位置情報を用いた出席管理システムの提案

廣瀬研究室 4 年
C1160818 佐々木大器

概要

大学の講義や演習において、学生の出欠席を以下に効率的に管理するかは古くからの課題である。講義や演習に毎回出席することは成績評価に対する前提条件となっていることが多いため、出席状況を把握し、授業の運営に反映させることが重要である。出欠管理は、名簿に記載された学生の氏名を順番に読み上げて返事を確認する方法、出席票を回覧し学籍番号や氏名を記入させる方法、出席票を配布し学籍番号と氏名を記入させたものを最後に回収する方法などの方式が主である。本学では出席票方法が主であり、メールで出席メールを送る場合もある。しかし、いずれの出欠方法にも、他人が欠席者になりすまして出席のふりを行う、「代返」や「代筆」の不正行為を防ぎにくいといった課題がある。さらに、本学で使われている出席票方法は、受講者数が増えれば増えるほど教員側の負担が増える。そのため、ICT を活用し、学生の出欠情報を自動化する試みが提案されている。本研究では、スマートフォンの位置情報サービスを利用した出席管理システムの構築をする。(442 文字)

目 次

第1章　はじめに

1.1　背景

大学の講義や演習において、学生の出欠席を以下に効率的に管理するかは古くからの課題である。東北公益文科大学 (以下、本学) も例外ではなく、講義や演習に毎回出席することは成績評価に対する前提条件となっていることが多いため、出席状況を把握し、授業の運営に反映させることが重要である。

出欠管理は、名簿に記載された学生の氏名を順番に読み上げて返事を確認する方法 (氏名読み上げ方法)、出席票を回覧し学籍番号や氏名を記入させる方法 (出席リスト方法)、出席票を配布し学籍番号と氏名を記入させたものを最後に回収する方法 (出席票方法) などの方式が主である [1]。本学では出席票 (図 1.1) 方法が主であり、メールで出席メールを送る場合もある。しかし、いずれの出欠方法にも、他人が欠席者になりすまして出席のふりを行う、「代返」や「代筆」の不正行為を防ぎにくいといった課題がある。さらに、本学で使われている出席票方法は、受講者数が増えれば増えるほど教員側の負担が増える。そこで、学生の出欠情報を、ICT を活用し、自動化する試みが提案されている。その中に学生のスマートデバイスを使った出欠管理がある。

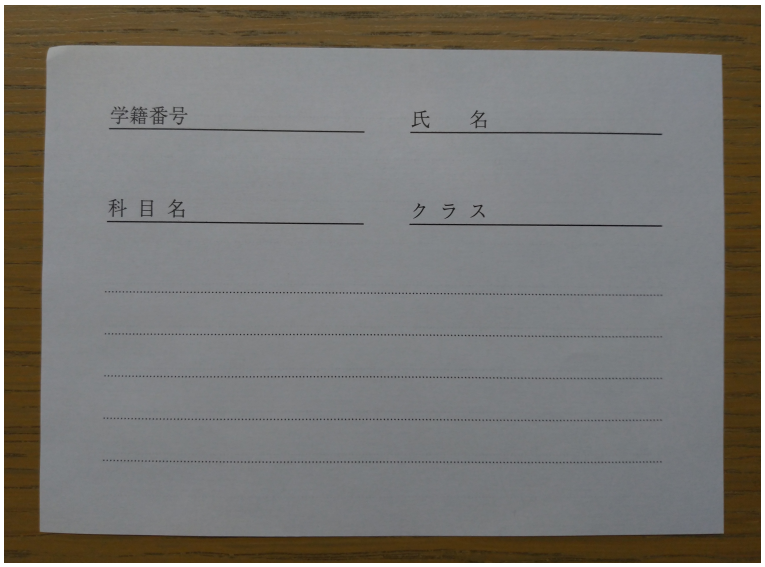

図 1.1: 本学で使われている出席票

総務省平成 30 年度版情報白書によると、2017 年の世帯における情報通信の保有率は 94.8 %となっている。また、2017 年における個人のモバイル端末の保有状況を見ると、スマートフォンの保有率が 60.9 %であり (図 4.2)、前年より 4.1 ポイント上昇してることから、2019 年でも伸び続

けていることが期待できる [2]。

スマートフォンには、GPS 機器等が標準的に搭載されており、通信サービス上の行動履歴や利用者の状態に関する情報として、精度の高い位置情報が存在する [3]。GPS や位置情報を使ったサービスの一例として、Google がインターネットを通して提供している地図、ローカル検索サービスである「Google マップ[1]」がある。他には、ユーピーアール株式会社は、貴重品輸送のサービスに GPS を使い、位置追跡を行うことで具体的な現在地を管理できるようにし、輸送品質やセキュリティ性の向上に成功している [4]。

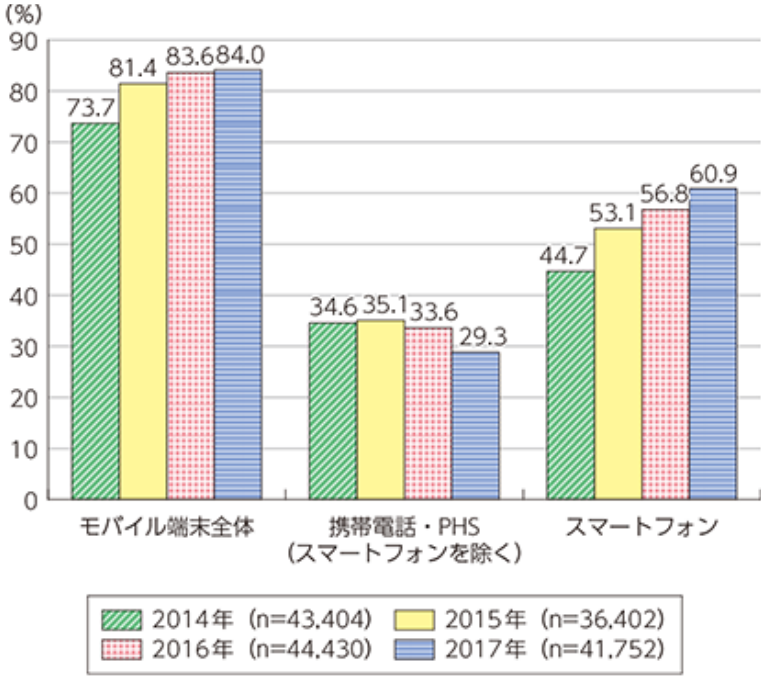

図 1.2: モバイル端末の保有状況 [2] 図 5-2-1-2 より引用

1.2　先行研究

スマートデバイスを使った出席管理システムに関した先行研究は以下のようなものがある。嶋川らは、スマートフォンと BLE ビーコン[2]を用いた出席管理手法を提案した [3]。学生が所有するスマートフォンで出席を行うため、出席管理システムを利用するための待ち時間が必要なく素早い出席管理を可能にする。また、学生は、BLE ビーコンが検出できる場所でしかログインができないため、出席票の代筆等の不正出席をなくすことに有効である。しかし、BLE ビーコンの設置を教室毎に行わなくてはならなく、コストが高い。また、BLE ビーコンの設定等を行わなくてはならないなどの問題点があげられている。

握美、久保は、学生が所有する Android 端末を用いた出席管理システムを提案した [5]。出席確認を行うシステムとして、IC カード式学生証とその読み取り端末を用いる場合に、履修者数の多

[1]https://www.google.co.jp/maps/
[2]Bluetooth を利用した屋内位置測位を行う装置

い授業は時間がかかってしまうという問題がある。そこで、複数の読み取り端末を並列的に利用可能な構成にすることで時間がかかってしまうという問題の解決を図るにあたり、スマートフォンなどの NFC[3]対応の Android 端末をシステムの一部として利用し、試作を行なった。握美らのシステムは、学生から任意により端末を提供させるという形を原則としているため、提供の有無によって授業内での学生の扱いに差別を生じさせてはならないという問題点があげられる。

1.3 出席管理の問題点

1.2 であげたスマートデバイスを使った出席管理の問題点をまとめる。

- BLE ビーコンの購入、設置等のコストが高い
- 端末の提供の有無によって学生の扱いに差別を生じさせてはならない

このような問題点が判明した。そのため、本学では、BLE ビーコンの設置を必要としない。かつ、学生に端末の提供を必要としないシステム作りが必要である。

[3]近距離無線通信。Near Field Communication の略語。RFID（Radio Frequency IDentification）と呼ばれる無線通信による個体識別の技術の一種であり、近距離無線通信の技術を統一化した世界共通の規格である。IC チップを内蔵した NFC タグを NFC のリーダ・ライタ機能を有する機器により読み取り・書き込みを行う。

第2章　システムの提案

2.1　GPSの概要

GPS(Grobal Positioning System:全世界的測位システム) は、人工衛星による位置決定システムである。1970 年代の初頭に米国国防総省 DOD(Department of Defense) により地球上どこでも実時間の連続測位が可能なシステムを目指し開発が開始された [6]。

約 32 機の人工衛星（測位衛星）が高度約 2 万 km を飛行しており、それらの衛星が発信する信号を GPS 端末が受信することで位置を特定する。測位衛星には、正確な時計が搭載されており、衛星はその時刻と軌道の情報を電波に乗せて発信していて、GPS 端末でその情報を受信すると、発信されてから届くまでの時間差を算出できる仕組みになっている。時間差といっても電波は光の速さで進むので差はわずかだが、衛星と地球との距離は遠いので、計算できるだけの時間差が生まれる。この時間差と光速とを掛けることで、衛星と GPS 機器との距離を算出できる [6]。

3 機の GPS 衛星を用いることで測位位置を求めることができる。これは、数学的に測位位置を表現する 3 次元座標の成分の 3 つの未知数を求めるために必要である。実際測位を行うには、受信機内の時計の誤差を求めることになるため、図 2.1 のように最低 4 機の衛星を同時に観測する必要がある。

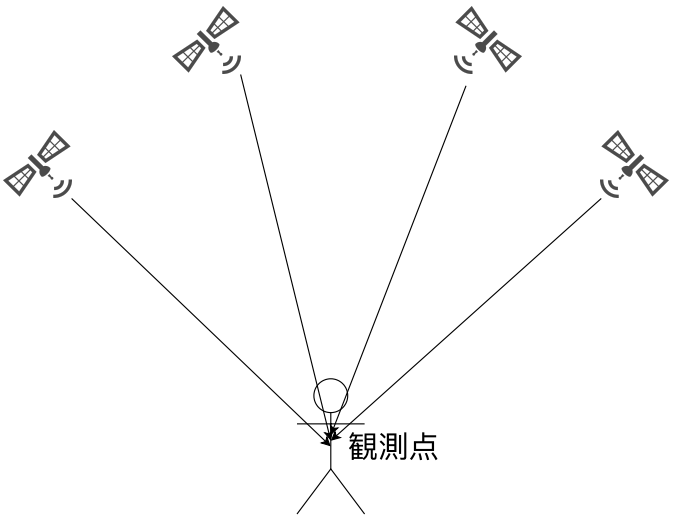

図 2.1: GPS 観測例

2.2　目的

本システムは、スマートデバイスに搭載されている位置情報システムを利用し、位置情報を取得し続けることで出席の有無を記録するシステムである。また、本システムに、ログイン機能を搭載することで誰が出席をしているのかの判断を行う。本システムは、本学で運用することを想定しており、現在本学で利用できる設備や仕組みの利用可能な範囲で設計、構築を行う。また、本システムの利用者は本学に所属する学生、教員を前提とする。

2.3　システムの概観

システムの概観は以下のようになる (図 2.2)。学生は、ログインフォームで自分の学籍番号とパスワードの入力を行う。学籍番号とパスワードは、事前に DB 等に入力しておく。このことにより、新規に作成する手間や、意図しない登録を防止する。

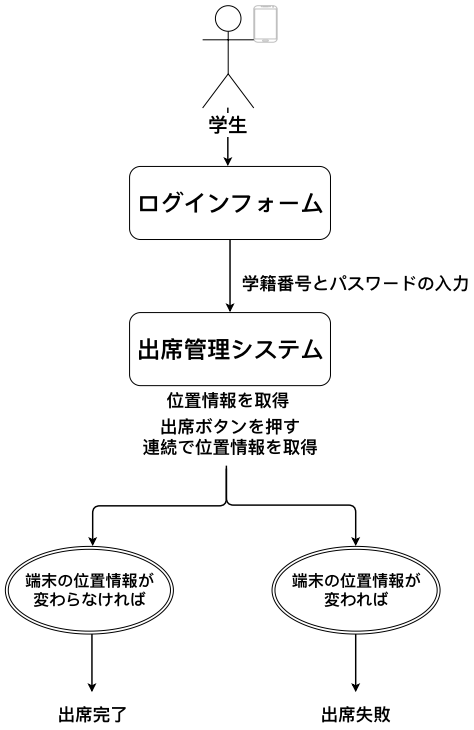

図 2.2: システムの概観図

第3章　システムの開発

ログインフォームと出席管理システムの位置情報取得方法について説明する。

3.1　開発環境

開発環境を以下に示す。

3.1.1　PHP

The PHP Group によってコミュニティベースで開発されているオープンソースの汎用プログラミング言語である。サーバーサイドで動的なウェブページ作成するための機能を多く備えていることを特徴とする。

3.1.2　JavaScript

ウェブブラウザ上で動作し動的なウェブサイト構築やリッチインターネットアプリケーションの開発に用いられるオブジェクト指向スクリプト言語である。

3.2　ログインフォーム

ログインフォームを以下の図に示す (図 3.1)。

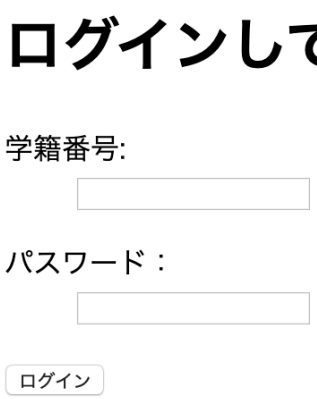

図 3.1: ログインフォームの画面

学生は本学で使っている学籍番号と、事前に学生が指定したパスワードを入力しログインを行う。

パスワードは、学生が指定したものをハッシュ化し保存することにより、万が一漏洩事故が起きた際に、パスワードがわかりにくくなる。詳しくは 3.4.1 で説明する。

3.3　セキュリティ問題

本システムのログインフォームのような動的システムには、適切な処置をしたプログラムを用意する必要がある。本来、本システムを用いて説明すれば、学籍番号やパスワードの記述欄に、JavaScript などの動的なプログラミング言語[4]を用いてプログラムコードを記入されると、学籍番号やパスワードの漏洩につながる危険がある。これは、動的なコンテンツというのは、毎回プログラムで生成されているため、プログラムが Web サーバで動いている。そのため、攻撃を許してしまう脆弱性があると情報が盗まれてしまう。システムの脆弱性を狙った攻撃手段を以下に示す。

3.3.1　SQL インジェクション

SQL インジェクション攻撃 (図 3.2) は、Web アプリケーションの入力の入力フォーム等に不正な入力をし、送信することによってサーバ側で予期せぬ動作を引き起こす攻撃である [8]。例えば、入力画面フォームに 1' or '1' = '1';– という文字を送信した際に、システムでは、以下のような sql 文を発行する。

```
SELECT user_id,password FROM users WHERE user_id='1' or '1' = '1'– AND password='$password';
```

まず、SELECT user_id,password FROM users WHERE user_id='1' or '1' = '1' の部分では、user_id が'1' か '1' が '1' なら真という条件文なので結果は必ず真になり、この例の場合ではテーブル内のすべてのレコードが結果として得られてしまう。また、MySQL では–後はコメントアウトとして使用されるので後半の SQL 文は無視される。ログイン認証のソースコードはレコードが帰ってくるかどうかで認証をしているのでこの例ではログイン認証ができてしまう。

Web アプリケーション自体に不正と思われる記号がないかをチェックする対策が採られているが、 マルウェアや不正アクセスといった攻撃の特徴的なパターンのマッチングを回避する攻撃が考え出されており、検出が難しくなっている。

[4] 一般の言語がソースコードを、コンピュータ上で実行可能な形式に変換される際に、行う操作を実行時に行うプログラミング言語である。

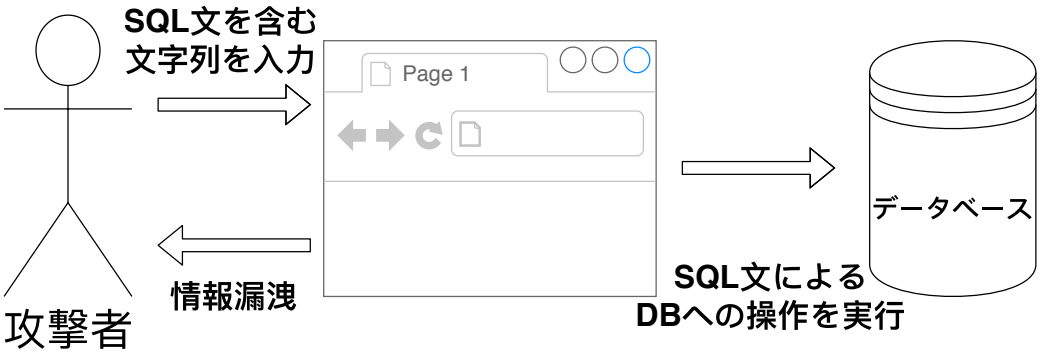

図 3.2: SQL インジェクション攻撃の例

3.3.2 XSS

XSS(クロスサイトスクリプティング) は、攻撃者が入力内容に、スクリプト付のリンクを貼る等の罠を仕掛け、被害者となるユーザが誤って罠を実行すると、セキュリティ的に問題のある別のウェブサイトに対し、脆弱性を利用した悪意を持った実行内容が含まれた通信が実行される攻撃手法である [9]。例えば、以下のようなスクリプトによって、Cookie に埋め込まれたセッション情報などの秘密情報を、盗まれてしまう。

```
<script>
location.href = 'http://悪意のあるサイト/getCookie.cgi?cookie=' + document.cookie;
<script>
```

3.3.3 クリックジャッキング

クリックジャッキング攻撃とは、ユーザを視覚的に騙して正常に見えるウェブページ上のコンテンツをクリックさせ、別のウェブページのコンテンツをクリックさせる攻撃のことである (図 3.3)。その結果、ユーザが公開するつもりのないプライバシー情報を公開させられたり、意図しない情報を登録させられたりするなどの被害を受ける可能性がある [10]。

3.4 セキュリティ対策

3.3 で挙げたセキュリティ問題を解決するために本システムでは、以下の対策を行う。

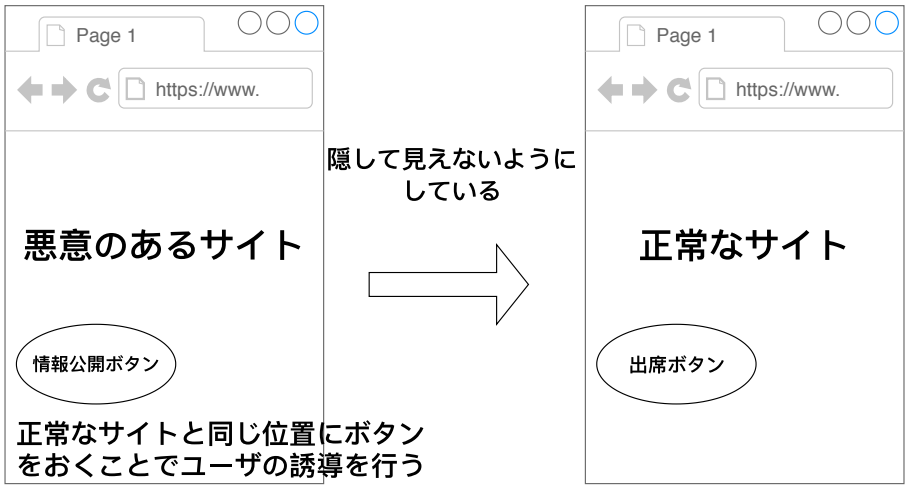

図 3.3: クリックジャッキングの例

3.4.1　パスワードのハッシュ化

パスワードが漏洩してもハッシュ化[5]を行うことで不正ログインの防止ができる。ハッシュ化されたパスワードの例を表 3.1 に示す。

表 3.1: ハッシュ化済のパスワード例

パスワード	ハッシュ化済みのパスワード例
akican19	$2y$10$aCPMH7J3OCR3qowFGfNX4ee5pFZQf6bKm/HduCS1Kf6w7d4N1Q6o2
password	$2y$10$y5CsiP9mbO3cEuSafrJBq.ewdrxnx30TJlaLTv6tc8auMI9ygzyve
Sasaki	$2y$10$zLGCcfjJUl1oMcEFmvWKteBvREGhNJCur9NyIwcbx76e4Lt1PDG76

3.4.2　エスケープ処理

エスケープ処理とは、マークアップ言語やプログラミング言語、スクリプト言語等で文字列を扱う際に、その言語にとって特別な意味を持つ文字や記号を、別の文字列に置き換えることである。例えば、攻撃者が入力フォームから Web ページに送信されるデータの中に script タグが含めていたとする。この場合にも、エスケープ処理によって「<」や「>」が「<」や「>」に置き換えられるため、script として動作することを防ぐことができる。本システムでは、エスケープ処理を行う関数を作ることでエスケープ処理を行なっている。

[5]元のデータから一定の計算手順に従ってハッシュ値と呼ばれる規則性のない固定長の値を求め、その値によって元のデータを置き換えること。

3.4.3 クリックジャッキング対策

X-Frame-Options は、HTTP のレスポンスヘッダで、frame 要素または iframe 要素で Web ページを表示させることを許可するか否かを指定できる仕組みである。このヘッダを使用することで、他のサイトで frame 要素または iframe 要素上で読み込ませたいページを除外することができる。

3.5 学生情報の管理

関数を図 3.4 のように指定している。

```
//1人目
$userid[] = 'C1160818';
$username[] = '佐々木大器';
$hash[] = '$2y$10$MeurUlzg8gzCHKYkDMrz/.9/3eq2qxl.GyBFy65F8BFym2/YS67dq';
// 2人目
$userid[] = 'C1000000';
$username[] = 'テストユーザ';
$hash[] = '$2y$10$Jb/beQEUPERIYRyzsZUcT.9U9qsLqQLOXQXaKJrjlIQwRreTkKns6';
```

図 3.4: ユーザ情報

userid に学籍番号を入れ、username に学生の名前を入れている。hash には、3.4.1 で説明した方法でハッシュ化したものを入れている。入力されたパスワード文字列とハッシュ化済みのパスワードを照合しログインができるようにしている。

3.6 出席管理システム

出席管理システム (図 3.5) では、授業を行う教室に入室した後にログインをすることを前提にシステム開発を行なっている。また、学生には、自身のスマートデバイスの GPS モジュールを ON にし、かつ、位置情報アクセスを特定のアプリに認めていることを前提としている。ログインが正常に行われると、位置情報を取得する。

出席ボタンを押すことで持続して位置情報を取得し続ける。ログインをした時に取得した位置情報と出席ボタンを押した後に取得し続ける位置情報を比べる。学生が途中退出を行なった際に位置情報が変更されると、出席失敗となる。本学では、授業時間が 105 分となっているため、出席ボタンを押してから 105 分が経つと出席完了となる。

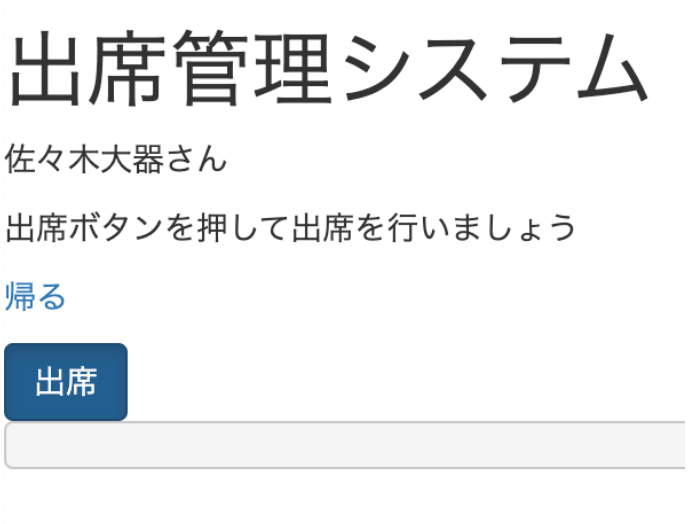

図 3.5: 出席管理システムの画面

第4章　実験

出席管理システムの使用実験を行う。

4.1　実験環境

実験環境を以下に書く。

4.1.1　実験場所

実験場所は、本学の 203 教室 (図 4.1) を使い実験を行う。

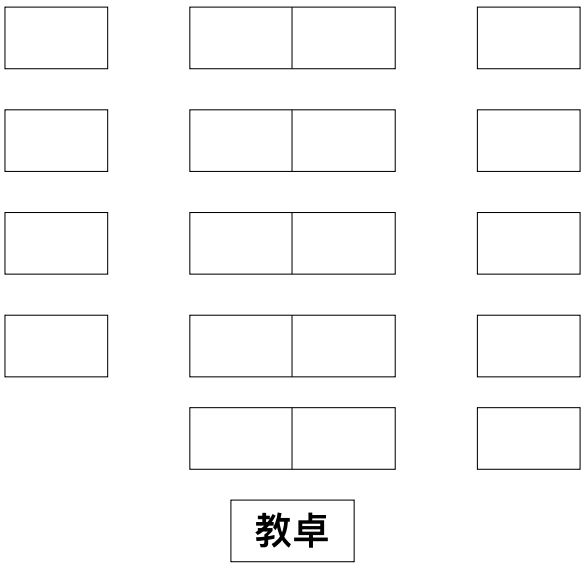

図 4.1: 実験を行なった 203 教室の見取り図

4.1.2　使用モバイル端末

実験に使ったモバイル端末とモバイル端末のバージョンは以下の通りである。

1. MacBook Pro (13-inch, 2019, Two Thunderbolt 3 ports)
   MacOS Mojave 10.14.6
2. SONY Xperia X Compact SO-02J
   Android バージョン 8.0.0
3. ASUS ZenFone 5 (ZE620KL)
   Android バージョン 8

以下、実験に使用した端末を箇条書き番号で記す。

4.2　実験条件と手順

実験の条件と手順を以下に示す。

1. 実験時間は、本学の授業時間 105 分とする。
2. 端末 1,2 は 105 分間動かさずに、スリープ状態にならないように管理する。
3. 端末 3 を途中退席を行なった生徒と想定し、実験途中に教室外に運び、位置情報が変化したことにより、位置情報取得を止めるか見る。
4. 105 分後、出席が完了するかを見る。

端末 1,3 は本学で VPN 接続することで使用することができる無線 LAN(以下、学内無線 LAN) を使用し、端末 2 は NTT ドコモの SIM カードを使い、NTT ドコモの LAN を使用する。端末 2 は、全ての学生が学内無線 LAN を使えるとは限らないためキャリア LAN を使用し実験を行う。

4.3　実験結果

端末 1,2 は、105 分間位置情報を取得し続け、出席完了することができた (図 4.2)。

図 4.2: 出席完了の alert

端末 3 を 203 教室から持ち出した際には、動かした警告が出て、出席停止するようにできた (図 4.3)。

図 4.3: 動いた際に出る alert

第5章　結論

5.1　結論

本研究は、位置情報を使った出席管理システムを作成することを目指した。

他人が欠席者になりすまして出席のふりを行う、「代返」や「代筆」の不正行為を防ぎにくいといった課題を、モバイル端末を使用して出席管理を行うことで「代返」や「代筆」を防ぐことができた。また、BLE ビーコンなどの、設置や設定等を必要とせず、学生のモバイル端末で出席管理を行うことができた。しかし、必ずしも 105 分間授業を行うとは限らず、早めに終わった場合に対応できない。また、学生がトイレにいった場合や、課外授業の際に位置情報がずれて出席失敗になることが課題である。

5.2　今後の展望

今回の実験では、iOS のスマートフォンを使えなかったため、iOS 端末での実験を行う必要性がある。また、キャリア回線を使う際に、データ通信量の問題点が出てくる。本システムは、1 秒ごとに位置情報を取得できればするようにしているため、通信量が多くなる。毎日使えるようにするには、位置情報の取得のスパンを長くするか、全ての学生に学内無線 LAN を使ってもらう必要がある。他には、出欠を管理するサイトを作らないと授業評価に使用できない。

参考文献

[1] 飯尾 淳. “スマートデバイスを用いた出席管理システムの利用に対する学生の意識調査” . 文学部紀要 社会学・社会情報学. 2017. 13-28

[2] 総務省. “基本データと政策動向”. http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd252110.html, (参照日 2019-12-9).

[3] 総務省. “スマートフォンを経由した利用者情報の取扱いに関する WG 中間とりまとめ (案)”. http://www.soumu.go.jp/main_content/000155904.pdf, (参照日 2019-12-10).

[4] ユーピーアール株式会社. “IoT ソリューション導入事例”. https://www.upr-net.co.jp/case/iot/usecase-17.html(参照日 2020-1-7)

[5] 嶋川 司 三木 光範 中原 蒼太 間 博人. “スマートフォンと BLE ビーコンを用いた出席管理手法の提案”. 同志社大学ハリス理化学研究報告. 2017,88-95

[6] 喬 耘. “GPS 単独測位の高精度化に関する研究”. 東京海洋大学 海洋工学部 海事システム工学科 GPS/GNSS 研究室 情報通信工学研究室. 2005

[7] 握美 孝明 久保 裕也. “学生の所有する NFC 対応 Android 端末を用いた出席管理システムの試作”. 第 77 回全国大会講演論文集. 2015,383-384

[8] 角田 直樹 安井 浩之 松山 実. “異常検出手法を用いた SQL インジェクション攻撃の検出”. 全国大会講演論文集. 2009,379-380

[9] 川内 英主 千葉 雄司 土居 範久. “社内ウェブサイトの脆弱性を悪用した XSS を防止するシステムの構築”. 全国大会講演論文集. 2009,373-374

[10] 情報処理推進機構. “知らぬ間にプライバシー情報の非公開設定を公開設定に変更されてしまうなどの「クリックジャッキング」に関するレポート”. https://www.ipa.go.jp/files/000026479.pdf(参照日 2020-1-7)