URL https://journal.ntt.co.jp/article/29294
DOI https://doi.org/10.60249/24093102

すべての人が自らの力で制御機器・危機を管理できる世界へ！ OT/ICSセキュリティリスク可視化サービス OsecT

近年，企業規模を問わず工場などのOT（Operational Technology）/ICS（Industrial Control System）システムが攻撃される事例が増えており，セキュリティ対策が急務な状況です．その中でNTTコミュニケーションズでは，OT/ICSセキュリティリスク可視化サービス「OsecT」を提供しています．本稿では，本サービスでの私たちのアプローチやユーザニーズに寄り添った機能・サービス展開，そして今後の展望を紹介します．

取り組む社会課題と私たちのアプローチ

近年，工場・プラントなどの生産現場や電力・ガスなどの社会インフラが攻撃される事例が国内外で増えています．攻撃の目的としては，金銭目的・製品品質の低下による評判の低下・自らの名声を広範囲にアピールすることなどが挙げられます．このような攻撃が増えてきたことにより，OT（Operational Technology：制御・運用技術）/ICS（Industrial Control System：産業制御システム）セキュリティ対策の必要性が高まっています．

しかしながら，OT/ICSシステム環境とITシステム環境では，優先すべき事項や管理状況が異なるため，既存のITセキュリティの手法をそのまま導入することは困難です．

まず，OT/ICSシステム環境では，制御系システムの安定稼動が第一優先です．セキュリティ対策をした結果，制御系システムへの影響があってはなりません．そのため，OSやアプリケーションの最新化はされていないことが多くなります．また，ランサムウェア対策のソフトウェア〔EDR（Endpoint Detection and Response）等〕を，制御系システム内に導入することも困難です．

次に，制御系システムの現状が把握できていないケースが多いことです．機器の通信状況が分からないため，攻撃されたことも分からない可能性があります．

さらに，中堅・中小企業の場合，セキュリティ対策に十分なコストをかけられない，セキュリティ担当者の不在といったコスト・人材不足の課題もあります．大企業は一定レベル以上のセキュリティ対策は行っていることから直接攻撃することが難しくなりつつあります．そこで，対策レベルが低い中堅・中小企業を攻撃の入り口とし，サプライチェーン全体に影響を与えるようなセキュリティ事故が発生しています．そのため，企業規模を問わず，セキュリティ対策を進める必要があります．

これらの課題に対して，私たちは次のようなアプローチで取り組んでいます（**図1**）．

「制御系システムの安定稼動が第一優先」という課題に対しては，制御ネットワーク内を流れるトラフィックのコピーのみをパッシブに監視・分析し，セキュリティ脅威の予防・早期発見を実現します（検知優先）．既存システムへのソフトウェアインストールなどは不要で，検査通信などをネットワーク内に流すこともないため，制御系システムに影響を与えることはありません．

「制御系システムの現状把握ができていない」という課題に対しては，トラフィックのコピーを分析することで，制御システム内にある機器だけでなく，機器の通信先や通信量，通信サービスなど多様な観点で見える化をしています．

最後に「コスト・人材不足」という課題に対しては，中堅・中小企業でも導入可能な価格帯で提供することと，誰でも簡単に導入・運用できるような設計にしています．特に私たちは，コスト・人材不足でOT/ICSセキュリティに手を出せない，ということを解消できるようなアプローチを重視して，サービスを開発しています．

NTTグループ内製開発によるサービス

私たちが提供するOT/ICSセキュリティリスク可視化サービスOsecT（オーセクト）とは，工場などの制御系システムのセキュ

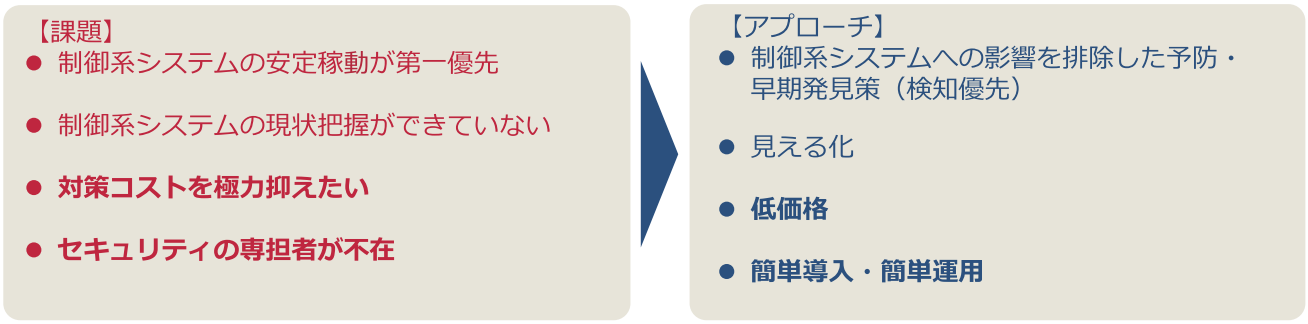

図1　OT/ICSセキュリティにおける課題とアプローチ

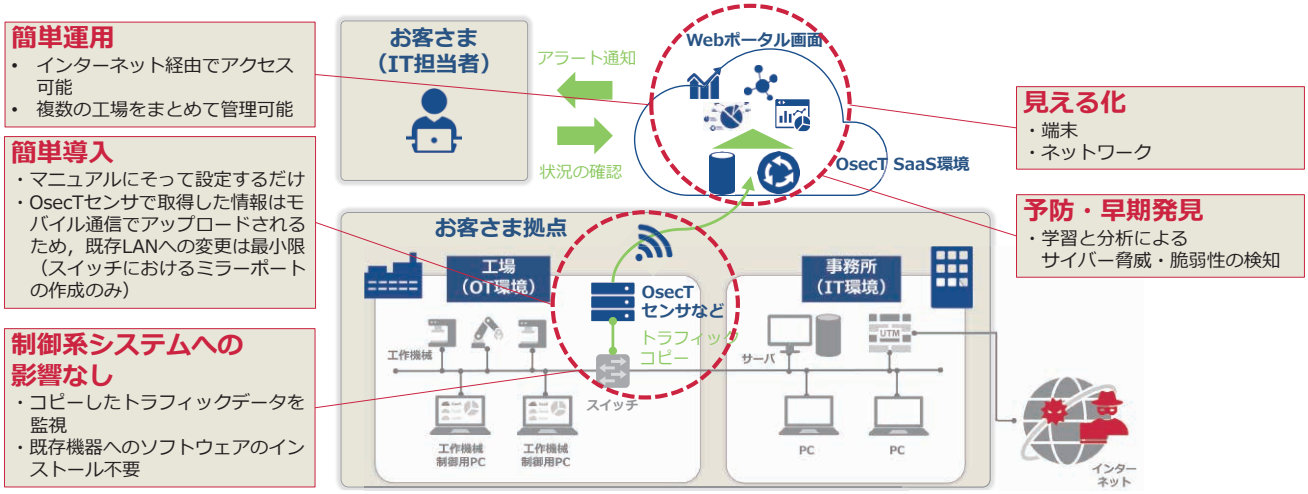

図 2　全体構成図と OsecT の特徴

リティリスクを可視化・検知するサービスです[(1)]．多様化する制御系システムのセキュリティ脅威に対して，トラフィックを解析するセンサ機器をお客さまの工場内に設置するだけで，制御系システムへの影響なく，端末・ネットワークの可視化と脅威・脆弱性検知ができます．これにより，早期にリスク感知できる状態をつくり，工場の稼動停止による損失を未然に防ぐことができます．

OsecTは従来のOT-IDS（OT-Intrusion Detection System：OT環境のネットワーク監視による資産可視化・侵入検知システム）と比較して，いくつか大きな違いがあります（**図 2**）．

1番目は価格が大幅に安価である点です．従来のOT-IDSはセキュリティ有識者が詳細な分析に使うための，高機能かつ高価なサービスが一般的でした．一方，OsecTは機器・ネットワークの可視化やセキュリティ脅威を検知するために，必要十分な機能のみに絞ってソフトウェアを実装しています．また，NTTグループの完全内製開発であるため，従来製品と比較して安価にサービス提供できます．

2番目はすでに稼動している制御系システムのスイッチにLANケーブルを接続し，ミラーリングの設定をするだけで，既存システムに影響を与えず，簡単に導入可能である点です．従来製品ではセキュリティ監視のために，既存のネットワークを改修する必要性があることが多いです．一方，OsecTでは工場に設置するセンサ機器にSIMが搭載されており，工場内を流れているトラフィックをセンサ機器が取得し，必要な情報のみをNTTコミュニケーションズが提供するモバイル閉域網を経由して，SaaS（Software as a Service）環境に送信・分析するため，既存ネットワークへの影響はありません．

3番目は，インターネット経由でSaaS環境に存在するOsecT管理画面にアクセスできるため，お客さまはどこからでも工場の状態を把握できる点です．従来製品ではセキュリティ監視のために，VPN（Virtual Private Network）などを利用して外部からアクセスするケースがあります．しかしながら，セキュリティ監視を目的とした外部から工場へのリモートアクセスが，工場のセキュリティポリシーに抵触するケースがあります．一方，OsecTでは工場へのリモートアクセスは行わず，SaaS環境で一元管理可能です．また，複数の拠点の情報を1つのSaaS環境で確認できるため，運用のハードルも低くなります．

多様なニーズに対応するOsecTシリーズ

OsecTは「すべての人が自らの力で制御機器を管理できる世界を実現する」というプロダクトビジョンを基に，開発・運用・拡販を続けています．そのため，ユーザや営業担当，パートナー企業へのヒアリングを通じてニーズを収集，誰からも求められるようなプロダクト・サービスにしていくことを心掛けています．

現在，WideAngle OsecTに加えて，さまざまなOsecTシリーズを展開中です．

1番目はOsecT Edge（オンプレミス版OsecT）であり，OsecTクラウド環境・分析基盤をお客さま拠点内のオンプレミスサーバに配置するサービスです．この形態ではセンサ・オンプレミスサーバの機種選定からお客さまの要望におこたえできます．例えば，以下のようなニーズがある場合，OsecT Edgeによってニーズを満たすことができます．

・お客さまによって，監視データをクラウドにアップロードすることが許容されない場合
・プライベートSOC（Security Operation Center）を運用しており，社内ネットワークで完結したい場合
・センサ機器設置場所（お客さま工場内など）のLTE（Long Term Evolution）がつながりにくい場合
・センサ機器1台当りのモニタリングポート数を増やしたい場合

2番目は，OsecT Free（期間限定版の無償OsecT）であり，お客さま自身で試用いただくためのサービスです．ソフトウェアをVM（Virtual Machine）形式で提供して，お客さま自身で用意したセンサ機器・オンプレミスサーバに導入してお使いいただきます．例えば，以下のようなニーズがある場合，OsecT Freeによってニーズを満たすことができます．

・お手持ちのサーバなどで，まずは機能を試したい場合
・2024年7月現在サービス提供できていない海外のお客さまが試したい場合

3番目は，OsecT Lite（可視化＋新規端末検知のみのOsecT）であり，可視化に重点を置いた，より安価なサービスです．WideAngle OsecTで提供している機能のうち，可視化と一部の検知機能のみ提供しています．例えば，以下のようなニーズがある場合，OsecT Liteによってニーズを満たすことができます．

・まずは，資産・ネットワークの可視化のみをより安価に行いたい場合
・セキュリティアラートに対して，専門組織やOTセキュリティ対応する十分な知識がない場合

ユーザヒアリングを通じた機能開発

私たちはユーザニーズを踏まえた複数のOsecTの提供形態の実現だけでなく，ユーザヒアリングを継続的に行ったうえで，真に求められる機能追加・改善を継続しています．ユーザヒアリングを通じて開発した機能として，「台帳連携機能」と「アセスメントレポート出力機能」があります．

台帳連携機能は，お客さまがすでにExcel等で資産台帳を持っている場合に，その台帳をOsecTにアップロードしていただくことで，OsecTが取得した情報と連携できるようにします．これにより，OsecTだけでは取得できない情報（例：設置場所）

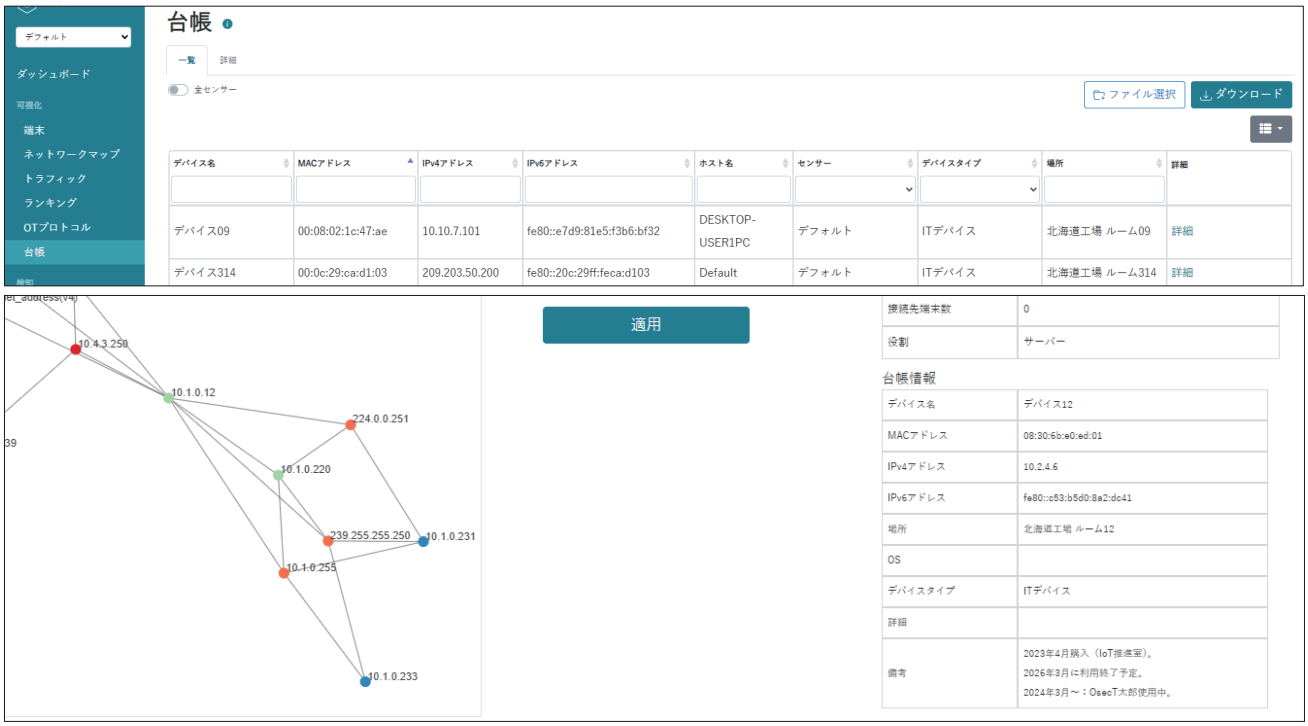

図3　台帳連携機能

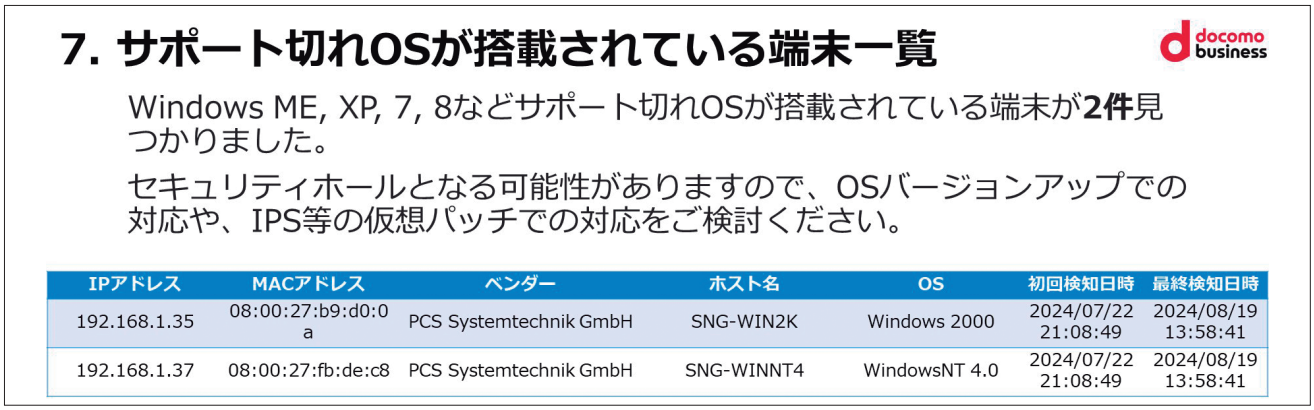

図 4　アセスメントレポート機能

を参照できるようになることや，資産台帳にある資産は検知アラートの対象外にして過検知を防ぐといったことができるようになります（**図 3**）．

アセスメントレポート出力機能は，OsecTで分析した情報をパワーポイント形式で出力します．出力された情報には，お客さまの機器・ネットワークにおいてセキュリティリスクにつながり得る分析内容だけでなく，推奨される対応案も併せて記載します．パワーポイント形式で出力するため，お客さま自身で情報の加筆修正もできます．これにより，セキュリティの専門的知識がなくても，自社の情報セキュリティ部署やB2Bサービスとしてアセスメントサービスを提供する場合のサービス提供先企業に対して，アセスメント結果の提示や状況説明が容易に行えます（**図 4**）．

今後の展望

現在，工場などを有して直接OsecTをご利用いただくお客さまだけでなく，私たちと一緒にOsecTを展開していくパートナーさまも募集しています．また，現在は国内での販売のみですが，アジア・ヨーロッパなどの国外での販売も検討中です．

引き続き，ユーザニーズに寄り添った開発を続けて，お客さまに愛されるプロダクト・サービスをめざしていきます．私たちのサービスに興味を持っていただいた方は，ぜひお問い合わせください．

■参考文献
(1) https://www.ntt.com/about-us/press-releases/news/article/2022/0425.html

◆問い合わせ先
NTTコミュニケーションズ
イノベーションセンター
E-mail　osect@ntt.com