日本独自のセキュリティ対策の推進へ

情報通信研究機構　主管研究員
JNSA 副会長　中尾　康二

近年の情報ネットワークの広域化、高速化、利便性の向上、及び情報システムの高度化、大容量化、高機能化などを背景に、通信の信頼性はもとより、情報システム及び企業における情報セキュリティ技術およびサイバーセキュリティ技術の重要性が増しています。

このような環境において、最近よく耳にするセキュリティ関連のキーワードとして、「ゼロトラスト」や「SBOM」などがありますが、ここでは、SBOMについて少し掘り下げてみたいと思います。

SBOMは、Software Bill of Materials（ソフトウェア部品表）の略称で、各製品のソフトウェア部品（コンポーネント等）をその製品の購入者/利用者に対して直接または公開情報として提供することを要求するものです。SBOMを利用することで、システム構築者はソフトウェアコンポーネントが最新であることを確認でき、新しい脆弱性にも迅速に対応することが可能となります。また、ソフトウェアの購入者にとっては、ソフトウェアの脆弱性分析、製品のリスク分析などに役立てることができ、SBOMはサプライチェーンの環境においてソフトウェア資産のセキュアな管理方法として早いタイミングで米国において注目されていました。2021年5月には「ソフトウェアのサプライチェーンセキュリティの強化」として、米国の大統領令（EO14028）に政府調達におけるSBOM活用が明記されたことをきっかけに、米国統制当局を中心とした取引組織へのSBOM整備の義務化などが急速に進みつつあります。米国における流れを受け、日本の総務省（通信分野におけるSBOM導入調査）、経済産業省（自動車業界、医療機器業界、ソフトウェア業界におけるSBOM活用モデルの検討等）などにおいてもSBOMがソフトウェア管理の施策として取り上げられるようになりました。

では、米国でどのようにSBOMが注目されるようになったのでしょうか。いろいろな解釈があるかもしれませんが、オープンソースソフトウェア（OSS）の活用の検討がその発端になっていると理解します。すなわち、OSSの活用にあたっては、各OSSソフトウェアの著作者が定めたライセンスを遵守し、OSSの適切な管理を実施することが必要となります。そのため、The Linux Foundation の公式プロジェクトの一つである「OpenChainプロジェクト」では、各組織が組織内に確立すべきOSSコンプライアンスプログラムの要件を「OpenChain仕様」として規定し、その普及を推進しており、OpenChain仕様をISO/IEC 5230として2020年に国際規格化を完了させました。

ISO/IEC 5230はOpenChain仕様がほぼそのまま国際規格となったもので、その要求事項の一つとして「BoM（Bill of Materials）」を規定しており、OSSコンポーネントの部品表の作成・管理のためのプロセスが存在することを要求しています。部品表としては、供給ソフトウェアを構成するOSSコンポーネント、識別されるライセンス、ユースケース、改変の有無などが部品要素として定義されています。

以上のことから、米国政府におけるSBOMの議論は、OSSコンポーネントの部品表の作成・管理プロセスと深い関係があり、サプライチェーンセキュリティのためのソフトウェア管理としてSBOMの整備に目を向け、政府調達におけるSBOM活用やSBOM整備の義務化を推進していく流れとなったと読み解けます。米国の活動の素晴らしいところは：

1. 早いタイミングでOSS業界団体により、OpenChain仕様化が手掛けられたこと
2. 当該仕様を国際標準化させ、世界的規模での仕様活用に目を向けたこと
3. 米国政府内部のサプライチェーンセキュリティの検討WGで、OpenChain仕様に目を付け、サプライチェーンセキュリティのソフトウェア管理の手法として提言し、それを大統領令としてトップダウンの指示をしたこと
4. 上記の活動を受け、政府調達ソフトウェアに対するSBOMの活用を促進したこと

などが挙げられると思います。

日本として、米国による素晴らしい活動を見習い、それらを積極的に取り入れることには大賛成ですが、今後は日本独自のセキュリティ要件を加味した日本主導型のセキュリティ対策の推進が大きく期待されるところです。特に、セキュリティベンダーが集結する我々JNSAにとっては以下のような活動が期待されるのではないでしょうか。

- 日本のビジネス環境で取得する生のセキュリティ要件を中立的、かつ網羅的に収集・整理できること
- 抽出した要件を満足するような対策仕様（OpenChain仕様のような）の検討を専門メンバで策定できること
- 作成する対策を政府に提言できること
- 検討した対策を各セキュリティベンダーにおいて実証評価を行い、対策仕様の改善、精度向上を推進できること

これまでのJNSAの活動においても、上記のような活動は個別の活動として実施されてきたと認識していますが、JNSAが主導して日本におけるセキュリティ対策の大きな流れを作っていける時期に来ていると痛感しております。そのためには、JNSAにおける若手メンバによる具体性をもった忌憚のないアイディアが必要です。2023年のJNSAにおいては、若手のアイディアや斬新な構想を真摯に捉え、それらのアイディアに基づいたJNSAにおける活動の構想を練り、日本独自のセキュリティ対策の推進に貢献するための第1歩を踏み出せるよう切に期待します。