セキュリティ・トランスペアレンシー・コンソーシアム

活動成果

# 「可視化データの実践活用に向けて～実務者向け～」

2026 年 7 月 15 日

セキュリティ・トランスペアレンシー・コンソーシアム

# 目次

# 1　はじめに

## 1.1　セキュリティ・トランスペアレンシー・コンソーシアムの活動について

セキュリティ・トランスペアレンシー・コンソーシアムは、「サプライチェーンを通して複雑化しているシステムやサービスの透明性を高め、安全安心な仕組みを構築する」ことを目的として設立された、業界横断的な活動体である。製造業、IT・ソフトウェア、インフラ、サービス業など多様な業種の事業者が参画し、サプライチェーン全体に関わる可視化データの活用促進に向けた「知見の共創」に取り組んでいる。

本コンソーシアムは、サプライチェーン横断的な透明性の確保に向けた実践的な知見を集積・体系化し、業界全体の底上げに貢献することを活動の核心に据えている。個社の枠を超えた協調によって、データ生成・共有・活用に関する課題を共同で検討し、そこから得られた知見をコンソーシアム内外に広く発信することが、本コンソーシアムの社会的役割である。本知見集は、そのような活動の成果の一つとして位置づけられる。

本コンソーシアムのこれまでの主要な成果として、2024 年 2 月に活動ビジョン「セキュリティ透明性の向上と活用に向けて」を公表し、可視化データを「つかう側」の事業者（調達部門・システム運用部門・セキュリティ部門等）が直面する問題・課題と対処の方向性を体系的に示した。さらに同年 10 月には、脆弱性管理という具体的なユースケースに焦点を当て、可視化データを「つかう側」が直面する問題・課題（フォーマット・データ品質評価、技術・ツール活用、活用コスト、継続的活用、サプライチェーン上の調整、可視化データがもたらす影響）に対処するための知見を共創し、知見集「セキュリティ透明性確保に向けた可視化データ活用～脆弱性管理編～」として公表している。また、本コンソーシアムでは 2026 年 3 月に経営層向け提言書として、「可視化データによるサイバーセキュリティ透明化とガバナンス強化」も公表している。本知見集は、これら一連の活動の継続として位置づけられる。

2024 年 10 月公表の知見集において脆弱性管理における可視化データの活用価値が示されたが、同時に実務での活用をさらに深めるためにはどうすればいいのかといった課題が残っていた。本知見集では、こうした認識のもと、可視化データそのものに求められる要素を体系的に整理し、データの「生成・共有・活用」の各段階における課題や実践知見を提供することで、サプライチェーン横断での実用化をさらに前進させることを目指す。

## 1.2　サプライチェーン上のセキュリティ透明性とは何か

サプライチェーン上のセキュリティ透明性とは、「サプライチェーンを通して開発・提供される機器やシステムの構成・依存関係・セキュリティ状態・取引関係などを、関係者が必要に応じて参照・活用できる状態にすること」を指す。それは単に情報をデジタル化することではなく、必要な主体が必要な情報に適切なタイミングでアクセスし、意思決定や対応に活用できる状態を実現することを本質としている。

「安全安心な仕組み」が示すべき態様は、特定の組織や局面に限定されない。調達・製造・流通・

利用にわたる複数の組織が連携し、それぞれの段階で必要な情報が生成・共有・更新される継続的な仕組みこそが、サプライチェーン全体の透明性を支える基盤となる。

この透明性は、SBOM（Software Bill of Materials）の生成といった特定の技術的手段に尽きるものではない。ソフトウェア構成情報にとどまらず、ハードウェア構成、取引先のセキュリティ状態、システム間の依存関係、BCP・復旧情報など、組織がサプライチェーン上のリスクを適切に管理するために必要な情報全般が透明性の対象となる。

## 1.3　現状認識:サプライチェーン全体のセキュリティ課題

こうした状況の中で、脆弱性管理はもはや自社だけで完結する問題ではなくなっている。関連するサプライヤー・ベンダー・インテグレーター・ユーザー事業者が連なるサプライチェーン全体の安全性を確保することが、脆弱性管理を高度化する上で不可欠となっている。実際に、ソフトウェアの依存関係が把握できず脆弱性の影響範囲を特定できなかった事例、取引先のセキュリティ状態が見えずに攻撃が伝播した事例、復旧に必要な情報が整備されていなかったために被害が拡大した事例など、必要な情報の可視化不足が深刻な影響をもたらした事案が多数報告されている。第 3 章では、これらの代表的な事例を詳しく分析する。

# 2　本コンソーシアムで捉える可視化データとは何か

## 2.1　背景・目的

近年、製品やシステムのサプライチェーンが複雑化・グローバル化する中で、単一の組織が自社内だけでセキュリティを完結させることは現実的でなくなっている。地政学リスクの高まりや経済安全保障の観点から、特定国のコンポーネントや技術への依存リスクを把握・管理することの重要性が増している。また、ESG の観点では、サプライチェーン全体を通じた社会的責任の透明性が求められ、投資家や顧客からの開示要請も強まっている。

規制面でも、EU のサイバーレジリエンス法（CRA）やデジタルプロダクトパスポート（DPP）、国内の経済安全保障推進法など、サプライチェーンに関わる制度的枠組みが相次いで整備されている。これらの規制は、製品の構成情報や脆弱性対応状況について、単なる自社管理にとどまらず、サプライチェーン全体を通じた可視化と開示を求めるものである。

こうした背景から、本コンソーシアムでは「サプライチェーン横断の可視化データ」を中心的なテーマとして位置づけている。自組織の境界を越えて、調達・製造・流通・利用にわたるサプライチェーン全体で、どのような情報を、どの形式で、誰が責任を持って管理・共有するかを問い直すことが、本知見集の出発点である。

本知見集の作成にあたり、2025 年 5 月に WG メンバー企業（製造業・電気通信業・サービス業等）を対象としたアンケートを実施した。SBOM の作成・活用状況や課題等を把握し、本知見集の課題・知見の整理に反映している。アンケートの詳細については付録 A を参照されたい。

## 2.2　概念整理

本章で扱う用語について、混乱を避けるため以下のとおり整理する。

「サプライチェーン横断」とは、自社内にとどまらず、原材料・部品の調達先から最終ユーザーまでの複数組織にわたる連鎖全体を対象とすることを指す。単一ベンダーとの二者間関係ではなく、多段階にわたる調達・開発・製造・提供の連鎖を視野に入れる点が特徴である。

「可視化データ」とは、サプライチェーンを通じたシステムや製品の構成、依存関係、セキュリティ状態、取引関係などを、組織間で参照・共有・活用できる形式に整理した情報の総称である。SBOM はその代表例であるが、可視化データの概念は SBOM に限定されない。ハードウェア構成情報、取引先のセキュリティ対策状況、システムの依存関係マップ、BCP/BIA 情報、連絡先・契約情報なども、文脈に応じた可視化データに含まれる。

「可視化」と「データ化」は混同されることがあるが、本知見集では区別して用いる。データ化とは情報をデジタル形式で記録・保存することを指し、可視化とはそのデータが必要な主体によって参照・判断に活用できる状態にあることを指す。データが存在しても、参照できない・使いこなせない状態では、可視化されているとはいえない。

「安全安心な活用」とは、データに電子証明書が付与されているだけで達成されるものではない。データが実態と一致しており（品質）、出所と流通過程が確認でき（真正性）、緊急時にすぐ活用できる形式で（適用性）、改ざんされていないことが検証でき（完全性）、最新の状態に維持されている

（運用性）という 5 つの観点が揃って初めて、安全安心な活用が実現する。これらの要素については第 4 章で詳述する。

## 2.3　対象とスコープ

本知見集が対象とするサプライチェーンは、製造業、IT・ソフトウェア、サービス業など、複数組織が連携してシステムや製品を開発・提供するあらゆる業種を含む。特定の業界や技術に限定せず、脆弱性管理の観点からサプライチェーン横断の可視化が求められる状況を幅広く対象とする。

対象とするライフサイクル範囲は、設計・調達・製造・流通・利用・廃棄・リサイクルの全段階にわたる。ただし、本知見集が特に重点を置くのは、脆弱性管理の実務において可視化データが活用される「利用」段階と、可視化データが生成・共有される「製造・調達」段階である。脆弱性が顕在化した際に迅速な影響特定と対応が求められる局面で、どのような可視化データがどの段階で整備されている必要があるかを意識して整理する。なお、本知見集は経済産業省が公表している「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」（以下「経産省 SBOM 手引」という）や前回知見集（脆弱性管理編）と相互補完的な関係にあり、SBOM を活用した脆弱性管理プロセスの全体像を把握したい読者は経産省 SBOM 手引を先に参照した上で本知見集を活用されたい。

## 2.4　既存フレームワークとの関係

本コンソーシアムの取り組みは、既存の品質保証・セキュリティ管理のフレームワークと独立したものではなく、それらを補完・拡張する位置づけにある。

品質保証の観点では、製品の品質管理プロセス（ISO 9001 等）において、サプライヤーに関する情報管理が求められてきた。可視化データはこの延長上にあるが、セキュリティの観点から対象情報の種類と更新頻度に対する要求水準が異なる点に注意が必要である。例えば、品質管理では半期ごとのサプライヤー評価記録で足りる場合でも、セキュリティの観点では重大脆弱性公表後数日以内の SBOM 更新が求められるなど、更新頻度・粒度・形式の要求が大きく異なる。

PSIRT（Product Security Incident Response Team）・CSIRT（Computer Security Incident Response Team）などのインシデント管理の観点では、脆弱性公表時の迅速な影響範囲特定と対応に可視化データが直接活用される。構成情報（SBOM はその代表的な形式の一つ）が整備されていれば、PSIRT による影響調査を大幅に効率化できる可能性がある。

CISO・SOC（Security Operations Center）などのサイバーセキュリティ管理の観点では、サプライチェーンを通じたリスクのモニタリングに可視化データが役立つ。特に取引先のセキュリティ状態に関する情報は、組織全体のリスク評価において重要な位置を占める。

コンプライアンスの観点では、CRA・DPP・経済安全保障推進法などの規制が SBOM や構成情報の整備・開示を求める方向に動いており、本知見集で整理する可視化データの実践がそのまま規制対応の基盤にもなり得る。ただし、各規制の要求仕様は異なるため、規制ごとの個別対応も必要である。また、経産省の SBOM ガイドラインや JC-STAR など国内制度との整合性についても、図 図 1 に示す可視化データの活用関係を踏まえながら、参照先として活用されたい。

## 2.5　脆弱性管理に役立つ可視化データに求められる要件

可視化データが脆弱性管理において実際に役立つためには、単に情報が存在するだけでは不十分であり、以下の要件を満たすことが求められる。

第一に、対象の網羅性である。脆弱性が検出された際に「影響を受けるシステムやコンポーネントが自組織内に存在するか」を迅速に判断するためには、可視化データが対象システム・コンポーネントを漏れなく含んでいる必要がある。網羅性に欠けると、影響範囲の特定が不完全になり、対応の抜け漏れが生じる可能性がある。

第二に、実態との一致である。可視化データは作成時点の情報を記録したものであり、システム構成の変更・更新が反映されていなければ、古い情報に基づいた誤った判断を招く可能性がある。継続的な更新の仕組みを組み込むことが重要である。

第三に、活用しやすい形式である。緊急時に人手で大量のドキュメントを検索することは現実的ではない。SBOM であれば CycloneDX や SPDX 等の標準フォーマットへの準拠、脆弱性データベース（NVD 等）との連携により、自動的な影響特定が可能になる。

第四に、情報の信頼性である。サプライヤーから提供されたデータが改ざんされていないか、実際の構成を反映しているかを検証できる仕組みが求められる。電子署名やハッシュ値による検証がその手段となる。

これらの要件を一度にすべて満たすことは容易ではなく、組織の状況に応じて段階的に整備していく現実的なアプローチが求められる。第 5 章では、これらの要件を実現する際に生じやすい課題と対処の知見を整理する。

## 2.6　本知見集の目的と対象読者

本知見集は、SBOM の取得・提供を前提とした技術仕様書ではなく、サプライチェーン横断の可視化データをいかに実務に根付かせるかについての実践的な知見を提供することを目的としている。SBOM は可視化データの重要な形式の一つであるが、本知見集の射程は SBOM に限定されず、より広義の可視化データ全般を対象とする。

本知見集が念頭に置くサプライチェーンの関係者は、大きく 4 者に分類される。①サプライヤー（部品・コンポーネントを提供する側）、②ベンダー（製品・サービスを開発・販売する側）、③インテグレーター（システムを組み合わせて提供する側）、④ユーザー事業者（最終的に利用・運用する側）である。これら 4 者はそれぞれ立場が異なり、可視化データに求める情報の種類・詳細度・更新頻度も異なる。本知見集は特定の立場に限定せず、各立場からの課題と知見を横断的に整理している（図 図 1）。なお、図 図 1 の脆弱性管理プロセスの作成にあたって、経済産業省が公表している「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引（以下「経産省 SBOM 手引」という）」を参照している。同手引は、SBOM を活用した脆弱性管理プロセスの全体像を（(1)脆弱性特定、(2)脆弱性優先付け、(3)脆弱性共有、(4)脆弱性対応の 4 段階として）体系的に示しており、本知見集では、可視化データとして必要な要素をあぶり出す際の分析枠組みとして参照した。なお、本知見集が扱う SBOM のライフサイクル（作成・共有・活用）と同手引が対象とする脆弱性管理プロセスとは視点が異なるため、本知見集の各知見が同プロセスの特定ステップに

一対一で対応するわけではない点に留意されたい。[1]

なお、本知見集のタイトルに含まれる「実務者」とは、サプライチェーン上のセキュリティ透明性確保に関わる現場の担当者・責任者を指す。具体的には、可視化データの生成・管理・活用に直接携わる開発担当者、PSIRT や CSIRT の担当者など、組織内でデータを実際に扱う立場にある者を想定している。経営層向けの判断・方針策定を主目的とした読み物ではなく、現場での実践に役立てることを主眼に置いている点で、本知見集は「実務者向け」と位置づけている。

想定する読者は、以下の 3 つのロールを念頭に置いており、開発担当のセキュリティ責任者、および CISO 配下の CSIRT・PSIRT の実務責任者を主な想定読者としている。

開発担当は、製品・システムの構成情報の生成・管理や、SBOM をはじめとする可視化データの作成・更新に関わる立場である。本知見集では、特に第 5 章のデータ生成段階に関する課題整理が参考となる。

PSIRT 担当（図 図 1 のベンダーにあたる立場のセキュリティ担当者）は、自社製品に関する脆弱性情報の収集・分析・対応調整を担う立場である。脆弱性公表時の影響範囲特定や顧客・ステークホルダーへの情報提供において可視化データを活用する。第 3 章の事例分析と第 4 章の要素整理が特に参考になる。

CSIRT 担当（図 図 1 のインテグレーター・ユーザー事業者にあたる立場のセキュリティ担当者）は、組織内のインシデント対応を担う立場である。攻撃発生時の影響範囲特定・封じ込め・復旧において可視化データを参照し、また取引先のインシデントが自組織に与える影響を評価する。第 3 章および第 5 章のデータ活用段階の課題が特に参考になる。

1 経済産業省「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0」, 2024 年 8 月.https://www.meti.go.jp/policy/netsecurity/wg1/SBOMv2.pdf


図 1：サプライチェーンにおける脆弱性管理と可視化データの関係性

# 3　可視化が求められる事例と可視化するデータ

## 3.1　事例分析の枠組み

本章では、可視化データの不備が実際のセキュリティインシデントにどのような影響を与えたかを、3 つの代表的な事例を通じて分析する。各事例は、可視化が不十分であったことで被害が拡大した局面が異なり、それぞれ異なる観点から「どのようなデータが必要だったか」を示している。

事例①（Log4j 脆弱性対応）は、ソフトウェア構成の可視化が不十分な状態で深刻な脆弱性が公表されたとき、影響範囲を迅速に特定できなかったことを示す事例である。事例②（サプライチェーン攻撃）は、取引先のセキュリティ状態が見えていないことで、自社が被害を受ける前にリスクを把握できなかったことを示す事例である。事例③（医療機関ランサムウェア攻撃）は、システムの依存関係や復旧手順が整理されていなかったことで、攻撃後の復旧判断が遅れた事例である。

各事例は「事例概要」「何が問題だったのか」「必要だった可視化データ」「学び」の 4 つの視点で分析する。この分析の結果は、第 4 章で可視化データに求められる共通要素を導出する際の根拠となる。

また、可視化データに対する要求は一様ではなく、利用する主体（例：CSIRT/PSIRT の実務責任者、調達、IR 等）や、その主体が担う意思決定・対応フェーズによって必要となる情報粒度や観点が異なる。本知見集ではまず共通する論点として可視化データの必要性を整理したうえで、各主体が置かれる状況に応じて参照すべき観点が変わり得ることを前提として議論を進める。

例えば、CSIRT 担当（インテグレーター・ユーザー事業者側）は、インシデント発生時に「自組織のどのシステムが影響を受けるか」を即座に判断するための構成情報・依存関係マップを必要とする。一方、PSIRT 担当（ベンダー側）は、脆弱性公表時に「自社製品のどのバージョンが影響を受けるか」を顧客・ステークホルダーに迅速に伝えるための詳細なコンポーネント情報を必要とする。さらに調達担当は、取引先選定や契約更改の場面で「サプライヤーのセキュリティ対策状況」や「取引依存度」を確認するための情報を必要とする。このように、同じ可視化データであっても、活用主体の立場・フェーズに応じて参照する情報の種類・粒度・優先度は大きく異なる。

## 3.2　事例①:Log4j 脆弱性対応

- 事例概要

2021 年 11 月に Alibaba のクラウドセキュリティチームが Apache へ秘密裏に報告し、同年 12 月 9 日に一般公開された広く使用されている Java のログ出力ライブラリ「Apache Log4j」の深刻な脆弱性(CVE-2021-44228、通称「Log4Shell」)。この脆弱性は、リモートから任意のコードを実行でき

る極めて危険なもので、CVSS(共通脆弱性評価システム)スコアで最高値の 10.0 を記録した。2

- 欧州 NATO 加盟国の国防省への攻撃

Log4j 脆弱性が公表された直後、欧州の NATO 加盟国の国防省が攻撃の標的となり、加盟国の国防省として初めてこの脆弱性による被害を受けた組織となった。

何が問題だったのか
当該国防省の事例で明らかになった主な問題点は以下の通りである。

① 影響範囲の迅速な特定ができなかった: 脆弱性公表から攻撃検知まで約 1 週間。この間に、自組織のどのシステムがLog4jを使用しているかを完全に把握できていなかったと推測される。
② 公表後の対応準備が不十分だった: 同国のサイバーセキュリティセンターは 12 月 16 日（中旬）に警告を発していたが、攻撃を防ぐことができなかった。事前の可視化と対策準備が不十分だったことが示唆される。
③ 業務への深刻な影響: 電子メールシステムを含む複数のシステムが数日間停止し、公式 Web サイトや Facebook での問い合わせ対応も不能になった。

- 必要だった可視化データ

① 製品・システムの構成に関する情報
「自組織のどのシステムが Log4j を使用しているか」を迅速に特定することが不可欠と考えられる。Log4j は多くの Java アプリケーションで使用されているが、表面的には見えない場所に含まれていることが多い。例えば、Web アプリケーションサーバー、管理ツール、監視システムなどが内部的に Log4j を使用しているケースがある。

② 脆弱性に関する情報
Log4j 脆弱性は公表後すぐに、複数の亜種や関連する脆弱性が発見された。この短期間での複数の脆弱性と修正版のリリースは、「どのバージョンが安全か」の判断を困難にした。また、Log4j を使用していても、設定や使用方法によって実際のリスクは異なるため、単に「使用している/していない」だけでは不十分だった可能性がある。

③ 責任者・連絡先に関する情報
大規模組織では、多数のシステムがあり、それぞれ異なる部門や担当者が管理している。緊急時には、各システムの責任者と連絡先、週末・夜間の緊急連絡体制、外部ベンダーの技術サポー

2 NVD/NIST「CVE-2021-44228 Detail」（原題: “CVE-2021-44228 Detail”, National Vulnerability Database）. https://nvd.nist.gov/vuln/detail/CVE-2021-44228

ト窓口、上層部へのエスカレーション経路などの情報が必要になる。

- 学び

当該 NATO 加盟国の国防省の Log4j 脆弱性対応事例は、脆弱性公表から攻撃までの猶予期間が極めて短い場合、平時からのシステム構成可視化が生命線となる可能性があることを示唆している。特に国防組織のように高度な標的となる環境では、どのシステムがどのライブラリを使用しているか、外部公開されているか、業務継続上の重要度はどうか、緊急時の連絡体制は整っているかといった情報が事前に可視化されていなければ、脆弱性公表後の迅速な影響範囲特定と優先順位付けができない。資産台帳と依存関係の完全な可視化、運用状態の継続的な把握、緊急時連絡体制の整備が、限られた時間内での的確な判断を可能にし、攻撃による被害を最小化する鍵となり得る。

## 3.3　事例②:国内製造業サプライチェーン攻撃

- 事例概要

2022 年 2 月、国内大手自動車メーカーB 社の取引先である国内自動車部品メーカーA 社がランサムウェア攻撃を受け、国内大手自動車メーカーB 社の国内全工場が停止する事態が発生した。攻撃者はリモートアクセス環境の脆弱性を突いて侵入し、基幹システムを停止させた。これにより受発注システムが機能せず、国内大手自動車メーカーB 社は翌日の生産を全面停止せざるを得なくなった。

何が問題だったのか
当該製造業の事例で明らかになった主な問題点は以下の通りである。

① サプライチェーン全体の可視化ができていなかった: 国内大手自動車メーカーB 社は国内自動車部品メーカーA 社との取引関係は認識していたものの、調達依存度の高さや代替調達先の有無を十分に把握できていなかった可能性がある。一社への依存が生産停止という重大なリスクにつながることを、事前に評価できていなかったと推測される。
② 取引先のセキュリティ状態を継続的に監視していなかった: 国内自動車部品メーカーA 社のリモートアクセス環境の脆弱性や、セキュリティ対策のレベルを国内大手自動車メーカーB 社側が把握していなかった可能性がある。サプライヤーに対するセキュリティ評価や監査の仕組みが不十分だったことが示唆される。
③ 攻撃発生時の影響範囲が予測できていなかった: 一つの取引先への攻撃が、国内大手自動車メーカーB 社の国内全工場の停止という広範囲な影響を及ぼすことを、事前に想定できていなかった可能性がある。受発注システムの依存関係や、攻撃発生時のビジネスインパクトが可視化されていなかったため、迅速な代替手段の検討や事業継続計画の発動ができなかったことも考えられる。

- 必要だった可視化データ

① 取引先・サプライチェーン構成に関する情報

「どの企業と取引関係にあるか」「その依存度はどの程度か」を把握することが不可欠と考えられる。事前に取引依存度が可視化されていれば、リスク分散や代替調達先の確保といった予防策を講じることができた可能性がある。

② 取引先のセキュリティ状態に関する情報

取引先のセキュリティレベルを把握する必要がある。事前にセキュリティ評価が実施され、リモートアクセスの設定やパッチ適用状況が可視化されていれば、攻撃を未然に防ぐか、少なくとも早期に検知できた可能性がある。

③ 外部から観測可能なリスク情報

取引先から直接情報を得ることが難しい場合や、提供された情報を補完する手段として、外部から観測可能なリスク情報の活用が有効である。これはアタックサーフェス管理と呼ばれるアプローチである。

- 学び

当該製造業の事例は、サプライチェーン全体の監視には取引関係の可視化が前提となる可能性があることを示唆している。特に製造業のように複雑な調達網を持つ環境では、どの取引先にどの程度依存しているか、代替調達先は存在するか、一社への攻撃がどこまで影響するかといった情報が事前に可視化されていなければ、予防的な対策も迅速な意思決定も困難になる可能性がある。製品の技術構成だけでなく組織・取引関係の可視化と共有体制の構築が、サプライチェーン攻撃のリスクを最小化し、適切な予防・対応判断を可能にする鍵となり得る。

## 3.4 事例③:医療機関ランサムウェア攻撃

- 事例概要

医療機関がランサムウェア攻撃を受け、電子カルテシステムや医療機器管理システムなど、診療に不可欠なシステムが暗号化され使用不能になった。攻撃により、救急患者の受け入れ停止、手術の延期、外来診療の制限など、医療サービスの提供に深刻な影響が生じた。

何が問題だったのか

医療機関ランサムウェア攻撃の事例で明らかになった主な問題点は以下の通りである。

① 復旧優先度の判断基準が明確でなかった: ランサムウェアにより複数のシステムが同時に使用不能になった際、どのシステムを優先的に復旧すべきかの判断基準が事前に定義されていなかった可能性がある。救急対応、入院患者の継続治療、外来診療といった医療業務の優先順位が、システム復旧計画に反映されていなかったと推測される。

② バックアップと復旧手順の実効性が検証されていなかった: バックアップは取得されていた可能性があるが、それらが実際に復旧可能か、復旧にどれだけの時間がかかるかが定期的にテストされていなかったことも考えられる。復旧手順書も最新のシステム構成を反映していない、担当者が手順を理解していないなど、「存在するが機能しない」状態だったことが示唆される。

③ システム間の依存関係が把握されていなかった: 電子カルテシステムをはじめとする医療システムは、データベース、認証サーバー、ネットワーク機器など多数のコンポーネントに依存している。これらの全体像と依存関係が可視化されていなかったため、どの順序でシステムを復旧すべきか、一つのシステムを復旧するために何が必要かが即座に判断できなかった可能性があり、復旧作業が長期化した。

- 必要だった可視化データ

① 事業継続・復旧優先度に関する情報

どのシステムを優先的に復旧すべきかを判断するには、BCP/BIA 情報、業務影響度評価、システム重要度分類、復旧目標時間(RTO)などの可視化が必要である。医療機関の場合、救急対応に必要なシステム、入院患者の継続治療に必要なシステム、外来診療用のシステムといった優先順位を事前に定義しておく必要がある。

② バックアップ・復旧手段に関する情報

どのバックアップがいつ時点のものか、復旧に何が必要かを把握するには、バックアップ管理台帳、バックアップ実施記録、復旧手順書、テスト結果などの可視化が必要である。単にバックアップを取得しているだけでなく、定期的な復旧テストの実施記録や、バックアップデータの保管場所、復旧に必要な時間の見積もりなども含まれる。

③ システム構成・依存関係に関する情報

システム間の依存関係や復旧の前提条件を理解するには、システム構成図、依存関係マップ、インフラ構成情報、ネットワーク図などの可視化が必要である。電子カルテシステム一つを取っても、データベースサーバー、アプリケーションサーバー、認証サーバー、ネットワーク機器など、多数のコンポーネントが関係しており、これらの全体像が把握できていなければ計画的な復旧は困難である。

- 学び

医療機関ランサムウェア攻撃の事例は、復旧計画には技術情報だけでなく、事業継続や業務優先度に関する情報の可視化が不可欠である可能性があることを示唆している。特に医療機関のように人命に関わる判断が求められる環境では、どのシステムを優先的に復旧すべきか、バックアップがいつ時点のものか、システム間の依存関係はどうなっているかといった情報が事前に可視化されていなければ、迅速な意思決定が困難になる可能性がある。BCP/BIA 情報の可視化と共有体制の構築が、緊急時の混乱を最小化し、適切な復旧判断を可能にする鍵となり得る。

## 3.5　本質的な失敗要因とは何か

- 事例①: Log4j 脆弱性対応

当該 NATO 加盟国の国防省の事例から浮かび上がる本質的な失敗要因は、単なる「パッチ適用の遅れ」ではない。より根本的な問題は、脆弱性対応のスピードと組織の準備状態が致命的にミスマッチしていた可能性がある。

- 事例②:国内製造業サプライチェーン攻撃

当該製造業の事例から浮かび上がる本質的な失敗要因は、単なる「セキュリティ対策の不足」ではない。より根本的な問題は、サプライチェーン全体が「見えていない」状態で運用されていた可能性があると考えられる。

- 事例③:医療機関ランサムウェア攻撃

医療機関ランサムウェア攻撃の事例から浮かび上がる本質的な失敗要因は、単なる「セキュリティ対策の不足」や「バックアップの欠如」ではない。より根本的な問題は、復旧に必要な情報が「整理されていない」「検証されていない」状態で運用されていた可能性があると考えられる。

- 3 事例を横断するパターン

3 つの事例を横断するパターンは、「使えるデータになっていなかった（データが存在しなかった場合も、存在していたが活用できなかった場合も含む）」という点である。Log4j の事例では構成情報が分散・陳腐化していた、当該製造業の事例では取引先情報が十分に共有されていなかった、医療機関の事例では復旧手順が検証・更新されていなかった。いずれも共通の本質は「使えるデータになっていない」ことであったと考えられる。

では、「使えるデータ」とはどのような条件を満たすものか。第 4 章では、この問いに答えるため、3 事例の分析結果から共通して求められる 5 つの要素を整理する。

# 4　可視化するデータに求められる要素

## 4.1　本章の考え方

第 3 章の 3 事例（Log4j 脆弱性対応、国内製造業サプライチェーン攻撃、医療機関ランサムウェア攻撃）から、可視化が不十分であったこと（可視化されていない場合も含む）で被害拡大につながった。可視化データの価値を高めるためには、活用シーンに応じた要素を整理する必要があることが分かった。

第 3 章の各事例で「必要だった可視化データ」として挙げられた情報（構成情報、脆弱性情報、取引先情報、BCP 情報など）は、種類は異なっていても、共通して 5 つの観点から問題が生じていた。①データが実態と合っていなかった（品質）、②データの出所・正しさを確認できなかった（真正性）、③緊急時に素早く参照・活用できなかった（適用性）、④データの改ざんリスクが排除できなかった（完全性）、⑤データが更新されず陳腐化していた（運用性）である。本章ではこの 5 要素を、それぞれの「要素の概要」「重要性」及び「第 3 章事例との関係」の順に整理する。また、本知見集で整理する 5 要素は、可視化データの活用において共通に重要となる観点である。一方で、仮に同じ可視化データの同じ 5 要素であっても、利用主体の目的や責任範囲に応じて“求められるレベル”や“重み付け”は変化し得る。したがって、5 要素は固定的なチェックリストとしてではなく、ユースケースに応じて優先度・要求水準を調整するための切り口として用いる。例えば、「サプライヤーの構成情報（SBOM 等）」という同じ可視化データを扱う場合でも、調達部門がサプライヤー選定の判断に用いる場面では、提供データが実態を正確に反映しているかを確認する「真正性」が特に重要となる。一方、CSIRT 担当がインシデント発生時の影響範囲特定に用いる場面では、緊急時に即座に参照できる形式であることを求める「適用性」の重要度が相対的に高まる。このように、同じ可視化データであっても、それを活用する主体の目的・フェーズによって、重視すべき要素とそのレベル感は変化し得る。なお、これらの 5 要素は、データ品質の国際規格である ISO/IEC 25012（データ品質モデル）が定める 15 の品質特性（正確性・完全性・一貫性・信憑性・最新性・アクセシビリティ等）を参考にして、本知見集では 5 要素を以下のように捉えている。

品質（データの正確性）：可視化データが実態と一致し、誤り・欠落・不整合が少ない状態。

真正性（データ生成・流通過程の正しさ）：データの出所と生成～流通過程が追跡でき、判断根拠として信頼できること。

適用性（データの明確性と可読性）：読みやすく取り込みやすい形で、意思決定に必要な情報が明確に示されていること。

完全性（改ざん防止）：データが改ざんされておらず一貫性が保たれていること（生成後～利用までの変更が技術的に検証できる状態が望ましい）。

運用性（継続的な最新性）：可視化データを継続的に更新し、環境変化（構成変更、脆弱性発見、体制変更等）を反映できる仕組みがあること。

すべての要素を一度に完璧に満たす必要はない。各要素に求められるレベル感は異なり、段階的にレベルを上げていくことが現実的である。

本知見集における 5 要素は「信頼性」という概念を内包しており、監査・セキュリティ評価の観点

では品質（正確性）・真正性・完全性（改ざん防止）が、インシデント対応の観点では適用性・運用性が特に重要となる。読者は自身の立場に応じて重視すべき要素を判断されたい。

### 4.2　品質(データの正確性)

- 要素の概要

  品質とは、可視化データが実態と一致し、誤り・欠落・不整合が少ない状態を指す。

- なぜ重要か

  可視化データは複数主体が共有し、緊急時は精査の余裕がない。不正確だと影響特定や優先順位付け、復旧判断を誤るため、作成後も突合・テスト等で正確性を保つ。

- 第 3 章の事例でどのように関連するか

  品質（正確性）が欠けると、医療機関ランサムウェア攻撃では復旧優先順位付けが属人的になりやすいだけでなく、そもそも脆弱性として検知されない見落としも生じやすく、復旧が長期化し得る。また、Log4j 脆弱性対応では自組織のどのシステムが Log4j を使用しているかを把握できておらず、影響を受けるシステムの特定自体に時間を要した。

### 4.3　真正性(データ生成・流通過程の正しさ)

- 要素の概要

  真正性とは、データの出所と生成～流通過程が追跡でき、判断根拠として信頼できることを指す。

- なぜ重要か

  意思決定の根拠にする以上、組織間で共有するデータは検証できなければ使えない。共有範囲が広いほど、途中改ざんや不正混入がないことの担保が重要になる。

- 第 3 章の事例でどのように関連するか

  真正性（出所・作成/流通プロセスの正しさ）が不明確だと、Log4j 脆弱性対応では稼働中のコンポーネントのバージョン情報を独立して検証できる手段がなく、影響を受けるバージョンかどうかの確認に時間を要した。国内製造業サプライチェーン攻撃では取引先のセキュリティ状態に関する情報を独立して検証できる仕組みがなく、リスク評価の判断根拠が不安定な状態に置かれていた。

### 4.4　適用性(データの明確性と可読性)

- 要素の概要

  適用性とは、読みやすく、システムや運用プロセスに組み込みやすい形で、意思決定に必要な情報が明確に示されていることを指す。

- なぜ重要か

  可視化データは使われて初めて価値がある。緊急時に必要情報へすぐ辿り着け、既存プロセスやツ

ールに取り込みやすい形式が対応を支える。

- 第 3 章の事例でどのように関連するか

適用性（明確性・可読性）が高いほど、医療機関ランサムウェア攻撃では判断するための時間短縮につながり、復旧の実効性が上がる。同様に、Log4j 脆弱性対応でも、システム構成や影響範囲の情報が複数の部門・担当者に分散して管理されていたため、集約・判断に余分な時間がかかった。可読性の高い統一フォーマットで管理されていれば、対応の初動を大幅に短縮できた可能性がある。

### 4.5　完全性(改ざん防止)

- 要素の概要

完全性とは、データが改ざんされておらず、一貫性が保たれていることを指す。生成後～利用までの間に変更がないことを技術的に検証できる状態が望ましい。

- なぜ重要か

改ざんや破損の恐れがあるデータは判断根拠にならない。組織間授受や長期保管では、改ざん検知と整合性確認の仕組みが信頼を支える。

- 第 3 章の事例でどのように関連するか

完全性（改ざん防止）が担保できないと、国内製造業サプライチェーン攻撃のように、取引先のセキュリティ状態に関する情報の信頼性を技術的に担保できず、リスク評価の判断根拠が不安定になりやすいため、署名・ハッシュ等で検証可能にしておく必要がある。また、Log4j 脆弱性対応でも、調達・導入されたコンポーネントのバージョンと実際に稼働しているバージョンが必ずしも一致しないにもかかわらず、その整合性を検証できる手段がなかった点が、影響範囲の正確な把握を困難にした。

### 4.6　運用性(継続的な最新性)

- 要素の概要

運用性とは、可視化データを継続的に更新し、環境変化（構成変更、脆弱性発見、体制変更等）を反映できる仕組みがあることを指す。

- なぜ重要か

データは古くなると価値を失う。緊急時に最新情報で判断できるよう、継続更新の仕組みで実用性を保つ。

- 第 3 章の事例でどのように関連するか

運用性（継続的な最新性）が欠けると、可視化データが陳腐化し、緊急時の判断を誤らせる。Log4j 脆弱性対応では、どのシステムが Log4j を使用しているかを把握できていなかったことが示すとおり、資産情報が最新の状態に保たれておらず影響範囲の特定に時間を要した。国内製造業サプライチ

ェーン攻撃では取引先のセキュリティ状態が継続的に監視されていなかったため、リスクの変化を事前に把握できなかった。医療機関ランサムウェア攻撃では復旧手順書が最新のシステム構成を反映しておらず、復旧作業の長期化を招いた。いずれも「更新を続ける仕組み」の欠如が根本原因と考えられる。

# 5　可視化データ要素に関する問題・課題と役立つ知見

## 5.1　本章の読み方

第 4 章の 5 要素を実現する際に生じやすい課題と、対処の要点を整理する。本章は「生成→共有→活用」の流れで整理する。自組織の状況に応じ、必要なセクションから参照できる。

また、生成・共有・活用の各段階で生じる課題は、利用主体の役割や組織内外の調整範囲によって現れ方が異なる。例えば、同じ「活用」段階であっても、インシデント対応の意思決定を担う主体と、説明責任・対外コミュニケーションを担う主体では、参照する可視化データの観点や必要十分な粒度が異なり得る。本章の整理は、こうした差異を踏まえてユースケースごとに適用・読み替えられることを意図している。

「生成→共有→活用」という整理を採用した理由は、第 3 章の事例分析が示すとおり、可視化データの問題は「作れない」だけではなく、「作っても共有されない」「共有されても使われない」という段階で生じることが多いためである。Log4j の事例では作成・更新が追いつかず（生成の問題）、当該製造業の事例では取引先への情報提供が進まず（共有の問題）、医療機関の事例では復旧手順書が実際には参照されなかった（活用の問題）。各段階で生じる課題を独立して把握することで、自組織のボトルネックがどの段階にあるかを特定しやすくなる。

また、「脆弱性対応責任のある範囲＝可視化・管理すべき範囲」を本章全体の原則として据える。自組織がパッチ適用やインシデント対応の責任を持つ対象こそが、可視化データを整備すべき対象である。Windows や Linux のようにベンダーがパッチを提供する OS であっても、自組織の SBOM に含めるべきか否かは、この原則に基づいて判断する。SBOM ツール（Black Duck 等）で自動収集されない対象については、別帳票等で補完する実務的対処を検討することが望ましい。

また、SBOM を実際に扱う中で、データが正しく入力されていないケースへの対処が難しいという実務上の課題も存在する。データ品質の確保は本章全体を通じて重要なテーマであり、各知見を参照する際にはデータの正確性・最新性の維持を常に意識することが望ましい。

## 5.2　データ生成段階の課題

生成は出発点だが、範囲の広さや自動化の難しさでつまずきやすい。本節では典型課題と対処の要点を示す。

簡易的なアンケート結果によると、SBOM 作成側（n=7）の回答では、作成方法として商用ツールの活用が最多（6 社）、次いで OSS（4 社）であった。作成にあたって主体となる組織は開発部門（5 社）が中心であり、セキュリティ部門（2 社）の関与は相対的に少ない。作成コストは IT 予算の 5% 未満（5 社）が大半を占め、作成に係る課題としては「作成した SBOM の品質が低い」（3 社）が最多で、ツール不足や社内規定の未整備（各 2 社）も課題として挙げられた。サーバ系（Linux 等）を対象とするケースが最多（5 社）であり、PC アプリ（3 社）・組み込み機器（3 社）が続く。

- 問題 どのデータから可視化を始めるべきか

5 要素との関連性: この課題と知見は、主に適用性と運用性の観点から重要である。

課題: 対象が多く全件可視化は難しい一方、既存運用と整合する着手点を決めにくい。

知見: 既存の脆弱性管理・資産管理・変更管理と整合しない（独立した）範囲から始める方が着手しやすく、運用しながら段階的に既存の仕組みに組み込んでいく。

- 問題: データ生成の自動化が困難ではないか

5 要素との関連性: この課題と知見は、主に品質、真正性、運用性の観点から重要である。

課題: SBOM に限らず、可視化データを生成するためのツールや手順を導入しても、既存の開発・調達・構成管理・変更管理の流れに統合できず、手作業が残る（結果として品質・真正性・運用性が担保できない)。

知見: 最初から完全自動化を狙わず、手動→半自動→自動の順に段階移行する。

段階 1（手動）: 既存資料からテンプレートへ転記し、項目を標準化する。

段階 2（半自動）: ツール収集→人が確認・補完・承認（例：業務影響度を追記)。

段階 3（自動）: CI/CD や構成管理と連携し、変更検知→更新までを自動化する。

## 5.3 データ共有段階の課題

共有段階では、受け渡し方法・範囲・前提条件（何を共有し、受領側に何を期待するか）を整理する。

簡易的なアンケート結果によると、SBOM 作成側における共有手段は、「特定システムへの手動アップロード」（3 社）と「ファイル共有」（3 社）が同数で最多となり、自動アップロード（2 社）・メール・チャット（1 社）が続く。受領側（活用側 n=8）においても、手動アップロード（4 社）・自動アップロード（3 社）・ファイル共有（3 社）が主な手段であり、依然として手動運用が多いことが確認された。脆弱性検知時の対応は、作成側では「自社にて対応」（6 社）が主流であり、活用側は「自社にて対応」と「開発元への対応要請」が同数（各 5 社）であった。

- 問題: SBOM の受け渡しスキームにおける責任モデルをどう選択するか

5 要素との関連性: この課題と知見は、主に品質、真正性、運用性の観点から重要である。

課題: SBOM の受け渡し責任の持ち方として「ベンダー全責任型」（最終ベンダーがサプライチェーン全体の SBOM を収集・保証）と「分散コンソーシアム型」（各社が自社分を責任を持って提供し、基盤上で統合）の 2 モデルが存在する。「ベンダー全責任型」は規模に応じてスケールしないため、どのモデルを採用するかを最初に合意することが必要である。

知見: 米国では、EO 14028 以降 SBOM の導入・活用が推進されたが、その後、EO 14306 および OMB M-26-05 を通じて、過度に負担の大きい画一的なソフトウェア保証要求は見直され、各機関が包括的なリスクアセスメントに基づいて判断する方向へ政策が転換している。分散的な役割分担と実運用に即した共有モデルを前提に設計することが、社会実装の観点では重要である。自動車業界では J-Auto-ISAC が SBOM 運用ガイドを公表し、業界横断の共有基盤の整備に向けて取り組んでいる。医療機器業界では SBOM 作成が事実上制度化されるようになっており、他業界でも同様の動き

が今後広がることが見込まれる。3

- 問題: データの正確性をどう確認するか

5 要素との関連性: この課題と知見は、主に品質、真正性、運用性の観点から重要である。
課題: 自社作成（手動・ツール生成を問わない）データ（例：SBOM）やサプライヤー提供データの正確性を確認する手段が不足している。
知見: 自動チェック＋主要コンポーネント名・バージョン・依存関係などの重要箇所の目視確認（例：実際のバイナリに含まれるバージョン文字列と記載値の一致確認、依存ライブラリの有無チェック等）＋（可能なら）実構成との突合を組み合わせ、変更時・定期で再確認する。

- 問題: 真正性をどう検証するか

5 要素との関連性: この課題と知見は、主に真正性、完全性の観点から重要である。
課題: 正規の提供元か、途中改ざんがないかを確認しにくい。
知見: 技術（署名・ハッシュ・安全な伝送）と組織（契約・監査等）を組み合わせる。
デジタル署名: 重要データに付与し受領側で検証（コストを踏まえ段階導入）。
ハッシュ値: ハッシュを併送し、受領側で再計算して一致確認（導入容易）。
セキュア伝送: HTTPS/SFTP や専用ポータル/API を使い、メール送付は避ける。

- 問題: サプライヤーからの情報提供が困難ではないか（共有を前提とした段階的要求）

5 要素との関連性: この課題と知見は、主に品質、真正性、適用性、運用性の観点から重要である。
課題: 共有フェーズで可視化データの授受を想定しても、サプライヤー側が可視化データ（例：SBOM、資産情報、構成情報、セキュリティ対策状況、連絡先・契約情報 等）を作成・更新・提供できない（未経験、方法不明、リソース不足、コスト負担、契約上の位置づけ不明確等）ため、サプライチェーン全体での共有が進まない。
知見: ①最小セット＋テンプレで開始、②更新・契約更改の節目で要求を段階的に引き上げ、③契約・評価（発注）に組み込んで提供を定着させる。
要求レベル: 初回は最低限（例：主要コンポーネント、作成方法、更新日）を受け入れ、実績を作る。

---

3 White House「国家のサイバーセキュリティ強化に向けた選択的取組の継続」（仮訳、原題: “Fact Sheet: Sustaining Select Efforts to Strengthen the Nation’s Cybersecurity”），2025 年 6 月 6 日. https://www.whitehouse.gov/fact-sheets/2025/06/fact-sheet-sustaining-select-efforts-to-strengthen-the-nations-cybersecurity/；OMB「ソフトウェア及びハードウェアのセキュリティに対するリスクベース・アプローチの採用」（仮訳、原題: “M-26-05: Adopting a Risk-based Approach to Software and Hardware Security”），2026 年 1 月 23 日. https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf

## 5.4　データ活用段階の課題

活用段階では、体制や既存プロセスとの統合がボトルネックになりやすい。

簡易的なアンケート結果によると、SBOM 活用側（n=8）の回答では、活用目的は「自社のセキュリティ管理への活用」が最多（7 社）であり、次いで「顧客への提出」（5 社）が続く。活用している SBOM の対象はサーバ系（Linux 等）が最多（7 社）、次いで PC アプリ（5 社）。活用に用いるツールは商用ツール（5 社）・自社開発（5 社）が並立している。活用にあたって主体となる組織は開発部門（6 社）が中心で、セキュリティ部門（3 社）の関与は限定的。活用に係る課題の自由記述（4 件）が最多であり、標準化や継続的更新の難しさが示唆された。活用コストは IT 予算の 5%未満（5 社）が大半を占め、導入初期の投資ハードルの低さが確認された。現時点では「一部組織で活用」（4 社）が主流だが、2〜3 年後には「組織全体で活用」を目指す回答（4 社）も多く、今後の拡大への強い意欲が示された。

- 問題: データを実務にどう組み込むか

  5 要素との関連性: この課題と知見は、主に適用性、運用性の観点から重要である。
  課題: 作成した可視化データが脆弱性対応やインシデント対応で参照されず、使われない。
  知見: 「参照・更新」が業務フローに組み込まれる形にする。
  既存プロセス統合: 脆弱性管理・変更管理・インシデント対応などに参照/更新を組み込む。
  ツール連携: 資産管理、脆弱性管理、SIEM 等と連携し自動参照できるようにする。
  定期レビュー: 活用状況を点検し、維持コストに見合わないものは簡素化/廃止も検討。
  使う場面を明確にし、運用に落とし込むことが重要と考えられる。

- 問題: データ更新の継続性をどのように担保するか

  5 要素との関連性: この課題と知見は、主に運用性、品質、適用性の観点から重要である。
  課題: 初回作成はできても更新が定着せず、データが陳腐化する。
  知見: 更新を「自動化・習慣化」する（トリガー定義、可能範囲の自動化、期限/アラート）。
  更新トリガー: リリース時、重大脆弱性公開時、定期（四半期等）、構成変更時などを明確化。
  自動化: CI/CD、構成管理、定期ジョブ等で更新負荷を下げる。
  期限/アラート: 有効期限を設け、期限接近時に通知する。
  属人的対応ではなく、更新が回る「仕組み」にすることが鍵となり得る。

## 5.5　脆弱性管理における可視化データ活用のまとめと今後の検討課題

本知見集では、第 3 章の 3 事例（Log4j 脆弱性対応・国内製造業サプライチェーン攻撃・医療機関ランサムウェア攻撃）を通じて、脆弱性管理の実務において「使えるデータになっていない」ことが共通の課題であることを示した。第 4 章では、この課題を解消するために可視化データが備えるべき 5 要素（品質・真正性・適用性・完全性・運用性）を体系化し、第 5 章では生成・共有・活用の各段階における具体的な課題と知見を整理した。これらを通じて、脆弱性管理における可視化データの活用においては、個々の要素はある程度整理できたものの、実務への定着・組織横断での共有・継続

的な更新という観点では、依然として多くの課題が残っていることも明らかになった。

特に、今回の検討を通じて浮かび上がった重要な示唆として、可視化データの 5 要素それぞれに対して、脆弱性管理という特定のユースケースにおける要求レベルや適用上の優先度を、さらに実務レベルで深掘りしていく必要がある。例えば、品質と運用性の両立、真正性確保のコスト対効果、適用性向上のためのフォーマット標準化など、各要素の相互関係や優先順位については、引き続きメンバー企業との実践的な議論を積み重ねることも有益ではないかと考えている。本コンソーシアムとしては、本知見集を起点として、可視化データの要素に関する検討をさらに深化させていくことも考えている。

# 6　今後の展望

第 3 章から第 5 章では、脆弱性管理の実務を主目的として、可視化データの概念・事例分析・求められる要素・課題と知見を論じてきた。本章では、その土台の上に立ちながら、可視化データ活用の今後の展望を技術環境・エコシステム・制度・組織の 4 つの観点から俯瞰する。各節の議論は脆弱性管理を軸足に置きつつ、より広い可視化データ活用への発展的な展望も含む。読者は自身のロールや目的に応じて参照いただきたい。

## 6.1　可視化データの多様なアプローチ

完全な可視化データが入手できない状況でも、利用可能な情報から着手することに意義がある。製品マニュアル・技術文書、ベンダー公式サイトのセキュリティアドバイザリ、既存の資産管理台帳や構成管理データベース（CMDB）、契約書・購買記録など、すでに組織内に存在する情報を体系的に整理するだけでも、脆弱性対応の初動は改善される可能性がある。アタックサーフェス管理サービスやセキュリティレーティングサービス、脆弱性データベース（NVD・JVN 等）といった外部サービスの活用も、可視化データを補完する手段となる。

可視化のレベルは段階的に引き上げることが現実的である。レベル 1（基本的な資産リスト：製品名・バージョン・所在等）から始め、レベル 2（詳細構成情報：コンポーネント・依存関係等）、レベル 3（リアルタイム可視化：動的な構成変更の追跡等）へと段階的に充実させていく。どのレベルをいつまでに達成するかは、自組織のリスクや規制要件、利用可能なリソースに基づいて判断することが望ましい。

可視化の手段は目的に応じて選択することが重要である。脆弱性管理が目的であれば（本知見集の主テーマ）、構成情報と脆弱性情報（CVE 等）を組み合わせられる形式が優先される。コンプライアンス対応が目的であれば、提出先の規制が求めるフォーマットへの対応が必要である。サプライチェーンリスク管理が目的であれば、取引先情報と外部評価の組み合わせが有効である。BCP・インシデント対応が目的であれば、復旧に必要な情報（BCP/BIA 情報、システム構成図、依存関係マップ等）の整備が優先される。手段と目的を明確に対応させることで、整備の優先順位と投資対効果の判断がしやすくなる。

なお、どのアプローチをとる場合でも、第 4 章で整理した品質・真正性・適用性・完全性・運用性の 5 要素を満たすことが、可視化データの実用性を担保する共通の前提となる。例えば段階的に整備を進める場合であっても、各段階で可視化データに求められる要素を意識しながら進めることが、第 3 章の 3 事例が示した「使えるデータになっていない」という根本課題を回避する上で望ましい。

## 6.2　技術環境の進化への対応

可視化データの整備を取り巻く技術環境は急速に変化しており、従来の想定に基づいた仕組みでは対応が難しくなりつつある局面がある。

SaaS・クラウドネイティブ環境では、アプリケーションのコンポーネントが頻繁に更新され、インフラが動的に変化するため、静的な SBOM を定期的に作成する従来型のアプローチには限界がある可能性がある。ソースコードを直接保有しない SaaS の利用においては、ベンダーからの情報提供

を契約条件に含めることや、API 経由で動的に構成情報を取得する仕組みが求められる。コンテナ・サーバーレス・マイクロサービスアーキテクチャでは、実行環境のリアルタイムな構成変更を追跡できる仕組みとの連携が重要になる。

IoT・組み込みシステムは、10 年以上にわたる長いライフサイクルを持つ製品が多く、更新が困難なシステムでの可視化データ管理という固有の課題がある。エッジデバイスが大量に展開される環境では、個々のデバイスの構成情報をどのように集約・管理するかが実務上の課題となり得る。

AI・ML システムについては、学習データ・モデル・ライブラリという従来のソフトウェアとは異なる構成要素の可視化が求められる。モデルが継続的な再学習によって変化する場合、その変化を可視化データに反映する仕組みも必要になる可能性がある。また、AI システム固有の脆弱性（モデルの毒化、敵対的サンプル等）への対応は、従来の CVE ベースの脆弱性管理とは異なるアプローチが求められる可能性がある。

可視化データの配布・管理方法についても、アクセス制御可能なプラットフォームによる管理、機密情報の保護と開示レベルの制御、監査証跡の記録など、セキュアな情報共有基盤の整備が求められる。中央集約型と分散連携型のハイブリッドなアーキテクチャや、ブロックチェーン等の新技術の活用可能性についても、引き続き検討が求められる。

技術環境がいかに変化しても、第 3 章の各事例（Log4j、国内製造業サプライチェーン攻撃、医療機関ランサムウェア攻撃）が示した「使えるデータになっていない」という課題は変わらない。SaaS・IoT・AI/ML システムへの対応においても、第 4 章の 5 要素が実用性の基準として機能することに変わりはなく、新たな技術形態に応じた実現方法を継続的に検討することが肝要である。

## 6.3　エコシステムの成熟に向けて

可視化データの社会実装を阻む要因の一つに、ツールの乱立（ツールスプロール）がある。例えば、SBOM 生成・管理・共有を目的としたツールが個別に開発・導入された結果、組織内での重複投資やツール間の連携不足が生じており、統合的な可視化データ管理を困難にしているケースが見受けられる。

この課題に対応するためには、ツールを個別に評価・導入するのではなく、可視化データ管理のライフサイクル全体（計画・開発・運用・廃棄）を見渡した統合的なアプローチが求められる。既存の脆弱性管理ツール・資産管理システム・SIEM・SOC・PSIRT/CSIRT プロセスとの連携を前提に、可視化データの生成・共有・活用の流れを設計することが重要である。標準 API・共通データフォーマットへの準拠が、ツール間の相互運用性を確保するための基盤となる。業界横断的な標準化活動やリファレンス実装の整備が、個社の試行錯誤を超えた底上げにつながる可能性がある。 この点に関連して、OpenSSF は SBOM を「globally shared data model」として位置づけ、国際的なソフトウェアサプライチェーン全体における自動化・追跡可能性・信頼の基盤となる方向性を示している。もっとも、その実現にはフォーマット、意味論、コンプライアンス解釈の断片化を乗り越える必要があ

り、規範的目標としての共有モデルと、現実の分散的な情報連携の間にはなおギャップがある。4

組織能力の観点では、可視化データへの取り組みを規制対応のための最低限の義務履行にとどめるのではなく、競争優位性の獲得やビジネス価値の創出に結びつける「戦略的活用」への転換が中長期的に重要である。製品の透明性を差別化要素として訴求したり、取引先との信頼関係構築やサプライチェーン全体のリスク低減を通じた事業継続性の向上に活用したりすることが、その例として挙げられる。組織の成熟度については、アドホック（レベル 1：個別対応・属人的）・定義済み（レベル 2：手順化・標準化済み）・管理済み（レベル 3：定量的モニタリングあり）・最適化（レベル 4：継続的改善が定着）という段階を意識し、自組織の現状を把握した上で次のレベルへの移行を計画的に進めることが望ましい。なお、6.1 節で示したレベル（可視化する対象の範囲・深度の段階）と本節のレベル（組織としての可視化対応の成熟度）は異なる軸を表している。読者は両者を混同しないよう注意されたい。

エコシステムの成熟とは、第 4 章で整理した 5 要素が、個社の努力にとどまらず業界全体の仕組みとして担保される状態に向かうことでもある。第 3 章の事例②（国内製造業サプライチェーン攻撃）が示したように、取引先のセキュリティ状態が「使えるデータ」として流通する状態は、個社の取り組みだけでは限界があり、業界横断での標準化・役割分担・信頼基盤の成熟が必要である。

## 6.4　制度・プロセスへの組み込み

DevSecOps の観点では、可視化データの生成をソフトウェア開発ライフサイクルの一部として組み込むことが有効である。ソースコード変更時の自動 SBOM 生成、ビルドパイプラインでの可視化データ生成・検証、リリース前のチェックを品質ゲートとして設けるなど、開発プロセスの節目に可視化データの生成・更新を組み込む。可視化データが整備されていない場合にリリースを抑止する仕組みの検討も、運用の定着に有効な可能性がある。自動化によるヒューマンエラーの削減も重要な観点である。

変更管理との統合も重要である。システム構成の変更が発生した際に可視化データを更新するトリガーを定義し、変更履歴と可視化データを紐付けることで、変更影響分析での活用が可能になる。

継続的改善のサイクルとしては、PDCA フレームワークの活用が有効である。Plan（可視化の目的・範囲・基準の設定）→Do（可視化データの生成・配布）→Check（活用状況の評価・フィードバック収集）→Act（改善施策の実施）のサイクルを確立し、定量的なメトリクス（可視化データの活用率、インシデント対応時間の短縮効果、脆弱性発見から対応完了までの時間、コスト削減効果等）に基づいて改善の方向性を判断することが望ましい。

こうしたプロセスへの組み込みは、第 4 章で整理した運用性や品質を日常業務の中で自然に維持するための実践的な仕組みでもある。「更新し続ける仕組みの欠如」は、DevSecOps や変更管理との統合、PDCA サイクルの確立によって解消できると考えられる。

---

4 OpenSSF Blog「CRA 時代の SBOM：統一的かつ実行可能な枠組みに向けて」（仮訳、原題: “SBOMs in the Era of the CRA: Toward a Unified and Actionable Framework”）, 2025 年 10 月 22 日. https://openssf.org/blog/2025/10/22/sboms-in-the-era-of-the-cra-toward-a-unified-and-actionable-framework/

## 6.5　サプライチェーン全体のセキュリティ透明性の実現に向けて

可視化データの整備を組織の実務に根付かせるためには、既存の開発・運用プロセスへの統合が不可欠である。

第 3 章の Log4j・サプライチェーン攻撃・医療機関ランサムウェアの 3 事例が共通して示した「使えるデータになっていない」という課題の根本には、組織内・組織間のガバナンスの欠如がある。サプライチェーン全体でデータの品質・真正性・完全性・運用性が担保され、緊急時に即座に参照できる適用性が確保された状態を実現するためには、以下に述べるガバナンスの整備が不可欠である。

サプライチェーン横断の可視化データを継続的に維持・活用していくためには、データの所有権・管理責任・開示範囲に関するガバナンスの整備が前提となる。どの組織がどの情報の主体となり、どこまで開示するかを明確にしないまま可視化データの共有を求めることは、参加者の抵抗を生みやすい。国際的なデータ流通への対応（越境データ移転規制等）も、グローバルなサプライチェーンを持つ組織には重要な検討事項である。

サプライチェーン全体での信頼の連鎖（Chain of Trust）を確立するためのトラストフレームワークの構築も、中長期的な課題として位置づけられる。第三者認証・監査による信頼の付与、デジタル署名や分散台帳等の技術を活用したトラストレスな仕組みの検討が、具体的な方向性として考えられる。 また、中央集約的な証明モデルのみでサプライチェーン全体の透明性を担保しようとすると、実運用との乖離や形骸化を招くおそれがある。可視化データの流通においては、中央的な監視・参照基盤と、サプライヤーからバイヤー、ユーザーへと情報をつなぐ分散的な連携の双方を視野に入れた設計が重要である。

規制・制度との関係では、CRA・DPP・経済安全保障推進法等の既存規制への対応に加え、今後の規制動向を先読みした準備が競争上の優位性につながる可能性がある。産業界からは、規制当局に対して実務的な要求事項を提言し、実現可能な制度設計に向けたフィードバックを継続的に行うことが重要である。

サプライチェーン全体の透明性向上は一朝一夕で実現するものではないが、本知見集で整理した課題と知見を踏まえて段階的に取り組みを進めることで、サプライチェーン全体の安全性と信頼性を着実に高めていくことができると考えられる。本コンソーシアムは、そのための知見の共創と発信の場として、引き続き業界横断的な対話を促進していく。

# 7　おわりに

## 7.1　読者へのメッセージ

本知見集を踏まえて、最後に読者へのいくつかの提言を示したい。

本知見集は、第 3 章の 3 事例（Log4j・サプライチェーン攻撃・医療機関ランサムウェア）が共通して示した「使えるデータになっていない」という課題を出発点として、第 4 章の品質・真正性・適用性・完全性・運用性の 5 要素、第 5 章の生成・共有・活用段階における実践知見を体系的に整理してきた。以下の提言はこれらの議論を踏まえた、読者の実践への道案内である。まず自組織の現状を 5 要素の観点で棚卸しし、どの要素が最も不足しているかを確認することが、具体的な第一歩となる。

まず、自社の状況に応じた最初の一歩を踏み出すことを強く勧める。可視化データの整備において、完璧な状態から始めようとすることは現実的ではない。全社展開を一気に目指す前に、まずは特定の製品・システムを対象とした小規模なパイロットから着手することで、組織としての経験と実績を積み上げることができる。理想的な可視化データの整備を待つのではなく、現時点で組織内に存在する資産台帳・構成情報・契約情報などを活用し、できるところから改善を始めることが重要である。自社のリスクと優先度に基づいて判断し、すべての資産を同じレベルで可視化しようとするのではなく、リスクの高い資産や業務継続上の影響が大きいシステムから着手することが現実的なアプローチである。

次に、段階的な取り組みの重要性を強調したい。可視化データの整備は一度に完結するプロジェクトではなく、継続的な改善の積み重ねである。長期的な視点でロードマップを策定し、各フェーズで達成した成果を確認しながら次のフェーズに反映させることが、持続可能な取り組みを可能にする。組織の成熟度に応じてペースを調整し、無理のない範囲で着実に前進することが重要である。早期の小さな成功体験は組織内での推進力となり、実用的な価値を具体的に示すことで、経営層や関係部署の理解と支援を得やすくなる。

最後に、エコシステムとの連携を積極的に活用することを勧める。本コンソーシアムへの参加を通じて、業界が蓄積してきた知見を自社の課題解決に役立てるとともに、自社の経験を共有することで業界全体の成熟に貢献していただきたい。業界全体での知見共有においては、競争領域と協調領域を見極めることが重要である。サプライチェーン透明性の確保は協調領域として位置づけ、業界標準の確立によって全体最適を実現することが、長期的には各社の利益につながる。サプライチェーン全体での協調においては、取引先の状況や能力を理解した上で相互に合意できる現実的な要求レベルを設定し、Win-Win の関係構築による持続可能な透明性の実現を目指していただきたい。

## 7.2　本コンソーシアムとしての今後の取り組み

本知見集で整理した可視化データに関する課題と知見は、現時点での成果であり、一つの到達点ではなく継続的な積み重ねの通過点として位置づけている。本コンソーシアムは、本知見集の継続的な充実を通じて、技術環境や規制動向の変化に応じた最新の知見を発信し続ける。また、新たな事例の

発生やメンバー企業での実践から得られた知見を随時収集・共有し、知見集の質と実用性を高めていく。会員企業間での実践的な議論の場を継続的に設け、現場の課題に根ざした知見の共創を促進することが、本コンソーシアムの中核的な活動として位置づけられる。

特に、第 4 章で体系化した品質・真正性・適用性・完全性・運用性の 5 要素については、さらに実務に落とし込むにはどうしたらいいかといったことを引き続き検討するとともに、各要素の相互関係と優先順位の整理を深めていく。

コミュニティ活動の観点では、業界横断的な連携を一層促進することが重要な課題である。製造・IT・金融・医療・インフラなど、異なるセクターが直面するサプライチェーン上の透明性確保の課題を相互に学び合い、共通解と業界固有の解を明確化することで、業界標準の確立に向けた議論を前進させる。またベストプラクティスの発信を継続し、教育・啓発活動を通じてセキュリティ人材の育成にも貢献していく。

政府関係機関等との連携については、実務の現場から得られた具体的な知見を政策立案に反映させるべく、積極的な情報提供と意見交換を継続する。国際標準化活動への貢献を通じて、グローバルなサプライチェーン透明性の向上にも関与していく。また、産学官連携を推進し、研究機関・教育機関・行政との協働により、実践的かつ科学的な根拠に基づいた知見の深化を図る。

今後、本コンソーシアムでは、本知見集の改定も含め可視化データの活用に関する具現化を検討していく。
本知見集に賛同し、ともに活動していただける皆さまをお待ちしております。以下のウェブサイト、もしくは連絡先までお気軽にお問い合わせください。

セキュリティ・トランスペアレンシー・コンソーシアム オフィシャルウェブサイト
https://www.st-consortium.org/
セキュリティ・トランスペアレンシー・コンソーシアム事務局
stc-info@st-consortium.org

2026 年 7 月 1 日における本コンソーシアムの参加事業者は以下のとおりです。
アズビル株式会社
一般社団法人沖縄オープンラボラトリ
ＮＲＩセキュアテクノロジーズ株式会社
ＮＴＴ株式会社
株式会社アシュアード
株式会社ＮＴＣ
株式会社ＮＴＴデータグループ
株式会社ＦＦＲＩセキュリティ
株式会社ジークス
株式会社ＰＥＧＡＳＵＳ　ＨＯＬＤＩＮＧＳ
Ｃｏｖａｌｅｎｔ株式会社
サイバートラスト株式会社
シスコシステムズ合同会社
大日本印刷株式会社
東京エレクトロン株式会社
TISI 株式会社
日本電気株式会社
株式会社日立製作所

## A.　付録 A：可視化データ活用状況アンケート集計結果

本付録 A は、本コンソーシアム 可視化データ活用 WG（チーム B）が 2025 年 5 月 26 日に実施したアンケート（集計時点：2025 年 6 月 19 日 9:00）の主要結果を抜粋・掲載する。本知見集の各章における課題・知見の整理はこのアンケート結果を踏まえている。

【調査概要】

・実施日：2025 年 5 月 26 日　集計時点：2025 年 6 月 19 日

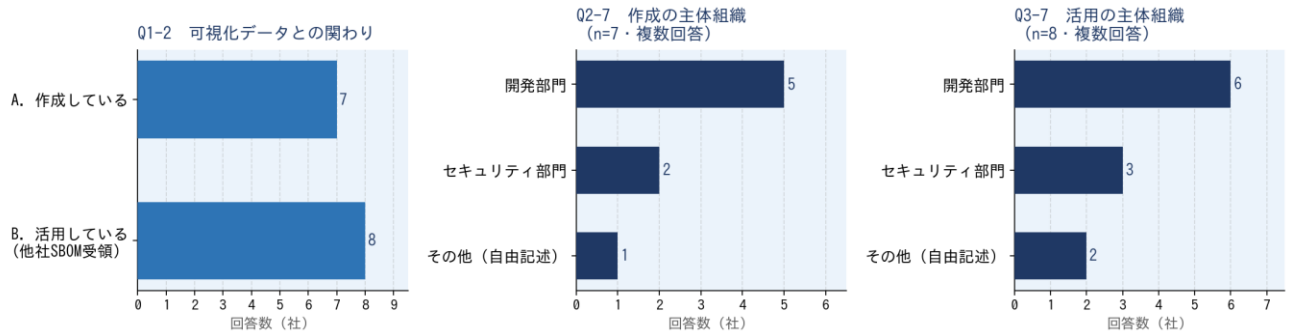
・対象：本コンソーシアム WG メンバー企業（製造業・電気通信業・サービス業等）

・回答者と可視化データの関わり：A. 作成している（n=7）、B. 活用している（n=8）（複数回答あり）

【主な知見】可視化データの作成・活用ともに開発部門が主体となっており、自社開発ソフトウェアの利用割合が増加している。SBOM 以外にも多岐にわたる可視化データが扱われており、具体的な活用策の分析が普及推進の鍵となりそうである。

### 1. 可視化データとの関わり・主体組織（Q1-2 / Q2-7 / Q3-7）

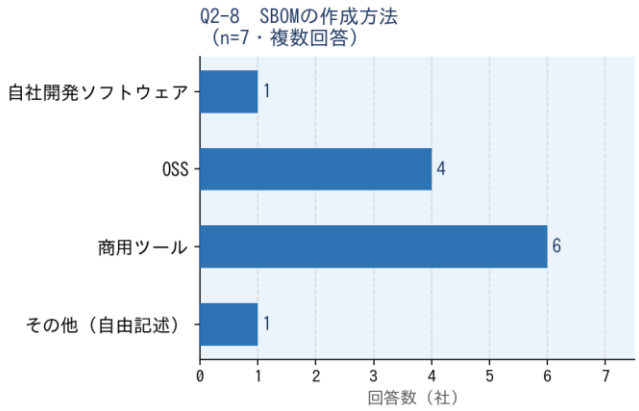
回答者のうち 7 社が SBOM を「作成している」、8 社が「活用している（他社作成 SBOM を受領）」と回答。作成・活用ともに開発部門が主体となっており、セキュリティ部門の関与は限定的。可視化データの品質・運用性の確保において、開発部門への負荷集中が課題の一つとして示唆される（→ 本知見集 第 5 章 5.2 節）。

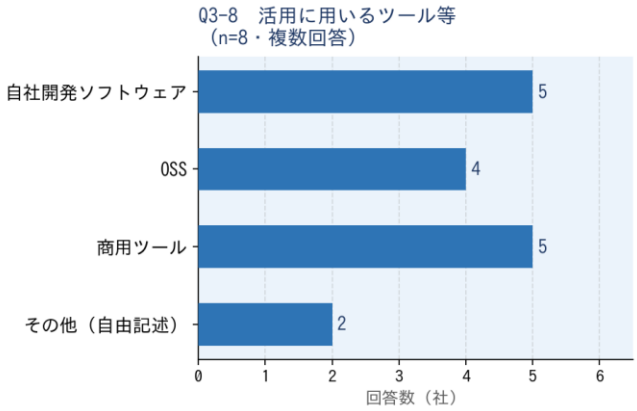



※ 複数回答あり。n=11（Q1-2）、n=7（Q2-7）、n=8（Q3-7）

### 2. 作成・活用ツールの状況（Q2-8 / Q3-8）

SBOM 作成では「商用ツール」（6 社）が最多。一方、活用では「自社開発ソフトウェア」（5 社）と「商用ツール」（5 社）が並立し、活用における自社開発の割合が増えている。活用ツールの多様化はデータ品質・適用性（フォーマット互換性）に課題を生みやすく、標準フォーマット（CycloneDX/SPDX）への準拠が重要となる（→ 本知見集 第 4 章 4.4 節）。

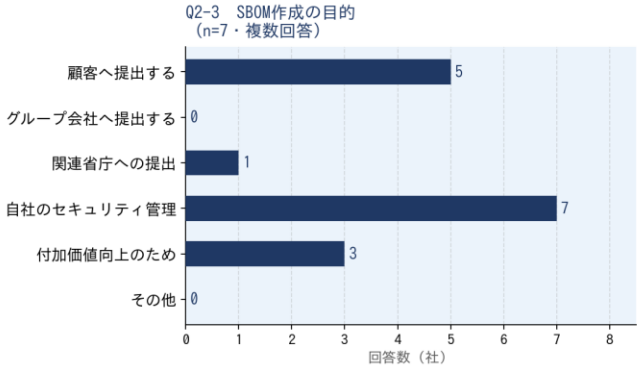


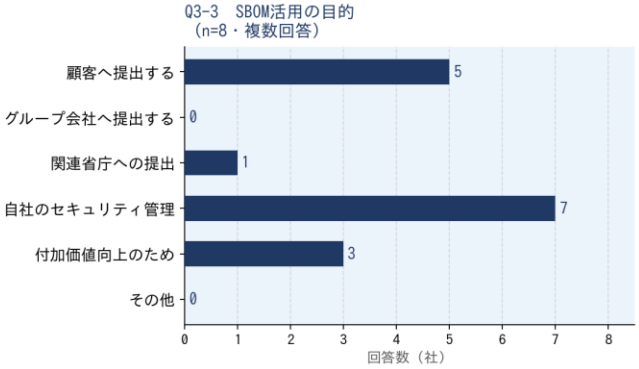




※ 複数回答あり。n=7（Q2-8）、n=8（Q3-8）

## 3. 作成・活用の目的（Q2-3 / Q3-3）

作成・活用ともに「自社のセキュリティ管理への活用」（7 社）が最多であり、次いで「顧客への提出」（5 社）が続く。外部提出よりも内部活用を優先する傾向が見られ、社内プロセスへの組み込みが普及の前提条件となっている（→ 本知見集 第 5 章 5.4 節）。

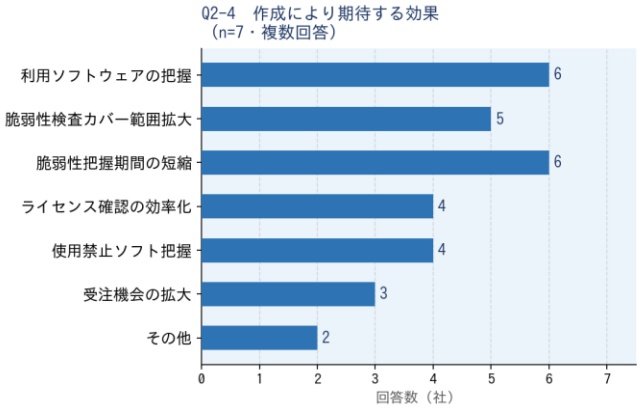


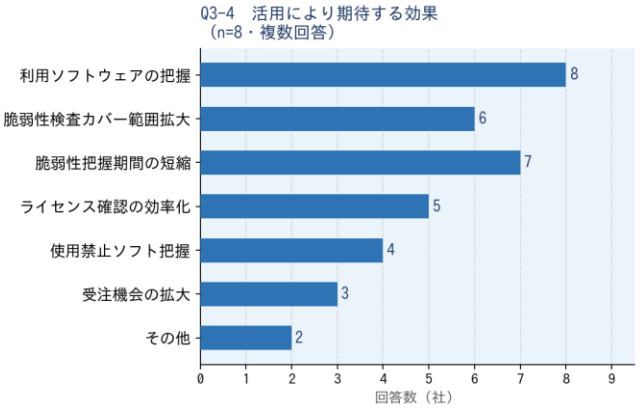




※ 複数回答あり。n=7（Q2-3）、n=8（Q3-3）

## 4. 期待される効果（Q2-4 / Q3-4）

「利用しているソフトウェアが把握できること」（作成側 6 社・活用側 8 社）、「脆弱性の有無の把握期間短縮」（作成側 6 社・活用側 7 社）への期待が高い。これは SBOM の基本的な価値（ソフトウェア構成の可視化→脆弱性対応の迅速化）と合致しており、品質・運用性の要素が特に重要（→ 本知見集 第 4 章 4.2・4.6 節）。

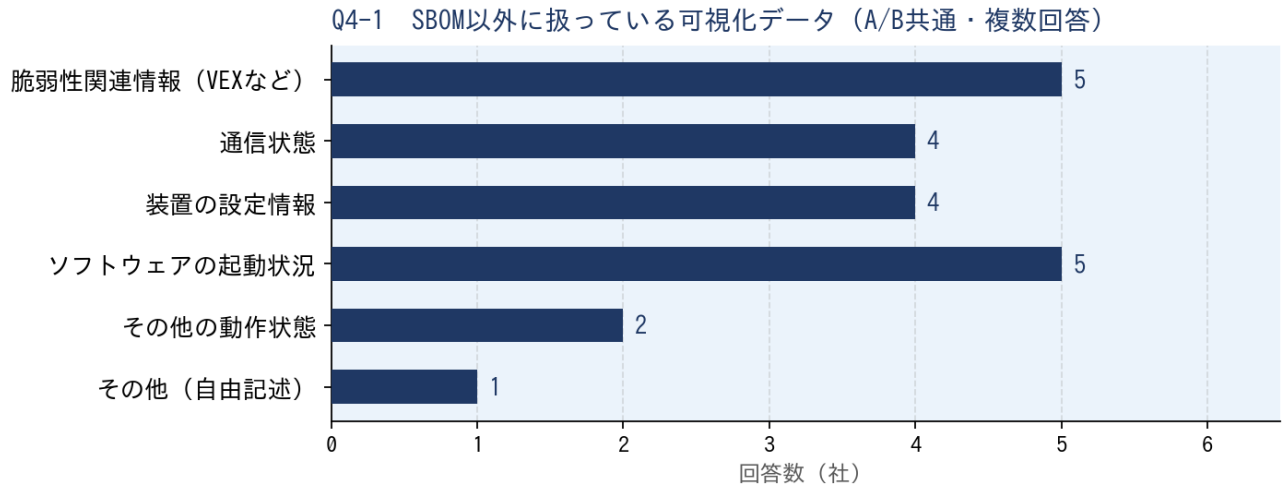



※ 複数回答あり。n=7（Q2-4）、n=8（Q3-4）

## 5. SBOM 以外に扱っている可視化データ（Q4-1）

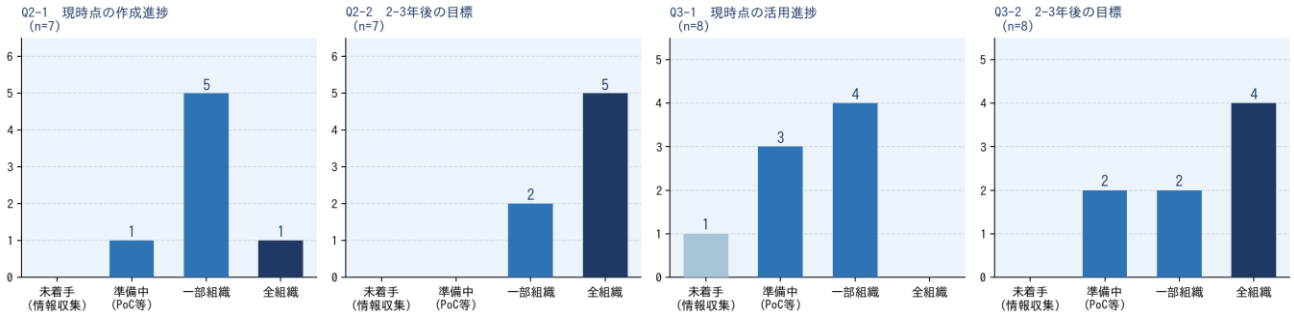
SBOM に加え、「脆弱性関連情報（VEX など）」（5 社）・「ソフトウェアの起動状況」（5 社）・「通信状態」「装置の設定情報」（各 4 社）など多岐にわたる可視化データが活用されている。本知見集が「可視化データ」を SBOM に限定せず広義に捉える理由の一つとして、こうした実態が挙げられる（→ 本知見集 第 2 章 2.2 節）。




※ 複数回答あり。A/B 共通設問。

## 6. 現状と今後の進捗目標（Q2-1 / Q2-2 / Q3-1 / Q3-2）

作成側では現状「一部組織で作成」（5 社）が主流だが、2〜3 年後は「全組織での作成」（5 社）を目指す回答が多い。活用側では現状「一部組織で活用」（4 社）が主流で、2〜3 年後は「全組織での活用」（4 社）を志向する。段階的な拡大意欲が示されており、組織全体への展開に向けた実務定着の仕組みづくりが課題となる（→ 本知見集 第 5 章 5.4 節）。




※ 単一回答。n=7（作成側）、n=8（活用側）

用語集

| 用語 | 定義 |
| --- | --- |
| サプライヤー | サプライチェーンにおいて、部品・コンポーネント・素材等を他の事業者に提供する側の事業者。本知見集では、可視化データを「つくる側」の代表的な立場の一つとして位置づけられる。 |
| ベンダー | サプライチェーンにおいて、製品・ソフトウェア・サービス等を開発・販売する側の事業者。サプライヤーから受け取った部品等を組み込んだ製品を構成し、インテグレーターやユーザー事業者に提供する。 |
| インテグレーター | サプライチェーンにおいて、複数のベンダーの製品・システムを組み合わせてソリューションとして提供する側の事業者。可視化データの生成・共有・活用の各段階に関わる立場にある。 |
| ユーザー事業者 | サプライチェーンを通じて提供される製品・システム・サービスを最終的に利用・運用する側の事業者。本知見集では、可視化データを「つかう側」の主要な立場として位置づけられる。 |
| 開発担当 | 製品・システムの構成情報の生成・管理や、SBOM をはじめとする可視化データの作成・更新に関わる担当者（セキュリティを兼務する IT 担当者を含む）。図 図 1 においてはサプライヤー・ベンダーにあたる立場に該当する。 |
| PSIRT | 自社製品に関する脆弱性情報の収集・分析・対応調整を担うチーム。脆弱性公表時の影響範囲特定や、顧客・ステークホルダーへの情報提供において可視化データを活用する。ベンダーにあたる立場での機能が典型的である。 |
| CSIRT | 組織内のサイバーセキュリティインシデント対応を担うチーム。攻撃発生時の影響範囲特定・封じ込め・復旧において可視化データを参照し、取引先インシデントが自組織に与える影響評価も行う。インテグレーター・ユーザー事業者に相当する立場での機能が典型的である。 |
| セキュリティ透明性 | サプライチェーンを通して開発・提供される機器やシステムの構成・依存関係・セキュリティ状態・取引関係などを、関係者が必要に応じて参照・活用できる状態にすること。単に情報をデジタル化することではなく、必要な主体が必要な情報に適切なタイミングでアクセスし、意思決定や対応に活用できる状態を実現することを本質としている。 |
| 可視化データ | サプライチェーンを通じたシステムや製品の構成、依存関係、セキュリティ状態、取引関係などを、組織間で参照・共有・活用できる形式に整理した情報の |

| 用語 | 定義 |
| --- | --- |
| | 総称。SBOM はその代表例であるが、ハードウェア構成情報、取引先のセキュリティ対策状況、BCP/BIA 情報、連絡先・契約情報なども含まれる。 |
| 品質 | 可視化データが実態と一致し、誤り・欠落・不整合が少ない状態のこと。品質が欠けると、脆弱性の影響を受けるシステムの特定漏れや、復旧優先順位付けの誤りが生じやすくなる。本知見集で整理する可視化データに求められる 5 要素のうちの一つ。 |
| 真正性 | データの出所と生成～流通過程が追跡でき、判断根拠として信頼できることを指す。真正性が担保されないと、取引先から提供された可視化データが実態を反映しているかを独立して検証できず、リスク評価の判断根拠が不安定になる。本知見集で整理する 5 要素のうちの一つ。 |
| 適用性 | 読みやすく取り込みやすい形で、意思決定に必要な情報が明確に示されていることを指す。適用性が低いと、緊急時にデータを迅速に参照・活用することが困難になる。SBOM であれば CycloneDX や SPDX といった標準フォーマットへの準拠が適用性の向上につながる。本知見集で整理する 5 要素のうちの一つ。 |
| 完全性 | データが改ざんされておらず、一貫性が保たれていることを指す。生成後～利用までの間に変更がないことを技術的に検証できる状態（電子署名・ハッシュ値等による検証）が望ましい。本知見集で整理する 5 要素のうちの一つ。 |
| 運用性 | 可視化データを継続的に更新し、環境変化（構成変更・脆弱性発見・体制変更等）を反映できる仕組みがあることを指す。更新を続ける仕組みの欠如が、Log4j や国内製造業の各事例における根本的な失敗要因の一つとして示されている。本知見集で整理する 5 要素のうちの一つ。 |
| SBOM （Software Bill of Materials） | ソフトウェアのコンポーネントやそれらの依存関係の情報を含めた機械処理可能なインベントリー（一覧表）のこと。OSS だけでなくプロプライエタリソフトウェアにも活用でき、可視化データの代表的な形式の一つである。主な標準フォーマットとして CycloneDX および SPDX が広く使われている。 |
| CycloneDX | OWASP が策定した SBOM の標準フォーマット。JSON・XML 形式に対応しており、脆弱性データベース（NVD 等）との連携が容易なため、脆弱性管理での自動活用に適している。本知見集では適用性の観点から標準フォーマット準拠の一例として挙げられている。 |
| SPDX | The Linux Foundation が策定した SBOM の標準フォーマット。ISO/IEC |

| 用語 | 定義 |
| --- | --- |
| | 5962:2021 として国際標準化されており、ライセンス情報の管理にも対応している。CycloneDX と並ぶ代表的な SBOM 標準フォーマットとして、適用性確保の観点から活用が推奨される。 |
| CVE | ソフトウェアやファームウェアの脆弱性を一意に識別するための共通識別子。MITRE が管理する。SBOM 等の可視化データと CVE を組み合わせることで、脆弱性公表時に影響を受けるコンポーネントを自動的に特定できる。 |
| NVD | 米国 NIST が管理する脆弱性情報データベース。CVE をベースに CVSS スコアや影響範囲の情報を付与して公開している。SBOM と NVD を連携させることで、自組織が利用するコンポーネントの脆弱性該当状況を効率的に確認できる。 |
| CRA | EU が策定したサイバーレジリエンス法。デジタル要素を持つ製品に対してセキュリティ要件を課し、SBOM 等の可視化データの整備・開示を求める制度的枠組みの一つ。製品のライフサイクル全体を通じた脆弱性対応・開示義務も規定している。 |
| DPP | EU が推進するデジタルプロダクトパスポート。製品の環境・素材・構成情報をデジタルで管理・開示する仕組みであり、サプライチェーンの透明性確保に向けた制度的枠組みの一つ。CRA と並び、可視化データの整備を事業者に求める動きの代表例として本知見集で言及されている。 |
| JC-STAR | 経済産業省が推進する国内の SBOM 関連制度・取り組みの一つ。本知見集では、経産省の SBOM ガイドラインとともに、国内制度との整合性を確認する際の参照先として位置づけられている。 |
| BCP | 事業継続計画。インシデント発生時にも事業を継続・早期復旧するための計画を指す。医療機関ランサムウェア攻撃の事例では、BCP 情報が可視化・共有されていなかったことが復旧の長期化につながったとして、可視化データとして整備すべき情報の一つに位置づけられている。 |
| BIA | ビジネス影響度分析。インシデント発生時に業務・システムが受ける影響の程度と優先復旧順位を分析するプロセス。BCP と組み合わせて BCP/BIA 情報として可視化・管理することで、緊急時の迅速な意思決定を支援できる。 |
| DevSecOps | 開発（Development）・セキュリティ（Security）・運用（Operations）を統合したソフトウェア開発・運用のアプローチ。SBOM の生成・更新を開発・CI/CD パイプラインに組み込むことで、可視化データの継続的な最新化（運 |

| 用語 | 定義 |
| --- | --- |
| | 用性の確保）を実現する手法として本知見集で言及されている。 |
| Log4j 脆弱性 | 2021 年 12 月に公表された Java のログライブラリ「Apache Log4j」に存在した深刻なリモートコード実行脆弱性（CVE-2021-44228）。本知見集では、ソフトウェア構成の可視化が不十分な状態で深刻な脆弱性が公表されたとき、影響範囲を迅速に特定できなかった事例として第 3 章で分析されている。 |

セキュリティ・トランスペアレンシー・コンソーシアム活動成果
「可視化データの実践活用に向けて～実務者向け～」

発行　　セキュリティ・トランスペアレンシー・コンソーシアム

連絡先：stc-info@st-consortium.org
URL：https://www.st-consortium.org

## 利用条件・免責事項等

利用について

本書は、サプライチェーンにおけるセキュリティ透明性向上のため、広く活用されることを目的として公開しています。出典を明記の上での引用を歓迎します。

引用・転載

著作権法上認められる引用は、出典を明記することにより利用できます。本書の全部又は一部を転載、複製又は改変して再配布する場合は、事前に本コンソーシアムへお問い合わせください。

免責事項

本書は、発行時点で入手可能な情報及び知見に基づいて作成したものです。本書に掲載された内容の正確性・完全性、有用性、最新性又は特定の目的への適合性について、いかなる保証も行うものではありません。本書の利用により生じたいかなる損害についても、本コンソーシアム及び参加組織は責任を負いません。本書の内容は、予告なく変更、訂正又は削除される場合があります。

商標

本書に記載されている会社名、製品名、サービス名等は、それぞれ各社又は各団体の商標又は登録商標です。

知的財産に関する考え方

本コンソーシアムは知的財産権の取得・管理を目的とする団体ではなく、知見の共有及び普及を目的として活動しています。本書についても、その趣旨に沿って広く活用されることを期待しています。

著作権