HITACHI

~Cisco Cyber Visionを活用した自動車部品工場のセキュリティ強化~

OTゾーンに適したセキュリティをネットワークで実現

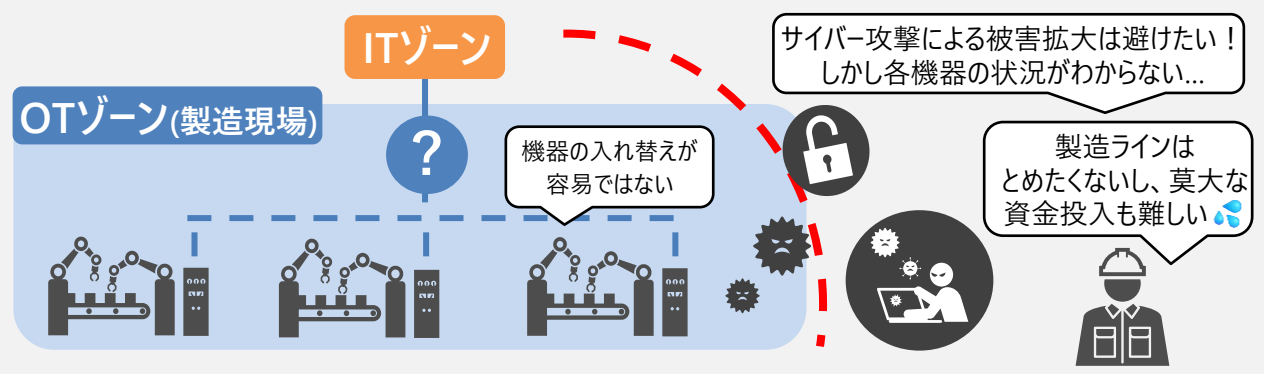
事例紹介vol.9 2025.8.28

背景

工場全体のIT化が進む中、OTゾーンでは製造ラインや流通を含むサプライチェーン全体のセキュリティ強化が急務です。しかし、古くからの自動車部品工場の中には、リスクを認識しつつも十分なセキュリティ対策が施せないケースが発生しています。

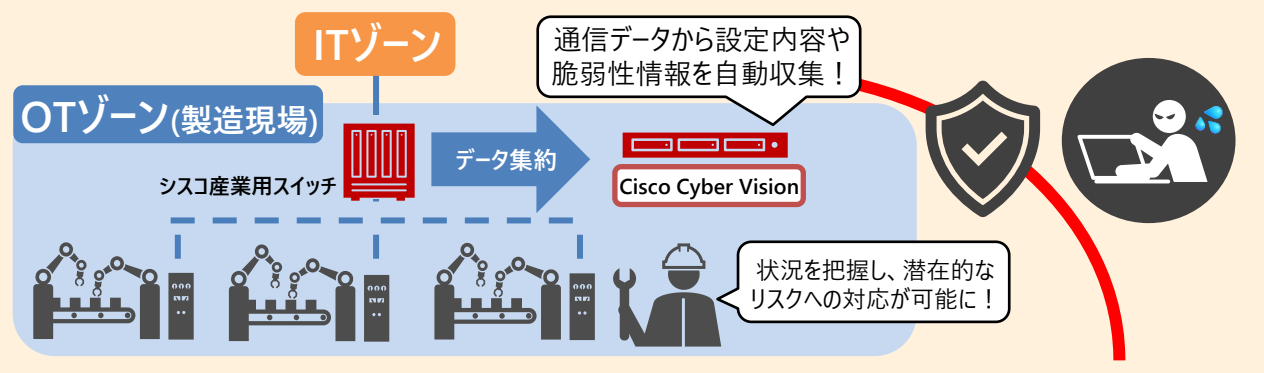
想定される課題

- サプライチェーンを経由したサイバー攻撃の感染拡大が発見できない
- 工場内のIT・OT間のデータ連携が増加したため、セキュリティの強化を図りたいが、独自のシステムが多くセキュリティ対策ソフトの導入が難しい
- セキュリティ対策ソフトウェアの導入には製造ラインの停止が伴い、高額な損失が発生



日立情報通信エンジニアリングが提案する解決策

- Cisco Cyber Visionとシスコの産業用ネットワーク機器の導入で、接続機器の識別情報や通信情報に加え、脆弱性情報を可視化、および不審な挙動を検知し、工場内に適したセキュリティ対策を事前に行うことができるネットワークを実現
- シスコの産業用ネットワーク機器がセンサーとなり、ネットワークの末端までカバー

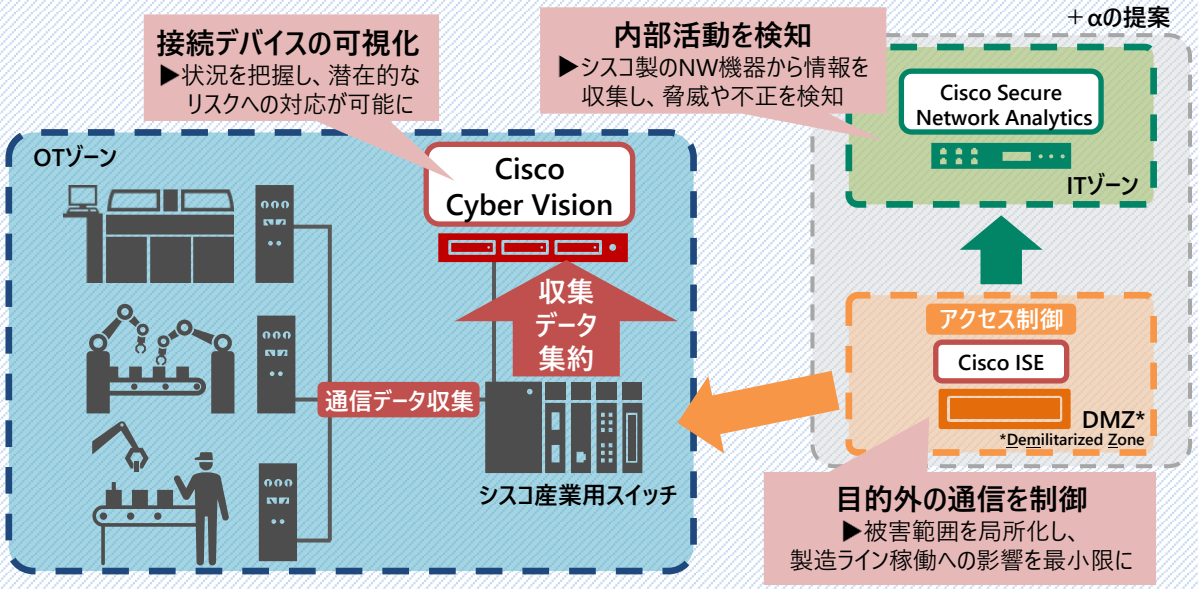


株式会社 日立情報通信エンジニアリング

提供可能なもの

Cisco Cyber Visionとシスコの産業用機器の導入により、
ネットワーク側でセキュリティ強化が可能な環境を提供します。

システム構成例



想定効果

☑無許可の機器や既知の脆弱性を**把握**することで、**リスクへの事前対策が可能**に
☑Cisco ISEの**アクセス制御との連携**によって**被害の局所化**を実現
☑IT領域のネットワークを常時監視するCisco Secure Network Analyticsも併せて導入することで、**OT領域に加えてIT領域のセキュリティも強化**

製品名	役割
Cisco Cyber Vision	ネットワーク上に流れる産業用プロトコル通信を収集し、平常時の通信内容を記憶することで、それを逸脱した怪しい振る舞いを検知。また、接続されている機器の識別情報や通信情報に加え、脆弱性情報を自動で収集して一覧化。
シスコ産業用スイッチ	通信データの情報を収集。 また、シスコの産業用ネットワーク機器を用いることによって、エージェントレスで導入が可能。
Cisco Identity Services Engine(ISE)	認証機能による**アクセス制御を用いて不審な通信を制限。**Cisco Cyber Visionが収集した情報を元に、特定のデバイスのみを遮断し目的外の通信を制御することも可能。
Cisco Secure Network Analytics	ネットワーク上を常時監視し、不審な端末を早期に検知。また、Cisco ISEと連携することで、ユーザ情報を詳細に把握し、検出した脅威を迅速に封じ込めることが可能。

さまざまな製造現場のご相談を承ります

当社は製造現場をはじめとしたOT領域におけるセキュリティ対策支援に関して、
導入支援はもちろんのこと、設計・構築、監視・運用まで一貫した対応が可能です。
お客さまの環境に最適なセキュリティ対策を提案いたします。ぜひお気軽にお声掛けください。

※本資料中の「シスコ」は、正式名称「シスコ合同会社」を指します。

当社事例

株式会社 日立情報通信エンジニアリング

神奈川県横浜市西区みなとみらい2丁目3番3号クイーンズタワーB 22階
〒220-6122　www.hitachi-ite.co.jp/

August.2025