1ZA-02

工場の IT・OT 分離ネットワークの効率的な運用方式

樋口 智之† 後藤 厚宏†
情報セキュリティ大学院大学†

1.はじめに

工場では、生産設備(OT)や IoT をネットワーク(NW)に接続し、モノづくり効率化や設備の保全管理などの取り組みも始まっている。工場では、既存の IT NW と OT や IoT NW を相互接続することで、普段利用している IT NW 上の PC やサーバーと OT・IoT NW 上の機器を通信させるという実現手段が考えられる。

「既存の IT NW を活用した NW 構築」を検討するにあたり、『NW 分離』[1]についても、見直しを行う必要が生じる [2][3]。その変化による課題を調査し、その課題を解決のための仮説を立て、その仮説が正しいかについても検証環境を用意し、検証を行う。

2. OT・IoT NW を IT NW に相互接続する際の分離要件と運用課題

表 1 対象とするNWの範囲と前提

#	内容
1	国内／海外に複数の工場を保有している製造業を対象とする
2	稼働中の工場に新しく OT NW および IoT NW を導入する
3	工場既存の階層 IT NW を活用し、OT および IoT NW との相互接続を行う
4	IT と OT・IoT NW 相互接続を行う場合は、機器停止時のリスクレベルに応じてゾーニングを行い、ゾーン間の NW は分離を行う
5	NW 分離を行う際は、ステートフルインスペクション型の FW(もしくは同等の機能を有する機器)を用いる
6	IoT NW のデバイスから、IT NW のサーバーに通信にしたり、IT NW の PC から、OT NW のデバイスに通信したり、双方向通信が行われる

IT NW 接続がある工場（表 1）にて、OT・IoT NW が導入され始めると、要件（表 2）を満たすために各建屋に Fire Wall(FW)を設置する図 1 のような NW 構成になると推測する。各建屋の NW の相互接続点に FW が必要になり、FW の管理台数が増加してしまう。それに比例して、デバイスに合わせた FW の通信許可ルールも増加してしまうことが懸念され、管理対象の FW 台数と通信許可ルールの増加による運用負荷が増大することが予測される。

表 2 NW 分離における要件

#	概要	詳細
機能面		
1	NW の分離	物理・論理的に IT と OT、IT と IoT の NW を分離でき、互いの通信を制限できること
2	通信制御	制限した NW 間はホワイトリスト型で、双方向の通信許可設定を行えること
3	移動する端末の通信制御	移動する端末についても、通信制御が実施できること
4	不正通信の検出・遮断	悪意のある内部犯行やマルウェアの不正通信を検出することができ、遮断ができること
5	アクセスログ	通信の履歴が取得できること
運用面		
1	実用性	すでに工場では、OT や IoT の NW 接続が始まっており、すぐに適用可能で運用が始められること
2	稼働実績	導入後、バグ、不具合等が無く、安定稼働ができること
3	設定変更対応	ユーザから利用したいというリクエストを受けると、すぐに利用できること
4	工数/コスト低減	NW 機器台数が増加し、NW 機器への設定変更時間が増大すると、運用工数/コストも比例して増えるため、抑制できること
5	変化最小限	できるだけ現在、保有している技術で運用がおこなえること
6	緊急対応	マルウェア感染時に該当機器がどこに通信できるかをすぐに取得できること。また、必要に応じて、速やかに通信の遮断・隔離が行えること
拡張性面		
1	事業対応	M&A、工場のフロア拡大やレイアウト変更等に柔軟に対応できること

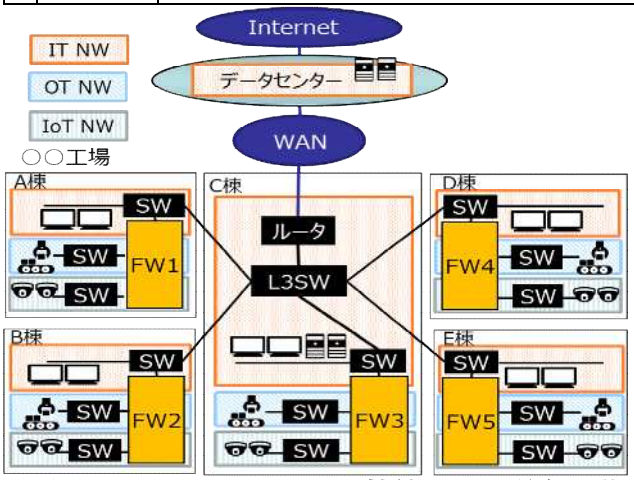

図 1 IT と OT・IoT の NW 接続がある場合の階層構造に基づいた NW 図

Efficient operation method of IT / OT separated network in factory
†TOMOYUKI HIGUCHI, ATSUHIRO GOTO
†INSTITUTE of INFORMATION SECURITY

3. 提案するNW運用課題の解決手法

工場のNW分離を行うためのガイドライン[4][5]などは充実してきているが、運用に移った後の考慮点などが不明瞭であるといえる。また、機能面での考察を行った研究はあるが、運用課題の洗出しと精査が不十分で、実用的であるとはまだ言い難い状況である。

特にNW分離後の通信制御の変更運用についての対策については述べられておらず、どのような実現方法が最適か不明確な状態である。NWのソフトウェア技術として、NETCONFとSDNでのソフトウェアによる自動化の検討を行なったが、SDNは工場への実用性や稼働実績が低いため、本研究では、NETCONFを用い、それぞれの運用のケースに応じて、通信制御の設定変更のために必要な情報を『FW通信制御ルール変更システム』に入力し、必要な承認を通すことで、NW機器上で必要な設定変更が自動で実施され、運用者の手を介さずにFWの通信制御ルールの変更を行う。

いずれのケースもNW分離の要件を満たし、NW運用者が手作業を行わずに、自動化を行い、完全性を担保できるかを検証する。

4. 運用課題の解決手法の実装と検証

前提となる工場を想定し、日常運用で考えられるFWの通信許可ルールの設定変更を検討した。

ⅰ. 新規端末接続
ⅱ. 既存端末変更
ⅲ. 既存端末取外し

本研究では、まず『ⅰ. 新規端末接続』について、FWの自動ルール変更の実装を行い、運用工数が削減できるか検証した。

予めFWや工場やNW情報をDBに登録した状態で、申請者が設定変更に必要なパラメータを入力することで、NW管理者の設定変更なしで、受け付けた申請の確認作業と承認作業のみを行い、NW管理者でFWの通信許可ルールを変更できることを確認できた。

自動ルール変更の実装にあたっては、FWの通信ルールの設定方法に無数の設定パターンがあり、人が管理しやすい設定パターン(表3)やソフトウェア観点から制御しやすい設定パターン(表4)があることが分かった。ただし、人が見て管理しやすい設定パターンはソフトウェア制御に適していない。変更が頻繁にしない場合の人手によるFW運用を考慮し、人がみても分かりやすく、かつソフトウェア制御に適した通信ルールの設定処理が必要であり、その両方を満たした設定変更処理と通信許可ルールの定義を行った。

表3 人の管理に適したFW通信許可ルール例

#	接続元	接続先	通信内容
1	IoT-Device1 IoT-Device2 IoT-Device3	Server-A Server-B	TCP/80 TCP/443
2	OT-Device1 OT-Device2	OT-Server	TCP/21

表4 SW管理に適したFW通信許可ルール例

#	接続元	接続先	通信内容
1	IoT-Device1	Server-A	TCP/80
2	IoT-Device1	Server-A	TCP/443
3	IoT-Device1	Server-B	TCP/80
4	IoT-Device1	Server-B	TCP/443
5	IoT-Device2	Server-A	TCP/80
6	IoT-Device2	Server-A	TCP/443
7	IoT-Device2	Server-B	TCP/80
8	IoT-Device2	Server-B	TCP/443
	・・・	・・・	・・・

5. まとめ

本稿では、工場におけるIoTとOTのITNWとの相互接続における課題を取り上げた。また、その課題の解決が期待できるFWの通信許可ルールのソフトウェア制御を行うことで課題解決の仮説を立て、NETCONFによるシステムの実装を行い、運用の効率化が図れるかの検証を行った。システムの実装にあたり、FWをソフトウェアで管理する場合と人が手動で管理する組み合わせの運用では、人とソフトウェアがそれぞれでFW機器を管理するために、最適な設定変更処理および通信許可ルールの定義が必要であることがわかった。

参考文献

[1] IEC, 62443-2-1 (JIP-CSCC100-2.0)
[2] アメリカ合衆国国土安全保障省(JPCERT/CC和訳), 制御システムのサイバーセキュリティ：多層防御戦略, 2006年5月
[3] IPA, 制御システムのセキュリティ分析ガイド, 2017年10月
[4] NCCIC/ICS-CERT, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, September 2016
[5] JPCERT／CC, 工場における産業用IoT導入のためのセキュリティ ファーストステップ, 2018年8月