FORTINET

IT / OT 統合環境の
セキュリティ保護アプローチ

目次

FORTINET

概要

運用テクノロジー（OT）* ネットワークは、公益事業や製造組立ラインといった重要なインフラストラクチャで稼働する**機器**を制御するものです。これまで OT ネットワークは、あらゆる組織の**データ**を制御する**情報テクノロジー（IT）**とは分離されてきました。近年、人工知能（AI）やビッグデータアナリティクスをはじめとする IT イノベーションが進み、OT ネットワークにも確かなメリットをもたらしています。その結果、OT ネットワークと IT ネットワークの統合が加速しつつある一方で、デジタル攻撃の対象領域が拡大しており、IT ネットワークを標的にした攻撃が OT ネットワークにも及んでいます。現在、OT セキュリティの侵害は日常茶飯事となっています。攻撃を阻止して OT のリスクを最小限に抑制する方法として、5 つのベストプラクティスの実装があります。そのベストプラクティスとは、1）ネットワークの可視化、2）ネットワークセグメンテーション、3）トラフィック分析、4）アイデンティティとアクセス管理、5）有線 / 無線アクセスの保護です。このベストプラクティスは、OT セキュリティ態勢を改善する基盤となります。

* OT は、**産業用制御システム（ICS）**と同義です。プロトコル、ベンダー、ユースケースが異なるという理由から、「OT」は IT と対比した用語として使用されています。**SCADA（監視制御データ収集）**システムは、OT の要素の 1 つです。SCADA システムは、GUI（グラフィカルユーザーインタフェース）を使用して OT / ICS プロセスの高度な監視と管理を行います。

01：IT と OT のコンバージェンスが進んでいる理由

機械学習（ML）、拡張現実（AR）、モノのインターネット（IoT）など、IT の新たな開発はプロセスを刷新し、さまざまなビジネス分野に多くの成果をもたらしています。この変革は一般的に、デジタルトランスフォーメーション（DX）と呼ばれます。

パイプライン、送電網、輸送システム、製造工場といった重要度の高いインフラストラクチャを制御する OT ネットワークの変革は、IT 環境に比べて緩やかな速度で進んでいます。OT 環境は、公安やグローバル経済に不可欠です。IT ネットワークが登場する何十年も前に開発された OT ネットワークには、IT とは異なるベンダーや独自仕様のプロトコルが存在します。当初、OT ネットワークと IT ネットワークの接続はサイバー攻撃のリスクが高まるだけで、ほとんどメリットはありませんでした。

ところが、先頃行われた調査によると、OT 組織の 4 分の 3 が、生産性向上とコスト効率の改善を目的として IT と OT の基本的な接続を実行していることが明らかになりました[1]。OT 環境で新たに登場したデジタルテクノロジーは非常に大きな変革を推進しており、第四次産業革命と称されています[2]。製造ラインには、最適化を目的としたセンサーが設置されています[3]。倉庫のスタッフは、拡張現実メガネを装着することでミスを軽減しています[4]。そのメリットは大きく、デジタルトランスフォーメーションのスコアが上位 4 分の 1 の組織は、下位 4 分の 1 の組織と比較して、ほぼ 2 倍の利益率と利益を達成しています[5]。

DX のスコアが高いリーダー企業は、低い企業に比べて 2 倍の利益率と利益をあげています。

IT と OT の統合の結果、デジタル攻撃の対象領域が拡大し、サイバー攻撃のリスクが高まるという課題が生まれています。OT 環境を持つ組織の 90% 近くが、OT ネットワークの侵害を経験しています[6]。

OT 組織の 90% 近くが、
セキュリティ侵害を経験しています。

02：推奨される OT サイバーセキュリティのベストプラクティス

では、リスクの最小化と成果の最大化を両立するには、どのような方法があるのでしょうか。サイバー攻撃に対抗するには、OT リーダーは次の 5 つの領域をチェックする必要があります。

1. 資産の特定、価値の分類、優先順位付け

可視化は、セキュリティ態勢を改善する第 1 歩です。把握できないものを保護することは不可能だからです。多くの組織において、可視性の欠如が深刻なセキュリティギャップとなっています。組織の 82% が、ネットワークに接続されているデバイスすべてを特定することは不可能な状態に陥っています [7]。

セキュリティチームは、ネットワーク上で稼働しているデバイスとアプリケーションの最新のインベントリを把握する必要があります。ところが、OT ネットワークの多くは、IT ネットワークで使用される手法では能動的にスキャンを実行することができません。能動的なスキャンはネットワークパフォーマンスを低下させ、PLC などの OT 要素に障害を引き起こす原因にもなります [8]。

セキュリティチームは、ベンダーやテクノロジーパートナーに脅威状態の評価を依頼すべきです。そのような評価では、OT アプリケーションのプロトコルを認識し、暗号化トラフィックを含むネットワークトラフィックを受動的に観察する NGFW（次世代ファイアウォール）などのシステムが使用されることがあります。このようなシステムは、収集した情報から、ネットワーク上にあるデバイスの特性や振る舞いに基づいてプロファイリングと分類を行います。その結果、次のような内容がレポートされます。

- 接続されているデバイスのインベントリ情報
- リスクの高いアプリケーションの指摘
- アプリケーション脆弱性の上位エクスプロイトを検知し、特定
- 各資産のリスク値を評価
- マルウェア、ボットネット、侵害の可能性があるデバイスの兆候を特定
- アプリケーションを分類し、ネットワーク使用状況を分析

このような情報は、リスクの優先順位付けやセキュリティ計画の最適化において、確かな基盤となります。

82% の組織は、自社ネットワーク上のデバイスすべてを特定することが不可能な状態に陥っています。

ネットワーク構築の計画では、
補完的な脅威評価が有効です。

2. ネットワークのセグメンテーション

ネットワークセグメンテーションは、OT 環境保護において最も効果的な設計概念の 1 つです [9]。

セグメンテーションとは、ネットワークを複数の機能的セグメントに分割することを指します。セグメントは「ゾーン」（サブゾーンやマイクロセグメントを含む）と呼ばれ、承認されたデバイス、アプリケーション、ユーザーのみにアクセスを許可します。ゾーンの定義と適用は、ファイアウォールで行います。また、重要なデータとアプリケーションが複数のゾーン間を移動するためのチャネルとなる導管も定義されます。

- **攻撃者がネットワーク内を移動する能力を制限します。**
- **厳格なアクセス制御により、各ゾーンへのアクセスを制限します。**

ゾーンと導管の設計モデルは、侵入リスクを大幅に低減します。このモデルでは、攻撃者による水平（ラテラル）方向の移動が制限されます。ユーザーやデバイス毎に個々のゾーンで実行可能な操作を承認することにより、稼働領域をそのゾーンに限定できます。

セグメンテーションは OT セキュリティ保護の基本的なベストプラクティスであり、ISA / IEC-62443（旧称：ISA-99）セキュリティ標準で規定されています [10]。この規定は、ISA（International Society for Automation）によって ISA-99 として策定された後、IEC（International Electrotechnical Commission）標準に沿って IEC-62443 となりました。

ISA / IEC-62443 標準では、OT ネットワークのセグメンテーションに関する実用的なガイダンスが示されています。このガイダンスでは、各ゾーンに 0 ～ 4 のセキュリティレベル（0 が最低、4 が最高を表します）を割り当てます。また、ユーザーやデバイスの認証済 ID に基づいて、それぞれのゾーンと導管に厳格なアクセス制御を適用します。

ファイアウォールについては、一般的な CPU を搭載したものではなく、特定のパケット処理やコンテンツスキャン機能の高速化を目的に設計された、専用のセキュリティプロセッサを搭載するファイアウォールを検討すべきです。専用セキュリティプロセッサは、暗号化やコンテンツインスペクションサービスを高速実行でき、ネットワークパフォーマンスが低下することもありません。この点は、ゾーンと導管ボトルネックにしないために重要なポイントとなります。

3. トラフィック分析による脅威と脆弱性の検知

NGFW が OT ネットワークをセグメントと導管に分割すると、ネットワークトラフィック分析を実行して既知と未知の脅威をチェックすることが重要になります。

セキュリティチームは、暗号化されたアプリケーショントラフィックのインスペクション機能を備えた NGFW を統合すべきです。さらに、ライブフィードサービスと NGFW が統合され、一般的な OT プロトコルと OT アプリケーションの脆弱性に関する最新情報を提供することも重要です。このタイプのサービスを利用することで、NGFW は OT アプリケーショントラフィックの検証とエクスプロイトの特定を実行できるようになります。リアルタイムのグローバルなインテリジェンスのアラートは、ファイアウォールを更新し、新たに登場する巧妙な脅威の検知を可能にします。互換性のあるエンドポイントセキュリティソリューションと統合することで、世界中の幅広いソースから収集された IOC（侵害指標）をエンドポイントで監視できるようになります。

また、ネットワークトラフィック分析から、ベースラインを確立し、IT / OT システムの正常 / 異常状態を把握することも可能です。異常や IOC が検知された場合には、隔離やブロック、アラート送信などのレスポンスを実行できます。NGFW に統合されている AI 機能は、自己進化型の脅威インテリジェンスシステムであり、ゼロデイ脅威が開発される前であっても捕捉するシグネチャを作成できます。

脅威検知とコンプライアンスレポートの容易な作成を実現するために、セキュリティチームは SIEM（セキュリティ情報 / イベント管理）ソリューションを追加すべきです。SIEM は、IT / OT ネットワークにある単機能セキュリティソリューションとデバイスログのデータを使用して相関付けを行います。最適なアプローチは、ネットワークのリアルタイムトポロジのマッピングと、セキュリティイベントの追跡 / 記録機能を備えた SIEM を統合する方法です。このアプローチでは、さまざまなソリューションの情報を相関付けることで、コンテキストの提供、応答時間の短縮、レポーティングの簡素化を実現します。

- **セキュリティレーティングは、セキュリティパフォーマンスをスコアで評価します。**
- **ライブグローバルフィードは、アプリケーション脆弱性の最新情報を提供します。**

脅威インテリジェンスフィードへのバンドルとして提供されるセキュリティレーティングサービスは、セキュリティパフォーマンスを評価し、自社のセキュリティ態勢を同業他社と比較することができます。コンプライアンスレポートを作成し、経営陣からのセキュリティの有効性に関する質問に回答する上で役立つサービスです。

45% の企業は、特権アクセスが可能な
アカウントを監視していません。

4. アイデンティティおよびアクセス管理の制御

認証情報の窃取は、多くの OT サイバー攻撃で悪用される手口であり、本書ですでにプロファイリングされた 4 種の攻撃のうち 3 つがこれに該当します。この攻撃で大きな役割を果たすのが、認証情報の窃取に使用されるスピアフィッシングです。脅威環境にあるマルウェアの実に 3 分の 2 が、メールを介して配信されています [11]。IAM（アイデンティティとアクセスの管理）エクスプロイトを制御する際にまず実装すべきセキュリティ階層は、シグネチャ / レピュテーションベースの防御機能を備えたセキュアメールゲートウェイです。

OT 組織の 45% が、ロールベースのアクセス制御を使用していません。

また、特権アイデンティティ管理の欠如も、アクセス制御に存在する脆弱性の 1 つです。特権アイデンティティ管理は、IT 環境内の特権アカウントの監視を可能にしますが、調査では 45% が「使用していない」と回答しています [12]。その結果、多くの攻撃者が標的とする管理者の認証情報が窃取され、悪用されるリスクが高まります。

また、OT 組織の 45% は、内部関係者の脅威リスクが高まっており [13]、ほとんどの組織がアクセス制御テクノロジーの採用計画があると回答しているにもかかわらず [14]、ロールベースのアクセス制御を従業員に適用していません。 セキュリティチームは、次のような機能を備えた IAM ソリューションを検討すべきです。

- ロールベースのアクセス制御機能をファイアウォールと統合することで、個々のユーザーにアクセス制御を適用し、適切なリソースとネットワークマイクロセグメントのみにアクセスを限定する
- ユーザーが知っている情報（ユーザー名やパスワードなど）と、ユーザーの所有物（電話、ラップトップ、認証、物理的なセキュリティキー）またはユーザーを識別するもの（指紋や生体情報など）を組み合わせた多要素認証で、アイデンティティを検証する
- 追加のサインオン用画面を利用させる手間と時間を節約し、企業ユーザーを対象としたアイデンティティベースのセキュリティを適用させることで、SSO（シングルサインオン）を有効化する
- ネットワーク接続されたデバイスの特性や振る舞いの監視、そしてソフトウェアアップデートを適用して脆弱性対策を講じることの必要性の喚起により、ネットワーク接続デバイスを認証する
- 認証済のデバイスのみにアクセスを限定し、他のポートをすべてロックする

5. 有線 / 無線アクセスの保護

OT 環境で最も狙われやすいのは、ネットワークスイッチと無線 AP（アクセスポイント）の 2 つです。複数のインタフェースを併用して管理しなければならない単機能セキュリティソリューションを追加して保護するのではなく、セキュリティを考慮した設計が採用され、単一のインタフェースによる一元管理が可能な製品を選択すべきです。

一元管理により、リスク軽減はもちろん、可視化や管理作業に要する時間の短縮を可能にします。

多くの OT 企業では、有線 / 無線 AP を経由した攻撃のリスクが高まりつつあります。ある調査においては、すべての企業が無線や IoT テクノロジーを導入しており、OT ネットワークへの接続もその 1 つとなっています [15]。接続された IoT テクノロジーは平均で 4.7 種類で、最も多いのは GPS による追跡とセキュリティセンサーでした [16]。

包括的なセキュリティプラットフォームに組み込まれたファイアウォールを選択することで、増大したリスクを最小限に抑えることができます。このようなプラットフォームでは、統合されたスイッチや無線 AP に対してきめ細かいセキュリティポリシーを適用し、従業員や機器のグループ別にカスタマイズされた VLAN を制御できます。また、この種類のファイアウォールはサードパーティベンダーが提供するレガシースイッチや無線 AP のプロビジョニングと管理を一元化することも可能です。

アクセスポイントセキュリティの一元管理によってリスクを軽減します。

ファイアウォール、スイッチ、無線 AP では、耐久性も重要なポイントです。分散システムが稼働する送電網や石油パイプラインといった極めて過酷な OT 環境や、地球上で最も暑いまたは寒い場所でも稼働できる設計のデバイスが求められます。防御態勢が不十分だとみなされるために攻撃の標的になりやすいネットワークの末端においては、一元的に作成されたセキュリティポリシーをサポートする機能が必要です。ネットワークエッジにある機器の故障は、単に手間がかかる問題というだけではなく、重大なダウンタイムによるコストも発生するため、迅速な導入によってこのような故障を解決する必要もあります。

包括的なセキュリティプラットフォームは、カスタマイズされた VLAN のグローバル展開を可能にします。

終わりに：OT ネットワークのリスクをプロアクティブに抑制

競争力を維持するために、組織は OT 環境を IT ネットワークに接続しています。ほとんどの組織は、戦略的な IT / OT のコンバージェンスを計画しています。また同時に、計画外の統合や、知られてもいない統合が存在するケースもあります。一例を挙げると、SHINE プロジェクト（SHodan INtelligence Extraction）では、グローバル規模で数年にわたりインターネットをスキャンし、200 万台の OT 接続デバイス（インフラストラクチャがサポートする、HVAC コントローラやシリアルコンバータといった OT 制御デバイスなど）が特定されています [17]。

IT と OT の統合は、戦略的なイニシアティブである一方で、OT のセキュリティ侵害リスクを高めるという側面もあります。フォーマットの経験から考えると、サイバーセキュリティ侵害は、もはや「起こるかどうか」ではなく「いつ起こるか」という問題であるといえます。セキュリティ侵害を完全に阻止することは不可能ですが、ネットワークセグメンテーションによる被害の抑制、トラフィック分析による迅速な検知、アイデンティティおよびアクセス管理や有線 / 無線アクセス制御による頻度の低下といった対策を講じることは可能です。ベストプラクティスに従うことで、万が一攻撃者が OT ネットワークに侵入した場合であっても、被害額やダウンタイムを最小限に食い止めることが可能になります。

[1] 「SCADA / ICS セキュリティリスクが独自調査で明らかに 」、フォーティネット、2019 年 6 月 28 日：
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ ja_jp/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf

[2] 最初の 3 つの産業革命とは、人力から蒸気機関による動力への変革（18 世紀）、蒸気機関から電動の組立ラインへの変革（20 世紀）、オートメーションの台頭（21 世紀初頭）です。「What is Industry 4.0? Here's A Super Easy Explanation For Anyone」、Bernard Marr 氏、Forbes、2018 年 9 月 2 日（英語）：https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/

[3] 「What is Industry 4.0? Here's A Super Easy Explanation For Anyone」、Bernard Marr 氏、Forbes、2018 年 9 月 2 日（英語）：
https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/

[4] 「Manufacturing's next act」、Cornelius Baur 氏および Dominik Wee 氏、McKinsey、2015 年 6 月（英語）：https://www.mckinsey.com/business-functions/operations/our-insights/manufacturings-next-act

[5] 「What the Companies on the Right Side of the Digital Business Divide Have in Common」、Robert Bock 氏、他、Harvard Business Review、2017 年 1 月 31 日（英語）：
https://hbr.org/2017/01/what-the-companies-on-the-right-side-of-the-digital-business-divide-have-in-common

[6] 「SCADA / ICS セキュリティリスクが独自調査で明らかに 」、フォーティネット、2019 年 6 月 28 日：
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ ja_jp/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf

[7] 「IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices」、eSecurity Planetm、2017 年 11 月 8 日（英語）：
https://www.esecurityplanet.com/network-security/iot-security-fail-82-percent-of-companies-cant-identify-all-network-connected-devices.html

[8] 「Vulnerability Analysis of Network Scanning on SCADA Systems」、Kyle Coffey 氏、他、Hindawi、2018 年 3 月 13 日（英語）：https://www.hindawi.com/journals/scn/2018/3794603/ref/

[9] 「Guide to Industrial Control Systems (ICS) Security」、Keith Stouffer 氏、他、NIST、2015 年 5 月（英語）：https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[10] 「ISA Standards: Numerical Order」、International Society of Automation、2018 年 1 月 3 日（英語）：https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards-in-numerical-order/

[11] 「Provide Customers with Advanced Threat Defense Against Email-Based Attacks」、David Finger 著、フォーティネット、2018 年 4 月 26 日（英語）：
https://www.fortinet.com/blog/business-and-technology/provide-customers-with-advanced-threat-defense-against-email-bas.html

[12] 「SCADA / ICS セキュリティリスクが独自調査で明らかに 」、フォーティネット、2019 年 6 月 28 日：
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ ja_jp/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf

[13] 同上

[14] 同上

[15] 同上

[16] 同上

[17] 「Critical infrastructure: Off the web, out of danger?」、Taylor Armerding 著、CIO、2017 年 3 月 22 日（英語）：https://www.cio.com/article/3183643/security/critical-infrastructure-off-the-web-out-of-danger.html

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

EB-Converged-IT-and-OT-202001-R1