平成23年度 情報工学コース卒業研究報告要旨

高倉 研究室	氏　　名	佐藤 正明
卒業研究題目	特徴抽出によるアノマリ型IDS警告ログからの未知攻撃検出	

侵入検知システム（Intrusion Detection System:IDS）はネットワーク上の攻撃者からコンピュータシステムやネットワークを守る手段として重要な役割を担っている．IDSの検知方法には，攻撃の特徴を予め定義したシグネチャを用いて検知するシグネチャ型と，正常トラフィックの特徴を学習し，その特徴から逸脱した異常トラフィックを攻撃として検知するアノマリ型が存在する．シグネチャ型IDSは事前に各攻撃に対してシグネチャを定義しなければならないため未知攻撃を検知する事が難しい．そこで，近年では未知攻撃を検知可能なアノマリ型IDSの研究が盛んに行われている．

しかし，アノマリ型IDSは誤検知率が高く，正しい警告が誤検知に埋もれてしまうという問題がある．さらに，通信トラフィックが正常か異常かという分類しかできず，また，既知の攻撃が日々大量に観測されているため，たとえ未知攻撃を検出できたとしても大量の警告の中からどれが未知攻撃なのかを判断することは非常に困難である．

この問題に対して本研究では，未知攻撃の特性を考慮した特徴抽出を行うことでアノマリ型IDSの警告から未知攻撃に関する警告を検出する手法を提案した (図1)．未知攻撃の特性として，長期的な攻撃が行われること，開発や改良に伴ってセッションサイズが頻繁に変化すること，またそのプログラミングに時間を要するため攻撃の間隔が不規則であること，攻撃の存在が世間に知られるのを防ぐため特定のホストやネットワークのみに攻撃を行うことなどが挙げられる．さらに，本手法では各警告に対するシグネチャ型IDSの検知結果も使用した．一般的にシグネチャ型IDSは未知攻撃を検知できないと言われているが，未知攻撃に対して複数の異なる種類のシグネチャが反応するという事例が確認されている．これらの未知攻撃の特性を利用し，接続時間，送受信バイト数，特定のホストへの接続回数，警告の時間間隔，警告の種類など10特徴をアノマリ型IDS警告ログから抽出した．そして，これらの特徴データを用いてOne-Class SVMの学習モデルを作成し，テストデータと学習モデルを比較することで警告ログから未知攻撃に関する警告を検出した．

提案手法に対する評価実験を行うために，過去の研究で未知攻撃の存在が確認されている日のデータについて本手法を適用した．その結果，未知攻撃に対する検知率と誤検知率はそれぞれ71%，3%であった．また，既存研究では検出できなかった，シグネチャ型IDSが反応していないがアンチウイルスソフトが検知している未知攻撃について18件中5件を検出することができた．このような未知攻撃に対する検知率をさらに向上させることが今後の課題である．

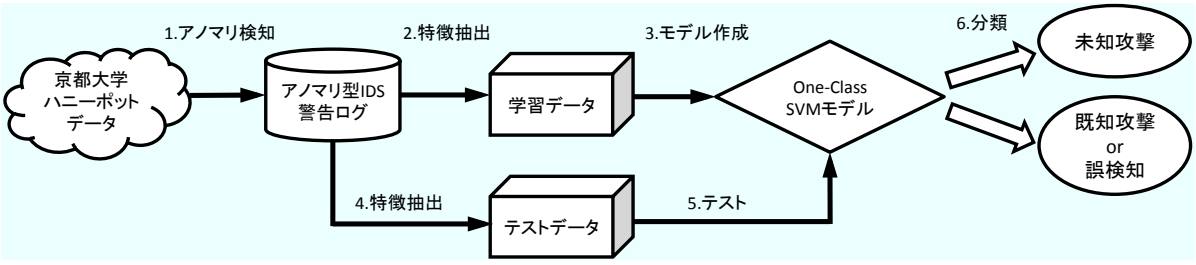

図1：提案手法の流れ