平成24年度 情報工学コース卒業研究報告要旨

高倉 研究室	氏　　名	廣 野 壮 志
卒業研究題目	適応的パケット誘導方式によるマルウェア動的解析環境の開発	

近年，マルウェアによるDoS攻撃や個人情報の漏洩，スパムメール送信などが社会問題となっている．このためマルウェアの動作を，比較的少ない労力で解明することのできるマルウェア動的解析が注目を集めている．マルウェアの多くは外部との通信に依存した動作をするため，マルウェアの詳細な動作を明らかにするためにはインターネットに接続した状態で解析を行う必要がある．しかしこうした解析環境でマルウェアの実行を行うと外部へ影響が及ぶことが問題となっている．

そこで本研究では適応的パケット誘導方式の提案を行い，安全に，かつ多くの動作を観測することのできるマルウェア解析環境の開発を行った (図1)．本方式では解析環境にインターネットサービスを模倣するサーバ群である擬似インターネットと実インターネットを接続する．マルウェアから発生したトラフィックを，過去の履歴やペイロード情報を用いて，実インターネットと疑似インターネットのうち適切な方へと転送を行う．この方式では，ペイロード情報を用いた動的な振分け先の変更を行うことができるため，より細やかな制御が可能となる．また過去のトラフィック履歴を用いて応答を返すことで，より安全で再現度の高い擬似インターネットを構成することが可能となった．

提案システムに対する評価実験を行うために，ファイルのダウンロードを行うマルウェアとDoS攻撃を模擬したプログラムの実行を行い，得られたトラフィックの内容を調査した．その結果，インターネット隔離環境では対応することのできないファイルのダウンロード動作にも対応できることがわかった．またDoS攻撃のようなトラフィックに対しても，履歴に基づく返答を行うことで外部への影響を最小限に留めることが可能であった．

今後の課題として，パケット振分け先を判断する手法の改良が挙げられる．トラフィックの履歴情報に加えて，IDSのシグネチャによるペイロードの検査や，通信流量の変動などを振分け先決定のための追加の情報として用いることで，より安全な解析環境の構築を行なっていく必要がある．

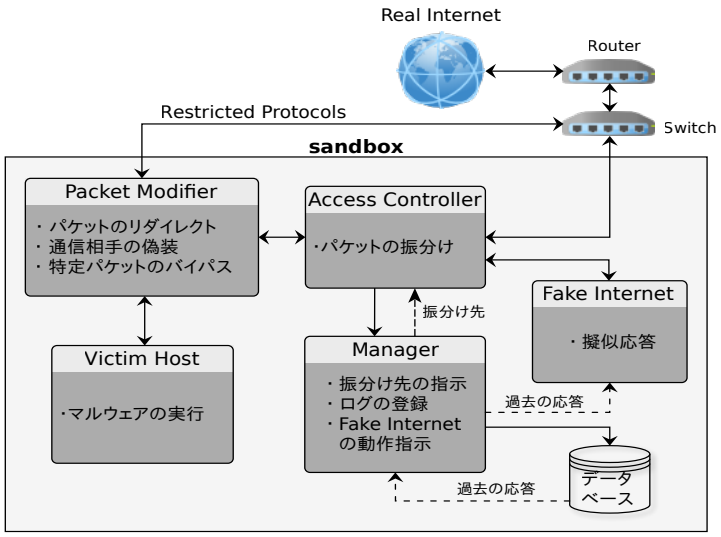

図1：マルウェア動的解析環境の構成図