国際連携によるサイバー攻撃予知・即応技術の研究開発

サイバー攻撃（マルウェア※1の感染活動、分散型業務妨害攻撃※2等）に関する情報収集ネットワークを国際的に構築し、ISP、大学等と協力して、サイバー攻撃に対抗するための研究開発を実施し、日本におけるサイバー攻撃等のリスクを軽減する。

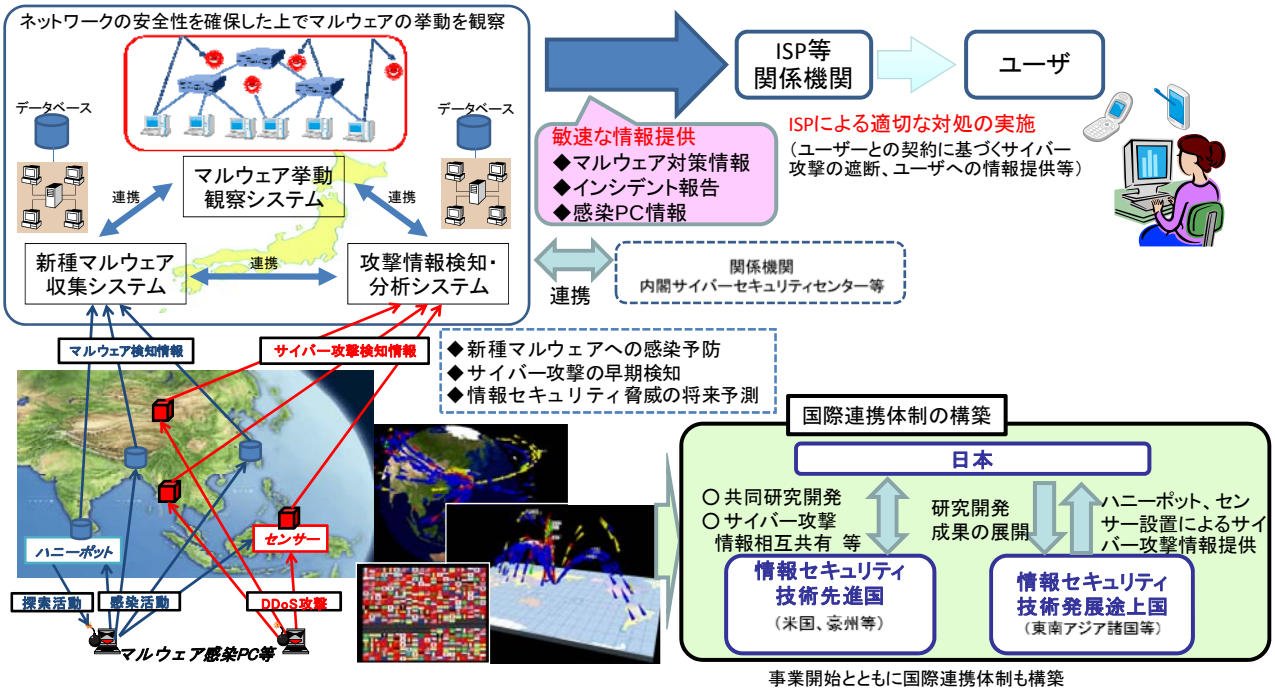
※1： マルウェア：コンピュータウイルス等の「悪意あるソフトウエア」の総称。
※2： 分散型業務妨害攻撃： 多数のＰＣから一斉に大量のデータを特定宛先に送りつけることにより、当該宛先のネットワークやサーバを動作不能にする攻撃。DDoS（Distributed Denial of Service）攻撃と呼ばれる。

1　施策の概要

（１）近年、大規模なサイバー攻撃が世界各国で発生し、問題となっている。平成19年にはエストニア、平成21年には米国及び韓国において大規模なサイバー攻撃が発生し、政府関係機関等の主要機関のウェブサイトのサービスが長期間に渡って停止する事態となり、国民生活や経済活動に甚大な影響を及ぼしたところである。
　サイバー攻撃の対応が現状後手に回っている背景に、Gumblar 等の新種マルウェアの発生数の急増、サイバー攻撃手法の高度化・巧妙化等がある。さらに、国境を越えた広域事例が増加しており、各国の協力体制強化が課題となっている。

（２）海外を含む多数の ISP、大学等と連携し、各地に設置されたセンサーやハニーポットにより、国際的なマルウェア感染・攻撃状況等をリアルタイムで検知・分析し、日本国内への情報セキュリティ脅威に対して即応可能な技術・手法を確立する。また、サイバー攻撃情報等を蓄積し、それを基に、将来の情報セキュリティ脅威を予測する技術の確立に向けた研究開発を行う。

2　イメージ図



事業開始とともに国際連携体制も構築