医療機関における エッジネットワーク監視システムの実証実験

田中　俊哉　　藤田　幸愛
中村　信之

昨今、企業や医療機関のシステムがサイバー攻撃によって大きな被害を受ける事例が増加している。2022年には、900床を超える医療機関がサイバー攻撃被害を受け、基幹システムサーバーの大部分をランサムウェアにより暗号化される事件が発生した。その影響で被害に遭った医療機関は救急診療を10日間、新規入院を約50日間停止した。さらに復旧に全てのサーバーと端末のクリーンインストールを要したため、全ての業務システムの復旧には73日間を要した[1),2)]。

2023年には事件の重大さを受け、厚生労働省は「医療情報システムの安全管理に関するガイドライン 第6.0版[3)]」を策定した。ガイドラインでは、医療分野及び医療情報システムに対するサイバー攻撃の一層の多様化・巧妙化が進み、診療業務に大きな影響が生じていることを踏まえて、医療機関に求められる安全管理措置を中心に内容を見直し、対策を推奨している。このように、医療現場におけるサイバーセキュリティ対策は急務となっている。

医療機関では、インターネットに直接接続しない閉域ネットワークで電子カルテや医療機器を運用している。閉域ネットワークは医療機関に限らず数多くの組織で運用されており、セキュリティ対策ニーズが存在する。そのためOKIでは閉域ネットワークに対する侵入監視・検知に関する研究開発を行い、エッジネットワーク監視システムとして開発している。

本稿では、エッジネットワーク監視システムの概説と、医療機関との実証実験の状況、今後の展開について述べる。

背景

従来、閉域ネットワークはインターネットに接続されていないためサイバー攻撃の脅威がない環境とされていた。しかし近年では閉域ネットワークに対しても、VPNやルーターなどのネットワーク機器の脆弱性やパスワード漏洩などから侵入するサイバー攻撃事例が増加している[4)]。

前述の事例に限らず、多くの医療機関のシステムの閉域ネットワークがサイバー攻撃の標的になり、実際にランサムウェアによってデータが暗号化され、電子カルテなどの情報が使えなくなるなど深刻な障害を受ける事件が発生している。また、ネットワークの運用や脆弱性検査などのセキュリティ監視には、少数の担当者しか従事できないなど、対策に不安が残る現場も多く存在する[5)]。このような背景を受け、次章でOKIが開発しているエッジネットワーク監視システムについて述べる。

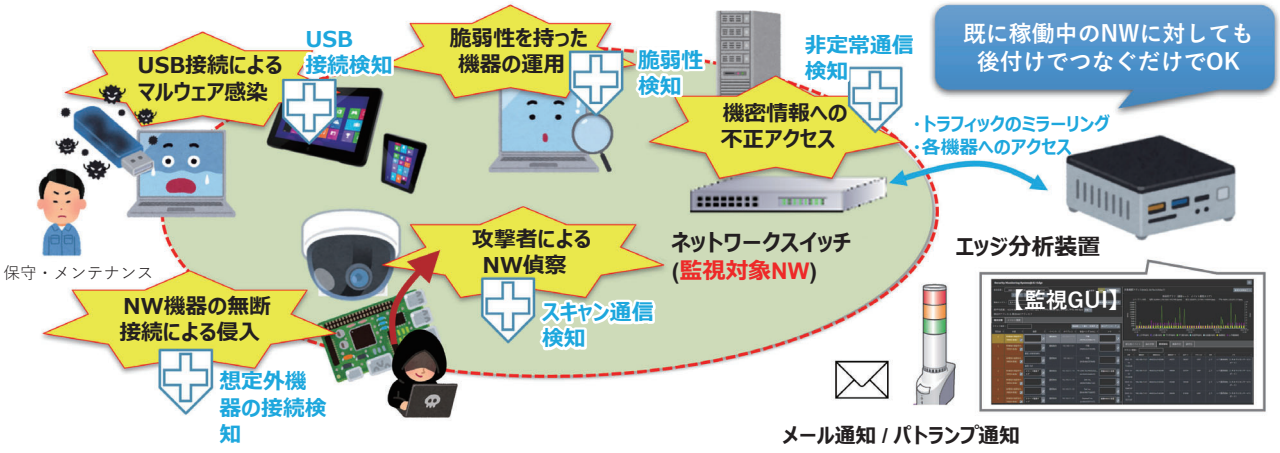

図 1　エッジネットワーク監視システム接続図

システム紹介

OKIが開発しているエッジネットワーク監視システムは、閉域ネットワーク内のトラフィックをリアルタイムで監視しセキュリティ脅威を検出する[6]。具体的には、通信トラフィックをキャプチャーしてリアルタイムに分析し、外部からの侵入試行の形跡や、普段と異なる通信状況、不明な端末の新規接続などを検出する。

本システムの機能検討にあたり、医療機関に閉域ネットワークの運用方法とその課題をヒアリングした。医療機関のシステム環境は、医療機器などでOSのアップデートが困難なものがあることや、医療機器でソフトウェアをアップデートするために専用の認定取得が必要となるものがあり、ウイルス対策ソフトなどエンドポイントセキュリティ製品の導入も困難である。こういった環境では最新のセキュリティ対策が困難になり、侵入の被害を受けやすい環境になっていることがわかった。

本システムでは、監視用ソフトウェアのインストールやネットワークの設定変更を不要とし、監視先のネットワークスイッチに小型装置を接続するだけで導入可能としている。本システムの接続図を図1に示す。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や軽量な深層学習モデルを用いることで、エッジ装置上で完結した動作を実現している。

また運用上の課題として、ネットワーク接続されているIT機器の把握やネットワークの実態把握に苦慮するところも多く、医療関係者の私物のUSB機器やPCが医療現場の閉域ネットワークに無断で接続されマルウェアに感染してしまう事例もあった。そこで本システムでは、IT機器の可視化機能、未許可機器の遮断機能を搭載し、不明な機器の接続に対処する。また昨今のランサムウェア被害では、ネットワーク機器の設定が脆弱な状態であることを把握しきれず侵入口にされる事例が多発していることから、脆弱機器を発見し、通知する機能を搭載する。さらに、実際にセキュリティインシデントが発生した際には、専門会社が過去の通信状況を調査して侵入経路や被害の範囲を特定できるようにするため、通信ログの記録機能を備える。

機能紹介

本章ではエッジネットワーク監視システムの代表的な機能を紹介する。

(1) IT機器の可視化

ネットワークに接続されている機器の種別[7]を自動で識別し、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である。

ダッシュボードはWebブラウザーからアクセスできるため、新たにソフトウェアを追加することなく機器を監視できる。加えて、メール通知やパトランプ通知機能を備えているためセキュリティ脅威の発生をいち早く把握できる。本システムで検知・識別した機器リストをWeb上のダッシュボードにまとめたものを図2に示す。

図2の左列より、発生した通信イベントの緊急度、システムで識別した通信の状態、識別した機器、発生した通信イベントの詳細説明、IPアドレス、メーカーを示している。機器の識別と通信の状態は、IPパケットのヘッダー情報のみを解析することで推定している。本システムで取得・解析した結果は、図中右上のダウンロードボタンよりCSVフォーマット形式にまとめられファイルへ出力できるため、ネットワークに接続している機器の棚卸や所有者が不明な機器の把握ができるため、ネットワーク管理者の管理へ寄与できる。

図２　エッジネットワーク監視システム GUI

(2) 未許可機器の遮断

ネットワークに未承認の機器が新たに接続されたとき、ネットワーク管理者がその機器の安全を判断できるまで、機器をネットワークから遮断する機能である。

新規機器を検知した際にまず遮断して確認するなどの、ネットワークごとに遮断のルールをあらかじめ設定しておくことで、未承認機器を自動的に遮断することができる。

機器の通信遮断は、ネットワークスイッチの遮断機能に依存しない、プロキシARPを用いた方法で実現している。プロキシARPは、機器のARP要求に対して本来の問い合わせ先の代理でARP応答をする機能である。本システムは、プロキシARPを用いて、該当機器の通信を妨害し通信が成立しない状態を作ることで、通信遮断された状態にする。

(3)不正侵入検知

ネットワークに新規の機器が接続したときや、すでにネットワークに接続されている機器に対して、不正侵入を検知するための機能である。本システムでは複数の不正侵入検知機能を持ち、環境に応じて適切な検知をできる工夫をしている。不正侵入を検知するための手法として、本節では深層学習を用いた方法と通信の振る舞いから検知する方法について述べる。

深層学習を用いた検知手法では、定常時の通信フローデータの通信パターンを用いてオートエンコーダによる異常検知モデルを構築する[8]。構築したモデルを用いて、普段と異なる通信パターンを検知することで、既知の不正侵入だけでなく未知の不正侵入を検知することを目指している。

通信の振る舞いを用いた検知手法では、普段の機器ごとの通信先数をあらかじめ計算するなど統計処理による学習を行い、普段の通信から逸脱した通信を不正侵入として検知する[9]。この手法は、機器ごとの通信先数をリアルタイムに集計するため、不正通信が発生してから検知するまで短時間で検知することが可能である。

(4)脆弱機器の発見

ネットワークに接続されている機器に対して、本システムから検査パケットを送信し、脆弱な状態にある機器を把握するための機能である。

具体的には、機器に対して不要なTCP/UDPポートの解放の有無を検査するポート検査と、開放されているポートが平易なID/パスワードで接続可能な状態にあるかを検査するパスワード検査を実施する。

ポート検査では、SSHやTelnetなどのリモート接続サービスに使われるポートを開放している機器を検知するほか、前回検査時とのポートの開閉状況の差分を比較し、差分がある場合はレポートする機能を持つ。また、パスワード検査では、世の中で使われる一般的なID/パスワードの組を用いてログインが成功するか否かを検査する機能である。

(5)通信ログの記録

本システムで解析する通信ログと解析結果を保存する機能である。保存するデータは、エッジネットワーク監視システムで取得した通信、分析結果、通信量などである。本システムでは保存された情報をダッシュボードからダウンロードできるようになっており、ネットワーク障害が発生したとき、ネットワーク管理者に特定の時間帯のログデータやトラブルが発生している機器情報を提供することで、早期の解決に寄与できる。また、通信ログを記録しておくことにより、万が一のセキュリティインシデント発生時に、侵入経路や、被害の範囲を特定しやすくなり、対処計画の立案に寄与する。

実証実験の経過背景

現在、実環境の運用を通して、価値の検証と課題を抽出することを目的とし、複数の医療機関でエッジネットワーク監視システムの実証実験を実施している。パートナーである医療系ネットワークの運用保守会社と協力し、本エッジネットワーク監視システムを用いたセキュリティ監視を数ヶ月にわたって試験運用した。

試験運用を通して各機能を改修すると共に、ネットワークに接続された未許可の機器の通信を遮断する通信遮断機能や、サイバー攻撃の侵入口となりうる脆弱性機器を検知する機能が必要であるとの要望を得て、追加機能として実装した。実証実験を通して、システムの利用感や有用性をヒアリングした結果を**表1**に示す。

各機能の価値については、おおむねポジティブな回答が得られた。一方で、運用工数の削減につながるかについては実証先によって既に監視業務をしているかが異なるため意見が分かれた。実際の医療機関の顧客への展開可能性については、医療機関側がITへの投資に積極的でないため予算確保が難しいという組織の現状に関する意見が得られた。

表 1　ヒアリング回答

項目	評価・コメント
IT 機器の可視化	● 通信状況の画面や図表がエビデンスとして有用 ● 接続機器を一覧で把握できるのは助かる ● 新規にネットワークに接続された端末がいつから接続されたのか追跡できることは有用
未許可機器の隔離	● 私物の端末を無断接続される現場もあり、不正な端末の接続などに有用
不正侵入検知	● 普段と異なる通信が頻発しているような状況を把握できることで、事前対策がしやすい
脆弱機器の発見	● 既知の脆弱性を侵入口とするサイバー攻撃の事例が多いことから、重要
運用工数削減	● 従来手作業の業務の半自動化 ● 従来監視を導入していない環境では監視工数が新たに発生
展開可能性	● リースなどで低価格に抑えられれば嬉しい ● 医療機関は IT 投資に後ろ向けで NDR 製品の展開が難しい

運用工数の削減に向けて、ネットワークセキュリティの知識に乏しい担当者でも少ない工数で確実にセキュリティリ

スクに対応できるよう、機能拡充していく。セキュリティ対策への投資が積極的でない現状については、ガイドラインの発行や補助金制度のような国の政策も踏まえつつ、実証実験により導入の容易性や運用可能性を体感いただけるよう引き続き提案していきたい。

まとめ

本稿では、医療機関内の閉域ネットワークにおけるサイバー攻撃被害やセキュリティ脅威について示し、OKIが開発中のエッジネットワーク監視システムの概説と、実際の医療機関での実証実験の状況について述べた。

今後も実証実験を通して、社会への影響が大きいネットワークへの侵入やサイバー攻撃に有効な監視・検知技術を製品化し、社会実装を進めていく。 ◆◆

■参考文献

1）大阪急性期・総合医療センター 情報セキュリティインシデント調査報告書 概要 2023.3.28 調査委員会
https://www.gh.opho.jp/pdf/reportgaiyo_v01.pdf
2）病院に逸失利益が数十億円規模の影響与えたランサムウェア攻撃の実際と対応策
https://dcross.impress.co.jp/docs/column/column20240314/003608.html
3）医療情報システムの安全管理に関するガイドライン 第6.0版（令和5年5月）
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html
4）Fortinet製 FortiOS SSL VPN の脆弱性対策について (CVE-2024-21762)
https://www.ipa.go.jp/security/security-alert/2023/alert20240209.html
5）徳島県つるぎ町立半田病院 コンピュータウイルス感染事案有識者会議調査報告書について
https://www.handa-hospital.jp/topics/2022/0616/index.html
6）土江康太、八百健嗣：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、OKIテクニカルレビュー 第239号、Vol.89 No.1、pp.24-27、2022年5月
7）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.
8）土江康太、中村信之、八百健嗣：エッジ分析で実現するリアルタイムセキュリティ異常検知方式の実装評価、電子情報通信学会、vol.122、IN-407、pp.247-252（IN）、2023年2月23日（IN）
9）田中俊哉：閉域ネットワークにおけるスロースキャン通信検知方式の検討、信学技報、vol.124、no.124、ICSS2024-22、pp.66-72、2024年7月

●筆者紹介

田中俊哉：Shunya Tanaka. 技術本部 先行開発センター モビリティIoT先行開発部
藤田幸愛：Sachia Fujita. 技術本部 先行開発センター モビリティIoT先行開発部
中村信之：Nobuyuki Nakamura. 技術本部 先行開発センター モビリティIoT先行開発部