情報通信ネットワークの安全性を向上するセキュリティトランスペアレンシー確保技術

岸本 衣緒　中島 一彰　植田 啓文

要 旨

重要インフラを狙ったサイバー攻撃が増大しており、すべての重要インフラの基盤であり、かつサイバー攻撃の侵入口となり得る情報通信ネットワークの安全性を維持することが課題になっています。また、経済安全保障推進法の成立により、重要インフラの事業者はセキュリティ管理の説明責任を求められており、ネットワーク機器を含めてITシステムの透明性を確保して、内部の状態を把握しておくことが重要です。NECはこの課題を解決するために、セキュリティトランスペアレンシー確保技術の開発に取り組んでいます。本稿では、セキュリティの透明性確保の重要性と、本技術を活用したシステムの安全性確保について紹介します。

KeyWords
セキュリティトランスペアレンシー／透明性／サプライチェーン／ネットワーク／重要インフラ

1. はじめに

昨今、重要インフラへのサイバー攻撃が数多く報告されています。重要インフラシステムはIT化が進んだことで、情報通信ネットワークが張り巡らされています。これらのネットワークはインターネットにはつながっておらず閉域網での運用が多いものの、攻撃者は重要インフラへのサイバー攻撃の侵入口として、その情報通信ネットワークを狙っています。

閉域網の情報通信ネットワークへの新たな脅威として、サプライチェーンを狙った攻撃が懸念されています。部品を調達し、機器やシステムを製造するサプライチェーンの一連の流れのなかで、防御が手薄な企業が狙われ攻撃されます。攻撃としては、バックドアという不正機能を仕掛けることで、外部からシステムへ侵入し不正操作するという事例が報告されています[1)]。

攻撃の増加と新たな脅威の出現が背景となり、重要インフラの事業者は、システムの安全性を維持する取り組みへの説明責任を果たすことが求められています[2)]。そのため、システムの安全性を説明するには、ネットワーク機器やシステムの状態を正しく把握し、適切に運用する必要があります。また、正しく把握するためには、セキュリティの透明性を確保することが重要になります。

2. セキュリティの透明性確保

2.1 セキュリティの透明性とは

セキュリティの透明性の確保は、**図1**に示すNISTサイバーセキュリティフレームワーク[3)]の識別に関連します。本フレームワークでは、最初に「識別」において対象となる情報通信ネットワークの機器の構成及びシステムの構成を把握することが明記されています。「識別」をもとに「防御」や「検知」の検討を実施していくというものです。

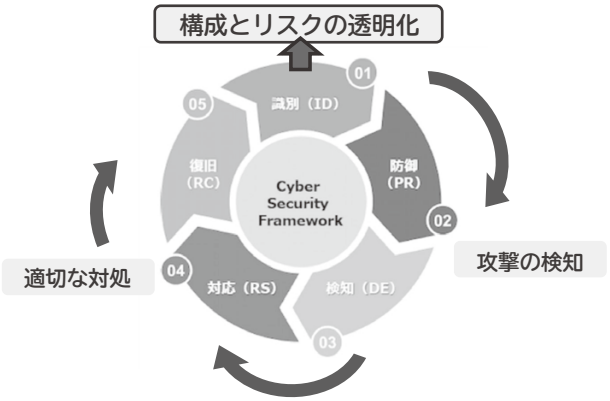

図1　NISTサイバーセキュリティフレームワークにおけるセキュリティの透明化の重要性

本稿では、この識別において、これらの構成及びリスクも把握することを「セキュリティの透明化」、把握できる状態であることを「セキュリティの透明性がある」と定義しています。

このセキュリティの透明性が不十分な場合は、どのようなリスクが存在しているのか不明瞭で、また、攻撃が内部で侵攻していても気付けず、対処することができません。つまりセキュリティの不透明さは、攻撃リスクを増加させてしまう要因になります。それゆえ、構成とリスクを正確に把握し、セキュリティの透明性を向上させることは、攻撃を検知して攻撃に対して適切に対処するインシデントレスポンスを素早く行うことにつながります。

2.2 セキュリティの透明性化における課題

セキュリティを透明化するためには、機器の構成及び、システムの構成に関するさまざまな情報を把握する必要があります。

構成の要素の1つとしてソフトウェアがありますが、その管理にあたっては、SBOM（Software Bill Of Materials）が注目されています[4]。特に米国を中心に、米国大統領令のもと、サプライチェーンにおけるSBOM活用の議論が行われています。SBOMでは、ソフトウェアの部品情報を一覧化することで、ソフトウェアを構成する部品を把握し、発見された脆弱性情報を紐付けることが可能になるため、サプライチェーンにおけるソフトウェアの脆弱性管理への活用が期待されています。

しかしながら、SBOMはあくまでもソフトウェア部品を一覧するためのものであるため、ソフトウェア内にバックドアのような不正機能があるかどうかを検出することはできません。更に、ソフトウェア部品ごとの脆弱性情報を検知することはできますが、当該脆弱性がシステムにおいて悪用可能であるかを判断することはSBOMだけではできません。一方で、セキュリティの透明化にかかわるSBOMなどの情報をサプライチェーン全体で共有する仕組みは現在なく、情報の流通という観点にも課題があります。

3. セキュリティトランスペアレンシー確保技術

サプライチェーンを通したSBOM活用の検討活動により、ソフトウェア構成の透明化は進んでいますが、第2章で述べたようにセキュリティの透明化には十分な情報があるとはいえません（**図2**）。これを解決するためにNECでは（1）バックドア検査技術、（2）システムリスク診断技術、（3）サプライチェーンを通した情報共有基盤、の研究開発に取り組んでいます。本技術を活用することで、セキュリティの透明化に必要な情報を補完し、それらを共有可能とし、迅速かつ確実なセキュリティ管理を行うことができるようになります。次に各技術について説明します。

3.1 バックドア検査技術

バックドア検査技術は、ソフトウェアの構成管理だけでは確認が困難である不正機能の混入を検査し、不正機能の有無を可視化する技術です。本技術の特徴は、ソフトウェアのバイナリから制御・データフローを分析して、ソフトウェアに含まれる不正機能を検出します。バイナリを直接検査できることで、ソフトウェアビルド時に不正機能が混入したとしても検出することが可能です（**図3**）。

3.2 システムリスク診断技術

システムリスク診断技術は、人手で把握が困難なシステムのリスクを網羅的に分析しそれらを可視化する技術で

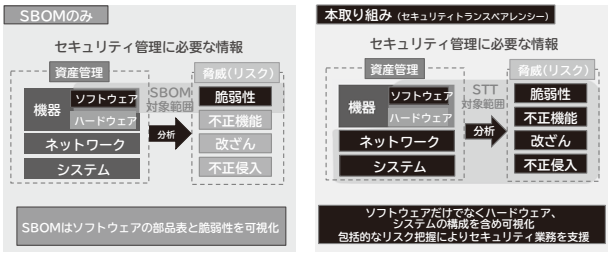

図2　セキュリティトランスペアレンシー確保技術が提供する付加価値の概要

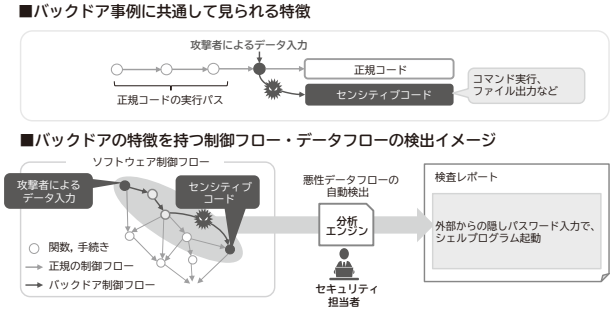

図3　バックドア検査技術の特徴

す。本技術では、実システムの構成情報やデータフローをもとにシステムの仮想モデルを生成し、仮想モデル上で攻撃シミュレーションを行うことで網羅的な分析を実現しています。分析によりシステムへの侵入経路とその攻撃手口（システムに存在する脆弱性の悪用可能性）を把握することができるため、適切なセキュリティ対策を実施していくことができるようになります（**図4**）。

3.3 情報共有基盤

情報共有基盤は、サプライチェーン上で構成情報、及び、リスク情報の共有、管理を実現するものです。本情報共有基盤では、サプライチェーン上の各事業者が作成した構成情報やリスク情報が登録されます。 登録された情報は、システムを運用する事業者（サプライチェーンにおけるエンドユーザー）のシステムの構成に紐付けられて表示されます。これにより、運用システムの管理者は、自身が運用するシステムにかかわるサプライチェーンの事業者から情報を収集することができ、また、当該システムのセキュリティ状況を把握することが可能になります。（**図5**）。

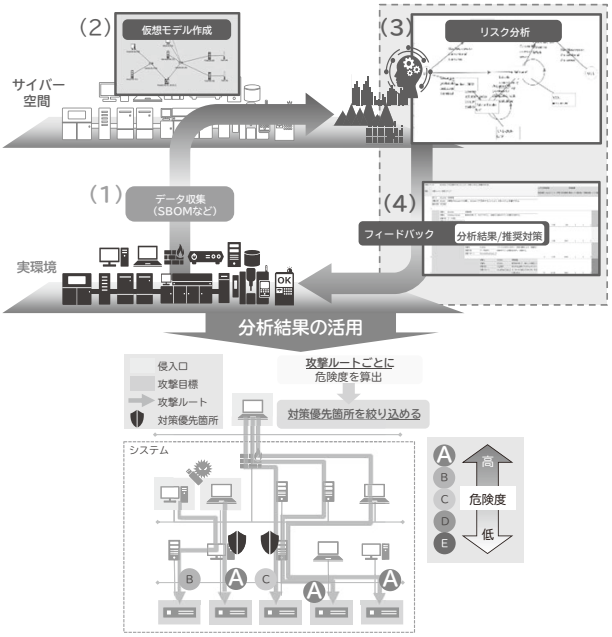

図4　システムリスク診断技術の特徴

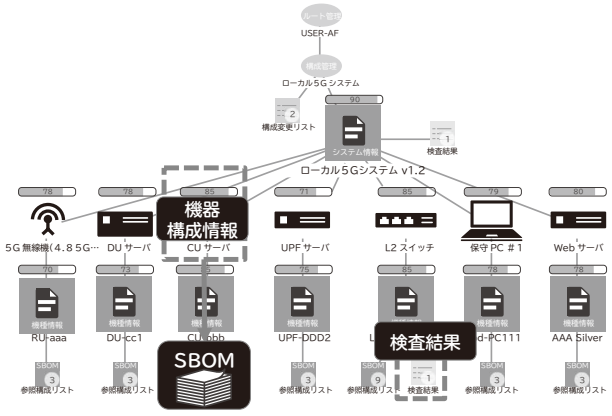

図5　情報共有基盤の特徴

4. セキュリティトランスペアレンシー確保技術の効果

第４章ではセキュリティトランスペアレンシー確保技術のユースケースを説明し、各技術の効果について述べます。ユースケースの登場人物として、**図6**に示すように、ソフトウェア開発を請け負うソフトウェアメーカー、機器を製造する機器メーカー、機器設定やシステム構築を行うSIer、システムを運用するユーザー事業者がおり、サプライチェーン上の事業者として想定します。また、ユースケースは、各登場人物間における取引として、(1) ソフトウェアメーカーから機器メーカーへのソフトウェアの納入、(2) 機器メーカーから調達した機器を用いたSIerによるシステムの構築、(3) SIerから納入されたシステムをユーザー事業者が運用、を例にして、各事業者におけるセキュリティトランスペアレンシー確保技術を用いたセキュリティの透明化について説明します。

4.1 機器メーカーにおけるセキュリティの透明化

機器メーカーにおけるセキュリティの透明化では、自社の機器の構成の把握、及び、ソフトウェアメーカーから納入されたソフトウェアに不正な機能がないかを確認します。構成の把握は、ソフトウェアメーカーから入手したSBOMで対応可能ですが、ソフトウェアにバックドアのような不正な機能が組み込まれていないかは判断できません。そこで、機器メーカーはバックドア検査技術を利用することで、機器内で使用されるソフトウェアの安全性を確認します。これによって、自社の機器のセキュリティの透明性を確保することができるようになります。また、機器メーカーはこれらの確認結果を共有基盤に登録することで、自社機器を調達するSIerと共有することができます。

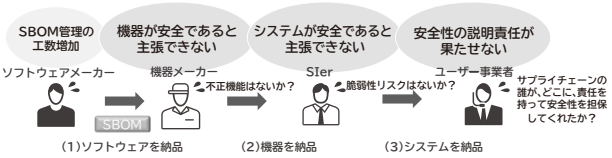

図6　ユースケースにおける各事業者の役割と抱えている課題

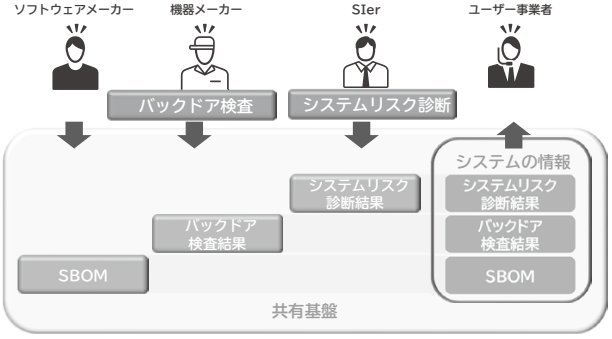

図7　情報共有基盤上でセキュリティ透明化されている状態

4.2 SIerにおけるセキュリティの透明化

SIerにおけるセキュリティの透明化では、調達した機器の構成及び、構築したシステムの構成、リスクの管理を行います。SIerは、機器メーカーから提供された構成情報をもとに機器の構成とリスクの把握は可能ですが、構築したシステムのリスクの把握は自身で実施する必要があります。例えば、各機器のSBOMを確認し脆弱性のあるソフトウェアが判明した際、構築したシステムへの影響を分析、把握し、適切な対応を実施すること、既にシステムを納入している場合は、ユーザー事業者へリスク情報を提供することが必要になります。その際に、SIerは、システムリスク診断技術を活用することで、適切な対処を円滑に行うことができます。共有基盤に登録されている調達機器のSBOM情報を使い、対象システムの仮想モデルを構築し、仮想モデル上で攻撃シミュレーションを行うことで、確認された脆弱性の悪用可能性を調査することができます。その際、当該脆弱性を利用した攻撃経路が検出された場合は、当該脆弱性に対する対応を実施するとともに、当該結果を共有基盤に登録することでユーザー事業者へ伝えることもできます。

4.3 ユーザー事業者によるセキュリティの透明化

ユーザー事業者のセキュリティの透明化は、機器メーカーやSIerから提供される情報をもとに自身が利用するシステムの構成を把握し、利用形態によるリスクを把握することです。**図7**に示すように、前述した2つのユースケースを通して、各事業者のセキュリティ透明化で得られた情報は共有基盤を通してユーザー事業者へ提供され、ユーザー事業者のシステムの構成と紐付けて管理されており、ユーザー事業者はサプライチェーンの事業者から送られてくる最新の情報を常に確認することが可能です。また、前述したシステムリスク診断技術を活用して、システムの仮想モデルにユーザー操作状況やアカウント管理情報を追加することで、利用形態におけるシステムのリスクを可視化することができます。これにより、ユーザー事業者自身のシステムの利用形態と照らし合わせてセキュリティの懸念が発生していないかを判断することができるようになります。

5. むすび

本稿では、セキュリティの透明性確保の必要性と、それを実現するトランスペアレンシー確保技術について紹介しました。

社会はすべての人とモノがつながる未来を切り拓こうとしています。その社会を支えるシステムでは、セキュリティの透明性が確保され、セキュリティが維持され続けることが重要です。NECはセキュリティのトランスペアレンシー確保の技術により、より安全な未来作りへ貢献します。

参考文献

1) THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY: Joint Statement By the Federal Bureau Of Investigation (FBI), The Cybersecurity And Infrastructure Security Agency (CISA), The Office Of The Director Of National Intelligence (ODNI), And The National Security Agency (NSA), 2021.5
https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure
2) 内閣府：経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法），2022
https://www.cao.go.jp/keizai_anzen_hosho/index.html
3) NIST：CYBERSECURITY FRAMEWORK
https://www.nist.gov/cyberframework
4) THE WHITE HOUSE ：Executive Order on Improving the Nation's Cybersecurity, 2021.5
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

執筆者プロフィール

岸本 衣緒
セキュアシステムプラットフォーム研究所
主任

中島 一彰
セキュアシステムプラットフォーム研究所
リードリサーチエンジニア

植田 啓文
セキュアシステムプラットフォーム研究所
ディレクター

関連URL

NTTとNEC、情報通信インフラにおけるサプライチェーンセキュリティリスクへの対策技術を開発
https://jpn.nec.com/press/202110/20211027_01.html

サプライチェーンセキュリティリスクを低減する技術のフィールド実証を開始
https://jpn.nec.com/press/202211/20221109_03.html

NEC、システムのセキュリティリスクとその対策効果を可視化するサービスを提供開始
https://jpn.nec.com/press/202106/20210629_01.html

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.75 No.1　オープンネットワーク技術特集
～オープンかつグリーンな社会を支えるネットワーク技術と先進ソリューション～

オープンネットワーク技術特集によせて
NECのオープンネットワークに向けた技術開発と提供ソリューション

◇ 特集論文

Open RANとそれを支える仮想化技術
Open RANがもたらすイノベーション
モバイルネットワークにおける消費エネルギー削減
自己構成型スマートサーフェス
Nuberu：共有プラットフォームによる高信頼性のRAN仮想化
vrAIn: vRANにおけるコンピューティングリソースと無線リソースのためのディープラーニングベースのオーケストレーション

5G/Beyond 5Gに向けた無線技術
グリーン社会の実現に向けたNECにおける5G/Beyond 5G基地局のエネルギー効率化技術開発
双方向トランシーバアーキテクチャを備えたミリ波ビームフォーミングICとアンテナモジュール技術
5G/6G屋内ワイヤレス通信向け1ビットアウトフェージング変調による光ファイバ無線システム
空間分割多重を用いた28GHz帯マルチユーザー分散Massive MIMO
28GHz帯マルチユーザー分散MIMOシステムを用いたOTFS変調信号のOTA測定
Sub6GHz帯アクティブアンテナシステムにおける空間多重性能の改善
トランジスタ非線形モデルを使用しないブラックボックスドハティ増幅器の設計手法
最大8マルチユーザー多重化を実現する39GHz帯256素子ハイブリッドビームフォーミングMassive MIMO

オープンAPN（オープン光・オール光）の実現への取り組み
APN実現に向けたNECの取り組み ～Openな光ネットワーク実現に向けて～
APN実現に向けたNECの取り組み ～APN製品（WXシリーズ）の特長～
APN実現に向けたNECの取り組み ～フィールドトライアル～
オールフォトニクスネットワークを支えるシリコンフォトニクス光源による波長変換技術
NEC Open Networksを支える光デバイス技術 ～800G超の光伝送技術～

コア&バリューネットワークへの取り組み
カーボンニュートラルな社会の実現に向けたデータプレーン制御を支える技術
5G時代の人々の暮らしを支えるNECのネットワークスライシング技術
Beyond 5G、IoT、AIを活用したDX推進を支えるアプリケーションアウェアICT制御技術
通信事業者向け5Gコアネットワークにおけるパブリッククラウド活用

高度なネットワークサービスを提供する自動化・セキュア化への取り組み
OSSにおける運用完全自動化へのNECの取り組み
利用者の要件に基づくネットワークの自律運用技術とセキュリティ対応の取り組み
情報通信ネットワークの安全性を向上するセキュリティトランスペアレンシー確保技術
ネットワーク機器のサプライチェーン管理強化に向けた取り組み

ネットワーク活用ソリューションとそれを支える技術
通信事業者向け測位ソリューション
5Gのポテンシャルを最大限に引き出すトラフィック制御ソリューション（TMS）
ローカル5G向け小型一体型基地局「UNIVERGE RV1200」及びマネージドサービス
産業DXを支えるローカル5G活用によるバーティカルサービス
ローカル5G、LAN/RAN融合ソリューション

グローバル5G xHaulトランスポートソリューション
トランスポートネットワークの高度化を実現するxHaulソリューション・スイート
xHaulトランスフォーメーションサービス
xHaulトランスポート自動化ソリューション
5G/Beyond 5Gにおける固定無線トランスポート技術
Beyond 5Gに向けたSDN/自動化
高効率・大容量無線伝送を実現するOAMモード多重伝送方式

Beyond 5G/6Gに向けて
Beyond 5G時代に向けた取り組み

◇ NEC Information
2022年度C&C賞表彰式典開催

Vol.75 No.1
（2023年6月）

特集TOP