2022 年度調査報告書

戦略的イノベーション創造プログラム（ＳＩＰ）第２期／ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティ／ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティに係るＯＳＳの管理手法及びＣＳＩＲＴ・ＰＳＩＲＴ連携等に関する調査

2022 年 12 月

国立研究開発法人新エネルギー・産業技術総合開発機構

委託先　　一般社団法人重要生活機器連携セキュリティ協議会

目次

1. 研究開発の成果と達成状況

1.1. 要約

1.1.1. 和文要約

本調査では、まずソフトウェアや OSS の管理手法に関する調査として、サプライチェーンや OSS を含むソフトウェアのセキュリティに関わる、組織マネジメントや開発プロセスなど対象にしたセキュリティ対策に関する 5 文献の調査を行った。ソフトウェア及び OSS の管理手法としては、各文献から抽出したセキュリティプラクティスを統合、集約し、セキュリティ対策のチェックシートとして整理を行った。セキュリティ対策のチェックシートは、サプライチェーンを想定し、対象を「ユーザ企業」と、「製品提供企業及び上流企業」に分類し、求められる管理対策については「必須」、「高度」の２つのレベルで定義を行った。また、チェックシートの作成にあたり、「IoT 社会に対応したサイバー・フィジカル・セキュリティに係る OSS の技術検証のあり方などに関する調査」において実施した IoT 製品の製品提供企業へのヒアリング結果を反映し、国内企業の現状を踏まえた項目の追記やレベルの調整を行っている。

さらに、ソフトウェアコンポーネントの管理については具体的な対応策として、SBOM（Software Bill of Materials） に関する 11 の文献から、標準フォーマットや利用方法に関する最新動向の調査を実施した。SBOM については、米国電気通信情報局（以下、NTIA）が複数の文献や情報を公開しており、大統領令 14028 を受けて、必要な最小要素を定義している。また国内における活用事例として、トヨタ自動車における SBOM の活用事例を紹介している。

次に、ソフトウェアや OSS に関わる CSIRT 及び PSIRT の連携方法や品質情報の管理方法について、調査を行った。まずは、国内で公開されている CSIRT、PSIRT のガイドラインを対象に 4 文献を調査し、それぞれに求められる体制や活動の整理を行った。CSIRT、PSIRT において連携、関係すべきステークホルダと、実施すべき活動（提供サービス）を一覧として提示している。

さらに、国内の IoT 製品提供企業を対象に CSIRT 及び PSIRT の体制や活動、連携の状況について、アンケート及びヒアリング調査を実施した。その結果、CSIRT については、かなり成熟した体制や活動が行われていることが明確になったが、一方で PSIRT の活動や CSIRT 及び企業間での連携については、多くの課題があることが明らかになった。

まず PSIRT 活動においては以下の課題が明らかになった。

- ステークホルダのエコシステムマネジメント：PSIRT の活動評価や定期的な報告、情報共有における課題。
- 脆弱性の発見：ソフトウェアコンポーネントリストの管理として全社統一の形式による管理や SBOM の導入、セキュリティテストの仕組み整備における課題。
- 脆弱性のトリアージと分析：脆弱性の再現テストの環境や方法、トリアージ方法の確立に関する課題。
- 脆弱性の改善及び対策：事後の追跡に利用可能な脆弱性データの管理に関する課題。
- 脆弱性の開示：製品の脆弱性情報の公開において、計画的な対応を行う上での課題。
- トレーニングや教育：PSIRT 関連部門への目的や役割分担に関する教育、脆弱性の分析やトラッキングなど技術面の教育に関する課題。

また、CSIRT・PSIRT 連携やその他として、以下の課題が明らかになった。

- CSIRT から共有されたインシデント情報を、PSIRT で活用する上での課題。
- CSIRT、PSIRT 運用に必要な人材の確保に関する課題。
- CSIRT のインシデント監視システムの導入、維持、運用コストの課題。
- 発見された脆弱性の対応において、製品に含まれるソフトウェアコンポーネントの対策や置換に関する課題。

最後にこれまでの調査結果を踏まえ、国内企業における CSIRT、PSIRT 活動のあり方について、ベースラインスキーム及び、ベースラインの要求事項を提言として整理した。以下にベースライン要求事項の概要を示す。

PSIRT と CSIRT 及び外部連携のベースライン要求

- 企業内の情報共有：CSIRT から PSIRT へのインシデント情報の共有。PSIRT による社内関係ステークホルダへの情報共有。
- 製品に関連する情報の報告、共有（川上企業から製品提供企業）：上流企業から製品提供企業への提供ソフトウェアに関する脆弱性や攻撃手法の情報共有。情報共有に関する契約の締結。
- 製品に関連する情報の報告、共有（製品提供企業から下流企業）：製品提供企業から下流企業への製品に影響が想定される脆弱性の情報の共有、今後の対応計画の報告。
- 外部機関への脆弱性報告：外部への脆弱性報告方針の定義。外部コーディネーション機関への報告の徹底。

OSS 管理及び PSIRT 活動のベースライン要求

- 対応方針・プロセスの立案・文書化：方針の定義や体制整備、関係部門の役割や責任の文書化。
- 脆弱性の影響分析のトリアージ：開発、品質保証部門による脆弱性情報の分析、トリアージの実施や、情報管理。経営層や責任者による最終的な意思決定。
- ソフトウェアコンポーネントリストの管理：国際標準に基づくソフトウェアコンポ―ネントリストの管理。自動化やサプライチェーン連携を踏まえた運用計画の立案と推進。
- 脆弱性の対策、改善：製品提供企業と上流企業、下流企業の間でアップデートプログラムの提供や保守サポートに関する責任や対応範囲を明確化。契約条項への記載。
- 脆弱性の情報、対策の記録管理：報告、発見された脆弱性情報のデータ管理と、事後活用の仕組み整備。

また、個別企業での対応が困難であると想定される課題については、国や行政による支援が必要であると考え、別途提言の内容を整理した。以下に概要を示す。

- PSIRT 活動のガイドライン発行、トレーニング・教育プログラムの策定。
- コンポーネント分析ツールの開発及びオープンソース化。

1.1.2. 英文要約

In this study, we first surveyed five guidelines and standards on security measures targeting organizational management and development processes related to security of supply chain and software including open source software (OSS), as a survey of software and OSS management practices. For software and OSS management practices, we integrated and consolidated security practices extracted from each guideline and standard, and organized them as a checklist of security measures. Targets of this checklist are classified into “user companies” and “product providers and upstream companies” to cover entities in a supply chain. The required control measures are classified into two levels: “mandatory” and “advanced.” In addition, we added some items to the checklist and we adjusted levels based on the current status of domestic companies, in consideration of the results of interviews with companies that provide IoT products conducted as part of the "Survey on the Technical Verification of OSS for Cyber Physical Security in the IoT Society."

Furthermore, we investigated 11 documents related to Software Bill of Materials (SBOM) for the latest trends in its standardized formats and usage, as a specific measure for software component management. The National Telecommunications and Information Administration (NTIA) has published several documents and information on the SBOM, which defines the minimum elements required in response to Executive Order 14028. As a case study of the use of SBOM in Japan, the report introduces the use of SBOM by Toyota Motor Corporation.

Next, we surveyed how CSIRTs and PSIRTs work together and how they manage quality information regarding software and OSS. First, we surveyed four CSIRT and PSIRT guidelines published in Japan, and organized the systems and activities required for each, listing stakeholders with whom CSIRTs and PSIRTs should cooperate and relate, and the activities (services to provide) that should be implemented.

Then, we conducted a questionnaire and interview survey with domestic IoT product-providing companies on the status of CSIRT and PSIRT systems, activities, and collaboration. As a result, we have found that CSIRTs have fairly mature systems and activities, but on the other hand, there are many issues regarding PSIRT activities and cooperation with its CSIRT and across companies.

As a result, the following issues were identified in PSIRT activities.

- Stakeholder ecosystem management: Issues in evaluation of PSIRT activities, regular reporting, and information sharing
- Vulnerability detection: Issues in management of software component inventory in a company-wide unified format, introduction of SBOM, and implementation of security testing
- Vulnerability triage and analysis: Issues related to the environment and methods of vulnerability reproduction testing and the establishment of triage methods
- Vulnerability mitigation and remediation: Issues related to the management of vulnerability data that can be used after incidents
- Vulnerability disclosure: Issues related to the systematic handling of product vulnerability disclosures

- Training and education: Issues related to educating PSIRT-related departments on the purpose and their roles, and technical education such as vulnerability analysis and tracking

The following issues also were identified as CSIRT/PSIRT collaboration and others.

- Issues in the PSIRT utilizing incident information shared by the CSIRT
- Issues in securing human resources for CSIRT and PSIRT operation
- Issues related to the cost of implementing, maintaining, and operating the CSIRT's incident monitoring system
- Issues related to countermeasures and replacement of software components included in products in response to discovered vulnerabilities

Finally, based on the results of the preceding survey, we have organized the baseline scheme and the baseline requirements as recommendations on how CSIRTs and PSIRTs in domestic companies should act. The following is a summary of the baseline requirements.

Baseline requirements for how the PSIRT should collaborate with its CSIRT and external entities:

- Information sharing within a company: Sharing of incident information from the CSIRT to the PSIRT, and information sharing by the PSIRT to relevant internal stakeholders
- Reporting and sharing of product-related information from upstream companies to product providers: Information sharing of vulnerabilities and attack methods related to provided software from upstream companies to product providers, and concluding information sharing agreements
- Reporting and sharing of product-related information from product providers to downstream companies: Sharing of information on vulnerabilities that may affect products from product providers to downstream companies, and reporting of future response plans
- Vulnerability reporting to external organizations: Defining external vulnerability reporting policy, and thorough reporting to external coordination bodies

Baseline requirements for OSS management and PSIRT activities:

- Development and documentation of response policies and processes: Definition of policies and systems, and documentation of roles and responsibilities of relevant departments
- Triage of vulnerability impact analysis: Analysis of vulnerability information by development and quality assurance departments, triage implementation, information management, and final decision making by management or responsible parties
- Software component inventory management: Management of software component inventory based on international standards, and planning and promotion of operational plans based on automation and supply chain coordination

- Vulnerability mitigation and remediation: Clarification of responsibilities and scope of actions regarding provision of updates and maintenance support between product providers, upstream companies, and downstream companies, and including in contract clauses
- Vulnerability information, record management of countermeasures: Data management of reported and discovered vulnerability information, and establishment of a system to utilize the information after incidents.

For issues that are assumed to be difficult for individual companies to address, we believe that support by the government and public administration is necessary. We have organized the contents of our recommendations. A summary is given below.

- Publication of guidelines for PSIRT activities and formulation of training and education programs
- Development of component analysis tools and their open-sourcing

1.2. 本文

本報告書に記載した会社名、製品名などは、一般に各社の登録商標または商標となる。

＜調査項目１＞組込み機器やソフトウェア・サービスでの OSS の管理手法の調査

1-1　調査の背景・目的・前提

CCDS が、2021 年度～2022 年度に OSS の技術検証のあり方などに関して調査・作成した NEDO 成果報告書[1]の調査項目２でセキュリティプラクティスが整理されているが、主に製品提供企業が自社のソフトウェア製品の技術検証を実施するという観点で整理されている。本調査ではこの調査結果を元に、さらにサプライチェーンという観点から、ソフトウェアを使用するユーザの視点を追加した。

1-2　OSS の管理方法、セキュリティ確保のための方策調査

サプライチェーンや OSS を含むソフトウェアのセキュリティに関わる、組織マネジメントや開発プロセスなど対象にしたセキュリティ対策に関する文献を調査した。さらに、ソフトウェアコンポーネントの管理に関わる実践として、SBOM（Software Bill of Materials）[2]に関する文献の調査を行った。

1-2-1　調査対象の文献一覧

表 1 に調査対象としたセキュリティ対策に関するガイドラインの一覧を、表 2 に調査対象とした SBOM に関する文献の一覧をそれぞれ掲載する。

表 1　調査対象の文献一覧

対象文書	発行機関	発行年月	文書の概要
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）	経済産業省	2019 年 4 月	サプライチェーン全体のサイバーセキュリティ確保を目的として、産業に求められるセキュリティ対策の全体像をフレームワークとして整理している。
NIST Special Publication 800-218 Secure Software Development Framework （SSDF） Version 1.1	米国商務省、米国国立標準技術研究所（以下 NIST）	2022 年 2 月	ソフトウェア開発プロセスに関して、これまでの一般的なソフトウェア開発ライフサイクル（SDLC）モデルではあまり扱われてこなかったセキュリティの観点をまとめた、セキュアソフトウェア開発フレームワーク（SSDF）。

[1] 「戦略的イノベーション創造プログラム（ＳＩＰ）第２期／ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティ/ＩｏＴ社会に対応したサイバー・フィジカル・セキュリティに係るＯＳＳの技術検証のあり方などに関する調査」、NEDO、2021 年度～2022 年度、報告書管理番号：20220000000436

[2] ソフトウェア部品表。あるソフトウェアに関してライセンスや含まれるコンポーネント、依存関係などをまとめたもの。

対象文書	発行機関	発行年月	文書の概要
Recommended Criteria for Cybersecurity Labeling of Consumer Software	NIST	2022 年 2 月	米国大統領令 14028[3]に基づく、コンシューマ向けソフトウェアのラベリングのためのセキュリティ基準。NIST SP 800-218 （SSDF）と整合を取る形でソフトウェアのセキュリティ対策が記載されている。
Guidelines for Securing the Internet of Things	欧州 ネットワーク情報セキュリティ庁（以下 ENISA）	2020 年 11 月	IoT 製品のサプライチェーンを保護するためのガイドライン。要件定義、設計から運用、保守、廃棄に至るまでの製品ライフサイクルにわたるセキュリティ対策が記載されている。
ISO/IEC 5230 （OpenChain）	ISO/IEC	2020 年 12 月	OSS のコンプライアンス、ライセンスを中心に管理基準を定義している。Linux Foundation 傘下の OpenChain プロジェクトによって取りまとめられ国際標準化された。

表 2　SBOM に関する文献一覧

対象文書	発行機関	発行年月	文書の概要
SBOM at a Glance	米国電気通信情報局（以下 NTIA）[4]	2021 年 4 月	SBOM の実践、サポート文献、およびソフトウェアサプライチェーンに必要な透明性を提供する上で SBOM が果たす重要な役割を紹介している。JPCERT/CC による日本語訳も掲載されている。
Framing Software Component Transparency: Establishing a Common Software Bill of Materials （SBOM） – Second Edition		2021 年 10 月	SBOM の概念と関連用語の定義、ソフトウェアコンポーネントを表す方法のベースラインの提供、及び SBOM の作成に関するプロセスの説明などが記載されている。
SBOM FAQ		2020 年 11 月	SBOM に関する詳細な情報、利点、およびよく寄せられる質問がまとめられている。
SBOM Myths vs. Facts		2021 年 11 月	SBOM に関してよくある都市伝説や誤解を理解し、払拭できるようにすることを意図して作られたもの。
The Minimum Elements For a Software Bill of Materials （SBOM）		2021 年 7 月	大統領令 14028 を受けて NTIA が米国商務省と共同で公表した、SBOM に必要な最小要素。

[3] 2021 年 5 月に発令された米国国家のサイバーセキュリティ向上に関するもの。ソフトウェアサプライチェーンのセキュリティ向上が要求されている。
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[4] National Telecommunications and Information Administration。電気通信政策などに関する米国大統領の諮問機関。

Enhancing the Security of the Software Supply Chain through Secure Software Development Practices	米国行政予算管理局（以下 OMB）	2022 年 9 月	大統領令 14028 を受けて OMB が公表した、政府機関が調達するソフトウェアに関する通達。SBOM の提供についても言及されている。
OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集	経済産業省	2022 年 5 月	OSS の管理手法などに関して参考になる取組を実施している企業に対して、ヒアリングなどによる調査を実施して事例集としてまとめたもの。
第 3 回 サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法など検討タスクフォース		2019 年 12 月	資料 3 に、トヨタ自動車から OpenChain プロジェクトの取り組みが解説されている。
Vulnerability Exploitability eXchange (VEX) – Use Cases	米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（以下 CISA）	2022 年 4 月	SBOM に関連して、あるソフトウェアコンポーネントに脆弱性が報告された場合に、製品に対するその脆弱性の影響を電子的に伝えるためのフォーマットである VEX（Vulnerability Exploitability eXchange）について書かれている。
Vulnerability Exploitability eXchange (VEX) - Status Justifications		2022 年 6 月	VEX において、ある脆弱性の影響を受けないと判断する場合、その判断の根拠についての説明が書かれている。
PCI[5] Secure Software Standard Version 1.2	PCI SSC	2022 年 12 月	クレジットカード決済などクレジットカードに関わるデータを扱うソフトウェアのセキュリティ認証規格。バージョン 1.2 にて SBOM 管理に関する要件が追加されている。

1-2-2　OSS の管理手法、セキュリティ確保のための施策

調査対象としたセキュリティ対策に関する各ガイドライン（表 1）から、サプライチェーンや OSS を含むソフトウェアの管理方法及びセキュリティ確保に関連するプラクティスを抽出した。以下では、ガイドラインごとに記載されているプラクティスを引用・紹介する。さらにこれらのプラクティスを集約しチェックリストの形にまとめたものを 1-2-4 項に掲載している。

１）　経済産業省： サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

[CPS.BE] ビジネス環境

自組織のミッション、目標、利害関係者、活動を理解し、優先順位付けを行う。この情報はサイバーセキュリティ上の役割、責任、リスク管理上の意思決定を伝達するために使用される。

[CPS.BE-1] サプライチェーンにおいて、自組織が担う役割を特定し共有する。

[5] Payment Card Industry の略。国際クレジットカードブランド会社によって設立された協議会：PCI SSC (Payment Card Industry Security Standards Council)が策定しているセキュリティ規格群の総称。

[CPS.BE-2] あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者（サプライヤ、第三者プロバイダなどを含む）に共有する。

[CPS.RM] リスク管理戦略

自組織の優先順位、制約、リスク許容度、想定を定め、運用リスクの判断に利用する。

[CPS.RM-2] リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。

[CPS.SC] サプライチェーンリスク管理

企業などの優先順位、制約、リスク許容値及び想定が、サプライチェーンリスク管理に関連するリスクの決定を支援するために確立され、利用される。企業などは、サプライチェーンのリスクを特定、評価、管理するプロセスを確立し、実施する。

[CPS.SC-1] 取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。

[CPS.SC-2] 自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。

[CPS.SC-3] 外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。

[CPS.SC-4] 外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。

[CPS.SC-5] 取引先などの関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。

[CPS.SC-6] 取引先などの関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。

[CPS.SC-7] 取引先などの関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。

[CPS.SC-9] 自組織が、関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。

[CPS.SC-10] 取引先などの関係する他組織との契約が終了する際（例：契約期間の満了、サポートの終了）に実施すべきプロシージャを策定し、運用する。

[CPS.SC-11] サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャなどを継続的に改善する。

２）　NIST： Special Publication 800-218（SSDF）

[PO.1] ソフトウェア開発におけるセキュリティ要件を定義する

ソフトウェア開発におけるセキュリティ要件を常に分かるようにしておく。これは、SDLC 全体を通してセキュリティ要件を考慮に入れられるようにするためである。また、要件情報は一度収集して共有できるため、労力の重複を最小限に抑えられるようにするためでもある。これには、社内ソース（組織のポリシー、ビジネス目標、リスク管理戦略など）と、外部ソース（適用される法律や規制など）からの要件が含まれる。

[PO.1.1] ソフトウェア開発環境、プロセスに関するセキュリティ要件をドキュメント化し、それらを維持する。

[PO.1.2] ソフトウェア製品のセキュリティ要件をドキュメント化し、それを維持する。

[PO.1.3] サードパーティにもセキュリティ対応を要求。ソフトウェアとその依存関係の出所データを提供するように要求する。

[PO.2] 役割及び責任を割り当てて実行する

SDLC に関与する組織の内外の全員が、SDLC 全体で SDLC 関連の役割と責任を果たす準備ができていることを確認する。

[PO.2.1] 必要に応じて新しい役割を作成したり、既存の役割に変更を加えたりして、SDLC のすべてを網羅する。定義された役割と責任を定期的に見直し、維持し、必要に応じて更新する。

[PO.2.2] セキュアな開発に貢献する責任を持つすべての担当者に役割に応じたトレーニングを提供する。定期的に習熟度、及び役割に応じたトレーニングをレビューし、必要に応じてトレーニングを更新する。

[PO.2.3] セキュアな開発に関する上層部や公式のコミットメントを取り付け、開発関連の役割と責任を持つすべての人にそのコミットメントを伝える。

[PO.3] サポート用ツールチェーンを実装する

自動化を使用して、人間の労力を削減し、SDLC 全体を通してセキュリティプラクティスの精度、再現性、操作性、および網羅性を向上させるとともに、これらのプラクティスの使用を文書化し、実証する方法を提供する。ツールチェーンとツールは、組織全体であったり、プロジェクト固有のレベルであったり、組織のさまざまなレベルで使用される。ビルドパイプラインなど SDLC の特定の部分に対処するものであることもある。

[PO.3.1] ツールチェーンに含めるべきツール、およびそれらの統合の仕方を指定する。

[PO.3.2] ツール及びツールチェーンをセキュリティ規則に従って展開する。

[PO.3.3] ツールがエビデンスを生成するように設定する。

[PO.4] ソフトウェアセキュリティチェックのための基準を定義し使用する

開発中にソフトウェアのセキュリティを確認するための基準を定義し、使用することにより、SDLC から生み出されるソフトウェアが組織の期待に適合していることを確認する。

[PO.4.1] セキュリティチェックの基準を定義する。

[PO.4.2] 基準をサポートするのに必要な情報を収集するようにプロセス、メカニズムを実装する。

[PO.5] ソフトウェア開発のためのセキュアな環境を実装し保守する

ソフトウェア開発用の環境のすべてのコンポーネントが、内部および外部の脅威から強力に保護され、環境やそこで開発中/保守中のソフトウェアに対するセキュリティ侵害を防ぐようにする。ソフトウェア開発の環境の例としては、開発、ビルド、テスト、および配布といった環境がある。

[PO.5.1] ソフトウェア開発に関係する環境を分離して保護する。

[PO.5.2] リスクベースアプローチを用いて、開発関連タスクを実行するための開発エンドポイントを堅牢化する。

[PS.1] すべての形式のコードを不正アクセスおよび改ざんから保護する

ソフトウェアの意図したセキュリティ特性を回避または無効化する可能性のある、不注意および意図的なコードに対する不正な変更を防止できるようにする。一般にアクセス可能なコードではない場合は、これによってソフトウェアの盗難を防ぎ、攻撃者がソフトウェアの脆弱性を見つけるのをより難しくするか時間がかかるものとできる可能性がある。

[PS.1.1] コードを保護するため、許可された担当者などのみに必要最小限のアクセス権を付与する。

[PS.2] リリースしたソフトウェアの整合性を検証するメカニズムを提供する

ソフトウェアの取得者が、取得したソフトウェアが正当であり、改ざんされていないことを確認できるようにする。

[PS.2.1] ソフトウェアの購入者が完全性チェック情報を利用できるようにする。

[PS.3] リリースしたソフトウェアをそれぞれアーカイブし保護する

リリースしたソフトウェアを保持し、リリース後にソフトウェアで発見された脆弱性を特定、分析、排除する。

[PS.3.1] ソフトウェアリリースごとに、ファイルや完全性検証情報などを安全にアーカイブする。

[PS.3.2] ソフトウェアリリースごとの、すべてのコンポーネントや依存関係の出所データを収集、維持、共有する。（例：SBOM）

[PW.1] セキュリティ要件を満たすようにソフトウェアを設計し、セキュリティリスクを軽減する

ソフトウェアのセキュリティ要件を特定し、評価する。運用中にソフトウェアが直面する可能性のあるセキュリティリスクと、それらのリスクを軽減するためにソフトウェアの設計やアーキテクチャがどうあるべきかを判断する。また、リスクベースの分析によってセキュリティ要件を緩和または放棄する必要性があるケースについて正当化を行う。ソフトウェア設計時のセキュリティ要件とリスクへの対処（セキュリティ・バイ・デザイン）は、ソフトウェアのセキュリティを向上させる鍵であり、開発の効率を向上させるのにも役立つ。

[PW.1.1] ソフトウェアのリスク評価のため、脅威モデルや攻撃モデル、アタックサーフェスマッピングなどのリスクモデルを使う。

[PW.1.2] ソフトウェアのセキュリティ要件やリスク、設計上の決定を文書化する。

[PW.2] ソフトウェア設計をレビューして、セキュリティ要件およびリスク情報に対応していることを確認する

確実にソフトウェアがセキュリティ要件を満たし、さらに特定されたリスク情報に適切に対処できるよう支援する。

[PW.2.1] 設計に関わっていない有資格者、もしくはツールチェーンに組み込まれた自動化プロセスにソフトウェア設計をレビューしてもらい、すべてのセキュリティ要件を満たし、特定されたリスク情報に適切に対処するようにする。

[PW.4] 既存の適切なソフトウェアが利用可能な場合は、同じ機能を作りこむのではなく、それを再利用する

セキュリティに取り組む姿勢が既にチェックされているソフトウェアモジュールやサービスを再利用することで、ソフトウェア開発のコストを削減し、ソフトウェア開発を迅速化し、ソフトウェアにセキュリティ脆弱性を無駄に追加してしまう可能性を減らす。これは、暗号化モジュールやプロトコルなどのセキュリティ機能を実装するソフトウェアにとって特に重要である。

[PW.4.1] 商用、OSS、サードパーティデベロッパから十分にセキュアなソフトウェアコンポーネントを入手する。

[PW.4.2] サードパーティのソフトウェアコンポーネントでは対応できない一般的な内部ソフトウェア開発のニーズに対応するために、SDLC プロセスに準拠しつつセキュアなソフトウェアコンポーネントを内作する。

[PW.4.4] 取得した商用、オープンソース、およびその他すべてのサードパーティソフトウェアコンポーネントが、組織が定義する要件に準拠していることを確認する。

[PW.5] セキュアコーディングプラクティスに従ってソースコードを作成する

組織で定義した脆弱性の重大度基準に達する脆弱性をソースコードの作成中に作りこむのを最小限に抑えることで、ソフトウェアに存在するセキュリティの脆弱性の数を減らし、コストを削減する。

[PW.5.1] 開発言語や環境に応じたセキュアコーディングを実施する。

[PW.6] 実行可能なセキュリティを向上させるためのコンパイル、インタプリタ、およびビルド プロセスを構成する

テストを実施する前に脆弱性を排除しておくことで、ソフトウェアのセキュリティの脆弱性の数を減らし、コストを削減する。

[PW.6.1] 実行ファイルのセキュリティを向上させる機能を持ったコンパイラを用いる。

[PW.6.2] 使用するコンパイラの機能、および、どのように設定するかを決定し、承認された設定を使用する。

[PW.7] 脆弱性を特定し、セキュリティ要件に準拠していることをチェックするため、人が判読できるコードを確認または分析する

脆弱性を特定し、悪用されないようソフトウェアをリリースする前に修正する。自動化された方法を使用すると、脆弱性の検出に必要な労力とリソースが削減される。人間が読み取り可能なコードには、ソースコード、スクリプト、および組織が可読であると判断したその他のコード形式が含まれる。

[PW.7.1] 組織の決まりに従い、コードレビュー（人が直接コードを確認し問題を見つける）、あるいはコード解析（ツールがコードを解析し問題を見つける。完全に自動化されるか、もしくは人手を介す場合もある）のどちらを使うかを決定する。

[PW.7.2] コードレビューやコード分析を実行し、開発チームのワークフローまたは問題追跡システムにおいて、発見されたすべての問題と推奨される修正を文書化しトリアージする。

[PW.8] 脆弱性を特定し、セキュリティ要件に準拠していることを確認するため、実行コードをテストする

脆弱性を特定し、悪用されないようソフトウェアをリリースする前に修正する。自動化された方法を使用すると、脆弱性の検出に必要な労力とリソースが削減され、トレーサビリティと再現性も向上する。実行可能コードには、バイナリ、直接実行されるバイトコードとソースコード、および組織が実行可能であると判断したその他のコード形式が含まれる。

[PW.8.1] ここまでのレビュー、分析、またはテストでカバーされていない脆弱性のクラスを特定して排除するために実行コードのテストを実施する必要があるかどうか、実施する場合はどのタイプを使用するかを決定する。

[PW.8.2] テストを設計し、テストを実行し、結果を文書化する。これには、開発チームのワークフローまたは問題追跡システム内にすべての問題と推奨される修正を文書化しトリアージすることを含む。

[PW.9] 既定でセキュリティ保護された設定を持つようにソフトウェアを構成する

インストール時のソフトウェアのセキュリティを強化し、セキュリティが侵害される危険性が高くなるような脆弱なセキュリティ設定でソフトウェアが展開される可能性を低くする。

[PW.9.1] デフォルト設定がセキュアであり、セキュリティ機能を弱めることがないよう、各セキュリティ設定を決定し、セキュアなベースラインを定義する。

[PW.9.2] デフォルト設定（または該当する場合はデフォルト設定のグループ）を実装し、ソフトウェア管理者向けに各設定を文書化する。

[RV.1] 継続的に脆弱性を特定し、確認する

脆弱性をより迅速に特定し、リスクに応じてより迅速に修正できるようにし、攻撃者の機会を減らす。

[RV.1.1] 購入者、エンドユーザ、および公開ソースから、ソフトウェアおよびソフトウェアが使用するサードパーティコンポーネントの潜在的な脆弱性に関する情報を収集し、すべての信頼できるレポートを調査する。

[RV.1.2] ソフトウェアのコードを確認、分析、および/またはテストして、以前は検出されなかった脆弱性の存在を特定または確認する。

[RV.1.3] 脆弱性の開示と修正に対処するポリシーを用意し、そのポリシーをサポートするために必要な役割、責任、およびプロセスを実装する。

[RV.2] 脆弱性の評価し、優先順位付けを行い、修復する

リスクに応じて脆弱性を修正し、攻撃者の機会を減少させる。

[RV.2.1] 各脆弱性を分析して、修正を計画するための十分な情報を収集する。

[RV.2.2] 各脆弱性の修正計画を作成して実装する。

[RV.3] 脆弱性を分析して根本原因を特定する

将来の脆弱性の頻度を減らす。

[RV.3.1] 特定されたすべての脆弱性を分析して、各脆弱性の根本原因を特定する。

[RV.3.2] 長期間にわたって根本的な原因を分析して、例えばコーディングルールが守られていないなどのパターンを特定する。

[RV.3.3] 同様の脆弱性について横展開し、事前に修正する。

[RV.3.4] SDLC プロセスを確認し、必要に応じて更新して、ソフトウェアのアップデートまたは新規ソフトウェアにおける根本原因の再発を防止する。

３） NIST： Recommended Criteria for Cybersecurity Labeling of Consumer Software

[2.2.2.2] 安全な設計と脆弱性の修復を実践する

脆弱性の発生と影響を最小限に抑えるためにソフトウェア開発で使用されるベストプラクティスが数多くある。これらの多くは、NIST SSDF に取り入れられている。ここで、推奨される最小限のプラクティスとタスクは次に紹介する。

- ソフトウェアのセキュリティ要件、リスク、そして設計においてなされた決定を追跡および維持する（SSDF PW.1.2 参照）。
- 人間が判読できるコードを確認、分析して脆弱性を特定し、セキュリティ要件への準拠を確認する（SSDF PW.7 参照）。
- 実行コードをテストして脆弱性を特定し、セキュリティ要件への準拠を確認する（SSDF PW.8 参照）。
- 脆弱性に対するリスク対応を計画および実装する（SSDF RV.2.2 参照）。
- 取得した商用、オープンソース、およびその他すべてのサードパーティソフトウェアコンポーネントが、定義したセキュリティ要件を満たしていることをチェックする（SSDF PW 4.4 参照）。

[2.2.2.3] 責任ある脆弱性の開示を実践する

消費者は、自身にとって重大なリスクとなる脆弱性について知らされるべきである。脆弱性情報の扱い

には内部でホストする、あるいはNVD[6]のような適切な脆弱性リポジトリに報告するといった方法があるが、いずれにせよ、その情報にアクセスしたい消費者に対して脆弱性情報へのアクセス方法を詳細に説明するべきである。

- 脆弱性の開示と修正に対処するポリシーを用意し、そのポリシーをサポートするために必要な役割、責任、およびプロセスを実装する。（SSDF RV.1.3 参照）

[2.2.2.4] ソフトウェアの整合性と出自を提供する

- 安全性の高い Web サイトで、リリースファイルの暗号ハッシュを提示する。
- 消費者の OS やその他のツールやサービスが、ソフトウェアを使用する前に署名の有効性を確認できるように、コード署名には確立された認証局を使用する。
- 証明書の更新、ローテーション、失効、保護といったコード署名プロセスを定期的に確認する。

[2.2.2.7] 強力な暗号化を使用

ソフトウェアがセキュリティ目的で使用するすべての暗号アルゴリズムは、少なくとも NIST 暗号標準とガイドラインに準拠すること。その他の暗号化アルゴリズムを認める場合、スキームの所有者が定義すること。

４） ENISA： Guidelines for Securing the Internet of Things

[ACT-01] セキュリティ保証を提供するサプライヤとの協力を優先する

外部のサプライヤと協業する場合、セキュリティ対策の管理が行き届かないことによる脅威があるが、これは通常避けられないものである。この脅威は、ISO 27036 などの標準や NISTIR 8259.10 などのベストプラクティスを実装した企業を採用することで最小限に抑えることができる。認証はコストのかかるプロセスであり、認証を取得するような企業はサプライチェーンのセキュリティの向上に真剣に取り組んでいることを示していると言える。標準準拠とまで行かなくても、包括的なセキュリティ対策が実施されており、それらについて透過的（監査の権利、契約上のセキュリティ要件など）である組織も信頼できると見なせるだろう。

[ACT-02] 透明性の向上に向けて取り組む

サプライチェーンのセキュリティを管理するには、透明性が不可欠である。供給する製品の運用や正常な動作に関して明確で詳細な情報を提供し、すべての関連情報をチェーンの次のステップに伝達するというように、利害関係者、特にサプライヤは透明性を持つ必要がある。

[ACT-03] 革新的な信頼モデルを開発する

利害関係者間の信頼は、IoT サプライチェーンを保護するために考慮すべき最も重要な課題の 1 つである。信頼モデルは、さまざまな関係者のふるまいに関する正式な保証を提供し、セキュリティを強化するためのフレームワークを定義するものである。革新的な信頼モデルを開発するか、既存のモデルを固

[6] National Vulnerability Database。NIST が管理する脆弱性データベース。

有のニーズに適応させることにより、サプライチェーンに大きな利益をもたらすだろう。ただし、信頼するための万能のアプローチはないことに注意する必要がある。

[ACT-04] 継続的なプロセスとしてサプライチェーンにおけるセキュリティの見通しを採用する

ペネトレーションテストなどの活動によってもたらされる保証は、時間の経過とともに価値が低下する。このため、セキュリティは、サプライチェーンのすべての段階において継続的かつ反復的なプロセスとして含める必要がある。

[ACT-07] ユーザの IoT セキュリティ意識を促進する

セキュリティの構成に関する知識がなく、セキュリティが弱いことによる影響を十分に認識していないユーザの割合はかなり高い。製品提供企業としてはセキュリティの負担をユーザの責任に残すべきではないが、ユーザに対して適切なセキュリティの重要性についての認識を高めるためのキャンペーンや活動を行うことが有益な場合がある。製品提供企業は、製品を安全でセキュアに使用する方法を説明する包括的なユーザーガイドまたはマニュアルを提供する必要がある。

[ACT-08] 顧客に対してセキュリティの保証を提供する

顧客に対して、セキュリティに関連する包括的な情報を明確かつ明示的に提供する必要がある。製品のライフサイクル中に発見された脆弱性や、フィールド上のデバイスに展開されるソフトウェアアップデート関係などが含まれる。これらの情報をサプライチェーンの下流に転送することが重要である。

[PRO-01] セキュリティ・バイ・デザインを採用する

セキュリティモジュールは、優先度の高いコンポーネントと見なされ、サプライチェーン全体の最初の段階から設計プロセスに組み込まれる必要がある。IoT サプライチェーンの適切な段階において、セキュリティに焦点を当てた安全なコーディング手法とテスト（ペネトレーションテスト、脆弱性スキャンなど）を実施する必要がある。設計段階では、人的要因も考慮に入れ、ユーザの意思決定が不十分なためにセキュリティが損なわれるのを防ぐために、ベストプラクティスを実施し、厳密に従う必要がある。さらに、セキュリティの専門家にレビューしてもらうことができるよう、彼らに概念設計の段階から直接関与してもらう必要がある。

[PRO-04] IoT サプライチェーンの脅威モデルを開発する

脅威モデルは、サイバーフィジカルシステムに固有な、物理的安全性とデジタルセキュリティの両方の概念を統合する必要がある。後で重要な資産とブロックを特定するため、サプライチェーンを機能ブロックに分割し、それらのブロック内の資産をリストアップするということを開発プロセスで実施する。費用対効果の高い保護とセキュリティコントロールを定義するため、サイバー攻撃の動機（たとえば、金銭的利益、テロリズム）も考慮する必要がある。

[PRO-05] サードパーティソフトウェアを特定する

サードパーティソフトウェアを使用することによって、サプライチェーンのセキュリティに対する脅威となるある程度の不確実性がもたらされる。これらのソフトウェアコンポーネントは、それを選択する際に従うべき基準を含め、サプライチェーンのセキュリティセキュリティプロセスの一部として文書化されなければならない。
ソフトウェアの識別プロセスを支援するために、組織は、SBOM を生成するためのツールである OWASP Dependency-Track などのコンポーネント分析に特化したソフトウェアツールが使用できる。スキャン製品を利用して、ソフトウェアコンポーネントと脆弱性を特定することもできる。ソースコードスキャニングツールは自作や OSS コンポーネントに使用でき、バイナリスキャニングツールはソースコードが公開されていない場合に使用できる。脆弱性情報を見つけた場合、それが OSS コミュニティにフィードバックされるようになると業界として大きな利益となる。

[PRO-06] 包括的なテスト計画を確立する
すべての IoT ソリューションには、製品がソフトウェアとハードウェアの両方で期待される機能を発揮していることを確認するための包括的なテスト計画を含める必要がある。受け入れテストは、サプライチェーンの前段階で実施された可能性のあるテストとは独立して行う必要がある。

[PRO-08] 一定期間のセキュリティパッチの提供を確約する
メンテナンスされていないソフトウェアで動くレガシーな IoT デバイスは、サプライチェーンの完全性に対する脅威である。IoT 製品の設計と計画において、拡張サポートとセキュリティパッチのタイムリーな配信を考慮に入れる必要があり、例えば将来の更新をサポートするためのリソース（メモリなど）の適切な設計などである。製品提供企業は、少なくとも保証期間が終了するまで、できればサポートが終了するまで、セキュリティパッチを提供する義務を負うべきである。

[PRO-11] 包括的なドキュメントを作成する
ヒューマンエラーを防止するための包括的なドキュメントを用意する。構成管理と障害後の復旧の観点は特に重要である。もしこれらのドキュメントがなければサプライチェーンにとって脅威となりうるが、あったとしても標準レベルに達しないものであるならそれはそれで有害である可能性が高い。

[PRO-13] IoT デバイス用のソフトウェア部品表（SBOMS）を提供する
SBOM は、オープンソースと商用の両方のパッケージやライブラリを含む、特定の製品の構成要素として使用されるソフトウェアコンポーネントを網羅的に記述したものである。これらのリストにより、製品の可視性が高まり、製品提供企業と外部ユーザの両方が既知の脆弱性をチェックし、セキュリティの観点からデバイスを検証できるようになり、攻撃者が悪意のある目的で脆弱性を利用できるという脆弱性ギャップを減らすことができる。

[TEC-01] デバイスのアップグレード可能性と廃止の計画と管理を確立および改善する

デバイスの品質と機能を最新化して改善する必要性があるため、IoT ソリューションは、デバイスとソフトウェアが何世代も共存するというものになる。IoT 製品は様々なコンポーネントからなり、一言に更新といっても単純ではなく、更新を計画し管理することが非常に重要である。

[TEC-04] ソフトウェアの完全性対策の存在を要求するサービスレベル契約の採用を支持する

セキュアブートとファームウェア署名は、改ざんに対するある程度の保護を提供するセキュリティ対策である。ファームウェア署名では、あるファームウェアイメージのハッシュがソフトウェアの正規の提供者のみが使用できる秘密鍵で署名される。そして、デバイスが公開鍵を使用してファームウェアイメージの整合性を検証する。セキュアブートとは、不変の信頼ルートから始まるデバイスのブートプロセスに参加するソフトウェアコンポーネントのチェーン全体を暗号的に検証することを指す。これらの 2 つの手段は、サードパーティとの既存のサービスレベル契約に統合することができる。

[TEC-07] リモート更新のメカニズムを実装する

サプライチェーンのセキュリティプロセスでは、フィールドのデバイスにリモートかつ自動化された方法で更新を適用する機能が重要である。IoT デバイスのライフサイクルは離散的ではなく、フィールドに出た後でさらに開発が行われる可能性がある。また、サプライチェーンシステムに影響を与える脆弱性が後日、または実際の攻撃によって発見される可能性もある。環境の変化に迅速に対応し、リモートデバイスの更新を展開する機能を、設計の初期段階から検討する必要がある。さらに、これらのメカニズムは、ミスやマルウェアの注入を防がなければならない。

５） ISO/IEC 5230（OpenChain）[7]

[3.1] プログラムにおける基本事項

- 提供ソフトウェアのオープンソースライセンスの遵守を管理する書面によるオープンソースポリシーが存在すること。本方針は、社内に周知すること。
- プログラムの関係者の役割と責任を特定し、必要な能力を定義し、適切な教育を実施し、プログラムの参加者が適格であることを保証すること。
- OSS ポリシーや関係者の役割、プログラム要件に従わなかった場合の影響などを周知すること。
- 各ライセンスによって付与される義務、制限および権利を決定するため、識別されたライセンスをレビューするプロセスが存在すること。

[3.2] 関連タスクの定義とサポート

- 外部からのオープンソースに関する問い合わせに効果的に対応するプロセスを維持すること。第三者がオープンソースのコンプライアンスに関する問い合わせ行う手段を公開すること。
- プログラムを実行するための責任、および、十分な時間と予算が割り当てられていること。ポリシーをレビュー、更新し、プログラムの実行をサポートするためのプロセスが存在すること。

---

[7] The OpenChain Project. “OpenChain Specification Version 2.1”. https://github.com/OpenChain-Project/License-Compliance-Specification/blob/master/Official/en/2.1/openchainspec-2.1.pdf から著者が抜粋・日本語訳

OSS のライセンス準拠に関して、必要に応じて法的な専門家に相談でき、OSS のコンプライアンス問題を解決するプロセスが存在すること。

[3.3] OSS コンテンツのレビュー及び承認

- 提供するソフトウェアを構成する各 OSS コンポーネント（およびその識別されたライセンス）を含む SBOM を作成および管理するためのプロセスが存在すること。
- プログラムにおいて、提供するソフトウェアについてプログラム参加者が経験する一般的な OSS ライセンスのユースケースを管理できること。例えば、バイナリ形式で配布するケース、ソース形式で配布するケース、他の OSS と組み合わせで追加のライセンス義務が課されるケース、など。

[3.4] コンプライアンス成果物[8]の作成と配布

- 提供するソフトウェアについての一連のコンプライアンス成果物を作成するプロセスが存在すること。

[3.5] OSS コミュニティへの貢献

- 組織が OSS プロジェクトへの貢献を考慮する場合、OSS プロジェクトへの貢献を管理する文書化されたポリシーが存在し、そのポリシーが内部的に伝達され、ポリシーを実施するためのプロセスが存在すること。

1-2-3　SBOM への対応について

1-2-2 に抜粋した各ガイドラインのセキュリティプラクティスにおいても SBOM の必要性が多く挙げられている。また、米国大統領令 14028 の中で NTIA に対して SBOM の最小要素を規定することが指示され、NTIA はこれを公開している。

今回、調査対象とした SBOM に関する文献（表 2）から、NTIA が SBOM に関して取りまとめた情報や大統領令への対応を紹介するとともに、国内での SBOM 利用の事例としてトヨタ自動車株式会社の取り組み例を紹介する。また、業界団体のソフトウェアのセキュリティ規格で SBOM 管理を要求する例がでてきており、これも参考情報として紹介する。

1）　NTIA の取り組み

NTIA では 2018 年からソフトウェアコンポーネントの透明性について取り組んでおり、特に SBOM に関して啓発活動を行っている。この活動の成果物として、SBOM を理解するための情報が NTIA のウェブサイト（https://www.ntia.gov/SBOM）上にまとめられている。また、NTIA は大統領令 14028 で指

[8] ISO/IEC 5230（OpenChain）への準拠を示すためのエビデンス

示された SBOM の最小要素を取りまとめ、The Minimum Elements For a Software Bill of Materials（SBOM）[9]として 2021 年 7 月に公開している。ここでは、それぞれを以下に紹介する。

① NTIA が取りまとめた SBOM 情報

NTIA のウェブサイト（https://www.ntia.gov/SBOM）に、NTIA が取りまとめた SBOM に関する様々な情報が掲載されている。以下にその一部を紹介する。

■SBOM とは[10]

Software Bill of Materials（SBOM）とは、ある規則に従い機械が読める形をした、ソフトウェアコンポーネント、および依存関係やそれらに関する情報の一覧である。SBOM は、ベンダやユーザなどソフトウェアの関係者にとって、ソフト開発の改善や脆弱性管理などに使用でき、コスト低減やセキュリティなどのリスク低減などのメリットがある。基本となる情報は、作者名、サプライヤ名、コンポーネント名、バージョン、コンポーネントハッシュ、ユニーク ID、関係性、である。対象製品のユースケースに応じてさらに情報を追加すること。SBOM の利点を享受するためには自動処理できる必要がある。SPDX[11]、CycloneDX[12]、SWID[13]の 3 つのフォーマットが定義されている。ソフトウェアエコシステムにおける要求は多岐にわたるため、SBOM を共有するための万能のソリューションはなく、既存のやり方にうまく合わせていくことが重要である。

■ベースライン属性の提案[14]

表 3　ベースライン属性の一覧

属性	意味	特記事項
作者名	SBOM の作者	必ずサプライヤであるとは限らない。その場合、その SBOM はサプライヤが作成したものではないということを示す。
タイムスタンプ	SBOM の最終更新日時	SBOM エントリが変更されたときに必ず更新する。

[9] The United States Department of Commerce/NTIA（2021 年）. “The Minimum Elements For a Software Bill of Materials (SBOM)”. https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
[10] NTIA（2021 年）. “SBOM at a Glance”. https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf
[11] Software Package Data eXchange。Linux Foundation によって策定され、バージョン 2.2.1 が ISO/IEC 5962:2021 として国際規格に採用されている。
[12] OWASP によって策定されている。フォーマットの中に SWID とのマッピングを示す要素あり。
[13] Software Identification （SWID） Tags。IT 資産管理に関する ISO 19770 シリーズの中において、ISO 19770-2:2015 に定義されている。
[14] NTIA（2021 年）. “Framing Software Component Transparency: Establishing a Common Software Bill of Materials（SBOM）”. https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

属性	意味	特記事項
サプライヤ名	SBOM エントリ内のコンポーネントのサプライヤの名前またはその他の識別子	複数の名前を扱えること。作者名とサプライヤ名が同じ場合、サプライヤが自身のコンポーネントについて SBOM を作成したということを示す。異なる場合は、コンポーネントのサプライヤではない者がそのコンポーネントについての主張を行っているということを示す。
コンポーネント名	コンポーネントの名前またはその他の識別子	複数の名前を扱えること。作者名かサプライヤがコンポーネント名を決める。コンポーネント名はサプライヤ名を伝えることができる。
バージョン文字列	コンポーネントのバージョン	サプライヤと作者はバージョンスキームを自由に選択してよい。
コンポーネントハッシュ	コンポーネントの暗号化ハッシュ	ハッシュの代わりにデジタル署名を使うことも可能だがキー管理や署名検証などが必要となる。複数のハッシュを提供することが可能であり、ソースコンポーネントのハッシュ、バイナリコンポーネントのハッシュ、およびコンポーネントのコレクションのハッシュを含めてもよい。
ユニーク ID	コンポーネントを一意に定義するのに役立つ追加情報	グローバルに一意の階層または名前空間に関連して生成することも、既存のグローバル座標系を参照することも可能。Common Platform Enumeration（CPE）、Package URL（PURL）、Universal Unique Identifier（UUID）（Globally Unique Identifier [GUID]）、Software Heritage ID（SWHID）などが使用可能。
関係性	SBOM コンポーネント間の関連付け	デフォルトの関係性タイプは includes であり、これはある別の上流コンポーネントを含む、あるいはそれに依存していることを示す。関係性タイプ primary はそのコンポーネントの上流に依存がないことを示す。

■ベースライン属性と既存のフォーマットとの比較 [14]

表 4　ベースライン属性と既存のフォーマットとの比較

属性	SPDX	CycloneDX	SWID
作者名	Creator:	metadata/authors/name	<Entity> @name（@role: tagCreator）
タイムスタンプ	Created:	metadata/timestamp	<Meta>[15]
サプライヤ名	PackageSupplier:	component/supplier/name	<Entity> @name

[15] <Meta>の属性にタイムスタンプ自体は定義されていないが、追加属性として定義可能。

		もしくは component/publisher	（@role: softwareCreator）
コンポーネント名	PackageName:	component/name	<SoftwareIdentity> @name
バージョン文字列	PackageVersion:	component/version	<SoftwareIdentity> @version
コンポーネントハッシュ	PackageChecksum: もしくは PackageVerificationCode:	component/hashes	<Payload>/../<File> @[hash-algorithm]:hash
ユニーク ID	以下の組み合わせ DocumentNamespace: SPDXID:	serialNumber もしくは component/bom-ref	<SoftwareIdentity> @tagID
関係性	Relationship: DESCRIBES および CONTAINS	ネスト構造で示すか、 dependency のグラフで示す	<Link> @rel, @href

※各規格の仕様を元に、引用元の表現から修正

■よくある質問／誤解[16]

Q: SBOM のメリットは？

A: ソフトウェアのサプライヤと消費者の双方にとって以下のようなメリットがある。

・既知の脆弱性の特定/回避

・ライセンスの管理

・セキュリティ及びライセンスのコンプライアンス要件の特定

・脆弱性の軽減対策の管理（新たな脆弱性に対するセキュリティパッチや代替コントロールを含む）

・効率を上げ、無計画な業務を減らすことによるオペレーティングコストの削減

Q: SBOM は「攻撃側にとってのロードマップ」になってしまうのでは？

A: 理論的には YES である。しかし現実では「防御側にとってのロードマップ」としての役割のほうが大きく、この一般的な懸念を防御側の利益がはるかに上回る。この情報は諸刃の剣ではあるが、ソフトウェアの透明性が欠けているほうが攻撃側にアドバンテージを与えてしまう。

Q: 誰が SBOM を作ってメンテナンスするのか？

A: SBOM はソフトウェアの製造者が作成し、メンテナンスする。「製造者」はベンダ、サプライヤ、そして作者個人など。製造者がサプライヤによって提供された SBOM をまとめるのが理想的だが、存在しない SBOM は製造者が作成する必要があるかもしれない。

[16] NTIA（2021 年）. “SBOM FAQ”. https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf, NTIA（2021 年）. ”SBOM Myths vs. Facts” https://www.ntia.gov/files/ntia/publications/sbom_myths_vs_facts_nov2021.pdf

Q: SBOM は購入者としてどのように活用できるか？
A: SBOM があれば、購入する前に以下のことを知り、できるようになる。
・ソフトウェアの部品とそれらの関係をカタログ化する
・ソフトウェア製品のライセンスチェーンを理解する
・ソフトウェアの複雑なところ（日付、ソフトウェア部品のバージョン）を理解する

Q: SBOM から知的財産や機密情報が漏洩するのでは？
A: SBOM は、含まれているソフトウェアコンポーネントの概要であり、知的財産（IP）は公開されない。特許とアルゴリズムは含まれない。SBOM のコンテンツと IP に関して考慮すべき点がいくつかある。
・原材料表とレシピは異なる。
・サードパーティのオープンソースコンポーネントの IP は、それぞれの作成者または著作権所有者に属する。
・コンポーネントのライセンス条項でそもそも開示が求められることが一般的になってきている。
・SBOM にはコードは含まれず、コンポーネント参照のみが含まれる。
・契約、法的合意、またはその他の要件により、特定のコンポーネントの開示が禁止される場合があり、この場合 SBOM では固有の「既知の未知」コンポーネントがあることを示すこと。

■SNS を使った推進活動

YouTube にて動画で SBOM の情報を公開しており、次のプレイリストが紹介されている。
https://www.youtube.com/playlist?list=PLO2lqCK7WyTDpVmcHsy6R2HWftFkUp6zG[17]

② 大統領令 14028 への対応

米国が直面するサイバーセキュリティの脅威に対抗すべく、2021 年 5 月に国家のサイバーセキュリティの向上に関する大統領令 14028 が発令された。この中で、ソフトウェアサプライチェーンセキュリティの強化が求められている。その背景として主に商用のソフトウェアの開発においてソフトウェアの透明性が欠けていることが多いと指摘しており、その対策の 1 つとして SBOM をソフトウェアの購入者に提供することが挙げられている。さらに、NTIA に対して SBOM の最小要素を公開することを指示した。

③ 大統領令 14028 を受けた SBOM の定義（NTIA）

前述の大統領令を受けて、NTIA は 2021 年 7 月に The Minimum Elements For a Software Bill of Materials（SBOM）を公開した。この中で、SBOM に必要な最小要素は「データフィールド」「自動化サポート」「実践とプロセス」であると定義している。

[17] NTIAGov. “Software Bill of Materials (SBOM)” (2022/12/22 確認)

表 5　SBOM の最小要素

最小要素	
データフィールド	コンポーネントごとに追跡すべきベースライン情報を文書化すること。その情報とは、サプライヤ、コンポーネント名、コンポーネントのバージョン、他のユニーク ID、依存関係、SBOM 作成者、タイムスタンプである。
自動化のサポート	ソフトウェアエコシステムで広く拡張することを可能とするため、自動生成や機械可読性を含む自動化をサポートすること。データフォーマットは、SPDX、CycloneDX、SWID などがある。
実践とプロセス	SBOM の運用である要求、生成、及び使用について定義すること。これには、頻度、深さ、既知の未知、配布、アクセスコントロール、及び、間違いにおける調整を含む

■（ベースラインである）データフィールド

ソフトウェアサプライチェーンの中でソフトウェアコンポーネントを追跡し、脆弱性やライセンスのデータベースといった他のデータソースとマッピングするための十分な識別情報となるベースラインを定義している（表 6）。

表 6　（ベースラインである）データフィールド

データフィールド	説明
サプライヤ名	コンポーネントを作成、定義、識別するエンティティの名前。
コンポーネント名	サプライヤによって定義されたソフトウェアのユニットに割り当てられた指定。
コンポーネントのバージョン	ソフトウェアにおいて、過去の特定のバージョンからの変更を特定するためにサプライヤによって使用される識別子。
他の[18]ユニーク ID	コンポーネントを識別するために使用される、あるいは関連するデータベースで検索するためのキーとして機能するその他の識別子。
依存関係	上流のコンポーネント X がソフトウェア Y に含まれているという関係性を特徴づけるもの。
SBOM 作成者	当コンポーネントの SBOM データを作成したエンティティの名前。
タイムスタンプ	SBOM データを組み立てた日時の記録。

NTIA は、この文書の中で、表 6 に挙げた最小要素として定義したデータフィールド以外にも推奨される項目として、「コンポーネントハッシュ」「ライフサイクルフェーズ」「その他のコンポーネント関係」「ライセンス情報」を挙げている（表 7）。このうち、「コンポーネントのハッシュ」と「その他のコンポーネント関係」は、表 3 に掲載した NTIA が提唱しているベースライン属性にも採用されている。

[18] 「他の（other）」と表現しているのは、「コンポーネント名」と「コンポーネントのバージョン」の組み合わせもユニークな ID となりうるが、それとは別のグローバルな ID を指しているためと思われる。

表 7　推奨データフィールド

データフィールド	説明
コンポーネントのハッシュ	脆弱性データベースなどと照合するために堅牢な識別子が必要であり、暗号ハッシュはこの目的に利用できる。さらに、リネームされた場合やホワイトリスト化が必要な場合にも役立つ。
ライフサイクルフェーズ	SBOM データはソースコードをビルドしたタイミングや、ビルド後にバイナリ解析ツールを使用するなど、異なるステージで収集できる。コンパイラが意図したバージョンと微妙に異なるバージョンのコンポーネントを参照することもある。どこで、いつ、どのように SBOM データが記録されたかを簡単に伝えることができれば便利である。
その他のコンポーネント関係	SBOM の最小要素では、「X は Y に含まれる」という「依存」というタイプの関係性だけを持っており、この関係性は SBOM のグラフ構造によって示唆される。直接的な「依存」以外には例えば「派生」や「子孫」といったものがあり、これは既存のコンポーネントに似ているが何らかの変更が加えられていることを示すことができる。
ライセンス情報	ライセンス管理は SBOM の初期のユースケースであり、大規模で複雑なソフトウェアポートフォリオを持つ組織が、特に OSS の多様なソフトウェアコンポーネントのライセンスと条件を追跡するのに役立つ。ユーザがこの情報を見て、法的リスクを発生させることなくこのソフトウェアを別のアプリケーションのコンポーネントとして使うことができるかどうかを知ることもできる。

■自動化のサポート

自動生成と機械可読性を含む自動化をサポートすることにより、特に組織の境界をまたがったソフトウェアエコシステムの中で拡張していくことが可能になると述べている。組織に既にある脆弱性管理への組込みや、セキュリティポリシーと照らし合わせたリアルタイムのコンプライアンス監査に SBOM を利用したいといった要望に対応するためには自動化が重要であり、そのためには機械可読性のある共通のフォーマットが必要であるとしている。

SBOM の生成と利用のために、グローバルでオープンなプロセスでいくつかのデータ形式が開発されてきた。そのデータフォーマットは以下の通りである。

・Software Package Data eXchange　（SPDX）
・CycloneDX
・Software Identification　（SWID）　Tags

SBOM は組織の境界を超えて伝達する場合、上記のいずれかのフォーマットである必要がある。他のデータフォーマットと互換性のある新しい仕様が出てきた場合は、SBOM 最小要素の観点で自動化のサポートに含められる必要がある。

■実践とプロセス

SBOM は構造化されたデータセット以上のものであり、組織がこれをセキュア開発ライフサイクルに組み込むためには、SBOM の使用のメカニズムにフォーカスした実践とプロセスに従う必要がある。以下のような観点が必要である。

表 8　実践とプロセスの観点

観点	取り組み
頻度	ソフトウェアコンポーネントがビルドやリリースされて更新された場合、ソフトウェアの新しいバージョンを反映するために SBOM が生成されなければならない。
深さ	SBOM は、すべてのトップレベルのコンポーネントを含むべきである。推移的に依存関係が調べられるよう、直接的な依存関係がすべてリストアップされていなければならない。
既知の未知（Known Unknowns）	すべての依存関係が列挙されていない場合、SBOM 作成者は「既知の未知」を識別しなければならない。つまり、依存関係がないと分かっているものと、依存関係が分からないものを明確に区別すること。
配布	SBOM は、それを必要として適切なアクセス権限を持つ者が利用可能である必要がある。SBOM が利用可能であることを伝える方法と、その SBOM へアクセスする方法を決める必要がある。
アクセスコントロール	SBOM データを機密にして、アクセスできるユーザを制限したい場合、その条件を定義する必要がある。これにはライセンスや契約など、既存のメカニズムが利用できる。
間違いにおける調整	SBOM の初期実装段階に、省略やエラーを許容することを含める必要がある。サプライチェーンデータの内部管理はまだ発展途上である。しかし、完成されるのを待つより、エラーを許容しつつすぐにスタートするべきである。

2）　米国行政予算管理局（OMB）の取り組み

OMB も大統領令 14028 の指令を受けて、2022 年 9 月に政府の各機関向けにソフトウェア開発プラクティスを通したソフトウェアサプライチェーンのセキュリティの向上のための覚書[19]を発行している。政府機関に対してソフトウェア調達の際に、大統領令 14028 を受けた NIST ガイダンス[20]への準拠を示す自己適合宣言をソフトウェアサプライヤから取得することを指示している。同時に、サプライヤに対してその準拠を示す成果物の 1 つとして SBOM を要求できるとしている。SBOM のフォーマットは先に示した NTIA の The Minimum Elements For a Software Bill of Materials（SBOM）か、サイバーセキュリ

[19] OMB（2022 年）. “M-22-18, SUBJECT: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”.
https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

[20] NIST（2022 年）. “Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e”.
https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

ティ・インフラストラクチャセキュリティ庁（CISA）が発行する後継のガイダンス[21]で規定されるフォーマットでなければならないとしている。

３）　トヨタ自動車の事例

2021 年に経済産業省が公開した「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集[22]」に国内の各社においてすでに SBOM が活用されている例が掲載されている。ここでは、その中からトヨタ自動車株式会社の事例を取り上げる。

■OpenChain 活動

トヨタ自動車では、サプライチェーン全体にわたって OSS コンプライアンスを実現する Linux Foundation による業界標準「OpenChain」の活動を行っている。プロジェクトの主な成果物は、「仕様（要件定義）」「適合（認証）」「カリキュラム（教育資料集）」の３点であり、この成果物の活用イメージを示したものが図 1 である。「仕様」に関しては、表 1 の調査文献にも挙げているが、2020 年 12 月に ISO/IEC5230 として国際標準化されている。

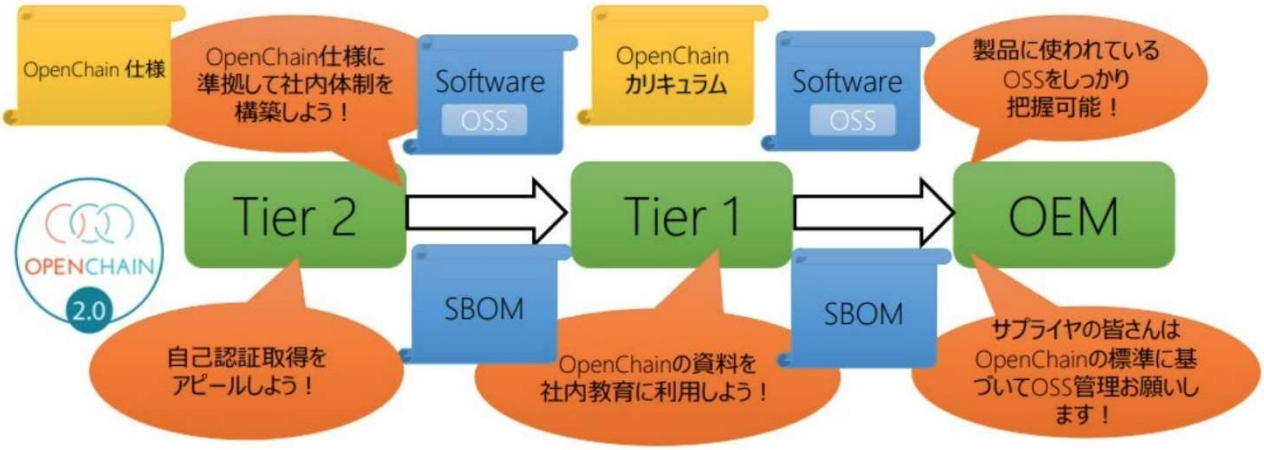


図 1　OpenChain の成果物の活用イメージ
出典）「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」図 4.1-2

■各サプライヤと使用ソフトウェアに関するガイドラインを合意

サプライチェーンにおける OSS コンプライアンスの役割、使用ソフトウェアリスト（SBOM）を提供することや、注意を払うべきライセンスなどについて、会社間でガイドラインの合意を行っている。業

[21] ただし、2022 年 11 月時点では、The Minimum Elements For a Software Bill of Materials (SBOM)の後継となるガイダンスをリリースしておらず、これを参照するのにとどまっている。
[22] 経済産業省（2022 年）. “OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集”. https://www.meti.go.jp/press/2022/05/20220510001/20220510001-1-2.pdf

界の商習慣として、供給先に対して必要以上の情報提供を避ける傾向があったが、ガイドラインの合意に向けて特にコンプライアンスの重要性について、各サプライヤに対して理解を求めている。

■各サプライヤと使用ソフトウェア報告の運用規則について合意

先のガイドラインに基づき、各サプライヤとの供給関係（プロジェクト）ごとに実務レベルで運用規則の合意を行っている。具体的には、規則の適用範囲（製品、サービスなど）、SBOM の報告方法、報告のタイミングなどをプロジェクトごとに定めている。OpenChain Project における OSS の Transparency 向上への取組[23]によると、SPDX Lite は、SPDX のハンドリングが困難な組織でも SBOM を取り扱い可能にする入門編として定義され、日本から SPDX コミュニティに提案したとのこと。

■SBOM のフォーマット

各サプライヤにおけるハンドリングのしやすさを考慮した結果、使用ソフトウェアリストのフォーマットは OpenChain で議論されている SPDX Lite を採用している。SPDX Lite は、SPDX の簡易バージョンであり、Excel などでの管理も可能である。

SPDX Liteの項目例
-パッケージ名
-パッケージSPDX識別子
-パッケージバージョン
-パッケージファイル名
-パッケージダウンロード位置（入手先）
-解析したファイル（手作業の場合false）
-ホームページ（開発コミュニティサイト）
-結論されたライセンス
-宣言されたライセンス
-ライセンスへのコメント
-著作権テキスト
-改変の有無
-パッケージに関するコメント
-ライセンス識別子

SPDXサンプルの一部抜粋

	3.1	3.2	3.3	3.4	3.7	3.8	3.11	3.13	3.15
	PackageName	Package SPDX Identifier	Package Version	PackageFileName	PackageDownloadLocation	Files Analyzed	PackageHomePage	Concluded License	Declared License
項	パッケージ名	パッケージSPDX識別子	パッケージバージョン	パッケージファイル名	パッケージダウンロード位置（入手先）	解析したファイル（手作業の場合false）	ホームページ（OSS開発コミュニティサイト）	結論されたライセンス	宣言されたライセンス
	LibXML2		2.99	libxml2-2.9.9.tar.gz	ftp://xmlsoft.org/libxml2/	FALSE	http://xmlsoft.org/	MIT	MIT
	PCRE		8.4343	pcre-8.43.tar.gz	ftp://ftp.pcre.org/pub/pcre/	FALSE	https://www.pcre.org/	BSD-3-Clause	BSD-3-Clause
	SQLite		3300100.tartar	sqlite-autoconf-3300100.tar.gz	https://www.sqlite.org/download.html	FALSE	https://www.sqlite.org/index.html	その他（ライセンス名を記載）	その他（ライセンス名を記載）
	Zlib (1.2.3)		1.2.11	zlib-1.2.11.tar.gz	https://www.zlib.net/	FALSE	https://www.zlib.net/	Zlib	Zlib
	cURL (7.41.0)		7.66.0	curl-7.66.0.tar.bz2	https://github.com/curl/curl/releases	FALSE	https://curl.haxx.se/	MIT	MIT

図 2　SPDX Lite フォーマット（サンプル）
出典）「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」図 4.1-1

4）　NTIA ベースラインと SPDX Lite の項目の比較

NTIA が提唱するベースライン属性と SPDX Lite の項目を比較したものを表 9 に掲載する。NTIA のベースラインは NTIA が提唱しているベースラインと、大統領令を受けて公開した最小要素のベースラインとで微妙に異なるため両方と比較している。

[23] トヨタ自動車株式会社（2019 年）. “OpenChain Project における OSS の Transparency 向上への取組”. https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_04_00.pdf

表 9　NTIA ベースラインと SPDX Lite の項目比較

Framing Software Component Transparency: Establishing a Common Software Bill of Materials（SBOM） - Second Edition – ベースライン属性[24]	The Minimum Elements For a Software Bill of Materials（SBOM） *データフィールド／推奨データフィールド*[25] （イタリック体の項目が推奨データフィールド）	SPDX Lite （SPDX v2.3）
Author Name（作者名）	Author of SBOM Data（SBOM データの作者）	Creator（作者）
Timestamp（タイムスタンプ）	Timestamp（タイムスタンプ）	Created（作成日時）
Supplier Name（サプライヤ名）	Supplier Name（サプライヤ名）	Package Supplier（パッケージサプライヤ）
Component Name（コンポーネント名）	Component Name（コンポーネント名）	Package Name（パッケージ名）
Version String（バージョン文字列）	Version of the Component（コンポーネントのバージョン）	Package Version（パッケージバージョン）
Component Hash（コンポーネントハッシュ）	*Hash of the Component（コンポーネントのハッシュ）*	—
Unique Identifier（ユニーク ID）	Other Unique Identifiers（他のユニーク ID）	Package SPDX Identifier（パッケージ SPDX 識別子）
Relationship（関係性）	Dependency Relationship（依存関係） *Other Component Relationships（その他のコンポーネント関係）*	—
—	*Lifecycle Phase（ライフサイクルフェーズ）*	—
—	*License Information（ライセンス情報）*	Concluded License（結論されたライセンス）
		Declared License（宣言されたライセンス）
		Comments on License（ライセンスへのコメント）
		License Identifier（ライセンス識別子）
		Extracted Text（ライセンステキスト）

[24] NTIA が提唱するベースライン属性。2021 年 10 月公開。
[25] NTIA が大統領令 14028 を受けて提示した最小要素であるデータフィールド（推奨データフィールドを含む）。2021 年 7 月公開。

Framing Software Component Transparency: Establishing a Common Software Bill of Materials （SBOM） - Second Edition – ベースライン属性[24]	The Minimum Elements For a Software Bill of Materials （SBOM） *データフィールド／推奨データフィールド*[25] （イタリック体の項目が推奨データフィールド）	SPDX Lite （SPDX v2.3）
		License Name（ライセンス名）
		License Comment（ライセンスコメント）
—	—	SPDX Version（SPDX バージョン）
—	—	Data License（データライセンス）
—	—	SPDX Identifier（SPDX 識別子）
—	—	Document Name（ドキュメント名）
—	—	SPDX Document Namespace（SPDX ドキュメント名前空間）
—	—	Package File Name（パッケージファイル名）
—	—	Package Download Location（パッケージダウンロード位置）
—	—	Files Analyzed（解析したファイル）
—	—	Package Home Page（ホームページ）
—	—	Copyright Text（著作権テキスト）
—	—	Package Comment（パッケージに関するコメント）
—	—	External Reference field（外部参照）

５）　米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）の取り組み

米国行政予算管理局（OMB）の通達で触れられている CISA においても、NTIA が進めてきた SBOM に対する取組をさらに発展させており、ウェブサイト（https://www.cisa.gov/sbom）で情報発信している。特に、元々NTIA で検討が進められてきた SBOM 関連のコンセプトの１つである VEX（Vulnerability Exploitability eXchange）の検討を引き継いでいる。

VEX とは、ある製品が脆弱性の影響を受けているかどうかを通知する、いわゆるセキュリティアドバイザリの機械可読フォーマット版であり、ツールによる自動化を想定している。また、SBOM をより有効に活用できるようにするものとしても期待されている。前述のウェブサイトで、推奨される VEX の最小データ要素とユースケースを提示した資料[26]が公開されている。表 10 に CISA が推奨する VEX の最小データ要素を示す。

表 10　VEX の推奨される最小データ要素

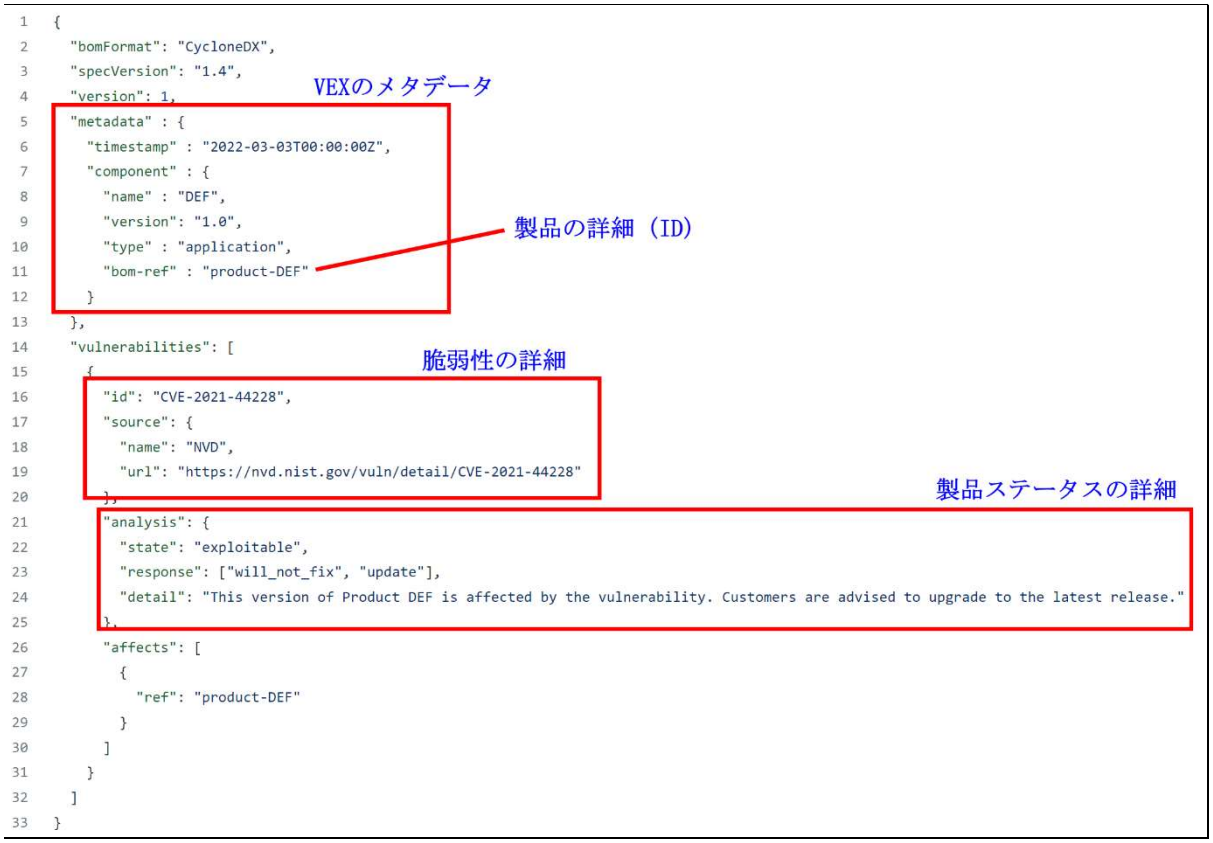
最小データ要素	最低限必要な情報
VEX のメタデータ	・VEX フォーマット ID ・VEX ドキュメント ID ・作成者 ・作成者の役割 ・タイムスタンプ
製品の詳細	・製品 ID、もしくは、製品ファミリ ID （例えばユニーク ID、もしくはサプライヤ名、製品名、バージョンの組み合わせ）
脆弱性の詳細	・脆弱性 ID（CVE やその他の ID） ・脆弱性の説明（例えば CVE description）
製品ステータスの詳細（製品の脆弱性に関するステータス情報）	・影響なし（当該脆弱性に対して対策不要） ・影響あり（当該脆弱性に対して修正もしくは対処することが推奨される） ・修正済み（このバージョンの製品は当該脆弱性に対して修正済み） ・調査中（このバージョンの製品が当該脆弱性の影響を受けるかどうかが不明。後報にて更新情報が提供予定） ※ステータスが「影響あり」の場合、VEX ドキュメントに対応方法を記載すること。「影響なし」の場合、VEX ドキュメントに根拠を記載すること。

[26] CISA（2022 年）. “Vulnerability Exploitability eXchange (VEX) – Use Cases”. https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Aprill2022.pdf

この情報を実際に伝えるユースケース例が併せて提示されており、ここでそのうちの１つを紹介する。

Example 社の製品「EDF」のバージョン 1.0 が脆弱な Log4j のライブラリを使用していた。Log4Shell の最初の脆弱性（CVE-2021-44228）が公開されたとき Example 社の PSIRT が、「製品 DEF は『影響あり』であり、顧客はバージョンを 1.1 にアップデートするべき」という内容の VEX をリリースした。

このユースケースに対応する VEX の例として、CSAF[27]と CycloneDX の２つのフォーマットの例が示されているが、ここではこのうち、SBOM の標準フォーマットの１つでもある CycloneDX の例を図 3 に示す。




```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.4",
  "version": 1,
  "metadata" : {
    "timestamp" : "2022-03-03T00:00:00Z",
    "component" : {
      "name" : "DEF",
      "version": "1.0",
      "type" : "application",
      "bom-ref" : "product-DEF"
    }
  },
  "vulnerabilities": [
    {
      "id": "CVE-2021-44228",
      "source": {
        "name": "NVD",
        "url": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228"
      },
      "analysis": {
        "state": "exploitable",
        "response": ["will_not_fix", "update"],
        "detail": "This version of Product DEF is affected by the vulnerability. Customers are advised to upgrade to the latest release."
      },
      "affects": [
        {
          "ref": "product-DEF"
        }
      ]
    }
  ]
}
```

図 3　製品ステータスが「影響あり」の場合の VEX 例（CycloneDX JSON フォーマット）[28]

■参考）影響なしと判断した場合の根拠について

ある脆弱性に対して「影響なし[29]」とした場合に、そう判断した根拠を示す必要があるが、この根拠に関する資料[30]も公開されており、その内容を整理したものを表 11 に示す。

---

[27] CSAF：Common SecurityAdvisory Framework

[28] CycloneDX（2022 年）. “vex-affected.json”. https://github.com/CycloneDX/bom-examples/blob/master/VEX/CISA-Use-Cases/Case-1/vex-affected.json

[29] 表 10 の「製品ステータスの詳細」参照。

[30] CISA（2022 年）. “Vulnerability Exploitability eXchange (VEX) - Status Justifications”. https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf

表 11　ステータスを「影響なし」と判断した根拠

種別	根拠	該当する例
Component_not_present	脆弱なコンポーネントが製品に含まれていない。	・当該製品は Python と Elixir で書かれていて、Java のコードは含まれていない。このため Log4j の脆弱性の影響を受けない。 ・Java JAR ファイルは別の JAR ファイルを含むことが多いことから、自動処理によってある JAR ファイルの中に当該コンポーネントがあるとみなされた。 ・ベースレイヤのコンテナイメージには使用されないパッケージが含まれることがよくあり、それが上位レイヤで削除されるケースがある。あるコンテナイメージに「sudo」が含まれているとみなされたが、実際は展開前に削除されていた。
Vulnerable_code_not_present	脆弱なコードはあるが、実行されることがない。	・古いライブラリが一緒に提供されたが、当該ソフトウェアからは使用されない。 ・すでにパッチが当てられているが、ロールバック目的で脆弱なバイナリが残っている。 ・コンテナイメージに、アプリケーションが使用していない OS のユーティリティが含まれている。そのユーティリティは削除ができない。 ・ライブラリの中の脆弱なコードを含む関数が決して呼ばれることがないケースもこのステータスになる。OpenSSL を乱数生成のためだけに使うアプリケーションには、Heartbleed の脆弱性はない。 ・当該コードが、取り付けられていないハードウェアモジュールからのみ実行される場合。
Vulnerable_code_cannot_be_controlled_by_adversary	直接攻撃者が当該脆弱性を突くことができない。	・脆弱な関数にユーザが生成した入力を与えても、ハードコーディングされた変数がそれを受け付けない。 ・ハードウェア異常の際やインストールの間にのみ呼ばれるログ機能。 ・ソフトウェアは EternalBlue の脆弱性を持っているが、SMB に関係ある 139 および 445 ポートは無効化していて、ユーザがこれを変更することもできない。ポートが開いていないため攻撃者がこの脆弱性を利用することはできない。

種別	根拠	該当する例
Inline_mitigations_already_exist	脆弱性から防御する仕組みが組み込まれている。	・上流で入力がサニタイズされている。 ・サンドボックスでメモリの分離が行われている。 ・脆弱なコードを利用するコンポーネントの出力や結果が検証可能になっている。 ・2 数の積によるバッファオーバフローにおいて、片方の引数が常に 1 のため発生しない。 ・ソフトウェアは EternalBlue の脆弱性を持っていて SMB ポートも開いている。しかし、組込みファイアウォールがそのアクセスをふさいでおり、ユーザがその設定を変更することもできない。

６） PCI Secure Software Standard[31]

PCI によるクレジットカードデータを扱うソフトウェアの認証規格である PCI Secure Software Standard の最新バージョンである 1.2 が 2022 年 12 月にリリースされ[32]、インターネットを通して決済処理を行う Web ソフトウェアに対する要件が新規に追加された。その中に、SBOM の管理に関する要件が新しく追加されており、業界の認証要件として SBOM 管理が要求される例となっている。SBOM に関する要件を以下に抜粋して紹介する。

- [C.1.1] すべてのソフトウェアコンポーネントとサービスを文書化、もしくはソフトウェア部品表(SBOM)の形でカタログ化すること。
- [C.1.2] SBOM には使用中している一次的なコンポーネントとサービスを記述すること。さらにそれらの二次的なコンポーネントに対する関係や依存関係を可能な限り記述すること。
- [C.1.3] ソフトウェアが SaaS として提供される場合、SBOM は本番ソフトウェア実行環境に存在するソフトウェア依存関係を可能な限り説明する情報を含むこと。
- [C.1.4] SBOM は、ソフトウェアサプライチェーン全体で各コンポーネントまたはサービスを追跡できるように、各コンポーネントまたはサービスに関する十分な情報を含むこと。
- [C.1.5] ソフトウェアが更新されるたびに、新しい SBOM を作成または生成すること。

31 PCI SSC. “Document Library”. https://www.pcisecuritystandards.org/document_library/

32 PCI SSC. “New Web Software Module Introduced in PCI Secure Software Standard Version 1.2”. https://blog.pcisecuritystandards.org/new-web-software-module-introduced-in-pci-secure-software-standard-version1-2 (2022/12/22 確認)

1-2-4　OSS 管理、セキュリティ対策チェックシート

＜調査項目１＞のまとめとして、前項までの調査結果をもとに、OSS 管理のセキュリティ対策をチェックシート形式で整理した（表 12、表 13）。なおチェックリストの作成にあたっては、「IoT 社会に対応したサイバー・フィジカル・セキュリティに係るＯＳＳの技術検証のあり方などに関する調査」において実施した IoT 製品の製品提供企業へのヒアリング結果を反映し、一部項目の追記やレベルの調整を行っている。

表 12　OSS 管理におけるセキュリティ対策チェックシート（全社で対応すべき事項）

ID	対象	大項目	中項目	小項目	レベル	チェック
1	・ユーザ企業 ・製品提供企業 及び上流企業	ルール・体制	ルール	・組織全体のセキュリティポリシーを規定している。	必須	□
2	・ユーザ企業 ・製品提供企業 及び上流企業			・組織内の各関係者（※）が果たすべきセキュリティに関する役割を規定している。 （※）PSIRT 専任者、PSIRT 兼任者（各部門のセキュリティ担当者）、役員、管理職、ソフトウェア開発者、テスター、など	必須	□
3	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアのライセンスの取り扱いを規定している。	必須	□
4	・ユーザ企業 ・製品提供企業 及び上流企業			・脆弱性対応に関する基準を規定している。 （例）脆弱性のスコアリングは CVSS v3 を採用する。CVSS 深刻度（9.0～10.0：緊急、7.0～8.9：重要、…）に応じて対応する（緊急に割り当たったものは 1 か月以内にセキュリティパッチを配布、など）。	必須	□

ID	対象	大項目	中項目	小項目	レベル	チェック
5	・ユーザ企業 ・製品提供企業 及び上流企業			・インシデント対応に関する基準を規定している。 （例）インシデント発生時の社内でのエスカレーションルールや判断基準、外部ステークホルダにいつまでに報告するかなど	必須	□
6	製品提供企業 及び上流企業		体制	・PSIRT を設置し、製品セキュリティに対する脆弱性対応やインシデント対応を行う体制が整っている。 （セキュリティ専任の人員がいること。これが困難な場合、各部署からセキュリティの知識をある程度持った人員を兼任させること。）	必須	□
7	・ユーザ企業 ・製品提供企業 及び上流企業			・CSIRT や自社のオペレーションを監視する機能を持った組織を設置し、情報セキュリティに対する脆弱性対応やインシデント対応を行う体制が整っている。 （セキュリティ専任の人員がいること。これが困難な場合、各部署からセキュリティの知識をある程度持った人員を兼任させること。）	必須	□
8	・ユーザ企業 ・製品提供企業 及び上流企業			・規定した役割を果たすためのリソース（人的、予算）が十分ある。	必須	□
9	・ユーザ企業 ・製品提供企業 及び上流企業			・OSS ライセンスに関して、専門家（法務部門など）に問い合わせるなどの対応方法を有している。	必須	□
10	・ユーザ企業 ・製品提供企業 及び上流企業		教育	・組織内のすべての関係者に必要なソフトウェセキュリティに関する基本要件（知識など）と、役割ごとに求められる要件をそれぞれ定義している。	必須	□

ID	対象	大項目	中項目	小項目	レベル	チェック
11	・ユーザ企業 ・製品提供企業 及び上流企業			・組織内の関係者のソフトウェアセキュリティに関するスキルを管理する方法を定義している。	必須	□
12	・ユーザ企業 ・製品提供企業 及び上流企業			・基本要件、及び役割ごとに求められる要件を満たすためのトレーニングを定義している。 （組織によって求められる内容が異なるため、独自で作成するのではなく、外部のセキュリティトレーニング提供者による教育を受けるような場合、自組織向けにカスタマイズが必要な場合あり。）	必須	□
13	・ユーザ企業 ・製品提供企業 及び上流企業			・ソフトウェアセキュリティに関する教育計画を立てている。	必須	□
14	・ユーザ企業 ・製品提供企業 及び上流企業			・ソフトウェアセキュリティに関する教育を入社時や開発に従事する前、及び定期的に実施している。	必須	□
15	・ユーザ企業 ・製品提供企業 及び上流企業			・ソフトウェアセキュリティに関する脆弱性対応やインシデント対応の演習を定期的に実施している。	必須	□
16	・ユーザ企業 ・製品提供企業 及び上流企業			・教育コンテンツを適宜見直している。 （これまで実施した教育の効果や演習のフィードバック、最近のインシデント傾向などを考慮して次の教育に反映する。）	必須	□

ID	対象	大項目	中項目	小項目	レベル	チェック
17	・ユーザ企業 ・製品提供企業 及び上流企業	対外対応	脆弱性対応・ インシデント対応	・考えられる脆弱性対応やインシデント対応のケース（以下例）についてのマニュアルを準備している。 （例） 脆弱性が一般公開されたケース、ゼロデイの報告を受けたケース、脆弱性が悪用されたケース、複数の関係者や OSS が関わる大規模なインシデントが発生したケース	必須	□
18	・ユーザ企業 ・製品提供企業 及び上流企業			・脆弱性データベースやセキュリティメーリングリスト、その他の脆弱性レポートなどを利用して、セキュリティ情報を得ている。	必須	□
19	・ユーザ企業 ・製品提供企業 及び上流企業			・脆弱性がどのように悪用されているかを理解するため、脅威インテリジェンスを利用している。	**高度**	□
20	製品提供企業 及び上流企業			・新たに発見された脆弱性を修正し、その情報を展開し、更新プログラムを配布するためのプロセスが存在する。	必須	□
21	製品提供企業 及び上流企業			・脆弱性対応基準に従って、必要であれば脆弱性に対応し、その更新プログラムが展開されるようになっている。脆弱性に対応しないという例外に対しては、個別に適切に承認されるようになっている。	必須	□
22	・ユーザ企業 ・製品提供企業 及び上流企業	サプライチェーン	役割の定義	・サプライチェーンにおける自組織の役割を特定し、サプライチェーンの関係者と共有している。	必須	□
23	・ユーザ企業 ・製品提供企業 及び上流企業			・サプライチェーンにおける自組織の役割に基づき、リスク許容度を決定している。	必須	□

ID	対象	大項目	中項目	小項目	レベル	チェック
24	・ユーザ企業 ・製品提供企業 及び上流企業			・サプライチェーンにおけるセキュリティ対策や運用について、継続的に見直し・改善を行っている。	必須	☐
25	ユーザ企業		サードパーティ対応	・セキュリティ対策を行っているサードパーティを採用している。	必須	☐
26	・ユーザ企業 ・製品提供企業 及び上流企業			・一般的なセキュリティレコメンデーション（例：NISTIR 8259.10）を実装している、あるいはセキュリティ標準（例：ISO27036、ISO28000）に準拠しているサプライヤを採用していること。	必須	☐
27	・ユーザ企業 ・製品提供企業 及び上流企業			・セキュリティの監査を契約に含め、定期的に監査・評価を実施している。	**高度**	☐
28	・ユーザ企業 ・製品提供企業 及び上流企業			・セキュリティ監査において不適合事項があった場合に実施すべき対応を定義し、運用している。	必須	☐
29	・ユーザ企業 ・製品提供企業 及び上流企業			・提供されるソフトウェアにセキュリティ対策を実施する契約を結んでいる。	必須	☐
30	・ユーザ企業 ・製品提供企業 及び上流企業			・提供されるソフトウェアにセキュリティ対策を実施する契約を結んでいる。	必須	☐
31	・ユーザ企業 ・製品提供企業 及び上流企業	対外対応	情報収集	・製品およびサービスに関する情報（セキュリティやライセンス）を受け付けるための窓口が存在する。	必須	☐

ID	対象	大項目	中項目	小項目	レベル	チェック
32	製品提供企業 及び上流企業			・コミュニケーションの窓口を通して社外の関係者（ユーザ、セキュリティ研究者など）がセキュリティ関連の問題を報告することができ、またその報告に対する進捗を受け取ることができるようになっている。	必須	□
33	製品提供企業 及び上流企業		情報発信	・ユーザに対して、製品のサポート条件やメンテナンスの方法などの情報を提供している。	必須	□
34	製品提供企業 及び上流企業			・ユーザに対して、製品の脆弱性が発見された場合にその情報や必要な対応方法、アップデートが利用可能になった場合や製品のサポート条件が変更された場合などにそのことを通知している。	必須	□
35	製品提供企業 及び上流企業			・CERT 団体と連携し、製品に脆弱性が出た場合、脆弱性に関する情報、対応方法などを連絡するようになっている。	必須	□
36	製品提供企業 及び上流企業			・製品のセキュリティに関する認証取得や評価結果を公開していること。	**高度**	□
37	製品提供企業 及び上流企業			・製品そのものではないが、関連する脆弱性情報やそれに対する対応方法の情報を提供していること。	**高度**	□

表 13　OSS 管理におけるセキュリティ対策チェックシート（開発部門/調達部門など）

ID	対象	大項目	中項目	小項目	レベル	チェック
1	製品提供企業 及び上流企業	ソフトウェア 開発プロセス	定義	・ソフトウェア製品のセキュリティ要件を定義し、文書化している。	必須	□

ID	対象	大項目	中項目	小項目	レベル	チェック
2	製品提供企業 及び上流企業			・ソフトウェア製品のセキュアな設定/構成を定義し、文書化している。	必須	□
3	製品提供企業 及び上流企業			・ソフトウェア製品のリスク評価基準が定義されている。	必須	□
4	製品提供企業 及び上流企業			・コードテストを実施するタイミングや、コードテストの実施方法が定義されている。	必須	□
5	製品提供企業 及び上流企業		構成管理	・ソフトウェア構成管理のためのリポジトリを構築し使用している。	必須	□
6	製品提供企業 及び上流企業			・リポジトリに格納したソースコードや設定/構成に対し、適切なアクセス制限を行っている。特に、制限なくインターネットに公開されるようなことがないこと。	必須	□
7	製品提供企業 及び上流企業			・リポジトリのバージョン管理機能により、コードに加えられた変更が追跡され、責任者がそれを確認して承認を行っている。	必須	□
8	製品提供企業 及び上流企業			・リリースイメージの整合性を担保している。	必須	□
9	製品提供企業 及び上流企業			・リリースイメージの整合性情報は、リリースイメージとは別のところで保管したり、データ署名を利用したりして保護している。	必須	□
10	製品提供企業 及び上流企業		SBOM	・ソフトウェア製品の SBOM データを社内外の関係者が利用できるようにしている。	必須	□
11	製品提供企業 及び上流企業			・ソフトウェアコンポーネントを更新するたび、SBOM を更新している。	必須	□

ID	対象	大項目	中項目	小項目	レベル	チェック
12	製品提供企業 及び上流企業			・SBOM データフォーマットは標準形式を使用。	必須	☐
13	製品提供企業 及び上流企業		開発環境	・セキュアコーディングの実施をサポートする自動化された開発環境を使用していること。	必須	☐
14	製品提供企業 及び上流企業			・プロジェクトの自動動的テスト環境を構築し、動的な脆弱性テストが実施される。	必須	☐
15	製品提供企業 及び上流企業			・開発以外の環境からネットワークを分離し、かつ、アクセス制御を実施している。	必須	☐
16	製品提供企業 及び上流企業			・ゼロ信頼アーキテクチャに基づく開発環境を導入している。	**高度**	☐
17	製品提供企業 及び上流企業			・ツール自体や設定/構成を適切に評価し、導入後のツールの脆弱性に随時対応し、必要に応じて新しい機能を追加している。	必須	☐
18	製品提供企業 及び上流企業		開発ツール	・コンパイラ、インタプリタ、ビルドツールはサポートされているバージョンを使用している。	必須	☐
19	製品提供企業 及び上流企業			・すべてのコンパイラ警告がエラーとして扱われるようにしている。	必須	☐
20	製品提供企業 及び上流企業			・メモリ配置のランダム化や難読化など、コンパイラが持つセキュリティ機能を有効にしている。	必須	☐
21	製品提供企業 及び上流企業			・コンパイラ、インタプリタ、ビルドツールの設定/構成が、定義、承認された通りであることを定期的に確認している。	必須	☐
22	製品提供企業 及び上流企業		脅威分析	・製品やシステムに対する脅威や脆弱性を特定するプロセスが存在する。	必須	☐

ID	対象	大項目	中項目	小項目	レベル	チェック
23	製品提供企業及び上流企業		設計	・脅威分析の結果として対策が必要とされたものに対して対策を行っている。	必須	□
24	製品提供企業及び上流企業		コーディング	・コーディングにおいて、セキュアコーディングを実施している。	必須	□
25	製品提供企業及び上流企業		レビュー	・コーディングチェックにおいて、セキュリティの観点でコードのピアレビューを実施している。	必須	□
26	製品提供企業及び上流企業			・コーディングチェックにおいて、セキュリティの専門家によるコードレビューを実施している。	**高度**	□
27	製品提供企業及び上流企業			・コードレビューから得られた教訓を記録し、wiki で公開するなどして開発者がいつでも見られるようにしている。	必須	□
28	製品提供企業及び上流企業		静的テスト	・コーディングチェックにおいて、セキュアコーディングが実施されていることをツールによって検証している。	必須	□
29	製品提供企業及び上流企業		動的テスト	・動的テストにおいて、セキュリティ観点の機能テストが実施されている。	必須	□
30	製品提供企業及び上流企業			・動的テストにおいて、ファジングテストが実施されている。	**高度**	□
31	製品提供企業及び上流企業			・動的テストにおいて、脆弱性スキャンが実施されている。	必須	□
32	製品提供企業及び上流企業			・動的テストにおいて、ペネトレーションテストが実施されている。	**高度**	□
33	製品提供企業及び上流企業			・動的テストから得られた教訓を記録し、wiki で公開するなどして開発者がいつでも見られるようにしている。	必須	□

ID	対象	大項目	中項目	小項目	レベル	チェック
34	製品提供企業及び上流企業		脆弱性対応	・ソフトウェア製品に対して、サポート対象である間はリリース後も定期的にセキュリティテストを実施している。	必須	☐
35	製品提供企業及び上流企業			・ツールチェーンを構成し、ソフトウェア製品に対して、サポート対象である間はリリース後も定期的に自動的にセキュリティテストを実行している。	必須	☐
36	製品提供企業及び上流企業			・発見された脆弱性は根本原因を特定し、横展開し、再導入されないようにするプロセスが存在する。	必須	☐
37	製品提供企業及び上流企業	調達	サードパーティソフトウェア〔発注者が設計する場合（OEM）〕	・サードパーティソフトウェアに対して、セキュリティの観点でレビュー、テストを実施している。	必須	☐
38	製品提供企業及び上流企業			・サードパーティソフトウェアに対して、ハッシュやデジタル署名などで完全性を確認している。	必須	☐
39	製品提供企業及び上流企業			・サードパーティソフトウェアに対して、提供された SBOM やコンポジションアナリシスを実施して、脆弱性や OSS ライセンスなどのリスクを評価している。	必須	☐
40	製品提供企業及び上流企業			・サードパーティソフトウェアの SBOM データを管理している。	必須	☐
41	製品提供企業及び上流企業			・サードパーティソフトウェアを SBOM データとともに社内のリポジトリで管理している。	必須	☐
42	製品提供企業及び上流企業			・サードパーティソフトウェアに対して、提供元がまだ修正していない既知の脆弱性がないか定期的に確認している。	必須	☐
43	製品提供企業及び上流企業			・サードパーティソフトウェアの既知の脆弱性を自動検出する機能を導入している。	**高度**	☐

ID	対象	大項目	中項目	小項目	レベル	チェック
44	・ユーザ企業 ・製品提供企業 及び上流企業		サードパーティソフトウェア 〔サードパーティが設計する場合（ODM）〕	・サードパーティソフトウェアに対して、セキュリティの観点でレビュー、テストを実施している。	必須	☐
45	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアに対して、ハッシュやデジタル署名などで完全性を確認している。	必須	☐
46	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアに対して、提供された SBOM やコンポジションアナリシスを実施して、脆弱性や OSS ライセンスなどのリスクを評価している。	必須	☐
47	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアの SBOM データを管理している。	必須	☐
48	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアを SBOM データとともに社内のリポジトリで管理している。	必須	☐
49	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアに対して、提供元がまだ修正していない既知の脆弱性がないか定期的に確認している。	必須	☐
50	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアの既知の脆弱性を自動検出する機能を導入している。	**高度**	☐

ID	対象	大項目	中項目	小項目	レベル	チェック
51	製品提供企業 及び上流企業		サードパーティソフトウェア 〔OSS の場合〕	・サードパーティソフトウェアに対して、セキュリティの観点でレビュー、テストを実施している。	必須	☐
52	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアに対して、ハッシュやデジタル署名などで完全性を確認している。	必須	☐
53	製品提供企業 及び上流企業			・バイナリで取得したサードパーティソフトウェアは完全性と SBOM を確認している。確認できない OSS はソースコードからビルドしている。	**高度**	☐
54	製品提供企業 及び上流企業			・サードパーティソフトウェアに対して、提供された SBOM やコンポジションアナリシスを実施して、脆弱性や OSS ライセンスなどのリスクを評価している。	必須	☐
55	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアの SBOM データを管理している。	必須	☐
56	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアを SBOM データとともに社内のリポジトリで管理している。	必須	☐
57	・ユーザ企業 ・製品提供企業 及び上流企業			・各サードパーティソフトウェアが保守されており、サポートが切れていないことを確認している。	必須	☐
58	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアに対して、提供元がまだ修正していない既知の脆弱性がないか定期的に確認している。	必須	☐

ID	対象	大項目	中項目	小項目	レベル	チェック
59	・ユーザ企業 ・製品提供企業 及び上流企業			・サードパーティソフトウェアの既知の脆弱性を自動検出する機能を導入している。	**高度**	□
60	・ユーザ企業 ・製品提供企業 及び上流企業			・脆弱性情報を見つけた場合、OSS コミュニティにフィードバックしている。	**高度**	□
61	製品提供企業 及び上流企業	機能	自社開発 ソフトウェア	・ソフトウェア全体、あるいは、そのソフトウェア製品に含まれる個々のコンポーネント（OSS など）がアップデートできる仕組みがある。	必須	□
62	製品提供企業 及び上流企業			・アップデートしようとしているソフトウェアあるいはソフトウェアコンポーネントを適用する前に検証できる仕組みがある。	必須	□
63	製品提供企業 及び上流企業			・ハッシュやコード署名などを使用して、実行ファイルの完全性を保護する機能がある。	**高度**	□
64	製品提供企業 及び上流企業			・通信データや保存データの保護などのために暗号技術を実装する場合、CRYPTREC などの標準に従った強力な暗号を用いている。	**高度**	□

＜調査項目２＞OSS に関わる CSIRT・PSIRT 連携案の調査

2-1 調査の背景・目的

本章の OSS に関わる CSIRT・PSIRT 連携案の調査では、文献による CSIRT・PSIRT 活動に求められる事項（2-2 節）の調査と、製品提供企業やユーザ企業へのアンケート及びヒアリングにより、企業の状況や課題調査（2-3 節）を行い、CSIRT・PSIRT 活動のあり方に関する提言の指針とする。

2-2 CSIRT・PSIRT 活動に求められる事項

本節では、CSIRT 活動及び PSIRT 活動に関する文献を調査し、それぞれの活動に求められる事項の整理を行う。

2-2-1　調査対象の文献一覧

本調査項目において調査対象とする文献一覧を表 14 に示す。

表 14　CSIRT 活動及び PSIRT 活動に関する調査対象の文献一覧

種別	対象文書	発行機関	発行日	文書の概要
CSIRT	CSIRT ガイド[33]	一般社団法人 JPCERT コーディネーションセンター（以下 JPCERT/CC）[34]	2021 年 11 月	自組織の情報セキュリティ問題に対処するための CSIRT（組織内 CSIRT）を対象に、CSIRT のコンセプトと組織構造、活動内容について、説明している。
CSIRT	インシデントハンドリングマニュアル[35]	JPCERT/CC	2022 年 2 月	企業がインシデント対応マニュアルを作成するためのノウハウや、必要な記載事項、一般的なインシデント対応プロセスを記載している。
CSIRT	組織内 CSIRT 構築の参考資料　インシデント対応マニュアルの作成について[36]	JPCERT/CC	2015 年 11 月	組織内における「インシデント対応マニュアル」の作成を支援することを目的に、ノウハウや考察すべきポイントを記載している。

[33] 出典）JPCERT コーディネーションセンター（JPCERT/CC）
「CSIRT ガイド」
https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20211130.pdf
[34] 一般社団法人 JPCERT コーディネーションセンター
https://www.jpcert.or.jp/
[35] 出典）JPCERT コーディネーションセンター（JPCERT/CC）
「インシデントハンドリングマニュアル」
https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf
[36] 出典）JPCERT コーディネーションセンター（JPCERT/CC）
「組織内 CSIRT 構築の参考資料　インシデント対応マニュアルの作成について」
https://www.jpcert.or.jp/csirt_material/files/13_incident_response_manual_20211130.pdf

PSIRT	PSIRT Services Framework Version 1.1（日本語版）[37]	Forum of Incident Response and Security Team[38]（以下 FIRST） ※日本語訳は Software ISAC（一般社団法人コンピュータソフトウェア協会）、JPCERT/CC により作成	2022 年 11 月	PSIRT の組織構造や提供するサービスを整理したフレームワークであり、フレームワークでは６つのサービス（Service Area）と、それを実現するための「機能（Function）」が詳細に解説されている

2-2-2　組織構成及び外部連携のステークホルダ

本調査においては、サプライチェーンのセキュリティリスク対策を前提として、特に PSIRT 活動において求められる組織構成、外部連携のステークホルダを、前述の調査文献“PSIRT Service Framework”を参考に調査を行った。

まず PSIRT 活動において、連携が必要な内部ステークホルダについては、以下のように定義されている（図 4）。PSIRT 活動では、PSIRT 組織を中心として、「広報/コミュニケーションチーム/法務/政府関係対応部門」、「顧客サポート/セールス」、「エンジニア/開発部門」、「ビジネスライン/製品提供の管理部門」「企業経営者（経営層）」と、５つのセクションとの連携が求められている。各セクションにおいて必要な活動については、後述の 2-2-3 項で調査結果を掲載している。

[37] 出典）JPCERT コーディネーションセンター（JPCERT/CC）
「組織内 CSIRT 構築の参考資料　インシデント対応マニュアルの作成について」
https://www.jpcert.or.jp/csirt_material/files/13_incident_response_manual_20211130.pdf

[38] Forum of Incident Response and Security Team（FIRST）
https://www.first.org/

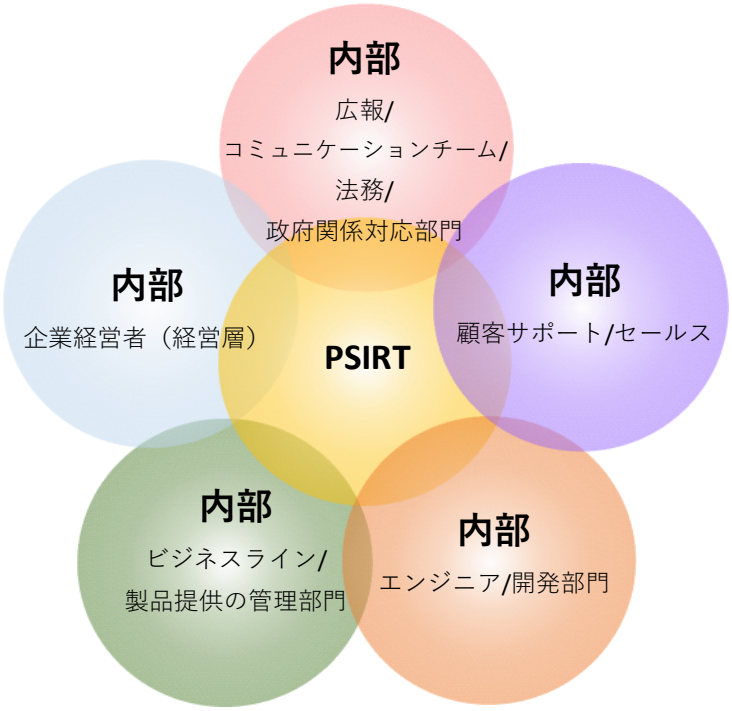


図 4　PSIRT における内部ステークホルダのマネジメント

出典）FIRST “PSIRT Service Framework Version1.1” Figure 6
https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf
を著者が日本語訳

次に PSIRT 活動において、連携が必要な外部ステークホルダについては、以下のように例が示されている（図 5)。PSIRT 組織を中心として、「他企業の PSIRT 群」、「CERT 機関（国内では JPCERT/CC に相当するコーディネーションセンター)」、「セキュリティ研究者」、「バグバウンティベンダ」、「協力関係にある CSIRT 群」、「サプライチェーンの上流（顧客)」、「サプライチェーン下流のコミュニティ」と合計 7 つの外部ステークホルダとの連携した対応が求められている。

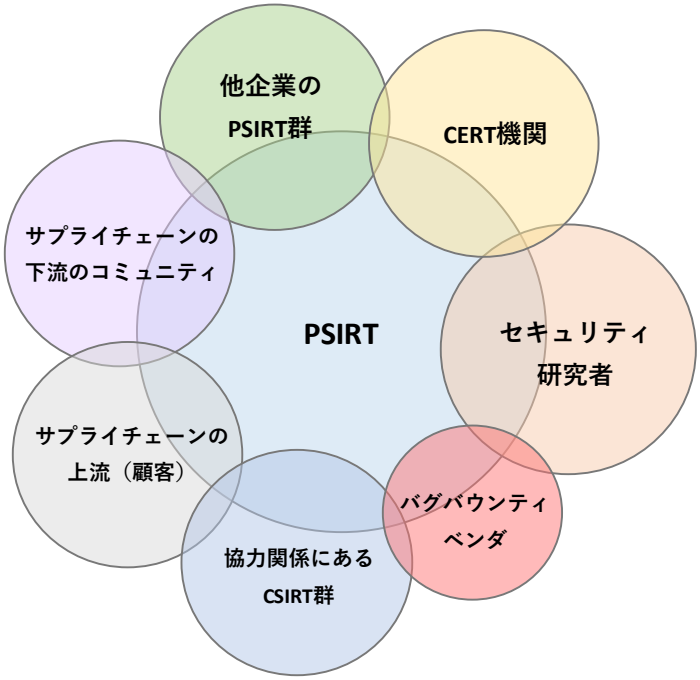


図 5　PSIRT における外部ステークホルダの例

出典）FIRST “PSIRT Service Framework Version1.1” Figure 7
https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf
を著者が日本語訳

2-2-3　CSIRT 及び PSIRT に求められる機能（サービス）

1）　CSIRT 活動に求められる機能（サービス）

本項では CSIRT 活動に求められる機能（サービス）について、前述の調査文献をもとに表 15 として整理を行った。CSIRT 活動の提供サービスは、JPCERT/CC「組織内 CSIRT 構築の参考資料　インシデント対応マニュアルの作成について」を参考に作成を行った。サービスの構成は「1.インシデントに対応する組織、発生前の準備」、「2.インシデントの発見及び報告」、「3.インシデント情報のトリアージと分析」、「4.インシデントの告知」、「5.インシデントの抑制措置と復旧」、「6.インシデントの事後対応」の 6 つのプロセスから構築される。また各プロセスの詳細については、上記資料に加え、JPCERT/CC の「CSIRT ガイド」、「インシデントハンドリングマニュアル」の内容を参考に、「関係するステークホルダ（内部・外部）」と「実施すべき活動（提供サービス）」に分類し、誰がどのような活動を行うべきか、各プロセスに求められるポイントを整理している。

表 15　CSIRT 活動に必要な提供サービス一覧

出典）JPCERT コーディネーションセンター（JPCERT/CC）
「組織内 CSIRT 構築の参考資料　インシデント対応マニュアルの作成について」
https://www.jpcert.or.jp/csirt_material/files/13_incident_response_manual_20211130.pdf
を参考に筆者が一部追記、修正を行った

1	**インシデントに対応する組織、発生前の準備**	
	関係するステークホルダ	[内部]経営層、IT 関連部署
		[外部]インシデント発見者、外部専門組織、顧客（提携先）、政府関係者
	実施すべき活動（提供サービス）	**①　インシデント対応に必要な連絡先の確保** ・インシデントの定義や想定外のインシデントに対して責任を持つ部門や担当者、また全体を統括する部門やチームを定義し、文書化する ・必要な内部、外部の連絡先を明確化し、連絡経路や手段を整備する
		②　各種規定文書や規則の把握と整合性の確認 ・組織内のインシデント対応活動に関する規定文書を調査し、文書や規則の相関関係を明確化する
		③インシデント対応の情報共有に有効なツールの整備 ・組織内の情報共有に必要なインフラやツール（もしくは他の代替手段）が確保する ・インシデントの発生に備え、事前に問題の発生を想定した教育やトレーニングを行う
2	**インシデントの発見及び報告**	
	関係するステークホルダ	[内部]経営層、IT 関連部署
		[外部]インシデント発見者、外部専門組織、顧客（提携先）

	実施すべき活動 （提供サービス）	**① インシデントの発見及びエスカレーションの仕組みの構築** ・インシデントを報告するための窓口（外部からの通報窓口を含む）を整備する ・報告を受けた場合の上位へのエスカレーションルールや判断基準（優先度）、インシデント対応の担当者など、必要な体制、仕組みを整備、文書化する
		② インシデントの検知に必要な装置や体制 ・インシデントの検知に必要な装置や体制が整備され、有効に活用できる状態を維持する 例1） 設置したセキュリティ機器やシステムによって異常を自組織内で検知する －侵入や改ざんの痕跡を調べるといったインシデントの検知に必要なチェック項目や、チェックの方法を明確化する －チェックの手順を自動化した「異常検知システム」を導入する場合は、誤検知を防ぐため、異常とみなす判断基準を明確化する 例2） 外部からの通報をもとにしてインシデントの発生を「検知=認知」する －インシデントが発生した外部（顧客や提携先など）から通報を受付可能な体制を整備する －外部の第三者やセキュリティベンダなどによる調査活動による通報を受付可能な体制を整備する ・最新の脆弱性や攻撃手法について、公開情報データベースや、マスメディア、カンファレンスなどを活用した情報の収集や共有を行う
3	インシデント情報のトリアージと分析	
	関係するステークホルダ	[内部]経営層、IT 関連部署
		[外部]インシデント発見者、外部専門組織、顧客（提携先）
	実施すべき活動 （提供サービス）	**① インシデント情報のトリアージ** ・インシデントの報告があった場合に、情報をトリアージするためのルール（対応すべきインシデントかどうか、情報の共有範囲、対応の優先度）を整備、文書化する ・対応すべきインシデントではないと判断した場合は、その判断の根拠を自組織の情報セキュリティポリシーに照らして可能な範囲で詳細に、報告者に回答する。 ・対応すべきインシデントであると判断した場合には、技術的な対応が可能か否かを判断する
		② インシデント対応の計画と実施 ・自組織での技術的対応が可能な場合は、主に IT 関連部署と連携し、対応計画を策定し、経営層や IT 関連部署と情報共有を行う ・自組織での技術的な対応が困難な場合は、主に経営層と連携し、対応計画を策定し、経営層や IT 関連部署と情報共有を行う
4	インシデントの告知	
	関係するステークホルダ	[内部]経営層、IT 関連部署

		[外部]インシデント発見者、外部専門組織、顧客（提携先）、政府関係者
	実施すべき活動 （提供サービス）	**①　インシデントの外部告知** ・インシデント発生の事実や対応状況について、外部への報告の要否、報告の対象（社会全体、所轄官庁、顧客、一般利用者など）、公開する情報の範囲、告知手段（Web サイト、マスメディアへのプレスリリース、記者会見など）について、判断を行う仕組みが整備、文書化する
5	**インシデントの抑制措置と復旧**	
	関係するステークホルダ	[内部]経営層、IT 関連部署
	実施すべき活動（提供サービス）	**①　インシデントの抑制措置** ・インシデントの被害を抑制するための措置について、その手段や実施機関、講じた措置によるビジネスへの影響を検討する仕組みを整備、文書化する ・抑制措置に対する最終的な意思決定者を明確に定義する ・業務時間外の意思決定と実施方法について定義する
		②　インシデントからの復旧 ・インシデントからの復旧について、組織の事業継続計画（BCP）との対応関係を明確化し、データなどの資産の一部損失も含めた復旧措置を検討する仕組みを整備、文書化する ・復旧計画に関する最終的な意思決定者を明確に定義する
6	**インシデントの事後対応**	
	関係するステークホルダ	[内部]経営層、IT 関連部署、組織内の従業員やスタッフ
	実施すべき活動 （提供サービス）	**①　インシデント復旧後のモニタリング** ・インシデント復旧後に、再発を防ぐためのモニタリングを実施し、表面的な問題の解決ではなく、本質的な問題の解決措置の検討を行える仕組みを整備する 例1）　マルウェアやワームの亜種による同様な感染発生を防止する仕組み 例2）　同じインシデント原因による他の資産への攻撃の可能性を防止する仕組みなど
		②　再発防止の情報共有と教育 ・同様なインシデントの再発防止のため、組織内にインシデント情報を共有する仕組みを整備する。 ・従業員やスタッフに対して、発生したインシデント事例を反映した情報セキュリティ教育の仕組みを整備、実施する

２）　PSIRT 活動に求められる機能（サービス）

本項では PSIRT 活動に求められる機能（サービス）について、前述の調査文献をもとに表 16 として整理を行った。PSIRT は対象となる活動の中心が製品のセキュリティとなり、図 6 に示すように 6 つのサービスエリアに分類されるサービスの提供が求められる。脆弱性やインシデントへの直接的な対応は、「脆弱性の発見（サービスエリア２）」、「脆弱性のトリアージと分析（サービスエリア３）」、「脆弱性の対策（サービスエリア４）」、「脆弱性の開示（サービスエリア５）」の４つのエリアで行われる。
この４つのエリアのサービスを円滑に行うために、それぞれのサービスに対応した、「ステークホルダのエコシステムマネジメント（サービスエリア１）」と「トレーニングと教育（サービスエリア６）」が求められる。

各サービスエリアにおける活動の詳細については、“PSIRT Service Framework”を参考に、「関係するステークホルダ（内部・外部）」と「実施すべき活動（提供サービス）」に分類し、誰がどのような活動を行うべきか、各サービスエリアに求められるポイントを整理している。

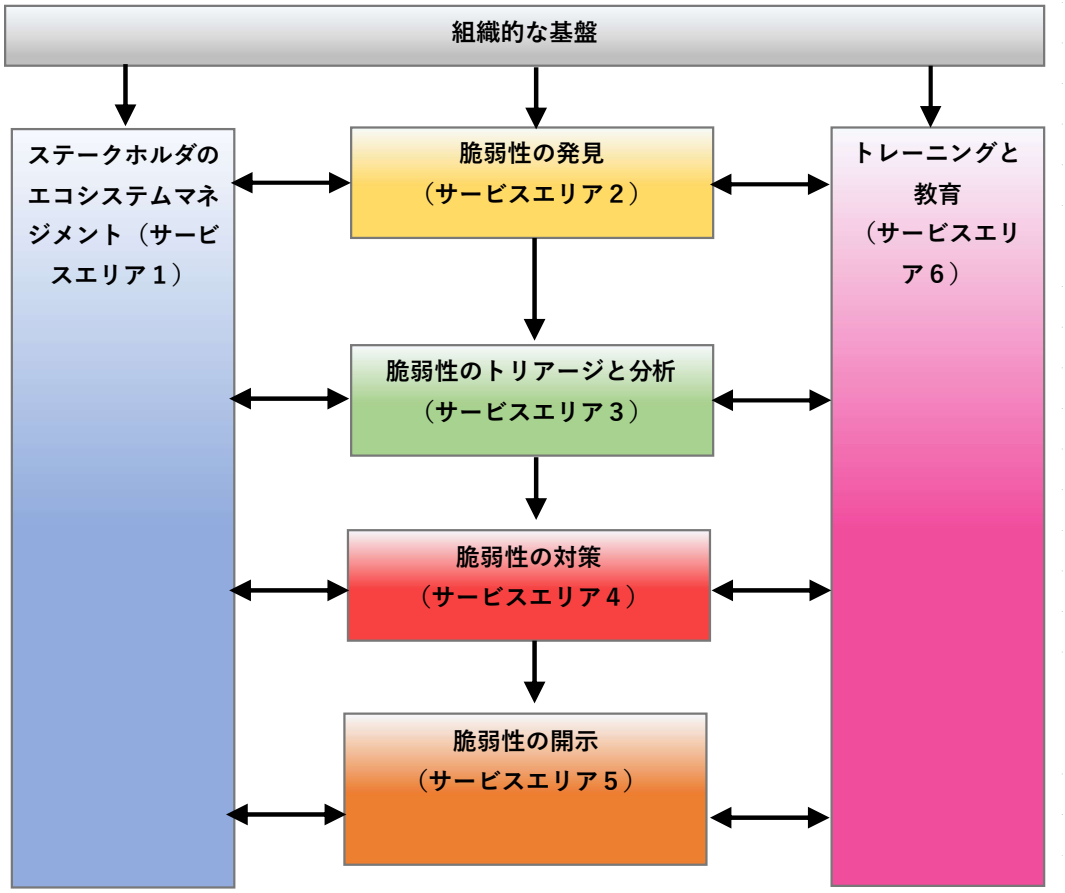


図 6　PSIRT における組織構造と提供サービス

出典）FIRST “PSIRT Service Framework Version1.1” Figure 1 を著者が日本語訳

表 16　PSIRT 活動に必要な提供サービス一覧

出典）FIRST「PSIRT Service Framework Version1.1 日本語版」
https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1_ja.pdf
をもとに筆者が要約
※日本語版は Software ISAC（一般社団法人コンピュータソフトウェア協会）、
JPCERT コーディネーションセンター（JPCERT/CC）が翻訳

1	**ステークホルダエコシステムマネジメント**	
1.1	**内部のステークホルダ管理**	
	関係するステークホルダ	[社内]経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
	実施すべき活動 （提供サービス）	**①関係する内部ステークホルダとのコミュニケーション** **②社内セキュア開発ライフサイクルの確認と調整** ・社内ワーキンググループ、SDL（セキュリティ開発ライフサイクル）活動、ガバナンスへの参画 **③インシデント事後対応プロセスの確立** ・脆弱性レビュープロセスの確立 ・インシデント発生後の対応プロセスを確立し、アップデートをリリースするタイミングを確認 ・注目すべきインシデントのレビュー
1.2	**発見者のコミュニティとの交流**	
	関係するステークホルダ	[社内]CSIRT、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]セキュリティベンダや研究者、セキュリティ課題の発見者（バグバウンティベンダなど）
	実施すべき活動 （提供サービス）	**①関係する社外のピア PSIRT（上流[39]、下流[40]企業の PSIRT など）の定義** **②脆弱性情報の協調的な開示プロセスの定義** **③安全なコミュニケーション経路の確立と管理（暗号化などによる保護対応）** **④関係する社外ステークホルダとのコミュニケーション** ・サプライチェーンにおける他企業（上流、下流）の PSIRT とのコミュニケーション及びプロセスの定義、文書化 ・セキュリティ研究者、セキュリティベンダ、バグバウンティベンダとのコミュニケーション及びプロセスの定義、文書化 **⑤CSIRT ニーズを予測する（CSIRT グループ固有の要求と観点を理解する）**
1.3	**コミュニティと組織の交流**	
	関係するステークホルダ	[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）

[39] 上流：自社製品に組込まれる部材やコンポーネント、ソリューションなどの調達先
[40] 下流：自社製品が、製品の一部として組込まれる場合の提供先など（顧客、一般消費者など）

	実施すべき活動 （提供サービス）	**①サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）の定義と文書化** **②上流、下流企業コミュニティ、パートナー（PSIRT 含む）とのコミュニケーション**
1.4	**下流のステークホルダマネジメント**	
	関係するステークホルダ	[社外]サプライチェーンにおける下流企業のコミュニティやパートナー（PSIRT 含む）
	実施すべき活動 （提供サービス）	**①ライフサイクルにおける相互サポートポリシーの確立及び、提供方法の定義**
1.5	**組織内でのインシデントに関するコミュニケーションの調整**	
	関係するステークホルダ	[社内]CSIRT、経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）
	実施すべき活動 （提供サービス）	**①内部や外部とのコミュニケーションチャネル（相互の窓口、連絡体制）の提供** **②安全なコミュニケーション経路の確立と管理（暗号化などによる保護対応）** **③製品の脆弱性をトラッキングするシステムのアップデート** ・製品のセキュリティ上の欠陥のトラッキングを提供 ・セキュリティ上の欠陥のトラッキングプロセスを作成、公開 **④情報の共有と公開** ・複数のコミュケーション窓口の提供とステークホルダへのフィードバック
1.6	**表彰と謝辞による報酬を発見者に与える**	
	関係するステークホルダ	[社外]セキュリティベンダや研究者、セキュリティ課題の発見者（バグバウンティベンダなど）
	実施すべき活動 （提供サービス）	**①バグバウンティ制度（脆弱性報奨プログラム）の実施** ・謝辞や報奨（報奨金やポイント制度など）の検討や策定、実施
1.7	**ステークホルダメトリクス**	
	関係するステークホルダ	[社内]CSIRT、経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）

	実施すべき活動 （提供サービス）	**①各ステークホルダの報告書の要件（PSIRT へのニーズや期待）を理解する** **②各ステークホルダのメトリクスの収集** ・PSIRT 活動の定量的な評価指標の定義や、評価結果の収集 **③メトリクスの分析** ・PSIRT 活動におけるデータ（評価結果）の傾向やパフォーマンスの分析 **④各ステークホルダへの報告** ・過去の活動の総括、課題や教訓による今後の課題や改善事項など
2	**脆弱性の発見**	
2.1	**脆弱性報告の受付**	
	関係するステークホルダ	[社内]CSIRT、経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）、セキュリティベンダや研究者、セキュリティ課題の発見者（バグバウンティベンダなど）
	実施すべき活動 （提供サービス）	**①製品のセキュリティ上の欠陥（脆弱性）に対する報告提出様式の定義** **②社外からの情報提供について、コンタクト先の詳細情報を公開する** **（製品マニュアル、ウェブサイトへの記載）** **③PSIRT 活動を内部の各部門（ステークホルダ）と連携させる** ・情報を受けられる体制を定義し、維持する（電話対応体制や 24 時間対応体制など）
2.2	**報告されない脆弱性を特定する**	
	関係するステークホルダ	[社内]CSIRT、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）、セキュリティベンダや研究者、セキュリティ課題の発見者（バグバウンティベンダなど）
	実施すべき活動 （提供サービス）	**①攻撃情報のデータベースを監視する** **②その他の脆弱性に関する情報のモニタリング** ・カンファレンスプログラム、高名な発見者による公開情報、マスメディアのリリース情報など
2.3	**製品コンポーネントの脆弱性のモニタリング**	
	関係するステークホルダ	[社内]CSIRT、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門

	実施すべき活動 （提供サービス）	**①製品を構成するコンポーネントリストの策定（ベンダ名、製品名、バージョンなどの情報）** **②コンポーネントに関する脆弱性情報のモニタリング** ・サードパーティベンダーのアドバイザリ情報の購入 ・NVD や商用のインテリジェンス情報（脆弱性データベース）の活用 ・サプライチェーン間で発見された脆弱性情報の共有　…など **③組織内の開発チームへのモニタリング情報への通知を確立**
2.4	**新しい脆弱性情報を見つける**	
	関係するステークホルダ	[社内]CSIRT、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
	実施すべき活動（提供サービス）	**①製品のセキュリティアセスメントの実施** ・脆弱性検出ツール、ペネトレーションテスティング技術による攻撃や、脆弱性の発見と解析 **②セキュリティテストツールに関する専門知識の維持** ・利用可能なツールに関する最新の知識の維持と、スタッフのトレーニング ・外部発見者からの報告の検証
2.4	**脆弱性発見のメトリクス**	
	関係するステークホルダ	[社内]CSIRT、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）
	実施すべき活動 （提供サービス）	**①運用レポートの提供** ・発見された脆弱性の総数と検証された脆弱性の総数 ・サードパーティ製コンポーネント毎に分類された検証済み脆弱性の総数 ・脆弱性発見のアプローチ毎に分類された発見された脆弱性の総数 ・情報ソース毎に分類された発見された脆弱性の総数 **②ビジネスレポートの提供** ・脆弱性のハンドリング対応の状況 ・オンタイム応答率（SLA の時間内での適時対応が行えたかどうか） ・報告受付からトリアージ完了までの時間 ・フルディスクロージャ、実際に攻撃に使用された脆弱性、メディアによって特定された脆弱性の数…など
3	**脆弱性情報のトリアージと分析**	
3.1	**脆弱性の認定**	
	関係するステークホルダ	[社内]CSIRT、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門

	実施すべき活動 （提供サービス）	**①製品における品質ゲート[41]とバグバー[42]を定義する。** ・品質ゲートとバグバーを定義し、社内ステークホルダ是認が閲覧可能な場所に保管する ・複数の製品や開発チームが存在する場合、開発関係者全員が関与する **②継続的改善を行う** ・受信レポートの件数、脆弱性として判定した件数、反映を受けていない報告件数、意見の相違などのデータを収集し、改善に活用する
3.2	**発見者との関係構築**	
	関係するステークホルダ	[社外]セキュリティベンダや研究者、セキュリティ課題の発見者（バグバウンティベンダなど）
	実施すべき活動 （提供サービス）	**①脆弱性を報告した個人及び組織のデータベースを作成、維持する** **②発見者のプロファイル（脆弱性を発見するための方法論、焦点を当てる製品/技術、インセンティブなど）を作成する** **③発見者のレポートの品質を定義** ・報告を受ける際の、脆弱性レポートのベースラインをガイドラインとして定義する
3.3	**脆弱性の再現**	
	関係するステークホルダ	[社内]CSIRT、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
	実施すべき活動 （提供サービス）	**①脆弱性の再現に関するサービスレベルアグリーメント（SLA）の設置** ・社内の技術的専門知識をもつ部門との社内調整を行う **②脆弱性の再現テストやツールなどの環境を用意する** ・発見者のレポートを検証するための専用テスト環境を用意する ・専用のネットワーク環境、シミュレータ、仮想化技術による安全な環境を構築する **③脆弱性情報を安全に保管する（参考 ISO27001 の参照）** **④再現確認において、影響を受ける製品（他の脆弱性のバリエーションも含めて）を判断する**
4	**脆弱性の対策**	
4.1	**対策リリースのマネジメント計画**	
	関係するステークホルダ	[社内]広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）

[41] 品質ゲート（クオリティゲート）　：　開発やリリースの次の段階に進む際に満たすべき基準のこと。
[42] バグバー（Bug Bars）：セキュリティ上の脆弱性として分類されるバグの種類を定義する基準のこと。

	実施すべき活動（提供サービス）	**①製品ライフサイクルの管理** ・社外ステークホルダと連携し、サポート範囲あるいはサポートから外れた製品の対応方針を決定する ・市場にリリースされている製品全ての製品リストを作成する（サポート期間についても管理） ・製品別に社外ステークホルダとのサポート契約を明確化する（有料サービス、延長保証、メンテナンスなど） **②アップデートの提供方法** ・対策ソフトの提供パッケージフォーマットの明確化（バイナリ実行形式、ソースコード差分の提供など） ・配布メカニズムの明確化（ホットフィックス、セキュリティパッチ、メンテナンスリリース、ファームウェアアップデートなど） ・対策の適用方法の明確化（リモートインストール、自動更新可否、オンサイト対応など） **③提供間隔や対策計画の明確化** ・例外ケースの文書化
4.2	**脆弱性の改善及び対策**	
	関係するステークホルダ	[社内]経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）

	実施すべき活動 （提供サービス）	**①分析** ・脆弱性に対する品質ゲートやバグバーの検証（脆弱性として取り扱わない基準の明確化） ・社外ステークホルダへのサポート契約の確認 ・脆弱性の原因、影響製品、バージョン、同時に対応すべき類似製品の特定 ・脆弱性の結果発生するリスクの軽減や対策方法、回避策の決定 ・脆弱性として取り扱わない基準の明確化、例外（対策できない脆弱性）の識別 **②対策の決定** ・対策を講じた製品の脆弱性の状況を検証する ・品質保証部門による対策の承認 ・対策の検証について、発見者、社外ステークホルダと協力する **③情報公開** ・社外ステークホルダと連携した対策及び、脆弱性情報の公開 ・対策を内部データベースに登録する **④リスクマネジメント** ・リスクを受け入れる権限を持つ役割の特定（CISO[43]、CSO[44]、リスクマネージャ） ・リスクマネジメントプロセスの定義 ・リスク評価と定量化 ・リスク登記簿の作成及び、調査結果や推奨事項の更新
4.3	**インシデントハンドリング**	
	関係するステークホルダ	[社内]経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
	実施すべき活動 （提供サービス）	**①緊急対応室の設立** ・PSIRT、法務、広報、開発、顧客サポート、サプライヤなどで構成される緊急対応室を設置する ・深刻な脆弱性の管理やインシデント対応を行う計画、リソース（人員、設備）、体制（役割、責任）を準備する **②インシデント管理** ・受信したインシデントの情報をカタログ化し保存する ・情報の分析（4.2 改善及び対策）を通じて、インシデントの影響を軽減、サービス対象の機能を回復させる ・インシデント解決までに取られたアクションを記録し、文書化する ・将来の危険を緩和、予防するため、プロセス、ポリシー、手順、リソース、およびツールの改善を検討する **③コミュニケーション計画**

[43] CISO：最高情報セキュリティ責任者
[44] CSO：最高セキュリティ責任者

		・内部ステークホルダへの情報公開用のリストを管理する ・公式の組織チャネルを通じてのみ、情報がステークホルダに展開されるようにする ・復旧のアクティビティを内部ステークホルダ（経営層、マネジメントチーム）へ伝達する ・PSIRT による説明会を実施し、事故後のインシデント対応や SDL 活動を改善するフィードバックを集める
4.4	**脆弱性リリースメトリクス**	
	関係するステークホルダ	[社内]経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
	実施すべき活動 （提供サービス）	**①運用レポートの提供** ・報告された脆弱性数と確認された脆弱性数（製品/事業単位別） ・サードパーティ製コンポーネント毎の脆弱性の数 ・確認された脆弱性の CWE による分類（製品/ 事業単位別） **②ビジネスレポートの提供** ・製品チームが SLA の時間枠内でどの程度影響評価を完了できたか ・製品チームが 指定された SLA 時間枠内でどの程度改修計画を提供できたか ・製品チームが SLA の時間枠内でどの程度修正プログラムを提供できたか ・製品チームがどの程度脆弱性報告から修正プログラムの提供までの全体的な目的や合意を満たしているか ・インシデントの数
5	**脆弱性の開示**	
5.1	**通知**	
	関係するステークホルダ	[社内]経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）、調整者（CERT/CC）
	実施すべき活動 （提供サービス）	**①中間ベンダ[45]（下流ベンダ）との連携** ・ステークホルダから脆弱性の報告を受けた場合、PSIRT から中間ベンダ（下流ベンダ）へ通知を行う ・中間ベンダ（下流ベンダ）が直接脆弱性の報告を受けた場合は、ベンダ企業の PSIRT へ通知を行う ・全ての中間ベンダ（下流ベンダ）を明確化し、法務部門を通じてタイムリーな

[45] 中間ベンダ（下流ベンダ）：OEM やパートナー企業、調達先など、他のベンダが出荷する製品の一部を開発・作成する企業。

		脆弱性対応の条項を契約に追記する **②調整者（コーディネータ）[46]との連携** ・調整者の特徴を把握（文書化）した上で連携を行い、影響を受ける全てのベンダ PSIRT へ脆弱性の通知を行う **③発見者との連携** ・「2　脆弱性の発見」に記載されている連絡手法を用いて、発見者による脆弱性の報告を受付可能とする
5.2	**調整**	
	関係するステークホルダ	[社内]経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）、調整者（CERT/CC）
	実施すべき活動 （提供サービス）	**①双方向の調整** ・発見者と協調して一般公表日程の調整など、情報開示を行う活動を推進する ・発見者へレポートの受領応答を返し、謝辞を述べる ・発見者に修正（ソフトウェア）を提供し、発見者が修正の検証を可能とする **②複数ベンダ間の調整** ・ベンダ PSIRT は、他ベンダや調整者から脆弱性レポートを受領した場合、受領の応答を返す ・ベンダ PSIRT や調整者は、報告された脆弱性の影響を受けるベンダを特定し、情報を共有する ・ベンダ PSIRT や調整者は、情報を共有するベンダ間で、対策情報を公開する時期や内容を調整する（下流ベンダが対策情報を受け取る方法を含む） ・ベンダ PSIRT や調整者は、他ベンダと連携し対策情報が適切であることを検証する。 ・ベンダ PSIRT や調整者は、脆弱性情報の公開時期、方法について関係ベンダと協議し、合意する
5.3	**情報開示**	
	関係するステークホルダ	[社内]経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
		[社外]サプライチェーンにおける上流、下流企業のコミュニティやパートナー（PSIRT 含む）

[46] 調整者（コーディネータ）：CERT Coordination Center（CERT/CC）やサードパーティなど、PSIRT から依頼を受け、ベンダへの通知やアドバイザリ公開のタイミングの調整を行う機関を指す。

	実施すべき活動 （提供サービス）	**①リリースノートの整備** ・リリースノートで開示する脆弱性を決定し、レビューのプロセスを定義する ・リリースノートのレビュー及び承認を行う **②公開ウェブサイトにセキュリティアドバイザリを掲載** ・セキュリティアドバイザリのテンプレートを定義し、提供する仕組み（RSS フィード、ウェブ）を定める ※アドバイザリはステークホルダやサービス対象者が自動化ツールで活用できるよう、CSAF など機解可読形式での提供を検討する ・セキュリティアドバイザリを発行する条件や、脆弱性に CVE 番号を割り当てる手順を定める ・アドバイザリの開示計画及び、レビュープロセスを定義する ・所定のステークホルダとアドバイザリをレビューする **③ナレッジベースの記事[47]の公開** ・どのような脆弱性をナレッジベースの記事にすべきか基準や、レビュープロセスを定義する ・記事のレビュー及び公開を承認する **④内部ステークホルダとのコミュニケーション** ・内部ステークホルダと連携し、脆弱性に関する顧客からの質問や回答（FAQ）を定め、レビューする
5.4	**脆弱性情報マネジメントの評価指標**	
	関係するステークホルダ	[社内]経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
	実施すべき活動 （提供サービス）	**①運用レポートの提供（経営層への情報提供）** ・セキュリティアドバイザリの公開数 ・NVD（公開脆弱性情報データベース） へ投稿した CVE の数 ・セキュリティアドバイザリへのアクセス数
6	**トレーニングと教育**	
6.1	**PSIRT のトレーニング**	
	関係するステークホルダ	[社内]PSIRT

[47] ナレッジベースの記事：重要度が低いアップデートや、却下した脆弱性に関する説明などの記事。

	実施すべき活動 （提供サービス）	**①技術的なトレーニング** ・サポートしている製品の基本的なセキュリティの概念と知識（定期的な資料のレビューと更新） **②コミュニケーショントレーニング** ・組織内ポリシーに従い社内及び社外ステークホルダとの円滑なコミュケーションを行うための方針理解 **③プロセスのトレーニング** ・報告された問題のトラッキング、管理、測定についてのプロセスガイドラインを定義する ・ガイドラインに基づき、セキュリティインシデント管理の情報フローを理解し、タイムリーな対応を可能とする **④タスクツールのトレーニング** ・組織内で認定されたバグトラッキングツールによる管理方法の理解 ・サードパーティ製のコンポーネント（OSS 含む）への適用と監視 **⑤トレーニングのトラッキング** ・定期的なトレーニングの実施状況をトラッキングする
6.2	**開発チームのトレーニング**	
	関係するステークホルダ	[社内]開発部門（エンジニア）
	実施すべき活動 （提供サービス）	**①PSIRT プロセスのトレーニング** ・適切なセキュアな開発ライフサイクル（SDL）の取り組みの理解（業界標準への適合など）※PSIRT 活動外だが必要なトレーニング ・PSIRT の目的、PSIRT 活動を支援するための製品開発の取り組みの理解
6.3	**検証チームのトレーニング**	
	関係するステークホルダ	[社内]開発部門（エンジニア）、品質保証部門（QA）
	実施すべき活動（提供サービス）	**①PSIRT プロセスのトレーニング** ・ペンテスト、脆弱性スキャン、ファジング、倫理的ハッキングなどの最新ツールと技術　※PSIRT 活動外だが必要なトレーニング ・PSIRT の目的、予想される時間的枠組み、PSIRT プロセスにおける診断や検証の役割などの理解
6.4	**すべてのステークホルダへの継続的な教育**	
	関係するステークホルダ	[社内]経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、営業部門、顧客サポート部門
		[社外]政府関係者

	実施すべき活動 （提供サービス）	**①PSIRT 活動におけるそれぞれの部門、ポジションの役割、責任を理解する** ・経営層のトレーニング ・法務チームのトレーニング ・政府関係（政策渉外）部門、コンプライアンスチームのトレーニング （企業コンプライアンスに関係する政府職員の連絡先を特定する） ・マーケティングチームのトレーニング ・広報チームのトレーニング ・営業チームのトレーニング ・サポートチームのトレーニング
6.5	**フィードバック機能の提供**	
	関係するステークホルダ	[社内]経営層、広報、法務部、開発部門（エンジニア）、品質保証部門（QA）、顧客サポート部門
	実施すべき活動 （提供サービス）	**①インシデントの根本原因を分析し、関係者の教育に活用、類似するインシデントの発生を防止する**

2-3　CSIRT・PSIRT 活動における企業の状況、課題調査

本節では IoT 機器の製品提供企業へのアンケート、ヒアリング調査を実施し、その結果をもとに CSIRT・PSIRT 活動における企業の状況や課題の分析を行う。

2-3-1　　調査の方針、前提

本章の企業における状況、課題調査は、アンケートシートの回収による一次調査と、各社へのヒアリングによる二次調査の 2 段階で実施した。ヒアリング調査では、アンケート回答結果の不明点や、より詳細な導入事例などを個別に確認している。調査は、5 製品分野より計 5 社（計 9 部門）を対象に実施（表 17）し、アンケート項目は下記の A～D の 4 分類、計 63 問で構成した（表 18）。

表 17　調査対象の製品分野及び企業・部門数

製品分野	調査対象企業・部門数
決済端末分野	1 社（計 1 部門）
金融端末分野	1 社（計 2 部門）
住設機器分野	1 社（計 2 部門）
情報システム機器分野	1 社（計 2 部門）
情報家電分野	1 社（計 2 部門）
合計	5 社（9 部門）

表 18　アンケート項目一覧

分類		アンケート項目		策定項目数
A	CSIRT・PSIRT の組成状況	A-1	CSIRT・PSIRT（もしくはそれに準ずる組織）の組成状況	全 10 問
		A-2	CSIRT・PSIRT の組成時期及び活動期間	
		A-3	現状の CSIRT、PSIRT の組織人員、体制	
B	CSIRT・PSIRT の活動状況について	B-1	CSIRT の運用状況	全 45 問
		B-2	PSIRT の運用状況	
		B-3	インシデントや脆弱性の外部ステークホルダへの報告タイミング	
		B-4	CSIRT・PSIRT の連携について（PSIRT 部門）	
		B-5	インシデント・脆弱性に関係する外部組織との連携状況（PSIRT 部門）	
C	CSIRT・PSIRT の有効性	C-1	CSIRT 活動の有効性について	全 8 問
		C-2	PSIRT 活動の有効性について	
D	CSIRT・PSIRT における課題	D-1	体制（人材）、管理運用面における課題（CSIRT・PSIRT 部門）	全 5 問
		D-2	CSIRT・PSIRT 及び外部機関との連携における課題（PSIRT 部門）	
合計				全 63 問

2-3-2　企業における活動状況、課題調査結果

1）　　企業における活動状況、課題調査結果一覧

本項では、企業別に実施した一次調査、二次調査の結果を一覧として示す。以下の結果一覧では、全体

の傾向を分かりやすく可視化することを目的に、過半数を越える回答及び、同じ項目内で比較的割合が高い回答を色付けして区別を行っている。

A）CSIRT・PSIRT の組成状況

調査対象企業に対して実施した「CSIRT・PSIRT の組成状況」に関する調査結果を表 19 に示す。

表 19　CSIRT・PSIRT の組成状況に関する調査結果一覧

ID		アンケート項目	回答項目	回答割合
A-1	A-1-1	CSIRT の組成状況	a）CSIRT あるいは、それに準ずる目的の組織が企業内に構成されている。	80%
			b）CSIRT あるいは、それに準ずる目的の組織は社内にない。	20%
		PSIRT の組成状況	c）PSIRT あるいは、それに準ずる目的の組織が企業内に構成されている。	100%
			d）PSIRT あるいは、それに準ずる目的の組織は社内にない。	0%
A-2	A-2-1	CSIRT の活動期間	a）3 年未満	0%
			b）3 年以上～5 年以下	25%
			c）5 年以上	75%
		PSIRT の活動期間	a）3 年未満	0%
			b）3 年以上～5 年以下	40%
			c）5 年以上	60%
A-3	A-3-1	CSIRT の構成人数	a）5 名未満	0%
			b）5 名～10 名	50%
			c）10 名以上	50%
		PSIRT の構成人数	a）5 名未満	20%
			b）5 名～10 名	0%
			c）10 名以上	80%
	A-3-2	CSIRT の体制	a）CSIRT は、専任の役割を担当する要員を中心に対応を行っている。	25%
			b）CSIRT は、専任の役割を担当する要員を中心に、一部を他の事業部の要員が兼任し、対応を行っている。	25%
			c）CSIRT は、中心となる構成メンバーが他の事業部と兼任で対応を行っている。	50%
		PSIRT の体制	a）PSIRT は、専任の役割を担当する要員を中心に対応を行っている。	0%
			b）PSIRT は、専任の役割を担当する要員を中心に、一	40%

ID		アンケート項目	回答項目	回答割合
			部を他の事業部の要員が兼任し、対応を行っている。	
			c）PSIRT は、中心となる構成メンバーが他の事業部と兼任で対応を行っている。	60%
	A-3-3	CSIRT の担当部門（複数回答可）	情報システム部門	100%
			管理部門	25%
			製品の開発部門	0%
			製品の顧客サポート部門	0%
			品質管理部門	0%
			その他	0%
			特に兼任する担当部門は決まっていない。	0%
			[その他回答内容] ※特になし	
		PSIRT の担当部門（複数回答可）	情報システム部門	40%
			管理部門	0%
			製品の開発部門	40%
			製品の顧客サポート部門	0%
			品質管理部門	80%
			その他	20%
			特に兼任する担当部門は決まっていない。	0%
			[その他回答内容] ・社長直轄の組織として組成されている。	

B）CSIRT・PSIRT の活動状況、連携の状況

調査対象企業に対して実施した「CSIRT・PSIRT の活動状況」に関する調査結果を表 20 に示す。

本調査では、現在の CSIRT・PSIRT 活動への対応状況について、それぞれ 5 段階評価で各社より回答を得た。（５：対応できている、４：どちらかと言えば対応できている、３：どちらとも言えない、２：どちらかと言えば対応できていない、１：対応できていない）

なお、本調査では CSIRT、PSIRT 活動のあるべき姿と、企業の活動実態とのギャップ分析を行うことを目的とし、以下の文献の調査結果をもとに、それぞれの活動に必要な事項をアンケート項目として抽出した。（詳細については表 14「CSIRT 活動及び PSIRT 活動に関する調査対象の文献一覧」参照）

・CSIRT :「組織内 CSIRT 構築の参考資料 インシデント対応マニュアルの作成について」をベースに、「CSIRT ガイド」、「インシデントハンドリングマニュアル」より補足

・PSIRT :「PSIRT Services Framework Version 1.1」

表 20　CSIRT・PSIRT の活動状況に関する調査結果一覧

５：対応できている、４：どちらかと言えば対応できている、３：どちらとも言えない、

２：どちらかと言えば対応できていない、１：対応できていない

ID		アンケート項目	回答項目	評価値	割合
CSIRT の活動状況					
B-1	B-1-1	インシデントに対応する組織、発生前の準備	①インシデントの定義や想定外のインシデントに対して責任を持つ部門や担当者、また全体を統括する部門やチームが明確化され、連絡先や連絡経路の整備や文書化は行われていますか。	5	75%
				4	25%
				3	0%
				2	0%
				1	0%
			②組織内の情報共有に必要なインフラやツール（もしくは他の代替手段）が確保され、運用に必要なプロセスの整備や文書化は行われていますか。	5	100%
				4	0%
				3	0%
				2	0%
				1	0%
			③インシデントの発生に備え、事前に問題の発生を想定した教育やトレーニングは、定期的に行われていますか。	5	75%
				4	25%
				3	0%
				2	0%
				1	0%
	B-1-2	インシデントの発見、報告	①インシデントを報告するための窓口（外部からの通報窓口を含む）や、報告を受けた場合の上位へのエスカレーションルールや判断基準など、組織内の報告に必要な仕組みが整備、文書化されていますか。	5	100%
				4	0%
				3	0%
				2	0%
				1	0%
			②インシデントの検知に必要な装置や体制が整備され、有効に活用できる状態が維持されていますか。	5	100%
				4	0%
				3	0%
				2	0%
				1	0%
			③最新の脆弱性や攻撃手法について、公開情報データベースや、マスメディア、カンファレンスなどを活用した情報の収集や共有は行われていますか。	5	50%
				4	50%
				3	0%
				2	0%
				1	0%
	B-1-3	インシデント情報のトリアージと分析	①インシデントの報告があった場合に、情報をトリアージするためのルール（対応すべきインシデントかどう	5	50%
				4	50%

ID		アンケート項目	回答項目	評価値	割合
			か、情報の共有範囲、対応の優先度）は整備、文書化されていますか。	3	0%
				2	0%
				1	0%
			②インシデントの情報（種類、発生原因、日時、影響など）や行われた対応を記録し、責任の明確化や今後の分析が可能なように、記録の保持、管理が実施されていますか。	5	75%
				4	25%
				3	0%
				2	0%
				1	0%
	B-1-4	インシデントの告知	①インシデント発生の事実や対応状況について、外部への報告の要否、報告の対象（社会全体、所轄官庁、顧客、一般利用者など）、公開する情報の範囲、告知手段（Webサイト、マスメディアへのプレスリリース、記者会見など）について、判断を行う仕組みが整備されていますか。	5	50%
				4	25%
				3	25%
				2	0%
				1	0%
	B-1-5	インシデントの抑制措置と復旧	①インシデントの被害を抑制するための措置について、その手段や実施機関、講じた措置によるビジネスへの影響を検討する仕組みが整備されていますか。また、抑制措置に対する最終的な意思決定者は明確に定義されていますか。	5	0%
				4	50%
				3	25%
				2	25%
				1	0%
			②インシデントからの復旧について、組織の事業継続計画（BCP）との対応関係を明確化し、データなどの資産の一部損失も含めた復旧措置を検討する仕組みが整備されていますか。また復旧計画に関する最終的な意思決定者は明確に定義されていますか。	5	0%
				4	75%
				3	0%
				2	25%
				1	0%
	B-1-6	インシデントの事後対応	①インシデント復旧後に、再発を防ぐためのモニタリングが実施され、表面的な問題の解決ではなく、本質的な問題の解決措置の検討を行える仕組みが整備されていますか。 例） ・マルウェアやワームの亜種による同様な感染発生を防止する仕組み ・同じインシデント原因による他の資産への攻撃の可能性を防止する仕組みなど	5	50%
				4	25%
				3	25%
				2	0%
				1	0%
			②同様なインシデントの再発防止のため、組織内にインシデント情報を共有する仕組みや、従業員やスタッフに対する情報セキュリティ教育が整備され、実施されていますか。	5	50%
				4	50%
				3	0%
				2	0%

ID		アンケート項目	回答項目	評価値	割合
				1	0%
	B-1-7	御社における CSIRT 活動について、上記全体を通して特に課題であるとお考えの部分があれば、ご回答ください（自由記述）	[自由記述回答内容] ※特になし		
PSIRT の活動状況					
B2	B-2-1	ステークホルダのエコシステムマネジメント	①PSIRT において、社内関係部門と連携し活動する仕組みや体制は整備、文書化されていますか。 ※社内関係部門は、経営層、広報、法務部、開発エンジニア、顧客サポート部門などを想定しています。	5	40%
				4	40%
				3	20%
				2	0%
				1	0%
			②外部組織と定期的に PSIRT 活動に関するコミュニケーションを行う場が設定されていますか。 ※社外組織は、サプライチェーンにおいて提携している他企業の PSIRT や、ISAC 機関、オープンソースコミュニティ、セキュリティベンダなどの有識者を想定しています。	5	0%
				4	60%
				3	0%
				2	20%
				1	20%
			③PSIRT の活動の実施状況や成果を評価する指標や仕組みがあり、社内へ定期的な報告や情報共有は行われていますか。	5	20%
				4	0%
				3	80%
				2	0%
				1	0%
	B-2-2	脆弱性の発見	①脆弱性が発見された場合に情報を伝達するため、社内及び、社外ステークホルダの連絡先や経路、報告の様式など、必要な仕組みが整備、文書化されていますか。	5	60%
				4	20%
				3	20%
				2	0%
				1	0%
			②報告や情報伝達の際に、安全な経路（暗号化など）は確立されていますか。	5	40%
				4	60%
				3	0%
				2	0%
				1	0%
			③最新の脆弱性や攻撃手法について、公開情報データベースや、マスメディア、カンファレンスなどを活用した情報の収集や共有は行われていますか。	5	40%
				4	40%
				3	20%

ID		アンケート項目	回答項目	評価値	割合
				2	0%
				1	0%
			④製品に使用されているソフトウェアコンポーネントのリスト（SBOM あるいはその他の方式による）について、継続的な管理や更新は、PSIRT 活動と連携して行われていますか。	5	20%
				4	0%
				3	60%
				2	0%
				1	20%
			⑤公開されていない脆弱性について、製品へのセキュリティテストなどによる発見の仕組みは整備されていますか。	5	40%
				4	0%
				3	0%
				2	40%
				1	0%
			⑥自社製品の脆弱性が発見された場合に、社外（発見者など）からの報告を受け取る仕組みは整備されていますか。	5	60%
				4	20%
				3	20%
				2	0%
				1	0%
	B-2-3	脆弱性情報のトリアージと分析	①収集あるいは報告された脆弱性や攻撃手法について、製品への影響や再現性をテストするための方法や環境の整備が行われていますか。	5	20%
				4	20%
				3	60%
				2	0%
				1	0%
			②製品のセキュリティに影響する脆弱性の定義や、セキュリティ開発ライフサイクル（SDL）におけるセキュリティ要求事項は文書化されていますか。	5	60%
				4	0%
				3	40%
				2	0%
				1	0%
			③報告、発見された製品の脆弱性に対して、作りこみの原因や、製品への影響、対策（回避策）の分析、優先度（対応しない場合を含む）を決定する仕組みは整備、文書化されていますか。	5	20%
				4	20%
				3	60%
				2	0%
				1	0%
	B-2-4	脆弱性の改善と対策	①製品ライフサイクルにおいて、脆弱性が発見された場合に、タイムリーな対策を行うプロセスや手順は、整備、文書化されていますか。	5	20%
				4	40%
				3	40%
				2	0%

ID		アンケート項目	回答項目	評価値	割合
				1	0%
			②脆弱性が製品や企業に与えるリスクについて、リスク評価（定量化）やリスクマネジメントのプロセスは整備、文書化されていますか。	5	40%
				4	40%
				3	0%
				2	20%
				1	0%
			③インシデント発生時の対応について、社内の緊急対応室（あるいはそれに準ずる組織）が設置され、対応方針が整備、文書化されていますか。その方針にはサプライチェーン上のステークホルダへの対応についても定義されていますか。	5	40%
				4	0%
				3	60%
				2	0%
				1	0%
			④報告、発見された脆弱性の件数や CWE 分類、対策の状況などが記録として整備、管理され、事後の分析や追跡に利用できる形式になっていますか。	5	0%
				4	0%
				3	60%
				2	40%
				1	0%
	B-2-5	脆弱性の開示	①製品の脆弱性が報告、発見された場合に、サプライチェーン上のステークホルダに対して、速やかに情報を伝達する仕組みが整備されていますか。	5	40%
				4	40%
				3	20%
				2	0%
				1	0%
			②製品の脆弱性の情報公開において、リリースノートの作成や情報の公開範囲や内容の事前レビュー、社内関係部門との連携など、計画的な対応が可能な形式として整備されていますか。	5	40%
				4	0%
				3	60%
				2	0%
				1	0%
	B-2-6	トレーニングと教育	①PSIRT 活動において、社内関係部門毎に責任や役割分担に基づく教育やトレーニングの方針が整備、文書化され、定期的な教育・トレーニングが実施されていますか。。 ※社内関係部門は、経営層、広報、法務部、開発エンジニア、顧客サポート部門などを想定しています。	5	0%
				4	0%
				3	20%
				2	60%
				1	20%
			②PSIRT 活動に関連する技術的な内容について、教育やトレーニングの方針が整備、文書化され、定期的な教育・トレーニングが実施されていますか。。 ※PSIRT 活動に関連する技術的な内容は、脆弱性の分析	5	0%
				4	0%
				3	20%
				2	40%

ID		アンケート項目	回答項目	評価値	割合
			や再現テストの方法、情報のトラッキングや管理のためのツールや環境の利用手順などを想定しています。	1	40%
	B-2-7	御社における PSIRT 活動について、上記全体を通して特に課題であるとお考えの部分があれば、ご回答ください（自由記述）	[自由記述回答内容] ・2022 年下期より活動開始のため、会社的な対応整備はこれからの状況。（主に「どちらとも言えない」で回答）各プロジェクト／製品毎には対応出来ているものもある。 ・脆弱性が発見された場合、可用性の担保とセキュリティ対策のバランスが難しい。また対策実施をした際、対策済みか否かの管理や、対策の代替手段の管理や運用が難しくなりそうであること。また、構成管理に関して、実施したセキュリティ対策のパラメータ管理や IT 化など、その運用が難しい。		

調査対象企業に対して実施した「CSIRT・PSIRT の連携状況」に関する調査結果を表 21 に示す。

表 21　CSIRT・PSIRT の連携状況に関する調査結果一覧

ID		アンケート項目	回答項目	回答割合
B-3	B-3-1	CSIRT における外部ステークホルダへのインシデント報告タイミング	a）外部ステークホルダへの報告は、インシデント発生後、いつまでに報告を完了すべきか対応期限が定義され、タイムリーな報告が行えるようになっている。	50%
			b）外部ステークホルダへの報告について、インシデント発生後の報告期限は特に定義されていないが、インシデントの状況や報告すべき対象者に応じて、報告のタイミングを検討する仕組みとしている。	50%
			c）原則として、自主的なインシデントの報告は行わず、外部ステークホルダからの問い合わせに応じて、対応を行う仕組みとしている。	0%
			d）上記以外の対応方針を定めている場合には、下記に対応内容の概要をご記載ください。	0%
			[d）その他回答内容（自由記述）] ※特になし	
	B-3-2	PSIRT における外部ステークホルダへの脆弱性情報の報告タイミング	a）外部ステークホルダへの報告は、脆弱性の検出後、いつまでに報告を完了すべきか対応期限が定義され、タイムリーな報告が行えるようになっている。	0%
			b）外部ステークホルダへの報告について、脆弱性の検出後の報告期限は特に定義されていないが、インシデントの状況や報告すべき対象者に応じて、報告のタイミングを検討する仕組みとしている。	80%

ID		アンケート項目	回答項目	回答割合
			c）原則として、自主的な脆弱性検出の報告は行わず、外部ステークホルダからの問い合わせに応じて、対応を行う仕組みとしている。	20%
			d）上記以外の対応方針を定めている場合には、下記に対応内容の概要をご記載ください。	0%
			[d）その他回答内容（自由記述）] ※特になし	
B-4	B-4-1	自社における CSIRT と PSIRT の連携について	a）CSIRT 活動で得られたインシデントや脆弱性などの情報は、定期的に PSIRT へ共有され、自社製品への影響分析を経て、品質向上に活用されている。	20%
			b）CSIRT 活動で得られたインシデントや脆弱性などの情報は、PSIRT へ共有されているが、自社製品への影響分析や、品質向上には、あまり活用されていない。	40%
			c）CSIRT 活動で得られたインシデントや脆弱性などの情報は、PSIRT へと共有されていない。	40%
	B-4-2	サプライチェーン間の PSIRT 連携について（複数回答可） ■下流企業（ユーザ企業など）から自社への情報共有について	a）サプライチェーン下流企業（＝ユーザ企業などの顧客）が収集したインシデント（脆弱性情報）は、定期的に自社の PSIRT（あるいは開発部門）に情報共有されている。	0%
			b）サプライチェーン下流企業（＝ユーザ企業などの顧客）が収集したインシデント（脆弱性情報）は、自社の PSIRT（あるいは開発部門）に情報共有されておらず、問題が発生した場合にのみ、問い合わせが発生する。	100%
		サプライチェーン間の PSIRT 連携について（複数回答可） ■自社から上流企業（調達先など）への情報共有について	c）自社製品において検出あるいは報告された脆弱性情報は、ソフトウェアコンポーネントのリスト（SBOM あるいはその他の方式による）で影響箇所を特定し、サプライチェーン上流企業（＝ソフトウェアの委託先、調達先）の PSIRT（あるいは開発部門）へ情報を共有している。	0%
			d）自社製品において検出あるいは報告された脆弱性情報は、影響箇所を特定する前に、まずはサプライチェーン上流企業（＝ソフトウェアの委託先、調達先）の PSIRT（あるいは開発部門など）へ情報を共有している。	80%
			e）自社製品において検出あるいは報告された脆弱性情報は、原則として自社内で対応する仕組みとしており、	20%

ID		アンケート項目	回答項目	回答割合
			サプライチェーン上流（＝ソフトウェアの委託先、調達先）企業の PSIRT（あるいは開発部門など）への情報共有は行っていない。※あるいは情報を共有する場合にも、脆弱性対応が完了した後、実施している。	
		サプライチェーン間の PSIRT 連携について（複数回答可） ■上流企業（調達先など）から自社への情報共有について	f）サプライチェーン上流企業（＝ソフトウェアの委託先、調達先）で検出あるいは報告された脆弱性情報は、自社の PSIRT（あるいは開発部門など）へ情報が共有されている。	80%
			g）サプライチェーン上流企業（＝ソフトウェアの委託先、調達先）で検出あるいは報告された脆弱性情報は、特に自社の PSIRT（あるいは開発部門など）への情報共有が行われていない。	20%
		サプライチェーン間の PSIRT 連携について（複数回答可） ■その他 PSIRT 連携について	h）上記 a～g 以外の方法で、PSIRT 間で連携を行っている。	20%
			[h）上記以外の対応例] 親会社が定期配信している脆弱性情報を活用して情報を共有している。	
	B-4-3	上記 B-4-2 に関連し、「CSIRT と PSIRT の連携」あるいは「サプライチェーン間の PSIRT 連携」について、過去に対応を行い、効果的な解決につながった事例、あるいは問題が発生した事例があれば、差支えがない範囲で、ご回答ください。	[課題・事例の自由記述内容] ・海外では組織が小さいために、社内イントラと社外サービスの狭間に落ちるようなシステムの問題対処を共同で行っているほか、お互いに情報共有を行い、多角的に対策を検討している。	
B-5	B-5-1	インシデント・脆弱性に関係する外部組織との連携状況について	a）製品の脆弱性情報について報告が必要と判断される場合には、IPA の脆弱性報告窓口を通じて、JPCERT/CC へ報告を行っている。	80%
			b）製品の脆弱性情報について情報の共有が必要と判断される場合には、業種別の ISAC 組織へ、情報の共有を行っている。	0%
			c）所属している OSS コミュニティにて、インシデントや脆弱性の事例及び、対応事例の情報共有を行っている。	0%
			d）情報の発信については、積極的に行っていないが、	0%

ID		アンケート項目	回答項目	回答割合
			バグバウンティ制度（セキュリティ課題の報告に対する報奨金や表彰制度など）を設定し、セキュリティ課題の情報収集を積極的に行っている。	
			E）a～d に該当する連携は行っていない。	20%
	B-5-2	上記 a～d に該当する過去の事例、あるいはそれ以外の方法で外部機関とインシデントや脆弱性を情報連携した事例があれば、自由記述にてご回答ください。	[上記以外の情報連携事例] ・過去の事例ではないが、外部連携する場合には、まず、親会社のセキュリティ管理部署に連絡を取り、そこと連携しながら外部組織との情報共有を行うことになる。	

C）CSIRT・PSIRT の有効性

調査対象企業に対して実施した「CSIRT・PSIRT の有効性」に関する調査結果を表 22 に示す。

本調査では、各調査対象企業における CSIRT・PSIRT 活動の経験を通じて、CSIRT や PSIRT が各項目の目的に対して効果的な手段であると考えられるかについて、それぞれ 5 段階評価で各社より回答を得た。（５：効果的である、４：どちらかと言えば効果的である、３：どちらとも言えない、２：どちらかと言えば効果的とは言えない、１：効果的とは言えない）

表 22　CSIRT・PSIRT の有効性に関する調査結果一覧

５：効果的である、４：どちらかと言えば効果的である、３：どちらとも言えない、
２：どちらかと言えば効果的とは言えない、１：効果的とは言えない

ID		アンケート項目	回答項目	評価値	割合
C-1	C-1-1	CSIRT 活動の有効性について	インシデント情報の収集や検出への効果	5	50%
				4	50%
				3	0%
				2	0%
				1	0%
			インシデントの再発防止効果	5	100%
				4	0%
				3	0%
				2	0%
				1	0%
			社内のセキュリティ教育への効果	5	75%
				4	25%
				3	0%
				2	0%

ID		アンケート項目	回答項目	評価値	割合
				1	0%
	C-1-2	PSIRT 活動の有効性について	脆弱性情報の収集や検出への効果	5	80%
				4	20%
				3	0%
				2	0%
				1	0%
			自社の製品開発におけるセキュリティ開発プロセスの向上効果	5	60%
				4	20%
				3	20%
				2	0%
				1	0%
			サプライチェーンの上流（＝ソフトウェアの委託先や調達先）へのセキュリティ品質管理の徹底効果	5	20%
				4	20%
				3	60%
				2	0%
				1	0%
			サプライチェーンの下流（＝ユーザ企業などの顧客、一般消費者）に対するセキュリティ品質の向上効果	5	20%
				4	20%
				3	60%
				2	0%
				1	0%
			製品開発上のセキュリティ教育への効果	5	60%
				4	20%
				3	20%
				2	0%
				1	0%

D）CSIRT・PSIRT における課題

調査対象企業に対して実施した「CSIRT・PSIRT の課題」に関する調査結果を表 23 に示す。

表 23　CSIRT・PSIRT の課題に関する調査結果一覧

ID		アンケート項目	回答項目	回答割合
D-1	D-1-1	CSIRT の体制（人材）、管理運用面における課題（複数回答可）	a）CSIRT の活動、運用に必要な人材の確保が難しい。	75%
			b）CSIRT 活動全般に掛かるコスト（人件費、インフラ費など）が大きな負担となっている。	0%
			c）現在運用している CSIRT 活動の対応プロセスが妥	0%

ID		アンケート項目	回答項目	回答割合
			当かどうか、懸念がある。	
			d) インシデントの監視に利用するシステムの導入、維持、運用に高いコストが発生している。	50%
			e) インシデントの監視に利用するシステムの性能や効果に不満がある。	0%
			f) インシデントの情報収集の仕組みに課題があり、情報の鮮度や粒度が必要な水準に達していない。	0%
			g) 対応すべきインシデントかどうかの判断やトリアージ（優先度設定）の判断が難しい。	25%
			h) インシデント発生時の抑制や復旧措置に、技術的あるいは運用上の課題がある。	25%
			i) 上記以外のその他の課題	0%
	D-1-2	PSIRT の体制（人材）、管理運用面における課題 （複数回答可）	a) PSIRT の活動、運用に必要な人材の確保が難しい。	80%
			b) PSIRT 活動全般に掛かるコスト（人件費、インフラ費など）が大きな負担となっている。	20%
			c) 現在運用している PSIRT 活動の対応プロセスが妥当かどうか、懸念がある。	0%
			d) ソフトウェアコンポーネントのリスト管理に、技術的あるいは運用上の課題がある。	40%
			e) ソフトウェアの委託先、調達先のセキュリティ対策が、必要な水準に達していない。	0%
			f) 脆弱性や攻撃手法の情報収集の仕組みに課題があり、情報の鮮度や粒度が必要な水準に達していない。	40%
			g) 対応すべき脆弱性の判断やトリアージ(優先度設定)の判断が難しい。	40%
			h) 発見された脆弱性の対応において、製品に含まれるソフトウェア（OSS,サードパーティ製）側の対策や置換に、技術的あるいは運用上の課題がある。	40%
			i) 上記以外のその他の課題	20%
			[i) 上記以外の課題（自由記述）] ・製品製造後の保守体制の維持	
	D-1-3	D-1-1～2 において課題としてチェックいただいた項目について、その理由や具体的な事例を差支えのない範囲でご回答ください。（自由記述）	[自由記述内容] ・組込み機器の場合、OS の設定情報の管理に課題がある。例えば、OS の場合、ソフトウェア名称やバージョンよりも、OS 設定情報の方が遙かに項目が多く、その管理が難しいこと。また、脆弱性の影響評価についても、ソフトウェアのバージョンチェックだけでなく、OS のハードニングレベルで大丈夫なのか、ソースコードまで見ないといけ	

ID		アンケート項目	回答項目	回答割合
		※CSIRT、PSIRT どちらの部門の方も回答をお願い致します。	ないかによって、調査工数が大きく変わり、全てが調べられないため、工数と費用の懸案がある。 ・古い製品はベース OS のバージョンが古く利用できない。また古い製品は開発環境がない点にも課題がある。	
D-2	D-2-1	CSIRT・PSIRT 及び外部機関との連携における課題（PSIRT 部門） （複数回答可）	a）CSIRT で収集したインシデント情報は、対象製品の違いなどの理由により、PSIRT ではあまり有効活用できない。	20%
			b）CSIRT で取集したインシデント情報を PSIRT で利用する際、製品への影響分析やトリアージが必要となり、対応の負担が大きい。	20%
			c）自社の PSIRT 活動と、サプライチェーン（特にソフトウェアの委託先、調達先）の PSIRT との連携に技術的あるいは運用上の課題がある。	0%
			d）ソフトウェアコンポーネントのリスト管理において、サプライチェーン（特にソフトウェアの委託先、調達先）と連携する仕組みが整備されていない。	20%
			e）脆弱性の情報をサプライチェーン（特にソフトウェアの委託先、調達先）間で共有する際、機密保持が大きな障害となっている。	0%
			f）委託先や調達先を含めたサプライチェーン全体のセキュリティ対策において、PSIRT が対応すべき内容が分からない（明確に定義されていない）。	20%
			g）製品の脆弱性情報について、機密保持やコンプライアンスの問題で、外部組織との情報共有（特に提供）が難しい。 ※本項の外部組織は、業種別の ISAC 機関、JPCERT:CC や IPA、OSS コミュニティなどを想定します。	0%
			h）製品に関連する脆弱性情報について、外部組織からの情報が欲しいが、適切な連携先がいない。 ※本項の外部組織は、業種別の ISAC 機関、JPCERT:CC や IPA、OSS コミュニティなどを想定します。	0%
			i）上記以外のその他の課題	20%
			[i）その他回答内容（自由記述）] ・CSIRT と PSIRT でどちらが担当するかといった、狭間に落ちるシステムがあり、その取扱いの基準が未整備なこと。	
	D-2-2	D-2-1 において課題としてチェックいただいた項目に	[課題の理由や事例（自由記述）] ・保守員（社員）が使用する保守作業管理用のサーバが、CSIRT が対	

ID		アンケート項目	回答項目	回答割合
		ついて、その理由や具体的な事例を差支えのない範囲でご回答ください。（自由記述）	処する社内インフラと見なされるのか、PSIRT が対処する事業サービスシステムと見なされるのか、が曖昧なこと。	

2）　企業における活動や情報連携及び課題の特徴

A）CSIRT・PSIRT の組成状況

各調査対象企業における CSIRT 及び PSIRT の組成状況の調査結果としては、まず CSIRT では「a）CSIRT あるいはそれに準ずる目的の組織（以下、CSIRT とする）を組成している」企業が全体の 80%、「b）CSIRT を組成していない企業」が 20%となっている。一方、PSIRT では「c）PSIRT あるいはそれに準ずる企業（以下、PSIRT とする）を組成している企業は 100%であった（図 7）。

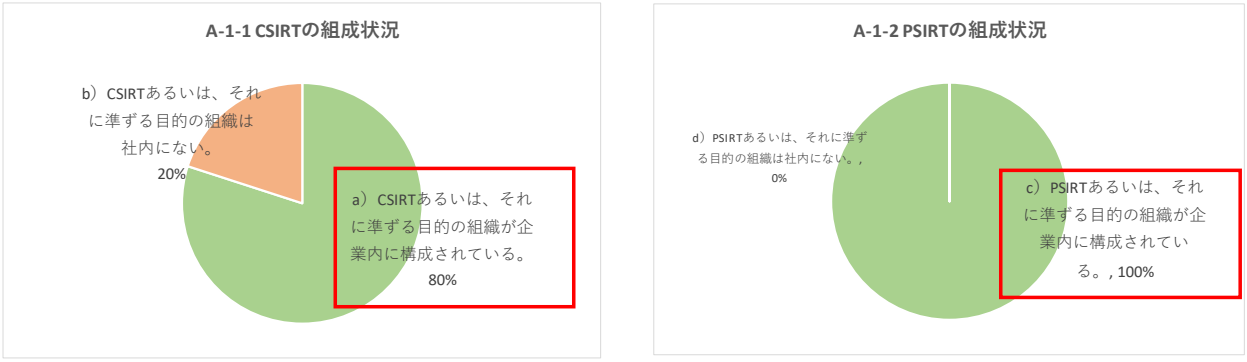


図 7　CSIRT 及び PSIRT の組成状況

CSIRT 及び PSIRT のこれまでの活動期間については、CSIRT では「c）5 年以上」の活動期間の企業は 75%、次いで、「b）3 年以上～5 年未満」の企業が 25%であり、一方 PSIRT では「c）5 年以上」の活動期間の企業は 60%、次いで、「b）3 年以上～5 年未満」の企業が 40%であった。両者では、CSIRT の方が比較的早期に組成され、活動実績も蓄積されていることが示された（図 8）。

図 8　CSIRT 及び PSIRT の活動期間

CSIRT 及び PSIRT の構成人数では、CSIRT では「b）5 名～10 未満」の企業及び、「c）10 名以上」の企

業がそれぞれ 50%であり、PSIRT では 80%の企業が「c）10 名以上」、20%の企業が「a）5 名未満」と回答があった。体制の面では、比較的 PSIRT の方が、比較的規模の大きい組織体制を有していることが示された（図 9）。

図 9　CSIRT 及び PSIRT の構成人数

CSIRT 及び PSIRT の人員構成については、CSIRT では 50%が「c」中心となる構成メンバーが他の事業部と兼任」となっており、25%が「b）選任のメンバーを中心とし、一部が他事業部と兼任の要員」となっている。また CSIRT が「a）専任の役割を担当する要員を中心に構成」している企業も 25%の回答があった（図 10）。PSIRT では、60%が「c）中心となる構成メンバーが他の事業部と兼任」であり、40%が「b）選任のメンバーを中心とし、一部が他事業部と兼任の要員」となっている（図 11）。人員構成の面では、CSIRT と PSIRT で大きな違いはなく、いずれも他の事業部の要員が兼任する形で柔軟な組織構成を行っていることが示された。

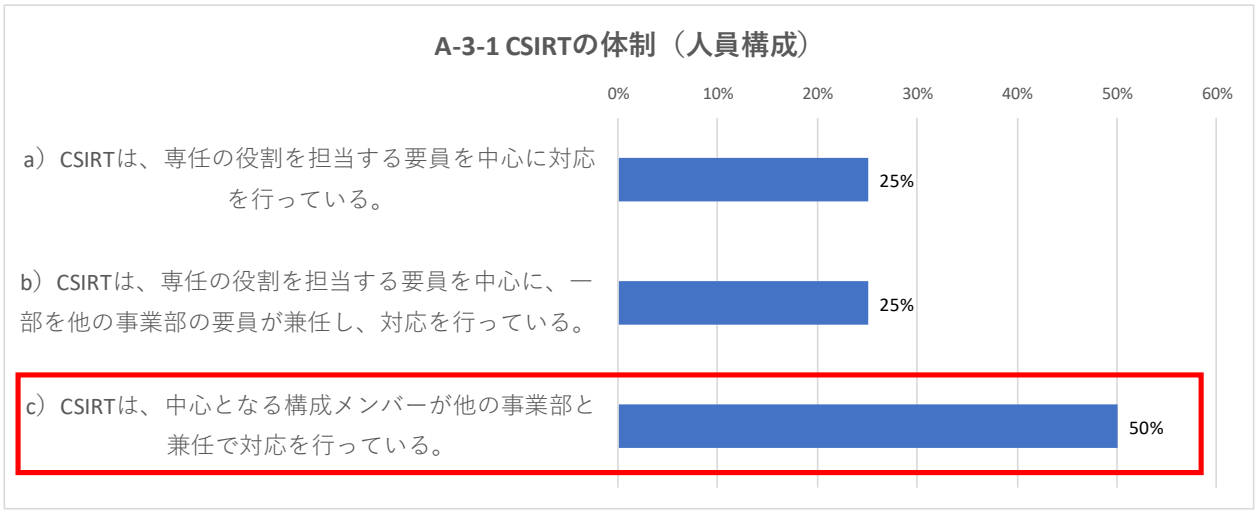


図 10　CSIRT の体制（人員構成）

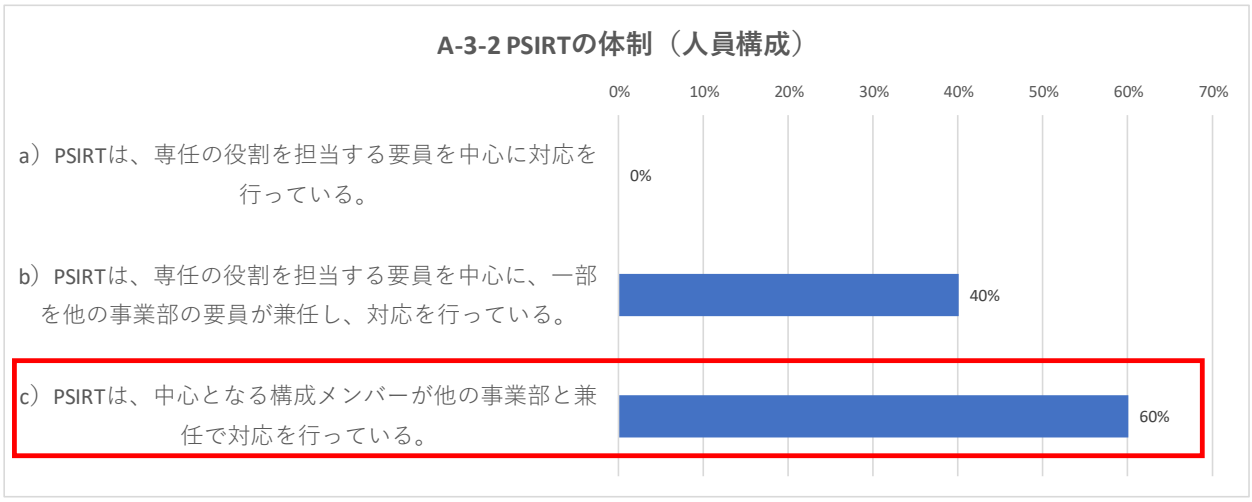


図 11　PSIRT の体制（人員構成）

CSIRT 及び PSIRT の対応部門については、CSIRT では、「情報システム部門」の兼任が 75%、次いで「管理部門」が 25%となっている（図 12）。PSIRT では、60%が「品質保証（品質管理）部門」の要員であり、次いで「情報システム部門」と「製品の開発部門」がそれぞれ 40%という回答であった（図 13）。

また続くヒアリング調査の結果からは、PSIRT では、主管となる部門は「品質保証（品質管理）部門」が担当し、また共有される脆弱性やインシデントの影響を分析については、開発部門の設計者（あるいは部門）が担当するケースが多いことが確認されている。

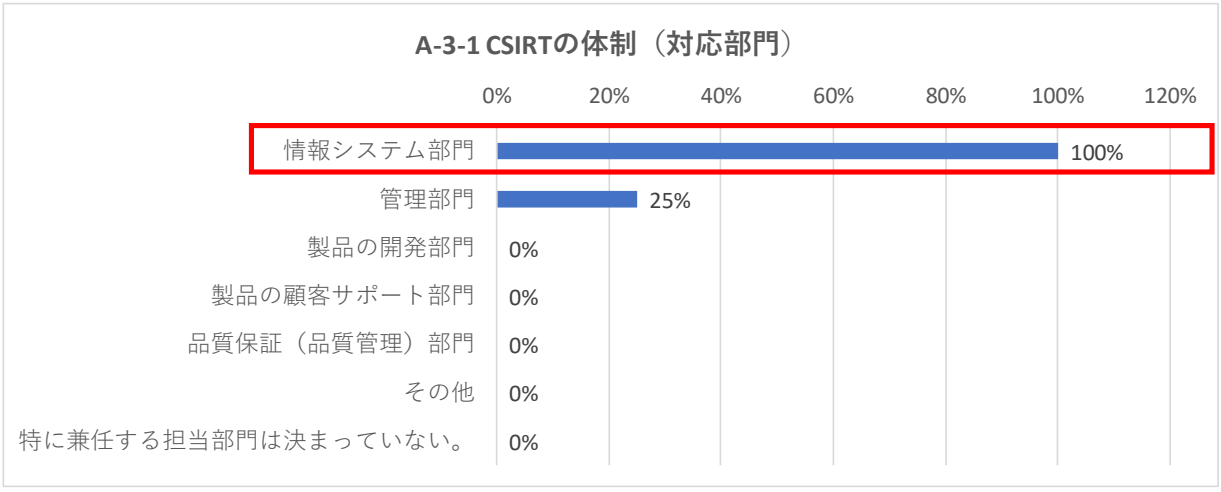


図 12　CSIRT の体制（対応部門）

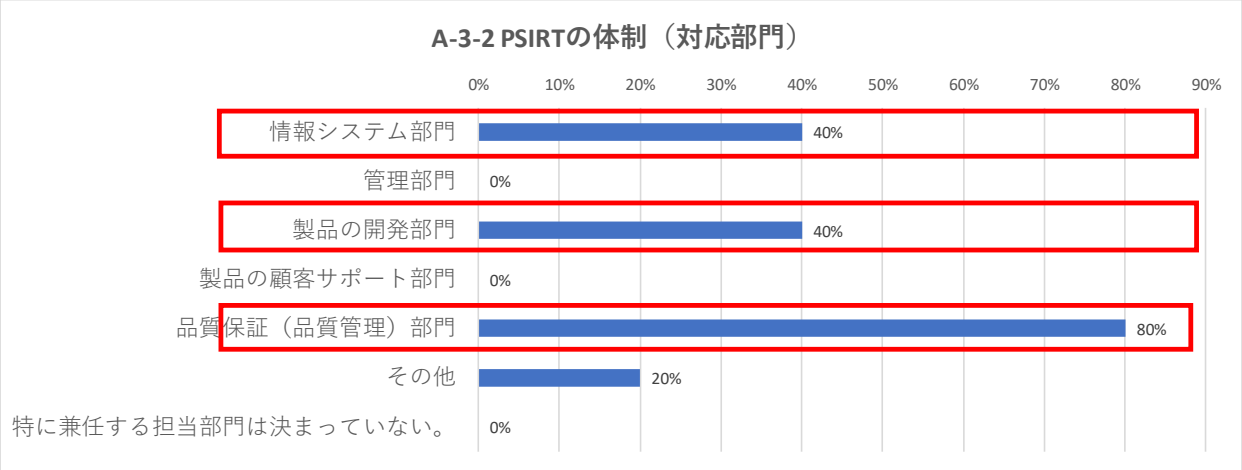


図 13　PSIRT の体制（対応部門）

B）CSIRT・PSIRT の活動状況

B1）CSIRT の活動状況

CSIRT の活動状況については、必要な活動を「B-1-1 インシデントに対応する組織、発生前の準備」、「B-1-2 インシデントの発見、報告」、「B-1-3 インシデント情報のトリアージと分析」、「B-1-4 インシデントの告知」、「B-1-5 インシデントの抑制措置と復旧」、「B-1-6 インシデントの事後対応」という６つのプロセスに区分し、それぞれのプロセスに対する各企業の対応状況を５段階の自己評価として回答を得た。本項では、アンケート及びヒアリング結果により、課題としてあげられている箇所を中心に整理を行っている。

CSIRT の６つのプロセスにおいて、「B-1-1 インシデントに対応する組織、発生前の準備（図 14）」、「B-1-2 インシデントの発見、報告（図 15）」、「B-1-3 インシデント情報のトリアージと分析（図 16）」の各プロセスは、質問に対する企業の殆どが「対応できている」あるいは「どちらかと言えば対応できている」と回答しており、CSIRT 活動が定着し、対応の熟練度も高まっていることから、特に課題はあげられていないことが確認された。

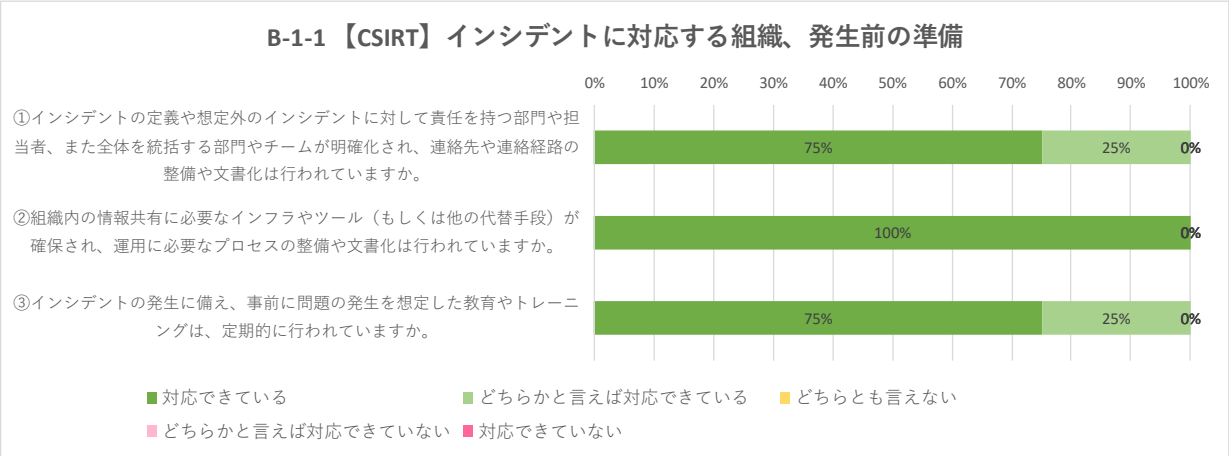


図 14　【CSIRT】インシデントに対応する組織、発生前の準備の評価

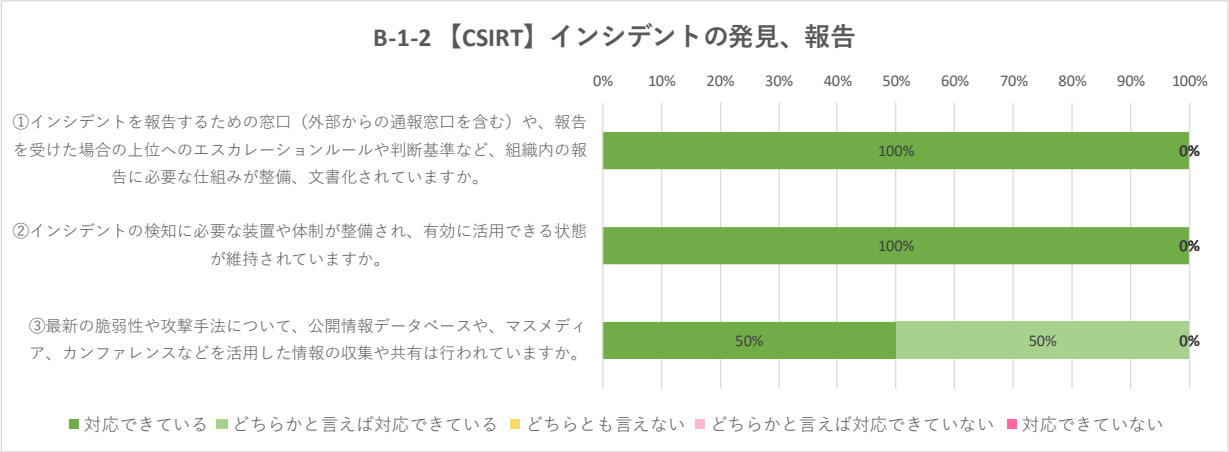


図 15　【CSIRT】インシデントの発見、報告の評価

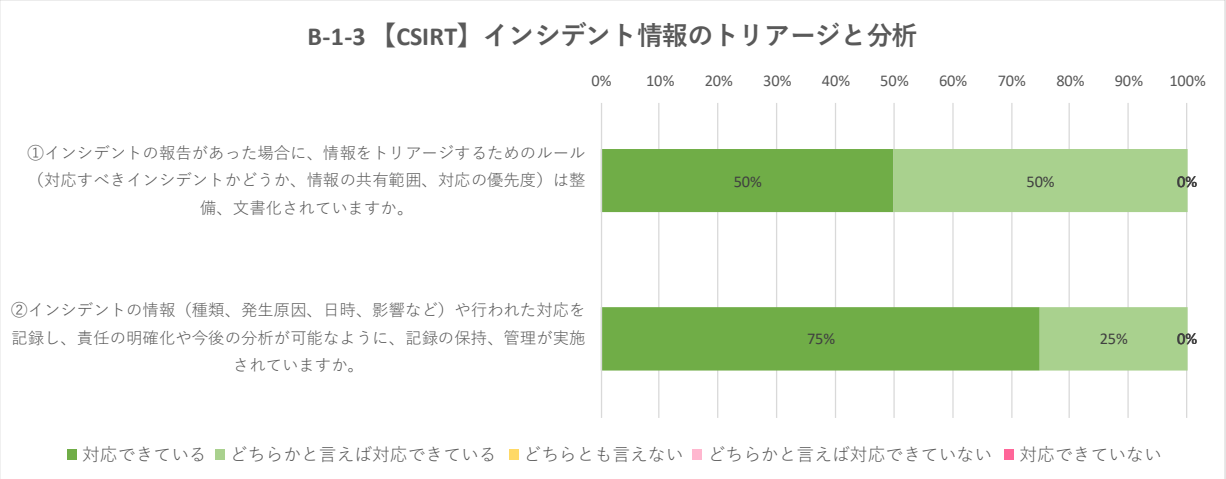


図 16　【CSIRT】インシデント情報のトリアージと分析

「B-1-4 インシデントの告知（図 17）」では、「①インシデント発生の事実や対応状況について、外部への報告の要否、報告の対象（社会全体、所轄官庁、顧客、一般利用者など）、公開する情報の範囲、告知手段（Web サイト、マスメディアへのプレスリリース、記者会見など）について、判断を行う仕組みが整備されているか」という質問に対して、25%が「どちらとも言えない」と回答している。回答としては少数ではあるが、インシデントを外部へ公開する際の公開範囲や方法、手段について、明確な基準が一部整備されてケースが確認されている。

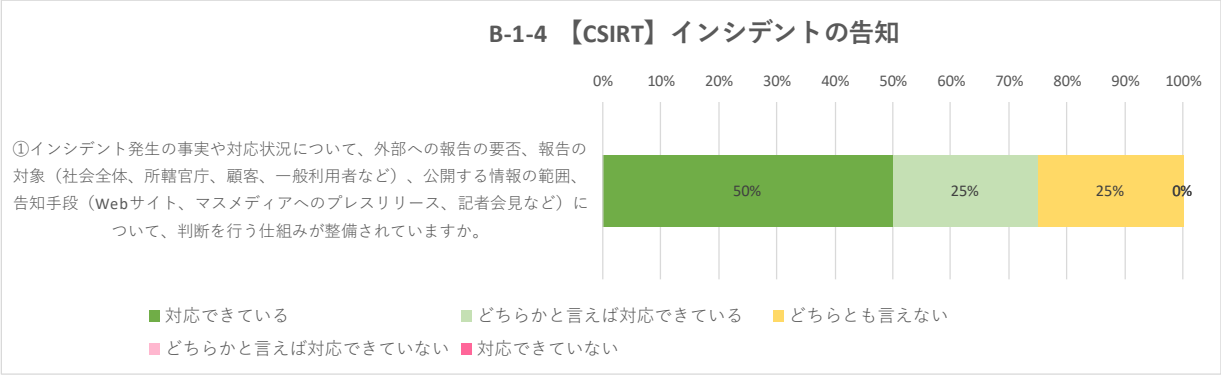


図 17　【CSIRT】インシデントの告知

CSIRT の 6 つのプロセスの中では「B-1-5 インシデントの抑制措置と復旧（図 18）」が最も自己評価が低い結果となった。まず「①インシデントの被害を抑制するための措置について、その手段や実施機関、講じた措置によるビジネスへの影響を検討する仕組みが整備されているか。また、抑制措置に対する最終的な意思決定者は明確に定義されているか」という質問に対して、「どちらとも言えない」が 25%、「どちらかと言えば対応できていない」が 25%という回答であり、特にビジネスへの影響の分析や検討について、全体の半数近くに課題があることが確認されている。

次に「②インシデントからの復旧について、組織の事業継続計画（BCP）との対応関係を明確化し、データなどの資産の一部損失も含めた復旧措置を検討する仕組みが整備されているか。また復旧計画に関する最終的な意思決定者は明確に定義されているか」という質問に対しては、25%が「どちらかと言えば対応できていない」という回答であり、特に BCP との対応を明確にした復旧計画の策定という部分で、課題を有する企業が少数存在することが確認された。

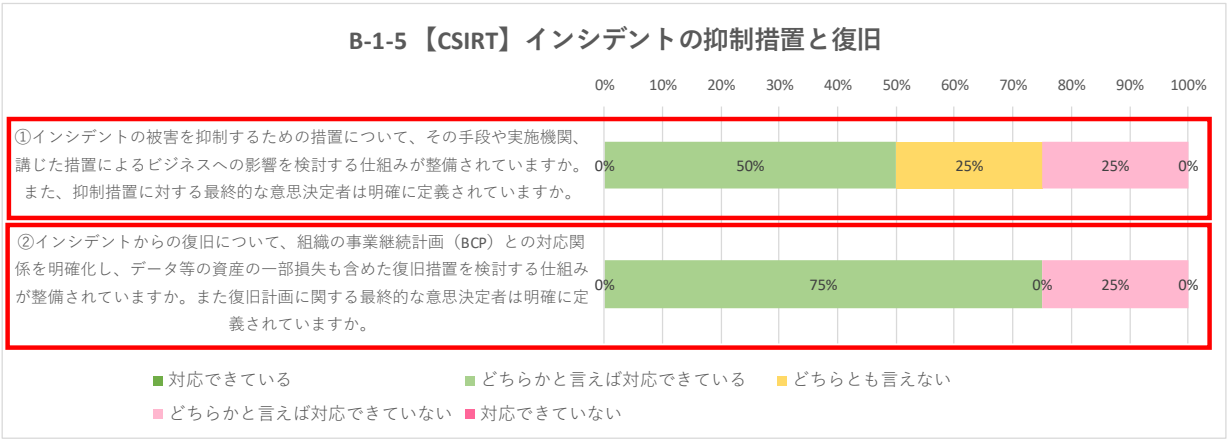


図 18　【CSIRT】インシデントの抑制措置と復旧

「B-1-6 インシデントの事後対応（図 19）」では、「①再発を防ぐためのモニタリングが実施され、表面的な問題の解決ではなく、本質的な問題の解決措置の検討を行える仕組みが整備されているか」という質問に対して、25%より「どちらとも言えない」という回答があった。調査対象企業の多くは対応できているという回答が多数であるものの、一部モニタリングの実施については、課題を有する企業が少数存在す

ることが確認された。

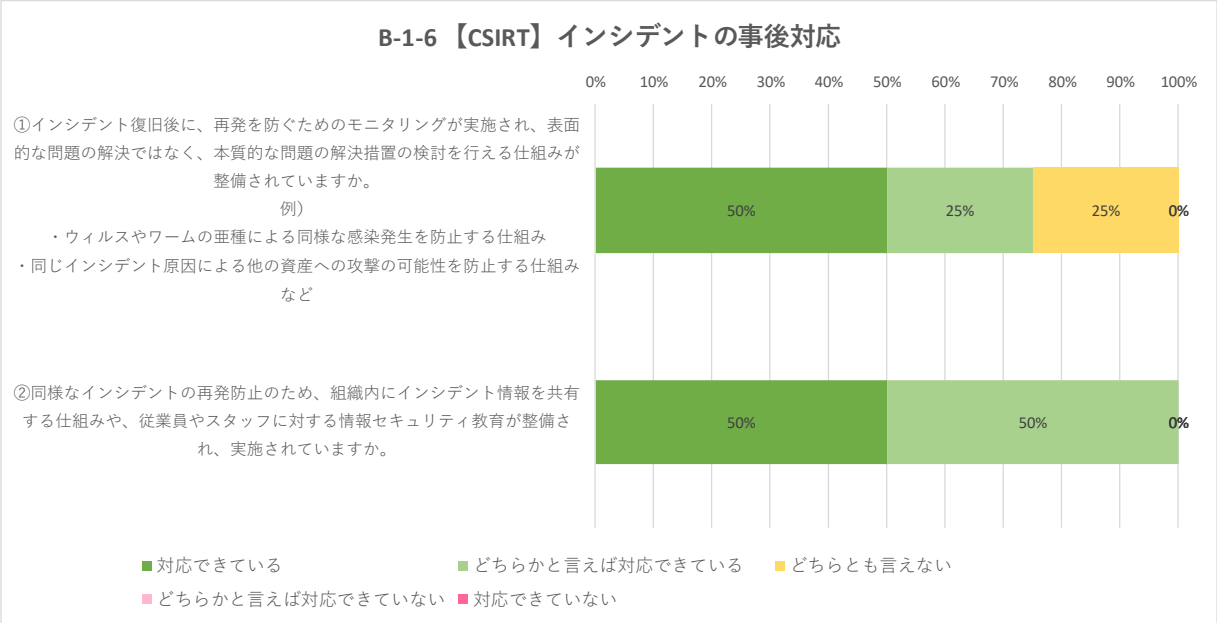


図 19　【CSIRT】インシデントの事後対応

B2）PSIRT の活動状況

PSIRT の活動状況については、必要な活動を「B-2-1 ステークホルダのエコシステムマネジメント」、「B-2-2 脆弱性の発見」、「B-2-3 脆弱性情報のトリアージと分析」、「B-2-4 脆弱性の改善及び対策」、「B-2-5 脆弱性の開示」、「B-2-6 トレーニングと教育」という 6 つのプロセスに区分し、それぞれのプロセスに対する各企業の対応状況を 5 段階の自己評価として回答を得た。本項では、アンケート及びヒアリング結果により、課題としてあげられている箇所を中心に整理を行っている。

「B-2-1 ステークホルダのエコシステムマネジメント（図 20）」では、まず「②外部組織と定期的に PSIRT 活動に関するコミュニケーションを行う場が設定されているか」という質問に対して、20%が「どちらかと言えば対応できていない」、20%が「対応できていない」と、全体の半数近くに課題がある回答となった。ヒアリング調査の結果、グループ企業の親会社から外部機関との連携機能を担っているため、グループ企業としては親会社との連携が中心になっているケースが確認されている。

また「③PSIRT の活動の実施状況や成果を評価する指標や仕組みがあり、社内へ定期的な報告や情報共有は行われているか」という質問については、80%が「どちらとも言えない」という回答であった。

ヒアリング調査では、PSIRT の活動を成果する仕組みが充分に整備されていないケースや、PSIRT からの状況報告は行われているが、定期的な実施にはなっていないというケースがあげられている。

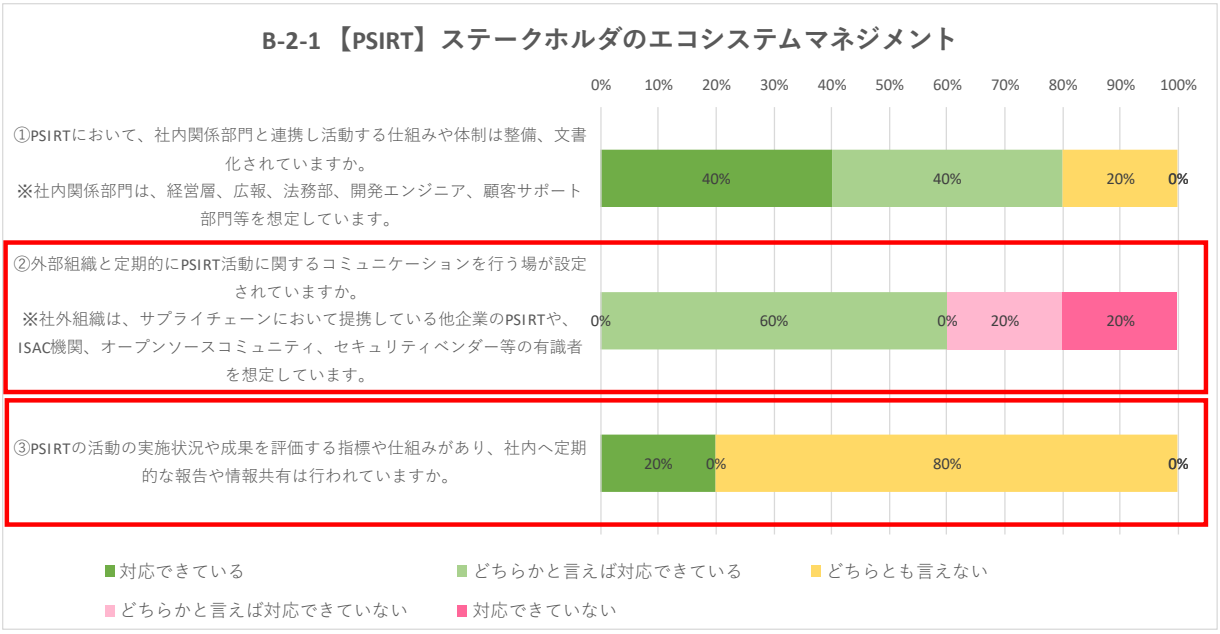


図 20　【PSIRT】ステークホルダのエコシステムマネジメント

「B-2-2 脆弱性の発見（図 21）」では、まず「④製品に使用されているソフトウェアコンポーネントのリスト（SBOM あるいはその他の方式による）について、継続的な管理や更新は、PSIRT 活動と連携して行われているか」という質問に対して、60%が「どちらとも言えない」、20%が「対応できていない」という回答であった。

ヒアリング調査では、全社で統一的なフォーマットを整備できていない点や、機械処理により読み取り可能な形式ではなく、開発部門ごとに異なるエクセル形式により管理が行われているため、上記のような

回答となっている。今回調査対象とした企業では、管理作業の簡便さを優先し、エクセル形式としているが、それによる問題や効率上の課題などは特に確認されていない。

また、「⑤公開されていない脆弱性について、製品へのセキュリティテストなどによる発見の仕組みは整備されているか。」という質問については、40%より「どちらかと言えば対応できていない」、20%より「対応できていない」という回答であった。

ヒアリング調査では、製品全体に対するセキュリティテストの実施は行われているが、OSS 単体を対象としていないケースや、製品に対するセキュリティテストについても、まだ課題があり、手法や手順の整備が不十分であるというケースがあげられている。

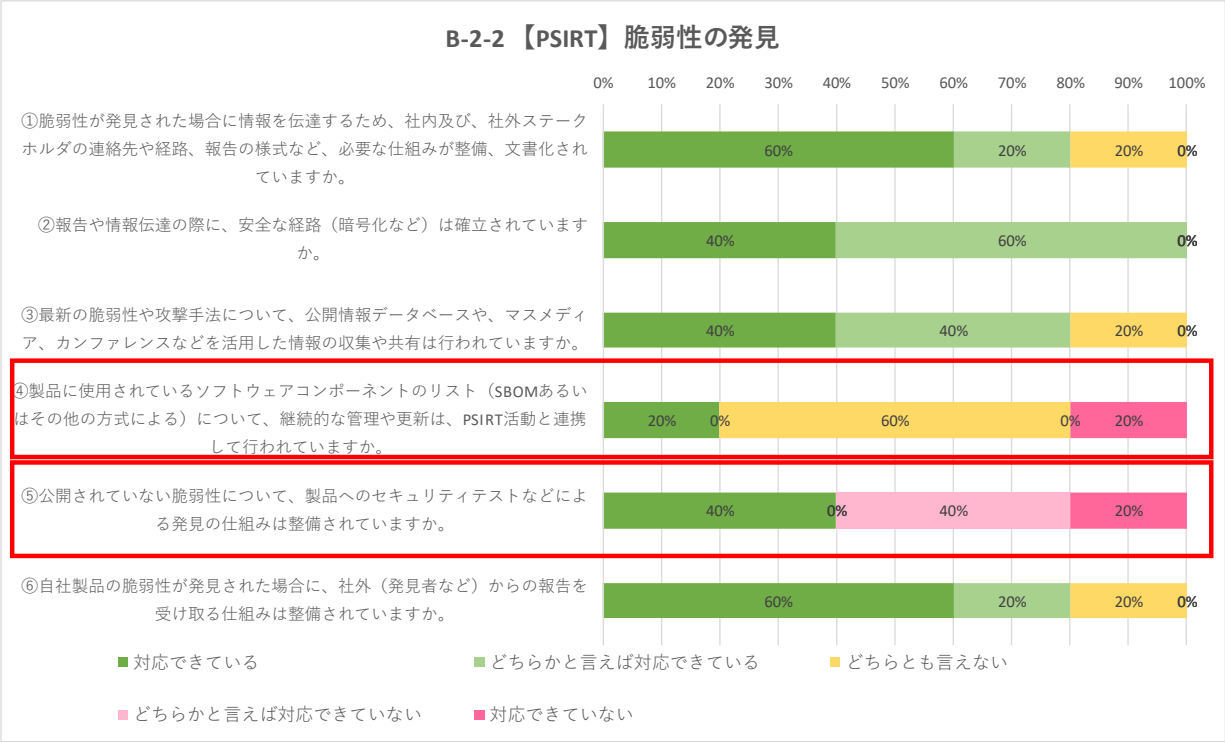


図 21　【PSIRT】脆弱性の発見

「B-2-3 脆弱性情報のトリアージと分析（図 22）」では、まず「①収集あるいは報告された脆弱性や攻撃手法について、製品への影響や再現性をテストするための方法や環境の整備が行われているか」という質問に対して、60%が「どちらとも言えない」という回答であった。

ヒアリング調査では、サーバやネットワークに対するセキュリティ検査については、対応可能な商用ツールが整備されているものの、組込み機器に対しては有効な商用ツールがない（あるいは情報として精査できていない）という回答であった。ただし、多くの企業では脆弱性データベースで開示されている PoC やエクスプロイトコードなどを利用し、組込み製品に対するセキュリティテストは実施されている。

次に「③報告、発見された製品の脆弱性に対して、作りこみの原因や、製品への影響、対策（回避策）の分析、優先度（対応しない場合を含む）を決定する仕組みは整備、文書化されているか」という質問に対して、60%より「どちらとも言えない」という回答であった。

ヒアリング調査では、脆弱性の原因や影響、対策、優先度の判断には、ケースバイケースでの対応が必要となるため、プロセスをオフィシャルな文書には落とし込めていないというケースが多くの企業で確

認されている。また CSIRT から共有された脆弱性の情報にもとづき、製品の影響分析を行うためには、ソフトウェアの名称やバージョン情報といった表層だけでなく、構成ファイルの状況分析や、最終的にはソースコードの確認まで必要となるケースがあり、その対応には相当な工数、コストを必要するため全ての情報を分析することが困難であるという課題もあがっている。

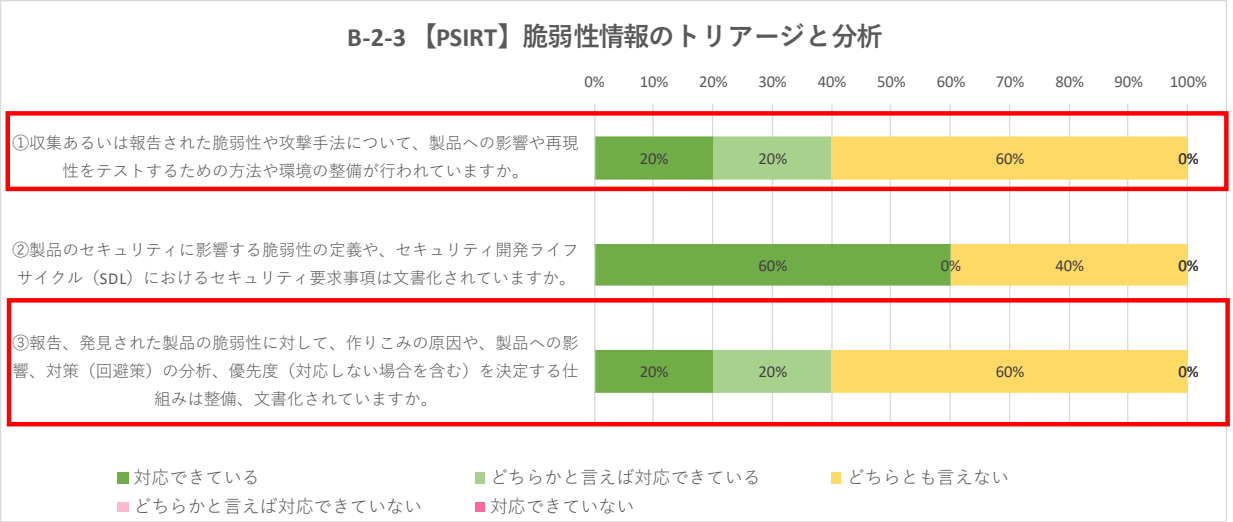


図 22　【PSIRT】脆弱性のトリアージと分析

「B-2-4 脆弱性の改善及び対策（図 23)」については、まず「③インシデント発生時の対応について、社内の緊急対応室（あるいはそれに準ずる組織）が設置され、対応方針が整備、文書化されていますか。その方針にはサプライチェーン上のステークホルダへの対応についても定義されていますか。」という質問対して。60%が「どちらとも言えない」という回答であった。

また、「④報告、発見された脆弱性の件数や CWE 分類、対策の状況などが記録として整備、管理され、事後の分析や追跡に利用できる形式になっているか」という質問に対して、60%より「どちらとも言えない」、40%より「どちらかと言えば対応できていない」という回答であり、多くの企業で課題を抱えていることが確認された。

ヒアリング調査では、記録の対応はできているものの、CWE の分類までは対応できていないというケースや、まだ製品ベースの PSIRT 活動では脆弱性やインシデントの事例が乏しく、記録をデータベースとして確立するところまでは整備できてないといったケースを確認している。

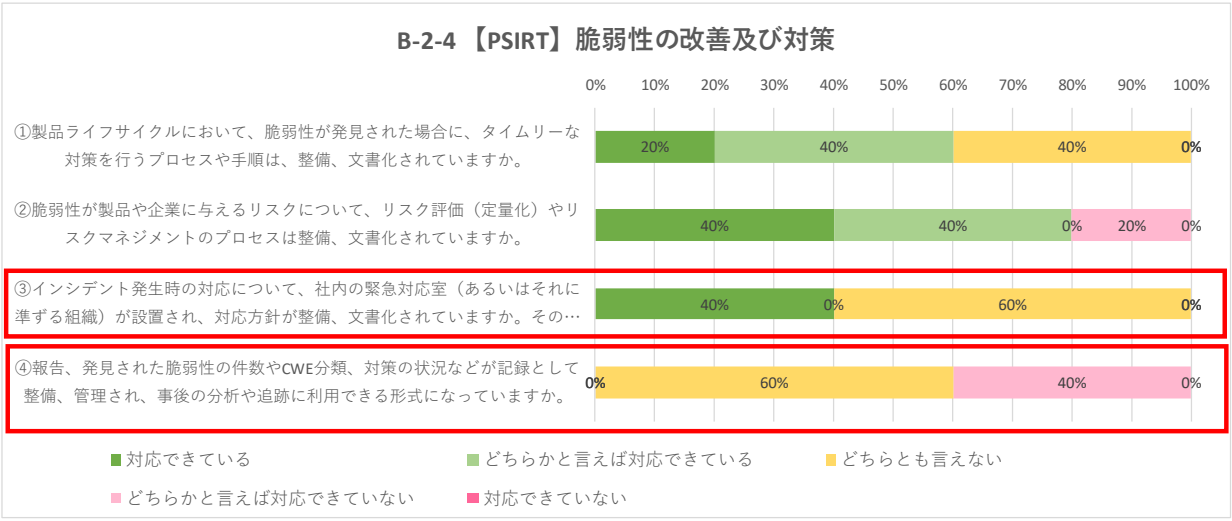


図 23　【PSIRT】脆弱性の改善及び対策

「B-2-5 脆弱性の開示（図 24）」については、「②製品の脆弱性の情報公開において、リリースノートの作成や情報の公開範囲や内容の事前レビュー、社内関係部門との連携など、計画的な対応が可能な形式として整備されているか」という質問に対して、60%より「どちらとも言えない」という回答であった。

ヒアリング調査では、情報公開の仕組みやプロセスの整備について、概ね対応はできているものの、会社として正式な文書として位置づけられていないというケースや、対応の仕組みやプロセスは整備されているものの、計画的な実施という面では課題があるケースなどがあげられている。

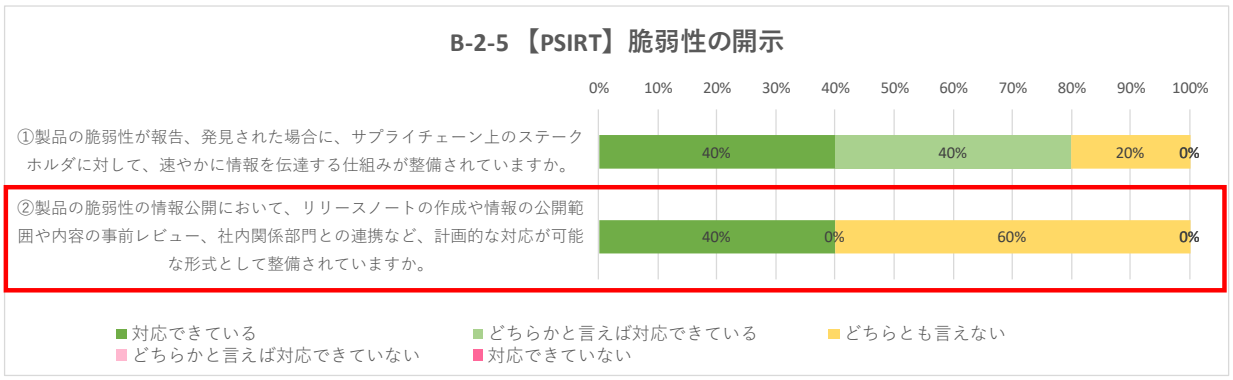


図 24　【PSIRT】脆弱性の開示

「B-2-6 トレーニングと教育（図 25）」については、PSIRT の 6 つのプロセスの中で最も自己評価が低い結果となった。まず「①PSIRT 活動において、社内関係部門毎に責任や役割分担に基づく教育やトレーニングの方針が整備、文書化され、定期的な教育・トレーニングが実施されているか」という質問に対しては、20%がどちらとも言えない。60%が「どちらかと言えば対応できていない」、20%が「対応できていない」という回答であった。ヒアリング調査では、PSIRT 部門に対する教育プログラムはあるものの、社内の関係部門に対する教育プログラムについては、整備が遅れているケースなどが確認されている。

次に「②PSIRT 活動に関連する技術的な内容について、教育やトレーニングの方針が整備、文書化され、定期的な教育・トレーニングが実施されているか」という質問に対しては、20%が「どちらとも言えな

い」、40%が「どちらかと言えば対応できていない」、40%が「対応できていない」という回答であった。

ヒアリング調査では、特に技術的な側面において、PSIRT 要員が保有するサイバーセキュリティの知識や技術レベルが一定ではないため、適切な教育、トレーニングプログラムを策定することの困難さがあげられている。また、脆弱性の分析や再現テストについては、開発部門（設計部門）や品質保証部門が担当しているため、PSIRT として教育プログラムが定義されていないというケースもあげられていた。また、課題への対応策として、複数のグループ組織を有する企業では、親会社による全社な教育、トレーニングプログラムの策定や展開を希望する提案も意見としてあげられていた。こうした意見を踏まえ、JPCERT/CC として、PSIRT 活動の目的な技術的な対応事項について、現行のガイドラインも更に細部の解説を加えた文書の開示などにより、企業側の PSIRT に対する教育面を支援することも検討が必要ではないかと考えられる。

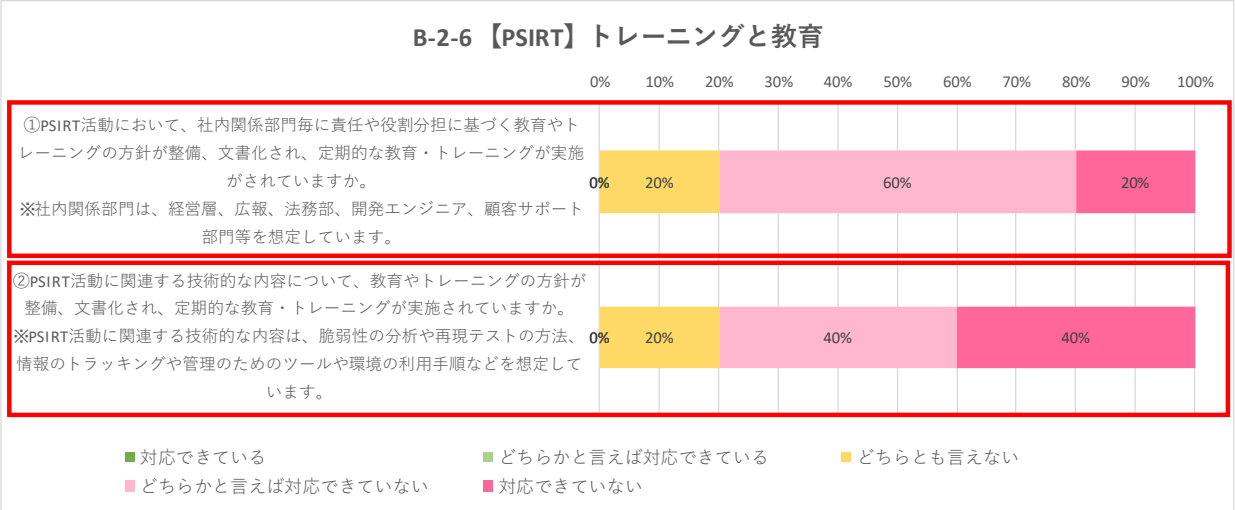


図 25　【PSIRT】トレーニングと教育

B3）CSIRT・PSIRT 連携状況調査

CSIRT と PSIRT 間の連携状況調査については、CSIRT からの情報展開をベースとした、「自社における CSIRT と PSIRT 間の連携の状況（図 26)」と、自社及びステークホルダにおける PSIRT からの情報展開をベースとした、「サプライチェーン間の PSIRT 連携状況（図 27)」という 2 種類の対応状況について、調査を実施している。

更に「サプライチェーン間の PSIRT 連携状況」については、自社（製品提供企業）を中心として、「下流企業（ユーザ企業など）から自社への情報提供」、「自社から上流企業（調達先など）への情報共有」、「上流企業（調達先など）から自社への情報共有」について、サプライチェーン全体を俯瞰した連携の状況をアンケート及びヒアリングによる調査を実施している。

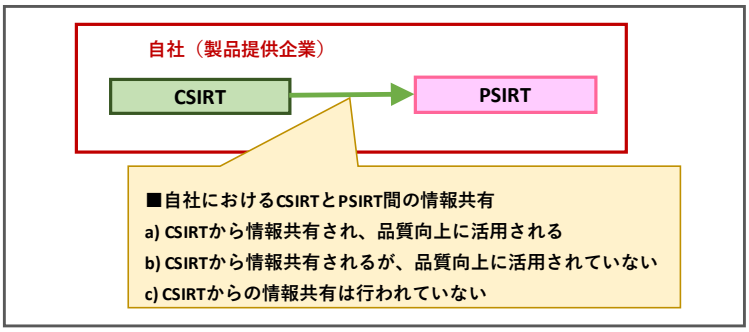


図 26　自社における CSIRT と PSIRT 間の連携について

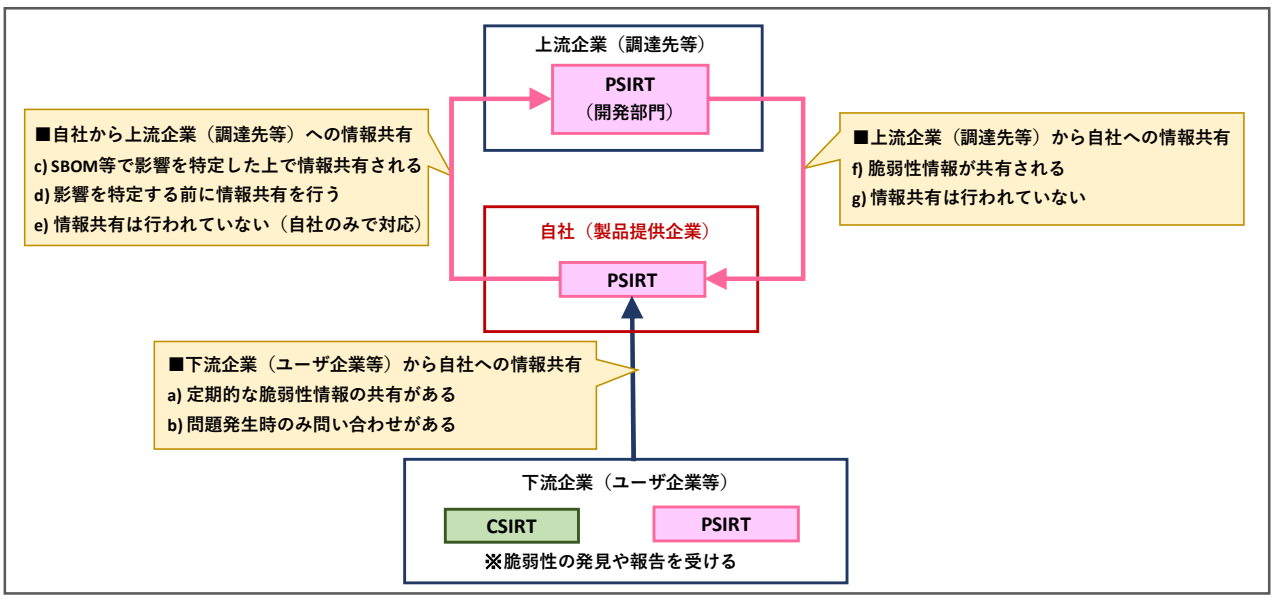


図 27　サプライチェーン間の PSIRT 連携について

【外部ステークホルダへのインシデント報告のタイミングについて】

まずは CSIRT、PSIRT の両組織が外部ステークホルダへインシデントの報告を行うタイミングについて、調査を実施した。

「B-3-1 CSIRT における外部ステークホルダへのインシデント報告タイミング（図 28)」では、50%が「a）外部ステークホルダへの報告は、インシデント発生後、いつまでに報告を完了すべきか対応期限が定義され、タイムリーな報告が行えるようになっている」と回答し、50%が「b）外部ステークホルダへの報告について、インシデント発生後の報告期限は特に定義されていないが、インシデントの状況や報告すべき対象者に応じて、報告のタイミングを検討する仕組みとしている」という回答であり、今回の調査対象企業の全てが、発生したインシデントの報告を外部ステークホルダに行う仕組みを有していることが確認されている。

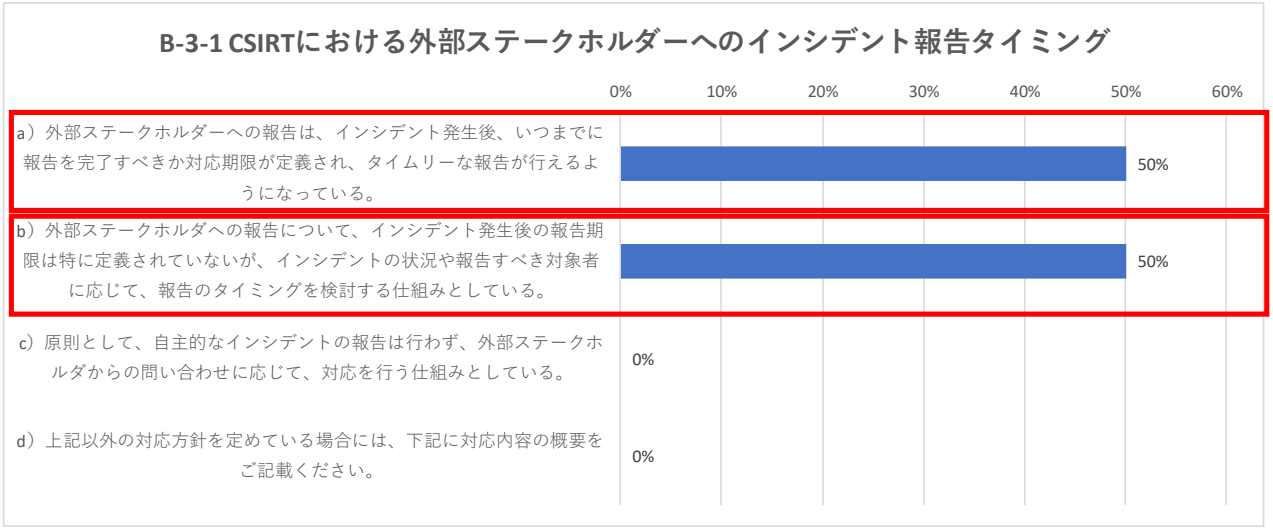


図 28　B-3-1 CSIRT における外部ステークホルダへインシデント報告タイミング

一方、「B-3-2 PSIRT における外部ステークホルダへのインシデント報告タイミング（図 29)」では、80%が「b）外部ステークホルダへの報告について、脆弱性の検出後の報告期限は特に定義されていないが、インシデントの状況や報告すべき対象者に応じて、報告のタイミングを検討する仕組みとしている」と回答し、明確な報告期限はないものの、製品の脆弱性の報告を外部ステークホルダに行う仕組みを有していることが確認されている。また少数ではあるが、20%より「c）原則として、自主的な脆弱性検出の報告は行わず、外部ステークホルダからの問い合わせに応じて、対応を行う仕組みとしている。」という回答があった。

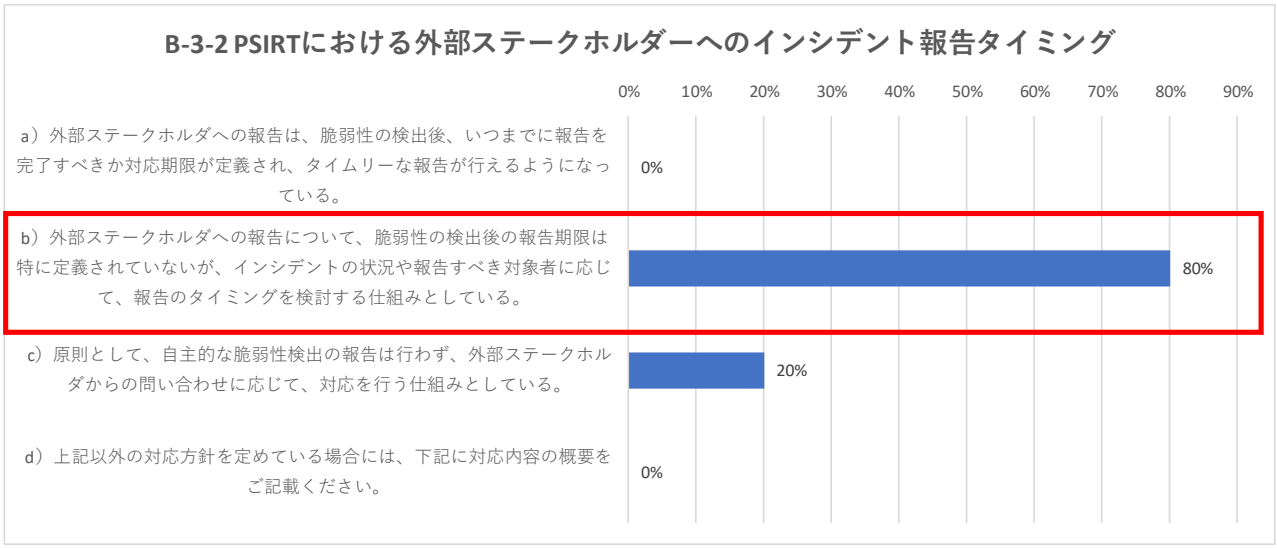


図 29　B-3-2 PSIRT における外部ステークホルダへインシデント報告タイミング

【自社における CSIRT と PSIRT の連携について】

次に、自社における CSIRT と PSIRT 間における連携について、調査を実施した（図 30）。アンケートの結果、「a）CSIRT 活動で得られたインシデントや脆弱性などの情報は、定期的に PSIRT へ共有され、自社製品への影響分析を経て、品質向上に活用されている」という回答は 20%に留まり、CSIRT の情報が PSIRT を含む製品向上にはあまり有効に活用されていないという結果となった。他の回答としては、40%が「b）CSIRT 活動で得られたインシデントや脆弱性などの情報は、PSIRT へ共有されているが、自社製品への影響分析や、品質向上には、あまり活用されていない」であり、40%が「c）CSIRT 活動で得られたインシデントや脆弱性などの情報は、PSIRT へと共有されていない」となっている。

ヒアリング調査では、b）、c）の理由について確認を行った結果、CSIRT で収集したインシデント情報は、組込み機器向けの情報が少なく、自社の製品に対して適用できる事例が少ないというケースや、対象の製品が異なるため、自社製品向けに影響分析をやり直す必要があり、インシデントの数が増えるほど、対応に工数を取られ、掛かるコストに見合った効果が得られないという意見がみられた。また CSIRT から共有された脆弱性の情報にもとづき、製品の影響分析を行うためには、ソフトウェアの名称やバージョン情報といった表層だけでなく、構成ファイルの状況分析や、最終的にはソースコードの確認まで必要となるケースがあり、その対応には相当な工数、コストを必要するため全ての情報を分析することが困難であるという意見もあがっている。

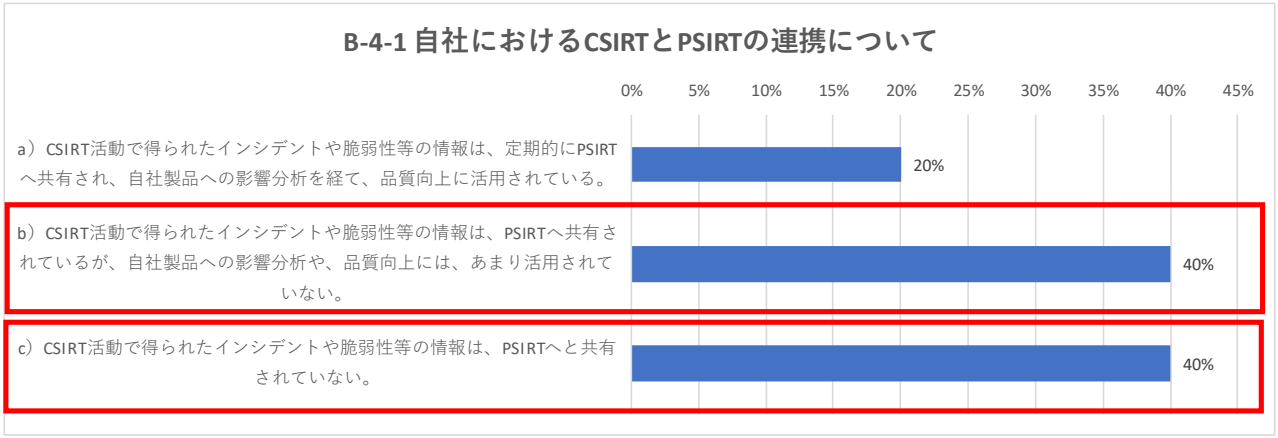


図 30　B-4-1 自社における CSIRT と PSIRT の連携について

【サプライチェーン間の PSIRT 連携について】

サプライチェーン間の PSIRT 連携について、まずは下流企業（ユーザ企業など）から自社への情報共有について、調査を行った（図 31）。アンケート結果では、100%の企業が「b）サプライチェーン下流企業（下流企業＝ユーザ企業などの顧客）が収集したインシデント（脆弱性情報）は、自社の PSIRT（あるいは開発部門）に情報共有されておらず、問題が発生した場合にのみ、問い合わせが発生する」と回答している。

ヒアリング調査では、製品の顧客が一般消費者である場合は、当然、問題発生時にクレームや問い合わせとして、情報連絡が発生するケースがあり、また B to B の製品やサービスにおいても、殆どの場合、ユーザ企業から定期的な情報共有が行われることはなく、基本的には問題が発生した場合、あるいは問題につながりそうな脆弱性のニュースリリースがあった場合にのみ、問い合わせや連絡があることが確認されている。

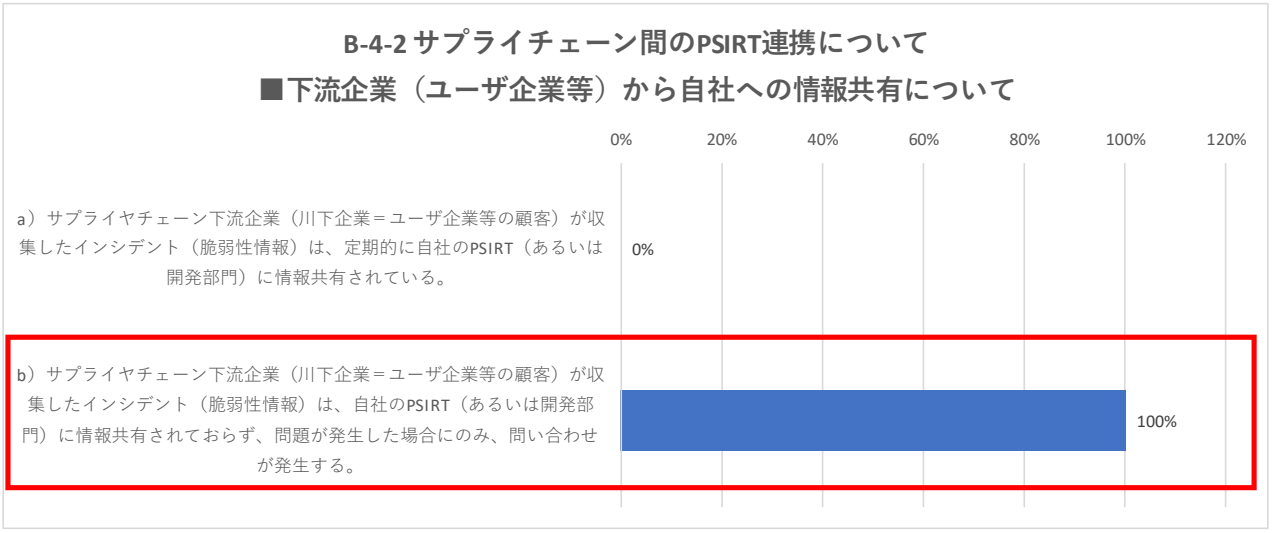


図 31　B-4-2 サプライチェーン間の PSIRT 連携について
～下流企業（ユーザ企業など）から自社への情報共有について

次に自社から上流企業（調達先など）への情報共有について、調査を行った（図 32）。アンケート結果では、80%が「d）自社製品において検出あるいは報告された脆弱性情報は、影響箇所を特定する前に、まずはサプライチェーン上流企業（＝ソフトウェアの委託先、調達先）の PSIRT（あるいは開発部門など）へ情報を共有している」と回答し、20%が「e）自社製品において検出あるいは報告された脆弱性情報は、原則として自社内で対応する仕組みとしており、サプライチェーン上流（＝ソフトウェアの委託先、調達先）企業の PSIRT（あるいは開発部門など）への情報共有は行っていない」と回答している。

続くヒアリング調査の結果、上流企業へ脆弱性の情報を共有している企業の多くは、セキュリティ課題への対応を上流企業側で実施することが委託契約の条項として組み込まれていることが確認されている。また 20%が「自社から上流企業への情報共有が行われていない」という回答であったが、これは製品の主要なソフトウェアコンポーネントを内製で開発していることに起因しており、特に課題となるケースは確認されていない。

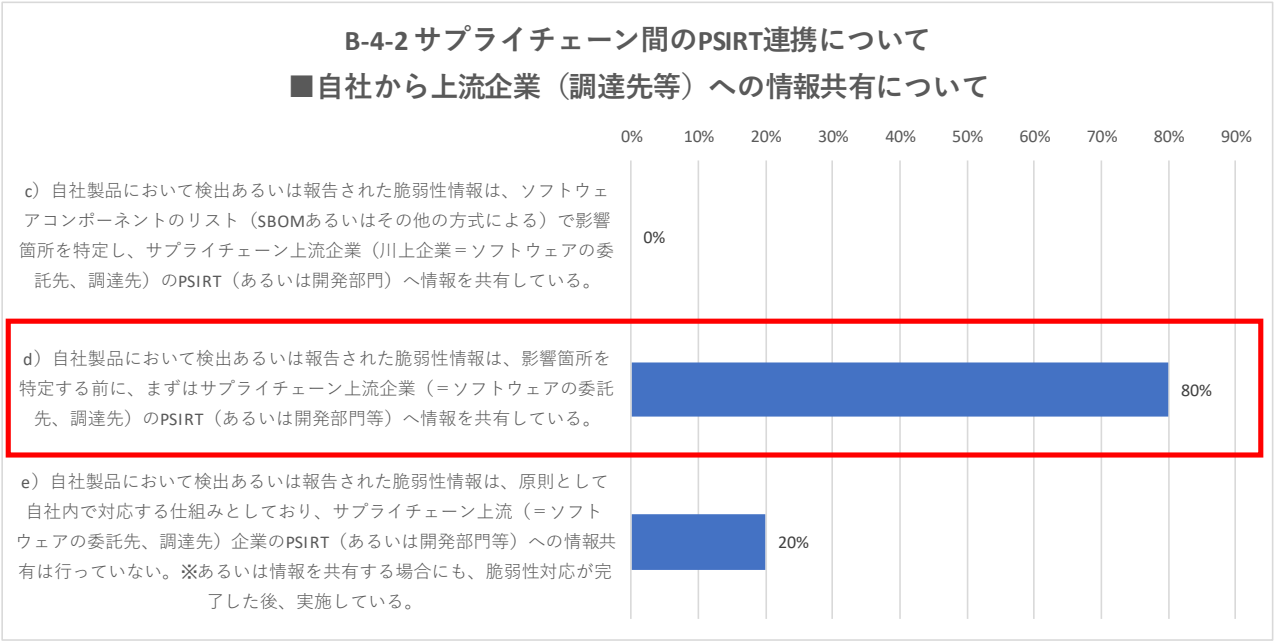


図 32　B-4-2 サプライチェーン間の PSIRT 連携について
～自社から上流企業（調達先など）への情報共有について

サプライチェーン間の PSIRT 連携について、最後に上流企業（調達先など）から自社への情報共有について、調査を行った（図 33）。アンケート結果では、80%が「f）サプライチェーン上流企業（＝ソフトウェアの委託先、調達先）で検出あるいは報告された脆弱性情報は、自社の PSIRT（あるいは開発部門など）へ情報が共有されている」と回答し、20%が「g）サプライチェーン上流企業（＝ソフトウェアの委託先、調達先）で検出あるいは報告された脆弱性情報は、特に自社の PSIRT（あるいは開発部門など）への情報共有が行われていない」と回答している。

続くヒアリング調査の結果、上流企業で検出された脆弱性の情報を自社へ共有している企業の多くは、上記結果と同様、上流企業で検出されたセキュリティ課題の報告についても、委託契約の条項として組み込まれていることが確認されている。やはりサプライチェーン間でセキュリティ対策を円滑に行うためには、こうした事例を参考に契約段階で、対応すべき事項を明確化しておく事が有効であると考える。ま

た 20%が「上流企業から自社への情報共有が行われていない」という回答であったが、これは製品の主要なソフトウェアコンポーネントを内製で開発していることに起因しており、特に課題となるケースは確認されていない。

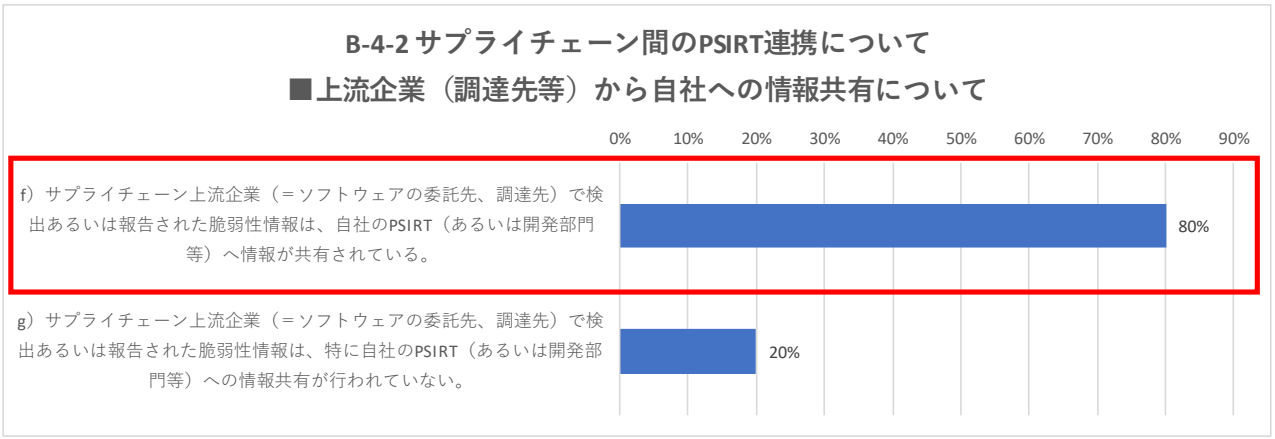


図 33　B-4-2 サプライチェーン間の PSIRT 連携について
～上流企業（調達先など）から自社への情報共有について

【インシデント・脆弱性に関係する外部組織との連携状況について】

連携状況に関する最後の調査では、調査対象企業における外部組織との連携状況について調査を行った（図 34）。アンケート結果では、80%が「a）製品の脆弱性情報について報告が必要と判断される場合には、IPA の脆弱性報告窓口を通じて、JPCERT/CC へ報告を行っている」と回答があった。また、今回の調査対象企業には、「b）ISAC 組織への情報の共有」、「c）所属している OSS コミュニティへの情報の共有」、「d）バグバウンティ制度の設定」を実施しているという回答は得られなかった。

続くヒアリング調査による確認の結果、今回の調査対象企業では、自社もしくはグループの親会社にて、製品の脆弱性に関する外部への報告ポリシーが適切に整備されており、社内の方針に沿って、外部機関へ報告を行うルールが厳密に遵守されていた（あるいはこれまで外部への報告事例はないものの、明確な報告ポリシーが整備されている）。今回の調査対象の回答には見られなかったが、社内の外部報告ポリシーが整備されていない企業の場合、判断の基準が曖昧となり、結果として社外への報告が行われないというケースも想定される。やはり、外部へ適切な報告を行うためには、報告が必要な脆弱性の判断基準や、情報の公開範囲や内容について、明確な判断の基準やプロセスを整備することが必要であると考えられる。

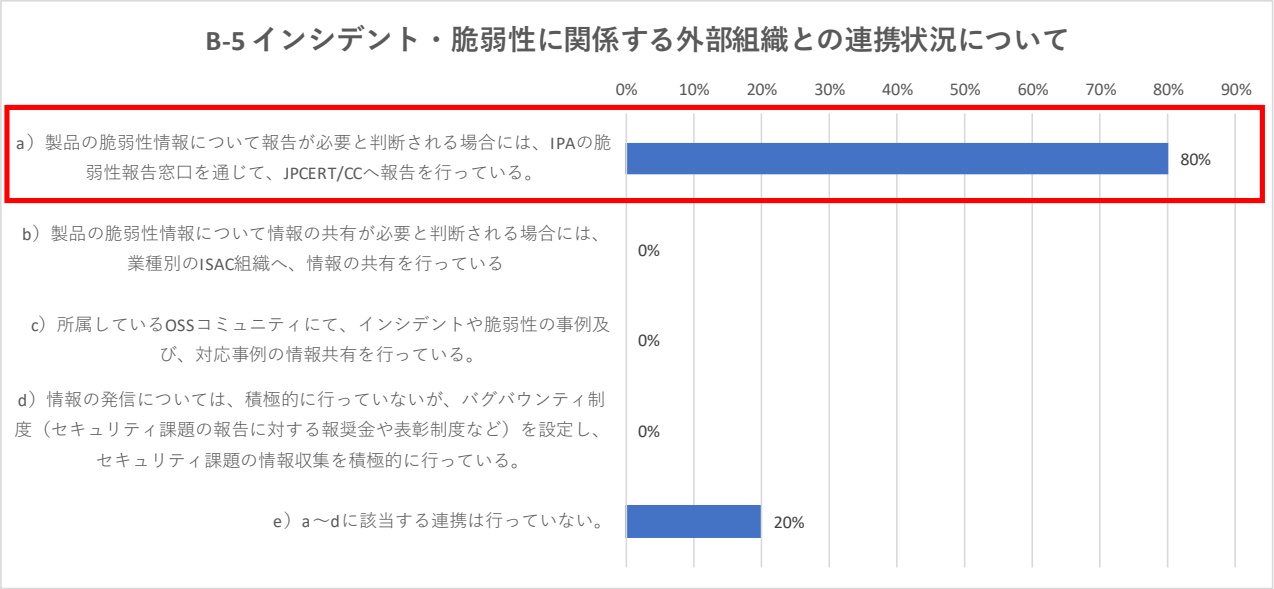


図 34　B-5 インシデント・脆弱性に関係する外部組織との連携状況について

C）CSIRT・PSIRT の有効性

続いて CSIRT、PSIRT 活動の有効性について、調査を実施した。本調査では、CSIRT・PSIRT 活動の経験を通じて、CSIRT や PSIRT が各項目の目的に対して効果的な手段であると考えられるかについて、それぞれ 5 段階評価で各社より回答を得た。（５：効果的である、４：どちらかと言えば効果的である、３：どちらとも言えない、２：どちらかと言えば効果的とは言えない、１：効果的とは言えない）

CSIRT 活動については、「①インシデント情報の収集や検出への効果」、「②インシデントの再発防止効果」、「③社内のセキュリティ教育への効果」の３項目の目的に対して、CSIRT という手段の有効性について調査を行った。結果としていずれの項目について、「有効である」もしくは「どちらかと言えば有効である」という回答であり、企業における CSIRT 活動がかなり成熟していることが確認され、その効果についても肯定的な回答となっている（図 35）。

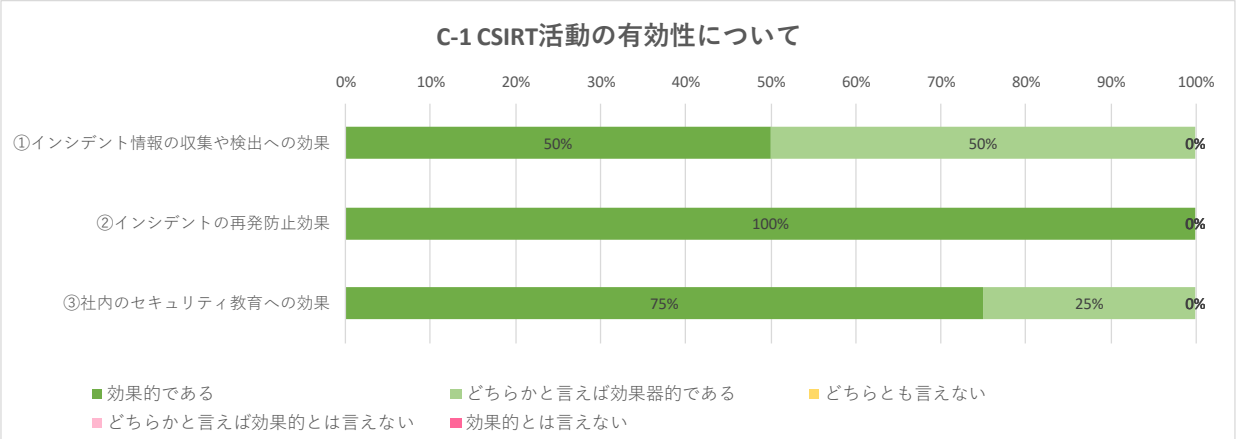


図 35　C-1 CSIRT 活動の有効性について

PSIRT 活動については、「①脆弱性情報の収集や検出への効果」、「②自社の製品開発におけるセキュリティ開発プロセスの向上効果」、「③サプライチェーンの上流（＝ソフトウェアの委託先や調達先）へのセキュリティ品質管理の徹底効果」、「④サプライチェーンの下流（＝ユーザ企業などの顧客、一般消費者）に対するセキュリティ品質の向上効果」、「⑤製品開発上のセキュリティ教育への効果」の５項目に対して、PSIRT という手段の有効性について調査を行った。アンケート結果では、項目③及び④については、「どちらとも言えない」という回答が、60％であり、CSIRT と比較すると、やや低い評価結果となった。

続くヒアリング調査を行った結果では、③及び④については、通常の開発プロセスあるいは品質保証（管理）プロセスにおける対応効果の比重が高いため、必ずしも PSIRT 活動の効果であるとは判断できないという意見が多かった（図 36）。

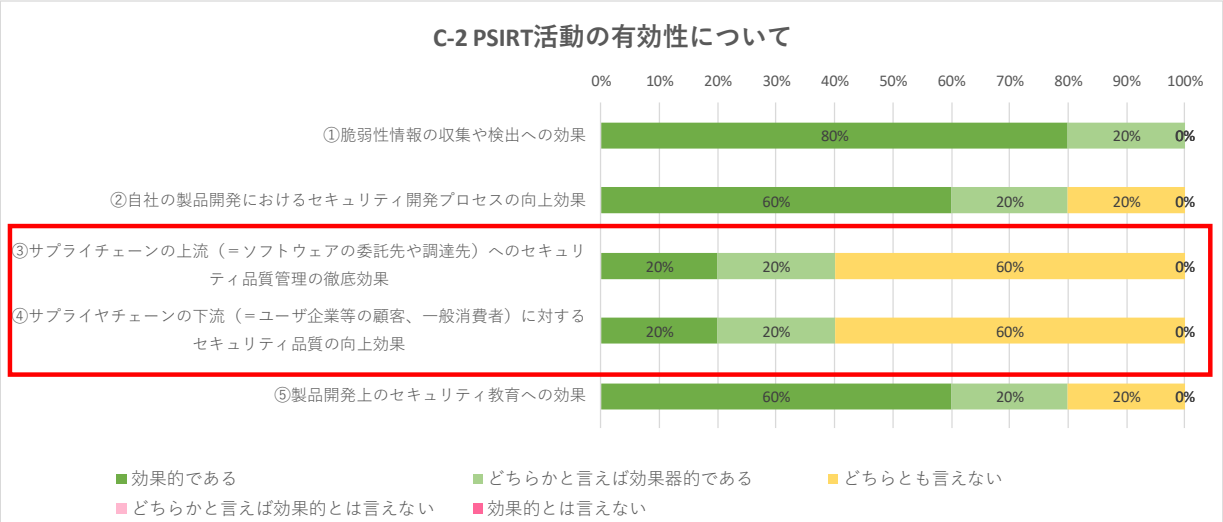


図 36　C-2 PSIRT 活動の有効性について

D）CSIRT・PSIRT における課題

最後に CSIRT、PSIRT の課題について、調査を行った。まず CSIRT の体制（人材）、管理運用面における課題のアンケート調査では、「a）CSIRT の活動、運用に必要な人材の確保が難しい」という回答が全体の 75%、「d）インシデントの監視に利用するシステムの導入、維持、運用に高いコストが発生している」という回答は全体の 50%であり、多くの調査対象企業で課題としてあげられている（図 37）。

ヒアリング調査において、それぞれの回答の詳細を確認したところ、「a）人材確保」の課題については、年々、CSIRT として対応すべき業務が増加しており、単純な人数においても、また一定のスキルを有する人材としても不足傾向にあるという回答であった。

「d）インシデントの監視システムのコスト」の課題については、会社全体としてはネットワークだけでなく、各自の業務用 PC など、様々な対象への監視システムが導入されており、高額なコストが発生しているという意見があった。

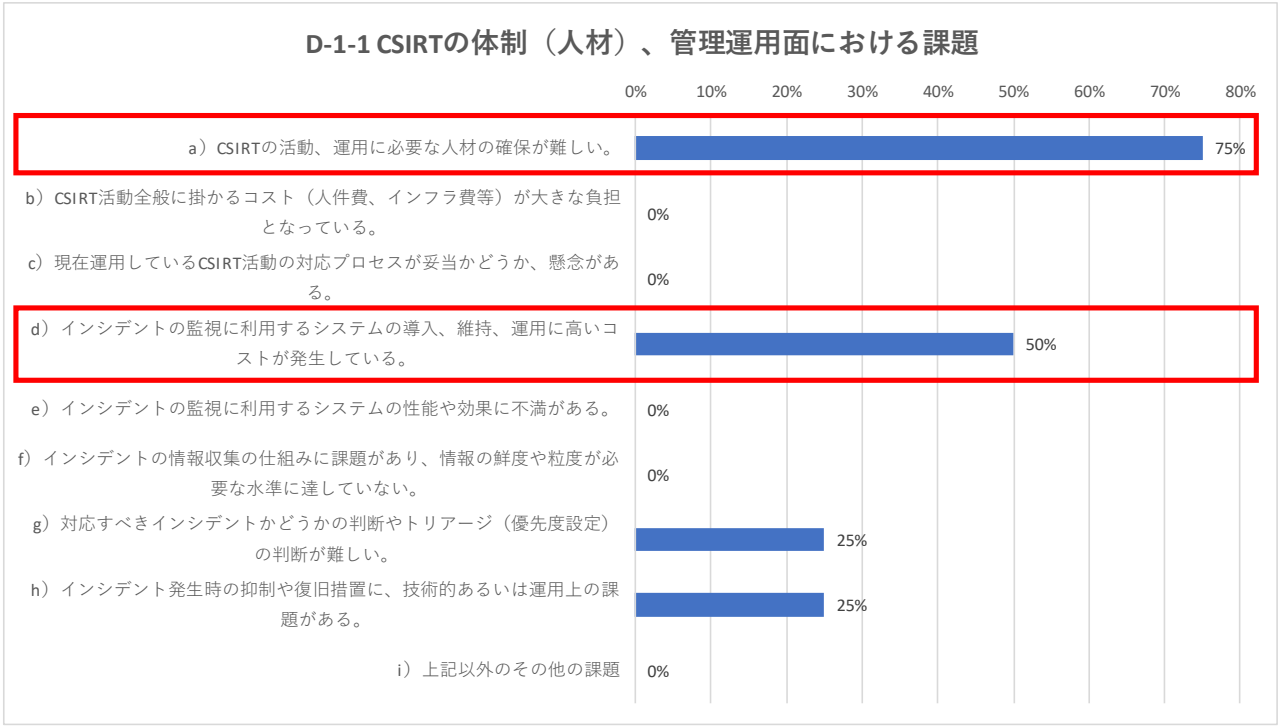


図 37　D-1-1 CSIRT の体制（人材）、管理運用面における課題

PSIRT の体制（人材）、管理運用面における課題のアンケート調査では、CSIRT と同様に「a）PSIRT の活動、運用に必要な人材の確保が難しい」という回答が最も割合が高く、全体の 80%となっている。他には、「d）ソフトウェアコンポーネントのリスト管理に、技術的あるいは運用上の課題がある」、「f）脆弱性や攻撃手法の情報収集の仕組みに課題があり、情報の鮮度や粒度が必要な水準に達していない」、「g）対応すべき脆弱性の判断やトリアージ（優先度設定）の判断が難しい」、「h）発見された脆弱性の対応において、製品に含まれるソフトウェア（OSS、サードパーティ製）側の対策や置換に、技術的あるいは運用上の課題がある」という 4 項目については、それぞれ全体の 40%が課題として回答している（図 38）。

ヒアリング調査では、それぞれの詳細について確認を行なった。

まず「a）の人材確保」の課題については、PSIRT 活動が他部門との兼任や連携で運用されているため、各部門の要員のスキルに差異があり、PSIRT 活動に関する理解を含め、知識・スキルに課題があるという意見があがっている。また海外の事業部とも連携して対応を行うケースでは、現地では人材の流動性が国内よりも高く、教育やトレーニングを実施した人材が定着しにくいという課題があげられていた。

「d）ソフトウェアコンポーネントのリスト管理」の課題としては、現状運用している製品別のエクセルによる管理から、将来的には IT 管理が可能な標準化形式への移行を想定しているという意見や、ソフトウェアのコンポーネントだけでなく、OS のハードニングに関する設定項目が多岐にわたり、管理方法の煩雑さやコスト上の課題が生じているという意見があがっていた。

「f）脆弱性の情報収集」及び「g）脆弱性の判断やトリアージ」に関する課題としては、CSIRT から展開される情報は、製品への影響度などを分析、トリアージする必要があるが、リスク分析にあたってはスキル、技術が求められるため、対応に工数（コスト）を要するという意見が見られた。

「h）製品に含まれるソフトウェア側の対策」の課題としては、過去の事例として、調達したアプリケーションに予期せぬ OSS が含まれていたケースがあげられていた。含まれていた OSS は GPL ライセンスのソフトウェアであり、製品のソースコードを公開する必要があり、販売中止の判断となった事例があることが確認された。

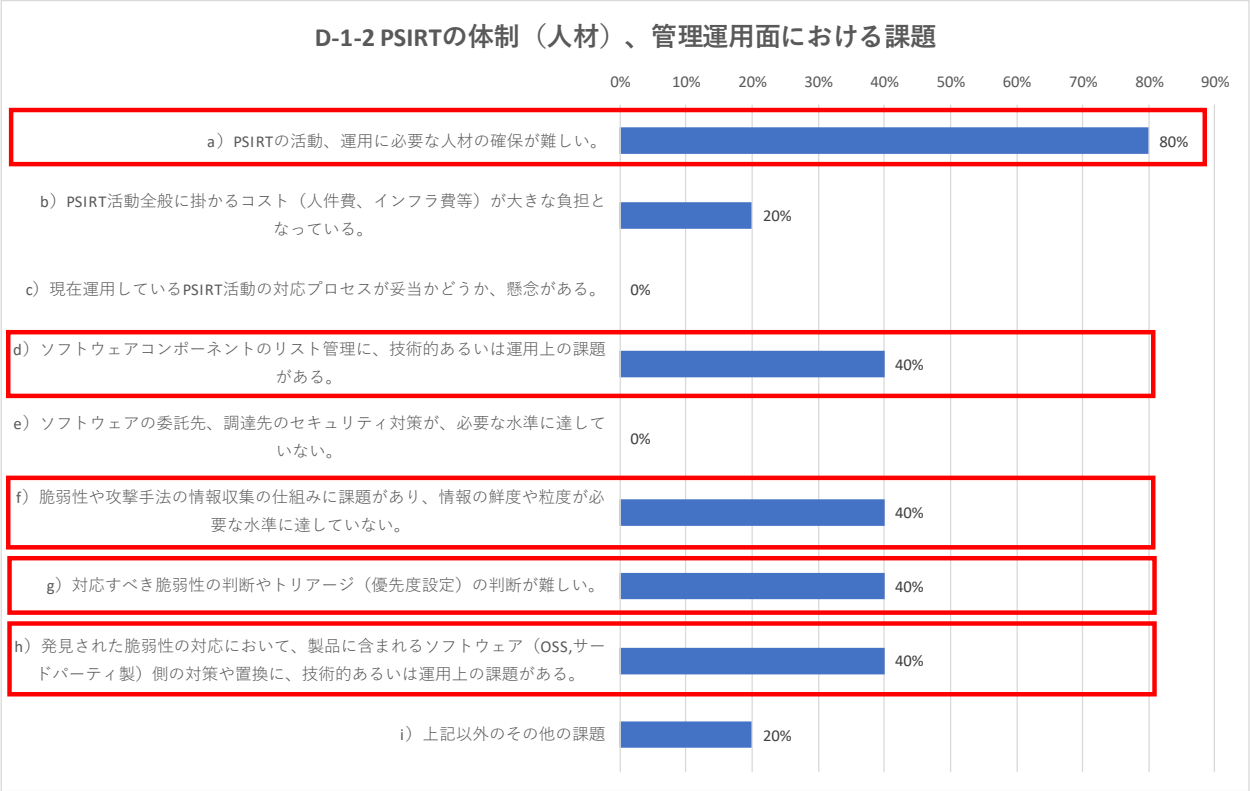


図 38　D-1-2 PSIRT の体制（人材）、管理運用面における課題

CSIRT・PSIRT 及び外部機関との連携における課題としては、いくつか課題があげられたが、いずれも割合が低く、特に調査企業の多くが課題としている事項はみられなかった（図 39）。

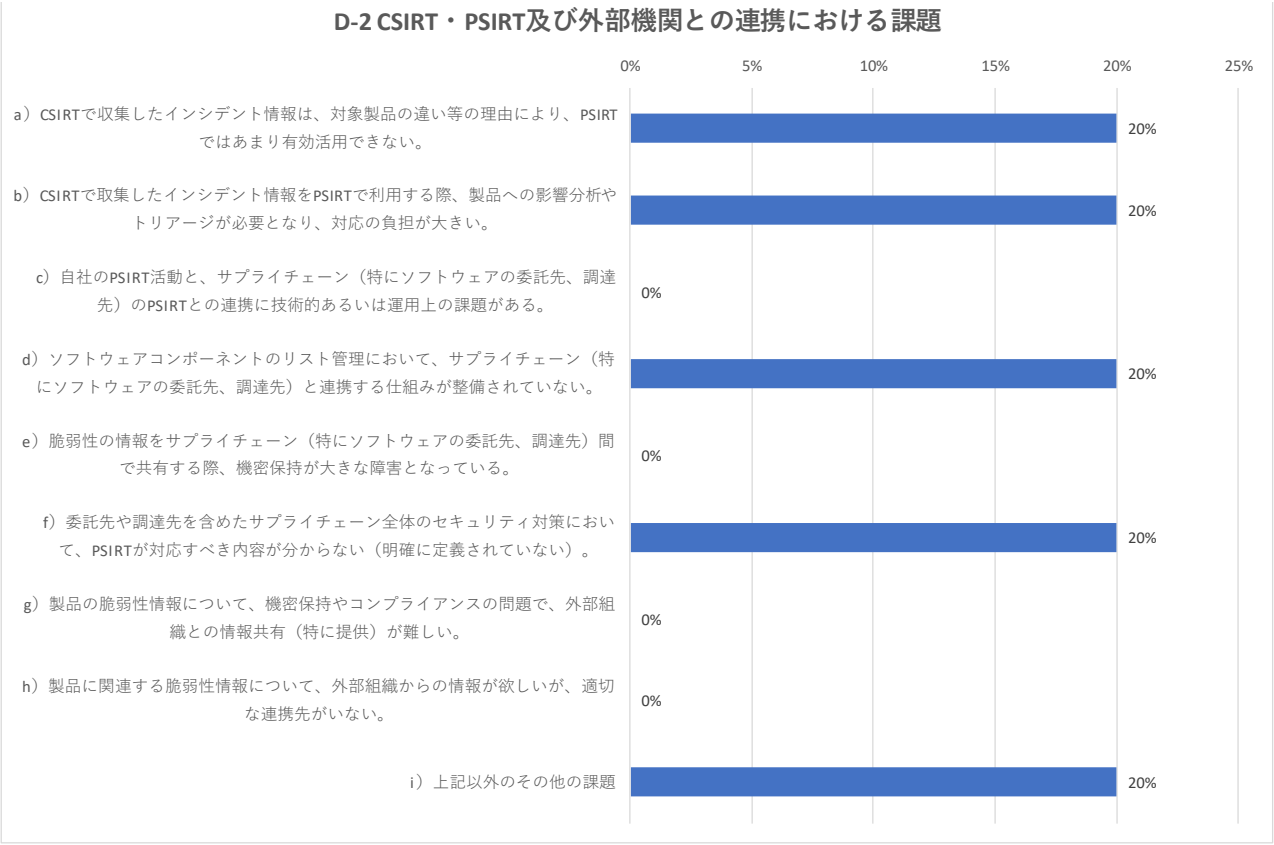


図 39　D-2 CSIRT・PSIRT 及び外部機関との連携における課題

2-3　　調査結果のまとめ

＜調査項目 2＞OSS に関わる CSIRT・PSIRT 連携調査結果のまとめとして、検出された課題一覧を表 24、表 25 に示す。表 24 では、文献調査による必要機能（サービス）に対して、調査対象企業の回答が「３：どちらとも言えない」以下であった項目の合計が、50%を超える項目を抽出している。また表 25 では、CSIRT・PSIRT 連携及び、課題として回答割合が 40%を超える項目を抽出している。本調査で提示された課題に対する提言については、後述の第 3 章＜調査項目３＞で示すものとする。

表 24　PSIRT 活動の課題一覧

アンケート項目		アンケートの質問事項		回答	回答率
B-2-1	**ステークホルダのエコシステムマネジメント**	③	PSIRT の活動の実施状況や成果を評価する指標や仕組みがあり、社内へ定期的な報告や情報共有は行われているか。	３：どちらとも言えない	80%
B-2-2	**脆弱性の発見**	④	製品に使用されているソフトウェアコンポーネントのリスト（SBOM あるいはその他の方式による）について、継続的な管理や更新は、PSIRT 活動と連携して行われているか。	３：どちらとも言えない	60%
				１：対応できていない	20%
		⑤	公開されていない脆弱性について、製品へのセキュリティテストなどによる発見の仕組みは整備されているか。	２：どちらかと言えば対応できていない	40%
				１：対応できていない	20%
B-2-3	**脆弱性情報のトリアージと分析**	①	収集あるいは報告された脆弱性や攻撃手法について、製品への影響や再現性をテストするための方法や環境の整備が行われているか。	３：どちらとも言えない	60%
		③	報告、発見された製品の脆弱性に対して、作りこみの原因や、製品への影響、対策（回避策）の分析、優先度（対応しない場合を含む）を決定する仕組みは整備、文書化されているか。	３：どちらとも言えない	60%
B-2-4	**脆弱性の改善及び対策**	③	インシデント発生時の対応について、社内の緊急対応室（あるいはそれに準ずる組織）が設置され、対応方針が整備、文書化されているか。その方針にはサプライチェーン上の	３：どちらとも言えない	60%

アンケート項目		アンケートの質問事項		回答	回答率
			ステークホルダへの対応についても定義されているか。		
		④	報告、発見された脆弱性の件数やCWE 分類、対策の状況などが記録として整備、管理され、事後の分析や追跡に利用できる形式になっているか。	3：どちらとも言えない	60%
				2：どちらかと言えば対応できていない	40%
B-2-5	脆弱性の開示	②	製品の脆弱性の情報公開において、リリースノートの作成や情報の公開範囲や内容の事前レビュー、社内関係部門との連携など、計画的な対応が可能な形式として整備されているか。	3：どちらとも言えない	60%
B-2-6	トレーニングと教育		PSIRT 活動において、社内関係部門毎に責任や役割分担に基づく教育やトレーニングの方針が整備、文書化され、定期的な教育・トレーニングが実施されているか。	2：どちらかと言えば対応できていない	60%
				1：対応できていない	20%
			PSIRT 活動に関連する技術的な内容について、教育やトレーニングの方針が整備、文書化され、定期的な教育・トレーニングが実施されているか。 ※PSIRT 活動に関連する技術的な内容は、脆弱性の分析や再現テストの方法、情報のトラッキングや管理のためのツールや環境の利用手順などを想定している。	2：どちらかと言えば対応できていない	40%
				1：対応できていない	40%

表 25　CSIRT・PSIRT 連携及び、その他の課題一覧

アンケート項目		アンケートの質問事項	回答率
B-4-1	自社における CSIRT と PSIRT の連携	b）CSIRT 活動で得られたインシデントや脆弱性などの情報は、PSIRT へ共有されているが、自社製品への影響分析や、品質向上には、あまり活用されていない。	40%
		c）CSIRT 活動で得られたインシデントや脆弱性などの情報は、PSIRT へと共有されていない。	40%

D-1-1	**CSIRT の体制（人材）、管理運用面における課題**	a）CSIRT の活動、運用に必要な人材の確保が難しい。	75%
		d）インシデントの監視に利用するシステムの導入、維持、運用に高いコストが発生している。	50%
D-1-2	**PSIRT の体制（人材）、管理運用面における課題**	a）PSIRT の活動、運用に必要な人材の確保が難しい。	80%
		d）ソフトウェアコンポーネントのリスト管理に、技術的あるいは運用上の課題がある。	40%
		f）脆弱性や攻撃手法の情報収集の仕組みに課題があり、情報の鮮度や粒度が必要な水準に達していない。	40%
		g）対応すべき脆弱性の判断やトリアージ（優先度設定）の判断が難しい。	40%
		h）発見された脆弱性の対応において、製品に含まれるソフトウェア（OSS,サードパーティ製）側の対策や置換に、技術的あるいは運用上の課題がある。	40%

＜調査項目３＞企業における CSIRT・PSIRT 活動のあり方の提言

調査項目 2 にて実施した調査の結果、CSIRT については、国内でも成熟した組織構築や対応プロセスが整備されていることが確認されている。一方で PSIRT については、対応する範囲が非常に幅広く、文献に紹介されているような理想的な体制やプロセスを構築できている企業は、非常に少数であることが明らかになった。本調査におけるまとめとして、サプライチェーンにおけるセキュリティリスク対応の観点から、特に PSIRT を中心とした活動や連携について、国内企業を対象に現実的かつ、ベースラインとなる要求事項を提言として示すものとする。なお、ベースラインとなる要求事項は、国内中小企業による対応を鑑み、”PSIRT Services Framework”をはじめとする各調査文献に準拠しつつ、最小限の必須事項として整理している。

3-1　BCP（事業継続計画）における CSIRT、PSIRT の位置づけ

企業内の IT インフラや提供製品・サービスに関わるセキュリティインシデントは、事業継続に影響する課題であり、BCP の一環として CSIRT、PSIRT を組成し、対応を行うことが求められる。図 40 に BCP における CSIRT、PSIRT の位置づけを示す。

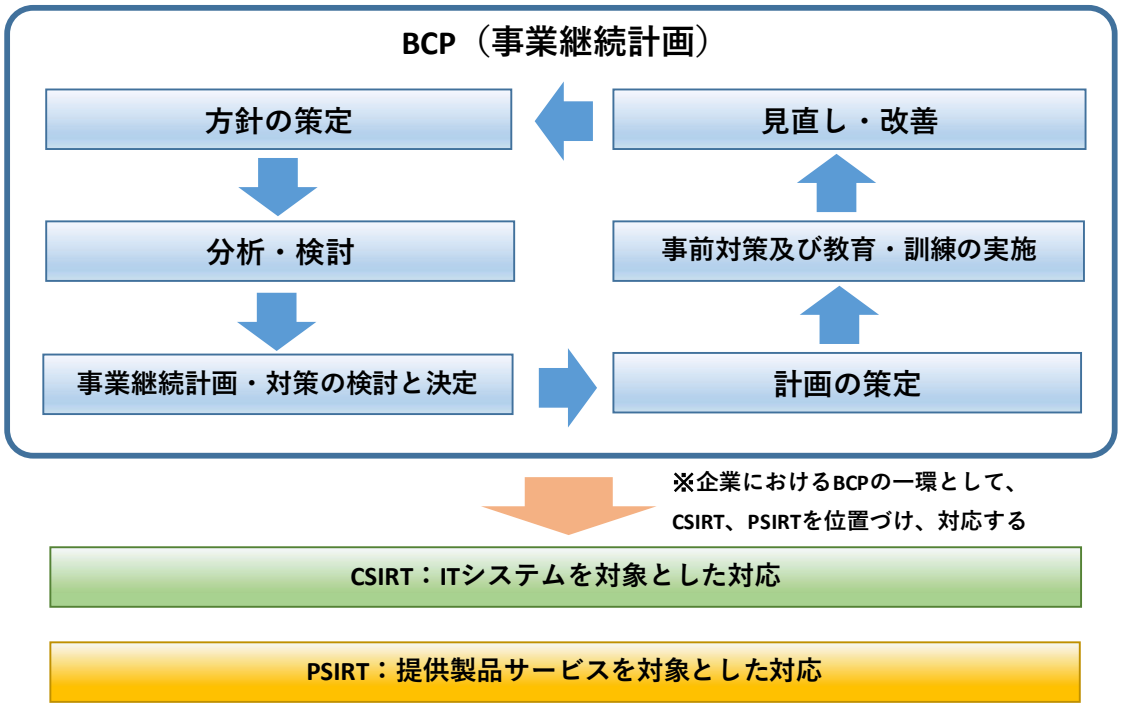


図 40　BCP における CSIRT、PSIRT の位置づけ

出典）内閣府 防災担当「事業継続ガイドライン　ーあらゆる危機的事象を乗り越えるための戦略と対応ー」[48]
2021 年 4 月公開版をもとに作図

[48] 内閣府　防災担当「事業継続ガイドライン　ーあらゆる危機的事象を乗り越えるための戦略と対応ー」（2021 年 4 月公開版）
https://www.bousai.go.jp/kyoiku/kigyou/keizoku/pdf/guideline202104.pdf

3-2 企業内、社外組織との情報連携方法の提言

3-2-1　PSIRT と CSIRT 及び外部連携のベースラインスキーム

PSIRT 組織における CSIRT 及び外部連携のベースラインのスキーム図を下記、図 41 に示す。ベースラインのスキームでは、製品提供企業を中心に、上流企業（＝ソフトウェアの調達先など）、下流企業（顧客・ユーザ企業など）との連携を示している。

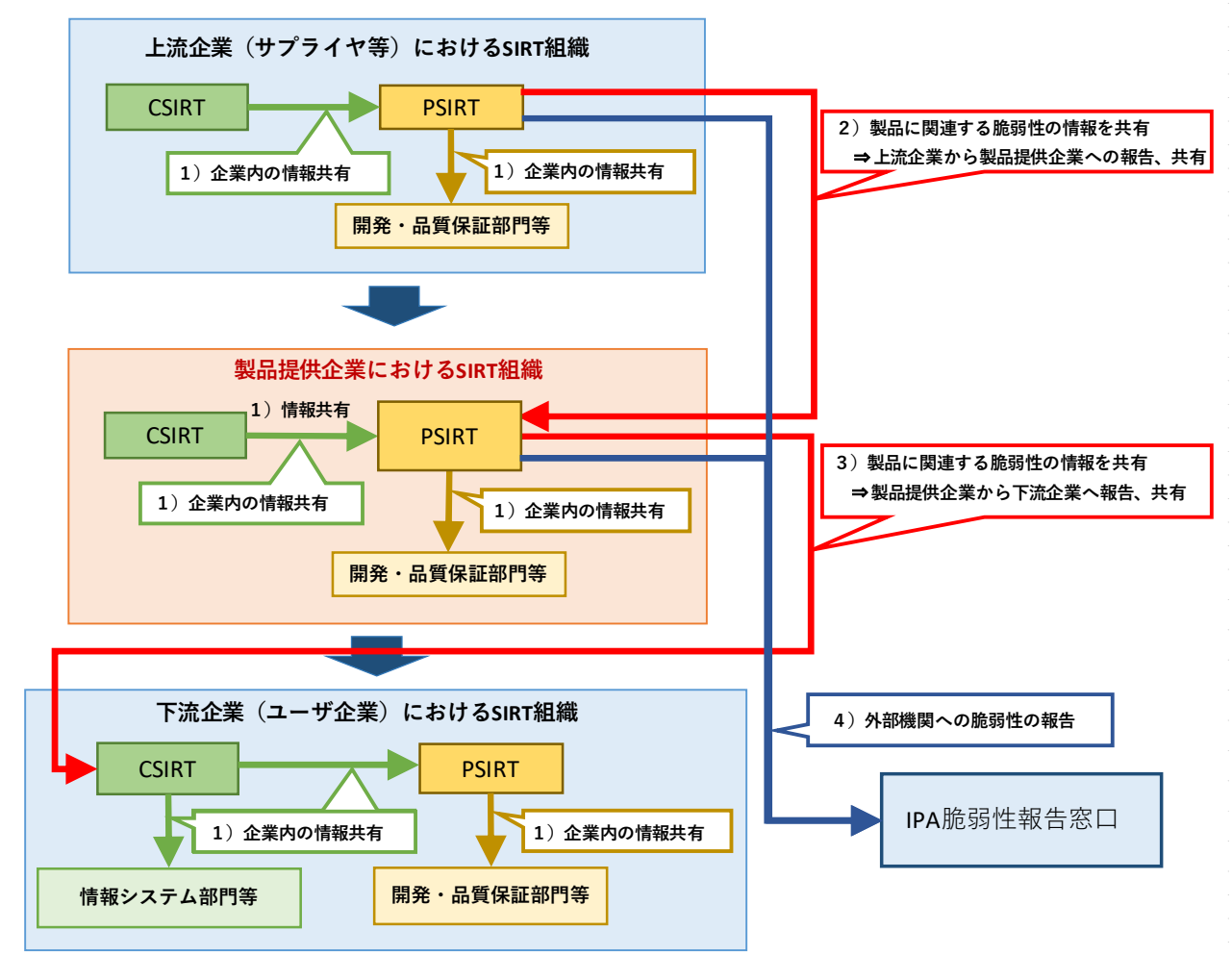


図 41　PSIRT と CSIRT 及び外部連携のベースラインスキーム

3-2-2.　PSIRT と CSIRT 及び外部連携のベースライン要求

前項のスキーム図（図 41）に記載した対応事項について、ベースラインとなる要求事項を以下に示す。

1）　企業内の情報共有

- インシデントや脆弱性、攻撃手法に関する情報は、各企業の CSIRT が収集した情報を、PSIRT へ情報共有を行う。
- PSIRT 組織は社内の関係ステークホルダ（開発部門・品質保証部門など）への情報共有を行う。
- CSIRT に該当する組織が組成されていない場合は、各企業の PSIRT 部門あるいは開発・品質保証部門が脆弱性情報データベースや、マスメディアのニュース、カンファレンスプログラムなどを活用し、自律的な情報収集を行う。

企業へのアンケート及びヒアリング結果では、調査対象企業の 80%より CSIRT から PSIRT へ情報共有されていない、もしくは CSIRT からの共有された情報が PSIRT 活動及び、品質の向上に活用されていないという課題があがっている。改善策として、CSIRT から PSIRT への情報共有を社内方針やプロセスとして定義し、実際に運用を行うことが必要となる。

2） 製品に関連する情報の報告、共有（上流企業⇒製品提供企業）

- 上流企業（ソフトウェアの調達先など）は、提供しているソフトウェアに関連する脆弱性や攻撃手法に関する情報を入手した時点で、製品提供企業へ報告、情報提供を行う。
- 製品提供企業は、上流企業との契約において、対象ソフトウェアの脆弱性に関する情報の提供や脆弱性への対策に関する情報提供、報告を含める形とする。
- 製品に OSS が利用されている場合は、関連する脆弱性情報の収集について、製品提供企業の PSIRT 部門あるいは開発・品質保証部門が脆弱性情報データベースや、マスメディアのニュース、カンファレンスプログラムなどを活用し、自律的な情報収集を行う。

企業へのアンケート及びヒアリング結果では、調査対象企業の 80%において、上流企業から脆弱性に関する情報の共有が行われていた。また 20%は上流企業から製品提供企業への情報共有が行われていない回答であったが、これは製品の主要なソフトウェアコンポ―ネントを内製で開発していることに起因しており、改善策として、本件に対応する課題はあがっていない。

3） 製品に関連する情報の報告、共有（製品提供企業⇒下流企業）

- 製品において影響が想定される脆弱性の情報について、製品提供企業から下流企業へ、今後の対応計画を含めた報告を行う。

企業へのアンケート及びヒアリング結果では、全ての調査対象企業において、顧客サポートの一環として、発生した問題はセキュリティ課題を問わず、下流企業（顧客）への報告プロセスが徹底されており、本件に対応する課題はあがっていない。

4） 外部機関への脆弱性の報告

- 外部への脆弱性報告の方針、プロセス（公開する脆弱性の判断基準、情報公開の範囲や内容、手段、意思決定者など）について、事前に詳細を定義しておく。
- IPA の脆弱性報告窓口などを活用し、外部コーディネーション機関（JPCERT/CC）へ製品の脆弱性に関する報告を行う。

企業へのアンケート及びヒアリング結果では、80%の調査対象企業において、社内の方針、ポリシーとして、外部への報告が必要な脆弱性やセキュリティ課題を報告するプロセスが整備されていた（ただし、これまでに報告が必要な事例がない企業も存在する）。また残りの 20%も詳細なプロセスの定義ができていないものの、脆弱性の指摘や報告を受けた場合には、対策内容を含め、外部への報告を実施している。

今回の調査対象企業では、適切な対応が行われており、多くの企業にとって模範となる事例となっている。

3-3 OSS 管理及び PSIRT 活動に関する提言

3-3-1　OSS 管理及び PSIRT 活動のベースラインスキーム

OSS 管理及び PSIRT 活動のベースラインのスキーム図を下記、図 42 に示す。
ベースラインのスキームでは、製品提供企業を例として、ベースラインスキームを定義しているが、このスキームは上流企業（＝ソフトウェアの調達先など）にも適用可能である。

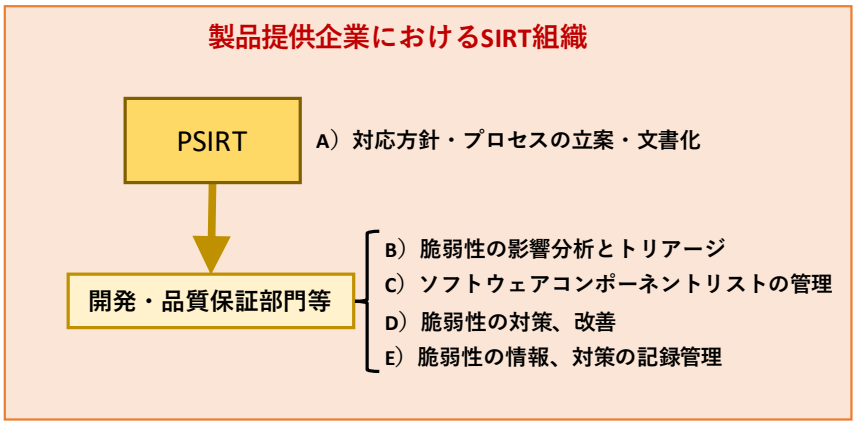


図 42　OSS 管理及び PSIRT 活動のベースラインスキーム

3-3-2　OSS 管理及び PSIRT 活動のベースライン要求

A）対応方針・プロセスの立案・文書化

・PSIRT において、社内関係部門と連携し活動する仕組みや体制を整備し、文書化する。
・一連の PSIRT 活動における各関係部門の役割や責任を定義し、文書化する。

企業へのアンケート及びヒアリング結果では、80%の調査対象企業において、社内関係部門と連携した PSIRT の仕組み、体制が整備、文書化されていた。20%の企業では、一部、公式な文書化について課題があがっていたが、改善策として上記に従い、社内の方針としてオーソライズされた文書を定義しておく必要がある。

B）脆弱性の影響分析とトリアージ

- 入手した脆弱性や攻撃方法の情報が製品に与える影響については、開発（設計）部門、品質保証部門などと連携し、分析及びトリアージを行う。
- 製品への影響分析の手順を文書化し、各部門で活用可能な共有の情報資産とする。
- 深刻な影響が想定されるセキュリティ課題は、最終的な対策方針、計画の最終判断を経営層あるいは、責任を有する意思決定者が行う。

※　脆弱性が悪用された場合に特定の組織に与える影響については、CISA[49]より、2022 年 11 月に”

[49] 米国サイバーセキュリティ・インフラストラクチャセキュリティ庁

Stakeholder-Specific Vulnerability Categorization Guide（SSVC）[50]”が公開された。3-3-3 項に参考情報として概要を掲載する。

企業へのアンケート及びヒアリング結果では、製品の影響分析について、60%の調査対象企業が、技術的あるいはコスト的な対応の難しさ、分析（特に検証）に利用可能なツールの不在（情報の不足）といった課題を抱えていることが明らかとなった。こうした課題への改善策は、製品提供企業による自助努力だけでは対応が難しく、企業間の枠組みを越えた外部との事例、情報共有や国や行政によるサポートも必要である。

C）ソフトウェアコンポーネントリストの管理

■SBOM の定義

- 脆弱性情報を入手した際に自社製品への影響の有無をすぐに判断できるよう、自社製品に使用されているソフトウェアコンポーネントリスト（SBOM）を管理する。自社内での管理だけではなく、下流企業における同様の管理のために製品とともに提供することも考慮に入れ、独自フォーマットではなく標準化フォーマットに準拠したデータフィールドの項目を満たす形式を定義する。

  （※）形式例）

  - NTIA “The Minimum Elements For a Software Bill of Materials”（1.2.3 項参照）のベースライン及び推奨データフィールドの項目を満たす形式を定義する。
  - 下記の標準化フォーマットに従ったデータフィールドの項目を満たす形式とする。

    （1.2.3 項参照）

    ・Software Package Data eXchange （SPDX） あるいは、SPDX Lite

    ・CycloneDX

    ・Software Identification （SWID） Tags

■SBOM の運用に関する取り決め

- 開発工程の中の製品をリリース段階で SBOM を作成するなど、どのタイミングで SBOM を作成および更新するかを定義し、既存のプロセスに組み込む。
- １つの SBOM データにどのレベルのコンポーネントまで SBOM に含めるかを定義する。あるコンポーネントが別のコンポーネントを含む場合、下位のコンポーネント情報まで SBOM に含めるか、下位のコンポーネントに依存しているという情報を残して、下位のコンポーネント情報は別の SBOM データとして提供するかを定義する。
- SBOM を下流企業に提供する方法を定義する。SBOM データ自体の機密性や完全性の担保を必要に応じて考慮する。

[50] CISA ”Stakeholder-Specific Vulnerability Categorization Guide”
https://www.cisa.gov/uscert/ncas/current-activity/2022/11/10/cisa-releases-ssvc-methodology-prioritize-vulnerabilities

■SBOM の運用

- 上流企業に対しても、製品提供企業が定義した形式、もしくは整合を行った形式によるコンポーネントリストの提出や管理を要求する。
- IT を活用した管理の自動化による運用方針を計画、実施することが望ましい。
  例）対応例
  - コンポーネントアナライシスツールを活用し、CD/CI 環境と連携した不具合管理、バージョン管理、ソフトウェアのビルド管理、トラッキングなどを一貫して実施できる仕組み …など。
- ただし、現時点で SBOM を運用していない企業において最初から管理の自動化を進めるのは負荷が高く、かえって導入が進まないことも考えられるため、段階的に対応を進めるのが望ましい。表 26 に自社内のコンポーネント情報を手動管理する場合から始め、サプライチェーン連携や自動化を進める場合の対応例をマトリックスで示す。

表 26　段階的な SBOM 管理例

	自社内管理	→	サプライチェーン連携
手動管理	・将来の自動化やサプライチェーン連携を考慮し、標準化された SBOM フォーマットに準拠した形で、自社で必要なコンポーネント情報を定義する。データはエクセル形式など社内で扱いやすい形式でよい。 ・SBOM を生成/更新するタイミングを取り決めてそれに従って運用する。		・自社と上流企業や下流企業との間でやり取りする SBOM フォーマットと最低限必要なコンポーネント情報を取り決める。やり取りするデータはエクセル形式など双方の企業で扱いやすい形式でよい。 ・上流企業や下流企業と SBOM を受けわたすタイミングや方法を取り決めてそれに従って運用する。
↓			
自動化	・SBOM データベースを構築する。 ・CD/CI 環境と連携し、ビルドと同時に SBOM データを生成/更新する仕組みを導入する。		・自社と上流企業や下流企業との間でやり取りする SBOM の電子フォーマット（例：SPDX Lite/JSON）を取り決める。 ・上流企業から入手した SBOM を自社の SBOM データベースに反映する仕組みを構築する。

企業へのアンケート及びヒアリング結果では、調査対象企業の 80%がソフトウェアコンポーネントのリスト管理に課題を抱えており、部門別に独自のフォーマットが利用され、エクセルによる管理運用が中心に対応されている。また調達したソフトウェアに予期せぬ OSS が内在した事例も確認されており、改善策としては、企業内及び、サプライチェーン間で効率的な管理が行なえるよう標準化フォーマットに準拠した形式の定義し、将来的には自動化（ＩＴ化）を想定した計画を検討することが必要である。

D）脆弱性の対策、改善

- 製品への影響分析を踏まえ、対応が必要とされる脆弱性については、上流企業あるいは製品提供企業による対策、改善を行い、アップデートプログラムの提供などの対応を計画、実施する。
- 製品提供企業は、上流企業との契約において、検出された脆弱性に対するアップデートプログラムの

提供を含める形とする。

- 製品提供企業は、下流企業の製品に対するアップデートプログラムの提供あるいは、アップデートの実行を行う。
- アップデートの対応については、製品提供企業の責任範囲を明確化するため、保守サポートの条件を、契約事項として下流企業及び、上流企業と事前合意しておく。
- 製品に OSS を活用している場合は、上記の脆弱性対策について、製品提供企業が自ら対応を行う必要がある。

保守サポート契約における考慮事項）

① 製品提供企業における保守サポートの対応期間を明確化する。

② 責任分解点を明確化し、確認しておく。

③ 製品提供企業の責任としてサポートすべき範囲を明確化する。

例1） 製品やサービス及び、利用しているソフトウェアコンポーネント（OS や OSS を含むソフトウェアなど）で確認された脆弱性に対して、リスクの影響度、深刻度によりサポート対象を明確化する。

例2） 自社開発以外のソフトウェアコンポーネントを利用している場合には、現行のバージョンだけでなく、遡って対応が可能なバージョンの範囲を明確化する。

例3） 対象分野において対応が求められる法制度や規格、デファクト基準をもとに対応すべき要件や範囲を明確化する。（クレジットカード情報の漏洩など、製品提供企業側の重過失に該当する問題については、契約上の損害賠償上限を超えた賠償額を認められた判例がある。）

※ 保守サポートの範囲については、将来的なリスクに対して、その影響やコストを対費用効果の観点から、明確化することが重要である。製品提供企業側とユーザ企業側で想定リスクや対応費用について、充分にコミュニケーションを行い、事前同意しておく事が双方のビジネスに取って有益である。製品提供企業側は将来的なリスクへの説明責任を果たせると同時に、ユーザ企業側はリスクを認識した上で費用や対応範囲に同意することでトラブル防止につながる。またその際のコミュケーションツールとして SBOM を活用することで内部構成に基づくより具体的な協議が行なえる効果を期待できる。

企業へのアンケート及びヒアリング結果では、脆弱性の発見、報告に伴い、60%の調査対象企業で迅速な対応が行なえるようプロセスや仕組みの整備、文書化が行われていた。残り 40%の企業では、文書化について一部課題を抱えているものの、プロセスや仕組み自体は整備されており、大きな課題は確認されていない。

E）脆弱性の情報、対策の記録管理

・報告、発見された脆弱性の件数や CWE 分類、対策の状況などを記録として整備、管理を行い、事後の共有や分析、追跡に活用できる仕組みを整備する。

企業へのアンケート及びヒアリング結果では、脆弱性の情報や実施した対策の記録（データベース化）については、全ての調査対象企業が、対応に課題を抱えていることが明らかとなった（製品のセキュリティ課題の数が少なく、データベースを構成できるほど件数が集まっていないケースを含む)。課題への改善策としては、脆弱性の報告を行うためのフォーマットを整備し、データベースとして情報の蓄積、共有環境を整備することが必要となる。

3-3-3　参考）脆弱性の影響分析とトリアージの手法や情報

■Stakeholder-Specific Vulnerability Categorization Guide（SSVC）

脆弱性の影響分析とトリアージに関する手法としては、2022 年 11 月に CISA より” Stakeholder-Specific Vulnerability Categorization Guide（以下、SSVC）”が公開された。以下に参考情報としてその概要を示す。

SSVC は脆弱性が悪用された場合に特定の組織に与える影響に基づいて、脆弱性の是正に優先順位をつけることを支援するものであり、下記表 27 に示す通り、「Track」、「Track*」、「Attend」、「Act 」の 4 段階評価に分類することができる。

表 27　SSVC における脆弱性の決定、想定される結果

Track	現時点では、この脆弱性に対処する必要はない。 組織は引き続き脆弱性を追跡し、新しい情報が利用可能になった場合に再評価を行う。CISA は、Track に該当する脆弱性を標準的な更新スケジュール内で是正することを推奨する。
Track*	この脆弱性には特定の特性が含まれており、その変化についてより綿密な監視が必要な場合がある。CISA は、Track* に該当する脆弱性を標準的な更新スケジュール内で是正することを推奨する。
Attend	この脆弱性は、組織内部の監督者レベルの個人による注意を必要とする。必要な措置には、脆弱性に関する支援や情報の要求が含まれ、脆弱性に関する通知を社内外に公表することが含まれる場合がある。CISA は、Attend に該当する脆弱性を標準的な更新スケジュールよりも早期に是正することを推奨する。
Act	この脆弱性は、組織内部、監督者レベル、および指導者レベルの個人による注意を必要とする。必要な対応としては、支援や脆弱性に関する情報の要請、社内外への通知などがある。通常、社内のグループは、全体的な対応策を決定するために会議を開き、合意した対応策を実行することになる。CISA は、Act に該当する脆弱性をできる限り早期に是正することを推奨する。

脆弱性の影響を判断する決定については、「攻撃の状態」、「技術的影響」、「攻撃の自動化の状況」、「ミッションの普及率」、「社会的な影響（パブリックウェルビーイング)」の 5 つの因子で構成され、デシジョンツリー（図 43）もしくは、優先順位表をもとに最終的な影響が判定される。

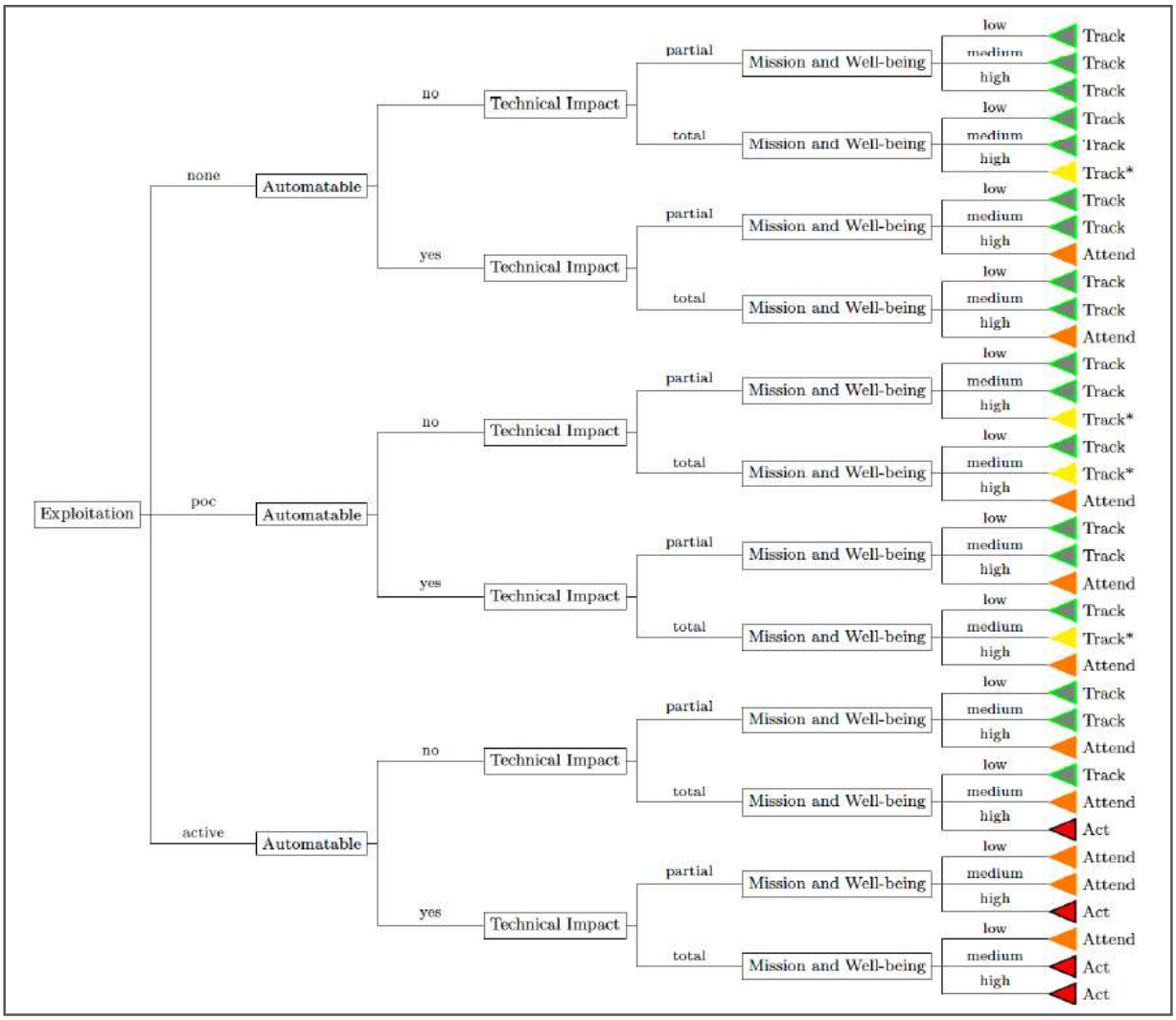


図 43　SVCC が定義するデシジョンツリー

出典）CISA "Stakeholder-Specific Vulnerability Categorization Guide"

■既知の悪用された脆弱性カタログ（known exploited vulnerabilities catalog）

CISA からは SVCC 以外に 2021 年～2022 年に実際に IoT 製品において悪用が確認され、早期の対応が求められる既知の脆弱性のカタログ（"known exploited vulnerabilities catalog"[51]）が公開されている。図 44 は、上記のカタログをもとに、脆弱性が報告された対象の製品について、件数の多い上位 30 位をグラフ化したものである。ランクの上位には、Windows や iOS といった OS に加えて、OSS もあげられており、製品に利用されるソフトウェアコンポーネントにおいて、危険性を判断するための情報として活用することができる。

[51] CISA "known exploited vulnerabilities catalog"
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

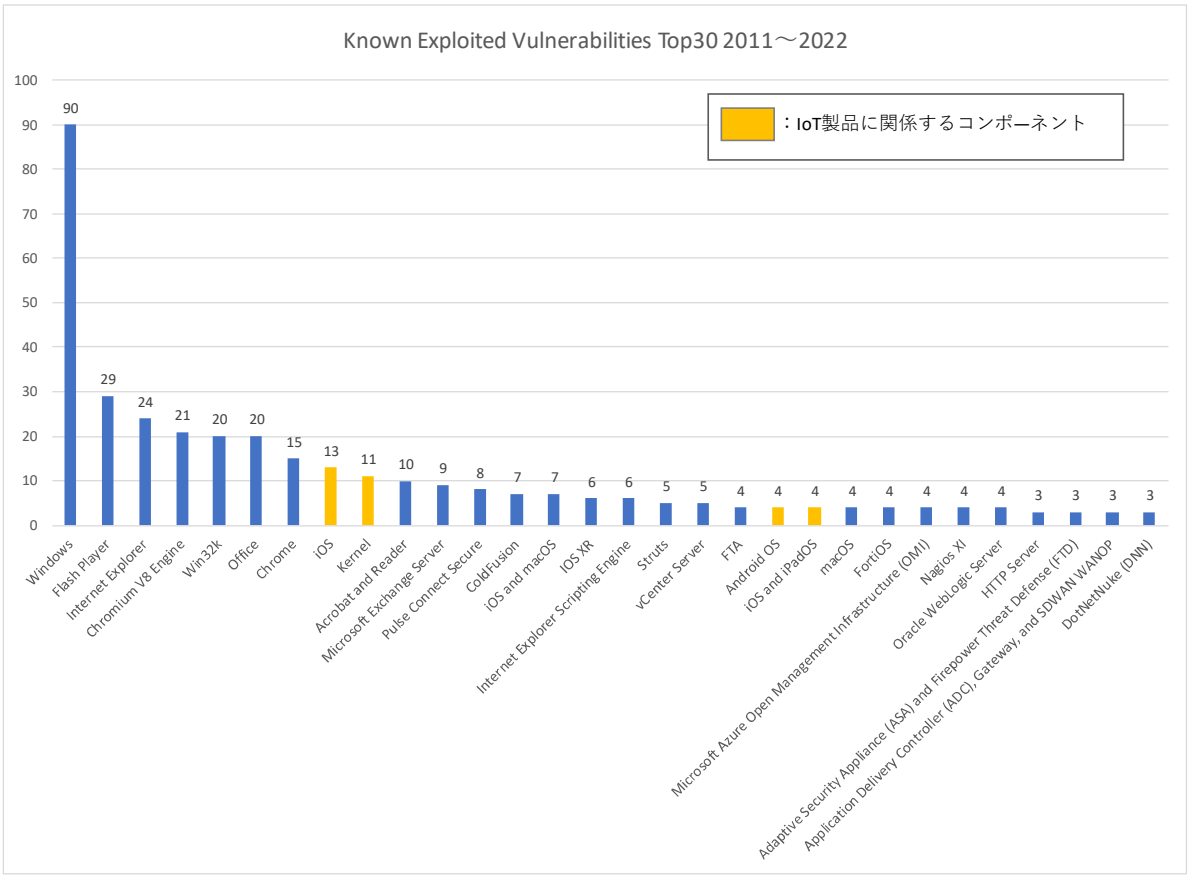


図 44　Known Exploited Vulnerabilities Top30 2011～2022

出典）[CISA]Known Exploited Vulnerabilities を元に、脆弱性の報告対象製品（Top30）をグラフ化

3-4　国や行政による支援についての提言

最後に企業へのアンケートやヒアリング調査から得られた結果を踏まえ、国や行政による PSIRT 活動の支援について提言を示す。

3-4-1　PSIRT 活動における詳細なガイドラインの発行、トレーニング・教育プログラムの策定

[現状の課題]

PSIRT 活動については、JPCERT/CC からは”PSIRT Services Framework”が翻訳、公開されており、PSIRT に求められる活動の指針として、非常に有用な文献となっている。一方でアンケート及びヒアリング結果では、調査対象企業全体で PSIRT のトレーニング・教育に関する自己評価が低い結果となった。企業からは、特にトレーニング・教育に関する以下の点について課題が多く、更に具体的かつ詳細なガイドライン文書のリリースが望まれていると考えられる。

[更に詳細なガイドラインが必要な事項]

■PSIRT の役割や目的

- 製品のライフサイクルのプロセスに沿って、企業の関連部門が果たすべき役割や責任をコンパクトに図示、一覧化したガイドライン文書。

■技術的な内容

- CSIRT で収集した脆弱性や攻撃手法について、製品への影響を分析、トリアージの指針や手順を示す文書発生した脆弱性の対応結果を追跡するための手法や、ツールの紹介や対応事例の紹介文書。
- ソフトウェアコンポーネントの管理方法について、標準化フォーマットの紹介や国内の対応事例、SBOM による自動化、IT 化の事例やメリット、デメリットを解説した文書。
- ソフトウェアコンポーネント（OS や OSS を含むソフトウェアなど）において、市場での普及率や、実際に攻撃が発生した状況、攻撃対象として狙われやすいコンポーネントの予測などの統計情報や解析結果のテクニカルレポート。

[今後の対策についての提言]

- 上記の事項については、企業の枠組みを越えた対応が必要であり、国や行政の関係団体がガイドライン文書の発行や、それに対応するトレーニング・教育プログラムを策定することで、各企業における PSIRT の目的や意義の浸透や、サプライチェーンのセキュリティ対策に関する普及啓発の促進や教育効果の向上に寄与するものと考えられる。また CSIRT では、一般社団法人 日本シーサート協議会[52]が、定期的にワークショップなど開催し、活動で得た知見を参画メンバーへ共有、啓発する機会を提供している。また、IoT 製品に利用されるソフトウェアコンポーネントの脆弱性は、JVN iPedia などで個別情報が公開されている。過去のデータをもとにコンポーネントの普及率や、実際に攻撃が発生した状況（件数や割合）、攻撃対象として狙われやすいコンポーネントの予測（注目度）などを統計情報や解析結果としてテクニカルレポートが発行されると製品提供企業やユーザ企業の基礎知識として有益なのではないか。

[52] 一般社団法人 日本コンピュータセキュリティインシデント対応チーム協議会
https://www.nca.gr.jp/

情報を整理すると、PSIRT に関係し、特に以下のような支援及び施策が必要であろう。

1. PSIRT ガイドラインの策定
2. トレーニング・教育プログラムの策定
3. ワークショップ・講習会の開催
4. ソフトウェアコンポーネントの脆弱性の悪用状況や攻撃対象予測などのテクニカルレポート

上記の施策を通じて、企業における PSIRT 活動成果の向上効果、及び個社が蓄積した知見、経験の共有により、国内全体の活動水準を高める効果が期待できるものと考える。

3-4-2　コンポーネントアナライシスツールの開発及びオープンソース化

[現状の課題]

アンケート及びヒアリング結果において、組込み機器に対応した脆弱性の診断ツールや、ソフトウェアコンポーネントのアナライシス（分析）ツールへの要望が数多くあがっていた。IoT 関連機器の中でも、特に組込み機器に利用可能なソフトウェアコンポーネントの分析ツールは、いずれも海外製であり、国内製のツールが存在しないため、機密保持の観点から利用のハードルが高いという課題がある。またツールの機能としては、いずれも製品に内在するソフトウェアコンポーネントの解析や、脆弱性の検出、SPDX などの標準化方式に対応した SBOM の自動生成など、必要機能を十分備えているものの、商用製品であるため高額であるという課題もある。

[今後の対策についての提言]

国内製のソフトウェアコンポーネントの分析ツールを国や行政主導で開発し、オープンソースあるいは低額な費用で利用できる形であれば、多くの企業にとってサプライチェーンのセキュリティ対策を行う上で有益であり、また対策の普及促進に寄与するものと考えられる。

OSS 管理及び CSIRT・PSIRT 連携調査検討委員会　構成員名簿

議長	荻野 司	一般社団法人　重要生活機器連携セキュリティ協議会 代表理事 情報セキュリティ大学院大学　客員教授
委員	秋本 諭史	株式会社サイバーナレッジアカデミー セキュリティコンサルティング部
委員	落合 正人	SOMPO リスクマネジメント株式会社 サイバーセキュリティ事業本部
委員	木田 良一	株式会社ラック　デジタルイノベーション統括部 デジタルペンテスト部
委員	佐藤 俊介	大日本印刷株式会社 情報イノベーション事業部 PF サービスセンター　セキュリティソリューション本部 マーケット開発部
委員	柴田 秀行	富士ソフト株式会社　ソリューション事業本部 インフラ事業部　セキュリティソリューション室
事務局		一般社団法人 重要生活機器連携セキュリティ協議会

2. 研究発表・講演、文献、特許等の状況

（1）研究発表・講演

なし

（2）論文

なし

（3）特許等（知財）

なし

（4）受賞実績

なし

（5）成果普及の努力（プレス発表等）

なし

契約管理番号：	22101190-0