URL https://journal.ntt.co.jp/article/23466
DOI https://doi.org/10.60249/23101201

NTTデータグループ　技術革新統括本部
システム技術本部　サイバーセキュリティ技術部

清宮聡史　Satoshi Seimiya

ソフトウェアサプライチェーンにおけるセキュリティの要：SBOM

最近，サイバー攻撃やセキュリティに関する話題が，メディア等に頻繁に登場しています．世の中を便利にする各種システムはもちろんのこと，それを使うためのスマートフォン等の端末に至るまで，ソフトウェアへの依存が高まっている中，サイバー攻撃等の多くはこうしたソフトウェアに内在する脆弱性を突いて行われています．脆弱性をソフトウェア開発の段階から管理して混入を防ぐために，SBOM（Software Bill of Materials）というソフトウェアの部品表を活用する動きがグローバルに展開し始めています．NTTデータグループ 技術革新統括本部 システム技術本部 サイバーセキュリティ技術部 清宮聡史氏に，SBOMを活用したソフトウェア脆弱性管理，SBOMをベースとしたセキュリティの専門家をめざす思いを伺いました．

SBOMによるソフトウェア脆弱性管理がグローバルなトレンド

現在，手掛けている開発の概要をお聞かせいただけますか．

私は，2018年にNTTデータに入社以降，商用システム開発におけるセキュリティ確保施策の推進に取り組んでいます．特に，2022年度からはソフトウェアサプライチェーンセキュリティ関連の開発に包括的に取り組むようになりました．現在，SBOM（Software Bill of Materials）統合管理に関する開発をメインに担当しています．SBOMは，オープンソースソフトウェア（OSS）や商用ソフトウェアを含むソフトウェアライブラリやモジュール等のコンポーネント（群）およびそれらの関連性と補足情報の一覧であるソフトウェア部品表のことです．

NTT DATAは，SIerとして公共，金融，法人，各分野のお客さまへ，サービスやシステムを提供していますが，OSSをベースとしたシステム開発が増加する中で，使っていたOSSの中に，気付かないうちに脆弱性が含まれていたケースも出ています．こうした脆弱性を突いて，悪意のある第三者が攻撃を仕掛けてくるという事例も世の中で増えています．2023年度の独立行政法人情報処理推進機構（IPA）による『情報セキュリティ10大脅威』では，「サプライチェーンの弱点を悪用した攻撃」が2位にランクされています．

NTT DATAでは，2022年度より施策要件を満たすすべてのWebアプリケーション開発プロジェクトにおいて，結合テストの段階で，IAST（Interactive Application Security Testing）という，アプリケーションが動作した個所の処理に脆弱性が含まれていないかを検査するツールの活用を全社的にルール化しており，これにバンドルされているSCA（Software Composition Analysis）ツールにより一部のソフトウェア部品は可視化できていました．しかし，それだけでは，IASTツールがサポートしていないテクノロジを用いてWebアプリケーションを開発される場合や外部から調達した機器・サービス（ネットワーク機器，Software as a Service等）をカスタマイズしてお客さまに納品する場合等において，ソフトウェア部品を可視化できません．そこでSBOMを活用して，IAST対象のソフトウェアだけではなく，サードパーティのソフトウェア部品も管理していくことになりました．

さて，SBOMは，「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」等の要素で構成されソフトウェアの脆弱性管理，ライセンス管理の一助になることが世界で期待されています．2021年5月の米国大統領令を受け，米国立標準技術研究所（NIST）等でガイドライン・ガイダンス整備等が進行中であり，欧州でも「EUサイバーレジリエンス法」草案が出され，SBOMの取得を推奨する動きが世界的に広がってきています．日本においても，経済安全保障推進法に基づき，2024年春ごろから段階的に基幹インフラの事前審査が始まる予定であるとともに，内閣サイバーセキュリティセンター（NISC）公開の『サイバーセキュリティ2023』でも，「SBOM」の実証・早期実用展開につ

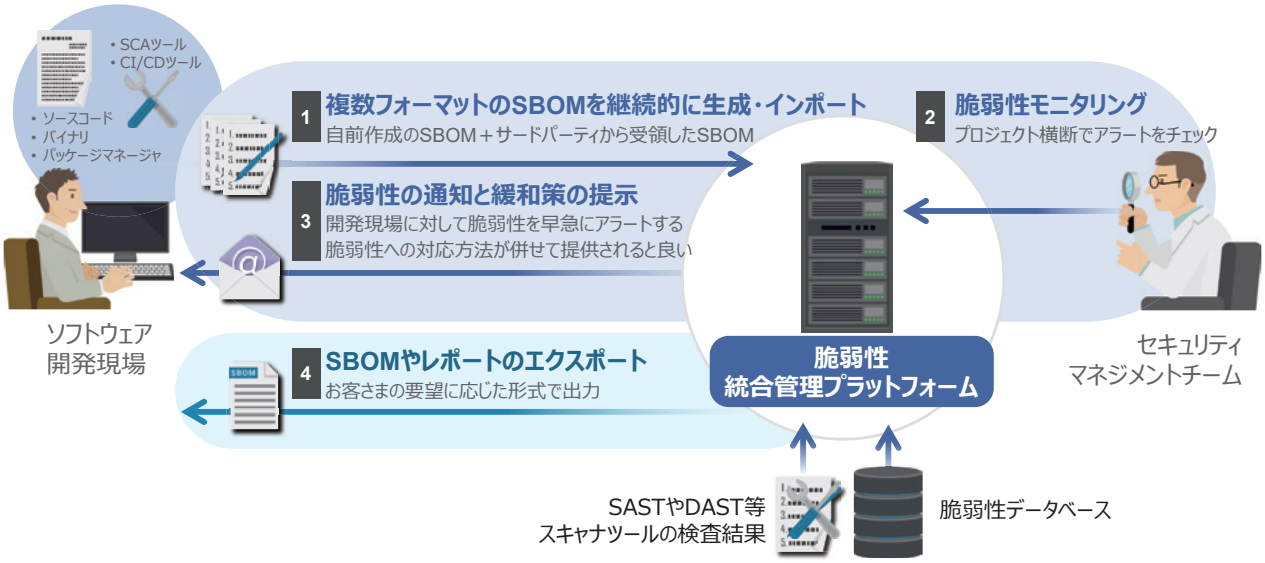

図1　脆弱性統合管理プラットフォーム

いて明記されています．こうした動きの中，私たちは，セキュリティガバナンスの観点から，開発プロジェクトにおける「脆弱性対応の効率化」「お客さまへのSBOM納品」を，セキュリティサービスの観点から，「お客さまへのサプライチェーンセキュリティリスク管理サービスの提供」の実現をめざして，SBOMの利活用を推進しています．

SBOMはグローバルな取り組みが進みつつあるのですね．

SBOMは，グローバルな展開が進みつつありますが，グローバルで統一的なレジストリ管理団体はなく（2023年8月現在），IETF（Internet Engineering Task Force）において，その構想を検討しています．したがって，各企業等で独自にSBOMを作成・活用しているのが現状です．その結果，①SCAツールごとにサポート対象のテクノロジ・参照先の脆弱性データベースが異なる，②大部分のSBOMで米国商務省電気通信情報局（NTIA：National Telecommunications and Information Administration）の定める最小構成要素を満たしていない（Chainguard社の品質調査），③SBOMは開発工程の中で一度作成するだけでは不十分でソフトウェアコンポーネント等の変更の都度作成しなければならない，等の課題があります．

こうした課題への対応策として，NTTデータグループ会社ではSBOMの生成からインポート，データの管理，脆弱性情報と紐付けてソフトウェアのセキュリティリスク管理を包括的に実現するための「脆弱性統合管理プラットフォーム」の開発を進めています．また，SBOMを活用し，NTT DATA海外グループ会社と連携し，お客さまのサプライチェーンセキュリティを包括的に保護するマネージドサービス「サプライチェーンセキュリティマネージドサービス」の開発も進めています．

「脆弱性統合管理プラットフォーム」はNTT関連各社との共同プロジェクトにて開発を進めており，次の4つの機能で構成されています（**図1**）．

まず，自前作成，サードパーティから受領したSBOMにかかわらず複数フォーマットのSBOMを継続的に生成・インポートする機能．2番目は，プロジェクト横断でアラートをチェックする脆弱性モニタリング機能，3番目は，開発現場に対して脆弱性を早急にアラートするとともに脆弱性への対応方法が併せて提示される，脆弱性の通知と緩和策の提示機能，そして，お客さまの要望に応じた形式で出力するSBOMやレポートのエクスポート機能です．「脆弱性統合管理プラットフォーム」により，全社的に必要とされる部品の情報をルールとして定めておくことで品質が悪いソフトウェアを排除するとともに，脆弱性情報とソフトウェア部品表を結びつける情報が一部抜けているような不完全なSBOMに対して，不足情報を付加するかたちで使えるSBOMにするといったことも可能になります．これにより，新規脆弱性発生時の対応稼働を1プロジェクト当り約1.5時間，年間では約53時間削減でき（NTT DATAの社内モデルによる試算値），人為的な確認・報告ミスの削減，脆弱性を放置している時間の削減が見込まれます．また，個々のSCAツールから出力される各SBOMについて，構成要素，記載内容等の整合性について社内標準との照合が可能になるとともに，提供するファイルフォーマットを含むお客さまの要望に応じて，脆弱性統合管理プラットフォームから臨機応変に，納品するシステム全体に関するSBOMを提供可能，といった社内のセキュリティガバナンスへの効果が期待できます．

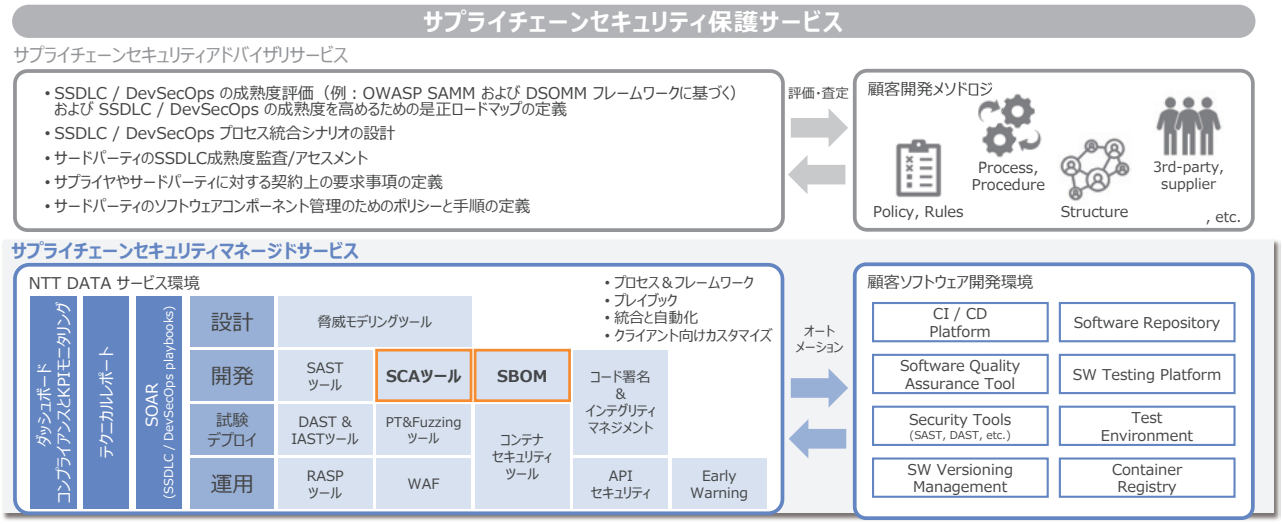

図2　サプライチェーンセキュリティマネージドサービス

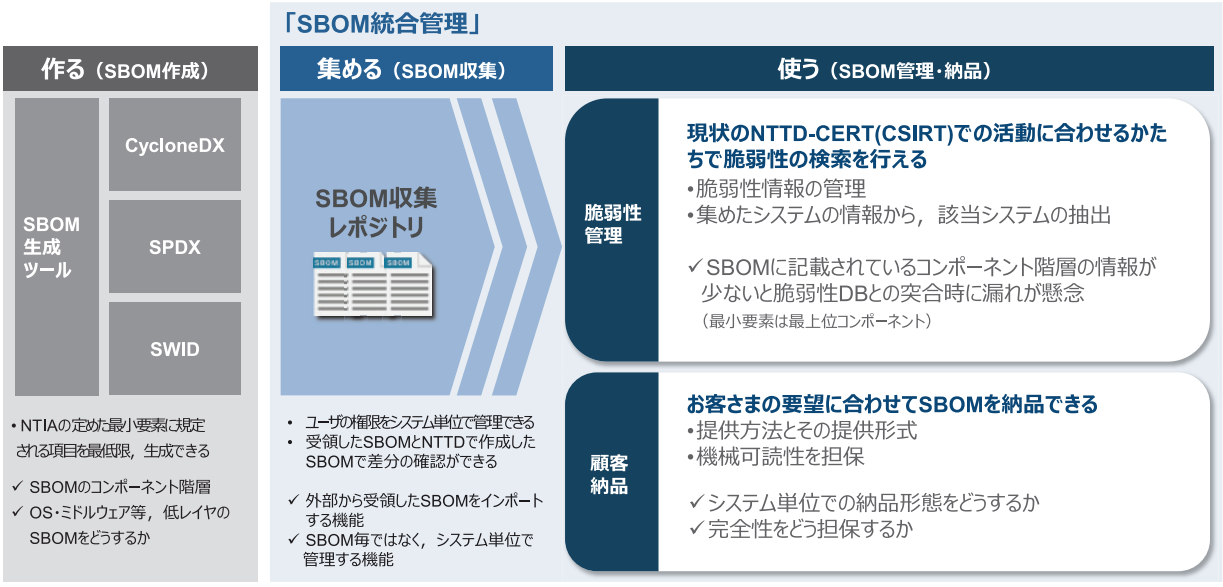

図3　社内でのSBOM統合管理の実現に向けて

「サプライチェーンセキュリティマネージドサービス」は，世の中でSBOMが一般化してその対応が求められてくると，その作成や活用に困るお客さまがたくさん出てくることが容易に想像されます．そういったところにNTT DATAのエンジニアが入ってサプライチェーンセキュリティに関して企画から実装，最終的なレポーティングまでワンストップで行えるようなサービスです（**図2**）．その中のサービスメニューの1つとして，お客さまのアプリケーションのSBOM生成・管理・脆弱性に対応するサービスを，海外から順次提供開始する予定です．

こうしたプラットフォームやサービスをベースとして，社内におけるSBOM統合管理の実現に向けて，SBOMのライフサイクルの3観点（「作る」「集める」「使う」）で，SBOM統合管理のToBe像とAsIsのギャップを抽出し，ツール類，収集体制，SBOM統合管理ガイドライン等の整備といった各課題の達成に向け，PoC（Proof of Concept）を実施しています（**図3**）．また，NTT DATA（海外グループ会社）のお客さまの開発チームとPoCを実施し，商用のソフトウェアを対象にSBOM活用のノウハウを蓄積し，サービス開発にフィードバックするといった取り

組みを継続しています．さらに，2022年11月よりNTTグループとNECで「セキュリティトランスペアレンシー確保技術」に関するフィールド実証を開始しました．2023年度には，SCAツールで出力されたSBOMの利活用，バックドア検索等の技術を使い，ステークホルダーやソフトウェアサプライチェーンの中のリスク低減を検討する，コンソーシアムの設立も予定しており，NTTデータグループ社も社内のPoCで得た知見をベースにこれに参画します．

セキュリティの専門家としてSBOMの普及に貢献できる日をめざして

開発者としてスキルの維持，スキルアップはどうしていますか．

学生時代は，無線情報通信関連の研究をしており，ソフトウェアやセキュリティとは直接関係のないテーマの研究を行っていました．NTTデータ入社後の研修の中でソフトウェアやセキュリティに関する基本的なスキルを習得し，現在の部署においては，セキュリティの診断を実際に実施する等のOJTを含む研修で，技術的なスキルをかなり習得することができました．

こうした中で業務を進めていくうえでは，技術以外に大きく4つのスキルが必要と考えます．まず，情報収集力です．SBOMは世界的に取り組みがなされており，コミュニティにおいてもSBOMの議論が多くなっています．日本のニュースに限らず，海外の人も含めて，SBOMソサイエティの人はどのようなことを考えているかという点も含めて情報収集することが1つポイントと思います．2番目は，分析力です．SBOMに関してさまざまな情報が世界中にあふれていますが，それぞれ正しい情報も不確かな情報もありますので，複数の情報源を比較したり組み合わせたりすることで分析していく力が必要だと思います．3番目が実装力です．仮説を立て，それがうまく進みそうだと思ったら自分で手を動かして試してみるという力です．権威のある論文であってもそれを鵜呑みにせず，どのようなアルゴリズムでつくられているのかといった本質を見極める力が必要だと思います．そして4番目は発信力です．自分なりに考えた結果を発信していかないことには，ディスカッションも，普及も進みません．

現在，SBOMに関して多くのOSSやツールが出てきていますが，単にそれを使っているだけでは，研究開発ではなく運用の話になるので，技術的に新規性を見出していくうえでは，それをブラックボックスにしないことを心掛けています．OSSやツールは省力化につながるから使うという場面ももちろんありますが，独自の視点で新規性を出していく場面では，OSSやツールの中のソースコードを読み解き，どのようなロジックで実装されているかというところまで深く入り込んでみることを意識し，それを通してさまざまなスキル向上を図っています．

事業会社は異動がありますが，こうしたスキルを活かして将来的に何を経験したいのでしょうか．

以前，Apache Log4jというオープンソースログ出力ライブラリの脆弱性対応のときに，うまく情報が集まらず苦労していたのですが，IASTを導入しているところでは情報が取れているのではないかと考え，実際に確認したら情報が取れていました．日常業務として対応してきたところが，世界的なソフトウェアコンポーネントの話をきっかけに，日常業務が別のところに応用できるかもしれないという感覚が印象的でした．

また，2022年12月にNTTデータのセキュリティへの取り組みを紹介する講演を行いましたが，その講演を見ていただいた方から直々に別の講演におけるゲスト登壇のお話をいただきました．自分が一生懸命発信したストーリーが誰かの心を動かして，次の発信につながっていくというのがとても印象に残りました．

こうした経験を通して，私としてはやはりセキュリティはとても面白いし，セキュリティに何かを掛け合わせることが，独自のセキュリティの概念や技術を考えるうえで役に立つと思っています．現在，IASTとSBOMを組み合わせたセキュリティ施策の推進を行っていますが，この先，これ以外のさまざまな組み合わせを考えていきたいと思います．そのうえで，最近，お客さま向けの勉強会の実施やお客さまの課題認識等を伺う機会が増えてきているので，社内だけではなく社外で交流しながら，ソフトウェアサプライチェーンのリスク等の話を通してセキュリティの啓発活動を行い，セキュリティの専門家としてキャリアを磨いていきたいと思います．

まずはできる範囲から試してみよう

読者，お客さまへのメッセージをお願いします．

現在，SBOMは世界的に各方面でさまざまな方々の間でディスカッションされています．しかし，ソフトウェアサプライチェーンにおけるSBOMは概念的でイメージしづらいうえに，世界統一的なSBOMはまだ存在していないので，活用に当たってはハードルが高いかもしれません．そこで，部品表のサンプルを見てイメージをつかんでいただき，ご自身がかかわっているシステム開発工程の中にその部品表を当てはめて考えてみる等，小さなところから興味を持って試してみることが大切だと感じます．そして，SBOMはさまざまな関連ツールやパッケージも出ているので，できる範囲から試しに使ってみていただけると良いと思っています．