サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証 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策の一層の強化が必要。

○ 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約5割がセキュリティの確保を課題としている。

【課題】

○ 現在、我が国のサイバーセキュリティ対策は、利用者や端末側の対策を中心に推進してきており、攻撃者がインターネット上に構築する攻撃用インフラや悪性ウェブサイトへの対処、大規模な情報窃取や通信障害を引き起こす経路ハイジャック攻撃への対策など、情報通信ネットワーク側（通信事業者側）において積極的・能動的な対策を行う必要性のある課題が多く残存している。

インプット（資源）

【予算】令和4年度要求額：1,800百万円

アクティビティ（活動）

○民間企業（通信事業者、ベンダ）等において、次の実証実験を行う。

① フロー情報分析によるC&Cサーバ検知技術の実証
インターネット利用者のトラフィックのうちフロー情報を大規模かつ統計的・相関的に分析し、C&Cサーバを検知する手法の有効性や、C&Cサーバの検知・共有に当たっての技術・運用面の課題を整理するべく実証事業を行う。

② 悪性Webサイトの検知技術・共有手法の実証
SNSや利用者による通報、自動巡回の仕組みにより収集した、悪性Webサイト（フィッシングサイト等）に関する情報を分析し、悪性Webサイトを検知する技術の有効性を実証するとともに、検知結果の共有手法の課題を整理。

③ ネットワークセキュリティ対策技術の導入実証
ISPにおけるセキュリティ対策を強化するため、ネットワークセキュリティ対策技術の円滑な導入、実装及び運用に係る技術的な諸課題を整理。

アウトプット（活動目標）

○ C&Cサーバの検知精度
令和4年度目標：90パーセント

○ 悪性Webサイト実証、関連のワークショップ等に参加する社数
令和4年度目標：25社

○ セキュリティ対策技術導入円滑化のためのガイドライン作成数
令和4年度目標：1件

アウトカム（成果目標）

【短期アウトカム】

実証した課題解決手法の事業者による活用

○ 検知したC&Cサーバ情報のリストを共有するISP数
令和5年度目標：10社

○ 悪性Webサイト対策ガイドラインに準拠した対策を講じた社数
令和5年度目標：5社

○セキュリティ対策技術導入円滑化のためのガイドラインを参照し、当該技術を導入した社数
令和5年度目標：9社

【長期アウトカム】

実証した課題解決手法が活用されることによる効果

○ C&Cサーバの所在を広くISP間で把握することで、実際にサイバー攻撃が起こった際の迅速な対処が可能になる。

○各社独自で自社偽装サイトを検知する仕組がより広範に活用され、対策が強化される。

○ ISPによる、ネットワークセキュリティ対策技術の円滑な導入を実現。

インパクト（国民・社会への影響）

電気通信事業者側における積極的・能動的なセキュリティ対策の推進により、安全かつ信頼性の高い情報通信ネットワークの確保を実現。これにより、社会全体のデジタル化の進展に寄与する。