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

曽根 泰斗　勝田 将史　野出 利緒　安達 智雄

要 旨

近年、サイバー空間における脅威が深刻化し、安全保障領域や重要産業インフラのサプライチェーンを狙った攻撃などにより、経済的・社会的に多大な損失が生じる可能性が懸念されています。NECでは、安全・安心なネットワーク機器を提供するため、国内工場の検査による出荷・運送時のリスク対処と、機器のセキュリティ情報を網羅的に収集・分析する製品による運用時のリスク対処をサポートします。本稿では、工場で実施しているセキュア生産・検査とNECで開発した製品を用いたセキュア運用で実現するサプライチェーン管理強化の取り組みを紹介します。

KeyWords
サプライチェーン／セキュリティ／ネットワーク／重要産業インフラ／トレーサビリティ／サイバーセキュリティ

1. はじめに

政府機関や重要産業インフラの安全保障領域において、機器の設計段階から製造・運送・保守までのサプライチェーン全体を狙った攻撃へのリスクを低減するため、リスク対策された機器や仕組みなど、選定時の考慮すべき要素を定めたガイドラインの整備が進んでいます。

内閣サイバーセキュリティセンター（以下、NISC）の「政府機関等のサイバーセキュリティ対策のための統一基準群」（以下、統一基準群）[1]では、サプライチェーンリスクに対する記載が強化されています。統一基準群を構成する「政府機関等の対策基準策定のためのガイドライン（令和３年度版、一部改定）」[2]では、機器などの選定基準として、機器などのライフサイクルで不正な変更が加えられない管理がなされていることを遵守事項としています。更に、NISCの「重要インフラのサイバーセキュリティに係る行動計画」[3]では、経営層、CISO（Chief Information Security Officer：最高情報セキュリティ責任者）をはじめ、組織全体でサプライチェーンにかかわる体制の強化やサプライチェーンリスクなどの新たな脅威に対して先取りした対応が求められています。

一方で、従来のネットワーク機器管理では、ネットワークの運用維持に主眼が当てられており、利便性を重視した共有IDの使用や、通信維持を優先し脆弱性対処を先送りにすることでリスクが生まれています。ネットワーク機器はサイバー攻撃の対象にもかかわらず、運用中のリスク対策は重要視されていない傾向があります。

2. ネットワーク機器のライフサイクルに潜むサプライチェーンリスク

サプライチェーンセキュリティ管理のためには、ネットワーク機器のシステムライフサイクルに潜むさまざまなリスクに対処する必要があります（**図1**）。

生産・流通時の主要なリスクには不正改造があります。

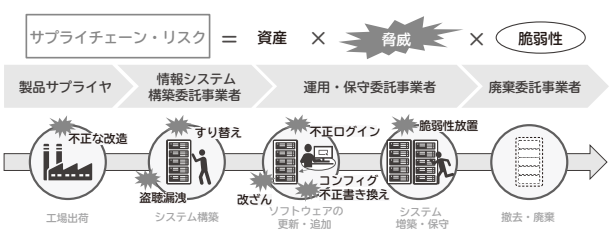

図1　ネットワーク機器のサプライチェーンリスク

従来は工場出荷した機器に対する改ざんや不正プログラムの組み込みを自ら確認する方法がないため、工場出荷時の真正性を確認することができませんでした。

運用中のリスクには脆弱性の放置、内部不正による機器や部品のすり替え、外部からの攻撃によるユーザーIDの不正窃取、設定の不正変更などがあります。利便性を重視した運用では、これらリスクに対処するには運用コストが掛かり過ぎるため、現実的ではないと考えられています。その結果、原因究明が十分行えず、経営者やCISOはインシデントに対する説明責任を果たせなくなります。

3. NECにおけるサプライチェーン管理強化の取り組み

NECで販売しているシスコシステムズ合同会社のネットワーク機器（以下、Cisco製品）は、各リスクにおいてNEC独自の仕組みで対策を講じ、サプライチェーン管理を強化しています（**図2**）。

3.1 国内での工場検査

NECの出荷するCisco製品[*1]は、国内工場でサイバーセキュリティやBCP（事業継続計画）の考え方を採用したセキュア生産と後述する独自拡張したセキュア検査を実施しています。Cisco製品を販売する際には、セキュア物流の施策として、運送中の開封を防止するために貼り直しができないテープによる封印を行います。また、セキュアな環境の国内工場で最終出荷検査されたことを示すセキュア生産証明書の発行が可能です。

3.2 セキュア検査による真正性担保

本取り組みにおけるCisco製品に対するセキュア検査では、ハードウェアとソフトウェアの不正変更を検出し、真正性を担保します。はじめに、ソフトウェアファイルと工場出荷バージョンファイルリストについて、デジタル証明書及びハッシュ値のブロックチェーン登録・比較により、正規のファイルかつ工場出荷バージョンであることを確認します。次に、Cisco Trustworthy技術[4)]に対応した製品では、セキュリティチップにより安全性が担保されたセキュアブートを実施します。具体的には、セキュリティチップ内のプログラムから製品の起動を開始し信頼性が確認できた場合のみ、次の段階のプログラムを実行します。そして、ソフトウェアファイルに含まれるデジタル署名の検証によりソフトウェア確認を行い、セキュアに起動することを確認します。最後に、セキュリティチップ内のデジタル証明書チェーンの検証を行うことで、正規のCisco製品であることを確認します。

3.3 ブロックチェーンによる証跡管理

セキュアブートで起動した記録は検査ログファイルに保存されます。一方向ハッシュ関数によってその検査ログファイルのハッシュ値を生成し、ブロックチェーンに送ることでデジタル証跡として保管します。ブロックチェーンは、特定の人や機関の信用に依存せず、同じ台帳を複数のノードで共有・管理することにより、改ざんできない仕組みになっているため、保管したデータの確実な保護が可能です。

4. ネットワークの正常を維持する仕組みを提供

NECでは、構築・運用フェーズにおいてネットワーク機器のログイン履歴や構成変更などの情報を運用管理者に通知し、リスクを可視化する製品「NECサプライチェーンセキュリティマネジメントforネットワーク（SCSM）」を開発・提

図2　生産時のサプライチェーン管理強化の特長

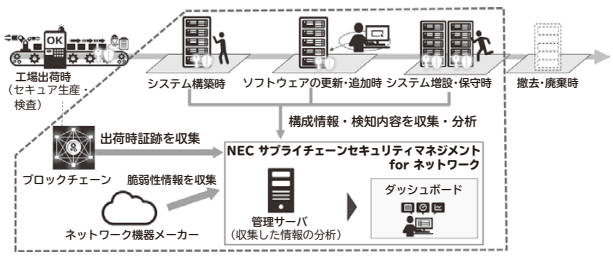

図3　セキュア運用の取り組み概要

[*1] 2022年以降に販売したCisco製品。

供しています。出荷時を起点とした証跡情報と、機器本体のセキュリティ情報を収集し、ネットワーク機器メーカーが持つセキュリティ情報を統合して機器状態を分析・可視化することで、安全かつセキュアな運用環境を支援します（**図3**）。

4.1 対象機器の真正性情報を管理

運用において、工場検査から運送中・構築時に改造などの不正が行われるリスクがあり、対策を取らないと不正な機器を使い続けることになります。この課題を解決するため、管理ツールは工場出荷時におけるセキュア生産・検査の証跡情報を取得、運用中の製品識別情報との照合も可能です。また、納品後のネットワーク機器でも、起動のたびにセキュアブートが動作し、機器の真正性が担保されます。このような仕組みにより、正しく検査・管理された機器を運用していることをお客様自身で確認できます。

4.2 脆弱性情報の収集と抽出

ソフトウェアバージョンや機種ごとの脆弱性情報をすべて調査するためには、膨大なコストが掛かります。多くのネットワーク機器を導入していると、十分に管理がされず、脆弱性の対処が行き届かない機器が残存する可能性があります。本製品では、ネットワーク機器メーカーとの連携により、公開されている脆弱性情報を収集し、管理ツールで可視化します。CVE番号、アドバイザリーID、CVSSのスコアなど、さまざまな要素から脆弱性情報が検索可能なため、早期の対策検討に役立ちます。また、収集した管理対象機器の情報をもとに、該当する脆弱性情報の自動抽出が可能です。それにより、保有機器の脆弱性情報が確認しやすくなり、対処が必要な脆弱性を簡単に絞ることができます（**図4**）。

図4　脆弱性情報の抽出イメージ

図5　設定変更の差分表示イメージ

4.3 トレーサビリティの強化

ネットワーク機器に対し、いつ誰が何をしたかの管理ができていない場合、インシデント発生時の調査には多くの時間が必要になります。更に、エビデンス不足により調査自体が十分にできない可能性もあります。本製品では、定期的に運用中機器から情報を収集し、機器構成や設定情報に変更があった場合には変更情報を提供します（**図5**）。これにより、管理者は意図した変更かどうか検知した変更情報を確認することで、不正攻撃に対する早急な対応が可能です。他にも、機器情報としてログイン情報も収集しています。ログイン履歴により、いつ誰が何をしたのか可視化することで、内部からの不正利用の機会を減らすことにつながります。これらの仕組みにより、運用可能なコストでの管理を可能にし、インシデント発生時にはこれらの情報をもとに状況把握が簡単に行えます。

5. むすび

本稿では、NECが取り組むサプライチェーン管理強化について紹介しました。本取り組みでは、工場出荷時における真正性確保を目的としたセキュア生産・検査の施策と、セキュリティリスクを自動検知するセキュア運用によりライフサイクルを通した安全なネットワーク機器を提供します。

今後は対象となるネットワーク機器メーカーを拡大し、またお客様の課題解決の取り組みを発展させることで、セキュアなネットワーク管理を実現します。本取り組みを通じ、通信を担うネットワーク機器をセキュアに保つことで、安全・安心な社会の実現に貢献していきます。

参考文献

1) 内閣サイバーセキュリティセンター：「政府機関等のサイバーセキュリティ対策のための統一基準群」，2021.7
https://www.nisc.go.jp/policy/group/general/kijun.html
2) 内閣サイバーセキュリティセンター：政府機関等の対策基準策定のためのガイドライン（令和3年度版），2022.12
https://www.nisc.go.jp/pdf/policy/general/guider3_2.pdf
3) 内閣サイバーセキュリティセンター：重要インフラのサイバーセキュリティに係る行動計画，2022.6
https://www.nisc.go.jp/policy/group/infra/siryou/index.html
4) Cisco：Cisco Trustworthy技術 データシート，2019
https://www.cisco.com/c/dam/global/ja_jp/about/doing_business/trust-center/docs/trustworthy-technologies-datasheet.pdf

執筆者プロフィール

曽根 泰斗
デジタルネットワーク統括部

勝田 将史
NECプラットフォームズ
アクセスソリューション事業部
エキスパート

野出 利緒
デジタルネットワーク統括部
プロフェッショナル

安達 智雄
デジタルネットワーク統括部
ディレクター

関連URL

NECサプライチェーンセキュリティマネジメントforネットワーク
https://jpn.nec.com/scrm/index.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