製造業向け
産業サイバーセキュリティ対策

工場のDX推進にあたり、サイバーセキュリティ対策はお済みですか?

Point 1
設計・構築・運用まで
セキュリティ対策を
サポート

Point 2
対象設備を把握し
ニーズに合わせた
対策を提案

Point 3
リスクアセスメントを
実施し最適な
設計・構築

Point 4
ネットワーク障害の
切り分けにも
対応

2022年11月16日に経済産業省で
「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」が策定されました。
このガイドラインは、産業界全体のセキュリティ向上を目的としています。
工場ネットワークの多数の構築実績と産業サイバーセキュリティエキスパートを保有するきんでんに、
工場のサイバーセキュリティ対策はお任せください。

工場ネットワークに対してサイバー攻撃を受けると様々なトラブルが想定されます

工場ネットワークには、様々な設備が繋がります。データ流出だけではなく、設備稼働の維持や作業員の安全確保のためにも、セキュリティ対策は重要です。例えば、ネットワークを細かくゾーン分けすることで、万が一、被害にあった際も影響を最小化し、復旧を早めることができます。

工場内ネットワークにおける サイバー攻撃ルートと被害例

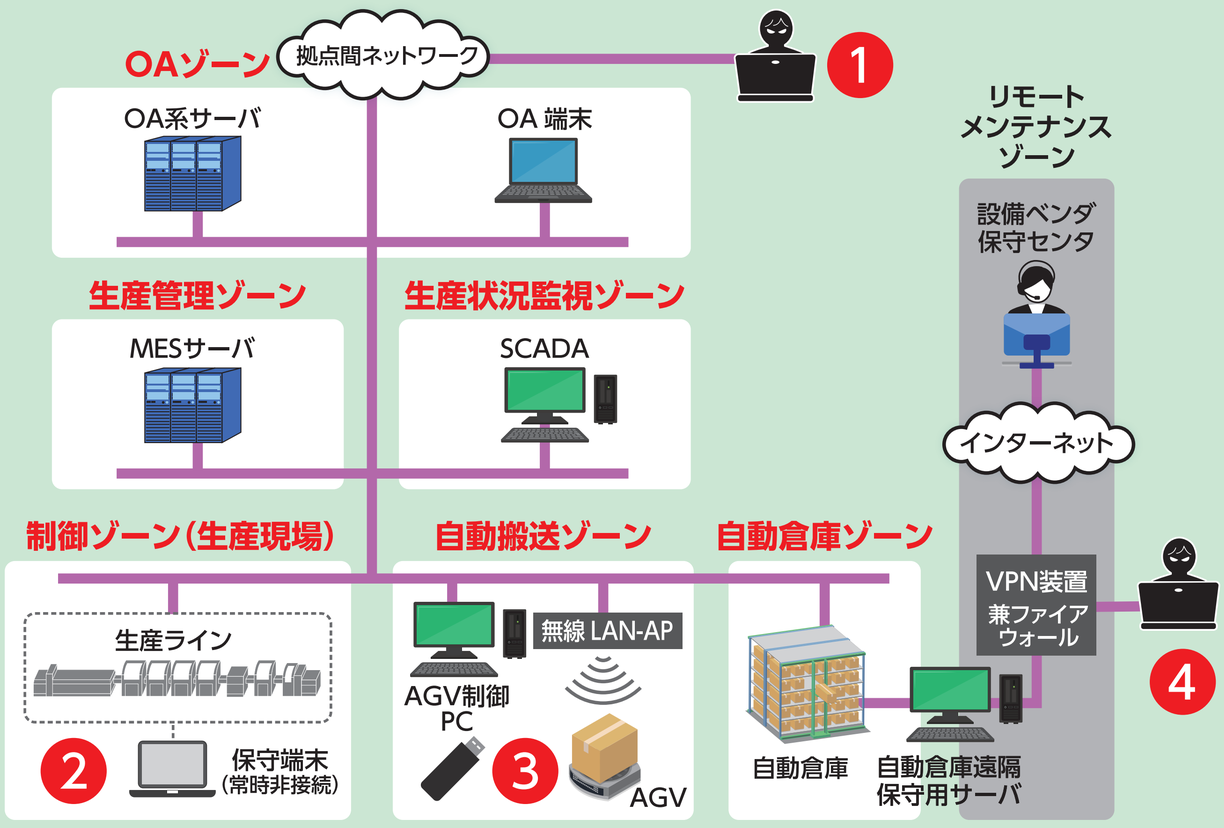
1 ネットワーク経由
●ウイルス感染
●不正コマンド送信攻撃など

2 保守端末経由
●ウイルス感染
●不正コマンド送信攻撃など

3 持ち込みUSB経由
●パソコンなどへのUSB
差し込みによるウイルス感染

4 メンテナンス回線経由
●ウイルス感染
●不正コマンド送信攻撃など

トラブル
- ●システムの停止
- ●品質の低下
- ●製造方法の流出
- ●人身事故の発生



参照元：経済産業省『工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン』

以下の4つのサービスを中心にお客様とともに工場の安定稼働に寄与します

1 リスクアセスメント サービス
導入されている機器の状況を把握し、リスクアセスメントにより、サイバー攻撃のリスクがどこにあるかを明確にします。

2 セキュリティ 対策構築サービス
リスクに対応するため、物理セキュリティも含めた多角的な視点からセキュリティ対策を設計し構築します。

3 運用支援サービス (OT-SOC)
導入したセキュリティ機器を24時間365日体制で遠隔監視し、インシデント発生時の対応支援を実施します。

4 リアルタイムサポート サービス(RTS)
万が一のネットワークトラブルに24時間365日対応。迅速なネットワークの障害切り分けと復旧を支援します。

Kinden