経済産業省

国家サイバー統括室
National Cybersecurity Office

「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

令和７年10月

「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※1 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年度中に、ガイドライン（案）としてとりまとめ、令和7年度、ガイドラインを成案化すると共に、活用促進に向けた付属文書としてのチェックリストの拡充、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。

※1：令和７年７月重要インフラ専門調査会の廃止に伴い、経済産業省 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 分野横断サブワーキンググループ 及び 内閣官房国家サイバー統括室 の合同ワーキンググループとして位置付け変更

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内閣官房国家サイバー統括室も共同署名

・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※2

サイバーインフラ事業者

○**ソフトウェア**※3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

※2：諸外国の関連ガイドライン等を参照

※3：製品として顧客に提供されるソフトウェアのほか、クラウドサービス等のソフトウェアサービス、IT/OT/IoT機器等のハードウェア製品として提供される組み込みソフトウェア・ファームウェア、システム・サービスの構成要素として提供されるソフトウェアも含む。

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

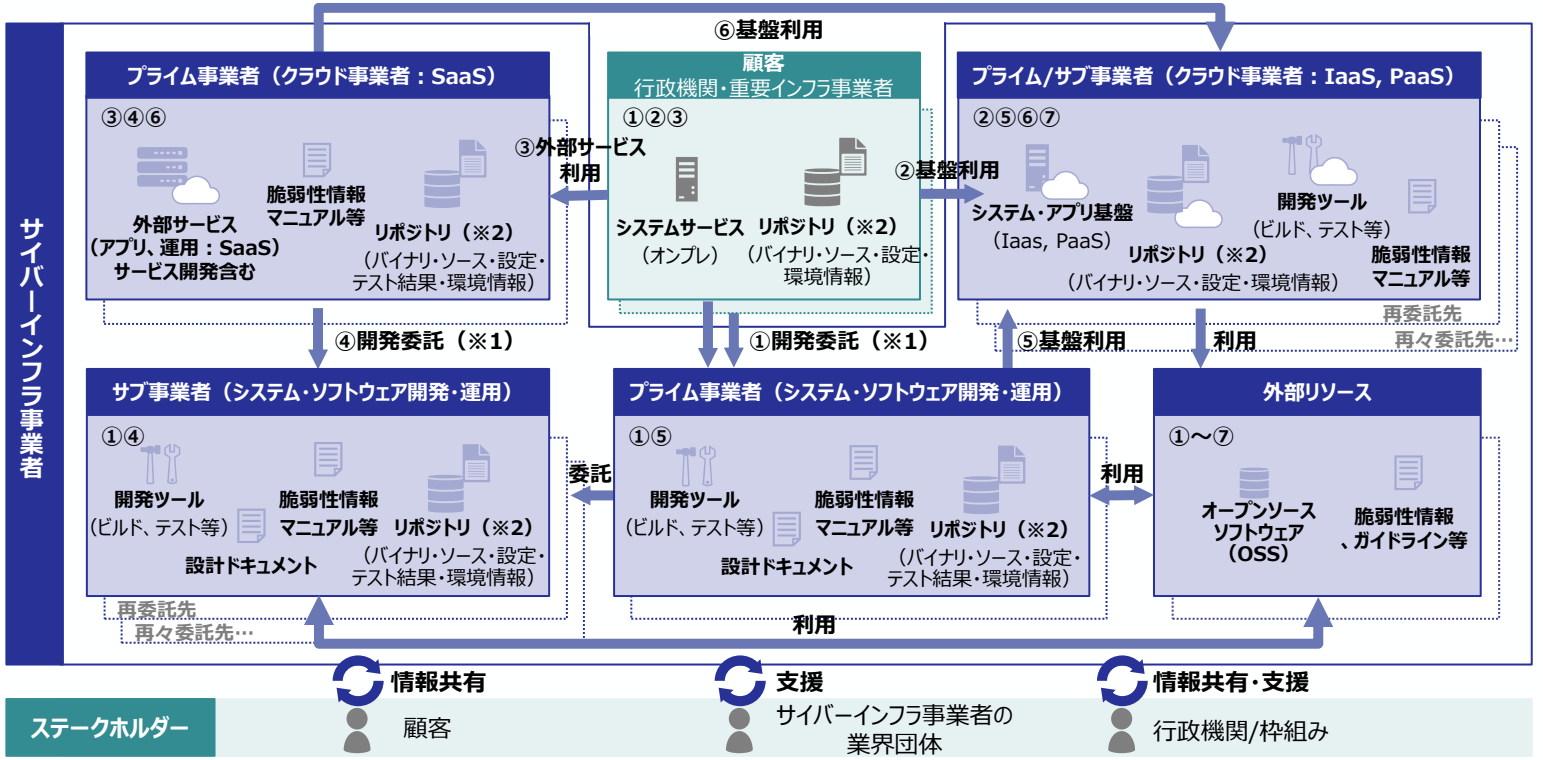
- 本ガイドライン（案）では、広くソフトウェアの開発・供給・運用に関わる「サイバーインフラ事業者」を対象として想定し、開発者、供給者、運用者の3つの主な役割で分類。
- ソフトウェアのサイバーセキュリティに関わるレジリエンスを向上するためには、サイバーインフラ事業者は、インシデントの防御を対象とした関わりだけではなく、インシデントの事前対処と事後対処における情報収集、分析、対処調整の協力者として、様々な面で関係を強化していくことが求められる。

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、組み込みソフトウェア、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、組み込みソフトウェア（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始め、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

サイバーセキュリティ基本法の改正

- 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の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）により、**サイバーセキュリティ基本法が改正され、情報システム等供給者に対する責務（努力義務）が新たに規定**された（第７条第２項の新設）。
- サイバーセキュリティ基本法第７条第１項及び第２項を踏まえ、情報システム等の供給者としてソフトウェアの開発・供給・運用を行う事業者を「サイバーインフラ事業者」と称し、その具体的な役割等を整理した国内のガイドラインとして、「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）」を取りまとめ。

（サイバー関連事業者その他の事業者の責務）

第七条　サイバー関連事業者（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をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

２　**情報システム若しくはその一部を構成する電子計算機若しくはプログラム、情報通信ネットワーク又は電磁的記録媒体（以下この項において「情報システム等」という。）の供給者**は、サイバーセキュリティに対する脅威により自らが供給した情報システム等に被害が生ずることを防ぐため、情報システム等の**利用者がその安全性及び信頼性の確保のために講ずる措置に配慮した設計及び開発、適切な維持管理に必要な情報の継続的な提供**その他の情報システム等の**利用者がサイバーセキュリティの確保のために講ずる措置を支援する取組**を行うよう努めるものとする。

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）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。今後はガイドラインの活用促進に向けた付属文書としてのチェックリストの拡充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(現NCO)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

- ガイドラインの活用促進に向けた付属文書としてのチェックリストの拡充、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の責務①

- サイバーセキュリティに関するレジリエンスを向上させるためには、サイバーインフラ事業者と顧客がそれぞれの責務を果たすことで、相補的な効果を得ることができる。
- サイバーインフラ事業者は、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に、以下の５つの責務を認識することが求められる。これらの全ての責務は、サイバーインフラ事業者の経営層が認識し、経営層のリーダーシップにより責務を果たす取組を実施することが求められる。

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

- **セキュアなソフトウェアの提供と対策評価**
  - 「セキュアバイデザイン」及び「セキュアバイデフォルト」の原則に則り、リスクベースのアプローチにより、ソフトウェア開発・運用に対する脅威を軽減するための対策を実施し、その有効性を判断する。
  - 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。
- **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**
  - セキュリティ要件の合意に始まり、セキュアなビルド、テスト、運用等、顧客と合意したソフトウェアライフサイクル全体にサイバーセキュリティを考慮する。

サイバーインフラ事業者の責務②

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**
  - 利用者がソフトウェアの調達と導入に関して、リスクに基づいたソリューションの選択を含む意思決定を行えるよう、供給者はソフトウェア開発の取組状況を開示する。顧客に周知する必要があるサイバーセキュリティの側面について透明性を確保する。
- **ソフトウェア構成情報の共有**
  - 利用者による脆弱性対策のため、ソフトウェア部品表（SBOM）、設定情報をはじめとするOSSも含めたソフトウェアの構成管理による情報を活用する。
- **サプライチェーンを含むリスクマネジメントの推進**
  - 供給者（システムインテグレーター、外部システムサービスプロバイダ、パートナー等）、開発者、その他の関連するIT/OT/ICT関連の事業者全てをソフトウェアサプライチェーン・リスクマネジメントの活動範囲に含める。

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**
  - 脆弱性開示ポリシーを整え、脆弱性対応に関する体制を整備する。
  - ベンダーは、クラウドサービス・ソフトウェアの脆弱性の特定と開示、セキュアなサービス構成と運用に必要な情報の提供、サービスのバージョンアップ、パッチの開発と配布に責務を有すること、ベンダーはバージョンアップ・パッチ適用プロセスを文書化して、顧客がプロセスへの参加方法を理解できるようにする。
  - 顧客に確実に通知する仕組みを整える。

サイバーインフラ事業者の責務③

4　ソフトウェアに関するガバナンスの整備

- **ソフトウェアサプライチェーン・リスク管理を企業のリスク管理に統合**
  - ソフトウェアサプライチェーン・リスク管理は、ソフトウェアライフサイクル全体にわたる活動を対象とし、企業のリスク管理プロセスの一部として集約する。
  - 自組織として許容可能なレベルまでリスクを低減するために必要なリソース（ヒト、モノ、カネ）を整える。サイバーセキュリティを経営の重要事項として位置付け、トップマネジメントがリスクマネジメント実施の責務を負う。
  - 法令を遵守する。

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・協力体制の強化

- **関係者間での脅威・脆弱性情報の共有と対処**
  - 脅威情報・脆弱性情報を、政府及び産業界のパートナーとの間で迅速かつ時宜を得た形で共有する。
  - 供給者がソフトウェアの脆弱性情報を所管する機関と共有する。
- **サイバーセキュリティに関わる関係者の協働**
  - コミュニティを含む全てのステークホルダーが健全に連携し合う。
  - 潜在的なリスクを特定し、サイバーセキュリティに関連するサプライチェーン・リスクの依存関係を評価するための枠組みを開発するために協働する。
  - セキュリティ対策は、プラットフォームプロバイダや消費テナント組織等も含むサプライチェーン全体で責務を共有して取組む。
  - 民間部門が、政府と協力しながら、必要な要件に継続的に適応し、重要インフラを提供する事業者が依存する技術、製品及びサービスのセキュリティを改善する。
  - ステークホルダーの適切で時宜を得た参加により、知識、認識等を共有でき、適切なリスクマネジメントにつながる。

サイバーインフラ事業者の顧客に求められる責務

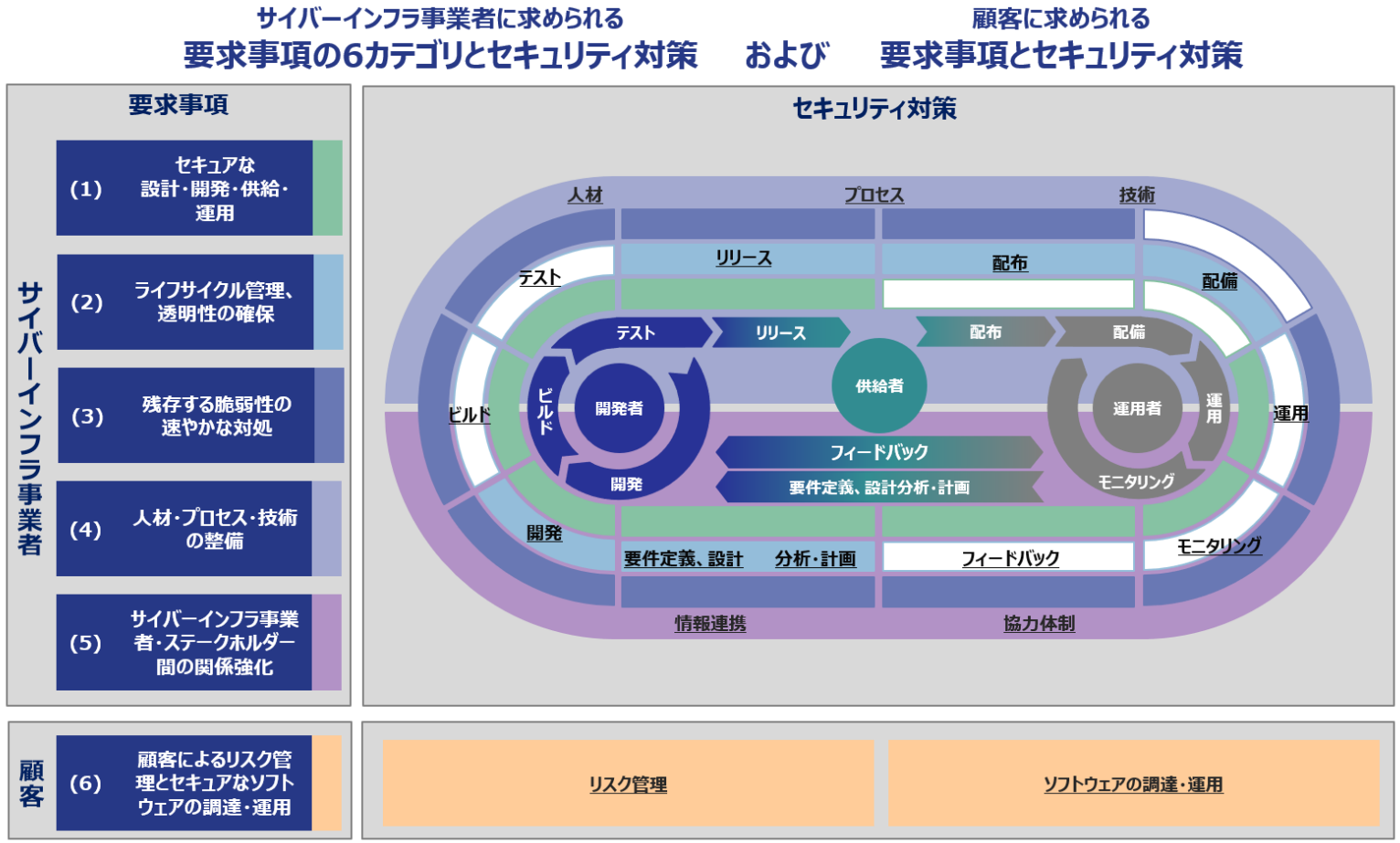
- 顧客がオーナーシップを持つシステムを構成するソフトウェアのセキュリティに関わる活動において、顧客には以下の責務が求められる。

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

- **顧客の経営層のリーダーシップによるリスク管理**
  - 顧客の独立した主体的な取組及びサイバーインフラ事業者との契約に基づく協力的な取組によるリスク管理
  - 既知の脆弱性への対処及び緩和策を主体的に実施するためのリソースの割り当てと整備
  - セキュリティ改善を目的とするコミュニティや協力体制の活用
- **顧客の経営層のリーダーシップによるソフトウェア調達・運用**
  - ソフトウェア設計計画にセキュリティ機能を組み込むためのセキュリティ要件の提示
  - ソフトウェアの調達・導入におけるセキュリティ慣行の要求の開示
  - ソフトウェアの調達・導入におけるリスク評価に基づいた意思決定
  - ライフサイクルを考慮したソフトウェアの運用、リスク対応及び契約に係る予算確保

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たすために、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。



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

＜参考＞

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）の要求事項（全体）

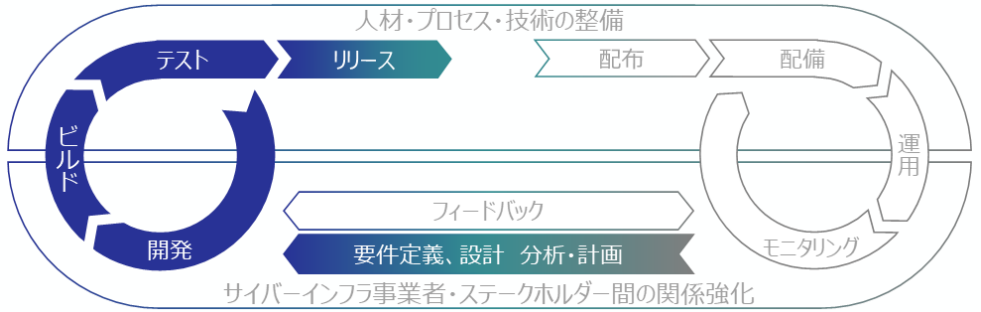
【サイバーインフラ事業者 要求事項１】セキュアな設計・開発・供給・運用①

設計時のリスク評価と対策の追跡

「セキュアバイデザイン」及び「セキュアバイデフォルト」の原則に則り、開発するソフトウェアのリスクを分析・評価し、リスク対応、セキュリティ要件、設計上の決定事項を追跡し、対策を維持する。

S(1)-1

- **開発者**
- 供給者
- 運用者
- 顧客



個別要求

- ☐ **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。
- ☐ **S(1)-1.2 設計レビュー**
  ソフトウェアの設計のレビューを通じて、全てのセキュリティ要件を満たし、識別されたリスク情報に十分に対応していることを確認し、レビュー結果を反映する。
- ☐ **S(1)-1.3 リスク対応の記録**
  設計上の決定事項、リスクへの対応、承認された例外措置に関する記録を保持し、ソフトウェアのライフサイクル全体を通じて監査や保守の目的で使用できるように維持する。
- ☐ **S(1)-1.4 リスクベースの定期的確認**
  セキュリティ要件に対して承認された全ての例外とソフトウェア設計、及びソフトウェアの設計時に作成したリスクベースの分析・評価結果をレビューし、リスクへの対処が適切か定期的に確認する。

【サイバーインフラ事業者 要求事項１】セキュアな設計・開発・供給・運用②

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、これに従いコードを生成・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。

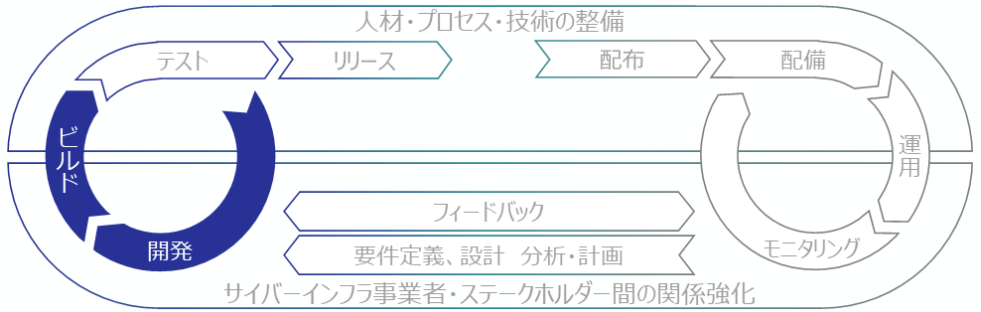
S(1)-2

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様々な形式のコード（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１】セキュアな設計・開発・供給・運用③

テスト

ビルドフェーズまでのレビュー及び分析で特定されなかった脆弱性を発見するために、機能テストに加え、脆弱性テスト、侵入テストを設計・実施し、発見された脆弱性への対策を実施する。

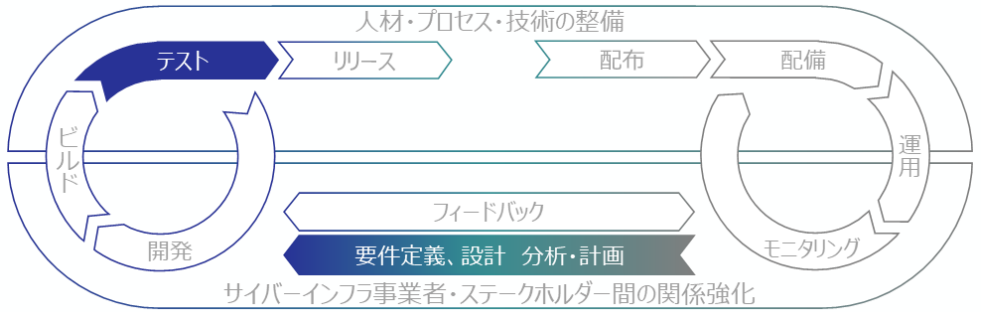
S(1)-3

開発者

供給者

運用者

顧客



個別要求

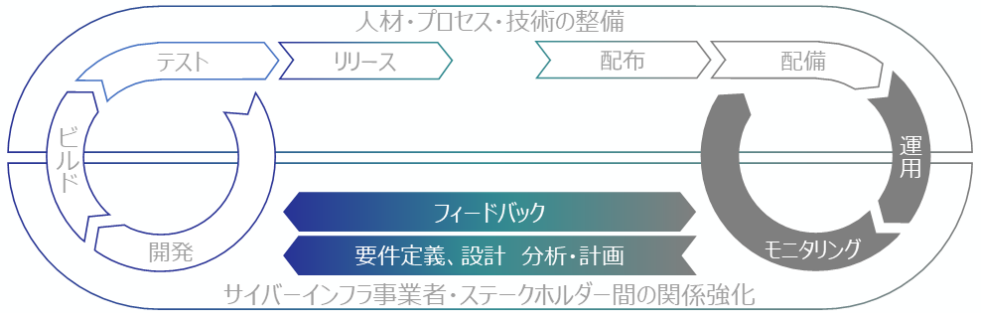
- ☐ **S(1)-3.1 テスト計画**
  脅威モデルとリスク分析に基づき、テスト範囲及びテスト方式を決定し、テスト計画を立案する。
- ☐ **S(1)-3.2 テスト方式**
  テスト方式には、機能テスト、脆弱性テスト、ファジング、侵入テストなどを含める。
- ☐ **S(1)-3.3 テスト実施**
  テスト計画に従ってテストを設計、実施し、結果を文書化する。
- ☐ **S(1)-3.4 問題への対応**
  テストの結果、発見された全ての問題と推奨される対応策を開発チームのワークフローに組み込み、対処する。

【サイバーインフラ事業者 要求事項１】セキュアな設計・開発・供給・運用④

サービスのモニタリング

ソフトウェアがその導入環境（ネットワーク、プラットフォーム、サービスなど）と整合性をもって情報資産を保護、維持することをモニタリングするプロセス及びシステムを整備し、実施する。

S(1)-4	
	開発者
	供給者
	運用者
	顧客



個別要求

- ☐ **S(1)-4.1 資産管理**
  運用者は、システム・サービスが扱う資産、及びシステム・サービスを構成する資産に関する資産管理手順と資産リストを整備する。
- ☐ **S(1)-4.2 モニタリング環境の整備**
  運用者は、リスク発生時の潜在的な影響を最小化するためにシステムを適切に分離し、ソフトウェアによる資産保護上重要なリスクを監視するモニタリング環境を整備する。
- ☐ **S(1)-4.3 セキュリティメカニズムの整備**
  ソフトウェア及びソフトウェアを適用するシステム・サービスが、動作環境又はデジタルインフラなどのリソース上にある情報資産及びデータの機密性・完全性を保護し、監視可能とするための適切なセキュリティメカニズムを整備する。
- ☐ **S(1)-4.4 モニタリングと評価**
  運用者は、重要なサービスを提供するソフトウェアに適用したメカニズムの動作状況をモニタリングするとともに、定期的にセキュリティ評価を実施し、組織のリスク管理の枠組みに統合する。

【サイバーインフラ事業者 要求事項２】ライフサイクル管理、透明性の確保①

セキュアなソフトウェアコンポーネントの手配

外部から手配した商用、オープンソース、その他のサードパーティのソフトウェアコンポーネントが、そのライフサイクルを通じて、組織が定義した要件に準拠していることを検証する。

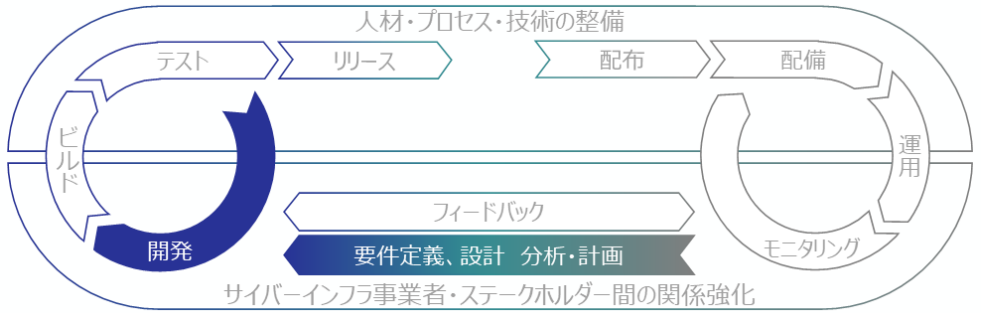
S(2)-1

開発者

供給者

運用者

顧客



個別要求

- ☐ **S(2)-1.1 ソフトウェアコンポーネントの手配**
  外部から手配する商用、オープンソース、その他のサードパーティのソフトウェアコンポーネントは、組織が定義した要件を満たす安全性の高いものを採用する。
- ☐ **S(2)-1.2 ソフトウェアコンポーネントの開発・維持**
  外部からソフトウェアコンポーネントを手配しない場合、組織で確立されたセキュリティ基準・慣行に従い、安全性の高いソフトウェアコンポーネントを社内で開発、維持する。
- ☐ **S(2)-1.3 ソフトウェアコンポーネントのリスク評価**
  各ソフトウェアコンポーネントの出所情報を取得・分析し、そのコンポーネントがもたらすリスクを評価する。
- ☐ **S(2)-1.4 ソフトウェアコンポーネントの公知脆弱性の確認**
  各ソフトウェアコンポーネントの公知脆弱性、サポート期間を定期的にチェックする。
- ☐ **S(2)-1.5 ソフトウェアコンポーネントの更新**
  各ソフトウェアコンポーネントを新しいバージョンにセキュアに更新するプロセスを導入する。

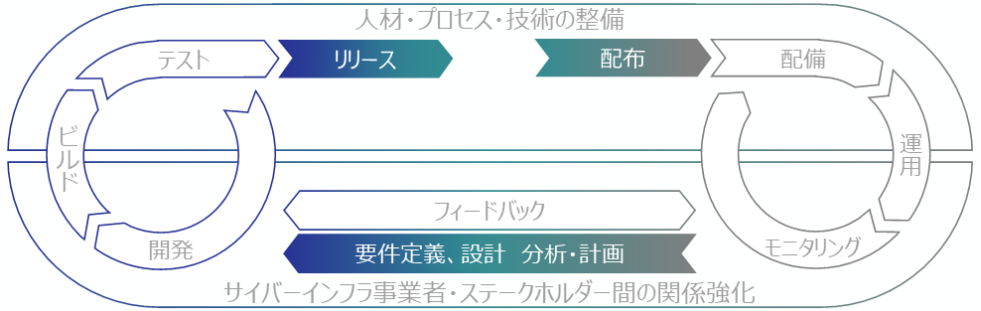
【サイバーインフラ事業者 要求事項２】ライフサイクル管理、透明性の確保②

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

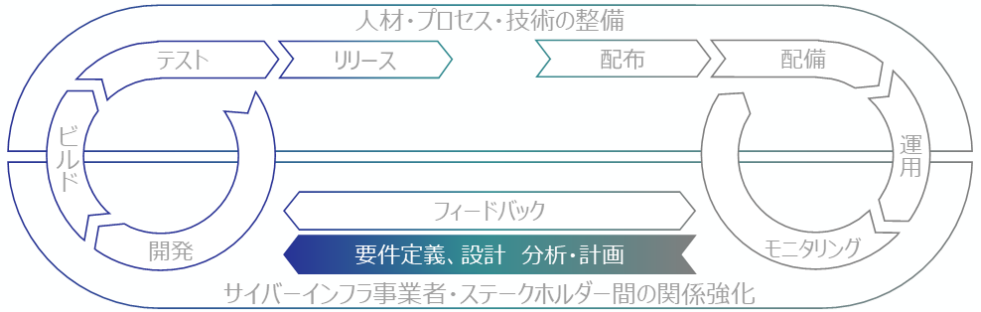
- ☐ **S(2)-2.1 コードベースの保護**
  全ての形式のコードベースを不正アクセスや改ざんから保護するために、リポジトリにコードや設定情報を保管し、承認された担当者、ツール、サービスなどのみがアクセスできるよう最小権限の原則に基づいたアクセス制御を実施する。
- ☐ **S(2)-2.2 リリースのアーカイブ**
  リリース後に発見された脆弱性を分析、特定できるようにするために、各ソフトウェアのリリースをアーカイブ化して保護する。
- ☐ **S(2)-2.3 リリースの出所データの共有**
  各ソフトウェアリリースの全てのコンポーネントの出所データを収集、保護、維持、共有す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

【サイバーインフラ事業者 要求事項２】ライフサイクル管理、透明性の確保③

関係者間のセキュリティ要件の確立

関係者間で合意すべきセキュリティ要件を確立し、契約又は共有するポリシーに盛り込む。

S(2)-3	
	開発者
	供給者
	運用者
	顧客



個別要求

- ☐ **S(2)-3.1 セキュリティ要件の合意**
  IT製品（自社のソフトウェアで再利用するための商用ソフトウェアコンポーネントを含む）又はサービスを提供するサードパーティとの契約又は共有するポリシーに、明示的なセキュリティ要件を盛り込む。
- ☐ **S(2)-3.2 サプライチェーンセキュリティ要求への対応**
  提供するIT製品又はサービスを受領・取得する組織が採用するサプライチェーンセキュリティ要件と同等のサプライチェーンセキュリティ要件に対応する。
- ☐ **S(2)-3.3 セキュリティ要件を満たさないリスクへの対処プロセスの整備**
  受領・取得するサードパーティ製のIT製品又はサービスが満たさないセキュリティ要件がある場合のリスクに対処するプロセスを整備する。

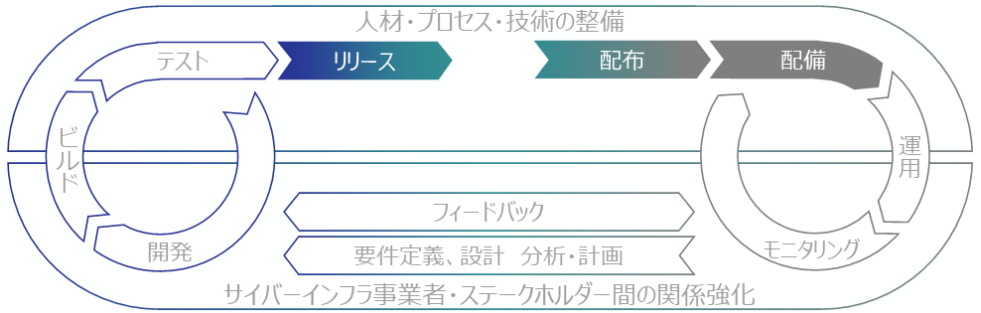
【サイバーインフラ事業者 要求事項２】ライフサイクル管理、透明性の確保④

利用者への適切な情報提供

ソフトウェアの導入・インストールから操作、利用終了までのライフサイクル全体でセキュアな利用を容易にするガイダンスをソフトウェア利用者が確実に利用できるようにする。

S(2)-4

- **開発者**
- **供給者**
- **運用者**
- **顧客**



個別要求

- ☐ **S(2)-4.1 セキュアな導入・設定・操作・変更・廃棄・終了**
  ソフトウェアをセキュアに導入・設定・操作するための情報、及び変更の影響・廃棄・提供終了・利用終了に係る情報をソフトウェア利用者が継続的に利用できるようにする。
- ☐ **S(2)-4.2 整合性検証情報の提供**
  ソフトウェアの整合性・完全性の検証に必要な情報をソフトウェア利用者が継続的に利用できるようにする。

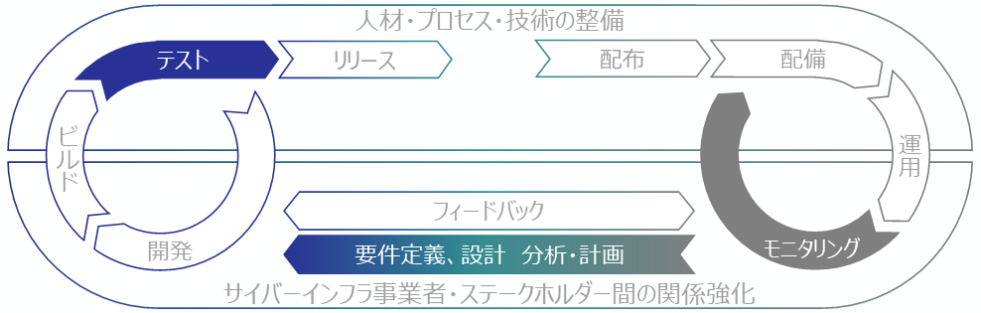
【サイバーインフラ事業者 要求事項３】残続する脆弱性の速やかな対処①

継続的な脆弱性調査

ソフトウェアの脆弱性の開示と是正に関する方針を定め、その方針に必要な役割、責務、プロセスを定義し、実施する。

S(3)-1

- **開発者**
- 供給者
- **運用者**
- 顧客



個別要求

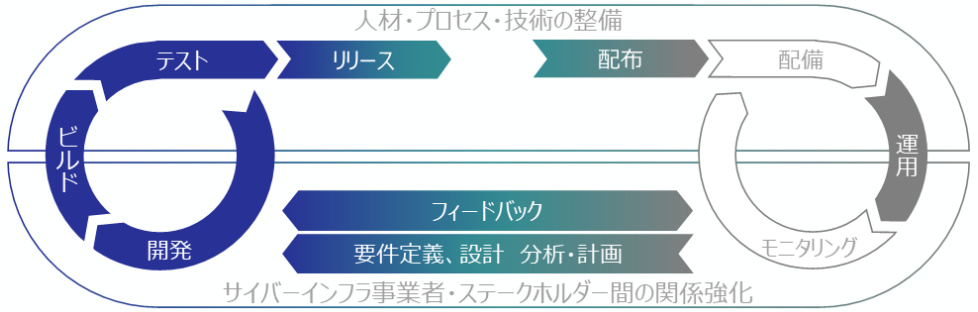
- ☐ **S(3)-1.1 脆弱性対応体制の設置**
  ソフトウェア製品の脆弱性の開示と修復に対処するポリシーを定め、そのポリシーをサポートするための脆弱性対応（インシデント対応を含む）に関する体制を設置し、必要な役割、責務、プロセスを定義する。
- ☐ **S(3)-1.2 コミュニケーション計画**
  全ての利害関係者に対するコミュニケーション計画を定める。
- ☐ **S(3)-1.3 脆弱性情報の収集**
  公知情報の探索、ソフトウェア利用者からの通知、外部脅威情報の取得、システム構成データのレビュー、その他の方法を通じて、新たな脆弱性情報を収集する。
- ☐ **S(3)-1.4 未検出の脆弱性の特定**
  継続的又は定期的に、ソフトウェアのコードのレビュー、分析、テストを実施し、今まで未検出の対処すべき脆弱性（不適切な設定などを含む）を特定する。

【サイバーインフラ事業者 要求事項３】残続する脆弱性の速やかな対処②

検知した脆弱性への対処

リリースしたソフトウェアに残存する脆弱性に対するリスク対応を定期的に計画し、実施する。

S(3)-2	開発者
	供給者
	運用者
	顧客



個別要求

- ☐ **S(3)-2.1 脆弱性の分析**
  開発者は、残存する各脆弱性の影響に伴うリスクを把握するために必要な情報を収集し、修復又はその他のリスク対応を計画するために、各脆弱性を分析する。
- ☐ **S(3)-2.2 脆弱性へのリスク対応**
  開発者は、各脆弱性に対するリスク対応を計画し、実装する。
- ☐ **S(3)-2.3 セキュリティ勧告**
  開発者は、セキュリティ勧告を作成し、リリースしたソフトウェアの供給先にその情報を提供するとともに、関連する制度の指定に従って報告する。また、運用者はセキュリティ勧告に従った配備を実施する。

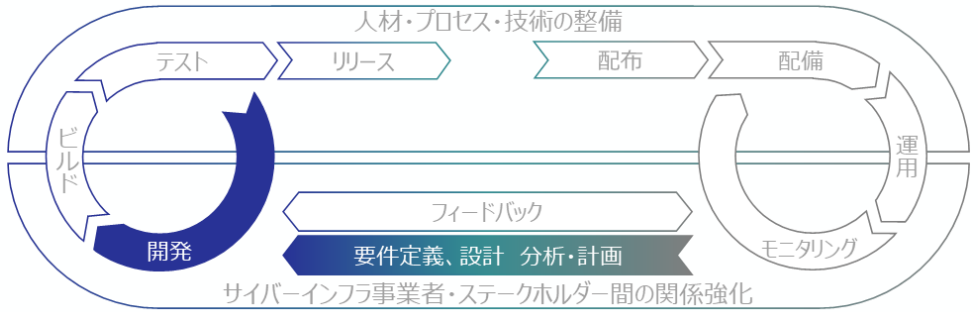
【サイバーインフラ事業者 要求事項３】残続する脆弱性の速やかな対処③

対処結果を組織のプロセス改善に活用

ソフトウェアに発見された問題の根本原因が再発しない、若しくはその可能性を低減するよう、脆弱性に基づき、開発と運用のプロセスを見直す。

S(3)-3

- **開発者**
- 供給者
- **運用者**
- 顧客



個別要求

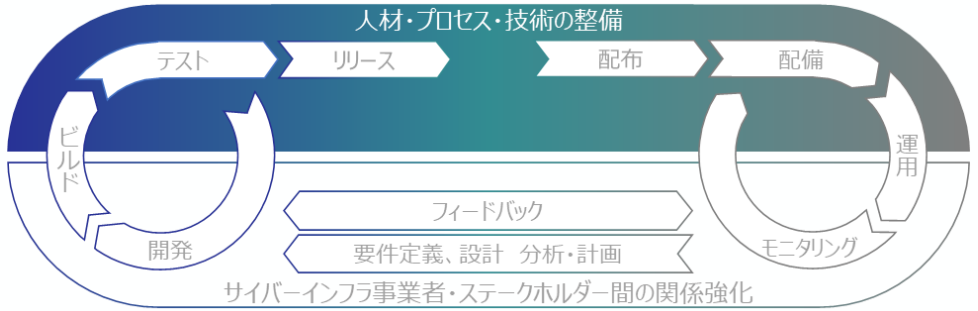
- ☐ **S(3)-3.1 根本原因の特定**
  根本原因を決定するために、識別された脆弱性を分析し、プロアクティブに対策する。
- ☐ **S(3)-3.2 プロセス改善**
  ソフトウェアの更新又は作成された新しいソフトウェアにより、根本原因の再発を防止又はその可能性を低減するために、ソフトウェアライフサイクル全体の開発と運用のプロセスをレビューし、必要に応じて見直す。

【サイバーインフラ事業者 要求事項４】人材・プロセス・技術の整備①

人材：経営層のコミットメントと人員の整備

ソフトウェアのライフサイクル全体を網羅した役割と責務を定義する。セキュア開発に対する経営層のコミットメントを周知し、セキュリティ対策のための人材を確保し、セキュアな開発・運用に関連する全要員に、要員の習熟度と役割に応じたトレーニングを提供し、定期的に見直す。

S(4)-1	開発者
	供給者
	運用者
	顧客



個別要求

- ☐ **S(4)-1.1 役割と責務の定義**
  ソフトウェア開発ライフサイクルを網羅する役割と責務を定義する。
- ☐ **S(4)-1.2 経営層のコミットメント**
  全要員に対してセキュア開発に対する経営層のコミットメントを周知し、組織にとってのセキュアな開発・運用の重要性を教育する。
- ☐ **S(4)-1.3 役割と責務の同意**
  各要員が、役割と責務を認識・同意していることを確認する。
- ☐ **S(4)-1.4 各役割のトレーニング**
  各役割のトレーニング計画を作成し、全要員が習熟度と役割に応じてトレーニングを実施できるように提供する。
- ☐ **S(4)-1.5 役割とトレーニングの見直し**
  役割やトレーニングは定期的に見直す。

【サイバーインフラ事業者 要求事項４】人材･プロセス･技術の整備②

プロセス：開発ポリシーの確立と法令順守

法令を遵守し、組織の開発インフラ及びプロセスに関するセキュリティポリシーを文書化・維持し、セキュリティ確保に必要な予算を確保する。

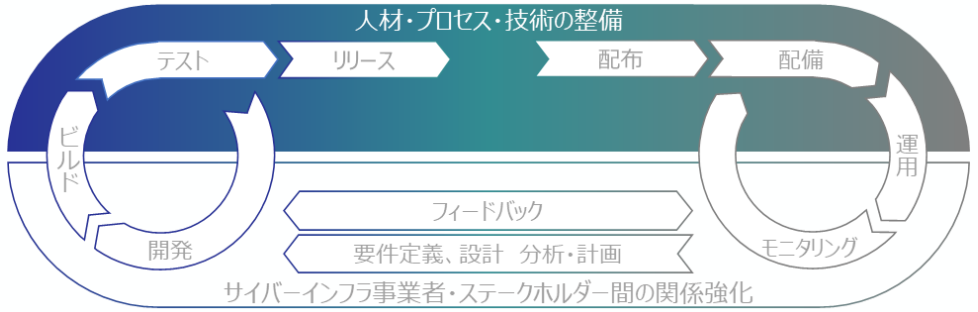
S(4)-2

開発者

供給者

運用者

顧客



個別要求

- ☐ **S(4)-2.1 ソフトウェア開発ポリシーの定義**
  ソフトウェア開発のインフラ及びプロセスの全てのセキュリティ要件を特定し、法令遵守の下SDLC全体を通じて維持するためのセキュリティポリシーを定義する。
- ☐ **S(4)-2.2 ソフトウェア･セキュリティポリシーの定義と維持**
  組織が開発するソフトウェアが満たすべき全てのセキュリティ要件を規定したポリシーを定義し、これらの要件をSDLC全体にわたって維持する。
- ☐ **S(4)-2.3 費用認識の共有と予算化**
  ポリシーに基づいてセキュリティを確保するために必要な予算を確保する。

【サイバーインフラ事業者 要求事項４】人材･プロセス･技術の整備③

プロセス：運用ポリシーの確立と法令遵守

法令を遵守し、ソフトウェアを適用したサービス運用インフラ及びプロセスに関する全てのセキュリティポリシーを文書化し、維持する。

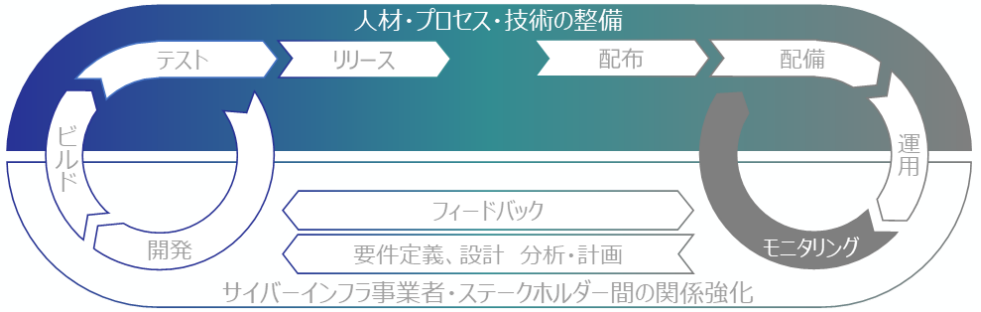
S(4)-3

開発者

供給者

運用者

顧客



個別要求

- ☐ **S(4)-3.1 ソフトウェアサービス運用ポリシーの定義**
  ソフトウェアを適用したサービス運用インフラ及びプロセスのすべてのセキュリティ要件を特定し、法令遵守の下SDLC全体を通じて維持するためのセキュリティポリシーを定義する。
- ☐ **S(4)-3.2 サービスのセキュリティポリシーの定義と維持**
  ソフトウェアを適用したサービスが満たすべきすべてのセキュリティ要件を規定したポリシーを定義し、これらの要件をSDLC全体にわたって維持する。
- ☐ **S(4)-3.3 運用ポリシーに基づく監査**
  ポリシーに基づくガバナンスにより、サービス運用インフラ及びプロセスの保護、及びサービスのセキュリティ要件がSDLC全体にわたって維持されていることを監査により確認する。

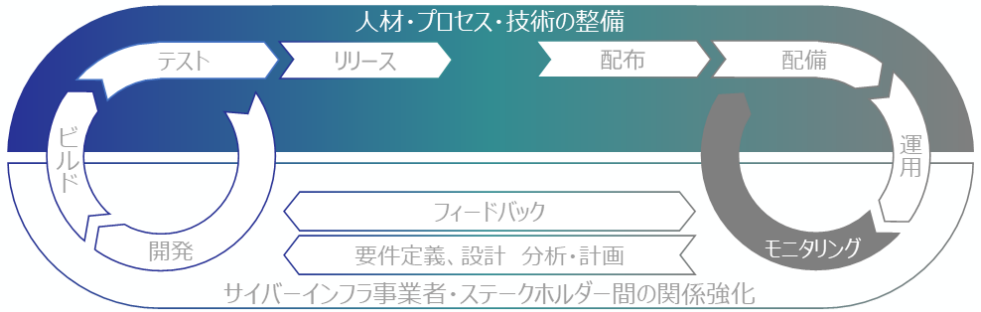
【サイバーインフラ事業者 要求事項４】人材･プロセス･技術の整備④

プロセス：開発･運用基準の策定

ソフトウェアの開発に関わるセキュリティ上の確認基準を定め、基準の裏付けに必要な情報を収集し、適合するためのプロセス、仕組みを実装する。ライフサイクル全体を通じて適合状況を追跡する。

S(4)-4

- **開発者**
- 供給者
- **運用者**
- 顧客



個別要求

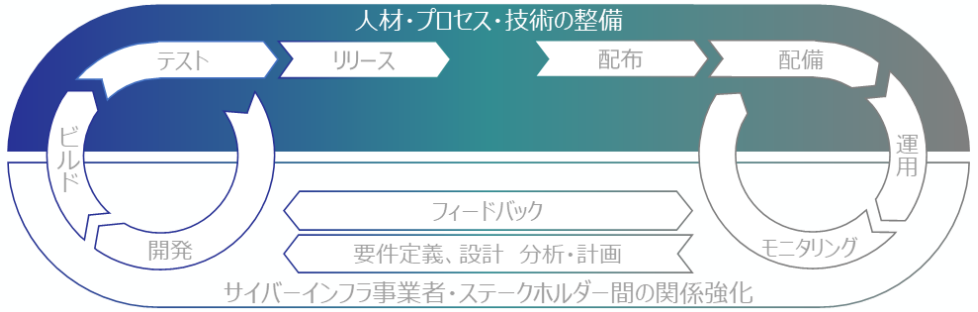
- ☐ **S(4)-4.1 セキュリティ確認基準の定義と追跡**
  ソフトウェアのセキュリティ確認基準を定義し、SDLC全体を追跡する。
- ☐ **S(4)-4.2 セキュリティ確認基準に基づく意思決定のサポート**
  セキュリティ確認基準に基づく意思決定をサポートするために必要な情報を収集し保護するためのプロセスや仕組みなどを実装する。
- ☐ **S(4)-4.3 セキュリティ確認基準に基づく監査**
  セキュリティ上の確認基準への適合を遵守するためのガバナンスにより、SDLC全体を追跡し意図する効果を得ていることを監査により確認する。

【サイバーインフラ事業者 要求事項４】人材･プロセス･技術の整備⑤

技術：セキュアな開発ツールの整備

ソフトウェアの開発ライフサイクル全体のリスクを分析し、開発ツールにセキュリティ対策を実施する。

S(4)-5	
	開発者
	供給者
	運用者
	顧客



個別要求

- ☐ **S(4)-5.1 ツールとツールチェーンの指定**
  特定されたリスクを軽減するために有効なツールを特定し、どのツールチェーンに含めることが必須若しくは必要であるか、及びツールチェーンのコンポーネントを相互に統合する方法を指定する。
- ☐ **S(4)-5.2 ツールとツールチェーンの配備･運用･保守**
  セキュリティ慣行に従ってツールとツールチェーンを配備、運用、及び保守する。
- ☐ **S(4)-5.3 ツール構成と証跡生成**
  組織によって定義されたセキュアなソフトウェア開発の慣行のサポートに関する証跡を生成するようにツールを構成する。

【サイバーインフラ事業者 要求事項４】人材･プロセス･技術の整備⑥

技術：セキュアな開発環境の整備

ソフトウェアの開発ライフサイクル全体のリスクを分析し、開発に関わる環境を保護強化する。

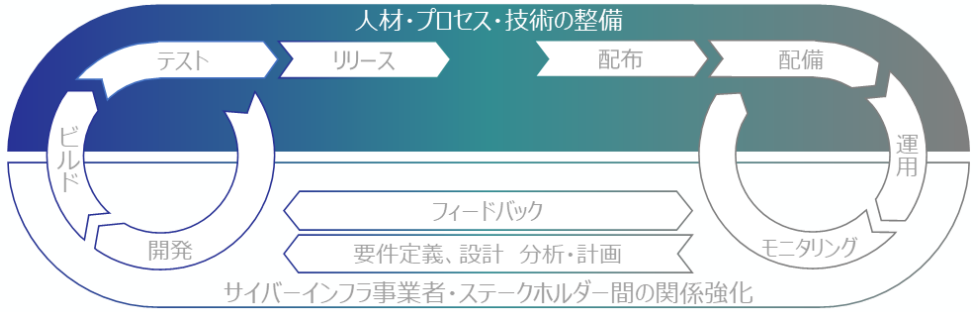
S(4)-6

開発者

供給者

運用者

顧客



個別要求

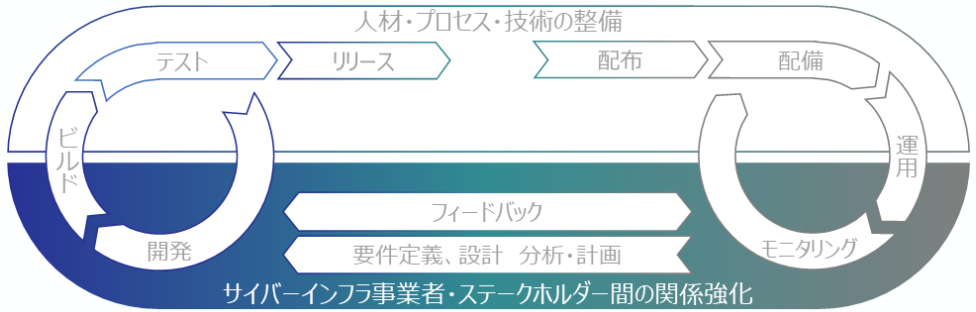
- ☐ **S(4)-6.1 環境の分離保護**
  ソフトウェア開発に関係する各環境を分離して保護する。
- ☐ **S(4)-6.2 開発用エンドポイントの保護**
  リスクベースのアプローチを使用して開発関連のタスクを実行するために、各開発者向けのエンドポイントを保護、強化する。

【サイバーインフラ事業者 要求事項５】ステークホルダーとの関係強化①

情報連携のための組織体制

ソフトウェアの製品及びサービスのセキュリティを改善するために、民間企業同士、関係当局、専門組織との情報連携のための組織体制を構築する。

S(5)-1	開発者
	供給者
	運用者
	顧客



個別要求

- ☐ **S(5)-1.1 情報連携のための組織体制の構築**
  ソフトウェアの製品及びサービスのセキュリティを改善するために、民間企業同士、関係当局、専門組織との情報連携のための組織体制を構築する。
- ☐ **S(5)-1.2 重要なセキュリティ関連情報の提供**
  業界固有の必須かつ重要なセキュリティ関連情報を選別・識別して、サプライチェーン先に提供する。
- ☐ **S(5)-1.3 脆弱性情報の通知サービスの利用**
  効率的に脆弱性情報の共有を図るため、脆弱性情報の通知サービスを利用する。

【サイバーインフラ事業者 要求事項５】ステークホルダーとの関係強化②

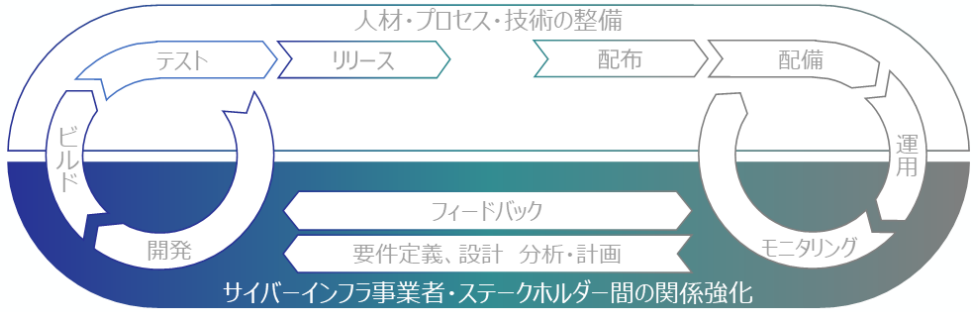
協力体制の強化

ソフトウェアの製品及びサービスのセキュリティを改善するために、民間企業同士、関係当局、専門組織との協力体制と枠組みを活用する。

S(5)-2

- 開発者
- 供給者
- 運用者

顧客



個別要求

- ☐ **S(5)-2.1 協力体制の活用**
  ソフトウェアの製品及びサービスのセキュリティを改善するために、外部の事業者、顧客、及び専門機関が参加するソフトウェアセキュリティの改善を目的とするコミュニティや協力体制を活用する。
- ☐ **S(5)-2.2 協力体制への貢献**
  コミュニティや協力体制に参加する場合には、積極的に活動に関与し、協力体制に対して貢献する。

【顧客 要求事項】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

顧客経営層のリーダーシップにより、顧客独自のリスク管理をサイバーインフラ事業者と協力して実施するリスク管理を統合する。

個別要求

- ☐ **S(6)-1.1 リスク管理**
  顧客の独立した主体的な取組とサイバーインフラ事業者との契約に基づく取組を統合したリスク管理を実施する。
- ☐ **S(6)-1.2 リソース整備**
  既知の脆弱性への対処、及び緩和策を主体的に実施するためのリソースを割り当て、整備する（SBOM活用を含む）。
- ☐ **S(6)-1.3 協力体制の活用**
  ソフトウェアセキュリティの改善を目的とするコミュニティや協力体制を活用する。

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

顧客経営層のリーダーシップにより、セキュアにソフトウェアを調達、運用する。

個別要求

- ☐ **S(6)-2.1 セキュリティ要件の定義**
  ソフトウェア設計計画にセキュリティ機能を組み込むためのセキュリティ要件を定義し、ソフトウェアを調達・導入する前に、サイバーインフラ事業者に提示する。
- ☐ **S(6)-2.2 セキュリティ慣行の要求開示**
  ソフトウェアの調達・導入前に、サイバーインフラ事業者に求めるセキュリティ慣行の要求を開示する。
- ☐ **S(6)-2.3 リスク評価に基づく意思決定**
  ソフトウェアを調達・導入する際に、リスク評価に基づいた意思決定を行う。
- ☐ **S(6)-2.4 予算確保**
  ソフトウェアのライフサイクルを考慮した運用、リスク対応、及び関連する契約に係る予算を継続的に確保する。