4F-6

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

馬場 達也　　小久保 勝敏　　松田 栄之
（株）NTT データ　情報科学研究所
e-mail: {baba, kokubo, matu}@rd.nttdata.co.jp

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、あらゆ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きている。そこで著者らは、プロトコルの仕様とサイトのポリシー情報を利用して、インターネット側からの WWW サーバ等への不正アクセスを、未知の手法によるものも含めて検知する方式について提案している[1]。

本稿では、本検知方式におけるプロトコルのチェック方式について検討し、その有効性を示す。

2. 不正アクセス検知方式の概要

著者らが提案している不正アクセス検知方式では、プロトコルの仕様とサイトのポリシー情報によって正常なアクセスを定義しておくことにより、未知の手法を含む不正アクセスを検知することができる。

本検知方式の処理の流れを図 1 に示す。まず、監視対象のネットワーク上を流れるパケットを捕獲する。次に、捕獲したパケットの内容をプロトコルの階層毎（WWW アクセスの場合は、IP→TCP→HTTP の順番）にチェックする。不正と判断された場合には、その危険度をニューラルネットワークにより算出し、危険度が一定値以上であれば、電子メール等で検知結果を管理者に通知する。

3. プロトコルチェックの手順

本章では、不正アクセス検知処理の中で、IP[2]、TCP[3]、HTTP[4]のプロトコル仕様チェック及びプロトコルポリシーチェック（以下まとめてプロトコルチェックと言う）について説明する。

3.1. 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されるフィールドとそのチェック内容は表 1 の通りである。インターネットサーバへのアクセスでは、通常、IP のフラグメント分割は生じないため、ここでは、フラグメントしていない場合のみを正常として判断する。

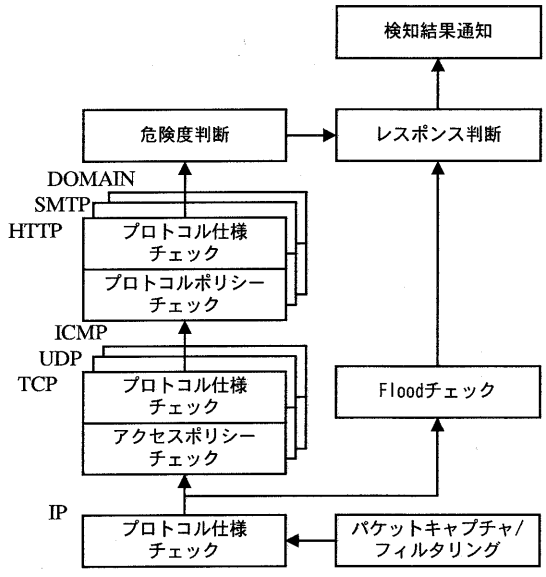

図 1 検知処理の流れ

また、IP オプションも通常は使用されないため、オプションの無い状態のみを正常として判断する。

表 1　IP ヘッダのチェック内容

フィールド名称	チェック条件
Version	4 であること
Internet Header Length	5 であること
Total Length	21～1500 の間であること
Flags（Reserved） Flags（MF） Fragment Offset	0 であること
Source Address	プライベートアドレスや内部使用グローバルアドレスでないこと
Destination Address	Source Address フィールドに設定されたアドレス以外であること

3.2. 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される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

フィールド名称	チェック条件
Source Port Destination Port	どちらか一方は 1024～65535 の間であること
Data Offset	5～15 の間であること
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
Urgent Pointer	0 であること

A study of protocol check method for intrusion detection
Tatsuya Baba, Katsutoshi Kokubo, Shigeyuki Matsuda
Laboratory for Information Technology
NTT DATA CORPORATION

3.3. 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される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

フィールド名称	チェック条件
Method	GET, PUT 等のコマンドが、あらかじめポリシーとして登録された、そのサイトで許可するコマンドであること
Request-URI	URL の内容が、あらかじめポリシーとして登録された、その WWW サーバで許可する URL であること。また、URL の長さがそのサイト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

4. プロトコルチェックの有効性の検証

本章では、実際の不正アクセスが本方式においてどのように検知されるかを具体的に示すことにより、本手法の有効性を示す。

4.1. 検証に使用する不正アクセス

不正アクセスは大きく以下の 4 種類に分類することができる。

(1) プロトコルの仕様に違反したアクセス
　(LAND Attack や Teardrop、UDP Bomb 等)
(2) 短時間に大量のアクセスを発生させる行為
　(TCP SYN Flood 等 Flood 系の不正アクセス)
(3) サイズの大きいデータを伴ったアクセス
　(バッファオーバーフロー系の不正アクセスや Ping of Death、Long URL Crash 等)
(4) 不正なコマンドや URL を使用したアクセス
　(SMTP DEBUG 攻撃やサンプル CGI 攻撃等)

これらの中から代表的な不正アクセスとして、LAND Attack、Long URL Crash、サンプル CGI 攻撃が発生した場合について以下で検証する。(2) の Flood 系の不正アクセスについては、図 1 の Flood チェック部で検知を行うため、本稿では説明を省略することとする。

4.2. LAND Attack

LAND Attack は、送信元 IP アドレスと宛先 IP アドレスが同じであり、かつ送信元ポート番号と宛先ポート番号が同じであるパケットを送信する不正アクセスである。

LAND Attack の場合は、送信元 IP アドレスと宛先 IP アドレスが同じであるため、IP プロトコルチェックの Destination Address フィールドのチェックにおいて不正であると判断することができる。

4.3. Long URL Crash

Long URL Crash は、異常に長い不正な URL を送信することによって WWW サーバをクラッシュさせる不正アクセスである。

Long URL Crash では、URL の長さが、そのサイトで許可する値を超えるため、HTTP プロトコルチェック部の Request-URL フィールドのチェックにおいて不正であると判断することができる。

4.4. サンプル CGI を悪用した不正アクセス

phf や campas 等の WWW サーバプログラムにサンプルとして付属している CGI プログラムを悪用する不正アクセスが存在する。

このような不正アクセスは、URL にそのサンプル CGI へのパスが含まれており、このようなパスを含む URL は、そのサイトでアクセスを許可する URL として登録されていない。このため、HTTP プロトコルチェック部の Request-URI フィールドのチェックにおいて不正であると判断することができる。

本方式は、プロトコルの仕様とサイトのポリシー情報によって正常なアクセスを定義することにより、不正アクセスを検知することを特徴としている。不正アクセスに関する特徴情報等は登録しないため、上述した不正アクセス以外であっても、未知の手法のものも含めて検知することが可能である。

5. まとめ

未知の手法による不正アクセスが発生した場合でも検知が可能な不正アクセス検知方式におけるプロトコルのチェック方式について検討し、その有効性を示した。今後は、この手法に基づいたプロトタイプを試作し、実機での評価を行う予定である。

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ているものである。

参考文献

[1] 馬場他, "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", 情処 60 全大講演論文集（3）, pp.285-286, March 2000.

[2] J. Postel, "Internet Protocol", RFC791, September 1981.

[3] J. Postel, "Transmission Control Protocol", RFC793, September 1981.

[4] R. Fielding, etc. "Hypertext Transfer Protocol -- HTTP/1.1", RFC2616, June 1999.