機器情報を用いたネットワーク管理システムの構築

07T2580　平川 健一 （最所研究室）

本研究では，管理者が機器情報を用いることで，特定のユーザの通信を時間や場所，予約の条件に基づいて柔軟に制御できるシステムを提案し，基本機能の設計や実装，および評価について述べる．

1　はじめに

ネットワークインフラの充実により，あらゆる場所でいつでもインターネットの利用が可能となった．このような環境においては，本来行うべき作業があるにもかかわらず，関係のないネットワークアクセスをつい行ってしまい，滞りを生じさせる可能性が高い．また，セキュリティの関係で一時的に特定のネットワーク以外にアクセスしてはならない状況が発生することもある．しかしながら，管理者がユーザのインターネット使用を常に監視し続けるのは困難である．本研究室では不正パケット遮断システム [1] を開発しているが，不正パケットを発した通信機器の自動遮断にのみ対応しており，任意に対象を時間や場所を指定しての遮断および解除はできない．

本研究では，本研究室で開発されている機器管理システム [2] を用いて，管理者が特定のユーザの通信をより簡単に制御出来るシステムを提案する．本システムは時間と範囲，そして予約の概念に基づいて，対象の通信機器を Firewall や L2 スイッチを用いて自動的に遮断または解除を行う．本稿では，提案するシステムに必要な機能の設計と実装について述べる．

2　概要

本システムの構成を図 1 に示す．Web インターフェス上で認証を行った管理者が，遮断する対象と日時や場所を指定し予約を行う．予約内容は DB に保存される．予約時間の条件を満たした場合に，現在接続されている通信機器の中から遮断対象の判別を行う． 条件に沿う通信機器は，Firewall や L2 スイッチを用いて遮断される．条件に沿う通信機器が複数であっても制御も可能である．本研究で提案するネットワーク管理システムに必要な機能は以下の通りである．

- 接続者を常時把握する機能
  接続している通信機器の情報を常に監視する．
- 管理者が指定した対象機器を判断する機能
  管理者が予約で行った遮断対象の機器を接続状況から判別する．
- 通信を自動で遮断または解除する機能
  遮断対象の機器情報から，Firewall あるいは L2 イッチを用いて自動で遮断または解除を行う．

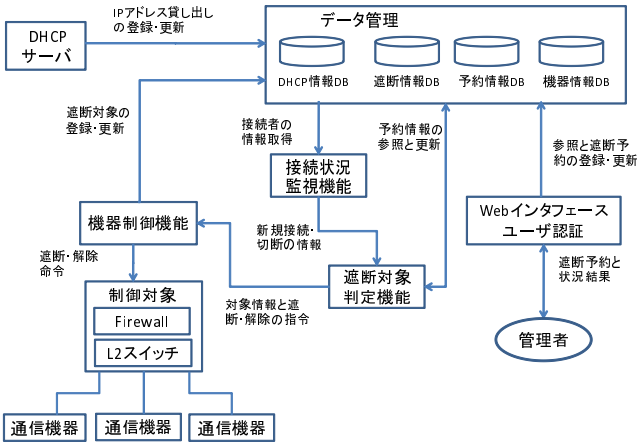

図 1: ネットワーク管理システムの構成

3　システムの各機能設計

3.1　接続状況把握機能

DHCP サーバが IP アドレスの貸し出し状況を記したログより，IP アドレス毎の貸し出し開始および終了時間や MAC アドレスなどの情報を取得し DB に登録する．一定時間毎にログの精査をすることにより最新の状態に保つ．遮断予約条件によっては新規貸し出しまたは更新された IP アドレスが遮断対象となる可能性がある為，遮断対象の判定を行うよう遮断対象判定機能へ問い合わせを行う．

3.2　遮断対象判定機能

予約開始および終了時間や遮断条件から，接続中のどの通信機器が適合するかを判定し，遮断の命令を制御機能に伝える．予約開始時間に達すると，現在の接続状況を登録した DHCP 情報 DB と機器情報 DB に対して，管理者が指定した条件に適合する接続状態の

IP アドレスや MAC アドレスを参照し，接続されている通信機器に該当するものがあれば，Firewall や L2 スイッチで遮断を行うためにその情報を機器制御機能へ送る．

遮断解除時間を過ぎた場合，機器制御機能から遮断情報 DB に登録された内容を参照し，遮断を行った IP アドレスや MAC アドレスの情報を送信する．

3.3 機器制御機能

遮断対象判定機能から得られた通信機器の IP アドレスや MAC アドレスを用いて，Firewall もしくは L2 スイッチによる通信機器の制御を行う．

- Firewall の遮断および解除

  得られた遮断対象の IP アドレスよりフィルタリングルールを作成し，シェルスクリプトとして登録を行い，チェインリストに追加を行う．解除の場合は同じフィルタリングルールをシェルスクリプト内から削除し，Firewall を再起動させることで対象のフィルタリングルールが存在しないチェインリストが読み込まれ，解除が行われる．

- L2 スイッチの遮断および解除

  遮断対象となる通信機器の MAC アドレスより，L2 スイッチに接続されているポート番号を SNMP を用いて検索する．該当するポートに対してフィルタリングの機能の設定を変更することで遮断を行う．遮断を行った MAC アドレスとポート番号を遮断完了情報として DB に格納する．解除の場合は，遮断完了情報より対象の接続ポートのフィルタリング設定を元に戻すことで，遮断対象の通信を可能にする．

4 実装と評価

機能設計で述べた機能を実装し，複数の通信機器を一定時間遮断する予約を用いて動作実験を行った．予約設定画面を図 2，対象となる各機器の ping による通信結果を図 3 および 4 に示す．この結果より，対象となる指定された開始時刻より複数の機器の遮断が行われ，設定された終了時間を過ぎると自動的に解除されていることが確認できる．

5 まとめ

接続状況から対象となる通信機器を把握し，時間や場所を指定して複数の機器を遮断可能なシステムを提案した．提案したシステムの基本の設計を行い，予約機能が正常に動作し，複数の機器を自動で遮断および解除が行えることを確認した．

今後の課題として，接続状況や遮断および解除の一定時間毎の判定方法を，接続状況の変化毎に判定するイベントドリブン型に変更することや，IP アドレス

図 2: 予約内容

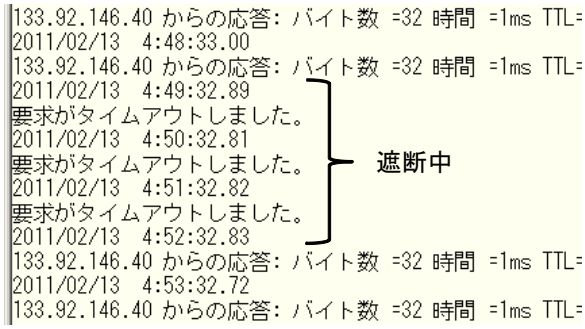

図 3: 所有者 ID:s07t258 の通信結果

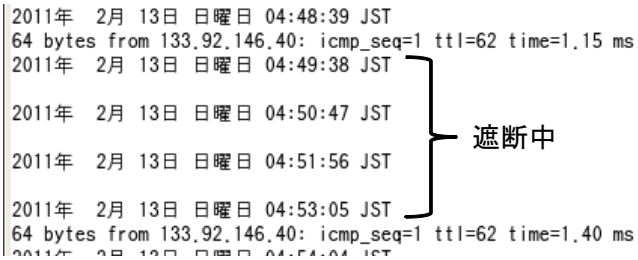

図 4: 所有者 ID:testc の通信結果

の範囲のみではなく，ユーザ単位での範囲や，適切に IP アドレスの割り振りが行われていない場合の遮断範囲指定方法の設計，遮断対象例外設定の管理方法，そして所有者 ID 以外を用いた，より柔軟な条件による遮断予約方法の実現などが挙げられる．

参考文献

[1] 原田和拡，“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，学士論文，2008.

[2] 宮崎貴充，“ネットワーク機器管理システムの開発”，香川大学工学部，学士論文，2010.