サイバー攻撃の解析・検知に関する研究開発

利用者の行動特性及び環境特性に応じて適切な対策を適用するとともに、被害が発生した場合においても、被害拡大の防止と業務継続を両立させるような組織内ネットワークを自動的に構成する技術などを確立する。

1　施策の概要

（１）近年、標的型攻撃をはじめとしてサイバー攻撃の高度化・複雑化が進展し、既存の情報セキュリティ施策ではネットワークへの侵入、マルウェア※の感染等の情報セキュリティ上の脅威を完全に防ぐことが困難となっている。

※マルウェア：コンピュータウィルス等の「悪意あるソフトウェア」の総称

（２）こうした状況においてサイバー攻撃の被害を最小化するには、攻撃を早期に検知し、迅速に対処することが必要である。そのため、本研究開発においては利用者の行動特性に応じて不正な通信を検知する技術や、被害が発生した場合に進行状況や侵入経路を適切に把握する技術等のサイバー攻撃への対策技術に関する研究開発を実施する。

2　イメージ図