課題 216

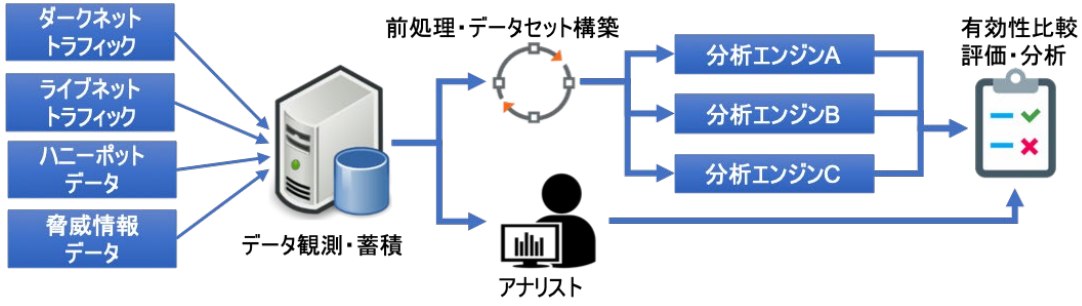
サイバー攻撃ハイブリッド分析実現に向けた セキュリティ情報自動分析基盤技術の研究開発

背景と課題

マルウェアへの感染は世界的な問題であり、政府、重要インフラなどの組織に対する脅威は増加の一途を辿っている状況であるが、感染活動の早期把握やそのマルウェアに関する情報の関連組織間での共有ができていない。

研究開発の目的

NICTが開発中のマルウェア活動の活性化を自動的に検知する技術と連携し、その検知したイベントに関連するマルウェア・脆弱性・脅威情報などを実時間で精緻に提供することで、より有用性の高いセキュリティ情報自動分析基盤技術の確立を目指す。



研究開発の概要

以下の3課題について研究開発を実施。

(1) サイバー攻撃インフラ情報の収集と分析	(2) 実時間で実現可能な大規模かつ構造的なマルウェア分析	(3) インテリジェンス情報の生成と分析
a) マルウェア検体が攻撃インフラに接続する通信の観測・分析 b) 検出されたマルウェア活動に関連するハニーポット分析結果を特定する技術の開発	a) マルウェアの機能を精緻に分析し、クラスタリングを行う技術の開発 b) 大規模かつリアルタイムに動作するマルウェア解析技術の開発	a) 脆弱性の種類や深刻度をAI技術により自動的に推定する技術の開発 b) Web情報を分析することによりインテリジェンス情報を生成する技術の開発 c) インテリジェンス情報とセキュリティインシデントを関連付ける技術の開発

研究開発期間：2019年度（契約締結日）から2020年度
研究開発予算：各年度、総額30百万円（税込）を上限、採択件数：1件