

## 産業制御システム向けセキュリティ対策

ForeScout

## eyeInspect (旧名 : SilentDefense)

eyeInspectは、産業制御システムの資産・ネットワーク構成・脆弱性を可視化し、サイバー攻撃を検知することで重要システムを守ります。

## 産業制御システムにもセキュリティ対策を！

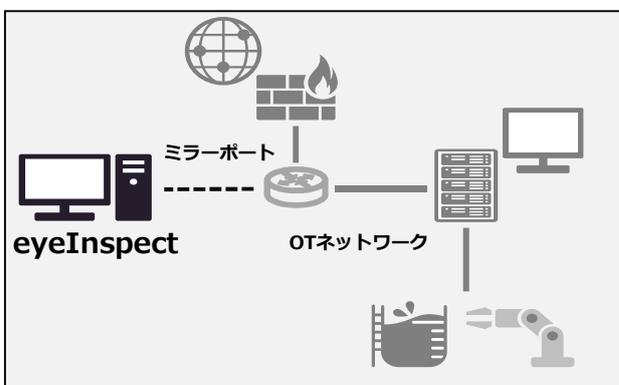
工場やプラントなどのデジタル化を推進するため、産業制御システムと情報システムの融合が進んでいます。これに伴い、産業制御システムもサイバー攻撃の脅威にさらされ、被害が増加しています。重要なシステムや資産を守るための対策が求められています。

## eyeInspectなら簡単に効果的なセキュリティ対策が導入可能

eyeInspectは24時間365日、安定稼働させることが重要な産業制御システムの特徴に合わせた設計でセキュリティ対策を実現します。

## パッシブ構成

ミラーポートからの受信で動作するため、産業制御システムに影響なく導入できます。



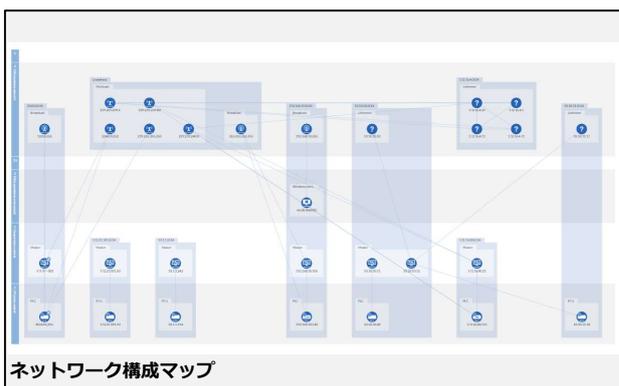
## アセット管理

資産の自動検出に加え、制御機器・端末それぞれの脆弱性も表示可能です。

IP address	Host MAC address	Operational Risk	Security Level
10.10.10.20	005C29CA...	PLC	Unknown
10.10.10.21	005C29CC...	Unknown	Fair
10.10.11.17		Host 10.10.11.1	Unknown
10.10.11.30		Unknown	Unknown
10.205.255...		Unknown	Unknown
100.1.1.1		Unknown	Unknown
100.1.1.11		Unknown	Unknown
100.1.1.20	mac-jk-10020	Unknown	Unknown
100.1.1.255		Unknown	Unknown
199.254.134...		Unknown	Unknown

## ネットワーク可視化

制御機器の役割でグループ分けしたりPurdueモデルに合わせて可視化できます。



## 脅威検知

制御機器向けの脅威データベースを内蔵し、産業制御システムを狙った攻撃を検知します。

Name	Database ID	Synchronization status
OT Database	1140	All entries synced
Discovered IP address	3864	All entries synced
OTD engine for discovered events	62	All entries synced
Discovered IP operation	107	All entries synced
Discovered OS class	419	All entries synced
Discovered OS version	419	All entries synced
Network file hashes	208	All entries synced
NTLM hashes	39	All entries synced

ネットワーク構成マップ

検知した脅威情報

## 豊富なセキュリティ機能でサイバー攻撃をリアルタイム検知

eyeInspectは、以下5つの手法を組み合わせることで脅威の検知を行います。既知の攻撃手法のほか、お客様ネットワークの使用状況を定義または学習して異常を検知することが可能です。加えて、SD Script機能によりお客様独自のプロトコルにも対応可能です。

■ 機能名	■ 概要/用途例
■ Built-in Module	<ul style="list-style-type: none"> <li>低レイヤの脆弱性、攻撃などを定義したブラックリスト</li> <li>ポートスキャンなど攻撃対象の検索の発見</li> </ul>
■ LAN CP LAN Connection Profiler	<ul style="list-style-type: none"> <li>通信方向をベースにしたホワイトリスト</li> <li>不要な通信、不正な端末の発見</li> </ul>
■ ITL Industrial Threat Library	<ul style="list-style-type: none"> <li>産業制御システムにおける脅威を定義したブラックリスト</li> <li>既知の攻撃手法による攻撃を検知</li> </ul>
■ DPBI Deep Protocol Behavior Inspection	<ul style="list-style-type: none"> <li>産業制御プロトコルの通信内容をベースにしたホワイトリスト</li> <li>通信内容の改ざん、操作ミスなどの検知</li> </ul>
■ SD Script	<ul style="list-style-type: none"> <li>スクリプト言語によるカスタマイズ</li> <li>お客様独自のプロトコルへの対応</li> </ul>

## 産業制御プロトコルに広く対応

eyeInspectは様々な産業制御プロトコルに対応し、セキュリティ対策をサポートします。

■ 産業制御プロトコル	■ メーカー固有の産業制御プロトコル	
<ul style="list-style-type: none"> <li>●BACnet</li> <li>●C-Link (Field, FieldBasic,Control)</li> <li>●DLMS/COSEM</li> <li>●DNP3</li> <li>●EtherCAT</li> <li>●EtherNet/IP + CIP</li> <li>●Foundation Fieldbus HSE</li> <li>●IEC 60870-5-101/104</li> <li>●ICCP TASE.2</li> <li>●IEC 61850 (MMS, GOOSE, SV)</li> <li>●IEEE C37.118(Synchrophasor)</li> <li>●Modbus ASCII</li> <li>●Modbus RTU</li> <li>●Modbus/TCP</li> <li>●OPC-AE</li> <li>●OPC-DA</li> <li>●OPC-UA</li> <li>●PROFINET (RPC, RTC, RTA,DCP and PTCP)</li> <li>●SLMP</li> </ul>	<ul style="list-style-type: none"> <li>●CNCP (ABB)</li> <li>●IAC/MMS (ABB)</li> <li>●CSLib (ABB 800xA)</li> <li>●DMS (ABB AC 800 F)</li> <li>●PN800 (ABB Harmony)</li> <li>●RNRP (ABB)</li> <li>●SPLUS (ABB Symphony Plus)</li> <li>●ADS/AMS (Beckhoff)</li> <li>●BSAP &amp; BSAP IP (Bristol Babcock)</li> <li>●CygNet SCADA (CygNet)</li> <li>●DeltaV (Emerson)</li> <li>●Ovation (Emerson)</li> <li>●ROC (Emerson/Fischer)</li> <li>●MarkVI/VIe (GE)</li> <li>●SRTP (GE)</li> <li>●SES 92 (GRE)</li> <li>●Experion (Honeywell)</li> <li>●FOX (Honeywell Niagara / Tridium)</li> <li>●NetIO (Kongsberg)</li> <li>●LonTalk (LonWorks)</li> <li>●Melsoft (Mitsubishi Electric)</li> <li>●COMEX (Schneider Electric Foxboro)</li> </ul>	<ul style="list-style-type: none"> <li>●Modbus/TCP Unity (Schneider Electric)</li> <li>●OASyS (Schneider Electric)</li> <li>●Triconex Tristation (Schneider Electric)</li> <li>●Sox (Sedona)</li> <li>●Fast Message Protocol (SEL)</li> <li>●Telnet extensions (SEL)</li> <li>●Sinec H1 (Siemens)</li> <li>●Step7 (Siemens)</li> <li>●S7COMM+/OMS+ (Siemens)</li> <li>●CAMS (Yokogawa)</li> <li>●Centum DCS (Yokogawa)</li> <li>●HART (Yokogawa, Emerson)</li> <li>●ISaGRAF IXL (Yokogawa ProSafe and others)</li> <li>●Vnet/IP (Yokogawa)</li> <li>●Vnet/IP WAN (Yokogawa)</li> <li>●CodeSys (Wago, ABB, and others)</li> <li>●ADE (Phoenix Contact)</li> <li>●CIP extensions (Rockwell/AB)</li> <li>●CSP (Rockwell/AB)</li> <li>●Citect (Schneider Electric)</li> </ul>

※その他、ITプロトコルにも対応します。

### NEC デジタルネットワーク事業部

NEC営業担当、または下記URLよりお問い合わせ下さい。

<http://jpn.nec.com/contactus/index.html>

- 本紙に記載された社名、商品名は各社の商標または登録商標です。
- 本製品の輸出（非居住者への役務提供等を含む）に際しては、外国為替及び外国貿易法等、関連する輸出管理法令等をご確認の上、必要な手続きをお取りください。ご不明な場合、または輸出許可等申請手続きに当たり資料等が必要な場合には、お買い上げの販売店またはお近くの弊社営業拠点にご相談ください。
- 本紙の内容は改良のため予告なしに仕様を変更することがありますのでご了承ください。