



# 重要インフラの使用事例

データダイオードサイバーセキュリティの使用による産業用制御システムの防御



**OWL CYBER DEFENSE**

1-866-695-3387

[WWW.OWLCYBERDEFENSE.COM](http://WWW.OWLCYBERDEFENSE.COM)

OWL 日本輸入販売総代理店

**Dírex**  
JAPAN DIREX CORPORATION

# 次世代サイバーセキュリティソリューション

**米国国土安全保障省 (DHS)** は、保有する資産、システム、およびネットワークが米国にとって必要不可欠であると見なされる 16 セクターの重要インフラを規定している。それらが、弱体化または崩壊した場合に国の安全保障、経済、および/または市民の健康と安全に著しい影響を及ぼす。

**該当するセクターは以下の通りです。**

- 化学産業
- 商業施設
- 通信
- 重要な製造業
- ダム
- 防衛産業基盤
- 緊急サービス
- エネルギー
- 銀行・金融サービス
- 農業・食料
- 政府施設
- ヘルスケアおよび公衆衛生
- 情報技術
- 原子力施設、核物質、核廃・棄物
- 輸送
- 上下水道

この報告書は、これらの多種多様な重要インフラセクターを防衛するために Owl 社のデータダイオードサイバーセキュリティを実装する 16 の使用実例について概略を記している。使用実例では、業界の大手企業について特記し、また Owl 社がいかに一方向の決定論的データフローを通して多くのセキュリティおよび運営上の要件を満たすために役立ったのかを明示する。これらの各使用実例において、Owl 社のデータダイオードは、以下に挙げる多様な最先端の運用技術との相互運用が行われている：それらは、OSIsoft PI System、Schneider Electric Wonderware、GE Historian、Rockwell Automation FactoryTalk、Modbus、OPC、モバイルネットワーク、およびソフトウェアファイアウォールなどであるが、この限りではない。**本書で言及される全セクターおよびテクノロジーの一覧と参照については、本書末尾の索引をご覧ください。**

これらの使用実例が、Owl 社の能力、そして今日のサイバーセキュリティ問題の解決にデータダイオードが役立ついくつかの方法をご紹介します手立てとなれば幸いである。

# 目次

- 1 .....** 世界的な石油・ガス企業が本社への一方向生産データ転送を実現
- 3 .....** 天然ガス企業が本社への生産データ転送の安全を確保し、遠隔警報監視を実現
- 5 .....** ガスタービンのベンダーが発電所の安全な監視を実現
- 7 .....** 石油化学製品企業がビジネス IT への安全な一方向生産データフローを実現
- 9 .....** レアアース採掘企業が最先端の持続的 攻撃に対する運営ネットワークの安全を確保
- 11 .....** 上下水道企業が DHS の多層防御サイバーセキュリティ戦略を実装
- 13 .....** 原子力発電所がアメリカ合衆国原子力規制委員会のサイバーセキュリティ規制を遵守
- 15 .....** 石炭発電所が NERC CIP バージョン 5 サイバーセキュリティ規制を遵守
- 17 .....** 天然ガス発電所が NERC CIP サイバーセキュリティ規制を遵守し、ベンダー遠隔監視を実現
- 19 .....** 電力公社が 10 箇所の発電所で NRC、NERC CIP サイバーセキュリティ規制を遵守
- 21 .....** 送配電変電所が NERC CIP バージョン 5 サイバーセキュリティ規制を遵守
- 23 .....** 米国法銀行がセントラルリポジトリデータベースで ATM データ収集の安全を確保
- 25 .....** 米国地方銀行が遠隔ネットワーク監視を実現監視
- 27 .....** 中堅企業向け全国銀行がフォレンジックデータファイルの捕獲キャプチャおよび収集を実行
- 29 .....** 米国地方銀行が取引および顧客記録の社外バックアップの安全を確保
- 31 .....** 全米通勤鉄道会社が遠隔車両・レール監視の安全を確保
- 33 .....** ヘルスケアシステムが電子医療カルテの研究データベースの安全を確保
- 35 .....** 索引

世界的な石油・ガス企業が本社への  
生産データの一方方向転送を実現

### 企業の概要

年間原油生産量が 30 億バレル以上の世界的な石油・ガス生産・製造・販売業者。

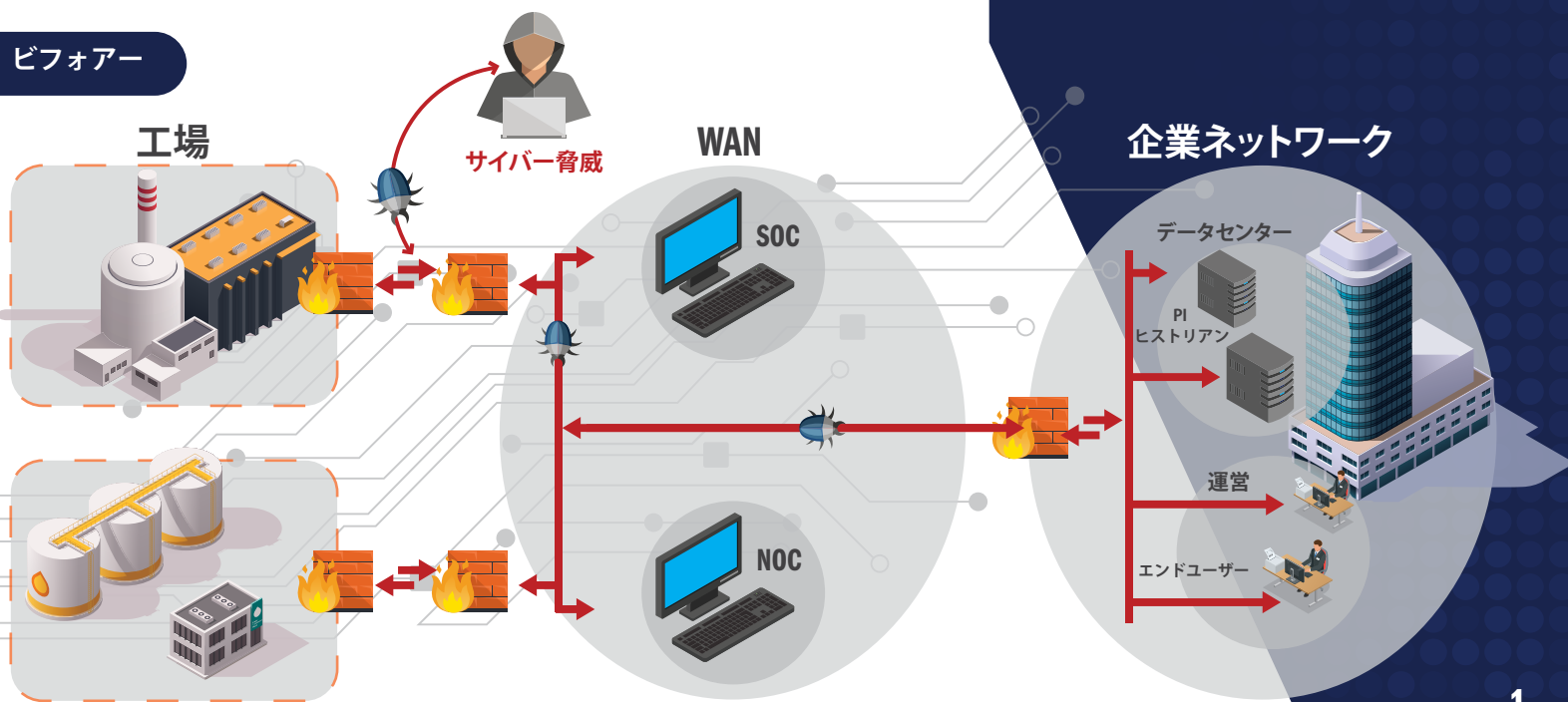
### サイバーセキュリティに関する課題

マルウェア侵害によりデータサーバーおよびアプリケーションサーバーが破壊され、日常業務に深刻な影響が及んだ。その対策として、会社は広域通信網 (WAN) から同社の運用技術 (OT) ネットワークを切り離し、企業 IT ネットワークから WAN を切り離した。工場を切り離すことでマルウェアが様々なネットワークに拡散することを防ぐことはできたが、業務を継続できず、また工場の稼働状況を把握できなくなった。

### 要求事項

- 業務の継続および稼働状況把握を回復すること
- 「切断された」またはセグメント化されたサイバーセキュリティアーキテクチャを維持すること
- フェイルオーバー、冗長性、および負荷分散機能
- 必要に応じて容量またはデータタイプを追加できる拡張可能なアーキテクチャ
- セキュリティ運用および技術を集中管理する能力

### ビフォー



### 事例の概要

👤 産業：  
石油・ガス生産

⚡ 課題：  
マルウェア侵害がデータを破壊し、その結果、会社が運営・事業ネットワークを切り離さなければならなかった

🛡️ 解決策：  
DualDiode® テクノロジーを備えた Owl 社のデータダイオードを OPTS PI System ヒストリアンレプリケーションソフトウェアと共に配備した。

📊 メリット：  
本社への決定論的一方方向生産データフローにより、リスクを高めることなく可視性を向上させることができた。集中化性能・データフローモニタリング

## 解決策

ネットワークの効果的なセグメント化、そして工場資産から WAN 内のネットワーク運営センターまでの IT シスログフローを含む確実な一方向データ転送に、Owl 社の DualDiode Technology® (OPDS/EPDS) が採用された。本社への OT データの転送を可能にするために、OSIssoft® PI System ヒストリアンレプリケーション (OPTS) も追加された。

### ハードウェア

#### Owl 周辺機器防御ソリューション - 多目的 (OPDS-MP)

ネットワークのセグメント化および決定論的一方向データ転送専用設計された内蔵型 1U データダイオード。



### ハードウェア

#### 企業周辺機器防御ソリューション (EPDS)

ネットワークのセグメント化と決定論的一方向データ転送に、独立型の送信専用および受信専用の商用サーバーにマウントされる一対のデータダイオード通信カード。



\*Owl 社では、一対の Dell PowerEdge R620 サーバーまたは同等製品を使用。

### インターフェースモジュール

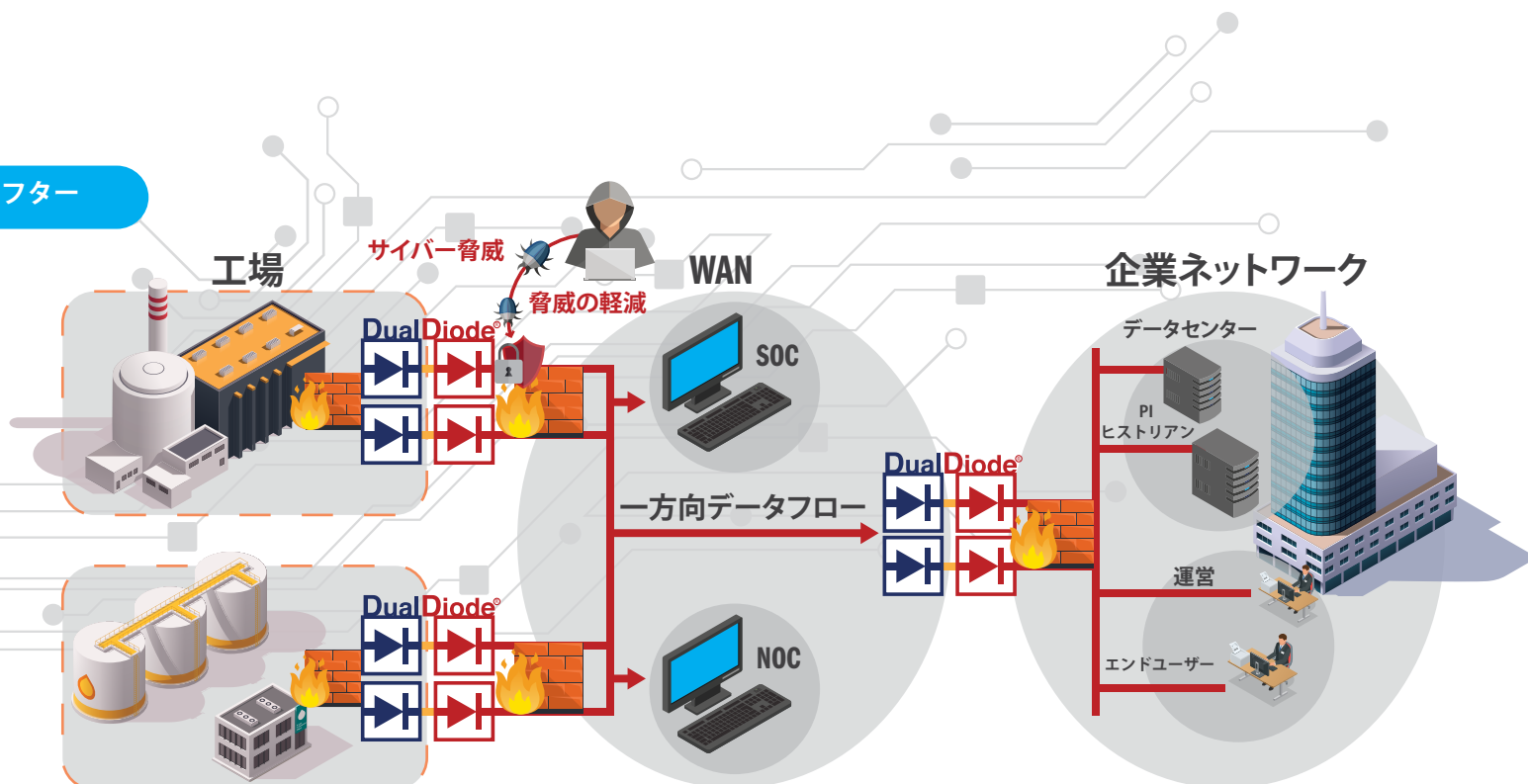
#### Owl PI 転送サービス (Owl PI Transfer Service、OPTS)

OSIssoft® PI System ヒストリアンデータをネットワーク境界を越えて安全に複製・転送するために特別に開発された専用ソフトウェア。

## 結果

- 工場の OT および本社の IT ネットワーク境界のどちらにおいても、効果的なネットワークのセグメント化を通してセキュリティを提供でき、マルウェアの侵害および拡散を防ぐことに役立った
- 工場から企業のデータストアまでの冗長的、決定論的なアウトバウンド OT データフローを可能にした
- OSIssoft® データヒストリアンを複製し、生産データのフル活用と本社内部からの可視性が実現した
- セキュリティ運営センターからの集中モニタリングによるセキュリティ性能について深い見識が得られた

アフター



遠隔監視のために、天然ガス企業が本社への安全な生産データ転送を実現

### 企業の概要

年間総生産能力が 3600 万トンの液化天然ガス生産業者。

### サイバーセキュリティに関する課題

マルウェア侵害によりデータサーバーおよびアプリケーションサーバーが破壊され、日常業務に深刻な影響が及んだ。その対策として、会社は企業 IT ネットワークから同社の運用技術 (OT) ネットワークを切り離した。工場との電子通信を切断することでマルウェアの拡散を防ぐことはできたが、業務を継続できず、また工場の稼働状況を把握できなくなった。

### 要求

- 業務の継続および稼働状況把握を回復すること
- 「切断された」またはセグメント化されたサイバーセキュリティアーキテクチャを維持すること
- OT ネットワークから企業 IT ネットワークへOSIsoft PI System ヒストリアン複製を可能にすること
- 企業ネットワーク運営センターからの遠隔警報監視を可能にすること

### 事例の概要

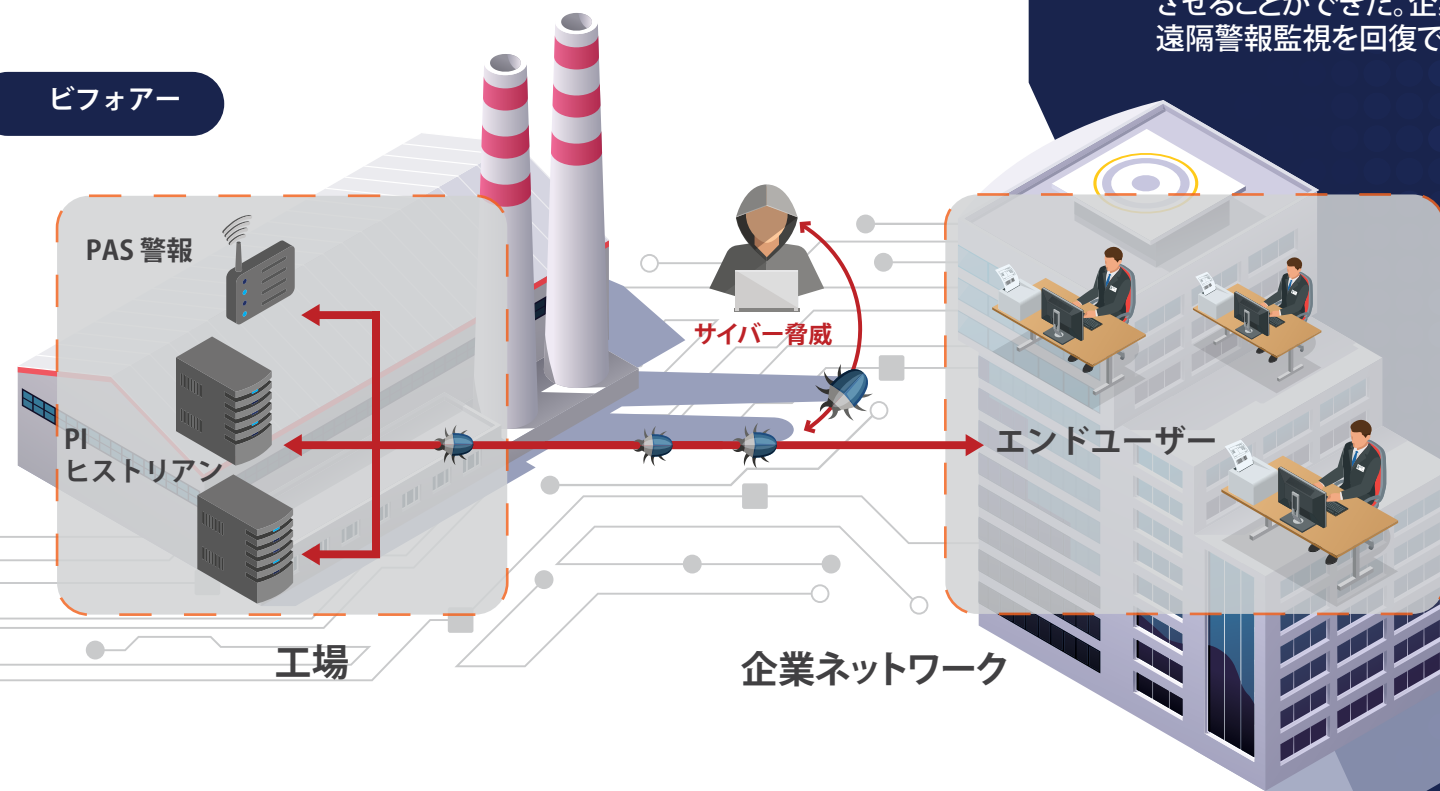
🏭 産業：  
天然ガス生産

🔦 課題：  
マルウェア侵害が運営データを破壊し、その結果、会社が運営・事業ネットワークを切り離さなければならなくなった

🛡️ 解決策：  
DualDiode Technology® を備えた Owl 社の EPDS データダイオードを OPTS PI System ヒストリアンレプリケーションアプリケーションと共に配備した。

📈 メリット：  
本社への決定論的一方向 PI System/OT データフローにより、生産設備へのリスクを高めることなく可視性を向上させることができた。企業 IT の遠隔警報監視を回復できた。

### ビフォー



## ▼ 解決策

ネットワークの効果的なセグメント化、そして工場資産から企業本社までの IT システムを含む確実な一方データ転送に、Owl 社の DualDiode Technology® (OPDS/EPDS) が採用された。本社への OT データの転送を可能にするために、OSIsoft® PI System ヒストリアンレプリケーション (OPTS) も追加された。

## ハードウェア

### 企業周辺機器防御ソリューション (EPDS)

ネットワークのセグメント化と決定論的一方データ転送用に、独立型の送信専用および受信専用の商用サーバーにマウントされる一対のデータダイオード通信カード。

## インターフェースモジュール

### Owl PI 転送サービス (Owl PI Transfer Service、OPTS)

OSIsoft® PI System ヒストリアンデータをネットワーク境界を越えて安全に複製・転送するために特別に開発された専用ソフトウェア。

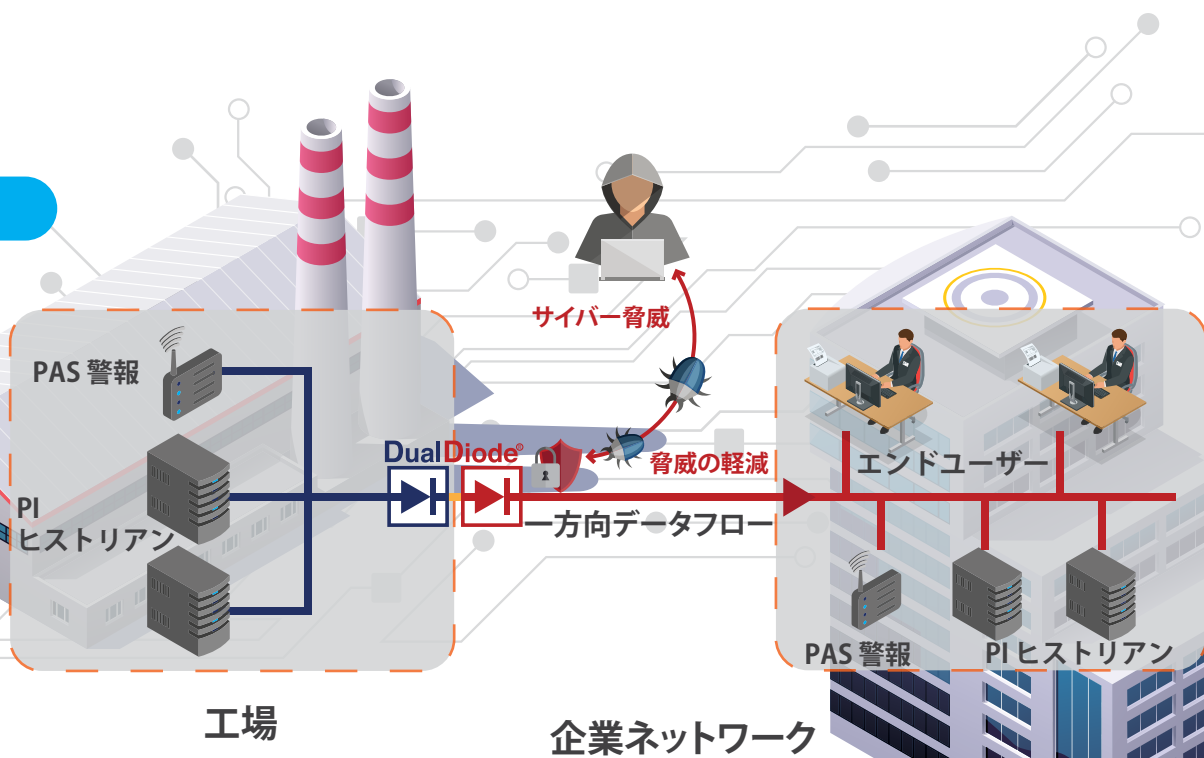


\*Owl 社では、一対の Dell PowerEdge R620 サーバーまたは同等製品を使用。

## ✓ 結果

- 工場 OT ネットワークの効果的なセグメント化によりネットワークサイバーセキュリティを提供することで、マルウェアの侵害および拡散を防ぐことに役立った
- 工場から会社のデータストアへ、決定論的アウトバウンド OT データフローを許可した
- PI System データヒストリアンを複製し、生産データのフル活用と本社内部からの可視性を実現した
- 工場資産から企業のユーザーまでの警報データフローを回復した

アフター





# 使用実例 ガスタービン

周辺機器防御ソリューション

ガスタービンのベンダーがタービンの  
安全な遠隔監視を実現

## 企業の概要

ガスタービンのメーカー兼ベンダーで、天然ガス発電所に製品および遠隔監視サービスを供給している。

## サイバーセキュリティに関する課題

天然ガス発電所と結んだサービスレベルアグリーメント (SLA) の合意に沿った義務に基づき、ガスタービンベンダーは発電所に設置されたそのタービン装置に遠隔監視機能を求めた。しかし、深刻なマルウェア侵害により工場のデータおよびサーバーが破壊されて日常業務に深刻な影響が及び、その結果、運用技術 (OT) を外部ネットワークから切り離すことになった。これによりマルウェアの拡散を防ぐことはできたが、タービンベンダーが設置した遠隔監視機能も無効になった。

## 要求

- SLA を履行するために、リモートタービン稼働状況の可視性を回復すること
- 「切断された」またはセグメント化されたサイバーセキュリティアーキテクチャを維持すること
- グローバルモニタリングセンターからタービンベンダーによるリモートタービンの性能・警報監視を可能にすること

## 事例の概要

👤 産業：  
製造

🔦 課題：

発電所におけるマルウェア侵害がデータを破壊し、多くのアプリケーションサーバーが動作不能となったため、その結果 OT ネットワークを切断し、タービンベンダーとの間で合意した SLA が履行されない

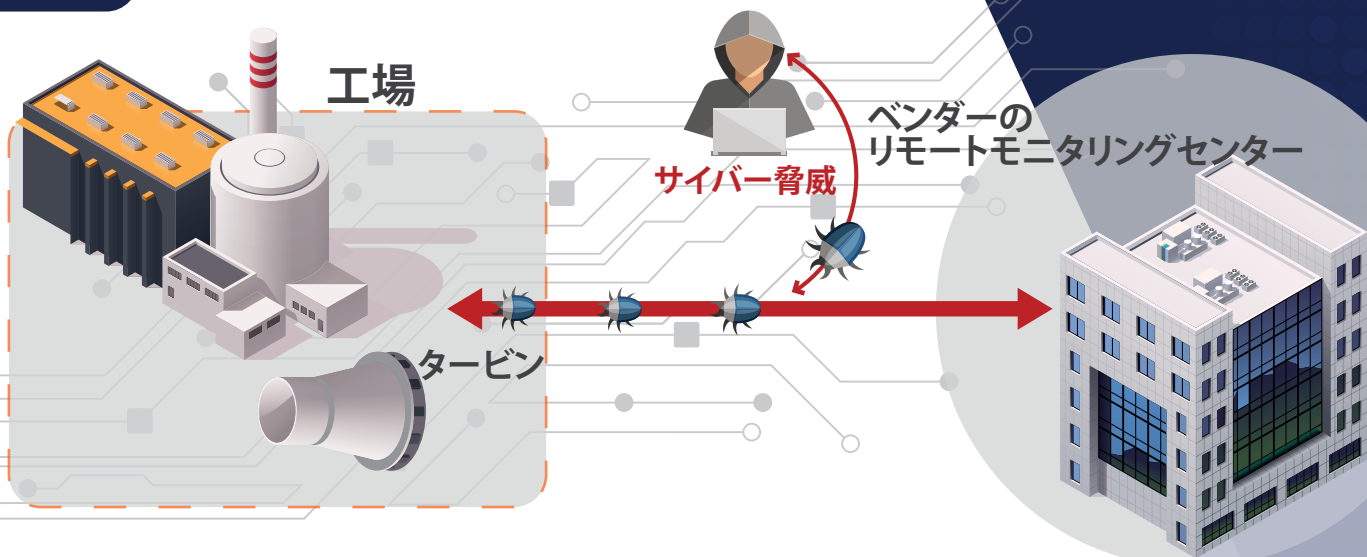
🛡️ 解決策：

工場の安全確保とタービンベンダーへのモニタリングデータの送信のために、Owl 社の DualDiode Technology® 付き OPDS-100 データダイオードが工場 OT ネットワークに配備された。

📋 メリット：

ベンダーへの決定論的一方向データ転送を通して、タービン性能データおよび警報データの遠隔監視が可能になった

## ビフォー



## 解決策

決定論的一方向データフローに、DualDiode Technology を使用した Owl 社のデータダイオード (OPDS-100) ネットワークセキュリティが採用された。これにより、重要なタービン性能および警報データの複製、そして工場 OT ネットワークからタービンベンダーのグローバルモニタリングセンターへの転送が可能になった。

### ハードウェア

#### Owl 社の周辺機器防御ソリューション - 100 (OPDS-100)

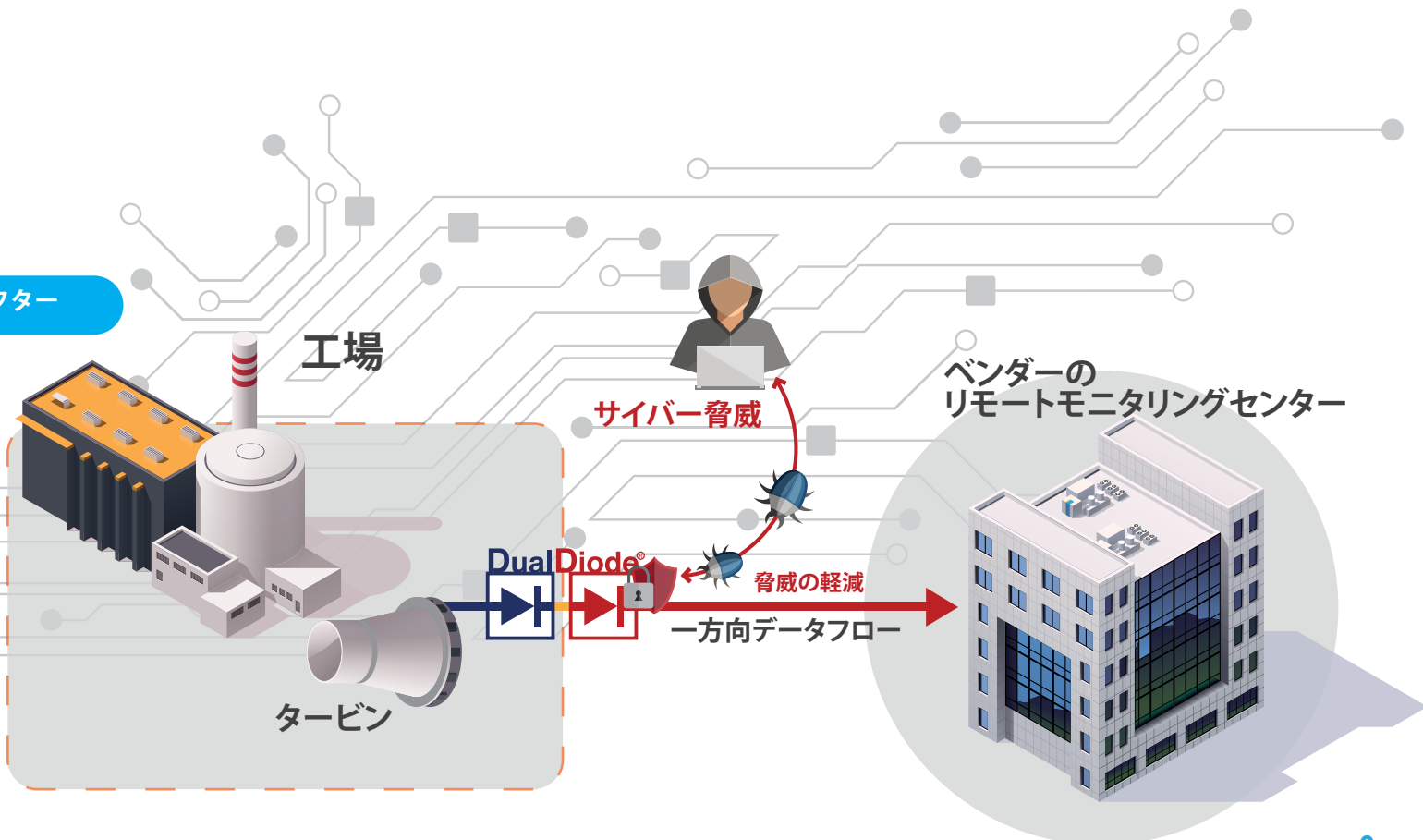
ネットワークのセグメント化および決定論的一方向データ転送専用のための内蔵型 1U データダイオード。



## 結果

- 工場 OT ネットワークの効果的なセグメント化によりネットワークサイバーセキュリティを提供し、マルウェアの侵害および拡散を防ぐことに役立った
- タービンベンダーデータ収集が、データダイオードからモニタリングセンターへ UDP 経由でデータを「プッシュ」するように改良された
- 工場からタービンベンダーまでのアウトバウンドタービン性能データフローが回復し、SLA 要件を満たした
- 工場資産からタービンベンダーのグローバルモニタリングセンターまでの警報データフローを可能にした

アフター





# 使用実例 石油化学製品

周辺機器防御ソリューション

石油化学製品企業がビジネス IT への  
安全な一方向生産データフローを実現

## 企業の概要

年間生産量が 200 万トンを超える大手の石油化学製品メーカー。

## サイバーセキュリティに関する課題

マルウェア侵害によりデータおよびサーバーが破壊され、日常業務に深刻な影響が及んだ。その対策として、会社は広域通信網 (WAN) から同社の運用技術 (OT) ネットワークを切り離し、本社の企業 IT ネットワークから WAN を切り離した。これによりそれ以上のマルウェアの拡散を防ぐことはできたが、深刻な電子通信の破壊により可視性の不足と業務継続の困難を招いた。

## 要求

- 「切断された」またはセグメント化されたサイバーセキュリティアーキテクチャの維持
- オープンプラットフォーム通信 (Open Platform Communications、OPC) サーバーの複製による工場性能データの企業 IT ネットワークへの復元
- OT ネットワークから企業 IT ネットワークへ OSIsoft PI System ヒストリアン複製を可能にすること
- 企業本社におけるリアルタイムな OPC 警報モニタリングを可能にすること

## 事例の概要

産業：

石油化学製品生産

課題：

マルウェア侵害がデータを破壊し、その結果、会社が運営・事業ネットワークを切り離さなければならなくなった

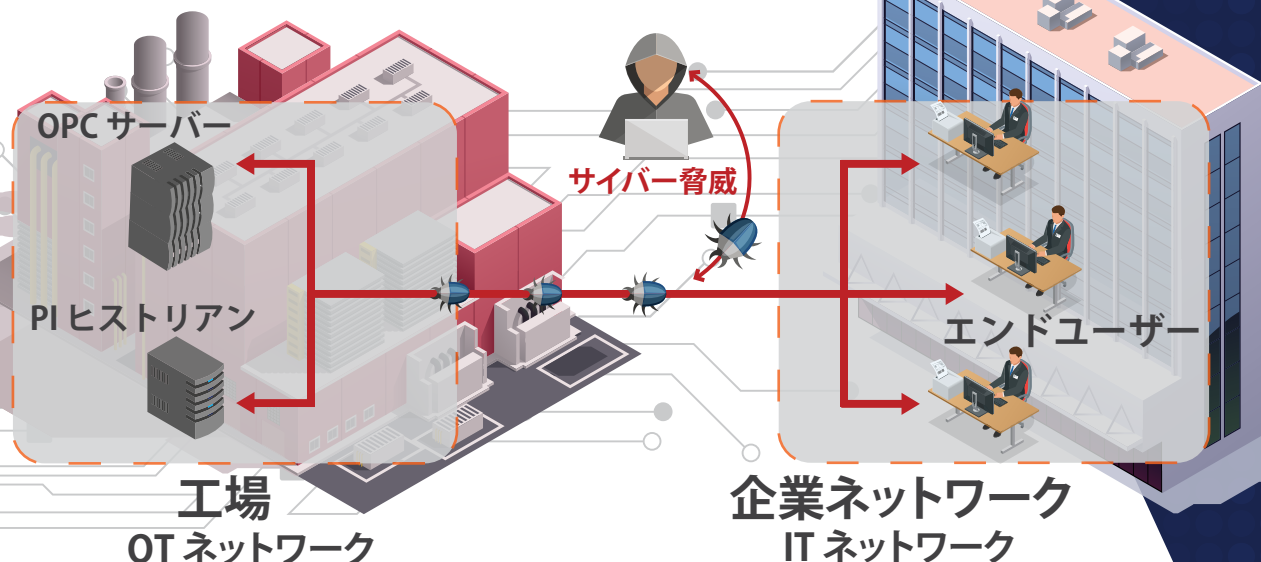
解決策：

業務の持続を再確立するために、DualDiode Technology® を備えた Owl 社の OPDS データダイオードを OPTS PI System レプリケーションおよび OSTs OPC レプリケーションアプリケーションと共に配備した

メリット：

本社への決定論的一方向 PI System/OT データフローにより、リスクを高めることなく可視性を向上させることができた。企業本社におけるリアルタイムな OPC 警報モニタリングを実現した

## ビフォー



## 解決策

ネットワークの効果的なセグメント化、OT 資産から企業ネットワークへの決定論的一方向データ転送に、DualDiode Technology (OPDS-MP) 使用した Owl 社のデータダイオードが採用された。OPC サーバーレプリケーションの他にも、工場稼働データをビジネスユニットに転送できるようにするために、PI System レプリケーション (OPTS) が追加された。

### ハードウェア

#### Owl 周辺機器防御ソリューション - 多目的 (OPDS-MP)

ネットワークのセグメント化および決定論的一方向データ転送専用設計された内蔵型 1U データダイオード。

### インターフェースモジュール

#### OPC セキュア転送サービス (Secure Transfer Service、OSTS)

ネットワークの境界を越えた安全でリアルタイムな OPC データおよびイベントのモニタリングのために特化し認定を受けたアプリケーション。

### インターフェースモジュール

#### Owl PI 転送サービス (Owl PI Transfer Service、OPTS)

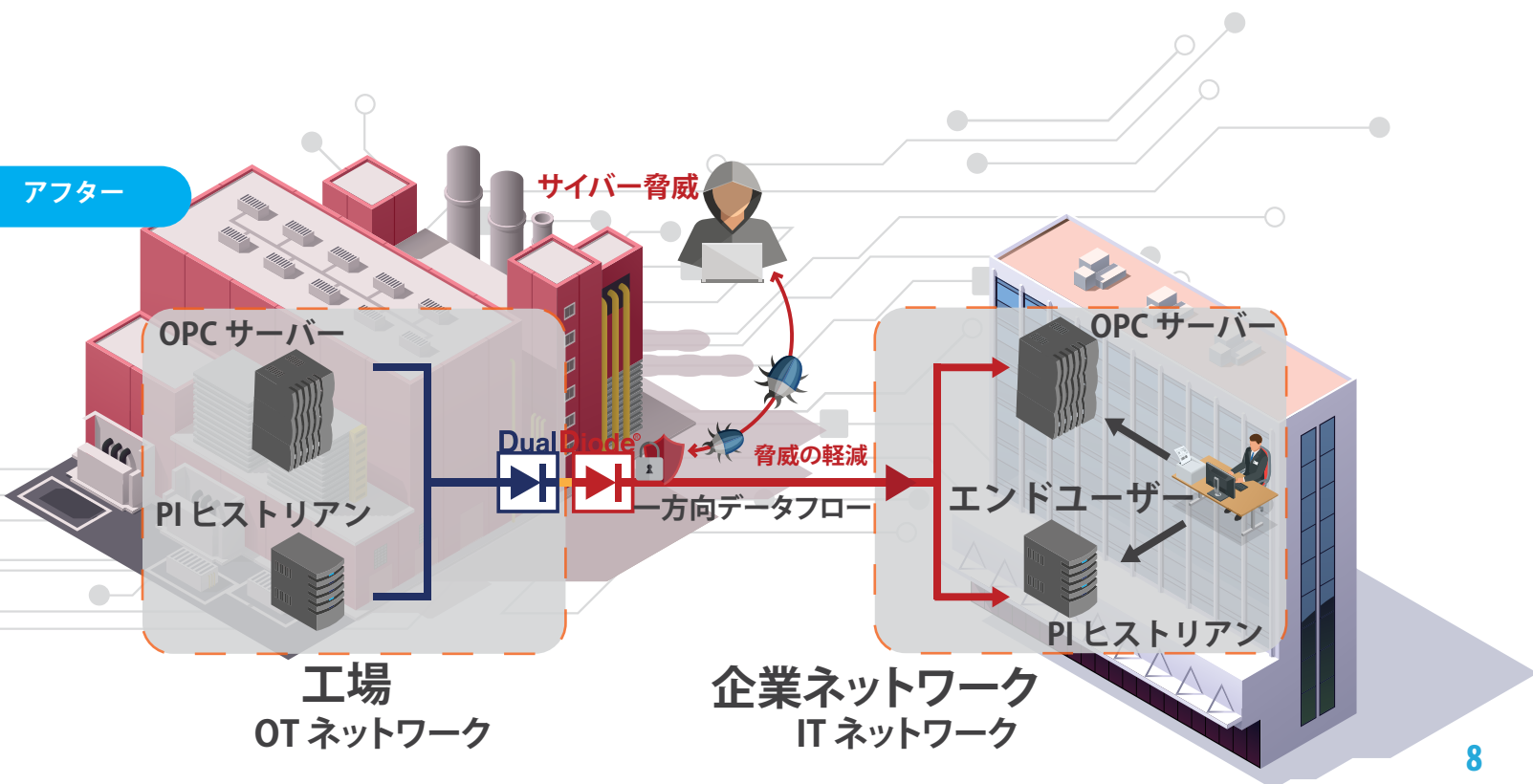
OSIsoft® PI System ヒストリアンデータをネットワーク境界を越えて安全に複製・転送するために特別に開発された専用ソフトウェア。



## 結果

- 工場の OT ネットワーク境界において効果的なネットワークのセグメント化を保持し、マルウェアの侵害および拡散を防ぐことに役立った
- 可視性の向上と業務の継続のため、工場から会社のデータストアまでの決定論的アウトバウンド PI System/OT データフローを許可した
- リアルタイムな OPC データを複製することで、性能、警報、およびイベントデータへの会社のエンドユーザーによるアクセスが可能になった

アフター



レアアース採掘企業が先進的な  
持続的脅威に対する運営ネットワーク  
の安全を確保

## 企業の概要

10 カ国に設備を構えるレアアースおよびレアメタルの採掘・生産会社。

## サイバーセキュリティに関する課題

この会社は、持続的標的型攻撃 (APT) を繰り返し受けた。その対策として、会社は外部の全ネットワークから同社の運用技術 (OT) ネットワークを切り離れた。これにより攻撃を防ぐことには成功したが、会社の運営施設における可視性の不足につながり、業務の継続に支障が出た。

## 要求

- Rockwell PLC によって生成される全運営データを OSIsoft® PI System ヒストリアンに保管すること
- OT ネットワークからの PI System データを会社のエンドユーザーへ複製すること
- 「切断された」またはセグメント化されたサイバーセキュリティアーキテクチャを維持し、一切の OT ネットワークへのインバウンドデータフローを防止すること

## 事例の概要

👤 産業：

レアアース採掘

🚀 課題：

APT で繰り返される侵害行為により、会社はあらゆる外部ネットワーク接続から OT ネットワークを切り離すことになった

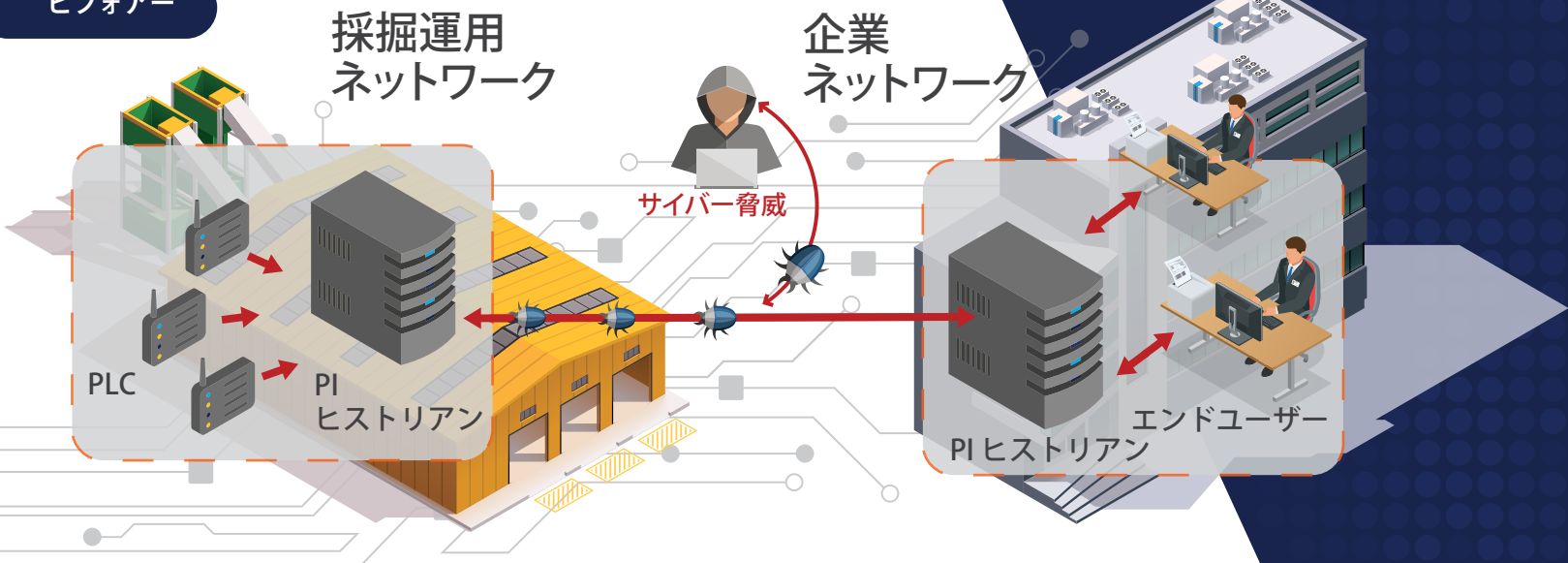
🛡️ 解決策：

DualDiode Technology® を備えた Owl 社の OPDS データダイオードを OPTS PI System レプリケーションアプリケーションと共に配備した

📋 メリット：

決定論的一方向データフローが OT ネットワークを外部の影響または攻撃から守り、会社のエンドユーザーにへの PI System 複製を可能にした

## ビフォー



## 解決策

APT に対する OT ネットワークの安全確保に、DualDiode Technology (OPDS-MP) を使用する Owl 社のデータダイオードが採用された。これにより、ネットワークの効果的なセグメント化、そして OT ネットワークから発信される決定論的一方方向データ転送を実現した。採掘運営データをビジネスユニットに転送できるようにするために、PI System レプリケーション (OPTS) が追加された。

### ハードウェア

**Owl 周辺機器防御ソリューション - 多目的 (OPDS-MP)**  
ネットワークのセグメント化および決定的一方方向データ転送専用設計された内蔵型 1U データダイオード。

### インターフェースモジュール

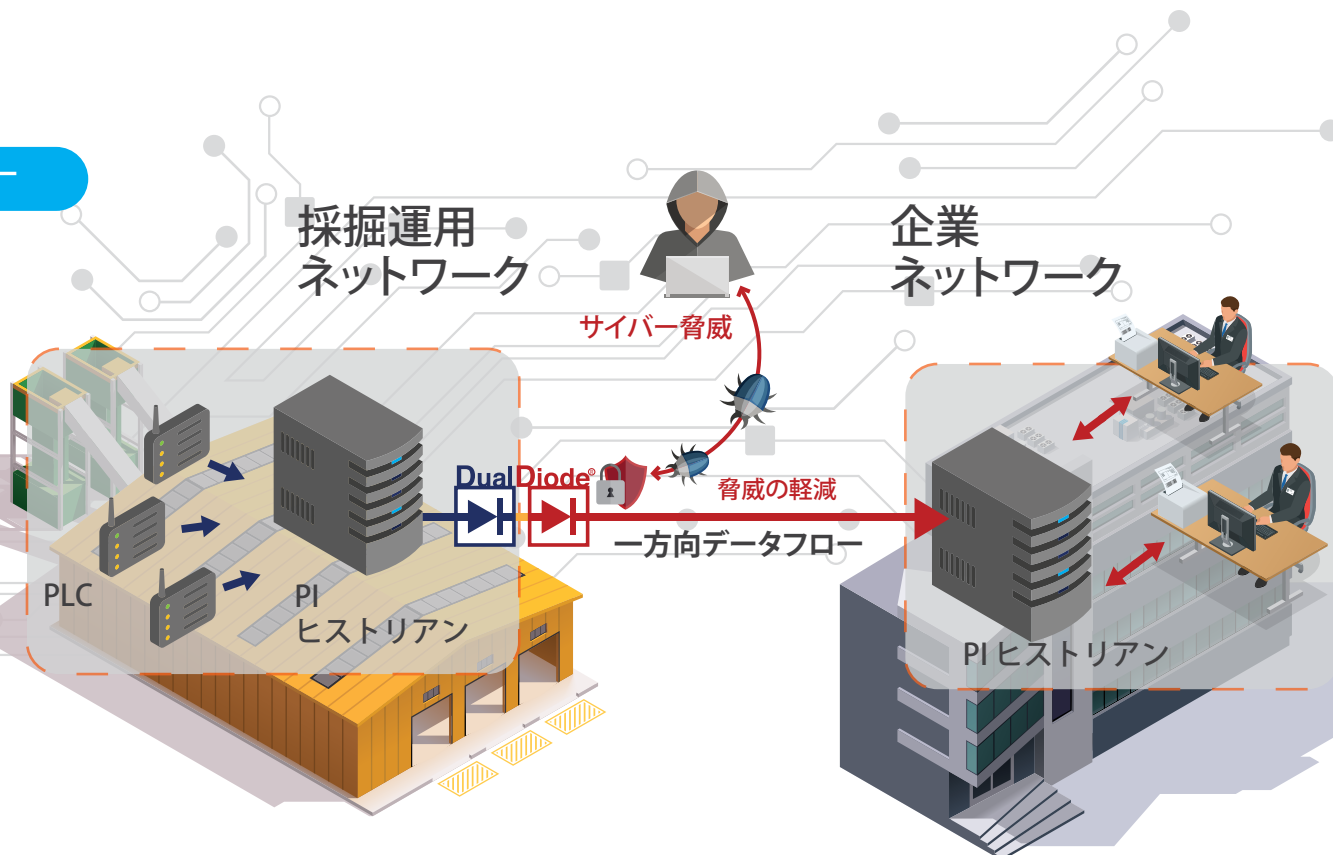
**Owl PI 転送サービス (Owl PI Transfer Service、OPTS)**  
OSIsoft® PI System ヒストリアンデータをネットワーク境界を越えて安全に複製・転送するために特別に開発された専用ソフトウェア。



## 結果

- OT ネットワークの効果的なセグメント化を通してセキュリティを提供し、APT による侵害を防ぐことに役立った
- 可視性の向上と業務の継続のため、OT ネットワークから会社のデータストアまでの決定論的アウトバウンドデータフローを許可した
- Rockwell 運営データがローカルの PI ヒストリアンに捕獲され、会社のネットワークに複製された
- PI System ヒストリアンを複製することで、性能、警報、およびイベントデータへの会社のエンドユーザーによるアクセスが実現した

アフター



#### 企業の概要

80 万人以上の顧客にサービスを提供する地方の大手水道公社。

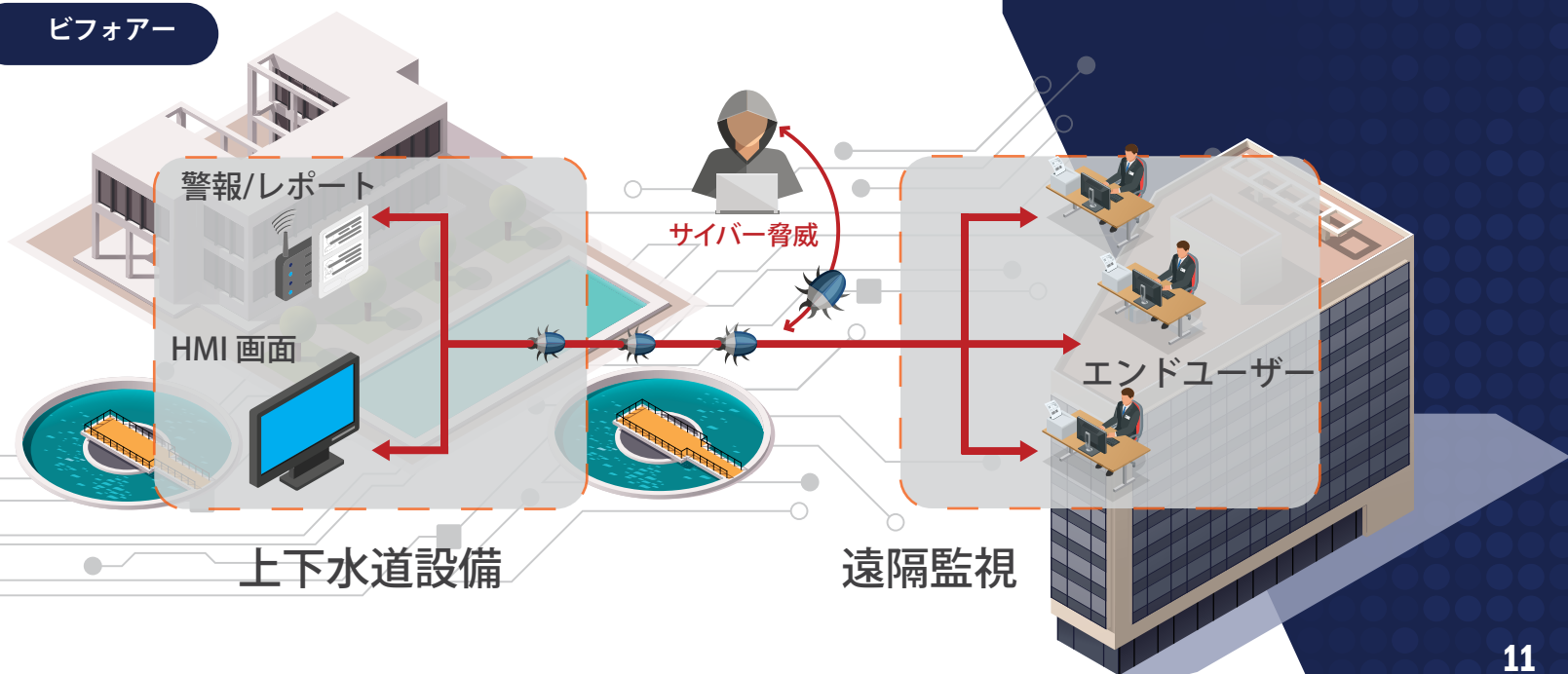
#### サイバーセキュリティに関する課題

報告書の米国国土安全保障省 (DHS) による指導、「産業制御システムを防御するための 7 つの戦略」に従い、同社は運用技術 (OT) ネットワークの攻撃対象領域を削減し、より防御可能な環境を作るためのサイバーセキュリティプランを策定した。

#### 要求

- セキュリティ方針を変更し、OT/工場のネットワーク境界の内部からのみ指令・制御操作を実行する
- 「切断された」(セグメント化された) サイバーセキュリティアーキテクチャを実現し、OT/工場ネットワークへの全リモートアクセスを排除すること
- 遠隔限定監視方針により業務の継続を維持すること
- 本社においてヒューマンマシンインターフェース (Human Machine Interface、HMI) 画面の複製を実現すること

#### ビフォー



#### 事例の概要

産業：

上下水道

課題：

会社は、業務の継続を維持しながら、DHS の指導に従いサイバーセキュリティ態勢を改善する必要性を認識している。

解決策：

情報のレポート・警報を転送し、リモート HMI 画面の複製を提供するために、DualDiode Technology を備えた Owl 社の OPDS-MP データダイオードが配備された

メリット：

決定論的一方向データフローが OT ネットワークを外部の影響または攻撃から守り、本社においてリアルタイムな遠隔 HMI 画面モニタリングを可能にした

## 解決策

OT ネットワークへのリモートアクセスを排除し、ネットワークの効果的なセグメント化を提供し、OT ネットワークからの決定論的一方向データ転送を実現するために、DualDiode Technology® を使用する Owl 社のデータダイオード (OPDS-MP) が採用された。これは、OV2S アプリケーションと共に、遠隔システム監視、運用レポートの転送、および遠隔地における HMI 画面の複製を提供した。

### ハードウェア

#### Owl 周辺機器防御ソリューション - 多目的 (OPDS-MP)

ネットワークのセグメント化および決定論的一方向データ転送専用設計された内蔵型 1U データダイオード。

### インターフェースアプリケーション

#### Owl バーチャルスクリーンビュー (OV2S)

工場または施設内の HMI 画面が遠隔地で複製できるようにするソフトウェアアプリケーション。



## 結果

- 産業制御システムの防御のため DHS 戦略に従ってセキュリティを改善した
- モニタリングおよび業務の継続のため、決定論的アウトバウンドデータフローを提供すると同時に OT ネットワークへの全インバウンド通信を排除した
- リアルタイム社外モニタリング用 HMI 画面の複製を実現した
- 本社における運用レポートおよび警報へのリモートアクセスを可能にした

アフター

上下水道設備

遠隔監視

警報/レポート

エンドユーザー

HMI 画面

HMI 画面

運用レポート

サイバー脅威

脅威の軽減

一方向データフロー

原子力施設がアメリカ  
合衆国原子力規制委員会の  
サイバーセキュリティ規制を遵守

### 企業の概要

発電容量が 1000 メガワットを超える、米国を拠点とする原子力発電所。

### Cybersecurity Challenge

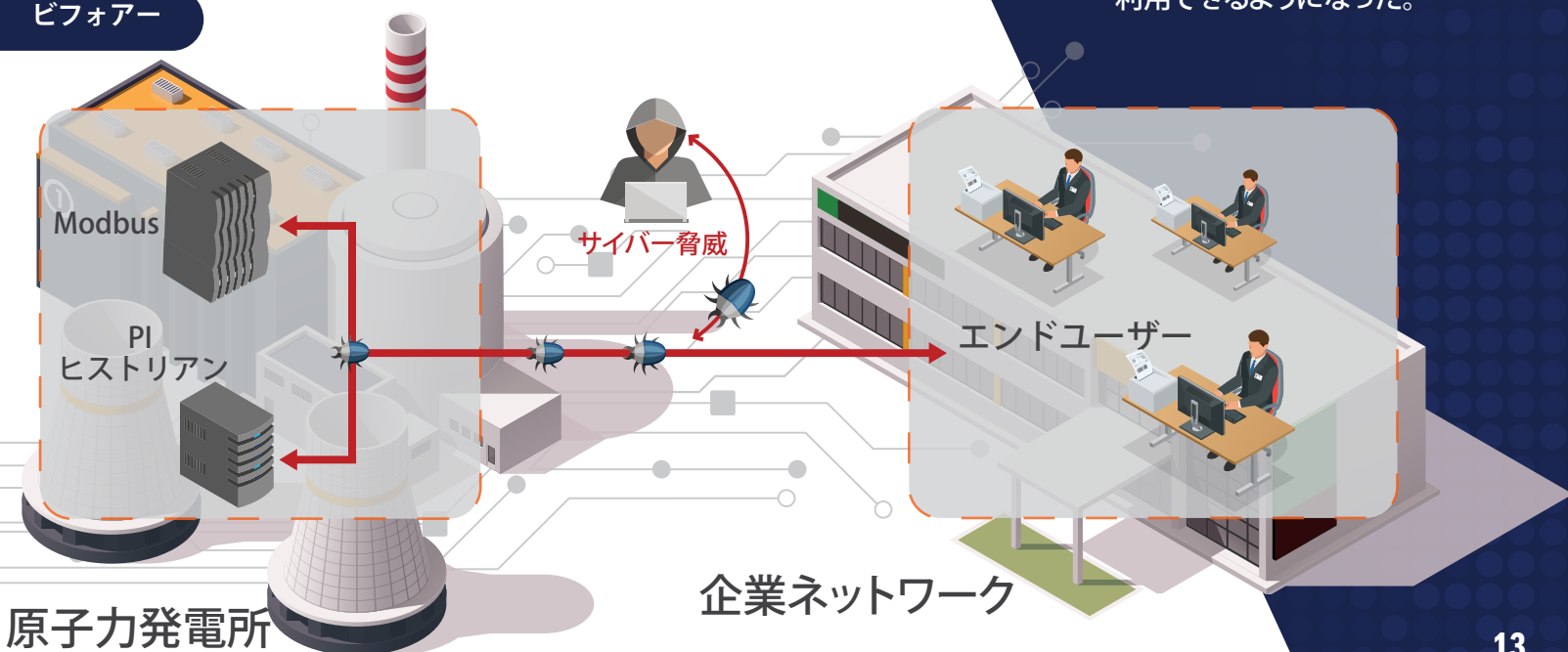
この工場は米国の原子力発電施設として、連邦規則集第 10 巻を含め NRC Regulatory Guide 5.71 に概説される通りに、アメリカ合衆国原子力規制委員会（NRC）のサイバーセキュリティ規制の対象である。この規制を遵守するために、同社は NRC の指導に基づきサイバーセキュリティの質を高めるための計画を策定した。

さらに同社は OSIsoft PI System ヒストリアンデータレプリケーション、そして会社の IT ネットワーク上でビジネスエンドユーザーがリモートで Modbus 重要サイバー資産のモニタリングが必要であった。

### 要求

- ネットワークセグメントを明確に定義し、外部ネットワークから重要な OT システムへの接続をすべて排除すること
- OT ネットワークから会社の IT ネットワークへの一方向フローを可能にすること
- IT エンドユーザーへの PI System レプリケーションにより業務の継続を維持すること
- 会社の IT 部門への Modbus レプリケーションにより重要サイバー資産の遠隔監視を可能にすること

### ビフォー



### 事例の概要

👤 産業：  
原子力発電

🚩 課題：  
会社はアメリカ合衆国連邦規則集および NRC 規則に従ってサイバーセキュリティおよびネットワークの防御の改善を求めている。

🛡️ 解決策：  
OPTS PI System ヒストリアンレプリケーション、および OMBI Modbus データレプリケーションと共に、OPDS-1000 データダイオードが配備された。

📊 メリット：  
外部からの影響または攻撃から OT ネットワークの安全が確保された。ビジネスエンドユーザーが PI System データおよび Modbus 重要資産モニタリングデータを利用できるようになった。



## 解決策

OT ネットワークへのリモートアクセスを防ぎ、ネットワークの効果的なセグメント化を提供し、決定論的一方向データ転送を可能にするために、DualDiode Technology® (OPDS-1000) を使用する Owl 社のデータダイオードが採用された。OT から IT ネットワークにヒストリアンデータを転送するために OSIssoft® PI System レプリケーション (OPTS) を追加し、重要なサイバー資産モニタリングデータを複製するために OMBI Modbus インテグレーションを使用した。



## ハードウェア

**Owl 社の周辺機器防御ソリューション - 1000 (OPDS-1000)**  
ネットワークのセグメント化および最大 1Gbps の決定論的一方向データ転送専用設計された内蔵型 1U データダイオード。

## インターフェースモジュール

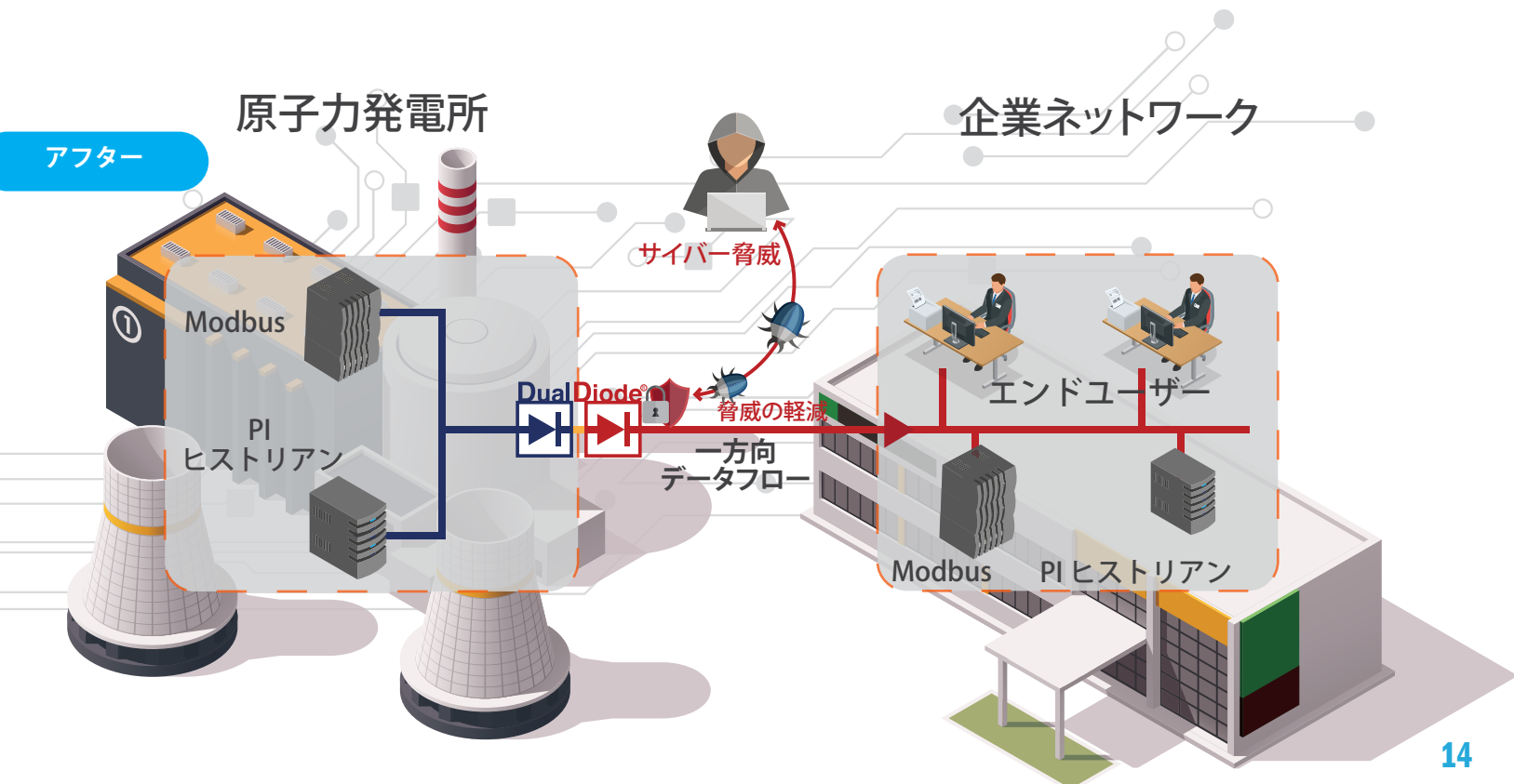
**Owl PI 転送サービス (Owl PI Transfer Service、OPTS)**  
OSIssoft® PI System ヒストリアンデータをネットワーク境界を越えて安全に複製・転送するために特別に開発された専用ソフトウェア。

## インターフェースモジュール

**Owl Modbusインターフェース (Owl Modbus Interface、OMBI)**  
Modbus プロトコルデータをネットワーク境界を越えて安全に複製・転送するために特別に開発された専用ソフトウェア。

## ✓ 結果

- サイバーセキュリティを改善し、NRC 規則および原子力施設の連邦指令が遵守された
- モニタリングおよび業務の継続のため、決定論的アウトバウンドデータフローを提供すると同時に、データダイオードが OT ネットワークへの全インバウンドアクセスを排除した
- 会社のネットワークでビジネスユーザーがアクセスできるように、PI System ヒストリアンおよび Modbus 重要サイバー資産のレプリケーションを可能にした



## 石炭発電所が NERC CIP バージョン 5 サイバーセキュリティ規制を遵守

### 企業の概要

発電容量が 2,500 メガワットを超える、米国を拠点とする石炭火力発電所。

### サイバーセキュリティに関する課題

この工場は米国の化石燃料発電施設として、北米電力信頼度協議会 (北米電力信頼度協議会、NERC) の重要インフラ保護 (Critical Infrastructure Protection、CIP) の Version 5、サイバーセキュリティ規制の対象。この規制を遵守するために、同社は外部アクセスから重要な運用技術 (OT) ネットワークを切り離さなければならなかった。しかし、ビジネス IT 部門による OSIsoft PI System ヒストリアンデータおよび OPC クライアント/サーバーデータへのアクセスは維持する必要があった

### 要求

- NERC CIP v5 に従って、ネットワークセグメントを明確に定義し、外部ネットワークから重要な OT システムへの接続をすべて排除すること
- OT ネットワークからビジネス IT ネットワークへの一方向通信を可能にすること
- PI System ヒストリアンレプリケーションによる業務の継続を維持すること
- ビジネス IT へのレプリケーションによる OPC データの遠隔監視を許可すること

### 事例の概要

産業：

石炭火力発電

課題：

ビジネスエンドユーザーによる OT データへのアクセスを中断することなく、NERC CIP v5 に従ってサイバーセキュリティコンプライアンスを遵守すること。

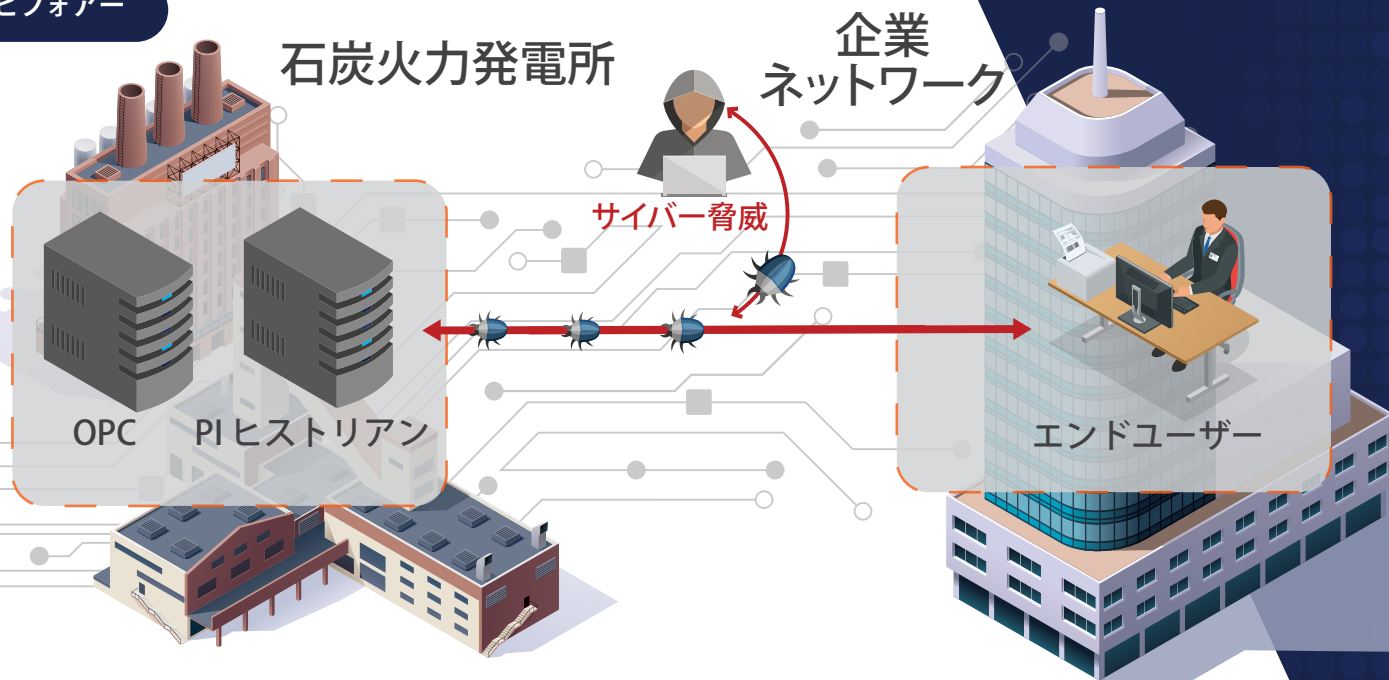
解決策：

OPTS PI System レプリケーションおよび Owl OPC データレプリケーションと共に、Owl OPDS-MP データダイオードが配備された。

メリット：

決定論的一方向データ転送が外部からの脅威に対して OT ネットワークの安全を確保し、会社のネットワークへの PI System データおよび OPC モニタリングデータの転送を可能にした。

### ビフォー



## 解決策

OT ネットワークへのリモートアクセスを防ぎ、OT ネットワークからの一方向データ転送を提供するために、DualDiode Technology® (OPDS-MP) を使用する Owl 社のデータダイオードが採用された。ビジネスエンドユーザー部門からの遠隔工場監視およびデータアクセスのために、PI System レプリケーション (OPTS) および OPC データレプリケーションを追加した。

### ハードウェア

**Owl 周辺機器防御ソリューション - 多目的 (OPDS-MP)**  
ネットワークのセグメント化および決定論的一方向データ転送専用設計された内蔵型 1U データダイオード。

### インターフェースモジュール

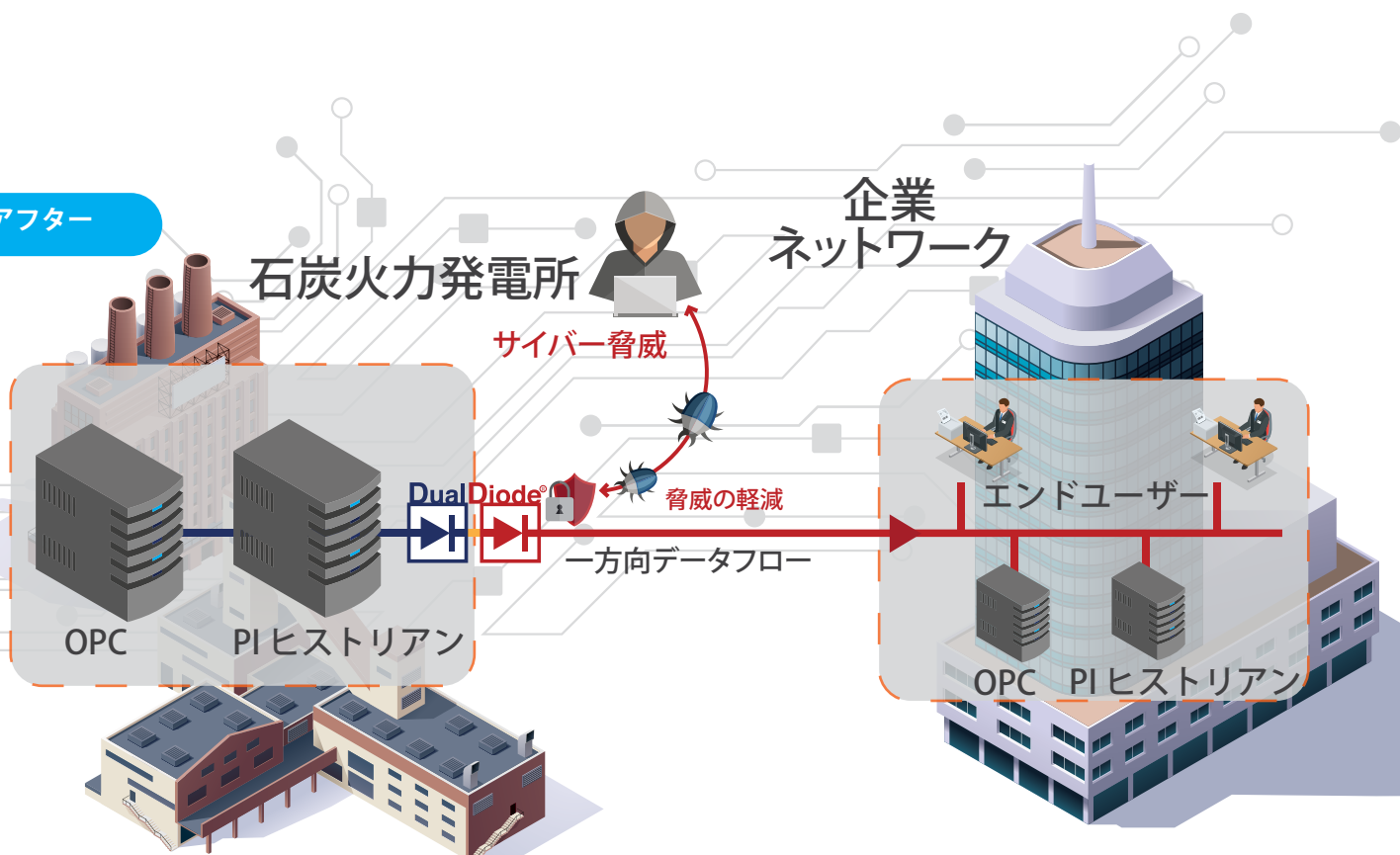
**Owl PI 転送サービス (Owl PI Transfer Service、OPTS)**  
OSIsoft® PI System ヒストリアンデータをネットワーク境界を越えて安全に複製・転送するために特別に開発された専用ソフトウェア。



## 結果

- 米国石炭火力発電施設サイバーセキュリティの NERC CIP v5 規制を遵守した
- NERC CIP v5 規制に基づきリスク軽減のためにデータダイオードが設置され、OT ネットワークへのインバウンド接続/脅威がすべて排除され、同時に決定論的一方向アウトバウンドデータフローを提供した
- IT ネットワークへの PI System ヒストリアンおよび OPC モニタリングデータレプリケーションを可能にして、ビジネス部門のスタッフが「仕事をやり遂げられるよう」にした

アフター





# 使用実例 ガス発電

周辺機器防御ソリューション

天然ガス発電所が NERC CIP  
サイバーセキュリティ規制を  
遵守し、ベンダー遠隔監視を実現

## 企業の概要

発電容量が 500 メガワットを超える、米国を拠点とする天然ガス発電所。

## サイバーセキュリティに関する課題

この発電施設は、北米電力信頼度協議会（北米電力信頼度協議会、NERC）の重要インフラ保護（Critical Infrastructure Protection、CIP）の Version 5、サイバーセキュリティ規制の対象。この規制を遵守するために、同社は取引先タービンベンダーを含む外部アクセスから重要な運用技術（OT）ネットワークを切り離さなければならなかった。しかし、同社のサービスレベルアグリーメント（SLA）によれば、ベンダーは工場からタービンモニタリングデータにアクセスする必要がある。

## 要求

- NERC CIP v5 に従って、ネットワークセグメントを明確に定義し、外部ネットワークから重要な OT システムへの接続をすべて排除すること
- OT ネットワークから外部のエンドユーザーへの一方向通信を可能にすること
- SLA を満たすために、タービンベンダーのグローバルモニタリングセンターに運営データを提供すること

## 事例の概要

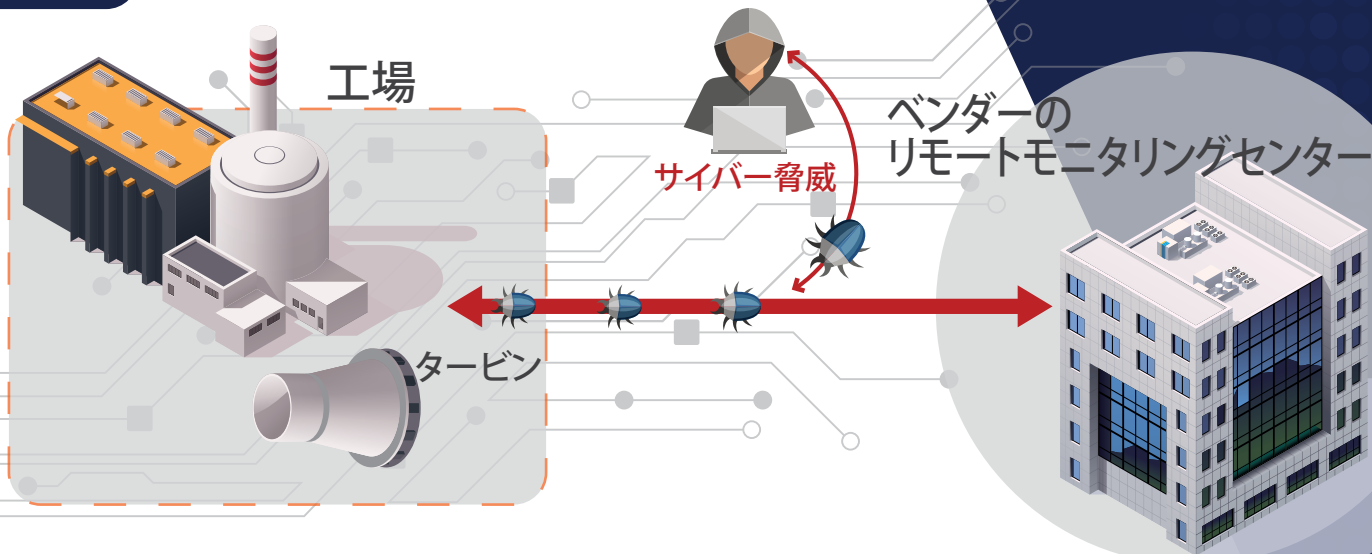
👤 産業：  
天然ガス発電

🚩 課題：  
NERC CIP v5 のサイバーセキュリティコンプライアンスを遵守し、SLA を満たすために OT モニタリングデータへのタービンベンダーによるアクセスを維持すること。

🛡️ 解決策：  
タービン運営情報をモニタリングセンターに転送するために、Owl 社の DualDiode Technology® 付き OPDS-100 データダイオードが配備された。

🏆 メリット：  
決定論的一方向データダイオードが外部からの脅威に対して工場の安全を確保し、ベンダーがリモートモニタリングセンターでタービンデータを受け取れるようになった。

## ビフォー



## 解決策

OT ネットワークへのリモートアクセスを排除し、決定論的一方向アウトバウンドデータフローを提供するために、DualDiode Technology® (OPDS-100) を使用する Owl 社のデータダイオードが採用された。これは、工場が NERC CIP v5 コンプライアンスを遵守するのに役立ち、ベンダーグローバルモニタリングセンターへのタービンデータの転送を可能にした。

### ハードウェア

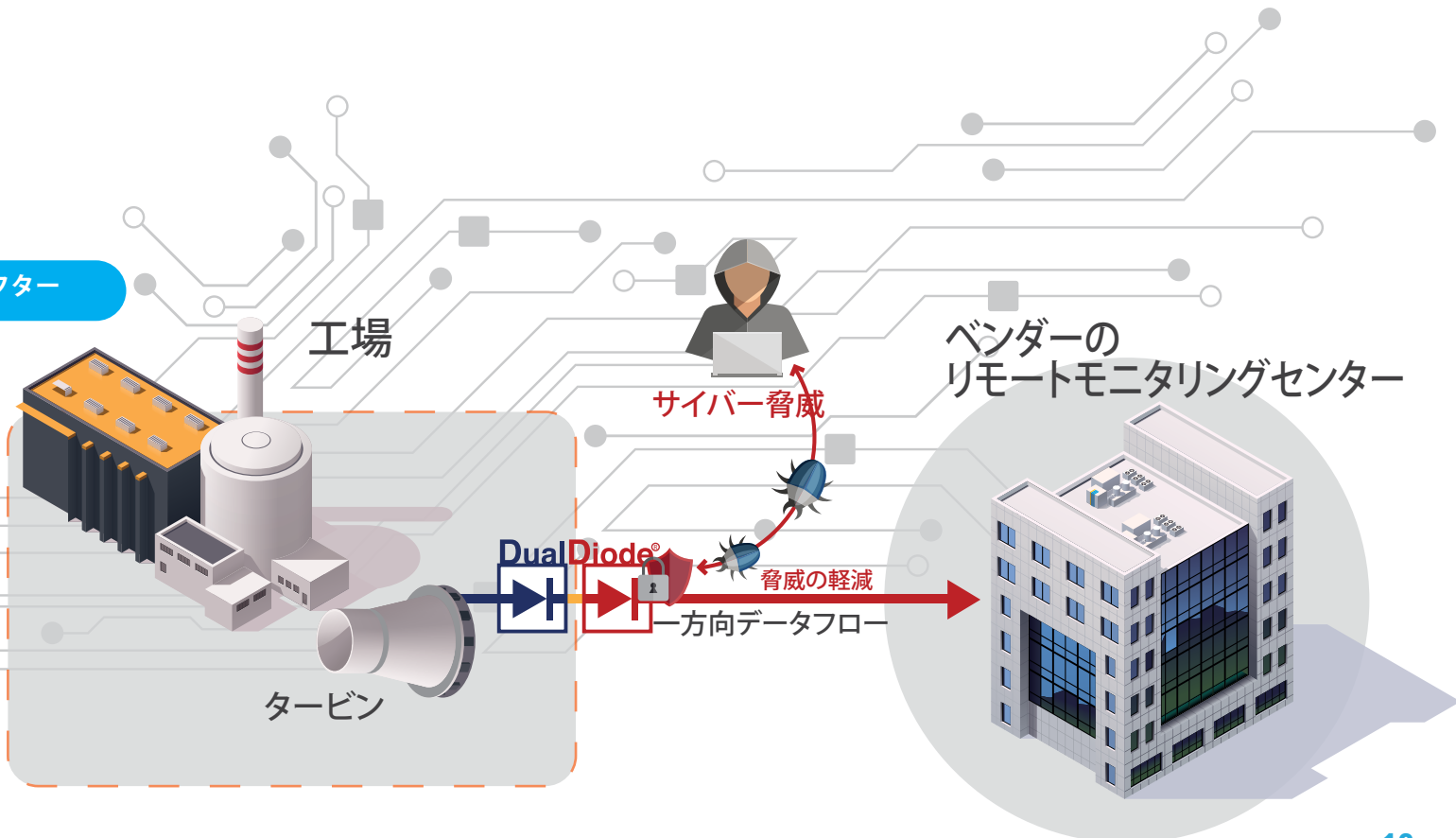
**Owl 社の周辺機器防御ソリューション - 100 (OPDS-100)**  
ネットワークのセグメント化および決定論的一方向データ転送専用設計された内蔵型 1U データダイオード。



## ✓ 結果

- 米国天然ガス発電施設サイバーセキュリティの NERC CIP v5 規制を遵守した
- NERC CIP v5 規制に基づきリスク軽減のためにデータダイオードが設置され、OT ネットワークへのインバウンド接続/脅威がすべて除去され、同時に決定論的アウトバウンドデータフローを提供した
- ベンダーのグローバルモニタリングセンターへのタービン運営データの一方向転送によってSLA を満たした

アフター



電力公社が 10 箇所の発電所で NRC、NERC CIP サイバーセキュリティ規制を遵守

### 企業の概要

米国拠点とする連邦政府所有の地方電力公社。原子力発電、化石燃料発電、水力発電を合わせて 150 地域の地方自治体に電力を供給している。

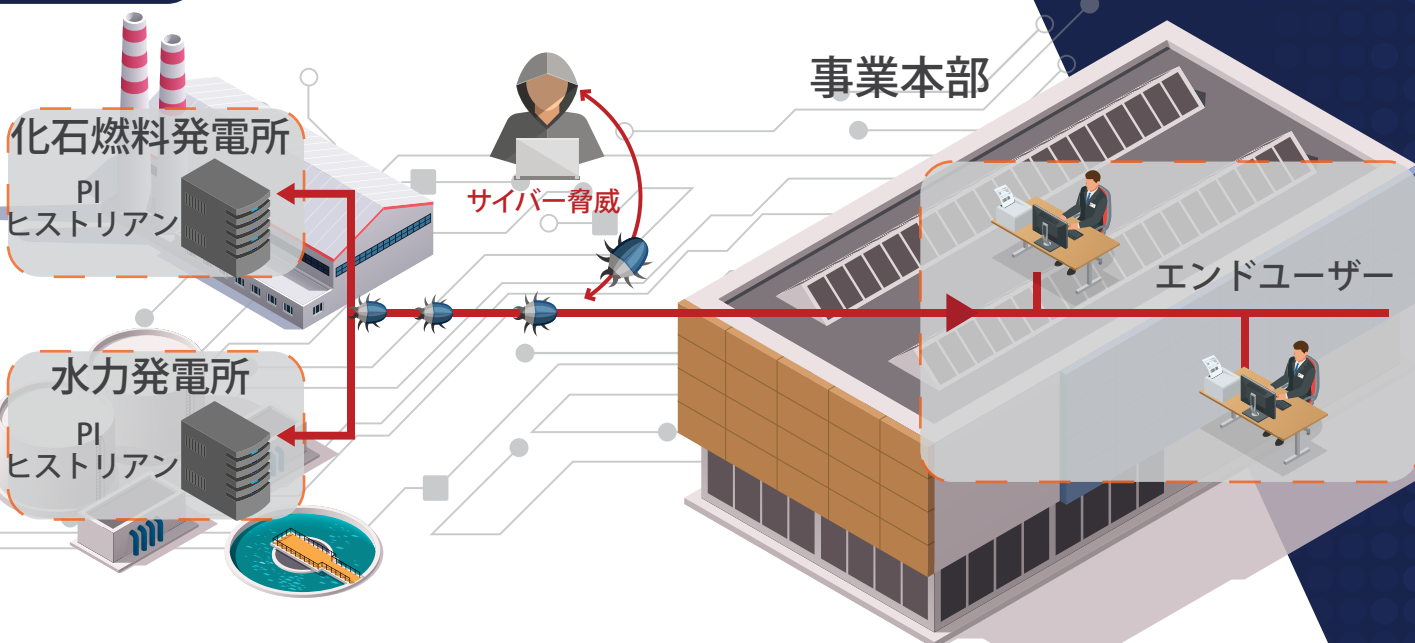
### サイバーセキュリティに関する課題

米国会計検査院 (US General Accounting Office、GAO) の監査により、サイバーセキュリティに多くの脆弱性が明らかにされた。この電力公社は発電手段として原子力、化石燃料、および水力による発電所を抱えているため、北米電力信頼度協議会 (北米電力信頼度協議会、NERC) の重要インフラ保護 (Critical Infrastructure Protection、CIP) とアメリカ合衆国原子力規制委員会 (NRC) のサイバーセキュリティの両規制の対象であった。同公社では、特定されたサイバーセキュリティの脆弱性を改良して、業務を継続しながら規制遵守を満たさなければならなかった。

### 要求

- NERC CIP v5 および NRC Regulatory Guide 5.71 に従って、ネットワークセグメントを明確に定義し、外部ネットワークから重要な OT システムへの接続をすべて排除すること
- OT ネットワークからビジネス IT ネットワークへの一方向データフローを可能にすること
- ビジネスグループがアクセスできるように、発電設備全体に渡って、ローカル PI System ヒストリアンを本社の集中化 PI System ヒストリアンへ複製すること

### ビフォー



### 事例の概要

#### 産業：

米国内でトップ10にランキングする民間電気事業者

#### 課題：

サイバーセキュリティの脆弱性を改良して、NERC CIP v5 および NRC のセキュリティ規制を満たすこと

#### 解決策：

OPTS PI System レプリケーションアプリケーションと共に Owl 社の EPDS データダイオードが配備された

#### メリット：

一方向データフローが外部の脅威から OT ネットワークの安全を確保し、NERC CIP v5 および NRC の規制に準拠することを達成した。本社にある複製された PI System ヒストリアンを通して業務を継続できた

## 解決策

NERC CIP v5 および NRC Regulatory Guide 5.71 規制のリスクに基づく特定条件を満たすために、DualDiode Technology® を使用した Owl 社のデータダイオード (EPDS) が採用された。データダイオードより OT ネットワークへの外部からのアクセスが排除され、本社への決定論的一方向データフローが可能になった。発電設備全体のヒストリアンモニタリングデータおよび運営管理レポートを本社に転送するために、OPTS PI System データレプリケーションソフトウェアが配備された。

## ハードウェア

### 企業周辺機器防御ソリューション (EPDS)

ネットワークのセグメント化と決定論的一方向データ転送用に、独立型の送信専用および受信専用の商用サーバーにマウントされる一対のデータダイオード通信カード。

## インターフェースモジュール

### Owl PI 転送サービス (Owl PI Transfer Service、OPTS)

OSIsoft® PI System ヒストリアンデータをネットワーク境界を越えて安全に複製・転送するために特別に開発された専用ソフトウェア。

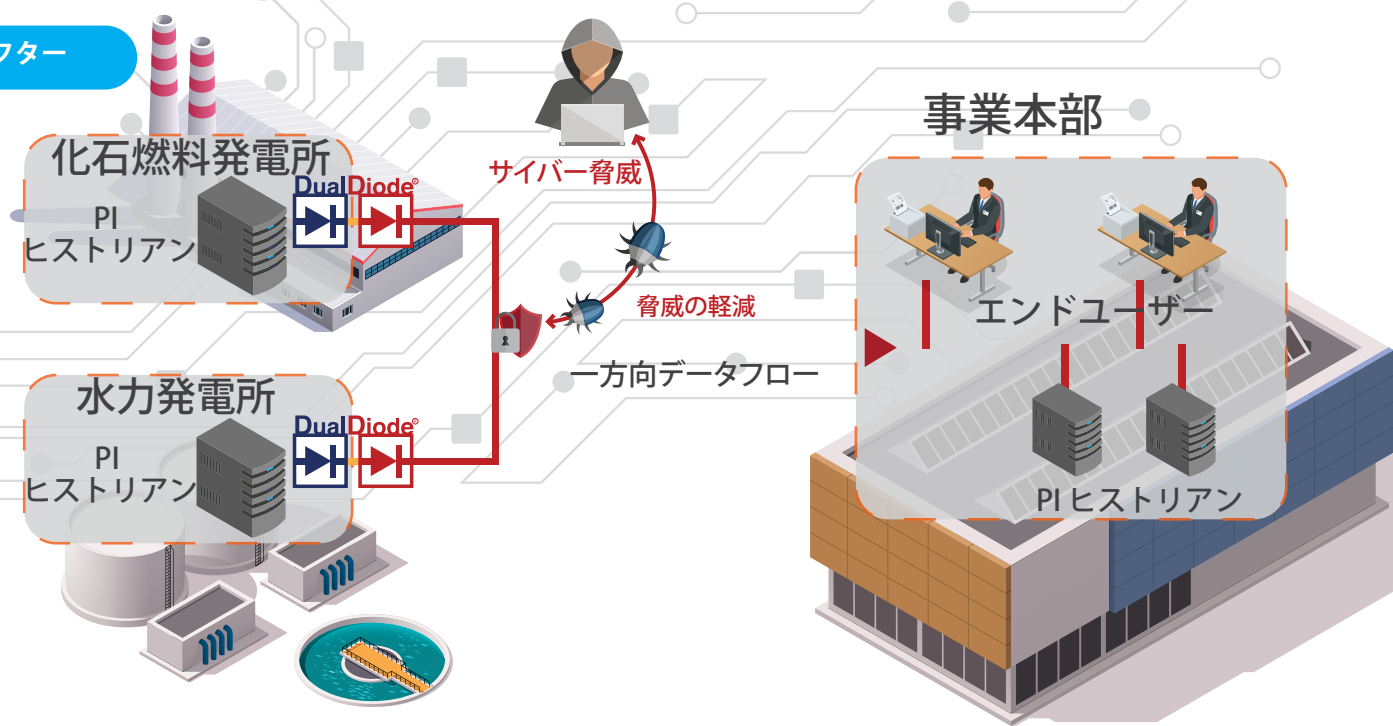


\*Owl 社では、一対の Dell PowerEdge R620 サーバーまたは同等製品を使用。

## 結果

- 米国発電設備の GAO ガイダンス、NERC CIP v5 および NRC Regulatory Guide に従い、多層防御セキュリティ要件を満たした
- データダイオードが設置され、OT ネットワークへのインバウンド接続/脅威がすべて排除され、同時に決定論的アウトバウンドデータフローを提供した
- 発電所全体にわたる PI System ヒストリアンデータを OT ネットワークから本社の IT ネットワークに複製したことにより、業務を継続できた

アフター



#### 企業の概要

米国全土にある様々な送配電所 (T&D) を多数保有する大規模電力システム (Bulk electric system、BES) 運営業者。

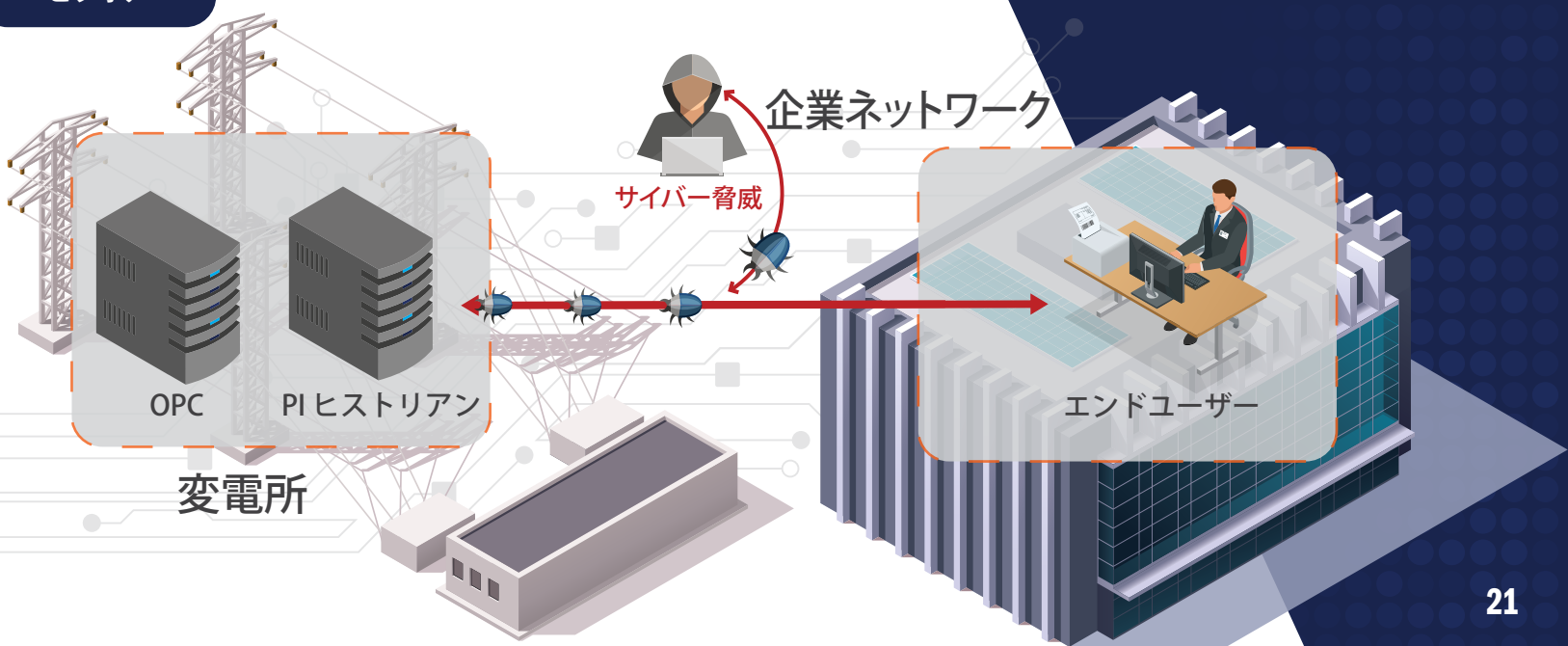
#### サイバーセキュリティに関する課題

T&D 変電所は、北米電力信頼度協議会 (北米電力信頼度協議会、NERC) の重要インフラ保護 (Critical Infrastructure Protection、CIP) の Version 5、サイバーセキュリティ規制の対象となり、BES へのネットワークの脅威を最低限に抑えることが求められる。この規制を遵守するために、同社は外部アクセスから変電所の重要な運用技術 (OT) ネットワークを切り離さなければならなかった。しかし、ビジネスエンドユーザーは、OSIsoft PI System ヒストリアンデータおよび変電所の OT ネットワーク内部で作成される OPC データへのアクセスを維持する必要があった。

#### 要求

- NERC CIP v5 に従って、ネットワークセグメントを明確に定義し、外部ネットワークから重要な OT システムへの接続をすべて排除すること
- OT ネットワークからビジネス IT ネットワークへの一方向データ転送を可能にすること
- 業務の継続のために PI System ヒストリアンデータを IT ネットワークへ複製・転送すること
- OPC クライアント/サーバー遠隔データ監視を許可すること

#### ビフォー



#### 事例の概要

産業：

電力 T&D 変電所

課題：

ビジネスエンドユーザーによる OT データへのアクセスを中断することなく、NERC CIP v5 に従ってサイバーセキュリティコンプライアンスを遵守すること

解決策：

OPTS PI System  
データレプリケーションおよび Owl  
OPC データレプリケーション  
ソフトウェアと共に、Owl OPDS-MP  
データダイオードが配備された

メリット：

決定論的一方向データ転送によって  
NERC CIP コンプライアンスを遵守し、  
ビジネスエンドユーザーによる  
PI System および OPC  
モニタリングデータへの  
リモートアクセスを可能にした

## 解決策

OT ネットワークへの外部アクセスを排除し、ネットワークの効果的なセグメント化を提供し、OT ネットワークからの決定論的一方向データ転送を実現するために、DualDiode Technology® を使用する Owl 社のデータダイオード (OPDS-MP) が採用された。本社のエンドユーザーによる遠隔変電所監視およびデータアクセスのために、OSIsoft® PI System レプリケーション (OPTS) および OPC クライアント/サーバーレプリケーション用 Owl アプリケーションも配備された。

### ハードウェア

#### Owl 周辺機器防御ソリューション - 多目的 (OPDS-MP)

ネットワークのセグメント化および決定論的一方向データ転送専用設計された内蔵型 1U データダイオード。

### インターフェースモジュール

#### Owl PI 転送サービス (Owl PI Transfer Service、OPTS)

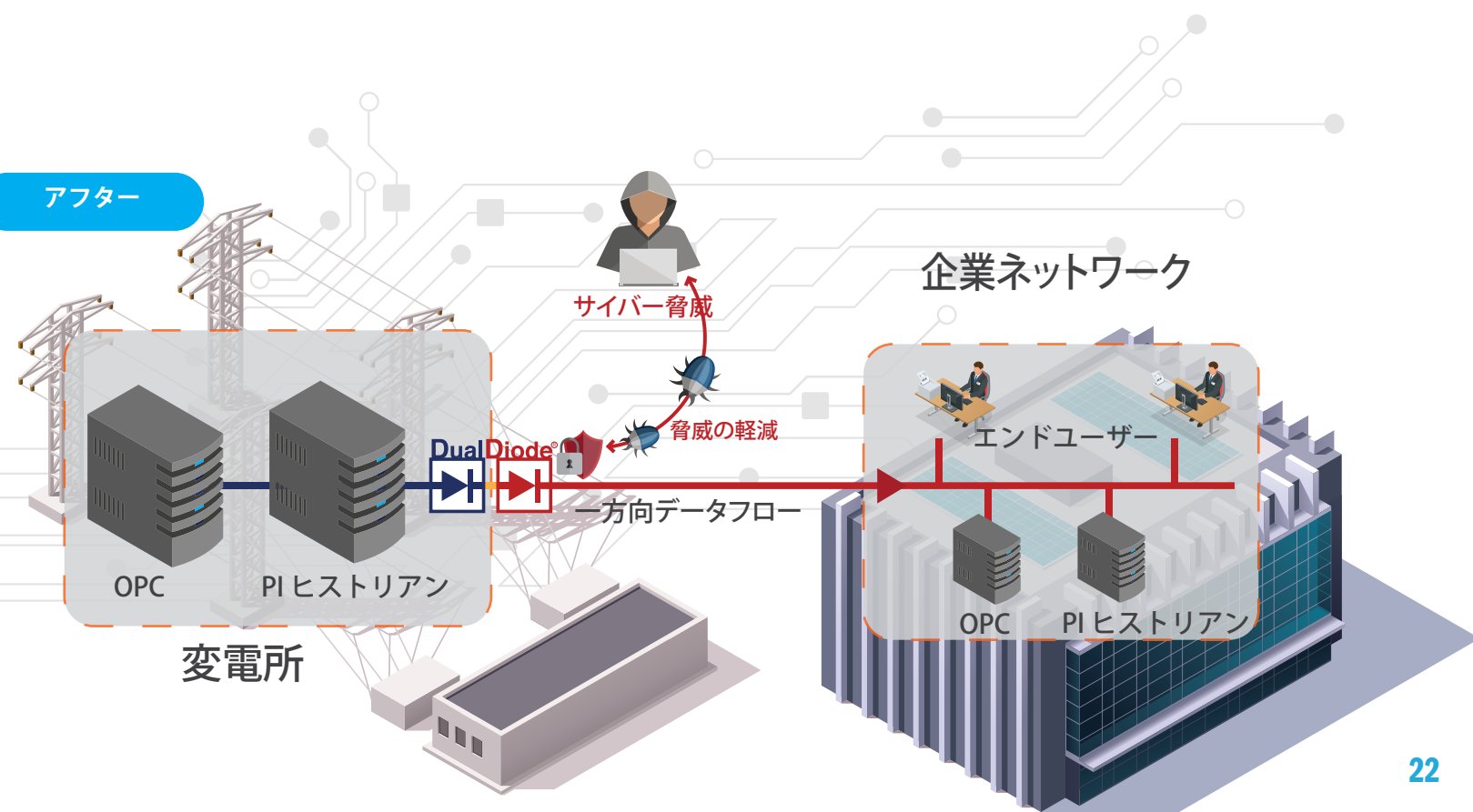
OSIsoft® PI System ヒストリアンデータをネットワーク境界を越えて安全に複製・転送するために特別に開発された専用ソフトウェア。



## 結果

- 米国電力 T&D サイバーセキュリティの NERC CIP v5 規制を遵守した
- NERC CIP v5 規制に基づきリスク軽減のためにデータダイオードが設置され、OT ネットワークへのインバウンド接続/脅威がすべて除去され、同時に決定論的アウトバウンドデータフローを提供した
- IT ネットワークへの PI System ヒストリアンおよび OPC モニタリングデータレプリケーションを可能にして、業務の継続および運用上の洞察を維持した

### アフター



全国銀行がセントラルリポジトリ  
においてデータベースにあるATM  
収集データの安全を確保

### 企業の概要

様々な地域に ATM を設置している国法銀行。

### サイバーセキュリティに関する課題

様々な多数の ATM からの取引およびセキュリティのデータが、使用および分析のために銀行のセントラルリポジトリデータベースに送られる。しかし、セキュリティの調査が実施され、銀行がソフトウェアのファイアウォールでは銀行のセントラルリポジトリデータベースを外部からのサイバー脅威に対して十分に保護できないと判断した。銀行は、セントラルデータベースのためにネットワークサイバーセキュリティの改善を求めているほか、引き続き ATM からデータを収集してセントラルリポジトリに転送する能力も必要であった。

### 要求

- ホワイトリストに記載された信頼できるファイルのみがデータリポジトリへ転送することを許可する安全なネットワーク周辺機器
- 一切のデータが外部からアクセスされたり抽出されたりしないように、リポジトリへの外部接続を排除する

### 事例の概要

👤 産業：  
銀行業

🚀 課題：  
セントラルデータリポジトリを隔離してその安全を確保すると同時に、現場の ATM からの信頼できるファイルの収集を保護すること

🛡️ 解決策：  
既存のファイアウォールソリューションと共に、DualDiode Technology® を備えた Owl 社の OPDS-MP データダイオードが配備された

📋 メリット：  
一方向データフローが、セントラルリポジトリが外部からのネットワークの脅威に対し安全であることを保証する。データダイオードが、ATM からの信頼できるファイルを安全なリポジトリに入ることを許可する

### ビフォー



## 🛡️ 解決策

リモートのデータリポジトリアクセスを排除し、ATM セキュリティおよび取引データのデータベースへの決定論的一方向データ転送を可能にするために、DualDiode Technology® を使用する Owl 社のデータダイオード (OPDS-MP) が採用された。このデータダイオードは既存のファイアウォールと連携して、ホワイトリストに記載された信頼できるファイルのみをデータリポジトリに許可する。

### ハードウェア

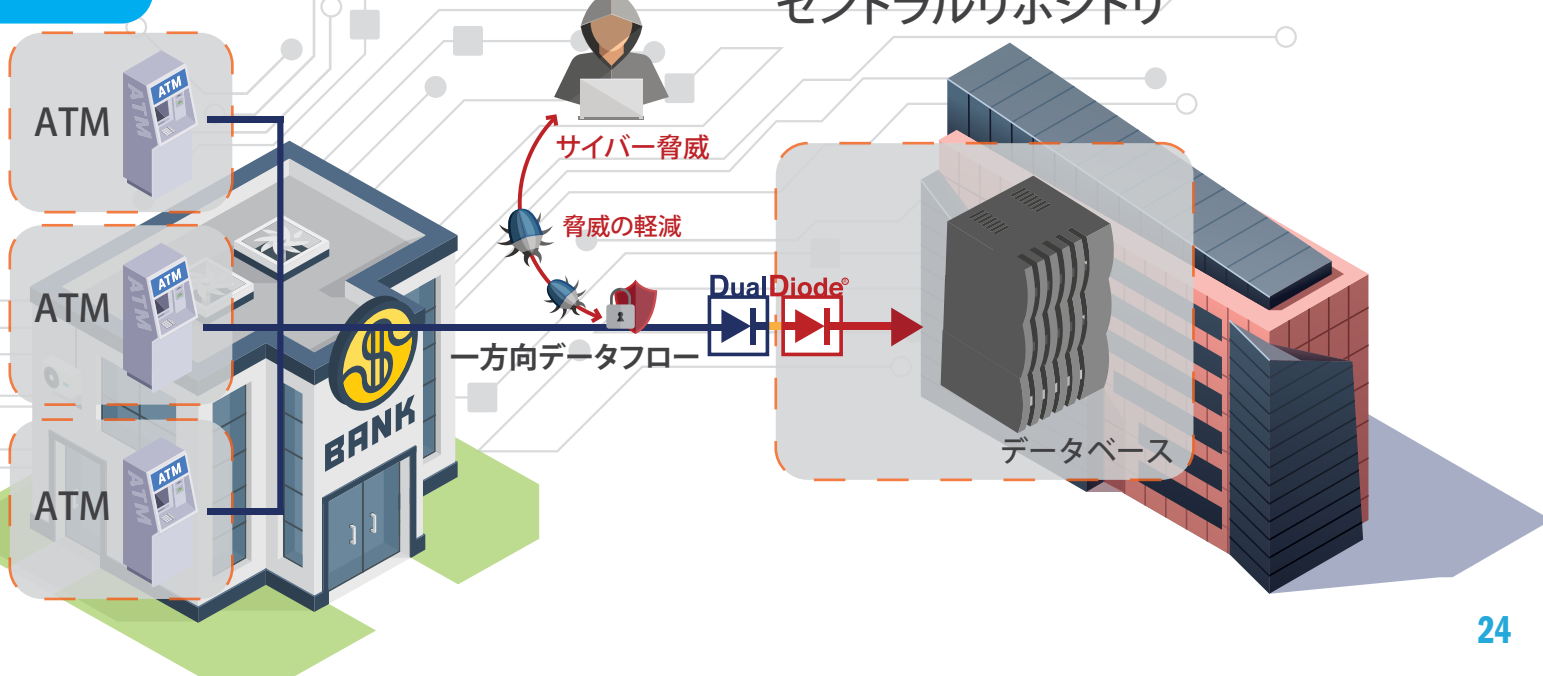
**Owl 周辺機器防御ソリューション - 多目的 (OPDS-MP)**  
ネットワークのセグメント化および決定論的一方向データ転送専用に設計された内蔵型 1U データダイオード。



## ✓ 結果

- ATM ネットワークとセントラルデータリポジトリとの間にハードウェアによる安全な境界が作成された
- データダイオードがデータリポジトリからのアウトバウンド接続をすべて排除すると同時に、信頼できる ATM データの決定論的インバウンドフローを提供した
- どのような外部のネットワーク接続によっても、データリポジトリからデータを盗み出すことはできない
- データリポジトリへの高度に制御された一方向 ATM データフローにより、業務を継続できた

アフター





# 使用実例 銀行業

遠隔ネットワーク監視

米国地方銀行が遠隔  
ネットワーク監視を実現

## 企業の概要

支店が 150 箇所以上あり、10 万人以上の顧客を抱え、取引需要が高い環境にある米国の地方銀行。

## サイバーセキュリティに関する課題

サイバー脅威を最小限に抑えるために、すべての外部ネットワークから取引センターを隔離した。しかしシステム上の取引需要は高いため、最高のパフォーマンスを達成し、ダウンタイムを限りなくゼロにするために、銀行の運営状況を常時監視する必要があった。銀行は、取引センターを外部のサイバーネットワークの脅威に再びさらすことなく、オンコール IT スタッフが年中無休で銀行の運用状況を遠隔監視できる方法を求めている。

## 要求

- 外部ネットワークからの接続またはアクセスが一切なく、取引ネットワークの「切断された」アーキテクチャを維持すること
- 取引センターシステムの遠隔監視担当のオンコールスタッフへ警報およびイベント通知が転送されるよう許可すること

## 事例の概要

👤 産業：  
銀行業

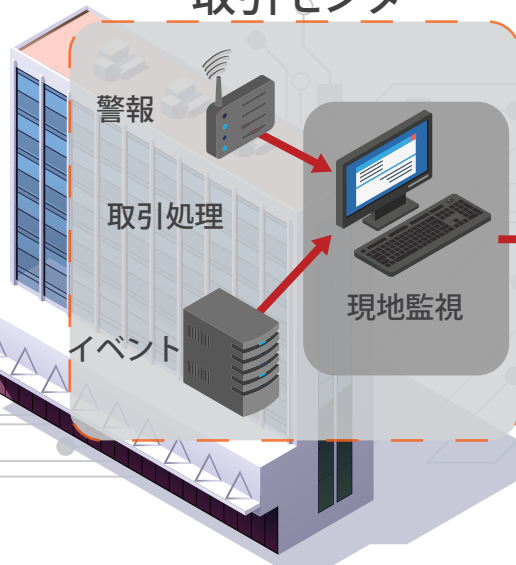
🚧 課題：  
銀行運営のセキュリティおよび隔離を維持しながら遠隔監視を可能にすること

🛡️ 解決策：  
電子メール通知、警報、およびファイルの転送が可能な、DualDiode Technology® 装備の OPDS-100 データダイオード

📋 メリット：  
一方向データフローが、銀行取引ネットワークが外部のサイバー脅威に対し安全であることを保証する。システムのパフォーマンス、警報、およびイベントを IT スタッフが遠隔監視できるようにした

## ビフォー

### 取引センター



## 解決策

銀行取引ネットワークを切断されたままで保護し、IT スタッフが遠隔監視できるように性能、警報、およびイベントのファイルを決定論的一方向データ転送できるように、DualDiode Technology® (OPDS-1000) を使用する Owl 社のデータダイオードが採用された。

### ハードウェア

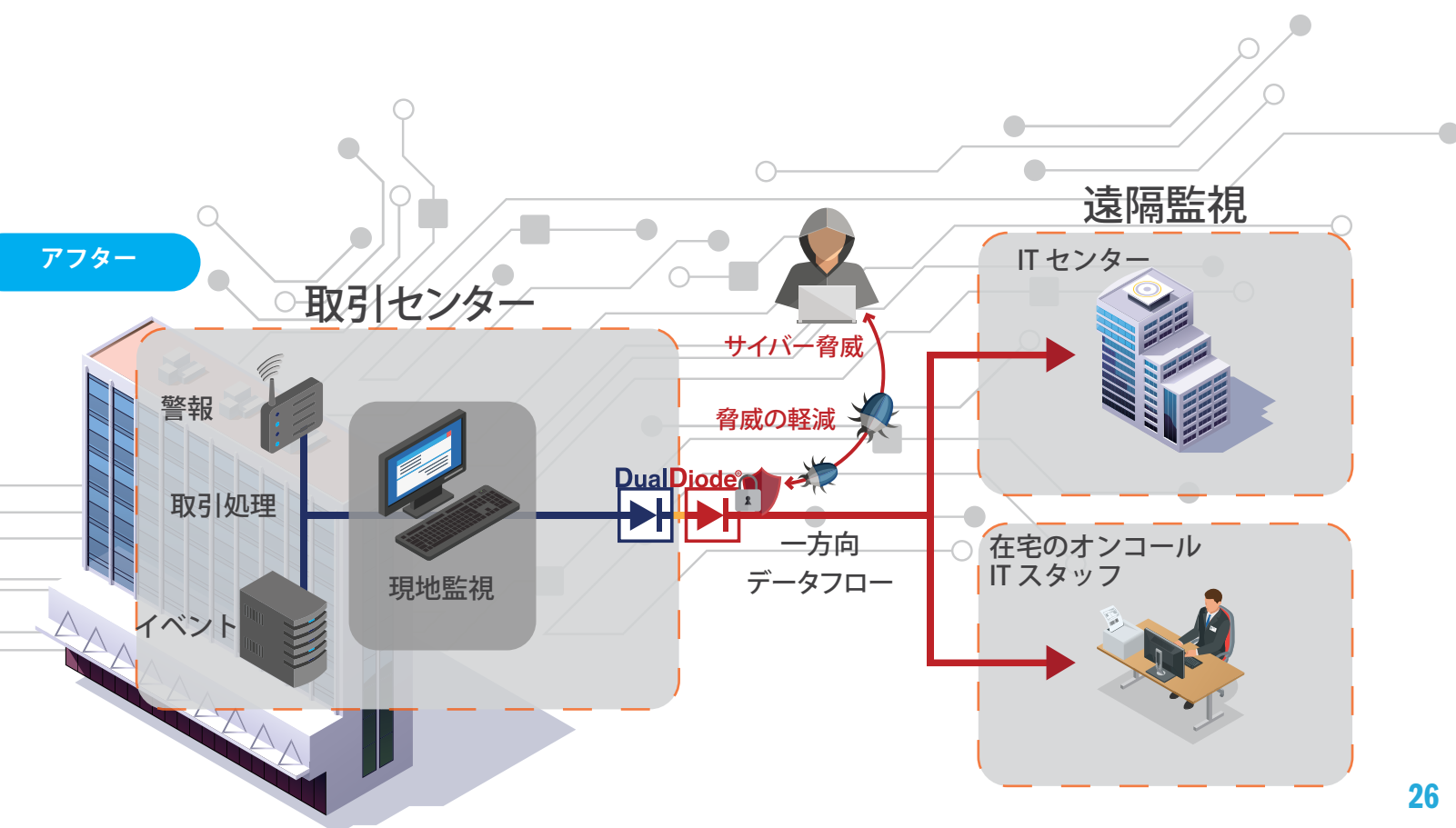
#### Owl 社の周辺機器防御ソリューション - 100 (OPDS-100)

ネットワークのセグメント化および決定論的一方向データ転送専用に設計された内蔵型 1U データダイオード。



## 結果

- 電子メール通知を含めた性能、警報、およびイベントのファイルの決定論的アウトバウンドフローを提供した
- IT スタッフが取引センターからの性能、警報、およびイベントのデータを遠隔監視できるようにした
- 切断されたアーキテクチャを保護するために、銀行取引ネットワークの周囲にハードウェアによる安全な境界を設定した
- 銀行取引ネットワークはどの外部ネットワーク接続によってもアクセスできなくなった





## サイバー資産の分析

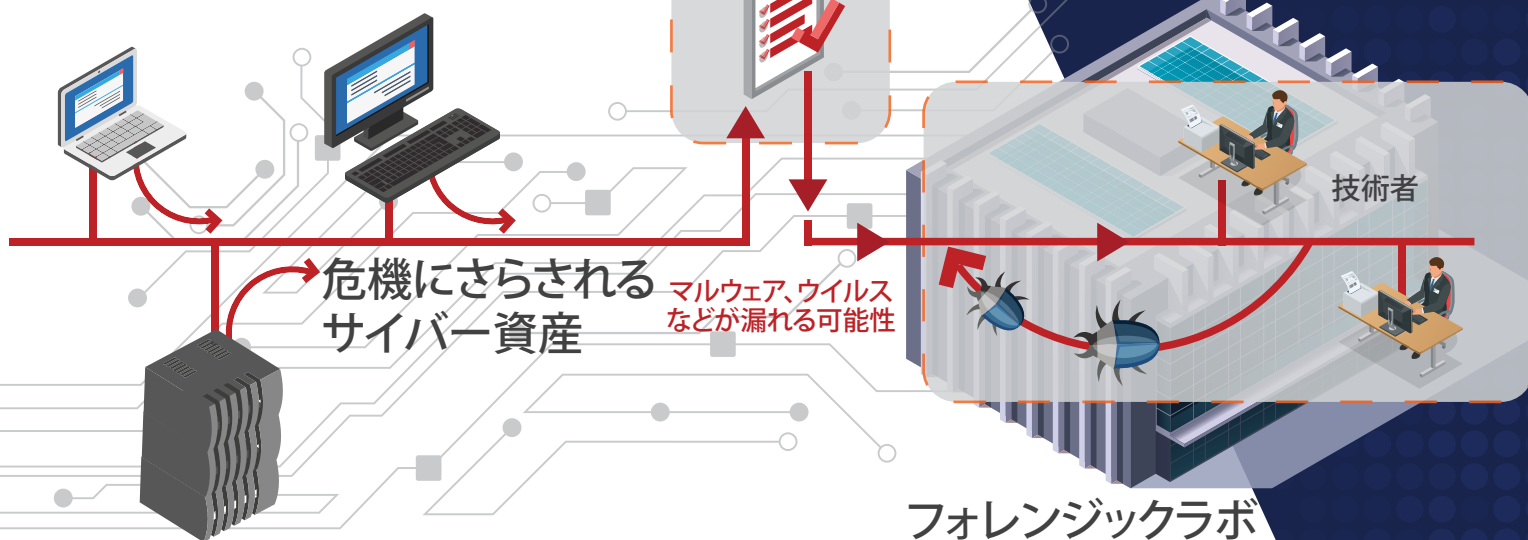
中小企業向け全国銀行が  
フォレンジックデータファイルの  
キャプチャおよび収集を実行

資産および資本額が5億ドルを超える中小企業向け全国銀行。

様々なネットワークやウェブサイト、ユーザーが利用する銀行のサイバー資産（ノートパソコンやサーバー、デスクトップパソコンなど）に関連するサイバー資産のフォレンジックメタデータをキャプチャして分析することは、サイバー脅威を調査し、最終的に修正を図る上で不可欠である。銀行は、危機にさらされるサイバー資産およびそれらの関連メタデータをキャプチャし、パッケージ化し、コピーし、その上でそれらを分析のためにフォレンジックラボへ安全に転送するための方法が必要であった。そのほかにも、銀行は信頼できるファイルのみがラボネットワークに入ること、そして感染が疑われるデータがラボの外に出ないようにすることも求めている。

- 危機にさらされる資産とそのメタデータをスキャンし、フォレンジックデータファイルにパッケージ化するソフトウェアユーティリティとの互換性
- 銀行ネットワークからフォレンジックラボ環境にフォレンジックデータファイルを安全な方法で転送できるようにすること
- フォレンジックラボネットワークの「切断された」安全なアーキテクチャを保護し、外部ネットワークからアクセスされないよう維持すること

## フォレンジックコピー



## 事例の概要

産業：  
銀行業

**⚡ 課題：**

フォレンジックデータファイルを銀行の安全なフォレンジックラボネットワークに転送し、同時にラボ環境の隔離を保護できるようにすること。

## 🛡️ 解決策：

フォレンジックエビデンスを  
キャプチャして格納するために、  
DualDiode Technology® 装備の  
OPDS-1000 データダイオードが  
配備された。

### ≡ メリット :

一方データフローが  
フォレンジックラボへのファイル  
転送を可能にし、同時にラボ環境  
が隔離された状態で維持され、  
外部のサイバー脅威からの安全  
が確保される。

## 解決策

フォレンジックデータファイルを安全が確保されたラボ環境へ転送するために、DualDiode Technology® (OPDS-1000) を使用する Owl 社のデータダイオードが採用された。

このフォレンジックデータファイルは第三者ソフトウェアツールによりパッケージ化されている。ダイオードはフォレンジックラボネットワークを切断されたままの状態を維持し、外部ネットワークからのアクセスを防ぐ。

### ハードウェア

#### Owl 社の周辺機器防御ソリューション - 1000 (OPDS-1000)

ネットワークのセグメント化および最大 1Gbps の決定論的一方方向データ転送専用設計された内蔵型 1U データダイオード。



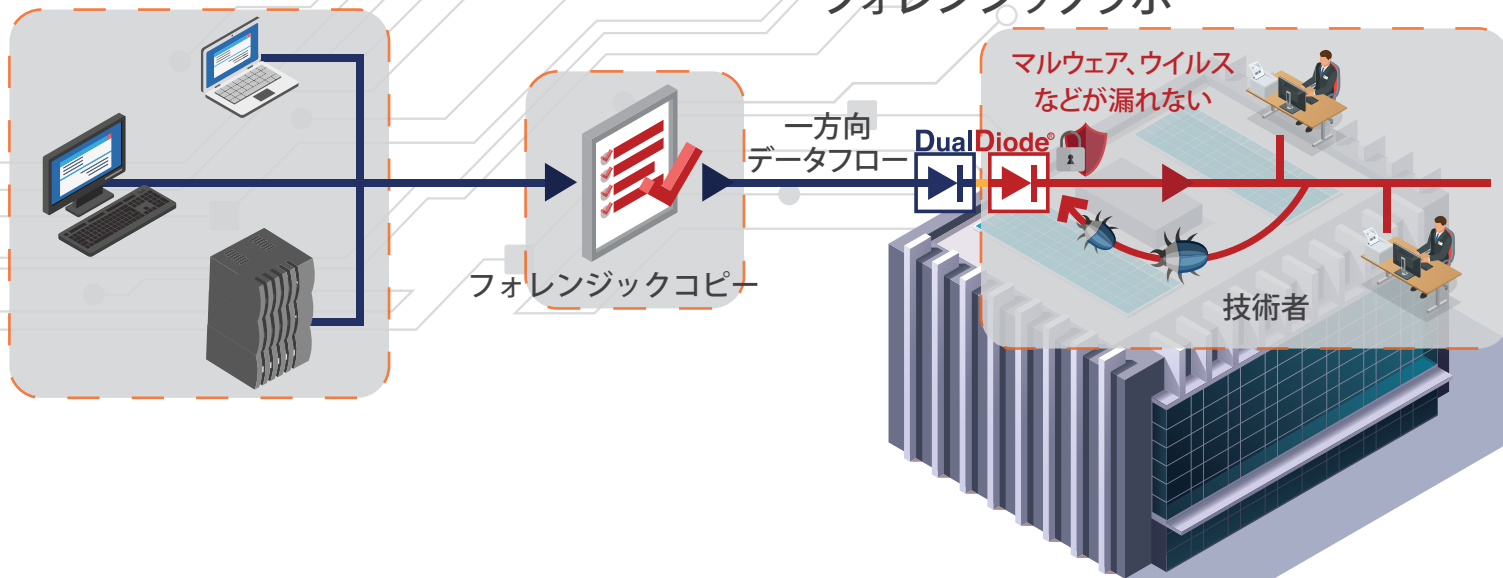
## 結果

- 銀行ネットワークから安全が確保されたフォレンジックラボ環境へのパッケージ化されたフォレンジックデータファイルの決定論的一方方向転送を提供した
- ハードウェアで強化された安全な境界でラボネットワークの切断されたアーキテクチャを保護した
- 銀行のフォレンジックラボネットワークはどのような外部のネットワーク接続によってもアクセスできず、証拠となる可能性があるデータに細工を加えることはできない
- 潜在的に危険なサイバー感染がフォレンジックラボの外に漏れることはない

アフター

危機にさらされる  
サイバー資産

フォレンジックラボ



米国地方銀行が取引および顧客記録の社外バックアップの安全を確保

### 企業の概要

支店が 40 箇所を超える米国の中規模地方銀行。

### サイバーセキュリティに関する課題

銀行は、業務の継続性を維持するために、システムの適時で安全なバックアップを求めている。しかし、銀行のネットワーク接続を防ぐために使用したソフトウェアファイアウォールのセキュリティに深刻な懸念があった。クラウド上と第三者ネットワーク上に置かれていた遠隔バックアップサイトが原因で、ネットワークが非常に危険度の高いリスクにさらされていた。銀行はネットワーク侵入の危険を生じさせることなく、バックアップファイルを社外に送信する安全な方法を必要としていました。

### 要求

- 銀行が外部からのサイバー脅威に侵害されないように、銀行の運営ネットワークへの外部接続を排除すること
- 銀行の運営ネットワークから遠隔ストレージサイトへ通常の定期バックアップが送信されるよう許可すること

### 事例の概要

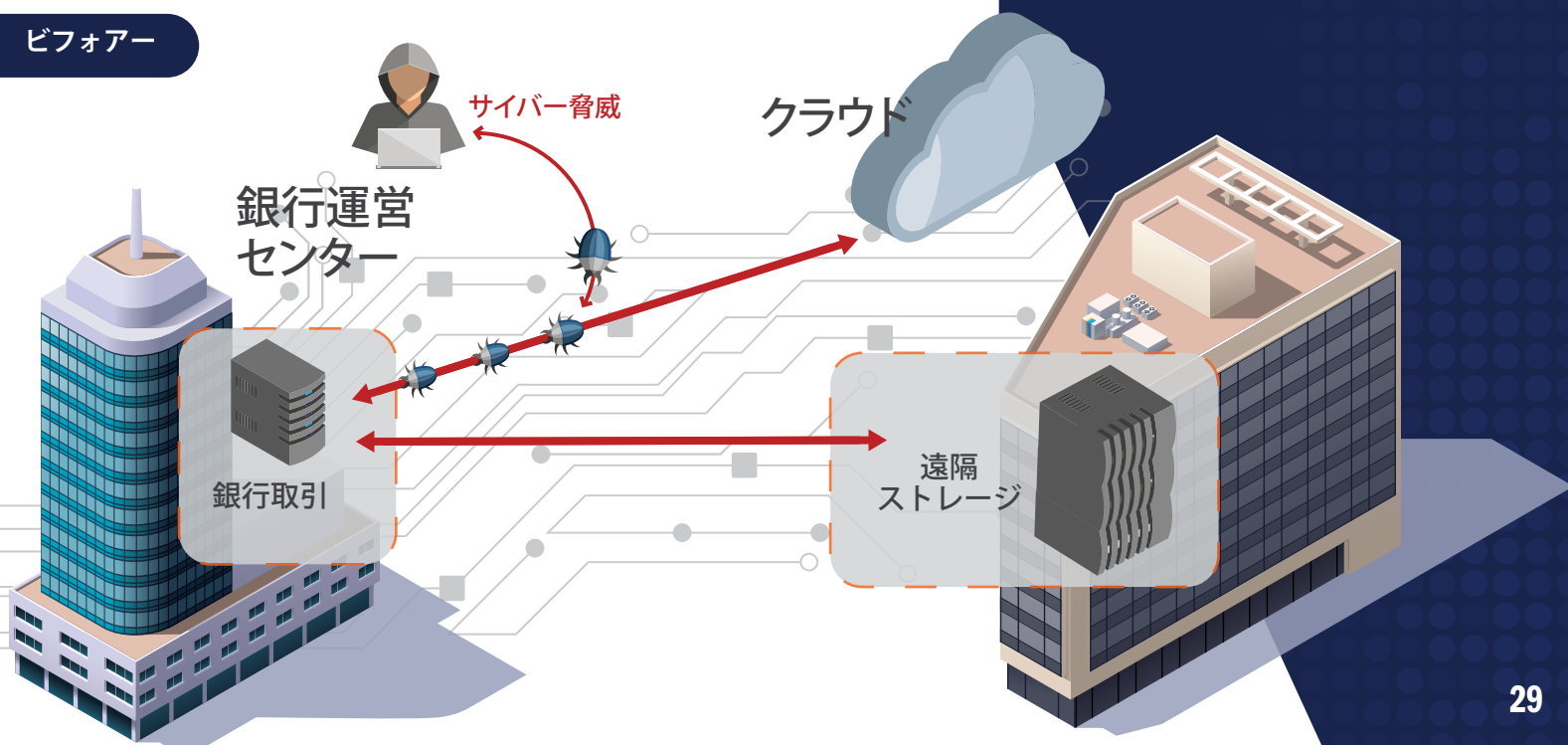
産業：  
銀行業

課題：  
銀行の運営ネットワークのセキュリティを保証し、社外ストレージへの通常データバックアップを可能にすること。

解決策：  
既存のソフトウェアファイアウォールと共に、DualDiode Technology® を備えた OPDS-100 データダイオードが配備された。

メリット：  
一方向データフローが、銀行運営ネットワークが外部のサイバー脅威に対し安全であることを保証する。データダイオードにより、信頼できるファイルの社外バックアップへの一方向転送が許可される。

### ビフォー



## 解決策

銀行運営ネットワークへのリモートアクセスを排除し、遠隔バックアップへの取引・顧客データの決定論的一方向データ転送を可能にするために、DualDiode Technology® を使用する Owl 社のデータダイオード (OPDS-100) が採用された。

### ハードウェア

#### Owl 社の周辺機器防御ソリューション - 100 (OPDS-100)

ネットワークのセグメント化および決定論的一方向データ転送専用に設計された内蔵型 1U データダイオード。



## ✓ 結果

- 銀行運営ネットワークの周囲に設定されたハードウェアで強化された安全な境界
- データダイオードが銀行運営へのインバウンド接続をすべて排除すると同時に、信頼できるバックアップデータの決定論的アウトバウンドフローを提供した
- 銀行運営ネットワークはどの外部ネットワーク接続によってもアクセスできなくなった
- 社外バックアップへの高度に制御された一方向データフローにより、業務を継続できた

アフター

銀行運営  
センター

銀行取引

DualDiode®

サイバー脅威

脅威の軽減

一方向データフロー

クラウド

遠隔  
ストレージ



# 使用実例 鉄道輸送

遠隔ネットワーク監視

全米通勤鉄道会社が列車および  
レールセンサの遠隔監視の安全を確保

## 企業の概要

毎日 15000 台以上の列車を運行する全米通勤鉄道企業。

## サイバーセキュリティに関する課題

この鉄道会社は、性能指標および安全指標を収集するために、列車とレールにセンサを設置した。このセンサは、中央処理施設からの遠隔監視を可能にするが、サイバー脅威の危険性も生まれた。サイバーセキュリティの必要性を認識していた会社は、センサの監視およびデータ集約システムの両方を外部のネットワークアクセスから隔離し、同時に引き続きワイヤレス伝送でセンサデータを集中監視運営センターに送信可能にすることを求めている。

## 要求

- 外部ネットワークからの接続を一切受け付けずに、レール監視ネットワークの「切断された」アーキテクチャを作成すること
- ワイヤレス伝送による集中監視センターへのレール性能および安全データの安全な転送を可能にすること

## 事例の概要

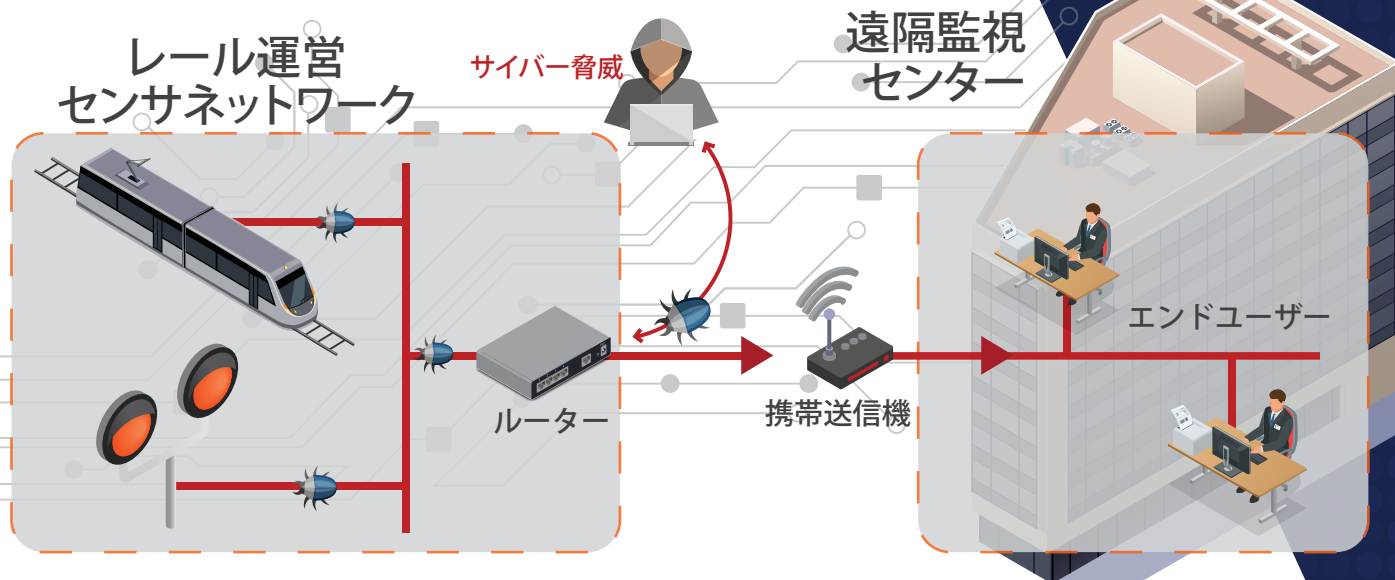
産業：  
輸送 - 鉄道

課題：  
レールセンサネットワークの隔離  
およびセキュリティと同時に  
遠隔監視能力を保護すること

解決策：  
センサデータを転送するために、  
DualDiode Technology® 装備の  
OPDS-100 データダイオードが  
配備された

メリット：  
一方向データフローが、レール  
監視ネットワークが外部の  
サイバー脅威に対し安全  
であることを保証する。  
集中監視運営センターからの  
遠隔監視能力を維持した。

## ビフォー



## 解決策

レール監視および集約ネットワークを外部アクセスから隔離するために、DualDiode Technology® を使用する Owl 社のデータダイオード (OPDS-100) が採用された。データダイオードにより、遠隔監視運営センターへの転送のために、性能・安全センサデータの決定論的一方向データ転送が可能になった。

### ハードウェア

#### Owl 社の周辺機器防御ソリューション - 100 (OPDS-100)

ネットワークのセグメント化および決定論的一方向データ転送専用設計された内蔵型 1U データダイオード。



## 結果

- レール監視ネットワークの周囲にハードウェアで強化した安全な境界を設定
- レールセンサおよび監視ネットワークはどの外部ネットワーク接続によってもアクセスできなくなった
- ワイヤレス伝送システムによる監視センターへの性能・安全センサデータの決定論的アウトバウンドフローを可能にした
- 集中監視運営センターからのレール・路線センサデータの遠隔監視能力を維持した

アフター

レール運営  
センサネットワーク

遠隔監視  
センター

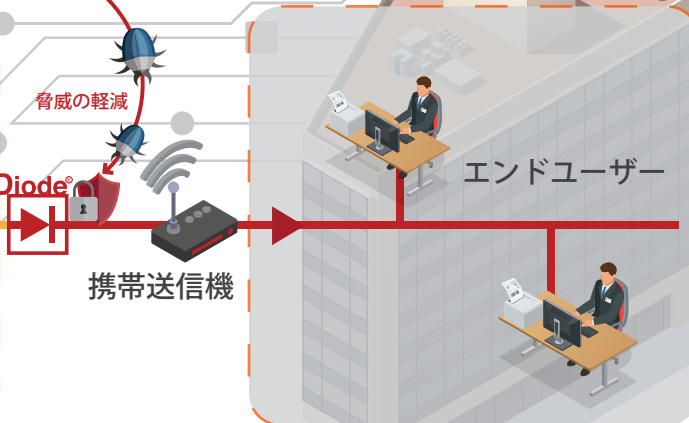
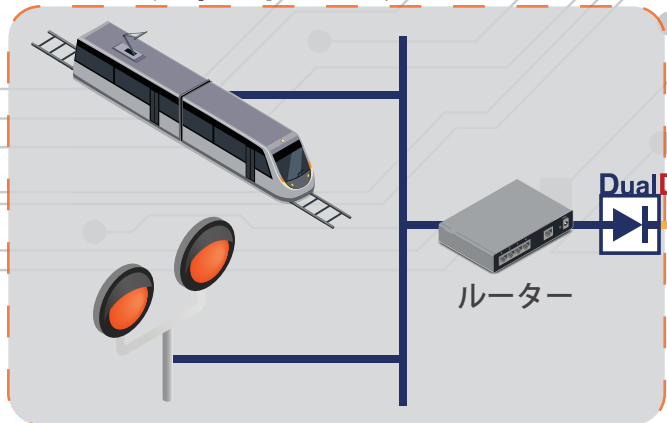
サイバー脅威

脅威の軽減

エンドユーザー

ルーター

携帯送信機



ヘルスケアシステムが電子医療カルテの  
研究データベースの安全を確保

### 企業の概要

病床数 500 床以上の 4 つの病院、および 1000 件を超える医療研究プロジェクトに関わる大学のヘルスケアシステム。

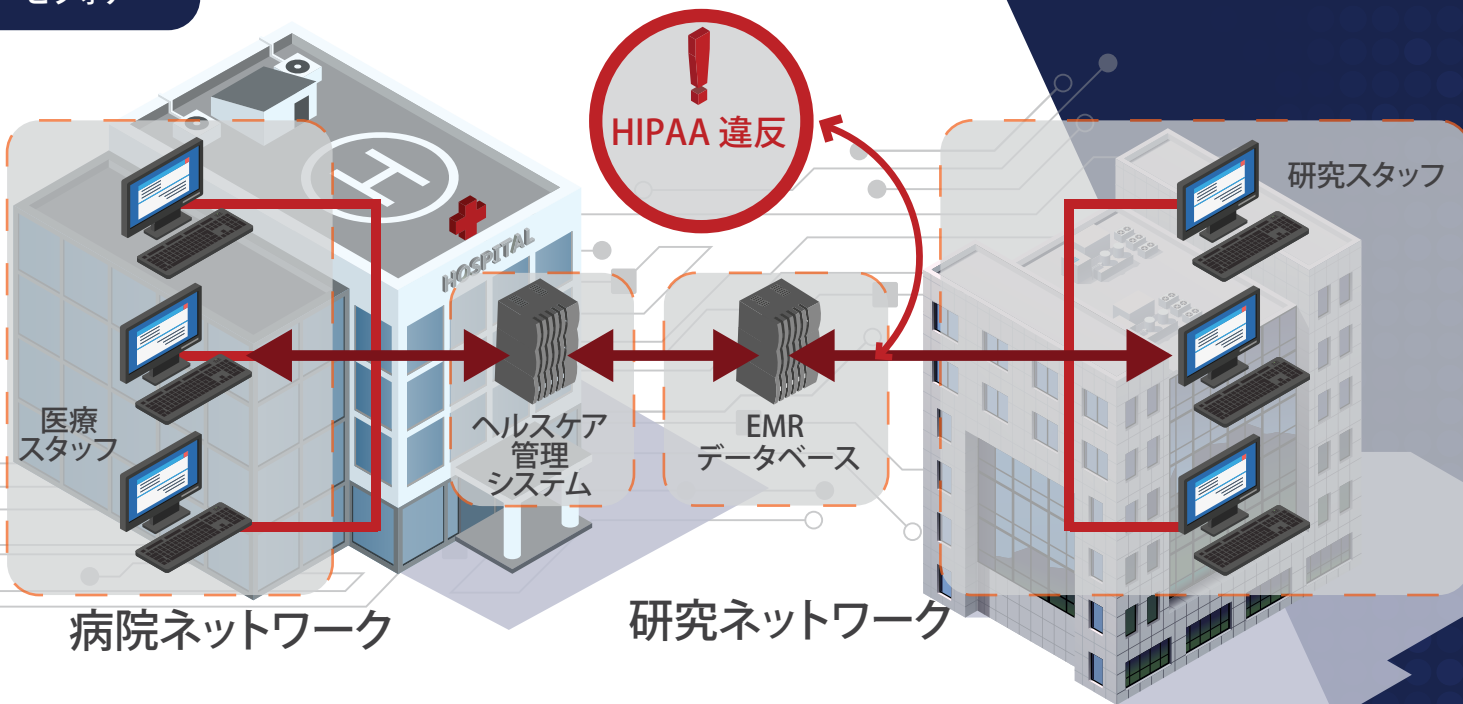
### サイバーセキュリティに関する課題

このヘルスケアシステムは、保護医療情報 (Protected Health Information、PHI) を含む数十万件の電子医療カルテ (EMR) を収録するデータベースを管理している。病院の職員は EMR にアクセスするために、ヘルスケア管理ソフトウェアを使用するが、アクセスは彼らが治療を担当する患者のものに限定されていた。しかし、大学の研究者はこれらのソフトウェアシステムの安全措置を守らず、研究目的で認められた範囲を超えてすべての EMR データベースにアクセスし、HIPAA 違反を犯していた。病院側は、HIPAA 規則を遵守し、研究目的で認められた EMR へのアクセスを管理する方法を求めている。

### 要求

- 研究者が HIPAA を遵守し、選択された患者記録を閲覧できるような、独立した新たな管理ネットワークを作成すること
- アクセス権限を持つヘルスケアワーカーのために、ヘルスケア管理ソフトウェア経由の EMR アクセスを維持すること

### ビフォー



### 事例の概要

産業：

ヘルスケア

課題：

HIPAA 規則を遵守して選択された EMR を研究のために提供し、取り扱いに慎重を要する研究ネットワークを隔離すること

解決策：

DualDiode Technology® 装備の OPDS-100 データダイオードが配備された

メリット：

一方方向データフローが、EMR データベースネットワークが外部のサイバー脅威に対し安全であることを保証し、同時に研究者が認められた PHI にアクセスするのを許可する。



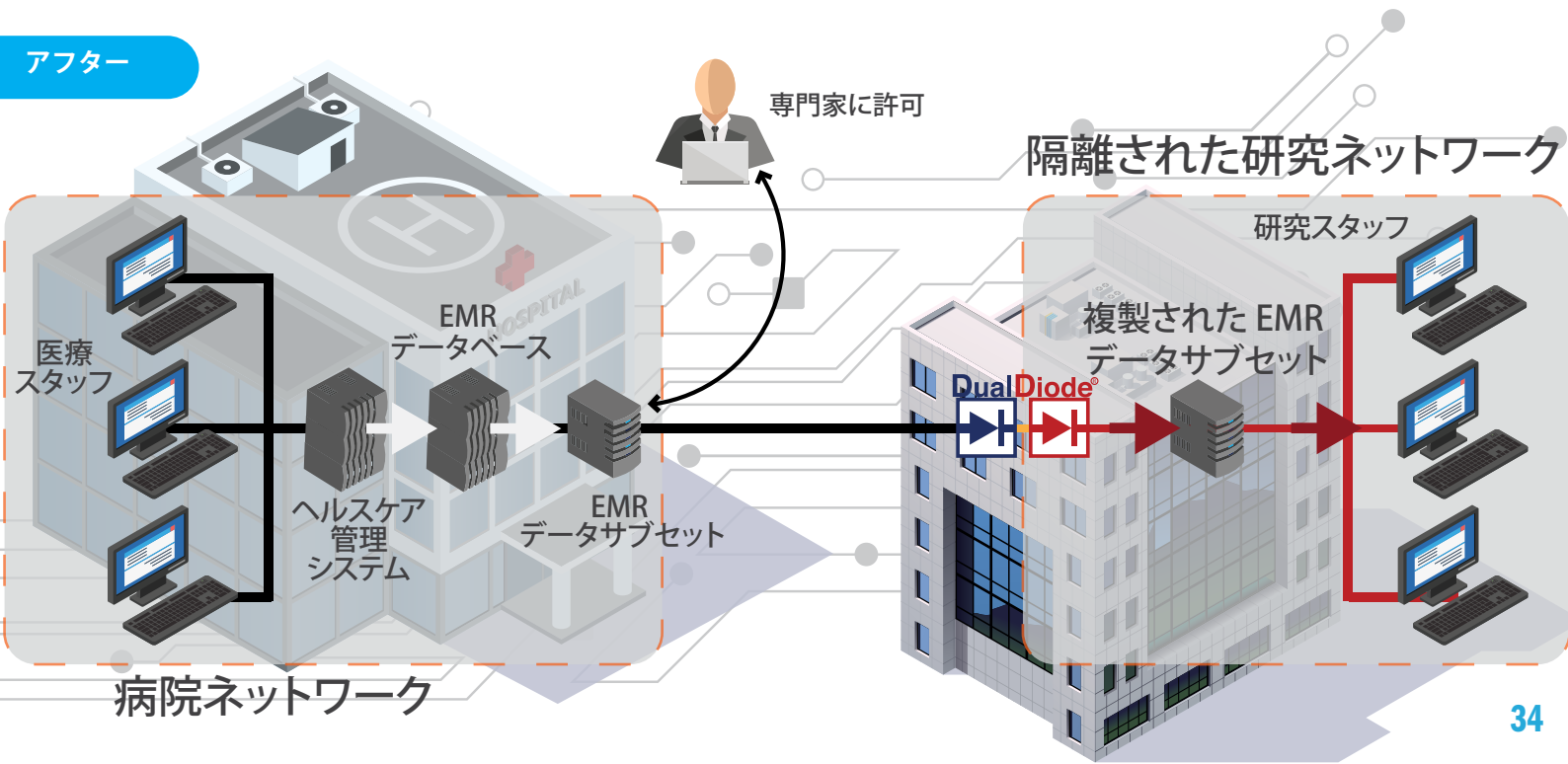
## Owl 社の周辺機

ネットワークのセグメント化および決定論的一方向データ転送専用設計された内蔵型 1U データダイオード。



- EMR 研究ネットワークの周囲にハードウェアで強化された安全な境界を設定し、研究者がすべての EMR データベースへアクセスすることから隔離した
- EMR & PHI のアクセスに関して確実に HIPAA 規則が遵守されるようになった
- 研究スタッフには選択、許可された患者記録の分析を引き続き行えるようにした

## アフター



# 索引

以下は、上述の使用事例に挙げられたセクター、製品、ソフトウェア、テクノロジー、および規制機関の総合リストと、本書内におけるこれらの参照先である。

## セクター

化学産業、7  
重要な製造業、5  
ダム、19  
エネルギー、1、3、13、15、17、19、21  
金融サービス、23、25、27、29  
ヘルスケア、33  
原子力、9、13、19  
輸送、31  
上下水道、11

## テクノロジー

ファイアウォール (ソフトウェア)、1、23、29  
HMI (レプリケーション)、11、21  
Modbus (レプリケーション)、2、13  
OPC (レプリケーション)、7、15、21  
OSIsoft PI System (レプリケーション)、1、3、7、9、13、  
15、19、21  
Rockwell Automation、9

## 製品

### ハードウェア

企業周辺機器防御ソリューション (EPDS)、2、4、20  
Owl 社の周辺機器防御ソリューション – 100 (OPDS-100)、6、18、26、30、32、34  
Owl 社周辺機器防御ソリューション – 1000 (OPDS-1000)、14、28  
Owl 社周辺機器防御ソリューション - 多目的 (OPDS-MP)、2、8、10、12、16、22、24

### ソフトウェア

OPC セキュア転送サービス (OSTS)、8  
Owl モdbusインターフェース (OMBI)、14  
Owl PI 転送サービス (OPTS)、2、4、8、10、14、16、20、22  
遠隔ファイル転送サービス (RFTS)、26  
セキュアディレクトリファイル転送システム (DFTS)、30  
Owl 社仮想スクリーンビュー (OV2S)、12、22

## 規制機関

会計検査院 (GAO)、19  
HIPAA、33  
北米電力信頼度協議会重要インフラ保護 (NERC CIP)、15、17、19、21  
原子力規制委員会 (NRC) Regulatory Guide、13、19





1-866-695-3387  
[WWW.OWLCYBERDEFENSE.COM](http://WWW.OWLCYBERDEFENSE.COM)

V1 | JUNE 2017

© Owl Cyber Defense Solutions, LLC

OWL 日本輸入販売総代理店

**Dírex**  
JAPAN DIREX CORPORATION

日本ダイレックス株式会社 ISO9001認証取得

〒135-0064 東京都江東区青海2-4-32 タイム24ビル4F

TEL 03-3242-3157

Email [sales@direx.com](mailto:sales@direx.com) URL <http://www.direx.com>

本資料に記載された仕様、デザインなどは、予告なしに変更することがあります。