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」

2024 年 2 月 16 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

サイバーセキュリティ対策やリスク管理において、ブラックボックス化され中身を確認することが困難な製品やシステム、サービスなどのセキュリティ管理はたいへん難しく、その構成品の存在や脆弱性に気づくことなくサイバー攻撃に悪用されるケースも少なくありません。このような中、構成品の中身を可視化したデータ（以降、可視化データ）をサイバーセキュリティ対策やリスク管理に活用する取り組みが進んでいます。特に、構成品の一部であるソフトウェア構成については、SBOM (Software Bill of Materials)と呼ばれるソフトウェア部品表によって製品やシステムの中身を可視化データとして生成する方法が、その対処策として注目されています。一方で、可視化データの作成および提供とともに、その活用性も十分に確保しなければ、可視化データの作成および提供に伴うコスト負担と釣り合わず、取り組みの効果が薄れ、形骸化すらまねくおそれがあります。つまり、可視化データを「つかう」側面からその効果と実践方法を具現化することが重要となります。

そこで本コンソーシアムでは、可視化データの社会浸透を前提とし、可視化データを「つかう」ことにより確保される透明性をもとにしたセキュリティ向上策に関する「知見の共創」について、サプライチェーンを構成する事業者が連携して取り組みを進めています。さらに、特定の業種や業界に縛られず参加事業者を募ることで、透明性がもたらす価値をより広範に発掘、具現化することをめざしています。

2. 背景

私たちが利用しているシステムやサービスは、さまざまなハードウェアやソフトウェアによって構成されています。これらは、国内外に広がる多様なサプライチェーンにおけるさまざまな環境を通じて生み出され、そして利用されています。特に、製品開発は分業化が進んでおり、製品の内部構成をすみずみまで把握することは非常に困難になっています。その結果、内在するサイバーセキュリティリスクを把握することの難易度は上がり、システムの安全な運用管理を求められる事業者の悩みは増すばかりです。

ソフトウェアに関するこの問題の象徴的な事例として、2021 年 12 月に世界的に話題となった「Log4shell」と呼ばれる脆弱性が挙げられます。これはシステムのログを記録するためのオープンソースソフトウェア(OSS) である「Apache Log4j」に関する脆弱性です。ログ出力は多くのシステムにとって必須機能であり、この OSS はログ出力用の「部品」として非常に幅広いシステムに組み込まれていたことから、多くの組織がこの脆弱性への対

応を迫られることになりました。さらに、システムのサプライチェーンを通じて間接的に部品として組み込まれているケースでは、その存在に気づかず対処が遅れるケースも発生しました。

このように、ソフトウェアサプライチェーンを通じて供給され、各組織のシステムに組み込まれた OSS がセキュリティリスクをもたらしたという点で、「Log4shell」はサプライチェーンセキュリティリスクについて多くの組織が目を向けるきっかけになりました。このように、守るべき対象の構成が複雑化し、内在するサイバーセキュリティリスクを把握することの難易度は上がる一方で、サイバー攻撃はますます巧妙化しており、サプライチェーン上でセキュリティ対策レベルが最も低い組織をねらって侵入し、目的の組織に対する攻撃も顕在化しています。したがって、サプライチェーンセキュリティリスクは、自組織のみで行うセキュリティ対策では限界があり、供給元なども含めたサプライチェーン全体での対応が求められます。また、システムの運用、及びソフトウェア更新や不具合対応などの保守もサプライチェーンに依存するため、サプライチェーンセキュリティリスクはシステムの調達・導入以後も継続する点にも留意する必要があります。

このような中、米国では大統領令(Executive Order 14028)を起点として、国家に影響を及ぼす可能性があるサプライチェーンセキュリティリスクに対抗するための取組みが活発化しています。従来からの NIST SP800 シリーズドキュメントによる政府調達先企業へのセキュリティ管理体制強化に加えて、「官民における脅威情報共有の活性化」「連邦政府における安全なクラウド及びゼロトラストアーキテクチャへの移行」などが新たに指示されました。また、政府機関による調達品に関するサプライチェーンの安全性を向上させるため、「調達品の構成情報を SBOM によって開示すること」も求められています。同様の方向性に関わる取組みは EU におけるサイバーレジリエンス法案、日本における経済安全保障推進法のように世界各国にも広がり始めています。

SBOM などの可視化データは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し、システム構成の透明性を高めセキュリティリスクを低減する効果をもたらす重要な要素となります。このような付加価値をもたらす可視化データについて、製品やシステム、サービスの供給と並行して、サプライチェーン上の必要な組織の間で共有すること、さらにそれをセキュリティ対策に活用することによって、各組織が協調してサプライチェーンセキュリティリスクに対応することが可能になります。

3. ゴール

本コンソーシアムは、SBOM などの可視化データの活用を通じて、サプライチェーン全体にわたってシステム構成の透明性を高め、自組織のみでは対応が難しいサプライチェーンセキュリティリスクの抜本的な低減をめざします。そのためには、可視化データを「つくる側」と「つかう側」のそれぞれによる取り組みが必要です。

可視化データの作成及び提供という「つくる側」の取り組みとして、SPDX や CycloneDX などの SBOM に関するデータフォーマットに関する標準化が行われています。これにより、組織横断での可視化データの授受が可能になります。また、各国が政策として可視化データの作成と提供を求める動きによって、取り組みが加速していくことが期待されます。

「つくる側」が作成した可視化データの活用性を十分に確保するためには「つかう側」の取組みが不可欠です。「つかう側」が可視化データの活用に伴うコスト負担以上の便益を享受できる状況を生み出すことが重要です(十分な費用対効果が見込まれなければ形骸化のおそれがあります)。この観点から、本コンソーシアムでは特に可視化データを「つかう側」の取り組みを加速させ、その活用性を向上させることをめざしています。

そして、SBOM などの可視化データの活用性を向上させることは、さらなる可視化データの作成と提供へとつながり、可視化データの「つくる」と「つかう」の好循環をもたらします。本コンソーシアムでは、この好循環の実現によって、サプライチェーン全体にわたって製品・システム・サービスなどの構成に関する透明性が適切かつ効果的に得られるようにし、サプライチェーンセキュリティリスクの抜本的な低減につなげることをめざしています。さらに、この製品・システム・サービスなどの構成に関する透明性は、可視化データの活用を前提としたサイバーセキュリティ対策の革新などのように、さまざまな社会課題の解決にもつながります。

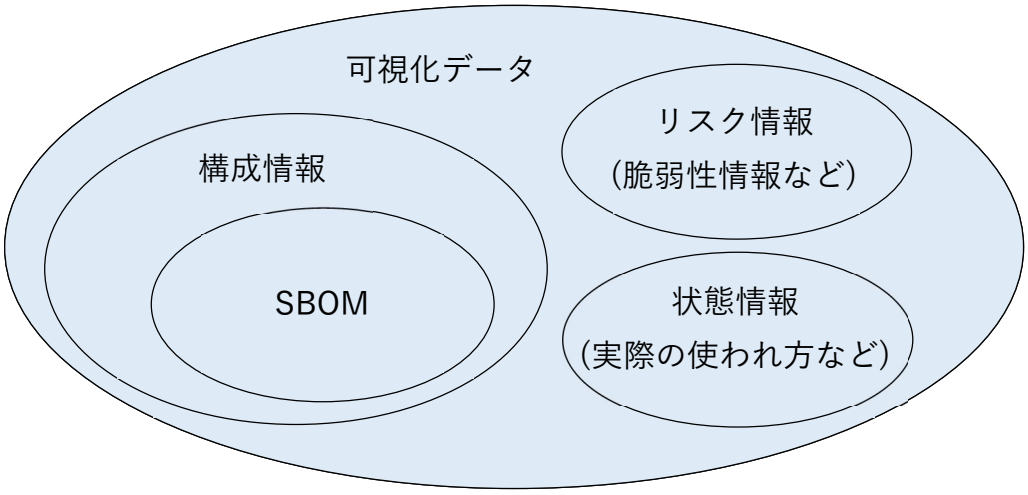
4. 問題・課題

本コンソーシアムにおける可視化データを「つかう側」の取り組みを進めるにあたり、取り扱う可視化データの考え方を整理したうえで、可視化データを活用する観点からの問題・課題について述べます。

下図に示すように可視化データには SBOM 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、状態(実際の使われ方など)、およびリスク(脆弱性など）に関連付く広範囲な情報が含まれます。ただし、議論の出発点として、本章では製品やシステムに含まれるソフトウェアに関する構成情報の表現方法としてSBOMの利用を前提とします。そのうえで、可視化データの活用に向けて対処が必要と考えられる代表的な問題やその問題解決に向けた課題について(１)から(８)に類型化して述べます。

なお、本章に記載の問題・課題は、可視化データを「つかう側」の視点によるものですが、これら問題解決に向けて取り組む必要がある課題には「つくる側」の視点によるものも存在します。例えばある製品に対するSBOMなどの可視化データについて、多くの場合はその製品ベンダが可視化データを「つくる側」であり、その製品を運用・利用する組織が可視化データを「つかう側」と理解できます。しかし、その製品を運用・利用する組織が運用上の設定変更などによりその製品の構成に変更を加える場合、当該組織が可視化データを更新することも想定され、その場合は当該組織が可視化データを「つくる側」と理解できます。つまり、一つの組織が「つくる側」、「つかう側」の双方の立場となりうることにも注意が必要です。



(1) 社会浸透・認知

- 可視化データの作成及び提供という「つくる側」の取り組みにより、社会全体で可視化データを幅広く収集できるようになることが期待されます。その一方で、現在はまだ可視化データの使い方などが十分に認知されておらず、特に可視化データを「つかう側」が可視化データの価値を具体的に理解し、使えるという認識が十分には広がっていない状況です。

- サプライチェーン全体を通じた対応のためには、活用する企業が一部に偏った状況ではなく、グローバルも含め社会全体に活用が均一に広がる必要があります。そのためには、個々の事業者により取り組みではなく、多様な事業者が協調していく必要があります。

(2) フォーマット・データ

- SBOM は標準仕様であり、可視化データのうちソフトウェアの構成を表現するフォーマットとして有用です。ただし、SBOM のデータフォーマットについては用途などに応じて複数の標準仕様が存在していることから、「つかう側」の期待とは異なるデータフォーマットの SBOM が提供される可能性があります。
- 可視化データとして SBOM を活用するためには、用途に対して必要十分な情報が記載されている必要があります。SBOM はデータ内容を柔軟に記述することができる仕様であるため、作成者の裁量に記載内容が依存する可能性があります。提供された SBOM のデータフォーマットが同一であっても、その記載項目や記載方法が製品によって異なり、SBOM を統一的に取り扱うことが難しくなる可能性に備えなければなりません。また、複数の SBOM 生成ツールの出力内容にバラつき(大文字/小文字や半角/全角の違い、一部省略など) や表記揺れがあることにも備える必要があります。
- SBOM における記載内容のバラつきは、それを「つかう側」における活用方法の違いに起因して生じる可能性もあります。産業や顧客企業ごとに必要とする情報を個別に定義して「つくる側」に求めるようになると、一つの製品などに対する SBOM であっても記載内容が異なる複数の SBOM が作成される可能性があります。

(3) 技術・ツール

- 可視化データを活用するためには、多くの事業者から広く、また過不足なく情報を収集する必要があります。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、それらが提供する情報は、「つかう側」が想定するユースケースによっては十分とは言えない可能性があり、技術・ツールの拡充とそれらを使いこなすための知見創出が必要です。
- 収集する可視化データが膨大になると、その管理や活用にあたってはツールを用いた自動化が欠かせなくなります。多くの事業者が手軽に可視化データを活用するためには、安価な技術・ツールの選択肢が存在することも重要です。

(4) 活用コスト

- 「つくる側」で必要となる可視化データ生成コストは製品・システム・サービスなどの「つかう側」への提供コストへ反映されることもあるため、可視化データの取り扱いに必要となるツールやしくみの導入コストが十分に安価である必要があります。
- 「つかう側」では、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ります。
- 「フォーマット・データ」において、一つの製品などに対する SBOM であっても記載内容が異なる複数の SBOM が作成される可能性について述べました。このことは、SBOM の作成や管理などのように「つくる側」の対応コストの増大に関する問題にもつながると考えられます。そして、そのコストは可視化データを「つかう側」が支払うコストの増大にもつながり得ることから、「つかう側」が必要とする情報を産業や企業の垣根を越えて、できる限り共通化していく努力も重要です。

(5) 継続的な活用

- 製品の運用・利用を開始した後に、ソフトウェアの継続的な更新が行われることが多くあります。この場合に、入手した可視化データが最新の製品・システム・サービスなどの内容と食い違ってしまうと、セキュリティの管理に不整合が発生するおそれがあります。おのずと「つかう側」では可視化データの継続的な内容保証を必要とするでしょう。正しい可視化データを安定的に入手可能であると同時に、「つくる側」も対応可能で合理的な対処法を検討する必要があります。
- 可視化データの対象となる製品のカスタマイズが運用・利用側において行われる場合があり、可視化データの内容を運用・利用側が更新するかもしれません。更新した可視化データに対して製品ベンダが完全な責任を負うことも、逆に運用・利用側が更新の基となった部分も含め責任を負うことも容易なことではなく、製品全体として可視化データの責任を明確にする方法が必要になります。

(6) サプライチェーン上の調整

- SBOM を含め製品のコンポーネントに関する情報は、製品ベンダにとっての機密情報である場合があり[1]、きちんとした機密保護の手段が講じられ、特定の相手に限定して開示することが必要となります。また、不注意によってそのデータが漏れると、サイバー攻撃に悪用される可能性もあり、管理は厳重に行う必要があります。このことから、「つかう側」は、まず活用を想定する可視化データの範囲を明確化

[1] NTIA(National Telecommunications and Information Administration)　Software Suppliers Playbook: SBOM Production and Provision において、サプライヤーは SBOM を競争情報とみなし、自社の SBOM が公に配布されることを望まない場合があることが指摘されている。

することが必要となり、さらに必要な可視化データを入手するためには、サプライチェーンにおける合意形成[2]が必要です。製品・システム・サービスのサプライチェーンは多段構成であることが一般的になっており、サプライチェーンを通じて可視化データを「つくる側」と「つかう側」の間で、組織を越えた相互共有の(契約に基づく)しくみが求められます。

- サプライチェーンでは製品の不具合に関する問い合わせやその対応と同様に、可視化データの正しさを確認する方法や修正を依頼する方法も必要になるでしょう。

(7) 可視化データがもたらす影響

- 可視化データの浸透によってセキュリティの透明性が高まると、従来は見えておらず対処することがなかった事象についても、対処の判断が求められるようになります。例えば、可視化データと脆弱性情報データベースの照合によって、既知の脆弱性を効率的かつ網羅的に自動確認できるようになる一方で、大量の脆弱性が検出され、脆弱性管理体制の対応能力を超えてしまう可能性を想定し、対処法を検討する必要があります。この際、照合の候補となる脆弱性情報データベースは世の中に多数存在するため、照合前に各々の脆弱性情報データベースの特性を把握し、照合の対象とする脆弱性情報データベースを選択[3]しておく必要もあります。
- 同様に可視化データの活用によって、各セキュリティ業務の実施方法を見直さなければならなくなるかもしれません。

(8) その他

- 可視化データの活用は、従来の業務には含まれていないこと、また各種ツールによる自動化を前提としていることや、継続的なデータの更新も踏まえて業務体制の見直しが必要になります。また、一般的にセキュリティ対策はIT部門が担うことが多いと言えますが、多忙なIT部門に対して安易に一任せず、全社的な業務の見直しを考える必要があります。
- 「つくる側」では、特に以下を踏まえて可視化データを生成・提供していく必要があります。
    ① 業界によっては特有な法規制やサプライチェーンモデルが存在する場合があり、それらと可視化データ活用の整合をとる必要があります。

[2] 経済産業省　第10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等検討タスクフォースの参考文献2において、製品等の調達者と供給者の間で、SBOMに求める情報項目やその情報で到達可能な脆弱性管理レベルなどを共通的な尺度を用いて合意形成を図る方法が提案されている。

[3] 経済産業省　第11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等検討タスクフォース　資料3において、脆弱性情報のカバレッジや費用等の観点から、各組織の脆弱性対応ポリシに応じた脆弱性DB選択の必要性が述べられている。

② 理論上は、製品の隅々まで可視化データを作成することが可能であるものの、製品の部品(及びその供給ベンダ)が多段構成になっている場合、現実的には可視化データをどの階層まで作成するのかを製品に応じて判断する必要があります。
③ 製品によっては構成の全体あるいは一部が非公開である場合があり、このような場合の可視化データの取り扱いについては検討が必要です。

5. コンソーシアム活動

(1) コンソーシアムの主な活動方針

セキュリティ・トランスペアレンシー・コンソーシアムでは、前述のような問題・課題に関する対処策の具現化をめざします。その活動方針の柱は「A)知見の共創」と「B)多様な事業者の協調」です。

A) 知見の共創
- 可視化データを「つくる」取り組みに呼応して、それらを「つかう」ことによって確保される「透明性」をもとにした「セキュリティ向上策に関する知見を共創」に取り組みます。
- さらに、上記の「つかう」の知見を起点として「つくる」に資する知見も共創します。

B) 多様な事業者の協調
- 価値ある「つかう」をより広範から発掘・具現化するため、特定の業種・業界に縛られず参加事業者を募り、可視化データによる「透明性」の活用範囲を拡大します。
- 参加事業者は、コンソーシアムを通じて「協調領域」における知見を共創・獲得し、自事業の「競争領域」に活用することとします。

(2) コンソーシアム活動内容

前述の活動方針に基づく活動項目とその主な内容は以下のとおりです。

A) 可視化データに関する技術的知見の共創
- 可視化データを「つかう側」の視点から、可視化データ活用に関する問題・課題の分析を行います。
- 上記の問題・課題について、可視化データの「つくる側」と「つかう側」の両者

の協調によって効果的に実践可能な対処策を具体化します。

- 具体的には、セキュリティ運用などを対象として参加事業者が持つ知見やノウハウを共有し、課題分析、解決策の検討、及び実証などを行います
- 上記に関する検討成果について、有用な知見から順次公表します。

B）コミュニティ形成

- 上記 A の取り組みを進めるために、上記知見の公表などを通じて、可視化データの「つくる側」と「つかう側」の両者について参加事業者の参加勧奨を行い、参加事業者の拡大を図ります。
- その際、特定の業種や分野に限定しない多様な事業者の参加を募ることで、可視化データの「つかう側」と「つくる側」の両者を含む広い視点から検討します。
- 上記 A の取り組みを通じて会員間の共通問題・共通課題認識を選定し、共に協調して問題・課題の対処に取り組む場を構築します。

C）外部連携

- 本コンソーシアムの活動を推進するにあたり、連携することが望ましい他機関・団体を選定し、関係構築のための働きかけや調整を行います。
- 本コンソーシアムと同様の問題・課題認識を持つ政府機関と官民による相補的かつ効果的な連携を行います。

(3) コンソーシアム運営指針

各活動の内容を踏まえ、以下の方針に基づきコンソーシアムを運営します。

A）多様な分野における活用法を深掘するため、サプライチェーンを形成するさまざまな立場の事業者（製品ベンダ、SI 事業者、サービス事業者、セキュリティベンダなど）を対象とする。

B）事業者間の相互信頼に基づく活動の場とするため、事業者の新規参加にあたっては参加事業者による協議を行う。

C）参加しやすい運営とするため、参加事業者には会費を求めない（あるいは最小限とする）。

D）知的財産を創出せず、参加事業者の「協調領域」を活動範囲とする。

E）参加事業者の機密情報を活動の前提とせず、各事業者が開示可能な情報のみを用いて活動する。

6. おわりに

本書において述べた問題・課題は、個別の事業者では対処困難なものであると同時に、完全な対処が困難なものも含んでいるかもしれません。本コンソーシアムでは、事業者横断による協調的な取り組みによって、そのような困難な状況を打開し、部分的あるいは段階的でも状況を改善していく策を具現化・実行することをめざしています。

本書の内容について賛同され、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・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・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

本書の公開時点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 NTT データグループ
- 株式会社ＦＦＲＩセキュリティ
- 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
- 三菱電機株式会社

7. 用語定義

用語の定義

用語	定義
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）	複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達にはじまり設計・開発・製造・加工・販売及び購入者への配送に至る一連の流れのこと。[ISO 28001:2007, NIST SP 800-53 Rev.4]
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]