JOINT SOLUTION BRIEF

Tempered

NOZOMI NETWORKS

**＜抄訳版＞**

**株式会社テリロジー**

# 可視化からポリシーエンフォースメントまでのゼロトラスト IoT/OT セキュリティプラットフォームとは

## AI を活用したネットワーク可視化と分析ソリューションで業界リードする Tempered セキュリティポリシーエンフォースメントと Nozomi Networks ICS IoT/OT セキュリティソリューションを連携。

（注）**セキュリティポリシーエンフォースメント**とは、業界用語でセキュリティポリシーを強制適用するという意味で使われています。

## 課題

IoT/OT ネットワークの可視化、そしてデータ共有のリモートアクセスのニーズで、インターネット接続のデマンドが高まっています。スマートビルディングやスマートシティを含む社会重要インフラは、IoT/OT/IT ネットワークの垣根を越えて、悪意なサイバー脅威に狙われています。

多くの産業系インフラの ICS システムは、セキュリティ“パッチ”や OS/ソフトのアップデートが難しく、又ゼロデイ攻撃からの防御が難しいレガシー環境となっています。そして多くの場合、事前の対処措置や既存監視ツールによる根本原因分析をすり抜けて素早く不正侵入し、ネットワークインフラ全体に感染を広げる恐れがあります。

企業ユーザは、こうした不正侵入する脅威や異常な振舞いの監視/検出、トラフィック分析に加えて、潜在的な脅威ドメインのセグメントを分離し、そのリスクを回避し、オペレーションを持続的に稼働させる自動修復プロセス、又はセキュリティポリシーエンフォースメントといった機能を必要としています。

### 両製品連携のハイライトとキーメリット

- 業界をリードする IoT/OT/IT セキュリティソリューション
- 産業制御システム(ICS)ネットワークの優れた可視性
- AI ベースのトラフィック分析、異常検出、イベント相関
- ネットワークセグメント分離による脅威リスクの自動修復
- セキュアなオーバレイトンネル(HIP)、ポリシーエンフォースメント及び Military グレードの暗号化
- Conductor により一元集中管理し、マルチパブリッククラウド全体の運用管理が容易
- 従来のセキュリティポリシーソリューションよりもコストパフォーマンスに優れ、かつ容易な設定手順
- 産業 SCADA システムや IoT デバイスのエンドポイントまでのサイバー脅威を守るアクセスポリシー管理
- ゼロトラストネットワークアーキテクチャ（ZTNA）の実装を容易に構築出来るマイクロセグメンテーションポリシー

## Tempered Airwall

Tempered Airwall は、ゼロトラストモデルや **SDP(Software Defined Perimeter)**をベースに安全で容易な運用管理を提供します。Airwall は既ネットワークに迅速に導入出来、Firewall、VLAN、VPN、アクセスコントロール等の面倒でミスしやすい設定手順のセキュリティコンフィグを置き換えることが出来ます。これは、グローバル通信回線を経由して世界中の拠点間で簡単にネットワークセグメントを設定し、安全なリモートアクセスを提供します。そして、セキュアなリモートアクセスを実現する要件として Airwall は十分対応出来る唯一の効果的かつ効率的なソリューションです。

## Nozomi Guardian™

Nozomi Networks Guardian は、OT/IOT の可視化を実現し、セキュリティと DX 化を推進します。Nozomi Guardian の物理アプライアンスと仮想アプライアンスは、多様なデバイスの異常な振舞いを検出し、OT/IoT ネットワークとそのトラフィックパターンを即座に分析します。最優先の脆弱性と脅威リスクを可視化し、高い信頼性とセキュリティを担保します。Nozomi Guardian は、世界中の社会重要インフラをはじめ、エネルギー、製造、鉱業、交通、ビルディングオートメーション等 OT 分野のセキュリティリスクを大幅に改善します。

## Tempered & Nozomi 連携ソリューション

Nozomi の ICS ネットワークの可視化/サイバー脅威検出/インシデント対応と Tempered のゼロトラストポリシーエンフォースメントと Airwall Conductor コンソールを連携します。ハイレベルで洗練されたサイバー攻撃に対しては、優れた可視化とインテリジェントな検出機能だけでなく、アクセス認証とビジネスの可用性を担保しながら脆弱なセグメントを分離させて自動修復を実施します。この連携には、セキュアなトラフィックを暗号化トンネル経由で Nozomi Guardian とミラー接続する Tempered のオーバレイネットワーク（HIP）が含まれています。Nozomi は Tempered Airwall のセキュアトラフィックを Nozomi Guardian の AI 学習機能を活用して、Airwall Conductor コンソールの API を介して Tempered のセキュリティポリシーにフィードバックします。Nozomi Guardian は、Tempered のポリシー集中管理の Conductor を活用して Airwall ゼロトラストポリシーをアップデートします。尚、この連携は Tempered Airwall 2.2.11 でサポートします。Airwall 2.2.11 では以下の追加機能が含まれます：

- ミラーポートを介したリモートトラフィック監視サポートの向上で、ネットワークを安全に監視し、脅威を検出することがこれまでになく簡単になりました。
- 新しい可視性および脅威検出機能は、Conductor 内で直接顧客ネットワーク上のトラフィックの不正な動きを洞察します。
- Airwall を多様な環境に適合させるための DNS の機能強化。

Tempered Airwall は、Military グレードの暗号化とセキュアなアクセスポリシーエンフォースメントを提供します。こうしたユニークな機能によって、顧客ネットワークで監視された異常なトラフィックセグメントを分離してサイバー脅威の迅速な修復に貢献します。 脅威検知と自動化されたプロアクティブなエンフォースメントの連携は、業界で比類のないものです。産業ネットワーク全体を危険にさらす可能性のある SolarWinds の脆弱性や、リモートワークや産業用スマートデバイスのネットワーク接続など、最近台頭している新たなサイバー脅威に対して、この連携ソリューションは、内部脅威の急速な拡散を防止し、攻撃対象領域を削減するための最良の機会を提供します。

**Edgard Capdevielle, CEO at Nozomi Networks**

## Use Case 1

**課題**

産業系制御システム(ICS)の SCADA 環境などのデバイスを含むリモートサイトのトラフィックをどのように監視および分析出来ますか？

**対応**

この連携により、リモートサイトで Airwall が収集したトラフィックをミラーリングして Nozomi Guardian に送ります。複数サイトでは、Airwall の暗号化トンネルを介して、AirWall Conductor に接続出来ます。企業は、数百のリモートサイトからのトラフィックを Airwall Conductor で監視および分析出来るようになりました。エンドポイントデバイスは脆弱性があり、攻撃ターゲットになることが多いため、新しい脅威の識別とトラフィックの可視性が重要になります。

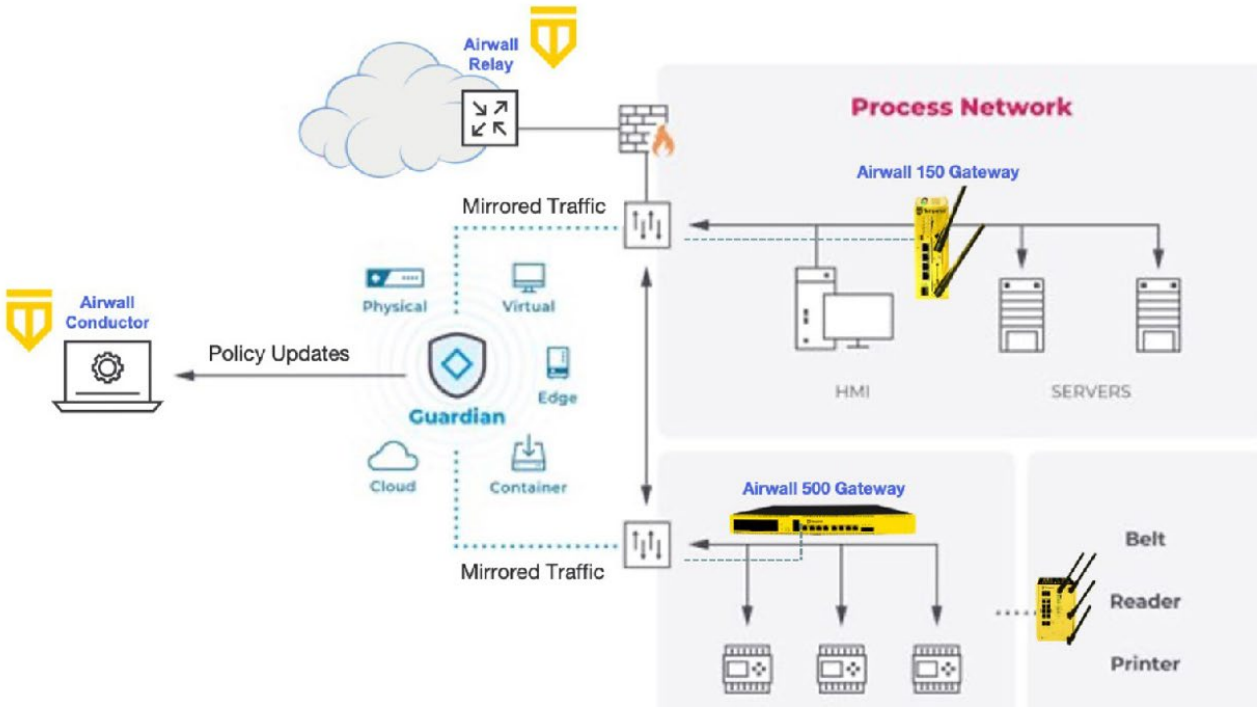
## Use Case 2

**課題**

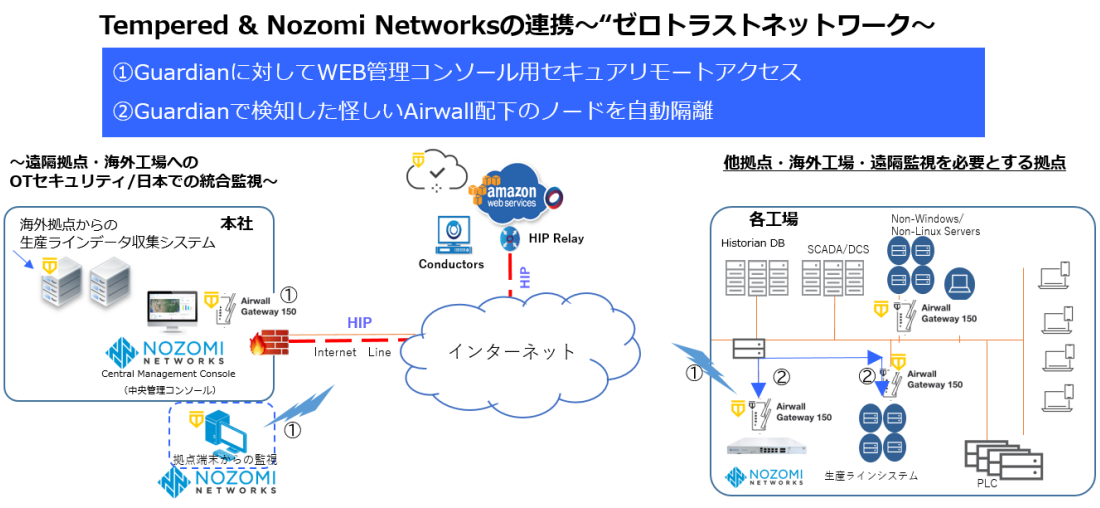
ネットワーク上のデバイスが異常な外部ネットワークに接続を行ったり、ポートスキャンして使用可能なポートを探し始めます。この場合、どのように対応する必要がありますか？

**対応**

システムがマルウェアによって感染した場合、又はその他異常なトラフィックの振舞いがある場合、Nozomi Guardian の分析機能で疑わしいデバイスを素早く識別し、Airwall Conductor に検疫リクエストを出して、Tempered によって感染したデバイスを別のセグメントに分離し、その脅威が修復されるまで、ネットワーク内でのマルウェア感染拡大を防止します。Airwall Conductor コンソール API で迅速かつ自動修復します。



以下の図では、セキュアリモートアクセスと異常検知したノードをセキュリティポリシーで特定ノードの自動隔離の連携ソリューションの仕組みを示します。Tempered Airwall は、本社または他拠点で別の Airwall に、直接トラフィックをミラーリングすることが出来ます。トラフィックは、Airwall HIP オーバーレイ ネットワーク内で完全暗号化することも出来ます。そして、Nozomi Networks からの検出アラートによって脆弱な脅威のデバイスへのネットワークセグメントアクセスを Conductor のオーケストレーション機能でネットワーク ポリシーを再構成し、隔離します。




## Tempered Networks について

Tempered は、業界で唯一の真のネイティブな Zero Trust Software-Defined Perimeter（SDP）ソリューションを提供し、同社 Airwall を使用すると、IT/OT/ICS/SCADA、リモート、クラウドなど、複雑なインフラ環境全体で安全なネットワークを簡単に構築および維持出来、Airwall ネットワークは、マルチ要素認証、マイクロセグメント化、そして暗号化されたエンドツーエンドセキュリティであり、ラテラルムーブメントへの感染を防御し、重要な資産とネットワークインフラに接続のデバイスをサイバー脅威から見えなくします。

https://tempered.io.

## Nozomi Networks について

Nozomi Networks は、OT/IoT 産業分野セキュリティ世界市場のリーダです。Nozomi Networks は、世界中の重要インフラ、エネルギー、製造、鉱業、交通、ビルオートメーション、およびその他 OT サイトのネットワークと資産の可視化、脅威検知およびサイバーリスクのアセスメントを提供します。

又、世界主要な制御システムベンダー、セキュリティベンダー及びコンサルティングベンダーともパートナーシップを結んでいます。尚、2020 年 Gartner Peer Review でトップスコア、Frost& Sullivan の市場調査では 2019 年度 ICS/OT セキュリティマーケットリーダをそれぞれ獲得しました。

www.nozominetworks.com

### 出典

Comprehensive Zero Trust IoT/OT Security Platform from Visibility to Policy Enforcement

（PDF 形式　ファイルサイズ：1.05 MB）

### 関連リンク

https://tempered.io/

https://www.nozominetworks.com/

### お問い合わせ窓口

株式会社テリロジー

グループ事業推進統括部

OT/IoT セキュリティ事業推進部

製品に関するお問い合わせは当社のお問い合わせフォームからお寄せください。