ケーブルテレビ事業者に適した注目ソリューション

NTTコミュニケーションズ

OT環境向けセキュリティ対策「OsecT」既存システムに影響を与えずネットワーク可視化・セキュリティリスク検知

1990年代後半から急速な拡大を見せてきた通信ネットワークにおいて、常に必要性が指摘されてきたセキュリティ対策。IT分野においては発展とともにセキュリティ対策も向上したが、安定運用が最優先されるOT（Operational Technology）分野では、ソフトウェアの未更新・サポート切れを含めやや置き去りにされてきた感がある。NTTコミュニケーションズが提供するOT環境のネットワーク可視化・セキュリティリスク検知ソリューション「OsecT（オーセクト）」は、そんな生産現場の安定業務を妨げることなく、セキュリティ対策を一気に進めることができる優れたソリューションだ。現在、ケーブルテレビ事業者が市場拡大に注力している地元製造業などB2Bの顧客のOT環境へ、簡単にサイバーセキュリティを提供できるソリューションとして適している。

（取材：渡辺 元・本誌編集長、文：高瀬徹朗・ITジャーナリスト）

OT環境におけるセキュリティの課題を解消

「OsecT」は、生産現場などにおける既存のOT環境に接続することでネットワークを可視化し、サイバーセキュリティの脅威・脆弱性を検知することができるNTTコミュニケーションズの独自開発サービス。OsecTセンサーを工場内などに設置されているスイッチのミラーポートに接続するだけで利用可能で、工場の生産ラインなどの業務に一切の影響を与えることなく簡単に導入することができる。

「WindowsやLinuxなど汎用的なソフトウェアを通じてネットワークと接続する以上、IT環境でもOT環境でもセキュリティの課題は同様で、脅威度にも変わりがありません。一方、OT環境においては安定稼働が最優先となるため、システム全体に影響を及ぼしかねない安易なセキュリティ対策は打ちづらい。そこで我々が独自開発したのが『OsecT』です」（NTTコミュニケーションズ株式会社 イノベーションセンター テクノロジー部門 担当部長 加島伸悟氏）。

スイッチのミラーポート設定は必要だが、OsecTセンサーを物理的に接続するだけで利用可能。既存機器へのソフトウェアインストールも不要で、あくまでコピーしたトラフィックデータを監視する形式だ。OsecTセンサー本体に差し込むUSBドングルにはSIMカードが搭載されており、OsecTセンサー本体とOsecT SaaS環境間のデータアップロードは閉域網の無線通信回線を確立。既存設備のネットワーク利用はなく、新たなネットワーク工事も不要な仕組みとなっている。

「見える化」と多彩な検知機能

機能は大きく2点。1点目は、OT環境のネットワークの「見える化」だ。OT環境のネットワーク状況を視覚的に把握し、手元のPCからWebポータル画面でネットワーク状況を可視化したレポートを確認することができる。「OT環境は端末や機器が管理されておらず、現状を把握しづらいのが難点。ネットワーク内の端末状況を可視化することで、脆弱性などを含む現状を正確に把握することができるようになります」（加島氏）。

NTTコミュニケーションズ株式会社 イノベーションセンター テクノロジー部門 担当部長・加島伸悟氏とOsecTセンサー工場などのスイッチのミラーポートに接続するだけで利用可能。「OsecT」のSaaS環境には、本体に差し込まれたUSBドングルから閉域網の無線で安全に通信できる

OsecTセンサーが取得したトラフィックデータから自動で端末を一覧化し、その接続数やトラフィック量が多い端末を一目で把握できるようになる。一覧化したデータはCSVで出力可能で、OTネットワークの傾向把握にもつながる。OTネットワークを視覚的に把握することは、資産管理や重要度の高い端末の特定にもつながるため、セキュリティ対策強化や有事の対応にも役立てることができるだろう。

２点目は、セキュリティ上の脅威や脆弱性を予防・早期発見するための検知機能だ。ネットワーク内に存在する端末情報を自動的に学習し、野良端末などの接続を見逃さずに早期発見。また、サポート切れ OS を利用する端末も自動検出し、アップデート漏れなどの状況を防止する。

マルウェア感染などの異常が発生した場合においては、トラフィック量の増加や定常業務ではない通信の発生などの挙動を検知・アラート通知することで、早期対応や影響の極小化を推進。「システムに影響を与える可能性のある OT プロトコルの通信を検知する OT 振る舞い検知機能、既知の脅威にマッチした通信を検知するシグネチャー検知機能など、複数の検知機能で迅速な異常発見が可能です」（加島氏）。

容易な設置性と価格面に強み

日本でも海外製品を中心に、OT 環境におけるセキュリティ対策の導入も徐々に進んできてはいるが、その重要度や認識の割には導入が進んでいない。「OsecT」は、その導入障壁をクリアできるソリューションだ。

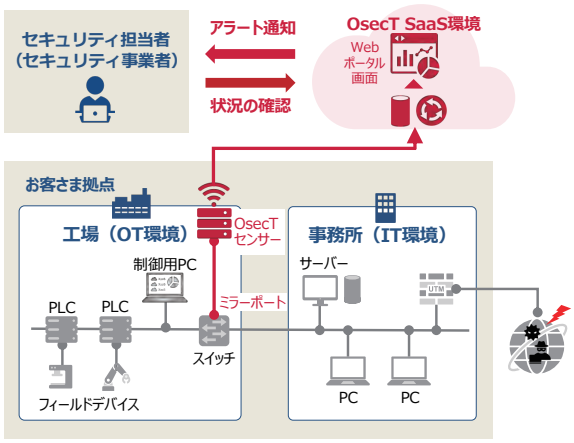
まず、前述した「設置の容易性」だ。既存システムに介入しない仕組みはもちろん、OsecT SaaS 環境へのデータアップロードは閉域網を使用、 新規にネットワークを構築する必要がないなど、設置のハードルが極めて低い。他社製品はセキュリティベンダーの SOC（Security Operation Center）との接続時に VPN を利用するものが多く、インターネット越しにサイバー攻撃を受ける可能性がある。セキュリティ対策を導入するのに、新たにセキュリティリスクが生じる結果になる。それに対して「OsecT」は、OsecT センサーと OsecT SaaS 環境間のネットワークは NTT コミュニケーションズが管理する閉域網なので、インターネット経由の攻撃リスクに対策を打つ必要がない。

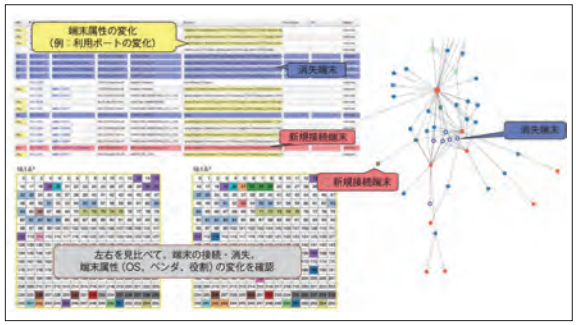
導入障壁の低さという意味では、価格面も大きな武器だ。初期費用 25万円、月額料金は一桁万円代という価格帯は、他社の OT セキュリティ対策と一線を画している。「元々、中小規模の事業者に向けて開発した製品。OT ネットワーク機器を管理するのに必要な機能に特化した製品として自社開発したため、かなりコストが抑えられています」（加島氏）。

Web ポータル画面の UI やサポート体制を含め、国内企業ならではの強みもある。「直近では、パートナー企業を通じて民放キー局にもご活用いただきました。IP化が進む放送機器へのサイバーセキュリティの脅威・脆弱性を検知するため導入されたようです。信頼性という点において、確かな評価をいただけていると考えています」（加島氏）。

導入においては最低使用期間を設けていないため、例えば最短１カ月での使用も可能な仕組みだ。「現場のニーズが高いネットワークの見える化をとりあえず実施し、現状のネットワーク環境を把握チェックする、という利用パターンもありました。定期的にネットワーク環境を可視化して把握するだけでも、セキュリティ対策の一環として十分に機能するケースもあるようです」（加島氏）。

【図】「OsecT」は工場の制御システムに
影響することなく簡単に導入できる





OT 環境の時間差分を分析し、「見える化」した「OsecT」の画面

こうした「見える化」の高い機能性から、「見える化」のみに機能を絞った「OsecT Lite（仮称）」のリリース準備も進んでいるそうだ。月額料金はさらに減額される見通しで、文字通りライトに導入できるようになる。

地域 DX の初手として

放送事業者の導入事例が出たことからもわかるとおり、システムの可用性を重視し、セキュリティ対策が困難で運用に影響を与えない範囲に限定せざるを得ないなどの制約は、放送局やケーブルテレビ事業者にも当てはまる。

一方、スマート化の進展とともに、システムの継続運用とセキュリティの両立という課題が顕在化している生産現場などへの導入という本来主旨から考えれば、ケーブルテレビ事業者が進める地域 DX の一手としても活用できるだろう。

実際、NTT コミュニケーションズでは専門性のある事業者による現場サポート対応を含めたパートナー販売も採用しており、今後の普及において「業種ごとに強いパートナーがいる形が理想的」（加島氏）としている。

設置面、コスト面など導入に向けた障壁は極めて低く、必要性は極めて高い OT 環境へのセキュリティ対策。地域 DX の初手として「OsecT」を活用するのはアリかもしれない。

■「OsecT」の製品紹介ページはこちら
https://www.ntt.com/business/services/security/security-management/wideangle/osect.html