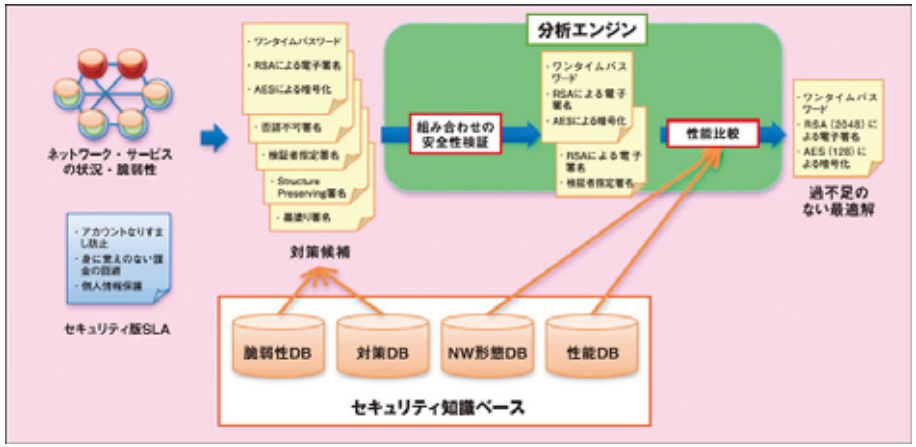
ネットワーク構成要素における適切な情報セキュリティ設定導出に関する研究開発

概要

■ 昨今のサイバー攻撃においては複数の攻撃手法を組み合わせた攻撃が増加しており、単体セキュリティ技術での対応が困難であるため、サービスのセキュリティ要求に応じて端末間の通信における適切なリスク評価とセキュリティ設定が必要である。

■ セキュリティ知識データベースの整備と分析エンジンの研究開発を行い両者が連携することで、端末間（End-to-End）の通信において状況に応じた過不足のないタイムリーなセキュリティ対策を導出する。

具体的内容



① 端末間の通信におけるネットワーク・サービスの状況や脆弱性について、セキュリティ知識データベースのデータを照合し、その通信に係るリスクを評価。

② リスク評価に基づき、セキュリティ知識データベースと連携しながら、複数のセキュリティ対策案の中から安全かつ処理性能が一番高い対策を選び出し、過不足のないセキュリティを実現。

有識者からの指摘事項

1.「セキュリティー知識データベースの整備」の具体的な協力先と体制を確立すべき。
2.「End-to-Endのリスク評価手法の確立」は、「知識データベース」と関連してないように思える。

対応

1. セキュリティ知識データベースの整備においては、**同種のデータを多数保有している米国の国立標準技術研究所（NIST）と連携**を進めるとともに、知識データベース内の暗号プロトコルに関する脆弱性情報について、**国際的に議論し集約するコンソーシアム「暗号プロトコル評価技術コンソーシアム（CELLOS）」を設立するなど国内企業・国外の研究機関等と連携**しながら進めているところ。

2. End-to-Endのリスク評価を行うにあたっては、ネットワークに接続された機器の**ハードウエア／ソフトウエアの脆弱性の情報や、利用されているプロトコルの安全性情報等をもとにリスクを評価する必要**があり、これらの情報をあらかじめデータベース化した知識データベースが必要である。

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

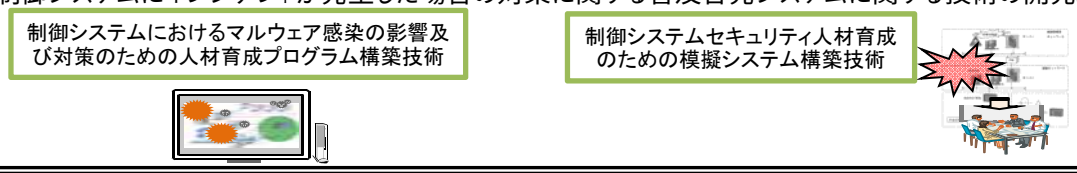
概要

■ 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。

具体的内容

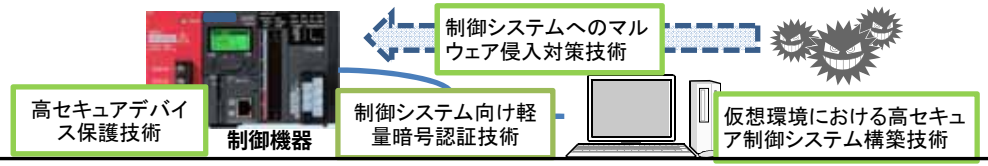
① 人材育成プログラムの開発

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関する技術の開発。



② 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等の開発。



③ 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の開発。

④ 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の開発。

有識者からの指摘事項

1. 「制御システム」に関する課題は重要。さらに、システム全体にも広げるべき。
2. 人材育成・普及啓蒙では不十分

対応

1. 平成25年4月にみやぎ復興パーク内に構築した制御システムセキュリティセンター（CSSC）東北多賀城本部において、制御システムのセキュリティ向上のための研究開発を実施。
制御機器から制御ネットワークまでを対象とした**システム全体のセキュリティ向上に係る取組**を対象に技術開発している。別事業では、**インフラ事業者のセキュリティ管理体制を評価認証するパイロット事業**が実施されている。

2. CSSCでは、人材育成・普及啓発にとどまらず、制御システムセキュリティに関する研究・技術開発に加え、**国際規格に則った制御システムの評価・認証**に取り組んでいる。制御システムメーカーの人的負担とコストを低減するセキュリティの認証取得を可能にして、**インフラ輸出の促進**につなげる。