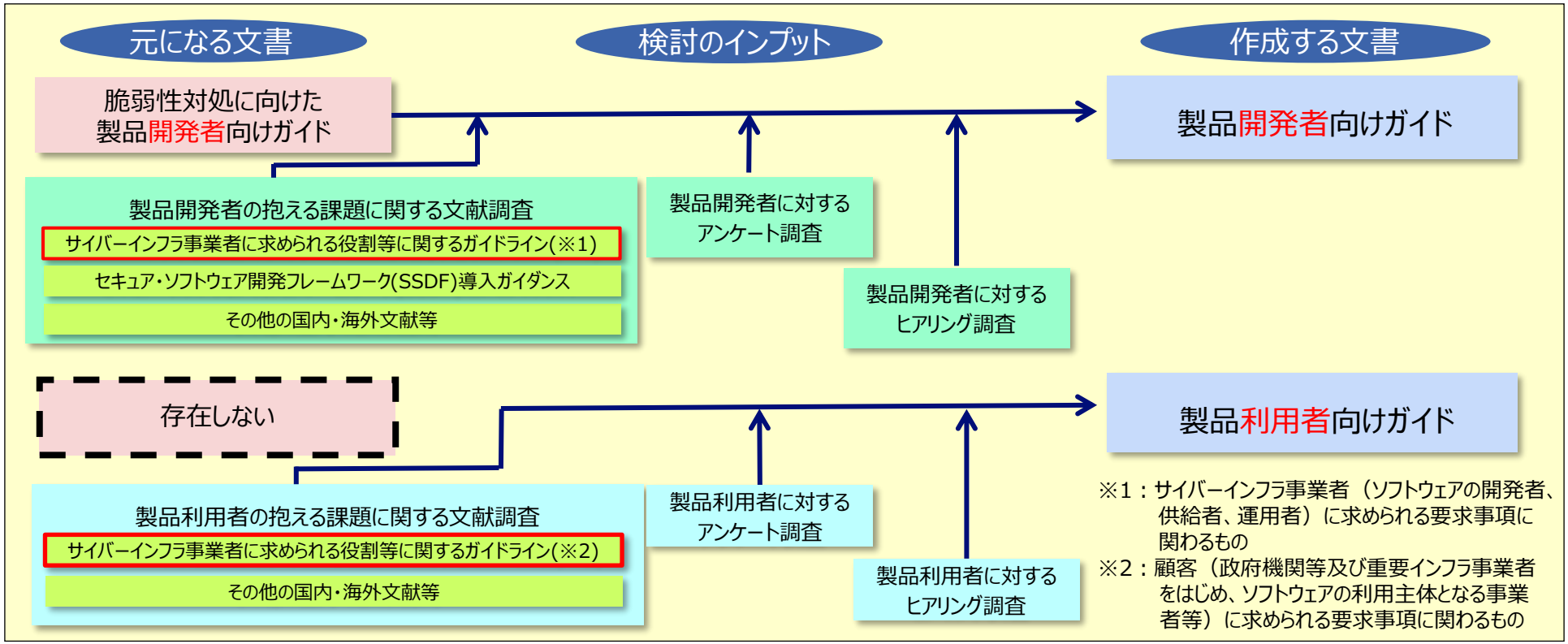
資料1-5

2025年度情報システム等の脆弱性情報の取扱いに関する研究会

今年度の脆弱性調査の方針

今年度の脆弱性調査の方針：調査の全体概要

- 製品開発者（PSIRT組織）における脆弱性対応、製品利用者（CSIRT組織）における脆弱性対応を支援するため、製品開発者、製品利用者のそれぞれに向けてガイドを作成する。
- ガイドの作成のため、① 文献調査、② アンケート調査、③ ヒアリング調査をそれぞれ実施する。
- ガイドについては、NCO（旧NISC）とMETIの「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」の規定事項を踏まえたものとする。



注：「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」と「セキュア・ソフトウェア開発フレームワーク(SSDF)導入ガイダンス」について、現在公表されているものは、いずれも「案」の段階である。（本年度中に成案化の予定）

2025年度情報システム等の脆弱性情報の取扱いに関する研究会

「製品開発者向けガイドの策定」の実施内容全体

文献調査 仮説検討

- 2019年度に脆弱性研究会で作成した「脆弱性対処に向けた製品開発者向けガイド」に関連して、国内外の文献調査を行う：
  - 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）
  - セキュア・ソフトウェア開発フレームワーク(SSDF)導入ガイダンス案（中間整理）
  - 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 ver 2.0
  - その他国内外の文献
- 製品開発者に対するアンケート調査を実施するにあたり、製品開発者が抱える課題について、仮説を立てる。

構成・規定 内容の検討

- 文献調査の結果を踏まえ、**ガイド骨子案**を作成する
- 検討した仮設に基づき、**アンケート調査票**案と**ヒアリング調査項目**案を作成

★ 第１回研究会での検討

ガイド案の検討

- 骨子案を踏まえ、ガイドの改訂案を作成

アンケート

- アンケート調査の実施
- アンケート結果の集計・分析

ヒアリング

- ヒアリング調査の実施

第2回研究会での検討

ヒアリング

- ヒアリング調査の実施（継続）

ガイド案の検討

- アンケート調査結果、ヒアリング結果を踏まえ、ガイドの改訂案を修正

第3回研究会での承認

製品開発者向けガイドの概要

ガイド作成の目的

製品開発者による開発時点での対策から製品利用者による利用（運用）時点での対策に至るまでのソフトウェア開発ライフサイクル全体における、適切な脆弱性対処を実現する。

考慮すべき事項

本ガイドを作成するにあたり、サイバーインフラ事業者が認識すべき責務や、SSDF導入の基本方針、導入プロセス、SBOMを活用した脆弱性管理プロセスについて考慮する。

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

＜サイバーインフラ事業者が認識すべき責務＞

(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・協力体制の強化

セキュア・ソフトウェア開発フレームワーク(SSDF)導入ガイダンス

＜SSDF導入の基本方針＞

(1) 目標の明確化
(2) アカウンタビリティベース・アプローチ
(3) 残留リスクの把握

＜SSDF導入プロセス＞

(1) 要求分析
(2) 現状把握
(3) タスク達成レベルの定義とギャップ分析
(4) タスクの実践
(5) 達成度評価
(6) 自己適合宣言

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 ver 2.0

＜SBOMを活用した脆弱性管理プロセス＞

(1) 脆弱性特定フェーズ
(2) 脆弱性対応優先付けフェーズ
(3) 情報共有フェーズ
(4) 脆弱性対応フェーズ

ガイド作成の元になる文書

本ガイドは、消費者向けIoT機器等のネットワークに接続する機器の製品開発者を対象として作成された、IPAの「脆弱性対処に向けた製品開発者向けガイド(以下「2020年ガイド」とする。)」（2020年8月）をもとにし、必要となる加除修正を施して作成する。

製品開発者向けガイド作成のための調査概要

ガイド作成のための文献調査の実施

「**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**」や「**セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス**」を含め、以下の国内外の文献を対象に文献調査を行う。同時に、アンケート調査の基礎となる**仮説も検討**する。

- CISA「サイバーセキュリティリスクのバランスを変える：セキュアバイデザイン、セキュアバイデフォルトの原則とアプローチ」
- NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1
- セキュア・ソフトウェア開発フレームワーク(SSDF)導入ガイダンス案（中間整理）
- 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 ver 2.0
- 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）
- FIRST PSIRT Services Framework Version 1.1
- ASD ACSC Choosing secure and verifiable technologies
- CISA Software Acquisition Guide for Government Enterprise Consumers
- CISA Information Technology (IT) Sector-Specific Goals (SSGs)
- BSA | The Software Alliance The BSA Framework for Secure Software：A NEW APPROACH TO SECURING THE SOFTWARE LIFECYCLE
- NSA ESF Securing the Software Supply Chain：RECOMMENDED PRACTICES GUIDE FOR DEVELOPERS

アンケート調査の実施

製品開発者が抱える課題（PSIRT構築や脆弱性の作りこみ防止、開示対応等）についてアンケート調査を実施する

- 製品開発者 50 社以上（個人開発者を除く）

ヒアリング調査の実施

課題・実情を深堀りするため、ヒアリング調査を実施する

- PSIRT をもつ製品開発者　5 社
- PSIRT をもたない製品開発者　5 社

2025年度情報システム等の脆弱性情報の取扱いに関する研究会

「製品利用者向けガイドの策定」の実施内容全体

文献調査 仮説検討

- 国内外の文献調査を行う：
  - 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）
  - その他国内外の文献
- 製品開発者に対するアンケート調査を実施するにあたり、製品開発者が抱える課題について、仮説を立てる。

構成・規定内容の検討

- 文献調査の結果を踏まえ、**ガイド骨子案**を作成する
- 検討した仮設に基づき、**アンケート調査票**案と**ヒアリング調査項目**案を作成

★ 第１回研究会での検討

ガイド案の検討

- 骨子案を踏まえ、ガイドの改訂案を作成

アンケート

- アンケート調査の実施
- アンケート結果の集計・分析

ヒアリング

- ヒアリング調査の実施

第2回研究会での検討

ヒアリング

- ヒアリング調査の実施（継続）

ガイド案の検討

- アンケート調査結果、ヒアリング結果を踏まえ、ガイドの改訂案を修正

第3回研究会での承認

製品利用者向けガイドの概要

ガイド作成の目的

製品利用者における方針・組織体制に加え、脆弱性対処の観点から調達先に要求すべき事項や、システム・サービスの計画・要件定義から、システム・サービスの運用中のセキュリティパッチの適用等、各フェーズにおける適切な脆弱性対処を実現する。

考慮すべき事項

本ガイドを作成するにあたり、顧客が認識すべき責務について考慮する。

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

＜顧客が認識すべき責務＞

(1) 顧客経営層のリーダーシップによるリスク管理

- リスク管理
- リソース整備
- 協力体制の活用

(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

- セキュリティ要件の定義
- セキュリティ慣行の要求開示
- リスク評価に基づく意思決定
- 予算確保

ガイド作成の元になる文書

本ガイドは、元になる文書は存在しない。IPAの2020年ガイドのうち、「IV. 一般消費者に向けて実施すべきこと」の内容を考慮しつつ作成する。

2025年度情報システム等の脆弱性情報の取扱いに関する研究会

製品利用者向けガイド作成のための調査概要

ガイド作成のための文献調査の実施

「**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**」を含め、以下の国内外の文献を対象に文献調査を行う。同時に、アンケート調査の基礎となる**仮説も検討**する。

- 日本セキュリティオペレーション事業者協議会「脆弱性トリアージガイドライン作成の手引き」
- 日本セキュリティオペレーション事業者協議会「ASM導入検討を進めるためのガイダンス（基礎編）」
- 日本セキュリティオペレーション事業者協議会「セキュリティ対応組織（SOC/CSIRT）の教科書 ～X.1060 フレームワークの活用～ 第3.2版」
- 日本シーサート協議会「脆弱性管理の手引書 システム管理者編 1.1版」
- 「CISO支援ワーキンググループ」の各種成果物
- NIST SP 80040 Rev.4 Guide to Enterprise Patch Management Planning Preventive Maintenance for Technology
- NIST SP 1800 31 Improving Enterprise Patching for General IT Systems Utilizing Existing Tools and Performing Processes in Better Ways
- NSA ESF Securing the Software Supply Chain : RECOMMENDED PRACTICES GUIDE FOR CUSTOMERS

アンケート調査の実施

製品利用者が抱える課題（CSIRT体制や製品開発者・SI事業者との契約、パッチ適用等）についてアンケート調査を実施する

- 製品利用者 200 社以上

ヒアリング調査の実施

課題・実情を深堀りするため、ヒアリング調査を実施する

- CSIRT をもつ製品利用者　3 社
- CSIRT をもたない製品利用者　3 社
- その他（重要インフラ事業者、SI事業者、ウェブサイト運営者、クラウドサービス事業者等）　14 社

2025年度情報システム等の脆弱性情報の取扱いに関する研究会

製品開発者向けガイドおよび製品利用者向けガイドの検討スケジュール案

- 第2回会合では、ガイド案の初案に対する意見を聴取し、第3回会合では、第2回会合で頂いた意見を反映したガイド案の最終案について承認をいただく予定。ガイド案のインプットとなるアンケート調査、ヒアリング調査を含む検討スケジュールは以下のとおり。