設 備 紹 介

生産工場のサイバーセキュリティ対策　～ファイアウォールの集中管理～

Cyber Security of Production Plants -Centralized Management of Firewall-

1. はじめに

今般，サイバー攻撃の脅威が生産工場の制御システムにまで及んでおり，実際に国内外の他社生産工場ではサイバー攻撃を受けた事案が発生している。こうした中，当社も制御システムサイバーセキュリティのガバナンス体制構築ならびにガイドライン制定などの取り組みを推進している[1]。当社が制定したガイドラインでは事務所等の情報系と装置やプラントの制御系ネットワークに接点がある場合，当該接点にファイアウォールを設置することを義務付けている。本項では，このファイアウォールの集中管理設備について紹介する。

2. 背景

2.1 ファイアウォールの導入

従来，制御システムは，閉じたネットワーク内での運用を前提としてセキュリティを確保してきたが，近年，生産管理システムなど情報系のシステムとの連携が行われるようになり，セキュリティ対策が急務となっている。しかし制御システムには「止められない」「変えられない」という特性があり，インターネット接続で自動更新される一般的なマルウェア対策ソフトウェアなどの対策を，そのまま適用することはできない。一方で，主なマルウェア等の脅威は情報系ネットワークとの接点から侵入することが想定される。そのため，当社では当該接点にファイアウォールを設置することでセキュリティを確保している。

2.2 集中管理の導入

一般的な生産工場においては，ファイアウォールは自工場で導入・運営管理を行う場合が多い。しかし，当社は生産拠点の数が他の製造業と比較して非常に多く，全ての生産工場に専門性を有する人員を配置することが困難である。加えて人員の課題だけでなく，ファイアウォールの運用には日々のログ確認などの運用管理が必要となる。そのため各生産工場のファイアウォールを大陽日酸ネットワーク上位のデータセンタにて集中管理する仕組みを導入し，効率的かつ確実な管理を実現した。

3. 設備概要

各生産工場の制御系ネットワークと情報系ネットワークの接点に設置したファイアウォールは，制御系ネットワークの防護壁の役割を担うとともに，データセンタに設置されている専用サーバにより集中管理されている（図 1）。これにより，日常の運用管理に加えログ収集やインシデント発生時のログ分析を迅速かつ一元的に行うことを可能にした。

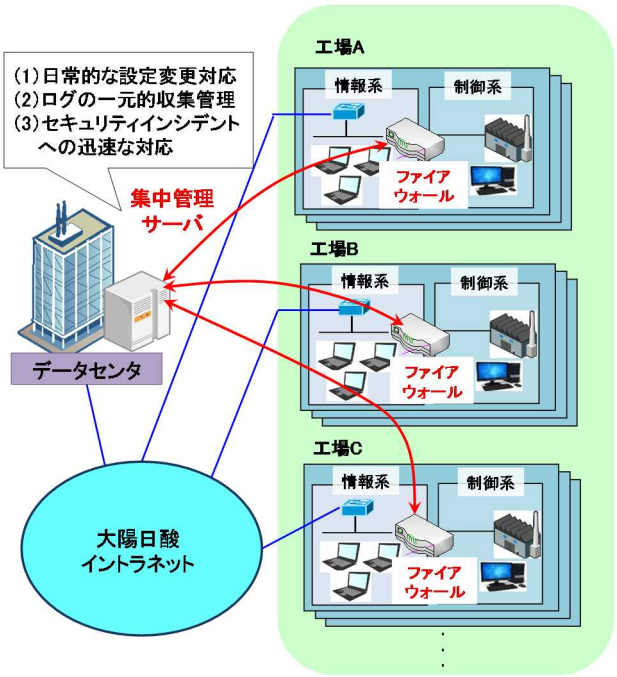

図 1 ファイアウォール集中管理の全体構成

4. まとめ

当社グループでは，「ガスを売ることは安全を売ること」の精神に則り保安管理を徹底している。サイバーセキュリティも保安管理の一つと捉え，今後もサイバー攻撃の高度化・巧妙化に耐えうる技術的安全対策を進めていく。

参考文献

1） 中辻利一. 制御システムサイバーセキュリティ対策の現状と今後. 計装.2018,vol.61,No.6,p38-39

（開発本部　デジタルソリューションセンター
デジタル革新推進部　企画推進課　　松島　洋輔）