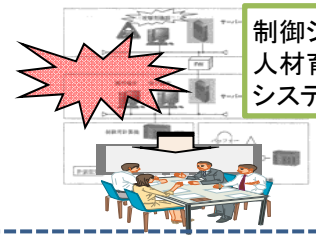
東北復興再生に資する重要インフラＩＴ安全性検証・普及啓発拠点整備・促進事業

重要インフラITの安全性検証・普及啓発のための産学官連携国際拠点の整備を目指し、現在構築中の「制御システム検証施設」を活用し、委託事業として人材育成プログラムの開発や、システム安全性評価・認証手法の開発、国際シンポジウムの開催等を実施。

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普及啓発システムについての技術を開発する。

制御システムにおけるマルウェア感染の影響および対策のための人材育成プログラム構築技術



制御システムセキュリティ人材育成のための模擬システム構築技術

評価・認証手法の開発

制御機器が実環境と同等の環境で稼働することを保証し、制御機器の接続性・脆弱性を検証し、それらの結果を視覚化する技術を開発する。

制御機器

制御機器間の接続性検証技術

制御システムにおける脆弱性検証技術

実環境エミュレーションソフトウェア技術

セキュリティ検証結果の視覚化技術

高セキュア化技術の開発

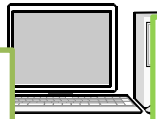
マルウェアの侵入防止や感染後の不正な動作の防止を図ることによるマルウェア対策技術、通信路での暗号化を図るための暗号化技術、構造自体をセキュアにする技術などを開発する。

制御機器

制御システムへのマルウェア侵入対策技術

高セキュアデバイス保護技術

制御システム向け軽量暗号認証技術

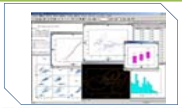


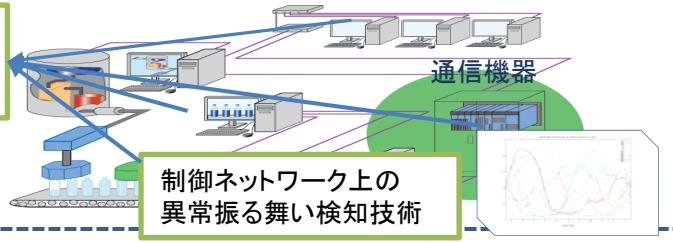
仮想環境における高セキュア制御システム構築技術

インシデント分析技術の開発

インシデントを検知するために、ネットワーク上の振る舞いや制御機器の異常を検知できる技術を開発する。

仮想環境化におけるサーバや制御機器の異常検知技術





制御ネットワーク上の異常振る舞い検知技術

【実施期間】　H25～H27
【実施機関】　経済産業省

「サイバーセキュリティの強化」の実施における出口戦略と課題について

出口戦略

「サイバーセキュリティの強化」については、マルウェア解析技術、ネットワークモニタリング技術、データマイニング技術、ぜい弱性検証・セキュリティ評価技術等の研究開発を実施。これらの技術について、外部有識者による評価会等の意見を踏まえながら、主に以下の3つの方向性から効果的な成果の展開を図ることで、社会全体におけるサイバー攻撃等に対する対処能力を向上させる。

■ テレコム・アイザック推進会議※等の業界団体との連携を通じたサービス化・事業化

（例）個人のインターネット利用者を対象としたマルウェア配布サイトへのアクセスを未然に防止する技術、サイバー攻撃の発生を予知し、即応を可能とする技術、サイバー攻撃に対する防御モデルについて、国内の主要インターネットサービスプロバイダ等から構成される団体等を通じて効果的な成果の共有を行う。

※ テレコム・アイザック推進会議：インターネット・サービス・プロバイダやウイルス対策ベンダ等の事業者間で情報セキュリティに関する情報を共有・分析し、サイバー脅威に対して適切な対策をとることを目的とする団体

■ 研究開発の受託事業者における実用化・製品化

（例）利用者の行動特性に応じてサイバー攻撃を早期に検知し動的な防御を実現する技術について、システムベンダ等の受託事業者において、技術の商品化・製品化を行う。

インフラを制御するシステムのセキュリティ評価・認証技術について、制御システムを運用する企業などにおいて活用を図る。

■ 独立行政法人・大学等の研究機関等の公的機関を通じた社会への還元

（例）マルウェア感染の早期検知技術で開発した一部の技術（DAEDALUS）について、地方公共団体向けに展開することで、成果の展開を図る。

課題

「サイバーセキュリティの強化」の推進において、主に以下の課題を認識しているところ。

－ サイバー攻撃については**常に攻撃手法が最新化され、高度化・複雑化していくため、研究開発する技術が陳腐化する可能性**がある。

－ サイバーセキュリティの分野においては、サイバー攻撃に対する防御を前提とするため**定量的な評価が困難**である。