サイバー攻撃の解析・検知に関する研究開発

目的

利用者の行動特性や環境特性等に基づいて不正な意図を検知し、侵入や感染の可能性、被害の程度、被害に至った経緯を明らかにするための技術を確立するとともに、被害拡大の防止と業務継続を両立させる組織内ネットワークを自動的に構成する技術などを開発する。

研究開発概要

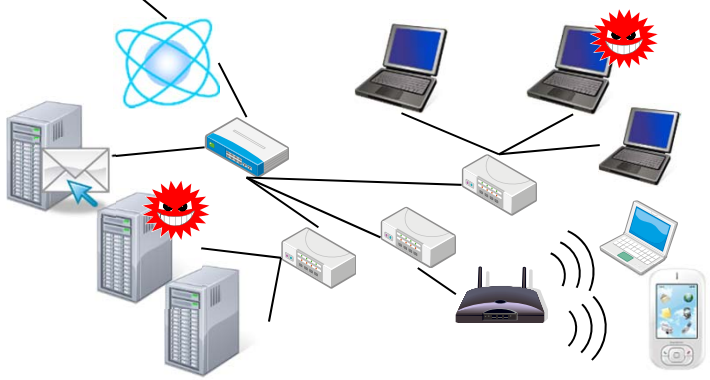
検知・解析（Observe）　情勢判断（Orient）　意思決定（Decide）　行動（Act）

Ⅰ. 行動特性

・利用者の行動特性の研究（騙され易い人、難い人の差　等）

Ⅱ. 環境特性

・端末情報の効果的な収集方法の研究開発
・ネットワーク状況の効率的なスキャン方法の研究開発　等



進行状況
進入経路
の把握

Ⅲ. 攻撃阻止と業務継続

・行動特性に応じたセキュリティレベルを適応的に設定する技術の研究開発
・進行状況や進入経路を適切に把握する技術の研究開発
・被害を拡大させずかつ業務を継続させる組織内ネットワーク構成技術の研究開発　等

【実施期間】　H25～H29
【実施機関】　総務省