コントローラに対する ホワイトリスト式サイバー攻撃検知

電気通信大学
i-パワードエネルギー・システム研究センター
准教授　澤田賢治

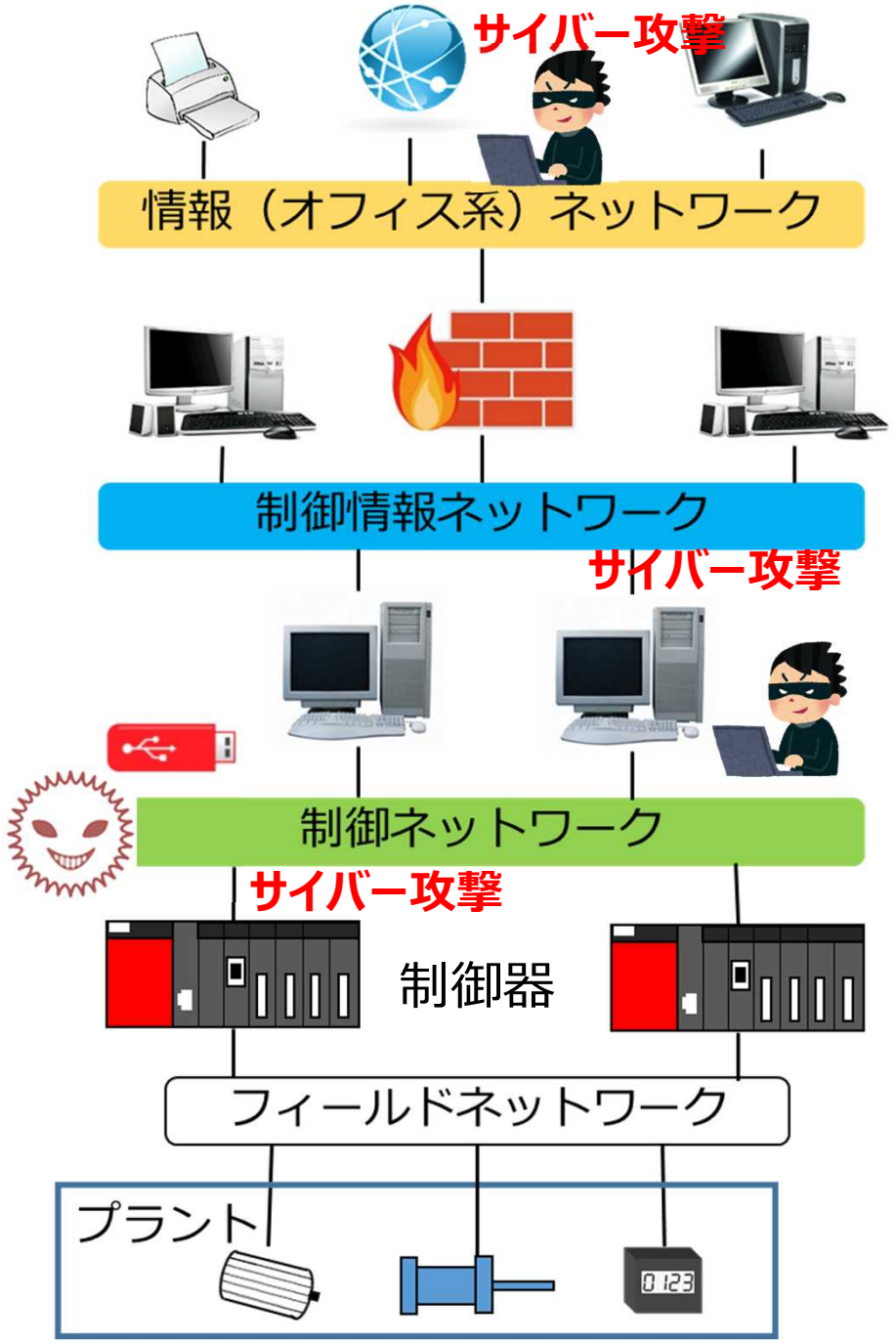
2019年5月14日

制御システムにおけるサイバーセキュリティ問題

重要インフラ
発電所，工場，化学プラントなど

サイバー攻撃(ほぼ全てのレイヤ)

物理的な影響



- 2010年

イランのウラン濃縮施設 ”Stuxnet”

- 2015年･2016年

ウクライナ電力会社へのサイバー攻撃

- 2017年以降

ウクライナ地下鉄

WannaCry，ランサムウェア

従来技術とその問題点

項目	情報系	制御系
寿命	2-3年 Multiple vendors	20年ほど Single vendor
更新時期	定期的	機器更新時，非定期的
遅延	可（金融系は除く）	不可
可用性	非連続	24x365 (連続)
セキュリティ意識	中程度	Poor
セキュリティ試験	定期的（標的型メール等）	機会があれば．．． （PoCレベル）

制御システムへのセキュリティ機能実装の問題点

- セキュリティ機能が，制御性能，安全機能，実装コストの足を引っ張らないか？（制御ユーザの懸念事項）．
- 可用性を担保しつつ，長寿命なセキュリティ機能の保証が必要（加速化・多様化するサイバー攻撃との矛盾）．

課題解決の指針：ホワイトリスト

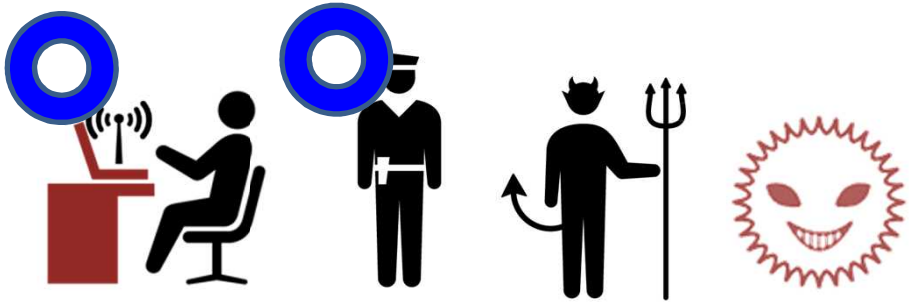
ブラックリスト型

実行不可の通信・プログラムのリスト化

- **常に最新の**パターンファイル更新が必須
- スキャン時のシステム負荷：**高**

ホワイトリスト型

実行可の通信・プログラムのリスト化



- **機能・構成変更時**にパターンファイル更新が必須
- スキャン時のシステム負荷：**低**

多くの制御システムは「ホワイトリスト」が有効

- レガシー問題（古いOS，最新プログラム動作保証外）
- 高負荷なウィルススキャンが不可能

例：アラクサラ「AX2530S」

制御ネットワーク用L2スイッチ
ホワイトリストの自動生成機能を有する

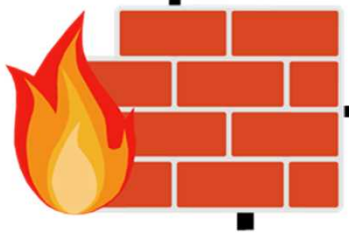
http://www.alaxala.com/jp/news/press/2015/20150525.html

従来のホワイトリスト製品

操作端末系
ウィルススキャンソフト

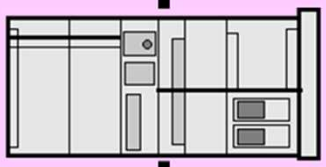
IDS
IPS

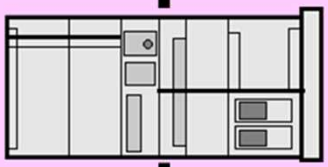
ホワイトリストスイッチ



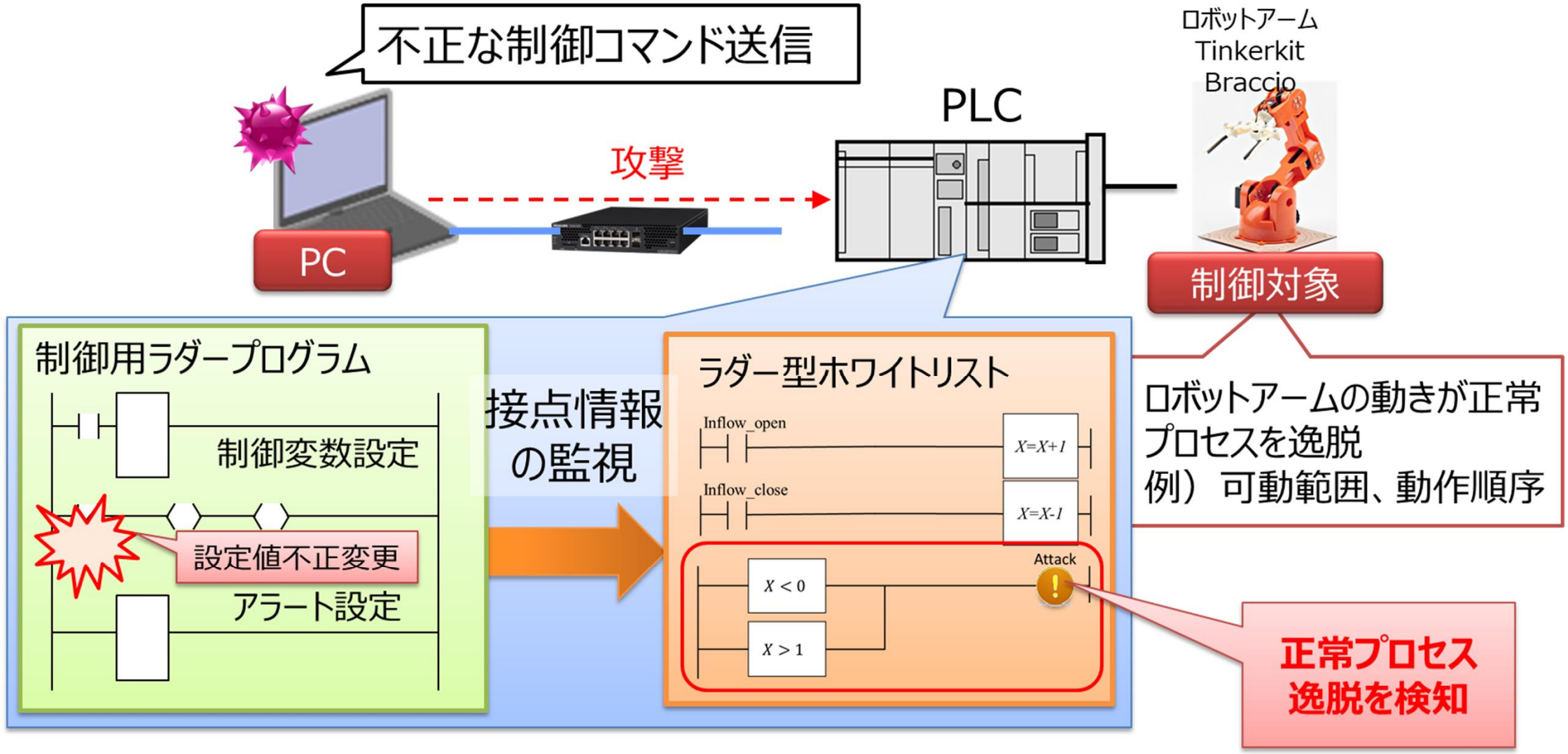
ファイヤーウォール

間接的な防御領域





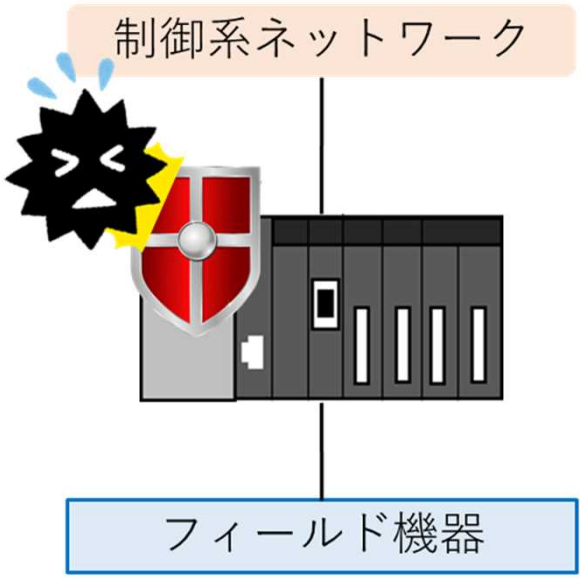
新技術の概要：コントローラ用ラダー型ホワイトリスト



- 種類：Programmable Logic Controller（PLC）
- PLCの制御プログラム「ラダー言語」でホワイトリスト機能を実現し，**ファームウェアの変更無し**で既存の制御システムに実装可能
- PLC のメイン制御機能への影響が低い.

なぜコントローラホワイトリストなのか？

◎コントローラはフィールド機器を守る最後の砦



上位ネットワーク層が攻撃されても

コントローラが正常ならば

フィールド機器も正常に動作する

◎PLC自体の汎用性の高さ

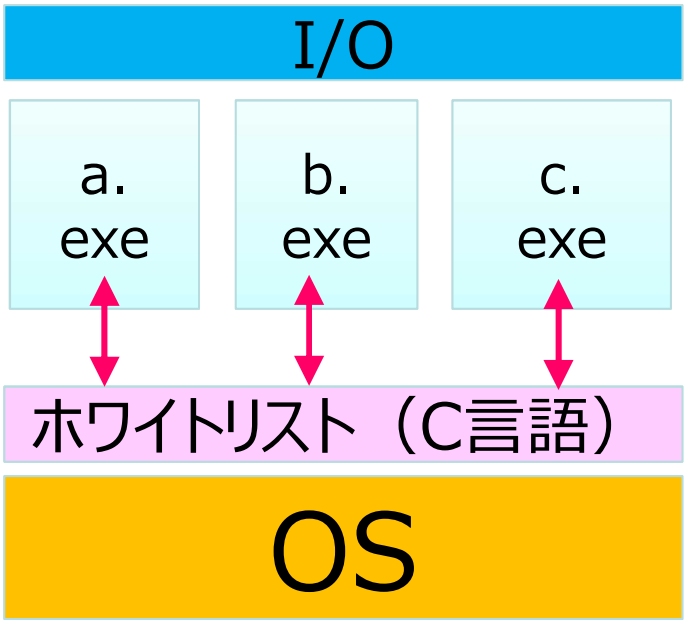
- 一般家電製品，自販機，信号機，ビル，工場，発電所，変電所
- 年間180万台の販売台数（2006年時点）

◎ホワイトリストはコントローラとの相性がよい

- コントローラのリアルタイム性を損なわない
- リストの作成が容易でかつ更新頻度が少ない

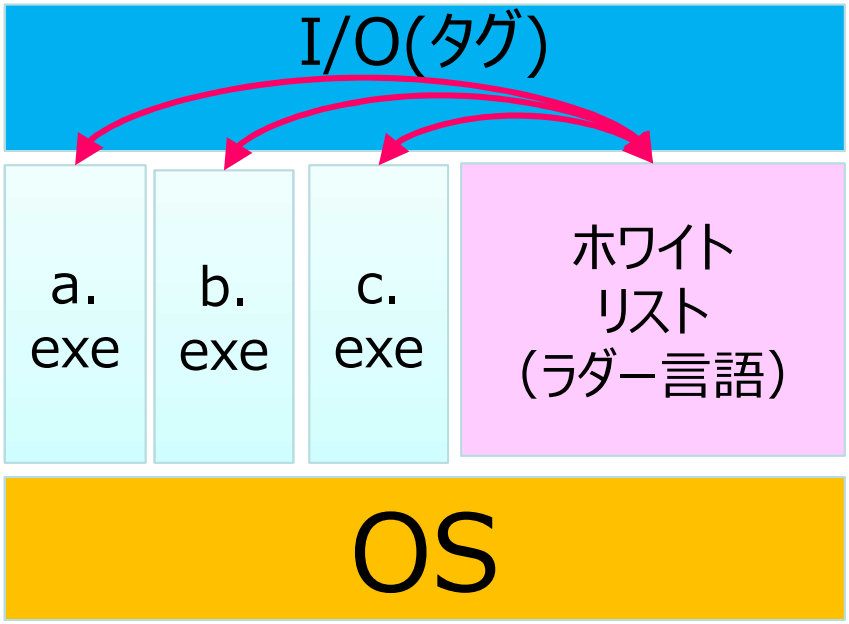
新技術の特徴・従来技術との比較

従来型



アプリケーションの一部

提案手法



プログラムの一部

ホワイトリスト機能のラダー言語実装の特徴

- ベンダーに依存しない実装
- 既存のアーキテクチャの変更いらず

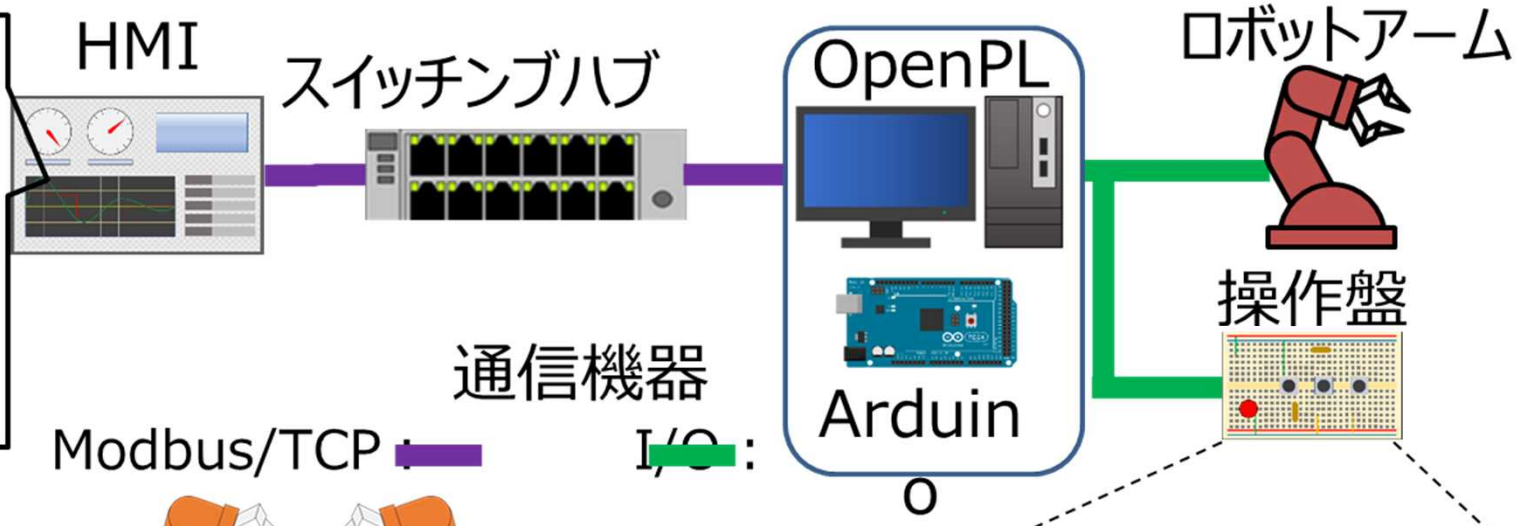
新技術の特徴・従来技術との比較（詳細）

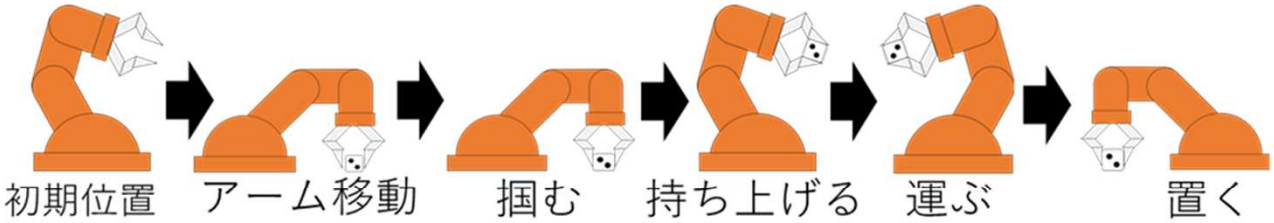
- 既存のコントローラのハードウェア・ファームウェア構成を変えることなく，適用可能である.
  - C言語実装の従来型ホワイトリストをラダー言語稼働のPLCに実装するには，ファームウェア変更が必要.
- セキュリティ機能による検知負荷はメイン制御機能に影響が低い，リアルタイムで異常を検知可能である.
  - セキュリティ機能がラダー言語実装のため，PLC の処理機能との親和性が高い.

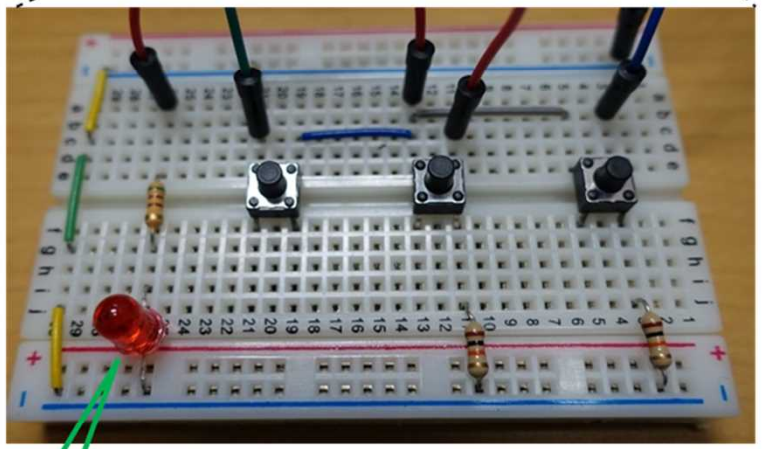
テストベッド検証

送信
- 電源ON/OFF
- 動作開始/一時停止
- システムのリセット

受信
- 各サーボの角度
- LEDのON/OFF
- ロボットアームの現在の状態

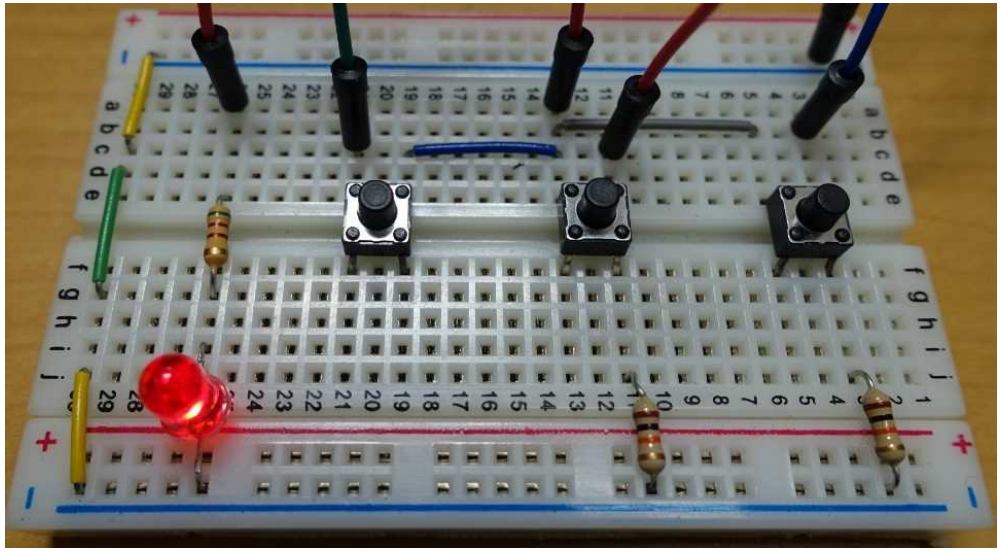




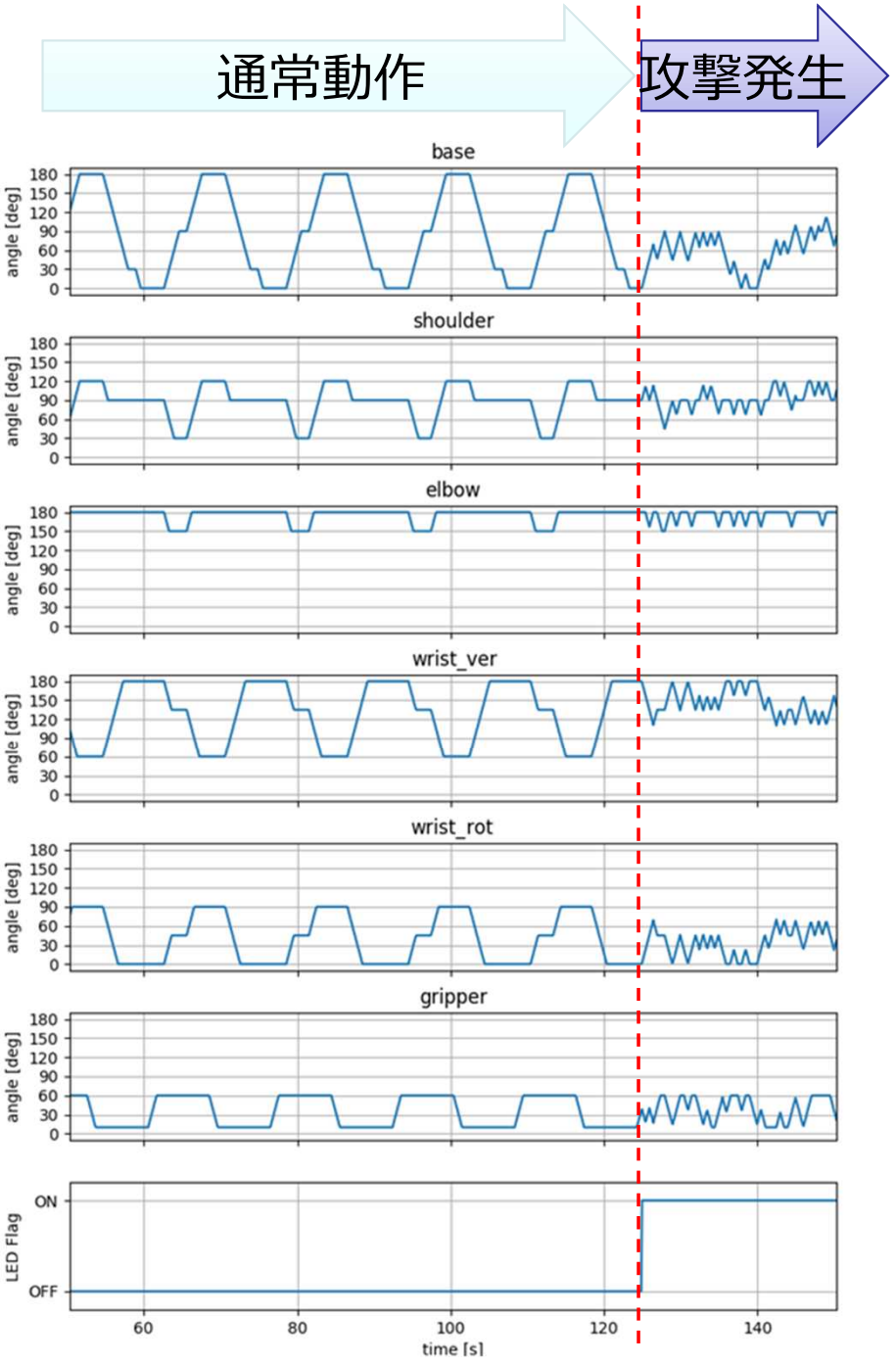


攻撃検知時にLEDが点灯

テストベッド検証



攻撃を検知しLEDが点灯



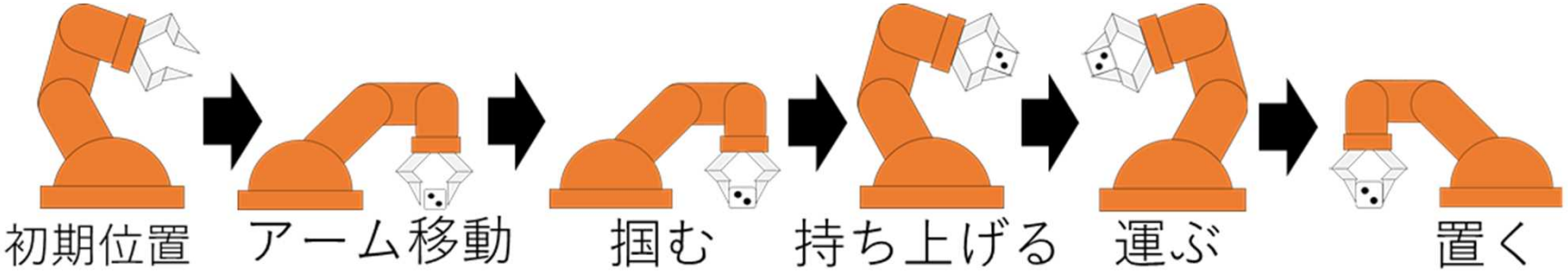
参考：他のテストベッドでの負荷

	ホワイトリストなし	ホワイトリストあり
プログラムサイズ	234.071kB	235.712kB
メモリー占有率	4.23%	4.26%
オブジェクトサイズ	1.496kB	3.248kB
オブジェクトメモリー占有率	0.04%	0.08%
総ステップ数	39	144
最大スキャンタイム	0.40ms	0.40ms
最小スキャンタイム	0.27ms	0.28ms

技術の概要：ロボットアームの例

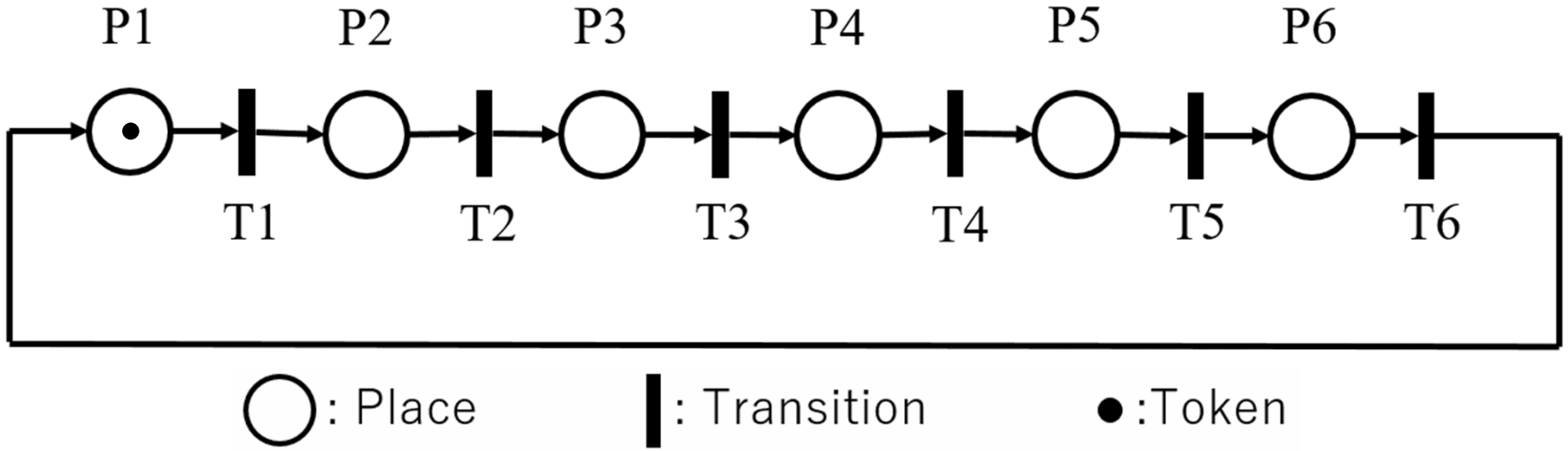
制御システムのセンサとアクチュエータに着目した状態遷移をホワイトリストとして定義

- ブロック運搬の順序



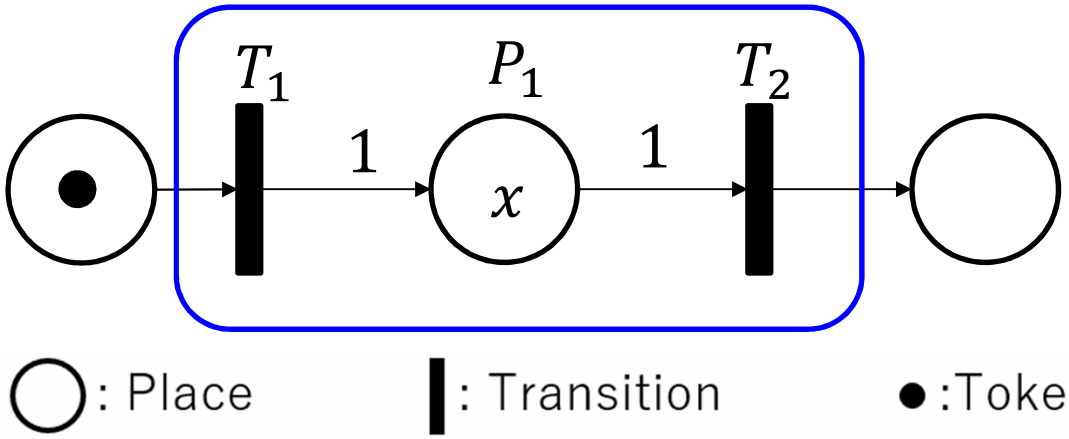
モデル化

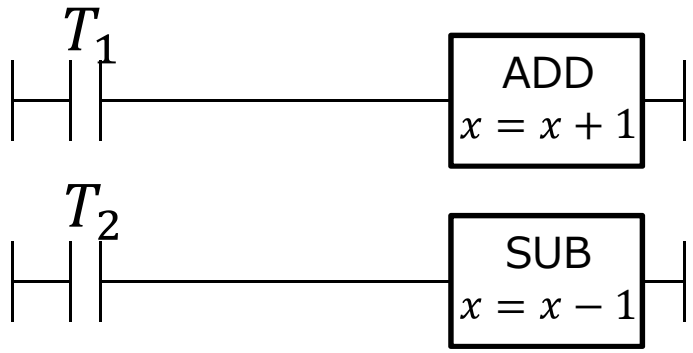
- ペトリネットモデル



技術の概要：ロボットアームの例

- リスト機能：トークンの移動による状態遷移を表現

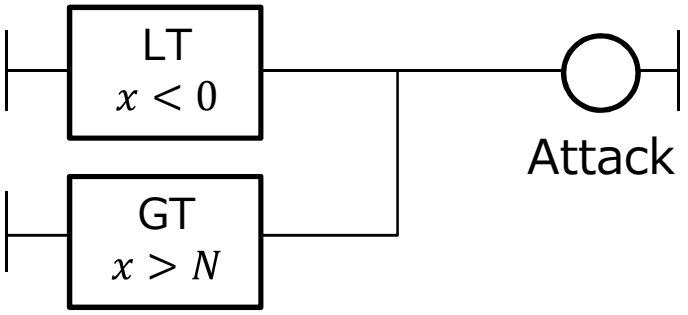




$x \in [0,1]$：トークンの有無

- スキャン機能：トークン移動が逸脱していないかを監視

$x < 0$もしくは$x > 1$なら異常

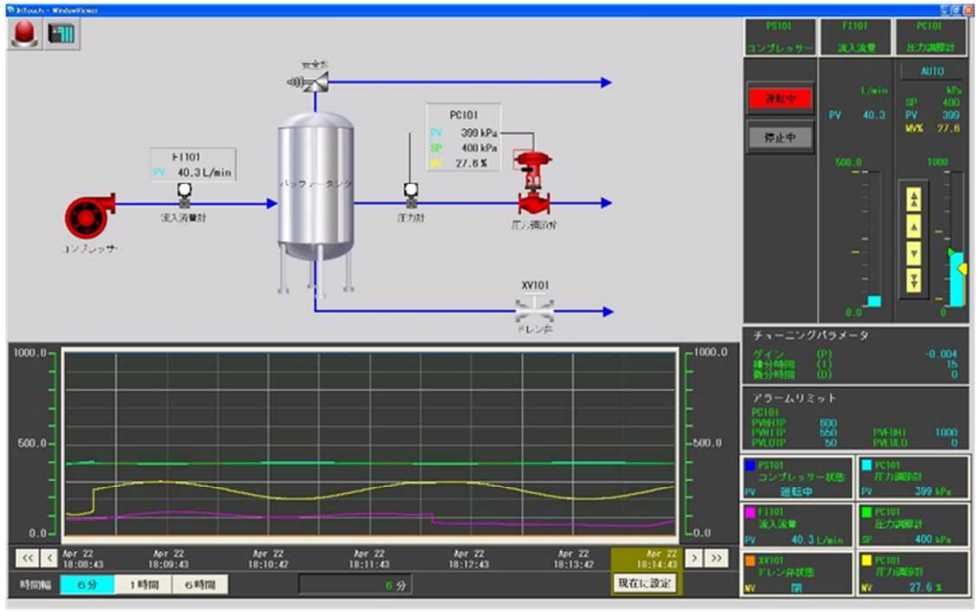


トランジションの発火順番や発火遅延時間もラダー言語で表現可能

模擬プラントでのPoC検証

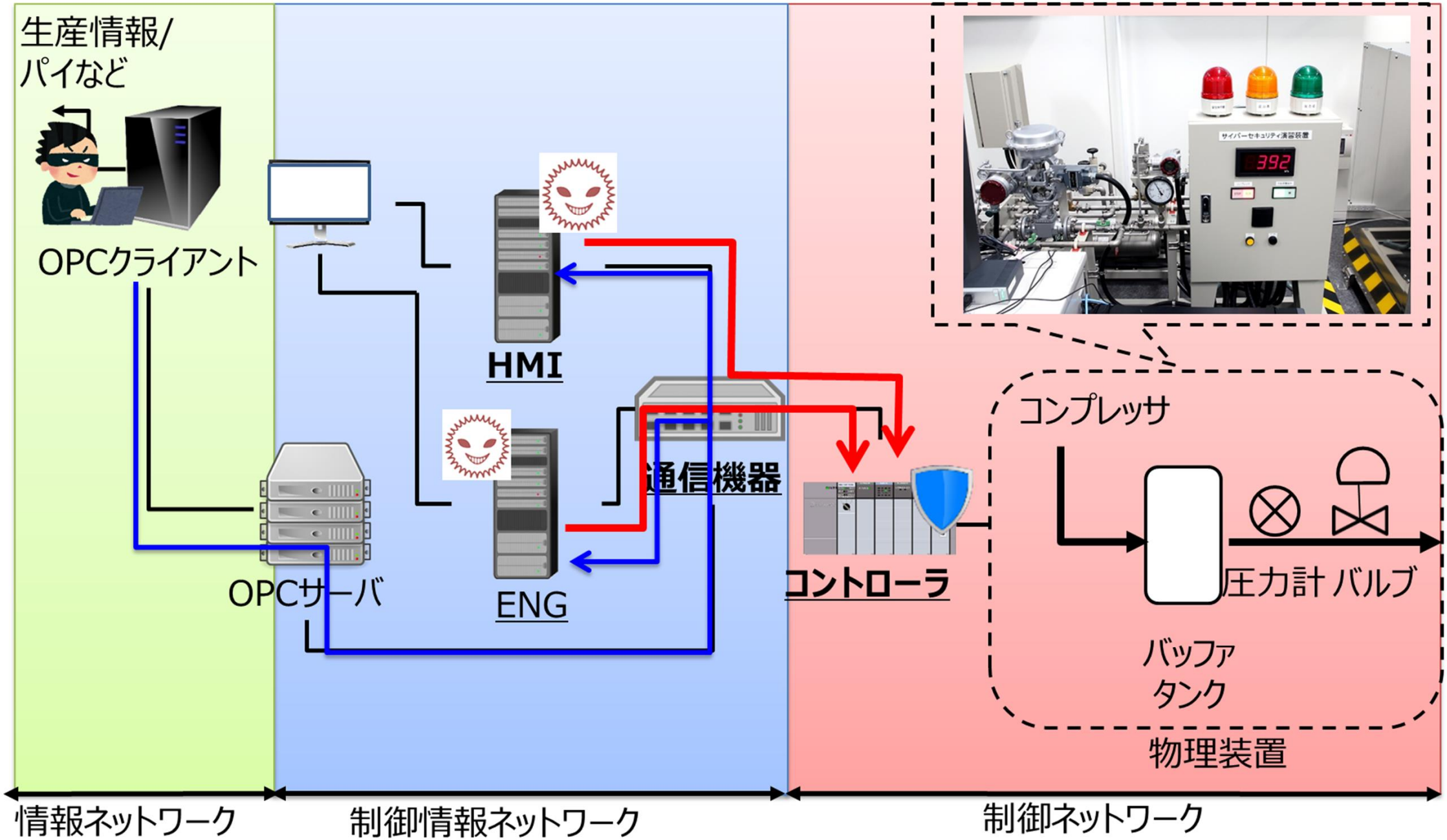
- 技術研究組合制御システムセキュリティセンター（多賀城市）のガス模擬プラントを利用.
- ガス製造工場の一部機能(圧力制御部分)を切り出しており，PLCやオペレータステーションなどを備えている
- 圧力制御1ループ構成で，サイバー攻撃などの影響を判別しやすい

模擬プラント



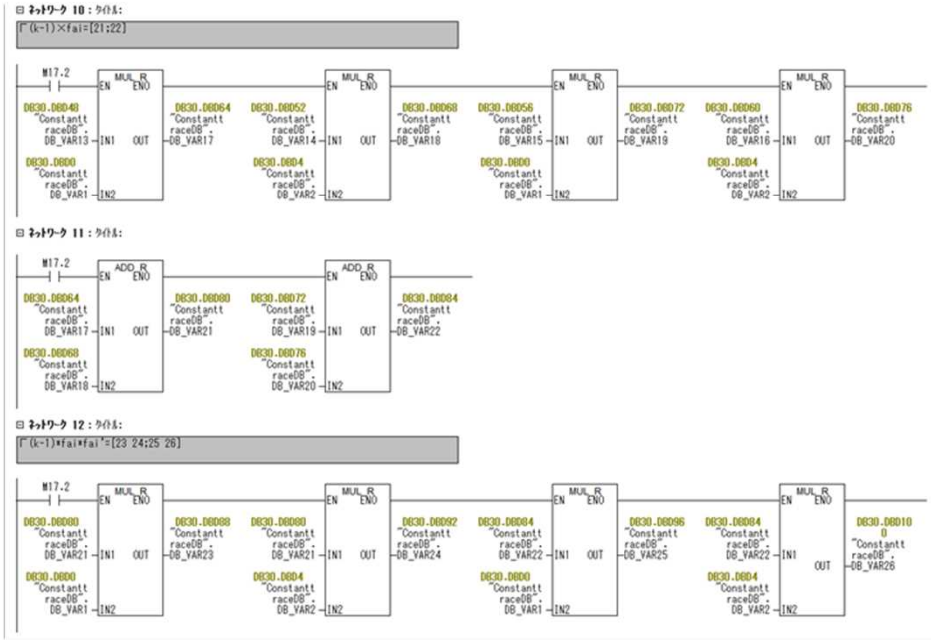
HMI画面

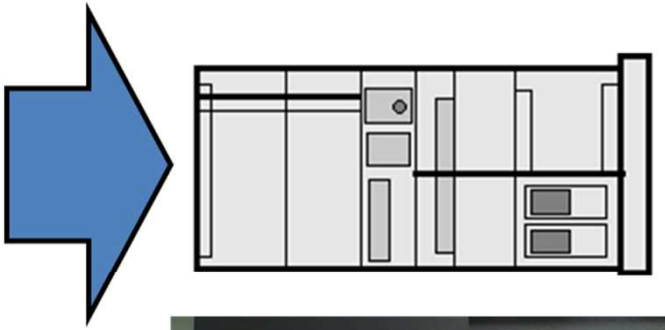
模擬プラントでのPoC検証（シナリオ例）

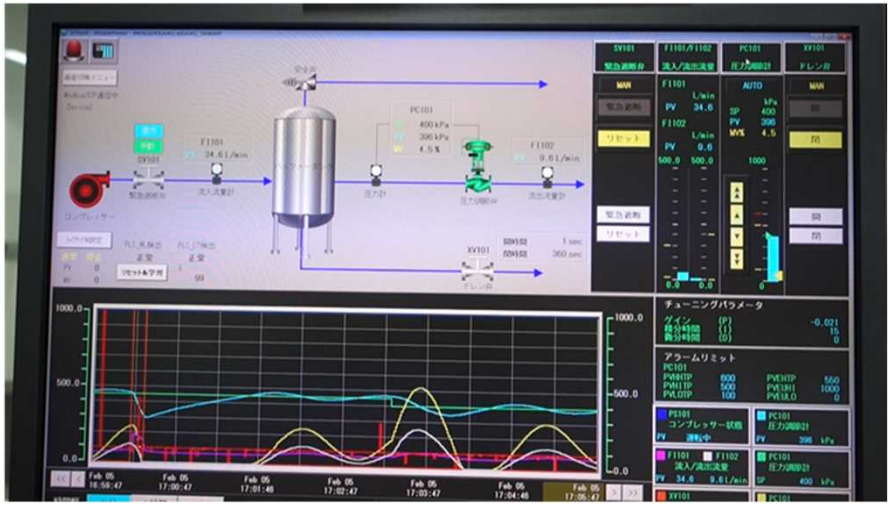


学習型ホワイトリストのPLC実装

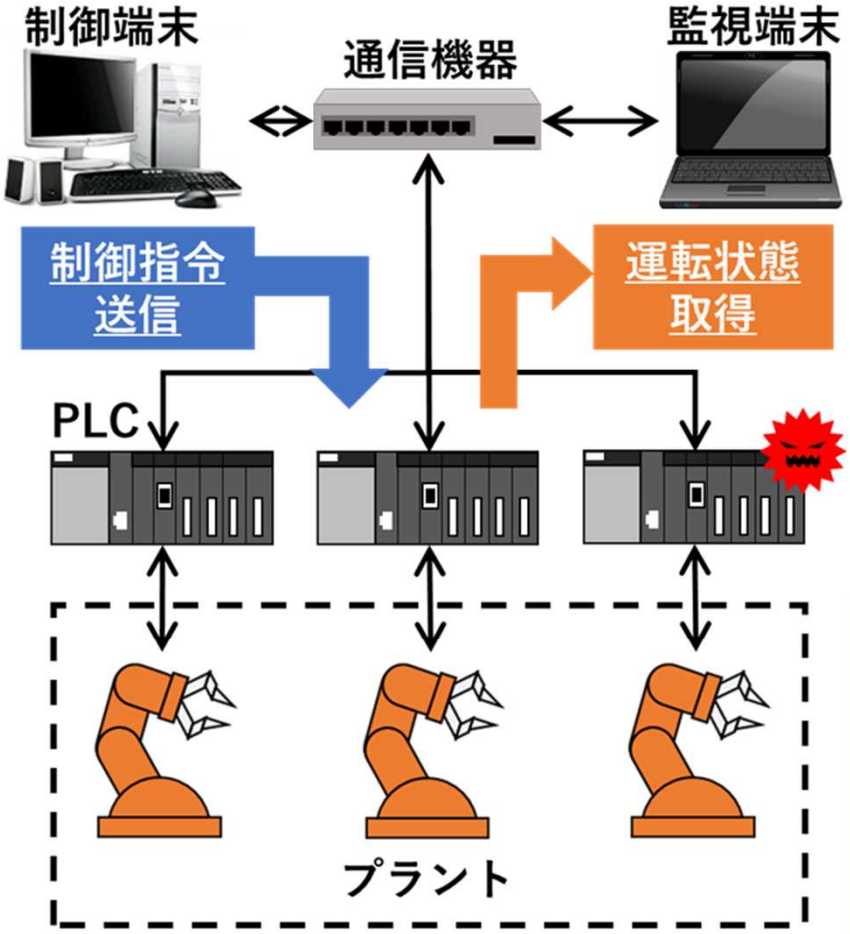
- アクチュエータの制御指令値とそれに対するセンサ計測値からホワイトリスト（正常振る舞いモデル）を自動学習
- 学習した正常振る舞いモデルの変化をホワイトリストからの逸脱として検知
- **学習アルゴリズムは全て「ラダー言語」実装**

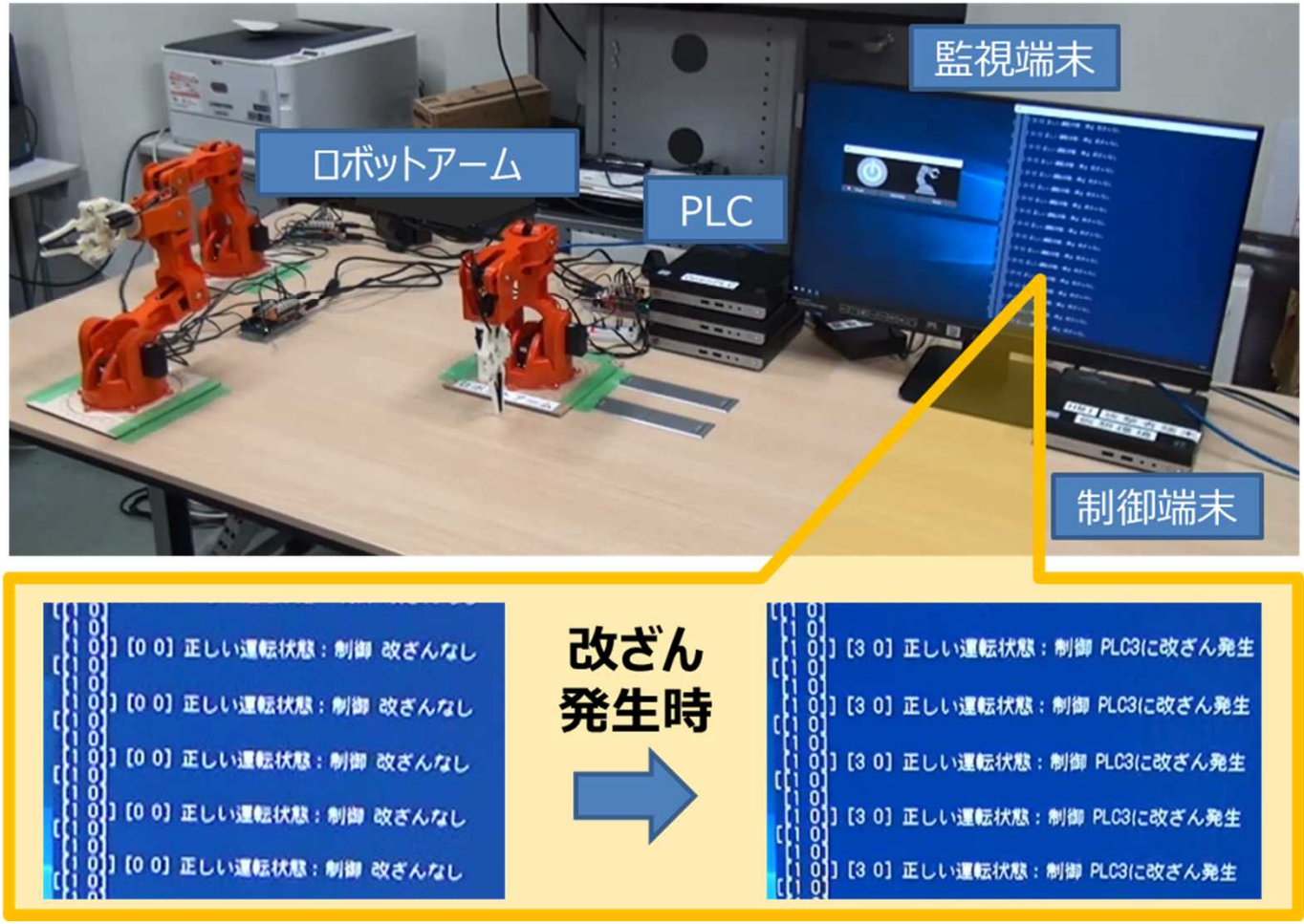






コントローラホワイトリストの状態管理





分散型台帳技術の部分的実装

- コントローラホワイトリストの動作状態を監視端末により制御
- 攻撃によりホワイトリスト単体としての検知機能を失っても，監視端末が異常を検知し正常な状態へ回復させる．

コントローラホワイトリストの関連技術

- **ラダー型ホワイトリスト**：基本形，シーケンス制御向き
- **学習型ホワイトリスト**：応用系，フィードバック制御向き
- **コントローラホワイトリストの状態管理**：複数のコントローラホワイトリストを同時管理するための技術
- **ラダー型ホワイトリストの自動生成**：PLC内のラダープログラムからホワイトリストを自動生成
- **ラダー型ホワイトリストの正当性検証**：ホワイトリストが正しく動作するかの検証
- 他，2019年以降，逐次情報公開予定

想定される用途

- シーケンス制御が多用されるFactory Automationシステムに適用可能である.
- Process Automationなどのフィードバック制御に適用可能である.
- ラダー言語で運用されている産業用コントローラへ適用可能である.
- エンジニアの誤操作の防止にも適用可能である.

実用化に向けた課題

- 汎用化から高機能化・カスタマイズ化へ
  - 根本的なファームウェア更新，C言語実装，仮想OS，冗長化などによる高精度化
- ホワイトリストの更新方法
  - 外部機器とのセキュアな接続による更新
- 自己監視から相互監視へ
  - 分散型台帳技術の完全実装

企業への期待

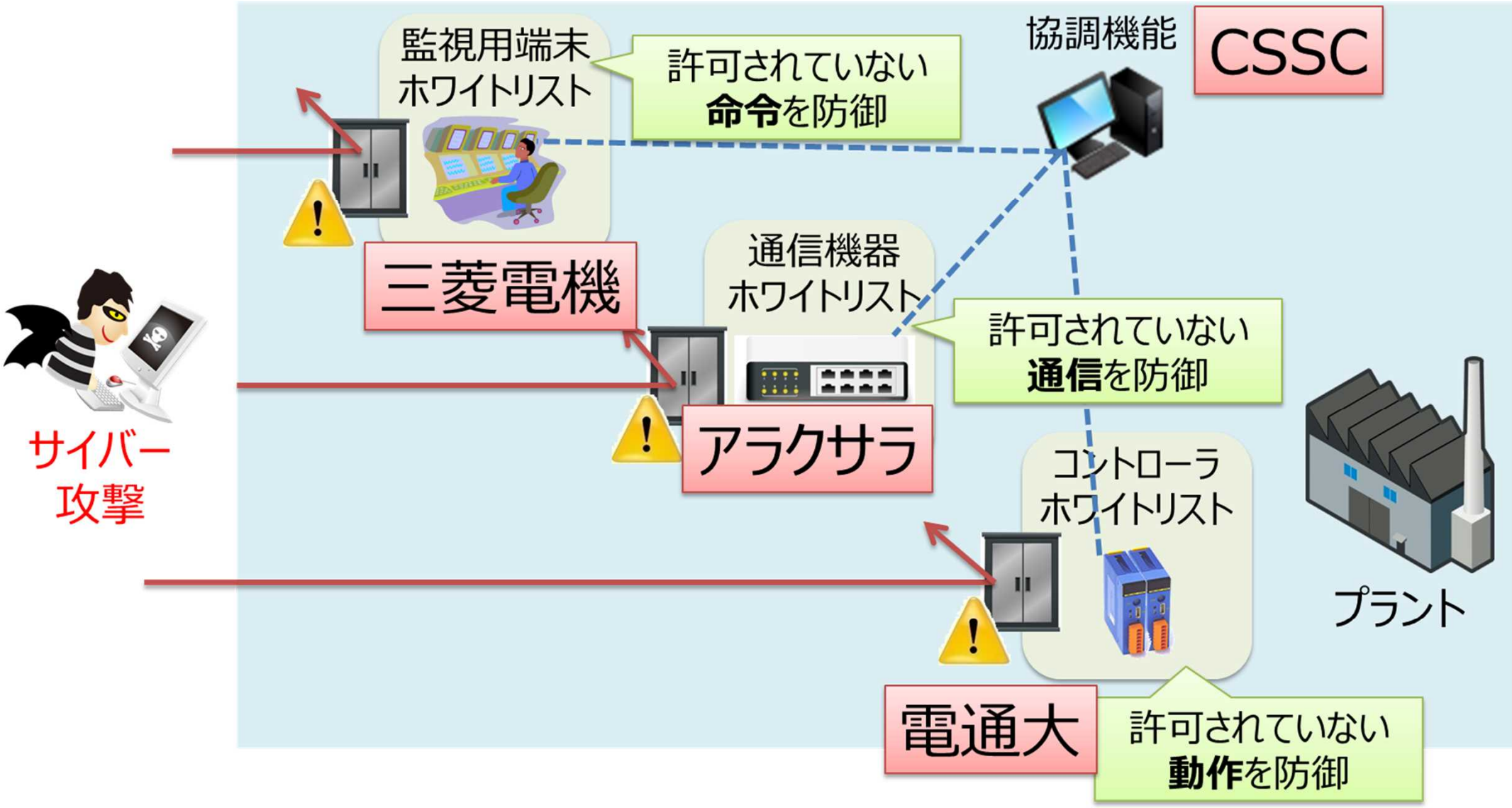
- PLCを開発している全てのベンダーに本技術の導入は有効と思われる.
- 汎用化を目指した故に犠牲にした機能があるので，**ある分野に特化したホワイトリスト機能**を開発したい企業との共同研究を希望.
- **仮想OS技術や冗長化技術**を持つ企業との共同研究を希望.
- PoC環境のある企業との共同研究を希望.

産学連携の経歴

- 総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）によって実施中
- 協調型ホワイトリスト技術：技術研究組合制御システムセキュリティセンター，アラクサラネットワークス，三菱電機，電気通信大学の共同研究
- こちらの内容で興味をもった方もご連絡ください.

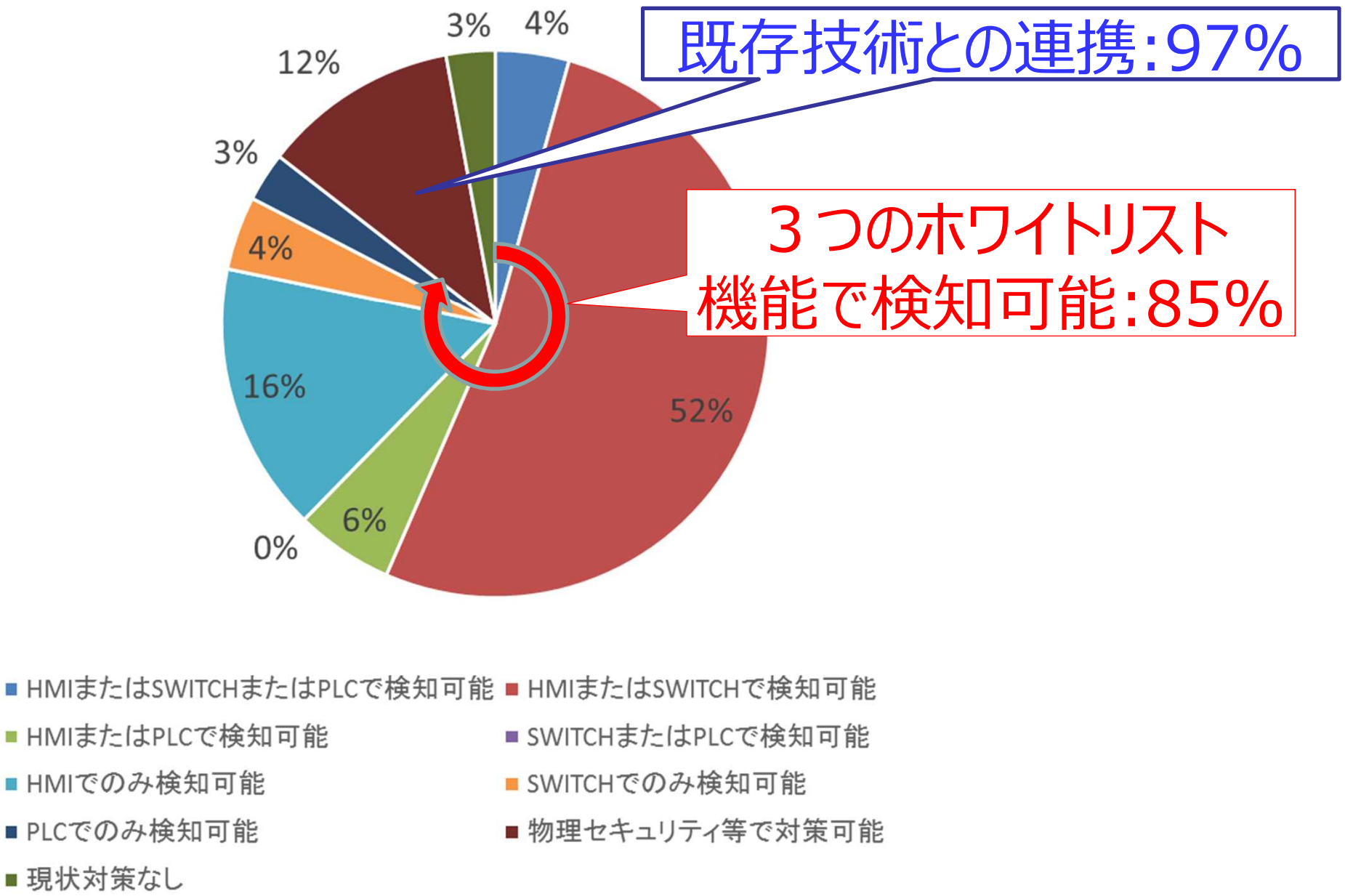
協調型ホワイトリスト技術

- 高度な攻撃から複数の方式（多層）で協調防御するWL提案
  - スキャン機能の高精度化：**稼働状態を反映して複数の検査**で防御
  - ブロック機能の適切化：**全く異なる複数機器で連携して**攻撃範囲を局所化



協調型ホワイトリスト技術の検知率

制御システムに関わる攻撃シナリオ：69件



お問い合わせ先

電気通信大学 産学官連携センター
今田 智勝
ＴＥＬ 042－443－5871
ＦＡＸ 042－443－5726
e-mail imada@sangaku.uec.ac.jp