制御システムのサイバーセキュリティ技術の研究開発

経済産業省

資料6－2

〇目的：電力・ガスなどの社会インフラを制御するITシステムのサイバーセキュリティを確保する。
〇概要：平成24年3月に発足した技術研究組合制御システムセキュリティセンター（CSSC）において、インフラを制御するITシステムのセキュリティ技術を研究開発する産学官連携の国際拠点の整備を図る。研究開発は主に次の2つのテーマを実施してる。

- 制御システムそのものを高セキュア化するための技術
- 制御システムのサイバーインシデントを早期に発見するための技術

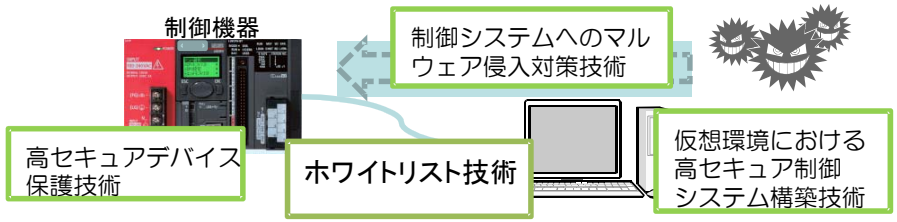
事業期間：H25年度～H27年度
事業費：　5．2億円（H26年度）

背景：制御システムは、外部ネットワークとの接続やOSの共通化が進行しているが、サイバーセキュリティ対策が遅れていた。
制御システムは一般のパソコンやサーバ等とは異なる特有の事情があるため、既存のセキュリティ対策を取れない場合があり、新しいセキュリティ対策技術を研究開発する必要があった。

制御システムは停止させられない

高セキュア化技術の研究開発

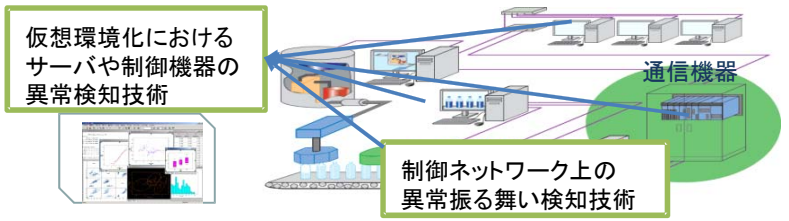
制御システムに不正なアクセスやマルウェア感染があった場合でも可用性に影響を及ぼさないように、予め決められた動きのみを許可するホワイトリスト技術、制御システムの構造自体をセキュアにする技術などを開発する。



現場ではインシデントに気づきにくい

インシデント分析技術の研究開発

インシデントを検知するために、ログをセキュアに蓄積し、かつ複数機器でのログを横断的に分析することにより、運転員に早期にインシデントの原因を提示するための技術などを開発する。



サイバーセキュリティテストベッド

経済産業省
Ministry of Economy, Trade and Industry

〇CSSCは平成25年5月にみやぎ復興パーク内にサイバーセキュリティテストベッドを設置し、開発した技術の実証実験を実施。
〇テストベッドは、具体的なシナリオに基づくサイバー演習の実施や、制御機器のセキュリティ評価・認証手法の開発にも利用。

高セキュア化技術の研究開発

インシデント分析技術の研究開発

研究開発した技術を実証実験。

評価・認証手法の開発

制御システム機器が定められたセキュリティ機能・性能を有することを保証する技術を開発する。

人材育成プログラムの開発

制御システムにインシデントが発生した場合の対策に関する制御セキュリティの啓発・教育コンテンツを開発する。