FORESCOUT
Active Defense for the Enterprise of Things™

製造業向けソリューション

産業用Internet of Things(IIoT)のサイバーセキュリティおよびリスク管理

近年、サイバーフィジカルシステムの普及により、これまで以上にフラットな異種混合ネットワークが出現しています。これにより、製造現場は増大するリスクに対応しつつ業務を運用し、コントロールや修復が困難なサイバーインシデントに立ち向かわなければいけません。

製造業のネットワーク保護に関する多くの課題のうち、最も困難なものは以下の3つです。

- リアルタイムでのネットワーク可視化
- プロアクティブなサイバーリスクの評価・管理
- ネットワークやオペレーションにおける問題の特定

適切なOT（オペレーショナルテクノロジー）ネットワーク監視ソリューションを導入することで、製造業が直面する上記すべての課題解決を促進できます。

「2021年までに、OTセキュリティ管理業務の70%が、CIOまたはCISOの直轄になるだろう。（現状より35%増加）」[1]

GARTNER社

製造業向けのサイバーレジリエンスプラットフォーム：eyeInspect

Forescout eyeInspect（旧SilentDefense™）は、産業用ネットワークを完全に可視化すると同時に、多岐にわたる脅威から保護するOTネットワーク監視ソリューションです。

eyeInspectは、特許取得のディープパケットインスペクション(DPI)と異常検知技術を併用し、数千種類にのぼるIoC（侵害痕跡）のライブラリを搭載しています。高度なサイバー攻撃、ネットワーク構成の不備、運用ミスを検知する各種技術を結集し、未知/既知の脅威検知を支援します。

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

リアルタイムのネットワーク図、ネットワーク可視化、通信状態の分析を提供するグラフィックインターフェース経由で、資産同士の通信状況やホストの挙動変更を完全に把握できます。eyeInspectはネットワーク通信を常時監視・分析し、適正オペレーションのベースラインおよび当社独自の脅威ライブラリで定義された「悪意ある既知の」特性と照合することで、サイバー/オペレーションにおける脅威をリアルタイムで特定し、報告します。

製造業ネットワークにおけるeyeInspectのユースケース

ネットワークをリアルアイムで可視化

eyeInspectは、産業用制御システム(ICS)ネットワーク全体の多岐にわたるOTデバイス情報をパッシブ方式（または選択的アクティブ方式）で収集し、常に最新の資産インベントリを提供します。

以下は検知可能な詳細情報の一例です。

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

eyeInspectは、バックプレーンモジュール、シリアルデバイス、資産の設定変更についても完全に可視化すると同時に、セキュリティ分析やフォレンジック業務に必要な変更ログを作成します。また、デバイスの詳細情報、各資産のベースライン、通信状況のビジュアル表示、ネットワークやロール単位での自動分類を反映した詳細ネットワーク図を自動作成します。分類については、パデューモデルでのレベルや接続関係その他の切り口に対応します。eyeInspectのアクティブ方式技術「ICSパトロール」は、ネットワーク上の特定ホストに対する局所的クエリーを安全に実行し、資産情報の粒度をさらに高めます。

サイバーリスクをプロアクティブに管理

多くのネットワーク監視ツールでは、リスクファクターを個別に把握することしかできません。eyeInspectは、複数のリスクファクターと個別データポイントを自動評価し、各資産のセキュリティリスクとオペレーショナルリスクの度合いをスコア化できる初のソリューションです。

EYEINSPECTによる脅威インテリジェンス

急速に進化する脅威トレンドに後れを取らないためには、新たな検知シグネチャ、検知アルゴリズムを素早く反映できるセキュリティソリューションが必要です。eyeInspectは、実用的な脅威インテリジェンスを様々な方法で提供します。以下はその一例です。

- パッシブ方式によるネットワークのリアルタイム監視およびOT/IIoTネットワークのセグメンテーション
- アクティブセンサー（業務を停止する事ないアクティブ方式技術）で、資産を細部にわたり可視化
- ServiceNowとの緊密な統合連携による、IT/OT環境のDevOps業務とセキュリティ戦略の効率化
- 高度なアラート統合機能で、脅威分析と修復を最適化
- 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とアナリストの生産性を改善
- Forescoutプラットフォームによ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展開

セキュリティアナリストはリスクスコアをもとに、攻撃発生リスクの高い資産および、「潜在攻撃が進行中」という実証のある資産をただちに特定できます。リスクスコアをドリルダウンして高リスクの原因を把握し、対応策を検討することもできます。

eyeInspectはシグネチャおよび振る舞い検知技術、特許取得の異常検知技術をもとに、既知/未知の脅威を、初期段階から実際のエクスプロイト発生段階までにわたって検知します。以下は、製造現場でeyeInspectが検知した脅威の一部です。

- L2サーバーとフィールドロボットの通信により、外部サーバーからファームウェアがダウンロードされた
- 不完全なセグメンテーションにより、脆弱なデバイスがインターネット環境に露出している
- WannaCryに類似したマルウェアが工場内に混入した
- デフォルトパスワードが慢性的に使用されている

eyeInspectの双方向型マップで、インシデント発生元と拡散先を特定できます。また、パケットキャプチャ(PCAP)が提供するデータを根本原因分析に活用することで、対応をスピードアップできます。

ネットワークおよびオペレーションの問題を特定

ネットワークやオペレーションのトラブルは随時発生しますが、大規模なシステムダウンを引き起こす前に食い止めることは可能です。OT技術者は前述のオペレーショナルリスクスコアをもとに、緊急対応が必要な資産（設定不備や機能不全の兆候があり、予期せぬダウンタイムを招く恐れがあるデバイスなど）を素早く特定できます。また、高度なアラート統合機能を使うと、発生原因および緊急度をもとに脅威をひもづけできます。

以下は、実際に特定された脅威の一例です。

- 安全でないプロトコルの使用
- ルーティング/ゲートウェイの問題
- 準拠違反のフォーマットによるデータ送信
- フィールドデバイス接続時の問題
- 重要デバイスの障害
- プロセス値のばらつき
- プロセス測定の誤り
- スイッチ/デバイスの設定不備

多要素ベースの脅威検知

OTネットワーク監視ツールには、ユーザーやアナリストが既知/未知の脅威をできる限り早期に検知し、迅速な対応・緩和策を実行できる機能が必要です。eyeInspectは、シグネチャおよび振る舞い検知技術、特許取得の異常検知技術を組み合わせ、初期段階（発見フェーズ）から実際のエクスプロイト発生段階までにわたり、重要デバイスに影響を及ぼす設定不備などの既知/未知の脅威を検知します。

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
- デバイスの機能不全/設定不備
- 無応答の新規資産
- 不正な形式のメッセージによるエクスプロイト未遂
- 無許可のファームウェア・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、安全制に問題がある認証
- PLCロジックの変更

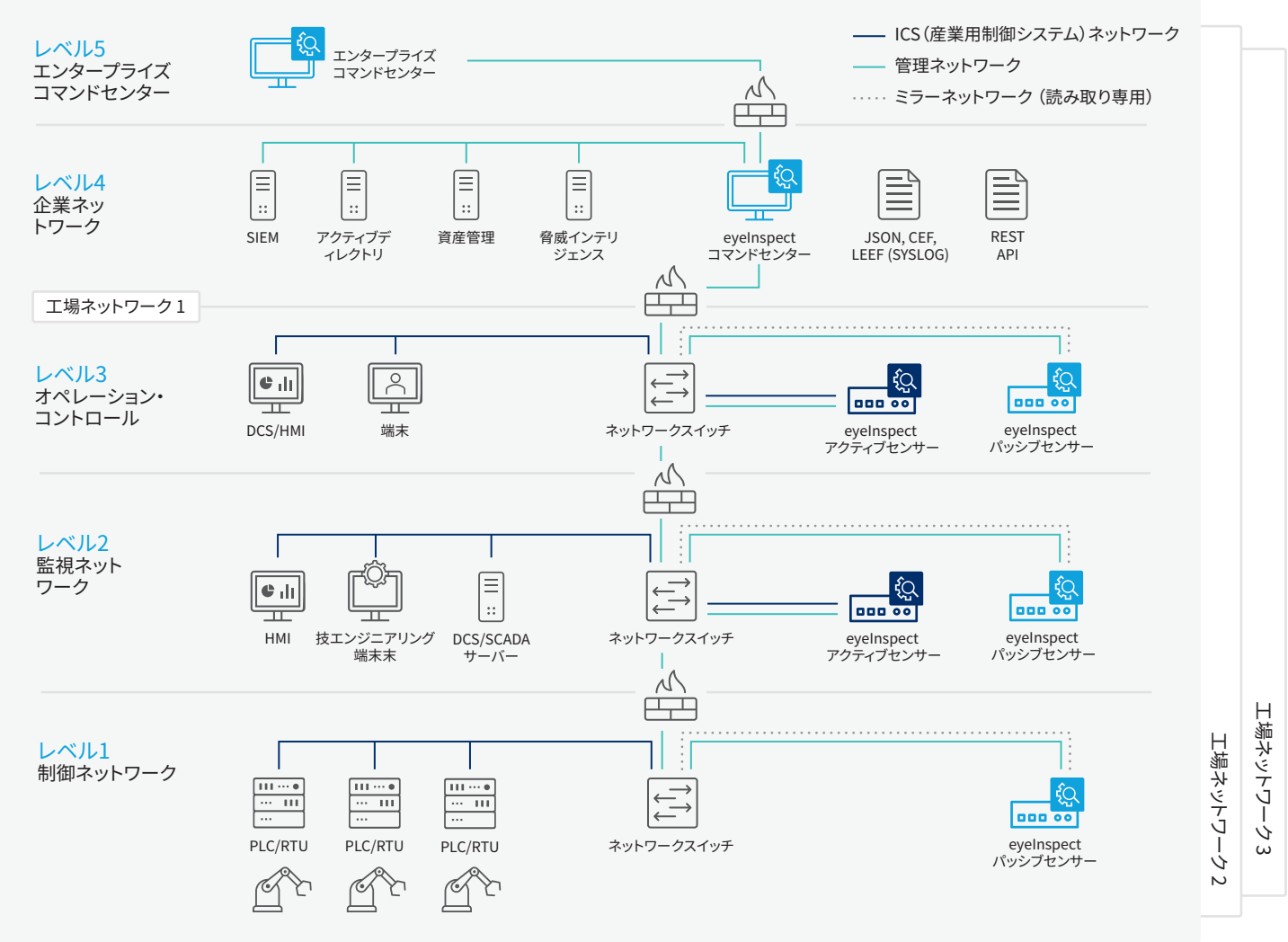

図1：eyeInspectは、拡張エンタープライズ環境全体でサイバーリスクとオペレーショナルリスクに関する状況認識および自動統制を実施するForescoutのIT/OT一体型セキュリティプラットフォームの一部です。

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著「7 Questions SRM Leaders Aren’t Asking OT Security Providers During Technology Selection」https://www.forescout.com/platform/operational-technology/gartner-report-7- questions-for-ot-security-providers/

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