MWS Cup2014では、参加チーム11中で優勝、MWS Cup2015では15チーム中で４位の成績を果たした。

研究活動について

１）マルウェア検知手法

マルウェアの一種であるボットの検知手法を研究する。まず、正規のプログラムとボットの振る舞いの違いを（a）空間的な側面、（b）時間的な側面、（c）通信の側面の３つ側面から分析し、分析結果を用いて、ボットの検出手法について提案する。ここで、正規のプログラムとはマルウェアに感染していない通常のソフトウェアのことであり、ボットとはネットワークを通じて外部から操ることを目的として作成された悪意のあるプログラムのことである。現在、「（b）時間的な側面」に着目して実際の検体の挙動を調査し、新たなマルウェア検知手法を検討中である。

２）セキュリティインシデント解析の基盤システム

日本国内の企業ではサイバー攻撃への遭遇率が増加しており、特に特定の団体を狙い多様な手法で攻撃する標的型攻撃と考えられる事例が多く報告されている。標的型攻撃は、攻撃手法の多様性から、初期での検知と対応が難しく、事後の分析により標的型攻撃であったと判断されることが多い。また、これらの分析は､分析に関わったセキュリティ技術者の経験や経済、国際情勢などに関する幅広い知識に依存することが多く、多様な情報を関連付ける解析をサポートする仕組みが必要である。そこで、サイバー攻撃や社会情勢の兆候を早期につかむ為、即時性の高いWebからの情報抽出に注目して、サイバーセキュリティに関する解析をサポートするデータマイニング基盤SIAS（Security Incident Analysis System）を開発し、サイバーセキュリティに関するイベントサマリ抽出や社会情勢を考慮した攻撃者の分析、Webを介して配布されるマルウェアの解析を進めている。

SIASは、データ基盤を中心にデータの収集と解析、可視化などを行うモジュールが連携するデータマイニングのプラットフォームである（**図１　研究**①）。Webサイトに書かれた文章を解析するために、Webブラウザと同様にスクリプトが実行可能なWebクローラや代表的な自然言語処理が行えるよう自然言語処理モジュールを開発した。さらに、異なる解析処理の連携や可視化を容易にするために、収集したデータや解析結果などの形式を定義した。

実応用に即した基礎実験としては、通信ログデータの解析と地理空間への可視化を行っている（**図１　研究**②）。解析結果を別途開発した時系列地理空間情報可視化システムと連携し、地理空間情報をヒートマップ

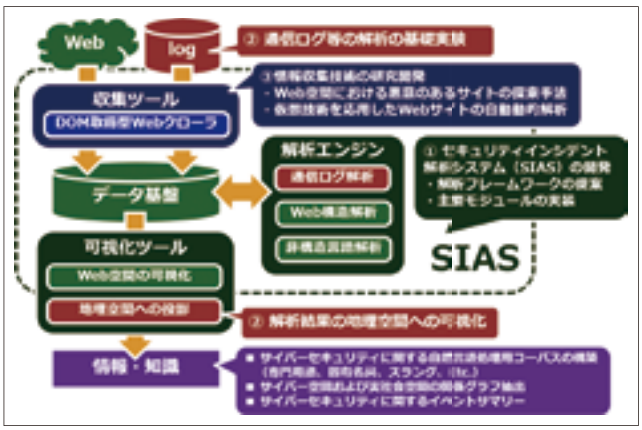

図１　サイバーセキュリティに関する分析処理の流れ

により可視化することで、直感的に配布元の地理空間情報の分布や密集具合を評価し，長期的な時間的推移を考慮した分析が可能となった。CCCデータセット（Cyber Clean Center Dataset）を使用して解析したマルウェア配布元の時系列遷移をヒートマップにより可視化した結果を**図２**に示す。

図２　マルウェア配布元のヒートマップ
左：2008年12月、中：2009年12月、右：2010年12月
赤の点はマルウェア配布元を示す。

現在は、SIASの基盤としてオープンソースのデータ管理基盤を応用し、システムの導入・運用の容易性の向上や人工知能の技術を応用した自然言語処理の精度向上を試みている。また、広大なWeb空間から悪意のあるWebサイトを発見する為に、複数のWebクローラによる自律分散探索手法や仮想化技術を応用したWebクローラでマルウェア解析を自動化する処理の検討を進めている（**図１　研究**③）。

３）サイバー犯罪者のプロファイリング手法

リバプール型（データを計量的、客観的に分析して結論を出す）プロファイリングを参考にして、Anonymous、LulzSecの文献やチャットログなどのデータからサイバー犯罪者の発言や行動パターンを抽出し、犯罪者のモデル化の可能性について検討する。更に、SIASを活用して，サイバー犯罪者の心理や指向と社会情報との関連性に基づくサイバー犯罪者像について研究する。