戦略的イノベーション創造プログラム（SIP）【アラクサラネットワークス株式会社 技術研究組合制御システムセキュリティセンター】

1－4 異常検知時においても安全な運用継続を可能とするシステム防御技術

動作監視防御技術

検知しづらい高度な攻撃から制御システム全体を保護して安全な運転を継続します

特長

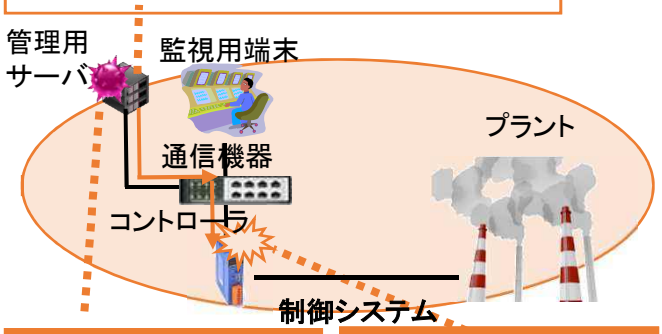
① 制御システムの異常箇所を迅速に特定
プラントの運転状態に応じて防御条件を適切に変更し、監視用端末（上位）、通信機器（中位）、コントローラ（下位）の3つのレベルで、制御システムへの命令・指示を階層的に監視。
既存技術にはない下位レベルの監視を含めた各階層の機器の特徴を活かした検査機能を利用して制御システムに対する攻撃箇所を迅速に特定し保護します（階層検査機能）。

② 異常検知時も安全な運用を継続
協調用端末により、攻撃を検知した機器の通信・処理を運用継続可能な範囲で制限。
コントローラを攻撃による停止・誤動作から保護しつつ運用を継続します（協調機能）。

検知しづらい高度な攻撃に備える必要があります

正規のコマンドによる攻撃

正規のコマンドにより、防御条件をすり抜ける攻撃を仕掛けられる可能性があります。



検知困難な攻撃

高度化されたサイバー攻撃は、単一の防御条件では防ぎきれない可能性があります。

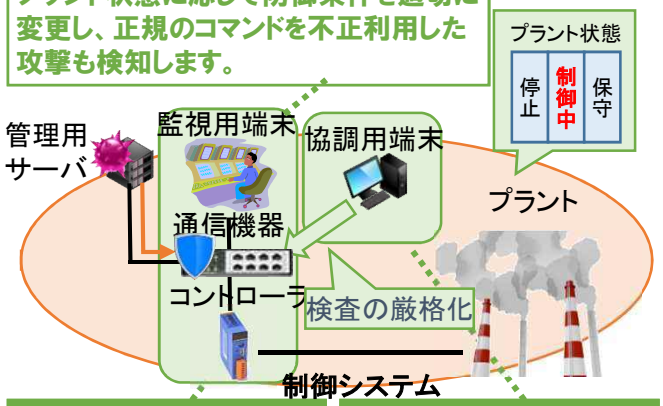
コントローラを狙うリスク

プラントの安全を維持する機器を狙ったサイバー攻撃により、大事故になる可能性があります。

高度な攻撃から制御システム全体を保護します

運転状態に応じた防御

プラント状態に応じて防御条件を適切に変更し、正規のコマンドを不正利用した攻撃も検知します。



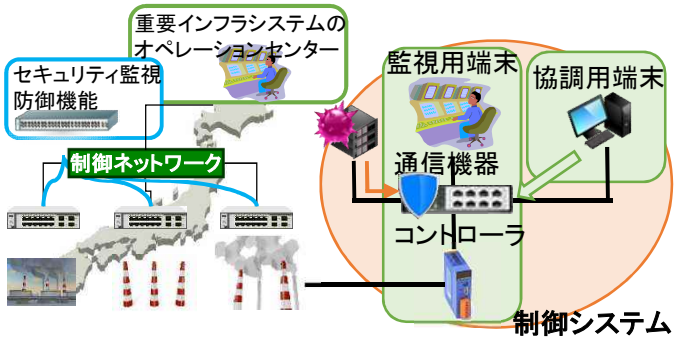
上～下まで全階層で防御

防御網を多段に設置する階層防御により、高度化された攻撃であってもすり抜けを阻止します。

現場から遠ざける防御

プラント全体を安全に稼働するため、可能な限り上位で攻撃を食い止めることができます。

社会実装に取り組みます



進捗

重要インフラ事業者と協働の技術開発を実施し、技術評価、導入・運用手順を成果目標にします。

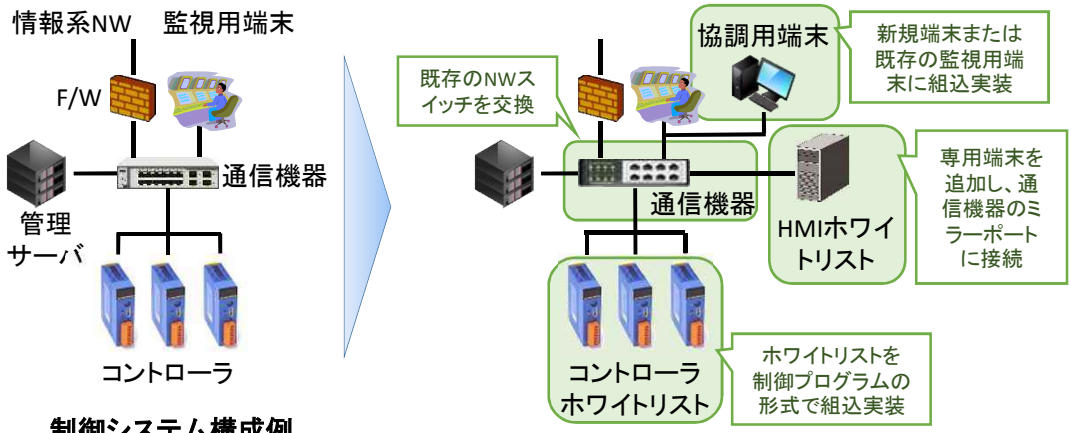
【社会実装へ向けて】
・先行して導入可能な技術から重要インフラ事業者様へ導入し、ご活用いただいています。

【研究技術について】
・協調ホワイトリスト防御機能を開発し、試験用模擬プラントに実装しました。
・複数種類の試験用模擬プラントを利用した検証を実施しました。

戦略的イノベーション創造プログラム（SIP）【アラクサラネットワークス株式会社 技術研究組合制御システムセキュリティセンター】

1－4 異常検知時においても安全な運用継続を可能とするシステム防御技術

導入イメージ

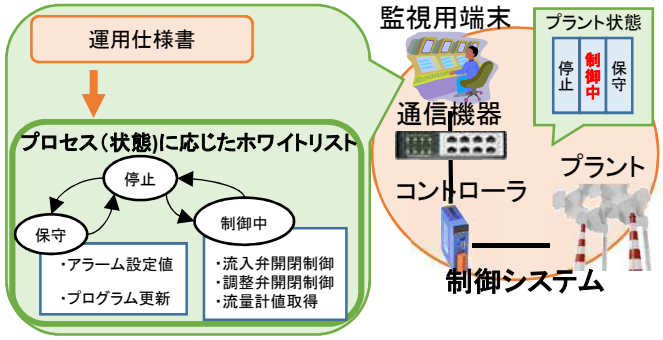


研究開発成果の導入

・3種類のホワイトリストセキュリティ機能およびホワイトリスト協調機能を導入することで、検知しづらい高度な攻撃から制御システムを守ります

・導入にあたっては、対象の制御システムに応じて必要な要素を個々に導入することも可能となります

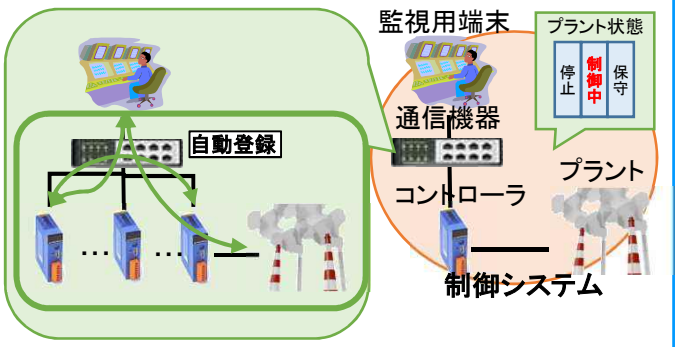
（上位）通常発生しない命令を検知・防御します



プラント状態に応じた防御

運用仕様書からプラント状態ごとに利用される命令をホワイトリストに定義し、ある状態では利用されるはずのない命令を攻撃として検知・防御します。

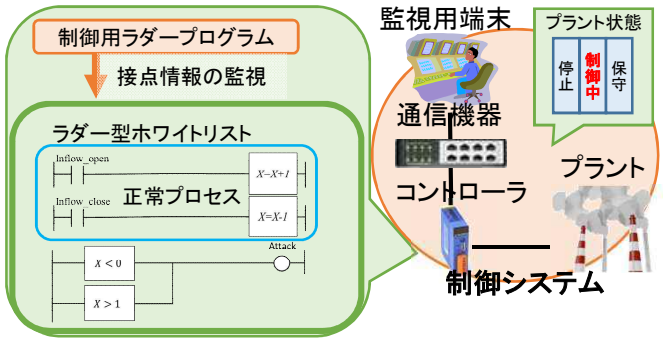
（中位）煩雑な管理なく攻撃を検知・防御します



制御プロトコルにも対応した学習機能を用いて防御

プラント状態ごとに利用される通信を自動学習によりホワイトリストに定義し、ある状態では利用されるはずのない通信を攻撃として検知・防御します。

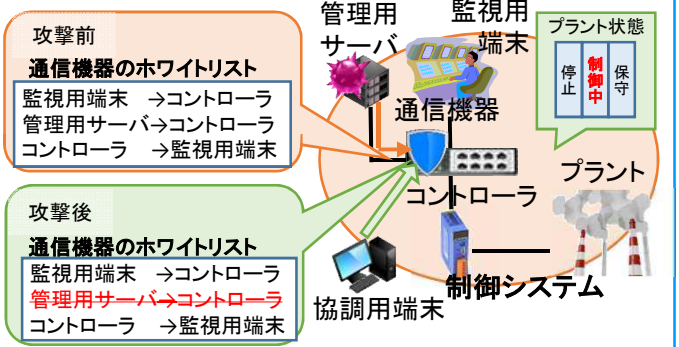
（下位）プラントの動作状態を監視・防御します



プラントの動作状態を監視し、動作が逸脱するものに対して防御

プラントの動作状態（I/Oの正常プロセス）を表現するラダープログラムが接点情報を監視することで、あらかじめ決められた動作を逸脱する場合を攻撃として検知・防御します。

状況に応じた防御機能を適用し攻撃を防御します



攻撃をより上位で防御するため、上位の防御機能を厳格化して保護

プラント全体を安全に稼働するため、上位ですり抜けてきた攻撃を下位で検知できた場合、上位の防御機能の条件を見直して検知・防御します。