グローバル製造業におけるOT/FAのセキュリティ対策課題と検証

Issues and verification of OT/FA security measures in the global manufacturing industry

梅田真子・システム分科会・情報セキュリティ大学院大学

Abstract

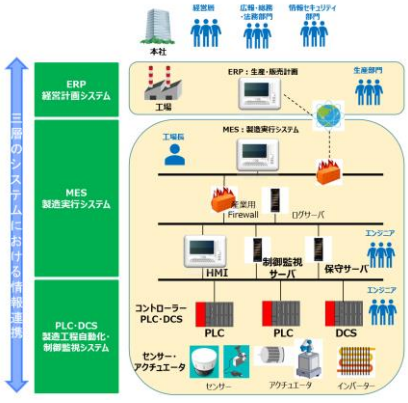
If the environment is not connected to a network, is information security protected? If technical security measures are in place, will there be any incidents in a networked environment? The answer is NO. This is because it is humans who construct the environment, and human errors will always occur there.

In this study, we examine how to prevent human errors and take effective countermeasures in OT/FA environments of manufacturing industries from the viewpoint of information security governance. As the final result of the research, we plan to present a checklist of security measures and a flow diagram, but this time we report on the proposed items to be included in the checklist.

1.研究背景

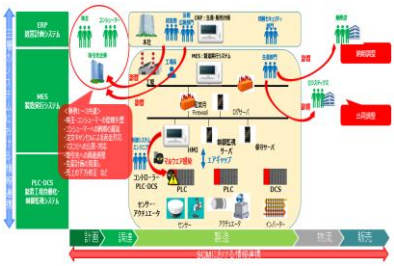
- 生産・販売計画の自動化（FA：Factory Automation）を含む運用技術（OT：Operational Technology）は、システムや通信がクローズドな環境からオープンな環境へ変化している。また、顧客サービスの向上や新規事業の拡大に伴い、IoT化が進められてきた。
- OT環境の変化とIoT化によるオープンなネットワーク環境への変化により、製造業はサイバーリスクが年々上昇傾向にある。そこで、過去に発生した製造業におけるサイバー攻撃事例を検証することにより、課題や対策の傾向が見えてくるのではないかと考えた。
- 事例を検証していくうちに、セキュリティリスクの課題は、独立した要因によるもはなく、情報セキュリティガバナンス（環境・教育・体制）全体で要因を捉え、対策を打つ必要があることがわかった。
- これを踏まえ、本研究においては、「情報セキュリティガバナンスの観点より、組織が具体的に行うべく対策を提言としてとりまとめること」とした。
- 提言の方法としては、要件をチェックリストで提示し、組織間連携を図やフローチャートで提示する。

2.OTにおける3構造：検証モデル



Reference Architectural Model Industrie 4.0 (RAMI4.0)の多層構造概念を用い、経営計画システム（ERP）、製造実行モシステム（MES）、製造工程自動化・監視システム（PLC・DCS）を3層に構造化し、検証モデルとして作成した。

3.検証と見直し案



①過去、製造業を狙ったサイバー攻撃事例を検証モデル上で検証

	情報システム（IT）	制御システム（OT）
優先順位	・CIAの機密性（Confidentiality）が重要視される（情報が適切に管理され、情報漏洩を防ぐことを重視）	優先順位	・CIAの可用性（Availability）が重要視される（システムが継続して安全に稼働できることを重視）
運用管理	情報システム部門	運用管理	現場技術部門
セキュリティの対象	情報	セキュリティの対象	モノ（設備、製品）サービス（連続稼働）
技術サポート期間	3~5年	技術サポート期間	10~20年
可用性	再起動は許容範囲のケースが多い	可用性	24時間365日の安定稼働（再起動は許容されないケースが多い）

②セキュリティ観点においてOTはITとどのような観点の違いがあるかを整理

	対策課題	対策見直し案
1.組織全体	危機管理体制の見直し・再構築・適正な運用の確認の実施	IT環境とOT環境の違いを把握したうえで、OT環境が組織全体にもたらす影響を見直す <確認ポイント> ①世の中の動向に合わせて、Availability（可用性）が脅威される主な要因を把握しているか （環境：情報収集と情報共有） ②組織全体で危機管理体制が確立されているか、既に確立されていても現状に応じ更新されているか （体制：体制の確立） ③制御システムの運用におけるリスクアセスメントを行い、実態把握と従業員のリスク認識を分析しているか （教育：リスク分析と教育）
2.社長（経営層）工場長	経営層、工場長の危機管理体制に対する積極的な関与と指示の実施	経営層自らによる組織内のコミュニケーション活性化とセキュリティ対策への予算確保を行う <確認ポイント> ①組織内の情報連携・情報収集においては、日ごろから縦横の垣根を超えたコミュニケーションの活性化が重要となる。このため、組織内のイベント等を通じて経営層が従業員と、また従業員同士の交流の場を設け積極的に参加しているか ②経営層は組織全体のセキュリティ体制構築を推進し、自ら指示をおこなっているか
3.情報セキュリティ部門	（情報セキュリティ教育とは別に）制御システムにおけるセキュリティ教育の実施	IT、OTの特性に合わせたセキュリティ教育担当・体制を確立する <下記いずれかを確認> ①情報セキュリティは情報セキュリティ部門が主担当、制御システムセキュリティは技術部門が主担当となり、双方が窓口としてセキュリティ教育・体制に取り組む →さらに、情報セキュリティ部門が全社的なCSIRTを構築し、技術部門がOT-SIRTを構築するなどの独自体制をとっているか ②技術部門から情報セキュリティ部門へ担当者を移籍させ、情報セキュリティ部門が窓口一本となり部内でセキュリティ教育の展開を計画する →さらに、組織全体でCSIRTを構築しているかどうか
4.現場技術部門	制御システム固有に起こりうるリスクの洗い出しとセキュリティ教育の実施	取り扱う制御システムやUSBメモリ、PC接続に対するセキュリティマニュアルの整備や遵守状況のアセスメントチェックシートの整備を行う <確認ポイント> ①制御システムの運用におけるリスクアセスメントを行い、実態把握と従業員のリスク認識を分析しているか

①の検証と②のOTのセキュリティ観点より、組織全体/社長（経営層）・工場長/情報セキュリティ部門/現場技術部門の各役割に対する、それぞれの対策課題と対策見直し案<確認ポイント>を導き出した。

4.今後について

- ✓ 3章で検証し導き出した対策見直し案（以下、「案」と記載）に加え、計画・調達・製造・物流・販売（SCM：Supply Chain Management）5つの横の連携構造の観点を考慮し、案の精査を行う。
- ✓ 案をチェックリストにまとめヒアリング準備を進めるとともに、有識者への調査協力の依頼をお願い、実施後の結果まとめ、再検証を行う。