URL　https://journal.ntt.co.jp/article/29276
DOI　https://doi.org/10.60249/24095103

可視化データ活用によるソフトウェア脆弱性管理

ソフトウェア脆弱性管理における可視化データの活用を促進するためには，活用イメージを具体化する必要があります．本稿では，組織内で実施される脆弱性管理の個々のアクションにおける可視化データの活用例を紹介します．

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

井上（いのうえ）　陽水（あきみ）
NTTデータグループ

ソフトウェア脆弱性管理における実施事項

組織のソフトウェア脆弱性管理では「セキュリティ上の問題の有無に関する調査」「影響と対策の方向性の検討」「対策作業計画の策定」「対策の実施」の4つのアクションが発生します[1]．

「セキュリティ上の問題の有無に関する調査」とは，入手した脆弱性情報について，情報システム上の脆弱性の有無や問題が発生する条件等の調査を実施することを指します．セキュリティ担当者は，公開された脆弱性情報を基に，該当する脆弱性を持つソフトウェア製品を使用する部署や情報システムの有無を確認し，対応が必要な個所を洗い出します．この作業の一例として，セキュリティ担当者が脆弱性情報を提供する外部のサービス等を利用して収集した情報を基に，緊急対応を要するシステムがある場合は周知を行うケースがあります．この際，周知を確認したシステム担当者は，セキュリティ担当者に対して，脆弱性による影響の有無を報告し，報告を受けたセキュリティ担当者は，組織内のどこに脆弱性による影響があるかを特定し，次のアクションを実施します．

脆弱性情報は，組織内外で適切に共有しなければソフトウェアの利用者が適切な対策を実施できません．この脆弱性情報の共有については，可視化データを利用する例を後述します．

「影響と対策の方向性の検討」とは，問題個所が及ぼす影響を明確にし，修正方法や回避方法を検討することを指します．現在，ソフトウェア脆弱性は，報告件数が年々増加傾向にあり，2023年にNational Vulnerability Database（NVD）で報告された脆弱性は28297件に上っています[2]．これは1日当り約70件を超える脆弱性が報告されていることを指します．システム開発において，利用しているソフトウェアに発生した脆弱性はすべて消し込むことが理想ではあるものの，報告された脆弱性すべてに対して対処することは，対応負荷やコストの観点で現実的ではありません．そこで実際に脆弱性への対応を実施する際は，脆弱性がシステムや組織に与える影響度に応じて，対策の優先度付けを検討することも必要になります．これは，組織内で取り扱うソフトウェアや開発のスタイルを考慮して，組織のセキュリティポリシーの中であらかじめ優先度付けの指標を規定し，これを活用することが効果的です．

「対策作業計画の策定」では，対策作業を進める手順や期間について，計画を策定します．ここでは，費用や人員を勘案しつつ，対策実施に伴うサービス停止計画やテスト計画を検討します．

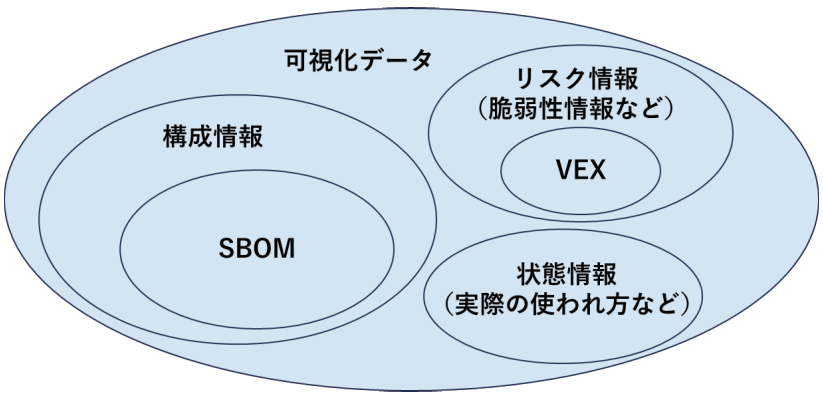
「対策作業計画の策定」で立てた計画を基に，「対策の実施」のアクションを行い，脆弱性対応の完了をめざします．セキュリティ担当者は，組織が「対策の実施」のアクションを実施したか確認することで，1つの脆弱性対応の完了判定を行うことができます．

可視化データを活用したソフトウェア脆弱性管理

ここでは，ソフトウェア脆弱性管理における可視化データの活用例として，可視化データの構成および可視化データを活用した脆弱性管理の一例を紹介します．

■可視化データの構成と脆弱性管理への活用

可視化データとは，ソフトウェア製品やシステムなどの構成を可視化したデータのことを指します．**図1**に示すように，可視化データには構成情報（ソフトウェア・ハードウェアの構成），リスク情報（脆弱性情報など），状態情報（実際の使われ方など）など広範囲の情報が含まれます[3]．



出典：https://www.st-consortium.org/?download=1103&tmstv=1719377936

図1　可視化データの構成

ここでは主に構成情報を示すフォーマットの1つであるSBOM（Software Bill of Materials）と脆弱性情報を取り扱うフォーマットの1つであるVEX（Vulnerability Exploitability eXchange）を対象に，可視化データを用いた脆弱性管理への活用事例を紹介します．

SBOMとは，ソフトウェア製品に含まれるコンポーネントとその関連情報のリストのことを指します．米国商務省のNTIA（国家電気通信情報局）では，SBOMの最小要素として，「サプライヤ名」「コンポーネント名」「コンポーネントのバージョン」「依存関係」「SBOMの作成者」「タイムスタンプ」「その他の一意な識別子」などの「データフィールド」と，SBOMを導入する組織が考慮すべきカテゴリである「自動化サポート」「プラクティスとプロセス」を定義しています[4),5)]．

VEXは，ソフトウェアベンダやその他の関係者からユーザ企業へ「ソフトウェア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機械可読なセキュリティアドバイザリの1つです．米国CISA（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）では，VEXドキュメントにどのような情報を記載するべきか，最小要件を示しており，日本国内でもすでにVEXを用いた脆弱性管理の検討が進んでいます[6)]．

前述のとおり，脆弱性対応管理の4つのアクションについて紹介しました．可視化データを脆弱性管理に活用するうえでは，その中でも特に「セキュリティ上の問題の有無に関する調査」「影響と対策の方向性の検討」に可視化データの要素が寄与することが期待されています．

経済産業省が公開している『ソフトウェア管理に向けたSBOMの導入に関する手引ver2.0（案）』では，「脆弱性の特定」「脆弱性対応優先付け」「情報共有」「脆弱性対応」のプロセスが紹介されています[5)]．ここで，「脆弱性の特定」はソフトウェアに含まれる脆弱性を特定することを，「脆弱性対応優先付け」は脆弱性を評価し対応の優先度付けを行うことを，「脆弱性の共有」は脆弱性情報を組織内外へ共有することを，「脆弱性対応」は発生した脆弱性に何らかのかたちで対処することを指します．

■可視化データを基にした脆弱性の影響調査・分析

可視化データを脆弱性管理に活用するうえでは，「可視化データを基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，可視化データを「つかう側」が可視化データの要素の1つであるソフトウェアの構成情報を用いて「脆弱性の特定」プロセスを実施する流れを想定しています．後者は，可視化データに含まれた脆弱性情報そのものを，可視化データを「つかう側」が活用して「脆弱性対応優先付け」プロセスに必要な情報を収集することを想定しています．可視化データを活用するにあたっては，その組織においてどちらのユースケースが適しているか判断したうえで，活用方法の検討を実施することが効果的です．それぞれの関係を**表**に示します．

以下では，それぞれのケースにおいて，可視化データの要素をどのように活用できるか紹介します．

まずは「可視化データを基にした脆弱性の影響調査・分析を行う」ユースケースについてです．「脆弱性の特定」では，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「脆弱性の特定」を行う場合は，可視化データの要素の1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．

実際に組織内のセキュリティ担当者が実施する場合には，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，脆弱性情報とSBOMに記載された情報とを機械的に突合する仕組みを構築することが効果的です．

セキュリティ担当者と，システム担当者による「可視化データを基にした脆弱性の影響調査・分析を行う」ケースにおける，ソフトウェア脆弱性管理の一連の流れの一例を**図2**に示します．

このうち，①～④が「脆弱性の特定」であり，⑤が「情報共有」，⑥が「脆弱性対応」のプロセスにあたります．また，③において多数の脆弱性が検出される場合に，④にて対応優先度の指標を設けて「脆弱性対応優先付け」を行い，⑤の対象を限定するようなケースも存在します．また，可視化データを活用するうえで重要なのは，⑥を実施すると，①で収集したソフトウェア構成情報も更新されている可能性がある点に留意することです．脆弱性対応の一例として，ソフトウェアコンポーネントのバージョンを変更することが挙げられます．この場合，①で収集した構成情報におけるバージョン

表　脆弱性管理のアクションと可視化データを用いたプロセスの例

ソフトウェア脆弱性管理における実施事項	可視化データを活用したソフトウェア脆弱性管理の例		
脆弱性管理のアクション	可視化データを用いたプロセスの例	各プロセスで用いる可視化データの例	可視化データの活用観点（ユースケース）の例
セキュリティ上の問題の有無に関する調査	脆弱性の特定	構成情報（SBOM）	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
影響と対策の方向性の検討	脆弱性対応優先付け	脆弱性情報（VEX） システム設定情報	可視化データそのものを脆弱性情報の把握に用いる
	情報共有	−	−
対策作業計画の策定	脆弱性対応	−	−
対策の実施		−	−

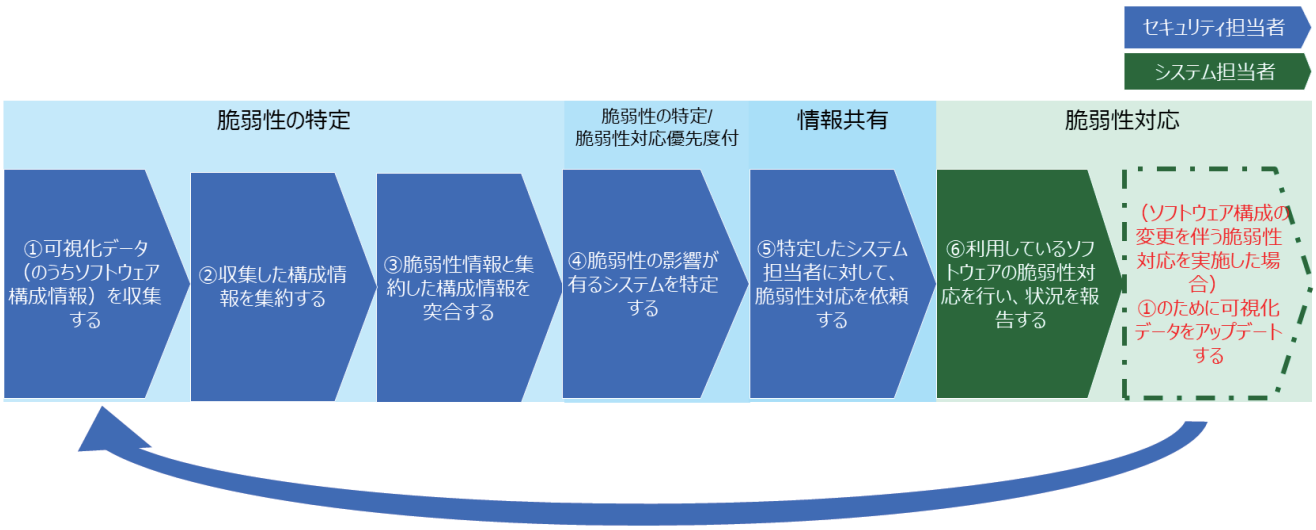


図 2　「可視化データを基にした脆弱性の影響調査・分析を行う」ケースのソフトウェア脆弱性

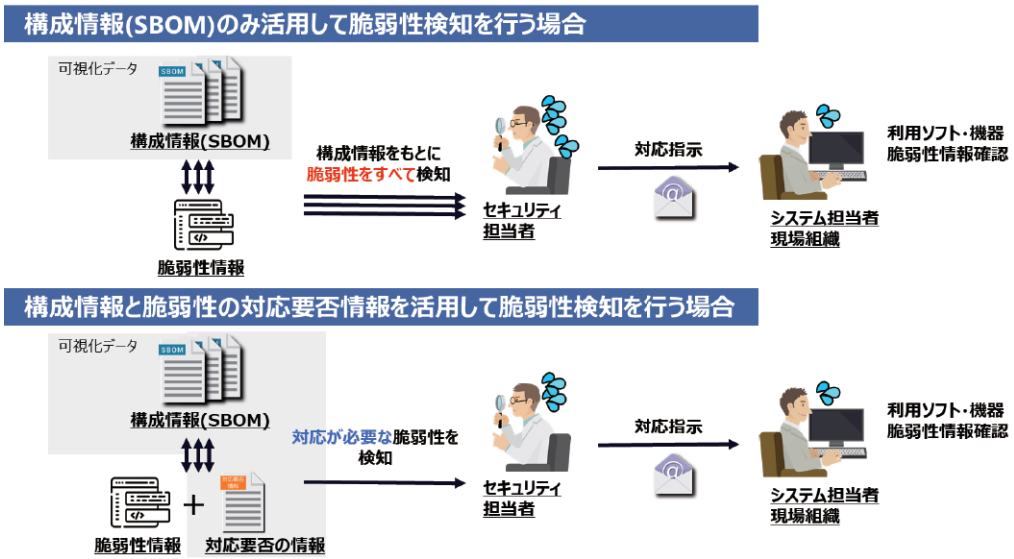


図 3　脆弱性情報を可視化データとして用いるケース

情報と，⑥の後のソフトウェアバージョン情報が異なってしまい，今後の脆弱性対応が適切に行えない可能性があります．そのため，一度構成情報を収集・集約したとしても，ソフトウェア構成の変更に伴い構成情報自体もアップデートし続けることが重要です．

上記の流れを用いることで期待される効果として，セキュリティ担当者やシステム担当者による脆弱性の特定にかかる工数の削減や脆弱性残留リスクを低減する効果が挙げられます（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[7]）．

■可視化データそのものを用いた脆弱性情報の把握

次に，「可視化データそのものを脆弱性情報の把握に用いる」ユースケースについて紹介します（**図 3**）．可視化データをこのユースケースに活用する場合は，「脆弱性対応優先付け」のプロセスへ寄与することが期待されます．

「脆弱性対応優先付け」では，システムのセキュリティ設定やアクセスコントロール機器のセキュリティ制御に加え，脆弱性情報も活用されます．ソフトウェア脆弱性は，特定の要件が満たされると脅威となるケースがほとんどです．この要件を確認する情報（設定や設計など）はシステム担当者やユーザが確認する必要があり，セキュリティ担当者は脆弱性情報を適切に伝える必要があります．また，ソフトウェア製品によっては，脆弱性が見つかっても影響がない場合があります．その場合，ソフトウェ

アベンダが情報を公開し，利用者はそれを理解し適切に対処する必要があります．例えば，Log4Shell（CVE-2021-44228）のケースでは，Log4jの脆弱性情報が公開された後も，使用しているソフトウェア製品に影響があるかを判断する必要がありました．このような場合に，可視化データを用いてソフトウェア製品ごとの影響情報を流通させる仕組みが期待されています．

具体的には，製品ベンダがソフトウェア製品に含まれるソフトウェアコンポーネントの構成や，ソフトウェアコンポーネントに含まれる脆弱性がソフトウェア製品に与える影響を調査し，その調査結果を可視化データとして公開します．これにより，利用者は製品ベンダに確認することなく，影響の有無を把握できるようになります．一方，可視化データを活用しない場合，ソフトウェア利用者は脆弱性のあるソフトウェアコンポーネントがその製品に含まれるか，含まれる場合は影響があるかどうかを製品ベンダに確認する必要があります．

OSS（Open Source Software）の普及率が増加している現在，１つのソフトウェアに対して活用されるOSSコンポーネント数も増加しています．可視化データを用いた脆弱性管理を行う場合，使用されているソフトウェアコンポーネントが多ければ多いほど，脆弱性の検知数が増加することが懸念されます．このような状況で「可視化データを基にした脆弱性の影響調査・分析を行う」場合，利用しているソフトウェア製品で使われているソフトウェアコンポーネントの脆弱性は，本当に対処が必要なのか，１つひとつ検証すると膨大な手間がかかります．そこで，可視化データを用いて，製品ごとにソフトウェアコンポーネントの脆弱性に対する対応要否の情報を連携することで，効果的な脆弱性対応管理が実施できると考えられています．

■目的に応じた可視化データの要素ごとの企業間でのやり取り

ここまで紹介したとおり，可視化データを活用したソフトウェア脆弱性管理ではいくつかの情報を組み合わせることが想定されます．可視化データはそれらソフトウェア脆弱性管理に有用な情報の組合せのサブセットであり，セキュリティ担当者は必要に応じて可視化データ以外の情報についても収集する必要があります．可視化データの収集においては，組織間で授受して脆弱性管理に活かす要素と，組織内で収集して脆弱性管理に活かす要素が存在します．

例えば，「脆弱性対応優先付け」で用いる可視化データのうち，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ファイアウォール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情報などは，攻撃者に情報が洩れることを避けるため，組織外への提供を避ける必要があります．したがって，ソフトウェアの受委託をする組織（企業）間での授受を想定せず，可視化データを使う側の組織内で収集・活用することが望ましいと考えられます．

一方で，「脆弱性対応優先付け」で用いる可視化データのうち，ソフトウェア製品ベンダが調査した脆弱性情報は，そのソフトウェアを利用する組織が自組織での影響調査を行うために必要な情報です．したがって，しかるべき方法で組織外に公開すべき情報となります．前述したVEXは，後者の情報にあたります．一例としてソフトウェアベンダが脆弱性データベースにVEXの情報を提供し，使う側は脆弱性データベースを介して情報を参照するというかたちが実際に検討されています[8]．

「脆弱性特定」で用いる可視化データのうち，SBOMのような情報は，サプライチェーンにおける脆弱性管理・責任範囲の確認の観点で，企業間で授受すべき情報です．一方で，SBOMを納品・公開した場合に発生する「ベンダ側の脆弱性確認稼働の増加」や「契約モデル」については，現在も検討が進んでおり，まだ統一的な方針はありません．そのため，仕入れ先と結んでいる契約や開発モデルに応じて，まずは自組織の中で可視化データを活用する体制を整えることが，ソフトウェア脆弱性管理の効率化に向けた第一歩であると考えます．

おわりに

現在，可視化データ，特にSBOMの活用について世界中で議論がなされています．また，実際にSBOMを作成する・管理するソリューションについても登場し始めています．一方で，ソフトウェア脆弱性管理の観点におけるサプライチェーンでのSBOMや可視化データの流通については，課題も多くあります．また，「脆弱性特定」のためにSBOMに記載されているべき情報の不足や，「脆弱性対応優先付け」のためにどのような指標を用いるべきかといった事項も検討が進んでいます．

■参考文献

(1) https://www.ipa.go.jp/security/guide/vuln/ug65p90000019by0-att/000058493.pdf
(2) https://nvd.nist.gov/vuln/data-feeds
(3) https://www.st-consortium.org/?download=1103&tmstv=1719377936
(4) https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
(5) https://www.meti.go.jp/press/2024/04/20240426001/20240426001-2.pdf
(6) https://www.cisa.gov/sites/default/files/2023-01/VEX_Use_Cases_Aprill2022.pdf
(7) https://www.meti.go.jp/press/2024/04/20240426001/20240426001-1.pdf
(8) https://www.meti.go.jp/meti_lib/report/2022FY/000372.pdf

井上　陽水

サプライチェーンセキュリティの強化に向けた可視化データ活用では，まず自組織でどのように可視化データを活用できそうか，個々の組織に合った運用を検討することが第一歩だと考えます．私たちも，引き続き検討を進めていきます．

◆問い合わせ先

NTTデータグループ
技術革新統括本部　Cloud&Infrastructure技術部
情報セキュリティ推進室
E-mail　sbom @ am.nttdata.co.jp