TOKYO FREE Wi-Fi
事例紹介
-自治体初、OpenRomaingの裏側-

2024年1月17日

株式会社ワイヤ・アンド・ワイヤレス
中野 健司

自己紹介

中野 健司（なかの　けんじ）

（株）ワイヤ・アンド・ワイヤレス（2022年1月～）

ネットワーク技術本部部長

（株）イオレ（2020年4月～2021年12月）

運用型求人広告プラットフォーム事業立ち上げプロジェクト 事業兼開発責任者

（株）ワイヤ・アンド・ワイヤレス（2013年8月～2020年3月）

技術運用本部部長

現ソフトバンクモバイル（株）（2000年7月～2013年7月）

データセンター・伝送設備・インフラ・ネットワークの企画、設計、構築、運用に従事（卒業時：部長）

（株）アステル関西（1996年4月～2000年6月）

基地局、課金、認証、ネットワーク設備の監視、運用、構築、新サービスの開発に従事

本日の内容

- 最近のWi-Fiに関する日本の動き、取り組み
- なぜ？OpenRoaming？OpenRoamingとは？
- いままでのWi-Fiとの違いとは？
- 東京都で、実現する為につかっている技術の話

最近のWi-Fiに関する日本の動きと取り組み

Wi-Fiの概況

モバイル通信事業者のWi-Fiサービス
（キャリアWi-Fi）

docomo　**SoftBank**

KDDI

など

・5Gへのシフトとともにデータ通信オフロードとしての活用は収束
・キャッシュレス決済のための補完的な通信環境提供、位置情報を活用した送客や利用促進等での活用用途にシフト

民間店舗、施設のフリーWi-Fiサービス

FREE Wi-Fi

Japan. Tax-free Shop

・コロナ禍によりインバウンド受入環境としてのWi-Fiは一時停滞するも観光需要の復調とともに徐々に回復
・リモートワークやキャッシュレス決済の急速な浸透により、一部の業種においては需要が増大

公共領域におけるフリーWi-Fi環境

Japan. Free Wi-Fi

〇〇City Wi-Fi

いのちをつなぐ 00000 JAPAN

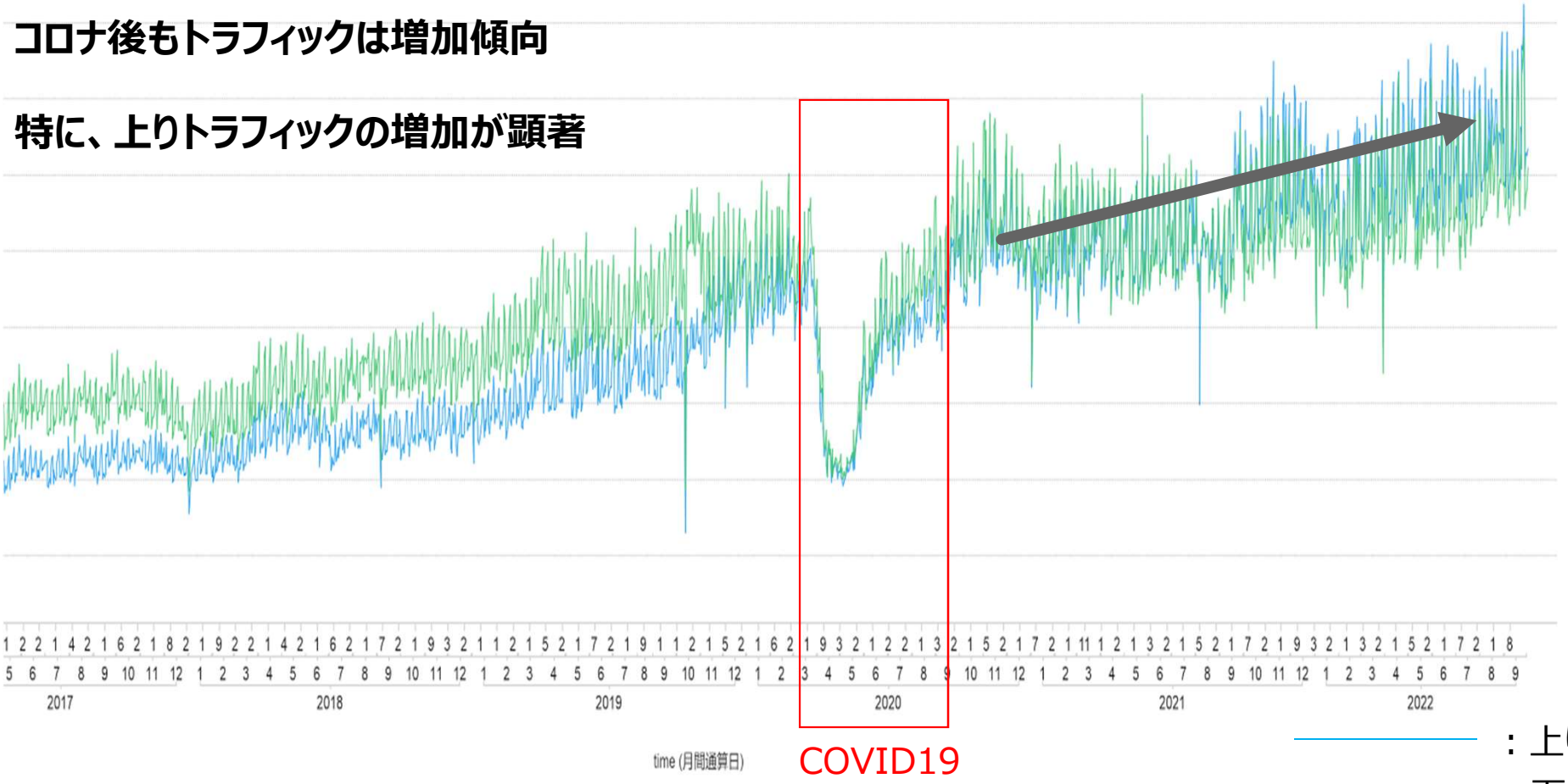
・これまで、観光振興、防災/減災を目的とした環境整備が着実に浸透
・これに加え、デジタル化の拡大とともに、デジタルデバイド対策としての環境整備、多面的な情報発信やデータの利活用の取組みが拡大
・一方で、既存設備の老朽課題も浮上
⇒設備更改にはデジタル田園都市国家構想等に即した、新たな価値提供が必要

Wi-Fiトラフィックの動向（2017年～）

（当社データ）

コロナ後もトラフィックは増加傾向

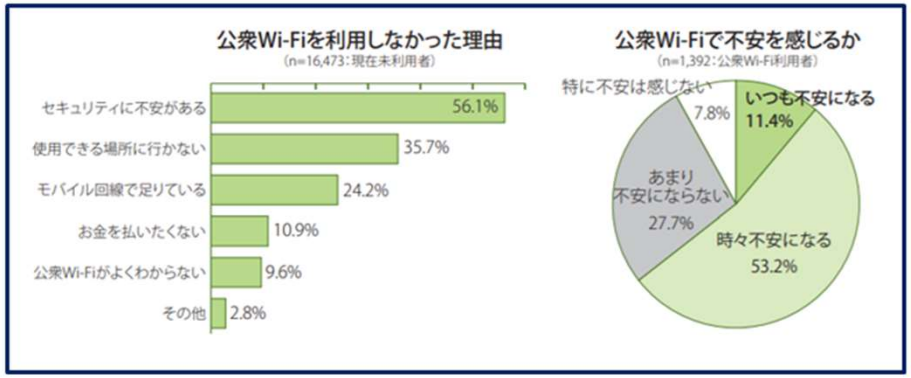
特に、上りトラフィックの増加が顕著



セキュリティに対する懸念

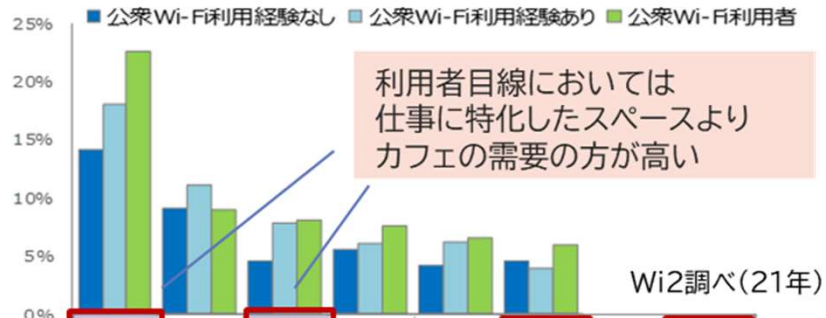
- 多くのが利用者がセキュリティ不安を感じつつ利用していることが伺え、利用しない理由でも最も多くなっています。
- 安全なWi-Fiを利用したリモートワーク需要があり、特にカフェでは利用意向が高いことが伺えます。

➢ セキュリティに対する利用者の意識



出典:総務省 Wi-Fi利用者向け簡易マニュアル(令和2年5月版)

今後新しい生活様式が浸透し、勤務先でテレワークが認められた場合、テレワーク先でのネット接続環境における、公衆Wi-Fiの利用をどのように考えますか。



n=		セキュリティ上安全であれば、カフェのWi-Fiを利用しテレワークを実施したい	セキュリティ上安全であっても、自宅や職場以外で通信は利用しない(してはいけない)	セキュリティ上安全であれば、シェアオフィスや、コワーキングスペースのWi-Fiを利用しテレワークを実施したい	テレワークの際は、会社支給のモバイルWi-Fiルーターやテザリングを利用する	テレワークの際は、自分で用意したモバイルWi-Fiルーターやテザリングを利用する	セキュリティ上安全であれば、レストランのWi-Fiを利用しテレワークを実施したい	テレワークをすることがない	Wi-Fiスポットを利用しテレワークを実施したい・計
全体	(2,934)	18.4	9.7	6.9	6.5	5.7	4.9	47.7	30.2
公衆Wi-Fi利用経験なし	(935)	14.1	9.1	4.6	5.6	4.2	4.6	57.9	23.3
公衆Wi-Fi利用経験あり	(934)	18.1	11.1	7.9	6.1	6.2	4.0	46.3	30.0
公衆Wi-Fi利用者	(1,065)	22.5	9.0	8.1	7.6	6.6	5.9	40.0	36.5

オンボーディングに対する懸念

・EAPによるセキュリティは、企業等で運用され、最も安全な無線LANの認証方式に位置づけられています。
・一方、不特定多数が利用されるWi-Fiサービスでは利用が難しいとされてきました。

無線区間における暗号化 【資料24】

	利便性	セキュリティ強度
（1）暗号化なし	◎	×
（2）暗号化あり:WPA2-PSK(Pre Shared Key) ■ パスフレーズ:全ユーザ共通(※1) ■ 「暗号化なし」よりはセキュリティを確保 ■ ただし、全ユーザが共通のパスフレーズを利用するため、高いセキュリティを確保するためには定期的なパスフレーズの変更が必要(実際は、企業において頻繁なパスフレーズの変更は実施されておらず、PSK利用における課題。)	○	○ (パスフレーズの定期的な変更をしない場合は△)
（3）暗号化あり:WPA2(IEEE802.1X／EAP:証明書ベース) ■ 認証クレデンシャル(証明書、ID・パスワード等):ユーザ個別 ■ 認証サーバと連携し、認証クレデンシャルを使用して異なる鍵(PMK、PTK(※2))を生成可能なため、高いセキュリティを確保可能 ■ ただし、証明書ベースのIEEE802.1Xは、証明書の運用が課題	△	◎

（※1） 同じSSID配下でユーザごとに異なる個別のパスフレーズを利用可能な機能を実装した製品がリリースされている。ただし、既存製品の仕組みでは、ユーザ登録との連携はうまく実現できていない。
（※2） PMK(Pairwise Master Key):PTKなどを生成するためのマスター鍵、PTK(Pairwise Transient Key):ユニキャスト通信用の鍵

公衆無線LANセキュリティ分科会(第2回)資料2－3を基に作成。

出典: 公衆無線 LAN セキュリティ分科会報告書(総務省 2018)
https://www.soumu.go.jp/main_content/000539751.pdf

総務省による啓蒙活動
(令和2年版)

コラム　WPA2でも安心できない

外出先で誰でも使えるWi-Fi（公衆Wi-Fi）は、WPA2で暗号化されているものも多くあります。

WPA2にはその詳細方式が複数あり、費用をかけずに手軽に利用できるものが「WPA2パーソナル（WPA2-PSK）」という方式です。この方式は、家庭や個人での利用に限れば十分な安全性を持った方式です。

しかしながら、この方式の特徴として、アクセスポイントに接続する人全員が同じパスワードを共有する必要があるため、不特定多数が利用する公衆Wi-Fiでは、利用者全員がパスワードを知っている状態にあります。パスワードが知られてしまっている場合、アクセスポイントの通信内容は、条件が整えば比較的容易に解読できてしまいます。加えて、パスワードが分かっていれば、同じ名前（SSID）とパスワードを設定することで、偽のアクセスポイントを設置して、容易に通信内容を盗むことも可能となります。

このため、WPA2パーソナル（WPA2-PSK）方式の公衆Wi-Fiについては、暗号化されていない場合と同様に留意して利用する必要があります。

コラム　安全なWi-Fiセキュリティ方式

上のコラムで、公衆Wi-Fiにおいては、WPA2パーソナル（WPA2-PSK）方式は必ずしも安心できないとお伝えしましたが、以下に挙げたものは安全性が高い方式です。これらの方式が利用可能な場合は積極的に利用しましょう。なお、いずれもWi-Fiの無線区間のみの暗号化方式であることに留意してください。

●WPA2エンタープライズ（WPA2-EAP）
共通のパスワードを利用するWPA2パーソナル（WPA2-PSK）方式とは異なり、利用者ごとにID等を設定し、接続の際に利用者側とアクセスポイント側で相互に認証する方式です。認証の際に暗号鍵も個別に設定されます。利用者からアクセスポイントに対する認証も行うため、偽アクセスポイントへ接続する心配もありません。しかしながら、個別にID等を配付し設定する必要があるため、不特定多数が利用するWi-Fiサービスでは利用が難しい状況です。

出典: Wi-Fi利用者向け簡易マニュアル
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/index.html

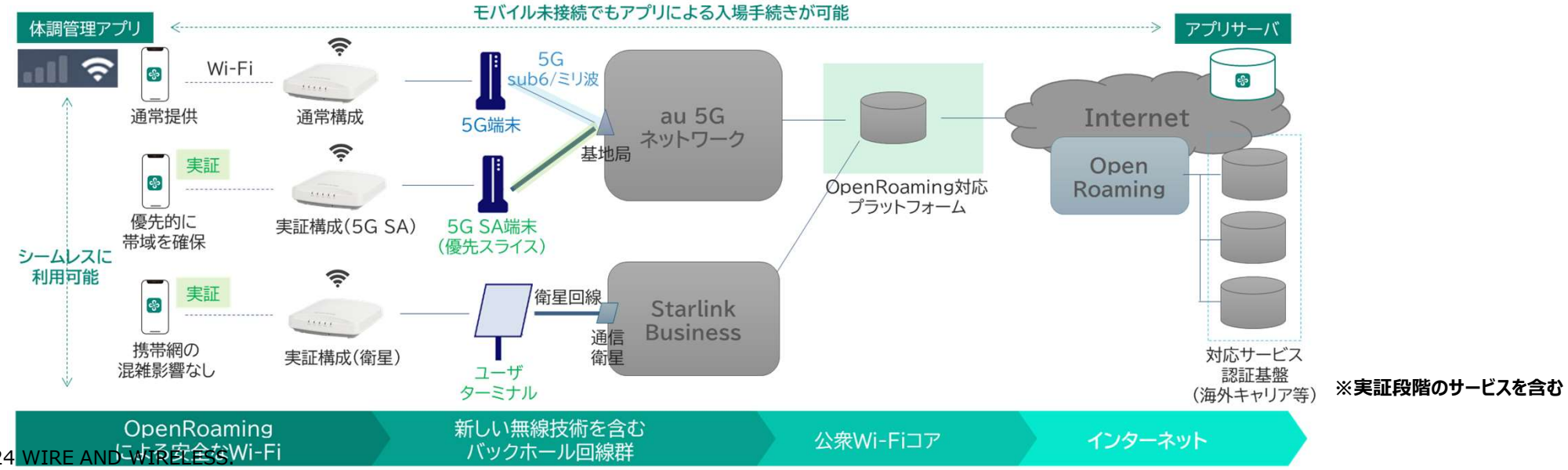
インバウンドの需要

東京マラソン２０２３：OpenRoamingの試験運用では多くの海外ランナーの利用がありました。

	ビッグサイト事前受付期間			大会当日	期間中累計
	3月2日(水)	3月3日(木)	3月4日(土)	3月5日(日)	3月2日~5日
QRコード方式	566	509	278	2,183	2,594
OpenRoaming方式	698	787	160	643	1,425
合計	1,264	1,296	438	2,826	4,019
	10:00 - 20:30	10:00 - 20:30	10:00 - 17:30	7:00 - 9:10	

アクセスポイント8台（受付）
及び、20台（当日）での利用者数

➢ **ネットワーク構成**



※実証段階のサービスを含む

フリーWi-Fiにおける直近の動き

【トピックス】

本日のご紹介

安全性/利便性の向上	・OpenRoamingの拡大（東京都から日本全国へ）
通信品質の向上	・Wi-Fi６/６Eの普及　⇒Wi-Fi７へ （令和5年12月22日総務省より「電波法施行規則等の一部を改正する省令（令和5年総務省令第95号）」ならびに関連する告示が公布
適用領域の拡大	・Wi-Fiの上空利用（５GHz）審議 ・802.11ah（Wi-Fi HaLow）商用化 ・災害用SSID「０００００JAPAN」通信障害時への適用開始 ・衛星通信＆Wi-Fiの活用拡大（Starlinkなど）

・キャリアWi-Fi（携帯オフロード）の縮小は一段落しつつある
　（インバウンドの回復とともにフリーWi-Fiの再整備の動きも）
・公共領域ではデジタル田園都市国家構想の取組みの拡大とともに都市基盤としての整備が拡大

東京都でOpenRoamingの取り組みが始まる

今後海外との入出国増加が想定される中、利用者が簡単に通信環境を確保する手段としてフリーWi-Fiが求められています。
一方で従来のフリーWi-Fiは、端末とアクセスポイントの間が暗号化されていないことが多く
なりすましのアクセスポイントへの接続の抑制が、困難などといったセキュリティの課題がありました。
東京都が、「つながる東京」構想の一つとして、これらの課題を解決した
フリーWi-Fi（Wireless Broadband Alliance（WBA）が推進する国際的な無線LANローミング基盤OpenRoaming）の
提供を、開始しています。

【OpenRoamingに関する日本の動き】

2020.11	Cityroamが、OpenRoamingトライアルを完了、サービス展開を開始。
2021.7～9	Cityroamが、一部の通信事業者を対象に、OpenRoaming（無料ローミング）のトライアルを東京で実施。
2023.4	東京都が、KDDI(株）／（株）ワイヤ・アンド・ワイヤレス／Cityroamと協同し、OpenRoamingの提供を開始。
2023.7	2025年大阪万博会場でのOpenRoamingの提供を発表（シスコシステムズ合同会社）
2023.11	函館市にて高速且つ安全性の高いフリーWi-Fiサービスを再構築（Wi-Fi6＆OpenRoaming）

Cityroam:2018年より東北大学が中心になり立ち上げたローミング基盤、WBAのメンバーとして認証ハブを構築、運用しています。
Cityroamについて：https://cityroam.jp/about

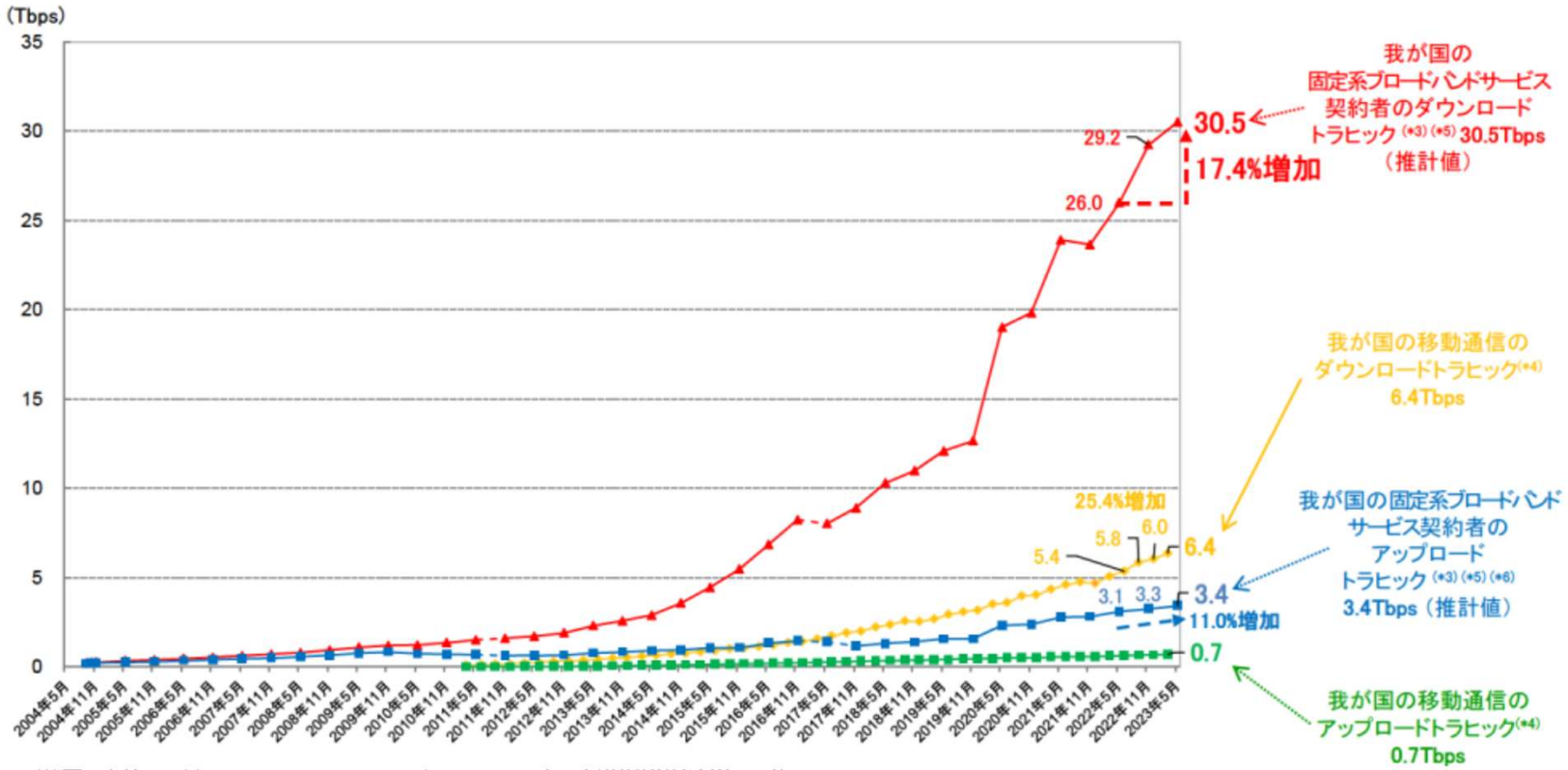
目次

目次

なぜ？OpenRoaming？
OpenRoamingとは？

1-1. 日本国内のインターネットトラフィック

固定系のダウンロードトラフィックは、前年同月比17.4%増、移動体は、25.4%増

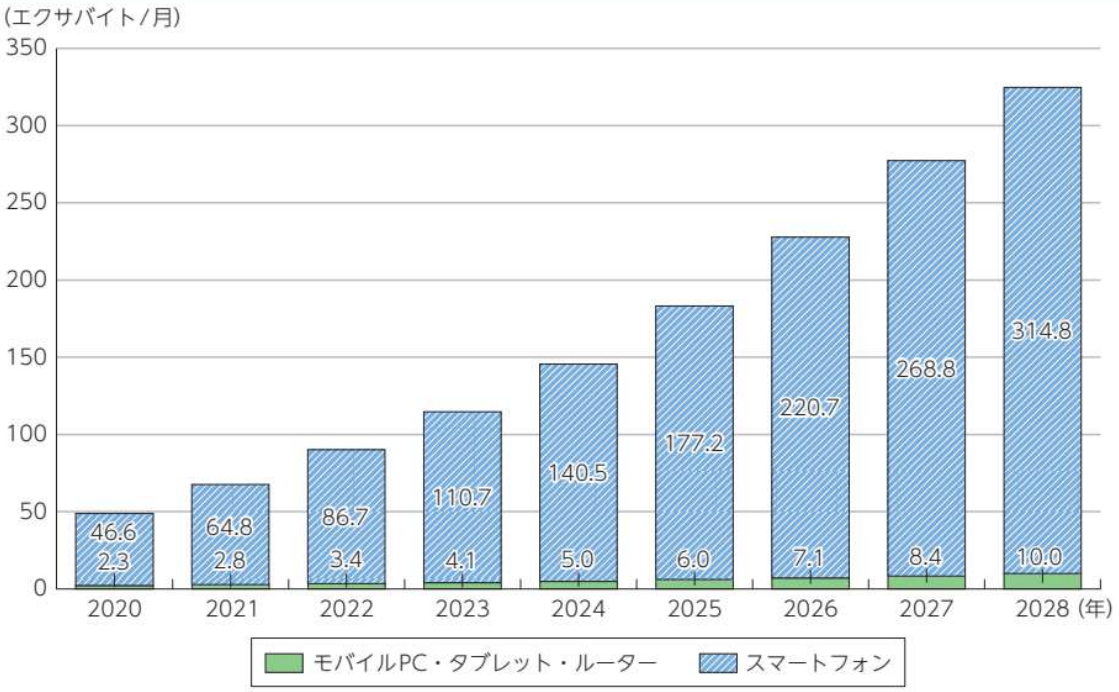


出展：https://www.soumu.go.jp/main_content/000896195.pdf

1-2. 世界のトラフィック予測（今後５年）

「Ericsson Mobility Report」では2028年には約325エクサバイト／月に達すると予測

図表2-1-1-1 世界のモバイルデータトラヒックの予測（デバイス別）



（出典）Ericsson “Ericsson Mobility Visualizer”*2を基に作成

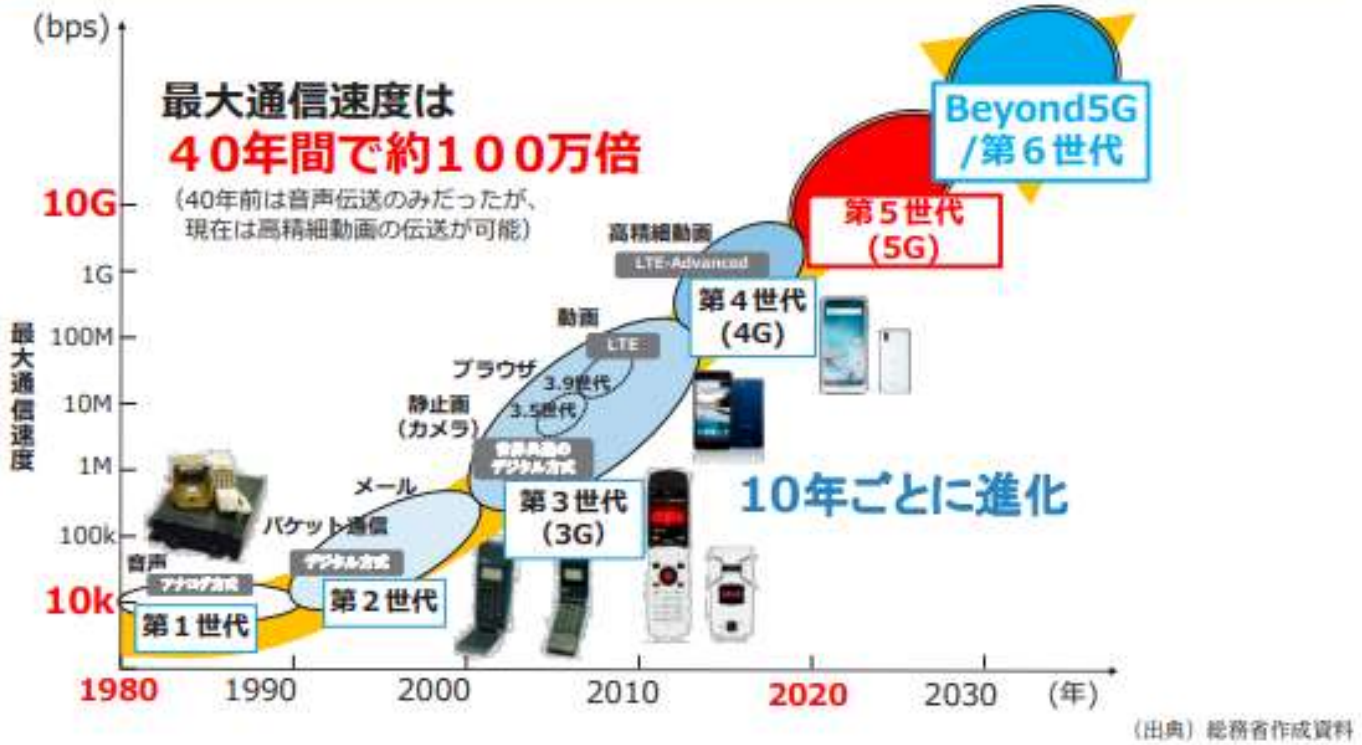
出典：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/pdf/n1100000.pdf

出典：https://www.ericssom.com/en/mobility-report/mobility-visualizer

1-3-1.通信速度

10年周期で世代交代が行われ、大容量化、高速化の方向で進化

図表1-1-2-1 移動通信システムの進化



出典：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/pdf/n1100000.pdf

1-3-2.通信速度

Wi-Fiも同様に、大容量化、高速化の方向で進化

出典：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/pdf/n1100000.pdf

野外フェスでの弊社調べでは
・Wi-Fi6利用者が約80%
・Wi-Fi5利用者が約19%
・Wi-Fi4利用者が約1%以下
Wi-Fi5からWi-Fi6に移行中。

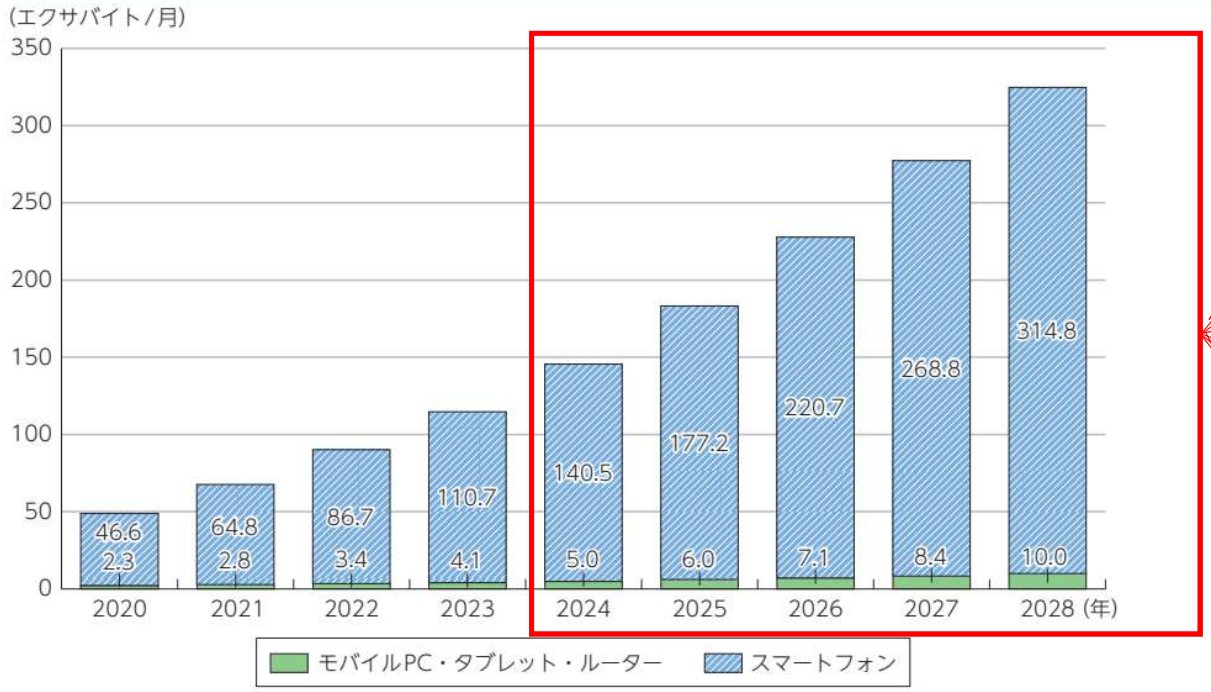
TOKYO FREE Wi-Fi 整備アクセスポイント

		Wi-Fi5	Wi-Fi6	Wi-Fi6E	Wi-Fi7
規格	IEEE仕様	802.11ac	802.11ax	802.11ax (6Ghz帯対応)	802.11be
	最大通信速度	3.5Gbps	9.6Gbps	9.6Gbps	46Gps
	周波数帯域(GHz)	5	2.4/5	2.4/5/6	2.4/5/6
	変調方式	256QAM Mu-MIMO	1024QAM OFDMA	1024QAM OFDMA	4096QAM OFDMA
	リソースユニット	×	RU	RU	Multi-RU
	パンクチャリング	×	×	×	○
	MLO	×	×	×	○
5Ghz /6Ghz帯 一般的なスマホ	リンク速度	0.87Gbps	1.2Gbps	2.4Gbps	?Gps
	20MHz幅 1ストリームのリンク速度	216Mbps	150Mbps	150Mbps	180Mbps
	帯域幅	80MHz(4ch)	80MHz(4ch)	160MHz(8ch)	?
	MLO	×	×	×	○?

1-4. 5年後10年後のトラフィックの中身

通信環境が高速、大容量であることは、当たり前、加えて、安心・安全・シームレスが必須な世の中になるはず。。。

図表2-1-1-1 世界のモバイルデータトラヒックの予測（デバイス別）



（出典）Ericsson “Ericsson Mobility Visualizer”*2を基に作成

- クラウド化
- メタバース
- 対話型AI／自立型AI
- 即時機械学習
- 偽情報検知
- Web3（NFT・DAO）
- 行政のデジタル化
- 災害、通信障害対策

出典：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/pdf/n1100000.pdf

出典：https://www.ericssom.com/en/mobility-report/mobility-visualizer

いままでのWi-Fiとの違いとは？

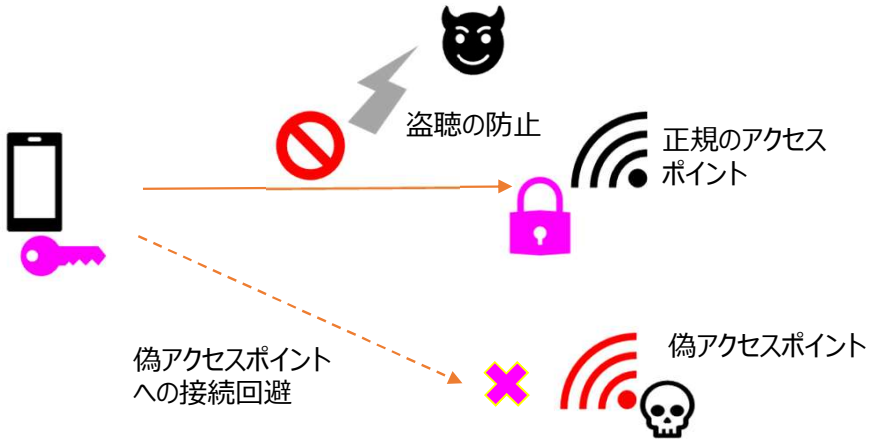
1-5.東京都が導入したOpenRoamingの特徴

①これまでの一般的なフリーWi-Fiにおいて課題とされてきたセキュリティ上の問題が大幅に改善し、オフィス内でのWi-Fiなどと同等の「安全性」が確保されます

②国際的なローミング基盤との連携及び自動接続機能により、一度の登録手続きで全世界のOpenRoaming対応エリアとの連携が可能となります

【安全性の向上】

オフィスなどでのWi-Fiと同様に、証明書を用いた通信により
安全に利用可能となります。



【海外との連携】

OpenRoamingを導入した都市間で、エリア跨って自動接続が
可能となります。

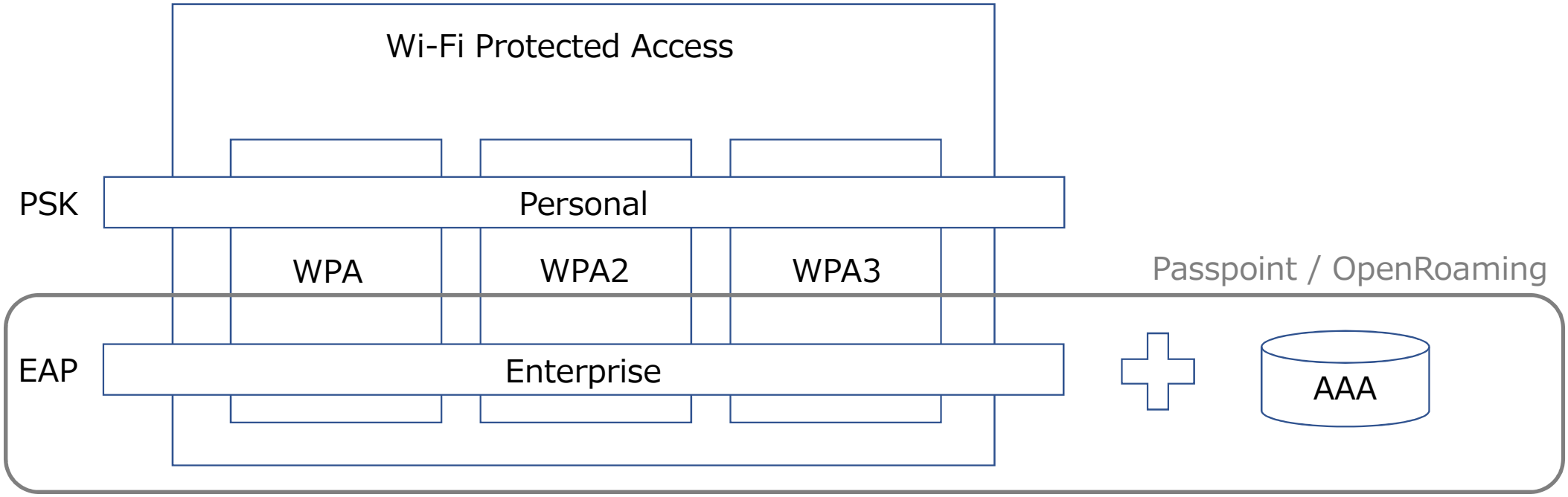
TOKYO FREE Wi-Fiとは？

「OpenRoaming」というフレームワーク
と
「Passpoint」という技術
を組み合わせた

セキュリティの不安なく、且つ、簡単に
世界中で、利用可能な
安心・安全な通信手段

1-6. Wi-Fiのセキュリティ

セキュリティ視点でのレガシー（従来のフリーWi-Fi/オープンWi-Fi、Passpoint、OpenRoamingの違い。

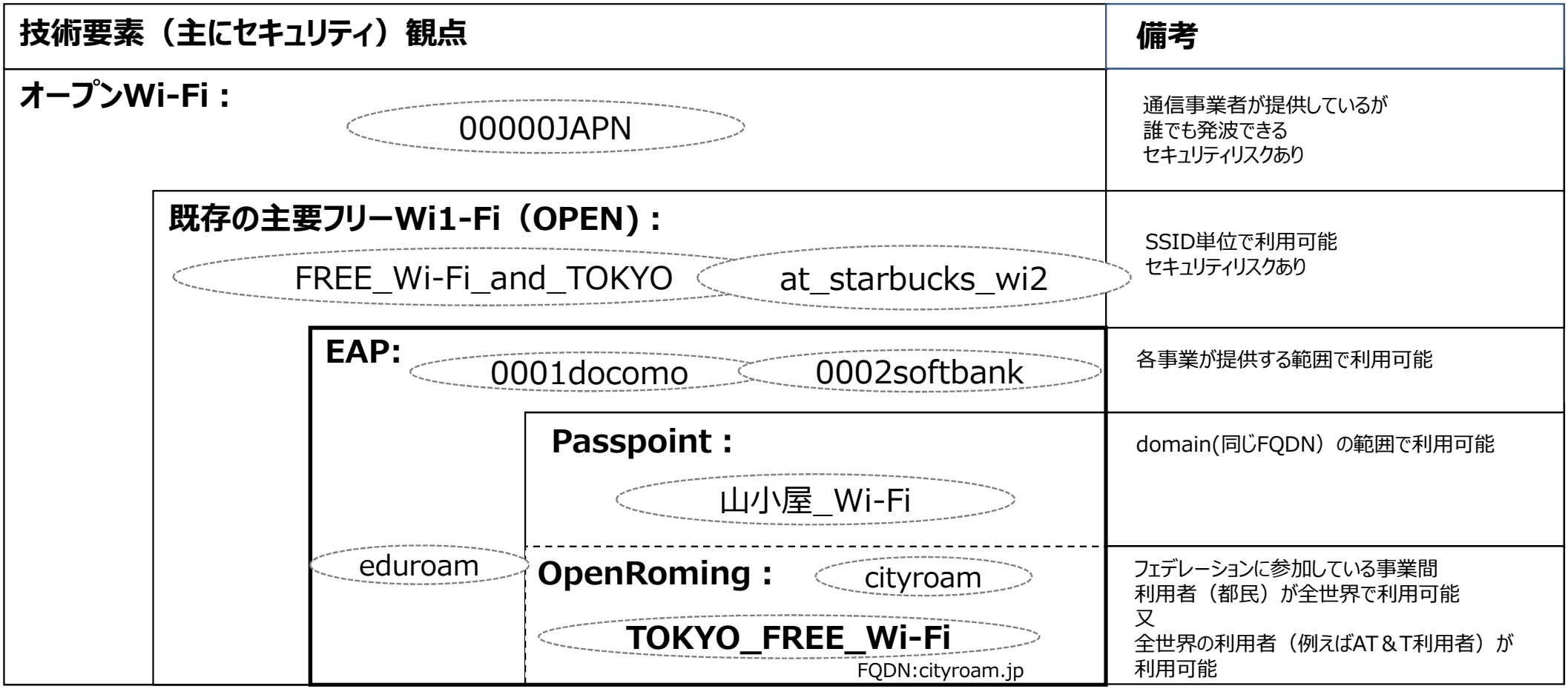


1-7.OpenRoamingを取り巻く技術の整理

技術要素（主にセキュリティ）観点	エリア・その他観点
オープンWi-Fi： 利用者手続きなしで使える。ただし、**リスク（盗聴、詐称）あり**	電波を吹いてるエリアで制限なく 利用可能
既存の主要フリーWi-Fi（OPEN）： 認可機能を追加、提供事業者がわかることが多い **リスクは、OPEN Wi-Fi**と同じ	認可したSSIDグループで利用可能 利用時間制限などの制限がある場合がある 提供している事業者が判別できることが多い。
EAP: 高キュリティ機能（暗号化、詐称防止）	IDの登録、手動設定、若しくは、ネイティブアプリ、 事業者初期設定で提供されている。 手続きは、非常に煩雑
Passpoint： 簡単設定（WEB）、自動接続、SSIDに代わって ドメインの概念を追加される	認可したサービスドメインで利用可能。 ローミング協定を締結している事業者間で接続可能 ドメインで判定し、自動接続が可能
OpenRoming： Passpointの技術を前提とした 相互ローミングネットワーク（WBA）	WBAに加盟しているエリアで利用可能。 エリアは、事業者がWBAへ、申請し合意を 得ることで、フェデレーションへの参加が可能に なるので包括的／動的に広がる。 SSIDに接続が依存しない。

※ 高セキュリティWi-Fiの定義：暗号化され、セキュリティが信頼される組織でコントロールされていること

1-8.SSID視点の整理



※ 高セキュリティWi-Fiの定義:暗号化されセキュリティが信頼され組織でコントロールされていること
※ 東京都の場合、SSID:cityroamは、Passpointに対応していない端末用、地域によっては、Passpointの場合があります。

東京都で、実現する為につかっている技術の話

1-9.OpenRoamingに関連する用語

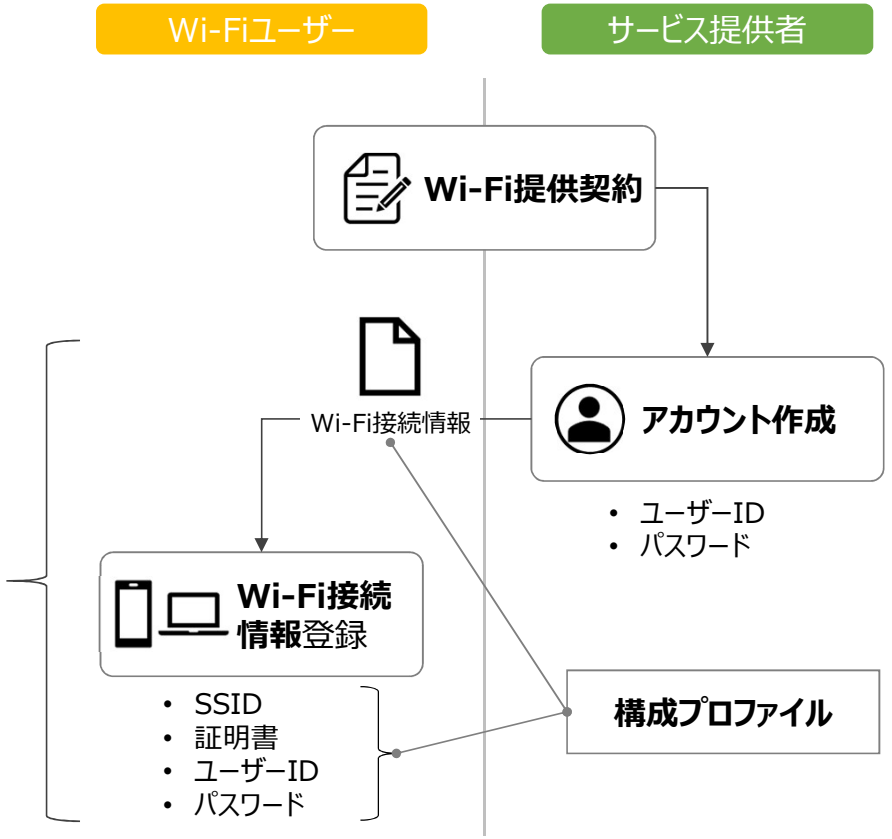
類似の用語が散在するため、各用語の解釈を整理。本資料において特に指定が無い限りは、PasspointとHotspot2.0は同一の意味として扱う

	用語	説明
1	**OpenRoaming**	Hotspot2.0の認証方式を中心として、グローバルな無線エコシステム内で、高セキュリティWi-Fiを活用しシームレスで相互運用可能なサービス体験を実現する為に、WBAによって開発されたフレームワーク
2	**Passpoint**	Wi-Fi Allianceが提供する認定プログラムの名称。Wi-Fi Alliance Hotspot 2.0の仕様に基づくデバイスに対して認定を与える 参考: https://www.wi-fi.org/ja/news-events/newsroom/wi-fi-alliance-wi-fi
3	**Hotspot2.0**	IEEE 802.11uのセキュリティ上の課題を解決するために、認証方式について見直しが行われた規格(技術仕様) ※ 規格の正式名称であるため、規格仕様等のドキュメントをWeb検索する場合は「Hotspot2.0」の用語を用いた検索が望ましい
4	**IEEE 802.11u**	IEEEにより標準化された、SSIDによらず自動的に無線LANの接続先を選択するための規格 参考: https://standards.ieee.org/ieee/802.11u/3694/

1-10.プロビジョニングに関する用語定義

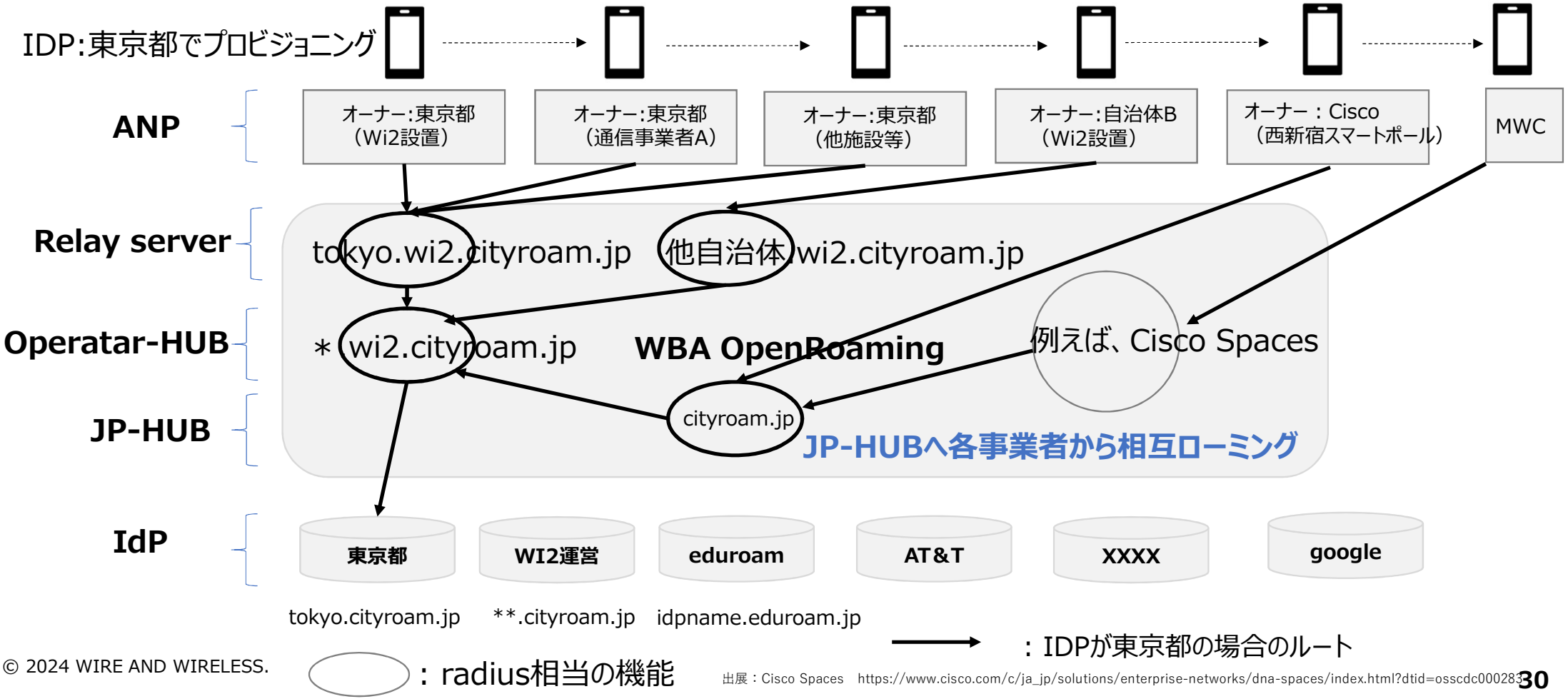
本資料では、アカウント作成から端末にWi-Fi接続情報を登録するまでの一連の流れを**プロビジョニング**と呼ぶ。また、端末に登録されたWi-Fi接続情報、及びWi-Fi接続情報を端末にインストールためのファイルを**構成プロファイル**と呼ぶ。プロビジョニングが完了することで、特定のAPへの接続が可能となる

	用語	説明
1	**Wi-Fi提供契約**	Wi-Fiユーザーとサービス提供者(及びネットワーク提供者)間で結ぶ、Wi-Fi提供契約
2	**アカウント作成**	サービス提供者側でアカウント情報を作成(ユーザーID/パスワードの発行等)
3	**Wi-Fi接続情報**	Wi-Fiに接続するための情報。SSIDの他、EAP-TTLSの場合は、証明書、ユーザーID、パスワード等
4	**構成プロファイル**	端末に登録されたWi-Fi接続情報、及びWi-Fi接続情報を端末にインストールためのファイル
5	**プロビジョニング**	アカウント作成からWi-Fi接続情報登録までの一連の流れ



1-11-1.OpenRoamig(TOKYO_FREE_Wi-Fi）のネットワーク基本構成

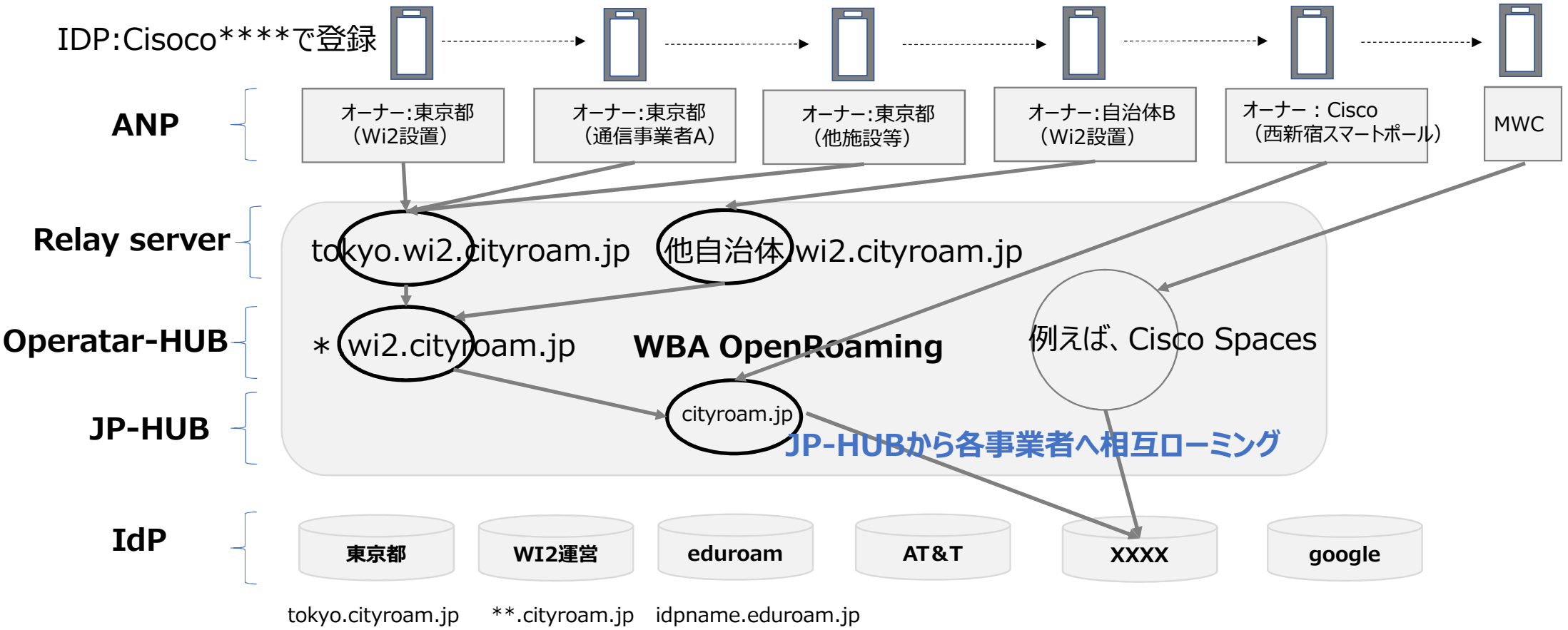
Passpointで接続された端末が、フェデレーションに参加している事業者間でシームレスな接続可能なように
ルールが定められており、階層的なRadius連携可能構成がとられており、レルムで各IDPにルーティングされ認証される。



出展：Cisco Spaces　https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/dna-spaces/index.html?dtid=osscdc000283

1-11-2.OpenRoamig(TOKYO_FREE_Wi-Fi）のネットワーク基本構成

Passpointで接続された端末が、フェデレーションに参加している事業者間でシームレスな接続可能なように
ルールが定められており、階層的なRadius連携可能構成がとられている。レルムで各IDPにルーティングされ認証される。



出展：Cisco Spaces　https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/dna-spaces/index.html?dtid=osscdc000283

2-1.Passpointの特徴

Passpointの特徴として、大きく「自動接続」「セキュア」「簡易プロビジョニング」及び「ローミング協定」を、標準機能として提供することが挙げられる

1. 自動接続

✓ Passpoint対応ホットスポットでは、**SSIDに依らずに自動接続**が可能

2. セキュア

✓ 規格レベルで**WPA2-Enterpriseを必須要件**とすることで、盗聴やアカウントなりすましに対する脅威・脆弱性を排除

3. 簡易プロビジョニング

✓ Webサイト上で**ワンタップで簡易的に**プロビジョニングが可能
✓ **OSU(Online Sign-Up)**によりWi-Fi接続前でも**ホットスポット内でプロビジョニング**が可能

4. ローミング協定

✓ ネットワーク提供者間でローミング協定を結ぶことで、**ネットワーク提供者間でのPasspoint対応ホットスポット内での自動接続が可能**

2-2.Passpointと既存Wi-Fiとの比較

PC/SP（スマートホン）双方において、アプリ開発無しで、簡易プロビジョニングかつ高セキュリティのWi-Fi提供が可能。
またSSIDに依らないAP接続により、1回のプロビジョニングで複数の異なるホットスポットへの接続が可能

さらに

ホットスポットでのAPへの接続がSSIDに依らないため、LO間接続/ローミングパートナーの追加により、
1回のプロビジョニングで複数の異なるホットスポットへの接続が可能

2-3.OpenRoamingの特徴

OpenRoamingの特徴として、PASSPOINTの特徴である「自動接続」「セキュア」「簡易プロビジョニング」標準機能を使い
WBAで定められたフレームワークに則りシームレスのローミングを可能にした仕組み

1. 自動接続

- ✓ Passpoint対応ホットスポットでは、**SSIDに依らずに自動接続**が可能

2. セキュア

- ✓ 規格レベルで**WPA2-Enterpriseを必須要件**とすることで、盗聴やアカウントなりすましに対する脅威・脆弱性を排除

3. 簡易プロビジョニング

- ✓ Webサイト上で**ワンタップで簡易的に**プロビジョニングが可能
- ✓ **OSU(Online Sign-Up)**によりWi-Fi接続前でも**ホットスポット内でプロビジョニング**が可能

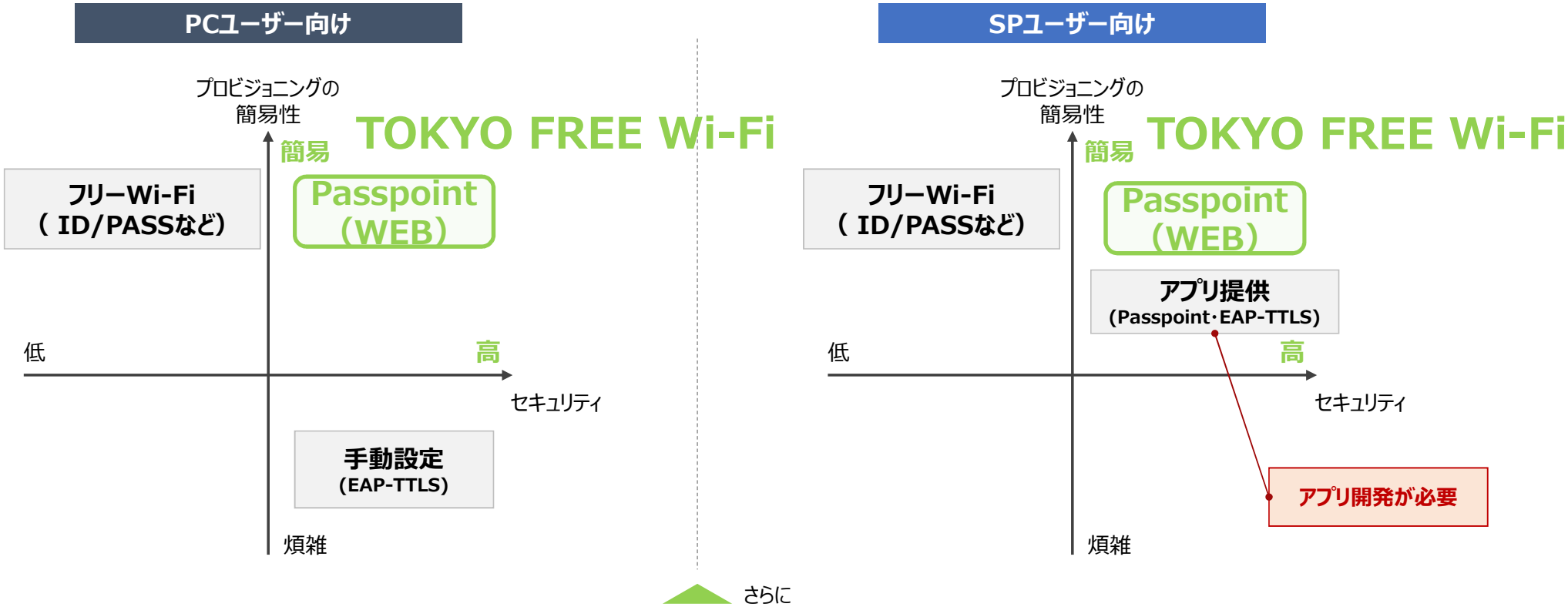
WBA

4. ローミング協定

- ✓ ネットワーク提供者間でローミング協定を結ぶことで、**ネットワーク提供者間でのPasspoint対応ホットスポット内での自動接続が可能**

2-4.OpenRoamingと既存Wi-Fiとの比較

PC/SP（スマートホン）双方において、アプリ開発無しで、簡易プロビジョニングかつ高セキュリティのWi-Fi提供が可能。
またSSIDに依らないAP接続により、1回のプロビジョニングで複数の異なるホットスポットへの接続が可能



さらに

ホットスポットでのAPへの接続がSSIDに依らないため、LO間接続/ローミングパートナーの追加により、
1回のプロビジョニングでOpenRoamingに参加している世界の事業者で接続が可能

2-5. MWC（バルセロナ）での接続例

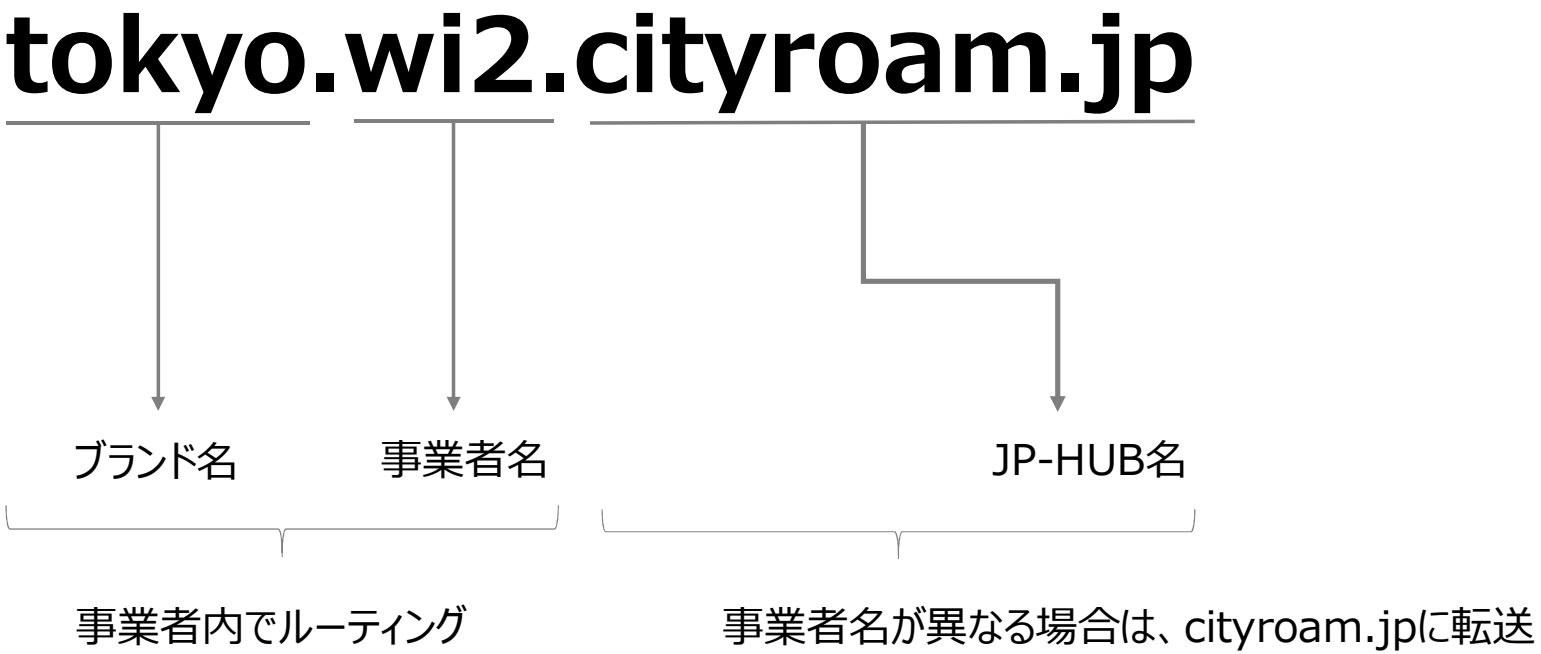
いつ：MWC（バルセロナ）期間

どこで：MWC（バルセロナ）会場で

なにで：MWC現地で発波している
SSID:MWC2023 OpenRoamingで

どうやって：TOKYO FREE Wi-Fiの
プロビジョニングファイルで接続

2-6. レルムのルール



3-1.EAP-TTLSとの比較（概要）

簡易化されたプロビジョニング、及びSSIDに依らない自動接続の面で、従来のEAP-TTLSと区別される

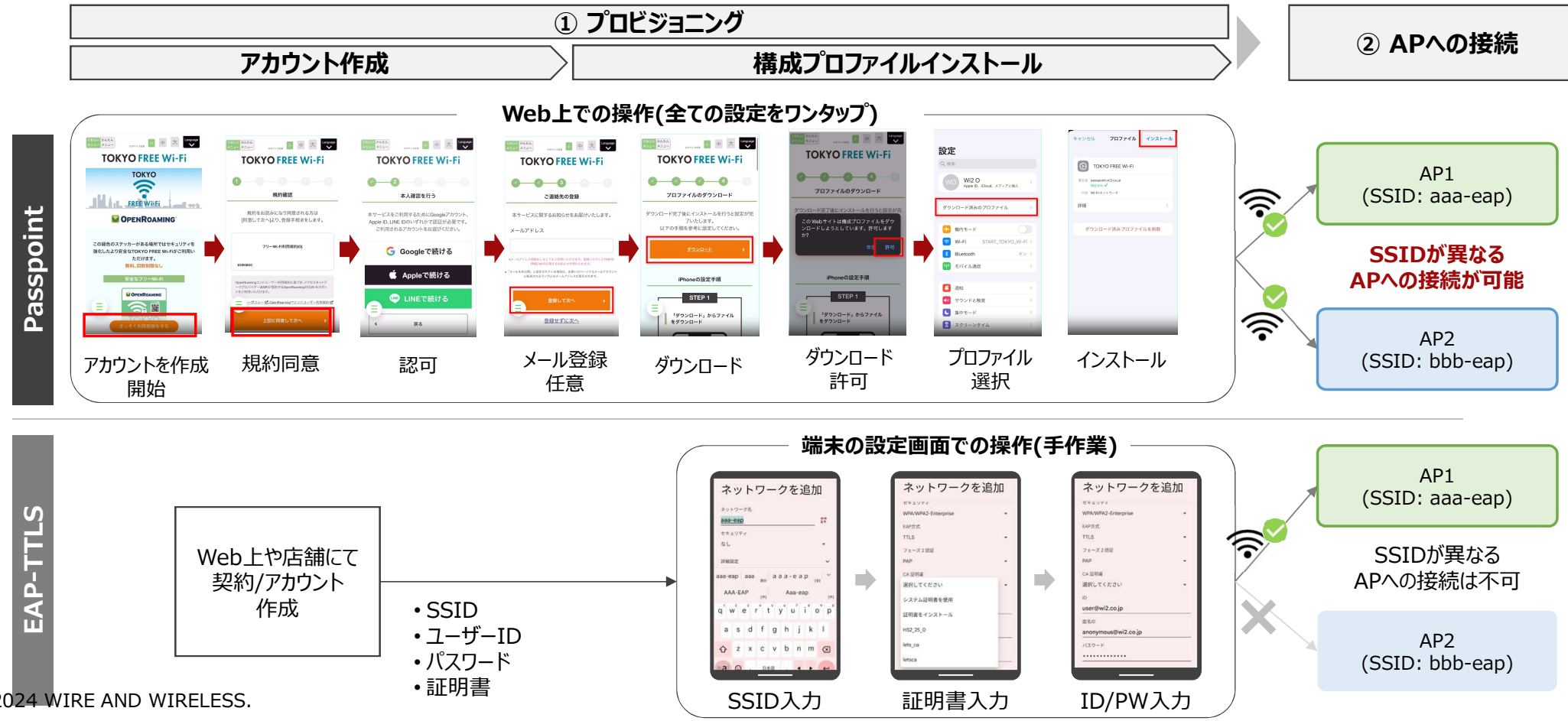
	Passpoint	EAP-TTLS
① プロビジョニング	**ワンタップでの簡易プロビジョニング**	【Android以外】 ワンタップでの簡易プロビジョニング 【Android】 手作業/アプリでのプロビジョニング
② APへの接続	**SSIDに依らない自動接続 (IEEE 802.11u)**	• SSIDを基にした自動接続
③ 認証	IEEE 802.1XによるEAP認証 ※ EAPでTTLSを使用する場合はEAP-TTLSと同じ認証仕様	• EAP-TTLS認証
④ Wi-Fi利用	• 認証に成功し、Wi-Fi利用開始	

Passpointでは、ホットスポットでのAPへの接続がSSIDに依らないため、LO間接続/ローミングパートナーの追加により、**1回のプロビジョニングでSSIDが異なる複数のAPへの接続が可能**

例: 国内のカフェでプロビジョニングしたユーザーが海外の空港に行った際に、ユーザーが意識することなく自動的にWi-Fiに接続される

3-2.EAP-TTLSとの比較（プロビジョニング～AP）

Passpointでは、Web上でプロビジョニングが完了。また、1回のプロビジョニングでSSIDの異なる複数のAPへの接続が可能



3-3-1.OpenRoamingプロビジョニングデモ（動画）

iPhone：初期設定方法

TOKYO FREE Wi-Fi(OpenRoaming対応版)

初期設定方法(iPhone版)

3-3-2.OpenRoamingプロビジョニングデモ（動画）

Android：初期設定方法

TOKYO FREE Wi-Fi(OpenRoaming対応版)

初期設定方法(Android版)

3-4.Wi-Fi一覧

Android、MacではFriendly Nameのみが表示され、iPhoneではSSID及びFriendly Nameが表示される。
Windowsについては、接続前は、SSID及びFriendly Name、接続後は、SSIDが表示される

SSID: TOKYO_FREE_Wi-Fi／Wi2_Demo_OpenRoaming

Friendly Name: TOKYO FREE Wi-Fi

Android

Mac

iPhone

Windows

4-1-1.Passpointのリリースバージョン

Passpointでは2012年の規格公開からR1, R2, R3とリリースバージョンを公開。R1では自動接続、R2ではOSU(Online Sign-Up)、R3ではユーザ体験向上が主機能として取り入れられている

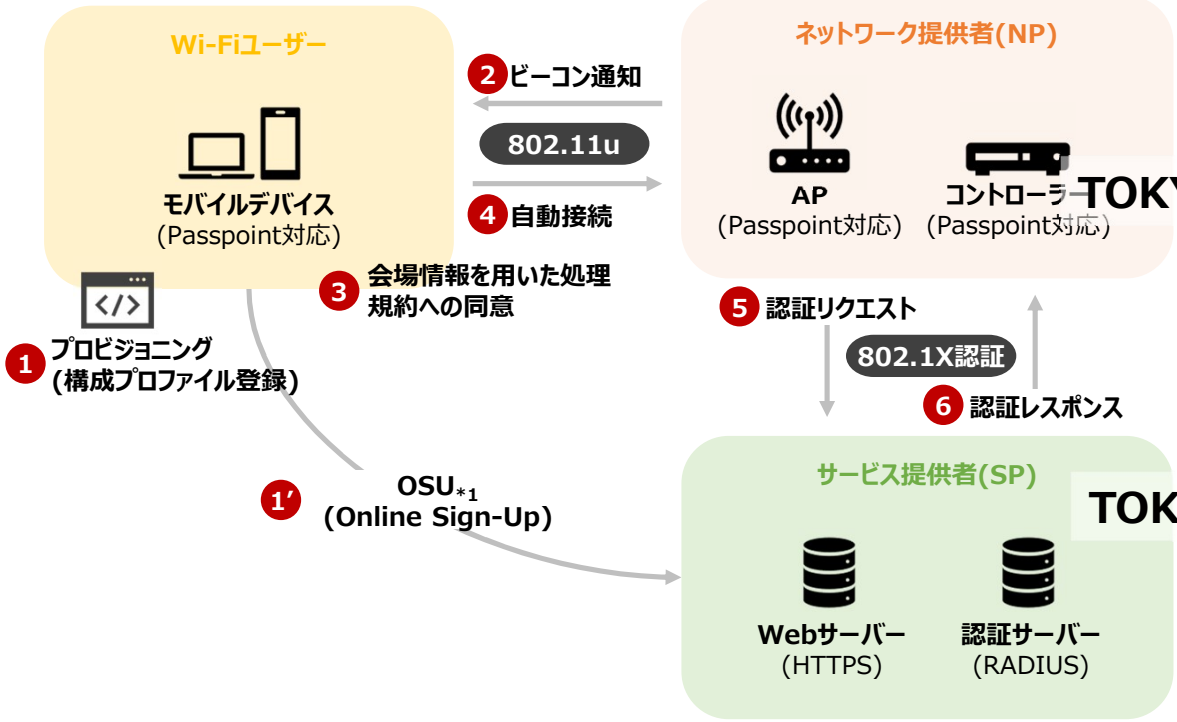
バージョン	主機能(テーマ)	リリース年*1	詳細
R1	自動接続	2012年	• IEEE 802.11uにより、Passpoint対応のAPに対して自動接続 • WPA2-Enterpriseを必須要件とすることでセキュアな通信を実現 • モバイルデバイスへのプロファイルは事前登録
R2	OSU (Online Sign-Up)	2016年	• OSU(Online Sign-Up)機能により、Wi-Fi一覧からセキュアにアカウントを登録する導線を提供 • OSUによるアカウント登録後、モバイルデバイス側での迅速な自動プロビジョニングを実施
R3	ユーザ体験向上	2019年	• 場所や会場によるネットワーク提供に関する規約への同意 • 場所や会場情報のURL通知 (会場の地図、案内、プロモーション、クーポン等の情報を提供) • オペレーターアイコンの通知 • プラン情報に、チャージアドバイスを追加 • OSU時のシングルSSIDの利用

*1: WFAの仕様書「Passpoint_Specification_v3.2」記載のメジャーバージョンを基に記載

4-1-2.Passpointのリリースバージョン

ネットワーク提供者及びサービス提供者によりPasspointの基盤が提供され、 Passpoint対応のモバイルデバイスに
構成プロファイルが登録されていることで自動接続を可能とする

構成・フロー



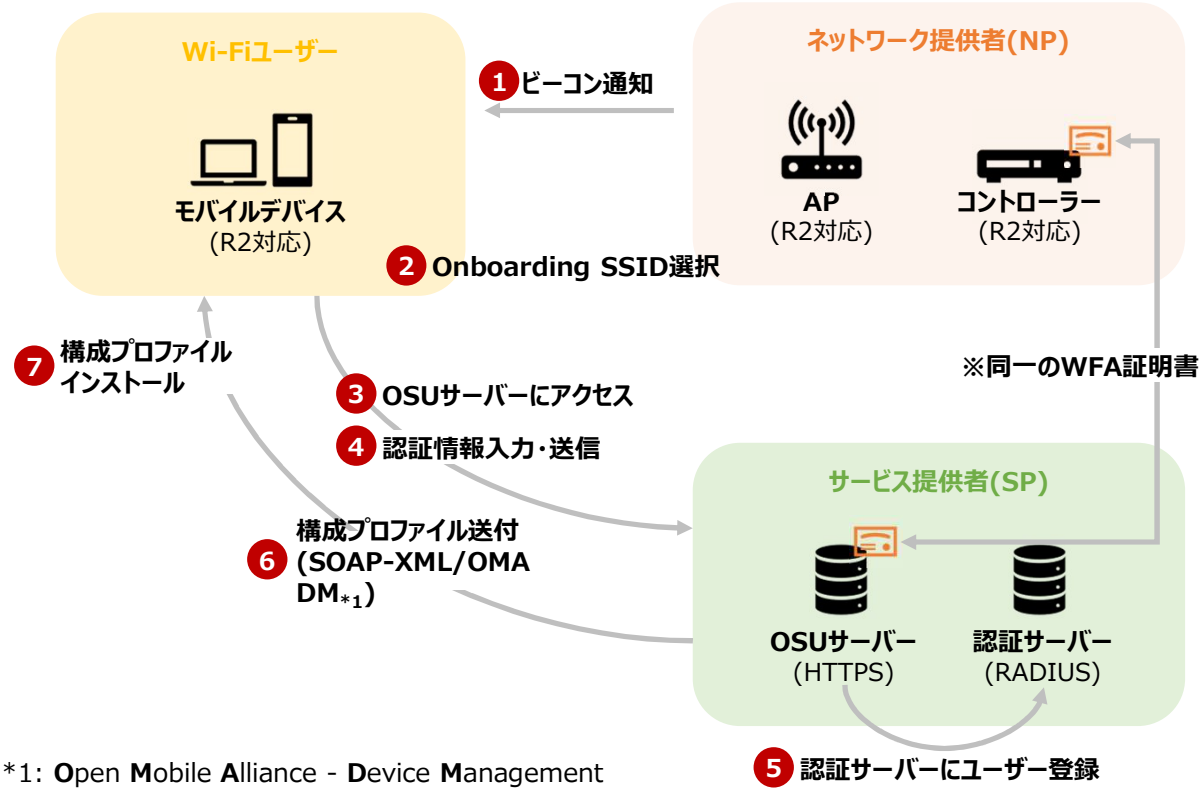
#	バージョン	説明
1	R1	SPが提供するプロビジョニングサイトから構成プロファイル(サーバー証明書・認証情報)を端末にインストール
1′	R2	NPの回線を用いてSPのOSUサイトにアクセスし、構成プロファイルをインストール
2	R1	APからPasspoint対応フラグ、SP情報、NP情報、会場情報等をビーコン通知
	R3	会場情報URL・利用規約等をビーコン通知
3	R3	会場に応じた地図表示・クーポン発行や規約への同意を実施
4	R1	端末が、構成プロファイルとビーコン情報から自動接続判断し接続
5	R1	レルム、SIM等の情報をもとに、適切なSPに対して認証をリクエスト
6	R1	SPが認証処理を行い、認証に成功すればWi-Fi接続完了

*1: 次ページ以降で詳細を説明

4-2. R2:OSU（Online Sign-Up）のイメージ（参考）

ネットワーク提供者(NP)側にあらかじめサービス提供者(SP)が提供するOSUサイトのURLを登録しておくことで、ユーザーはAPから提供される回線でOSUサイトにアクセスし、サインアップが可能

構成・フロー

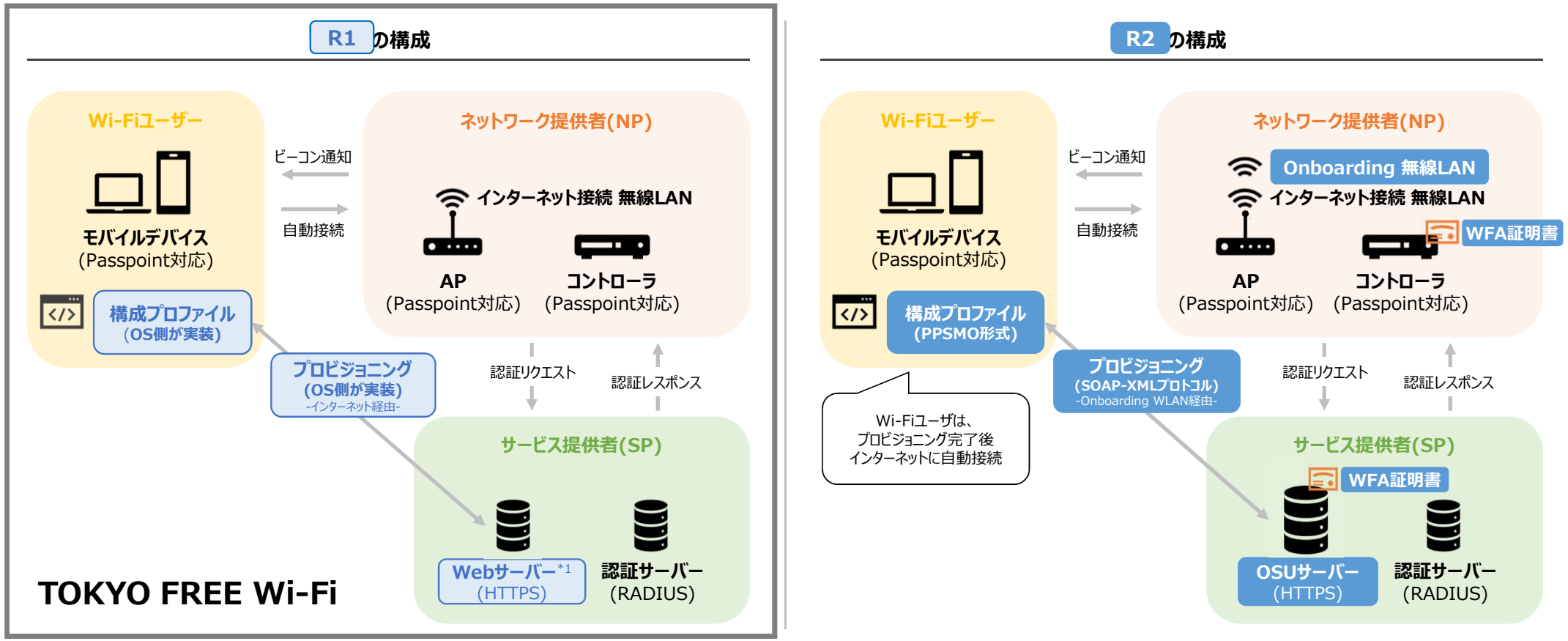


*1: **O**pen **M**obile **A**lliance - **D**evice **M**anagement

#	説明
1	APから、事前登録されたOSU用SSID(Friendly Name)及びOSUサイトのURLをビーコン通知
2	モバイルデバイスのSSID一覧からOSU用のSSID(「Tap to sign up」の記載あり)を選択
3	NPの回線を使用し、OSUサーバーにHTTPSでアクセス。OSUサーバーおよびAPコントローラには**同一のWFA認証局のサーバー証明書が必要**
4	OSUサイト上で認証情報を入力し送信。OSUサイトの画面UI・入力項目はSPで任意に設定
5	SP内でOSUサーバーから認証サーバーに対してユーザー・アカウント登録を実施
6	SOAP-XMLまたはOMA DMプロトコルにより構成プロファイルを送付
7	モバイルデバイスにて、構成プロファイルを自動インストール

4-3.R1とR2の構成比較

R1と比較すると、R2はプロビジョニング(SOAP-XMLに基づく実装)と構成プロファイル(PPSMO形式)に強い制約がある。
さらに、R2ではWFA証明書が登録されたOSUサーバーおよびOnboarding 無線LANの構築が必要。
※ 各構成の詳細については後続ページで説明



*1: R1のWebサーバーはR2ではOSUサーバーとして代替され、Onboarding 無線LAN経由でプロビジョニングが実施される

4-4.Passpoint OS対応状況

R1はほとんどのデバイスで対応済みだが、R2はApple製品が非対応、R3については現時点の対応は稀有。
また、Android以外の端末ではワンタップでEAP-TTLSのプロビジョニングが可能

2022年7月時点

機能 (R1～R3はPasspoint)	Wi-Fiユーザー(モバイルデバイス) Android*1	iOS*2	macOS*2	Windows*2	ネットワーク提供者 AP・コントローラ (Ruckus製品*3)
R1 (自動接続)	**Android6** 以降	**iOS7** 以降	**10.9** 以降	**Windows10** 以降	2012年6月以降販売の **208モデル**が対応
R2 (OSU)	**Android10** 以降*4	対応OSなし	対応OSなし	**Windows10** 以降	2016年1月以降販売の **181モデル**が対応
R3 (ユーザ体験向上)	**Android12** 以降	対応OSなし	対応OSなし	対応OSなし	対応製品なし
EAP-TTLS (ワンタップ*5)	対応OSなし	対応OS調査中	対応OS調査中	対応OS調査中	**EAP-TTLS提供製品**

TOKYO FREE Wi-Fi

*1: AndroidオープンソースプロジェクトのPasspoint項目(https://source.android.google.cn/devices/tech/connect/wifi-passpoint?hl=ja)を参考
*2: SecureW2のサイト(https://www.securew2.com/blog/list-passpoint-operating-systems)を参考
*3: WFA公式のProduct Finder(https://www.wi-fi.org/product-finder-results)にて、認定済み製品検索により調査
*4: **AndroidのVersion11以上はOSU完了後インターネット接続ができることを確認、Version10はOSUサーバ証明書の検証エラーにより接続失敗**
*5: Webサイト上からワンタップでEAP-TTLSの構成ファイルをプロビジョニングし、EAP-TTLSのWi-Fiネットワークに接続

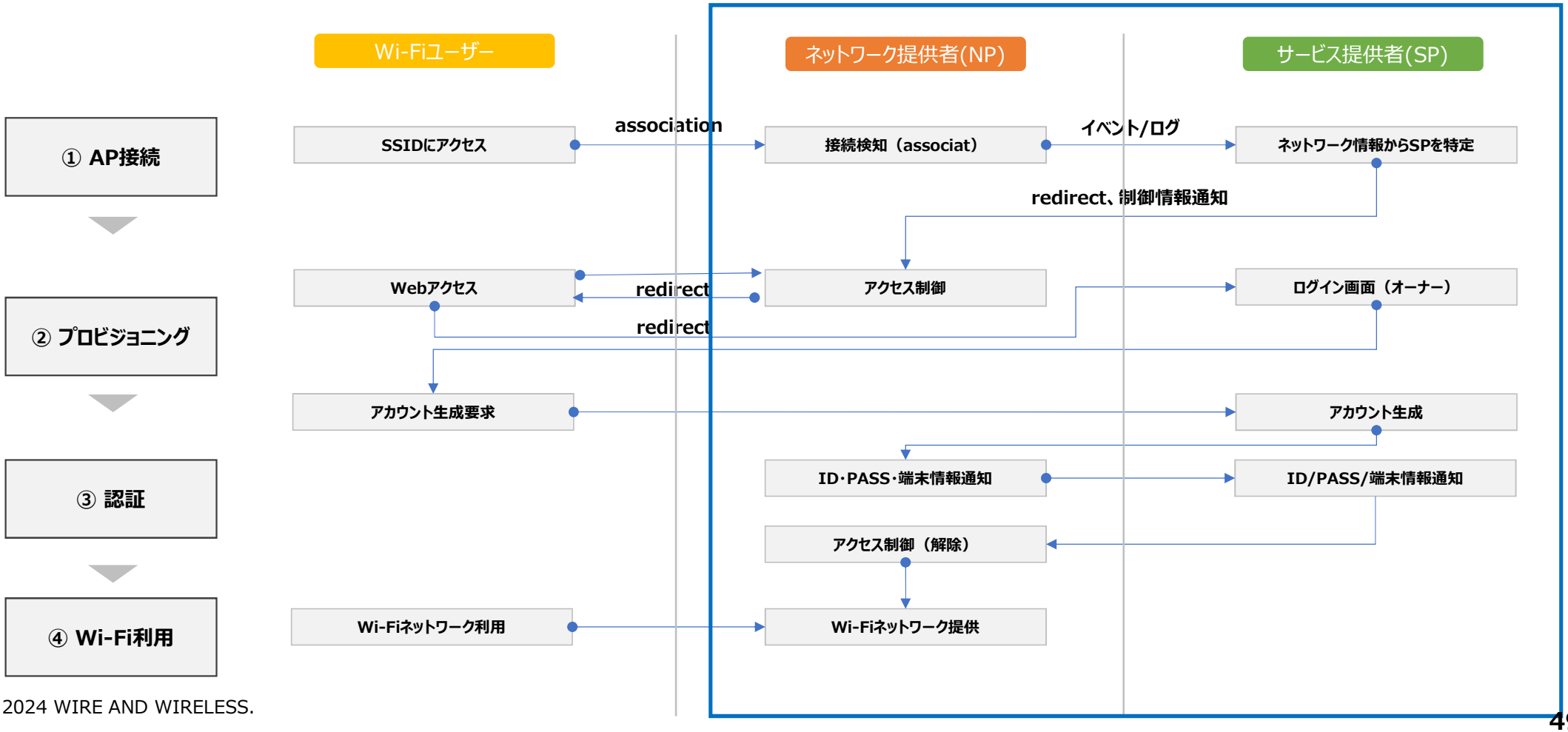
4-5.TOKYO FREE Wi-Fiオンボードでの工夫

R2のサポートが、端末によって異なる為、セキュリティを重視しつつ、既存のキャプティブポータルを工夫

プロビジョニングに必要なアクセス先のみをACLで許可

5-1.従来のフリーWi-Fi

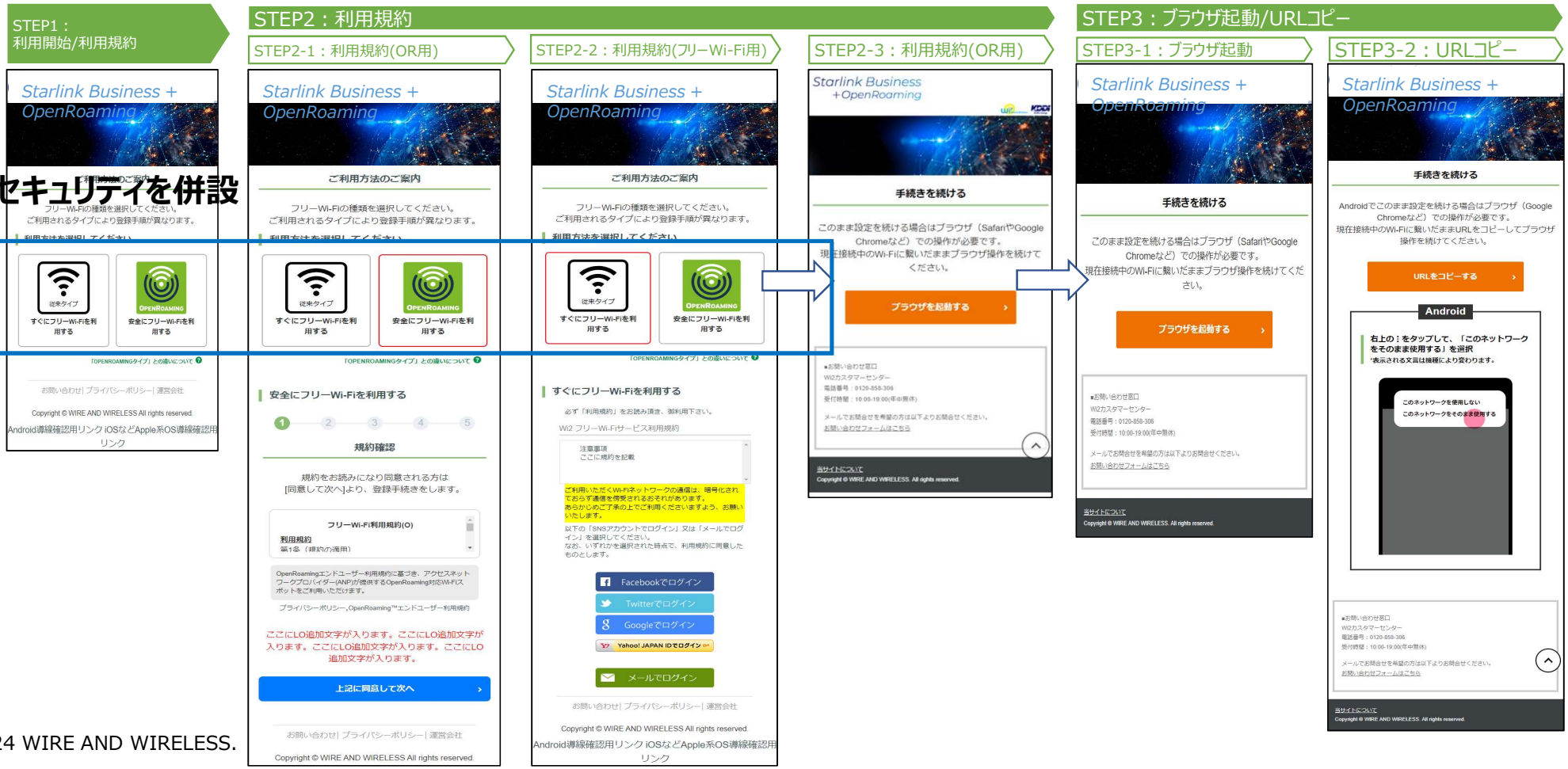
ネットワーク提供者（NP）とサービス提供（SP）は、構造上垂直統合



5-2-1.従来のフリーWi-Fiと高セキュリティWi-Fiの併波

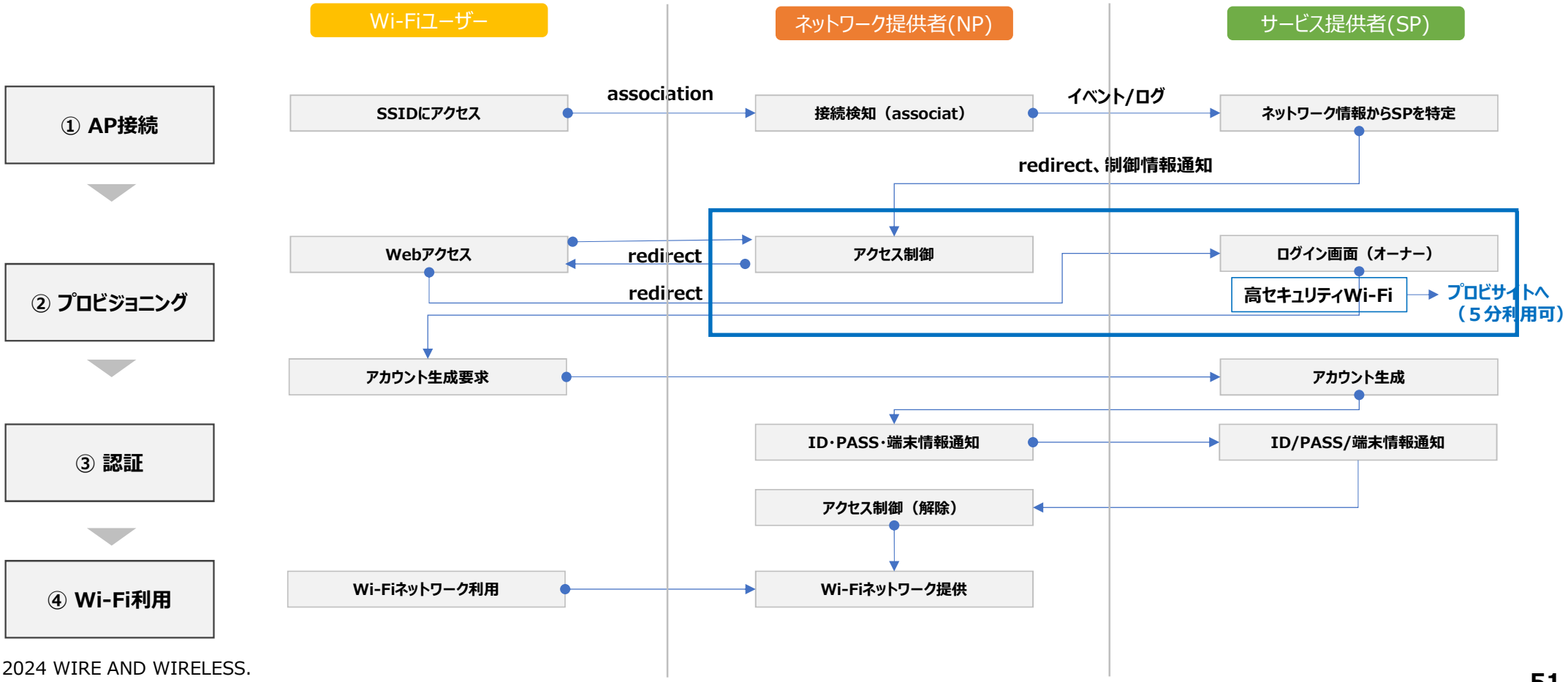
まだ、まだ、普及途上の為、既存のOPENなフリーWi-Fiと併設（Starlinkを利用したOpenRoamingの例）

高セキュリティを併設

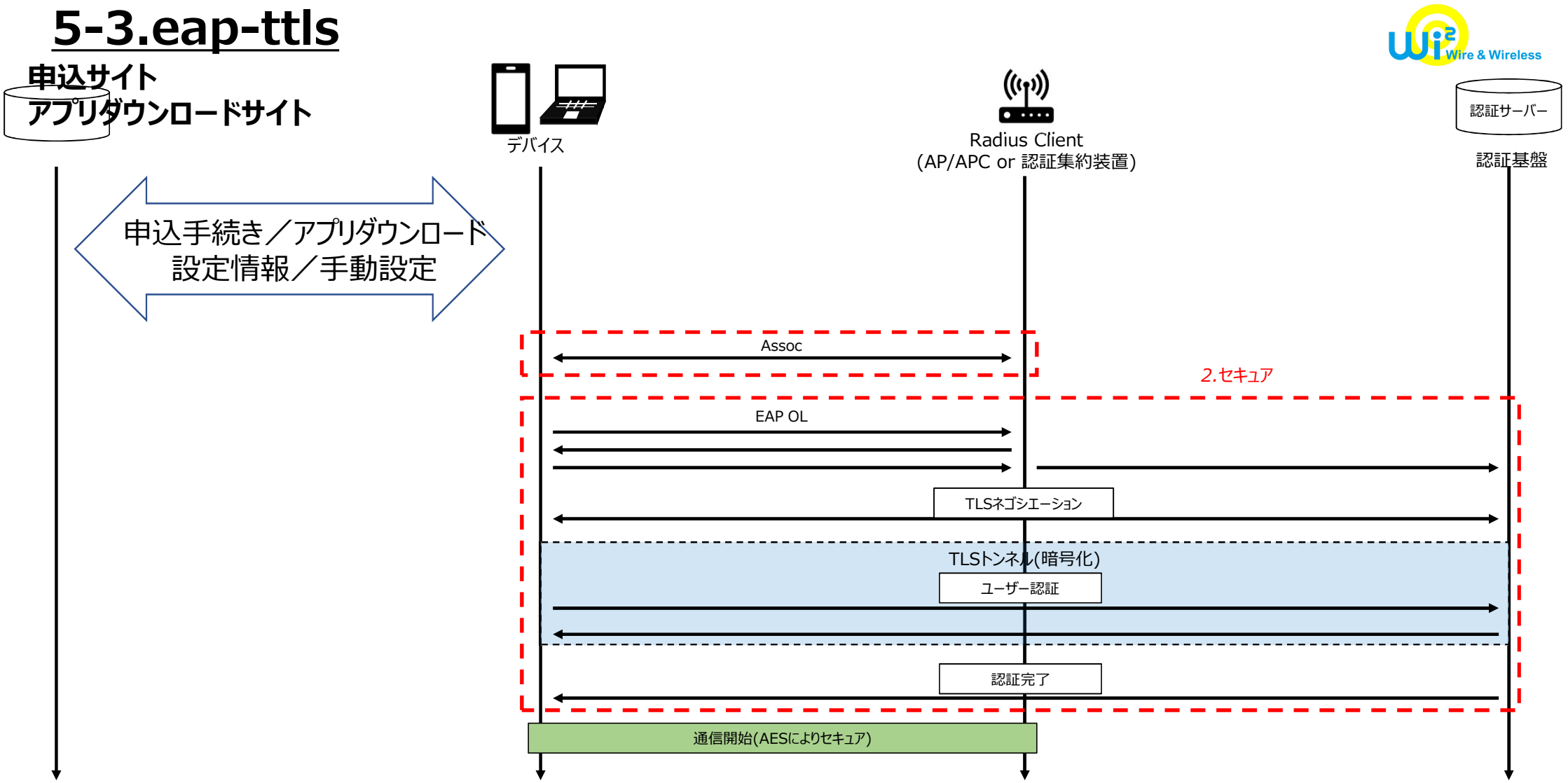


5-2-1.従来のフリーWi-Fiと高セキュリティWi-Fiの併波

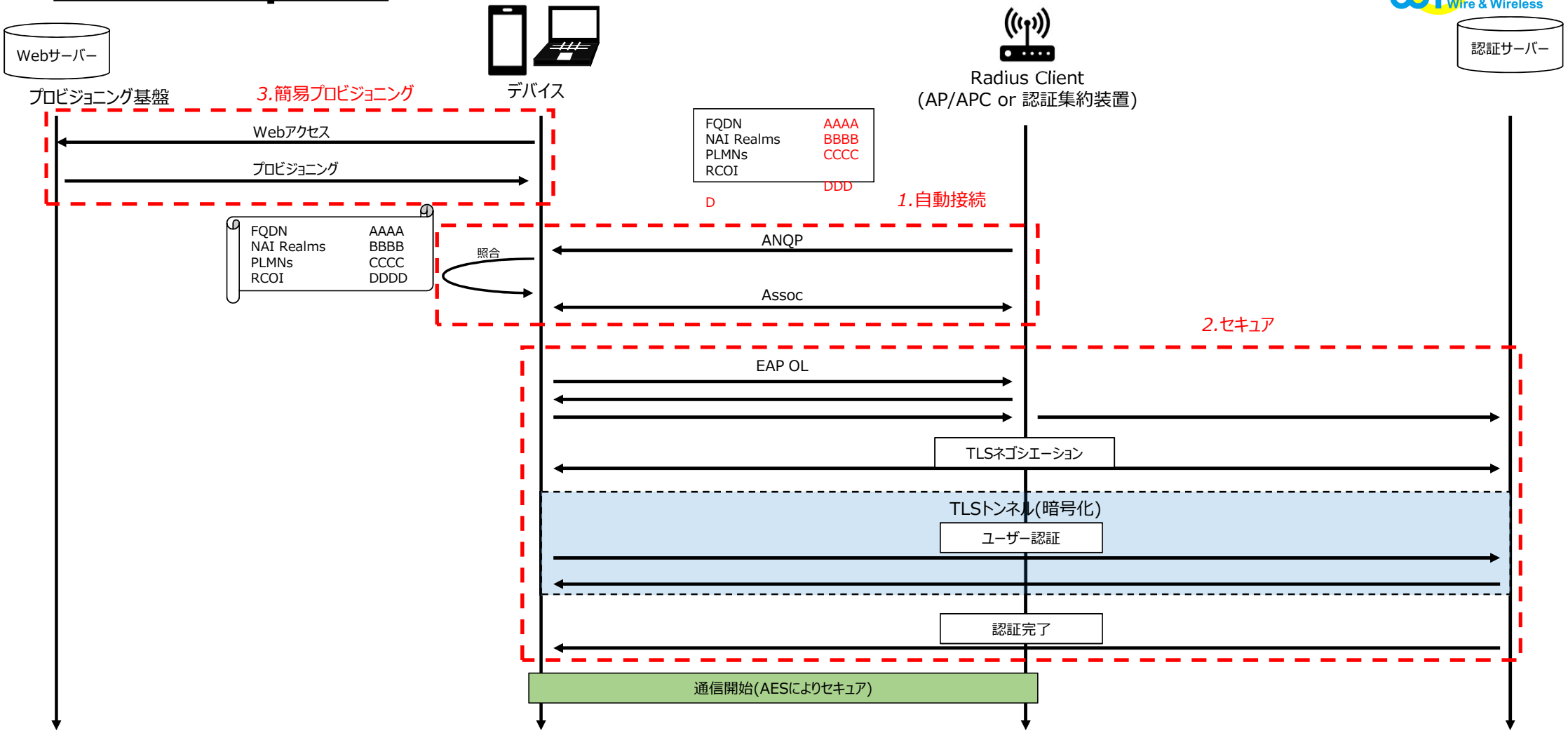
従来のフリーWi-FiとOpenRoamingを併設する場合は、ログイン画面で「高セキュリティWi-Fi」の導線を追加



5-3.eap-ttls

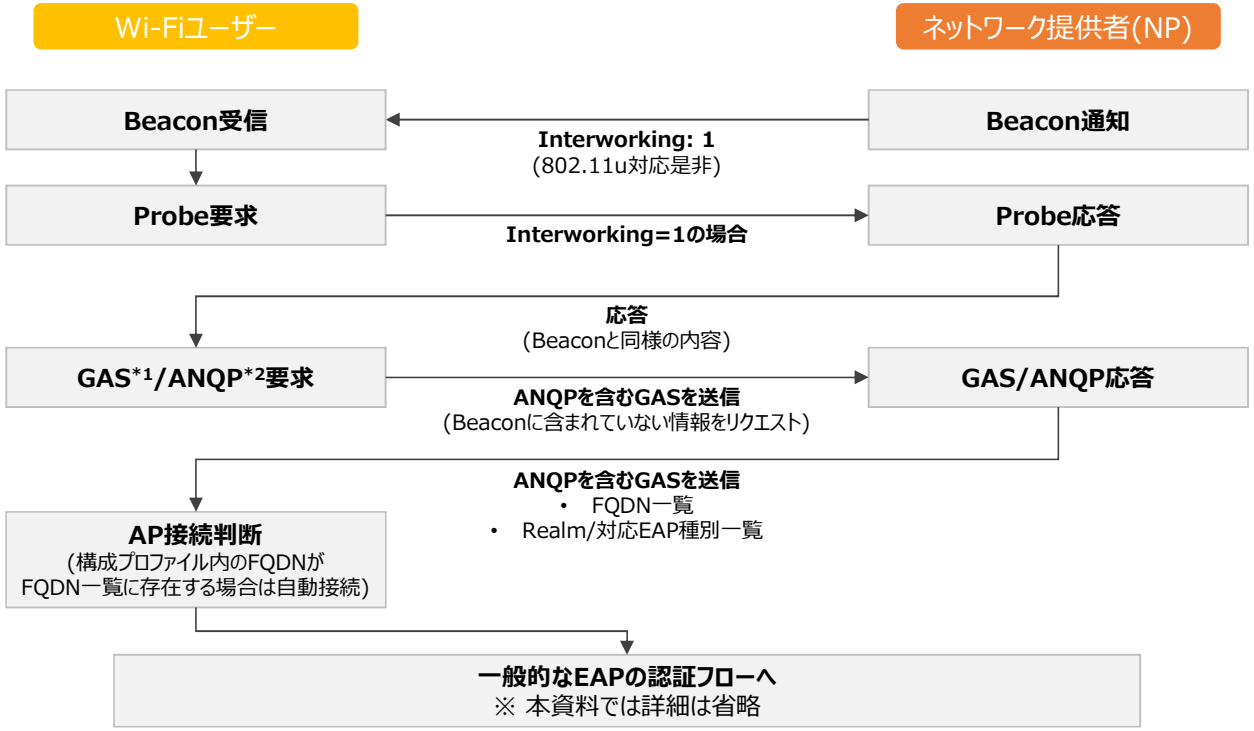


5-4.Passpoint



5-5.AP接続（IEEE 802.11u）

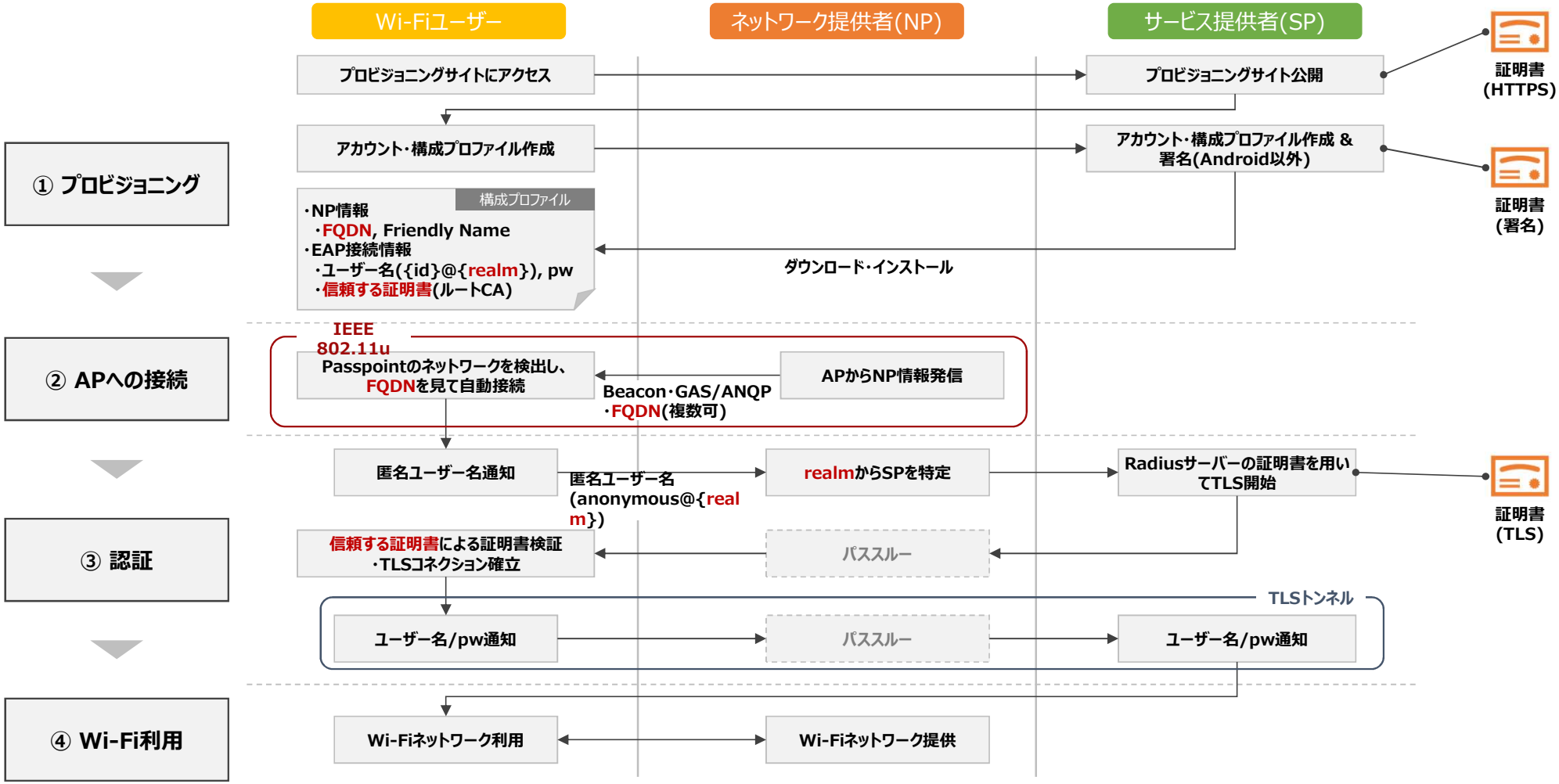
APからBeaconにより802.11u対応是非を受信後、Probe要求を行い、GAS/ANQPにより端末とAP間で必要な情報の相互通信を行った上で、APへの接続を完了し、認証フローに進む



*1: Generic Advertisement Serviceの略。ANQPを送信するためのフレームワーク
*2: Access Network Query Protocolの略。クライアント端末がネットワークの情報を取得するためのクエリプロトコル

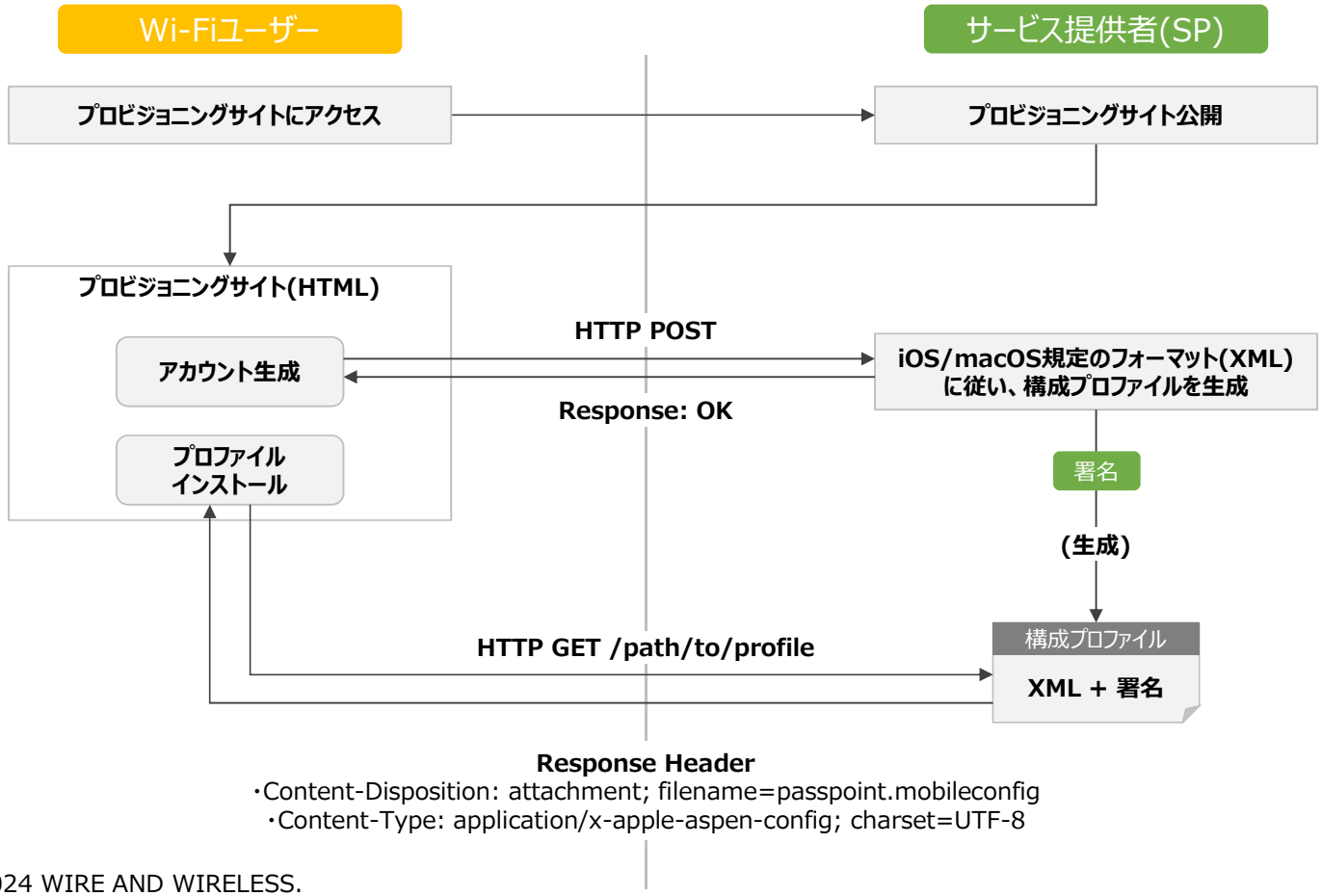
【参考】
- Ruckus. How Interworking Works. https://www.commscope.com/globalassets/digizuite/1528-1358-wp-how-interworking-works.pdf
- CISCO. Wi-Fiの最新技術動向. https://iwparchives.jp/files/pdf/iwp2014/iwp2014-ch04-03-p201.pdf

5-6.全体シーケンス（R1）



5-7.プロビジョニング（R1）（IOS/macOS）

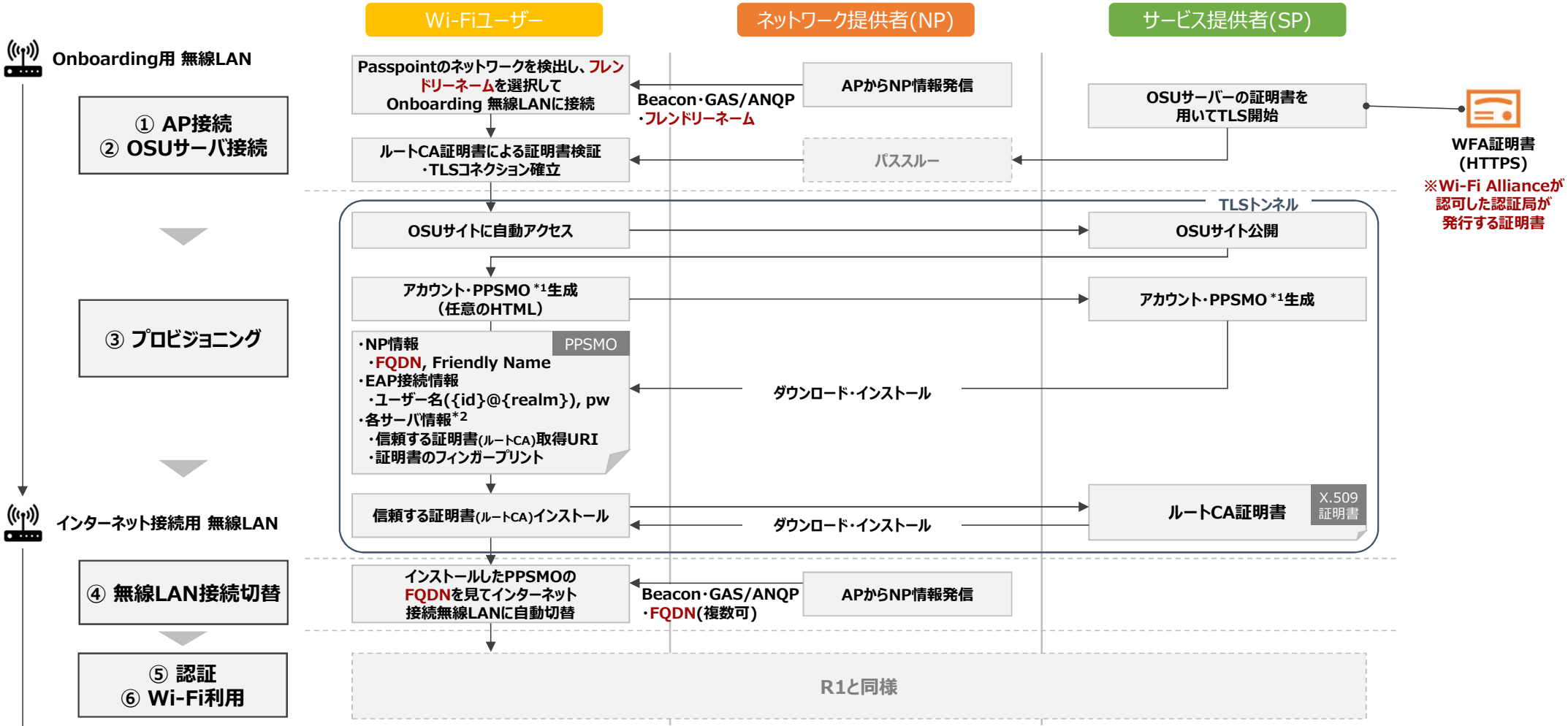
プロビジョニングサイトにアクセスし、HTTPS経由で構成プロファイルをダウンロードし、インストール。
iOS/macOSの場合は署名が必要



iOS/macOS規定のフォーマットは以下参照
https://developer.apple.com/documentation/devicemanagement/configuring_multiple_devices_using_profiles

※ EAP-TTLSの信頼する証明書
(com.apple.security.pkcs1)には**中間証明書(※)**を登録
※ 構成プロファイルへの中間証明書の登録要否確認中

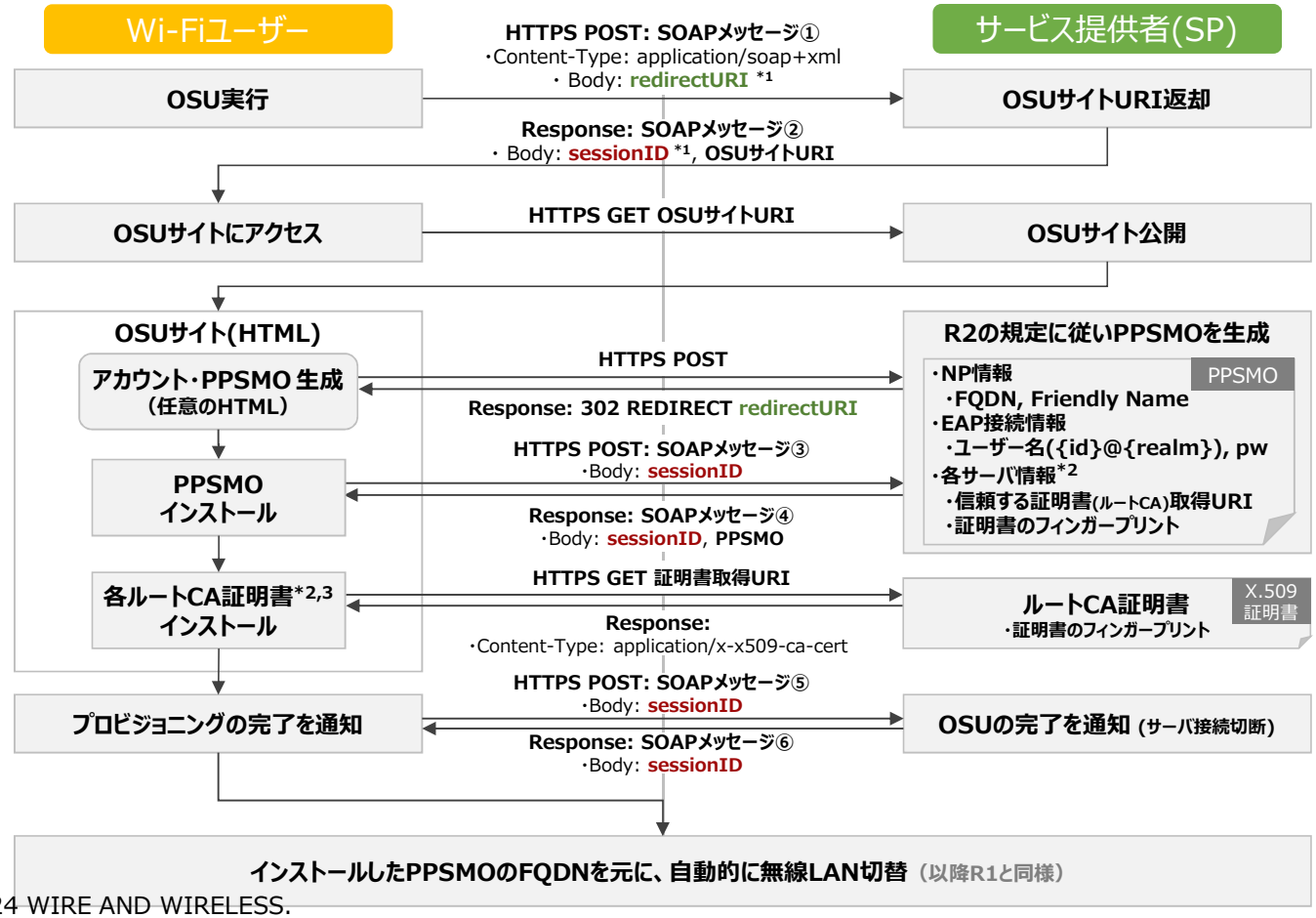
5-8.全体シーケンス（R2）（参考）



*1: PerProviderSubscription-ManagementObjectの略。 Passpoint対応ネットワークの自動接続および認証に利用されるXML形式のデータ
*2: OSUで利用する認証用のAAAサーバ, サブスクリプション更新用のSubscription Remediationサーバ, ネットワーク選択に関するポリシーを管理するPolicyサーバ (任意)

5-9.プロビジョニング（R2）（参考）

OSUサイトにアクセスし、HTTPS経由で**SOAP-XML**を利用して**PPSMO**および**ルートCA証明書**を
ダウンロードし、インストール ※SOAPメッセージおよびPPSMOの詳細に関しては後続ページで説明

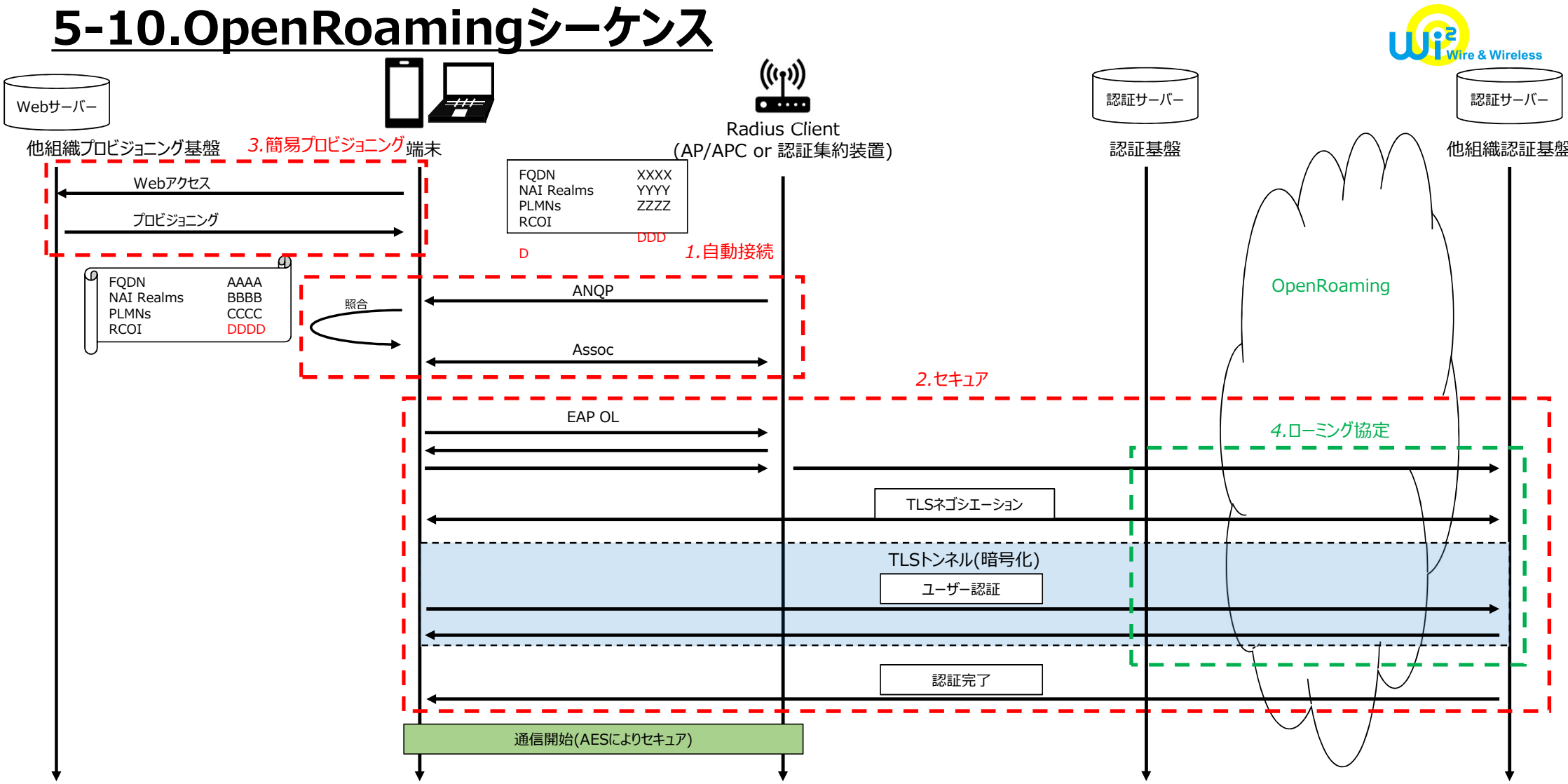


※ **R2規定のSOAPメッセージのフォーマットは**
「Passpoint_Specification_v3.2 (WFA Passpoint仕様書)
8.4節 Provisioning using SOAP XML」を参照

※ **R2規定のPPSMOのフォーマットは**
「Passpoint_Specification_v3.2 (WFA Passpoint仕様書)
9章 Management objects」を参照

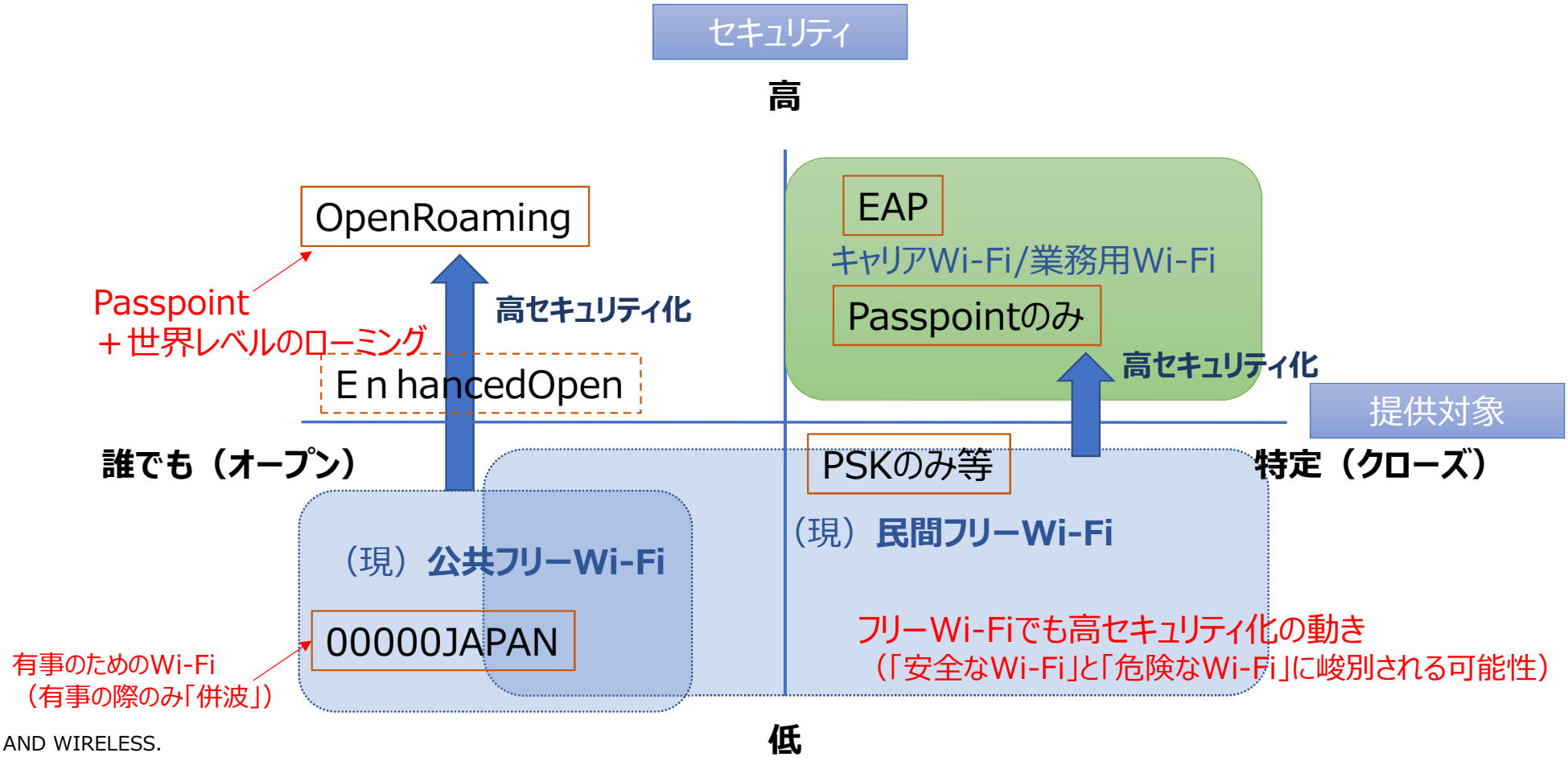
*1: sessionID / redirectURIの値はOSUプロセスごとに固有の値を取るため、KVSなどのDBによって値を管理する必要がある
*2: 認証用AAAサーバ, サブスクリプション更新用サーバ, ネットワーク選択のルールを管理するPolicyサーバ (任意)のルートCA証明書を取得するためのURI
*3: インストール時にダウンロードした証明書のフィンガープリントとPPSMOに登録されたルートCA証明書のフィンガープリントが一致するかを確認

5-10.OpenRoamingシーケンス



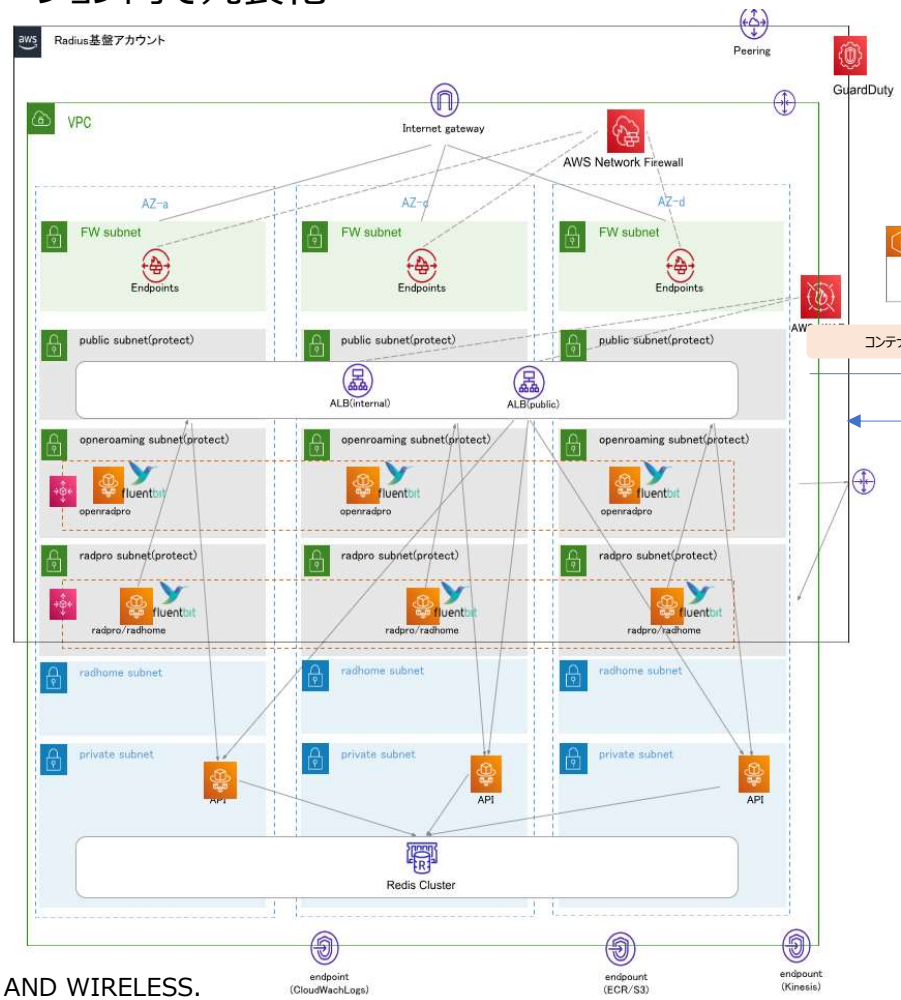
5-11.OpenRoamingの従来サービスとの違い

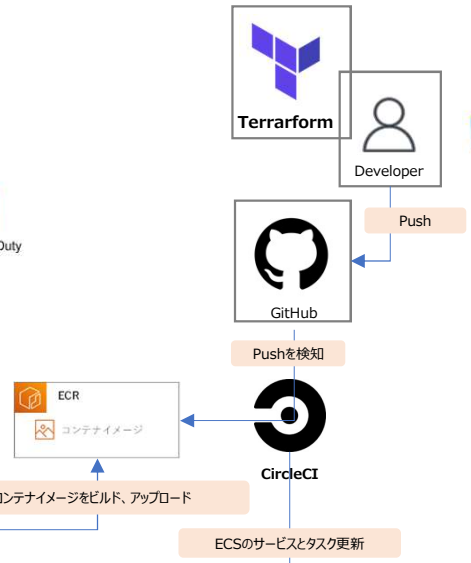
＜安全性向上の動きと適用領域のイメージ＞



6-1.インフラアーキテクチャAS-IS

東京リージョン内で冗長化





サーバー／アプリ監視

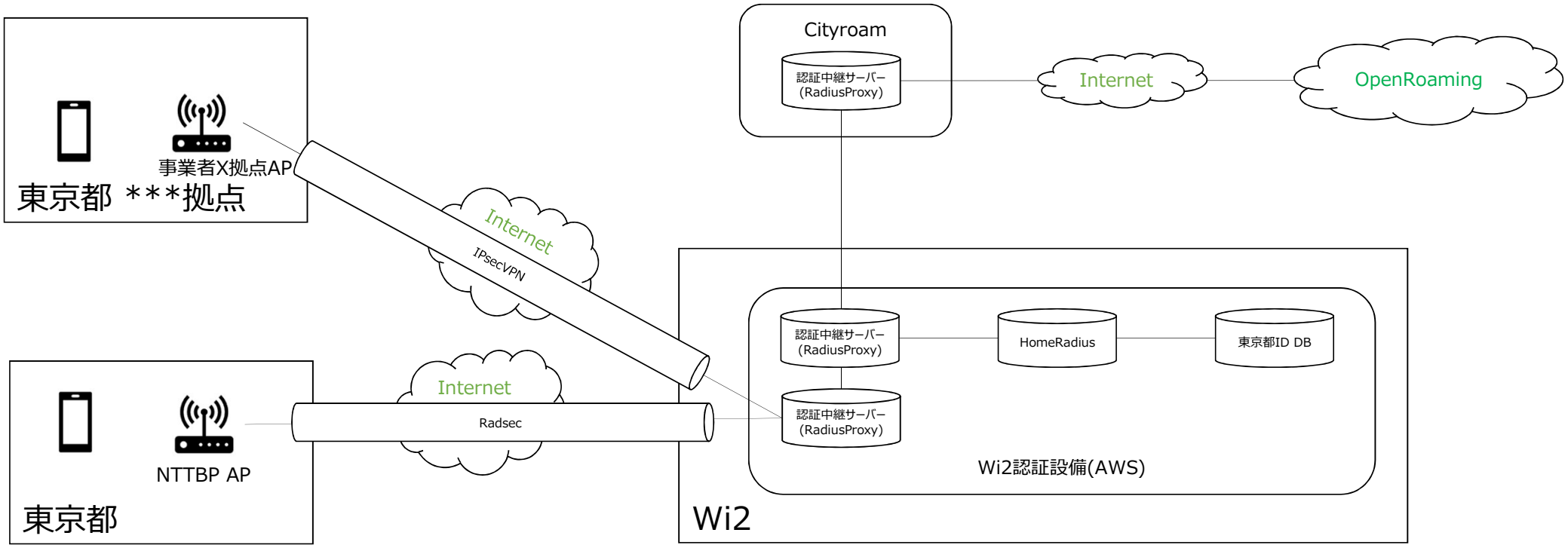
dynatrace

- AWSを利用
- 東京リージョンを利用
- 3AZで対象外弾力性を確保
- コンテナベースで構築
- セキュリティをGuardDuty／WAF／NetworkFirewallで担保
- トランザクションに応じてオートスケール
- リリース前に自動テスト

6-2.事業者間アクセスポイント接続インフラアーキテクチャ

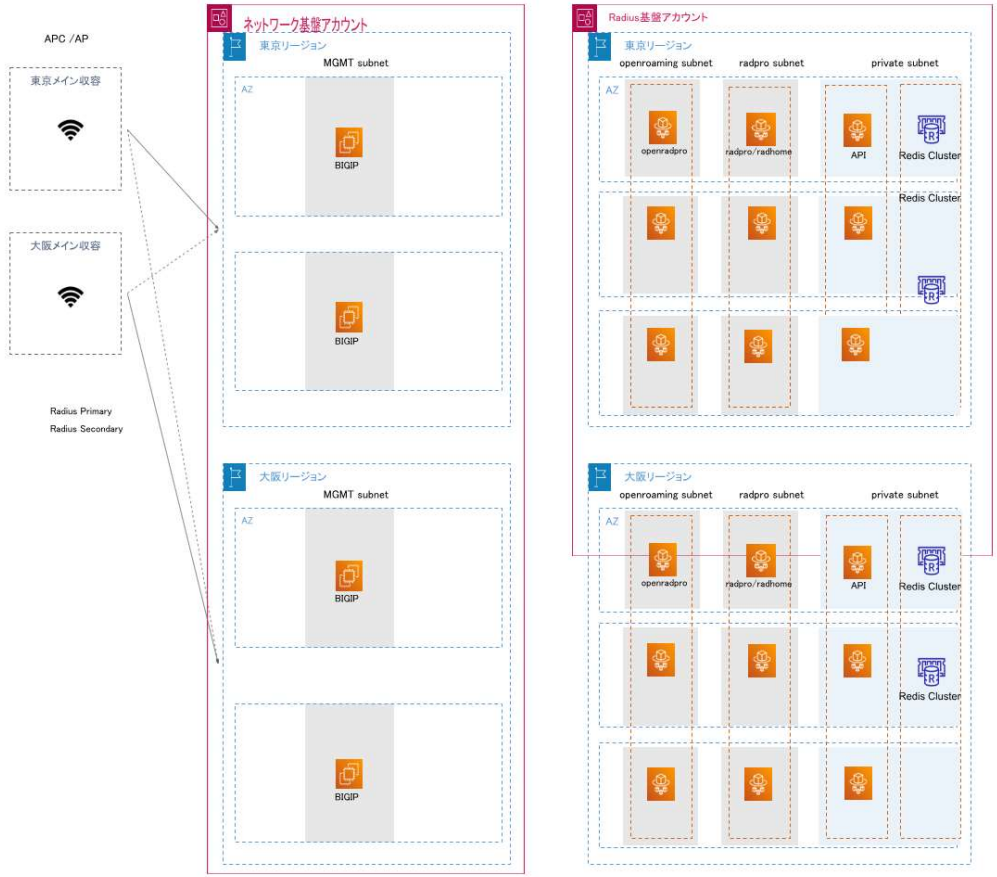
垂直統合では無く、水平分割、相互補完の思想、専用線／IPsecVPN／Radsecで認証中継することが可能。

インフラアーキテクチャは、AWS上に構築（6-1に同じ）



6-3.インフラアーキテクチャTO-BE

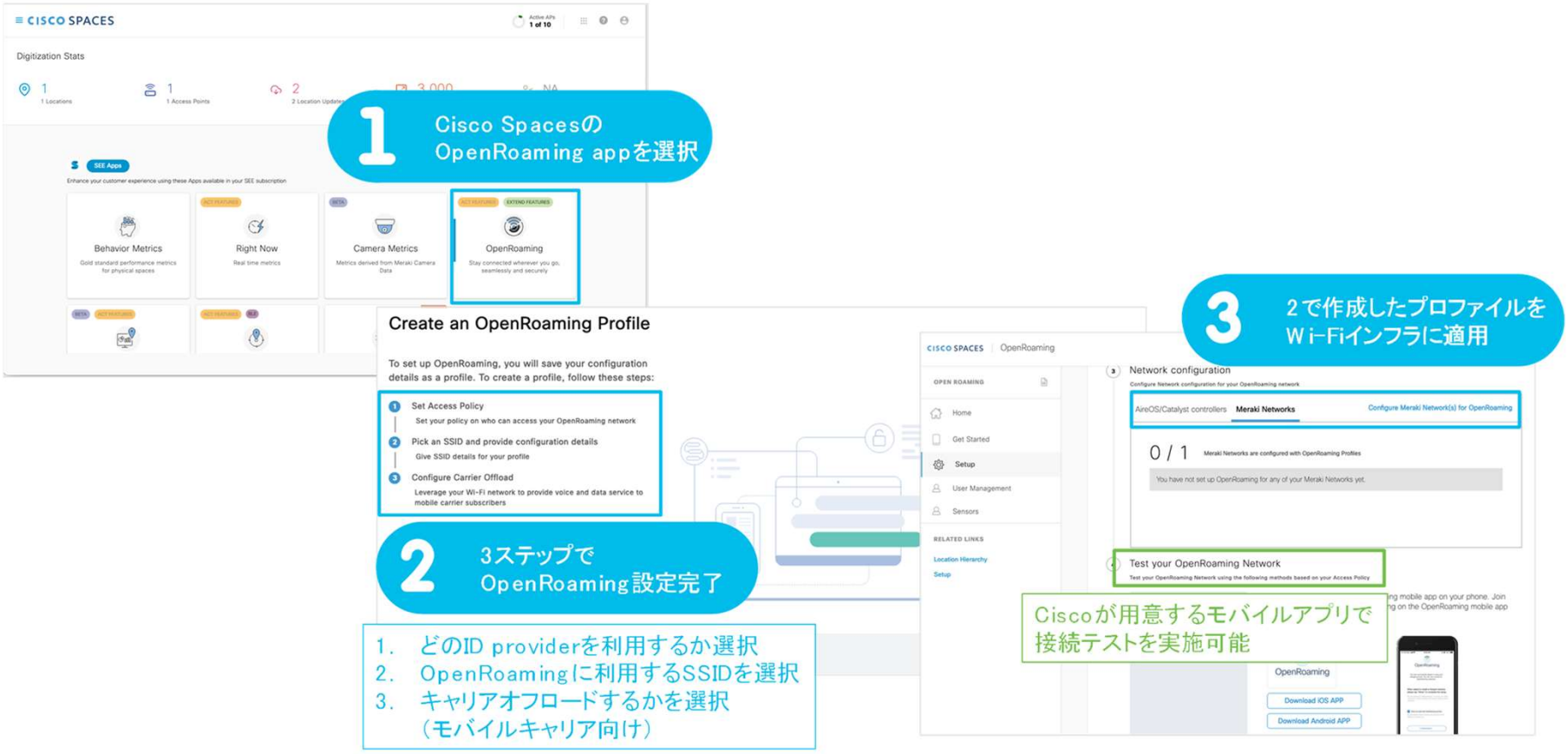
東京リージョンの冗長化に加え、大阪リージョンで冗長化



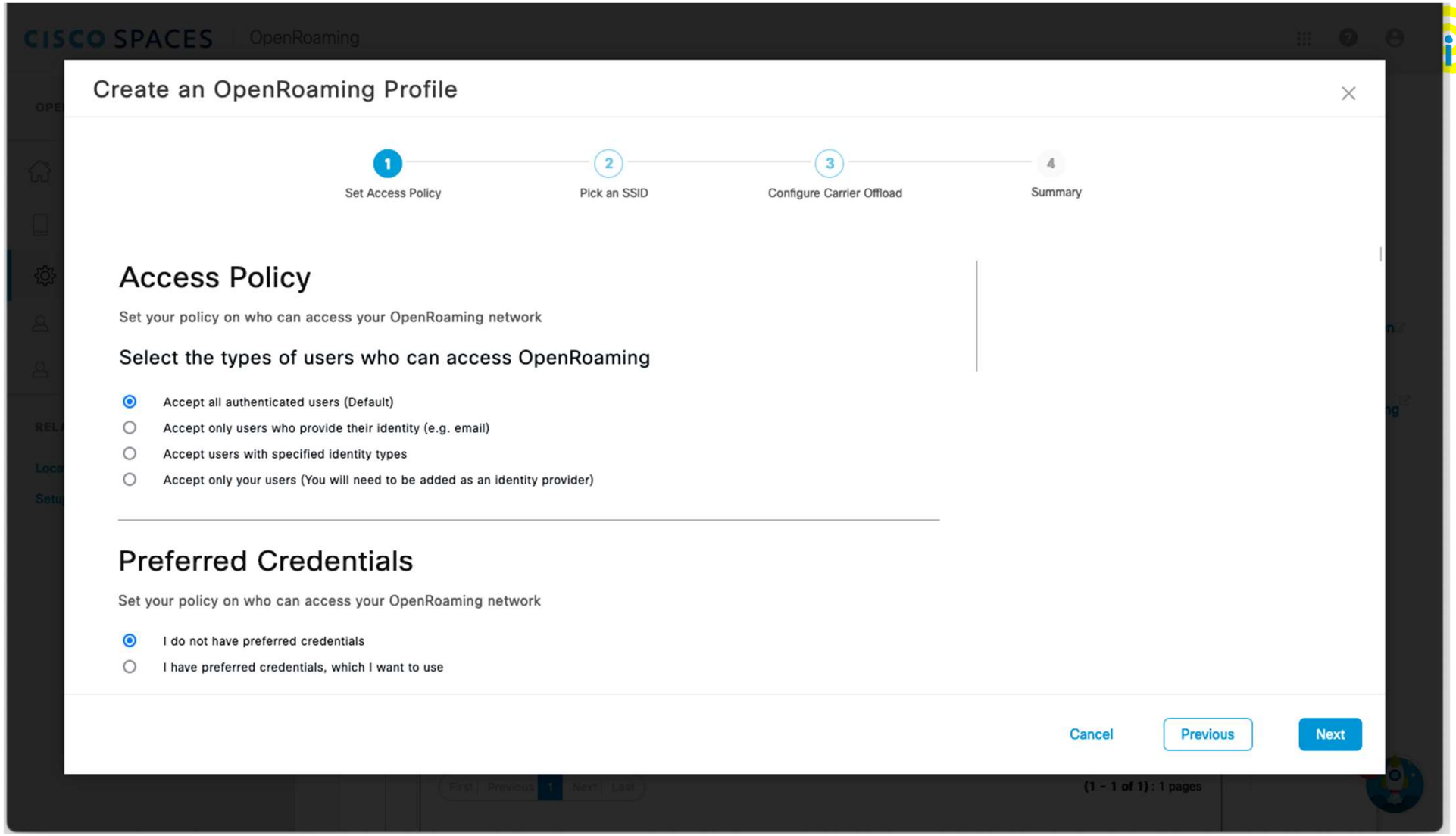
- 7-1-1のアーキテクチャに加え
  大阪リージョンを追加（工事中）
- 東京リージョン、大阪リージョンで
  認証トラフィックを分散
- 災害・障害時にどちらかのリージョンで
  サービスを継続

7-1.AP/コントローラの設定（CISCO SPACES/Meraki）

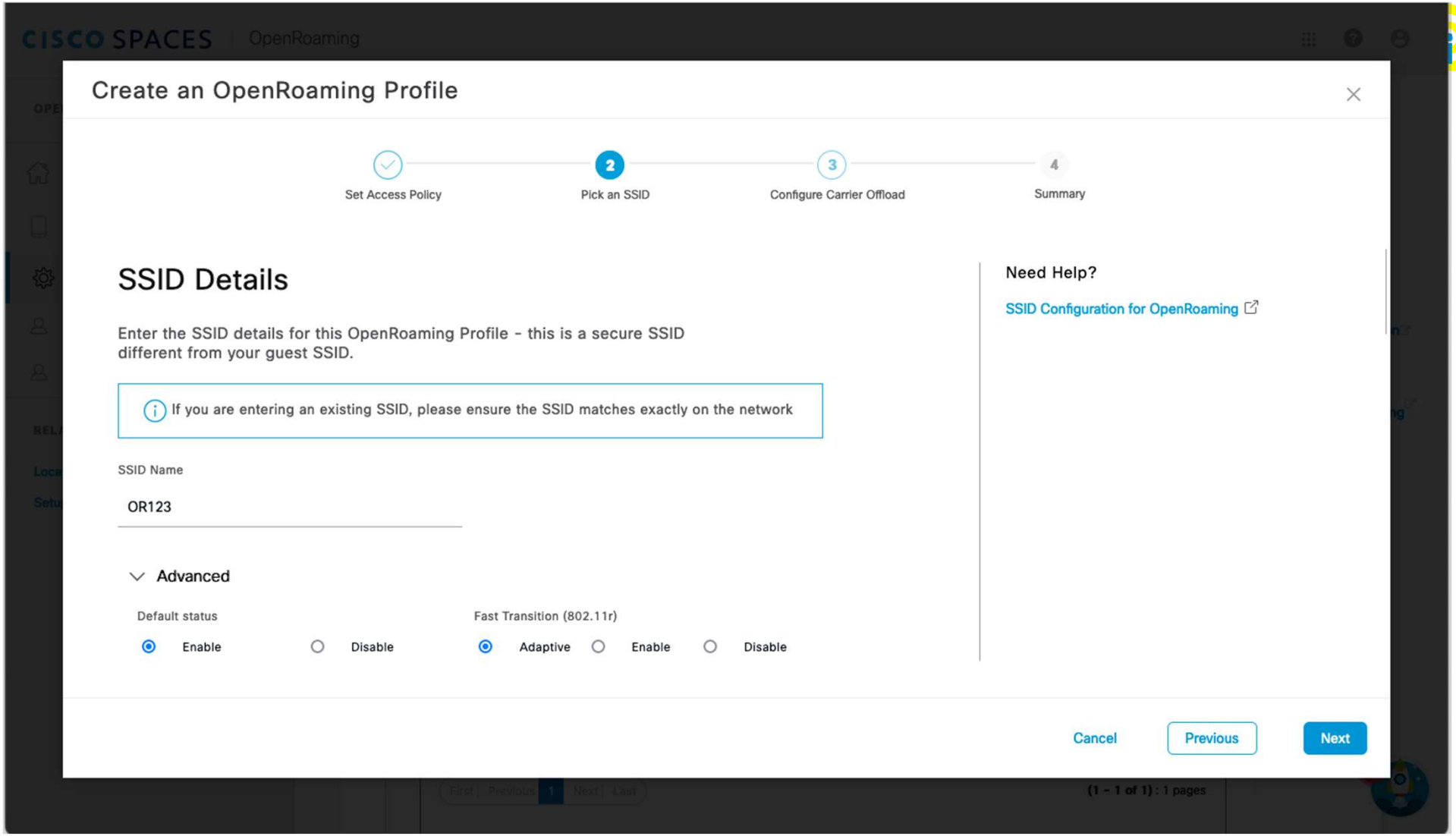
Cisco OpenRoaming 設定方法



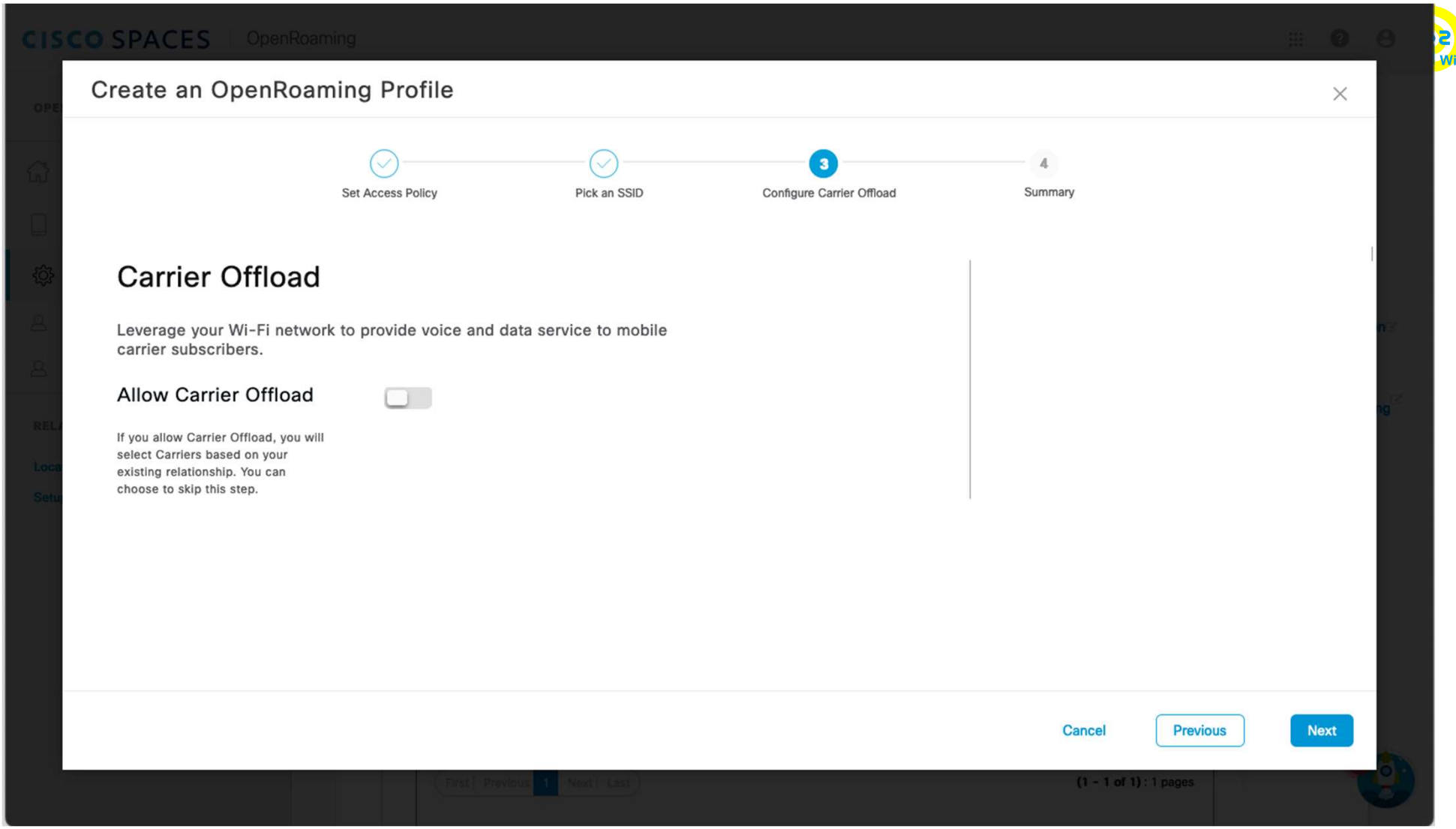
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/dna-spaces/index.html?dtid=osscdc000283



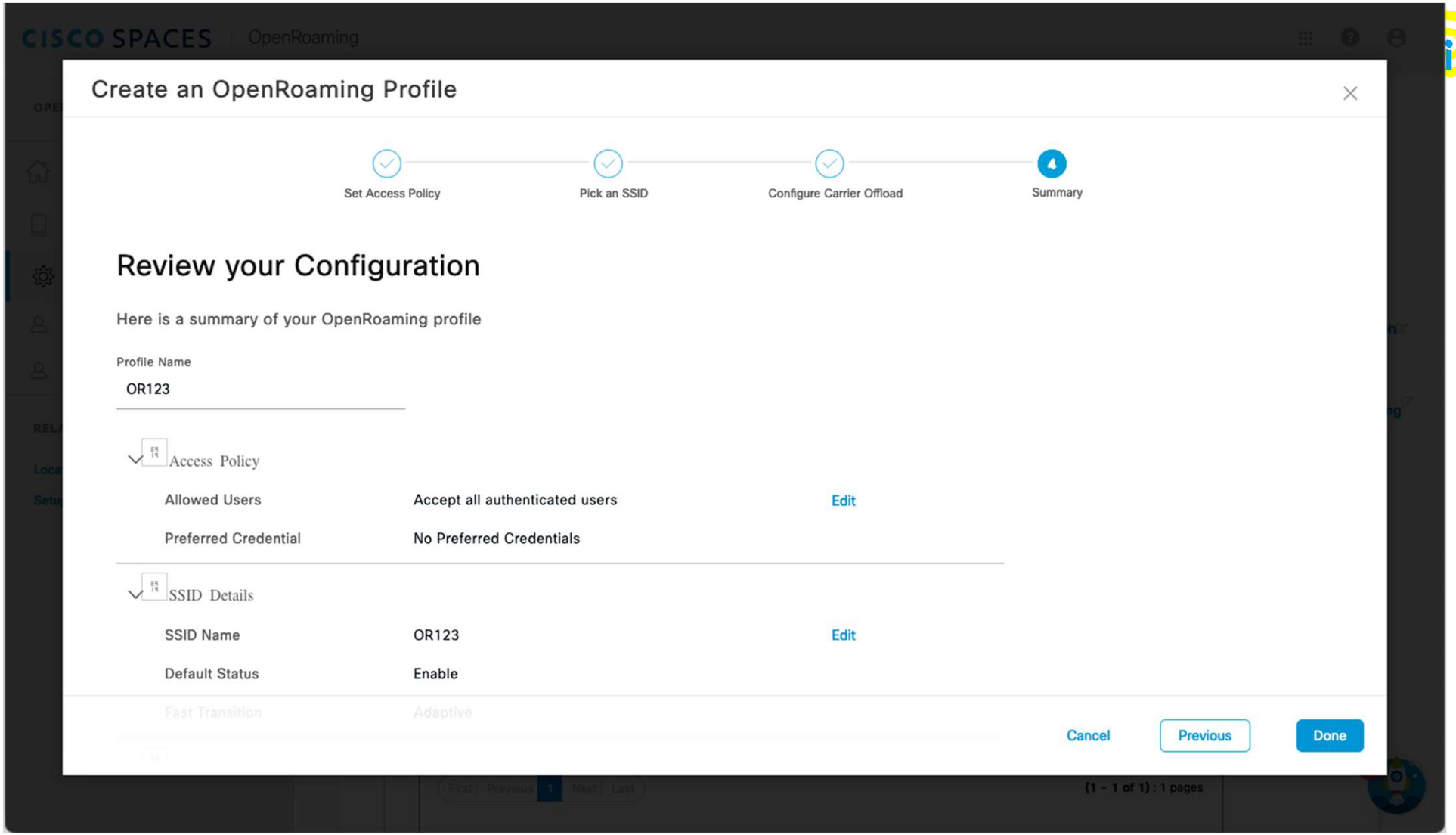
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/dna-spaces/index.html?dtid=osscdc000283



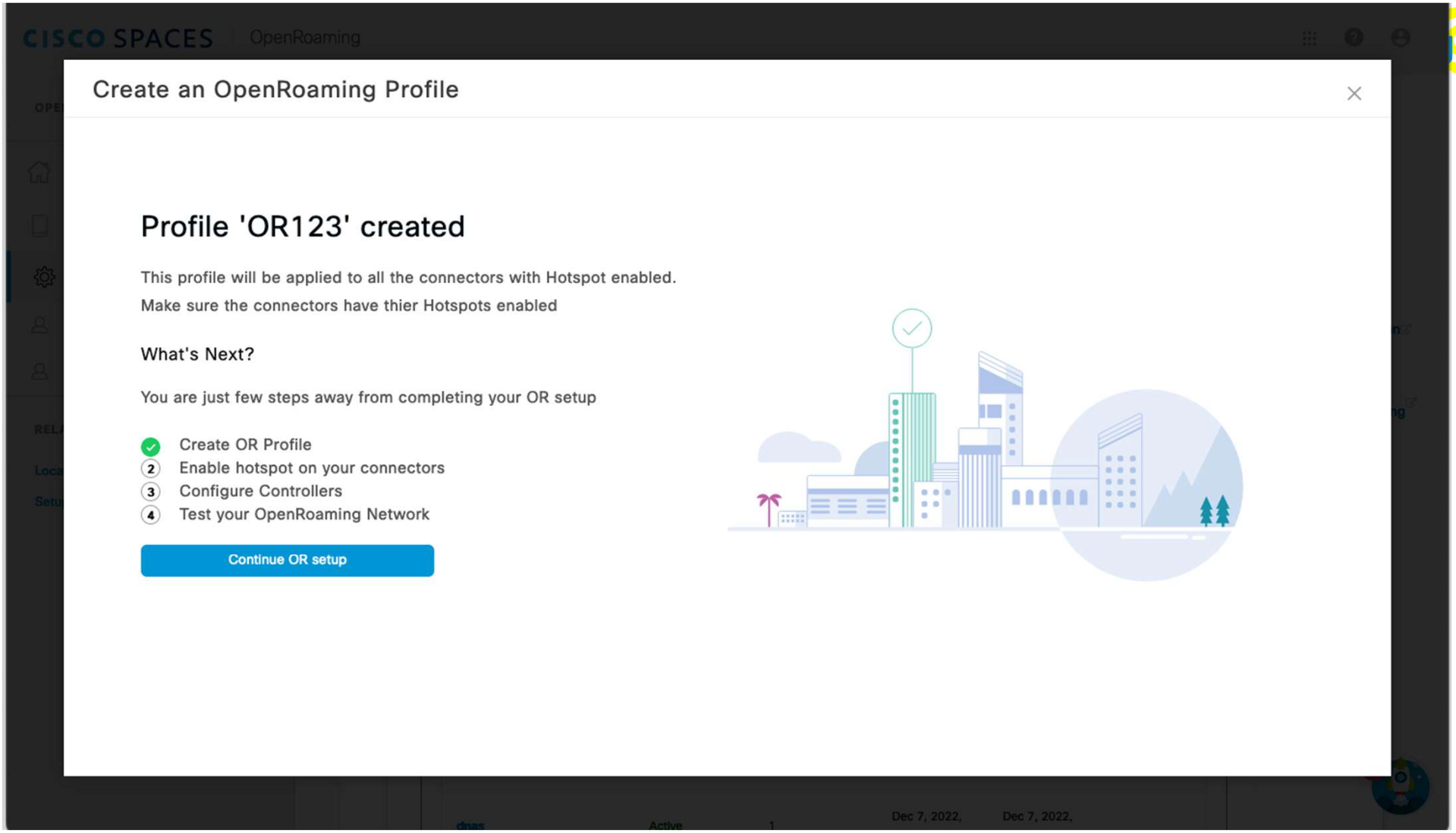
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/dna-spaces/index.html?dtid=osscdc000283



https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/dna-spaces/index.html?dtid=osscdc000283



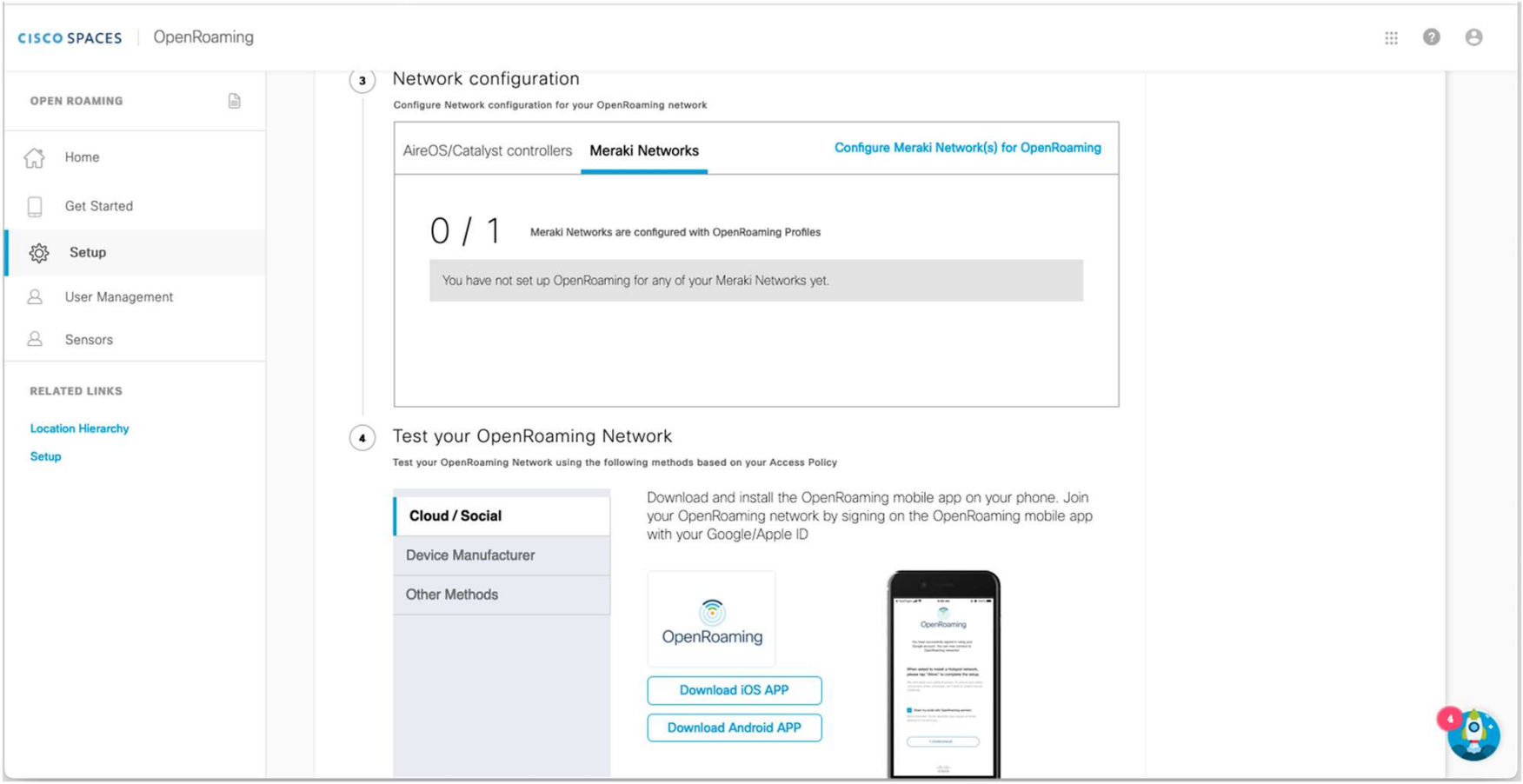
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/dna-spaces/index.html?dtid=osscdc000283



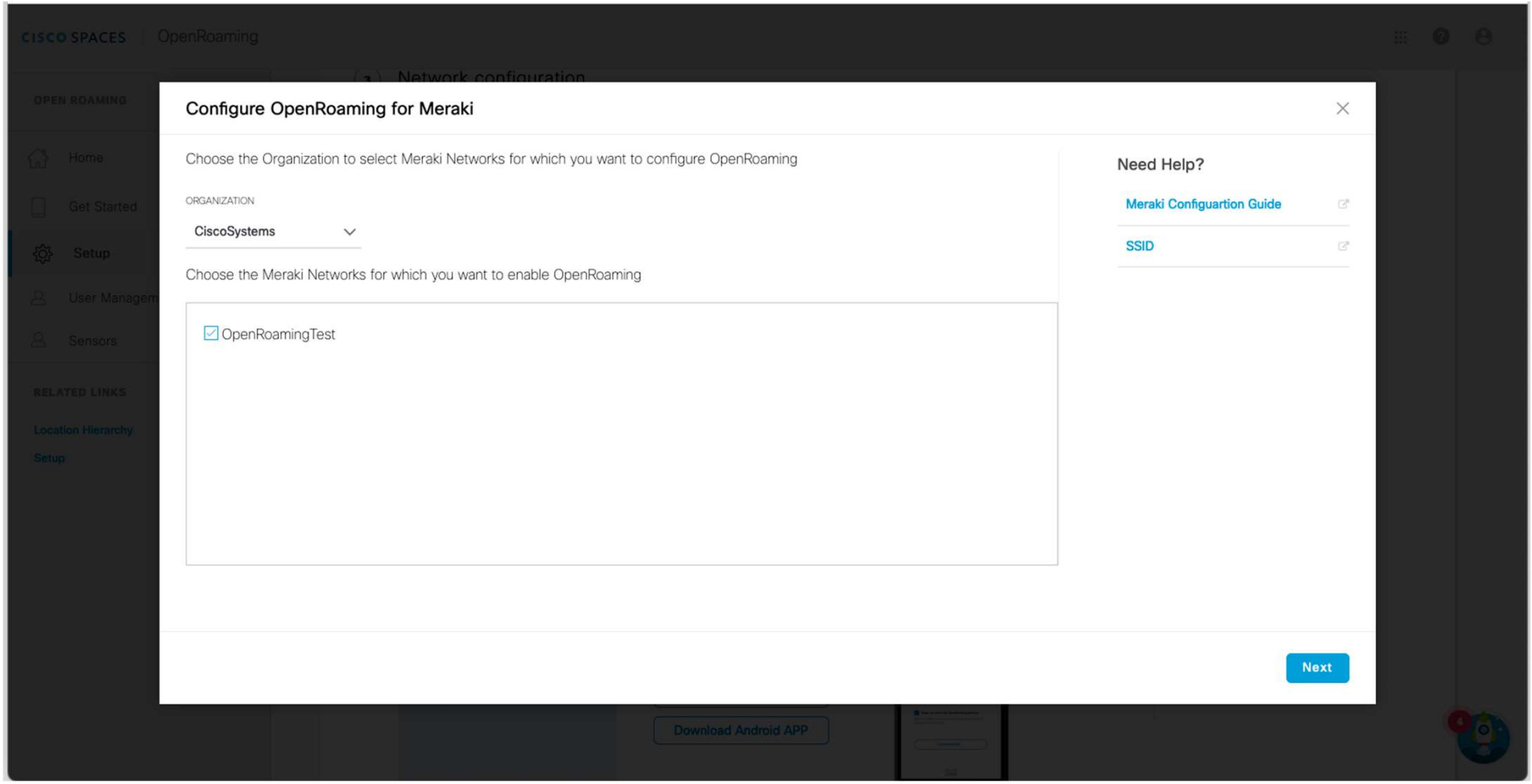
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/dna-spaces/index.html?dtid=osscdc000283

Merakiへの設定適用

- 3)Network Configuratino->Meraki Networks



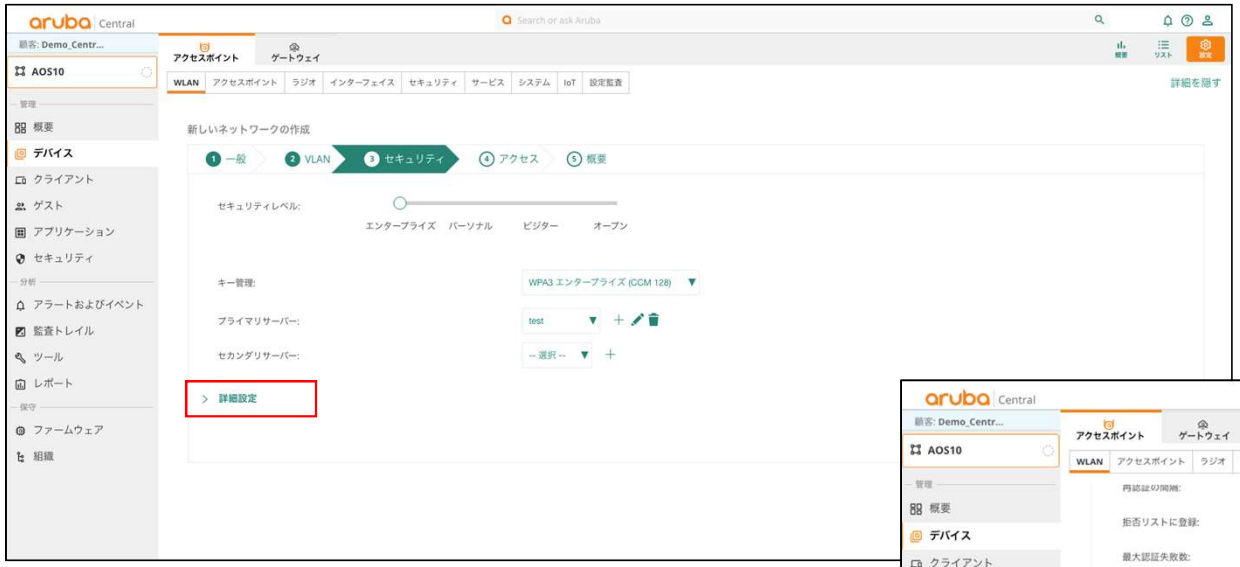
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/dna-spaces/index.html?dtid=osscdc000283



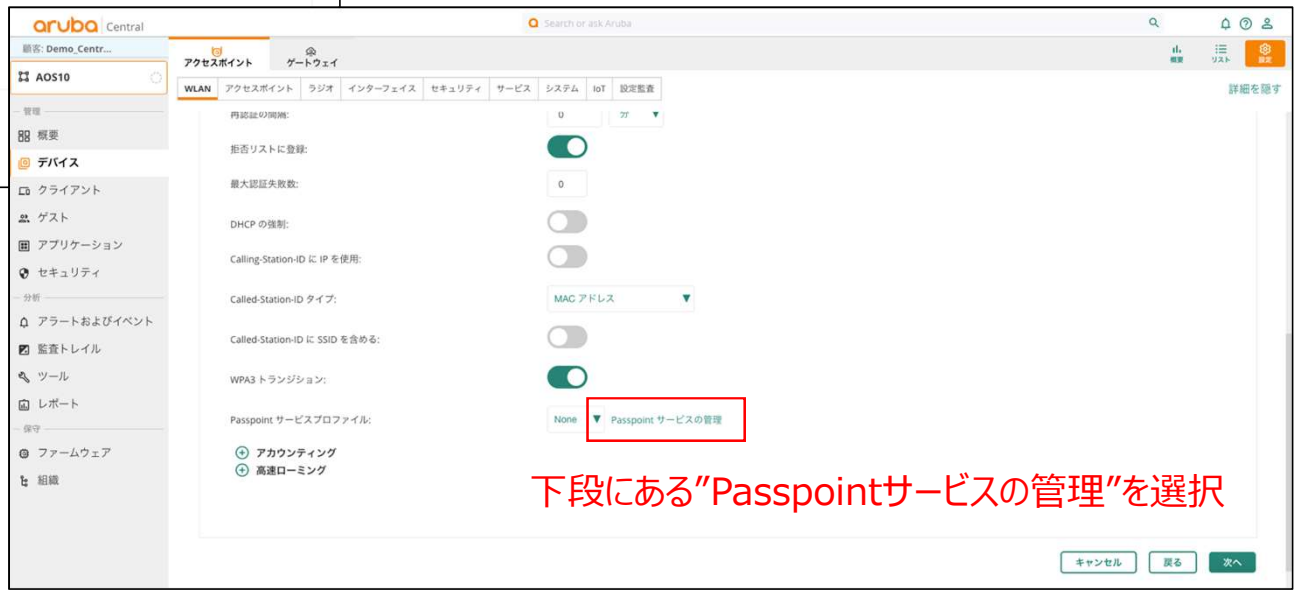
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/dna-spaces/index.html?dtid=osscdc000283

7-2.AP/コントローラの設定（Aruba Central）

PassPoint Profile設定 (1)



SSID作成 (ここではSSID名 OpenRoaming としています) の “セキュリティ”設定画面から“詳細設定”を選択



下段にある”Passpointサービスの管理”を選択

https://www.arubanetworks.com/techdocs/central/2.5.7/content/nms/access-points/cfg/networks/passpoint.htm?Highlight=passpoint
https://www.arubanetworks.com/ja/press-release/wi-fi-alliance-passpoint-2014/

PassPoint Profile設定 (2)

https://www.arubanetworks.com/techdocs/central/2.5.7/content/nms/access-points/cfg/networks/passpoint.htm?Highlight=passpoint
https://www.arubanetworks.com/ja/press-release/wi-fi-alliance-passpoint-2014/

7-3.AP/コントローラの設定（R1）（ラッカス）

vSZを使用し、Passpointで使用するネットワーク提供者情報、サービス提供者の情報等を登録

【動作確認バージョン情報】
- AP: **Ruckus ZoneFlex R310 Access Point**
- vSZ: **Ruckus Virtual SmartZone 5.2.2.0.317**

① ネットワーク提供者の設定

② サービス提供者の設定
サービス提供者のRealm、RADIUSサーバーへの接続情報を設定

③ 無線LANの設定
Authentication Type = Hotspot 2.0 Accessとすることで、Passpoint対応のAPとなる

④ 無線LANの詳細設定
フリーWi-Fi等の設定や、①,②への参照を設定

⑤ Venue(会場情報)の設定
ビジネス・教育、アウトドアなど、機関や外部環境の情報を設定

⑥ APの設定
⑥への参照を設定

vSZの設定(抜粋)

← : 参照

vSZ[t-*****001-C-02]

① Wi-Fi Operator
(Service & Profiles/Hotspots & Portals/Hotspot2.0)

Domain Names	＊＊＊＊＊

② Identity Provider
(Service & Profiles/Hotspots & Portals/Hotspot2.0)

Network Identifier

Realms	**Name**	＊＊＊＊＊
	Encoding	UTF-8
	EAP-Methods	EAP-TTLS

Online Signup & Provisioning

Enable Online Signup & Provisioning	OFF

Authentication

Realm	＊＊＊＊＊
Protocol	RADIUS

② Authentication
(Service & Profiles/Authentication/Proxy(SZ Authenticator))

Service Protocol		RADIUS
Primary Server	**IP Address**	※ RADIUSサーバーのIP
	Port	1812
	Shared Secret	testing123

Zone[vSZ_Passpoint]

③ Access WLAN
(Wireless LANs/Create)

SSID	＊＊＊＊＊_demo
Authentication Type	Hotspot 2.0 Access
Method	802.1X EAP

④ WLAN Profile
(Service & Profiles/Hotspots & Portals/Hotspot2.0)

Internet Option	ON (Specified with connectivity to the Internet)
Access Network Type	Free Public

⑤ Venue Profile
(Service & Profiles/Hotspots & Portals/Hotspot2.0)

Venue Category	Group: Unspecified Type: Unspecified

AP[XXR310RU0077]

⑥ Access WLAN
(Access Points/Access Points)

Hotspot 2.0 Venue Profile	※ Venue Profileの参照

7-4.AP/コントローラの設定（R2）（ラッカス）

vSZを使用し、R1の設定に加えて、サービス提供者のOSUサーバおよびOSU用無線LANの情報を登録
OSUを利用する場合、vSZでWFA証明書の登録が必要

【動作確認バージョン情報】
- AP: **Ruckus ZoneFlex R310 Access Point**
- vSZ: **Ruckus Virtual SmartZone 5.2.2.0.317**

R1の設定値との変更点

① **ネットワーク提供者の設定**
OSUサーバで使用するWFA証明書を設定

② **サービス提供者の設定**
Enable Online Signup & Provisioning: ONとすると、OSU対応のAPとなる

③-1 **インターネット用無線LANの設定**

③-2 **OSU用無線LANの設定**
Authentication Type = Hotspot 2.0 Onboardingとすることで、OSU用の無線LANを設定

④ **無線LANの詳細設定**
①,②に加えて④への参照を設定

⑤ **Venue(会場情報)の設定**

⑥ **APの設定**

vSZの設定(抜粋)

←：参照

vSZ[t-iidvSZ001-C-02]

① **Wi-Fi Operator**
(Service & Profiles/Hotspots & Portals/Hotspot2.0)

Domain Names	aaaaaaaaaa
Signup Security	ON
Certificate	passpoint.wi2.mobi

② **Identity Provider**
(Service & Profiles/Hotspots & Portals/Hotspot2.0)

Network Identifier

Realms	Name	aaaaaaaaaa
	Encoding	UTF-8
	EAP-Methods	EAP-TTLS

Online Signup & Provisioning

Enable Online Signup & Provisioning		ON
External Service URL		https://******/osu
Provisioning Protocol		SOAP-XML
OSU Service Description	Language	English
	Friendly Name	WiredAndWireless
	Icon	https://***i2_Logo.gif

Authentication
R1と同様

② **Authentication**
(Service & Profiles/Authentication/Proxy(SZ Authenticator))
R1と同様

Zone[vSZ_Passpoint]

③-1 **Access WLAN**
(Wireless LANs/Create)

SSID	aaaaaaaaaa_demo
Authentication Type	Hotspot 2.0 Access
Method	802.1X EAP

③-2 **Onboarding WLAN**
(Wireless LANs/Create)

SSID	aaaaaaaaaa_demo_OSU
Authentication Type	Hotspot 2.0 Onboarding
Method	Open

④ **WLAN Profile**
(Service & Profiles/Hotspots & Portals/Hotspot2.0)
R1と同様

⑤ **Venue Profile**
(Service & Profiles/Hotspots & Portals/Hotspot2.0)
R1と同様

AP[XXR310RU0077]

⑥ **Access WLAN**
(Access Points/Access Points)
R1と同様

ご清聴ありがとうございました。