別紙１－１

論文審査の結果の要旨および担当者

報告番号	※ 甲 第 号

氏　　名　　長谷川　皓一

論　文　題　目　　動的ネットワーク構成によるサイバー攻撃対策支援手法の研究

論文審査担当者

主　査	名古屋大学教授	村瀬　勉
委員	名古屋大学教授	高田　広章
委員	国立情報学研究所教授	高倉　弘喜
委員	名古屋大学准教授	嶋田　創

論文審査の結果の要旨

長谷川皓一氏提出の論文「動的ネットワーク構成によるサイバー攻撃対策支援手法の研究」は、近年において大きな社会問題となっている標的型サイバー攻撃に対し、組織内でのマルウェア感染拡大を防止するネットワーク構築から侵入された後の対応時間の短縮手法に関する一連の研究をまとめたものであり、全体は7章から構成される。

第1章は序論であり、近年のサイバー攻撃の傾向について、技術的な面や社会に及ぼす影響などを多角的に述べている。

第2章では、本論文で対象とする標的型サイバー攻撃などの近年のサイバー攻撃の特徴について述べており、典型的な標的型攻撃の一連の流れ、社会的に話題となった実標的型攻撃の詳細、手動によるネットワーク分割などの従来対策について述べている。

第3章では、本論文で提案する動的ネットワーク構成によるサイバー攻撃対策支援のシステム構成の全体像について説明するとともに、提案システムおいて基盤とする既存技術である、ネットワーク機器自動設定や不正通信監視などについて述べている。

第4章では、組織内ネットワークに侵入したマルウェアの感染拡大活動を抑える内部分離設計されたネットワーク構成の自動構築についての提案を行っている。提案では、組織内ディレクトリサービスから得られたアクセス権限と現ネットワークの通信トラフィックから得られた情報をもとに、分離するのが妥当な通信対象を抽出する。提案システムは、内部分離設計を構築の補助を可能とするのみならず、ネットワーク管理者に対する内部分離設計の学習にも効果があるという評価結果が得られている。

第5章では、内部分離設計されたネットワークを利用し各セグメント単位で脅威レベルを設定した巡回監視を行なうことにより、全ネットワークを一括して監視することによる監視のための機器や人材のコストを低減し、コストと検知時間について議論を行った。同時に、誤検知や端末側の防衛機構で止められた軽度の攻撃の検知など、脅威度の低いアラートの除外の実現に関する提案を行った。

第6章では、マルウェア感染が確認された組織内ネットワークに対し、業務停止を伴う全ネットワークを停止という対策を取るのではなく、算出した業務影響度と感染拡大危険性をもとに、業務影響度を最小化した通信遮断などの対策案を提示する手法について提案している。算出結果より有効性の高い方から複数対策案を管理者に提示する実システムを構築して評価し、対策適用時間を大幅に短縮する成果が得られている。

第7章は結論であり、本論文の成果のまとめと今後の発展について述べている。

以上のように、本論文は、対標的型サイバー攻撃技術おいて、ネットワーク構築段階から初期侵入後までの幅広い攻撃段階において、動的ネットワーク構成手法の応用で対応する提案を行っている。また、実組織を模したネットワークにおける実証実験によりその有効性を確認し、その有効性は対外的な学術論文発表で広く認められている。

よって、情報科学の学術上・技術上の寄与が大きいと考え、本論文提出者である長谷川皓一氏は博士(情報科学)の学位を受けるに十分な資格があるものと判定した。