4S-06

講義室内ネットワークスイッチを利用したアクセス制御システム

衛藤　雄平†　　神屋　郁子‡　　下川　俊彦‡
†九州産業大学大学院情報科学研究科　　‡九州産業大学情報科学部

1　はじめに

近年, 学校施設でネットワークを利用できる教室が増加している. それに伴い講義でネットワークを利用する機会も増加している. 講義中自由にネットワーク利用ができるため, 講義とは無関係のネットワークアクセスを行う学生がいる. 例えば, 動画サイト, SNS サイトへのアクセスやトークアプリの使用などである. このようなネットワークアクセスを制御するために, フィルタリングを用いることが多い.

フィルタリングを行うには専門知識が必要になる. 例えば, ネットワークスイッチでアクセス制御を行うには, スイッチのコマンドや IP アドレス, ポート番号の知識が必要である. したがって, 専門知識がない教員にはフィルタリングを行うことは難しい. 一方, 専門知識がある教員でも, 実際にフィルタリングを行うには作業工数が多く手間がかかる. さらに, 講義内容や進行によって制限したい内容が異なるため, その場合に応じて適切にネットワークアクセス制御する必要がある.

そこで本研究では, 教員が自身の講義中, フィルタリングの制限内容を柔軟に切替えることができる仕組みを提案する.

2　講義室内ネットワークスイッチを利用したアクセス制御システム

2.1　システムの概要

本システムは, 講義とは無関係のネットワークアクセスを制限するため, 講義中に教員が任意のタイミングでアクセス制御を行うことができるシステムである. 例えば, ある講義においては自由にネットワークアクセスが可能, 同じ教室で次の時間に開講される講義では, ある時間帯は全ての通信を遮断し, それ以外の時間帯は特定のネットワーク範囲のみアクセスを許可するというアクセス制御の設定の切り替えを講義中に実現可能である.

教員はシステムを用いてアクセス制御の設定を行う. システムがネットワークスイッチと通信し, アクセス制御の設定を行うため, 教員はネットワークスイッチの操作を直接行う必要がない.

具体的なアクセス制御を行うためには, ネットワークスイッチに, アクセスリストを登録する必要がある. アクセスリストを作成するためには, 専門知識が必要となる. そこで, 予め利用者から要望を聞き, 事前にアクセスリストを本システムに登録しておく. アクセスリストには以下の 4 つのような動作をするものがある. 1) 全ての通信を許可, 2) 全ての通信を遮断, 3) 九州産業大学内のみ許可, 4) 情報科学部内のみ許可.

本システムでは, 利用者を管理者と一般ユーザに権限をわける. アクセスリストを登録可能なのは管理者のみである. 専門知識を持つ人を管理者, 講義担当教員を一般ユーザとする. 一般ユーザは管理者が登録したアクセスリストを選択し利用する. これにより, 専門知識がない教員でも自身が担当する講義室へのアクセス制御が可能となる.

2.2　アクセス制御手法

本システムではネットワークスイッチを用いてアクセス制御を行う. 近年の高性能なネットワークスイッチではフィルタリング機能を持ったものが多く, MAC アドレス, IP アドレス, ポート番号を用いたアクセス制御が可能である. ネットワークスイッチを用いることにより, 大学内ネットワークでは, 既存の機器を利用しアクセス制御を行うことができる. そのため, 新規の機器を導入する必要がない.

2.3　システムの設計

本システムは図 1 のような構成になっている. 教員は Web ブラウザを用いて本システムを利用する. 教員の操作画面については 2.3.2 で説明する.

2.1 で述べたように, 本システムでは利用者を管理者と一般ユーザで権限をわける. それぞれの機能について以下で説明する.

2.3.1　管理者機能

管理者機能では, アクセスリスト, ユーザ管理, 各教員が担当する講義の登録, 編集, 削除を行うことができる. アクセスリストは, 優先度を指定する順序番号, 送信

Development of an Access Control System using Network Switch in a Class Room
†Yuhei ETO　‡Yuko KAMIYA　‡Toshihiko SHIMOKAWA
†Graduate School of Information Science, Kyushu Sangyo University Unified Graduate School
‡Faculty of Information Science, Kyushu Sangyo University

Copyright ©2016 Information Processing Society of Japan.
All Rights Reserved.

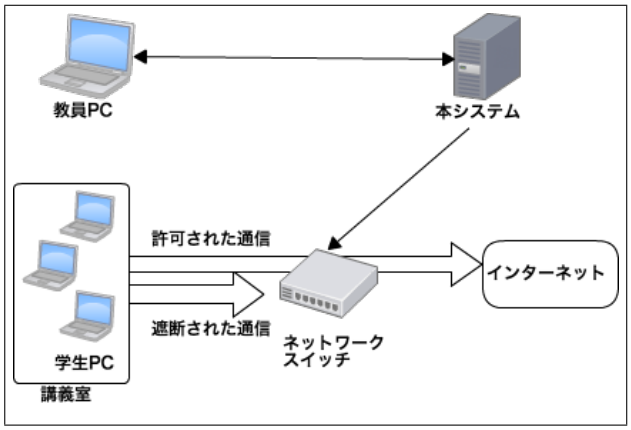

図 1: システム構成図

図 2: 教員の操作画面

元の IP アドレスとワイルドカードマスク, 送信先の IP アドレスとワイルドカードマスク, TCP/UDP のプロトコル指定, 指定したプロトコルのポート番号, 許可/拒否の動作で構成される. なお, プロトコル, ポート番号は省略可能である. プロトコルを省略した場合, TCP/UDP の双方のパケットが対象となる. ポート番号を省略した場合, ポート番号を無視して判定する. また, 各教員の担当する講義は, 講義名, 教室, 開講時期, 曜日, 時限で構成される.

2.3.2 一般ユーザ機能

一般ユーザ機能の主要な機能は以下の 2 つである. a) アクセスリストを即時に切り替える, b) アクセスリストを指定した時間に自動的に切り替える.

a) は, 教員の操作画面 (図 2) から使用できる. 通常, この画面では各教員の担当する講義一覧が表示される. 各教員の担当講義の時間帯の場合, その講義に関する情報が画面上部に LIVE 情報として表示される. LIVE 情報の中にアクセスリストの動作が書かれたボタンがあり, このボタンを押すことで即時にアクセスリストを切り替えることができる.

b) は, 講義が始まる前に必要な情報をあらかじめシステムに登録しておくことで使用できる. 登録は教員の操作画面 (図 2) の各講義名のリンク先から行うことができる. 登録に必要な情報は, 適用したいアクセスリスト, 講義の日付, 時間から構成される. 登録した日時になると自動的にアクセスリストが切り替わる. また, 複数の日付をまとめて同じ内容で登録できる. その場合, 追加で終了日を入力する必要がある. 日付から終了日までの期間, 講義が行われる曜日で毎週同じ内容が登録される.

アクセスリストのデフォルト状態は「全ての通信を許可」である. 講義終了時間になると, デフォルト状態のアクセスリストが適用される.

2.4 システムの実装

本研究では, 九州産業大学情報科学部のネットワーク上に提案システムを実装した. 情報科学部では ALAXALA 社のネットワーク機器が使われているため, AX-ON-API[1] という NETCONF プロトコルをベースにしたネットワーク機器制御ツールキットを使用した. これにより, ネットワーク機器の構成設定, 状態の管理等の操作を Java のクラスライブラリとして利用でき, アクセスリストの設定をすぐに反映させることが可能である.

3 おわりに

教員が自身の講義中, フィルタリングに用いるアクセスリストを講義内容や進行に応じて柔軟に切替えることができるシステムを開発した. Web ブラウザからメニュー選択でネットワークスイッチの設定を行うことができ, 知識のない教員でも扱えるシステムを実現した. また, 九州産業大学情報科学部のネットワーク上に提案システムを実装し動作確認を行った.

今後として, 提案システムの使いやすさの評価および改善を行う.

参考文献

[1] OAN AX-ON-API, http://www.alaxala.com/jp/products/oan/ (参照:2015-1-4)

Copyright ©2016 Information Processing Society of Japan.
All Rights Reserved.