

# 産業用サイバーセキュリティの強化 -石油・ガスのパイプライン監視-

石油・ガス業界の某大手企業は、既存のシリアルベースの通信インフラストラクチャをイーサネットベースのネットワークにアップグレードすることによって、パイプライン監視ソリューションのセキュリティを強化したいと考えていました。

## 課題

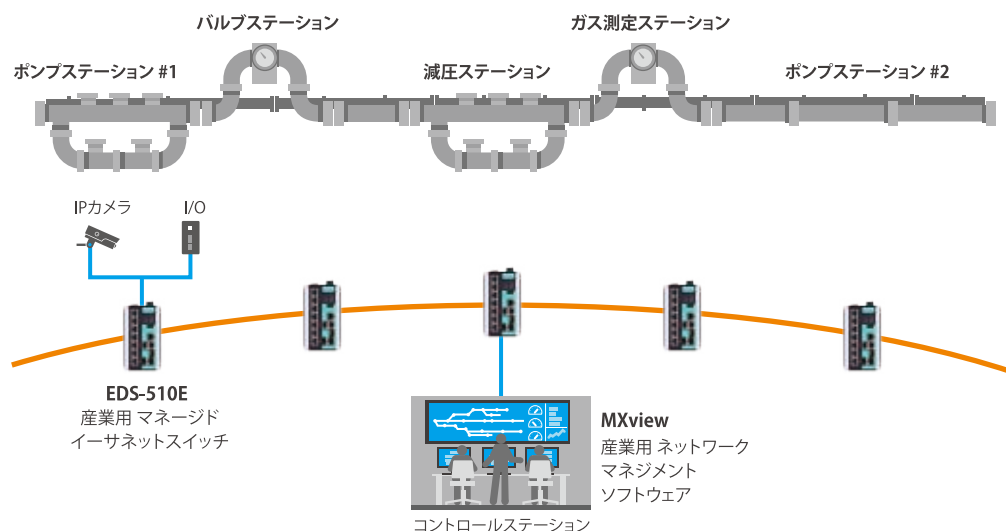
大容量の石油およびガスパイプラインは非常に揮発性が高く、多くの場合数千キロメートルに及びます。パイプライン沿いのポンプ場には分析装置とPLCが装備されています。PLCとI/Oデバイスにはセキュリティ機能が欠けていたため、同社はステーションとリモートSCADAシステム間の安定したネットワーク接続を維持することが困難であると考えました。産業用サイバーセキュリティを強化するために、同社はまずセキュリティポリシーを強化し、各ネットワーク機器に強化されたセキュリティ機能を搭載することを要求するIEC 62443規格に準拠するようにしました。

## Moxaの解決策

Moxaは、現場の産業用ネットワークを産業用マネージドイーサネットスイッチでアップグレードすることを推奨しました。これは、同社のセキュリティポリシーに完全に準拠した高度なセキュリティ機能を備えているためです。

## デバイス保護

- IEC 62443規格に基づく強化された産業用サイバーセキュリティを提供
- MXviewネットワークMXview管理ソフトウェアを介して、リアルタイムで視覚化された中央ネットワーク管理を提供



導入場所:アメリカ合衆国  
分野:石油・ガスパイプライン監視

### 解決のヒント

- IEC 62443規格に基づいて強化されたセキュリティ機能を備えた産業用管理型イーサネットスイッチを配備します。



### MXview

産業用ネットワーク管理ソフトウェア



### EDS-510E

産業用マネージドイーサネットスイッチ

© Moxa Inc. All rights reserved.

MOXAロゴはMoxa Inc.の登録商標です。  
この文書に記載されている他のすべてのロゴは、そのロゴに関連する各企業、製品、または組織の知的財産です。

Copyright © 2019 IBS Japan Co., Ltd.

※このデータシートに掲載されているイラスト・画像についての著作権はMOXAに帰属します。  
※記事内容(日本語翻訳分)についての著作権はアイ・ビー・エス・ジャパン株式会社帰属します。



# 大規模ファクトリーネットワークのセキュリティ状態の可視化

アメリカの某自動車部品メーカーは、製造工程をデジタル化したいと考えていました。しかし、昔に構築された産業用制御ネットワークを使用しており、生産能力要件の増加に対応するために時間外労働を拡大していました。すべてのデバイスを効果的に管理することは、会社にとって難題でした。

## 課題

フィールドデバイスは、制御の統一とデータ収集のためにEtherNet / IPプロトコルで動作します。このプラントは大規模なネットワークインフラストラクチャを必要としていたため、プラントマネージャがすべてのデバイスを監視してネットワークポロジを視覚化することは非常に困難でした。さらに、デジタル化を実現するためには、ネットワークを現場からERPまで、さらにはクラウドまで相互接続する必要があります。生産効率を犠牲にすることなく、この大規模な変更を行うためには、適切なサイバーセキュリティ対策を講じることが不可欠です。

## Moxaの解決策

Moxaは、EtherNet / IPマルチキャストフィルタリングと高度なセキュリティ機能をサポートするように、同社が自社のネットワークを産業用マネージドイーサネットスイッチにアップグレードするのを支援しました。さらに同社は、リアルタイム制御と産業用制御ネットワークの可視化に当社のMXviewネットワーク管理ソフトウェアを導入しました。

## デバイス保護

- マルチキャストトラフィックを管理し、ジッタを軽減するためのEtherNet / IPプロトコルとIGMPスヌーピングをサポート
- セキュリティステータスが一目でわかるリアルタイムの視覚化された中央ネットワーク管理
- IEC 62443規格に準拠した産業用サイバーセキュリティ機能を提供

導入場所:アメリカ合衆国  
分野:ファクトリーオートメーション

### 解決のヒント

- マネージドスイッチとネットワーク管理ソフトウェアの組み合わせは、EtherNet / IPマルチキャストトラフィックフィルタリングの要件も満たしながら、高度なセキュリティ機能とリアルタイムモニタリングを提供するのに理想的なソリューションです

### Moxa 導入製品



EDS-510E

産業用マネージドイーサネットスイッチ



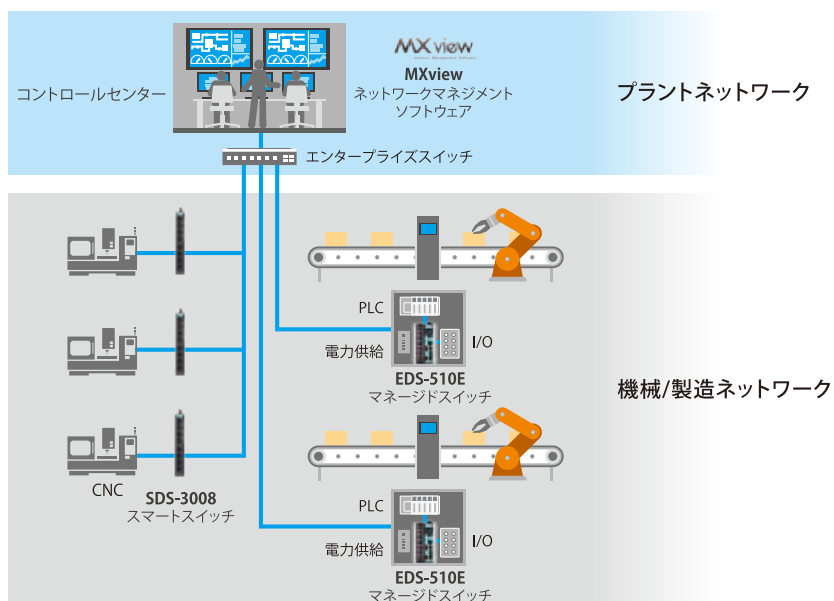
MXview

産業用ネットワーク管理ソフトウェア



SDS-3008

産業用スマートイーサネットスイッチ



© Moxa Inc. All rights reserved.

MOXAロゴはMoxa Inc.の登録商標です。  
この文書に記載されている他のすべてのロゴは、そのロゴに関連する各企業、製品、または組織の知的財産です。



# ファクトリーネットワークをセグメント化することで産業用サイバーセキュリティを強化

台湾の某製鋼工場内には、異なる加工エリアと生産ラインがあります。工場長は、予期しない動作が他の生産ラインに影響を与えるのを防ぐために、生産ライン間のデータ伝送を隔離して分離することを望んでいました。

## 課題

エンタープライズネットワークを制御ネットワークに接続する際、プラントマネージャは潜在的なリスクを軽減するためにITポリシーを順守する必要がありました。プラント管理者にとって最も困難な作業の1つは、すべてのIPアドレスを管理することでした。さらに、ネットワークの産業用サイバーセキュリティを強化するために、プラントは、企業ネットワークから制御ネットワークへのデータ伝送を保護するネットワーク設計を必要としていました。

## Moxaの解決策

エンタープライズネットワークと制御ネットワークを保護するために、MoxaはプラントマネージャにデュアルWANポートを備えたセキュアルータを導入することを推奨しました。これにより、ネットワークの両側が直接通信できない産業隔離領域(DMZ)が確立されます。さらに、Moxaは、IPアドレスの管理を簡素化するために、ファイアウォールを装備した安全なルータを使用してネットワークをセグメント化し、ネットワークアドレス変換を実行することを提案しました。

## デバイス保護

- 産業用レイヤ2スイッチをサポートし、ネットワークをセグメント化してトラフィックをフィルタリングするためのファイアウォール
- IPアドレスのマッピングと管理用にNATをサポート
- 異なるネットワークサブネット間のルーティングをサポート
- 重要なアプリケーションの信頼性を高めるための工業用設計

導入場所:台湾  
分野:ファクトリーオートメーション

### 解決のヒント

- ファイアウォールとスイッチ機能を備えた安全なルータを配置すると、ネットワークを分割してデータフィルタリングを実行できます。さらに、NATを利用してIPアドレスの管理を簡素化できます。

### Moxa 導入製品



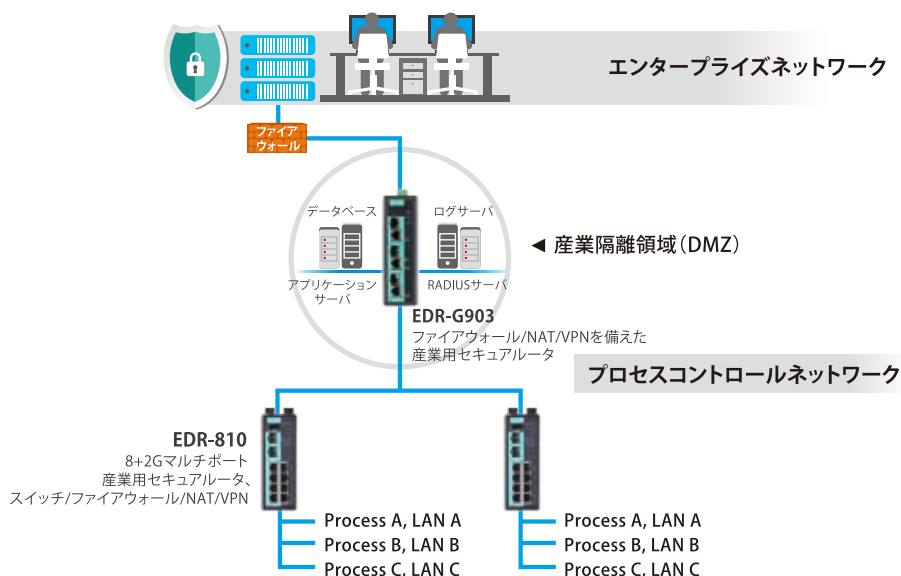
**EDR-G903**

ファイアウォール/NAT/VPNを備えた産業用セキュアルータ



**EDR-810**

8+2Gマルチポート産業用セキュアルータ、スイッチ/ファイアウォール/NAT/VPN



© Moxa Inc. All rights reserved.

MOXAロゴはMoxa Inc.の登録商標です。  
この文書に記載されている他のすべてのロゴは、そのロゴに関連する各企業、製品、または組織の知的財産です。



# 改良されたマシナリーサービスへの 簡単で安全なリモートアクセス

ネットワークの稼働時間を最大化すると、機械の生産性が向上します。したがって、機械式動力プレスの大手メーカーは、改善された機械性能と効果的なトラブルシューティングを確実にするために、世界中の顧客に対してよりタイムリーで効率的なアフターサービスを提供する必要がありました。

## 課題

当初、マシンビルダーはWindowsベースのリモートデスクトップコントロール(RDC)テクノロジーを採用していましたが、回避したいと重大なセキュリティリスクと追加コストがありました。WindowsベースのRDCでは、Windowsで動作するコンピュータを工場にインストールする必要があります。ただし、Windowsベースのコンピュータはセキュリティ上のリスクを受けやすく、インターネットに接続するとサイバー攻撃の可能性がさらに高まります。セキュリティリスクを回避するために、機械メーカーは複雑なIT関連のファイアウォール機器を採用する必要がありますが、これは時間がかかり管理が困難です。

## Moxaの解決策

リモート接続ソリューションの中でも、MoxaのMRCソリューションは、エンドツーエンドのセキュリティと完全に統合されたセキュリティ、使いやすさ、クラウドベースの柔軟性、厳しい工場環境での信頼性など、さまざまな理由で際立っています。クラウドベースのリモートアクセス接続を構築するために必要なコンポーネントは、MRCゲートウェイ、クラウドサーバー、およびクライアントソフトウェアの3つだけです。

## セキュアなネットワークインフラストラクチャ

- エンドツーエンドのデータ暗号化を使用した完全に統合された安全な接続
- クラウドベースの相互接続とサービススケーラビリティのためのセキュリティ管理
- ワンクリックで、ITの専門知識を持たないエンジニアは、複雑なファイアウォール設定やIP管理を行わなくてもリモートマシンにアクセス可能

導入場所:台湾  
分野:ファクトリーオートメーション

### 解決のヒント

- ローカルネットワークからの隔離された保護のためのアウトオブバンドLTEセルラー接続と、エンドツーエンドのデータ暗号化を備えた完全に統合された安全な接続の導入により、ITセキュリティ要件と安全なリモートアクセスニーズを同時に満たすことができます。

### Moxa 導入製品



### Moxa Remote Connect Suite

安全なリモートアクセスのための  
リモート接続管理プラットフォーム



© Moxa Inc. All rights reserved.

MOXAロゴはMoxa Inc.の登録商標です。  
この文書に記載されている他のすべてのロゴは、そのロゴに関連する各企業、製品、または組織の知的財産です。

Copyright © 2019 IBS Japan Co., Ltd.

※このデータシートに掲載されているイラスト・画像についての著作権はMOXAに帰属します。  
※記事内容(日本語訳分)についての著作権はアイ・ビー・エス・ジャパン株式会社に帰属します。



## 相互接続された交通信号通信の保護

米国のHenrico Countyは、既存のクローズドループ交通信号制御システムをNEMA TS2に準拠した分散交通管理システムにアップグレードしたいと考えていました。中央の指令センターから、オペレータはリアルタイムの監視のために遠隔の交通管制場所で交通信号にアクセスし、緊急事態により迅速に対応することができます。

### 課題

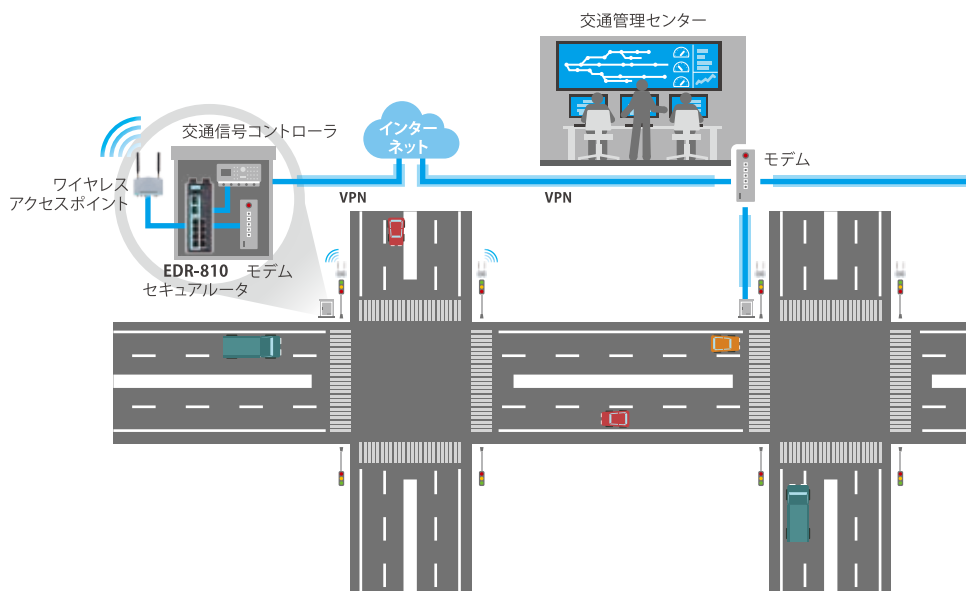
この高度な交通管制ネットワークは、公衆ネットワーク全体に展開され、システム通信の整合性を確保するために、信頼性の高い接続とVPNやファイアウォールなどのサイバーセキュリティ保護が必要になります。交通管制官が円滑にデータを交通管制センターに送信するために、システムインテグレータは、通信にモデムを必要とする既存のISP公衆網を利用しました。ただし、トラフィック制御ネットワークはセキュリティ上の脅威に弱いため、安全なデータ通信を確保するためにはVPNとファイアウォールが不可欠です。

### Moxaの解決策

Moxaは、データ通信とデータセキュリティのために各交差点にある路側キャビネットにEDR-810セキュアルータを設置することを推奨しました。EDR-810シリーズは、安全なリモートアクセスを提供し、重要なフィールド機器を保護するVPNおよびファイアウォール機能をサポートしています。

### セキュアなネットワークインフラストラクチャ

- フィールドキャビネットと中央オペレーションセンター間のVPNトンネリング用に20MbpsのVPN帯域幅をサポート
- 光ファイバリングトポロジを必要とする将来の拡張のためのRSTPおよびTurbo Ringテクノロジーを備えた2ギガビットファイバポート



導入場所: Henrico County  
(アメリカ合衆国)  
分野: インテリジェント交通

### 解決のヒント

- ファイアウォール、VPN、およびスイッチを備えた安全なルーターを配置すると、データ転送が暗号化され、信頼性が向上する冗長ネットワークが提供されます。

### Moxa 導入製品



#### EDR-810

8+2Gマルチポート産業用セキュアルータ、スイッチ/ファイアウォール/NAT/VPN

© Moxa Inc. All rights reserved.

MOXAロゴはMoxa Inc.の登録商標です。  
この文書に記載されている他のすべてのロゴは、そのロゴに関連する各企業、製品、または組織の知的財産です。

Copyright © 2019 IBS Japan Co., Ltd.

※このデータシートに掲載されているイラスト・画像についての著作権はMOXAに帰属します。  
※記事内容(日本語翻訳分)についての著作権はアイ・ビー・エス・ジャパン株式会社に帰属します。