L-005

自己組織化マップによる不正アクセスの予測
An Intrusion Prediction Based On Self-Organizing Maps

中山 亮介† 納富 一宏† 斎藤 恵一‡
Ryosuke NAKAYAMA Kazuhiro NOTOMI Keiichi SAITO

1. はじめに

近年，インターネットへの常時接続やモバイル端末等の普及によりインターネットへ接続する人口が増加し，インターネット上でのサービスの普及が著しい．それに伴い，扱われる個人情報や機密情報も膨大な量となった．これらの情報が目的の侵入行為や，意図的にサービスを提供不能にさせる DoS(Denial of Service)などのネットワーク経由の攻撃が増加し，大きな問題になっている．このような行為によって企業への損害，個人情報の流出等が懸念され，情報セキュリティというものが重要視されるようになってきた．インターネット上の不正アクセスの種類は増え続けているため，管理者はそれに対応するためのパッチやアップデートなどを導入し，ネットワークを監視し続ける必要がある．しかし，それぞれの攻撃に対策はあるものの，すべてに対策をしていると非常に手間がかかってしまう．攻撃方法も様々なものが存在し，それを防ぐ方法もあるが，それぞれに別途対策をしていては管理者の負担が非常に高まってしまう．

本研究では未知である攻撃の予測を目的とする．具体的な実現方法として，自己組織化マップ(SOM: Self-Organizing Maps)を用いて既存の攻撃をあらかじめ特徴ごとに分類し，アクセスごとに既存の攻撃に類似しているかどうかで予測する方法を提案する．また，本研究では予備実験を行い[1]，不正アクセス検知に対する SOM の有効性を確認している．

2. 自己組織化マップ(SOM)

SOM とは，教師なし競合学習型のニューラルネットワークモデルの一つで，n 次元属性ベクトルにより表現された入力データを，属性の類似度に従って二次元平面上にマッピングする能力を持つ．属性ベクトルの持つ各属性の値よってマップに着色することも可能であり，単なるマップ上のユークリッド距離だけではなく，様々な視点で距離を求めることが可能である．本研究では，既知の不正アクセスとどの程度類似しているかを求めるのに SOM を用いた．

3. 提案手法

3.1 SOM による不正アクセス予測

不正アクセスの予測には SOM を用いる．SOM の属性ベクトルには OSS である Snort のシグネチャとして用いられているルールファイルを利用し，データ収集にかかるコストを省いた．

Snort とは，OSS(Open Source Software)として開発されているシグネチャ型 IDS で，侵入者を早い段階で検知して警告するシステムである．OSS であるため，誰でも自由に利用したり改変したりすることができる．不正アクセスの定義であるシグネチャをまとめたルールファイルは，Snort のコミュニティによって更新されているため，管理者はそれをダウンロードして適用しなければならない．

3.1.1 予測方法

あらかじめルールファイルからマップを生成，保持しておき，実際にネットワークを通過したデータの情報と照合する．その結果で不正アクセスかどうかを判断する．まず Snort のルールファイルから属性ベクトルを生成する．生成方法は後に述べる．次に属性ベクトルからマップを作成し，不正アクセスの種類ごとに保存しておく．そして，ネットワーク上を流れてきたデータから属性ベクトルを生成し，保存しておいたマップと照合する．照合の結果，不正アクセスと判断した場合は，警告を出したりネットワークから切断したりといった処理が考えられる．

不正アクセスにはさまざまな分類があるが，本研究では SOM を用いた未知の不正アクセスの予測を目的とするため，ベクトルの生成方法を 1 種類に限定して実験を行った．

3.1.2 属性ベクトル

SOM を利用する際には通信データなどから得られるパラメータを属性ベクトルにする必要がある．属性にはポート番号，通信方向，トランスポート層のプロトコル，通信内容に含まれる特徴的なデータ列を用いることとした．本研究で用いた実際の属性と値の例を表 1に示す．これは 12 バイト長のデータで，文字列の場合は基本的に ASCII エンコード，日本語の場合は Shift-JIS エンコードしたもの，バイナリデータの場合はそのままの値を用いる．ルールファイルに定義されているデータ長が 12 バイトに満たない場合は，残りの属性を 0.5 で埋める．トランスポート層のプロトコルが ICMP の場合はポート番号が存在しないため，代わりに ICMP ID の値を与える．それぞれの値を正規化し，0 から 1 の間に収まるようにする．表に示した 3 属性と，データ列 12 属性の計 15 属性でベクトルを作成する．

表 1 マップ作成に用いる属性一覧

Attribute	Range of value
Port No. or ICMP ID	0.0～1.0(normalized)
Connection direction	0.0(in) , 1.0(out)
Transport layer	0.0(tcp),0.5(udp),1.0(icmp)
Data (12 bytes, 12 attributes)	0.0～1.0(normalized)

†神奈川工科大学大学院工学研究科 Graduate School of Engineering, Kanagawa Institute of Technology
‡東京電機大学先端工学研究所 Research Center for Advanced Technologies, Tokyo Denki University

3.2 検証実験

実験は，11 種類の不正アクセス定義と，それらに類似した不正アクセス 15 種類，学習させたものと全く違う不正アクセス 10 種類，更に正常アクセス 10 種類を用い，FPR(False Positive Rate)と TPR(True Positive Rate)を算出する．FPR とは不正ではないのにもかかわらず不正と判断してしまう失敗率のことで，TPR とは不正を不正と判断できる成功率のことである．不正アクセス定義は Snort のルールファイルから本研究に適用できる形式のものを選択，正常アクセスは，一般的な HTTP 通信中に出現するデータから抽出した．これらより属性ベクトルを作成して予測するアクセスのベクトルと共に SOM で学習させる．

実験は全部で 3 種類行った．実験 1 では学習済み不正アクセスと類似した不正アクセスがどのように分類されるかの確認，実験 2 では正常アクセスが不正アクセスと分類されないかの確認を行った．実験 3 では，用意した不正アクセスとは全く違う不正アクセスを学習させ，どのように分類されるかを確認した．

実際に学習させたマップを図 1，図 2に示す．丸で囲んだ部分が不正アクセスである．

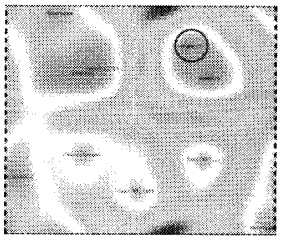

図 1　実験 1 で実際に作成したマップ

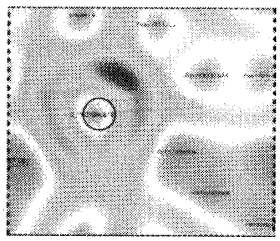

図 2　実験 2 で実際に作成したマップ

4. 分析・考察

実験より得られたマップから，学習済み不正アクセスのノードと投入ベクトルのノード間の距離を，2 次元座標におけるユークリッド距離を用いて求めた．ユークリッド距離に閾値 n を設け，n よりもユークリッド距離が大きければ正常，n 以下ならば不正アクセスと判断する．実験結果より，分類の失敗率である FPR と FNR のグラフを図 3に，最も低くなった閾値を表 2に示す．

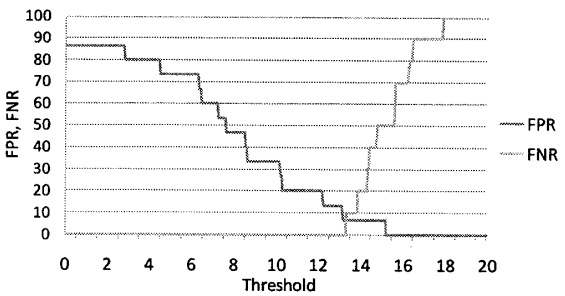

図 3　FPR と FNR の関係

表 2　FPR と FNR の低い閾値

Threshold	FPR[%]	FNR[%]
13.3	0.0	7.7
13.6(intersection)	10	7.7
15.3	50	0.0

分析には ROC(Receiver Operating Characteristics: 受信者動作特性)解析を用いた．ROC 解析は分類器の性能を表す指標である．本研究では，ROC 解析の結果で不正アクセス予測の精度を求めた．実験で得られた TPR と FPR からプロットしたグラフを図 4に示す．左のグラフは定義と類似した不正アクセス，右のグラフは全く新しい不正アクセスの ROC 曲線である．グラフは左上に沿っているほど分類器の性能が高く，原点から右上へ伸びる直線となるほどランダムと同等の性能しか有していないことを表す．

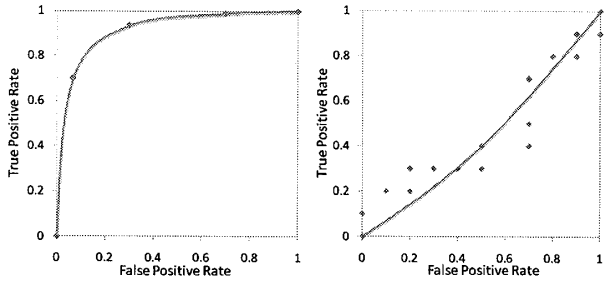

図 4　実験結果の ROC 曲線

図 4より，Snort のルールファイルに記載されている不正アクセス定義に類似しているアクセスは，80%以上の精度が出ている．しかし，学習したものと全く異なる不正アクセスは，ランダムに分類したときと同程度の精度しかないことがわかる．このことから，既知の不正アクセスに類似した不正アクセスについては，精度向上が期待でき，Snort などのソフトウェアに組み込むことによって，既存のものより精度が高くなると考えられる．

5. おわりに

本論文では，SOM を用いた未知の不正アクセスの予測方法について述べた．現存するアクセスの亜種や類似とみなせるアクセスは 80～90%程度で予測が可能であることが確認された．これらは従来の方法では検知できないため，大きな利点となり得る．また，予測に SOM を用いているため，得られたマップをリアルタイムで描画したものを管理者が確認したり，ノード間距離を用いてネットワークの危険度を測定したり，あるいは不正アクセス検知目的以外にも，Snort などにおける不正アクセス定義の作成支援にも応用できると考えられる．

今後は実際に応用ソフトウェアを作成し，ネットワーク上を流れるデータで検証を行っていくことが望ましい．

参考文献

[1]中山亮介，納富一宏，斎藤恵一，“自己組織化マップを用いた不正アクセス検知”，バイオメディカル・ファジィ・システム学会　第 21 回年次大会講演論文集, pp34-35(2008).