ネットワーク接続を考慮したレガシー制御システムにおける脅威分析と対策の評価

Threat Analysis and Countermeasure Assessment in Legacy Industrial Control Systems with Network Connection

情報セキュリティ大学院大学　　法制・倫理分科会　　平澤 凌一

研究背景

スマート工場化に伴うレガシー制御システムの
セキュリティリスク増大

↓

具体的なシステムの脅威分析と対策評価
実施対策選定のための指標の提案

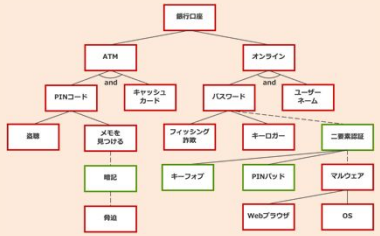
脅威分析

STRIDE

脅威カテゴリ	
Spoofing (なりすまし)	Information Disclosure (情報漏洩)
Tampering (改竄)	Denial of Service (サービス拒否)
Repudiation (否認)	Elevation of Privilege (権限昇格)

6つのカテゴリに沿って脅威の洗出し

Attack-Defense Trees



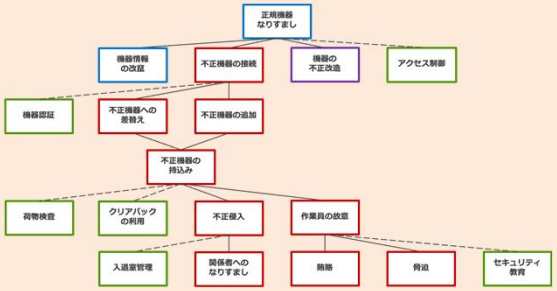
攻撃手段と防御策をツリー構造で可視化

脅威分析結果例

STRIDE

S:正規操作なりすまし
　正規機器なりすまし
T:情報資産/センサ信号の改竄
　アカウント情報/機器情報の改竄
R:操作履歴の削除
I:機密情報の漏洩
D:制御端末の制御不能
E:管理者権限の不正取得

Attack-Defense Trees



制御システムに特有なものも含んだ脅威の洗出し
脅威を実現させうる攻撃手段と防御策を視覚的に関連付けて把握

セキュリティ対策の評価例

脅威		情報資産の改竄	操作履歴の削除	正規操作なりすまし
対策		バックアップ	アクセス制御	多要素認証
実施時の影響		低	中	高
実施時のコスト		低	低	中
CVSS環境値	対策後	4.6	6.0	6.4
	対策前	7.6	7.6	7.6
CVSS基準値		8.7	7.4	7.8

実施時の影響とコストの観点および対策前後のCVSS環境値により評価