複数の授業でMACアドレスと出席者が重複した時間による端末所有者の特定

遠藤 空[1]　高橋 風太[2]　串田 高幸[1]

概要：出席管理は教育機関において重要なプロセスである．紙やファイルベースでこれを行うと人為的ミスが発生しやすくなってしまう．よってこのプロセスを自動化する必要がある．課題は DHCP サーバでは，IP アドレスを割り当てた端末所有者を特定することができない点である．本稿では授業開始時刻前に割り当てられた IP アドレスを持つ端末の MAC アドレスと，授業に出席している学生の名前をそれぞれ授業ごとにリストとして保持し，複数の授業で共通の MAC アドレスと学生の名前があるかを比較することで端末所有者を特定することを提案する．基礎実験では CDSL 内の実際の入退室を目視で記録し，これと DDNS・DHCP ログとの照らし合わせを行った．その結果，複数人同時の入退室があることから，1 日だけでは個人の特定を行うことが出来ないことが分かった．評価は実際に確認した個人の端末の MAC アドレスと本稿の提案を用いて特定した MAC アドレスの正答率と，学生全員を特定できるまでにかかった時間を算出する．

1. はじめに

背景

東京工科大学コンピュータサイエンス学部の Cloud and Distributed Systems Laboratory(以下 CDSL) では，各自の研究内容に関連する論文を要約して発表する論文輪講会や，各自の研究内容の進捗を発表する Cadence がある．これらの授業の出席管理を学生が全て手動で行っている．出席管理は学生の成績を取るために，教育機関では重要なプロセスである [1]．QR コードやバーコードを組み込んだ Web 技術による出席システムが使われているが，従来の出席管理の方法は紙やファイルベースにより手動で行っていた [2,3]．これは時間がかかる上に，出席簿への誤記入のような人為的ミスが発生しやすいため，効率的な方法ではない [4,5].

教育機関では Moodle や Canvas を例とする学習管理システム (LSM) を使用した出席管理を使用しており，これにはインターネット接続を必要としている [6]．インターネットによる出席管理の自動化を行うことで，ユーザは端末をネットワークに接続するだけで出席管理を行うことができる．したがって，CDSL 内の出席管理をネットワークを使用して自動化する必要がある．

CDSL にはプライベートネットワークがある．プライベートネットワークとは，組織が所有する，または専用の回線を介して制御するネットワークのことである [7]．そのため，CDSL には Dynamic Host Configuration Protocol Server(以下 DHCP サーバ)，Domain Name System Server(以下 DNS サーバ), Dynamic Domain Name System Server(以下 DDNS サーバ) がある．

DHCP サーバとはネットワーク内のクライアントが IP アドレス，サブネット，デフォルトゲートウェイ，DNS サーバの IP アドレスを例とするネットワーク利用に必要な設定を動的に割り当てるサーバである [8,9]．これにより，CDSL ネットワークに接続している機器の台数を把握することが可能である．また，ネットワーク内のクライアントの識別は MAC アドレスをもとに行っている．

MAC アドレスとはネットワーク内のデバイス間の通信を行うためのアドレスであり，IEEE802 で定義された一意の 48 ビットのアドレスであり，通常は 16 進数で表される [10,11]．IEEE802 とは IEEE Computer Society が主催する標準化委員会のことで，主に Local Area Network(LAN) や Personal Area Network(PAN)，イーサネットの標準化を行っている [12,13].

DNS サーバとは，インターネットドメイン名と IP アドレスの関連付けや，電子メールのホストの指示を行える機能を持つサーバのことである [14].

[1] 東京工科大学コンピュータサイエンス学部
〒 192–0982 東京都八王子市片倉町 1404-1
[2] 東京工科大学大学院バイオ・情報メディア研究科コンピュータサイエンス専攻
〒 192–0982 東京都八王子市片倉町 1404-1

DDNS サーバとは DHCP サーバによって割り当てられた IP アドレスが更新される際に，新しい IP アドレスをネットワークドメインに動的に関連付けるサーバのことである [15].

課題

課題は，DHCP サーバで IP アドレスを割り当てることにより端末を識別することは可能であるが，DHCP サーバで割り当てた IP アドレスだけでは端末所有者を特定することはできないことである．本稿の課題を図 1 に示す．

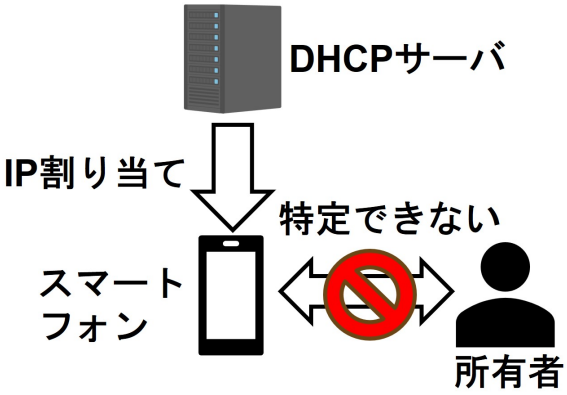

図 1: 課題となるケース

例えば，CDSL に端末所有者である学生 A が入室したとする．この時，学生 A の所有しているスマートフォンがネットワークに接続されると，DHCP サーバから IP アドレスが割り当てられる．しかし，DHCP サーバは端末所有者を識別するための名前や学籍番号といった情報を持たず，端末の MAC アドレスにもとづいて IP アドレスを割り当てる．したがって，特定の IP アドレスを学生 A の端末と結びつけることはできない．このことから，端末所有者を特定する必要がある．

各章の概要

第 2 章では，本稿の関連研究について述べる．第 3 章では，本稿の課題を解決するための提案方式とユースケースについて述べる．第 4 章では，提案方式をもとに作成したソフトウェアの実装について述べる．第 5 章では，課題の基礎実験と提案方式の評価について述べる．第 6 章では，本稿の議論についてを述べる．第 7 章では，本稿のまとめを述べる．

2. 関連研究

Radio Frequency Identification(以下 RFID) タグの付いた携帯電話を用意して学生の軌跡を取得し，学生の出席管理システムに分析データを提供している研究がある．[16]. 学生分の RFID タグの付いた携帯電話を用意しなければならず，同一インターネット上の端末とその所有者の特定は行っていないため，本稿の課題は解決できない．

Wi-Fi に焦点を当て，ポータブルデバイス MAC アドレスが所有者に影響を及ぼす問題とその悪用について調査している研究がある [17]．無線ネットワークにおいて端末が定期的に発信するビーコンフレームをキャプチャし，それを再送信することで特定の MAC アドレスを追跡するビーコンリプレイ攻撃により，MAC アドレスと端末の紐づけを行っているが，端末所有者の特定までは行えていない．

Raspberry Pi を使用した出席管理システムを作成している研究がある [18]．この出席管理システムでは，名前で出席確認をするのではなく，MAC アドレスに対して出席確認を行っている．そのため，本稿の課題で挙げている端末所有者を特定することはできない．

顔認証や指紋，位置情報を用いたスマート出席管理システムを作成している研究がある [19]．学生の軌跡をスマートフォンの顔認証センサーや指紋認証センサーを用いて複数期間記録している．また，実際の出席状況も同じように記録している．しかし，指紋や顔認証は授業毎に学生本人がそれぞれスマートフォンを用いて行っており，この研究では出席管理の自動化を行うことはできない．

3. 提案

本稿では DDNS サーバと DHCP サーバのログをもとに作成した DDNS・DHCP ログから，端末所有者を特定することを提案する．提案方式ではログの整理，端末所有者の特定について説明する．

提案方式

- **ログの整理**

本稿では DDNS サーバと DHCP サーバのログファイルと，出席名簿を使用する．DDNS・DHCP ログの中身はタイムスタンプ，IP アドレス，MAC アドレス，DNS マッピングである．本稿における DNS マッピングとは，レコードを DNS サーバに追加する add と，DNS サーバからレコードを削除する remove を意味する．このログの例をログファイル 1 に示す．

ログファイル 1: DDNS・DHCP ログの例

```
1 2024-06-12T07:43:41.12,add,192.168.100.44,
      56:35:21:f2:02:5d
2 2024-06-12T10:01:39.39, remove, 192.168.100.44
```

DDNS サーバのログには MAC アドレスが含まれていないため，タイムスタンプと IP アドレスが一致するものを DHCP サーバのログから取得する．また，DHCP サーバのログにはリースが切れたログが残らないため，ログファイル 1 のように DNS マッピングが remove の際には MAC アドレスは存在せず，IP アドレスのみを記述している．出

席名簿の中身は授業のある曜日とその時間帯，授業を受けている学生の名前と出席状況である．

- **端末所有者の特定**

各授業にどの学生が出席しているのかが書かれている出席名簿と，DDNS・DHCP ログから取得した MAC アドレスのリストをそれぞれ授業ごとにリストとして保持する．図 2 に授業ごとにリストを作成する例を示す．2 時限以降

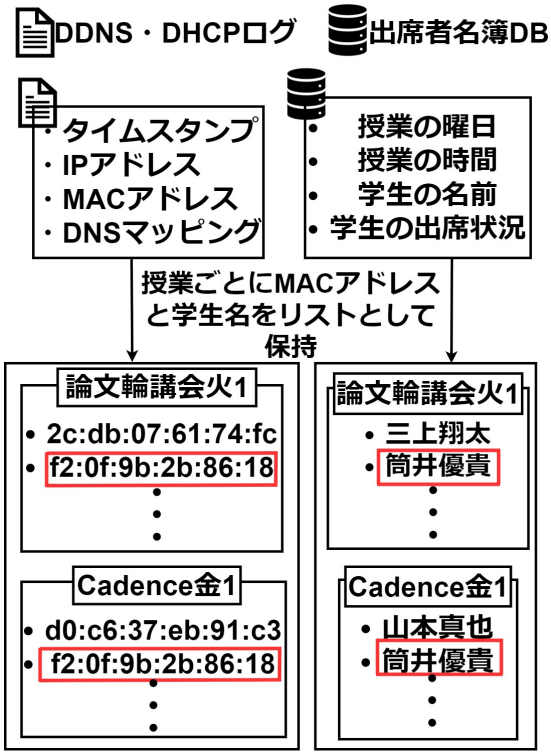

図 2: 授業ごとにリストを作成

の授業の場合，DNS マッピングで remove のログがない MAC アドレスを保持する．

次に，授業ごとに同一の MAC アドレスがあるかを確認する．また，同じ出席者が存在するかどうかも確認する．その後，比較した授業の期間が MAC アドレスのリストとメンバーリストで一致していれば，同一の MAC アドレスを出席者の端末として特定する．この処理の流れを図 3 に示す．

図 3 では火曜日 1 時限にある論文輪講会と金曜日 1 時限にある Cadence の MAC アドレスのリストと，メンバーリストをそれぞれ比較している．この比較の結果，保持しているアドレスが同じで，メンバーリストから同じ学生であることが確認できれば，この MAC アドレスの「f2:0f:9b:2b:86:18」は学生である筒井優貴の所有する端末であるとして所有者の特定を行う．この時，リストの比較を行う回数は 1 週間の授業回数分である．これは 1 週間に全員同じメンバーで行う授業が存在しないためである．比較を行う回数は組み合わせの公式を用いて，式（1）で算出する．

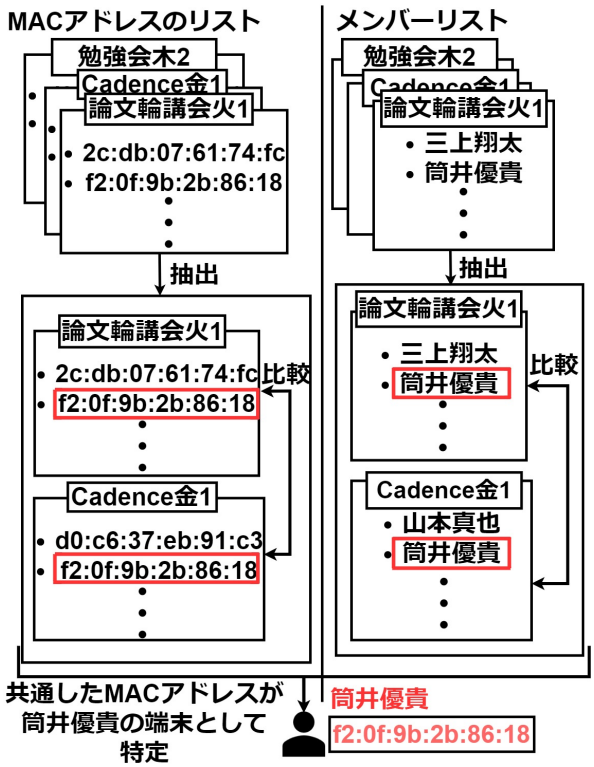

図 3: 総当たりでリスト同士を比較

$$\binom{n}{k} = \frac{n(n-1)}{k} \tag{1}$$

k は 1 度の組み合わせで行う比較の対象の個数である．本稿では図 2 のように 2 つずつ比較を行うため，k は 2 となる．n は要素数を表し，今回では 1 週間の授業総数である．

ユースケース・シナリオ

本稿では CDSL をユースケースとする．図 4 に提案ソフトウェアを使用した本稿のユースケースを示す．

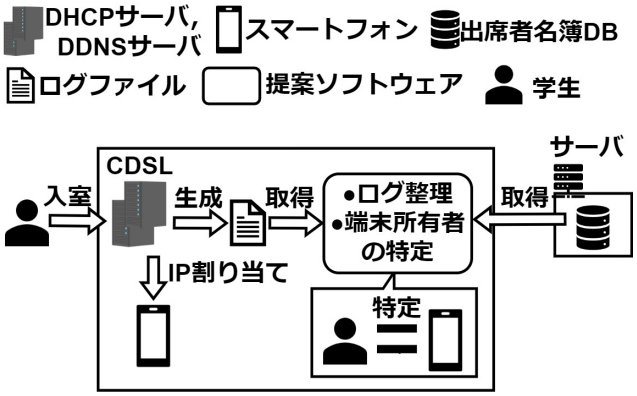

図 4: ユースケース

学生が CDSL に入室した段階で DHCP サーバは学生が所持している端末に IP アドレスを割り当てる．IP アドレスを割り当てられた DHCP サーバのログと DDNS サーバのログを提案ソフトウェアが取得する．同時に出席名簿

DB から学生の名前と出席状況を取得する．その後，本稿の提案ソフトウェアを用いることにより，端末所有者の特定が可能である．

4. 実装

本稿では Python でログを整理するソフトウェアと，端末所有者を特定するソフトウェアを作成した．ログを整理するソフトウェアは，DDNS サーバと DHCP サーバのそれぞれのログからタイムスタンプ，IP アドレス，MAC アドレスを取得する log_output である．端末所有者と特定するソフトウェアは，log_output で整理した DDNS・DHCP ログと出席名簿から端末所有者を特定する identify である．提案ソフトウェアの詳しい説明をプログラムごとに説明する．

ログを整理するソフトウェア

K3s によって組み込まれた Kubernetes クラスタに 3 台ある DDNS サーバと DHCP サーバのログからタイムスタンプ，IP アドレス，MAC アドレス, add や remove を例とする DNS マッピングを取得する．K3s とはエッジデバイスや小規模なデプロイメントを例とするエッジコンピューティング向けに改良された認定 Kubernetes ディストリビューションの 1 つである [20]．このソフトウェアを log_output として，流れを図 5 に示す．

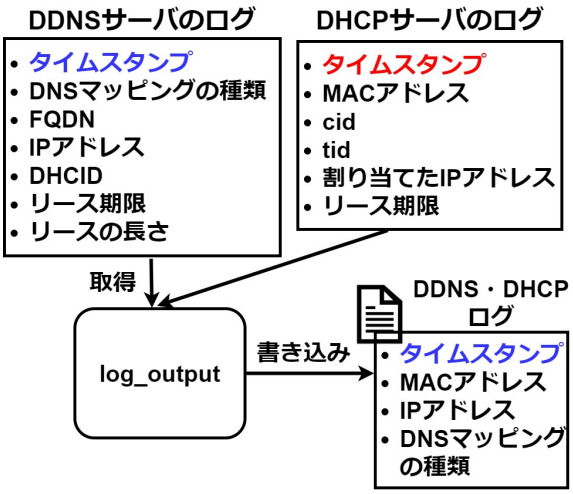

図 5: log_output の流れ

DHCP サーバはネットワークに接続されていてもリースの期限が切れたら再度割り当て，そのログが残る．また，リースが切れた際に，IP アドレスを削除するログがない．DDNS には DNS マッピングが remove である際も，ログが残るため，DDNS サーバのログをベースとして，MAC アドレスを加えた新たな DDNS・DHCP ログを作成する．

図 5 の DDNS サーバのログの例をログファイル 2 に示す．

ログファイル 2: DDNS サーバのログの例

```
1 2024-06-20T02:15:18.703355431Z stdout F INFO D
      HCP_DDNS_ADD_SUCCEEDED DHCP_DDNS Request
      ID 0001018C999D4775FFF95C30008BB
      B125744944CFD9738688539854B22F1AFA985
      B298: successfully added the DNS mapping
      addition for this request: Type: 0 (CHG_A
      DD)
2 2024-06-20T02:15:18.70340973Z stdout F Forward
       Change: yes
3 2024-06-20T02:15:18.703414818Z stdout F Revers
      e Change: yes
4 2024-06-20T02:15:18.703417344Z stdout F FQDN:
      [ip-192-168-100-199.a910.tak-cslab.org.]
5 2024-06-20T02:15:18.7034196Z stdout F IP Addre
      ss: [192.168.100.199]
6 2024-06-20T02:15:18.703421871Z stdout F DHCID:
       [0001018C999D4775FFF95C30008BBB125744944
      CFD9738688539854B22F1AFA985B298]
7 2024-06-20T02:15:18.703423879Z stdout F Lease
      Expires On: 20240620022518
8 2024-06-20T02:15:18.703425918Z stdout F Lease
      Length: 600
9 2024-06-20T02:15:18.703427998Z stdout F Confli
      ct Resolution: no
```

ログファイル 2 の各行の先頭にはタイムスタンプが記述されている．1 行目には DNS マッピングの種類が記述されている．ログファイル 2 の例では，DHCP_DDNS が DNS マッピングの追加を送信し，DNS サーバが受信したことを表している．2 行目にはフォワード DNS レコードが変更され，3 行目にはリバース DNS レコードが変更されたことが記述されている．4 行目には FQDN が記述されている．5 行目には，IP アドレスが記述されている．6 行目には DHCID が記述されており，DHCP クライアント識別子を表している．7 行目にはリース期限が記述されており，リースが切れる日時を表している．8 行目にはリースの期間が記述されている．9 行目には競合解決が行われなかったことが記述されている．

図 5 の DHCP サーバのログの例をログファイル 3 に示す．

ログファイル 3: DHCP サーバのログの例

```
1 2024-06-14T01:13:23.374458585Z stderr F
      2024-06-14 01:13:23.374 INFO [kea-dhcp4.l
      eases/102.139947519214080] DHCP4_LEASE_AD
      VERT [hwtype=1 4a:80:5f:6e:f0:ce], ci
      d=[01:4a:80:5f:6e:f0:ce], tid=0xb44934b5:
       lease 192.168.100.178 will be advertised
2 2024-06-14T01:13:24.387827422Z stderr F
      2024-06-14 01:13:24.387 INFO [kea-dhcp4.l
      eases/102.139947519214080] DHCP4_LEASE_AL
      LOC [hwtype=1 4a:80:5f:6e:f0:ce], ci
      d=[01:4a:80:5f:6e:f0:ce], tid=0xb44934b5:
```

```
lease 192.168.100.178 has been allocated
for 600 seconds
```

ログファイル 3 の各行の先頭にはタイムスタンプが記述されている．また，各行にクライアントを識別する cid と DHCP メッセージを識別する tid が記述されている．1 行目には MAC アドレスをもとにクライアントに IP アドレス 192.168.100.178 を提供する準備が出来たことが記述されている．2 行目には同じ IP アドレスがクライアントに 600 秒の期間で割り当てられたことが記述されている．

端末所有者を特定するソフトウェア

アドレスリスト，名前のリストをそれぞれ授業ごとに比較し，一意の MAC アドレスと重複した名前から端末所有者の特定を行う．このソフトウェアの名前を identify とし，この流れを図 6 に示す．

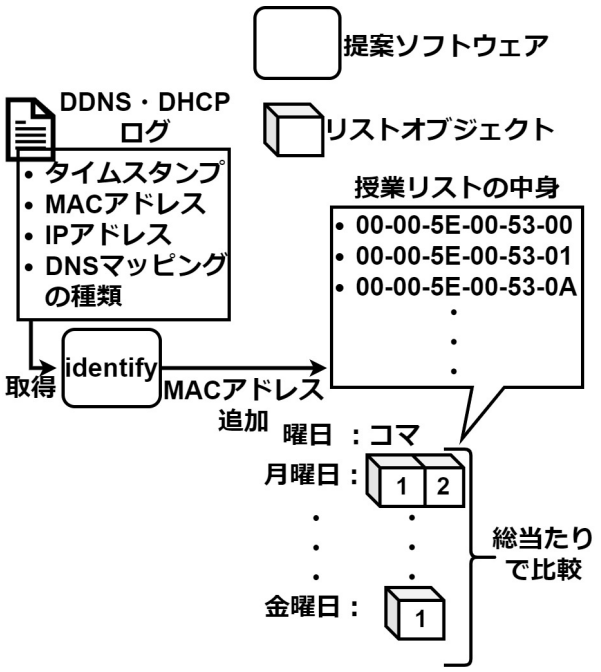

図 6: identify の内容

図 5 で作成した DDNS・DHCP ログの内容を取得する．取得したログのタイムスタンプが 1 時限の始まる 8 時 50 分以前に割り当てられた MAC アドレスを 1 時限のアドレスリストとして保持する．また，このソフトウェアの identify を実行するのは，授業の周期が 1 週間であることから 1 週間に 1 回とする．図 6 のリストオブジェクトの番号はインデックス番号を示し，1 番目は 1 時限，2 番目は 2 時限の授業リストとする．MAC アドレスを授業リストに保持したら，式（1）を用いて総当たりで授業リストの比較を行う．この比較の結果，MAC アドレスが一意になり，メンバーリストの比較で授業の名前が重複していた場合，この MAC アドレスを持つ端末を授業リストの比較で重複した学生の所有物として特定し，この 2 つを出力する．

5. 評価実験

目視で記録した学生の実際の MAC アドレスと提案によって特定した MAC アドレスの正答率と，学生全員を特定できるまでにかかった時間を評価する．

実験環境

実験で使用する環境を図 7 に示す．

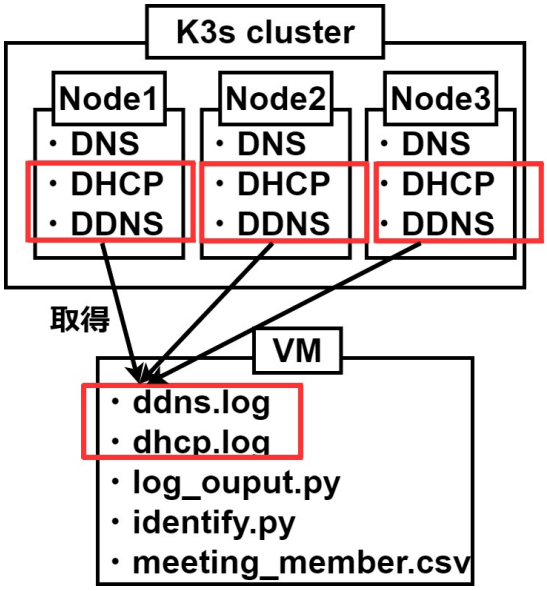

図 7: 実験環境

図 7 で仮想マシン (以下 VM) には Ubuntu22.04 をインストールした．DHCP サーバ，DDNS サーバがあるノードは VM と同じ環境である．DHCP サーバは kea-dhcp4 の 2.5.7 をインストールし，DDNS サーバは kea-dhcp-ddns の 2.5.7 をインストールしている．これらのサーバは K3s によって組み込まれた Kubernetes クラスタ内に，Pod として 3 台配置している．図 7 の赤枠で囲んだ VM 内の ddns.log と dhcp.log は k3s cluster 内の各ノードにある DDNS サーバ，DHCP サーバの Pod のログから取得している．また，Node1，Node2，Node3 はそれぞれマスターノードである．log_output.py はログを整理するソフトウェア，identify.py は端末所有者を特定するソフトウェアである．meeting_member.csv は本稿の提案手法で記述した出席名簿 DB から取得した出席名簿のことである．

基礎実験

実際の研究室の入退室を目視で記録し，DHCP サーバ・DDNS ログと照らし合わせた．CDSL の 1 日における入退室を目視で記録した結果を図 8 に示す．

図 8 のアルファベット a〜o はそれぞれ学生の入退室を示し，空白箇所は外出を意味する．

学生が入室した時刻に割り当てられたアドレスを, DDNS・

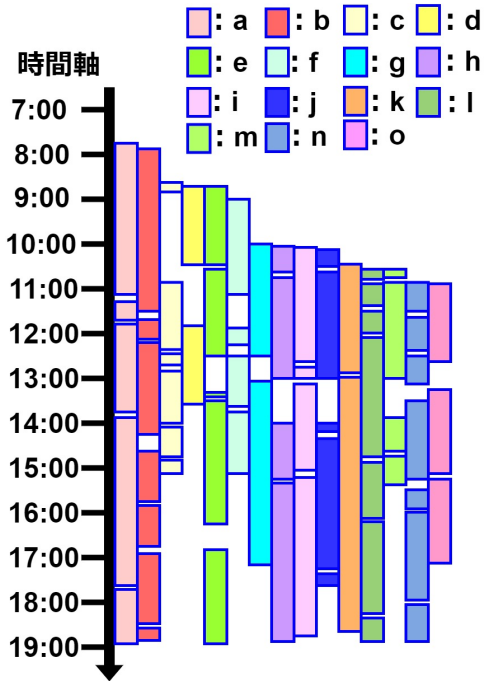

図 8: 研究室の入退室の状況

DHCP ログから取得している．その際の記録を図 9 に示す．図 9 のアルファベット A〜H は DNS・DHCP ログの MAC アドレスで add されてから remove されるまでの時間を示し，アルファベット O〜V は目視で記録した学生の入退室を示す．図 9 のように，複数人が同時に入退室することがあるため，1 日だけでは期間が足りないことが分かった．

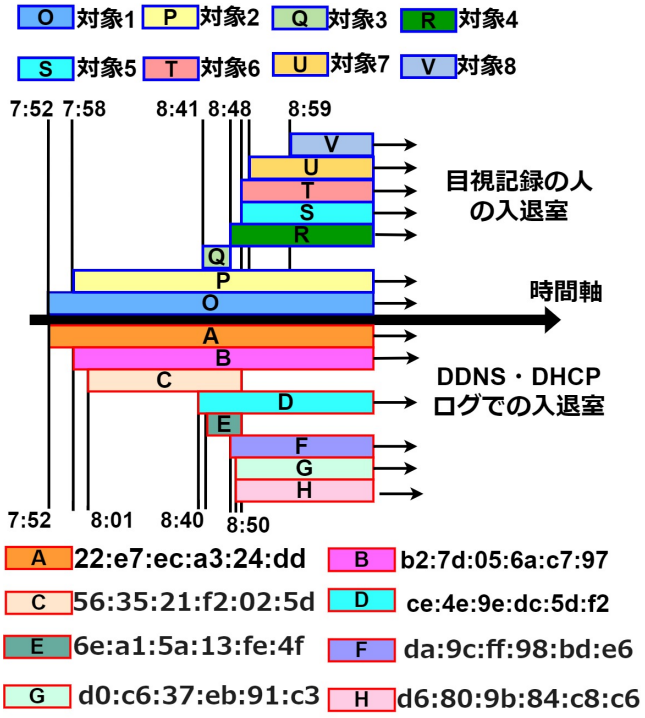

図 9: 基礎実験の結果

6. 議論

無線技術を使用した出席管理の自動化を実現するために，端末所有者を特定することを目的とした．しかし，本稿では出席管理の自動化までを行えていないため，個人の特定以外にも 10 分以内の退出や，研究室内から少しも出ていないのかを判別出来ていない．そのため，DHCP サーバのリースの期間をさらに短くすることで改善可能である．

本稿の提案手法では，全て同じ授業を受講している学生の特定が行えない．この対処として DNS クエリと研究内容で頻出する単語とその特徴を見ることで改善可能である．この対処の流れを図 10 に示す．研究内容は毎週 Cadence

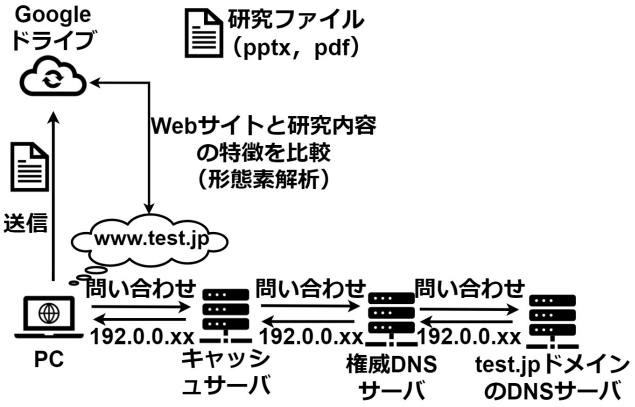

図 10: Web サイトと研究内容の特徴を比較

の授業開始時 Google ドライブへ送信する PowerPoint や PDF を参照する．また，形態素解析を使用して頻度分析を行うことで，研究内容と検索内容の頻出する単語とその特徴を調べる．しかし，この方法が実現可能であれば本稿の提案手法を用いる必要がなくなる．また，テキストにおける特徴量の解析になってしまい，精度が低くなる．加えて，学生が Web サイトで検索することが必須になってしまう．

7. おわりに

課題は DHCP サーバでは端末所有者を特定できないことである．本稿では授業開始時に割り当てられた MAC アドレスと授業ごとの出席名簿の中身をリストとして保持し，同じ時間帯で重複した名前と MAC アドレスを同一人物とすることを提案する．評価実験では学生の実際の MAC アドレスと提案によって特定した MAC アドレスの一致率と，学生全員を特定できるまでにかかった時間の評価を行う．

謝辞

本稿の執筆にあたり，名前と MAC アドレスを提供してくださった東京工科大学コンピュータサイエンス学部の筒井優貴さん，三上翔太さん，山本真也さんに御礼申し上げます．

参考文献

[1] Iio, J.: Attendance management system using a mobile device and a web application, *2016 19th international conference on network-based information systems (NBiS)*, IEEE, pp. 510–515 (2016).

[2] Siew, E. S. K., Chong, Z. Y., Sze, S. N. and Hardi, R.: Streamlining Attendance Management in Education: A Web-Based System Combining Facial Recognition and QR Code Technology, *Journal of Advanced Research in Applied Sciences and Engineering Technology*, Vol. 33, No. 2, p. 198–208 (online), DOI: 10.37934/araset.33.2.198208 (2023).

[3] Jayant, N. K. and Borra, S.: Attendance management system using hybrid face recognition techniques, *2016 Conference on Advances in Signal Processing (CASP)*, pp. 412–417 (online), DOI: 10.1109/CASP.2016.7746206 (2016).

[4] Samet, R. and Tanriverdi, M.: Face Recognition-Based Mobile Automatic Classroom Attendance Management System, *2017 International Conference on Cyberworlds (CW)*, pp. 253–256 (online), DOI: 10.1109/CW.2017.34 (2017).

[5] Salim, O. A. R., Olanrewaju, R. F. and Balogun, W. A.: Class Attendance Management System Using Face Recognition, *2018 7th International Conference on Computer and Communication Engineering (ICCCE)*, pp. 93–98 (online), DOI: 10.1109/ICCCE.2018.8539274 (2018).

[6] Conijn, R., Snijders, C., Kleingeld, A. and Matzat, U.: Predicting Student Performance from LMS Data: A Comparison of 17 Blended Courses Using Moodle LMS, *IEEE Transactions on Learning Technologies*, Vol. 10, No. 1, pp. 17–29 (online), DOI: 10.1109/TLT.2016.2616312 (2017).

[7] Vishwakarma, A.: Virtual private networks, *Network Security Attacks and Countermeasures*, IGI Global, pp. 78–114 (2016).

[8] Hubballi, N. and Tripathi, N.: A closer look into DHCP starvation attack in wireless networks, *Computers & Security*, Vol. 65, pp. 387–404 (2017).

[9] Wachira, F. N.: A Model to detect and prevent rogue DHCP attacks on wireless LAN communication, PhD Thesis, Strathmore University (2021).

[10] Fan, X. and Xia, Z.: A Mutual Authentication Method For Local MAC Address Allocation, *2018 Sixth International Conference on Advanced Cloud and Big Data (CBD)*, pp. 237–242 (online), DOI: 10.1109/CBD.2018.00050 (2018).

[11] Jayavel, S.: NETWORK SECURITY–MAC ADDRESS BLOCK.

[12] Kato, T.: Standardization and Certification Process for “Wi-SUN” Wireless Communication Technology, *Anritsu, Technical Review*, No. 23, pp. 23–04 (2015).

[13] Jindal, V. and Verma, A.: The underlying technologies in WSNs: ZigBee vs. wireless HART, *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, IEEE, pp. 2208–2213 (2015).

[14] Segawa, S., Masuda, H. and Mori, M.: Proposal and Prototype of DNS Server Firewall with Flexible Response Control Mechanism, *2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, pp. 466–471 (online), DOI: 10.1109/SNPD.2019.8935681 (2019).

[15] Lin, K. and Jiang, Z.: Using a Dynamic Domain Name System (DDNS) Technology to Remotely Control a Building Appliances Network, *Proc. Int. MultiConference Eng. Comput. Sci*, Vol. 1, pp. 15–18 (2017).

[16] Jiang, Z.: Analysis of student activities trajectory and design of attendance management based on internet of things, *2016 International Conference on Audio, Language and Image Processing (ICALIP)*, pp. 600–603 (online), DOI: 10.1109/ICALIP.2016.7846537 (2016).

[17] Hack, J. C. V.: I know your MAC address: targeted tracking of individual using Wi-Fi, SpringerLink, pp. 219–227 (2014).

[18] Banepali, A., Kadel, R., Guruge, D. B. and Halder, S. J.: Design and Implementation of Wi-Fi Based Attendance System Using Raspberry Pi, *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–6 (online), DOI: 10.1109/ITNAC46935.2019.9077985 (2019).

[19] Albahrani, A., AL-Ali, Z. A., Al-Ali, Z. Y., Al-Mssri, A. and AL-Shalan, M.: Smart attendance management system, *IJCSNS*, Vol. 22, No. 6, p. 762 (2022).

[20] Korontanis, I., Makris, A., Kontogiannis, A., Varlamis, I. and Tserpes, K.: StreamK3s: A K3s-Based Data Stream Processing Platform for Simplifying Pipeline Creation, Deployment, and Scaling, *SoftwareX*, Vol. 27, p. 101786 (2024).