主　論　文　要　旨

報告番号	甲　乙　第　　号	氏　名	川口　信隆

主 論 文 題 目 :
Detection of Hit-list Worms based on Propagation Behavior
(感染特性に着目したヒットリストワームの検知手法)

（内容の要旨）

本論文は，感染特性に着目したワームの検知手法に関する研究成果をまとめたものである．

コンピュータネットワークにおける脅威のひとつとして，ネットワークワームが挙げられる．ワームは，ホストの脆弱性を悪用し侵入することで，ネットワーク中に自身を拡散していくプログラムである．ワームによる被害を抑えるためには，早期検知が重要となる．ここで，多くのワームは脆弱性ホストを発見するためにアドレススキャンを行う．既存の検知手法の多くはこの点に着目し，スキャンホストを検出することでワームを検知してきた．しかし，近年，これまでのワームとは異なる感染形態をとる「ヒットリストワーム」というワームが出現しつつある．ヒットリストワームは，アドレススキャンの代わりに，脆弱性ホストのアドレスリストを用いて感染先を決定する．このため，既存手法による検知が非常に難しいという問題がある．

本研究の目的は，エンタープライズネットワークを対象に感染を行うヒットリストワームの早期検知を実現することにある．我々は，ワームが感染を行っていく段階で，感染ホストをノード，感染コネクションをエッヂとするツリー構造が現れるという点に着目した検知を行う．また，複数のIDS(Intrusion Detection System)が協調する事で，ワームを分散的に検知する手法を確立する．

本論文の構成を以下に示す．第１章は本論文の序論であり，本研究の背景と目的，位置づけについて述べている．

第２章では，本研究に関連する技術的背景，特にネットワークワームの分類と既存の検知手法について概説する．

第３章において，ACTM(Anomaly Connection Tree Method)というワーム検知手法を提案する．ACTM は，ワームの感染コネクションにより構成されるツリー構造を追跡していくことで，ワームの存在を検知する．ACTM は，ツリーを構成する各コネクションの異常性を考慮することで，既存のアプローチに比べて高速なワーム検知を実現する．

次に第４章において，ACTM に基づく分散ワーム検知手法について述べる．この手法では，ネットワーク内に配置された複数の IDS が協調動作することでワームを検知する．各 IDS は，自身の監視対象ホストと他の IDS から得られた情報を元にツリー構造を追跡していく．この手法では，ネットワーク全体の情報を１つのサーバに集約する必要が無く，個々の IDS が保持する必要がある情報量が少ないため，ネットワークサイズに対してスケーラブルであるといえる．

最後に第５章において，一連の研究を総括し，また今後の課題と展望について述べる．

本研究では，ワームの感染特性に着目し，また IDS を協調動作させることで，ヒットリストワームの分散検知手法を確立した．また評価実験を通じて，本手法の有効性について確認した．