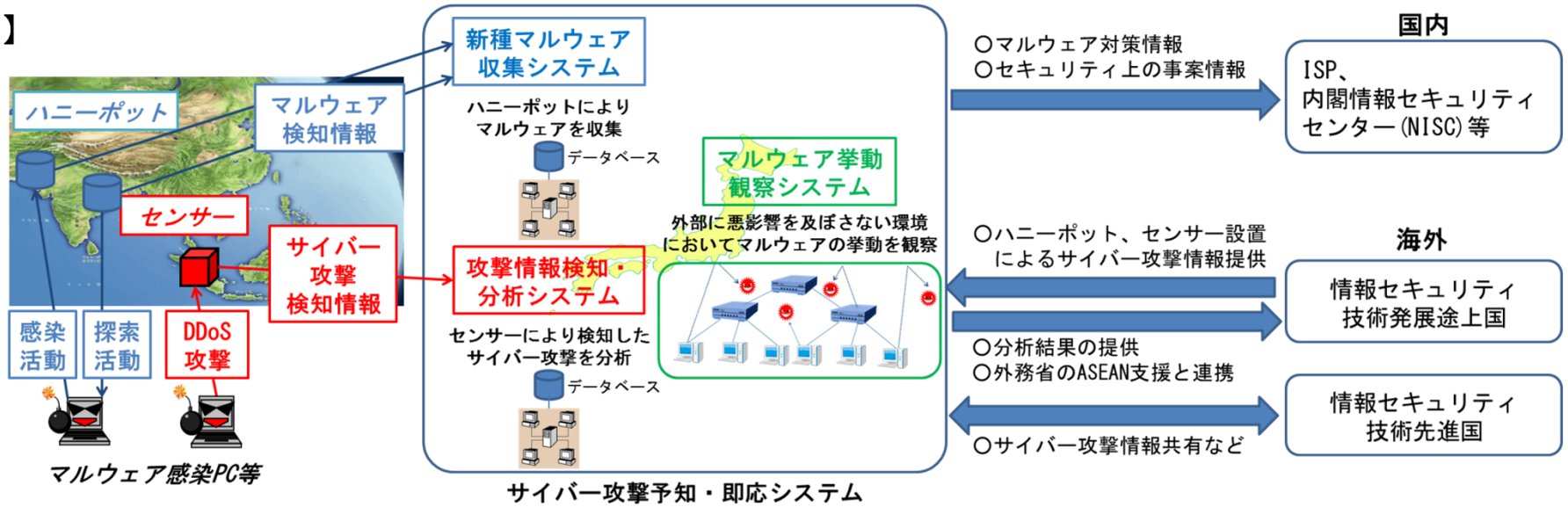
国際連携によるサイバー攻撃予知・即応技術の研究開発

プロジェクト略称：PRACTICE, Proactive Response Against Cyber-attacks Through International Collaborative Exchange

○目的：
近年、被害が拡大しているサイバー攻撃（分散型サービス妨害攻撃、マルウェアの感染活動等）に対処し、我が国におけるサイバー攻撃のリスクを軽減。

○概要：
国内外のインターネットサービスプロバイダ（ISP）、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するネットワークを国際的に構築し、諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術について、その研究開発及び実証実験を実施。

【イメージ図】



○マルウェア：コンピュータウイルスのような有害なソフトウェアの総称。
○DDoS（Distributed Denial of Service）攻撃：分散型サービス妨害攻撃。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。
○ハニーポット：故意に外部からの進入を容易にした囮のネットワーク機器。マルウェアの感染活動等の検知を目的にネットワーク上に設置。

【実施期間】　H23～H27
【実施機関】　総務省

国際連携の状況

○　平成23年11月、「第4回日・ASEAN情報セキュリティ政策会議」において、ASEAN各国に連携を呼びかけ。
○　平成24年3月には、サイバー攻撃の予知のための研究開発の協力について、**米国と合意**。6月に研究者中心の日米会合を実施。
○　そのほか、平成24年3月に**インドネシア**、4月に**モルディブ**、平成25年2月に**タイ**、3月に**マレーシア**との間で合意。
○　現在、欧州諸国、シンガポール等と連携に向けて協議中。