

Technical Note



# Aruba Central 基本操作ガイド

## ～AP 編 (AOS10)～

日本ヒューレット・パカード合同会社  
Aruba 事業統括本部

## 目次

<b>1.</b>	<b>はじめに.....</b>	<b>5</b>
1.1.	本資料について.....	5
1.2.	注意事項.....	5
1.3.	Software Version .....	5
<b>2.</b>	<b>Central へ AP のオンボーディング.....</b>	<b>6</b>
2.1	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.....	6
2.2	グループ・サイト・ラベルの作成方法.....	6
2.3	初期状態の AP のプロビジョニング.....	6
<b>3.</b>	<b>AP の起動.....</b>	<b>7</b>
3.1	AP を起動する前に.....	7
3.2	電源の投入.....	7
3.3	コンソールケーブルを用いての IP アドレス設定.....	7
<b>4</b>	<b>AP 基本設定.....</b>	<b>9</b>
4.1	各 AP の AP 名・IP アドレス設定.....	9
4.2	NTP 設定.....	11
4.2.1	時刻同期の確認1 (GUI) .....	12
4.2.2	時刻同期の確認2 (GUI コンソール).....	13
4.3	AppRF.....	14
4.4	工場出荷状態への戻し方.....	16
4.4.1	グループを使った AP の初期化.....	16
4.4.2	リモートコンソールからの初期化.....	16
4.4.3	CLI からの初期化.....	17
4.4.4	リセットボタンからの初期化.....	17
<b>5</b>	<b>有線ポート設定.....</b>	<b>19</b>
<b>6</b>	<b>SSID の設定.....</b>	<b>23</b>
6.1	SSID の作成手順.....	23
6.2	設定例)オープン認証(暗号/認証なし).....	26
6.3	設定例)WPA3-PSK.....	29
6.4	設定例)WPA3-PSK+MAC 認証.....	32
6.5	設定例)802.1x Internal Radius 利用.....	37
6.6	設定例)802.1x External Radius 利用.....	41
6.7	Dynamic VLAN (External Radius 利用).....	44
6.8	設定例)Web 認証 規約ページのみ.....	48
6.9	ユーザ/パスワードでのログイン.....	エラー! ブックマークが定義されていません。
6.10	Central ゲスト(メール認証).....	51
6.11	SSID の隠蔽.....	61
6.12	ユーザ同士の通信制御 (User Isolation) について.....	62
6.13	ゾーン設定について.....	エラー! ブックマークが定義されていません。
6.14	時間ベースの SSID 制御.....	63
<b>7</b>	<b>アラートとレポート.....</b>	<b>67</b>

7.1	アラートの設定方法	67
7.2	レポートの出力方法	69
8	FLOORPLANS	72
10	AIOPs	76
11	メンテナンス	78
11.1	Version UP について	78
11.2	ツール	79
11.3	リモートコンソール	80
13	AP の削除	81
14	不具合かと思ったら	81

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



## 1. はじめに

### 1.1. 本資料について

本資料は Aruba Central におけるインスタントアクセスポイント(AOS10)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ません。  
また、Windows, Windows Server など Aruba 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.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/>

### 1.3. Software Version

本資料は Aruba Central 2.5.6 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 画面と異なる場合がございます。ご了承ください。

## 2. Central へ AP のオンボーディング

### 2.1 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

Central へ AOS10 AP をオンボーディングするには以下のことが GLCP で完了している必要があります。

- Central で管理する AP 数分のサブスクリプションが GLCP に登録されていること
- AP が GLCP へ登録されていること
- サブスクリプションが AP に割り当てられていること

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 設定入門ガイドを参照してください。

<https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/>

### 2.2 グループ・サイト・ラベルの作成方法

Central 内で事前に AP を割り当てるためのグループ (作成必須)・サイト (作成推奨)・ラベル (オプション) を作成する必要があります。

グループ・サイト・ラベルそれぞれの昨日説明・作成方法に関しては、以下 Central 設定入門ガイドを参照してください。

<https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/>

### 2.3 AP のプロビジョニング

上記で作成したグループ・サイト・ラベルに AP を割り当てます。グループへ AP を割り当てる際には“Central でオンラインになったことがあるデバイス”と“Central で一度もオンラインになったことがないデバイス”で操作方法が異なります。

それぞれの操作方法に関しては、以下 Central 設定入門ガイドを参照してください。

<https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/>

### 3. AP の起動

#### 3.1 AP を起動する前に

AP が AOS10 のデフォルトイメージで起動してくることを確認ください。AOS6 or AOS8 のデフォルトイメージで起動する場合、AOS10 のイメージへバージョンアップしてください。AOS6 or AOS8 で既存の設定がある場合、**AOS10 のイメージへバージョンアップすると設定は初期化されるためご注意ください。**

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。

#### 3.2 電源の投入

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。

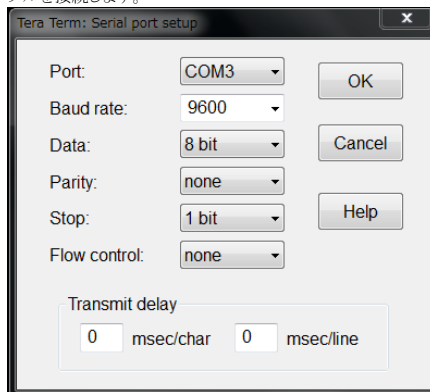
\* モデルによって起動に必要な電力が違います。詳しくはアクセスポイントのデータシート等を確認ください。

#### 3.3 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は同梱されておらず別売りとなっておりますので、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 AP にコンソールケーブルを接続します。

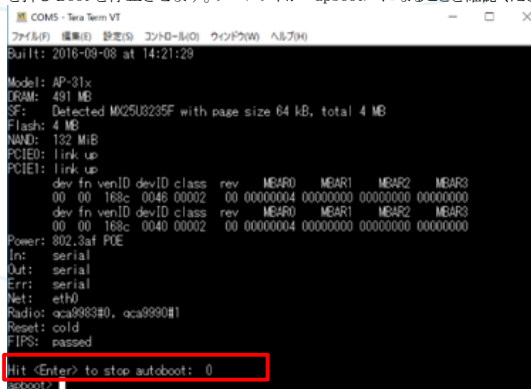


##### ② 電源の投入

アダプタもしくは、PoE から AP に給電を行います。

##### ③ Boot の停止

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 秒で表示されます。

## 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 を指定します。

- setenv ipaddr <ip アドレス>
- setenv netmask <netmask>
- setenv gatewayip <default gateway アドレス>
- setenv dnssip <DNS Server アドレス>

```
arboot> setenv ipaddr 10.215.212.20
arboot> setenv netmask 255.255.255.0
arboot> setenv gatewayip 10.215.212.1
arboot>
```

## 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るかを確認します。

```
COM3 - Tera Term V1
ファイル(F) 編集(E) 設定(S) コントロール(C) ランドウ(W) ヘルプ(H)
autostart=yes
bootfile=ipos06x.ari
btaddr=rand0
ethaddr=80:3d:b7:c2:e9:02
ENV_SBL2=1
name=AP102
uap_controller_less=1
os_partitions=0
stdin=serial
stdout=serial
stderr=serial
machid=1260
mtddparts=mtddparts=rand0:0x200000000x0(aos0),0x200000000x2000000(aos1),0x400000000x
40000000(ubifs)
partition=rand0,0
mtddvname=0
mtdddevname=aos0
ethact=eth0
ipaddr=10.215.212.20
netmask=255.255.255.0
gatewayip=10.215.212.1
Environment size: 512/65532 bytes
arboot>
```

\*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”コマンドで再起動します。

```
arboot> saveenv
Saving Environment to Flash...
Erasing flash...
Writing to flash... .....done
arboot>
```

起動後 Central 接続前は User:admin Password:AP のシリアルナンバーで入り、Central 接続後は User:admin Password:Central のグループで設定したパスワードでログイン後、“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ます。

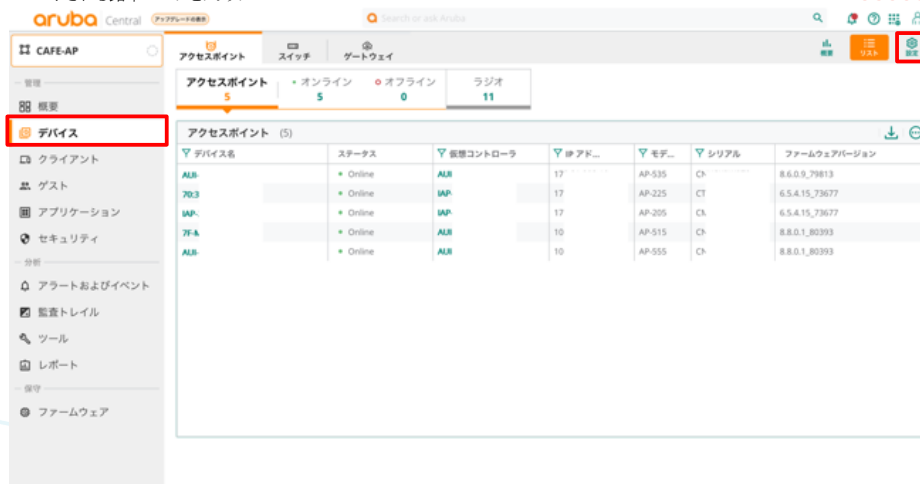
## 4 AP 基本設定

### 4.1 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



Aruba Central console showing the Access Points list. The 'IP' column for the selected AP is highlighted, and the edit icon is circled in red.

名前	VLAN	ステータス	IP アドレス	IP 割り当て	モード	タイプ	2.4GHz (チャネル)	5GHz (チャネル)	アクション
ALL	AI	Up	172.31	DHCP	access	AP-535	Auto	Auto	
IAP	IA	Up	172.31	STATIC	access	AP-205	Auto	Auto	
IAP	IA	Up	172.31	DHCP	access	AP-225	Auto	Auto	
ALL	AI	Up	10.215	DHCP	access	AP-555	Auto	Auto	
RF-I	AI	Up	10.215	DHCP	access	AP-515	Auto	Auto	

- 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。自動で再起動は行われません。

Aruba Central console showing the configuration page for an Access Point. The 'System' tab is selected, and the 'Static IP' option is chosen. The IP address, netmask, default gateway, and DNS server fields are highlighted with red boxes.

アクセスポイント / b8:3a:5a:c1:1f:0a

名前: AOS10-AP1

アクセスポイントの IP アドレス: ☐ IP アドレスを DHCP サーバーから取得 ☒ スタティック

IP アドレス: 192.168.1.20 変更を有効にするには AP を再起動します。

ネットマスク: 255.255.255.0

デフォルトゲートウェイ: 192.168.1.1

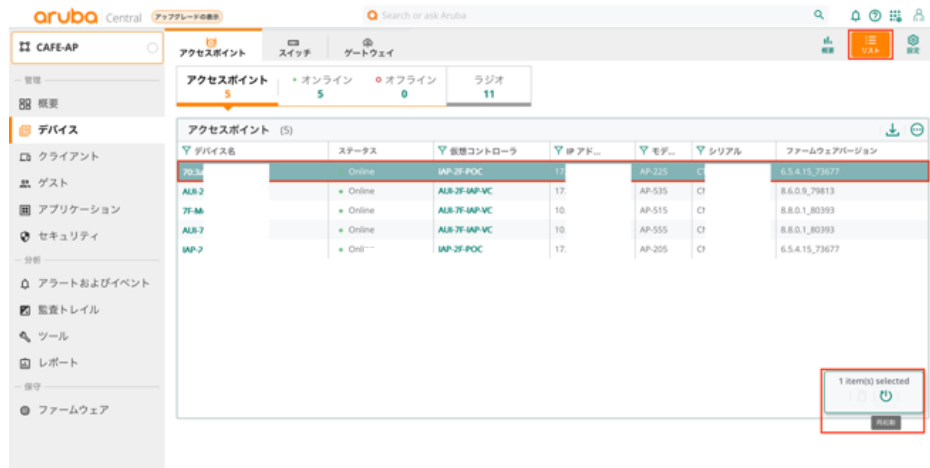
DNS サーバー: XXX.XXX.XXX.XXX,XXX.XXX.XXX.XXX

ドメイン名:

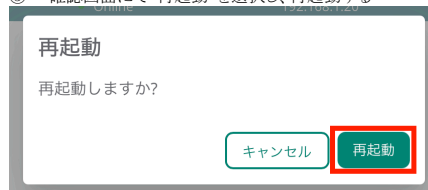
LAGP モード: バッファ

Cancel Save Settings

- 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する



- ⑤ 確認画面にて“再起動”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。

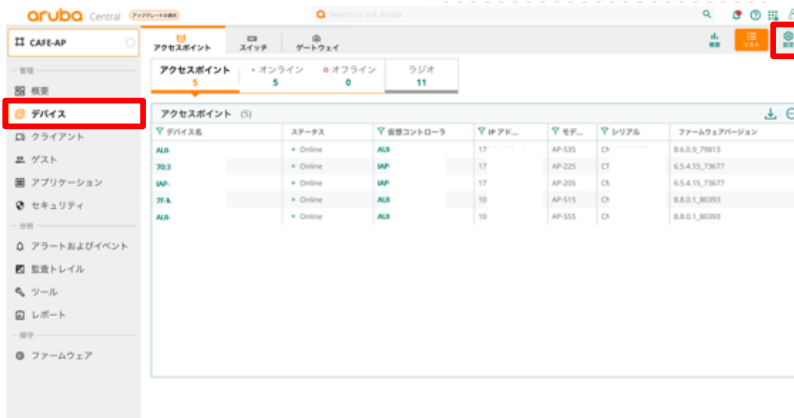
## 4.2 NTP 設定

AP 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ありますので、設定していただくことを推奨いたします。

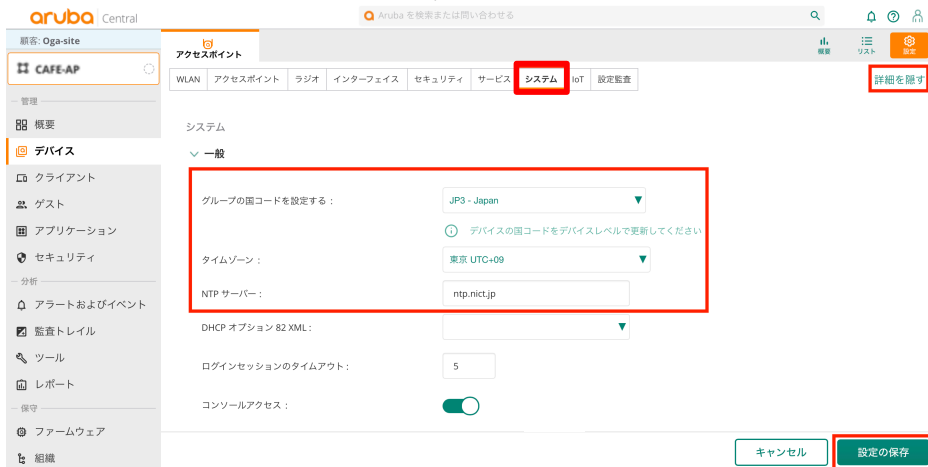
- ① フィルターよりグループを選択



- 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”ボタンをクリック



#### 4.2.1 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



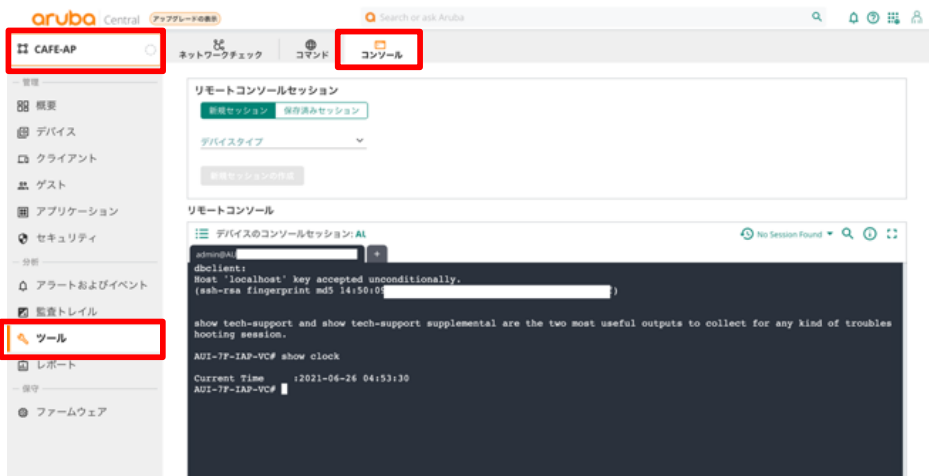


#### 4.2.2 時刻同期の確認2 (GUI コンソール)

Central では GUI から AP のコンソールが開けます。

- ① グループを選択後、メニューから“ツール”を選択し、“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




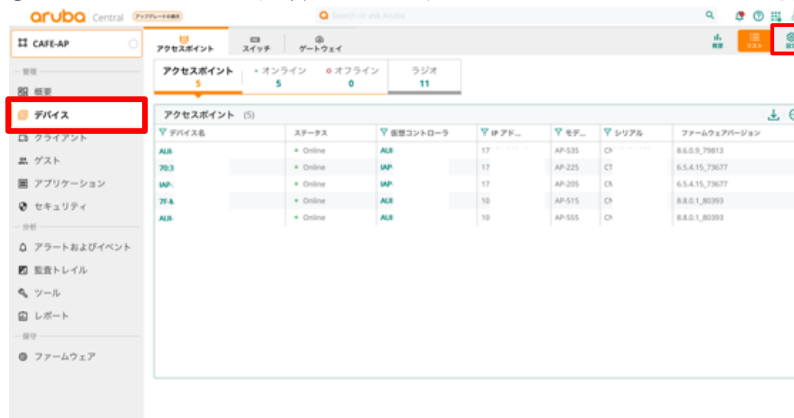
### 4.3 AppRF

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 を付与や、拒否することが可能となります。必要に応じ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

The screenshot shows the Aruba Central web interface for a customer named 'Oga-site'. The left sidebar contains navigation links for '管理' (Management), '概要' (Overview), 'デバイス' (Devices), 'クライアント' (Clients), 'ゲスト' (Guests), 'アプリケーション' (Applications), 'セキュリティ' (Security), '分析' (Analysis), 'アラートおよびイベント' (Alerts and Events), '監査トレイル' (Audit Trail), 'ツール' (Tools), 'レポート' (Reports), '保守' (Maintenance), 'ファームウェア' (Firmware), and '組織' (Organization). The main content area is titled 'アクセスポイント' (Access Points) and includes tabs for 'WLAN', 'アクセスポイント', 'ラジオ', 'インターフェイス', 'セキュリティ', 'サービス', 'システム', 'IoT', and '設定監査'. The 'サービス' (Services) tab is active, showing a list of services: 'リアルタイム位置情報システム', 'CALEA', 'ネットワーク統合', and 'ダイナミック DNS'. The 'AppRF' section is expanded, showing '詳細なパケット検査' (Detailed Packet Inspection) set to 'すべて' (All), 'アプリケーションのモニタリング' (Application Monitoring) turned on, and 'AirSlice ポリシー' (AirSlice Policy) turned off. The '設定の保存' (Save Settings) button is highlighted in red.

## 4.4 工場出荷状態への戻し方

### 4.4.1 グループを使った AP の初期化

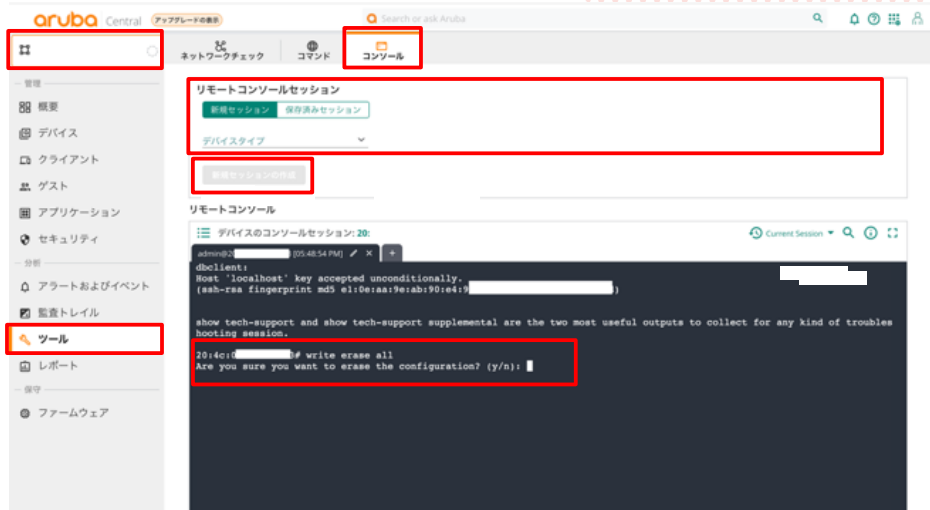
設定の入っていない新規グループを作成し、AP を作ったグループに移すことで設定の初期化をします。グループの作り方と AP の割り当てについて詳しくは Central 設定入門ガイドを参照してください。

<https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/>

### 4.4.2 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



#### 4.4.3 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。

```
COM5 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
FIPS: passed

Hit <Enter> to stop autoboot: 0
apboot>
apboot> factory_reset
Clearing state... Checking OS image and flags
Image is signed: verifying checksum... passed
Preserving image partition 0
Erasing flash sector @ 0x3a0000...OK

Device 0: nand... is now current device
Erasing UBIFS ...OK
Remove UBI volume ubifs (id 0)
Creating dynamic volume ubifs of size 63361024
Device 1: nand... is now current device
done
Purging environment... preserving os_partition (0)
Erasing flash...
Writing to flash... .....done
Erasing flash... .....done
Writing to flash... .....done
done
apboot> boot
```

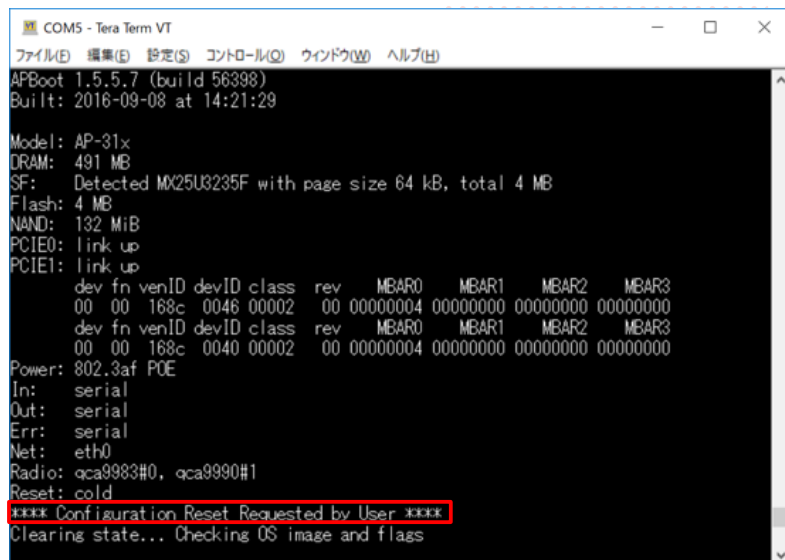
#### 4.4.4 リセットボタンからの初期化

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



```
COM5 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(C) ウィンドウ(W) ヘルプ(H)
APBoot 1.5.5.7 (build 56398)
Built: 2016-09-08 at 14:21:29

Model: AP-31x
DRAM: 491 MB
SF: Detected MX25U3235F with page size 64 kB, total 4 MB
Flash: 4 MB
NAND: 132 MiB
PCIe0: link up
PCIe1: link up
  dev fn venID devID class rev  MBAR0  MBAR1  MBAR2  MBAR3
  00 00 168c 0046 00002 00 00000004 00000000 00000000 00000000
  dev fn venID devID class rev  MBAR0  MBAR1  MBAR2  MBAR3
  00 00 168c 0040 00002 00 00000004 00000000 00000000 00000000
Power: 802.3af POE
In: serial
Out: serial
Err: serial
Net: eth0
Radio: qca9983#0, qca9990#1
Reset: cold
**** Configuration Reset Requested by User ****
Clearing state... Checking OS image and flags
```


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

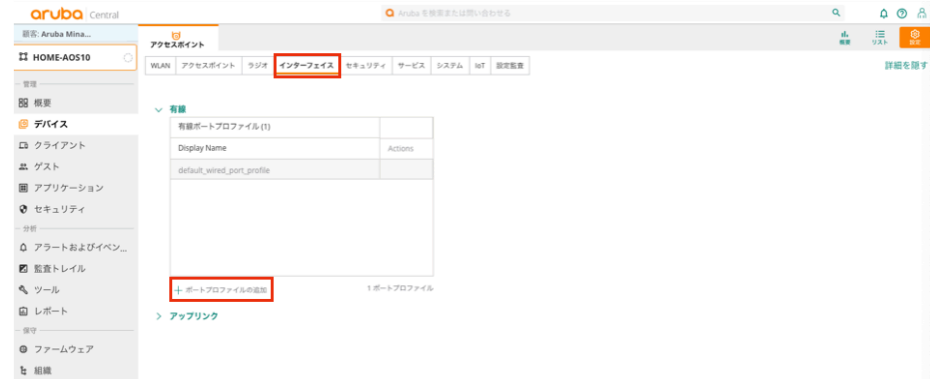


- ② 左メニューよりデバイスを選択し、右上の  をクリック

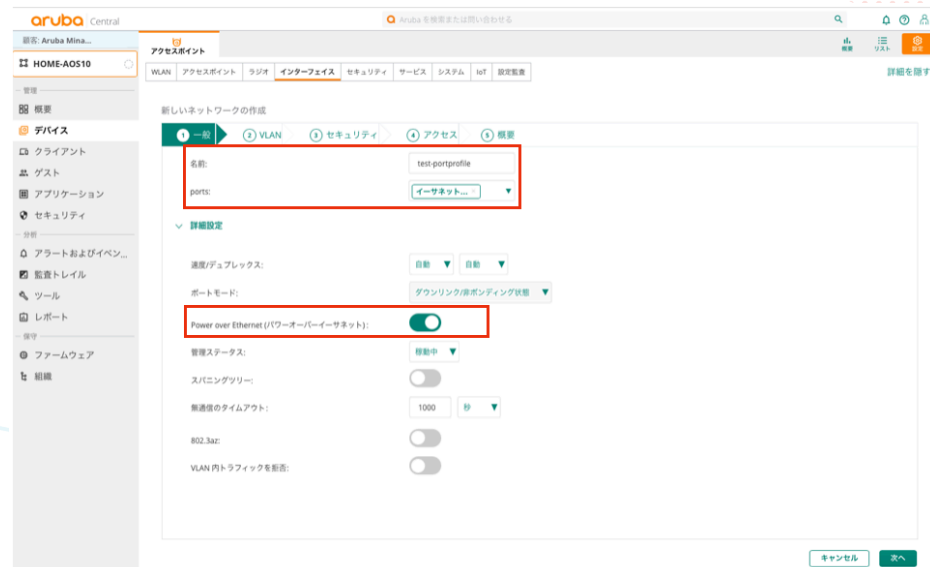


コメントの追加 [OY1]: 南くん担当スタート

- 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

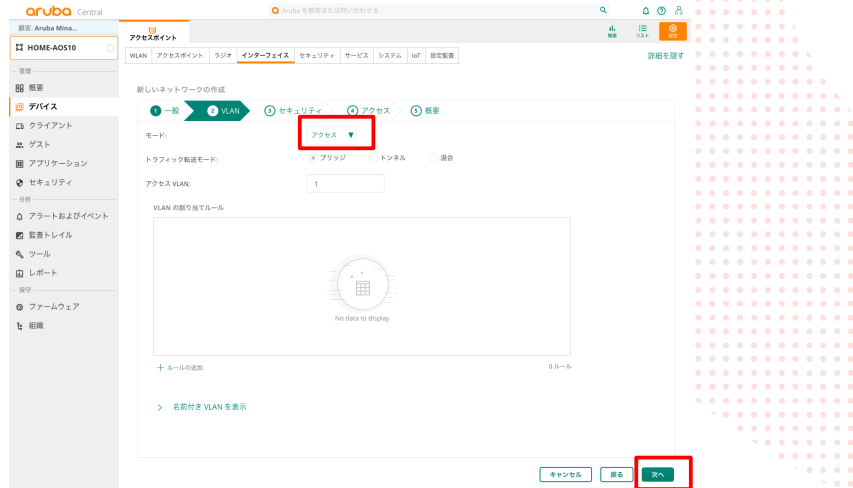


- ④ 名前は任意のものを設定し、当インターフェイスプロファイルを割り当てるポートを選択  
 ＊PoE 給電を行うことが可能な有線ポートを持つ AP もあるので、必要によって詳細設定を開き、PoE を”有効”と設定します。IP Phone や IP Camera に給電を行うことができます。  
 “次へ”をクリック





# 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

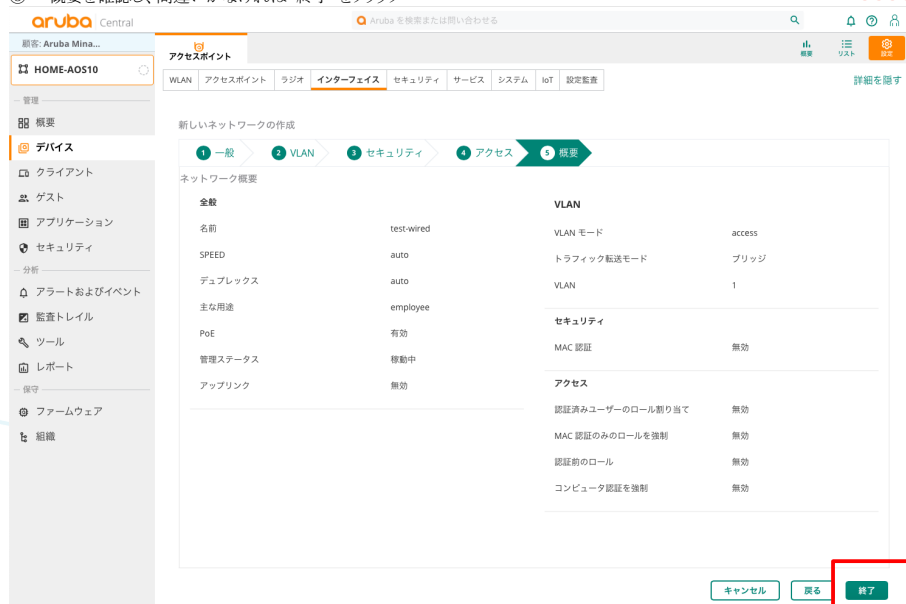


- ⑦ Trusted ポートを有効としたため、アクセスルールは制限なしになる  
“次へ”をクリック



The screenshot shows the 'New Network Creation' wizard in Aruba Central. The 'Access Rules' step is active, showing a progress bar with steps 1 (General), 2 (VLAN), 3 (Security), 4 (Access), and 5 (Summary). A warning message states: '△制限なしオプションを選択すると、ネットワークへの完全なアクセスが許可されます。これにより、潜在的なセキュリティの問題が生じる可能性があります。' (Selecting the unlimited option allows complete access to the network, which may cause potential security issues). The 'Access Rules' section shows a slider set to 'No Restrictions' (制限なし). Buttons at the bottom include 'キャンセル' (Cancel), '戻る' (Back), and '次へ' (Next).

- ⑧ 概要を確認し、間違いがなければ“終了”をクリック



The screenshot shows the 'Summary' step of the 'New Network Creation' wizard. The progress bar shows steps 1 (General), 2 (VLAN), 3 (Security), 4 (Access), and 5 (Summary). The 'Network Summary' section displays configuration details for the network 'test-wired'.

全般		VLAN	
名前	test-wired	VLAN モード	access
SPEED	auto	トラフィック転送モード	ブリッジ
デュプレックス	auto	VLAN	1
主な用途	employee		

セキュリティ	
PoE	有効
管理ステータス	稼働中
アップリンク	無効


アクセス	
認証済みユーザーのロール割り当て	無効
MAC 認証のみのロールを強制	無効
認証前のロール	無効
コンピュータ認証を強制	無効

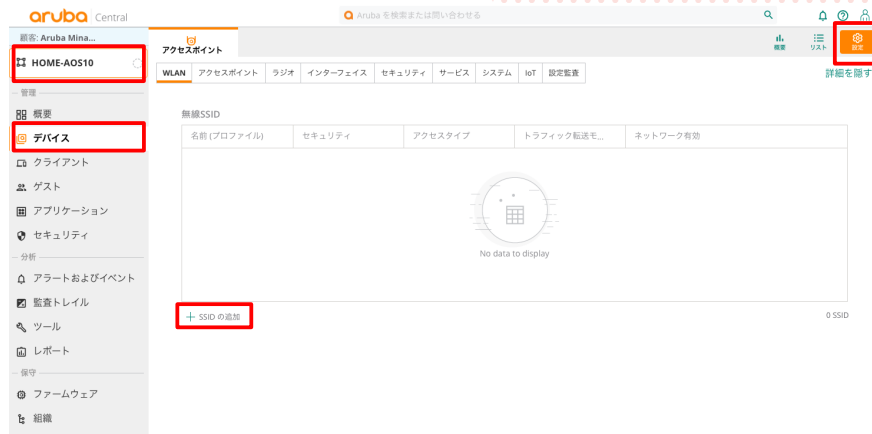
Buttons at the bottom include 'キャンセル' (Cancel), '戻る' (Back), and '終了' (End), which is highlighted with a red box.

## 6 SSID の設定

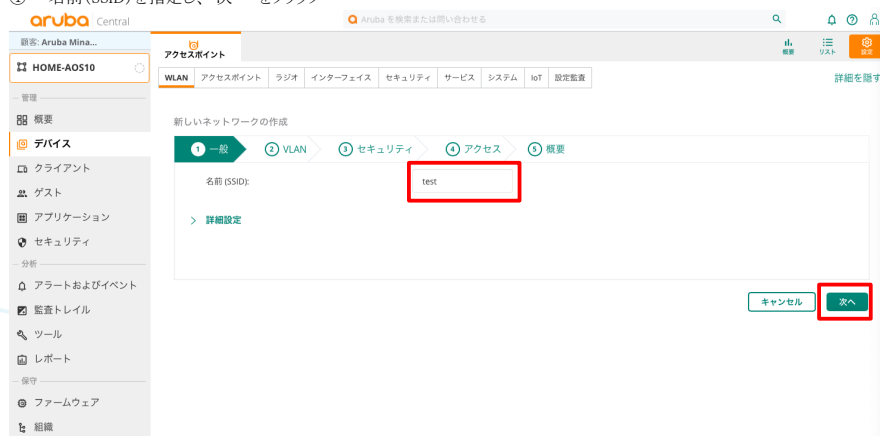
### 6.1 SSID の作成手順

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 アドレスやユーザ名等を指定可能です。

コメントの追加 [YM2]: トラフィック転送モードを追記

## 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。

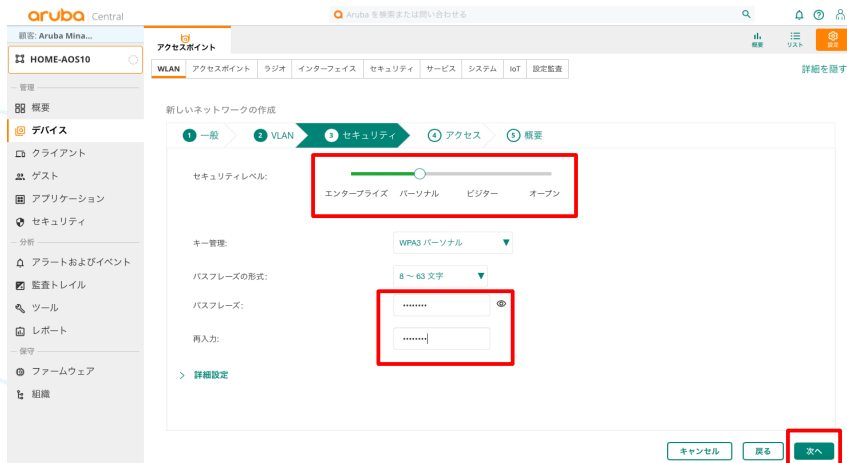
“ダイナミック” → Radius Attribute の利用や、特定文字列等をトリガーにして Dynamic VLAN を行うことができます。有線側には指定した VLAN Tag がついて出力されますので、AP と接続している Switch 側で Tag VLAN 設定をしてください。



## 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

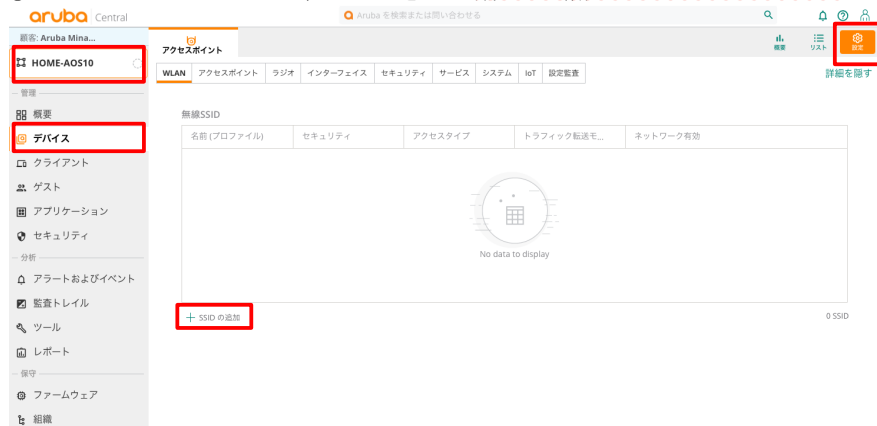
ロールベース/ネットワークベース/制限なし のアクセス制御を設定する



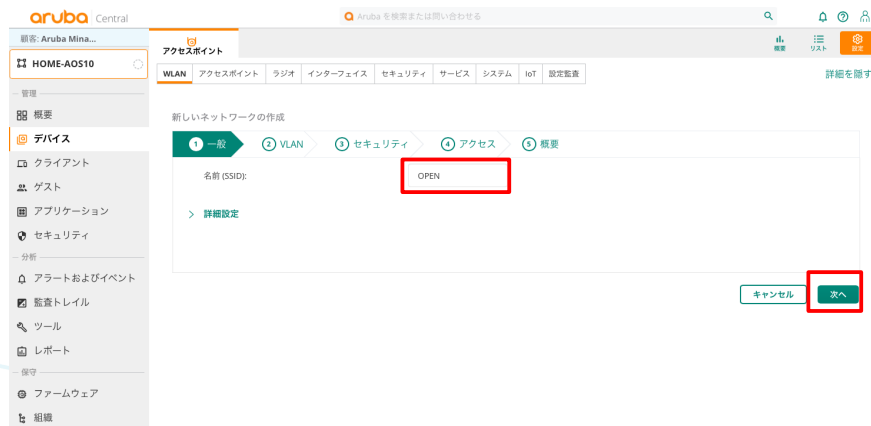
- ⑧ 概要で設定内容に間違いなければ“終了”ボタンをクリックすると、SSID が作成され、しばらくしてから Instant AP から SSID が出力し始める

## 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“名前付き VLAN を表示”から新規作成可能



The screenshot shows the Aruba Central web interface for configuring a new network. The left sidebar contains navigation menus for 'HOME-AOS10', '管理' (Management), '概要' (Overview), 'デバイス' (Devices), 'クライアント' (Clients), 'ゲスト' (Guests), 'アプリケーション' (Applications), 'セキュリティ' (Security), 'アラートおよびイベント' (Alerts and Events), '監査トレイル' (Audit Trail), 'ツール' (Tools), 'レポート' (Reports), 'ファームウェア' (Firmware), and '組織' (Organization). The main content area is titled '新しいネットワークの作成' (Create new network) and has tabs for 'WLAN', 'アクセスポイント', 'ラジオ', 'インターフェイス', 'セキュリティ', 'サービス', 'システム', 'IoT', and '設定監査'. The 'WLAN' tab is active, showing a step-by-step wizard: 1. 一般 (General), 2. VLAN (highlighted), 3. セキュリティ (Security), 4. アクセス (Access), 5. 概要 (Summary). Under 'トラフィック転送モード' (Traffic transfer mode), 'ブリッジ' (Bridge) is selected. Under 'クライアント VLAN の割り当て' (Client VLAN assignment), 'スタティック' (Static) is selected. The 'VLAN ID' dropdown is set to '10'. A link '> 名前付き VLAN を表示' (Show named VLAN) is present. At the bottom right, there are buttons for 'キャンセル' (Cancel), '戻る' (Back), and '次へ' (Next), with '次へ' being highlighted with a red box.

- ⑥ 暗号なし・暗号なし設定となるため セキュリティレベルにて“オープン”を選択



The screenshot shows the 'セキュリティ' (Security) step of the network configuration wizard. The 'セキュリティレベル' (Security level) dropdown is set to 'エンタープライズ' (Enterprise), but a red box highlights the 'オープン' (Open) option. A warning message states: '△ これはセキュリティ保護されていないネットワークです。ユーザーは認証なしでネットワークに接続します。' (This is an unsecured network. Users can connect to the network without authentication). Below this, the 'キー管理' (Key management) dropdown is set to 'エンハンスドオープン' (Enhanced Open). The '暗号化' (Encryption) field is set to 'なし' (None). A link '> 詳細設定' (Advanced settings) is available. At the bottom right, there are buttons for 'キャンセル' (Cancel), '戻る' (Back), and '次へ' (Next), with '次へ' being highlighted with a red box.

- 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




The screenshot shows the Aruba Central web interface for configuring a new network. The left sidebar contains navigation menus for '管理' (Management), 'デバイス' (Devices), '分析' (Analytics), '保守' (Maintenance), and '組織' (Organization). The main content area is titled '新しいネットワークの作成' (Create New Network) and includes a breadcrumb trail: 'アクセスポイント' > 'WLAN' > 'アクセスポイント' > 'ラジオ' > 'インターフェイス' > 'セキュリティ' > 'サービス' > 'システム' > 'IoT' > '設定監査'. The 'アクセス' (Access) step is highlighted in the progress bar. Below the progress bar, there are three radio button options for 'アクセスルール' (Access Rules): 'ロールベース' (Role-based), 'ネットワークベース' (Network-based), and '制限なし' (No restrictions). The '制限なし' option is selected. A warning message is displayed below the options: '△[制限なし] オプションを選択すると、ネットワークへの完全なアクセスが許可されます。これにより、潜在的なセキュリティの問題が生じる可能性があります。' (Selecting the [No restrictions] option allows full access to the network, which may lead to potential security issues). At the bottom right, there are three buttons: 'キャンセル' (Cancel), '戻る' (Back), and '次へ' (Next), with the '次へ' button highlighted by a red box.

- 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

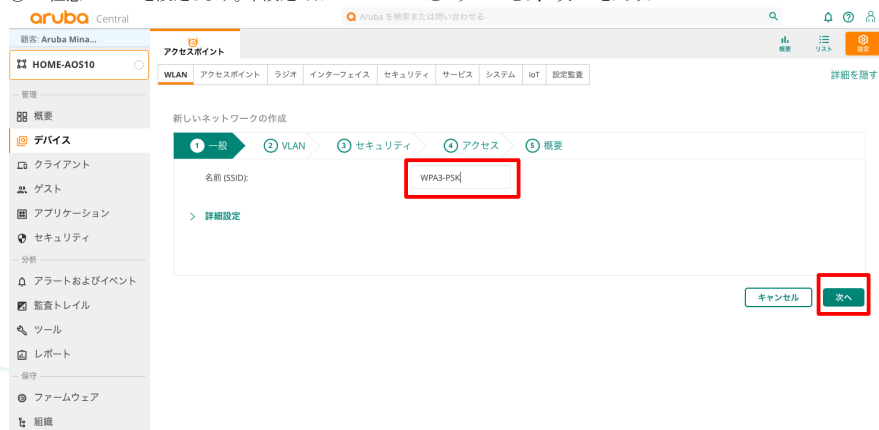


### 6.3 設定例)WPA3-PSK

- 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-PSK”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“名前付き VLAN を表示”から新規作成可能



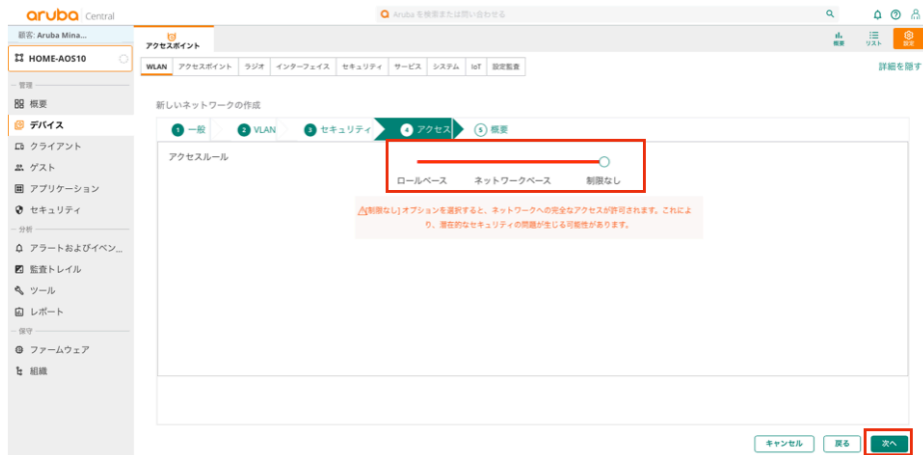
The screenshot shows the '新しいネットワークの作成' (Create New Network) wizard in the 'VLAN' tab. The 'トラフィック転送モード' (Traffic Transfer Mode) is set to 'ブリッジ' (Bridge). The 'クライアント VLAN の割り当て' (Client VLAN Assignment) is set to 'スタティック' (Static). The 'VLAN ID' is set to '20'. The '名前付き VLAN を表示' (Show Named VLAN) link is visible. The '次へ' (Next) button is highlighted.

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




The screenshot shows the '新しいネットワークの作成' (Create New Network) wizard in the 'セキュリティ' (Security) tab. The 'セキュリティレベル' (Security Level) is set to 'パーソナル' (Personal). The 'キー管理' (Key Management) is set to 'WPA3 パーソナル' (WPA3 Personal). The 'パスフレーズの形式' (Passphrase Format) is set to '8 ~ 63 文字' (8 ~ 63 characters). The 'パスフレーズ' (Passphrase) field is empty, and the '再入力' (Re-enter) field is also empty. The '詳細設定' (Advanced Settings) link is visible. The '次へ' (Next) button is highlighted.

- 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



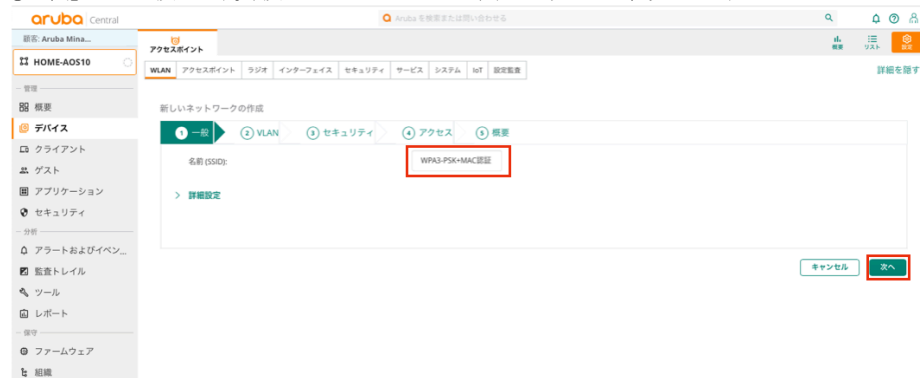
- ⑧ 概要で設定内容に間違いがないことを確認し、終了ボタンをクリックすると、SSID=WPA3-PSK が作成され、全ての Instant AP から出力される

#### 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



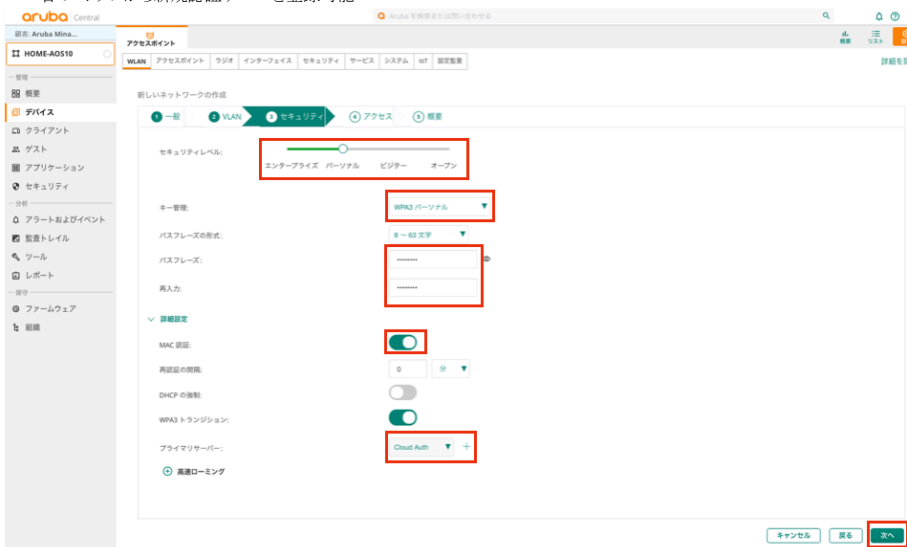
- ④ 任意の SSID を設定します。本設定では“WPA3-PSK+MAC 認証”という SSID とし、“次へ”をクリック



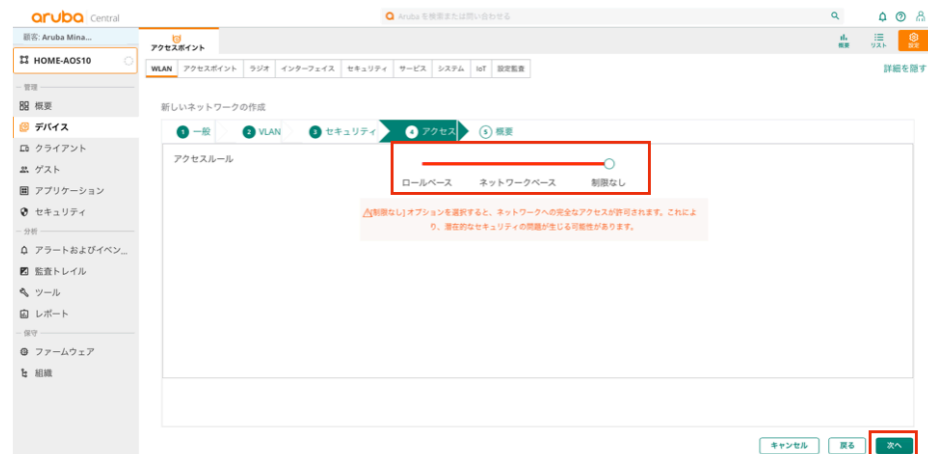
- ⑤ SSID と VLAN との紐付けを行う  
 本設定ではトラフィック転送モードを“ブリッジ”、SSID=WPA3-PSK+MAC 認証と VLAN30 を紐付けるため“スタティック”を選択し、VLAN ID に “30” を入力  
 VLAN は“名前付き VLAN を表示”から新規作成可能



- ⑥ セキュリティレベルにおいて、“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

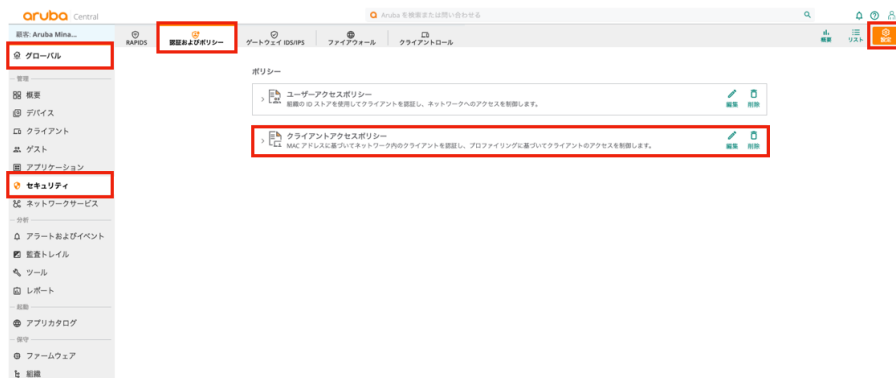


- ⑦ 本設定では、アクセスルール制限をしないため、“制限なし”を選択



- ⑧ MAC アドレスの登録

Aruba 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

RAPIDS

登録およびポリシー

ゲートウェイ IPS/IPS

ファイアウォール

クライアントロール

検索

リスト

設定

MAC 認証

ネットワーク上のクライアントを MAC アドレスに基づいて管理、認証します。

許可された MAC アドレス (2)

クライアントデバイスの MAC アドレスがネットワークへのアクセスを許可されました。

検索

+

下

上

MAC アドレス	クライアント名
5K	Client-1
01	Test

Items per page: 5 1 - 2 of 2

クライアントプロファイルタグとクライアントロールのマッピング (1)

クライアントプロファイルタグをクライアントロールに関連付け、優先順位の高いものから順番に当てます。

+

クライアントプロファイルタグ	クライアントロール
未設定	authenticated ▲

Wi-Fi Easy Connect™ サービス

Wi-Fi Easy Connect™ は、Wi-Fi ネットワークに接続する際の信頼性を高め、ユーザーエクスペリエンスを向上させます。

WLAN で使用

Select an option

Aruba UXI センサー

開始

キャンセル

保存

## MAC ベースのクライアントを追加

MAC アドレス \*

000011112222

例: 0123456789AB または 01:23:45:67:89:AB

クライアント名 \*

client-X

キャンセル

保存

MAC アドレス一覧に追加されていることを確認する

MAC 認証  
ネットワーク上のクライアントを MAC アドレスに基づいて管理、認証します。

許可された MAC アドレス (3)  
クライアントデバイスの MAC アドレスがネットワークへのアクセスを許可されました。

MAC アドレス	クライアント名
9C	Client-1
01	Test
00:00:11:11:22:22 (new)	client-x

Items per page: 5 1 - 3 of 3

クライアントプロファイルタグとクライアントロールのマッピング (1)  
クライアントプロファイルタグをクライアントロールに関連付け、優先順位の高いものから順番に並びます。

クライアントプロファイルタグ	クライアントロール
未設定	authenticated

Wi-Fi Easy Connect™ サービス  
Wi-Fi Easy Connect™ は、Wi-Fi® ネットワークに機器を接続する際の複雑さを軽減し、ユーザーエクスペリエンスを向上させます。

WLAN で使用  
Select an option

Aruba UX センサー  
無効 ☒

キャンセル 保存

- 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

MAC 認証  
ネットワーク上のクライアントを MAC アドレスに基づいて管理、認証します。

許可された MAC アドレス (3)  
クライアントデバイスの MAC アドレスがネットワークへのアクセスを許可されました。

MAC アドレス	クライアント名
9C	Client-1
01	Test
00:00:11:11:22:22 (new)	client-x

Items per page: 5 1 - 3 of 3

クライアントプロファイルタグとクライアントロールのマッピング (2)  
クライアントプロファイルタグをクライアントロールに関連付け、優先順位の高いものから順番に並びます。

クライアントプロファイルタグ	クライアントロール
Mobile & Gadgets	WPA3-PSK+MAC
未設定	wired-SetMetIp

Wi-Fi Easy Connect™ サービス  
Wi-Fi Easy Connect™ は、Wi-Fi® ネットワークに機器を接続する際の複雑さを軽減し、ユーザーエクスペリエンスを向上させます。

WLAN で使用  
Select an option


Aruba UX センサー  
無効 ☒

キャンセル 保存

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+MAC が作成され、全ての AP から出力される



## 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“名前付き VLAN を表示”から新規作成可能



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

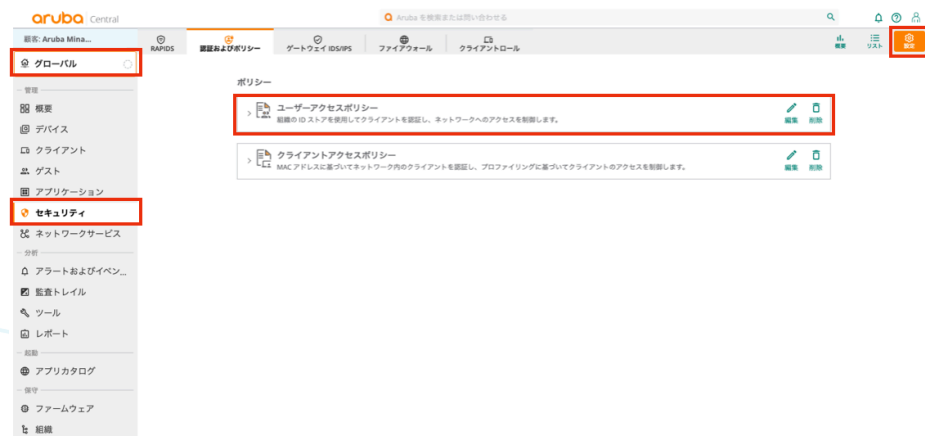


- ⑦ 本設定では、アクセスルール制限をしないため、“制限なし”を選択



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 Instant 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いただきます)

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

ユーザー認証  
組織の ID ストアを使用してクライアントを認証し、ネットワークへのアクセスを制御します。

ユーザー情報はどこに保存されていますか? Microsoft Azure AD 接続済み

ID プロバイダ  
Microsoft Azure AD

Microsoft Azure AD 向けクイックスタートガイド

テナント ID  
9da0b485-3098-42a0-8180-c360bcaaf48

クライアント ID  
d39857a5-001f-46de-9b72-2ef4309048f

クライアント秘密キー 表示

リダイレクト URI のコピー

接続

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

ユーザーグループとクライアントロールのマッピング (1)

ID ストアのユーザーグループをクライアントロールに関連付け、優先順位の高いものから順番に並べます。

ユーザーグループ	クライアントロール
不特定	Dot1x-CloudAuth

## ネットワークプロファイル

コンピューターやスマート デバイスにネットワーク プロファイルをインストールして、ネットワークへの接続を容易にすることができます。Aruba Onboard アプリケーションを使用して、プロファイルを自動的にインストールし、ダウンロード可能なリンクをユーザーと共有します。

組織名  
Aruba Minami

Aruba Onboard モバイルアプリレビュー

非 Passpoint クライアント用の WLAN

Dot1x-CloudAuth



## MPSK


ユーザーは、クライアントをネットワークに接続するための独自の Wi-Fi パスワードを持つことができます。パスワードは、パスワードポータルからログインした後、各ユーザーが利用できます。

MPSK WLAN は使用できません。①

キャンセル

保存

## 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

コメントの追加 [OY3]: 南くん担当ゴール



- 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“名前付き VLAN を表示”から新規作成可能

Aruba Central 画面のスクリーンショット。新しいネットワークの作成 - VLAN ステップ。トラフィック転送モードがブリッジに設定され、スタティックモードで VLAN ID が 50 に設定されている。画面には「名前付き VLAN を表示」のリンクと「次へ」ボタンが確認できる。

- 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  
プライマリサーバー項目で“+”から RADIUS サーバーを登録する


Aruba Central 画面のスクリーンショット。新しいネットワークの作成 - セキュリティ ステップ。セキュリティレベルがエンタープライズに設定され、キー管理が WPA3 エンタープライズ (COM 128) に設定されている。プライマリサーバー項目には「+」ボタンがあり、その下に「このフィールドは必須です。」というメッセージが表示されている。画面には「詳細設定」のリンクと「次へ」ボタンが確認できる。

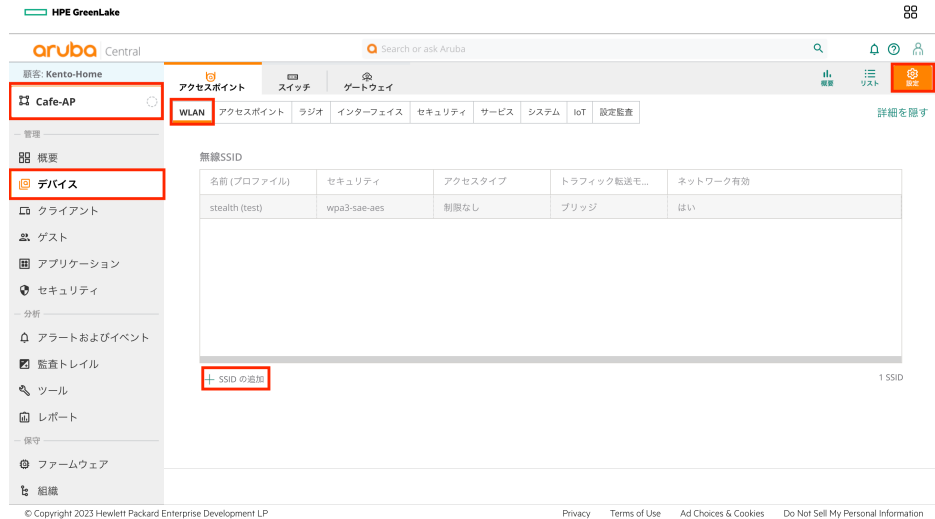
- ⑦ Radius サーバ名、IP アドレス、共有キー(シークレットキー)を入力し”OK”をクリック

- 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)

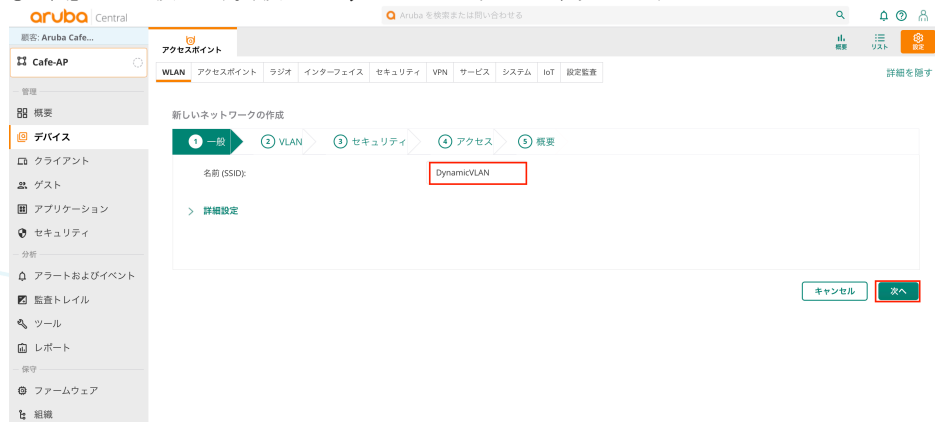
- ① フィルターアイコンより SSID を作成するグループを選択
- ② 左メニューより“デバイス”を選択し、右上の  ボタンをクリック
- ③ アクセスポイントタブ内の WLAN より、“+ SSID の追加”から新規 SSID を作成



Aruba Central interface showing the WLAN configuration page for 'Cafe-AP'. The left sidebar has 'デバイス' (Devices) selected. The main area shows a table of wireless SSIDs. A red box highlights the '+ SSID の追加' button at the bottom left of the table.

名前 (プロファイル)	セキュリティ	アクセスタイプ	トラフィック転送モ...	ネットワーク有効
stealth (test)	wpa3-sae-aes	制限なし	ブリッジ	はい

- 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



Aruba Central interface showing the 'DynamicVLAN' SSID configuration page. The left sidebar has 'デバイス' (Devices) selected. The main area shows the '新しいネットワークの作成' (Create new network) wizard. A red box highlights the 'DynamicVLAN' text in the '名前 (SSID):' field. The '次へ' (Next) button is highlighted with a red box.

新しいネットワークの作成

1 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要

名前 (SSID): DynamicVLAN

> 詳細設定

キャンセル 次へ



- 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

本設定ではトラフィック転送モードを“ブリッジ”、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  
VLAN の割り当てルール欄の“+ルールを追加”ボタンをクリック  
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

HPE GreenLake

aruba Central

検索 or ask Aruba

名前: Kento-Home

管理

概要

デバイス

クライアント

ゲスト

アプリケーション

セキュリティ

分析

アラートおよびイベント

監査トレイル

ツール

レポート

保守

ファームウェア

組織

アクセスポイント

スイッチ

ゲートウェイ

WLAN

アクセスポイント

ラジオ

インターフェイス

セキュリティ

サービス

システム

IoT

設定監査

詳細を隠す

新しいネットワークの作成

1 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要

トラフィック転送モード: ☒ ブリッジ ☐ トンネル ☐ 混合

クライアント VLAN の割り当て: ☐ スタティック ☒ ダイナミック ☐ ネイティブ VLAN

VLAN の割り当てルール

デフォルト VLAN: 1

+ ルールの追加

1 ルール

> 名前付き VLAN を表示

キャンセル 戻る 次へ

© Copyright 2023 Hewlett Packard Enterprise Development LP

Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

VLAN の割り当てルールの編集

属性: Tunnel-Private-Group-Id オペレータ: 次に一致 文字列: VLAN-ID VLAN: VLAN20[20]

キャンセル OK

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 10.215

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


The screenshot shows the Aruba Central web interface. The left sidebar contains navigation links for various management tasks. The main content area is titled '新しいネットワークの作成' (Create new network) and shows a progress bar with five steps: 1. General, 2. VLAN, 3. Security, 4. Access (highlighted), and 5. Summary. Under the 'Access' step, the 'Access rules' section shows three radio button options: 'Rule-based', 'Network-based', and 'No restrictions'. The 'No restrictions' option is selected. Below this, a warning message states: '△[制限なし]オプションを選択すると、ネットワークへの完全なアクセスが許可されます。これにより、潜在的なセキュリティの問題が生じる可能性があります。' (Selecting the [No restrictions] option allows complete access to the network, which may lead to potential security issues). At the bottom right, there are three buttons: 'キャンセル' (Cancel), '戻る' (Back), and '次へ' (Next), with the '次へ' button highlighted by a red box.

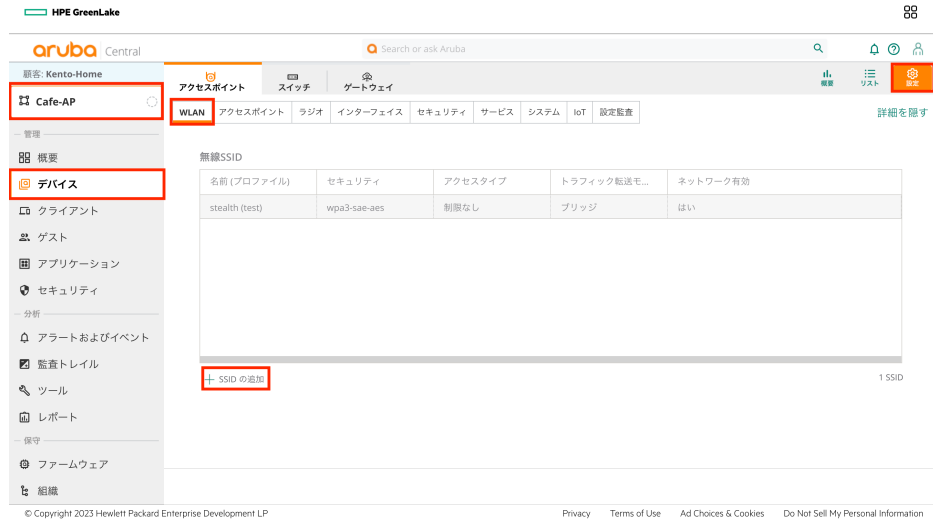
© Copyright 2023 Hewlett Packard Enterprise Development LP

[Privacy](#) [Terms of Use](#) [Ad Choices & Cookies](#) [Do Not Sell My Personal Information](#)

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)クラウドゲスト

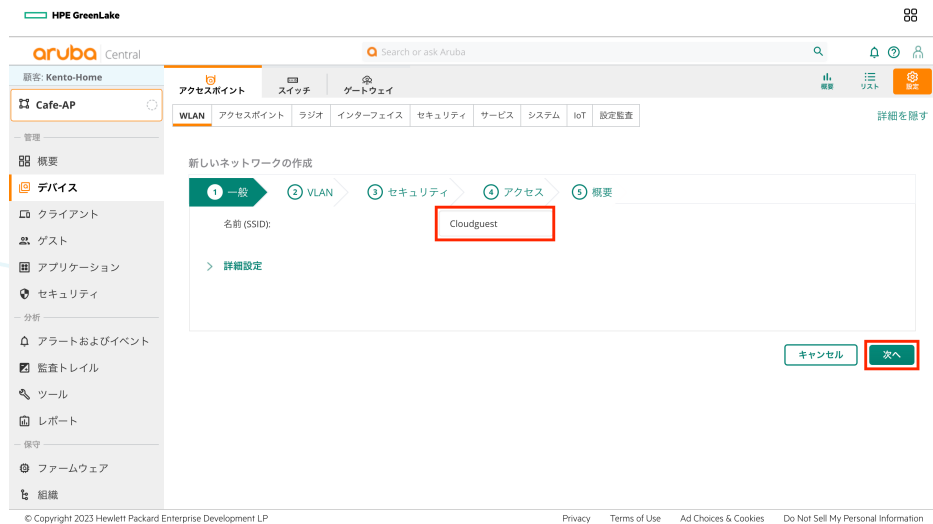
- ① フィルターアイコンより SSID を作成するグループを選択
- ② 左メニューより“デバイス”を選択し、右上の  ボタンをクリック
- ③ アクセスポイントタブ内の WLAN より、“+ SSID の追加”から新規 SSID を作成



Aruba Central 画面のスクリーンショット。左側のナビゲーションメニューで「デバイス」が選択されています。中央のタブで「WLAN」が選択されており、その下に「無線SSID」のテーブルが表示されています。テーブルには「名前 (プロファイル)」、「セキュリティ」、「アクセスタイプ」、「トラフィック転送モ...」、「ネットワーク有効」の列があります。テーブルの下部には「+ SSID の追加」ボタンが赤い枠で囲まれています。

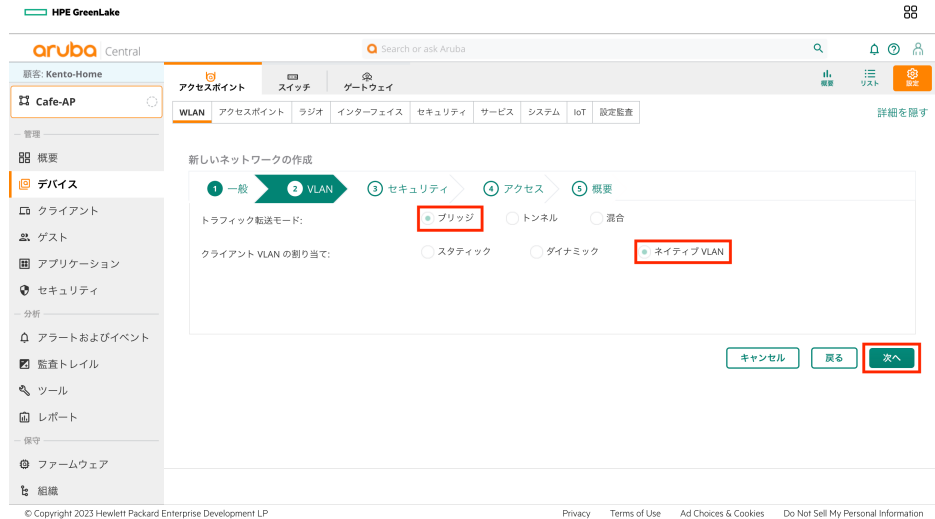
名前 (プロファイル)	セキュリティ	アクセスタイプ	トラフィック転送モ...	ネットワーク有効
stealth (test)	wpa3-sae-aes	制限なし	ブリッジ	はい

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



Aruba Central 画面のスクリーンショット。左側のナビゲーションメニューで「デバイス」が選択されています。中央のタブで「WLAN」が選択されており、その下に「新しいネットワークの作成」のウィザードが表示されています。ウィザードのステップは「1 一般」、「2 VLAN」、「3 セキュリティ」、「4 アクセス」、「5 概要」です。現在のステップ「一般」では「名前 (SSID):」のフィールドに「Cloudguest」が入力されています。右下には「キャンセル」と「次へ」のボタンがあり、「次へ」ボタンが赤い枠で囲まれています。

- ⑤ 本設定ではトラフィック転送モードを“ブリッジ”、クライアントVLANの割り当てにおいて、“ネイティブVLAN”を選択

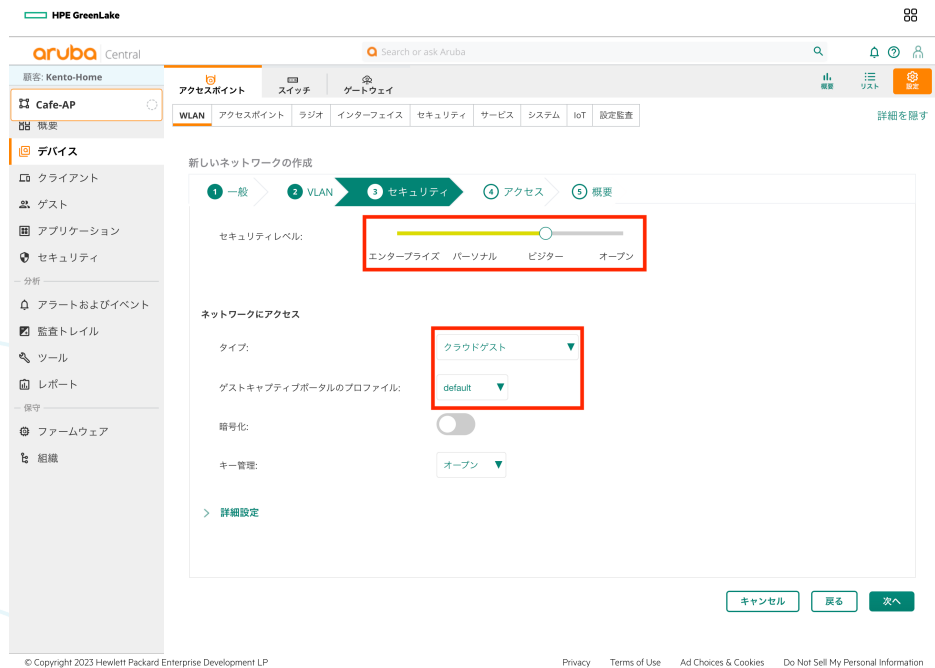


The screenshot shows the Aruba Central web interface for a new network setup. The left sidebar lists navigation options like '概要' (Overview), 'デバイス' (Devices), 'クライアント' (Clients), 'ゲスト' (Guests), 'アプリケーション' (Applications), 'セキュリティ' (Security), 'アラートおよびイベント' (Alerts and Events), '監査トレイル' (Audit Trail), 'ツール' (Tools), 'レポート' (Reports), 'ファームウェア' (Firmware), and '組織' (Organization). The main content area is titled '新しいネットワークの作成' (Create new network) and shows a progress bar with five steps: 1. 一般 (General), 2. VLAN, 3. セキュリティ (Security), 4. アクセス (Access), and 5. 概要 (Overview). The 'VLAN' step is currently active. Under 'トラフィック転送モード:' (Traffic transfer mode), the 'ブリッジ' (Bridge) option is selected. Under 'クライアントVLANの割り当て:' (Client VLAN assignment), the 'ネイティブVLAN' (Native VLAN) option is selected. At the bottom right, there are buttons for 'キャンセル' (Cancel), '戻る' (Back), and '次へ' (Next).

© Copyright 2023 Hewlett Packard Enterprise Development LP

Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

- ⑥ セキュリティレベルにおいて、“ビジター”を選択  
⑦ タイプにおいて“クラウドゲスト”、ゲストキャプティブポータルのプロファイルにおいて“default”を選択



The screenshot shows the Aruba Central web interface for the 'セキュリティ' (Security) step of the new network setup. The progress bar shows steps 1. 一般 (General), 2. VLAN, 3. セキュリティ (Security), 4. アクセス (Access), and 5. 概要 (Overview). The 'セキュリティ' step is currently active. Under 'セキュリティレベル:' (Security level), a slider is shown with four options: 'エンタープライズ' (Enterprise), 'パーソナル' (Personal), 'ビジター' (Visitor), and 'オープン' (Open). The 'ビジター' option is selected. Under 'ネットワークにアクセス' (Access to network), there are three sections: 'タイプ:' (Type) with a dropdown menu set to 'クラウドゲスト' (Cloud guest), 'ゲストキャプティブポータルのプロファイル:' (Guest captive portal profile) with a dropdown menu set to 'default', and '暗号化:' (Encryption) with a toggle switch turned off. At the bottom right, there are buttons for 'キャンセル' (Cancel), '戻る' (Back), and '次へ' (Next).

© Copyright 2023 Hewlett Packard Enterprise Development LP

Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

- 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

The screenshot shows the Aruba Central web interface. The left sidebar contains navigation links for various management tasks. The main content area is titled '新しいネットワークの作成' (Create new network) and shows a multi-step process. Step 4, 'アクセス' (Access), is the current step. Under 'アクセスルール' (Access rules), three radio buttons are present: 'ルールベース' (Rule-based), 'ネットワークベース' (Network-based), and '制限なし' (No restrictions). The '制限なし' option is selected. A red box highlights this selection. Below the radio buttons, a warning message in Japanese states: '△[制限なし]オプションを選択すると、ネットワークへの完全なアクセスが許可されます。これにより、潜在的なセキュリティの問題が生じる可能性があります。' (Selecting the [No restrictions] option allows complete access to the network, which may lead to potential security issues). At the bottom right, three buttons are visible: 'キャンセル' (Cancel), '戻る' (Back), and '次へ' (Next), with the '次へ' button highlighted by a red box.

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=Cloudguest が作成され、全ての AP から出力される

## 6.9 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: Aruba 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

HPE GreenLake

aruba Central

検索: Kento-Home

検索 or ask Aruba

管理 止 三 リスト 設定

Cafe-AP

管理 概要 デバイス クライアント **ゲスト** アプリケーション セキュリティ アラートおよびイベント 監査トレイル ツール レポート 保守 フォームウェア 組織

ゲストアクセス

スプラッシュページ ビジター

ゲストアクセス > スプラッシュページ

スプラッシュページ (1)

名前	タイプ	状態
default	匿名	共有

5 10 25 50 1 ページあたり

10 < > 11 ページ 1/1

© Copyright 2023 Hewlett Packard Enterprise Development LP

Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

③ 任意のsplash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



HPE GreenLake

aruba Central

顧客: Kento-Home

検索 or ask Aruba

3 分間 検索 1/24/24 設定

カフェ-AP

デバイス

クライアント

ゲスト

アプリケーション

セキュリティ

分析

アラートおよびイベント

監査トレイル

ツール

レポート

保守

ファームウェア

組織

ゲストアクセス

スプラッシュページ ビジター

新しいスプラッシュページ

1 設定 2 カスタマイズ 3 ローカライゼーション

名前: mail-auth

タイプ: 匿名 認証済み Facebook Wi-Fi

ユーザー名/パスワード: ☒

自己登録: ☒

検証が必要: ☐

電子メールベース: ☒

電話ベース: ☐

有効期限:  日  時間  分

☒ 無制限

ソーシャルログイン: ☐

失敗した場合にインターネットを許可: ☐

コメントをアップロード: ☐

認証に成功した場合の動作: ☒ 元の URL に戻る ☐ リダイレクト URL

認証失敗のメッセージ:

セッションのタイムアウト:  日  時間  分

☐ MAC キャッシュの有効化

このプロファイルを共有: ☒

同時ログイン制限: 無制限

日次使用制限: ☒ 無制限 ☐ 時間基準  時間  分 ☐ データ基準  MB ユーザーごと

許可リスト URL:  + URL をさらに追加

スポンサーされたゲスト: ☐

キャンセル 次へ

## 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

HPE GreenLake

aruba Central

検索: Kento-Home

ゲストアクセス

スプラッシュページ ビジター

新しいスプラッシュページ

① 設定 ② カスタマイズ ③ ローカライゼーション

レイアウト: 模型、コンピュータ向け

背景色: #ffffff

ボタンの色: #0096d6

ヘッダーの塗りつぶし色:

ページのフォントの色: #bbbbbb

ロゴ: 参照...

背景イメージ: 参照...

④ 使用条件の設定

⑤ 広告の設定

キャンセル 戻る 次へ

© Copyright 2023 Hewlett Packard Enterprise Development LP


Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

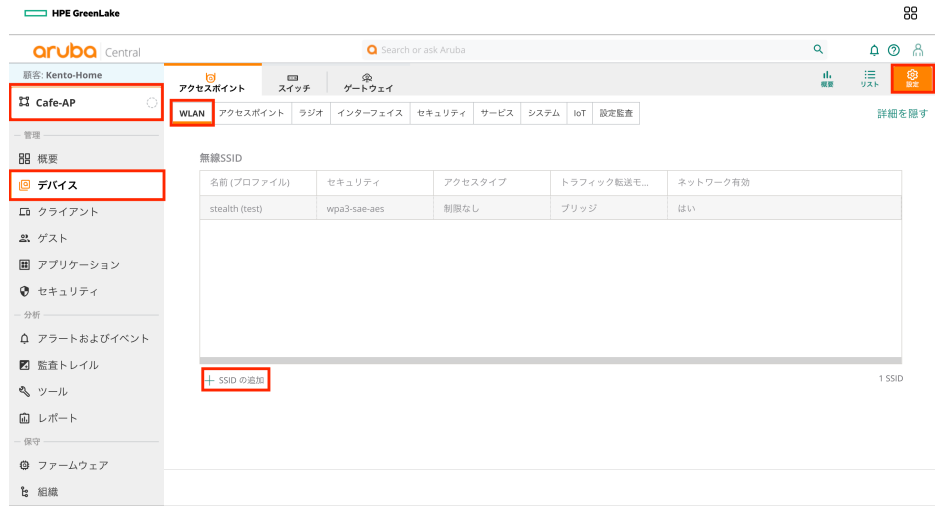
- ⑤ 必要に応じて各セクションをカスタマイズし、プレビューボタンから最終確認をし、終了をクリック

[キャンセル](#)
[戻る](#)
[プレビュー](#)
[終了](#)

## 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

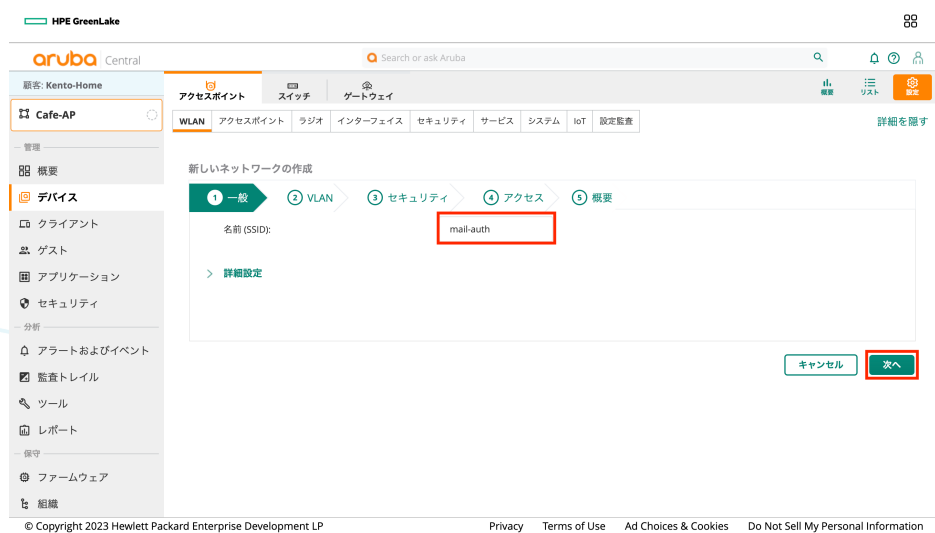


Aruba Central 画面のスクリーンショット。左側のナビゲーションメニューで「Cafe-AP」が選択されている。中央のタブで「WLAN」が選択されている。右側の「無線SSID」テーブルの下に「+ SSID の追加」ボタンがある。

名前 (プロファイル)	セキュリティ	アクセスタイプ	トラフィック転送モ...	ネットワーク有効
stealth (test)	wpa3-sae-aes	制限なし	ブリッジ	はい

© Copyright 2023 Hewlett Packard Enterprise Development LP Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

- 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



Aruba Central 画面のスクリーンショット。新しいネットワークの作成ウィザードの「VLAN」ステップがアクティブで、「mail-auth」が SSID として入力されている。右下に「次へ」ボタンがある。

新しいネットワークの作成

1 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要

名前 (SSID): mail-auth

> 詳細設定

キャンセル 次へ

- ⑨ 本設定ではトラフィック転送モードを“ブリッジ”、クライアント VLAN の割り当てにおいて、“ネイティブ VLAN”を選択

HPE GreenLake

aruba Central

検索 or ask Aruba

顧客: Kento-Home

Cafe-AP

管理

概要

デバイス

- クライアント
- ゲスト
- アプリケーション
- セキュリティ

分析

- アラートおよびイベント
- 監査トレイル
- ツール
- レポート

保守

- ファームウェア
- 組織

アクセスポイント

WLAN

新しいネットワークの作成

1 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要

トラフィック転送モード:

ブリッジ トンネル 混合

クライアント VLAN の割り当て:

スタティック ダイナミック ネイティブ VLAN

キャンセル 戻る 次へ

© Copyright 2023 Hewlett Packard Enterprise Development LP

Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

- ⑨ セキュリティレベルにおいて、“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

HPE GreenLake

aruba Central

検索 or ask Aruba

顧客: Kento-Home

Cafe-AP

管理

概要

デバイス

- クライアント
- ゲスト
- アプリケーション
- セキュリティ

分析

- アラートおよびイベント
- 監査トレイル
- ツール
- レポート

保守

- ファームウェア
- 組織

アクセスポイント

WLAN

新しいネットワークの作成

1 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要

セキュリティレベル:

エンタープライズ パーソナル ビジター オープン

ネットワークにアクセス

タイプ: クラウドゲスト

ゲストキャプティブポータルのプロファイル: mail-auth

暗号化: ☐

キー管理: オープン

> 詳細設定

キャンセル 戻る 次へ

© Copyright 2023 Hewlett Packard Enterprise Development LP

Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

- ⑩ 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

The screenshot shows the Aruba Central web interface. The left sidebar contains navigation links: 概要 (Overview), デバイス (Devices), クライアント (Clients), ゲスト (Guests), アプリケーション (Applications), セキュリティ (Security), アラートおよびイベント (Alerts and Events), 監査トレイル (Audit Trail), ツール (Tools), レポート (Reports), ファームウェア (Firmware), and 組織 (Organization). The main content area is titled '新しいネットワークの作成' (Create New Network) and shows a progress bar with five steps: 1. 一般 (General), 2. VLAN, 3. セキュリティ (Security), 4. アクセス (Access), and 5. 概要 (Overview). The 'アクセス' step is currently active. Below the progress bar, there are three radio button options: 'ルールベース' (Rule-based), 'ネットワークベース' (Network-based), and '制限なし' (No restrictions). The '制限なし' option is selected. A warning message is displayed below the options: '△[制限なし] オプションを選択すると、ネットワークへの完全なアクセスが許可されます。これにより、潜在的なセキュリティの問題が生じる可能性があります。' (△[No restrictions] Selecting this option allows full access to the network, which may lead to potential security issues). At the bottom right, there are three buttons: 'キャンセル' (Cancel), '戻る' (Back), and '次へ' (Next), with the '次へ' button highlighted by a red box.

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 AP から出力される



## 6.10 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”をクリック  
ステイルスモードを有効にする

The screenshot shows the Aruba Central interface for configuring a new network. The 'WLAN' tab is active, and the 'SSID' is set to 'test'. The 'Stealth Mode' (ステイルスモード) toggle is highlighted with a red box and is currently turned on. The 'WLAN' tab is selected in the top navigation bar.

新しいネットワークの作成

1 一般 2 VLAN 3 セキュリティ 4 アクセス 5 概要

名前 (SSID): test

▼ 詳細設定

- ブロードキャスト/マルチキャスト
- 送信レート (レガシーのみ)
- ビーコンレート
- 帯域幅制御
- Wi-Fi マルチメディア
- その他

ESSID: test

周波数帯: ☒ 2.4 GHz ☒ 5 GHz ☐ 6 GHz

6GHz メッシュで無効化: ☐

無通信のタイムアウト: 1000 秒

ステイルスモード: ☒

最大クライアント数のしきい値: 64

ローカルプロンプト要求のしきい値: ☐ 自動 ☒ 手動 0

認証要求の最小 SNR: ☐ Automatic ☒ Manual 0

無通信状態の端末へ deauth を送信: ☐

アップリンクなしで使用可能: ☐

次の場合に SSID を無効化: なし ▼

VLAN 内トラフィックを拒否: ☐

管理フレーム保護: ☐

ファインタイムング測定 (802.11mc) レスポンダモード: ☐

AP 名のアドバタイズ: ☐

時間範囲のプロファイル

キャンセル 次へ


## 6.11 ユーザ同士の通信制御 (User Isolation) について

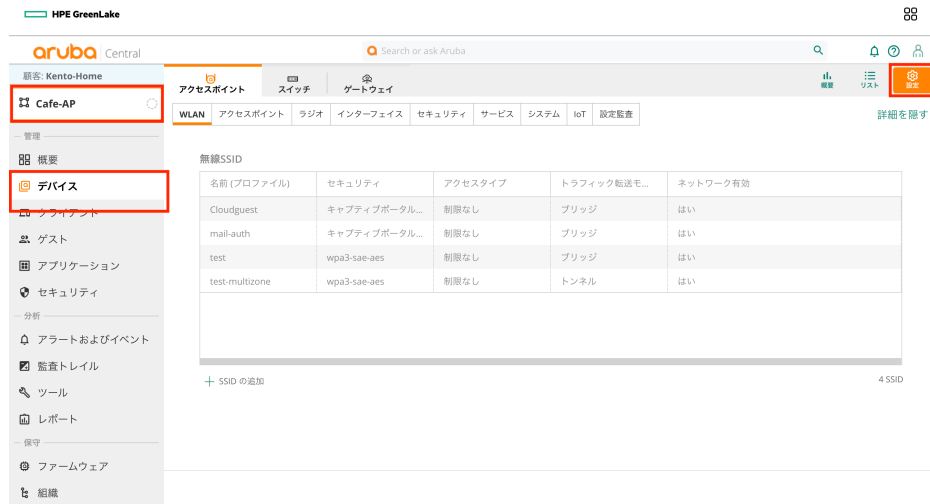
ゲスト用 SSID 等において、ユーザ同士の通信を禁止したい場合は WLAN 設定にて”詳細設定”をクリックし、”VLAN 内トラフィックを拒否”項目を有効にする

The screenshot shows the Aruba Central management console. On the left is a navigation menu with options like 'デバイス' (Devices), 'クライアント' (Clients), 'ゲスト' (Guests), 'アプリケーション' (Applications), 'セキュリティ' (Security), 'アラートおよびイベント' (Alerts and Events), '監査トレイル' (Audit Trail), 'ツール' (Tools), 'レポート' (Reports), 'ファームウェア' (Firmware), and '組織' (Organization). The main content area is titled '新しいネットワークの作成' (Create new network) and has a breadcrumb trail: 一般 > VLAN > セキュリティ > アクセス > 概要. The 'VLAN' step is currently active. Under the '詳細設定' (Detailed Settings) tab, various configuration options are listed. The 'VLAN 内トラフィックを拒否' (Deny VLAN traffic) option is highlighted with a red box and is currently enabled (the toggle switch is turned on). Other options include 'ブロードキャスト/マルチキャスト' (Broadcast/Multicast), '送信レート (レガシーのみ)' (Transmit rate (legacy only)), 'ビーコンレート' (Beacon rate), '帯域幅制御' (Bandwidth control), 'Wi-Fi マルチメディア' (Wi-Fi Multimedia), and 'その他' (Other). At the bottom of the configuration area are 'キャンセル' (Cancel) and '次へ' (Next) buttons.

## 6.12 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



The screenshot shows the Aruba Central web interface. The left sidebar has a menu with 'Cafe-AP' and 'デバイス' (Devices) highlighted with red boxes. The main content area shows a table of wireless SSIDs. The table has columns for Name (Profile), Security, Access Type, Traffic Forwarding, and Network Status. There are 4 SSIDs listed.

名前 (プロファイル)	セキュリティ	アクセスタイプ	トラフィック転送モ...	ネットワーク有効
Cloudguest	キャプティブポータル...	制限なし	ブリッジ	はい
mail-auth	キャプティブポータル...	制限なし	ブリッジ	はい
test	wpa3-sae-aes	制限なし	ブリッジ	はい
test-multizone	wpa3-sae-aes	制限なし	トンネル	はい

コメントの追加 [OY5]: 横山くんゴール

- 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

HPE GreenLake

aruba Central

Search or ask Aruba

顧客: Kento-Home

Cafe-AP

管理

概要

デバイス

クライアント

ゲスト

アプリケーション

セキュリティ

分析

アラートおよびイベント

監査トレイル

ツール

レポート

保守

ファームウェア

アクセスポイント

スイッチ

ゲートウェイ

WLAN

アクセスポイント

ラジオ

インターフェイス

セキュリティ

サービス

システム

iOT

設定監査

詳細を隠す

システム

一般

管理者

メッシュ

時間ベースのサービス

この機能は NTP が必要です。

時間ベースのプロファイル

名前

時刻

アソシエーショ...

表示するデータがありません。

ログ

SNMP

プロキシ

IPM

© Copyright 2023 Hewlett Packard Enterprise Development LP

Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

## ⑤ 任意の名前、利用時間を指定し、OK をクリック

新しいプロファイル

名前: employee

タイプ: 定期的 ▼

繰り返し: ☒ 毎日 ☐ 毎週

毎日範囲: ☒ 月曜日～日曜日 (全日) ☐ 月曜日～金曜日 (平日) ☐ 土曜日～日曜日 (週末)

開始時間: 時間 8 分 0 ▼

終了時間: 時間 19 分 0 ▼

キャンセル OK

## 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

HPE GreenLake

aruba Central Search or ask Aruba

顧客: Kento-Home

管理 概要 デバイス クライアント ゲスト アプリケーション セキュリティ アラートおよびイベント 監査トレイル ツール レポート ファームウェア

アクセスポイント スイッチ ゲートウェイ

WLAN アクセスポイント ラジオ インターフェイス セキュリティ サービス システム IoT 設定監査

無線SSID

名前 (プロファイル)	セキュリティ	アクセスタイプ	トラフィック転送モ...	ネットワーク有効
Cloudguest	キャプティブポータル...	制限なし	ブリッジ	はい
mail-auth	キャプティブポータル...	制限なし	ブリッジ	はい
test	wpa3-sae-aes	制限なし	ブリッジ	はい
test-multizone	wpa3-sae-aes	制限なし	トンネル	はい

+ SSID の追加 4 SSID

詳細を隠す

© Copyright 2023 Hewlett Packard Enterprise Development LP Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

- 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。

HPE GreenLake

aruba Central

Search or ask Aruba

顧客: Kento-Home

Cafe-AP

管理

概要

デバイス

クライアント

ゲスト

アプリケーション

セキュリティ

分析

アラートおよびイベント

監査トレイル

ツール

レポート

保守

ファームウェア

アクセスポイント

スイッチ

ゲートウェイ

WLAN

アクセスポイント

ラジオ

インターフェイス

セキュリティ

サービス

システム

IoT

設定監査

詳細を隠す

ネットワーク > 設定 - test

一般 VLAN セキュリティ アクセス 概要

ESSID: test

▼ 詳細設定

ブロードキャスト/マルチキャスト

送信レート (レガシーのみ)

ビーコンレート

帯域幅制御

Wi-Fi マルチメディア

その他

時間範囲のプロファイル

この機能は NTP が必要です。

時間範囲のプロファイル ステータス

employee (Periodic Daily 08:00 - 19:00) 有効

新しい時間範囲プロファイル

メモ: 可視化はほぼ 1 時間ごとに行われます。

MON TUE WED THU FRI SAT SUN

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

有効な接続時間 無効な接続時間

キャンセル 設定の保存

## 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。  
本設定では仮想コントローラの接続が解除された際に、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

Aruba Central console screenshot showing the 'Alerts and Events' configuration page. The left sidebar has 'Alerts and Events' selected. The main area shows a table of alerts with columns for 'Alert Name', 'IP', 'Category', 'Severity', and 'Status'. The 'Alerts and Events' button in the top right is highlighted.

② アクセスポイントの中から“AP 切断”をクリック

Aruba Central console screenshot showing the 'Alerts and Events' configuration page. The left sidebar has 'Alerts and Events' selected. The main area shows a table of alerts with columns for 'Alert Name', 'IP', 'Category', 'Severity', and 'Status'. The 'Alerts and Events' button in the top right is highlighted.

コメントの追加 [OY6]: 南くんスタート

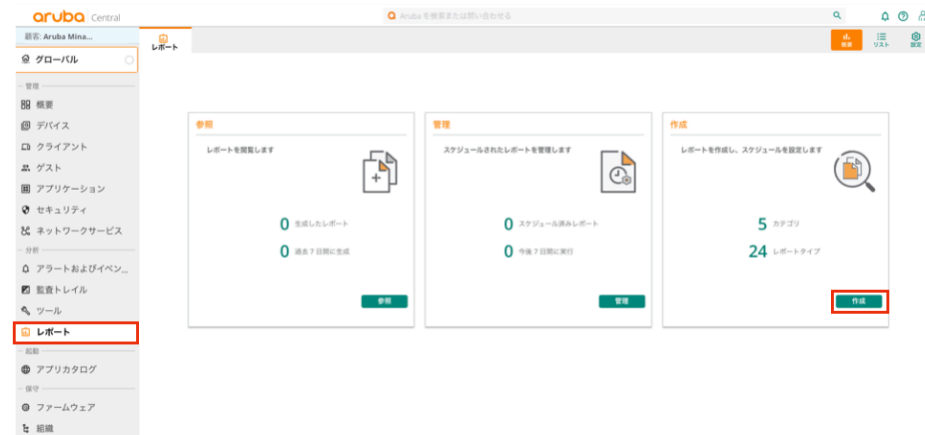
- ### 、通知を送るメールアドレスを指定する



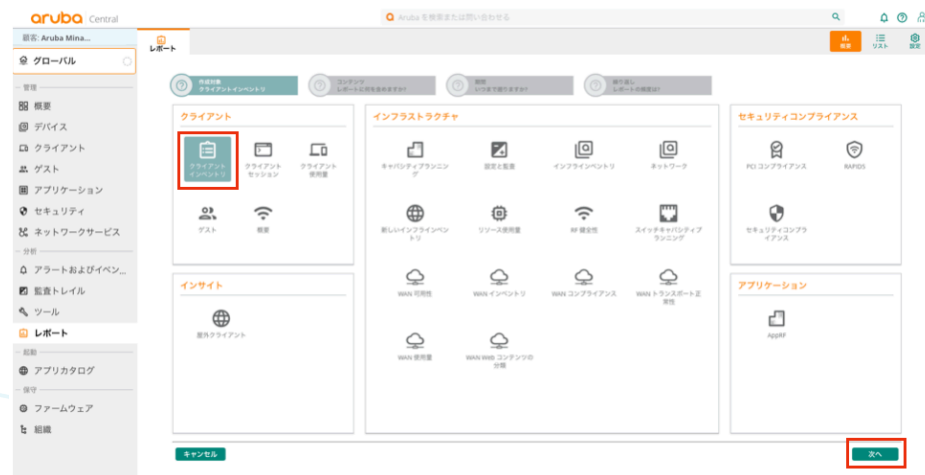
## 7.2 レポートの出力方法

Aruba Central では現在4カテゴリ、24 種類のレポートタイプを出力可能です。

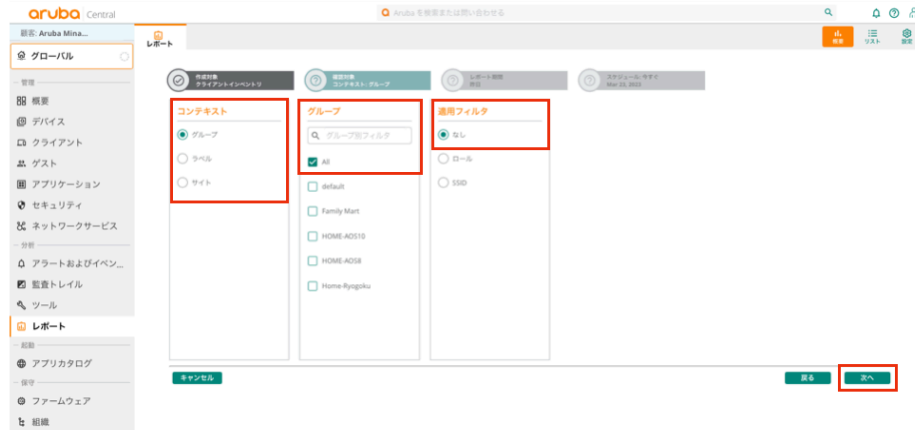
① 左メニューから“レポート”を選択し、“作成”ボタンから新規レポートを作成



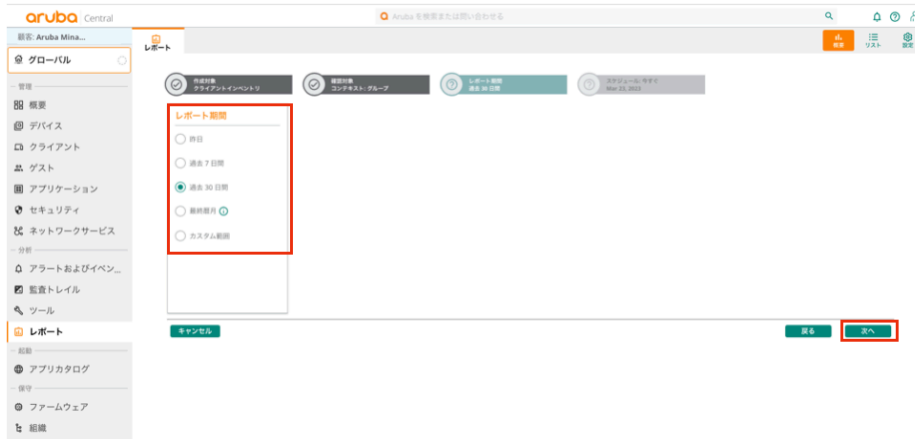
② どのタイプのレポートを作成するかを選択し、次へ



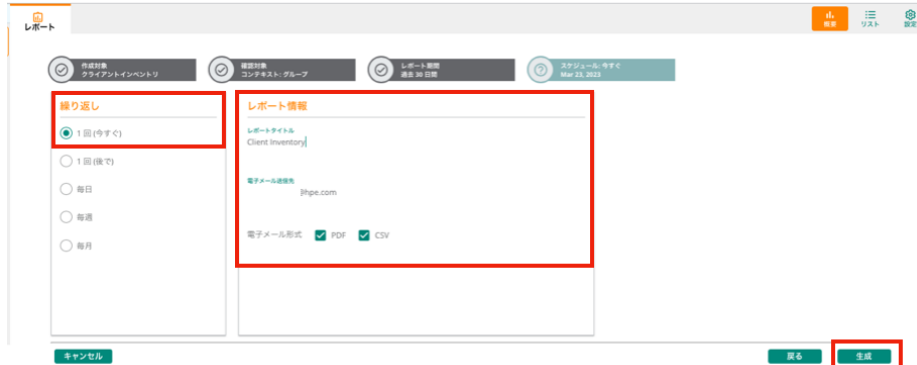
③ レポートを作成する確認対象を確定させ、次へ



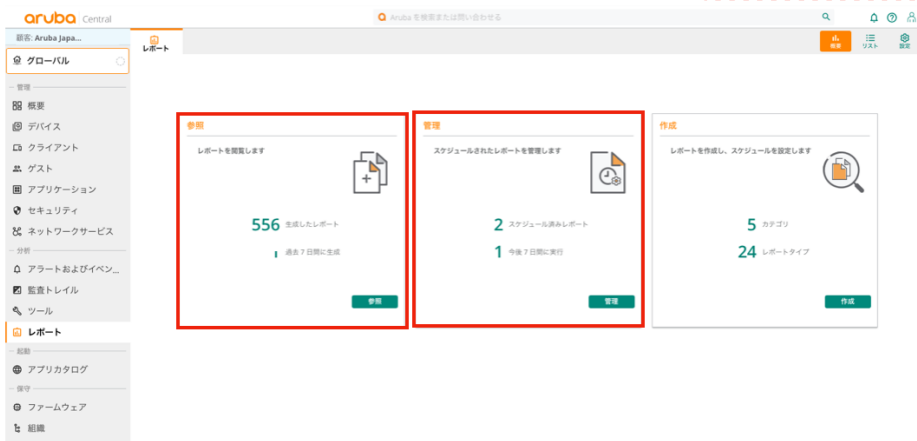
④ レポートに出力する期間を指定する



## 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。

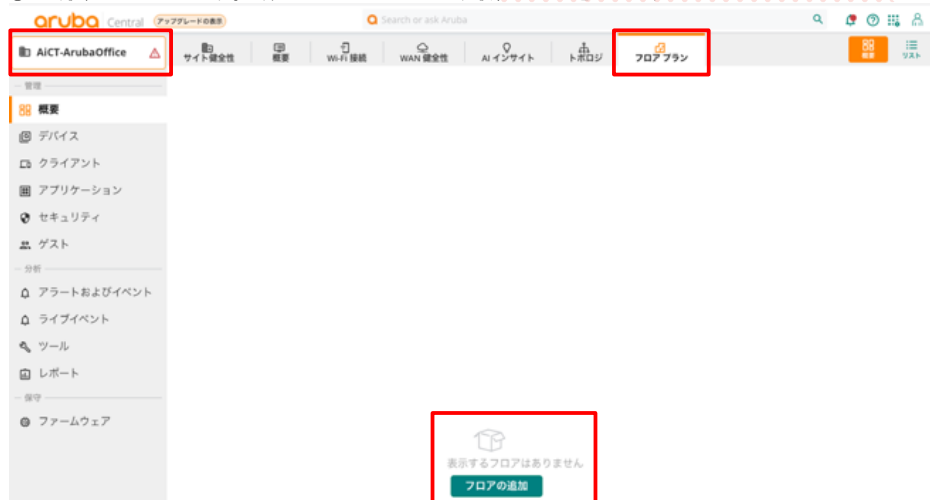


## 8 FLOORPLANS

### 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



- 新しいフロアプラン

フロアプランファイル

選択...

ファイルが選択されていません。

サポートされるファイル形式: jpg、jpeg、gif、bmp、pdf、および png。

フロア名

フロア 1

フロア番号

1.0

Save

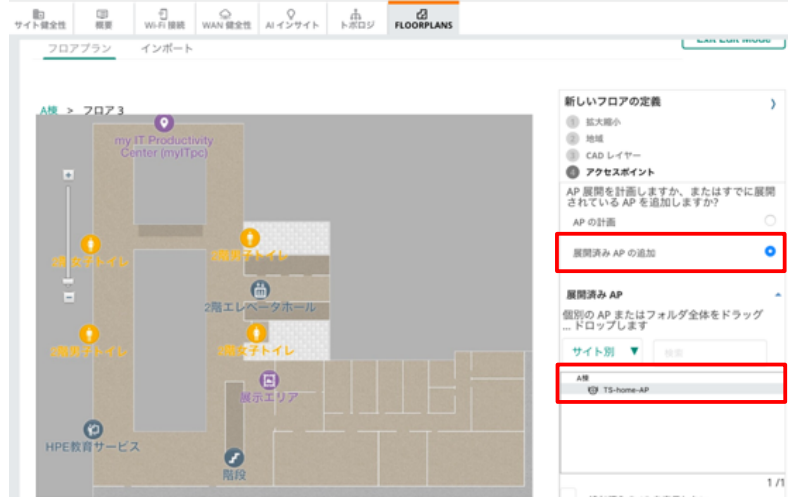
Cancel

-

## 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。

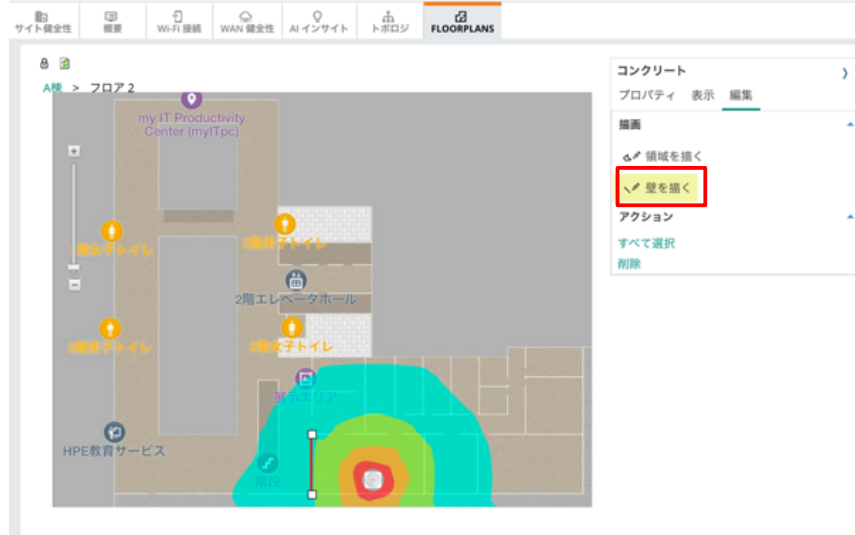


## B) 仮想的に AP を配置する場合

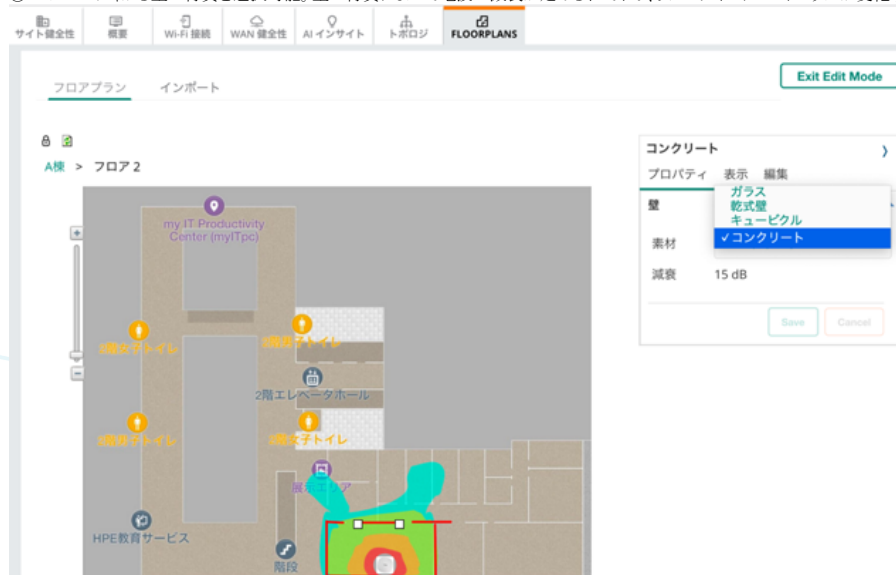
“AP の計画”より配置したいモデルを選択し“フロアプランに AP を追加”をクリックし終了



- 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。



## 10 AIOPs

## AIOPs について

AIOPs は AI Insights・AI Assist・AI Search の 3 つの AI の機能からなり立っています。今回は AI Insights に焦点を当ててご説明いたします。

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

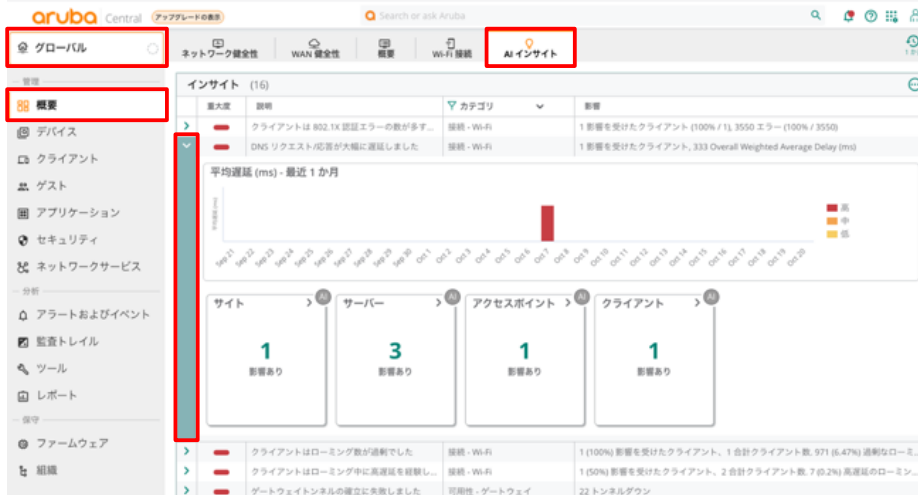
AI Insights のダッシュボードには、ネットワークに影響を与える可能性のあるイベントのレポートが表示されます。これは選択した時間範囲、特定のサイト・デバイスごとやクライアント毎のネットワークイベントのレポートが表示されます。

## 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。

- 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
- 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
- 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

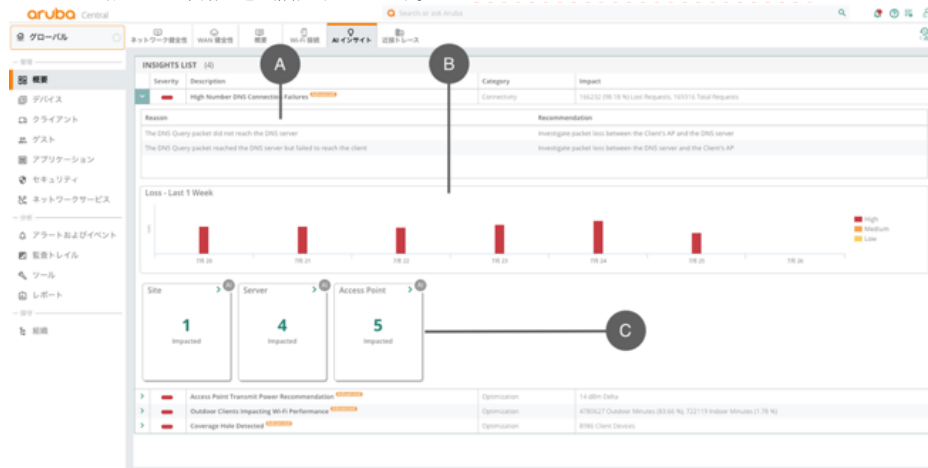


コメントの追加 [OY8]: 横山くんスタート



## 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。



## 11 メンテナンス

### 11.1 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。

Aruba Central 画面のスクリーンショット。左側のナビゲーションメニューで「ファームウェア」が選択されています。中央の「アクセスポイント (1)」テーブルには、IAP の情報が表示されています。右側の「アップグレード」ボタンが赤枠で囲まれています。

名前	サイト	現在のバージョン	推奨バージョン	アップグレードのステータス	コンプライアンスステータス
IAP	Home	10.4.0.0_86033	10.4.0.0_86033	ファームウェアは最新です	未設定

- ② ファームウェアのバージョン、アップグレードする日時を選択し“アップグレード”をクリック  
※AOS 10 から AOS 8 へダウングレードすることも適切なファームウェアを選択することで可能です。

「アクセスポイントファームウェアのアップグレード」ダイアログボックスのスクリーンショット。バージョン選択とアップグレード時期の指定が行われています。

コメントの追加 [YK9]: AOS10→AOS8 の手順も追加

## 11.2 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

顧客: Kento-Home

aruba Central

Search or ask Aruba

グローバル

管理

- 概要
- デバイス
- クライアント
- ゲスト
- アプリケーション
- セキュリティ
- ネットワークサービス

分析

- アラートおよびイベント
- 監査トレイル
- ツール
- レポート

保守

- ファームウェア

ネットワークチェック

デバイスチェック

コマンド

コンソール

ネットワークチェック

デバイスタイプとテストを選択し、パラメータを設定して、テストを実行します

デバイスタイプ	ソース	
アクセスポイント	IAP	
テスト	実行タイプ	ホスト名/IP アドレス
Ping テスト	ホスト名/IP アドレス	8.8.8.8

その他のテスト設定を表示

既にコマンドを実行しているデバイスで、新しく追加されたコマンドを実行してはなりません  
バッファスペースの問題があるデバイスの出力履歴は自動的に消去されます

実行

デバイス出力

デバイス

デバイス出力: IAP

デバイス

デバイス出力: IAP

Output Time: 2023-03-27 10:11:42 UTC

COMMAND=ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes

64 bytes from 8.8.8.8: icmp\_seq=1 ttl=118 time=4.3 ms

64 bytes from 8.8.8.8: icmp\_seq=2 ttl=118 time=4.0 ms

64 bytes from 8.8.8.8: icmp\_seq=3 ttl=118 time=3.9 ms

64 bytes from 8.8.8.8: icmp\_seq=4 ttl=118 time=4.7 ms

--- 8.8.8.8 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 3.9/3.9/4.7 ms

=== Troubleshooting session completed ===

Central では GUI から AP の CLI がひらけます

Central では GUI から AP の CLI がひらけます

- からスタートします。

## 13 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 Aruba Central 基本操作ガイド 入門編を参照

<https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/>

### デバイスインベントリからの削除方法

Aruba 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、Aruba Central 基本操作ガイド 入門編を参照

<https://www.arubanetworks.com/ja/resource/aruba-central-basic-operation-technical-guide/>

## 14 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 AP の “show tech support dump” および、”show tech support dump supplemental ” は必須となります。

以上

コメントの追加 [OY10]: 横山くんゴール