6Q-05 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

馬場 達也　山岡 正輝　小久保 勝敏　松田 栄之
（株）NTT データ　情報科学研究所
e-mail: {baba, yamaoka, 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[1]。

本稿では、特に 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未知の手法も含めて検知する手法について提案する。

2. 従来の不正アクセス検知技術

従来の不正アクセス検知技術は、シグネチャと呼ばれる不正アクセスの特徴情報をあらかじめ保持しておき、それを実際のアクセスと比較して一致した場合に不正アクセスとして検知する misuse detection 方式と、通常時のアクセスパターン（プロファイル）を保持し、それを実際のアクセスと比較して大きく異なる場合に不正アクセスとして検知する anomaly detection 方式の 2 種類に分類される[2]。

しかし、misuse detection 方式では、シグネチャとして登録されていない未知の不正アクセスは検知することができないという問題がある。また、anomaly detection 方式では、未知の手法も含めて検知することが可能であるが、プロファイルを実際のアクセスから取得するため、攻撃者に不正アクセスと判定されないようにプロファイルを操作されてしまう可能性がある[3]。また、プロファイルを取得するために事前にデータを収集する時間が必要となってしまい、導入後即座に利用するのは難しい。

3. 不正アクセス検知の考え方

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分類すると表 1 のようになる。

この分類より、不正アクセスは以下の 4 種類に分けることができる。この 4 種類の不正アクセスを検知できれば、これらの種類に分類される未知の不正アクセスもあわせて検知することが可能となる。

表 1　不正アクセスの被害とその手法

サービスへの被害	被害を引き起こす原因	不正アクセス手法
サービスのレスポンスタイムの増加	ネットワークが混雑/ホストの処理が超過	サイズの大きい IP パケットを短時間に大量に送りつける。
	サービスの処理が超過	大量のデータを送りつける。短時間に大量のアクセスを発生させる。
サービスの停止	システムダウン	プロトコルの仕様で想定されていない不正な値を入力して送信する。
情報の漏洩	システム内のファイルを取得された	サイズの大きいデータを送信し、バッファオーバーフローを発生させ、コマンドを実行する。CGI プログラム等にコマンドを引数として渡す。
偽情報の発信	システム内のファイルが書き換えられた	

(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）

3.1. プロトコルの仕様に違反したアクセス

仕様でプロトコル毎に決められている、パケットのフィールドの形式や含まれるべき値の範囲を「プロトコル仕様データ」として保持し、これに違反したアクセスを検知することで対処できる。

3.2. 短時間に大量のアクセスを発生させる行為

そのサイトで許可するアクセスの頻度を「アクセスポリシー」として記述し、これに違反したアクセスを検知することで対処できる。

また、「アクセスポリシー」にアクセスを許可する宛先 IP アドレス、送信元 IP アドレス及びプロトコルも記述しておくことで、外部からのアクセスを許可していないサービスへのアクセスも検知することができる。

A study of intrusion detection system based on network protocols and site access policy
Tatsuya Baba, Masaki Yamaoka, Katsutoshi Kokubo, Shigeyuki Matsuda
Laboratory for Information Technology
NTT DATA CORPORATION

3.3. サイズの大きいデータを伴ったアクセス

そのサイトで許可するデータの大きさやパラメータ（コマンドやURL）の長さを「プロトコルポリシー」として記述し、これに違反したアクセスを検知することで対処できる。

3.4. 不正なコマンドやURLを使用するアクセス

アプリケーションプロトコル毎に、そのサイトで許可するパラメータ(コマンドやURL)の内容を「プロトコルポリシー」に記述し、これに違反したアクセスを検知することで対処できる。

このように、正常なアクセスをプロトコルの仕様とサイトのポリシーとして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、実際のアクセスから取得するプロファイルを使用するよりも正確に検知することが可能となると考えられる。

4. 検知処理手順

本方式では、図1の手順で検知処理を行う。

4.1. パケットキャプチャ/フィルタリング

監視対象となるホスト宛のパケットのみを BPF (Berkley Packet Filter)等のパケットキャプチャプログラムによりネットワークから取得する。パケットから直接情報を取得するため、アクセス発生後、即座にチェック処理を開始することが可能となる。

4.2. プロトコル仕様チェック

プロトコル仕様チェックは、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「プロトコル仕様データ」と比較することにより行われる。この時、IPでフラグメントされている場合やTCPでセグメント分割されている場合には次プロトコルのチェックの前に再構成を行う。

4.3. アクセスポリシーチェック

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。

4.4. プロトコルポリシーチェック

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「プロトコルポリシー」で許可されているかどうかをチェックする。

4.5. Floodチェック

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。

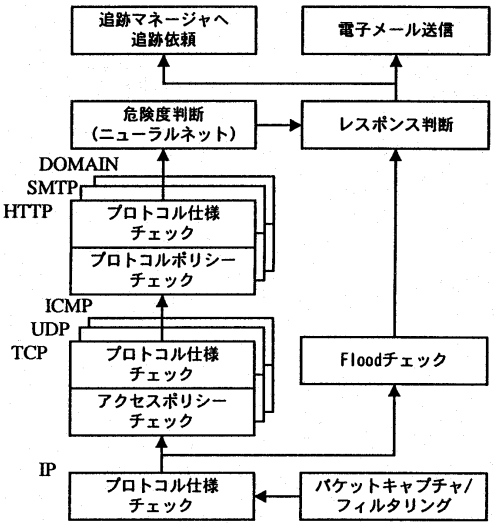

図1 検知処理の流れ

4.6. 危険度判断/レスポンス判断

以上の方式により、未知の手法を含む不正アクセスを検知することが可能となるが、それが実際にどの程度危険なものであるかは知ることができない。そのため、各チェック結果をあらかじめ学習されたニューラルネットワークに入力し、危険度を得る。

この危険度が一定値以上であれば、発信源の追跡を管理する追跡マネージャに対して追跡を依頼し、電子メール等で検知結果と追跡結果を通知する[1]。

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技術について提案した。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] 小久保他：不正アクセス発信源追跡システムのモデル検討，情処60全大，6Q-04，March 2000.

[2] B. Mukherjee, L.T. Heberlein, and K.N. Levitt. Network Intrusion Detection. *IEEE Network*, pp. 26-41, May/June 1994.

[3] P.A. Porras and P.G. Neumann. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In *Proceedings of the 20th National Information Systems Security Conference*, pp. 353-365, October 1997.