

導入事例

化学プラントを支えるOTシステムセキュリティを強化
脅威の特定から遮断まで一気通貫でのOTセキュリティ対策をTXOne EdgeIPSで実現

背景

石油化学コンビナートにおけるエチレンセンターとしての役割を担う丸善石油化学株式会社（以下、丸善石油化学）。プラスチック・合成繊維・合成ゴム・塗料の原料となるエチレンやプロピレンから、世界トップクラスのシェアを有する半導体フォトレジスト用ポリマーまで、多岐にわたる石油化学製品及び機能性原材料の開発・製造を行っています。そんな同社では、サイバーセキュリティ基本法に基づき、化学分野の重要インフラ事業者に位置づけ、TXOne Networks の「EdgeIPS」を導入することで、OT システムのセキュリティ強化を図りました。

ますます悪質化・高度化する昨今のサイバー攻撃は、IT システムのみならず工場やプラントの OT（制御技術）システムにもターゲットを広げています。万一、OT システムが侵害された場合、長期間にわたる操業停止に追い込まれるほか、最悪の場合、生命に関わる重大事故につながるおそれもあるだけに、対策は極めて重要です。

丸善石油化学が OT システムセキュリティの抜本的な強化に本格的に乗り出すきっかけとなったのが、2022 年のことです。代表取締役社長直下の CSR 委員会（サステナビリティ委員会）において、OT システムセキュリティが特定重要リスクの一つに選定され、全社的な取り組みとして推進されることになりました。

同社の執行役員であり、技術部 部長ならびに D X 戦略推進部 部長を兼務する小林 秀徳氏は、「もちろん以前からもサイバーセキュリティ対策は重視していましたが、経営層から明確な指示が出たことで、優先順位がさらに引き上げられました。翌 2023 年 12 月に施行を控えていた高圧ガス設備の『特定認定高度保安実施者制度』（通称：A 認定）を取得するためにも、高度なリスク管理に加え、テクノロジー活用やサイバーセキュリティ対策に対する厳格な要求事項を満たす必要があったのです。2024 年度からは技術部門を統括する取締役をトップとする『制御システムセキュリティ委員会』が設置され、体制面でも大きな強化が図られました」と振り返ります。

Chemiway
丸善石油化学株式会社

“プラント内の主要設備の運転を司るOTシステムへの不正侵入を防ぐための対策を強化しています”



丸善石油化学株式会社
千葉工場 生産管理部長
渕向 純一 氏



丸善石油化学株式会社
千葉工場 生産管理部 技術課長
伊藤 克佳 氏



丸善石油化学株式会社
千葉工場 生産管理部 技術課
主事 **加藤 俊之** 氏



丸善石油化学株式会社
千葉工場 生産管理部 技術課
主事 **込山 章吾** 氏



株式会社テリロジー
宇宙・社会インフラセキュリティ事業本部
山口 颯太 氏

ソリューション

丸善石油化学の OT システムは、プラント内の主要設備の運転を司る DCS（分散制御システム）ならびに OPC サーバー、高度制御サーバー、生産管理データを集約するデータベースサーバーなどから構成されており、これらのアセットに対する不正侵入を防ぐことが、セキュリティ対策の目的となります。

その強化に向けて同社が目指したのが、OT 系ネットワークの可視化です。

「当初はファイアウォールがあれば大丈夫と考えていましたが、それだけでは昨今の巧妙なサイバー攻撃から重要システムを守り切ることはできません。まずはプラント内のネットワーク全体を監視し、攻撃を検知する仕組みが不可欠と考えました」（小林氏）

そこで同社は、IDS（不正侵入検知システム）に着目し、パートナーであるテリロジーから提案の受け、導入を決意しました。

同社 千葉工場 生産管理部 技術課 主事の加藤 俊之氏は、「攻撃を検知した際のアラート発報の理由を明確に説明し、脅威の真偽判定まで確実に対応できる技術を有していることを評価し、IDS 製品の導入に至りました」と話します。

もっとも、この IDS だけでは課題は解決できません。

同社 千葉工場 生産管理部 技術課長の伊藤 克佳氏は、「単に攻撃を検知するだけでは脅威を取り押さえることはできません。特に生産現場に近いところで主要設備・装置の制御を担っているアセットを守るためには、リスクの高い通信の遮断まで行う IPS（不正侵入防止システム）が必要です」と強調します。

こうして同社は、テリロジーから追加提案された TXOne Networks の「EdgeIPS」を導入するに至りました。

「当社が監視対象とする OT アセットは 100 ～ 200 程度であり、大量エンドポイントを前提とする IT システム向け IPS ではコストに見合いません。導入時のダウンタイム抑制や高い可用性、きめ細かな制御プロトコル検査など、OT システム専用に設計された IPS という観点で、EdgeIPS のメリットが際立っていました」と話すのは、同社 千葉工場 生産管理部 技術課 主事の込山 章吾氏です。

さらに、同社 千葉工場 生産管理部長の渕向 純一氏が、このように続けます。

「2024 年 10 ～ 11 月にかけて PoC を実施したところ、その結果はセキュリティ委員会でも高い評価を得ました。特にネットワーク内のすべての OT アセットの状態を詳細に可視化するレポート機能は、『これだけでも導入に値する十分な価値がある』と経営層が予算確保を即断し、正式採用が決定しました」

この PoC を提案したテリロジー 宇宙・社会インフラセキュリティ事業本部の山口 颯太氏は、EdgeIPS を勧めた理由をこう説明します。

「OT 環境では生産装置の稼働継続が最優先であり、IT システム向けのセキュリティ製品をそのまま適用することはできません。EdgeIPS は OT 専用設計で可用性を重視しており、稼働中の環境に導入できる点が大きな特長です。PoC では実際のネットワーク上で EdgeIPS の検知・遮断機能と可視化レポートを検証していただきました。現場の通信リスクが具体的な形で示されたことが、経営層の意思決定につながったと認識しています」

導入効果

2025 年 12 月、千葉工場の中央制御室内サーバールームへの EdgeIPS 設置が完了。稼働開始と同時に実感できたのが、OT 系ネットワーク全体の通信リスクの可視化です。サーバー間の日常的なファイル転送も含め、あらゆるトラフィックにリスクレベルが表示されるようになりました。

「EdgeIPS の導入により『受け入れられるリスク』と『排除すべき不要通信』を、初めて体系的に判断できるようになりました。そのうえで不審な通信を遮断するルールを設定しておくことで、効果的な防御を実装することができます」（込山氏）

IDS 製品と組み合わせた IDS-IPS 連携でも、大きな効果が発揮されています。

「例えば OT 系ネットワークに誤って IT 系の端末を接続した際など、不正なトラフィックを即座に検知し、IP/MAC アドレスから端末を特定して管理者にメール通知する一連のプロセスが自動的に実行されます。これに基づき当事者への再教育を行うなど、ポリシー遵守を社内に徹底させる運用改善にも役立っています」（加藤氏）

加えて特筆すべきが、従前から OT 系ネットワークが抱えていた構造的な脆弱性の解消です。IT 系ネットワーク上で運用している PC やサーバーについては、一般的なウイルス対策ソフトの導入や最新パッチを適用することで防御を固めることができますが、OT システムにはこの手法を用いることができません。生産現場で稼働している設備・装置の運転継続性を損なうリスクがあるためです。

「これに対して EdgeIPS には、頻繁に更新されるシグネチャーに基づいて既知のウイルスを排除する OT システム専用のマルウェア侵入防止機能や高度な脆弱性データベースが備わっています。これまでの“ノーガード状態”から脱却し、セキュリティレベルを格段に向上することができました」（小林氏）

“「受け入れられるリスク」と「排除すべき不要通信」を体系的に判断できるようになったことで、不審な通信を遮断する効果的な防御を実装できました”

導入事例

今後の展望

丸善石油化学の千葉工場は大きく 4 つのエリアに分かれており、現時点ではまだそのうちの 1 つ目のエリアに EdgeIPS の導入を終えた段階にすぎません。同社は 2026 年度内に 2 台目を導入し、以降も順次拡大を図っていく計画です。

「EdgeIPS の導入効果はすでに実務レベルで実証されており、できる限り早期に全エリアへの展開を完了したいと考えています」（小林氏）

複数台の EdgeIPS の配置が実現した暁には、OT システムのセキュリティレベルのさらなる強化が期待されています。

「サイバー攻撃が起こり得る重要アセットを相互につなぐ通信経路の両側に EdgeIPS を配置し、マイクロセグメンテーションを設定することで、ラテラルムーブメント（横移動）をブロックすることが可能となります。侵害された OT アセットを物理的に停止するまでもなく、ソフトウェアのみで迅速かつ容易に脅威を封じ込めることができるメリットは絶大です。また、複数の EdgeIPS Pro 間で相互バックアップを行うことで、IPS 自体の可用性もさらに高めたいと考えています」（伊藤氏）

ただし、ツールに頼るだけでは OT システムのセキュリティ対策は不十分です。同社はサイバー攻撃に「やられない」ための防御に加え、「万一やられた際にも最短で復旧する」ための備えも急ピッチで進めています。

「ランサムウェア被害を想定したシミュレーションを常に実施し、生産現場の関係者も加えた訓練を重ねることで、24 時間以内の復旧を目指しています。こうした取り組みを支えるために、セキュリティ専門人材の育成にも継続的に投資しています」（渕向氏）

こうした取り組みを長期にわたって支えるパートナーとして、テリロジーも意欲を示します。

「OT セキュリティは、一度導入して終わりではなく、脅威の進化に合わせて継続的に強化していくものです。EdgeIPS の展開はもちろん、バックアップ・リカバリーを含めたレジリエンス強化に向けても、丸善石油化学様と共に歩んでいきたいと考えています」（山口氏）



導入製品

TXOne Edgeシリーズ

- EdgeIPS
- EdgeIPS Pro

OTネットワークを止めずに守るハードウェア型セキュリティ TXOne Edgeシリーズ

TXOneは、OT環境に特化した4つのセキュリティソリューションにより、可視化からリスク評価、防御までを一貫して支援します。これらは、Discover.、Assess.、Protect. の各フェーズを個別のツールとしてではなく、相互に連携するポートフォリオとして提供されます。必要な領域から導入でき、既存環境を活かしながら段階的にセキュリティを強化することが可能です。



EdgeIPS

インラインでの脅威防御

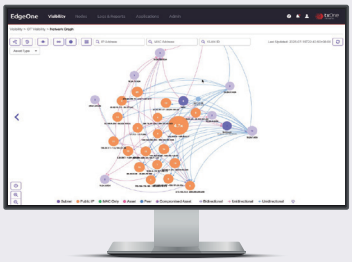
ファイアウォール、IPS、マルウェアスキャン、仮想パッチやマイクロセグメンテーション、ポリシー制御によりインライン防御を実現



EdgeFire

拠点単位の統合防御

ファイアウォール、IPS、VPNを一体化し、仮想パッチやマイクロセグメンテーション、ポリシー制御により拠点単位でOTネットワークを保護



EdgeOne

ネットワーク全体の統合管理

EdgeIPS/EdgeFireのデータとAVMにより資産や脆弱性を可視化し、複数拠点・複数デバイスの一元管理と統一ポリシー運用を支援

- ☑ 仮想パッチによるパッチ未適用機器の保護
- ☑ 物理セグメンテーションによる被害の局所化
- ☑ OTプロトコルに対応した通信制御とパケット検査
- ☑ 異常なネットワーク動作の検知（CPSDR）
- ☑ ハードウェアバイパスによる通信継続性の確保

TXOne Networksについて

TXOne Networksは、産業用制御システム（ICS）および運用技術（OT）環境に特化した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。現場の実情に即した実践的なアプローチにより、OT環境が直面するさまざまな課題を克服し、「セキュリティ」と「運用の安定性」の両立を実現します。TXOneのソリューションは、ネットワークベースおよびエンドポイントベースの両面からリアルタイムかつ多層的な防御を提供。ミッションクリティカルなデバイスを守り、安定した運用を支援します。詳しくは、www.txone.com/ja をご覧ください。

txOne networks

https://www.txone.com/ja

TXOne Networks Japan合同会社
〒105-5532 東京都港区虎ノ門2丁目6－1虎ノ門ヒルズステーションタワー32階

TXOneおよびTXOne NetworksロゴはTXOne Networks Incorporatedの登録商標です。本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。本データシートの記載内容は2025年5月現在のものです。内容については今後変更となることがございます。最新情報については弊社担当営業もしくは代理店にお問合せください。

Copyright © 2026TXOne Networks Incorporated. All rights reserved.

CS-TXON-025