各　位

2025年7月30日
サイバネットシステム株式会社

産業用制御システム(ICS)・OTサイバーセキュリティソリューション「TXOne Networks製品群」販売開始のお知らせ

TXOneで製造現場を「止めずに守る」。OT環境のセキュリティ課題に対応し、製造業DXを安全に進める体制強化を支援

サイバネットシステム株式会社（本社：東京都、代表取締役 社長執行役員：白石 善治、以下「サイバネット」）は、OTセキュリティ分野に特化したTXOne Networks Inc.（本社：台湾）の日本法人であるTXOne Networks Japan合同会社（本社：東京都港区、代表執行役員社長：近藤 禎夫、以下、「TXOne」）と販売代理店契約を締結し、産業用制御システム（ICS）・OTサイバーセキュリティソリューション「TXOne（ティーエックスワン）製品群」の販売・サポートを、2025年7月30日より開始したことをお知らせします。

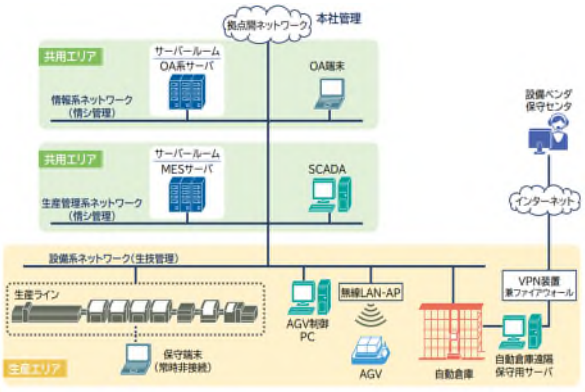
製造業DXの加速に伴い拡大するOTセキュリティリスク

製造現場の“外部接続”が引き起こすセキュリティ課題

近年、世界各国で工場や重要インフラ施設におけるICS（産業用制御システム）／OT（システム制御・運用技術）へのサイバー攻撃が報告されています※1。その背景には、製造業のDXに伴い、従来は閉域運用が前提だったOT環境が、外部ネットワークと接続されるようになった構造的な変化があります※2。

製造現場では、稼働状況や生産データをリアルタイムで把握・分析し、全体最適化や迅速な意思決定を進める動きが広まっており、こうした取り組みの中で、IoTやクラウドとの連携が進み、インターネット経由でのアクセスや侵入といった、これまで想定されていなかったセキュリティリスクが顕在化しています。

実際、ICS／OTを標的とした攻撃事例では、生産ラインの停止、設備の損傷、情報漏洩といった深刻な被害が発生しています。こうした脅威は、企業の事業継続性と社会的信用に大きな影響を及ぼすことから、OTセキュリティへの対応は今や選択肢ではなく、避けて通れない経営課題となりつつあります。



設備系ネットワーク、生産管理系ネットワーク、情報系ネットワークで接続される工場システムの例
（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』８頁より※2）

さらに、製造業のDXが進む中、各国政府もOTセキュリティに関する制度整備を加速させています。

- **日本：経済産業省によるガイドライン整備**
  2022年11月、経済産業省は「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 Ver1.0」を策定。工場のセキュリティ対策に関する基本的な考え方や手順を提示し、国内企業に対して早期の体制整備を促しています。

- **EU：サイバーレジリエンス法（CRA：Cyber Resilience Act）の施行**
  2024年12月に施行され、2027年12月から適用されるCRAにより、デジタル要素を含む製品に対して、設計から廃棄に至るまでのライフサイクル全体にわたるセキュリティ対策の強化が義務化されます※3。EU市場で製品を展開する企業にとって、CRA要件への準拠は必須となり、グローバル市場に進出する製造業にとって、OTセキュリティへの対応がこれまで以上に重要な課題となります。

製造現場のセキュリティ要件に応えるTXOneのソリューション

製造現場では、生産ラインの停止が大きな損失に直結するため、システムの再起動や運用変更を伴うセキュリティ対策の導入が困難です。そのため、セキュリティ強化と安定稼働を両立させることが、製造現場のセキュリティにおける本質的な課題となっています。

さらに、製造現場のOT環境には以下のような特有の制約があり、従来のITセキュリティ対策だけでは十分に対応できないケースが多く見られます：

- レガシーOSの継続利用
  製造装置は長期間の稼働を前提としており、更新が困難な旧型のレガシーOSを使用し続ける現場も多く、標準的なアップデートによる防御が困難。
- 可視性の欠如
  ネットワーク内に何が接続されているか正確に把握しづらく、潜在的なリスクの特定が難しい。
- 閉域環境での運用
  クラウド連携やインターネット接続を前提としたソリューションを導入できない環境も多い。

こうした環境下では、「止めずに守る」ことを実現する専用のセキュリティ対策が不可欠です。

外部デバイスの制御から設備系ネットワークの防御まで──TXOne 製品ラインアップ

TXOneは、OT特有の制限と要件を踏まえ、可用性を維持しながらセキュリティを強化できるソリューションを提供しています。特長は、「止めずに守る」というOT環境の要件に応え、現場での実運用を前提とした柔軟かつ現実的な設計にあります。

TXOne製品は、現場のセキュリティニーズに応じて、「セキュリティ検査」「エンドポイント保護」「ネットワーク防御」に対応した3つのシリーズで構成されています。

【セキュリティ検査】Elementシリーズ

閉域網内の端末やスタンドアロンPC、外部からの持ち込みデバイスなどはセキュリティ対策の盲点になりがちです。Elementシリーズはこのような機器に対し、検査・可視化することでリスクを最小化します。

- Portable Inspector
  USBメモリ型のマルウェアスキャナ。PCへのインストール不要で、USB接続するだけでデバイスの検査や資産情報の取得が可能です。
- Safe Port
  工場内に常設して使用する検査ステーション。外部から持ち込まれたリムーバブルメディアを、設備系ネットワーク接続前にスキャンし、リスクを防ぎます。
- ElementOne
  Portable InspectorやSafe Portから収集されたスキャンログや資産情報を一元管理し、ダッシュボード形式で表示。脆弱性、OSの更新状況、インストール済のアプリケーション、詳細なシステム情報など、資産を見える化する機能を提供します。

【エンドポイント保護】Stellar

多くの製造装置は長期稼働を前提としており、サポートの終了したレガシーOSを使い続ける現場が存在します。Stellarは、こうしたレガシー環境にも対応可能なエンドポイント保護ソリューションです。

- Stellar
  アンチウィルススキャン、アプリケーション制御、USB制御、ふるまい検知などを搭載し、端末を多層的に守ります。また、機能を限定して使用している端末にも対応でき、ホワイトリスト型のロックダウン運用も可能です。導入時の再起動が不要で、現場への影響を最小限に抑えられます。

【ネットワーク防御】Edgeシリーズ

OT環境にウイルスなどの脅威が侵入すると、ネットワーク内での水平移動（ラテラルムーブメント）により、複数の装置へと被害が拡大する恐れがあります。Edgeシリーズは、マイクロセグメンテーションによるウイルスの水平移動対策と、産業用ネットワークに特化した制御と検知で、感染の拡大を防止するネットワークセキュリティソリューションです。

- EdgeIPS / EdgeFire / EdgeOne
  過酷な環境や可用性を重視した性能・機能を有し、産業用ネットワーク特有のプロトコルや制御コマンドの可視化・制御が可能なネットワーク機器。仮想パッチによる脆弱性攻撃対策、AIによるトラフィック自動学習機能を備え、ネットワーク通信上のリスクをリアルタイムで検知・防御します。

TXOneの詳細については、下記Webサイトをご覧ください。
https://www.cybernet.co.jp/txone/

OTセキュリティを含め、総合的に製造業DXを支援できる体制へ

サイバネットは、これまで製造業の設計・開発領域において技術支援やコンサルティングを通じてDX推進を支援してまいりました。新たにTXOne製品の取り扱いを開始することで、OTセキュリティの側面からも製造業DXを支えるソリューションの提供が可能となりました。

今後も、DXの加速に伴い一層重要性を増すOTセキュリティ分野への取り組みを強化し、より多くの製造業のお客様が安心してDXを推進できる環境整備に貢献してまいります。

TXOne社からのコメント：

TXOne Networks Japan 合同会社 代表執行役員社長 近藤 禎夫氏のコメント

このたび、サイバネットとの協業を通じて、日本の製造業におけるOT環境のセキュリティ強化に貢献できることを心より光栄に思います。TXOneのソリューションは、現場の稼働を止めることなく、サイバー脅威に対応することを可能にします。サイバネットの技術力と市場理解を活かし、製造業のDX推進を安全に支える体制づくりを共に進めてまいります。

注釈

※1：出典：公安調査庁『サイバー空間における脅威の概況』（2024 年 12 月）
https://www.moj.go.jp/content/001396422.pdf

※2：出典：経済産業省 産業サイバーセキュリティ研究会『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 ver1.1』（2025 年 4 月 11 日改訂）「工場セキュリティガイドラインの目的」
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.1.pdf

サイバネットシステム株式会社 〒101-0022 東京都千代田区神田練塀町３ https://www.cybernet.co.jp/

※3：出典：欧州委員会「サイバーレジリエンス法」
https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

TXOne Networksについて

TXOne Networksは、産業用制御システムや運用技術（OT）環境の信頼性と安全性を確保するサイバーセキュリティソリューションを提供しています。大手製造業や重要インフラ事業者への多くの実装経験から得た知見を活かし、サイバー防御に対する実用的で運用に適したアプローチを開発しています。ネットワーク防御およびエンドポイント保護の製品を提供し、リアルタイムかつ徹底的な防御アプローチにより、OTネットワークとミッションクリティカルなデバイスを保護します。
TXOne Networksに関する詳しい情報については、下記Webサイトをご覧ください。
https://www.TXOne.com/ja/

サイバネットについて

1985年の創業以来、物理学などの科学技術とデジタル技術の両面に精通した技術者集団として、製造業の研究・開発・設計部門や大学・政府の研究機関を中心に、コンピュータシミュレーションやサイバーセキュリティ、AR/VR、医用画像処理などに関わるデジタルソリューションおよび技術コンサルティングサービスを提供しています。

近年は、CAE、MBD、MBSEを中心とした製造業におけるエンジニアリングチェーンの革新に加え、PLMやIoTを活用したサプライチェーンの高度化に関わる分野にもソリューションの提供範囲を拡大しています。また、サイバーセキュリティ分野では、最新の脅威に対応した先端的なソリューションを複合的に提供できる体制を構築してきました。さらに、AIを活用したプログラム医療機器の分野において国内で初めての医療機器承認ならびに公的医療保険の適用を受けるなど、医療AIのパイオニアとして業界をリードしています。
サイバネットシステム株式会社に関する詳しい情報については、下記Webサイトをご覧ください。
https://www.cybernet.co.jp/

本件に関するお問い合わせ先：**サイバネットシステム株式会社**

内容について：
ITソリューション統括部
担当：櫻木
E-MAIL：itdsales@cybernet.co.jp

報道の方は：
コーポレートコミュニケーション室
担当：宮本
E-MAIL：prdreq@cybernet.co.jp