

# アクティブ手法を選択的に適用し、OT全体を可視化

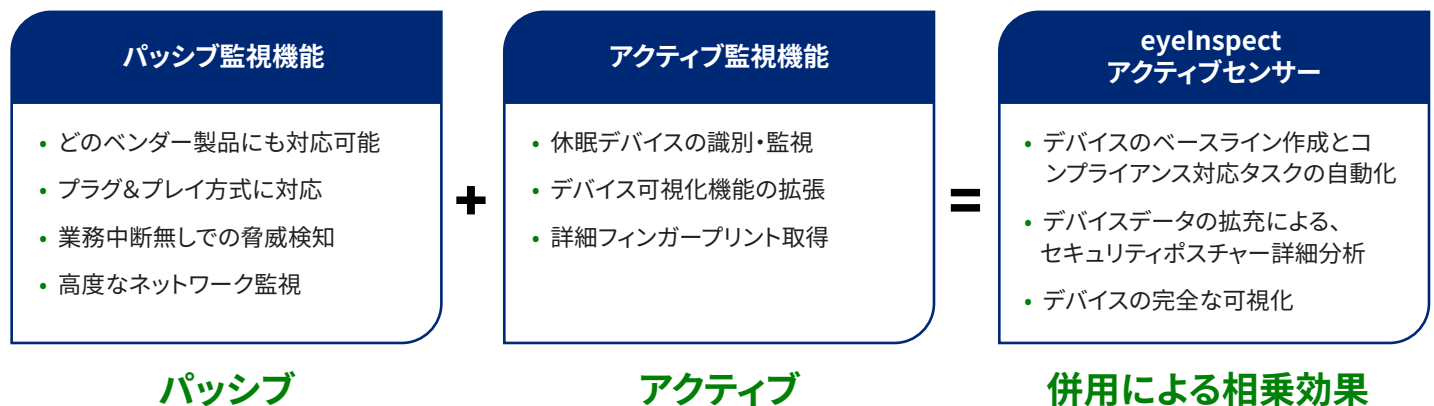
コンプライアンス対応タスクを大規模・自動展開し  
準拠違反とコストを低減

オペレーショナルテクノロジー(OT)のサイバーセキュリティ対応関係者や産業用制御システム(ICS)の資産所有者が管理するネットワークには、完全なパッシブ型サイバーセキュリティソリューションだけでは把握できない死角があるかもしれません。資産情報やデバイス可視化が不十分だと、ネットワークがさらされるサイバーリスク、オペレーショナルリスクのレベルが高まります。

OT資産所有者は、eyeInspectのアクティブセンサーが提供するデバイスのコンテキストデータをもとに、脅威分析を簡略化できます。無駄のないダッシュボードに実用的なアラートが満載されているため、脅威分析および大規模環境でのコンプライアンス対応を効率化できます。

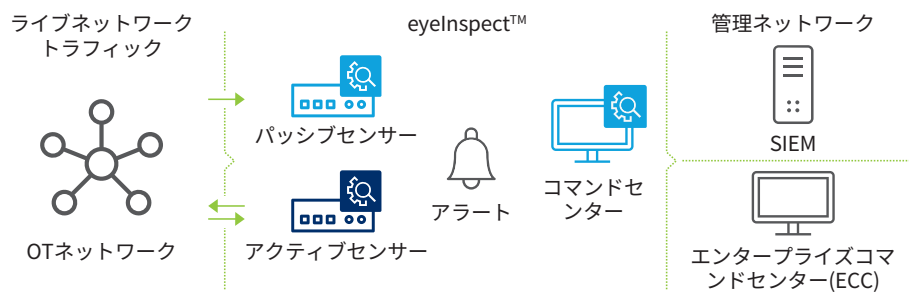
**SCADA/ICSネットワークを展開する組織の79%が、過去24か月以内に侵害の被害を受けています。<sup>1</sup>**

**FORRESTER社**



## eyeInspect アクティブセンサー:すべてを可視化

eyeInspect (旧SilentDefense™) のアクティブセンサーは、パッシブ方式の異常検知とアクティブ方式のサイバーセキュリティ機能を一体化し、ICSネットワークの可視化と運用インテリジェンスをエンタープライズ環境全体に業務を中断する事なく展開します。eyeInspectのオプション機能である「アクティブセンサー」は、ひとつまたは複数の資産インベントリの特徴をもとに、特定ホストへのクエリーを選択的に実行します。資産のベースライン作成機能を備えた可視化レイヤーが追加されることで、コンプライアンス監視や報告プロセスの大幅な効率化にもつながります。



eyeInspect アクティブセンサーの実装例

### eyeInspect アクティブセンサー

- 資産や資産グループをコンプライアンスポリシーと照合のうえ、ベースラインを作成し、コンプライアンスチェックを自動またはオンデマンドで実施
- NERC CIPその他のコンプライアンスフレームワークに対する準拠チェックと報告書作成を自動化
- 詳細な資産インベントリとデバイスフィンガープリント情報を提供 (インストール済パッチ/アプリ、オープンポート/サービスなど)
- OT/ICSネットワークの状況認識をさらに高度化
- アクティブセンサーのOT専用スキャンポリシーで、繊細な設備機器を保護

## アクティブセンサーのユースケース

### デバイスとネットワークのあらゆる対象物を検知

eyeInspectのアクティブセンサーは、ICSネットワークの特定ホストに対する選択的クエリーを安全に実行します。これにより、資産の可視性を高め、より包括的なインベントリ (ホストステータス、OSバージョン、メーカー名、ソフト/アプリ名、シリアル番号、ネットワークユーザーの挙動、インストール済パッチその他の情報) を提供します。

### リスクと脆弱性を包括的に評価

資産情報を業務を中断する事なく、かつ自動で収集するため、サイバーセキュリティ対応関係者は、リスクや潜在的脆弱性をさらに細かい粒度で評価できます。eyeInspectのアクティブセンサーは、パッシブ型ソリューションだけでは見過ごされる恐れがある貴重なコンテキストデータを提供し、アラートの詳細情報を補完します。

## 資産のベースライン作成およびコンプライアンス対応の自動化

eyeInspectのアクティブセンサーをもとに、資産や資産グループのベースラインを作成し、それぞれのベースラインを規制ポリシー（NERC CIP 007、010その他）やコンプライアンス施策と照合し、状況を評価することができます。また、データ一式を選択的にエクスポートし、ネットワーク状態に関する定期報告を簡単に作成可能なため、運用コストの低減および、NERC CIP基準やNIS指令などへの準拠違反による罰金発生リスクの低減を図れます。

1. Forrester社による2018年の調査 - 「Protecting Industrial Control Systems And Critical Infrastructure From Attack」

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。今すぐお問い合わせください。

forescout.com/platform/eyeInspect

japan-sales@forescout.com

電話番号: 81 50-1746-6455