産業系サイバーセキュリティ推進事業

令和４年度概算要求額　21.0億円（19.4億円）

事業の内容

事業目的・概要

- 近年、企業や個人の情報を狙ったサイバー攻撃にとどまらず、プラントやインフラそのものの停止を狙い、制御系システムまで含めた社会システム全体を標的とするサイバー攻撃のリスクが高まっており、海外では攻撃事例も出てきています。

  ※制御系システム：工場やプラントの機械や設備などのコントロールを行うために用いられるシステムのこと

- こうした状況の中で安全・安心な社会を築くためには、重要インフラや我が国経済・社会の基盤を支える産業のサイバーセキュリティに関する人材・技術・ノウハウを結集することで、サイバー攻撃への防護力を強化することが不可欠です。

- このため、（独）情報処理推進機構（IPA）に平成29年4月に設立した「産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence）」において、模擬プラントを用いた演習等を通じて、官民の共同によりサイバーセキュリティ対策の中核となる人材を育成します。また、サイバーインシデントの観点から、インフラ等における事故の原因究明を行う機能の整備に係る検討を含め、実際の制御系システム等の安全性検証等により、産業分野におけるサイバーセキュリティ対策のノウハウを創出します。

成果目標

- センターのプログラム提供により、100人以上の人材を育成します。良質なプログラムの提供により、これらの受講者による、人材育成プログラムに対する上位の回答割合が80%以上となることを目指します。

条件（対象者、対象行為、補助率等）

国 → 交付金 → （独）情報処理推進機構

事業イメージ

模擬プラントを用いた演習等を通じた人材育成

- 情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家と共に安全性・信頼性の検証や早期復旧の演習を行う。修了後も中核人材としての活動を支援。
- 最新の攻撃情報の調査・分析結果に応じてプログラムのアップデート等を実施。
- 海外との連携も積極的に実施。

実際のシステムの安全性・信頼性検証等

- 社会インフラ等で活用されている実際の制御システムやIoT機器の安全性・信頼性を検証。
- サイバーインシデントの観点から事故原因の究明を行う機能（いわゆる「サイバー事故調」機能）の整備に向けた検討を実施。
- あらゆる攻撃可能性を検証し、必要な対策立案を行うことで、業界全体で活用可能なサイバーセキュリティ対策のノウハウを創出・蓄積。