氏　名	宋　中錫

（論文内容の要旨）

本論文は、教師無し機械学習に基づくネットワーク型侵入検知システム（Intrusion Detection System; IDS）の性能向上に関するもので、全７章から構成されており、それぞれの章の内容は以下の通りである。

第１章は緒論であり、本研究の背景と目的および全体の構成と各章の概要について説明している。

第２章では、侵入検知システムおよび教師無し機械学習に基づく異常検知手法に関する基本概念と、性能評価に用いるデータについて説明している。

第３章では、異常検知型侵入検知手法の性能向上について論じ、K-meansクラスタリング手法を改良した新しいクラスタリング手法を提案している。計算量の少ないK-means法の特長を維持しつつ、正常パターンベースIDSの検知精度およびFalse Positive(正当な通信を攻撃として誤検知すること)率を改善したものである。

第４章では、サポートベクターマシン(SVM)と第３章での提案手法とを併合した侵入検知手法を提案している。第３章の手法により全体的なシステム性能は改善されたものの、正当な通信に似せた新種の攻撃に対する検知精度が低い問題点があった。この問題点を指摘し、このような攻撃に対する検知精度を向上させるための手法を提案している。具体的には第３章のクラスタリング手法にSVMを適用することで、この問題を解決している

第５章では、シグネチャベースのIDSが発する警告を分析データとして、新種の攻撃（いわゆるゼロデイ(0-day)攻撃）を効率的に検知する一般的な手法について論じている。学習アルゴリズムとしてはSVMをそのまま利用しているが、IDS警告から未知の攻撃を検知するのに適した新しい特徴量およびその抽出手法を提案している。

第６章では、実データを用いた既存手法と提案手法の性能評価について述べている。京都大学のハニーポットから収集した実データを用いて、これらの提案手法と既存の手法を検知精度、False Positive率、新種の攻撃の検知精度、トレーニング時間、テスト時間等の観点から多角的に評価し、既存のシステムに対する優位性を示している。

第７章では、結論と今後の展望について述べている。

氏　名	宋　中錫

（論文審査の結果の要旨）

ネットワークの普及とともに、不正アクセスやウイルス、ワームなど、安全なネットワーク利用を脅かす諸問題も多様化・複雑化しており、いかに安全にネットワークを運用できるかが重要課題となっている。本論文は、ネットワークの安全確保のための効果的な防御機構である侵入検知システム（IDS）の性能向上を主題としている。IDSはネットワーク上の不審なアクセスの兆候を検知し、ネットワーク管理者に通報するシステムである。

IDSによる侵入検知にはさまざまな手法が提案されているが、本論文では教師無し機械学習に基づくネットワーク型侵入検知システムの性能向上手法を提案している。現在の商用のIDS製品などの大半が採用しているシグネチャ(攻撃パターン)ベースのIDSの検知精度の限界、特にシグネチャが未定義の新種の攻撃には対応できない問題点に着目し、本論文では以下の特徴的な手法を提案している。

1. 正常時の状態やパターンと比較することで侵入を検知する異常検知ベースのIDSについて、K-meansクラスタリング手法を改良している。具体的には良い初期センター値を導く手法と、クラスタを適応的にマージする手法である。これにより、計算量が少ないなどのK-means法の利点を損なうことなく多くの従来手法を凌駕している。

2. 異常検知ベースのIDSにおいて、正当な通信に似せた新種の攻撃に対する検知精度を向上させるために、SVMを用いる手法を提案している。従来研究では正常領域を一つのhypersphereとして扱っていたのに対し、本論文では正常領域を複数のhypersphereによる細分化を可能にし、未知の攻撃に対する検知精度を飛躍的に向上させている。

3. シグネチャベースのIDSが発する警告から新種の攻撃を検知する新しい手法を提案している。実観測データに基づき新種の攻撃が持つ特徴を精緻に分析し、未知の攻撃によりIDSが発する「誤報」から攻撃を検知するための新しい特徴量およびその抽出手法を定義している。

今日のIDSが、膨大なトラフィックデータの中から日々現れる新種の攻撃を検知しなければならない現状を考え、本研究が、正常時の状態やパターンの生成を機械学習により自動化し、検知性能の維持と向上のための作業を効率化した点は意義深い。さらに、既存研究がシミュレーションデータに基づいた競争に終始している問題点を指摘し、実環境における観測データによるシステム評価を行い、より現実的なシステムを提案している点も特筆すべきである。よって、本論文は博士（情報学）の学位論文として価値あるものと認める。

また、平成２１年２月１６日実施した論文内容とそれに関連した試問の結果合格と認めた。