2007 年 5 月 01 日（水）
1031060322 松本　亮介

自己組織化マップを用いた ネットワークトラフィックからの異常検出（概略）

0 はじめに

※この資料は，参考文献を元に，参考文献の概略を作成したものです．この研究を私が実際に行ったわけではありませんので注意してください．

1 概略

ネットワークの不正アクセスが普及してきている中，不正検出によるパターンマッチング手法では，検出できないような不正アクセスが現れてきている．そこで，未知の不正アクセスを検出することができる異常検出の内，自己組織化マップを用いた手法に注目する．

まず，パケットのヘッダ情報を種別ごとにカウントする．次に，ネットワークトラフィックのパケット長フィールドの値の数を，任意の範囲でカウントする．その値の数を圧縮してカテゴリーとし，カテゴリーを要素とする多次元ベクトルデータを数値化する．数値化されたベクトルデータの有効性を検証するために，重回帰分析を行い，異常検出において有効である特徴量を分析する．そして，作成されたベクトルデータを基に，教師なし学習を行うニューラルネットワークの一種である自己組織化マップを用いて，トラフィックが正常な状態のデータベースを作成する．最後に，トラフィックから得られる入力データとそのデータベースとのベクトル距離を計算し，距離の離れたデータを異常として検出する．

通常，異常検出手法において，異常か正常かを分類するデータベースを作成する処理に時間がかかってしまう．しかし，自己組織化マップの学習アルゴリズムである教師なし競合近傍学習を用いることで，その処理時間を早くすることができる．というのは，異常検出の場合，異常か正常かといった２種類のデータしかなく，一方のデータ数が多いようなデータ群で学習させる場合，正常状態のデータはデータ数が多くなるため，その特徴を持ったマップは大きく形成される．そのため，少数の異常データでマップが大きく変化することはない．このように，正常状態のデータのみで作成されたマップと，異常状態を含んだデータで作成されたマップは，大きい違いはないと考えられる．そのため，異常状態のデータを削除する処理を行うことなく，正常状態のデータベースを作成できる．

この手法だと，FTP，Telnet，SMTP，DNS，では有効な結果が得られるが，HTTP に関しては，単位時間に含まれる正常パケット数が多いため，非常に特徴のある文字列を含むパケットであっても，それが少数の異常パケットである場合は，全体として特徴が現れないという結果になることがある．というのは，HTTP における DOS 攻撃では，１パケット送信するだけでサーバーをクラッシュできるような有名なものがあり，そのような攻撃を多用することが多いからである．

参考文献

[1] 宮本雅人，“自己組織化マップを用いたネットワークトラフィックからの異常検出”