国際情勢の緊張により増大するOTセキュリティリスク

www.pwc.com/jp

制御（Operational Technology：OT）システムは、国際情勢の緊張を背景とするサイバー紛争において主要な標的となっており、重要インフラや事業活動に関するリスクが高まっています。こうした脅威から組織を防衛するために、OTセキュリティの責任の所在とリソースの分配に関して経営層が足並みをそろえ、ネットワークの分離を徹底し、OT環境全体の可視性を高めるべきです。

海外の敵対者やサイバー犯罪者、アクティビストによるサイバー攻撃が増加の一途をたどっており、産業インフラや重要インフラを担うOTシステムは脅威にさらされています。OTシステムを標的にするマルウェアは、AIに対応することで一層高度化し、エネルギー供給網から製造・物流に至るまで、あらゆる分野を混乱に陥れています。国家の支援を受けた攻撃者は、長期的に攻撃活動を続けています。その手法は、認証情報の収集（クレデンシャルハーベスティング）や環境寄生型（Living Off The Land：LOTL）攻撃によって、ITやOTのシステムに侵入し、破壊工作（サボタージュ）やスパイ活動（エスピオナージ）を行うものです。このように高度化する脅威を前に、米国をはじめとする各国は先般、共同指針を発出しました。新たに出現したリスクの低減を目的とするこの指針には、OTシステムにAIを安全に組み込むための原則が記されています。

近年発生したOTシステムに対するサイバー攻撃の事例

- ジャガー・ランドローバーでの生産障害（2025年3月）：サイバー攻撃により、生産の停止、大規模な操業休止を余儀なくされ、自動車サプライチェーンの脆弱性を露呈した。
- 米国の上下水道インフラの脆弱性を突いた攻撃（2024年9月）：脅威アクターは、基本的な戦術を用いて上下水道システムの脆弱性につけ込み、生活に不可欠なサービスが継続的にリスクにさらされている実状を浮き彫りにした。
- ウクライナの電力網に対する攻撃（2024～2025年）：複数のサイバー攻撃により配電系統が麻痺し、大規模停電が発生。紛争地域におけるエネルギーインフラの脆弱性が明らかに。
- 米国の変電所への攻撃（2023年）：カリフォルニアおよびノースカロライナの両州の変電所が侵害され、米国の電力網の安全性が脅威にさらされた。
- イスラエル、イラン両国間のサイバー紛争（2024～2025年）：重要インフラを狙ったサイバー攻撃が継続。両国における地政学的緊張とOTシステムにおけるリスクが判明した。

OT環境に対する脅威の増大に伴い、セキュリティ戦略の実効性が求められています。重要システムの防御に手落ちがないよう、多くの組織が懸命に努力しています。課題は、個々の脅威への対処にとどまりません。多くの場合、組織のガバナンスや運営、コンプライアンス、物理セキュリティの弱点にまで及び、脆弱性は相互に関連しています。このような課題を解決するためには、事後対応的な消火活動から、日常的な防火活動による未然防止的でレジリエントなセキュリティのあり方への転換が必要です。

地政学的紛争とサイバー戦争

世界各国で、OTシステムがサイバー紛争に巻き込まれる事例が続いています。OTシステム自体が標的とされることもあれば、副次的に被害を受けることもあります。

- 国の重要インフラ（Critical National Infrastructure：CNI）事業者とその他の（non-CNI）事業者は、OTシステムの脆弱性と防御メカニズムの限界に起因する課題に引き続き直面しています。
- エネルギー、公益事業、輸送などの重要インフラ事業者を戦略的に狙うサイバー攻撃が増加をたどっています。
- 製造業、航空宇宙産業、消費財産業など、重要インフラ部門以外の事業者も、このような課題を同様に抱えています。このような事業者は、OEM企業と部品やサプライチェーンを共有していることから、波及的なリスクがあります。
- 最新のランサムウェアグループは、IT資産を暗号化したり、生産や安全制御を混乱させたりすることを狙い、より多くのOT環境を標的にしています。

規制の重圧

各国の政府と産業団体は、サイバーセキュリティとOTセキュリティに特化した要件と基準の強化に向けて動いていますが、各国の足並みがそろっているわけではありません。各国の規制間に相違があった場合、規制の改正時の対応や、コンプライアンス計画の策定に際して問題を生じることがあります。

- NIS2指令（EU）：管理を義務付ける重要インフラ事業者の範囲を拡大するとともに、インシデント報告のタイムラインとエグゼクティブの説明責任を規定しています。
- 米国サイバーセキュリティ・社会基盤安全保障庁（CISA）、米国運輸保安庁（TSA）、米国環境保護庁（EPA）：OTに特化したレジリエンスおよびインシデント対応目標を導入しています。
- IEC 62443：産業用オートメーションおよび制御システム（IACS）のサイバーセキュリティに関する国際標準規格になりつつあるものの、適用状況は国によって大きく異なります。最近行われた改訂では、重要インフラ事業者に共通する一貫した基準を採用することの重要性が強調されています。

レガシーシステムの脆弱性

数十年前の古いOTシステムが、技術的負債を抱えたまま、サイバーセキュリティの成熟度に適合することなく、最新のデジタルインフラに接続されています。

- OTシステムの多くは、設計に際し、セキュリティよりも運用の効率性を重視しています。
- サードパーティのインテグレーター、ベンダー、メンテナンスプロバイダーがOTネットワークにアクセスできることがしばしばあり、しかも頻繁にリモートからアクセスしています。こうした状況はアタックサーフェスを拡大し、監視や管理が困難になるリスクにつながります。SolarWindsやMOVEitなど、よく知られているサプライチェーン攻撃は、このような脆弱な状態を突かれると、下流組織のOT環境に大きな影響が及ぶことを認識させるものでした。
- エッジコンピューティングを採用してオンサイト分析やデータモデリングを実現することによって、OT環境内でエンドポイントを新たに強く結合できます。多くの場合、基幹システムに適用するような厳格なセキュリティ管理は必要とされません。

物理セキュリティのリスク

OT環境では、スタッフがオンサイトで操作や保守を行わねばならないことがしばしばありますが、このような物理的アクセスは大きなリスクになります。安全が確保されたデータセンターに格納されるITシステムと違って、OT機器は、安全管理水準にばらつきがある現場に分散配置されていることがあります。

- OT資産は、生産現場、工場やその他の重要インフラの現場に設置されていますが、このような場所は、物理セキュリティやモニタリング管理が不十分であることが少なくありません。
- オンサイトのスタッフ（オペレーター、請負業者、ベンダーを含む）は、管理手順を省略したり、間違ったり、対策を回避したりすることがあり、システムがリスクにさらされる可能性があります。
- 物理的アクセスが可能な場合、攻撃者に対して、デバイスへの直接接続（USBプラグアンドプレイ、ダイレクトコネクションなど）、機器の改ざん、マルウェアの導入のチャンスを与えてしまう可能性があります。

OTセキュリティにおいて見逃されがちな側面

多くの組織のOTセキュリティは進展していますが、誰も気づかないところに重大な落とし穴が隠されているかもしれません。それは一時的な不具合というよりも、ガバナンスや可視性の問題、組織的な弱点に起因し、本来ならば有効であるはずのセキュリティ対策の実効性が損なわれていることが懸念されます。

1. ITとOTの融合

ITとOTの融合はとどまることがなく、ネットワーク、データフロー、インフラの共有化が進んでいます。OTシステムは、収益を生み出すプロセスや生産過程に不可欠な存在ですが、多くの組織では、ITとは切り離された領域、またはITに従属する領域と見なされています。こうした認識や扱いが、セキュリティの保護策、改善のための投資、リソースの配分において、ITとOTに不均衡が生じる原因になっています。加えて、セグメンテーション（分離）、可視化、保護対策が不十分な状況で、ITとOTの融合が進められると、ITへの脅威が重要なOT資産に波及する可能性（またはOTへの脅威がIT資産に波及する可能性）が高まります。

このような脆弱性に対処するため、ITとOTの融合が運用に及ぼす影響に関して戦略を策定し、利益を生み出す資産を保護するためにOTセキュリティへ投資することが重要です。ITとOTの融合では、セキュリティが最優先です。OT環境とネットワークサービスをできるだけ切り離すことでアタックサーフェスを減らし、Blast-Radiusのような脆弱性を狙った攻撃の可能性を限定的にします。

2. OT資産の管理

OT環境の多くは、堅牢な資産インベントリを備えていません。理由としては、ネットワークの可視性に限りがあること、ネットワークの管理がなされていないこと、最新のSIEMやネットワーク検知ツールに適合したテレメトリーが不足していることが挙げられます。経年したOT設備の場合、侵襲的なモニタリングの負荷に耐えられず、アクティブな資産検出手法を限定的にしか適用できないことが少なくありません。可視性が隅々まで確保されない限り、OT環境全体にセキュリティ対策を講じることは難しくなります。

このような問題を克服するため、OTネットワークのセキュリティモニタリングを優先的に実行して、ネットワークトラフィックをパッシブスキャンします。このアプローチは、信頼性のある資産インベントリの作成や脆弱性の特定の一助になる他、接続されているOTシステムにおいて、脅威を特定、監視し、対応するためにアラートを発することもできるようになります。

3. セキュリティに対する当事者意識とスキル

多くの場合、OTセキュリティに係る責任はCISOが負うのに対し、リスクの説明責任は、セキュリティ、オペレーション、エンジニアリング、コンプライアンスの各部門に跨ることが一般的です。このような細分化が進むと、予算の不足、意思決定の停滞、一貫性のないインシデント対応につながる恐れがあります。同時に、OT環境に求められるハイブリッドな専門知識を有する人材を確保し、維持するための取り組みの実効性が損なわれる懸念もあります。多くの組織が、エンジニアリング、安全、ITといったさまざまな制約が複雑に絡み合う状況を理解している専門家の発掘に苦労しています。教育と人材開発への集中的な投資、組織のリーダーによる取り組みへのコミットメントがない限り、スキルの不足と部門間連携の齟齬によってOTセキュリティは損なわれ続けます。

このような状況を乗り越えるには、経営層にOTセキュリティの予算権限に対する明確な当事者意識を持たせる必要があります。また、専門領域を横断するクロストレーニングや実践教育の場を設けることにより、OTに関する専門能力を開発することも求められます。

4. ベンダーの透明性とリスク

多くの場合、重要なOTシステムの管理にはベンダーが関与しますが、ベンダーとの関係性は明瞭ではありません。OEM企業は、ファームウェアのアップデート、診断を目的とするアクセス、デバイス挙動の可視性を管理します。そのため、独自にインシデントの調査、資産の監視、制御の確認を行うとしても、実施できることが限定されることがあります。

このようなリスクを管理するため、透明性の確保とセキュリティを明確に規定する条項がベンダーとのサービスレベル契約（SLA）に盛り込まれていることを確認します。また、テレメトリーの共有とアクセスの標準化を要求します。

5. OTネットワークのセグメンテーション

OTのネットワークとITのネットワークは、しばしばフラットなネットワーク上で混在しており、双方がサイバー攻撃に対して脆弱な状態になります。OTネットワークのセグメンテーションは、組織のOT環境を複数の独立したセキュリティゾーンに分割することで、脅威が重要な資産やプロセス全体に広がるリスクを低減します。この体系的なアプローチにより、潜在的な侵害を局所化して封じ込め、防御力を強化し、重要業務の継続性を維持し、攻撃発生時の財務的影響を軽減することが可能になります。

OT環境でセグメンテーションを実施するには、製造現場を複数のセキュリティゾーンに分割します。これにより、潜在的な侵害を局所化し、重要なプロセスを保護し、攻撃発生時の業務停止リスクを軽減できます。

6. クラウドコネクティビティとエッジデバイス

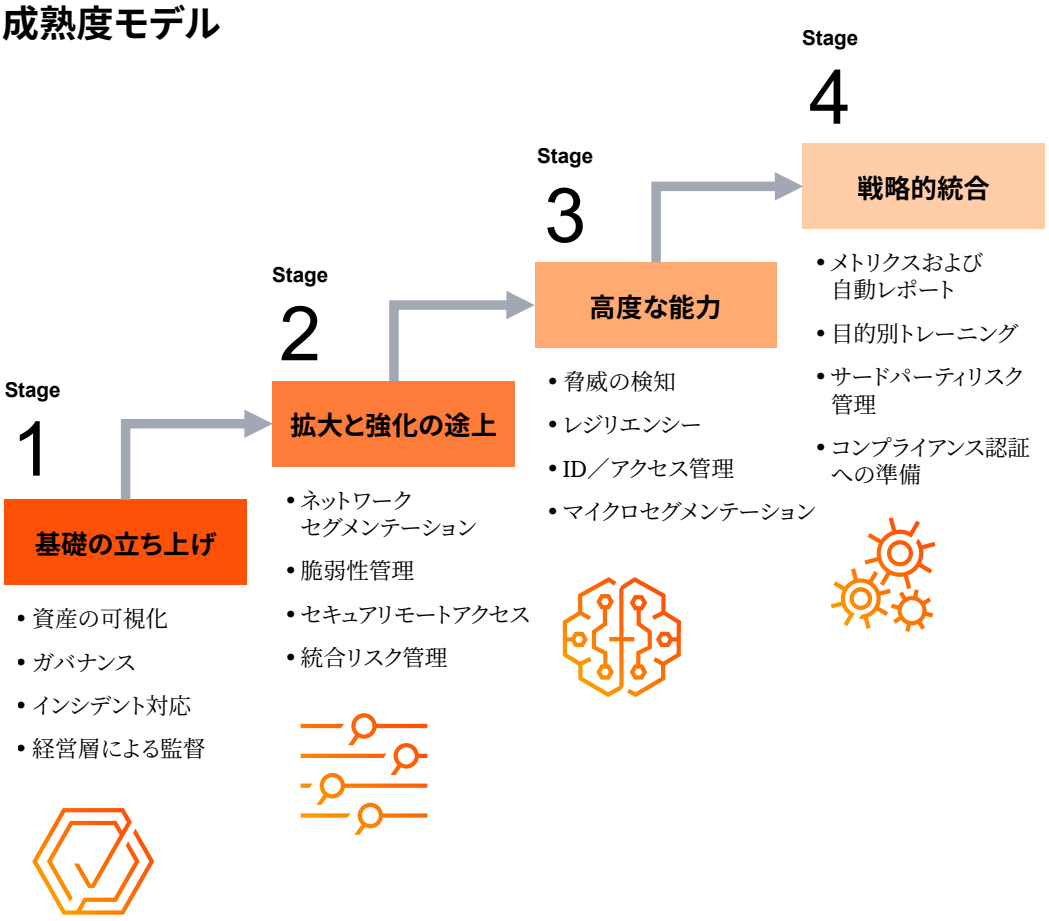
デジタルトランスフォーメーション（DX）の取り組みの一環として、企業は予知保全、AIを活用した最適化、遠隔操作を目的に、運用データや制御機能をクラウドへ移行しようとしています。しかし、これにより、従来は分離されていた環境において、インターネット接続やサードパーティのクラウドセキュリティ、ID連携といったリスクにつながる新たな依存関係が生じる可能性があります。

DXが進むにつれて、運用環境内のコネクティビティはさらに高まり続けています。セキュリティをDXの“設計段階から”組み込むことがますます重要になります。技術的に可能な範囲でネットワークセグメンテーションを織り込み、エッジセキュリティに関する規格（OPAS規格など）の最新動向をチェックしましょう。

OTセキュリティにおける適用可能な能力の構築

OTセキュリティは一度きりの取り組みではありません。組織は、問題が生じてから対処する事後処理型の対応から、将来を見据えた拡張性のあるセキュリティプログラムを推進すべきです。以下に示すのは、組織でOT環境のセキュリティを確保するための4段階のアプローチです。それぞれの成熟度レベルは、長期的なレジリエンスのための技術とガバナンスの両面で構成されます。

成熟度モデル



基礎の立ち上げ

IT環境の保護に必要なインフラストラクチャと可視性を構築する段階

- **資産の可視化とモニタリング：**OTに関連するデバイスとシステム（管理されていない資産やベンダー所有資産を含む）を継続的かつリアルタイムに監視します。運用環境を正確かつ動的に把握することで、セキュリティ状態の監視を実現します。
- **ガバナンス：**OTセキュリティの管理を行うための正式なガバナンスフレームワークを策定・導入します。このガバナンスフレームワークには、OTセキュリティの運用モデル、RACIによる明確な役割と責任、強固な方針と経営層の監督下で実行される標準が含まれます。
- **インシデント対応計画：**OTに関連するサイバーセキュリティイベントに対応するために、OTに特化したプレイブックを作成します。また、部門横断的な机上訓練を実施します。
- **経営層による監督：**経営層へのリスク報告や経営会議におけるリスク戦略の検討にOTセキュリティのリスクを含めます。

拡大と強化の途上

可視化から対応へのシフト。脅威の検知と阻止に向けた運用態勢を強化する段階

- **ネットワークの分離：**ITとOTのネットワーク間に強固な境界を構築し、クロスコンタミネーション（相互汚染）や脅威が横展開するラテラルムーブメントを防止します。
- **脆弱性の管理：**OTに存在する既知の脆弱性を特定・評価します。たとえパッチを適用できない場合であっても、代替策を適用します。
- **セキュアなリモートアクセス：**OT環境に適したリモートアクセスの強固な管理策を導入します。多要素認証の導入、通信の暗号化、アクセス権限の厳格化などにより不正侵入を防止します。
- **統合リスク管理：**OTセキュリティのリスク管理を組織全体のリスク管理の枠組みに組み入れます。これにより、OT固有のリスクをビジネス目標と整合した形で継続的に特定、評価、低減できる態勢を構築します。

高度な能力

検知からプロアクティブ防御へのシフト。攻撃者の滞留時間を短縮し、可視性をさらに高める段階

- **脅威の検知：**センサーやアナリティクスを展開し、OT環境全体を通じて異常な挙動を監視します。
- **レジリエンス：**確実なバックアップを設計します。「技術的故障」のみならず「サイバーセキュリティイベント」からの復旧操作もテストします。
- **ID・アクセス管理（IAM）とアクティブディレクトリのセグメンテーション：**厳格なIAMを導入し、ディレクトリサービスを分離することで、アクセスを制限し、OTシステムのアタックサーフェスを減らします。
- **OTネットワークのマイクロセグメンテーション：**OTシステム内に、機能やリスクに応じた管理区域（ゾーン）を設けることにより、OTシステム内の移動を制限します。

戦略的統合

OTセキュリティを企業の最上位のリスク管理とガバナンスに組み入れる段階

- **メトリクスおよび自動レポート：**OTセキュリティに関連する重要業績評価指標（KPI）を定義して、継続的に追跡します。自動化されたレポートにより、タイムリーで行動につながるインサイトを出力し、継続的な改善と経営層による監督を促します。
- **目的別のトレーニングと意識向上：**OTセキュリティのリスク、先進的な実践、運用上の制約に的を絞った専門教育プログラムを開発・提供することによって、スタッフの能力開発とヒューマンエラーの減少を目指します。
- **サードパーティリスク管理：**OTシステムベンダーやサービスプロバイダーに由来するサイバーセキュリティリスクの評価と管理を行うために、契約時の要件、透明性の確保、セキュリティ管理責任の分担を含む、厳格なプロセスを確立します。
- **コンプライアンス認証の準備：**公式な監査や業界に応じた認証（NIS2、IEC 62443、ISO 27001のアドオン規格など）に向けて準備します。

謝辞

本レポートの作成に当たり、Morgan Adamski、Harshul Joshi、Amanjit Makesh、Scott Schill、Omar Sherin、Sean Sutton、上村益永の各氏からご協力をいただきました。

PwCグローバルネットワーク

Sean Joyce
Principal, Global Cybersecurity & Privacy Leader
PwC米国
Email

あとがき：日本の読者の皆様へ

本稿は、2025年春にPwCグローバルネットワークでOTセキュリティをリードする英国、米国、日本、インドのリーダーが集まり、各国・地域の実情を持ち寄り、OTセキュリティに関する脅威の高まり、リスク、対策の難しさ、課題、進化に向けた提言について、ディスカッションした内容をまとめたものです。

これからOTセキュリティに取り組む企業の皆様におかれましては、リスクの大きさや検討すべき事項の多さと幅広さ、難しさに圧倒されてしまう場面もあるかと思いますが、本稿が少しでもヒントや希望になることを願っています。

また、すでにOTセキュリティに取り組まれている企業の皆様は、共感していただける部分、言うは易く行うは難しいと感じられる部分、さまざまだと思いますが、少しでも皆様の活動の一助になれば幸いです。

OTセキュリティは、複雑な背景を持つ難しい経営課題だと考えています。私たちは今後も、PwCグローバルネットワークの知見を集約し、各国・地域の事情に落とし込み、クライアントと共に実践し、新たな知見を創出することを通じて、皆様の課題解決に貢献します。

pwc

日本のお問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約13,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、クライアントが複雑性を競争優位性へと転換できるよう、信頼の構築と変革を支援します。私たちは、テクノロジーを駆使し、人材を重視したネットワークとして、世界137の国と地域に364,000人以上のスタッフを擁しています。監査・保証、税務・法務、アドバイザリーサービスなど、多岐にわたる分野で、クライアントが変革の推進力を生み出し、加速し、維持できるよう支援します。

本報告書は、PwCメンバーファームが2026年1月に発行した『Geopolitical shifts amplify OT security risks』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。オリジナル（英語版）はこちらからダウンロードできます。
https://www.pwc.com/gx/en/issues/cybersecurity/geopolitical-shifts-amplify-ot-risks.html

日本語版発刊年月：2026年3月　　管理番号：I202601-08