不正パケット遮断システムのユーザインタフェース開発

04T215 岡原 聖 （最所研究室）

不正パケットが検出されると L2 スイッチあるいは Firewall で自動遮断し、問題が解決されれば自動解除するシステムの開発を行っている。本研究では、不正パケットを発する不正なホストを特定し、管理者の判断で手動遮断・手動解除を行うためのユーザインタフェースの開発を行う。

1 はじめに

インターネットの普及に伴い、十分な知識のないユーザの利用が増えている。そのため、コンピュータウィルスに感染していても、意図せずに個人情報を流出させる事例が増加している。また、悪意のあるユーザによる攻撃も問題となっている。このような問題の対策として、不正パケットを遮断するシステムを提案している。[1]、[2]

本システムは、侵入検知システム (IDS) が検知した情報をもとに処理レベルを決定するポリシ機能 [3]、ポリシ機能の命令をもとに自動遮断・自動解除を行う制御ツール [4]、管理者の判断で手動遮断・手動解除を行うユーザインタフェースから構成される。

システムは、IDS が不正パケットを検知した後、ポリシ機能が不正パケットを流したホストへの処理レベルを決定し、制御ツールがポリシ機能の処理レベルに基づいて遮断を行うものである。本研究では、管理者の判断で手動遮断･手動解除を行うユーザインタフェースの開発を行う。

2 ユーザインタフェースの設計

本システムでのユーザインタフェースは、ポリシ機能で判断できない不正パケットを IDS が検知した場合、管理者の判断で遮断を行うためのインタフェースを実装する。実装する上での設計方針、必要な機能について説明する。

2.1 設計方針

本ユーザインタフェースの設計方針について述べる。

- ユーザビリティ
  ユーザビリティ[5] とは「学習しやすさ」「効率性」「記憶しやすさ」「間違えにくさ」「主観的満足度」の 5 項目から構成されるソフトウェア、Web サイトなどの使いやすさの指標である。ユーザビリティを考慮して設計することで、システムの操作性、快適性などを向上させることができる。具体的には、手動遮断・手動解除を行う時に必要な情報をインタフェースに表示させる際に、ユーザビリティを考慮して開発を行う。

- ユーザ分析
  ユーザのスキルレベルに応じて、提供するインタフェースは異なる。本インタフェースのユーザは、管理者であると仮定している。管理者は、比較的スキルの高い人物と定義している。

- 対策事項
  Web アプリケーションへの攻撃の対策を行う必要がある。攻撃の一例として SQL インジェクションがある。SQL インジェクションとは、データベースと通信を行う入力フォームで不正な SQL コマンドを実行し、データベースの内容を取得される攻撃である。これを防ぐために、入力フォームで使用可能な文字を、半角英数字とメールアドレスに使用する特殊文字のみに制限する。

2.2 機能

本システムに必要な機能について述べる。

- 情報の取得
  Firewall での遮断を行う場合、ポリシ機能から受け取った IP アドレスから、MAC アドレスを取得する。L2 スイッチでの遮断の場合、さらに不正ホストの接続ポートを取得する。

- 不正パケットの遮断
  L2 スイッチでの遮断と Firewall での遮断がある。遮断に必要な情報は、情報の取得機能で得られており、その情報を用いて遮断を行う。

- 遮断の解除
  パケット遮断機能で遮断されたホストの遮断を解除するための機能である。

本研究では、Linux マシン上で動作するパケットフィルタリングをもつ Firewall と、ポートフィルタリングの可能な Allied Telesis 社の L2 スイッチである CentreCOM GS908M を使用した。

3 ユーザインタフェースの実装

各機能は PHP を用いて実装した。

- 情報の取得
  ポリシ機能から受け取った不正ホストの IP アドレスをキーとして、ルータから対応する MAC アドレスを取得する。L2 スイッチでの遮断の場合には、取得した MAC アドレスから不正ホストが接続している L2 スイッチの接続ポートを取得する。Firewall での遮断の場合には、IP アドレスのみで遮断可能であるが、IP アドレスは変化することがあるため、MAC アドレスで不正ホストの特定を行う。

- 不正パケットの遮断

  L2 スイッチでの遮断
  L2 スイッチでの遮断は、情報の取得で得られた、MAC アドレス、スイッチポートを用いてコマンドを生成する。L2 スイッチに Telnet で接続し、生成したコマンドを実行して、L2 スイッチのフィルタリング機能の設定を変更することで遮断を実現する。L2 スイッチでの遮断を行った場合、FDB から MAC アドレスが消えてしまうため、不正者データベースに遮断者情報を登録しておく。この情報は解除の時に用いる。遮断結果を図 1 に示す。なお、この図は L2 スイッチでの解除の結果も示している。

  Firewall での遮断
  Firewall での遮断は、情報の取得で得た IP アドレス、MAC アドレスを用いて、フィルタリングルールを作成し、Firewall に接続して、実行する。ブラウザ上から Firewall を更新する場合、apache ユーザ権限のため Firewall を更新できない。そのため、管理者権限でコマンドを実行出来るようにした。遮断結果を図 2 に示す。

- 遮断の解除
  遮断の解除は、基本的に各遮断と同様の処理を行うが、実行するコマンドが解除の為のものとなっている。コマンド生成時には、遮断時に登録した不正者データベースの内容などをインタフェース上に表示し、その内容を基にしてコマンドを生成し、遮断の解除を行う。

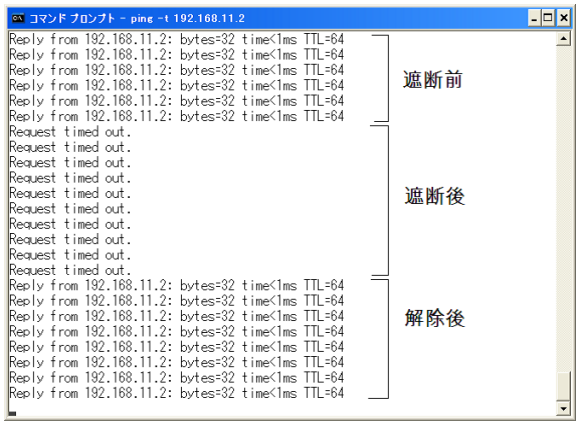

図 1: L2 スイッチでの遮断・解除結果

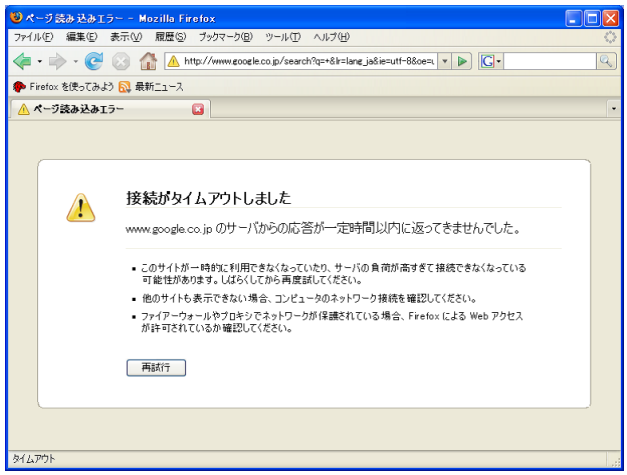

図 2: Firewall での遮断結果

4 今後の課題

システム全体の結合テストが十分ではないため、結合テストを十分に行う必要がある。また、本研究では必要機能の開発を行っただけにすぎず、インタフェースとしての評価が行われていない。様々なユーザに評価してもらうことや、機能の追加や不必要な機能の削除などのインタフェースの調整が必要である

参考文献

[1] 長野一樹, “不正パケット遮断システムのユーザインタフェースに関する研究”, 香川大学大学院工学研究科修士論文, 2006 年.

[2] 串間竜治, “L2 スイッチを用いた不正パケット遮断システムの研究”, 香川大学大学院工学研究科修士論文, 2006 年.

[3] 高橋巧, “組織内における不正パケット遮断システムの運用ポリシ設計および実装”, 香川大学大学院工学研究科修士論文, 2007 年.

[4] 原田知拡, “不正パケット遮断システムにおける自動制御ツールの開発”, 香川大学工学部卒業論文, 2007 年.

[5] Jakob Nielsen, “ユーザビリティエンジニアリング原論 - ユーザーのためのインタフェースデザイン”, トッパン社, 1999 年.