2004－CSEC－27　(12)
2004／12／20

ネットワーク型侵入検知システムにおける アラートベースシグネチャの実現方式

田辺光昭　　勅使河原可海
創価大学大学院工学研究科
E-mail: fmsnabe@rio.odn.ne.jp　teshiga@soka.ac.jp

近年，JPSERT/CC や IPA などの報告を見ても分かるとおり，不正アクセスなどによる被害が増加傾向にあることが言える．そのことにより，各組織においてファイアウォール，ウィルス対策ソフトや侵入検知システム（IDS：Intrusion Detection System）などのセキュリティ製品を導入するところが増えている．しかしながら，IDS 製品の問題になっているのが，誤検知という問題である．本研究では，誤検知の中でもフォールスポジティブに焦点を当て，このフォールスポジティブを減らすことを目的としたアラートベースのシグネチャを作成する方式を提案する．

A Realization Method of Alert Base Signatures in Network Intrusion Detection Systems

Mitsuaki Tanabe　　Yoshimi Teshigawara
Graduate School of Engineering, Soka University

Recently, according to incident reports of JPSERT/CC, IPA, and so on, it can be said that the damage by such as unauthorized accesses is increasing. Therefore, the number of organizations which introduce security products such as firewalls, anti-virus software and intrusion detection systems is increasing. However, it becomes a serious problem that intrusion detection system products induce incorrect detections. In this research, focusing on the false positive among incorrect detections, we propose a realization method which creates alert base signatures to decrease false positive.

1. はじめに

近年，IPA[1]や JPCERT/CC[2]などの報告を見ても分かるとおり，不正アクセスなどによる被害が増加傾向にあると言える．日本国内において大企業の個人情報漏洩事件が相次ぎ，セキュリティに関心が置かれている．そのことによりファイアウォール，ウィルス対策ソフトや侵入検知システム（IDS:Intrusion Detection System）などのセキュリティ製品を導入するところが増えている．しかしながら，IDS 製品の問題点として誤検知が挙げられる．多くの誤検知は管理者の設定によるものか侵入検知システムそのものによるものである．特にフォールスポジティブによって攻撃を示すアラートが多くの誤検知に埋もれてしまうという問題点がある．

本研究では，ネットワーク型侵入検知システムの誤検知に着目し，特に誤検知の中でもフォールスポジティブに焦点を当てている，本研究では，仮想環境をとしてのハニーポットを構築することにより，このフォールスポジティブを減らすことを目的としたアラートベースのシ

グネチャを作成する方式を提案する.

2. 侵入検知システム(IDS)の問題点

セキュリティ技術として, ファイアウォールや侵入検知システムなどが挙げられるが, これらは種々問題点がある. 例えば, 一般的に侵入検知システムの問題点として挙げられるのが, 誤検知の問題である. この誤検知が起こる原因はいくつかあるのだが, 管理者の設定によって引き起こされるものと, 侵入検知システムそのものによって引き起こされるものがある. 誤検知にはフォールスポジティブとフォールスネガティブの 2 種類があり, フォールスポジティブとは攻撃ではないパケットを攻撃であると判断してしまい積極的にアラートをあげることであり, フォールスネガティブとは攻撃であるパケットなのに攻撃ではないとしてアラートをあげないことである. この問題点の解決策としては, ホスト型侵入検知システムとネットワーク型侵入検知システム両方を使用し, 互いの短所を補うことで解決するようなハイブリッド型の侵入検知システムがあるが, これは結局管理者の設定によっては誤検知を引き起こす可能性があるため根本的な解決に至っていない. また, 侵入検知システムをセグメントごとに分散配置することで解決するようなこともある. これもセグメントごとの侵入検知システムがそれ自身によって誤検知を引き起こす可能性があると考えられる.

最近の動向として, IPS（Intrusion Prevention System）や IDP（Intrusion Detection and Prevention）というような製品も市場に出てきているが, これらの製品をインライン型で用いる場合, 誤検知によって正規の通信をブロックしてしまう可能性があるというような問題があることなどが挙げられる.

3. IDS に関する標準化動向

現在, IETF で IDS に関する標準化が進められており, 本研究では以下の標準を使用することを考えている.

(1) IDMEF(Intrusion Detection Message Exchange Format)[3]
・IDMEF とは, IDS が疑わしいと考えられる事象に対して自動的にアラートを報告する際に使用する標準のデータフォーマットである.

(2) IDXP(Intrusion Detection eXchange Protocol)[4]
・IDXP とは, IDMEF のフォーマットに基づいたデータをやり取りするためのプロトコルを規定したものである.

上記のような標準を使用することで, 商用製品やオープンソースの相互運用を可能にすることができると考えられる.

4. アラートベースシグネチャ

4.1 アラートベースシグネチャの目的

ネットワーク型侵入検知システムにおける問題点として誤検知を挙げたが, この誤検知が起こる原因はいくつかあるものと考えられる. 例えば, シグネチャベースの侵入検知システムであれば, 監視しているセグメントのサーバの OS が Windows 系であるのに, Linux 系の攻撃に対するシグネチャを有効にしていたり, mail サーバを稼動していないのに, mail サーバに対する攻撃のシグネチャを有効にしていたりと各組織におけるネットワーク環境またサーバ環境に適した設定を管理者が行えていないために, 誤検知が引き起こされている現状がある. また, 侵入検知システムそのものの検知率の精度によって誤検知を引き起こしている場合がある. 特に本研究で焦点を当てているのは誤検知の中でもフォールスポジティブであり, このフォールスポジティブの大量発生によって, 管理者は正しく侵入検知システムの管理を行えなくなってしまう可能性がある. そこで, 本研究ではフォールスポジティブをアラートベースシグネチャという概念を導入することで減らすことを目的とする.

4.2 アラートベースシグネチャの概要

アラートベースシグネチャとは, 侵入検知システムから出力されるアラートを, ある一連の攻撃の流れに沿ってまとめ, 1 つのシグネチャとして定義したものである. 一連の攻撃の流れとは, 例えば, ping で稼動しているサーバがあるかどうかの確認を行い, 次に portscan を行うことで稼動しているサーバが何番ポートをオープンにしているかを調べ, 次に telnet などでそのポートに接続を試みることで, カーネル, apache などのバージョン情報を取得し, 最後にそのソフトのバージョンに合った exploit ツールで攻撃をサーバに仕掛けるといったようなことである. これら 1 つ 1 つを検出した時点でアラートとして出力するのではなく, ある程度意味のあるものまたは, まとまりのあるものとして出力することを考え, ネッ

トワーク型侵入検知システムにおける誤検知の問題を解決する.

4.3　アラートベースシグネチャの有効性

本研究での実現方式では, 従来の侵入検知システムにおける問題点である多量のフォールスポジティブを出力してしまうということを減らすことができる. Portscan で例を挙げるならば, 従来の侵入検知システムでは, Portscan を定義したシグネチャのアラートが多く出力されてしまい, 攻撃の予兆があることは分かるが, 実際に攻撃が行われたか, または侵入されたことは分からない. 本研究での実現方式では, Portscan 一つ一つに対してアラートを出力するのではなく, 攻撃者が Protscan から攻撃または侵入にいたるまでのプロセスをアラートレベルで抽象化することでフォールスポジティブを減らすことができる. また, ネットワーク構成を自由に構築できるという点から, 各組織におけるネットワーク構成に合わせたアラートベースシグネチャを作成することができる. また, ハニーポットというセキュリティリソースを使用することで, 実際に攻撃者から攻撃を受けることができ, 攻撃のトレンドを知ることに伴って, トレンドにあったアラートベースシグネチャを作成または選択することができる.

4.4　実験環境

本研究では, 実際の攻撃者からの攻撃データの取得とそこから得られた攻撃データを基にアラートベースシグネチャを作成するために図 1 のような仮想環境を用いた実験環境を構築した.

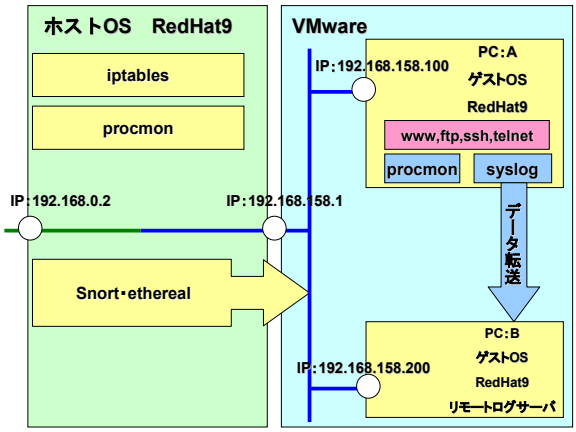

図 1　実験ネットワークの構成

サーバのスペックを以下に示す.

- OS Linux9.0 karnel-2.4.20
- CPU Pentium4 3.2GHz
- Memory 2Gbyte
- HD 120Gbyte

実験環境で導入しているソフトウェアを以下に示す.

- Snort
- Ethereal
- iptables
- Apache
- Open-ssh
- Syslog
- procmon

本研究の実験環境は, VMware という 1 つのホスト上で, 複数の仮想 OS を動かすことができるソフトウェアを用いて仮想環境を実現している. VMware をインストールする OS をホスト OS とし, VMware 上にインストールする OS をゲスト OS とする. 本研究では, ホスト OS, ゲスト OS ともに RedHat9 を使用している.

ホスト OS 上では, iptables, Snort, ethereal, procmon がインストールされている. また, Snort を管理しやすくするために, ACID 等の Snort 管理ツールもインストールされている. VMware 上には 2 つのゲスト OS, PC:A と PC:B が存在し, PC:A は実際にサービスを提供するサーバとして稼動している. 提供しているサービスは, www, ftp, ssh, telnet の 4 つである. PC:B は, リモートログサーバとして稼動している. これは, PC:A に侵入された時, ログの改竄等を行われても PC:A のログの正当性を保証するために一定時間毎に PC:B のリモートログサーバに PC:A のログを転送するようにしている. iptables では, NAT の設定を行い, PC:A と外部の通信を可能にしている. また, ホスト OS, PC:B のリモートログサーバに侵入されないように, 外部から通信が出来ないようにしている. Snort は, 仮想環境上のネットワークを監視するために導入している. ethereal は, 仮想環境上のネットワークに流れているデータを取得するために導入している. procmon は, ネットワークを監視している場合, ssh などを使ったバックドアを仕掛けられた際に, 暗号化された通信により攻撃者の行動が不明になってしまうので, システム側でコマンド履歴を自動保存してくれるため導入している.

ネットワーク構成は，ブロードバンドルータとの接続地点は IP アドレス:192.168.0.2 が固定で割り当てられており，ホスト OS と仮想環境のデフォルトゲートウェイは IP アドレス:192.168.158.1，PC:A の IP アドレス:192.168.158.100，PC:B の IP アドレス:192.168.158.200 がそれぞれ割り当てられている．

4.5 取得データ

本研究では，4.4 で述べたような実験環境のもとで，攻撃者による攻撃データを取得した．本研究で用いている実験環境は，仮想環境としてのハニーポットを構築している．ハニーポットとはプローブされ，攻撃され，侵害されることに価値を持つセキュリティリソースであることから，攻撃者の実際の攻撃データを取得するには適した環境と言える[5]．

ハニーポットを稼動した回数は全 2 回であり，期間は以下の通りである．

(1) 2004 年 10 月 15 日～2004 年 10 月 18 日
(2) 2004 年 10 月 26 日～2004 年 10 月 28 日

ethereal でキャプチャされた総パケット数は 8715 であり，Snort が出力したアラート数は 1064 である．一般的に侵入検知システムの運用を行うと大量のアラートを出力するのだが，今回の運用で Snort のアラート数が少ないのは，ハニーポットに攻撃をしてくる攻撃者がなかなか現れないことや，ハニーポットの稼動期間が短いということが挙げられる．これらの解決策として，稼動期間を長期にわたり運用することが必要であることが言える．しかし，そのデータの中でも有用なデータが取れていることを確認した．具体的には，ftp にユーザ :anonymous，パスワード:Hgpuser@home.com で接続をしてきたユーザの行動は，ディレクトリ pub に移動した後に 040629221246p というディレクトリを作成し，パッシブモードに切り替えてから 2 回ほど p の文字列を 2828 バイト送信した後に RST パケットを送信して通信を終了している．ftp に接続をして同じような行動をする攻撃者が何人か存在したことを確認した．また，www サーバに接続して，長い文字列の URL を送信し続ける攻撃者も存在したことも確認できた．実際のデータ取得時の画面を図 2 に示す．

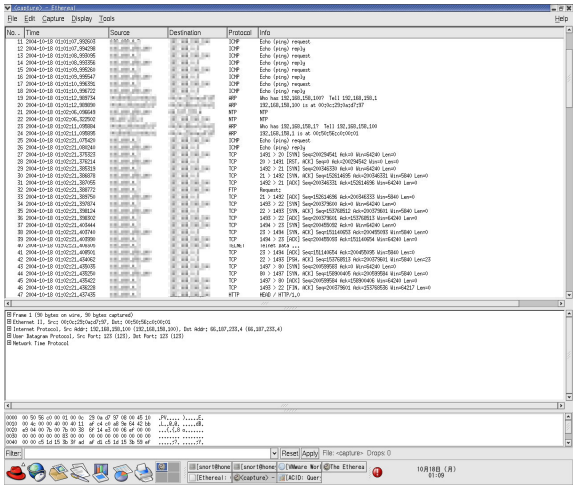

図 2 データ取得時の画面

取得したデータはアラートベースシグネチャを作成する際に，Snort から出力されるアラートを分析するデータとして扱う．

4.6 アラートベースシグネチャの作成

4.3 で述べた実験環境から取得できたデータと Snort から出力されたアラートを基にアラートベースシグネチャを作成するために，今回は一般的な攻撃手順について考察した．一般的な攻撃手順を以下に示す．

(1) ping でサーバが稼動しているか確認を行う．
(2) portscan を行うことで稼動しているサーバが何番ポートをオープンにしているかを調べる．
(3) telnet などでそのポートに接続を試みることで，カーネル，apache などのソフトウェアのバージョン情報を取得する．
(4) 取得したバージョンに合った exploit ツールを使用してサーバに攻撃を実行する．

今回は，ブロードバンドルータが ICMP パケットのルーティングに対応していないという実験環境自体の問題によりリモートからの ICMP パケットをキャプチャできないという問題があり，プローブに関してのデータが取得できないということにより，ローカルから上記の攻撃手順を行った．使用したツールは(1)～(3)をまとめて実行する superscan というスキャンツールを使用し，(4)は www への攻撃を行った．これらより Snort から出力されたアラートを用いることで，アラートベースのシグネチャを作成する．

実際のアラートベースシグネチャは，Snort

のシグネチャは SID（Snort rule ID）で管理されているので，この SID の組み合わせによってアラートベースシグネチャを表現する. 例えば，(1)～(4)の攻撃手順をアラートベースシグネチャにすると以下の SID を抽出したものになる.

・ICMP PING：sid 384
・ICMP Echo Reply：sid 408
・ICMP superscan echo：sid 474
・TELNET access：sid 716
・TELNET Login incorrect：sid 718
・INFO TELNET Bad Login：sid 1251

これらを一つにまとめたものをアラートベースシグネチャとして定義する. また，今回は 4.3 で示した最小のネットワーク構成の実験環境でアラートベースのシグネチャを作成したが, 仮想環境を生かして様々なネットワーク構成を想定したアラートベースのシグネチャを作成することができると考えられる. 例えば，www サーバ以外に mail サーバや DNS サーバを導入したネットワーク構成や，DMZ（DeMilitarized Zone）をはさみ, そこに www サーバや mail サーバを導入したネットワーク構成を構築するなどができる.

5. 実験結果および考察

本研究では，4.2 で述べたような実験環境のもとでアラートベースシグネチャを作成した. 作成したアラートベースシグネチャを使用した結果は, 調査をしたところ従来の侵入検知システムでのアラート数は 1064 であったが，アラートベースシグネチャを適用させた時は, 攻撃の可能性があると示されるアラートの数が 39 になるという結果が得られた（図 3，図 4 参照）. この結果より，アラートベースシグネチャが侵入検知システムの問題であるフォールスポジティブを減らすのに有効であることが言える. そして，侵入検知システムが検出した攻撃やプローブに対して 1 つ 1 つアラートを出力するのではなく, 一連の攻撃手順に従ったもの, ある程度意味のあるものにまとめられた形すなわちアラートベースシグネチャを適用させることは有効であると言える.

考察として，ping の数が 221 から 21 に減少したことは, 使用したスキャンツールの影響によるものだと考えられる. scan の数が 143 から 0 に減少したことは, スキャンツールとの相関関係により ping との相関が取れなかったために 0 になったと考えられる. telnet の数が 643 から 6 に減少したことは，時間軸で ping との相関関係が取れたのが 6 つのアラートであった. apache の数が 57 から 12 に減少したことは，これも telnet の時と同様に時間軸で telnet との相関関係が取れたのが 12 個のアラートであったので減少したと考えられる.

また, 今回はサンプルとして 1 つのアラートベースシグネチャを示したが, 他の組み合わせによるアラートベースシグネチャを用いることで, 他の攻撃の可能性があるアラートを抽出できることが考えられる.

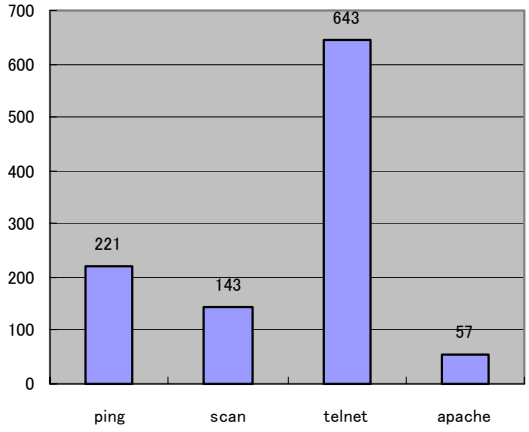

図 3　従来の IDS におけるアラート数

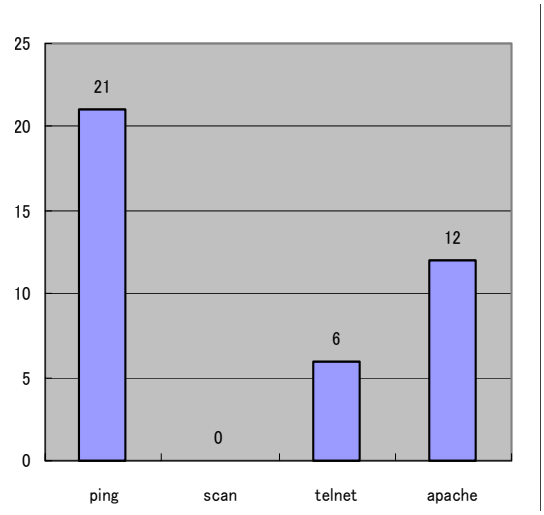

図 4　本研究の実現方式適用時のアラート数

6. システムの運用方法

本研究の実現方式の運用方法としては, ネットワーク型侵入検知システムが各セグメントに配置され, 統合管理サーバが配置されたようなネットワーク環境があるとする. ここでは，最小のネットワーク構成として 3 つのセグメントで考える. 1 つはインターネット側，2 つは DMZ，3 つはイントラネットに侵入検知シ

ステムが配置されており, 図 5 に示したように, イントラネット内には 3 つの侵入検知システムを統合管理するための統合管理サーバを配置している（図 5）. 3 つのセグメントにおける侵入検知システムと統合管理サーバの役割としてインターネット側の侵入検知システム（IDS1）は，すべての通信に対してアラートを発するものである．DMZ の侵入検知システム（IDS2）は，ファイアウォールを越えた通信に対してアラートを発するものである. イントラネット側の侵入検知システム (IDS3) は, DMZ からファイアウォールを越えたパケットまたは, 内部からの通信に対してアラートを発するものである. また, 統合管理サーバは IDS1, IDS2, IDS3 が出力するアラートをまとめる役割と共に, アラートベースシグネチャを格納した統合データベースを保持しており，IDS1, IDS2, IDS3 から出力されたアラートとマッチングを行い, アラートベースシグネチャとマッチングが取れたら管理者にアラートを通知するものである.

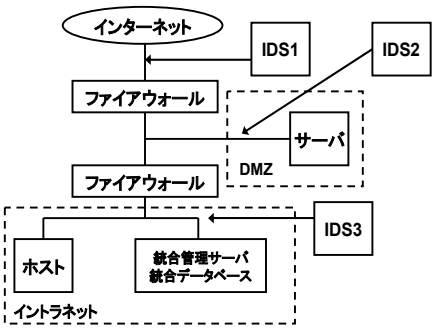

図 5　IDS 配置例

IDS1，IDS2，IDS3 と統合管理サーバとの関係を図 6 に示す.

IDS1，IDS2，IDS3 は各セグメントでどのような事象が起こっているのかお互いにアラートの情報共有をする関係にあり，IDS1, IDS2, IDS3 と統合管理サーバは IDS1, IDS2, IDS3 で出力されるアラートを受け取り集中管理する関係にある. このような関係の必要性は, ネットワーク全体で何が起こっているかを把握することと, IDS 間で連携をとることにより, さらに誤検知が減少すると考えられるからである. IDS 間で連携を取るというのは, 例えば, イントラネット内の IDS3 で何か起こっているのに, インターネット側の IDS1 では何も起こっていないということが分かれば, 内部に攻撃者がいるという状況を把握することができると考えられる.

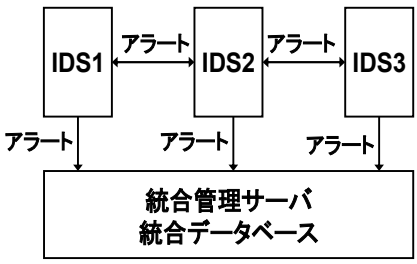

図 6　IDS と統合管理サーバの関係

7. まとめと今後の課題

本研究では, 侵入検知システムの問題点である誤検知, 特にフォールスポジティブに焦点を当て, フォールスポジティブを減らすことを目的としたアラートベースシグネチャの実現方式を提案した. 本研究では, 実際に実験環境を構築し, 攻撃者が行う行動すなわち攻撃データを取得した. その攻撃データと Snort が出力したアラートを用いてアラートベースシグネチャを作成し, その有効性を検証した. その結果, 従来の侵入検知システムで出力されるアラート数よりも, 本研究の実現方式の方がアラート数が非常に少ないことが分かった.

今後の課題として, 本研究の実現方式は攻撃は一連の流れとして行われることを前提として, アラートベースシグネチャを作成しているので, 攻撃者が時間的に間隔をあけた攻撃やプローブを行った場合, 攻撃元が単体ではなく複数にわたる場合にそれらを検知できるような手法を検討する必要がある. また, データ分析からアラートベースシグネチャの作成まで全てが手動であるため, 自動化を検討する必要がある.

8. 参考文献

[1] IPA:http://www.ipa.go.jp/
[2] JPCERT/CC:http://www.jpcert.or.jp/
[3] IDMEF:
http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-12.txt
[4] IDXP:
http://www.ietf.org/internet-drafts/draft-ietf-idwg-beep-idxp-07.txt
[5]ランス・スピッツナー著，電気通信大学小池研究室セキュリティ研究グループ訳，“ハニーポット-ネットワーク・セキュリティのおとりシステム”慶応義塾大学出版会，2004 年