情報系資産を扱うレガシー制御システムのセキュリティ

Security Analysis of Legacy Industrial Control System dealing with Information Assets

情報セキュリティ大学院大学　　法制・倫理分科会　　井澤 佑介

研究背景

制御システムの社内NW接続によるIoT推進

レガシー制御システム

- 保守が終了した解消困難なセキュリティリスクの多数保持
- 社内NW接続を考慮しない設計・環境のシステムの存在
- 従来は**可用性リスク**における分析を実施

機密性リスクにおける脅威分析・対策例示

脅威分析

STRIDE

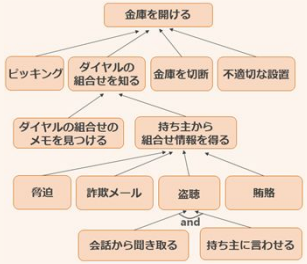
6種の脅威の可能性を判断する分析手法

想定される脅威	
S poofing	なりすまし
T ampering	改ざん
R epudiation	否認
I nformation Disclosure	情報漏えい
D enial of Service	サービス拒否
E levation of Privilege	権限昇格

	S	T	R	I	D	E
外部エンティティ (外部との接続サーバ)	○		○			
プロセス (サーバ/PC)	○	○	○	○	○	○
データフロー (ネットワーク経路)		○			○	○
データストア (サーバのストレージ)		○			○	○

Attack Trees

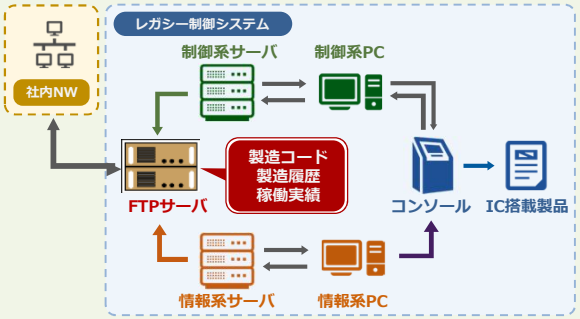
脅威の関係性をツリー構造により図示



想定するレガシー制御システムの社内NW接続例

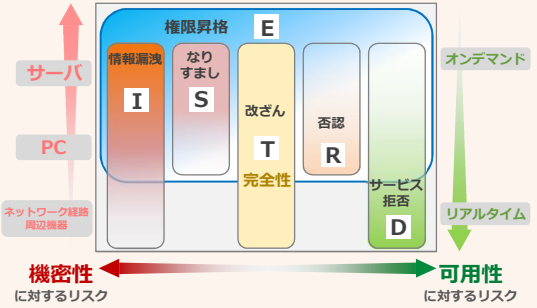
FTPサーバによる社内NWとのデータ共有

- 「製造コード」「製造履歴」を「情報系資産」に設定
- 制御システムからFTPサーバへの一方向通信

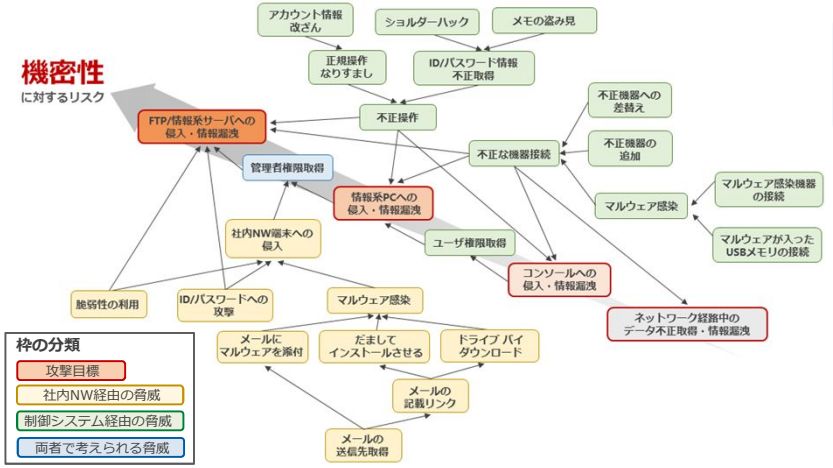


STRIDEを用いたリスク整理

機密性: 権利を保持しない者に情報開示しないこと
完全性: 情報やシステムが完全であること
可用性: 情報やシステムを必要なときに使用できること



分析結果（Attack Trees のグラフ例）



レガシー制御システムの社内NW接続における機密性リスクの分析

分析に基づいた具体策の検討(本文)

今後の展望

分析内容・対策例の妥当性検証