C-13

BYOD に対応した出席管理システムの構築

Construction of attendance management system corresponding to BYOD

中西 久実†　　川橋 裕‡
Kumi Nakanishi　　Yutaka Kawahashi

1. はじめに

近年，ネットワーク環境の急速な普及に伴い，ネットワークを利用するためにモバイル端末を所有する人々は日々増え続けている．そこで，企業では，従業員が使いなれた自身の端末 を持ち込んで事業に活用することで，作業効率の向上をはかる BYOD (Bring Your Own Device)[1]と呼ばれる動きが広まってきている．また，この動きは企業にとどまらず，大学からも注目を浴びている．BYOD の導入により，これまで従業員が使用していた端末の設置や管理のコストを削減することができるといったメリットがある．しかし，その一方でデメリットも少なくはない．

和歌山大学で BYOD を導入した時に挙げられる問題点の中で，Wingnet が使用できなくなる点が挙げられる．Wingnet とは，端末に学生がログインした時のアカウント情報を元に出席管理などをおこなうことができるシステムである．しかし，Wingnet はデスクトップ端末等の固定端末への導入が前提となるシステムである．そのため，BYOD 環境下の個人端末の導入には対応しておらず，その代わりとなるシステムが必要となる．そこで，本研究では BYOD に対応した個人端末に向けた出席管理システムの構築を目的とする．

2. RADIUS 認証

RADIUS（Remote Authentication Dial In User Server）[2]とは，リモートアクセスにおけるユーザ認証プロトコルの一つである． RADIUS による認証システムは RADIUS サーバ，RADIUS クライアント，ユーザの 3 つの要素で構成される．RADIUS クライアントは，無線 AP へアクセスしようとするユーザの認証要求を RADIUS サーバに転送する役割を持つ．RADIUS サーバは，認証要求に応じて認証を実行し，アクセスを許可するかどうかを決定する．このとき，認証時に使用するユーザ情報は RADIUS サーバに保存される．図 1 に RADIUS 認証の流れを示す．

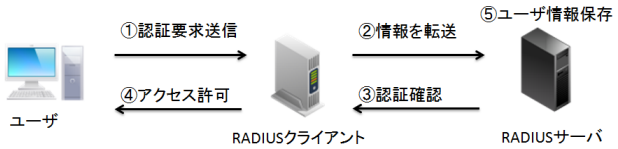

図 1：RADISU 認証の流れ

3. 提案手法

以下から研究目的を実現するために実装する手法について述べる．

3.1 RADISU サーバから情報を抽出

Wingnet は固定端末に学生がログインした時の情報を収集することで出席管理をおこなっていた．そこで，本システムでは，学生が無線 AP に接続する際におこなわれる RADIUS 認証で得られる情報を収集することで出席管理をおこなう．RADIUS 認証で得られる情報は，RADIUS サーバに一日単位でログとして保存されている．図 2 は RADIUS サーバに保存されるログの一例である．図 2 の青字で示されている Acct-Status-Type は，ログの内容が通信の開始または終了時点のものであることを示している．さらに，ユーザが接続を開始してから終了するまでのログには，全て同じ図 2 の青字で示されている Acct-Unique-Session-Id が付与されている．この Acct-Unique-Session-Id をもとにログファイル内を検索することで，無線 AP に接続した多くのユーザのログの中から，特定ユーザの一回分の通信のログを選択することができる．その選択したログから図 2 の赤字で示されているユーザ名，通信時間，端末の IP アドレス，隣接アクセスポイント(以下，AP) の MAC アドレスの情報を抽出する．その情報を通信記録として整形したものをデータベースに格納する．図 3 がデータベースに格納される通信記録の一例である．

† 和歌山大学大学院, Wakayama University
‡ 和歌山大学システム情報学センター,Center for Information Science, Wakayama University

図 2：RADIUS サーバに保存されるログ

ユーザー名	端末IPアドレス	隣接APのアドレス	通信開始時間	通信終了時間
s18xxxx	133.42.xx.xx	5c-4f-ac-3d-ee-67	12:00:34	14:45:08
l65xxxx	133.42.xx.xx	4e-3c-7b-ab-44-8e	12:05:54	14:50:13
s18xxxx	133.42.xx.xx	cc-b1-da-c4-31-22	13:07:37	16:01:09
s17xxxx	133.42.xx.xx	c0-7d-cc-5a-60-21	13:20:43	16:22:53
t11xxxx	133.42.xx.xx	c4-7d-4f-33-56-10	16:27:18	18:00:02

図 3：データベースに格納される通信記録

3.2 講義情報を登録

実施される講義の情報をあらかじめデータベースに登録しておく．図 4 に講義情報の一例を示す．講義情報は講義名，時間，曜日，教室名の要素で構成される．さらに，このテーブルに対応する授業時間，開催日，隣接 AP 情報のテーブルを別に作成する．これらのテーブルを組み合わせることで，より詳細な講義の情報を参照することができる．加えて，講義情報を変更する必要があった場合に，最小限の変更で済む．

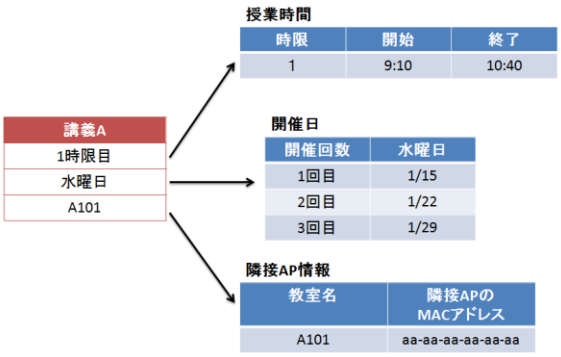

図 4：講義情報の例

3.3 受講者を判別

3.1 節で述べた通信記録の隣接 AP の MAC アドレスを用いることで，ユーザが講義を受けている教室を特定することができる．また，同じく通信時間を用いることでユーザが講義を受けている時間を特定することができる．そのため，これらの情報と登録されている講義情報の時刻や隣接 AP の MAC アドレスを比較することで，講義の受講者である可能性が高い接続ユーザを見つけることができる．加えて，受講者リストと接続ユーザ名を比較することで接続ユーザが受講者であるかを判別することが可能となる．これらの結果を，受講者リストに出欠として記録する．上記より，一講義ごとの出欠リストを作成，提示することが可能となる．図 5 に受講者を判別するまでの流れを示す．

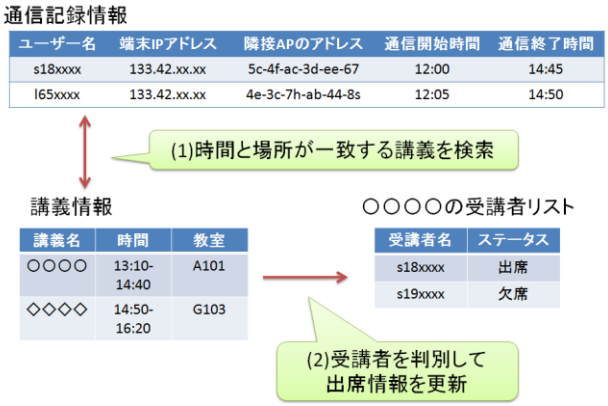

図 5：受講者を判別する流れ

4. システム構成

提案システムの処理手順と各部について図 6 と下記に示す．

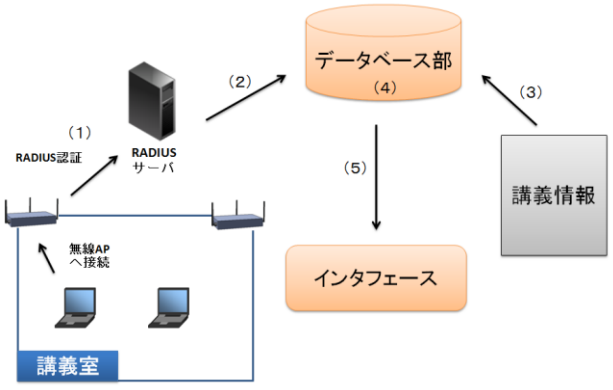

図 6：提案システムの構成

(1) RADIUS 認証が発生した際，ユーザ情報を含んだ認証情報が一日ごとにログとして RADIUS サーバに保存される．

(2) RADIUS サーバからログ情報を取得．ユーザ名，端末の IP アドレス，隣接 AP の MAC アドレス，接続時間などの情報を元に整形し，データベース部に通信記録情報として格納する．

(3) 講義名，教室名，実施時間，受講者リストを含んだ，講義情報をデータベース部に登録しておく．

(4) 通信記録情報と講義情報を比較し，一致した場合は受講者リストの出欠情報を更新．

(5) インタフェースに受講者リストを提示する．

5. 実験・評価

本実験では，ローカル環境に提案システムを構築し，実際に本学で使用されている RADIUS サーバのログを元に，2 日分のテストデータを作成した．このテストデータを用いて，整形した接続情報をデータベース部に格納し，登録された講義情報をもとに受講者リストを更新することが可能かどうかの実験をおこなった．加えて，受講者リストをインタフェースに表示し，更新内容が正確であるかを確認した．

テストデータは，ユーザ 6 人，教室数 3 部屋，講義数 8 つを想定して作成した．なお，AP1 台につき隣接する教室は 1 部屋とした．

前述で述べた実験をおこなった結果，3.1 節で述べた要素を元にテストデータを整形し，通信記録としてデータベースに格納したことを確認できた．さらに，テストデータと講義情報を比較することで期待される各講義の出欠情報と，同じ内容の出欠情報の更新を各受講者リストにおこなうことが可能であることも確認できた．テストデータを基に作成された通信記録の一例と，インタフェースに表示した 1 講義分の受講者リストのインタフェース画面を図 7 に示す．

id	studentID	IPaddress	AP_MACaddress	start	stop
1	s111101	133.42.555.1	aa-aa-aa-aa-aa-aa	09:02:00	12:23:00
2	s111103	133.42.555.3	aa-aa-aa-aa-aa-aa	09:08:00	10:41:00
3	s111105	133.42.555.5	aa-aa-aa-aa-aa-aa	10:45:00	14:58:00
4	s111102	133.42.555.2	aa-aa-aa-aa-aa-bb	11:00:00	12:21:00
5	s111106	133.42.555.6	aa-aa-aa-aa-aa-cc	11:00:00	12:25:00
6	s111103	133.42.555.3	aa-aa-aa-aa-aa-cc	12:58:00	14:42:00
7	s111102	133.42.555.2	aa-aa-aa-aa-aa-bb	13:05:00	14:41:00
8	s111101	133.42.555.1	aa-aa-aa-aa-aa-bb	14:45:00	18:05:00
9	s111102	133.42.555.2	aa-aa-aa-aa-aa-cc	14:47:00	16:30:00
10	s111105	133.42.555.5	aa-aa-aa-aa-aa-aa	15:00:00	16:21:00
11	s111106	133.42.555.6	aa-aa-aa-aa-aa-bb	16:22:00	18:02:00
12	s111105	133.42.555.5	aa-aa-aa-aa-aa-bb	16:25:00	17:50:00

図 7：実験結果画面

本システムは無線 AP からおこる RADIUS 認証の情報を用いて出席管理をおこなうことができた．よって，BYOD 環境下で Wingnet が使用できなくなった場合でも本システムが出席管理機能を補うことが可能である．

6. 今後の予定

本研究では，RADIUS サーバのログを参考に作成したテストデータを用いて運用実験をおこなった．テストデータの内容は実際の本学の講義数や生徒数，AP の台数などの想定より少ないものとなっている．そのため，実験でシステムにかかった負荷は，提案システムを実際の RADIUS サーバと連携させた場合より少なかったため，さらに大規模な情報量である実環境の RADIUS サーバと本システムを連携させ，動作の検証と評価をおこなう必要がある．

加えて，講義数がさらに増えた場合に，情報を参照しやすくインタフェースを改善する必要がある．また，受講者リストの画面に受講者が接続した時間などを追加するなど表示する内容を増やすことで，受講者が遅刻をしているなどの判別も可能となるため，システム利用者が受講者の授業評価の際，出席についての評価をより細かくおこなうことが可能であると考える．

参考文献

[1] BYOD とは｜Bring Your Own Device
http://e-words.jp/w/BYOD.html
[2] Radius 認証とは
http://www.infraexpert.com/study/security20.html