FORTINET

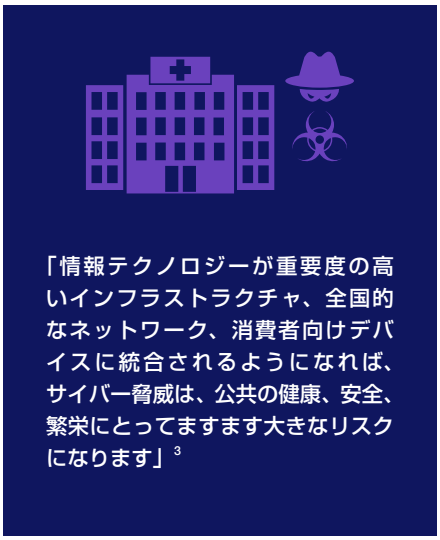
WHITE PAPER

# IT / OT ネットワークコンバージェンスの原因と結果

## 概要

**最近まで、運用テクノロジー（OT）と情報テクノロジー（IT）はまったく別の目的を持ち、相互に独立したネットワーク上にありました。ところが、デジタルトランスフォーメーション（DX）の登場により、コスト削減、生産性の向上、競争力の強化や維持を目的にしたネットワーク統合が進んだのです。現在、ネットワーク機能とデジタル通信を OT 環境に統合し、産業用モノのインターネット（IIoT）デバイスを導入する部門が増加しています [1]。また、これ以外の IT ベースのテクノロジー、機械学習（ML）、ビッグデータも、OT ネットワークに統合されようとしています。**

**現在、OT ネットワークの大半はインターネットに接続されており、大きな脅威にさらされています。攻撃対象領域が拡大したため、サイバー犯罪者、国家的組織、ハッカーは、OT システムをいとも簡単に侵害できるようになっています。これは、OT を標的にしたサイバー攻撃が驚くほど多発していることからも明らかです。実際、過去 1 年間に OT システムの 74% でセキュリティ侵害が発生しており、生産性の低下、売上喪失、ブランドの信頼性低下、知的財産の侵害、物理的な安全性の低下の被害が発生しています [2]。**




## そもそも、OT とは何でしょうか

OT とは、IT を活用して、物理的なプロセス、デバイス、インフラストラクチャを監視および制御するテクノロジーです。OT システムが停止すると、業務の中断から人命に関わるインシデントまで、多大な影響が発生します。IT は、システムとデータの機密性、整合性、可用性を確保します。簡単に言うと、OT が機器を制御するのに対して、IT はデータを制御します。

OT システムは幅広い部門に導入されており、重要なインフラストラクチャの監視から生産フロアで稼働するロボットの制御まで、幅広いタスクを担います。OT システムを構成するハードウェアとソフトウェアは、産業界の環境にある物理的なデバイス、プロセス、イベントを監視または制御することにより、変化を検知し、変更を行います。

ICS（産業用制御システム）は、OT の主要なコンポーネントの 1 つです。ICS には、さまざまなタイプのデバイス、システム、制御機能、ネットワークが含まれ、幅広い産業プロセスを管理します。最も一般的な ICS は、SCADA（監督制御データ収集）システムや DCS（分散制御システム）です。SCADA システムは、分散した拠点などに設置されているセンサーからデータを収集し、データの管理や制御を行う中央のコンピュータに送信します。DCS は、運用環境にあるローカルのコントローラやデバイスを管理します。

OT の最小コンポーネントには、センサー、モニター、アクチュエーターなど、機器そのものや周辺に実装されているコンポーネントなど、多様なものがあります。発電機、パイプライン、ファン、産業ロボットなど、変更を監視および開始する機器などがあり、広く普及しています。このようなセンサーは、IIoT の一例です。

## IT / OT のコンバージェンスが進む理由

DX テクノロジーの推進には、OT システムと IT システムのインタラクションが必要です。プロセッサ、ストレージ、システム管理といった IT コンポーネントは、OT 制御システム、SCADA、OT ネットワークに接続されます。OT と IT のコンバージェンス（統合）により、物理的な機器や IIoT デバイスが収集したデータを、問題の特定や効率化に役立てることができます。さらに、高頻度のデータ収集や、安価なストレージ（パブリッククラウドなど）への格納も可能になります [4]。

このコンバージェンスは、最新テクノロジーの活用を可能にするだけでなく、省スペース化、物理ハードウェアの削減、導入時間の短縮、コスト削減、パフォーマンス向上、IT および OT 部門にあるサイロの解体などを実現します [5]。IT と OT が連携すれば、さらに効率的な最先端ソリューションの提供が可能になるのです。

たとえば、OT と IT のコンバージェンスによって、リモート環境から生産ラインをプログラミング可能となり、週替わりで異なるコンポーネントを製造できるようになります。また、受注後すぐに倉庫から商品を発注することも可能になります。重要度の高いシステムでは、データの分析に要する時間を短縮し、問題の特定を迅速化できます。

## 魅力的な目標である OT

しかしながら、残念なことに OT デバイスとネットワークはセキュリティを念頭に置いた設計になっていません。その理由は、OT がこれまで物理的に隔離され、インターネットに接続されていない「エアギャップ」で保護されてきたためです。ところが、グローバルにネットワーク接続されるようになった OT は新たなリスクやサイバー攻撃の標的となり、単なるデータ漏えいを超える深刻な問題が発生しています。上記の例では、攻撃によって生産ラインや倉庫が乗っ取られて完全に停止してしまう恐れがありますし、送電網や水処理場が標的になる可能性もあります。

製造ラインや倉庫への攻撃は多大な被害をもたらしますが、たとえば食品製造工場にある機器が攻撃されたらどうでしょうか。適切な検査が行われないまま、安全性が確保されていない食品が流通および販売されてしまう危険もあります。また、忍耐強く年月をかけて農作物の種に細工しようとするハッカーが現れるかもしれません。農作物を収穫不能にする細工をすれば、食糧不足が発生しかねません[6]。

市民生活の質を維持するために 100% のアップタイムが求められる重要なインフラストラクチャシステムでも、統合が進んでいます。ところが、DX が推進する OT イニシアチブは、極めて重要な運用資産が壊滅的なセキュリティ侵害の被害を受ける可能性を発生させます。このような OT システムは、発電所、鉄道、運輸システム、交通管理、水処理施設、緊急対応システムといった重要なインフラストラクチャを制御しています。

**「IT と OT を組み合わせることで、重要度の高いシステムの可用性を確実に高めることができます。OT がプロセスの継続的な実行を保証し、IT がハードウェアシステムの可用性、常時接続性、サイバーセキュリティ、アプリケーション、そしてデータの分析を支援します」[7]**

このような危険性を認識した米国は、2013 年、「PPD-21（大統領政策指令第 21 号）：重要インフラのセキュリティと回復力」を公布しました。その目的は、脆弱性の低減、脅威の阻止、攻撃による被害の最小化を実現し、米国内にある重要なインフラストラクチャを堅牢化し、保護することにあります。この指令では、州政府、国家、地方自治体、専門組織や地域の組織、インフラストラクチャの公的 / 私的な所有者、運用者が、この責務を共有すべきだとしています[8]。

さらに、この指令の中で重要なインフラストラクチャとして次の 16 項目が指定されています[9]。

| | | | |
|---|---|---|---|
| 化学分野 | ダム | 金融サービス | 情報テクノロジー |
| 商業施設 | 防衛関連産業基盤 | 食品 / 農業 | 原子力発電 / 核物質貯蔵 / 廃棄施設 |
| 重要製造設備 | 救急サービス | 官公庁施設 | 運輸システム |
| 通信 | エネルギー | 医療および公衆衛生 | 上下水道設備 |

これまでのサイバー犯罪者の行為はデータの窃取が中心でしたが、OT のセキュリティが十分ではなく、混乱を起こすことが可能であるという認識が広がったため、OT 環境が攻撃の標的になりつつあります。このような犯罪者は、OT ネットワークやコンポーネントに標的を絞り、巧妙で大きな被害をもたらす攻撃を開発しています。

## OT に混乱をもたらす攻撃の例

重要インフラストラクチャの攻撃は、実際に被害が発生したケースと危うく回避できたケースのいずれにおいても、世界中で驚くほどの件数が発生しています。ここで、いくつか例を挙げます。

- 2017 年、サウジアラビアにあるとされたワークステーションをサイバーテロリストが乗っ取り、リモートから制御可能な状態になりました。ICS 用に構成したマルウェアを使用し、安全システムを無効化することで爆発を企てたのです。報道によれば、この攻撃はコーディングのエラーが原因で失敗したとされています[10]。
- 2016 年には、ニューヨーク市のライ・ブルックに位置し、洪水を防ぐボーマン・アベニュー・ダムの制御システムにイランのハッカーが何度もアクセスし、水位、温度、水位を制御する水門の状態に関する情報を入手しました。理論的には、このハッカーがダムを制御できるはずでしたが、メンテナンスの目的で水門は手動でシステムから切り離されていたため、難を逃れました[11]。
- 2015 年にはウクライナの送電網が攻撃され、大規模停電が発生しました。ハッカーは 3 つの電力会社のシステムに侵入し、国内 3 つの地域の電力をシャットダウンしたのです。6 時間に及ぶ冬場の停電で、250 万人近い市民が大きな影響を受けました[12]。

原子力施設の爆発、長時間にわたる断水や停電、運輸や交通システムの停止は、社会や経済に壊滅的な影響を与えかねません。

## OT におけるサイバーセキュリティの現状

OT ネットワークの保護は極めて重要であるにもかかわらず、多くの OT ネットワークではセキュリティ侵害が多発しており、この状況は今後も続くと考えられます。堅牢で包括的なサイバーセキュリティの制御機能が提供されているにもかかわらず、なぜハッカーはシステムに侵入できるのでしょうか。

フォーティネットは先頃、製造、エネルギー / 水道や光熱、医療、運輸の各業界の大手企業を対象に調査を行いました。工場などの設備運用 / 製造の責任者に参加いただいたこの調査から、OT のサイバーセキュリティの現状を示す興味深いデータを得ることができました[13]。ここからは、OT 環境のセキュリティ態勢を明らかにする調査結果をいくつかご紹介します。

- **OT 環境を狙ったサイバー攻撃は、広範囲で深刻な影響を及ぼしている：**OT 組織の 4 分の 3 以上（74%）が、過去 12 か月の間にセキュリティ侵害を経験しています。これは、生産性の低下、売上喪失、ブランドの信頼性低下、知的財産の侵害、物理的な安全性の低下を引き起こしています。

- **サイバーセキュリティの欠如がリスクを増大させている：**回答者の 78% の組織では、OT 環境のサイバーセキュリティの一元的な可視化が不十分です。ロールベースのアクセス制御を実装していない組織が全体の 65%、多要素認証や社内ネットワークのセグメンテーションを導入していない組織は半分以上にのぼります。
- **環境の急速な変化や人的リソースの不足が、OT セキュリティ態勢の改善を阻んでいる：**OT リーダーの 3 分の 2 近く（64%）が、急速な変化への追随を最大の課題としており、半分近く（45%）がスキルを持つ人材の不足に悩んでいます。
- **OT 部門では、OT のサイバーセキュリティに注力している：**回答者の 70% が、「翌年には、CISO の指揮の下で OT サイバーセキュリティ対策を講じる計画がある」としており（現在 OT セキュリティを担当する CISO はわずか 9%）、62% の組織でサイバーセキュリティ予算が増加しています [14]。

## サイバーセキュリティソリューションの評価において OT リーダーが検討すべき機能

今日の OT ネットワークを保護するためには、非常に幅広い要件があります。IT と OT のネットワークにはさまざまな目標があり、多様なデバイスが存在しますが、1 つのセキュリティソリューションでネットワーク全体を保護することが可能です。つまり、セキュリティソリューションの要件は、攻撃対象領域全体を保護する機能、透過的な可視化機能の完全な統合、脅威の検知、防御、修復を自動実行する機能です。

ここからは、OT 環境の保護に不可欠な最も重要な 5 つのセキュリティ機能について解説します。

1. **ネットワークに接続するあらゆるデバイスを識別する：**認識できないデバイスや未知のデバイスを保護することは不可能です。したがって、セキュリティ戦略の第一歩は、すべてのデバイスを特定し、カタログを作成することにあります。
2. **ユーザーのアイデンティティとロールをベースにしたアクセス制御を確立する：**OT 環境では、アクセスするすべてのユーザーを識別することが重要です。特権レベル、アクセス可能なデバイスとアプリケーション、許可する操作を、文書にまとめる必要があります。
3. **ネットワークをセグメント化する：**システムとデバイスのセグメント化、横方向のトラフィックの監視、脆弱性や感染したデバイスの特定と隔離を行うには、OT インフラストラクチャの詳細を把握する必要があります。
4. **通信を暗号化する：**データベース、管理 / 制御システム、その他の接続デバイス間の通信を保護するには、トラフィックを暗号化する必要があります。メッセージやプロトコルへのアクセスを阻止することで、正当なコマンドを模倣するスクリプトの開発を阻止できます。
5. **IIoT を保護する：**IIoT デバイスは、セキュリティが不完全なことで知られています。IIoT デバイスが使用する通信プロトコルを特定し、セグメント化と保護を実行するセキュリティのリソースが必要です。

## その強化が急務な OT セキュリティ

IT ネットワークを介して OT 環境が攻撃されている今日、攻撃対象領域全体を保護できるセキュリティを導入することがますます重要になっています。その実現には、可視性、制御、コンテキスト認識の機能を備えた包括的な統合セキュリティのアプローチが必要です。民間の産業分野や公共機関で運用されている重要度の高いインフラストラクチャの OT が停止すれば、デバイスレベルとシステムレベルのいずれかを問わず、深刻な影響が発生します。

フォーティネットの OT に関する情報 Web サイトでは、フォーティネットが提供する包括的な OT ソリューションをご紹介しています：
https://www.fortinet.com/jp/solutions/industries/scada-industrial-control-systems.html

[1] 「Resolving the Challenges of IT-OT Convergence」、John Maddison 著、CSO Online、2018 年 6 月 21 日（英語）：https://www.csoonline.com/article/3283238/resolving-the-challenges-of-it-ot-convergence.html
[2] 「State of Operational Technology and Cybersecurity Report（運用テクノロジーの現状とサイバーセキュリティレポート）」、フォーティネット、2019 年 3 月 15 日（英語）：https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf
[3] 「National Intelligence Strategy of the United States of America」、2019 年（英語）：https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf
[4] 「IT/OT Convergence: Linking Legacy to an Industrial Internet of Things World」、Craig Resnick 著、ARC Advisory Group、2019 年 7 月 13 日にアクセス時の情報（英語）：https://arcadvisorygroup.sharepoint.com/sites/extranets/client-portal/arc-forums/Orlando2017/IT-OT Convergence-Linking Legacy to an IIoT World.pdf
[5] 「7 ways industries benefit from OT and IT Convergence」、Tom Bradicich 著、IIoT World、2017 年 9 月 6 日（英語）：https://iiot-world.com/connected-industry/7-ways-industries-benefit-from-ot-and-it-convergence/
[6] 「Manufacturing cyberattacks could cripple the UK」、Nafeez Ahmed 著、Raconteur、2019 年 2 月 19 日（英語）：https://www.raconteur.net/manufacturing/manufacturing-cyberattacks
[7] 「IT/OT convergence: resistance is useless」、Suzanne Gill 著、Control Engineering Europe、2018 年 6 月 29 日（英語）：https://www.controlengeurope.com/article/155615/IT-OT-convergence--resistance-is-useless.aspx
[8] 「Presidential Policy Directive 21 (PPD-21)」、Corinne Bernstein 著、TechTarget、2019 年 7 月 13 日にアクセス時の情報（英語）：https://whatis.techtarget.com/definition/Presidential-Policy-Directive-21-PPD-21
[9] 「Presidential Policy Directive -- Critical Infrastructure Security and Resilience」、2013 年 2 月 13 日発行（英語）：https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[10] 「Cyber attacks targeting critical infrastructure」、Michael A. Mullane 氏、IEC e-tech、2019 年 2 月（英語）：https://iecetech.org/index.php/Technology-Focus/2019-02/Cyber-attacks-targeting-critical-infrastructure Cyber attacks targeting critical infrastructure
[11] 「Rye dam cyberattack: 5 things to know」Jordan Fenster 氏、2016 年 3 月 24 日（英語）：https://www.lohud.com/story/news/local/westchester/rye-city/2016/03/24/rye-dam-cyberattack-5-things-know/82207990/
[12] 「Cyber attacks targeting critical infrastructure」、Michael A. Mullane 氏、IEC e-tech、2019 年 2 月（英語）：https://iecetech.org/index.php/Technology-Focus/2019-02/Cyber-attacks-targeting-critical-infrastructure
[13] 「State of Operational Technology and Cybersecurity Report（運用テクノロジーの現状とサイバーセキュリティレポート）」、フォーティネット、2019 年 3 月 15 日（英語）：https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf
[14] 同上

FORTINET
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© 2019 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。

WP-OT-Network-Covergence-201911-R1