

ネットワークセキュリティ管理のための ネットワーク可視化システムの実装

幅野莞佑 *

黒米祐馬 †

武田圭史 ‡

村井純 ‡

January 13, 2017

1 序論

近年, 技術の進歩によって, ネットワークはより身近なものになっている. サーバを手元に持たなくともその運用に携わるユーザが増加傾向にある. しかし, それに伴ってセキュリティの知識が十分に持っていない人の管理するサーバが存在するようになっている. サーバのセキュリティを保つには, ファイアウォールの設定が重要である. ファイアウォールは設定ファイルにあるルールに従って通信しようとするパケットを遮断できるが, その挙動を確認する手段などは備わっていない. ファイアウォールの挙動やルール, そしてネットワークの状況などを把握するには管理者がネットワークについてある程度の知識をもっている必要がある.

2 提案手法

本研究ではネットワークの知識を十分に持っていない個人サーバ管理者に対して, ネットワークとファイアウォールの挙動をリアルタイムで確認し, 状況の理解を支援する可視化システムを提案する. 現状, ネットワークやファイアウォールの状況を確認する方法としては設定ファイルやパケット情報, ログ・ファイルなどの文字形式の情報で確認することが挙げられる. その情報を文字ではわかりにくかった通信の状況や, ファイアウォールの挙動を同時に確認することができる.

3 実装

本システムはパケットキャプチャプログラムと, 可視化プログラムから構成される. パケットキャプチャプログラムは監視対象のサーバでパケットを分析し, 可視化プログラムはクライアントとしてパケットの分析結果を取得, 3D 描画する.

3.1 パケットキャプチャプログラム

表 3.1: パケットキャプチャの実装環境

要素	環境
OS	Ubuntu 14.04
言語	C
コンパイラ	gcc version 4.8.4
ライブラリ	libpcap version 1.5.3 mysql version 5.5.53 netstat 1.42[1]
ファイアウォール	iptables version 1.4.21[2]

このプログラムで実装するプロセスを以下に述べる.

1. パケットのデータ収集
2. 収集したパケットの必要なヘッダデータの抽出
3. netstat コマンドによりポートの状況を取得
4. iptables の設定ファイル, ログファイルを取得
5. データを可視化プログラムに取得した各データをソケットで送信

パケットのデータ収集には libpcap ライブラリを用いた. 取得する情報は送信元 IP アドレス, 送信先 IP アドレス, 送信元ポート番号, 送信先ポート番号, プロトコル, TCP フラグ情報の 6 つである. これらの情報をリアルタイムでソケットで送信する. ここで, 送信相手のアドレス毎にデータベースで通信回数などの状況を管理する. また, 通信回数が多くなった場合, 可視化プログラムに負荷をかけないようデータベースにある情報を一定時間ごとに取得して送信するようにする. そして一定時間で通信回数でソートされた IP アドレスのリストを送信する.

iptables は設定ファイルから filter テーブルを参照し, パケットのフィルタ基準を取得する. このとき, 本システムは設定ファイルの変更があれば取得して, 送信する. また, iptables がドロップしたパケット情報などをログファイルから取得することによってパケットをドロップする挙動を可視化することが可能になる.

*慶應義塾大学 総合政策学部

†慶應義塾大学 環境情報学部

‡慶應義塾大学

