

H3C 無線製品WiFi7基本設定 v1.5

2025年11月現在 v1.5

ソフトウェアバージョン:E0730以降
マテリアルバージョン:5W100-20230727

Copyright©2023 New H3C Technologies Co.,Ltd. All rights reserved.
このマニュアルのいかなる部分も、New H3C Technologies Co.,Ltd.の書面による事前の同意なしに、いかなる形式
または手段によっても複製または送信することはできません。
New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者に帰属
します。このドキュメントの情報は予告なく変更されることがあります。

内容

WiFi7概要	4
メリット	4
Wi-Fi周波数帯と干渉がない場合の到達距離の目安(数字).....	6
Wi-Fi周波数帯と干渉がない場合の到達距離の目安(図)	6
Wi-Fi 7ネットワーク構築時の注意事項	7
1. 新機能の活用と制約	7
2. インフラ設計	7
3. セキュリティと認証	7
4. 端末対応と移行計画	7
5. 運用・監視.....	7
Wi-Fi 7 ネットワーク構築チェックリスト.....	8
ヒートマップシュミレーション.....	9
無線アクセスポイントの機種、電波、設置場所	9
ヒートマップシュミレーションのサンプル	10
レポートのサンプル	10
iMCによる実測のヒートマップのサンプル	12
H3CのWiFi7概要	13
1. セキュリティ	13
2. 無線クライアントでの注意点	14
H3CのWiFi7アクセスポイント	16
超高密度オフィスのシナリオ	16
高密度オフィスのシナリオ	16
一般的なオフィスのシナリオ	17
アクセスポイントの動作モード	18
1. FIT APモード(無線コントローラーで管理).....	18
冗長化(方式その1)	18
冗長化(方式その2)	19
冗長化(方式その3)	19
2. Anchor-ac(仮想無線コントローラー)モード	20
3. CloudAPモード.....	21
無線コントローラー又はAnchor-ac(仮想無線コントローラ)でのCLIによる設定例22	
例(WiFi 7):WPA3 PSK設定例	22
ネットワーク構成.....	22
制限事項およびガイドライン	22
手順	22
例(WiFi 7):WPA3 802.1x認証設定例	23
ネットワーク構成.....	23
制限事項およびガイドライン	23
手順	23
例(WiFi 7):6G OWE(Opportunistic Wireless Encryption)設定例	24
ネットワーク構成.....	24
制限事項およびガイドライン	24
手順	24
構成を確認する	24
MLO(Multi-Link Operation)関連コマンド.....	25
無線コントローラー又はAnchor-ac(仮想無線コントローラ)のGUIによる設定例 .	26
無線コントローラーへログイン	26
WiFi7非対応製品のGUI	27
WiFi7対応製品のGUI	28

例(WiFi 7):WPA3 PSK認証設定例	28
生成されたCLIコマンド	29
例(WiFi 7):WPA3 802.1x認証設定例	30
生成されたCLIコマンド	31
生成されたCLIコマンド	32
生成されたCLIコマンド	33
例(WiFi 7): enhanced-open認証設定例	34
生成されたCLIコマンド	34
CloudAPのCloudnetからの設定例	35
Cloudnetへログイン	35
WiFi7非対応製品	36
Radioタイプ設定	36
無線モード設定(5GHz)	38
周波数帯域設定(5GHz)	39
電波出力設定(5GHz)	40
電波チャネル設定(5GHz)	41
電波出力設定(2.4GHz)	42
電波チャネル設定(2.4GHz)	43
WiFi7対応製品	45
例(WiFi 7):WPA3 PSK認証設定例	45
例(WiFi 7):WPA3 802.1x認証設定例	46
例(WiFi 7): enhanced-open認証設定例	48
(WiFi 7)無線モード設定	49
周波数帯域設定(6GHz)	50
周波数帯域調整(チャネルボンディング)	51
スマートO&M > ダッシュボード > WiFi7 Dashboard	52
用語解説	55
H3C WLAN Wi-Fi 7 エンドポイント	56
互換性試験レポート	56
試験項目	57
試験結果	58
6 GHz サポート	58
Intel	58
Qualcomm	59
Realtek	59
Apple	59
SAMSUNG	60
ASUS	60
Google	60
(参考)WiFi 8概要	61

WiFi7概要

メリット

Wi-Fi 7には次のような利点があります。

- **より高いスループット** - Wi-Fi 7は、**320 MHzの帯域幅、4096-QAM変調、および16×16 MU-MIMOを使用します**。理論的な最大レートは**46.1 Gbps**に達する可能性があります。これは、Wi-Fi 7が8Kまたは16Kのリアルタイムビデオ伝送、超高リフレッシュレート、VR/AR体験などのより高いスループットのアプリケーションをサポートできることを意味します。
- **低遅延の保証** - Wi-Fi 7は、2.4GHz、5GHz、および6GHzの帯域を使用します。さらに、**マルチリンクオペレーション(MLO)テクノロジーを使用して、さまざまな帯域でリソースを柔軟にスケジュールし、高遅延で低品質のチャネルを自動的に回避します**。**マキシマム・レシーブ・ユニット(MRU)および共同伝送(JTX)テクノロジー**により、Wi-Fi 7はチャネルリソースの使用率を大幅に向上させ、高帯域幅と低遅延を必要とするアプリケーションを実行できます。
- **より強力な高密度機能** - Wi-Fi 6デバイスは2.4GHzと5GHzの帯域で動作し、Wi-Fi 7デバイスは2.4GHz、5GHz、6GHzの帯域で動作して、より高いアクセス機能を提供します。**より高次の変調方式、2倍のMIMO機能、およびより高い帯域幅により、Wi-Fi 7はより多くのステーション、より高いスループット、およびより高いデータレートを可能にします**。プレアンブルパングチャリングおよびMRU技術は、周波数資源の使用を改善し、RF競合によって引き起こされるリソースの浪費を回避します。いくつかのチャネルが占有されていても、パケット伝送は時間内に完了できます。マルチAP調整は、APの動作チャネルと電力を動的に調整して、ユーザエクスペリエンスを向上させ、RF競合と干渉を低減し、高密度シナリオでのAPの同時サービス処理機能とパフォーマンスを大幅に向上させます。

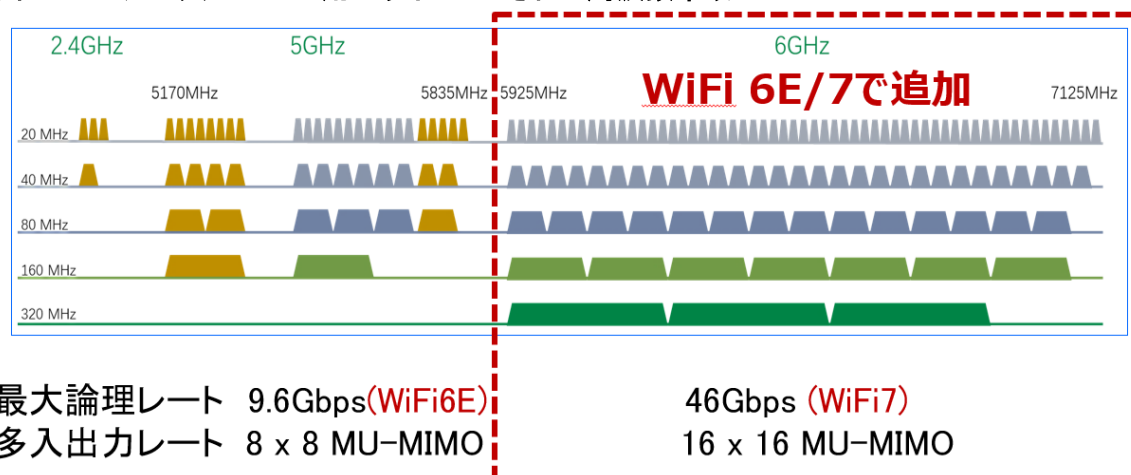
表1 Wi-Fi 7、Wi-Fi 6、Wi-Fi 6Eの比較

パラメータ	Wi-Fi 6(802.11 ax)	Wi-Fi 6E(802.11 ax)	Wi-Fi 7(802.11 be)
周波数帯	2.4 GHz、5 GHz	2.4 GHz、5 GHz、6 GHz	2.4 GHz、5 GHz、6 GHz
最大帯域幅	160 MHz		320 MHz
変調モード	OFDMA、最大1024-QAM		OFDMA、最大4096-QAM
最大理論レート	9.6 Gbps		46.1 Gbps
多入出力	8×8 UL/DL MU-MIMO		16×16 UL/DL MU-MIMO

新しい6GHz帯の総帯域幅は1200 MHzであり、59×20 MHz、29×40 MHz、14×80 MHz、7×160 MHz、3×320 MHzのチャンネル帯域幅を提供することができる。6GHz帯の総帯域幅は、2.4GHz帯と5GHz帯の帯域幅の合計の2倍であり、Wi-Fiアプリケーションの使用可能帯域幅を3倍にし、Wi-Fi周波数資源不足の問題を大幅に緩和する。Wi-Fi6の拡張として、Wi-Fi6Eは6GHz帯で動作することができ、大規模に適用されている。

次の図は、Wi-Fiアプリケーションのライセンスされた周波数帯域を示しています。

図1 Wi-Fiアプリケーション用のライセンスされた周波数帯域



各周波数ごとの利用可能なチャンネル番号

2.4G

1,2,3,4,5,6,7,8,9,10,11,12,13,14

5G

36,40,44,48

52,56,60,64,52,56,60,64

100,104,108,112,116,120,124,128,132,136,140

6G

1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93

3,11,19,27,35,43,51,59,67,75,83,91

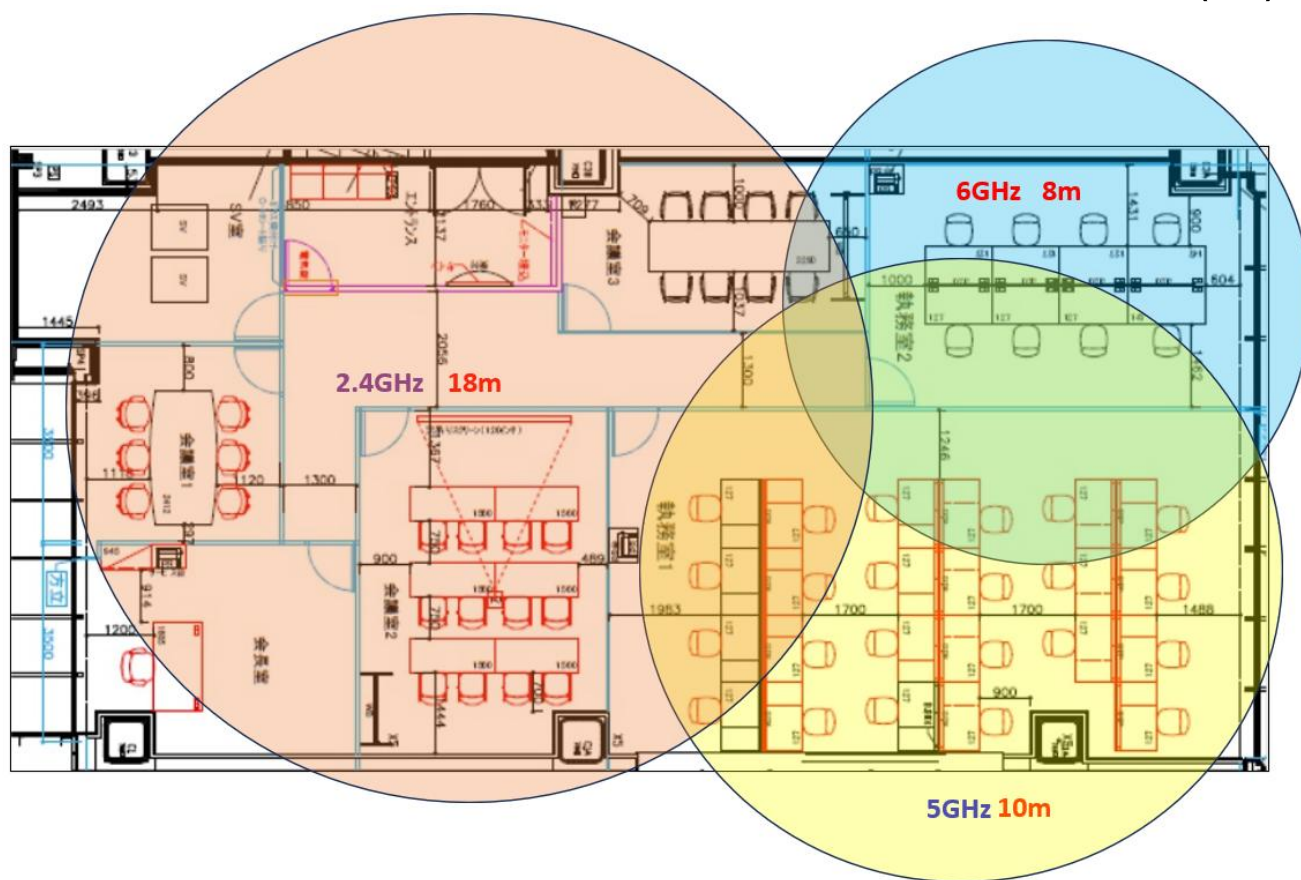
7,23,39,55,71,87

15,47,79

Wi-Fi周波数帯と干渉がない場合の到達距離の目安(数字)

周波数帯	屋内目安	屋外目安	特徴
2.4GHz	20～30m	最大100m	・ 壁や床を通りやすく、障害物に強いので遠くまで届く。 ・ 電子レンジやBluetoothなど干渉が多い。 ・ 遅延は少ないが速度はやや落ちる。
5GHz	10～20m	30～50m	・ 2.4GHzに比べて高速・低遅延。 ・ 障害物に弱く、壁を通過すると減衰が大きい。電波が届く範囲は2.4GHzよりも狭くなる。 ・ 干渉は少ないので安定しやすい。 ・ W53/W56帯は、航空無線や気象レーダーなどのレーダー波を検出した場合、該当チャネルを一時的に停止。
6GHz	5～10m	VLPモード (Very Low Power)でのみと規定されていて20～30m	・ 最も高速・低遅延。 ・ ただし障害物に非常に弱く、壁を挟むとすぐ減衰。 ・ 周囲に使う人が少ないため干渉が少なく、混雑回避に有効。 ・ レーダー波による一時的な停止もない。

Wi-Fi周波数帯と干渉がない場合の到達距離の目安(図)



Wi-Fi 7ネットワーク構築時の注意事項

1. 新機能の活用と制約

- **MLO (Multi-Link Operation)**
→ 複数バンドを同時利用することで低遅延・冗長化を実現。ただし AP 及び端末双方の対応が必要。
- **4K QAM**
→ 高速化につながるが、信号品質が良好な環境(近距離・干渉が少ない)でないと効果が限定的。
- **Multi-RU 割り当て**
→ 周波数利用効率は向上するが、ファームウェアやコントローラーの最適化が重要。

2. インフラ設計

- **有線バックボーンの強化**
→ Wi-Fi 7 の理論値は最大 46Gbps 級。実際には AP あたり数 Gbps～10Gbps のスループットが想定されるため、以下の環境が望ましい。
 - AP 接続用は **2.5G/5G/10GBASE-T** 対応スイッチ
 - uplink には **10Gbps** 以上
- **PoE 要件**
→ 高性能 AP は PoE++ (802.3bt) を要求する場合がある。

3. セキュリティと認証

- **WPA3 が必須**(Wi-Fi 7 認証では基本要件)。
- **企業環境では 802.1X / RADIUS 連携が標準**。
- **OFDMA** や **MLO** 利用時のセキュリティ検証も必要。

4. 端末対応と移行計画

- **Wi-Fi 7 対応端末はまだ限定的**(2025 年時点)。
→ 当面は **Wi-Fi 6/6E と混在運用になるため、下方互換性を確保**。
- **ファームウェア更新の重要性**
→ 規格の細かい仕様は進化中のため、最新 FW で安定性を確保。

5. 運用・監視

- **電波干渉・利用状況を可視化できる仕組み**(WIDS/WIPS, 無線コントローラー, Cloudnet により監視)を導入。
- **QoS 設計(音声・映像のリアルタイム性確保)**
→ Wi-Fi 7 は低遅延性能が強化されているため、業務利用(XR/AR/会議システム)で効果的。

まとめ

Wi-Fi 7ネットワーク構築では「チャンネル計画」「バックボーン強化」「端末の対応状況」が特に重要です。**単純にAPを入れ替えるだけでなく、有線LANや電源設計を含めてトータルで見直す必要があります。**

Wi-Fi 7 ネットワーク構築チェックリスト

項目	チェック内容	チェック
法規制・準備	6GHz帯に関する電波法の規制を確認したか	
	既存機器（Wi-Fi 6/6E）との互換性を考慮したか	
	社内ポリシー（セキュリティ・利用ルール）を見直したか	
インフラ設計	バックボーンの帯域（10Gbps以上uplink）を確保しているか	
	AP接続用に2.5G/5G/10GBASE-T対応スイッチを準備したか	
	PoE給電能力（PoE+ / PoE++）を確認したか	
	配線・電源容量を見直したか	
電波設計・最適化	サイトサーベイを実施してカバレッジを確認したか	
	チャンネルプランを設計し干渉を最小化したか	
	320MHz幅利用を検討したか	
	MLO（Multi-Link Operation）の利用シナリオを定義したか	
セキュリティ	WPA3を社内、学内標準としたか	
	802.1X / RADIUS認証を導入したか	
	管理系通信の暗号化・分離を行ったか	
	ゲスト用SSIDの分離設計を行ったか	
クライアント対応	対応端末（Wi-Fi 7/6E/6）の混在運用を考慮したか	
	主要業務アプリ（音声・映像・XR等）の性能検証を行ったか	
	ファームウェア・ドライバの更新方針を策定したか	
運用・監視	無線コントローラーやクラウド管理基盤(Cloudnet)を導入したか	
	電波干渉や利用状況をモニタリングできる仕組みを用意したか	
	アラートや障害時の運用手順を整備したか	
	QoS設計（VoIP・映像会議用トラフィック優先）を適用したか	
導入後検証	実際のスループット・遅延・ローミング性能を測定したか	
	6GHz帯利用の安定性・干渉状況を検証したか	
	業務アプリの動作確認を行ったか	

ヒートマップシミュレーション

6GHzは高速、低遅延などメリットが多いが、2.4GHz、5GHzに比べて、電波の到達する距離が短くなっております。そのため、事前に机上でのヒートマップシミュレーションやサイトサーベイが重要となります。

H3C Cloudnetでは無料のヒートマップシミュレーションを提供しております。

ヒートマップシミュレーションのトレーニング教材およびサイトのリンクは以下のリンクからドキュメントセンター及びCloudnet上のサイトをご覧ください。

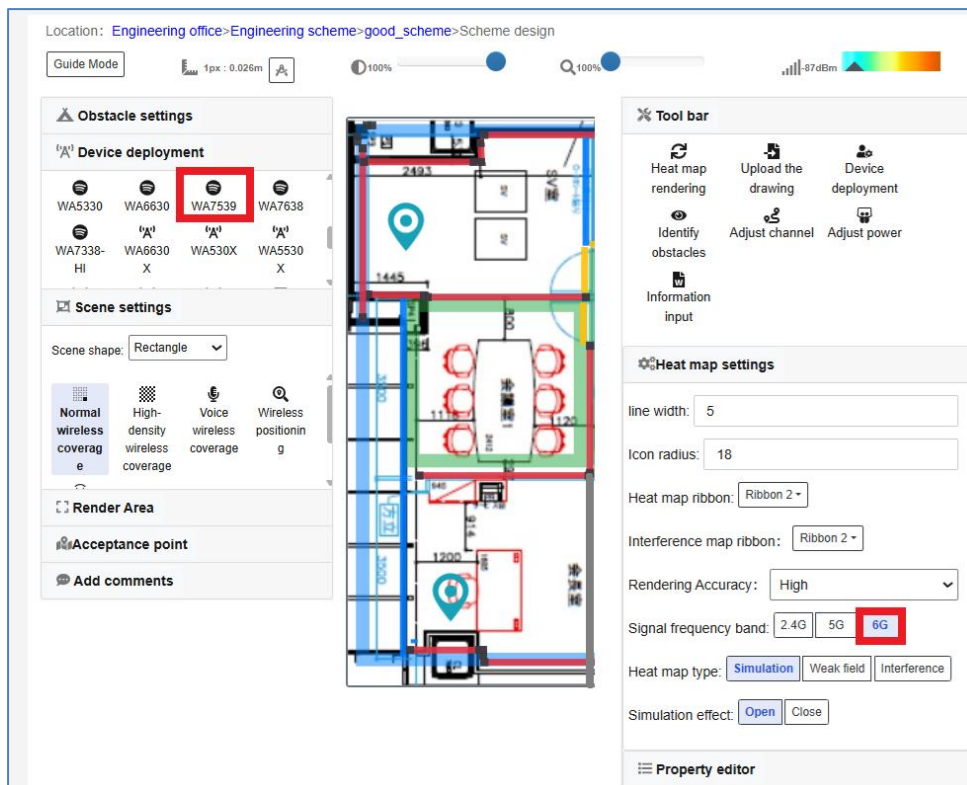
[Cloudnetを利用したヒートマップシミュレーション入門](#)

ヒートマップシミュレーションを利用するにはCloudnetにログインして、サービスメニューからクラウド工学調査を選択します。Cloudnetは以下のリンクからアクセスします。

<https://oasiscloud.h3c.com/>にアクセスします。



無線アクセスポイントの機種、電波、設置場所



ヒートマップシミュレーションのサンプル



レポートのサンプル

xxxx大学様



2 XXX大学様無線エンジニアリング調査の概要

2.1無線ネットワークのカバー範囲

2.2装置チェックリスト

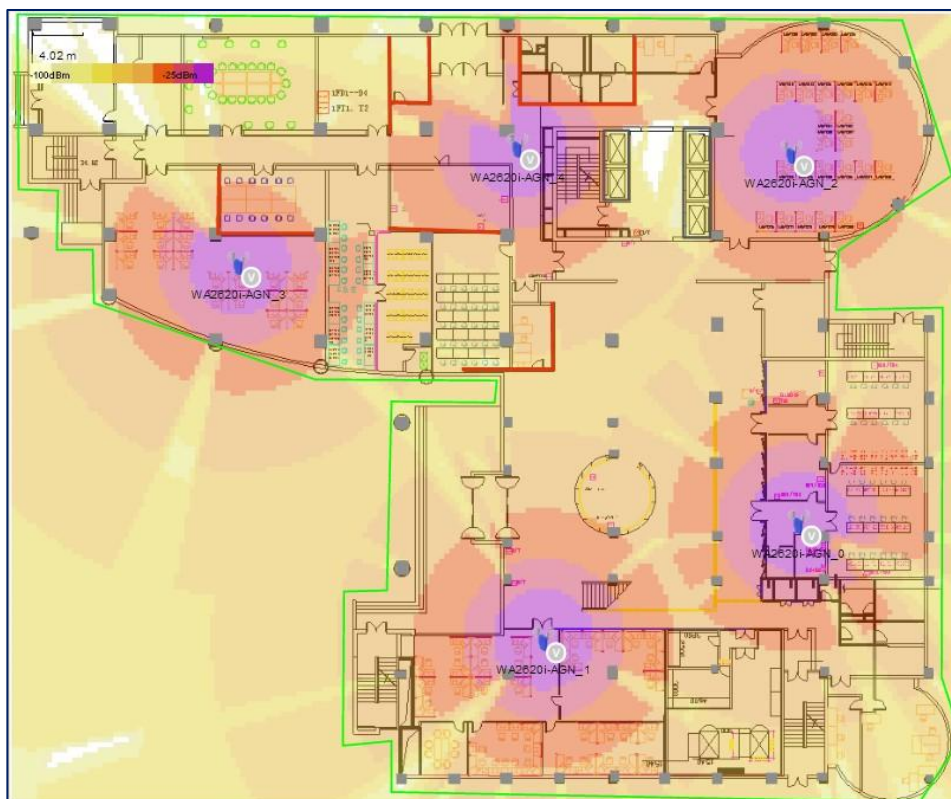
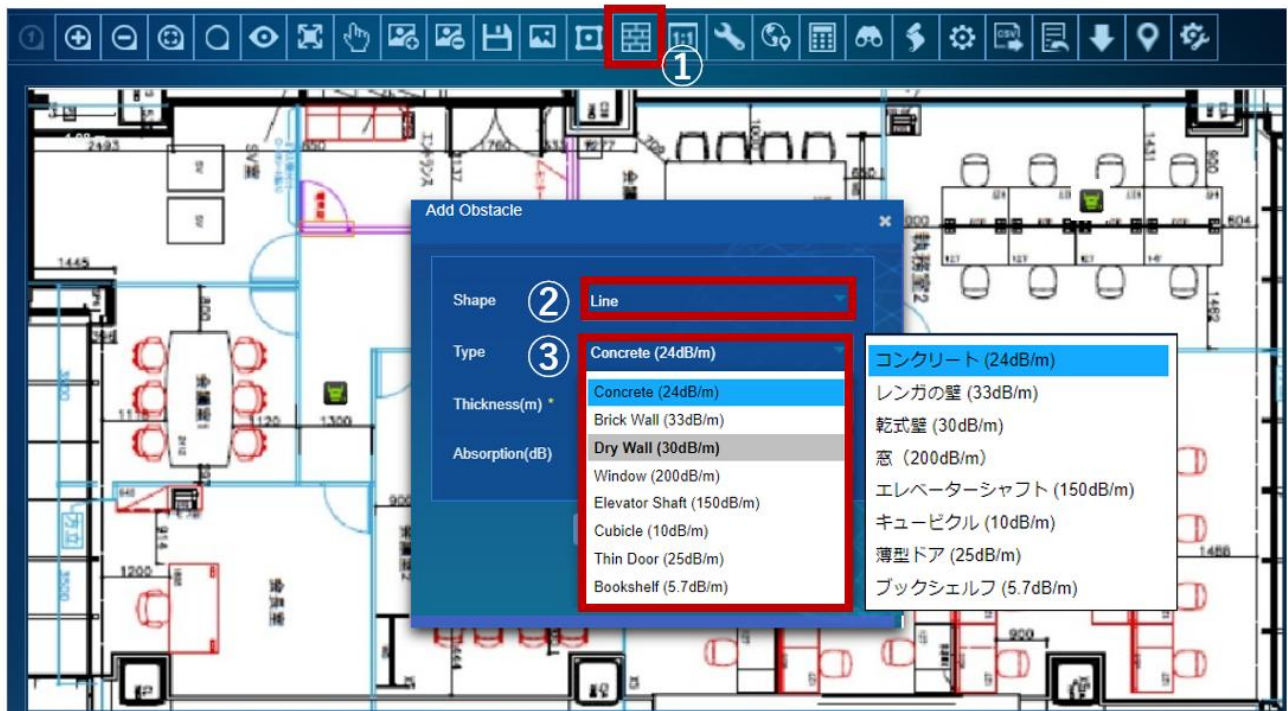
合計(無線デバイスのリスト)		
装置モデル	台数	コメント
WA7539	355	

注意: インストールおよび展開中に、実際の状況に応じてテーブルデータと矛盾が生じる可能性があります。

ソリューションワイヤレスデバイスのリスト						
計画名	装置モデル	APの台数	アンテナ タイプ	外部アンテ ナ数	APの合計 計画	アンテナ数 計画
研究棟1号 館5階	WA7539	4	内蔵	0	4	0
研究棟1号 館4階	WA7539	5	内蔵	0	5	0
A学科棟6 階	WA7539	16	内蔵	0	16	0
A学科科学 棟5階	WA7539	13	内蔵	0	13	0
A学科科学 棟4階	WA7539	9	内蔵	0	9	0
A学科科学 棟3階	WA7539	12	内蔵	0	12	0
A学科科学 棟2階	WA7539	8	内蔵	0	8	0
A学科科学 棟1階	WA7539	7	内蔵	0	7	0
以下省略						

iMCによる実測のヒートマップのサンプル

壁、ドア、窓など障害物を指定して線、枠で明示する



iMCの詳細は以下のリンクからドキュメントセンターをご覧ください。

[iMC WSMのRF管理を利用したヒートマップ作成](#)

H3CのWiFi7概要

H3CのWiFi7固有の設定について説明いたします。

1. セキュリティ

・6GHzのSSIDのセキュリティはSAE-H2EまたはOWEでなければなりません。

1. 1 6GHz RFの概要

無線周波数は高周波の交流電流を変化させる電磁波であり、長距離に渡ってデータを送信し、空中に放射できる電磁周波数を表します。WLANは伝送媒体の1つとして無線に放射してデータを伝送することができます。無線周波数は300KHzから300GHzです。WLANで使用される周波数範囲は2.4GHzでは2.412GHz～2.472GHzです。5GHz帯域は5.15GHz～5.725GHzです。6GHz帯域は5.925GHz～6.425GHzです。

1. 2 RFモード

無線周波数は高周波の交流電流を変化させる電磁波であり、長距離に渡ってデータを送信し、空中に放射できる電磁周波数を表します。WLANは伝送媒体の1つとして無線に放射します。

1. 3 チャンネル

IEEEでは、6GHzの周波数範囲は5.925GHz～7.125GHz、合計1.2GHzと規定されておりますが日本では5.925GHz～6.425GHzです。

1. 4 6GHz無線構成の制約とガイドライン

6GHz無線は、次の機能が有効になっているサービステンプレートのみにはバインドできます。

1. 拡張オープンシステム認証サービスを有効にするにはenhanced-open enableコマンドを使います。

Enhanced Open(OWE)の概要

- 従来の Open 認証(暗号化なし SSID)では、通信内容が平文で送受信されるため盗聴に弱い。
- Enhanced Open(OWE)認証は、利用者にパスワード入力を求めず、自動的に端末ごとに暗号化セッションを確立する仕組み。
- 鍵交換方式は Diffie-Hellman を利用し、接続ごとに固有の暗号鍵を生成。
- ユーザー体験は通常のオープン SSID と同じ(パスワード不要、ワンクリック接続)だが、通信は WPA3 同等レベルの暗号化(AES-CCMP)で保護される。

2. **wpa3 personal mandatory**コマンドでWPA3パーソナルにし、**akm sae pwe h2e**コマンドを使用してH2EがPWE(Pass Word Element)を算出するように設定します。
3. **wpa3 enterprise**及び**gcmp**スイートを介して、**wpa3 enterprise** レベルの192ビット暗号化が可能になります。

2. 無線クライアントでの注意点

802.11be規格ではWi-Fi 7 クライアントは、2.4GHzまたは5GHz帯域でのプローブ要求フレームの応答フレームに含まれるReduced Neighbor Report (RNR)情報から6GHz帯域のチャンネルとSSIDの詳細を得るものと、6GHzの応答フレームから直接得るものがあります。

そのため、無線コントローラーが6GHzだけでSSIDを送出すると、クライアントでは6GHzのSSIDが検出されないものがあるため、2.4GHzまたは5GHzでも何らかのSSIDを送出する必要がありますが、6GHzと異なるSSIDである必要があります。理由としては、同じSSIDが2.4GHz, 5GHz, 6GHzで送信されると6GHz以外に接続される可能性が高いため、6GHz専用のSSIDを用意します。

参考

6GHz SSIDを 2.4GHz又は6GHzビーコンで広告するために使われる主なIE(Information Elements)

1. RNR(Reduced Neighbor Report) Element

6GHz APの存在とBSSID/チャンネル情報を他バンドのビーコンで通知するためのIE。

6GHzデバイスはこのIEを読んで「このAPは6GHzでも動作している」と知る。

RNR IE の構造(簡略)

Element ID = 201 (0xC9)

Length

- └─ Neighbor AP Information (複数サブエレメント)
 - └─ TBTT Information Header
 - └─ TBTT Information Count
 - └─ TBTT Information Length
 - └─ Op Class / Chan Number
 - └─ TBTT Information (複数)
 - └─ TBTT Offset
 - └─ BSSID
 - └─ Short SSID

ここに **6GHz BSSIDとShort SSIDが入る**

これによりSTAは 2.4GHz又は6GHzをスキャンしても6GHzのSSIDが存在することを察知できる。

2. Multiple BSSID IE(MBSSID IE)

1つのビーコンで複数SSIDを広告する仕組み。

2.4GHz又は6GHzの“transmitted BSSID”の下に、6GHz SSIDの“non-transmitted BSSID profile”を含められる。

MBSSID IE の構造(簡略)

Element ID = 71 (0x47)

Length

- └─ Max BSSID Indicator
- └─ Subelement (非送信BSSIDプロフィール)

- └─ **Non-transmitted BSSID Profile**
- └─ SSID IE
- └─ Supported Rates IE
- └─ RSN IE
- └─ HE Operation IE
- └─ EHT Operation IE (Wi-Fi 7)
- └─ 6GHz Operation IE

非送信BSSIDプロファイルの中に、6GHzのSSID/設定が丸ごと入る

3. 6GHz Operation Information IE(6GHz Operation IE)

6GHzのチャネル幅、Primary channel、中心周波数などを含むIE。

Element ID = 255 (Vendor specific) or IE59 depending on variant
Length

- └─ Primary Channel
- └─ Channel Width
- └─ Center Frequency Segment 0
- └─ Center Frequency Segment 1 (必要に応じて)

6GHz BSSがどのチャネルで運用されているかをSTAが把握できる。

2.4GHz又は6GHzビーコン内に6GHz SSIDを広告する場合のIEの典型的な並び
ビーコンフレームの内容(簡略)

MAC Header

Timestamp

Beacon Interval

Capability Information

--- Mandatory IEs ---

SSID

Supported Rates

DS Parameter Set

...

--- Optional IEs used for 6GHz SSID Advertise ---

Multiple BSSID IE

- └─ Non-transmitted BSSID Profile
 - └─ SSID (6GHz SSID)
 - └─ RSN
 - └─ HE Operation
 - └─ EHT Operation
 - └─ 6GHz Operation IE

RNR IE

- └─ TBTT Info Header

- └─ 6GHz BSSID / Short SSID / Channel

H3CのWiFi7アクセスポイント

超高密度オフィスのシナリオ WA7539-JP



- このデバイスは、3バンド12ストリーム設計を使用し、最大アクセスレート18.670Gbpsをサポートします。
 - 無線1: **6GHz帯域**、4つの空間ストリーム、および11.53Gbpsの最大ネゴシエートレートをサポートします。
 - 無線2: **5GHz帯域**、4つの空間ストリーム、および5.76Gbpsの最大ネゴシエートレートをサポートします。
 - 無線3: **2.4GHz帯域**、4つの空間ストリーム、および1.38Gbpsの最大ネゴシエートレートをサポートします。
- 3つのイーサネットインターフェイス:
 - 802.3bt/at 電源をサポートする1つの10G銅線ポート。
 - 802.3bt/at 光電複合電源をサポートする1つの10G PSFPファイバポート。
 - PoE出力およびIoT拡張をサポートする1つの1000M銅線ポート。

高密度オフィスのシナリオ WA7330i-JP



- このデバイスは、3バンド8ストリーム設計を使用し、17.29Gbpsの最大アクセスレートを提供します。
 - 無線1: **6GHz/5GHzバンドスイッチオーバー**、2つの空間ストリーム、および5.765Gbpsの最大ネゴシエートレートをサポートします。
 - 無線2: **5GHz帯域**、2つの空間ストリーム、および2.882Gbpsの最大ネゴシエートレートをサポートします。
 - 無線3: **2.4GHzバンドスイッチオーバー**、2つの空間ストリーム、および0.688Gbpsの最大ネゴシエートレートをサポートします。
 - 無線4: **2.4GHz/5GHz/6GHz帯域切り替え**をサポートします。この無線はスキャンのみに使用されません。
- 3つのイーサネットインターフェイス:
 - 802.3bt/at 電源をサポートする1つの10G銅線ポート。

- 802.3bt/at 光電複合電源をサポートする1つの10G PSFPファイバポート。
- PoE出力およびIoT拡張をサポートする1つの2.5G銅線ポート。

一般的なオフィスのシナリオ WA7320i-JP



- このデバイスは、デュアルバンドの4ストリーム設計を使用し、最大アクセスレート8.647Gbpsをサポートします。
 - 無線1: **6GHz/5GHzバンドスイッチオーバー**、2つの空間ストリーム、および5.765Gbpsの最大ネゴシエートレートをサポートします。
 - 無線2: **5GHz/2.4GHzバンドスイッチオーバー**、2つの空間ストリーム、および最大ネゴシエートレート2.882Gbpsをサポートします。
- 3つのイーサネットインターフェイス:
 - 802.3at/af 電源をサポートする10G銅線ポート×1。
 - 802.3at/af 光電複合電源をサポートする1つの10G PSFPファイバポート。
 - 1000M銅線ポート×1、PoE出力をサポート

WA7220-HI-JP



- このデバイスは、デュアルバンドの4ストリーム設計を使用し、最大アクセスレート6.453Gbpsをサポートします。
 - 無線1: **6GHz/5GHzバンドスイッチオーバー**、2つの空間ストリーム、および5.765Gbpsの最大ネゴシエートレートをサポートします。
 - 無線2: **2.4GHz帯域**、2つの空間ストリーム、および0.688Gbpsの最大ネゴシエートレートをサポートします。
- デュアル2.5G銅線ポート: 1つは802.3at電源をサポートし、もう1つはIoT拡張に使用できるPoE出力をサポートします。リンクアグリゲーションを設定した後、最大有線帯域幅を5Gbpsに拡張できます

アクセスポイントの動作モード

H3CのWiFi7アクセスポイントもWiFi6のアクセスポイントのように、**1つのファームウェアでコマンドにより3つの動作モードに切り替えて利用することができます。**

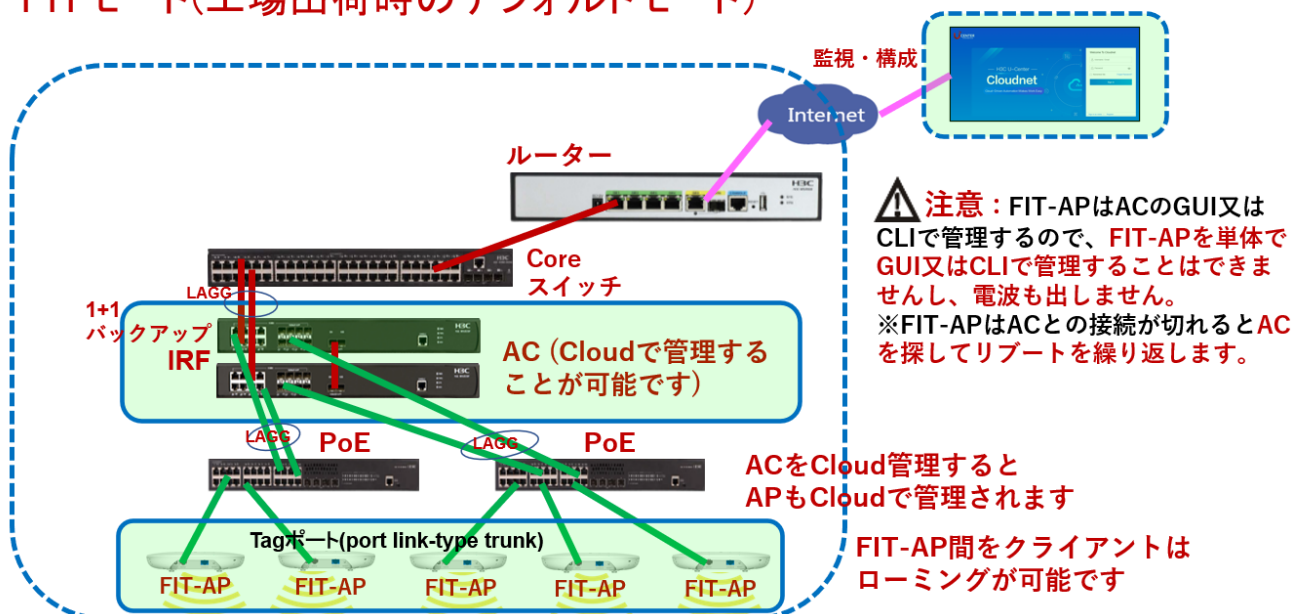
APの動作モードの変更の詳細は以下のリンクからドキュメントセンターをご覧ください。

[H3C APの動作モードの特徴と変更](#)

1. FIT APモード(無線コントローラーで管理)

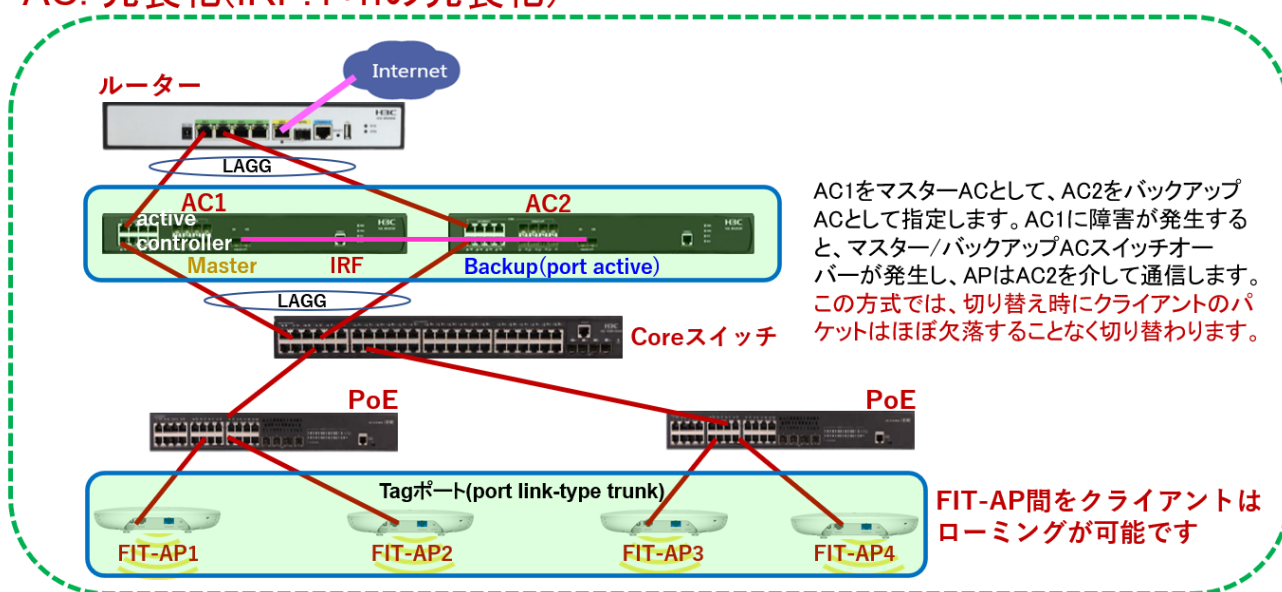
H3Cの無線コントローラーは無線コントローラーのハードウェアのみを購入しても、1台のFIT APも管理できません。FIT AP台数分のライセンスを購入して無線コントローラーにインストールしなければなりません。無線コントローラーの設定はGUIでもCLIでも行えます。

FITモード(工場出荷時のデフォルトモード)



冗長化(方式その1)

AC: 冗長化(IRF:1+nの冗長化)

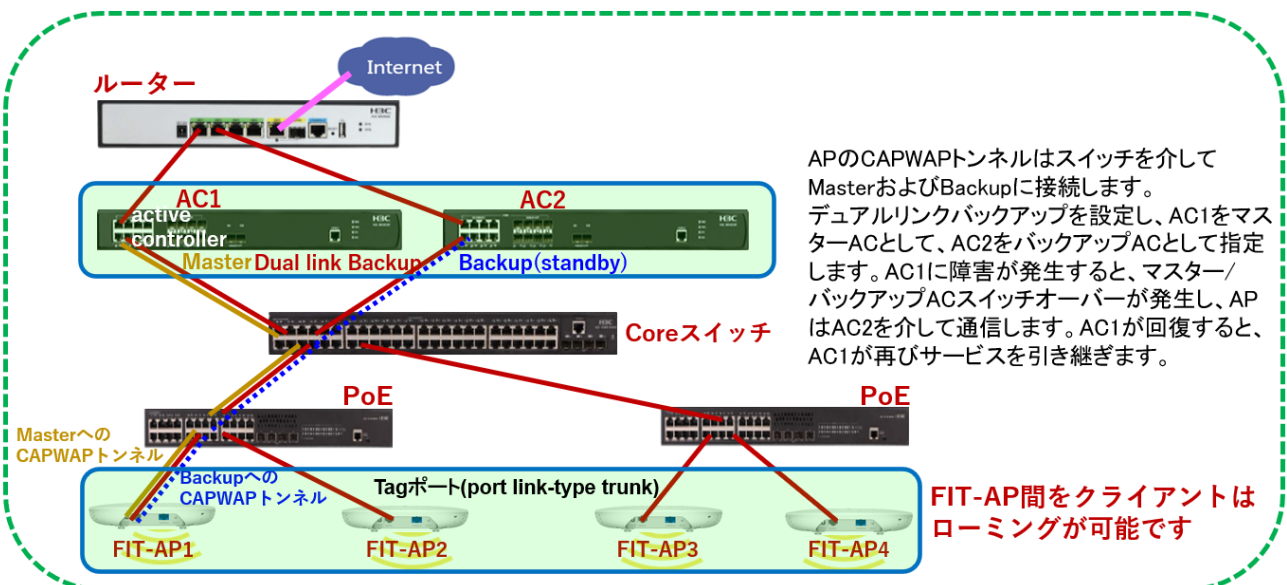


IRFの詳細は以下のリンクからドキュメントセンターをご覧ください。

[H3C製品基本操作トレーニング v3.3](#)

冗長化(方式その2)

AC: 冗長化(Dual link backup:1+1の冗長化)



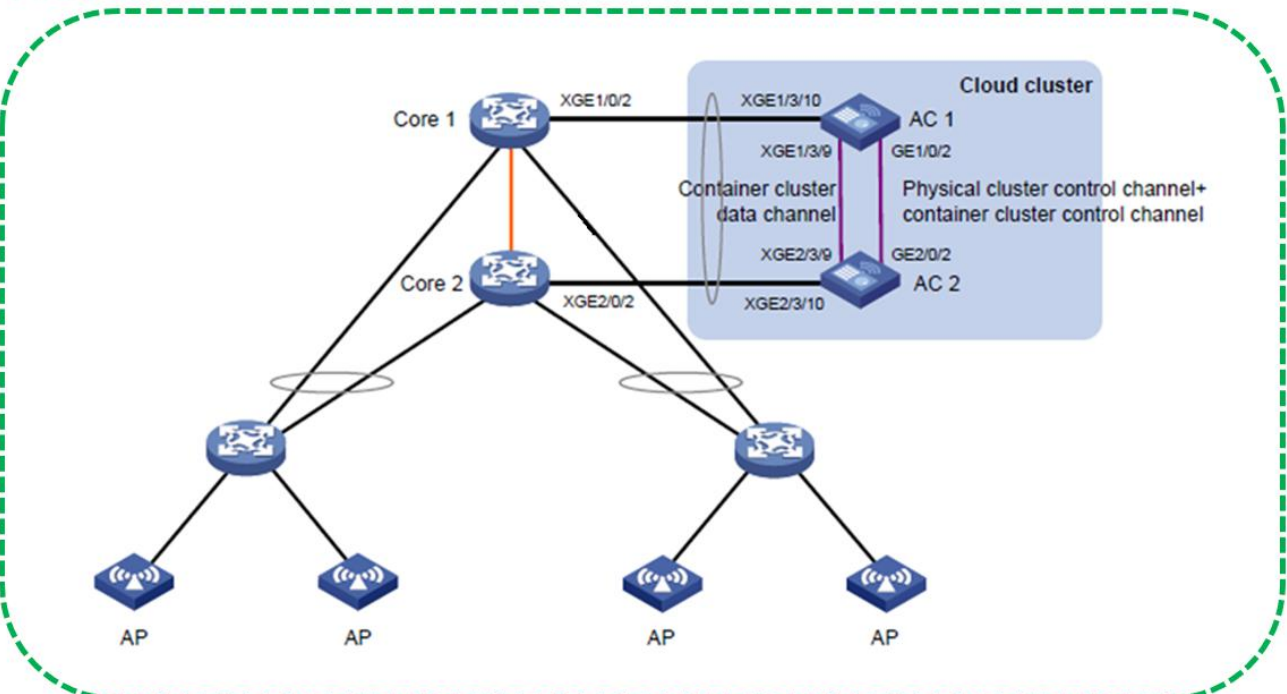
Dual link backupの詳細は以下のリンクからドキュメントセンターをご覧ください。

[H3C AC Dual-link backupコンフィギュレーションガイド](#)

[H3C AC Dual-link backupとライセンス同期コンフィギュレーションガイド](#)

冗長化(方式その3)

AC冗長化(Cloud cluster)



Cloud Clusterの詳細は以下のリンクからドキュメントセンターをご覧ください。

[Cloud Clusterコンフィギュレーションガイド](#)

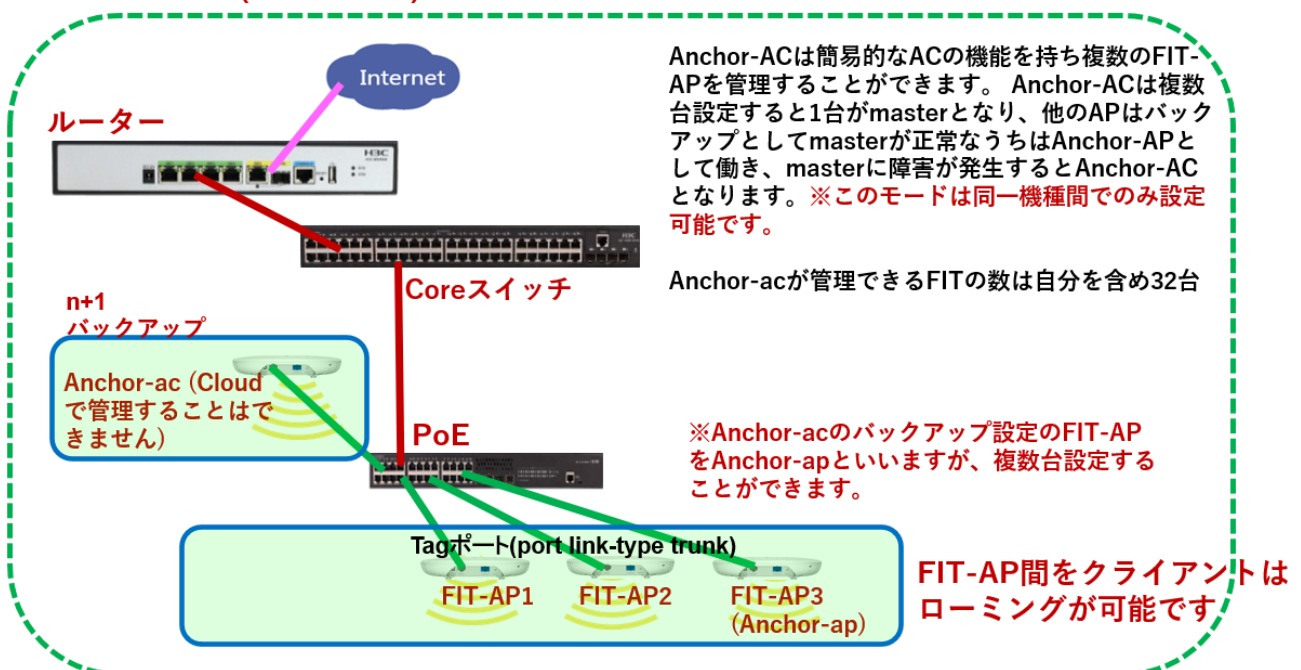
2. Anchor-ac(仮想無線コントローラー)モード

H3Cの仮想無線コントローラーはライセンス無しで仮想無線コントローラー自身を1台目のFIT APとして合計32台のFIT APを管理することができます。仮想無線コントローラーのGUIは無線コントローラーとほぼ同様で、FIT APの設定、管理はGUIでもCLIでも行えます。

FIT APの台数が32台を超える場合: 32台ごとに別々の仮想無線コントローラーを作成し、それぞれの仮想無線コントローラーが管理するFIT APをマニュアルで設定し、お互いが共存するモードにして運用します。その場合の制約は、クライアントのローミングは1つの無線コントローラーに管理されているFIT AP間だけとなります。別の仮想無線コントローラーに管理されているFIT APへローミングすることはできませんので、新たにつなぎなおすことになります。設定はGUIでもCLIでも行えます。

仮想コントローラーの冗長化: 仮想コントローラーのバックアップは何台でも構成できますが、通常はもう1台で十分です。バックアップに設定されたFIT APが仮想コントローラーとの通信が切断されると、仮想コントローラーとして働くために、Anchor-acモードになるためにリブートします。このバックアップは稼働していた仮想コントローラーのコンフィグと同期していますから、立ち上がると以前の仮想コントローラーと同じIPアドレスで稼働します。

Anchor-ac(仮想AC)モード: 冗長化(Anchor-ac/Anchor-ap)



Anchor-acの詳細は以下のリンクからドキュメントセンターをご覧ください。

[H3C Anchor-AC設置ベストプラクティスガイド\(GUI編\)](#)

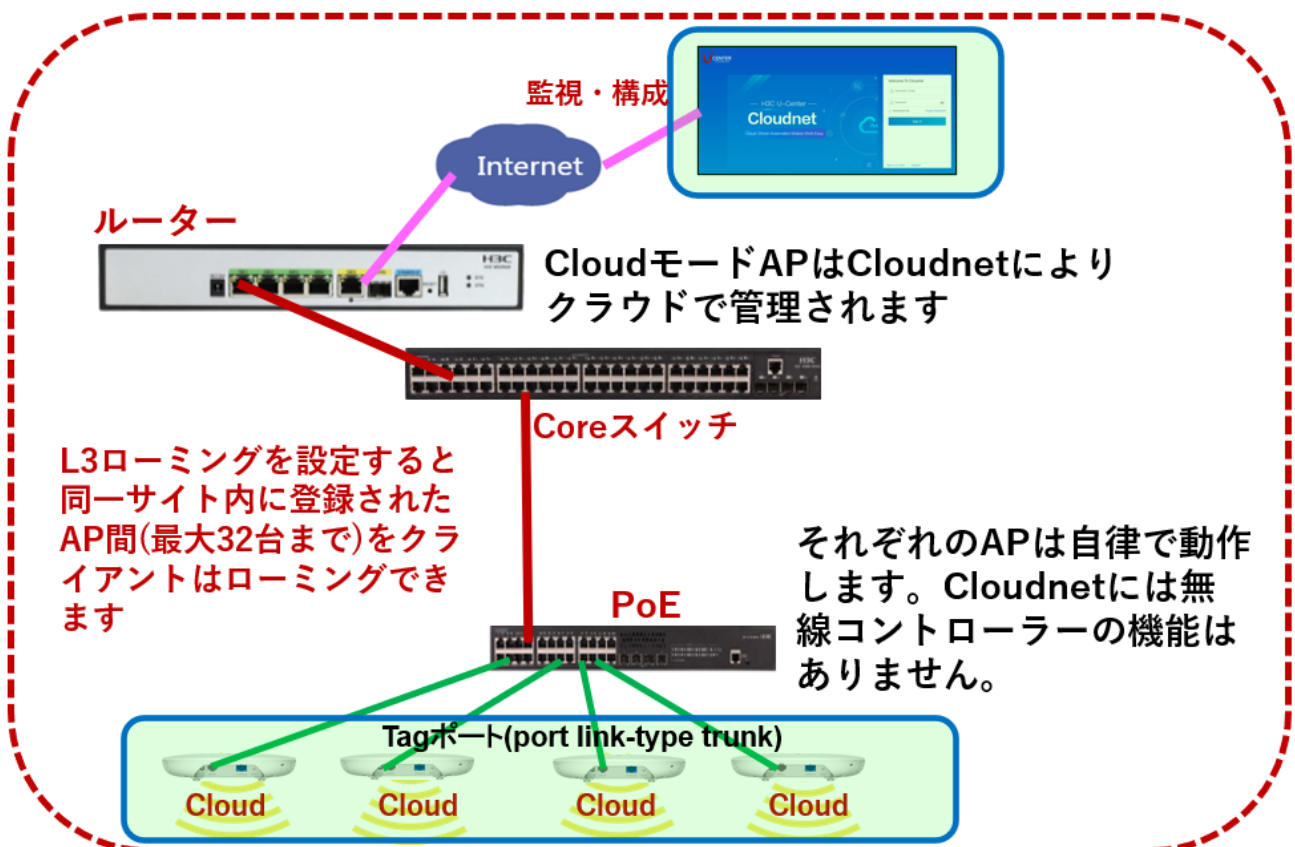
3. CloudAPモード

CloudAPモードのAPは、**最初に行うことは製品を箱から出してインターネットに接続するだけです** (DHCPクライアントなので、IP取得、ゲートウェイアドレス取得、DNSサーバーのアドレス取得でCloudnetにアクセスします)。**Cloudnet側では、このアクセスポイントに印刷されているシリアル番号を登録するだけで、オンラインになったアクセスポイントとの接続が終了します。全般的なSSIDや電波の種類など一切の設定は、Cloudnetから行います。**

大事な注意事項：一切の設定はCloudnetのGUIでおこないますので、ローカルのCloudAPのコンソールからCLIで変更することは基本、許されません。たとえ、ローカルでCLIで設定しても、CloudnetにGUIで設定されたコンフィグが保存されていて、1日に数回程度ダウンロードされますので、ローカルで設定した設定は消えてしまいます。

Cloudnetで保存されているコンフィグと同期がとれなくても良い場合は、**自己責任でCloudnet上の同期フラグをoffにすると、ローカルの設定はそのまま使い続けられます。**この場合、Cloudnet上に保存されているコンフィグとローカルのコンフィグは一致していませんから、CloudnetはCloudAPの監視装置としてのみ利用します。

CloudAPモード



CloudAPの詳細は以下のリンクからドキュメントセンターをご覧ください。

[Cloudnetを使い始めましょうv1.2](#)

[H3C Cloud管理AP設置ベストプラクティスガイドv1.2](#)

無線コントローラー又はAnchor-ac(仮想無線コントローラ)でのCLIによる設定例

例(WiFi 7):WPA3 PSK設定例

ネットワーク構成

図1 ネットワーク図



制限事項およびガイドライン

なし

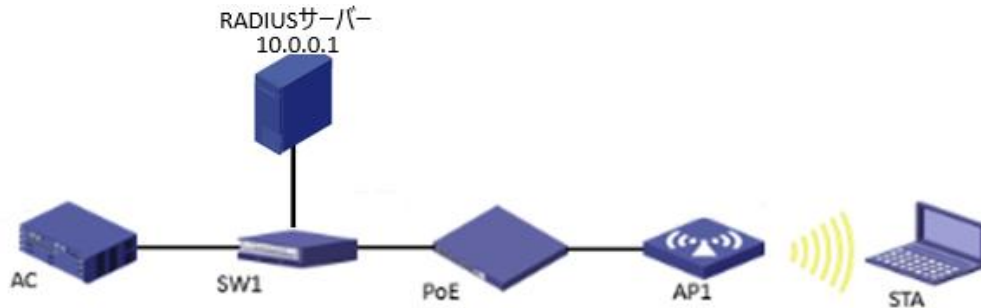
手順

- (1) システムビューに入ります。
`<AC> system-view`
- (2) WPA3ワイヤレスサービスを作成し、ビューに入ります。
`[AC] wlan service-template wpa3`
- (3) SSIDを設定します。
`[AC-wlan-st-wpa3] ssid wpa3`
- (4) WPA3ワイヤレスサービスを作成し、ビューに入ります。
`[AC-wlan-st-wpa3] akm mode psk`
`[AC-wlan-st-wpa3] preshared-key pass-phrase simple 12345678`
- (5) 暗号化スイートをCCMPに設定し、セキュリティをRSNに設定します。
`[AC-wlan-st-wpa3] cipher-suite ccmp`
`[AC-wlan-st-wpa3] security-ie rsn`
- (6) WPA3セキュリティモードをパーソナル必須モードにします。
`[AC-wlan-st-wpa3] wpa3 personal mandatory`
- (7) H2EのみをサポートするメソッドでPWEを設定します。
`[AC-wlan-st-wpa3] akm sae pwe h2e`
- (8) 保護管理フレーム(Protect Management Frame)機能を必須モードに設定します。
`[AC-wlan-st-wpa3] pmf mandatory`
- (9) 無線サービスを有効にします。
`[AC-wlan-st-wpa3] service-template enable`

例(WiFi 7):WPA3 802.1x認証設定例

ネットワーク構成

図2 ネットワーク図



制限事項およびガイドライン

なし

手順

- (1) システムビューに入ります

```
<AC> system-view
```

- (2) 802.1x認証方法をeapにします

```
[AC] dot1x authentication-method eap
```

- (3) 無線サービステンプレートに入ります

```
[AC] wlan service-template 1
```

```
[AC-wlan-st-1] ssid dot1x
```

```
[AC-wlan-st-1] akm mode dot1x
```

```
[AC-wlan-st-1] cipher-suite ccmp
```

```
[AC-wlan-st-1] security-ie rsn
```

```
[AC-wlan-st-1] wpa3 enterprise-only-mode
```

```
[AC-wlan-st-1] client-security authentication-mode dot1x
```

```
[AC-wlan-st-1] dot1x domain user-domain
```

```
[AC-wlan-st-1] undo bss transition-management enable
```

```
[AC-wlan-st-1] sqa-profile Application_Identification
```

```
[AC-wlan-st-1] service-template enable
```

- (4) RADIUSサーバーを定義します

```
[AC] radius scheme user-scheme
```

```
[AC-radius-user-scheme] primary authentication 10.0.0.1
```

```
[AC-radius-user-scheme] key authentication cipher $c$3$Iz5gSTshA7lpDkZN4C1ztB
```

- (5) ドメインを定義します

```
[AC] domain user-domain
```

```
[AC-isp-user-domain] authentication lan-access radius-scheme user-scheme
```

```
[AC-isp-user-domain] authorization lan-access radius-scheme user-scheme
```

例(WiFi 7):6G OWE(Opportunistic Wireless Encryption)設定例

ネットワーク構成

図3 ネットワーク図



制限事項およびガイドライン

なし

手順

(1) システムビューに入ります。

```
<AC> system-view
```

(2) 無線サービステンプレートビューに入ります

```
[AC] wlan service-template wpa3
```

```
[AC-wlan-st-wpa3] ssid guest
```

(3) 拡張オープン認証 サービスを有効にする

```
[AC-wlan-st-wpa3] enhanced-open enable
```

デフォルトでは拡張認証サービスは無効になっています

(4) 無線サービスを有効にする

```
[AC-wlan-st-wpa3] service-template enable
```

(5) 無線サービスを6G無線周波数に結び付ける

構成を確認する

上記の設定が完了したら、モバイル端末を利用してサービスにアクセスします。

```
「H3C-wlan-ap-1240_1-radio-1」 display wlan client verbose
```

```
MAC address      : 5a23-83c0-d9f4
```

```
IPv4 addressd    : 192.168.1.7
```

```
IPv6 address     : N/A
```

```
Username         :N/A
```

```
AID              : 1
```

```
AP ID            : 6
```

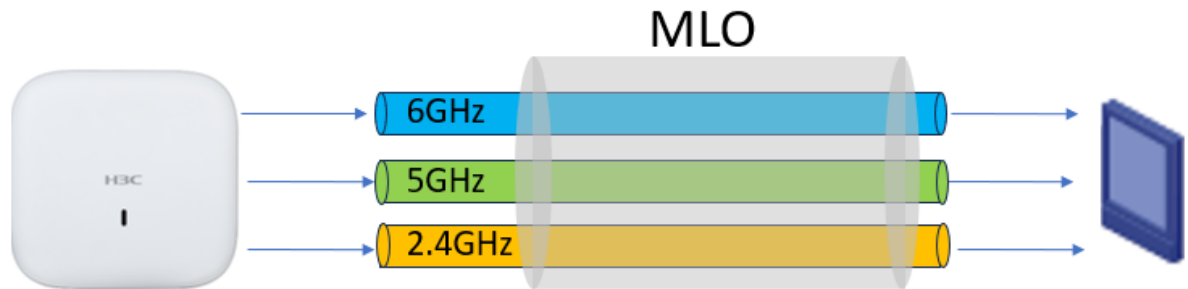
```
AP name          :1240_1
```

MLO(Multi-Link Operation)関連コマンド

Wi-Fi 7の最大空間ストリーム数(NSS)は、最大16ストリームです。これはWi-Fi 6/6Eの最大8ストリームから2倍に増加し、通信経路が増えることで通信速度の向上に貢献します。

NSSは複数のアンテナを使用して同時にデータを送受信する際の、独立した通信経路の数です。ストリーム数が増えると、同じ帯域幅でもより多くのデータを同時に送受信できるため、通信速度が向上します。

EHT-MCSは無線通信の変調方式と符号化方式の組み合わせです。



<H3C> system-view

```
[H3C] wlan ap ap1 model WA7539
```

```
[H3C-wlan-ap-ap1] radio 1
```

```
[H3C-wlan-ap-ap1-radio-1] type dot11be
```

#802.11be の最大必須 NSS を設定する

```
[H3C-wlan-ap-ap1-radio-1] dot11be mandatory maximum-nss NSSの最大値(1 ~ 8 の範囲)
```

#802.11be でサポートされる最大 NSS を設定する

```
[H3C-wlan-ap-ap1-radio-1] dot11be support maximum-nss NSSの最大値(1 ~ 8 の範囲)
```

#802.11be のマルチキャスト NSS および EHT-MCS を設定する

```
[H3C-wlan-ap-ap1-radio-1] dot11be multicast-nss NSSの最大値(1 ~ 8 の範囲) eht-mcs インデックス(1~13)
```

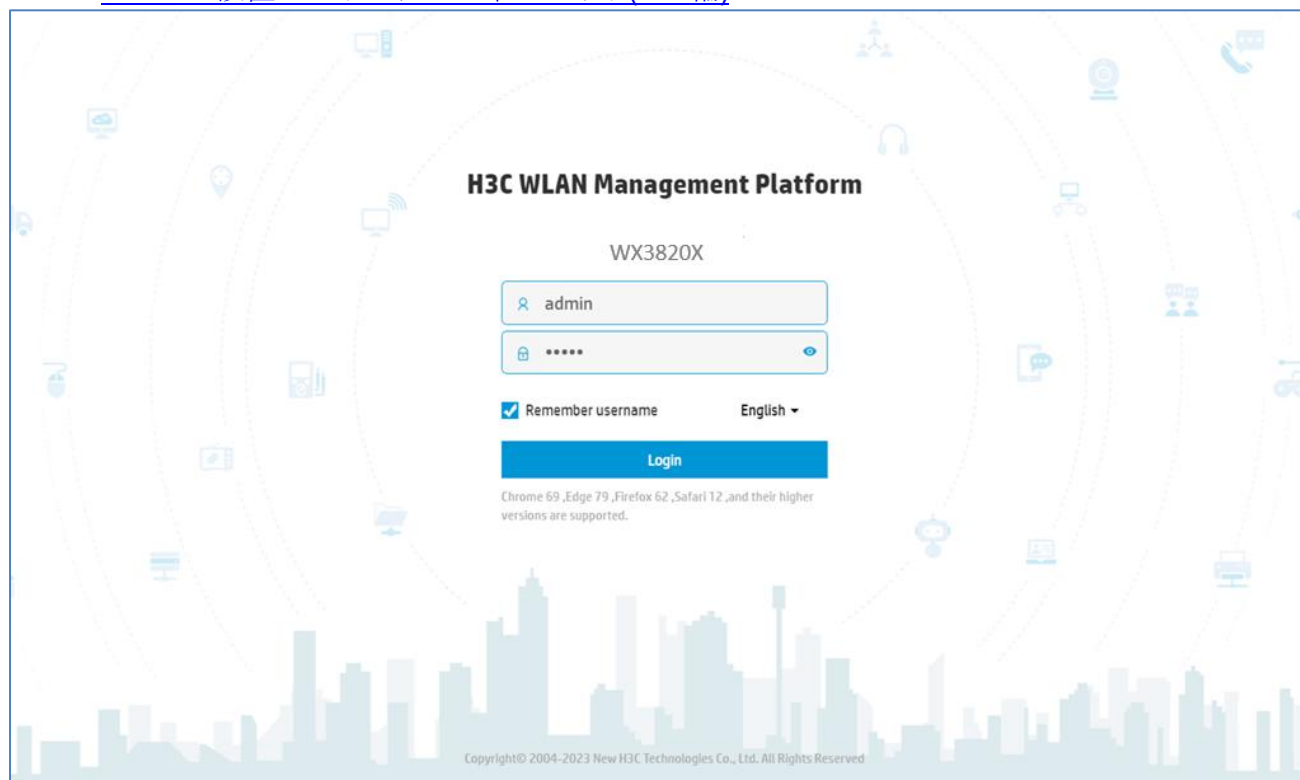
```
[H3C-wlan-ap-ap1-radio-1] quit
```

無線コントローラー又はAnchor-ac(仮想無線コントローラ)のGUIによる設定例

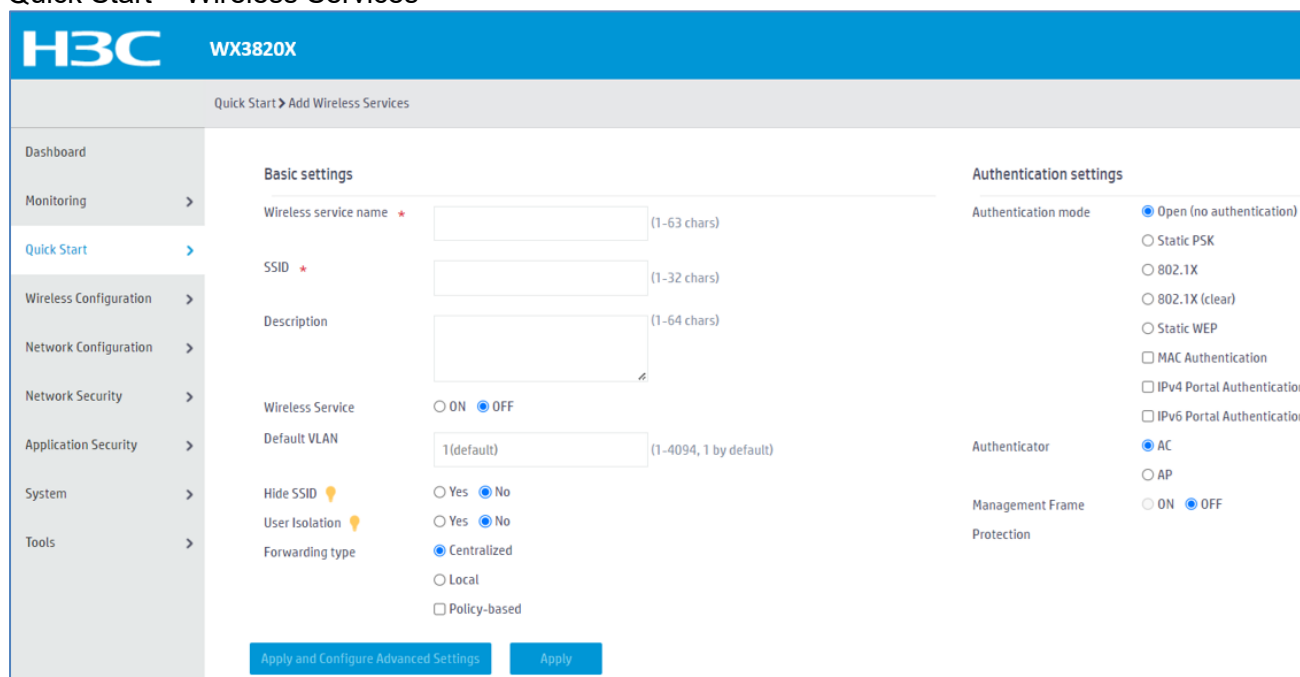
無線コントローラーへログイン

無線コントローラーの詳細は以下のリンクからドキュメントセンターをご覧ください。

[H3C AC設置ベストプラクティスガイド\(GUI編\)](#)



Quick Start > Wireless Services



WiFi7非対応製品のGUI

Authentication mode	☐ Open (no authentication)
	☒ Static PSK
	☐ 802.1X
	☐ 802.1X (clear)
	☐ Static WEP
	☐ MAC authentication
	☐ IPv4 Portal Authentication
	☐ IPv6 Portal Authentication
Authenticator	☒ AC
	☐ AP

Security mode	☐ WPA	☐ WPA2	☒ WPA or WPA2	☐ WPA3-Personal		☐ WPA3-Enterprise
Cipher suite	☐ TKIP	☐ CCMP	☒ TKIP or CCMP	☐ GCMP		
Management Frame Protection	☐ ON	☒ OFF				

Static PSK

Key type	☒ Passphrase	☐ Rawkey
Key		(8-63 alphanumeric chars)
		Confirm password

WiFi7対応製品のGUI 例(WiFi 7):WPA3 PSK認証設定例

Authentication mode	☐ Open (no authentication) ☐ Enhanced-Open ☒ Static PSK ☐ 802.1X ☐ 802.1X (clear) ☐ Static WEP ☐ MAC authentication ☐ IPv4 Portal Authentication ☐ IPv6 Portal Authentication
Authenticator	☒ AC ☐ AP

Security mode	☐ WPA ☐ WPA2 ☐ WPA or WPA2 ☒ WPA3-Personal ☐ WPA3-Personal Transition ☐ WPA3-Enterprise ☐ WPA3-Enterprise Transition ☐ WPA3-Enterprise 192-Bit Encryption ☐ H2E or HnP ☒ H2E ☐ HnP ☐ ON ☒ OFF ☐ TKIP ☒ CCMP ☐ TKIP or CCMP ☐ GCMP ☒ ON ☐ OFF ☒ Required ☐ Optional
SAE Password Element	
WPA3 Anti-Downgrade	
Cipher suite	
Management Frame Protection	
Management Frame Protection Mode	
Static PSK	
Key type	☒ Passphrase ☐ Rawkey
Key	(8-63 alphanumeric chars) Confirm password

生成されたCLIコマンド

```
wlan service-template 1
  ssid guest
  akm mode psk
  preshared-key pass-phrase cipher $c$3$1o4Sqn5jyA4Tid
  cipher-suite ccmp
  security-ie rsn
  wpa3 personal mandatory
  akm sae pwe h2e
  pmf mandatory
  service-template enable
```

Security mode

ベスト プラクティスとして、WPA3 を有効にしてセキュリティ モードを**Personal**に設定した後、Management Frame保護をONにします。

SAE PasswordElement

WPA3-SAEセキュリティモードにおいて、SAEプロセス中にPWEを生成する方法を指定します。特定の方法を指定すると、その方法をサポートしていない端末はワイヤレスネットワークに接続できなくなります。

WPA3 Anti-Downgrade

この機能を有効にすると、WPA3ネットワークに接続したWPA3クライアントは、同じSSIDを持つWPA2ネットワークに接続できなくなります。これにより、端末がセキュリティ性能の低い無線ネットワークに接続するのを防ぎます。

Management Frame

この機能を有効にすると、偽造された認証解除フレームやアソシエーション解除フレームなどの攻撃を防ぐための管理フレーム保護が行われます。

例(WiFi 7):WPA3 802.1x認証設定例 認証設定

Authentication mode	☐ Open (no authentication) ☐ Enhanced-Open ☐ Static PSK ☒ 802.1X ☐ 802.1X (clear) ☐ Static WEP
Authenticator	☒ AC ☐ AP
Security mode	☐ WPA ☐ WPA2 ☐ WPA or WPA2 ☐ WPA3-Personal ☐ WPA3-Personal Transition ☒ WPA3-Enterprise ☐ WPA3-Enterprise Transition ☐ WPA3-Enterprise 192-Bit Encryption ☐ TKIP ☒ CCMP ☐ TKIP or CCMP ☐ GCMP ☒ ON ☐ OFF ☒ Required ☐ Optional
Cipher suite	
Management Frame Protection	
Management Frame Protection Mode	
802.1X	
Dynamic WEP	☐ ON ☒ OFF
Handshake 	☐ ON ☒ OFF
Reauthentication	☐ ON ☒ OFF
Domain name	user-domain * ▼
Maximum clients	512 (1-512, 512 by default)

生成されたCLIコマンド

```
wlan service-template 2  
ssid lobby  
akm mode dot1x  
cipher-suite gcmp  
security-ie rsn  
wpa3 enterprise-only-mode  
client-security authentication-mode dot1x  
dot1x domain user-domain  
service-template enable
```

認証ドメイン設定

Domain *	user-domain
State	Active
Service type	☐ Login ☒ LAN access ☐ Portal
AAA for LAN users	
Authentication	☒ RADIUS Scheme user-scheme ☐ Local ☐ None
Authorization	☒ RADIUS Scheme user-scheme ☐ Local ☐ None
Accounting	☐ RADIUS ☐ Local ☐ None

生成されたCLIコマンド

domain user-domain

authentication lan-access radius-scheme user-scheme

RADIUSスキーム設定

Scheme name * (1-32 chars)

Authentication server

Primary authentication server
* Port range is 1-65535, 1812 by default.

VRF	Type	Host	Port *	Key	State	
Public network	IP address	10.0.0.1	1812	*****	Active	 

Secondary authentication server
* Port range is 1-65535, 1812 by default.

VRF	Type	Host	Port *	Key	State	
Public network	IP address	X.X.X.X	1 - 65535	Question marks(?) not allowed		 

The shared key for authentication (1-64 chars) 

Accounting server

Primary accounting server
* Port range is 1-65535, 1813 by default.

VRF	Type	Host	Port *	Key	State	
Public network	IP address	10.0.0.1	1813	*****	Active	 

Secondary accounting server
* Port range is 1-65535, 1813 by default.

VRF	Type	Host	Port *	Key	State	
Public network	IP address	X.X.X.X	1 - 65535	Question marks(?) not allowed		 

The shared key for accounting (1-64 chars) 

生成されたCLIコマンド

radius scheme user-scheme

primary authentication 10.0.0.1 key cipher \$c\$3\$OxLKS1h8=

primary accounting 10.0.0.1 key cipher \$c\$3\$2yh+Ypdyk28=

key authentication cipher \$c\$3\$c21fN3N97hY0F+AuvJ9KQ=

key accounting cipher \$c\$3\$ZaYWB6lxSgYUocAugBVufpY=

例(WiFi 7): enhanced-open認証設定例

Basic settings

Authentication mode

☐ Open (no authentication)

☒ Enhanced-Open

☐ Static PSK

☐ 802.1X

☐ 802.1X (clear)

☐ MAC authentication

☐ IPv4 Portal Authentication

☐ IPv6 Portal Authentication

生成されたCLIコマンド

```
lan service-template user  
ssid user  
enhanced-open enable  
service-template enable
```

CloudAPのCloudnetからの設定例

Cloudnetへログイン

Cloudnetの詳細は以下のリンクからドキュメントセンターをご覧ください。

[Cloudnetを使い始めましょうv1.2](#)

<https://oasiscloud.h3c.com/>にアクセスします。



ネットワーク > 設定 > クラウドAP > Wi-Fi設定

H3C

ネットワーク

クライアント

モニタリング

設定

自動展開

パッチテンプレート

クラウドAP

メンテナンス

メッセージ

システム

ネットワーク

クライアント

モニタリング

設定

自動展開

パッチテンプレート

クラウドAP

メンテナンス

メッセージ

システム

スマートO&M

SD-WAN

サービス

ブランチ: B社案件

サイト: 東京本社オフィス

WLAN設定

エリアコード

Wi-Fi設定

無線帯域設定

ネットワーク最適化

無線サービス設定

追加

削除

オープンサービス

クローズサービス

SSIDを隠す

SSID表示

More

	番号	SSID	サービス状態	SSIDを隠す	暗号化状態	セキュリティ方法	自動SSID	認証状態
☐	1	user	クローズ	クローズ	クローズ	拡張されたオープンな取得	クローズ	クローズ
☐	2	guest	クローズ	クローズ	PSK	WPA3	クローズ	クローズ
☐	3	lobby	クローズ	クローズ	802.1X	WPA3	クローズ	-
☐	4	office	クローズ	クローズ	PSK	WPA3	クローズ	クローズ
☐	5	room101	クローズ	クローズ	クローズ	拡張されたオープンな取得	クローズ	クローズ
☐	6	room102	クローズ	クローズ	PSK	WPA2	クローズ	クローズ

WiFi6をサポートしている無線アクセスポイントをCloudnetに登録した場合の設定画面とWiFi7をサポートしている無線アクセスポイントをCloudnetに登録した場合の設定画面は異なります。以下にWiFi6とWiFi7の設定画面を載せます。

WiFi7非対応製品

Radioタイプ設定

Wi-Fi設定

自動SSID ☐ オープン ☒ クローズ

* SSID 

room101

SSID説明

説明を入力してください50文字を超えてはいけません

0/50

サービス状態 ☒ オープン ☐ クローズ

| 高度な構成

AP転送モード

Bridgeモード

VLAN

1

SSIDを隠す ☐ オープン ☒ クローズ

* Radioタイプ 

☒ 2.4GHz ☒ 5GHz ☐ 6GHz

暗号化状態 ☐ PSK ☒ 802.1X ☐ クローズ

RADIUS設定 

☐ 内蔵サーバー ☒ 外部サーバー

設定

room-scheme

* セキュリティモード 

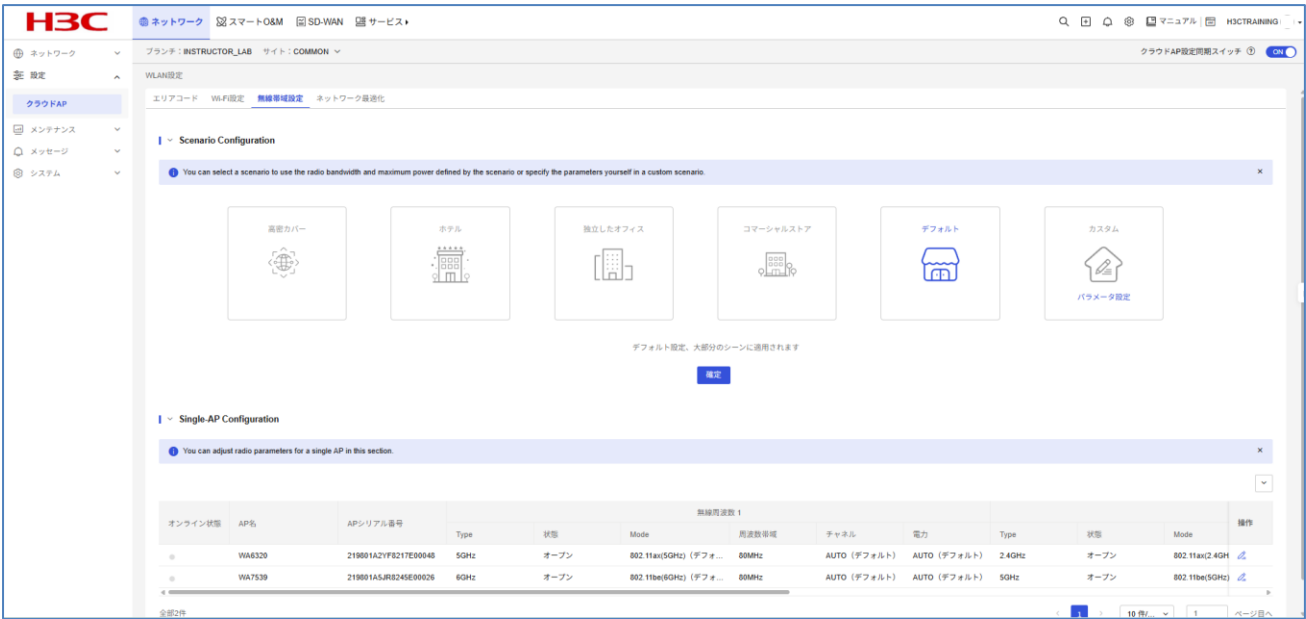
WPA2

ユーザ分離 ☐ オープン ☒ クローズ

ユーザー制限速度 ☐ オープン ☒ クローズ

EoGRE ☐ オープン ☒ クローズ

ネットワーク > 設定 > クラウドAP > 無線帯域設定



オンライン状態	AP名	APシリアル番号	無線周波数 1										操作
			Type	状態	Mode	周波数帯域	チャネル	電力	Type	状態	Mode		
●	WA6320	219801A2YF8217E00048	5GHz	オープン	802.11ax(5GHz) (デフォ...	80MHz	AUTO (デフォルト)	AUTO (デフォルト)	2.4GHz	オープン	802.11ax(2.4GH		
●	WA7539	219801A5JR8245E00026	6GHz	オープン	802.11be(6GHz) (デフォ...	80MHz	AUTO (デフォルト)	AUTO (デフォルト)	5GHz	オープン	802.11be(5GHz)		

個別のAP毎に周波数帯域、チャネル、電波出力を調整

AP名	APシリアル番号	無線周波数 1					Mode	操作
		Type	状態	Mode				
WA6320	219801A2YF8217E00048	5GHz	オープン	802.11ax(5GHz) (デフォ...			802.11ax(2.4GH	
WA7539	219801A5JR8245E00026	6GHz	オープン	802.11be(6GHz) (デフォ...			802.11be(5GHz)	

無線モード設定(5GHz)

修正Radio状態

×

無線周波数 1

Radioタイプ 5GHz

状態 ☒ オープン ☐ クローズ

Antenna Type internal (デフォルト) ▼

Mode 802.11ac(5GHz) (デフォルト) ^

周波数帯域

チャンネル

電力

Please select Mode

802.11a(5GHz)

802.11n(5GHz)

802.11ac(5GHz) (デフォルト)

AUTO (デフォルト) ▼

無線周波数 2

Radioタイプ 5GHz

キャンセル

確定

周波数帯域設定(5GHz)

修正Radio状態

×

無線周波数 1

無線周波数 2

Radioタイプ

5GHz

状態

☒ オープン ☐ クローズ

Antenna Type

internal (デフォルト)

▼

Mode

802.11ac(5GHz) (デフォルト)

▼

周波数帯域

AUTO (デフォルト)

^

チャンネル

電力

周波数帯域を選択してください

20MHz

40MHz

80MHz

AUTO (デフォルト)

Radioタイプ

5GHz

キャンセル

確定

電波出力設定(5GHz)

修正Radio状態

×

無線周波数 1

Radioタイプ 5GHz

状態 ☒ オープン ☐ クローズ

Antenna Type internal (デフォルト) ▾

Mode 802.11ac(5GHz) (デフォルト) ▾

周波数帯域 80MHz ▾

チャンネル AUTO (デフォルト) ▾

電力 ☒ パーセンテージ ☐ 数値 # スウ #

AUTO (デフォルト) ^

無線周波数 2

Radioタイプ

出力を選択してください

AUTO (デフォルト)

30%

40%

50%

60%

70%

80%

90%

100%

電波チャネル設定(5GHz)

修正Radio状態

無線周波数 1

Radioタイプ

5GHz

状態

☒ オープン ☐ クローズ

Antenna Type

internal (デフォルト)

Mode

802.11ac(5GHz) (デフォルト)

周波数帯域

80MHz

チャネル

AUTO (デフォルト)

電力

チャンネルを選択してください

36

40

44

48

52

56

60

64

AUTO (デフォルト)

無線周波数 2

Radioタイプ

各周波数ごとの利用可能なチャネル番号

2.4G

1,2,3,4,5,6,7,8,9,10,11,12,13

5G

36,40,44,48,52,56,60,64

電波出力設定(2.4GHz)

修正Radio状態

×

AUTO (デフォルト)

▼

無線周波数 3

Radioタイプ

2.4GHz

状態

☒ オープン ☐ クローズ

Antenna Type

internal (デフォルト)

▼

Mode

802.11n(2.4GHz) (デフォルト)

▼

周波数帯域

20MHz

▼

チャンネル

AUTO (デフォルト)

▼

電力

☒ パーセンテージ ☐ 数値#スウ#

AUTO (デフォルト)

▲

出力を選択してください

AUTO (デフォルト)

30%

40%

50%

60%

70%

80%

90%

100%

Max Power

電波チャネル設定(2.4GHz)

修正Radio状態

×

AUTO (デフォルト)

▼

無線周波数 3

Radioタイプ

2.4GHz

状態

☒ オープン ☐ クローズ

Antenna Type

internal (デフォルト)

▼

Mode

802.11n(2.4GHz) (デフォルト)

▼

周波数帯域

20MHz

▼

チャネル

AUTO (デフォルト)

▲

電力

チャンネルを選択してください

1

2

3

4

5

6

7

8

9

10

11

12

13

AUTO (デフォルト)

ネットワーク > 設定 > クラウドAP > ネットワーク最適化

エリアコード	Wi-Fi設定	無線帯域設定	ネットワーク最適化
--------	---------	--------	-----------

▼ 基本設定

5GHzと6GHzを優先します ②

☐ オープン

☒ 閉じる

むせんふかへいこう ②

☐ オープン

☒ 閉じる

ローミングナビ 2.4GHz ②

☐ オープン

☒ 閉じる

ローミングナビ 5GHz ②

☐ オープン

☒ 閉じる

Broadcast Optimization ②

☐ オープン

☒ 閉じる

Distributed RRM

☒ オープン

☐ 閉じる

▼ 詳細設定

弱い信号の拒否 ②

☐ オープン

☒ 閉じる

Channel Reuse-2.4GHz ②

☐ オープン

☒ 閉じる

Channel Reuse-5GHz ②

☐ オープン

☒ 閉じる

低レートを禁止にする-2.4GHz ②

☐ 禁止

☒ 禁止なし

低レートを禁止にする-5GHz ②

☐ 禁止

☒ 禁止なし

Roaming Config ②

☐ Roaming Group

☐ Neighbor AP Roaming

☒ 閉じる

Power Optimization

☐ オープン

☒ 閉じる

Client IPv6 Address Learning

☒ オープン

☐ 閉じる

ネットワーク最適化の詳細は以下のリンクからドキュメントセンターをご覧ください。

[H3C Cloud管理AP設置ベストプラクティスガイドv1.2](#)

WiFi7対応製品

例(WiFi 7):WPA3 PSK認証設定例

Wi-Fi設定

* SSID ?

guest

SSID説明

説明を入力してください50文字を超えてはいけません

0/50

サービス状態

☒ オープン ☐ クローズ

高級な構成

AP転送モード

Bridgeモード

VLAN

1

SSIDを隠す ?

☐ オープン ☒ クローズ

* Radioタイプ ?

☐ 2.4GHz ☐ 5GHz ☒ 6GHz

暗号化状態 ?

☒ PSK ☐ 802.1X ☐ クローズ

* セキュリティモード ?

WPA3

* Password ?

.....

* Confirm Password

.....

ユーザ分離 ?

☐ オープン ☒ クローズ

ユーザー制限速度 ?

☐ オープン ☒ クローズ

認証

☐ オープン ☒ クローズ

EoGRE ?

☐ オープン ☒ クローズ

例(WiFi 7):WPA3 802.1x認証設定例

Wi-Fi設定

自動SSID ☐ オープン ☒ クローズ

* SSID

SSID説明

サービス状態 ☒ オープン ☐ クローズ

高級な構成

AP転送モード

VLAN

SSIDを隠す ☐ オープン ☒ クローズ

* Radioタイプ ☐ 2.4GHz ☐ 5GHz ☒ 6GHz

暗号化状態 ☐ PSK ☒ 802.1X ☐ クローズ

RADIUS設定 ☐ 内蔵サーバー ☒ 外部サーバー

* セキュリティモード

ユーザ分離

ユーザ制限速度

EoGRE

WPA+WPA2 または WPA2 を選択した場合、サービスは 6GHz 対応無線機にバインドされません。AUTO を選択した場合、Wi-Fi 7 端末では WPA2+WPA3 方式が有効となり、非 Wi-Fi 7 端末では WPA2 方式が有効となります。

外部RADIUSサーバーの定義

* RADIUSスキーマ		user-scheme	
認証サーバー			
* プライマリサーバーIP	10.0.0.1	バックアップ・サーバーIP	サーバーIPを指定
* チャンネル数	1812	チャンネル数	1-65535
* ライセンス共有キー			
アカウントingサーバー			
* プライマリサーバーIP	10.0.0.1	バックアップ・サーバーIP	サーバーIPを指定
* チャンネル数	1813	チャンネル数	1-65535
* アカウントing共有キー			
* ISPドメイン名	user-domain		
NAS ID	最大31文字。\\?\		
ドメイン名の割り当て	☐ ドメインあり ☒ ドメインなし ☐ そのままにして		

例(WiFi 7): enhanced-open認証設定例

基本設定

自動SSID ② ☐ オープン ☒ クローズ

* SSID ② user

SSID説明

説明を入力してください50文字を超えてはいけません

0/50

サービス状態 ☒ オープン ☐ クローズ

高度な構成

AP転送モード Bridgeモード

VLAN

1

SSIDを隠す ② ☐ オープン ☒ クローズ

* Radioタイプ ② ☐ 2.4GHz ☐ 5GHz ☒ 6GHz

暗号化状態 ② ☐ PSK ☐ 802.1X ☒ クローズ

* セキュリティモード 拡張されたオープンな取得

トランジション無線サービス ② 選択

ユーザ分離 ② ☐ オープン ☒ クローズ

ユーザー制限速度 ② ☐ オープン ☒ クローズ

認証 ☐ オープン ☒ クローズ

(WiFi 7)無線モード設定

修正Radio状態

×

Radioタイプ

6GHz

状態

☒ オープン ☐ クローズ

Antenna Type

internal (デフォルト) ▼

Mode

802.11be(6GHz) (デフォルト) ^

周波数帯域

Please select Mode

チャンネル

802.11ax(6GHz)

電力

802.11be(6GHz) (デフォルト)

AUTO (デフォルト) ▼

無線周波数 2

Radioタイプ

5GHz

状態

☒ オープン ☐ クローズ

キャンセル

確定

周波数帯域設定(6GHz)

修正Radio状態

×

無線周波数 1

無線周波数 2

Radioタイプ

6GHz

状態

☒ オープン ☐ クローズ

Antenna Type

internal (デフォルト)

▼

Mode

802.11be(6GHz) (デフォルト)

▼

周波数帯域

80MHz

^

チャンネル

電力

周波数帯域を選択してください

20MHz

40MHz

80MHz

160MHz

320MHz

AUTO (デフォルト)

Radioタイプ

キャンセル

確定

周波数帯域調整(チャネルボンディング) パラメータ

20MHz：帯域幅モードを 20MHz に設定します。

40MHz：帯域幅モードを 40MHz に設定します。

80MHz：帯域幅モードを 80MHz に設定します。

160MHz：帯域幅モードを160MHzに設定します。このキーワードのサポートはAPモデルによって異なります。

320MHz：帯域幅モードを320MHzに設定します。このキーワードのサポートはAPモデルによって異なります。

auto：無線の帯域幅モードを20MHzと40MHzの間で切り替えることを可能にします。このキーワードは、802.11gnおよび802.11gac無線にのみ適用されます。

使用ガイドライン

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および802.11gax無線にのみ適用されます。無線のモードを変更すると、このコマンドの新しい無線モードのデフォルト設定が復元されます。

隣接チャネルを結合して40/80/160/320 MHzチャネルを形成できる場合、無線は指定された

40/80/160/320 MHz帯域幅を使用します。

隣接チャネルを結合して40/80/160/320MHzチャネルを形成できない場合、無線は指定された帯域幅よりも小さい、次に利用可能な帯域幅を使用します。

例えば、帯域幅モードが80MHzに設定されているとします。無線は、結合可能な隣接チャネルが存在する場合、80MHzの帯域幅を使用します。

80MHzチャネルに結合可能な隣接チャネルが存在しないが、40MHzチャネルに結合可能な隣接チャネルが2つ存在する場合、40MHzの帯域幅が使用されます。

結合可能な隣接チャネルが存在しない場合、無線は20MHzの帯域幅を使用します。

スマートO&M > ダッシュボード > WiFi7 Dashboard



接続端末AI分類

モード分布

非Wi-Fi 7

メーカーの分布

Wi-Fi 7



データがありません

主要指標 PK ②

非Wi-Fi 7

VS

Wi-Fi 7

-



-

平均遅延

-



-

帯域幅

-



-

アップリンク速度の選択

-



-

ダウンリンク速度の選択

-



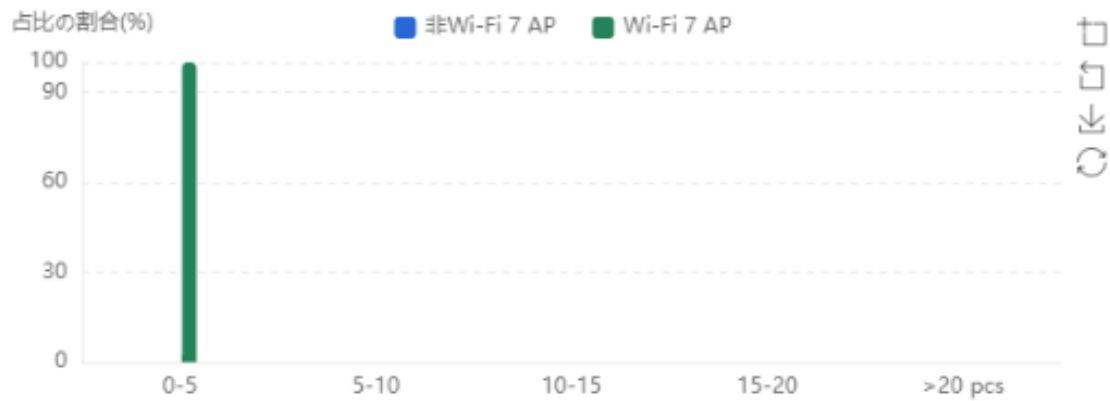
0

接続ユーザーの平均数

オンラインAP統計



AP同時接続端末の分布



端末平均遅延の分布



接続端末の帯域幅の分布



用語解説

SAE H2Eは、WPA3で使われるSAE (Simultaneous Authentication of Equals) プロトコルにおける、パスワードから秘密の要素を生成する新しい方式です。**H2E**とは**Hash to Element**の略です。

AES-CCMP (**C**ounter Mode with **C**ipher Block Chaining **M**essage Authentication Code **P**rotocol) と

AES-GCMP (**G**alois/**C**ounter **M**ode **P**rotocol) は、Wi-Fiネットワークにおける暗号化方式の一部であり、それぞれに特徴と用途があります。以下に両者の主な違いを示します。

1. 暗号化モード

AES-CCMP:

カウンタモード (Counter Mode) を使用して暗号化を行い、CBC-MAC (Cipher Block Chaining Message Authentication Code) を使用してデータの整合性を確認します。

データのセキュリティと整合性をバランスよく提供します。

AES-GCMP:

ガロア/カウンタモード (Galois/Counter Mode) を使用します。

ガロアフィールドを利用した高速なデータ整合性チェックを可能にします。

より新しいプロトコルで、計算効率が高い。

2. セキュリティ

AES-CCMP:

WPA2の標準暗号化方式として広く使用されています。

セキュリティは高いが、特定の攻撃シナリオではGCMPよりも若干遅いことがあります。

AES-GCMP:

WPA3において採用され、WPA2と比較してさらに強化されたセキュリティを提供します。

データの認証と暗号化が統合されているため、効率的かつ安全性が高い。

3. パフォーマンス

AES-CCMP:

暗号化と認証が独立して実行されるため、計算量が多くなりがちです。

パフォーマンスが求められるシナリオではGCMPに劣ることがあります。

AES-GCMP:

認証と暗号化を一体化した設計により、CCMPよりも処理速度が速い。

特に高速ネットワークや大規模な通信量がある環境で有利。

4. 適用シナリオ

AES-CCMP:

既存のWPA2ネットワークでの使用。

互換性を重視する場合に適しています。

AES-GCMP:

新しいWi-Fi規格 (特にWi-Fi 6やWPA3) に対応するアクセスポイントやデバイスに適しています。

高速かつ安全な通信が必要な場合に推奨。

H3C WLAN Wi-Fi 7 エンドポイント 互換性試験レポート

2025年8月現在

表 1 試験対象

メーカー	モデル	OSのバージョン
Intel	Intel® Wi-Fi 7 BE200 	Windows 11(24H2)
MTK	MediaTek Wi-Fi 7 MT7925	Windows 11(24H2)
MTK	MediaTek Wi-Fi 7 MT7927	Windows 11(24H2)
Qualcomm	Qualcomm FastConnect 7800 	Windows 11(24H2)
Realtek	Realtek 8922AE	Windows 11(24H2)
Apple	iPhone 16 (WiFi 6E 対応) この時点では試験していませんが iPhone 17 (WiFi 7 対応)	iOS 18.1(22B5075a)
SAMSUNG	Galaxy S24 Ultra (WiFi 7 対応))	Android 14(One UI UP1A.231005.007.S9280ZHS3AXI1)
ASUS	ROG 7	Android 14(ROG UI CN_34.1010.0820.90)
Google	Pixel 9 Pro	Android 15(AP4A.241205.013)
	Pixel 9	Android 15(AP3A.241105.008)
	Pixel 8	Android 15(AP41.240823.009)
	Pixel 8 Pro	Android 15(AP41.240823.009)

試験項目

テストは、市場で主流のWi-Fi 7エンドポイントで実施されます。テストには、基本的なアクセス機能、認証と暗号化、プロトコル、ローミングなどの側面が含まれます。表2にテスト項目を示します。

表 2 試験項目一覧

項目番号	説明
1	Wi-Fi 7 radio mode negotiation (open)
2	Wi-Fi 7 radio mode negotiation (wpa2)
3	Wi-Fi 7 radio mode negotiation (owe)
4	Wi-Fi 7 radio mode negotiation (wpa3-personal)
5	Wi-Fi 7 radio mode negotiation (wpa3-h2e only)
6	Wi-Fi 7 radio mode negotiation in roaming scenarios (wpa2-wpa2)
7	Wi-Fi 7 radio mode negotiation in roaming scenarios (wpa3-wpa2)
8	Wi-Fi 7 radio mode negotiation in roaming scenarios (wpa2-wpa3)
9	Wi-Fi 7 radio mode negotiation in roaming scenarios (wpa3-wpa3)
10	4KQAM negotiation (wpa3)
11	MLO mode negotiation (wpa3/owe)
12	MLO mode negotiation (wpa2)
13	Chinese SSID
14	All configurable channels in the CN country code.
15	2.4 GHz 40 Mbps bandwidth negotiation
16	5 GHz 80 Mbps bandwidth negotiation
17	5 GHz 160 Mbps bandwidth negotiation
18	WPA2-Enterprise (dot1x)
19	Enhanced open transition mode
20	WPA3-Personal transition mode
21	WPA3-Enterprise transition mode
22	WPA3-Enterprise mandatory mode
23	WPA3-Enterprise 192-bit mode
24	802.11r fast roaming
25	802.11kv cooperative roaming
26	Support for 6 GHz frequency band
27	6 GHz 320 Mbps bandwidth negotiation
28	MLO mode negotiation (6 GHz radio)

試験結果

このレポートのテスト結果は、表1に指定されたエンドポイントバージョンのみに基づいています。テスト結果はエンドポイントバージョンによって異なる場合があります。

結果の意味は次のとおりです：

- √—完全互換
- ○—部分的に互換性あり、注意が必要な問題あり
- —エンドポイントはこの試験項目をサポートしていない

6 GHz サポート

表3 無線エンドポイントが6 GHzをサポート

エンドポイントモデル	サポート試験項目						
	26	27	28				
Intel® Wi-Fi 7 BE200	√	√	√				
MediaTek Wi-Fi 7 MT7925	√	√	√				
MediaTek Wi-Fi 7 MT7927	√	√	√				
Qualcomm FastConnect 7800	√	√	√				
Realtek 8922AE	√	√	-				
iPhone 16	√	√	√				
Galaxy S24 Ultra	√	√	√				
Pixel 9 Pro	√	√	√				
Pixel 9	√	√	√				
Pixel 8	√	√	√				
Pixel 8 Pro	√	√	√				

Intel

表4 ワイヤレスネットワークアダプタでサポートされている項目

エンドポイントモデル	サポート試験項目																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Intel® Wi-Fi 7 BE200	-	-	√	√	√	-	-	-	√	√	√	-	√	√	√	√	√	√
エンドポイントモデル	サポート試験項目																	
	19			20			21			22			23			24		
Intel® Wi-Fi 7 BE200	√			√			√			√			-			○		

Qualcomm

表 5 Qualcomm ワイヤレス ネットワーク アダプタでサポートされているテスト項目

エンドポイントモデル	サポート試験項目																						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18					
Qualcomm	-	-	√	√	√	-	-	-	√	√	√	-	√	√	√	√	√	√					
エンドポイントモデル	サポート試験項目																						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18					
FastConnect 7800																							
エンドポイントモデル				サポート試験項目																			
				19			20			21			22			23			24			25	
Qualcomm FastConnect 7800				√			√			√			√			-			○			√	

Realtek

表 6 Realtek ワイヤレス ネットワーク アダプタでサポートされているテスト項目

エンドポイントモデル	サポート試験項目																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Realtek 8922AE	√	√	√	√	√	√	-	-	√	√	-	-	√	√	√	√	√	√

エンドポイントモデル	サポート試験項目													
	19		20		21		22		23		24		25	
Realtek 8922AE	√		√		√		√		-		○		√	

Apple

表 7 Apple エンドポイントでサポートされているテスト項目

エンドポイントモデル	サポート試験項目																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
iPhone 16	√	-	√	√	√	-	-	-	√	-	√	-	√	√	-	√	√	√

エンドポイントモデル	サポート試験項目						
	19	20	21	22	23	24	25
iPhone 16	√	√	√	√	√	√	√

SAMSUNG

表 8 SAMSUNGエンドポイントでサポートされているテスト項目

エンドポイントモデル	サポート試験項目																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Galaxy S24 Ultra	-	-	√	√	√	-	-	-	√	√	√	-	√	√	○	√	√	√
エンドポイントモデル	サポート試験項目																	
	19		20		21		22		23		24		25					
Galaxy S24 Ultra	√		√		√		√		√		√		√					

ASUS

表9 ASUSエンドポイントでサポートされているテスト項目

エンドポイントモデル	サポート試験項目																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18		
ROG 7	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√		
エンドポイントモデル	サポート試験項目																			
	19			20			21			22			23			24			25	
ROG 7	√			√			√			√			√			√			√	

Google

表10 Google エンドポイントでサポートされているテスト項目

エンドポイントモデル	サポート試験項目																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Pixel 9 Pro	√	-	√	√	√	-	-	-	√	○	√	-	√	√	-	√	√	√
Pixel 9	√	-	√	√	√	-	-	-	√	○	√	-	√	√	-	√	√	√
Pixel 8	√	√	√	√	√	√	√	√	√	○	√	√	√	√	-	√	√	√
Pixel 8 Pro	√	√	√	√	√	√	√	√	√	○	√	√	√	√	-	√	√	√

エンドポイントモデル	サポート試験項目							
	19	20	21	22	23	24	25	
Pixel 9 Pro	√	√	√	√	√	√	√	
Pixel 9	√	√	√	√	√	√	√	
Pixel 8	√	√	√	√	√	√	√	
Pixel 8 Pro	√	√	√	√	√	√	√	

(参考)WiFi 8概要

NAVIGATE

H3C

**World's First
Enterprise-Grade Wi-Fi 8 AP**
Interference-Proof Intelligent Connectivity

WA8648 Five-Band Flagship Wi-Fi 8 AP

25%↑ Higher Throughput Throughput improved in harsh RF environments	25%↓ Lower Latency P95 latency response reduced	25%↓ Lower Packet Loss Packet loss reduced during roaming
--	--	--

AIを活用したエッジアプリケーションが急増し、超高信頼性かつ低遅延の接続が求められる中、従来のWi-Fiの速度重視のアップグレードモデルでは不十分であることが明らかになっています。H3Cの新しいフラッグシップ5バンドWi-Fi 8アクセスポイントは、「速度追求」から「ユーザーエクスペリエンスの保証」へとパラダイムシフトを起こし、混雑した環境、干渉を受けやすい環境、そして高移動環境においても、安定したほぼロスレスの接続を実現します。

内蔵AIエンジンを搭載したこのアクセスポイントは、Wi-Fi 8の協調型空間再利用と動的スペクトルスケジューリングを活用し、ミリ秒レベルのマルチアクセスポイント連携によってスペクトル効率を30%向上させます。

主な特長は3つあります。

過酷な環境下でも25%以上高いスループットを実現するエッジカバレッジ

産業制御や遠隔医療などレイテンシに敏感な用途向けに25%低いレイテンシ

ハンドオフ時のパケットロスと25%削減し、途切れることのないモバイルワークフローを保証するロスレスローミングです。

企業の運用負担を軽減するため、本デバイスはエージェントAIを採用し、メンテナンスを簡素化します。リアルタイムの環境認識、周波数帯域の自動最適化、迅速な障害根本原因分析を実現し、手動介入を排除します。

特筆すべきは、H3CがWi-Fi 7+製品にWi-Fi 8の主要機能を事前に搭載し、企業向けに現在のパフォーマンスと将来のアップグレード性を両立させた移行ソリューションを提供している点です。今回の製品発表は、マルチ周波数スケジューリングと高密度同時接続の課題に対応するコアチップを提供するBroadcomとの戦略的パートナーシップによって支えられています。