工場セキュリティ対策は万全ですか?

～いまさら聞けない「IEC62443」や北米工場向け「NIST」対策の秘訣をロックウェル・オートメーションよりご紹介しております～

ネットワークセキュリティサービス
(NSS: Network/Security Services)

OTセキュリティ動向、共通課題

旧式システムの運用
パッチ未適用のレガシーシステム

インセキュアデザイン
ネットワークセグメンテーションの欠如

知識・スキル不足
ITセキュリティ⇔OT知識

OT環境の可視化
OT資産、プロセスの可視化

アクセス管理
進化するアクセス・ニーズ

変更管理、導入後の運用
24時間 / 365日運用

ビジネスニーズ
リアルタイム情報

IT対策同様にOTもセキュリティ対策は必須だが、現状は課題山積!

特にOTは外部ネットワークから切り離した「鎖国状態」で長年放置されてきました。そのため「個別最適化」「ガラパゴス化」の典型となっている事例が日本国内で散見されます。

問い合わせ先:
ロックウェル オートメーション ジャパン株式会社
問い合わせフォーム: https://www.rockwellautomation.com/ja-jp/company/about-us/contact-us.html

ロックウェル・オートメーションの強み、提供できる価値

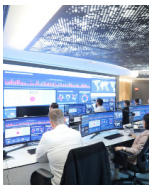
700+ グローバルのフィールド・サービス・リソース

300+ 専任コンサルタントとテクニカルリソース

120年以上の産業オートメーション経験

世界屈指のパートナと、カスタムソリューションを提供

豊富なグローバル展開の専門知識



頼りになるセキュリティ・オペレーション・センター

IEC62443・NIST標準ガイドラインに準拠した対策サービスを提供

識別	資産可視化	脆弱性評価	N/Wセキュリティアセスメント	リスクアセスメント	ペネトレーションテスト		
防御	N/Wセグメンテーション	産業用DMZ	OTデータセンター	セキュアなリモートアクセス	パッチ適用管理	エンドポイント保護	データバックアップ&リカバリプラン
検知	24時間年中無休のハードウェア監視サービス	24時間年中無休のセキュリティ監視サービス	アラート・レポーティング・サービス				
対応	インシデント対応、隔離・リスク緩和対応	コミュニケーション計画・実行					
復旧	復旧支援	調査・分析	改善計画				

サイバーセキュリティの標準規格・ガイドライン

経済産業省(産業サイバーセキュリティ研究会)「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」2022.11.16

IEC 62443

IEC 62443は、国際電気標準会議(IEC)とISA99によって共同で開発されたOTセキュリティの国際規格。組織、システム、コンポーネントを横断的にカバーしており、海外では国の標準ガイドラインのベースとしてIEC 62443を採用することが多い。

NIST

National Institute of Standards and Technology

米国国立標準研究所(National Institute of Standards and Technology: NIST)」が発行した国際標準。サイバーセキュリティを向上させるために、識別(Identify)、防御(Protect)、検知(Detect)、対応(Respond)/ 復旧(Recover)の5つのコアで構成されたフレームワークを提示している。