機械学習によるネットワークIDSのfalse positive削減手法

小宅宏明[†] 宮地玲奈[†] 川口信隆[†]
重野寛[†] 岡田謙一[†]

近年，セキュリティ侵害の増加にともない，つねにネットワークを通過するパケットを監視できるネットワークIDS（ネットワーク侵入検知システム）への関心が高まっている．しかし，ネットワークIDSは誤検知，特にfalse positive（実際には攻撃でない事象を誤って攻撃と認識すること）が多発することが知られている．False positiveが多発すると，管理者はIDSのログの中から本当のセキュリティ侵害とfalse positiveとを見分けなければならないため，ログの監視作業を行ううえで大きな障害になる．そこで本論文では，機械学習によってfalse positiveのパターンを学習することで，IDSのログに含まれるfalse positiveを検出する手法を提案した．そして提案した手法を実装，評価し，提案の有効性を確認した．

A Technique to Reduce False Positives of Network IDS with Machine Learning

Hiroaki Ohya,[†] Reina Miyaji,[†] Nobutaka Kawaguchi,[†]
Hiroshi Shigeno[†] and Ken-ichi Okada[†]

Recently, network-based IDS (network-based Intrusion Detection Systems), which always observes the packets flowing in the networks, has become the focus of the public attention with increasing security incident. However, network-based IDS frequently mistakes attacks. Especially, IDS generates many false positives, that are bogus alerts caused by mistakes normal events with attacks. Many false positives cause problems for administrators, who have to distinguish real attacks with false positives in IDS log. In this paper, we proposed a technique to detect false positives in IDS log by learning patterns of false positives with machine learning. And we implemented and evaluated the proposal system, and proved effectiveness of our proposal.

1. はじめに

近年，セキュリティ侵害の増加にともない，Firewallの導入が当たり前になってきている．しかしFirewallだけでは以下の理由から，セキュリティ対策として必ずしも十分とはいい難い．

- トランスポート層以下のプロトコルに違反しないパケットを通過させるが，アプリケーションレベルの攻撃には対応できない．
- 攻撃の状態をリアルタイムで監視することができない．
- 外部のネットワークからの攻撃に対する防御には有効であるが，内部からの攻撃には対応できない．

そこで，このようなFirewallの欠点を補完する目的で，侵入検知システム（IDS）が注目を集めている．IDSは常時セキュリティの状態を監視し，不審な振舞いを発見すると管理者に警告（alert）を発する．IDSは監視対象によって次のように分類される．

ネットワークIDS ネットワークを通過するパケットを監視する．

ホストベースIDS ホスト上のプロセスやリソースの状況などを監視する．

また，検知手法によって次のように分類される．

不正検出 攻撃のパターンを記述したデータベース（signature）を用意し，signatureにマッチした状態を異常として検出する．

異常検出 正常な状態をプロファイルとして記録し，正常でない状態を異常として検出する．

実際に利用されているIDSのほとんどが，不正検出の手法を用いたネットワークIDSである．

IDSはセキュリティ状態の監視において非常に有効な手段を提供するものの，誤検知が多いという欠点がある．特に，攻撃でない現象を誤って攻撃と認識する

† 慶應義塾大学大学院理工学研究科
Faculty of Science and Technology, Keio University

false positive は管理者がログ閲覧作業を行う際の大きな障害になっている．

本研究では不正検出を用いたネットワーク IDS を対象とし，IDS の false positive を減らすことによって管理者のログ閲覧作業を支援する手法について議論する．具体的には，false positive において頻繁に現れるパターンを抽出し，そのパターンに合致するものを false positive として検出する手法を提案する．そして，提案した手法を実装したシステムに対して評価を行う．

本論文の構成は次のとおりである．2 章では本論文で問題とする false positive について述べ，3 章では機械学習による false positive の削減手法について提案する．4 章では提案内容を実装したシステムについて説明する．5 章では評価実験について述べ，6 章では評価実験の結果について述べる．7 章では本論文の結論と課題を述べる．

2. False Positive

この章では IDS における false positive の問題について述べる．

IDS は攻撃の可能性があると判断したとき，たとえ実際には攻撃はなくても警報を発することがある．このように実際には攻撃ではない行為を不正として検出する誤検出のことを false positive という．これに対し，実際の攻撃を攻撃として検出しない誤検出のことを false negative という．

IDS の感度を増したり（たとえば，検出すべきパターンを記述した signature の種類をセキュリティの重要度の低いものまで増やす），抽象的な signature を用いることにより，false positive の割合は増加する．false negative の方が false positive よりも実害が大きいため，一般に false negative が発生しにくく，false positive が発生しやすいような設定がなされる傾向にある．

false positive が多発すると，false positive に紛れて本当の攻撃（true positive）を見逃す恐れがある，監視すべきログの情報量が増えて管理者の負担が増す，などの問題が生じる．false positive でなくとも，重要度の低い alert が多発することで同様の問題が生じる．

2.1 False Positive が発生する原因

false positive は以下のような原因によって発生する．

初期設定の問題 IDS の導入に際しては，管理者が利用環境に合わせて IDS の設定をカスタマイズする必要がある．IDS のカスタマイズとは，ネットワーク構成や IDS の監視対象に合わせて使用する signature の種類を限定したり，signature の内容を書き換えたりすることである．IDS のカスタマイズは管理者にとって多くの経験を必要とする．カスタマイズを行わなかったり，不適切なカスタマイズを行うと攻撃の検知に失敗したり，false positive が大量に発生したりするなどの問題が生じる．初期設定状態の IDS では，全 alert のうち false positive が占める割合の許容範囲は 10%程度といわれている[1]．

signature の表現性の問題 IDS で使用される signature では，パフォーマンスを落とさずに（正規表現やワイルドカードなどの）柔軟な表記を用いることは困難である．このため，攻撃のパターンが必ずしも signature において正確に表現されるわけではなく，表記の不備によって false positive が発生することがある．

明確な判定が困難な攻撃 port scan や service scan などの攻撃を検出するためには，トラフィックを統計的に処理し，適切な閾値を設けて攻撃か否かを判断しなければならない．判定の手法は多数提案されているが，こうした攻撃の検出では false positive が発生しやすいことが知られている．

2.2 False Positive への対策

IDS の false positive への対策として，次のような手法が提案されている．

ポリシーチューニング 監視する必要のない signature を検知エンジンから削除することで，ログの分量を減らし，検知エンジンの効率を高める効果がある．しかし，誤って重要なシグニチャを外してしまう人為的なミスが起こりうるうえ，様々な角度から侵入を試みる侵入者の分析には一見無駄とも思える多くのログが必要になってくるため，検知エンジンから外すべき signature を決定するのは困難をともなう．

ログの視覚化 IDS が出力するログは管理者にとって読みやすいものではないので，ログ情報を直感的に把握しやすい形式に変換して表示することで，管理者のログ閲覧作業を支援する方式[2] が提案されている．情報を効果的に視覚化することができれば，短長期的な傾向や個々のログの前後関係を理解する助けになり，結果として false positive の削減につながる．しかし，ログの解析を管理者の経験と直観に依存している点は同じであり，人為的なミスが発生する危険性を排除できない．また，視覚化の際に失われる情報があるため，逆に見落としを招いてしまう恐れがある．

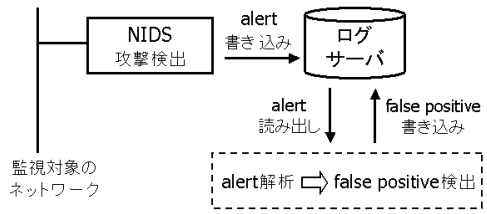

図 1 概要図
Fig. 1 Overview.

3. 機械学習による False Positive 削減手法の提案

本論文では，2 章で述べた問題を解決するために，機械学習によって管理者によるネットワーク IDS の初期設定の支援および false positive と重要度の低い alert の抑制を行う手法を提案する．

2 章で述べた問題のうち，初期設定の問題と signature の表現性の問題に関しては，パケットの評価が不十分なことが false positive 発生の原因となっている．IDS が発する alert の中からすべての false positive を特定することは不可能であるが，パケットの評価が不十分なために，同一の原因による似たような false positive が多発する場合には，false positive を特定することが可能である．

ただし，2 章の明確な判定が困難な攻撃については，個々のパケットの比較によって false positive であるかどうかを判断することが不可能なため，検出の対象から除外する．

本提案では，false positive の原因となったパケットを収集し，特徴を抽出する．次に収集した false positive パケットの特徴を元に，IDS が発する alert の中から類似したものを選び出し，管理者に対して false positive の疑いを指摘する．

IDS の処理を遅延させないために，システムの構成は IDS の出力したログを入力として使用し，IDS の処理と false positive の検出は独立して動作するようになっている．false positive を検出した場合には，その旨を IDS のログに追記する．**図 1** に概要図を記す．

提案する手法は構築フェーズと運用フェーズから構成される．

- 構築フェーズ
  （1） false positive のサンプルを収集する．
  （2） 収集した false positive を signature ごとに分類する．
  （3） false positive をクラスタ分析する．
  （4） クラスタごとにパターンを抽出する．
  （5） 抽出したパターンをニューラルネットワークに学習させる．
- 運用フェーズ
  （1） 発生した alert を signature ごとに分類する．
  （2） 学習したニューラルネットワークを用いてパターンを識別する．
  （3） false positive を検出する．

各フェーズの詳細については後述する．

3.1 構築フェーズ

構築フェーズでは，false positive を検出するための準備を行う．続く運用フェーズで false positive の検出を行う際に必要となる情報を収集・整理し，運用フェーズでの処理を削減するのがこのフェーズの目的である．

3.1.1 False Positive の収集

まず，false positive のサンプルを収集する．

3.1.1.1 必要な情報

alert は以下の情報を含んでいる必要がある．

- パケットの送信元 IP アドレス
- パケットの送信先 IP アドレス
- パケットの送信元ポート番号
- パケットの送信先ポート番号
- パケットのペイロード
- IDS が判定した signature

これらの情報は，大抵の IDS ならばログとして出力することができる．

3.1.1.2 情報の収集方法

サンプルとなる false positive の収集には，以下の 2 通りの方法が考えられる．

- 攻撃がない状態で IDS を運用し，false positive のデータを収集する．
  この方法では攻撃のない状態を用意する必要があるが，サンプルの収集を一度に行うことができる．発生した alert はすべて false positive か重要度の低い alert と判断できる．
- 攻撃が起こりうる状態で IDS を運用し，alert の中から false positive と思われるものを管理者が抽出する．
  この方法では，IDS を実際に運用しながら管理者が alert の内容を見て false positive と判断したものをサンプルとして用いる．サンプル収集のために特殊な環境を用意する必要がないのが利点である．

3.1.2 Signature による分類

次に，false positive を引き起こしたパケットを sina-

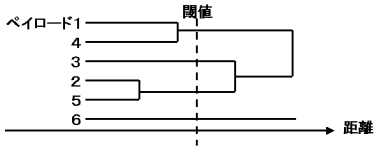

図 2 樹状図
Fig. 2 Dendrogram.

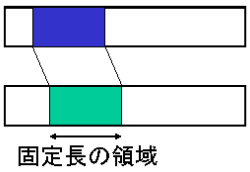

図 3 パターンの抽出
Fig. 3 Pattern extraction.

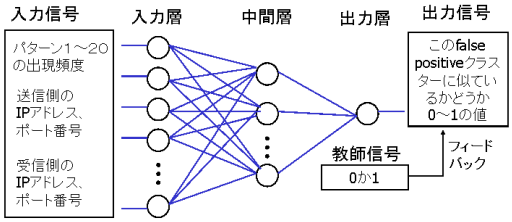

図 4 ニューラルネットによる学習
Fig. 4 Neural network learning.

ture ごとに分類する．signature は IDS が判断した攻撃の種類であり，同一の signature によって誤検出された false positive には signature という共通部分がある．これを用いることにより，大まかに類似した false positive の集合を形成し，次のプロセスであるクラスタ分析の計算量を削減することができる．

3.1.3 クラスタ分析

signature ごとに分類したパケット集合を，さらにいくつかの類似した集合（クラスタ）に分類する．クラスタ分析を行う理由は，類似した原因によって発生したと思われる false positive のみを選び出すためである．2 つの alert に同じ signature が付けられているからといって，それらが同じ原因によって発生したものであるとはいい難い．この操作は，後のフェーズで学習を行う際にノイズとなる入力を除去することを目的とする．

クラスタ数は未定であるため，階層的クラスタ分析という手法を用いる．まず，signature ごとにグループ化された alert に対して，似通ったものどうしをさらにグループ化して**図 2** のような樹状図を作成する．次に，類似度に関して適当な閾値を決定し，その閾値未満の距離にある要素をクラスタとしてまとめる．

距離（非類似度）の計算方法として，ペイロードの最小編集距離[3] を用いる．最小編集距離とは 2 つの文字列の間で，一方の文字列に編集を加えて他方の文字列に一致させるために必要な編集操作の最小回数を表す．

階層的クラスタ分析にはグルーピングの基準などが異なるいくつかの手法があるが[5]，ここでは最長距離法を使用する．これは学習の際にノイズとなる情報を除去することを目的としてクラスタ分析を行っているので，なるべく距離の大きい alert どうしが同一のクラスタに属さないようにするためである．

3.1.4 クラスタごとのパターン抽出

これまでの処理により，false positive が signature ごとに分類され，さらに signature の中でいくつかの集合（クラスタ）に分類された．こうして分類された false positive のクラスタに対し，ここでは次の方法でクラスタ内で共通して出現するパターンを探し出す．

(1) クラスタの中から 2 つの alert を選ぶ．
(2) 2 つの alert の間で共通するパターンを探し，出現頻度を数える．
(3) (1)，(2) の処理をクラスタ内のすべての alert の組合せに対して行う．
(4) クラスタ全体で出現頻度の高いパターンを選び出す．

パターンを探すには，alert に含まれる情報のうち，パケットのペイロード部分を用いる．2 つのペイロードから共通するパターンを見つけるには**図 3** のように一定の長さの領域を移動させながら比較していくという方法をとる．

3.1.5 ニューラルネットワークによる学習

次に，ニューラルネットワークをクラスタの数だけ用意し，クラスタごとに教師あり学習を行う．ニューラルネットワークは脳の情報処理機構をヒントとしたモデルで，神経細胞（ニューロン）を模した素子をネットワーク状に多数接続した構造を持ち，以下の特徴を持っている．

- 分散並列処理方式をとること
- 情報をパターンとして表現すること
- 学習や自己組織化能力を持つこと

ニューラルネットワークを利用した侵入検知については，これまで様々な手法が提案されてきた[4]．本研究ではニューラルネットワークをパケットの類似度判定に利用する（**図 4**）．

ニューラルネットワークのアルゴリズムには，時間応答が速いバックプロパゲーションを用いる．入出力

信号および教師信号は次のようにする．

3.1.5.1 入力信号

クラスタに属するパケット全部と，その他のパケットを適当に選んで入力とする．パケットのバイト列をそのまま入力してしまうと学習が収束しないので，パケットごとに次の 24 個の値を求めて使用する．

- クラスタ内で頻出する 20 個のパターンそれぞれの出現回数
- パケット送信元の IP アドレスとポート番号
- パケット送信先の IP アドレスとポート番号

3.1.5.2 出力信号

クラスタのパケット群と類似したパケットであれば 1，そうでなければ 0 を出力する．

3.1.5.3 教師信号

どのパケットがクラスタに含まれるかはあらかじめ分かっているので，クラスタに含まれるパケットのときは 1，それ以外は 0 をフィードバックする．

3.2 運用フェーズ

運用フェーズでは IDS のログから，実際に false positive の検出を行う．運用フェーズは 2 つのプロセスで構成される．まず学習を行ったのニューラルネットワークを用いて，構築フェーズで作成した false positive のクラスタの中から，false positive の疑いのある alert と最も類似したクラスタを見つける．次に alert と発見されたクラスタの間での類似度を調べ，alert がクラスタと非常に類似している場合には alert はそのクラスタと同じタイプの false positive であると判断する．

3.2.1 パターンの識別

学習の内容を元に運用フェーズで false positive を検出するにあたり，まず学習のときと同様に，false positive を signature ごとに分類する．次に，学習済みのニューラルネットワークに IDS の alert を入力して逆解析を行う．入力信号，および出力信号は学習の際に用いた項目と同じである．ニューラルネットワークはクラスタに対して 1 つずつ用意されているので，それぞれに対して出力を求め，出力結果を比較する．出力結果が最も 1 に近い値を出したクラスタが alert に最も近いクラスタである（**図 5**）．

3.2.2 False Positive の検出

次に，alert が今選択したクラスタに実際に似ているかどうかを調べる．クラスタから任意に 3 つの alert を選択し，選択した個々の alert のペイロードと alert の原因となったペイロードとの間で最小編集距離を計算する．すべての最小編集距離がクラスタを決定した際の閾値以下になった場合には，この alert はクラスタに属するものと判断し，したがって false positive であると判断する．

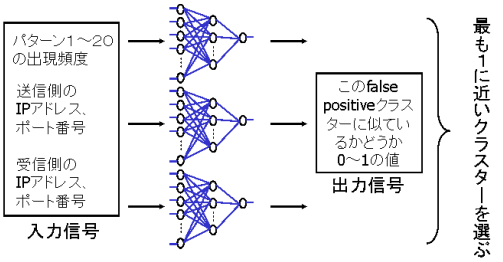

図 5 パターンの識別
Fig. 5 Pattern recognition.

4. 実　　装

提案した手法を実装し，プロトタイプを作成した．プロトタイプの作成には，実装言語として C++を利用し，動作プラットフォームとして Linux を使用した．実装にあたって以下のソフトウェアを利用した．

IDS IDS にはオープンソースの IDS である Snort[6] を利用した．Snort は signature を用いて不正検出を行うネットワーク IDS である．Snort はログを DBMS に出力することができる．本研究ではログを DBMS の 1 つである PostgreSQL に出力した．

ニューラルネットワークエンジン ニューラルネットワークのアルゴリズム部分には Annie[7] を用いた．Annie はニューラルネットワークのアルゴリズムを提供する C++ クラスライブラリで，バックプロパゲーションを含む複数のアルゴリズムが利用可能である．本研究ではバックプロパゲーションを利用した．

5. 評　　価

実装したプロトタイプを用いて，提案手法の評価を行った．

5.1 評価用データ

評価用のデータとして，MIT の LINCOLN 研究所が作成した IDS 評価用のデータ[8] を使用した．これは同研究所が DARPA（高等研究計画局）の支援によって 1998 年から作成しているもので，IDS の性能を評価するための統一的なデータとして広く利用されている．データには以下のような内容が含まれている．

LAN の外部のトラフィック パケットを tcpdump の出力形式で記録したもの．

LAN の内部のトラフィック tcpdump の出力形式

で記録されている．

各種ログや設定ファイル /var/log や/etc 以下のファイル一覧．

行った攻撃 行ったすべての攻撃に関する情報．

攻撃を識別するための情報 どの攻撃がログなどのどの部分に該当するのかを既述したファイル．

ネットワーク構成図 実験を行ったネットワーク内のルータやホストの配置図．

5.2 評価用データの利用方法

本研究で利用したのは 1999 年に作られたもので，3 週間分のデータから構成される．1 週目と 3 週目は攻撃がなかったことが明記されている．2 週目には攻撃が含まれており，トラフィックやログ中におけるどの部分が攻撃であったかが書かれている．

評価実験では，LAN の外側のトラフィックデータをを次のように使用する．

1 週目 false positive パターンの学習

2 週目 false negative 発生率の評価

3 週目 false positive 発生率の評価

2 章の明確な判定が困難な攻撃については，個々のパケットの比較によって false positive であるかどうかを判断することが不可能なため，評価用データから除くことにする．

5.2.1 False Positive パターンの学習

1 週目のトラフィックデータはニューラルネットワークの学習に利用する．トラフィックデータを IDS に読み込ませると alert が発生する．このデータには攻撃は含まれていないので，このデータを読み込んで発生した alert は，すべて false positive もしくは重要度の低い alert と考えることができる．この操作によって発生した alert を実装したプロトタイプへの入力として学習を行う．

5.2.2 False Negative 発生率の評価

2 週目のトラフィックデータには攻撃が含まれているので，false negative 発生率の評価に利用する．IDS に検出された攻撃と，実際にトラフィックに含まれていた攻撃とを比較することで，IDS がどの程度攻撃の検出に失敗したか（false negative を発生させたか）を評価できる．

次の 2 通りを実行し，発生した false negative の数を比較する．

- Snort にトラフィックデータを読み込ませた場合
- Snort にトラフィックデータを読み込ませてから提案システムが誤って false positive と判断した攻撃を取り除いた場合

表 1 false negative および false positive 発生数の比較
Table 1 A comparison of incidence between false negative and false positive.

	false negative の発生数	false positive の発生数
オリジナルの IDS	73	24,122
実装したプロトタイプ	73	15,792

表 2 第 1 週のトラフィックデータにより発生した false positive
Table 2 False positives caused by traffie data in the first week.

攻撃の種類	回数
WEB-CGI redirect access	5,257
POLICY FTP anonymous login attempt	4,710
ATTACK RESPONSES Invalid URL	2,856
SNMP public access udp	2,682
WEB-MISC count.cgi access	2,016
ATTACK RESPONSES 410 Forbidden	1,996
WEB-MISC open access	1,682
TELNET access	1,403
ICMP Destination Unreachable	982
WEB-IIS fpcount access	767
その他	4,273

5.2.3 False Positive 検出率の評価

3 週目のトラフィックデータには攻撃が含まれていないので false positive 発生率の評価に利用する．次の 2 通りを実行し，発生した false positive の数を比較する．トラフィックデータに攻撃は含まれていないので，発生した alert はすべて false positive である．

- Snort にトラフィックデータを読み込ませた場合
- Snort にトラフィックデータを読み込ませてから，プロトタイプによって検出された false positive を取り除いた場合

6. 評価結果

評価結果の概要を，**表 1** に示す．2 つの列はそれぞれ 5.2.2 項と 5.2.3 項における評価実験の結果を表しており，IDS をそのまま用いた場合と，IDS の出力を実装したプロトタイプに入力した場合とを比較している．個々の結果については後で詳説する．

6.1 学習結果

第 1 週のトラフィックデータを用いて実装したシステムの学習を行ったところ，21,657 個，36 種類の alert が発生した．false positive の具体的な内訳を**表 2** に記す．次に，発生した false positive をシステムの入力として，学習を行った．

6.2 False Negative の発生率の評価結果

本論文で提案する手法には，実際に行われた攻撃を誤って false positive と判断してしまう危険性，すな

表 3 検出した false positive
Table 3 Detected false positives.

攻撃の種類	回数
WEB-CGI redirect access	3,242
POLICY FTP anonymous login attempt	2,680
ATTACK RESPONSES Invalid URL	1,211
SNMP public access udp	1,104
WEB-MISC count.cgi access	37
WEB-MISC open access	23
TELNET access	18
WEB-IIS fpcount access	15

わち false negative を発生させる危険性が存在する．この実験では第 2 週のトラフィックデータを用いて，IDS とプロトタイプの検出結果を比較することで false negative の発生率を測定した．

トラフィックデータには，4,592 個，168 種類の攻撃が含まれていることが記録から分かっている．このうち，5.2 節で述べた明確な判定が困難な攻撃を除外すると，3,557 個，132 種類の攻撃が評価の対象となった．

Snort[6] を用いて侵入検知を行ったところ，3,557 個の攻撃のうち，3,484 個の攻撃を正しく検出し，73 個の false negative が発生した．

Snort が正しく検出した 3,484 個の alert をプロトタイプに入力したところ，誤って false positive と判断したものは 1 つもなかった．すなわち，この実験ではプロトタイプは false negative をまったく発生させなかった．

6.3 False Positive の検出率の評価結果

第 3 週のトラフィックデータを用いて，本提案の目的である，“false positive の検出” がどの程度達成できたかを測定した．

IDS にトラフィックデータを読み込ませたところ，24,122 個，29 種類の false positive が発生した．IDS の出力を本システムに入力したところ，8,330 個（35%），8 種類の false positive を検出した．

検出した false positive の詳細を**表 3** に記す．

6.4 評価結果の考察

評価実験の結果から，false negative の数を増加させることなく，一部の false positive を検出することができた．

false positive の検出精度は false positive 全体の 35%程度であり，学習を行った 29 種類の false positive に限定すれば 52%の検出精度であった．管理者がログを閲覧する作業を考えれば，見る必要のない情報が 1/3 程度減少したということであり，ログ監視作業を支援するという，本提案の目的は達せられていると考えられる．

検出した false positive の内訳について考えると，表 3 より，学習に用いた第 1 週のデータに多く含まれていた false positive は第 3 週のデータを用いた実験でも多く検出されていることが分かる．これは，同一のネットワークで発生する false positive にある程度一貫した傾向があることを示唆している．したがって，この傾向を学習することで false positive を検出しようという本提案の発想は誤りでないといえる．

IDS の評価基準としては，一般に false negative を発生させないことが最も重要であり，次いでパフォーマンス，false positive の発生頻度の順に重要である．このため，false positive への対策は後回しになりがちなのが現状である．今回実装したプロトタイプは，false negative の検出には影響を与えず，false positive だけを検出することができた．このようなシステムに対する必要性は，今後ますます高まってゆくと思われる．

7. 結　　論

近年，セキュリティ侵害の増加にともない，常時ネットワークのセキュリティ侵害を監視できる IDS（侵入検知システム）への関心が高まっている．しかし，IDS は誤検知が多発することが知られており，特に false positive （実際には攻撃でない事象を攻撃と誤認識すること）が多い．管理者は false positive を含んだ IDS の警告（alert）の中から本当のセキュリティ侵害（true positive）を見分けなければならないため，false positive の発生は管理者がログ閲覧作業を行う際の障害になっている．

そこで，本研究では，現在最も一般的に利用されている signature マッチングを用いたネットワーク型 IDS において，alert の中から false positive と思われるものを検出し，false positive の発生を管理者に通知することで管理者のログ監視作業を支援するシステムを提案した．

提案した手法を用いてプロトタイプを作成した．提案の有効性を確認するために，実装したプロトタイプと手を加えない状態の IDS に対して DARPA が作成した IDS 評価用データを適用し，false positive と false negative の発生数を比較した．

その結果，オリジナルの IDS と比べて，false negative の発生数は変らず，false positive の発生数をおよそ 35%削減することができたことから，提案の有効性が確認された．

今後，本論文で提案した手法を用いることにより，IDS の検知精度を向上させることができ，管理者がロ

グ閲覧作業を行う際の負担を軽減させることができるようになると思われる．

謝辞 この研究は，応用セキュリティフォーラムの支援を受けて行われた．

参 考 文 献

1) Timm, K.: Strategies to Reduce False Positives and False Negatives (Sept. 2001). http://online.securityfocus.com/infocus/1463
2) 大野一広，高田哲司，小池英樹：SnortView：NIDS の誤検知判別を目的とした視覚化システム，情報処理学会論文誌，Vo.44, No.11 (2003).
3) Maner, S.W., Myers, G. and Miller, W.: An O(NP) Sequence Comparison Algorith, *Algorithmixa*, pp.251–266 (Aug. 1989).
4) Planquart, J.-P.: Application of Neural Networks to Intrusion Detection (July 2001). http://rr.sans.org/intrusion/neural.php
5) 青木繁伸：クラスター分析 (Jan. 2003). http://aoki2.si.gunma-u.ac.jp/lecture/misc/clustan.html
6) Snort (Jan. 2003). http://www.snort.org/
7) Shankar, A.: Annie (Jan. 2003). http://annie.sourceforge.net/
8) Lincorn Lab, MIT (Jan. 2003). http://www.ll.mit.edu/IST/ideval/

(平成 15 年 6 月 10 日受付)
(平成 16 年 6 月 8 日採録)

小宅 宏明（正会員）
2001 年慶應義塾大学理工学部情報工学科卒業．2003 年同大学大学院理工学研究科開放環境科学専攻情報通信メディア工学専修修士課程修了．セキュリティの研究に従事．

宮地 玲奈（学生会員）
2002 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科開放環境科学専攻情報通信メディア工学専修修士課程に在学中．セキュリティの研究に従事．

川口 信隆（学生会員）
2003 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科開放環境科学専攻情報通信メディア工学専修修士課程に在学中．セキュリティの研究に従事．

重野 寛（正会員）
慶應義塾大学理工学部情報工学科助教授，工学博士．無線 LAN の構成法と媒体アクセス制御方式，計算機ネットワークにおけるステーション移動サポート，モバイル・コンピューティング，アクティブネットワーク，遠隔教育システム等の研究に従事．

岡田 謙一（フェロー）
慶應義塾大学理工学部情報工学科教授，工学博士．専門は，グループウェア，コンピュータ・ヒューマン・インタラクション．『コラボレーションとコミュニケーション』（共立出版）をはじめ著書多数．GN 研究会運営委員，MBL 研究会運営委員，日本 VR 学会仮想都市研究会幹事．情報処理学会論文誌編集主査，電子情報通信学会論文誌編集委員．ECSCW2001 プログラム委員，INTERACT2001 財務委員長．IEEE，ACM，電子情報通信学会，人工知能学会各会員．