氏　名　　小　島　　俊　輔

主論文審査の要旨

近年、コンピュータウィルスによる感染被害や各種サーバに対する妨害、サービスの停止を狙ったDoS/DDoS（Denial of Service/Distributed DoS）攻撃などのサイバー攻撃が後を絶たない。DoS/DDoS攻撃、コンピュータウィルスやワーム、攻撃自動化プログラム（通称ボット）に感染したPCのパケットを瞬時に、かつ自動的に発見できれば、サイバー攻撃の被害を最小限に抑えることができる。そのためには、コンピュータネットワークにおいてパケットをリアルタイムに監視し、通常とは異なるトラヒックの変化を捉えることが重要である。そこで、本論文は統計的攻撃検出手法において正確性を向上させることを目的とし、新たな検知手法を提案して、その評価を行っている。

本論文は全7章から構成されている。

第1章では、本論文の研究背景と目的が述べられている。

第2章では、攻撃検知の概要について述べ、関連用語を定義している。そして、統計的な攻撃検知に関する従来研究についてまとめ、従来手法の問題点を明らかにしている。

第3章では、攻撃検知や侵入検知、サイバー攻撃などの分野において攻撃の検知性能を評価するために公開されている各種データセットについて論じ、データセットとしてDARPA（Defense Advanced Research Projects Agency:国防高等研究計画局）データセットを選択している。DARPAデータセットは、多くの種類の攻撃を含んでおり、攻撃パケットや通常パケットに匿名化などの加工が施されておらず、さらに全ての攻撃パケットに付与されたラベルにより攻撃検知の正確性を客観的に評価することができる。

第4章では、エントロピー手法にマハラノビス距離を適用した統計的手法であるEMMM（Entropy-based Multi-dimensional Mahalanobis Method）を提案している。EMMMはDDoS攻撃やIPアドレススキャンを高い精度で検知し、正確性に加え攻撃多様性を有し、即応性と追従性を備える手法であることを示している。

第5章では、$\chi 2$値をベースにした、複数の特徴量を同時に攻撃に用いることができるCSDM（Chi-square based Space Division Method）を提案している。攻撃検知性能の評価結果から、従来手法と比較して正確性が向上することを明らかにしている。また、CSDMにおいて補助的に使用する動的Bin（ビン）手法を提案し、組織多様性に加え追従性を備えた手法であることを示している。

第6章では、第4章および第5章の提案手法の特性を調査している。評価結果からCSDMはエントロピーベースの手法と比較して、複合攻撃耐性を有することを明らかにしている。また、理論的な計算量の検討と実際の計算時間の計測の結果、EMMM、CSDMのいずれの提案手法も高速計算性を有することを示している。

最後に、本論文で得られた研究成果を第7章で総括している。

以上のように、本論文の内容は、新たなネットワークベースの統計的攻撃検知手法を提

案し、実装実験によりその実用性を示しており、学術的及び工学的に価値が高いものである。また、これらの研究成果の主要部は、審査付き学術雑誌論文 3 編、審査付き国際会議論文 8 編として公表されている。よって本審査委員会は、本論文が博士（工学）の学位授与に値する論文であると判断した。

審査委員　情報電気電子工学専攻　先端情報通信工学講座　末吉　敏則　教授
審査委員　情報電気電子工学専攻　先端情報通信工学講座　趙　　華安　教授
審査委員　情報電気電子工学専攻　人間環境情報講座　　上田　裕市　教授
審査委員　情報電気電子工学専攻　先端情報通信工学講座　久我　守弘　准教授
審査委員　情報電気電子工学専攻　先端情報通信工学講座　飯田　全広　准教授