HPE Aruba Networking Central 基本操作ガイド

～IAP 編 (AOS6, AOS8)～

日本ヒューレット・パッカード合同会社
Aruba 事業統括本部

目次

以下の表に、本文書の修正点を示します。

表 1: 改訂履歴

版数	主な変更内容
第1版	初版発行
第2版	Central 2.5.2における変更点を追加
第3版	Central 2.5.3における変更点を追加
第4版	Central 2.5.4における変更点を追加
第5版	テンプレート変更に伴う修正等

1. はじめに

1.1. 本資料について

本資料は HPE Aruba Networking Central におけるインスタントアクセスポイント（AOS6,AOS8）の基本操作、設定についてサンプル構成を用いた設定例を紹介しています。

1.2. 注意事項

本資料は弊社内において基本動作等を確認したものであり、お客様の環境における動作の保証をしているものではございません。また、Windows, Windows Server など HPE Aruba Networking で取り扱っていない製品を使用して説明しているため、設定内容における保証は致しかねます。構成を構築する上での参考にしていただくドキュメントであることを予めご了承ください。本資料の内容は予告なく変更される場合があります。

Central を初めて使われる方は以下の Central 基本操作ガイド（入門編）をはじめに参照いただくことを推奨いたします。

https://www.hpe.com/psnow/doc/a00143744jpn

1.3. Software Version

本資料は HPE Aruba Networking Central 2.5.4 を元に作成しております。

※一部キャプチャ画像が最新の Central 画面と異なることがございます。ご了承ください。

2. Instant AP へのアクセス

2.1 Instant AP と PC との接続について

Instant AP は初期値として IP アドレスが設定されておりません。**DHCP サーバが動作をしている環境**、もしくは**コンソールケーブル**をご用意ください。DHCP サーバを利用する場合は、配布をする Default Gateway に通信が可能な環境で行ってください。

2.2 電源の投入

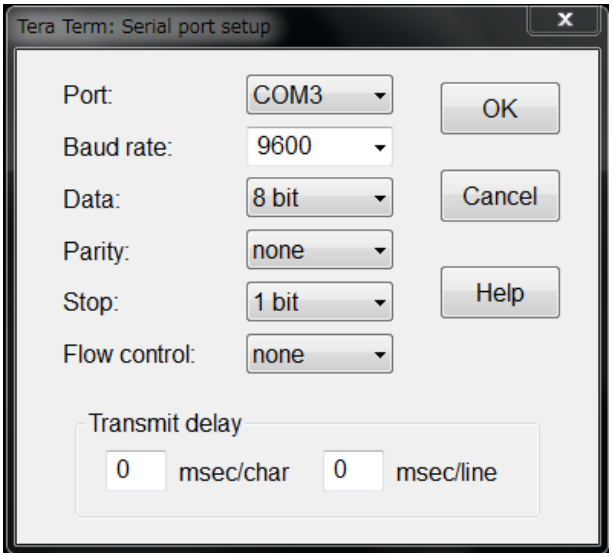
Instant AP には電源アダプタ、もしくは PoE にて給電を行うことができます。
＊モデルによって起動に必要な電力が違います。詳しくはアクセスポイントのデータシート等を確認ください

2.3 コンソールケーブルを用いての IP アドレス設定

コンソールケーブルは AP の製品により異なります。コンソールケーブルが同梱されている製品および同梱されておらず別売りとなっている製品の 2 つのパターンがありますので、ご注意ください。

①　ターミナルソフト設定

Baud rate:9600 , Data:8bit , Parity: none , Stop:1bit , Flow control: none に設定をし 、電源が入っていない Instant AP にコンソールケーブルを接続

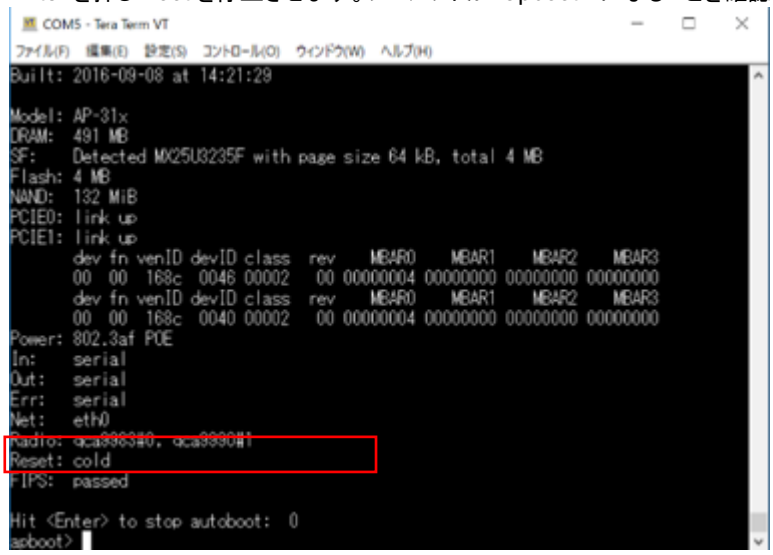


②　電源の投入

アダプタもしくは、PoE から Instant AP に給電を行う

③　Boot の停止

Instant AP に IP アドレスを振るためには、Boot 途中で ”Hit <Enter> to stop autoboot:” が表示されますので、このメッセージが出たら Enter を押し Boot を停止させます。プロンプトが ”apboot>”になることを確認ください。



このメッセージが出たら Enter を押します。

＊”Hit <Enter> to stop autoboot:”は電源投入後、3，4 秒で表示される

④　IP Address/Subnet Mask/Default Gateway/DNS の設定

下記のコマンドで IP Address/Subnet Mask/Default Gateway を指定する

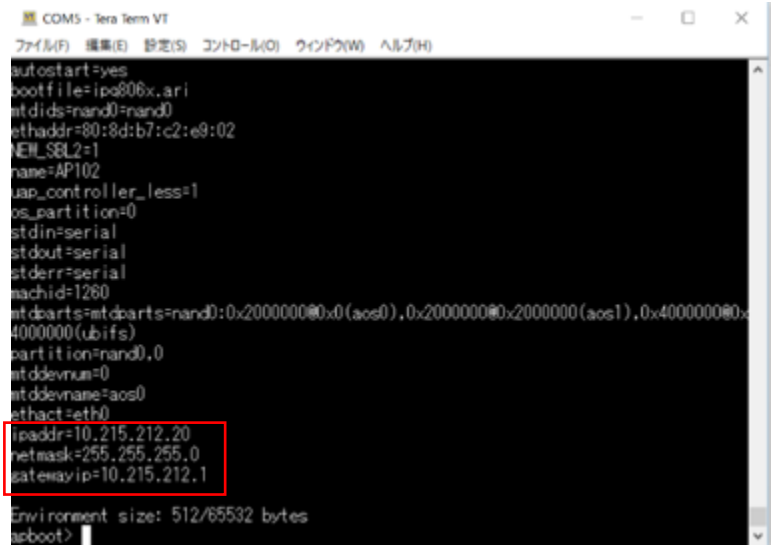
・setenv ipaddr <ip アドレス>

・setenv netmask <netmask>

・setenv gatewayip <default gateway アドレス>

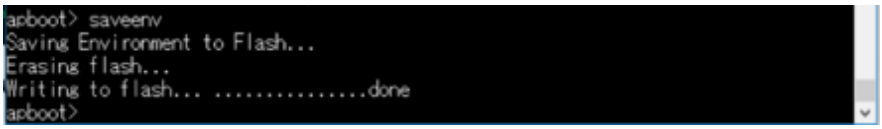
・setenv dnsip <DNS Server アドレス>

⑤　設定内容の確認
“printenv”コマンドで設定されている内容があっているかを確認する



＊コマンドが間違っていた場合は反映されません。再度設定をやり直してください。

⑥　設定内容の保存・起動
“ saveenv ” コマンドで設定を書き込み、” boot ”コマンドで再起動する



起動後 User:admin Password:admin または AP のシリアルナンバーで入り、” show ip interface brief ”で設定した内容が反映されていることが確認できる

2.4 GUI からのアクセス

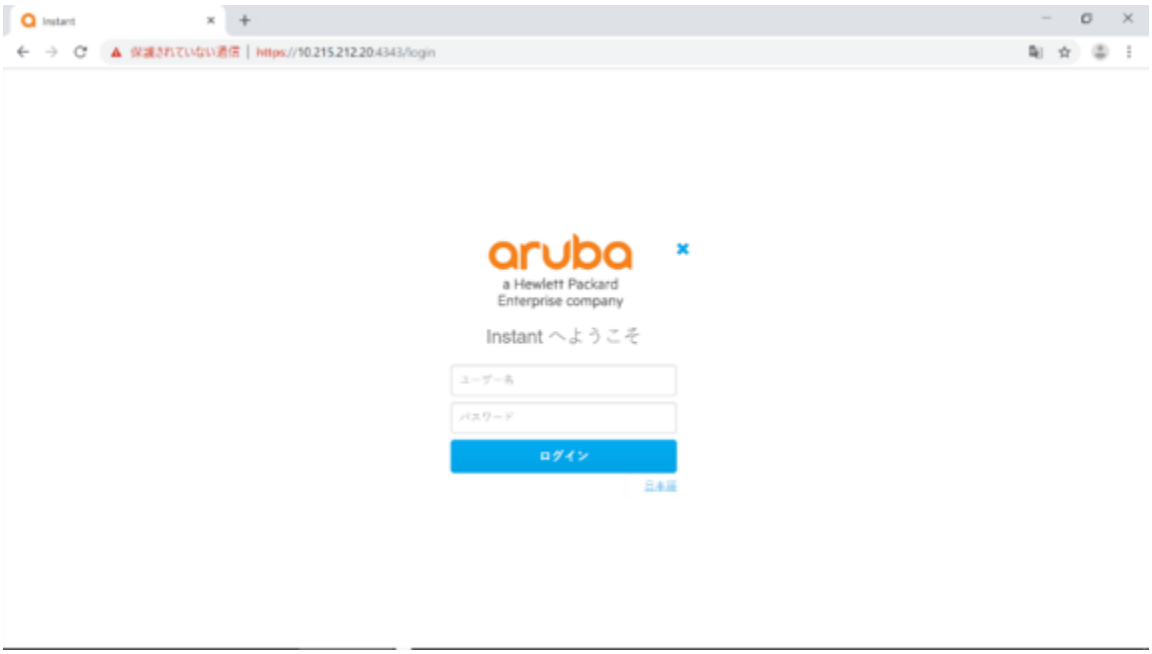
Instant AP は GUI/CLI どちらを用いても設定が可能ですが、GUI からの設定が基本となります。

推奨のブラウザは以下の通りです。

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 38.14393.0.0 and Microsoft EdgeHTML 14.14393) on Windows 10
- Firefox 48 or later on Windows 7, Windows 8, Windows 10, and Mac OS
- Apple Safari 8.0 or later on Mac OS
- Google Chrome

2.4.1　有線側 IP アドレスへの接続

DHCP サーバ または CLI より IP アドレスを確認し、Instant AP に割り当てられた IP アドレスへブラウザからアクセスしてください。アドレスのみの場合は自動的に https ページへリダイレクトされます。



＊ログインボタン右下に言語設定があります。ブラウザの言語設定に対して表示されますが、必要によって言語を変更してください。

2.4.2 無線側 IP アドレスへの接続

① 初期設定では設定用に”SetMeUp-xx:xx:xx”(xx:xx:xx には IAP の MAC アドレス下 6 桁が入ります)という SSID が出力されています。この SSID に対して PC を無線接続した上で、ブラウザから https://setmeup.arubanetworks.com にアクセスします。

② SSID SetMeUp-xx:xx:xx に接続

③ PC の IP アドレスを確認します。
Instant AP で DHCP サーバが起動しています。SSID=” SetMeUp-xx:xx:xx” に接続すると、PC に IP アドレスが振られます。

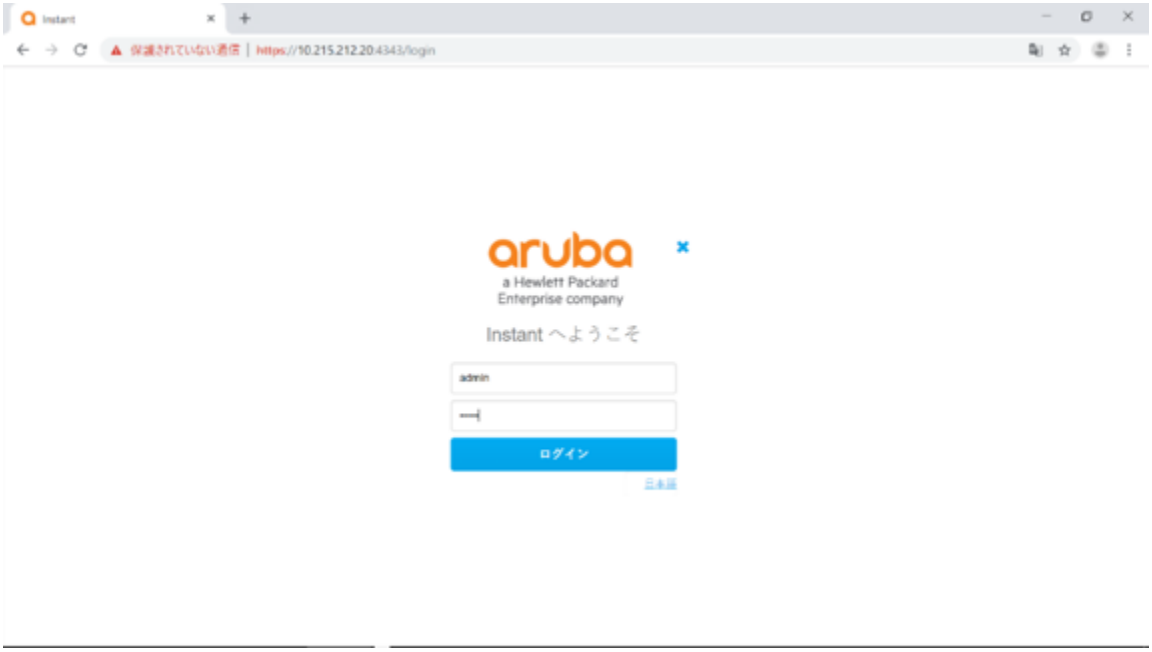
```
Wireless LAN adapter ワイヤレス ネットワーク接続:

   接続固有の DNS サフィックス . . . :
   リンクローカル IPv6 アドレス. . . . : fe80::6152:5300:f7c3:f584%12
   IPv4 アドレス . . . . . . . . . . : 10.254.99.70
   サブネット マスク . . . . . . . . : 255.255.254.0
   デフォルト ゲートウェイ . . . . . : 10.254.98.1
```

④ PC のブラウザから Instant AP にアクセスする
” https://setmeup.arubanetworks.com”（もしくは、(2)で確認したゲートウェイ）にアクセスをします。

2.5 Instant AP へのログイン（GUI/CLI 共通）

初期設定では ユーザ名：admin パスワード：admin でログインすることができます。
AOS8.5 以降ではユーザ名：admin パスワード：AP のシリアルナンバー



3. Instant AP の登録

3.1 サブスクリプション、デバイスの追加方法とサブスクリプションの割り当て

サブスクリプション、デバイスの追加方法とサブスクリプションの割り当てに関しては、以下 Central 基本操作ガイド（入門編）を参照

https://www.hpe.com/psnow/doc/a00143744jpn

3.2 グループ・サイト・ラベルの作成方法

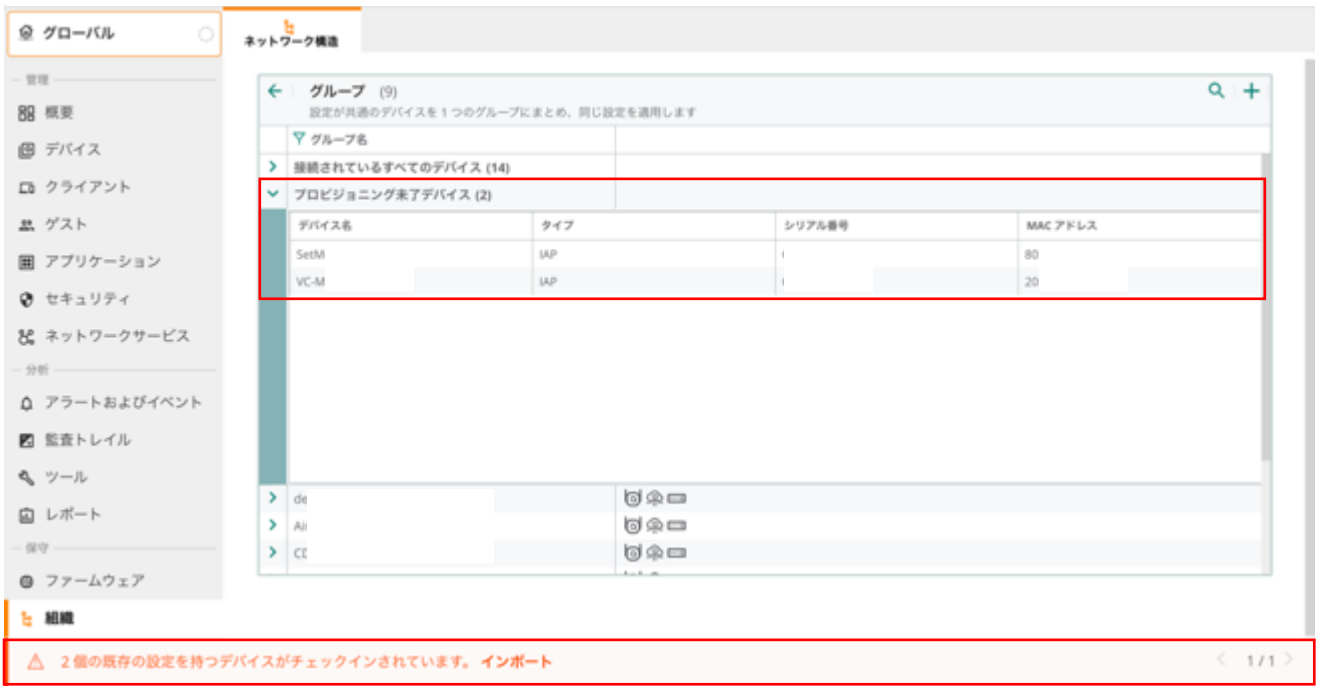
グループ・サイト・ラベルの作成方法に関しては、以下 Central 基本操作ガイド（入門編）を参照

https://www.hpe.com/psnow/doc/a00143744jpn

3.3 初期状態の AP のプロビジョニング

工場出荷状態の AP をプロビジョニングする方法です。この方法で AP をプロビジョニングした場合、AP の設定は Central に帰属するグループの設定へと上書きになるため、ご注意ください。
AP にある既存のコンフィグを Central にインポートしたい場合は、設定済み AP のプロビジョニングを参考にしてください。
＊グループに VC を割り当てた時点で、その VC 配下にある AP は全てグループのコンフィグを反映させるためにリブートします。ただしグループ内のコンフィグと IAP のコンフィグに差分がない場合はリブートしません。

① ネットワーク操作アプリ内、右上の マークをクリック
② 追加する AP を Central のデバイスインベントリーに追加
　＊詳しくは Central 基本操作ガイド（入門編）を参照（https://www.hpe.com/psnow/doc/a00143744jpn）
③ 追加したデバイスにサブスクリプションを割り当てる
　＊詳しくは Central 基本操作ガイド（入門編）を参照（https://www.hpe.com/psnow/doc/a00143744jpn）
④ IAP を起動する
　＊IAP に DNS の設定が必須です。詳しくは、InstantAP へのアクセスを参照
　サブスクリプションの当たっている IAP は、起動プロセス中 Activate 接続のタイミングで自身が Central 配下の IAP であることを認識し、自動的に Central へ接続しにいきます。
⑤ グループ管理画面から、プロビジョニング未完了デバイスとして IAP が認識されていることを確認
　＊グループに所属していないデバイスが Central で認識された場合、画面下部のようなアラートが出る



⑥ 新しいグループを作成、未割り当てのデバイスをとして認識されているデバイスをグループへ割り当て
　＊詳しくは Central 基本操作ガイド（入門編）を参照（https://www.hpe.com/psnow/doc/a00143744jpn）

3.4 設定済み AP のプロビジョニング

既存のコンフィグを残したまま IAP を Central にプロビジョニングする方法です。
＊この方法は既存のコンフィグを残すため、VC からグループを作成したとしても AP のリブートは起こりません。

① 初期状態の AP のプロビジョニング①～⑤まで同じ手順
② プロビジョニング未完了のデバイスを選択して、“グループのインポート”をクリック

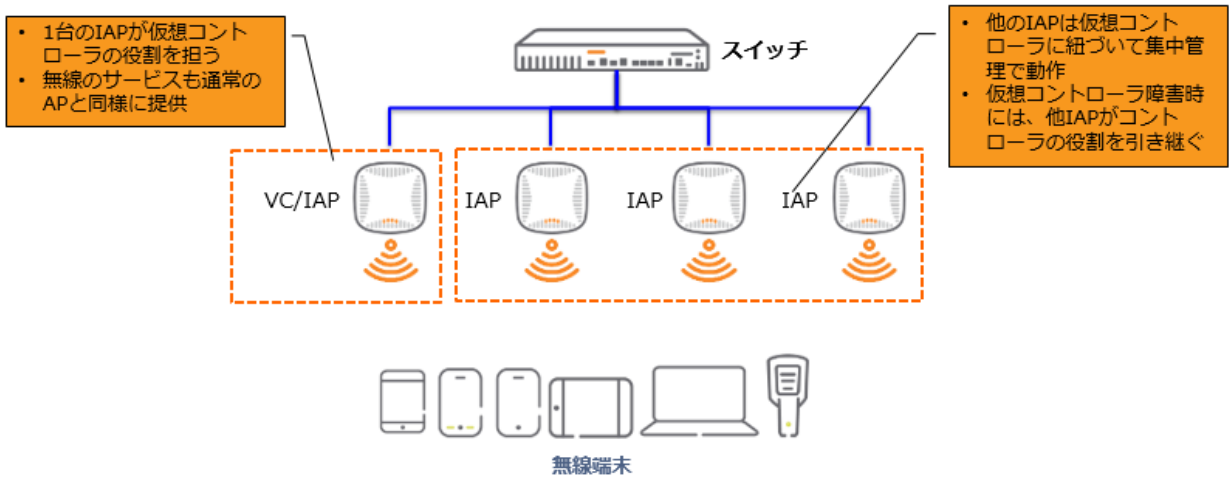
③ グループ名を入力し、“追加”をクリック

④ IAP の設定がインポートされていることを確認し、設定済み IAP のプロビジョニングが完了

4　Instant AP 基本設定

4.1　Instant AP 仮想コントローラの考え方

同一 L2NW 内の Instant AP のうち 1 台が仮想コントローラの役割を行います。仮想コントローラが起動している Instant AP に障害が発生した場合は、ネットワーク上にある他の Instant AP に仮想コントローラ機能が引き継がれ動作をし続けます。



Instant AP の動作条件は下記のとおりです。
・同一 L2NW のみでの稼動

・同一 L2NW 内で複数の Instant AP クラスタは作成できません。

・異なる型番の Instant AP でも Version が同一であれば管理可能（Version UP 時の制限あり）

・優先マスター設定をしていない場合、ネットワーク上で最初に立ち上がった Instant AP で”仮想コントローラ”がマスターとして動作を行います。

4.2　仮想コントローラ名変更・仮想コントローラ IP 指定

仮想コントローラ IP は設定しなくても問題ありませんが、設定をすることで常に この IP アドレスへアクセスすれば良くなりますので、管理性が向上します。Instant AP のネットワーク内で重複していないアドレスを付与することを推奨します。
①　フィルターよりグループを選択

② 左メニューよりデバイスを選択し、右上の ⚙ をクリック

③ 右側の“詳細を表示”をクリックし、システムタブをクリック
仮想コントローラを選択し、右の鉛筆マークをクリック

④　名前と IP アドレスを入力し、“OK”をクリック

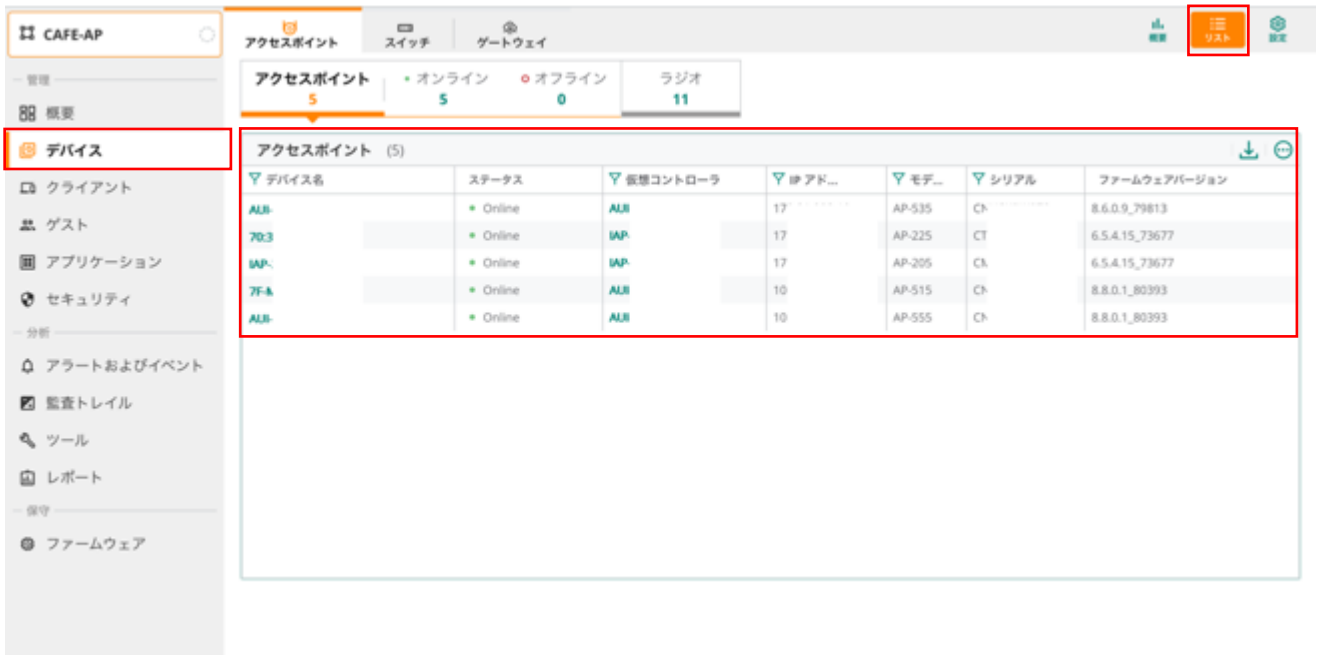
⑤　内容を確認し“設定の保存”をクリック

4.3 クラスタへの AP 追加

新しい Instant AP を仮想コントローラが立ち上がっている同一ネットワークに追加をするだけで自動的にクラスタへの AP 追加ができます。Central 上管理するためには新しく追加した AP のデバイス追加とサブスクリプションの割り当て作業が必要となります。

① 追加したい AP をデバイスインベントリに追加
　＊詳しくは Central 基本操作ガイド（入門編）を参照（https://www.hpe.com/psnow/doc/a00143744jpn）
② AP にサブスクリプションを割り当てる
　＊詳しくは Central 基本操作ガイド（入門編）を参照（https://www.hpe.com/psnow/doc/a00143744jpn）
③ AP を仮想コントローラが立ち上がっている同一ネットワークに追加
④ フィルターより仮想コントローラが所属するグループを選択

⑤ デバイス一覧で追加した AP があることを確認する

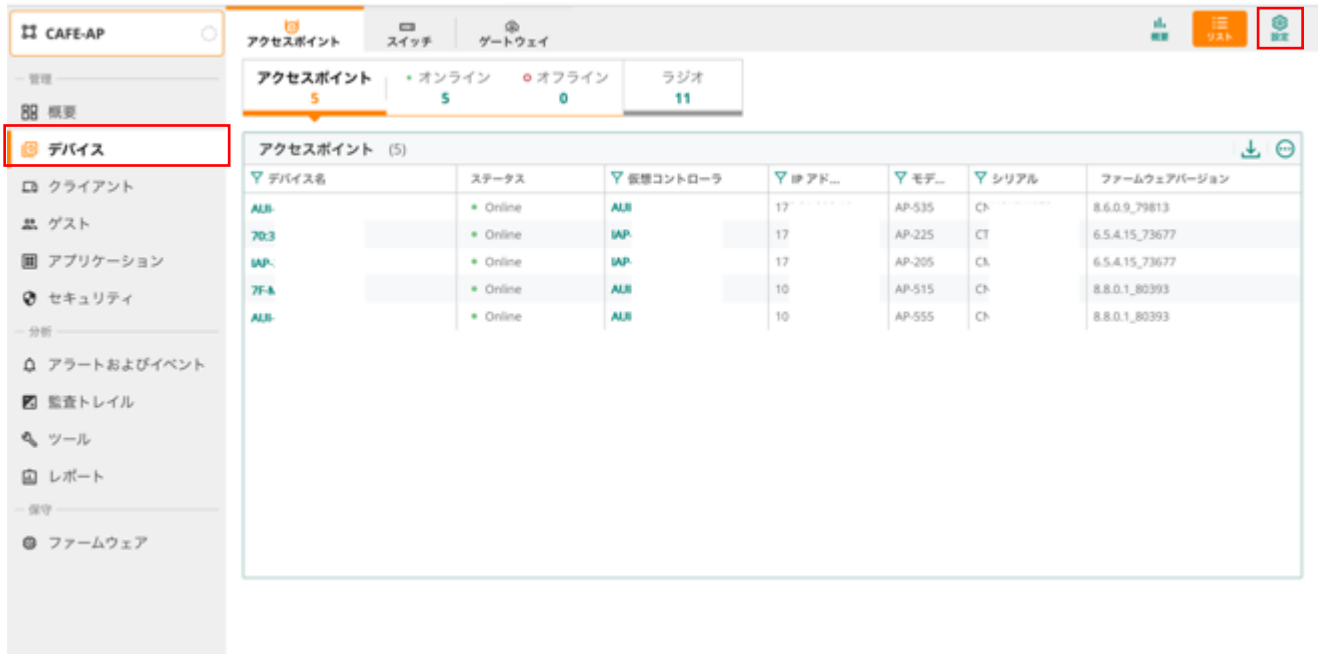


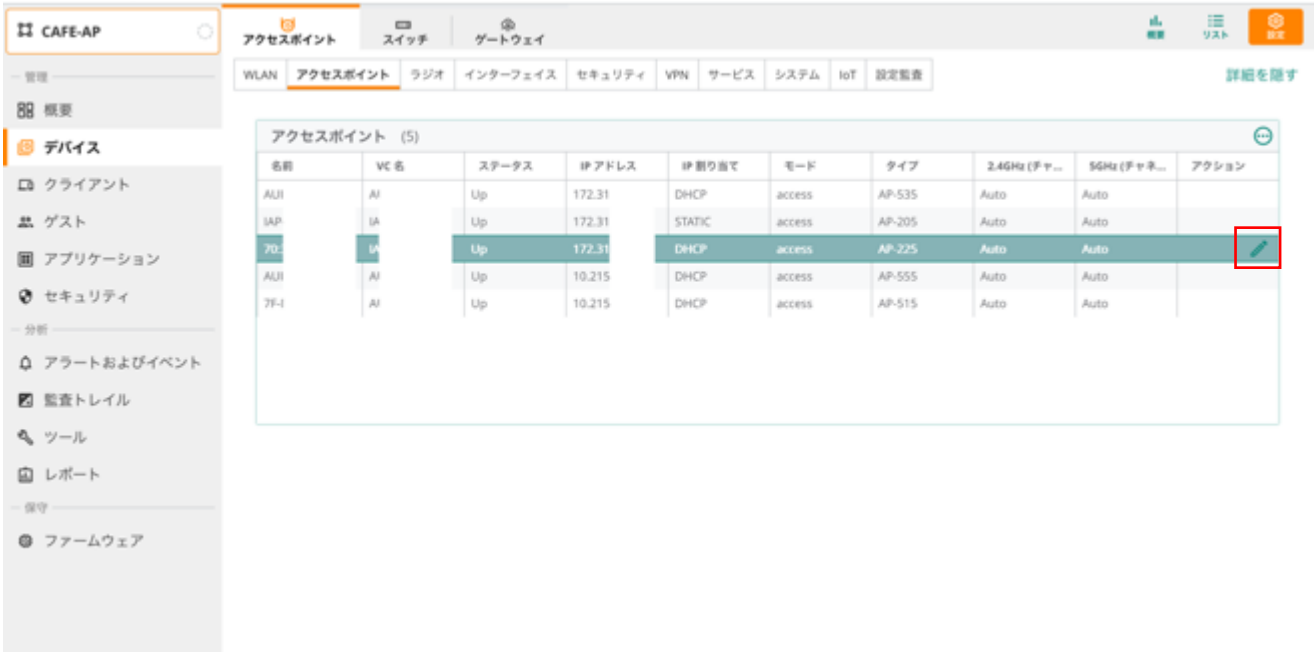
注1）　新しい Instant AP にコンフィグが入っている場合でも、すでに立ち上がっている仮想コントローラを認識すると仮想コントローラにあるコンフィグに書き換えられます。
注2）　同一型番の Instant AP を追加する場合には仮想コントローラに入っている Version に合わされますが、異なる型番の場合には予め Version を合わせた上でネットワークに追加してください。

4.4 各 AP の AP 名・IP アドレス設定

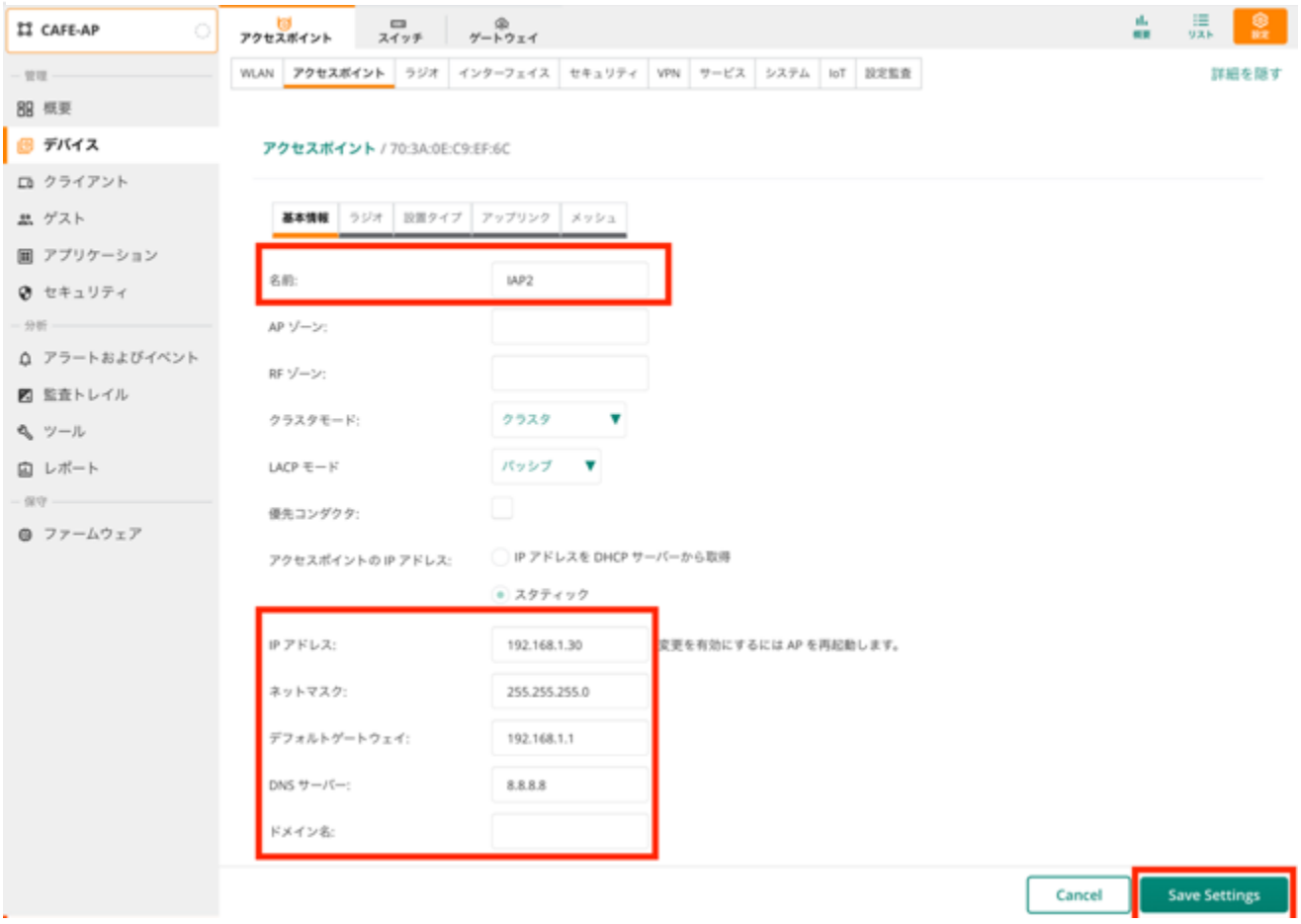
① フィルターからグループを選択

② デバイスメニューを選択し、右上に表示されるギアマークをクリックして、設定変更画面へ移動し、該当の AP を選択して右に表示される鉛筆マークをクリック

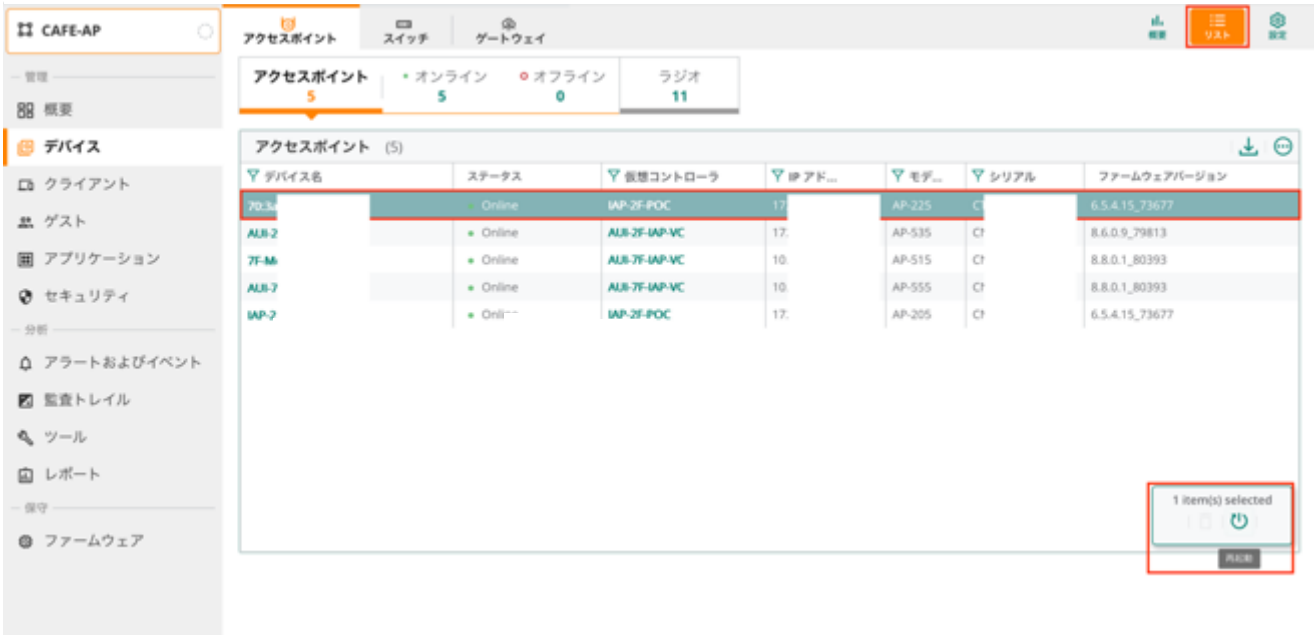




③　名前を編集し、アクセスポイントの IP アドレスをスタティックで設定し、”設定の保存”ボタンをクリック
＊アドレスを変更した場合は再起動が促されます。再起動は行われません。



④　再起動するため右上のリスト表示アイコンをクリックして、デバイス一覧に戻る。
AP 名、IP アドレスの変更をしたデバイスを選択すると“再起動”タブが表示されるため、それをクリックして再起動させる、



⑤　確認画面にて“はい”を選択し、再起動する

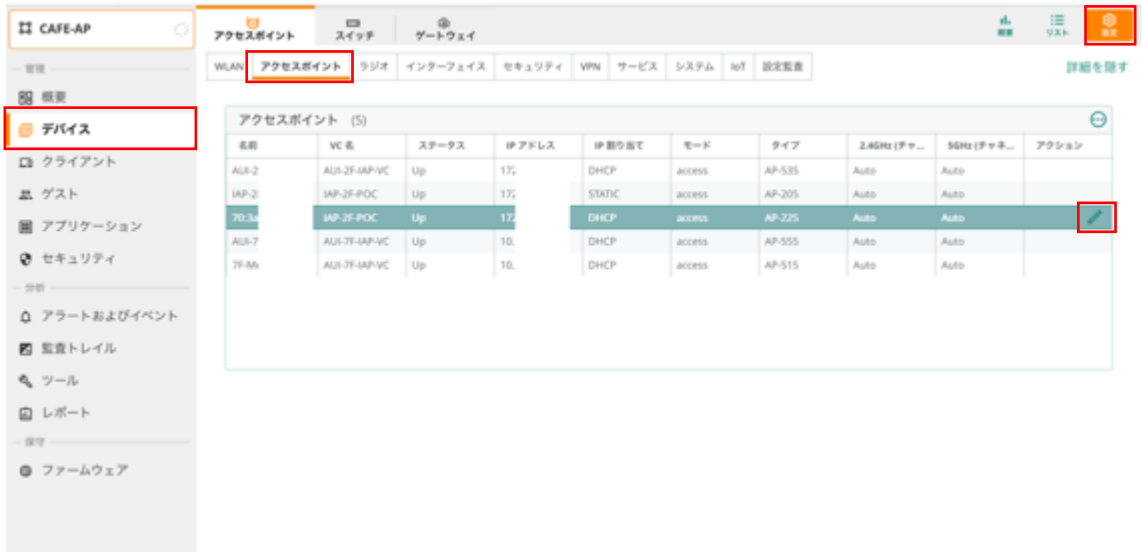
再起動が終わったら、該当デバイスがオンラインになっていることを確認し、AP 名と IP アドレスが変更されていることをご確認ください。

4.5 優先マスター設定

“優先マスター” 設定をしておくことで、仮想コントローラは常に指定した Instant AP で稼動をするようになります。 “優先マスター”に障害が発生した場合は、一時的に他の Instant AP にマスターが引き継がれますが、 ”優先マスター”が復旧した場合は設定した Instant AP に戻ります。管理上必要な場合に設定を行います。

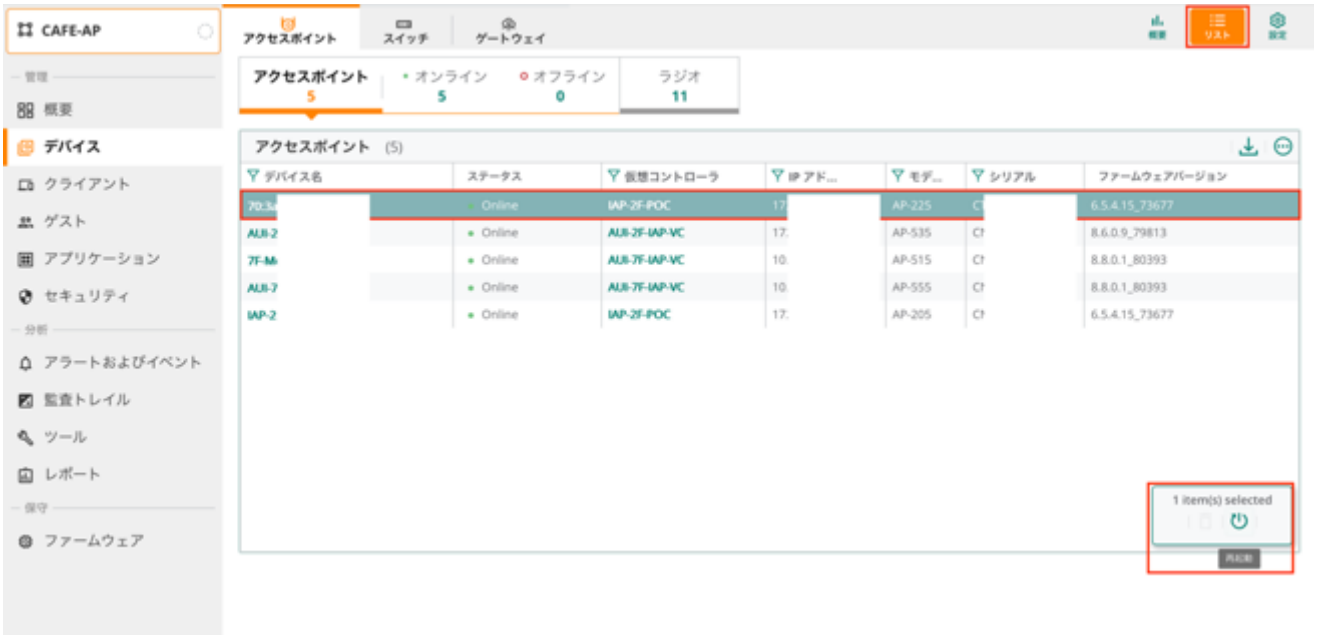
①　フィルターからグループを選択

②　デバイスメニューより設定アイコンをクリックし、優先マスターに設定する AP を選択し、右の鉛筆マークをクリック



③　“優先コンダクタ”を有効にして“設定の保存”をクリック

④　この設定を有効とするには AP の再起動が必要なため、デバイス一覧に戻って再起動する。

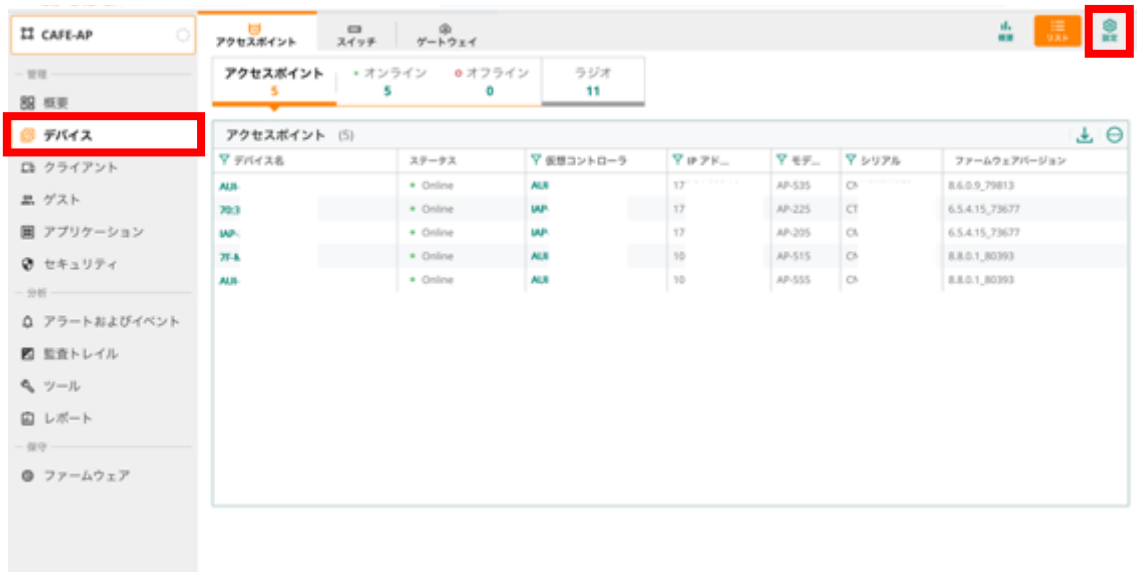


4.6 NTP 設定

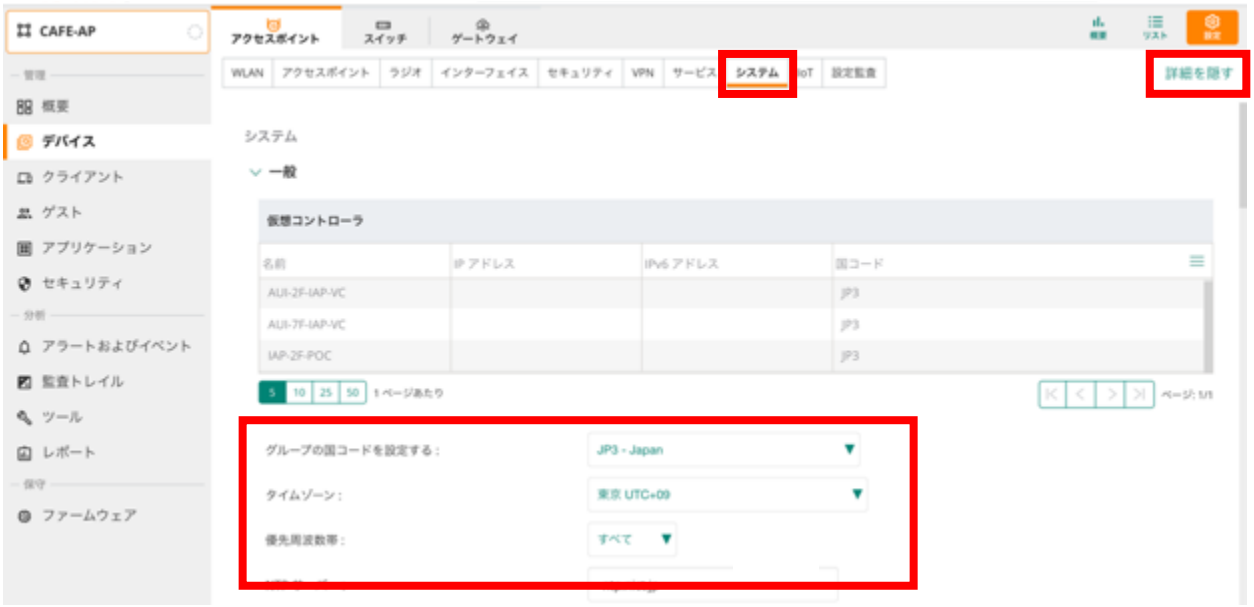
IAP はデフォルトで pool.ntp.org と時刻同期をします。他の任意の NTP サーバと時刻同期を行う場合に設定を行います。不具合発生をした場合には他機器とのログ比較を行う必要が出てきますので、設定していただくことを推奨いたします。

①　フィルターよりグループを選択

②　左メニューよりデバイスを選択し、右上の ⚙ をクリック



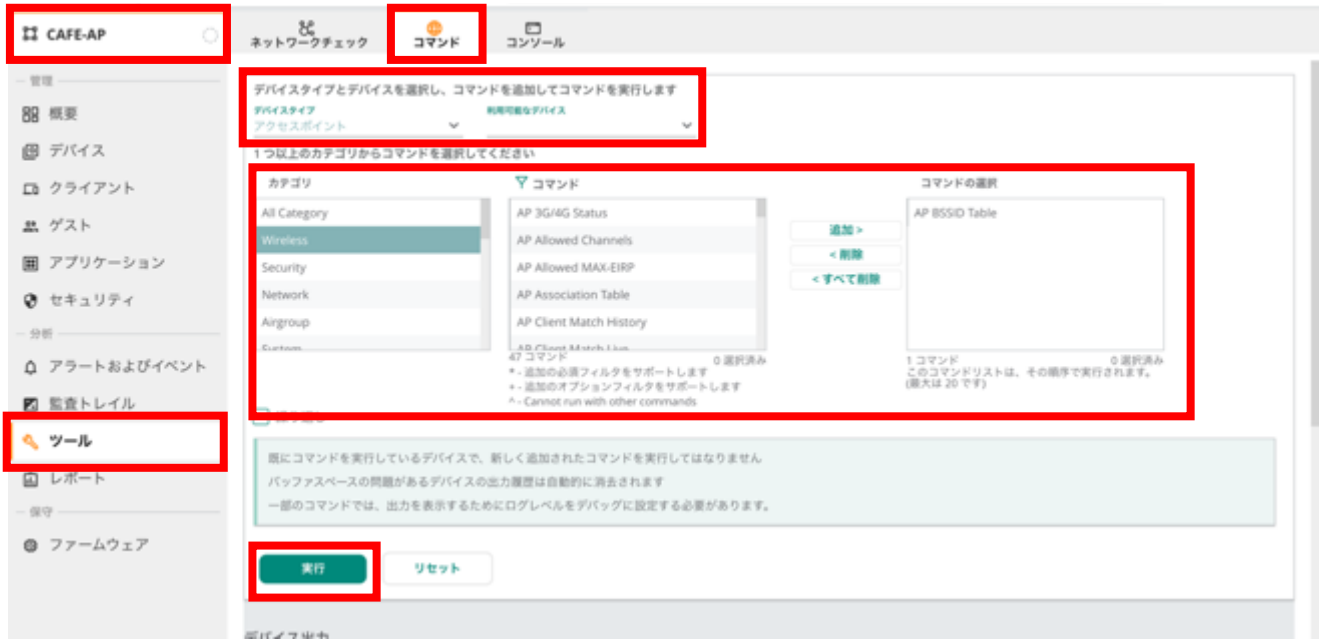
③　　右側にある“詳細を表示”をクリックし、“システム”タブを選択
NTP サーバーのアドレスを入力し、タイムゾーンは“Tokyo UTC +09”に変更し、“設定の保存”



4.6.1　時刻同期の確認1（GUI）

①　グループを選択後、メニューから“ツール”を選択し、“コマンド”タブをクリック
デバイスタイプとデバイスを選択してから、適当なコマンドを選んで“実行”をクリック

実行結果の時間から時刻が同期されていることを確認

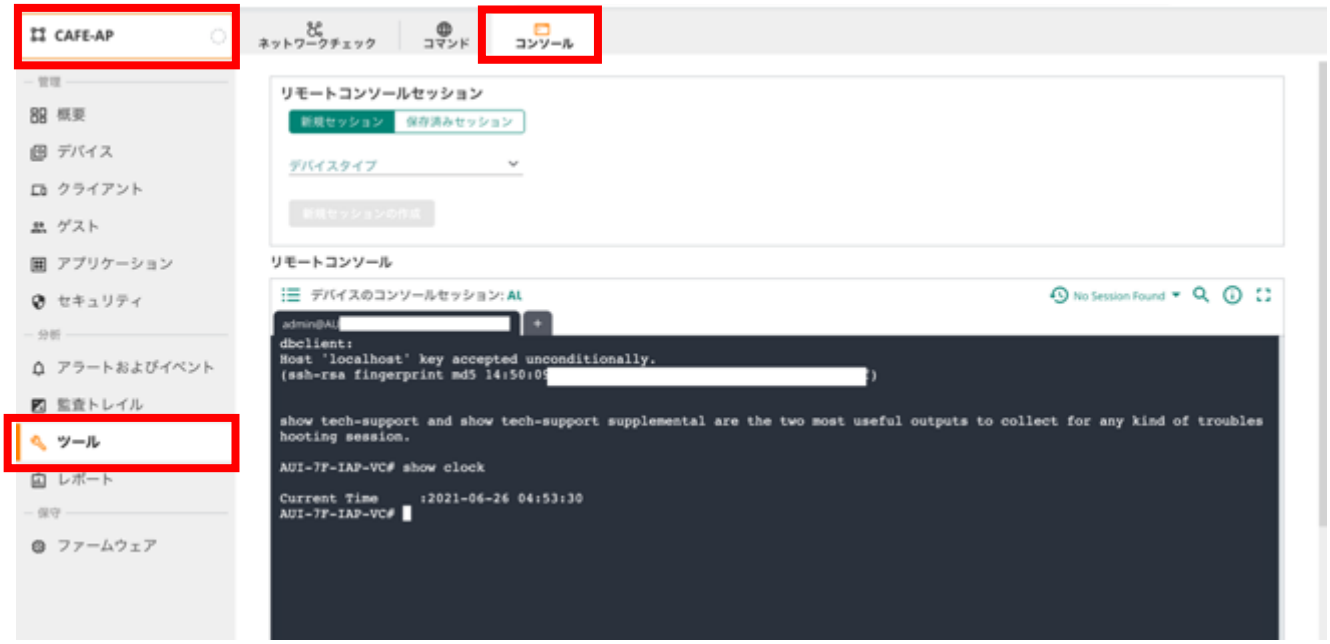


4.6.2　時刻同期の確認2（GUI コンソール）

Central では GUI から AP のコンソールがひらけます

① グループを選択＞ツール＞コンソールタブをクリック
② コンソールを開きたいデバイスタイプ・デバイス名・ユーザー名・パスワードを入力して“新規セッションの作成”をクリック
※Central 管理のデバイスのユーザー名・パスワードは基本的に、admin/グループのパスワード　になります。

コンソールで“show clock”で時刻を確認

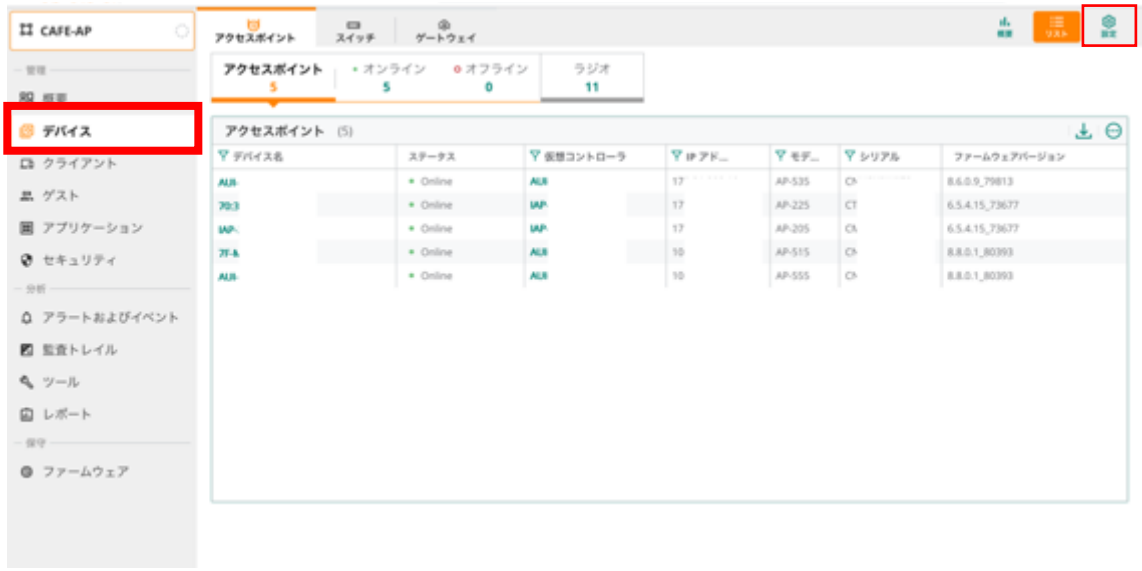


4.7. ダイナミック Radius プロキシ

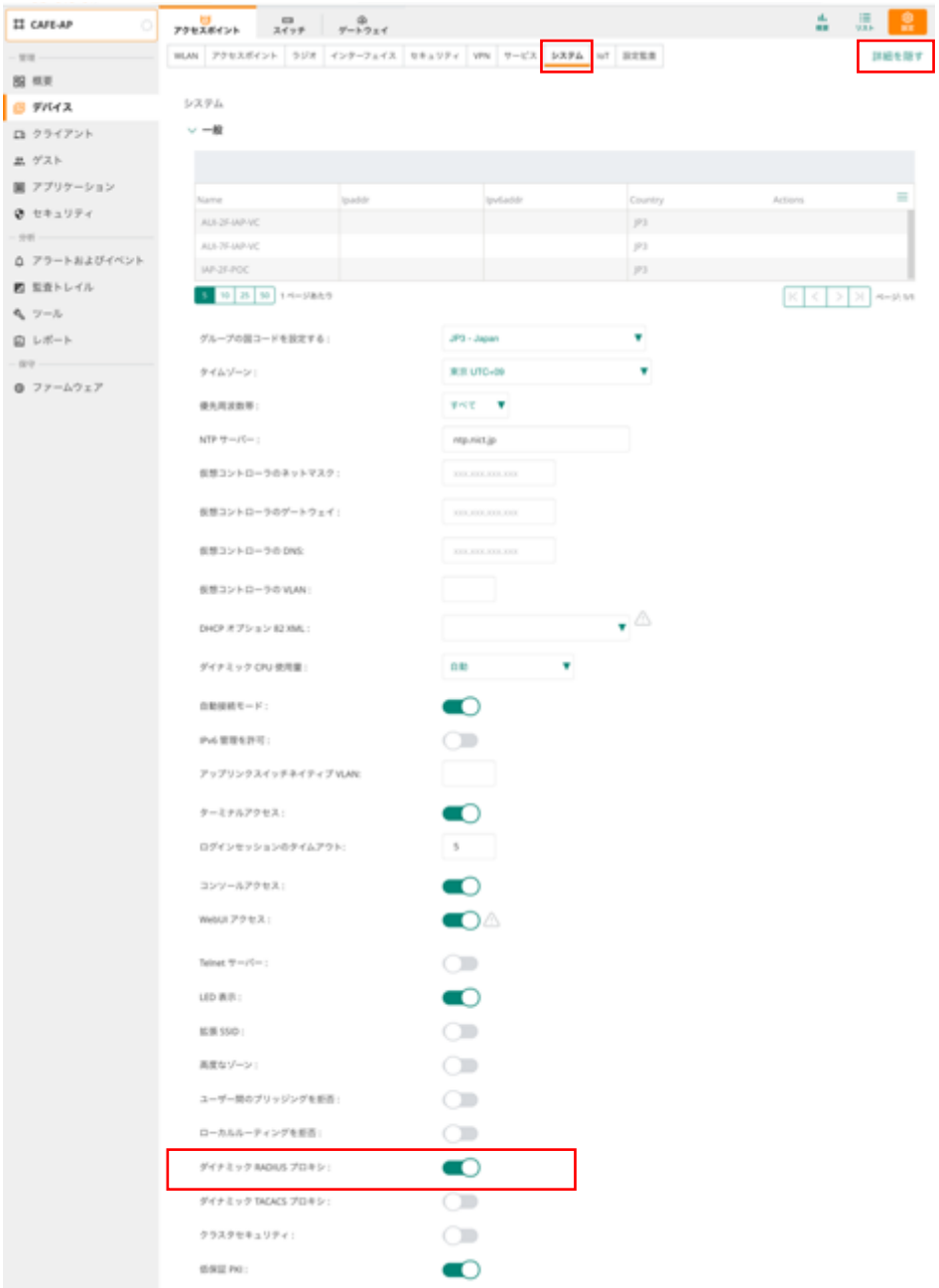
外部の Radius サーバへ認証を行う際、ダイナミック Radius プロキシを利用することで、認証パケットは仮想コントローラを経由させることができます。(この設定をしていない場合は AP 毎に外部 Radius に認証を行います。)必要によって設定を行ってください。

①　フィルターよりグループを選択

②　左メニューよりデバイスを選択し、右上の ⚙ をクリック



③　“詳細を表示”をクリックし、システムタブをクリック
“ダイナミック RADIUS プロキシ”を有効にし“設定の保存”

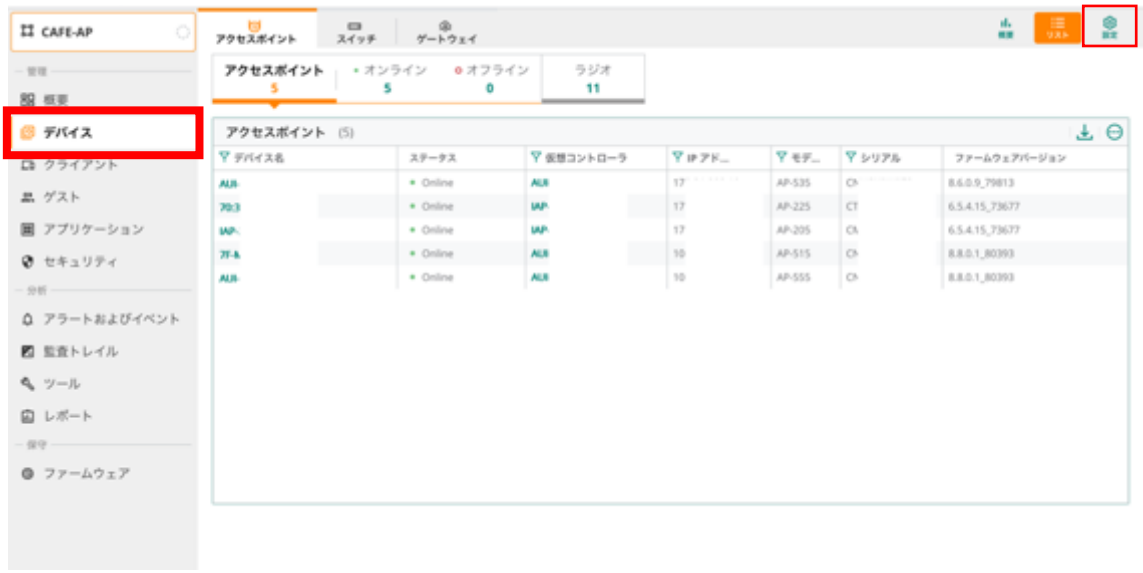


4.8. AppRF

AppRF を有効にすることで、Instant AP を通過するパケットから利用しているアプリケーションを特定することが可能になります。SSID のアクセスルールと組み合わせることにより、特定のアプリケーションに対して QoS を付与したり、拒否することが可能となります。必要によって設定を行ってください。

①　フィルターよりグループを選択

②　左メニューよりデバイスを選択し、右上の ⚙ をクリック



③　“詳細を表示”をクリックし、サービスタブをクリック
“AppRF”から詳細なパケット検査：ですべてを選択し、“アプリケーションのモニタリング”を有効にして“設定の保存”をクリック

4.9. 工場出荷状態への戻し方

4.9.1 グループを使った AP の初期化

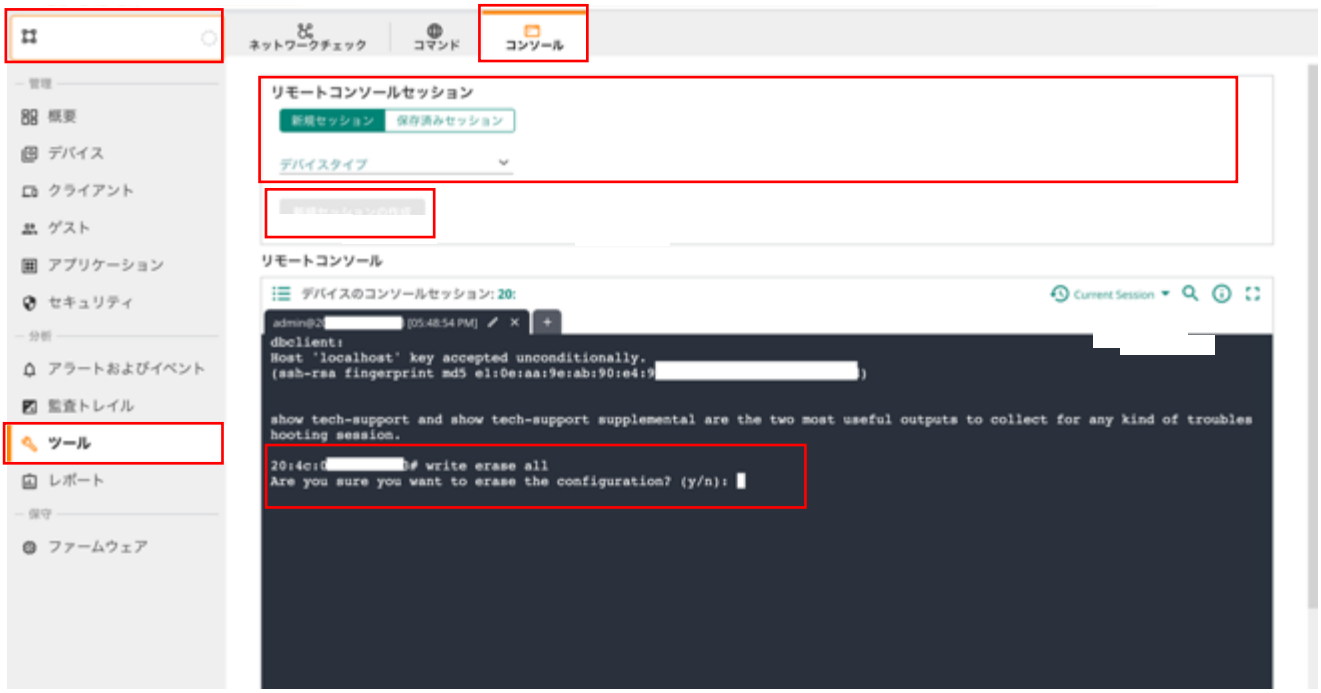
設定の入っていない新規グループを作成し、AP を作ったグループに移すことで設定の初期化をします
グループの作り方と AP の割り当てについて詳しくは Central 基本操作ガイド（入門編）を参照

https://www.hpe.com/psnow/doc/a00143744jpn

4.9.2 リモートコンソールからの初期化

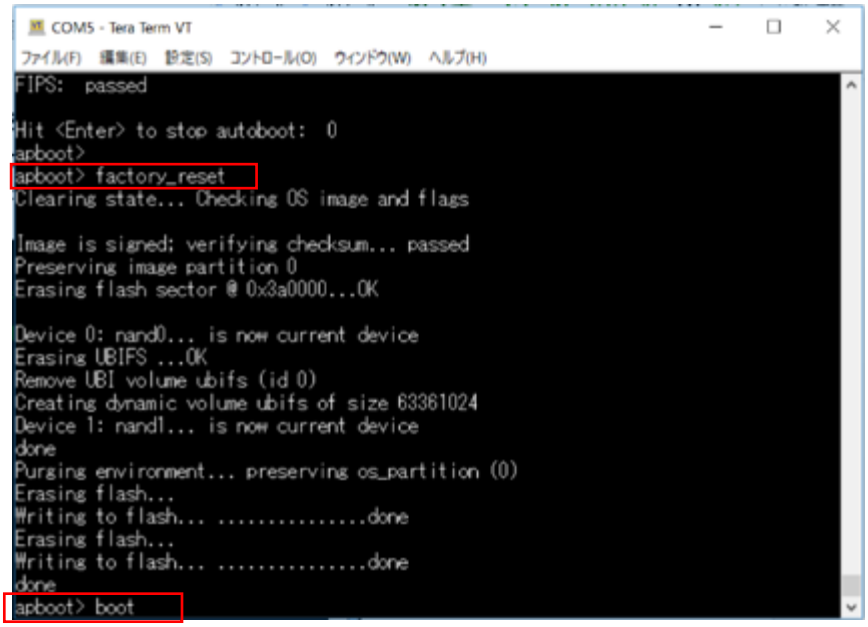
GUI から AP の CLI にリモート接続ができます

① グループを選択し、ツールメニューをクリックし、コンソールタブをクリック
② CLI を開く AP を選択し、ユーザ名・パスワードを入力して“新規セッションの作成”をクリック
③ CLI が起動したらログイン後 write erase all を実行し初期化する



4.9.3 CLI からの初期化

Instant AP の電源の OFF/ON を行います。Boot 途中で ”Hit <Enter> to stop autoboot:” が表示されますので、このメッセージが出たら Enter を押し Boot を停止させます。プロンプトが ”apboot>”になった後、”factory_reset” コマンドを入れます。コンフィグの初期化が終わると ”apboot>” が表示されますので、”boot”と入れ再起動をすると初期化されます。



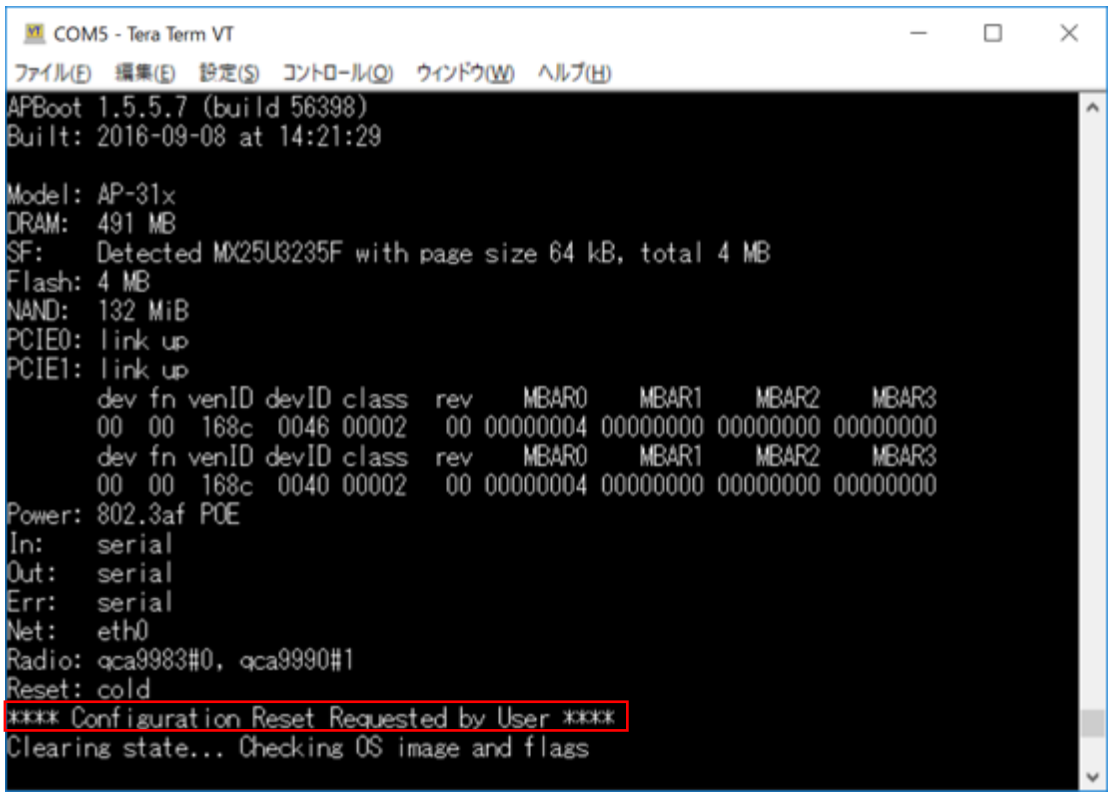
4.9.4　リセットボタンからの初期化

全ての Instant AP にはリセットボタンがついています。

リセットボタンを押しながら電源投入し、約 5 秒後リセットボタンをはなすことで初期化を行うことができます。

IAP-315 リセットボタン位置

AP-345 リセットボタン位置



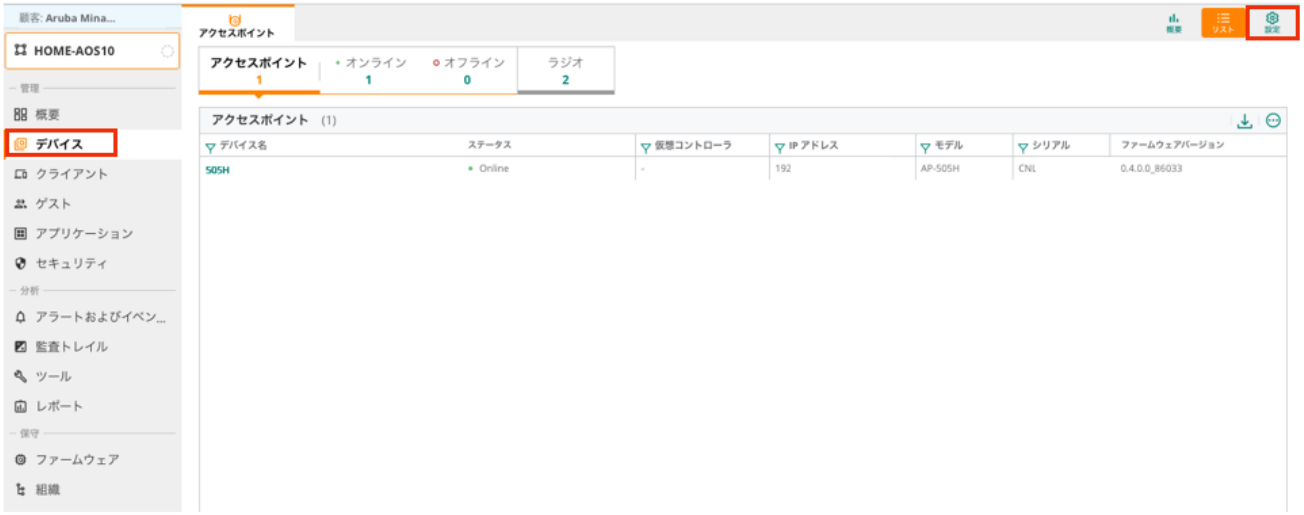
コンソールケーブルで確認している場合には、” **** Configuration Reset Requested by User **** ”のメッセージが出るまで、リセットボタンを押し続けてください。

5　有線ポート設定

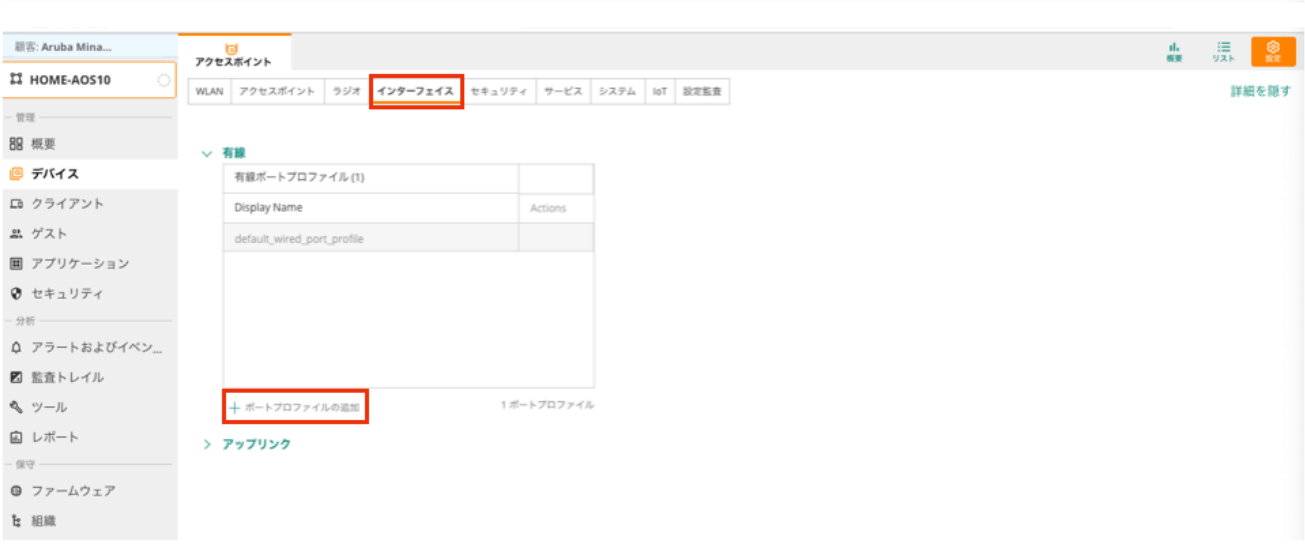
有線 Port は設定をしなければ利用することができません。本設定では有線ポートを L2SW として利用する方法を紹介します。

①　フィルターよりグループを選択

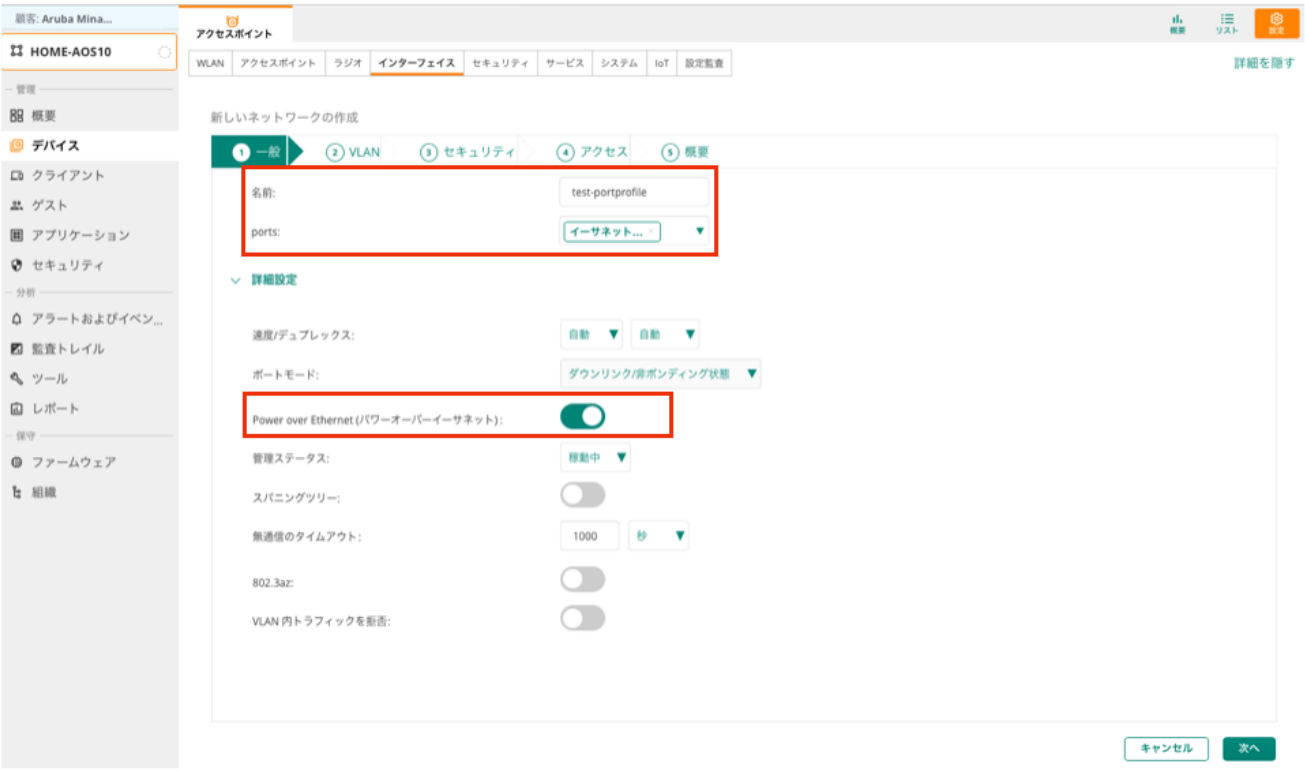
②　左メニューよりデバイスを選択し、右上の ⚙ をクリック



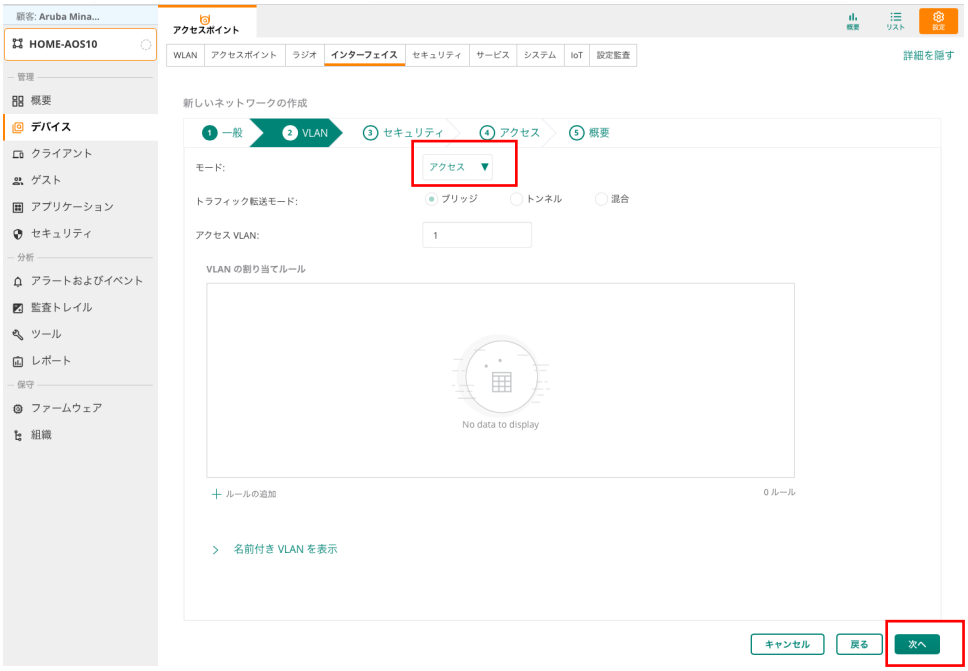
③　“詳細を表示”をクリックし、インターフェイスタブをクリック
“＋ポートプロファイルの追加”から新規ポートプロファイルを作成



④　名前は任意のものを設定し、当インターフェイスプロファイルを割り当てるポートを選択
＊PoE 給電を行うことが可能な有線ポートを持つ AP もあるので、必要によって詳細設定を開き、PoE を”有効”と設定します。IP Phone や IP Camera に給電を行うことができます
“次へ”をクリック



⑤　モードをアクセスにし、“次へ”をクリック



⑥　Trusted ポートを有効にします。Trusted ポートを無効にすると、MAC 認証、802.1x 認証を有効にすることができる“次へ”をクリック

⑦　Trusted ポートを有効としたため、アクセスルールは制限なしになる
“次へ”をクリック

⑧　概要を確認し、間違いがなければ“終了”をクリック

6　SSID の設定

6.1 SSID の作成手順

基本的な SSID の作成フロー

①　フィルターアイコンより SSID を作成するグループを選択

②　左メニューより“デバイス”を選択し、右上の　ボタンをクリック
③　アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成

④　名前（SSID）を指定し、“次へ”をクリック

⑤　トラフィック転送モードとクライアント VLAN の割り当て設定をする

トラフィック転送モード

”ブリッジ”→AP はブリッジとして動作を行い、トラフィックは接続先スイッチに転送されます。ネイティブ VLAN もしくは、接続先スイッチに設定された VLAN を指定します。

”トンネル”→トラフィックはトンネル経由でゲートウェイに転送されます。ゲートウェイに設定された VLAN を指定します。（GRE トンネルによる L2 延伸）

”混合”→ルールに基づいてフォワーディング・モード（Bridge もしくは Tunnel）と VLAN をクライアントに割り当てます。ルールには MAC アドレスやユーザー名等を指定可能です。

クライアント VLAN の割り当て

“ネイティブ VLAN” → VLAN との紐付けをせず、AP が属するネットワークに出力されます。

“スタティック” → 指定をした VLAN と紐付けます。有線側には指定した VLAN Tag がついて出力されますので、AP と接続している Switch 側で Tag VLAN 設定をしてください。

“ダイナミック” → Radius Attribute を利用したり、特定文字列等をトリガーにして Dynamic VLAN を行うことができます。有線側には指定した VLAN Tag がついて出力されますので、AP と接続している Switch 側で Tag VLAN 設定をしてください。

⑥　セキュリティレベルを設定
エンタープライズ WPA(2,3) Radius 利用/パーソナル WPA(2,3)-PSK/キャプティブポータル(web 認証)/オープン(暗号化なし)の設定を行う
エンタープライズ-内蔵 Radius 利用については、この画面からでもユーザ追加を行うことができる

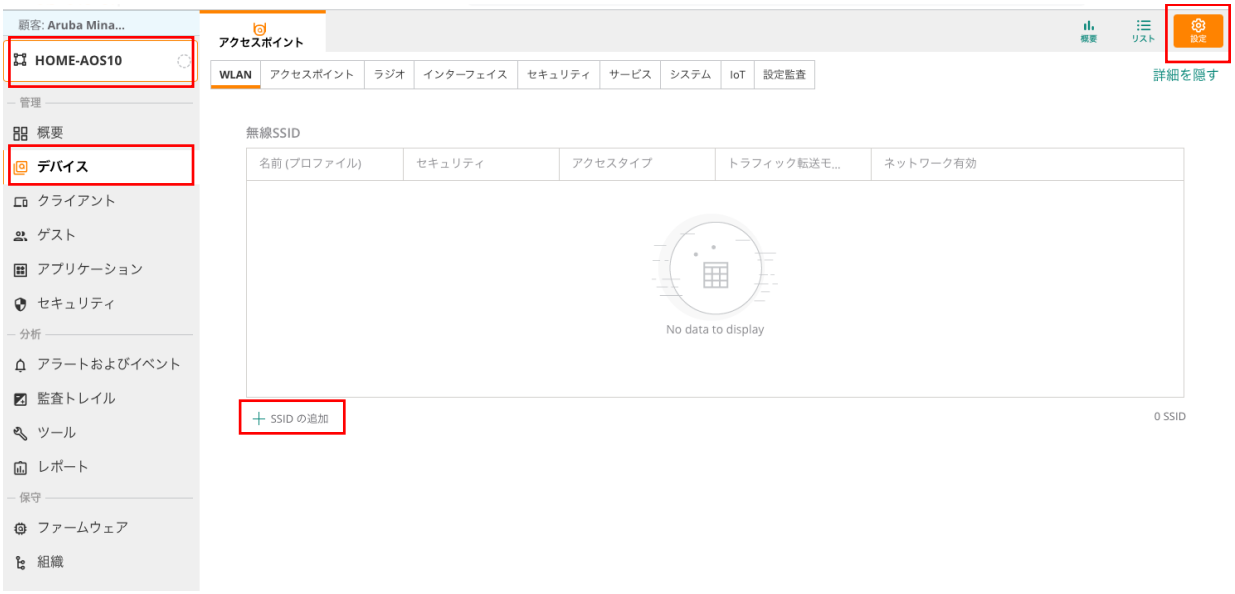
⑦　アクセスルールを設定
ロールベース/ネットワークベース/制限なし　のアクセス制御を設定する

⑧　概要で設定内容に間違いなければ“終了”ボタンをクリックすると、SSID が作成され、しばらくしてから Instant AP から SSID が出力し始める

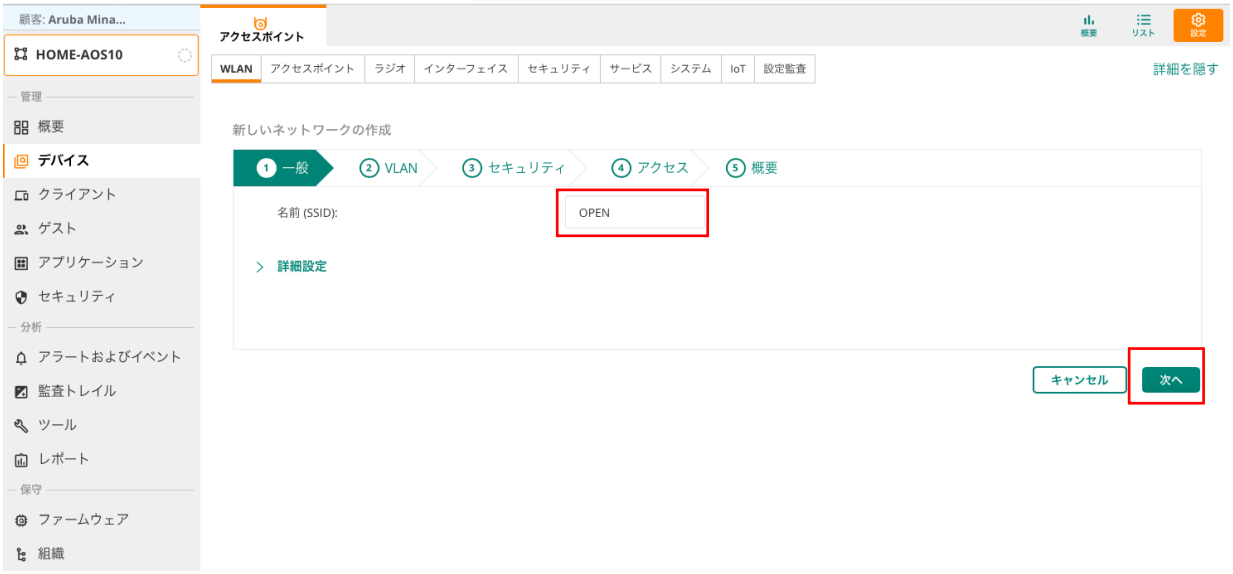
6.2 設定例）オープン認証（暗号/認証なし）

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



④ 任意の SSID を設定します。本設定では“OPEN”という SSID とし、“次へ”をクリック



⑤　SSID と VLAN との紐付けを行う
本設定ではトラフィック転送モードは“ブリッジ”、SSID=OPEN と VLAN10 を紐付けるため”スタティック” を選択し、VLAN ID に ”10 ” を入力します。
VLAN は“名前つき VLAN を表示”から新規作成可能

⑥　暗号なし設定となるため セキュリティーレベルにて”オープン”を選択

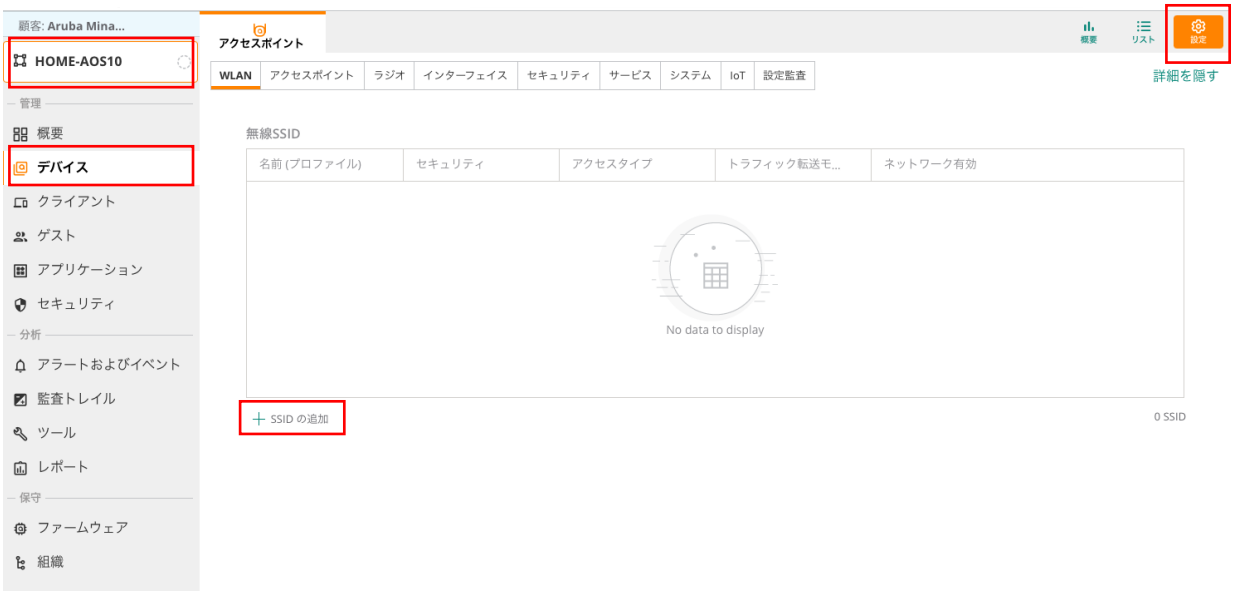
⑦　本設定では、アクセスルール制限をしないため、”制限なし”を選択

⑧　概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=OPEN が作成され、全ての Instant AP から出力される

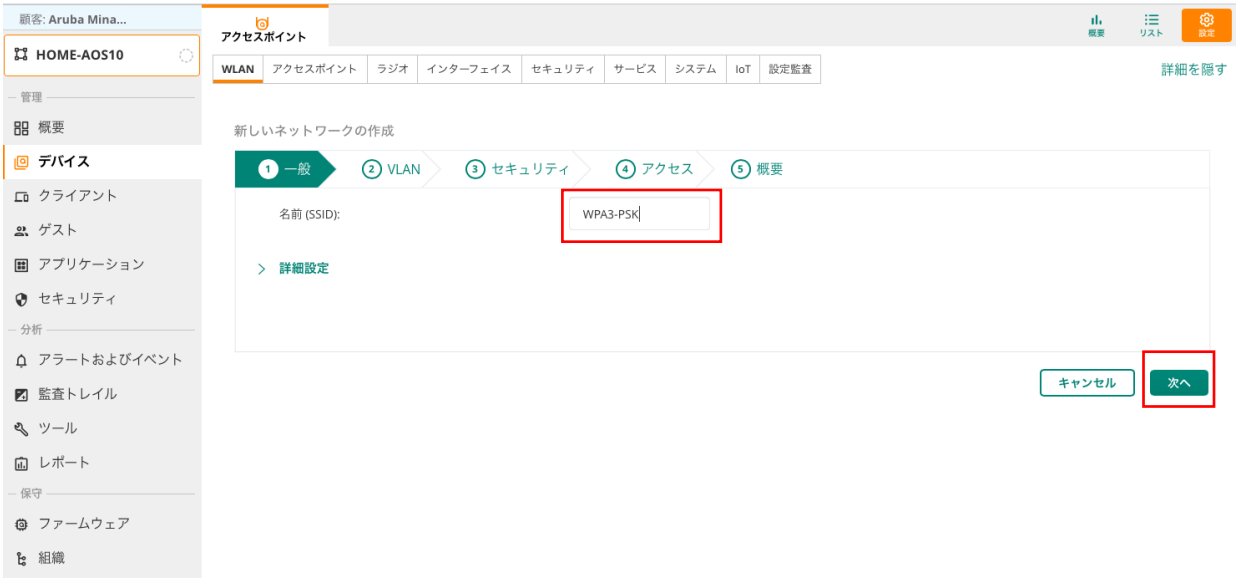
6.3 設定例）WPA3-PSK

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成

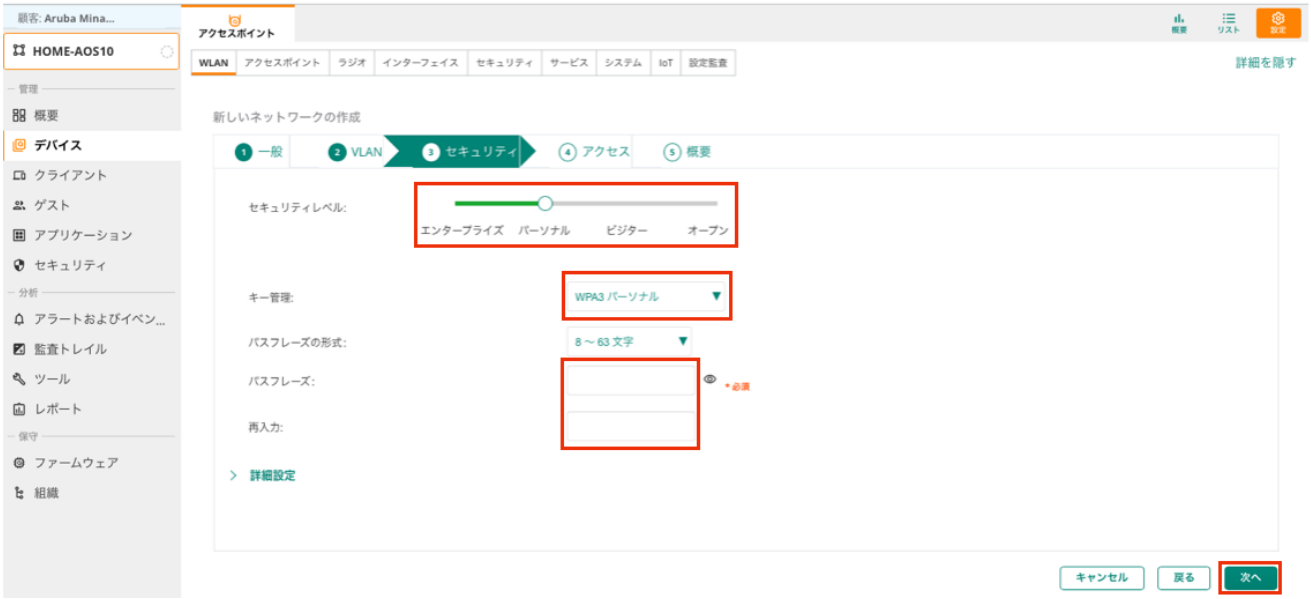


④ 任意の SSID を設定します。本設定では“WPA3-PKS”という SSID とし、“次へ”をクリック

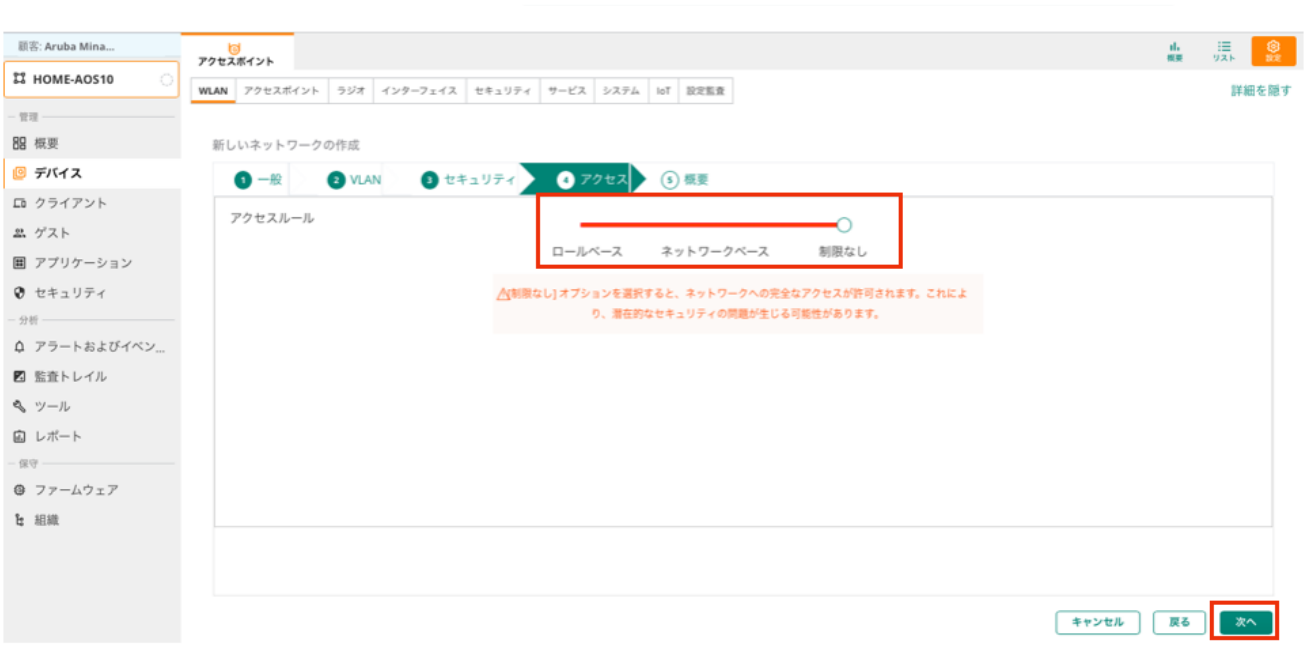


⑤　SSID と VLAN との紐付けを行う
本設定では、トラフィック転送モードを“ブリッジ”、SSID=WPA3-PSK と VLAN20 を紐付けるため”スタティック” を選択し、VLAN ID に ”20 ” を入力
VLAN は“名前つき VLAN を表示”から新規作成可能

⑥　セキュリティーレベルにおいて、”パーソナル”を選択
パスフレーズ（8 文字以上）を入力



⑦　本設定では、アクセスルール制限をしないため、”制限なし”を選択

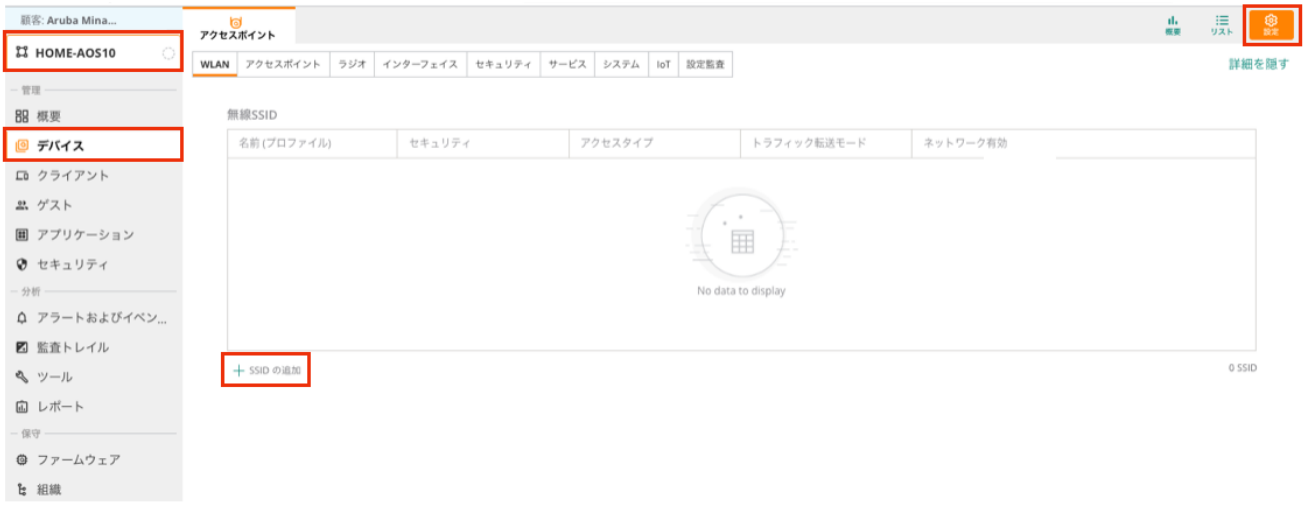


⑧　概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=WPA3-PSK が作成され、全ての Instant AP から出力される

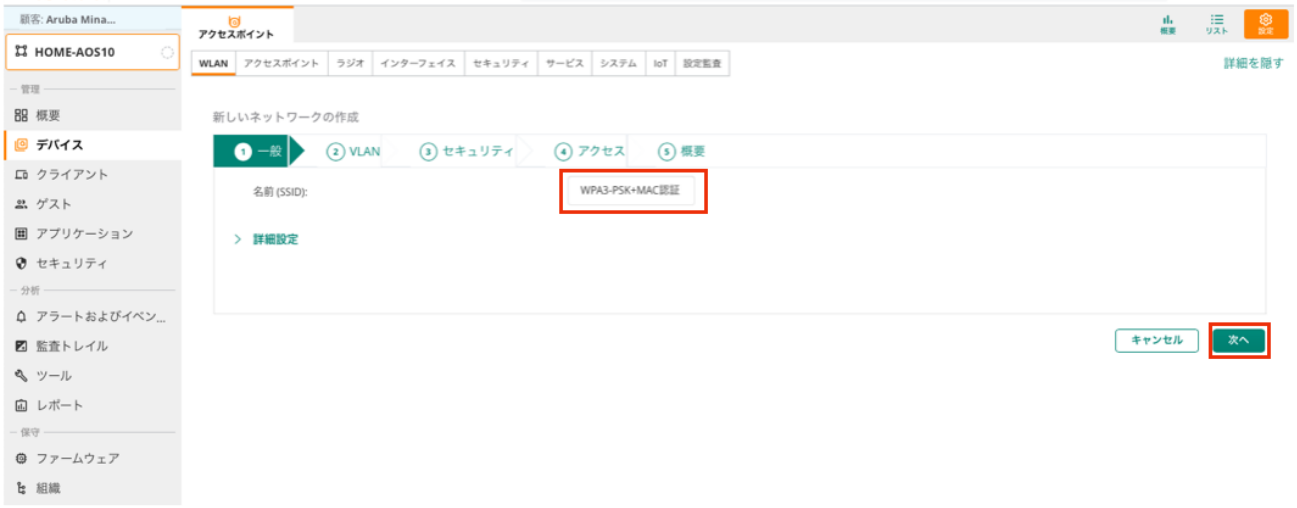
6.4 設定例）WPA3-PSK＋MAC 認証 (Cloud Auth)

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成

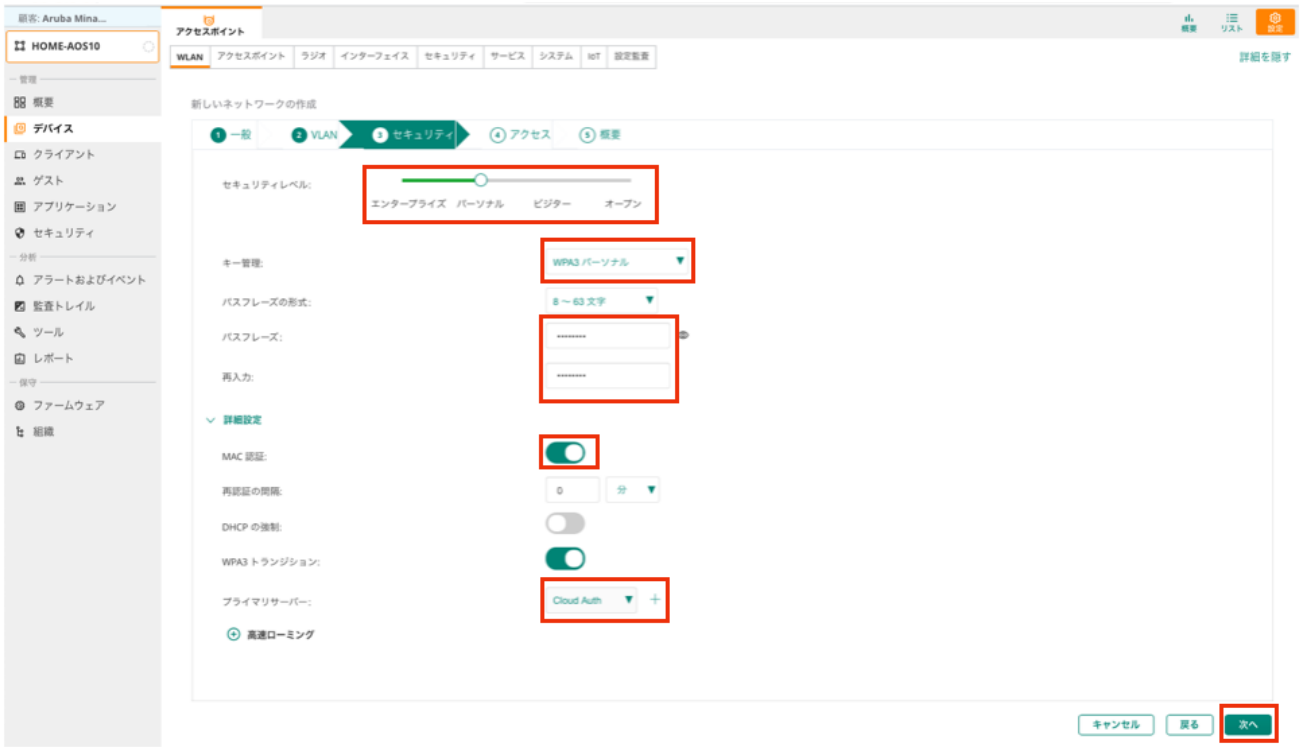


④ 任意の SSID を設定します。本設定では“WPA3-PKS＋MAC 認証”という SSID とし、“次へ”をクリック



⑤　SSID と VLAN との紐付けを行う
本設定ではトラフィック転送モードを“ブリッジ”、SSID=WPA3-PSK＋MAC 認証と VLAN30 を紐付けるため”スタティック” を選択し、
VLAN ID に ”30 ” を入力
VLAN は“名前つき VLAN を表示”から新規作成可能

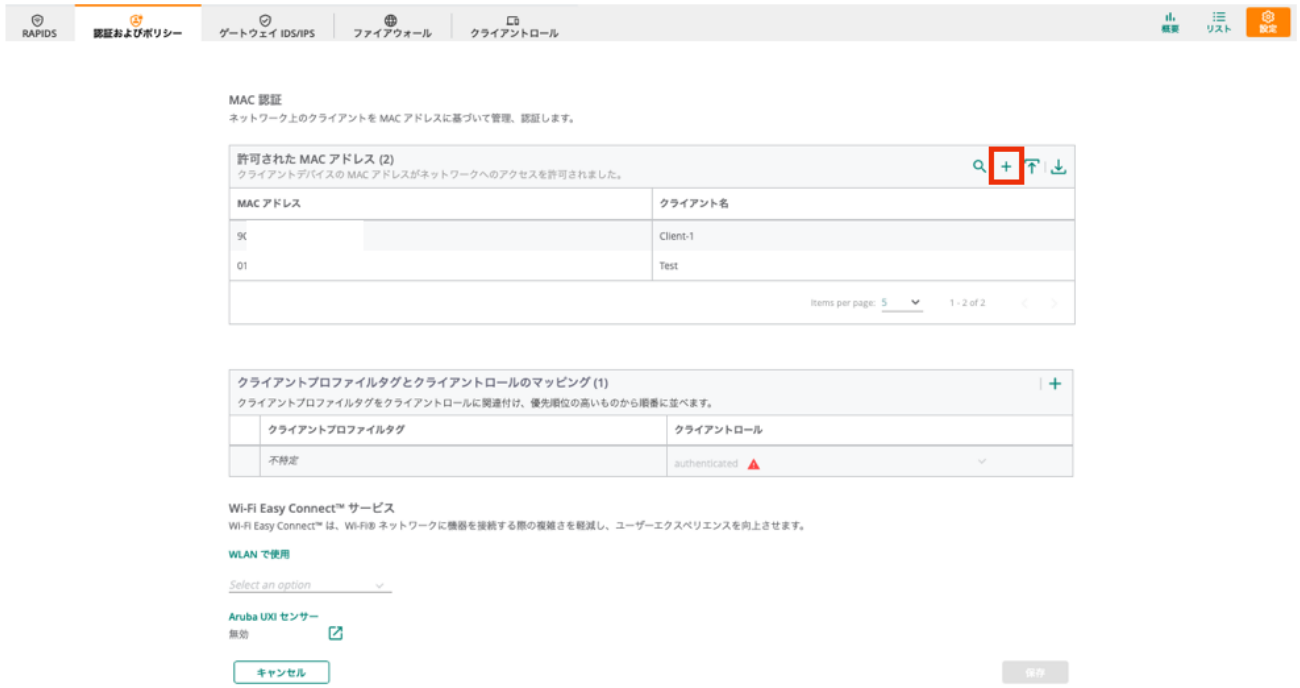
⑥　セキュリティーレベルにおいて、”パーソナル”を選択
パスフレーズ（8 文字以上）を入力
PSK を入力した後、詳細設定を開き MAC 認証を”有効”
MAC 認証を有効にすると、認証サーバ項目が表示されるようになる
今回は“Cloud Auth”を選択　Cloud Auth の概要についてはこちらをご参照ください。
右の+ボタンから新規認証サーバを登録可能



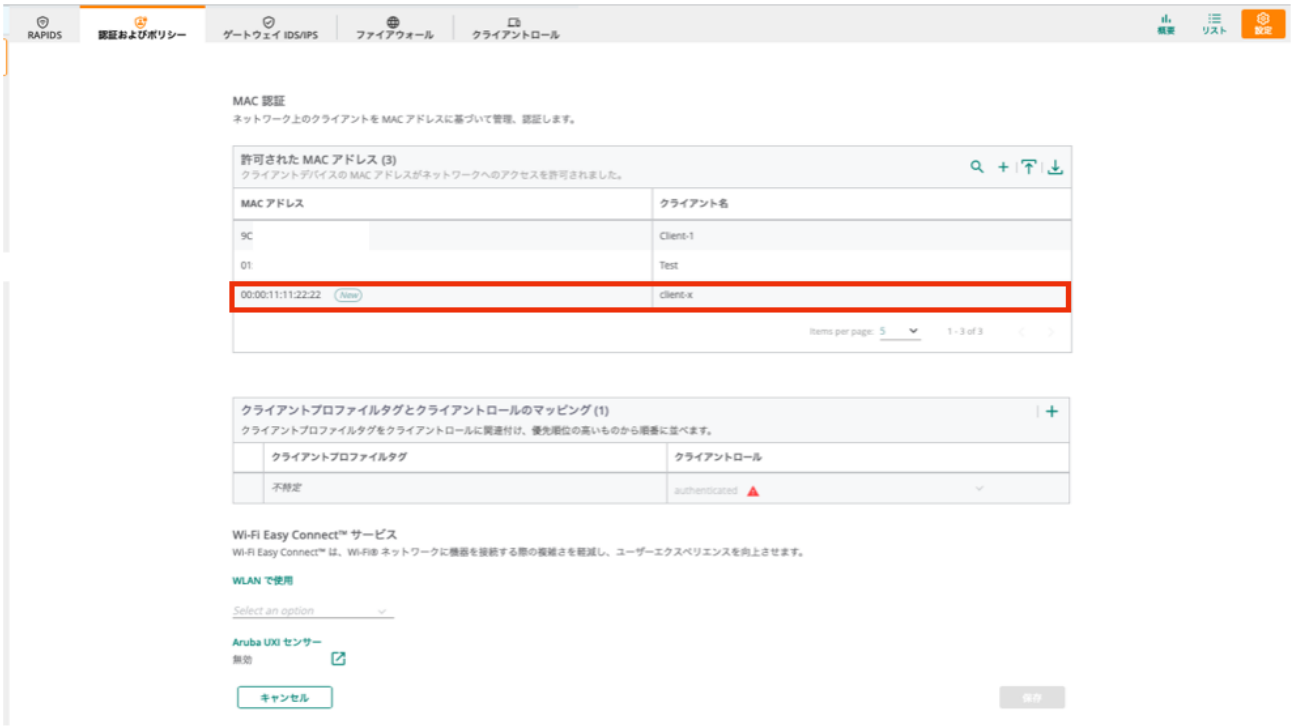
⑦　本設定では、アクセスルール制限をしないため、”制限なし”を選択

⑧　MAC アドレスの登録
HPE Aruba Networking Central 側に MAC アドレスを登録します。
“グローバル”レベルの階層から“セキュリティ”→“認証およびポリシー”を選択
“設定”をクリックして“クライアントアクセスポリシー”の編集ボタンをクリック

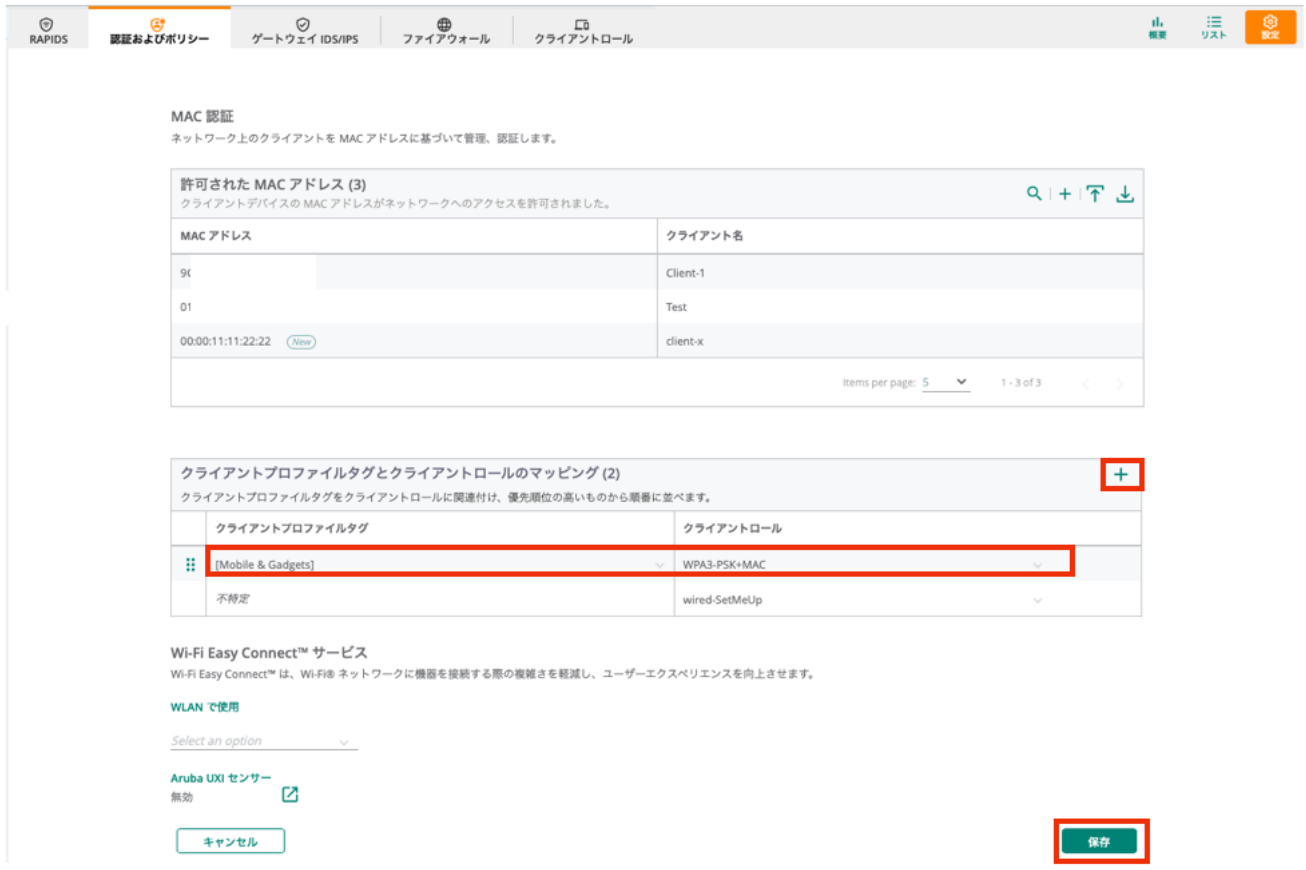
⑨　＋ボタンから MAC アドレスを登録する



MAC アドレス一覧に追加されていることを確認する



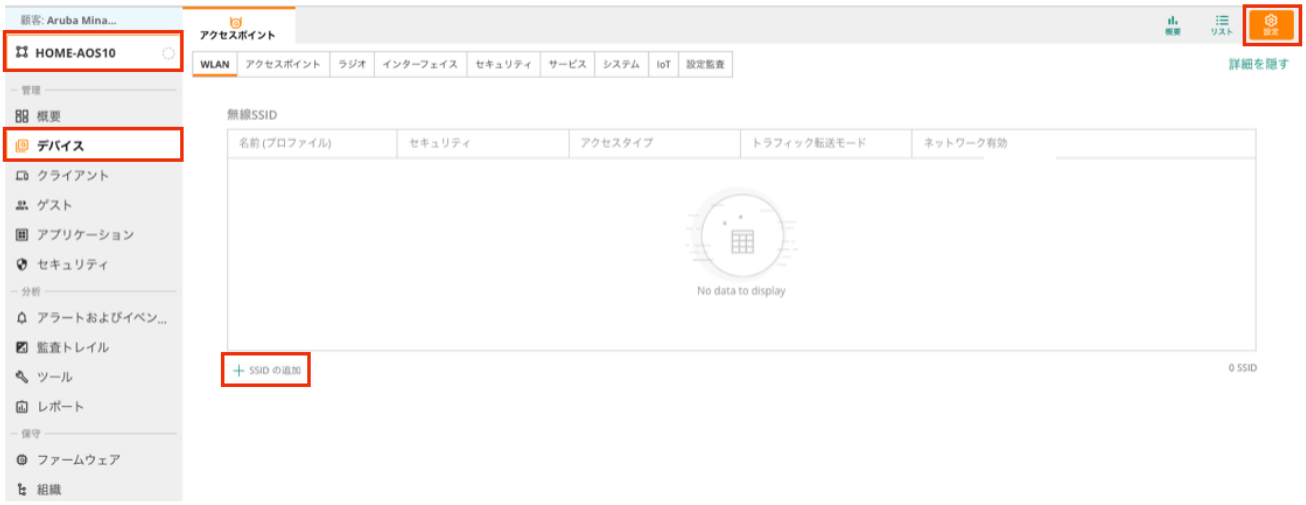
⑩　クライアントプロファイルタグのマッピング＆クライアントロールのマッピング
クライアントプロファイルタグを“Mobile & Gadgets”（スマホ・タブレット等の場合）
クライアントロールを作成した SSID と同じ名前のロールに割り当てる



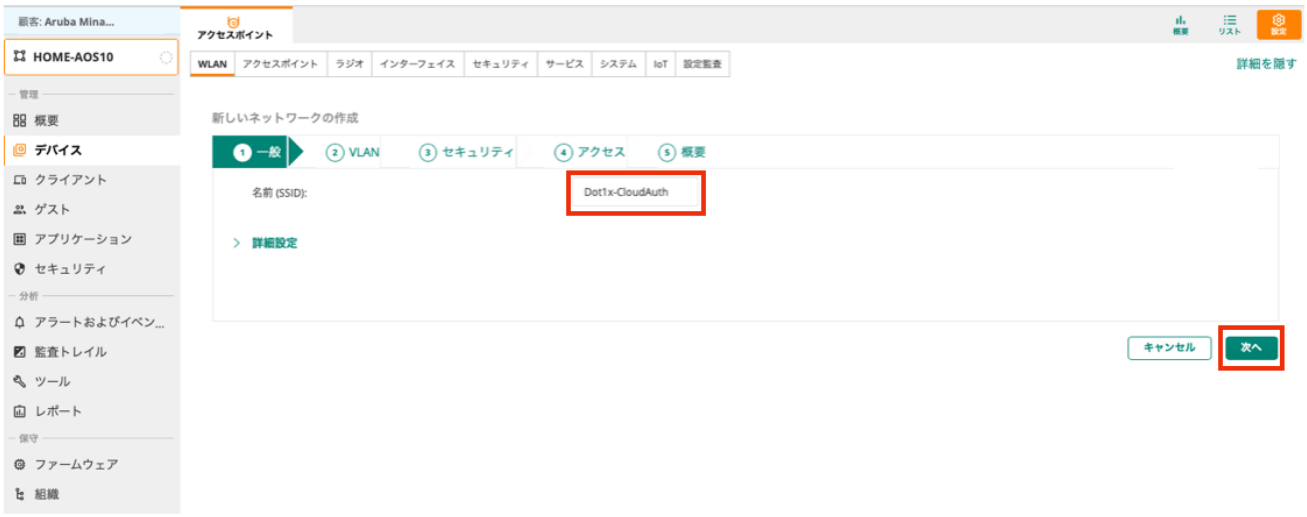
6.5 設定例）802.1x　Cloud Auth 利用

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ⚙ ボタンをクリック
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



④ 任意の SSID を設定します。本設定では“Dot1x-CloudAuth”という SSID とし、“次へ”をクリック



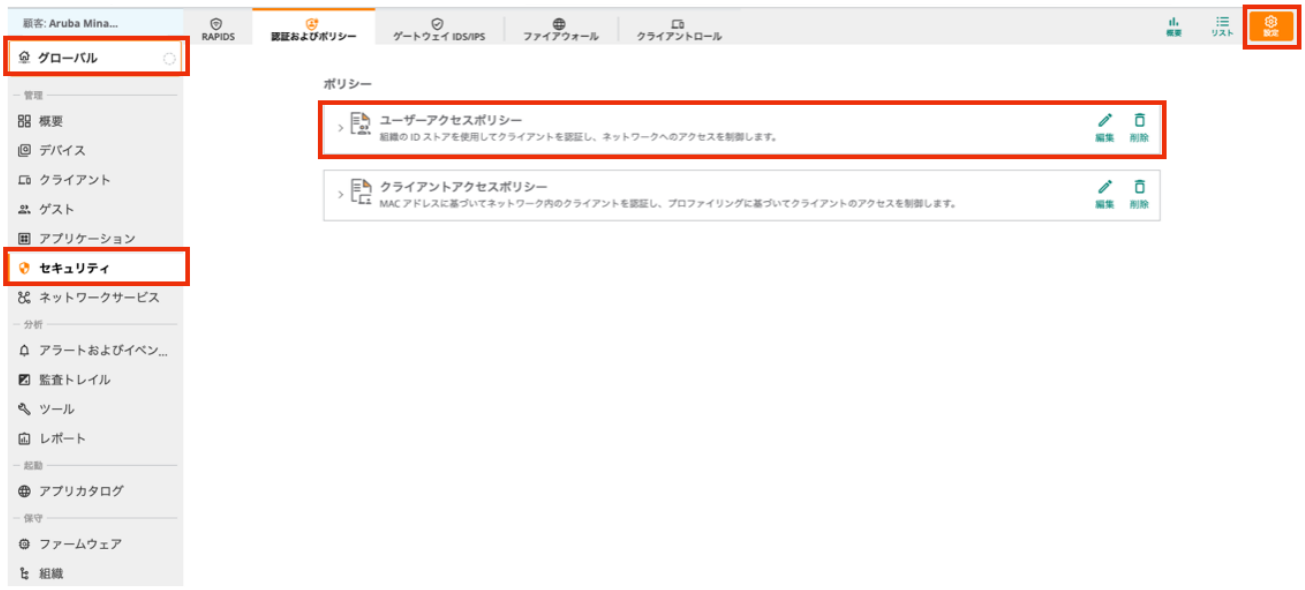
⑤　SSID と VLAN との紐付けを行う
本設定では、トラフィック転送モードを“ブリッジ”、SSID=Dot1x-CloudAuth と VLAN40 を紐付けるため”スタティック” を選択し、VLAN ID に ”40 ” を入力
VLAN は“名前つき VLAN を表示”から新規作成可能

⑥　セキュリティーレベルにおいて、”エンタープライズ”を選択
プライマリーサーバー項目で”Cloud Auth”を選択

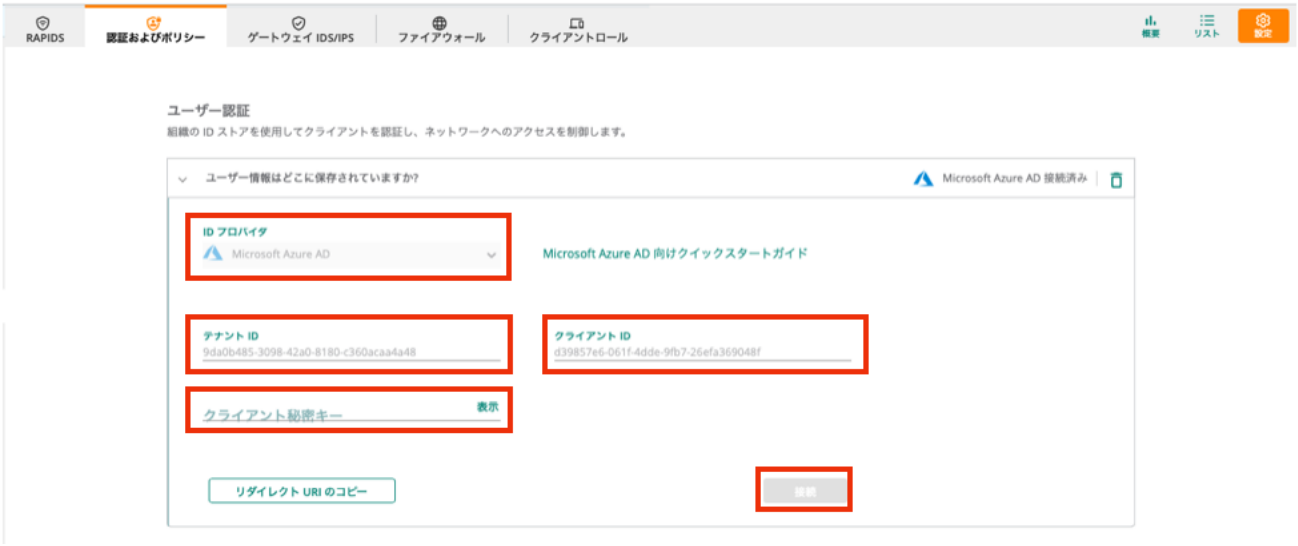
⑦　本設定では、アクセスルール制限をしないため、”制限なし”を選択

概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=Dot1x-CloudAuth が作成され、全ての AP から出力される

⑧　Cloud Auth 認証ソース指定
“グローバル”レベルの階層から“セキュリティ”→“認証およびポリシー”を選択
“ユーザーアクセスポリシー”を選択して編集ボタンをクリックする



⑨　ID ストアの設定
ID ストアを Microsoft Azure AD に指定
（Microsoft Azure AD 側の設定は本稿では割愛させて頂きます）
テナント ID・クライアント ID・クライアント秘密キーを入力
“接続”をクリックする
正常に接続されている場合“接続済み”と表示されます

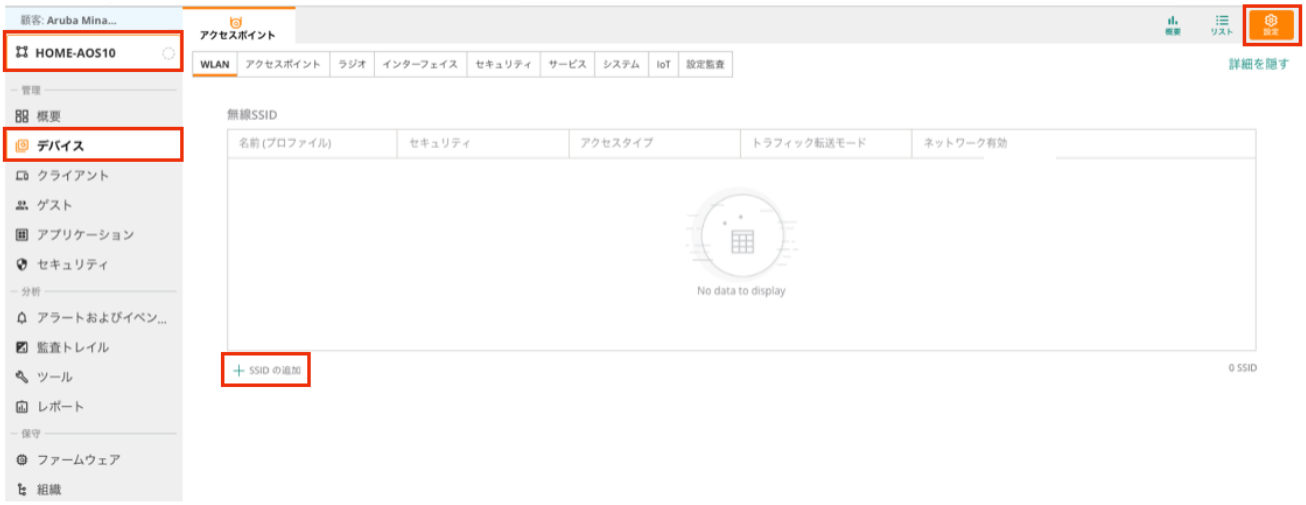


必要に応じてユーザーグループとロールのマッピングを設定します

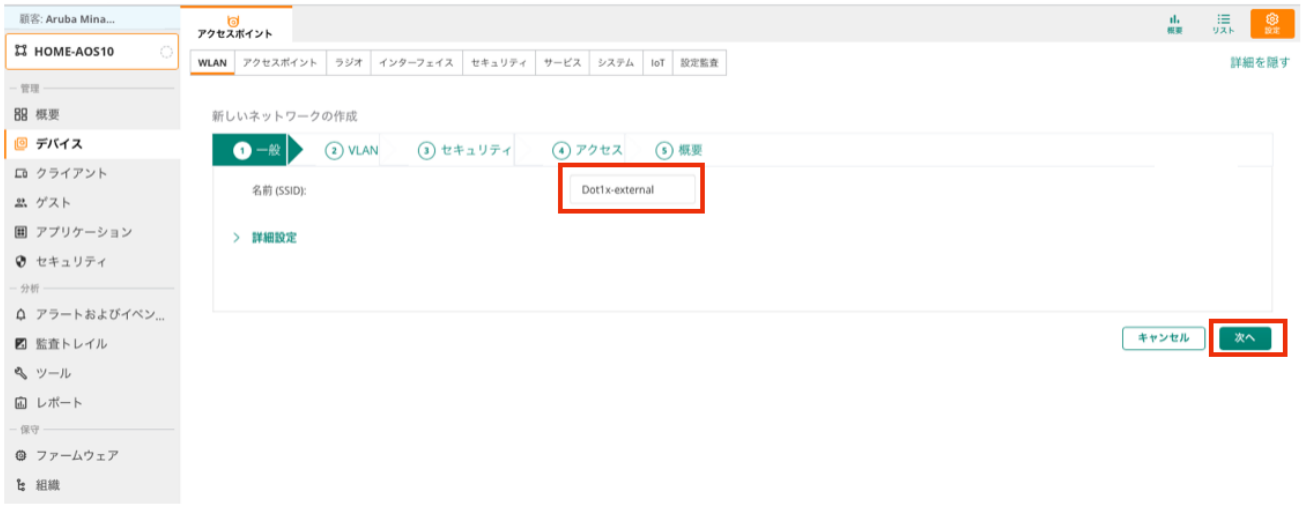
6.6 設定例）802.1x　External Radius 利用

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ⚙ ボタンをクリック
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



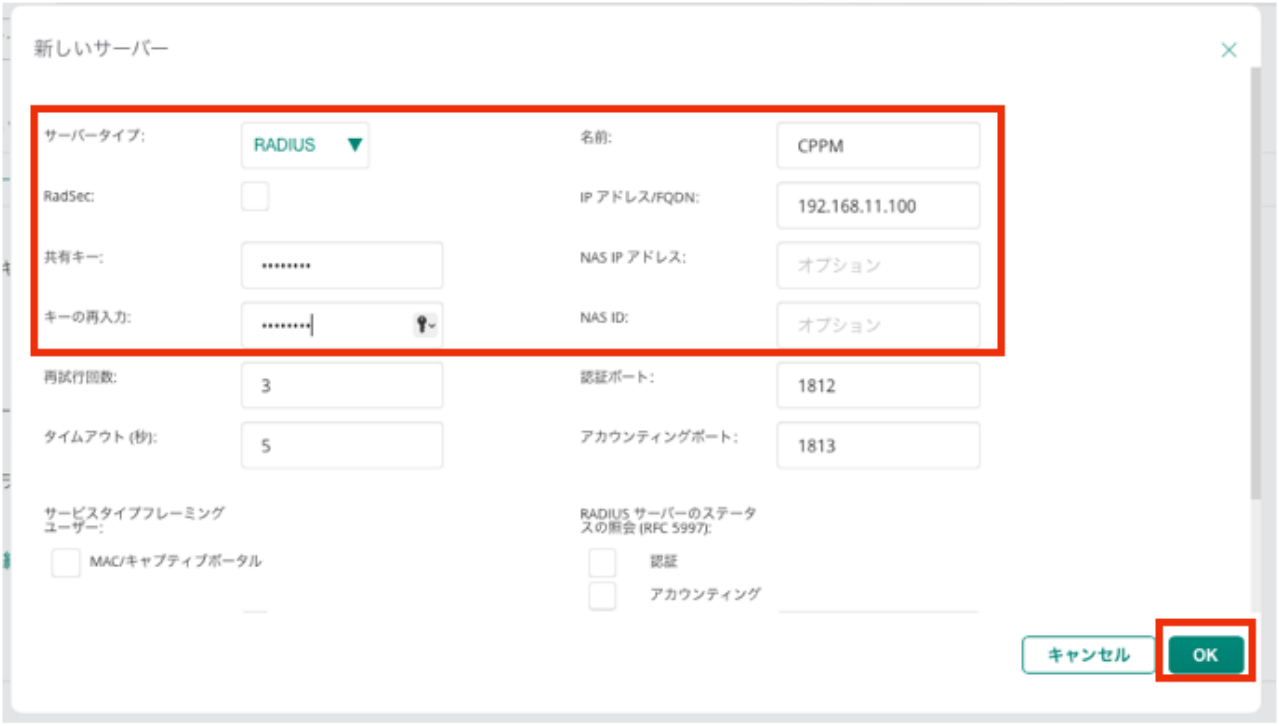
④ 任意の SSID を設定します。本設定では“Dot1x-external”という SSID とし、“次へ”をクリック



⑤　SSID と VLAN との紐付けを行う
本設定ではトラフィック転送モードを“ブリッジ”、SSID=Dot1x-external と VLAN50 を紐付けるため”スタティック” を選択し、VLAN ID に ”50 ” を入力
VLAN は“名前つき VLAN を表示”から新規作成可能

⑥　セキュリティーレベルにおいて、”エンタープライズ”を選択
プライマリーサーバー項目で“＋”から RADIUS サーバーを登録する

⑦　Radius サーバ名、IP アドレス、共有キー（シークレットキー）を入力し”OK”をクリック



=

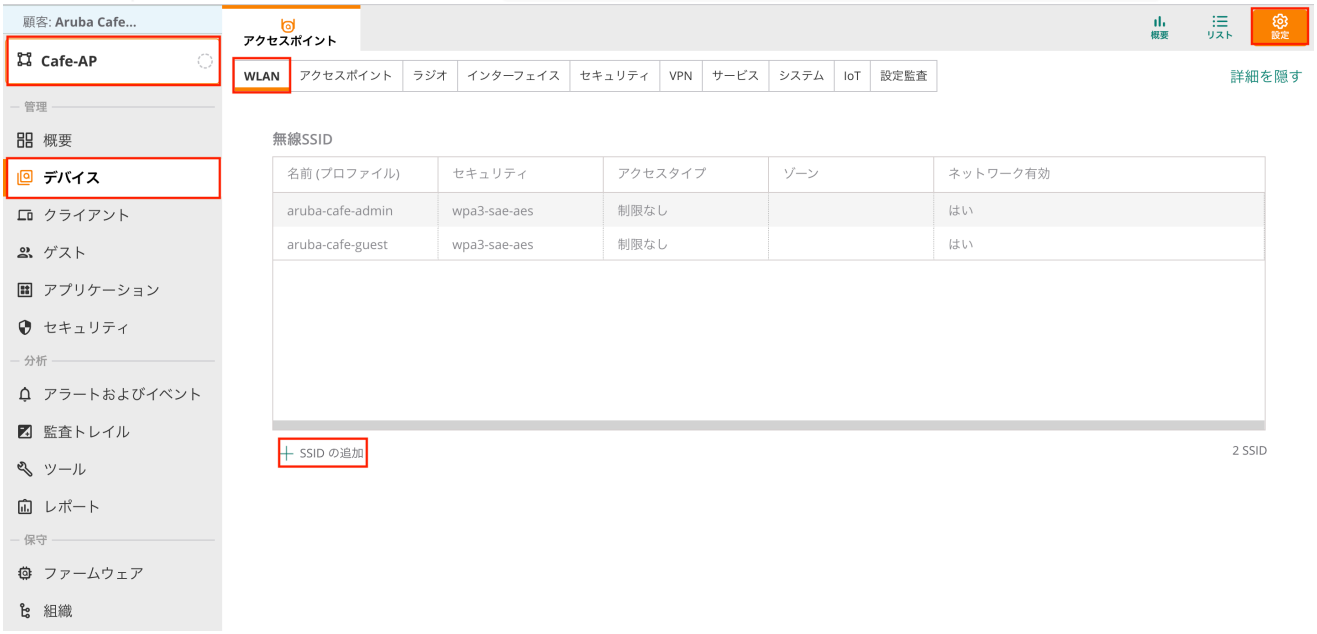
⑧　本設定では、アクセスルール制限をしないため、”制限なし”を選択

概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=Dot1x-external が作成され、全ての Instant AP から出力される

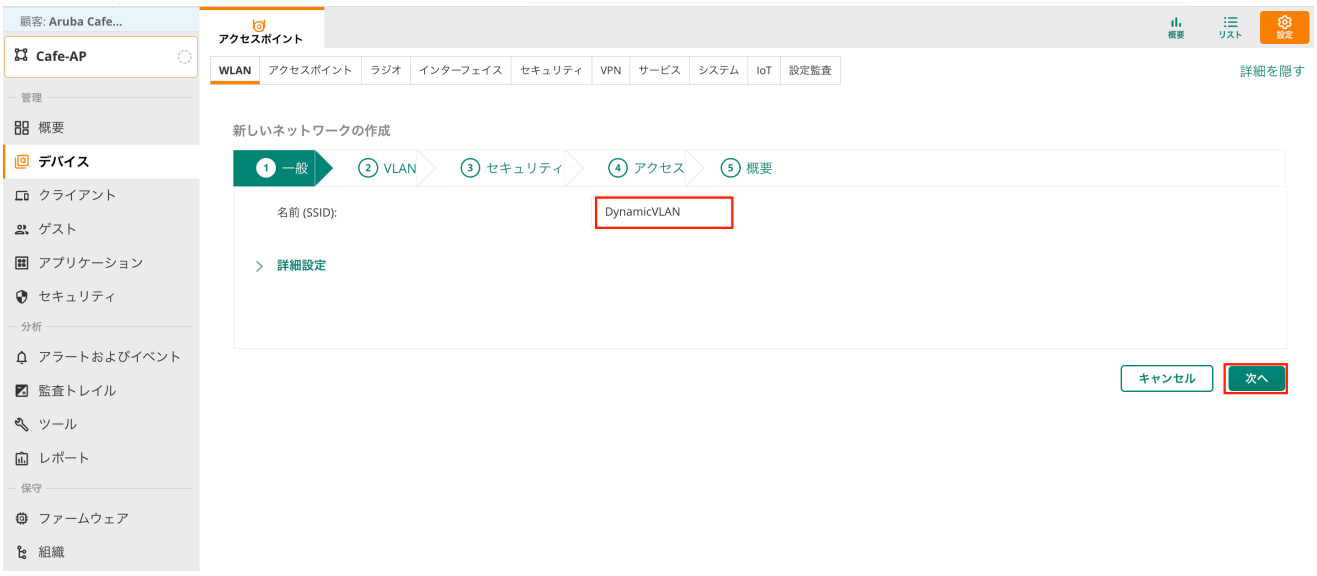
6.7 Dynamic VLAN（External Radius 利用）

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成

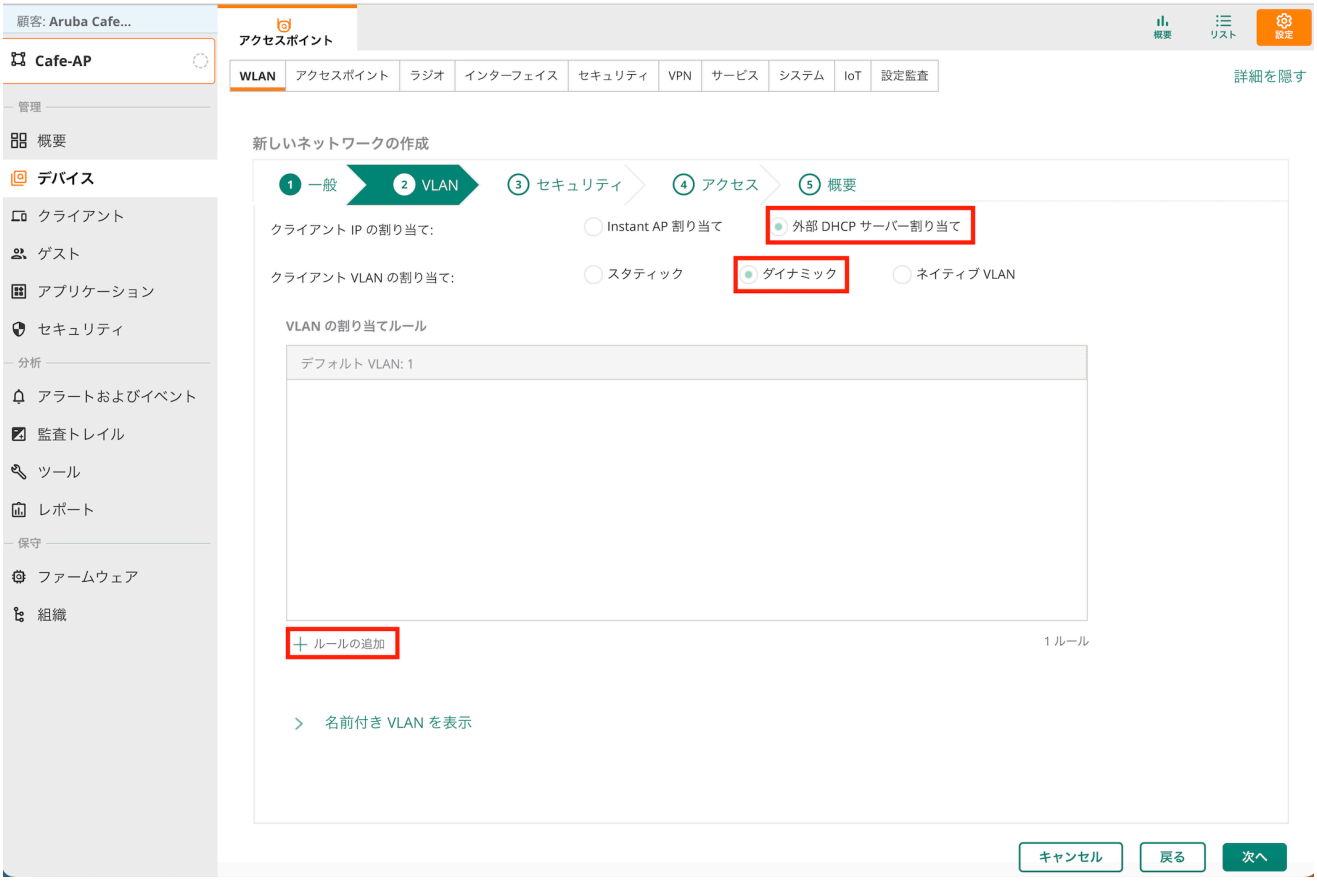


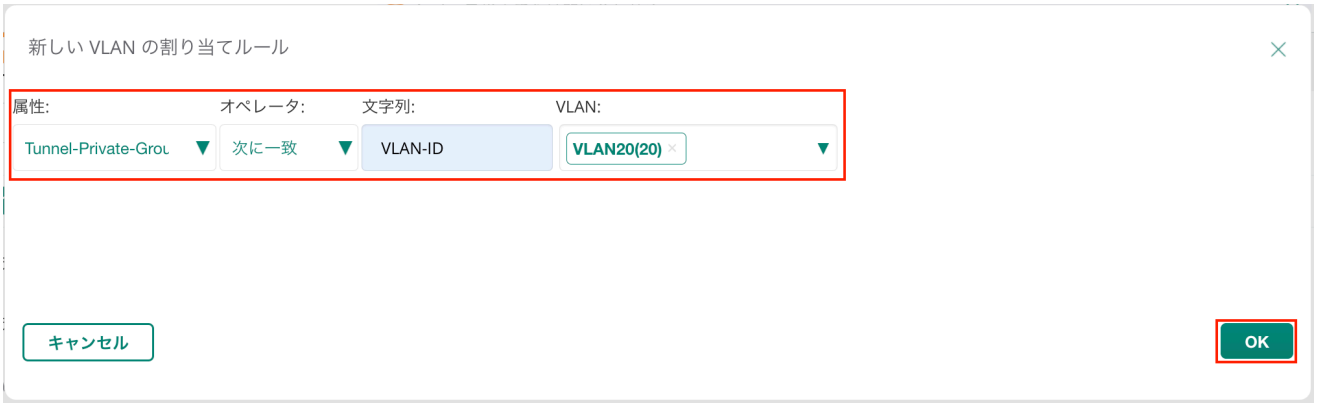
④ 任意の SSID を設定します。本設定では“DynamicVLAN”という SSID とし、“次へ”をクリック



⑤　SSID と VLAN との紐付けを行う
Dynamic VLAN となるため、SSID との紐付けは行わず、Radius サーバからの情報で VLAN をアサインできるようにする
本設定では、一般的に利用される”Tunnel Private Group Id”を利用して VLAN を振り分けられるようにする

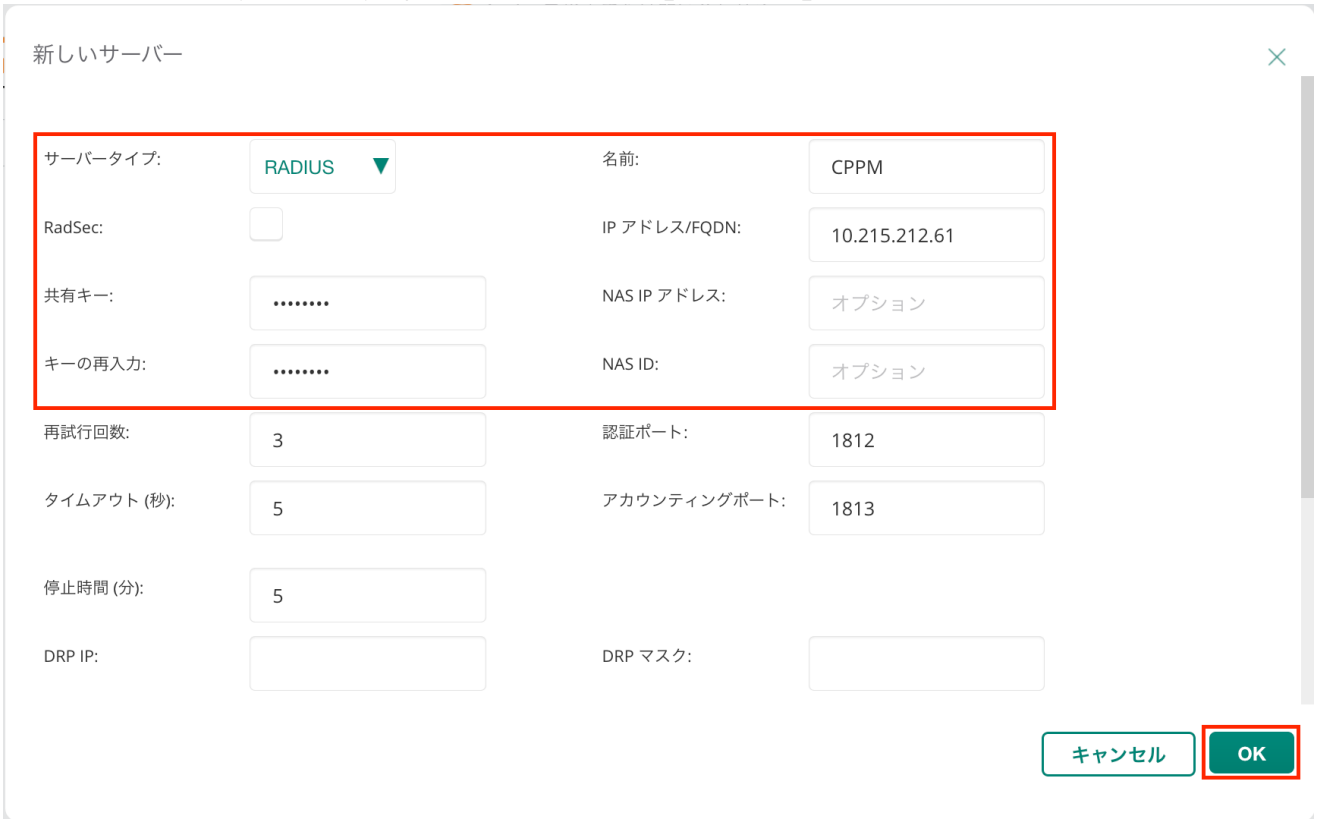
クライアント VLAN の割り当てにおいて、”ダイナミック”を選択
割り当てルール欄の”+ルールの追加”をクリ
割り当てルールにおいて　“属性” ＝ ”Tunnel-Private-Group-Id” ，”オペレータ” = ”次に一致” ，”文字列”=”VLAN-ID” , “VLAN” = ”VLAN-ID”で割り振られる VLAN を追加
デフォルトは作成したルールに合わなかった場合に付与される VLAN となる





⑥　セキュリティーレベルにおいて、”エンタープライズ”を選択

⑦　プライマリーサーバー項目で”+ボタン”をクリック
“+”をクリックすると、Radius サーバを登録可能
Radius サーバ名、IP アドレス、共有キー（シークレットキー）を入力し”OK”をクリック



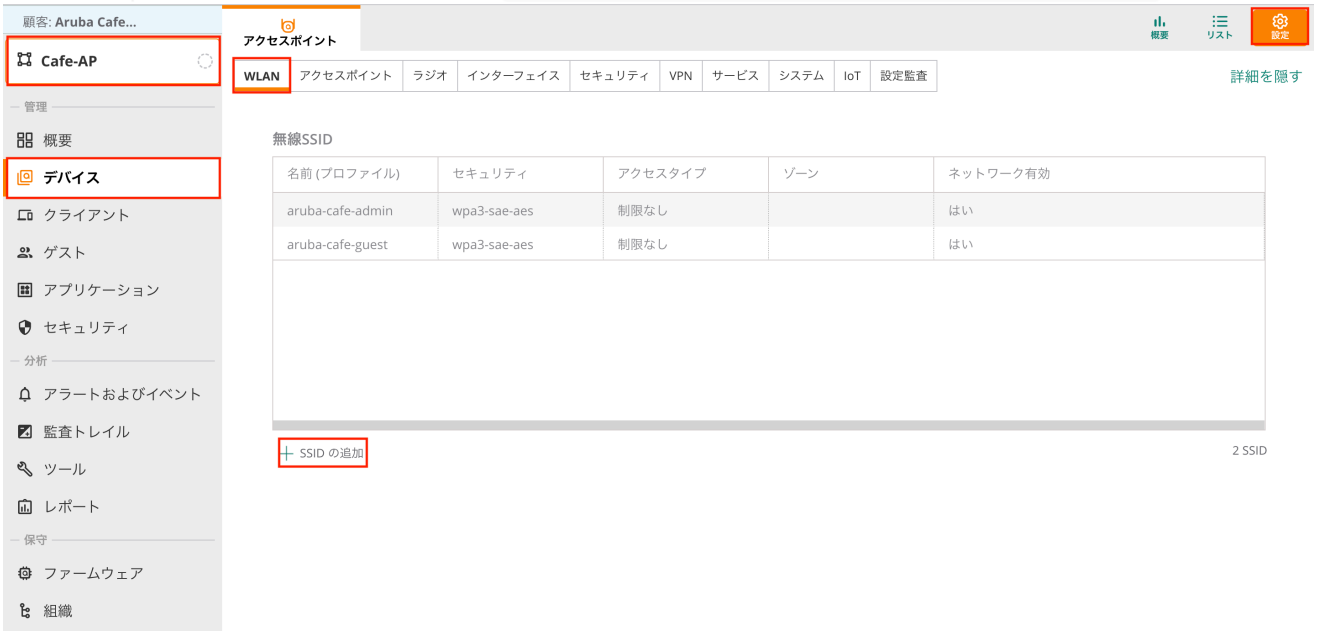
⑧　本設定では、アクセスルール制限をしないため、”制限なし”を選択

概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=DynamicVLAN が作成され、全ての Instant AP から出力される

6.8 設定例）Web 認証　規約ページのみ

①　フィルターアイコンより SSID を作成するグループを選択

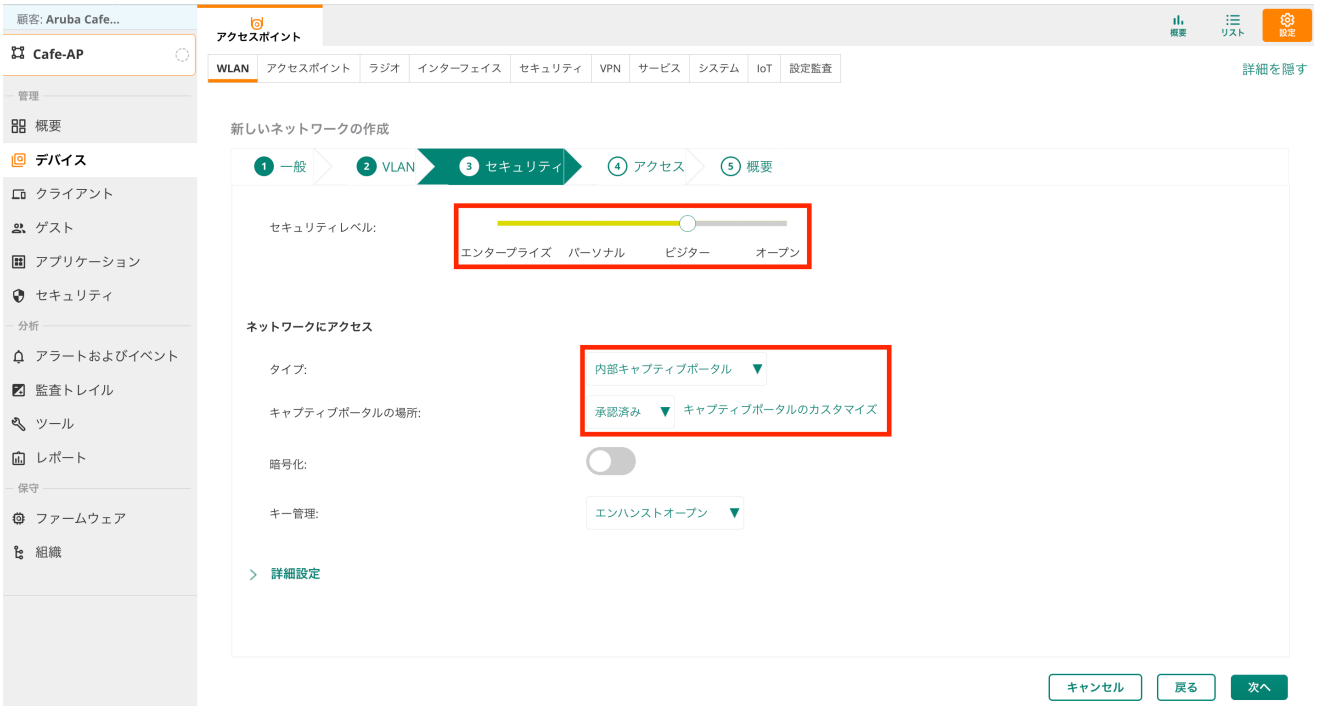
②　左メニューより“デバイス”を選択し、右上の　ボタンをクリック
③　アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



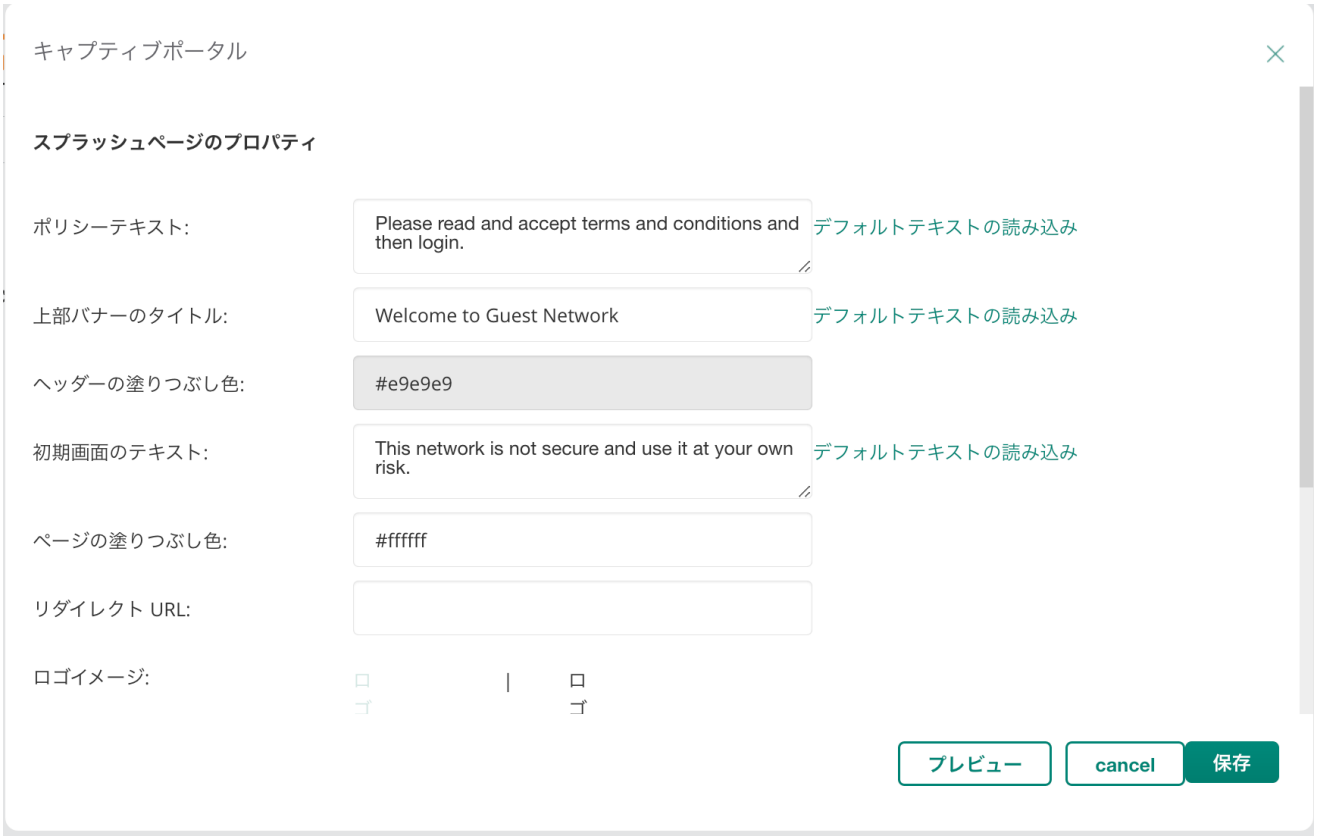
④　任意の SSID を設定します。本設定では“Webauth”という SSID とし、“次へ”をクリック

⑤　本設定では、Instant AP の DHCP サーバを利用する
クライアント IP の割り当てにて、”InstantAP 割り当て”を指定

⑥　セキュリティーレベルにおいて、”ビジター”を選択
キャプティブポータルのタイプにおいて”内蔵キャプティブポータル” “承認済み”を選択



⑦　必要によって、“キャプティブポータルのカスタマイズ”をクリックして、認証後にリダイレクトをする URL を入力する



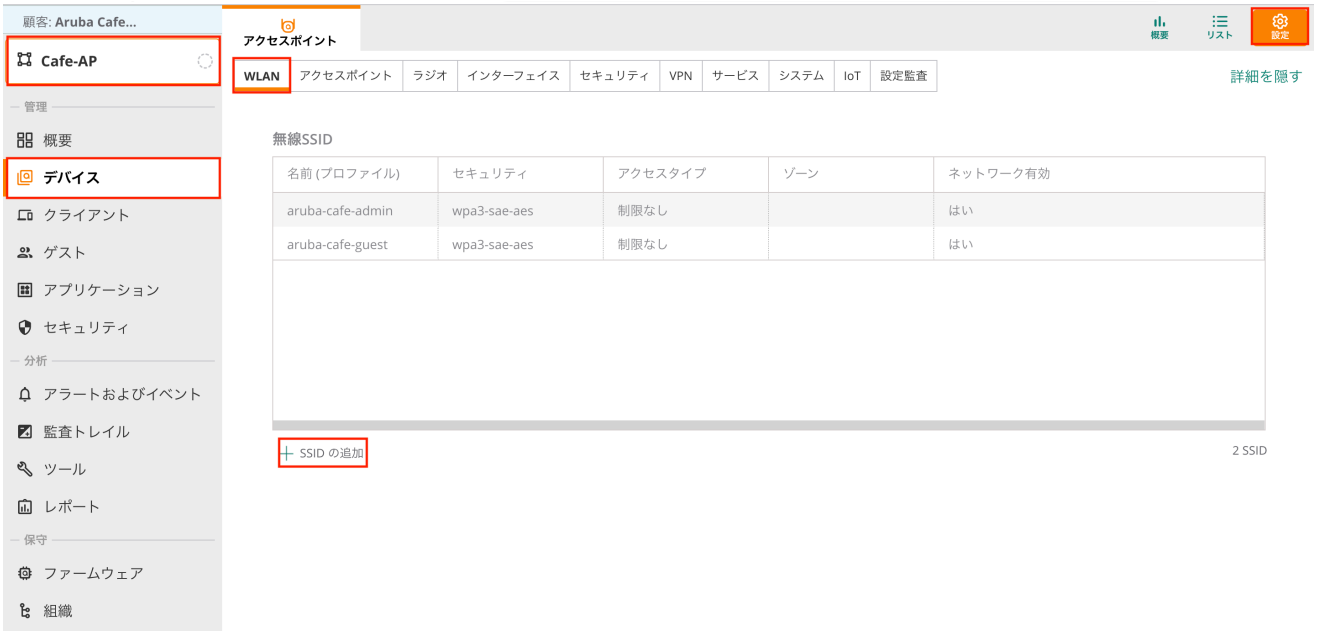
⑧　本設定では、アクセスルール制限をしないため、”制限なし”を選択

概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=Webauth が作成され、全ての Instant AP から出力される
この SSID に接続をすると、Instant AP の DHCP サーバから IP アドレスが割り当てられ、Instant AP で NAT が行われて通信を行うようになる

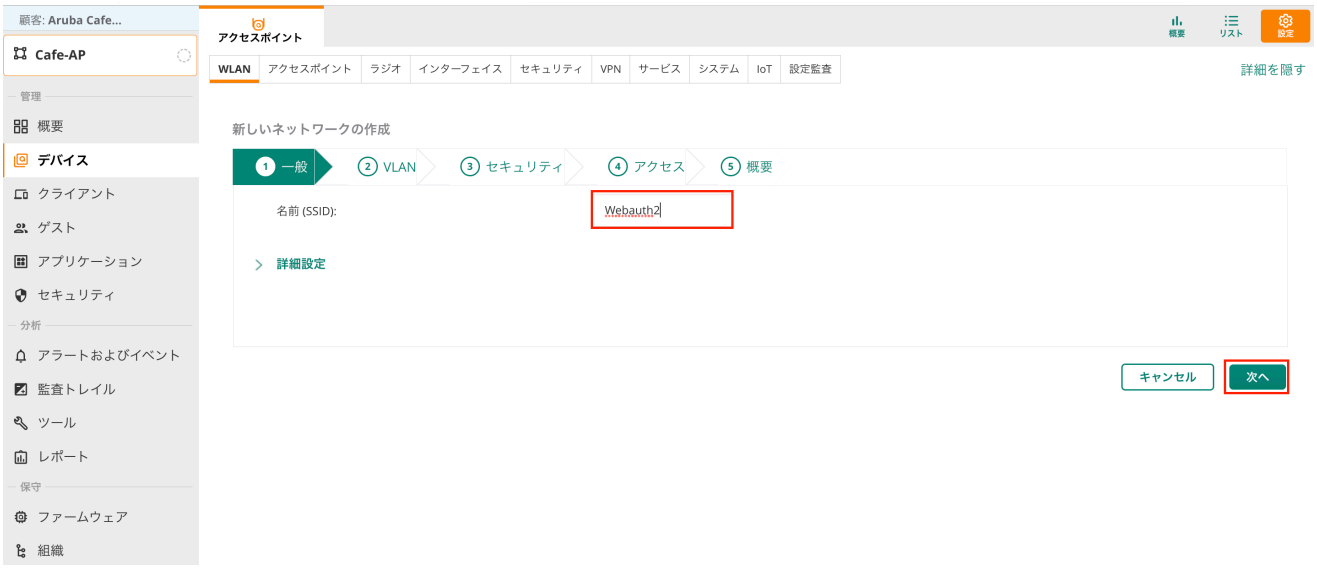
6.9 ユーザ/パスワードでのログイン

① フィルターアイコンより SSID を作成するグループを選択

② 左メニューより“デバイス”を選択し、右上の ボタンをクリック
③ アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



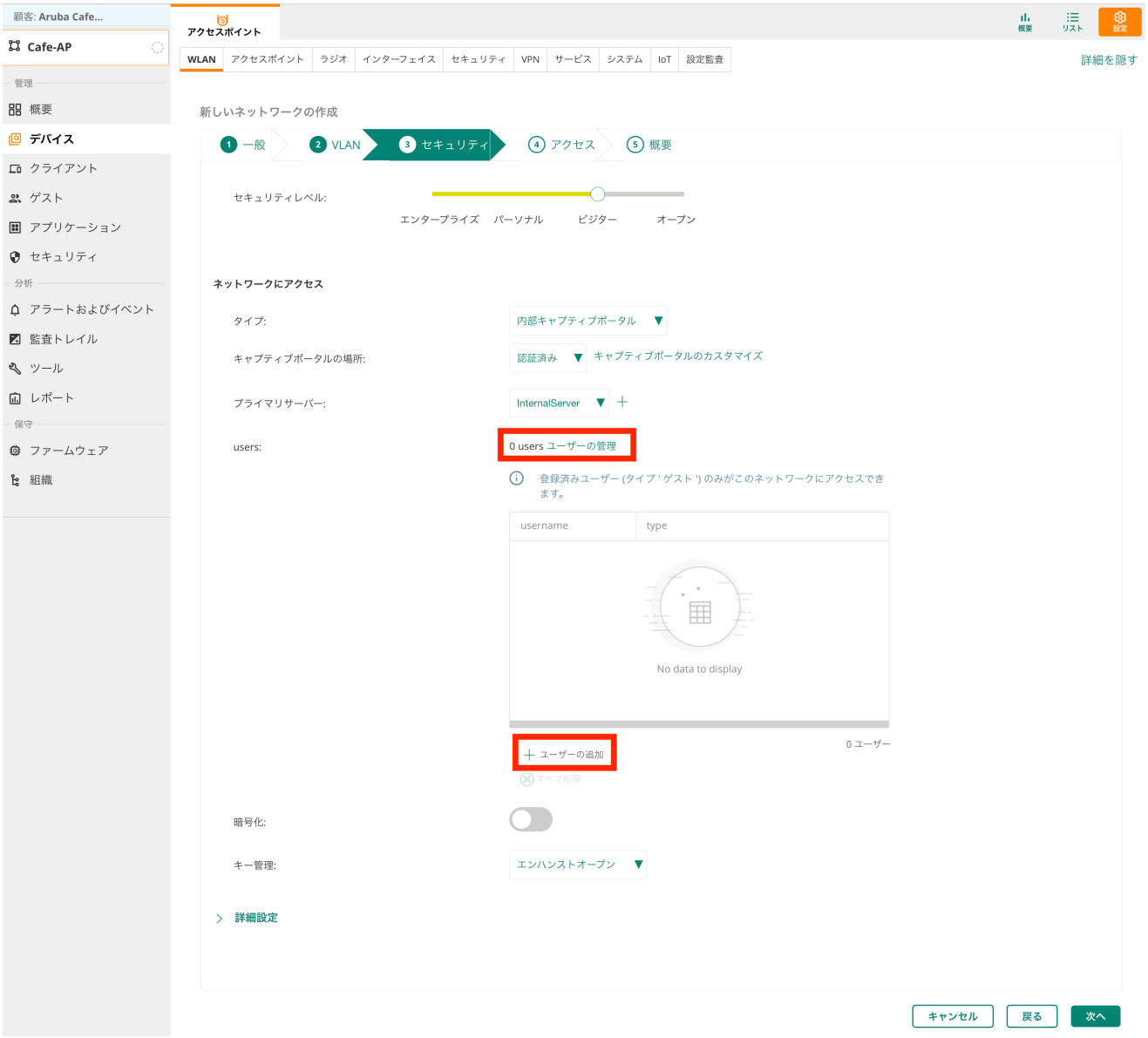
④ 任意の SSID を設定します。本設定では“Webauth2”という SSID とし、“次へ”をクリック



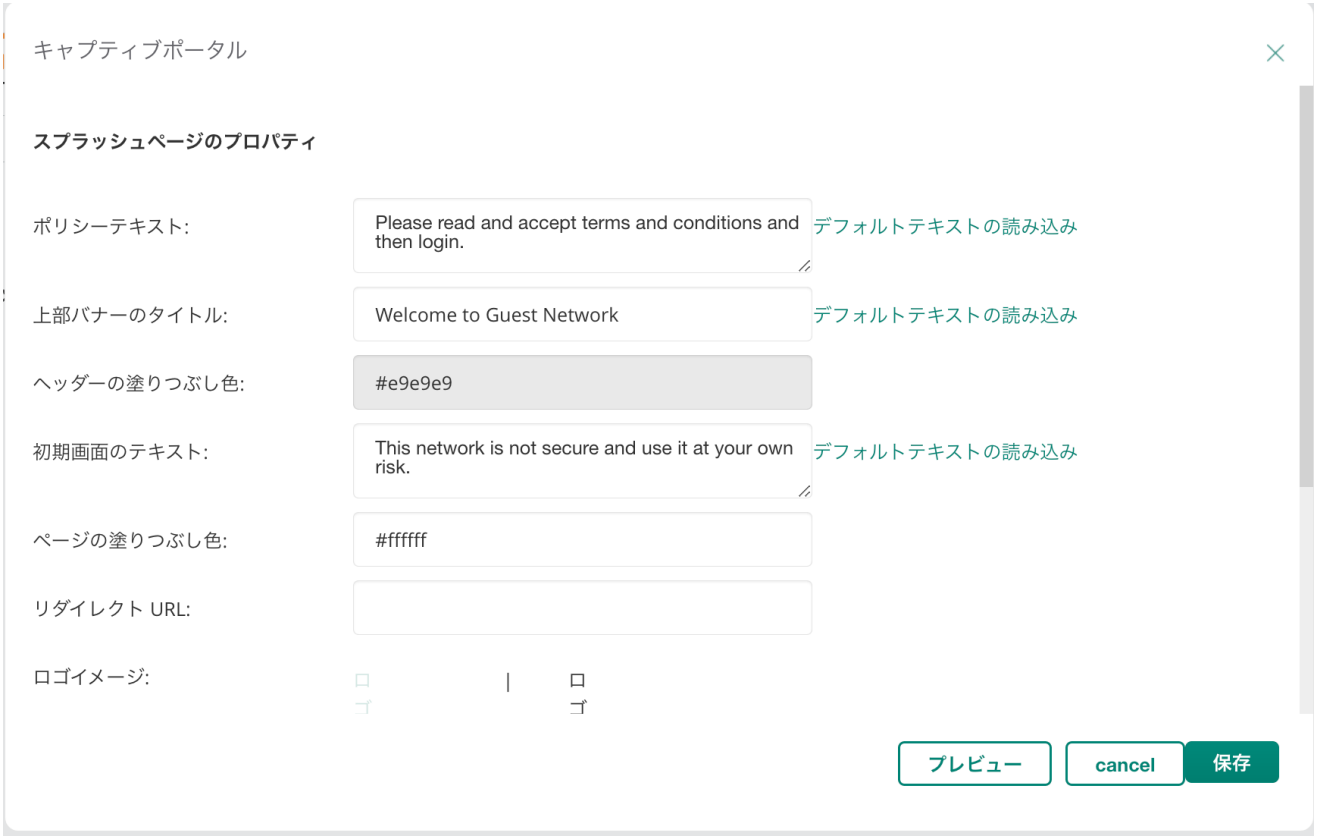
⑤　本設定では、Instant AP の DHCP サーバを利用します。クライアント IP の割り当てにて、”InstantAP 割り当て”を指定

⑥　セキュリティーレベルにおいて、”ビジター”を選択
キャプティブポータルのタイプにおいて”内蔵キャプティブポータル” “認証済み”を選択

⑦　ユーザーの管理をクリックして”+ユーザーの追加”からユーザを追加
タイプは“ゲスト”とする



⑧　必要によって、“キャプティブポータルのカスタマイズ”をクリックして、認証後にリダイレクトをする URL を入力する



⑨　本設定では、アクセスルール制限をしないため、”制限なし”を選択

概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=Webauth2 が作成され、全ての Instant AP から出力される
この SSID に接続をすると、Instant AP の DHCP サーバから IP アドレスが割り当てられ、Instant AP で NAT が行われて通信を行うようになる

6.10　Central ゲスト（メール認証）

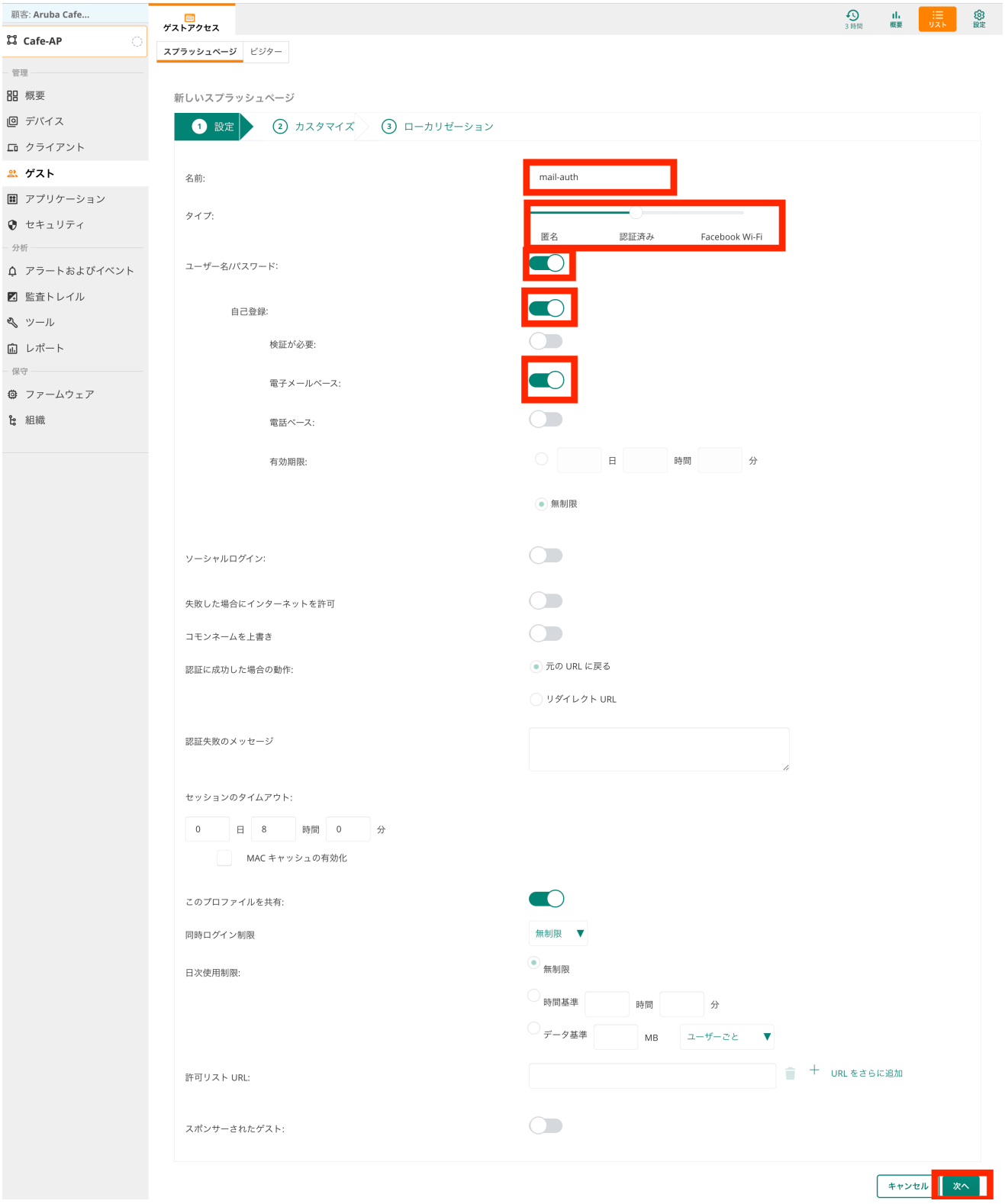
Central のゲスト機能を追加すると、ゲスト wi-fi 作成時に以下のような認証方式が利用できます。

- 同意認証：利用規約に同意（利用規約は任意に設定が可能）
- メール認証：メールアドレスを登録して認証する
- SNS 認証：SNS アカウントでログイン可能
- Facebook Wi-Fi：Facebook ページでチェックイン
- SMS 認証：電話番号に ID を通知し、ID を使って認証
- ID 認証：HPE Aruba Networking Central に登録した ID/Pass を入力して認証

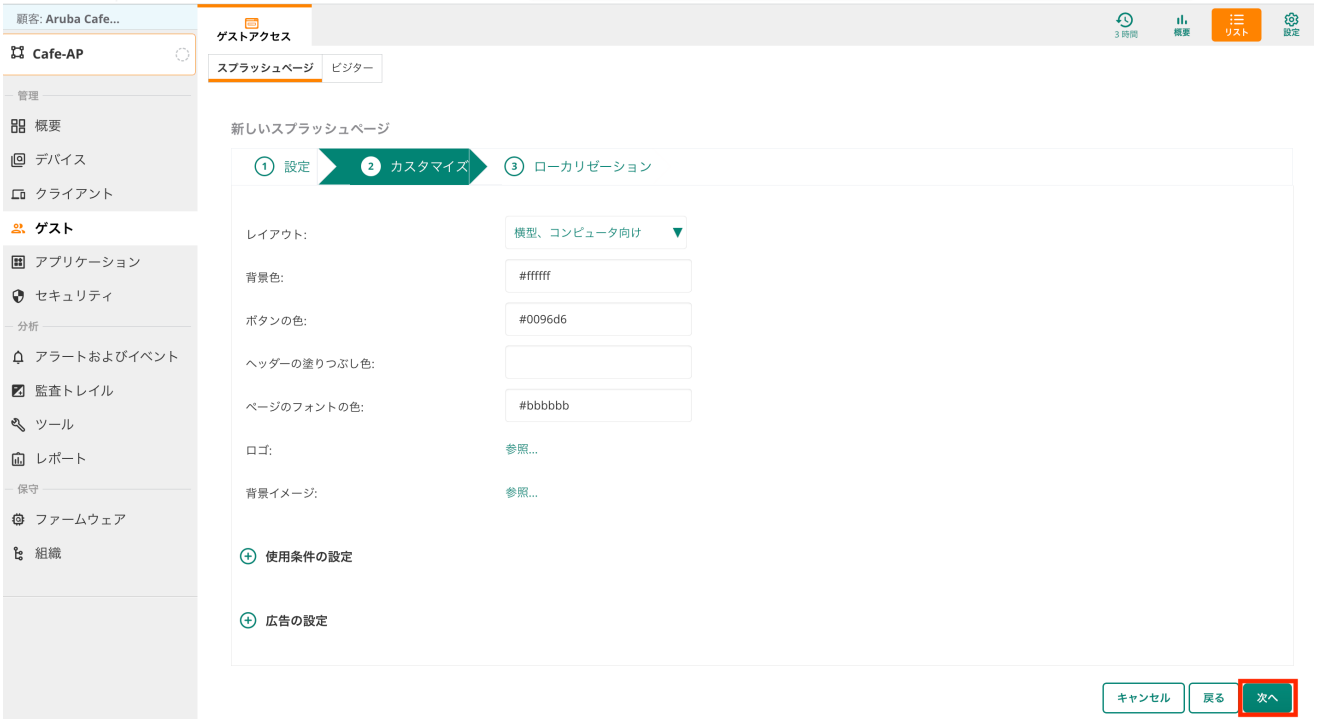
また、キャプティブポータルのカスタマイズも柔軟に行えるため、以下のようなページも作成することができます

① フィルターアイコンよりスプラッシュページを作成するグループを選択
② 右上の“＋”ボタンから新規スプラッシュページを作成

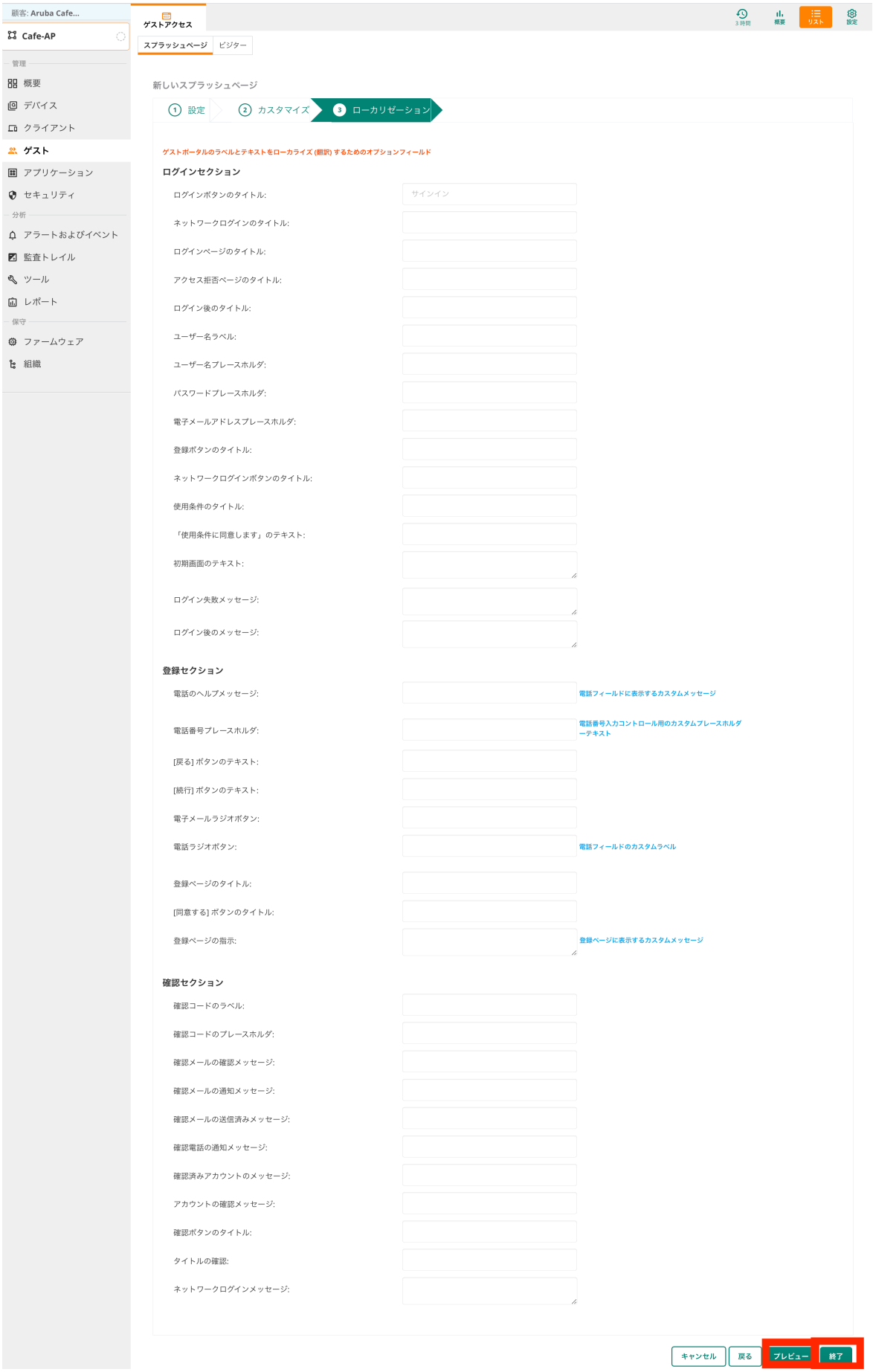
③　任意のスプラッシュページ名を指定
本設定では“mail-auth”とし、タイプを“認証済み”に設定
ユーザー名/パスワードを有効にし、自己登録を有効にすると、自己登録のタイプが表示されるため、今回は“電子メールベース”を有効にする



④　必要に応じてページのデザインや使用条件等をカスタマイズする

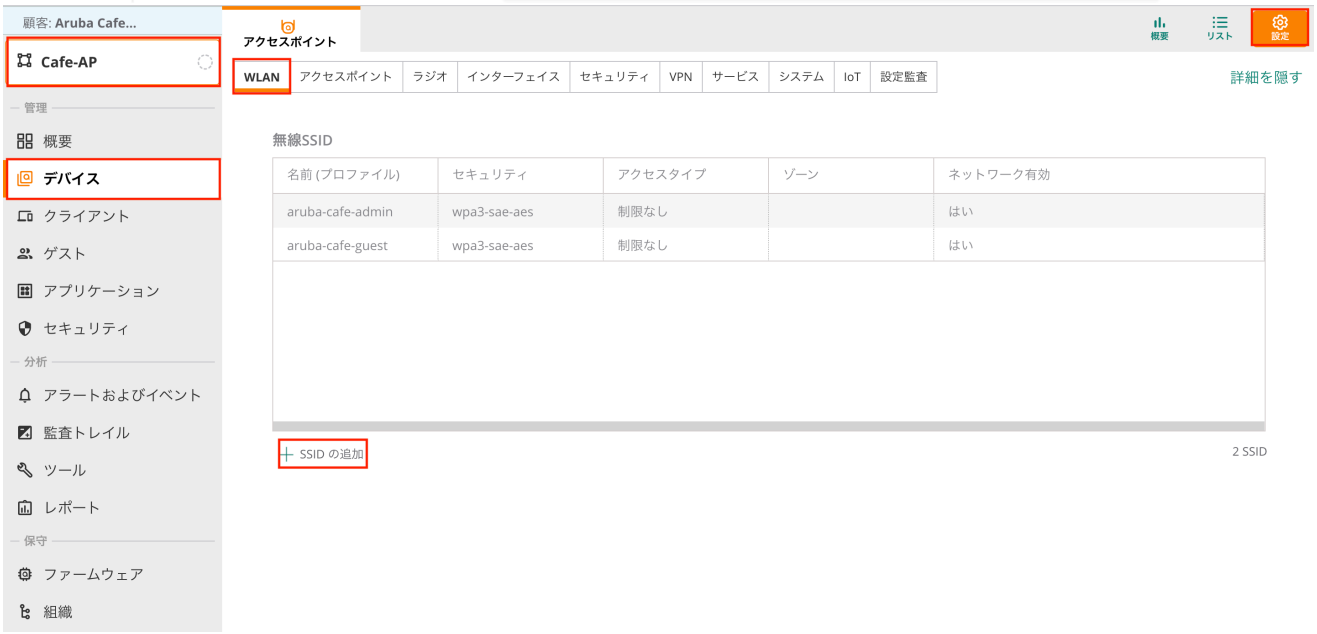


⑤　必要に応じて各セクションをカスタマイズし、プレビューボタンから最終確認をし、終了をクリック




JA
サインイン
ユーザー名
パスワード
サインイン
登録

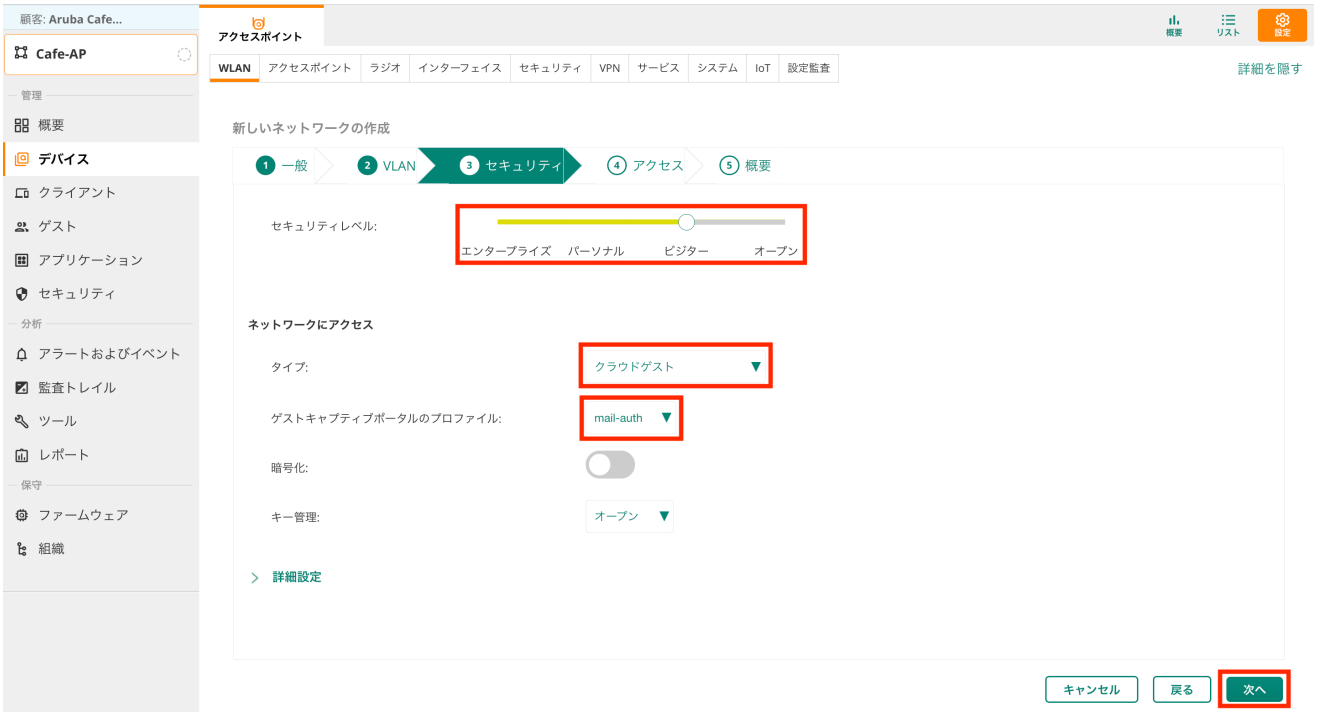
⑥　正しいグループが選択されていることを確認し、左メニューより“デバイス”を選択し、右上の ボタンをクリック
⑦　アクセスポイントタブ内の WLAN より、“＋ SSID の追加”から新規 SSID を作成



⑧　任意の SSID を設定します。本設定では“mail-auth”という SSID とし、“次へ”をクリック

⑨　本設定では、Instant AP の DHCP サーバを利用します。クライアント IP の割り当てにて、”InstantAP 割り当て”を指定

⑩　セキュリティーレベルにおいて、”ビジター”を選択
キャプティブポータルのタイプにおいて”クラウドゲスト”を選択し、プロファイルに先ほど作成した“mail-auth”を選択

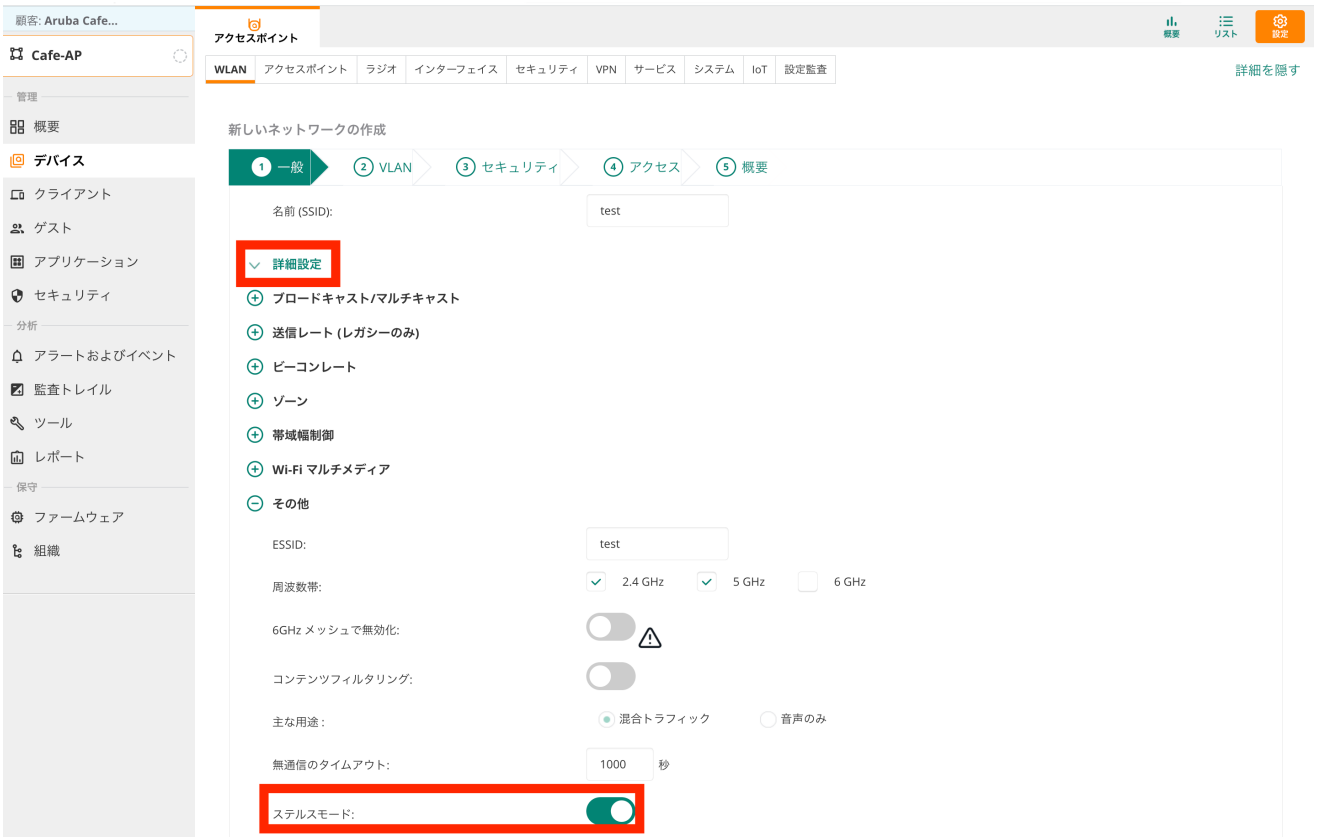


⑪　本設定では、アクセスルール制限をしないため、”制限なし”を選択

概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=mail-auth が作成され、全ての Instant AP から出力される
この SSID に接続をすると、Instant AP の DHCP サーバから IP アドレスが割り当てられ、Instant AP で NAT が行われて通信を行うようになる

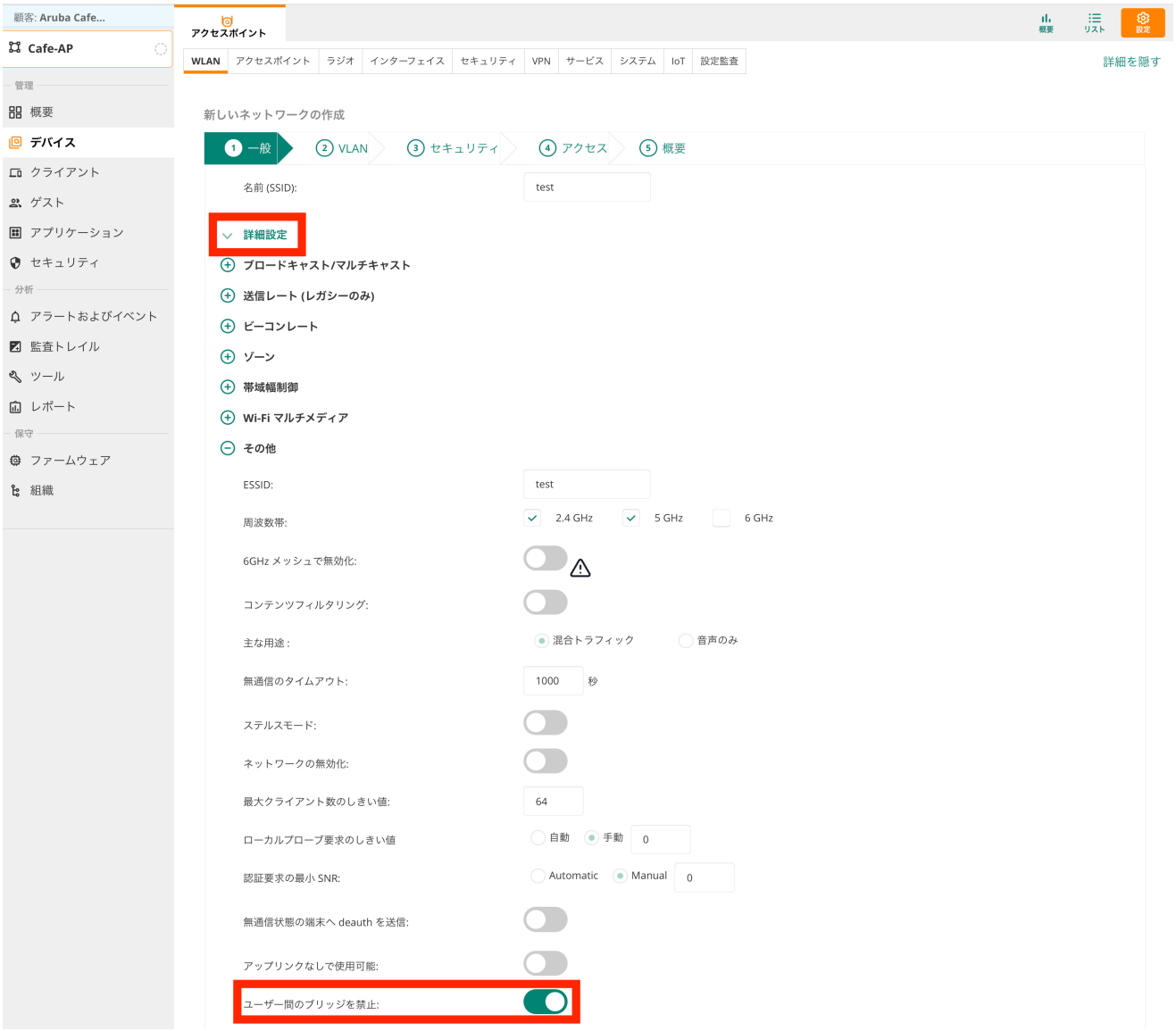
6.11　SSID の隠蔽

SSID を隠蔽して運用したい場合は、WLAN 設定にて”詳細設定”よりその他をクリック
ステイルスモードを有効にする



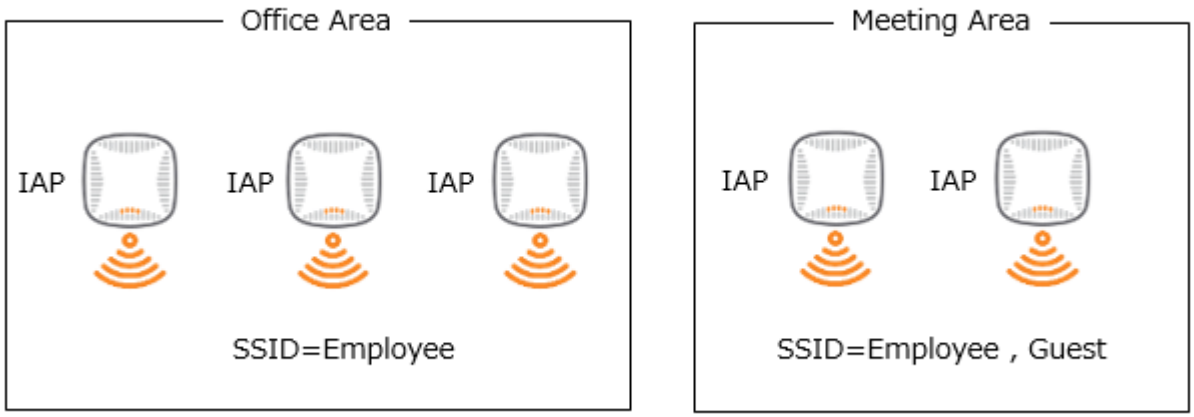
6.12　ユーザ同士の通信制御（User Isolation）について

ゲスト用 SSID 等において、ユーザ同士の通信を禁止したい場合は WLAN 設定にて”詳細設定”をクリックし、”ユーザ間のブリッジを禁止”項目を有効にする



6.13 ゾーン設定について

複数台管理されている Instant AP において、場所ごとに出力したい SSID を分けて運用したい場合はゾーン設定を行います。



（運用例）

①　作成されている SSID を選択し、鉛筆マークをクリックして編集する

② “詳細設定”を表示し、ゾーン項目にユニークな文字列を入力したら“設定の保存”をクリック

③ “アクセスポイント”タブよりアクセスポイントを選択し、鉛筆マークをクリックして編集する

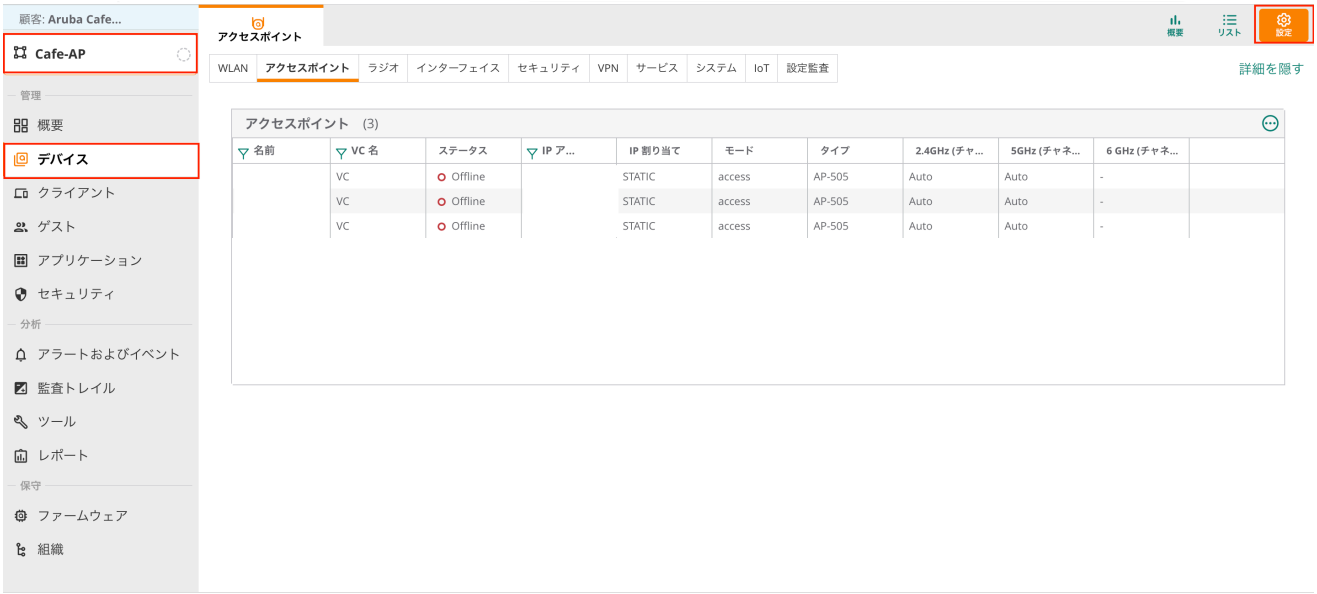
④　AP ゾーンの項目に WLAN 設定で入力したものと同じ文字列を入力
“設定の保存”をクリックすると、ゾーン設定を行った SSID は、同じゾーン設定を行っている Instant AP のみで出力されるようになる
ゾーン設定を行っていない SSID は全ての Instant AP から出力される

6.14　時間ベースの SSID 制御

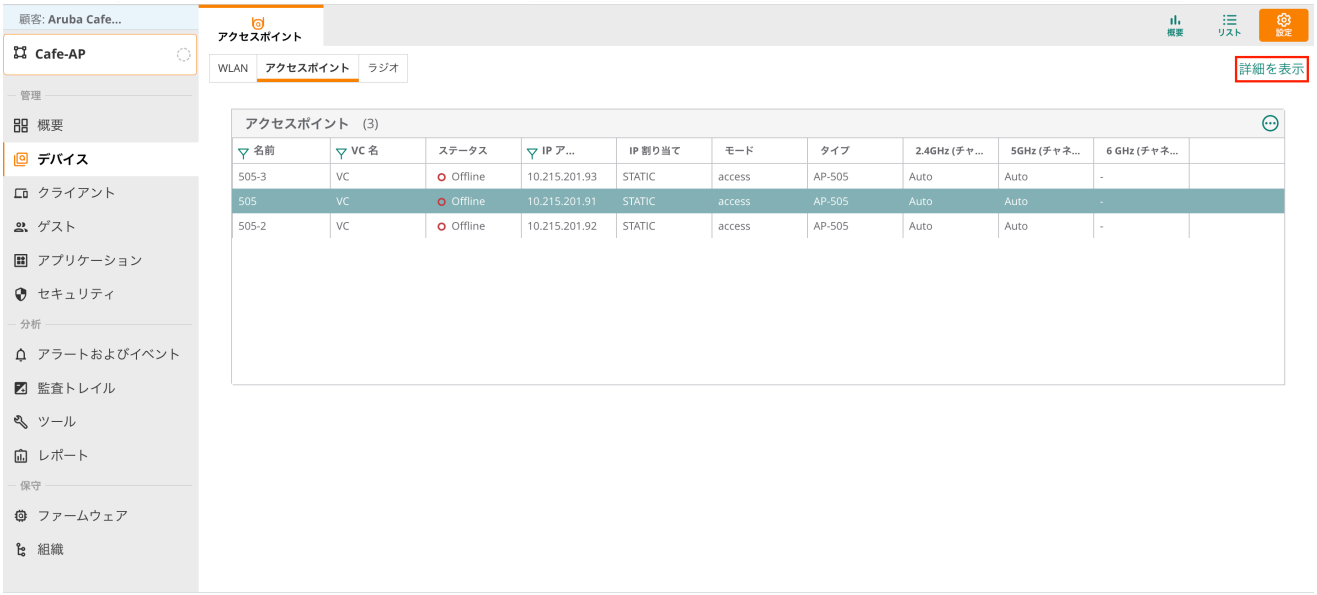
Instant AP では SSID 毎に時間制限を行うことができる
ゲストに対しての利用時間を制限したい等で利用を行う

①　フィルターアイコンよりグループを選択

②　左メニューより“デバイス”を選択し、右上の　ボタンをクリック



③　“詳細の表示”をクリックして、システムタブを開きます

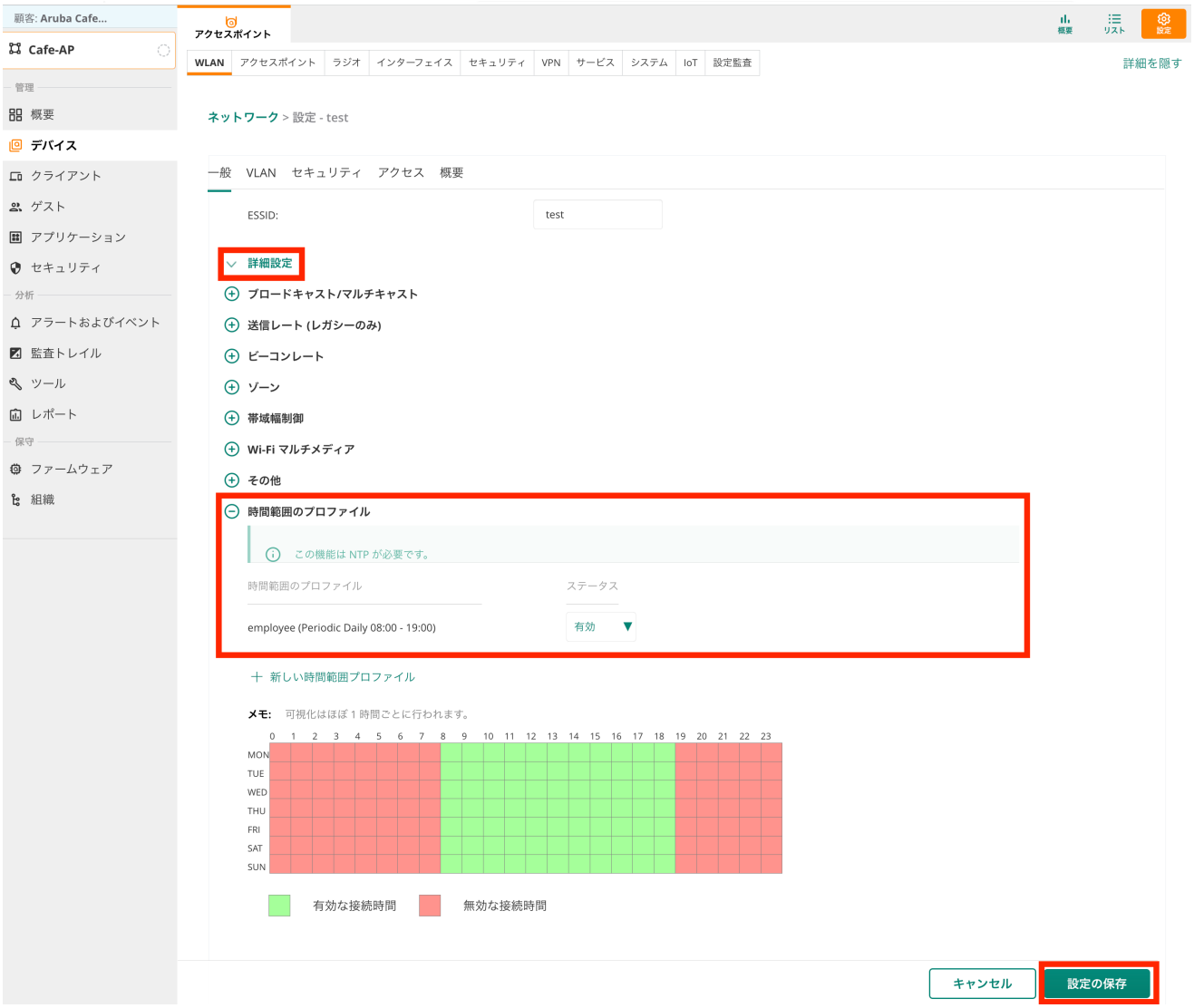


④　“時間ベースのサービス”から＋ボタンで利用時間のプロファイルを作成

⑤　任意の名前、利用時間を指定し、OK をクリック

⑥　WLAN 設定に戻り、時間プロファイルを割り当てる SSID の鉛筆マークから編集する

⑦　“詳細設定”をクリックし、“時間範囲のプロファイル”で先ほど作ったプロファイルを有効
設定の保存をクリックし、SSID 設定を終了する
時間サービスの設定を行った場合、該当の時間のみ SSID を出力するようになる
＊この設定を行う場合、合わせて NTP 設定を行う必要があります。



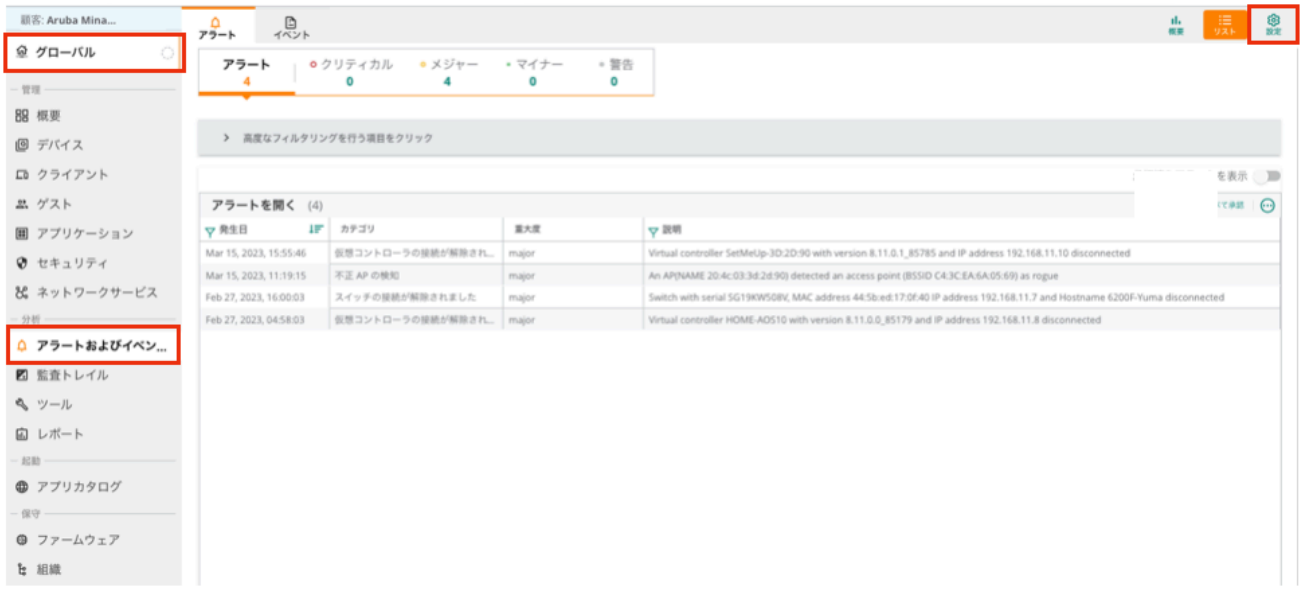
7　アラートとレポート

7.1 アラートの設定方法

Central ではデフォルトの通知ポリシーに沿ってアラートを出すことができます。
デフォルトの通知ポリシーを編集することも可能です。

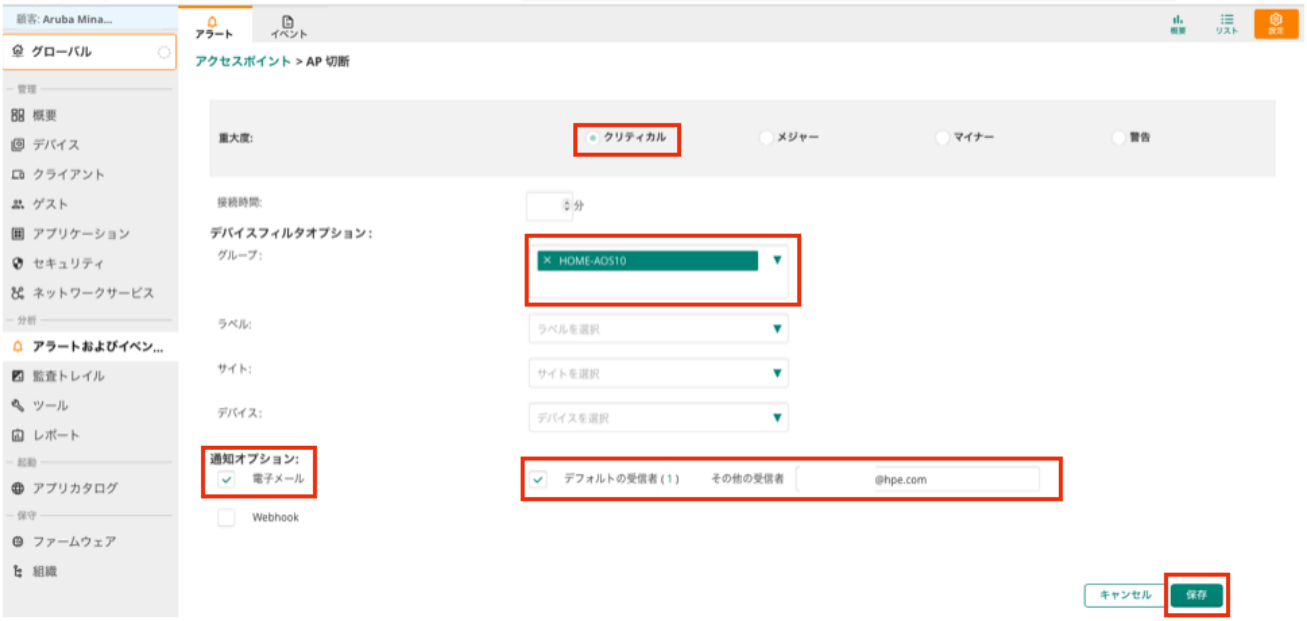
本設定では AP の接続が切断された際に、指定のメールアドレスへ通知メールが来るように設定をします。

①　フィルターがグローバルになっていることを確認の上、“アラートおよびイベント”を選択し、右の設定ボタンをクリック



②　アクセスポイントの中から“AP 切断”をクリック

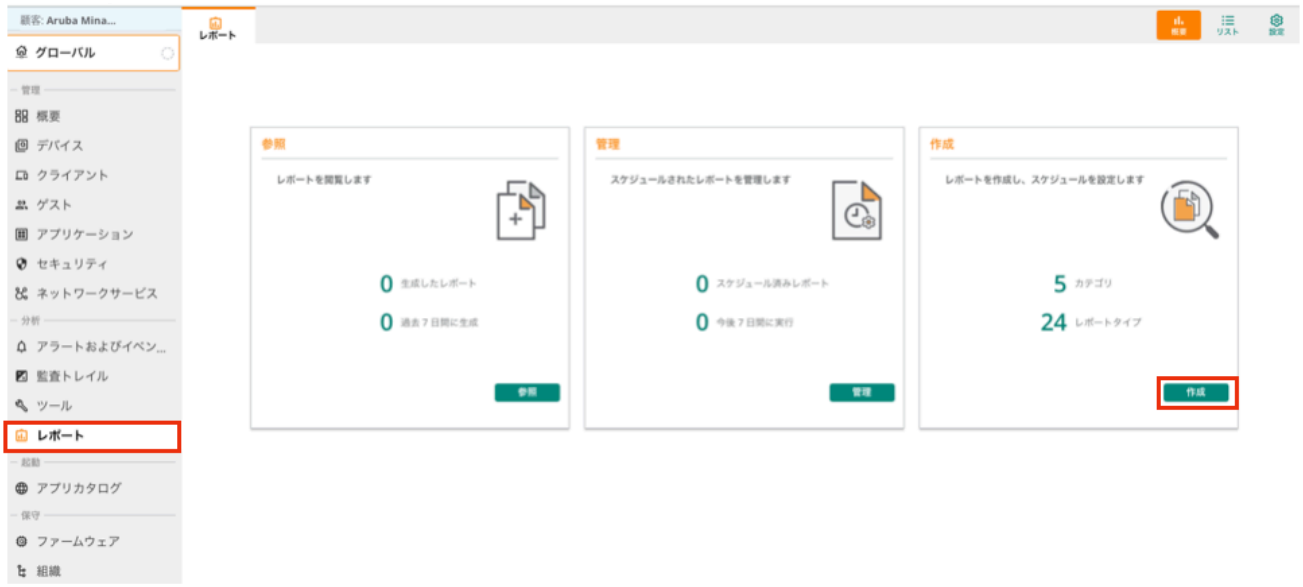
③　重要度を“クリティカル”とし、グループを指定
電子メールアドレスのチェックボックスにチェックを入れ、通知を送るメールアドレスを指定する
保存をクリックすると、アクセスポイントの接続が解除された際に、指定メールアドレスにメール通知が来るようになる



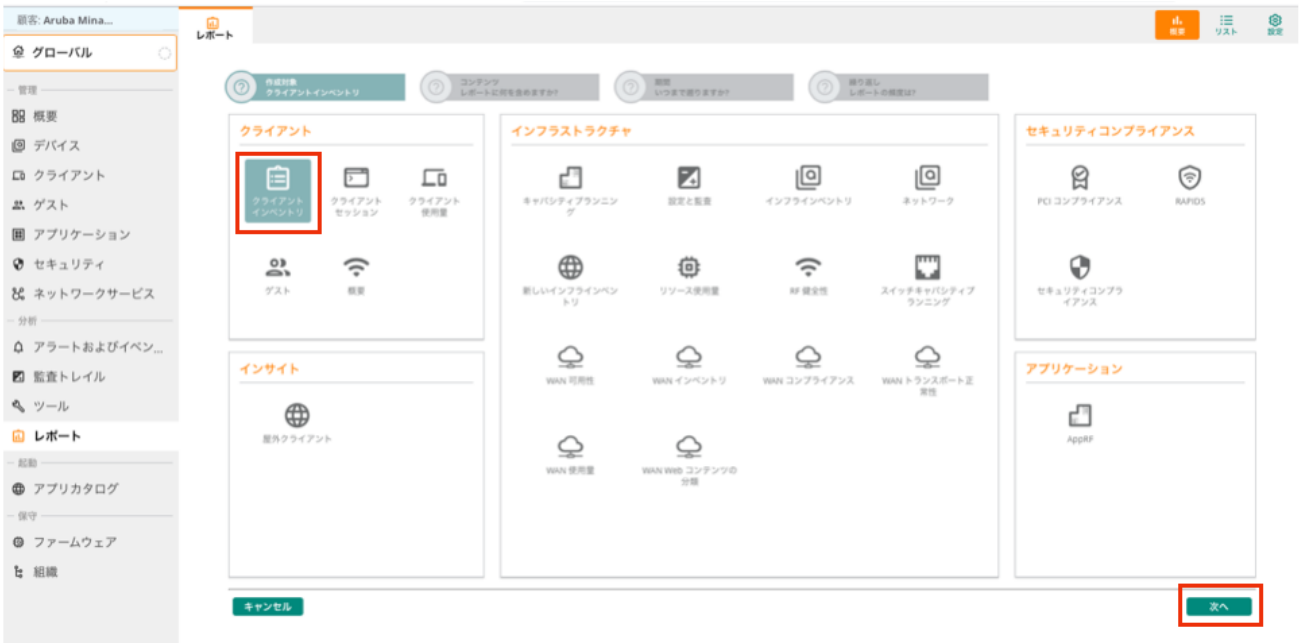
7.2 レポートの出力方法

HPE Aruba Networking Central では現在 5 カテゴリ、24 種類のレポートタイプを出力可能です。

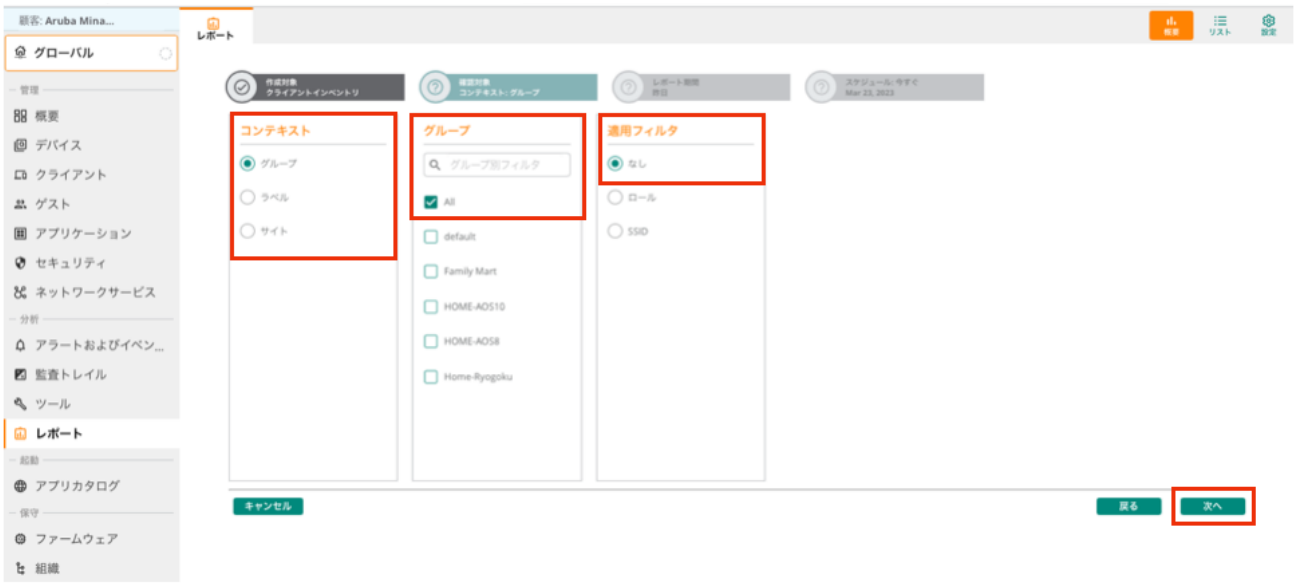
①　左メニューから“レポート”を選択し、“作成”ボタンから新規レポートを作成



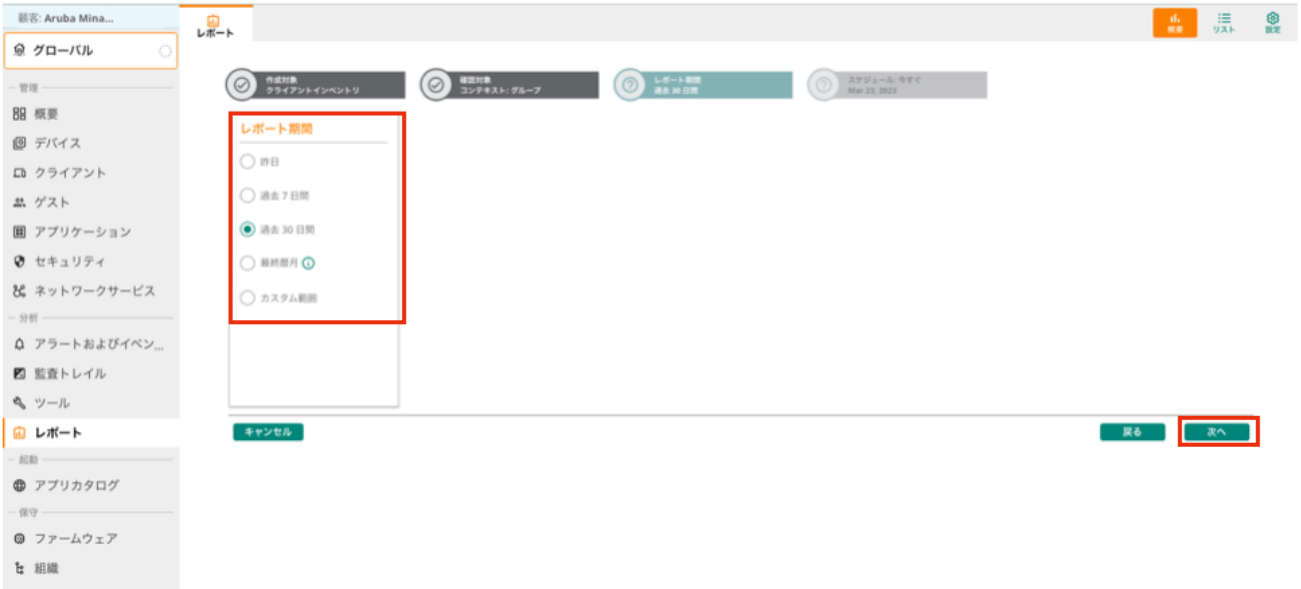
②　どのタイプのレポートを作成するのかを選択し、次へ



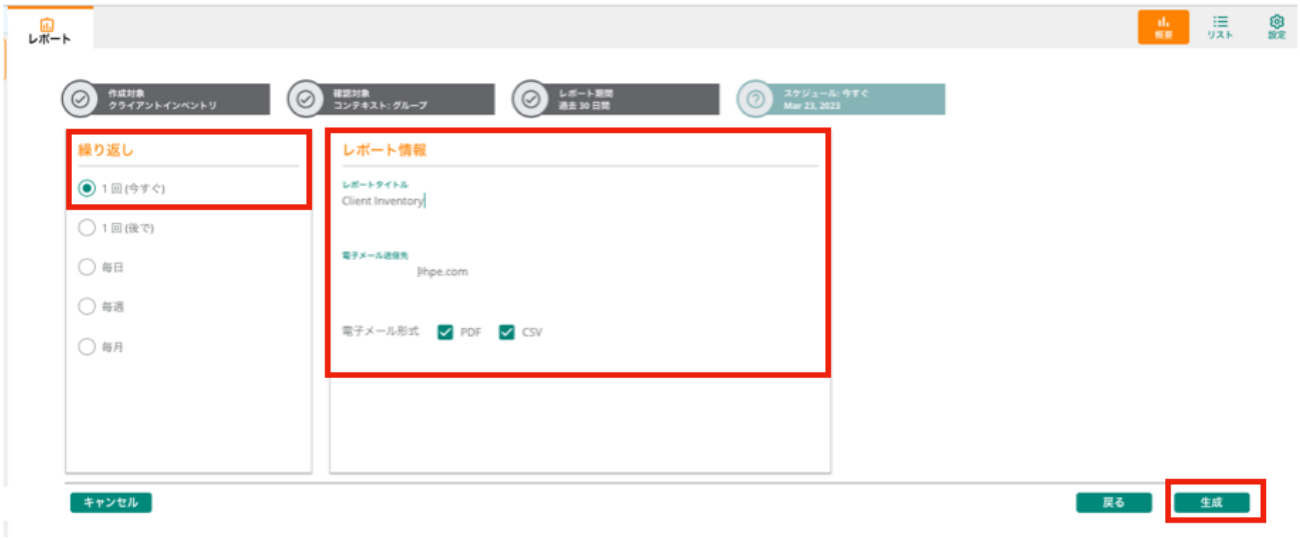
③　レポートを作成する確認対象を確定させ、次へ



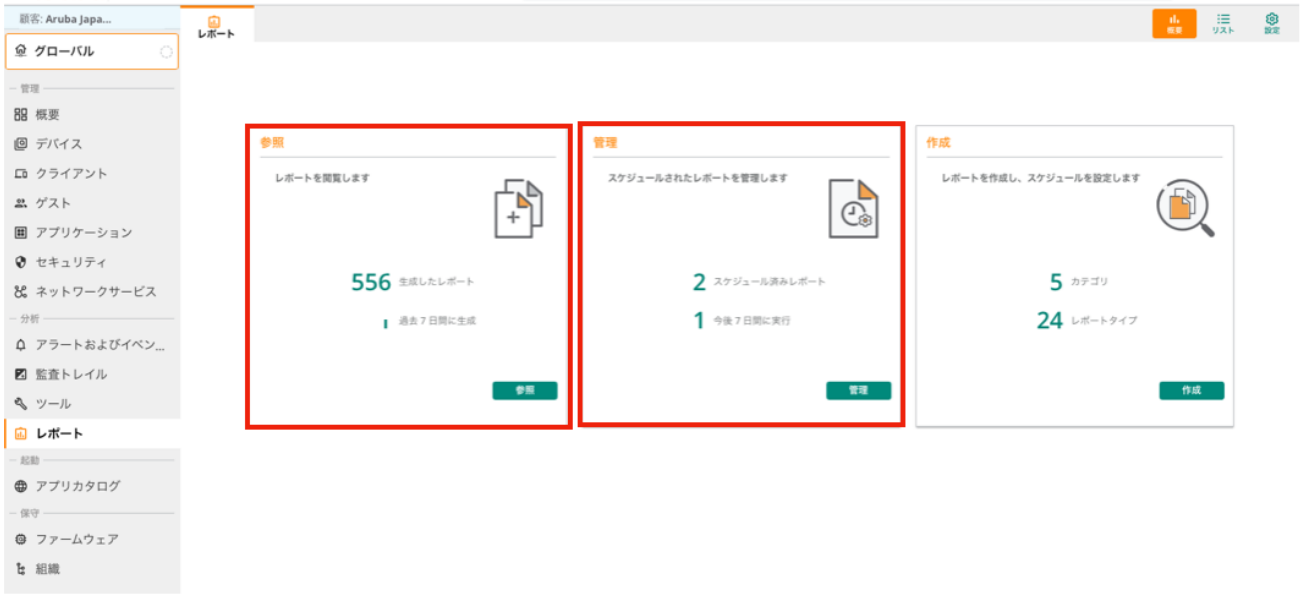
④　レポートに出力する期間を指定する



⑤　レポートを出力する日時を指定し、生成をクリック



⑥　スケジュールしたレポートを管理するには“管理”ボタンから、生成したレポートを確認する場合は“参照”から行えます



8　FLOORPLANS

FLOORPLANS について

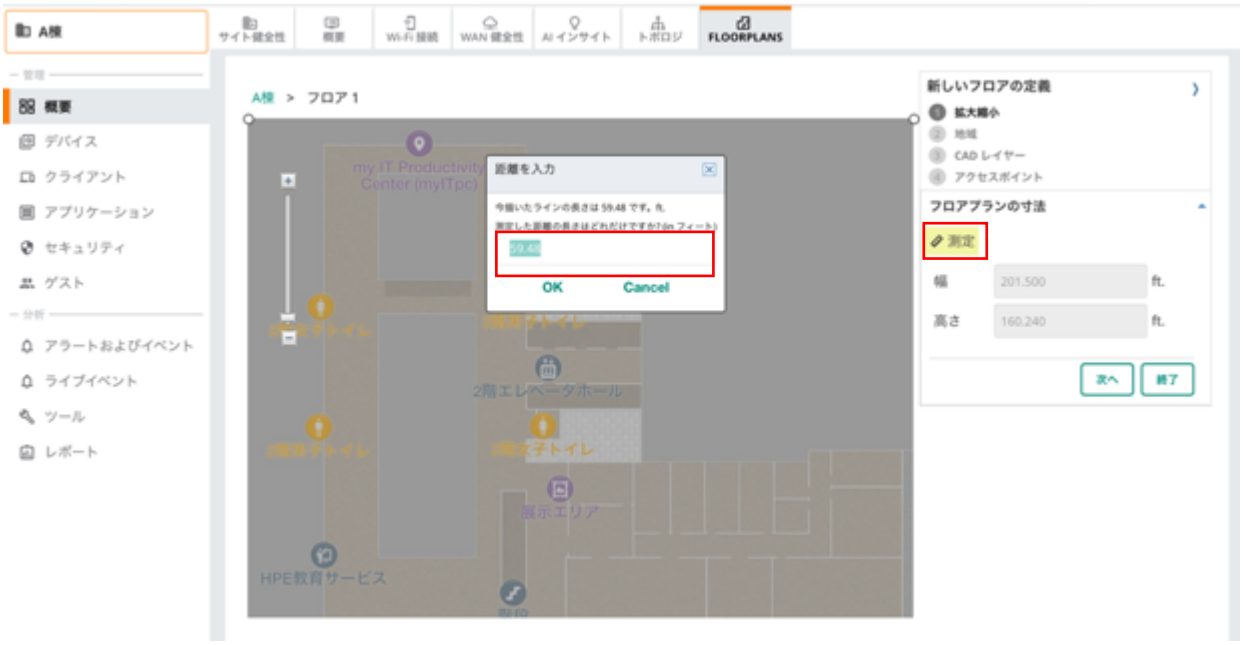
Central ではサイトごとの無線を可視化することができます。また、展開済みの AP だけではなく、仮想的に AP を配置したカバレッジシミュレータとして使用することができます。

①　可視化したいサイトを選択。上部タブの“フロアプラン”を選択後、“フロアの追加”をクリック

②　“新しいフロアプラン”をクリック

③　サイトの図面をアップロードする。jpg、jpeg、gif、bmp、pdf、png 形式をサポートしています。

④　フロアプランの寸法より、“測定”をクリック。図面にドラッグで線を引き実測値を入力（フィート、メートルをサポート）



⑤　アクセスポイントを追加する

A)　展開済み AP を追加する場合

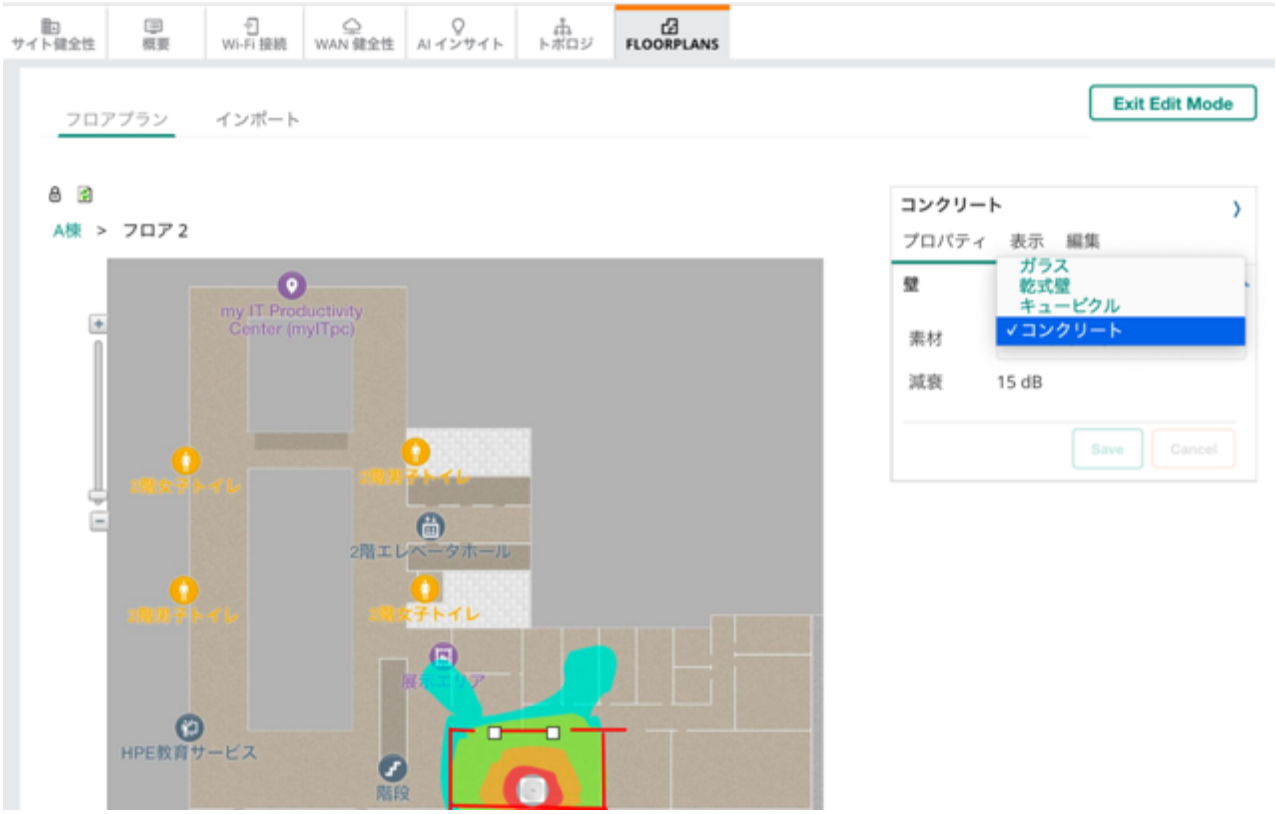
”展開済み AP の追加”より。サイトに登録している AP を選択。AP をドラッグして実際の位置に配置する。

B)　仮想的に AP を配置する場合

“AP の計画”より配置したいモデルを選択し“フロアプランに AP を追加”をクリックし終了

⑥　AP を追加した後、“編集”から“壁を描く”をクリック。フロアプランにドラッグで壁を描画する。

⑦　プロパティから壁の材質を選択可能。壁の材質によって電波の減衰が定められており、リアルタイムにヒートマップが変化する。



9　AIOPs

AIOPs について

Central では AI によってネットワーク内の問題を特定し、ピンポイントの推奨構成を提案します。

AI Insights

AI Insights のダッシュボードには、ネットワークに影響を与える可能性のあるイベントのレポートが表示されます。これは選択した時間範囲特定のサイト、デバイスごとやクライアント毎のネットワークイベントのレポートが表示されます。

AI Insights の表示方法

AI Insight の表示方法は Central で管理しているネットワーク、サイトごと、AP ごとの 3 通りあります。

A)　フィルターから“グローバル”を選択し、左メニューから“概要”をクリック
B)　左上メニュー“サイト”より、AI Insights を見たいサイトをクリック。左メニュー“概要”をクリック
C)　グローバルより、左メニュー“デバイス”をクリック。AI Insights を見たい AP をクリック。左メニュー“概要”をクリック。

①　“AI インサイト”タブをクリックし、各インサイトの矢印をクリックすると詳細を表示

② インサイトのタブについて

A.インサイトが生成された理由と推奨事項が表示されます

B.選択した時間範囲で発生したイベントをグラフで表示しています

C.カードには各インサイト固有の追加情報が表示されます。

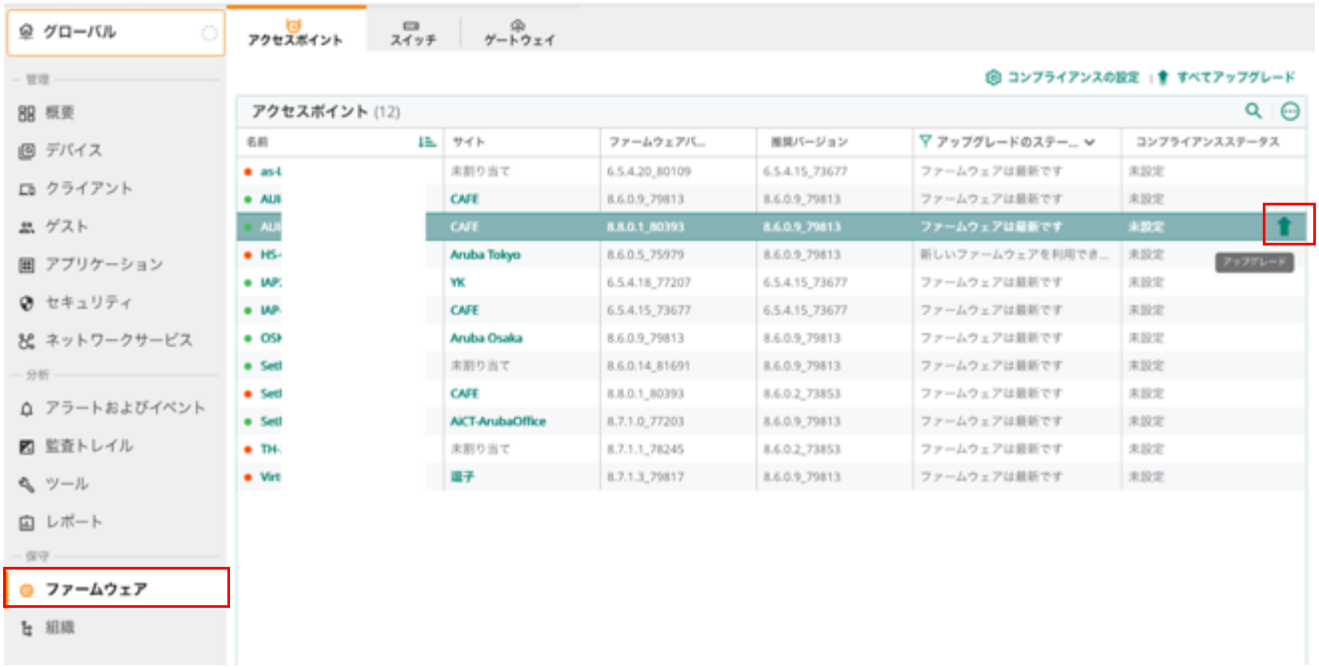
10　メンテナンス

10.1　Version UP について

Instant AP では異なる型番においても Version が同じものであれば、1 つのクラスタとして管理することができます。同一型番で統一している場合は、仮想コントローラを Version UP することにより全ての Instant AP の Version を一括で変更することが可能ですが、異なる型番とのクラスタを組んでいる場合は型番ごとに Version UP を行っていただく必要があります。ご注意ください。

Version UP 方法

①　左メニューから“ファームウェア”を選択し、アップグレードする VC を選択し“アップグレード”をクリック
　　複数の VC を選択してまとめてアップグレードすることも可能です



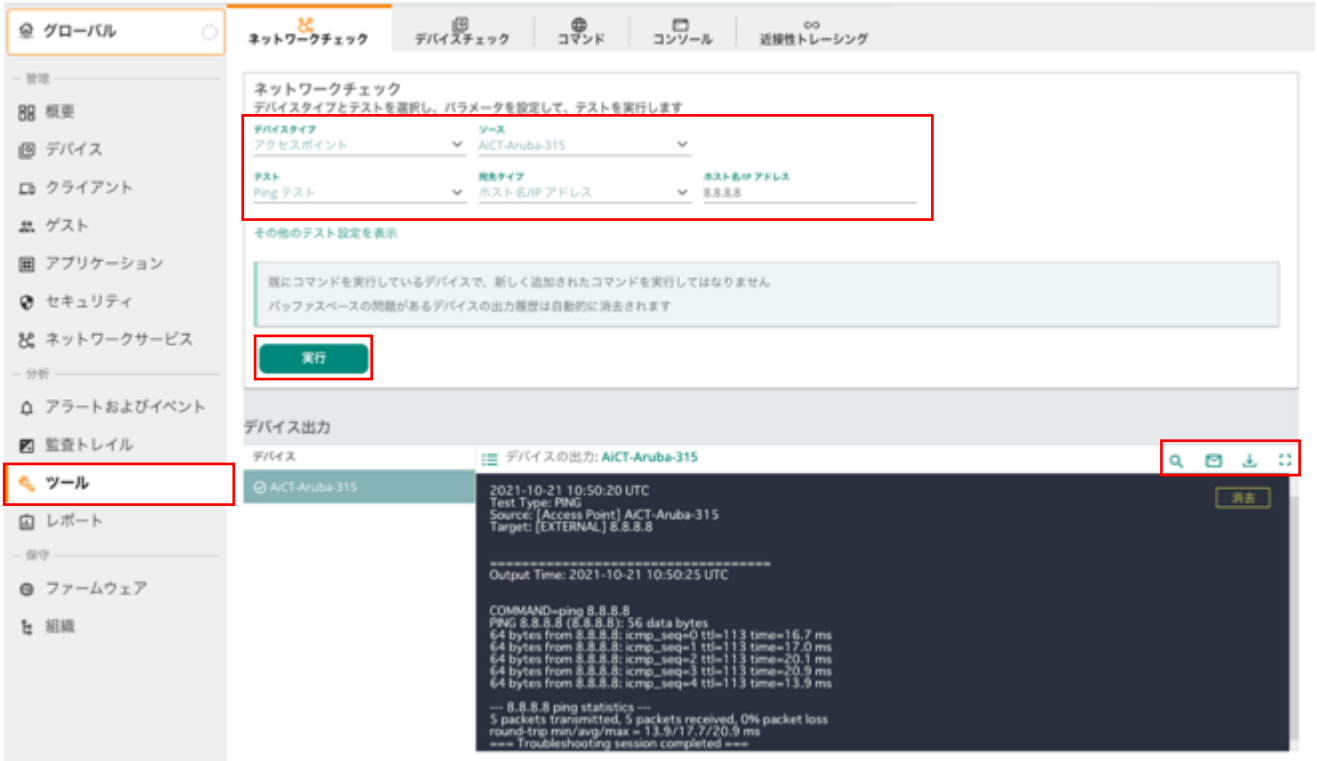
②　ファームウェアのバージョン、アップデートする日時を選択し “アップグレード”をクリック

10.2 ツール

ネットワークチェック

デバイスタイプ、テストのタイプ、ソースを選択し、パラメータを設定してテストを実行できる

① 左のメニューより“ツール”を選択し、ネットワークチェックのタブをクリック
② デバイスタイプ、テスト項目、ソース等を指定し“実行”ボタンをクリックし、デバイス出力より結果を確認する。
デバイス出力は電子メールでの共有、あるいはテキストベースでのアウトプットが可能



10.3 リモートコンソール

Central では GUI から AP の CLI がひらけます

① 左メニューより“ツール”を選択し、“コンソール”タブを開きます。デバイスタイプとデバイス、ユーザ名とパスワードを入力し、“新規セッションの作成”をクリックするとリモートコンソールがスタートします。

11 AP の削除

グループからの削除方法

グループからデバイスを削除する方法は HPE Aruba Networking Central 基本操作ガイド 入門編を参照

https://www.hpe.com/psnow/doc/a00143744jpn

デバイスインベントリからの削除方法

HPE Aruba Networking Central からデバイスを完全に削除することはできませんが、アーカイブにデバイスを移動させるか、デバイスのサブスクリプションを解除することはできます。

グループの削除

グループの削除は中身が空の状態の時のみ
詳しくは、HPE Aruba Networking Central 基本操作ガイド 入門編を参照

https://www.hpe.com/psnow/doc/a00143744jpn

12 不具合かと思ったら

詳細な不具合内容、物理構成、不具合発生時のログ、コンフィグ、不具合再現方法をそろえた上で製品を購入した弊社販売代理店へご連絡ください。販売代理店側のサポート経由で弊社 TAC が対応をいたします。

解析に必須となるログ取得

全ての Instant AP の “show tech-support “ および、”show tech-support supplemental ” は必須となります。

以上