# 機器および時間・場所を用いたネットワーク制御システムの開発

11G484 平川 健一　(最所研究室)

本稿では，管理者が機器情報や講義情報を用いることで，特定のユーザの通信を時間や場所などの条件に基づいて，自動的にアクセス制御できるシステムを提案し，必要な機能の設計と実装について述べる．

## 1. はじめに

近年，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り，利便性が向上している．

その反面，関係のないネットワークアクセスを行うことで，本来行うべき作業に滞りを生じさせる場合がある．また，セキュリティの関係で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一時的に発生することもある．しかしながら，ネットワーク管理者がユーザのネットワーク使用を監視し続けるのは困難である

このような問題を解決するために，対象や場所・時間を考慮したネットワーク管理を行うシステムの開発を行っている[1]．本研究ではこのシステムをベースにして，大学構内ネットワークを対象としたネットワークアクセス制御システムの開発を行う．本稿では，講義中にて，対象となる通信機器を Firewall や L2 スイッチ，侵入検知システム(IDS)を用い，通信機器に付随する情報や時間・場所に応じて自動的にアクセス制御を行うシステムを提案および，必要な機能と実装について述べる．

## 2. ネットワーク制御システムの概要

本システムの構成を図 1 に示す．本システムでは，教務システムなどの外部システムにあらかじめ登録されている情報を用いることで，学内における講義と連動し，時間や講義室，学生などの身分応じて柔軟な通信制御を可能にする．適用例として，講義の管理者である先生は受講者である学生の通信のみを制限するものがある．対象となりうる通信機器の情報は機器管理システム[2]より得る．講義科目に関する情報は教務システムを想定したシステム上に構築している．この 2 つのシステムと連携を行いつつ，接続状況を DHCP サーバより得ることで自動的な通信制御を可能にする．担当者である先生は Web インタフェースを用いて接続中の通信機器の情報を確認することや，個別に通信制御を行うことが可能である．接続者の把握や通信制御の実施および管理などは，制御・管理部の各機能にて行う．

## 3. 各機能の設計

### 接続状況監視機能

特定のユーザのネットワークアクセスを自動的に

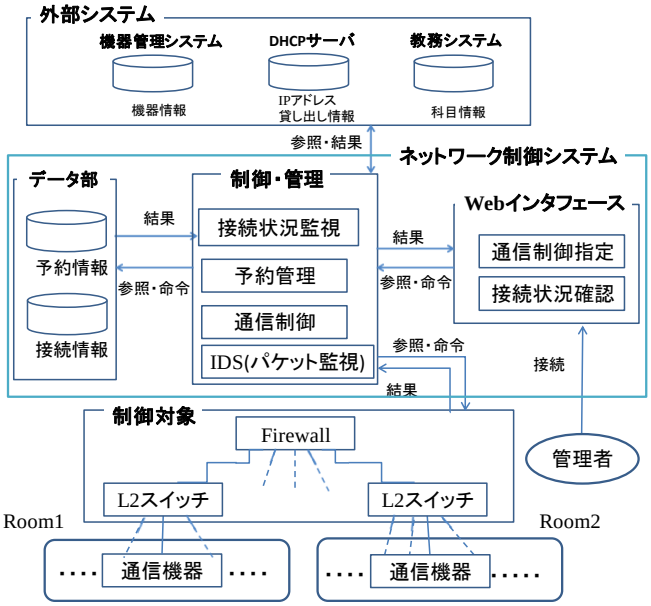


図 1 ネットワーク制御システムの構成

制限するためには，ネットワーク全体の接続状況を常に監視し，対象となりえるユーザの接続状況を把握し続ける必要がある．外部システムの DHCP サーバから得られるログを定期的に精査し，接続中の通信機器の状況を把握する また L2 スイッチの ARP テーブルより得られた IP アドレスと MAC アドレスの対を収集し，L2 スイッチのフォワーディングテーブル(FDB)より得られる MAC アドレスと接続ポート番号の対を SNMP を用いて調べることで，通信機器の接続情報を補完する．この接続情報と機器管理システムより得られる MAC アドレスに紐付けられたユーザ情報を精査することで，ネットワーク接続者を把握することができる．

### 予約管理機能

本機能では，周期的に制御対象となる通信機器の情報や講義情報から通信制御条件を判断し，必要であれば生成し，通信制御機能に命令を行う．通信制御条件は，通信制御を行うための条件であり，機器情報や講義科目，通信制御時間，利用する制御機器の情報を含む．機器管理システムより得られる機器機器およびそのユーザ情報を利用することで，講義履修者の判断や，先生や学生などといったユーザの身分に応じた通信制御条件の設定が可能となっている．

### パケット監視機能

管理者が管理下にある利用者を特定のアクセス先のみに接続を許可させたい場合，その都度指定するアクセス先を設定することは困難である．このため管理者のアクセス先を自動的に把握し，その情報を元にした制御を行う機能を用意する．本機能では IDS に担当者のアクセス先を監視するルールを設定し，アクセス情報を収集することで，管理下にある利用者に対してアクセス許可を行う通信制御条件の自動生成を行う．

### 通信制御機能

予約管理機能より送られてきた通信制御条件に含まれる通信機器や制御内容の情報を用いて Firewall もしくは L2 スイッチによる通信機器の制御を行う．

- **Firewall による通信制御**
  得られた遮断対象の IP アドレスや制御内容よりフィルタリングルールを作成し，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の解除を行う．
- **L2 スイッチによる通信制御**
  L2 スイッチに対して，遮断対象となる通信機器の MAC アドレスをフォワードしないように設定することで遮断を行う．解除の場合，他に制御する通信機器がない場合はフィルタリング設定を元に戻し，ある場合は MAC アドレスを再登録する．

## 4. 評価

教務システムおよび機器管理システムに講義情報やユーザ情報を登録し，複数の通信機器を用いて動作実験を行った．その結果，接続中の通信機器と付随するユーザ情報を Web インタフェース上で確認できた．それぞれの通信機器に対して身分に沿った通信制御が自動で行われていることを確認した．図 2 は 5 分間の講義を設定した時の例である．

次に接続人数が Firewall の通信制御条件生成の処理時間および CPU 使用率にどのように影響するか調査した．図 3 は接続人数に対する処理時間の変化である．結果として，処理時間は接続人数に比例して増加することが判った．その中で処理条件の生成からスクリプトの書き込みまでが大半を占めており，制御条件の適用にはそれほどかからなかった．現在の制御条件の監視間隔が 1 分毎であるが，結果より接続する機器が増加した場合に処理が追いつかない可能性が判明した．実験中のサーバマシンの CPU 使用率は平均して 97.3%であったことより，サーバの処理能力の向上や機能の分散化により処理時間を軽減することが可能である．それ以外の対応策としては，接続数に応じて動的に監視間隔を変更する方法が挙げられる．

```
guest 2013/02/05 20:49  133.92.147.224  successful
guest 2013/02/05 20:50  133.92.147.224  successful
guest 2013/02/05 20:51  133.92.147.224  timeout
guest 2013/02/05 20:52  133.92.147.224  timeout
guest 2013/02/05 20:53  133.92.147.224  timeout
guest 2013/02/05 20:54  133.92.147.224  timeout
guest 2013/02/05 20:55  133.92.147.224  timeout
guest 2013/02/05 20:56  133.92.147.224  successful
```

制御中

図 2 自動制御実行例

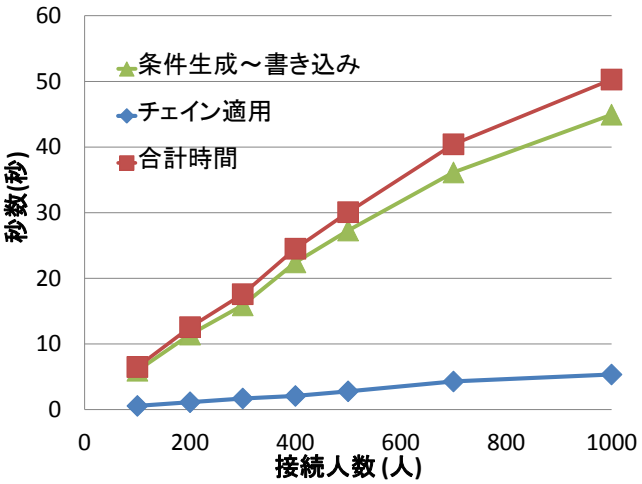


図 3 通信制御条件生成から適用までの処理時間

## 5. まとめと今後の課題

機器情報や講義情報を用い，対象や時間・場所に応じて複数の通信機器のネットワークアクセスを自動で制御するシステムを提案し，設計と実装，および Firewall での制御実行の性能評価を行った．その結果，実装した機能は正しく動作しており，1000 人程度の接続状況であれば 1 分間隔で制御可能であることが判った．本システムにおける今後の課題としては，通信制御条件の例外管理，動的な監視周期の実現，IDS を用いた監視機能の改良，講義外の状況への対応などが挙げられる．

### 参考文献


[1] 平川健一,最所圭三, “機器情報を用いたネットワーク管理システムの構築”,平成 23 年度電気関係学会四国支部連合大会論文集, 16-30, p.317, 2011

[2] 宮崎貴充,最所圭三,“ネットワーク機器情報管理システムにおける登録支援機能の開発”,平成 23 年度電気関係学会四国支部連合大会論文集, 16-30, p.317, 2011