



サイバー攻撃の可視化から遮断まで、一貫した対策を Nozomi GuardianとTXOne EdgeIPSで実現できました

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や機能性原材料の開発・製造を行っている。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として位置づけられている同社が目指したのが、OT（制御技術）システムセキュリティの抜本的な強化だ。

「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、 生命に関わる重大事故につながるおそれもあります」

2022年、代表取締役社長直下のCSR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として選定された。

丸善石油化学の執行役員であり、技術部 部長ならびにDX戦略推進部 部長を兼務する小林 秀徳氏は、こう語る。

「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の厳格な要求事項を満たす必要がありました」

さらに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た。

「プラント内のネットワーク全体を監視・可視化し、 攻撃を検知する仕組みが不可欠でした」

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る。

だが、導入していたIDS（不正侵入検知システム）は、誤検知が多く、実際の脅威かどうかの切り分けもできない状態が続いていた。

そうした中、この課題の解決策を求めて訪れたある展示会でテリロジー

と出会い、Nozomi Networks社の「Nozomi Guardian」の導入を検討することになった。

丸善石油化学 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しっかりできる技術を有していることを評価しました」と語る。

「OTシステムの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）も必要です」

ただし、IDSだけでは不十分であり、丸善石油化学 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」と語る。そして導入したのが、テリロジーから追加提案されたTXOne Networksの「EdgeIPS」である。

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 颯太は、この提案理由を次のように示す。



丸善石油化学株式会社

<https://www.chemiway.co.jp/>

「化学技術を基盤とし、くらしと産業の健全な発展に貢献する」ことを使命とし、1959年に創業。2016年にコスモエネルギーグループの一員となった。石油化学コンビナートにおけるエチレンセンターに位置づけられ、石油精製会社から原料を調達し、誘導品会社に製品を安定的に供給していく役割を担っている。

「OTシステムはITシステム以上の可用性が要求されます。EdgeIPSはこの条件を満たしており、プロセス系の環境でも安全に使える製品として選定しました」

丸善石油化学 千葉工場 生産管理部 技術課 主事の込山 章吾氏も、「当社が監視対象とするOTアセットは100～200程度で、桁違いに多くのエンドポイントを監視することを前提としたITシステム向けのIPSはコストが見合いません。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システム専用で設計されたIPSという観点で、EdgeIPSのメリットが際立っていました」と評価する。

さらに、丸善石油化学 千葉工場 生産管理部長の渕向 純一氏が、このように続ける。

「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られました。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』と経営層からお墨付きをいただき、正式採用にいたりました」

「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できました」

EdgeIPSは2025年12月、千葉工場の中央制御室内のサーバールームに最初の1台目の設置が完了。導入後、すぐにOT系ネットワーク内で行われる通信リスクの可視化という効果が得られた。これにより、業務上の必要性から日常的に行われているサーバー間のファイル転送などを含め、あらゆるトラフィックについてセキュリティ観点に基づいたリスクレベルが表示されるようになった。

「『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」（込山氏）

そのうえで発揮されたのが、Nozomi GuardianとEdgeIPSの連携効果だ。

「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）

OT系ネットワークが抱えていた構造的な脆弱性も解消された。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が、OTシステムにはこの手法を用いることができない。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だ。

「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）

「千葉工場内の4つのエリアすべてにEdgeIPSを 展開予定です」

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

ない。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だ。

「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る。

「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）

新たなセキュリティ対策の技術的な柱として、データダイオードの追加設置を検討中だ。

「データの流れを一方方向のみに制限する厳重な制御を行うことで、ネットワーク防御をさらに物理的に強化する計画です」（小林氏）

また、これまでの「侵入されない」ための防御に加え、「万一、侵入さ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られている。

「ランサムウェア被害を想定したシミュレーションを常々実施し、DCSのハードディスクについてはあらかじめスペアを調達済みです。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」（渕向氏）

こうした構想を受けて山口は、「もちろんテロロジーでは、データダイオードやレジリエンス強化のソリューションをトータルで提案することができます。社員の皆様の教育・訓練の支援も含め、長期的に伴走サポートしていく所存です」と応える。

丸善石油化学とテロロジーのパートナーシップのもと、千葉工場における包括的なOTシステムセキュリティ強化の取り組みは、さらに大きく前進していくことになるだろう。



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



株式会社テロロジー
宇宙・社会インフラセキュリティ
事業本部
山口 颯太