ハイライトレポート【製造現場の最新セキュリティ対策】
情報セキュリティ10大脅威2024から見る工場システムのセキュリティリスクについて

2024. 4. 18

情報セキュリティの重要性　ランサムウェアの脅威から工場システムを守れ！

工場システムのDX化で新たな付加価値を生み出す取り組みが進む中、サイバー攻撃は年々脅威を増しており、情報セキュリティ10大脅威で1位となっているランサムウェアからの対策はもちろんのこと、それ以外でも被害にあえば会社として大きな損失につながりかねません。一方で、DX化には、IoTやICT技術の活用が不可欠であり、導入するIoT機器や情報端末のセキュリティ上のリスクをどう担保していくか、また、工場設備として必要な信頼性・耐久性をどう確保するかが課題です。

今回はIPA独立行政法人 情報処理推進機構が毎年発表している、組織向け情報セキュリティ10大脅威をもとに、**工場システム向け産業用PCでのセキュリティ対策と、セキュリティ運用**について事例も交えて解説いたしました。

情報セキュリティ10大脅威2024について

毎年更新されるIPAの「情報セキュリティ10大脅威」は一見すると代わり映えがしないようにも見えるため、自社に置き換えるとどのようなリスクがあるのかイメージが付きにくいかと思います。

そのため、様々なステークホルダーから対策を求められはじめていても、実際にどのセキュリティ対策から実施すべきかが不明で優先順位が付けられなくなってしまいます。

■ 本日の登壇者 ■

株式会社セキュアイノベーション
セキュリティ事業部 副部長
金城 夏樹 氏

OAセキュリティとOTセキュリティの違い

一般的なOAセキュリティとOTセキュリティとでは右図のようなポイントの違いを考慮する必要があります。

出所：投影資料より一部抜粋

OAセキュリティとOTセキュリティの違い

	OA	OT
管理・統括部門	情報システム部門	現場・工場長等
経営上	コストセンター	プロフィットセンター (コストだけでなく利益も生み出す)
保護対象 (主な目的)	個人情報等のデータの保護	モノ(設備、製品)、サービス(操業)の維持
セキュリティ対策	1.Confidentiality（機密性） 2.Integity(完全性) 3.Availability（可用性）	1.Availability（可用性） 2.Integity(完全性) 3.Confidentiality（機密性） ＋ 健康(Health) 安全(Safety) 環境(Environment)
償却期間	3~5年	10～20年 ※攻撃者にとっては穴を見つけやすい状況。
通信プロトコル	標準の通信プロトコル	標準またはベンダ独自のプロトコル
ネットワーク接続	常時接続されていない	常時接続
アカウント管理	共有ID	個人ID

情報セキュリティ10大脅威2024への対策

OTセキュリティとOAセキュリティの共通点から

エンドポイント対策の強化
境界防御の徹底
通信ログ・検知ログの可視化
＋
セキュリティ運用

が重要であり、**OAセキュリティの経験が活きるものもあります。**

リョーサン テクラボ
エンジニアによりそうマガジンサイト

他記事、ウェビナ、お問い合わせはこちら