FAOPセキュリティモデル研究会の専門委員会への変更提案
（企画部会案 2025年6月23日）

FA運2025-1-5-1

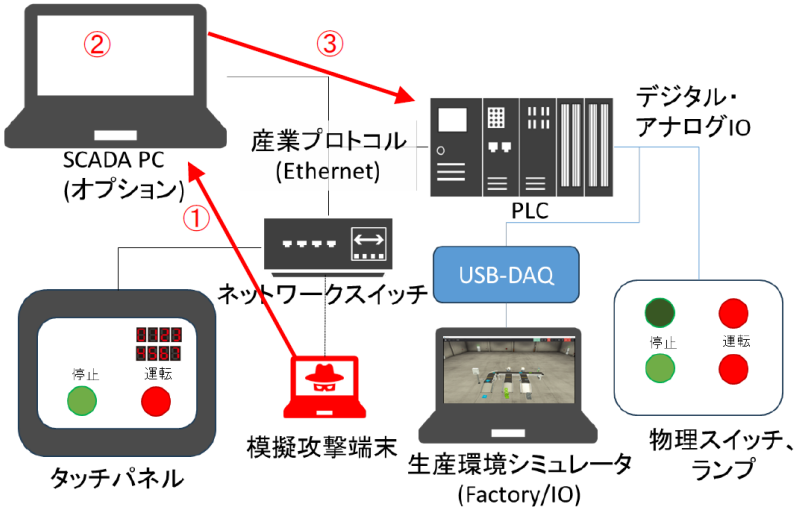
提案1： FAOPセキュリティモデル研究会(委員長　澤田先生)を専門委員会に移行する

背景： 2021年度に研究会として発足し、勉強会と並行しながら当初提案のセキュリティ検証用ベンチマークモデルの実試作機が2024年度に完成し、5月に関係者にお披露目された。研究会設置時に目的とした”候補テーマの調査”(＝研究会)は完了し、事実上“具体的テーマの調査、研究”(＝専門委員会)の段階に到達しているので、企画部会としてこれを提案する。
今後FAOP会員企業による実証を進め狭義の貢献をすすめると共に、更に外部に対して働きかけを行い参画の輪を広げ、会員の拡充や数による実証の確度を高めて会員にも貢献できることが期待される。(具体的には今回情報開示の制限も条件としながらNEDOの懸賞金プロジェクトに応募した)

提案2： 会則　第11条の3項は削除する

背景： 現在当該研究会委員は一般会員4者、情報会員1者、学術会員1者で構成されているが、会則に記載のある一般会員5者以上の要件は満たされていない。現在FAOPの一般会員は5企業・1法人の構成であり5者以上を必須とすると一般会員はほぼ全ての活動に委員として参加しなければならず柔軟な活動を阻害する恐れがある。本来この規定の趣旨は特定の会員だけの利益に偏らないようにとの趣旨であるが、運営委員会にて決定することと規定されているのでそこで歯止めがかかりその趣旨は保たれるため、第11条の3項は削除することを提案する。
今後の研究会・プロジェクト・専門委員会の決定と活動を、柔軟かつスピード感をもって対応されることが期待される。

(参考資料)FA運2025-1-5-1 FAOPセキュリティモデル専門員会提案書
FA用3Dシミュレータを活用した
セキュリティ検証用機器（デモ機）の構築



・仮想化された製造制御装置および製造ラインを用い、事前に用意された複数のサイバー攻撃シナリオを実行・再現することで、攻撃の挙動とその影響、対策効果を可視化するシミュレーション環境である。
・本システムは、製造業におけるDX推進計画策定時や、製造設備の設計・導入前の段階、またはサイバーセキュリティ教育の一環として活用される。主に生産システムエンジニア、情報システム部門、経営者層などが対象となり、仮想環境内でリスク評価と対応策検討、トレーニングを行う。

デモ機で実現したい事

- 本デモ機を使った研究会活動では以下の達成を目指す.
  - 仮想製造環境におけるセキュリティ攻撃の再現機能
  - 攻撃の影響や脆弱性箇所の可視化
  - 対策実施前後の挙動比較機能
  - セキュリティ教育用シナリオと操作ガイドの提供
- 関係者間でのセキュリティリスクと対策への共通理解を促進し、DX推進に必要な合意形成を加速することが期待される。
- 本提案ではスーツケースで持ち運び可能な可搬型模擬プラントを利用し、3つの攻撃シナリオでのトレーニングが現状可能となっている。今後、このシナリオを本プログラムで潤沢にしていく。
  - シナリオ例1(SCADA端末乗っ取りによる不正プログラムの不正書き込み)
  - シナリオ例2(マルウエア感染を想定したトラフィックストーム)
  - シナリオ例3(中間者攻撃による操作・監視妨害)