サイバーセキュリティ統合知的・人材育成基盤ロジックモデル

現状・課題

【現状】

○ 巧妙化・複雑化するサイバー攻撃により、我が国の民間企業等から情報が漏えいし、場合によってはシステム停止に追い込まれる等の被害が発生しており、サイバーセキュリティ対応能力の一層の向上が必要。

○ さらに、新型コロナウイルス感染拡大を受けてテレワークの利用拡大など、社会構造の急速なデジタル化への変革が求められている。その一方で、セキュリティに対する不安は解消されておらず、テレワーク実施企業の4割がセキュリティの確保が課題としている。

【課題】

○ 現在、我が国のサイバーセキュリティ対策は、海外製品や海外由来の情報に大きく依存しており、国内のサイバー攻撃情報等の収集・分析等が十分にできず、日本特有の攻撃事例を必ずしも反映できていない。

○ サイバーセキュリティに係る人材育成施策は既に実施されているものの、セキュリティ対策を先導できる人材、及び広く企業等でセキュリティ対策を担う人材が不足するとともに、海外教材に依存し、日本特有の攻撃に対して速やかに対処できない。

インプット（資源）

【予算】令和3年度要求額：2,000百万円

アクティビティ（活動）

○ 国立研究開発法人情報通信研究機構（NICT）において、次の通り活用可能な基盤を構築する。

① 国産セキュリティ情報の収集・蓄積・分析・提供
セキュリティ事業者が攻撃状況を分析する環境を提供することにより、幅広くサイバーセキュリティ情報を収集・蓄積し、そのビッグデータをAIを駆使して横断的に分析することで、我が国独自の攻撃に対応した高信頼で即時的なセキュリティ情報を生成し、提供。

② セキュリティ機器テスト環境
収集した国内向けの最新のサイバー攻撃情報を活用し、我が国向け攻撃への対応状況をセキュリティ事業者がテストできる環境を提供。

③ 高度解析人材の育成
多種多様な情報を多角的・横断的に解析し、日本に特化した高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成。

④ 人材育成のための基盤提供
NICTが有する人材育成に関する環境・知見を教育機関・民間事業者等に開放するとともに、最新の攻撃情報を踏まえて民間演習教材の活用を図ることで、自律的なサイバーセキュリティ人材育成を推進。

アウトプット（活動目標）

○ サイバー攻撃分析環境の利用回数
令和3年度目標：40回

○ 民間企業が開発した人材育成コンテンツ数
令和3年度目標：1件

アウトカム（成果目標）

【短期アウトカム】

構築した基盤の産学による利用

○ セキュリティ製品テスト環境の利用回数
令和7年度目標：900回

○ 外部による人材育成プラットフォームの延べ利用者数
令和7年度目標：3,000人

【長期アウトカム】

基盤が利用されることによる効果

○ 日本特有の攻撃に迅速かつ的確に対応可能な製品やサービスが開発・提供

○ 最新のサイバー攻撃情報を解析する高度人材や、民間等における幅広いサイバーセキュリティ人材が育成

インパクト（国民・社会への影響）

政府機関や重要インフラ事業者等のサービスを支えるセキュリティのコア技術の開発・運用を中心に、国産技術・産業の育成が図られるとともに、我が国全体のサイバーセキュリティ対応能力を強化する。