OTセキュリティ対策を進めるためのサポートガイド

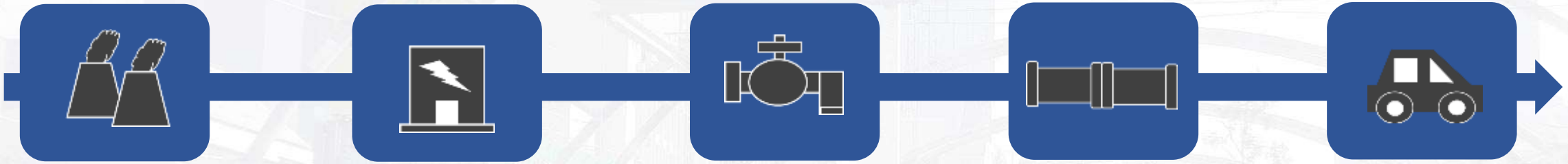
NTTアドバンステクノロジ株式会社
ソーシャルプラットフォーム・ビジネス本部
セキュリティビジネス部門

目次

サイバー攻撃の新たなターゲットとなる製造分野

近年、製造分野でのDX(デジタルトランスフォーメーション)の推進により、ITシステムやインターネットとの接続が増えた結果、IT機器だけでなく、OT*1/IoT機器が新たなサイバー攻撃の対象として危険視されています。

これまで、ICS(産業用制御システム)やSCADA(監視制御・データ収集システム)とネットワークの間にはエアギャップが存在していましたが今では取り払われ、ITシステムや、ひいてはインターネットと接続するようになり、これらのシステムは拡大する脅威にさらされるようになりました。



2010 イラン

マルウェア(Stuxnet)による核燃料施設の制御システムを標的とした攻撃事例

2015 ウクライナ

電力設備へのサイバー攻撃(不正侵入と遠隔操作)が原因で、大規模停電が発生した事例

2021 米国

水道局施設へのサイバー攻撃(不正侵入と設定変更)による飲料水の汚染未遂事例

2021 米国

ランサムウェアによるサイバー攻撃によるパイプラインへの影響(予防保全的な停止)事例

2022 日本

サプライチェーンの事業者のサーバがサイバー攻撃の影響で停止し、自動車の国内工場が稼働停止した事例

*1:Operational Technologyの略。産業オートメーションおよび制御システムのコンポーネントなどのシステムやその技術

製造分野を狙った国内の攻撃事例

様々な企業規模・業種がサイバー攻撃の被害に！

■ T社サプライチェーン（2022年）
取引先の部品メーカーがサーバ攻撃を受けた影響で、T社14工場28ラインの稼働が一時停止した。
攻撃者は、部品メーカーの子会社のリモート接続機器に脆弱性があることを利用し、子会社のネットワーク経由で部品メーカーのネットワークへ不正にアクセス。サーバー、PCの一部が暗号化された。

■ H病院（2021年）
外部からのサイバー攻撃により、電子カルテなどのデータが暗号化された。
サイバー攻撃前の状態で通常診療を再開するのに、約2か月の時間を要した。

■ H社（2020年）
外部からのサイバー攻撃によって、社内ネットワークのサーバが暗号化された。
この影響で製造拠点での出荷停止、新型コロナウイルスの影響で在宅勤務を行っていた従業員も社内システムが使えず有給休暇の取得を推奨された。

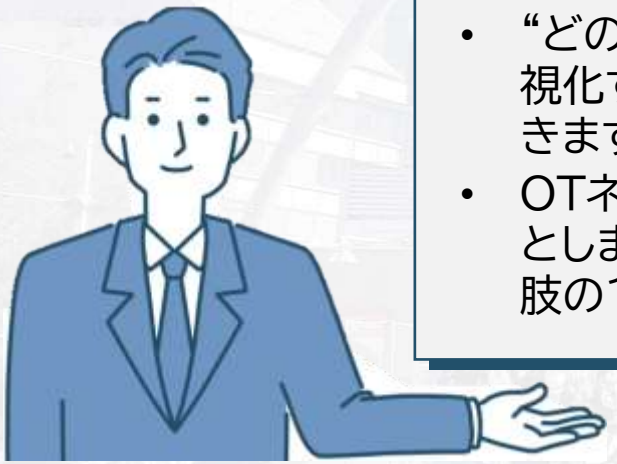
OTセキュリティ対策が重要な理由と課題

- 「停止しないことが最優先」というOTシステムの特徴が、サイバー攻撃の危険性を高めています。
- OTシステムに対するサイバー攻撃は、システムや設備破壊・営業停止など広範囲に及び短い停止時間で大きな損害を発生させるため、OTセキュリティ対策の重要性が高まっています。

	OTシステムの特徴 （産業用オートメーション・制御システム）	OTシステムのセキュリティ課題
システムの最優先事項	継続的な安定稼働	◆不十分な脆弱性対策 • 多くの場合パッチ適用不可のため、既存のセキュリティホールが放置 • 適用する場合は動作影響を十分に検討・検証する時間が必要
システム稼働期間	10年以上	
システムの遅延耐性	深刻な稼働影響が懸念されるため許容の余地がない	
データ保護の優先順位	「可用性」＞「完全性」＞「機密性」	
管理組織	各工場拠点の技術部門	◆内部不正・人的ミスの危険性 • サイバーセキュリティが専門ではないため、意図しない事故を引き起こす危険性が高い
ネットワーク構成	・工場・拠点ごとに独自の仕様で構築されており、ネットワーク構成も複雑 ・何が接続されているのか把握できない、ブラックボックス化している場合が多い。	◆不十分なセキュリティ監視 • 独自仕様製品の多くはセキュリティを考慮せず開発されており、セキュリティホール化している可能性が高い。 • ブラックボックス化しているため、OTシステム内の異変を把握できず、攻撃の発見・止める等の早期対応ができない。そのため、長期間のシステム停止を伴う大規模サイバー攻撃を仕掛けられる危険性が高い。 （例）サイバー攻撃が原因で工場設備の動作が不安定になっていたが、継続稼働を優先し、不調の原因調査を放置していたらある日突然停止した。

OTセキュリティ対策は、何から取り組むべき？

現状のまま放置することは危険だし、OTセキュリティ対策を進めるべきだと考えているが、OTシステムの変更は簡単ではない、、、。



まず、OTネットワークのセキュリティ監視・可視化に取り組みませんか？

- “どのような通信を行う機器”が“いくつ接続されているか”、“どう変化したのか”を監視・可視化することができれば、“OTシステム内の異変＝サイバー攻撃の予兆”を把握することができます。
- OTネットワークの監視・可視化は、一般的に既存のOTシステムに対して物理的な変更を必要としません。そのため現在のOTシステムの稼働を妨げずに、セキュリティ対策を強化する選択肢の1つです。

OTセキュリティ監視・可視化サービスを選ぶポイント

OTシステムの規模・構成の複雑さ・拠点数などによって、監視システムの要件は異なります。

以降のページは、資料をダウンロードいただくと

ご覧になることができます。

＼3項目のフォーム入力後、その場でダウンロード！／

専用ダウンロードページ＞＞
https://mal.ntt-at.info/inquiry/ot-iot-guide-dl/