FORESCOUT
Active Defense for the Enterprise of Things™

電力業界向けソリューション

電力業界におけるリスク管理の最適化、スピーディーなコンプライアンス対応を支援

電力会社のセキュリティ/オペレーション担当者は毎日、様々なセキュリティツールやダッシュボードから何千件ものアラートを受信します。電力系統の保護に関するサイバーセキュリティの課題は数多くありますが、もっとも困難な課題は以下の3つです。

- 正確な最新版資産インベントリの維持
- アラート分析および平均修復時間(MTTR)の短縮
- 規制要件（北米のNERC CIP基準や欧州のNIS指令などの）へのコンプライアンス対応

2019年の調査では、電力会社の56%が「1年に1回以上、業務データのシャットダウンまたは損失が発生している」と回答しています。[1]

Forescout eyeInspect：電力業界向けのサイバーレジリエンスプラットフォーム

Forescout eyeInspect（旧SilentDefense™）は、パッシブ方式および選択的なアクティブ方式の検知機能を提供します。これにより、リアルタイムの資産インベントリを自動作成すると同時に、特許取得のディープパケットインスペクション(DPI)と異常検知技術を駆使して多岐にわたる脅威から産業用制御システム(ICS)ネットワークを保護します。また、高度なアラート統合機能が関連アラートをグループ化し、人為ミスのないスピーディーなプロセスで脅威分析とインシデント対応を効率化します。

eyeInspectは脅威検知・対応に加え、コンプライアンス監査とポリシー適用タスクの自動化も支援します。資産所有者は、独自のポリシーを設定し、個別デバイスやデバイスグループのベースラインを簡単に作成した後、eyeInspectのアクティブセンサー（オプション機能）でベースラインからの逸脱を自動検知できます。たとえば、ベースライン項目のNERC CIP監査やNIS指令要件への準拠を正式に証明する文書や報告書を簡単に作成できます。

eyeInspectを社内アナリストの希望言語にローカライズされる場合は、12種類の言語からお選びいただけます。資産所有者は、ファイルをドラッグ&ドロップするだけで言語を変換できるため、UIメッセージや日付/数字フォーマットをご希望の言語で閲覧いただけます。

ICSネットワークでのeyeInspectユースケース

素早いアラート分析

ネットワーク上でのトレンドを発見しやすい多次元的アラートグループを作成します。送信元IP、脆弱性の種類、センサーなどの複数の切り口からアラートを分類し、ピボットテーブルのような形で統合します。ユーザーにとって使いやすく強力なアラート統合機能で、業務効率を改善し、アラート分析の工数を削減できます。

OTネットワークのセグメンテーション

eyeInspectは、当社製品eyeSegmentとの連携により、IT/OTドメインにまたがるセグメンテーションポリシーを統合します。OT資産所有者は、変電所のセグメンテーションゾーン構成を、最上位層のクラウド/データセンター環境に合わせて同期化し、既存のトラフィック遠隔計測インフラ（NGFW、スイッチ、SDN、クラウドなど）とシームレスかつ業務の中断なく（エージェントレス方式）で統合できます。これにより、既存投資を有効活用できます。

規制コンプライアンス対応の最適化

eyeInspectは、資産の自動検出、継続監視機能、柔軟な報告書作成機能により、電力業界の各種規制要件（北米のNERC CIP、欧州のNIS指令など）へのコンプライアンス対応の自動化を支援します。eyeInspectをお使いいただくと、以下を実現できます。

- 完全な資産インベントリー一覧の作成（SEL/IP対応デバイスおよびシリアルデバイスを含む）
- ホストポートとサービスの変更監視
- BESフィールドデバイス（リレー、RTUその他）のフィールドポートとサービススキャンの自動化
- すべての通信経路を可視化し、デバイスとネットワークをリアルタイムで監視
- WindowsのOTデバイスすべてにインストールされたパッチ/アプリケーションの識別

リスク管理およびNERC CIP準拠対応の効率化

電力会社は、これまで以上にリスク管理とコンプライアンス監査タスクを効率化することが求められています。Forescoutは、以下の領域におけるリスク管理とNERC CIP要件対応を支援します。

- 資産のベースライン作成
- BES（基幹系統）サイバーシステム分類
- セキュリティ管理の統制
- 要員およびトレーニング
- 電子的セキュリティ境界
- BESサイバーシステムの物理セキュリティ
- システムセキュリティ管理
- インシデント報告/対応計画
- BESサイバーシステムの復旧計画
- 設定変更管理と脆弱性評価

リスクの検知および管理

eyeInspectは、何千種類もの侵害の痕跡(IoC)を伴うネットワーク通信を常時監視することで、サイバー、オペレーション両面の脅威を検知し、優先順位付けします。当社独自のユーザーインターフェースと資産マップで、脅威の発生元および水平移動の経路を特定すると同時に、関連アラートと脅威をひも付けして集約し、詳細な復旧計画やアクションに結びつけることができます。資産所有者やアナリストはeyeInspectをピボットテーブルのように活用し、素早くドリルダウン/スケールアップできるため、セグメンテーションとポリシーアクションと合わせてインシデントの全体像を捉え、対応できます。エンタープライズコマンドセンター(ECC)経由で、マルチサイトや遠隔地域に分散するネットワークから発信されたアラートにズームインできるため、より一層のスケーラビリティを実現できます。

eyeInspectには、以下をはじめとする幅広いリスク管理・監視機能が搭載されています。

- 資産または資産グループ別のベースライン作成
- SEL/IP対応およびシリアルデバイスへのアクティブクエリー
- 高度なアラート統合による自動修復
- 150以上のプロトコルに対応する特許取得ディープパケットインスペクション(DPI)
- デバイスの脆弱性、脅威へのエクスポージャー、ネットワークやオペレーションの問題を自動で評価

多要素ベースの脅威検知

eyeInspectは、本資料で解説するすべての要素と個別データポイントを統合し、ネットワーク資産別にセキュリティリスク/オペレーショナルリスクの一元的スコアを生成可能な、これまでにないOTネットワーク監視ソリューションです。このリスクスコアをもとに、修復アクションの特定および優先付けを一貫した方法で実施できます。eyeInspectはサイバー、オペレーション両面におけるあらゆる種類の脅威（以下に例示）を特定し、修復を支援します。

- サイバー攻撃（DDoS、MITM、スキャン攻撃など）
- 無許可のネットワーク接続や通信
- 疑わしいユーザー挙動/ポリシー変更
- デバイスの機能不全/設定不備
- 無応答の新規資産
- 不正な形式のプロトコルメッセージによるエクスプロイト
- 不正なファームウェアのダウンロード
- 安全でないプロトコルの使用
- デフォルトの認証情報、安全性に問題のある認証
- ロジックの変更
- IP対応デバイスおよびシリアルデバイスの可視化

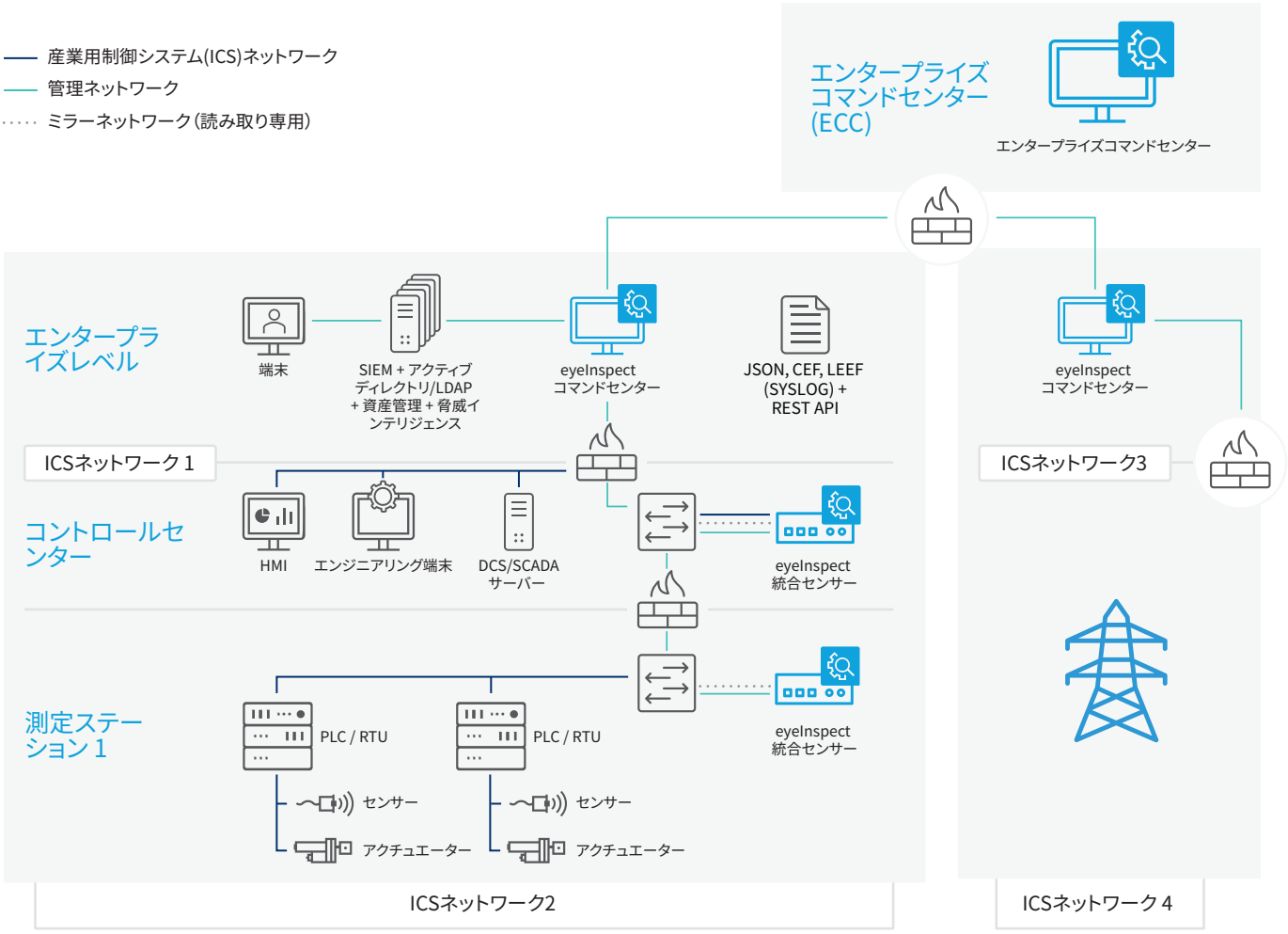

図1：eyeInspectは、拡張エンタープライズ環境全体でのサイバーリスクとオペレーショナルリスクに関する状況認識および自動統制を実施するForescoutのIT/OT一体型セキュリティプラットフォームの一部です。

1. https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa version:1572434569/siemens-cybersecurity.pdf

Don't just see it. Secure it.™

EoT(Enterprise of Things)のアクティブ防御を支援します。今すぐお問合わせください。

forescout.com/platform/eyeInspect　japan-sales@forescout.com　電話番号: 81 50-1746-6455

FORESCOUT
Active Defense for the Enterprise of Things™

〒101-0051
フォアスカウト・テクノロジ ーズ株式会社
東京都千代田区神田神保町2-11-15
住友商事神保町ビル2階

詳細はForescout.jpをご覧ください