日立ソリューションズ・クリエイト

HITACHI
Inspire the Next

工場機器はインターネットに繋げていないから、何もしなくて大丈夫…？

工場セキュリティソリューション

現在のサイバー攻撃はビジネス化・テロ化が進み、工場機器は、これまで以上に脅威に晒されています。
さらにIoT化も進むことで、工場は既に情報セキュリティにおいて聖域ではありません。

サイバー攻撃による工場被害事例

隔離環境での被害事例

国内の自動車工場で、設備の端末入れ替え時にウイルスに感染。
生産ラインの一部が停止。

サプライヤーへの感染

ドイツの工場がサイバー攻撃を受け、生産が50分停止。サプライヤーへの感染も疑われ、**影響額は約17億円。**

今後、セキュリティ規格への準拠はさらに重要視されます。

IEC62443やNIST SP 800-82といったセキュリティ規格が標準化

調達要件

セキュリティ規格への準拠を、調達要件とする事業者が増えてきています。

サプライチェーン

サプライチェーン全体で一定水準のセキュリティを確保するSP 800-171を満たしていなければ、今後、**調達先から除外される可能性**があります。

当社は豊富なメニューでお客さまを支援します。まずはご相談ください。

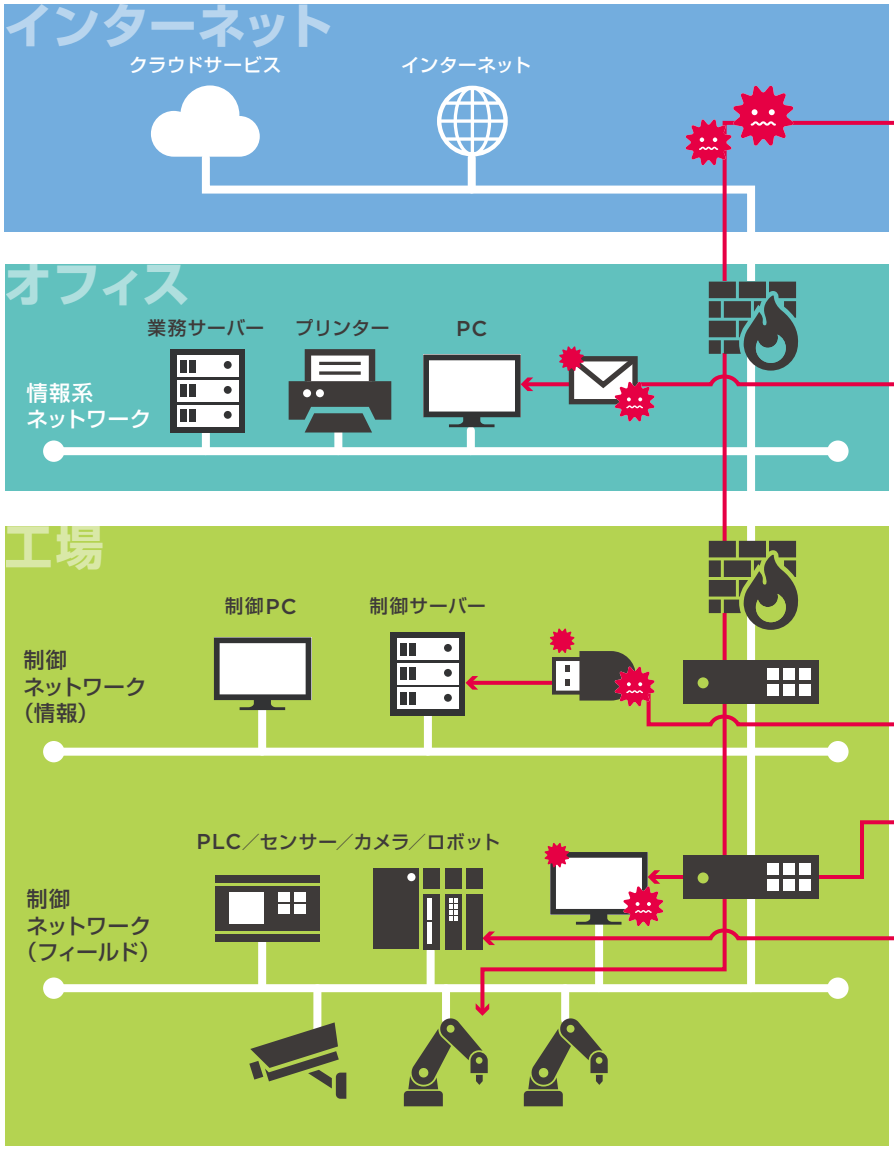
まずは、工場内のセキュリティ状況を確認しましょう

チェックしてみてください

- ☐ 情報セキュリティの規則はあるが、工場セキュリティの規則はない
- ☐ 工場内の制御情報ネットワークや保守用の回線と、オフィスのインターネットが適切に分離されていない
- ☐ 生産機器（PLCなど）が管理できていない
- ☐ OT資産の汎用OS管理、アクセス制御、ぜい弱性管理、無線LAN管理、ログ管理などが、徹底されていない
- ☐ インシデント発生時の影響範囲が管理できていない

1つでも、当てはまる項目がありますか？ それが**「リスク」**です。

「脅威」や「ぜい弱性」が潜む場所は、以下のような場所です



ぜい弱性を狙って、外部から工場設備をリモート操作

メールの添付ファイルからマルウェア感染

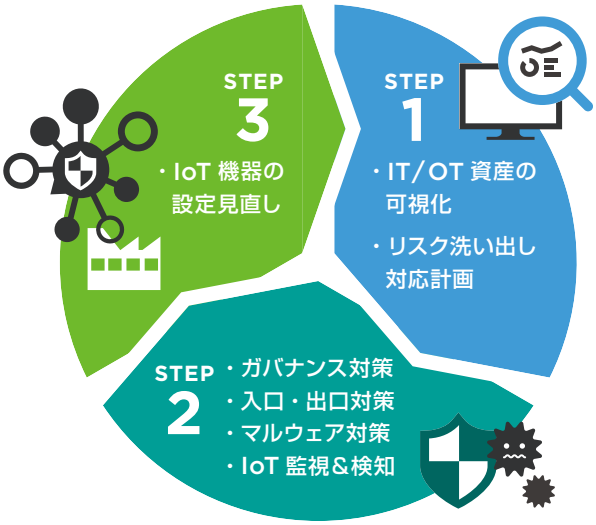
悪意を持つ従業員がUSBから不正プログラムを実行

保守用端末からマルウェア感染

SMBv1など、今は危険とされるプロトコルが残っており、情報が外部に露出

制御システムのセキュリティリスク対策

IEC62443※1**やNIST SP 800-82**※2**、NIST SP 800-171**※3
といったセキュリティ規格へ対応することで、**組織のセキュリティを強化**するとともに、**事業者としての社会的責任**を果たしていることを対外的に証明します。



※1: IEC62443　ISA（国際自動制御学会）とIEC（国際電気標準会議）が開発した制御システムのセキュリティを確保するための要求事項です。データ処理基盤だけでなく、システムの運用にかかわる「人」と「業務」も対象です。

※2: NIST SP 800-82　NIST（米国国立標準技術研究所、以下略）が開発、産業用制御システムのセキュリティ設定のガイドラインです。

※3: NIST SP 800-171　NISTが開発、機密ではない重要情報の適切な取り扱いを規定したガイドラインです。米国政府の調達、日本でも防衛調達時に取引先が準拠を求められます。今後、準拠状況がビジネスへ影響する可能性があります。

セキュリティ規格への準拠に向けた活動

		セキュリティ規格準拠に向けた支援	OUTPUT
STEP 1	IT/OT資産の可視化	IT/OT資産、通信経路の棚卸し	・資産管理台帳 ・ネットワーク構成図
STEP 1	リスク洗い出し	ぜい弱性の把握、リスク影響度の確認	・リスク報告書
STEP 1	対応計画	リスク対策の計画、優先付け	・経営幹部の承認
STEP 2	ガバナンス対策	セキュリティ規格に基づく基準作成	・ポリシーと組織
STEP 2	入口・出口対策	ゼロトラストに基づく通信制御の実装	・リスク対策の選択、導入 ・事業継続、インシデント対応の計画更新
STEP 2	マルウェア対策	ゼロトラストに基づくエッジ対策	
STEP 2	IoT監視＆検知	IoT機器と通信の可視化	
STEP 3	IoT機器の設定見直し	IoT機器の管理・運用面の見直し	・制度への適合監査

工場セキュリティソリューション

コンサルティングサービス

STEP 1

IT/OT資産の可視化

工場内情報セキュリティ現状調査

情報セキュリティのプロの視点で、現場の状況を調査します

リスク洗い出し

調査結果分析

現状調査の結果を基に、セキュリティの問題点の洗い出しを行います

対応計画

情報セキュリティ対応計画策定支援

分析を基に、お客さまの今後のセキュリティ対応計画策定を支援します

STEP 2

ガバナンス対策

ガバナンス対策支援

リスク分析・対応計画を基に、セキュリティ規格への準拠を支援します

セキュリティソリューション

入口・出口対策

ぜい弱性攻撃対策

SQLインジェクションなどWebサーバーに対する攻撃を防御。パスワードリスト攻撃からもWebサーバーを保護。

セキュリティトレーニング

認定ホワイトハットハッカーによるオンライン版セキュリティトレーニング。動画配信とライブ中継を融合した新たなスタイル。

マルウェア対策

標的型攻撃対策ソリューション

未知のマルウェア、悪意のある不正プログラムの実行を防止。スキャンや定義ファイルのアップデート不要、システムへの負荷を抑えた対策を実現。

※セキュリティポリシーの統合管理オプションあり

標的型メール訓練サービス

標的型攻撃を模擬した【訓練メール】をユーザーに配信し、標的型攻撃メールへの対応を学ぶ教育訓練。

IoT監視&検知

制御システム脅威検知ソリューション

ネットワークへの負荷を抑制しながら自動的に資産を可視化。100種類以上の産業用プロトコルのパケット検査が可能で、異常な挙動を検知。

※OT資産の統合管理オプションあり

ぜい弱性・リスク管理ソリューション

エージェントレス型製品、ネットワーク上のホストに関するデバイス診断・ぜい弱性分析が可能な、ぜい弱性リスク管理ソリューション。

STEP 3

IoT機器の設定見直し

商品・サービスに関するお問い合わせ・ご相談受付

Webによる受付

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールによる受付

hsc-contact@mlc.hitachi-solutions.com

HSC202208

株式会社 日立ソリューションズ・クリエイト

www.hitachi-solutions-create.co.jp/