6 セキュリティトランスペアレンシー確保技術

セキュリティの可視化によって サプライチェーンセキュリティリスクを低減

サプライチェーンを通じてシステムや機器に不正な構成要素や脆弱性などが紛れ込み、従来にない大きなセキュリティリスクを社会にもたらす問題が世界的に注目されている。そこでNTT社会情報研究所（以下、社会研）は、システムや機器に関するソフトウェア構成や脆弱性などによるリスクを可視化し、リスクを低減する技術の開発および社会実装に向けたコンソーシアムの立ち上げに取り組んでいる。

NTT社会情報研究所　社会イノベーション研究プロジェクト
（左から）　プロジェクトマネージャ　**中嶋 良彰**氏、同プロジェクト　担当課長　**佐藤 亮太**氏
社会実装推進グループ グループリーダ　**長島 武生**氏
システム基盤技術グループ　主任研究員　**上原 貴之**氏

サプライチェーンセキュリティリスクへの対策が課題に

システムや機器にはOSS（Open Source Software）を含むさまざまなソフトウェアが活用される。開発効率が良い一方で脆弱性やバックドアが混入しやすい。また多数の政府や企業が利用するソフトウェアの開発工程でマルウェアが混入した事例もある。このような脆弱性や攻撃を組織や企業が個々に把握することは難しく、対策が必要な重要課題として国内外で認識されるようになった。

セキュリティトランスペアレンシー確保技術の概要

社会研は数年前よりこの問題の解決に取り組んでおり、2020年6月の資本業務提携を契機にNECと共同で研究開発を進めている。2021年10月にはその成果として「セキュリティトランスペアレンシー確保技術」（以下、本技術）を発表した。本技術は3つの要素技術から構成されている。1つは社会研が開発した「構成分析技術」。システムや機器のソフトウェア構成を自動で把握し、構成情報を生成・更新する。残り2つはNECにより開発された、バックドアが存在しないことを確認する「バックドア検査技術」、およびシステムのリスクを評価する「サイバー攻撃リスク自動診断技術」だ。

本技術はシステムや機器の構成とリスクを可視化し、可視化データをサプライチェーンにおいて共有しやすくする。調達時に不正なソフトウェアの有無を確認できるほか、運用開始後に発見された脆弱性の影響を素早く把握し対処可能、といったように、製品ベンダ、SI事業者、製品を導入・運用するユーザ事業者のいずれにもメリットがある。

SBOMを利用し可視化データの活用性を向上

ソフトウェア構成の可視化には、SBOM（Software Bill Of Materials）と呼ばれるソフトウェア部品の一覧表のようなデータを用いる。SBOMは、もともとはOSSの活用が進み複雑になったソフトウェア開発のサプライチェーンにおけるライセンス管理などのために発展してきた。現在、SBOMはサプライチェーンセキュリティに関する各国政策にも関係するようになっている。

「2021年5月に米国で『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、これに対応する形で米国NTIA（国家通信情報管理局）が製品ベンダに対しSBOMによる情報開示を求めています。2023年3月に公表された米国国家戦略でもサプライチェーンセキュリティリスクへの対応が謳われています。」（上原氏）

米国政策はグローバルに影響すると考えられ、SBOMへの注目が日本国内でも高まっている。

「日本でも一部民間企業が注目しているほか、経済産業省もSBOMの活用に向けた検討会を開催しています。」（長島氏）

SBOMには、用途が異なる複数のデータ仕様が存在する。そのうちSPDXとCycloneDXという2つの仕様をベースに、セキュリティトランスペアレンシー確保技術においては、ソフトウェア構成やリスクに関する可視化データを生成し、サプライチェーンにおいて共有していくことを検討している。

標準的な仕様を利用することにより製品ベンダ等が情報提供しやすくなるほか、SBOMに対応した各種ツールやシステムの利用が可能になり、可視化データを活用しやすくなるといった効果も期待できる。

可視化データの情報量と品質を強化する独自技術の開発

製品には製品ベンダが開示し難い情報も含まれる可能性があるため、本技術では構成情報の全開示を前提としていない。製品の通常利用において知り得る「通信や動作の仕様」など、製品ベンダにとってより開示しやすい情報を可視化データの生成に利用でき、製品の利用側ではこのような情報からソフトウェアの構成や脆弱性の存在を自動的に推定する技術を開発した。

情報量に加え、可視化データの品質を強化するための技術開発も行っている。その一例がサプライチェーンにおいて共有した情報を比較・分析することによる正確性の向上だ。

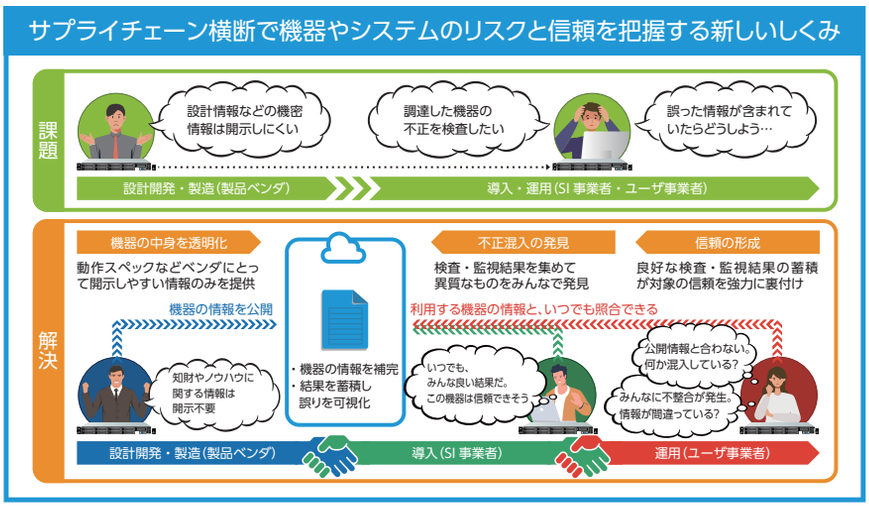

図1　サプライチェーン全体でのリスク把握に向けた課題を解決

「複数の事業者がそれぞれ行う検査や監視の結果を横断的に分析します。同種の対象を同じ可視化データに基づき検査したにも関わらず、ある事業者の結果にだけ差異がある場合、可視化データがおかしい（または対象が不正に動作している）と推測できます。このように可視化データの共有によって、一社ではわからなかったことに気づけるようになる可能性があります。」（佐藤氏）

事業適用をめざしたフィールド実証

2022年11月にはNTTグループの事業会社、およびNECと共同で本技術のフィールド実証をスタートしている。各社の通信サービスやシステム、またそのなかで用いられる機器に関する可視化データをいかに生成し、運用に活かすかを検討・実証することが目的だ。

「可視化データの活用によってセキュリティ検査などを効率化できることを確認できました。さらなる活用として、脆弱性に関する評価や対処など、システムの運用に関わる多くの課題に対し、パートナと一緒に検討を進めています。」（上原氏）

さまざまな企業・組織と協調するためコンソーシアムを設立

本技術の有効活用にはサプライチェーンにおいて各事業者が連携・協力することが欠かせない。そこで2023年度上期を目処に“セキュリティ・トランスペアレンシー・コンソーシアム（Security Transparency Consortium：以下、本コンソーシアム）”を設立する予定だ。

「本技術やSBOMなどをどのように活用すればセキュリティを高めることができるかといった知見を、サプライチェーンを形成する事業者間で協調して検討することが、コンソーシアムのねらいです。」（中嶋氏）

コンソーシアムへの期待を佐藤氏は次のように述べている。

「コンソーシアムの参加メンバが知見や技術を持ち寄り、相互に活用・磨き合うことによって、サプライチェーンセキュリティリスクを低減していくことも想定しています。」