セキュリティトランスペアレンシー確保技術によるソフトウェア構成の分析・可視化

近年，機器・システム等の調達および保守・運用に関し，サプライチェーンを介して，製品・サービス・事業環境がセキュリティ侵害を受ける「サプライチェーンセキュリティリスク」が顕在化しています．本稿では，このような状況の中，NTT社会情報研究所が取り組んでいるセキュリティの透明性を確保する技術について紹介します．

上原 貴之（うえはら たかゆき）　鐘本 楊（かねもと よう）
野村 啓仁（のむら ひろと）
NTT社会情報研究所

はじめに

経済活動や社会の変化に伴って，機器やソフトウェアに対するリスクも様変わりしています．その中でも顕著な変化はソフトウェアのサプライチェーンに対するセキュリティリスクの高まりです．米国ではこのリスクへの対応を目的とした大統領令が発令され，SBOM（Software Bill of Materials，ソフトウェア部品表）などを活用した機器やソフトウェアに関する構成の把握が求められています．本稿では，このようなサプライチェーンセキュリティリスクに関する動向と研究所の取り組みを紹介します．

ソフトウェアサプライチェーンのセキュリティリスクとは

令和4年版情報通信白書では，ICTが「社会・経済のインフラとして定着」している段階にあるとされています．それまでICTには生産性の向上や効率化などが期待されていましたが，「攻めのIT」のような言葉に代表される新たなビジネスを切り拓く原動力としての役割が期待され，ソフトウェアも長期的な計画を立ててリリースする開発スタイルから，継続的インテグレーションと呼ばれる矢継ぎ早に機能をリリースするスタイルへ変革しています．その開発スピードを支えるために，データベースやフレームワークだけでなく，ログ出力やWeb画面の描画まで多岐にわたりOSS（Open Source Software）によるライブラリが活用されています．また，機能をアップデートするために頻繁にファイルを更新，あるいは機能を追加するためにプラグインを組み合わせるなどのように，ソフトウェアの役割が細分化・複雑化しています（**図1**）．

このようなソフトウェアの作成・提供・利用・更新などの一連の流れをソフトウェアサプライチェーンと呼びます．そして，ソフトウェアサプライチェーンこそが新たなサイバー攻撃の標的になっています．一例を挙げる

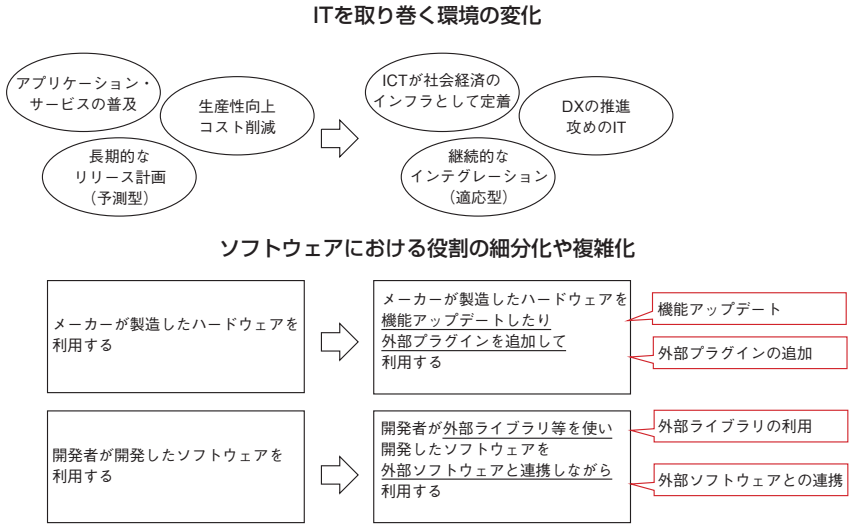

図1　ITを取り巻く環境の変化とソフトウェアにおける役割の細分化や複雑化

と，ソフトウェアに組み込まれたソフトウェア部品（ライブラリ）に脆弱性が発見され，この脆弱性をねらった攻撃によって情報漏洩が発生する事例，あるいはソフトウェア部品がファイル・アップデート機によってマルウェアに感染するといった事例などがあります．注目すべきことは，ソフトウェア本体を安全な状態に保つことをサポートするサプライチェーンが，逆に深刻なインシデントを発生させる脅威になる場合があるという点です．

米国では国家に対する幾度ものセキュリティインシデントを経て，2021年5月に「国家のサイバーセキュリティ改善に対する大統領令」が発令されました．これに基づき，米国NTIA（国家通信情報管理局）はSBOMをベンダが購入者に対して開示することを求めています．

透明性をキーコンセプトとするリスク対応策とその課題

SBOMは機器やシステムに含まれるソフトウェアを一覧化するためのデータであり，SPDX（Software Package Data Exchange）やCycloneDXなどのデータフォーマットが提案されています．どのようなフォーマットであるにせよ，ソフトウェアのモジュールやライブラリまで情報が網羅されていれば，ライブラリに脆弱性が発見された場合でも，素早く影響の有無を調べることができるようになります．また，機器の調達からユーザの利用までの各フェーズでSBOMを作成することによって，どこで不正なソフトウェアが混入したのかを調べることもできます．

このようにSBOMによる透明性の確保はリスク対応として大変有効ですが，その有効性をさらに高めるために解決すべき以下のような課題があります．

① ソフトウェアが他のソフトウェアを利用して動作する依存関係がある場合でも，漏れなくソフトウェアの構成を把握すること（ソフトウェア依存関係の把握）

② 商業上の理由などによってソフトウェア作成者が一部の構成情報を開示できない場合でも，リスク対応の効果を最大限得られること（構成情報の一部非開示への対応）

③ 構成情報やその関連情報（脆弱性情報など）が多様かつ膨大でも，効率的・効果的に管理・活用できるようにすること（多様かつ膨大な構成情報の管理・活用）

以降では，これらの課題に関するNTT研究所の取り組みを紹介します．

ソフトウェア依存関係の把握

SBOMによって機器やシステムに含まれるソフトウェアを一覧できても，多くの場合，実際に明らかにできるソフトウェアの構成は一部です．ソフトウェアの多くは，他のソフトウェアをさらに利用するかたち，すなわち依存関係がある構成をとります．ソフトウェアの依存関係はパッケージマネージャと呼ばれるシステムによって管理されています．そのため，ソフトウェアが他に何のソフトウェアを利用しているのかはパッケージマネージャの管理情報から把握することができます．例えばPythonにはPackage Installer for Python（PIP）という仕組みがあり，利用するパッケージ情報はPIPによって管理されています．開発者がPIPの管理情報を提供することによって，あるソフトウェアが依存しているソフトウェアの情報が明確になります．このように，管理情報によって示される明示的な依存関係がある一方で，暗黙的な依存関係も存在します（**図2**）．

もっとも有名な暗黙的な依存関係にコードクローンがあります．コードクローンとはソフトウェアのソースコードが一致あるいは類似していることを指します．同じような機能を実装するために他のソフトウェアのソースコードを参考にし，ソースコードをコピーすることによってコードクローンが生まれます．つまり，ソフトウェア利用者は知らぬ間に他のソフトウェアと同じコードを利用することになります．同様に，コードのQAサイトにも一部のコード例が示されており，これをそのまま利用しているソフトウェアも存在します．つまり，ソフトウェアのコードがQAサイトのコード例に依存していると考えることができます．

それでは，仮に，あるソフトウェアが依存しているソフトウェアのコードに脆弱性（セキュリティの欠陥）が発見された場合，どうなるでしょうか．当該ソフトウェアと同様のコードを有するすべてのソフトウェアに脆弱性が存在する可能性があります．また，当該ソフトウェアが別のプログラムから

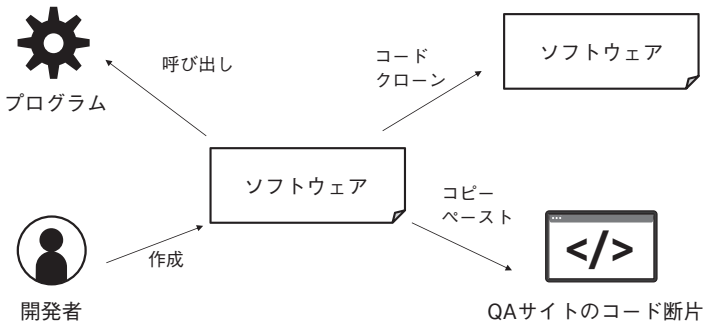

図2　ソフトウェアのさまざまな暗黙的な依存関係

起動される関係にある場合，その別のプログラムにも脆弱性による影響が波及し，当該ソフトウェアが動作するシステムの動作に影響を与える可能性があります．

また，ソフトウェアの開発者やその開発環境による依存関係がもたらすリスクも考えられます． OSSの場合，開発者が不特定多数になり，その中には悪意を持つ開発者，あるいは知らぬ間にセキュリティ侵害を受けた開発環境を利用している開発者が存在する可能性があります．そのため，十分な確認をせず，他の開発者が作成したソフトウェアを利用することはセキュリティリスクになり得ます．

このようにソフトウェアには，SBOMが可視化する明示的な依存関係には表現されていない暗黙的な依存関係があり得ます．私たちは，このような暗黙的な依存関係を把握することによって，ソフトウェアおよびソフトウェアを利用する機器の透明性をより高める技術の研究開発に取り組んでいます．

構成情報における一部非開示への対応

ソフトウェアの構成情報を開示すると攻撃者にヒントを与えるなどのデメリットが生じる可能性があります．そのため，開発者によっては構成情報の一部または全部を非開示にしたいと考えるかもしれません．このような場合でも，機器やシステムの透明性を確保するためにはどうすればよいでしょうか．

利用者が機器やシステムを購入する場合，まずカタログやマニュアルに書かれているとおりの動作をするのかを確認するでしょう．さらに，機器の利用を始めると，マニュアルに書かれていない通信を検知する場合もあるかもしれません．例えば，ネットワーク機器の中には最新バージョンのソフトウェアやデータを，インターネットを介して取得するものがあります．多くの場合，この通信についてはマニュアルには記載されていませんが，このような通信も機器の正当な動作仕様といえます．

そこで私たちは，このような動作仕様と，装置やシステムの外部から観測したデータを活用することによって，当該動作をもたらすソフトウェアの構成要素を推定できる可能性に着目した研究開発に取り組んでいます．例えば，通信ログや動作ログなどに記録・蓄積される情報を用いることによって，SBOMによって可視化される構成情報を補うことを可能にし，開発者が構成情報の一部を開示できない場合でも，利用者がセキュリティリスク対応の効果を最大限得られる状況をつくることをめざしています．

多様かつ膨大な構成情報の管理

ここまでは，サプライチェーンセキュリティリスク対応を目的として，ソフトウェアの構成情報に関する情報量を高める取り組みについて紹介してきました．情報の多様化や増大は，セキュリティ対策への活用の可能性を高める一方で，必要な情報を特定して的確に活用することを難しくする可能性もあります．また，構成情報から関連付くさまざまな情報（例えば脆弱性情報）も増え，管理・対処すべき情報は膨大になるでしょう．

私たちは，構成情報の充実化によってセキュリティの透明性を確保した先で想定される新たなセキュリティ対策業務（セキュリティオペレーション）のあり方とそれを実現するための技術についても研究に取り組んでいきます．

米国国立標準技術研究所（NIST）が規定するCyber Security Framework（CSF）では，セキュリティ対策を「特定」「防御」「検知」「対応」「復旧」の５つの機能で大別しています．このうち，セキュリティの透明性を確保するために構成情報を充実化させることは「特定」を強化することにつながります．そこで，私たちは，この「特定」の強化によって，CSFにおける他の４つの機能の効果を効率的に高める可視化データの統合的な管理・活用技術に関する研究（構成情報を活用した効率的な脆弱性対応，高精度な異常検知・原因推定，自動対処など）にも取り組んでいきます．

今後の展開

本稿では，セキュリティの透明性をキーコンセプトとするサプライチェーンセキュリティリスク対応技術の研究開発について紹介しました．本技術は，NECとの資本業務提携により一緒に検討を進めており，多様なプレイヤがオープンに共創を行うIOWN（Innovative Optical and Wireless Network）や社会・経済の基幹インフラを支える技術となることをめざしていきます．

（左から）上原　貴之／鐘本　楊／野村　啓仁

サプライチェーンをねらうサイバー攻撃は甚大な被害をもたらし得る脅威です．私たちは，この脅威に対抗する新技術の創出によって社会に貢献していきます．

◆問い合わせ先
NTT社会情報研究所
企画担当
E-mail　solab＠hco.ntt.co.jp