

藤井 誠司、大越 丈弘、河内 清人、勝山 光太郎

三菱電機(株) 情報技術総合研究所

1. はじめに

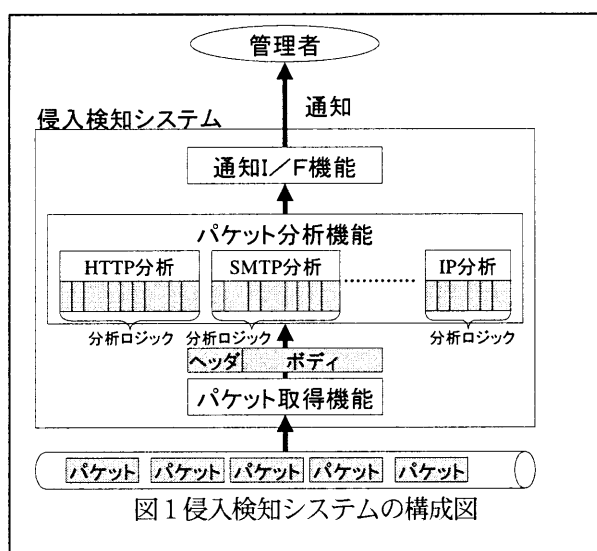
近年増加しているインターネットにおける組織内ネットワークへの不正侵入やシステムの破壊などの犯罪行為に対する対策技術のひとつとして、侵入検知システムがある。侵入検知システムもネットワークの高速化に対応すべく、より高速な検知性能が求められている。

現在、我々はネットワーク上を流れるパケットを監視するネットワーク型侵入検知システムを試作している。

本稿では、試作中の侵入検知システムの処理性能を調べるために、ネットワーク型侵入検知システムで最も処理時間がかかるパケット分析機能の検知性能の評価を行い、処理性能の低下にかかわる問題点について考察した結果について報告する。

2. 侵入検知システム

図1に、ネットワーク型侵入検知システムの構成を示す。



本システムは、ネットワークからパケットデータを取得し、パケットデータの再構築を行うパケット取得機能、取得したパケットデータが不正アクセスに関係するデータであるか否かを判別するパケット分析機能、パケット分析機能が不正アクセスを検知した場合管理者に通知する通知I/F機能から構成される。

パケット分析機能は、不正アクセスを分析する通信プ

ロトコルの種別で分類した分析機能を持ち、各通信プロトコル毎の分析機能は、不正アクセスに対する特徴をパターンマッチングによって分析する分析ロジックの集合で構成される。分析ロジックは分析する不正アクセスの種別によって処理時間が異なる。

分析対象のパケットデータがパケット分析機能へ渡されると、該当する通信プロトコルの分析機能へパケットデータが渡され、その通信プロトコル毎の分析機能は、包含するすべての分析ロジックを順番に実行し、そのデータが不正アクセスであるか否かの判別を行う。

3. 性能測定

開発中の侵入検知システムのパケット分析機能の不正アクセスデータの分析処理の性能を測定した。

3. 1. 測定方法

パケット分析機能は、DLLとして実現しており、パケット分析関数をコールすることで、パケットの分析を行う。測定では、開発中の侵入検知システムで検知する不正アクセスのデータを試験データとし、パケット分析関数に、そのデータを入力し、検知結果の出力を得る処理を20,000回ループし、その処理時間をmsec単位で測定した。評価指標として、単位時間当たりの処理速度(Mbps)を計算した。

入力されるデータは、パケット取得機能からの出力であり、単位時間当たりの処理速度の計算において、ネットワークからのパケット取得、フラグメントされたパケットの組み立て、メッセージの組み立て等の処理時間を含んでいない。また、処理したデータにはパケットのヘッダデータは含んでいない。

3. 2. 測定環境

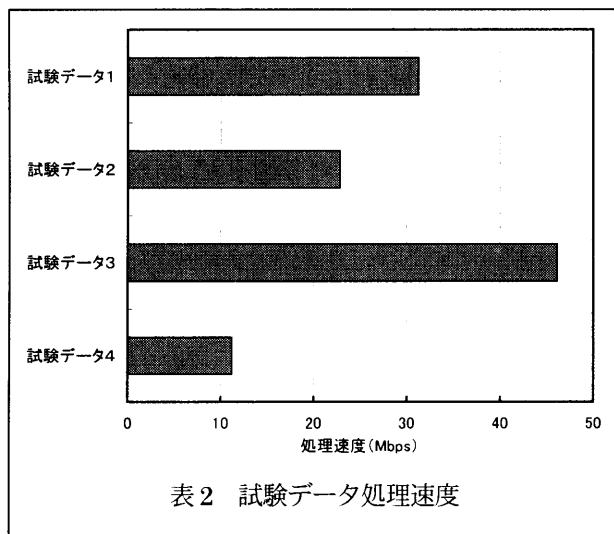
表1にパケット分析機能の処理性能の測定に使用した計算機の仕様を示す。

構成要素	仕様
CPU	PentiumIII 600MHz
RAM	128M バイト
OS	WinNT4.0 SP5

表1 評価に使用した計算機の仕様

3. 3. 測定結果

試験データの中から、特にパケット分析処理の遅かった4つの試験データについて、表2に測定結果を示す。



- 試験データ1: expn xxx...x (expn の後に128文字)
- 試験データ2: expn zzzzz
- 試験データ3: get yyy...y (get の後に1024文字)
- 試験データ4: get www...w (get の後に1023文字)

3. 4. 考察

評価結果は、特にパケット分析処理の遅かった試験データにおいても、10Base-Tの転送速度に比較して、十分な処理性能を実現していることが確認できる。ただし、より高速な転送速度のネットワークでは処理性能が不足していると考えられる。

●課題1：データ長の長いデータのパターンマッチング処理

本システムのパケット分析機能は、将来の不正アクセスの増加を考慮して、容易に分析ロジックを組み込むことができるように、分析ロジックで使用されるパターンマッチングの処理を共通関数化している。試験データ1、3および4のようなデータ長の長いデータでは、データの中から任意のデータを検索するためには、同じ検索パターンで、繰り返し、パターンマッチング処理を行うことが必要となり、性能を低下させている。

●課題2：分析ロジックの実行順序

試験データ2はパターンマッチング処理の頻度が低いにもかかわらず、他の試験データよりも処理速度が低下している。これは、分析ロジックの実行順序が影響している。試験データ1、2は同じSMTPのEXPNコマンドに関する不正アクセスのデータであるが、試験データ1の分

析ロジックが試験データ2の分析ロジックより先に実行されるため、試験データ2の処理が遅くなっている。試験データ4が試験データ3とほぼ同じデータ長に関わらず、処理性能が遅い原因も同様である。

4. 高速化の手法の検討

分析ロジックの容易な拡張性を実現しつつ、上記のような課題を解決するために、以下のような手法が考えられる。

(1) 並列処理によるパターンマッチング処理の高速化

不正アクセスのパターンマッチング処理はデータ更新処理を含まない検索処理であることから、パターンマッチング処理ヘスレッドを割り当て、複数のスレッドを並列に処理することにより、パターンマッチング処理のスループットを向上させる。

(2) 不正アクセスの検知回数に基づく分析ロジックの動的な配置

検知回数の高い不正アクセスの分析ロジックが検知回数の低い不正アクセスの分析ロジックより後に実行されることによる分析性能の低下が問題となる。そこで、実行される順序で並ぶ分析ロジックの関数へのポインタとその分析ロジックの不正アクセスの検知回数を保持するテーブルを持つ。検知回数は分析ロジックで不正アクセスを検知する毎にインクリメントされる。そして、一定間隔毎に、検知回数の高い順に、分析ロジックの関数へのポインタを動的に再配置する。これにより、検知回数の高い分析ロジックが優先的に実行される。

5. おわりに

本稿では、試作中のネットワーク型侵入検知システムのパケット分析機能の検知性能の評価を行い、処理性能の低下にかかわる問題点について考察した。今後は、解決策を実現した侵入検知システムを試作し、その有効性の評価を実施する。

6. 参考文献

- [1] W. Richard Stevens, "TCP/IP Illustrated, Volume1 The Protocols", Addison-Wesley Publishing Company, 1994.