制御システムの情報セキュリティ

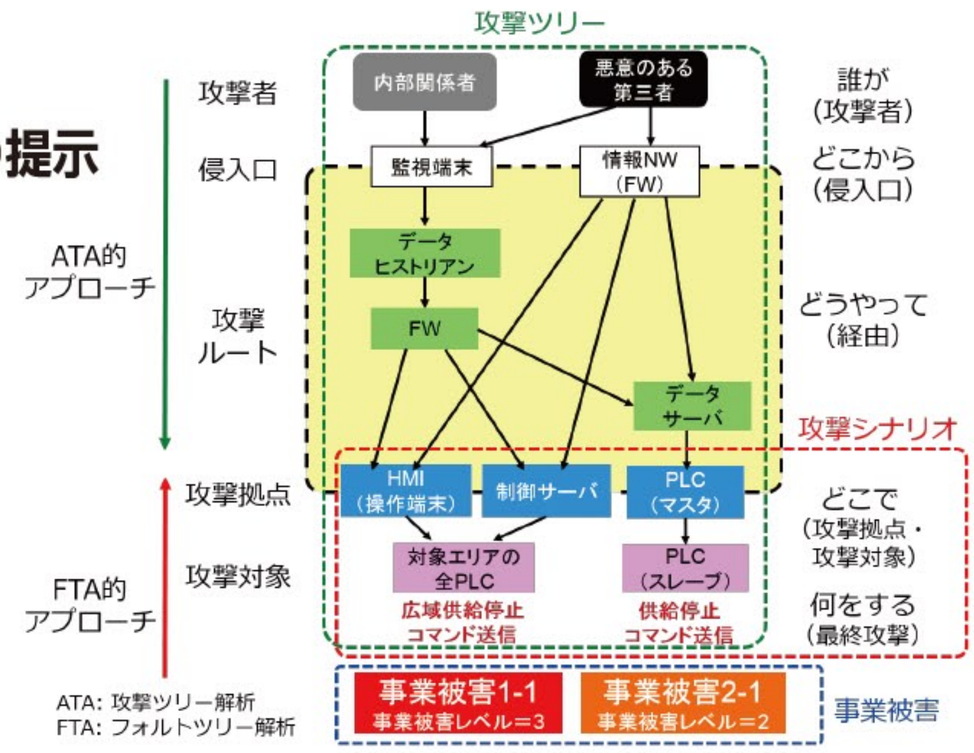
制御システムへのサイバー攻撃の脅威

- 制御システムの安全神話の崩壊
  - 汎用プラットフォーム（Windows, UNIX）や標準プロトコルの採用
  - 外部ネットワークとの接続（遠隔監視／遠隔管理、リモートメンテナンス）
  - 記憶媒体の持込みによる外部とのデータ交換
  - 攻撃者による制御用通信プロトコルの理解
- 最近のインシデント事例
  - 電力システムへのサイバー攻撃による大規模停電（2015年・2016年、ウクライナ）
  - 自動車の生産管理システムのランサムウェア感染による生産停止（2017年、日英仏）
  - 安全計装システムへの攻撃（2017年、サウジアラビア）

制御システムのセキュリティリスク分析ガイド

- 制御システムのセキュリティの抜本的向上を可能とするために重要な位置付けとなるセキュリティリスク分析ガイド
  - リスク分析の全体像の理解向上と取り組み促進
  - リスク分析を具体的に実施するための手順や手引きの提示
- ２通りの詳細リスク分析の手法を解説
  - 資産ベースのリスク分析
  - 事業被害ベースのリスク分析

- リスク分析のための素材の提供
  - リスク分析シート（フォーマット、実施例）
  - 脅威（攻撃方法）や対策の一覧
  - 特定対策に関する詳細チェックリスト
  - 工数低減手法の提示
- リスク分析結果の活用例の提示
  - リスク低減の対策強化策の検討方法
  - セキュリティテストの解説



【ガイド本編】

【別冊】

【早分かり 活用の手引き】

制御システム利用者のための脆弱性対応ガイド 第３版

- 制御システムのリスク
- 制御システムに関して経営者がすべきこと
- 制御システムのセキュリティ対策のポイント

制御システムのセキュリティリスク分析ガイド
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

制御システム利用者のための脆弱性対応ガイド 第３版
https://www.ipa.go.jp/files/000058489.pdf