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 †

明治大学総合数理学部 †

1　はじめに

近年，スマートフォンの普及に伴い，ゲームや食事サイトなどのインターネットサービスで，位置情報の利用が増え，社会インフラとして必要性が高まった．その一方，GPS への攻撃として，スプーフィング攻撃の脅威が指摘されている [1]．これを受けた GPS は実際にいる位置とは異なる位置を示し，社会インフラの混乱を引き起こす原因となる．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，イオンアプリの来店ポイントを不正取得したとして，男が逮捕された [2].

デバイスは，周囲にあるアクセスポイント（AP）の MAC アドレスをサーバに送信し，AP の情報が格納されているデータベースと照合して，位置情報を推定する．従って，偽装された偽の MAC アドレスを与えられるとデバイスの現在位置を操作されてしまう恐れがあると考えられる．

そこで，本稿ではこの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する．

2　提案手法

本研究で検証する位置スプーフィング攻撃は，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 を複数設置することにより，現在位置を誤推定させることで実現する．

Geolocation API[3]

W3C 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．JavaScript の navigator.geolocation オブジェクトを通じて提供される．デバイスがこのオブジェクトに対してメソッドを実行する時に，実行したデバイスの周囲にある Wi-Fi の MAC アドレス，GPS の情報などを API を介して，サーバーにリクエストを送り，位置情報を取得する．

MAC アドレスの偽装

ネットワークインターフェイスの MAC アドレスを任意な値に変更する Linux のパッケージである macchanger[4] を使用する．

Fake Wi-Fi Access Points Exploit for spoofing current location

†Kazuki Eto and Hiroaki Kikuchi, School of Interdisciplinary Mathematical Science, Meiji University.

表 1　実験場所の AP 数

場所	AP の数	
	μ	σ
研究室	123	11.8
自宅	63	4.8
公園	19	4.8
地下室	2	0.4

3　実験

3.1　実験環境

位置スプーフィング攻撃が成功するためには，既に存在する AP 数を上回る必要があると仮定し，偽 AP を 5 台用意する．

本研究では，ユーザの現在地を地図上に表示する次の 2 つのサイトを利用する．Googole 社が提供している地図サービス “Google Maps”．すかいらーくグループの公式サイトが提供している「ガスト店舗検索」サービスである．

3.2　実験方法

（実験 1）位置スプーフィング実験

スマートフォンと PC をオンライン，オフラインの二つの状態にし，位置スプーフィングの影響を受けるか調べる．観測場所は，本研究室，自宅，江古田の森公園付近，本学地下室である．偽 AP が偽装する MAC アドレスは，東京都小金井市のたけのこ公園付近にある AP の MAC アドレスである．

他の場所の AP の MAC アドレスに変えて偽装が可能か調べる．偽装に使用する AP は，京都府と沖縄県，香港にある．攻撃対象を PC のみ，実験場所を本学地下室とする．

（実験 2）AP 数とデバイス間の距離

偽 AP と攻撃対象の距離を 0m，3m，6m，9m，12m と変化させた時の信号強度と偽装結果を調べる．偽 AP と攻撃対象の距離を 0m にし，偽 AP の数を 5~1 まで変化させて，位置情報が偽装されるか否かを調べる．攻撃対象を PC のみ，実験場所を本学地下室とする．

3.3　実験結果

（実験 1）観測場所の AP 数を表 1，オンライン時の位置情報の観測結果を表 2 に示す．オフラインでも同様の

表 2　実験結果

GPS	実験場所	Google Map	すかいらーく
あり	研究室	×	×
	自宅	×	×
	公園	×	×
	本学地下室	×	×
なし	研究室	×	×
	自宅	×	×
	公園	×	×
	本学地下室	○	○

図 1　実験 1 の偽装結果（那覇）

結果である．ここでの○は偽装されたこと，×は正常の位置推定が行われたことを示す．位置情報が偽装されたのは，本学地下室で PC を対象とした時だけである．その為，位置情報の偽装に最も関係する条件は，既存 AP と偽 AP の数である．スマートフォンに対する位置情報が偽装されないのは，AP の情報ではなく，GPS か携帯基地局のセンサーに基づいて位置を推定していると考えられる．

PC による実験では，京都，沖縄，香港の位置スプーフィングができ，結果例を図 1 に示す．

（実験 2）距離を変えた実験結果を表 3 に示す．複数ある既存 AP と偽 AP から 1 台ずつ選択した結果であり，a が偽 AP，a' が既存 AP を示す．偽 AP の数を変えた実験では，偽 AP が 1 台の時に正常な位置情報を指し，2~5 台の時は位置が偽装された．両結果から位置情報の偽装に必要なのは，既存 AP より多い偽 AP を設置することだと分かる．

3.4　考察

GPS の電波が届きにくい地下室の実験では，位置情報の精度は悪くなるが，実験場所付近を指す．従って，GPS ありのデバイスの位置情報が偽装されないのは，位置情報の推定に AP の結果より GPS の結果を優先していることだと分かる．

京都，沖縄，香港に偽装されたことから，AP の MAC アドレスがデータベースに格納されていれば，偽装がされる場所に制限ないと考える．

既存 AP の信号強度は非常に弱い電波であるが，既存 AP が偽 AP の数を上回った時に，実験場所付近を指したことから，位置スプーフィングに信号強度が関係しないと考える．その為，電波を拾えれば 12m より距離を離しても偽装がされてしまうリスクがある．

表 3　距離を変えた実験結果

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

4　対策

本リスクへの対策は，GPS の使用を必須にする，多様なリソースからの推定，キャッシュ，履歴からの推定の三つである．本研究で，GPS が搭載されているデバイスに対する偽装がされなかったことが示された．従って，位置情報を利用するデバイスに GPS を搭載することが効果的である．しかし，より安全に位置推定をするために，位置情報に使えるリソースを複数組み合わせる必要がある．スプーフィング攻撃により位置情報が急に変化した時，キャッシュや履歴から現在地を推定するか，ユーザに対して警告を送るべきである．

5　おわりに

本研究では，インターネットサービスで利用される現在地を取得する機能に対して，位置スプーフィング攻撃の実現可能性を調査し，攻撃のリスクと条件を明らかにした．位置情報の取得に，デバイス周辺にある AP の MAC アドレスが利用されていることから，既存 AP の数を上回る MAC アドレスを偽った AP を設置することで，GPS を搭載していないデバイスの位置情報が偽装されることが分かった．

参考文献

[1] 海老沼，”GPS 信号の脆弱性と今そこにある危機”，中部大学工学部紀要，2017.

[2] 朝日新聞デジタル，“イオンから来店ポイント詐取容疑　ＰＣで位置情報偽装”，2018 年 11 月 12 日.

[3] Geolocation API Specification 2nd Edition（https://www.w3.org/TR/geolocation-API/，2019 年 12 月参照）

[4] ubuntu manuals（http://manpages.ubuntu.com/ manpages/bionic/man1/macchanger.1.html，2019 年 12 月参照）