FORESCOUT
Active Defense for the Enterprise of Things™

OTのサイバーセキュリティとリスク管理

産業用制御システムとOT環境におけるリスク低減、コンプライアンスの自動設定、脅威分析の最適化

情報セキュリティ(IT)と オペレーショナルテクノロジー(OT)ネットワークの融合が進み、これまで隔離されていた産業用制御システム(ICS)ネットワーク上の複雑性や脆弱性が増しています。同時に、産業用IoT (IIoT)デバイスが爆発的に増え、大規模な可視性ギャップ、複雑なコンプライアンス設定などの問題が発生しています。組織はOTとICSネットワークを細部まで可視化し、オペレーショナルリスク/サイバーリスクを有効かつリアルタイムで管理可能なセキュリティツールを求めています。

OT環境における主な課題

インフラの更新、新技術の採用、OT/ITネットワークの一体化が進む組織環境では、異種混合のモダンネットワーク上の脆弱なOTや産業用制御システムを適切に維持し、保護する必要があります。このため、セキュリティ/運用部門は以下のような課題に直面しています。

- 管理対象/対象外を問わず、接続するすべてのITデバイス、IIoTシステム、OT資産を識別・分類し、コントロール
- 業務への支障を最小化しつつ、アラートの分析、脅威の優先付け、インシデント対応を迅速に実施
- レガシーOTシステムを含むすべての接続デバイスによる規制要件やポリシー順守の徹底
- 正確な、最新版資産インベントリの維持

「2021年までに、産業用IoT(IIoT)プロジェクトの80%にOT固有のセキュリティ要件が発生するだろう。」[1]

ガートナー社

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

Forescout eyeInspect：IIoT、OTインフラのサイバーレジリエンスとリスク管理

Forescout eyeInspect（旧SilentDefense™）は、多岐にわたる脅威からOT/ICSネットワークを保護し、パッシブ・アクティブ検知手法を駆使してリアルタイムの資産インベントリを自動作成します。さらに、業務への潜在的影響をもとに修復アクションを局所的に実施します。

- パッシブ方式によるネットワークのリアルタイム監視とセグメンテーション
- 高度なアラート統合機能による脅威分析の最適化および脅威の修復
- ServiceNow®との緊密な統合およびSIEMソリューション、ファイアウォール、IT資産管理、サンドボックス、認証サービスとのネイティブ連携
- アセットリスクフレームワークによるリスク分析の自動化で、SOCとアナリストの効率を改善
- Forescoutプラットフォームが提供する卓越したデバイス可視化、分類、プロファイリング機能をクラウドからエッジデバイスまで、広範囲に拡張

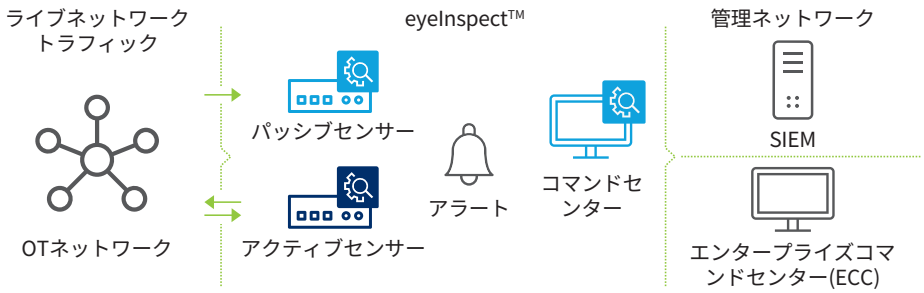

図1：eyeInspectの基本構成

eyeInspectのユースケース

資産の可視化および監視

eyeInspectはOTネットワークやサイト全体で資産を常時可視化します。豊富な資産情報およびネットワーク/役割別の自動分類にもとづく詳細ネットワーク図を自動作成し、Purdueレベルや接続関係など複数の切り口で表示します。eyeInspectは、以下をはじめとする様々な検知機能を活用しています。

- 150種類以上のIT/OTプロトコルに対応する特許取得済みのディープパケットインスペクション(DPI)
- ポリシーと挙動の継続的監視（自由に設定可能）

完全な可視化および脅威検知

eyeInspectは、業界先端のForescoutプラットフォームのデバイス可視化、分類、プロファイリング機能を、OT/ICS環境の細部まで拡張します。以下をはじめとするサイバーおよび運用上のあらゆる脅威を特定し、効果的に修復します。

- サイバー攻撃（DDoS、MITM、スキャンによる攻撃など）
- 無許可のネットワーク接続、通信
- 不正が疑われるユーザーの挙動/ポリシー変更
- デバイスの機能不全や設定不備
- 応答不全の新規資産
- メッセージの破損
- 無許可のファームウェアによるダウンロードや安全でないプロトコル
- デフォルトのログイン情報、安全性に欠ける認証
- ロジックの変更
- IP対応およびシリアルデバイスの可視化

- デバイスの脆弱性、脅威へのエクスポージャー、ネットワークや運用の問題を自動評価
- 特定ホストへの選択的クエリを業務の中断なく実行できるアクティブコンポーネント（オプション）

資産の構成管理

eyeInspectは多岐にわたるOTの資産情報を自動収集し、セキュリティや運用のフォレンジック分析に必要な構成変更をすべてログに記録します。以下は、検知可能な詳細項目の一例です。

- ネットワークアドレス
- ホスト名
- 資産のベンダー名、機種
- シリアル番号
- OSのバージョン
- ファームウェアのバージョン
- ハードウェアのバージョン
- デバイスモジュール情報

コンプライアンス設定の自動化

資産所有者はeyeInspectのアクティブセンサー経由で、個々のコンプライアンスポリシーをもとに資産や資産グループのベースラインを簡単に設定し、逸脱項目を自動検知できます。また、ベースラインをもとに、組織の要件または、NERC CIP、ISA99/IEC 62443、NIS、NIST CSF、FDA、FIPSなどのコンプライアンスガイドラインに準じたカスタムポリシーを定義することもできます。これらのコンプライアンスフレームワークのベースラインに関する正式な証明書／報告書を作成することも可能です。

ネットワークアクセスコントロールとセグメンテーション

eyeInspectは、ForescoutプラットフォームのACLとVLAN割り当て機能を活用し、オペレーショナルネットワーク上でポリシーベースのセグメンテーションとアクセス制御を実施します。これによりIT、IoT、OT環境全体で統合されたリアルタイムの資産管理をサポートします。

資産所有者はIT、OT、ヘルスケア環境にまたがる各資産の関係性（通信パターン）に関するコンテキスト認識型（プロトコル認識/DPI）マップと可視化情報を入手し、既存のトラフィックフロー遠隔測定システム/製品（Medigate、NetFlow、SPANなど）と統合できます。

OTのサイバーレジリエンスによる純利益の改善

Forescout eyeInspectはオペレーショナルシステムのセキュリティとレジリエンスを改善すると共に、管理者の業務やリスク管理、コンプライアンス対応を大幅に効率化することで、純利益の改善を支援します。

当社は最近、米国の大手食品メーカー（産業用制御システムのサイバーセキュリティ・コンプライアンスの担当者：フルタイム換算で17名規模）を対象に、OTネットワーク監視による財務効果を調査しました。結果は以下のとおりです。

- 資産やネットワーク可視化における人件費削減、管理業務の生産性アップ、脅威ハンティングの機能強化による年間のコスト節減効果：$820,336
- 実用的な脅威管理の最新情報、インシデント対応の迅速化、ダウンタイムリスクの低減など、サイバー脅威の検知・対応機能の強化による年間節減額：$346,456
- 産業用制御システムや資産管理ソリューションとの統合（連携機能のビルトイン）による、コンプライアンス費用の年間節減額：$158,120

脅威検知とインシデント対応

eyeInspectのアラート調査・対応ツールで、脅威の検知、封じ込め、修復を自動化し、ダッシュボードとウィジェットでユーザーのコラボレーションを強化できます。きめ細かいアラート情報で根本原因の分析をサポートし、効果的/効率的な対応を促進します。また、エンタープライズコマンドセンター（ECC）経由で、複数サイトや複数地域にまたがるネットワーク上の個別アラートに焦点を当て、アラート対象デバイスやコンテキストを含むインシデントの詳細を分析できます。

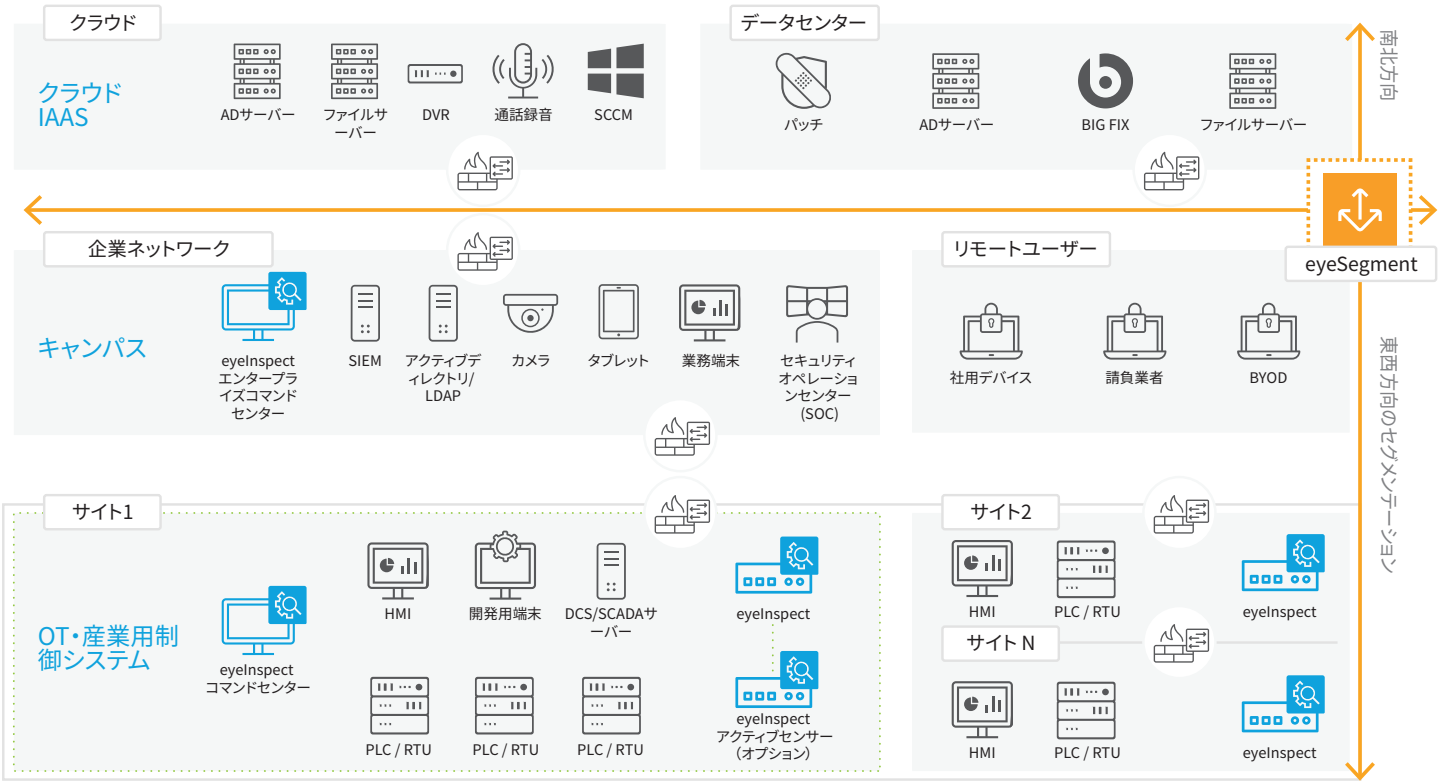

図2：eyeInspectは、拡張エンタープライズ環境全体のサイバーリスクとオペレーショナルリスクの状況認識および自動コントロール機能を提供するForescoutのIT/OT一体型セキュリティプラットフォームの一部です。

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。

1. Gartner社Saniye Alaybeyiによる2018年の調査「7 Questions SRM Leaders Aren't Asking OT Security Providers During Technology Selection」https://www.forescout.com/gartner-report-7-questions-for-OT- security-providers
2. 標準的な顧客データにもとづく予測。実際の節減効果は、様々な要因によりこの数字と は異なる場合があります。

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