MAC認証や位置情報が使えなくなる！？ Private MACアドレス説明と影響について

iOS 14/Android 10,11/Windows 10

シスコシステムズ合同会社/WiBiz技術調査委員会
前原　朋実
2021/01/22

注意

- 現在わかっている情報に基づいての説明となります。
- 今後、内容について追加・修正される可能性があります。

説明内容

- 以前の Random MAC おさらい
- Private MAC の概要
- 採用に至った経緯
- 各社どのような実装？
- 影響を受けそうな製品/技術
- まとめ

以前の Dummy MAC(iOS 7), Random MAC(iOS 8) おさらい

[iOS7 の Dummy MAC]

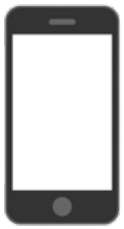
- **アプリがMACアドレスを取得しにいくとダミーのMACアドレスを返します**
- SSID に繋いでいない状態ではアプリは自身の端末の MACアドレスが分かりません
- 一度 SSID に接続すると、CMX/MSEが 端末のMAC/IP情報をアプリサーバに通知、端末アプリはアプリサーバから自身の実MACを取得し位置情報を得ることができます

[iOS8 の Random MAC]

- **802.11 プローブに対して MAC アドレスをランダム化、ロケーションマスキングを提供**
- Random MAC には Locally Administered MAC アドレスを使用
- SSID に繋いでいない状態では、63秒毎にMACが変化
- SSID に接続している場合、実MACで通信
- CMXやDNA Spaces では、Locally Administered MAC アドレスをフィルタ可能（一部、無接続クライアントの分析に制限あり）

Private MAC(iOS14) の概要

今までと何が違う？



Private MAC対応デバイス：32:28:6D:51:13:AF
実際のWi-Fi MACアドレス：~~00:11:22:33:44:55~~

SSID毎に Private MAC に上書きされて通信する

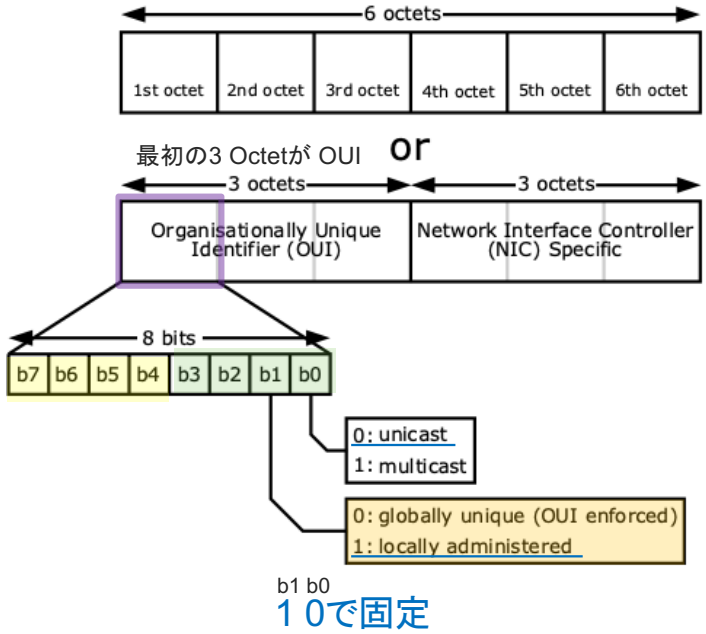
iOS14からは、実際のMAC アドレスではなく、ランダム化で選択された Private MACアドレスを使い通信を行うように変更されます。（Default で有効）
SSID 毎に異なる Private MACアドレスを使用します。
デバイス側の設定変更により、Private MAC を無効にすることも可能です。

Private MAC を詳しく

Private MAC になったと区別できるか？

Private MAC は IEEE802.11 RCM (Random & Changing MAC address) Study Group で策定している内容に基づいています。但し、MACアドレスをアサインするアルゴリズムについては各OSメーカに依存します。

[MACアドレスのOctet]



By Inductiveload, modified/corrected by Kju - SVG drawing based on PNG uploaded by User:Vtraveller. This can be found on Wikipedia here., CC BY-SA 2.5, https://commons.wikimedia.org/w/index.php?curid=1852032

[Private MAC の特徴]

- 32-28-6D-51-13-AF
- 56-EF-68-F6-0D-30
- 0A-13-A8-8E-B5-EF
- AE-83-37-55-A7-22

これら1オクテット目と、残りのオクテットがランダムに割り当てられます

02-	32-	62-	92-	C2-	F2-
06-	36-	66-	96-	C6-	F6-
0A-	3A-	6A-	9A-	CA-	FA-
0E-	3E-	6E-	9E-	CE-	FE-
12-	42-	72-	A2-	D2-	
16-	46-	76-	A6-	D6-	
1A-	4A-	7A-	AA-	DA-	
1E-	4E-	7E-	AE-	DE-	
22-	52-	82-	B2-	E2-	
26-	56-	86-	B6-	E6-	
2A-	5A-	8A-	BA-	EA-	
2E-	5E-	8E-	BE-	EE-	

特徴として、MACアドレスの頭から2番目は2,6,A,E が割り当てられます。

[なぜ2,6,A,E？]

b7 b6 b5 b4 b3 b2 b1 b0

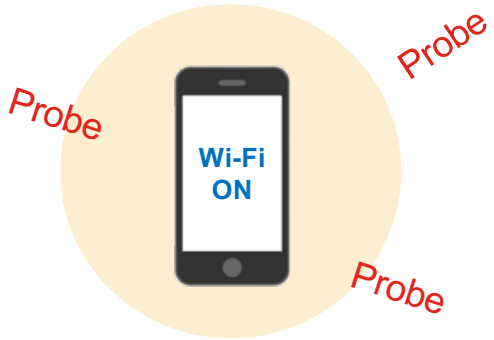
x x x x 0 0 1 0 = X2
x x x x 0 1 1 0 = X6
x x x x 1 0 1 0 = XA
x x x x 1 1 1 0 = XE

2進表記　16進表記

MACアドレスの最初の2つを表す 8bit のうち最後の2つが 1 0（b1の1は locally administered = Random MAC, b0 の 0 は unicast) となり固定されますので、b2 と b 3 で 0 or 1 の組み合わせで 16進表記にすると 2,6,A,E となります。

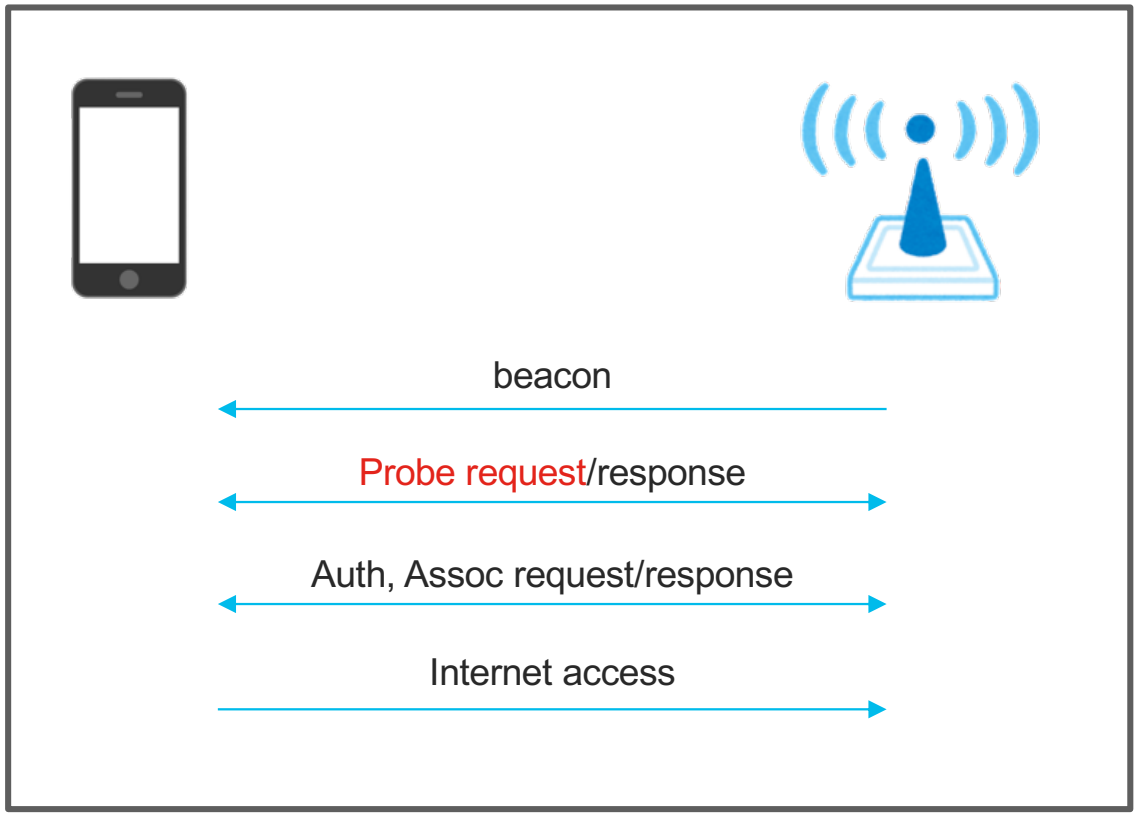
Private MAC 採用に至った経緯

提供者と利用者の認識とズレがありそうなところ



Wi-Fi 設定がデバイスでONになっているだけでプローブと呼ばれるSSIDを検索するフレームが送信され、これを取得して位置情報を取得することができます。

フリー Wi-Fi に接続しようとする人は個人情報を意識することはあっても、無意識に Wi-Fi が ON になっている人は位置情報を提供しているという認識がないかもしれません。



Private MAC 採用に至った経緯

一般利用者の認識と今回のデバイスメーカーの対応

[利用者、端末デバイスメーカーの意見]

- デバイスで Wi-Fi を ON にしていると、MACアドレスをもとに位置情報を取得されている。
- MACアドレス はデバイス固有、何となく人に紐づいていそうで、プライバシーを守りたい。

日本におけるMACアドレスの扱い

MACアドレスって個人情報？

【図表2－3：電気通信事業者が取り扱う位置情報の概要】

	基地局に係る位置情報		GPS位置情報	Wi－Fi位置情報	
	個々の通信の際に利用される基地局の位置情報	位置登録情報		端末利用者とアクセスポイント設置者間の通信に基づく位置情報	端末利用者がアクセスポイントから外部と通信を行うことで把握される位置情報
概　要	個々の通信の際に把握される利用者の基地局に係る位置情報	移動体端末が着信等を行うために、移動体端末がどの基地局のエリア内に所在するかを明らかにするため、自動的に取得される位置情報	携帯端末のGPS機能により端末の具体的所在地を示す情報。利用者が当該情報を取得する機能・サービスを利用する際に取得される。	端末がアクセスポイントと接続し、外部と通信を行う前提として、端末がMACアドレス等をアクセスポイントに送信することにより把握可能な位置情報	端末が特定のアクセスポイントと接続し、外部と通信を行うことにより、把握可能な位置情報
通信の秘密・個人情報への該当性、他の識別情報との結びつき	・電気通信事業者にとって、通信の秘密に該当する。 ・携帯電話事業者の契約者情報と紐づくことから個人情報	・携帯電話事業者の契約者情報と紐づくことから個人情報	・他の個人情報と紐づく場合、個人情報	・他の個人情報と紐づく場合、個人情報 ・MACアドレスと紐づく。	・電気通信事業者にとって、通信の秘密に該当する。 ・他の個人情報と紐づく場合、個人情報 ・MACアドレスと紐づく。
取得の経緯	・通信時に取得される。	・通信の前提として取得される。	・利用者が当該情報を取得する機能・サービスを利用する際に取得されるが、設定によりバックグラウンドで取得されることもある。	・通信の前提として取得される。	・通信時に取得される。
精　度	基地局単位（数百メートル～）		緯度経度情報（数メートル～）	アクセスポイント単位（数メートル～）	
利用者の認識	・通信目的で取得・利用されることについては、予測可能と考えられる。	・携帯電話を使用していなくても、基地局に位置情報を把握されていることについて、利用者の理解が及んでいない可能性がある。	・位置情報を利用することが明らかなサービスを自ら利用する際は、その取得・当該サービスにおける利用について予測可能と考えられる。	・Wi－Fi通信を利用していなくても、アクセスポイントにMACアドレス等が取得されていることについては、利用者の理解が及んでいない。	・通信目的で取得・利用されることについては、予測可能と考えられる。

位置情報の基となるプローブリクエスト及び接続要求(Wi-Fi端末がアクセス ポイントに接続するために送信する信号、以下「プローブリクエスト等」という。) の情報は、Wi-Fiという通信システムの仕様上、通信を成立させる前提として アクセスポイント設置者に取得されていると考えられる。

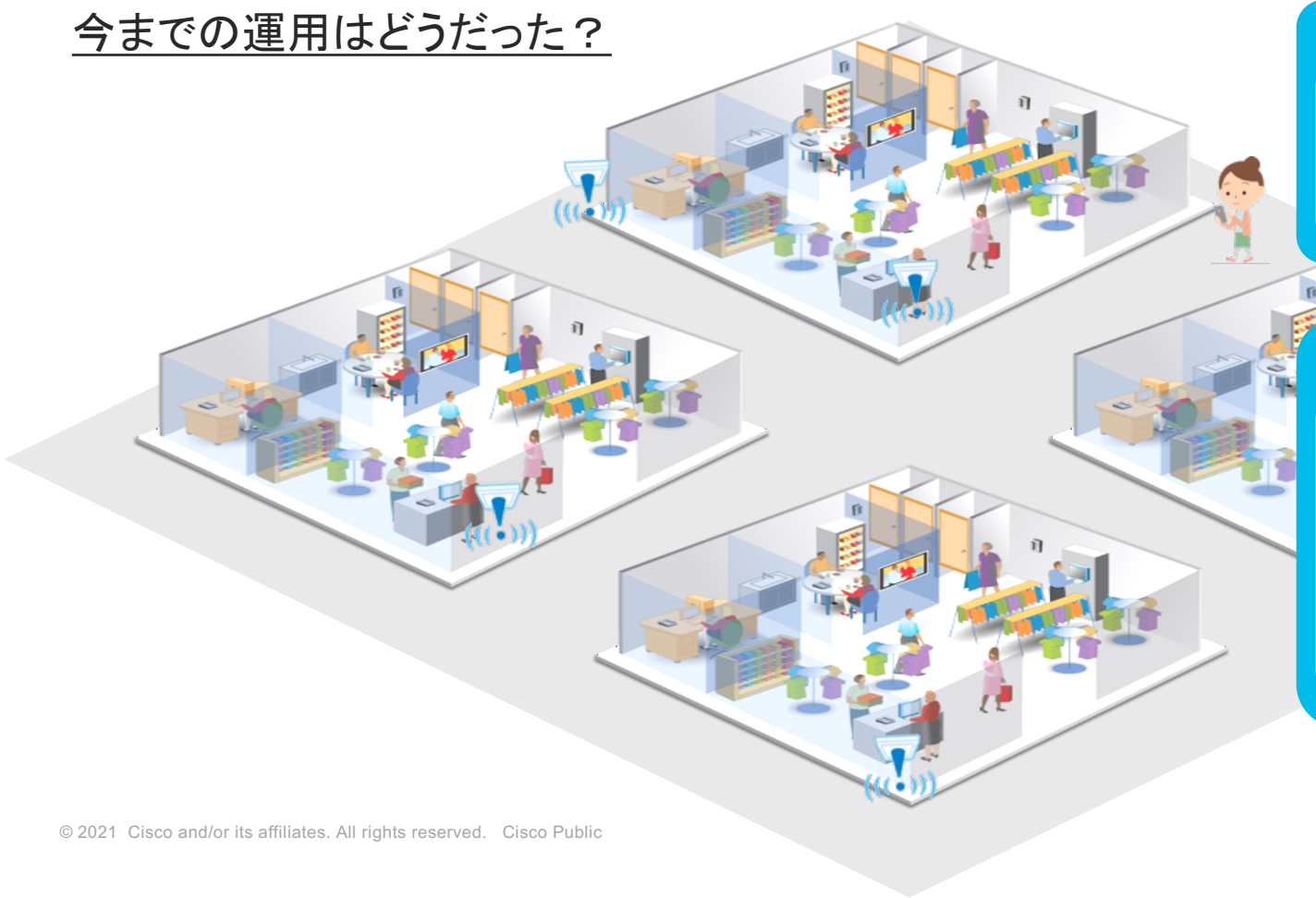
・プローブリクエスト等の情報に含まれるMACアドレスは、端末やアクセスポイ ント等のネットワーク機器に原則として一意に割り当てられ、利用者側では変 更困難なものである[80]。

MACアドレスは、単体では個人識別性を有しないが、 総務省パーソナルデータ研究会報告書においては、「個人のPCやスマートフ ォン等の識別情報(端末ID等)などは、一義的にはPCやスマートフォンといっ た特定の装置を識別するものであるが、実質的に特定の個人と継続的に結び ついており、プライバシーの保護という基本理念を踏まえて判断すると、実質 的個人識別性の要件を満た」すものとされ[81]、SPIにおいては、MACアドレス 等の契約者・端末固有IDについて、単体では個人識別性を有しないが、同一I Dに紐付けて行動履歴や位置情報を集積する場合、プライバシー上の懸念が あるとされ、「個人情報に準じた形で取り扱うことが適切」とされた[82]。また、見 直し方針においても、「保護されるパーソナルデータの範囲については、実質 的に個人が識別される可能性を有するもの」とするとされている[83]ことから、プ ローブリクエスト等の情報に含まれる端末のMACアドレスは、実質的な個人 識別性を有するものとして、今後個人情報保護法上保護される情報として取り 扱われる可能性がある。

総務省　位置情報プライバシーレポート
https://www.soumu.go.jp/main_content/000434727.pdf

日本におけるこれまでのMACアドレスを利用したWi-Fi位置情報の扱い

今までの運用はどうだった？



システム側

- データベースをハッシュ化
- 定期的にデータを削除
- オプトアウト実装、など

ユーザ向け対応

- 張り紙、Web画面等で Wi-Fi における位置情報収集に関する説明を明記
- IDなど他の個人情報と紐づく場合、ユーザに同意を得る仕組みを提供

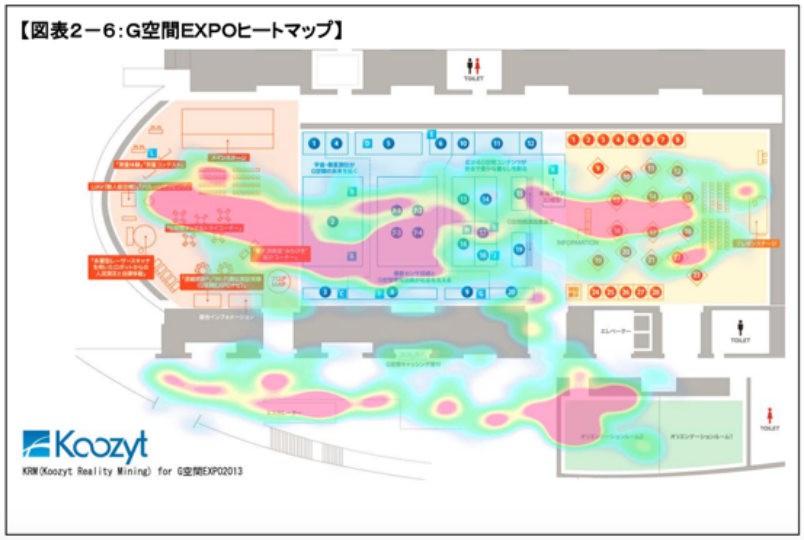
日本におけるこれまでのMACアドレスを利用したWi-Fi位置情報の扱い

今までの個人情報に対する対応は？(イベント会場の対応例)

[個人を特定できない形で位置データを表示]

一方で、実証実験では、アプリを利用していない来場者のプローブリクエスト等も取得し、Wi－Fi位置情報を収集してしまう性質上、G空間EXPOナビの利用に関する注意をウェブサイト及びポスターで周知した。具体的には、Wi－Fi位置情報の取得を望まない来場者には会場内で通信機器のWi－Fi機能をオフにするよう周知した上で、サービスにおいて、MACアドレス及び位置情報を収集すること、実際の製品を用いてその動作、分析結果などをリアルタイムに展示会場で確認するために当該情報を取得すること、取得されたデータは個人を特定できない形で保存し分析終了後データは抹消すること、取得した情報は特定の第三者に提供すること等が明示された。

【図表2－6：G空間EXPOヒートマップ】



[Webサイト、ポスター等で通知、オプトアウトの仕組みを用意]

各OS の Private MAC 対応状況 まとめ

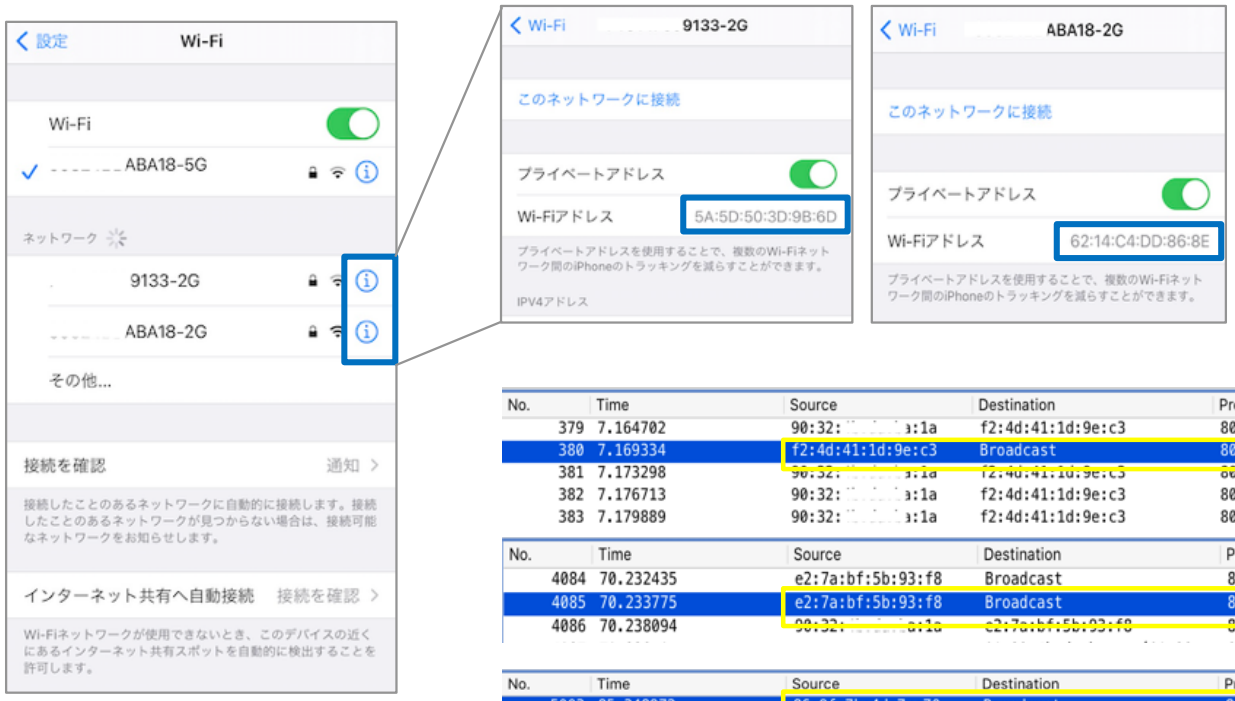
Private MAC は Apple 以外もあるの？どんな実装？

各OS における Private MAC の実装	iOS14	Android10,11	Windows10
該当バージョンの Default 設定	有効	有効	無効
既存で SSID 設定があり該当バージョンにバージョンアップした際の動作	有効	無効	無効
SSID 毎に有効/無効の設定が可能か	可能	可能	可能（全体も可）
SSID 毎に異なる Private MAC	Yes	Yes	Yes
一度割り当てられた Private MAC を使い続けるか	Yes	10: Yes 11: No (option: 24時間)	No (option:24時間)
SSID の設定を削除し、作り直しても同じ Private MAC を使うか	Yes	Yes	No
端末をリブートしても同じ Private MAC を使うか	Yes	Yes	Yes
Probe 送信時は Random MAC	Yes	Yes	Yes

2020/09時点の実装。端末の実装により変更される可能性もあります。

iOS14 で実際試してみた

繋いでない SSID でも Private MAC？



接続はしていないが、デバイスから見えている SSID の i マークをクリックすると、これらの SSID に接続した際の Private MAC（頭から2番目が 2,6,A,Eのいずれか) がスタンバイしていることが分かります。

[疑問]
では、これらの SSID への Probe は Private MAC を使用するのでしょうか？

No.	Time	Source	Destination	Protocol	Length	Info
379	7.164702	90:32:[illegible]:1a	f2:4d:41:1d:9e:c3	802.11	435	Probe Response, SN=665, FN=0, Flags=....R...C, BI=100, SSID=[illegible]A18-2G
380	7.169334	f2:4d:41:1d:9e:c3	Broadcast	802.11	152	Probe Request, SN=161, FN=0, Flags=........C, SSID=Broadcast
381	7.173298	90:32:[illegible]:1a	f2:4d:41:1d:9e:c3	802.11	435	Probe Response, SN=666, FN=0, Flags=........C, BI=100, SSID=[illegible]A18-2G
382	7.176713	90:32:[illegible]:1a	f2:4d:41:1d:9e:c3	802.11	435	Probe Response, SN=666, FN=0, Flags=....R...C, BI=100, SSID=[illegible]A18-2G
383	7.179889	90:32:[illegible]:1a	f2:4d:41:1d:9e:c3	802.11	435	Probe Response, SN=666, FN=0, Flags=....R...C, BI=100, SSID=[illegible]A18-2G

No.	Time	Source	Destination	Protocol	Length	Info
4084	70.232435	e2:7a:bf:5b:93:f8	Broadcast	802.11	191	Probe Request, SN=870, FN=0, Flags=........C, SSID=Pod02
4085	70.233775	e2:7a:bf:5b:93:f8	Broadcast	802.11	152	Probe Request, SN=871, FN=0, Flags=........C, SSID=Broadcast
4086	70.238094	90:32:[illegible]:1a	e2:7a:bf:5b:93:f8	802.11	435	Probe Response, SN=1336, FN=0, Flags=........C, BI=100, SSID=[illegible]A18-2G

No.	Time	Source	Destination	Protocol	Length	Info
5003	85.348972	86:9f:7b:4d:7a:70	Broadcast	802.11	152	Probe Request, SN=1124, FN=0, Flags=........C, SSID=Broadcast
5004	85.352857	90:32:[illegible]:1a	86:9f:7b:4d:7a:70	802.11	435	Probe Response, SN=1500, FN=0, Flags=........C, BI=100, SSID=[illegible]A18-2G
5005	85.356137	90:32:[illegible]:1a	86:9f:7b:4d:7a:70	802.11	435	Probe Response, SN=1500, FN=0, Flags=....R...C, BI=100, SSID=[illegible]A18-2G
5006	85.359487	90:32:[illegible]:1a	86:9f:7b:4d:7a:70	802.11	435	Probe Response, SN=1500, FN=0, Flags=....R...C, BI=100, SSID=[illegible]A18-2G
5007	85.363021	90:32:[illegible]:1a	86:9f:7b:4d:7a:70	802.11	435	Probe Response, SN=1500, FN=0, Flags=....R...C, BI=100, SSID=[illegible]A18-2G

無線のパケットをキャプチャしてみると、Private MAC ではない、ランダム化された MAC アドレスが Probe の MAC として使用されていることが分かりました。
SSID に接続していないと ランダムな MAC を変更しながら使うようです。(iOS 8 の時と類似）

Private MAC有効時

定期的に変更される
可能性あり

SSID A: x2:xx:xx:xx:xx:xx
（associate）
SSID B: x6:xx:xx:xx:xx:xx
SSID C: xA:xx:xx:xx:xx:xx
SSID D: xE:xx:xx:xx:xx:xx
SSID E: x2:yy:xx:xx:xx:xx

実MAC: AB:CD:xx:xx:xx:xx

端末Probe/Association時

ネットワークインフラ

端末数が増えた！？

新しい端末接続？？

どこの端末？？

影響を受けそうな製品/機能を列挙してみる

	常時影響	該当OSにバージョンアップ時影響 (ユーザが接続SSIDを変更しない/プロファイル作り直し/24時間ごとに変更するオプションを有効にしない場合)
無線LAN製品(コントローラ、アクセスポイント)、管理装置	デバイス検索	ユーザテーブル
	MACアドレスやOUIによるプロファイル識別	クライアント/不正クライアント履歴・統計・分析
位置情報を活用した製品	Probe による位置情報の計算	MACアドレスで識別した個別位置情報履歴
	位置情報統計・分析	
認証サーバ、セキュリティ	MACアドレスフィルタ、MACアドレス認証	キャプティブポータル
	プロファイル, プロビジョン, MDMなど (MACアドレスによってデバイスを識別している場合)	
その他	各OS独自のアルゴリズムでMACをアサイン。極稀*にMACアドレスの重複の可能性あり	端末のOS Upgradeのタイミングで DHCPのアドレスプールが枯渇する可能性

無線LAN製品(コントローラ、アクセスポイント)、管理装置 影響のありそうな機能

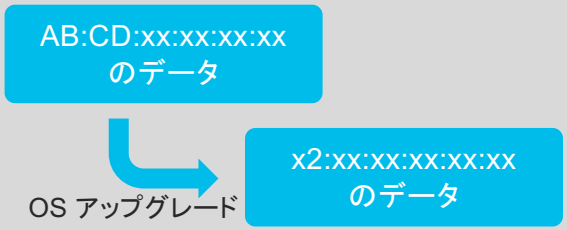
デバイス検索	• MACアドレスでの検索はユーザに都度聞くなどオペレーションが煩雑になる可能性があります。 • 複数のSSIDを移動するクライアントの場合、ユーザ名もしくはデバイス名で検索すると、複数のデバイスを所持しているかのように重複して表示されます。
MACアドレスやOUIによるプロファイル識別	• OUIによるメーカの識別ができなくなります。製品によって表記が異なる可能性があります。
ユーザテーブル	• Private MAC に変更された後は別のデバイスと認識され、ユーザテーブルには以前の実MACのタイムアウトまで2つが載ることとなります。
クライアント/不正クライアント履歴	• デバイスがPrivate MACに変更後別のデバイスとして表示され、さらに複数のSSIDへ移動/Probeするクライアントは個別のものとしてカウントされます。 • クライアント履歴の保持期間次第で管理装置の最大クライアント数を超えることも考えられます。
クライアント統計・分析	• Private MACに対応後は、クライアント数が多くなり統計・分析データに影響することが考えられます。

無線LAN製品(コントローラ、アクセスポイント)、管理装置 影響のワークアラウンド・対応

デバイス検索

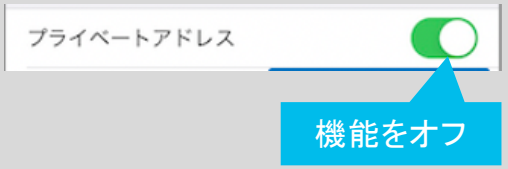
- 802.1x認証などを活用し、ユーザIDを検索に使用

Private MAC対応前後で別データとして管理



- クライアント履歴や統計はPrivate MAC対応後*のデータで集計し直し

Private MACをオフ



- ユーザポリシーで許可されればRandom/Private MAC機能をMDMなどで無効化

*ユーザが接続SSIDを変更しない/プロファイル作り直し/24時間ごとに変更するオプションを有効にしない場合

Wi-Fi位置情報ソリューション 影響のありそうな機能

Probe による位置情報の計算

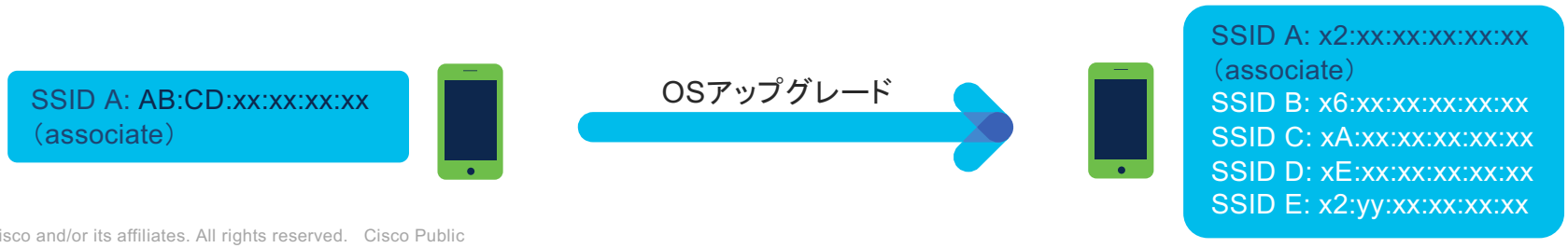
- 以前から約1分ごとにMACアドレスが変わる端末があるので位置情報データとしては使えません。

MACアドレスで識別した端末位置情報履歴

- Private MAC に変更された後は別のデバイスとして履歴もわかれて載ります。
- 異なるSSIDに接続/Probeした場合も別のデバイスとしてカウントされ、MAP上も重複したクライアントが表示されます。

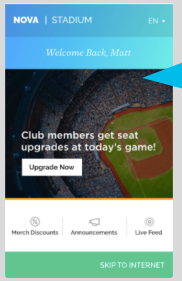
位置情報統計・分析

- Private MAC に切り替え後、別のデバイスとしてカウントされる為、訪問者の延べ人数が増加する可能性があります。(SSIDが複数ある場合はさらに増えます)
- データベースの保持期間次第でDBの上限を超えるケースも考えられます。



Wi-Fi位置情報ソリューション ワークアラウンド・対応

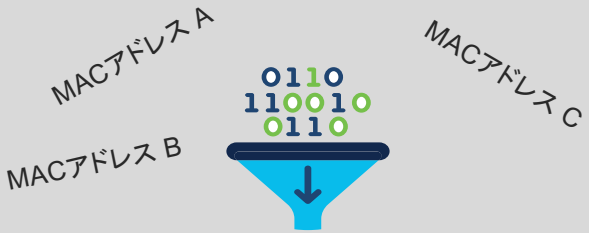
IDでのトラッキング



アプリのIDなどを
利用してトラッキング

- アプリ、SNS認証などを使用してIDベースでトラッキング

フィルタリング活用



- 統計情報はシステム管理外のSSID関連情報をフィルタリングするなど工夫が必要になる可能性*

Private MACをオフ

- ユーザポリシーで許可されればRandom/Private MAC機能をMDMなどで無効化

IDと位置情報を紐づけた場合個人情報になりますので相応の配慮・対応が必要です

Probeは約1分ごとに変わるRandom MACなので履歴としては利用不可です

Random/Private MACは自動的に捨てる位置情報ソリューションもありますので確認してください

*ユーザが接続SSIDを変更しない/プロファイル作り直し/24時間ごとに変更するオプションを有効にしない場合

認証サーバ、セキュリティ 影響のありそうな機能

MACアドレスフィルタ
MACアドレス認証

- SSID毎にも異なるMACアドレスとなりフィルタや認証が難しくなります。
- MACアドレスフィルタ/認証はセキュリティとしても脆弱であり利用停止も含めて検討してください。

プロファイル, プロビジョン, MDMなど*

- MACアドレスやOUIを利用したセキュリティポリシーの適用は利用できなくなります。

* MACアドレスによってデバイスを識別している場合

キャプティブポータル

- Private MAC に切り替え後、キャプティブポータル画面で再度認証を求められます。

認証サーバ・セキュリティ 影響のワークアラウンド・対応

ユーザ認証へ移行

- 802.1x認証（ユーザ認証、証明書認証）へ移行
- 多要素認証には多要素認証ソリューション・アプリを採用
- MACアドレスフィルタ・認証はセキュリティ脆弱性がありますので高セキュリティ方式の検討を推奨

MACアドレスを使わない仕組みの利用

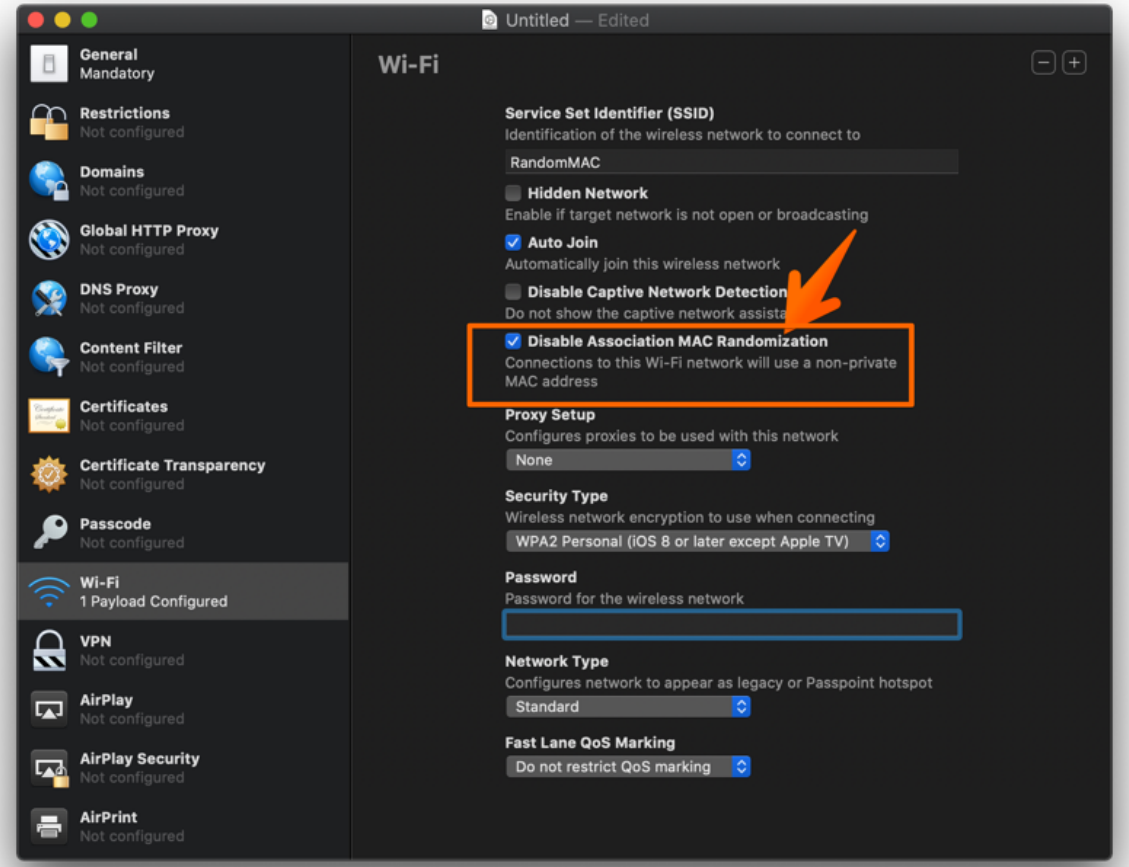
- プロファイル, プロビジョン, MDMなどはMACアドレスを使わない仕組みで回避可能な場合も

Private MACをオフ

- ユーザポリシーで許可されればRandom/Private MAC機能をMDMなどで無効化

Private MAC アドレスの無効設定の配布

[Apple Wi-Fi Profile Management による配布]



- 管理者用Appleのツールで無効にできます
- 他MDMでも無効にすることができます

その他 影響のありそうな機能

MACアドレス

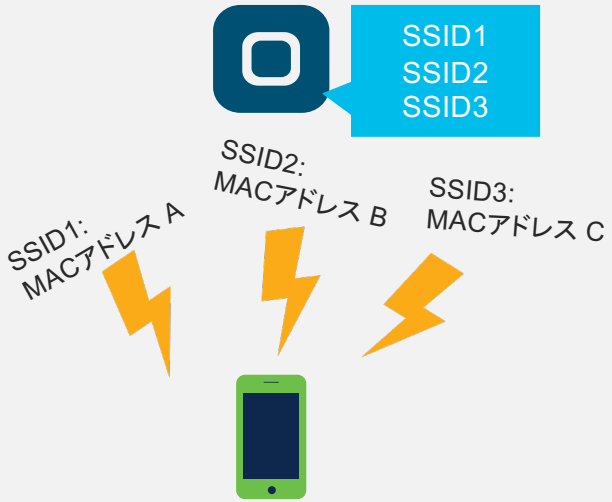
- 各OS独自のアルゴリズムでMACをアサインするため極稀にMACアドレスが重複する可能性があります。
- 16x4x16^6 = 1,073,741,824個から選ばれるので極稀

DHCPアドレスプール

- 端末のOS Upgradeのタイミングで DHCPのアドレスプールが枯渇する可能性があります。

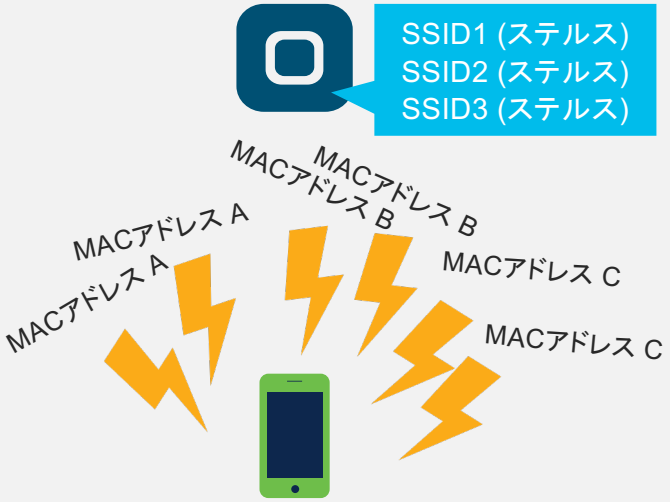
【おまけ】Random MACによるProbeを増やしてシステムを逼迫させるかもしれないもの

多SSID



- 端末に登録されているSSIDが複数見えている場合、それぞれにRandom MACが生成されます

ステルスSSID



- ステルスSSID設定にしていると端末からProbeが頻繁に出るため、1端末からさらに複数のMACアドレス情報がシステムに流れやすくなります

その他

- 現在把握している限り、Apple, Google, Microsoftが先行してPrivate MACをOS実装しています。今後対応OSが増えるかどうかは不明です。
- ただし、すでに本日説明したルールとは異なる方法でMACアドレスをランダム化している製品があるという報告もあります。
- MAC PrivacyについてはIEEE 802.11aq working groupで標準化が進められています。
- BLEにもRandom Device Addressというプライバシー保護機能があります。

まとめ

- プライバシー配慮はグローバル単位のトレンドです。ネットワークの世界でも様々な形で機能実装・標準化が進んでおり、Private MACはその一環です。

- 影響のある/ありそうな製品や機能を把握し対応を進めてください。
- ユーザポリシーで許可されればRandom/Private MAC機能を無効化することも候補のひとつです。

参考 URL

- Apple
  - iOS 14、iPadOS 14、watchOS 7 でプライベート Wi-Fi アドレスを使う
- Android
  - プライバシー: MAC アドレスのランダム化
- Microsoft
  - ランダム ハードウェア アドレスを使う理由


CISCO

iOS14 で実際試してみた

[無線でOS update後]

Private MAC 有効

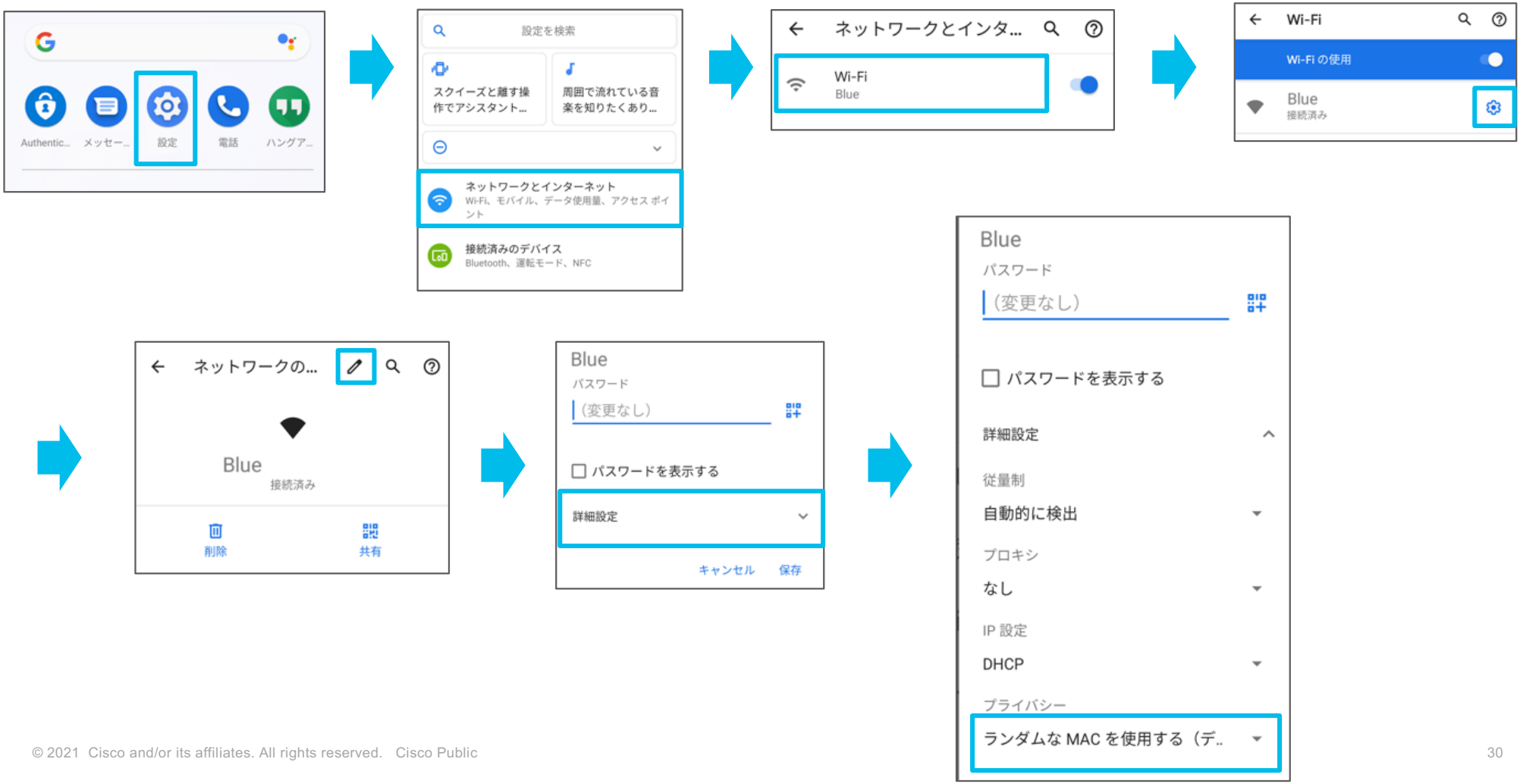
あれ？実MAC！？

[無線を Off/On 後]

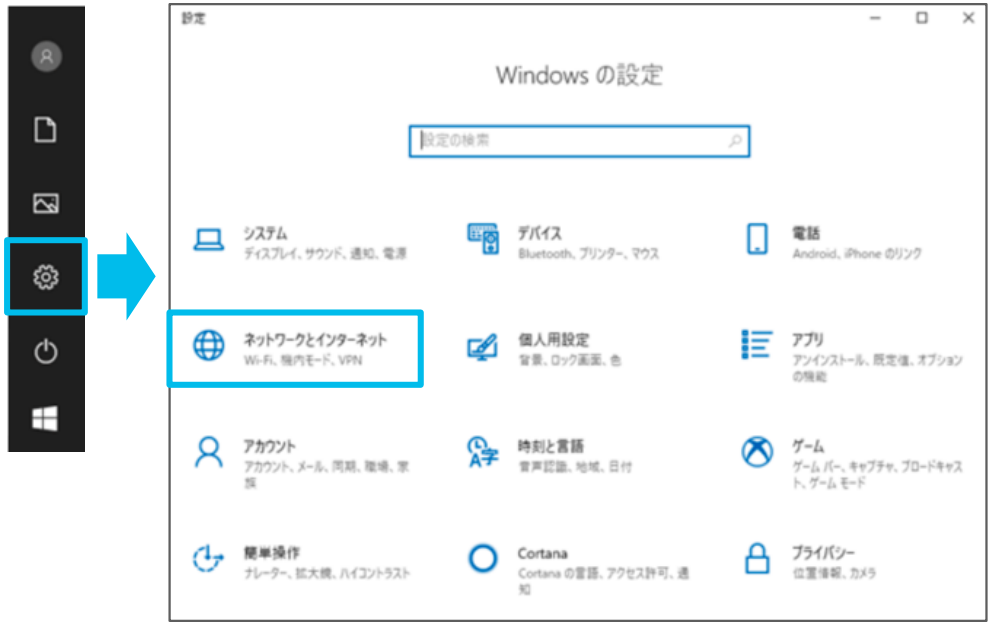
無線 Off/On 後は
MACの頭から2番が
A の Private MAC に
変更された

iPhone で動作確認したところ、iOS14 にバージョンアップ後、Private MAC を有効にする「プライベートアドレス」は有効になっていたが、既に接続している SSID は実 MAC を使用し続けていました。
Wi-Fi を Off/On、もしくは他の SSID に接続する、プライベートアドレスを Off/On のいずれかを行うと Private MAC がアサインされました。
iOS のアップデート後の最初は Private MAC になっていないことがある為注意が必要。
MACの頭から2番目が、2,6,A,E のいずれかであるかで判断すると良いです。

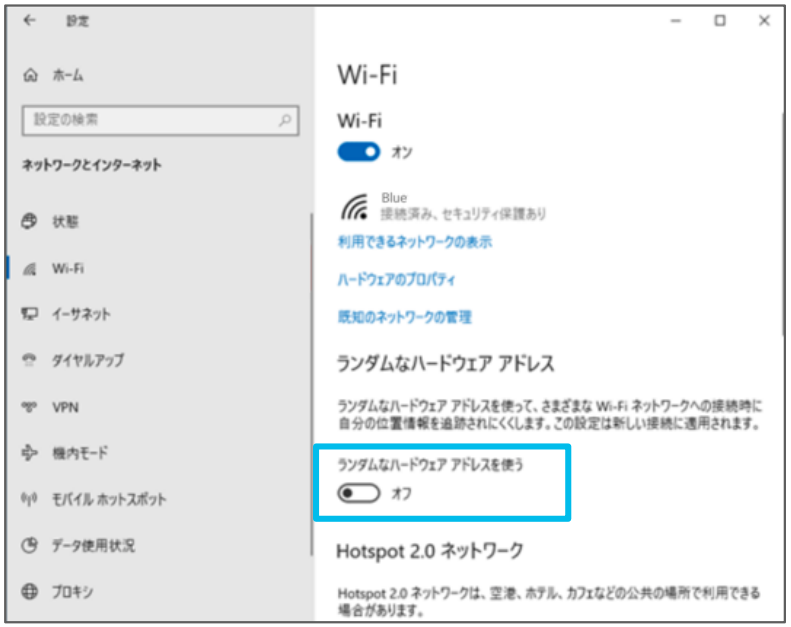
参考）Android10 の設定画面



参考）Windows10 の設定画面



[全体設定]



[各SSIDの設定]