ネットワークエッジで実現するIoTリアルタイムセキュリティ脅威検知システム

土江　康太　　八百　健嗣

近年、IoT機器を活用したソリューションが拡大し、IT機器が直接接続される末端領域（ネットワークエッジ）に多種多様な機器が接続されるようになった。一方で、脆弱（ぜいじゃく）なIoT機器を踏み台として組織内部に不正侵入される事例が問題となっている[1)]。例えば、モバイル通信機能を備えたIoT機器がオフィスのLANに無断接続され、外部回線を介して社内ネットワークに侵入され機密情報が漏洩（ろうえい）した事例がある。

このような問題に対して、OKIはネットワークエッジでIoT機器の通信トラフィックの特徴を分析する技術を用いて、未知の機器や普段と異なる通信の振舞いを軽量かつリアルタイムに検知するシステム（IoTリアルタイムセキュリティ脅威検知システム、以下本システム）を開発している。

本稿では、本システムの概要と機能、及び実証の取組みを紹介する。

セキュリティ脅威増大の背景

ネットワークエッジを起点としたセキュリティ脅威が増加している背景には、IoT機器の利活用拡大による機器管理の複雑化がある。これまでのネットワークエッジでは、従業員のPCが接続され、各PCはエンドポイントセキュリティ製品や資産管理システムなどのエージェント型ソフトウェアを導入することが主なセキュリティ対策であった。しかし、業務効率や生産効率の改善を目的としてIoT機器を利用したシステムの導入により、ネットワークエッジには多種多様な機器が接続されるようになってきた。機器の中には計算資源が乏しくエージェント型ソフトウェアを導入できないものも多く、管理者が全ての機器を把握し管理することが困難になっている。そのため、ネットワークエッジに接続される機器を管理し、不正侵入などによるセキュリティ脅威を検出する対策が必要となっている。

NDRによる対策と既存構成の課題

ネットワークエッジのセキュリティ対策としてNDR（Network Detection and Response）がある。NDRは、ネットワークスイッチのミラーリング機能で通信トラフィックをキャプチャーすることで接続されている機器を把握し、各機器の通信の振舞いから不正通信を検出する。不正通信の検出方法として、機器の普段の通信パターンを機械学習し、通信パターンが異なる場合に情報漏洩やマルウェア感染拡大などの異常と判断する方法がある。またNDRは、機器にソフトウェアを導入する必要が無いため、IoT機器のセキュリティ対策として有効である。

NDRのシステム構成として、ネットワークエッジに通信トラフィックをキャプチャーする装置を置き、キャプチャーした結果をクラウドサーバーで分析する構成がある。しかし、このような構成では、各ネットワークエッジからクラウドサーバーに大量のトラフィックデータが送信されることになるため、通信帯域を圧迫し通常業務の通信に影響を及ぼす恐れがある。またトラフィックデータ送信と結果通知の往復伝搬遅延が発生するため、不正通信の検出・対処に時間を要する。そのためエッジで分析までする構成が望ましいが、各エッジに高スペックな分析装置を配置する必要があり、価格面や設置場所確保などの課題があった。

そこで、前述した既存NDRの課題に着目し、計算資源の限られたエッジ装置でもネットワークエッジのトラフィックをリアルタイムに分析しセキュリティ脅威を検出する、セキュリティ脅威検知システムの研究開発に至った。

提案システムと研究目標

提案するシステムは、エッジ装置上で通信トラフィックをキャプチャーして分析しネットワークエッジのセキュリティ脅威を検出する。本システムのエッジ装置は、AI分析処理を高速に実現するOKIのAIエッジコンピューター「AE2100[2)]」を用いる。本システムの接続構成を図1に示す。AE2100は、監視対象ネットワークスイッチのミラーポートに接続し、スイッチを流れるトラフィックをキャプチャーする。またAE2100は、監視対象ネットワークの通信ポートにも接続することで、監視対象機器に対して脆弱性検査なども可能となる。

本研究では、上述の構成でトラフィックを実時間処理しセキュリティ脅威をリアルタイムに検知する異常検知機能を開発することを目的とする。

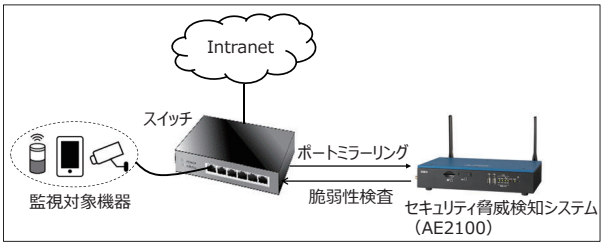

図１　システム接続構成

解決すべき技術課題と解決方針

本システムを実現する上での技術的な課題は、計算資源の限られた装置で通信トラフィックをリアルタイムに分析することにある。この技術課題の解決方針として以下二つを掲げている。

一つ目はパケットのヘッダー情報のみを用いて分析することである。従来のパケットのペイロードまで分析する手法では、通信内容を詳細に把握できる一方、処理負荷が大きくエッジ装置での分析が困難である。パケットのヘッダーだけで分析する手法では、分析に用いることができる情報は限られるため異常検知の難易度は高いが、軽量に分析できる。このような軽量な分析を実現するため、少ない情報量でトラフィックを分析する技術を大学と共同研究し、本取組みに応用している。

二つ目は、AIを活用した分析をハードウェア上で実行できる、VPU（Vision Processing Unit）を用いて分析することである。AI分析では、深層学習を用いることにより高度な分析ができる場合が多い。一方深層学習は、処理負荷が大きいため、リアルタイムに流れるトラフィックを分析する場合は高スペックな装置を用いる必要があった。VPUは、ディープラーニングの推論処理に特化したハードウェアであり、エッジ装置でもディープラーニング推論処理を高速実行できる。本システムでは、AE2100に搭載されたVPUを利用することによりエッジでのリアルタイム分析を実現している。

次章では、以上の解決方針の下で開発した異常検知機能を説明する。

異常検知機能

本システムは、機器接続時と機器運用時に対して2種類の異常検知機能をもつ。

（1）機器接続時の異常検知機能

機器接続時の異常検知機能は、機器がネットワークに接続された時に検疫的に実行される機能である。具体的には、意図しない機器が接続されたことを検出する不正端末接続検知機能と、接続された機器が脆弱性をもっていることを検出する脆弱性検知機能からなる。これらの検知機能を実現するための要素技術として、接続された機器の機器種別を識別する機器種別判定技術を大学と共同開発した[3)]。以下では、まず機器種別判定技術を説明し、その後各異常検知機能を説明する。

機器種別判定技術の特徴は、通信フロー先頭200パケットのヘッダー情報のみを用いて複数種類の機器種別を判定するところにある。機器種別を識別するイメージを図2で説明する。図2では、ネットワークカメラとスマート電源プラグの通信パターンを、横軸を通信パケットの発生タイミング、縦軸を通信パケットのサイズで表している。ネットワークカメラの通信パターンは、PCなどからカメラに接続するための制御パケットが発生し、その後カメラからの映像伝送のストリーム通信が発生する。またスマート電源プラグは、プラグ接続時の制御パケットの発生後、電源のON/OFFを切り替えるパケットが不定期に発生する。機器種別判定技術ではこのような機器種別特有の通信パターンを学習している。機器種別判定技術を活用することで、後述の不正端末接続検知機能を実現し、脆弱性検知機能の検査時間を短縮できる。

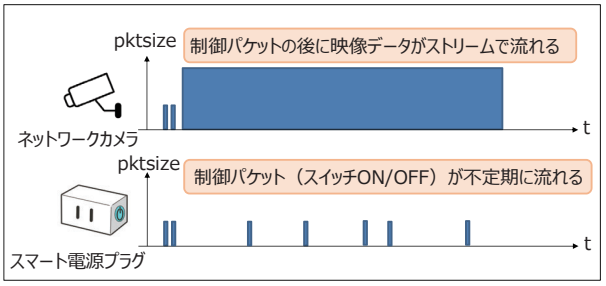

図２　機器種別判定技術

不正端末接続検知機能は、機器種別判定技術でいずれの機器種別の特徴にも似ていない通信パターンを持つ機器を未知の機器種別として判定する機能である。未知の機器種別と判定された場合、不正な機器が接続されたと判断する。

脆弱性検査機能は、機器がもっている脆弱性を検出する機能である。具体的には、機器に対して不要なTCP/UDPポートが開放されていないか確認するポート検査と、開放されているポートが平易なID/PASS（パスワード）で接続できる状態にないかを総当たり的にリストで確認するパスワード検査を実施する。一般に脆弱性検査は、漏れが無いように幅広い検査項目で実施することが望ましいが検査に時間がかかる問題がある。本機能では、機器種別判定技術の結果を用いて、機器ごとに検査項目を最適化するこ

とで検査時間の高速化を図っている。そのためポート検査では、機器種別によって注意すべきポートだけを検査する。例えば、ネットワークカメラのようなIoT機器では、攻撃を受けやすいtelnetなどのリモート接続ポートやftpなどのファイル転送ポートに限定して検査する。パスワード検査では、機器種別ごとにIDとPASSのリストを用意し検査項目数を削減する。例えばPCであれば、ユーザーが安易に設定しがちなPASSのリストを用いて検査し、IoT機器であればデフォルトのID/PASSでよく使われるリストを用いて検査することで検査項目数を削減できる。

(2) 機器運用時の異常検知機能

機器運用時の異常検知機能では、接続されている機器の通信トラフィックを分析し、内部不正による情報漏洩やマルウェア感染後の感染拡大活動を攻撃通信として検出する。このような事象を検出するために、機器の定常通信パターンを教師無し機械学習し、定常通信パターンから逸脱する非定常な通信パターンを攻撃通信として検出する方法を用いる。従来このようなAIアプローチを用いて通信トラフィックをリアルタイムに分析するには高スペックな装置が必要であり、エッジ装置上では実現が困難であった。しかし近年、深層学習の推論処理を専用に実行するハードウェアとしてVPUが開発され、エッジ装置にも搭載されるようになってきた。本機能はAE2100に搭載されるVPUを活用しネットワークエッジのトラフィックをリアルタイムに分析し攻撃通信を検出する。本機能は研究開発段階にあり、現在は既存研究[4]をベースとした方式をAE2100に実装し、実験ネットワーク環境での評価、及び後述の実証実験で動作・検証している。

これまでの取組みとして、実装した方式がどの程度の通信レートであれば実時間処理可能かを明らかにするため、実験ネットワーク環境で評価した。評価の結果、VPUで動作させた場合に9Mbpsまでの通信レートのトラフィックを実時間処理できることを確認した[5]。現在は、実証先の環境で本機能を動作させ、現状の方式で実運用に耐え得るか検証している。今後は、攻撃通信が検知できる方式の開発に向けて、方式の検知精度を評価する予定である。また、通信負荷の高い環境にも適用できるように、実時間処理できるスループット向上に向けて方式を改良する予定である。

可視化・通知機能

本システムは、異常検知結果をダッシュボード及びレポート出力により可視化する機能を備え、Webブラウザーからアクセスできる。またメール通知機能を備え、脅威の発生を把握できる。

ダッシュボード画面を**図3**に示す。左側の画面では、接続されている機器の情報を確認できる(①)。機器の情報として、IP/MACアドレス、製造ベンダ、機器種別判定技術による機器種別、機器の状態が分かる。機器の状態は、対処の優先度を緊急度によって色分けし緊急度の高い機器が一目で分かる。画面右側では機器ごとの詳細情報を確認でき、機器の通信量や異常検知数の時系列推移(②)、異常検知結果の詳細情報や通信先情報(③)などが確認できる。

図3　ダッシュボード画面

実証の取組み

最後に本システムの適用例として、現在我々が進めている実証の取組みを2件紹介する。

(1)サイバー分析支援ソリューション

サイバー攻撃への対策は、インターネットとの境界となる出入口対策だけでなく、各拠点への侵入や内部不正者によって引き起こされる攻撃に対処するためのネットワーク内部での対策も求められている。OKIのお客様である中央省庁もその一つであり、現在中央省庁内部の専用ネットワークに本システムを設置し、異常検知機能の検知性能を評価している。実験の様子を**図4**に示す。本実証の目的は、主に機器運用時の異常検知機能の有効性評価である。業務時間外にファイルサーバーから異常なダウンロードトラフィックを発生させ、マルウェアの感染拡大を模擬したトラフィックを発生させるなどして、それら事象が通信の振る舞いから検知できるかを検証している。

図4　中央省庁内部ネットワーク監視実験

(2)工場内ネットワーク監視

昨今、サイバー攻撃の対象は工場内の設備機器にも拡大している。社内PCのマルウェア感染を起点として、工場内の設備がつながるネットワークに侵入され、一時操業停止にまで発展する事例も発生している。そこでOKI社内工場に本システムを設置し、機器接続時の異常検知機能により、工場内の資産や脆弱性を可視化し、マルウェア感染拡大などの脅威を未然に防止できるかを評価中である。実際に本システムを設置することで、工場内のネットワーク機器の通信状況が明らかになり、ネットワーク機器の想定外の通信や、想定していなかった接続機器の設定状況が明らかになった。本実証の目的は主に工場内ネットワーク監視の実運用面での課題抽出である。今後は社外にも実証のフィールドを拡大しつつ、抽出された運用課題をシステム開発にフィードバックしていきたい。

まとめ

本稿では、ネットワークエッジのセキュリティ脅威を検出するIoTリアルタイムセキュリティ脅威検知システムを紹介した。本システムは、パケットヘッダーを用いた軽量なトラフィック分析と、VPUを活用したAI処理により、計算資源の限られたエッジ装置上でもリアルタイム性の高いセキュリティ監視を実現するものである。

今後は、実証で得られた知見をもとに、現検知機能の改良、及び新規機能を開発し、現場での運用課題を解決できるシステムへ改修していく。

謝辞

本稿記載のシステム搭載機能の一部は、大阪市立大学の阿多信吾教授との共同研究により開発したものです。ここに謝意を表します。

◆◆

■参考文献

1)BBC News,Raspberry Pi used to steal data from Nasa lab,24 June 2019 https://www.bbc.com/news/technology-48743043,(21 Feb. 2022).

2)島田貴光:高速ディープラーニング推論処理をエッジで実現するAIエッジコンピューター「AE2100」、OKIテクニカルレビュー 第234号、Vol.86 No.2、pp.16-19、2019年12月.

3)H. KAWAI et al.:Identification of Communication Devices from Analysis of Traffic Patterns, Proc. 13th International Conference on Network and Service Management (CNSM 2017), Japan, 2017.

4)T.D.Nguyen et al.:"DÏoT:A Federated Self-learning Anomaly Detection System for IoT",Proc. 39th IEEE International Conference on Distributed Computing Systems (ICDCS2019), Jul, 2019.

5)土江他:ネットワークエッジにおけるリアルタイムセキュリティ異常検知システムの実装評価、信学技報、vol.121、No.434、IN2021-31、pp.1-6、2022年3月.

●筆者紹介

土江康太:Kota Tsuchie. イノベーション推進センター ネットワーク技術研究開発部

八百健嗣:Taketsugu Yao. イノベーション推進センター ネットワーク技術研究開発部