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

江藤一樹，菊池浩明　明治大学

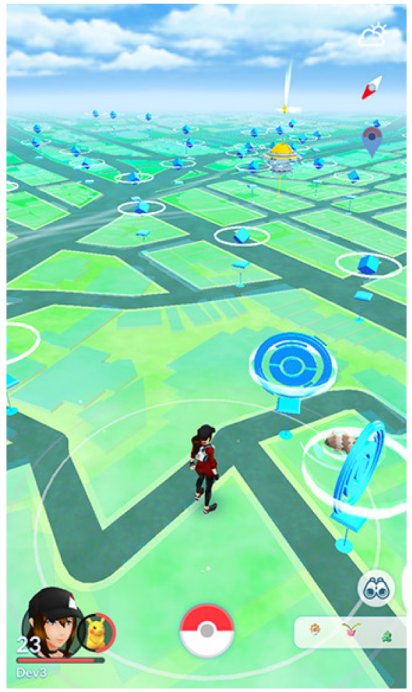
デモ動画

- https://www.youtube.com/watch?v=g7cbriuyfsM&feature=youtu.be

背景「位置情報の脅威」

- 位置情報を利用したアプリが増加
- 位置が偽装されると，以下の応用に被害が生じる

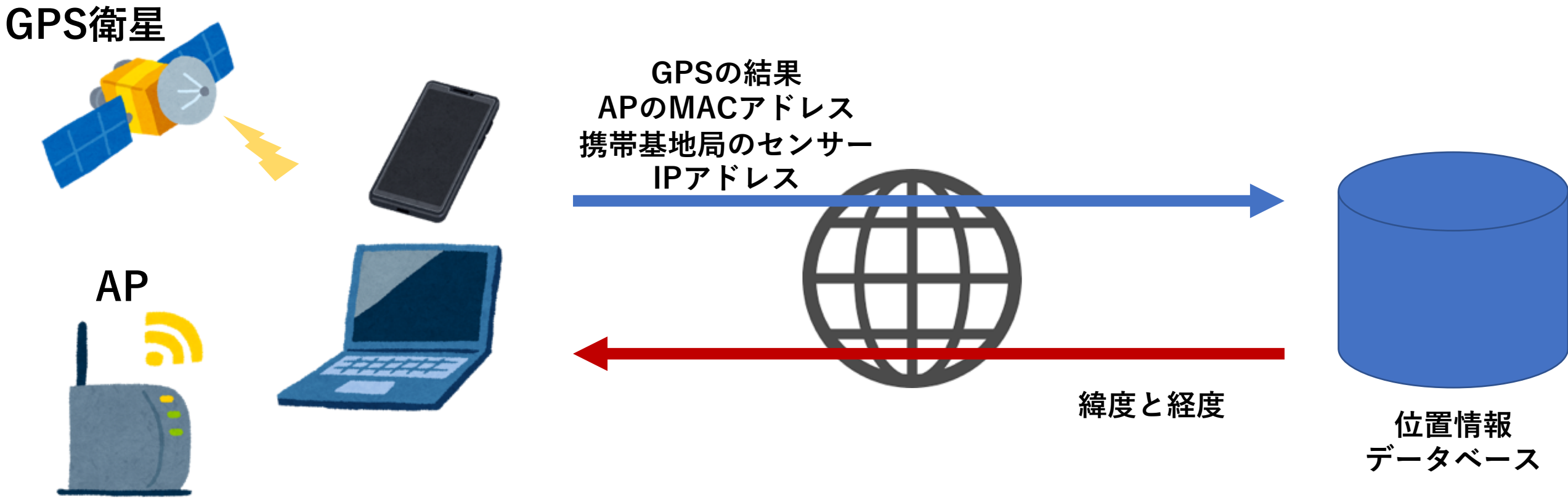
例1：ポケモンGo



例2：カーナビ

位置推定の仕組み：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．**

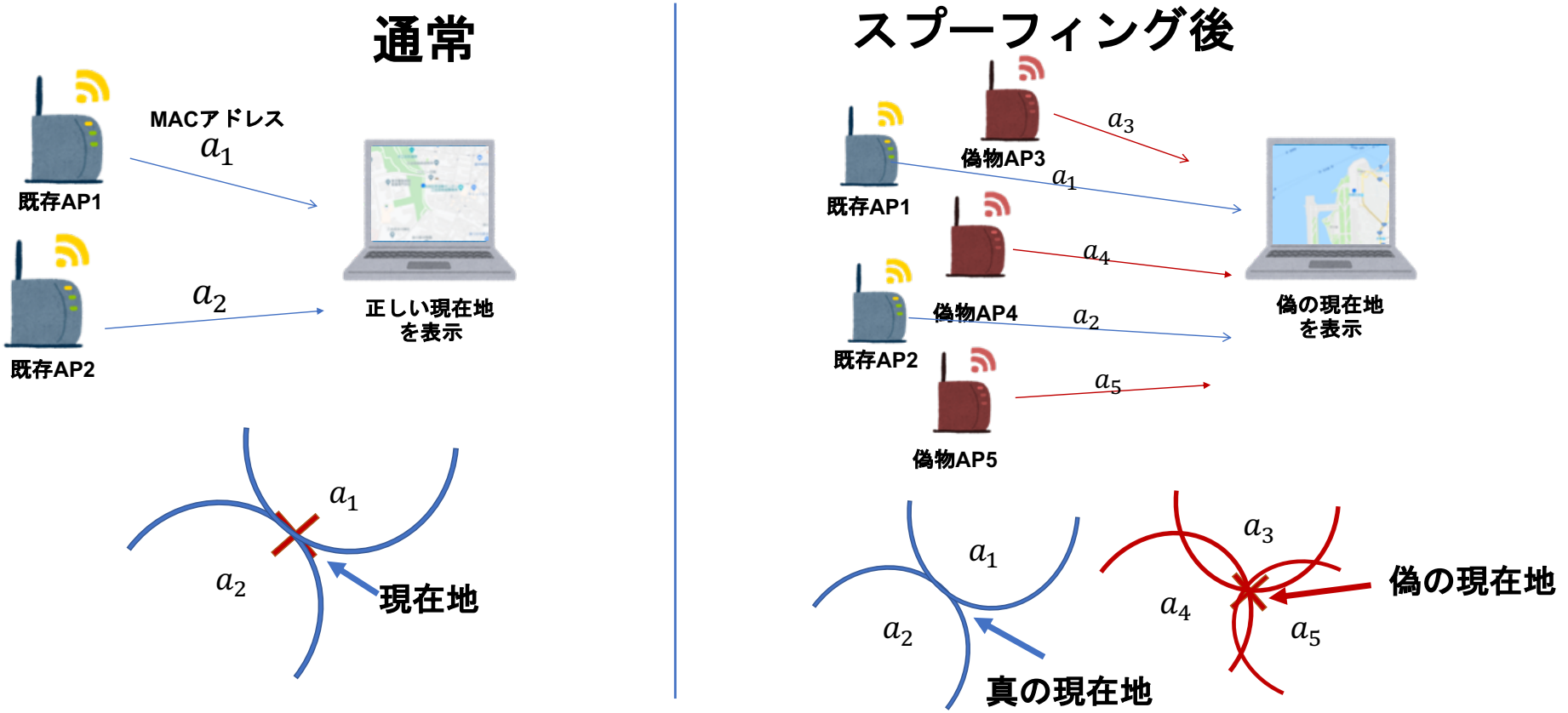


本研究の目的

1. 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を検討する.

偽装手法

■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.



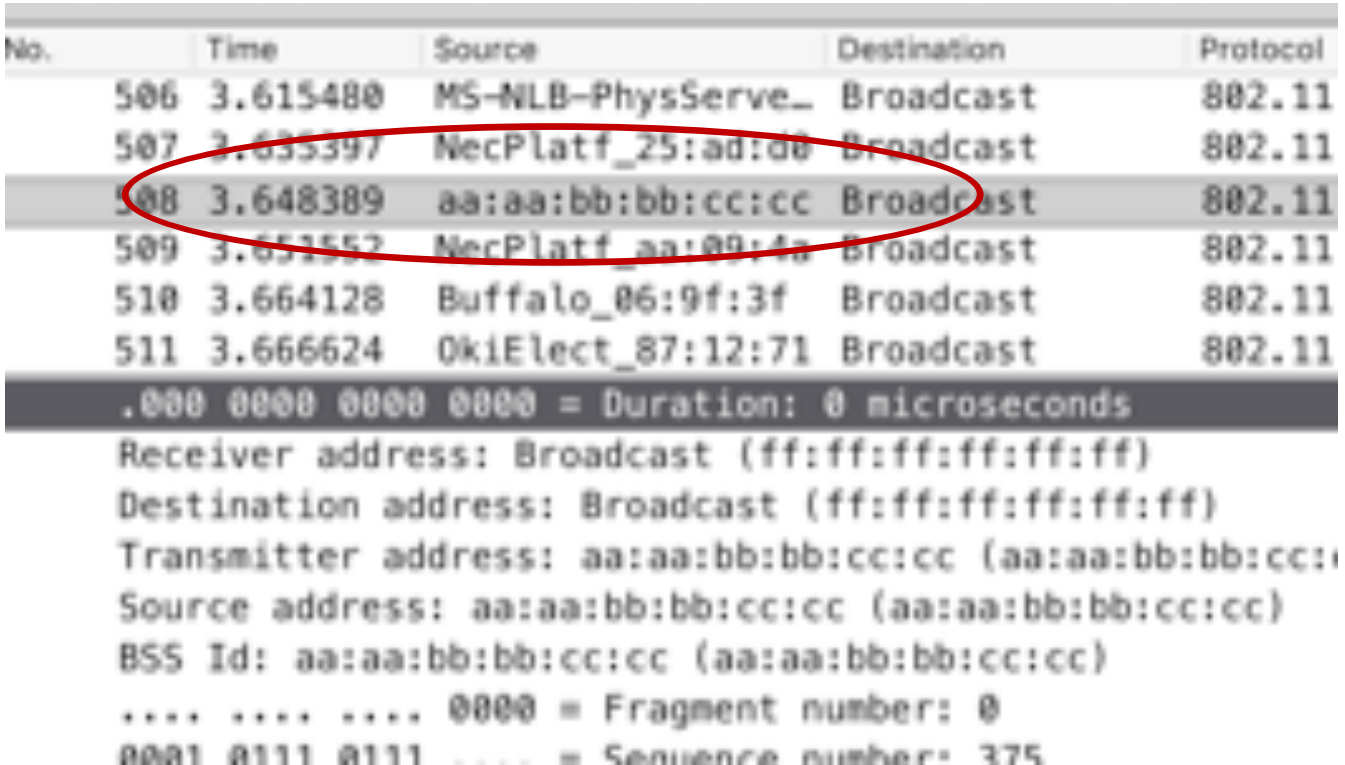
AP情報の取得

- macOSの"airport"コマンド：APの数と情報を取得する.
- デバイス周辺にあるAPのSSID，MACアドレス，信号強度，チャンネルを含む7つの情報が表示する.

```
➜  ~ airport -s
                            SSID BSSID             RSSI CHANNEL HT CC SECURITY (auth/unicast/group)
                      HUMAX-02B7D-A cc:4e:ec:70:2b:82 -81  136,-1  Y  JP WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                      HUMAX-21388-A 90:f3:05:a2:13:94 -90  116     Y  JP WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                      HUMAX-ED9CF-A 90:f3:05:9e:d9:d4 -56  112,-1  Y  JP WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                    9CB2B23F61C4-5G 9c:b2:b2:3f:61:c7 -77  100     Y  JP WPA(PSK/AES/AES) WPA2(PSK/AES/AES)
                    rs500k-8712d1-3 00:25:36:87:12:b1 -86  100     Y  JP WPA2(PSK/AES/AES)
                         HUMAX-02B7D cc:4e:ec:70:2b:8a -79  11      Y  JP WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                         HUMAX-21388 90:f3:05:a2:13:8c -72  11      Y  -- WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
```

MACアドレスの偽装

- **Linuxパッケージのmacchanger.**
  - **MACアドレスを任意な値に変更する.**



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.
- 環境：　Google Maps　　すかいらーく

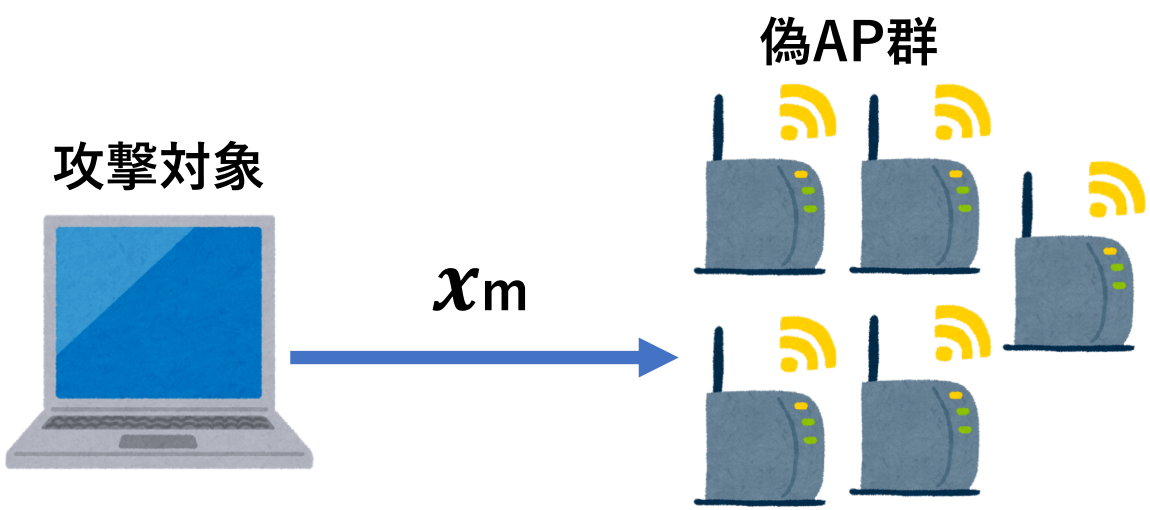
実験1：実験条件

- デバイス：iPhone SE (GPS有り)， Mac book pro(GPS無し).
- 偽装先：たけのこ公園，(京都府)法然寺，(沖縄県)那覇空港，香港郊外.
- 偽装元：本学研究室，本学地下室，自宅(高円寺)，江古田の森公園.

	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2：実験方法（偽装条件）

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.



実験1：実験結果

GPSあり

デバイスの状態	実験場所	既存APの数		Google Map	すかいらーく
		μ	σ		
オンライン	研究室	123	11.8	×	×
	自宅	63	4.8	×	×
	公園	19	4.8	×	×
	地下室	2	0.4	×	×
オフライン	研究室	123	11.8	×	×
	自宅	63	4.8	×	×
	公園	19	4.8	×	×
	地下室	2	0.4	×	×

実験1：実験結果

GPSなし

デバイスの状態	実験場所	既存APの数		Google Map	すかいらーく
		μ	σ		
オンライン	研究室	123	11.8	×	×
	自宅	63	4.8	×	×
	公園	19	4.8	×	×
	地下室	2	0.4	○	○
オフライン	研究室	123	11.8	×	×
	自宅	63	4.8	×	×
	公園	19	4.8	×	×
	地下室	2	0.4	○	○

実験1：偽装例

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]	偽AP信号強度 [dBm]		既存AP信号強度 [dBm]		既存AP数	偽AP数
		μ	σ	μ	σ		
○	0m	-36.4	0.68	-89.2	1.2	2	5
○	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．

結果	偽AP数	既存AP数	距離
○	5台	2	
○	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(GPS，基地局，WiFi)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，APが少ない場所では位置が偽装されるリスクがあることを示した.
- 位置スプーフィング攻撃を受ける以下の条件である.
  1. MACアドレスを偽装した偽のAPが既存APより多く設置されていること
  2. GPSの信号を受信しないこと
- 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. Locaiton APIのサーバに送る内容を明らかにする