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

「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～」

2024 年 10 月 21 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 背景

製品・システム・サービス等の高度化が進むにつれて、サプライチェーンは複雑かつ深く広くなり、結果としてサプライチェーンにおいて生じるセキュリティリスクは見落とされやすくなります。サプライチェーンでは、リスクを適切に捉え評価することが難しく、サプライチェーンに参加するすべての事業者にとってサプライチェーンセキュリティリスク対策は経営上の重要課題になっています。

この課題への対処として、製品等におけるセキュリティの透明性を向上する取り組みが注目されています[1]。特に欧米では、製品等のソフトウェア構成に関する「可視化データ」を SBOM フォーマット（ソフトウェア部品を一覧化する標準データ形式）によって作成・提供することをサプライチェーンの各事業者に求める動きが活発化しています。このような中、日本では経済産業省が、2024 年 8 月 29 日に、「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」[2]（以下、「導入手引」）を公表し、SBOM の導入促進に取り組んでいます。

1.2 本コンソーシアムの活動ビジョン

製品等のサプライヤーが SBOM 等によって可視化データを「つくる側」の役割を担うことが典型的には考えられますが、そのためには可視化データの作成・提供コストに見合うレベルの効果的な可視化データの活用が不可欠です。逆に言えば、可視化データを「つかう側」における効果的な活用方法が明確であればあるほど、可視化データのさらなる作成及び提供を促され、活用の拡大を生む好循環につながるものと考えられます。

また、可視化データの活用方法の検討には、セキュリティ部門のみならず、対象となる製品等の調達に関わる部門や経営者などの様々な関係者がそれぞれの立場から関わり、組織全体として統一的に取り組むことが重要です。サプライチェーンは組織全体に様々な形で影響を及ぼすことから、多様な立場から問題・課題認識をもって対処にあたることが可視化データの価値ある活用方法を広く考案することにつながります。

---

[1] NTT 技術ジャーナル 2024 年 9 月号特集記事　「サプライチェーンにおけるセキュリティ透明性の向上と活用に向けた取り組み」,https://journal.ntt.co.jp/article/29301

[2] 「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」,
https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf

本コンソーシアムでは、上記の考え方に基づいて可視化データの「つかう側」が直面する問題・課題を提起し、その対処策の具現化に向けた本コンソーシアムの活動方針を定めた活動ビジョン[3]を 2024 年 2 月に公表しました。

1.3 本書の目的

本書は、上記の活動ビジョンに基づき会員企業が共同で検討した成果(知見)をまとめたものであり、特に「脆弱性管理において SBOM 等の可視化データを活用するシーン」を対象としています。

なお、本コンソーシアムでは、活動ビジョンに基づいて、特定の業種や業界に縛られない参加事業者の拡大と、可視化データのより魅力的な活用方法の具現化に引き続き取り組んで参ります。

1.4 本書の構成

本書は、1 章において背景・目的などを述べた後、2 章において脆弱性管理に可視化データを活用することで、各アクタにもたらされる価値について示しています。3 章においては活動ビジョンで提起した 8 つの問題・課題に対して、脆弱性管理に活用した場合に役立つ知見の分析結果を示し、個々の知見の具体的な実施内容を 4 章において示しています。

1.5（参考）本書と経済産業省の「導入手引」の関係

経済産業省が策定した「導入手引」では、主にソフトウェアサプライヤー向けに、SBOM を導入するメリットや実際に導入するにあたって認識・実施すべきポイント、SBOM 導入の効果及びコストを勘案して実際に SBOM を導入することが妥当な範囲を検討するためのフレームワーク、委託先との契約等において SBOM に関して規定すべき事項（要求事項、責任、コスト負担、権利等）などが幅広くまとめられています。

さらに、本書と同様に脆弱性管理業務を対象として、ソフトウェアの脆弱性を管理する一連プロセスにおいて SBOM を効果的に活用するための具体的な手順と考え方をまとめた「脆弱性管理プロセスの具体化」が記載されており、SBOM を活用した脆弱性管理の全体像を把握することができます。

前述のとおり本書も脆弱性管理に可視化データを活用するシーンを対象としていることから、本書の作成にあたっては「導入手引」を参考にして検討を行い、脆弱性管理の実務において相補的に両文書を活用できるようまとめています。

---

[3] 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ビジョン「セキュリティ透明性の向上と活用に向けて」https://www.st-consortium.org/?page_id=1066

2　脆弱性管理における可視化データ活用の価値

多様なソフトウェアサプライチェーンを通じて製品・システム・サービスが提供されており、脆弱性に気が付かず攻撃されてしまうケースがあります。このような中で、構成品の中身を可視化した可視化データは、脆弱性等のリスク確認を容易にし、脆弱性の残留リスクの低減をもたらすと考えられています。本書においては、この可視化データ活用のユースケースとして現在特に期待されている脆弱性管理を対象とし、2.1 節においては、可視化データを活用した脆弱性管理のプロセスとそのアクタを示し、2.2 節においては、可視化データを「つかう側」である各アクタにとって、どのような価値をもたされるのかを示します。

2.1　可視化データを活用した脆弱性管理におけるアクタとプロセス

本書では、製品等のサプライチェーンに関わる複数の事業者の存在も考慮し、可視化データを活用した脆弱性管理プロセスにおける代表的なアクタを採用しています（図 1 参照）。

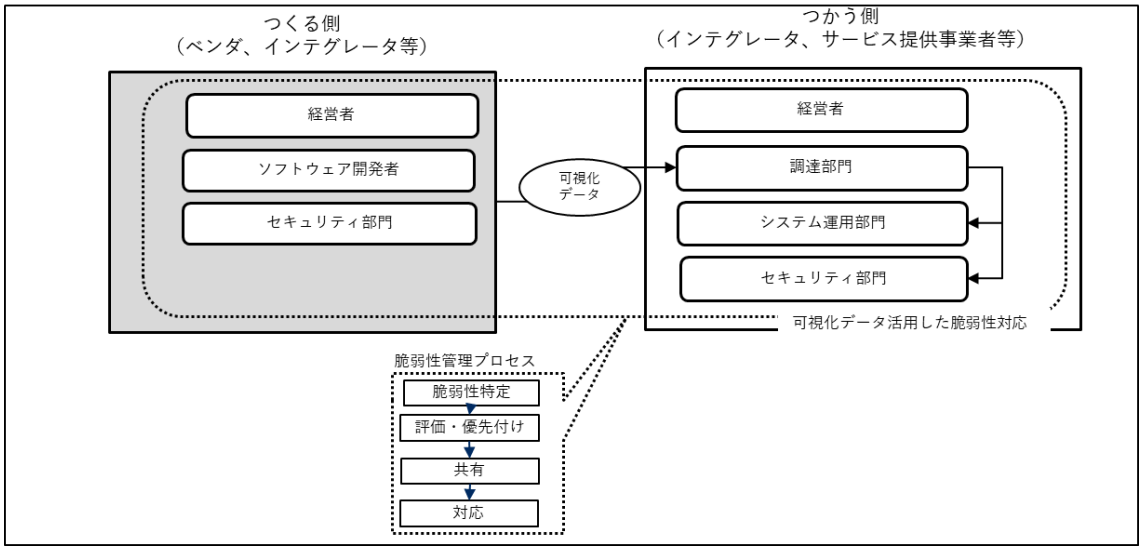

図 1　可視化データを活用した脆弱性管理の主なアクタとプロセス

SBOM 等の可視化データを「つくる側」のアクタとしては、経営者や、製品等に組み込むソフトウェアを開発するソフトウェア開発者や、開発した製品等のセキュリティ向上やインシデント対応を行うセキュリティ部門があります。一方、可視化データを「つかう側」のアクタとしては、経営者に加え、製品等を調達する調達部門や調達した製品等の運用を行うシステム運用部門、脆弱性対応を担当

するセキュリティ部門があります。

続いて脆弱性管理のプロセスについてです。「つくる側」が作成した可視化データは「つかう側」の調達部門を経由して、システム運用部門やセキュリティ部門に共有されます。「つかう側」のアクタが可視化データを用いて脆弱性管理を行う場合には、「脆弱性特定」、「評価・優先付け」、「共有」、「対応」のプロセスとなります。各プロセスは、一般的にはセキュリティ部門を中心に対応することが想定されますが、「脆弱性特定」プロセスにおいては調達部門との連携や、「評価・優先付け」プロセスではシステム運用部門と連携しながらの対応が想定されます。「共有」、「対応」プロセスにおいては、調達部門およびシステム運用部門と連携します。また、全てのプロセスにおいて、「つかう側」だけでなく「つくる側」のソフトウェア開発者やセキュリティ部門と連携する場合もあります。

なお、上述した脆弱性管理プロセスについては、経済産業省が策定した「導入手引」に記載の「SBOM を活用した脆弱性管理プロセスの重要ステップと手順」も参考としています。

2.2　可視化データ活用によりもたらされる価値

「つかう側」のアクタである、経営者、調達部門、システム運用部門、セキュリティ部門の各々の視点で、脆弱性管理における困り事と、可視化データを活用することでもたらされる価値を記載します。

✓ 経営者

- 経営者にとっては、脆弱性管理は直接の利益を生まないので、できるだけ低コストで、最低限での対策や体制に留めたいと考える場合が多いです。その一方で、インシデントが発生した時の損失は非常に膨大になることが多く、対策の投資対効果について、適切に判断できないという困り事があります。業界や法制度に関するものや競合他社での対策を参考にすることも多いですが、判断材料として十分であるとは言えない状況です。
- 可視化データは、自社及びサプライチェーン上の提供する製品・システム・サービス等の透明性を高め、脆弱性のリスク把握の正確性が増すため、投資額を絞ることによる被害のリスクと過剰投資による収支の悪化を低減できる可能性が高まります。これにより、企業全体のセキュリティ費用を適正化でき、必要最低限のベストな費用のリスク管理措置の実施判断等、経営者の役割として要求される適切なセキュリティリスクの経営判断ができます。また、可視化データに基づいた正確な情報をもとに経営判断していることをステークホルダーに説明することで、経営責任を果たしていることを主張できます。

「サイバーセキュリティ経営ガイドライン Ver3.0」[4]においても、「サイバーセキュリティに関する情報の収集、共有及び開示の促進」が経営者に求められており、可視化データの活用が期待されています。

✓ 調達部門
- 調達部門にとって、ベンダから調達する製品が安全であるかは最大の関心事になりますが、製品のサプライチェーンが複雑になる中、製品が安全であるかを容易に判断できない困り事があります。また、インシデント対応時に、迅速に解決するためのベンダとの連携方法がわからない懸念もあります。
- 可視化データを活用することで、調達する製品の透明性が増すので、保護すべき対象の把握とそこに潜む脆弱性などのリスク確認を容易にできる可能性が高まります。

✓ セキュリティ部門
- セキュリティ部門にとって、脆弱性の残留リスクを把握することは非常に重要であり、そのためにセキュリティアセスメントは欠かせない作業になりますが、脆弱性の残留リスクが複雑化する中、セキュリティアセスメントを実施するための手順も複雑化し、稼働が逼迫してしまう困り事があります。
- セキュリティアセスメントに可視化データを活用することで、利用しているソフトウェアの透明性が高まり、セキュリティアセスメントを効率的に行えるだけでなく信頼性の向上に繋がります。

✓ システム運用部門
- システム運用部門にとって、運用システムに脆弱性が含まれていることに気が付かず、その脆弱性を悪用されることで重要な情報の漏えい等のインシデントが発生しないかが関心事の一つになります。更に、インシデント対処の時間が膨大となり、その間に被害が拡大してしまわないかも関心事となります。特に、業務に影響を及ぼすことを回避したいが、具体的な対処方法までは確立できていないという困り事があります。
- 可視化データの活用により、運用システムの透明性が高まり、脆弱性の把握が容易に行えるようになると共に、サプライチェーン上の必要な組織間で共有を行うことで、脆弱性対応の効率化が期待できます。

[4] 経済産業省　独立行政法人　情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0」
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

3　脆弱性管理において可視化データを「つかう側」が直面する課題

本コンソーシアムは、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」を公表しましたが、可視化データは、図 2 に示すとおり SBOM (Software Bill of Materials)により取り扱える情報だけでなく、ソフトウェアやハードウェアの構成情報、実際の使われ方などを示す状態情報、および脆弱性情報などのリスク情報が含まれます。

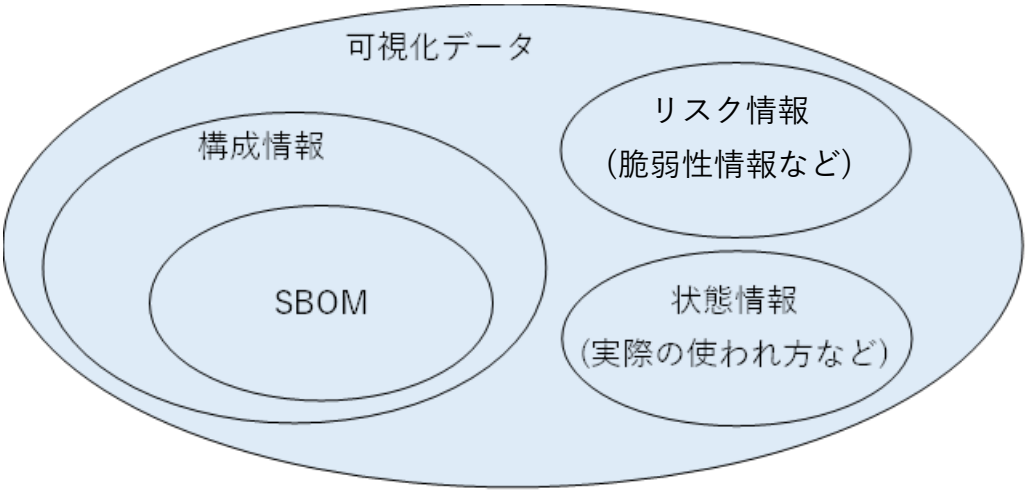

図 2　可視化データの分類

脆弱性管理において活用する可視化データの例としては、ソフトウェア構成情報（SBOM を含む）及びネットワーク構成情報、ソースコード、バイナリコード、開発文書などが構成情報に該当し、外部アクセス可否情報及びシステム設定情報などが状態情報、脆弱性情報などがリスク情報に該当することになります。

また、図 3 に示すように、活動ビジョンでは、これら可視化データを「つかう側」が直面する８つの問題・課題を提起しました。

(1) 社会浸透・認知 可視化データの価値が具体的に理解できないため、どう利用してよいかわからない等	(5) 継続的な活用 ソフトウェア更新時に正しい可視化データを継続的に入手する必要がある等
(2) フォーマット・データ 可視化データを統一的に扱うために「つかう側」の活用方針を定めなくてはいけない等	(6) サプライチェーン上の調整 多段のサプライチェーン上で「つくる側」と「つかう側」の相互共有のしくみが必要等
(3) 技術・ツール 膨大な可視化データを扱うためには自動化が必要等	(7) 可視化データがもたらす影響 可視化データによってセキュリティの透明性が高まり、従来は見えず対処していなかった事象にも対処が必要となる等
(4) 活用コスト 可視化データの導入がもたらす業務の変化に対応するため、担当者の教育や関連ツールの習熟を効率的に行える必要がある等	(8) その他 可視化データ活用は従来の業務には含まれていないため、業務体制の見直しが必要になる等

図 3　可視化データ活用における８つの問題・課題

これら８つの問題・課題は、可視化データの特定の活用方法を示しているわけではないので、脆弱性管理に活用した場合の課題として整理し、課題に対処するために必要と思われる知見について分析しました。その結果を以下に示します。

- (1)社会浸透・認知

  可視化データの価値が、特に「つかう側」で十分に浸透しておらず、脆弱性管理に拘らずに「つかう側」の活用シーンを増大させる検討なども必要になってきます。脆弱性管理を先行ユースケースとして可視化データ活用の価値を伝えていくことで、脆弱性以外のユースケースにおいても可視化データの活用が拡大していくことが期待できます。このことが社会浸透にもつながっていくと考えられるため、(2)以降の課題対処を優先します。

- (2)フォーマット・データ

  SBOM は、用途により複数の標準仕様が存在し、SBOM のデータフォーマットが同一でも、SBOM 生成ツールの出力内容にバラつきが生じる場合があります。脆弱性管理においては、脆弱性特定に用いる可視化データの品質を正しく評価できないと、本来は必要なかった対応が発生する場合があります。また、対応すべき脆弱性がみつけられなかったか等、実務レベルでは非常に切実な状況があります。可視化データを評価するための指標について、4.1「可視化データの品質指標」に示します。本知見は、脆弱性管理の脆弱性特定プロ

セスで有益と考えます。

- (3)技術・ツール

  脆弱性管理においては、多様な事業者からの可視化データを過不足なく収集することは脆弱性特定に非常に重要です。可視化データに対応する多様な技術・ツールが既に利用可能になっていますが、ユースケースによっては十分とは言えない可能性もあります。脆弱性管理においても可視化データを「つかう側」がうまく使いこなせるのかは切実な課題で、対処するための知見創出が必要です。可視化データを脆弱性管理にどう使っていくかについて、4.2「脆弱性管理における可視化データ活用」に示します。本知見は、脆弱性管理の脆弱性特定プロセスで有益と考えます。

- (4)活用コスト

  脆弱性管理に可視化データを活用すると、「つかう側」であるセキュリティ運用部門の担当者が、これまでにない業務変化に対応する必要が生じます。具体的には、関係者間での意思決定やコミュニケーションにおいて、可視化データを正しく理解していく必要があり、そのために人材育成も急務となり、教育に関する知見も必要になっていきます。「つかう側」が可視化データ自体を理解し、脆弱性対応に活用するために必要な教育については、0「可視化データをつかうための教育」に示します。

- (5)継続的な活用

  脆弱性管理は可視化データを活用する前から行われているケースも多く、利用する製品・サービス・システムによっては、可視化データの活用を段階的に進めていくことが必要になってくる場合もあります。脆弱性管理に可視化データを段階的に活用していくかについて、0「既存業務からのマイグレーション」に示します。

- (6)サプライチェーン上の調整

  製品・サービス・システムのサプライチェーンは多段構成であることが多く、脆弱性が発生した場合には、組織内だけでなく組織を越えた相互協力が必要となります。例えば、可視化データを「つかう側」であるサービス提供事業者が、「つくる側」であるインテグレータとの契約関係で必要事項を定めたりすることが必要になります。また、サービス提供事業者が利用するインテグレータから提供されたソフトウェアの中には、可視化データが提供されない場合も想定されます。このように、サプライチェーン上で合意形成に関す

る知見は非常に重要となります。組織間での相互協力や合計形成に関する知見は、4.5「可視化データの円滑運用に向けた体制整備」で示します。

- (7)可視化データがもたらす影響

  可視化データが浸透し、セキュリティの透明性が高まると、脆弱性情報データベースの照合によって、大量の脆弱性が検出され、従来は対処が不要な事象についても、対処の判断が求められるケースが増えてきます。そのため、検出された脆弱性を適切に評価・優先付けを行うための知見が求められます。評価・優先付けの指標や効率的に行う知見を 0「脆弱性対応優先付けの指標」で示します。本知見は、脆弱性管理の評価・優先付けプロセスで有益と考えます。

- (8)その他

  可視化データの活用は、従来の業務には含まれず、各種ツールによる自動化や継続的なデータ更新も踏まえ、業務体制を見直していく必要があります。脆弱性管理においては、「つかう側」が直面する様々な課題があり、これらの対処方法により、業務体制が変わってくる可能性が考えられます。そのため、まずは(7)までの課題対処の知見創出を優先させていきますが、4.3、4.4、4.5の知見は、業務体制が見直しになる場合にも役立つ知見です。

4　課題に対処するための知見

3 章では、脆弱性管理における可視化データを「つかう側」が直面する課題を述べましたが、課題に対処するために役立つ知見を以下に示します。なお本書では、「つかう側」のセキュリティ部門向けを中心とした知見となっており、一部は調達部門や「つくる側」のソフトウェア開発者向けの知見もあります。4.1 以降では、個々の知見を記載しますが、＜背景＞においては、コンソーシアム活動で得られた知見を説明するための前提条件などを示し、知見の実施内容などの具体的な内容は＜内容＞で示します。

4.1　可視化データの品質指標

✓　＜背景＞

可視化データの品質が低い場合、その可視化データに基づいて脆弱性管理を実施しても、信頼性のない結果となってしまいます。可視化データの品質に関する課題をいくつか紹介し、どうすればよいかを考えます。

【課題 1 ：最小要素不足】

米国の NTIA では可視化データの一種である SBOM の品質を定め、SBOM の最小要素、推奨要素および追加要素について定義を行っています。

最小要素は、ソフトウェアの名称、ベンダ、そのソフトウェアを構成するコンポーネント等があり、ソフトウェア本体やそのコンポーネントを識別するために必要な最低限のデータです。現状、SBOM の作成ツールやコンポーネントに関する情報である名称や識別子に関する記載、ベンダやバージョンに関する記載は比較的多いですが、SBOM の作成者や作成時刻に関する記載は少ない状況でした。なお、各要素における記載状況は以下のとおりです（詳細な記載割合については、参考文献(http://id.nii.ac.jp/1001/00228550/)に記載されています）。

表 1　SBOM の最小要素の記載割合

要素	記載割合
SBOM の作成ツールやコンポーネントに関する名称や識別子	9 割程度
ベンダやバージョン	6 割程度
SBOM の作成者	3 割程度
SBOM の作成時刻	1 割程度

SBOM 作成者や作成時刻は、最小要素でもあり、「つかう側」の視点として今後、

これら情報が明確に記載されることに期待します。

【課題２：要素の表現が不適切・表記ゆれ】

可視化データの要素があっても表現が不適切であると、利用できない情報となってしまいます。SBOM の要素にはソフトウェアの開発元を示すベンダ項目がありますが、例えば、httpd というソフトウェアのベンダ項目に Apache が記載されていれば、開発元は Apache であることがわかります。しかし、pip や maven のようなソフトウェア管理マネージャ名が記載されている場合もあり、開発元が特定できなくなってしまいます。開発元が特定できないと、そのソフトウェアの脆弱性やバグといった問題点が存在するか確認できません。また、バージョンにソフトウェアレポジトリのブランチ名を記載しても、厳密ではないのでソフトウェアに問題があった際に正確に調査できなくなってしまう恐れがあります。

要素の表記にゆれがあると、可視化データの利用者は混乱してしまいます。例えばベンダ名や製品名の表記ゆれとしてよくあるのが略称と正式名称です。表記ゆれがあると脆弱性データベースとの機械的なマッチングができなくなってしまうので、脆弱性の検知漏れの恐れがあります。

以上のように、今後可視化データに記載された情報が適切な表現か確認・検証する技術、および表現を統一したり、名寄せしたりする技術が必要になるのではないかと考えます。

【課題３：コンポーネントの網羅性】

可視化データで表現されるソフトウェアコンポーネントはソフトウェア間の利用関係（依存関係）を表現していると考えることができます。依存関係には明示的なものと暗黙的なものが存在します。

明示的依存関係とはソフトウェアのパッケージ情報から提供されている依存関係を指します。例えば、Linux のディストリビュージョンではパッケージを利用してソフトウェアを管理しており、パッケージにはソフトウェアの依存関係を示す情報（Depends, Build-Depends といった項目）が含まれており、ソフトウェアをインストールする際に依存しているソフトウェアも同様にインストールされます。パッケージ情報に記されている明示的な依存関係を参照することで、ソフトウェアが依存しているコンポーネントを明らかにすることができます。

一方で、暗黙的依存関係は明示的依存関係に現れない依存関係を指します。つまり、パッケージ情報には記されないソフトウェアの依存関係であり、ソースコードのコピーペーストや一部を改変した再利用によって発生します。暗黙的依存関係は隠れた依存関係となり、発見できていないと脆弱性管理の際に脆弱性が存在することに気づけなくなってしまいます。そのため、パッケージ情報のみでなく、コ

ードベース関係性を検知・把握する技術を利用することで暗黙的依存関係を明らかにすることが必要と考えます。

以上の３つの課題が可視化データの品質に存在していると考えます。

✓ ＜内容＞

上記の３つの課題も含めて、可視化データを通じてソフトウェアの透明性を評価し、確かな透明性をもつソフトウェアを明らかにする仕組みが必要になってきます。開発者から提供されるソフトウェアに関する情報の豊富さ、正確さを軸に，これらの程度を評価するため観点をいくつか紹介します。各観点の詳細について参考文献（http://id.nii.ac.jp/1001/00228550/）を参照ください。

表 2　ソフトウェアに関する情報の評価観点

分類	観点
提供情報の豊富さ	ソフトウェアに対して十分説明がなされているか
	コンポーネントに対して十分説明がなされているか
提供情報の正確さ	コンポーネントに関する追加情報の提供があるか
	コンポーネントに関する情報の意図的な消去があるか
	コンポーネントが十分可視化できているか
	依存関係の深さが十分可視化できているか

「提供情報の豊富さ」とはソフトウェアの目的･動作等を十分に説明しているかという観点です。説明が十分にない場合、ソフトウェア利用者は正しくソフトウェアの仕組みを理解せずに利用することになり、脆弱性の残留リスクにさらされます。例えば、ソフトウェアに情報の外部送信機能があることを知らずに利用した場合、情報漏えいにつながってしまいます。

「提供情報の正確さ」とは「つくる側」が提供する可視化データの情報が正確なものであるかという観点です。コンポーネント情報の意図的な消去があるか、ソフトウェアのコンポーネント数や依存関係の深さが十分可視化されているかを「つかう側」で把握することが大事です。依存関係の深さはコンポーネントのトレーサビリティに相当し、直接的に利用しているものだけでなく間接的に利用しているもの可視化されていることが「つかう側」にとってのメリットになります。

このように可視化データに基づいてソフトウェアの透明性を評価できるようにすること、加えて、重要なコンポーネントの透明性が可視化できているか評価することで「つかう側」のソフトウェア選定の一助になることが期待されます。

4.2　脆弱性管理における可視化データ活用

✓　＜背景＞

2.1 で述べたように、可視化データを用いた脆弱性管理では、「脆弱性特定」「評価・優先付け」「共有」「対応」のプロセスが発生します。

なお、ここでの「脆弱性特定」とは、「組織が使用するソフトウェアに対して、発生したソフトウェア脆弱性による影響の有無を判断すること」を指します。

可視化データを脆弱性管理に活用する上で、『可視化データをもとにした脆弱性の影響調査・分析を行う』、『可視化データそのものを脆弱性情報の把握に用いる』の 2 つの観点が存在します。前者は、可視化データの要素の一つである構成情報を用いて「脆弱性特定」からソフトウェア脆弱性管理におけるそれぞれのプロセスを行う流れを想定しており、後者は、可視化データ内に記載された脆弱性情報そのものを「つかう側」が活用して「脆弱性特定」に必要な情報を収集することを想定しています。

本節では、ソフトウェア脆弱性管理のプロセスの中でも「脆弱性特定」「評価・優先付け」について、『可視化データをもとにした脆弱性の影響調査・分析を行う』の観点で知見をまとめ、一部『可視化データを脆弱性情報の把握に用いる』の観点について触れることとします。

✓　＜内容＞

「脆弱性特定」においては、脆弱性の影響を受けるソフトウェアの名称やそのソフトウェアにおいて脆弱性の影響を受けるバージョンの情報を収集し、組織内で当該のソフトウェアを使用していないか調査します。可視化データを活用して「脆弱性特定」を行う場合は、可視化データの要素の一つである SBOM などのソフトウェア構成情報を用いて、収集した脆弱性情報との突合を行うことができます。一例として、脆弱性情報と可視化データの突合のイメージを以下に示します。

■脆弱性情報

└　脆弱性の影響を受けるソフトウェアの名称・バージョン

↕

■可視化データの要素（SBOM）

└　構成情報として記録されているソフトウェアの名称・バージョン

これらの活用例として、脆弱性情報を提供するサービスや脆弱性データベース、各種ソフトウェアベンダのサイトを参照し、SBOM に記載された情報と機械的に突合するサービス・仕組みを構築することが挙げられます。組織のセキュリティ部門が、組織内で利用・展開しているソフトウェアの SBOM を管理することで、脆弱性特定に係る工数の削減や脆弱性の残留リスクを低減する効果が期待できます

（経済産業省が実施した実証では、SBOM を活用した脆弱性管理によって、従来の手動管理に比べて管理工数を 70%程度削減した報告が挙げられています [2])。一方で、機械的な突合を行うにあたって生じる表記ゆれの課題や、組織における SBOM の導入コストが課題ですが、それらについては、今後の WG 内の議論で知見創出を目指します。「評価・優先付け」のプロセスにおいては、「脆弱性特定」で脆弱性の影響が有ると判断されたソフトウェアに対して、当該脆弱性に対する対応の緊急性を評価します。具体的な評価の方法や指標については、4.6.2 で紹介します。

「評価・優先付け」のプロセスにおいては、ソフトウェアが稼働するシステム自体のセキュリティ設定や FW 等のアクセスコントロール機器によるセキュリティ制御に加え、脆弱性情報そのものを用いることが想定されます。背景で述べた『可視化データそのものを脆弱性情報の把握に用いる』という観点は、このプロセスにおいて活用されることが期待されます。一例として、可視化データの要素の一つとして VEX(Vulnerability Exploitability eXchange)を含める例が挙げられます。VEX は、ソフトウェアベンダ(つくる側)からユーザ企業(つかう側)へ「その製品が既知の脆弱性の影響を受けるか」といった情報を提供するための一つの文書形式であるが、これを用いて「評価・優先付け」を行うことが期待されます。[5]

[5] 「令和 4 年度 サイバー・フィジカル・セキュリティ対策促進事業 SBOM を導入・活用するサプライチェーンモデルの構築に向けた調査・実証事業報告書」, https://www.meti.go.jp/meti_lib/report/2022FY/000372.pdf

4.3　可視化データをつかうための教育

✓　＜背景＞

SBOM をはじめとした可視化データを企業内で運用するには、可視化データの活用に携わる担当者がデータに含まれる情報を理解・検証の上、業務での意思決定・コミュニケーションにおいて活用しなければなりません。

この点、SBOM ツールや脆弱性管理ツール等、可視化データを人間が理解しやすいような UI を備えたツールも登場し、それに伴い可視化データも機械可読な形式で作成・流通しつつあります。しかし、依然として人間が可視化データを読み取る必要が生じる場面は存在します。例えばツールで入出力した際に意図した結果にならない、表示される情報に疑義がある等でトラブルシューティングが必要な場合は、目検で可視化データに問題が無いか確認する場合があります。また、SPDX-Lite 形式の SBOM のように、そもそも手運用を想定した可視化データも存在します。

このような場合に、可視化データの種類やそれぞれの目的・内容・形式、実務上の用途に応じた参照箇所・読解方法を担当者が理解できていないと、可視化データの品質上の問題が特定・対処されないままとなったり、脆弱性対応の際に担当者の混乱により対応リードタイムが増加したりする等の悪影響が懸念されます。本来サプライチェーンセキュリティリスクを軽減するために運用する可視化データにより、かえってリスクが増加してしまうという本末転倒な事態にもなりかねないため、対策が必要と考えられます。

✓　＜内容＞

上記の課題への対策として、可視化データの活用に携わる担当者が、可視化データ自体への理解を深めるための教育プログラムを実施することが挙げられます。ここでは、SBOM を例に、本コンソーシアム会員が実施した社内教育の内容を例示します。

- 「(1)ソフトウェアサプライチェーンにおけるサイバーセキュリティリスクの高まり」

  SBOM の意義を理解頂くための前提知識として、自業界におけるソフトウェア開発の環境変化、環境変化への対策としての OSS・商用オフザシェルフ活用やソフトウェア開発外注の必要性、OSS・商用オフザシェルフや外注による脆弱性混入の可能性を解説しました。生成 AI による自動コード生成の利用が広がっていることへの対応として、生成 AI の OSS コードスニペット出力による脆弱性混入の可能性に言及することも有用でした。

- 「(2)SBOM の意義」

全社的・社会的な SBOM の意義も重要ですが、社内教育としては、受講者の業務におけるメリットに言及することも重要でした。例えば、セキュリティ部門の担当者に対しては脆弱性の自動監視の実現を訴求した一方、利用者・ソフトウェア運用部門・ソフトウェア開発者に対しては利用コンポーネントの可視化による開発時検証の効率化や、脆弱性発生時の対応責任有無のエビデンスとして利用可能な点を訴求しました。

- 「(3)SBOM の構成と解読方法」

  SBOM に何がどこに書いてあるかを、SBOM の実データを交えて解説しました。SBOM 規格の位置づけや制約についてもここで解説することで、SBOM 規格についての知識普及や誤解の解消にもつながりました。

- 「(4)自社における SBOM 運用ルール」

  ソフトウェアサプライチェーン・ソフトウェアライフサイクルにおいて、SBOM を作成・活用するために必要な業務や、自社の業務との対応関係を示しました。

- 「(5)（適宜）SBOM ツールの運用方法」

  SBOM ツールを導入済の場合、SBOM を作成・活用するための業務の実施手順を理解頂くため、実際の SBOM ツールを表示・操作しつつ手順を解説することで、受講者が SBOM 運用を具体的にイメージできるようになりました

  特に、「SBOM の構成と解読方法」において、SBOM の実データを見せることが効果的でした。SBOM への理解が浅い段階であると、SBOM そのもののイメージが全くつかない受講者や、ハードウェアの BOM と混同していた受講者、SBOM ツールの出力結果の画面を SBOM と同一視している受講者等が見られました。そこで、自社の開発ソフトウェアに近しい仮想的なケースを提示し、SBOM 規格である SPDX 形式・CycloneDX 形式の SBOM でそれらがどのように表現されるかを例示することで、「SBOM のどの項目に何の情報が表示されるのか」の理解を深めることに繋がりました。

図 4　SBOM の構成と解読方法の説明用資料イメージ（Covalent 株式会社作成）

NVD 等脆弱性データベースや、VEX 等の機械可読なセキュリティアドバイザリについても、同様のアプローチが適用可能と期待されます。CVSS・対象バージョン・対策の公開有無・影響有無の判定結果等、脆弱性対応の実務においてセキュリティ部門の担当者が参照すべき情報が実データ上のどの項目に記載されているか教育することで、脆弱性情報からの必要情報の抽出を円滑化でき、脆弱性対応のリードタイム短縮に有効と期待されます。

可視化データを活用可能な人材の育成は、社会全体としてサプライチェーンセキュリティリスクを低減する上で有効な取組と認識しています。今後への提言として、可視化データを有効的に活用するために必要な知識・技術を整理したスキルセットの定義や、スキルセットを十分有することを証明する資格認定制度の構築を進めることで、可視化データを活用する人材のスキルレベルの平準化を通じて、社会全体でのサプライチェーンセキュリティリスク低減に寄与すると期待されます。

4.4. 既存業務からのマイグレーション

✓ ＜背景＞

可視化データを活用しての脆弱性管理を一気に進めるのは現実的ではありません。可視化データは多種多様なサプライヤーに関連するので、可視化データのない運用から、可視化データ全体の運用に一挙に切り替えることは困難です。現在の脆弱性管理に対して段階的、かつ部分的に浸透させていくことで、普及を促進させていくことが可能になります。

✓ ＜内容＞

現状では、「つくる側」であるベンダ等から脆弱性情報の通知を受けて、「つかう側」であるサービス提供事業者等はパッチ適応を実施しています。まずは、第一段階として、この取り組みに SBOM などの可視化データを追加して、何のパッチがあたっているかを可視化することで、「つかう側」の管理責任を果たせるようにしていきます。まずは、可視化することから始めます。徐々に可視化データを提供していくことで、その範囲を広げていきます。

そして、可視化データ(SBOM)がある程度揃うようになったら、第二段階として、可視化データを活用した脆弱性の評価を CVSS の基本評価基準で実施します。調達した機器やシステムごとに実施するので、可視化データがそろった機器から適用してくことが容易です。CVSS の基本評価基準での評価の実施は、「つくる側」であるベンダ等で実施することが理想です。その結果を「つかう側」であるサービス提供事業者に送付するのが望ましいです。しかし、可視化データ(SBOM)や脆弱性情報の提供のサービスを受けられない場合は、不足分を「つかう側」で実施することも最近は容易です。SBOM などの可視化データを脆弱性診断サービスに登録しておく、または、SBOM 生成ツールでバイナリから SBOM を生成してサービスに登録しておくことで、自動的に基本評価基準での脆弱性診断を実施するサービスも提供されてきています。

ここまで普及してきたら、第三段階として、CVSS の環境評価基準に相当する脆弱性診断を実施することが現実的になってきます。CVSS の基本評価基準での診断では、過検知の可能性が高いアラートが上がってきます。様々な機器やシステムで基本評価基準での評価結果がそろってくると、統合されたシステムにおいて、環境値を組み込んだ、環境評価基準での評価を実施し、対策の実施を最小限に絞り込むことが可能になります。

4.5. 可視化データの円滑運用に向けた体制整備

✓ <背景>

自社が開発するソフトウェアにベンダの開発範囲が含まれる場合、脆弱性対応が発生した場合はベンダの協力が必要となります。例えば、脆弱性情報を確認した際に、ベンダの開発範囲に影響を及ぼすかを調査・回答頂くことが必要な他、影響がある場合にはベンダに改修を実施頂く必要があります。対象のソフトウェアが使用するソフトウェア部品の可視化データがベンダ（「つくる側」）から提供されない場合、使用するソフトウェア部品を「つかう側」で当該部品の脆弱性の監視や対応ができず、ソフトウェア全体での脆弱性管理を行えなくなります。

このような、脆弱性発生時にベンダに実施頂く必要のある対応は、契約上の義務として規定し、金銭負担の所在を明確化しなければ、円滑な対応は期待しがたいものとなります。そこで、使用するソフトウェア部品の「つかう側」とベンダ（「つくる側」）との間での契約、およびその前段階の RFP・見積条件において、可視化データの提供や脆弱性管理における役割分担など、脆弱性対応に関する対応内容を明文化し、ベンダと合意することが必要となります。一方で、脆弱性対応についての明文化状況は、企業によってバラつきがあります。

明文化の阻害要因の一つとして、明文化すべき要件の網羅性・具体性担保の難しさが挙げられます。契約上で必要な要件が漏れている、運用可能なレベルまで具体的に規定できていない等で、実際の脆弱性対応時にベンダと契約上の疑問点が顕在化し、脆弱性対応が円滑に進まない場合があります。例えば、脆弱性の監視・報告・対応のそもそもの進め方や、監視・報告すべき脆弱性の範囲や、対応要否・優先付けの基準、コミュニケーションプランが契約上明確でない結果、脆弱性および対応状況を誰に・いつまで・どの連絡手段で・何の情報をどう記載して連絡すべきか分からない状態に陥ります。疑問点につき、インテグレータまたはベンダの片方が一方的に条件を設定し、契約時点で十分レビューされないまま契約が進んだ結果、脆弱性発生時に契約のスコープ・金銭負担に関するトラブルが発生する場合もあります。

また、脆弱性対応に関する画一的なモデルを定めることが難しい点も、明文化の阻害要因となっています。脆弱性対応を明文化しようとした際にベンダと合意可能な内容は、ベンダとの契約体系や交渉力等の関係性、ベンダの企業体力に左右されます。ソフトウェア開発・サイバーセキュリティに関する業界的な規範・慣行も脆弱性対応に影響を与え、画一的なモデルを定めることを難しくしています。例えば組込ソフトウェア開発では、知財保護等の観点から慣習的に情報開示を最小限にする傾向があります。また、可視化データ（SBOM）に含まれる使用部品の一覧がサイバー攻撃に悪用される懸念等から、他社への共有には抵抗感がある企業も

存在します。

契約主体双方のサイバーセキュリティおよび関連規範への認識の相違も、明文化の阻害要因として挙げられます。例えば、欧州サイバーレジリエンス法（EU CRA）における「SBOM を公開する義務を負うべきではない」との記述の解釈の違いにより、SBOM 開示可否についてベンダとトラブルが発生した事例があります。なお、CRA における「公開」とは自社の Web サイト等に SBOM を掲載するなどして不特定の第三者が入手できる状態にすることを指していますが、情報開示を最小限にしたい意向を背景に、このような解釈の違いが生じるものと思われます。

✓ ＜内容＞

上記の課題への対策として、脆弱性対応の明文化に向けたベンダとの交渉準備にあたり、以下を実行することを推奨します。

① 脆弱性対応明文化の要件洗い出し

② ベンダによる合理的で現実的な可視化データ共有範囲の整理を通じた、各論点での要求内容調整

以下、①②を進める上での知見を解説します。

① 脆弱性対応明文化の要件洗い出し

脆弱性対応の運用上必要な合意内容が契約から漏れることが無いよう、そもそも明文化すべき要件が何かを洗い出すことを推奨します。その際には、各種のモデル契約書や、同業界の他社が公開しているベンダ要件等を参照することで、重要な条項の漏れを防ぐことができます。

特に、同業界の他社事例は、実務の実態に即していると期待できることや、要求内容が業界の相場と照らしても妥当であることをベンダとの契約交渉で示す根拠として有効と期待されます。ここでは、欧州の自動車メーカーが、ソフトウェア調達の際にベンダに要求している脆弱性対応の要件を例として紹介します。

表 3　適切な脆弱性対応に向けた取引先との契約内容（例）

カテゴリ	取引先との契約内容例
対応プロセス	・ 脆弱性の上市後監視・対応プロセスの確立 ・ 上市後対応の開発へのフィードバック
役割分担・責任分界	・ 取引先の納品物の脆弱性監視・対応義務を、取引先が負うこと ・ 自動車メーカー側が脆弱性対応期限を設定できる権限
対応ルール	・ 製品サイバーセキュリティ関連活動の状況管理を隔週で実施

	・構成管理ツールのアクセス権限管理を隔週で実施
成果物	成果物名と必須情報項目。以下例： ・SBOM 必須情報項目：利用するソフトウェア部品の名称、一意の識別子等 10 項目以上を明記 ・脆弱性対応結果 必須情報項目：解決策の説明、変更点、実施したテストの詳細等を明記
体制	・サイバーセキュリティ教育を受けた者のみプロジェクトに関与する旨 ・責任者の設置単位
コミュニケーションプラン	・自動車メーカー側の脆弱性対応依頼への受領確認送付義務 ・回答期限（営業日単位で設定）

② ベンダによる合理的で現実的な可視化データ共有範囲の整理を通じた、各論点での要求内容調整

先述のとおり、ベンダと合意可能な内容はベンダとの関係性や業界慣行等に左右されるため、合意可能な領域を見据え、各論点で何をベンダに要求するか調整する必要があります。

この調整に有用な軸の一つに、「ベンダによる合理的で現実的な可視化データ共有範囲」が挙げられます。ベンダから共有される可視化データが限定的であれば、自社が実施可能な対応にも制約が生じるため、そこからベンダへの要求内容を導き出すという考え方です。

「ベンダによる合理的で現実的な可視化データ共有範囲」には様々なパターンが考え得ますが、ここでは以下の(a)および(b)の場合を想定した際の要求内容調整イメージを例示します。

(a) 使用するソフトウェア部品の可視化データがベンダから提供される場合の例

この場合、使用するソフトウェア部品の可視化データがベンダから提供されるため、「つかう側」で当該部品を含めた対象のソフトウェア全体の脆弱性の監視を行うことができます。

使用するソフトウェア部品の可視化データがベンダから提供されることで「つかう側」でソフトウェア部品の脆弱性の監視が可能になりますが、検出された脆弱性の対応を行うにあたっては、情報提供やソフトウェアの修正な

どのベンダの協力が必要です。そのため、使用するソフトウェア部品の可視化データの提供、ならびに検出された脆弱性の対応にあたってベンダに協力をもとめる内容について事前に協議の上取り決め、文書を取り交わすことが望ましいです。

(b) 使用するソフトウェア部品の可視化データがベンダから提供されない場合の例

使用するソフトウェア部品の可視化データがベンダから提供されない場合、「つかう側」で当該部品の脆弱性の監視を行うことができません。この場合、当該部品の脆弱性の監視はベンダ側で行い、脆弱性が検出された際に「つかう側」へ情報や修正したソフトウェアを提供する形になります。なお、「つかう側」としては、当該部品についてはこれらのベンダから提供される情報以外の脆弱性管理も必要に応じて検討します。例えば、市中にはソースコードやバイナリデータを解析し、使用されている OSS を抽出するツールがあり、これらを利用することが考えられます。

従って、この場合では対象のソフトウェアの脆弱性管理を、当該部品を「つかう側」とベンダ（「つくる側」）で分担して行う形になります。この場合においても、同様に脆弱性管理における役割分担やベンダに協力をもとめる内容について事前に協議の上取り決め、文書を取り交わすことが望ましいです。

これらの知見に基づく対応を実行することで、契約の改定・交渉に伴う工数は追加で発生するものの、その結果脆弱性対応時に契約上の議論無く円滑にベンダとの連携が可能となり、脆弱性対応の工数・リードタイム削減、セキュリティリスクの低下に寄与すると認識しています。

4.6. 脆弱性対応優先付けの指標

4.6.1. SBOM と開発成果物間のトレーサビリティ確保

✓ ＜背景＞

ソフトウェア開発者とセキュリティ部門の担当者が脆弱性対応の優先付けを行う際は、脆弱性対応の対象ソフトウェアへの影響を踏まえて優先付けを行うため、例えば以下の事項につき判断が求められます。

- そもそも対象の脆弱性が開発したソフトウェアで発生するのか
- 発生する場合、ソフトウェア内のどこで発生するのか、波及して脆弱性の残留リスクが発生する範囲はどの程度か
- 改修必要なファイルや、改修結果を反映して更新必要な開発文書はどれか
- ベンダの開発範囲も改修必要な場合、関与すべきベンダはどこか

上記の判断を SBOM の情報のみで行うことは一般的に困難であり、ソースコードや設定ファイル、要件定義書・仕様書等の開発文書等の参照が必要となります。その際に、脆弱性に関係のあるファイル・文書を探し出すのに時間を要し、脆弱性対応の優先付けにかかる工数が増加することが課題となります。これは脆弱性対応のリードタイムの長期化要因にもなり、脆弱性の残留リスクを高める恐れがあります。最悪の場合、影響範囲を正しく特定できず、誤った優先付けおよび改修を実施するなど、脆弱性対応の品質に悪影響をもたらします。

✓ ＜内容＞

上記の課題への対策として、SBOM に起票されたコンポーネントと開発成果物間のトレーサビリティの確保を通じて、脆弱性に関係のあるファイル・成果物を探し出す工数を削減した事例が存在します。

この事例においては、あるべき姿として、SBOM に起票されたコンポーネントから脆弱性情報が発出されたものを指定するだけで、そのコンポーネントと依存関係のあるソースコード、設定に影響を与える設計ファイル、その他コンポーネントにつき言及された開発文書といった、紐づくファイル・開発成果物が自動的に特定される状態を設定しました。

上記の状態を実現すべく、トレーサビリティ管理ツールを使用して、SBOM のコンポーネント単位で、関連のあるファイル・開発文書を開発段階で紐づけて管理しました。脆弱性発生時は、対象コンポーネントをトレーサビリティ管理ツール上で指定することで、関連のあるファイル・開発文書を即時に呼び出すことに成功しました。

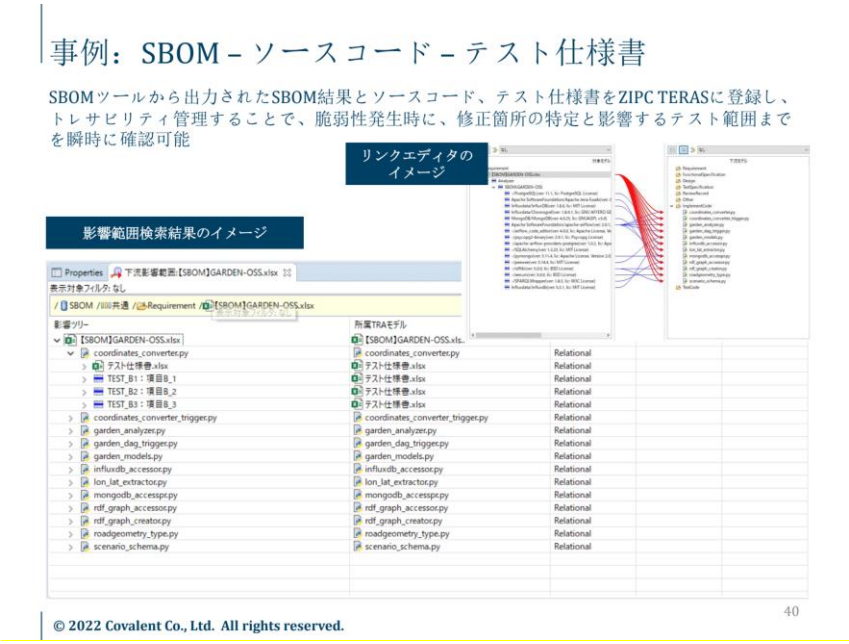

図 5　SBOM と開発成果物のトレーサビリティ管理・影響範囲検索の例
（Covalent 株式会社作成）

本事例では、SBOM と開発成果物間のトレーサビリティ確保を通じた脆弱性対応の工数削減効果も分析されました。この事例の企業においては、一つの脆弱性に対する特定から対応完了までの一連の脆弱性管理プロセスのうち、約 2 割の工数を影響範囲特定に充てていました。これは後段の脆弱性対応の計画策定にあたり、要改修範囲や改修後の再テスト範囲、その他影響のある社内ファイルを特定するための工数として必要としていました。トレーサビリティ管理ツールを使用して SBOM のコンポーネント単位で関連のあるファイル・開発文書を即時に呼び出せるようにすることで、当該工数の削減を実現しました。また、従来の手作業での影響範囲特定では影響範囲の特定漏れが発生し、後続の改修・テストでの手戻りによる工数増に繋がっていた中、トレーサビリティ管理ツールの利用によって影響範囲の特定漏れを防止し、後続対応の工数増抑制に繋げられる可能性も示唆されました。

なお、本事例の様にトレーサビリティ管理ツールを使用するためには、SBOM のコンポーネント単位で、関連のあるファイル・開発文書を紐づけることが開発段階で必要であり、そのための工数がいわゆる「初期投資」として発生する点には留意が必要です。本事例においては、当該工数を後続の脆弱性対応工数の削減分で「投資回収」できるか否かの実証には至っていません。

トレーサビリティ管理の工数は追加で発生するものの、その結果脆弱性対応時の必要情報の迅速な収集が可能となり、脆弱性対応の工数・リードタイム削減に繋

がり、脆弱性の残留リスクの低下に寄与すると期待されます。特に、サービス提供事業者とインテグレータで締結した SLA、インテグレータがベンダに求める脆弱性対応時の要件、欧州サイバーレジリエンス法をはじめとした関連法令などで、脆弱性管理プロセスのリードタイムにつき厳格な要件が定められている場合は、SBOM と開発成果物間のトレーサビリティ管理が契約履行・コンプライアンス上有用と考えられます。

4.6.2. 脆弱性評価基準

✓ ＜背景＞

可視化データの一つである SBOM を利用することで該当のソフトウェアの脆弱性を特定することができます。一般に、SBOM は OSS で広く用いられると想定されますので、多くの技術者が検証することで脆弱性が多数発見される傾向にあります。そこで、脆弱性がシステムに与える影響を判断して、脆弱性への対策を、いつ、どのように実施するべきかのトリアージをすることが、投資対効果を最大化する上で重要になります。

✓ ＜内容＞

一般的に、脆弱性の影響の判定には、CVSS「共通脆弱性評価システム」を参照し、段階的に脆弱性を評価します。CVSS は、情報システムの脆弱性に対するオープンで汎用的な評価手法であり、ベンダに依存しない共通の評価方法を提供します。CVSS を用いると、脆弱性の深刻度を同一の基準で定量的に比較できます。一般的に、３つの評価基準が定義されています。

(1) 基本評価基準（Base Metrics)

脆弱性そのものの特性を評価する基準です。ネットワークから攻撃可能かどうかといった基準で CIA を評価し、CVSS 基本値(Base Score)を算出します。 SBOM 活用の脆弱性評価サービスの基本です。

(2) 現状評価基準（Temporal Metrics)

脆弱性の現在の深刻度を評価する基準です。攻撃コードの出現有無や対策情報が利用可能であるかといった基準で評価し、CVSS 現状値(Temporal Score)を算出する。 攻撃インテリジェンスや対策情報が必要になります。

(3) 環境評価基準（Environmental Metrics)

製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する基準です。攻撃を受けた場合の二次的な被害の大きさや、組織での対象製品の使用状況といった基準で評価し、 CVSS 環境値（Environmental Score）を算出します。 環境情報や想定被害の情報が必要になりますが、正確な評価ができます。

これらの基準でどれを採用するべきか、システムのリスクの大きさや対策の難易度に則って、決定しておくことがよいです。

さて、このトリアージの関する脆弱性検査をベンダ等の「つくる側」とサービス提供事業者等の「つかう側」と分担して実施することで、全体のコストを抑制することが可能です。もっとも、最適な方法は、「つくる側」が基本評価基準で評価して、その結果を顧客である「つかう側」に通知して、「つかう側」が自身のシステムでの環境評価基準で評価する方法です。ただし、注意するべきは、「つくる側」

が脆弱性を発見しても、基本評価基準の CVSS スコアが小さいことを理由に、更新ファイルを作成しない可能性があることです。その場合、「つかう側」は、自身の環境評価基準での評価結果を通知して、対応をしなければリスクが大きいことを、数値をもって説明することで、更新ファイルを作成の必要性を主張することが理想的なコミュニケーションとなります。

5. おわりに

本書は、脆弱性管理に可視化データを活用する際に、可視化データを「つかう側」が直面する課題に対処するために、主にセキュリティ部門向けの知見をまとめたものです。本コンソーシアムでは、「つくる側」「つかう側」双方の多様な事業者が集まり議論を進めていますが、可視化データを普及推進していく上では、セキュリティ部門だけでなく、経営者向けの知見創出も必要と考えており、知見創出するための策を具現化、実行することを目指しています。また、セキュリティの透明性確保のために、脆弱性管理以外のユースケースにおいても可視化データの活用に取り組んでいきます。

本書に賛同し、ともに活動して頂ける皆さまをお待ちしております。
以下のウェサイト、もしくは連絡先までお気軽にお問合せください。

- セキュリティ・トランスペアレンシー・コンソーシアム 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

2024年9月30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。

- アラクサラネットワークス株式会社
- NRIセキュアテクノロジーズ株式会社
- 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
- 株式会社ラック
- Contrast Security, Inc.
- 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
- 東京エレクトロン株式会社
- 日本電気株式会社

- 日本電信電話株式会社
- 株式会社日立製作所
- 三井住友トラストグループ株式会社
- 三菱電機株式会社

用語集

用語	定義
経営者	ソフトウェアサプライチェーンを構成する事業者や、ソフトウェアサプライチェーンを通じて提供される製品・システム・サービスを利用する事業者の経営層
セキュリティ部門	ソフトウェアサプライチェーンを構成する事業者や、ソフトウェアサプライチェーンを通じて提供される製品・システム・サービスを利用する事業者の中で、脆弱性対応を担当する部門
調達部門	ソフトウェアサプライチェーンを通じて提供される製品･システム・サービスを調達する部門
システム利用部門	ソフトウェアサプライチェーンを通じて提供される製品･システム・サービスを利用する部門
SBOM	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も含めた機械処理可能なインベントリー(一覧表) のこと。コンポーネントやその依存関係をすべて表現している場合もある。OSS だけではなくプロプライエタリソフトウェアに活用することもでき、広く一般に公開するほか関係者だけに提示するという使用方法も存在する。
可視化データ	サプライチェーンにおいて事業者間で授受される製品・システム･サービス等などにおけるソフトウェアやハードウェアについての「構成」や「状態」、「リスク」を表現する情報のこと。 SBOM は製品などのソフトウェアについての「構成」を表現した情報であり、可視化データに含まれる。
サプライチェーン（Supply Chain）	製品とサービスの調達から始まり、ライフサイクル全体に及ぶ、組織の複数の階層間でのリソースとプロセスのリンクされたセット [ISO 28001:2007, NIST SP 800-53 Rev.5]
サプライチェーンセキュリティリスク（cybersecurity risks throughout the supply chain）	供給者やその先のサプライチェーン、その製品、またはそのサービスからから生じる危害の可能性のこと。サプライチェーン全体のサイバーセキュリティリスクは、製品およびサプライチェーンを横断するサービスの脆弱性などを悪用した脅威やサプライチェーン自体がもつ脆弱性などにより脅威が高まる。[NIST SP 800-161r1]
脆弱性（Vulnerability）	一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点のこと。[JIS Q 27000:2014]