。

S(2)-2

- 開発者
- 供給者
- 運用者
- 顧客



個別要求

- ☐ **S(2)-2.1 コードベースの保護**
  全ての形式のコードベースを不正アクセスや改ざんから保護するために、リポジトリにコードや設定情報を保管し、承認された担当者、ツール、サービスなどのみがアクセスできるよう最小権限の原則に基づいたアクセス制御を実施する。
- ☐ **S(2)-2.2 リリースのアーカイブ**
  リリース後に発見された脆弱性を分析、特定できるようにするために、各ソフトウェアのリリースをアーカイブ化して保護する。
- ☐ **S(2)-2.3 リリースの出所データの共有**
  各ソフトウェアリリースの全てのコンポーネントの出所データを収集、保護、維持、共有する。

＜参　考＞

サイバーインフラ事業者及びステークホルダーについて①

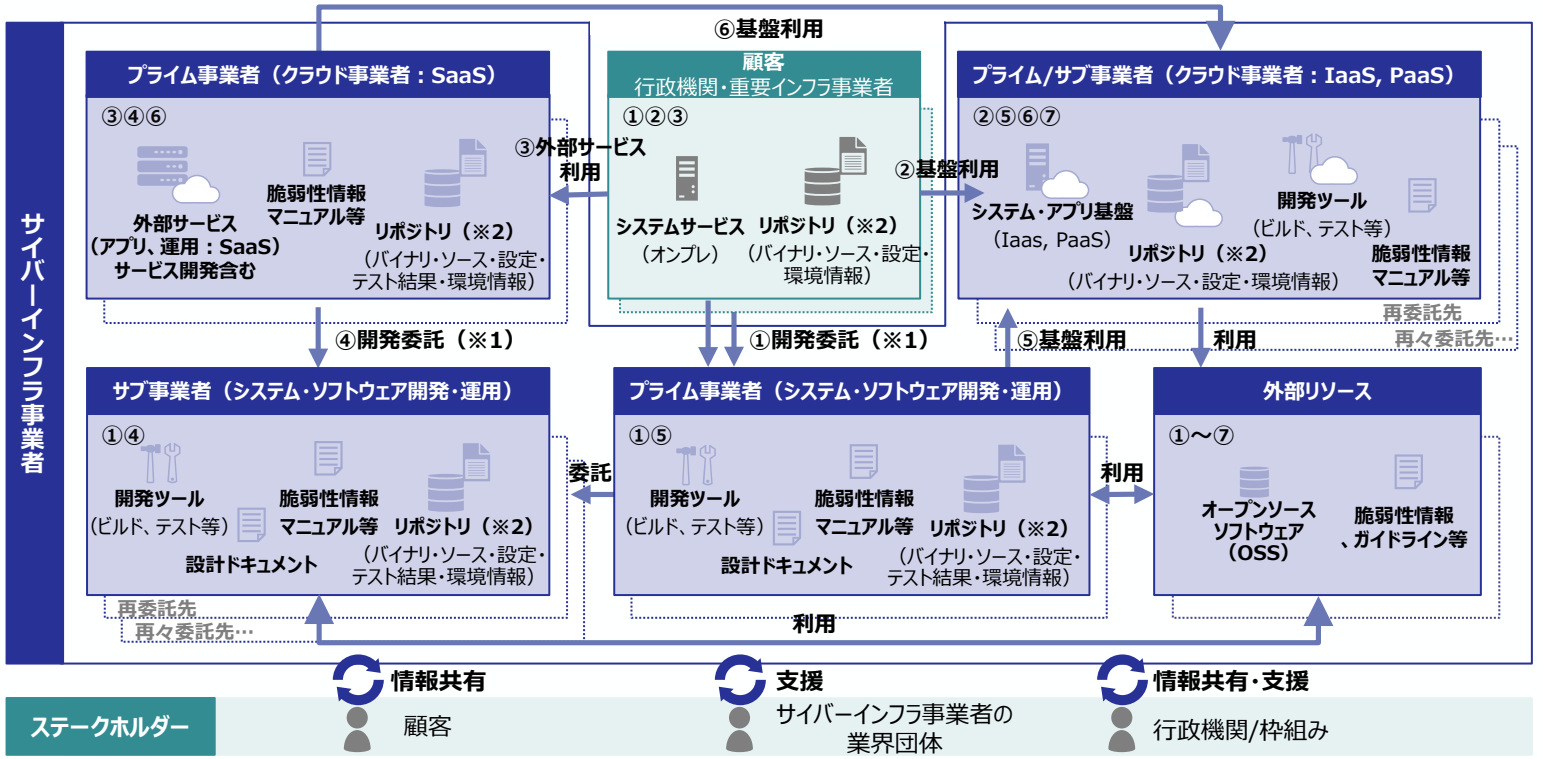
- 本ガイドライン（案）では、広くソフトウェアの開発・供給・運用に関わる「サイバーインフラ事業者」を対象として想定し、開発者、供給者、運用者の3つの主な役割で分類。
- ソフトウェアのサイバーセキュリティに関わるレジリエンスを向上するためには、サイバーインフラ事業者は、インシデントの防御を対象とした関わりだけではなく、インシデントの事前対処と事後対処における情報収集、分析、対処調整の協力者として、さまざまな面で関係を強化していくことが求められる。

分類	名称	説明
サイバーインフラ事業者	開発者	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、あるいはこれらのソフトウェアで構成されるシステム・サービスの設計を含めた開発又はインテグレーションに従事する事業者・人員 ソフトウェア開発ベンダー、ソフトウェアサービスプロバイダ、機器開発ベンダー、ソフトウェアやシステムの開発請負事業者、ソフトウェアコンポーネント開発事業者、インフラ事業者、自社開発ソフトウェアの開発部門などにおいて、ソフトウェアの開発又はインテグレーションを行う事業者等が対象となる。
	供給者 [1]	顧客にソフトウェア製品、ソフトウェアサービス、組込みソフトウェア（ハードウェア製品を含む）、あるいはこれらのソフトウェアで構成されるシステム・サービスを提供する事業者・人員 ソフトウェア製品やソフトウェアを含む機器の販売会社、ソフトウェアサービスプロバイダ、システムの開発運用請負事業者、インフラ事業者、ソフトウェア開発ベンダーなどにおいて、ソフトウェアやシステム・サービスを提供する事業者等が対象となる。
	運用者	顧客に対して主にシステム・サービスの運用を支援する役務を提供する事業者・人員
ステークホルダー	顧客	政府機関等及び重要インフラ事業者をはじめ、ソフトウェアの利用主体となる事業者等
	その他関係機関 [2]	サイバーレジリエンス向上の支援を担う組織

[1] 供給者内に、開発者・運用者が含まれるケースもある。また、サイバーインフラ事業者に販売会社が含まれるケースでは、供給者に準じた責務が求められる。
[2] ソフトウェアの利用主体である顧客がソフトウェアを運用することが一般的であるが、システム・サービス又はこれらを構成するソフトウェアの運用には専門的な知識や技能が必要な場合も多い。ここでは、顧客との契約により、サイバーインフラ事業者がソフトウェアの運用（又はその一部）を支援する場合を想定する。

サイバーインフラ事業者及びステークホルダーについて②

- 本ガイドライン（案）が対象とするサイバーインフラ事業者が扱うソフトウェアの資産について、ソフトウェアで構成するシステムの開発・契約形態・利用形態を踏まえた関係は以下の図のとおり。
- システムの開発・契約・利用の観点から、サイバーインフラ事業者には、以下の2つの役割を想定。
  プライム事業者：顧客と直接契約を結びシステムやクラウドサービスの開発・供給・運用を実施する1次請け事業者
  サブ事業者：プライム事業者と契約を結びシステム・クラウドサービスの開発・供給・運用を実施する2次請け以降の事業者



※1 ①④にて下請けを使用しないケースもある。顧客がサイバーインフラ事業者として自ら開発するケースもあり。

※2 サービス及びシステム開発や契約形態等によりソフトウェアの所有権が異なるが、所有権については表記していない。

[システムの開発・運用・利用形態の例]
①：オンプレミスのシステム（プライム事業者に開発委託）
②：顧客がIaaS, PaaSを利用
③：SaaSを利用したシステムの利用
④：クラウド事業者（SaaS）が開発委託
⑤：プライム事業者（SIer等）がIaaS, PaaSを利用
⑥：クラウド事業者（SaaS）がIaaS等を利用
⑦：クラウド事業者（IaaS, PaaS）が相互利用

サイバーインフラ事業者及び顧客に求められる要求事項（全体像）

- サイバーインフラ事業者と顧客は、サイバーセキュリティに関するレジリエンス向上の責務を果すために、対象となるソフトウェアの特性や組織に適した方法で、以下のサイバーセキュリティ対策の要求事項（6のカテゴリ、21の要求事項）を実施することが求められる。
- これらを実現するため、組織のリスクマネジメントを担う経営層のリーダーシップの下、リスクに応じた対策の実施方針、予算や人材の割り当て、実施状況の確認や問題の把握と対応、その他の関係機関との協力等を的確に進めることが求められる。