別紙様式第２号

学位論文及び審査結果の要旨

横浜国立大学

氏　　名	齊藤　聡美
学位の種類	博士（情報学）
学位記番号	環情博甲第 1997 号
学位授与年月日	平成 30 年 3 月 23 日
学位授与の根拠	学位規則（昭和 28 年 4 月 1 日文部省令第 9 号）第 4 条第 1 項及び横浜国立大学学位規則第 5 条第 1 項　（論博の場合は第２項）
学府・専攻名	環境情報学府　情報メディア環境学専攻
学位論文題目	複数サーバログの関係性分析による攻撃検知に関する研究
論文審査委員	主査　横浜国立大学　教　授　松本　勉 横浜国立大学　教　授　森　辰則 横浜国立大学　教　授　四方順司 横浜国立大学　准教授　吉岡克成 横浜国立大学　講　師　白川真一

論文及び審査結果の要旨

組織のネットワークやクラウドサービスの顧客に対するサイバー攻撃を監視するため、セキュリティオペレーションセンター（SOC）の導入が進んでいる。SOC ではファイアウォールや侵入検知システムといったセキュリティ機器、ネットワーク機器や端末のログなどを定常的に監視し、脅威となるインシデントの発見や特定を行う。近年、攻撃の巧妙化により、個々のセキュリティ機器やサーバのログ分析による攻撃の検知が難しくなっており、SOC において攻撃の状況を把握する上で問題となっている。本論文は、巧妙化する攻撃に対応するため、個々の機器やサーバのセキュリティログだけでなく、複数の機器からのログを対象に分析を行うことにより、攻撃検知精度を向上する方法について論じたものである。

本論文では、複数のサーバから取得したセキュリティログを対象とし、サーバ間の関係性に着目することで、攻撃事象を抽出する方法が提案されている。異なる目的で設置された複数のサーバの通信は、通常異なる特徴を持っていると考えられる一方で、サイバー攻撃は多様なサーバに対して脆弱性を探索し、これを狙うといったように共通の特徴を有している場合がある。そこでサーバ間で関係性が高い事象を攻撃通信として検出する。

本論文ではこのアプローチの有効性を検証するため、複数の Web サーバに対するアクセスログ、および、複数のサーバを保護する侵入検知システム（Intrusion Detection System, IDS）の攻撃検知ログを用いて評価実験を行っている。評価の結果、既存の攻撃検知手法では悪性の判断が難しかった攻撃事象を抽出できることを示している。

本論文の貢献は、複数のサーバ間の関係性に着目するアプローチに基づき、具体的な分析手法を提案し、実際に運用されているサーバからの膨大なログに潜む攻撃事象の抽出を行っているところにある。

本論文は 6 章からなり、第 1 章の序論で研究の背景と目的、本研究の実証実験で分析対象とするログについて説明している。第 2 章で先行研究に触れ、3 章では、Web ホスティングサービスにおける複数サーバのログを用いた攻撃検知手法とその評価を行っている。その結果、Web アプリケーションに対する攻撃を目的とした悪意あるリクエストのうち、既存の侵入検知システムでは検知が難しい攻撃の検知に成功している。4 章では複数のサーバに設置された侵入検知システムから得られる攻撃検知ログから、SSH（Secure Shell）サ

ービスを狙った分散型ブルートフォース攻撃の検知を行っている。その結果、送信元の IP アドレスを変更しながら特定の目標に対して行われるステルス性の高い攻撃の検知に成功している。5 章では、4 章と同様に複数のサーバに設置された侵入検知システムから得られる攻撃検知ログから RDP (Windows Remote Desktop) サービスを狙った分散型ブルートフォース攻撃の検知を行っており、送信元 IP アドレスを変更しながら行う攻撃の共通規則に着目してこれを検知できることを示している。そして最後に 6 章で結論を述べている。

以上のように、本論文は、様々な実運用サービスにおいて実際に発生しているサイバー攻撃を検知する手法を提案し、膨大な実際のログを用いてその効果を示しており、サイバーセキュリティ分野に貢献する内容を有していると評価できる。本論文の研究内容は、査読付論文誌論文 3 篇、査読付き国際会議論文 4 篇（ショートペーパー1 件、ポスター発表 1 件を含む)、研究会論文 9 篇により公表され、学会で評価を得ている。

よって、本論文は博士（情報学）の学位論文として十分な価値を有すると論文審査委員全員一致で認め、平成 30 年 2 月 9 日 10 時から 11 時 30 分まで、環境情報 1 号棟 515 号室において博士論文発表会（公聴会）を開催した。博士論文発表会は 50 名の参加者を得て充実した質疑応答がなされた。同日 11 時 30 分から 12 時まで、同棟 303 号室において論文審査委員全員出席のもとで、齊藤聡美氏の最終試験を行った。審査委員からの博士論文に関する質問、セキュリティを中心とする専門分野および情報工学関連分野における口頭試問を行い、これらの専門知識に関する質問に対する応答から、専門知識、博士論文の内容の公表状況について十分であることを確認した。外国語については、英語による論文執筆ならびに発表があることをもって学力を確認した。また、履修単位が修了要件を満たすことを確認した。これらから、同氏は最終試験に合格であると、論文審査委員全員一致で判定した。

以上の論文審査委員会の結論に基づき、平成 30 年 2 月 15 日に開催した環境情報学府 情報メディア環境学専攻会議にて審議し、全員一致で本論文を博士（情報学）の学位論文としての価値があるものとして環境情報学府教授会に付議することを決定した。その後、環境情報学府学務委員会での確認を経て、平成 30 年 3 月 5 日に開催された環境情報学府教授会において審議を行い、無記名投票により、齊藤聡美氏に博士（情報学）の学位を授与することを決定した。

注　論文及び審査結果の要旨欄に不足が生じる場合には、同欄の様式に準じ裏面又は別紙によること。