

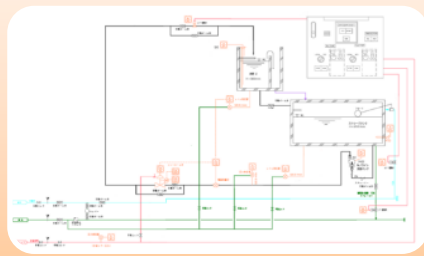
研究開発概要

2018年5月版

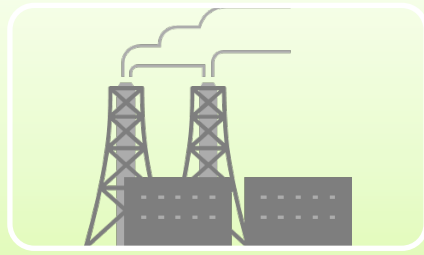
研究開発全体マップ



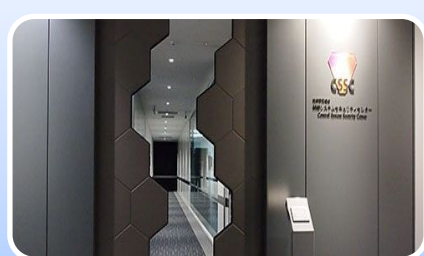
[製品] コントローラ等を対象にして、現状の確認・対策、およびセキュアな製品開発についての研究開発



[システム] (IT)システムを中心とした現状のシステムの確認・対策、およびセキュアなシステムを作るための研究開発



[プラント] 現状のプラントの確認・対策、およびセキュアなプラントを作るための研究開発



[テストベッド] 製品・システム・プラントについて、模擬プラント等による確認・対策を実施できる環境そのものに関する研究開発

各分類の代表テーマ

大項目	小項目	期間
現状製品の評価・検証技術	ISCI/EDSA準拠のための評価技術の研究	2012 -
	CSSC独自の評価項目策定	2012 -
	EDSA認証のための実証実験と環境整備	2015 -
	CSSC独自の検証技術の研究	2012-
セキュアな製品に向けた技術開発	ホワイトリストスイッチ	2012 -
	ホワイトリスト（端末・サーバ向け）	2012 -
	ホワイトリスト（コントローラ）	2016-

大項目	小項目	期間
現状システムの評価・検証技術	ISCI/SSA準拠のための評価技術の研究	2012 -
	CSSC独自の評価項目策定	2012 -
	CSSC独自の検証技術の研究	2013-
セキュアなシステムに向けた技術開発	セキュアな制御システム構築ガイド	2013 -
	ネットワークの構成要素から生成されるログを活用した分析技術の研究開発	2015 -
	ビル分野におけるセキュリティ検証を目的としたログ分析手法の研究	2015 -
	制御システム全体のホワイトリストの研究	2016 -
	スマートメーターシステム検証技術の研究	2015-
	リスクアセスメント技術の研究	2016-

検証手順

- 各プラントのネットワークスイッチをホワイトリストスイッチと入れ替える
- すべての通信を登録外としてSyslogサーバに送信させ、ネットワーク内通信の挙動を確認する
- ホワイトリストを自動生成する
- 各プラントで攻撃を実施し、状態を確認する
- ネットワーク内端末を入れ替える
- ホワイトリストを部分更新し、通信に影響がないことを確認する

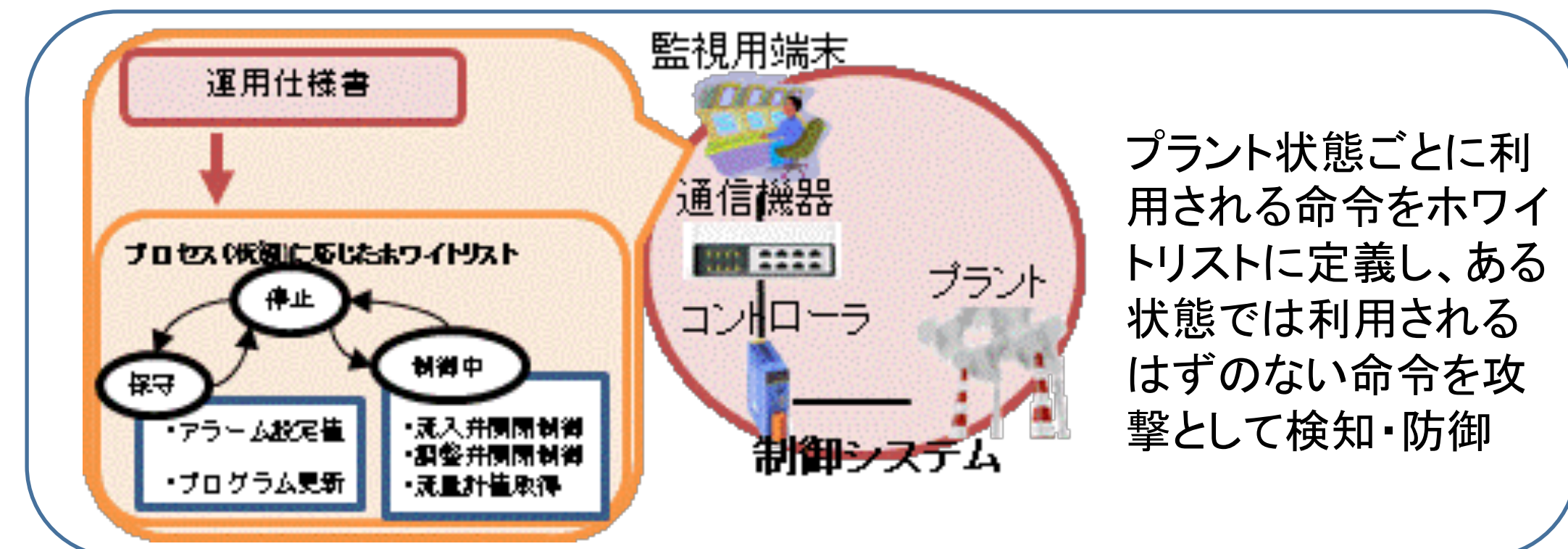
※1.～4.→自動生成ホワイトリストの有効性検証
5.～6.→システム部分更新時のホワイトリスト更新検証

検証結果

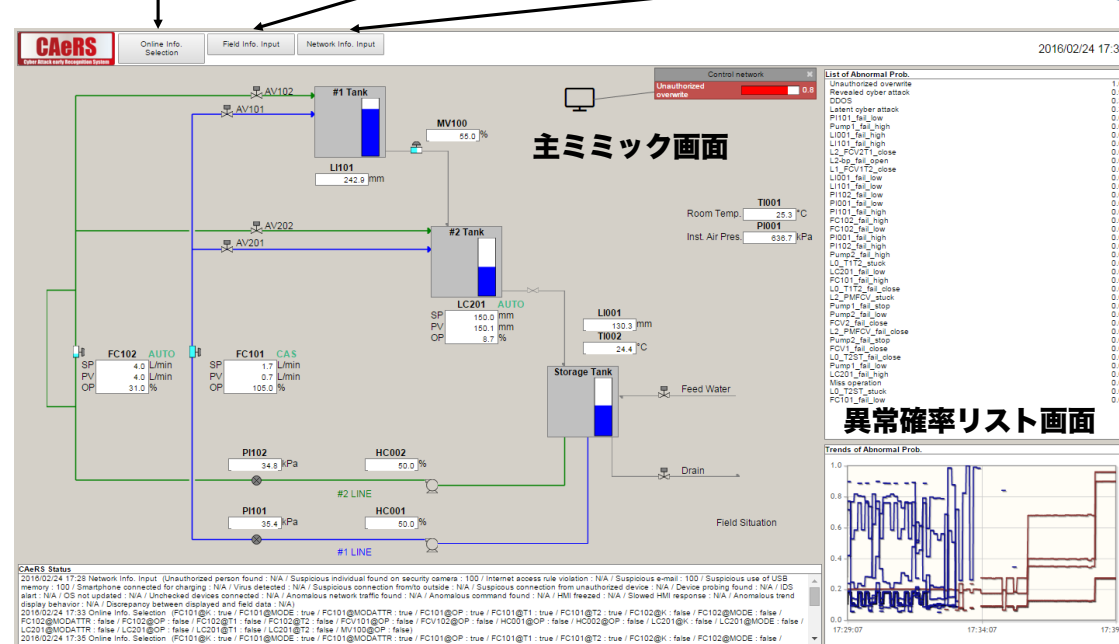
- 各検証プラントにおいて、自動生成したホワイトリストから攻撃パケットのみを検知・排除できることを確認
- ホワイトリスト設定に要する時間を、手動と比較して約1/3に短縮できることを確認

設定方法	85行の作成に要する時間	手動作成に対する効率
自動	30分	2.8
手動	85分	1

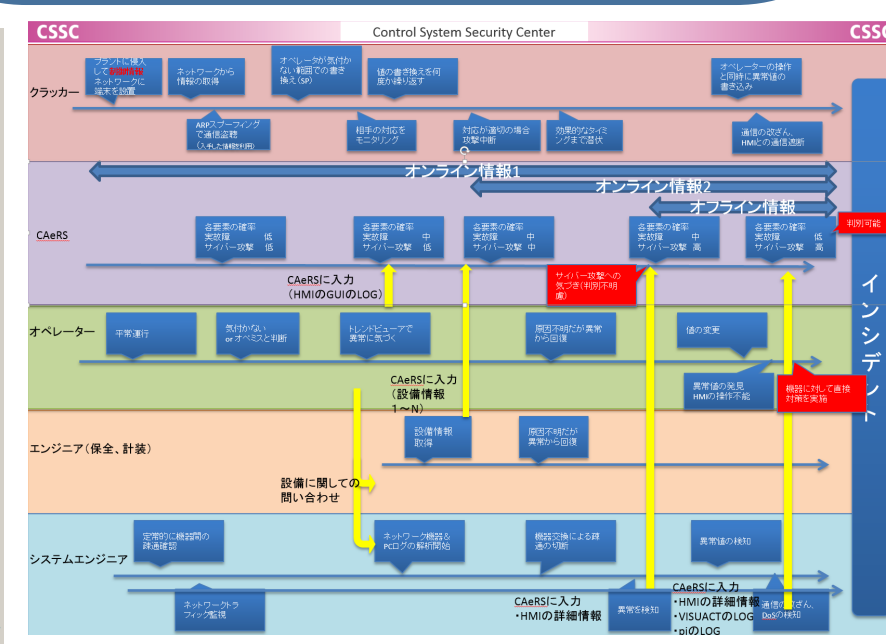
制御システムの部分的な更新時にホワイトリストの一部更新が可能であることを確認



オンライン情報入力画面へ オフライン情報入力画面へ ネットワーク情報入力画面へ



システムログ画面 インタフェース 異常確率トレンド画面



シナリオ



大項目	小項目	期間
現状のプラント運転の検証技術	ケイパビリティモデルに基づくシステムリスク管理体制成熟度評価	2013
	CSMS演習コンテンツ	2013
セキュアなプラントに向けた技術開発	ヒューマンファクター対策	2012 - 2013
	サイバー攻撃早期認識技術の開発	2012 -
	FA模擬プラントへのセキュアログ収集基盤および縮退運転機構の実現	2013 -
	サイバー演習シナリオ	2015 -

大項目	小項目	期間
テストベッドの構築	模擬プラントおよび模擬システムの構築	2012 - 2016
	OPCによる相互接続環境の構築	2013
	マルウェアの動作を検証する機能の構築	2012 -
	対策製品の評価	2012 -
	可搬型模擬プラントの構築	2015-
テストベッドへの検証環境の構築	遠隔検証環境の構築	2012 -
	疑似攻撃環境の構築	2013 -



技術研究組合制御システムセキュリティセンター

Email: cssc-sec@css-center.or.jp

URL: <http://www.css-center.or.jp>

← CSSCでは組合員・特別賛助会員・賛助会員を募集しております。
詳細はホームページをご覧ください。