Trellix

SOLUTION BRIEF 翻訳版

Trellix® for Operational Technology (OT) Security

特徴
Trellix for OT Security

- 業界での実績で実証されたソリューションに支えられた、包括的なセキュリティプラットフォーム
- ATMおよびPOSシステム向けでシェアNo.1のセキュリティソリューション
- 世界の公共インフラ(電力・ガスなど)の90%がTrellixによって保護
- 米国の水道システムの75%がTrellixによって保護
- 業界をリードする主要なICS/OTベンダーとの、数十年にわたるパートナシップ

Trellixセキュリティプラットフォームで産業制御システム(ICS)を保護

近年、サイバー脅威の情勢において、ランサムウェアの発生頻度とその影響の大きさが顕著にエスカレートしています。特に製造業やインフラなどの産業企業が標的となっており、操業停止(生産停止)とそれに伴う金銭的損失が発生しています。こうしたランサムウェアの増加により、産業制御システム(ICS)のセキュリティに注目が集まるようになりました。その結果、国際的に規制強化への動き(欧州のNIS2指令、米国のNERC-CIPなど)が加速しており、CISO(最高情報セキュリティ責任者)には制御技術(OT)システムのセキュリティ対策に取り組むことが求められています。

OTシステムは、独自の脅威や規制要件に直面しているだけでなく、従来の企業向けIT環境とは異なるセキュリティアプローチを重視しています。重要インフラ、製造業、医療機関といった「常時稼働」が前提の環境を制御するという性質上、OTシステムは多くの場合、ダウンタイム(停止時間)を最小限、あるいはほぼゼロに抑えて運用しなければならず、可用性(継続稼働)と安全性の確保が最優先されます。こうした背景から、従来の企業向けITとは異なるアプローチが求められます。具体的には、以下のような特有の課題が挙げられます。

- **セキュリティよりも可用性(稼働)を最優先:** 24時間365日稼働する製造現場では、いかなる中断も避けなければなりません。これは、メンテナンス時間の確保(可用性)だけでなく、重大な製造プロセスを自動的にブロックし、結果として停止させてしまうような能動的な検知(アンチウイルスソフトやネットワーク侵入防止システム〈IPS〉による遮断など)を回避することにも当てはまります。
- **セキュリティよりも安全性を最優先:** 製造現場における最優先事項は、従業員の安全確保です。実際の産業制御システム(ICS)のセキュリティ強化に関する取り組みは、通常、二の次の考慮事項となります。

- **製品ライフサイクルの長期化：** IT領域では、約5年周期などで定期的にインフラ機器を刷新することが比較的一般的です。しかしOT領域では、コンポーネントや製造インフラ全体が10年以上のライフサイクルを持つことが珍しくありません。

- **レガシーOSの残存：** 製品のライフサイクルが長いため、OT環境にはMicrosoft Windows NTやWindows XPといった「レガシー（旧式）」とされるシステムが残っていることがよくあります。これらのシステムは、非常に厳格な品質管理（バリデーション）が適用されているため、容易に交換や変更、さらには新しいバージョンへのアップグレードや移行を行うことができません。

- **ICSベンダーの責任と制約：** 産業制御システム（ICS）を構築したベンダーは、使用されているコンポーネントの動作検証を行う必要があり、また独自の要件（システムへのリモートアクセスなど）を設けている場合もあります。産業用部品のポートフォリオは複雑でベンダーによる制約が多いため、ベンダー側での広範なテストが不可欠です。その結果、ICSの脆弱性に対する修正パッチが提供されるまでに、1年以上かかるケースもあります。

- **機器への物理的アクセス：** 多くの製造工場や発電所は、オンサイト（現地）の作業員がアクセスできます。しかし、洋上風力発電所や石油掘削プラットフォームのように遠隔地に位置する産業もあり、こうした場所では特定の周期、あるいは天候条件によってしか機器にアクセスできないという制限があります。

Trellixは、ICS（産業制御システム）メーカーと連携し、システムの安全な運用を支援しています。Trellixはポートフォリオ全体を通じて、エンドポイント対策とネットワーク監視に重点を置いた、産業環境向けの最適なソリューションを提供します。これらのソリューションは、完全なオンプレミス環境で利用できるだけでなく、ハイブリッド環境やクラウド環境での運用にも対応しています。

TrellixのOTシステム向けアーキテクチャ

Trellixは、お客様のOT環境を監視・保護するための多様なソリューションを提供しています。OTシステムプロバイダーのパートナー企業と連携し、防御および検知技術によって、お客様のITとOTが融合した企業環境全体のセキュリティ確保を支援することが当社の戦略です。
当社のソリューションは、脅威インテリジェンス、コンサルティング、そして業界で実績が実証されたソリューションに支えられたセキュリティプラットフォームに及び、戦略的パートナーシップや数十年におよぶ専門知識を背景に、お客様のセキュリティ成熟度の向上、コンプライアンス目標の達成、リスク評価、さらにはOT特有の脅威やIT・OTをまたぐクロスオーバー脅威の特定を支援します。
また、制御システムのより下位の階層に対して制御性と可視性を提供することで、OT特有の脅威を防御し、システムを正常な状態（既知の適正なイメージ）にロックダウンして不正な変更を防止するとともに、ラテラルムーブメント（組織内横展開）を検知し、単一のコンソールを通じてポリシー管理とレポート作成を可能にします。

これらのソリューションは、インターネットから隔離されたエアギャップ環境、ハイブリッド、クラウドの各アーキテクチャで運用でき、他のOTベンダーの監視・制御ソリューションとも統合可能です。

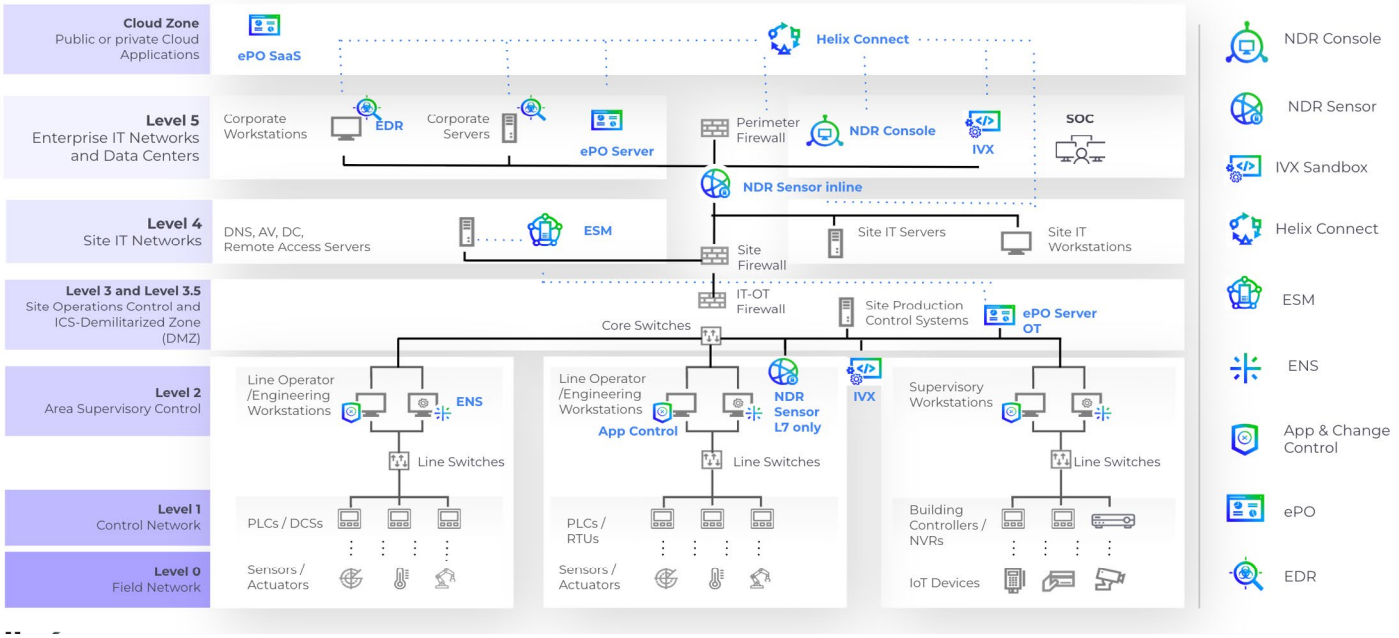

Figure 1: Trellix for Industrial Control Systems Architecture

Trellix solutions for OT

Trellix Asset Visibility for OT

Trellix Agentは、未管理のシステムをプロアクティブ(能動的)に検出し、その結果をTrellix ePolicy Orchestrator(ePO)に報告します。制御システムネットワークはアクセスが制限されているため、未知のシステムや未管理のシステムが存在することは、セキュリティ違反となる可能性があります。さらに、Trellix Agentはインストールされているソフトウェアについても報告し、管理対象システムの基本的なインベントリ(資産一覧)を提供します。制御システムはベンダーによって管理されているため、未知のソフトウェアがインストールされていると、安全性やセキュリティ上のリスクとなるおそれがあります。この資産インベントリ情報は、コンプライアンス報告や構成監視のためにePOにもレポートされます。最終的に、Trellix ePOはAPIを介して、Nozomi、Armis、Tenableといったネットワークセキュリティツールによって検出された他の資産情報をエクスポートまたはインポートできるため、ePOは制御システム環境におけるITとOTの両方の資産の可視化に最適です。

SIR(Software Inventory Report)拡張機能を備えたTrellix Agentは、OTシステムにインストールされているソフトウェアを表示する機能を提供します。これは、ソフトウェアサプライチェーンの可視化やコンプライアンス要件において重要であり、拠点がパッチ適用の優先順位を決定し、脆弱性を低減するのに役立ちます。

Trellix Endpoint Security for OT

エンジニアリングワークステーションやオペレータワークステーションは、それぞれ異なるICS（産業制御システム）ベンダーの製品である場合が多く、Active Directoryのような中央管理システムで管理されていないことがよくあります。そのため、これらのシステムを特定し、パッチの適用状況やセキュリティアラートに関するステータスを確認し、継続的に監視することは困難です。

Trellix ePOは、企業がOT環境にあるマシンの集中管理を実現できるよう支援します。完全なオンプレミスまたはSaaSソリューションとして利用可能なePOは、マシンの管理や特定のWindows設定の適用に使用できます。また、そのレポート機能により、管理者は使用中のマシンに関する情報を上位の経営層に提供できるため、適切なリスク管理を確実に実施できるようになります。

ePOのアーキテクチャでは、コンテンツのアップデートを本番の製造環境に導入する前に、ユーザーとICSベンダーの両方がその内容をチェックおよび検証できます。これにより、重要インフラにおけるアンチウイルスソリューションの管理に、さらなるセキュリティレイヤーを追加することができます。

Trellix Endpoint Security（ENS）は、多くのベンダー（ABB、シーメンス、エマソンなど）から、ICS向けのアンチウイルスソフトウェアとしての認定を受けています。ICSの文脈において、ENSは従来型のエンドポイント保護プラットフォーム（EPP）として機能し、エンドポイント上で実行されようとした瞬間にサイバー脅威を検知してブロックします。このシナリオにおいて、ENSは既知の悪意ある攻撃から保護するために、エンドポイントに必要最小限のセキュリティレイヤーを追加します。さらに、この機能はエクスプロイト防止や機械学習モジュールへと拡張することも可能であり、一部のベンダーからもこの構成がサポートおよび推奨されています。

OT環境においてエンドポイントセキュリティへの懸念がますます高まる中、ユーザーやベンダーは、インシデントへの迅速な対応や従来のアンチウイルスソフトウェアの機能拡張を目指し、Endpoint Detection and Response（EDR）機能を重要インフラに導入しようとしています。Trellixは、それを必要とする環境向けに、完全にオフラインで運用可能なオンプレミス型EDRソリューションを提供しています。さらに、OT環境はオンプレミスのePOサーバーで管理し、ITシステム（ユーザーのエンドポイントなど）はSaaS型のePOから管理するといった、ハイブリッドアプローチにも対応しています。

Trellix Application and Change Control for OT

OTのワークステーションにおいて最も重要な要件は、導入するエージェントやクライアントが軽量であり、ICS（産業制御システム）の稼働に不可欠なプロセスを決して妨げないことです。（ICSベンダーの承認が得られない、あるいはレガシーOSであるといった理由で）特定のシステムをアンチウイルスソリューションで保護できない場合でも、Trellix Application and Change Control（ACC）を使用すれば、潜在的に悪意のあるアプリケーションの実行を防ぎ、極めて重要なファイルが誰によっても（あるいは特定の人物以外によって）変更されないように保護できます。

Trellix Application and Change Controlを使用すると、許可されたユーザーによる、ホワイトリスト(許可リスト)に登録されたアプリケーションの実行のみがシステム上で許可されます。未知の(したがって禁止された)実行ファイルの実行はすべて拒否することができます。ユーザーが特定のファイルを実行したい場合は、管理者が例外的に実行権限を付与することが可能です。同様に、Application and Change Controlはオペレーティングシステム(OS)自体も保護します。ユーザーによるシステムファイルの編集や削除が許可されないためです。
これらのホワイトリストは、定期的なアップデートが必要な従来のアンチウイルスと比べて比較的静的であるため、Application and Change Controlはアンチウイルスソリューションを維持・運用するよりも、組織における管理上の負担(運用負荷)を軽減できる可能性があります。

ePOによる集中管理を利用すれば、たとえば事前に検証されたファイルのみを許可することで、アップデーターファイルによる重要アプリケーションへのアップデート適用が可能になります。さらに、Application and Change Controlは、必要なWindowsレジストリキーへのアクセスを拒否することで、環境内でのUSBデバイスの使用を禁止することもでき、重要環境におけるUSBメモリの使用を効果的に遮断します。

OT環境において、現在の生産内容を定義する設定ファイル(コンフィグレーションファイル)は「クラウンジュエル(最も重要な資産)」です。悪意のある攻撃者がPLC(制御装置)の設定ファイル変更を企てた場合、OTプロセスそのものや生産現場の動作が操作され、最悪の場合、現場で働く作業員に危害が及ぶおそれもあります。Application and Change Controlは、権限のないユーザーによるファイル変更を防御しつつ、生産技術エンジニアが必要に応じてファイルを調整できるようにし、重要インフラにおけるコンプライアンスを確実に維持します。また、Application and Change Controlは、規制要件として重要なファイル整合性監視(FIM:File Integrity Monitoring)の達成にも貢献します。

Trellix NDR for OT (in partnership with Nozomi Networks)
レガシーOSや特殊なOT機器は、従来のエンドポイントセキュリティで直接保護できないことが多く、継続的なネットワーク監視が不可欠となっています。ファイアウォールによるマイクロセグメンテーションは、小規模な産業用セル(区画)を構築することで初期の保護を提供しますが、ファイアウォール技術だけでは、ネットワーク通信の完全な可視化や、すでに境界内部に侵入している脅威の検知までは行えません。また、OT機器はIT環境では馴染みのない独自プロトコルを使用しているため、ICS(産業制御システム)の運用に関する専門知識が必要となります。

Trellix Threat Intelligence for OT
Trellix は、脅威インテリジェンスを活用(実用化)して、OT システムとIT 環境の両方の保護を向上させるための方法をいくつか提供しています。

Trellix Threat Intelligence Exchange (TIE)は、OT 環境内におけるローカル(局所的)なレピュテーション(評価)サービスとして機能し、Trellix Global Threat Intelligence (GTI)から提供されるレピュテーション情報を補完、または上書き(優先設定)することができます。TIE は、以下の方法でOT 環境のセキュリティを強化します。

- TIEが未知と判断したファイルの自動ブロック：Trellix製品は、TIEによって「未知」と判定されたファイルを自動的にブロックできます。
- Trellixサンドボックス（IVX、Cloud IVX）との統合：TIEはTrellixのサンドボックスと連携し、OT環境内の新しいファイルを自動的に分析して、実行の許可またはブロックを判定します。
- 外部脅威フィードとの連携：OT-ISAC、WaterISAC、ONE-ISAC、あるいはその他のOT特有の脅威フィードからレピュテーション情報をインポートできます。
- OpenDXLを介した外部レピュテーションの共有：TIEは、OpenDXLを通じてサードパーティ製のレピュテーション情報を保存し、共有することができます。
- カスタムツールの例外処理（レピュテーションの上書き）：ユーザー独自（カスタム）のツールが誤検知によってOT環境に影響を与えないよう、Trellixの既定のレピュテーションを任意に上書きできます。
- GTIレピュテーションプロキシとしての機能：TIEがGTIへのプロキシ（代理）として機能するため、OT環境内でインターネットアクセスをTIEサーバーだけに制限し、セキュリティを損なうことなく運用できます。
- ファイルの普及度（プレバレンス）の追跡：ファイルがどのシステムで確認され、どこで実行されたかを追跡することで、OT環境内でのラテラルムーブメント（組織内横展開）や予期しないソフトウェアの拡散の特定を支援します。
- 高速かつ軽量なクエリ：Trellix DXLを介したTIEのレピュテーション照会は高速かつ軽量であり、帯域やリソースに限りのあるOT環境に最適です。
- Trellix Private GTIとの統合：完全に隔離された「エアギャップ」環境のOTや、厳格なデータ主権・コンプライアンス要件を持つネットワーク向けに、オンプレミス版のTrellix Private GTIとの統合に対応しています。

Trellix GTIは、すべてのTrellix製品の基盤となるグローバルなレピュテーションデータベースです。インターネットへのアクセスが制限されている、または完全に遮断されているクローズド環境や高セキュリティ環境向けには、環境内に「Private GTI」を導入することでセキュリティを担保できます。さらに、Private GTIをTIEと連携させることで、よりきめ細かなレピュテーション分析と制御が可能になります。

Trellix Insightsを利用すると、Trellixが収集した膨大な脅威インテリジェンス（OT環境を標的にしたり影響を与えたりする可能性のあるキャンペーン、攻撃グループ、ツール、マルウェア、CVEなど）を閲覧・調査できます。この情報を活用することで、お客様は潜在的な脅威を予測し、ITおよびOT環境に有効な防御戦略を構築できます。

Trellixは、OTシステムや特定の産業セクター向けに最適化された、脅威インテリジェンスのレポートおよび分析サービスを提供しています。Trellixの「Tailored Intel Reports（テーラード・インテル・レポート）」サービスは、総合的なオールソース（全情報源）の調査と分析を通じて、お客様の組織特有のインテリジェンスニーズを満たすように設計されています。