ボットネット攻撃元データの解析に関する研究

広口直樹
情報通信学研究科情報通信学専攻
指導教員　石井啓之教授

近年，インターネットの規模の拡大，利用度の高まりと相まって，セキュリティ上の数々の問題が顕在化している．

サイバー攻撃に対しては，攻撃元の特定，ボットの特定，マルウェアの種別の特定と対策，次回攻撃への準備など多角的な検討が必要である．それを行うために囮となるハニーポットが設置され，ウイルスやワームなどの検体の入手，不正アクセスを行う攻撃者をおびき寄せ重要なシステムへの攻撃を逸らしたり，記録された操作ログ・通信ログなどから不正アクセスの手法と傾向の調査を行うなど挙げられる．

本研究は，サイバークリーンセンター（CCC）が提供している，ハニーポットにより収集されたボット観測データ CCCDATAset を利用して，攻撃の各種パラメータについて統計的に解析し，その各種パラメータの分布が，異なる攻撃元同士，同じ攻撃元であって時間が異なるもの同士などに類似性があるか，相関を調べて評価することを目的としている．

その結果，社会事象と攻撃の関連性を図示システムを作成することにより示した．また，各国からの攻撃の時間推移のパターンが非常に関連が強いこと，また日本のインターネットトラヒックの動きとの関連性のあることを示した．