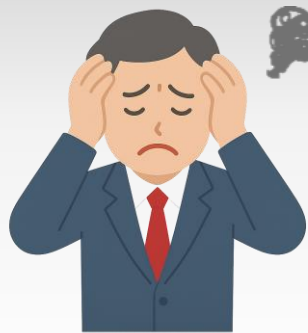


日立ソリューションズ × Fortinetソリューションで実現する

OTセキュリティ

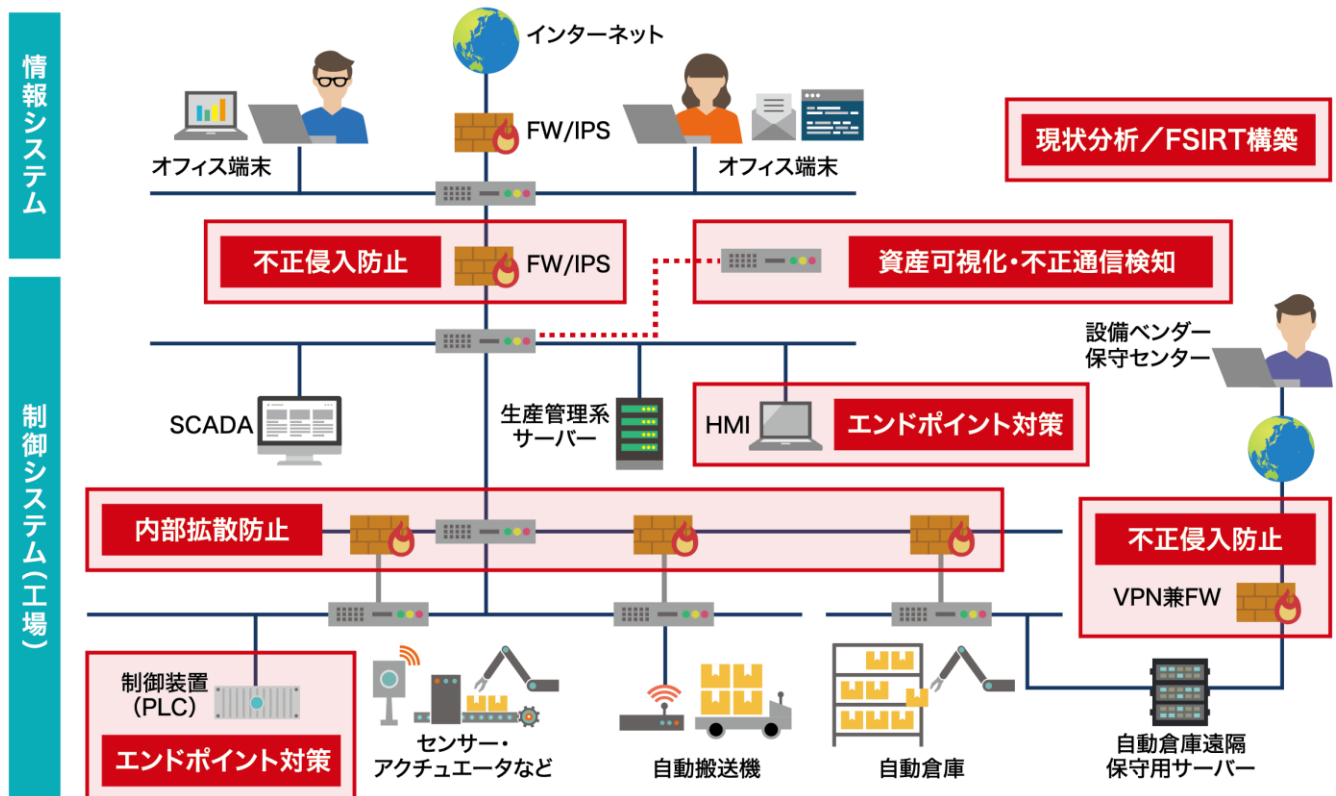
近年のデジタル化やDX（デジタルトランスフォーメーション）の推進により、工場の制御システム（OT）がネットワークと接続されたことで、製造業を狙うサイバー攻撃のリスクは高まっています。一度の攻撃が、生産停止や人命に関わる事故を引き起こし、企業の存続を揺るがす事態にもなりかねません。事業継続性を確保する観点からも、OTセキュリティは今や、不可欠な対策です。

制御システム（OT）で、このような課題はありませんか？



- OTセキュリティについて**どのように取り組めばいいかわからない**
- **現状の対策が十分なのか**わからない
- 経営層に**事業継続リスク**の認識を得られない
- **IT部門とOT部門を横断**したセキュリティ対策が不足している
- **誰に相談すべきかわからない**

日立ソリューションズなら、段階的なOTセキュリティ対策のご提案が可能



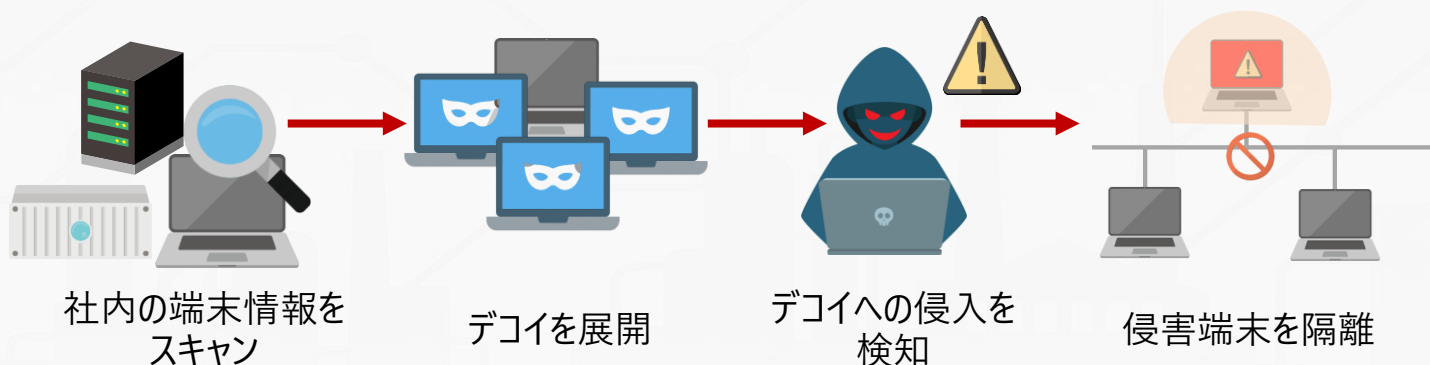
FW : Firewall IPS : Intrusion Prevention System FSIRT: Factory Security Incident Response Team SCADA : Supervisory Control And Data Acquisition
HMI : Human Machine Interface PLC : Programmable Logic Controller VPN : Virtual Private Network

日立ソリューションズ × Fortinetソリューションが提供する 主なOTセキュリティ

攻撃者の早期検出と自動隔離 (FortiDeceptor※)

デセプション（欺瞞）技術を活用し、攻撃者を偽のシステム（デコイ）へ誘導することで、ネットワーク内部の脅威を早期に検知し、自動で遮断・隔離。

- ラテラルムーブメント（横展開）を早期検知し、FortiGateと連携して自動遮断
- WindowsやLinuxなどのITデコイにくわえ、さまざまなIoT／OTデコイに対応
- OT環境の稼働に影響を与えずに、容易に導入可能



※2026年7月末当社取り扱い開始予定

産業用プロトコルの制御 (FortiGate × OTセキュリティライセンス)

従来のアプリケーション制御／IPSシグネチャに加え、産業用プロトコルを可視化・制御。



<対応プロトコル例>

BACnet、Modbus/TCP、DLMS/COSEM、OPC、ELCOM、IEC.61850、DNP3、PROFINET、S7

資産の可視化 (FortiNAC)

ネットワークに接続するだけでIoT／OT含むさまざまなデバイスを可視化。未管理のデバイスは自動的に隔離VLANへ誘導。



デバイスの
可視化と識別



デバイスの
コントロール

製造業のシステム構築で培った豊富なノウハウを生かし、お客さまのご要望に応じた提案が可能。OTセキュリティのご相談は当社まで！



※本資料の一部は、生成AIにより生成されたコンテンツを使用しています。※Fortinet、FortiDeceptor、FortiNAC、FortiGateは、Fortinet, Inc.の米国およびその他の国における商標または登録商標です。※その他、本リーフレット中の会社名、商品名は各社の商標、または登録商標です。※本文中および図中では、TMマーク、®マークは表記していません。※製品の仕様は、改良のため、予告なく変更する場合があります。※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認のうえ、必要な手続きをお取ください。なお、ご不明な場合は、当社担当営業にお問い合わせください。※本リーフレット中の情報は、作成時点のものです。

株式会社 日立ソリューションズ

www.hitachi-solutions.co.jp

本リーフレット掲載商品・サービスの詳細情報

<https://www.hitachi-solutions.co.jp/fortinet/>

