

一芯一方通信装置データダイオードの 最新動向および事例

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

1. OWL社の紹介
2. サイバーセキュリティ標準と最良事例(技法)
3. 米国 国土安全保障省(DHS)
重要インフラを守るための7つの戦略
4. 産業系ネットワーク利用事例
5. OWL社データダイオード製品の紹介



企業概要

米国内で研究開発と国内製造
米国のサプライチェーン利用による一環品質確保
米国ベースの直接テクニカルサポート&サービス
米国の機密情報及び最高機密情報取扱許可に基づく厳正な対応
自己資金による長期を見通した研究開発



経営と実績

17年間のサイバーセキュリティ専門に活動
各国2000システムのグローバル展開
グローバルセールスとリモートサービスの提供
認定サービスの提供
構成管理サービスの提供



市場戦略

政府クロスドメインソリューション
国防総省 & 諜報機関
UCDSMOベースライン リスト(*1)に認定済み
重要インフラネットワークの防衛
ユーティリティ: 原子力、電気、ガス、水道
エネルギー: 石油・ガス、石油化学
電気通信 金融サービス



技術革新

シングル1U、オールインワンソリューション
サーバーベースの通信カードシステム
24の技術特許を保持
ハードベースの完全一芯一方向転送を実現
EAL認定取得
UCDSMO サイバーベースライン認証

(*1)UCDSMO Baseline list : Unified Cross Domain Services Management Office Baseline list
米国の国防、諜報部門がCross domain サービス管理に関する技術やソリューションとして有効性を認証したプロダクトのリスト

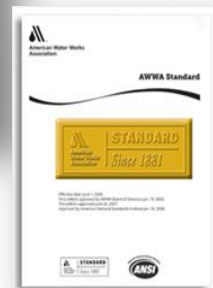
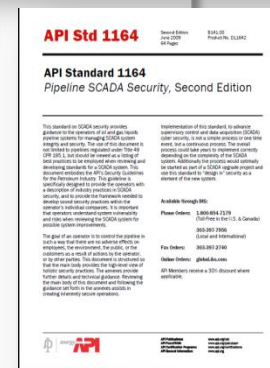
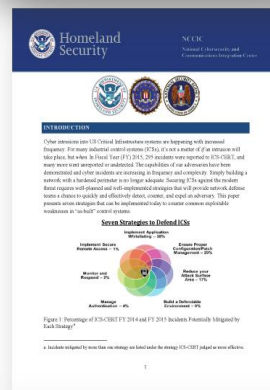
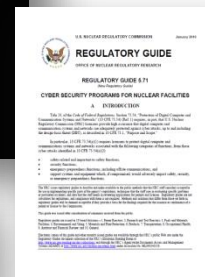
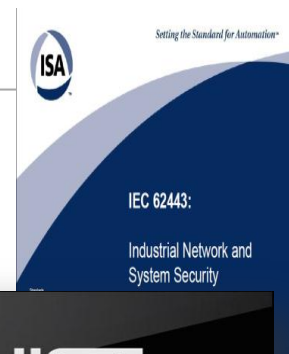
- 産業用オートメーションIEC-62443
- 機密性、完全性、可用性
- 米国DHS/FBI とNSAのガイダンス(7つの戦略)
- アメリカ合衆国原子力規制委員会(NRC) 5.71
- 北米電力信頼度協会 (NERC) CIP 5 002-009
- Industry Analysis and Guidance

(Gartner, ARC Advisory Group Advisory Group)

- NIST(アメリカ国立標準技術研究所) SP800-82
- アメリカ石油協会標準1164
- ChemITC
- アメリカ水道協会 G430-09
- 国際原子力機関-IAEA

日本

- サイバーセキュリティ基本法
- サイバーセキュリティ経営ガイドライン
- 電力制御システムセキュリティガイドライン (JESCZ0004)

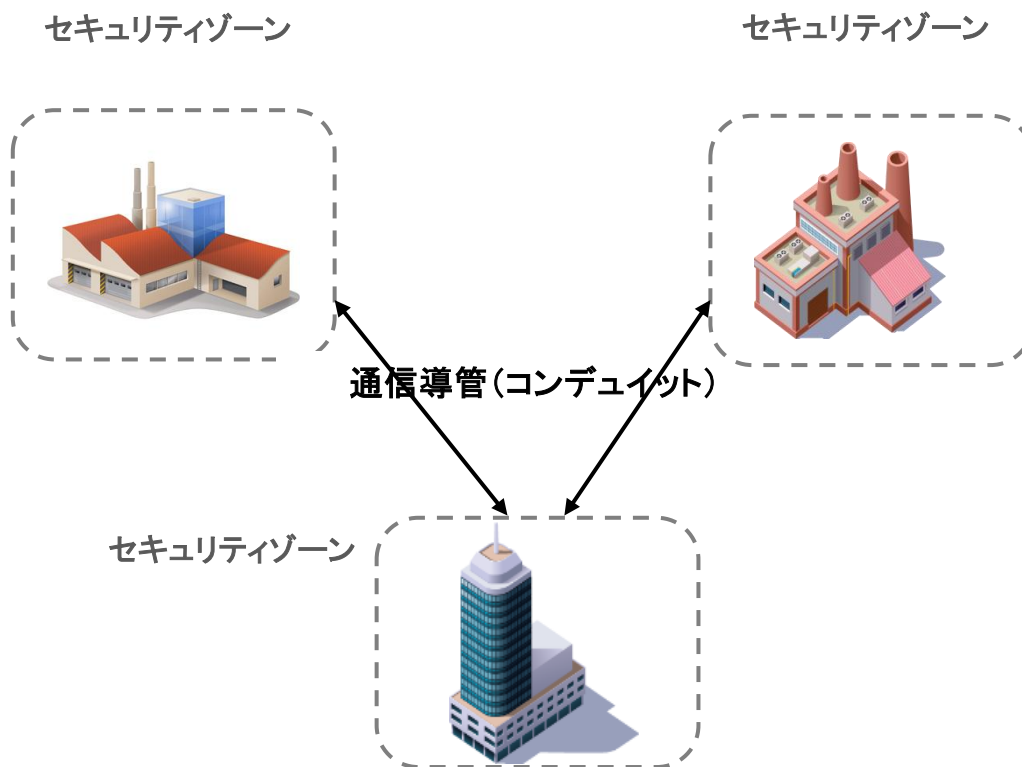


セキュリティゾーンを明確にする

- セキュリティプログラムを組み立てる際、ゾーンは、セキュリティプログラムが成功するための最も重要なツールの一つであり、ゾーンとセキュリティ・レベルを明確にすることは、そのプロセスにおいて最も重要な思考工程の外観（アспект）である。

セキュリティゾーン: 隔離ネットワーク体
共通のセキュリティ要件をもつ
物理・情報資源の論理的グループの
明確化

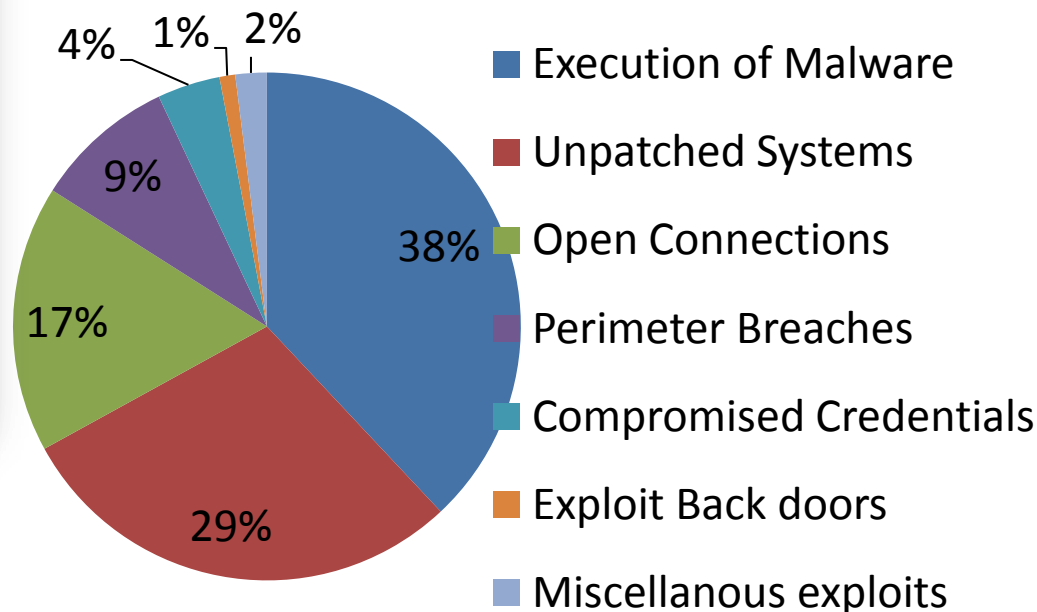
コンデュイット: 通信導管
セキュリティゾーン間で情報交換を行う
手段の特定



アメリカ合衆国国土安全保障省(DHS)によるリサーチ

Cyber Threats Against Industrial Controls

産業向けコントロールに対するサイバー脅威



マルウェアの実行

パッチを当ててない
システム
オープンコネクション

境界線破損

危険な資格証明

エクスプロイトバック
ドア
混合エクスプロイト



1. Application Whitelisting -アプリケーション・ホワイトリスト
2. Configuration/Patch Management
セキュリティ設定/パッチ管理
3. Reduce Attack Surface Area 攻撃面を減らす
4. Defendable Environment 防衛可能な環境
5. Manage Authentication 認証管理
6. Implement Secure Remote Access
安全な遠隔アクセスの導入
7. Monitor & Respond モニター&レスポンス



これらの戦略で、2014年と2015年にあった攻撃の98%は防ぐことができた。

- **Application Whitelisting:** Only allow predesignated applications to run, no need to be aware of new threats since only authorized software will run.

アプリケーション・ホワイトリスト: あらかじめ指定されたアプリケーションのみ作動許可。権限を与えられたソフトウェアのみ作動するので、新たな脅威を警戒する必要がない。

- **Reduce Attack Surface Area:** Isolate industrial control system (ICS) networks from untrusted networks, lock down unused services and ports, use a **data diode** to provide network segmentation, if bidirectional communication is needed use a single port over a restricted path.

攻撃面の削減: 産業コントロールシステム(ICS)ネットワークを信頼できないネットワークから隔離させ、使用していないサービスやポートの利用を厳禁しネットワークセグメンテーションを実現するために**データダイオード**を使用する。もし、双方向性のコミュニケーションが必要な際には、限定された専用の経路上に立てたシングルポートを使用する。

- **Build a Defendable Environment:** Consider using **optical separation technologies**. Limit damage from network perimeter breaches. Segment networks and restrict host-to-host paths to prevent and contain the spread of infection.

防衛可能な環境の構築: **光学的に分離する技術**を使用することを検討する。ネットワーク境界線からの侵害によるダメージを限定する。感染の蔓延を防ぎ、阻止するために、ネットワークを分離し、ホストとホスト間の通信経路を限定する。

- **Implement Secure Remote Access:** Remove back doors and modem access, implement monitoring only with access enforced by **data diodes**, do not rely on "read only" software configurations, don't allow persistent remote connections.

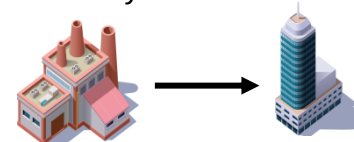
安全な遠隔アクセスの導入: バックドアとモデムアクセスを除去し、**データダイオード**によるモニターのみの強制アクセス制御を導入。「閲覧のみ」というソフトウェア設定を当てにしない。継続的なリモートコネクションを許可しない。

#1 One-Way Communications Path out of the Plant

#1 プラント側からの一方向コミュニケーションパス

- Build a Defendable Environment: Segment networks and restrict host-to-host paths to prevent and contain the spread of infection
- 防衛可能な環境の構築: 感染の蔓延を防ぎ、阻止するために、ネットワークの分割と、ホストとホスト間の通信経路を限定する。
- Reduce Attack Surface Area: Use a **data diode** to provide network segmentation
- 攻撃面の削減: ネットワークを分割するために、**データダイオード**を使用する。
- Implement Secure Remote Access: Implement monitoring only solution with access enforced by **data diodes**
- 安全な遠隔アクセスの導入: **データダイオード**の強制的アクセス制御によってモニタリングのみのソリューションを導入する。

One-Way OUT

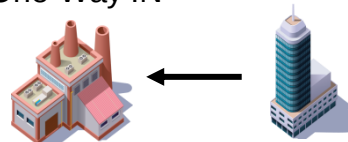


#2 One-Way Communications Path into the Plant

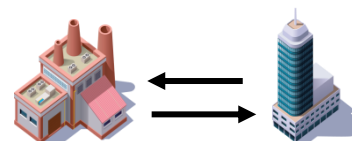
#2 プラントへの一方向コミュニケーションパス

- Configuration/Patch Management: Provide secure configuration/patch management program centered on safe importation of trusted patch updates
- セキュリティ設定/パッチ管理: 信頼できるパッチアップデートの安全性に重きを置いたセキュリティ設定/パッチ管理プログラムを用意する。

One-Way IN



One-Way IN and OUT

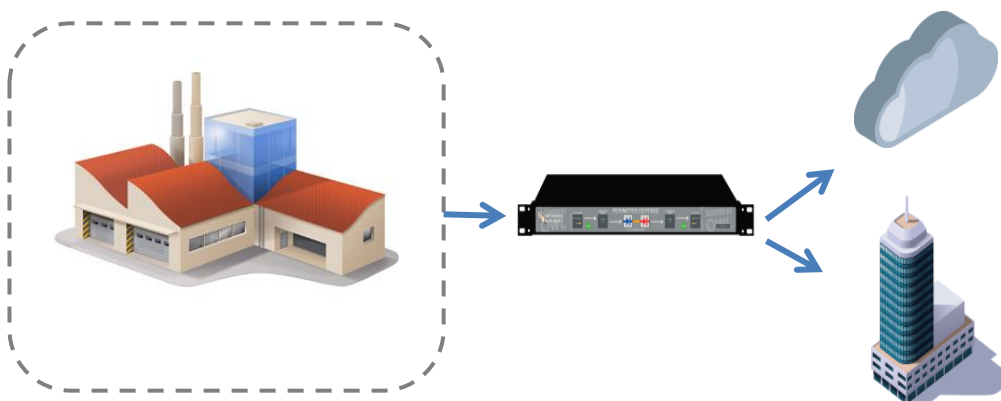


#3 Two-Way Communications Path with the Plant

#3 プラントとの双方向コミュニケーションパス

- Reduce Attack Surface Area: If bidirectional communication is needed use a single port over a restricted path
- 攻撃面の削減:もし、双方向性のコミュニケーションが必要な際には、限定された専用経路上に立てた、シングルポートを使用する。

1. 制御された電子セキュリティペリメーター（「**隔離ネットワーク体**」）を確立する。
2. **一方向データフロー**を導入する。



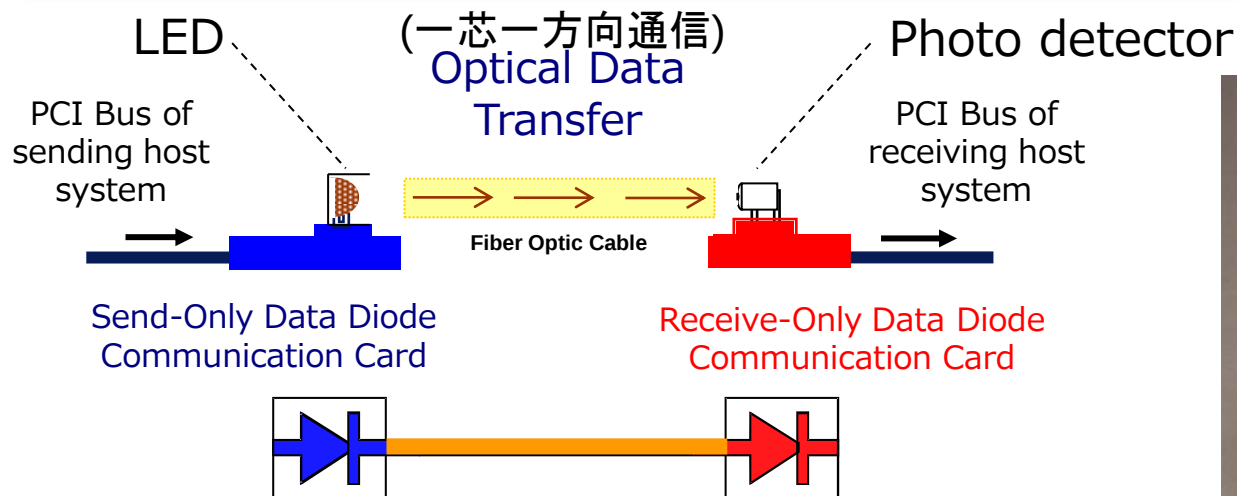
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

 **U.S. NRC**
United States Nuclear Regulatory Commission

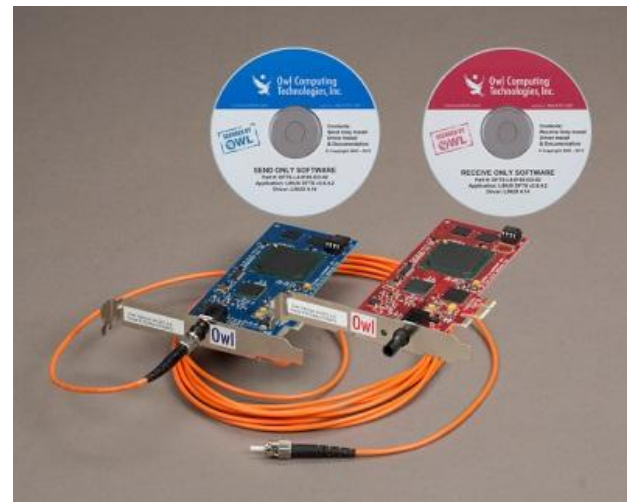
データダイオードは下記のために使われる配置ソリューションである。:

- サイバーリスクを減らす。
- 重要（監視）サイバーアセットをサイバーアセットに 転換する。
- オペレーターを企業コンプライアンスに合わせられるよう手助けする。

- ハードウェアベースのサイバーセキュリティ対策装置です。
- 一方方向のみに設計されたハードウェアを使用しています。
- ソフトウェアの改ざんや攻撃を遮断します。
(ハードウェアの変更は不可)
- ネットワークの各エンドポイントが終端・保護されています。
- ネットワーク間のNon-Routable (IPアドレス、MACアドレスを転送しない) ATMによるプロトコルブレイクを実現しています。



ソフトウェアの攻撃は100%防御します。



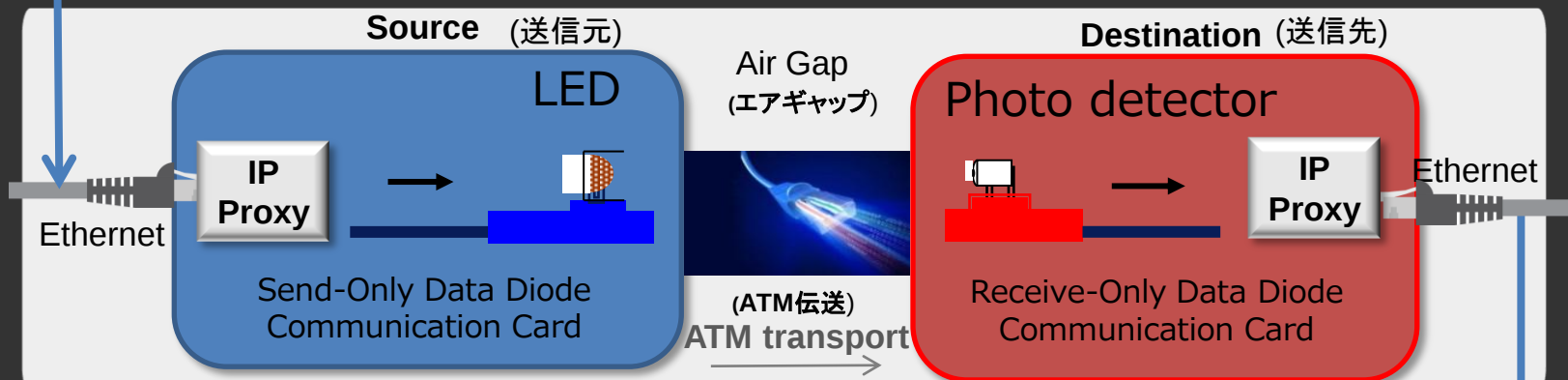
デュアルダイオード: ハードウェア回路ベースの一芯一方方向データフローポリシーを適用



OT Network

- ・ハードウェアDualDiode、2つの通信カードを直列に接続したハードウェア構成。
- ・エアギャップを作り、強制的にネットワークを分離。
- ・IPプロキシ…IPトラフィックを(ブルー側で)終端、(レッド側で)起動する。
- ・一方方向ハードウェアは、単一の光ファイバケーブルによって強制的に一芯一方方向通信を実現。

DualDiode Technology



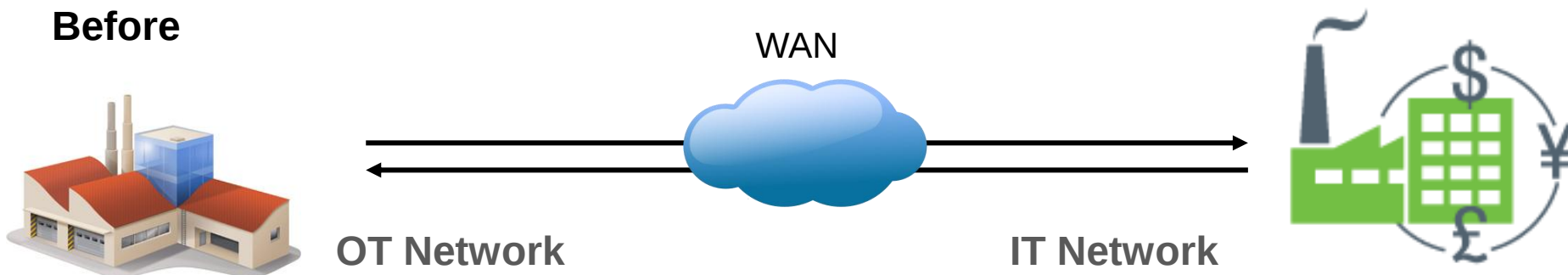
セキュリティ属性:

- ・ルーティング可能な情報(MAC、IPアドレスなど)は、OTネットワークの外部にさらされることはありません。ペイロードのみがエアギャップ間を転送されます。
- ・信頼性の高い高速ATM転送は、「ディープ・プロトコルブレイク」を提供します。
- ・すべてのデータタイプの転送がホワイトリスト化され制御されます。

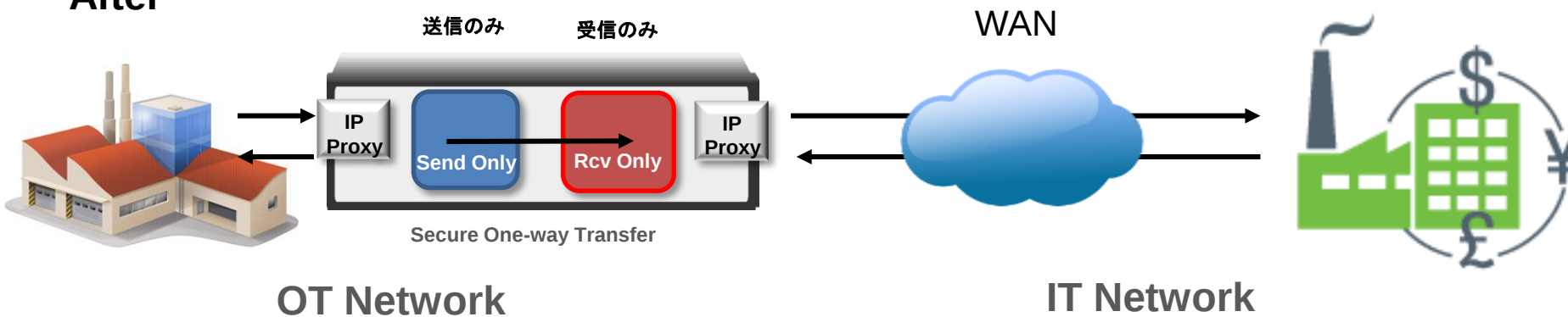


IT Network

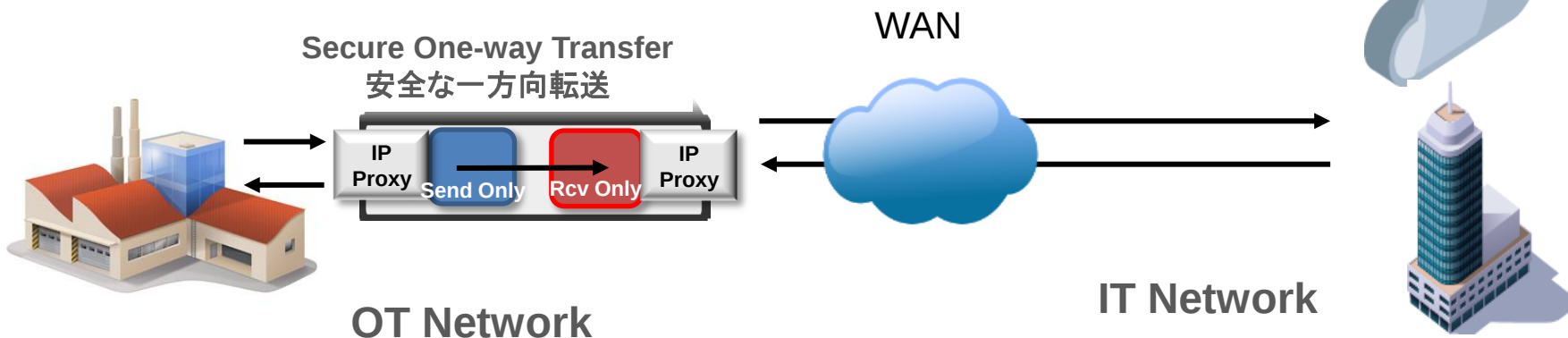
Before



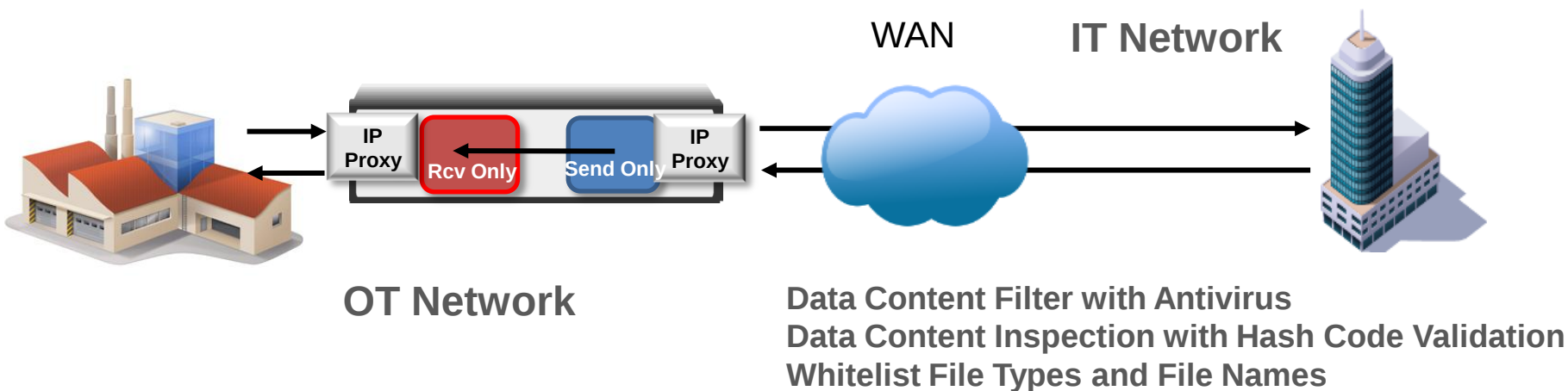
After



#1 DHSが推奨する一方向アウト (One-Way out)

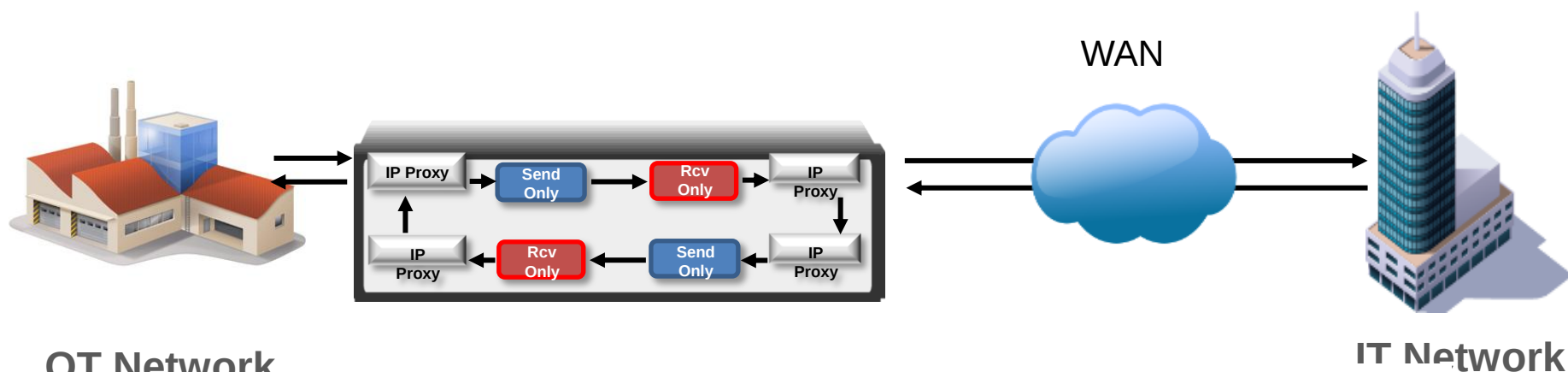


#2 DHSが推奨する一方向イン (One-Way in)



DHSの戦略#3:攻撃面を減らす

もし、双方向性のコミュニケーションが必要な際には、限定された通信経路上に、シングルオープンポートを使用する。



Owl Bilateral Communication System (OBCS):

- 限定された通信経路上でのシングルポート
- 一方向にはなりえないTCP/IPアプリケーションをサポートする
- 1U以内に安全な一方向転送のペア
- ノンルータブルATMプロトコルブレイク
- シングルのホワイトリストセッションを分離して接続するTCP/IPプロキシ

発電、変電、配電

- ・タービン、原子力、火力・水力発電所のパフォーマンスデータ
- ・ヒストリアンのレプリケーション
- ・セキュアリモート監視 - syslog、アラーム、イベント
- ・コンプライアンスレポート



製造業・鉱業

- ・システムアラーム、イベント、Syslogメッセージなどのセキュアな監視
- ・ファイル、電子メール、セキュリティビデオの転送



石油とガス

- ・ヒストリアン・データ、アラーム、イベントの転送
- ・インターフェース: MODBUS、OPC



水処理、廃水処理

- ・WindowsのHMI画面の複製
- ・ヒストリアン・データ



金融と銀行

- ・セキュアな場所とセキュリティの低い場所間のデータ転送
- ・金融取引



石油・ガス

周辺機器防御ソリューション

世界的な石油・ガス企業が本社への生産データの一方転送を実現

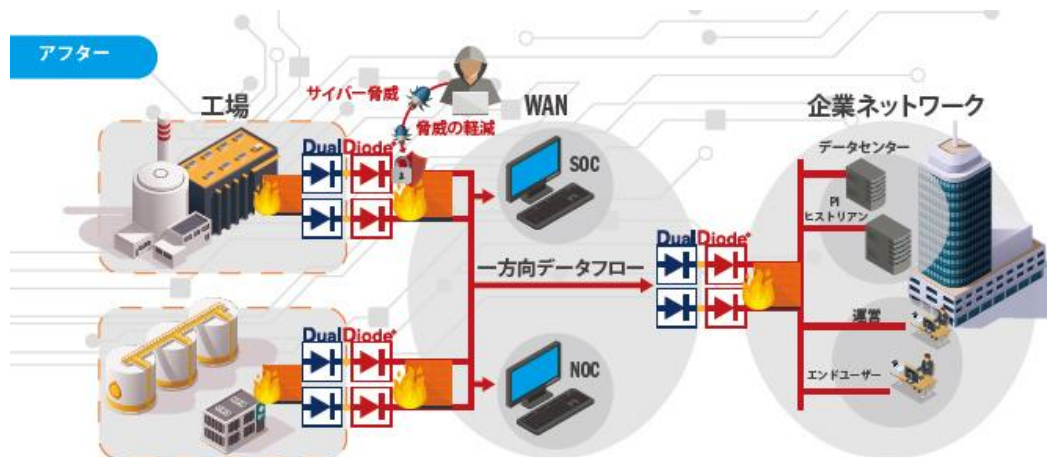
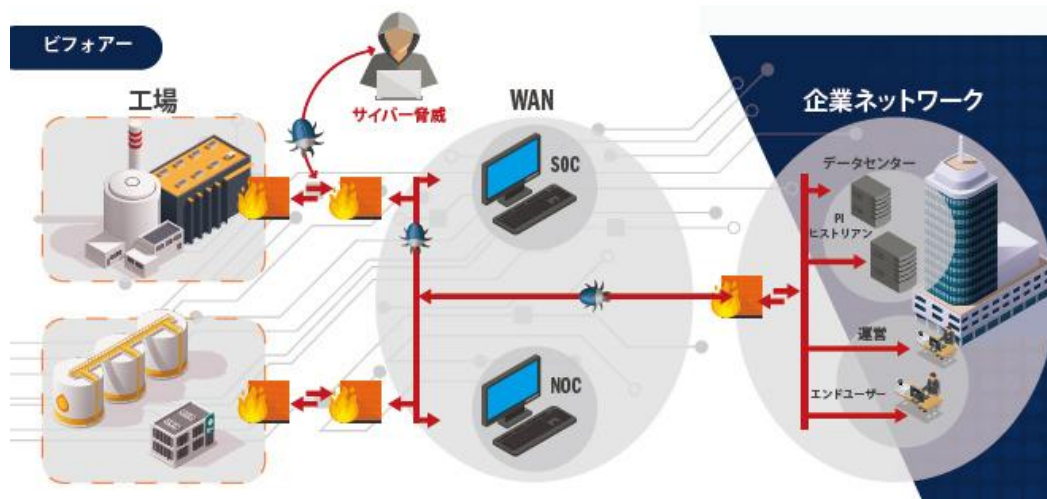
事例の概要

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くなった

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



原子力発電

周辺機器防御ソリューション

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

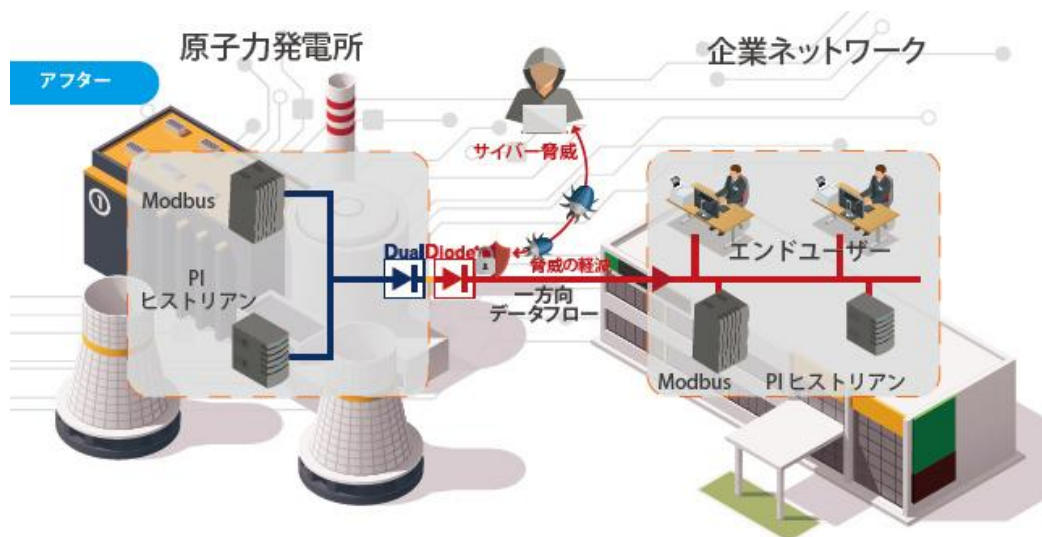
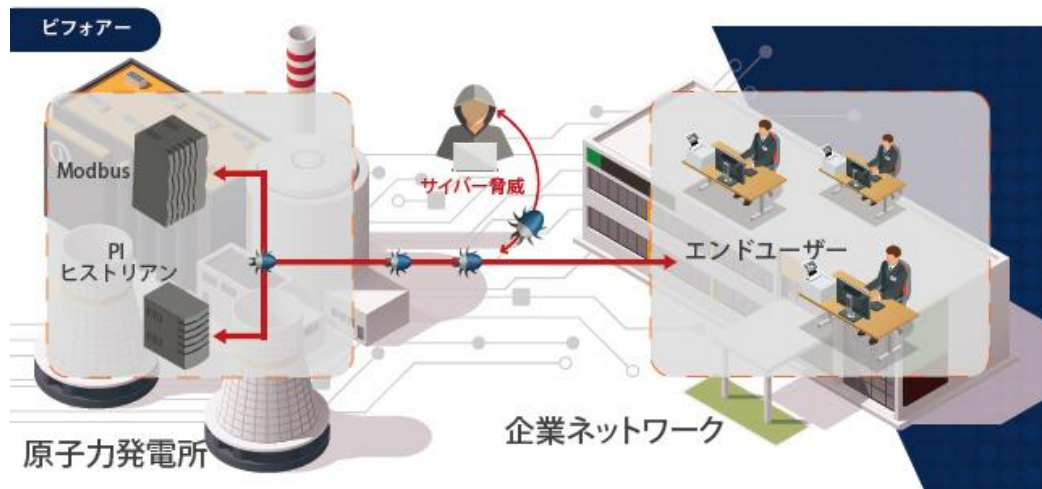
事例の概要

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。



銀行 ATM

データリポジトリデータベース

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 内のATM 収集データの安全
を確保

事例の概要

産業：
銀行業

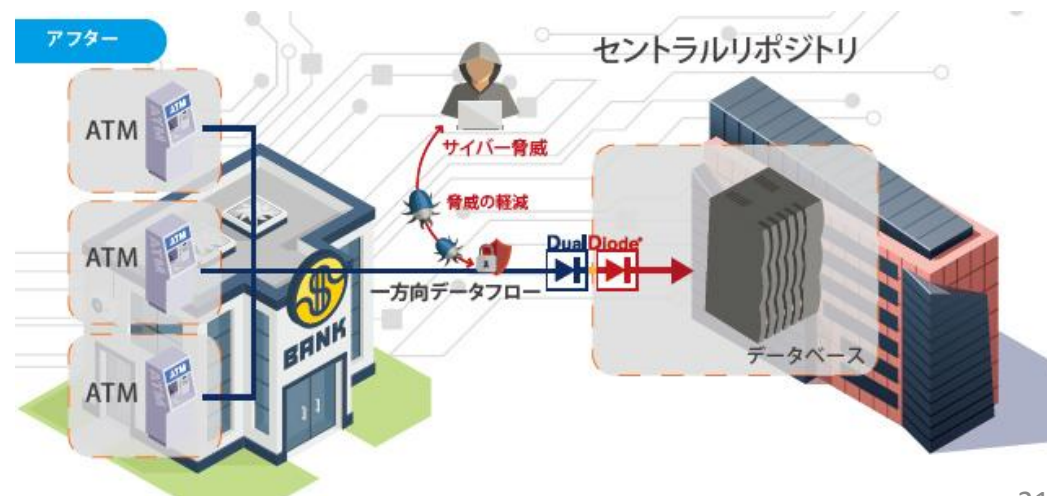
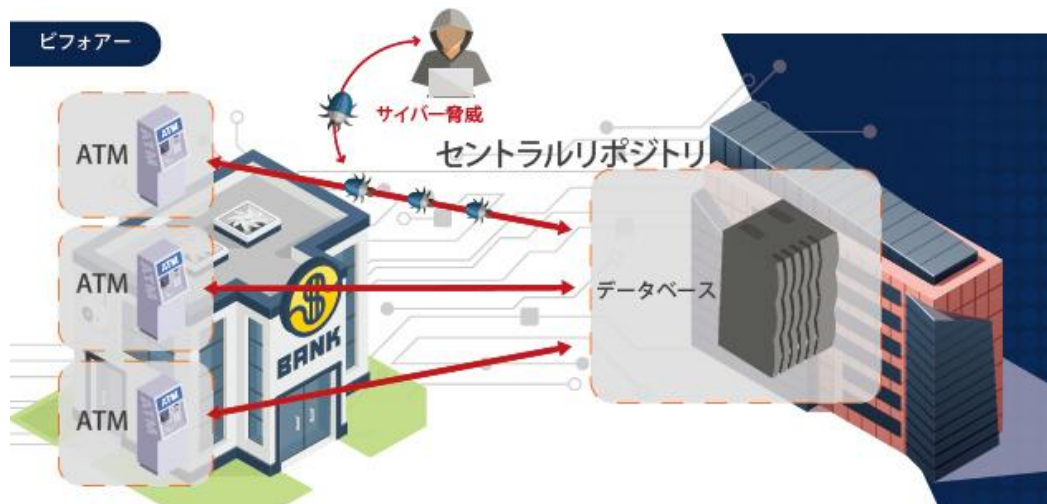
課題：
セントラルデータリポジトリを隔離してその
安全を確保すると同時に、現場の ATM から
の信頼できるファイルの収集を保護する
こと

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許可する



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

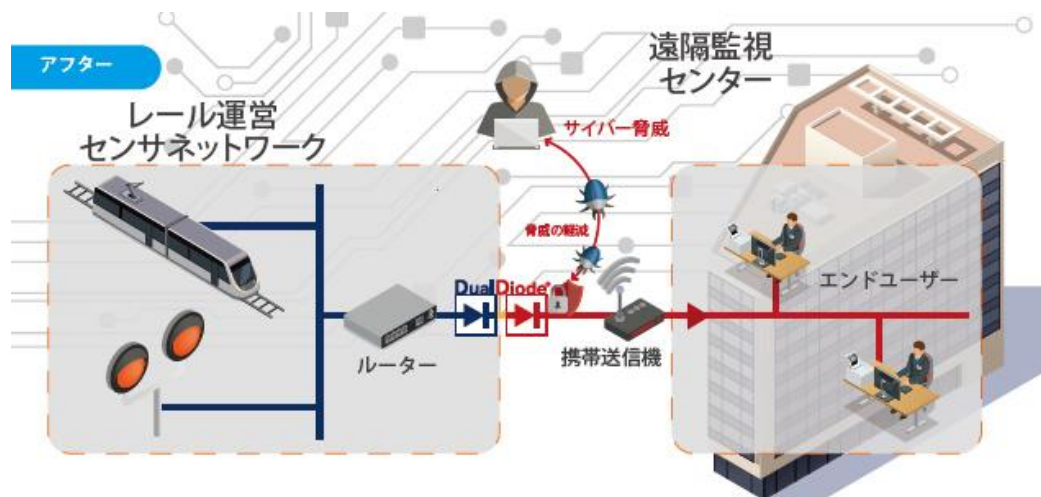
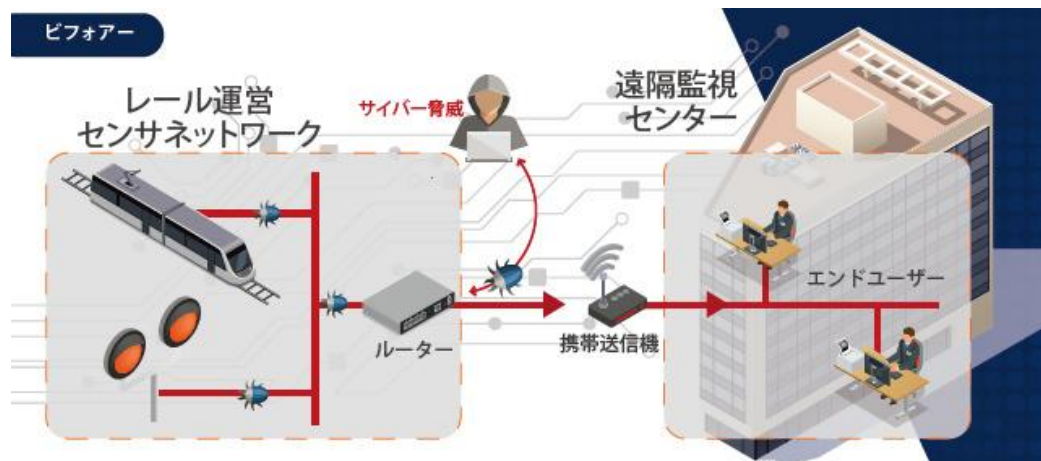
事例の概要

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。



ヘルスケア

周辺機器防御ソリューション

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

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

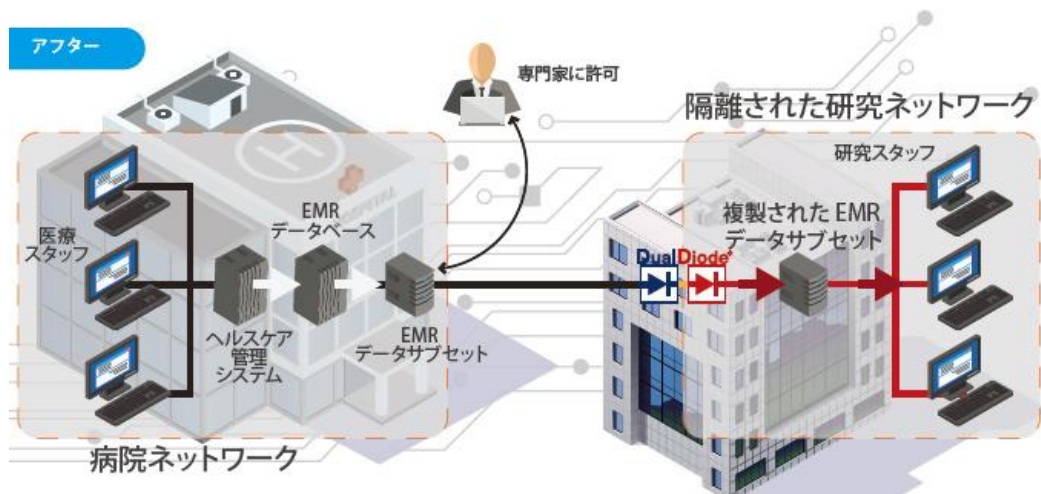
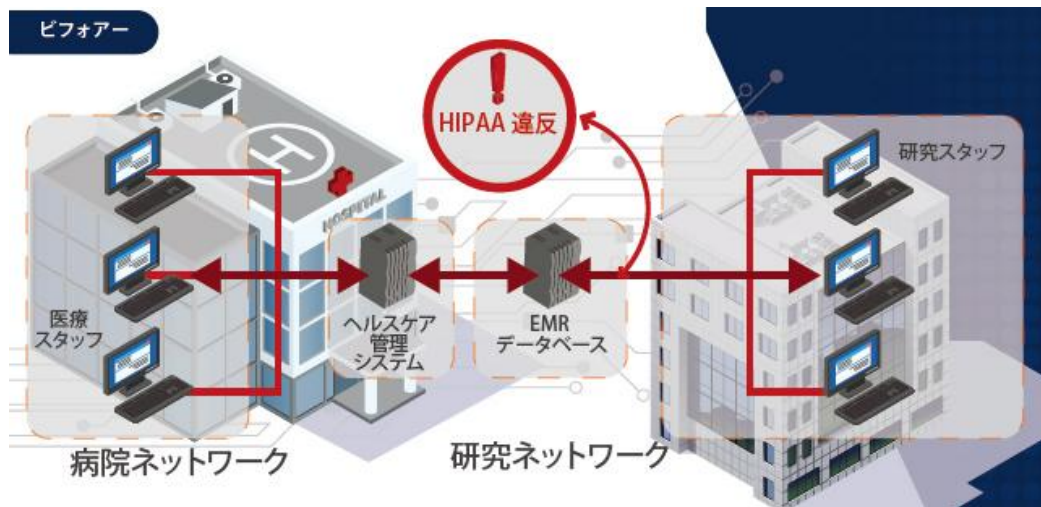
解決策：

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。

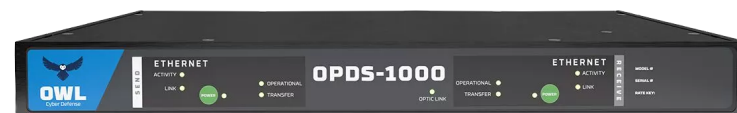
HIPAA: 医療保険の携行性と責任に関する法律
(Health Insurance Portability and Accountability Act)
EMR: 電子カルテ (Electronic Medical Record)
PHI: 保護対象保健情報 (Protected Health Information)



- ネットワークハードウェアインターフェイス
 - Ethernet, serial RS232 & 422, USB, dial up modem, very small embedded diode products イーサネット、シリアルUSB、ダイヤルアップモデム
- 標準的なベンダーソフトウェアインターフェイス
 - Yokogawa, OSIsoft, GE, Rockwell, Honeywell, Schneider, InStep, AspenTech, Mitsubishi, PAS Alarm, McAfee, Symantec, Tripwire, Splunk, Rolls Royce, Scientech, MS SQL, Oracle
- ネットワークアプリケーションインターフェイス
 - Syslog, SNMP, FTP, SFTP
 - Email (SMTP)
 - UDP, multicast, broadcast, unicast (video)
 - TCP/IP
- スタンダードボディインターフェイス
 - OPC Foundation interfaces: DA, A&E, UA
 - Modbus

1. 相互接続したIIoTは、最良のサイバーセキュリティ対策を必要としている。
2. 標準化団体、産業組合、行政体は、多大な努力を払って、重要インフラに対するサイバーセキュリティ標準及びガイダンスを作成し、発表している。
3. アメリカ合衆国国土安全保障省は、ICSを守る、7つの戦略を発表している。
その中でデータダイオードを使用することを以下の項目で推奨している。
 - ・ 防衛可能な環境の構築
 - ・ 攻撃面の削減
 - ・ 安全な遠隔アクセスの導入
4. データダイオード使用事例は、DHSによるICSを守るための推奨をわかりやすく説明している。

- **Owl Perimeter Defense Solutions (OPDS): OWL境界防衛ソリューション**
 - DualDiode設計(一芯一方向通信)でサイバー攻撃からネットワークを保護します。
 - ネットワークドメイン間でのデータのセキュアな転送を提供します。
 - 統合 DualDiodes(送信元プロキシ発光部、着信先プロキシ受光部の機能統合)
 - インターネットセキュリティセンターのしっかりしたガイダンスに基づく OwlCentOSの搭載。
 - <http://www.cisecurity.org>
 - Owlのロールベースのアクセス制御システム(RBAC)のオーバーレイ
 - データフローをサポートするコア転送アプリケーション
 - UDP, TCP
 - File transfer, FTP, email transfer
 - Syslog, SNMP
- OPDS-100D
- OPDS-1000
- Specialty Software Connectors



- OPDS-100D
 - All-in-one, DIN rail form factor solution
- Common Features:
 - Owl Red HatOS
 - Owl RBAC
 - Owl Core transfer Applications
- Bandwidth across DualDiode
 - 10Mbps
 - 26Mbps
 - 52Mbps
 - 104 Mbps
 - All filed upgradeable from 10, to 26, to 52 to 104Mbps



- OPDS-1000
 - All-in-one, 1u 19" rackmount solution
- Common Features:
 - Owl Red HatOS
 - Owl RBAC
 - Owl Core transfer Applications
- Bandwidth across DualDiode
 - 104 Mbps
 - 155 Mbps
 - 300 Mbps
 - 600 Mbps
 - 1,000 Mbps = 1 Gbps
 - All filed upgradeable from 104, to 155, to 300, to 600 to 1,000 Mbps



- 特別なソフトウェアコネクタ(アプリケーションソフトウェアのサポートパッケージ)
 - Remote File Transfer Service (RFTS)
 - OSISoft PI replication
 - OPC Server replication
 - MS SQL and Oracle SQL replication
 - Window Screen replication
 - ModBus register replication

- ・セキュアソフトウェア更新サービス(SSUS)
 - ・ネットワークを介してソフトウェアのパッチやアップデートを実行するための特別な製品です。
 - ・セキュアハッシュアルゴリズム(SHA)コードを利用しています。
 - ・ワークフロー内でSHAコードホワイトリストが必要です。
 - ・ファイル転送承認のためのファイルSHAコード値の計算・比較を実行します。
- ・Owl パフォーマンス管理サービス(OPMS)
 - ・Owl製品の管理とパフォーマンスのダッシュボードを提供します。
 - ・Owlデュアルダイオード製品はOPMSにすべてのパフォーマンスログを送信します。
 - ・OPMSは、パフォーマンス・メトリックのダッシュボードを提示します。
 - ・ファイル転送性能、ファイル数、速度、合計バイト
 - ・ログファイルでエラーと警告のイベントを送信

Owl Computing Technologies, Inc



Owl 日本輸入販売総代理店



日本ダイレックス株式会社

本社：〒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

URL <http://www.direx.com>