コンピュータセキュリティ　18－6
(2002.　7.　18)

# プロトコル仕様及びポリシー情報を利用した不正アクセス検知システムの実環境評価

馬場 達也　鴨田 浩明　小久保 勝敏　松田 栄之

株式会社 NTT データ 技術開発本部

〒104-0033 東京都中央区新川 1-21-2 茅場町タワー

E-mail:　{baba, kamochan, kokubo, matu}@rd.nttdata.co.jp

**あらまし**　現在、未知の手法も含めて不正アクセスを即座に検知する技術が強く求められている。著者らは、これまでに、ネットワーク上のパケットを監視し、プロトコル仕様及びサイトのアクセスポリシーと比較することによって、未知の手法も含めて不正アクセスを検知する方式について提案してきた。また、提案した方式をプロトタイプシステムとして実装し、第三者が公開している不正アクセスデータベースを用いて検知率の評価を行っている。本稿では、実装したプロトタイプシステムを実環境に設置し、実際に運用されているサーバへのアクセスに対して誤検知の評価を行うことによって、本方式を実装した検知システムが、高い精度で不正アクセスを検知できることを示す。

**キーワード**　侵入検知，IDS，ネットワークセキュリティ，不正アクセス

# Evaluation of Protocol and Policy-Based Intrusion Detection System in Real Environment

Tatsuya BABA, Hiroaki KAMODA, Katsutoshi KOKUBO, and Shigeyuki MATSUDA

Research and Development Headquarters, NTT Data Corporation

Kayabacho Tower, 1-21-2, Shinkawa, Chuo-ku, Tokyo, 104-0033 Japan

E-mail:　{baba, kamochan, kokubo, matu}@rd.nttdata.co.jp

**Abstract**　Currently, unauthorized access detection technology is strongly required. We have proposed a method of detecting unauthorized accesses including unknown ones by monitoring packets and comparing them with protocol specifications and site access policy. In this paper, we show the effectiveness of the proposed detection method by evaluating the false positive rate of prototype system in a real environment.

**Keyword**　Intrusion Detection, IDS, Network Security, Unauthorized Access

## 1. はじめに

近年、電子商取引等のインフラとしてインターネットの重要性が高まる中、システムに被害を発生させる不正アクセスを即座に検知する技術が強く求められている。最近では、不正アクセス検知システム（IDS：Intrusion Detection System）が多くの企業で導入されるようになってきたが、多くの IDS は、パケットの内容を既知の不正アクセスの特徴（シグネチャ）と比較するシグネチャベースのものであるため、新しい手法の不正アクセスには対応できないという問題がある。

そこで著者らは、特に不正アクセスのターゲットとされやすい、WWW サーバ等のインターネットサーバに対する不正アクセスを、プロトコル仕様及びサイトのアクセスポリシーと比較することによって、未知の手法も含めて不正アクセスを即座に検知する方式について提案してきた[1,2]。そして、提案した方式が高い精度で不正アクセスを検知できることを示すため、第三者が公開している不正アクセスデータベースを使用して検知率の評価を行い、89.6%の不正アクセスを検知できることを示した[3]。本稿では、実装したプロトタイプシステムを、正常アクセスが多く発生する実環境ネットワークに設置し、正常アクセスを不正アクセスとして検知してしまう誤検知に関する評価を行うことによって、本方式による検知システムが低い誤検知率で機能することを示す。

## 2. 不正アクセス検知の考え方

本方式では、未知の不正アクセスも含めて検知を行うために、正常なアクセスの条件を定義し、正常ではないアクセスをすべて不正アクセスとして検知する。しかし、正常なアクセスの条件を実際のアクセスから学習して生成すると、学習期間中に発生しなかった正常なアクセスを不正アクセスとして誤って検知したり、学習期間中に攻撃者が意図的に不正アクセスを多く発生させることによって正常アクセスの条件を操作することが可能となるため、正常アクセスの条件は、あらかじめ手動で設定しておく。

正常アクセスの条件は、プロトコルの仕様とアクセス先のサーバの設定内容によって決定される。ただし、プロトコルの仕様には、IP オプションや IP フラグメントなど、サーバへのアクセスでは通常使用されない機能等も含まれている。このため、「プロトコル仕様準拠範囲」から、通常は使用されない機能の範囲を除いた「通常アクセス範囲」を設定する。そして、アクセス先のサーバの設定内容によって決定されるサイト依存部分の条件を「アクセスポリシー」として設定し、図 1 のように正常アクセス範囲を設定する。

こうすることで、学習という処理を行わずに未知の手法を含む不正アクセスを検知することが可能となる。プロトコル仕様準拠範囲および通常アクセス範囲の条件は、事前に検知システムに組み込んでおき、アクセスポリシーは、サイトの管理者が検知システムの導入時に設定する。

ただし、通常アクセス範囲やサイトのアクセスポリシーで許可する範囲を広く設定してしまうと、不正アクセスであるものを検知できなくなる可能性がある。また、逆にこれらの範囲を狭く設定してしまうと、正常アクセスであるものを不正アクセスであるとして検知してしまう可能性があるので、これらの範囲を適切に設定することが重要となる。

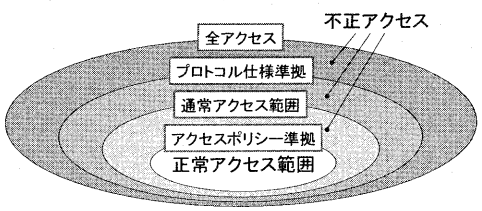


図 1 正常アクセス範囲

## 3. 検知処理手順

本方式では、図 2 の手順で検知処理を行う。「プロトコル仕様チェック」では、IP 層、トランスポート層、アプリケーション層の順で、プロトコル毎にあらかじめ決められたプロトコル仕様準拠の条件および通常アクセスの条件と比較することにより行われる。

「アクセスポリシーチェック」では、パケットの送信元/宛先 IP アドレス及び利用プロトコルがアクセスポリシーで許可されているかどうかをチェックする。また、プロトコルで使用されているコマンドや URL 等の内容、データの長さがアクセスポリシーで許可されているかどうかについてもチェックを行う。

また、「Flood チェック」では、単位時間あたりのアクセスの回数が、アクセスポリシーに記述されているアクセスの許容頻度以内であるかどうかをチェックする。

プロトコル仕様チェック、アクセスポリシーチェック、Flood チェックの結果に異常が存在した場合には、不正アクセスが発生したと判断し、電子メールなどにより管理者に通知する。

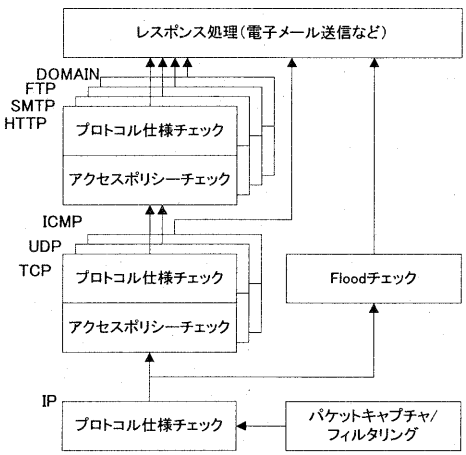


図 2 検知処理の流れ

## 4. プロトコルチェック処理

プロトコル仕様チェック及びアクセスポリシーチェック(以後まとめてプロトコルチェックと呼ぶ)は、インターネットサーバへのアクセスで使用される IP, TCP, UDP, ICMP, HTTP, SMTP, FTP, DOMAIN [4-11]などのプロトコル毎に行う。ここでは、この中から IP, TCP, HTTP のプロトコルチェック処理の一部について説明する。

### 4.1. IP プロトコルチェック

IP プロトコルチェック部でチェック対象としたフィールドとそのチェック内容は表 1 の通りである。

表 1　IP ヘッダのチェック内容

| フィールド名 | チェック条件 |
|---|---|
| Version | 4 であること |
| Internet Header Length | 5 であること（IP オプションなし） |
| Total Length | 21 バイト以上であること |
| Flags（Reserved）<br>Flags（MF）<br>Fragment Offset | 0 であること（フラグメントなし） |
| TTL | 4 以上であること |
| Header Checksum | チェックサムが正しいこと |
| Source Address | ホストが使用できるグローバルアドレスであること |

### 4.2. TCP プロトコルチェック

TCP プロトコルチェック部でチェック対象としたフィールドとそのチェック内容は表 2 の通りである。

表 2　TCP ヘッダのチェック内容

| フィールド名 | チェック条件 |
|---|---|
| Source Port<br>Destination Port | どちらか一方は 1024 以上であること |
| Data Offset | 5 以上であること |
| Reserved | 0 であること |
| Control Bits（URG, ACK, PSH, RST, SYN, FIN） | SYN, RST, ACK, FIN+ACK, SYN+ACK, RST+ACK, ACK+PSH, FIN+ACK+PSH のいずれかであること |
| Checksum | チェックサムが正しいこと |

### 4.3. HTTP プロトコルチェック

HTTP プロトコルチェック部でチェック対象としたフィールドとそのチェック内容は表 3 の通りである。

表 3　HTTP のチェック内容

| フィールド名 | チェック条件 |
|---|---|
| Method | あらかじめアクセスポリシーとして登録された、サイトで許可するコマンドであること |
| Request-URI | 通常使用される文字（0-9, a-z, A-Z, チルダ, ハイフン, アンダースコア, ピリオド, "+", "$", "#", "%7E", "%7e"など）で構成されていること<br>CGI を使用しない場合は、"?"を含まないこと<br>URL の長さがサイトのアクセスポリシーで定める長さの範囲内であること |
| HTTP-Version | 存在する場合は、"HTTP/1.0"または"HTTP/1.1"のどちらかであること |
| HTTP ヘッダ | 仕様に記述されている HTTP ヘッダであること<br>HTTP ヘッダの長さがサイトのアクセスポリシーで定める長さの範囲内であること |

## 5. 検知精度の評価

提案した検知方式が有効であることを検証するため、作成したプロトタイプシステムを用いて検知精度に関する評価を行った。

### 5.1. 評価の考え方

検知精度を測る指標としては、「検知率」と「誤検知率」の 2 つがある。「検知率」は、不正アクセスが検知できる割合のことであり、True Positive Rate とも呼ばれる。また、「誤検知率」は、正常アクセスを不正アクセスとして誤って検知してしまう割合のことであり、False Positive Rate とも呼ばれる。この 2 つの指標のどちらか一方だけが良くても検知精度が良いとは言えない。

本方式では、プロトコルの仕様に基づいた仕様準拠範囲と、実際の利用に基づいた通常アクセス範囲、そして、サイトで設定するアクセスポリシーによって、正常アクセスの範囲を定義している。このため、これらの範囲の設定の仕方が、検知率と誤検知率の値に大きく影響すると考えられる。

検知率に関しては、Whitehats 社が公開している不正アクセスデータ[12]を使用して評価を行い、89.6%の検知率を得ることができている[3]。そこで、今回は、さまざまな種類の正常アクセスが発生する実環境にプロトタイプを設置することによって、誤検知率の評価を行った。

### 5.2. 評価に使用したプロトタイプ

評価に使用したプロトタイプは表 4 のとおりである。実装した PC には、ネットワークカードを 2 枚装着し、一方を不正アクセス監視専用のインタフェース（IP アドレスを付与しない）とした。

表 4 実環境評価で使用したプロトタイプのスペック

| | |
|---|---|
| OS | FreeBSD 4.2-RELEASE |
| CPU | 2GHz Pentium 4 |
| メモリ | 512MB RAM |
| ネットワークカード | Intel Pro/100+ ×2 |
| パケットキャプチャ | BPF + libpcap |

### 5.3. 評価環境

評価を行った環境のネットワーク構成を図 3 に示す。不正アクセスセンサのプロトタイプと共に、TCPDUMP によりターゲットサーバへの全パケットデータを取得するマシンを接続し、WWW/FTP サーバおよびメール/DNS サーバへのアクセスを監視した。

検知システムのアクセスポリシーでは、監視対象サーバに対して、表 5 に示すプロトコルを使用したパケットを許可するように設定した。さらに、アクセスポリシーでは、表 6 に示す DOMAIN の OPCODE 値および QTYPE 値と、表 7 に示す HTTP、SMTP、FTP のコマンドを許可するように設定した。HTTP の URL 長、

HTTP ヘッダ長、SMTP で送信するコマンドラインの長さ、ICMP のメッセージ長は、それぞれ 200 バイト以下を許可し、FTP で送信するコマンドラインの長さは 100 バイト以下を許可するように設定した。そして、FTP で許可するユーザを"anonymous"および"ftp"のみに設定した。また、検知率の評価では、CGI へのアクセスを禁止する設定にしたが、実環境の Web サーバでは CGI を使用していたため、CGI へのアクセスを許可する設定にした。

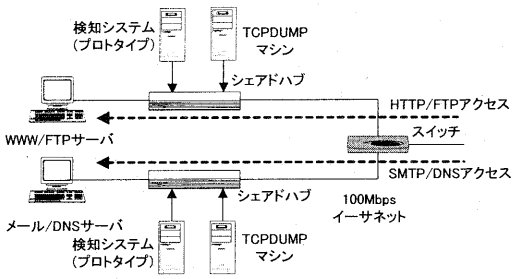


図 3 評価環境におけるネットワーク構成

表 5 アクセスポリシーで許可したプロトコル

| | |
|---|---|
| TCP | HTTP（ポート 80）, SMTP（ポート 25）<br>FTP（ポート 21）,<br>FTP-DATA（ポート 20, 1024～65535） |
| UDP | DOMAIN（ポート 53） |
| ICMP | Destination Unreachable（タイプ 3）<br>Time Exceeded（タイプ 11）<br>Parameter Problem（タイプ 12） |

表 6 アクセスポリシーで許可した DOMAIN パラメータ

| パラメータ | 許可した内容 |
|---|---|
| OPCODE | QUERY |
| QTYPE | A, NS, CNAME, PTR, MX, ANY |

表 7 アクセスポリシーで許可したコマンド

| プロトコル | 許可したコマンド |
|---|---|
| HTTP | GET, HEAD |
| SMTP | HELO, EHLO, MAIL, RCPT, DATA, QUIT |
| FTP | USER, PASS, CWD, CDUP, PORT, PASV, TYPE, MODE, RETR, ABOR, PWD, XPWD, LIST, NLST, SYST, SIZE, NOOP, QUIT |

## 5.4. 評価方法

2001 年 11 月 21 日から 2002 年 2 月 1 日までの間、監視対象サーバへのアクセスに使用されたパケットの数とプロトタイプによって発生したアラームの数を取得した。発生したアラームには、不正アクセスによるものと、誤検知によるものが含まれているため、TCPDUMP を動作させているマシン上に蓄積されたデータの中から、アラーム発生の原因となったパケットデータを取得し、このデータの不正であると判断された部分を過去の不正アクセスデータなどと比較することによって、不正アクセスか正常アクセスかの判別を行った。

## 5.5. 結果

結果を表 8 に示す。すべてのパケットから、攻撃パケットまたは異常パケットと判断したものを抜いたものを正常パケットとし、誤検知数を正常パケット数で割ったものを誤検知率とした。DOMAIN（UDP）の誤検知率が 5.1%となったが、その他は 0～2%程度の誤検知率となった。

表 8 プロトコル別結果

| プロトコル | 総数 | アラーム | | 誤検知率 |
|---|---|---|---|---|
| | | 攻撃 | 誤検知 | |
| HTTP/TCP | 187,092 | 531 | 2,190 | 1.2% |
| SMTP/TCP | 13,968 | 3 | 281 | 2.0% |
| FTP/TCP | 537 | 34 | 0 | 0% |
| DOMAIN/TCP | 85 | 1 | 0 | 0% |
| DOMAIN/UDP | 1,987 | 6 | 101 | 5.1% |
| ICMP | 11,860 | 158 | 0 | 0% |
| 計 | 215,529 | 733 | 2,572 | 1.2% |

※誤検知率＝誤検知数／（総数－攻撃数）

### HTTP パケットの誤検知

HTTP を使用したパケットのチェックにおいて、誤検知となった原因は以下のとおりである。

① プロトタイプに登録されていない非標準 HTTP ヘッダを使用していたため、不正であると判断された（1,801 件）
② ヘッダの 1 行の長さがポリシーで設定した値（200 バイト）を超えていたため、ポリシー違反であると判断された（228 件）
③ ポリシーで許可するように設定されていなかった POST コマンドを使用したアクセスが存在したため、ポリシー違反であると判断された（113 件）
④ プロトタイプに登録されていない記号や日本語を含んだ URL へのアクセスがあったため、不正であると判断された（33 件）
⑤ パケットのキャプチャ漏れによる TCP セグメント再構成の失敗による誤検知（13 件）
⑥ ポリシーで設定した大きさ（1,500 バイト）を超えたデータのアップロードが行われたため、ポリシー違反であると判断された（2 件）

誤検知の多くは、プロトタイプに登録されていない非標準 HTTP ヘッダが使用されたとして発生したアラ

ームである。これは、クライアントが過去の仕様（インターネットドラフト）で指定されていたヘッダを使用していたり、キャッシュサーバやプロキシサーバなどがクライアントから要求されたメッセージ中のヘッダを仕様（RFC：Request for Comments）で規定されていないヘッダに書き換えていることが原因である。

**SMTP パケットの誤検知**

SMTP を使用したパケットのチェックにおいて、誤検知となった原因は以下のとおりである。

① プロトタイプに登録されていない非標準メールメッセージヘッダを使用していたため、不正であると判断された（148 件）
② メッセージの 1 行の長さがポリシーで設定した長さ（200 バイト）を超えたため、ポリシー違反であると判断された（81 件）
③ MAIL FROM コマンドで指定する送信元メールアドレス中にプロトタイプに登録していない記号が含まれていたため、不正であると判断された（35 件）
④ 宛先として指定したアドレスが多いために、メールメッセージのヘッダの行数がポリシーで設定した数（100 行）を超えたため、ポリシー違反であると判断された（10 件）
⑤ 宛先到達不能などの理由でエラーメールが返送された場合に、MAIL FROM コマンドで指定する送信元メールアドレスが空となるため、不正であると判断された（4 件）
⑥ パケットのキャプチャ漏れにより、TCP セグメントの再構成に失敗したため、不正であると判断された（3 件）

誤検知の多くは、プロトタイプに登録されていないメッセージヘッダが使用されたとして発生したアラームである。プロトタイプでは、仕様で定められている標準のメールメッセージヘッダのみを登録し、チェックしていた。しかし、実際には、仕様で定められていない非標準のヘッダや、プロトタイプに登録されていない、比較的新しい仕様で定められたヘッダが多く使用されており、これらがアラームの原因となった。

**DOMAIN パケットの誤検知**

DOMAIN を使用したパケットのチェックにおいて、誤検知となった原因は以下のとおりである。

① UDP の 53 番ポートへの問い合わせにおいて、送信元ポートに 1024 以上または 53 以外のポート（137 番ポート）が使用されていたため、不正であると判断された（101 件）

マイクロソフト社の Windows などでは、137 番ポートを利用して、ネームサーバの 53 番ポートへ問い合わせを行なうため、これが誤検知の原因となった。

### 5.6. 検知率と誤検知率

検知率と誤検知率は一般的にトレードオフの関係にあるため、本来は、同じアクセスポリシーで両方の評価を行うべきである。しかし、不正アクセスデータベースを使用して行った検知率の評価では、CGI へのアクセス（"?"を含む URL へのアクセス）を禁止するアクセスポリシーにして評価を行い、誤検知率の評価では、逆に CGI へのアクセスを許可するアクセスポリシーにして評価を行った。このように、検知率の評価と誤検知率の評価で CGI へのアクセスに関するポリシーの設定が異なっているが、CGI へのアクセスを禁止している環境を想定すると、"?"を含む URL へのアクセスは必ず不正アクセスとなるため、誤検知率には影響しない。このため、表 9 のように、CGI へのアクセスを禁止している環境でも、誤検知率は CGI へのアクセスを許可した今回の結果と同様となると考えられる。

表 9 検知精度（CGI へのアクセスを禁止した場合）

| 検知率 | 誤検知率 |
|---|---|
| 89.6% | 1.2% |

## 6. 考察

今回得られた誤検知率と以前に行った検知率の結果から、本方式の有効性について考察する。

### 6.1. アクセスポリシーの適切な設定による精度向上

本方式の特徴は、正常アクセスの範囲をサイトのアクセスポリシーによって、環境に合わせて決定できる点にある。このアクセスポリシーを適切に設定することによって、検知精度を向上させることが可能となる。

今回の評価では、本方式が高い検知精度で不正アクセスを検知できることが確認できた。しかし、設定したアクセスポリシーが、実際の利用状況とあっていなかったために発生した誤検知も存在した。アクセスポリシーは、事前に利用環境を十分調査して設定するべきものであるが、必ずしもそれが実際の利用状況とあっているとは限らない。このため、本方式による検知システムの導入当初は、試験的な運用を行い、その際にアクセスポリシー違反によるアラームが多いようであれば、その内容を十分確認した後で、アクセスポリ

シーを修正していく必要がある。これにより、誤検知を減らすことが可能となると考えられる。

### 6.2. プロトコルチェックの改良による精度向上

今回の誤検知の原因としては、設定したアクセスポリシーが実際の利用状況と合っていなかったために生じたものに加えて、通常アクセス範囲を狭く取りすぎていたことも大きく影響している。このため、以下のようにプロトコルチェックの条件を緩和し、通常アクセス範囲を広くすることで、さらに誤検知を抑えることができると考えられる。

① HTTP プロトコルチェックの HTTP ヘッダチェックの廃止
② SMTP プロトコルチェックのメールメッセージヘッダチェックの廃止
③ SMTP プロトコルチェックのメールアドレスチェックにおいて、メールアドレスに含まれる記号として、ダブルクォーテーション（"）、イコール（=）、アスタリスク（*）を追加する。
④ UDP プロトコルチェックの送信元ポート番号チェックを廃止する。

以上の改良を施すことにより、CGI を使用していない環境を想定した場合の検知率および誤検知率は、表 10 および表 11 のようになる（これまでの評価で使用したデータと同じものを使用して算出）。検知率は以前の評価結果よりも 0.5%ほど下がるが、誤検知率を 0.2%にまで下げることができる。

表 10 改良実施後の検知率

| プロトコル | 総数 | 成功 | 失敗 | 検知率 |
|---|---|---|---|---|
| HTTP | 83 | 70 | 13 | **84.3%** |
| SMTP | 15 | 12 | 3 | 80.0% |
| FTP | 39 | 31 | 8 | 79.5% |
| DOMAIN | 8 | 8 | 0 | 100% |
| ICMP | 41 | 41 | 0 | 100% |
| TCP | 20 | 20 | 0 | 100% |
| UDP | 1 | 1 | 0 | 100% |
| IP | 14 | 14 | 0 | 100% |
| 計 | 221 | 197 | 24 | **89.1%** |

表 11 改良実施後の誤検知率

| プロトコル | 総数 | アラーム | | 誤検知率 |
|---|---|---|---|---|
| | | 攻撃 | 誤検知 | |
| HTTP/TCP | 187,092 | 531 | 389 | **0.2%** |
| SMTP/TCP | 13,968 | 3 | 98 | **0.7%** |
| FTP/TCP | 537 | 34 | 0 | 0% |
| DOMAIN/TCP | 85 | 1 | 0 | 0% |
| DOMAIN/UDP | 1,987 | 6 | 0 | **0%** |
| ICMP | 11,860 | 158 | 0 | 0% |
| 計 | 215,529 | 733 | 487 | **0.2%** |

## 7. まとめ

今回の評価では、誤検知率 1.2%という結果が得られ、検知率の評価で得た 89.6%という結果とあわせて、本方式では十分な精度で不正アクセスを検知することが可能であることを確認した。さらに、プロトコルチェックの条件を修正することによって、検知率を大きく下げることなく、誤検知率を 0.2%程度にまで下げることが可能となることを示した。

## 謝辞

本研究は、通信・放送機構（TAO）の委託研究テーマ「不正アクセス発信源追跡技術に関する研究開発」の一環として行われたものである。

## 参考文献

[1] 馬場，山岡，小久保，松田，“プロトコル仕様及びポリシー情報を利用した不正アクセス検知方式の検討”，情報処理学会第 60 回全国大会講演論文集（分冊 3），pp.285-286, March 2000.
[2] 馬場，小久保，松田，“不正アクセス検知のためのプロトコルチェック方式の検討”，情報処理学会第 61 回全国大会講演論文集（分冊 3），pp.257-258，October 2000.
[3] 馬場，鴨田，小久保，松田，“プロトコル仕様及びポリシー情報を利用した不正アクセス検知システムの実装と評価”，情報処理学会コンピュータセキュリティシンポジウム 2001（CSS2001）論文集，pp.173-178，October 2001.
[4] J. Postel, "INTERNET PROTOCOL", RFC 791, September 1981.
[5] J. Postel, "TRANSMISSION CONTROL PROTOCOL", RFC 793, September 1981.
[6] J. Postel, "User Datagram Protocol", RFC 768, August 1980.
[7] J. Postel, "INTERNET CONTROL MESSAGE PROTOCOL", RFC 792, September 1981.
[8] R. Fielding, etc. "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.
[9] J. Klensin, "Simple Mail Transfer Protocol", RFC 2821, April 2001.
[10] J. Postel and J. Reynolds, "FILE TRANSFER PROTOCOL (FTP) ", RFC 959, October 1985.
[11] P. Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", RFC 1035, November 1987.
[12] Whitehats, Inc., arachNIDS（advanced reference archive of current heuristics for network intrusion detection systems）, http://www.whitehats.com/ids/