NTT AT

工場の安全・安心な稼働を継続するためのアセスメント

OT@Mo®シリーズ「OTセキュリティアセスメント」

工場やビル内のセキュリティリスクの現状を把握し、効果的なセキュリティ対策を進めることができます。



“止められない製造ライン”と、“止まらないサイバー攻撃の進化”

近年、製造業を含む産業分野においてもDXが浸透した結果、ITシステムやインターネットに接続された製造機器(OT機器：Operational Technology)がサイバー攻撃のあらたな対象となり、そのリスクが課題となっています。これは最新の攻撃を防ぐセキュリティパッチ適用などの保守作業のためにその都度、製造ラインを停止することが困難で、日々進化するサイバー攻撃に対処できないケースも予想され、工場が稼働したままでも万全のセキュリティ対策が取れる手段が求められています。
NTT-ATのOTセキュリティアセスメントサービスを利用することで、止めることができない製造機器に差し迫るサイバー攻撃のリスクを洗い出し、被害を未然に防ぐためのセキュリティ対策を、御社の状況に合わせて進めることができます。

POINT 1
経産省のガイドライン等で工場のリスクを見える化

経済産業省のガイドラインで提言されたチェックリスト※をベースに、国際標準規格「ISA/IEC62443」の要件を盛り込んだ弊社独自のヒアリングシートで、製造設備のリスクを多角的に評価します。

POINT 2
各種セキュリティ資格を保有するスペシャリストが一連の工程を対応

セキュリティ業務経験が豊富で、各種資格（CISSP/情報安全確保支援士/IEC62443他）を持つスペシャリストが、プロならではの視点で、製造設備に潜んだセキュリティの抜け穴を探り当てます。

POINT 3
アセスメント／対策／運用保守までトータルサポート

弊社では長年にわたり、数多くの通信業界や企業、自治体においてネットワーク構築から運用保守まで幅広く携わっており、自社保有のICT-24SOCによるリモート監視も含めた、包括的なご提案も可能です。

※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」に記載

セキュリティ Security

https://www.ntt-at.co.jp/product/ot-asses/

サービス概要

御社の持つ課題やご要望に合わせた2種類のアセスメントを用意しています。網羅的なアセスメントを実データで裏を取るように2つのアセスメントをセットで提供することが可能です。また、机上で網羅的なアセスメントを実施したいお客様や実態調査から入りたいお客様などに向けて個別に提供することも可能です。

ガイドラインベース

経済産業省ガイドラン記載のチェックリスト32項目ごとの実状を、IEC62443の要件を用いた弊社独自のヒアリングシートを使って網羅的に効率よく把握します。主に4つのカテゴリー(組織／運用／技術／サプライチェーン)ごとに現状のリスクを考察し、優先度を考慮したセキュリティ対策をご提案します。

● このような課題をお持ちの企業に最適です。
- OTセキュリティ対策をどう進めたらよいかわからない
- どのような対策を実施すべきなのかわからない
- どこまでコストをかけて実施すべきなのかわからない

実施フロー例

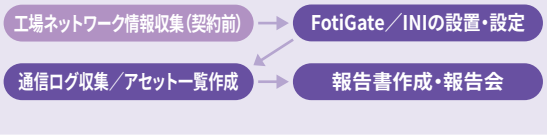
Web簡易診断(無償)
↓
現状把握・ヒアリング
↓
リスクの洗い出し・分析
↓
対策案検討
↓
報告書作成・報告会

実環境ベース

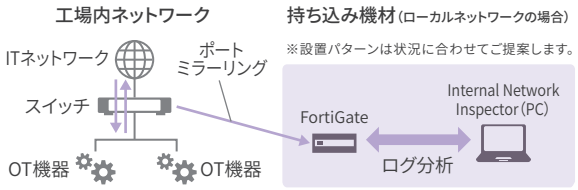
ネットワークに接続された製造機器を弊社のツールによりリスト化します。あらかじめ機器台帳をご提供頂ける場合は機器台帳と照合し、把握されていない機器を提示します。また、社外への不審な接続履歴がある機器の情報などをピックアップするなど、実態調査にもとづいた効果的なセキュリティ対策をご提案します。

● このような課題をお持ちの企業に最適です。
- 製造設備の通信の実態がわからない
- アセット一覧のベースを自動生成したい
- 工場内のネットワークにリスクがあるかを確認したい

実施フロー例



機器の設置例



※ FortiGate：米国Fortinet社の開発した統合脅威管理アプライアンス
https://www.fortinet.com/jp/solutions/industries/manufacturing
※ Internal Network Inspector：NTT-ATで開発した未承認機器を検出するためのソフトウェア

OTセキュリティサービス「OT@Mo®(オーティーオトモ)シリーズ」ラインナップ

STEP0	セキュリティ対策レベルの概要把握	無料・簡単・その場で結果がわかる!「OTセキュリティクイック診断」
STEP1	どのような対策が必要か検討	リスクの洗い出しと対策案を検討「OTセキュリティアセスメントサービス」
STEP2	セキュリティ対策の実施	サイバー攻撃の検知と監視・運用「OTセキュリティモニタリング」(旧称：工場・ビル向けOT/IoTセキュリティサービス)
STEP3	対策の定常的運用・見直し	FortiGateを24時間365日監視する「FortiGate SOC プラスOTオプション※2」

※OTセキュリティクイック診断　https://www.ntt-at.co.jp/inquiry/io-security/

お問い合わせ　https://www.ntt-at.co.jp/product/ot-asses/

※記載された社名、各製品名等は、各社の商標または登録商標です。※本カタログ記載の内容は予告なく変更することがあります。※カタログ記載内容 2025年10月現在

NTTアドバンステクノロジ株式会社