

工場内脅威可視化ソリューション In-Line Security Monitor HAT

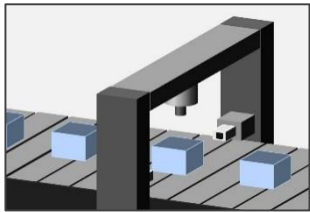
「つながる」からこそ高まる「稼働停止」リスク、対策は充分ですか？

見える化による生産効率改善、設備稼働状況の傾向分析による障害予兆検知、工場間リアルタイム情報連携による在庫・生産計画最適化など、今「つながる工場」が普及しはじめています。しかし、それに比例して拡大しているのが、サイバー攻撃や偶発的なウイルス感染などによる工場の稼働停止リスクです。

事例報告1 : 国内工場

品質検査装置のウイルス感染で不良品が市場流出

工場の最終工程にある品質検査装置がウイルス感染し、システム負荷が異常に高まり、本来、不良品として判定すべきものがそのまま出荷され、リコールにいたりしました。



※図はイメージです

侵入経路 USBメモリ

出典：トレンドマイクロ調べ

事例報告2 : 国内自動車工場

ランサムウェア感染により、生産一時停止

国内自動車工場で、工場の生産ラインの制御システムがランサムウェアWannaCryに感染。操業停止により、1,000台分の生産が影響を受けました。

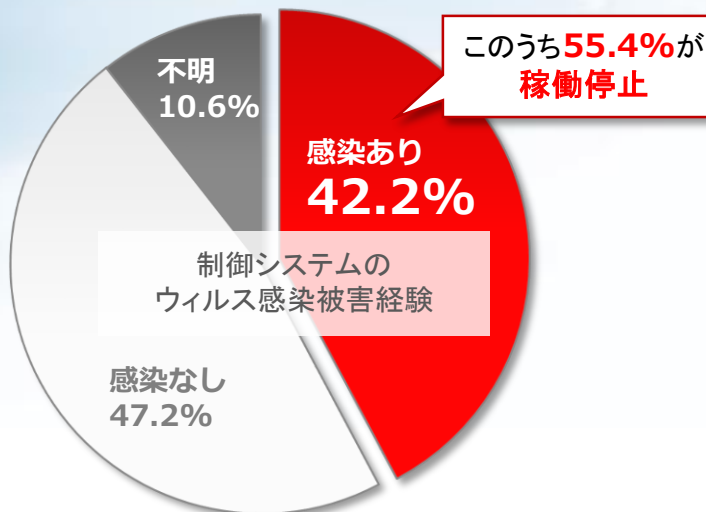


※写真はイメージです（アラクスネットワークス株式会社提供）

侵入経路 不明

出典：トレンドマイクロ調べ
(複数報道による)

日本における制御システムの被害実態（図1）



稼働中の工場は止められないため
制御システムの脆弱性は残ります

工場では、ネットワーク内部のサイバー
リスクがそもそも計測できていません

+

IoT技術を活用した制御機器の
ネットワーク接続は今後増えていきます

工場向けセキュリティ対策のPoint

- ① 入口対策
— 「OT側に残る脆弱性」への対策
- ② 出口対策
— 「レシピア情報の漏えい」への対策
- ③ 内部対策（コントロール～フィールド）
— 「内部不正の早期通知→保全」対応

『In-Line Security Monitor HAT』 3社共同開発！



内部対策

AlaxaIA — HAGIWARA

In-Line Security Monitor HAT システム構成

AlaxaIA

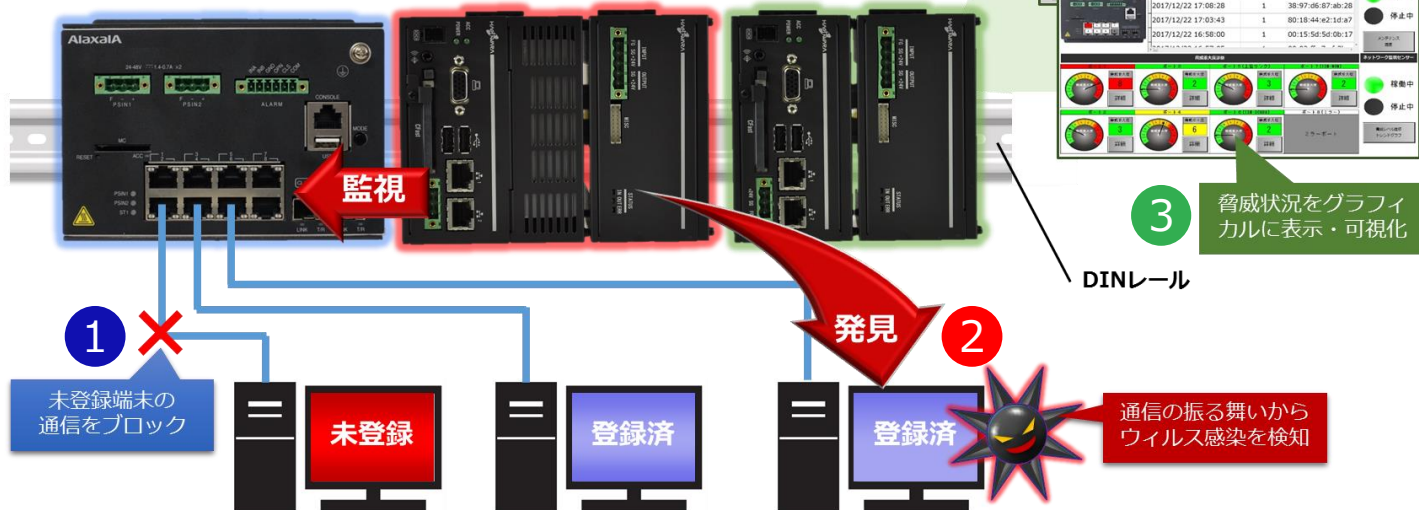
**TREND
MICRO**

HAGIWARA

ホワイトリスト機能搭載
スイッチ

ネットワークセンシング技術

セキュリティ情報可視化



1 ホワイトリスト機能搭載スイッチ

- 登録済端末の通信を許可し、未登録端末の通信を遮断
- ホワイトリストの自動学習可能

通信遮断

既存のL2スイッチと入れ替えるだけ
ホワイトリスト型セキュリティスイッチ

AlaxaIA
ホワイトリスト機能搭載スイッチ

2 ネットワークセンシング技術

- 通信の振る舞いを監視し、怪しい通信を発見・通知
- ホワイトリストで許可された端末のウイルス感染を発見

検知分析

工場ネットワーク内部のサイバーリスク可視化を実現する高度化検知センサーソリューション

**TREND
MICRO**
ネットワークセンシング技術

萩原電気製
HPU A100ECシリーズ

3 セキュリティ情報可視化

- 以下の情報を現場保全員が理解可能な情報として表示
- I. ホワイトリスト機能搭載スイッチで検知された不正通信
- II. ネットワークセンシング技術で検知された脅威

可視化

脅威検知の結果を現場担当者が理解できる情報として表示する見える化ソリューション

HAGIWARA
セキュリティ情報可視化

萩原電気製
HPU A100ECシリーズ

オプション
ウイルス発見時の
ウイルスチェックツール

スタンドアロン/クローズド環境向け
ウイルス検索・駆除ツール

**TREND
MICRO** Trend Micro
Portable Security 2™

※仕様は予告なく変更される可能性があります。

■ HPU、HAGIWARAロゴは、萩原電気ホールディングス株式会社の登録商標です。
 ■ トレンドマイクロ株式会社、TREND MICROロゴは、トレンドマイクロ株式会社の登録商標です。
 ■ AlaxaIAロゴは、アラクスアラネットワークス株式会社の登録商標です。

お問い合わせ先
 萩原テクノソリューションズ株式会社 **HAGIWARA**
 システムインテグレーション事業部 IoTソリューション部
 〒461-0001 名古屋市中区泉2丁目28番23号 高岳KANAMEビル
 TEL : 052-931-3624
 Mail : 1s-iot@hagiwara.co.jp