

ソフトウェアのセキュリティ強化を実現する SBOM (Software Bill of Materials) を活用した脆弱性管理手法

Vulnerability Management Techniques Using SBOM to Enhance Software Security



ソフトウェアのサプライチェーンセキュリティの強化の一手法としてソフトウェアの部品表 SBOM (Software Bill of Materials) を活用した脆弱性管理が注目されている。SBOM と公開脆弱性データベース情報の照合により、ソフトウェアに含まれる脆弱性の検出が可能であるが、年間 5 万件以上登録される脆弱性の中から早期対応が必要な脆弱性を適切に自動抽出し、対応しなければならない。本報では脆弱性の深刻度に加え、攻撃の受けやすさや攻撃を受けた際の被害を評価する情報を判断条件とした決定木分析による優先順位付け手法を導入し、有効性を確認した。

[三菱重工グループのマテリアリティはこちら](#)

1. はじめに

製品におけるソフトウェアの重要性が高まる一方、サプライチェーンの複雑化、OSS (Open Source Software) 利用の一般化が進んでおり、悪用された脆弱性や深刻なインシデントを迅速に抽出することで製品の安心・安全を担保することが求められている。上記を実現する一手段として、依存関係を含むソフトウェアの構成情報を可視化し適切なリスク対策を可能とする SBOM の活用が注目されている。

本報では、SBOMを活用した脆弱性管理手法について、SBOM 活用の背景と SBOM を活用したソフトウェアの脆弱性検出手法について説明した上で、検出した脆弱性に対する決定木分析を用いた層別手法について述べる。その後、層別の有効性を評価した結果を示す。

2. 製品における SBOM 活用の背景

製品開発において、機能要求に対し都度ソフトウェアを開発することは合理的ではなく、汎用的に利用可能な機能をライブラリとして開発し複数の案件に利活用する手法が一般的である。また近年ではライブラリの自社開発を行わずに他社供給ライブラリや OSS を利用することが一般的になっており、自社開発ソフトウェアでもどのようなライブラリが含まれているかを把握することが困難な状況となっている。2021 年の“Log4Shell”では、世界中のメーカーで莫大なコストをかけた調査がおこなわれる事態となった。

本例を教訓に昨今、ソフトウェアの脆弱性管理に関して SBOM を用いた脆弱性管理手法が注目されている。欧州ではデジタル製品のライフサイクルを通じたサイバーセキュリティ向上を目標とする Cyber Resilience Act (CRA) ⁽¹⁾ が公表され、CRA の付属書 I パート II の脆弱性処理要件では SBOM の作成が記載されている他、国内では経済産業省からソフトウェア管理に向けた SBOM 導入の手引き ⁽²⁾ が発行されている。

*1 総合研究所 制御システム研究部 主席研究員

*2 総合研究所 制御システム研究部 博士(工学)

SBOM とはソフトウェアを構成するライブラリやモジュール等のソフトウェアコンポーネントとその関連性及び補足情報の一覧である。具体的には、名称やバージョン情報、開発者等の情報に加え、依存関係を含めるため意図せず混入されているライブラリなどのソフトウェア情報も含まれ、機械判読可能な XML などで作成される。これにより脆弱性の特定や脆弱性修正結果の確認への短縮効果が期待される(図1)。

また SBOM はサプライチェーンの上流から下流に向かって相互共有されることでソフトウェアの透明性がより高まる。以上より、他社供給ライブラリや OSS を利用した脆弱性管理の課題に対する解決策として期待されている。

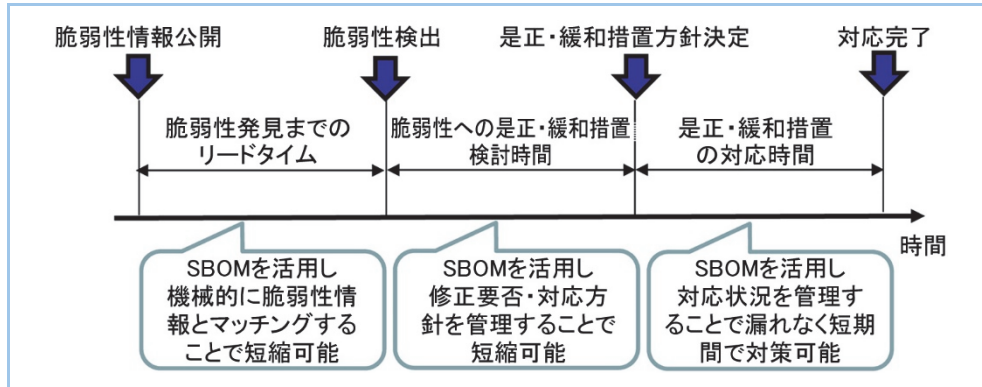


図1 SBOM 導入による脆弱性対応期間短縮のメリット

3. SBOM を活用した脆弱性検出方法の概要

発見された脆弱性の脅威度や防御策等の詳細情報は Qualcomm などの半導体メーカ(ファームウェアに潜む脆弱性)や Google, RedHat などの OS ベンダー等によって日々、収集/分析され、脆弱性データベースとして一般に公開されている⁽³⁾。代表的なものとしては、アメリカ国立標準技術研究所が管理する NVD (National Vulnerability Database)⁽⁴⁾や GitHub Advisory Database などがあげられ、NVD における 2023 年度単年での脆弱性の登録件数は 5 万件を超え、累計では 20 万件を超える脆弱性が公開されている。

SBOM を活用したソフトウェアの脆弱性検出では、SBOM に含まれるソフトウェア情報と脆弱性データベースに登録されているソフトウェア情報を基に、脆弱性の有無を専用のソフトウェアやツールで照合させる。

4. SBOM を活用した脆弱性管理システム

SBOM を活用した脆弱性管理手法を検討するにあたり、最低限必要となる自動化への対応に加え、社内運用を想定したユースケースから手動登録とローカル環境での運用を確認したため、必要要件について下記のようにまとめ、脆弱性管理システムの構築を行った。

1. SBOM 生成/登録の自動化が可能なこと。
2. SBOM の手動登録が可能なこと。
3. 外部の脆弱性データベースからの脆弱性情報の取込みが可能なこと。
4. 検出した脆弱性の対応状況が管理可能なこと。

システムの構築では、はじめに SBOM フォーマットの選定に取り組んだ。SBOM フォーマットには SPDX と CycloneDX の 2 種類が存在し、ライセンス管理には SPDX、脆弱性管理には CycloneDX が有効とされている。本報においても CycloneDX の公式サイト内 Tool Center から入手可能な生成ツールとソフトウェア構成分析ツールである Dependency-Track を組み合わせることで、上記システム要件を満たすことを確認した。

5. 脆弱性管理における課題と対応手法および評価

5.1 従来の脆弱性管理における課題

脆弱性管理では従来、脆弱性の基本的な性質に基づいた CVSS (Common Vulnerability Scoring System) ベーススコアが活用されている。CVSS ベーススコアとはソフトウェアやシステムが有する基本的な性質を基に脆弱性の深刻度を示す 0.0～10.0 の数値にて定量評価したものであり、さらにベーススコアに応じて 5 段階の深刻度レベルに分類される(表1)。脆弱性管理では上記深刻度レベルを基に脆弱性への対応方針を策定し、例えば“High”以上のものは早期対応が必要といった対応優先順位付けによる運用が行われている。

一方、CVSS ベーススコアによる優先順位付けには以下のような問題があり、ベーススコア単独での優先順位付けは適切でない。

- CVSS ベーススコアは多くの場合、対象ソフトウェアの開発元が評価するが、開発元による評価結果は高くなる傾向にあるため、多数の脆弱性において早期対応が必要となる。結果、運用形態によりアプリケーションを停止してまでの早期対応が見送られる脆弱性にまでも対応する体制が求められ実用性に欠ける。
- CVSS ベーススコアは技術的な観点でのみ評価しており、実行環境について考慮されていない。(例:インターネットへの直接接続の有無など)

このような問題に対し、本報では脆弱性の深刻度による一律の優先順位付けに加え、製品の運用形態に応じ、攻撃の受けやすさを評価する情報と攻撃を受けた際の被害を評価する情報を判断条件とした決定木分析による優先順位付け手法の適用と評価を行った。

表1 CVSS ベーススコアと深刻度レベルの定義

深刻度レベル	ベーススコア	補足
Critical	9.0 - 10.0	脆弱性がシステムに与える影響が致命的で早急な対応が必須
High	7.0 - 8.9	脆弱性が可用性・機密性・完全性の観点でシステムに影響を与える可能性が高い
Medium	4.0 - 6.9	脆弱性がシステムに与える影響がある可能性があるが、さほど高くない
Low	0.1 - 3.9	脆弱性がシステムに与える影響が限定的である
None	0.0	脆弱性がシステムに与える影響は殆どない

5.2 決定木分析による優先順位付け手法の適用

三菱重工業株式会社の製品群では火力プラントなど連続稼働を前提としているものも多く、システムの停止を伴うソフトウェアのアップデートを選別する必要がある。また、システムの停止においても関係各所との停止に向けた調整時間が必要となる。以上から、決定木分析では説明可能な判断指標を持つ Exploitation, Exposure, Utility, Well-being and Mission Impact の 4 種の判断要素を設け、以下 4 段階の優先順位を導出した⁽⁵⁾。

- Immediate: 緊急対応
攻撃を受ける可能性が高く、アプリケーション一時停止も含めた緊急対応が必要。
- Out-of-Cycle: 計画外対応
緊急対応は不要だが、早期対応が必要。
- Scheduled: 計画対応
直近で攻撃を受ける可能性は低いが、定期メンテナンス等での対応が必要。
- Defer: 静観
攻撃を受けた時の想定被害が小さいなど、リスクとして許容できるためしばらく様子を見る。

判断要素の解説を表2に、判断指標として参考にした情報の一覧を表3に示す。

表2 決定木分析における判断要素の解説

判断要素名	概要
Exploitation	現時点での脆弱性悪用状況
Exposure	攻撃を受けるアプリケーションがどの程度外部に公開されているかを評価
Utility	攻撃者視点での脆弱性の有用性
Well-being and Mission Impact	攻撃を受けた際の影響評価

表3 各判断要素における判断指標の情報源

情報	概要	情報提供元	判断要素名との紐づけ
KEV カタログ	実際に悪用が確認された脆弱性のリスト	CISA	Exploitation
EPSS スコア	対象脆弱性が 30 日以内に攻撃を受ける可能性を示した値	FIRST	Exploitation
アプリケーション実行環境 (インターネット直接接続有無)	対象アプリケーションを稼働しているサーバにおけるインターネットへの直接接続の経路有無	社内システム運用部門	Exposure
CVSS ベクトル文字列	脆弱性の特性を示す情報	NIST	Utility Well-being and Mission Impact

5.3 決定木分析による優先順位付け手法の評価

決定木分析の有効性を確認するために 2023 年 4 月～6 月に公開された脆弱性約 7000 件に対して、CVSS ベーススコアを用いた深刻度レベルによる優先順位付けと決定木による優先順位付けを用いて比較検証を行った。検証結果を表4に示す。

表4 決定木分析による優先順位付け検証結果(インターネット直接接続有)

		深刻度レベル (CVSS)				総計
		Critical	High	Medium	Low	
決定木による分析結果	Immediate	14 (0.2%)	4 (0.1%)	0 (0.0%)	0 (0.0%)	18 (0.3%)
	Out-of-Cycle	80 (1.1%)	40 (0.6%)	4 (0.1%)	0 (0.0%)	123 (1.8%)
	Scheduled	925 (13.0%)	2619 (36.7%)	1392 (19.4%)	2 (0.0%)	4939 (69.1%)
	Defer	0 (0.0%)	13 (0.2%)	1944 (27.2%)	100 (1.4%)	2057 (28.8%)
	総計	1019 (14.3%)	2676 (37.5%)	3340 (46.8%)	102 (1.4%)	7137 (100.0%)

システムへの影響が懸念され、対処が必要とされる深刻度レベル“Critical”と“High”を足し合わせた結果は全体の 51.8%となり 5.1 項であげた多くの脆弱性が早期対応の対象となる懸念が確認された。一方、決定木による分析結果では、対処が必要とされる“Immediate”と“Out-of-Cycle”を足し合わせた結果が全体の 2.1%となり、抽出された脆弱性の特徴としては、重要機能が長期的に機能停止する脆弱性、もしくは継続的に攻撃可能であり機能停止に至る脆弱性のいずれかとなり、早期対応すべき脆弱性が抽出されることを確認した。“Scheduled”内に抽出すべき脆弱性が選別されていないかについても検証したところ“CVE-2023-20867”という KEV カタログに含まれ注意喚起されている脆弱性を確認している。本脆弱性は攻撃の複雑さ、攻撃によるシステムへの影響度から早期対応は不要と判断しているが、KEV カタログを重視する場合には見直しが必要となる。また深刻度レベルでは“Medium”にもかかわらず決定木では“Out-of-Cycle”に分類される脆弱性が 4 件確認された。この 4 件は複雑な攻撃を必要とするため深刻度レベルが低くなる一方で、悪用されたもしくは悪用される可能性が高い脆弱性のため、Exploitation 及び Utility の判断指標を適用することで、早期対応の優先度付けを算出できた。以上のことから決定木による優先順位付けが対策を必要とする脆弱性の検出法として有効に機能していると言える。

また、表4はインターネット接続有を前提とした結果であるため、比較のためインターネット接続

無を前提とした検証結果を表5に示した。表4と表5の差異からインターネット接続の有無による決定木の分類変化が確認可能であり、5.1 項であげた CVSS ベーススコアによる優先順位付けの問題点についても解消されることを確認した。

表5 決定木分析による優先順位付け検証結果(インターネット直接接続無)

		深刻度レベル(CVSS)				総計
		Critical	High	Medium	Low	
決定木による分析結果	Immediate	0(0.0%)	0(0.0%)	0(0.0%)	0(0.0%)	0(0.0%)
	Out-of-Cycle	15(0.2%)	15(0.2%)	2(0.0%)	0(0.0%)	32(0.4%)
	Scheduled	1004(14.1%)	2648(37.1%)	1394(19.5%)	2(0.0%)	5048(70.7%)
	Defer	0(0.0%)	13(0.2%)	1944(27.2%)	100(1.4%)	2057(28.8%)
	総計	1019(14.3%)	2676(37.5%)	3340(46.8%)	102(1.4%)	7137(100.0%)

6. まとめ

SBOMを活用した脆弱性管理手法として、SBOM を活用したソフトウェアの脆弱性検出手法と検出した脆弱性に対する決定木分析による層別手法について示した。独自に設定した評価指標にもとづく決定木分析は脆弱性の優先順位付けを可能とし、年間 5 万件以上登録される脆弱性の中から早期対応が必要な脆弱性を抽出することができる。CRA では 24 時間の脆弱性報告が求められる(CRA14 条)が SBOM と決定木を組み合わせた脆弱性管理は法規制対応にも貢献できる手法である。

現在、複数の製品にて実用化に向け SBOM を活用した脆弱性管理の試用に取り組んでいる。

参考文献

- (1) European Parliament, Cyber Resilience Act, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.pdf, (2024-3)
- (2) 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 Ver. 1.0, <https://www.meti.go.jp/press/2023/07/20230728004/20230728004-1-2.pdf>, (2023-7)
- (3) 独立行政法人 情報処理推進機構, 脆弱性対策情報データベース JVN iPedia, <https://www.ipa.go.jp/security/reports/vuln/jvn/ipedia2024q1.html>
- (4) NIST, NATIONAL VULNERABILITY DATABASE, <https://nvd.nist.gov/>
- (5) Spring, J. et al., PRIORITIZING VULNERABILITY RESPONSE: A STAKEHOLDER-SPECIFIC VULNERABILITY CATEGORIZATION (VERSION 2.0), https://insights.sei.cmu.edu/documents/606/2021_019_001_653461.pdf, (2021-4)