平成29年度 情報工学コース卒業研究報告要旨

村瀬（勉） 研究室	氏　　名	大 橋　宗 治
卒業研究題目	ハニーポットへの攻撃に対するNIDS検知反応を利用したシグネチャ自動チューニングに関する研究	

近年、サイバー攻撃が深刻化し、大規模な被害が多く確認されており、セキュリティ対策への需要は増々高まっている。サイバー攻撃への一般的なセキュリティ対策のひとつとして侵入検知システム（IDS）がある。IDSにおいては、シグネチャ型の検知方法が広く用いられている。これはあらかじめ不正な通信のパターンを記述したシグネチャをもとに、通過するパケットとパターンマッチングすることで不正を検知する仕組みである。

しかし、シグネチャ型IDSはシグネチャのチューニングが不可欠であり、専門的な知識と多くの運用コストを必要とする。これは膨大なシグネチャからIDS下で運用中のシステムに応じたものを選び、さらに日々変化する攻撃の傾向にも対処していく必要があるためである。不適切なチューニングは不正アクセスの見逃しや、通信量の多い環境におけるパフォーマンスの低下に繋がるためシグネチャのチューニングは重要である。

そこで、本研究ではハニーポット及びチューニング情報収集用IDSを新たに用い、この問題点を解決する手法を提案する（図1）。本手法ではセキュリティ設定の甘いシステムを装い攻撃者を誘い込むシステムであるハニーポットを用い、多くのシグネチャを適用させたチューニング情報収集用IDSでハニーポットへの攻撃に対するシグネチャの検知反応に関する情報を取得し、分析する。この分析結果をもとにチューニングされたシグネチャセットを実運用IDSに反映させることで、実運用ネットワークの安全性を高めるというものである。

提案手法の評価実験では、インターネットからアクセス可能な環境に設置した複数のハニーポット（T-Pot、Glastopf、Cowrie、Dionaea）、及びEmerging Threat rulesとSnort VRT rulesから得た68,371個のシグネチャを適用させたチューニング情報収集用IDS（Suricata）を用いた。2018年1月12日から7日間、これらで攻撃情報を取得しシグネチャのチューニングを行い、その後7日間を検証期間とし、チューニングされたシグネチャセットにおける検知結果を分析した（図2）。デフォルトで設定されていた12,976個のシグネチャとチューニングされたシグネチャセットとの検知結果を比較検証した。検証期間に反応を示したシグネチャは213個であり、デフォルト設定では見逃し率は約54%であった。これに対して、チューニングによって得た198個のシグネチャでは見逃し率を約29%に抑えることが可能であった。

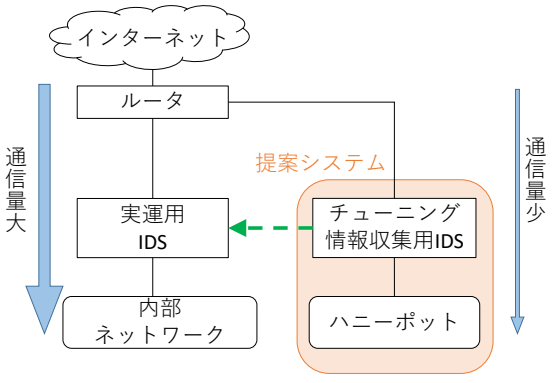

図1 提案手法

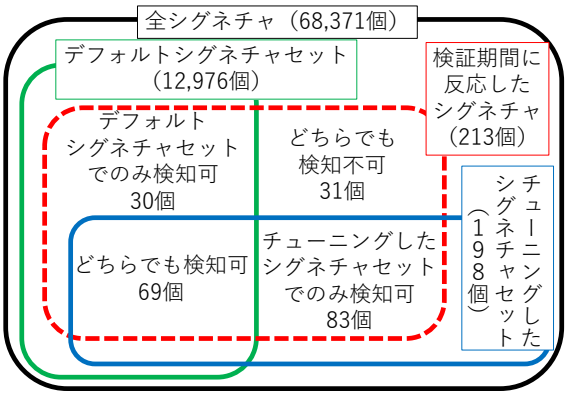

図2 実験結果