平成25年度 情報工学コース卒業研究報告要旨

高倉 研究室	氏　　名	荒 木 翔 平
卒業研究題目	通信間隔に着目したOne-Class SVMを用いた未知攻撃検出	

近年，インターネットの社会インフラ化に伴い，インターネットを介したサイバー攻撃による被害が急増しており，その対策が増々重要になっている．サイバー攻撃への対策の一つに侵入検知システム (IDS:Intrusion Detection System) がある．IDSには通過するトラフィックがあらかじめ登録されている攻撃パターンと一致するかどうかで攻撃の検知を行うシグネチャ型と，正常なトラフィックの学習を行い，通過するトラフィックが学習モデルから逸脱していた場合に攻撃と検知するアノマリ型IDSが存在する．シグネチャ型IDSでは攻撃パターンが登録されていない未知の攻撃を検知できないため，それらの攻撃も検知できるアノマリ型IDSが注目されている．

しかし，アノマリ型IDSにはシグネチャ型IDSと比較して，検知率が低く，誤検知率が高いといった問題がある．これは、新しいアプリケーションの登場などネットワーク利用の状況が頻繁に変化し，また，正常な通信であってもRFC等に準拠しない通信が多いため，正常な通信と不正な通信の特徴量が似てしまい、最新のネットワークの状態を適切に反映した学習モデルの作成が難しいためだと考えられる．また，アノマリ型IDSでは正常か攻撃かの識別しか行われないため，検知された結果の中からどれが未知の攻撃であるのかを判断できない．

そこで，本研究では複数のOne-Class SVMを用いて未知攻撃検知を行う手法を提案した (図1)．提案手法では，まず，セッションデータから特徴量を抽出し，学習データとテストデータを作成する．作成したデータに対してOne-Class SVMを用いて学習，識別を行い，未知攻撃を含む攻撃のセッションの検知を行う．その後，攻撃と判定されたセッションを学習データとしてOne-Class SVMに学習させる．攻撃と判定されたセッションの大部分は既知の攻撃であるので，この識別器では既知の攻撃かどうかを判断を行う．その後，別の日付のテストデータに対する検知結果について識別を行い，攻撃が未知の攻撃であるか既知の攻撃であるかの分類を行う．

提案手法に対する評価実験を行うため，京都大学ハニーポットデータに対して従来のセッションデータの特徴量にパケットの送信間隔やそのサイズ，セッションの通信間隔といった6つの特徴量を新たに追加し，本手法を適用した．その結果，未知攻撃を含む攻撃の検知では誤検知率5%に至るまでに検知率80〜90%と高い検知率を得ることができ，新たな特徴量を追加しない場合よりも低い誤検知率にて高い検知率を得ることができた．また，シグネチャ型IDSが反応せず，シェルコードやエクスプロイトコードが含まれている未知の攻撃の検知では誤検知率が高かったものの70%の検知率にて検知できた．これらの攻撃検知に関して，新たなフィルタリングやクラスタリングを適用することで適切な学習データを作成し，検知の際の誤検知率を低く抑え，検知率を高くしていくことが今後の課題である．

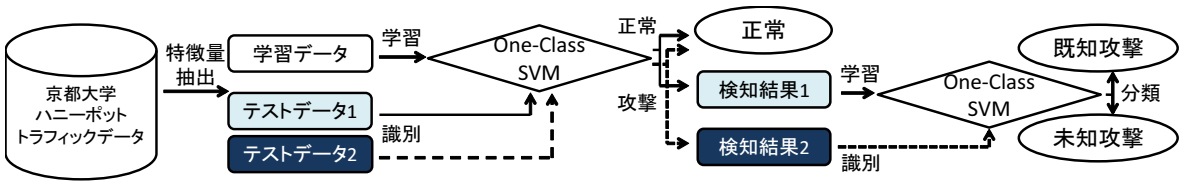

図1 提案手法の流れ