氏　名　ルデニャ　ロマニャ　デニス　アルトゥロ
LUDEÑA ROMAÑA, Dennis Arturo

主論文審査の要旨

本論文は、コンピュータウィルスに感染し、攻撃者の操り人形と化したボットと呼ばれるPCやサーバのIPアドレスを検知する技術を開発評価したものである。ボットが攻撃通信を行うと同時に送信されるDNSクエリパケット流量ログ(DNSパケットログ)の送信元IPアドレスとクエリキーワードについてエントロピー値の測定を行い、ボットのIPアドレスを特定する技術を提案した例はまだない。また両エントロピー値の変化パターンから、ランダム攻撃モデル、標的攻撃モデル、およびホスト名探索攻撃モデルを提案し、評価している。

本論文は全１０章から構成されている。

第１章では、ICT社会におけるボットの脅威と対策技術および関連研究について述べている。

第２章では、本論文の研究の背景およびボットとボット連結ネットの脅威について述べている。

第３章では、一般的なセキュリティ防御技術として侵入検知システム(IDS)について述べ、シグネチャ非依存型のIDSの必要性について述べている。

第４章では、ログの回帰分析やエントロピー分析などの一般的な統計的分析手法について述べている。

第５章では、本論文における、統計的分析を行うに当たって、DNSパケットログ中の送信元IPアドレスとクエリキーワードに着目したことについて述べている。

第６章では、閾値を越えたDNSパケットログ中のキーワードについて回帰分析を行い、その結果、迷惑メール送信型(スパム)ボットのIPアドレスの検知が可能であること、またDNSパケットログ中の送信元IPアドレスとクエリキーワードのエントロピー値の変化を測定することにより、組織内の攻撃を行ったボットのIPアドレスの検知が可能なことを見出している。

第７章では、DNSパケットログ中の送信元IPアドレスとクエリキーワードの両エントロピー値変化の観察から、ランダム攻撃、標的攻撃、およびホスト名探索攻撃の３種類のボット攻撃モデルについて提案し、本学のDNSサーバで採取した一年分(2008年)のDNSパケットログの送信元IPアドレスとクエリキーワードの両エントロピー値の変化を測定したところ、学内からのDNSパケットログでは標的攻撃を行うボットのIPアドレスのみが検知できることを見出しており、また学外からのDNSパケットログではランダム攻撃、ホスト名探索攻撃、標的攻撃を行うボットのIPアドレスが検知できることを見出している。

第８章では、ランダム攻撃を行うスパムボットとSSH辞書攻撃ボットに関するDNSパケットログ中の送信元IPアドレスとクエリキーワードのエントロピー値の変化の仕方は、それぞれ対称的および非対称的であることを、またそれがインターネット上におけるメー

ルサーバ数とSSHサーバ数の相違によるものであることを見出している。

第９章では、本論文で提案されたDNSパケットログ中の送信元IPアドレスとクエリキーワードのエントロピー値の変化に基づくDNSパケットログ監視型ボット検知システム装置の開発を行い、ブロードバンドルータ配下に構築されたテスト用LANにおける実験運用の結果、プライバシーに配慮しなければならない現場での調査を行う場合に有効であると述べている。

第１０章では、結論として本論文の研究で得られた成果について総括している。

以上のように、本論文の内容は、企業や大学などの組織に潜伏するボットのIPアドレスの検知を効果的に行うための知見が得られており、またDNSパケットログの送信元IPアドレスとクエリキーワードのエントロピー値の変化のパターンから３種類以上のボットの攻撃が判別可能であることや、またエントロピー値の変化の対称性を観察することで、２種類の攻撃が分離可能であるという知見を提案しており、学術的に価値が高いと認められる。またこれらの研究成果の主要なものは、６編の査読付の国際学術論文誌および９編の査読付の国際学術会議発表とそのプロシーディングまたは抄録で公表されている。よって本審査委員会は、本論文が学位論文に値すると判断した。

最終試験の結果の要旨

審査委員会は、学位論文提出者に対して当該論文の内容ならびに関連分野の事項について試問を行った。その結果、学位論文提出者は、当該の研究分野及び関連分野について十分な知識と理解力を示し、研究遂行能力を有していると判断した。また、外国語に関しては、論文業績の中で、９件の英語による学会発表が示されており、十分なレベルの能力があると認めた。以上の結果に基づいて、審査委員会は最終試験を合格と判定した。

審査委員	情報電気電子工学専攻先端情報通信工学講座	教授	松島　章
審査委員	情報電気電子工学専攻先端情報通信工学講座	教授	末吉　敏則
審査委員	情報電気電子工学専攻先端情報通信工学講座	教授	杉谷　賢一
審査委員	情報電気電子工学専攻先端情報通信工学講座	准教授	武藏　泰雄
審査委員	情報電気電子工学専攻人間環境情報講座	教授	上田　裕市