URL　https://journal.ntt.co.jp/article/29274
DOI　https://doi.org/10.60249/24095102

可視化データ活用シーン拡大に向けたセキュリティ・トランスペアレンシー・コンソーシアムの活動

可視化データを活用した「サプライチェーンセキュリティリスク」への対応の促進には，サプライチェーンを形成する多様な事業者が協力し，可視化データの有効活用を進める「協調領域」の活動が重要となります．本稿では，協調領域における活動として，サプライチェーンを形成する多様な事業者が協力し，可視化データの活用促進に資する「知見の共創」に取り組むために2023年9月に発足した「セキュリティ・トランスペアレンシー・コンソーシアム」の活動と，可視化データ活用促進に向けた課題について紹介します．

キーワード：#セキュリティ・トランスペアレンシー・コンソーシアム，#可視化データ，#SBOM

熊崎　裕亮[†1※]
山田　暁[†1]
佐藤　亮太[†2]

NTT研究企画部門[†1]
NTT社会情報研究所[†2]

可視化データ活用拡大における協調の重要性

「サプライチェーンセキュリティリスク」への対応が重要な課題として認識されるようになり，国内外ではSBOM（Software Bill of Materials）をはじめとする可視化データの導入が本格的に進展しています．可視化データの普及のためには，可視化データを「つくる側」だけでなく「つかう側」も含めたサプライチェーンを形成する多様な事業者が，協調しながら可視化データの有効活用を進めることが求められるため，その「協調領域」における活動が重要となります．

本稿では，協調領域における活動の一環として，「セキュリティ・トランスペアレンシー・コンソーシアム」の活動趣旨や取り組みについて紹介します．

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

■コンソーシアムの活動方針と運営体制

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構成する多様な事業者が協調し，可視化データの活用促進に資する「知見の共創」に取り組むことを目的として，2023年9月に発足しました．

本コンソーシアムにおいては，サプライチェーンを構成する多様な事業者が協調して知見を創出し，可視化データ活用範囲を拡大する活動を推進するにあたり，以下の活動指針を掲げています．

- 多様な分野における活用法を深堀りするため，サプライチェーンを形成する多様な事業者（製品ベンダ，システムインテグレータ，セキュリティベンダ，製品・システム・サービスを利用・運用する事業者等）を対象とする．
- 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り選出された運営委員会で協議を行う．
- 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．
- 知的財産を扱わず，参加事業者の「協調領域」を活動範囲とする．
- 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．

本コンソーシアムでは，運営に関する議論を行う総会・運営委員会，そして「知見の共創」に向けたワーキンググループ（WG）という体制で活動を行っています．運営に関しては，原則すべての会員事業者が参加する総会で基本方針を決議し，随時発生する新規会員の参加に関する審議などの事項については，運営委員が参加する運営委員会における決議等により，意思決定の効率化を図っています．また，具体的な「知見の共創」に向けた活動は，WG単位で行われます．現在，WGは「可視化データ活用WG」の1つだけですが，今後は目的に応じて増設していく予定です．可視化データ活用WGは月1～2回の頻度で，対面とオンライン併用の形態で会議が開催されており，そこでは会員間の活発な意見交換が行われています．また，これらの活動の成果についてはWebサイト[(1)]を通じてオープンに発信しています．

本コンソーシアムの参加事業者については，発足時点の8事業者から，2024年7月時点では18事業者にまで拡大しています．これにより，より多くの知見が事業者間で共有され，協力体制が一層強化されています．

■可視化データの活用シーン拡大に向けた活動ビジョン

前述のとおり，可視化データの活用を広げるためには可視化データを「つくる側」だけでなく「つかう側」の取り組みも加速させることが重要となります．そこで，本コンソーシアムの活動方針，活動内容に加えて，本コンソーシアムにおいて取り扱う問題・課題として可視化データを「つかう側」が直面する問題・課題を中心に取りまとめた活動ビジョン「セキュリティ透明性の向上と活用に向けて」を2024年2月に公表しました[(2)]．

可視化データは，ソフトウェアやハードウェアの構成，リスク（脆弱性など）および状態（機器設定などの実際の使われ方）などに関連付く広範囲な情報が含まれます．

※　現，NTT西日本．

活動ビジョンの中では，まずは可視化データ活用の議論の出発点として，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代表的な表現方法であるSBOM の利用を念頭に置きながら検討を開始しています．次にこのSBOMを中心に，可視化データを「つかう側」がサプライチェーンの透明性を確保するうえで直面する課題について紹介します．

可視化データを「つかう側」が直面する課題

可視化データの活用には現状まだ多くの課題が残されています．コンソーシアムでは，「つかう側」が直面する課題を**表**のようにまとめました．ここでは，各課題の内容を簡単に紹介します．

まず，社会全体で取り組むべき課題として，課題(1)の可視化データの社会浸透・認知の不足が挙げられます．サプライチェーンセキュリティを確保するためには，一部の企業だけではなく，社会全体で協力し，サプライチェーンを構成する企業全体に可視化データの活用を広げていくことが求められます．次に，技術的観点において解くべき課題として課題(2)，(3)が挙げられます．これには，データフォーマットの統一化や，膨大な可視化データを取り扱うためのツール・技術の拡充などが挙げられます．これらは，可視化データの活用を促進するためには不可欠です．さらに，課題(4)～(8)のように，「つくる側」での可視化データ活用のためのツール導入・社内教育や，「つかう側」と「つくる側」の組織間での取り決め，「つかう側」や「つくる側」での業務体制の見直しなど，組織内・組織間で取り組む必要のある課題も挙げられます．各課題について詳しく説明していきます．

表　「つかう側」が直面する課題

(1)　社会浸透・認知の不足 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・データの未整備 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」の相互共有の仕組みが必要等
(3)　技術・ツールの不足 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)　活用コストの負担 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

■社会浸透・認知の不足

可視化データの作成および提供に取り組む「つくる側」の活動により，社会全体で可視化データを幅広く収集できることが期待されます．この取り組みによって，データの収集と共有が進展し，より多くの情報が可視化されることで，さまざまな分野での活用が促進されることが期待されます．しかしながら，現時点では可視化データの使用方法やその価値についての認識が十分に広まっておらず，特に可視化データを「つかう側」がその具体的な価値を理解し，適切に活用できるという認識がまだ十分に浸透していない状況です．

可視化データの活用が一部の企業に偏っている状況では，サプライチェーンセキュリティという観点において効果を発揮することが困難です．したがって，グローバルを含むサプライチェーンを構成する企業全体において，可視化データの活用が均等に広がることが求められます．

ただし，社会浸透の課題はそれ単体で解決できるものではないということには注意が必要です．後述するさまざまな課題をクリアしていくことで可視化データの利用価値を高め，「つかう側」自身が価値を体感できるようになることで，初めて社会浸透が加速するものと考えています．

■フォーマット・データの未整備

SBOMは，ソフトウェアの構成を表現するための標準仕様であり，可視化データを表現するうえで非常に有用です．しかし，SBOMのデータフォーマットにはさまざ

まな標準仕様が存在しており，その表記方法が異なることが問題となる場合があります．加えて，SBOMはデータ内容を柔軟に記述できる仕様であるため，その記載内容は作成者の裁量に依存しがちです．記載項目や記載方法が製品によって異なることがあり，統一的に取り扱うことが難しくなる可能性があります．

また，複数のSBOM生成ツールによって出力される内容にばらつき（例：大文字・小文字や半角・全角の違い，一部省略など）や表記揺れが発生することにも注意が必要です．さらに，SBOMの記載内容のばらつきは，利用者の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作成者に求めるようになると，１つの製品に対しても異なる記載内容を持つ複数のSBOMが作成される可能性があります．

SBOMの記載内容のばらつきは，可視化データの品質にも大きくかかわります．例えば，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し，対応すべき脆弱性がみつけられないなどの問題が発生してしまいます．

■技術・ツールの不足

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．現在，可視化データに対応する多様な技術やツールがすでに利用可能となっています．しかしながら，これらのツールが提供する情報は，使用者が想定するユースケースにおいて十分でない可能性があり，そのため技術やツールのさらなる拡充，およびそれらを効果的に利用するための知見の創出が求められています．さらに，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，安価で利用しやすい技術やツールの選択肢が存在することも重要です．

また，事業者によっては他のシステムやデータとの連携が必要になる場合もあるため，１つの選択肢として独自にカスタマイズ可能なOSS（Open Source Software）のツールの充実などが求められることも考えられます．

■活用コストの負担

「つくる側」で必要となる可視化データ生成にかかるコストは，製品やサービスを提供する際のコストに反映されるため，ツールや仕組みの導入コストは安価であることが重要です．一方で，「つかう側」では，ツールの導入コストに加え，可視化データの導入に伴う業務変化に対応するための担当者の教育やツールの習熟を効率的に行う必要があります．特に，可視化データの導入段階においては，社内での意思決定やコミュニケーションのために可視化データを正しく理解している人材の育成が急務で，これらの教育コストにも考慮する必要があります．

また，「フォーマット・データの未整備」において述べたように，１つの製品に対するSBOMでも複数の異なるSBOMが作成される可能性があり，これが「つくる側」のコスト増大につながることがあります．このコストは「つかう側」にも影響を及ぼすため，必要な情報を業界や企業の枠を超えて共通化する努力が求められます．

■継続的な活用

製品の運用・利用を開始した後にも，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．このような場合，製品調達時点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一致しないと，セキュリティ管理に不整合が生じる可能性があります．そのため，「つかう側」では可視化データの継続的な内容保証が必要となります．さらに，「つかう側」において脆弱性管理がすでに行われている場合は数多くあるため，現行の脆弱性管理から可視化データを活用した脆弱性管理へのスムーズな移行手段の確保も必要となる可能性があります．

また，可視化データの対象となる製品のカスタマイズが「つかう側」で行われる場合があります．一部分の可視化データが「つかう側」のカスタマイズによって更新された場合に，製品全体として可視化データの責任範囲を明確にする方法も必要です．

■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機密情報となることが多々あります．したがって，これらの情報は適切な機密保護手段を講じたうえで，特定の相手に限定して開示することが必要です．不注意でデータが漏洩すれば，サイバー攻撃に悪用される可能性があるため，厳重な管理が求められます．

まず，「つかう側」は活用を想定する可視化データの範囲を明確化することが求められます．そのうえで，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であり，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，組織を超えた相互協力が必要となります．例えば，契約に基づいて，ソフトウェアを調達する場合には，契約書に可視化データに関する合意形成事項を記載していく方法も考えられます．

さらに，サプライチェーンにおいては製品の不具合に関する問合せや対応と同様に，可視化データの正確性を確認する方法や修正を依頼する方法も必要です．

■「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．SBOMと外部の脆弱性データベースを用いて製品の脆弱性を管理する例ですと，SBOMと外部の脆弱性データベースなどのマッチングによって得られる脆弱性の中には，製品でのコンポーネントの利用方法によっては攻撃リスクがないようなものも多く含まれることになります．このような場合，脆弱性が製品へのどのような影響を及ぼすかを示すことができるVEX（Vulnerability Exploitability eXchange）を組み合わせることで，脆弱性対応の運用効率化を図れることもあります．

■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，各種ツールによる自動化を前提としていること，継続的なデータの更新が必要であることから，業務体制の見直しが求められます．特に，セキュリティ対策は一般的にIT部門が担当することが多いものの，多忙なIT部門に安易に一任せず，全社的な業務の見直しを考える必要があります．

また，「つくる側」では，業界特有の法規制やサプライチェーンモデルと可視化データの整合をとることが重要です．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すが，現実的には製品の部品やその供給ベンダが多段構成になっている場合，どの階層までデータを作成するのかを製品ごとに判断する必要があります．さらに，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，これらのデータの取り扱いについても検討が必要です．

おわりに

本稿では，「サプライチェーンセキュリティリスク」に対処するための協調領域における取り組みや課題について紹介しました．現在，これらの課題に対処するための知見やユースケースを公開するために，コンソーシアムの参加事業者が自社の運用知見を持ち寄り，WGで活発に議論を行っています．議論を通じて，運用知見だけでなく現在のSBOMフォーマットの限界など，これまで見えてこなかった新たな課題も見え始めてきました．これらの知見は継続的にWebサイト上で発信していく予定です．

業界全体のサプライチェーンセキュリティリスク対策の向上のため，これからも多様な事業者による多角的な視点からの知見をコンソーシアムの活動を通じて広く公開していく予定です．

■参考文献

(1) https://www.st-consortium.org/
(2) https://group.ntt/jp/newsrelease/2024/02/16/240216b.html



（左から）　熊崎　裕亮／山田　暁／佐藤　亮太

サプライチェーンセキュリティリスクへの対応には，技術的な取り組みだけでなく，事業者間の協調といった組織的な取り組みも不可欠です．私たちは，これら両面からアプローチし，サプライチェーンセキュリティの確保に取り組んでいきます．

◆問い合わせ先

NTT社会情報研究所
企画担当
E-mail　solab @ ntt.com