製造革新からみたサイバーセキュリティの着眼点と新展開

【セキュリティ対策ソリューション】

新旧融合 DX ネットワークとセキュアリモートアクセス

日本ダイレックス　松尾　義司

1. はじめに

スマート工場や製造 DX への展開が話題を集め，製造 DX を実現するために製造に関わるデータをデジタル化し，IT 技術を使って利活用することが求められている。

製造 DX という言葉は，ドイツ政府が主張し世界に広がった Industry4.0 や日本が提唱している Society5.0 と密接に結びついているが，弊社では製造 DX を「進化したデジタル技術の活用，新しい価値の創造および個別要求に対応した製造システムの実現（変種，変量生産）」と捉えている。

本稿では，製造 DX を実現する上で必須となるサイバーセキュリティ対策の着眼点として，既存設備の有効利用（新旧設備の融合）とゼロトラストアーキテクチャに基づいたセキュアなリモート監視システム（ZeRA：Zero Trust Remote Accessor）を紹介する。

制御システムの更新には，莫大な予算と移行期間を要するため，既存設備を有効利用しながら，サイバーセキュリティ対策と製造 DX を実現していくことが重要であり，実態に即した長期的な計画が必須となる。また，スマート工場化を進める上では，リモート監視システムが重要であり，製造データの収集分析と予兆監視を進める上でもサイバーセキュリティ対策を完備したリモート監視システムが必要である。

2. 製造 DX に必須なセキュリティ対策

従来の工場では，制御システムと企業の基幹系および情報系システムは分離され，いわゆる IT 系システムと OT 系システムを完全分離することで制御システムのサイバーセキュリティ対策としていた。しかし，現在では社会の変化，生産性の向上など製造 DX への要求に伴い，IT 系システムと OT 系システムの接続が進んでいる。また，現場部門の利便性向上を目的とした「隠れ接続」や保守端末の持ち込みなど，サイバーセキュリティ上のリスクも増大している。(図 1)

最近のセキュリティインシデントでは，制御システムを標的とした攻撃事例も増加しており，サイバー攻撃により重大な被害や人命にかかわる事態も発生している。

そのため，製造 DX を進める上でサイバーセキュリティ対策は必須と考えるべきである。

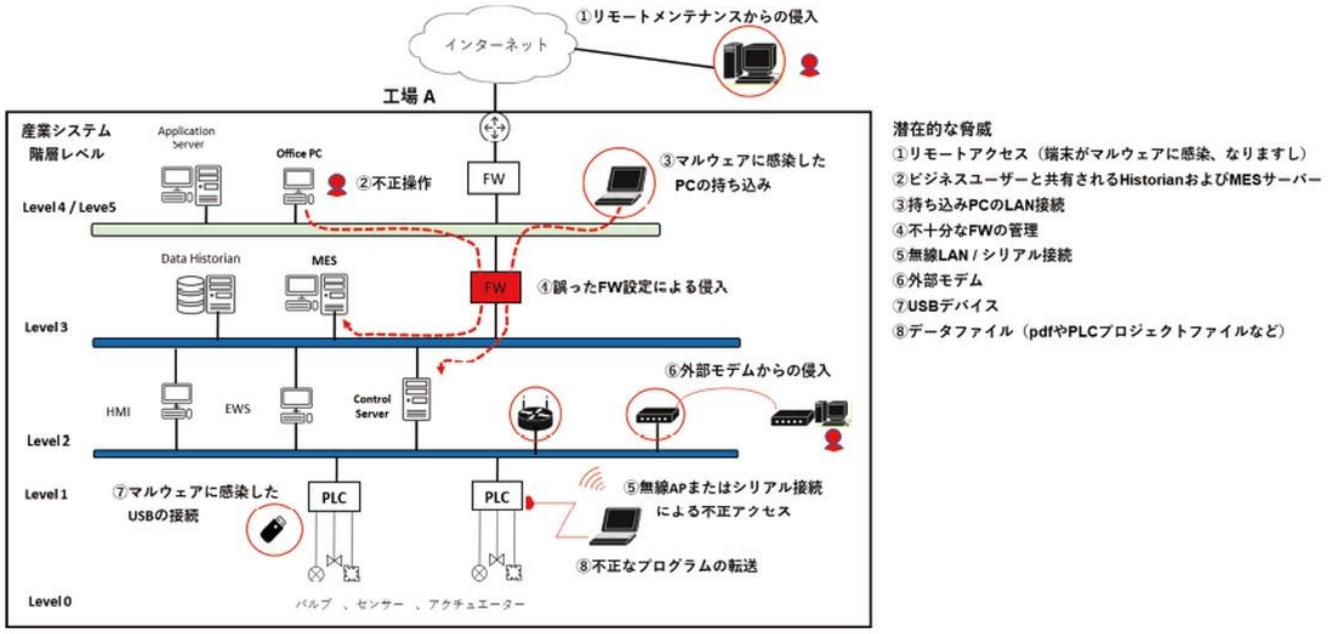


図 1　従来の制御システムで考えられるサイバーセキュリティリスク

3. 製造 DX からみたサイバーセキュリティの着眼点

3.1「IT-OT 中間層システム」

弊社では製造DXを進める上でサイバーセキュリティ対策は必須と考えており，IT システムと OT システムを結合する場合に最も焦点を当てる必要がある部分を「IT-OT 中間層システム」と考えている。

制御システムの最重要資産である PLC/DCS およびフィールドシステムは，安全性重視，可用性重視で開発されており，セキュリティシステムを実装するのが困難である。そのため，IT 系ネットワークと OT 系ネットワークを結合する製造 DX へのセキュリティ対応では，IT 系ネットワークと OT 系ネットワークの中間層である広義の SCADA 層と MES 層である IT-OT 中間層システムで防御することが必須と考えるからである。

IT-OT 中間層システムのセキュリティ対策を進めるには，現状のシステムの課題を確認する上でも実態調査を実施することが重要である。弊社では IT-OT 中間層システムを中心とした実態調査サービス（「ありもの調査サービス」）を提供している。弊社の IT-OT 中間層システムの考え方については，**図 2** を参照のこと。

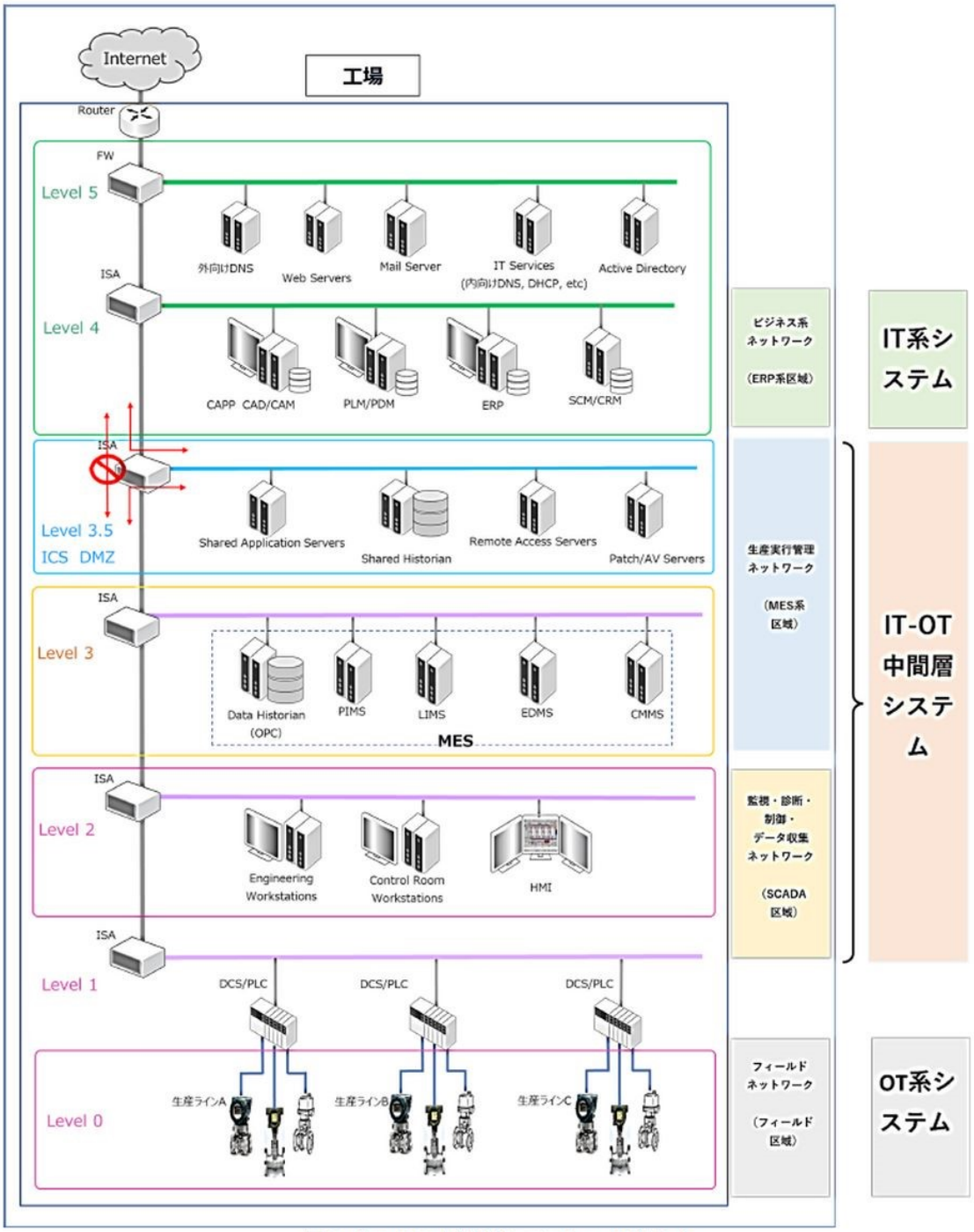


図 2「IT-OT 中間層システム」の考え方

3.2 既存設備の有効利用（新旧設備の融合）

制御システムのサイバーセキュリティ対策で重要な点は，サイバーセキュリティ対策の全面展開はOTシステムの実情に合わないということである。昨今，サイバーセキュリティ対策の世界ではゼロトラストアーキテクチャに基づいた対策が注目されている。ゼロトラストアーキテクチャは，ネットワークの内外（境界）を意識せず，すべてを信頼しないことを前提にすべてのトラフィックの検査やログの取得を行うアプローチで，新型コロナ禍によるテレワーク型勤務体制に適していることもあり，注目されている。

しかし，制御システムでは，システムの全面的な更改には莫大な費用と期間が必要なため，既存ネットワークにゼロトラストネットワークを載せるオーバレイ型ソリューションや既存システムを変更せずに外部ネットワークとセキュアに接続する「後付け型セキュリティソリューション」が必要と考える。

4章で弊社の具体的な新旧融合DXネットワーク事例として，「X-Connector」を使用した「後付け型セキュリティソリューション」を紹介する。

3.3 セキュアなリモート監視システム

製造DXを実現する上では，複数の工場を有機的に接続し，製造工程の最適化，サプライチェーンや基幹システム（ERP等）との連携などセキュアなネットワーク結合が必須となる。この場合，クラウドベースのDXプラットフォームサービスを利用する形態も含め，リモート監視ネットワークとその体制整備が重要となる。

弊社では，工場のリモート監視システムとしてゼロトラストアーキテクチャに基づいたリモート監視システム「ZeRA:Zero Trust Remote Accessor」を提供している。

次章ではセキュアなリモート監視システムZeRAの概要と接続事例を紹介する。

4. 新旧融合DXネットワークとセキュアなリモート監視システム「ZeRA」

4.1「X-Connector」を使用した新旧融合DXネットワーク

プロセスオートメーション系の工場を中心にPLCやDCSの操業データをOPC DAサーバで収集し活用するシステムが存在する。このOPC DAサーバの情報を，デジタルトランスフォーメーションを実現するためのデータ分析や利活用を提供するクラウド（以下「DXクラウド」と表記）に上げて分析し活用する動きが進んでいる。

しかし，OPC DAプロトコルは，Microsoft社が開発したDCOMプロトコルがベースとなっており，セキュリティ上，脆弱性が高いプロトコルである。Microsoftは既にDCOMのサポートを終了しており，新しいプロトコルであるOPC UAへの更新には，このプロトコルをサポートする制御システムの更新も必要な場合が多く，莫大な費用と安全性の確認に長期間を要する。そのため，新しいプロトコルであるOPC UAへの更新が進んでいない現状がある。

弊社は，このOPC DA通信でのセキュリティを強化するための，OT専用ファイアウォール「Tofino」装置を提供している。このTofino装置は，OPC DAサーバの直近に配置してOPC DAサーバを守る直近型ファイアウォールである。

さらに弊社は，DXクラウドなどのIT系システムに安全にOPC DAサーバを接続するための中間装置として今回紹介する「X-Connector」を提供している。

X-Connectorには，OPC DAクライアントおよびOPC DAサーバが内蔵されており，既存のOPC DAサーバにはOPC DAクライアントとしてアクセスし，必要なタグ情報などのデータを取得する。取得したデータは，X-Connectorに内蔵されたOPC DAサーバで再構築され，セキュリティ完全防御を実現する一方向通信装置（データダイオード）を経由してIT系システム側へ転送される。

この時，X-ConnectorのIT系システム側では，既存のOPC DAサーバから収集し転送されてきたデータを最新のセキュアなプロトコルであるOPC UAに変換し，OPC UAサーバとしてDXクラウドに接続させることができる。

このようにX-Connectorは，既存のOPC DAサーバを一切変更することなく，DXクラウドと最新でセキュアなプロトコルであるOPC UAで接続することに加え，データダイオードを使用することでOT側システムのセキュリティ完全防御を実現する。

X-Connectorの接続構成については**図3**を参照のこと。

このX-Connectorは，今回紹介したOPC DA以外のプロトコルにも対応でき，セキュリティレベルに関してもデータダイオードのような一方向通信による完全防御までは必要とせず，双方向通信が必要なシステムにも適用できるモデルも用意している。

4.2 セキュアなリモート監視システム「ZeRA」

昨今，サイバーセキュリティの世界では，従来の境界防衛型セキュリティではセキュリティ攻撃手法の進化に対応できないため，ネットワークの内外（境界）を意識せず，すべてを信頼しないことを前提にすべて

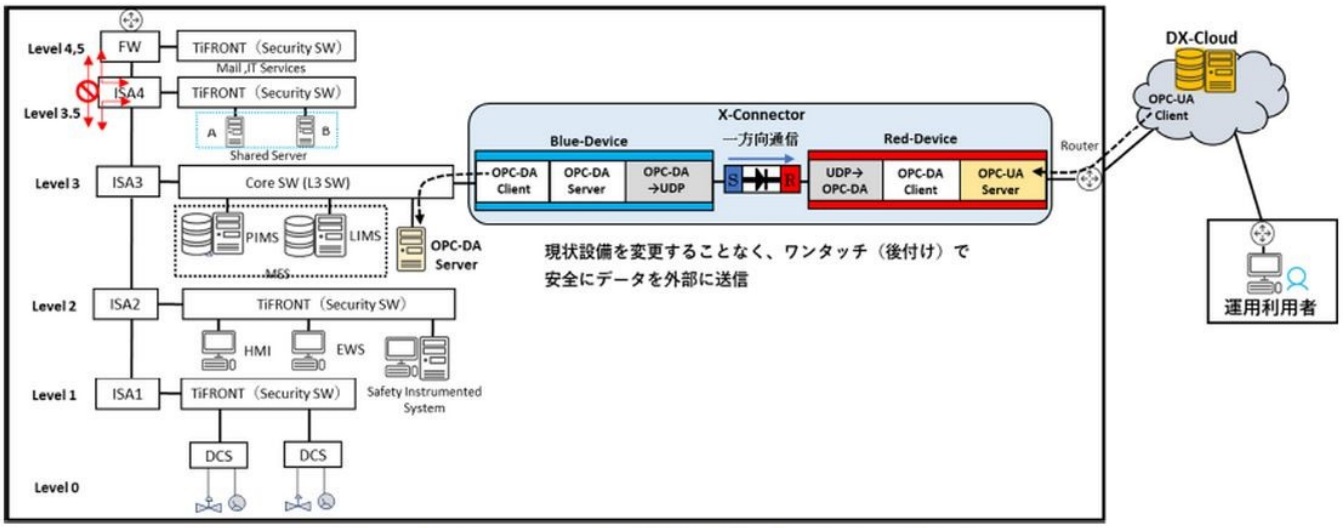


図 3「X-Connector」を使用した新旧融合 DX ネットワーク

のトラフィックの検査やログの取得を行うゼロトラストアーキテクチャが注目されている。

ゼロトラストアーキテクチャに基づいた商品やサービスも多数のベンダから紹介されている。しかし，工場のリモート監視や複数の拠点の制御システムの接続などには，クラウドの利用やインターネット接続を前提としたソリューションが多く，従来の制御システムとの整合性に課題がある。

そのため，弊社はスマート工場などの制御システムのリモート監視や OT システムと IT システムの接続に特化したゼロトラスト・リモート・アクセサー（ZeRA）システムを提供する。

セキュアなリモート監視システム ZeRA は，従来の VPN システムの欠陥である以下の課題を解決する。

①接続後認証（一旦，TCP/IP の接続をした後に認証をするため，スキャン等でその IP アドレスの存在を知られ，攻撃の対象とされる。）

②横展開（一旦，VPN ゲートウェイを通過したら，その中のネットワークに自由にアクセスできる。）

③設置，移設，増設，改変等の運用業務が複雑で大変

ZeRA システムには,データダイオードを使用した「完全防御型モデル」や HIP（Host Identity Protocol）を使用した「ZeRA-AW モデル」，SDP（Software-Defined Perimeter）を使用した「ZeRA-AG モデル」など，ユーザの使用形態やセキュリティレベルに応じた種々のモデルを用意している。

今回は，制御システムのリモート監視に最も親和性の高い ZeRA-AW について接続構成図と特長を説明する。

(1) ZeRA-AW リモート監視システムの特長

ZeRA-AW リモート監視システムの特長を以下に示す。

①固有のＩＤ（証明書）による相互認証

ZeRA-AW 装置は固有の ID（証明書）が出荷時に内蔵されており，固有 ID（証明書）を使用した相互認証により,なりすまし等の防止と接続前認証を実現している。

②コンダクタによるアクセス制御の一元管理

ZeRA-AW システムは，データ転送を実施するデータプレーンと管理制御を実施するコントロールプレーンが分かれており，統合管理制御装置として構成情報管理，セキュリティポリシーの管理やアクセス制御などをコンダクタにより一元管理できる。

③マイクロセグメンテーション（最小ネットワーク隔離による横展開防止）

ゼロトラストアーキテクチャの実現方式であるマイクロセグメンテーション（最小ネットワーク隔離）を ZeRA-AW が実現する。ZeRA-AW 装置は，既存のネットワークの上に隔離ネットワークを構築（オーバーレイネットワーク）する。

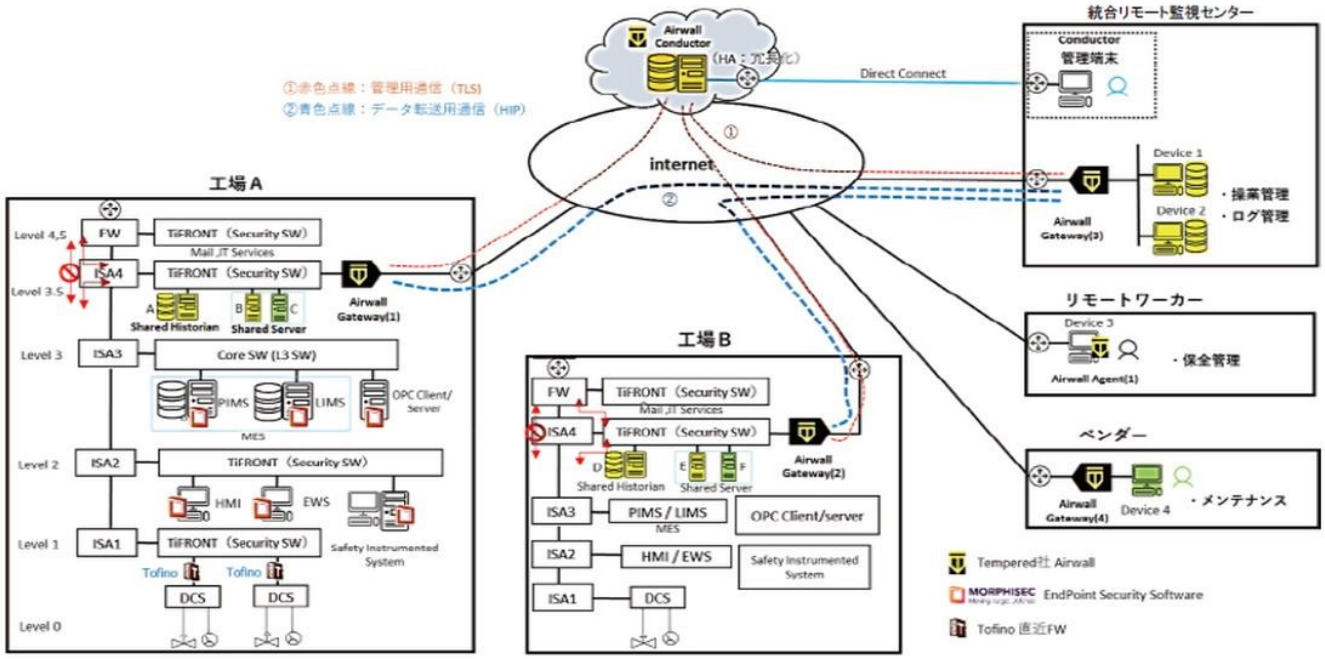
④構築の容易性（ゼロタッチプロビジョニング）

ZeRA-AW 装置はコンダクタで一元管理でき，リモート側の ZeRA-AW 装置は最小限の設定で自動的にコンダクタに接続されネットワークの構築が容易に実現できる。

⑤保護対象ネットワークのスティルス化（隠れネットワーク化）

最近では，サイバー攻撃技術が進化し，ネットワークノードに対して，全 IP アドレスのスキャン攻撃を実施することも可能となった。そのため，スキャンに対して応答する従来の VPN システムなどは，サイバー攻撃のターゲットになる可能性が高くなった。

ZeRA-AW 装置は，最初の認証パケットに固有のホスト ID に基づいた識別子を入れ込んでおり，相手か



ZeRA-Airwallの特長

1. 固有のID（証明書）による相互認証
2. Conductorによるアクセス制御の一元管理
3. マイクロセグメンテーション（最小ネットワーク隔離による横展開防止）
4. 構築の容易性（ゼロタッチプロビジョニング）
5. 保護対象ネットワークのスティルス化（隠れネットワーク化）
6. 軍事レベルの暗号化（AES-256暗号化）

図4　セキュアなリモート監視システム「ZeRA」

らのパケットにその識別子がないものに対して一切応答を返さない。また，認証パケットはUDPベースでTCP/IPのSYNパケットスキャンなども無視することにより，ZeRA-AWネットワークをスティルス化（隠れネットワーク化）することができる。

⑥軍事レベルの暗号化

ZeRA-AW装置は，保護対象ネットワークのトラフィックを軍事レベルの暗号強度をもつAES256を使用した暗号化トンネルで転送する。

(2) セキュアなリモート監視システムZeRAのネットワーク事例

図4にセキュアなリモート監視システムZeRAのネットワーク事例を示す。

これは，工場Aおよび工場BのICS DMZ（製造システムDMZ）に配置された共有サーバおよび共有ヒストリアンを統合リモート監視センタから監視するネットワークの例である。統合監視センタからの監視以外にベンダやリモートワーカからの接続も可能である。

弊社はセキュリティ上の観点からLEVEL3以下にある制御システム用オリジンサーバへの直接アクセスを禁止し，リモートアクセス用の共有サーバ（リプリケーションサーバ）をICS DMZに配置する構成を推奨している。また，ZeRAシステムのSI（システムインテグレーション）に加えて，共有サーバの構築などOT-IT結合に関わるエンジニアリングサポートも実施している。

5. 今後の動向

弊社では，工場のセキュリティ総合対策として，ICS水平・垂直多層防御の必要性を訴えてきたが，これに加えて今回紹介した製造DXのセキュアなネットワーク構築に対して既存設備を有効利用しながらIT-OT結合を構築できる「X-Connectorシステム」やセキュアなリモート監視を実現する「ZeRAシステム」のサポート範囲を広げていく計画である。

プロトコル面ではOPC UAに加えてMQTTやOPC UAパブ・サブモデルなどの主要なプロトコルの開発を進めていくと同時に，既存のプロトコル対応に関してはModbus-TCP，Ethernet/IP等を追加していく予定である。

マツオ・ヨシジ
日本ダイレックス㈱　代表取締役社長
〒135-0064・東京都江東区青海2-4-32
電話（03）3242-3157
E-mail：sales@direx.com