IT と OT の融合に伴う OT セキュリティの課題と対策

森 下 直 樹，白 木 啓 子

1. はじめに

人工知能（AI），デジタルツインなどのデジタル技術の進展や，製造・サプライチェーンの連携といったエコシステム化が進むことで，情報技術（Information Technology：以下，IT）と運用技術（Operational Technology：以下，OT）の融合が進んでいる．この融合により，製造業やエネルギー分野において，生産性や品質の向上，さらには現場要員の削減などが実現されている[1]．

OT とは，工場や発電所などに使われるシステムや設備を最適に稼働させるための技術やその装置の総称である．OT の目的は，物理的なプロセスを安全かつ効率的に動かすことであり，リアルタイム性や長期運用（10年以上）といった特性を持つ．

IT と OT の融合により，現場で取得した膨大なデータをクラウドなどのデジタル空間で分析し，その結果を現場にフィードバックすることで，デジタルツインなどのサイバーフィジカルシステム（CPS）を構築することができる．その結果，生産ラインを最適化し，工場生産の可視化を実現することができる．具体的には，センサーや機械から収集した稼働データをクラウドで解析し，その結果を即座に現場へ反映することで，遠隔監視や即時の意思決定ができるようになる．さらに，エネルギー消費や稼働率などの KPI を可視化することで，ボトルネックを特定し，プロセス改善に活かすことができる．加えて，スキル・役割・導線を考慮した人員配置のシミュレーションを行うことで人員の最適化を実現できる．このように，IT と OT の融合が，経営と製造現場の乖離を解消し，スマートマニュファクチャリング（生産プロセスの可視化・自動化・最適化）の発展を促進する．それを発展させるには，現場のデジタル情報の収集が不可欠であり，IT と OT の融合はますます重要になってくる[2]．

しかしながら，これまでの OT は閉鎖した環境で運用されてきたため，生産設備の安全かつ安定した稼働を最優先とした設計がなされており，外部からの影響やサイバー脅威に対する考慮は最小限にとどまっている．IT において必須とされるセキュリティ機能を欠いた通信プロトコルが利用され，侵入後の被害を拡大させる恐れがあることから，サイバー脅威への対策が急務となっている．本稿では，IT と OT の融合によるメリット，ならびにそれに伴うデメリットと対応策について述べる．まず，2章で IT と OT の融合によるメリットを説明し，3章で両者の違いに触れた後，4章で融合によって生じる問題を述べる．5章で OT のセキュリティ対策，6章でインシデント対応のために求められる全社的な体制について述べる．

2. IT と OT の融合がもたらすメリット

IT と OT の融合により，生産のボトルネックを特定し，生産効率を向上させることができる．また，製品不良の要因を特定して製品品質を管理することができる．製品品質の判別に AI を利用することで属人化を解消し，それらの作業を自動化することで，人材不足の解消も含めて，多くのメリットが得られる．これらのメリットは単に期待される効果ではなく，現場の OT 機器やセンサーからのデータを継続的に収集・集約し，IT 側の解析基盤（AI や分析モデル）で傾向・異常・予兆を検出したうえで，その結果を現場へ迅速にフィードバック（制御指示や運用改善）する一連の仕組みによって実現される．以下の節で具体例を詳述する．

2.1 データドリブン経営

データドリブン経営とは，データに基づいて迅速な意思決定を行う経営手法である．その一例として，現場の OT から取得したリアルタイムのデータを IT 側で集約・分析することで，経営層や管理者は生産状況を可視化して的確な意思決定ができるようになる．センサーや機械から集まる稼働データをクラウドで解析し，その結果を即座にフィードバックすることで，工場の生産状況を素早く把握することができる．また，IoT で収集したリアルタイムデータにより，遠隔監視や即時の意思決定ができるため，生産効率の向上やダウンタイムの削減が実現できる．エネルギー消費や稼働率などの KPI を可視化することで，ボトルネックを特定し，プロセス改善に活かすことができる．

2.2 AI による予知保全

製造装置や設備のセンサー情報を蓄積し，AI で解析することで，故障の予兆を検知し，事前に保守対応を行う予知保全が実現できる．従来の定期点検や事後保全に比べて，必要最小限の交換や修理で，設備のダウンタイム短縮と保守コスト削減につながる．例えば，トヨタ自動車株式会社（以下，トヨタ自動車）では，機械の劣化状況を AI が予測し，部品交換の頻度を必要最小限に抑えることで，保全業務の効率化と保守費用の削減を実現している．また，花王株式会社では製造プロセスの異常を AI が自動検知し，オペレーターにアラートを出す仕組みを導入し，熟練者でなくとも品質を維持できるように支援している[3]．

2.3 プロセス改善・生産性向上

OT から収集された稼働データや品質データを分析することで，製造プロセスを最適化することができる．ライン上のセンサーデータを解析して不良品発生の原因を特定・改善し，機械の稼働パターンから最適な生産スケジュールを導き出すことができる．データに基づいて工程全体を調整することでムダやバラツキを削減し，品質と生産性の向上が期待される[4]．

デジタルツインを用いて生産ラインをシミュレーションし，レイアウトの変更や設定の調整の効果を事前に検証することができる．これにより，生産工程全体の継続的改善が

データドリブンで行なわれ，製造のリードタイム短縮や在庫の圧縮が実現される．

2.4　人手不足の解消・技能の伝承

日本の製造業では，少子高齢化に伴う人材不足や熟練技能者の高齢化が深刻な課題となっている．その課題に対して，IT と OT の融合による自動化・効率化は，限られた人員でも生産を維持・向上させる手段となる．

例えば，AI 画像検査装置によって人間の目視検査を代替し，AGV（自動搬送車）や協働ロボットを用いて搬送・組立作業を自動化することで，単純作業に割いていた人手を削減できる．また，現場のノウハウや報告書などを IoT データとして蓄積・分析することで，暗黙知を可視化し新人育成に活用することもできる．技能者の勘所をデータとしてモデル化し，作業手順の標準化や MR/AR 技術による支援システムに組み込むことで，ベテランの知見を若手に継承しやすくすることができる[5]．

3.　IT と OT の違い

IT と OT では，その目的や動作環境の違いから，情報セキュリティの優先順位が異なる．工場の制御システムやインフラ監視システムなどの OT システムでは，物理的プロセスを直接制御・監視するため，安全性や継続稼働が最優先となる．一方，企業の情報処理システムなどの IT システムは機密性の保持が最優先であり，データの処理や保存を主目的として設計されている．この違いにより，両者のパフォーマンス要件，可用性要件，リスク管理の重点，運用方法などに大きな差異が生じている．以下の各節で，IT と OT の違いを 10 の観点から整理する[6]．

3.1　パフォーマンス要件（リアルタイム性，スループット，ジッタ，緊急対応）

OT システムではリアルタイム性が極めて重要である．産業用機器の制御においては，厳格なタイミングと決まった応答時間が要求され，わずかな遅延やジッタ（応答のばらつき）も許容されない．一方，IT システムでは高いスループットや安定した平均応答が重視され，多少の遅延やジッタは問題とならない場合が多い．例えば，モーター制御のループが通信遅延によりタイミングを逸脱し，ステップ運転ではオーバーラン，繊細な調整を要する制御では不安定化を引き起こす恐れがある．

3.2　可用性要件（信頼性，冗長性，再起動の許容性など）

OT システムでは連続稼働の可用性が極めて重視される．製造プラントや社会インフラは 24 時間 365 日の稼働が求められており，予期せぬダウンや再起動は，稼働停止による生産遅延，納期遅延などの経営影響や緊急停止による人災につながる可能性がある．一方，IT システムでは一部サービスの一時停止や定期的な再起動が業務上許容されることもあり，可用性要求は IT システムの用途に応じて異なる．

3.3　リスク管理（対象リスク，影響，優先事項）

OT システムでは人命・安全の保護やプロセスの継続が最優先され，フォールトトレランスによって物理的被害を防ぐことに重点が置かれる．IT システムでは主にデータ資産の機密性・完全性の確保が最重要であり，サイバー攻撃による情報漏洩や改ざんのリスク対策に重点が置かれる．

3.4　システム運用（OS，アップグレード，ベンダー依存）

OT システムでは，組込み OS のような一般的でない OS や古いソフトウエアが継続して使用されることが多く，システムのアップグレードやパッチ適用が容易ではない．一方，IT システムでは最新の OS や自動化ツールを用いた定期的なアップデートが一般的であり，比較的頻繁にソフトウエア更新や機器更替が行われる．

OT の運用管理は IT 部門ではなく制御エンジニアによって行われることが多く，IT とは異なる運用文化が存在する．制御システム特有のソフトウエア（SCADA ソフト[*1] や PLC プログラム[*2] など）は一般にベンダー依存が強く，バージョンを変更するとサポート対象外となるためベンダーとの検証などの期間や費用がかかり，更新についても工場などの環境の停止を伴うため，容易にアップデートは適用できない問題がある．

3.5　リソース制約（ハードウエア・ソフトウエア拡張性）

OT 機器（PLC や組込みコントローラなど）は計算資源やメモリ容量が限られている場合が多く，導入後にセキュリティ機能を追加することが難しい．

一方，IT システムはリソースが不足すると CPU やメモリを増設し，ソフトウエアを追加インストールして機能拡張することが比較的容易である．

OT 機器は専用装置としてコスト最適化されており，産業用コントローラは大量導入されるため，一台あたりのコストや消費電力を抑える目的で余計なハード資源を積んでいないことが要因となっている．

3.6　通信（プロトコル，ネットワーク構成，設計者）

OT システムの通信では，工業用専用プロトコル（例：Modbus，CC-Link IE，PROFINET，DNP3 など）や特殊な通信媒体（フィールドバス，シリアル回線，無線）が使用されることもある．

これらはベンダー独自仕様や業界ごとの標準仕様となっており，一般的な IT 通信（TCP/IP，イーサネット，HTTP など）とは異なる．IT エンジニアではなく制御システムエンジニアが設計する場合が多く，IT の常識とは異なり，ネットワークセグメントを分割しない設計が一般的である．リアルタイム制御通信を最優先するために，IT トラフィックとは分離したネットワークを構築するという設計思想が採られることが一般的である．

3.7　変更管理（アップデート頻度，影響範囲，検証）

OT システムでは，制御システムが一度停止すれば安全・生産両面で重大な影響があるため，変更そのものがリスクと考えられる．また，システムごとのカスタマイズ度合いが高く，現場ごとに異なる構成のため，変更前には念入りな検証が行われ，変更の影響範囲を極力局所化するよう慎重に計画して実施される．IT システムでは，組織的に整備された変更管理手順（承認フロー，バックアップ，検証テストなど）に基づいて，計画的に変更作業を実施している．変更に伴う一時的なサービス停止も許容される範囲で行われる．

3.8　サポート体制（ベンダー依存，サポート方法）

OT システムの保守・サポート体制は，特定ベンダーに大きく依存するケースが多い．制御装置やソフトウエアはメーカー独自仕様が多く，トラブル時にはそのメーカーやシステムインテグレータに頼らざるを得ない．特にプラント全体を制御する DCS（分散制御システム）[*3] や SCADA システムの場合，導入したベンダー技術者が定期点検や障害対応を行う．IT システムはマルチベンダー環境が一般的であり，社内の IT 部門や複数のベンダーから成る体制でサポートすることが多い．

3.9　コンポーネントの寿命（ライフサイクル）

OT システムを構成する機器・コンポーネントの寿命（ライフサイクル）は非常に長く，工場の制御装置などは 10 ～ 15 年単位で使用され続けることが多い．そのため，ソフトウエアについても古いバージョンを長期間使用し続けることになり，その結果，サポート期限を過ぎた OS が残存することになる．一方，IT 機器（サーバや PC，ネットワーク機器など）は 3 ～ 5 年程度で更新されることが多い．

3.10　コンポーネントの設置場所（アクセス性，遠隔性）

OT システムの構成要素は，工場現場や遠隔地に設置されることが多く，その物理的アクセスには制限や困難が伴う．工場の生産エリア，プラントの制御室，遠隔監視所，さらには地理的に離れた変電所・上下水施設・石油プラットフォームなど，現地に行かなければ直接操作や交換ができないため，保守員が現地対応するには時間と労力がかかる．

IT システムは，社内のサーバルームや IT に特化したデータセンターにあり，物理的にアクセスしやすい場合が多い．

4.　IT と OT が融合していくことで起きる問題

IT と OT の融合がもたらす利点の一方で，従来は分離・閉鎖されていた工場制御システムなどが企業内ネットワークやインターネットに接続されるケースが増えている．それに伴い，サイバー攻撃の対象範囲が IT 領域から OT 領域まで拡大し，OT 環境がサイバー攻撃の標的になるリスクが高まっている．IT と OT のネットワーク接続によって効率向上やデータ活用が期待できる一方で，新たな脆弱性や予期せぬ問題が発生する可能性がある．

4.1　OT のセキュリティにおける課題

以下の各項で OT システムの特性上の課題を述べる．

4.1.1　脆弱性の顕在化

OT システムは本来インターネットに接続しない前提で設計されているため，外部からの攻撃に対する防御に手薄な部分が多い．OT システムが，ネットワーク経由で IT システムと接続することで，攻撃者が OT 側に侵入する足掛かりが増加する．例えば，外部に公開されるポートが増えるとアタックサーフェスを発見され，攻撃するための情報を収集される．その後，攻撃が成功し，OT ネットワークが悪用されると，エネルギー設備や製造プラントなどの基幹インフラが遠隔から混乱させられる危険性がある．

4.1.2　攻撃面（アタックサーフェス）の拡大

OT 環境に接続するデバイスや産業用 IoT 機器の増加により，サイバー攻撃対象が増加する．複雑に相互接続された OT デバイス群の場合，どれか一つでもセキュリティ保護が不十分であれば，システム全体に脆弱性が連鎖する可能性がある．

4.1.3　レガシー機器の問題

OT システムで使用される制御機器は寿命が長く，古い OS や老朽化したシステムが多数稼働しており，メーカーサポートがないため，セキュリティの維持に課題がある．古い機器は設計当時にサイバーセキュリティが考慮されておらず，暗号化や認証機能を欠くものも多く，Modbus のような古い産業用通信プロトコルは不正アクセスや改ざんに対して脆弱であり，攻撃者に狙われやすいという問題がある．

4.1.4　セキュリティパッチ適用の困難性

OT システムを止めることが難しいため，OT 機器へのソフトウエア更新やパッチ適用ができず，セキュリティの維持が難しい．その結果，放置された脆弱性が残った状態でネットワーク上に晒されることになり，攻撃者の標的になる可能性がある．

4.1.5　資産の可視化不足

多くの企業では OT ネットワーク上の機器や通信の可視性が不十分で，自社の資産を十分把握・監視できていない．グローバルな調査では 73%が把握できていないとの回答がある[7]．見えない機器が放置され，資産管理台帳が整備されておらず，IT システムのような統合ログ監視や侵入検知体制が無い，もしくは不十分な場合，脅威の検知や影響範囲の把握が遅れるリスクが高まる．

4.1.6　IT セキュリティ製品の適用が困難

一般的な IT セキュリティツールを OT 環境に適用するには以下の問題がある．

1）可用性への課題

ネットワーク上でアクティブにスキャンを行うものや大量のリソースを消費するものがあり，これをOTシステムに適用すると制御システムの誤作動や停止，データ欠損を引き起こす可能性がある．そのため，可用性を損ねない専用ソリューションの選定が不可欠となる．

2）OT資産の可視化不足

OT製品は独自の通信を行っているため，IT製品ではOT資産の可視化は困難である．そのため，どのような脅威が存在するか把握ができず対策不足となる可能性がある．

3）OT通信の可視化不足

OT独自の通信をIT製品では把握することは困難であり，ITとOTをネットワーク接続する時に，ファイアウォールなどによるネットワーク分離やアクセス制御の設計が難しい．設計や設定を適切に実施しなければ，IT側の侵害がOT側に波及する可能性がある．

4.2　セキュリティ運用上の課題

OTセキュリティとITセキュリティを運用する上で，以下の問題が存在する．

4.2.1　組織体制

OTセキュリティでは，責任の所在が不明確であり，指揮命令系統や役割分担が明確でないケースが散見される．IT部門のセキュリティ担当者がOTの知見を持っていない場合が多く，OT側にも専任のセキュリティ責任者が置かれていない状況がある．その結果，IT部門とOT部門の連携が不足し，OTへの対策が遅れる．また，インシデント発生時に速やかに対処する体制・フローが整備できていない企業が多く，初動対応は現場担当者に委ねられることになる．そのような体制では，セキュリティインシデントに対する知識の不足から，初動判断や情報連携が遅れる恐れがある．

4.2.2　技術的課題

PwCが2023年11月に実施した国内企業向けOTセキュリティの実態調査[14]によると，有効回答を得た299社のうち82%の企業が自社のOT環境の資産を把握できていないことが分かっている．隠れたデバイスがセキュリティホールになるリスクがある．パッチ適用やセキュリティ対策に伴う停止リスクへの懸念から，OT機器の更新には膨大な時間とコストを要するため，既知の脆弱性が放置される傾向がある．OT環境特有の制御プロトコルや製造機器は，一般的なIT向けセキュリティ製品では監視・防御できない場合が多く，専用の製品が不可欠である．OT環境はITのような統合監視体制が整っていない場合が多く，障害の原因の特定が難しい．

4.3　実際に起きたインシデント事例

ITとOTの融合がもたらす利点の一方で，そこにつけ込む脅威も顕在化している．特に，

ランサムウエアとサプライチェーン攻撃が挙げられ，従来のIT システムだけでなく，融合したOT 環境にも深刻な被害を及ぼしている．以下の各項で，実際に発生した事例を示す．

4. 3. 1　ランサムウエア

工場系組織へのランサムウエア攻撃は，2024 年には前年度より 87％増加[12]しており，Dragos[*4] がモニターしている 80 グループのうち 50％が製造業を狙っている．IT 環境との融合が進む中で，単なるデータの暗号化だけでなく，OT プロセスの停止や物理的な設備への損害につながる可能性が高いため，より脅威が拡大していくと考えられる．

WannaCry（2017 年）の事例を紹介する．WannaCry は，Windows の脆弱性を悪用し，ユーザの操作なしに拡散し，感染後にファイルを暗号化し，ファイルの複合と引き換えにビットコインで身代金を要求した[8]．これにより，ランサムウエアの脅威が広く認識され，対策が検討されるようになった．

4. 3. 2　ICS 特化型マルウエア

ウクライナやイスラエルのような紛争地帯でICS 特化型マルウエア[*5] を利用した攻撃が行われている[12]．電力網の一部を乗っ取る，検出の困難なマルウエア（IOCONTROL）や，簡易的な攻撃でセンサーやコントローラに対して攻撃を行うマルウエア（Fuxnet, FrostyGoop）などが存在し，侵入後は容易に攻撃できる脆弱性があることが攻撃グループに認識されている[12]．脆弱性が放置されている状態では，今後も被害が拡大していくと考えられる．

Stuxnet（2010 年）と Industroyer（2016 年）の事例を紹介する．Stuxnet は，世界初の産業制御システム向けマルウエアであり，イランの核燃料濃縮施設においてOT ネットワークがエアギャップ環境であったため，最初の感染経路は感染したUSB ドライブを介してSiemens 製PLC に侵入した．このマルウエアは，遠心分離機を異常回転させる一方で，監視画面には正常稼働を装うよう設計されており，遠心分離機を破壊させたことがOT/ICS のセキュリティに注目を集める要因となった[8]．

Industroyer は，民間インフラを標的とした最初のマルウエアであり，OT プロトコルである IEC-104 を直接操作する機能を持ち，ウクライナにおいて大規模な停電を引き起こした[8]．これはOT プロトコルのセキュリティ脆弱性を突いた例となった．

4. 3. 3　フィッシング（標的型メール）攻撃

TXOne Networks の 2024 年調査で確認されたサイバー攻撃の 68％がIT 環境から侵入しており，攻撃の入り口となっている．フィッシィング攻撃もその一部に挙げられ[11]，IPA の情報セキュリティ 10 大脅威 2025 にも挙げられており，今後も継続すると考えられる[13]．

BlackEnergy（2015 年）の事例を紹介する．サイバー攻撃者集団が送信した標的型メールを，ウクライナの電力会社の従業員が開封してウイルスに感染した．IT ネットワーク

に侵入した攻撃者は，電力網を制御する SCADA システムにアクセスして攻撃を行った．停電を引き起こし数十万人に影響を与えた BlackEnergy は，重要インフラに対するサイバー攻撃の事例となった．

4. 3. 4　サプライチェーン攻撃

部品メーカーや関連会社を攻撃し，取引先のネットワークが侵害されると，そこから上流企業や取引先全体に被害が連鎖的に広がる[11]．これも IPA の情報セキュリティ 10 大脅威 2025 にも挙げられており，今後も継続すると考えられる[13]．

TSMC 新規導入機器からの感染（2018 年）とトヨタ自動車サプライチェーン攻撃（2022 年）の事例を紹介する．TSMC は，新規導入した製造設備のソフトウエア導入時に供給業者経由でウイルスに感染し，1 万台以上の装置がマルウエアに汚染された．この結果，一部製造ラインの停止や出荷遅延が発生した[9]．新規に導入する装置に対してもセキュリティ対応を検討するべき例となった．

小島プレス工業株式会社の子会社の脆弱なリモート機器経由でランサムウエアに感染し，システムが停止した．サプライヤーの業務停止により，トヨタ自動車は国内 28 ラインを 1 日停止することになった[10]．サプライチェーンのセキュリティについても対応を検討するべき例となった．

5.　OT セキュリティの対策手法

OT のリスクマネジメントには，「組織・人」，「運用」，「技術」の三要素が不可欠である．経済産業省が公開している「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン[15]」は，チェックリストを利用して現状を把握するのに有益ではあるが，実行する具体的なツールについては明記されていないため，以下に紹介する．

5. 1　OT 資産管理

OT 資産管理ツールの特徴としては，以下の点が挙げられる．

1）OT ネットワークをパッシブで監視し，正常時の通信を把握
2）OT プロトコルを把握し，PLC や IoT 機器のような資産情報を可視化
3）脆弱性データベースとの紐づけ
4）製品の EoL（End of Life：サポート終了）情報との紐づけ
5）ゾーン設定を行い，ゾーンを跨る通信を把握
6）正常時から逸脱する通信を検知

OT 資産管理ツールは，資産を可視化して構成の管理を行うだけでなく，IDS（不正侵入検知システム）の側面も持つ．また，パケットキャプチャなどで（パッシブ）監視する場合，セグメント毎に情報を収集する．すべてを取得することは困難であるが，能動的に通信して（アクティブ）監視する場合，古い機器への負荷がかかる懸念があるため，慎重に導入することが肝要である．

製品例としては，Claroty 社の「xDome」，Armis 社の「Armis Centrix」，Nozomi Networks 社の「Guardian」，Forescout 社の「Forescout eyeSight」，Cisco Systems 社の「Cyber Vision」などがある．これらのツールは，「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の以下の項目に対して有効である．

- ●業務の重要度の設定
- ●保護対象の整理
- ●保護対象の重要度の設定
- ●ゾーンの整理と，ゾーンと業務，保護対象の結びつけ
- ●ゾーンとセキュリティ脅威による影響の整理
- ●セキュリティインシデントの検知
- ●ライフサイクルマネジメントの資産管理

ただし，本製品を導入してすべてが解決するわけではなく，導入の目的に達するかどうかの確認と運用が重要になるため，PoC（概念実証）と運用体制の構築が不可欠である．

5.2　ネットワークセキュリティ・ゾーニング

ネットワークセキュリティ・ゾーニング製品の特徴としては，以下が挙げられる．

1）セグメント単位で通信の制御を行う
2）OT プロトコルを把握し，制御を行う
3）IPS 機能，正常時の通信の把握
4）リモート保守用 VPN

FW（ファイアウォール），IPS（侵入防止システム）機能がメインとなるため，一部製品では資産の可視化ができるが，IT 資産管理と比べると資産の脆弱性情報やソフトウエアバージョン情報の管理などができないことが多い．リモート保守用 VPN は，2020 年から新型コロナウイルス感染症の影響により，リモートメンテナンスの需要増加に伴って導入が増加した．その後，運用管理者が不在などの管理体制の問題により，脆弱性が存在する状態で放置されることで，攻撃され侵入される事象が多く報告されている．また，ID・パスワードが窃盗された場合は，攻撃者が自由に工場内へアクセスするリスクが存在し，ゼロデイ脆弱性を悪用した攻撃も多く存在するため運用には注意が必要である．

製品例としては，TXOne Networks 社の「EdgeIPS」や「EdgeFire」，Fortinet 社の「FortiGate Rugged NGFW」，Cisco Systems 社の「ISA3000 Series」などがある．

TXOne については，IPS 機器に問題が発生した場合はバイパスモードに切り替わるため，既存環境に導入する際の影響検討が少なくて済む利点がある．現状の通信を把握するために Auto Rule Learning を用いて整理することもできる．

これらのツールは，「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の以下の項目に対して有効である．

- ●ネットワークにおけるセキュリティ対策

構成分割，接続機器制限，内部秘匿，通信データ制限，通信監視・制御，構成管理，脆弱性対策と幅広く対応することができる（表 1）．しかし，適用できる範囲はネットワー

ク境界であるため，可視化できる範囲が狭く，対処が難しい内部からの攻撃に対しては個別の検討を要する．

表 1　ネットワークにおけるセキュリティ対策（例）の IPS 対応範囲[15]

対策項目	対応強度	対　　策	侵入防止	活動抑止	運用支援
構成分割	中	VLAN などによる論理ドメイン細分	○	○	
接続機器制限	中	IP アドレス，MAC アドレス制限	○	○	
内部秘匿	高	NAT 内部ネットワークの隠匿 不正通信防止（ゲートウェイ）	○		
通信データ制限	高	送信元/宛先の制限（FW） 通信電文種別制限（DPI） 電文内容解析，異常通知（IDS） 電文内容解析，異常通信遮断（IPS）	○	○	
利用者制限	中	パスワードポリシー策定 個人 ID 認証 多要素認証は外部 IdP が必要	○	○	
通信監視・制御	高	通信状況可視化・監視（NDR） 異常検知（IDS） 異常通信遮断（IPS，フィルタリング）	○	○	○
構成管理	中	接続機器管理・可視化			○
脆弱性対策	高 （一部）	仮想的な対策（IPS，仮想パッチなど）	○	○	
ログ取得	中	機器内ログ取得 IDS ログ連携			○

5. 3　ゼロトラストネットワークアクセス（ZTNA）

ゼロトラストネットワークアクセス製品は，VPN 製品と比較して以下の特徴がある．

1）外部からの攻撃に強い

ZTNA ゲートウェイからクラウドと接続することにより，TCP ポートを直接インターネットに公開せずに済むため，仮に脆弱性が発見されたとしても，外部から攻撃することは難しい．

2）ユーザ毎にアクセスできる資産を制限できる

ユーザ毎に認証と認可を設定して，アクセスできる資産を最小化することで，不要な資産へのアクセスを制限することができ，ユーザ情報が漏れた場合のリスクを軽減できる．また，利用の申請・承認フローを組み込むことができるため，想定外の利用についても制限することができる．しかし，IT 用の ZTNA を入れた場合，OT 特有のセグメンテーション管理や IP アドレス管理の問題があり，OT では利用できない場合がある．そのため，OT 向けの ZTNA ソリューションを利用するべきである．

製品例としては，Cisco Systems 社の「Secure Equipment Access」，Dispel 社の「Dispel」，Claroty 社の「xDome Secure Access」などがある．

これらのツールは，「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の以下の項目に対して有効である．

●ネットワークにおけるセキュリティ対策

ZTNA は，「ネットワークにおけるセキュリティ対策（例）」にそのまま当てはめることはできないが，以下のような観点（対策項目）で有効である（図 2）．ZTNA の導入にはリモートアクセスの制御及び認証・認可の管理，アクセス許可対象を最小化することが重要である．また，外部からのアクセス手段を増やすため，攻撃手段として利用されないように運用を検討することが肝要である．

表 2　ネットワークにおけるセキュリティ対策（例）の ZTNA 対応範囲[15]

対策項目	対応強度	対　　策	侵入防止	活動抑止	運用支援
構成分割	中	アクセス許可対象の範囲制御による論理ドメイン細分	○	○	
接続機器制限	高	接続機器の論理証明 接続機器の信頼性確保	○	○	
内部秘匿	高	内部ネットワークの隠匿 不正通信防止（ゲートウェイ）	○		
通信データ制限	—	ユーザ毎で IP + Port による制御	○	○	
利用者制限	高	パスワードポリシー策定 個人 ID 認証 多要素認証	○	○	
通信監視・制御	—	外部への IP 公開を行わないことによる攻撃面の軽減	○	○	○
構成管理	中	接続機器管理・可視化			○
脆弱性対策	—	VDI での自動的な更新	○	○	
ログ取得	中	機器内ログ取得 IDS ログ連携			○

●セキュリティ対策の実行，及び計画・対策・運用体制の不断の見直し（PDCA サイクルの実施）

ZTNA は，利用者に対して詳細な権限を付与して管理し，接続対象以外のアクセスを防ぐことができるため，セキュリティ管理作業を行う上で有益である．製品ごとに機能が異なるため，自社での管理者，運用者，利用者を定義して，運用を検討するべきである（表 3）．

表3　ZTNA におけるセキュリティ管理作業（例）[15]

管理対象	管理すべき情報	運用技術
利用者	装置・機器別の利用者一覧（ID，権限）	ID と権限をシステム上で一元管理することができる．利用者への権限付与及び削除が容易に行える．
接続機器	ネットワーク別の登録機器一覧	アクセスする対象機器を制限することができるため，必要な利用者に必要な対象機器のみを提供できる．
実行プログラム	装置・機器ごとの実行プログラム	Dispel はクラウド上で VDI（仮想のデスクトップ）の作成・パスワード発行・削除の管理を行うため，必要なアプリケーションのみをインストールして，利用者が実行する． Secure Equipment Access は，端末管理は利用者となるため他の手段での対応が必要となる．
媒体	媒体一覧 媒体別利用管理	Dispel は，VDI 上のアクセス対象を制限可能であるため，外部サービスを用いて持ち込む情報を制限することができる．
装置・機器バックアップ	バックアップ履歴	機器の設定情報などを取得保管する上でリモートアクセスを利用することができる．
パッチ	パッチに関する情報	Dispel は VDI の OS パッチ管理は自動で行う．

5.4　EoL 機器へのセキュリティ対策

Windows や Linux のような汎用 OS を利用している場合，EoL（End of Life：サポート終了）を迎えた後も利用し続けるケースがある．その場合，ウイルスや脆弱性に対して無防備になるが，以下の方法でリスクを軽減することができる．

製品例としては，TXOne Networks 社の「EdgeIPS」や「Stellar Protect」などがある．

EdgeIPS は既知の攻撃に対して防御を行い，アンチウイルス機能などを利用してネットワークからの攻撃を軽減することができる．Stellar Protect については，Windows でのみ利用できる．Windows 2000 SP4 以降に対応しているため，機器の延命として利用することができる．ただし，いずれも軽減策であるため，汎用 OS の更新も併せて検討すべきである．

5.5　外部記憶媒体対策

製造・保守ベンダーが持ち込む新規機器や PC，USB について，チェックを実施しない場合，ウイルスが持ち込まれ，社内・工場内に拡散する恐れがある．

持ち込み対策の製品例としては，TXOne Networks 社の「Portable Inspector」や「SafePort」，ハギワラソリューションズの「ワクチン USB3」などがある．

Portable Inspector は，インストールが不要であるため，ベンダーの PC やオフライン環境の PC をチェックする上で有効である．ただし，持ち込み PC を利用する際は，運用上ウイルススキャン実行時間を考慮すべきである．SafePort については，持ち込み USB

のウイルススキャンを実行して，持ち込まれたデータがウイルスに感染していると判定した場合，そのデータを一時退避させてUSBを持ち込ませることができる．ワクチンUSB3は，Portable Inspectorと同様にウイルスチェックによりベンダーのPCのチェックを行う事ができるが，ストレージ機能を持たない．したがって，持ち込まれるUSBはウイルススキャンのためにPCへの接続を要するため，注意しなければならない．

本ツールは，「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の以下の項目に対して有効である．

●機器におけるセキュリティ対策

通信制限のある機器に対しての利用ポート，構成管理，脆弱性対策に対応している．汎用OSの新規持ち込み機器内にマルウエアが存在するセキュリティ脅威に対しても対応できる．しかし，USBによる対応は運用負荷が高くなるため，継続して対応するには，システムの改善を個別に検討しなければならない．

6. OTセキュリティの運用体制

OTインシデントへの対応には，組織横断的な体制の整備が不可欠である．まず，経営層（CISOやCSO）は，企業の情報セキュリティ活動全般を統括する役割を担い，ポリシーの策定とリソースの配分を行い，経営判断への参加体制を整えなければならない．OTの環境特有の問題を理解して，全社的なセキュリティ戦略や標準を策定することが求められる．そのため，本社ITセキュリティ部門が策定する際には，OTに関する理解者が助言できる環境を整えて，各工場やプラントのOT部門に展開することが重要である．工場レベルでは，日常的な運用・監視を行うOTセキュリティ担当者の他に，異常時に初期対応を実施するFSIRT（Factory Security Incident Response Team）の体制を構築することが求められる．インシデント対応を行うためには，以下の体制と関係性が不可欠である．

1）SOC（Security Operations Center）

各工場やプラントを監視するチームであり，IDSやネットワーク監視ツールを用いてOTネットワークを常時モニタリングする．異常が検知された場合には，工場現場の担当者へ通知し，対応支援を行う．IT部門のSOCと連携することで，ITおよびOT両領域を横断して広範な脅威に対応できる体制を構築することが求められる．

2）FSIRT（Factory Security Incident Response Team）

CSIRT（Computer Security Incident Response Team）とは違い，工場の安定稼動実現のためにインシデント発生時の対応を統括するチームであり，問題発生現場と本社ITチーム，SOCチームをつなぐハブとして機能する．事態の収束に向けて調査・対策をコーディネートし，対応状況や分析結果を経営層，法務，広報などの関係部門へ報告する．また，外部CSIRT（例：JPCERT/CCなど）や関係取引先への連絡・情報共有窓口も担う．

3）工場（OT）部門

制御システムや運用プロセスに精通した技術者が，OT環境固有のリスクや制約を理解しつつ，障害時には迅速に現地対応し，安全措置を実施する．

4）IT 部門

IT ネットワークや情報セキュリティの技術者が，OT 環境への侵入経路の遮断，IDS 導入，フォレンジック技術（証拠保全や原因分析に用いられる技術）の提供などを行う．IT セキュリティ人材は OT システム特有の通信プロトコルや可用性要件を把握し，OT 担当者と協力して対策を検討する．

7. お わ り に

本稿の目的は，IT と OT の融合に伴うセキュリティの課題と，体制を含めた対策の重要性を明示することである．IT と OT の融合を図り，セキュリティを維持するためには，IT と OT の相互理解が不可欠であり，経営層の調整が重要である．インシデントが発生した場合の被害額は年々増加しており[16][17]，OT を対象とした攻撃も増加している．今後，新たな攻撃手法が開発され，その対策が急務になる中，継続してセキュリティインシデントに対応する体制が不可欠であり，セキュリティシステムも重要である．本稿が，OT セキュリティの体制や対策を検討中の読者にとって参考になれば幸いである．

＊1 SCADA（Supervisory Control And Data Acquisition）ソフトは，工場などの施設にある機器や設備の状態を，ネットワーク経由で遠隔から一元的に監視および制御するシステムである．

＊2 機械や設備を自動制御するためのプログラム．入力信号と出力機器の動作を論理的に結び付け，様々な機会の自動運転を実現する．PLC は，Programmable Logic Controller（プログラマブルロジックコントローラ）の略．

＊3 大規模プラントなどで，各機器の制御装置を分散し，それらをネットワークで接続して，全体を統合的に監視・制御するシステムのこと．長期の安定稼働，オペレーションの効率化や省力化を実現する．

＊4 OT に特化したサイバーセキュリティ企業である．OT セキュリティに関する包括的なソリューションを提供している．

＊5 産業制御システム（ICS：Industrial Control Systems）や運用技術（OT：Operational Technology）環境に物理的な悪影響を及ぼすことを目的として特別に設計された悪意のあるソフトウエアである．一般的な IT マルウエアとは異なり，産業機器の挙動や制御プロトコルを理解した上で攻撃を行う点が特徴である．

参考文献

［1］ 長野・直富商事，AI で産廃選別を省人化　新工場に導入，日本経済新聞社，日本経済新聞会員限定記事，2024 年 10 月，https://www.nikkei.com/article/DGXZQOCC262IZ0W4A920C2000000/

［2］ 三菱電機デジタルイノベーション，製造業に影響を与える CPS（サイバーフィジカルシステム）とは？概念から活用事例まで紹介，三菱電機デジタルイノベーション，2022 年 9 月，https://www.mdsol.co.jp/column/column_123_2169.html

［3］ AI による予知保全の事例 5 選｜導入方法や 2 大メリットも紹介，AI 総研，2024 年 7 月，https://metaversesouken.com/ai/ai/predictive-maintenance/

［4］ 武田薬品工業が製造 DX の事例を紹介，2023 年は作業時間を年間 11 万時間削減，アイティメディア，2024 年 09 月，https://monoist.itmedia.co.jp/mn/articles/2409/06/news080_2.html

［5］ 中期事業計画を支えるブリヂストン流の DX「モノづくり領域」にて匠の技を伝えるシステムを開発，ブリヂストン，2021 年 04 月，https://www.bridgestone.co.jp/corporate/news/2021041301.html

［6］ Keith Stouffer, “NIST SP 800-82 Rev.3 Guide to Operational Technology（OT）Security”, NIST, 2023年9月,
https://csrc.nist.gov/pubs/sp/800/82/r3/final
［7］ Cyolo, “New Research from Cyolo and Ponemon Institute Identifies Significant Gaps in Securing Access to Connected OT Environments”, Cyolo, 2024年2月,
https://cyolo.io/press-releases/ponemon-survey-secure-access-risk-ot-environments
［8］ Forescout, “Since Stuxnet: A Brief History of Critical Infrastructure Attacks”, Forescout, 2025年2月,
https://www.forescout.com/blog/since-stuxnet-a-brief-history-of-critical-infrastructure-attacks/
［9］ TSMC, “TSMC Details Impact of Computer Virus Incident”, TSMC, 2018年8月,
https://pr.tsmc.com/english/news/1969
［10］ 小島プレス工業株式会社, “ウイルス感染被害によるシステム停止事案発生のお知らせ（第2報）”, 小島プレス工業株式会社, 2022年3月,
https://www.kojima-tns.co.jp/news/news0003406/
［11］ TXOne Networks, “Annual OT/ICS Cybersecurity Report 2024”, TXOne Networks, 2025年3月,
https://www.txone.com/security-reports/ot-ics-cybersecurity-2024/
［12］ “Annual OT/ICS Cybersecurity Report 2024”, Dragos, 2025年3月,
https://www.dragos.com/ot-cybersecurity-year-in-review/
［13］ 独立行政法人情報処理推進機構, “情報セキュリティ10大脅威2025”, 独立行政法人情報処理推進機構, 2025年1月,
https://www.ipa.go.jp/security/10threats/10threats2025.html
［14］ PwC Japan, “エンドユーザーとベンダーの視点から考える, OTセキュリティの現実解（三菱電機）”, PwC Japan, 2024年8月,
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/dtf2024-06.html
［15］ 経済産業省, “工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン”, 経済産業省, 2024年4月,
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html
［16］ IBM, “Cost of a Data Breach Report 2024”, IBM, 2024年7月,
https://www.ibm.com/reports/data-breach
［17］ 日本ネットワークセキュリティ協会, “インシデント損害額調査レポート 別紙2025年版”, 日本ネットワークセキュリティ協会, 2025年7月,
https://www.jnsa.org/result/incidentdamage/202507.html

※ 上記参考文献に示したURLのリンク先は, 2025年11月10日時点での存在を確認.

執筆者紹介 森 下 直 樹（Naoki Morishita）
2009年入社. 2018年まで金融業界のネットワーク導入保守作業に従事. その後2023年よりOTセキュリティに関する研究製品検証に従事しビジネス化に関する業務を担当している. ネットワークスペシャリスト取得. 情報処理安全確保支援士.

白　木　啓　子（Keiko Shiroki）

2006年入社．2018年まで無線ネットワーク設計構築および各種プロジェクトのPMに従事．その後DXビジネス企画開発業務を経て，2023年よりOTセキュリティに関する企画開発業務を担当している．