SBOMとセキュリティリスク評価技術による脆弱性ハンドリングの効率化

Improvement of Vulnerability Handling Efficiency through Application of SBOM and Risk Evaluation Technologies

金井　遵 KANAI Jun　　上原　龍也 UEHARA Tatsuya　　鬼頭　利之 KITO Toshiyuki

近年，各国でSBOM（Software Bill of Materials）の提出，及び早期の脆弱（ぜいじゃく）性対応の義務化が進んでいる。多様な製品や出荷先を持つ製品製造者には，PSIRT（Product Security Incident Response Team）での脆弱性ハンドリングの効率化が求められる。

そこで東芝は，SBOMと脆弱性情報のマッチング結果を基に把握した脆弱性が対象製品に影響を与えるか否かを，自然言語処理技術を用いて判断するスクリーニング技術と，製品に導入されたセキュリティ対策の情報に基づいて，影響の大きさを判定する環境評価技術を開発した。専門家へのヒアリングに基づく脆弱性ハンドリングコストの机上評価の結果，最大94％の工数削減効果を確認した。

In line with recent trends obligating businesses to submit a software bill of materials (SBOM) and quickly respond to software vulnerabilities in various countries, manufacturers providing multiple customers with various products have found it necessary to efficiently address vulnerabilities with a product security incident response team (PSIRT).

To improve the vulnerability handling processes, Toshiba Corporation has developed the following techniques: (1) a vulnerability screening technique to judge whether vulnerabilities impact the target product based on the matching results between SBOM and the information on vulnerabilities through the use of natural language processing techniques, and (2) an environment evaluation technique to estimate the magnitude of the impact based on security measures information introduced to the target product. Through evaluations of vulnerability handling costs based on interviews with experts, we have confirmed that these techniques can reduce the vulnerability handling workload up to 94%.

1. まえがき

世界で報告されるソフトウェアのセキュリティ上の欠陥（脆弱性）は，年間数万件に上る。PSIRTによる脆弱性ハンドリング活動では，開発した製品ごとに各脆弱性が製品に含まれるかどうかを判断し，リスクを評価して対応計画の決定を行う。製品には自社開発ソフトウェアだけでなく，OSS（オープンソースソフトウェア）や商用ソフトウェアなどの外部調達したものも搭載される。一つの製品に数千のソフトウェアが搭載されることも多く，これらを含めたリスク判断が求められる。したがって，製品数が多く，大規模なシステムを扱う製品製造者ほど脆弱性ハンドリングの負荷が大きく，自動化によって効率化することが喫緊の課題となっている。

また，長期的に安定稼働が求められる社会インフラシステム，いわゆるOT（制御・運用技術）システムでは，一般的なIT（情報技術）システムと異なり，頻繁にシステムを停止してパッチを一律に適用することが困難である。一方で，パッチを適用しないことで，サイバー攻撃によるシステムの可用性低下リスクが増大する。法令により継続的な脆弱性監視が要求される流れもあり，二律背反の課題となっている。これを背景に，OTシステムを扱うPSIRTでは脆弱性のリスクを精度良く把握し，限られたパッチ適用タイミングで，真に必要なパッチを適用することが求められる。しかし，既存技術ではリスクを精度良く把握するにはセキュリティ専門家によるリスク判断に頼らざるを得ないため，脆弱性ハンドリングに大きなコストが掛かっていた。

そこで東芝は，PSIRT支援システム[(1)]を導入し，整備の義務化が進むSBOMと，脆弱性情報の照合結果に基づいて，迅速かつ，確実に脆弱性に対応する基盤を運用している。更に今般，脆弱性が製品に与える影響を自動評価する技術を開発した。これにより従来セキュリティ専門家が行っていたリスク判断の多くの部分を自動化した。この技術のようなPSIRT支援のためのリスク評価技術を活用し，当社では脆弱性ハンドリングを効率化する試みを進めている。

ここでは，開発した脆弱性の自動評価技術の概要と，脆弱性ハンドリングを効率化する試みについて述べる。

2. SBOM及び脆弱性への対応の法的要請と課題

製品に含まれる脆弱性を把握し，適切に対応するためには，製品に含まれるソフトウェアを把握することが重要であ

る。近年注目されているSBOMは，製品を構成するソフトウェア部品や，その依存関係，ライセンス情報などをリスト化したものである。SBOMを用いることで，自社の製品に含まれるOSSなどのソフトウェアの情報を効率的に管理できる。またSBOMは，EO 14028（米国のサイバーセキュリティ改善に関する大統領令）[2]や欧州連合（EU）のサイバーレジリエンス法（CRA）[3]などで整備が義務付けられつつある。

一方で，脆弱性情報を収集し，公開するデータベースとして，米国のNVD（National Vulnerability Database）[4]や日本のJVN（Japan Vulnerability Notes）[5]などが存在する。NVDやJVNを参照することで，特定のソフトウェアに存在する脆弱性の情報が分かる。すなわち，**図1**のようにSBOMにより製品に含まれるソフトウェアを管理し，更に脆弱性情報データベースの情報と照合することで，製造者や製品を利用するユーザーは製品に存在する脆弱性を機械的に把握できる。

SBOMへの対応に加えて，脆弱性への対応もまた義務化される流れにある。例えば，CRAでは積極的な悪用が確認されている脆弱性が製品に含まれる場合には，製造業者は脆弱性の認識後，脆弱性情報を当局に報告する義務が2026年9月から課される予定である。ここでの報告は，認識後24時間以内に早期警告通知を連絡し，認識後72時間以内に脆弱性の性質などの情報を含めた通知を報告しなければならない。また，報告内容には，製品や脆弱性の情報，ユーザーが利用可能な是正措置や緩和措置などの情報を含めなければならない。この報告義務に適切に対応するためには，脆弱性の存在を認識するだけでなく，脆弱性が製品に及ぼす影響を判断する必要がある。影響を把握しなければ，脆弱性情報，是正措置，及び緩和措置を適切に報告できないためである。

脆弱性が製品に及ぼすセキュリティリスクの深刻度の定量化手法や，対応方法の決定手法としては，CVSS（Common Vulnerability Scoring System）[6]の環境評価基準やSSVC（Stakeholder-Specific Vulnerability Categorization）[7]などが広く利用される。しかし，これらの手法を利用するためには，深刻度を決定するための情報をセキュリティ専門家が脆弱性ごとに決定して計算を行わなければならない。CVSSの環境評価基準の例は，脆弱性の可用性・完全性・機密性といったセキュリティ要素への影響や環境を考慮した攻撃の難しさであり，SSVCの例は，その脆弱性が人命や業務に及ぼす影響である。これらの決定を，限定的な人数のセキュリティ専門家が，多くの製品の多くの脆弱性に対して，前述の報告義務に基づき24時間あるいは72時間といった短期間内に行うことは困難である[8]。

3. リスク評価技術

当社は，2章で述べた課題の解決のため，脆弱性の影響分析を効率化する2種類の技術を開発した[9]。一つは脆弱性が対象製品に“影響を与えるか否か”を判断するスクリーニング技術である。もう一つは製品に導入されたセキュリティ対策を考慮して製品に与える脆弱性の“影響の大きさ”を判定する環境評価技術である。**図2**のように，従来のSBOMと脆弱性情報の照合によるフィルターでの処理に加え，スクリーニング技術と環境評価技術により，対応が必要な深刻な脆弱性を絞り込むことで，脆弱性ハンドリングコストを削減できる。それぞれの技術について以下に概略を示す。

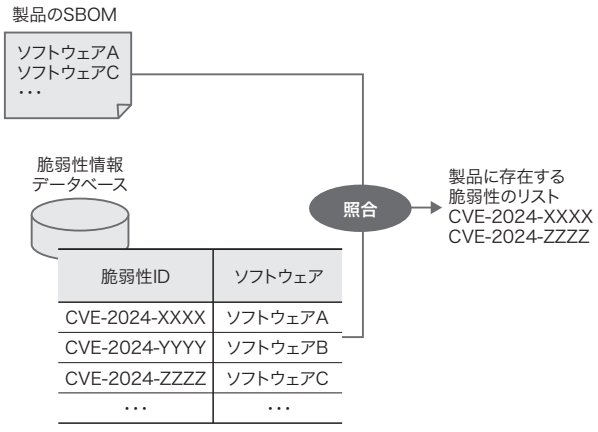


図1. SBOMと脆弱性情報データベースによる脆弱性の照合

製品に含まれるソフトウェアをSBOMにより管理することで，脆弱性情報データベースから機械的に脆弱性情報を抽出する。

Vulnerability matching of SBOM to vulnerability information database

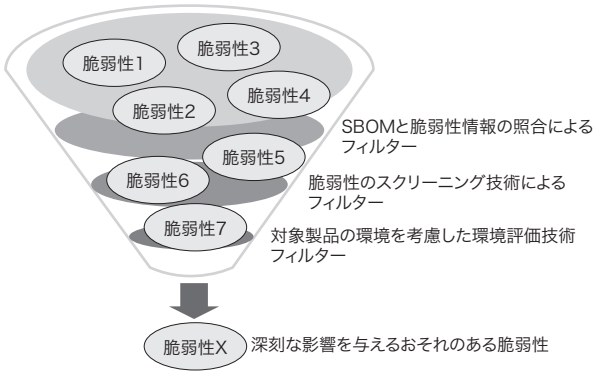


図2. リスク評価技術の概要

SBOMによる脆弱性の照合に加えて，スクリーニング技術と環境評価技術により深刻な影響を与える可能性のある脆弱性を絞り込む。

Overview of security risk evaluation techniques

3.1　スクリーニング技術

製品に，脆弱性があるソフトウェアが含まれていた場合にも，それが必ずしも製品に対して深刻な影響を及ぼすとは限らない。ソフトウェアの全ての機能を製品で利用しているとは限らず，例えば，利用されていない機能に脆弱性があっても，サイバー攻撃に悪用できない場合には製品には問題は発生しない。しかし，SBOMには個々のソフトウェアレベルで製品に搭載するソフトウェアが記載されるため，機能単位での脆弱性の影響の有無の判定はできない。

そこで，脆弱性情報から脆弱性が存在する機能を分析し，製品への影響の有無を判断する技術を開発した。脆弱性が存在する機能は，NVDやJVNの脆弱性情報では自然言語で記載されている。そこで**図3**のように，自然言語処理技術を用いて脆弱性が存在する機能を分析するとともに，その機能が対象機器で利用されているかどうかを判別し，脆弱性が与える影響の有無を自動的に判定する機能を開発した。

従来の脆弱性ハンドリングでは，機能利用の有無に基づく影響の判定をセキュリティ専門家と製品の専門家が連携して行っていたが，この方式により影響を与えるか否かの自動判定を実現した。

3.2　環境評価技術

同じ脆弱性であっても，その脆弱性が与える影響は環境によって変わる。特に，有効なセキュリティ対策が導入されている環境と導入されていない環境では影響に大きな差が出る。例えば，ネットワークから特定の通信データを送った際に，ソフトウェアの誤作動を起こす脆弱性があった場合でも，ファイアウォールがその通信を遮断できれば，攻撃の影響を最小化できる。

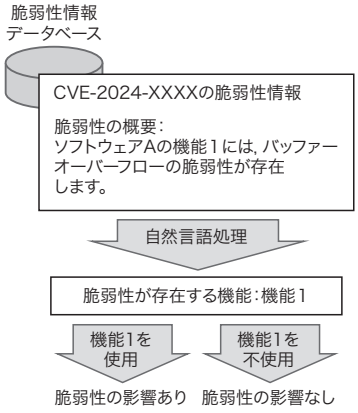


図3．スクリーニング技術の概要

自然言語処理により自然言語で記載されている脆弱性情報から，脆弱性が影響を及ぼす条件を抽出する。

Outline of vulnerability screening technique

今回開発した環境評価技術では，あらかじめ，アンチマルウェアソフトウェア，ファイアウォールといったセキュリティ対策ごとに，攻撃を防止できる脆弱性情報をデータベース化しておく。更に，対象環境に導入されたセキュリティ対策の情報と脆弱性情報に基づいて，影響の深刻度をCVSS環境評価基準の計算式を使って計算する。計算した深刻度は標準的に利用されているCVSSのスコアとして算出されるため，セキュリティリスクの深刻度を客観的に評価できる。

環境ごとのセキュリティリスクの深刻度評価も従来はセキュリティ専門家の関与が必須であった。この技術により一部を自動化できるため，セキュリティ専門家はスクリーニング技術と合わせて真に危険な脆弱性の評価にリソースを割くことができる。

4.　リスク評価技術の導入効果

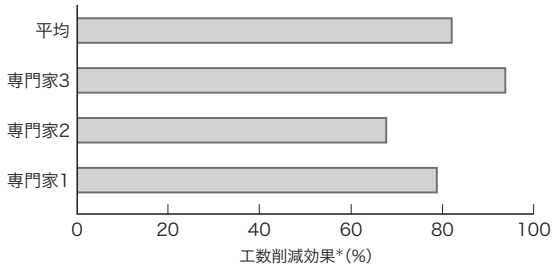
脆弱性ハンドリングコストの改善効果を机上評価するため，PSIRT活動に従事する3名の担当製品分野の異なるセキュリティ専門家に，手動での脆弱性ハンドリングに掛かる時間のヒアリングを行った。ヒアリング結果を分析するため，脆弱性ハンドリングのプロセスを，(A)SBOMによる脆弱性抽出（自動），(B)スクリーニング，(C)環境評価，(D)対応策検討という4ステップに分けて考える。ここで，一連のプロセスでは，まず(A)でSBOMと脆弱性情報データベースを照合して脆弱性一覧を自動抽出する。(A)は元々自動化されていた部分である。次に，(B)で脆弱性一覧に対してスクリーニングを行った後，(C)で環境に応じたリスク評価を行う。最後に(D)で対応策を検討し決定する。これらの4ステップに分けた場合，従来の脆弱性1件の判断に要する工数は**表1**に示すとおりである。

更に，模擬環境の3,532件の脆弱性に対して，この技術の導入前後で脆弱性を評価する(A)から(C)のプロセスの総工数の削減効果を評価した。その結果を**図4**に示す。元々自動化されていた(A)に対して，(B)と(C)が自動化された結果として，平均82％，最大94％の工数削減効果を確認した。これは，従来，脆弱性評価のプロセスである表1の(B)と(C)

表1．脆弱性1件当たりの従来のハンドリング工数

Conventional workloads required for one vulnerability handling process

脆弱性ハンドリングのプロセス	脆弱性1件当たりの専門家の判断時間（min）			
	専門家1	専門家2	専門家3	平均
(A) SBOMによる脆弱性抽出（自動）	0	0	0	0
(B) スクリーニング	10	40	60	37
(C) 環境評価	20	20	60	33
(D) 対応策検討	30	120	30	60



＊従来の全工数に対する開発技術導入後の削減工数の割合

図4. 脆弱性評価プロセスの総工数の削減効果

スクリーニング技術と環境評価技術により，平均82％，最大94％の工数削減効果を確認した。

Reduction of vulnerability handling workloads

の合計時間が，表1のように平均70分であったとする場合，3,532件の評価に平均で4,120.7時間（171.7日）掛かっていたところ，平均82％削減され741.7時間（30.9日）で評価が終わることを意味する。

5. あとがき

SBOMと脆弱性情報のマッチング結果を基に，脆弱性の影響の有無を判定するスクリーニング技術と，製品に導入されたセキュリティ対策の情報に基づき脆弱性の影響の大きさを判定する環境評価技術を開発した。また，机上評価にて，これらの技術の適用により，脆弱性ハンドリング工数が最大94％削減できることを確認した。工数削減により，セキュリティ専門家は真に深刻な脆弱性への対応に注力し，セキュアな製品の提供に寄与することができる。

今後も，法令対応を含む社会的に安全な製品の提供の要請に応えるべく研究開発活動を進めていく。

文　献

(1) 東芝．サイバーセキュリティ報告書 2025．2025，26p．<https://www.global.toshiba/content/dam/toshiba/jp/cybersecurity/corporate/report/pdf/CyberSecurityReport2025_A3_rev02.pdf>，（参照 2025-07-09）．

(2) NIST(NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). "Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order". Executive Order 14028, Improving the Nation's Cybersecurity. <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity>, (accessed 2025-04-21).

(3) EU (European Union). "REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)". EUR-Lex. <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>, (accessed 2025-04-21).

(4) NIST. NATIONAL VULNERABILITY DATABASE. <https://nvd.nist.gov/>, (accessed 2025-04-21).

(5) JPCERT/CC (Japan Computer Emergency Response Team Coordination Center) and IPA(Information-technology Promotion Agency, Japan). Japan Vulnerability Notes (JVN). <https://jvn.jp/>, (accessed 2025-04-21).

(6) Forum of Incident Response and Security Teams, Inc. Common Vulnerability Scoring System SIG. <https://www.first.org/cvss/>, (accessed 2025-04-21).

(7) America's Cyber Defense Agency. Stakeholder-Specific Vulnerability Categorization (SSVC). <https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc>, (accessed 2025-04-21).

(8) Luca Allodi et al. "Estimating the Assessment Difficulty of CVSS Environmental Metrics: An Experiment". Future Data and Security Engineering : 4th International Conference (FDSE 2017) Proceedings. Vietnam, 2017-11, International Conference on Future Data and Security Engineering. Springer International Publishing AG, 2017, p.23–39.

(9) 金井 遵，ほか．“PSIRT向け脆弱性スクリーニング技術と環境毎リスク評価技術”．コンピュータセキュリティシンポジウム2024論文集，兵庫，2024-10，情報処理学会コンピュータセキュリティ研究会．2024，p.1218–1225.

金井　遵　KANAI Jun, D.Eng
総合研究所 AIデジタルR&Dセンター
セキュリティ基盤研究部
博士（工学）　情報処理学会・電子情報通信学会会員
Security Research Dept.

上原　龍也　UEHARA Tatsuya
総合研究所 AIデジタルR&Dセンター
セキュリティ基盤研究部
Security Research Dept.

鬼頭　利之　KITO Toshiyuki
技術企画部 サイバーセキュリティセンター
製品セキュリティ推進室
Product Security Promotion Office