SOLUTION BRIEF

マイクロセグメンテーションによる OT の保護

概要

これまで、オペレーショナルテクノロジー（OT）ネットワークは、スイッチで VLAN（仮想 LAN）などの LAN（ローカルエリアネットワーク）ソリューションを使用して、ネットワークに侵入したマルウェアの水平移動による攻撃から保護していました。VLAN ソリューションのセグメンテーションは柔軟性に優れていますが、それでも OT ネットワークを保護するには不十分です。

フォーティネットのマイクロセグメンテーションを導入することで、ゼロトラストのセキュリティポリシーを適用し、次世代ファイアウォール（NGFW）を使用して VLAN 内のすべてのトラフィックをスキャンできるため、マルウェアがネットワークを水平移動する攻撃が大幅に減少します。また、マイクロセグメンテーションでは、OT ネットワークに必要なレベルのセキュリティを確保するために、ネットワークパフォーマンスが犠牲になることもありません。

VLAN ではレイヤー 2 で単一の通信ネットワークが複数の仮想ネットワークに分割されます。単一のブロードキャストドメインが複数の小さなドメインに分割されるため、ネットワークパフォーマンスが向上します。VLAN を使用することにより、通信ネットワーク内に物理的に分散しているネットワークの構成要素を論理的にグループ化することもできます。

ICS / OT ネットワークの概要

ICS（産業用制御システム）/ OT（オペレーショナルテクノロジー）の通信ネットワークは、PCN（プロセス制御ネットワーク）として知られています。PCN によって PLC（プログラマブルロジックコントローラー）、RTU（リモートターミナルユニット）、DCS（分散制御システム）、SCADA（監視制御 / データ取得）システムなど、ICS の個別のコンポーネントの多様な自動化プロセス間の通信が可能になります。

PCN では制御ユニットと測定ユニット間の命令やデータの送受信、ICS / OT 環境内のさまざまなコンポーネントの相互接続も行えます。これらは、パフォーマンスと信頼性に優れた堅牢な LAN で接続します。ICS のダウンタイムをゼロにし、高信頼性でエラーのない継続的な運用を可能にするには、PCN で一貫した可用性、迅速なレスポンス、強力なエラーチェックと修正の機能が必要です。

ICS の信頼性と堅牢性の要件を満たすため、PCN は多くの場合、ICS のコンポーネント間に境界がないか、あってもわずかなフラットなネットワークとして構成します（図 1 参照）。このようにフラットなネットワーク構成の PCN では保守も簡略化されます。

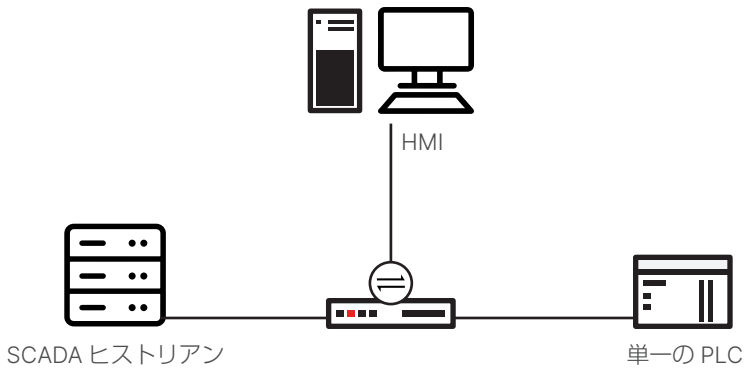

図 1：PCN のフラットなトポロジの例

ただし、このような構成では、PCN がマルウェアの水平移動攻撃やフラッド攻撃などの標的になるセキュリティリスクは高くなります。これらの攻撃を受けると PCN の通信が中断し、ICS 全体が停止する可能性があります。また、フラットなネットワーク構成では、ICS の境界外の他の通信ネットワークと PCN の統合が困難になります。

これまで、製造業界ではネットワークブリッジやゲートウェイなどの LAN ソリューションを利用してさまざまなコンポーネントを分離し、PCN 内のブロードキャストやフラッディングを制限してきました。VLAN を導入した場合、このセグメンテーションプロセスの柔軟性が向上し、物理的なレイアウトに関係なくネットワークを分離できます。ただし、VLAN だけでは PCN に大きな被害を及ぼす可能性のあるセキュリティの問題には対応できません。また、PCN に VLAN ベースのセグメンテーションを採用するとなると、エンタープライズネットワークよりも通信速度は遅くなります。

PERA（パデューエンタープライズ参照アーキテクチャ）は 1990 年代にコンピュータ統合生産（CIM）のために開発されました。システムインテグレーターやシステム所有者に向けて大規模システムを複数のレベルで分類するためのガイダンスが提供されるため、さまざまなコンポーネントやサブシステムの統合をより的確に制御できます。ISA-99 では ICS のレベルの分類とセキュリティ制御にこのモデルを採用しています。ISA-99 は後に IEC 規格（ISA / IEC62443）になりました。

ICS / OT ネットワークのゾーンとコンジット

ICS / OT ネットワークのセキュリティの課題に対応するために、製造業界にゾーンとコンジットの概念が導入されました。それによって、PCN は複数のゾーンに分類され、ICS のさまざまなコンポーネントが分離されました。ICS では同じセキュリティ要件を共有する論理的または物理的資産をゾーンによってグループ化し、ゾーンで送受信する情報のセキュリティ境界を定義します。コンジットはゾーン間に配置され、通信とセキュリティを制御するゾーンの境界間の制御メカニズム（ゲートキーパー）として機能します。

ゾーンとコンジットのモデルは、ISA / IEC62443-1-1 と IEC 62443-3-2 に採用され、ゾーンとコンジットの定義について詳細なガイダンスが提供されています。PERA のフレームワークを使用することにより、ICS 内のさまざまなゾーンとコンジットを複数のレベルに分類できます。

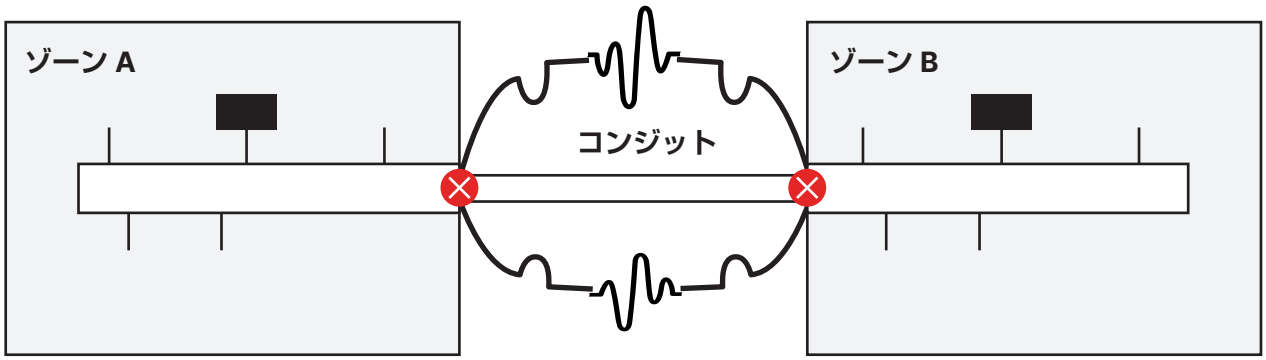

図 2：ゾーンとコンジットの概念

製造業の課題：OT、IIoT、IT、IoT、統合

インダストリー 4.0 の進化に加え、IoT（モノのインターネット）や IIoT（産業用 IoT）などの創造破壊的なテクノロジーにより、ICS / OT ネットワークはより統合されたネットワークへと変化しました。ICS / OT はもはや孤立した環境では機能しません。エンタープライズ IT ネットワークと外部のインターネットに接続し、ビジネスインテリジェンスの収集やビジネスの意思決定に使用されています。

ICS / OT と IT インフラストラクチャが統合された現在、通信にはもはや ICS / OT 固有の通信プロトコルを含め、専用のネットワーク通信プロトコルは使用されません。ICS / OT と IT の統合ネットワーク通信には専用のプロトコルとオープンスタンダードのプロトコルが複雑に組み合わされて使用されるため、さまざまな攻撃に対して脆弱になります。特に、OT ネットワークと IT ネットワークを統合した場合、ネットワークの攻撃対象領域が拡大するため、VLAN などの従来のセキュリティでは ICS を十分に保護できません。

ゾーンとコンジットを定義してネットワークを分類することは ICS / OT と IT の統合には不可欠ですが、それだけでは統合インフラストラクチャのネットワークセキュリティの課題に完全に対応することはできません。VLAN は高度なネットワーク攻撃の防御には不十分です。

VLAN の場合、同じブロードキャストドメインのデバイス間においてネットワークパケットは自由に転送されます。しかし、ブロードキャストドメインの境界を超えてパケットが移動する場合、ネットワークルーティングのメカニズムが必要です。通常、ルーティングのメカニズムは仮想または物理のコンジットとして機能し、2 つのブロードキャストドメイン間の通信のセキュリティ制御に使用されることもあります。ただし、VLAN ルーティングのメカニズムによるセキュリティでは、最新の ICS / OT と IT の統合インフラストラクチャには不十分です。

また、VLAN は同じブロードキャストドメイン内のネットワーク通信の検査にも対応していません。VLAN のデバイスはブロードキャストドメイン内では、検査や制御を受けることなく互いに無制限に通信できます。

一般的な ICS / OT ネットワークでは、1 つの VLAN に数十のグループ化されたコンポーネントがあり、これらのコンポーネントはコンジットを通らずに相互に自由に通信できます。そのため、PCN 内では異常なネットワーク通信も水平方向に移動できます。

ゼロトラストセキュリティモデルでは、組織のシステムへの接続の試行は組織のネットワークの内外を問わず、すべてアクセスを許可する前に検証する必要があります。ICS / OT インフラストラクチャでも、異なる ICS コンポーネント間のネットワーク通信を保護するために同じゼロトラストセキュリティの概念を採用します。

このようなネットワークを他のネットワーク（通常は ICS / OT の境界外）と統合する場合、すべての通信チャネルを検査する必要があります。さもないと、統合したネットワークが複雑な場合、ネットワークへの攻撃が検知されない可能性があります。また、ICS / OT ネットワークと IT ネットワークの間の情報交換にオープンな通信プロトコルを使用するとリスクが増大します。通信プロトコルが脆弱で攻撃が可能であれば ICS / OT 環境は格好の標的になります。

ICS / OT ネットワークのマイクロセグメンテーション

VLAN では論理セグメンテーションを柔軟に行えますが、マイクロセグメンテーションなら VLAN をさらに分割し、それぞれにセキュリティポリシーを適用できるため、ネットワークトラフィックをよりきめ細かく制御できます。また、セキュリティポリシーをネットワークトラフィックのタイプに合わせて調整し、ICS のさまざまなコンポーネント間のネットワークとアプリケーションのフローも制限できます。ICS の所有者はゼロトラストセキュリティモデルを導入できるため、同じ VLAN の PLC であってもセキュリティポリシーで明示的に許可されない限り PLC 間で通信することはできません。

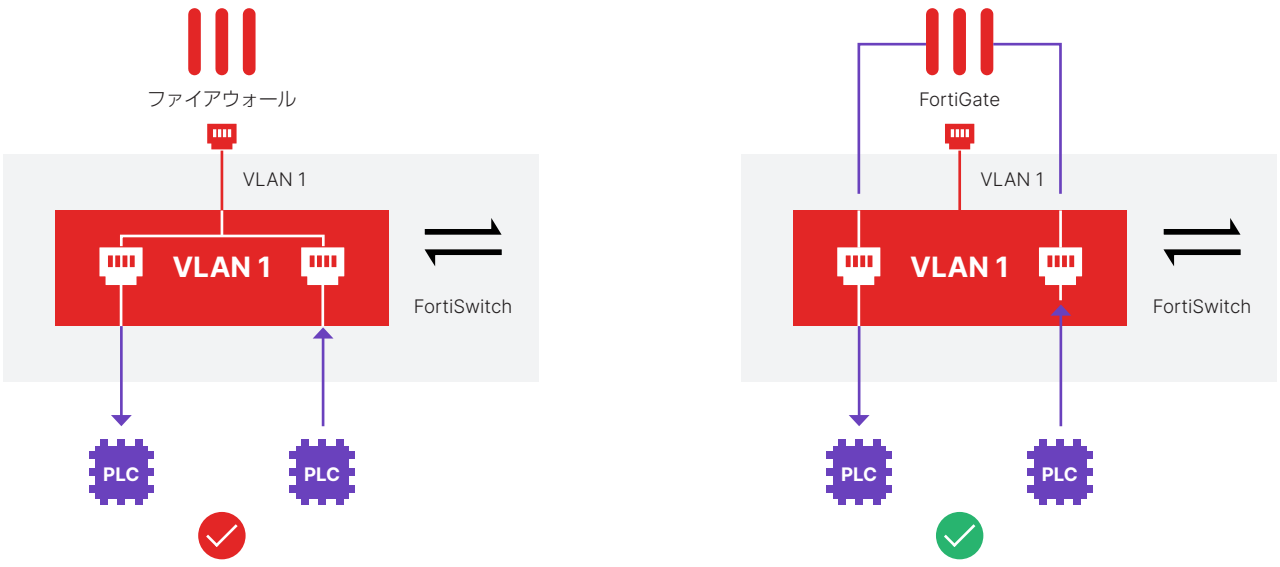

図 3：通常の VLAN ルーティングと、フォーティネットの FortiSwitch と FortiGate を使用したマイクロセグメンテーション

通常、ネットワークのマイクロセグメンテーションでは、セキュリティポリシーの適用、ネットワーク通信の検査とフィルタリングのために NGFW を VLAN に連携させます。フォーティネットの FortiSwitch と FortiGate NGFW にはマイクロセグメンテーションに統合するためのアプローチが用意されています。この統合ソリューションでは、VLAN の機能がレイヤー2のネットワーク通信からレイヤー3(ルーティング)とレイヤー7(可視化)へと拡張され、ネットワークトラフィック検査が可能になります。FortiSwitch によってレイヤー 2 で VLAN が定義され、FortiGate NGFW によってレイヤー 3 で同じ VLAN 内と異なる VLAN 間のすべての通信のルーティングが行われます。また、きめ細かいセキュリティポリシーによるネットワークトラフィック検査が可能になり、NGFW によってレイヤー 7 でファイアウォールを通過するネットワークプロトコルと情報を検査できます。

FortiGate NGFW はフォーティネット独自のオペレーティングシステムの FortiOS で実行するため、ICS / OT プロトコルの DPI をはじめ、業界をリードするネットワークセキュリティ機能が提供されます。また、並列冗長プロトコル（PRP）などの ICS / OT 固有のネットワークプロトコルがサポートされ、高度なマルウェア保護、侵入防止システム（IPS）、ソフトウェア定義の広域ネットワーク（SD-WAN）などの機能も利用できます。

フォーティネット統合ソリューションによる ICS / OT ネットワークのマイクロセグメンテーションには以下をはじめ、多くのメリットがあります。

- **ホスト / デバイスの分離：**ICS ネットワーク内の各デバイスを分離して、ネットワーク通信をきめ細かく制御できます。デバイスで送受信するネットワークトラフィックは強制的に FortiGate NGFW を通過するため、セキュリティポリシーの適用、トラフィック検査、アプリケーション制御、侵入の検知と防止が可能になります。
- **ICS プロトコルのディープパケットインスペクション（DPI）：**FortiGate NGFW では 32 以上の ICS / OT プロトコルと 1,500 以上のアプリケーション制御のシグネチャ（設定不要）で DPI がサポートされます。
- **ラテラルムーブメントの防止：**ICS の各コンポーネントが分離しているため、マルウェアが ICS ネットワークに侵入しても水平方向に拡散できません。また、ICS ネットワーク内のすべてのトラフィックに検査とポリシーが適用されます。
- **高性能：**FortiGate NGFW は、高性能なファイアウォールであり、最小のレイテンシーを実現しているため、マイクロセグメント化された ICS ネットワーク内のネットワーク トラフィック検査に最適です。
- **シームレスな統合：**論理と物理のいずれのネットワーク接続も変更は必要ありません。
- **単一ペインの管理：**ソリューション全体を統合管理コンソールで管理できるため、ICS のセキュリティの自動化が簡略化されます。

マイクロセグメンテーションに対応したフォーティネット統合ソリューションに対しても、ソリューションの導入に PERA のガイダンスを使用します。ICS のコンポーネント間が接続されていれば、ICS / OT ネットワーク内のレベルを問わず、マイクロセグメンテーションを適用できます。

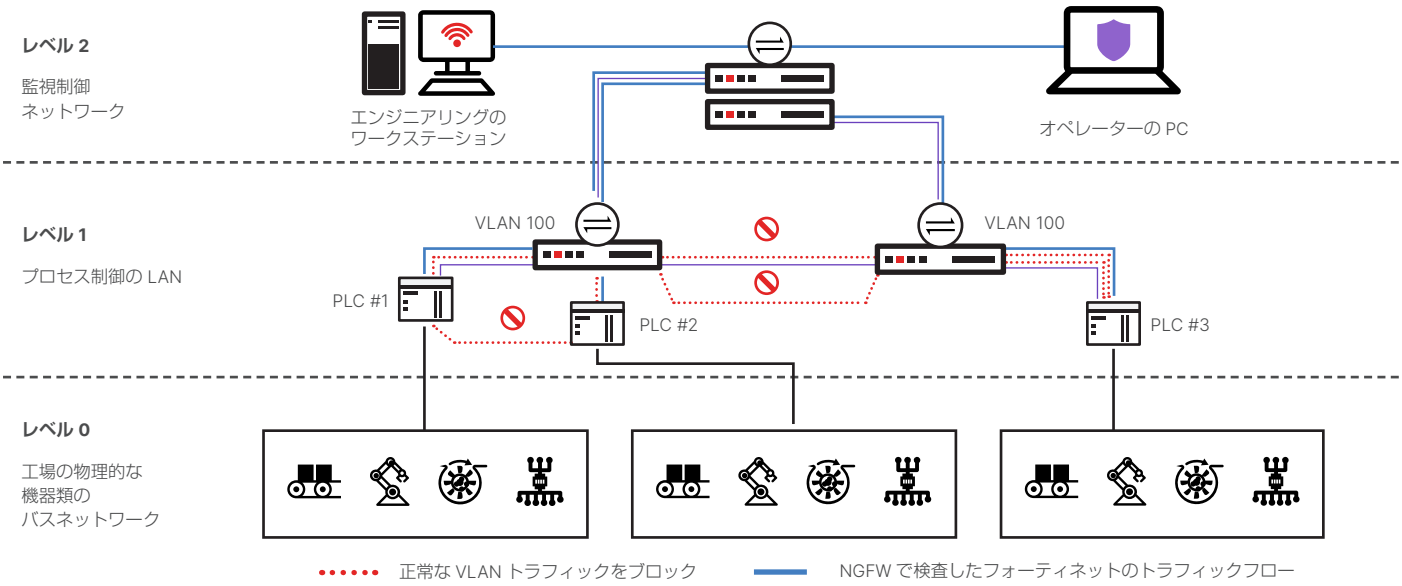

図 4：フォーティネットの FortiSwitch と、FortiGate のマイクロセグメンテーションを適用した PERA アーキテクチャの例

終わりに

ICS / OT ネットワークの多くはそれぞれに運用要件の異なるライフサイクルの長いデバイスで構成されています。そのため、セキュリティには OT 固有のアプローチが必要です。

フォーティネットは ICS / OT ネットワークセキュリティに独自の視点で取り組んできました。これによりフォーティネットは、FortiGuard Labs により追跡された OT 特有の脅威報告と洞察を活かして、OT に特化したセキュリティ脅威レポートをまとめ、OT 環境のニーズを満たすソリューションを独自に開発しています。

その VLAN ベースのマイクロセグメンテーションでは、ビジネスリスクを制御しながら論理的に分類されたネットワークの利点を ICS に活用できます。フォーティネット セキュリティ ファブリックでこれらのソリューションを統合することで、すべてのセキュリティインフラストラクチャの完全な可視化と制御が実現します。

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

Copyright© 2021 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。

SB-Secure-Vlan-Technology-202110-R1