SnortView: NIDSの誤検知判別を目的とした視覚化システム

大野一広[†] 高田哲司[††] 小池英樹[†]

現在ネットワークを経由した不正アクセスが増加している．ネットワーク型不正侵入検知システム（Network-based Intrusion Detection System: NIDS）は，不正アクセスの検知に有効なシステムであるが，現状では効果的にシステムの運用を行うことは容易でない．これは，NIDSがもたらす誤検知（False Positive）の取扱いが困難であることが原因である．そこで本研究では，誤検知の判別を支援するため，NIDSログ視覚化システム“SnortView”を構築した．本システムでは情報視覚化の技術を使用することでNIDSの誤検知を視覚的に判別することが可能である．これによりNIDSの調整作業の負担を削減することが可能になる．本システムを用いることによって，従来運用が困難であったNIDSをより効果的に活用することが可能になるだけでなく，不正アクセスを実時間で監視することが可能になる．

SnortView: Visualization System for Distinction of False Alarms from NIDS Alerts

Kazuhiro Ono,[†] Tetsuji Takada[††] and Hideki Koike[†]

Computer attacks via network are increasing now. Network-based Intrusion Detection System (NIDS) is a capable system to detect such attacks, but it is not easy to handle the system. The reason is that it is difficult to manage “False Alarms” in NIDS alert log. In this research, we have developed a visualization system of NIDS alert information, which is called “SnortView”, in order to support such task. SnortView represents NIDS alerts visually. That makes it is not only to distinguish false alarms but also to reduce NIDS configuration . As a result, SnortView makes it both to operate NIDS effectively and to find intrusion activities in real time.

1. はじめに

近年，ネットワークに接続された計算機に対する不正アクセスが増加している．その対策として，ネットワーク型不正侵入検知システム（Network-based Intrusion Detection System: NIDS）が注目されている．NIDSはネットワークトラフィックの監視を行い，不正アクセスに関連する事象を検知した場合，管理者へ警告を行う．NIDSを使用することで，不正アクセスによる被害の早期発見が可能になる．

しかしNIDSの運用には，誤検知の発生にともなうシステムの調整作業が必須である．調整作業は自動化が困難であるため，手作業で繰り返し行う必要がある．またNIDSからの警告を閲覧するためには，不正アクセスに関する専門的な知識が要求される．さらに警告は膨大な量であるため，内容の把握には時間がかかる．NIDSはこの運用時の繁雑さから，NIDSを使用した効果的な不正アクセスの検知を行うことができるのは，一部の上級者に限られている．

筆者らは，実時間による不正アクセス事象の監視およびNIDSがもたらす誤検知の判別を支援するため，情報視覚化の手法を用いることを提案する．本論文では，その提案に基づいた視覚化システムについて述べる．本システムでは，NIDSの警告から不正アクセスの監視に必要な情報を，情報視覚化の技術を用いて図化して利用者へ提示する．さらにNIDSの誤検知を判断する際の基準や誤検知の判断に必要な情報についての視覚化を行う．

以下，2章ではNIDSとその誤検知について述べ，3章で本論文で提案するNIDSログ視覚化システム“SnortView”についてその詳細を述べる．4章でSnortViewを用いた調査事例について述べた後，5章

† 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, University of Electro-Communications
†† 電気通信大学サテライトベンチャビジネスラボラトリ
Satellite Venture Business Laboratory, Universty of Electro-Communications

で考察を行う．

2. NIDS とその誤検知

2.1 NIDS の問題点：誤検知

ネットワーク型不正侵入検知システム（Network-based Intrusion Detection System: NIDS）はネットワークからの不正アクセスを，実時間で検知することが可能なシステムである．NIDS は既知の不正アクセスの特徴（ルール）を定義したデータベース（ルールセット）を保持し，このルールとネットワークのトラフィックを比較し，一致すれば不正アクセスとして警告を行う．しかし NIDS では誤検知の大量発生が問題となっている．誤検知とは NIDS の不正アクセスを誤って判定する動作のことを指し，以下の 2 種類が存在する．

False Positive 正常なアクセスを不正と警告する
False Negative 不正なアクセスを警告しない

NIDS では，False Positive の発生が問題となっている．NIDS の管理者は，False Positive を抑制するために，システムの調整作業を行う必要がある．具体的には，NIDS のルールセットから False Positive の原因となるルールを調査し削除する作業を，False Positive が発生しなくなるまで繰り返す．この作業を過剰に行った場合，必要なルールまで削除してしまい，実際の不正アクセスを検知することができない．その結果 False Negative の増加につながる．誤検知は，NIDS を設置している個々の計算機環境によって発生状況が異なる．そのため調整作業は不正アクセスに関する経験を備えた管理者による手作業で行われ，自動化は困難である．さらに新しい不正アクセスへ対応するため，ルールセットを追加する必要があり，そのたびに新たな誤検知が発生していないか確認する作業がともなうため，調整作業は NIDS の運用と切り離すことができない．

また False Positive は短時間のうちに大量に発生する．それにより警告閲覧時の負荷が増大し，監視作業の効率を大幅に低下させている．現在 NIDS を用いた不正アクセスの監視では，大量の誤検知に含まれた不正アクセス事象を見分ける作業を行っている．そのため現状では，実時間による不正アクセス事象の発見は困難である．

2.2 誤検知の判断基準

はじめに，NIDS の調整作業についての調査を行った．本調査では 2002 年 4 月より同年 12 月まで，2 種類の調査環境で NIDS の実運用を行い，NIDS の警告情報の取得を行った．1 つ目の調査環境は筆者が所属する研究室のネットワークである．調査人員は 6 名である．2 つ目は企業内ネットワークである．ここでの調査人員は 5 名である．これにより，誤検知を判断する際に警告ログの中で着目している項目，また誤検知を判断する際に参考となる情報が得られた．次に筆者らは得られた情報の分析を行い，その結果，警告ログ中における誤検知の出現分布には数種類の特徴が存在することが明らかになった．また警告の詳細情報を調査することや，他の情報と比較することで，誤検知の判別が可能な場合があることが分かった．誤検知を判断するために有効な警告の例および情報は，以下の 6 点であると考えられる．

(1) 連続して多量に出現する警告
(2) 監視中頻繁に出現する警告
(3) サービス内容と実際の通信に矛盾のある警告
(4) 他のネットワークに関する警告
(5) NIDS が記録したパケットペイロード情報
(6) 計算機のシステムログ情報

(1) と (2) は警告ログ中における出現分布から明らかになった特徴的な誤検知の警告である．(3) と (4) は警告の詳細を確認することで誤検知の判断が可能になる種類の警告である．また (5) と (6) は警告と比較した場合に誤検知の判断に有効な情報である．

2.3 不正侵入検知に必要な情報

不正侵入検知では，以下の情報を把握する必要がある．

2.3.1 発 生 時 刻

はじめに，いつ不正アクセスの兆候が現れたか，その発生時刻を把握する．これは不正アクセスの被害状況を判断するためである．不正アクセスに対しては，可能な限り早い段階で対処することが望ましい．それにより不正アクセスの被害を最小限にとどめることが可能なだけでなく，計算機のログファイル中に，後の調査時に有効な不正アクセスの痕跡が残されている可能性が高い．逆に不正アクセスから長い時間が経過していた場合，侵入者によるログファイルの消去や改ざんなどにより，計算機の内部情報には有用な情報が残されていない場合が多い．そのため，不正アクセスの行われた時間を確認することで，被害の状況を判断するための情報を得ることができる．

2.3.2 アクセス元計算機

2 番目に，アクセス元の計算機を特定する．これは一般に計算機の IP アドレスや，DNS を用いた計算機名である．これらから得られるネットワーク情報から所属組織を判別し，不正なアクセスを行ったかを判断することができる．例として Web，FTP などの代理

（proxy）サーバがあげられる．これらのサーバでは，踏み台行為を防止するため，外部ネットワークからの接続要求は許可しない．そのため組織外からの接続がある場合，不正アクセスの兆候として注意する必要がある．

2.3.3 アクセス先計算機

3 番目に，アクセス先の計算機に関する情報を得る．これにより，調査を行う際の優先順位を決定する．たとえば組織にとって重要な Web サーバや Mail サーバへのアクセスについては，即座に調査を開始する必要がある．それに対して，一般のクライアント用計算機へのアクセスについては調査の優先順位を低くするなどの対応をとることができる．

2.3.4 アクセスの内容

最後にアクセスの内容を把握する．これはアクセスの種別により調査を行う際の対処方法や確認する情報が異なるためである．またサービスの種別を把握することで，提供を行っていないサービスに対するアクセスについては，調査を省略することが可能になる．

2.4 視覚化システムにおけるデザイン手法

以上の考察により，本研究では情報視覚化の技術を適用した視覚化システムの提案を行う．2.3 節で示した不正侵入検知に必要な情報は，個別に使用するだけでなくそれぞれを総合的に判断することで，より正確な不正アクセス事象の判断が可能になる．具体的には，以下の 5 点が視覚的に一覧が可能であるよう実装を行う必要がある．

- 時間情報
- アクセス元計算機
- アクセス先計算機
- アクセス内容
- 誤検知の判断基準

3. NIDS ログ視覚化システム SnortView

本研究では，NIDS の問題点である誤検知の判別および不正アクセス事象の早期発見を目的として，NIDS ログ視覚化システム “SnortView” を構築した．

3.1 システム構成

図 1 に，SnortView システムの構成図を示す．本システムは，警告情報取得処理，視覚化処理の 2 つの処理で構成される．はじめに警告情報取得処理で NIDS からの警告情報および Syslog サーバからの情報の取得，解析を行う．次に視覚化処理で結果の視覚化を行う．

図 2 に警告情報取得処理の詳細を示す．警告情報取得処理では，NIDS の警告情報および Syslog メッセージの取得を行う（図 2 (1) 事象の取得）．本システムでは代表的な NIDS である Snort [7),8)] を使用し，警告情報の取得を行っている．警告情報は，実時間で監視を行うため，短い間隔（2 秒ごと）で定期的に取得する．また監視用計算機では，Syslog サーバを稼働させており，監視対象の計算機から Syslog メッセージを受信して，ログファイルへ記録する．本システムでは，このログファイルを常時監視し，計算機からの警告メッセージを取得する．

次に警告事象の統合処理を行う（図 2 (2)）．ここでは複数の経路から収集した情報を，1 つの情報へ統合する処理を行う．本システムでは NIDS の警告事象と Syslog メッセージを事象が発生した時間順に並べ換え，1 つの情報にまとめる．Syslog メッセージは各種のサーバプログラムがシステム情報の記録を行う方法として広く用いられている．ここにはサーバプログラムの異常終了など，不正アクセスの証拠となる情報が含まれている．ある時刻に発生した NIDS の警告事象が誤検知であるかどうかを確認するためには，同じ時間帯に記録された Syslog メッセージを調査するこ

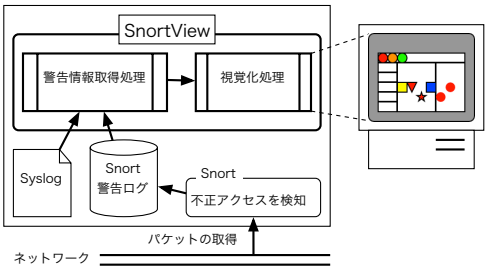

図 1 SnortView のシステム構成
Fig. 1 System overview of SnortView.

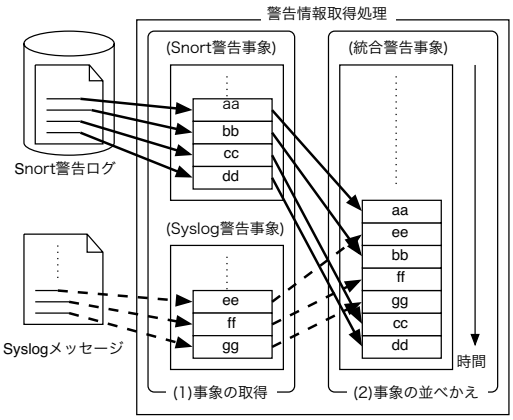

図 2 警告情報取得処理
Fig. 2 Gathering alert information process.

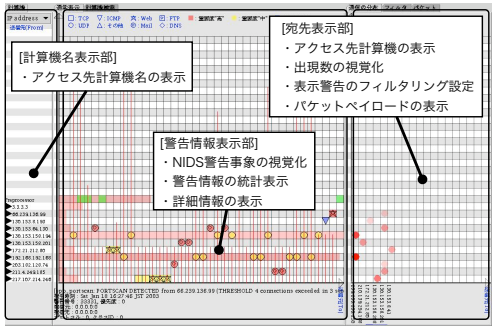

図 3 SnortView の画面
Fig. 3 A display image of SnortView.

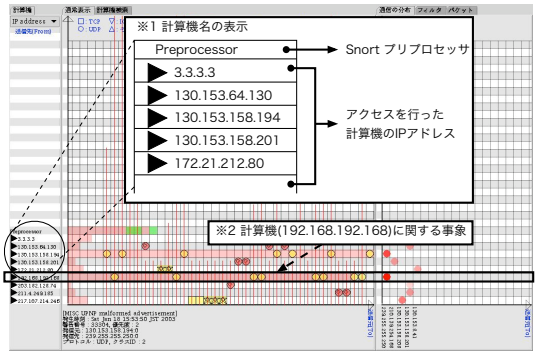

図 4 計算機名表示部
Fig. 4 Visualization of computer names.

とで明らかになる場合がある．通常 NIDS の警告事象と Syslog メッセージは異なる場所に保存されているため，内容の比較作業は繁雑である．これらの情報をまとめることで，NIDS の警告情報の誤検知を判別する際の作業を簡略化することが可能になる．

視覚化処理では，警告情報取得処理で得られた情報をもとに，それらを図化してユーザに提示する．また視覚化された結果に対する対話的な処理が可能であり，さらに詳細な情報の取得が可能である．

3.2 視覚化手法

図 3 に SnortView の実行画面を示す．本システムでは，NIDS の警告情報および Syslog メッセージを，以下の 3 つのコンポーネントを用いて視覚化を行っている．

計算機名表示部 アクセス元計算機の表示
警告表示部 NIDS 警告情報の表示
宛先表示部 アクセス先計算機の表示

図 4 に計算機名表示部の拡大画面を示す．計算機名表示部では，監視対象のネットワークへアクセスを行ってきた計算機の IP アドレスをソートし，縦方向に並べて表示する．本システムでは，NIDS からの警

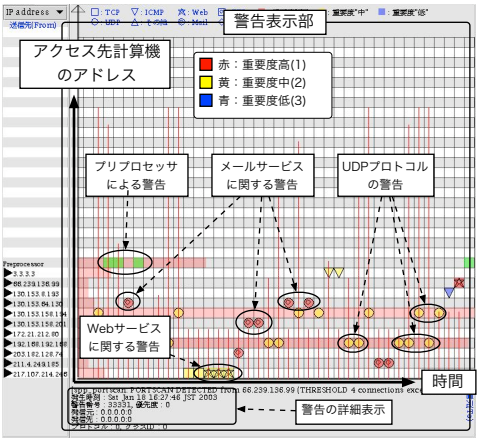

図 5 警告表示部
Fig. 5 Visualization of NIDS alerts.

告情報を計算機別に分類して表示を行っている．この表示方法は，2.1 節で示した誤検知の判断基準（他のネットワークに関する警告）と 2.3 節で示した不正アクセスの監視に必要な情報（アクセス元計算機）を提示するためのものである．

図 5 に警告表示部の拡大画面を示す．警告情報表示部では，NIDS の警告，警告の統計情報および警告の詳細を視覚化する．本システムでは最新の警告情報を随時表示することで，実時間による不正アクセス事象の監視が把握可能である．縦方向は計算機名表示部と同様に計算機の IP アドレスである．計算機別による表示方法では，アクセス元とアクセス先の判別が容易なことが利点である．さらに IP アドレスからネットワーク情報も把握可能であり，アクセスを行ってきた計算機の組織情報の判別も容易である．横方向は時間である．時間軸による表示は，時間情報を容易に把握するために有効である．またこの表示方法では情報の追加が行いやすく，実時間による監視状況を提示する際にも適用可能であると考えられる．また NIDS の警告事象は，色分けしたシンボルで表示を行う．シンボルの色は NIDS があらかじめ定義している重要度に対応している．本システムで使用している Snort では，個々の警告ごとに 3 段階の重要度を定めており，重要度が高い順番に 1 から 3 までの数値を割り当てている．本システムではそれぞれの重要度に対して 1 を赤色，2 を黄色，3 を青色に割り当てた．シンボルの形状については，サービスの種別および通信を行っているプロトコルの種別で判別を行うことが可能になっている．サービスの種別は，通信先，通信元の計算機が使用しているポート番号により判断する．サービス名およびそれに対応するシンボルの形状，サービスの判

表 1 シンボルの形状と意味
Table 1 Shape and meaning of symbols.

サービスの種別（※ 1）		
サービス名	形状	ポート番号
Web	★	80, 3128, 8080
Mail	◎	25, 110, 143
FTP	⊡	20, 21
DNS	◇	53
システムのメッセージ		
システム名	形状	ポート番号
プリプロセッサ	緑色の □	53
Syslog	☒	なし
プロトコルの種別		
プロトコル名	形状	ポート番号
TCP	□	※ 1 での定義以外
UDP	○	なし
ICMP	▽	なし
その他	△	なし

別に使用しているポート番号についての詳細を，**表 1** に示す．これらの実装は不正アクセスの監視に必要な情報（発生時刻，アクセスの内容）および誤検知の判断基準となる警告（他のネットワークに関する警告）の提示を目的としている．シンボル表示は，アクセス内容の判断を容易にする．これにより，NIDS の警告情報を閲覧して内容を理解する負担と時間を削減することが可能になり，実時間による不正アクセスの監視に役立つと考えられる．

NIDS の警告ログでは，同じ内容の警告が連続して発生する場合が多いため，本システムでは，それらを 1 つの警告事象として取り扱う．警告の連続量は，警告のシンボルと重ね合わせて縦方向のラインを描画する（**図 6** ※ 1）．また現在警告表示部に出現している計算機が，過去にどれだけ出現していたかを，画面の横方向のラインで重ね合わせて表示を行う（図 6 ※ 2）．このラインはシステムが監視を開始してからの出現回数の累計である．ラインの長さは他のラインとの関係（計算機の出現回数）を保持して，表示枠内で長さの伸縮を行う．これらの表示は，それぞれ誤検知の判断基準となる警告（連続して多量に出現する警告，監視中頻繁に出現する警告）の提示を目的として実装を行った．また，画面下部には警告メッセージの詳細を表示している（図 6 ※ 3）．これは誤検知に特徴的な警告（サービス内容と実際の通信に矛盾のある警告）および誤検知の判断に有効な情報（計算機のシステムログ情報）の提示を行うためのものである．これにより，誤検知の判別を視覚的に判断することが可能になるだけでなく，従来困難であった NIDS の調整作業を大幅に削減することが可能になると考えられる．

宛先表示部では，アクセスが行われた計算機情報の

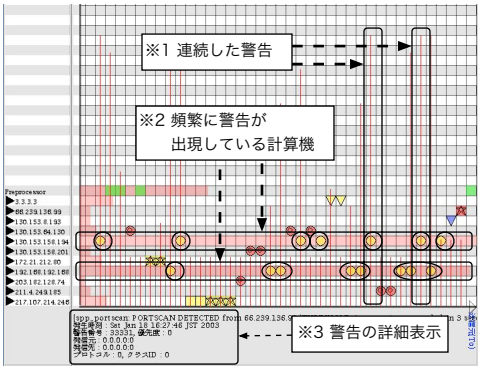

図 6 警告事象の統計表示および詳細表示
Fig. 6 Visualization of statistics processing result and message of alert.

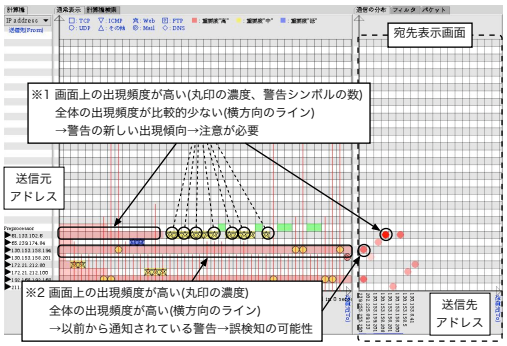

図 7 出現傾向から見た誤検知の判断
Fig. 7 Distinction of false alarms from alert appearance tendency.

表示および NIDS がとらえた通信の記録（パケットペイロード）の表示を行う．宛先表示画面は，アクセスが行われた計算機に関する情報を表示する（**図 7**）．画面は格子状になっており，縦軸方向は計算機名表示部と同様にアクセス元の計算機のアドレスである．横軸方向はアクセスが行われた計算機の IP アドレスをソートして表示を行う．これらの実装は，不正アクセスの監視に必要な情報（アクセス先計算機）および誤検知の判断に有効な情報（NIDS が記録したパケットペイロード情報）の提示を行うことを目的としている．格子の縦と横の交点には丸印を表示し，丸印は画面上にある警告の出現数によって濃度を変化させる．本システムの画面上に出現している警告の数が多い場合，丸印の濃度が濃くなり，警告の数が少ない場合，丸印の濃度が薄くなる．警告表示部に描画された警告のシンボルおよび計算機ごとの出現頻度を表す横方向のラインと比較することにより，警告の出現傾向から見た誤検知の判断を行うことが可能であると考えられる．図 7 ※ 1 では，警告情報表示部のシンボルの数と宛

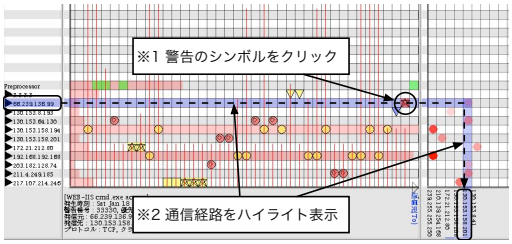

図 8 通信経路のハイライト表示
Fig. 8 Visualization of highlighting a route of packet.

先表示部の丸印の濃度から，警告が多量に現れていることが確認できる．しかし警告情報表示部に描画した横方向のラインが比較的短いことから，過去にはあまりこの計算機に対して警告が発生していないことが分かる．これは警告の新しい出現傾向を示しており，注意が必要である．図 7 ※ 2 では，宛先表示部の丸印の濃度が比較的濃いことから，警告が多く現れていることが分かる．しかし警告情報表示部に描画した横方向のラインも他と比較して非常に長い．これは以前からこの計算機への警告が頻繁に発生していることを示しており，誤検知の可能性が高い．

3.3 対話的機能

はじめに，通信経路のハイライト表示について述べる．本システムでは情報視覚化の手法を用いることにより，警告情報の認識を支援する対話的機能を実現する．この機能により，図的表現から得られた情報の抽出を直感的に行うことが可能である．以下にその機能を示す．

警告表示画面では，警告のシンボルをマウスでクリックすると，通信の経路が青色の帯でハイライトされる（**図 8**）．これにより，警告情報がどこからどこへのアクセスであるかを直感的に認識することが可能であると考えられる．

警告表示画面では，警告のシンボルをマウスでクリックすることにより，警告に関する情報の表示を行う．表示の内容は，警告に関する詳細情報およびパケットペイロードである．この領域に表示される情報は，警告メッセージ，事象の発生時刻，警告番号，警告の優先度，アクセス元計算機の IP アドレスおよびポート番号，アクセス先計算機の IP アドレスおよびポート番号，プロトコル種別，NIDS が定義している警告の種別 ID 番号である．**図 9** に，“WEB-IIS cmd.exe access” に関する警告情報について，詳細の確認を行っている際の例を示す．

さらに宛先表示画面の “パケット” タブの画面にパケットペイロードが表示される．**図 10** に，“WEB-IIS

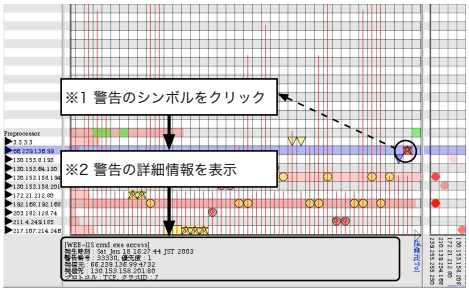

図 9 警告情報の詳細表示
Fig. 9 Visualization of alert details.

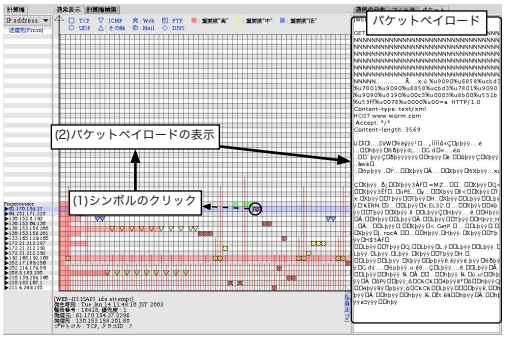

図 10 パケットペイロードの表示
Fig. 10 Visualization of a packet payload.

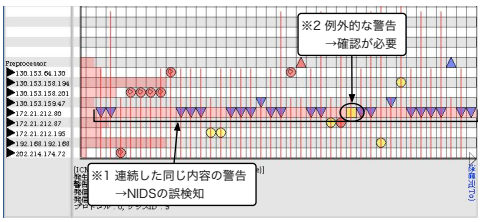

図 11 例外的な警告の検出
Fig. 11 An example of defection exceptional alerts.

ISAPI .ida attempt” というアクセスに関して，NIDS が取得したパケットペイロードの確認を行っている際の例を示す．

4. 検 出 例

4.1 例外的な警告の検出

図 11 では，特定の計算機が ICMP のパケットを定期的に送出しており，それが NIDS の誤検知を引き起こしている（図 11 ※ 1）．通常同じ種類の警告が定期的に発生しているものに関しては，NIDS の誤検知である可能性が高い．しかし図の中で，例外的に形状の異なるシンボルを確認することができる（図 11 ※ 2）．これをテキスト情報で閲覧した場合，頻出する警告情報に埋もれてしまい，例外的な警告を即座に発見

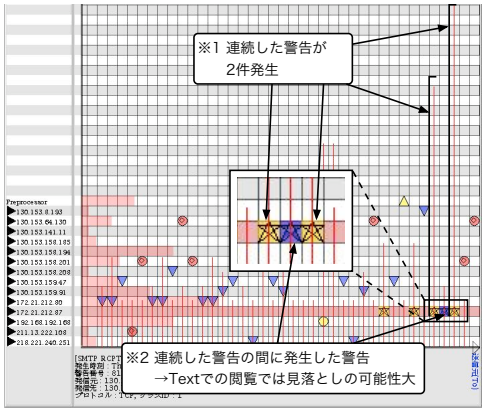

図 12 隠れた警告の判別例
Fig. 12 An example of distinction hidden alerts.

することは困難である．

4.2 隠れた警告の判別例

図 12 の例では，画面上で大量に連続している警告事象を 2 件確認することができる（図 12 ※ 1）．本システムでは，同じ内容の警告が連続している場合，警告のシンボルに重ね合わせて，縦方向に連続量を表すラインを描画する．またそれらの警告事象にはさまれる形で，別の事象を確認できる（図 12 ※ 2）．通常ログファイルをテキスト情報として閲覧する場合，同じ内容の警告が多数発生していると，それらに隠れた少量の警告事象を読み取ることは非常に困難である．本システムではこのような場合でも，見落としなく不正アクセスの監視が可能であると考えられる．

4.3 調査から攻撃までの流れをとらえた例

図 13 の例では，約 15 分に 1 度，外部ネットワークの計算機から，監視対象の計算機に向けて，ごく少数のパケットの送信が行われていた．これは比較的高度な技術を持つ攻撃者が，攻撃の対象とする計算機に対して，計算機の稼働状況を確認するために行う手法である．一般に技術的に未熟な者が調査作業を行う場合，作業の簡略化が可能な専用のプログラムを使用する．その場合，大量のアクセスが NIDS のログへ記録されるため，調査行為の発見は比較的安易に行うことが可能である．しかし攻撃者が間隔を空け，手作業で少しずつ調査を行う場合，監視者は攻撃者の調査行為を見落とすことが多い．

図 13 は，外部の攻撃者が数度にわたる調査の末，サーバに対して攻撃を行うまでの経過をとらえたものである．本システムを用いることで，単一の警告事象だけではなく，他の事象を含めて視覚的に総合的な判断を行うことが可能になると考えられる．

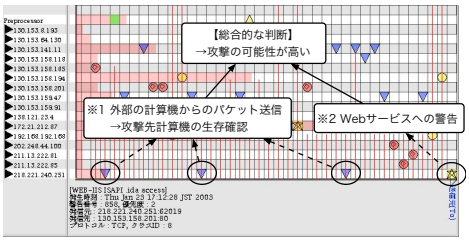

図 13 調査から攻撃までの流れをとらえた例
Fig. 13 An example of defecting “Scan and attack” process.

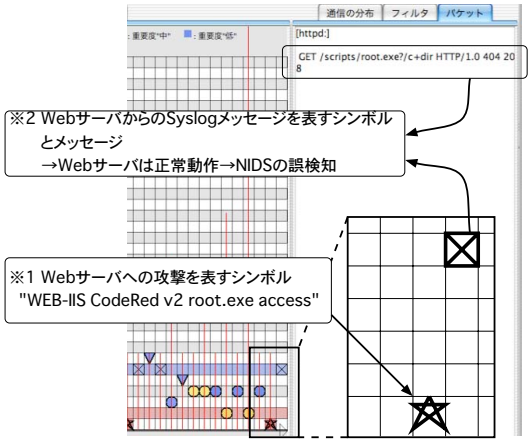

図 14 Syslog を用いた誤検知の判別例
Fig. 14 An example of detecting false alarms with syslog information.

4.4 Syslog を用いた誤検知の判別例

図 14 に，Syslog サーバからの情報を用いた NIDS の誤検知の判別例を示す．画面では，ある計算機より Web サービスへの攻撃を示す警告が発生したことを示すシンボルが表示された（図 14 ※ 1）．これは監視対象のネットワークに存在する Web サーバが，CodeRed ワームに攻撃を受けたことを示す警告である．その直後，Syslog メッセージの受信を示すシンボルとメッセージが表示されている（図 14 ※ 2）．以下に Syslog メッセージの詳細を示す．

```
httpd: GET /scripts/root.exe?/c+dir
       HTTP/1.0 404 208
```

メッセージの Web サーバログの後方から 2 番目，“404” は HTTP Not Found エラーコードである．これは，指定された URL は存在しないことを示している．この場合，Web サーバは停止せず適切にエラーコードを返送していたため，CodeRed ワームの攻撃は成立していないことが分かる．本システムでは，NIDS からの警告情報と各サーバから受信した Syslog メッセージを同時に表示することにより，NIDS の誤検知

判別を容易にしている．

5. 考　　察

5.1 利　　点

本システムにおける利点を以下に示す．

第 1 の利点は，視覚的機能による誤検知の判別が可能である点である．本システムでは，NIDS の管理者がログ情報から誤検知を判断する際の基準をもとに，システムの視覚化機能へ適用を行っている．このため，システムの利用者側で誤検知を判断することが可能になり，誤検知抑制にともなう NIDS の調整作業を大幅に削減することが可能であると考えられる．

第 2 の利点は，実時間による監視が可能である点である．NIDS の警告ログには，継続して大量の情報が出力される．またログファイルを閲覧し，書かれている内容を理解する作業には時間がかかるため，実時間による不正アクセスの監視は現実的には困難である．本システムでは，これらの問題を情報視覚化の技術を適用することで解決した．まず警告事象のシンボル化により警告ログの認識にかかる負荷の軽減が可能である．また警告事象を計算機別および時系列に配置することにより，不正アクセスを行ってきた計算機の行動を早期に特定することが可能であると考えられる．

5.2 今後の課題

本システムにおける今後の課題について述べる．

1 つ目は，警告シンボルの表現力についてである．本システムでは，警告情報をシンボルの色と形状に対応して視覚化を行っている．現在のところ，状態数の多い警告の種別（約 30 種類）や，警告個々の ID 番号（約 1600 種類）については，視覚化を行っていない．今後，これらの情報を文字情報に頼らずに提示するための手法の検討が必要である．

2 つ目は誤検知の判断基準の実装についてである．現在の実装では，多量に発生する警告や頻繁に発生する警告について，個々の計算機単位での表示が可能である．しかし監視中の警告全体を見た場合に，多量または頻出の警告情報については提示を行っていない．これについては，警告の統計処理機能をシステムに追加し，視覚化を行う必要がある．

3 つ目は，未使用の警告情報についての対処である．現在本システムでは，NIDS が取得する情報のうち，パケットのヘッダ情報および警告に関連する Web ページへの URL 情報が未使用である．計算機に仕掛けられたバックドアや DoS 攻撃などでは，ヘッダ情報の中に仕様外の値が書き込まれている場合がある．それらを提示することで，誤検知の判断材料になる可能性がある．今後，これらのヘッダ情報の提示について検討する必要がある．また，関連する Web ページへの URL 情報については，閲覧先が基本的に文字情報であるため，内容を読む行為が発生してしまう問題がある．しかし不正アクセスの調査などを行う際，詳細な情報を取得する目的には，URL 情報の提示が有効だと考えられる．

4 つ目は，警告事象の表示量に関するものである．本システムでは，NIDS が通知する警告のうち，同じ内容が連続しているものについては 1 つの警告事象として取り扱う．NIDS の警告は同じ内容のものが連続して大量に発生する傾向があるため，この方法で 1 度により多くの警告事象を表示することが可能である．本システムでは最新の警告事象を 40 個程度表示を行う．これは筆者らの観測環境においては平均 4 時間の警告事象を表示しているのに相当した．通常ネットワークを介した不正アクセスでは，システムの乗っ取りや不正なファイルの送り込みなどの作業が数分から十数分で完了する．本システムでは，この範囲の時間帯の事象を表示するのに十分な表示能力を有していると考えられる．ただし NIDS を設置する環境により警告の出現数は異なるため，特定の環境では画面の更新が行われ不正アクセスを検知できない可能性がある．今後ネットワークトラフィックの変動に対するシステムの性能について評価を行う必要がある．さらに，後日被害の確認作業などのために日単位など長い時間間隔での警告事象の閲覧も考えられる．これに対処するため，過去の情報を遡って利用者に提示する機能の実現が必要である．

5.3 関 連 研 究

5.3.1 Snort 関連

SnortSnarf[1] および ACID[2] は，Snort の警告ログを解析し，その結果を利用者に提示するシステムである．解析する内容は，警告メッセージに関するもの（警告の総数，警告ごとの出現数），アクセス先およびアクセス元の計算機に関する情報（IP アドレス，ポート番号）である．集計の結果は Web ブラウザを用いて表形式で閲覧を行う．システムの利点としては，Web ブラウザを使用することによって遠隔地からの監視が可能な点や，警告情報にあらかじめ付加されている関連情報への URL（CVE☆，Whitehats☆☆および SecurityFocus☆☆☆）が容易に参照可能な点である．問題点としては，SnortSnarf の場合，警告メッセージ

☆ http://cve.mitre.org/
☆☆ http://www.whitehats.com/
☆☆☆ http://www.securityfocus.com

の解析を一括で行うため，実時間での解析は困難である点，パケットペイロードなどの詳細情報に参照ができない点などがある．ACID においては，情報の解析処理をシステムの実行中に行っているが，解析された情報は文字情報であるため，内容の閲覧および理解が必要である．

RazorBack [3] は，Snort の警告情報を読み込み，ウインドウ画面に表示を行う．ログファイルの場所の指定やファイルの再読み込みの操作は，GUI を使用して操作する．画面には警告情報の優先度が色の付いた丸印で表示されており，優先度の高い警告を判断可能である．また再読み込みボタンを押すことで，最新の警告情報を閲覧可能である．しかし，基本的に警告情報を並べて表示するだけであり，less や more などのページャで閲覧する場合と大きな変化はない．また警告情報の詳細を確認する機能など，対話的な機能は備えていない．視覚化の方法についても，警告の重要度だけはアイコン化されているが，その他の情報は文字情報であり，内容を読んで理解する作業を必要とする．NIDS の警告情報は，膨大な量が出力される．これには誤検知が大量に含まれるため，警告情報を読み取り誤検知と不正アクセスとを判別しなければならない．これは NIDS の警告情報を解析する作業における問題点である．この作業はページャなどのツールでは非常に困難な作業である．本プログラムを使用した場合においても，同種の問題は解決していない．

5.3.2 ログ情報の視覚化

“鼓” [5] は計算機の各種ログ情報を収集し，計算機への接続情報およびユーザに関する状態を視覚化したシステムである．接続が行われた計算機の情報は，ドメイン名によって分類が行われており，計算機の所属が視覚的に判断できる．また計算機にログインを行っているユーザ名や，管理者権限の取得状況についても判断が可能である．さらにマウス操作による対話的なログ情報閲覧を容易にしている．システムの課題としては，複数の計算機の監視や実時間による監視が困難な点がある．

Erbacher らは，計算機間の接続時の情報を，計算機は円，計算機間の接続状態を複数の形状の矢印で視覚化したシステムの提案を行っている[6]．利用する情報は，TELNET や SSH，FTP などのログイン情報，NFS マウントなどのシステム情報である．本システムの利点として，計算機間の接続方向や接続の内容を比較的素早く行うことができる点がある．問題点として，本システムは一定期間のアクセス状況を 1 度に視覚化しているため，連続した時間の流れがとらえにくい点がある．

6. おわりに

本論文では，NIDS の発生する誤検知の判別および実時間による不正侵入検知の支援を目的とした，NIDS ログ視覚化システム “SnortView” について述べた．

NIDS には，誤検知の発生にともなう調整作業が運用上の大きな問題点として存在する．誤検知の発生状況は計算機環境によって異なるため，手作業による繁雑な作業が必要である．また調整作業には計算機管理に熟達し，かつ不正アクセスに関する知識が必要となり，現状では上級者以外には NIDS の取扱いは困難である．これらの作業を支援するため，本研究では管理者が NIDS のログ情報を閲覧する際に用いる誤検知の判断基準をシステムの視覚的機能へ適用したシステムの提案を行った．本システムを用いて NIDS が発生する誤検知の判断を利用者側で視覚的に判断することで，従来困難であった誤検知発生にともなう NIDS の調整作業を大幅に削減することが可能になる．

また本システムでは，連続する同種の警告情報を 1 つの警告事象にまとめ，視覚的なシンボルとして利用者に提示した．これにより，利用者が大量の警告ログを閲覧し内容を理解する負担を軽減する．さらに最新の警告事象を随時表示することで，現在の警告事象を容易に判別することが可能である．本システムを用いることで，最新の警告事象の理解と誤検知の判断を，同時にかつ視覚的に行うことが可能である．これにより，従来実質的に困難であった，NIDS を用いた実時間での不正侵入検知が可能になる．

今後の課題としては，NIDS の誤検知を判断する基準について，より進んだ調査および体系化が必要である．またそれらの結果について，システムへの視覚的機能への適用もあわせて行う必要がある．さらに不正侵入検知を支援するために，NIDS の警告事象を一目で判断可能な視覚化機能の追加，NIDS ログの統計処理機能の追加が必要である．

参考文献

1) Hoagland, J.A. and Staniford, S.: Viewing IDS alerts: Lessons from SnortSnarf, *Proc. 2001 DARPA Information Survivability Conference and Exposition* (*DISCEX 2001*), pp.12–14 (2001).
2) Analysis Console for Intrusion Databases (ACID). http://www.andrew.cmu.edu/%7Erdanyliw/snort/snortacid.html
3) RazorBack. http://www.intersectalliance.com/

projects/RazorBack/index.html
4) Base, R.G.: *Intrusion Detection*, Macmillan Technical Publishing USA (1999).
5) 高田哲司，小池英樹：鼓：不正侵入検知を目的としたログ情報の視覚化，コンピュータセキュリティシンポジウム 2000（CSS2000），pp.271–276, 情報処理学会 (2002).
6) Erbacher, R.F. and Frincke, D.: Visualization in Detection of Intrusions and Misuse in Large Scale Networks, *Proc. IEEE International Conference on Information Visualisation*, pp.244–249 (2002).
7) Snort NIDS. http://www.snort.org
8) Roesch, M.: Snort — Lightweight Intrusion Detection for Networks, *Proc. 1999 USENIX LISA Conference* (1999).
9) 大野一広，高田哲司，小池英樹：SnortView：Snort ログの視覚化システム，マルチメディア，分散，協調とモバイル（DICOMO2002）シンポジウム，pp.361–364, 情報処理学会 (2002).

(平成 15 年 4 月 10 日受付)
(平成 15 年 9 月 5 日採録)

大野　一広（学生会員）

2003 年電気通信大学大学院情報システム学研究科博士前期課程修了．現在同大学院情報システム学研究科博士後期課程在学中．情報視覚化，不正侵入検知に興味を持つ．

高田　哲司（正会員）

2000 年電気通信大学大学院情報システム学研究科情報システム運用学専攻博士課程修了．工学博士．2000 年電気通信大学サテライトベンチャビジネスラボラトリ研究員．現在に至る．情報視覚化と不正侵入検知の研究に従事．IEEE/CS，ACM 各会員．

小池　英樹（正会員）

1991 年東京大学大学院工学系研究科情報工学専攻博士課程修了．工学博士．同年電気通信大学電子情報学科助手．1994 年同大学院情報システム学研究科助教授．現在に至る．1994 年〜1996 年，1997 年 U.C.Berkeley 客員研究員．2003 年 University of Sydney 客員研究員．情報視覚化の研究に従事．特に視覚化へのフラクタルの応用，Perceptual User Interface，情報セキュリティへの視覚化の応用に興味を持つ．1991 年日本ソフトウェア科学会高橋奨励賞，2000 年情報処理学会 DICOMO'2000 最優秀論文賞，2001 年 IEEE VR2001 Honorable Mention for the Outstanding Paper Award 受賞．ACM，IEEE/CS，日本ソフトウェア科学会各会員．