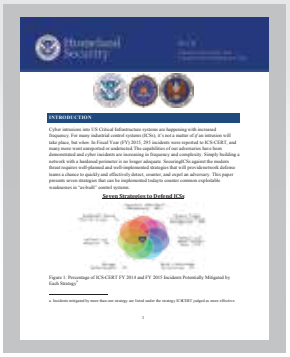
OPDS サポート
DHS (米国国土安全保障省) の 7 つの戦略

DHS はサイバー攻撃を阻止するための戦略を提供

重要な社会的生産基盤 (輸送、エネルギー供給、水道など) に対するサイバー攻撃のリスクを軽減するために、米国国土安全保障省 (DHS) は産業制御システム・サイバー・緊急. 対応チーム (Industrial Control Systems Cyber Emergency Response Team、ICS-CERT) を運営しています。ICS-CERT は、様々な機関、警察、所有者、オペレーター、およびベンダーと協力して産業事件に関する情報を共有することで、サイバー脅威に対する制御システム環境防御指針を提供します。

多くの産業用制御システムは、デジタル資産 (SCADA、PLC、ヒストリアン)です。デジタル資産は、工場設備、ポンプ場、製油所、変電所、ダムなどを包括する制御技術 (Operational Technologies、OT) ネットワークを運営し、その活動を記録します。2015年中、DHS は 295 件のセキュリティインシデントが ICS-CERT に報告され、未報告あるいは未検出の事案が他にもあることを指摘しました。つまり、2015 年中には、営業日には一日に 1 件以上のインシデントがあったということです。DHS は、同じ期間 に「サイバー攻撃は頻度が増加し、複雑化し」、「...最新の攻撃に対して ICS の安全を確保するには、良く計画され、正しく遂行される戦略が必要...」であると報告しました。



産業用制御システムの防御

この増え続けるサイバーセキュリティに対する脅威の対策を講じるために、FBI と NSA の専門家の尽力を受け DHS は、**「産業制御システムを効果的に守る7つの戦略 *(Seven Steps to Effectively Defend Industrial Control Systems)*** [1] と呼ばれる報告書を公表しました。この報告書は、産業用制御システム内で弱点となったサイバーセキュリティの脆弱性に対応する 7 つの戦略が述べられています。

戦略は、データダイオードの使用を特徴としており、ホワイトリスティング、攻撃対象領域の削減、認証管理、およびセキュアリモートアクセスが含まれます。DHC は、これらの戦略が非常に重要かつ効果的であること、そしてシステム所有者が戦略を実装すれば 2014 年と 2015 年の 2 年間に ICS-CERT が応酬したインデントの 98 パーセントを防御できるだろうと結論しました。

7 つの戦略で多層防御を実施

最新のサイバー攻撃を防御するには、幾層ものセキュリティが必要です。この多層化アプローチは多層防御と呼ばれます。Owl 社のデータダイオードを基本とする DualDiode 製品は、多くの重要インフラ運営者が多層防御セキュリティアーキテクチャを構築するために使用されています。

Owl 社の DualDiode による全 7 戦略の維持方法

DHS は、全戦略のうち3つにデータダイオードの使用を明確に勧めています。Owl 社の DualDiode ソリューションがどのように全 7 戦略をサポートするのかをご理解いただくために、Owl 社のデータダイオードの能力と本戦略で提供される様々な推奨事例を対応させたマトリックスを作成しました。

しかし、Owl 社の多層防御の構想はこれで終わりではありません。Owl 社の DualDiode 製品がオペレーターによる各戦略の実装をサポートする役割を担うというだけでなく、DualDiode 自体がその多層防御戦略で自分を防御するようにこれらの戦略が組み込まれています。

これらの可能性については、裏表紙に「デュアルダイオードの自己防衛 (DualDiode Self-Defense)」表として掲載されています。

1 DHS 戦略：

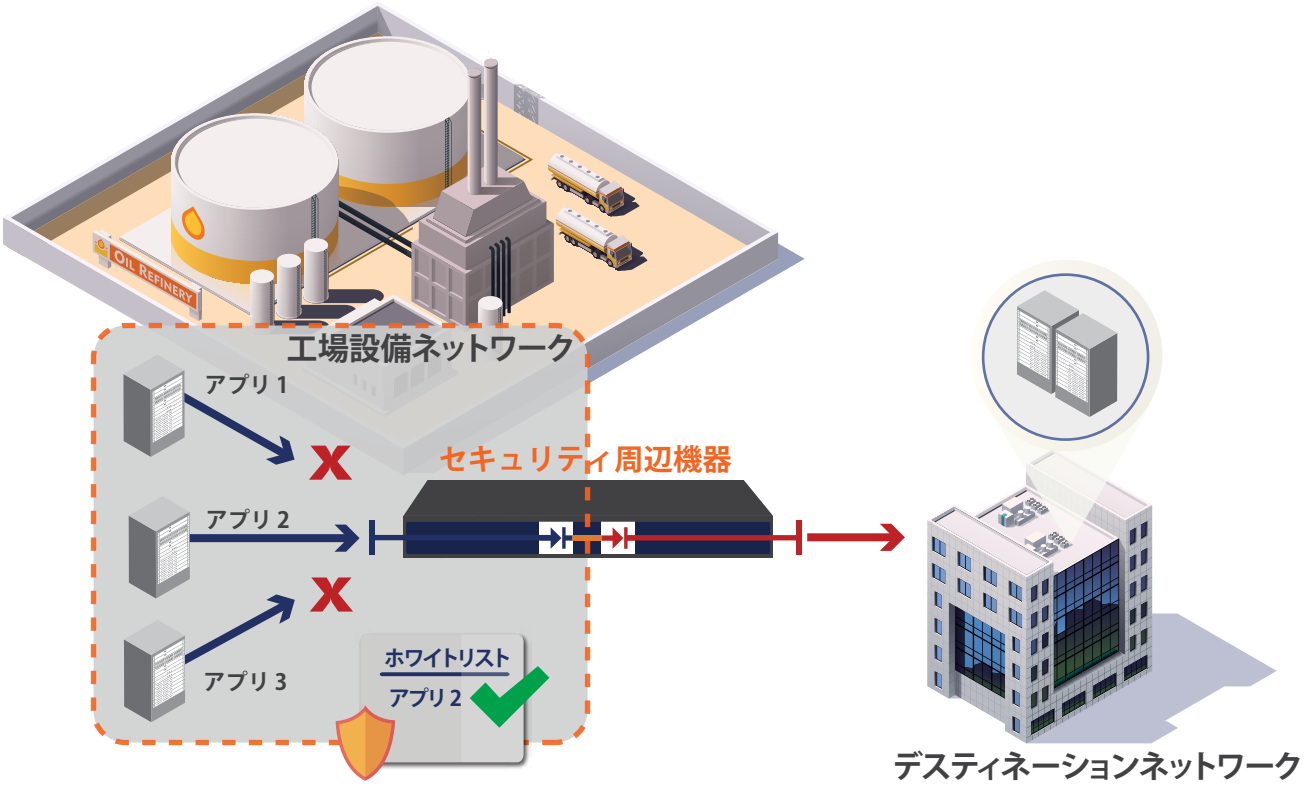
アプリケーションのホワイトリスティング «

実行できるアプリケーションを事前に選択することが可能で、認証されたソフトウェアのみが実行されるため、新たな攻撃を心配する必要はありません。

Owl 社のソリューション

ホワイトリスティングを最優良事例として、Owl 社の DualDiode は既知の「ホワイトリスト記載」のデータソースのデータ以外は受け付けません。データソースは、IP アドレス、ネットワークポート、およびプロトコルの 組み合わせで規定されます。万一、悪意のあるアプリケーションが有効なアウトバウンド IP アドレス、ネットワークポート、およびプロトコルの組み合わせを乗っ取ることができたとしても、相手はこちらの状況をまったく把握できないペアードエンド通信先となり、「phone home通信（帰るコール通信）」を行ったり、ターゲットを選んで攻撃をかけることはできません。

DualDiode には、データダイオードによって物理的に分離された 2 つのマッピングテーブルがあります。ソース側のテーブルは、ホワイトリストに記載されたデータソースを、デスティネーション側への転送用のチャンネルにマッピングします。デスティネーション側では、このチャンネルが真のデスティネーションアドレスにマッピングされます。このアーキテクチャでは、ソース側はデスティネーションがどれかも、どこかも知ることはできません。悪意のあるアプリケーションは、特定のプロトコルのみを使用し、何ら応答を受けずに、不明なエンドポイントと盲目的に通信することしかできないのです。



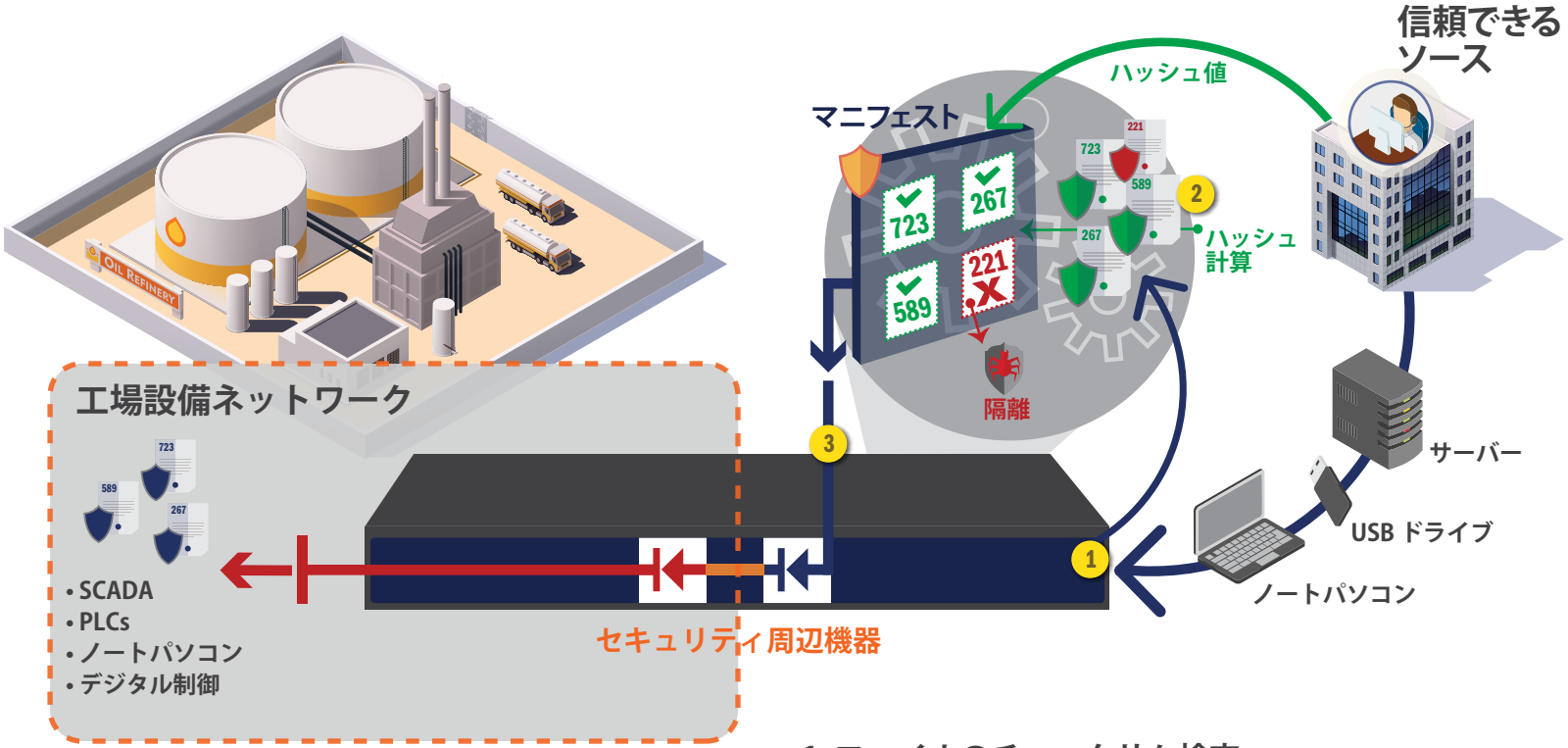
DHS 戦略:

構成/パッチ管理 «

攻撃者は常に弱点や脆弱なポイントを狙います。強化されていないシステムや時代遅れのシステムが狙われます。システムを最新の状態に維持し、制御ネットワークへの外部接続を制限し、認証済みソフトウェアパッチの導入に安全な方法を使用するようにしてください。

Owl 社のソリューション

Owl 社が開発したセキュアソフトウェア更新サービス (Secure Software Update Service、SSUS) は重要インフラの運営者が直面するソフトウェア更新の問題の対策に特化して設計され、運営者がシステムを最新の状態に維持できるようにサポートします。SSUS は、ウィルス感染の可能性があるノートパソコンや携帯型端末を使用するリスクを冒さずに、ソフトウェアパッチの転送と制御センターの更新を安全に実行します。コアデータダイオードは、ネットワークセグメント化セキュリティを提供し、同時にアプリケーションは、ベンダーのセキュアハッシュコードを使用して各ファイルのアイデンティティを検証します。ファイルにはアンチウイルススキャンも実行されます。ファイルに問題が見つかれば隔離され、制御ネットワークへの到達が阻止されます。



1. ファイルのチェックサム検査
2. チェックサムによるマニフェスト照合確認
3. 確認済みファイルは開放され、その他は隔離される

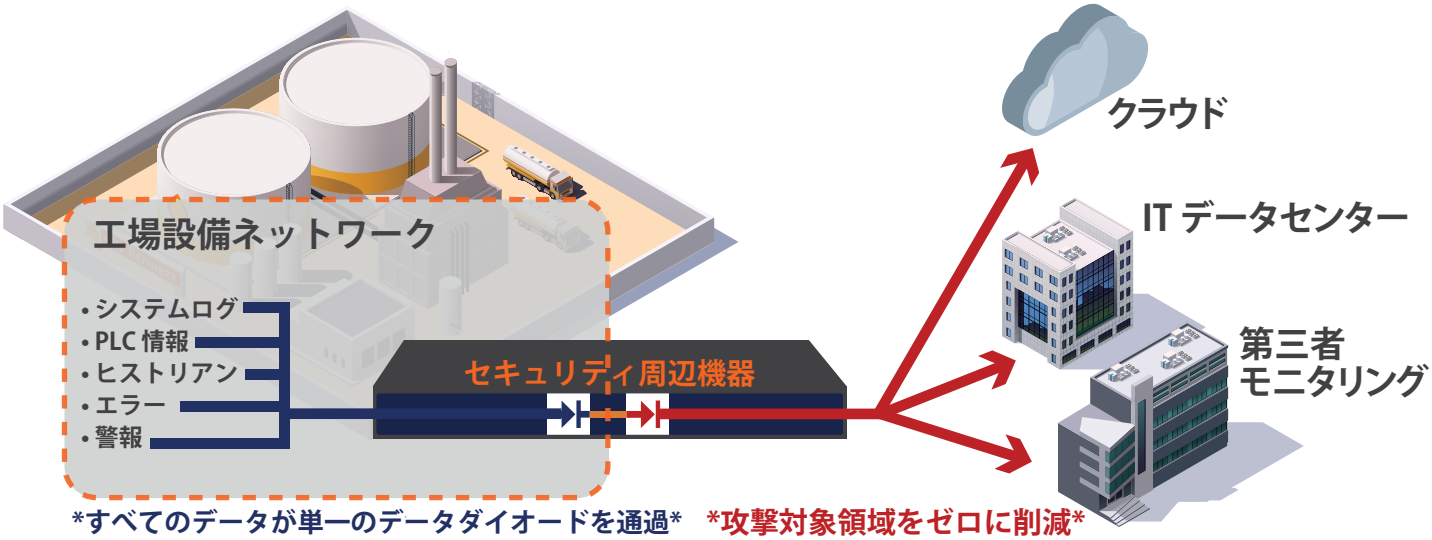
3

DHS 戦略：
攻撃対象領域の削減 «

産業用制御システム (ICS) ネットワークを不審なネットワークから切り離し、使用していないサービスおよびポートをロックダウンし、データダイオードを使用してネットワークのセグメント化を提供し、双方向通信が必要な場合には制限されたパスを経由して単一ポートを使用します。

Owl 社のソリューション

Owl 社の DualDiode はどれも当社独自のデータダイオードの実装に基づいており、ICS ネットワークの分離、サービスのロックダウン、ネットワークセグメントの保護など DHS の推奨事項に対応します。Owl 社のデータダイオードは、その名称のとおり、制限されたパス上の一方向通信のみを許可します。攻撃対象領域を削減するのではなく、一方向通信でゼロにします。Owl 社は、BiLateral と呼ぶ双方向通信双方向通信ソリューションも提供しています。単一の 1UI ボックスに収納された 2 組のデータダイオードが限定的で単一の TCP/IP 接続を提供して、双方向通信を実現します。データダイオードは双方向で使用されるため、一方向通信に提供されている保護層が双方向ソリューションにも適用されます。



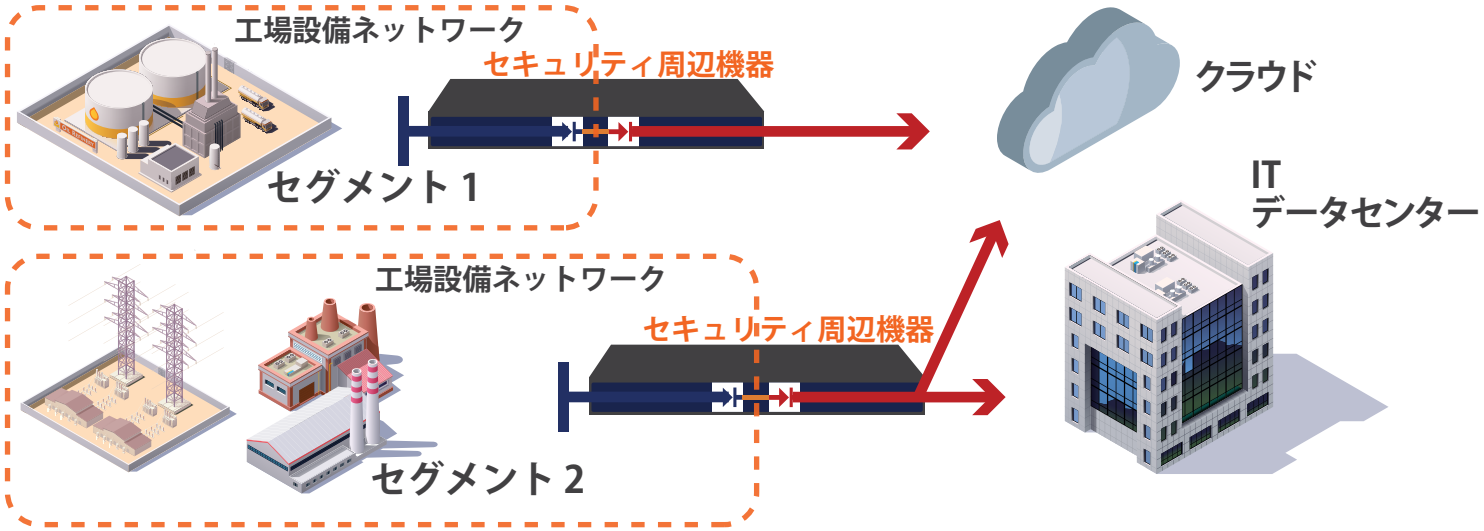
DHS 戦略:

防衛可能な環境を構築する «

ネットワーク周辺への侵入による被害を制限します。ネットワークをセグメント化し、ホスト間のパスを制限して、感染を防止し拡大を封じ込めます。

Owl 社のソリューション

ネットワークのセグメント化を提供することは、一方向通信のみを許可するように特別に設計された Owl 社の DualDiode の本来の目的です。多層防御戦略に沿って、Owl 社は ATM プロトコルを使用してデータダイオード経由でデータを転送し、保護されたネットワークと外部の脅威の間のプロトコルブレークを実現します。これにより、ホスト間のパスを規制し、あるセグメントから別のセグメントに感染が拡散するのを防ぎます。DualDiode は IP ルーティングを行ったり、許可したりせず、どのようなルーティング情報 (IP アドレスなど) も DualDiode を通過できないようにします。



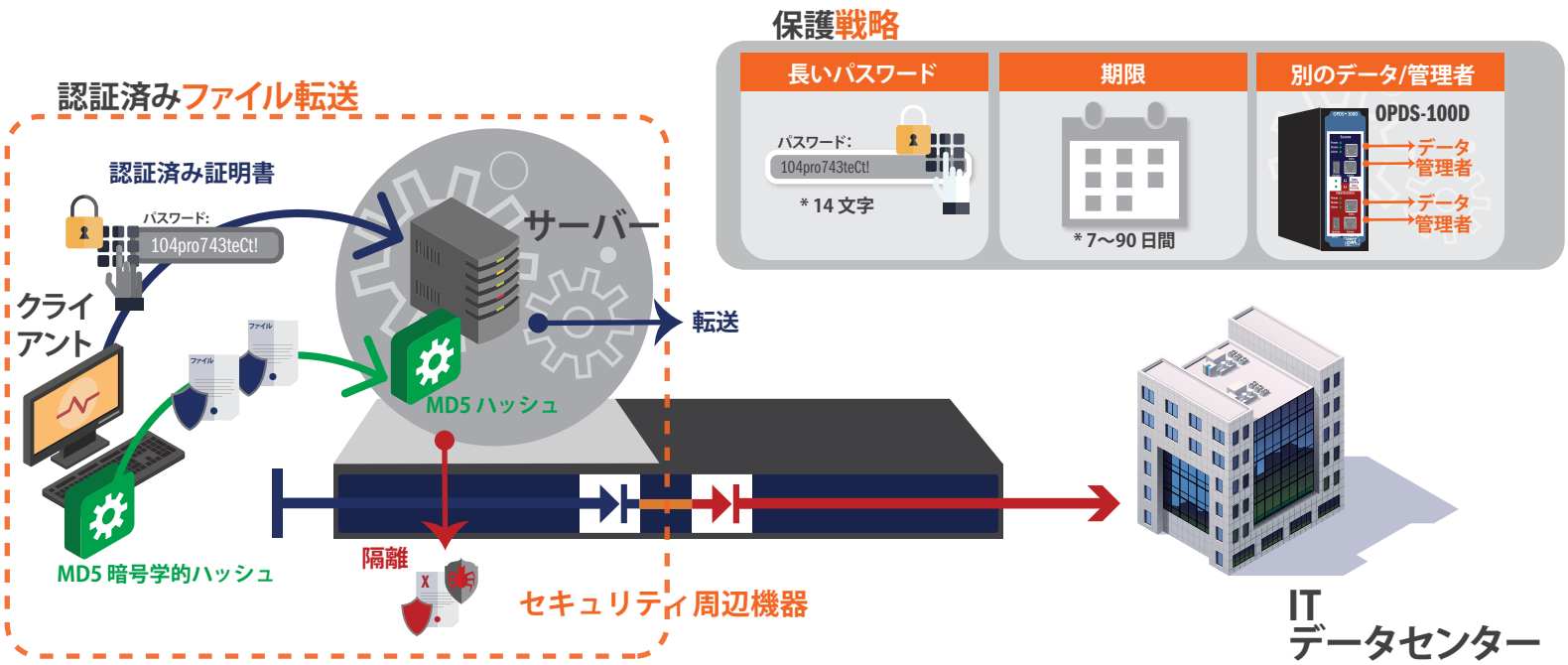
5 DHS 戦略:

認証管理 «

正当なユーザーになりすました攻撃者を防ぎます。複雑で長いパスワードを課し、各ユーザークラスで必要なユーザーのみに権限を縮小し、少なくても 90 日毎にパスワードを変更し、企業 (IT) と制御ネットワーク (OT) ゾーンに対しては別々の証明書を要求します。

Owl 社のソリューション

Owl 社の DualDiode は、長いパスワード、IT と OT ユーザーの分離、パスワードの変更、権限の最小化といった推奨条項を守るだけではなく、転送ファイルの認証も提供します。FTP および NFS のようなプロトコルのさらに安全で強固なバージョンである Owl 社のリモートファイル転送サービス (Remote File Transfer Service、RFTS) を使用することで、クライアント/サーバーアーキテクチャは非認証ファイルが DualDiode を通過しないようにします。クライアントは DualDiode の外部で動き、DualDiode 上で実行するサーバーアプリケーションに登録されます。各クライアントユーザーは、割り当てられたポートでログイン ID とパスワードを使用してサーバーの認証を受けなければ、DualDiode に到達できません。さらにファイルも、クライアント/サーバー間で交換される前後に MD5 を使用して審査を受け、転送キューに待機しているファイルが適正なことを保証します。



DHS 戦略:

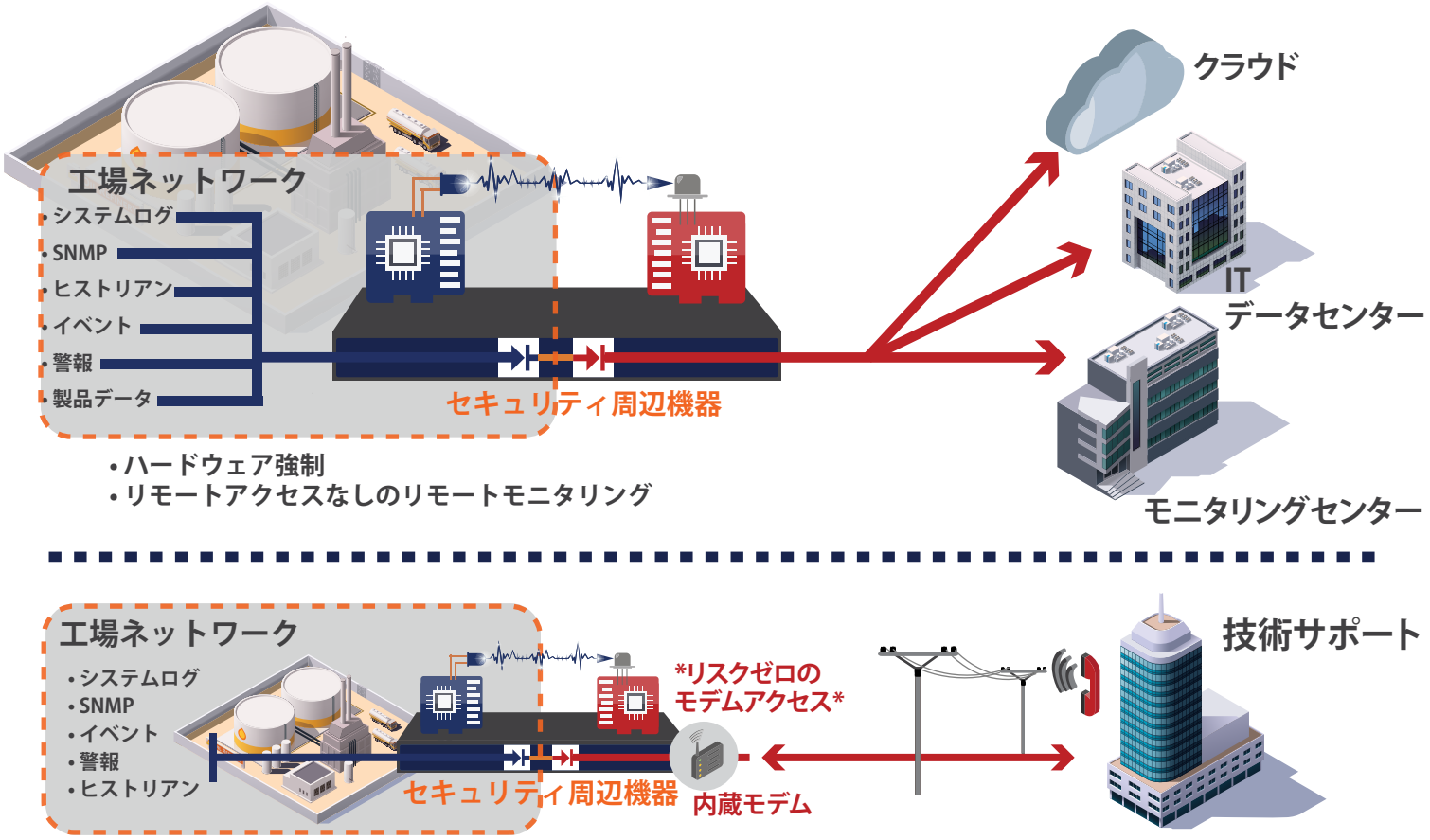
セキュアリモートアクセスを実装する «

バックドアおよびモデムアクセスの排除、モニタリング専用アクセスの実行、データダイオードによる強化、そして「読み取り専用」ソフトウェア構成に依存せず、持続的なリモート接続を許可しません。

Owl 社のソリューション

DHC によるデータダイオード使用推奨に従い、Owl 社の DualDiode はリモートアクセスのリスクを招くことなく安全なリモートモニタリングを容易にするように特別に設計されています。ハードウェアベースのソリューションなので「読み取り専用」ソフトウェア構成に依存しません。バックドアを排除し、モニターが Owl 社のデータダイオードからリモートエンドユーザーまで流れます。遠隔地のエンジニアおよび技術者 は、ほぼリアルタイムにシステムを観察することができ、同時に装置ベンダーは彼らの装置を監視し、集中監視センターからサービスレベルアグリーメント (SLA) を履行できます。モニターデータには、タグ情報、警報、警告、SNMP トラップ、シスログメッセージなどを含めることができます。

モデムは、制御ネットワークにリスクを生じさせる危険がありますが、Owl 社では内蔵モデムモデルを有するデータダイオード製品を提供することでこの問題を解決してきました。制御ネットワークはデータダイオードで保護されていますが、モニターデータはセキュアリモートアクセス経由で利用できるようになっています。データは、私たちの標準的なデータダイオード上の場合と同じ方法でデータダイオードを通って転送されてから、データダイオードの IT 側に格納されます。内蔵モデムは、リモートユーザーが制御ネットワークへのアクセスを一切開放することなくデータを読み込むためにダイヤルインを許可します。



7

DHS 戦略：

監視および応答 «

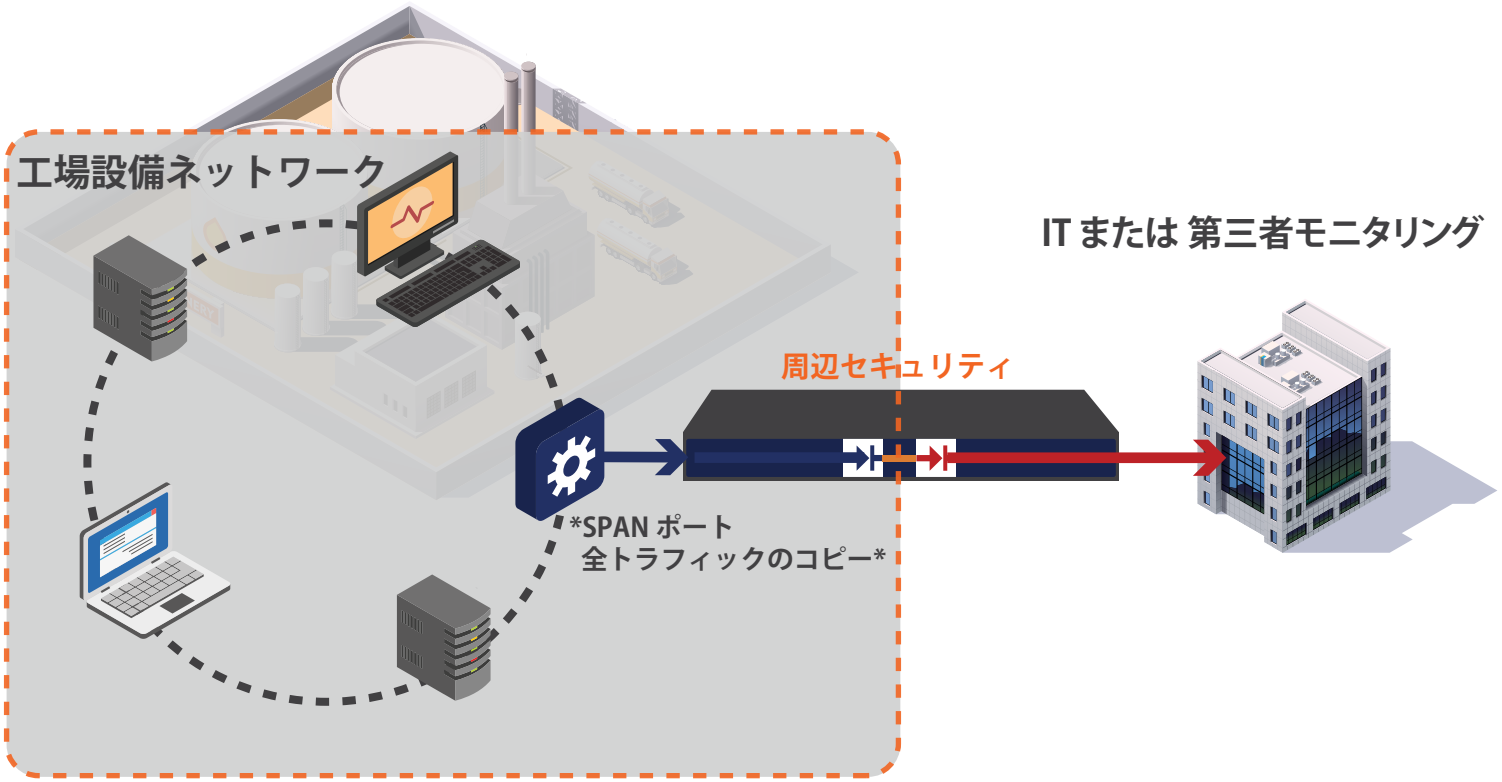
ICS 境界のトラフィックを見て、ICS ネットワーク内のトラフィックを監視し、悪意のあるソフトウェアおよび攻撃を検知する製品を使用し、ログイン分析を実行し、アクセス制御の改ざんを注視します。

Owl 社のソリューション

Owl 社の データダイオードが提供するオプションの 1 つに、分析のためにネットワークトラフィックを外部ネットワークに安全に転送する能力があります。ラインレートトラフィックの 100% がキャプチャされ、別のエンクレーブに転送され、第三者が制御ネットワークにアクセスすることなくネットワーク分析を実行できるようにしています。

Owl 社にはさらに Owl パフォーマンス監視システム (Owl Performance Monitoring System、OPMS) と呼ばれる製品があり、これはリアルタイムな監視、および制御ネットワークとデータダイオード間の全接続の表示と分析を実現します。OPMS は、攻撃を示唆するデータフローの停止や中断があった場合に警告と通知を行います。その他にも、OPMS はシスログファイルおよびイベントの中央収集ポイントとしても機能し、制御ネットワーク内で警報が発せられた場合にキーワードを使用してスタッフに警告します。

OPMS は Owl 社の DualDiode プラットフォーム上で動作するため、攻撃への対応計画として全インターネット接続の切断が含まれている場合でも、稼働を続けます。内部へのネットワーク侵入を許すことなく、引き続き情報を外部関係者に転送できます。



1. 産業制御システムを効果的に守る7つの戦略
https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems

OWL CYBER DEFENSE
1-866-695-3387
WWW.OWLCYBERDEFENSE.COM