O-008

製造業の OT/FA における情報セキュリティガバナンスへの提案
Proposal for Information Security Governance in Manufacturing OT/F

梅田　真子†
Naoko Umeda

1. はじめに

近年，日本の製造業へのサイバー攻撃がニュース報道により目にする機会が増えている．IT 調査会社 IDC Japan が，国内 443 社に対して行った調査結果によると，『IoT/IIoT，OT に関わるシステム特有のセキュリティ事件／事故を 36.4%の企業が経験』と発表した［1］．

製造業の OT/FA における体制や構造は各企業の製造部門により異なるため定義が難しく，セキュリティガイドラインの発行を困難なものにさせている．本研究では，IPA の制御システムの構成［2］を参考に作成した構造イメージをもとに，過去のインシデント事例を当てはめ検証・分析することで，経営層や工場長向けの「OT/FA のサイバーセキュリティチェックリスト」として提案する．

2. 対象とする OT 環境と研究方針

本研究は，製造業において組織内に工場を保有する，大企業及び中小企業（小規模事業者を除く）の「加工・組立てメーカー」を対象とする．また， OT 環境の一要素として浸透した産業システム（ICS）が， スマートセンサー，スマートアクチュエータなどの IT ソリューション（IIoT）を活用し，機械とシステムが自動的に情報共有・分析するようになっていることから IIoT も対象要素として取り扱う．

3. OT/FA におけるセキュリティ要件のリスト化

3.1 インシデント事例

過去発生したインシデント事例より，OT/FA に関連し影響が異なる以下 3 つの事例をモデルケースとして取り扱う．[3][4][5]

事例(1)2010 年イラン核施設 USB 経由のマルウェア感染

・ドイツ SIEMENS 社製 プロセス制御システムを標的としたマルウェア Stuxnet による核施設の操業が一時停止した

事例(2)2018 年 日本半導体工場 USB 経由のウイルス感染

・ ウイルス感染による工場の品質検査システムへの影響により，不良製品の出荷や生産ラインが停止した

事例(3)2021 年 アメリカ水処理施設ソフトウェア脆弱性攻撃

・ リモートアクセス用ソフトウェアの脆弱性を悪用し，アクセス権を奪取したうえでデータを改ざんした

3.2 脅威の分析

これらの事例をビジネスインパクトの視点より脅威分析を行ない，導出した対策課題を以下に記す.

➢ **組織全体に対する脅威**

従来の工場の生産活動では，閉域網による閉ざされた通信であったため，可用性を担保し，生産ラインを止めないことが最優先されてきた．しかし，近年 情報システムとの接続経路やリモートメンテナンスなど，通信や接続経路に変化が生じ，機密性や完全性という点も十分考慮し対策を講じる必要性が出てきた.

事例(1) ビジネスインパクト

マルウェア攻撃による制御システムへの感染の広がりにより，工場の制御システムの稼働が停止に追い込まれ，Availability（可用性）が阻害された

事例(2) ビジネスインパクト

ウイルスが品質を管理する制御システムに侵入し正常に機能しなくなった場合，品質不良の製品が出荷され，Integrity（完全性）が阻害された

事例(3) ビジネスインパクト

攻撃者の不正アクセスにより，制御システムのアクセス権が奪われ，Confidentially（機密性）が阻害された

➢ **経営層や工場長に対する脅威**

社会的な企業イメージのダウン

・事例(1)生産ラインの停止による納期遅延とそれによる生産計画の下方修正
・事例(2) 品質不良の製品を出荷したことによる製品回収のためのコスト発生
・事例(3) 制御システムのデータ改ざんによる製品安全性への不安や実被害

➢ **運用に対する脅威（情報セキュリティ部門）**

事例(1)～(3) ビジネスインパクト

「OT 固有のリスク」「OT 環境の変化」を理解せずセキュリティ対策が未対策のまま放置されることによる，安全への侵害・生産ラインの停止など

➢ **運用に対する脅威（現場技術部門）**

事例(1)～(3) ビジネスインパクト

・制御システムにおける，破壊，暗号化，アクセス権奪取，データの改ざんなどにより，制御システムの使用停止や制御不能な状態に陥る
・また，それによるシステムの再構築や新規システムへの入替えなど想定外のコストが発生する恐れがある

3.3 対策要素

脅威分析よりそれぞれの対策課題として挙げられる案を以下に記す.

➢ **組織全体に対する必要な対策：危機管理体制の強化・重要資産の防衛強化**

IT 環境と OT 環境の違いを把握し，OT 環境が組織全体にもたらす影響を見直す

➢ **経営層・工場長：危機管理体制に対する積極的な関与と指示**

†情報セキュリティ大学院大学　Institute of Information Security

経営層自らサイバーセキュリティ対策予算や組織内コミュニケーションの活性化へ積極的に関与する

- **情報セキュリティ部門：OT 環境に対するセキュリティ知識の強化教育の実施**
  教育：制御システムに携わる従業員向けのセキュリティ教育・研修プログラムを実施する
  体制：OT 環境におけるセキュリティ体制を確立する（CSIRT/OT-SIRT/F-SIRT の構築など）
  規程・ルール：OT/FA におけるセキュリティ基準の整備と標準化を行う
- **現場技術部門：制御システム固有のセキュリティ技術対策**

OT 環境特有のセキュリティリスクに対する技術対策を，セキュリティ評価結果の重要度レベルに応じて優先度を付けて対応する

4. セキュリティ対策と追加要件の検討

4.1 OT ガバナンスにおけるセキュリティ要件の作成

4.1.1 経営者の 2 原則

危機管理体制の強化・重要資産の防衛強化

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

- 世の中の動向に合わせて，OT 環境における CIA が阻害される主な要因を把握すること（国内外の情勢把握）
- 組織全体で危機管理体制を確立し，現状に応じて更新すること （体制の確立または見直し）
- OT 環境におけるリスクアセスメントを行い，重要資産の把握とそれに対する運用実態のリスク分析をすること（リスク分析）

改善に向けた積極的な関与と指示

経営層自らサイバーセキュリティ対策予算や組織内コミュニケーションの活性化へ積極的に関与する

- 情勢，体制，リスク分析を踏まえた改善計画を指示すること
- リスクジャッジやサイバーセキュリティ対策の投資において，バランスを保った判断や予算配分を行うこと
- また，サイバーセキュリティ対策に関わる予備費を確保すること
- 日ごろから組織内の垣根を超えたコミュニケーションの活性化を図り，経営層が従業員の声に積極的に耳を傾けること

4.1.2 OT/FA 固有のセキュリティ要件リストの作成

本節では，OT/FA 環境における固有のセキュリティを検討するために最低限必要とされる項目をリストとしてまとめた．

教育

① OT 環境に携わる従業員向けに，OT 固有*のセキュリティリスクに関する教育を実施すること
② OT における重要資産の取り扱いルールや基準を決め，関係者へ周知すること

体制

③ OT 環境を踏まえたインシデント対応チーム，体制を確立すること

規程・ルール

④ 全社に共通するセキュリティ規程を整備・展開すること

技術対策：MES

⑤ 不要なアプリケーションの禁止措置を行うこと
⑥ USB メモリの禁止や代替措置を取り入れること
⑦ 保守 PC を接続する際には，マルウェアなどの簡易ウイルス検査を実施すること

技術対策：PLC・DCS

⑧ 制御システムにおけるデフォルトパスワードは必ず変更してから使用すること

技術対策：ネットワーク

⑨ 外部からの不正侵入を防ぐために，制御装置ネットワーク上に産業用ファイアウォールを設置すること
⑩ OT/FA の構成見直しや構成管理をすること
⑪ FA の無線 LAN 環境を保護すること
⑫ IIoT 機器を監視し，異常を早期発見できるような対策を行うこと

技術対策：システム全体

⑬ サイバー攻撃や内部不正に備え，ログ収集・分析を行なうこと

5. 有識者インタビューと今後について

4 章にて作成した OT ガバナンスと OT/FA 固有のセキュリティ要件のチェックリストについて，大手製造業 2 社の有識者にご協力いただき，インタビューを行ったところ，記載項目や内容については概ね賛同いただいた．

そのほか，「予算確保とリスク判断のためには，一定のベンチマークが必要であり，それをもとに精度の高い企画を行うことで初めて経営層のリスク判断が可能になる」というコメントをいただいた．OT 環境の技術対策には，全社で本格的な対策を実施すると規模によっては，数億から何百億単位のコストがかかるため，世界動向も含めた最新のセキュリティ動向や最新の技術対策，ベンチマークについても成熟度モデルのような指標が必要ということがわかった．また，近年セキュリティ対策は経営層の判断として投資の意味合いがあったが，今後は世界情勢を踏まえると企業必然的防衛の色合いが強くなるのではないかと感じた．今後，本提案内容の評価を行っていただく予定となっており，インタビューでいただいた貴重な意見を反映できるよう検討を進めたい．

参考文献

[1] IDC, “2021 年 国内企業の IoT/OT セキュリティ対策実態調査結果 ” https://www.idc.com/getdoc.jsp?containerId=prJPJ47631521
[2] 独立行政法人情報処理推進機構(IPA), “重大な経営課題となる『制御システム』のセキュリティリスク” (2015) P.9
[3]福田俊博, “工場・プラントのサイバー攻撃への対策と課題がよ～くわかる本” (2015)秀和システム, PP.96-99
[4]池上雄太, “河田芳秀, “制御システムセキュリティ入門” (2020)NTT 出版, PP.96-99
[5]IPA “「制御システム関連のサイバーインシデント事例」シリーズ”,
https://www.ipa.go.jp/security/controlsystem/incident.html
（2022 年 5 月 3 日時点）