「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 2.0 （案）」に対するBSA｜The Software Allianceからの意見

2024年5月27日

総論

BSA｜The Software Alliance（BSA ｜ ザ・ソフトウェア・アライアンス、以下BSA）[1]は、「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 2.0 （案）」（以下、手引案）に関し、経済産業省（以下、貴省）に意見を提出する機会[2]を得られたことに感謝します。

BSAは、政府やグローバル市場において、世界のソフトウェア産業を代表する主唱者です。BSAの会員企業は、世界で最もイノベーティヴな企業であり、企業や政府の競争力と効率性を高めるソリューションを提供することで、デジタルトランスフォーメーション（DX）の推進に貢献しています。BSAの会員企業は、IDおよびアクセス管理、データアナリティクス、クラウド・ストレージおよびデータ処理サービス、CRM（顧客管理）ソフトウェア、人事管理プログラム、コラボレーション・システムなど、様々なツールを提供しています。

ソフトウェアのセキュリティに関しては、BSAも貴省と同様の懸念があります。サイバーセキュリティに関する提言をまとめたBSAの「2024 Global Cyber Agenda（2024年度グローバル・サイバー・アジェンダ、以下、アジェンダ）」[3]においては、「ソフトウェア・セ

[1] BSAの活動にはAdobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Cohere, Dassault, Databricks, DocuSign, Dropbox, Elastic, ESTECO SpA, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc. が加盟企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

[2] https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595224009&Mode=0

[3] https://www.bsa.org/files/policy-filings/2024cyberagendabsa.pdf

22F Shibuya Mark City
1-12-1 Dogenzaka, Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

キュリティの強化」を最優先事項としています。 ソフトウェア・セキュリティの向上には、多面的なアプローチが必要です。BSA のアジェンダでは SBOM に関する考えも示しており、SBOM の標準化に向けて産業界と政府が継続して協力していくことを推奨しています。SBOM は万能薬ではありませんが、顧客が SBOM を利用する準備が整えば、インシデント対応を迅速化することが可能となります。この点に関し、貴省が企業の自主的取り組みを支援し、SBOM 導入の課題とメリットを評価するための実証をいくつかの産業分野で実施したことを我々は高く評価しています。

SBOM（Software Bill of Materials）は有望だが限定的なツールであると認識すること

最新のソフトウェア、特にサービスとして提供されるクラウドベースのソフトウェアには、状況に応じて変化する、動的（ダイナミック）なコンポーネントの一覧が利用される可能性が高く、これらのコンポーネントの数は数千になることもあります。このようなコンポーネントの動的な特性と数は、SBOM の作成と活用の両方を複雑にします。このため、SBOM によってサイバーセキュリティを確実に向上させるには、慎重な検討が必要です。手引案が示すように、SBOM は効率的なソフトウェア管理のために利用することは可能ですが、SBOM を実装する上では、対処しなければならない様々な課題があります。SBOM は、現在開発されているツール、標準、自動化と組み合わせることで、サイバーセキュリティを向上させますが、包括的な解決策ではありません。SBOM は、広く信頼されるために必要な成熟度にはまだ達しておらず、現段階では一般的に利用されている規格も存在しません。例えば、コンポーネント名を決定する、グローバルな単一の規程された手法はありません。そのため、二つの異なる SBOM 作成者が同じコンポーネントに対して二つの異なる識別子を使用する可能性があります。これは、ソフトウェアコンポーネントのサプライヤーが、それぞれのニーズに応じてコンポーネント名を定義するからです。さらに、特定の SBOM フォーマットのバージョンは、製品に含まれるコンポーネントの記載に加え、脆弱性の記録に使用することができますが、それはフォーマットの意図された用途ではありません。製品のリリース後に脆弱性が発見されたり、脆弱性の特性が変化することもあります。したがって、脆弱性が発見・変更される度に SBOM 全体を再公開することは、非効率です。

多様な主体が参加するサイバーセキュリティのコミュニティは、検証可能な精度を備えた SBOM の作成に取り組んでいます。手引案の「2.5. SBOM に関する誤解と事実」で触れているように、SBOM にソフトウェアコンポーネントに関する既知の脆弱性が記されたとしても、 それが必ずしも、SBOM で示されているソフトウェアが脆弱であるということにはなりません。例えば、手引案の脚注 17 に記されているように、一部の実務者は、ソフトウェアの脆弱性を機械判読可能なかたちで自動分析できる方法の 一つとして、SBOM および製品のメタデータを VEX（Vulnerability Exploitability eXchange）と組み合わせることをしています。これにより、脆弱なコンポーネントが脆弱な製品につながるかどうかを判別することが可能となります。このような取り組みは、SBOM を実用的かつ有益にしていく上で、非常に重要となります。

クラウド環境特有の課題

手引案の「2.5. SBOM に関する誤解と事実」では、「コンテナイメージに対する SBOM、SaaS ソフトウェアに対する SBOM、クラウドサービスに対する SBOM 等のオンラインアプリケーションに対する SBOM の議論も米国を中心に行われている」と記されています。この点に関し、クラウド環境特有の課題があることを挙げておきます。例えば、SaaS（Software-as-a-Service）におけるアップデートやパッチは、通常、継続的に（自動化されて）行われ、脆弱性の迅速な解決につながっています。このため、SBOM をクラウドの文脈で採用しても、すぐに SBOM が最新状態を反映していないこととなり、効果を発揮できません。このため、SBOM を自主的に導入する上では、オンプレミス・ソフトウェアの方が実装上の課題が少ないかもしれません。

SBOM に含む詳細のレベルを制限することにより、SBOM の普及と利用を促進する

BSA は、SBOM の開発と利用を支持しますが、少なくとも当面は、SBOM に含む情報の範囲を限定し、SBOM の土台を構築することに集中することを推奨します。SBOM に含む情報の詳細と範囲を限定することで、企業は SBOM のメリットをより早く享受することが可能となります。このアプローチは、産業界がより詳細で包括的な SBOM を実施するために必要な人材、プロセス、技術を開発するにつれて、追加条件を構築する可能性を排除するものではありません。

デジタルな要素を特定の状況で使用する製品のみに SBOM を推奨すること

SBOM の利用を推奨するのは、特定の文脈で使用されるデジタルな要素（エレメント）を持つ製品に限定するべきです。初期段階において、SBOM が特定の状況で利用されることがあるかもしれません。「2.5. SBOM に関する誤解と事実」では、「SBOM を公開する必要はなく、SBOM 作成者やサプライヤーの判断で SBOM の共有方法を判断することができる」と記されています。また「SBOM はソフトウェアに含まれているコンポーネントの一覧リストであり、特許やアルゴリズムは含まれておらず、知的財産を公開するものではない」とも記しています。ここで言及されているように、SBOM の公開は、製品のセキュリティだけでなく、知的財産に対するリスクももたらす可能性があることを強調しておくことが重要です。本記載にあるように、SBOM だけではソースコードのような機密性の高い企業秘密は提供されませんが、他の専有情報が含まれる可能性があります。例えば、特定の製品を製造するために使用されるソフトウェアプロバイダ、ベンダー、およびパートナー等の特定の組み合わせです。これらは貴重な知的財産および専有情報を構成するものです。企業は、SBOM を顧客に提供することはできますが、その情報を公開したり、秘密保持契約などの適切な保護措置なしにその情報を開示したりすることを要求されるべきではありません。また、脆弱性の開示に SBOM を使用したり、技術文書に SBOM を完全に含めることは、悪意ある行為者による脆弱性の悪用を招くことになりかねません。

最後に、SBOM を理論から具体的なセキュリティ改善につなげるためには、欠落している要素を特定し、埋めることが必要となります。現在、このために産業界と政府による重

要な取り組みが進んでいることを強調しておきます。この取り組みが完了する前に SBOM を実施することに対し、政府は引き続き慎重であるべきです。

結論

BSA と会員企業は、ソフトウェアの脆弱性を制御し、ソフトウェアのセキュリティを強化するという目標を支援するために、貴省に協力していけることを期待しています。SBOM はこの取り組みの重要な一部です。また、BSA 会員企業を含む、グローバルなソフトウェアベンダーが議論に貢献し、詳細な提言をすることを可能とするために、今後は意見募集の段階で手引案の英訳を準備することを奨めます。本取り組みに我々がどのように協力できるかを話し合う機会を頂ければ幸いです。