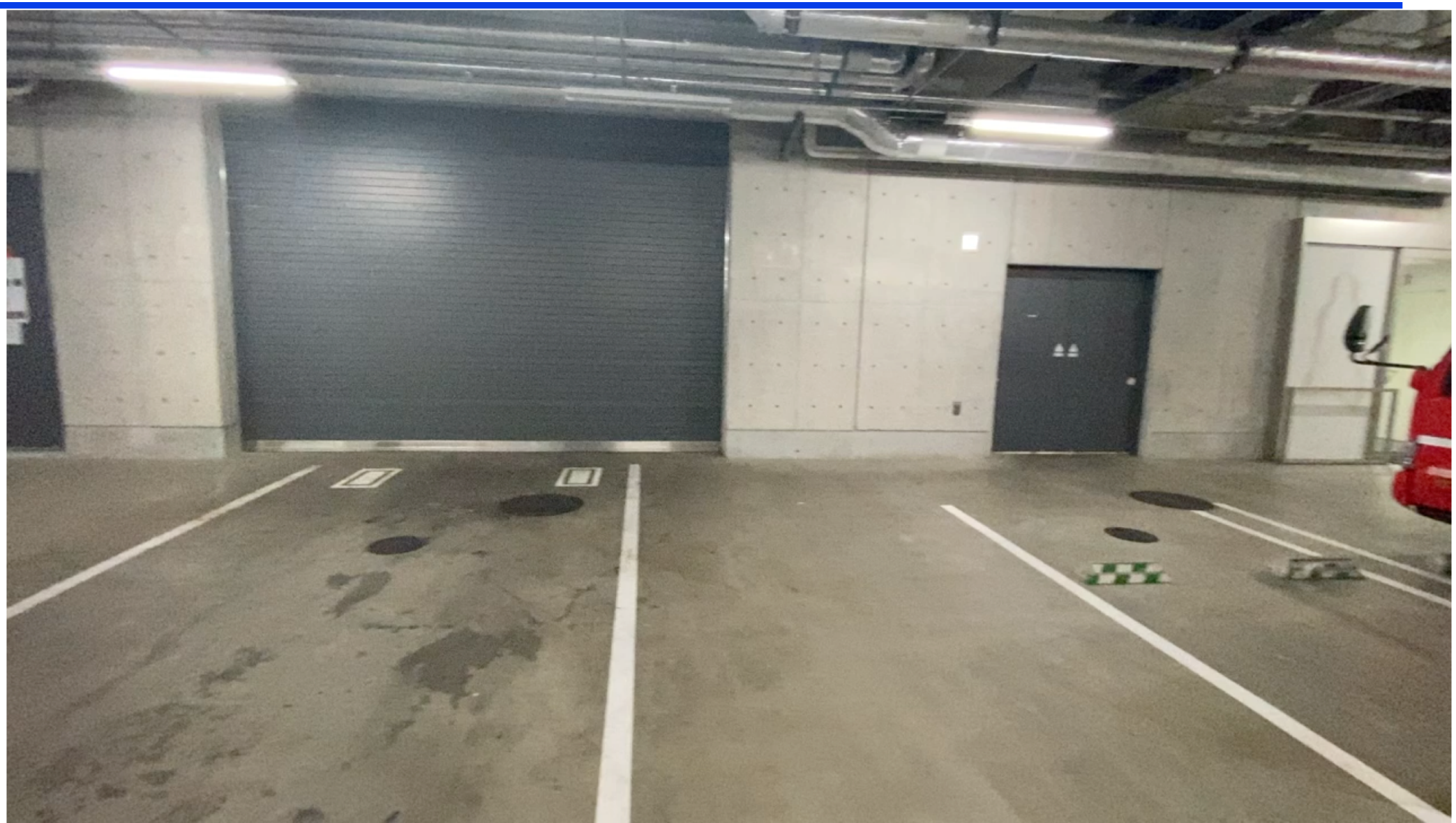
# 偽造 Wi-Fi アクセスポイントによる 現在地情報のスプーフィ ング攻撃の脅威

**菊池研究室　B4 江藤一樹**

# デモ動画

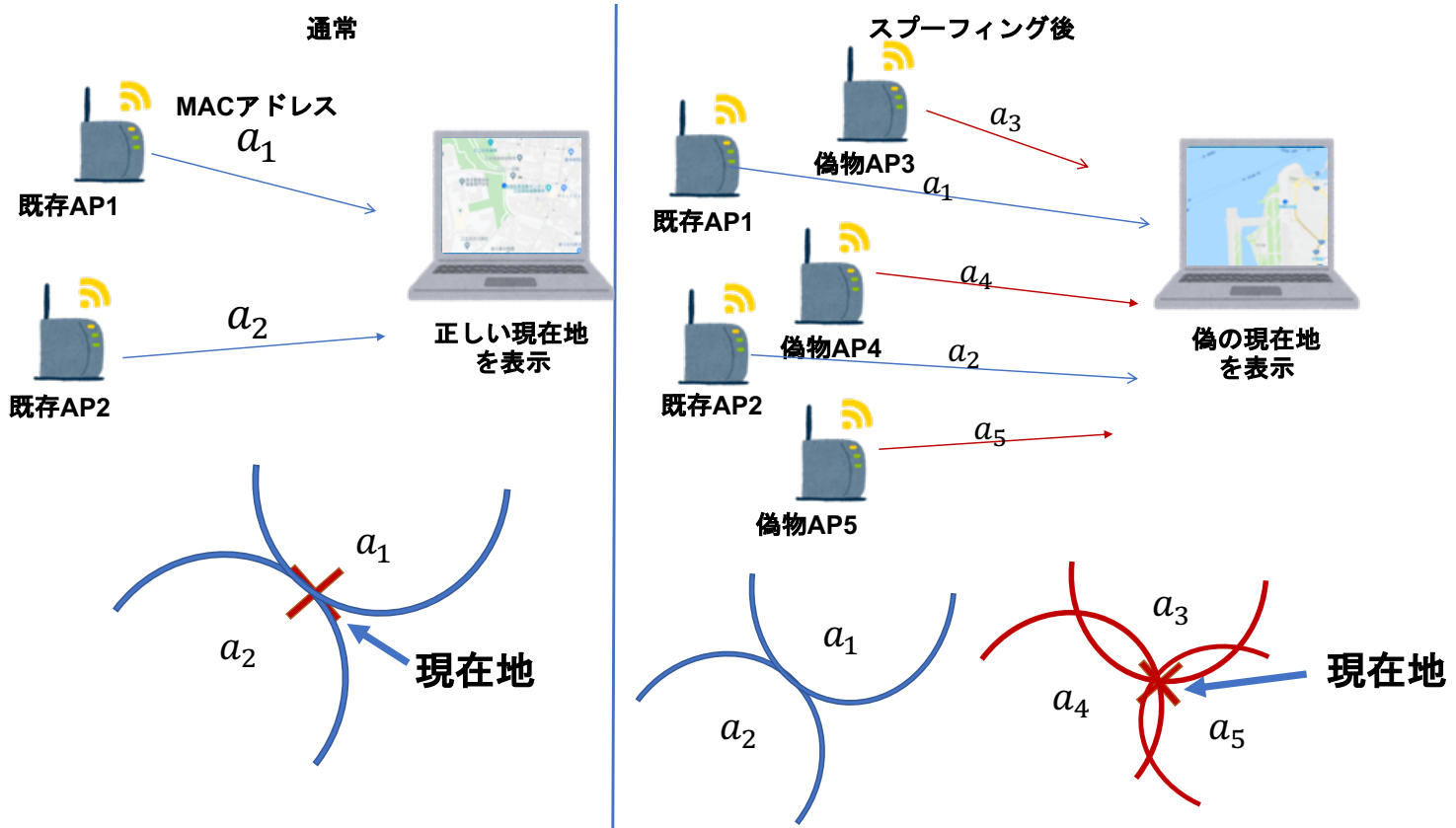


# 背景

- 近年、インターネットサービスによる位置情報の利用が増加した為，位置情報を偽る攻撃への対策が必要である．
  - 2018年11月12日に，店舗に訪れたかのように位置情報を偽り，来店ポイントを不正取得したとして，男が逮捕された
- デバイスは、周囲のアクセスポイントのMACアドレスを利用して、位置を推定している．
- 従って、MACアドレスを偽装した偽のAPを複数設置すると、位置情報が偽装される恐れがある．

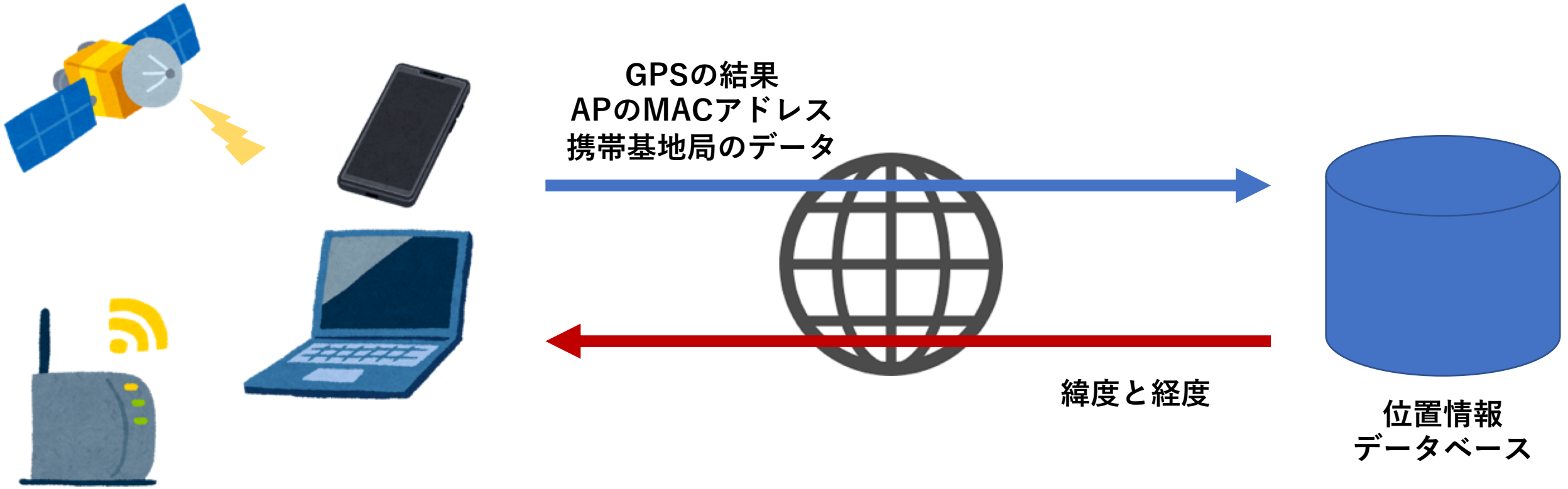
# 提案手法

■攻撃対象のデバイス付近に、異なる場所にあるAPのMACアドレスに偽装した偽のAPを複数設置し、現在地を誤推定させる.



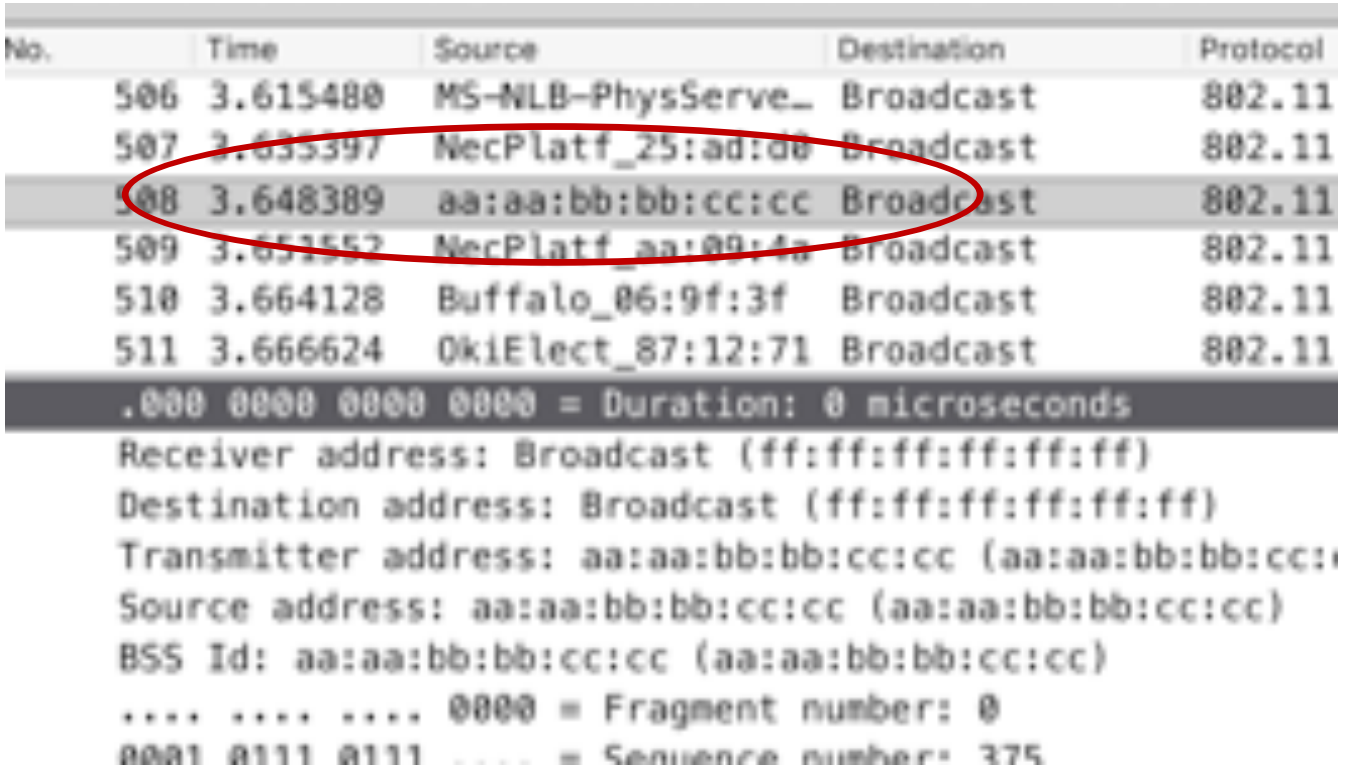
# Geolocation API[1]

- W3C（World Wide Web Consortium）によって標準化された，Webからデバイスの位置情報を取得するAPIである．



# MACアドレスの偽装

- Linuxパッケージのmacchangerを使用する.
- ネットワークインターフェースのMACアドレスを任意な値に変更する.



# 本研究の新規性

1. デバイスに対する位置情報のスプーフィング攻撃のリスクを明らかにすること.
2. 位置が偽造される条件を明らかにする.
3. 位置情報スプーフィング攻撃への対策.

# 実験

- 実験1：PCとスマートフォンによる位置情報の観測とスプーフィング実験.
- 実験2：偽APと対象デバイスの距離，APの数についてのスプーフィング実験.

# 実験環境

- 異なる場所にあるAPのMACアドレスに偽装した偽のAPを5台設置する.
- 実験結果の確認に「Google Maps」と「すかいらーくグループの店舗検索サービス」の2つを利用する.


# 実験1：観測方法

- GPS有りのデバイスにiPhone SE，GPS無しのデバイスにMac book proを使用する．
- 小金井市のたけのこ公園のMACアドレスに偽装する．
- 実験場所は，本研究室，自宅，江古田の森公園付近，本学地下室の四箇所．
- 以下の条件で実験を行う．

| | オフライン | オンライン |
|---|---|---|
| スマートフォン | 機内モード | LTE or ルータ接続あり |
| PC | ルータ接続なし | ルータ接続あり or デザリング |

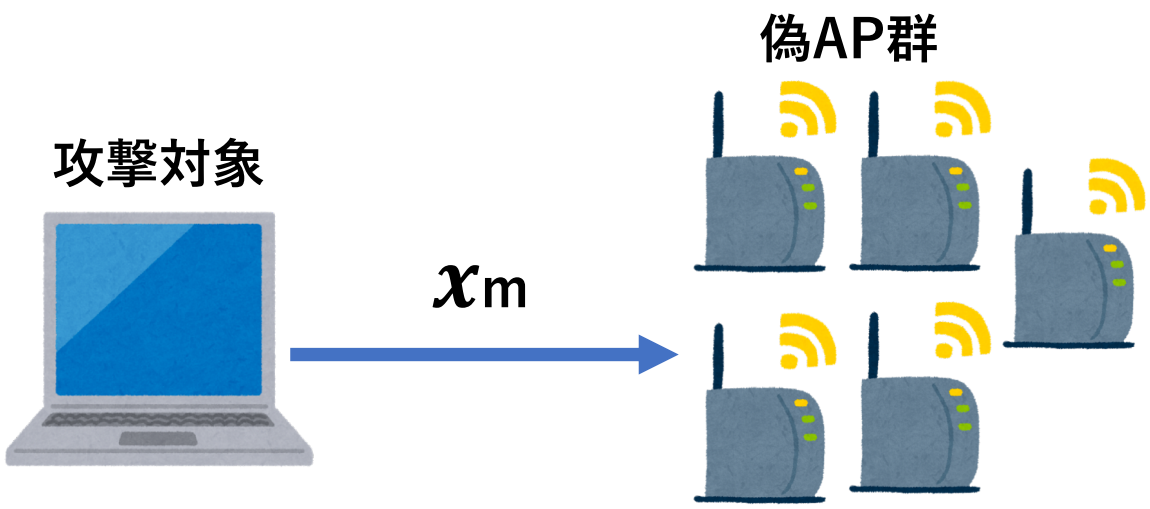
# 実験1：実験方法

- 偽装に使用するAPは，京都府にある法然寺付近，沖縄県の那覇空港，香港の三ヶ所にある．
- 攻撃対象をPCのみ，実験場所を本学地下室．

# 実験2：実験方法

1. 偽APと攻撃対象の距離を0m, 3m, 6m, 9m, 12mに変化させる.
2. 偽APと攻撃対象の距離を0mにし，偽APの数を5~1まで変化させる.

■攻撃対象をPCのみ，実験場所を本学地下室とする.




# 実験1：観測結果

## GPSあり

| 場所 | APの数 | |
|---|---|---|
| | $\mu$ | $\sigma$ |
| 研究室 | 123 | 11.8 |
| 自宅 | 63 | 4.8 |
| 公園 | 19 | 4.8 |
| 地下室 | 2 | 0.4 |

| デバイスの状態 | 実験場所 | Google M |
|---|---|---|
| オフライン | 自宅 | × |
| | 公園 | × |
| | 地下室 | × |

## GPSなし

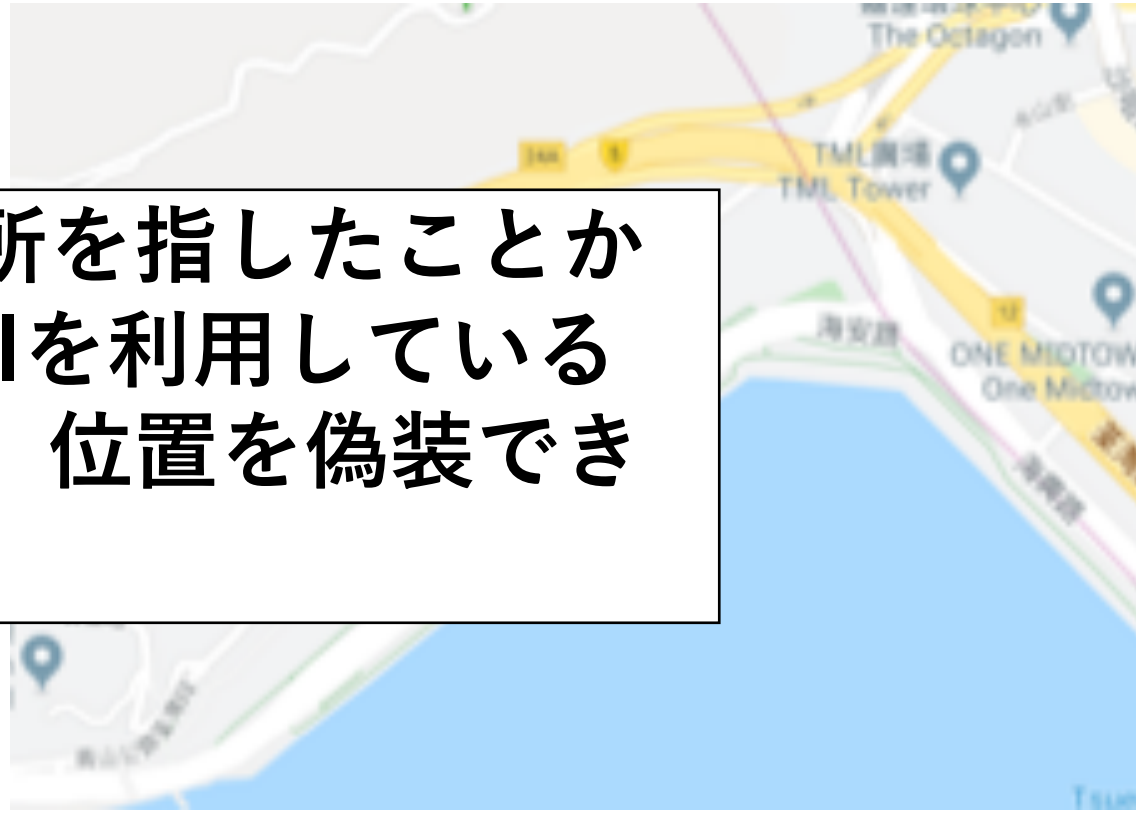
| デバイスの状態 | 実験場所 | Google Map | すかいらーく |
|---|---|---|---|
| オフライン | 地下室 | ○ | ○ |
| | 研究室 | × | × |
| | 自宅 | × | × |
| | 公園 | × | × |
| | 地下室 | ○ | ○ |

位置情報の偽装に最も関係する条件は，既存APと偽APの数と分かる．

# 本研究室でのAP取得結果

| SSID | MACアドレス |
| --- | --- |
| MIND-wireless-ap-bg | 6c:f3:7f:e4:bd:00 |
| White-Kikuchi-5G | 00:1a:eb:82:e0:90 |
| Black-Kikuchi-2G | 00:1a:eb:82:e0:80 |
| arakawa-Lab | 34:3d:c4:4b:ac:c0 |
| keita-lab-device5 | 98:f1:99:b2:c7:47 |
| 0000_MIND_1x | 6c:f3:7f:e4:b7:f9 |

# 実験1：実験結果




**両サイトで同じ場所を指したことから，Geolotion APIを利用しているサービスに対して，位置を偽装できることが分かった．**

**那覇空港**
**（すかいらーく）**

**香港**
**（Google Maps）**

# 実験2：実験結果

| 結果 | 距離[m] | a[dBm] | | a'[dBm] | |
|---|---|---|---|---|---|
| | | $\mu$ | $\sigma$ | $\mu$ | $\sigma$ |
| ○ | 0m | -36.4 | 0.68 | -89.2 | 1.2 |
| ○ | 3m | -55.6 | 4.1 | -85.4 | 1.9 |
| ○ | 6m | -63.6 | 1.8 | -86 | 3.2 |
| ○ | 9m | -66 | 1.4 | -88.6 | 1.0 |
| ○ | 12m | -69.3 | 1.8 | -87.4 | 1.9 |

**位置情報の偽装に必要なのは，既存AP数より多い偽AP数を設置することだと明らかになった．**

| 結果 | 偽AP数 |
|---|---|
| ○ | 5台 |
| ○ | 4台 |
| ○ | 3台 |
| ○ | 2台 |
| × | 1台 |

# 対策

1. GPSの使用を必須にする
2. 多様なリソースからの推定
3. キャッシュ，履歴からの推定

# おわりに

- 位置情報のスプーフィング攻撃の実現可能性を調査し，攻撃のリスクと攻撃を受ける条件を明らかにした.

- 位置スプーフィング攻撃は，MACアドレスを偽装した偽のAPを既存APより多く設置することで実現する.

- 今後の課題
  1. 異なるブラウザによる観測
  2. 既存APと偽APを同数にした実験
  3. サーバに送る内容を明らかにする