先端科学技術研究科　修士論文要旨

所属研究室 (主指導教員)	情報基盤システム学 (藤川　和利 (教授))		
学籍番号	2011113	提出日	令和 4年 1月 21日
学生氏名	小松　聖矢		
論文題目	IPフロー情報を用いた最適化されたスライディングウィンドウに基づくマルウェアトラフィック検知		

要旨

マルウェアの活動トラフィックをネットワーク上で検知するネットワーク型マルウェア検知システムの研究が盛んに行われている. しかし, このシステムが検知に利用するIPフロー情報には特徴量の出力がフロー終了やタイムアウトに依存しフロー終了前に検知することが困難であるという問題と, パケット送信間隔の偏りといったフロー中間部の特徴を捉えられず検知が回避されるという問題が存在する. 加えて, IPフロー情報を利用する関連研究は, フロー単体での検知ができないため, NAPT, NAT, VM等のアドレス変換装置内の複数ノードがアドレスを共有した際に一つの検知システムでマルウェアに感染したノードを特定することができない.

本研究ではIPフロー情報に存在するこれらの問題に対し, スライディングウィンドウ方式に基づくマルウェアトラフィック検知手法を提案する. 評価では, 本方式を導入した検知システムの検知性能と本方式が前述した問題を解決できるかを調査した. 本方式を導入することにより, フロー終了前の検知とフロー中間部の特徴を考慮した検知が可能となる.