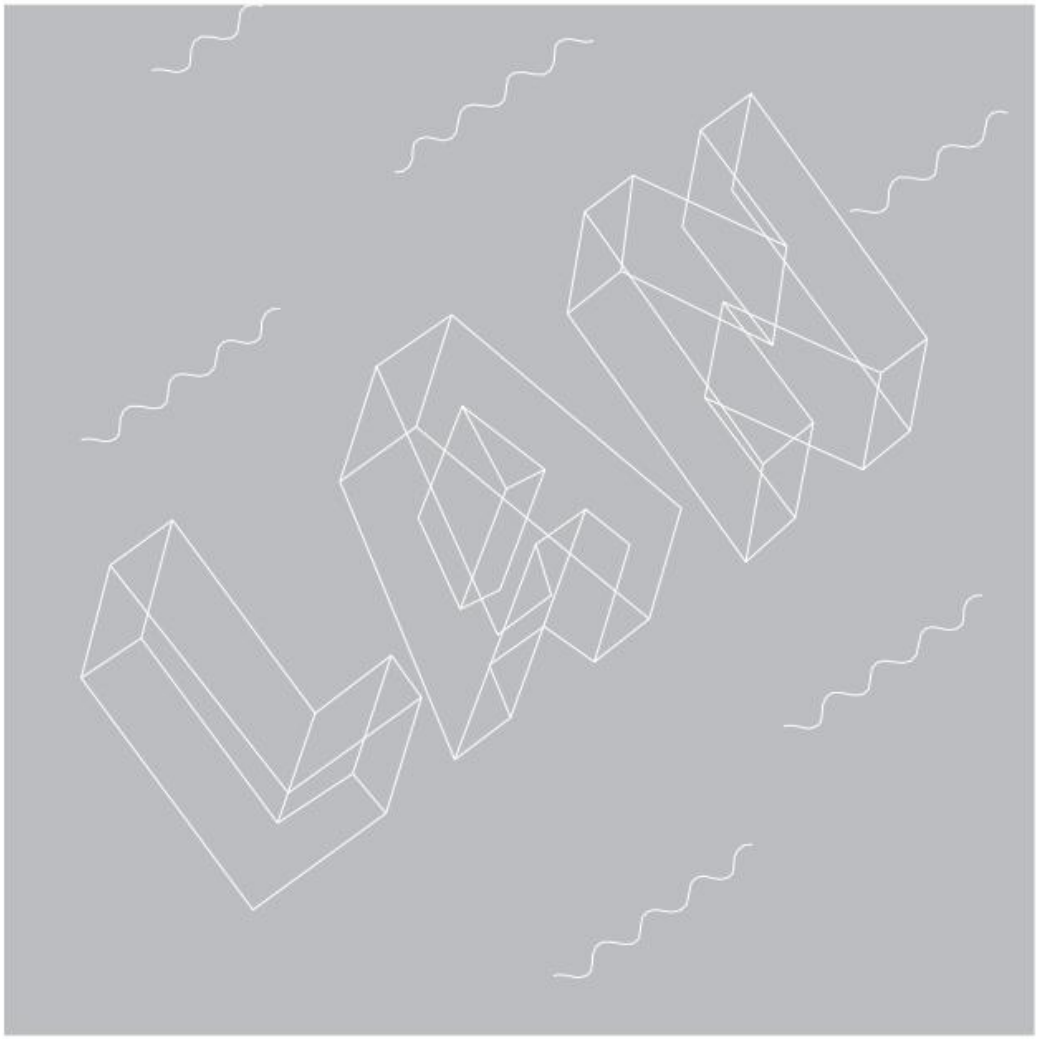
Panasonic®

WEB リファレンス

AIRRECT Cloud

品番　PN91000

●本書の内容の一部または全部を無断で転載することを禁止します。
●ご使用前に「使用上のご注意」（2ページ）を必ずお読みください。



使用上のご注意

■ご使用の前に本書「取扱説明書」をよくお読みの上、正しくご使用ください。

■免責および注意事項

●本製品の使用により、お客様が使用した機器またはシステム等に障害・不具合等が発生し、お客様または第三者に損害が発生したとしても、弊社は一切の責任を負いません。

●本製品の仕様は予告なしに変更する事があります。

●本製品を無断で複製、変更、譲渡することを禁止します。

●本製品を改造して使用することを禁止します。

●本免責および注意事項は予告なく全部または一部を修正、変更する場合があります。

●本製品をご利用の前には、あらかじめユーザーライセンス契約書および個人情報保護契約書への同意が必要となります。詳しくは当社Webサイトを確認ください。

目次

1. はじめに 8
1.1 AIRRECT Cloud について 8
1.2 対応品名・品番 9
1.3 AIRRECT Cloud をはじめる 10
1.3.1 AIRRECT Cloud へのログイン 10
1.3.2 ダッシュボード 11z
2 . Wi-Fi 統合管理設定 13
2.1 基本情報と操作 14
2.1.1 動作バージョン、ユーザー情報の確認 14
2.1.2 Wi-Fi ネットワーク・カウンターと検索機能 15
2.1.3 テーブル・レベルの操作 19
2.1.4 ウィジェットのフィルタ 20
2.1.5 構成変更による再起動の発生 22
2.2 ナビゲーターの管理 23
2.2.1 階層管理設定 23
2.2.2 無線アクセスポイント グループ 27
2.3 ベースラインとしきい値 29
2.3.1 ベースライングラフの見方 30
2.4 ダッシュボード 36
2.4.1 ダッシュボードで接続状況を確認する 36
2.4.2 パフォーマンス情報を確認する 43
2.4.3 アプリケーションの接続状態を確認する 52
2.4.4 WIPS 情報を確認する 56
2.4.5 ハードウェアの情報を確認する（インフラストラクチャ） 66
2.4.6 SLA ダッシュボード 69
2.5 モニター機能 70
2.5.1 接続されているクライアントを確認する 71
2.5.2 管理しているアクセスポイントを確認する 83
2.5.3 モニターからアクセスポイントの設定を変更する 102
2.5.4 アクセスポイントのファームウェアを更新する 111
2.5.5 動作中の無線リストを確認する 115
2.5.6 送信電力制御と自動チャネル選択の固定化 118
2.5.7 アプリケーションの可視性 119
2.5.8 トンネル 122

2.5.9 WIPS で管理対象 WiFi デバイスを確認する 123
2.5.10 WIPS で管理しているアクセスポイントを確認する 124
2.5.11 WIPS に接続されているクライアントを確認する 128
2.5.12 WIPS のネットワーク監視 130
2.5.13 モニターからスイッチングハブ情報を確認する 131
2.6 Wi-Fi の構成 135
2.6.1 SSID の設定 136
2.6.2 SSID のセキュリティ設定 139
2.6.3 グループ PSK 147
2.6.4 SSID のネットワーク設定 149
2.6.4.a SSID ネットワーク情報の基本設定 153
2.6.4.b VLAN ID への VLAN 名マッピング 155
2.6.4.c VLAN プール 159
2.6.5 SSID アクセス制御 160
2.6.5.a SSID ファイアウォールの設定 160
2.6.5.b クライアント認証 167
2.6.5.c ロールベースの制御 168
2.6.5.d DHCP フィンガープリント・ベースのアクセス制御 174
2.6.5.e Bonjour ゲートウェイの構成 175
2.6.5.f MAC アドレスフィルタリング 177
2.6.5.g クライアント分離 178
2.6.6 SSID アナリティクス 179
2.6.7 SSID キャプティブポータル 184
2.6.7.a キャプティブポータルの基本構成 186
2.6.7.b スプラッシュページのデザイン 191
2.6.7.c プラグインの共通設定を構成する 192
2.6.7.d プラグインを構成する 195
2.6.7.e 外部 RADIUS プラグインを構成する 210
2.6.7.f サードパーティーホスト設定の構成 211
2.6.8 ゲスト Wi-Fi の管理 214
2.6.8.a ゲストユーザーの作成/編集 214
2.6.8.b ゲストバッチ 217
2.6.8.c ゲストユーザー/ゲストバッチ共通 219
2.6.9 SSID RF 最適化 221
2.6.9.a SSID プロファイルでの RF 最適化の基本構成 226
2.6.9.b IGMP スヌーピング 227

2.6.10 メッシュネットワーク 230
2.6.11 トラフィックシェーピングと QoS 235
2.6.12 SSID スケジューリング 242
2.6.13 Wi-Fi 7 244
2.6.14 SSID の有効化/編集 245
2.6.15 SSID 属性のカスタマイズ 248
2.7 RADIUS 249
2.7.1 RADIUS プロファイルの設定 249
2.8 トンネルインターフェイス 252
2.8.1 トンネルインターフェースの機能概要 253
2.8.2 トンネルインターフェイスの構成 256
2.8.3 IPSec トンネルの設定 261
2.8.4 リモートアクセスポイント 266
2.9 ロールプロファイル 269
2.9.1 ロールプロファイルの構成 271
2.10 WiFi 無線通信設定 279
2.10.1 無線通信設定の構成 291
2.10.1.a クライアントステアリングの共有パラメーター 291
2.10.1.b 2.4GHz/5GHz/6GHz の無線通信設定の構成 292
2.11 デバイス設定 300
2.11.1 デバイス設定の構成 302
2.11.2 デバイス設定のセキュリティ概要 306
2.11.3 デバイス設定のセキュリティを構成 308
2.11.4 LAN ポートの設定 310
2.11.5 グループの設定 313
2.12 アラート 315
2.12.1 アラートの構成 316
2.12.2 アラートの確認 320
2.13 WIPS の構成 322
2.13.1 アクセスポイントの自動分類 325
2.13.2 クライアントの自動分類 327
2.13.3 自動侵入防止 331
2.13.4 認定 WiFi ポリシー 338
2.13.5 デバイスインポート 342
2.13.6 WLAN 統合 344
2.14 チェックポイントによる設定の保存・復旧機能 347

2.15 トラブルシューティング 351
2.15.1 クライアントのパケットトレースのキャプチャ 351
2.15.2 アクセスポイントのパケットトレースのキャプチャ 354
2.15.3 自動パケットトレース 357
2.15.4 クライアント接続テスト 359
2.15.5 ライブクライアントデバッグ 364
2.15.6 LED の点滅 367
2.15.7 監査ログ 368
2.15.8 デバッグログ 370
2.15.9 アクセスポイント Web シェル 371
2.15.10 スペクトラム分析 373
2.15.11 イベントログの一覧表示 376
2.15.12 ACS/DCS のメカニズムとレポート 378
2.15.13 干渉分類 383
2.15.14 アクセスポイントのデバイス証明書 384
2.16 フロアプラン 388
2.16.1 フロアプランの設定 389
2.16.2 ヒートマップ 390
2.16.3 アクセスポイントとクライアントの検索 394
2.16.4 スイッチのトポロジー表示 398
2.16.5 マップビューの表示 400
2.17 レポート 402
2.18 サードパーティサーバーの連携 410
2.18.1 CIP(Cloud Integration Point)モード 410
2.18.2 Google 統合設定 412
2.18.3 SNMP サーバー統合 413
2.18.4 Syslog サーバー設定 415
2.18.5 Web フック 417
2.19 ホットスポット SSID 419
2.20 脆弱な SSID 420
2.21 AP-サーバ通信キー 421
3. 管理者設定 423
3.1 Launchpad ユーザーの管理 423
3.1.1 プロファイルの種類 423
3.1.2 ユーザー管理の構成 425
3.2 ユーザー定義プロファイルの管理 429

3.3 ユーザーのサービス特権の管理 431
3.3.1 Launchpad での権限割り当て 431
3.3.2 キャプティブポータルでのサービス権限割り当て 432
3.3.3 無線管理でのサービス権限割り当て 436
3.3.4 パケット解析でのサービス権限割り当て 440
3.4 キーの管理 441
3.4.1 キーのロック/ロック解除 443
3.5 設定の管理 444
3.5.1 二要素認証の構成 447
3.5.2 自身のアカウント設定の管理 448
3.6 ユーザーアクションログ 450
3.7 権限レポート 451
3.8 Wi-Fi 統合監視の初期値一覧 453
4. Wi-Fi 簡易設定 475
4.1 SSID の基本設定 476
4.2 SSID のネットワークタイプ 478
4.2.1 ADVANCED 共通設定 478
4.2.2 ADVANCED ゲスト設定 480
4.3 稼働状況/ゲストアクセス解析 482
4.3.1 接続デバイスの稼働状況 482
4.3.2 ゲストアクセスの解析 483
5. パケット解析 - 導入ガイド 489
5.1 トレースファイルの分析 489
5.2 マーカー一覧 494

1. はじめに

1.1 AIRRECT Cloudについて

AIRRECT Cloudは、無線アクセスポイント「AIRRECT AP」シリーズのネットワークの通信状況監視や、操作・設定、トラブルシューティング等を遠隔から行うことができる無線LANクラウドコントローラです。

●AIRRECT CloudおよびAIRRECT APの利用には、利用期間に合わせたライセンスの購入が必須となります。詳細については、当社ホームページをご確認ください。

●AIRRECT AP 1台につき、1ライセンスが必要となります。ライセンス期間が過ぎるとAIRRECT APがご利用できなくなりますので、利用期間にご注意ください。

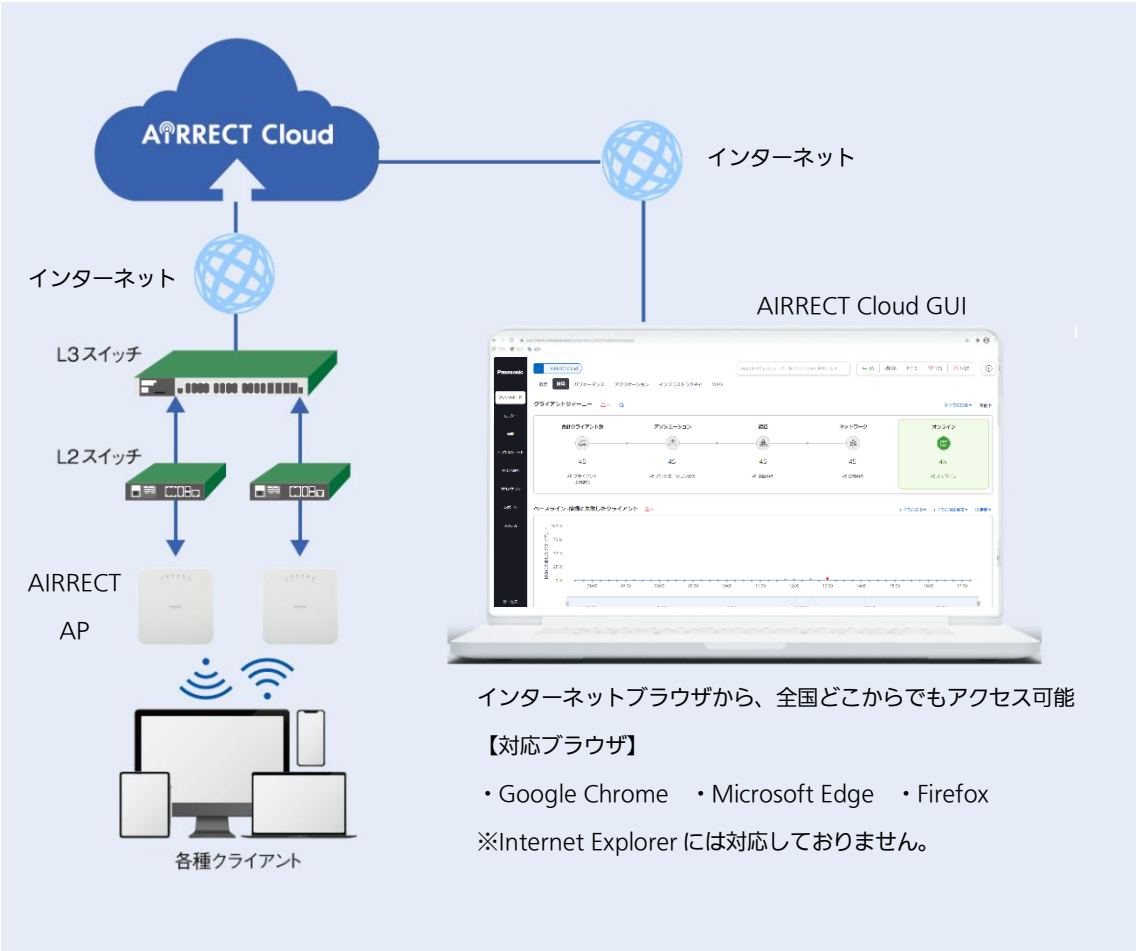
●AIRRECT APは、ゼロタッチプロビジョニング（ZTP）で動作できるように、デフォルトではDHCPサーバーからIPアドレスを取得する設定となっています。ZTPにより、ネットワークに接続するだけでAIRRECT Cloudと接続・インターネットブラウザから操作・監視ができるようになります。ネットワーク接続環境によって、手動でAIRRECT APのIPアドレス固定やプロキシ等の設定が必要な場合は、コマンドライン（CLI）を使用することで設定可能です。コマンドラインの設定方法は、当社ホームページのCLIリファレンスをご確認ください。

●AP-6410/AP-6220は、AIRRECT Cloudとの通信にTCP443ポートを使用します。AP-6810は、AIRRECT Cloudとの通信にTCP443またはUDPの3851ポートを使用します。ご利用の前にポート開放を行ってください。

●AIRRECT Cloudを利用する際には、ユーザー登録が必要となります。対応のブラウザから、ユーザー登録時に設定したユーザーID、パスワードを入力することで、Launchpadにログインすることができます。

●本ユーザーマニュアルは、AIRRECT Couldのバージョン20について記載しております。AIRRECT Cloudは自動でバージョンアップされるため、内容に差分が生じる場合があります。最新の機能については随時当社HPで更新されますので、そちらをご参照ください。

【AIRRECT 接続イメージ】



1.2 対応品名・品番

品名	品番	ソフトウェアバージョン
AIRRECT Cloud	PN91000	20.0.0-175以上
AIRRECT AP-6810	PN91568	20.0.0-175以上
AIRRECT AP-6410	PN91564	20.0.0-175以上
AIRRECT AP-6220	ZLA91622	20.0.0-175以上

※将来対応製品は予告なく変更となる場合がございます。

1.3 AIRRECT Cloudをはじめる

1.3.1 AIRRECT Cloudへのログイン

AIRRECT Cloudのライセンスの登録をおこなうためのEメールが当社より送付されます。
送付されたEメールのURLより、記載の期限内にパスワードの設定を行ってください。
※もし期限が切れた場合、URLの再発行が必要となります。サポートメールまたは、
　ご購入先までお問い合わせください。

注意：パスワードは右下のパスワードポリシーに従って設定をしてください。
また、予測しやすい文字列（繰り返し(aaa)、シーケンス(abcd)、キーボードパターン(qwertyuiop）など）を利用していると、設定できないことがあります。

ログインすると、AIRRECT Cloudの利用規約が表示されますので、ご確認の上、同意をしてください。本利用規約画面は最初のログインのみ表示されますが、内容につきましては当社HPよりいつでも確認することができます。
利用規約に同意すると、[Launchpad]と呼ばれる画面が表示されます。

[Launchpad画面]

Launchpadにアクセスし利用するには、サービスのアクセス権限が必要です。
Launchpadログイン時に必要なサービスタイルが見当たらない場合は、AIRRECT Cloudの管理者にご確認ください。
AIRRECT APは電源を入れただけではアクティベートせず、無線出力しません。
Launchpadの[Wi-Fi統合管理]または[Wi-Fi簡易設定]タイルからネットワークの設定をした後、AIRRECT APをAIRRECT Cloudに接続することでアクティベートされます。
なお、管理するAIRRECT APについては、お客様が購入後に当社で行われるため、お客様が追加登録の操作をする必要はありません。
ネットワーク設定完了後に、AIRRECT APをインターネット経由でAIRRECT Cloudに接続するだけで、コンフィグデータがアクセスポイントに自動でインストールされます。
※環境によって、IPアドレス固定設定などを行う必要があります。

注意：初めてアクティベートする場合、コンフィグデータのインストールやファームウェアの更新に9分ほど時間がかかる場合があります。その際、アクティベート完了まで、再起動を何度か繰り返す場合がありますが、電源を切らないでください。また、複数台のAIRRECT APを同時に接続した場合、データの衝突を回避するため、アクティベートは順次行われます。

1.3.2 ダッシュボード

Launchpadの[**ダッシュボード**]の各タイルは、以下の設定が可能です。

●Wi-Fi統合管理

AIRRECT APの設定や、無線クライアントとの接続状態など確認ができます。
詳細は、2章 [Wi-Fi統合管理設定]をご参照ください。

●パケット解析

不具合等が発生したときに、パケットの分析を行える上級者向けのツールです。
詳細は、5章 [パケット解析 - 導入ガイド]をご参照ください。

●Wi-Fi簡易設定

SSID設定や、ゲストWi-Fi設定などを簡単に、感覚的に行うことができます。
本設定は、Wi-Fi統合管理の設定と連動されます。
詳細は、4章 [Wi-Fi簡易設定]をご参照ください。

●Wi-Fi機器登録

新しいアクセスポイントの登録や、アクセスポイントの削除が行えます。
本機能は、サポート用にPanasonicが利用する場合があります。

管理者

[管理者]タブからは、AIRRECT Cloudを利用できるユーザーや、ログインの制限などを設定することができます。詳しくは、3章**[管理者設定]**をご参照ください

通知表示

Launchpadでは、全ユーザーに重要なメッセージを通知で表示します。通知のアイコンは、ダッシュボードページの右上に表示されます。アイコンをクリックすることで、通知の一覧を見ることができます。

●通知アイコンをクリックすると、未読の通知がハイライト表示されます。
リストにある通知のひとつをクリックすると、その通知の詳細が掲載されているURLまたはダイアログボックスへリダイレクトされます。

●新たに発行された通知については、通知カウントが通知アイコン上に表示されます。

●重要な通知は、Launchpadの全ページにおいて、メニュー下のバナーとして表示されます。(バナー上の) [View more]をクリックすると、通知の詳細がダイアログボックスまたは異なるブラウザータブ上に新たなURLの元で表示されます。

2 . Wi-Fi統合管理設定

Launchpadのダッシュボードから Wi-Fi統合管理タイルをクリックすると、
AIRRECT APの操作設定、監視を行う画面に推移します。

AIRRECT APを導入する際、まずはネットワークの設定をWi-Fi統合管理から行う
必要があります。最低限、以下のネットワーク設定を推奨します。

1. 利用するビルやフロアなど、管理単位ごとにロケーションを作成します。
   初期値ではアクセスポイントはすべて「Staging Area」に所属しています。
   Staging Areaだけでも利用は可能ですが、用途に応じてロケーションを分けること
   で管理が簡単になります。
   ロケーションの設定については、[2.2 ナビゲーターの管理]をご参照ください。
2. 設定したロケーションに、SSIDやネットワークポリシー等の設定を行います。
   SSIDの設定については、[2.6 Wi-Fiの構成]以降の章をご参照ください。

2.1 基本情報と操作

2.1.1 動作バージョン、ユーザー情報の確認

●AIRRECT Cloudバージョン、ビルドおよびライセンス契約に関する詳細の取得
画面左上のPanasonicのアイコンをクリックすることで、AIRRECT Cloudに関するバージョン番号、ビルド番号、契約条件、およびライセンス契約が表示されます。
●ログイン中のユーザー情報を取得
AIRRECT Cloudにログインしているユーザーの基本情報を表示するには、画面左下にあるユーザーのイニシャルマークをクリックすると、以下の情報が表示されます。

オプション	説明
ログインID	ログインしたユーザーのID
ユーザーロール	ユーザーの役割 (スーパーユーザーや管理者など)
Eメール	ユーザーのEメールアドレス。ログインID、メールアドレスは同じです。
現在時刻	システムの現在の日時
タイムゾーン	ユーザーが選択したタイムゾーン

AIRRECT Cloudからサインアウト

AIRRECT Cloudからサインアウトするには、以下の手順を実行します。
1. 画面左下のイニシャルアイコンをクリックします。
2. [**サインアウト**]をクリックするとログアウトされ、サインインページに移行します。

オープンソースソフトウェアライセンスの表示

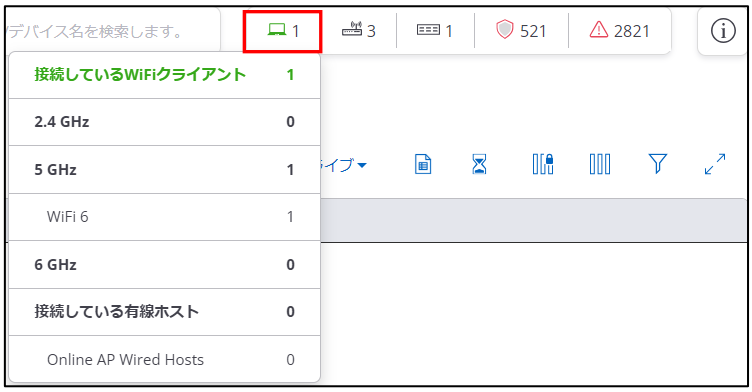
UIからオープンソースソフトウェア（OSS）のライセンスを表示できます。ライセンスはローカルドライブにダウンロードされます。
1. Launchpad > Wi-Fi統合管理から、画面左上の[Panasonic]ロゴをクリックします。
2. [**OSSライセンス**]で、各コンポーネントのリンクをクリックします。ライセンスはローカルドライブにダウンロードされます。

2.1.2 Wi-Fiネットワーク・カウンターと検索機能

Wi-Fiネットワーク・カウンターは、Wi-Fiネットワーク・インフラの概要を表示します。カウンターはAIRRECT Cloudの画面右上に表示されており、選択することで詳細情報を確認できます。カウンターで確認できる情報は以下になります。

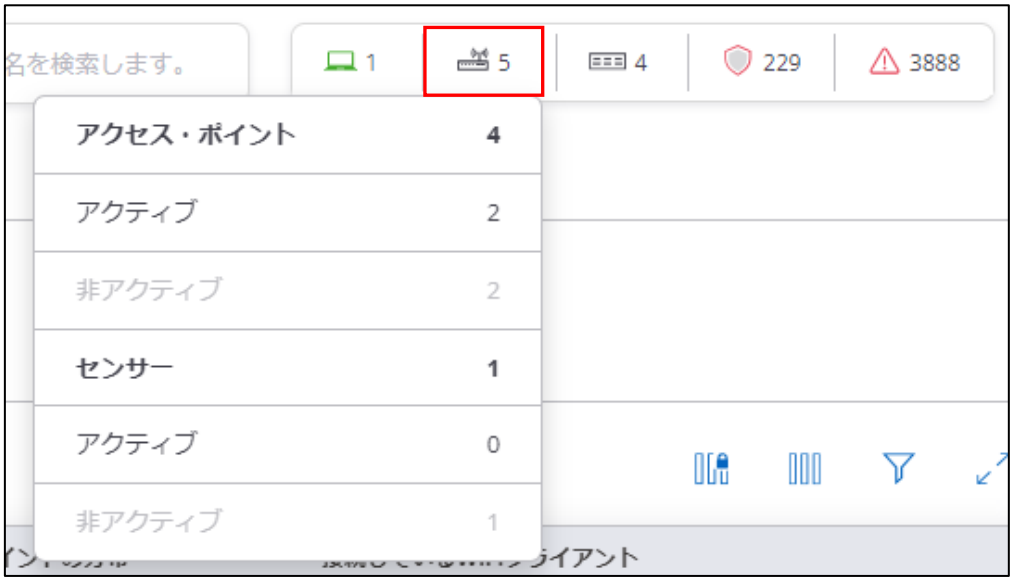
Wi-Fiクライアント

管理対象のWi-Fiネットワークに、現在接続されているクライアントの種類を表示します。



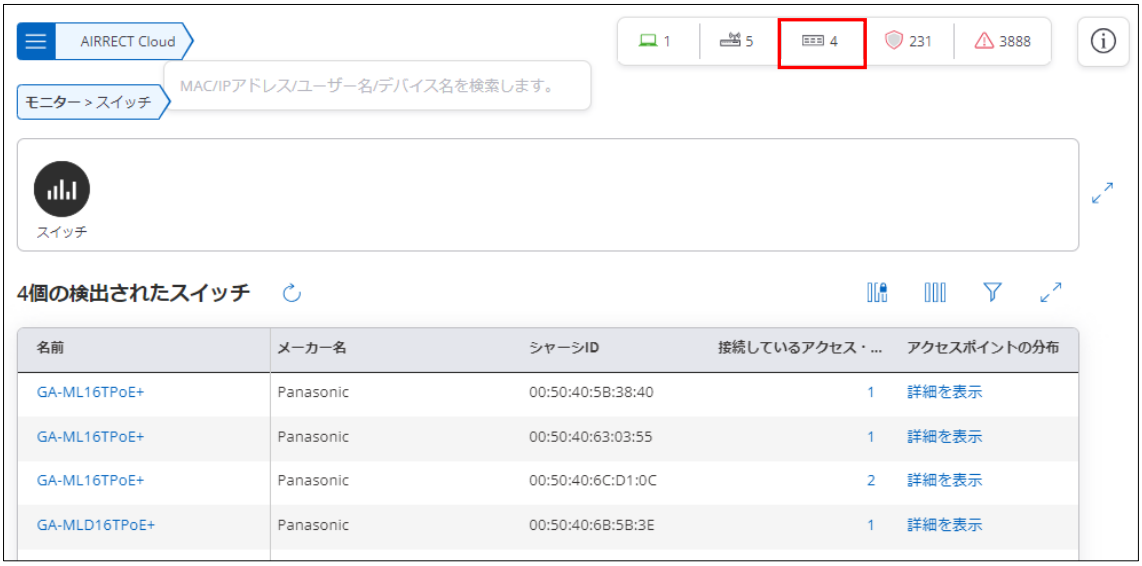
管理対象Wi-Fiデバイス

管理対象であるアクセスポイントのアクティブおよび非アクティブのステータスを表示します。



管理対象スイッチ

管理対象であるスイッチの詳細情報を表示します。



脅威対策のデバイス

脅威をもたらすデバイスの存在 (例：不正または不適切に構成されたアクセスポイント、不正クライアント、誤動作など) を表示します。

トンネル

トンネルのアクティブおよび非アクティブのステータスを表示します。

アラート

Wi-Fiのパフォーマンスとセキュリティ、およびシステム状態に関連するアラートを表します。

検索

Wi-Fiネットワーク・カウンター横の検索バーにMACアドレス、IPアドレス、ユーザー名、デバイス名を入力することで、クライアントやアクセスポイントを検索できます。選択したフォルダ、またはフロアで使用可能なクライアントやデバイスのみを検索できます。

●選択したフォルダやフロアの SSID に対象のクライアントが接続されていない場合、検索結果は表示されません。

●アクセスポイントまたはBSSIDのMAC、IPアドレス、ユーザー名、またはデバイス名をグローバル検索ボックスに入力すると、デバイスの詳細が表示されます。

●クライアントとアクセスポイントの各々の詳細については、『接続されているクライアントを確認する』と『管理しているアクセスポイントを確認する』を参照して下さい。

検索を使用する場合は、以下に注意する必要があります。

●大文字と小文字が区別されません。

●文字列または部分文字列を入力すると、クライアントとアクセスポイントが一覧表示されます。例えば、iPhoneと入力すると、名前またはユーザー名の一部としてiPhoneが含まれるいくつかのクライアントと[**詳細を見る**]リンクが検索に表示されます。[**詳細を見る**]をクリックすると、全ての検索結果が表示されたページにリダイレクトされます。

●検索結果は、クライアントとアクセスポイントで分かれて表示されます。

●すべてのクライアントを検索できます。

- AIRRECT APに現時点でアソシエーションされているクライアント
- 過去にAIRRECT APにアソシエーションされていたクライアント
- AIRRECT APに接続を試している、もしくは接続を試したが失敗したクライアント

● “*” や ” ?” などの特殊文字を使用したパターン・ベースの検索は、サポートされていません。例えば、iP*と入力した場合、グローバル検索はその結果を一覧表示しません。

2.1.3 テーブル・レベルの操作

[**モニター**]タブで表示されるモニタリング・テーブルから全てのクライアントの状態が表示され、必要に応じてフィルタリング、表示変更をすることができます。操作はテーブルの右上にあるアイコンにより行います。

テーブル・レベルに関する操作は以下の通りです。

●**列を固定**：列の固定により、ユーザーはテーブルの列の固定や、固定解除を実行できます。この操作の詳細は、『**列の固定**』を参照して下さい。

●**列を追加/削除**：列の追加と削除の操作は、複数列を追加または削除するために使用されます。この操作の詳細は、『**列の追加と削除**』を参照して下さい。

●**フィルタ**：データをフィルタリングすることで、特定の基準に基づきデータの並べ替えや、特定データの検索ができます。

●**フルスクリーン**：フルスクリーン操作を選択すると、テーブルをフルスクリーンモードで表示できます。同じ操作でフルスクリーンモードを終了できます。

列の固定

モニタリング・テーブルは、テーブルを縦線で2つに分割できます。左側のセクションには、列の固定でチェックした項目が含まれます。これらの列はロックされており、水平方向にスクロールした時に、常に表示されるようになります。右側のセクションには、固定されていない列が含まれています。固定できる列は、最大5項目です。ステータス、名前列については、固定、または、固定の解除はできません。

列を固定、固定解除するには

1. テーブルの右上の隅にある列の[**固定アイコン (列を固定)**]をクリックします。名前の横にチェック・ボックスがついている列のリストが表示されます。
2. 固定や固定を解除する列を選択または、選択解除を実行します。

列の追加と削除

列の追加や削除に関する操作は、テーブルに列を追加または削除します。初期設定では、すべての列がテーブルに追加されています。

列の追加や削除を実行するには、以下を実行します。

1. テーブルの右上の隅にある[**列を追加/削除**]をクリックします。
2. 名前の横にチェックボックスがついている列のリストが表示されます。
3. 追加または削除する列を選択、または選択解除します。

2.1.4 ウィジェットのフィルタ

AIRRECT Cloudの各ウィジェットは、フィルタを使用して特定のクライアントデータの表示や取得ができます。フィルタはウィジェットの右上隅にあり、フィルタリングにより、ネットワーク監視が効率的に行えます。

SSIDフィルタ

ドロップ・ダウンで特定のSSIDを選択すると、選択したSSIDに関連するデータが抽出されます。[**すべてのSSID**]をクリックすると、すべてのSSIDに関するグラフに集計データが表示されます。

周波数帯フィルタ

周波数に基づいてフィルタリングできます。選択した周波数で動作するアプリケーションのデータが表示されます。

時間間隔フィルタ

以下の時間間隔の情報をフィルタリングし、表示可能です。

2時間/4時間/8時間/12時間/1日/1週間/1ヶ月

特定の時間間隔を選択すると、それに応じてデータが提供されます。例えば、「2時間」を選択すると、過去の2時間分の統計データが提供されます。

※一部の時間間隔は、ウィジェットによっては使用できない場合があります。

アプリケーションフィルタ

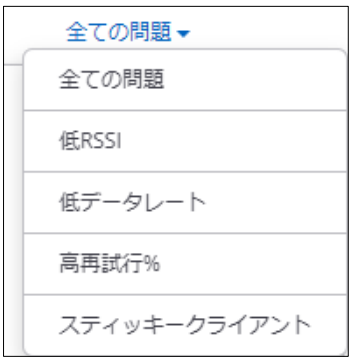
特定のアプリケーションの統計情報 データ を表示できます。本フィルタは[**ダッシュボード**]>[**アプリケーション**]のアプリケーションエクスペリエンスで利用されます。
監視可能なアプリケーションデータの内、「通信品質が悪い順」はアプリケーションエクスペリエンスの低いアプリケーションを表します。最も使用されているアプリケーションまたは、最も影響を受けるアプリケーションを選択し、それぞれ上位５つを表示します。

障害フィルタ

障害フィルタを使用すると、接続に失敗した原因に基づいて、データの表示や取得が可能になります。適用可能な設定は、全ての障害/アソシエーション/認証/ネットワーク の4種類です。
[**全ての障害**]をクリックすると、上記の障害に関する詳細が一度にすべて表示されます。

問題フィルタ

選択した問題の原因に基づいてフィルタします。適用可能な設定は以下になります。
全ての問題/低RSSI/低データレート/高再試行%/スティッキークライアント
[**全ての問題**]をクリックすると、上記に関する問題の詳細が一度にすべて表示されます。



2.1.5 構成変更による再起動の発生

AIRRECT Cloudから設定変更を行った際に、項目によってはSSIDまたはアクセスポイントの再起動が発生する場合があります。例えばSSID 設定を変更すると、そのSSID が再起動し、5秒程度通信ができなくなりますが、例外として、サービスの中断を発生しない項目もあります。以下に、設定変更による影響がある項目を示します。

設定項目	設定内容	インパクト
SSID設定	設定変更	変更対象となるBSSIDの再起動発生
ロールプロファイル設定	プロファイル名変更	再起動なし
	上記以外の設定変更	適用されたSSIDの再起動
トンネルインターフェース設定	プロファイル名変更	再起動なし
	上記以外の設定変更	適用されたSSIDの再起動
Radius設定	プロファイル名変更	再起動なし
	上記以外の設定変更	適用されたSSIDの再起動
デバイス設定	・バックグラウンドスキャン設定 ・WiFiスキャンの長さ/WiFiアクセスの長さ設定 ・クライアントRSSIの更新間隔	適用されたフォルダのSSIDの再起動
	・アクセスポイントを専用WIPSセンサーに変換 ・SSID VLANモニタリング ・IPv4/IPv6デュアルスタック ・リンクアグリゲーション設定	適用されたフォルダのアクセスポイントの再起動
[モニター]>[WiFi]>[アクセスポイント]から設定	VLAN設定	アクセスポイントの再起動
	送信電力とチャネル	SSIDの再起動
	グループの割り当て/再割り当て	SSID/アクセスポイントの再起動（移動先の設定に依存）
設定の引継ぎ	上位のフォルダまたは別グループから引継ぎ実行	SSID/アクセスポイントの再起動（移動先の設定に依存）
ロケーションの変更	アクセスポイントを別フォルダに移動する。	SSID/アクセスポイントの再起動（移動先の設定に依存）

2.2 ナビゲーターの管理

2.2.1 階層管理設定

ナビゲーター機能から、全国の拠点や店舗等のネットワークを整理するための階層構造について定義できます。ナビゲーターは、フォルダとフロアで構成されており、フォルダは、組織の部署、事業単位や、都市、建物などを論理的なグループに分けることができます。フロアは、アクセスポイントの共通セットを使用するグループや、アクセスポイントが配置されている建物のフロアなどを設定します。ナビゲーター画面には、画面左の[**システム**]>[**ナビゲーター**]から移行します。
ナビゲーターは、スーパーユーザー、管理者およびオペレーターに限り編集可能です。ビューワーは、ナビゲーターの表示、閲覧のみ可能です。

フォルダやフロアの追加

ルートフォルダや他のフォルダの下に、複数のフォルダを追加できます。

フォルダやフロアを追加するには、以下の手順を実行します。

1. [**システム**]をクリックすると、フォルダとフロアの階層が表示されます。
2. 新しいフォルダやフロアを追加するフォルダを選択します。右クリックして、[**フォルダー/フロアを追加**]を選択すると、[**新規フォルダー/フロア**]ダイアログボックスが表示されます。
3. フォルダを選択してフォルダを追加するか、フロアを選択してフロアを追加します。
4. フォルダやフロアの名前を入力して、[**追加**]をクリックすると、選択したフォルダの配下に新規のフォルダやフロアが追加されます。

   注意：フロアの配下にフォルダやフロアを追加することはできません。

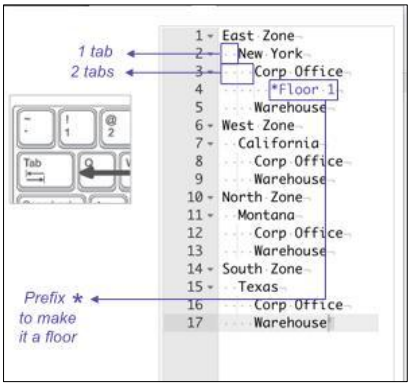
フォルダやフロアを複数追加する

本機能ではフォルダやフロアを同時に複数追加できます。ルートフォルダや他のフォルダの配下に、フォルダを複数追加できます。不明なフォルダの下にフォルダやフロアを、追加することはできません。

フォルダやフロアを複数追加するには、以下の手順を実行します。

1. [**システム**]をクリックします。フォルダとフロアの階層が表示されます。
2. 追加したい複数のフォルダやフロアを右クリックし[**複数のフォルダー/フロアを追加**]をクリックすると、[**新規フォルダー/フロア**]のダイアログボックスが表示されます。
3. 指定したテキスト領域に追加するフォルダやフロア名を入力します。
4. フォルダやフロアの階層を作成するには、**Tabキー**を使用します。

   フォルダやフロアのサンプル階層は、以下のようになります。



   フロア名の前に「*」を付けて作成します。フロア配下に、フォルダやフロアを追加することはできません。

5. [**追加**]をクリックすると、選択したフォルダ配下に、複数のフォルダとフロアが追加されます。

フォルダとフロアの削除

不要なフォルダやフロア、および該当しないものを取り除きます。

フォルダやフロアを削除するには、以下の手順を実行します。

1. [**システム**]をクリックすると、フォルダやフロアの階層が表示されます。
2. 削除するフォルダやフロアをクリックします。
3. 選択したフォルダやフロアのいずれかを右クリックして、[**削除**]を選択します。
   削除するダイアログボックスが表示されます。
4. [**削除**]をクリックします。
   複数のフォルダやフロアが正常に削除されたことが、メッセージで表示されます。
   フォルダやフロアの階層の上にある削除のアイコンを使用して、同様の方法でフォルダやフロアを削除することもできます。

注意：APが1台以上所属しているフォルダ・フロアは削除できません。

フォルダやフロア名の変更

1つまたは複数のフォルダやフロアの名前を変更します。

ファイル名を変更するには、以下の手順を実行します。

1. [**システム**]をクリックすると、フォルダやフロアの階層が表示されます。
2. 名前を変更するフォルダとフロアを選択します。
3. 選択したフォルダやフロアのいずれかを右クリックして、[**名前を変更**]を選択すると、
   ダイアログボックスが表示されます。
4. 必要な変更をおこない、[**名前を変更**]をクリックして変更を保存します。
   選択したフォルダやフロアの名前の変更が、正常に行われたことを通知するメッセージが表示されます。

フォルダやフロアの検索

文字列やフォルダ、フロアなどの名前を入力して検索できます。フォルダを検索するには、以下の手順を実行します。

1. [**システム**]をクリックすると、フォルダやフロアの階層が表示されます。
2. [**フォルダー/フロアを検索**]のテキストボックスに、フォルダやフロアの名前と一致するテキスト・サブストリング (部分文字列) を入力します。
3. テキスト文字列や部分文字列のパターンに一致するフォルダやフロアが、親フォルダと共に表示されます。“*”や“ ?”などの特殊文字を使用したパターン・ベースの検索は、サポート対象外になります。

フォルダに関するタイムゾーンの設定

[**システム**]>[**ナビゲーター**]の順に移行し、選択したフォルダに適切なタイムゾーンを設定します。ロケーションのロケーション・タイムゾーンを設定できるユーザーは、スーパーユーザー、管理者、およびオペレーターのユーザーに限られます。

タイムゾーン設定は、分析をおこなう際に役立ちます。選択したフォルダにおいて、タイムゾーンが適切に選択されていることを確認して下さい。

注意：フロアにタイムゾーンを設定することはできません。
設定されたタイムゾーン・フロアの親フォルダはフロアに即時に適用されます。

フォルダのタイムゾーンを設定するには、以下の手順を実行します。

1. [**システム**]>[**ナビゲーター**]へ移動します。
2. ナビゲーターのページで、フォルダ名を右クリックして、[**ロケーション・プロパティ**]>[**ロケーションのタイムゾーン**]をクリックします。[**タイムゾーンを設定**]のダイアログボックスが表示されます。
3. ドロップダウンリストから適切なタイムゾーンを選択し、[**設定**]をクリックします。
   タイムゾーンの設定アイコンを使用して、同様の方法でタイムゾーンを設定することもできます。

2.2.2 無線アクセスポイント グループ

グループを使用すると、階層ロケーションツリーのさまざまなフォルダにあるアクセスポイントにカスタム構成（例. SSID、無線設定、デバイス設定など）を適用できます。
グループを設定するには、グループが作成されたフォルダでSSIDをオンにするか、デバイス設定または無線通信設定を変更します。

設定

設定されたグループのアクセスポイントは、グループと同じ設定を使用します。さらに、各グループには単独のWi-Fi構成があります。どのグループにも属していないアクセスポイントは、それらが作成された場所のWi-Fi構成を引き続き使用します。ロケーションを削除すると、削除されたロケーションのグループが削除され、グループに割り当てられたデバイスが親ロケーションに移動します。

注意：アクセスポイント1台につき、1つのグループにのみ属することができます。

グループの追加

グループを追加するには、以下の手順を実行します。

1. [**システム**]>[**ナビゲーター**]>[**グループ**]へ移行します。
2. [**＋アイコン**]をクリックして、グループを追加します。
   [**グループを追加**]のダイアログボックスが開き、グループが作成された場所の名前が表示されます。

3. グループの名前を入力し、[**追加**]をクリックします。
   グループ名は、利用可能なすべてのグループおよびフォルダ全体で一意である必要があります。

AIRRECT Cloudは、ユーザーがアクセスできるすべてのロケーション共通のルートフォルダ を検索し、それに応じてそのフォルダ内にグループを作成します。
ユーザーがルートフォルダに対するアクセス権限を持たない場合は、グループはユーザーがアクセスできる最上位フォルダ内に作成されます。

割り当てられたデバイスの表示

特定のグループに割り当てられているアクセスポイントリストを表示します。
アクセスポイントのリストには、名前、MACアドレス、操作モード、グループ、モデル、場所があります。リストの表示は、以下の手順を実行します。

1. [**システム**]>[**ナビゲーター**]>[**グループ**]に移動します。
2. デバイスリストを表示することを選択したグループの横にある3つの縦の点をクリックします。
3. [**割り当てられたデバイスの表示**]をクリックすると、選択したグループのアクセスポイントリストがグループ名と表示されます。

グループ名の変更

必要に応じて、グループの名前を変更できます。グループ名を変更するには、以下の手順を実行します。

1. [**システム**]>[**ナビゲーター**]>[**グループ**]に移動します。
2. 名前を変更するグループの名前を右クリックするか、メニューアイコン⋮をクリックして、[**名前を変更**]を選択します。
3. グループ名を変更し、[**名前を変更**]をクリックして変更を保存すると、グループ名の変更を確認するメッセージが表示されます。

グループの削除

グループを削除すると、いくつかの機能に影響を及ぼします。

- グループが削除されると、そのグループに割り当てられたデバイスは、それぞれのフォルダのデフォルトのWi-Fi設定を使用して起動します。
- 同様にフォルダを削除すると、その配下に作成されたグループも削除されます。その後、そのデバイスは、それぞれのフォルダのデフォルトのWi-Fi設定の使用を開始します。

グループを削除するには、以下の手順を実行します。

1. [**システム**]>[**ナビゲーター**]>[**グループ**]に移動すると、グループのリストが表示されます。
2. 削除するグループの名前を右クリックするか、メニュー・アイコン⋮をクリックし、[**削除**]を選択します。
3. グループの削除について通知するメッセージ表示を確認し、[**削除**]をクリックします。

2.3 ベースラインとしきい値

ネットワークの状態を判別する基準として、AIRRECT Cloudではベースラインとしきい値を使います。
ベースラインは、測定する際の基準となる値です。例えば、無線ネットワークを最適化する場合、再試行率や平均データレートなどの指標をベースラインにして、変更がプラスに作用したかマイナスに作用したかを測定する必要があります。
しきい値は、あるアクションを起こすために超えなければならないレベルのことです。例えば、再試行率のしきい値を50%に設定すると、再試行率が50%を超えたときにシステムが警告を発することになります。しきい値は静的なものであり、状況の変化には対応できません。
AIRRECT Cloudのベースライン機能は、クライアント、アクセスポイント、アプリケーションの履歴データから動作を調査し、自動的にベースラインを15分間隔で算出します。ベースラインから大きく逸脱した動作は異常とみなされ、グラフで強調表示されます。通常のネットワーク監視システムでは、しきい値は静的で、同じ値が全ロケーションに適用されてしまいます。しかし、ワイヤレスネットワークの特性は環境によって異なるため、動的に判断する必要があります。

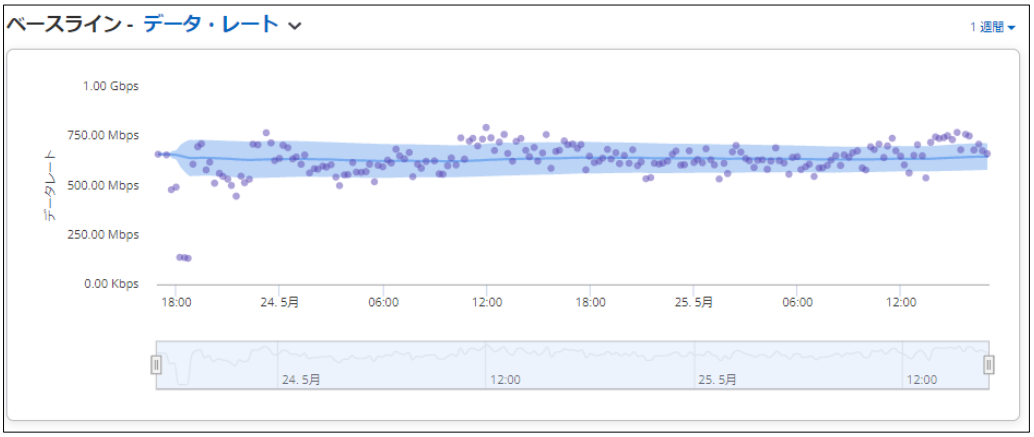
しきい値で判断する場合は、正しいしきい値を決めることが重要です。しきい値を低く設定すると、アラームが多すぎてネットワーク管理者は、いわゆる「アラーム疲労」を起こしてしまいます。こうなると、有効なアラームが、重要でないアラームの中に紛れてしまうため危険です。この「アラーム疲労」に対抗するために、多くのネットワーク管理者は、しきい値を高く設定します。それにより、問題が起きている場合もアラート表示がされない危険性があります。

ベースラインは、以下の方式により計算され求められます。
●平均値（青線）：EWMA（指数関数的加重移動平均）
●データの範囲（青背景）：EWMASD（指数加重移動平均標準偏差）

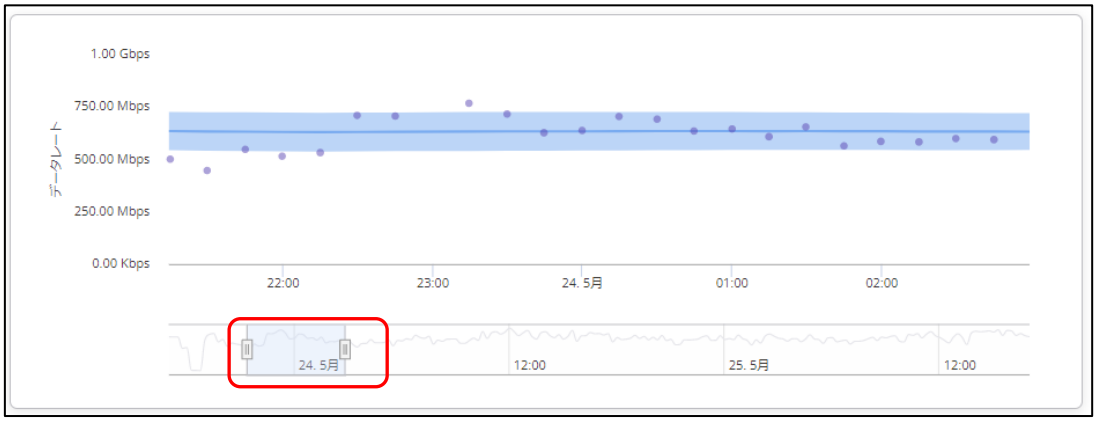
2.3.1 ベースライングラフの見方

AIRRECT Cloudはダイナミックベースラインにより、ネットワークの正常な状態を定義し、ネットワーク状況の変化に応じて自動調整されます。例えば、少数のクライアント環境では問題がなくとも、その後Wi-Fiネットワークに多くのクライアントが追加されると、再試行率は大きく変化する可能性があります。ダイナミックベースラインにより、しきい値の問題が回避されるとともに、ベースラインと比較することで実際の問題を特定することができます。

ベースライングラフは、以下の4つの要素で構成されています。
●ベースライン - 青線
●偏差値の範囲 - ベースラインの周りの水色の影の部分
●観測点 - 15分間隔のデータの平均値をとります。
●異常点 - 赤い点は、標準から大きく外れた観測点



ベースライングラフの特定の時間を拡大/縮小して、粒度を詳細に見ることができます。
グラフの下部のバーを操作することでズーム機能を使用できます。



ベースラインには、接続イベントとパフォーマンスイベントの両方あります。

以下の表は、利用可能なベースラインとAIRRECT Cloudで確認できる該当箇所の一覧です。該当箇所により、IPv4とIPv6のベースラインを分けて表示しています。

タイプ	ベースライン チャート	要素	AIRRECT Cloud上の該当箇所
接続	接続に失敗したクライアント	ロケーション	[ダッシュボード]>[接続]
		アクセスポイント	[モニター]>[アクセスポイント]>[アクセスポイント]ドリルダウン
	ベースライン - AAA遅延時間	ロケーション	[ダッシュボード]>[パフォーマンス]>[平均遅延時間]>[AAA]ドリルダウン
	ベースライン - DHCP遅延時間	ロケーション	[ダッシュボード]>[パフォーマンス]>[平均遅延時間]>[DHCP]ドリルダウン
	ベースライン - DNS遅延時間	ロケーション	[ダッシュボード]>[パフォーマンス]>[平均遅延時間]>[DNS]ドリルダウン
パフォーマンス	データレート	クライアント	[モニター]>[クライアント]>[クライアント]ドリルダウン
	再試行率 %	アクセスポイント クライアント	[モニター]>[アクセスポイント/クライアント]>[アクセスポイント/クライアント]ドリルダウン
	RSSI	クライアント	[モニター]>[クライアント]>[クライアント]ドリルダウン
	パフォーマンス不良によって影響を受けたクライアント	ロケーション	[ダッシュボード]>[パフォーマンス]
		アクセスポイント	[モニター]>[アクセスポイント]>[アクセスポイント]ドリルダウン
	劣悪なアプリケーションエクスペリエンス(%)	ロケーション	[ダッシュボード]>[アプリケーション]
	ベースライン - アプリケーション遅延時間	ロケーション	[ダッシュボード]>[パフォーマンス]>[平均遅延時間]>[アプリケーション]ドリルダウン

これらの各ウィジェットでは、データをフィルタリングすることができます。
フィルタの詳細については、「ウィジェットのフィルタ」を参照してください。

ベースラインの利用例

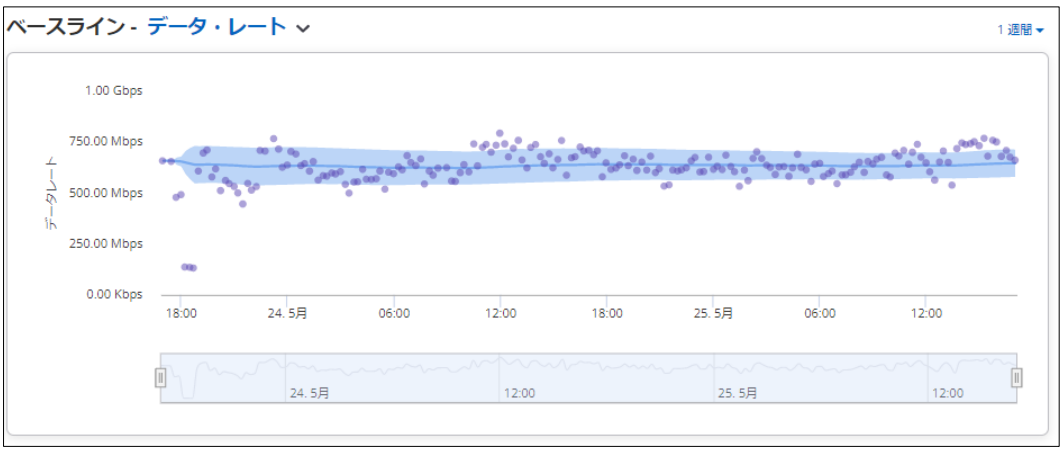
例1：ベースライン - 接続に失敗したクライアント

このチャートは、選択したアクセスポイントの接続障害の影響を受けるクライアントのベースラインを表します。

データポイントは、接続されたクライアントの総数と、15分間隔でのクライアントの最後の接続状態によって決定されます。データポイントの上にカーソルを置くと、ツールチップが表示されます。このツールチップには、使用感の良し悪しを示すパーセンテージと、所定の時点で算出されたベースラインの情報が集約されています。グラフ上のデータポイントをクリックすると、詳細情報が表示されます。

例2：ベースライン - データレート

下図は、データレートのベースライングラフです。個々のクライアントが消費する平均データレートのベースラインを計算して表示します。異常値は、グローバルに設定可能なしきい値とデータレートとを比較して算出されます。データレートは、ネットワークや環境ごとに許容範囲が異なるため、異常を検知するためのしきい値の使用が適切です。ベースラインと偏差値帯は引き続き計算されますが、異常の有無はデータレートのしきい値によって判断されます。



データの報告と保持

クライアント接続の成功と失敗は、原因を分析した上で、発生後、ほぼ即座にアクセスポイントからAIRRECT Cloudに報告されます。パフォーマンス、その他のデータは15分ごとに集約され報告されます。

クライアントアプリケーションデータを除き、直近1週間分の情報がクラウド上に保持され、利用できます。

データタイプ	アクセスポイント レポートインターバル	クラウド 保存期間
クライアントの接続試行	即時	1週間
AAA、DHCP、DNS及びTCP遅延時間	検出後、即時	1週間
クライアントアプリケーションデータ	15分	12時間
クライアント・パフォーマンス・メトリクス	15分	1週間
BSSIDパフォーマンスメトリクス	15分	1週間
SSID アプリケーションデータ	15分	1週間
ベースラインデータ	15分	1週間

データポイントの情報

下記表には、接続されているクライアントの詳細情報を指定する属性が含まれています。これらの情報は、どのベースラインチャートからでも、データポイントをドリルダウンすると表形式で表示されます。

ベースラインチャートの名前が特定されていない属性は、すべてのチャートで共通です。

パラメータ	概要
名前	クライアント名
ユーザー名	クライアントのユーザー名
MACアドレス	製造元によってネットワークアダプタに割り当てられたクライアントの一意の48ビットIEEE形式アドレス
前回の失敗時間	クライアントがネットワークへの接続に失敗した最新の日時
前回の失敗原因	クライアントがネットワークへの接続に失敗した原因
関連付けられたSSID	クライアントが接続されているWLANのSSID
関連付けられたアクセスポイント	クライアントがネットワーク上の他のクライアントやデバイスと通信するために使用するアクセスポイント
ロケーション	クライアントのロケーション
IPアドレス	クライアントのIPアドレス

パラメータ	概要
周波数帯	クライアントが接続している周波数帯を表します。
Wi-Fi規格	クライアントと接続している802.11プロトコルを表します。 ※過去に接続した中で最新のプロトコル表記を保持します。例えば、Wi-Fi6で接続後、Wi-Fi5で接続した場合も、表記はWi-Fi 6となります。
チャネル	クライアントが接続を試みたアクセスポイントのチャネル
OS	クライアント上で動作しているOS名
平均RSSI(dBm)	クライアントのRSSI値
接続・切断された日時	クライアントがアップまたはダウンした時からの最新の日時
接続/切断以降 (ベースライン - パフォーマンス不良によって影響を受けたクライアント)	
パラメータ	概要
First Detected Time	クライアントが最初に検出された日時
ロール	SSIDに関連付けられてクライアントに割り当てられたロール
Google認可	クライアントが、Google統合でインポートされたクライアント認証リストに含まれているかどうかを表すブール値
メーカー名	メーカー名
アップリンクデータ（ベースライン - パフォーマンス不良によって影響を受けたクライアント）	クライアントが転送したデータ量
ダウンリンクデータ（ベースライン - パフォーマンス不良によって影響を受けたクライアント）	クライアントが受け取ったデータ量
再試行率（ベースライン参照不可 - 失敗の影響を受けたクライアント）	再試行率のパーセンテージ
スティッキー（ベースライン参照不可 - 失敗の影響を受けたクライアント）	隣接するアクセスポイントからの信号強度が優れているにもかかわらず、別のアクセスポイントに接続されてしまっているクライアントの有無

パラメータ	概要
アプリケーション名（ベースライン - 劣悪なアプリケーションエクスペリエンス）	アプリケーション名
アプリケーション使用時間（ベースライン-劣悪なアプリケーションエクスペリエンス）	クライアントのアプリケーション使用時間
劣悪なアプリケーションエクスペリエンス（ベースライン - 劣悪なアプリケーションエクスペリエンス）	クライアント接続時の劣悪なアプリケーションエクスペリエンス
アップリンクビットレート（ベースライン-劣悪なアプリケーションエクスペリエンス）	クライアントがデータを送信する際のレート（単位：ビット）
ダウンリンクビットレート（ベースライン-劣悪なアプリケーションエクスペリエンス）	クライアントがデータを受信する際のレート（単位：ビット）
ダウンリンクジッタ（ベースライン - 劣悪なアプリケーションエクスペリエンス）	クライアントが受信したパケットの遅延時間のバリエーション。VoIPアプリケーションの品質測定に使用されます。
アップリンクジッタ（ベースライン - 劣悪なアプリケーションエクスペリエンス）	クライアントが送信したパケットの遅延時間のバリエーション。VoIPアプリケーションの品質測定に使用されます。

2.4 ダッシュボード

AIRRECT Cloudは、関連するクライアントの統計のみならず、接続性とパフォーマンスに関する情報をダッシュボードのさまざまなウィジェットで表示し、迅速にトラブルシューティングをおこなうことができます。

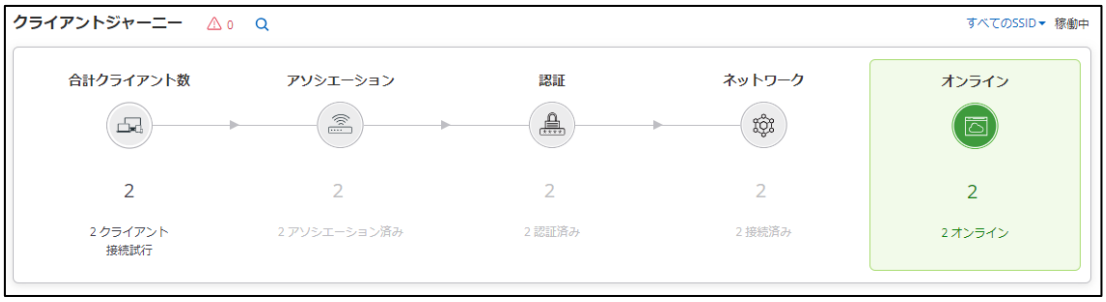
2.4.1 ダッシュボードで接続状況を確認する

接続ダッシュボードには、選択したフォルダやフロア上の、WLANネットワークに存在するクライアントやデバイスに関する情報がすべて表示されます。**[ダッシュボード]>[接続]**をクリックすると、接続状況が可視化された以下のウィジェットが表示されます。

パラメータ	概要
クライアントジャーニー	ネットワークに接続を試みるクライアントの接続状況 (アソシエーション/認証/ネットワークの各接続ステップ) を表示します。
ベースライン - 接続に失敗したクライアント	接続の問題が原因で失敗したクライアントの割合のベースラインを計算し表示します。(接続に関する問題の内容は、認証失敗、アソシエーションの失敗、およびネットワーク障害など。)
接続失敗回数が多いクライアント	クライアントが接続に失敗した回数が表示される。失敗した試行の降順でクライアントが表示されます。
接続が失敗したクライアントが存在するロケーション	アソシエーション、認証、またはネットワーク障害の影響を受けた上位5つのロケーションが表示されます。ロケーションは、接続障害のパーセンテージに基づいて降順で表示されます。

クライアントジャーニー

選択したフォルダまたはフロアのネットワークの状態を示します。現在アクティブなクライアント数、Wi-Fiへのアソシエーション、正常に認証されたクライアント、ネットワークに接続されているクライアントの総数など、クライアントに関する概要が表示されます。



クライアントジャーニーの各フェーズの数値上にカーソルをあてると、追加情報を取得できます。認証フェーズの数値上にカーソルをあてると、認証されたクライアントの割合、認証に失敗したクライアントの数、認証失敗の原因、認証の種類などの情報が表示されます。また、[**アソシエーション**]をクリックすると、クライアントの正常性に関する情報が表示されるページへリダイレクトします。

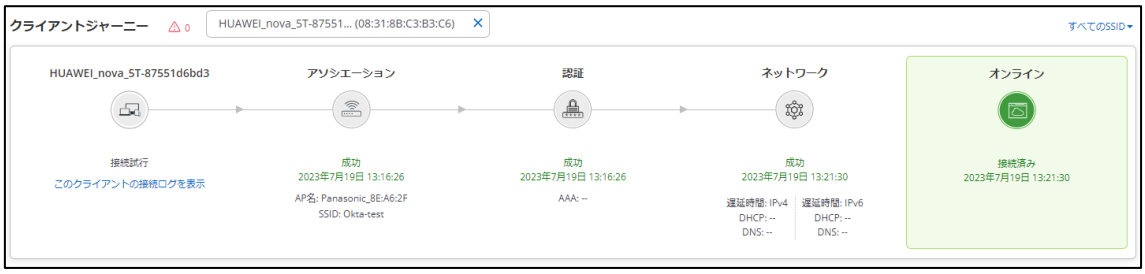
クライアントジャーニーで表示される情報は以下の通りです。

パラメータ	概要
合計 クライアント数	[**合計クライアント数**]セクションには、ネットワークに接続した、または接続を試みたクライアントの数が表示されます。これには、ネットワーク上のSSIDにアソシエーションされたクライアントの総数と、アソシエーションに失敗したクライアントの総数が含まれています。[**合計クライアント数**]をクリックすると、クライアントとその詳細情報に関するリストが表示されます。
アソシエーション	[**アソシエーション**]セクションには、Wi-Fiネットワークへのアソシエーションに成功したクライアントと、Wi-Fiネットワークとのアソシエーションに失敗したクライアントの総数が表示されます。[**アソシエーション**]をクリックすると、アソシエーションが失敗したクライアントに関するリストが表示されます。
認証	[**認証**]セクションには、正常に認証されたクライアントと、Wi-Fiネットワーク経由で認証に失敗したクライアントの総数が表示されます。
ネットワーク	[**ネットワーク**]セクションには、DHCP、DNSなどのネットワークサービスに正常にアクセスできたクライアント、およびこれらのサービスにアクセスできなかったクライアントの総数が表示されます。
オンライン	[**オンライン**]セクションには、Wi-Fiネットワークに正常に接続したオンラインのクライアント総数が表示されます。また、ネットワークの認証、アソシエーション、またはネットワークへのアクセスに失敗したクライアントの総数も表示されます。

クライアントジャーニーの検索アイコン

MACアドレス、IPアドレス、ユーザー名、またはデバイス名を指定して、アクティブなクライアントを検索できます。アクティブなクライアントのさまざまなフェーズで、最後に試行された接続のステータスをタイムスタンプとともに取得します。
選択したフォルダまたはフロアで、使用可能でアクティブなクライアントのみを検索できます。検索したクライアントのデバイス名が、選択したフォルダやフロアのSSIDに接続されていない場合、以下の内容が表示されます。

・現在アクティブなクライアントで接続記録が見つかりませんでした：
選択したフォルダやフロアで検索したアクティブなクライアントが利用できないため、結果が表示されません。
・過去のクライアントレコードを検索しますか？：
検索履歴からクライアントを探すように促すリンク。このオプションは、検索されたクライアントが以前はアクティブであったにも関わらず、現在は利用できない場合に表示されます。リンクをクリックすると、クライアントリストへリダイレクトします。
クライアント名をクリックすると、その詳細を確認できます。ログの詳細については、『**クライアント・イベント**』を参照してください。過去7日間の履歴やデータについては、ログを元に確認可能となります。
検索されたクライアントがアクティブな状態で、選択したフォルダやフロアのSSIDに接続されている場合、タイムスタンプを使用したクライアント接続のさまざまなフェーズにおいて、前回の接続のステータスを表示できます。以下の図は、クライアント接続に関するさまざまなフェーズを示しています。



アクティブクライアントを検索すると、ウィジェットにはフェーズに関するさまざまな情報が表示されます。

パラメータ	概要
接続試行	クライアント名と、検索したアクティブクライアントの接続ログにリダイレクトするリンクを示します。
アソシエーション	・ステータス（成功または失敗） ・アソシエーション成功時のタイムスタンプ ・クライアントが接続しているアクセスポイント名 ・SSID名
認証	・ステータス（成功または失敗） ・認証成功時のタイムスタンプ ・認証サーバー名と平均待ち時間
ネットワーク	・ステータス（成功または失敗） ・直近の接続成功時のタイムスタンプ ・認証サーバーの名前と平均待ち時間
オンライン	・ステータス（成功または失敗） ・直近の接続成功時のタイムスタンプ

ウィジェットのデータについては、ウィジェットの右上にあるフィルタを使用してフィルタリングできます。
フィルタの詳細については、『**ウィジェットのフィルタ**』を参照してください。

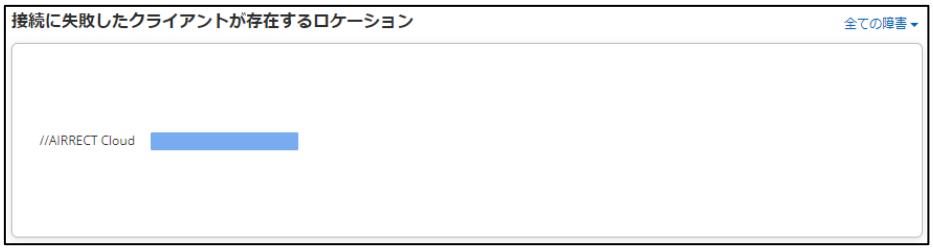
接続失敗回数が多いクライアント

[**接続失敗回数が多いクライアント**]には、接続失敗回数が多いクライアント順に、リスト化されます。
データは表形式で表示され、接続に失敗したクライアント名と、クライアントが接続に失敗した回数 (合計数) が表示されます。

[**クライアント名**]をクリックすると、クライアント接続ログウィジェットが表示され、エラーの詳細を取得できます。グラフの閲覧期間は2時間から1週間です。
期間はウィジェットの右上にあるドロップダウンリストから選択できます。

接続に失敗したクライアントが存在するロケーション

ウィジェットには、アソシエーション、認証、またはネットワーク接続の障害が影響をおよぼす上位5つのロケーションを示す水平棒グラフが表示されます。グラフには、選択した親フォルダとその直接の子フォルダのデータが含まれています。グラフには、接続障害の割合(%)が最も高い上位5つのロケーションが、以下のように降順で記載されています。グラフのバーの上にカーソルをあてると、その場所で管理されているアクセスポイントに接続されているクライアントの総数のうち、接続障害によって影響を受けるクライアントの数が表示されます。そのロケーションのバーをクリックして表示されるページでは、そのロケーションで発生した接続障害が及ぼす影響やクライアントの情報などを閲覧できます。ウィジェットの右上にあるドロップダウンリストから障害の種類を選択できます。
[**全ての問題**]の詳細については、『**ウィジェットのフィルタ**』を参照してください。



クライアントと障害に関する分類

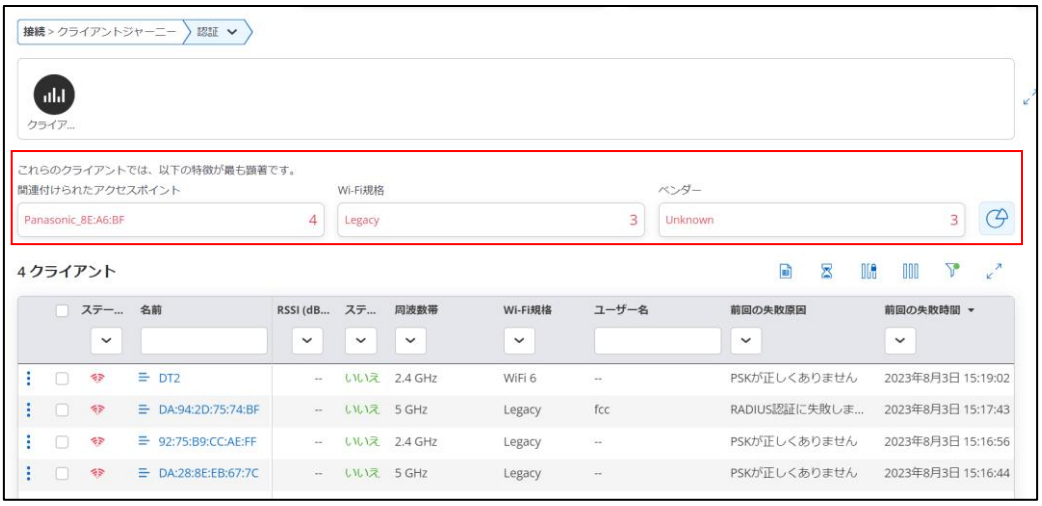
AIRRECT Cloudはクライアントの論理カテゴリを作成し、クライアントを動作周波数帯やOSの種類などのプロパティに基づいてグループ化します。これらのクライアント・プロパティに基づいて問題を調査し、トラブルシューティングを行えます。例えば、特定の帯域幅のクライアントでアソシエーションエラーが発生したかどうかについて確認など、クライアント接続の問題に関する根本原因分析を効率的に行えます。
クライアントは、以下のカテゴリ別にグループ化されます。

●OSの種類：クライアントのオペレーティングシステムの種類（AndroidやiOSなど）
●プロトコル/帯域幅：クライアントが運用時に利用している802.11プロトコル、または、帯域幅（b/g、ac、ax）
●メーカー：クライアントの製造元（Apple,Microsoftなど）
●スティッキーステータス：信号強度が良好ではないアクセスポイントに接続している「スティッキークライアント」を示します。

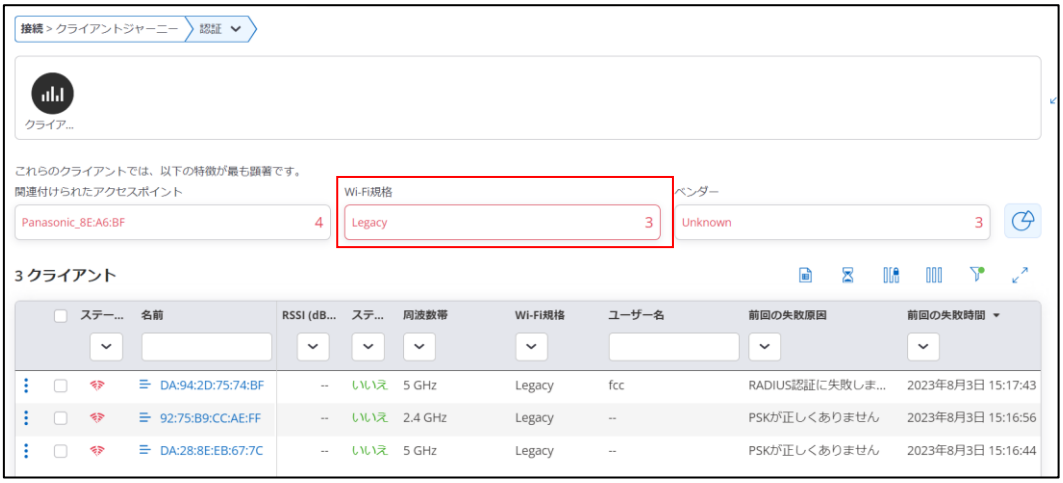
論理クライアントのカテゴリ別ドリルダウン

論理的にフィルタリングすることで、クライアントの接続性とパフォーマンスの問題をドリルダウンして早急に分析できます。クライアントのカテゴリ(例えば、周波数帯2.4GHzのクライアントのすべての認証エラーを論理クライアントのカテゴリごとに分析するには以下の手順を実行します。

1. [**ダッシュボード**]>[**接続**]>[**クライアントジャーニー**]の順にクリックします。
2. 分析したいクライアントジャーニーのステージをクリックします。
   例として、認証の失敗を分析するには、[**認証**]をクリックします。認証に失敗したクライアントリストが表示され、最も顕著な特徴である論理グループのフィルタタブが表示されます。フィルタは、Wi-Fi規格、周波数帯、アソシエーションされたSSID、OSなどが表示されます。



3. クライアントリストをフィルタリングする特性 (論理カテゴリ) を選択します。下図では、古いWi-Fi規格で接続しているクライアントにフィルタをしています。



4. フィルタタブの右側にある円グラフをクリックすると、論理カテゴリ全体のクライアントの分布について確認できます。以下のように、[**クライアントの分類**]（ベンダーやOSなどの種類によってグループ化されている）ウィンドウペインが表示されます。
このウィンドウの**各カテゴリ**をクリックすると、クライアントリストがフィルタリングされます。

2.4.2 パフォーマンス情報を確認する

パフォーマンス・ダッシュボードには、多数のグラフやウィジェットを含む、Wi-Fiネットワークのパフォーマンスに関する情報が表示されます。

[ダッシュボード]>[パフォーマンス]の順にクリックすると、以下の項目のグラフやウィジェットなどが表示されます。

パラメータ	概要
クライアントの動作状態	選択したフォルダまたはフロアのクライアントの合計数が表示されます。低RSSI、低データレート、高再試行%、スティッキークライアントが表示されます。
平均遅延時間	選択したフォルダやフロアのクライアントに関して、DHCP、DNS、AAAサーバーなどのサーバーが使用した平均待機時間（応答時間）が表示されます。
ベースライン - パフォーマンス不良によって影響を受けたクライアント	一定期間におけるすべてのクライアントの中で、パフォーマンス低下による影響を受けたクライアントの割合を示すベースラインが表示されます。
平均データレート別クライアント	選択したフォルダまたはフロアのクライアントの平均データ転送速度を示す棒グラフが表示されます。
RSSI別クライアント	クライアントの総数とRSSIの値を示す棒グラフが表示されます。
トラフィックが最大のクライアント	データ使用量が最も多いクライアントの横棒グラフが表示されます。
問題のあるクライアントが存在するロケーション	パフォーマンスの問題が最も多いロケーションについて、横棒グラフで降順に表示されています。
ネットワーク使用率	クライアントのアソシエーション数を示す折れ線グラフと、トラフィック量を示す棒グラフが表示されます。

クライアントの動作状態

クライアントの動作状態ウィジェットは、選択したフォルダまたはフロアにおける、低RSSI、低データ、再試行率が高いクライアント、スティッキークライアントが表示されます。対象合計フィールドには、これらの影響を受けるフォルダまたはフロアにあるクライアントの総数が表示されます。これらの値をクリックすると、各問題の詳細が表示されます。クライアントの動作状態の情報は2分ごとに更新されます。

クライアントの動作状態ウィジェットには、以下の内容がリストされます。

パラメータ	概要
対象合計	一部のクライアントには複数の問題がある可能性があります。 例えば、低RSSIで低データレートのクライアントは、両方のカテゴリに表示されます。AIRRECT Cloudは、このようなクライアントが2回カウントされないように合計が表示されます。これは、以下の**[対象合計]**フィールドにリストされている問題の影響を受ける個別のクライアントの数を意味します。
低RSSI	設定されたRSSIしきい値を下回っているクライアントの数を表します。
低データレート	設定されたデータ転送速度値を下回っているクライアントの数を表します。
高再試行%	再試行率が20%を超えるクライアントの数を表します。再試行率の%は、クライアントのデータパケットの総数で割った再試行パケットの数を意味します。
スティッキークライアント	スティッキークライアントとは、信号強度が低い場合でも、アクセスポイントにアソシエーションされたままになる傾向があるデバイスを意味します。

しきい値の設定方法については『**ベースラインとしきい値**』を参照してください。

インテリジェンスエンジン（AI機能）の概要

選択したロケーションのクライアントを分析することで、低RSSI値、低データレート、高再試行%などのパフォーマンスの問題に関する根本原因を把握するためにAI機能を搭載しています。この機能はクライアントが抱える問題のみならず、その原因を導き出します。また、根本原因を認識すると、推奨事項を通知することで、システム内の障害等の再発防止および制御方法をユーザーに通知します。

以下のパラメータに基づいて障害に関する根本原因を検出します。

●発生事象と、ロケーション内での該当事象が発生している端末数の分析

- 帯域の使用率の問題や、アップリンクのトラフィック量が多い端末数、カバレッジが悪い状態などを、問題の潜在的な理由として特定します。

●問題の原因となり得るWi-Fi設定についての情報の分析

- 送信電力が「自動」に設定されているか、ダイナミックチャネル選択が有効になっているかなど設定の問題について分析します。

AI機能は、一部の特定の根本原因タイプに対してのみ推奨を提供します。（根本原因が場所、SSID、メーカー名、OS、またはアクセスポイントに基づいている場合は、未サポートです。）

単一のクライアントと合計クライアントの根本原因分析

単一のクライアントと、問題に直面しているクライアントの総数に対して根本原因分析を実行します。単一のクライアントの場合、AI機能以外にも、[**モニター**]>[**クライアント**]から推奨事項を表示できます。

合計クライアントの場合、クライアントヘルスウィジェットで分析を実行する必要があり、根本原因分析はロケーションに基づいて実行されます。[**ダッシュボード**]>[**パフォーマンス**]>[**クライアントの動作状態**]>[**対象合計**]から実行します。

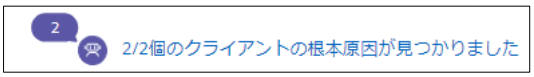
根本原因の究明

インテリジェントエンジンにより、パフォーマンスに関する問題解決を効率的に行えます。生成されたビューは60分後に有効期限が切れます。

根本原因の究明は、以下の手順を実行します。

1. [**ダッシュボード**]>[**パフォーマンス**]の順にクリックします。
2. [**クライアントの動作状態**]の分析したいパラメータ (低RSSI、低データレート、高再試行%) を選択します。下図では例として「低データレート」のクライアントの合計数を示す値をクリックします。

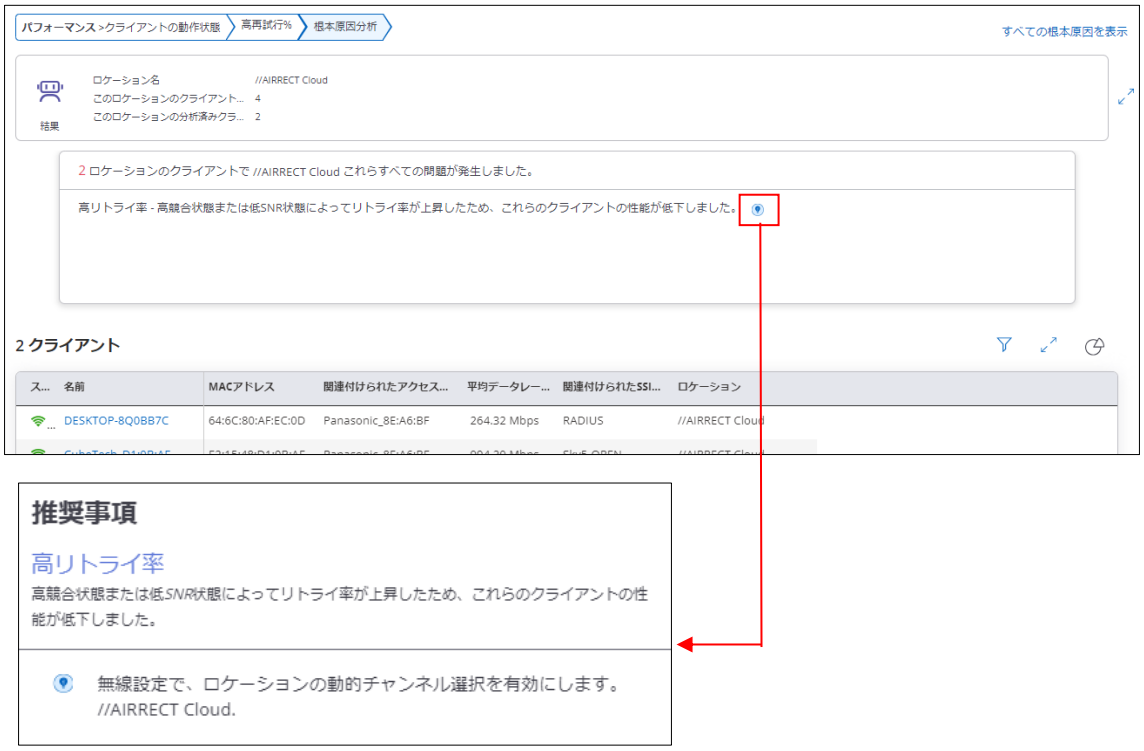
3. 画面右上の[**根本原因を探しますか？**]をクリックすると、根本原因分析がバックグラウンドで開始します。
   分析を行っている間、AIRRECT Cloudの他の操作を行うことも可能です。



   バックグラウンドプロセスが完了すると、根本原因分析が行われたクライアントの数を含むメッセージが、ロボットアイコンの隣に表示されます。また、根本原因分析の結果にリンクしている [**進行中のアクティビティ**]メッセージボックスが画面の右下に表示されます。そのリンクには、根本原因が見つかった (または、その原因を把握できた) クライアントの数が含まれています。
4. リンクをクリックすると、根本原因分析に関する結果が表示されます。

   影響を受けた上位のロケーションのカバレッジの低下、競合の増加などの問題について、根本原因を解説するページにリダイレクトします。

5. 対象のロケーションを選択し、画面右上にある[**すべての根本原因を表示**]をクリックすると、分析に関するすべての結果を一目で確認することができます。
6. 根本原因の隣にある青い電球アイコンをクリックすると、問題を修正するための推奨事項が表示されます。



単一のクライアントの根本原因分析の実行

単一のクライアントの詳細を開くと、クライアントが直面している症状と問題の理由が表示されます。インテリジェンスエンジンはバックグラウンドですべての計算を自動的に実行し、症状と考えられる解決策を表示します。

1. [**モニター**]>[Wi-Fi]>[**クライアント**]をクリックします。
2. リストからクライアント名をクリックします。クライアントが問題に直面している場合は、クライアントの詳細の下に症状と理由が表示されます。
3. 症状に対する推奨事項を表示するには、原因の横にある「この問題を解決するには」（電球のアイコン）をクリックします。

平均遅延時間

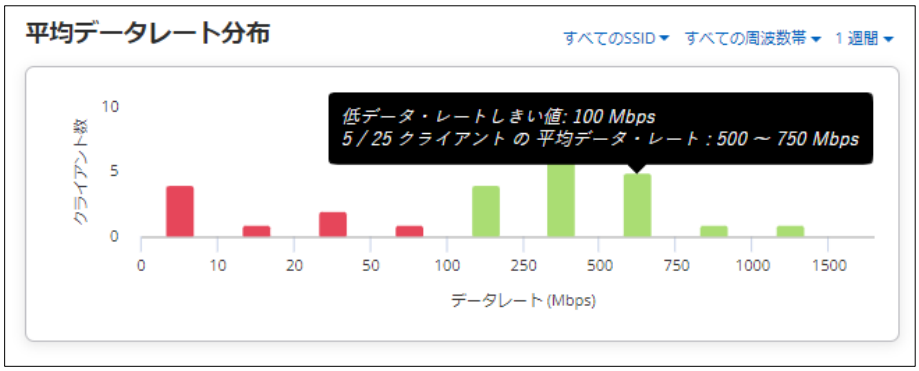
[平均遅延時間]の画面には、選択したフォルダやフロアに存在するクライアントに関して、AAA、DHCP、DNSなどの認証サーバーや、アプリケーションが使った平均待ち時間（応答時間）が表示されます。

平均遅延時間は、個々のサーバーがミリ秒 (ms) 単位で応答する際に必要となる平均時間を意味します。

各遅延情報をクリックすると、その遅延時間のベースライングラフが表示されます。詳細については、『ベースライングラフの見方』を参照してください。

クライアントの分類　(平均データ転送速度別による分類)

[平均データレート分布]ウィジェットには、クリックしたフォルダやフロア内のクライアントが消費する平均データ転送速度が表示されます。このウィジェットでは、すべてのクライアントで使用されるデータの平均転送速度が計算され、そのグラフが表示されます。その他、データ転送速度のしきい値を設定できます。



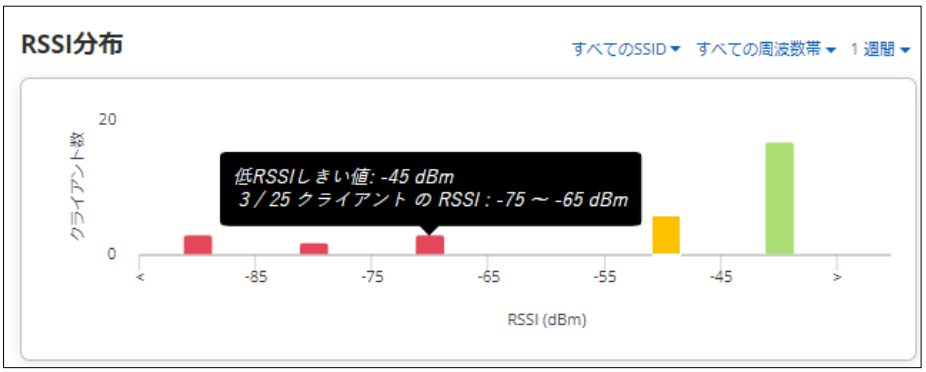
データは赤色、緑色、黄色の棒グラフが表示され、その分類は以下の通りです。

赤色	データ転送速度が設定されたしきい値を下回っているクライアント
緑色	データ転送速度が設定されたしきい値を超えるクライアント
黄色	バケット内のしきい値が下がるクライアント 例えば、上記の画像では、75Mbpsと設定されたしきい値が、50MBps～100Mbpsのバケットに該当しています。しきい値が50Mbpsから100Mbpsの間にあるクライアントは黄色で表示されています。

しきい値の設定方法については『**ベースラインとしきい値**』を参照してください。

クライアントの分類 (RSSIによる分類)

RSSI別分布ウィジェットは、クリックしたフォルダやフロアにあるクライアントの 平均RSSI[dBm]を表示します。このウィジェットには、すべてのクライアントが使用する平均のRSSIが表示されます。また、RSSIのしきい値について設定できます。



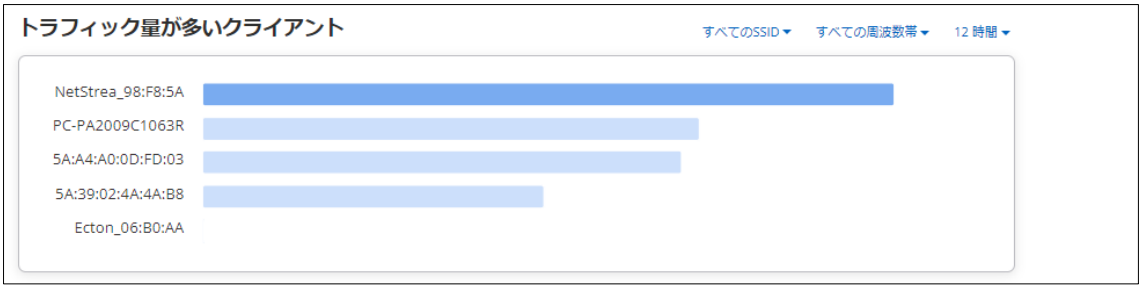
データは赤色、緑色、黄色の棒グラフが表示され、その分類は以下の通りです。

赤色	設定されたしきい値を下回るRSSIのクライアント
緑色	設定されたしきい値を超えるRSSIのクライアント
黄色	設定したしきい値に近しいRSSIのクライアント 誤差範囲は±5dBmです。例えば、しきい値を-70dBmに設定した場合、-75dBm～-65dBmのクライアントは、黄色でマークされます。

しきい値の設定方法については『**ベースラインとしきい値**』を参照してください。

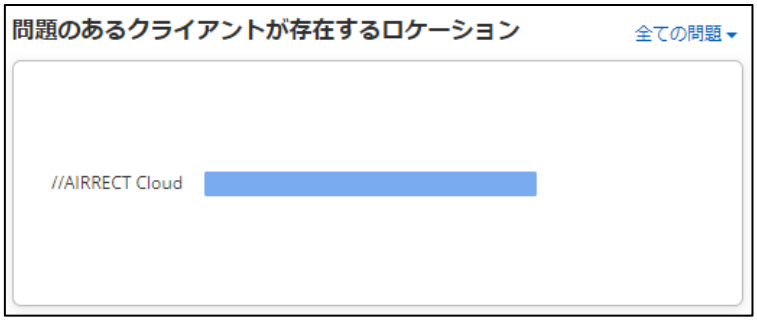
トラフィック量が多いクライアント

データ使用量が最も多い5つのクライアントを示す棒グラフが表示されます。ここで表示されるデータは、クリックしたフォルダやフロア内のクライアントに関する内容です。グラフをクリックすると、クライアントのアクティビティ詳細が表示されます。また、グラフのバー上にカーソルをあてるとクライアントが使用しているデータの総量が表示されます。使用期間については、ウィジェット右上のドロップダウンリストから選択できます。



問題のクライアントが存在するロケーション

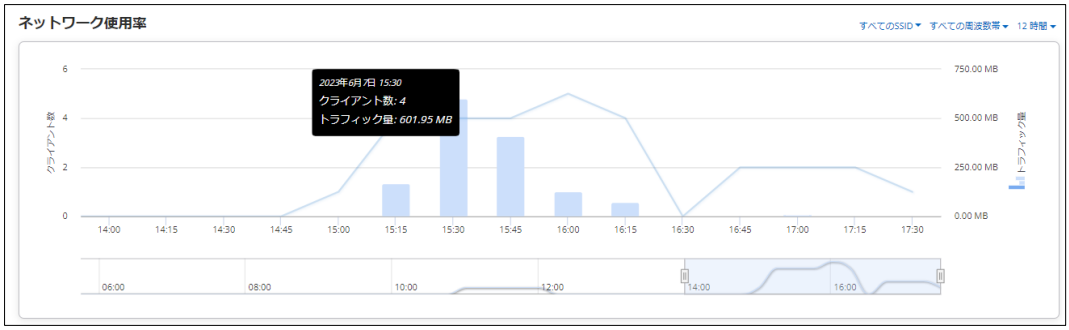
Wi-Fiネットワークのパフォーマンス低下による影響を受けている上位5つのロケーションやクライアントが表示されます。グラフには、クリックした親フォルダと子フォルダに関するデータが含まれています。パフォーマンス低下は、低RSSI、低データレート、高再試行%、スティッキークライアントの4つの基準に基づいて算出されます。グラフのバーにカーソルをあてると、パフォーマンス低下による影響を受けたクライアントの合計数が表示されます。この情報は、上記の5つのロケーションに関連しています。また、クリックすると、パフォーマンス低下の影響を受けているすべてのクライアントを表示するページにリダイレクトします。例えば、低RSSIをクリックすると、RSSIの値が低いクライアントとそのロケーションに関する詳細のページを表示します。
ウィジェットの右上にあるドロップダウンリストから、発生しているパフォーマンスの問題の種類を選択できます。



ネットワーク使用率

[ネットワーク使用率]グラフには2つのアクセス方法があります。

1. ダッシュボードのパフォーマンスタブからアクセス
   選択したフォルダやフロアにあるすべてのクライアントに関する情報 (SSIDにアソシエートされたクライアント数とトラフィック量を示す折れ線グラフ) が表示されます。
2. アクセスポイントドリルダウン経由でグラフにアクセス
   同様のデータが表示されますが、この場合はクリックしたアクセスポイントに関する内容になります。グラフにカーソルを合わせると、タイムスタンプ、クライアントの数、使用されたトラフィック量などの簡易情報が表示されます。



グラフのデータをクリックすると、選択した時間に接続したすべてのクライアントのリストと、以下の詳細情報が表示されます。

パラメータ	概要
クライアント接続テーブル	すべてのクライアント接続のリストや、選択したタイムスタンプの詳細が表示されます。
上位のアプリケーション	データ使用量が最も多い10個のアプリケーションが表示されます。テーブルの左上にあるドロップダウン・リストからアプリを選択できます。選択したアプリケーション名と、アプリケーション固有のデータ消費量が表示されます。
すべてのアプリケーショントラフィック	アプリケーションが使用するデータの総量が表示されます。選択したアクセスポイントまたはロケーションを示し、この情報はテーブルの右上に表示されます。
クライアント接続	**[クライアント接続]**をドリルダウンから選択すると、[上部のアプリケーションリスト]から選択したアプリケーションを使用しているすべてのクライアント・リストが表示されます。
アクセスポイントの分散	**[アクセスポイントの分散]**をドリルダウンから選択すると、アソシエートされているすべてのアクセスポイントリストが表示されます。

2.4.3 アプリケーションの接続状態を確認する

[**ダッシュボード**]から[**アプリケーション**]に移動すると、[**アプリケーションの動作状態**]ウィジェットが表示されます。本ウィジェットで、アプリケーションエクスペリエンスの影響を示すクライアントの数と、直近2時間分のアプリケーションエクスペリエンスの影響を示す進行状況バーが確認できます。

WebベースアプリケーションのQoEについて

Webベースのアプリケーション（Web会議、メール、イントラネット、オンラインドライブなど）のパフォーマンスの監視をサポートします。AIRRECT APは、WebアプリケーションのTCPフローをキャプチャし、当該アプリケーションの状態を判断するために情報をサーバーに送信します。全体的な通信状態が悪いと判断された場合、その該当期間内のアプリケーションエクスペリエンスの割合を表示します。このアルゴリズムでは、監視対象のアプリケーションに関連する各TCPストリームのIPおよびTCPヘッダーに含まれる情報のみを検査するため、ユーザーデータはサーバに保存されません。

また、[**アプリケーション・エクスペリエンス別のクライアント**]は、集約されたアプリケーションエクスペリエンス、または、各アプリケーションごとのアプリケーションエクスペリエンスを提供します。デフォルトでは、表示設定をしたアプリケーションの中で、最も影響を受けたアプリケーションや最も使用されているアプリケーションが、[**ダッシュボード**]>[**アプリケーション**]タブのカードビューに表示されます。特定のアプリケーションを優先的に使用したい場合は、[**アプリケーションエクスペリエンス**]ウィジェットに固定することもできます。

各カードの赤いバーは、アプリケーションエクスペリエンス（通信品質）が低かった割合を示しています。一方、緑色のバーは、高かった割合を示しています。上図のMicrosoft Teamsの例を参照すると、二割のユーザーにとって通信品質が悪いと感じている可能性があります。

アプリケーションの監視設定

アプリケーションエクスペリエンスでは、TCPおよびVoIPベースのアプリケーションを含む、最大25個のアプリケーションを監視できます。Web QoEはグローバルな設定なので、監視するアプリケーションをルートフォルダで設定する必要があります。ナビゲーションツリーのフォルダごとに、異なるWeb QoEの設定をすることはできません。

監視の実行手順は以下のとおりです。

1. [**ダッシュボード**]>[**アプリケーション**]タブを開きます。
2. [**アプリケーションエクスペリエンス**]ウィジェットで、[**アプリケーション・エクスペリエンスを監視する**]アイコンをクリックします。

3. 画面右に表示される[**アプリケーションエクスペリエンスを監視する**]パネルで[**追加**] をクリックして監視対象のアプリケーションを追加します。監視するアプリケーションは、最大 25 個まで追加できます。

リストに含まれていないアプリケーションを監視したい場合、該当のアプリケーションをカスタムアプリケーションとして追加し、ダッシュボードから監視することができます。その場合は、左下の[**独自アプリケーション**]をクリックして、[**アプリケーション名**]、および、アプリケーションが使用するIPアドレス[**IPアドレス/ホスト名**]と[**ポート**]番号を入力します。

入力後、[**保存**]を押下すると設定したアプリケーションが[**アプリケーションエクスペリエンスを監視する**]リストに入りますので、[**追加**]ボタンをクリックすればウィジェットに登録されます。

5. [**保存**]を押下し、変更内容を保存します。

ダッシュボード上のアプリケーションの表示とピン留め

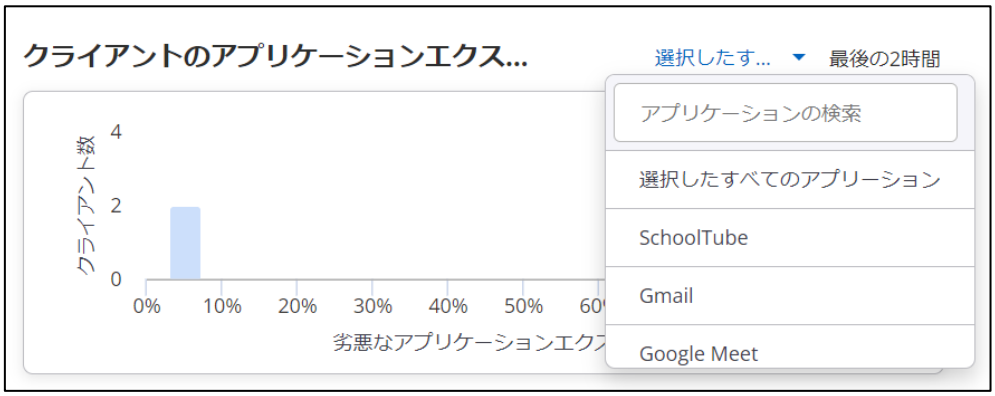
アプリケーションダッシュボードページでは、[**アプリケーションエクスペリエンス**]ウィジェット25個のアプリケーションのうち、5個をカードビューで表示します。25個すべてのアプリケーションのカードビューを表示するには、[**すべて表示**]をクリックします。

さらに、必要なアプリケーションをピン留めすることで、ダッシュボードに表示するアプリケーションを選択することができます。ダッシュボードにアプリケーションを固定してデフォルトで表示するには、[**アプリケーションエクスペリエンス**]ウィジェットの[**すべて表示**]をクリックし、Pinボタンを使ってアプリケーションを固定します。

アプリケーションをピン留めしていない場合、使用状況やアプリケーションエクスペリエンスに基づいて、自動でアプリケーションを決定、表示します。
ダッシュボードにアプリケーションを固定したくない場合は、[**最も影響を受ける**]（最も影響を受けたアプリケーション）または、[**最も使用される**]（最も使用されたアプリケーション）フィルタに基づいてアプリケーションをフィルタリングすることもできます。

クライアントのアプリケーションエクスペリエンス%分布 ウィジェット

このウィジェットは、過去2時間における各アプリケーションのクライアント数によるプリケーションQoEを表示します。また、過去2時間に、選択したすべてのアプリケーションで、いくつのクライアントのエクスペリエンスが低かったかを示す集計ビューもあります。単一のアプリケーションのアプリケーションエクスペリエンスのグラフを表示するには、[**選択したすべてのアプリケーション**]をクリックし、リストからアプリケーションを選択します。アプリケーションのQoEは、過去2時間分を参照することができます



2.4.4 WIPS情報を確認する

ネットワークに脅威をもたらす悪意のあるデバイス、または、企業のセキュリティポリシーに違反するデバイスの存在を手動で追跡することは現実的には困難です。WIPS（ワイヤレス侵入防止システム）は、そのプロセスを自動化しWi-Fiベースの脆弱性や攻撃から企業ネットワークを保護できます。また、企業内のアクセスポイントの物理的なロケーションを追跡することもできます。

備考：WIPSの詳細に関しては『WIPSの構成』を参照ください。

[ダッシュボード]>[WIPS]の順にクリックすると、以下の項目のグラフやウィジェットなどが表示されます。

パラメータ	概要
発生中のセキュリティアラート	現在発生中のセキュリティに関するアラートが表示されます。
自動侵入防止	Wi-Fiセキュリティの脅威、および、Wi-Fiセキュリティポリシーの違反を自動的に防ぐ機能のオン/オフが表示されます。
アラート	アラートのオン/オフが表示されます。
アクセスポイントの分類	アクセスポイントの分類が表示されます。
クライアントの分類	クライアントの分類が表示されます。
侵入防止ステータス	侵入防止ステータスが表示されます。
管理対象デバイス	管理対象デバイスが表示されます。
セキュリティアラート別の上位のロケーション	セキュリティアラート別の上位のロケーションが表示されます。
上位のセキュリティアラートカテゴリ	上位のセキュリティ・アラート・カテゴリが表示されます。

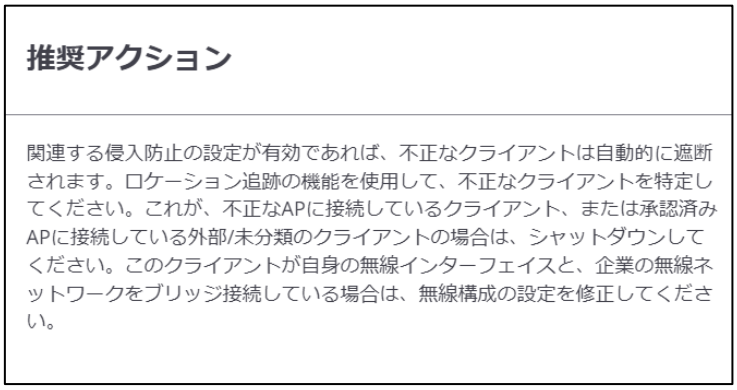
発生中のセキュリティ・アラート

現在発生中のセキュリティステータス/セキュリティ・アラートの詳細を確認するには、以下のパネルをクリックします。

クリックすると詳細ページにリダイレクトします。

また、任意のログを選択すると、詳細の状況や、問題発生時のタイムスタンプ等の追跡が可能です。

更に、詳細情報右の[推奨アクション]をクリックすると、本アラートを解決のための提案するための方法を提示されます。



自動侵入防止

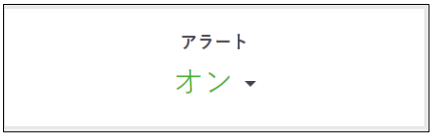
自動侵入防止のオン/オフを制御します。デフォルトではオフとなっています。

プルダウンを押下することで、オフ/オンの設定ができます。

任意で、[**サブフォルダーにも繰り返し適用します**]にチェックを入れることで、配下のフォルダーの自動侵入防止も有効化されます。

アラート

アラートのオン/オフを制御します。初期値は[**オン**]です。



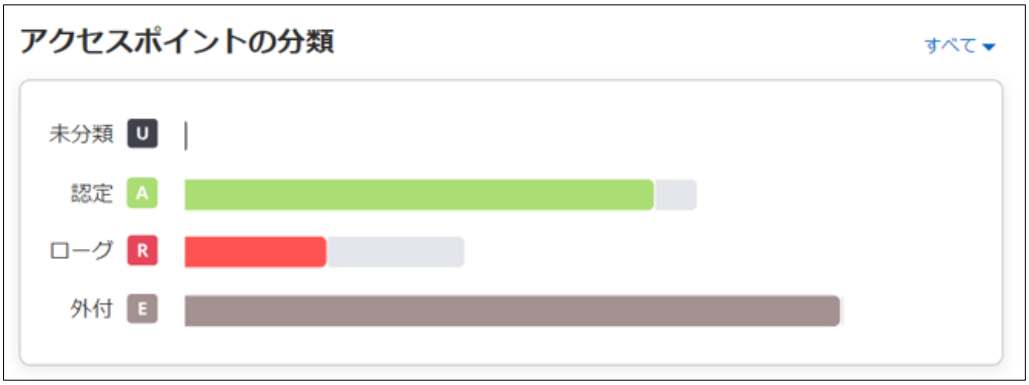
プルダウンを押下することで、オフ/オンの設定ができます。

任意で、[**サブフォルダーにも繰り返し適用します**]にチェックを入れることで、配下のフォルダーのアラート設定も変更されます。

アラートの詳細に関しては、『アラート』を参照ください。

アクセスポイントの分類

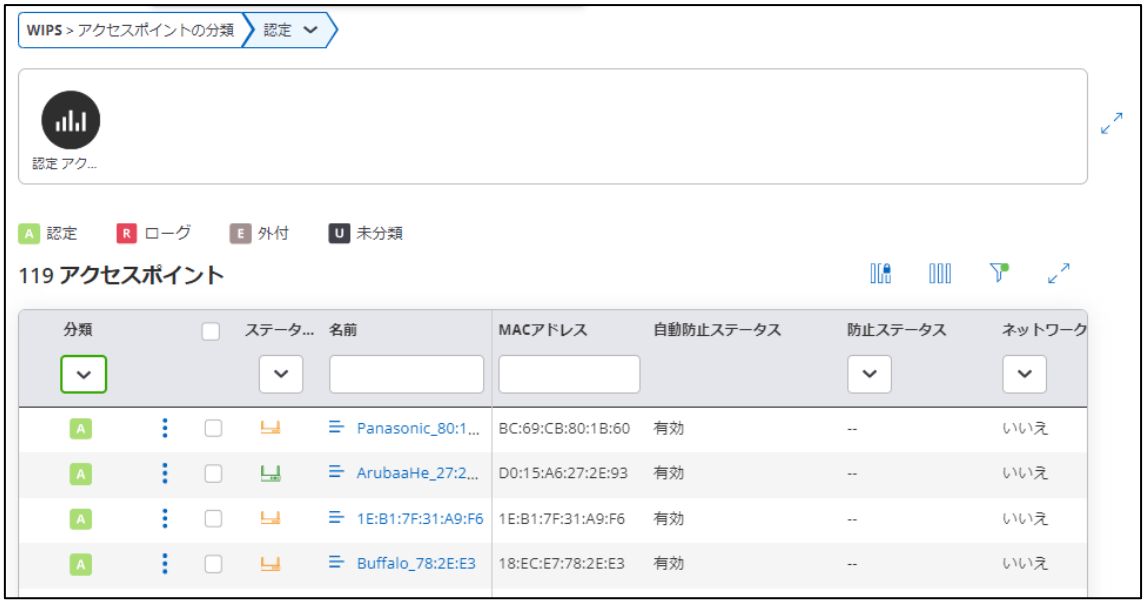
AIRRECT Cloudが認識しているアクセスポイントの分類が表示されます。



グラフ内右上のプルダウンから表示範囲（すべて/アクティブ/非アクティブ）を選択することができます。

各棒グラフの上にカーソルを置くと、内訳が表示されます。

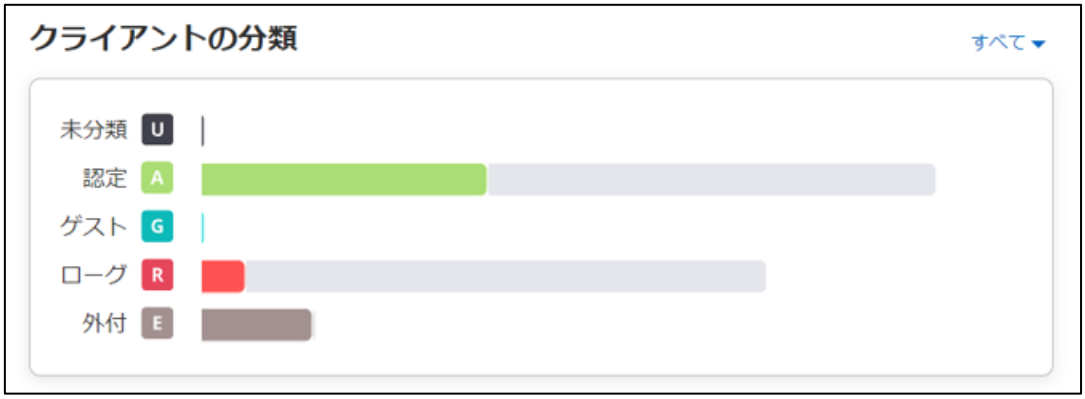
詳細を参照したい棒グラフをクリックすると、当該分類の詳細ページにリダイレクトします。



[**アクセスポイントの分類**]の詳細に関しては、『認定Wi-Fiポリシー』、および、『アクセスポイントの自動分類』をご参照ください。

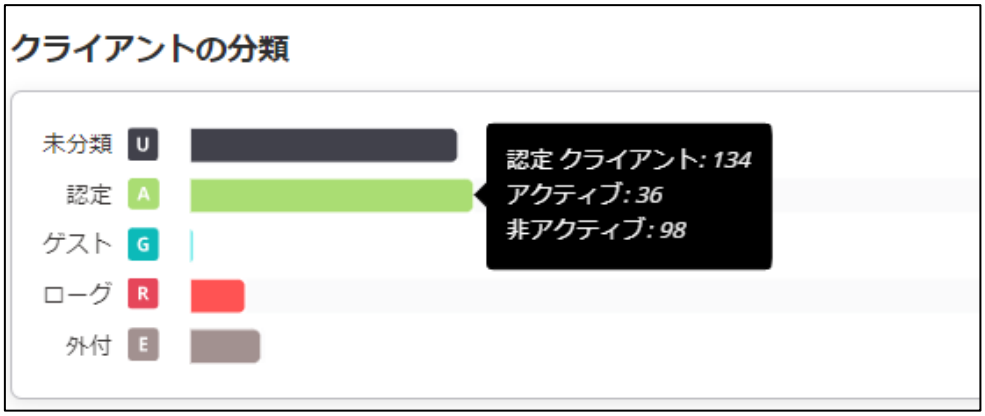
クライアントの分類

AIRRECT Cloud（AIRRECT AP）が認識しているクライアントの分類が表示されます。

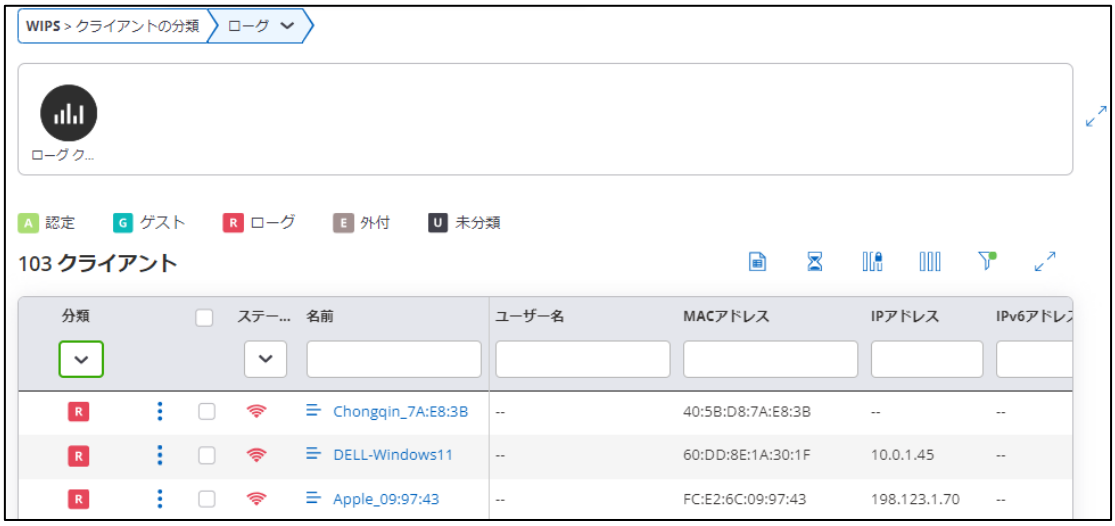


グラフ内右上のプルダウンから表示範囲（すべて/アクティブ/非アクティブ）を選択することができます。

各棒グラフの上にカーソルを置くと、内訳が表示されます。



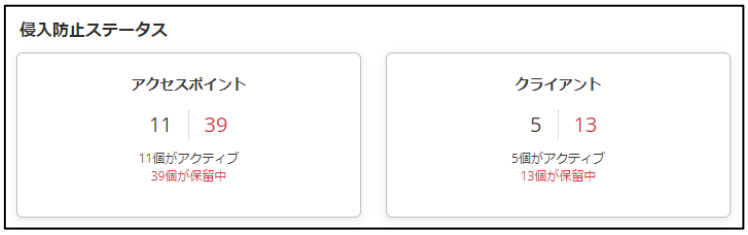
詳細を参照したい棒グラフをクリックすると当該分類の詳細ページにリダイレクトします。



[**クライアントの分類**]の詳細に関しては、『認定Wi-Fiポリシー』、および、『クライアントの自動分類』をご参照ください。

侵入防止ステータス

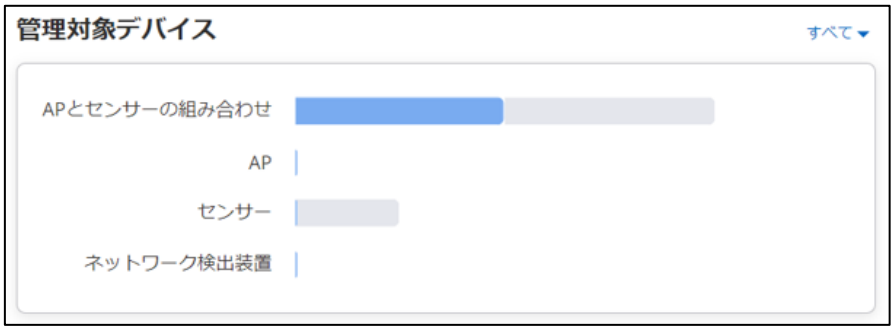
AIRRECT APの現在の侵入防止の稼働状況が表示されます。



左のアクティブの表記は、防御中のアクセスポイントまたはクライアントを表示します。

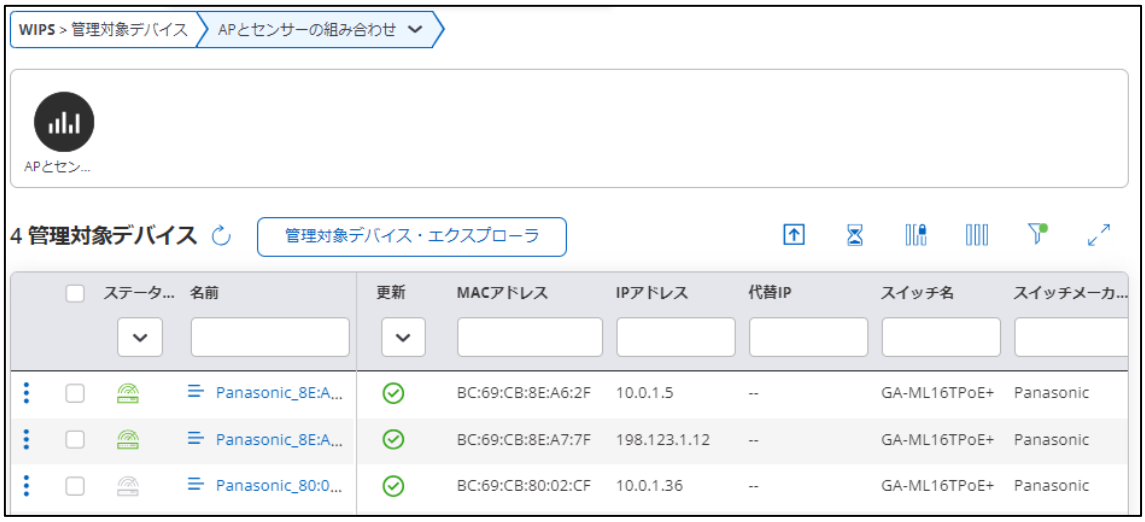
管理対象デバイス

AIRRECT Wi-Fiの管理対象デバイスの内訳が表示されます。



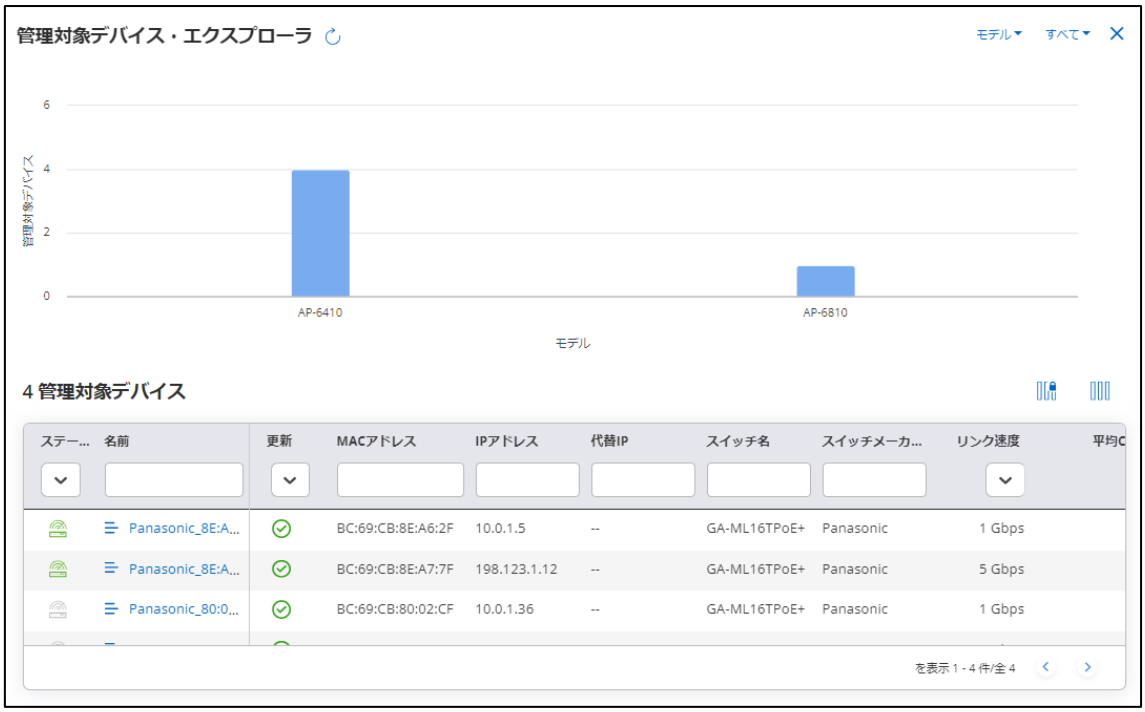
[**アクセスポイントの分類**]と同様に、グラフ内右上のプルダウンから表示範囲（すべて/アクティブ/非アクティブ）を選択することができ、各棒グラフの上にカーソルを置くと、その内訳が表示されます。

詳細を参照したい棒グラフをクリックすると、当該分類の詳細ページにリダイレクトします。



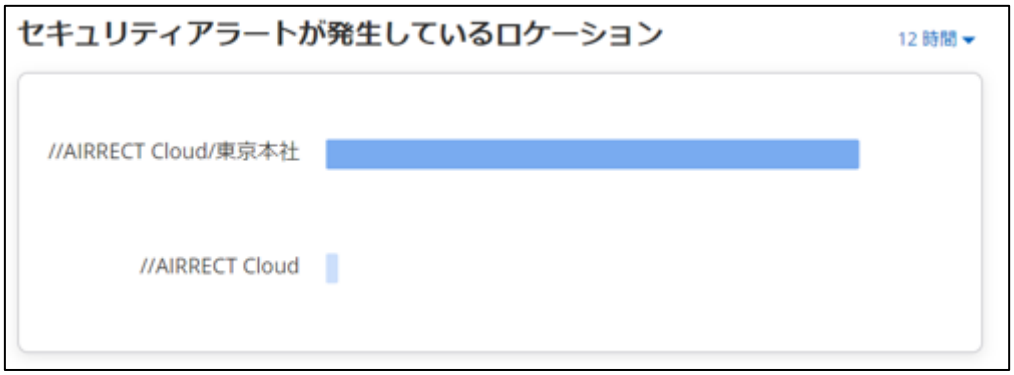
[**管理対象デバイスエクスプローラ**]を押下すると、該当の分類のアクセスポイントに関する情報が可視化できるクライアントエクスプローラ画面に移行します。

フィルター内容に関しては、『クライアントエクスプローラ』をご参照ください。



セキュリティアラートが発生しているロケーション

セキュリティアラート別が多く発生しているロケーションが降順で最大5つ表示されます。



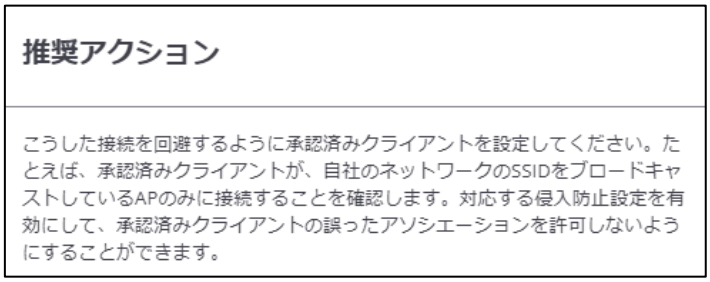
グラフ内右上のプルダウンから時間間隔（2時間/4時間/8時間/12時間/1日/1週間）を選択することでフィルタリングができます。初期値は12時間です。
また、各棒グラフの上にカーソルを置くと、アラート数が表示されます。

詳細を参照したい棒グラフをクリックすると当該分類の詳細ページにリダイレクトします。

任意のアラートを右クリックすることで、アラートの削除や重大度の設定変更等を行えます。アラートに関しては、[モニター]>[アラート]からも設定ができます。詳細は、『アラート』をご参照ください。

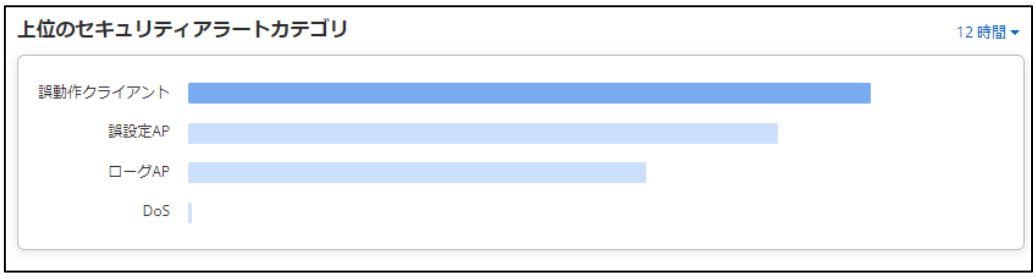
また、任意のアラートを選択すると、アラートの詳細と、ログの表示がされます。

また、[**推奨アクション**]をクリックすると、回避策の提案を表示することが出来ます。



上位のセキュリティ・アラート・カテゴリ

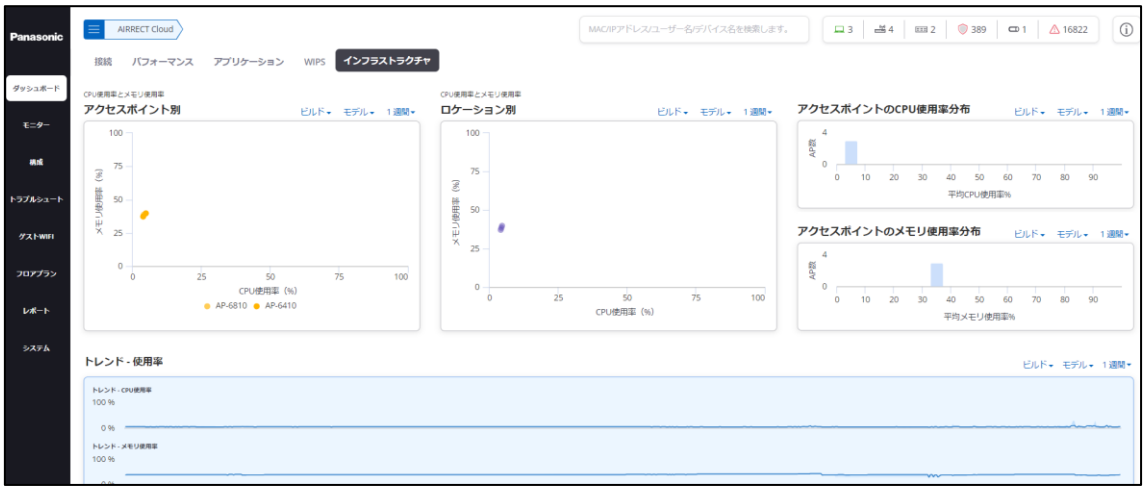
セキュリティアラートの種別で発生頻度が高いカテゴリが降順で最大５つ表示されます。



対象のカテゴリを選択すると、[**セキュリティアラートが発生しているロケーション**]と同様の詳細情報の確認が可能です。

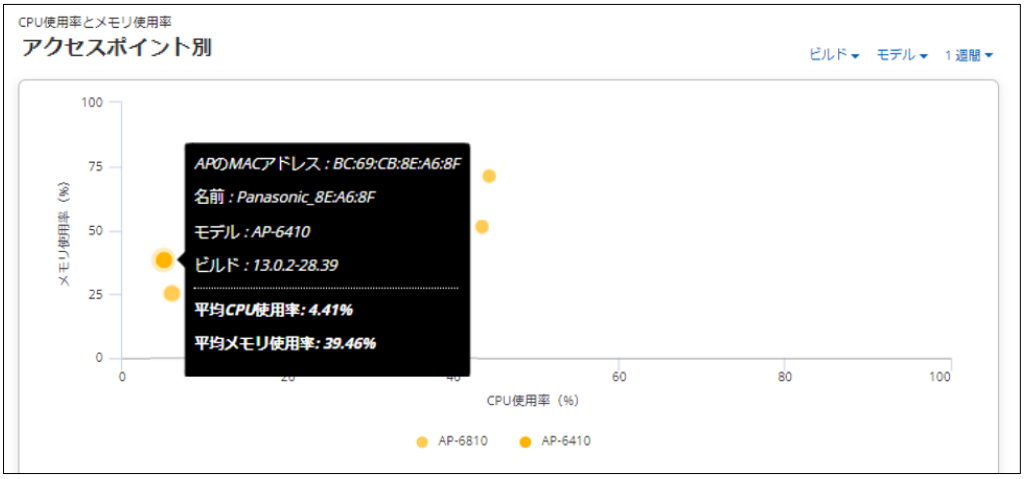
2.4.5 ハードウェアの情報を確認する（インフラストラクチャ）

インフラストラクチャダッシュボードから、アクセスポイントのハードウェアの状態を一括でモニタリングできます。
インフラストラクチャダッシュボードでは、AIRRECT Cloudに存在するすべてのアクセスポイントのCPU使用率とメモリ使用率から、平均CPU使用率とメモリ使用率が計算されグラフ表示します。これにより、ネットワーク障害が発生した場合、異常な動作を示しているアクセスポイントを特定しやすくなります。 また、CPU またはメモリの高負荷によって、再起動やカーネルパニックによるネットワークのダウンタイムにつながる可能性があります。そのようなアクセスポイントを特定することで、障害予防および是正措置を講じることができます。
インフラストラクチャ ダッシュボードは、[**ダッシュボード**]>[**インフラストラクチャ**]の順にクリックすると、以下の項目のグラフやウィジェットなどで表示されます。
●アクセス ポイントごとの CPU とメモリの使用率
●場所別の CPU とメモリの使用率
●CPU 使用率/メモリ使用率別の AP
●トレンド - CPU 使用率/メモリ使用率



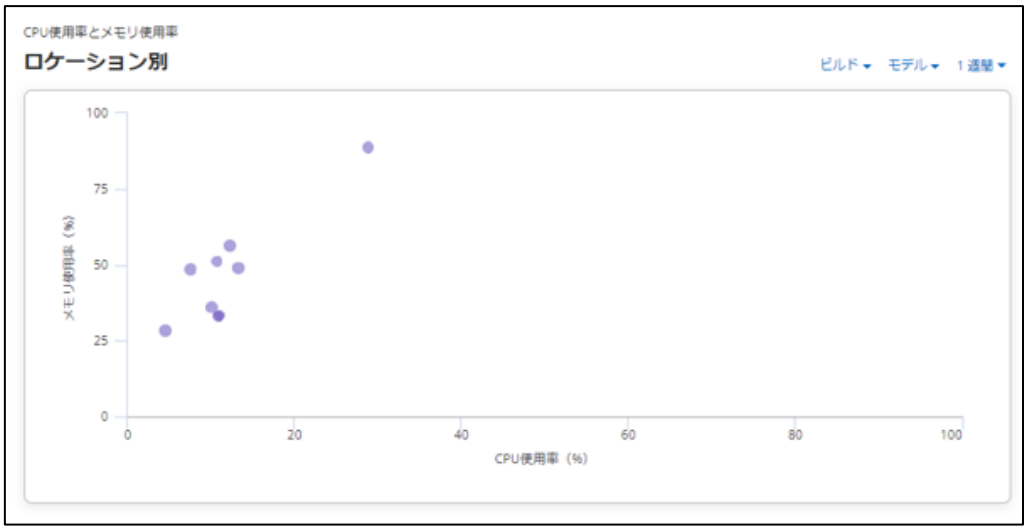
アクセスポイント別の CPU使用率とメモリ使用率サマリー

サーバー上のすべてのアクセスポイントのCPU対メモリ使用率データを表します。
散布図上の各データ ポイントは、各アクセスポイントのデータごとに表します。
各アクセスポイント上にカーソルを置くと、プロットされたデータポイントの概要が表示されます。さらに、データポイントをクリックするとアクセスポイントの詳細ページが表示されます。また、アクセスポイントのビルドバージョン、モデル名、継続時間で フィルタリングして表示を絞り込むこともできます。



ロケーション別のCPU使用率とメモリ使用率サマリー

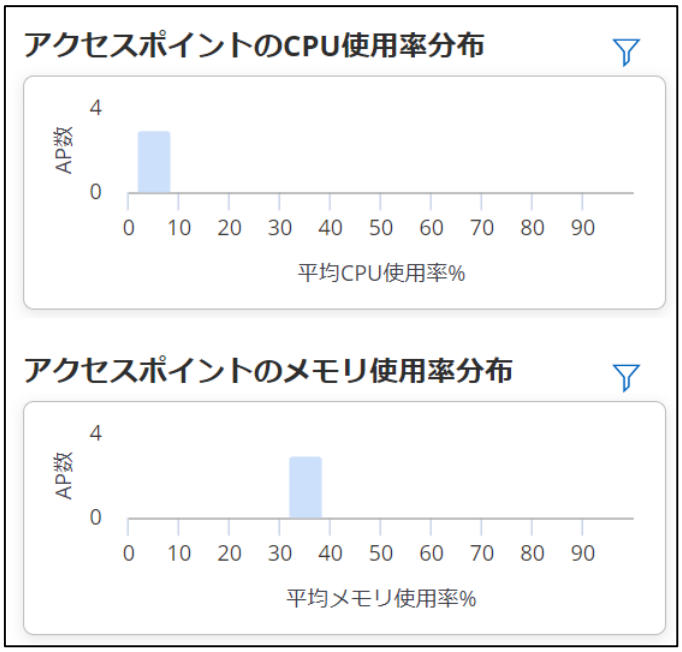
アクセスポイントをロケーションごとにグループ化します。選択されたロケーションとその子ロケーションのすべてのアクセスポイントがこのチャートでグラフ化されます。
各ロケーションにカーソルを合わせると、アクセスポイント数、平均CPU使用率、平均メモリー使用率についての詳細情報が表示されます。
また、アクセスポイントのビルドバージョン、モデル名、継続時間で フィルタリングして表示を絞り込むこともできます。



任意のデータをクリックすると、詳細が表示されます。

アクセスポイントのCPU使用率/メモリ使用率別分布

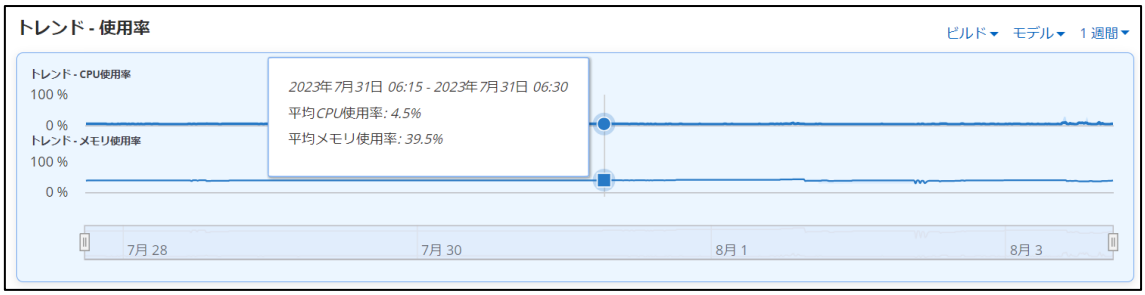
任意のバーにカーソルを合わせると特定の利用率の範囲にあるアクセスポイント数が表示され、バーをクリックすると、その詳細情報を表示することができます。
アクセスポイントの利用率が閾値以上である場合、バーが黄色で表示され、利用率が80%以上のアクセスポイントは赤色のバーで表示されます。
閾値は以下の式で算出されます。
閾値＝（全 AP の平均利用率＋標準偏差 *2)



トレンド - CPU使用率/メモリ使用率

選択したロケーションに設置されたすべてのアクセスポイントの平均CPUまたはメモリ使用率の平均的な使用率の傾向をパーセンテージで示します。

トレンドチャートは、絶対的なデータではなく、ロケーション内のアクセスポイント内で、比較データを使用して表示されます。特定の時間帯におけるトレンドの変化によって、管理者がネットワークの問題を特定するのに役立ちます。または、ハードウェアの負荷からネットワークの混雑が最も激しい時間帯を特定することもできます。



2.4.6 SLAダッシュボード

[**ダッシュボード**]>[**概要**]から[**SLA/リストビューに切り替える**]をクリックすることで、SLA ダッシュボードを開くことが出来ます。

SLA ダッシュボードでは、各ロケーションのサービス品質が表示されます。表示される内容は以下の通りです。

パラメータ	概要
接続	接続試行した端末に対する、接続が成功した端末の割合を表します。
パフォーマンス	接続成功端末に対する、パフォーマンスが良好な端末の割合を表します。
アプリケーションエクスペリエンス	対象のアプリケーション通信中の端末に対する、アプリケーションエクスペリエンスが良好な端末の割合を表します。
インフラストラクチャ	登録されているAPに対する、アクティブなAPの割合を表します。
不正AP	アクティブなローグAPの数を表します。

2.5 モニター機能

AIRRECT Cloudの[**モニター**]タブは、ネットワーク内の情報を監視する目的で利用されます。[**モニター**]タブにある監視対象の以下の各項目の情報を基に、トラブルシューティングを実行できます。

パラメータ	概要
クライアント	接続されているクライアントとAIRRECT APへの接続に失敗したクライアントのリストが表示されます。
アクセスポイント	アクセスポイントまたはアクセスポイント/センサーモードで動作しているAIRRECT APが一覧で表示されます。
無線通信	動作しているアクセスポイントが周波数毎に一覧で表示されます。
アクティブなSSID	SSIDプロファイルが一覧で表示されます。
アプリケーションの可視性	特定のSSIDで使用されているアプリケーションの情報が一覧で表示されます。
トンネル	トンネルの情報が一覧で表示されます。

右上のグローバルカウンターによって、クライアントとアクセスポイントの概要が表示されます。グローバルカウンターを使うと、以下の数値を取得できます。

●アクセスポイントの合計
●アクティブなアクセスポイントの合計
●インアクティブなアクセスポイントの合計
●現時点でのオンラインクライアントの合計

2.5.1 接続されているクライアントを確認する

[**クライアント**]**タブ**は、アクセスポイントに接続しているクライアントが表示されます。クライアントグリッドの右上にドロップダウンリストがあり、[**ライブ**]と[**すべて**]を選択できます。クライアントは、以下の基準でリスト化されます。

[**ライブ**]を選択した場合、以下のステータスのクライアントリストが表示されます。

●正常にアクセスポイントに接続できたクライアント

●接続に失敗したクライアント

[**すべて**]を選択した場合、[**ライブ**]の情報に加えて、以下のステータスのクライアントリストが表示されます。

●検知されているが、アクセスポイントに接続していないクライアント

●現在検知されていないが、以前アクセスポイントに接続していたクライアント

●現在検知されておらず、以前接続に失敗したクライアント

クライアントモニター画面では、現在接続しているクライアントが一覧表示されます。

各クライアントは、右クリックすると以下のアクションが選択できます。

アクション	概要
名前を変更	クライアント名を変更します。
パケットトレースをキャプチャ	特定の端末間を通過または移動するデータパケットの取得をします。
パケットトレースの履歴	過去30分間にキャプチャされたパケット・レースが表示されます。
ライブクライアントデバックを開始	クライアントに関するライブ・クライアント・ログが表示されます。
切断	クライアントを切断します。
デバイス・タグを更新する	デバイス・タグを更新します。
検索	クライアントの端末の位置がフロアマップ上に表示されます。

クライアント一覧画面では、以下のようにクライアントの情報が表形式で表示されます。また、リストの上部にある[**クライアントビュー**]をクリックし[**リンクビュー**]を選択すると、リストがクライアントのリンク情報に切り替わります。

パラメータ	概要
ステータス	クライアントが正常にアソシエーションされているか、接続に失敗したかを表します。
名前	クライアント名を表します。
MACアドレス	メーカーによってネットワークアダプタに割り当てられたクライアント固有のMACアドレスを表します。
リンクMACアドレス	クライアントのリンクMACアドレスを表します。 ※リンクビューで表示されます
ユーザー名	クライアントのユーザー名を表します。
ローカル管理されているアドレス	クライアントがランダムMACアドレスを使用している場合、「はい」と表示されます。
IPv4アドレス	クライアントのIPv4アドレスを表します。
IPv6アドレス	クライアントのIPv6アドレスを表します。
VLAN	クライアントのVLANを表します。
OS	クライアント先で運用しているOSを表します。
関連付けられたアクセスポイント	クライアントがアソシエーションされているアクセスポイントを表します。
関連付けられたSSID	クライアントがアソシエーションされているアクセスポイントのオペレーティングSSIDを表します。
セキュリティ	接続に使用しているセキュリティレベルを表します。
認証	接続に使用している認証方式を表します。
周波数帯	クライアントが接続している周波数帯を表します。
Wi-Fi規格	クライアントと接続している802.11プロトコルを表します。 ※過去に接続した中で最新のプロトコル表記を保持します。例えば、Wi-Fi6で接続後、Wi-Fi5で接続した場合も、表記はWi-Fi 6となります。
チャネル	クライアントが接続しているチャネルを表します。
RSSI (dBm)	クライアントのRSSI(受信信号強度)を表します。
最も近いAP RSSI (dBm)	クライアントから最も近いAPのRSSI(受信信号強度)を表します。
アップリンクデータ	クライアントによって転送されたデータ量を表します。
ダウンリンクデータ	クライアントが受信したデータ量を表します。
平均データレート	単位時間あたりの平均データレートを表します。

再試行率(%)	再試行率をパーセントで表します。
SNR(dB)	クライアントの信号/ノイズ比を表します。
接続・切断された日時	クライアントがシステムアップまたはダウンしてからの日時を表します。
最初の検出	最初にクライアントが検出された日時を表します。
ロケーション	クライアントが接続されている場所を表します。
スティッキー	アクセスポイントに接続しているクライアントが、ローミング中に信号強度が高い別のアクセスポイントを見つけた場合でも、元のアクセスポイントとの接続を維持している場合、「はい」と表示されます。
メーカー名	クライアントのメーカー名を表します。
ロール	クライアントがSSID経由で接続された後は、SSIDプロフィールで設定されたロールが割り当てられます。
Google認可	クライアントがグーグル統合を使用して承認されているかどうかを表すブール値を表します
キャプティブポータルの認証ステータス	クライアントがキャプティブポータルを用いた認証で接続されているかどうかを表します。
タグ	ユーザーが設定したタグを表します。
手動タグ付け	クライアント端末を別のロケーションに移動した場合に「はい」と表示されます。
帯域能力	クライアントが接続可能な帯域が表示されます。
ローカル認証	クライアントがローカル認証で接続されているかどうかを表します。
MLO	MLOクライアントであるかどうかを表します。

クライアントテーブルの右上にある[**進行中のアクティビティを表示**]オプション を使用すると、各クライアントに関する 進行中のアクティビティが表示されます。

利用可能なアクティビティは、以下の通りです。

●ライブクライアントデバッグ：クライアントのアクティビティをトラブルシューティングできます。選択すると、アクティビティが進行中のクライアントが表示されます。

●パケットトレース：パケットキャプチャを実行中のクライアントが表示されます

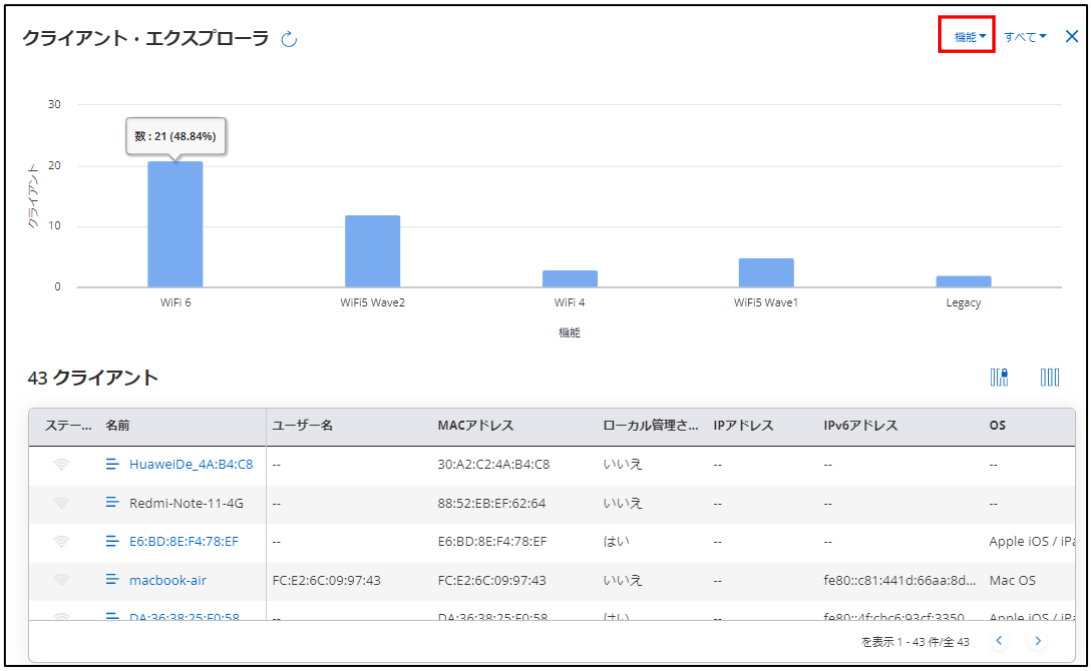
●防御：防御アクティビティで隔離されたクライアントが表示されます。

●なし：すべてのクライアントが表示されます。

クライアントエクスプローラ

クライアントエクスプローラでは、クライアントの機種や状態、情報を棒グラフで表示します。[**クライアントエクスプローラ**]画面を表示するには、[**モニター**]>[**クライアント**]>[**クライアントエクスプローラ**]の順にクリックします。

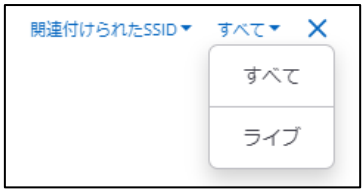
右上のフィルターで、表示したいグラフに変更します。



フィルタによって、以下のパラメータに切り替えることができます。

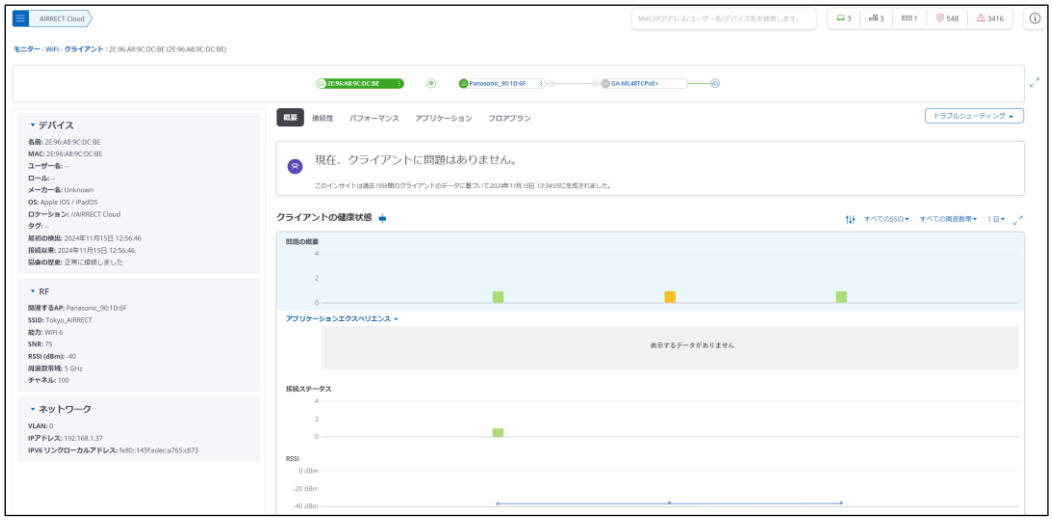
パラメータ	概要
関連付けられたSSID	クライアントがアソシエーションされているアクセスポイントのSSIDごとに分類します。
メーカー名	クライアントのメーカー名ごとに分類します。
Wi-Fi規格	クライアントが接続している、または対応している最新のWi-Fi規格ごとに分類します。
チャネル	クライアントが接続しているチャネルごとに分類します。
アソシエートされているAP	クライアントがアソシエーションされているアクセスポイントごとに分類します。
接続障害タイプ	クライアントが接続失敗した際の種別ごとに分類します。
プロトコル	クライアントの周波数ごとに分類します。
Google認証ステータス	クライアントがグーグル統合を使用して承認されていかいないかで分類します。
ロール	クライアントに適用されているロール名ごとに分類されます。
OS	クライアントで利用しているOSを表します。

また、[**ライブ**]のフィルタは、現在アソシエーションされているクライアントのみ表示されます、[**すべて**]を選択すると、過去にアソシエーションされたクライアントや、接続に失敗したクライアントも含めて表示がされます。



クライアントダッシュボード

クライアントリストまたは任意のダッシュボードからクライアント名をクリックすると、クライアントダッシュボードを確認できます。



●クライアント接続ウィジェット

ダッシュボード上部に、選択したクライアントのネットワーク接続経路を表示するウィジェットが表示されます。任意のデバイスにカーソルを合わせると詳細情報が表示されます。また、アイコンの横にある[⋮]をクリックすると、そのデバイスで実行可能なアクションが表示されます。

●クライアントプロパティウィジェット

ダッシュボード左部に、次のセクションが表示されます。

・デバイス：デバイスの詳細

・RF：接続している無線の詳細

・ネットワーク：ネットワークの詳細（接続されたクライアントでのみ利用可能）

●クライアントダッシュボードタブ

クライアントダッシュボードには、クライアント接続ウィジェット、クライアントプロパティウィジェット、およびクライアントの詳細を示すさまざまなチャートとグラフを含む複数のタブが含まれています。

概要

[**概要**]タブの画面上部には、クライアントに発生している問題の分析とその解決策が表示されます。

「クライアントの健康状態」には、アプリケーションエクスペリエンス、接続ステータス、RSSI、データ・レート、再試行率%など複数のグラフが表示されます。このグラフはカスタマイズマーク から構成を変更することができ、特定のグラフを追加・削除したり、グラフの表示順を変更したりできます。

接続性

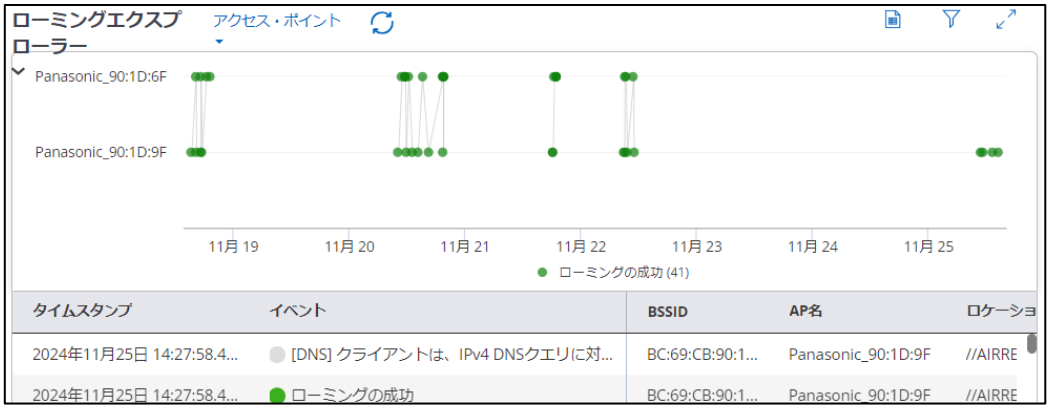
[**接続性**]タブでは、クライアントのアソシエーションやローミングに関する情報を確認できます。

●ローミングエクスプローラー

ローミングエクスプローラーでは、クライアントのローミングログをグラフで確認することができます。グラフは縦軸がアクセスポイント名（ローミングイベント数の降順）、横軸が日時で構成されています。

ローミングエクスプローラーを表示するには以下の手順を行います。

1. [**モニター**]>[WiFi]>[**クライアント**]の順に移動します。
2. ローミングエクスプローラーを表示させるクライアント名をクリックします。
3. [**接続性**]タブを開きます。



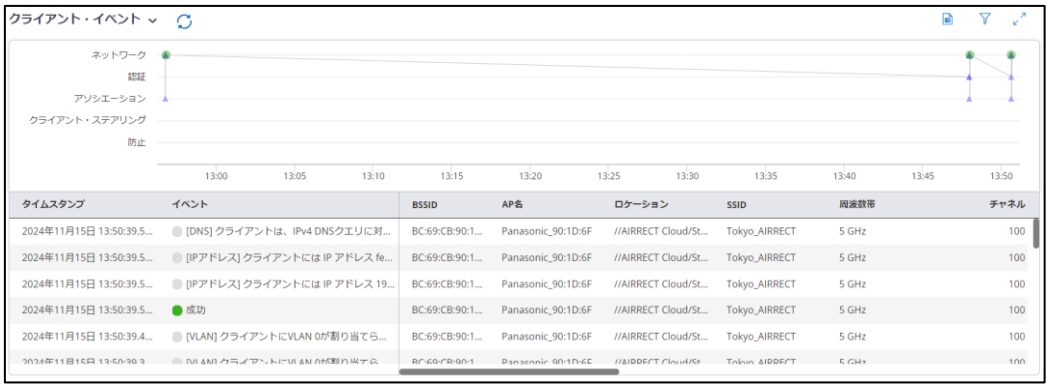
グラフ上のプロットへカーソルを合わせると以下のイベントの詳細を表示できます。

パラメータ	概要
タイムスタンプ	クライアントがアクセスポイントに接続した日時を表します。
イベント	クライアントが正常にローミングされたかどうかを表します。
BSSID	クライアントが接続したBSSIDを表します。
AP名	クライアントが接続したアクセスポイントの名前を表します。
SSID	クライアントが接続したSSIDを表します。
チャネル	クライアントが接続したアクセスポイントの動作チャネルを表します。
ロケーション	クライアントが接続したロケーションを表します。
周波数帯	クライアントが使用している周波数帯を表します。

●**クライアント・イベント**

クライアント・イベントを表示させるには以下の手順を行います。

1. [**モニター**]>[WiFi]>[**クライアント**]の順に移動します。
2. クライアント・イベントを表示させるクライアント名をクリックします。
3. [**接続性**]タブを開き[**ローミングエクスプローラー**]をクリックして、プルダウンから[**クライアント・イベント**]を選択します。



クライアントのイベントログは接続の試行を含むクライアント・イベントの大部分がリスト化されます。表記にある、緑色は正常な接続イベントを表し、灰色はイベントフローを表します（グラフ上では青色でプロットされます）。また、赤色は失敗した接続イベントを表します。

グラフ・ログで表示されるパラメータの詳細は以下の通りです。

パラメータ	概要
タイムスタンプ	クライアントがアクセスポイントに接続した日時を表します。
イベント	クライアントの接続状態に関する情報を表します。
BSSID	クライアントが接続したBSSIDを表します。
AP名	クライアントが接続したアクセスポイント名を表します。
ロケーション	クライアントが接続したロケーションを表します。
SSID	クライアントが接続したSSIDを表します。
周波数帯	クライアントが使用している周波数帯を表します。
チャネル	クライアントが接続したアクセスポイントの動作チャネルを表します。
パケットキャプチャ	障害発生時のパケットを表します。
DHCPサーバーIPv4	DHCPサーバーのIPv4アドレスを表します。
DNSサーバーIPv4	DNSサーバーのIPv4アドレスを表します。
AAAサーバーIPv4	AAAサーバーのIPv4アドレスを表します。
AAAサーバーのホスト名	AAAサーバーのホスト名を表します。

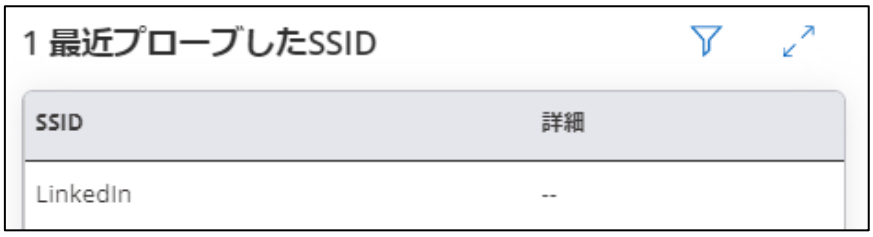
DHCPサーバーIPv6	DHCPサーバーのIPv6アドレスを表します。
DNSサーバーIPv6	DNSサーバーのIPv6アドレスを表します。
AAAサーバーIPv6	AAAサーバーのIPv6アドレスを表します。
DHCP遅延	DHCP通信のレイテンシを表します。
DNS遅延	DNS通信のレイテンシを表します。
AAA遅延	AAA通信のレイテンシを表します。

クライアント接続ログのイベント列の赤色の記号は、クライアントの接続障害を表しています。赤色の記号にカーソルを合わせると、障害の種類が確認できます。その種類は、以下の通りです。

障害の種類	概要
アソシエーションエラー	アクセスポイントアソシエーションの制限を超えている等のアソシエーションエラー。
認証エラー	Eapol 4wayハンドシェイクの失敗、Pre-Shared Keyの誤り等の認証エラー、キャプティブポータルの認証失敗。
ネットワークエラー	DHCPの障害、WAN障害等のエラー。

●最近プローブした SSID

クライアントで最近接続したSSIDを表します。



●アソシエーション履歴

クライアントが最近接続したアクセスポイントの履歴を表します。

●このクライアントを認識しているデバイス

選択しているクライアントを認識しているアクセスポイントのリストを表します。画面の左上には、クライアントを認識している アクセスポイントの総数と、クライアントにアソ

シエーションされているアクセスポイントの名前が表示されています。

以下が、上記の画面に関する説明となります。

パラメータ	概要
名前	クライアントを認識しているアクセスポイントの名前を表します。
RSSI (dBm)	クライアントとアクセスポイント間の信号強度を表します。
無線1の動作チャンネル	2.4GHzが動作しているチャネルを表します。
無線2の動作チャンネル	5GHzが動作しているチャネルを表します。
無線3の動作チャンネル	6GHzが動作しているチャネルを表します。
2.4GHz アソシエーション	2.4GHz無線にアソシエーションされているクライアントの数を表します。
5GHz アソシエーション	5GHz無線にアソシエーションされているクライアントの数を表します。
6GHz アソシエーション	6GHz無線にアソシエーションされているクライアントの数を表します。

アクセスポイント名をクリックすると、**アクセスポイントの情報**ページが表示されます。

パフォーマンス

[**パフォーマンス**]タブでは、クライアントの通信品質に関するグラフを確認できます。
このグラフはカスタマイズマーク から構成を変更することができ、特定のグラフを追加・削除したり、グラフの表示順を変更したりできます。
表示できるグラフは以下の通りです。

●RSSI
●データ・レート
●再試行率%
●トラフィック量
●トラフィック量 - アップリンク
●トラフィック量 - ダウンリンク

アプリケーション

[アプリケーション]タブでは、クライアントが使用するアプリケーションに関する情報が表示されます。

上部に表示されるグラフは**カスタマイズマーク**から構成を変更することができ、特定のグラフを追加・削除したり、グラフの表示順を変更したりできます。

表示できるグラフは以下の通りです。

●申請数

●アプリケーションエクスペリエンス

●アプリケーションエクスペリエンスの低下 - アップストリーム（クライアントから）

●アプリケーションエクスペリエンスの悪さ - ダウンストリーム（クライアントへ）

●アプリケーション遅延時間

●有線アプリケーションの遅延

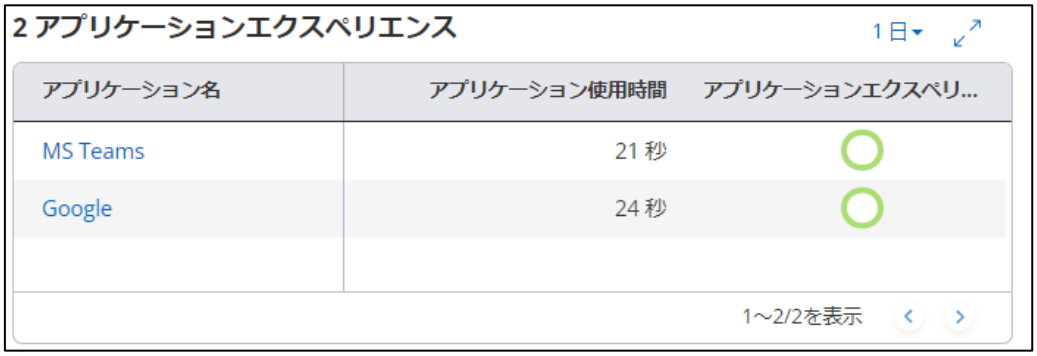
●ワイヤレスアプリケーションの遅延

●利用頻度の高いアプリケーション

[利用頻度の高いアプリケーション]グラフは、アプリケーションに関するデータ使用量を表しています。このグラフは、常にトラフィック量が多い上位5つのアプリケーションデータを表します。正確にデータ使用量を表示するには、グラフ内の特定のバーにカーソルを合わせます。

●アプリケーションエクスペリエンス

クライアントが使うアプリケーションの詳細が表示されます。



●アプリケーションエクスプローラー

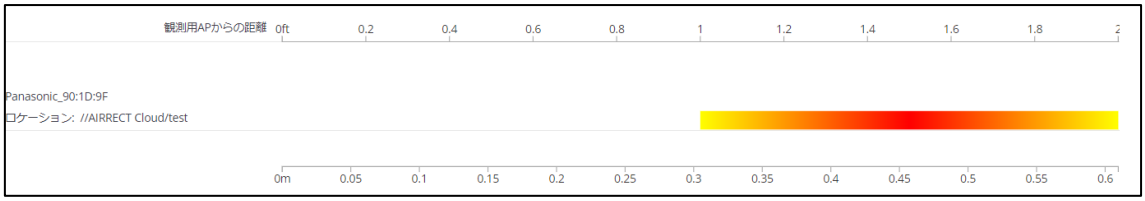
グラフ左上にある[**アプリケーションエクスプローラー**]をクリックすると、アプリケーションエクスペリエンスのグラフと表をまとめた画面が表示されます。

フロアプラン

[**フロアプラン**]タブでは、フロア上のクライアントの位置が表示されます。フロアプランにクライアントが配置されるためには、同じ周波数帯域で動作する3台以上のAPがクライアントを認識し、かつそのAPがフロア上に配置されている必要があります。

フロアにアクセスポイントが3つ以上ない場合、代わりに位置情報ビューが表示されます。

位置情報ビューは、クライアントと観測用AP間の距離を表します。



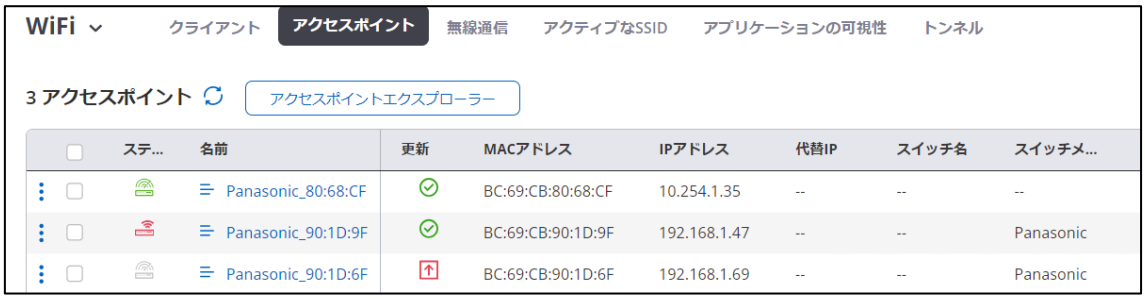
クライアント名の変更

クライアント名を変更するには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**クライアント**]の順にクリックすると、クライアントのリストが表示されます。
2. 名前を変更する場合、クライアント名を右クリックするか、メニュー・アイコン ⋮ で[**名前を変更**]をクリックすると、[**クライアントの名前を変更**]のページが表示されます。
3. クライアント名の変更後は、[**終了**]をクリックするとその変更が保存されます。
   最後に、クライアント名が変更されたことが、メッセージで通知されます。

2.5.2 管理しているアクセスポイントを確認する

アクセスポイントタブには、アクセスポイントの名前、IPアドレス、ステータスなどの詳細情報が表示されます。



以下のアクセスポイントに関する情報が表示されます。

パラメータ	概要
ステータス	アクセスポイントのステータスを表します。アクセスポイントがアクティブ状態であればアイコンは緑色となり、非アクティブの場合は、灰色になります。 注意：アクセスポイントから10分間KEEP-ALIVEパケットが10分間受信できなかった場合に非アクティブと判定されます。そのため、切断したから灰色アイコンに切り替わるまで、10分程度かかります。 アクティブ時も、状態によって、アイコンが異なります。 ：正常に動作している場合 ：フェイルセーフモードなど異常な動作の場合
名前	アクセスポイントの名前を表します。
MACアドレス	アクセスポイントのMACアドレスを表します。
モデル	アクセスポイントのモデル名を表します。
場所	アクセスポイントのロケーションを表します。
更新	ファームウェアの更新ステータスを表します。
IPアドレス	アクセスポイントのIPv4アドレスを表します。
代替IP	アクセスポイントのIPv6アドレスを表します。
スイッチ名	アクセスポイントと接続しているスイッチングハブの品名を表します。
スイッチメーカー	アクセスポイントと接続しているスイッチングハブのメーカー名を表します。
リンク速度	アクセスポイントの有線ポートが接続しているリンクスピードを表します。

パラメータ	概要
平均CPU使用率%	アクセスポイントの平均CPU使用率を表します。
平均メモリ使用率%	アクセスポイントの平均メモリ使用率を表します。
ビルド	ビルド番号を表します。
最終更新時刻	ファームウェアを最後に更新した日時を表します。
更新予定日時	アップデートのスケジュール機能で設定したファームウェア更新開始日時を表します。
接続・切断された日時	アクセスポイントがアップまたはダウンしてからの日時を表します。
最終起動日	アクセスポイントの最終起動日を表します。
アソシエーション件数	アクセスポイントに接続されているクライアント数を表します。
電源	アクセスポイントが供給されている電源を表します。
Wi-Fi規格	アクセスポイントのWi-Fi規格を表します。
グループ	選択したアクセスポイントに適用されているグループを表します。
SSID	クリックすると、割り当てられているSSID名が表示されます。
メッシュモード	メッシュモードを表します。 詳細は「メッシュネットワーク」をご参照ください。
タグ	アクセスポイントのタグを表します。
フェイルセーフモード	フェイルセーフモードのオン/オフを表します。フェイルセーフモードは、機器の予期せぬ故障を防ぐために、15分間で10回再起動を繰り返したときに移行します。フェイルセーフモードから復旧させるには、アクセスポイントを再起動する必要があります。

注意：アクセスポイントが接続するスイッチングハブの情報は、LLDPパケットで取得します。スイッチングハブでLLDPが無効の場合、スイッチ名等の情報を取得することができません。当社製スイッチングハブの場合、デフォルトでLLDPが無効のため、CLIにて以下の設定が必要です。

【設定例：GA-MLシリーズ、MGA-ML4TWPoE++共通】

⑴スイッチ名設定　｜　(config)# snmp-server name <switch name>

➡スイッチ名が設定済みの場合は⑴はスキップして下さい。

⑵LLDP有効化　｜　(config)# lldp run

⑶スイッチ名の表示 ｜　(config-if)# lldp tlv-select system-name

その他の機種のコマンドについては、各スイッチングハブのCLIリファレンスをご確認ください。

アクセスポイントテーブルの右上にある [**進行中のアクティビティを表示**]オプションを使うと、アクセスポイントで進行中のアクティビティが表示されます。アクセスポイントで表示されるライブ・アクティビティのリストは、以下の通りです。

パラメータ	概要
パケットトレース	パケットのキャプチャ後、検査をおこなうことでネットワークの問題に関する診断や解決に役立ちます。このアクティビティをクリックすると、パケットトレースが動作中のデバイスに関するリストが表示されます。
防御	防御アクティビティには、すべての検疫デバイスに関するリストが表示されます。
クライアント接続テスト	クライアント接続に問題があるアクセスポイントをトラブルシューティングします。クライアント接続テスト・アクションには、トラブルシューティングが進行中のデバイスに関するリストが表示されます。
スペクトラム分析	使用率とスペクトラム密度、各チャネルのパワーレベルの解析や、無線Wi-Fi以外の電波干渉を確認しているアクセスポイントを表示します。
LED点滅中	LEDが点滅中のアクセスポイントを表示します。
なし	フィルタなしのアクセスポイントリストがすべて表示されます。

すべてのアクセスポイントにおいて、以下のアクションを実行できます。これらのアクションは、アクセスポイントを右クリックして任意で実行できます。

アクション	概要
クライアント接続テストを実行	クライアント接続試験を実施します。
パケットトレースをキャプチャ	パケットをトレースすることで、アクセスポイントのトラブルシューティングができます。
パケットトレースの履歴	クリックしたアクセスポイントのパケットトレース履歴が表示されます。
イベントログの表示	アクセスポイントのイベントログを保持しているテーブルを表します。
デバッグログをダウンロード	デバッグログをダウンロードします。
デバッグログの履歴	デバッグログの履歴を確認します。
Webシェルを開く	AIRRECT Cloudから指定したアクセスポイントのCLIを開きます。
RFエクスプローラを表示	RFエクスプローラを表示します。
送信出力またはチャネル	アクセスポイントの送信電力をカスタマイズできます。
VLAN	アクセスポイントが監視しているVLANのリスト全体をカスタマイズできます。
IPSec認証情報	IPSec認証情報をカスタマイズできます。
アラートを設定	しきい値を超えたときのアラートをカスタマイズできます。
ファームウェアの更新	このオプションを使うとアクセスポイントのファームウェアが、最新または前回のバージョンに更新されます。
グループに割り当て/再割り当て	グループへの割り当て/再割り当てを制御します。
検索	このオプションを使うと、アクセスポイントが配置されているフロアマップ上のロケーションにリダイレクトします。
アクセス・ポイントをグループから削除	アクセスポイントをグループから削除します。
再起動	アクセスポイントを再起動します。
名前を変更	アクセスポイントの名前を変更します。
タグを変更する	アクセスポイントのタグを変更します。
移動	アクセスポイントのロケーションを変更できます。
削除	アクセスポイントのリストからアクセスポイントを削除します。

アクセスポイントリストまたは任意のダッシュボードからアクセスポイント名をクリックすると、アクセスポイントダッシュボードを確認できます。

アクセスポイントのダッシュボード

詳細ページの画面左に、以下アクセスポイント情報が表示されます。

●基本

アクセスポイントの名前やMACアドレスなど、基本情報が表示されます。

●APの正常性

アクセスポイントのCPU使用率、メモリ使用率を表示されます。

●構成

アクセスポイントが所属しているロケーションやメッシュモード、各無線の設定など構成状態が表示されます。

●有線のプロパティ

アクセスポイントの有線ポート情報が表示されます。

●ダイナミックVLAN

ダイナミックVLANの情報が表示されます。

概要

[**概要**]タブでは、アクセスポイントイベント、CPU 使用率、メモリ使用率、トラフィック量、クライアント数、チャネル使用率のグラフが表示されます。

グラフはカスタマイズマーク から構成を変更することができ、特定のグラフを追加・削除したり、グラフの表示順を変更したりできます。

RF

[RF]タブでは、無線に関する情報が表示されます。

パラメータ	概要
スペクトル占有率	RFスペクトル全体のアクティブな無線とクライアントの数が表示されます。
チャネル使用率	APチャネルの使用率が表示されます。
チャネルマップ	チャネル毎のデバイス数がグラフで表示されます。
このAPを認識している無線	デバイスを監視している管理対象デバイスのリストが表示されます。
メッシュ・ネットワーク・リンク	APのメッシュネットワークが表示されます。
ラジオネイバーズ	近隣の無線が表示されます。

クライアントエクスペリエンス

[**クライアントエクスペリエンス**]タブでは、アクセスポイントに接続されているクライアント情報に関するグラフが表示されます。

グラフはカスタマイズマーク から構成を変更することができ、特定のグラフを追加・削除したり、グラフの表示順を変更したりできます。

パラメータ	概要
アプリケーションエクスペリエンス	アプリケーション使用量に関する分析の概要が表示されます。
トラフィック量	クライアントのデータ使用量が表示されます。
ベースライン - 接続に失敗したクライアント	接続に失敗したクライアントに関するベースラインが表示されます。
ベースライン- パフォーマンス不良によって影響を受けたクライアント	パフォーマンス低下によって、一定期間に影響を受けたクライアントの割合 (%) に関するベースラインが表示されます。
再試行率 %	選択されたアクセスポイントに接続しているクライアントの再試行率 (%) が表示されます。
平均データレート	各クライアントの平均データレートが表示されます。
クライアント数	クライアント数が表示されます。
平均データレート分布	クライアントの平均データレートの分布が表示されます。
RSSI分布	クライアントのRSSI(受信電波強度)の分布が表示されます。
再試行率別のクライアント(%)	クライアントの再試行率の分布が表示されます。
利用頻度の高いアプリケーション	利用頻度が高い上位5つのアプリケーションとその使用量が表示されます。

WIPS

[WIPS]タブでは、WIPS 情報が表示されます。

パラメータ	概要
可視BSSID – 管理対象	選択したアクセスポイントが認識している管理対象のBSSID（アクセスポイント）のリストが表示されます。
可視BSSID – 管理対象外	選択したアクセスポイントが認識している管理対象外のBSSID（アクセスポイント）のリストが表示されます。

可視VLAN	選択したアクセスポイントが認識しているVLANが表示されます。
可視クライアント	選択したアクセスポイントが認識しているクライアントが表示されます。

イベントログ

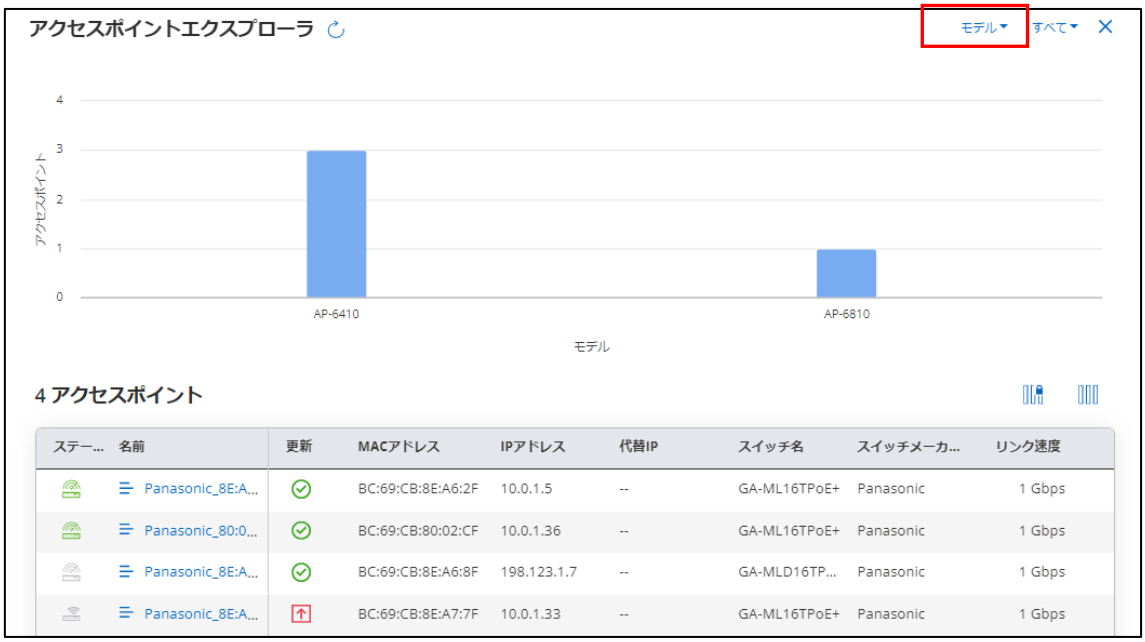
[**イベントログ**]タブでは、アクセスポイントのイベントログが表示されます。

CCT結果

[**CCT結果**]タブでは、CCT（クライアント接続テスト）の結果が表示されます。

アクセスポイントエクスプローラ

アクセスポイントエクスプローラでは、アクセスポイントの機種や状態、スイッチ名等の以下の情報を棒グラフで表示します。[**アクセスポイントエクスプローラ**]画面を表示するには、[**モニター**]>[**アクセスポイント**]>[**アクセスポイントエクスプローラ**]の順にクリックし、右上のフィルターで表示したいグラフに変更します。



フィルタによって、以下のパラメータに切り替えることができます。

パラメータ	概要
モデル	デバイスのモデル名を表します。
スイッチ名	スイッチ名を表します。
電源	電源を表します。（PoE/PoE+/PoE++）
グループ	グループを表します。
Wi-Fi 規格	Wi-Fi 規格を表します。
ビルド	ビルド環境を表します。
更新	デバイスのファームウェア状態を表します。
リンク速度	リンク速度を表します。
スイッチメーカ	スイッチのメーカを表します。
平均 CPU 使用率（%）	平均の CPU 使用率を表します。
平均メモリ使用率（%）	平均のメモリ使用率を表します。
タグ	タグ情報を表します。
フェイルセーフモード	フェイルセーフモードの有効/無効状態を表します。

チャネルマップ

各チャンネルに接続されているアクセスポイントとクライアント数を表示します。

[**チャンネルマップ**]を表示するには以下の手順を実行します。

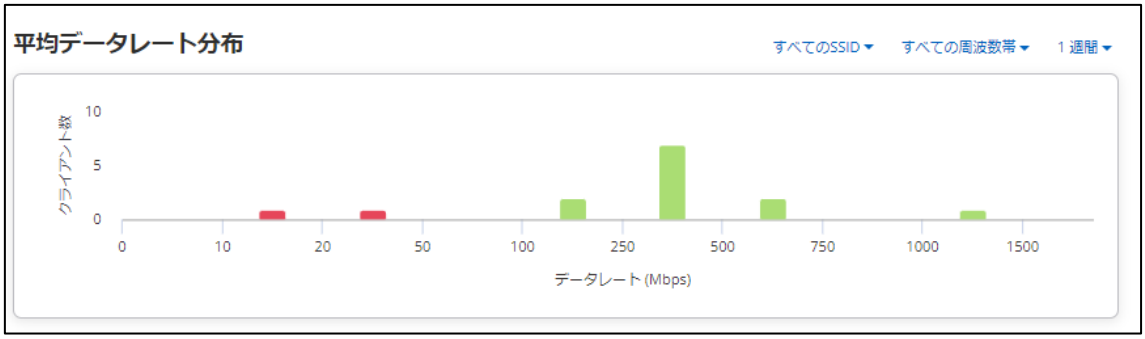
1. [**モニター**]>[WiFi]>[**アクセスポイント**]の順にクリックします。
2. チャンネル・マップを表示したいアクセスポイントをクリックします。
3. [**スペクトル点有率**]の[**チャンネル・マップ**]をクリックします。

以下のように[**チャンネル・マップ**]では、フィルタにより各情報が表示されます。

パラメータ	概要
ISM	チャネル 1～13、周波数 2.4GHz～2.5GHz のバンドです。
UNII - 1	チャネル 36～48、周波数 5.180GHz～5.240GHz のバンドです。
UNII - 2	チャネル 52～60、周波数 5.260GHz～5.320GHz のバンドです。
UNII - 3	チャネル 100～140、周波数 5.500GHz～5.700GHz のバンドです。
UNII - 4	チャネル 140～165、周波数 5.745GHz～5.825GHz のバンドです。
UNII - 5	チャネル 1～93、周波数 5.925GHz～6.425GHz のバンドです。
UNII - 6	チャネル 97～113、周波数 6.425GHz～6.525GHz のバンドです。
UNII - 7	チャネル 117～185、周波数 6.525GHz～6.875GHz のバンドです。
UNII - 8	チャネル 189～233、周波数 6.875GHz～7.125GHz のバンドです。
時間	過去のクライアントおよびアクセスポイント数のログを表示することが出来ます。

平均データレート分布

データレートに基づいて分類された各クライアントが表示されます。AIRRECT Cloudには、平均データレートに関するしきい値が定義されており、しきい値は任意で設定可能です。例えば、ユーザーがデータレートのしきい値を75Mbpsに設定し、RSSIしきい値を-68dBmに設定すると、これらの値はそれぞれ「50～100Mbps」のデータレートバケットと「-65～-75dBm」のRSSIバケットに分類されます。



以下のロジックを使うと、これらのバケットに含まれるバーの色について決定できます。

・「50～100Mbps」バケットにある値のすべてが75Mbps未満の場合、「50～100Mbps」バケットのバーは赤色になります。
・「50～100Mbps」バケットにある値のすべてが75Mbpsを超える場合、「50～100Mbps」バケットのバーは緑色になります。
・「50～100Mbps」バケットにある値の一部が75Mbpsの上下にある場合、「50～100Mbps」バケットのバーは黄色になります。

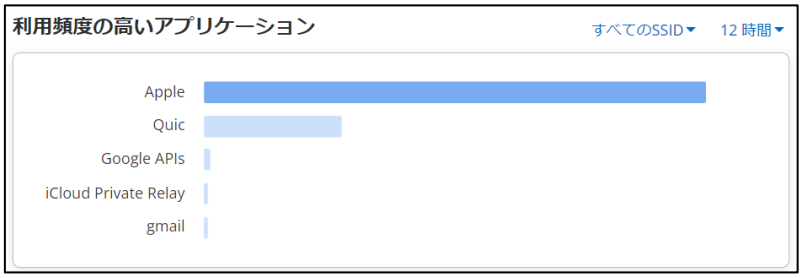
現在アソシエーションされているクライアント

[現在アソシエーションされているクライアント]ウィジェットには、現時点でアクセスポイントにアソシエーションされているクライアント・リストが表示されます。

グラフには、以下の情報が表示されます。

パラメータ	概要
名前	アクセスポイントが接続されているデバイス名を表します。
ユーザー名	ユーザー名を表します。
MACアドレス	アクセスポイントのMACアドレスを表します。
IPアドレス	アクセスポイントのIPv4アドレスを表します。
IPv6 アドレス	アクセスポイントのIPv6アドレスを表します。
OS	クライアントが動作しているOSを表します。
関連づけられたSSID	クライアントがアソシエーションされているSSID名を表します。
周波数帯	クライアントが接続されている周波数帯を表示します。
RSSI (dBm)	受信電波強度を表します。
Tx データレート	クライアントの「送信時のデータレート」を表します。
Rx データレート	クライアントの「受信時のデータレート」を表します。
平均データレート	クライアントの平均データレートを表します。
再試行率 (%)	クライアントの再送信率を表します。
接続・切断された日時	クライアントが接続、または切断された日時を表します
スティッキー	クライアントがスティッキークライアントかどうかを表します。クライアントがアクセスポイントに接続中、且つ、ローミング中に、より良い信号強度を含むアクセスポイントが見つかっているにも関わらず、弱い電波のアクセスポイントとの接続を維持してしまっているアクセスポイントが表示されます。

利用頻度の高いアプリケーショントラフィックチャート別の上位アプリケーションには、アプリケーションに関するデータ使用量が表示されます。その画面には、データ使用量が最も多い5つのアプリケーション（送受信）に関するデータが表示されます。正確にデータ使用量を表示するには、グラフ内の特定のバーにカーソルを合わせます。



ネットワーク使用率　トラフィック

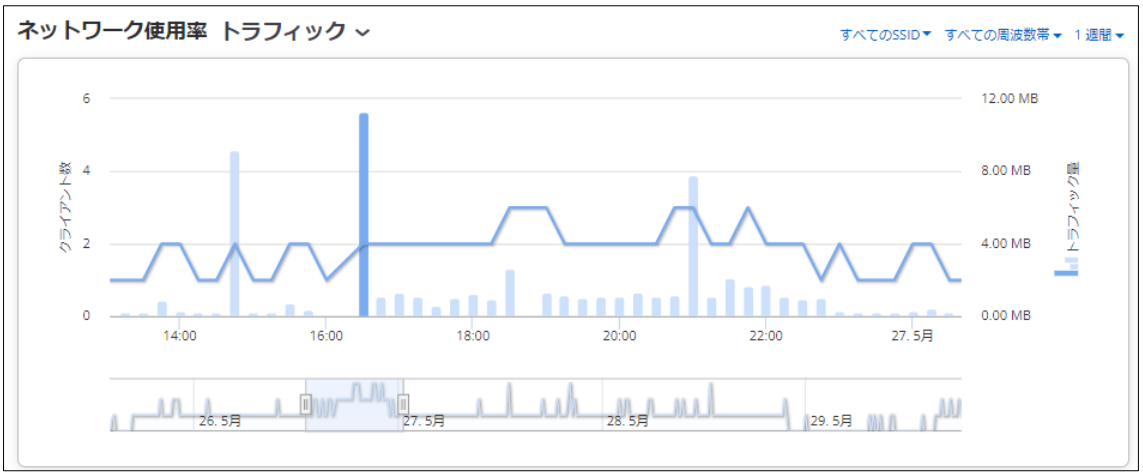
[ネットワーク使用率]グラフには2つのアクセス方法があります**。**

1. ダッシュボードのパフォーマンスタブからグラフにアクセス。

選択したフォルダやフロアにあるすべてのクライアントに関する情報 (SSIDにアソシエーションされたクライアントの数とそのトラフィック量を示す折れ線グラフ) が表示されます。

2. アクセスポイントドリルダウン経由でグラフにアクセス。

同様のデータが表示されますが、この場合はクリックしたアクセスポイントに関する内容になります。グラフにカーソルを合わせると、タイムスタンプ、クライアントの数、使用されたトラフィック量などの簡易情報が表示されます。



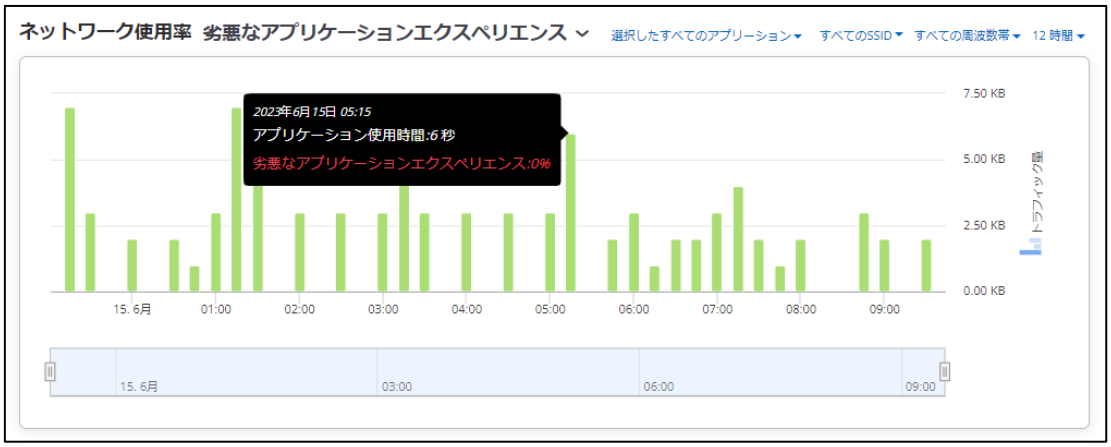
また、フィルタを使うと特定のデータの表示が可能です。

ネットワーク使用率のデータは、クライアントのデータとアプリケーションが使うデータ量の2つのパラメータに基づいてグラフ化されます。グラフのデータポイントをドリルダウンすると、クライアント接続テーブルが含まれるページにリダイレクトします。

パラメータ	概要
クライアント接続テーブル	すべてのクライアント接続のリストや、選択したタイムスタンプの詳細が表示されます。
上位のアプリケーション	データ使用量が最も多い10個のアプリケーションが表示されます。テーブルの左上にあるドロップダウンリストからアプリを選択できます。選択したアプリケーション名と、アプリケーション固有のデータ利用量が表示されます。
すべてのアプリケーショントラフィック	アプリケーションが使用するデータの総量が表示されます。選択したアクセスポイントまたはロケーションを示し、この情報はテーブルの右上に表示されます。
クライアント接続	[**クライアント接続**]をドリルダウンから選択すると、[**上部のアプリケーションリスト**]から選択したアプリケーションを使用しているすべてのクライアントがリスト表示されます。
アクセスポイントの分散	[**アクセスポイントの分散**]をドリルダウンから選択すると、アソシエーションされているすべてのアクセスポイントリストが表示されます。

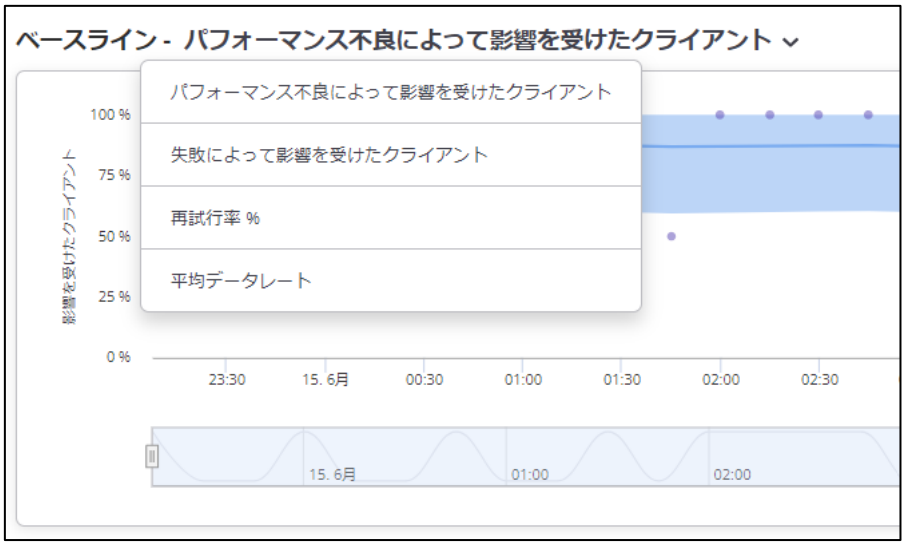
ネットワーク使用率 - 劣悪なアプリケーションエクスペリエンス

アプリケーション使用量に関する分析とその概要、アプリケーションの品質が良好な時間と劣悪な時間を表示します。劣悪な品質のアプリケーションエクスペリエンスについては赤色で表示され、良好な品質のアプリケーションエクスペリエンスについては緑色で表示されます。X軸はタイムスロットを表し、Y軸はアプリケーションに関する品質の良し悪しを表します。また、グラフにカーソルを合わせると、タイムスタンプ/アプリケーション使用時間/劣悪なアプリケーションエクスペリエンスのツールチップが表示されます。



ベースライン

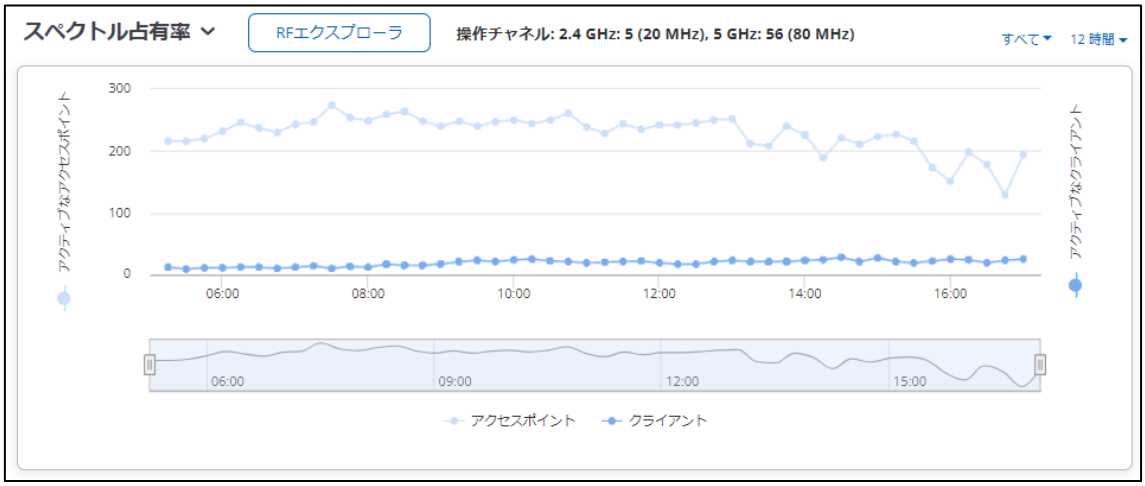
アクセスポイントごとのベースラインを表示します。ベースラインは、以下の4種類で表示されます。



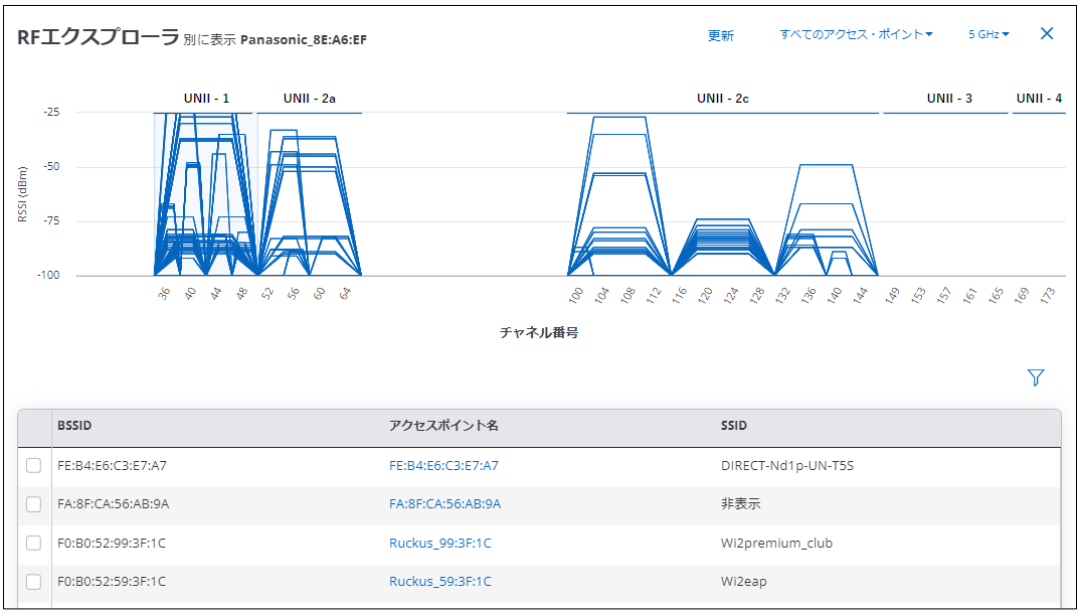
ベースラインの詳細については、『2.3ベースラインとしきい値』をご参照ください。

スペクトル占有率

下図に示すように、帯域と期間をフィルタリングし、特定の期間や帯域でアクティブだった無線通信とクライアント数を確認ができます。これは、混雑した帯域や十分に活用されていない帯域の特定に役立ちます。また、上部のRFエクスプローラを押すと、該当のアクセスポイントが検知している周囲の電波状態を確認することができます。



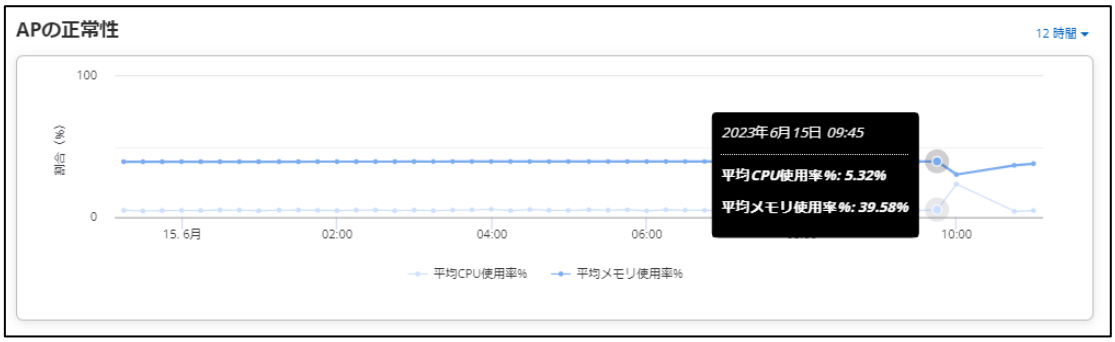
RFエクスプローラは、アクセスポイントがRFで認識している情報（対象のアクセスポイントの近くにある他のアクセスポイントが占有しているチャネルや、近隣の各アクセスポイントのRSSI値）を表示することができます。



RFエクスプローラを使用することで、チャネルの干渉や、アクセスポイントが占有しているDFSチャネルなどの問題を特定することができます。RSSI軸を横切る灰色の長方形は、選択したアクセスポイント自体の動作チャネルを表しています。チャネルの台形の高さは、選択したアクセスポイントから見たチャネルのRSSI値を示します。リストから特定のアクセスポイントをクリックすると、該当アクセスポイントの[**現在アソシエーションされているクライアント**]と[**このAPを認識している無線**]が表示されます。チャートにカーソルを合わせると、チャネルの詳細が表示されます。

APの正常性

次の図に示すように、グラフには、選択した期間におけるAPの平均CPUおよびメモリ使用率が表示されます。



メッシュ・ネットワーク・リンク

アクセスポイントが属するメッシュネットワークの状況が表示されます。

メッシュ・ネットワーク・リンク

アクセスポイント	メッシュ・リンク・タイ...	RSSI (dBm)	セキュリティ
Panasonic_8E:A6:BF	ダウンリンク	-28	WPA3
Panasonic_8E:A6:EF	ダウンリンク	-21	WPA3

可視BSSID

管理対象アクセスポイントと非管理対象アクセスポイントが表示されます。ドロップダウンリストにより、表示させる対象をフィルタ選択できます。

●[可視BSSID -管理対象]は、選択中のアクセスポイント付近に存在している管理されているアクセスポイントを確認できます。

可視BSSID - 管理対象

BSSID	AP名	関連付けられたSSID	RSSI (dBm)	チャネル	クライアン...	チャネル幅
BC:69:CB:80:02:A1	Panasonic_80:02:CF	RADIUS	-31	48	--	80 MHz
BC:69:CB:80:02:A2	Panasonic_80:02:CF	Sky5-ID8	-31	48	--	80 MHz
BC:69:CB:80:02:A3	Panasonic_80:02:CF	Sky5_UPSK	-31	48	--	80 MHz
BC:69:CB:80:02:A5	Panasonic_80:02:CF	RADIUS-FQDN	-31	48	--	80 MHz

●[可視BSSID -管理対象外]は、選択中のアクセスポイント付近に存在しているが管理されていないアクセスポイントを確認できます。

可視BSSID - 管理対象外

BSSID	AP名	関連付けられたSSID	RSSI (dBm)	チャネル	クライアン...	チャネル幅
FA:8F:CA:66:48:C4	FA:8F:CA:66:48:C4	非表示	-87	4	--	20 MHz
F8:B7:97:C8:F5:8F	NECPlatf_C8:F5:8F	非表示	-88	100	--	80 MHz
EA:CB:BC:B7:54:B2	EA:CB:BC:B7:54:B2	非表示	-48	11	--	20 MHz
EA:CB:BC:8C:F2:1C	EA:CB:BC:8C:F2:1C	非表示	-92	11	--	20 MHz
EA:CB:AC:B7:54:B2	EA:CB:AC:B7:54:B2	非表示	-48	44	--	80 MHz

●[可視クライアント]は、アクセスポイントが認識しているクライアントが表示されます。

可視クライアント

名前	MACアドレス	RSSI (dBm)
IntelCor_C6:DF:63	F8:59:71:C6:DF:63	-58
Apple_0F:9B:70	F4:34:F0:0F:9B:70	-96
Apple_01:28:A5	F4:34:F0:01:28:A5	-96
IntelCor_D9:69:76	F0:57:A6:D9:69:76	-50
DE:CB:BC:B7:54:B2	DE:CB:BC:B7:54:B2	-96
DE:CB:AC:B7:54:B2	DE:CB:AC:B7:54:B2	-96

●[**可視 VLAN**]は、アクセスポイントが認識している VLAN の詳細情報が表示されます。「ステータス」列の[**モニタリング対象**]は、VLANが管理対象アクセスポイントによって監視されていることを表します。[**モニタリング対象外**]は、別の管理対象アクセスポイントによって監視されていることを意味します。

可視VLAN

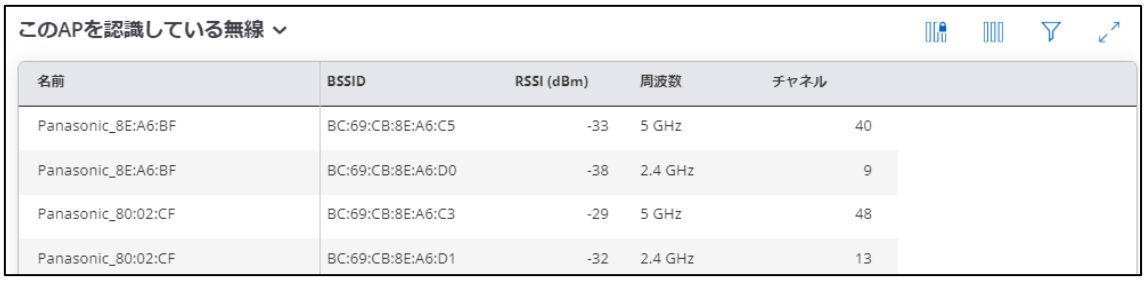
VLAN ID	IPアドレス	サブネットマスク	ステータス
10	10.0.10.6	255.255.255.0	モニタリング対象
30	10.0.30.3	255.255.255.0	モニタリング対象外
タグが解除されました*	10.0.1.11	255.255.255.0	モニタリング対象

選択されたアクセスポイントで認識されるVLANは、以下に応じて設定されます。

- AIRRECT Cloudと通信する目的で、VLANがデバイスによって使用されている場合（通信 VLAN）。この時、アスタリスクマークが表示されます。
- [**構成**]>[**SSIDの設定**]でVLAN IDが追加された場合
- [**構成**]>[**デバイス**] >[**アクセスポイント**]の[**セキュリティ**]タブを選択し、[**VLANモニタリング**]の中の[**VLAN自動モニタリング**]を有効にすると、アクセスポイントが自動的にVLANを発見し、そのVLANを監視します。
  VLANの監視は、最大のMACアドレスを持つデバイスによって行われます
- [**監視するVLANの追加**]を有効にする場合は、監視対象のVLANをコンマ区切りのリストで指定すると、指定されたリストのアクティブなVLANが監視されます。

デバイス
アクセスポイント
全般的
セキュリティ
WiFi無線
LANポート
VLANモニタリング
推奨設定
SSID VLANモニタリング
VLAN自動モニタリング
監視するVLANを追加
10,20
[0～4094]

●[**このAPを認識している無線**]は、管理対象アクセスポイントを認識している周囲のアクセスポイントのリストが表示されます。



名前	BSSID	RSSI (dBm)	周波数	チャネル
Panasonic_8E:A6:BF	BC:69:CB:8E:A6:C5	-33	5 GHz	40
Panasonic_8E:A6:BF	BC:69:CB:8E:A6:D0	-38	2.4 GHz	9
Panasonic_80:02:CF	BC:69:CB:8E:A6:C3	-29	5 GHz	48
Panasonic_80:02:CF	BC:69:CB:8E:A6:D1	-32	2.4 GHz	13

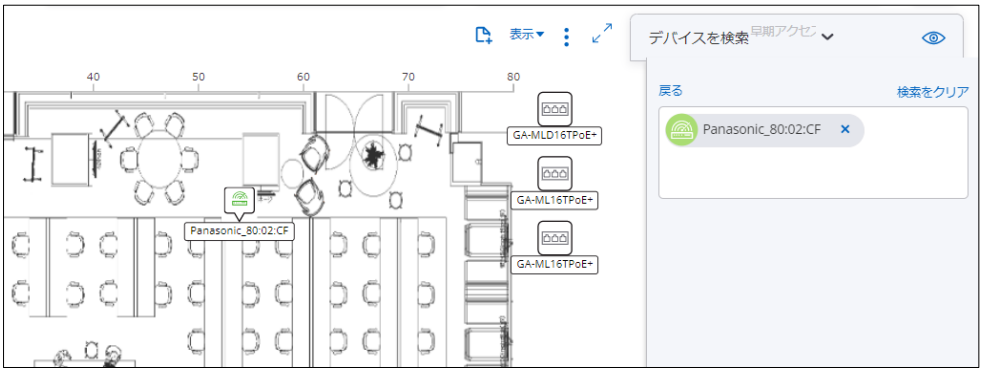
フロアマップでアクセスポイントの場所を確認する

[**検索**]オプションにより、アクセスポイントが置かれている フロアマップのロケーションへ、リダイレクトします。

フロアマップでアクセスポイントを表示するには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックします。
2. [**アクセスポイント**]を右クリックして、[**検索**]をクリックします。

選択したアクセスポイントがフロアマップに置かれている場合のみ、本機能を利用できます。



2.5.3 モニターからアクセスポイントの設定を変更する

送信電力またはチャネルをカスタマイズする。

[**構成**]>[**デバイス**]>[**アクセスポイント**]>[WiFi**無線**]での設定（詳細は『無線設定で送信電力選択パラメータを設定する』または『2.4GHz/5GHz/6GHzの無線通信設定の構成』）とは、異なり、[**送信電力またはチャンネルをカスタマイズ**]では、アクセスポイント固有の送信電力、チャネル設定ができます。以下の手順で固有設定を行います。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックします。
2. 設定をカスタマイズする [**アクセスポイント**]を右クリックします
3. [**カスタマイズ**]>[**送信電力またはチャンネル**]をクリックすると、画面の右側に[**送信電力またはチャネルのカスタマイズ**]ウィンドウが表示されます。

4. 設定をカスタマイズする周波数を選択します。
5. 送信電力設定の [**送信出力をカスタマイズ**]をクリックします。
   その後、[**自動**]または[**手動**]オプションをクリックします。[**手動**]オプションをクリックすると、[**送信出力**]テキストボックスではアクセスポイントの送信電力をdBmで供給できます。
6. チャネル設定の[**チャネル設定をカスタマイズ**]をクリックします。
   [**自動**]または[**手動**]として[**操作チャネル**]をクリックします。[**手動**]オプションをクリックすると、[**チャネル番号**]テキストボックスにチャネル番号を入力できます。
7. [**保存**]をクリックすると、カスタマイズ設定が保存されます。

アクセスポイントごとの監視するVLAN/IPアドレスのカスタマイズ

監視する個々のアクセスポイントのカスタムVLANを設定できます。

また、アクセスポイントに割り当てられたIPアドレスを変更することができます。

設定は、以下の手順を実行します。

1. [**モニター**]>[WIPS]>[**管理対象Wi-Fiデバイス**]または[**モニター**]>[Wi-Fi]>[**アクセスポイント**]に移動するか、[**フロアプラン**]に移動してフロアプランでアクセスポイントを選択します。
2. 変更対象となるアクセスポイントを右クリックして、[**カスタマイズ**]>[VLAN]を選択します。

3. 右側のパネル（アクセスポイントのVLANのカスタマイズ）の[**カスタマイズ**]にチェックを入れます。
4. アクセスポイントが監視するVLANを追加します。[検出されたVLAN]は、アクセスポイントがネットワーク上で検出したVLANです。監視するVLANを選択するのに役立つ場合があります。すでに設定してあるVLANのIPアドレスを変更したい場合は、[監視対象VLAN]に表示されたVLAN ID一覧の中からIPアドレスを変更したいVLAN IDをクリックし、IPアドレスの設定方法を [静的]、[DHCP]のいずれから選び選択します。
5. [**静的**]を選択した場合には、必要事項（IPアドレス、サブネットマスク、ゲートウェイ）を入力します。

6. [**監視対象VLAN**]で作成したVLANの中から、通信に用いるVLANを[**通信VLAN**]で選択します。
   アクセスポイントは、通信VLANを介してWi-Fiサーバーと通信するため、通信VLANは、アクセスポイントが監視するVLANの1つである必要があります。
7. パネル下部の[**終了**]ボタンをクリックして、設定を反映します。

アクセスポイントを移動する

AIRRECT Cloudは、[**移動**]オプションを使い、アクセスポイントのロケーションを変更する機能を提供します。

アクセスポイントを移動するには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックすると、監視中のアクセスポイントリストが表示されます。
2. 移動するアクセスポイントの名前を右クリックして、[**移動**]をクリックすると、[**ロケーション ナビゲータ**]が表示されます。
3. 次に移動先のロケーションをクリックして、アクセスポイントを移動させます。
4. [**移動**]をクリックすると、[**確認**]ウィンドウが表示されます。
5. 適切なオプションをクリックすると次の画面を確認できます。その後、[**はい**]をクリックすると、選択したアクセスポイントは、宛先フォルダで適用された構成を採用します。また、アクセスポイントがいずれかのフロアマップに現在置かれている場合、アクセスポイントがそのマップから削除されます。その後、ロケーションが変更されたことが、メッセージで通知されます。

アクセスポイントの移動に関連する動作

グループは、ロケーションごとに作成することが可能です。アクセスポイントを複数のロケーション間で移動すると、設定状況によってアクセスポイントに適用される構成が変わる場合があります。例えば、ロケーション[東京]フォルダとロケーション[大阪]フォルダがあった場合、東京フォルダで作成したグループは、大阪フォルダには存在しません。そのため、東京フォルダのグループに属したアクセスポイントを大阪フォルダに移動したとき、グループ設定は解除され、大阪フォルダのデフォルト設定が適用されます。

アクセスポイントを再起動する。

アクセスポイントを再起動するには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックすると、監視中のアクセスポイントリストが表示されます。
2. 再起動するアクセスポイントの名前を右クリックして、[**再起動**]をクリックすると、[**再起動**]ダイアログボックスが表示されます。
3. [**再起動**]をクリックしてアクセスポイントを再起動します。しばらくすると、ステータスについて確認することができます。

アクセスポイントの名前を変更する。

アクセスポイントの名前を変更する際は、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックすると、監視中のアクセスポイントリストが表示されます。
2. 名前を変更したいアクセスポイントの名前を右クリックし、[**名前を変更**]を選択すると、[**アクセスポイントの名前を変更**]ページが表示されます。

注意：名前に半角スペースを含めると、パケットキャプチャやデバッグログ機能、モニター機能表示が正常に動作しないことがあります。

3. アクセスポイントの名前を変更した後は、[**終了**]をクリックすると変更が保存されます。

アクセスポイントを削除する。

アクセスポイントタブのアクセスポイントリストから、アクセスポイントを削除できます。

アクセスポイントを削除するには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックすると、監視中のアクセスポイントリストが表示されます。
2. 削除したいアクセスポイントを右クリックして、[**削除**]を選択すると、[**削除**]ダイアログボックスが表示されます。
3. [**削除**]をクリックします。

注意：アクセスポイントが削除された後に再度アクセスポイントをAIRRECT Cloudに接続すると、アクセスポイントはStaging Areaに移動し、Staging Areaのデバイステンプレートが適用されます。

進行中のアクティビティをアクセスポイントで表示する

[**進行中のアクティビティを表示**]は、[**アクセスポイント**]画面において使用できるアクションです。アクセスポイントにおいて進行中のアクティビティを表示するには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックします。
2. 画面の右上にある[**進行中のアクティビティを表示**]をクリックします。
3. ドロップダウン・メニューから、以下のいずれかを選択します。

●スペクトラム分析：スペクトラム分析中のアクセスポイントがリスト表示されます。

●パケットトレース：パケットトレースが進行中のアクセスポイントとその情報のリストが表示されます。

●防御：隔離された状態のアクセスポイントがリスト表示されます。

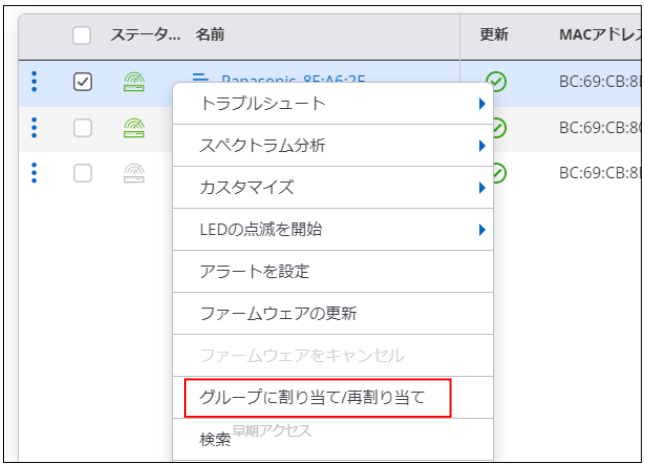
●クライアント接続テスト：クライアント接続テストが進行中のアクセスポイントとその情報がリスト表示されます。

●LED点滅中：LED点滅中のアクセスポイントがリスト表示されます。
●なし：アクティビティが行われていないアクセスポイントがリスト表示されます。

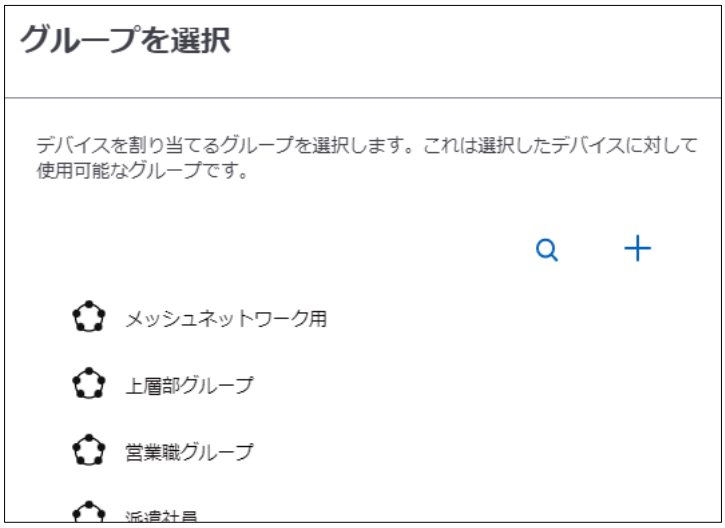
アクセスポイントタブからグループにデバイスを割り当てる

アクセスポイントをグループに割り当てるには、[**アクセスポイント**]ページにある[**アクセスポイント**]リストから実行します。既存のグループにデバイスを割り当てるには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックします。
2. グループに割り当てるアクセスポイントの名前を右クリックし、[**グループに割り当て/再割り当て**]を選択すると[**グループの選択**]ウィンドウが右のパネルに表示されます。



3. アクセスポイントを割り当てるグループをクリックします。
   グループがリスト内で見つからない場合は、以下のパネルから、新たにグループを追加できます。新たに追加されたグループは、選択したロケーションのフォルダの一番上に作成されます。ユーザーがそのフォルダにアクセスできない場合は、グループ・オプションの追加が無効になります。複数のアクセスポイントを割り当てる場合は、選択したアクセスポイント・フォルダで使用できるグループのみが[**グループの選択**]パネル配下にリストされます。



4. [**割り当て**]をクリックします。

デバイスをグループに割り当てる。

ロケーション・サブツリーから、複数のアクセスポイントをグループに割り当てることができます。これは、さまざまなロケーションにある複数のデバイスに対して、単一のWi-Fi設定を適用するために利用する方法です。

グループに設定がない場合、割り当てられたデバイスは、それぞれのロケーションのデフォルトWi-Fi設定を利用します。一方で、アクセスポイントには既にカスタムWi-Fi設定が適用されていると想定し、アクセスポイントをグループに割り当てるとグループのWi-Fi設定は以下の2種類のタブから使用できます。

●アクセスポイント

●フォルダ/フロアのページ

フォルダ/フロアのページから、デバイスをグループに割り当てる

[**アクセスポイント**]ページから、デバイスをグループに割り当てる以外に、[**フォルダ/フロア**]ページからも、実行可能です。

デバイスを既存のグループに割り当てるには、以下の手順を実行します。

1. [**システム**]>[**ナビゲーター**]>[**フォルダー/フロア**]の順にクリックします。
2. グループに割り当てたい単一のアクセスポイントの名前を右クリックするか、メニュー・アイコン⋮をクリックし、リストの[**利用可能デバイスの表示**]オプションを選択すると、アクセスポイントリストが、右側のパネルに表示されます。
3. グループに割り当てたい単一のアクセスポイント名を右クリックするか、メニュー・アイコン⋮をクリックし、[**グループに割り当て/再割り当て**]を選択します。その後、[**グループを選択**]ウィンドウが表示されます。
4. 選択したアクセスポイントに割り当てたいグループを選択します。もしグループがリス

トの中に存在しない場合は、このパネルから新しいグループを追加できます。最上位の親フォルダにアクセスできない場合は、グループを追加できません。新たに追加されたグループは、選択したロケーションの最上位の (許可された) 親フォルダに作成されます。

5. **[割り当て]**をクリックします。

デバイスを別のグループに再割り当てをする

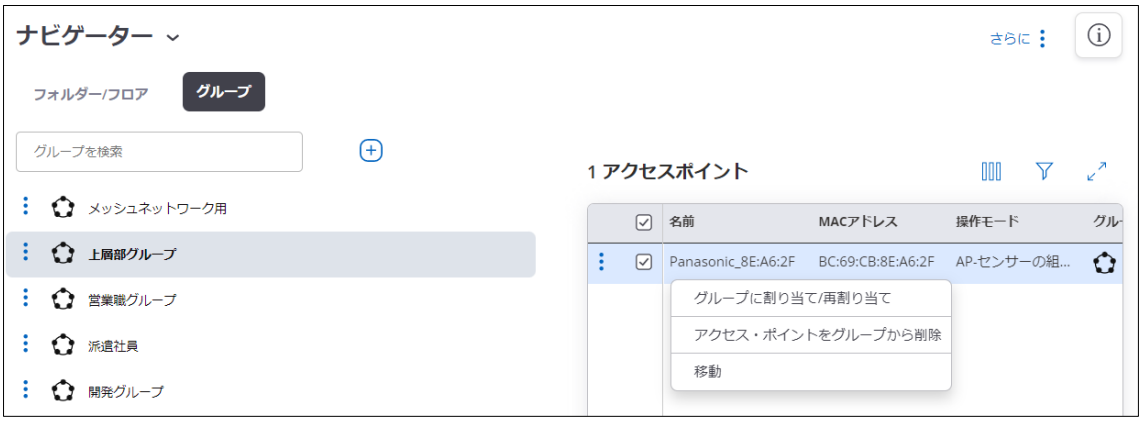
任意のグループから別のグループにアクセスポイントを移動できます。再割り当てがされると、選択したアクセスポイントは再割り当て後のグループのWi-Fi設定で動作します。
再割り当て後のグループにWi-Fi設定が適用されていない場合、アクセスポイントはそのロケーションのデフォルトWi-Fi設定を利用します。
選択したアクセスポイントがどのグループにも割り当てられていなかった場合でも、再割り当てを実行すると、選択したグループに割り当てられます。
アクセスポイントの再割り当ては、以下のタブから実行できます。

●アクセスポイント
●フォルダ/フロア
●グループ

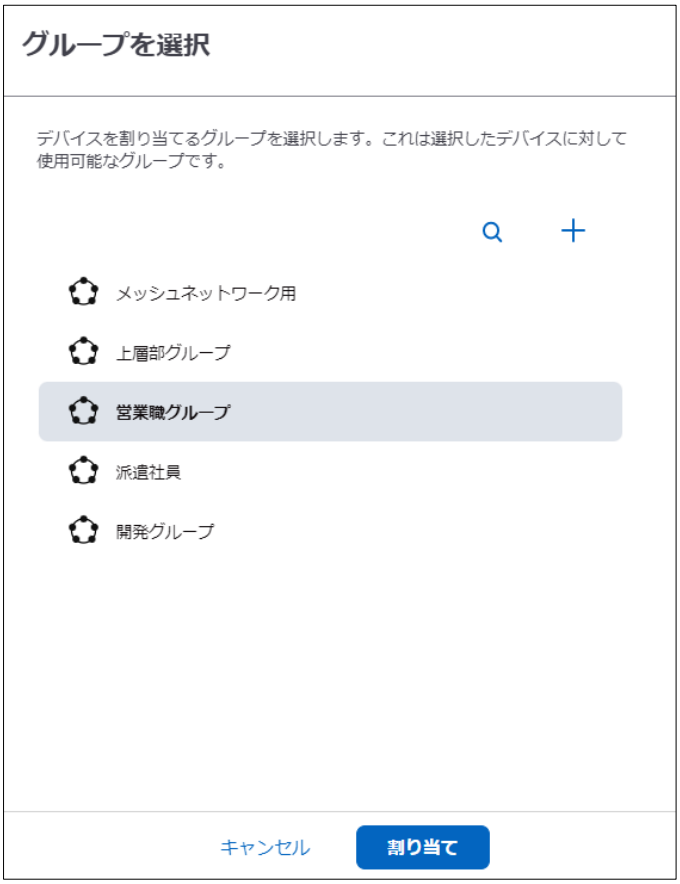
アクセスポイントおよびフォルダ/フロアタブからの設定は、デバイスをグループに割り当てる方法と同じです。グループタブからの設定は、アクセスポイントを再割り当てする場合に限り、適用されます。
任意のグループからの再割り当ては、以下の手順を実行します。

1. **[システム]>[ナビゲーター]**から、**[グループ]**タブをクリックし、移動します。
2. 選択したグループを右クリックして、**[割り当てられたデバイスの表示]**を選択します。
   選択したロケーションにおいて**[アクセスポイント]**リストが、右側のパネルに表示されます。

3. 再び割り当てたいアクセスポイントの名前を右クリックし、[**グループに割り当て/再割り当て**]を選択すると、画面の右側に [**グループを選択**]ウィンドウが表示されます。リストからグループを選択して、選択したグループに再びそのデバイスを割り当てます。



4. リストからグループを選択し、[**割り当て**]をクリックすることで、選択したグループに対象のアクセスポイントを再割り当てします。



2.5.4 アクセスポイントのファームウェアを更新する

AIRRECT APのファームウェアはAIRRECT Cloudから手動または自動設定が更新可能できます。初めてサーバーに接続するアクセスポイントや、既に設置しているアクセスポイント等に対する更新のルール付けや、スケジューリングができます。ファームウェアの更新は、以下の定義で動作します。

●ファームウェアの自動更新に関する設定はロケーションフォルダに置かれるすべてのAIRRECT APに適用されます。個々のアクセスポイントごとに、独立した自動ファームウェアアップデート設定をすることはできません。

●ファームウェアの更新設定は、フロアでの設定は行えません。親ロケーションフォルダのファームウェアの更新設定がフロアに引き継がれます。

●ロケーション内にあるAIRRECT APにスケジュールを設定できます。
設定されたスケジュールで最新のファームウェアバージョンに更新されます。

●ファームウェアの更新設定を作成または編集する際は、子ロケーションのフォルダにも同様のファームウェアの更新設定が適用されますが、子ロケーションのフォルダの更新設定と分けることも可能です。親ロケーションフォルダのスケジュールが既に定義されている場合に、子ロケーションフォルダ固有のファームウェア更新設定を定義すると、子ロケーションに設定されたスケジュールが適用されます。

●ファームウェアのアップデートは、デフォルトでは、AIRRECT APを初めてAIRRECT Cloudに接続したときのみ自動で最新のバージョンが適用されます。
その後のアップデートは、手動、またはスケジューリングの設定をする必要があります。

●ファームウェアをアップデートするためには、ポート80またはポート443がオープンになっている必要があります。

更新できるファームウェアがある場合、[**モニター**]>[**アクセスポイント**]画面で ⬆ マークが表示されます。

アクセスポイントのファームウェアを更新する

アクセスポイントのファームウェアを最新版または前回リリースされた任意のバージョンに更新ができます。更新が完了すると、アクセスポイントが自動的に再起動します。

アクセスポイントのファームウェアを更新するには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックすると、監視中のアクセスポイントのリストが表示されます。
2. [**オプション**]アイコン (縦に3つ並んだ点) をクリックするか、アクセスポイントの名前を右クリックして、[**ファームウェアの更新**]を選択します。
3. [**バージョン**]ドロップダウン・リストから、必要なファームウェアのバージョンを選択します。アクセスポイントのファームウェアを、任意のバージョンに更新することができます。
4. [**更新**]をクリックすると、「ファームウェアの更新が開始しました」とメッセージが表示されます。しばらくすると、ファームウェアの更新状況について確認できます。

複数のアクセスポイントのファームウェアを更新する

複数のアクセスポイントのファームウェアを、同時に更新することができます。

複数のアクセスポイントのファームウェアを更新するには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックすると、監視中のアクセスポイントのリストが表示されます。
2. 必要なアクセスポイントを選択し、オプション・アイコン（縦に3つ並んだ点）をクリックして、[**ファームウェアの更新**]をクリックします。その後、[**ファームウェアの更新**]ページに選択したアクセスポイントのモデル名、選択されたアクセスポイント数、変更するバージョンのリストが表示されます。

3. バージョン・ドロップダウン・リストから、アクセスポイントのモデルごとに必要なバージョン番号を選択します。
4. [**更新**]をクリックすると、ファームウェアを更新できます。また、「ファームウェアの更新が開始しました」というメッセージが表示されます。しばらくすると、ファームウェアの更新状況について確認できます。

アクセスポイントの自動更新設定

ロケーションにあるすべてのアクセスポイントのファームウェアを、クラウドに接続した際や、設定した時間で自動更新することができます。

ファームウェアのアップデート設定は、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックすると、監視中のアクセスポイントのリストが表示されます。
2. ↑ マークをクリックし、[**更新**]をクリックすると、ファームウェアのアップデート設定画面が表示されます。

ファームウェアのアップデート設定では、以下の設定が可能です。

パラメータ		概要
設定の更新をサブフォルダーに再帰的に適用		アップデート設定を、子ロケーションにも適用する場合は有効にします。
既存のアクセスポイント	ヒットレスアップデート	有効にすると、フロアに複数のアクセスポイントがある環境の場合、隣接するアクセスポイントが同時に再起動しないように、順番にアップデートを行いクライアントへの影響を最小限に抑えます。本機能を無効にした場合、アクセスポイントはランダムにアップデートされますので、カバレッジホールが考慮されません。
	アップデートのスケジュール	繰り返し、または一度限りのスケジュールにより、アップデートを自動で実施する日時を設定できます。アップデート間隔では、更新を完了させたい期間を選択することができます。例えば、開始時刻を午前2時とし、アップデート間隔を4時間にした場合は、全てのアクセスポイントのアップデートを午前6時までに完了するように更新を行います。

新規のアクセスポイント	サーバーに接続しているときは自動的にアップデート	有効にすると、初めてAIRRECT APをAIRRECT Cloudに接続したときに限り、自動で最新のファームウェアに更新されます。アクセスポイントに適用するバージョンは、選択することも可能です。

3. [**終了**]を押下すると、設定が反映されます。

ファームウェア更新をキャンセルする

ファームウェアの更新はキャンセルが可能です。ただし、アクセスポイントの更新が開始してしばらくすると、非アクティブな状態になりますが、このステータスでは更新のキャンセルはできません。

ファームウェアの更新をキャンセルするには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックすると、監視中のアクセスポイントのリストが表示されます。
2. ファームウェアの更新をキャンセルするアクセスポイントを右クリックし、[**更新のキャンセル**]を選択します。その後、ファームウェアの更新がキャンセルされた旨のメッセージで通知されます。
3. [**はい**]をクリックして、更新をキャンセルします。

ファームウェアコンプライアンスの設定

アクセスポイントのモデルごとに準拠ファームウェア（対応バージョン）を設定できます。準拠ファームウェアの設定は、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順にクリックすると、アクセスポイントのリストが表示されます。
2. ↑マークをクリックし、[**バージョンの準拠**]をクリックすると、ファームウェアバージョンの準拠に関する設定画面が表示されます。
3. [**対応バージョン**]にチェックを入れ、2 つのオプションのいずれかを選択します。
   ・すべてのモデルの最新バージョン：最新のファームウェアを準拠ファームウェアとします。
   ・カスタマイズ：選択したファームウェアを準拠ファームウェアとします。

2.5.5 動作中の無線リストを確認する

[**モニター**]>[**無線通信**]の順にクリックすると、2.4/5/6GHz帯で動作する無線のリストが表示されます。また、選択した無線にアソシエーションされたクライアントのリストが表示されます。

[**無線通信**]**タブ**には、以下の無線に関する情報が表示されます。

パラメータ	概要
ステータス	アクセスポイントの状態を表示します。緑色は動作中のアクセスポイントであり、赤色は、動作していないアクセスポイントを表します。
名前	アクセスポイント名を表します。
APのMACアドレス	アクセスポイント固有の48ビットのアドレスを表します。
IPアドレス	IPアドレスを表します。
チャネル	無線が割り当てられているチャネル番号が表示されます。
クライアント	無線に接続されているクライアントの数が表示されます。
Tx.電力(dBm)	無線アクセスポイントの送信電力を表します。
周波数帯	無線が動作している周波数を表します。
RF使用率（%）	無線空間のチャネル使用率を表します。
アップストリーム使用率	最新の4時間、または、最新の100個の端末のアップストリーム使用率を表します。
ダウンストリーム使用率	最新の4時間、または、最新の100個の端末のダウンストリーム使用率を表します。
最低クライアントRSSI (dBm)	最も低いクライアント信号強度が表示されます。
再試行率 (%)	再試行率をパーセントで表します。
ロケーション	無線アクセスポイントの所属場所が表示されます。

パラメータ	概要
モデル	アクセスポイントのモデル名が表示されます。
ノイズフロア (dBm)	測定システム内の、すべてのノイズ源と不要な信号の合計によって生成された信号の測定値を示しています。
チャネル幅	動作しているチャネル幅が表示されます。
無線MACアドレス	BSSIDのMACアドレスが表示されます。
プリアンブルパンクチャ	プリアンブルパンクチャリングされているかどうか表示されます。
センター周波数	帯域の中央となる周波数を表示します。
送信電力モード	送信電力がカスタマイズされているかどうか表示されます。
チャンネル選択モード	チャンネルがカスタマイズされているかどうか表示されます。

また、[**モニター**]>[WiFi]>[**アクティブなSSID**]の順にクリックすると、動作中のSSIDプロフィールのリストが表示されます。

[**アクティブなSSID**]ページには、以下の情報が表示されます。

パラメータ	概要
SSID	SSID名を表示します。
認証	クライアントとの接続に使用される認証方法を表します。
2.4GHzクライアント	2.4GHz周波数帯で接続されているクライアントの数を表します。
5GHzクライアント	5GHz周波数帯で接続されているクライアントの数を表します。
6GHzクライアント	6GHz周波数帯で接続されているクライアントの数を表します。
2.4GHz無線通信	2.4GHzの無線SSIDを出力している数を表します。
5GHz無線通信	5GHzの無線SSIDを出力している数を表します。
6GHz無線通信	6GHzの無線SSIDを出力している数を表します。
マルチリンククライアント	マルチリンクが有効なSSIDに接続しているクライアントの数を表します。
合計アクセスポイント数	SSIDを出力しているアクセスポイントの合計を表します。

マルチリンクアクセスポイント	マルチリンクが有効になっているアクセスポイントの数を表します。
合計クライアント数	SSIDに接続しているクライアントの合計を表します。
周波数帯	SSIDを出力している周波数帯を表します。
アップリンクデータ	アップリンクのデータ使用量を表します。
ダウンリンクデータ	ダウンリンクのデータ使用量を表します。

2.5.6 送信電力制御と自動チャネル選択の固定化

自動送信電力制御(TPC)モードや自動チャネル選択(ACS)モードで動作するアクセスポイントに対し、フリーズ操作を行うことで、送信電力またはチャネルをフリーズ実施時点の値に固定化させることができます。フリーズ操作は各アクセスポイントの周波数単位で実施が可能です。

注意：フリーズ時、フリーズ対象となるBSSIDは再起動します。

送信電力制御と自動チャネル選択をフリーズする際は、以下の手順を実行します。

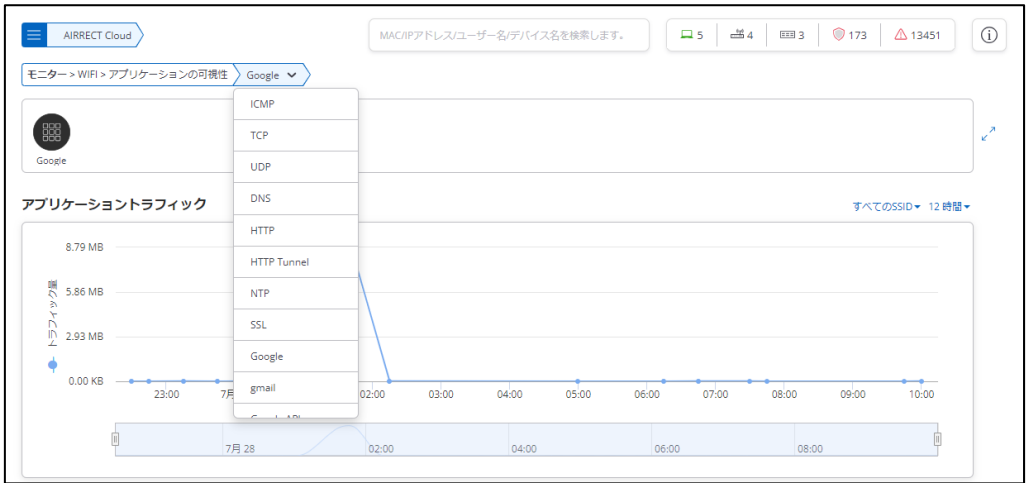
1. [**モニター**]>[WiFi] >[**無線通信**]の順に移動します。
2.アクセスポイントを選択して、三点メニュー（⋮）をクリックします。
3. [**ACPをフリーズ**]または[**TPCをフリーズ**]を選択します。

4.確認ダイアログにて、[**続行**]ボタンをクリックします。

●フリーズを解除する場合、同様の手順で[**フリーズを解除する**]を実行します。
●フリーズ状態の確認は、[**モニター**]>[WiFi] >[**無線通信**]の[**送信電力モード**]列と[**チャネル選択モード**]列を確認します。
●送信出力・チャネル設定のカスタマイズ画面からもフリーズが可能です。

2.5.7 アプリケーションの可視性

[モニター]>[アプリケーションの可視性]の順にクリックすると、アプリケーション監視情報の詳細が表示されます。リストの中から特定のアプリケーションを選択すると、使用している上位10個のクライアントリストや一定期間において選択されたアプリケーションの使用状況をプロットしている折れ線グラフが表示されます。また、ドロップダウンリストから別のアプリケーションを選択できます。



アプリケーション情報を含むページには、以下の情報が表示されます。

パラメータ	概要
アプリケーショントラフィック	一定期間、選択したアプリケーションデータの使用状況が表示されます。詳細については、『アプリケーショントラフィック』を参照してください。
アプリケーショントラフィックが最大のクライアント	ユーザー名、MACアドレス、IPアドレス、最近アソシエーションされたSSIDなどのクライアントの詳細情報と、選択したアプリケーションのデータ使用量が最も多い上位10のクライアントリストが表示されます。詳細については、『アプリケーショントラフィックが最大のクライアント』を参照してください。

アプリケーションを監視する

[アプリケーションの可視性]タブに表示されるアプリケーションリストから、アプリケーションを監視することができます。アプリケーションを監視するには、以下の手順を実行します。

1. **[モニター]>[アプリケーションの可視性]**の順にクリックすると、監視中のアプリケーションのリストが表示されます。

名前	カテゴリ	15 分	1 時間	4 時間	15 分(%)	1 時間(%)	4 時間(%)	脅威
ICMP	Network Monitoring	0 Bytes	168 Bytes	20.3 KB	0	0	0.03	
TCP	Networking	1.54 KB	15.49 KB	467.04 KB	0.36	0.38	0.61	
UDP	Networking	0 Bytes	886 Bytes	84.4 KB	0	0.02	0.11	
DNS	Networking	948 Bytes	6.43 KB	145.65 KB	0.21	0.16	0.19	
DHCP	Networking	0 Bytes	576 Bytes	2.82 KB	0	0.01	0	
HTTP	Web Services	0 Bytes	0 Bytes	3.99 MB	0	0	5.37	

一覧画面では、各アプリゲーションごとの利用量と一定期間での利用割合、脅威インデックスが表示されます。脅威インデックスとは、アプリケーションのリスクスコアに基づいて計算された値であり、脅威指数として、1～5で表示されます。

※AIRRECT CloudにはProcera DPI エンジンが組み込まれており、
　Procera DPI エンジンにて提供されている値となります。

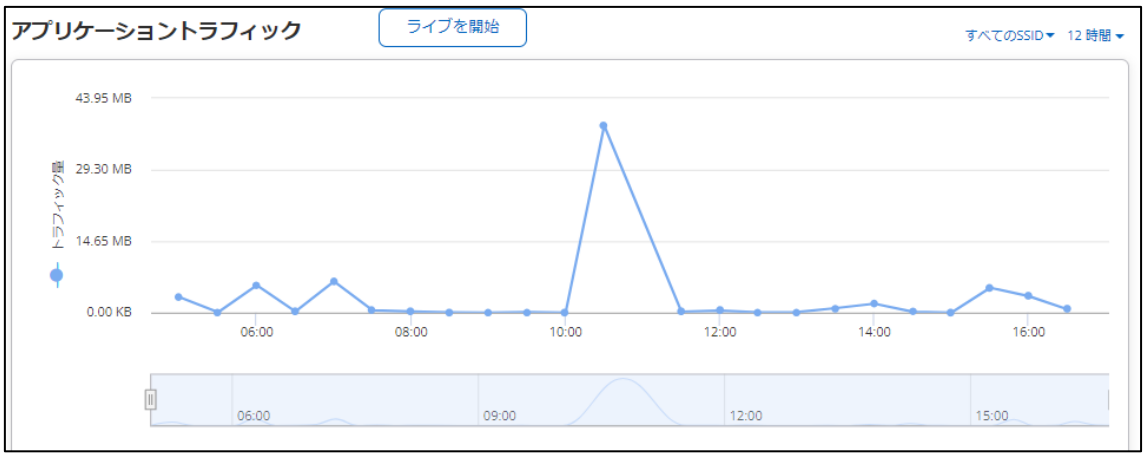
アプリケーションは、フィルタリングすることで、AIRRECT Cloudに登録されているすべてのアプリケーションの表示か、使用されたことのあるアプリケーションか表示を変更することが出来ます。また、SSIDごとの表示にフィルタリングすることも可能です。

2. 確認したいアプリケーションの名前をクリックすると、アプリケーションの詳細ページが表示されます。

アプリケーショントラフィック

[**アプリケーショントラフィック**]ウィジェットには、選択したアプリケーションのデータの一定期間の利用状況が表示されます。

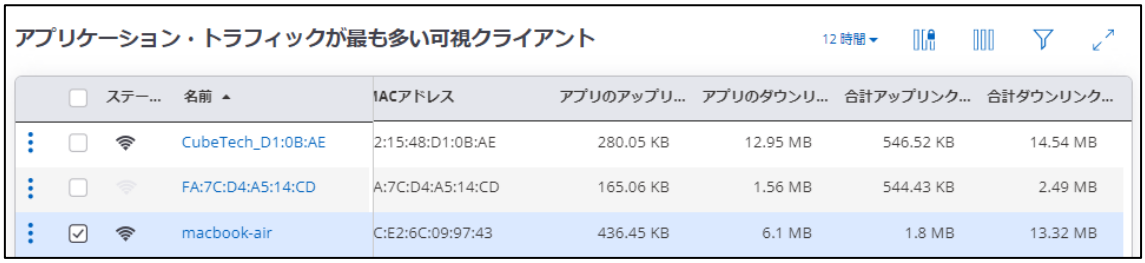
SSID、周波数、時間フィルタを使い、データをフィルタリングできます。これらのフィルタの詳細については、『ウィジェットのフィルタ』を参照してください。ライブデータの確認には、[**ライブを開始**]ボタンを使用します。



グラフは、15分間隔でプロットされます。ライブデータの場合は、3秒ごとにプロットされます。グラフの上にカーソルを合わせると、タイムスタンプとトラフィック量が表示できます。

アプリケーション・トラフィックが最も多い可視クライアント

[**アプリケーション・トラフィックが最も多い可視クライアント**]ウィジェットには、選択したアプリケーションの利用率が高いクライアントのリストと、クライアントの詳細が表示されます。また、ウィジェットの右上にあるツールを利用して、フィルタリングや、テーブルの表示を変更することができます。



2.5.8 トンネル

[モニター]>[WiFi]>[トンネル]画面にて、トンネル状況をモニタリングできます。

パラメータ	概要
トンネルステータス	トンネルの稼働状況を表します。 緑：アクティブ 赤：非アクティブ 橙：スタンバイ（セカンダリVXLANトンネル）
トンネルのタイプ	EoGRE、EoGRE over IPSec、VXLAN、IPSec、VxLAN over IPSecを使用するVPNなどの、ネットワークトンネルタイプを表します。
アクセスポイント名	アクセスポイント名を表します。
アクセスポイントのMACアドレス	アクセスポイントのMACアドレスを表します。
トンネルインターフェース	トンネルインターフェース名を表します。
リモートエンドポイント	プライマリーリモートサーバー、または、セカンダリ・リモートサーバーの種別を表します。
リモートエンドポイントのIP	リモートエンドポイントのIPアドレスを表します。
SSID	SSID名を表します。
接続・切断された日時	トンネルが接続、または切断された日時を表します
受信されたデータ	Rxトラフィック量を表示します。
送信されたデータ	Txトラフィック量を表示します。

2.5.9 WIPSで管理対象WiFiデバイスを確認する

[**モニター**]>[WIPS]>[**管理対象WiFiデバイス**]画面では、クラウドに帰属させている全てのAIRRECT APと、その詳細情報が表示されます。

パラメータ	概要
操作モード	アクセスポイントの動作モードを表します。
防止ステータス	アクセスポイントの防止状態を表します。
CIP対応	アクセスポイントがCIPに対応しているかどうかを表します。CIPについては『WLAN統合』を参照ください。
CIPモード有効	アクセスポイントのCIPモードが有効になっているか表します。
CIPトンネル・ステータス	アクセスポイントのCIPトンネルがクラウドとの間で確立されているを表します。

備考：当画面の上記以外の内容については、[**モニター**]>[WiFi]>[**アクセスポイント**]と共通になります。詳細については『管理しているアクセスポイントを確認する』を参照ください。

2.5.10 WIPSで管理しているアクセスポイントを確認する

[モニター]>[WIPS]>[アクセスポイント]画面では、WIPSアンテナにより検知されたアクセスポイントと、その詳細情報が表示されます。

パラメータ	概要
分類	アクセスポイントの分類を表します。分類についての詳細は、『認定Wi-Fiポリシー』を参照ください。
ステータス	アクセスポイントがアクティブか非アクティブかを表します。
名前	アクセスポイント名を表します。
MACアドレス	アクセスポイントのMACアドレスを表します。
自動防止ステータス	アクセスポイントが不正端末等を自動で防止している状態かを表します。
防止ステータス	アクセスポイントが不正端末等を自動または手動設定で防止しているかを表します。
ネットワーク状態	アクセスポイントの同一セグメント上に他のアクセスポイントが存在しているかを表します。

パラメータ	概要
ネットワーク	アクセスポイントの同一セグメント上に他のアクセスポイントが存在している場合、そのネットワークセグメントを表示します。
アクティブ/ 非アクティブ日時	アクセスポイントがアクティブまたは非アクティブになってからの日時を表します。
最初の検出	最初にアクセスポントが検出された日時を表します。
場所	アクセスポイントのロケーションを表します。
RSSI(dBm)	アクセスポントのRSSI(受信信号強度)を表します。
チャネル	アクセスポイントが接続しているチャネルを表します。
アソシエーション件数	アクセスポイントに接続されているクライアント数を表します。
SSID	クリックすると、割り当てられているSSID名が表示されます。
セキュリティ	ユーザーの認証方式を表します。
認証	アクセスポイントの認証方式を表します。
802.11w	アクセスポイントが802.11wを使用しているかどうかを表します。
暗号化	アクセスポイントの暗号化方式を表します。
メーカー名	アクセスポイントのメーカー名を表します。
Wi-Fi規格	アクセスポイントのWi-Fi規格を表します。
禁止状態	アクセスポイントの禁止状態の有無を表します。
タグ	アクセスポイントで設定されたタグを表します。
手動で分類	アクセスポイントが手動で分類されたかどうかを表します。
手動でタグ付けされました	クライアント端末を別のロケーションに移動した場合に「はい」と表示されます。

アクセスポイントの右クリックで以下のアクションを実行できます。

アクション	概要
分類を変更する	アクセスポイントの分類を「認定」「外部」「ローグ」のいずれかに変更します。
パケットトレースをキャプチャ	接続している端末間のパケットデータをキャプチャします。
パケットトレースの履歴	過去30分間にキャプチャされたパケットトレースが表示されます。
このデバイスを防止する	選択したアクセスポイントを不正端末と認識し、ネットワークやクライアントとの接続を遮断します。
自動防止を無効化する	自動遮断機能で不正アクセスポイントとして判断されても、自動防止されないようにします。

禁止リストに追加する	アクセスポイントを禁止デバイスリストに追加します。禁止デバイスリストについての詳細は『禁止デバイスリスト』を参照ください。
名前を変更	アクセスポイント名を変更します。
タグを変更する	アクセスポイントのタグを変更します。
移動	アクセスポイントのロケーションを変更できます。
削除	リストから該当のアクセスポイントを削除します。
検索	アクセスポイントの位置がフロアマップ上に表示されます。

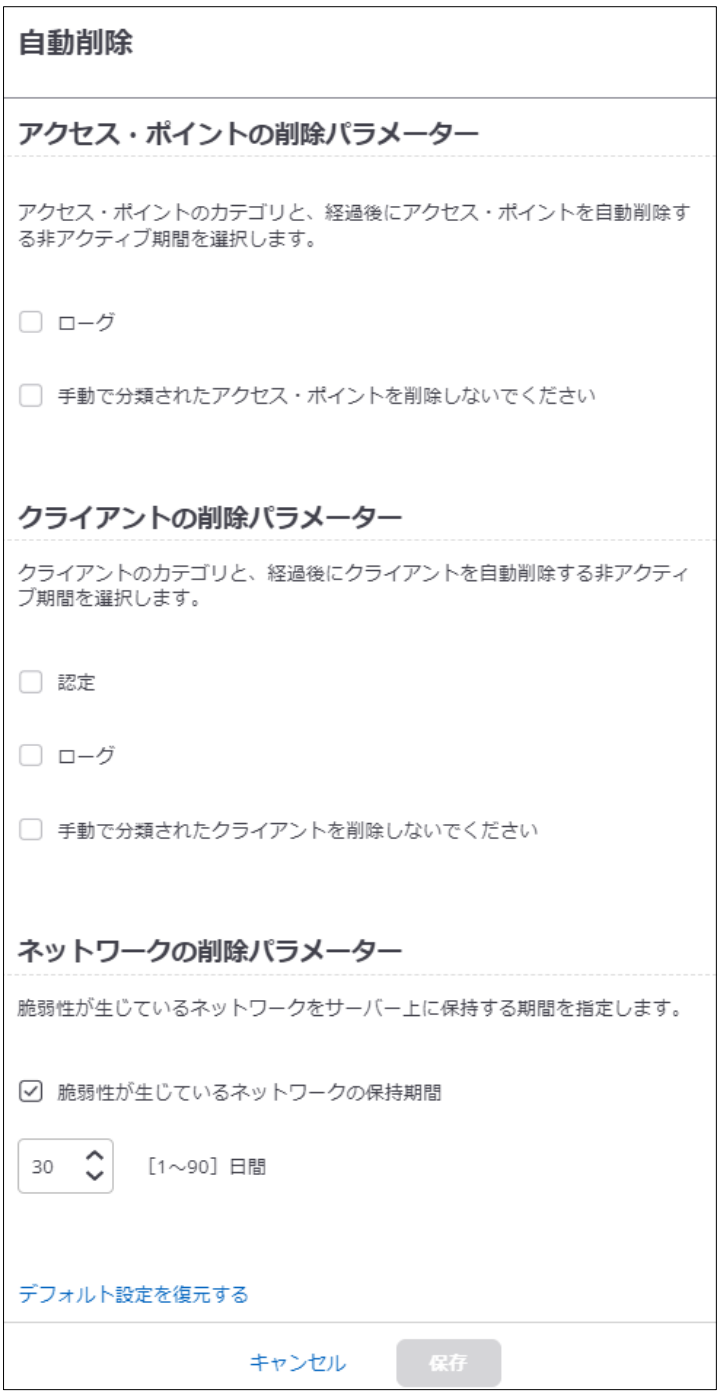
非アクティブな認定アクセスポイントの削除

非アクティブの認定アクセスポイントを、現在のロケーションから削除できます。画面左下に表示されている[**非アクティブな認定アクセス・ポイントを削除**]をクリックすします。

以下のウィンドウが開きます。[**続行**]をクリックすると、当該ロケーション内の非アクティブな認定アクセスポイントを削除します。

アクセスポイントの自動削除

不正アクセスポイントが自動的に削除されるまでの非アクティブ期間を指定できます。
設定をするには、 [**モニター**]>[WIPS]>[**クライアント**]または[**ネットワーク**]タブ画面右上の[**自動削除**]をクリックし、以下の[**アクセスポイントの削除パラメーター**]を入力して保存します。自動削除設定を使用するには、Superuser、AdminまたはOperatorの権限が必要です。自動削除は、作成したフォルダではなくルートフォルダ（AIRRECT Cloud）で行う必要があります。



2.5.11 WIPSに接続されているクライアントを確認する

[モニター]>[WIPS]>[クライアント]画面では、WIPSアンテナにより検知されたクライアントと、その詳細情報が表示されます。

パラメータ	概要
ステータス	クライアントがアクティブか非アクティブかを表します。
名前	クライアントのユーザー定義名を指定します。
ユーザー名	クライアントのユーザー名を通知します。
MACアドレス	メーカーによってネットワークアダプタに割り当てられたMACアドレスを表示します。
ローカル管理されているアドレス	クライアントがランダムMACアドレスを使用している場合、「はい」と表示されます。
IPv4アドレス	クライアントのIPv4アドレスを表します。
IPv6アドレス	クライアントのIPv6アドレスを表します。
OS	クライアントで利用しているOSを表します。
関連付けられたアクセスポイント	クライアントがアソシエーションされているアクセスポイントを表示します。
関連付けられたSSID	クライアントがアソシエーションされているアクセスポイントのSSIDを指定します。
周波数帯	クライアントが接続している、または送信しているプローブリクエストの周波数帯を表します。
Wi-Fi規格	クライアントが接続している、または対応している最新のWi-Fi規格を表します。
チャネル	クライアントが接続しているチャネルを表します。
RSSI (dBm)	クライアントのRSSI(受信信号強度)を表します。

接続・切断された日時	クライアントがシステムアップまたはダウンしてからの日時を表します。
最初の検出	最初にクライアントが検出された日時を表します。
自動防止ステータス	クライアントの自動防止の状態を表します。
防止ステータス	クライアントの防止の状態を表します。
ロケーション	クライアントが接続されているロケーションを表します。
メーカー名	クライアントのメーカー名を表します。
禁止状態	クライアントの禁止状態を表します。
手動で分類	クライアントが手動で分類されたかどうかを表します。
手動でタグ付け	クライアント端末を別のロケーションに移動した場合に「はい」と表示されます。
セルID	クライアントがアドホック通信をしている場合、セルIDを表します。
タグ	クライアントのタグを表します。

クライアント名の右クリックで、以下のアクションを実行できます。

アクション	概要
分類を変更する	クライアントの分類を変更します。
名前を変更	クライアント名を変更します。
パケットトレースをキャプチャ	特定の端末間を通過または移動するデータパケットのキャプチャをします。
パケットトレースの履歴	過去30分間にキャプチャされたパケット・レースが表示されます。
ライブクライアントデバックを開始	クライアントに関するライブ・クライアント・ログが表示されます。
デバイス・タグを更新する	デバイス・タグを更新します。
検索	クライアントの位置がフロアマップ上に表示されます。
移動	クライアントのロケーションを変更できます。
このデバイスを防止する	クライアントを防止します。
削除	リストからクライアントを削除します。
自動防止を無効化する	クライアントの自動防止を無効化します。
許可 SSID を管理する	クライアントの許可 SSID を管理します。

クライアントの自動削除

一定期間アクティブになっていないクライアントを自動で削除することができます。手動で分類されたクライアントを保持する場合は、自動削除パラメータで指定できます。

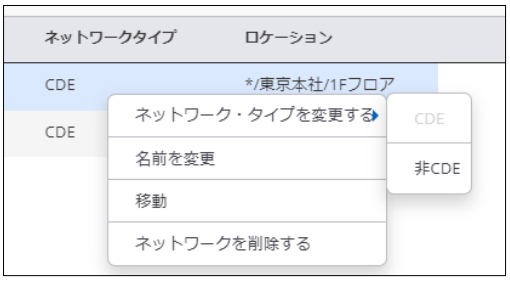
クライアントを自動削除するには、画面右上の[**自動削除**]をクリックし、[**クライアントの削除パラメーター**]で設定します。自動削除設定を使用するには、Superuser、AdminまたはOperatorの権限が必要です。

削除内容については、『アクセスポイントの自動削除』をご参照ください。

2.5.12 WIPSのネットワーク監視

[**モニター**]>[**WIPS**]>[**ネットワーク**]で、WIPSによって監視されているネットワークを確認できます。以下に示すように、監視されていないネットワークは赤色で表示されます。

カードデータホルダー環境(CDE)ネットワークは、気密性の高いクレジットカードのデータを取り扱うネットワークです。CDEネットワークは、PCIDSS準拠の範囲内にあります。ネットワークを右クリックして、ネットワークタイプをCDEか非CDEに変更できます。



ネットワークの自動削除

ネットワークがサーバー上に保持される期間を定義できます。指定された保持期間が経過すると、ネットワークはサーバーから自動的に削除されます。ネットワークを自動削除するには、画面右上の[**自動削除**]をクリックし[**ネットワークの削除パラメーター**]を入力します。削除内容については、『アクセスポイントの自動削除』をご参照ください。

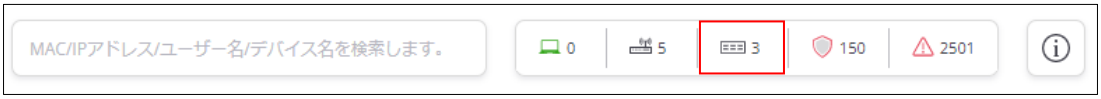
2.5.13 モニターからスイッチングハブ情報を確認する

[**モニター**]>[**有線**]画面では、アクセスポイントの接続先スイッチングハブを表示します。スイッチングハブ名のクリックで [**アクセスポイント**]と[**WiFiクライアント**]の詳細情報が表示されます。本機能を使用するには、スイッチングハブにて、LLDP(Link Layer Discovery Protocol)を有効にする必要があります。

パラメータ	概要
名前	スイッチの名前を表します。
メーカー名	スイッチのメーカー名を表します。
シャーシ ID	スイッチの MAC アドレスを表します。
接続しているアクセスポイント	接続しているアクセスポイントの数を表します。
接続している WiFi クライアント	接続しているクライアント数を表します。

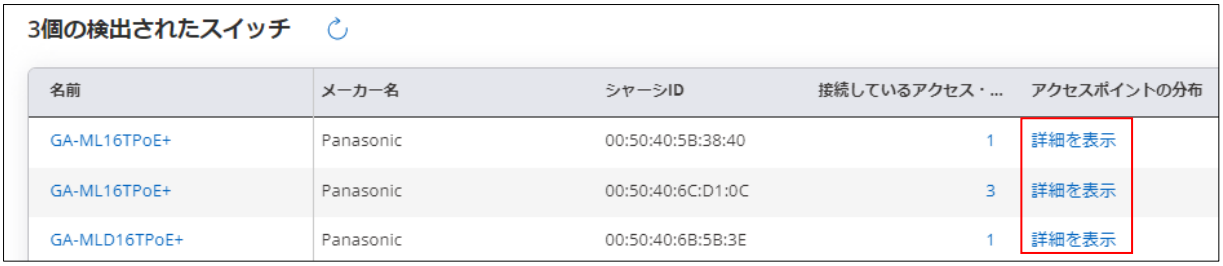
グローバルカウンターからもスイッチングハブの情報が確認できます。カウンターでは、選択したロケーションによりステータスがアクティブのスイッチングハブ数を表示します。上位ロケーションでは、配下のフォルダを含めた総アクティブスイッチングハブ数を表示します。

注意：ステータスが非アクティブのスイッチはカウンターに含まれません。

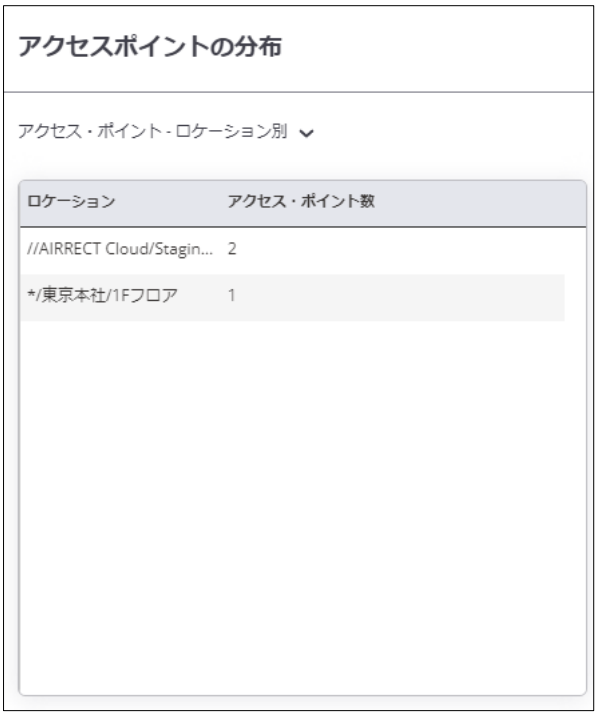


スイッチングハブ情報

スイッチングハブの情報として、「名前/メーカー名/シャーシ ID/接続しているアクセスポイント/アクセスポイントの分布/接続している WiFi クライアント」が表示されます。
アクセスポイントの分布は、接続されている全てのアクセスポイントが確認できます。
確認するには、[**詳細を表示**]をクリックします。



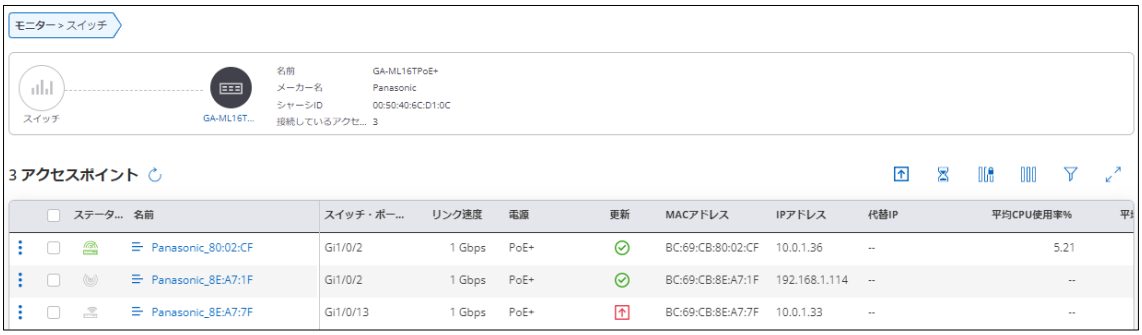
アクセスポイントの分布では「ロケーション別/PoE タイプ別/リンク速度別」のフィルタが使用し、それぞれの分類での状態を確認することができます。



・[**ロケーション別**]：アクセスポイントが所属しているロケーションが表示されます。
・[**PoE タイプ別**]：アクセスポイントが接続している PoE タイプ「PoE」、「PoE＋」、「PoE＋＋」のいずれかが表示されます。
・[**リンク速度別**]：アクセスポイントが接続しているリンク速度「10Gbps」、「5Gbps」、「2.5Gbps」、「1Gbps」、「100Mbps」、「10Mbps」のいづれかが表示されます。

スイッチ情報の詳細

[検出されたスイッチ]の一覧から、任意のスイッチングハブの名前を選択するとスイッチングハブに接続されている全てのアクセスポイント情報が表示されます。



パラメータ	概要
ステータス	アクセスポイントのステータスを表します。（アクティブスイッチ/非アクティブ）
名前	アクセスポイントの名前を表します。
スイッチ・ポート	接続されているスイッチのポート情報を表します。
リンク速度	リンク速度を表します。
電源	電源を表します。（PoE/PoE+/PoE++）
更新	デバイスのファームウェア状態を表します。
MAC アドレス	アクセスポイントの MAC アドレスを表します。
IP アドレス	アクセスポイントの IP アドレスを表します。
代替 IP	アクセスポイントの代替 IP を表します。
平均 CPU 使用率（%）	平均の CPU 使用率を表します。
平均メモリ使用率（%）	平均のメモリ使用率を表します。
ビルド	ビルド環境を表します。
最終更新時刻	更新を行った最終時刻を表します。
更新予定日時	更新予定日時を表します。
接続・切断された日時	アクセスポイントが接続・切断された日時を表します。
最終起動日	アクセスポイントの最終起動日を表します。
Wi-Fi 規格	Wi-Fi の規格を表します。
モデル	デバイス・モデル名を表します。
グループ	グループを表します。
SSID	アクセスポイントの SSID を表します。
場所	アクセスポイントの場所を表します。
メッシュモード	メッシュモードの状態を表します。（有効/無効）
タグ	タグ情報を表します。

さらに、任意のアクセスポイントを選択すると、アクセスポイントに接続されている以下のクライアント情報が表示されます。

パラメータ	概要
名前	クライアント端末の名前を表します。
ユーザー名	ユーザー名を表します。
関連付けされたアクセスポイント	関連付けされたアクセスポイントの名前を表示します。
スイッチ・ポート	アクセスポイントが接続されているスイッチのポート情報を表します。
MAC アドレス	クライアント端末の MAC アドレスを表します。
ローカル管理されているアドレス	クライアントがランダム MAC アドレスを使用している場合、「はい」と表示されます。
IPv4 アドレス	クライアント端末の IPv4 アドレスを表します。
IPv6 アドレス	クライアント端末の IPv6 アドレスを表します。
OS	クライアントの OS 情報を表します。
関連付けられた SSID	関連付けられた SSID の情報を表します。
チャネル	アクセスポイントのチャネルを表します。
周波数帯	アクセスポイントの周波数帯を表します。
Wi-Fi 規格	アクセスポイントの Wi-Fi 規格を表します。
RSSI（dBm）	アクセスポイントの信号強度を表します。
アップリンクデータ	クライアントの端末からアクセスポイントへ送られた信号やデータの量を表します。
ダウンリングデータ	アクセスポイントからクライアントの端末へ送られた信号やデータの量を表します。
平均データレート	平均のデータレートを表します。
再試行率（%）	再試行率を表します。
接続・切断された日時	クライアント端末が接続・切断された日時を表します。
First Detected Time	最初に検出された日時を表します。
場所	場所を表します。
スティッキー	スティッキー情報を表します。（はい/いいえ）
メーカー名	クライアント端末のメーカー名を表します。
ロール	ロールを表します。
Google 認可	Google 認可有無を表します。
タグ	タグ情報を表します。
手動でタグ付けされました	クライアント端末を別のロケーションに移動した場合に「はい」と表示されます。

2.6 Wi-Fiの構成

[構成]タブより、Wi-Fiネットワークを構成するための設定ができます。デフォルトでは、特定のロケーションで変更した設定は、その配下のロケーションにも自動的に継承されます。例えば、支社1と支社2のロケーションフォルダを含む、本社フォルダがあるとします。本社にネットワーク構成を設定すると、自動的に支社1と支社2にも適用されます。ただし、配下のロケーション構成をカスタマイズして、上位のロケーションとは異なるように設定することも可能です。

[構成]タブでは、以下の内容について設定することができます。

●SSID設定
●デバイス設定
- デバイスCLIパスワードやLED消灯等の設定
- 無線通信設定

●ネットワークプロファイル設定
- RADIUSプロファイル
- トンネルインターフェイスプロファイル
- ロールプロファイル

●WIPS設定
●アラート設定

2.6.1 SSIDの設定

[構成]>[Wi-Fi]でAIRRECT Cloudに新規SSIDの追加、編集、コピー、削除、ON/OFF切り替えを行うことができます。SSID設定画面では、Wi-Fiネットワークで設定されているSSIDとその主要機能のすべてが表示されます。また、SSIDとその主要構成がカードとして表示されるカードビューと、これらの項目が表に一覧表示されるテーブル表示に切り替えることができます。

任意のSSIDを選択すると、 以下のタブにより各設定が可能です。

●基本
●セキュリティ
●ネットワーク
●アクセス制御
●アナリティクス
●キャプティブポータル
●RF最適化
●SSIDスケジューリング
●トラフィックシェーピングとQoS

「基本」、「セキュリティ」、「ネットワーク」はSSID設定に必須の項目です。
ロケーションごとに最大14個のSSIDを有効にすることができます。

SSIDの新規追加

SSIDをロケーションに追加するには、以下の手順を実行します。

1. [**構成**]に移動すると、[**SSID**]**タブ**が表示されます。
2. [**SSIDを追加**]ボタンをクリックすると、[**SSID**]>[**基本**]**タブ**が表示されます。
3. [**基本**]**タブ**でSSID名等を設定します。詳細については『SSIDの基本設定』を参照してください。
4. [**次へ**]をクリックすると、[**セキュリティ**]**タブ**が表示されます。
5. [**セキュリティ**]**タブ**で暗号化方式等を設定します。詳細については『SSIDのセキュリティ設定』を参照してください。
6. [**次に**]をクリックすると、[**ネットワーク**]**タブ**が表示されます。
7. [**ネットワーク**]**タブ**で、基本的なネットワーク設定をします。詳細については『SSIDのネットワーク設定』を参照してください。
8. [**保存**]をクリックしてSSIDを保存するか、 [**SSIDを保存して有効にする**]をクリックしてSSIDをオンの状態で保存します。

SSIDの基本設定

[**基本**]**タブ**には、以下のフィールドが含まれています。

パラメータ	概要
SSID名	SSID名は、SSIDに割り当てる名前を表します。
プロファイル名	通常、SSID名と同じです。これは、重複するSSIDを区別するために使用します。そのため、同じロケーションにあり重複するSSIDには異なるプロファイル名がつけられます。例えば、「ABC Corp」 を同じロケーションに重複する場合、新規のSSID名は「ABC Corp」 になりますが、そのプロファイル名は 「Copy of ABC Corp (1)」 になります。プロファイル名については、変更可能です。
SSIDタイプを選択	[**SSIDタイプ**]は**ゲストSSIDに**することができます。通常は、**キャプティブポータル**ログイン時にゲストSSIDを使用します。[**ゲスト**]をクリックすると AIRRECT Cloudでは、[**ネットワーク**]**タブ**の隣に[**キャプティブポータル**]**タブ**が表示されます。
SSIDを非表示	[**SSIDを非表示**]をクリックすると、自動でクライアント端末にSSIDが非表示となり、セキュリティが向上します。
AP名にビーコンを含める	有効にすると、パケットにアクセスポイントのビーコン名が追加されるため、ユーザーや管理者は複数のアクセスポイントが設置されている環境下でも、任意のアクセスポイントの特定、識別が容易になります。アクセスポイント名から役割や場所を認識したり、不正アクセスポイントであることの確認としても使用できます。

SSIDの基本設定の構成

[基本]タブは、SSIDの設定において必須となる、SSIDタブ　(**[基本]**、**[セキュリティ]**、および **[ネットワーク]**) のうち、最初のタブを意味します。以下の項目に、情報を入力します。

1. **[SSID名]**には、割り当てたいSSID名を入力します。**[プロファイル名]**フィールドには、自動的にSSID名が入力できます。ただし、これが元のロケーションと重複するSSIDの場合については除きます。
2. **[SSIDタイプを選択]**で**[プライベート]**または**[ゲスト]**のどちらかを選択します。
3. SSIDをブロードキャストしない場合は、**[SSIDを非表示]**をクリックします。
4. 問題発生時のパケットにアクセスポイント名を表示させたい場合は、**[AP名をビーコンに含める]**を有効化します（デフォルト有効）

5. 以下の手順に関しては、SSIDを新規追加するか、または既存のSSIDを更新するかによって異なります。
   - ●SSIDを新規で追加する場合、**[次に]**をクリックして **[セキュリティ]タブ**へ移動します。
   - ●既存のSSIDを更新する場合、**[保存]**または**[SSIDを保存して有効にする]**をクリックします。この場合、「**SSIDが正常に更新されました。**」というメッセージが表示されます。

2.6.2 SSIDのセキュリティ設定

クライアント端末と接続するセキュリティレベルを選択します。
セキュリティレベルはユーザーの認証方式を定義します。設定項目は以下の通りです。

パラメータ	概要
オープン	セキュリティ設定が適用されないことを表します。
WPA2	WPAよりも堅牢性が高く、IEEE 802.11i規格を実装しています。事前共有鍵（PSK）または802.1x、UPSKで使用することができます。
WPA/WPA2 混合モード	WPAとWPA2プロトコルの混合の認証方式です。PSKまたは802.1x、UPSKで使用することができます。
ホットスポット 2.0 OSEN	ホットスポット2.0の設定を行います。 ※AIRRECT Cloudはバージョン2.0のみ対応です。
WPA3	WPA3-PersonalまたはWPA3-Enterprise、UPSKを使用できます。WPA3-Personalは、WPA2から改善されたパスワードベースの認証と128ビットデータのAES暗号化により堅牢性を強化し、パスワードを推測しようとする辞書攻撃等から保護します。WPA3-Enterpriseは、192ビット暗号化を使用するオプションがあり、データのセキュリティと保護の必要性が高いオフィスネットワークに最適です。
WPA2/WPA3 混合モード	WPA2とWPA3プロトコルの混在の認証方式です。WPA2のみ対応のクライアントも、WPA3をサポートしているクライアントと同じSSIDで接続できます。このモードでは、WPA3クライアントはWPA3-Personalを使用します。
OWE	オープンネットワークの拡張機能であり、オープンネットワークに暗号化されたセッションでクライアントにデータセキュリティを提供します。

注意：802.11wはWPA2, WPA3, WPA2/WPA3混合モードのみサポートしており、WPA/WPA2混合モードではサポートされません。
また、802.11rはWPA2のみサポートしています。

RADIUS設定の詳細については、『RADIUS』セクションを参照してください。

●[802.11w]は管理フレーム保護（MFP）に関する機能を提供します。MFPは認証解除、アソシエーション解除、および、ロバストアクション管理フレームを保護し、スプーフィング攻撃を防ぐセキュリティメカニズムです。また、インテグリティ・グループ・テンポラル・キー（IGTK）は、マルチキャスト管理アクションフレームの整合性チェックにおいて使用されます。ペアワイズ・トランジェント・キー（PTK）は、ユニキャスト管理アクションフレームの暗号化と保護の目的において使用されます。

●[**グループ管理暗号**]は、管理フレームの保護で使用するセキュリティと暗号化アルゴリズムの組み合わせを意味します。AIRRECT CloudではAES-128-CMACアルゴリズムを使用しており、デフォルトとして当アルゴリズムが選択されています。アソシエーションフレームは、アクセスポイントとの接続を確立するために、クライアントに向けてオープンにしておく必要があるため保護されていません。
クライアントのアソシエーションリクエストがスプーフィングされないように、アクセスポイントはセキュリティアソシエーション (SA) クエリをクライアントが要求しているアソシエーションに向けて送信します。本物のクライアントは、保護されたフレームに対して応答します。

●[**SAクエリーの最大タイムアウト**]は、クライアントがSAクエリに応答するまでアクセスポイントが待機する時間（秒単位）を表します。この期間内に、アクセスポイントが応答を受信しない場合、クライアントは無視されます。また、アソシエーションリクエストをスプーフィングするクライアントは応答しないので、アクセスポイントはそれらを拒否します。

●[**SAクエリーの再試行タイムアウト**]は、SAクエリーの最大タイムアウトの後にクライアントが、アクセスポイントとのアソシエーションを要求できる、ミリ秒単位の時間です。

SSIDセキュリティ設定の構成

[セキュリティ]タブは、SSIDの設定において必須となる、SSIDタブ ([**基本**] 、[**セキュリティ**]、および [**ネットワーク**]) のうち、 2番目のタブを意味します。

SSIDセキュリティ設定に関する作業手順は、以下の通りです。

1. [**構成**]>[SSID]配下の[**セキュリティ**]**タブ**に移動します。
2. SSIDの[**アソシエーションのセキュリティレベルを選択**]をクリックします。

a) [**アソシエーションのセキュリティレベルを選択**]で[**オープン**]や[OWE]を選択した場合、セキュリティの設定はありません。
OWEの詳細については、『OWEの動作』を参照してください。
SSIDを新規で追加する場合、[**次に**]をクリックして[**ネットワーク**]**タブ**に移動します。

b) [**アソシエーションのセキュリティレベルを選択**]で[WPA2]を選択する場合は、[PSK]、[UPSK]、[802.1x]より選択します。

- [PSK]を選択する場合は、[**パスフレーズを入力**]にパスフレーズを入力します。
- [グループPSK]機能を有効にすることもできます。
グループPSKの詳細については、『グループPSK』を参照してください。

- [802.1x]を選択する場合は、[**RADIUS設定**]を入力する必要があります。[**RADIUS設定**]には、以下の項目があります。

●[**認証サーバー**]：[**認証サーバー**]として使用するRADIUSサーバーを表します。

●[**アカウンティングサーバー**]：[**アカウンティングサーバー**]として使用するRADIUSサーバーを表します。

[**認証サーバー**]または[**アカウンティングサーバー**]として選択するRADIUSプロファイルが、まだ定義されていない場合、[**追加/編集**]をクリックすると表示される設定画面から定義することができます。RADIUSプロファイルの設定の詳細については、『RADIUSプロファイルの設定』を参照してください。

●[**再試行パラメータ**]：アクセスポイントがRADIUSサーバーでの認証を試みる回数、および、タイムアウトを制御するパラメータを表します。

●[**発信先ステーション/NAS ID**]：アクセスポイント、または、ネットワークアクセスサーバー（NAS）がRADIUSサーバーに送信するIDを表します。

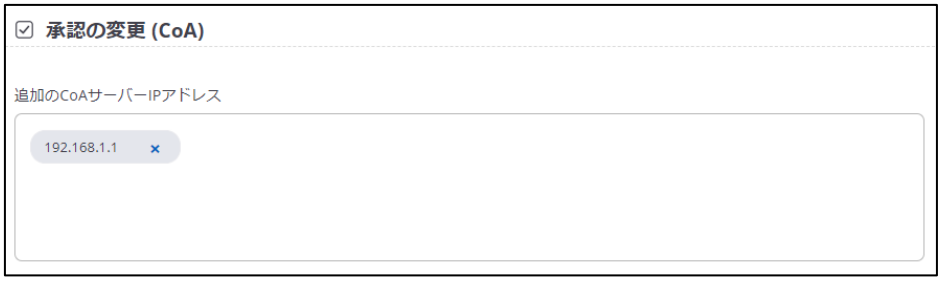
注意：同一アクセスポイント上にある2つのSSIDに同じNAS IDを使用できません。

●[**高速ハンドオフサポート**]：あるアクセスポイントから別のアクセスポイントにローミングする際、クライアントにとって必要な認証時間を削減するためのパラメータを表します。

- Opportunistic Key Caching(OKC): クライアントが同じアクセスポイントに再度接続する場合に、最初の接続キー情報をキャッシュすること認証プロセスをスキップし、で接続時間を高速化します。これにより、ローミング時のネットワーク切り替えを高速化すると同時に、ネットワークリソースの削減もすることができます。
- 事前認証: アクセスポイントが保持しているクライアントの認証情報を、あらかじめ隣接するアクセスポイントと共有することで、ローミング時のハンドオーバーが発生する前に高速で切り替えを可能とする機能です。

●[**ダイナミックVLAN**]：RADIUS（認可サーバ）から受信したVLAN情報に基づき、VLANを動的に割り当てます。割り当てを許可するVLAN IDやVLAN名を指定する場合には「**VLAN ID**」または「**VLAN 名**」を選択し、指定しない場合には「**自動VLAN**」を選択します。

●[**承認の変更 (CoA)**]：CoAは、Change of Authorizationの略称であり、クライアント認証の変更を行うことが出来ます。ユーザーのセッション中に特定のアクセス権の変更、ポリシーの更新、セッションの切断などがあった場合、CoAを利用することで、既存のセッションに対して動的な変更を適用します。
CoAでは、RADIUSサーバーがネットワークデバイスに対して変更命令を送信します。この変更命令には、ユーザーのアクセス権の変更、セッションの切断、再認証の要求などが含まれる場合があります。ネットワークデバイスは、CoAを受信すると、それに従ってユーザーのセッションに対する変更を実施します。CoAはネットワーク管理者がリアルタイムでユーザーアクセスを管理し、ポリシー変更やセキュリティ要件の対応を容易にするためにも使用されます。
また、
CoAサーバーは、認証サーバとして設定しているサーバだけでなく、使用環境に合わせてCoAリクエストの送信元IPを最大16台まで追加できます。



- [UPSK]は、サードパーティのNAC(Network Access Control)サーバとの連携が可能です。UPSKの詳細については、『UPSK(Unique PSK)の動作』を参照してください。

c) [**アソシエーションのセキュリティレベルを選択**]で[WPA/WPA2**混合モード**]を選択する場合、[PSK]、または、[802.1x]を選択する必要があります。その後、[WPA2]を選択した場合と同じ方法で続けることができますが、[802.11w]と[802.11r]はサポートされていません。

d) [**アソシエーションのセキュリティレベルを選択**]で[WPA3]を選択する場合は、[WPA3-Personal]または[WPA3-Enterprise]のいずれかを選択する必要があります。[WPA3-Personal]は、イコールの同時認証（SAE）を使用してデータを保護し、ホームユーザーを対象としています。[WPA3-Enterprise]は、データセキュリテ

ィに192ビットセキュリティを追加するオプションが含まれており、企業ネットワークを対象としています。

e) [**アソシエーションのセキュリティレベルを選択**]で[**ホットスポット2.0 OSEN**]が選択できます。Hotspot 2.0は、Wi-Fiネットワークと携帯電話ネットワークの間でシームレスなローミングを可能にする、公衆アクセスWi-Fi規格です。Hotspot 2.0では、Passpoint認証されたノートパソコンやスマートフォンなどのモバイル機器が、Wi-Fiネットワークを自動的に検出し、接続することができます。Hotspot 2.0は、外部ネットワークとの連携に関する規格である、IEEE802.11u（Interworking with External Network）をベースにしています。
Hotspot 2.0 は、WPA2 802.1x、WPA3 Enterprise、WPA3 Transition Mode でのみ機能します。本機能は、RADIUS サーバーを設定し、802.11w 管理フレーム保護が[**必須**]または[**オプション**]に設定する必要があります。

3. 次の手順は、SSIDを新規で追加する、または既存のSSIDを更新するかによって異なります。
   - SSIDを新規で追加する場合は、[**次に**]をクリックして [**ネットワーク**]**タブ**まで移動します。
   - 既存のSSIDを更新する場合、[**保存**]または[**SSIDを保存して有効にする**]をクリックします。この場合、「SSIDが正常に更新されました」というメッセージが表示されます。

OWEの動作

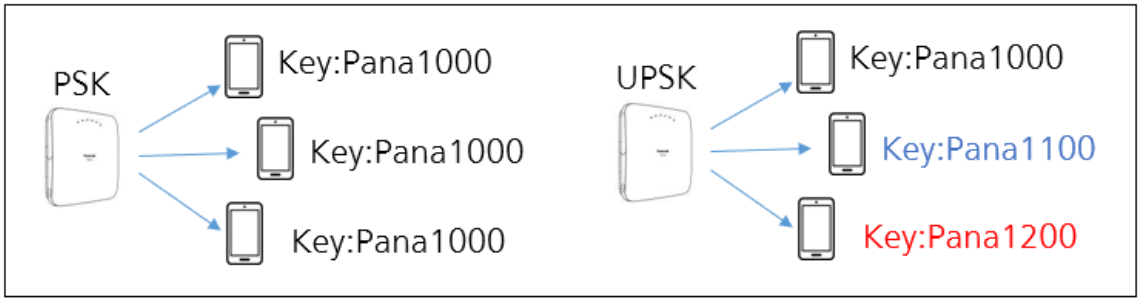
OWE（Opportunistic Wireless Encryption）は、認証は不用でセキュリティプロトコルをサポートする新しい認証方式です。OWEで移行モードのチェックボックスを有効にすると、OWEをサポートしないクライアントは、従来と同様のOpenプロトコルを使用してOWE SSIDに接続することができます。
移行モードを有効にすると、OWE SSIDと、オープンセキュリティのSSIDが自動で作成されます。セキュリティポリシーを除いて、他のすべての設定は同一であり、編集できません。また、移行モードでOWE SSIDを作成する場合は、12個以上のSSIDがオンになっていないことが必要です。

注意：一度OWEの設定をすると、SSIDの編集ができなくなります。SSIDの編集が必要な場合、作成したSSIDを削除し、再設定をする必要があります。

UPSK(Unique PSK)の動作

UPSKは、一つのSSIDで複数のクライアントに対して固有のパスフレーズに接続することを可能にします。それにより、シングルPSKと比較して、セキュリティが強化されます。

UPSKは、BYOD/IOTデバイスが大量に存在する、大学等の大規模なキャンパスで有効です。UPSKの利用には、RADIUS MAC認証が必須となります。



●UPSK接続ワークフロー

1. 新規ユーザーがログインし、デフォルトのPSKを使用してクライアントを接続します。
2. アクセスポイントは、RADIUSサーバーとMAC認証を開始します。MACアドレスが登録されていないため MACアドレスが登録されていないとき、RADIUSサーバーはクライアントにデフォルトのロールを割り当てます。
3. クライアントは登録のためのポータルにリダイレクトされます。
4. 登録後、ユーザーは自動生成または管理者が設定したUnique PSKを取得します。
   ユーザーは、RADIUSサーバーにMAC登録した後、このUPSKを使用して他のデバイスに接続することができます。
5. デバイスが登録されると、RADIUSサーバーはクライアントにCOA-Disconnectを送信することができるようになります。

●登録ユーザーオンボーディングフロー

1. ユーザーは、登録した端末をUPSKが有効なSSIDに接続し、割り当てられたPSKを入力します。
2. アクセスポイントはRADIUSサーバとMAC認証をします。MACアドレスは既に登録されているため、 RADIUSサーバーは、割り当てられたPSK にRADIUS Tunnel-Password属性を含むaccess-acceptを送信します。
   - 属性名 Tunnel-Password
   - 属性ID：69
3. アクセスポイントは、ユーザーが入力したPSKのハッシュと、access-acceptパケットで受信したPSKのハッシュを照合します。正しく一致した場合、ユーザーデバイスはオンボードされます。

ローカル認証の動作

802.1X、または WPA3-Enterprise を選択した場合、[**ローカル認証**]チェックボックスが出現します。RADIUS サーバーへ到達不能な場合にはアクセスポイントが EAP サーバーとなりデバイスを TLS 認証します。アクセスポイントへは TLS 証明書の署名検証を行う CA 証明書と RADIUS サーバー証明書を入力する必要があります。

●**CA 証明書をアップロード**：TLS 証明書の署名検証を行う CA 証明書を入力します。

●**証明書タグを選択**： RADIUS サーバー証明書を選択します。この証明書はアクセスポイントから生成した CSR を基に発行、署名する必要があります。

●**デッドタイム**：ローカル認証モードを継続する期間（5-120 分）を指定します。

●**ロールを割り当て**：ローカル認証成功デバイスへ割り当てるロールを選択します。

※これは一時的な認証システムであり、プライマリ認証としては使用しないでください。

※ローカル認証でサポートする認証方式はEAP-TLSのみです。

KRACKによる脅威の軽減

WPA/WPA2 混在モード、または WPA2 を選択した場合、[**KRACK による脅威の軽減**]チェックボックスが表示されます。有効にすることで、以下に示す WPA2 の脆弱性「KRACK」を緩和する効果が付与されます。

CVE-2017-13077、13078、13079、13080、13081

ローカルで管理されているMACアドレスを拒否する

ランダム MAC アドレス（プライベート MAC アドレス）を使用しているクライアントが SSID に接続できなくなります。

RADIUSプーリング

通信に使用する RADIUS サーバーを SSID 単位で分散することで、RADIUS サーバーの負荷を軽減し、AAA 通信品質を向上できます。

2.6.3 グループPSK

IoTデバイスをWi-Fiネットワークに接続させたい場合、ネットワーク管理者は、同じSSIDを異なる種類のクライアントデバイスに使用し、且つそれぞれにVLANやアクセスリストを割り当てたいときがあります。
例：プリンターとビデオカメラを別々のVLANにマッピング

IoTデバイスは通常、クライアントを個別のVLANにセグメント化するために使用する802.1xベースの認証方法をサポートしていません。グループPSKを使用すると、同じSSIDを異なるPSKで構成できます。例えば、あるPSKはプリンター用、別のPSKはビデオカメラ用といった具合です。また、各グループPSKにロールを割り当てることもできます。

また、小規模な支店や小売店で、同じSSIDのユーザーを部門別（人事、財務、法務など）に分けたい場合でも有用です。このような施設では、通常、802.1xのインフラを持っていませんが、グループPSKを使用することでユーザーを分けることができます。

グループPSKは1つのSSIDで最大32個サポートし、それぞれがWiFiクライアントのグループに対応します。

制限事項
グループPSKを使用するにあたっては、以下の制限があります。
●グループPSKは、以下のセキュリティ方式でのみサポートされます：
　WPA2（PSKを選択時）
　WPA/WPA2混合モード（PSKを選択時）
●グループPSKでは、セカンダリ認証（RADIUS MAC認証やGoogle認証など）はサポートされていません。
●キャプティブポータルは、グループPSKではサポートされていません。
●グループPSKは、VPN（L3トンネル）またはNATを使用するSSIDではサポートされていません。

グループPSKの構成

SSID設定の[**セキュリティ**]>[**アソシエーションのセキュリティレベルを選択**]で[WPA2]または[WPA/WPA2 **混在モード**]を選択する場合に限り、グループPSKを有効にするチェックボックスが表示されます。

1. [**パスフレーズを入力**]に任意のパスフレーズを入力します。
2. [**ロールの割り当て**]**から、**構成>WiFi>ロールプロファイルで作成したロールを割り当てます。ロールを作成していない場合、下の[追加/編集]より、新規のロールを作成することもできます。
3. ウインドウ横の[＋]ボタンを押下することで、二つ以上のグループを作成します。
   一つ目のグループとは異なるパスフレーズを入力し、設定を保存してください。

2.6.4 SSIDのネットワーク設定

[ネットワーク]タブとは、SSIDを保存してオンにする前に設定が必要となるSSIDタブ（基本、セキュリティ、ネットワークなど）の一つです。本設定から、SSIDのデフォルトVLAN IDを設定する必要があります。また、アクセスポイントの設定をブリッジモード、NATモード、またはトンネルモードから選択して、動作させることができます。

ブリッジモード

アクセスポイントとアクセスポイントにアソシエーションされたクライアントを同一のサブネット上に配置する場合は、ブリッジネットワークを使用します。

NATモード

アクセスポイントとそのクライアントを別々のサブネットに配置する場合は、ネットワークアドレス変換 (NAT) を使用します。NATを使用すると、パブリックIPアドレスが必要なくなるため、多数のクライアントが追加できます。NATによって、ローカルIPアドレスはグローバルアドレスに変換されます。

注意：SSIDセキュリティ設定において、802.1x認証でダイナミックVLANが有効な場合、NATは選択できません。

●NATを構成するには、**[開始IPアドレス]**、**[終了IPアドレス]**、および、**[サブネットマスク]**などを入力する必要があります。これらは、アクセスポイントがクライアントにIPアドレスを割り当てるためのIPプールを定義します。また、**[ローカルIPアドレス]**は、ワイヤレス側のアクセスポイントのIPアドレス（クライアント側のIPアドレス）を表します。アソシエーションが正常に行われると、ワイヤレスクライアントは、**[DNSサーバー]**フィールドに入力したIPアドレスのリストからDNS情報を取得します。DNSサーバーのIPアドレスは1つ入力する必要があります（最大6つまで入力可能）。

●[**リース時間**]は、クライアントに割り当てられた IPが期限切れになるまでのDHCPリース時間 (分) を意味します。
● [**有線拡張**]を選択すると、アクセスポイントのセカンドイーサネットポートを使用して、無線LANと同様のNAT機能を有線側に拡張することができます。

トンネルモード
トンネルインターフェースは、SSID上のネットワークトラフィックを単一のエンドポイントとの間でルーティングし、このエンドポイントでポリシーを適用したい場合に便利です。トンネルモードでは、SSID上のアクセスポイントは、トンネルを介してすべてのトラフィックを、選択したトンネルインターフェースに設定されたリモートエンドポイントにルーティングします。詳細は『トンネルインターフェース』を参照してください。トンネルインターフェースをまだ定義していない場合は、「ネットワーク」タブ内の「追加／編集」リンクから定義できます。
トンネルネットワークでは、RADIUSサーバーがリモートエンドポイントの背後にあるプライベートコーポレートネットワークに設置されている場合があります。[**RADIUSメッセージにトンネルを使用**]を有効にすると、AIRRECT Wi-FiはアクセスポイントとRADIUSサーバとの間でRADIUSメッセージをトンネルします。

主な特徴は以下の通りです。
●すべてのタイプのトンネルインタフェースは、アクセスポイントとトンネルエンドポイントの背後にあるRADIUSサーバとの間のRADIUSメッセージのトンネリングをサポートします。
●RAP VPNトンネル以外のトンネルタイプでは、アクセスポイントはSSID VLAN上のリモートネットワークのDHCPサーバからIPアドレスを取得します。
●VPNトンネルでSSIDを実行しているRAPは、リモートVPNエンドポイント（ファイアウォールアプライアンスなど）からそのVPN IPアドレスを取得します。
●RAPのVPNトンネルは、IPv6をサポートしていません。RAPがRADIUSサーバーと通信するためにはRADIUSサーバーがIPv4アドレスを持っている必要があります。

トンネル経由の通信では、以下のRADIUSメッセージタイプがサポートされています。
●認証 (802.1X または RADIUS MAC 認証)
●アカウンティング
●認証の変更(CoA)

アクセスポイント間コーディネーション

アクセスポイント間コーディネーションは、アクセスポイントが相互に情報を交換する仕組みです。アクセスポイントが情報を交換する方法を次の3つから選択できます。

パラメータ	概要
レイヤー2 ブロードキャスト	有線ネットワークを経由しアクセスポイントによってブロードキャストされます。L2ブロードキャストはSSID VLANにおいて機能し、レイヤー2 GREが有効な場合、通信VLANにおいて機能します。トンネリングを使用すると、アクセスポイント間の調整に関する情報（RSSI、ステアリング等）がトンネルを経由して流れるようになります。
付近のRF	近くにあるアクセスポイントのみと無線で情報交換がおこなわれます。デバイス設定において、バックグラウンドスキャンが有効に設定されていない場合、SSIDをオンに設定して有効にするように求められます。トンネリングを使用して、アクセスポイント間コーディネーションに関する情報をトンネルエンドポイントから別のアクセスポイントへ受け渡しをすることもできます。
クラウドサーバー	アクセスポイントによって、AIRRECT Cloudサーバーを経由し情報交換が行われます。情報は、親ロケーションからその配下のロケーションの範囲において共有されます。 AIRRECT Cloudを経由するため、トンネリングモードを使用しての情報交換はできません。

[SSID VLANでクライアントアソシエーションをアドバタイズ]をクリックすると、同一SSID VLAN上の他のアクセスポイントにクライアントアソシエーションがブロードキャストされます。これは、クライアントの高速ローミングに役立ちます。

[802.11mc(Wi-Fi RTT)]をクリックすると、フロアマップでの位置情報の精度があがります。従来はRSSI強度によってクライアントの位置情報を認識しておりましたが、RSSI強度では正確にクライアントとアクセスポイントの距離を測るのが困難でした。
IEEE802.11mcの位置検知は、電波の到達速度で距離を測るため、従来よりも正確に距離を測ることが可能です。ただし、本機能を利用するにはクライアントも802.11mcに対応している必要があります。

[DHCPオプション82]は、通常、ロードバランシングDHCPサーバー環境において使用され、クライアントのロケーションに基づきIPアドレスがクライアントに割り当てられます。アクセスポイントによって、DHCPオプション82は、DHCPディスカバーやDHCPリクエストなどのDHCPパケットに挿入され、クライアントの接続ポイントを識別するための追加情報が提供されます。DHCPオプション82には、ロケーションとDHCPサーバーによって構成できる回路IDが含まれています。IDに適切なIPプールを選択した後、IPプールからDHCPサーバーによって、クライアントにIPアドレスが割り当てられます。

【使用例】
2つの支社があり、本社のデータセンターに1台のDHCPサーバーが設置されている企業の場合
●条件：SSIDは1つだけ設定されており同じ設定がすべての支社に割り当てられている
同じVLAN IDが設定されていますが、支社ごとに異なるサブネットが割り当てられています。

1. 本社、支店1、支店2の3つのSSIDプロファイルを作成します。
2. ロケーションツリーの各ロケーション（本社および支社）に適切なロケーションタグを設定します。
3. [DHCPオプション82]を有効に設定し、また[回路ID]は「%l」に設定されるので、ロケーションタグはDHCPサーバーに送信されます。DHCPサーバーでは、DHCPから受信した情報に基づいてポリシーを構成します。

オプション82　例
●回路ID=本社:172.16.0.0/16-172.16.8.255/16サブネットからIPを割り当てます。
●回路ID=支社1:172.16.9.0/16-172.16.12.255/16サブネットからIPを割り当てます。
●回路ID=支社2:172.16.13.0/16-172.16.15.255/16サブネットからIPを割り当てます。

[DHCPパケット転送]を有効にすると、アクセスポイントがDHCPパケットをリレーします。異なるセグメントに位置するDHCPサーバーからもIP情報を取得できます。

2.6.4.a SSID ネットワーク情報の基本設定

[**ネットワーク**]**タブ**は、SSIDの設定において必須となる、SSIDタブ ([**基本**] 、[**セキュリティ**]、および [**ネットワーク**]) のうち、 3番目のタブを意味します。
以下の設定が必要です。

1. [**構成**]>[Wi-Fi]>[SSID]>[**ネットワーク**]の順にクリックします。
2. SSIDのデフォルトの[VLAN ID]を入力します。
3. SSIDのアクセスポイント動作モードを選択します。
   a) [**ブリッジ**]を選択する場合、手順4に進みます。
   b) [NAT]を選択する場合は、以下のNATに関するパラメータを設定する必要があります。
      ●[**開始IPアドレス**] : アクセスポイントがクライアントにIPアドレスを割り当てるIPプールの開始IPアドレスが定義されます。
      ●[**終了IPアドレス**] : アクセスポイントがクライアントにIPアドレスを割り当てるIPプールの終了IPアドレスが定義されます。
      ●[**ローカルIPアドレス**] : ワイヤレス側のアクセスポイントのローカルIPアドレスを表します。
      ●[**サブネットマスク**] : IPプールのサブネットマスクを表します。
      ●[**DNSサーバー**] : クライアントがDNS情報を取得するために使用するサーバーです。DNSサーバーのIPアドレスについては、少なくとも1つ、入力する必要があります。DNSサーバーのIPアドレスは6つまで入力可能です。
      ●[**リース時間**] : クライアントに割り当てられたIPが期限切れになるまでのDHCPリース時間を分単位で表します。
      ●[**有線拡張**] : アクセスポイントの2番目のイーサネットポートを使用し、有線側にNAT対応を有効にします。
   c) [**L2トンネル**]、または、[**L3トンネル**]を選択する場合、アクセスポイントがすべてのトラフィックをトンネリングするエンドポイントを含む、[**トンネルインターフェイス**]を選択する必要があります。トンネルインターフェイスが定義されていない場合は、[**追加/編集**]をクリックすると画面右側に[**トンネルインターフェイス**]ウィンドウが表示されるので、そこでインターフェイスの定義を作成できます。
4. [**AP間コーディネーション**]メカニズムを選択します。
   a) [**レイヤー2ブロードキャスト**]をクリックすると、有線ネットワーク経由で、情報がアクセスポイントによってブロードキャストされます。
   b) [**付近のRF**]をクリックすると、アクセスポイントはRFネイバーのみと情報を交換できます。

（a,b共通）SSIDのアクセスポイント動作モードに[**L2トンネル**]を選択し、アクセスポイント間の調整に関する情報をトンネルに流す場合は[**AP間コーディネーションにトンネリングを使用**]をクリックします。

c) [**クラウドサーバー**]をクリックすると、AIRRECT Cloudサーバーを経由し、情報交換がおこなわれます。

5. SSID上のアクセスポイントがクライアントアソシエーションを同一SSID VLAN上の他のアクセスポイントにブロードキャストする場合は、[**SSID VLANでクライアントアソシエーションをアドバタイズ**]を有効にします。
6. フロアマップを利用する場合は、[**802.11mc(Wi-Fi RTT)の有効化**]をクリックします。
6. [**DHCPオプション82**]を選択すると、分散DHCPサーバー環境での場所に基づいてクライアントのIPアドレスを割り当てます。
7. [**保存**]または[**SSIDを保存して有効にする**]をクリックします。[**SSIDを保存して有効にする**]をクリックした場合の詳細については、『SSIDの有効化/編集』を参照してください。
   - SSIDを新規追加した場合、「SSIDが正常に追加されました」というメッセージが表示されます。
   - SSIDを更新した場合、「SSIDが正常に更新されました」というメッセージが表示されます。

2.6.4.b VLAN IDへのVLAN名マッピング

VLAN名マッピング機能により、1つのVLAN名を複数のVLAN IDにマッピングすることができます。マッピングは、以下2つの方法があります。

1. 「SSID VLANマッピング」：同じVLAN名を異なるロケーション、異なるSSIDのVLAN IDにマッピングすることができます。
   VLAN IDは最大32個、VLAN名は最大64個まで登録することができます。
2. 「ロケーションベースVLANマッピング」：VLAN IDを特定のロケーションのVLAN名にマッピングすることができます。
   VLAN IDは最大32個、VLAN名は最大64個まで登録することができます。

両方に同VLAN名のマッピングが存在する場合は、「ロケーションベースVLANマッピング」が「SSID VLANマッピング」よりも優先されます。

SSID VLANマッピングの使用例

本機能を使用すると、複数のロケーションで同じSSIDプロファイルと同じVLAN名としながら、VLAN IDをロケーションごとに異なる値にすることができます。
たとえば、VLAN名「CORP-VLAN」がVLAN1にマッピングされている「Emp-Access」という名前のSSIDをコピーし、同じVLAN名を使用し、SSID名を「Guest-Access」に変更する場合、ゲストアクセス用のVLAN IDを分けたいとします。このようなケースで、「Guest-Access」SSIDでは、VLAN名は同じ（CORP-VLAN）ですが、個別設定によりVLAN2にマッピングすることができます。

SSID名	VLAN名	VLAN ID
Emp-Access	CORP-VLAN	1
Guest-Access	CORP-VLAN	2

ロケーションベースのVLANマッピングの使用例

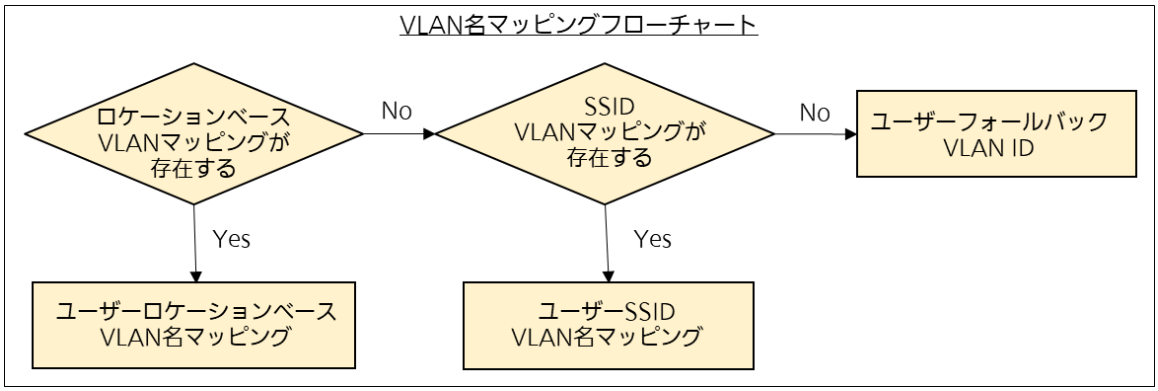
特定のロケーションにおいて、VLAN名をVLAN IDにマッピングして適用することができます。

例えば下のテーブルで、VLAN名「CORP-VLAN」にマッピングされた「Emp-Access」というSSIDが、6つのビルのすべての拠点で有効になっているとします。このとき、建物B1のロケーションで「CORP-VLAN」にVLAN ID 10をマッピングし、且つ「Emp-Access」のSSID設定にてVLAN名を同様に「CORP-VLAN」を指定すると、「Emp-Access」はロケーションベースのVLANマッピングに則りVLAN10で通信を行います。同様に、建物B2ではVLAN ID 20が指定されているため、建物B2では「Emp-Access」はVLAN20で通信が行われます。

SSID名	VLAN名	ロケーション	VLAN ID
Emp-Access	CORP-VLAN	建物B1	10
Emp-Access	CORP-VLAN	建物B2	20
Emp-Access	CORP-VLAN	建物B3	30
Emp-Access	CORP-VLAN	建物B4	30
Emp-Access	CORP-VLAN	建物B5	30
Emp-Access	CORP-VLAN	建物B6	30

VLANマッピングのフローチャート

VLAN名を使用するごとに、AIRRECT APは、そのVLAN名がロケーションにマッピングされているか確認します。もしマッピングされていれば、VLAN名はその場所に指定されたIDを使用します。ロケーションベースのVLANマッピングが定義されていない場合、SSID VLANマッピングの名前を確認します。SSIDマッピングが利用可能であれば、それが使用されます。両方のマッピングが利用できない場合、指定されたフォールバックVLAN IDを使用します。



VLAN名マッピングの設定

VLAN名とVLAN IDの関連付けは、AIRRECT Wi-Fi内の以下の3か所から行うことができます。

●SSID設定
●ロケーションベースマッピング
●ロールプロファイル

SSID VLANマッピング

SSID の VLAN マッピングを有効にするには以下の手順で行います。

1. [**構成**]>[SSID]>[SSID **を追加**]の順で進みます。
2. [**ネットワーク**]タブをクリックします。
3. [VLAN]配下の[VLAN **名**]ラジオボタンを選択し、VLAN 名を入力します。

4. [**フォールバック** VLAN ID]を入力します。
5. [SSID VLAN **マッピング**]をクリックします。画面右側にパネルが開き、名前を VLAN ID にマッピングすることができます。また、このマッピングが使用されている場所も確認できます。

6. 追加する場合は、[**追加**]の青字の文言をクリックし、[VLAN **名**]と[VLAN ID]を入力後、[**追加**]のアイコンをクリックします。
7. SSIDを保存して有効にします。

ロケーションベースのVLANマッピング

ロケーションベースのVLANマッピングを有効にするには以下の手順で行います。

1. [**構成**]>[Wi-Fi]と進みます。
2. メニューアイコンをクリックし、[**ロケーションベースVLANマッピング**]をクリックします。

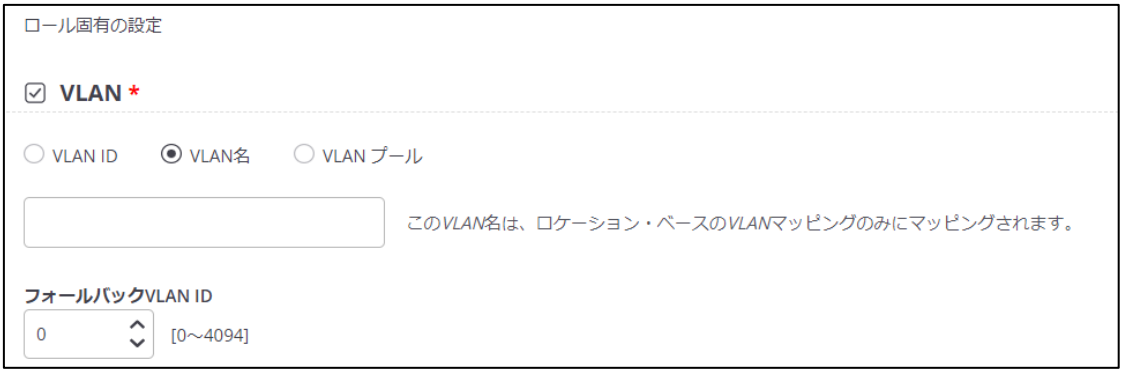
3. 画面にパネルが開き、名前を VLAN ID にマッピングすることができます。また、このマッピングが使用されている場所も確認できます。

4. 追加する場合は、青文字の[**追加**]をクリックし、[VLAN名]と[VLAN ID]を入力後、[**追加**]**ボタン**をクリックします。
5. 設定を保存します。
6. [**構成**]>[Wi-Fi]>[SSID]>[SSID を追加]>[**ネットワーク**]タブをクリックします。
7. [VLAN]配下の[VLAN 名]ラジオボタンを選択し、設定した VLAN マッピングと同じ VLAN 名を入力します。
8. SSIDを保存して有効にします。

ロールプロファイルのVLAN名マッピング

ロールプロファイルの定義時に VLAN 名のマッピングを作成することもできます。

1. [**構成**]>[**ネットワークプロファイル**]>[**ロールプロファイル**]を選択します。
2. 設定したいロールプロファイルをクリックして開きます。
3. [**ロール固有の設定**]配下の[VLAN]にチェックを入れ、[VLAN 名]のラジオボタンをクリックし、VLAN 名を入力します。



5. [**フォールバックVLAN ID**]を入力します。
6. ロールプロファイルを保存します。

2.6.4.c VLANプール

通信に使用する VLAN をクライアント単位で分散することで、輻輳を軽減し、通信品質を向上できます。

2.6.5 SSIDアクセス制御

クライアントのアクセスを制限するMACアドレスフィルタやファイアウォール設定等を、SSIDごとに制御できます。設定をするには、SSIDのメニューから、「アクセス制御」を選択します。

2.6.5.a SSIDファイアウォールの設定

AIRRECT Cloudは以下のファイアウォール設定に対応しております。

●レイヤー3/4ファイアウォール

●アプリケーションファイアウォール

注意：[構成]>[Wi-Fi]>[SSID]>[セキュリティ]>[802.1x]で動的VLANが有効になっている場合、ファイアウォール設定を有効にすることはできません。

アクセスポイントのファイアウォールは、アクセスポイントを通過するトラフィックを監視し、ユーザー定義のルールに基づいてアクションを実行します。

ファイアウォールのルールはSSIDごとに定義および適用されます。複数のSSIDプロファイルがサポートされているアクセスポイントは、複数のファイアウォール構成をもつことができます。

以下は、ファイアウォール機能の一般的な使用例です。

●ゲストWi-Fiユーザーからのプライベート/企業サブネットへアクセスをブロックし、ゲストWi-Fiユーザーがパブリック・インターネットにのみアクセスを許可する。

●特定のドメイン名へのアクセスをブロック、または、許可する。

●ゲストWi-Fiユーザーがインターネットの HTTP、および、HTTPSコンテンツにのみアクセスできるようにする。これは通常、ゲストユーザーが生成できるトラフィックのタイプを制御するために行われます。

●DNSベースのコンテンツ・フィルタリングを実装して、不適切なWebサイト、セキュリティ上の脅威、および ピアツーピアのファイル共有へのアクセスを制限する。

●ワイヤレスクライアントにIPsec VPNの使用を強制する。

ファイアウォール利用の注意点：

●レイヤー3/4ファイアウォールのルールを有効にし、かつルールを定義しない場合、デフォルトルールが適用されます。（すべてのトラフィックがブロック）

●アクセスポイントは、最初の一致が見つかるまで、トラフィックのルールを上から下に比較します。最初の一致が見つかると、アクセスポイントは残りのルールを比較しません。定義されたどのルールとも一致しない場合、アクセスポイントは最後にデフォルトのルールを使用します。ドラッグアンドドロップでルールを並べ替え、目的のレベルに配置し直すことができます。

L3-4ファイアウォールのルールとアプリケーション・ファイアウォールのルールが競合する場合、『レイヤー3/4ファイアウォールとアプリケーション・ファイアウォールのデシジョンテーブル』に基づいて決定します。

以下のテーブルは、小売店で展開されるゲストSSIDにあるルールセット利用例です。
目的；HTTP/HTTPSインターネットアクセスのみを許可し、コンテンツ・フィルタリング有効、プライベートサブネットへのアクセスをさせない。

No	ルール名	IP/ホストネーム	ポート	アクション	プロトコル	方向
1	コンテンツフィルタリングDNS1	199.85.126.30	53	許可	UDP	発信
2	コンテンツフィルタリングDNS2	199.85.127.30	53	許可	UDP	発信
3	その他の全てのDNSを拒否	*	53	ブロック	UDP	発信
4	ローカルアクセスなし	192.168.0.0/16 172.17.0.0/21, 10.0.0.0/8		ブロック	Any	すべて
5	HTTP / HTTPSの許可	*	80, 443	許可	TCP	発信
6	デフォルト			ブロック		

ルール1 - アウトバウンドUDPポート53をコンテンツ・フィルタリングDNS1/199.85.126.30(Norton)に許可します。このルールは、DNSベースのコンテンツ・フィルタリングを実装して、子供向けではないコンテンツ（アダルト、ギャンブル、麻薬他）を含むWebサイトへのアクセスをブロックし、コンテンツを保護し、セキュリティ・リスクを低減します。DNSはUDPポート53を使用します。このルールは、199.85.126.30 のホスト/IPアドレスを持つコンテンツ・フィルタリングDNSサーバーのポート53宛ての発信UDP接続を許可します。ファイアウォールはステートフルなので、通信の復路は自動的に許可されるため、個別のルールは必要ありません。これは他のルールにも当てはまります。

ルール2 - コンテンツ・フィルタリングDNS2/199.85.127.30(Norton)への送信UDPポート53を許可します。ルール1と同様にコンテンツ・フィルタリングの内容です。このルールによって、DNSサーバーの冗長性が確保されます。

ルール3 - すべての送信UDP53をブロックします。このルールは、ルール1および2で許可されているものを除くすべてのDNSトラフィックをブロックします。ユーザーがコンテンツ・フィルタリングを回避するためにクライアントでDNSサーバーアドレスを静的に構成することを防止します。

ルール4 - プライベート/企業サブネットへのアクセス先である192.168.0.0/16、172.17.0.0/21、および10.0.0.0/8へのトラフィックをブロックします。このルールに指定されたプロトコルは[Any]であり、IPで伝送されるすべてのプロトコルをカバーします。プロトコルとして[Any]をクリックすると、ポート番号がグレー表示されます。ポートの概念が実装されていないプロトコル（ICMPなど）があるため、プロトコルとして「Any」を選択すると、ポート番号がグレーアウトされます。このルールは、ゲストWi-Fiのユーザーがプライベートサブネットにアクセスすることを制限するために最適です。

ルール5 - TCPポート80、443へのすべての送信トラフィックを許可します。クライアントがポート80,443へのTCP接続を許可します（HTTP/HTTPS接続を許可）。ワイルドカード文字（*）は「任意の」ホストを表します。

ルール6 - デフォルトのルールは [**ブロック**] に設定されています。つまり、ルール1～5で有効にされたものを除いて、他のすべての種類の通信は許可されません。

アプリケーション・ファイアウォール

アプリケーションレベルでファイアウォール・ルールを定義することができます。

ファイアウォール定義の注意点：

●アプリケーション・ファイアウォールのルールを有効にするには、アナリティクスタブで アプリケーションの可視性を有効に設定する必要があります。無効のまま設定しようとすると、アプリケーション・ファイアウォール設定画面からアプリケーションの可視性を有効に設定するように求められますので、[**アナリティクス**]タブに移動する必要はありません。

●アプリケーション・ファイアウォールのルールを有効にすると、デフォルトのルールアクションを確認できます。ルールを定義しない場合、デフォルトのルールが適用されます。（すべてのトラフィックがブロック）

●アクセスポイントは、最初の一致が見つかるまで、ルールを上から下にテストします。最初の一致が見つかると、アクセスポイントは残りのルールを参照しません。定義されたどのルールとも一致しない場合、アクセスポイントは最後にデフォルトのルールを使用します。ドラッグアンドドロップ機能を使用してルールを並べ替え、目的のレベルに配置し直すことができます。

レイヤー3/4ファイア・ウォールのルールとアプリケーション・ファイアウォールのルールが競合する場合、『レイヤー3/4ファイアウォールとアプリケーション・ファイアウォールのデシジョンテーブル』に基づいて決定します。

以下のテーブルは、企業の SSID で使用される SSID ルールの使用例です。
目的：FacebookやX（旧Twitter）をブロックしたい場合

ルール名	カテゴリ	アプリケーション名	アクション
FacebookとXを拒否する	ソーシャルネットワーキング	Facebook, Facebook Apps, Facebook Event, Facebook Messages, Facebook Post, Facebook Search, Facebook Video, Facebook Video Chat, X	ブロック
デフォルト			ブロック

レイヤー3/4ファイアウォールとアプリケーションファイアウォールのデシジョンテーブル

L3ファイアウォールアクション	アプリケーションファイアウォールアクション	最終アクション
拒否	Any	拒否
許可	拒否	拒否
許可	一致無し	許可
一致無し	拒否	拒否
一致無し	許可	許可
一致無し	一致無し	デフォルト
許可してマーク	許可してマーク	アプリケーションマークを許可
許可してマーク	許可	L3マークを許可
許可してマーク	一致無し	L3マークを許可
一致無し	許可してマーク	アプリケーションマークを許可
一致無し	一致無し	デフォルト

アプリケーションの優先度設定

任意のアプリケーションにおいて、[許可してマーク]を選択することで、そのアプリケーションの通信の優先度を DSCP で選択することができます。

例えば、Teamsのアプリケーションを優先にしたい場合は、以下のような設定をすることで、優先度の設定が出来ます。

この設定は、**[マーク方向]**にて、有線（アクセスポイントからスイッチポートへのアップストリーム）と無線（アクセスポイントからクライアントへのダウンストリーム）方向において、Teamsのトラフィックが**DSCP**値**56**としてタグ付けされ、音声送信キューを使用して送信されることになります。アクセスポイントの音声送信キューは最も優先度が高いため、他の送信キューのトラフィックよりも優先して送信されることで通信品質を担保します。

レイヤー3/4ファイアウォールとアプリケーションファイアウォールの両方について、以下の手順で設定することができます。

1. [**構成**]>[Wi-Fi]>[SSID]>[**アクセス制御**]の順にクリックします。
2. [**ファイアウォール**]をクリックすると、[**レイヤー3/4ファイアウォールのルール**]および[**アプリケーションファイアウォールのルール**]オプションが表示されます。
3. レイヤー3/4ファイアウォールを設定するには、[**レイヤー3/4ファイアウォールのルール**]を選択します。
   a) [+]記号をクリックして、ファイアウォールに新しいルールを追加します。
   b) ファイアウォール・ルールに関する以下の詳細を設定します。
      ●[**ルール名**]を入力します。
      ●ルールを適用する[IP/**ホスト名**]を入力します。
      ●[**ポート**]にルールを適用するポート番号を入力します。
      ●[**アクション**]でこのルールの下でパケットを[**許可**]、[**ブロック**]、または[**許可してマーク**]のいずれかの動作を選択します。
      ●[**プロトコル**]でルールを適用するプロトコルについて選択します。
      ●[**方向**]でルールを[**すべて**]の方向、[**着信**]（受信パケット）、または[**発信**]（送信パケ　ット）のいずれかに適用するかを選択します。
4. [**アプリケーションファイアウォールのルール**]をクリックして、アプリケーションファイアウォールを設定します。
   a）[+]をクリックして、ファイアウォールに新しいルールを追加します。
   b) ファイアウォールのルールに関する、以下の詳細を設定します。
      ●[**ルール名**]を入力します。
      ●[**カテゴリ**]をクリックし、ルールを適用するカテゴリを選択します。
      ●[**アクション**]でこのルールの下でパケットを[**許可**]、[**ブロック**]、または[**許可してマーク**]のいずれかの動作を選択します。
      [**レイヤー3/4ファイアウォールのルール**]と[**アプリケーションファイアウォールのルール**]との間で優先されるルールについては、『レイヤー3/4ファイアウォールとアプリケーションファイアウォールのデシジョンテーブル』を参照してください。
5. [**保存**]または[**SSIDを保存して有効にする**]をクリックします。
   新しいSSIDを追加する場合は、「SSIDが正常に追加されました。」というメッセージが表示されます。SSIDを更新する場合、「SSIDが正常に更新されました。」というメッセージが表示されます。

2.6.5.b クライアント認証

クライアント認証によって、ネットワークに別のセキュリティ層を追加します。SSIDの**[セキュリティ]タブ**で構成された、ユーザーを認証するメカニズム（WPA2-PSKなど）に加えて、クライアント (ユーザーデバイス）を認証します。クライアント認証は、**Google統合**、または、RADIUS MAC認証のいずれかを使用します。Google統合については、『Google統合設定』を参照してください。

また、クライアント承認が失敗した場合、ユーザーに対して **[切断]**または**[接続を維持]**を選択できます。

クライアント認証を設定するには、以下の手順を実行します。

1. **[構成]**>**[Wi-Fi]**>**[SSID]**から任意のSSIDを選択し、**[アクセス制御]**の順にクリックします。
2. **[クライアント認証]**をクリックします。**[Google統合]**または**[RADIUS MAC認証]**オプションが表示されます。
3. **[Google 統合]**または**[RADIUS MAC 認証]**を選択します。

   a) **[Google統合]**をクリックした場合は、クライアント認証が失敗した場合の処理を選択します。

   ●**[クライアント承認が失敗した場合]**：

   クライアントの接続を切断するには、**[切断]**を選択します。

   クライアントの接続を維持するには、**[接続を維持]**を選択し、**[ロールを選択]**から割り当てるロールを選択します。

   ロールを追加/編集する場合には**[追加/編集]**をクリックします。ロールプロファイルの設定の詳細は、『ロールプロファイルの構成』を参照してください。

   b) **[RADIUS MAC認証]**をクリックすると、**[RADIUS設定]**が表示されます。

   注意：802.1xはRADIUSベースのメカニズムであるため、**[SSIDセキュリティ]タブ**で802.1x認証をすでに設定している場合、**[RADIUS MAC認証]**は使用できません。

   クライアント認証のRADIUS設定項目は、以下の通りです。

   ●**[認証サーバー]**および**[アカウンティングサーバー]**として使用するプライマリおよびセカンダリRADIUSサーバー

   ●**[再試行パラメータ]**：アクセスポイントがRADIUSサーバーでの認証を試みる回数、および、タイムアウトを制御するパラメータ

   ●**[ユーザー名とパスワード]**：項目ごとにリスト内のMACアドレス形式から選択

   ●**[発信先ステーション/NAS ID]**：アクセスポイント、または、ネットワークアクセスサーバー (NAS) がRADIUSサーバーに送信するID

   注意：同じアクセスポイント上の異なるSSIDが同じNAS IDを使用することはできません。

●[**クライアント承認が失敗した場合**]：
クライアントの接続を切断するには、[**切断**]を選択します。
クライアントの接続を維持するには、[**接続を維持**]を選択し、割り当てるロールを選択します。ロールを追加/編集する場合には[**追加/編集**]をクリックします。画面右に**ロールプロファイル**を設定してクライアント認証を続行することができるウィンドウが表示されます。ロールプロファイルの設定の詳細は、『ロールプロファイルの構成』を参照してください。

4. [**保存**]または[**SSIDを保存して有効にする**]をクリックします。

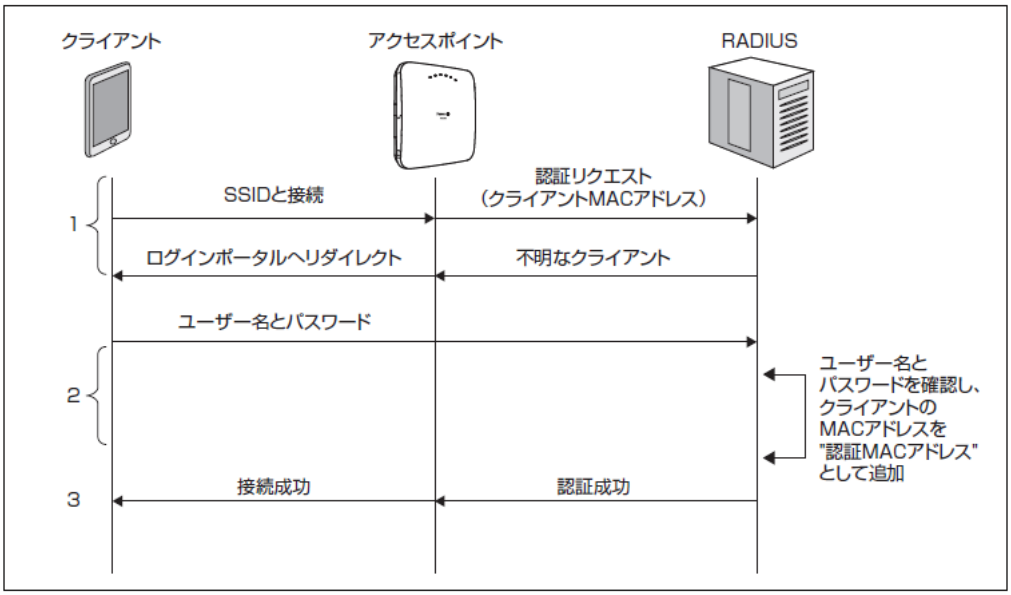
2.6.5.c ロールベースの制御

割り当てられたロールまたはユーザーが属するグループに基づいて、ネットワークリソースへのアクセスを制御することができます。通常、組織はRADIUSを使用してアクセス制御を実装します。
Google統合 または **RADIUS**ルールに基づいて、SSIDに接続するユーザーにロールプロファイルを割り当てることができます。
●Googleを使用してロールベースの制御を実装するには、Google統合を有効にする必要があります。
●RADIUSを使用してロールベースの制御を実装するには、802.1xを有効に設定する必要があります。
GoogleやRADIUSを設定するために[**SSIDアクセス制御**]**タブ**を離れる必要はありません。**ロールベースの制御**配下の[**設定の変更**]をクリックするだけで、設定が可能です。
AIRRECT Cloudでは、右ペインのウィンドウを開き、関連する設定を構成して保存し、ロールベースの制御を続行することができます。
また、複数のVSAルール(RADIUS）または Google OUルール（Google統合）を定義し、SSIDに接続するユーザーにこれらのルールに基づいてロールプロファイルを割り当てることができます。
RBACのルールタイプを定義する場合、Googleから返されるOUまたはRADIUS VSAから取得されるロールには、[**値の入力**]フィールドに入力された文字列が含まれている必要があります。例えば、[**値の入力**]フィールドの文字列が「/ * / Elementary School / * / Student」の場合、これはGoogle/VSAの「/ SJUSD / Elementary School / Almaden Elementary / Student」と一致する必要があります。

[**SSID**]タブの設定と[**ロールプロファイル**]タブの設定が異なる場合は『ロールプロファイル』の項目を参照してください。

一般的なRADIUS MAC認証フロー

AIRRECT CloudでRADIUS MAC認証を構成/設定して、認証の前後にクライアントにロールを割り当てることができます。RADIUS MAC認証を使用して、SSIDにアソシエーションされているクライアントを認証する場合の一般的なRADIUS MAC認証ワークフローについて、以下の図で示します。



1. クライアントがSSIDに接続すると、アクセスポイントはクライアントのMACアドレスを含む認証要求をRADIUSサーバーに送信します。
2. RADIUSサーバーは、クライアントのMACアドレスが不明であることをアクセスポイントに通知します。次に、アクセスポイントはクライアントをログインポータルにリダイレクトします。
3. ユーザー名とパスワードをポータルに入力します。RADIUSサーバーはこれらの資格情報を認証し、このユーザーに対してクライアントのMACアドレスを登録します。
4. RADIUSサーバーは、認証が成功したことをアクセスポイントに通知します。これでユーザーはネットワークに接続できます。通常、このクライアントによるその後のSSIDへの接続試行はシームレスです。RADIUSサーバーは対象のMACアドレスを認識しているので、クライアントはログインポータルにリダイレクトされません。

RADIUS MAC認証を使用したロールベースの制御は、以下のいずれかを使用してAIRRECT Cloudに実装できます。

●ロールプロファイル

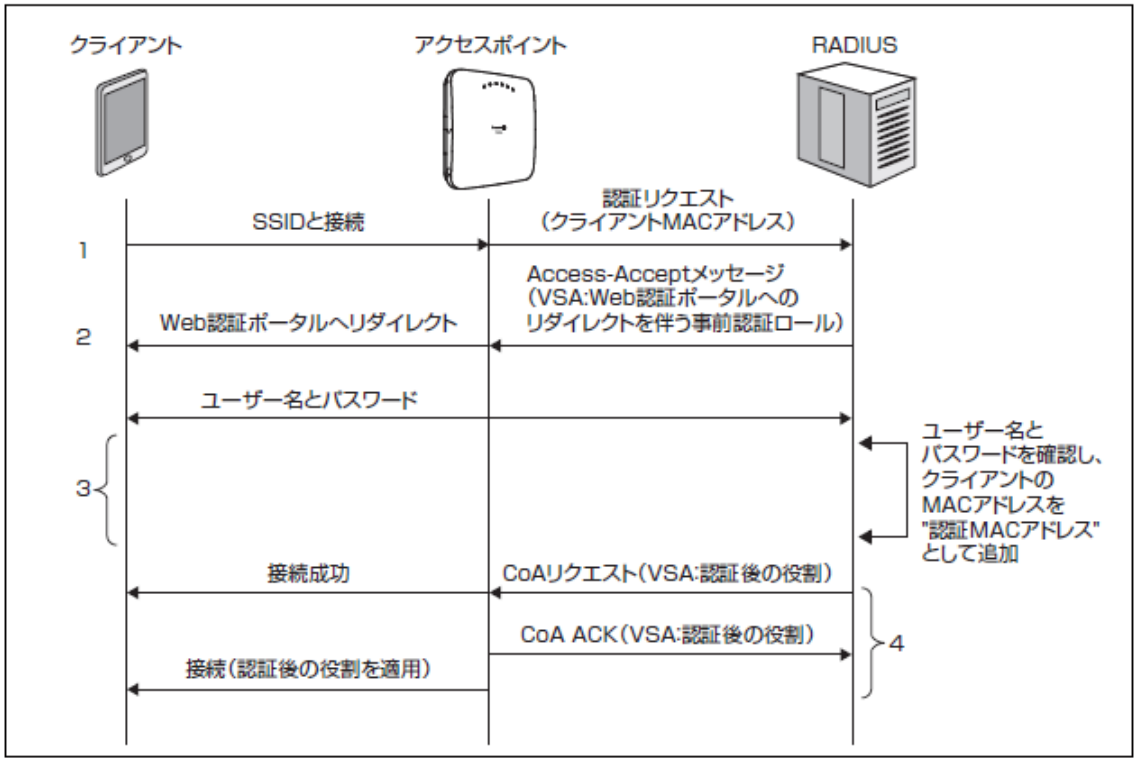
●AIRRCT Cloud上のキャプティブポータル

●サードパーティサーバー上のキャプティブポータル

AIRRECT Cloudは、Cisco ISEおよびAruba ClearPassとの統合もサポートしています。

ロールプロファイルを使用した実装

ロールプロファイルを使用して RADIUS MAC認証でロールベースの制御を実装するには、AIRRECT Cloudで2つのロールを定義する必要があります。**事前認証ロール**と**認証後のロール**です。ロールを使用したワークフローは、以下の図に示す通りです。



1. クライアントがSSIDに接続するとWi-Fiアクセスポイントはクライアントの MACアドレスを含む認証要求をRADIUSサーバーに送信します。
2. RADIUSサーバーは、事前認証の役割を含むAccess-Acceptメッセージで応答します。事前認証ロールは、クライアントを、RADIUSサーバーでホストされているWeb認証ポータルにリダイレクトします。
3. ユーザーはユーザー名とパスワードをポータルに入力します。RADIUSサーバーはこれらの資格情報を認証し、このユーザーに対してクライアントのMACアドレスを登録します。
4. RADIUSサーバーは、認証後の役割を含む**認証変更（CoA）**メッセージをアクセスポイントに送信します。
5. アクセスポイントはクライアントをネットワークに接続します。

RADIUS MAC認証を使用してロールを設定する

AIRRECT Cloudで2つのロールを定義し、ロールベースのMAC認証ワークフローを実行する方法については以下の手順で設定します。**[構成]>[ネットワークプロファイル]>[RADIUS]タブ**から、**[RADIUSサーバーを追加]**をクリックします。その後、以下の画面に RADIUSサーバーの詳細を入力します。

事前認証ロール：

[事前認証ロール]を使用すると、Web認証ポータルのURLにリダイレクトします。

注意：「承認前にアクセスできるWebサイト」リストに、Web認証ポータルのURLとポート80および443を追加する必要があります。

ロールプロファイルを使用した実装のワークフローの手順2）が実装され、クライアントがRADIUSサーバー認証ポータルにリダイレクトされます。アクセスポイントに送信する[Access-Accept]メッセージでこの役割を返すようにRADIUSサーバーを設定する必要があります。

認証後のロール：

認証後のロールプロファイルは、以下に示すように、正常に認証されたクライアントの接続設定 (例. VLAN、ファイアウォール・ルールなど）を定義します。アクセスポイントに送信する認証変更（CoA）メッセージでこのロールを返すようにRADIUSサーバーを構成する必要があります。

RADIUS MAC認証とロールベースの制御

RADIUS MAC認証は、セキュリティモードが[**オープン**]に設定されている場合にのみ使用できます。WPA2および混合モードでは、PSKを選択する必要があります。このオプションは、802.1xでは使用できません。

RADIUS MAC認証と**ロールベースの制御**を設定する手順は次のとおりです。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDを選択し、[**アクセス制御**]を選択します。
2. [**クライアント認証**]を選択し、[RADIUS MAC認証]を有効にし、[**クライアント承認が失敗した場合**]で[**切断**]を選択します。これにより、認証が失敗した場合にクライアントが切断されます。認証が成功すると、SSIDで定義されたロールが適用されます。
3. 次に、[RADIUS設定]で使用するRADIUSサーバーを選択します。
   [**発信先ステーションID**]を%m-%s（MACアドレスとSSID）に設定し、[NAS ID]を「%s」（SSIDのみ）に設定します。
4. 最後に、SSIDのロールベース制御を有効に設定し、以下のようにRADIUS VSAを経由して2つのロールを割り当てます。
   ※VSAとその値は、使用するRADIUSサーバーによって異なる場合があります。

ロールベースの制御を設定するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDを選択し、[**アクセス制御**]の順にクリックします。
2. [**ロールベースの制御**]をクリックします。
   a) [RADIUS VSA]を選択して、RADIUSサーバーのルールに基づいてロールを割り当てます。
   ●[**ルールのタイプ**]を選択します。[802.1X**の独自**VSA]を選択した場合は、[**ベンダーID**]と[**属性ID**]を入力します。[802.1X**のデフォルト**VSA]の場合、ベンダーはPanasonicで、ベンダーIDと属性IDは RADIUSサーバーで事前に定義されているため、これらの値をここに入力する必要はありません。
   ●[**オペランド**]でルールに使用する文字列パターンを選択します。
   ●[**値を入力**]フィールドに文字列パターンを入力します。
   ●[**ロールを割り当て**]で、このルールに割り当てるロールを選択します。
   割り当てるロールをまだ定義していない場合は、[**追加/編集**]をクリックします。
   画面右側にウィンドウが表示され、**ロールベースの制御**を定義できます。詳細については、『ロールプロファイルの構成』を参照してください。
   b) Google OUのルールに基づいてロールを割り当てるには、[Google OU]を選択します。
   ●[**ルールのタイプ**]は、Google OUで事前に設定されています。
   ●[**オペランド**]でルールに使用する文字列パターンを選択します。
   ●[**値を入力**]フィールドに文字列パターンを入力します。
   ●[**ロールを割り当て**]で、このルールに割り当てる役割を選択します。割り当てるロールをまだ定義していない場合は、[**追加/編集**]をクリックします。画面右側にウィンドウが表示され、**ロールベースの制御**を定義できます。詳細については、『ロールプロファイルの構成』を参照してください。
3. [**保存**]または[SSID**を保存して有効にする**]をクリックします。

2.6.5.d DHCPフィンガープリント・ベースのアクセス制御

DHCP フィンガープリント・ベースでは、アクセス制御を使用してクライアントの SSID 接続を[**許可**]または[**拒否**]することができます。アクセスポイントはクライアントと DHCP サーバー間の DHCP 交換パケットに基づいてクライアントの OS を識別します。DHCP はオプション 55 を使用してクライアント OS 情報（Macintosh、Windows など）をキャプチャ/交換し、特定の OS を搭載したクライアントのネットワーク接続を制限することができます。

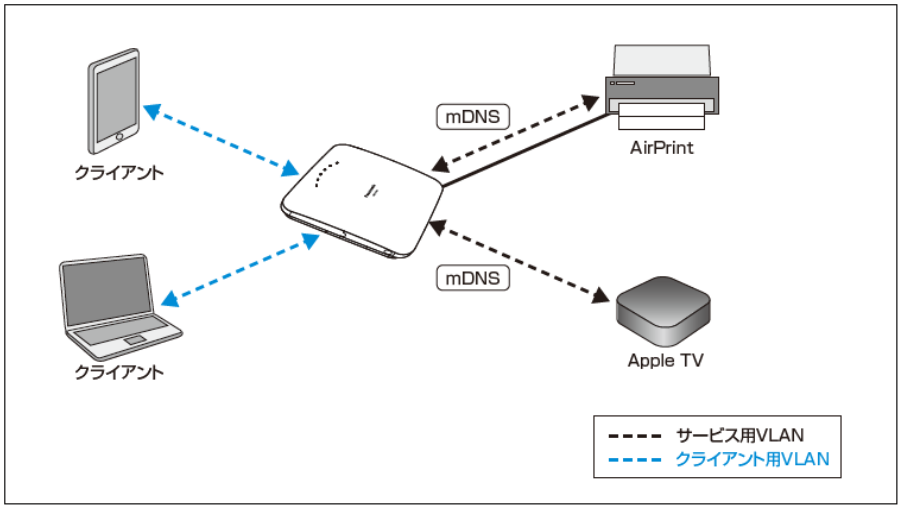
[**DHCP フィンガープリント・ベース**]のアクセス制御を行うには以下の手順を実行します。

1. [**構成**]>[WiFi]>[SSID]>[**SSID 追加**]をクリックします。
2. [**アクセス制御**]をクリックし、[**DHCP フィンガープリント・ベースのアクセス制御**]を有効にします。
3. 識別されたクライアントの場合には、デフォルトルールを指定します。
   注意：OS タイプは[Any]から変更はできません。
4. アクションを[**許可**]または[**拒否**]を選択します。デフォルトのルールは、識別されたすべてのクライアントに適用されます。

5. デフォルトのルールから[**許可**]または[**拒否**]するＯＳタイプを[⊕]を選択して追加します。複数の例外を追加できます。（OS タイプ：Android・iOS/iPadOS・Linux・macOS・Windows）
6. [**許可**]または[**拒否**]をクリックして設定を[**保存**]します。

2.6.5.e Bonjourゲートウェイの構成

ネットワーク上のAppleデバイスへのアクセスが可能にするBonjourゲートウェイ機能を有効に設定することができます。
Bonjourは、Appleによるゼロ構成ネットワーキングの実装です。マルチキャスト・ドメインネーム・システム(mDNS)を使用して、ローカル・ネットワーク上のBonjour対応デバイスによってアドバタイズされたデバイスとサービスを検出するために使用されます。
通常、Bonjourデバイスはローカル・ネットワークで実行され、Bonjourサービス・アドバタイズはネットワークの境界を越えません。それらは、単一VLAN/サブネットのブロードキャスト・ドメインに制限されています。異なるVLANに接続されているクライアントは、これらのサービスを検出できません。
クライアントがWLAN上でBonjour対応デバイスに接続する方法を理解するために、以下のVLANを例とします。
●Bonjour対応デバイスが展開されているサービスVLAN
●クライアントが展開されているクライアントVLAN



上図に示すように、Bonjourゲートウェイが有効でサービスVLANが構成されているSSIDにクライアントが接続すると、アクセスポイントはmDNSパケットをサービスVLANからクライアントVLAN（SSIDで構成されたVLAN ID）に転送します。その逆も同様です。
これでクライアントは、WLANで利用可能な Bonjourサービスを認識し接続できます。

Bonjourゲートウェイを設定するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDを選択し、[**アクセス制御**]の順にクリックします。
2. [**Bonjourゲートウェイ**]をクリックします。

注意：Bonjourゲートウェイは、SSIDのネットワークタイプが「ブリッジ」に設定されている場合にのみ設定できます。ネットワークがNATモードに設定されている場合、Bonjourゲートウェイは機能しません。ネットワークをNATモードに設定した場合、AIRRECT CloudはBonjourゲートウェイをグレー表示し、[**アクセス制御**]**タブ**内からネットワーク設定を変更するように求められます。

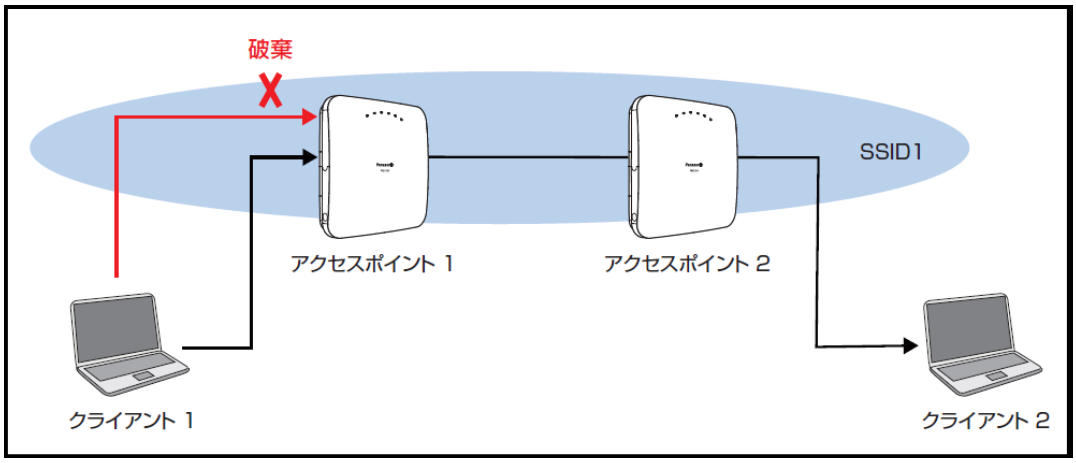
3. [**サービスVLAN**]を入力します。これらはBonjourデバイスのVLANです。アクセスポイントによって、サービスVLANからクライアントVLAN (SSIDで構成されたVLAN ID)にパケットが転送されます。またその逆も同様です。
4. [**保存**]または[**SSIDを保存して有効にする**]をクリックします。

2.6.5.f MACアドレスフィルタリング

SSIDごとにクライアントMACアドレスの許可リスト、または、拒否リストを定義することで、SSIDに接続できるデバイスを制御できます。1つSSIDに最大1024個のMACアドレスを登録することができます。
許可リストと拒否リストの定義は以下になります。
許可リスト：許可リストのクライアントのみがSSIDに接続できます。他のクライアントは接続できません。
拒否リスト：拒否リストのクライアントはSSIDに接続できません。他のすべてのクライアントは接続できます。
特定のSSIDに対して、許可リスト、または、拒否リストのいずれかを作成できますが、両方を作成することはできません。
MACアドレスは、CSVファイルから一括でインポート/エクスポートをすることができます。

2.6.5.g クライアント分離

SSIDでクライアント分離を有効にすると、SSIDにアソシエーションされたWi-Fiクライアントはゲートウェイとのみ通信できます。同じサブネット上の他のホスト（同じSSID上の他のクライアント、同じサブネット上の他のSSIDにアソシエーションされているクライアント、同じサブネット上の有線ネットワークに接続されているホストなど）と直接通信することはできません。クライアント分離を使用してSSIDを実行しているアクセスポイントは、宛先IPアドレスがクライアントと同じネットワーク上にある場合、ゲートウェイ宛てのパケットを除き、クライアントからのすべてのパケットを破棄します。
下図のように、SSID1上の異なるアクセスポイントにアソシエーションされた2つのWi-Fiクライアント、クライアント1とクライアント2について考えてみます。クライアント分離を有効にすると、AP1はクライアント1から発信され、クライアント2宛てのパケットを破棄します。



SSIDでNATが有効に設定されている場合でも、アクセスポイント自身がプライベートサブネットのゲートウェイノードになりますので、クライアント1やクライアント2がNAT処理されたSSIDにアソシエーションされているときは双方の通信はできません。ただし、クライアント分離とは通信を防止するメカニズムは異なります。NATは異なるアクセスポイント上のクライアント間の直接通信を防ぎ、クライアント分離は同じアクセスポイントのクライアント間の直接通信を防ぎます。

2.6.6 SSIDアナリティクス

[アナリティクス]タブから、アクセスポイントによって収集された分析情報をどこに保存するか設定ができます。保存場所は、AIRRECT Cloudまたはサードパーティのサーバーのどちらか選択できます。
[アソシエーション]をクリックした場合は、**[Wi-Fiユーザーがアクセスする**Webサイトの**URL（CSV としてダウンロード可能）]**フィールドが有効になり、こちらもクリックすることで**HTTPコンテンツ**分析ができます。
コンテンツ分析には以下の内容が含まれます。
●クライアントがアクセスするドメイン名
●ドメインに転送されたバイト単位のデータ
●ドメインから受信したバイト単位のデータ
AIRRECT Cloudは、データをCSV形式で保存、ダウンロードが可能です。

アプリケーションの可視性
アプリケーションの可視性は、アクセスポイントがこのSSIDについてレイヤー3以上のすべてのアプリケーションを監視する機能であり、ネットワーク上で最も利用されているアプリケーションがわかります。また、不要なアプリケーションや有害なアプリケーションの特定に役立ちます。これらのアプリケーションは、AIRRECT Cloudの**[モニター]タブ**で、クライアントごとまたはアプリケーションごとに表示できます。
また、分析をサードパーティのサーバーに送信することも選択できます。この場合、HTTPコンテンツを選択するときは、サーバーのユーザー名とパスワードを入力する必要があります。送信間隔は、データがサーバーに送信される頻度を決定します。また、分析の一部として送信するHTTPコンテンツを選択できます。 アクセスポイントは、HTTP Postメッセージの一部としてクライアントMACおよびRSSIデータを送信します。詳細については、『HTTPポストフォーマット』を参照してください。

HTTPポストフォーマット

Curlプログラムは、RSSI値をサーバーに送信するために使用されます。使用されるコマンド形式は以下の通りです。

curl <upload_URL>?sensor_mac=<sensor's MAC address>&timestamp=<time in seconds> -F
data=@"<file_on_airtight_device>"

POSTコマンドには2つの引数が含まれます。

●sensor_mac: The MAC address of the Panasonic device. Example 00:11:74:90:00:1F

●timestamp: The time in number of seconds from boot of the Panasonic device.

このPOSTコマンドの内容は、クライアントのRSSIデータを含むアップロードファイルです。ファイル名はrssi_dataです。ファイルの各行は、以下の形式です。

<client_mac>, <RSSI in dBm>, <time in seconds at which RSSI reading was taken>

SSID設定で収集する情報を選択する

アクセスポイントで収集した分析情報は、AIRRECT Cloudに保存する方法と、サードパーティサーバーに送信する方法があります。SSID設定で分析した情報を収集する設定における、必要なパラメータの詳細については、「アナリティクスパラメータ」を参照してください。

SSID設定で分析情報の設定を行うには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDを選択し[**アナリティクス**]タブに移動します。
2. 分析情報を保存するには、[**クラウドサーバーに分析結果を保存**]内の設定をします。
   a）アクセスポイントに接続されるクライアントに関する情報については、[**アソシエーション**]をクリックします。これを選択すると、[**Wi-Fiユーザーがアクセスする**Web**サイトのURL（CSV としてダウンロード可能）**]フィールドが有効になります。
   b）[**Wi-Fiユーザーがアクセスする**Web**サイトのURL（CSV としてダウンロード可能）**]をクリックして、アクセスポイントにアソシエーションされたクライアントがアクセスするインターネットドメインに関する情報をキャプチャします。
   c）[**アプリケーションの可視性**]を選択して、アプリケーションの可視性機能をオンにします。
   d）分析情報をダウンロードするには、［**レポート**］＞［**アナリティクス**］＞［**接続**］＞［**クライアント・アソシエーション**］で、分析情報をCSVファイルでダウンローケします。

3. [**分析結果をサードパーティーサーバーにプッシュ**]を選択し、以下の設定情報を構成します。
   a）[**サーバーURL**]に外部サーバーのサーバーURLを入力します。
   b）[**ユーザー名**]に外部サーバーにログインするためのユーザー名を入力します。
   c）[**パスワード**]に外部サーバーへのログイン用のユーザーパスワードを入力します。
   d）[**送信間隔**]にサーバーへの送信間隔を分単位で入力します。
4. [**HTTPコンテンツ**]で、[**要求本文の投稿**]や[**ユーザーエージェント**]などのサードパーティーサーバーと共有する情報を選択します。
5. [**保存**]をクリックします。

アナリティクスパラメータ

パラメータ	概要
クラウドサーバーにアナリティクスを保存	
アプリケーションの可視性	有効にした場合、アプリケーションの表示機能をオンにします。アプリケーションの可視性を有効にすると、このSSIDに接続したクライアントが使用したレイヤ3以上のすべてのアプリケーションが[**モニター**]>[**アプリケーションの可視性**]リストに表示されます。
アプリケーションQoE監視	アプリケーションのQoE監視機能をオンにします。 有効にすると、このSSIDに接続したクライアントが使用したTCPを使用したアプリケーションが[**ダッシュボード**]>[**アプリケーション**]>[**アプリケーションエクスペリエンス**]でQoEの状況を確認できます。 ※監視できるアプリケーションはIPv4のみです。IPv6は未サポートとなります。
アソシエーション	有効にした場合、 アクセスポイントと接続されたクライアントのアソシエートに関する以下のデータが収集されます。 収集されたデータは［**レポート**］＞［**アナリティクス**］＞［**接続**］＞［**クライアント・アソシエーション**］からCSVファイルとしてダウンロードできます。 ●クライアントのMACアドレス ※CSVファイルでは、この項目は暗号化されます。 ●プロトコル ※クライアント端末が利用した周波数帯を表示します。 ●クライアントが接続するネットワークのSSID ●クライアントの場所 ●アクセスポイントとのクライアントアソシエーションの開始時間 ●アクセスポイントとのクライアントアソシエーションの終了時間

	●セッション時間 ●クライアントデバイスからのバイト単位のデータ転送 ●クライアントデバイスへのバイト単位のデータ転送 ●Kbps単位のデータレート ●ローカルタイムゾーン ●ロケーションID ●アクセスされたドメイン ●ユーザー名

パラメータ	概要
クラウドサーバーにアナリティクスを保存	
Wi-Fiユーザーがアクセスする WebサイトのURL ※CSVとしてダウンロード可能	このチェックボックスは、アクセスポイントに接続されたクライアントがアクセスするインターネットドメインに関する情報をキャプチャします。 この情報は、アソシエート分析ファイルにあります。以下の情報は、コンテンツ分析情報として各インターネットドメインに存在します。 ●ドメイン名 ●ドメインに転送されたデータ（バイト単位） ●ドメインから受信したデータ（バイト単位）
パラメータ	概要
分析結果をサードパーティーサーバーにプッシュ	
サーバーURL	情報が保存される外部サーバーのURLを表します。
ユーザー名	外部サーバーにログインするためのユーザー名を表します。
パスワード	ユーザーが外部サーバーにログインするためのパスワードを表します。
送信間隔	HTTPコンテンツ分析JSONファイルを、外部サーバーに送信する際の、繰り返しの時間間隔（分単位）。値は[1-60]分から変更できます。初期値は10分です。
HTTPコンテンツ	アクセスポイントは、HTTPまたはHTTPSを介したクライアントから、この情報を格納できる外部サーバーへのクライアントHTTPコンテンツ分析または閲覧データの転送をサポートします。この機能が有効な場合、ユーザーは以下のオプションを設定する必要があります。
要求本文の投稿	チェックした場合、POSTメソッドのリクエスト本文がJSONファイルに含まれます。
ユーザーエージェント	チェックした場合、JSONファイルにユーザーエージェント(ブラウザ)が含まれます。

リファーラー	チェックした場合、JSONファイルにHTTPリファーラーが含まれます。

2.6.7 SSIDキャプティブポータル

キャプティブポータルは、ユーザーがSSIDにアクセスする際にスプラッシュページ上でユーザー登録等をすることでWi-Fiにアクセスを許可するシステムです。
キャプティブポータルは、アクセスポイント内、AIRRECT Cloud内、またはサードパーティのサーバー内に設定できます。

●アクセスポイント内のホストポータル：最もシンプルなケースで、クリックスルーのみ対応したスプラッシュページとなります。通常はユーザーに使用条件の同意を求めるのみで利用可能となります。また、スプラッシュページのコンポーネントを含む「.zip」ファイルであるスプラッシュページバンドルをアップロードすることで任意のデザインのページを作成できます。[**サンプルをダウンロード**]から、バンドル作成の参考用サンプルがダウンロードできます。
●クラウドホストキャプティブポータル：AIRRECT Cloud内に存在するポータルです。「プラグイン」と呼ばれる方法でユーザーを認証し、各認証方法のサービス品質の設定を定義し、複数の作業を実行できます。サービス品質の設定には、ログインとブラックアウトのタイムアウト、ダウンロードとアップロードの帯域幅制限が含まれます。
以下はユーザーがクラウドホストのキャプティブポータルにアクセスするためのプラグインです。

●**クリックスルー**：認証は不用であり、ユーザーがクリックするだけでWi-Fiに接続可能となるページ。利用規約の同意のみでログインできます。
●**ソーシャルメディアプラグイン**：SNSのログイン認証情報を使用して認証しネットワークにアクセスします。Facebook,X,LinkedIn,Okta,プラグインをサポートしています。
●**ユーザ名/パスワード**：この方法には以下2つの選択肢があります。

1. ユーザーの自己登録を許可
   自己登録は、無料のWi-Fiまたはホスト承認で行うことができます。ホスト承認は企業等で来訪者のWi-Fiアクセスを承認するときなどに利用できます。ホスト承認により、承認されたユーザーのみがWLANネットワークにアクセスできるようになります。
2. 管理者生成の資格情報
   AIRRECT Cloud内で管理しているプライベートゲストブック方式です。ゲストユーザーが定義したゲストユーザーアカウントの資格情報を使用して、Wi-Fiにアクセスできるようにします。

●**SMS経由のパスコード**：ユーザーは、SMS経由で認証コードを受け取るために、携帯電話番号を通知します。ユーザーはコードを使用してWi-Fi認証とネットワークアクセスを行います。ここでは、パスコードの最大長やSMSが再送信される最大回数などを定義できます。

●**外部RADIUS**：外部RADIUSサーバーを経由して認証が行われます。設定済みのRADIUSサーバーを選択するか、[**追加/編集**]オプションを使用して新しいサーバーを追加します。

注意：RADIUSプラグインを他のプラグインと共に使用することはできません。RADIUSプラグインを有効にした場合、他のプラグインが自動的に無効になります。

●**共通設定**：プラグインとは別に、Wi-Fiユーザーとの通信時に使用されるEメール、SMSなどの共通設定を構成できます。共通設定については、SSIDキャプティブポータル内のプラグイン全体だけでなく、SSID全体、および、ロケーション全体にも適用できます。新しいロケーションのSSIDを作成した場合も、共通設定がそのロケーションにも適用されます。キャプティブポータルでプラグインの組み合わせを使用することが可能です。例えば、ソーシャルメディアのプラグインを設定したとします。しかし、ソーシャルメディアアカウントを持っていない、またはソーシャルメディアアカウントの認証情報を使用したくないゲストにもWi-Fiアクセスを提供したい場合は、ポータルページにリンクを設けて、当該ゲストが特定の利用規約に同意するだけでWi-Fiにアクセスできるようにすることができます。

注意：利用規約はお客様が定義するものであり、当社が保証するものではありません。

●サードパーティホストにより、キャプティブポータルとして外部サーバーを利用できます。利用するには、ポータルをホストする「サーバーのスプラッシュページURL」と「共有シークレット」を入力する必要があります。また、RADIUS認証を有効にして、802.1x設定を入力することができます。詳細については、『RADIUS』のセクションを参照してください。サードパーティホストでは、ポータルがチャレンジ/レスポンスベースのユーザー認証に使用するリクエストとレスポンスの属性など、拡張ポータルパラメータを設定する必要があります。

アクセスポイントホスト型、クラウドホスト型、およびサードパーティホスト型のポータルに適用されるいくつかの一般的なフィールドがあります。例えば、ログイン前にユーザーがアクセスできるWebサイトや、ユーザーがログイン後にリダイレクトされるURLなどのログイン後のフィールド、およびログイン時間とブラックアウト時間を定義できます。サードパーティがホストするポータルの場合、ユーザーのログイン後のサービス識別子を定義できます。

キャプティブポータルのウォールドガーデンサイト

スプラッシュページのユーザーエクスペリエンスを向上させるためには、[**ウォールドガーデン**]リストに以下のサイトの追加を推奨します。ウォールドガーデンは認証が完了するまでに、ユーザーがアクセスできるネットワークの宛先を定義します。

●akamaihd.net
●googleapis.com
●gstatic.com
●google.co.jp

コンテンツに基づくサイト

スプラッシュページで使用されているコンテンツタイプに基づき、ウォールドガーデンに追加します。例えば、スプラッシュページにYouTubeを埋め込む場合、以下のウォールガーデンエントリーを推奨します。

●youtube.com
●googleusercontent.com (サムネイル用)
●lh5.googleusercontent.com (サムネイル用)

2.6.7.a キャプティブポータルの基本構成

アクセスポイント ホストキャプティブポータルの構成

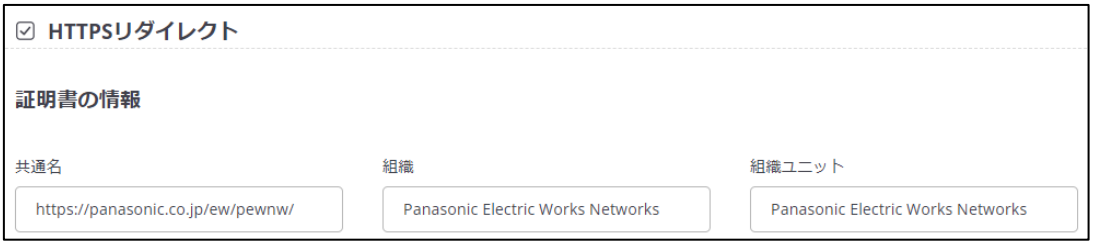
ホスト型キャプティブポータル設定を構成するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDを選択し、[**キャプティブポータル**]の順に移動します。
2. [**キャプティブポータル**]チェックボックスをオンにして、ゲストネットワークの使用時にクライアントに表示されるポータルページを表示します。
3. [**キャプティブポータル**]チェックボックスの下のプルダウンから、[**APホスト**]を選択します。

4. [**サンプルをダウンロード**]をクリックして、デフォルトのポータルバンドルファイルを

ダウンロードします。ポータルバンドルファイルをテンプレートとして使用して、カスタムポータルバンドルを作成できます。

5. [**カスタムスプラッシュページバンドルのアップロード**]をクリックして、バンドルをアップロードします。ポータルが正しく機能するには、zipファイルが以下の要件を満たしている必要があります。
   a) zipファイルには、ルートレベルに 「index.html」 という名前のファイルが必要です。これはメインのポータルページであり、index.htmlファイルによって参照される他のファイル、および、フォルダをルートレベルで持つことができます。
   b) バンドル内のファイルの解凍された合計サイズは、100KB未満である必要があります。大きな画像やその他のコンテンツをページに表示したい場合、index.htmlファイルからの参照を使用して、外部Webサーバーに配置できます。この場合、外部WebサーバーのIPアドレスが免除ホストのリストに含まれている必要があります。（以下を参照）
   c) ポータルが正しく機能するには、index.htmlファイルに、以下のHTMLタグが含まれている必要があります。
   ●開始タグを持つフォーム要素：<form method = "POST" action = "$ action">
   ●上記のフォーム要素内の 「mode_login」 という文字列
   例：<input type = "image" name = "mode_login" src = "images / login.gif">
   タグ：上記のフォーム要素内の<input type = "hidden" name = "redirect" value = "$ redirect">
6. [**HTTPSリダイレクト**]を有効にすると、Wi-FiクライアントのHTTPS通信時にもスプラッシュページへのリダイレクトが可能となります。この機能の利用には証明書が必要となります。以下の情報からアクセスポイントが証明書を生成します。
   ●[**共通名**]　　：FQDN
   ●[**組織**]　　：組織名
   ●[**組織ユニット**]：組織単位名



7. [**ユーザーがログイン前にアクセスできるWebサイト。**]リストを入力します。

8. [**ログイン後**]の設定で、以下のフィールドに詳細を入力します。

a) [**リダイレクトURL**]を指定します。
ユーザーがポータルページの送信ボタンをクリックすると、ブラウザはこのURLにリダイレクトされます。空のままにすると、ポータルページが表示されたブラウザからアクセスされた元のURLにブラウザがリダイレクトされます。

b) [**ログインタイムアウト**]を指定します。ユーザーがポータルページのログイン後にゲストネットワークにアクセスできる時間を定義します。タイムアウト後、ゲストネットワークへのアクセスが停止され、ポータルページが再び表示されます。ユーザーは、ゲストネットワークへのアクセスを回復するために、ポータルページから再度ログインする必要があります。ユーザーがセッション・タイムアウトする前に接続を切断してゲストネットワークに再接続した場合、スプラッシュページで資格情報を入力する必要はありません。

c) [**ブラックアウト時間**]を指定します。これは、前のセッションがタイムアウトした後、ユーザーがログインを許可されない時間です。例えば、セッション・タイムアウトが1時間で、ブラックアウト時間が30分である場合、ユーザーはログイン成功後1時間でタイムアウトし、その後ユーザーは30分間再ログインできなくなります。30分が経過すると、ユーザーは再度ログインできます。

d) SSID接続時のゲストユーザーに対し、APがインターネット接続障害が発生していることを伝えるポップを表示する場合には、[**インターネット接続のダウンを検出してゲストユーザーに知らせる**]をクリックします。既にSSID済みのゲストユーザーに対しては通知されません。

9. [**保存**]または、[**SSIDを保存して有効にする**]をクリックします。

クラウドホスト型キャプティブポータルの構成

[SSID]>[**キャプティブポータル**]**タブ**に最初にアクセスしたときのデフォルト設定です。このオプションでは、キャプティブポータルはAIRRECT Cloudでホストされます。[**クラウドホスト型キャプティブポータル**]を設定するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDを選択し、[**キャプティブポータル**]の順にクリックします。
2. [**キャプティブポータル**]を選択します。[**クラウドホスト**]は、デフォルトで選択されています。

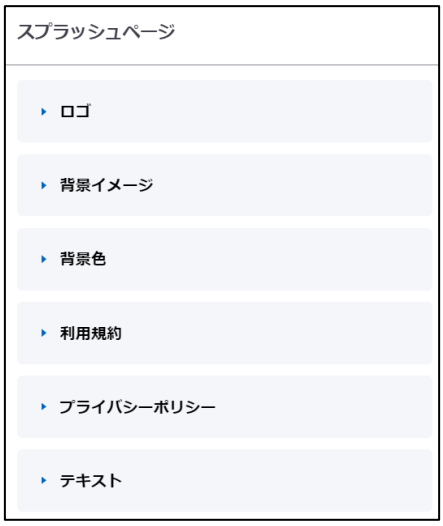
3. [**スプラッシュページ**]をデザインします。詳細については、『スプラッシュページのデザイン』を参照してください。
4. 使用するプラグインを設定します。デフォルトのプラグインは、「クリックスルー」です。プラグインの詳細は 『プラグインを構成する』を参照してください。
5. [**スプラッシュページをスキップ**]を有効にすると、スプラッシュページでの初回認証情報が記録され、その後、[**アプリケーション使用時間**] で設定した期間内（最大90日間）はスプラッシュページを表示させません。クリックスルー、RADIUSを除くプラグイン方法に適用される機能となります。
6. スプラッシュページからのサインイン時に、ログインセッションの残り時間の確認、及びサインアウトが可能となるポップを表示する場合は、[**サイン・アウトのポップアップ**]を設定します。本機能の利用は、ブラウザのポップアップブロックを無効にする必要があります。

7. [**HTTPSリダイレクト**]を有効にすると、Wi-FiクライアントのHTTPS通信時にもスプラッシュページへのリダイレクトが可能となります。この機能の利用には証明書が必要となります。以下の情報からAPは証明書を生成します。
   ●[**共通名**]　　：FQDN
   ●[**組織**]　　：組織名
   ●[**組織ユニット**]：組織単位名
8. [**ユーザーがログイン前にアクセスできるWebサイト。**]リストを入力します。
   これは、ユーザーがログインする前にアクセスを許可するサイトのウォールドガーデンです。キャプティブポータルページに動画などを埋め込みたい場合、ウォールドガーデンに追加する必要があります。詳細は、『キャプティブポータルのウォールドガーデンサイト』を参照してください。
9. [**ログイン後**]の以下のパラメータを設定します。
   ●[**リダイレクトURL**]：ユーザーをリダイレクトするURLを表します。
   ●[**ログインタイムアウト**]：ユーザーログインが切断される有効期限を表します。
   ●[**ブラックアウト時間**]：ユーザーログインがタイムアウトした後に、ユーザーがポータルに再ログインできない期間です。
   ●SSID接続時のゲストユーザーに対し、APがインターネット接続障害が発生していることを伝えるポップを表示する場合には、[**インターネット接続のダウンを検出してゲストユーザーに知らせる**]をクリックします。既にSSID済みのゲストユーザーに対しては通知されません。
10. [**保存**]をクリックしてSSIDを保存するか、[**SSIDを保存して有効にする**]をクリックして保存し、オンに設定します。

2.6.7.b スプラッシュページのデザイン

クラウドでホストされるキャプティブポータルにはデフォルトのスプラッシュページが表示されていますが、スプラッシュページは以下の手順で編集することができます。

1. [SSID]>[**キャプティブポータル**]>[**クラウドホスト**]を選択する。
2. [**スプラッシュページ**]セクションの編集アイコンをクリックします。画面右側にスプラッシュページの編集画面が開きます。



3. [**ロゴ**]を展開して、スプラッシュページにロゴを追加します。
   a) [**ロゴイメージのアップロード**]をクリックし、アップロードするロゴ画像を選択します。
   b) 画像配下のスライダーを利用すると、ロゴの大きさを調整できます。
4. [**背景イメージ**]オプションを展開して、背景画像をスプラッシュページに追加します。
   [**イメージをアップロード**]をクリックすると、アップロードする背景画像を選択できます。
5. [**背景色**]オプションを展開します。
   a）カラーバーから背景色と、選択した色の濃淡を選択します。
   b）カラーペインの下のスライダーを使用して透明性のレベルを設定します。
   スライダーの下のRGBA値は、選択した色、色合い、透明度レベルに対応しています。RGBAは、赤、緑、青、アルファを表し、アルファは透明度パラメータです。
   (0:完全に透明、1:完全に不透明)
6. [**利用規約**]オプションを展開すると、利用規約を定義できます。
   a) [**利用規約**]のタイトルを入力します。
   b) [**利用規約**]の本文を入力します。
7. [**プライバシーポリシー**]オプションを展開します。
   a) [**プライバシーポリシー**]のタイトルを入力します。
   b) [**プライバシーポリシー**]の本文を入力します。
8. [**テキスト**]オプションを展開します。

a) プラグインのタイトルを入力します。文章の見出し、または、ウエルカムメッセージ等を記載します。

b) 著作権に関する文章を入力します。

注意：文字数によってはスプラッシュページ画面が崩れてしまう可能性があります。設定後、プレビューより表示画面をご確認ください。

9. [**保存**]をクリックすると、スプラッシュページのプレビューが表示されます。設計したスプラッシュページが [SSID]>[**キャプティブポータル**]**タブ**に表示されます。

2.6.7.c プラグインの共通設定を構成する

共通設定はシステム全体に適用されます。SSIDキャプティブポータル内のプラグインだけでなく、SSIDやロケーション全体にも適用できます。共通設定にはWi-Fiユーザーとの通信に使用されるメール、SMSの設定が含まれます。共通設定は、以下のタスクで構成されています。

●Eメールアカウント設定の構成

●SMS/MMSアカウント設定の構成

共通設定を構成するには、[SSID]>[**キャプティブポータル**]で[**クラウドホスト**]を選択し、[認証プラグインとサービス品質(QoS)]の右上のギアアイコンをクリックすることで設定が出来ます。

Eメールアカウント設定の構成

Wi-Fiユーザーとの通信に使用されるメールアカウントの設定を共通設定から行います。

Eメールアカウントを設定するには、以下の手順を実行します。

1. [**共通設定**]ウィンドウから、メールアカウントのアイコンをクリックするとメールアカウント設定が表示されます。

2. [**メールサービスのタイプ**]をクリックします。

●[**システムメール**]を選択する場合：

- [**差出人のメールID**]と[**差出人の名前**]を入力します。これらは、ユーザーが受信する際の差出人名に表示されます。
- [**返信用のメールID**]を入力します。[**確認**]をクリックすると、**返信用IDでユーザーがメッセージを受信できるか確認できます。**

●[**SMTP設定**]を選択する場合：

- [**差出人のメールID**]と[**差出人の名前**]を入力します。 これらは、ユーザーが受信する際の差出人名に表示されます。
- [**返信用のメールID**]を入力します。
- [**サーバーホスト**]にSMTPサーバーのホストネーム、またはIPアドレスを入力します。
- [**サーバーポート**]にSMTPサーバーのサーバーポート番号を入力します。
- [**ログイン方法**]にSMTPサーバーのログイン方法をクリックします。
- [**ログインユーザー名**]と[**ログインパスワード**]にSMTPサーバーの**ログインユーザー名**と**ログインパスワード**を入力します。
- [**接続セキュリティ**]でSMTPサーバーへの接続セキュリティの種類を選択します。

3. [**テストアカウント**]を入力し、[**テストメールの送信**]をクリックすると、設定が正しく機能するか確認できます。入力したアカウントに設定したパラメータを含むテスト用のEメールが送信されます。
4. 最後に[**保存**]をクリックすると、設定が保存されます。

SMS/MMSアカウント設定の構成

Wi-Fiユーザーとの通信に使用される SMS/MMSアカウントを共通設定から設定します。SMS/MMSアカウントを設定するには、以下の手順を実行します。

1. [**共通設定**]ウィンドウから、メールアカウントのアイコンをクリックするとSMS/MMSアカウント設定が表示されます。

2. [**アカウント**]オプションで、既存のアカウントをクリックするか、[**新規追加**]をクリックして新規のアカウントを追加します。
3. [**名前を入力**]にアカウント名を入力します。

4. [**サービスプロバイダー**]をクリックします。
   Twilio、Msg91、またはカスタムを選択します。構成は選択内容によって異なります。
   ●[Twilio]を選択した場合、[**アカウントSID**]、[**認証トークン**]、[**Twilio番号**]を入力します。
   ●[Msg91]を選択した場合、[**ユーザー名**]、[**パスワード**]、[**差出人のID**]を入力し、[**SMSルート**]を選択します。
   [**カスタム**]を選択した場合、[**サービスURL**]を入力します。
7. [**テストアカウント番号**]と[**テストSMS設定**]を入力して、構成が機能することを確認できます。すべてを正しく設定すると、入力した番号にテストSMSが送信されます。
8. [**保存**]をクリックして構成を保存します。

2.6.7.d プラグインを構成する

クリックスループラグインの構成

クリックスループラグインは認証がありません。ユーザーはクリックするだけ、または利用規約に同意するだけでWi-Fiにアクセスできます。

プラグインを構成するには、[SSID]>[**キャプティブポータル**]で[**クラウドホスト**]をクリックします。プラグインを設定するには、以下の手順を実行します。

1. [**ゲストWi-Fiユーザーのログイン方法を選択**]をクリックすると、[**プラグインとQoS**]ウィンドウが画面右側のパネルに表示されます。
2. [**クリックスルー**]をクリックし、編集アイコンをクリックします。

3. 共通プラグイン設定の[**サービス品質**(QoS)]の各項目、および、[**リダイレクトURL**]を設定します。
4. [**保存**]をクリックすると、[**プラグインとQoS**]ページに戻ります。
5. [**プラグインとQoS**]ページで、[**保存**]をクリックすると、[**クリックスルー**]**設定**が保存されます。
6. SSIDを保存します。

ソーシャルメディア(SNS)プラグインを設定する

ゲストユーザーがアクセスポイントを経由してWi-Fiにアクセスしようとすると、キャプティブポータルページが表示されますが、その際にSNSアカウントで認証するためのオプションを提供します。ゲストユーザーが認証するSNSを選択すると、SNSアカウント認証情報のログインページにリダイレクトし、情報の一部をSNSアプリと共有する許可を求められます。Facebook, Xのアカウントでのログインでは、ログインをするために、ユーザーがSNSのページを「いいね」または「フォロー」するように要求させることもできます。キャプティブポータルから設定できるソーシャルメディアプラグインはFacebook、LinkedIn、Xの3種類です。ソーシャルメディアプラグインを行うには、事前にAIRRECT Cloudと連携を行うためのID,パスワードをソーシャルサイトで入手する必要があります。本マニュアルでは、『Facebookプラグインの構成』を例として詳細に記載します。

Facebookプラグインの構成

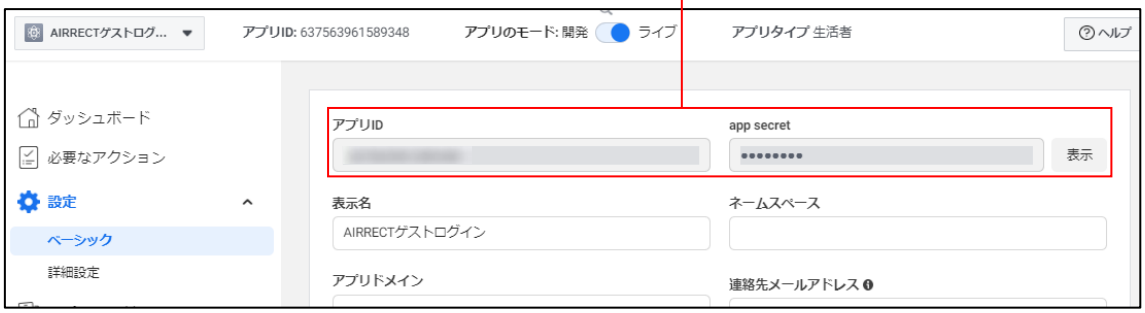
Facebookプラグインを構成するには、FacebookのApp IDとアプリシークレットを、Mata社のDeveloper Page(https://developers.facebook.com/)にて事前に設定、入手する必要があります。また、Facebookアプリケーションの詳細ページのリダイレクトURLには、以下のURLを設定します。

●https://agm17001.panasonic.cloudwifi.com/plugin/facebook/auth

また、AIRRECT Cloud との連携は「アクセス許可と機能」の[public_profile]のアクセスレベルを[Advanced Access]にリクエストする必要がありますのでご注意ください。

1. [構成]>[Wi-Fi]>[SSID]>[キャプティブポータル]>[プラグインとサービス品質(QoS)]>[ソーシャル]の順に移動します。
2. [Facebook]を有効にし、アイコンをクリックします。

3. [App ID]にFacebook APIと通信するためにFacebookから提供されたApp IDを入力します。



4. [App Secret]にゲストマネージャーがFacebookアプリへの接続に使用するアプリシークレットを入力します。
5. ゲストがFacebookアカウントの認証情報を使用して認証するときに、Facebookページを高く評価する必要がある場合は、[**いいねページの表示**]を選択します。選択すると[**いいねページのURL**]の入力欄が表示されます。
6. ゲストユーザーに、[**メールアドレス**]、[**誕生日**]、[**いいね**]、[**場所**]などの追加情報へのアクセス許可を求める場合は、[**拡張プロファイルの許可**]を選択します。ユーザーはユーザープロファイルから選択した情報にアクセスする許可を求められます。
7. 最後に、[**保存**]をクリックします。

設定後、スプラッシュページのプレビュー画面からサイインイン画面を確認できます。

Xプラグインの構成

キャプティブポータルでXプラグインを構成できます。Xプラグインを構成する前に、『Facebookプラグインの構成』と同様に、X社のDeveloper Page（https://developer.x.com）でアプリを作成し、そのConsumer KeyとConsumer Secretの入手が必要となります。その際のリダイレクトURIには、以下を設定します。

●https://agm17001.panasonic.cloudwifi.com/plugin/twitter/auth

プラグインを構成するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]>[**キャプティブポータル**]>[**プラグインとサービス品質(QoS)**]>[**ソーシャル**]の順に移動します。
2. [X]を有効化し、クリックします。

3. X APIと通信するためにX社から提供された[**カスタマーキー**]と[**カスタマーの秘密**]を入力します。
4. ゲストがXアカウントの資格情報を使用して認証するときにXでフォローをする必要がある場合は、[**フォローページの表示**]を選択します。すると、[**フォローページのURL**]を入力するテキストボックスが有効になります。
5. ゲストに表示されるXページのURLを[**フォローページのURL**]に入力します。
6. [**保存**]をクリックして設定を保存します。

LinkedInプラグインの構成

LinkedInプラグインを構成できます。LinkedInプラグインを構成するには、管理者ロールが必要です。LinkedInプラグインを構成する前に、ソーシャルメディアでアプリケーション/プロジェクトを作成したことを確認する必要があります。LinkedInプラグインを構成するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]>[**キャプティブポータル**]>[**プラグインとサービス品質**(QoS)]>[**ソーシャル**]の順に移動します。
2. [LinkedIn]を有効化し、クリックします。

3. [App ID]にLinkedIn APIと通信するためにLinkedInから提供されたApp IDを入力します。
4. [Secret Key]にゲストマネージャーがLinkedInへの接続に使用するシークレットキーを入力します。
5. ゲストがLinkedInアカウントの資格情報を使用して認証する際に、LinkedInでフォローする必要がある場合は、[**フォローページの表示**]を選択します。選択すると、[**フォローページのURL**]が表示されるので、ゲストに表示するフォローページのURLを入力します。
6. ゲストユーザーに許可を求める場合は、[**拡張プロファイルの許可**]、[**メールアドレス**]を選択します。選択した場合、ユーザーは、ユーザープロファイルから上記の情報にアクセスするためのアクセス許可を求められます。
7. [**保存**]をクリックして設定を保存します。

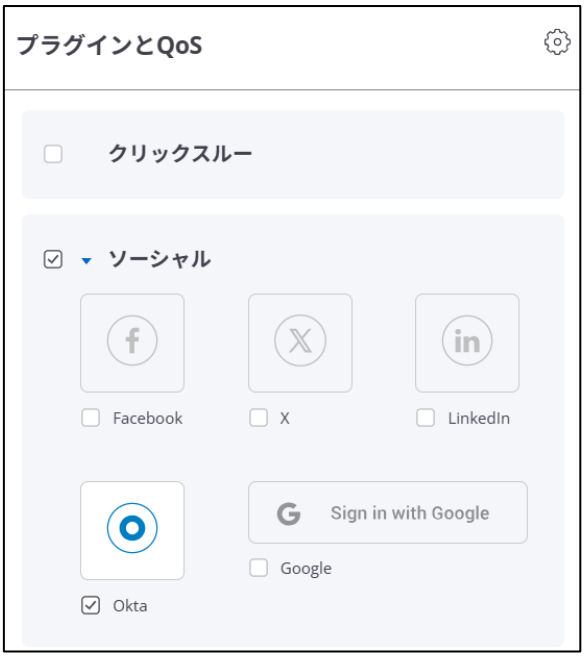
Oktaプラグインの構成

キャプティブポータルでは、ゲストユーザーが利用するSNSの他に、シングルサインオンなどで利用されるOkta社のプラグインを構成できます。Oktaプラグインを構成する前に、管理者によりOkta社の開発者向けプラットフォームにて、アプリケーションを作成し、クライアントID、クライアントキー、組織ドメインの入手が必要となります。

注意：Oktaログインページは、Apple CNAブラウザをサポートしておりません。そのため、ウォールガーデンにて特定のドメインを許可することでApple CNAブラウザで自動リダイレクトが発生しないよう設計されております。Appleユーザーは通常のブラウザアプリケーションでのHTTPリクエストを契機にOktaログインページへリダイレクトされます。

プラグインを構成するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]>[**キャプティブポータル**]>[**プラグインとサービス品質(QoS)**]>[**ソーシャル**]の順に移動します。
2. [Okta]を有効化し、クリックします。



3. Okta開発者ポータルサイトにて事前設定した[Client ID]、[Client Secret]、[**組織ドメイン**]を入力します。
4. [**保存**]をクリックして設定を保存します。

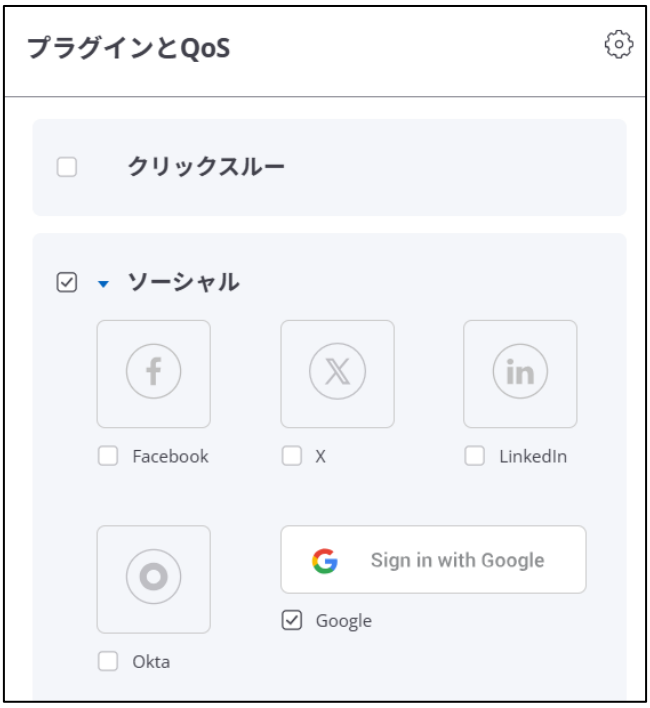
Okta の設定手順に関しては、当社ホームページの「設定例」からご確認いただけます。
https://panasonic.co.jp/ew/pewnw/support/wlan/setting.html

Googleプラグインの構成

キャプティブポータルでは、Googleアカウントを利用して「Sign in with Google™」プラグインを構成できます。
AIRRECTでGoogleプラグインを構成する前に、 Google Cloudサービスから、クライアント ID、クライアントキー、APIキーを入手しておく必要があります。

プラグインを構成するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]>[**キャプティブポータル**]>[**プラグインとサービス品質(QoS)**]>[**ソーシャル**]の順に移動します。
2. [Google]を有効化し、[Sign in with Google]をクリックします。



3. Google Cloudで事前に設定した[Client ID]、[Client Secret]、[APIキー]を入力します。
4. [**保存**]をクリックして設定を保存します。

ユーザー名/パスワードプラグインの設定

ユーザー名/パスワードプラグインを使用すると、ユーザーが自分でアクセスのための情報を登録や、ゲストブック（管理者が生成した資格情報）を利用することができます。プラグインを構成するには、[SSID]>[**キャプティブポータル**]で[**クラウドホスト**]を選択します。

ユーザー名/パスワードプラグインを構成するには、以下の手順を実行します。

1. [SSID]>[**キャプティブポータル**]**タブ**で、[**ゲストWi-Fiユーザーのログイン方法を選択**]をクリックすると、[**プラグインとQoS**]ウィンドウが画面右側に表示されます。
2. ユーザーに自己登録を許可するには、[**ユーザー名/パスワード**]>[**ユーザーの自己登録を許可**]を選択します。

3. 自己登録に使用するオプションを選択します。

●無料のWi-Fiアクセスを許可：ユーザーに無料のWi-Fiアクセスを許可する場合には、[**無料のWi-Fi**]を選択します。以下の項目が選択できます。

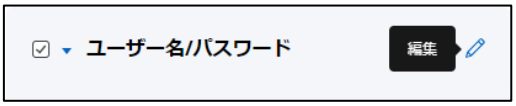
- [**自己登録のゲストユーザーにパスワードの設定を許可**]
  自己登録で設定したEメール宛てにワンタイムパスワード（OTP）を送付します。
- [**パスワードを忘れた場合のリンクを有効にする**]
- [**ゲストユーザーに期限切れアカウントのアクティブ化を許可**]
- [**自己登録のゲストユーザーに自動ログインを許可**]
  ゲストユーザーはEメールアドレスを入力するだけでインターネットにログインすることが出来ます。
- [**自己登録のゲストユーザーにWebページで資格情報を表示**]
  自己登録で設定したEメール宛てにパスワード等の接続に関するメッセージを送付します。メッセージの内容は、編集アイコンより設定ができます。

●ホスト承認：ユーザーがホストの承認を要求するメールをリクエストするには、[**ホスト承認**]を選択します。 [**ホスト承認**]アイコンをクリックして、ホスト承認設定を構成します。

- [**ゲストアクセスの承認要求を受信するためのメールドメイン**]
  リクエストが本設定で登録したドメインにのみ送信されるようになります。
- [**承認者のメールアドレス**]
  - [**ゲストユーザーにスプラッシュページのホストメールのスキップを許可**]
  - [**自己登録のゲストユーザーに自動ログインを許可**]
  - [**自己登録のゲストユーザーにWebページで資格情報を表示**]

認証までの手順に関しては、『ホスト承認によるゲストWi-Fiユーザー認証』を参照してください。

4. 任意で、編集アイコンをクリックしてユーザー登録時の設定を作成します。



設定項目は、以下の通りです。

パラメータ	概要
配信メディア（ゲストユーザー資格情報用）	ゲストユーザーがスプラッシュページで設定したメールアドレスまたはSMSへメッセージを送付します。 SMSの利用には、事前に外部SMSサービスとの連携が必要です。
メール/SMS内容	ユーザー登録時に、ゲストユーザー宛ての送付されるメッセージの内容が編集できます。
ゲストユーザーの有効性とデバイス制限	ログインしたユーザーのアクセスを許可する時間と、一つのユーザーアカウントで接続できるデバイス数の制限ができます。
ログイン数の制限	ユーザーがログインできる回数を制限できます。
ゲストユーザー情報	Wi-Fi接続をするためにユーザーが入力すべき設定を選択できます。必須項目は、ユーザーが必ず入れる必要がある項目で、表示項目は、ユーザーが任意に入れる項目です。ユーザー名、パスワードは必ず入力する必要があります。 また、SSID、SSIDキーの表示チェックボックスをオンにすると、登録後に送付されるメールにSSID、SSIDキーが表示されます。これは、セミナー等で不特定多数にゲストWi-Fiを利用してもらう際に、メール転送などで利用するSSID情報を展開する際に役立ちます。 ゲストユーザー情報 フィールド / 表示 / 必須 ユーザー名 / ☑ / ☑ パスワード / ☑ / ☑ 姓 / ☐ / ☐ 名 / ☐ / ☐ 会社 / ☐ / ☐ メール / ☑ / ☑ 電話番号 / ☑ / ☑ 住所 / ☐ / ☐ ホスト / ☐ / ☐ 備考 / ☐ / ☐ SSIDキー / ☑ / ☑ SSID / ☑ / ☑
サービス品質(QoS)	ログインタイムアウト時間、ブラックアウト時間、最大利用帯域幅制限、リダイレクトURLを設定します。詳細は、『プラグインのサービス品質(QoS)設定』をご参照ください。

5. [**保存**]をクリックすると、[**プラグインとQoS**]ページに戻ります。
7. [**プラグインとQoS**]で[**保存**]をクリックすると、プラグイン設定が保存されます。
8. [**SSID**]を保存します。

ホスト承認によるゲストWi-Fiユーザー認証

「ホストが承認されたゲストブック プラグインを使用してユーザーがWi-Fiにアクセスする方法」の概要は、以下の通りです。

1. ゲストユーザーがSSIDに接続し、スプラッシュページにリダイレクトされます。ゲストユーザーは、連絡先情報とホストのEメールアドレスを入力して、スプラッシュページに登録します。ユーザーアカウント情報は、ポータルのゲストブックに保存されます。
2. ユーザーには、承認リクエスト送信のメッセージが表示されます。
3. ホストは、ゲストユーザーが登録したEメールを受信します。
4. ホストがEメールで[**承認**]をクリックすると、ゲストユーザーは承認メッセージを受信します。リクエスト時から5分以内に承認が得られた場合、ゲストユーザーは再度ログインしなくてもWi-Fiにアクセスできます。ゲストユーザーは、[**続行**]をクリックすると自動的にログインします。
5. 5分後にリクエストの承認が付与された場合、ゲストユーザーは、提供されたユーザー名とパスワードを使用してログインする必要があります。ゲストユーザーは、[**ここをクリックしてログイン**]をクリックして認証を行い、Wi-Fiにアクセスする必要があります。

SMS経由のパスコードを構成する

ユーザーが電話番号を提供することで、Wi-Fiアクセス用のパスコードを提供します。プラグインを構成するには、[SSID]>[**キャプティブポータル**]で[**クラウドホスト**]をクリックします。SMSプラグインを経由してパスコードを構成するには、以下の手順を実行します。

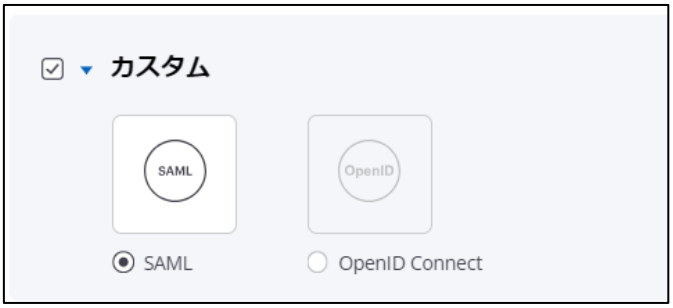
1. [SSID]>[**キャプティブポータル**]**タブ**で、[**ゲストWi-Fiユーザーのログイン方法を選択**]をクリックします。[**プラグインとQoS**]ウィンドウが画面右側に表示されます。
2. [**SMS経由のパスコード**]を選択し、編集アイコン をクリックすると、[**SMS経由のパスコード設定**]画面が表示されます。
3. [**ユーザー1人あたりのデバイス最大数を次に制限:**]を選択します。これは、同じパスコードを使用してWi-Fiにアクセスできるデバイスの最大数です。
4. [**パスコードの長さ**]と[**パスコードの有効性**]の選択をします。パスコードは、有効期間が経過すると期限切れになります。
5. [**SMSの再送信可能な最大回数を次に制限:**]と[**SMSが再送信されるまでの最小間隔を次に設定:**]でSMSを再送信するためのパラメータを選択します。SMSを再送信する最大回数の制限と、SMSを再送信するまでに経過されるまでの最小の時間間隔です。
6. [**ゲストユーザーに送信するテキスト(160文字)**]を入力します。
7. [**サービスの品質（QoS）**]と[**リダイレクトURL**]を設定します。
8. [**保存**]をクリックすると、[**プラグインとQoS**]ページに戻ります。
9. [**プラグインとQoS**]ページで[**保存**]をクリックして、設定を保存します。

SAML SSOを構成する

本機能により、SAML SSO(シングルサインオン)をサポートするIDP(IDプロバイダー)のアカウント情報を使用してキャプティブポータルへログインすることができます。SAML SSOを構成する前に、管理者によりIDPの開発者向けプラットフォームにて、アプリケーションを作成し、IDPメタデータの入手が必要となります。

SAML SSOを構成するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]>[**キャプティブポータル**]>[**プラグインとサービス品質(QoS)**]>[**カスタム**]の順に移動します。
2. [SAML]をクリックします。



2. スプラッシュページで表示されるアイコンを、必要に応じて変更することができます。対応している画像は、JPEG、PNGのみです。

3.[**SPメタデータのXMLをダウンロード**]をクリックしてSPメタデータをダウンロードできます。

注意：SPメタデータとは、サービスを提供するSPの情報(エンティティID、証明書、SAMLバージョン、エンドポイントURLなど)を含むXMLドキュメントです。

4. IDPの開発者ポータルサイトにて入手したIDPメタデータを設定します。IDPメタデータは[**手動で追加**]、または[**XMLをアップロード**]で設定します。
   [**手動で追加**]の場合には、以下のパラメータを設定します。
   ●[**エンティティID**]　：SAML SSO IDPのID
   ●[**ログインURL**]　　：IDPアプリケーションのURL
   ●[**ハッシュアルゴリズム**]：[**SHA256**]、[**SHA512**]から選択
   ●[**証明書ファイルを選択**]：データの署名、暗号化に使用する証明書
   [**XMLをアップロード**]の場合には、[**XMLファイルを選択**]をクリックして、XML(IDPメタデータ)ファイルをアップロードします。
5. IDP側に事前設定した[**SAML属性**]と[**ターゲット属性**]のマッピングを設定します。
   ●[**SAML属性**]　　：ユーザーがUI上で確認する事前定義された属性
   ●[**ターゲット属性**]　：IDPによって定義された属性

注意：ユーザーがIDPでの認証情報(ユーザ名/メールアドレス)をSP側で利用するため、ターゲット属性のマッピングは必須となります。

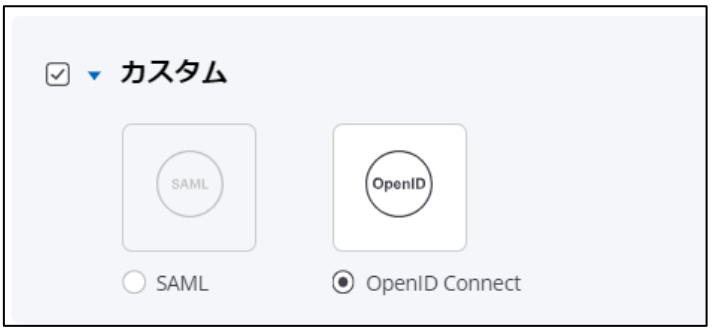
6. [**保存**]をクリックして設定を保存します。

OpenID Connectプラグインを構成する

本機能により、OpenID Connect SSO(シングルサインオン)をサポートするIDP(IDプロバイダー)のアカウント情報を使用してキャプティブポータルへログインすることができます。OpenID Connect SSOを構成する前に、管理者によりIDPの開発者向けプラットフォームにて、アプリケーションを作成し、クライアントID、クライアントキー、発行者URLの入手が必要となります。

OpenID Connect SSOを構成するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]>[**キャプティブポータル**]>[**プラグインとサービス品質(QoS)**]>[**カスタム**]の順に移動します。
2. [OpenID Connect]をクリックします。



3. スプラッシュページで表示される表示名と、表示アイコンを設定します。画像は、JPEGまたはPNGデータをアップロードし適用します。

4. IDPの開発者ポータルサイトにて事前設定した[**クライアントID**]、[**クライアントの秘密(クライアントキー)**]、[**発行者のURL**]を入力します。
5. [**保存**]をクリックして設定を保存します。

2.6.7.e 外部RADIUSプラグインを構成する

認証が外部RADIUSサーバーを経由して行われます。

注意：RADIUSプラグインを他のプラグインと共に使用することはできません。外部RADIUSを選択すると、AIRRECT Cloudによって他のプラグインは自動的に無効に設定されます。

外部RADIUSプラグインを構成するには、以下の手順を実行します。

1. [SSID]>[**キャプティブポータル**]**タブ**の[**ゲストWi-Fiユーザーのログイン方法を選択**]をクリックすると、[**プラグインとQoS**]ウィンドウが右側に表示されます。
2. [**外部RADIUS**]をクリックすると、**802.1x設定**が表示されます。
   a) 画面右の編集アイコンをクリックすると、[**外部RADIUS設定**]ウィンドウが表示され、[**サービス品質**(QoS)]と[**リダイレクトURL**]の設定が可能となります。
3. [**認証サーバー**]をクリックします。RADIUSサーバーをまだ追加していない場合は、[**追加/編集**]をクリックして追加できます。RADIUSサーバーの追加方法に関する詳細については、『RADIUSプロファイルの設定』を参照してください。
   備考: 少なくとも1つの**プライマリ認証**サーバーを選択する必要があります。オプショで、**アカウンティング**サーバーとセカンドリ認証サーバーも選択できます。
4. [**アカウンティングサーバー**]をクリックします。
   RADIUSサーバーを追加していない場合、[**追加/編集**]をクリックして追加できます。RADIUSサーバーの追加方法に関する詳細については、『RADIUSプロファイルの設定』を参照してください。
5. [**アカウンティング間隔**]を設定します。
6. [**発信先ステーションID**]と[NAS ID]の値を入力します。
   注意：同じアクセスポイント上の2つのSSIDが同じNAS IDを使用することはできません。
7. [**保存**]をクリックすると、[**プラグインとQoS**]ページに戻ります。
8. [**プラグインとQoS**]ページで[**保存**]をクリックしてプラグイン設定を保存します。

プラグインのサービス品質（QoS）設定

パラメータ	概要
ログイン タイムアウト	ポータルのゲストユーザーセッションが期限切れになるまでの期間を表します。Wi-Fiサービスの使用を継続したい場合、ユーザーはログイン資格情報で再認証する必要があります。「0」にした場合、ユーザーセッションがタイムアウトせず、ユーザーがポータルから明示的にログアウトする必要があることを示します。プラグインで設定された「0」以外のタイムアウトは、SSIDプロファイルで設定されたタイムアウトよりも優先されます。期間については、時間、分、日、週、または月で指定できます。
ブラックアウト 時間	最後に成功したログインがタイムアウトした後、ユーザーがポータルにログインできない期間を表します。「0」はログインできない期間がないことを示します。プラグインで構成されたブラックアウト時間は、SSIDプロファイルで構成されたブラックアウト時間よりも優先されます。期間については、時間、分、日、週、または月で指定できます。
リダイレクト URL	プラグインを使用してポータルからログインに成功したときにゲストユーザーをリダイレクトさせるページのURLを表します。
最大ダウンロード 帯域幅を制限	プラグインの最大ダウンロード帯域幅（KbpsまたはMbps）
最大アップロード 帯域幅を制限	プラグインの最大アップロード帯域幅（KbpsまたはMbps）

2.6.7.f サードパーティーホスト設定の構成

キャプティブポータルのサードパーティーホスト設定を構成するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDを選択し、[**キャプティブポータル**]へ移動します。
2. ゲストネットワークの使用時にクライアントに表示されるポータルページを表示するには、[**キャプティブポータル**]をクリックします。
3. アクセスモードを[**サードパーティーホスト**]として選択します。ゲストユーザーは、外部サーバーでホストされているポータルにリダイレクトされます。
4. サードパーティのホスティング内で基本設定を構成するには以下の手順を実行します。
   a) [**RADIUS認証あり**]を選択します。
   ゲストユーザーは外部ポータルにログインする際、RADIUSサーバーによって認証されます。[**RADIUS認証あり**]をクリックすると、802.1x設定を構成するためのリンクが表示されます。

b) 802.1x設定を構成は『外部RADIUSプラグインを構成する』を参照してください。

c) [**スプラッシュページのURL**]を入力します。このURLを使用すると、ユーザーは外部ポータルにリダイレクトされます。

d) SSID外部ポータル通信の[**共有シークレット**]を入力します。

e) [**HTTPSリダイレクト**]を有効にすると、Wi-FiクライアントのHTTPS通信時にもスプラッシュページへのリダイレクトが可能となります。この機能の利用には証明書が必要となります。以下の情報からAPは証明書を生成します。

●[**共通名**]　：FQDN

●[**組織**]　　：組織名

●[**組織ユニット**]：組織単位名

f) [**ユーザーがログイン前にアクセスできるWebサイト**]を入力します。

5. ログイン後の設定で、以下のフィールドに詳細を入力します。

a) [**リダイレクトURL**]を指定します。
ユーザーがポータルページの送信ボタンをクリックすると、ブラウザはこのURLにリダイレクトされます。入力しない場合、ポータルページが表示されたブラウザからアクセスされた元のURLにブラウザがリダイレクトされます。

b) [**サービス識別子**]の値を指定します。これは、外部ポータルに渡すことができる形式自由のパラメータです。

c) ユーザーがポータルページを送信した後にゲストネットワークにアクセスできる[**ログインタイムアウト**]を指定します。タイムアウト後、ゲストネットワークへのアクセスが停止され、ポータルページが再び表示されます。
ユーザーは、ゲストネットワークへのアクセスを回復するためにポータルページを送信する必要があります。ユーザーのセッションがタイムアウトする前に切断してゲストネットワークに再接続した場合、スプラッシュページで資格情報を入力する必要はありません。

d) [**ブラックアウト時間**]を指定します。
前の正常なセッションがタイムアウトした後に、ユーザーがログインを許可されない時間です。セッションタイムアウトが1時間で、ブラックアウト時間が30分の場合、ユーザーはログイン成功後1時間でタイムアウトし、その後30分は再ログインできません。30分後に、ユーザーは再度ログインできます。

e) SSID接続時のゲストユーザーに対し、APがインターネット接続障害が発生していることを伝えるポップを表示する場合には、[**インターネット接続のダウンを検出してゲストユーザーに知らせる**]をクリックします。既にSSID済みのゲストユーザーに対しては通知されません。

6. [**詳細なポータルパラメーター**]の設定には、『要求と応答の属性』を参照してください。

7. [**保存**]をクリックし設定を保存します。

要求と応答の属性

要求の属性	概要
要求のタイプ	要求のタイプのフィールド名を表します。
チャレンジ	使用されるランダムテキストのフィールド名を表します。
クライアントのMACアドレス	クライアントのMACアドレスのフィールド名を表します。
アクセスポイントのMACアドレス	外部ポータルと通信しているアクセスポイントのMACアドレスのフィールド名を表します。
アクセスポイントのIPアドレス	外部ポータルと通信しているアクセスポイントのIPアドレスのフィールド名を表します。 これは、外部ポータルで使用されるフィールド名と一致する必要があります。
アクセスポイントのポート番号	アクセスポイント、および、外部サーバーが接続されているアクセスポイントポート番号のフィールド名を表します。
失敗数	失敗数のカウントのフィールド名を表します。
要求されたURL	クライアントからリクエストされたURLである、リクエストされたURLのフィールド名を表します。
ログインURL	ログインURLのフィールド名を表します。
ログオフURL	ログオフURLのフィールド名を表します。
残りのブラックアウト時間	残りブラックアウト時間のフィールド名を表します。
サービス識別子	サービス識別子値を外部ポータルに渡すために使用されるポータルパラメータの名前を表します。サービス識別子値は、SSIDプロファイルのキャプティブポータルセクションで指定されます。このパラメータを外部ポータルで使用して、様々なSSID、ポータルなどのSSIDプロファイル固有の機能を実装できます。
応答の属性	
チャレンジ	チャレンジのフィールド名を表します。
応答のタイプ	応答タイプのフィールド名を表します。
チャレンジ応答	チャレンジ応答のフィールド名を表します。
リダイレクトURL	リダイレクトURLのフィールド名を表します。
ログインタイムアウト	ログインタイムアウトのフィールド名を表します。
ユーザ名	ユーザー名のフィールド名を表します。
パスワード	パスワードのフィールド名を表します。

2.6.8 ゲストWi-Fiの管理

ゲストWi-Fi機能によって、キャプティブポータル機能でWi-Fiアクセスを許可するゲストユーザーや、ログイン時の登録データを管理するリストの管理が可能です。ゲストブックを管理するには、管理者ロールまたはオペレーターロールのいずれかの権限が必要です。Guestbook用のSSIDで作成した後は、画面左の[**ゲストWiFi**]から一元管理を行います。

2.6.8.a ゲストユーザーの作成/編集

ゲストユーザーアカウントを作成し、インターネットにアクセスを許可するゲストユーザーへ配布するID/パスワードや、ユーザー情報の設定を行います。ゲストブックへの登録数に制限はありません。
ゲストユーザーアカウントを作成/編集するには、次の手順を実行します。

1. [**構成**]>[WiFi]>[SSID]の順に移動します。
2. 任意の SSID を選択し、[**キャプティブポータル**]タブで、[**ゲスト WiFi ユーザーのログイン方法を選択**]をクリックすると、[**プラグインと** QoS]ウィンドウが画面右側に表示されます。
3. [**ユーザー名/パスワード**]を選択し、[**任意でユーザーの自己登録を許可**]の設定をします。

4. 設定を保存した後、SSIDの保存をします。

5. SSID情報の保存後、画面左の[**ゲストWIFI**]からゲストユーザー設定ができます。
ゲストWi-Fiを複数設定している場合でも、本画面からフィルタリングすることで利用が可能です。一覧は、SSID名[プロファイル名]が表示されます。

6. 作成時/編集時で以下の手順を実施します。
作成時：[**ユーザー**]タブで、SSID名横の[**追加**]をクリックします。
新規ユーザーのフィールドが表示されます。
編集時：[**ユーザー**]タブで、ユーザーが編集するユーザー名のリンクをクリックします。

7. ユーザーアカウントの詳細を設定します。

オプション	説明
ユーザー名	ゲストユーザーアカウントの名前。作成時はランダムな値が生成されます。任意のユーザー名を入力することもできます。
パスワード	ゲストユーザーアカウントのパスワード。作成時はランダムな値が生成されます。任意のパスワードを入力することもできます。
メール	ゲストマネージャーのアカウントにEメールが設定されている場合、ユーザーアカウント情報の送信先となるゲストユーザーのEメールアドレス
ユーザー・ステータス	[**ロック済み**]を選択すると、ロックされたユーザーはWi-Fiアクセスが拒否されます。
有効性	ゲストユーザーアカウントの有効期限の日時。この日付を過ぎると、ゲストはこのアカウントを使用できなくなります。カレンダーアイコンと時計アイコンをクリックして、それぞれ有効期限と時刻を選択します。

オプション	説明
デバイスの上限	ゲストユーザーが単一のユーザーアカウントで同時にログインできるデバイスの最大数。デフォルト値はN/Aであり、デバイス制限がないことを意味します。デバイス制限は、ゲストブックプラグインレベル、ゲストバッチレベル、およびゲストユーザーレベルで設定できます。それぞれでデバイス制限が設定されている場合、優先度は「ユーザーレベルで設定されたデバイス制限」＞「ゲストバッチレベルでのデバイス制限」＞「ゲストブックプラグインレベルでのデバイス制限」の順番になります。
ログイン数の上限	ゲストユーザーが特定の資格情報のセットを使用してスプラッシュページからログインできる回数。このオプションは、ゲストブックプラグインを構成するときにも使用できます。ゲストユーザーの作成時に記載された値は、ゲストブックプラグインの構成時に記載された値よりも優先されます。 注：アカウントが有効で、ユーザーがログイン数の制限を超えた場合、ユーザーはログインできません。
SSID名	割り当てられたAPのSSID名
SSIDキー	割り当てられたAPのSSIDキー
サービス品質設定-ログインタイムアウト	プラグインのゲストユーザーセッションが期限切れになるまでの期間。Wi-Fiサービスを引き続き使用する場合、ユーザーはログイン資格情報を使用して再認証する必要があります。この値がゼロの場合は、ユーザーセッションがタイムアウトせず、ユーザーがポータルから明示的にログアウトする必要があることを示します。プラグインで構成されたゼロ以外のタイムアウトは、ポータルで構成されたタイムアウトよりも優先されます。
サービス品質設定-ブラックアウト時間	ユーザーがタイムアウトした後、ポータルにログインできない時間を指定します。この値がゼロの場合は、ブラックアウト時間がないことを示します。プラグインで構成されたゼロ値を含むブラックアウト時間は、ポータルで構成されたブラックアウト時間よりも優先されます。
サービス品質設定-最大ダウンロード/アップロード帯域幅	ゲストユーザーの最大ダウンロード帯域幅（Kbps）と最大アップロード帯域幅（Kbps）の設定をします。

9. User Profileを必要に応じて設定します。
10. [**保存**]をクリックして設定を保存します。[**保存して通知を送信**]をクリックすると、アカウントの詳細を[**メール**]で設定したアドレスに送信されます。

2.6.8.b ゲストバッチ

セミナーや主催したイベントなど、特定のイベント用に多数のゲストユーザーアカウントを作成し、ゲストにWi-Fiアクセスを提供する場合などは、ゲストユーザーアカウントのバッチを作成することで効率的にユーザーを登録できます。作成したゲストバッチの編集や、インポート/エクスポート設定は[**ユーザー**]タブでの設定と同一です。

ゲストバッチの作成/編集

ゲストユーザーアカウントのバッチを作成/編集するには、次の手順を実行します。

1. [**ゲストWIFI**]>[**バッチ**]タブを選択します。作成時/編集時で以下の手順を実施します。
   作成時：[**追加**]をクリックします。バッチリストが表示されます。
   編集時：変更するバッチのバッチIDをクリックします。

2. ユーザーバッチ情報を設定します。

オプション	説明
ユーザー名のプレフィックス	ゲストユーザーアカウントバッチのプレフィックスです。バッチ内のすべてのユーザーに適用されます。
バッチ・タイプ	ゲストユーザーバッチでランダムユーザーを生成するには、[**ランダム・ユーザー**]を選択します。[**インクリメント・ユーザー**]を選択すると、指定したプレフィックスと増分インデックスを持つユーザー名をバッチで生成します。
ユーザー名の長さ	ランダムに生成されたユーザー名の長さを指定します。 このフィールドは、[**ランダム・ユーザー**]を選択した場合にのみ表示されます。
パスワードの長さ	生成するパスワードの長さを指定します
開始インデックス	増分するユーザーバッチに追加される開始番号です。このフィールドは、[**インクリメント・ユーザー**]を選択した場合にのみ表示されます。
ユーザー数	バッチで作成するユーザーの数を指定します。
有効期限	バッチ内のゲストユーザーアカウントの有効期限の日時です。この日付を過ぎると、ゲストはこのアカウントを使用できなくなります。カレンダーアイコンと時計アイコンを使用して、それぞれ有効期限と時刻を選択します。
バッチの説明	バッチが表す内容の詳細を示すテキストを入力します。たとえば、会

	議用にバッチが作成されている場合は、ここで会議の詳細を指定できます。
デバイスの上限	ゲストユーザーが単一のユーザーアカウントで同時にログインできるデバイスの最大数。デフォルト値はN/Aであり、デバイス制限がないことを意味します。デバイス制限は、ゲストブックプラグインレベル、ゲストバッチレベル、およびゲストユーザーレベルで設定できます。それぞれでデバイス制限が設定されている場合、優先度は「ユーザーレベルで設定されたデバイス制限」＞「ゲストバッチレベルでのデバイス制限」＞「ゲストブックプラグインレベルでのデバイス制限」の順番になります。
ログイン数の制限	ゲストユーザーが特定の認証情報を使用してスプラッシュページからログインできる回数です。このオプションは、ゲストブックプラグインを構成するときにも使用できます。ゲストバッチの作成時に指定された値は、ゲストブックプラグインの構成時に指定された値よりも優先されます。ユーザーがログイン数の制限を超えた場合、ユーザーはログインできません。

3. サービス品質を設定します。

「ゲストユーザーの作成/編集」の項目と共通です。

4. [**保存**]をクリックします。 ゲストバッチが作成/更新されます。

2.6.8.c ゲストユーザー/ゲストバッチ共通

ゲストユーザーのエクスポートとインポート

ゲストユーザーアカウントをCSVファイルにエクスポートできます。

ゲストユーザーアカウントをエクスポートするには、画面右上の[**すべてのユーザーをダウンロード**]マークをクリックします。

特定のユーザーアカウントのみをエクスポートする場合は、任意のユーザーアカウントを選択した後に、右クリックをして[**ユーザーをエクスポート**]を選択します。

また、ゲストユーザーアカウントをCSVファイルからインポートできます。インポートするCSVファイルは、一度手動などで作成された以下のようなデータをエクスポートしてフォーマットを入手後、一行目を残してデータ修正、インポートすることを推奨します。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Username	Password	Login Cou	First Nam	Last Name	Email	Company	Mobile Phone	Address	Notes	Gender	Host	Ssid Name	Ssid Key
2	matsushitaaro564	09jr1kcy		松下	太郎	matsushit	パナソニッ	8.10311E+11	東京都港区	試験用のアカウント		松下幸之助	Guest Wi-Fi1	
3	musenlan@panas	8rv2loxe		無線	二郎	musenlan	無線通信コ	8.10462E+12	神奈川県相	セミナーゲスト用		無し	Guest Wi-Fi1	
4														

ゲストユーザーアカウントをインポートするには、画面右上の[**ユーザーをインポート**]マークを選択します。

ゲストユーザーの編集をする

作成されたゲストユーザーアカウントを右クリックすると、状態の編集が可能です。複数ユーザーを選択し右クリックすると、複数のクライアントを纏めて編集ができます。

●ユーザーの有効化/無効化：登録したユーザーのアクセスを有効化/無効化することができます。ユーザーが有効化されているかどうかは、アイコンマークで確認が可能です。

-緑色の鍵マーク：アクセスが有効化

-赤色の鍵マーク：アクセスが無効化

-グレーの×マーク：利用有効期間が終了したユーザー

●ユーザーの削除

●電子メールを送信：登録されているメールアドレスに登録情報を送付します。

●使用期限を設定：利用期間の終了日を任意に設定可能です。

●パスワード：ログインパスワードを変更できます。

ゲストユーザー/ゲストバッチ情報のソート

ゲストユーザー/ゲストバッチのリストは、[**ユーザー**]/[**バッチ**]タブの下に、それぞれ表形式で表示されます。この情報は、さまざまなフィールドで並べ替えることができます。

並べ替えるには、次の手順を実行します：

1. 情報を並べ替えるフィールドの名前をクリックします。フィールドはアルファベット順にソートされています。
2. 並べ替え順序を逆にするには、フィールド名をもう一度クリックします。

2.6.9 SSID RF最適化

SSID設定の[**RF最適化**]**タブ**では、SSIDに対してさまざまなタイプのステアリングを簡単に有効化できます。クライアントステアリングに関連するパラメータの設定は[**WiFi無線**]**タブ**に移動する必要があります。

●[**最小RSSIベースのアソシエーション**]は、クライアントがSSIDのアクセスポイントとのアソシエーションを許可される最小RSSIです。この値は、[**構成**]>[**デバイス**]>[**アクセスポイント**]>[**Wi-Fi無線**]の、[**クライアントステアリングの共通パラメータ**]から設定できる[**ステアリングRSSIしきい値**]が参照されます。例えば、ステアリングRSSIしきい値が-70dBmの場合、アクセスポイントとクライアント間のRSSI値が-70dBm以下だと接続できなくなります。ただし、本機能は二台以上のアクセスポイントが存在する場合に効果を発揮する機能であり、しきい値を以下のアクセスポイントしか存在しない場合は、クライアントはアクセスポイントとアソシエーションを行います。
例：しきい値が-70dBmでアクセスポイントが二台あるケース
1.-72dBmと-78dBmのSSIDを検知しているとき、最小RSSI値以下であるが、どちらかには接続される
2.-65dBmと-75dBmのSSIDを検知しているとき、必ず-65dBmのAPに接続される

●[**ステアリングを強制**]を有効にすると、アクセスポイントは2.4GHz帯のステアリング要求を拒否し、クライアントを6GHzまたは5GHzに強制ステアリングします。（デフォルト有効）

●[**スマートクライアントのロードバランシング**]機能を有効にできます。
詳細は『スマートステアリングのロードバランシング』をご参照ください。

●[**スマートステアリング**] 機能を有効にできます。
詳細は『スマートステアリング』をご参照ください。

●[**付近の802.11kリスト**]を有効にすると、クライアントはアクセスポイントからネイバーリストを要求できるようになり、ローミングが高速化されます。802.11kを有効にすると、アクセスポイントが両帯域でクライアントのネイバー情報を送信する[**周囲に2.4GHz/5GHz/6GHz帯のリストを送信**]を選択できます。802.11kは個々のクライアントが無線環境を把握するための方法を定義しますが、[**802.11v BSS移行**]は全体的なネットワークパフォーマンスの向上に関する定義をします。802.11vを有効にすると、

クライアントとの接続解除に関する詳細設定ができます。
[802.11r]を有効にすると、認証の時間が短縮され、高速なローミングを行うことが出来ます。それぞれのローミング規格の詳細は、『802.11kの詳細と使用例』、『802.11kの詳細と使用例』、『802.11rの詳細』をご確認ください。

● [プロキシARPとNDP]を有効にすると、アクセスポイント自体が、ARP、および、NDP要求を低データレートで代理応答し、アソシエーションされたワイヤレスクライアントのプロキシとして機能できます。

●[DGAF(Downstream Group-Addressed Forwarding)の無効化]を有効にすると、有線側から無線側へのすべてのブロードキャスト/マルチキャストトラフィックをブロックします。

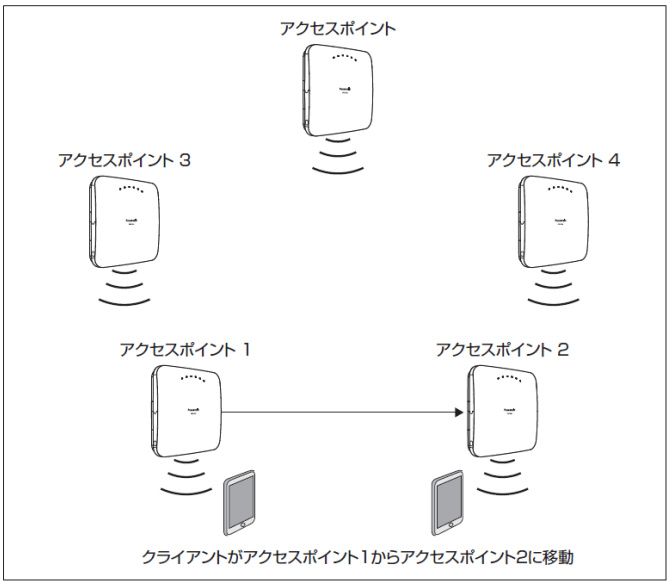
● [ブロードキャスト/マルチキャスト制御]を有効にすると、アクセスポイントはイーサネットからワイヤレスへのブロードキャスト/マルチキャストパケットをブロックします。不要なトラフィックをブロックすることにより、RF帯域をクリーンアップします。
また、[無線から有線への流入をブロック]をクリックして、無線からイーサネットへのブロードキャスト/マルチキャストパケットをブロックすることもできます。
ブロードキャスト/マルチキャストパケットの使用を許可する必要があるアプリケーションの場合、プロトコル情報を除外リストに追加して除外することもできます。

●Bonjourは、Bonjour対応のデバイスとサービスをネットワーク経由で簡単に使用および構成できるように設計された Appleプロトコルです。Bonjourはブロードキャストを多用し、Apple製品利用に不可欠なので、[Bonjourを許可]をクリックすると、自動的に除外するアプリケーションとして認識させる必要があります。

●[IGMPスヌーピング]は、マルチキャストパケットをスヌーピングして、クライアントが参加しているマルチキャストグループのポートにのみ転送される仕組みです。これにより、不要なパケットフローが回避され、帯域幅が節約されます。

802.11kの詳細と使用例

以下のように、アクセスポイント 1 からアクセスポイント 2 に移動するクライアントがあるとき、アクセスポイント1からの信号強度は弱くなるため、クライアントは他の最適なアクセスポイントを検索します。802.11kが無効の場合、クライアントは、最適なアクセスポイントの検索のため、周囲のチャネルをスキャンする必要があります。多くのクライアントは、Beaconを100ms間隔でスキャンするため、5GHz帯で21のチャネルが利用可能であるとき、利用可能なすべてのチャネルのスキャンには最短でも2.1秒程度かかることとなります（100ms x 21ch = 2.1s）。この場合、リアルタイムアプリケーションの通信要件（VoIPでは一方向の遅延が50ms未満）が満たせず、通信切断などが発生することがあります。



無線リソース測定（RRM）とも呼ばれるIEEE 802.11kは、各アクセスポイントがそれぞれの無線周波数（RF）環境について互いに通知できるようにする方法を定義しており、共有したそれらの情報に基づき、迅速にローミング先を決定します。
802.11kでは、クライアントは接続しているアクセスポイントに、隣接するアクセスポイントの情報（ネイバーレポート）を送信するよう要求できます。ネイバーレポートには、どのアクセスポイントが現在接続しているSSIDを出力しているか、それらのアクセスポイントがどのチャネルで動作しているか、また、それらの情報を参照するときの各アクセスポイントの信号強度のRSSI値はいくつか、などの情報が含まれます。
上図で、クライアントは、接続しているアクセスポイント1に対しネイバーレポートを要求しています。5GHz帯域の同SSIDを出力しているアクセスポイントが周囲に4台（アクセスポイント2から5）あるとき、クライアントは、4つの接続候補チャネルのネイバーレポートを受信します。そうすることで、スキャンするチャネルを限定し、4台の場合であればクライアントは0.5秒以内にどのアクセスポイントへ移動するかを決定できます。

参考：802.11kがある場合/ない場合のスキャン時間

5GHz	すべてのチャネル	11k Neighbors
スキャンするチャネル	21ch	4ch
スキャン時間	2.1秒	400ミリ秒

注意：本機能は、クライアントが802.11k規格に対応している必要があります。非対応の端末については、アクセスポイントリストを受け取った際の動作が不安定になる可能性もあるため、初期値では無効となっています。利用端末の状況に応じて、有効化をしてください。

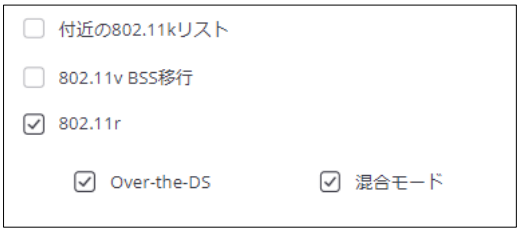
802.11vの詳細と使用例

アクセスポイントに接続されているクライアントについて、信号強度が設定されたしきい値を下回るか、ネットワークの負荷分散アルゴリズムが別のアクセスポイントと接続したほうが快適な通信をできると判断する場合、アクセスポイントとのアソシエーションを解除することがあります。これはクライアントに予期しない負荷を与える可能性があり、また、新しく接続するアクセスポイントを選択するために、クライアントが周囲のチャネルスキャンを実行する原因となります。これにより、特にリアルタイムアプリケーションを利用している場合はユーザーエクスペリエンスが低下する可能性があります。
IEEE 802.11vは、ワイヤレスネットワーク管理（WNM）、とも呼ばれ、802.11kより広い範囲を定義しています。
802.11kは個々のクライアントが無線環境を把握する方法を定義していますが、802.11vは全体的なネットワークパフォーマンスの向上のための機能を定義します。
また、重要なサービスとして、BSSトランジション・マネジメント（BSTM）があります。アクセスポイントは、クライアントとのアソシエーションを解除することを決定すると、BSTM要求と呼ばれる802.11vフレームを送信します。基本的にはアクセスポイントが60秒後にアソシエーションを解除することをクライアントに警告します（時間間隔は変更可能です）。これは、非送信請求要求と呼ばれます。この間に、クライアントは別のアクセスポイントを見つけてアソシエーションすることができます。非送信請求メッセージには、クライアントがアソシエーションをすることができる同じESS上の隣接アクセスポイントのリストが含まれます。BSTM応答メッセージと呼ばれる802.11vのメッセージでは、クライアントはアクセスポイントの要求を受け入れまたは拒否できます。
アクセスポイントにさらに時間を要求することもできます。BSTM応答メッセージには、BSS終了遅延フィールドが含まれます。クライアントが「60秒は短すぎるため、3分後にアソシエーションを解除する」と応答した場合、基本的にアクセスポイントはこの要求を受け入れます。
802.11kでは、クライアントのみがネイバーリストを要求できますが、802.11vでは、クライアントまたはアクセスポイントのどちらからでもネゴシエーションを開始できます。

クライアントは、BSTMクエリを送信して、アクセスポイントに「別のアクセスポイントとアソシエートする必要があるか、必要な場合、どのアクセスポイントにするか」を確認できます。クライアントは、その実装に応じて、このクエリを定期的に送信したり、信号強度の低下などのトリガーに基づいて送信したりすることができます。アクセスポイントは、クライアントがアソシエートすることができる推奨アクセスポイントのリストを含むBSTMリクエスト（送信請求要求）で応答します。
ネイバーのリストを含むBSTMリクエストを送信して、アソシエーション解除の警告を表示せずに、クライアントに別のアクセスポイントを探すよう指示するだけの場合もあります。例えば、ネイバーアクセスポイントの負荷が低く、十分に近い場合に発生する可能性があります。802.11vはネットワーク全体の状況を把握しているため、負荷の少ないアクセスポイントに移動することをクライアントに推奨します。これを可能にするために、802.11vは、アクセスポイントがクライアントとのアソシエーションを解除するつもりであるかどうかを示すアソシエーション解除通知フラグビットを提供します。

802.11rの詳細

802.11rまたは、高速移行（FT）により、クライアントは 新しいアクセスポイントをアソシエーションする前にセキュリティとQoSパラメータを再構築し、移行中にクライアントが直面する中断時間を大幅に削減することができます。



ローミングの 「オーバーディストリビューションシステム」モードを使用して、クライアントがローミングするように基本設定をおこなう場合は、[Over-the-DS]を選択します。Over-the-DS有効時、クライアントは、現在接続しているアクセスポイントを介して移行先のアクセスポイントへ認証要求を行います。[**混合モード**]をクリックすると、802.11r互換クライアントと802.11r非互換クライアントの両方がSSIDに接続できるように設定できます。

注意：802.11w、および、802.11rは[WPA2]ではサポートされていますが、[**オープン**]または [WPA/WPA2**混合モード**]ではサポートされていません。

2.6.9.a SSIDプロファイルでのRF最適化の基本構成

RF関連の最適化を有効にするには、[**構成**]>[Wi-Fi]>[SSID]>[RF**最適化**]の順に移動します。

1. 有効にするステアリングのタイプを選択します。ステアリングのタイプは以下の通りです。

   ●スマートクライアントのロードバランシング

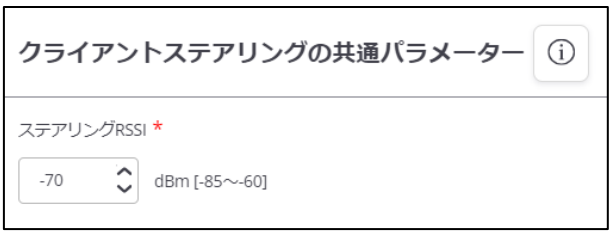
   ●スマートステアリング

   ●最小RSSIベースのアソシエーション

   ●バンドステアリング

   ●ステアリングを強制

   ステアリングを行うためのクライアント間の接続/切断要求は、[**構成**]>[**デバイス**]>[**アクセスポイント**]>[WiFi**無線**]の、[クライアントステアリングの共有パラメータ]にある、ステアリングRSSIの値を下回ったことを起因に動作します。

   スマートステアリングを有効化する場合は、最小RSSIベースのアソシエーションも有効化する必要があります。

2. [**付近の802.11kリスト**]と[802.11v BSS**移行**]を有効にできます。（デフォルト無効）

   ●[**付近の802.11kリスト**]を有効にする場合：オプションで、[**周囲に2.4GHz/5GHz/6GHz帯のリストを送信**]を有効にできます。無効の場合は、クライアントからリストの要求があった際に、クライアントが接続している周波数帯のリストのみを送信します。

   ●[802.11v BSS**移行**]を有効にする場合：[**アソシエーション解除通知**]を有効にし、クライアントがアクセスポイントから切断されるまでの時間である[**アソシエーション解除タイマー**]を設定する必要があります。アソシエーション解除タイマーは、ビーコン間隔の数で表されます。この解除タイマーの範囲は、10～3000TBTT（ターゲットビーコンの送信時間）です。アソシエーション解除タイマーがゼロになると、強制切断設定に基づいて、クライアントのアソシエーションを解除できます。

   ●[**強制的に接続解除**]を選択して、アソシエーション解除タイマーの期限が切れた後でクライアントを強制的に切断できます。クライアントがBSS遷移応答で否定的な応答をしても、クライアントは切断されます。[**強制的に接続解除**]が選択されていない場合、アクセスポイントはクライアントを切断しません。（クライアントが自動的に切断するのを待ちます）

●[**アソシエーションのセキュリティレベルを選択**]で[WPA2]を選択した場合は802.11rの設定が出来ます。

注意：802.11w、および、802.11rは[WPA2]ではサポートされていますが、[**オープン**]または [WPA/WPA2**混合モード**]ではサポートされていません。

3. [**プロキシARPとNDP**]をクリックします。
プロキシARPとNDPを有効にすると、アクセスポイントはダウンストリームARP (IPv4)およびNDP (IPv6)パケットをフィルタリングし、ワイヤレスクライアントに代わって応答し、ワイヤレス帯域幅を節約します。プロキシARPとNDPを有効にすると、DGAFを無効にできる[**DGAFの無効化**]フィールドが有効になります。
4. [**DGAFの無効化**]をクリックします。
有効にした場合、アクセスポイントはIPv4のプロキシARP、および、IPv6のプロキシNDPを開始します。また、送信パス内のすべてのマルチキャストおよびブロードキャストパケットをドロップします。このオプションを有効にすると、ブロードキャスト/マルチキャスト制御とIGMPスヌーピングが無効になります。
5. [**保存**]をクリックします。

2.6.9.b IGMPスヌーピング

IGMPスヌーピングは、マルチキャストパケットをスヌーピングして目的のクライアントにのみ転送する方法です。マルチキャストパケットは、複数のネットワークセグメントに転送されます。例えば、ビデオストリーミングパケットがビデオストリーミングクライアントのいないセグメントに送信された場合にネットワーク帯域幅を圧迫します。IGMPプロトコルは、このような無駄なデータを排除するために、マルチキャストストリームを受信する必要があるクライアントを、接続先のレイヤ2デバイスに通知します。
クライアントは、参加したいマルチキャストセッションのマルチキャストアドレスを含むIGMPレポートを送信することにより実行します。レイヤ2デバイスは、IGMPスヌーピングを使用してマルチキャストパケットを調べ、それらをクライアントが参加しているマルチキャストアドレスのリストと照合します。このようにIGMPスヌーピングを有効にすると、アクセスポイントはイーサネットからワイヤレスへのマルチキャストトラフィックをブロックします。
マルチキャストパケットを受信するには、クライアントは、参加するマルチキャストグループのアドレスを含むIGMPレポートを送信する必要があります。
クライアントアプリケーションは、通常IGMPレポートの送信をします。クライアントアプリケーションがIGMPをサポートしていない場合でもIGMPスヌーピングを有効にすることができますが、その場合はアプリケーションが使用しているマルチキャストアドレスをIGMPスヌーピングの例外リストに追加する必要があります。

例外リストに追加されたSSIDを使用するすべてのアクセスポイントは、クライアントが参加するためにIGMPレポートを送信したかどうかにかかわらず、そのアドレスを持つすべてのマルチキャストパケットを転送します。例外リストには、最大30個のマルチキャストアドレスを追加できます。
マルチキャストパケットを受信するクライアントが別のアクセスポイントにローミングすると、IGMPスヌーピングテーブルが転送されるため、クライアントは新しいIGMPレポートを送信する必要はありません。[**マルチキャストをユニキャストに変換**]は、例外リストのアドレスを除いて、マルチキャストパケットをユニキャストに変換します。

例外リスト

機能	概要	デフォルト	レンジ
IGMPスヌーピング	IGMPスヌーピングを有効にする。	有効	-
IGMPスヌーピングの例外リスト	クライアントがIGMPレポート（ジョイン）を送信しなくてもマルチキャストを配信できるようにする。	-	最大30

IGMPスヌーピングの制限

機能	制限
IGMP スヌーピング	●クライアントのIGMPレポートに基づく 有効：マルチキャストをブロック 無効：すべてのマルチキャストを転送 ●イーサネットからワイヤレスへのマルチキャストに適用 ●マルチキャスト/ユニキャスト変換に依存しない。 ●クライアントのローミング時にスヌーピングテーブルが転送される。 ●アクセスポイントはIGMPクエリを送信しない。
IGMP スヌーピング で保護された アドレス	●最大30のマルチキャストアドレス ●内部保護されたアドレス ●224.0.0.1/24 - すべてのシステムのクエリ ●224.0.0.22/24 - IGMP v3アドレス ●[**マルチキャストをユニキャストに変換**]を有効にしても、ユニキャストパケットが変換されない。 ●クライアントが参加するためのIGMPレポートを送信しなくても、すべてのパケットを送信する。

IGMPスヌーピングの構成

IGMPスヌーピングは、IGMPネットワークトラフィックを監視する機能です。選択したSSIDに対してIGMPスヌーピングを有効にすると、クライアントがマルチキャストグループに参加していない場合、マルチキャストパケットがブロックされます。IGMPスヌーピングを有効にしても、[**マルチキャストからユニキャストに変換**]を有効にするまで、パケットはマルチキャストからユニキャストに変換されません。

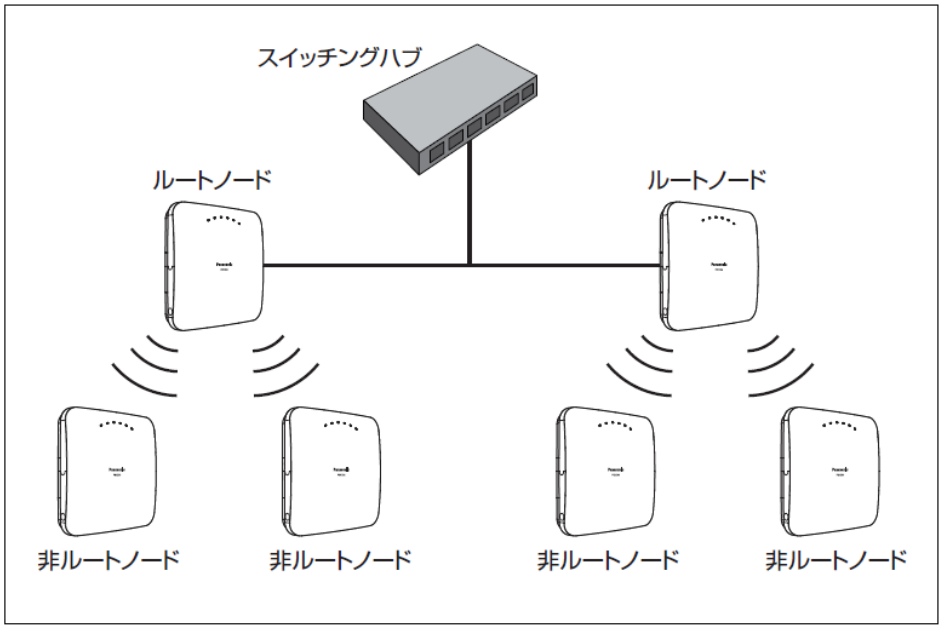
IGMPスヌーピングを構成するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDの[RF**最適化**]タブをクリックします。
2. 下にスクロールして、[**IGMPスヌーピング**]を選択します。
3. [**IGMPスヌーピングの例外リスト**]にIPアドレスを入力します。
4. [**スヌーピングのタイムアウト**]を分単位で入力します。
5. [**マルチキャストをユニキャストに変換**]をクリックします。

   デフォルトでは無効になっています。IGMPスヌーピングが有効になっている場合にのみ、有効にできます。有効にすると、すべてのマルチキャストパケットは、スヌーピングに合格した後でMACレイヤーユニキャストパケットに変換されます。
6. [**選択した優先度でパケットをタグ付け**]に適切な値を選択します。
7. [**保存**]をクリックします。

2.6.10 メッシュネットワーク

メッシュネットワークは、アップリンク有線接続が困難なアクセスポイントが存在する場合に使用します。一部のアクセスポイント（ルートノード）のみが有線接続を持っており、他のアクセスポイント（非ルートノード）は「メッシュリンク」または「ホップ」を形成し、最終的にルートノードにリンクするルートを動的に形成します。



ルートノードはスイッチに直接接続されますが、非ルートノードは、1つ以上の無線ホップを介して有線へ接続します。ホップごとにスループットが低下します。
AIRRECT Cloudでは、メッシュプロファイルを介したメッシュ構成をサポートします。

AIRRECT Cloudメッシュネットワークの利用上の注意と特徴

●AIRRECT Cloudは、ロケーションではなく、グループに対してのみメッシュをサポートします。フォルダにメッシュプロファイルを作成することはできません。

●メッシュネットワークを初めてセットアップする際、メッシュネットワークを利用するすべてのアクセスポイントがAIRRECT Cloudに接続されている必要があります。

●メッシュネットワークが機能するにはルートノードがアクティブで常に使用可能である必要があります。

●メッシュ内のアクセスポイントは自動的にパスを見つけ、最適なルートノードに接続します。個々のアクセスポイントが起動すると、メッシュネットワークが起動して実行されるまでに時間がかかります。

●メッシュアクセスポイントは、ルートノードが到達可能かどうかを定期的にチェックします。到達可能でない場合は、ルートノードへの別のパスを自動的に設定します。

●メッシュリンクの場合、重複しないチャネルが多いため5GHz帯域を使用することを推奨します。

メッシュアクセスポイントの前提条件

メッシュネットワークを設定する前に、メッシュに参加しているアクセスポイントが以下の前提条件を満たしていることを確認する必要があります。

●メッシュアクセスポイントでは、バックグラウンドスキャンをオフにする必要があります。バックグラウンドスキャンは、グループのメッシュプロファイルを有効にすると自動的にオフになります。

●メッシュ内のアクセスポイントの場合、メッシュリンクに使用する帯域でチャネル選択を手動に設定する必要があります（メッシュリンクには5GHz帯域を使用することを推奨します）。[**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]で、[**チャンネル選択**]を[**手動**]に設定し、アクセスポイントがメッシュリンクの設定に使用するチャネルを選択します。

●メッシュは、動的周波数選択（DFS）チャネルでは動作できません。メッシュアクセスポイントに5GHzチャネルを選択するときは、それがDFSチャネルではないことを確認してください。

●メッシュプロファイルは、基本的に特別な種類のSSIDであり、メッシュ構成を備えています。メッシュネットワークに参加するために、つまり、メッシュプロファイルを有効にするために、アクセスポイント無線は最大6つの他の（非メッシュ）SSIDを実行できます。したがって、アクセスポイントを5GHz帯域メッシュの一部にする場合、最大6つの他の（メッシュ以外の）5GHzSSIDを実行できます。

●グループごとに有効にできるメッシュプロファイルは1つだけです。

メッシュネットワークの設定

メッシュネットワークを設定するには、アクセスポイントを展開する前に、参加しているすべてのアクセスポイントでメッシュプロファイルを有効にし、ルートノードを定義する必要があります。定義した後に、それらをそれぞれの場所に展開してルートノードを接続できます。

展開前の初期設定の手順は以下のとおりです。

1. 参加しているすべてのアクセスポイントを有線ネットワークに接続し、AIRRECT Cloudに接続します。メッシュプロファイルを有効にするまで、すべてのメッシュアクセスポイントを有線ネットワークに接続したままにします。
2. [**システム**]>[**ナビゲーター**]>[**グループ**]に移動し、[+]アイコンをクリックして、メッシュネットワークのグループを作成します。メッシュプロファイルを作成するには、最初にグループを作成し、そのグループにメッシュアクセスポイントを追加してから、メッシュプロファイルを作成する必要があります。
3. [**モニター**]>[WiFi] >[**アクセスポイント**]で、メッシュに追加するアクセスポイントを選択し、右クリックして[**グループに割り当て/再割り当て**]を選択、作成したグループにメッシュアクセスポイントを追加します。
4. ルートノードとして使用するアクセスポイントを決定します。これらのアクセスポイントのMACアドレスを書き留めます。
5. 左側のナビゲーターで、作成したメッシュグループに移動します。[**構成**]>[Wi-Fi]>[**メッシュ**]で、[**メッシュプロファイルの追加**]をクリックします。

6. 次の表に示すフィールドを構成します。

パラメータ	概要
メッシュSSID名	アクセスポイント同士がメッシュ接続する際に使用するSSID名 ※クライアントが本SSIDに接続してもネットワークに接続することはできません。
メッシュ プロファイル名	システムの内部でメッシュプロファイルを識別するために使用。
最大ホップカウント	非ルートアクセスポイントとそのルートノード間のワイヤレスホップの最大数。最大許容値：8つ
最大ダウンリンク	アクセスポイントのダウンリンクアクセスポイントの最大数、つまりアクセスポイントが持つことができる「子」アクセスポイントの最大数。最大許容値：5つ
最小RSSI	アクセスポイントが相互にメッシュリンクを形成するために必要な最小RSSI

7. メッシュプロファイルを保存します。
8. [**構成**]>[Wi-Fi]>[**メッシュ**]に戻ります。メッシュプロファイルで[**有効化**]をクリックします。メッシュの有効化ウィザードが開きます。
9. メッシュの有効化ウィザードでは、メッシュネットワークを有効にするために必要な、アクセスポイントの構成手順を示します。例として、メッシュリンクに使用する周波数帯域とチャネルを選択するように求められます。ウィザードの手順は、メッシュアクセスポイントが満たす前提条件によって異なります。
10. ウィザードの最後の手順で、[**メッシュを有効にする**]をクリックします。
これにより、グループ内のアクセスポイントのメッシュモードがアクティブになります。この状態を確認するには、[**モニター**]>[WiFi]>[**アクセスポイント**]に移動し、[**メッシュモード**]列にこれらのアクセスポイントの「有効」が表示されていることを確認します。
※アクセスポイントは、メッシュが有効になっている場合に再起動します。そのため、[**メッシュモード**]列に「有効」と表示されるまでに時間がかかります（数分かかる場合があります）。アクセスポイントがメッシュモードであることを確認したら、VLANの輻輳を回避するために、非ルートアクセスポイントを有線ネットワークから切断することを推奨します（ただし、ルートノードはネットワークに接続したままにします）。
11. [**ルートノードの選択**]右側のパネルからルートノードを選択します。有線接続のアクセスポイントを選択し、ルートノードとして保存します。

注意：ルートノードとして保存するまで、ルートノードアクセスポイントを切断しないでください。

メッシュネットワークの展開と展開後について

メッシュネットワークを適切に計画している場合（カバレッジとアクセスポイントごとのメッシュリンクの数を考慮に入れる）、展開プロセスは簡単です。ルートノードを有線ネットワークに接続し、非ルートノードをメッシュリンクに形成することになっているアクセスポイントから最小RSSIの半径内に配置できます。その際、最大ダウンリンク値を超える「子」アクセスポイントを持つアクセスポイントがないことを確認してください。本機能は自己作動型で、且つ、自己修復型です。非ルートアクセスポイントは、最初とリンク障害が発生した場合の両方で、ルートノードへの最適なパスを自動的に見つけ出すことができます。

メッシュグループ構成への展開後の変更について、AIRRECT Cloudは構成をルートノードにプッシュします。次に、ルートノードはそれを非ルートノードにプッシュし、非ルートノードはそれを「子」アクセスポイントにプッシュします。

※Wi-Fiクライアントに使用させたいSSIDをメッシュグループに追加して、メッシュ内のすべてのアクセスポイントにプッシュされるようにする必要があります。

注意：メッシュ使用時、メッシュプロファイルは2つのSSIDスロットを占有します。そのため、有効にできるSSIDは12個となります。

2.6.11 トラフィックシェーピングとQoS

[**トラフィックシェーピングとQoS**]タブで、SSIDの帯域幅使用率とサービス品質（QoS）設定を最適化できます。

トラフィックシェーピング

アップロードおよびダウンロード帯域幅を制限できます。また、SSIDが許可する同時アソシエーション数を制限することもできます。

SSIDの設定方法によっては、ここで定義されたトラフィックシェーピングパラメータ以外のソースから帯域幅制限が発生する可能性があります。例えば、RADIUSサーバーを使用してアクセスポイント全体にネットワークポリシーを共有している場合、ユーザーはグループに分けられて各グループにポリシーが適用され、営業グループと開発グループとで異なる帯域幅制限がある場合があります。このような場合、帯域幅の制限はRADIUSサーバーの設定が優先されることがあります。アクセスポイントがRADIUSサーバーから値を取得しない場合、[**トラフィックシェーピングとQoS**]タブで定義された値が適用されます。

●SSID が帯域幅制御値を取得できるソースは以下が想定されます。

a) SSIDに外部キャプティブポータルを設定しており、そのポータルがRADIUSサーバーを使用してポリシーを伝達する場合

b) AIRRECT Cloudでキャプティブポータルを使用するようにSSIDを設定した場合）

c) 802.1xセキュリティを使ってSSIDの設定をした場合

d) [**トラフィックシェーピングとQoS**]タブで定義した値

通常、上記のソースの1つだけが適用されます。例えば、SSIDで外部キャプティブポータルを定義した場合、このSSIDのAIRRECT Cloud内のポータルは適用されません。例外として、RADIUSサーバーまたはキャプティブポータルが帯域幅制御値をアクセスポイントに渡さない場合、[**トラフィックシェーピングとQoS**]で定義された値が適用されます。

トラフィックシェービングでは、SSID ごとの同時アソシエーション数や、ユニキャストトラフィックのデータレートの最小値と最大値の間で制限できます。マルチキャスト、ブロードキャスト、管理トラフィックレート制御のパラメータを設定すると、アクセスポイントの基本レート、または、必須レートが設定されます。これは、ブロードキャスト/マルチキャストパケットが送信されるデータレートを制御するだけでなく、ビーコンが送信されるデータレートにも適用されます。
※アクセスポイントの基本レートを上げると、送信通信時間は減少しますが、有効なカバレッジエリアも減少します。クライアントでのアクセスポイントのカバレッジがそのデータレートに対して十分でない場合、クライアントに問題を引き起こす可能性があります。

[ユーザー1人あたりの帯域幅制御]では、ユーザーごとに帯域幅を制限します。ユーザーごとの帯域幅制御の設定に使用されるRADIUS属性は、ベンダー固有の属性であるIETF ID: 26に該当します。以下の表は、当社属性のRADIUS属性へのマッピングを示しています。当社のベンダーIDは396です。

当社からRADIUS - 帯域幅制御属性のマッピング

Panasonic属性	RADIUS属性
ユーザー1人あたりのダウンロード制限	5
ユーザー1人あたりのアップロード制限	6

サービスの品質（QoS）

サービス品質 (QoS)は、さまざまなタイプのトラフィックに割り当てられる優先順位を決定します。音声通話やオンラインゲームなどのアプリケーションについては、QoS優先度に基づいて適切な帯域幅を割り当てることで通信品質を向上させることが出来ます。

使用されている主なQoS標準は以下の通りです。

●サービスのタイプ（TOS）：旧バージョンのIPv4ヘッダーのフィールド3bitで優先度(IP precedence)を決定するIEEE802.1p内で定められた規格です。輻輳によって、いくつかのパケットを破棄する必要がある場合は、優先順位が最も低いパケットが最初に破棄されます。数値は0から7の値が割り当てられており、値が大きいほど優先度が高くなります。（優先度0が最も低い優先度であり、7が最も高い優先度）

●DiffServeコードポイント（DSCP）：QoS設定値を細分化するためにTOSフィールドを拡張し８ビットのフィールドで定義されています。DSCPの値は、0～63の値が割り振られています。

●802.1pサービスクラス：イーサネットフレームのフィールド

●802.11e Wi-Fi Multi Media（WMM）：トラフィックタイプに基づきMACレイヤの動作を変更する802.11拡張機能。

上記標準は、トラフィックをどのように分類するかという点で互いに異なっています。

[**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]において、設定された受付制御設定を適用する場合は、[**受付制御必須**]をクリックします。[**無線通信設定**]で構成されたWMM受付制御設定は、[**トラフィックシェーピングとQoS**]タブで構成されたQoS設定より優先されます。

[**SSID優先度**]を使用すると、優先するトラフィックのタイプ（バックグラウンド、ベストエフォート、ビデオ、音声）を選択できます。優先度のタイプは以下の2種類です。

●固定：SSIDで送信されるすべてのトラフィックに、802.1pまたはIPヘッダーで示される優先順位に関係なく、選択したSSID優先度を設定します。例えば、バックグラウンドに設定した場合、SSIDは音声およびビデオパケットもバックグラウンドトラフィックとして扱います。[**固定**]を選択すると、AIRRECT Cloudはダウンストリームマッピングをグレー表示します。これは、すべてのトラフィックが選択された優先度でマークされ、実行するダウンストリームマッピングがないためです。

●上限：SSIDのトラフィックの優先度を、選択した優先度を上限とする場合は、これを選択します。例えば、SSID優先度をベストエフォートに設定した場合、SSIDはバックグラウンド、ベストエフォートトラフィックをベストエフォートとして扱いますが、より優先度の高いビデオ、音声トラフィックは適用されません。
[**上限**]を選択した場合は、ダウンストリームトラフィックをDSCP、802.1p、またはTOSから選択、マッピングできます。アクセスポイントは、ダウンストリームトラフィックをWMMアクセスカテゴリにマッピングすることにより、トラフィッククラスマークを標準（DSCPなど）からサービス保証に変換します。これは、802.11e WMMがMACレイヤーの動作を誘発して適切なWi-Fi帯域幅を割り当てるためです。そのため、アクセスポイントは選択された標準（802.1p、DSCP、TOS）から優先度を抽出し、選択されたSSID優先度の最大値に従って、WMMアクセスカテゴリにマッピングします。ダウンストリームトラフィックの場合、マッピングは、DSCP値、TOS値、または802.1pアクセスカテゴリの最初の3ビット（クラスセレクター）に依存します。 唯一の例外は、DMM値46で、WMMアクセスカテゴリ「音声」にマッピングされます。

以下の表は、QoS規格におけるダウンストリームトラフィックのマッピングを示しています。AIRRECT Cloudでの設定は、0 (バックグラウンド)、1 (ベストフォート)、4 (ビデオ)、5 (音声)の4種類の設定ができます。

DSCP/ TOS/ 802.1pサービスクラス	802.11e/WMMアクセスカテゴリー
0 (バックグラウンド)	1 (バックグラウンド)
1 (ベストフォート)	0 (ベストフォート)
2 (エクセレントエフォート)	3 (ベストフォート)
3 (重要なアプリケーション)	4 (ビデオ)
4 (ビデオ)	5 (ビデオ)
5 (音声)	6 (音声)
6 (インターネットコントロール)	7 (音声)
7 (ネットワークコントロール)	7 (音声)

アップストリームマッピングの場合、802.1pとDSCP/TOSマーキングの両方を有効にできます。以下の表は、アップストリームトラフィックに使用されるマッピングを示しています。例えば、[音声]、[DSCP]を選択した場合、DSCP値は46でマッピングされます。

802.11e/WMMアクセスカテゴリ	802.1pサービスクラス	DSCP
0	1	0
1	0	10
2	0	18
3	2	0
4	3	26
5	4	34
6	5	46
7	6	48

トラフィックシェーピングの設定

トラフィックシェーピングは、ネットワークのアップロードとダウンロードの制限を設定し、クライアントアソシエーションの数やバンドステアリングなどを制限することで、ネットワーク帯域幅の効果的な利用に役立ちます。

トラフィックシェーピングとQoSを設定するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDを選択し、[**トラフィックシェーピングとQoS**]の順に移動します。
2. 無線ごとにSSIDにアソシエーションするクライアントの数を指定します。
   クライアントと接続できる最大数を指定する場合は、[**同時アソシエーションの最大数を次に制限**]をクリックし、クライアントの最大数を指定します。
3. SSID帯域幅制御、ユーザー1人あたりの帯域幅制御で、SSIDのアップロード/ダウンロード帯域幅やユーザーごとの帯域幅を指定します。アップロード帯域幅またはダウンロード帯域幅を1～1024Kbpsの範囲で設定できます。
4. 802.11bだけ対応した無線クライアントを利用する場合、[**802.11b レート**]を有効にする必要があります。
5. マルチキャスト、ブロードキャスト、管理レート制御で管理トラフィックのデータレートを指定します。デフォルトでは有効になっており、12Mbpsに設定されています。また、[**周波数帯ごと**]を選択することで、周波数帯ごとにデータレートを指定することも可能です。
6. ユニキャストレート制御で、クライアント通信の最小および最大データレートを指定します。指定するには、以下の手順を実行します。
   a) [**最小ユニキャスト・トラフィック・データ・レートを制限**]をクリックし、データレートを指定します。
   b) [**最大ユニキャストトラフィックデータレート**]をクリックし、[**最大ユニキャスト・トラフィック・データ・レートを制限**]でデータレートを指定します。

   最小および最大データレートの最大しきい値は54Mbpsです。すべてのクライアントにユニキャストトラフィックの指定された最大データレートを適用する場合は、[**802.11n以上を含むすべてのクライアントに適用**]をクリックします。
   これにより、11n以上のクライアントも54Mbps以上で通信を行わなくなります。
   また、[**周波数帯ごと**]を選択することで、周波数帯ごとにユニキャストレートを指定することも可能です。
7. [**保存**]をクリックします。

サービス品質 (QoS) の設定

サービス品質(QoS)は、さまざまなタイプのトラフィックに割り当てられる優先順位を決定します。ボイスオーバーIP、ビデオ、オンラインゲームなどのストリーミングマルチメディアアプリケーションの場合、サービスの保証は必須です。QoSの詳細内容については『トラフィックシェーピングとQoS』を参照して下さい。

サービス品質 (QoS) を設定するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDを選択し、[**トラフィックシェーピングとQoS**]の順に移動します。
2. 下方にスクロールして、[**QoS**]をクリックすると、QoS設定に必要なパラメータが有効になります。
3. [**WMM受付制御を強制**]をクリックします。
   このフィールドは、アクセスポイントに適用されるデバイステンプレートで構成された受付制御パラメータをネットワークに適用する必要があるかを指定します。受付制御パラメータは、[**無線通信設定**]で設定できます。
   注意：[**無線通信設定**]で構成されたWMM受付制御設定は、[**トラフィックシェーピングとQoS**]タブで構成されたQoS設定より優先されます。
4. 要件に応じて、音声、ビデオ、ベストエフォート、または、バックグラウンドを[**SSID優先度**]として選択します。
5. [**優先度のタイプ**]の[**固定**]または[**上限**]をクリックします。
   このSSIDのすべてのトラフィックを、802.1p、またはIPヘッダーに示されている優先度に関係なく、選択した優先度で送信する必要がある場合は、優先度タイプ[**固定**]を選択します。このSSIDのトラフィックが選択した優先度以下の優先度で送信できる場合、優先度タイプ[**上限**]を選択します。
6. [**優先度のタイプ**]が[**上限**]として選択されている場合、[**ダウンストリームマッピング**]が有効になるので、適切なマッピングタイプを選択します。優先度は選択したフィールド（802.1p、DSCP、TOS）から抽出され、選択したSSIDの最大値に従うダウンストリームトラフィックのワイヤレスアクセスカテゴリにマッピングされます。ダウンストリームマッピングの場合、マッピングは、DSCP値、TOS値、または802.1pアクセスカテゴリの最初の3ビット（クラスセレクター）に依存します。唯一の例外は、DSCP値46で、WMMアクセスカテゴリ 「音声」 にマッピングされます。
7. 要件に応じて、[**アップストリームマーキング**]オプションを選択します。
   ワイヤレスアクセスのカテゴリは、選択されたSSID優先度の最大の優先順位にマッピングされ、802.1pヘッダーとIPヘッダーに選択されたとおりに設定されます。
8. [**保存**]をクリックします。

2.6.12 SSIDスケジューリング

SSIDの有効期間を設定する場合、SSIDスケジュールを定義します。使用例として、ゲストSSIDを使用したイベントでの限定的な無線提供や、従業員のSSIDの使用を営業時間に制限することがきます。[**タイムスロットを選択**]を有効に設定すると、日（行）と時間（列）に分割された週のカレンダービューを表示します。

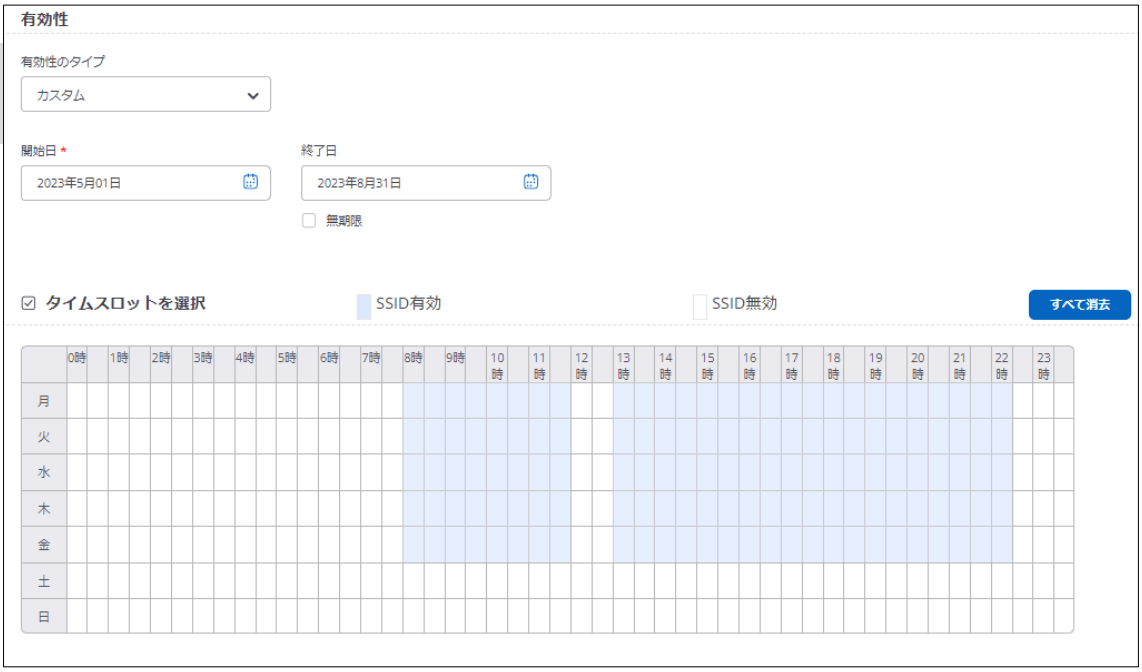
SSIDスケジューリングを構成する。

SSIDスケジューリング機能を使用すると、設定されているSSIDを利用可能にしたり、限られた時間だけ、または1日のうちの限られた時間だけアクティブにできます。
SSIDスケジューリングを構成するには、以下の手順をクリックします。

1. [**構成**]>[Wi-Fi]>[SSID]から任意のSSIDを選択し、[**SSIDスケジューリング**]の順に移動します。

2. SSIDを常時、または、特定の時間にアクティブにしておくかどうかに応じて、[**有効性のタイプ**]を[**現在から無期限**]または[**カスタム**]から選択します。[**現在から無期限**]を選択するとSSIDが常に有効になります。[**カスタム**]を選択すると、[**開始日**]および[**終了日**]フィールドが有効になります。
3. 有効性タイプとして[**カスタム**]を選択した場合は、[**開始日**]および[**終了日**]フィールドを指定することで、SSIDが有効になる期間を指定することができます。
4. [**タイムスロットを選択**]をクリックします。

5. タイムスロットはSSIDが有効化される期間/時間です。選択できる最小の期間/時間は30分です。時刻を表すマスをクリックして、有効化する時間を選択します。青色はSSID有効の期間/時間を示し、白色はSSID無効の期間/時間を示します。



6. [保存]をクリックします。

注意：SSIDを無効にした場合はこの機能が利用できません。そのため、スケジュールでSSID無効→有効の設定をしても、反映されずSSIDは出力されません。

2.6.13 Wi-Fi 7

SSIDメニューの[WiFi 7]**タブ**では、マルチリンクオペレーションの設定ができます。

マルチリンクオペレーション

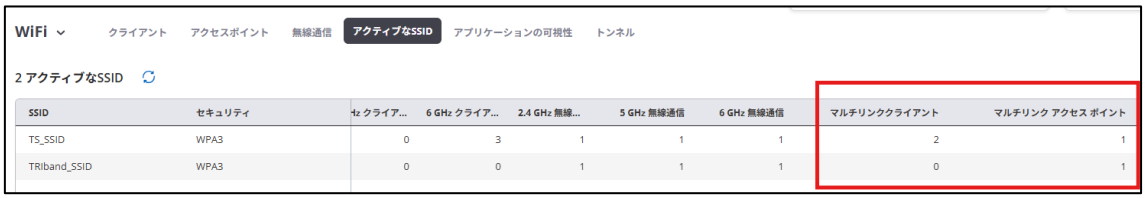
マルチリンク（複数の周波数帯に同時に接続）を有効化できるようになります。これにより、通信容量が拡大し通信速度が向上するほか、干渉波を受けても影響のない通信帯域を利用し、通信の安定化が期待できます。

マルチリンクオペレーションの設定

1．[**構成**]>[WiFi]>[SSID]に遷移します。
2．新しいSSIDを作成、または既存のSSIDを編集します。
3．[WiFi 7]タブを選択し、[**マルチリンクオペレーション**]のチェックボックスを選択します。
4．設定を保存します。

注意：無線設定を「802.11be」にしたWi-Fi 7対応アクセスポイントのみ対応。

アクティブなマルチリンクアクセスポイントとマルチリンククライアントは、[**モニター**]>[WiFi]>[**アクティブなSSID**] に移動して確認できます。



2.6.14 SSIDの有効化/編集

SSIDを有効にする

SSIDは以下の手順で有効にします。

1. 設定が完了した後、新しいSSIDを有効に設定するか、既存のSSIDを有効に設定することができます。
   - ●新しいSSIDを追加する場合、少なくとも3つの必須SSIDタブ（基本、セキュリティ、およびネットワーク）の構成が完了した後、[**SSIDを保存して有効にする**]をクリックします。
   - ●既存のSSIDを有効に設定する場合は、[**構成**] >[Wi-Fi]に移動し、カードビューで有効にするSSIDの [**オン/オフ**]スイッチをクリックします。[**SSIDを有効にする**]ダイアログウィンドウが表示されます。
2. SSIDの周波数帯を1つ、または複数選択し、[**SSIDを有効にする**]をクリックします。
   - ●SSIDの一部の機能は、[**構成**]>[**デバイス**]>[**アクセスポイント**]>[**全般的**]の[**バックグラウンドスキャン**]に依存しています。バックグラウンドスキャンを有効に設定していない場合、ダイアログウィンドウで有効化を求められます。バックグラウンドスキャンを有効にしなくてもSSIDをオンにすることはできますが、バックグラウンドスキャンに依存するSSIDの機能は正しく動作しない可能性があります。

SSIDを編集する

既存のSSIDを編集するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]に移動すると、[SSID]タブが表示されます。
2. カードビューで編集するSSIDの**編集アイコン**をクリックすると[**基本**]タブが表示されます。
3. [**保存**]をクリックして SSIDを保存するか、[**SSIDを保存して有効にする**]をクリックして保存してSSIDをオンにします。

SSIDを削除する

SSIDを削除するには、以下の手順を実行します。

1. [**構成**] >[Wi-Fi]に移動すると、SSIDタブが表示されます。
2. 削除したいSSIDのメニューアイコンをクリックし、[**削除**]をクリックします。SSIDを削除することを確認するダイアログが表示されます。
3. [**削除**]をクリックします。「SSIDが正常に削除されました」というメッセージが表示されます。

SSIDをコピーする

同じ場所、または、別の場所にSSIDのコピーを作成することができます。SSIDのコピーを作成するには、以下の手順を実行します。

1. [**構成**] >[Wi-Fi]に移動すると、SSIDタブが表示されます。
2. コピーしたいSSIDのメニューアイコンをクリックし、[**コピーを作成**]をクリックします。[**現在選択中のフォルダー**]または[**他のフォルダー**]にSSIDのコピーを作成するかどうかを尋ねるポップアップ・ダイアログが表示されます。
   - [**現在選択中のフォルダー**]を選択した場合、現在の選択しているロケーションにコピーされたSSIDが表示されます。
     ※現在の場所にコピーした際、SSIDプロファイル名は自動で変更されます。例えば「ABC Corp」を同じ場所にコピーすると、SSID名はそのまま「ABC Corp」になりますが、プロファイル名は「Copy of ABC Corp(1)」になります。
   - [**他のフォルダー**]を選択した場合、ロケーション階層が右側ウィンドウに表示されます。SSIDをコピーする場所を選択し、[**コピー**]をクリックします。

SSIDの優先度

APのファームウェアがバージョン20以前の場合、APは周波数ごとに最大8個のSSIDを出力します。
各周波数でSSIDを9個以上有効にしている場合、帯域ごとに8個のSSIDを優先設定することが出来るようになり、APは優先されているSSIDのみ出力します。

優先SSIDの設定

いずれかの周波数で9個目のSSIDを有効にすると、[**構成**]>[Wi-Fi]に[**SSIDを優先する**]ボタンが表示されます。クリックすると、優先SSIDのリストが表示されます。
優先SSIDのリストでは、SSIDが有効になっている周波数とSSIDが優先されている周波数が表示されます。優先SSIDを変更する場合、優先したいSSIDをリストにドラッグします。
優先SSIDが無効化された場合は、非優先SSIDのうち一番上にあるSSIDが自動的に優先SSIDになります。
また、デフォルトでは作成された日時が古いSSIDから優先SSIDになります。
注意：OWE移行モードに設定されたSSIDはリストの8番目に配置できません。

2.6.15 SSID属性のカスタマイズ

継承 SSID の一部設定内容をロケーション（フォルダー）ごとにカスタマイズできます。カスタマイズできる設定は、VLAN、RADIUS サーバー、トンネルエンドポイント、ロールプロファイル、SSID セキュリティパスフレーズです。

SSID属性をカスタマイズする

SSID 属性をカスタマイズするには、以下の手順を実行します。

1. 子フォルダーにて、**[構成]** >[Wi-Fi]>[SSID]に遷移します。
2. SSID プロファイルのメニューアイコン(⋮)をクリックし、**[SSID 属性をカスタマイズする]**をクリックします。
3. フォルダー名の右の**編集アイコン** をクリックして設定をカスタマイズします。
4. フォルダー名の右の**✓アイコン**をクリックして設定を保存します。

カスタマイズされた SSID は、青い点でマークされます。

2.7 RADIUS

[RADIUS]タブでRADIUSサーバを作成、編集、削除できます。

RADIUSサーバのIPアドレス、認証とアカウンティングのポート番号、およびアクセスポイントとRADIUSサーバ間の共有シークレットを定義できます。
任意のロケーションでRADIUSプロファイルを定義した後、その他の複数のロケーションでRADIUSプロファイルを適用することができます。例として、SSIDセキュリティ設定、またはSSIDキャプティブポータル設定で802.1x認証を使用する場合、ここで定義したRADIUSプロファイルの中から選択できます。また、SSID、従業員SSIDとゲスト用SSIDなど、異なるSSIDでも同じRADIUSプロファイルで異なる認証方式（従業員は802.1x、ゲストはWPA2-PSK、など）を使用できます。

2.7.1 RADIUSプロファイルの設定

RADIUSプロファイルの設定は、ロケーション階層で共有されます。特定のロケーションで定義されたRADIUSプロファイルは、そのすべての配下のロケーションで表示されます。RADIUSプロファイルリストは、カードグリッドビューレイアウトで使用できます。
RADIUS設定の構成に必要なパラメータの詳細については、『RADIUS設定パラメータ』を参照してください。
RADIUSプロファイル設定を構成するには、以下の手順を実行します。

1. [**構成**]>[**ネットワークプロファイル**]>[RADIUS]の順に移動します。
2. [**RADIUSサーバーを追加**]をクリックします。
3. [**RADIUSサーバー名**]フィールドに新しいRADIUSプロファイルの名前を指定します。
4. [**IPアドレス/FQDN（最大200文字）**]フィールドにサーバーのIPアドレス、またはFQDNを指定します。FQDNの文字数は最大200文字までです。
   注意：ホスト名で設定されたRADIUSサーバーは、キャプティブポータルでは使用できません。
5. [**認証ポート**]フィールドで、認証RADIUSサーバーのポート番号を指定します。
6. [**アカウンティングポート**]フィールドで、アカウンティングRADIUSサーバーのポート番号を指定します。
7. [**共有シークレット**]フィールドで、共有シークレットを指定します。目のアイコンで表示/非表示を切り替えることができます。
8. [**保存**]をクリックします。

RADIUS設定パラメータ

以下の表に、**RADIUS設定**パラメータに関連する情報を示します。

パラメータ	概要
RADIUSサーバー名	RADIUSプロファイル名を設定します。
IPアドレス	RADIUSサーバのIPアドレス、またはFQDNを設定します。
認証ポート	RADIUS（認証・認可）通信の宛先通信ポートを設定します。デフォルトは1812です。
アカウンティングポート	RADIUS（アカウンティング）通信の宛先通信ポートを設定します。デフォルトは1813です。
共有シークレット	RADIUSサーバとアクセスポイント間における共有シークレットを設定します。
RadSec	RadSecを使用する場合には「ON」を選択します。
RadSecポート	RadSecの宛先通信ポートを設定します。デフォルトは2083です。
CA証明書を追加	RadSecサーバ証明書を追加します。
証明書タグ	証明書タグ（TLSデバイス証明書）を選択します。

RADIUSプロファイルを編集する。

既存のRADIUSプロファイルは、作成されたロケーションで編集できます。親ロケーションで作成されたプロファイルで行われた変更は、子ロケーションで継承されたプロファイルに反映されます。

RADIUS設定の編集に必要なパラメータの詳細については、『RADIUS設定パラメータ』を参照してください。

RADIUSプロファイルを編集するには、以下の手順を実行します。

1. 編集するRADIUSプロファイルのオプションタブをクリックします。
2. [**編集**]をクリックします。
   a) プロファイルが作成された場所にいる場合は、手順3に進みます。
   b) 子ロケーションにいて、プロファイルが継承されたプロファイルである場合は、以下のいずれかを選択します。
   - ●[**親フォルダに移動して編集**]を選択：手順3に進みます
   - ●[**コピーを作成して続行**]を選択：子ロケーションに編集可能な複製プロファイルが作成されます。

3. 変更を行い、[**保存**]をクリックします。

RADIUSサーバーのコピーを作成する

既存のRADIUSサーバーは、同じロケーションまたは別のロケーションにコピーできます。コピーされたプロファイルには、元のプロファイルの名前と構成されたプロパティが含まれています。親ロケーションに作成されたサーバーのコピーは、子ロケーションにも存在します。

既存のRADIUSサーバーのコピーを作成するには、以下の手順を実行します。

1. コピーするRADIUSサーバのオプションタブをクリックします。
2. [**コピーを作成**]をクリックします。
3. RADIUSサーバをコピーする場所に応じてオプションを選択します。
   - ●[**現在選択中のフォルダー**]を選択すると、RADIUSサーバーが現在のロケーションにコピーされます。
   - ●[**他のフォルダー**]を選択すると、画面右に[**コピーを作成**]ウィンドウが表示されます。ロケーションを選択し、[**コピー**]をクリックします。

RADIUSプロファイルを削除する

RADIUSプロファイルは、削除オプションを使用して削除できます。削除されたプロファイルは、特定のロケーションとその子ロケーションからも完全に削除されます。継承されたプロファイルは、子ロケーションから削除できません。プロファイルは作成されたロケーションでのみ削除できます。

注意：SSIDで現在使用されているRADIUSプロファイルは削除できません。RADIUSプロファイルを削除する前に、SSID設定からRADIUSプロファイルを無効にするか削除する必要があります。

RADIUSプロファイルを削除するには、以下の手順を実行します。

1. 削除するRADIUSプロファイルのオプションタブをクリックします。
2. [**削除**]をクリックします。
3. 以下のロケーションに依存するアクションを実行します。
   - ●RADIUSプロファイルを作成したロケーションにいる場合、[**削除**]をクリックします。
   - ●子ロケーションにいて、削除するプロファイルが継承されたプロファイルである場合は、[**親フォルダーに移動して削除**]をクリックします。
8. [**削除**]をクリックします。

2.8 トンネルインターフェイス

トンネルインターフェイスは、SSID上のネットワークトラフィックを単一の集約ポイント、または、エンドポイントとの間でルーティングするために使用されます。例えば、分散型エンタープライズネットワークは、リモートロケーションから本社にWi-Fiトラフィックをチャネリングして、検査、ポリシーの適用、コンプライアンスの順守を行うことができます。AIRRECT Cloudは、以下のタイプのトンネリングプロトコルをサポートしています。

●**EoGRE**：Ethernet over GREを表します。詳細については、『EoGRE』を参照してください。

●**EoGRE over IPSec**：イーサネットフレームがカプセル化されているEthernet over GRE over IPsecを使用し、IPsecを使用して暗号化します。
詳細については、『EoGRE over IPsec』を参照してください。

●**VXLAN**：仮想拡張LAN（VXLAN）は、データセンターなどの大規模なネットワーク展開における VLANの制限されたスケーラビリティを解決します。
詳細については 『VXLAN』を参照してください。

●**VxLAN over IPSec**：IPSecで暗号化されたデータをVxLAN経由で転送することができます。詳細については 『VXLAN』を参照してください。

L3トンネル（IPSecを使用するVPN）については、『リモートアクセスポイント』を参照してください。

2.8.1 トンネルインターフェースの機能概要

EoGRE

汎用ルーティングカプセル化(GRE)は、IPインターネットワーク上の仮想ポイントツーポイントリンク内のさまざまなネットワークレイヤープロトコルをカプセル化できるトンネリングプロトコルです。イーサネット・オーバー・GRE(EoGRE)は、イーサネットフレームをカプセル化し、アクセスポイントからルーターなどの集約デバイスへの複数のEoGREトンネルを設定する機能です。

クライアントが送信するパケットには、以下のものが含まれます。

●Inner Eth

- ソース: クライアントMAC / 宛先 : ゲートウェイMACアドレス

●Inner IP

- ソース: クライアントIP / 宛先: クライアントがデータに到達しようとしている宛先を表します。アクセスポイントはこのパケットに、以下の内容を追加します。

  ●SSID VLAN (オプション) - VLAN IDがSSIDで構成されている場合は、パケットに追加されます。

  ●GRE - すべてのフラグが0に設定されています。ネイティブイーサネットのイーサタイプを0x6558に設定します。

  ●外部IPソース - アクセスポイントのIP/トンネルエンドポイントのIPを表します。

  ●N/W VLAN (オプション) - トンネルにVLANが構成されている場合、パケットに追加されます。

  ●外部Ethソース - アクセスポイントMAC /宛先 : ネクストホップのMACを表します。パケットレイアウト例を以下に示します。

```
⊞ Frame 7978: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits)
⊞ Ethernet II, Src: f2:e0:47:9f:00:7f (f2:e0:47:9f:00:7f), Dst: Cisco_40:e6:7f (00:0a:b8:40:e6:7f)
⊟ 802.1Q Virtual LAN, PRI: 6, CFI: 0, ID: 127
⊞ Internet Protocol Version 4, Src: 192.168.62.43 (192.168.62.43), Dst: 192.168.61.252 (192.168.61.252)
⊞ Generic Routing Encapsulation (Transparent Ethernet bridging)
⊞ Ethernet II, Src: Apple_89:07:8c (8c:fa:ba:89:07:8c), Dst: IcannIan_00:10:01 (00:00:5e:00:10:01)
⊞ Internet Protocol Version 4, Src: 192.168.66.33 (192.168.66.33), Dst: 8.8.8.8 (8.8.8.8)
⊞ User Datagram Protocol, Src Port: 58361 (58361), Dst Port: 53 (53)
⊞ Domain Name System (query)
```

EoGRE over IPsec

IPSec上のEoGRE(EoGRE over IPSec)は、GREトンネルを通過するイーサネットパケットにセキュリティを提供する方法です。汎用ルーティングカプセル化(GRE)はデータパケットをカプセル化しますが、IPSecはさまざまな暗号化方法を使用して、そのようなカプセル化されたデータパケットのセキュリティを保証します。IPSecを使用すると、盗聴や変更からクライアントの機密情報を保護するために、GREパケットにセキュリティの追加レイヤーが追加されます。

GREパケットは、次の2つのフェーズで保護されます。

●フェーズ1：エンドポイント間で共有されるキーの認証と検証に使用されるさまざまなセキュリティメカニズムについて説明します。

●フェーズ2：パケットのペイロードを暗号化して、なりすましや改ざんの可能性のある脅威から高レベルのプライバシー、機密性、およびセキュリティを提供するさまざまな方法について説明します。

注意：スループットを低下させないため、フェーズ1とフェーズ2で以下のデフォルトの暗号組み合わせを推奨します。

●Aes-128-sha1-modp1024

●Aes-128-sha2_256-modp1024

●Aes-256-sha1-modp1024

●Aes-256-sha2_256-modp1024

VXLAN

VXLANは、データセンターネットワークなどの大規模なネットワーク展開におけるVLANの制限されたスケーラビリティを解決するために開発されました。VXLANによって、物理ネットワークの上に仮想ネットワークが構成されます。仮想ネットワークは 「オーバーレイ」 と呼ばれ、仮想ネットワークが実行される物理ネットワークインフラストラクチャは「アンダーレイ」 と呼ばれます。VXLANに参加するスイッチとルーターには、VTEPと呼ばれる特別なインターフェイスがあります。VTEPは、アンダーレイとオーバーレイ間の接続を提供します。VXLANトンネルを移動するイーサネットフレームは、送信元ホストでIP、および、UDPヘッダーにカプセル化され、宛先クライアントでカプセル化が解除されます。

当社のアクセスポイントとスイッチングハブはVXLANをサポートし、Wi-Fiアクセスポイントから中央集約ポイント（スイッチなど）へのデータのトンネリングを可能にします。これにより、企業は、基盤となるキャンパスネットワークの設計変更を行うことなく、既存のコントローラーベースのWi-Fiネットワークをクラウドアーキテクチャに移行できます。

MSSクランピング

パス最大伝送ユニット（MTU）とは、ネットワークパスに沿ったスイッチとルーターのMTU値の最小値です。基本的に、パスに沿って移動するパケットの最大許容サイズを決定します。企業ネットワークでは、Wi-Fiトラフィックを有線エンドポイントにトンネリングすることがよくあります。TCPセッションがトンネリングされると、各プロトコルレイヤーにヘッダーが追加されるため、各パケットのフレームサイズは50～200バイト増加します。そうすると、新しいフレームサイズはMTUトンネルよりも大きくなる可能性があるため、パケットをフラグメント化するか、ジャンボフレームに結合する必要があります。ただし、どちらの方法でも、トンネルネットワークで問題を引き起こす可能性があります。トンネルエンドポイントでは、フラグメンテーションやリアセンブリをサポートしていない可能性があり、また、アンダーレイネットワークには、ジャンボフレームをサポートしていない可能性があります。

アクセスポイントはトンネルネットワークの最大セグメントサイズ(MSS)クランプをサポートしており、アクセスポイントは、MSSをトンネル最大伝送ユニット(MTU)値よりも低い値に最適化します。これにより、トンネルを流れるパケットがMTUトンネルのサイズを超えないようにします。Wi-Fiクライアントが、MTUトンネルより大きいMSSを使用してTCP接続をセットアップしようとすると、アクセスポイントはTCP Syn、および、Syn-AckメッセージのMSS値を変更して、パケットサイズが超えないようにします。詳細は『アクセスポイントがMSSを計算する方法』を参照してください。

2.8.2 トンネルインターフェイスの構成

トンネルインターフェイスは、設定されたSSIDからのネットワークトラフィックをリモートエンドポイントにルーティングするためのトンネルを表します。この機能を使用して、EoGRE、EoGRE over IPsec、または、VXLANトンネルを構成できます。特定のロケーションで定義されたトンネルインターフェイスプロファイルは、そのすべての子ロケーションで表示されます。トンネルインターフェイスプロファイルの作成は、以下の手順で設定できます。ここでは、VxLANトンネルの構成の追加について記述します。

1. [**構成**]>[**ネットワークインターフェース**]>[Tunnel]の順に移動します。
2. 画面右上の[**トンネルインターフェースを追加**]をクリックします.
3. [**プライマリエンドポイント**]を設定します。

4. オプションで[**セカンダリーエンドポイント**]を設定します。

5. トンネルインターフェースの設定を保存します。
6. [構成]>[Wi-Fi]>[SSID]に移動し、トンネルインターフェースを設定したいSSIDの[ネットワーク]タブから、作成したトンネルインターフェースのネットワークプロファイルを追加します。

5. 設定を保存し、トンネルが正常に作成されると、Wi-Fiネットワークカウンターでトンネルのアップ/ダウンステータスを確認できます。

MSSクランプを構成する

AIRRECT APは、自動または手動トンネルMTU経路探索をサポートしています。MSSクランプの設定は、以下の手順で実行します。

1. [**構成**]>[**ネットワークプロファイル**]>[Tunnel]の順に移動します。
2. [**トンネルのタイプ**]をクリックします。
3. [**MSSクランプ**]を有効にします。
4. [**トンネルMTU検出**]で[**手動**]、または、[Auto]をクリックします。手動の場合は、適切なトンネルMTU値を設定します。
5. [**保存**]で設定を保存したあと、[SSID]>[**ネットワーク**]タブで[**トンネル**]をクリックすると、このトンネルインターフェイスをSSIDに追加できます。

アクセスポイントがMSSを計算する方法

トンネルMTU (TMTU)= 1550バイトと仮定します。

[**トンネルMTU検出**]が[**自動**]、または、[**手動**]のどちらに設定されているかに応じて、アクセスポイントが検出する値（自動）、または、UIで構成された値（手動）になります。

MSSは以下の計算式で求められます。

MSS = TMTU - { (TUNNEL_HDR) + (IPHDR + TCPHDR) }

オーバーレイとアンダーレイの両方のトラフィックがIPv4の場合

TUNNEL_HDR = eth + ipv4 + udp + vxlan = 50 bytes

TCP + IPv4ヘッダー = (20 + 20) = 40 bytes

となるので、MSS値は 1550 - {（50）+（20 + 20）} = 1460です。

これは、アクセスポイントがクライアント接続を最適化する値です。

トンネルインターフェイス・パラメータ

次の表は、トンネルインターフェイス・プロファイルの構成に必要な情報を示しています。

パラメータ	概要
トンネルインターフェイス名	トンネルインターフェイス・プロファイルの名前を表します。
トンネルのタイプ	EoGRE、EoGRE over IPSec、VXLANから適切なネットワークトンネルタイプを選択します。
プライマリエンドポイントパラメータ	
リモートエンドポイント（IP/ホスト名）	プライマリーリモートサーバーまたはエンドポイントのIPアドレスまたはホスト名を表します。
ローカルエンドポイントVLAN	トンネル・トラフィックにタグ付けされるVLAN IDを表します。0～4094の値を入力する必要があります。
セカンダリエンドポイントパラメータ	
セカンダリエンドポイントを有効にする	セカンダリエンドポイントは、ワイヤレストラフィックが転送されるリモートエンドポイントです。プライマリエンドポイントがダウンした場合にセカンダリエンドポイントの設定が有効になります。
リモートエンドポイント（IP/ホスト名）	セカンダリ・リモートサーバーまたはエンドポイントのIPアドレスまたはホスト名を表します。
ローカルエンドポイントVLAN	トンネル・トラフィックにタグ付けされるセカンダリVLAN IDです。 0～4094の値を入力する必要があります。
プライマリエンドポイントを優先	アクセスポイントでプライマリトンネルの可用性をチェックする場合は、チェックボックスを選択します。プライマリエンドポイントに障害が発生した場合、トラフィックはセカンダリエンドポイントにブリッジされます。 このオプションがオンにすると、セカンダリエンドポイントはプライマリエンドポイントの可用性をチェックし、起動して実行されると、制御をプライマリエンドポイントに戻します。
スイッチイング・エンド・ポイントでクライアントの接続を切断	スイッチング・エンド・ポイントでのクライアント接続の切断を表します。

再試行パラメータ	
パラメータ	概要
ネットワークプローブ間隔	ping要求パケットを送信してリモートエンドポイントとの接続を確認する間隔（秒単位）を表します。設定範囲は10～3600です。間隔は10の倍数である必要があります。また、ネットワークPingのタイムアウトよりも大きくする必要があります。
ネットワーク・リトライ回数	リモートエンドポイントに送信するping要求パケットの数を表します。初期値は2です。
ネットワーク・タイムアウト	ping応答の待機時間（秒単位）を表します。初期値は10秒です。
EoGREパラメータ	
GREプライマリキー	オプション設定です。設定する場合、トンネルの両端で同じキーを使用する必要があります。
GREセカンダリキー	オプション設定です。設定する場合、トンネルの両端で同じキーを使用する必要があります。

2.8.3 IPSecトンネルの設定

IPSecトンネルおよび、VxLAN over IPSecの設定は、以下の手順で実行します。
※この設定では、IKEバージョン2のセキュリティアソシエーション（SA）プロトコルとESPのIPSecプロトコルによるトンネルモードと考えます。

1. [**構成**]>[**ネットワークプロファイル**]>[Tunnel]と進みます。
2. [**トンネルのタイプ**]を[EoGRE over IPSec]**または**[VxLAN over IPSec]に設定します。
3. [**リモートエンドポイント**(IP/**ホスト名**)]、[GRE**プライマリキー**]、[**ローカルエンドポイント**VLAN]など、プライマリエンドポイントの詳細を指定します。
4. プライマリエンドポイントが到達できなくなったときにアクセスポイントが通信できるように、セカンダリエンドポイントの詳細を指定します。トンネルがプライマリとセカンダリの間でどのように切り替わるかを理解するには、「トンネル型ネットワークでのフェイルオーバーの仕組み」を参照してください。

以下のフィールドは、セカンダリーエンドポイントの構成で設定します。
- [**ネットワークプローブ間隔**]：アクセスポイントがping要求パケットを送信して、リモートエンドポイントとの接続性を確認する間隔を秒単位で指定します。10～3600の値を定義できます。間隔は10の倍数で指定する必要があります。この値は[**ネットワーク・タイムアウト**]の値よりも大きい値である必要があります。
- [**ネットワーク・リトライ回数**]：アクセスポイントがリモートエンドポイントに送信するping要求の回数。初期値は2です。
- [**ネットワーク・タイムアウト**]：アクセスポイントがPingの応答を待つ時間（秒）を指定します。初期値は10秒です。

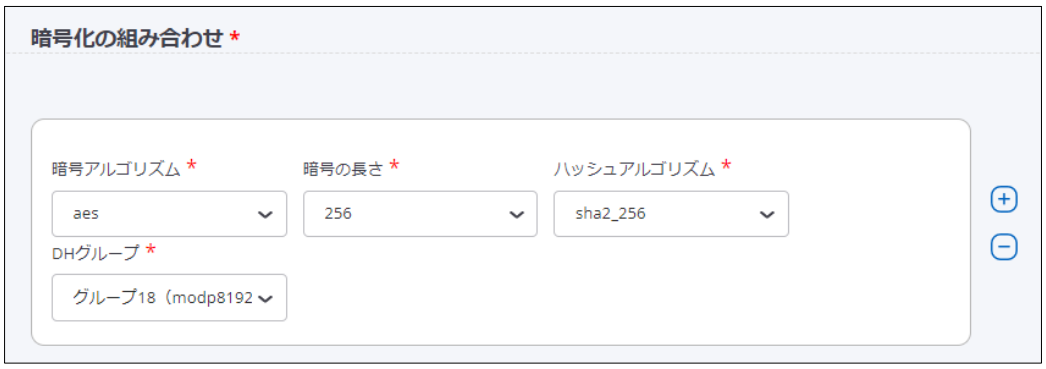
5. [IPSEC**を設定**]をクリックします。

6. [**モード**]を設定します。
7. GREトンネルの[**リモートエンドポイント(IP/ホスト名)**]を入力します。
8. [**バーチャルIPアドレスサポート**]のチェックボックスを選択します。このフィールドを選択すると、リモートエンドポイントは受信パケットに仮想IPアドレスを割り当てます。
9. [**フェーズ1パラメータ**]をクリックします。フェーズ1パラメータは、[**IKE設定**]と[**暗号化の組み合わせ**]で構成されています。
10. [**ライフタイム/IKEキープアライブ**]の値を指定します。
    - インターネット鍵交換(IKE)のキープアライブは、生成された鍵が有効である期間(時間)を表します。
    - 指定された時間が経過すると、新しい鍵が生成され、エンドポイント間で共有されます。
11. [**ローカル(左)**]と[**リモート(右)**]の認証方法と認証パラメータを選択します。使用できる認証方式はPSKとEAPです。認証パラメータは、PSKとEAPで異なります。

12. [暗号アルゴリズム]、[暗号の長さ]、[ハッシュアルゴリズム]、[DHグループ]の値を選択します。

注意：最大のスループットを得るためには、以下のいずれかの暗号の組み合わせを使用してください。他の暗号の組み合わせを使用すると、スループットが低下する可能性があります。

●aes-128-sha1-modp1024
●aes-128-sha2_256-modp1024
●aes-256-sha1-modp1024
●aes-256-sha2_256-modp1024



13. [**フェーズ2パラメータ**]をクリックします。[**フェーズ2パラメータ**]には、暗号の設定があります。
14. [**ライフタイム/フェーズ 2　キープアライブ**]の値を指定します。
15. [ESP]（セキュリティペイロードのカプセル化）、または、[AH]（証ヘッダープロトコル）を選択し、[**暗号アルゴリズム**]、[**暗号の長さ**]、[**ハッシュアルゴリズム**]、[**DHグループ**]の値を選択します。
16. [**MSSクランプ**]の値を指定します。
17. [**保存**]をクリックして、設定を保存します。

トンネル型ネットワークでのフェイルオーバーの仕組み

トンネル型ネットワークを介して通信を行う場合、可用性を維持し、アクセスポイントにトンネルの状態を伝える目的で、プライマリエンドポイントとセカンダリエンドポイントを設定します。それにより、アクセスポイントはプライマリエンドポイントに到達できない場合、セカンダリエンドポイントに接続することで、ネットワークのダウンタイムを解消します。

アクセスポイントは、ICMPリクエストとレスポンスを使用して、エンドポイントが到達可能かどうかを判断します。アクティブなクライアントを持つアクセスポイントは、リモートエンドポイントからカプセル化されたパケットを受信した場合、ICMPリクエストを抑制することができます。アクティブなクライアントを持たないアクセスポイントは、ICMPリクエストを抑制できない場合があります。

トンネル内のセカンダリエンドポイントを設定するには、[**ネットワークプローブ間隔**]、[**ネットワーク・リトライ回数**]、[**ネットワーク・タイムアウト**]のパラメータを使用します。アクセスポイントはこれらのパラメータを使用して、リモートエンドポイントが到達可能かどうかを検出します。アクセスポイントは、ネットワークプローブ間隔ごとにICMPリクエストを送信し、リモートエンドポイントからのICMPレスポンスを待ちます。ICMP応答がない場合、アクセスポイントは再試行し、[**ネットワーク・リトライ回数**]の値に基づいて再度ICMP要求を送信します。

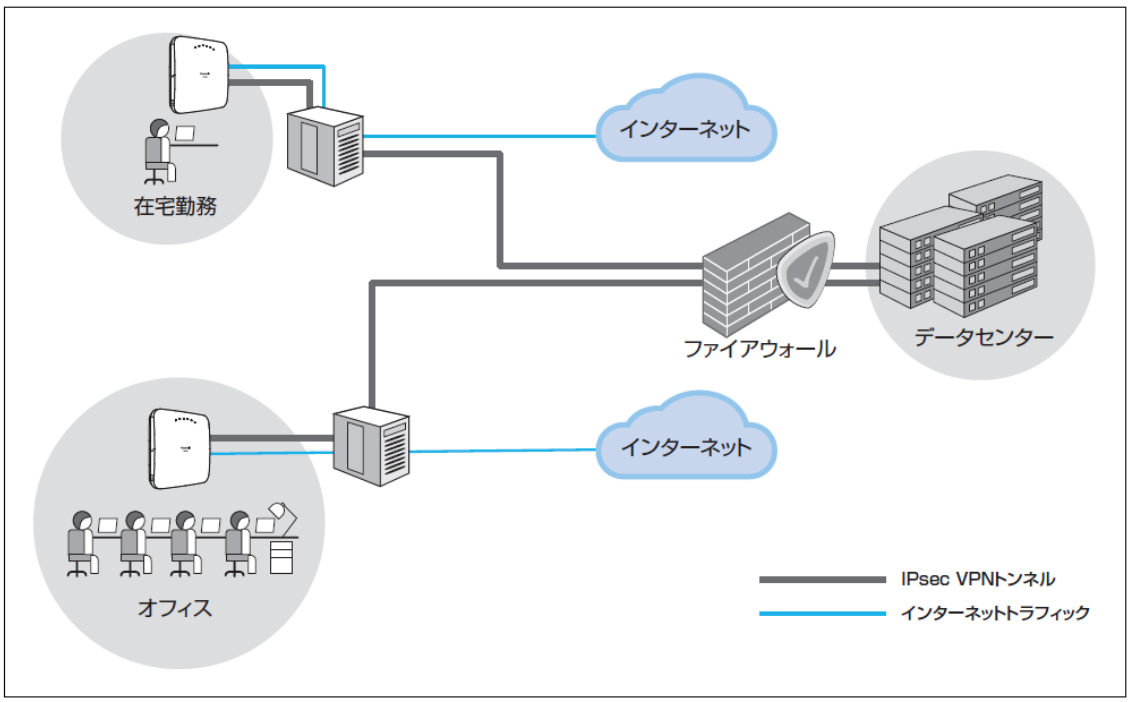
設定時に[**プライマリエンドポイントを優先**]パラメータを有効にしていた場合、プライマ

リエンドポイントがアクティブになるたびに、アクセスポイントはプライマリエンドポイントに切り替わります。例えば、アクセスポイントがプライマリエンドポイントとの接続を確立できず、セカンダリエンドポイントに切り替わったあと、プライマリエンドポイントが再び機能し始め、アクセスポイントが接続を確立できると、アクセスポイントはセカンダリエンドポイントから切断し、プライマリエンドポイントに切り替わります。

また、アクセスポイントは再起動するたびに、まずプライマリエンドポイントとの接続を確立しようとします。アクセスポイントがプライマリエンドポイントとの接続を確立できない場合、アクセスポイントはセカンダリエンドポイントに切り替わります。

2.8.4 リモートアクセスポイント

リモート・アクセスポイント（RAP）ソリューションにより、企業は在宅勤務者のホームオフィスや小規模な支社に設置したAIRRECT APにエンタープライズSSIDを拡張することができます。RAPソリューションは、業界標準のプロトコルを使用して、職場に設置されたリモートアクセスポイントと企業のデータセンターをインターネット経由で安全に接続します。ネットワーク管理者は、適切なセキュリティと設定でアクセスポイントを構成し、遠隔地の従業員にアクセスポイントを引き渡します。遠隔地の従業員は、自身の作業場にアクセスポイントを設置し、ブロードキャストされたエンタープライズSSIDに接続するだけです。アクセスポイントとリモートエンドポイント間のすべての通信は、安全なIPSec VPNトンネルを介して行われます。ネットワーク管理者は、必要に応じて各リモートアクセスポイントのVPNトンネルを削除することもできます。例えば、リモートの従業員が組織を辞めた場合、ネットワーク管理者は特定のリモートアクセスポイントのVPNトンネルを終了させ、リモートの従業員が企業ネットワークに接続できないようにすることができます。



リモートアクセスポイントの設定

リモートアクセスポイントは、以下の手順で構成できます。

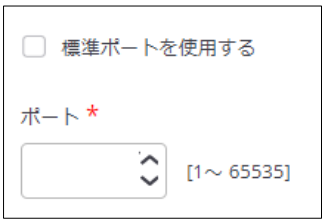
1. [**構成**]>[**ネットワークプロファイル**]>[Tunnel]を選択し、[**トンネルインターフェースを追加**]をクリックします。
2. [**トンネルのタイプ**]ドロップダウンリストから[**IPSecを使用するVPN**]を選択します。
3. プライマリサーバーとセカンダリサーバーのエンドポイントの詳細を入力します。

4. [**標準ポートを使用する**]チェックボックスをクリックし有効化すると、UDPに以下のIKEポートを使用します。

   ●ポート500（NATが検出されない場合）

   ●ポート4500（2つのエンドポイント間でNATが検出された場合）

   IKE接続用にカスタムポートを設定していて、それを使用したい場合は、[**標準ポートを使用する**]チェックボックスをオフにして、[**ポート**]フィールドにカスタムポート番号を指定します。



5. IPSec [**フェーズ 1 パラメータ**]と[**フェーズ 2 パラメータ**]の詳細を入力します。
※PANOSの場合、XAUTH認証のIKEバージョン1パラメータを設定する際には、[**ローカル (左) 識別子**]に16進数（16進数）の文字列のみを入力する必要があります。[**ローカル (左) 識別子**]フィールドに何らかのASCII文字列を入力すると、[Convert to Hex]テキストが表示されます。当テキストをクリックすると、16進数の文字列が変換されて[**ローカル (左) 識別子**]フィールドに表示されます。また、16進数文字列は必ず@#で始まる必要があります。当テキストをクリックすると、文字列の先頭に自動的に@#が付けられます。他のASCIIから16進数への変換ツールを使用している場合は、[**ローカル (左) 識別子**]フィールドに文字列を追加する前に、16進数文字列の先頭に@#を付けてください。

その他の IPSecパラメータの詳細については、『IPSecトンネルの設定』および『トンネルインターフェース・パラメータ』を参照してください。

各リモートアクセスポイントのIPSec認証情報の設定

各アクセスポイントのIPSec認証情報を設定する場合、この設定はトンネルプロファイルで定義されたIPSec認証情報よりも優先されます。
アクセスポイントごとにIPSec認証情報をカスタマイズすることにより、ネットワーク管理者は、リモートアクセスポイントとエンタープライズ・データセンターとの間のトンネルを無効化、または使用できないようにするオプションを提供します。例えば、リモートの従業員が組織を辞めた場合、ネットワーク管理者は認証情報を変更することでリモートアクセスポイントをブロックし、当該アクセスポイントがエンタープライズ・データセンターへのトンネルを作成できないようにすることができます。

各アクセスポイントのIPSec認証情報を設定するには、次の順に操作します。
1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順に移動します。
2. 該当のアクセスポイントを右クリックし[**カスタマイズ**]>[IPSec**認証情報**]を選択します。
3. 画面右側に表示される[IPSec**認証情報のカスタマイズ**]パネル内の[**カスタマイズ**]にチェックを入れ、[PSK]、または[XAuth/EAP]のいずれかの認証情報を入力します。

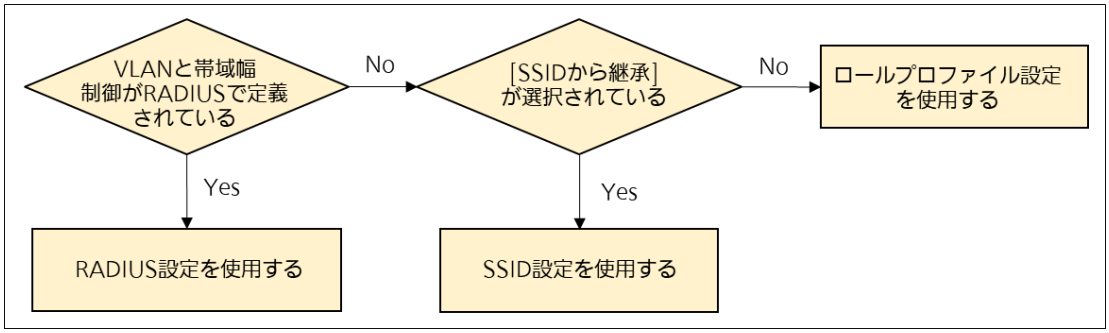
同様に、以下のナビゲーションを使って、各アクセスポイントの[IPSec**認証情報のカスタマイズ**]ページにアクセスすることもできます。
●[**モニター**]>[WIPS]>[**管理対象Wi-Fiデバイス**]
●[**フロアプラン**]

2.9 ロールプロファイル

ロールプロファイルは、ロールが割り当てられているユーザーのVLAN、ファイアウォール、帯域幅制御などの制限を定義します。ロールベースのアクセス制御(RBAC)を使用すると、ネットワーク管理者は割り当てられたロール、または、ユーザーが属するグループに基づいて、ネットワークリソースへのアクセスを制御できます。RBACには、ポリシーをネットワークに伝えるRADIUSサーバーが含まれることがあります。これらの設定（VLAN、ファイアウォールルール、帯域幅制御など）は、「ロールプロファイルの構成」以外でも設定することができます。

例：- [**構成**]>[Wi-Fi]>[SSID]>[**ネットワーク**]タブでSSIDのVLAN ID
- [**構成**]>[Wi-Fi]>[SSID]>[**アクセス制御**]タブでファイアウォールルール
- [**構成**]>[Wi-Fi]>[SSID]>[**トラフィックシェーピングとQoS**]タブで帯域幅制御値

SSIDタブでの設定と、[**ロールプロファイル**]タブに異なる設定がある場合は、以下の図に示すように、ロールがユーザーに割り当てられる優先順位に従います。



ロールプロファイルの構成における重要なポイント

●SSIDから継承：このオプションを選択すると、ロールプロファイルよりもSSID設定を優先させることができます。ただし、これらの設定がRADIUSサーバーで定義されている場合は、RADIUSサーバーの設定が常に優先されます。優先順位は、デフォルトではRADIUS、ロールプロファイル、SSID設定の順になります。
※[**SSIDから継承**]オプションを選択せず、ファイアウォールルールを指定していない場合、ロールプロファイル設定はSSID設定より優先されるため、SSID設定でルールを定義していてもファイアウォールルールはユーザーに適用されません。

●VLAN：この設定をロールプロファイルで構成しない場合、ロールには少なくとも1つのVLANが割り当てられている必要があるため、[**SSIDから継承**]オプションを選択します。[**SSIDから継承**]を選択しない場合、VLANを設定する必要があります。

●ユーザー帯域幅制御：ロールプロファイルで帯域幅制御を設定する場合、[SSID]>[**トラフィックシェーピングとQoS**]タブでユーザーごとの帯域幅制御を有効にする必要があります。

次の表は、ロールプロファイルがユーザーに適用されている場合の各設定の優先順位を示しています。

設定	SSIDプロファイル	ロールプロファイル	SSIDから継承	優先
VLAN	設定/未設定(※1)	設定	設定/未設定	ロールプロファイル
VLAN	設定	未設定	設定(※2)	SSIDプロファイル
帯域幅制御	設定/未設定	設定	設定/未設定	ロールプロファイル
帯域幅制御	設定	未設定	設定	SSIDプロファイル
帯域幅制御	設定	設定(※3)	設定	ロールプロファイル(※3)
帯域幅制御	設定	設定/未設定	未設定	ロールプロファイル
ファイアウォールルール	設定/未設定	設定	設定/未設定	ロールプロファイル
ファイアウォールルール	設定	未設定	設定	SSIDプロファイル
ファイアウォールルール	設定	設定(※4)	設定	ロールプロファイル(※4)
ファイアウォールルール	設定	設定/未設定	未設定	ロールプロファイル

(※1) SSIDにVLANが構成されていない場合、タグなしVLANを示す「0」が設定されます。

(※2) [**SSIDから継承**]を有効にしていない場合は、ロールプロファイルでVLAN設定を定義する必要があります。

(※3) ロールプロファイルでアップロード、または、ダウンロードのユーザー帯域幅制限を有効にしていても、数値を入力していない場合は、[SSID]>[**トラフィックシェーピングとQoS**]での設定値が適用されます。

(※4) ロールプロファイルでファイアウォールのルールを有効にしていても、設定を入力していない場合は、[SSID]>[**ファイアウォール**]での設定値が適用されます。

2.9.1 ロールプロファイルの構成

ロールプロファイルは、Wi-Fiユーザーにロールベースのアクセス制御を適用するために作成されます。ロールプロファイルは、特定の場所で定義されたすべての子ロケーションで表示されます。ロールプロファイルリストは、カードグリッドビューレイアウトで使用できます。
ロールプロファイルを作成するには、以下の手順を実行します。

1. [**構成**]>[**ネットワークプロファイル**]>[**ロールプロファイル**]の順に移動します
2. [**ロールプロファイルを追加**]をクリックします。
3. [**ロール名を入力**]フィールドにロール名を入力します。マッピングを容易にするために、RADIUSサーバで定義した名称と同じロール名を使用できます。
4. [**プロファイル名を入力**]フィールドにプロファイル名を入力します。
5. SSIDプロファイルで設定した定義をユーザーに適用する場合は、[**SSIDからの継承**]を選択します。
6. [**保存**]をクリックします。

ロールプロファイルでSSIDからの継承を構成する。
上記のすべての構成はSSIDプロファイルでも使用でき、SSIDプロファイルに接続するユーザーに適用されます。代替設定を強制したくない場合は、上記の1つ以上の設定のSSIDプロファイルから構成を継承することを選択できます。
例えば、SSIDプロファイルでファイアウォールルールを設定し、それをすべてのユーザーに適用する場合は、ロールプロファイルでこのオプションを選択でき、ロールプロファイルでファイアウォールルールを構成する必要はありません。

[**SSIDからの継承**]を設定するには以下の手順で行います。

1. [**構成**]>[**ネットワークプロファイル**]>[**ロールプロファイル**]に移動します
2. [**SSIDから継承**]を選択して、SSIDプロファイルからロール属性を継承します。
   オプションで、ロールプロファイルがロールベースの制御ルールに追加されているSSIDプロファイルからロールプロファイル設定を継承することを選択できます。
3. [**保存**]をクリックします。

ロールプロファイルでのVLAN設定

プロファイルが割り当てられているユーザーが、WLANネットワーク経由でアクセスできる複数のVLANを指定できます。

ロールがWi-Fiユーザーに割り当てられると、ロールプロファイルで構成されたVLAN設定は、SSIDプロファイルの設定より優先されます。この設定をロールプロファイルで構成しない場合は、[**SSIDから継承**]オプションを選択する必要があります。

SSIDプロファイル	ロールプロファイル	SSIDから継承	優先	備考
はい / いいえ	はい	はい / いいえ	ロールプロファイル	VLANが構成されていない場合、SSID、タグなしVLANを示す初期値0が設定されています。
はい	いいえ	はい	SSIDプロファイル	SSIDから継承せず、ロールプロファイルで有効になっている場合は、VLAN設定をロールプロファイルで構成する必要があります。

SSIDがロールプロファイルで有効になっていない場合、VLAN設定をロールプロファイルで構成する必要があります。

VLANを構成するには、以下の手順を実行します。

1. [**構成**]>[**ネットワークプロファイル**]>[**ロールプロファイル**]の順に移動します
2. [**VLAN**]セクションでは、VLANを有効に設定することができます。
3. ロールプロファイルがユーザーに割り当てられている場合に、ユーザーがアクセスできるVLAN IDを指定します。VLAN IDの範囲は0～4094です。スイッチポートのタグなしVLANにマッピングするには、スイッチでタグなしVLANにどんなVLAN IDが割り当てられているかに関係なく、VLAN ID = 0を入力します。
4. [**保存**]をクリックします。

ロールプロファイルでファイアウォールルールを構成する

以下の 2 つのファイアウォールルールを定義できます。

1. 特定のプロトコルを使用してホスト/IP：ポートへの通信を許可するか禁止するかを定義するレイヤー3/4ファイアウォールのルール。通信は、クライアントデバイスとの間で、または双方向で、ブロック/許可することができます。
2. 二番目のファイアウォールルールは、システムで定義された各アプリケーションカテゴリーの中で、クライアントデバイスがアクセスできるアプリケーションを定義するものです。このようなアクセスを許可/禁止するルールを定義できます。
   さらに、定義されたルールが適用されない場合にクライアントデバイスに適用する必要があるデフォルトのルールを定義できます。デフォルトのルールは、上記1,2のファイアウォールに共通です。

以下の表に、SSIDプロファイルとロールプロファイルの構成に基づき、ユーザーにロールプロファイルが適用されている場合のファイアウォールルールの優先順位を示します。

SSID プロファイル	ロール プロファイル	SSIDから継承	優先
はい/いいえ	はい	はい/いいえ	ロールプロファイル
はい	いいえ	はい	SSIDプロファイル
はい	はい	はい	ロールプロファイル SSIDプロファイル(※1)
はい	はい/いいえ	いいえ	ロールプロファイル(※2)

(※1) L3およびアプリケーションファイアウォール規則を有効にして構成できます。ファイアウォールのいずれかがで構成されていない場合、ロールプロファイル、次にSSIDプロファイルの対応する設定がユーザーセッションに適用されます。

(※2) L3およびアプリケーション・ファイアウォール規則を有効にして構成できます。ファイアウォールがロールプロファイルで構成されていない場合、ロールプロファイルで定義されたファイアウォールルールのみがユーザーセッションに適用されます。SSIDプロファイルで定義されているファイアウォールルールは、ユーザーセッションには適用されません。

ファイアウォールルールを構成するには、以下の手順を実行します。

1. [**構成**]>[**ネットワークプロファイル**]>[**ロールプロファイル**]の順に移動します。
2. [**ファイアウォール**]をクリックします。
3. [**レイヤー3/4ファイアウォールのルール**]を有効にして定義します。
4. [**アプリケーション・ファイアウォール規則**]を有効にして定義します。
   アプリケーションファイアウォールを有効にする場合は、SSIDプロファイルで[**アプリケーションの可視性**]をクリックする必要があります。
5. [**既定のルール**]セクションで、アクションを選択します。アクションは、[**許可**]、[**ブロック**]、[**許可してマーク**]のいずれかです。
6. [**保存**]をクリックします。

ロールプロファイルでのユーザー帯域幅制御の構成

帯域幅制御により、ユーザーが利用できるアップロードおよびダウンロード帯域幅に適用される制限を定義できます。これは1Kbpsから1024Mbpsまでの範囲です。

注意：ロールプロファイルで帯域幅制御を構成する場合は、SSIDプロファイルの[**トラフィックシェーピングとQoS**]セクションで[**ユーザーごとの帯域幅制御を有効にする**]を選択する必要があります。

以下の表は、SSIDプロファイルとロールプロファイルの構成に基づいて、ユーザーにロールプロファイルが適用されている場合の帯域幅制御構成の優先順位を示しています。

SSID プロファイル	ロール プロファイル	SSIDから継承	優先
はい/いいえ	はい	はい/いいえ	ロールプロファイル
はい	いいえ	はい	SSIDプロファイル
はい	はい/いいえ	いいえ	ロールプロファイル(※1)
はい	はい	はい	ロールプロファイル / SSIDプロファイル(※2)

(※1) 帯域幅制御では、アップロードとダウンロードの帯域幅を設定できます。これらの値のいずれかがロールプロファイルに設定されていない場合、ロールプロファイルで定義された値のみがユーザーセッションに適用されます。SSIDプロファイルで定義された対応する値はすべて無視されます。

(※2) 帯域幅制御では、アップロードとダウンロードの帯域幅を設定できます。これらの値のいずれかがロールプロファイルに設定されていない場合、SSIDプロファイルで構成された対応する値がユーザーセッションに適用されます。

ユーザー帯域幅制御を設定するには、以下の手順を実行します。

1. [**構成**]>[**ネットワークプロファイル**]>[**ロールプロファイル**]の順に移動します。
2. [**ユーザー帯域幅制御**]タブまでスクロールします。
3. [**ユーザー1人あたりの最大アップロード帯域幅を次に制限**]を選択して、アップロード制限を設定します。
4. アップロード制限値をMbps、または、Kbpsで入力します。ここに1～1024の値を入力する必要があります。
5. ダウンロード制限を設定するには、[**ユーザー1人あたりの最大ダウンロード帯域幅を次に制限**]を選択します。
6. ダウンロード制限値をMbps、または、Kbpsで入力します。ここに1～1024の値を入力する必要があります。
7. [**保存**]をクリックします。

ロールプロファイルでリダイレクトを設定する

リダイレクトを有効にすると、ロールが割り当てられているユーザーを指定したURL(WEBポータルサイト)へリダイレクトすることができます。ユーザーはリダイレクト先URLで承認されるまでネットワークへアクセスすることができません(ウォールガーデンを除く)。**ウォールドガーデン**については『ウォールドガーデン(承認前にアクセスできるWebサイト)とは』を参照してください。

リダイレクトを構成するには、以下を実行します。

1. [**構成**]>[**ネットワークプロファイル**]>[**ロールプロファイル**]の順に移動します。
2. [**リダイレクト**]をクリックします。
3. [**静的リダイレクト**]または[**動的リダイレクト**]をクリックします。

注意：リダイレクトURLをAIRRECT Cloudで設定する場合には[静的リダイレクト]、RADIUSサーバーで設定する場合には[動的リダイレクト]を選択します。

4. [**リダイレクトURL**]を入力します。
5. 通常、クライアントのHTTP通信を契機としてリダイレクトが実行されますが、HTTPS通信も契機としたい場合は、[**HTTPSリダイレクト**]を選択します。
   [**HTTPSリダイレクト**]を有効に設定すると、証明書情報の入力が必要となります。
   ●共通名：証明書に関連するホスト名
   ●組織　　：組織の名称
   ●組織ユニット：組織単位の名称
6. [**承認前にアクセスできる Web サイト**]を入力します。ここでは、ログイン前アクセスできるドメイン名を入力します。

注意：ユーザーがログイン前に[リダイレクトURL]へアクセスできる必要があるため、少なくとも[リダイレクトURL]は入力する必要があります。

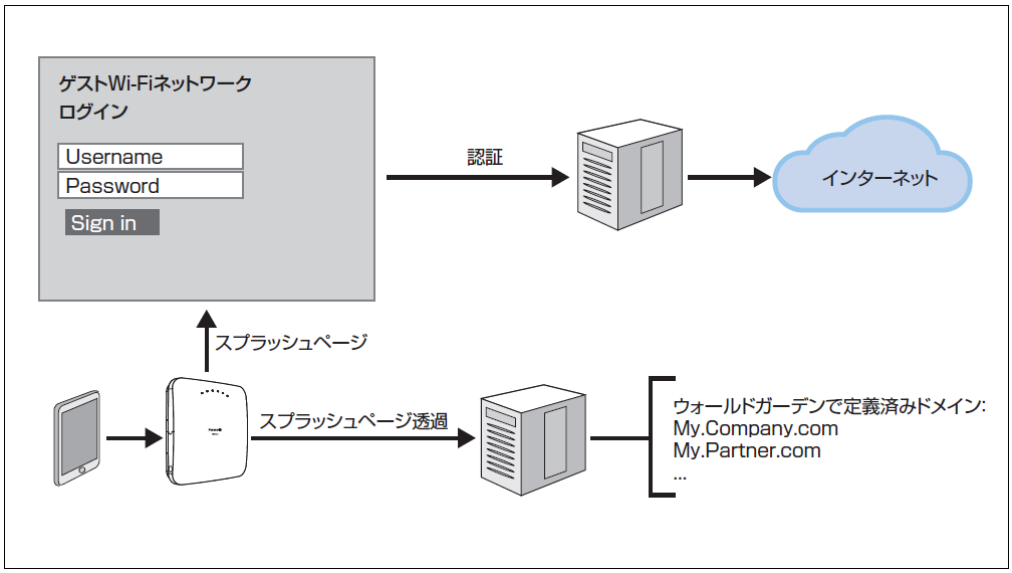
7. [**保存**]または[**SSIDを保存して有効にする**]をクリックします。

ウォールドガーデン(承認前にアクセスできるWebサイト)とは

ウォールドガーデンを使用することで、ユーザーのアクセス先の許可/拒否について制御することができます。ウォールドガーデンは、キャプティブポータル機能と組み合わせて使用できます。キャプティブポータル機能は、ユーザーがWi-Fiネットワークにログインするときにユーザーを認証する手段として使われます。SSIDで、キャプティブポータルが有効に設定されている場合、Wi-Fiアクセスが許可される前にユーザーへスプラッシュページが送信されます。スプラッシュページではWi-Fiアクセスを許可するための管理機能として、以下のような設定をおこなうことができます。

●利用規約への同意をユーザーに求めること
●Webベースのログインおよびパスワード画面を使用したユーザー認証の促進
●ソーシャルWi-Fi資格情報を使用したログインの促進

状況によっては、スプラッシュページのゲートキーピング機能をバイパスする必要があるケースがあり、このバイパス機能は、ウォールドガーデンによって使いやすくなります。ウォールドガーデン内に特定の宛先を定義すると、スプラッシュページをバイパスして、ユーザーが指定された宛先まで直接アクセス可能になります。



ロールプロファイルを編集する

既存のロールプロファイルは、作成された場所で編集できます。変更親の場所で作成されたプロファイルに加えられた変更は、子の場所で継承されたプロファイルに反映されます。

ロールプロファイルを編集するには、以下の手順を実行します。

1. 編集するロールプロファイルのオプションタブ⁞をクリックします。
2. [**編集**]をクリックします。
   - ●プロファイルが作成された特定の場所にいる場合は、手順3に進みます。
   - ●子の場所にいて、プロファイルが継承されたプロファイルである場合、適切なオプションを選択します。

オプション	概要
親フォルダに移動して編集	手順2を再度実行後、手順3を進みます。
コピーを作成して続行	重複するプロファイルが作成され、複製したプロファイルで手順2と手順3を実行して、子のロケーションでプロファイルを編集できます。

3. [**保存**]をクリックします。

ロールプロファイルのコピーを作成する

既存のロールプロファイルと継承されたプロファイルは、どちらも同じ場所、または、異なる場所にコピーできます。このプロセスでは、既存のロールプロファイルのコピーが作成されます。プロファイルのコピーには、元のプロファイルと同じ名前と構成済みのプロパティが含まれています。親の場所に作成されたプロファイルのコピーは、子の場所にも存在しますが、子から親へコピーされることはありません。

既存のロールプロファイルのコピーを作成するには、以下の手順を実行します。

1. 複製するロールプロファイルのオプションタブ⁞をクリックします。
2. [**コピーを作成**]をクリックします。
3. ロールプロファイルをコピーする場所に応じてオプションを選択します。

[**現在選択中のフォルダー**]を選択すると、ロールプロファイルが現在の場所にコピーされ、[**他のフォルダー**]を選択した場合は、[**コピーを作成**]ウィンドウから新しいロケーションを選択します。

1. [**コピー**]をクリックします。

ロールプロファイルを削除する

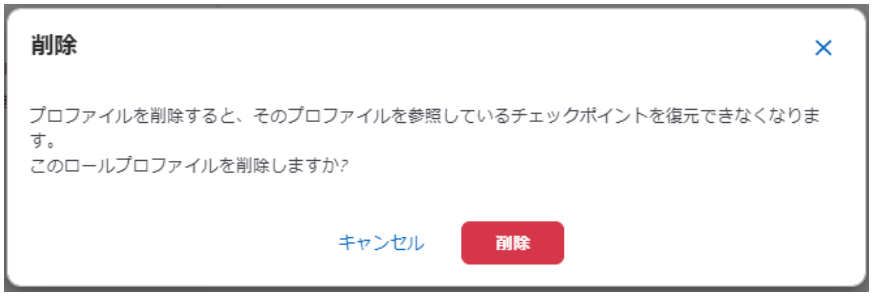
既存のロールプロファイルと重複するロールプロファイルは、どちらも削除オプションを使用して削除できます。削除されたプロファイルは、特定の場所とその子の場所からも完全に削除されます。継承されたプロファイルは、子の場所から削除できません。プロファイルは、作成された場所でのみ削除できます。

注意：SSIDで現在使用されているロールプロファイルは削除できません。ロールプロファイルを削除する前に、ロールプロファイルを無効にするか、SSID設定から削除する必要があります。

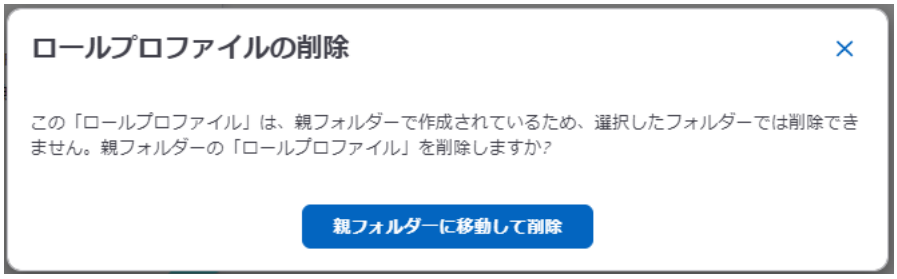
ロールプロファイルを削除するには、以下の手順を実行します。

1. 削除するロールプロファイルのオプションタブ（縦に3つ並んだドット）をクリックします。
2. [**削除**]を選択します。
3. 操作中のロケーションにより、以下の操作を実行します。

●ロールプロファイルを作成したロケーションにいる場合は、[**削除**]を選択します。



●「子」のロケーションにいて、削除するプロファイルが継承されたプロファイルである場合は、[**親フォルダーに移動して削除**]をクリックします。



この操作により、親ロケーションに誘導されます。

2.10 WiFi無線通信設定

[**構成**]>[**デバイス**]>[**アクセスポイント**]の[**WiFi無線**]タブでは、アクセスポイントの無線関連の設定を行います。デフォルトでは、ロケーションに適用される無線設定は、その子ロケーションに自動的に継承されます。子ロケーションの無線設定をカスタマイズして、親ロケーションと異なる設定にすることも可能です。
無線通信設定では、送信電力、クライアントステアリング、ロードバランシングパラメータ、および、アドミッション制御ポリシーなどを設定できます。

●2.4GHz、5GHz、6GHzタブを使用して、それぞれの帯域の無線設定ができます。チャネルは、Wi-Fi干渉が最小のチャネルを自動的に選択します(初期設定)。また、定期的により適切なチャネルを探し、必要に応じて動作チャネルを変更します。この期間は、[**選択間隔**]フィールドで指定できます。選択間隔ごとに1回、アクセスポイントは現在のチャネルのWi-Fi干渉が増加しているか確認し、増加している場合は Wi-Fi干渉が最小のチャネルに変更します。利用可能な候補チャネルの一部、または、すべてを選択できます。また、長期利用をすることでDFSによる問題を回避できるDFS履歴機能を有効化することが出来ます。これにより、使い勝手の悪かったW53、W56帯のチャネルを有効活用することができます。詳細については、『チャネル選択でDFS履歴を使用』をご参照ください。

●画面の下部にある[**クライアントステアリングの共通パラメータ**]リンクを使用すると、共通のパラメータ設定ができます。さまざまなタイプのクライアントステアリングが連携することで、クライアントのQoEを向上させます。例えば、スマートステアリングとバンドステアリングは、共通RSSIしきい値を基準として使用します。詳細については、「統合クライアントステアリングとは」を参照して下さい。

802.11ax設定の概要

無線通信における、Wi-Fi6 の機能を有効化、無効化することが出来ます。

●MU-MIMO：

MIMO とは、アクセスポイントやクライアントに複数のアンテナを使用することで、データレートの向上（空間多重化）と干渉の低減（空間ダイバーシティ）を実現することを指します。マルチユーザーMIMO（MU-MIMO）は、マルチアンテナストリームを使用して、複数のユーザーに同時にサービスを提供します。

●ダウンリンク MU-MIMO

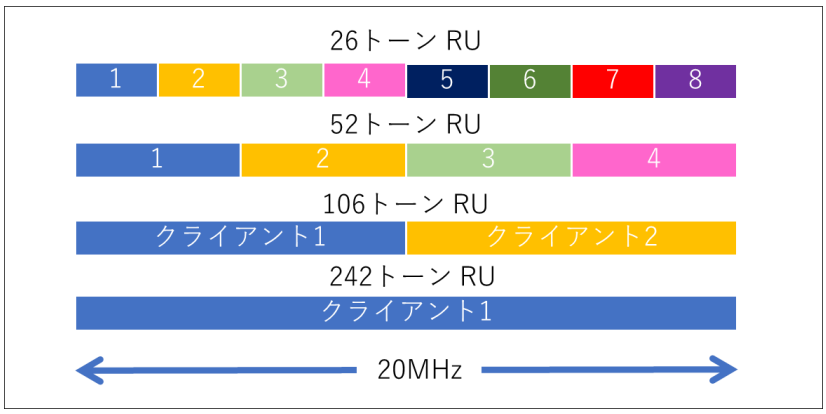
クライアントのチャネル状態に応じて、アクセスポイントはシングルユーザーMIMO（SU-MIMO）を使用して、クライアントのデータレート改善や、エラーレート低減ができます。高密度環境は、個々のユーザーデータレートだけでなく容量に関係するため、ダウンリンク MU-MIMO は、多数のユーザー間でリソース（ストリーム）を効率的に割り当てることにより、高密度環境で役立ちます。802.11ax は、8x8MIMO までをサポートするため、製品により最大 8 人のユーザーに同時にデータを送信できます。

●アップリンク MU-MIMO

アップリンク MU-MIMO は、SNS、ビデオ通話など、アップリンクを多用するアプリケーションで役立ちます。ダウンリンクと同様 SU-MIMO の場合と比較し容量を増やします。これにより、コンテンツをアップロードするときの通リン効率が向上します。

●OFDMA

直交周波数分割多元接続（OFDMA）は、Wi-Fi チャネルを「トーン」とも呼ばれるサブキャリア（それぞれ 78.125KHz 幅）に分割します。トーンは組み合わされて、異なる幅のリソースユニット（RU）を形成します。以下の図に示すように、RU は 26、52、106、または 242 のトーンで構成できます。これは、約 2MHz、4MHz、8MHz、および 20MHz のチャネル幅に対応します。各スケジューリング間隔で、OFDMA は 1 つ以上の異なる幅の RU を複数のユーザーに割り当て、チャネルの効率的で柔軟な運用を実現します。



●ダウンリンク OFDMA

統合的にクライアントの送信RUをスケジューリングし、割り当てます。802.11acまでは、20/40/80MHzチャネル全体が1つのRU（トーン242）で1人のユーザーに割り当てられており、最適化されていませんでした。本機能により、クライアント間でRUを分散し、必要に応じて各クライアントにRUを割り当て、または割り当てを変更することで、より効率的な通信を行います。リソースの割り当てとスケジューリングは、必要なアプリケーションQoSやRU条件などの要素に基づいています。

●アップリンク OFDMA

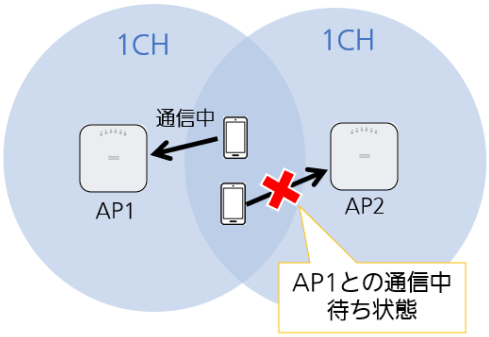
クライアントは送信スケジュールを調整できないためWi-Fiアップリンクは分散型の通信をします（ダウンリンクとは異なり、アクセスポイントはトランスミッターとスケジューラーの両方を担う）。802.11acまでは、クライアントはランダムに分散されたタイミングでパケットをアクセスポイントに送信します。この場合、多数のクライアントが存在する場合にアップリンクの帯域が足りなくなる可能性があります。本機能により、CSMA-CAを使用してメディアを確実に送信できるようにしながら、クライアント間の送信スケジュールを調整するメカニズムを介して、アップリンクリソースの割り当てを管理します。これにより、アップリンクの競合が減少し、ユーザーエクスペリエンスが向上します。

●Spatial Reuse(SR)

BSS Color 機能をより有効的に利用し、電波干渉を低減することができます。これまでの干渉回避方式の CSMA/CA は、同一チャネルが干渉している空間では、1 台しか送信ができないというデメリットがあります。そのため、エリア内の AP/クライアント密度が増加すると、無線帯域の利用効率が悪化し、遅延、切断などが発生してしまうことがありました。BSS Color は、自分の電波(BSS)と、他の AP の BSS を判別することによって、同時通信を実現する機能です。

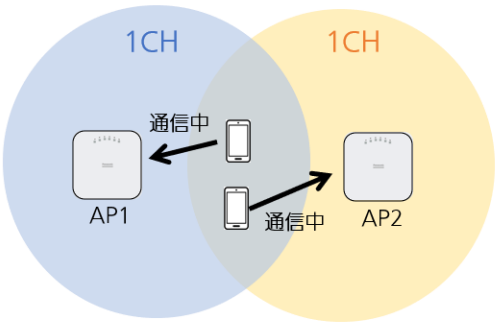
【CSMA/CA 方式】

同じチャネルのセルが被っている場合、別の AP への通信であっても待ち状態となってしまう。

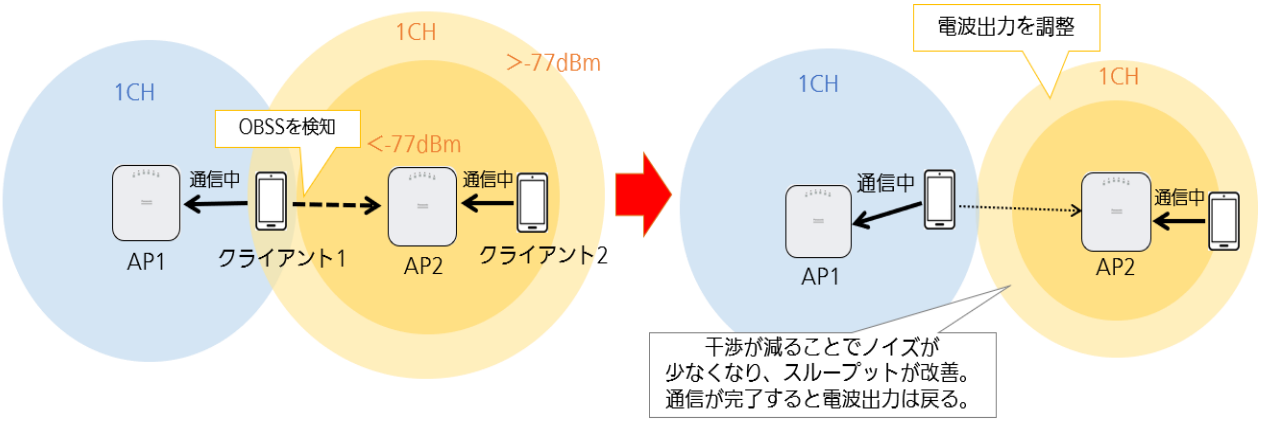


【BSS Color】

同一チャネルであっても、クライアントは同時通信が可能となる。

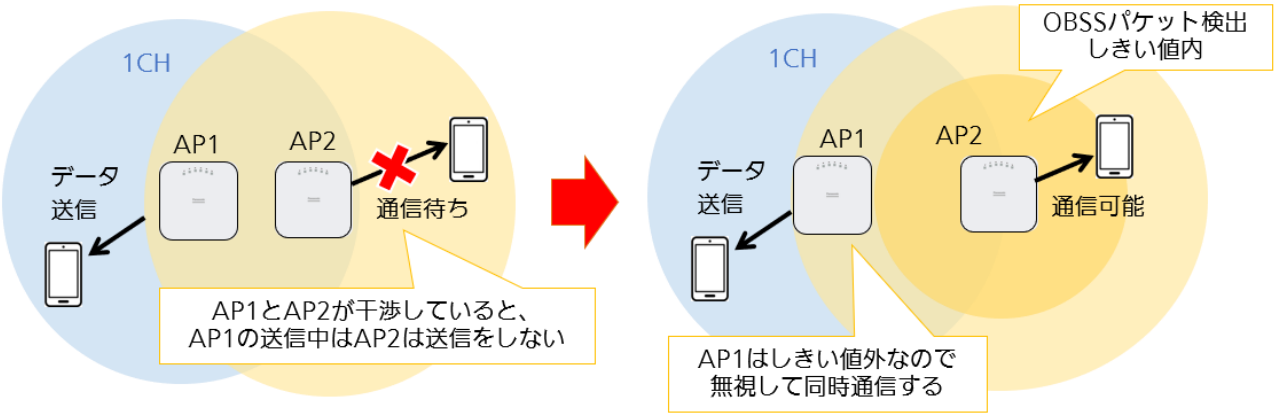


BSS カラーによって、同時通信は実現しますが、同じチャネル内に複数のクライアントが存在する場合はノイズの発生により通信品質が低下してしまいます。Spatial Reuse 機能では、クライアントの通信中に電波調整をすることで干渉を減らすことが出来る機能です。
下図のように、クライアント 1 が設定したしきい値(-77dBm)以上の OBSS(隣接する AP の BSS)を検知しているとき、クライアント 2 が通信を開始すると、クライアント 2 の通信中は AP2 の電波を抑えることでノイズを低減します。



OBSS パケットを検出するしきい値は IEEE802.11ax の規格により、-81～-62dBm の範囲で設定されるように定められており、デフォルト値で-77dBm となります。

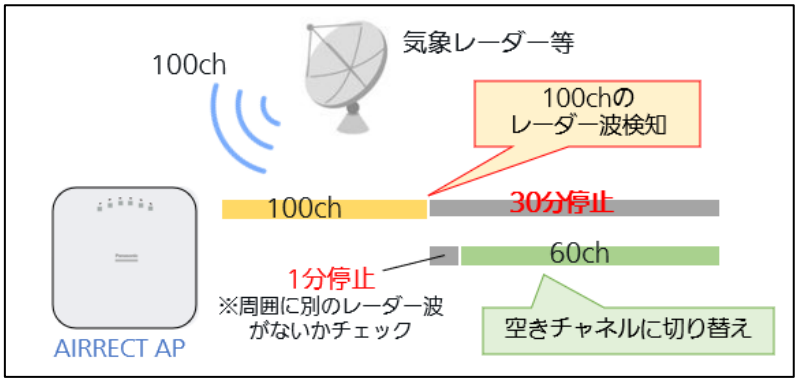
また、アクセスポイント同士が干渉している場合でも、効果を発揮することができます。アクセスポイントは、同チャネルで干渉があると、一つの送信しか行うことができません。Spatial Reuse を有効にしている場合は、しきい値外の通信に関しては干渉していても無視をして通信が可能となり、通信効率が向上します。



チャネル選択でDFS履歴を使用

DFS(Dynamic Frequency Selection)とは、5GHz 帯の無線 LAN で、W53(52ch～64ch)および W56(100ch～140ch)のチャンネルを使用している場合、気象・航空レーダー波を検出した際に使用できるチャネルを調べて移動する一連の処理のことです。DFS はアクセスポイントには実装が必須となり、レーダー波を検知すると、AP は無線電波を 1 分間以上停止　(周囲の電波調査)をし、その後別のチャネルに切り替えなければなりません。この問題を DFS 履歴のリスト管理機能によって回避することが可能です。本機能により、過去のレーダーヒット率(チャンネルスコア)に基づき、DFS チャンネル候補リストを自動生成することができます。アクセスポイントの運用を継続し学習させることで、レーダーを避ける最適なチャネルが選択されることで、DFS による問題が解消されます。

●DFS による問題

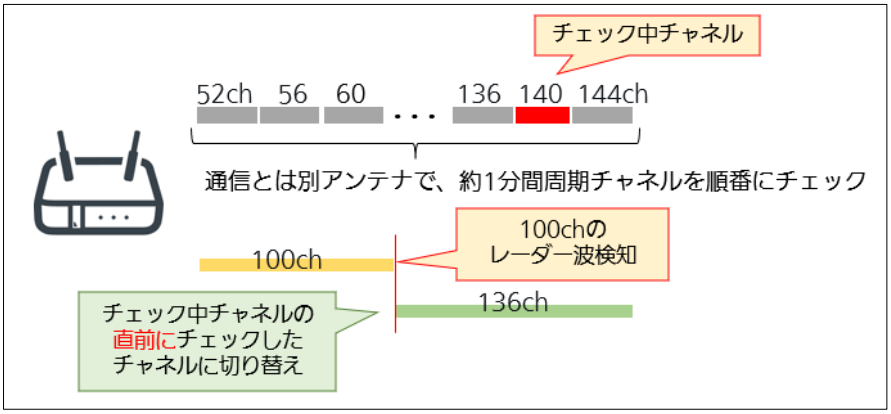


●一般的な DFS 回避機能との差分

一般的な DFS 回避機能のメカニズムとして、レーダー波を検知する前に別のチャネルに変更する機能があります。しかしながら、本方式では以下の欠点があります。

1. 検知するレーダー波が多数あると、頻繁にチャネル変更が発生する可能性がある。
2. チャネルの変更先の混雑具合は考慮されない。

そのため、長期的には DFS チャンネル候補リスト管理の方が、通信品質は安定します。



送信電力選択

送信電力値はEIRP（実効等方性放射電力）に対応します。これは、アンテナから放射される、無線で送信される実際の電力です。送信電力選択は自動または手動に設定できます。自動モードでは、アクセスポイントは自動的に送信電力を調整して、隣接するアクセスポイントとの干渉を最小限に抑えます。指定した最小値と最大値に加えて、使用される実際の送信電力は次の要因によって制約されます。

●規制ドメイン(TELEC)で許可される最大値
　2.4GHz(ISM): 23dBm
　5GHz(UNII-1/2a/2c): 23dBm
　6GHz(UNII-5): 23dBm
●無線がサポートする最大電力
●アンテナゲイン

スマートステアリング

スマートステアリングは、「スティッキークライアント」 の問題を解決します。スティッキークライアントとは、信号強度が高い別のアクセスポイントがある場合でも、信号強度が低いアクセスポイントに接続されたままのクライアントです。

[ローミング開始間隔]は、設定した時間以上、クライアントの信号強度がローミング開始RSSIしきい値より低くなっている場合、ローミングを開始します。本設定を調整することで、頻繁にローミングが発生することによる通信品質低下を防ぎます。

[ローミング開始パケットのしきい値]は、アクセスポイントがクライアントを頻繁にステアリングさせないことでQoEを悪化させないために設定します。アクセスポイントは、クライアントの RSSI がこのパケット数でステアリング RSSI しきい値を下回っている場合にのみ、クライアントをステアリングします。これにより、ステアリングがローミング開始間隔中に送信されたわずか数パケットの RSSI に基づいていないことが保証されます。ただし、このパラメータの値を大きすぎる値に設定すると、アクセスポイントがクライアントとの切断要求をする前にパケット通信を待機するため、スムースにステアリングが行

われない可能性があります。

スマートクライアントのロードバランシング

アクセスポイントが多く配置されている環境にも関わらず、複数のクライアントが1台のアクセスポイントと接続し、特定のアクセスポイントの負荷が高くなる場合があります。周囲に負荷が低いアクセスポイントが存在する場合、負荷の高いアクセスポイントとの新たなクライアント接続を拒否し、負荷が低いアクセスポイントに接続しやすくするように誘導します。

バンドステアリング

アクセスポイントがクライアントを、2.4GHz帯から6GHzまたは5GHz帯へ移行します。バンドステアリングは単一方向です。バンドステアリングパラメータは2.4GHzタブにて設定します。

WMM受付制御ポリシー

Wi-Fiマルチメディア（WMM）は、音声、ビデオ、ベストエフォート、バックグラウンドの4つのアクセスカテゴリに基づいてネットワークトラフィックに優先順位を付けます。[受付制御必須]にチェックを入れると、音声およびビデオ通話の受付制御パラメータを設定することができます。

ローミング予約

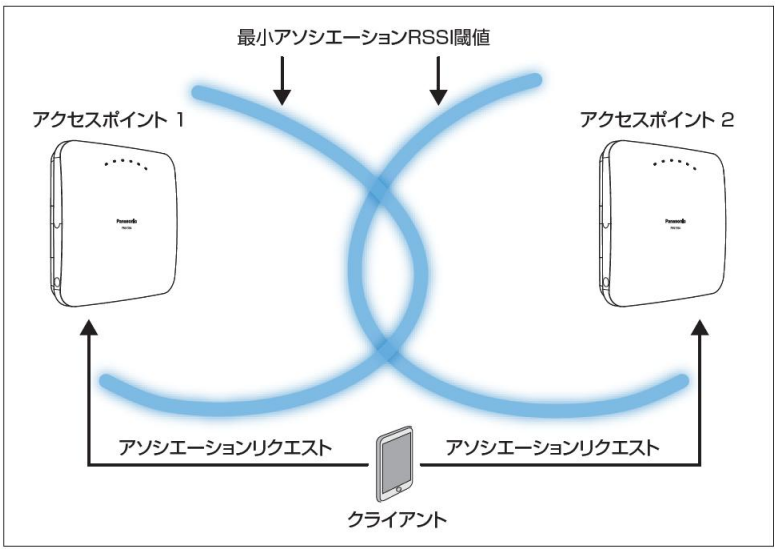
ローミングが実行された際に、ローミング先に通信帯域のリソースがなければ通信品質が低下する場合があります。ローミング予約機能は、この問題を軽減するために、移動前にクライアントが接続先のアクセスポイントへ接続通知がされた際、あらかじめ音声通話、またはビデオ通話を行うための一部のリソースを予約します。
これにより、通信の中断や品質低下を最小限に抑えることができます。

アクセスポイント間同期

クライアントステアリングをするためには、隣接するアクセスポイントとクライアント(自身のクライアントと隣接するクライアント）を認識している必要があります。アクセスポイントはそれらの情報に基づいてステアリングを行い、最適な通信環境を保証します。AIRRECT APは、それぞれのクライアントに関する情報を定期的に交換します。RSSI最小値を見る場合、クライアントRSSI値を有線ネットワーク上のRFネイバーに送信します。RFネイバーだけがクライアントRSSI値を更新し、各アクセスポイントは周囲のクライアントと、隣接するアクセスポイントに接続されているクライアントのRSSI値のデータベースを維持します。クライアントのRSSIが少なくとも1つのRFネイバーの最小しきい値を超えている場合（クライアントが正常に接続できる他のアクセスポイントを少なくとも1つ持っている場合）、クライアントを誘導します。

例えば、下図の2つのアクセスポイント両方から見たクライアントのRSSI値が、それらにアソシエーションするために必要な最小値よりも低いと仮定します。統合クライアントステアリングがないと、アクセスポイント1もアクセスポイント2もクライアントのアソシエーション要求を受け入れないため、クライアントは接続できません。

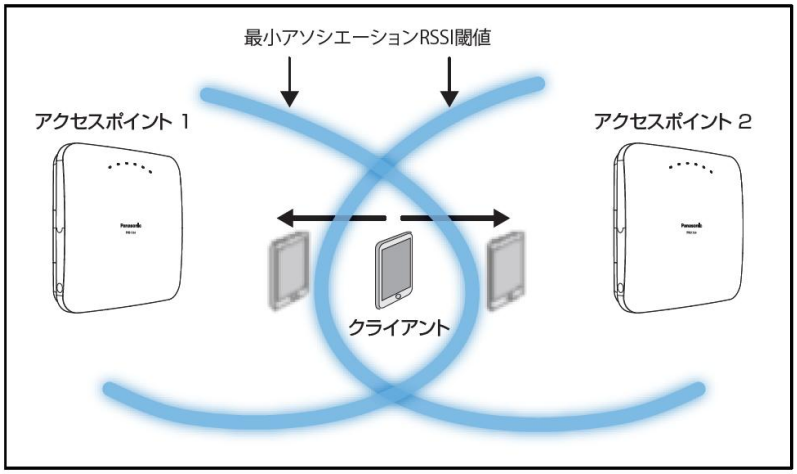
統合クライアントステアリングでは、互いのアクセスポイントのRSSI値を共有するため、アクセスポイント1は、最小アソシエーションしきい値より大きいRSSIを持つクライアントを認識できる隣接アクセスポイントがないことを把握し、クライアントのアソシエーション要求を拒否しません。これにより、クライアントが接続されQoEが向上します。



スマートステアリング概要

下図のスマートステアリングの例は、アクセスポイント1とアクセスポイント2の間のカバレッジオーバーラップ領域にあるクライアントを示しています。クライアントのRSSIは、チャネルのフェージング中や、クライアントの移動中は、頻繁に変化する可能性があります。 スマートステアリングを使用しない場合、アクセスポイント1で設定されたRSSIが構成されたしきい値を下回るとアクセスポイント2にクライアントを誘導し、逆にアクセスポイント2のRSSIが低下すると、アクセスポイント1に誘導され、頻繁にステアリングされることで、継続的な切断が発生する可能性があります。

統合クライアントステアリングでは、クライアントは10分間に行われる最大ステアリング回数と、ステアリングを行わないブラックアウト間隔の設定により、頻繁なステアリング問題を解決できます。（デフォルトでは10分間に二回のステアリングと15分のブラックアウト間隔となります。）



統合クライアントステアリングの仕組み

以下の表は、クライアントステアリングのさまざまなタイプを示しています。クライアントがステアリングされるタイミング（アソシエーション前、または、アソシエーション後）とステアリングされる基準[受信信号強度（RSSI）、負荷または帯域]を表します。

クライアントステアリングのタイプ

方法		概要
アソシエーション前	最小アソシエーションRSSI	クライアントのRSSIが構成されたしきい値よりも小さい場合、アソシエーション要求を拒否します。
	バンドステアリング	マルチバンドクライアントの2.4GHzでのアソシエーション要求を拒否します。バンドステアリングは単一方向です。6GHz、5GHz帯は干渉が発生しにくく、より高速であるため、クライアントを誘導します。
	スマートクライアントロードバランシング	アクセスポイントのクライアント負荷が高く、利用可能な隣接アクセスポイントの負荷が少ない場合、アソシエーション要求を拒否します
アソシエーション後	スマートステアリング	RSSIが特定のしきい値を下回るとクライアントを切断します。
	バンドステアリング	6GHz、5GHzアクセスポイント無線がしばらくダウンしてから起動した場合（例えば、レーダー検出、高RF干渉検出によるチャネル変更など）、アクセスポイントは、6GHz、5GHzがダウンしたときに2.4GHzに接続されていたクライアントをステアリングします。

802.11be機能の設定

AIRRECT では以下の Wi-Fi 7 の機能を有効化、無効化することが出来ます。

●320MHz 通信

●マルチリソースユニット（Multi-RU）

●プリアンブルパンクチャリング

●マルチリンクオペレーション

●320MHz 通信

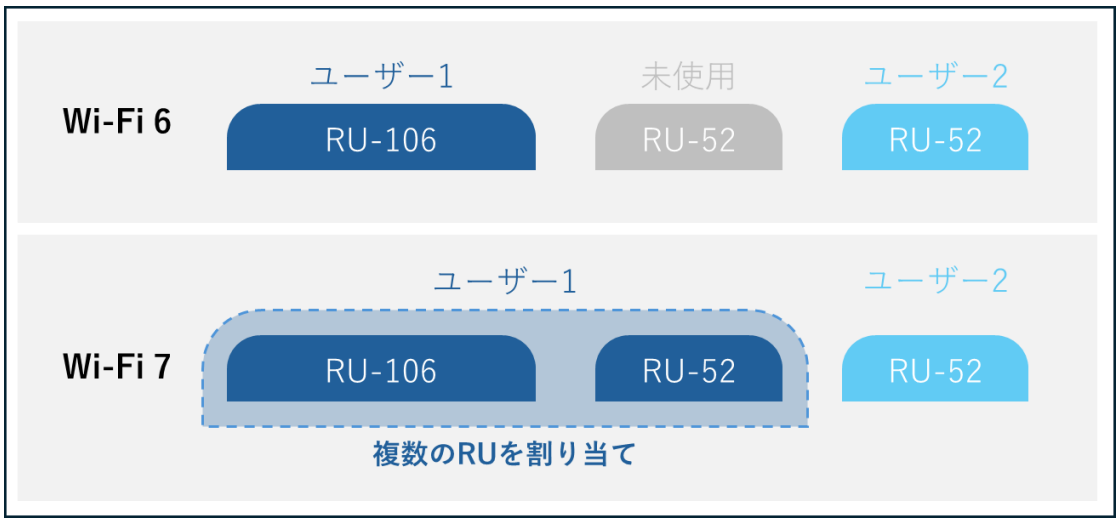
Wi-Fi 7 では、6GHz 帯域においてチャネル幅 320MHz で通信することが可能です。
これにより、160MHz 運用と比較して最大理論スループットは 2 倍となります

320MHz通信の有効化

1. [構成]>[デバイス]>[アクセスポイント]>[WiFi無線]に遷移します。
2. [6GHz]を選択し、[Wi-Fi規格]で[802.11be]を選択する。
3. [チャネル幅]で「20/40/80/160/320MHz」を選択する。

●マルチリソースユニット

マルチリソースユニット（Multi-RU）は、802.11axで導入されたOFDMAのRUの拡張機能です。従来は1ユーザーに対して1つのリソースユニット（RU）のみ割り当てていましたが、Multi-RUを利用することで、1ユーザーに対して複数のRUを割り当てることができます。



マルチリソースユニットの有効化

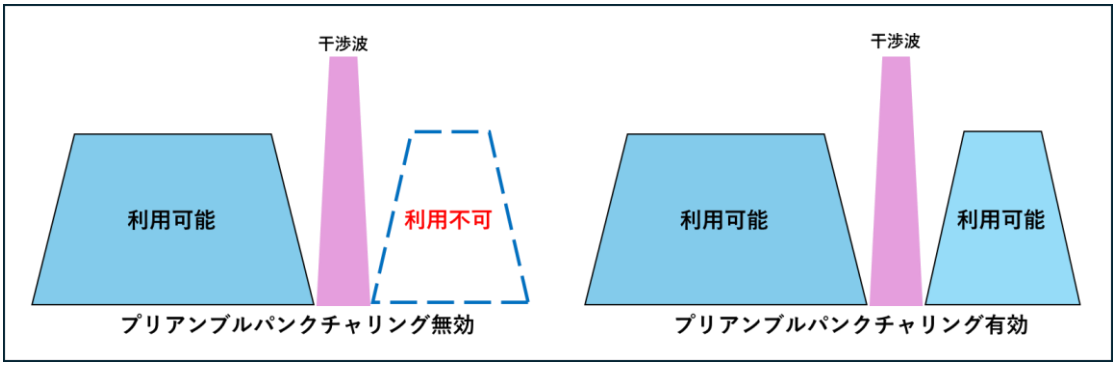
1. [構成]>[デバイス]>[アクセスポイント]>[WiFi無線]に遷移します。
2. 周波数帯域を選択し、[Wi-Fi規格]で[802.11be]を選択する。

3. 下にスクロールして[802.11beの機能強化]まで進みます。
4. [マルチリソースユニット]のチェックボックスをクリックします。
5. 設定を保存します。

注意：[ダウンリンクのOFDMA]と[アップリンクのOFDMA]を有効にしておく必要があります。

●プリアンブルパンクチャリング

従来は、80/160/320MHzの広帯域を使用する場合、一部の帯域で干渉が発生すると、利用可能な帯域幅全体を縮小する必要がありました。
プリアンブルパンクチャリングを使用すると、干渉のある帯域のみを避け、残りの帯域を引き続き利用することができます。これにより、干渉の影響を最小限に抑えながら、広帯域通信のメリットを維持できます。
アクセスポイントでは、80MHzおよび160MHz帯域で20MHz単位、320MHz帯域で40MHz単位のパンクチャリングが行われます。
注意：2.4 GHz帯ではプリアンブルパンクチャリングはサポートされていません。



プリアンブルパンクチャリングの有効化

1. [構成]>[デバイス]>[アクセスポイント]>[WiFi無線]タブに遷移します。
2. 周波数帯域を選択し、[Wi-Fi規格]で[802.11be]を選択する。
3. 下にスクロールして[802.11beの機能強化]まで進みます。。
4. [プリアンブルパンクチャリング]のチェックボックスをクリックします。
5. 設定を保存します。

●マルチリンクオペレーション

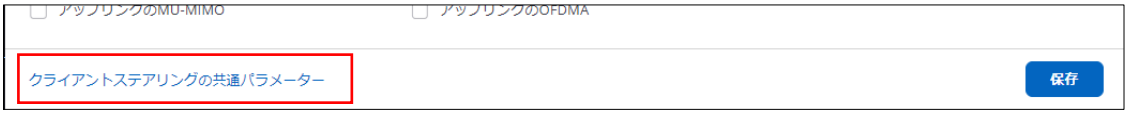
機能の詳細と設定方法は『マルチリンクオペレーション』をご確認ください。

2.10.1 無線通信設定の構成

2.10.1.a クライアントステアリングの共有パラメーター

クライアントステアリングの共通パラメータを構成するには、以下の手順を実行します。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]の順に移動します。
2. 画面の下部にある [**クライアントステアリングの共通パラメータ**]リンクをクリックします。



3. [**ステアリングRSSI**]フィールドでしきい値の値を入力します。
4. [**最大ステアリング試行回数**]フィールドでクライアントのステアリング試行の最大数を設定します。
5. [**ステアリングブラックアウト期間**]フィールドでクライアントのステアリング一時停止期間を設定します。
6. [**クライアントステアリングのアクセスポイント同期**]フィールドでRSSI情報を同期する頻度を設定します。
7. [**終了**]をクリックします。

統合クライアントステアリングとは

AIRRECT APは、クライアントを、別の周波数帯、または、別のAIRRECT APに誘導できます。クライアントをアソシエーションの前、または、後にステアリングできます。クライアントをステアリングするかどうかの決定は、信号強度、負荷（つまり、無線機に接続されているクライアントの数）、優先操作帯域などの考慮事項に基づきます。クライアントステアリングはユーザーエクスペリエンス品質（QoE）にとって重要ですが、クライアントの頻繁なアドホックステアリングは実際にはQoEを悪化させる可能性があります。AIRRECT APでは、統合クライアントステアリングと呼ばれるアプローチを使用しています。このアプローチでは、アクセスポイントは相互に情報を交換するため、クライアントエクスペリエンスの全体像を把握することができます。このようにしてさまざまなタイプのクライアントステアリングが連携することで、クライアントのQoEを向上させる、という共通の目標を実現します。例えば、スマートステアリングとバンドステアリングは、共通のRSSIしきい値を基準として使用します。

クライアントステアリングパラメータ

パラメータ	概要
クライアントステアリングの共通パラメータ	
ステアリングRSSI	ステアリングRSSIしきい値は、-60～-85dBm の範囲で設定することができます。初期値は-70dBmです。
ステアリング試行回数	これは、クライアントのステアリングがステアリングブラックアウト期間で指定された期間、中断された後、10分のウィンドウ内でのクライアントのステアリング試行の最大数です。ステアリング試行の初期値は2です。最小値は1で、最大値は5です。
ステアリング ブラックアウト期間	クライアントのステアリング停止期間を示します。クライアントがこの期間内に滞在する場合、クライアントにはステアリング方法は採用されません。ステアリングブラックアウト期間の初期値は15分です。最小値は10分、最大値は60分です。
クライアントステアリングのアクセスポイント同期	クライアントRSSIの更新間隔は10～60秒の範囲で設定することができます。初期値は10秒です。

2.10.1.b 2.4GHz/5GHz/6GHzの無線通信設定の構成

2.4GHzと5GHzの両方の無線設定を構成できます。構成はロケーションによって異なります。

無線設定パラメータの詳細については、『基本的な無線設定パラメータ』を参照して下さい。基本的な無線設定は以下の手順で設定します。

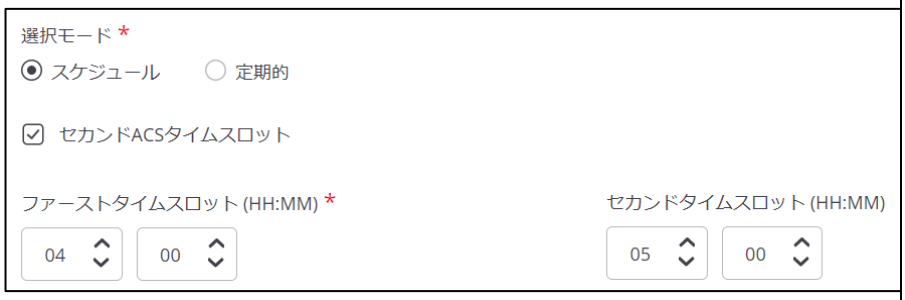
1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]の順に移動します。
2. [**周波数帯域**]：**周波数帯（2.4GHz/5GHz/6GHz）**を選択します。
3. [**チャンネル選択**]：[**自動**]または[**手動**]を選択します。

・チャンネル選択が自動の場合、以下のフィールドに適切な値を入力します。無線設定パラメータの詳細については、『基本的な無線設定パラメータ』を参照してください。

- [**候補チャネル**]
- [Schedule]または[**定期的**]を選択し、チャネル変更のタイミングを指定します。
- [**動的チャネル選択**]：現在のチャネルを干渉の少ない使用可能なチャネルに自動的に切り替えることができます。選択したWi-Fi規制ドメインに応じて、候補チャネルを選択します。チャネル選択が手動の場合は、適切なチャネル番号を入力します。

4. [**保存**]をクリックします。

基本的な無線設定パラメータ

パラメータ	概要
周波数帯	周波数帯を示します。設定可能な値は2.4GHz、5GHz、6GHzです。
候補チャネル	電波の操作チャネルを示します。デフォルトでは、アクセスポイントは自動的に動作チャネルを選択します。ユーザーは、必要に応じてチャネルを手動で設定できます。
選択モード	チャネル選択が自動の場合のみ表示されます。以下の2つのモードから選択を行います。 **スケジュール**: チャネル選択が行われる時間の指定が出来ます。指定した時間に他のチャネルが現在のチャネルよりも干渉が低いことが判明した場合、チャネルが自動的に変更される場合があります。また、[**セカンドACSタイムスロット**]を有効化することで、２つの時間帯でチャネル選択が可能となります。 **定期的**：チャネル選択が行われる間隔を時間単位で指定します。1から48までの任意の値を入力できます。他のチャネルが現在のチャネルよりも干渉が低いことが判明した場合、この時間間隔の後、チャネルは自動的に変更される可能性があります。 
チャネル選択でDFS履歴を使用	DFSレーダーを検知したチャネルをリスト管理し、自動チャネル選択時に選択しないように管理します。
動的チャネル選択	チャネル選択が自動の場合のみ表示されます。[**動的チャネル選択**]をオンにすると、現在のチャネルの干渉が増加したときに、現在のチャネルから干渉の少ない使用可能なチャネルへの自動切り替えが有効になります。選択間隔の時間設定は適用されません。 **デフォルト無効**：干渉率の高い高密度環境では、頻繁にチャネル変更が行われ、クライアントが切断/再接続される可能性があるため無効となっています。環境状況に基づいて有効化してください。
候補チャネル	チャネル選択が自動の場合のみ表示されます。アクセスポイントは、現在のチャネルの干渉状態を動的にチェックし、選択されたチャネルの中から干渉の少ないチャネルに変更します。

パラメータ	概要
プロトコル	接続可能なIEEE規格の選択をします。例えば、5GHz帯で802.11acを選択した場合、802.11axに対応した無線クライアントであっても、802.11ac以前（802.11a/nを含む）のプロトコルで通信を行います。
チャネル幅	無線のチャネル幅を示します。2.4GHz帯では20/40MHz、5GHz/6GHz帯では、20/40/80/80+80/160MHzから選択できます。 また、6GHz帯でプロトコル「802.11be」を選択している場合、320MHzを選択することが出来ます 注意：チャネル幅は、クライアントからのプローブ要求に従い設定されます。例えば、80MHzで接続を要求するクライアントがいる場合、そのSSIDは80MHzで接続されますが、広い周波数を選択すると環境によっては電波干渉によるトラブルが発生する場合があります。干渉が発生した際には、チャネルを20MHzに変更するなどの対応を推奨します。
ガード・インターバル	無線クライアントと通信を行うガード・インターバルの値を設定できます。

無線設定で送信電力選択パラメータを設定する

アクセスポイントの送信電力を手動で修正するか、アクセスポイントが自身の送信電力を自動的に調整するように設定できます。

構成パラメータの詳細については、『送信電力選択パラメータ』を参照してください。

無線設定で送信電力制御を構成するには、以下の手順を実行します。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]の順に移動します。
2. [**送信電力選択**]の[**自動**]または[**手動**]を選択します。
   - ●[**自動**]を選択すると、しきい値フィールドが有効になります。
     [**ラウドネスRSSI**]、[**ネイバー数**]、[**最小EIRP**]、[**最大EIRP**]に適切な値を入れます。
   - ●[**手動**]を選択すると、dBm単位の[**EIRP**]（送信制御パワー）を入力できます。
3. [**保存**]をクリックします。

送信電力選択パラメータ

パラメータ	概要
高度な無線設定	
送信電力選択/自動および手動ラジオボタン	このフィールドでは、アクセスポイントの送信電力を制御できます。これは必須フィールドです。 ●手動：アクセスポイントの送信電力をdBmで手動で指定するには、手動を選択します。 ●自動：自動を選択して、隣接するAIRRECT APとの干渉を最小限に抑えるようにアクセスポイントが自動的に送信電力を調整するようにします。
ラウドネスRSSI	設定した値より大きいRSSIを持つアクセスポイントが近くにある場合、電波出力が大きい隣接アクセスポイントがあると判断し、自動で出力を小さく調整します。許容範囲は、-95dBm～-45dBmです。デフォルトは-75dBmです。
ネイバー数	許可されるラウドネスRSSIの隣接アクセスポイント最大数を表します。許容範囲は1～10です。初期値は3です。
最小EIRP	最小送信電力を表します。許容範囲は4～36dBmです。初期値は4dBmです。
最大EIRP	最大送信電力を表します。許容範囲は4～36dBmです。初期値は30dBmです。

無線設定でスマートステアリングを構成する

スマートステアリング機能は、スティッキークライアントの問題を解決するのに役立ちます。以下の手順でスマートステアリングを設定します。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]の順に移動します。
2. [**スマートステアリング**]で[**ローミング開始間隔**]の時間を秒単位で入力します。
   設定した時間以上、クライアントの信号強度がローミング開始RSSIしきい値より低くなっている場合、ローミングを開始します。本設定を調整することで、頻繁にローミングが発生することによる通信品質低下を防ぎます。
   時間の範囲は、5～900で、初期値は10です。
3. [**ローミング開始パケットのしきい値**]フィールドに、クライアントを切断するパケットのしきい値を入力します。クライアントの信号強度が設定したパケット数でステアリングRSSIしきい値を下回ると、アクセスポイントはクライアントを切断し、ローミングを開始します。パケットのしきい値は5～500で、初期値は5です。
4. [**保存**]をクリックします。

無線設定でスマートクライアントロードバランシングを構成する

スマートクライアントのロードバランシングはSSIDごとに構成されますが、無線帯域（2.4/5/6GHz）にアソシエーションされたすべてのSSIDによって共有されます。ロードバランシングのメカニズムは、ビデオや音声などのリアルタイムアプリケーションを使用するクライアントが影響を受ける可能性があるため、クライアントがローミングした際にアクセスポイントへ即時にアクセスすることを拒否する場合があります。リアルタイムアプリケーションをサポートするSSIDで、スマートクライアントのロードバランシングを有効にすることは推奨されません。

スマートクライアントのロードバランシングは、以下の手順で設定できます。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]の順に移動します。
2. [**スマートクライアントのロードバランシング**]で、[**最小クライアント負荷**]フィールドにアクセスポイントに接続できるクライアントの最小数を入力します。このフィールドでは、クライアントのロードバランシングがトリガーされる前にアクセスポイントに接続できるクライアントの最小数を指定できます。初期値は30で、15～45までの値を設定することができます。単一アクセスポイントの負荷がチェックされている間、各無線の最小クライアント負荷が考慮されます。
3. [**最小クライアント負荷の差**]フィールドに、隣接アクセスポイントに接続されているクライアント数の最小差を入力します。この差は、クライアント負荷のバランスをとるために考慮されます。初期値は5で、範囲は2～10です。
4. [**保存**]をクリックします。

無線設定でバンドステアリングを構成する

バンドステアリングとは、1つのバンドで複数のクライアントが動作している場合に、Wi-Fiクライアントが空いているもう1つのバンドに切り替えて、アクセスポイントの負荷を分散させる機能です。

以下の手順でバンドステアリングを設定できます。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]の順に移動します。
2. [**バンドステアリング**]で[**バンドステアリングクライアント負荷の差**]の値を入力します。5GHz（または6GHz）と2.4GHzにアソシエーションされているクライアント数の差が設定されたしきい値を超えるまで、5GHzまたは6GHzへのバンドステアリングは実行されません。初期値は25で、最大値は50です。
3. [**保存**]をクリックします。

WMM受付制御ポリシーを構成する

Wi-Fiマルチメディア（WMM）はネットワークトラフィックを優先するために、音声およびビデオコールのアドミッション制御パラメータの設定を行います。

WMM受付制御ポリシーは、以下の手順で設定します。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]の順に移動します
2. [**WMM受付制御ポリシー**]で[**音声通話**]、または、[**ビデオ通話**]を選択します。
3. [**受付制御必須**]を選択して、受付制御を必須にします。
4. [**ACK不使用ポリシー**]を選択すると、確認応答ポリシーが無効になり、ユニキャストQoSデータパケットの確認応答がレシーバーから要求されません。[**ACK不使用ポリシー**]が有効な場合、QoSデータパケットの再送信は行われません。
5. [**最大許可通話**]フィールドでの選択に応じて、許可された音声通話またはビデオ通話の最大数を入力します。音声通話の数の上限は127です。
6. [**最大メディアのシェア時間**]フィールドに、エアタイム内で、通話/メディアにて使用可能なエアタイムの最大使用率を入力します。最大割合値の範囲は0～100です。初期値は0です。
7. [**予約された通話**]フィールドに、ローミングクライアント用に予約されている音声通話の数を入力します。このフィールドの範囲は、0から[**最大許可通話**]フィールドで指定された数までです。
8. [**予約されたメディアのシェア**]フィールドに、ローミングクライアント用に予約されているメディアのシェア時間を入力します。シェアの割合の範囲は、0から[**最大メディアのシェア時間**]フィールドで指定された割合までです。
9. [**保存**]をクリックします。

フレームアグリゲーションを構成する

フレームアグリゲーションは、802.11プロトコルのオーバーヘッドを削減し、1回の送信で複数のデータフレームをグループ化することでスループットを最大化するMAC拡張機能です。802.11データリンク層は、2つのサブ層（論理リンク制御（LLC)、メディアアクセス制御（MAC））があります。ネットワーク層がデータリンク層にパケットを送信すると、LLCに渡され、MACサービスデータユニット（MSDU）となります。MSDUがMACサブレイヤーに送信されると、MACヘッダーが追加されます。このカプセル化されたフレームはMACプロトコルデータユニット（MPDU）となります。

このMSDUとMPDUにおいて、フレームアグリゲーションを行うには以下の 2 つの方法があります。

1. A-MSDU: 複数のMSDUを単一のMPDU内にカプセル化できるため、MACヘッダーのオーバーヘッドが削減されます。
2. A-MPDU: 複数のMPDUを単一のPHYヘッダーでカプセル化できます。

フレームアグリゲーションは、以下の手順で設定できます。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]の順に移動します。
2. 実行したいフレームアグリゲーションに応じて、[A-MSDU]と[A-MPDU]のどちらか、もしくは、両方にチェックを入れます。
3. [**保存**]をクリックします。

RTSしきい値、DTIM期間を構成する

RTS しきい値：RTS は、データの送信を行う前に、送信権を要求するために使用されます。データ送信したいデバイスは、周囲のデバイスに対して RTS フレームを送信し、送信権を要求します。周囲のデバイスは、CTS（Clear to Send）フレームを返すことで、送信権を許可するかどうかを通知します。送信権が与えられたデバイスは、データの送信を開始します。

RTS/CTSプロトコルは、無線環境において複数のデバイスが同時に送信を行う場合に、衝突や干渉を防ぐために使用されます。これにより、データの送信がより効率的に行われることが期待されます

しかしながら、多くの送信オーバーヘッドを利用するため、小さいサイズのフレームを送信する場合などはスループットの低下が懸念されます。そのため、RTS しきい値によって、RTS/CTS プロトコルを送信するフレームの長さのしきい値を指定することで、小さなフレームを送信する際には RTS/CTS プロトコルを送信しないようにできます。

DTIM 期間：パケットが送信待ちであることを示すビーコン（DTIM ビーコン）を送信する間隔を表します。DTIM ビーコン後に送信するデータには、ブロードキャストメッセージまたはマルチキャストメッセージを含みます。

たとえば、DTIM 期間が「3」の場合は、ビーコンを 3 回送信する毎に DTIM ビーコンが 1 回送信されることを意味します。送信されるビーコンが DTIM ビーコンか否かは、送信されるビーコンに含まれる情報要素である TIM 情報要素中の DTIM カウント値が「0」であるか否かで決まります。

以下の手順で RTS しきい値、DTIM 期間を設定できます。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**WiFi無線**]の順に移動します。
2. 画面を下にスクロールし、無線通信詳細設定内にある、[**RTSのしきい値**]、[**DTIM期間**]の設定を行います。
   - ●[**RTSのしきい値**]：しきい値の設定は、パケットサイズをバイト単位で入力して行います。256～2347の範囲で任意の値を入力します。初期値は2347です。
   - ●[**DTIM期間**]：1～10の範囲で任意の値を入力します。初期値は1です。
3. [**保存**]をクリックします。

2.11 デバイス設定

[**デバイス設定**]で、バックグラウンドスキャンなどのデバイス関連の設定や、WIPSなどのセキュリティ関連の設定を構成できます。親ロケーションに適用されるデバイス設定は子ロケーションによって自動的に継承されます（初期設定）。例えば、支社1と支社2の2つの子ロケーションを持つ本社の親ロケーションでは、本社に適用されたデバイス設定が自動的に支社1と支社2に適用されます。子ロケーションのデバイス設定をカスタマイズして、親のデバイス設定と変えることもできます。[**構成**]>[**デバイス**]>[**アクセスポイント**]>[**全般的**]タブから設定を行います。以下は、主な設定項目です。

●[**アクセスポイントを専用WIPSセンサーに変換**]から、アクセスポイント機能をOFFにして不正な端末を検知するセンサーとして動作させることができます。
●[**デバイスのパスワード**]を使用すると、そのロケーションにあるデバイスのパスワードを設定できます。
●[**バックグラウンドスキャン**]により、アクセスポイントがチャネルをスキャンする時間と、スキャンする頻度を設定できます。バックグラウンドスキャン中に取得した情報は、パフォーマンスの最適化 (動的チャネル選択、クライアントステアリングなど) およびセキュリティ(WIPS不正アクセスポイント検出など)に利用されます。RF最適化機能を利用するには、[**バックグラウンドスキャン**]を有効にする必要があります。クライアントステアリングのアクセスポイント間同期により、アクセスポイントはクライアント情報を相互に交換します。[**バックグラウンドスキャン**]を[**オフ**]にすると、SSIDの⋮を右クリックすることで表示されるアクション一覧内に「推奨設定」が追加されます。そこからもバックグラウンドスキャンのオン/オフの設定ができます。
●[**WiFiセキュリティ機能**]により、不正アクセスポイントを検知するWIPS機能を有効にします。設定内容に関係なくAIRRECT APは常に有効となります。
●[**クライアントRSSIの更新間隔**]により、アクセスポイントがクライアント情報を収取するためのビーコンを送付する間隔を設定します。
●[**NTP設定**]では、AIRRECT APが時刻の基準を取得するために使用するプライマリサーバーとセカンダリサーバーを定義します。
●[**デバイスログをSyslogサーバーに送信**]を有効にすると、アクセスポイントがアクセスログを送信するSyslogサーバーのホスト名、または、IPアドレスを指定できます。
また、SSHバナーの表示有無と、未使用時のタイムアウト時間の設定も可能です。

●[**IPv4/IPv6デュアルスタック**]を有効にすると、アクセスポイントがIPv4アドレスとIPv6の両方を扱えるようになります。
●[**SSH IP許可リストの有効化**]を有効にすると、アクセスポイントへSSH接続を許可する

IPアドレスを制限できます。

●[**可視性分析をサードパーティ・サーバーにプッシュ**]を有効にすると、AIRRECT APは分析情報を外部サーバーに送信します。

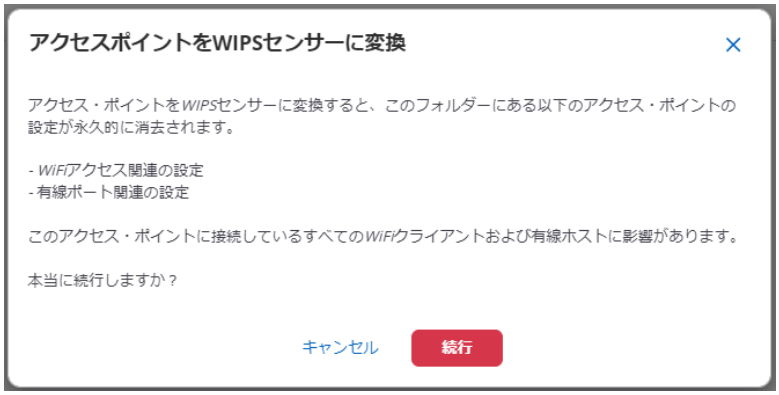
●[**LEDの無効化**]を選択すると、デバイス設定を適用するアクセスポイントのすべてのLEDが消灯します。LEDは、アクセスポイントの起動時のセットアップが完了した後に消灯します。

2.11.1 デバイス設定の構成

アクセスポイントを専用WIPSセンサーに変換

アクセスポイントの動作モードをセンサーモードへ移行します。
センサーモードでは、アクセスポイントのWi-FiアンテナはWIPSアンテナとして動作します。クライアントへWi-Fiを提供すること（SSID出力）ができなくなりますのでご注意ください。反対に、センサーモードからAP-センサーモード（デフォルト）へ戻す場合には本項目のチェックを外します。以下の手順でセンサーモードへ切り替えます。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**全般的**]に移動します。
2. [**アクセスポイントを専用WIPSセンサーに変換**]を選択します。
3. [**続行**]をクリックの後、[**保存**]をクリックします。



デバイスパスワードの設定

アクセスポイントのCLIアクセスに必要となるパスワードを設定します。ユーザー名はデフォルトから変更できません。以下はデバイスパスワードの設定手順です。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**全般的**]に移動します。
2. [**デバイスのパスワード**]の[**パスワード**]フィールドへパスワードポリシーに従うパスワードを入力します。
   ※ポリシーは[**パスワードポリシー**]へのマウスオーバーで確認できます。
4. [**パスワードの確認**]フィールドに再度パスワードを入力します。
5. [**保存**]をクリックします。

スキャン設定（バックグラウンドスキャン）
RF環境をスキャンすることで、WIPSデバイス（アクセスポイント/クライアント）検出や自動チャネル変更やRF最適化（スマートローミング/スマートステアリングなど）といった機能を実現しています。本機能により、バックグラウンドスキャンを行う期間と間隔を設定できます。
注意：AIRRECT APは多機能アンテナを搭載するため、バックグラウンドスキャンを常時使用しており、本設定内容は適用されません。

[通常]（バックグラウンドスキャン）
Wi-Fiアンテナが、サービス外チャネルを断続的にスキャンする方式です。「Wi-Fiスキャンの長さ」は、サービス外チャネルをスキャンする時間(ミリ秒)を示し、「Wi-Fiアクセスの長さ」は、サービス外チャネルのスキャン開始までの時間(秒)を示します。デフォルトでは、60秒ごとにサービス外チャネルを100msでスキャンします。

[VoIP対応]（VoIPスキャン）
VoIP通信などリアルタイム性を必要とする通信を妨害しないクイックチャネルです。10秒ごとにサービス外チャネルを30msでスキャンします。

オフ
バックグラウンドスキャンを実施しません。

欠落VLANの検出
APが接続しているスイッチと一定時間VLAN通信できないとき、そのVLANを「欠落したVLAN」として検出できます。検出するまでの時間は1～15分の間で設定できます。
検出したVLANはモニター画面([モニター]>[Wi-Fi]>[アクセスポイント])に表示されます。

NTP設定
アクセスポイントのシステムクロックの同期先NTPサーバーを設定します。デフォルトでは「ntp.nict.jp」が設定されています。システムクロックは、ログのタイムスタンプなどに使用されます。設定されたNTPサーバーに到達できない場合はクラウドサーバーと時刻同期を行います。クラウドサーバーにも到達できない場合、アクセスポイントは、時刻保持のための内部バッテリーを持たないため、再起動の度、UNIX時間（1970年1月1日）にリセットされます。
注意：NTP通信はAIRRECT APの管理VLANを、UDP123を使用して行われます。

ローカルアクセスポイントのデバイスログをSyslogサーバに送信する

センサーのアクセスログをSyslogサーバーに送信することができます。
「SyslogサーバーIP/ホスト名」へは、アクセスログの送信先となるSyslogサーバーのIPアドレス、またはホスト名を入力します。

IPv4/IPv6デュアルスタックの設定

IPv4/v6デュアルスタックネットワークのサポートを有効にすると、IPv4アドレスとIPv6アドレスの両方で同時に通信できます。無効にすると、IPv4ネットワークでのみ動作します。IPv6は機能によりサポート、未サポートがありますので、以下をご参照ください。

大項目	中項目	IPv6サポート
トンネルインターフェース		○
Radiusプロファイル		○
ロールプロファイル		×
デバイス設定	NTPサーバーIP	○
	SyslogサーバーIP	○
	SSH IP許可リスト	×
	可視性分析をサードパーティサーバにプッシュ	○
SSID設定	NAT設定	×
	ファイアウォールルール	×
	リダイレクトURL	×
	分析結果をサードパーティサーバにプッシュ	○
	ユーザーがログイン前にアクセスできるWebサイト	×
クライアント接続テスト	ポータル認証のテスト	×
	アプリケーションテスト	×
SMTPサーバー		×
SNMP -アラート-		×
Syslog		×
WLAN統合		×

SSH IP許可リストの有効化の設定

[SSH IP許可リストの有効化]にて登録されたIPアドレスとワイルドカードマスクに一致するIPアドレスを持つデバイスからのみSSH接続が許可されます。デフォルトは無効です。
最大20個のエントリを登録できます。

可視性分析をサードパーティ・サーバーにプッシュ

可視性分析データをサードパーティの外部サーバーに送信できます。分析データは、CSVファイルまたはJSONファイルとして送信できます。「**サーバーURL**」には転送先サーバーのURL、「**送信間隔**」には転送先サーバーに送信する間隔(秒)、「**承認**」へは転送先サーバーへアクセスするための認証情報を設定します。

アクセスポイントのLED点灯設定

アクセスポイント本体の LED ライトの明るさが気になる場合には、「**LED の無効化**」を有効にすることで、LED を消灯することが可能です。

また、PoE 給電容量が十分ではない場合の機能縮小モードを示す橙点灯は、ユーザーによってはエラー表示と誤解してしまうこともあります。「**縮小機能の LED 表示を無効化する**」を有効にすることで、機能縮小モード時も緑点灯にすることが可能です。

2.11.2 デバイス設定のセキュリティ概要

[**デバイス設定**]の[**セキュリティ**]タブで、VLANモニタリングとWIPS設定ができます。
AIRRECT Cloudは、VLAN上のアクセスポイントとアクセスポイントにアソシエーションされたクライアントを監視することで、不正なアクセスポイントやクライアントを発見することが出来ます。自動VLANモニタリングの詳細については、『自動VLANモニタリングの仕組み』を参照してください。また、監視する追加のVLANを任意で指定できます。
※AIRRECT APが監視できるVLANの数には制限があります。詳細は『監視されるVLANの数』を参照してください。
VLANモニタリングは、ワイヤレス侵入防止システム(WIPS)用の検知パケットを、どのVLANで送付をするか指定することができます。WIPSによって、デバイスを自動的に分類し、不正デバイスをネットワークから切り離します。
注意：検知パケットを送付するために、1つのVLANごとに1つのIPアドレスが必要です。
また、[**WIPS設定**]で、オフラインモードを有効にして、監視および防御するチャネルを選択できます。オフラインモードは、アクセスポイント（センサー）とサーバー間が接続されていない場合にも、一定のセキュリティ効果を提供します。
センサーは、イベントを発生させて保存し、再接続時にサーバーにプッシュします。

自動VLANモニタリングの仕組み
[**VLANモニタリング**]を使用すると、VLAN上のアクセスポイントとアクセスポイントにアソシエーションされたクライアントを監視できます。
AIRRECT CloudのWIPS機能は、監視対象のVLAN上のデバイスを承認済み、不正、または外部デバイスに自動的に分類します。[**デバイス設定**]>[**セキュリティ**]>[**VLANモニタリング**]で、次のタイプのVLANモニタリングを有効にできます。
●[**SSID VLANモニタリング**]：アクセスポイントはSSIDで設定したVLANを監視します。
●[**VLAN自動モニタリング**]：アクセスポイントはアクティビティを検出したVLANを自動的に監視します。
●[**監視するVLANを追加**]：フォルダまたはグループ内のアクセスポイントで監視するVLANを任意に追加できます。
これらの設定は、フォルダ（ロケーション）またはグループに適用されます。各アクセスポイントが異なるVLANセットを認識するような場合は、アクセスポイントごとに監視するカスタムVLANを定義できます（[**モニター**]>[Wi-Fi]>[**アクセスポイント**]で、[Wi-Fi**の監視**]>[**アクセスポイント**]セクションを参照）。SSID VLANモニタリングは初期値で有効になっています。アクセスポイントで設定されたSSIDに対応するVLANをアクセスポイントで監視しない場合は、この機能を無効にできます。

監視されるVLANの数

AIRRECT APは、アクセスポイント、センサー、またはネットワーク検出装置（ND）モードで動作できます。以下の表は、AIRRECT APがこれらの各モードで監視できるVLANの最大数を示しています。NDモードはCLIからのみ設定することができます。詳しい設定方法は『CLIリファレンス』をご確認ください。

APモード	センサーモード	NDモード
16	16	100

初期値では、AIRRECT Cloudサーバーとの通信に使用するVLANを監視します。SSID VLAN監視機能を有効にしている場合、SSID VLANを監視します。また、ユーザー定義のVLANは、**[監視するVLANを追加]**オプションを使用することで監視できます。

SSID VLANモニタリングが有効/無効の場合の例は以下になります。

●SSID VLANモニタリングが有効になっている場合：

アクセスポイントが自動的に監視するVLANの数は、アクセスポイントが監視できる最大数からSSID VLANとユーザー定義VLANの合計を引いた数と等しくなります。

自動監視されるVLANの数 = 16(最大数) - (SSID VLAN+ユーザー定義VLAN)

4つのSSID VLANと2つのユーザー定義VLANがある場合、自動的に監視されるVLANの数は16 -（4 + 2）= 10です。アクセスポイントは、アクティブであると検出した最初の10個のVLANを監視します。

●SSID VLANモニタリングが無効になっている場合：アクセスポイントが自動的に監視するVLANの数は、アクセスポイントが監視できる最大数からユーザー定義のVLANを引いた数に等しくなります。

自動的に監視されるVLANの数 = 16 - ユーザー定義VLAN

2.11.3 デバイス設定のセキュリティを構成

デバイス設定でのVLAN監視

有線側の接続状態検出、ホスト名検出、スマートデバイス検出、不正アクセスポイント検出などには、VLANモニタリングの設定が不可欠です。
VLANモニタリングの設定中に、SSID VLANモニタリング/VLAN自動モニタリング/監視するVLANを追加、の３つのタスクを実行できます。
VLANモニタリングは以下の手順で設定します。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**セキュリティ**]の順に移動します。
2. [**VLANモニタリング**]タブで[**VLAN自動モニタリング**]を選択してVLANを自動的に監視します。
3. [**監視するVLANを追加**]をクリックして、デバイスが監視するVLANを追加できるようにします。VLAN IDを追加するためのテキストボックスが有効になります。
4. 監視する追加のVLANをカンマ区切りのリストとして入力します。
5. [**保存**]をクリックします。

VLANモニタリングパラメータ

以下の表は、VLANモニタリングに関連するパラメータの概要を示しています。

パラメータ	概要
VLAN自動モニタリング	SSIDで追加されたVLAN、追加VLANで設定されたVLAN、またはCLIで設定されたVLANを自動でモニタリングするパラメータです。 自動でモニタリングされるVLANの動作は以下になります。 ●ユーザーが設定したVLANを常に優先します。SSIDのVLANに加えて、4つの追加VLANを監視することができます。 ●センサーモードでは、最大16個のVLANを監視できます。 ●NDモードでは100個のVLANを監視することができます。
監視するVLANを追加	デバイスが追加で任意のVLANを監視できるようにするパラメータです。
VLAN IDのカンマ区切りリスト	デバイスがサーバーとの通信に使用するVLANは常に監視されており、ここで指定する必要はありません。VLAN IDの範囲は0～4094です。監視する追加のVLANは、デバイスが接続されているスイッチポートで構成し、DHCPを有効にする必要があります。VLAN ID「0」は、スイッチの実際のVLAN番号に関係なく、デバイスが接続されているスイッチポートのタグなしVLANを示します。 **重要：**VLANに静的IPアドレスが構成されている場合は、CLIからVLANを構成します。

WIPSのオフラインモードを構成する

WIPSのオフラインモード機能を有効に設定すると、AIRRCT Cloudと切断を検知した後にアクセスポイントがオフラインモードに切り替わるまでの時間を指定できます。また、チャネル設定で侵入を監視および防御するチャネルを設定できます。

WIPS設定を構成するには、以下の手順を実行します。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**セキュリティ**] の順に移動します。
2. [**オフラインモード**]を選択します。[**デバイスが接続の喪失を検出した後にオフラインモードに切り換える時間**]を入力するフィールドが有効になるので、時間を分単位で入力します。
3. オプションとして、デバイス分類ポリシー、侵入防止ポリシーおよび、監視や防御を行うチャネルを設定します。
4. [**保存**]をクリックします。

WIPS設定パラメータ

以下の表には、WIPS設定に含まれるパラメータに関する詳細情報が含まれています。

パラメータ	概要
オフラインモード	AIRRECT Cloudから切断されたときに、AIRRECT APのセンサーによって、デバイス分類および防止機能が提供されます。センサーは、イベントをアクセスポイントに保存し、再接続時にAIRRECT Cloudへ情報をプッシュします。また、アクセスポイントが接続の切断を検出した後、デバイスがオフラインモードに切り替わる時間を分単位で指定できます。 (最小：1分、最大：60分、初期値：15分)
チャネル設定	センサーが侵入を監視および防御するためのチャネルのリストを表します。
監視するチャネル	侵入を監視するためのチャネルリストを表示します。
保護するチャネル	侵入を防御するためのチャネルリストを表示します。
すべての標準チャネルを選択	すべてのチャネルが自動的に選択されます。
すべての許可されたチャネルを選択	指定したカントリーコードで許可されているチャネルが自動的に選択されます。

デバイス分類ポリシーおよび侵入防止ポリシーに関しては、「2.13 WIPS の構成」をご参照ください。

2.11.4 LANポートの設定

[LANポート]タブでは、リンクアグリゲーションの設定をすることができます。リンクアグリゲーションを有効に設定すると、有線の2ポートが1つの論理リンクにマージされ、利用できる帯域幅が増加します。また、帯域幅をより効率的に利用します。論理オーバーヘッドは2つの物理リンク間で共有されます。

注意：リンクアグリゲーションを有効にする場合は、接続するスイッチングハブにもリンクアグリゲーションの設定をする必要があります。

リンクアグリゲーションの設定

リンクアグリゲーションを有効にすると、複数のポートを論理的に1つのリンクにマージできます。これにより、2ポート、５Gbpsのリンクスピードをもつアクセスポイントであれば、理論的には10Gbps近くの帯域幅を利用できるようになります。リンクアグリゲーションを有効にする場合、SSIDプロファイルの[**有線拡張**]オプションが無効になります。

リンクアグリゲーションを構成するには、以下の手順を実行します。

1. [**構成**]>[**デバイス**]>[**アクセスポイント**]>[**全般的**]の順に移動します。
2. [**リンクアグリゲーション**]を選択します。
3. [**送信ハッシュポリシー**]を選択します。次のオプションのいずれかを選択して、送信ハッシュポリシーを定義できます。
   - ●[**レイヤー2（MAC）**]
   - ●[**レイヤー3+4（IP+ポート）**]
   - ●[**レイヤー2+3（MAC+IP）**]

   送信ハッシュポリシーは、スイッチでは複数ある物理リンクがあるため、どれを使ってパケットを送信するかを決定するために使用されます。
   通常、ハッシュ関数はパケットの特定のヘッダ情報（例：送信元IPアドレス、送信先IPアドレス、ポート番号など）を使用してハッシュ値を計算します。
4. [**保存**]をクリックします。

アップリンクポートの設定

802.1X（EAP-TLS）認証により、アクセスポイントをスイッチングハブに接続した際、アクセスポイントの有線ポート（eth0）を認証することができます。認証前、認証失敗後、認証成功後の動作は接続先スイッチングハブの設定に依存します。
例として、認証失敗時は、ゲストVLAN(一時VLAN)を割り当て、認証成功後はデフォルトVLANを割り当てるなどがあります。

本機能を使用する場合、アクセスポイントへデバイス（TLS）証明書をアップロードする必要があります。アップロード方法は「アクセスポイントのデバイス証明書」をご確認下さい。
注意：アップリンクポート認証は[リンクアグリゲーション]と併用できません。

アップリンクポート認証を設定するには以下の手順を実行します。
1.[**設定**]>[**デバイス**]>[**アクセスポイント**]>[**LANポート**]タブに移動します。
2.[**アップリンクポートの認証**]チェックボックスをオンにします。
3.[**クライアント証明書タグ**]を選択します。
4. [**CA証明書のアップロード**]をクリックし、ローカルドライブからRadiusサーバーのCA証明書をアップロードします。
5.[**保存**]をクリックします。

優先ポートの設定

AP-6410 以外の AP では、両方の LAN ポートがスイッチに繋がっている場合、一方の LAN ポートがダウンした時にもう一方の LAN ポートにリンクを切り替えます。

PoE1 および PoE2 の 2 つのポートがありますが、番号による優先度はありません。最初に接続されたポートがプライマリポートとして動作します。

両方の LAN ポートが繋がっているとき、以下の設定で LAN1 をプライマリポートにできます。

1. **[設定]>[デバイス]>[アクセスポイント]>[LANポート]**タブに移動します。
2. **[優先ポート(LAN1)]**のチェックボックスをオンにします。
3. **[保存]**をクリックします。

注意：優先ポート(LAN1)は[リンクアグリゲーション]と併用できません。

2.11.5 グループの設定

グループは、作成後、2つの方法で設定できます。

●グループで使用可能なSSIDをオンにすると、SSIDの構成がグループに適用されます。

●SSIDをオンにしたくない場合は、デバイスと無線の設定を構成して保存すると、これらの設定をグループに適用できます。

SSIDをオンに切り替えて、構成をグループに適用

SSIDをオンにしてグループを構成するには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]>[SSID]の順に移動します。
2. ページの左上にあるメニューアイコン（3本の横線）をクリックします。
3. ロケーションペインの下部にあるグループのリストが展開されます。
4. 構成を適用するグループを選択します。グループを選択すると、右側のパネルのSSIDのリストが更新されます。
5. SSIDのリストから目的のSSIDを[**オン**]にします。上記の手順が正常に実行されると、SSIDの構成が選択したグループに適用されます。

フォルダー/グループから構成をコピーする

このオプションでは、フォルダー/グループから別のフォルダー/グループにWi-Fi構成設定をコピーできます。

設定を別のロケーションまたはグループにコピーするには、以下の手順を実行します。

1. [**構成**]>[Wi-Fi]に移動すると[SSID]タブが表示されます。
2. Wi-Fi設定をコピーするロケーションを選択し、[**設定を取得**]をクリックします。これにより、右側のペインに [**フォルダまたはグループの選択**]ウィンドウが開きます。

3. [**フォルダの選択**]タブで、設定をコピーするロケーションを選択します。

4. [**コピー**]をクリックします。
   既存の設定を選択したフォルダで置き換えるかどうかを尋ねるポップアップダイアログが表示されます。
5. ポップアップダイアログで[**次へ**]をクリックして、選択したロケーションにWi-Fi構成をコピーします。

同様に、グループナビゲータを使用して、あるロケーションにあるグループの設定を別のロケーションにある別のグループにコピーできます。

2.12 アラート

[構成]>[アラート]では、アラートの有効/無効、及び各アラートの動作を設定できます。アラートの重大度（高・中・低）や通知手段（表示・メール・通知）を定義できます。WIPS／システムアラートの場合には、セキュリティステータスへの影響（重大な問題へ発展するアラート）可否も定義できます。セキュリティステータスは、 **[モニター]>[アラート]**の[セキュリティステータスに影響する]列で「はい」と表示されるため、フィルタリングにより、簡単に影響範囲を確認できます。

アラート構成も、他の多くのポリシーと同様、ロケーション毎の設定となります。親ロケーションで定義されたアラート構成は子ロケーションへも継承されます（子ロケーションをカスタムフォルダー化することで、継承を解除することもできます）。アラートの有効/無効は**[構成]>[アラート]**の画面左下の[**アラートのアクティブ化**]で設定できます。

2.12.1 アラートの構成

ネットワーク上で問題が発生した際の、アラートが発生するタイミングとネットワーク管理者への通知方法を定義できます。例えば、特定のアラートのみを有効に設定することや、アラートを発生させるしきい値を追加（しきい値を超えるとアラートが生成）したりすることができます。また、アラートの通知方法も設定できます。通知方法には、UI上での通知、メール、通知（Syslogメッセージ、SNMPトラップなど）を選択できます。

アラートの通知方法	概要
表示	UI上へ通知します。アラート内容は[モニター]>[アラート]画面で確認することができます。
メール	Eメールで通知します。Eメール受信者の登録は、[構成]>[アラート]>[Eメールの受信者]から登録できます。
通知	サードパーティサーバーへSyslogメッセージ、SNMPトラップ、Webフックなどで通知します。サードパーティのサーバーの設定方法は2.19 サードパーティサーバーの連携をご参照下さい。

重大な問題であれば**[セキュリティ・ステータスに影響する]**を有効にします。

アラートは、Wi-Fi、WIPS、システムの3つのタイプに分類されます。

Wi-Fiアラート

Wi-Fiアラートは、接続時のトラブルや、通信品質に関する問題が発生した際にアラートを上げます。

例：Wi-Fi通信パフォーマンスアラート

5GHzで動作するSSIDへ接続する全クライアントの内、パフォーマンス低下の影響を受けたクライアント数が30%を超過した際にアラートを発生させ、UIとSyslog/SNMPサーバーへ通知したい場合、次の手順で設定できます。

1. **[構成]>[アラート]>[アラートを設定]>[Wi-Fi]>[ベースライン]**を選択します。
2. 「パフォーマンス不良によって影響を受けたクライアント」を選択します。
3. 「すべて」のSSIDと「5GHz」の周波数帯を選択します。
4. しきい値を「30」%で設定します。
5. アラート通知タイプで、「表示」と「通知」を選択し、保存します。

WIPSアラート

WIPSアラートは、セキュリティ上の問題が発生する可能性がある場合にアラート発生します。以下の表に、WIPSアラートの種類と説明を示します。

WIPSアラートタイプ	概要
ローグAP	不正アクセスポイントに関するアラートです。 エンタープライズネットワークに接続するアクセスポイント、禁止に分類したアクセスポイント、電波法違反チャネルで動作するアクセスポイントなどが不正に該当します。
誤設定AP	認定Wi-Fiポリシーに準拠しない設定で動作するアクセスポイントに関するアラートです。
誤動作 クライアント	ネットワークセキュリティの危険性がある誤動作クライアントに関するアラートです。 未認定に分類されたアクセスポイントへ接続する認定クライアントなどが誤動作に該当します。
中間者攻撃	中間者攻撃に関するアラートです。 Evil TwinやPS-POLL攻撃が中間者攻撃に該当します。 ※PS-Poll攻撃は、攻撃者がMACアドレスをスプーフィングすることで正規クライアントになりすまし、大量のPS-Poll フレーム（ウェイクアップ通知）を送信することで、アクセスポイントにバッファリングされたフレームを取得します。この攻撃は標的クライアントのフレーム 損失を引き起こす可能性があります。
アドホック ネットワーク	アドホックネットワークに参加している認定クライアントに関するアラートです。
防止	侵入防止機能に関するアラートです。 侵入防止動作中や防止可能デバイス数に達したなどが該当します。
DoS	DoS攻撃に関するアラートです。
探索	「過度のNULLプローブ」のアラート

例：禁止 AP のアクティベート

アクティブな禁止AP（[システム]>[禁止アクセスポイント]へ手動登録したアクセスポイント）の存在は、ネットワークに深刻な脅威をもたらす可能性があります。次の手順で「禁止APのアクティベート」アラートを設定できます。

1. **[構成]>[アラート]>[アラートを設定]>[WIPS]>[ローグAP]**を選択します。
2. 「禁止APがアクティブです」の項目の「表示」「メール」「通知」「セキュリティ・ステータスに影響する」にチェックします。
3. 「重要度」を高にして、保存します。

システムアラート

システムアラートは、クラウドサーバーとアクセスポイントに関するイベントがトリガーとなります。システムアラートは、WIPSアラートと同様、セキュリティ・ステータスへの影響、重大度の設定が可能です。

<u>アラートの自動削除</u>

UIへ保存するアラート数やアラートの保存期間（アラートを自動削除するまでの期間）を設定できます。期間はアラートが生成された時間から始まります。

[構成]>[アラート]画面の右上の **[自動削除]**のクリックで設定画面が表示されます。

※Wi-Fiアラートは保存アラート数の設定ができません。

<u>デフォルト設定を復元する</u>

デフォルトのアラート構成（当社推奨のアラート）を復元できます。復元はアラートカテゴリ単位での実施となります。

※Wi-Fiアラートは復元（デフォルトである未設定状態化）ができません。

2.12.2 アラートの確認

アラートは、Wi-Fi、WIPS、システムの3つのタイプに分類されます。さらに、アラートの性質に基づいて、次のように分類されます。

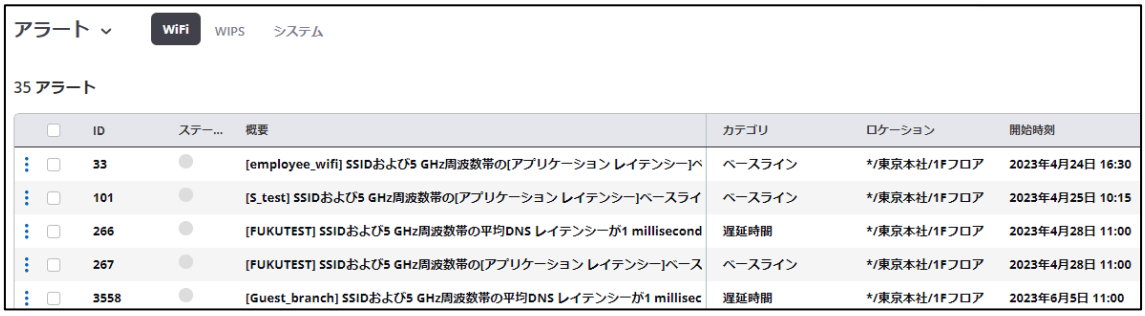
●瞬時：長期にわたって持続しない1回限りのイベントに対して生成されたアラート。

●ライブ：長期間続くイベントに対して生成されたアラート。このアラートは、何らかの条件によりトリガーされ、条件が真になるまで持続します。

●期限切れ：アラートのトリガー条件が満たされない場合、期限切れになります。

Wi-Fiアラートの確認

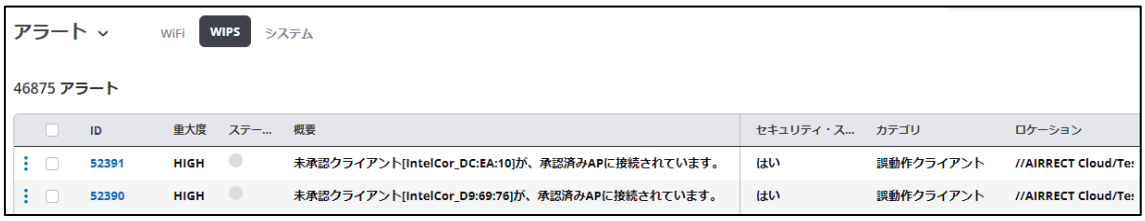
[モニター]>[アラート]>[WiFi]で、Wi-Fiアラートを確認できます。



Wi-Fiアラートは、ネットワーク接続と、クライアント認証失敗や遅延などのネットワークのパフォーマンスについてのイベントです。

WIPSアラートの確認

[モニター]>[アラート]>[WIPS]で、WIPSアラートを確認できます。

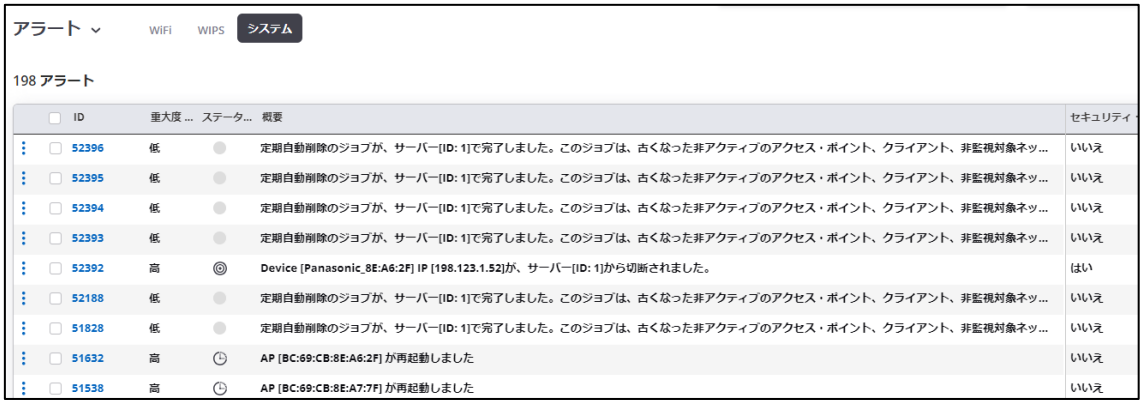


WIPSアラートは、ネットワークにセキュリティ脅威をもたらす可能性のある脆弱性と攻撃についてのイベントです。「**セキュリティステータス**」列では、セキュリティへの影響有無を確認できます。アラートIDのクリックで詳細情報を確認できます。

「**応答トレイル**」は、ネットワーク管理者が、どのアラートを承認および影響を与えると判断したか等をメモとして記録することで、他のネットワーク管理者へ知らせるための機能であり、「**推奨アクション**」は、ネットワーク管理者へネットワークを保護するために実行できるアクションを提供するための機能です。

システムアラートの確認

[モニター]>[アラート]>[システム]でシステムアラートを確認できます。



システムアラートは、Wi-Fiサーバーとインフラストラクチャの状態についてのイベントです。「**セキュリティステータス**」列では、セキュリティへの影響有無を確認できます。アラートIDのクリックで詳細情報を確認できます。「**応答トレイル**」は、ネットワーク管理者が、どのアラートを承認および影響を与えると判断したか等をメモとして記録することで、他のネットワーク管理者へ知らせるための機能であり、「**推奨アクション**」は、ネットワーク管理者へネットワークを保護するために実行できるアクションを提供するための機能です。

セキュリティステータス

ロケーションのメニューアイコンから[**ステータスを表示する**]>[**セキュリティステータス**]を選択すると、脆弱なロケーションが赤色で表示されます。脆弱なロケーションとは、セキュリティステータスに影響するアラートが発生中であるロケーションが該当し、この設定については、「アラートの構成」をご参照ください。

2.13 WIPSの構成

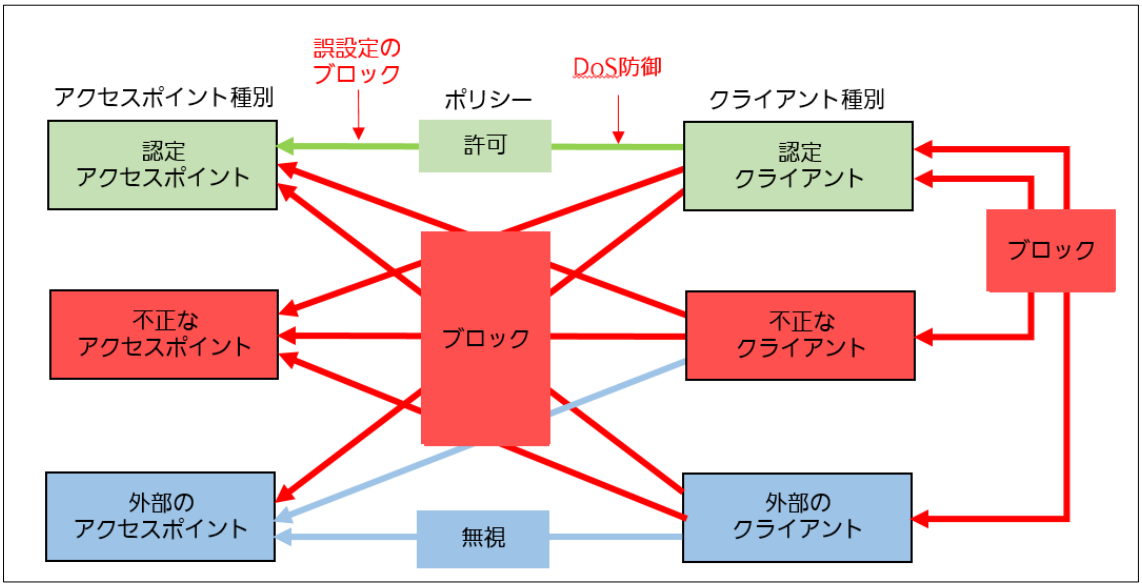
悪意のある不正なデバイス、または企業のセキュリティポリシーに違反するWi-Fi接続の存在を手動で追跡することは現実的には困難です。ワイヤレス侵入防止システム(WIPS)は、そのプロセスを自動化しWi-Fiベースの脆弱性や攻撃から企業内ネットワークを保護できます。また、企業内のアクセスポイントの物理的なロケーションを追跡することもできます。AIRRECT CloudのWIPSは、さまざまな技術を使用してアクセスポイントを次のように分類します。

●認定：企業が所有、管理している、正式な端末

●外部：周辺にある、無関係な端末

●不正：管理ネットワーク上にあるが管理していない不正な端末

これはWi-Fiセキュリティポリシーを適用するための基盤として機能します。正確なデバイス分類に基づき、WIPSは脅威をもたらすアクセスポイントと接続を自動的にブロックできます（以下の図においては、赤色で示されています）。



WIPSは以下の3種類の防止設定ができます。

●アクセスポイント防止:

不正アクセスポイント、禁止されたアクセスポイント、誤って設定されたアクセスポイントなどの脅威をもたらすアクセスポイントへのすべての接続を自動的にブロックします。

●クライアント防止:

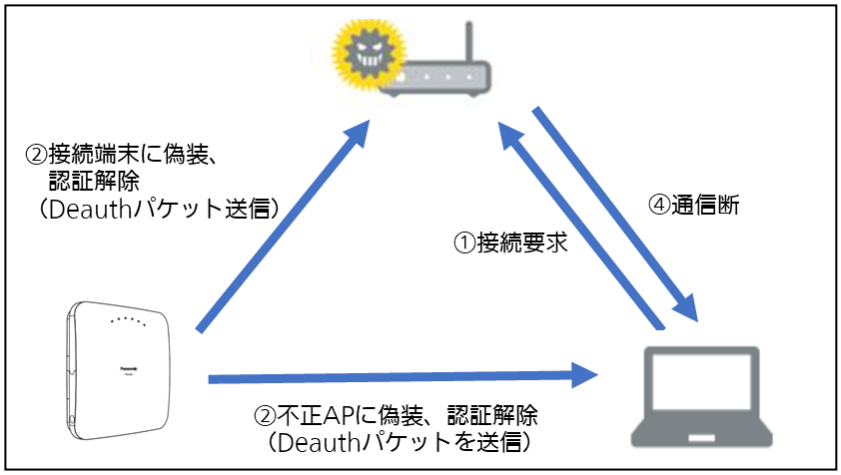
関係するクライアントのタイプ（承認済み、ゲスト、不正、外部、禁止など）および接続しようとするアクセスポイント、クライアントのタイプに基づきクライアント接続を自動的に防止することで、脅威をもたらすさまざまな種類のWi-Fi接続をブロックできます。

●脅威防止:
DoS攻撃をブロックし、ハニーポットやEvil Twin APなどの不正デバイスを遮断できます。

WIPS機能は、アクセスポイント自動分類ポリシーに従って、近隣のアクセスポイントを認定、不正、または外部として自動的に分類します。WIPSはアクセスポイントの多目的アンテナによって、バックグラウンドスキャンで行われます。侵入防止方法が以下のように、複数の方法で行われます。これらは、AIRRECTが自動で最適な防御方法を選択します。

1. **破棄：**クライアントが接続要求を送信すると、アクセスポイントは、定義済みのクライアント自動分類ポリシーに従って、不正または許可されたクライアントか判別します。不正であると認識された場合、アクセスポイントはパケットを破棄し続けます。

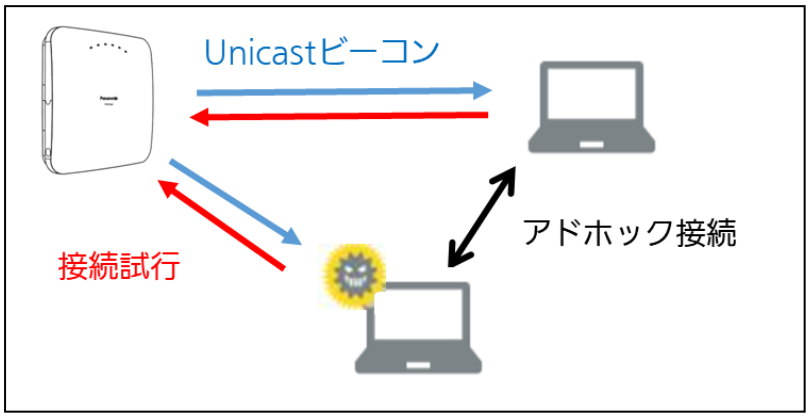
2. **認証解除：**動作に問題のあるクライアントが不正なアクセスポイントに接続してネットワークにアクセスしようとすると、802.11メッセージング形式に準拠した認証解除パケット(Deauthパケット)を送信することにより、許可された接続を防止します。



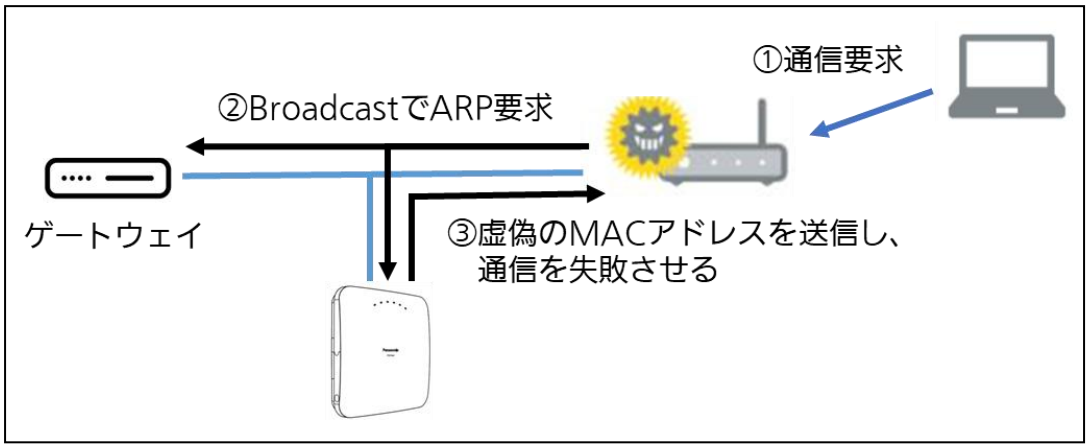
暗号化されたアドホッククライアントの防止をする際も、同様に防止ビーコンが送信されます。アクセスポイントがアクティブの場合、アクセスポイントの自動分類で定義されているすべての不正な接続のデータをリストに保存し続けます。アクセスポイントがオフラインになった場合でも、保存したリストを元に不正アクセスポイントを検出し、自動的に防止することができます。
Deauthパケットによる防御は、以下のような場合は使用できないため、別の防御方法を取ります。
・無線管理フレームが11w機能等により暗号化されている（WPA3利用時は不可）
・センサー上の無線防御機能をフルで利用している
・不正な無線APが送信できないチャネル上に存在している

3. **ワイヤレスARP防止：**不正クライアントがアドホック接続をしている際、AIRRECT AP

もアドホック接続に参加しUnicastビーコンを発信します。AIRRECT APとアドホック端末に誤った接続要求を行い、接続エラーを発生させることで、アドホック接続の通信を止めます。信号は継続的に送り続け、アドホック通信をさせないようにします。



3. **有線ARPポイズニング**：無線接続で遮断が出来ないようなケースや、定義された侵入防止レベルを超えた場合に、本技術により遮断が実行されます。例えば、無線ごとに1つのチャネルを阻止する「ブロック」レベルを選択していて、脅威をもたらすデバイスが検出された場合は、有線ARPに切り替えます。
ARPポイズニングパケットが有線インターフェイスから送信され、ワイヤレスクライアントが不正なアクセスポイントを介して安全な有線ネットワークに接続されることを防ぎます。パケットは許可されたクライアントにユニキャストされるため、他の接続には影響しません。



5. **選択的ＮＡＶ(Network Allocation Vector)**：DOS 攻撃により、空間使用率が大量に消費され、認定端末が通信できなくなることを 802.11w の選択的 NAV によって防止します。クライアントに一定のタイムスロットを許可し、ＣＴＳフレームを利用して本来通信すべきデバイスが正常にパケット送信できるようにします。DoS 攻撃は、完全にブロックすることができないため、根本原因の調査が必要となります。

2.13.1 アクセスポイントの自動分類

WIPSは周囲の電波を継続的にスキャンし、近くに存在する他のアクセスポイントを検出します。検出されたアクセスポイントが、問題のないデバイスかどうか、以下のようなステップで自動的に判断されます。

1.新しいアクセスポイントが検出されると、最初は未分類と見なされます。

2.検出されたアクセスポイントが管理された有線ネットワークに接続されているかどうかを判断します。

- アクセスポイントが管理された有線ネットワーク上にある場合、認定Wi-Fiポリシーに準拠しているかどうかに応じて、認定、または不正デバイスとして事前に分類されます。
- アクセスポイントが管理された有線ネットワーク上にない場合、外部デバイスとして事前に分類されます。

3. 有線ネットワーク上にあり、[**認定Wi-Fiポリシー**]に準拠しているAIRRECT Cloud管理のアクセスポイントは、自動的に承認済みとして分類されます。
アクセスポイントの自動分類ポリシーを使用すると、WIPS機能で不正なアクセスポイント(ローグアクセスポイント)、または外部のアクセスポイントとして自動的に分類できます。

初期値では、アクセスポイントの自動分類は有効になっています。[**構成**]>[WIPS]>[**アクセスポイントの自動分類**]でポリシーを編集できます。

以下の[**認定APリストのロック**]機能を使用して、認定済みのアクセスポイントのリストを固定して、それ以降に接続するアクセスポイントが自動的に承認済みとして分類されないようにすることもできます。

アクセスポイントをロックすると、新しく接続されたアクセスポイントは不正な端末（ローグ・アクセスポイント）の可能性があると分類されます。
また、Wi-Fiポリシー設定などにより、外部やローグの可能性がある端末として分類したアクセスポイントを、以下のチェックボックスを選択することにより、割り振ります。

各アクセスポイントの分類タイプと、自動振り分けは以下の通りです。

判定タイプ	自動判定ルール（初期値）
認定アクセスポイント	管理ネットワークに接続されているAIRRECT AP
ローグアクセスポイント	管理ネットワークに接続されている不正なAP
外部アクセスポイント	管理ネットワーク外の近隣のアクセスポイント
誤設定アクセスポイント	**構成＞WIPS＞認定WiFiポリシー**の設定した定義に沿わないアクセスポイント
[外部の/ローグの/認定されている]可能性があるアクセスポイント	デバイスロックポリシーでロック後に検知したアクセスポイントや、RSSIポリシーにより信号強度しきい値を下回ったアクセスポイント、その他、不確定AP同様に正確な情報が取れないが、ネットワークポリシーが一致していない場合など、確証が取れていない状態。ネットワーク環境を確認の上、手動設定を推奨します。
未分類アクセスポイント	分類前のアクセスポイント。WIPS機能により、アクセスポイントを検知すると初めに未分類と認識します。
不確定アクセスポイント	分類が出来なかったアクセスポイント。有線側のネットワーク情報が取得できなかった際に分類されます。その原因として、無線リンクの暗号化がされており、且つアクセスポイントにNAT設定されている場合や、有線LANに接続されていない無線APなどが当てはまる可能性があります。

2.13.2 クライアントの自動分類

無線クライアントを接続すると、セキュリティポリシー等により、クライアントは以下のように分類されます。

●**認定**：管理されているクライアントであり、ネットワーク管理者のセキュリティポリシーに準拠しています。管理しているアクセスポイント以外の、認定していないアクセスポイントには接続させないような設定ができます。

●**ゲスト**：通常、ゲストWi-Fiのネットワーク接続のみ許可されており、内部ネットワークへのアクセスは拒否、または制限されているクライアントです。

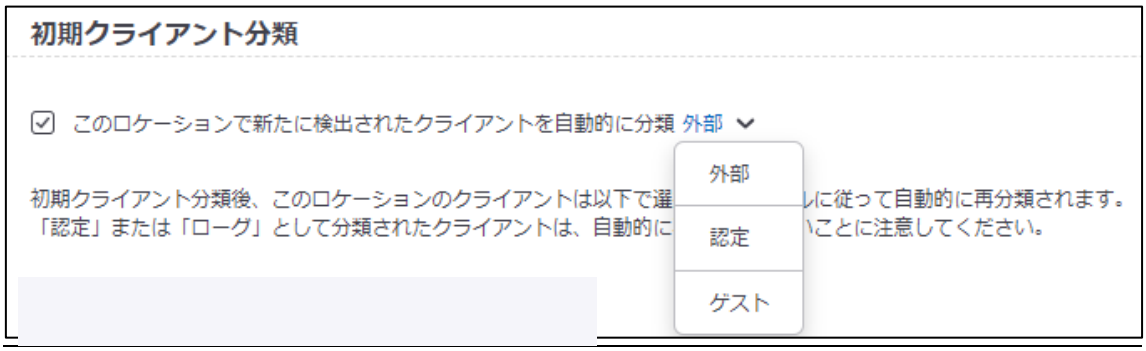
●**外部**：管理下のアクセスポイントが検出した管理対象外のクライアントです。
その動作が管理ネットワークのセキュリティに脅威を与えない限りは無視されます。

●**ローグ**：不正アクセスポイントに接続するなどして、管理下のネットワークに侵入しようとする不正なクライアントです。

上記の各クライアントのアクティビティを監視し、クライアントの不正アクセスをブロックする必要があります。AIRRECT Cloudは、クライアントを自動的に分類することが可能です。クライアントの自動分類ポリシーは、[**構成**]>[WIPS]>[**クライアントの自動分類**]で設定できます。

初期値では、クライアントは未分類であり、接続するアクセスポイント、または無線ネットワークタイプに基づいて分類されます。オプションで、新しく検出されたクライアントを外部、認定、ゲストのいずれかに分類するルールを設定することでアソシエーションに基づいて再分類できます。アソシエーションベースの分類は、アクセスポイントのタイプに基づいて行うことができます。

[**このロケーションで新たに検出されたクライアントを自動的に分類**]を選択することで、強制的に任意のクライアント分類に設定することも可能です。



認定アクセスポイントに接続しているクライアント

認定アクセスポイントに接続されたクライアントは自動でクライアントのタイプが分類されますが、外部クライアントやゲストクライアントを認定クライアントやローグクライアントに強制的に分類することができます。初期値を以下になります。

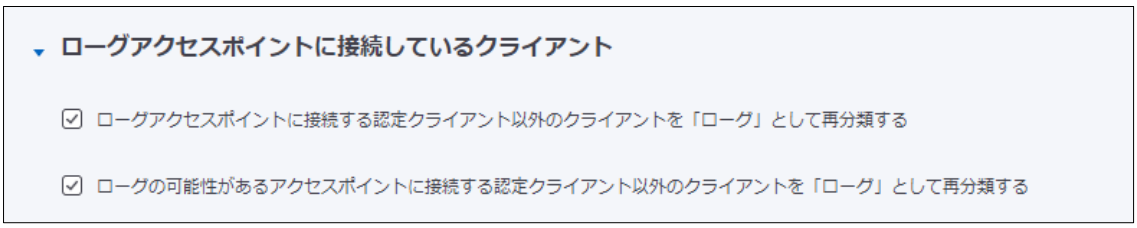
また、以下の特殊なケースにおける分類に対応します。

●[**誤設定されている認定アクセスポイントに接続しているクライアント**]のチェックボックスを選択すると、[**認定WiFiポリシー**]で設定したアクセスポイント以外のアクセスポイントと接続したときに、未分類のクライアントとして認識されます。

●[**有線ネットワークに接続されていないアクセスポイントと接続しているクライアント**]のチェックボックスを選択すると、認定アクセスポイントと同じ動作をしているように見えても、管理ネットワーク上で通信パケットを検知できないアクセスポイントと接続しているクライアントを未分類のクライアントとして認識されます。例えば、AIRRECT Cloudとの接続が切断されているが、アクティベートをしているアクセスポイントなどが該当します。

ローグアクセスポイントに接続するクライアント

クライアントが不正なアクセスポイントとのアソシエーションを試みる場合、再分類はクライアントの初期分類とアクセスポイントの分類に基づいて行われます。初期値は以下になります。



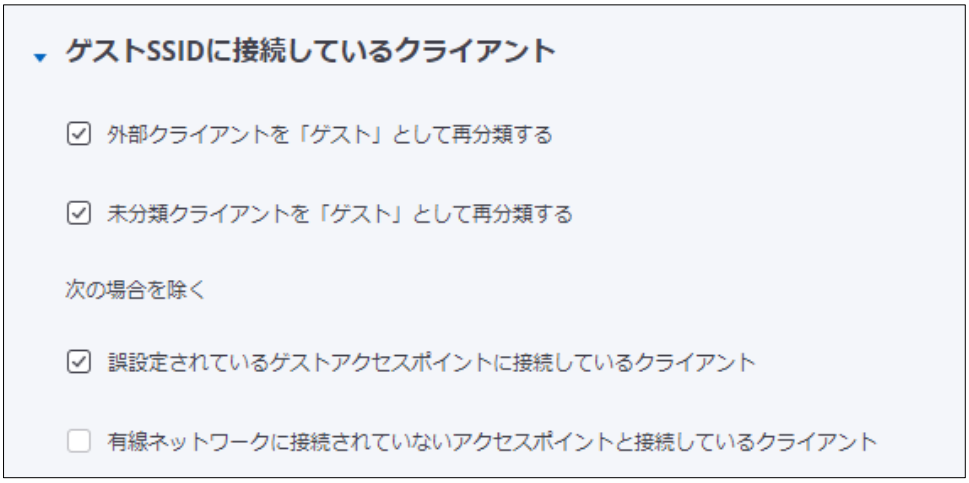
●[**ローグアクセスポイントに接続する認定クライアント以外のクライアントを「ローグ」として再分類する**]のチェックボックスを選択すると、未分類クライアントを含む、認定クライアント以外の全ての新規クライアントを不正なクライアントとして認識します。

●[**ローグの可能性があるアクセスポイントに接続する認定クライアント以外のクライアントを「ローグ」として再分類する**]のチェックボックスを選択すると、不正の可能性があるアクセスポイントへ接続したクライアントを不正なクライアントとして認識します。

注意：クライアントが手動で不正または承認済みとして分類されると、削除されて再度検出されない限り、クライアントは自動的に再分類されません。

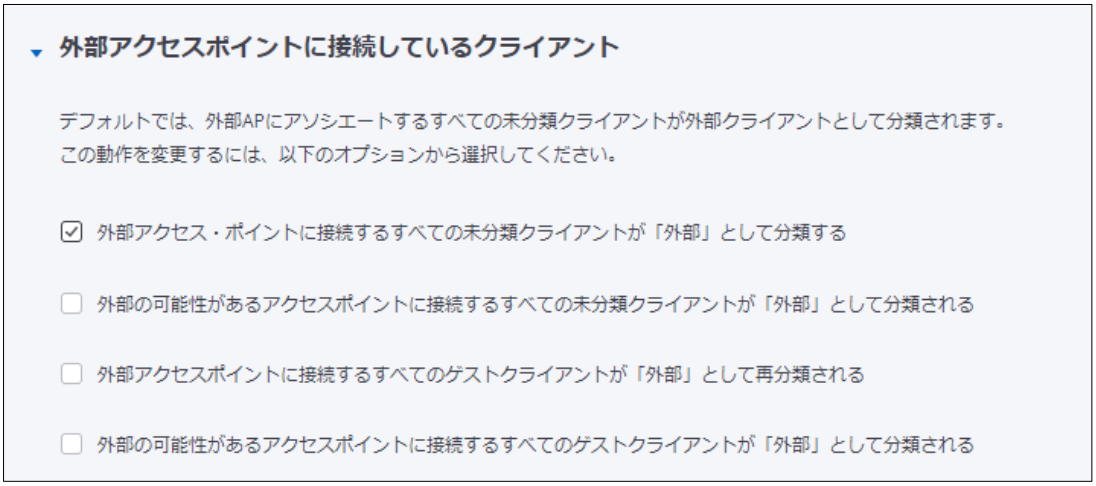
ゲストSSIDに接続しているクライアント

認定アクセスポイントに接続しているクライアントと同様に、ゲスト SSID に接続しているクライアントについても分類することができます。初期値は以下の通りです。



外部アクセスポイントに接続しているクライアント

外部アクセスポイントと接続をするクライアントを、外部のクライアントとして分類する設定です。初期値は以下の通りです。



コーポレート・ネットワークへのブリッジング

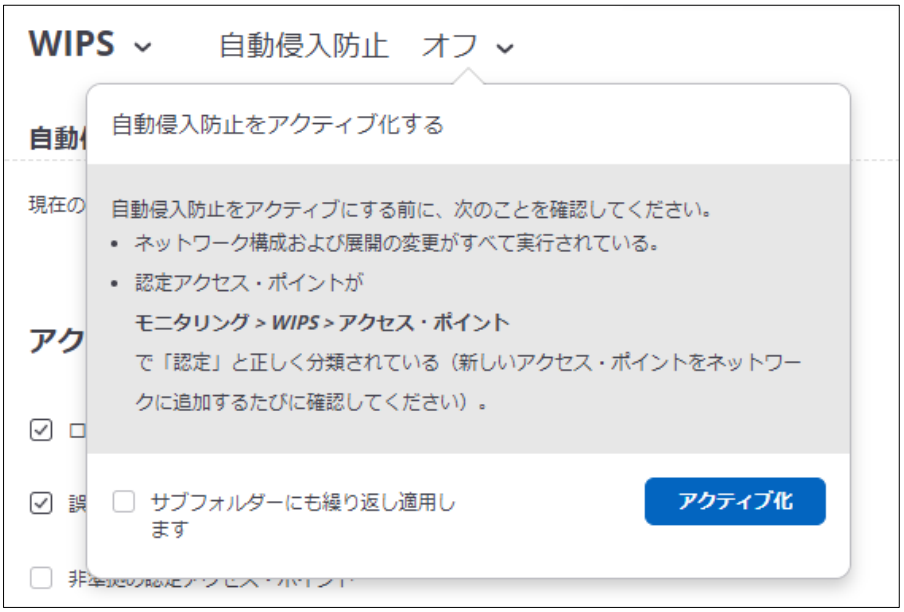
認定以外のクライアントが監視対象サブネットに対して、テザリング機能等で Wi-Fi/ICS ブリッジを実施していることが検知されると、該当のクライアントを不正として再分類します。初期値は有効です。

RSSIベースのクライアント分類

クライアントとアクセスポイント間の信号強度が設定したしきい値より低い場合に、認定、ローグ、ゲストのいずれかに分類することができます。RSSI ベースで分類できるクライアントは、未分類クライアントか、外部クライアントであり、チェックボックスを選択することで適用できます。

2.13.3 自動侵入防止

[**構成**]>[WIPS]>[**自動侵入防止**]の順番に移動し、使用する環境に応じて、アクセスポイントやクライアントをどのように防止するか設定することができます。
自動侵入防止設定は初期値ではオフになっています。有効化するには、以下の侵入防止設定でオンにするか、または[**ダッシュボード**]>[WIPS]からも設定が出来ます。



自動侵入防止レベル

WIPS機能は、以下に示す4つのレベルの自動侵入防止機能があります。

レベル	無線チャネルごとの防止数
ブロック	1
中断	2
割り込み	3
デグレード	4

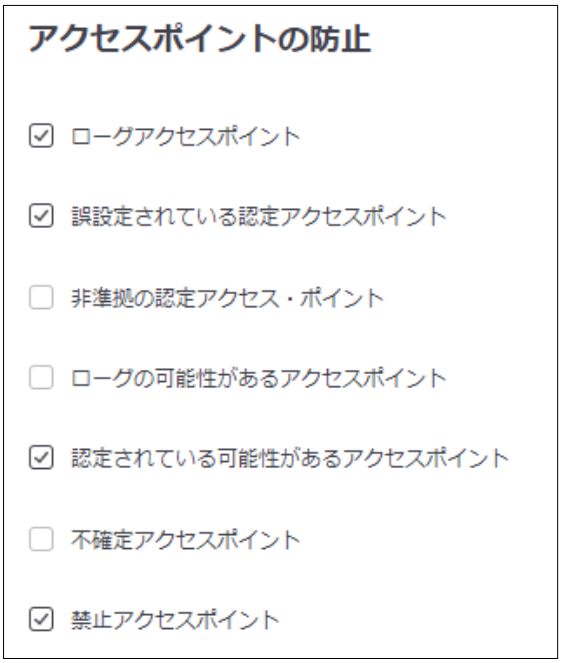
各自動侵入防止レベルは、アクセスポイントが防止できる無線ごとのチャネル数を定義します。侵入を検出するために、アクセスポイント無線は動作している周波数帯域内のすべてのチャネルをスキャンし、各チャネルにおいて、120ミリ秒を費やします。
1つのスキャンサイクルは、アクセスポイント無線がすべてのチャネルのスキャンを1回完了するのにかかる時間です。各レベルで、最大10台の侵入デバイスを防止できます。

例1：侵入防止レベルが 「ブロック」 に設定されているアクセスポイントが、チャネル36への侵入を検出する場合
アクセスポイントは帯域ごとに1つのチャネル（この場合はチャネル36）を防止できます。次に、スキャンサイクル中、アクセスポイントはより頻繁にチャネル36を検査し、認証解除パケットを送信してチャネル36での不要な通信をブロックします。(その後、他のチャネルで検出された侵入は「保留」リストに入れられます。）

例2：侵入防止レベルが 「中断」 に設定されているアクセスポイントが、2つのチャネルで侵入を検出する場合
2つのチャネル間で認証解除パケットの送信を行います。これにより、2つのチャネルのそれぞれで不要な通信が中断されますが、2つのチャネルを交互に検査するため、完全にはブロックされず、侵入デバイスに属する一部のパケットが通過する可能性があります。したがって、「中断」は「ブロック」よりも弱い予防策になります。
「割り込み」と「デグレード」も同様に、アクセスポイントが認証解除パケットの送信に費やす時間をより多くのチャネル間で分割するほど（防止される無線ごとのチャネル数が多いほど）、防止による効果が弱まります。Wi-Fi環境のニーズに基づいて侵入防止レベルを選択してください。初期値では、侵入防止レベルは「中断」に設定されています。

アクセスポイントの防止

自動で防止する不正なアクセスポイントの種類を設定することができます。初期値は以下の通りです。



禁止アクセスポイントの設定については、『禁止デバイスリスト』をご参照ください。

クライアントの防止

防止するクライアントのタイプを選択できます。 クライアント通信のタイプは、次の2つの要素に基づいています。

●クライアントの自動分類によって決定されたクライアントのタイプ
（不正、認定、外部、またはゲスト）

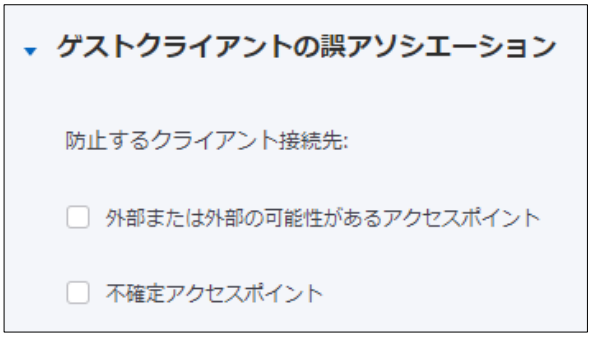
●クライアントが接続を試みるアクセスポイント

認定クライアントの誤アソシエーション

認定済みのクライアントは、付近にある無関係の外部アクセスポイントともアソシエートを試みる可能性があるため、不明なSSIDやアクセスポイントとの接続を拒否することが推奨されます。初期値は以下の通りです。

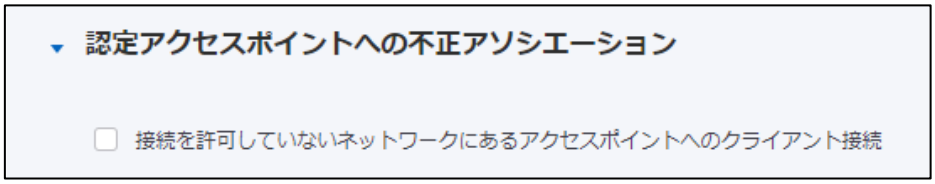
ゲスト・クライアントの誤アソシエーション

ゲストに分類されたクライアントが、認定アクセスポイントではなく外部のアクセスポイントや、不確定なアクセスポイントに接続することを防止したい場合、チェックボックスを選択します。



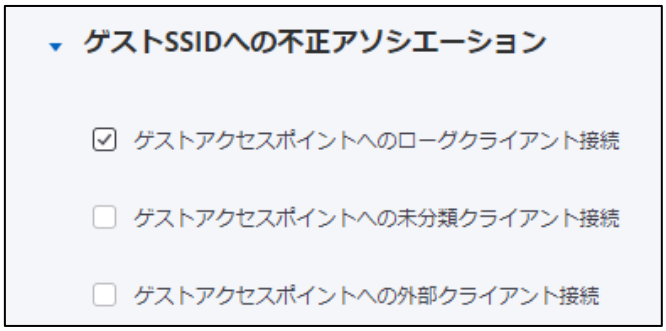
認定アクセスポイントへの不正アソシエーション

ゲストWi-Fiアクセスの場合、無許可のクライアントが「ゲスト」クライアントとしてマークされる前に、アクセスポイントにアソシエートする必要がありますが、クライアントの自動分類がゲストSSIDに接続しているすべての外部クライアントと未分類クライアントを「ゲスト」として再分類するように設定されていると、許可されていないクライアントを「不正クライアント」として接続を拒絶する場合があります。本設定を無効にすることで、このようなアソシエーションを許可することができます。



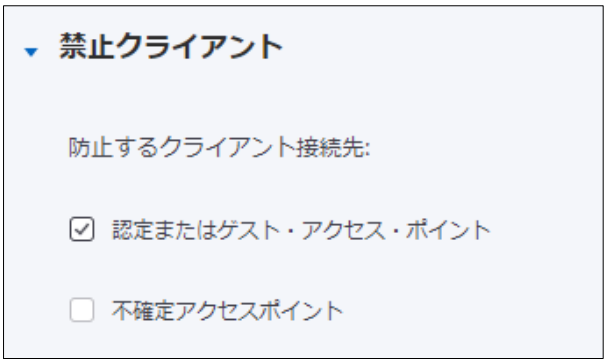
ゲストSSIDへの不正アソシエーション

SSID 設定で、ゲストに設定した SSID に対し接続しようとする不正なクライアント、または未分類、外部のクライアントからのアソシエーションを遮断します。
初期値は以下の通りです。



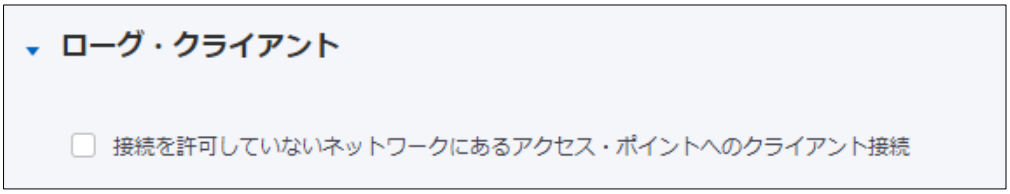
禁止クライアント

禁止クライアントで指定されているクライアントを、認定アクセスポイントやゲスト SSID への接続を遮断できます。禁止クライアントの設定は、『禁止デバイスリスト』をご参照ください。



ローグ・クライアント

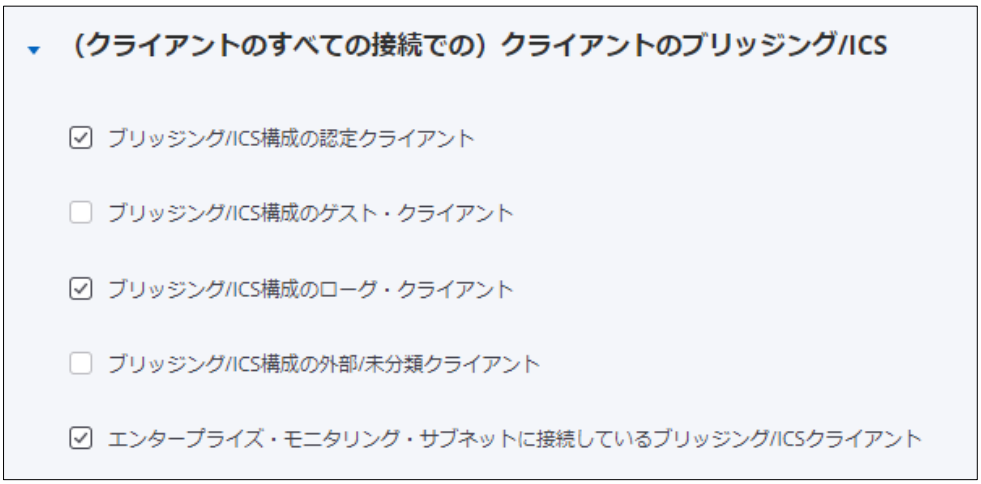
『Wi-Fi ネットワークを定義しない』で設定をした非 WiFi 環境にアクセスポイントが設置されている場合、そのアクセスポイントへのクライアントの接続を遮断します。



クライアントのブリッジング/ICS

ブリッジングとは、有線ネットワークに接続されたPCなどがアクセスポイントとして動作させることができる機能であり、インターネット接続の共有（ICS）は、PCを他のクライ

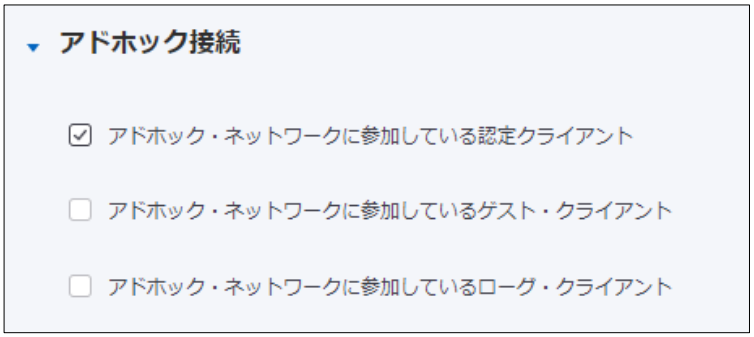
アントが直接接続できるルータとして動作させるサービスです。どちらの方法も、管理ネットワークへの不正アクセスの可能性が発生します。ブリッジング、または、ICSを防止することが可能です。初期値は以下の通りです。



尚、本設定で記載の「エンタープライズ・モニタリング・サブネット」は、[**構成**]>[**デバイス**]>[**アクセスポイント**]のセキュリティタブで設定した[**VLANモニタリング**]の監視範囲になります。

アドホック接続

アドホック・ネットワークに接続しているクライアントを分類ごとに遮断します。
初期値は以下の通りです。



脅威の防止

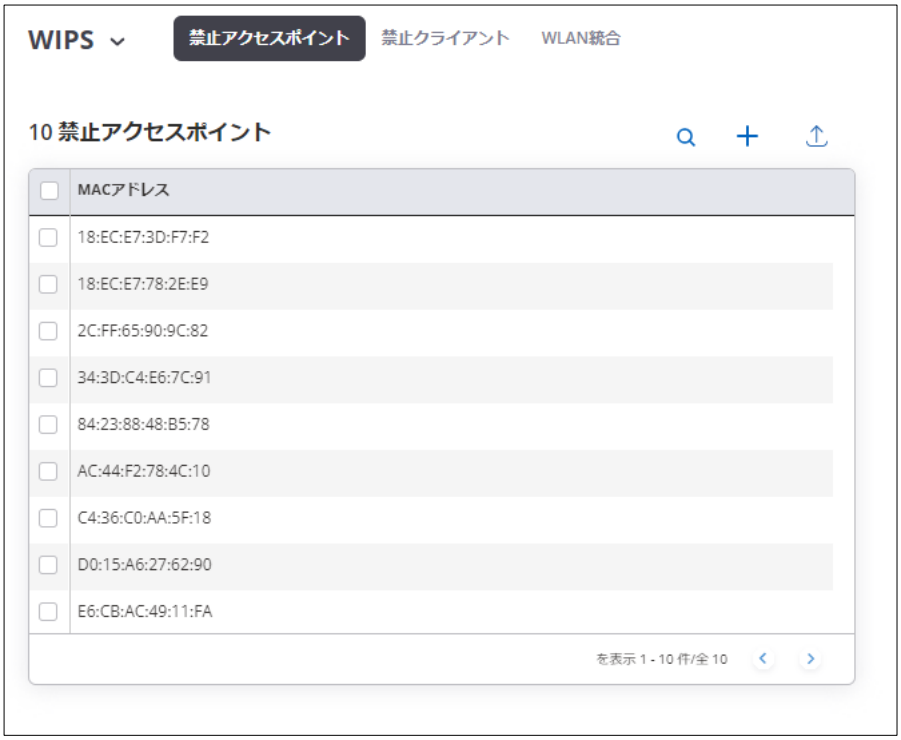
次のような悪意のある攻撃から自動的に保護するように設定ができます。

●**ハニーポット/Evil Twin**：正規のSSIDと同様のSSIDを持つ不正なアクセスポイントを企業や店舗の付近に設置し、接続させることで情報を盗聴する攻撃です。

禁止デバイスリスト

必要に応じて、特定のアクセスポイントやクライアントを企業のネットワークにアクセスすることを禁止できます。例えば、企業のノートPCが盗まれた場合、そのPCからのネットワークへの不正アクセスを制限するようなケースで利用できます。

これは、個々のアクセスポイント、または、クライアントのMACアドレスを入力するか、カンマ区切りのMACアドレスのリストを含む.csvファイルをアップロードすることによって実行できます。禁止デバイスリストを追加するには、[**システム**]>[WIPS]に移動します、[**禁止アクセスポイント**]または[**禁止クライアント**]で行います。



禁止されたデバイスは、ロケーションツリーの最上位またはルートフォルダでのみ定義できます。さらに、リストから禁止されたアクセスポイント、または、クライアントが近くで検出された場合に警告するアラートを設定できます。禁止されたアクセスポイント、または、クライアントとのWi-Fi接続は、関連する侵入防止ポリシーを設定することによって自動的に防止することもできます。

2.13.4 認定WiFiポリシー

認定WiFiポリシーにより、指定した通信以外の動作をするSSIDを検知し、アクセスポイントとクライアントを以下の３つに自動的に分類することができます。

●認定：所有、管理している、正式な端末

●外部：周辺にある、無関係な端末

●ローグ：管理ネットワーク上の不正な端末

自動デバイス分類は、以下の観点から定義されます。

1. 無線ネットワークの特性（SSIDがゲスト用か否か等）、使用される認証と暗号化のタイプ、特定のエンタープライズサブネットワークへのSSIDマッピング、許可されたメーカーなど
2. 事前に許可された端末、監視対象のネットワークに接続されている端末、アクセスポイントの信号強度（RSSI）

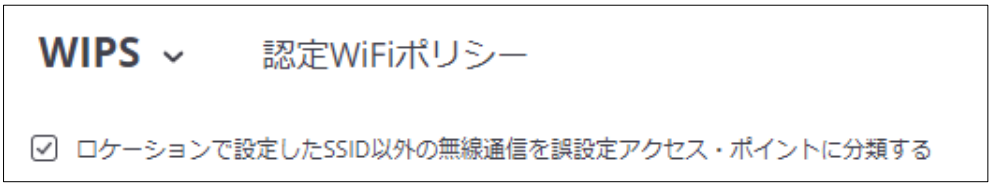
ポリシーに反するSSIDを出力するアクセスポイントは、「誤設定されているアクセスポイント」として分類されます。

SSIDプロファイル設定を使用し、アクセスポイントで実行されている構成を認定Wi-Fiとするか、SSIDごとに認証済みWi-Fiプロファイルを作成するかのいずれかの方法でポリシーを実装できます。それぞれの方法について以下に記載します。

SSIDプロファイル設定の使用

[**構成**]>[Wi-Fi]>[SSID]で設定したSSIDプロファイルについては認定WiFiとして扱う方法となります。

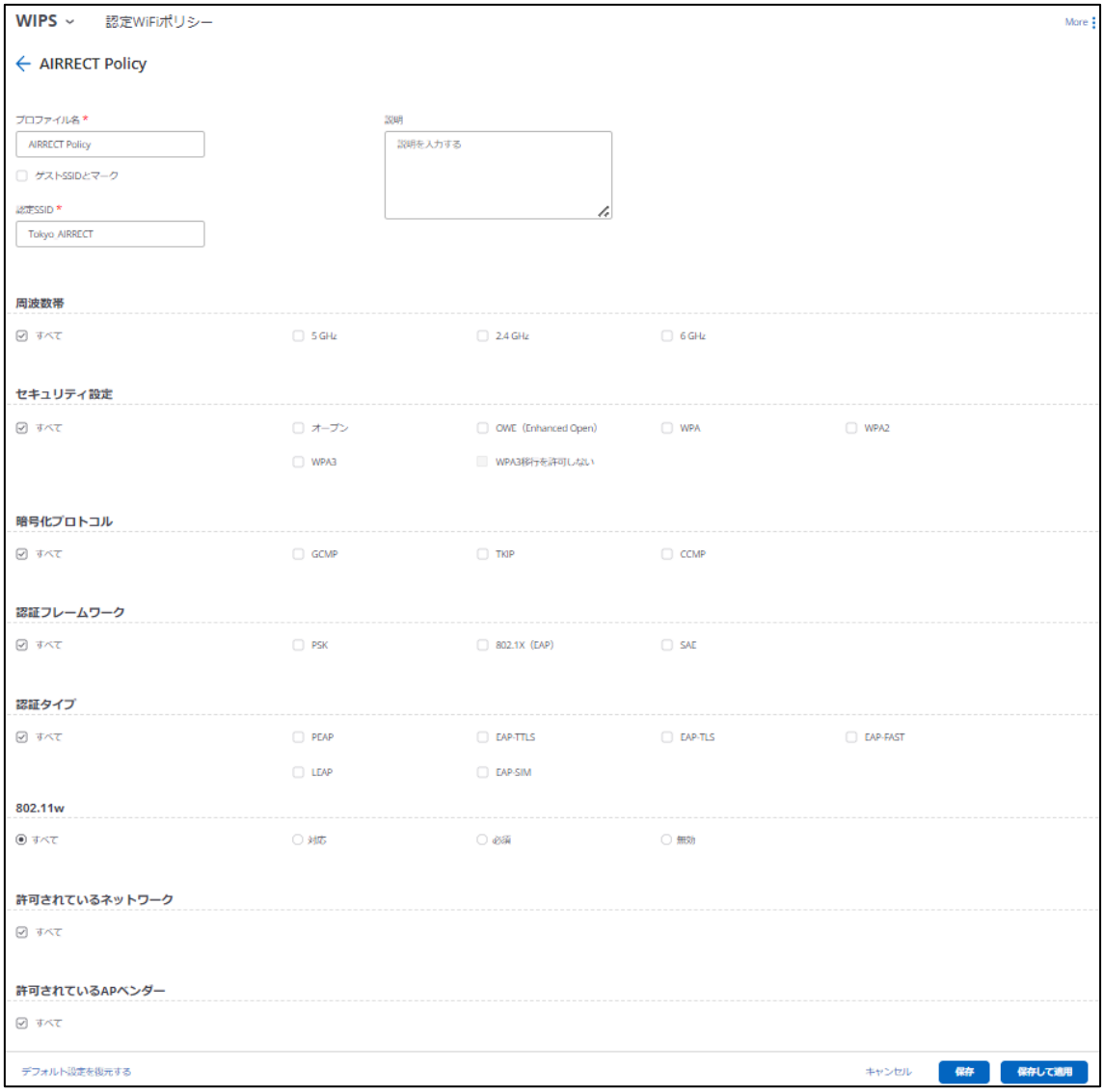
[**構成**]>[WIPS]>[**認定WiFiポリシー**]の順に移動して、[**ロケーションで設定したSSID以外の無線通信を誤設定アクセス・ポイントに分類する**]を有効にすることで実行できます。



このオプションは初期値有効になっています。設定済みのSSIDプロファイルの情報に関わらず、認定Wi-Fiプロファイルを手動で設定したい場合は、本チェックボックスを無効にする必要があります。

SSIDごとの認定Wi-Fiプロファイル

[認定WiFiプロファイルを追加する]ボタンから、任意の設定を行います。
ここで設定したSSIDや周波数帯、セキュリティ設定等と異なるSSIDをアクセスポイントが検知した場合、誤って設定されたSSIDとしてマークされます。

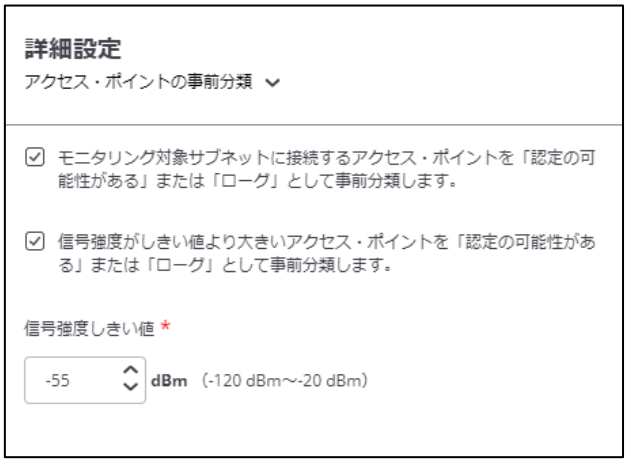


[モニター]>[WIPS]>[アクセスポイント]の[分類]列でフィルタリングすると、誤設定されたSSIDを実行しているアクセスポイントを確認できます。

アクセスポイント名を選択すると、SSIDの誤設定理由を確認できます。誤設定されたSSIDを実行しているアクティブなアクセスポイントは、[モニター]>[WIPS] および [モニター]>[Wi-Fi]タブで橙色にマークされます。

WIPS詳細設定

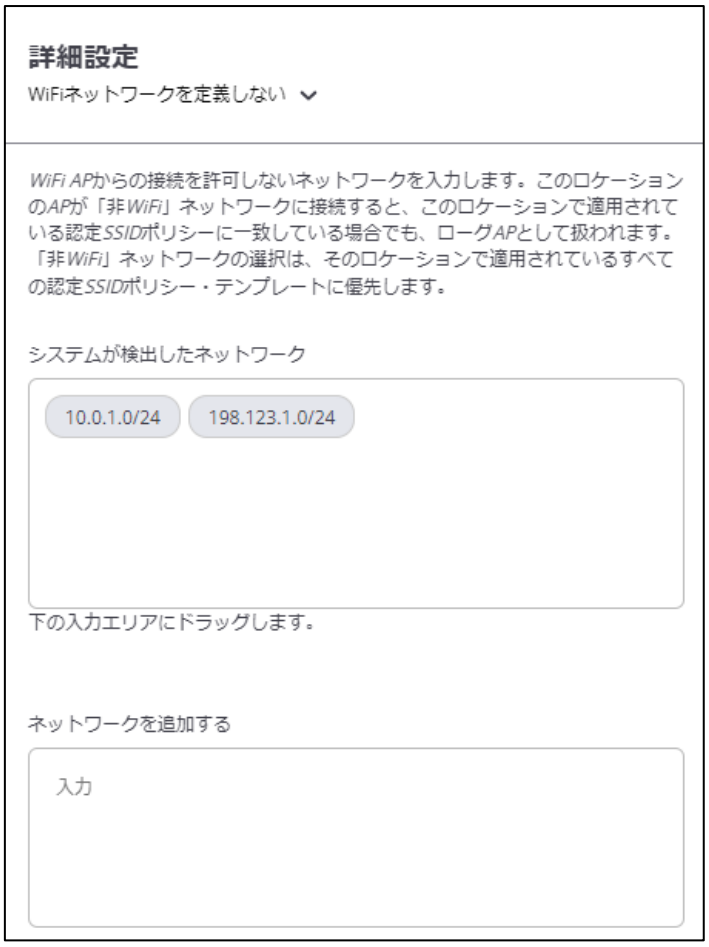
[構成]>[WIPS]>[認定 Wi-Fi ポリシー]の下部にある[詳細設定]ボタンを押すと、アクセスポイントを事前に分類するための詳細設定を定義できます。初期値では、監視対象ネットワークに接続されているアクセスポイントは、承認または不正の可能性があるものとして事前に分類されています。これらのアクセスポイントは、[モニター]>[WIPS]タブに適切な分類で表示されます。次に、それらの未確定なデバイスを不正または認定として適切に再分類し、不正アクセスポイントの場合は遮断を実施できます。また、以下のように信号強度ベースの事前分類を有効にすると、強度のしきい値に従ってアクセスポイントを事前分類することもできます。信号強度がしきい値よりも大きいアクセスポイントは、認定、または、不正として自動的に分類されます。



ただし、隣接施設からの正当なアクセスポイントがしきい値より高い信号強度で表示される場合に、そのアクセスポイントを不正として分類すると、アクセスポイントへの正当なWi-Fi接続が中断される可能性がありため、本設定のみに依存することは推奨しません。
したがって、この分類は、許可されていないWi-Fiがユーザーの近くで動作していないことが確実な場合にのみ使用してください。また、信号強度に基づく分類では、しきい値よりも弱い信号強度で動作する不正なアクセスポイントは検出されません（例. Wi-Fiホットスポットを実行しているスマートフォン）。

Wi-Fiネットワークを定義しない

セキュリティの影響を受けやすい環境では、特定のロケーションにおいてWi-Fiネットワークが動作しない設定が必要な場合があります。
以下のように、ロケーションに接続を許可しないWi-Fiネットワークを定義できます。このようなネットワークを定義すると、そのロケーションのネットワーク上で検出されたアクセスポイントは、承認されたポリシーに準拠していても、不正アクセスポイントとして自動的に分類されます。



2.13.5 デバイスインポート

WIPS機能による不正端末の防御は自動で行われますが、複数のメーカーのアクセスポイントが同ネットワークに存在する場合など、手動でデバイスのタイプを設定する必要がある場合があります。
モニター>WIPSから任意にデバイスのタイプを変更することができますが、デバイスインポート機能を利用することにより、デバイス数が多い場合にも効率的に設定することが可能です。
デバイスインポート機能は、以下のタイプのリストをCSVファイルからインポートできます。
●認定アクセスポイント
●ローグ（不正）アクセスポイント
●認定クライアント
●ローグ（不正）クライアント
●ゲストクライアント

次の手順でデバイスのインポートを行います。
1. **[システム]>[詳細設定]>[デバイスインポート]**を選択します。
2. CSVテンプレートから、[ダウンロード]をクリックすると、インポートを行うためのフォーマットがダウンロードされます。

3. 以下のフォーマットに、必要なアクセスポイントまたはクライアント情報を入力します。

	A	B	C	D	E	F	G	H	I	J
1	このファイルにはサンプル・データが格納されています。サンプル・データを削除して、デバイス情報を追加してください。									
2	デバイスは、選択したサーバーの指定した場所にインポートされます。									
3	ノート：									
4	*各行には一意の MAC アドレスが 1 つだけ含まれている必要があります。コンマ区切り値はサポートされていません。									
5	*ロケーション ID を指定しない場合、デバイスはステージング エリアにインポートされます。									
6	*特定の場所にデバイスをインポートしたくない場合は、対応する行をテンプレートから削除します。									
7	*インポート操作では、ロケーション名ではなくロケーション ID が使用されます。									
8	*区切り記号の有無にかかわらず空白行は無視されます。									
9										
10	MAC Address	IP Address	Device Na	Location Id	Location Name					
11	aa:bb:cc:dd:ee:f1	192.168.8.180	Device 1	-1	//AIRRECT Cloud/Staging Area					
12	aa:bb:cc:dd:ee:f1	192.168.8.180	Device 1	0	//AIRRECT Cloud					
13	aa:bb:cc:dd:ee:f1	192.168.8.180	Device 1	7	//AIRRECT Cloud/2階					
14	aa:bb:cc:dd:ee:f1	192.168.8.180	Device 1	8	//AIRRECT Cloud/3階					

4. [**タイプを選択**]から一括でインポートしたいタイプを選択します。
5. [**ファイルを選択**]から、作成したインポートファイルを選択し、[インポート]を押下します。

2.13.6 WLAN統合

AIRRECT Cloudサーバーを他社のオンプレミスのWLANコントローラーと統合すると、コントローラーベースのWLANを引き続き使用しながら、クラウドサーバーの主要な機能を活用できます。AIRRECT Cloudサーバーは、SNMPを使用してWLANコントローラーからアクセスポイント、クライアント、および信号強度に関する情報を取得します。
WIPS機能は、この情報を使用してコントローラーが管理する承認済みデバイスを自動的に分類し、Wi-Fiクライアントのロケーションを追跡できます。AIRRECT Cloudは、「Arubaモビリティ・コントローラ」および「Cisco WLC」との統合をサポートします。
また、統合のためには、CIPモードで動作するAIRRECT APが必要です。
CIPモードへの変更方法は、「2.19.1 CIP(Cloud Integration Point)モード」を参照してください。

WLAN統合の設定

WLANコントローラーを追加するには、[**システム**]>[WIPS]>[**WLAN統合**]に移動します。
[Aruba Networks]、または、[Cisco WLC]のどちらを追加するかを選択し、「Arubaモビリティ・コントローラ」、または、「無線LANコントローラ」の[**追加**]をクリックすると、[**コントローラを追加する**]パネルがウィンドウ右に表示されます。

設定を入力し、[**終了**]をクリックします。コントローラーがプライベートIPアドレスを使用している場合、コントローラーをクラウドと統合するには、クラウド統合ポイントが必要になることに注意してください。また、WLAN統合タブで、自動同期間隔を設定します。これは、AIRRECT Cloudがコントローラから情報を呼び出す頻度を定義する間隔です。
設定を保存してコントローラーの追加を完了します。

メインの[WLAN統合]タブで、[自動同期間隔]を設定します。
これは、AIRRECT Cloudがコントローラーから情報をフェッチする頻度を定義する間隔です。
設定を保存して、コントローラーの追加を完了します。

コントローラー設定

パラメータ	概要
コントローラ (IPアドレス/ ホスト名)	コントローラーのホストネームかIPアドレスを入力します。 コントローラーがプライベートIPアドレスを使用する場合、 クラウド統合ポイント(CIP)を選択する必要があります。
ポート番号	データをインポートするコントローラーのポート番号
プライマリ クラウド統合 ポイント（CIP）	ドロップダウンリストから、プライマリクラウド統合ポイント(CIP)として使用するAIRRECT APを選択します。 クラウド統合ポイント(CIP)からAIRRECT Cloudに接続するには、ネットワークでポート番号3852を開く必要があります。
セカンダリ クラウド統合 ポイント (CIP)	ドロップダウンリストから、セカンダリクラウド統合ポイント(CIP)として使用するAIRRECT APを選択します。プライマリCIPに障害が発生した場合、セカンダリCIPを使用することでサービスとクラウドの接続が確保されます。
SNMPバージョン	通信には、SNMP v2またはv3を選択します。
コミュニティ 文字列	AIRRECT Cloudがコントローラーと通信するために使用するユーザー定義のコミュニティ文字列。初期値は「public」です。
インポート	コントローラーからのデータのインポートを有効にする場合に選択します。
管理対象 アクセスポイント	コントローラーから管理型アクセスポイントの情報をインポートする場合に選択します。
管理対象 クライアント	コントローラーが管理するアクセスポイントにアソシエーションされたクライアントに関する情報をインポートする場合選択します。
管理対象 クライアントの アソシエーション	コントローラーが管理するアクセスポイントにアソシエーションされたクライアント、に関するアソシエーションの情報をインポートする場合に選択します。
管理対象外 アクセスポイント	コントローラーによって管理されていないアクセスポイントに関する情報、をインポートする場合に選択します。
管理対象外 クライアント	コントローラーによって管理されていないアクセスポイントにアソシエーションされているクライアント、に関する情報をインポートする場合に選択します。
管理対象外 クライアントの アソシエーション	コントローラーによって管理されていないアクセスポイントにアソシエーションされているクライアントに関する情報をインポートする場合に選択します。
信号強度	コントローラーからの信号強度情報をインポートする場合に選択します。

2.14 チェックポイントによる設定の保存・復旧機能

チェックポイントを作成することにより、現在の構成やグループ設定、プロファイル等を保存することができます。 保存したチェックポイントは、ロケーションごとに構成の復元や、以前の構成との比較が可能です。これにより、ネットワーク障害やパフォーマンスの低下が発生した場合は、以前に作成したチェックポイントを復元して、以前の動作状態に戻すことができます。チェックポイントは 、3 種類の設定があります。

1. ロケーションチェックポイント：選択したロケーションの SSID の設定、ネットワークポリシー、デバイス設定、WIPS 設定などを保存します。
2. グループチェックポイント：現在のグループ設定をチェックポイントとして保存します。
3. グローバルチェックポイント：システムで作成される WIPS、サードパーティ等の項目全ての設定を保存します。
   グローバルチェックポイントは、比較用だけであり復元はできません。

注意：以下の制限事項があります。
1. キャプティブポータル(ゲスト WiFi 設定)は保存できません。
2. クラウドサーバーのアップデートに伴って、過去のバージョンで保存した設定は復元できません。
3. ルートロケーション(フォルダ名:AIRRECT Cloud)の設定は復元できません。

チェックポイントを作成する機能は、以下の UI 画面で利用できます。

- [設定] > [WiFi]
- [設定] > [デバイス]
- [設定] > [ネットワーク プロファイル]
- [設定] > [WIPS]
- [設定] > [アラート]
- システム > ナビゲータ
- システム > サードパーティサーバー
- システム > WIPS
- システム > ログ
- システム > ユーザーアカウント

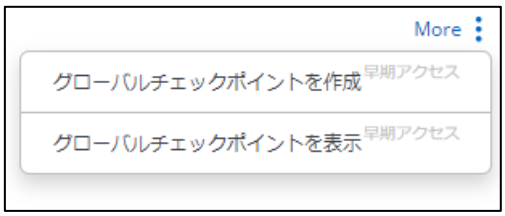
ロケーションまたはグループのチェックポイント作成

ロケーションまたはグループのチェックポイントの作成は、次の手順で行います。

1. ナビゲータからチェックポイントを作成したいロケーションまたはグループを選択します。
2. [**設定**]>[WiFi] または任意の 設定画面に移動します。
3. 右上のメニュー画面から[**チェックポイントの作成**]をクリックします。

4. チェックポイントの名前と説明を入力し、[**作成**]をクリックします。

グローバルチェックポイントの作成



グローバル チェックポイントを作成するオプションは、[システム] メニューの下にあるすべての画面で利用できます。
グローバル チェックポイントを作成するには、その他の 3 点メニューから [グローバル チェックポイントの作成] をクリックします。
ロケーション ツリーでルートの場所を選択することにより、任意の [設定] 画面からグローバル チェックポイントを作成することもできます。

チェックポイントを表示

ロケーションまたはグループで利用可能なすべてのチェックポイントを表示できます。
グローバルチェックポイントは、**[システム]**メニューのどの画面からでも見ることができます。

作成したチェックポイントに対して、以下の操作を行うことができます：
●編集
●復元
●削除
●ダウンロード
●現在または、特定の 2 つの設定の比較

チェックポイントの比較

比較したいチェックポイントを選択、右クリックすると、現在の設定と比較することができます。また、チェックポイントを二つ選択することで、選択したチェックポイントの比較をすることが出来ます。

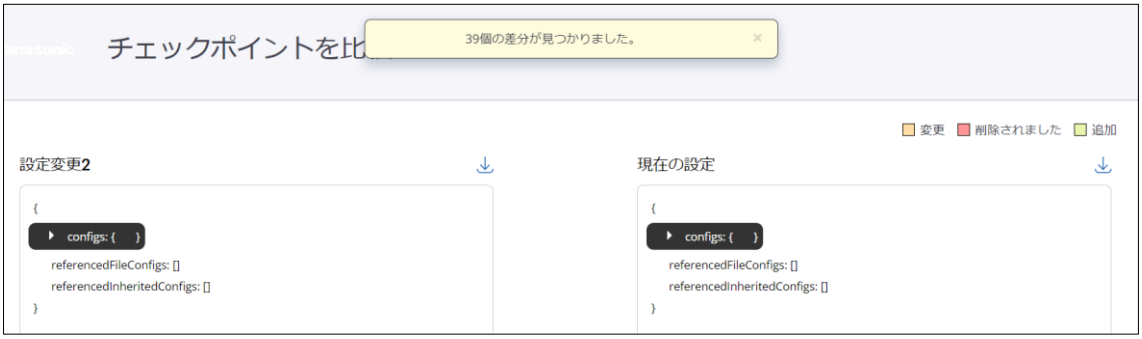
チェックポイントはツリー表示され、変更点に関しては背景で色分けされます。

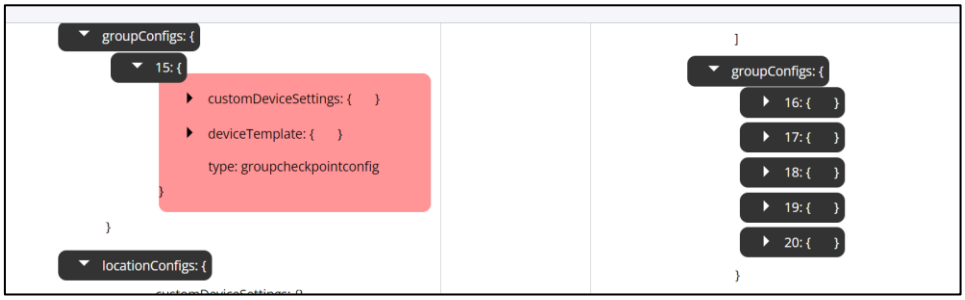
設定を変更した項目：黒背景

設定の変更：橙背景

設定の削除：赤背景

設定の追加：黄背景





設定は、アイコンからもダウンロード可能です。

ダウンロードした設定は、閲覧可能な JSON ファイルに変換され表示されます。

2.15 トラブルシューティング

ネットワーク管理者がWi-Fiネットワークの問題におけるトラブルシューティングを行うツールとして、パケットトレースやクライアントとの接続性試験などができます。

2.15.1 クライアントのパケットトレースのキャプチャ

パケットトレースを実行することで、クライアントのデータパケットをキャプチャすることができます。パケットキャプチャには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**クライアント**]の順に移動します。
2. クライアント名を右クリックするか、メニューアイコンを選択すると、利用可能なアクションが表示されます。[**パケットトレースをキャプチャ**]をクリックすると、キャプチャダイアログボックスが開きます。
3. 以下詳細を入力し、[**パケットキャプチャの開始**]をクリックします。

オプション	概要
モード	ワイヤレスキャプチャモードを選択します。 ●多機能ラジオ：多機能アンテナを介し、[**周波数帯とチャンネルの選択**]にて選択したチャネルをキャプチャします。 ●インライン無線アクセス：現在接続中クライアントのパケットをキャプチャします。 ●無線無差別アクセス：Wi-Fiアンテナが使用するチャネルをキャプチャします。
パケット トレース期間	パケットトレースキャプチャを実行する期間を設定します。 設定範囲は1～720分です。
ストリーミング オプション	使用するパケットキャプチャのタイプを指定します。 ・サーバーにアップロード: パケットキャプチャプロセスのすべてが完了した後に限り表示できる、キャプチャファイルを作成します。 ・ローカルマシンのWireshark：進行中のキャプチャプロセス中にパケットトレースを開くことができます。
ファイル名の プレフィックス	ファイル名のプレフィックスを指定します。プレフィックスを「Packet_wireless_143438.pcap」の場合、「Packet」がファイル名のプレフィックス、「wireless_143438」がファイル名、「pcap」がファイル拡張子となります。
クライアントの ローミングを追跡	選択したロケーション内のアクセスポイント間でクライアントがローミングした場合、追跡してパケットキャプチャを取得することが出来ます。

無線設定	このオプションを選択して、無線の詳細設定を編集します。
トラフィックを選択	キャプチャされるトラフィックのタイプを表します。 ●選択されたクライアントのパケットのみ<MAC address>：選択したクライアントからのパケットのみを表示します。 ●チャネル上のすべてのパケット：アクセスポイントセンサーから見えるすべてのクライアントからのすべてのパケットをキャプチャします。
パケットタイプ	キャプチャするパケットのタイプを選択します。
周波数帯とチャンネルの選択	トラブルシューティングする周波数とチャネルを選択します。単一のチャネルを選択する場合は、[**チャネルの選択**]オプションをクリックし、[**チャネル番号**]と[**幅**]（チャネルオフセット）を指定します。初期値では、周波数とチャネルは、トラブルシューティングセンサーに適用されたデバイステンプレートに基づいて表示されます。[**すべてのチャネルで回転**]オプションを選択することで、使用可能なすべてのチャネルのトラブルシューティングを行うこともできます。

4. キャプチャパケットトレースの進行状況を示すダイアログが表示されます。パケットキャプチャを強制的に停止するには、[**停止**]をクリックします。
5. パケットトレースが正常に完了したら、[**ダウンロード**]をクリックしてWiresharkでファイルを表示します。

クライアントのパケットトレース履歴の表示

選択したクライアントのパケットトレース履歴を表示できます。過去30分間にキャプチャされたパケットトレースのみが履歴に表示されます。

パケットトレース履歴を表示するには、以下の手順を実行します。

1. クライアントを右クリックするか、メニューアイコンを選択して、[**パケットトレースの履歴**]をクリックします。
2. [**パケットトレースをキャプチャ**]ウィンドウの [**履歴**]タブを選択して、パケットキャプチャの履歴を表示します。
3. パケットトレースを選択すると、詳細情報を表示します。
4. パケットキャプチャファイルのメニューアイコンをクリックすると、
   利用可能なアクションが表示されます。

5. 以下のいずれかのアクションを選択します。

●ダウンロード - トレースファイルをダウンロードします。

●削除 - トレースファイルを削除します。

●開く - トレースファイルを開きます。

2.15.2 アクセスポイントのパケットトレースのキャプチャ

パケットトレースを実行することで、アクセスポイントのデータパケットをキャプチャすることができます。パケットキャプチャには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順に移動すると、認識されているアクセスポイントのリストが表示されます。
2. パケットトレースをキャプチャするアクセスポイントの名前を右クリックするか、メニューアイコンを選択し、[**トラブルシュート**]>[**パケットトレースをキャプチャ**]をクリックします。[**パケットトレースをキャプチャ**]ダイアログボックスが開きます。
3. [**パケットトレースをキャプチャ**]タブで各オプションを入力し、[**パケットキャプチャの開始**]をクリックするとキャプチャパケットトレースの進行状況を示すダイアログが表示されます。
   パケットキャプチャを強制的に停止するには、[**停止**]をクリックします。

オプション	概要
モード	ワイヤレスキャプチャモードを選択します。 ●多機能ラジオ：多機能アンテナを介し、[**周波数帯とチャンネルの選択**]にて選択したチャネルを全てキャプチャします。 ●インライン無線アクセス：Wi-Fiアンテナへ接続しているクライアントのパケットのみをキャプチャします。 ●無線無差別アクセス：Wi-Fiアンテナが使用するチャネルのパケットを全てキャプチャします。
パケット トレース期間	パケットトレースキャプチャを実行する期間を設定します。 設定範囲は1～720分です。
ストリーミング オプション	使用するパケットキャプチャのタイプを指定します。 ●サーバーにアップロード： キャプチャするファイルを作成します。パケットトレースは、パケットキャプチャプロセス全体が完了した後にのみ表示できます。 ●ローカルマシン上のWireshark： パケットトレースは、進行中のキャプチャプロセス中に開かれます。
ファイル名の プレフィックス	ファイル名のプレフィックスを指定します。プレフィックスを「Packet_wireless_143438.pcap」の場合、「Packet」がファイル名のプレフィックス、「wireless_143438」がファイル名、「pcap」がファイル拡張子となります。
無線設定	このオプションを選択して、無線の詳細設定を編集します。

トラフィックを選択	トラブルシューティングでキャプチャされるトラフィックのタイプです。 ●このアクセスポイント上のすべてのBSSIDのパケット： 該当の無線アクセスポイントが通信しているパケットをキャプチャします。 ●単一BSSIDのパケット<MACアドレス>：選択したBSSIDのパケットのみを表示します。 ●チャネル上のすべてのパケット: 他の無線アクセスポイントと通信しているパケットも含めて、同一チャネル上のパケットをキャプチャします。
パケットタイプ	キャプチャするパケットのタイプを選択します。
周波数帯とチャネルの選択	トラブルシューティングする周波数とチャネルを選択します。単一のチャネルを選択する場合は、[**チャネルの選択**]オプションをクリックし、[チャネル番号]と[**幅**]（チャネルオフセット）を指定します。 初期値では、周波数とチャネルは、トラブルシューティングセンサーに適用されたデバイステンプレートに基づいて表示されます。 [**すべてのチャネルで回転**]オプションを選択することで、使用可能なすべてのチャネルのトラブルシューティングを行うこともできます。
有線設定	有線デバイスからパケットをキャプチャするには、このオプションを選択します。
インターフェイス	リストから利用可能なイーサネットポートを選択します。初期値はeth0です。
VLAN ID	VLAN IDを入力します。
ICMP, UDP, DHCP, MDNS, LLMNR, DNS, RADIUS, ARP, TCP	リストから必要なプロトコルを選択します。

4. パケットトレースが正常に完了したら[**ダウンロード**]をクリックして、Wiresharkでファイルを表示します。

アクセスポイントのパケットトレース履歴の表示

選択したアクセスポイントのパケットトレース履歴を表示できます。 過去30分間にキャプチャされたパケットトレースが履歴に表示されます。

パケットトレース履歴を表示するには、以下の手順を実行します。

1. アクセスポイントを右クリックするか、メニューアイコンを選択して、利用可能なアクションを表示します。
2. [**トラブルシュート**]>[**パケットトレースの履歴**]を選択します。
3. [**パケットトレースのキャプチャ**]ウィンドウの [**履歴**]タブを選択して、パケット キャプチャの履歴を表示します。
4. パケットトレースを選択して、以下の詳細情報を表示します。
5. パケットキャプチャファイルのメニューアイコンをクリックすると、利用可能なアクションが表示されます。

6. 以下のいずれかのアクションを選択します。

●ダウンロード - トレースファイルをダウンロードします。

●削除 - トレースファイルを削除します。

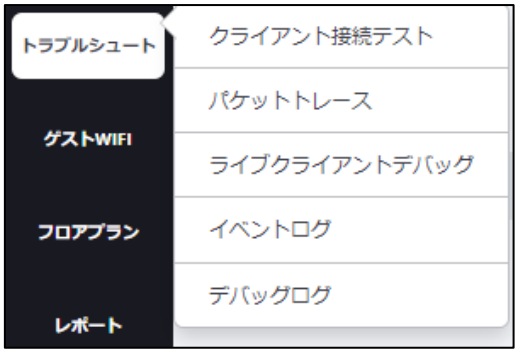
●開く - トレースファイルを開きます。

2.15.3 自動パケットトレース

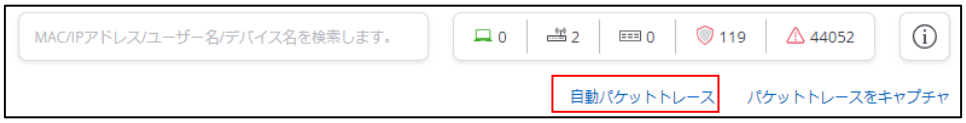
AIRRECでは、APが接続障害を検出すると、パケットトレースを自動的にキャプチャすることができます。キャプチャされたパケットトレースは、クライアント接続ログからアクセスおよびダウンロードできます。

この機能は、短時間で発生する（パスワード誤設定やDHCP/DNS問題など）クライアント接続の問題のトラブルシューティングに役立ちます。当機能を使用するには管理者以上の権限が必要です。自動パケットトレースを実行するには、以下の手順を実行します。

1. [**トラブルシュート**]>[**パケットトレース**]の順に移動します



2. [**自動パケットトレース**]をクリックします



3. 画面右側に表示される[**自動パケットトレース**]パネルで1つ以上のSSIDを選択します。

4. [**保存**]をクリックします。

●自動的にキャプチャされたパケットトレースファイルのリストを表示するには、
特定のクライアントのクライアント接続ログを参照してください。
過去30分間にキャプチャされたパケットトレースのみが使用可能です。
●クライアントごとに、最大5つのパケットトレースがシステムに保持されます。
●トレースファイル名はシステム定義であり、クライアントのMACアドレス、AP BSSID、
およびパケットキャプチャセッションのタイムスタンプに基づきます。

2.15.4 クライアント接続テスト

アクセスポイントの多機能アンテナを通信テスト用の仮想クライアントとして動作させることができます。これにより、ネットワーク保証、ネットワークサービスの到達可能性、VoIPなどの重要なアプリケーションのエクスペリエンス品質を事前に検証できます。
テスト対象のアクセスポイントはターゲットアクセスポイントと呼ばれ、クライアントとして動作するアクセスポイントの多機能アンテナは、ターゲットアクセスポイントに接続、テストを実行してネットワークの状態を評価し、問題がある場合は特定します。また、スケジュール設定によりテストを自動することもできます（詳細は「スケジュール」をご参照してください）。

テストプロファイル
テストプロファイルは、以下の要素で構成されます。
●テストSSID
●テスト周波数帯
●実行するテスト
例えば、企業SSIDの場合には、Microsoft TeamsやOfficeなど、ゲストSSIDの場合には、SNSなどを含むテストプロファイルを定義して、通信品質をテストします。
1回のテスト実行で、テストプロファイルに含まれるすべてのテストが実行されます。
※EAP-TLS認証を使用するSSIDのプロファイルを作成する場合、以下の入力が必要です。
CA証明書：RADIUSサーバー証明書の署名検証を行うCA証明書。
証明書タグ：AIRRECTから生成したCSRを基に発行/署名したTLS証明書。

テストプロファイルの重要な点は、以下の通りです。
●クライアント接続テストを実行する前にテストプロファイルを作成する必要があります。
●アクセスポイントがテストするSSIDをブロードキャストしている必要があります。

スケジュール

テストスケジュールを構成することで、クライアント接続テストを自動実施させることができます。定期的なテストの実施は、ネットワークの可用性やパフォーマンスを最適化し、事後対応型のネットワークトラブルシューティングを避けることができます。
スケジュールは、単一のテスト、または数日/数週間ごとの複数回テストが可能です。あるロケーションでクライアント接続テストのスケジュールを設定すると、そのスケジュールは自動的にすべての子ロケーションに適用されます。

スケジュールされたテスト用のアクセスポイントの選択

スケジュールテストでは、フォルダごとに2つのアクセスポイントが自動で選出されテストが開始されます。アクセスポイントの選出は、以下の考慮事項に基づいています。

ターゲットアクセスポイント	クライアントアクセスポイント
同じアクセスポイントで繰り返しテストされることを回避するため、ランダムに選出。	-70dBm以上の良好なRSSIで認識できるアクセスポイントである。
アクセスポイントがテストプロファイルに合致するSSIDを出力している。	多機能アンテナが、他のアクティビティ（侵入防止、トラブルシューティング、別のテストなど）を実行していない。
ターゲットアクセスポイントが別のテストを実行してない。	最も高いRSSIを持つアクセスポイントが選出される。

上記の基準を満たすターゲットアクセスポイントとクライアントアクセスポイントが見つかった場合、スケジュールに従ってテスト実行が開始されます。それ以外の場合、テストは実行されず、実行できなかった理由が[**結果**]に記録されます。
結果：[**結果**]ページの[**結果ステータス**]列には、各テスト実行に対して緑、赤、橙、または灰色のドットが表示されます。テスト実行は複数のテストで構成されることに注意してください。各色は以下を示します。
●灰色：クライアント接続テストを完了
●緑：すべてのクライアント接続テストが成功
●赤：1つ以上のクライアント接続テストが完全に失敗
●橙：クライアント接続テストが部分的な成功または失敗
「部分的な成功」とは、例えば、アプリケーションテストの一部のアプリケーションは失敗したが、他のアプリケーションは成功した場合などです（詳細については、以下の「アプリケーションテスト結果」セクションを参照して下さい）。

アプリケーションテスト結果

アプリケーションテストは、アプリケーションのタイプ（例. 生産性、ソーシャル）ごとにグループ化されています。以図は、アプリケーションテストの結果を示しています。

アプリケーションテストは、テスト対象のアプリケーションにHTTP GET要求を送信します。HTTP GETが失敗した場合、Pingテストが実行されアプリケーションサーバーへの接続が確認されます。

HTTP GETが成功した場合、結果は以下のパラメータを取得します。

- ページ・サイズ
- 応答コード　(コード100-399は成功を表します)
- ページ読み込み時間：ページ読み込み時間にカーソルを合わせると、
  DNS検索時間、初回接続時間、SSL接続時間の詳細が確認できます。

●アプリケーションテスト結果のロジックは、以下の通りです。
緑：すべてのアプリケーションテストが成功
赤：すべてのアプリケーションテストが失敗
橙：アプリケーションテストの一部が成功、一部が失敗
アプリケーションの1つでも失敗すると、アプリケーションテストの結果は橙色になります。

テスト結果

以下は、各テスト結果のフィールドの説明です。クライアント接続テスト結果の保存可能数は50個、保存期間は30日となります。

パラメータ	概要
接続テスト中のアクセスポイント/クライアントとして機能しているアクセスポイント	●テスト開始時間とテスト完了時間 ●テストを実行したアクセスポイント情報とプロファイル情報
アソシエーション	成功（緑）、失敗（赤）
認証	●成功（緑）、失敗（赤） ●セキュリティ方法：使用されるセキュリティ方法 セキュリティモードが802.1xの場合、遅延時間が表示されます。
DHCP	●DHCPステータス：成功（緑）、失敗（赤） ●IPアドレス：成功した場合にDHCPサーバーが使用するIPアドレス ●遅延：成功した場合のDHCP遅延（ミリ秒単位） ●DNSサーバーオプション ●DHCPゲートウェイ
ゲートウェイ	●到達可能：成功（緑）、失敗（赤） ●成功した場合の遅延時間
DNS	●DNSステータス： 成功（緑）、失敗（赤）、部分的に成功（橙） ●IPアドレスと成功した場合の遅延時間
WAN遅延時間	●WAN到達可能性：成功（緑）、失敗（赤） ●WAN URL：接続テストの際に使用されるURL ※初期値URL：www.google.comは編集できません。 ●到達可能な場合の遅延時間
Ping テスト	●Pingテスト：成功（緑）、失敗（赤） ●ホスト：ホストURL ●成功した場合の遅延時間

アプリケーションテスト	●HTTP GET：成功（緑）、失敗（赤） 成功すると、以下のものがキャプチャされます。 ●ページ・サイズ ●HTTP応答コード（コード100～399は成功を表す。） ●ページ読み込み時間： ページの読み込み時間にカーソルを合わせると、 DNS検索時間、初回接続時間、SSL接続時間の内訳を確認できます。
VoIPテスト	●VoIP通話ステータス：成功（緑）、失敗（赤） ●0～5の平均オピニオンスコアを5つ星で表示 スコア上にマウスを置くと以下の値を表示できます。 - 平均遅延時間 - ジッタ - パケット損失 - パケットレート - 平均ビットレート
スループットテスト	●インターネット/Wi-Fiスループットテストの ステータス：成功（緑）、失敗（赤） ●インターネットスループットテスト:アップロードと ダウンロードに関する速度 ●Wi-Fiスループットテスト:TCP/UDPアップロード およびダウンロード速度

2.15.5 ライブクライアントデバッグ

ライブクライアントデバッグ機能を使用すると、クライアントアクティビティのログをライブで表示し、トラブルシューティングを行うことができます。この機能はオペレーター以上の権限を持つユーザーが使用できます。閲覧者権限では、ライブクライアントのデバッグを実行したり、ログにアクセスしたりすることはできません。ライブクライアントデバッグ機能を使用すると、以下のタスクを実行することができます。

●ライブクライアントデバッグの開始
●ライブクライアントデバッグの停止
●ライブクライアントデバッグの表示
●ライブクライアントデバッグログの削除
●ライブクライアントデバッグログのダウンロード
●ライブクライアントデバッグログのアーカイブ

ライブクライアントデバッグの開始

1つのクライアントを指定してライブクライアントデバッグを開始できます。連続して行うことで、最大10クライアントを並行してデバッグできます。
ライブクライアントデバッグを開始するには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**クライアント**]の順に移動します。
2. デバッグしたいクライアントを右クリックして、[**ライブクライアントデバッグを開始**]を選択します。
3. 表示された[**ライブクライアントデバッグ**]ページの[**期間を選択**]から、ライブクライアントデバッグを実行する必要がある期間を選択します。
4. [**場所を変更**]をクリックします。（オプション）
   デフォルト以外の場所でクライアントのログを追跡する場合にのみ使用してください。これは、クライアントが複数の場所にローミングしているときに利用されます。
5. 停止/タイムアウト後のクライアントログを破棄、または、保存を選択します。
   [**ログを破棄**]をクリックすると、ライブクライアントデバッグが停止してから30分後にログは破棄されます。[**ログをアーカイブ**]をクリックすると、タイムアウト期間が経過した後、またはライブクライアントデバッグセッションを停止したときに、ログがサーバーに保存されます。
6. [**開始**]をクリックすると、ライブクライアントデバッグページにリダイレクトされ、クライアントログがライブで表示されます。
   ※[**クライアント**]ページで、太字および斜体になっているクライアント名は、ライブクライアントデバッグ中です。ログにはテキストファイルとしてアクセスできます。

ログには以下の情報が含まれています。

●クライアントのMACアドレス

●SSID

●BSSID

●アクセスポイント名

●チャネル

●ログが開始されたときのタイムスタンプ

●2つの連続するイベント間のミリ秒単位の時差

●イベント

```
Client MAC: 5C:51:88:31:05:67
SSID    : WebAppsDevC120
BSSID   : 00:11:74:F2:17:B0
AP NAME :मोजो F2:17:BF
Chan    : 11
Time    : 2017.04.03 11:40:21 (Asia/Kolkata)
Tdiff(msec)             Timestamp
Event        0          2017.04.03 11:40:21            Deauthentication received from client because sending STA is leaving
             2          2017.04.03 11:40:21            Node LeftSSID   : WebAppsDevC120BSSID   : 00:11:74:F2:17:B0AP NAME
             12         2017.04.03 11:40:23            Client successfully (re)associated
             13         2017.04.03 11:40:23            First phase of WPA/WPA2 4-Way Handshake Completed
             66         2017.04.03 11:40:23            Second phase of WPA/WPA2 4-Way Handshake Completed
             67         2017.04.03 11:40:23            Third phase of WPA/WPA2 4-Way Handshake Completed
             95         2017.04.03 11:40:23            Node Authorized
             96         2017.04.03 11:40:23            Fourth phase of WPA/WPA2 4-Way Handshake Completed
            203         2017.04.03 11:40:23            Client sent DHCP DISCOVER
            271         2017.04.03 11:40:23            DHCP OFFER sent to Client from [172.16.100.254]
            272         2017.04.03 11:40:23            Client has received IP [172.16.100.1]
            295         2017.04.03 11:40:23            Client sent DHCP REQUEST
            370         2017.04.03 11:40:23            DHCP ACK sent to Client from [172.16.100.254]
```

●[**トラブルシュート**]>[**ライブクライアントデバッグ**]からライブクライアントデバッグを開始することもできます。必要なクライアントを検索し、ページの右上隅にある[**ライブクライアントデバッグを開始**]をクリックします。

●アーカイブされたクライアントログにアクセスするには、[**トラブルシュート**]>[**ライブクライアントデバッグ**] に移動します。太字の斜体で表示されているログのファイル名は、デバッグが進行中であることを示しています。

ライブクライアントデバッグの停止

デバッグの進行中は、ライブクライアントデバッグを停止できます。デバッグセッションを停止するには、以下のタスクを実行します。

1. [**トラブルシュート**]>[**ライブクライアントデバッグ**]に移動します。
   進行中のログは、太字の斜体で表示されています。
2. 目的のログを右クリックし、[**ライブクライアントデバッグを停止**]を選択します。
   [**モニター**]>[Wi-Fi]>[**クライアント**]の順に移動すると、デバッグを停止することができます。[**クライアント**]ページで、ライブクライアントデバッグを行うクライアントは、太字の斜体で示されています。必要なクライアント（太字の斜体）を右クリックし、[**ライブクライアントデバッグを停止**]を選択します。

ライブクライアントデバッグの表示

ライブクライアントデバッグは、クライアントの進行中のイベントのうち、終了していないものについてのみ表示できます。

ライブクライアントのデバッグを表示するには、以下の手順を実行します。

1. [**トラブルシュート**]>[**ライブクライアントデバッグ**]の順に移動します。
   ログのリストが表示されます。 進行中のログは太字および斜体で表示されます。
2. 進行中のログファイルを右クリックし、[**ライブクライアントデバッグの表示**]をクリックすると、[**ライブクライアントデバッグ**]ページにリダイレクトされます。
   ライブクライアントデバッグを表示するには、[**モニター**]>[Wi-Fi]>[**クライアント**]の順に移動することもできます。太字および斜体のクライアントは、ライブクライアントデバッグが進行中のクライアントです。ライブクライアントデバッグログを表示するクライアントを右クリックし、[**ライブクライアントデバッグ**]を選択します。ログファイルを開いた後のイベントは、ライブクライアントデバッグセッションで確認できます。また、バックグラウンドで実行中に発生したイベントは記録され、ダウンロードできます。ログファイルのダウンロードの詳細については、『ライブクライアントデバッグログのダウンロード』を参照してください。

ライブクライアントデバッグログの削除

完了したセッションのライブクライアントデバッグログファイルを削除できます。進行中のログファイルは削除できません。

ログを削除するには、次のタスクを実行します。

1. [**トラブルシュート**]>[**ライブクライアントデバッグ**]の順に移動します。
2. 削除するログを右クリックして、[**ライブクライアントデバッグを削除**]を選択します。

ライブクライアントデバッグログのダウンロード

ライブクライアントデバッグセッションのログをダウンロードできます。
ログをダウンロードするには、以下の手順を実行します。

1. [**トラブルシュート**]>[**ライブクライアントデバッグ**]の順に移動します。
2. ログ名をクリックすると、ファイルをZIP形式でダウンロードします。または、ダウンロードするログを右クリックし、[**ライブクライアントデバッグログをダウンロード**]をクリックします。複数のログをダウンロードする場合は、ログのチェックボックスを選択し、右クリックし、[**ライブクライアントデバッグログをダウンロード**]をクリックします。アーカイブできる上限は、登録しているアクセスポイントの台数が250台までの場合は最大アクセスポイントの台数x2のログファイル、登録しているアクセスポイントの台数が250台以上の場合は最大500のログファイルです。または、ログファイルのサイズが2MBに達すると、ライブクライアントデバッグは1分後に停止しますので、定期的なダウンロードの実施を推奨します。

2.15.6 LEDの点滅

トラブルシューティングの目的で、多数のAPがある大規模なフロアに配置されているアクセスポイントを見つけやすくするために、APのLEDを点滅させることができます。
アクセスポイントのLEDを点滅させるには、次の手順を実行します。

1.[**モニター**]>[WiFi]>[**アクセスポイント**]
（または[**モニター**]>[WIPS]>[**アクセスポイント**]）に移動します
2.検索するAPのオプションタブ⁞をクリックします。
3.[**LEDの点滅を開始**]と、アクセスポイントのLEDが点滅し続ける時間（最大24時間）を選択します。
4.[**LEDの点滅を開始**]をクリックすると、アクセスポイントのPOWER LED、無線LED、LAN LEDが順番に点滅し、フロアにあるアクセスポイントを簡単に見つけることができます。
上記の手順に従って、上記の手順3で[**LEDの点滅を停止**]を選択して、LEDの点滅を開始したアクセスポイントでLEDの点滅を停止することもできます。

フロアプランからLEDの点滅開始（または停止）することもできます。
フロアプランからアクセスポイントのLEDを点滅させるには、次の手順を実行します。

1. 点滅させたいアクセスポイントが配置されているフロアプランに移動します。
2. 検索するAPを選択し、右クリックします。
3. [**LEDの点滅を開始**]を選択し、LEDを点滅させ続ける時間を選択します。

2.15.7 監査ログ

監査ログは、ログイン/ログアウト、ロケーション階層変更など、様々なユーザーアクションに関するログを指します。監査ログのダウンロードや監査ログの保存設定は、Superuser のみが行うことができます。

監査ログの種類

ログタイプ	説明
すべて	すべてのログタイプが含まれます
ユーザー・アクセス	パスワードの変更、RADIUS認証の変更など、ユーザーアクセスに関連するユーザーアクションをログに記録します
デバイス	アクセスポイント名の変更、再起動、ファームウェア更新など、アクセスポイントに関連するアクションを記録します
アラート	アラートの削除など、アラートに関連するアクションを記録します
グローバル設定	Google統合、Syslogサーバー、SNMP設定の変更などのグローバル設定に関連するアクションを記録します。
ロケーションベース設定	ファイアウォール、ロールベースのアクセス制御、SSID設定などのロケーションベースの設定に関連するアクションを記録します
ロケーション階層	フォルダまたはグループの追加または削除、フロアマップ関連の変更など、ロケーションの階層に関連するアクションを記録します
レポート	フォルダまたはグループの追加または削除、フロアマップ関連の変更など、ロケーションの階層に関連するアクションを記録します
機能の開始/停止	データベース、Webサーバーなどのシステムサービスに関連するアクションを記録します
システム	ネットワークの追加または削除、サービスモジュールの変更、タイムゾーン関連の変更など、システム関連の操作に関連するアクションを記録します。
サードパーティおよびその他	サードパーティのサーバーとカスタムファイルに関連する変更が含まれます

監査ログのダウンロード

1. [**システム**]>[**ログ**]をクリックして、[**監査ログ**]ページを開きます。
2. [**ログ・タイプ**]を選択し、ログをダウンロードする期間を指定します。
3. ダウンロードしたログを並べ替えるには、[**並べ替え**]の値を指定します。
4. [**ダウンロード**]をクリックして、ログをtsv形式でダウンロードします

監査ログの保持設定を構成する

監査ログには、7日から365日（両方を含む）のカスタム保存期間を定義できます。以前に設定した期間を復元して、システムのデフォルトのログ保持期間にリセットすることもできます。デフォルトの保存期間は7日です。

監査ログ保持ポリシーを設定するには、次のようにします。

1. [**システム**]>[**ログ**]をクリックして、[**監査ログ**]ページを開きます。
2. [**監査ログ保持ポリシー**]をクリックします。
3. 右側のパネルで、[**直近のユーザー・アクション・ログを保持します**]フィールドに日数を指定します。
4. 設定を保存します。

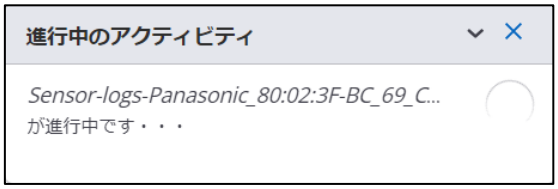
※監査ログ保持ポリシーの保持期間は、設定を変更すると期間外のログが削除されます。
設定を変更する際は、バックアップを取得してから変更する事を推奨します。

2.15.8 デバッグログ

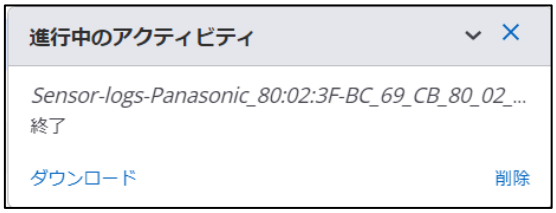
AIRRECT AP からデバッグログを取得することができます。デバッグログはトラブルシューティング時に使用するもので、ダウンロードして保存することができます。
デバッグログを作成/参照するには、以下の手順を実行します。

デバッグログの作成

1. [**モニター**]>[WiFi]>[**アクセスポイント**]の順に移動します。
2. アクセスポイントを選択し右クリックします。
3. [**トラブルシュート**]>[**デバッグログをダウンロード**]を選択します。
4. デバッグログの作成が開始されます。画面右下に[**進行中のアクティビティ**]ウィンドウが表示されます。



5. デバッグログの作成が終了すると、ステータスが[**終了**]に変わり、作成されたログの[**ダウンロード**]、または[**削除**]を選択できるようになります。



注意：[**進行中のアクティビティ**]ウィンドウで[**削除**]を選択すると、[**デバッグログ**]画面には表示されません。

デバッグログの参照

作成されたデバッグログを参照し、ダウンロード、または削除するには以下の手順を実行します。

1. [**トラブルシュート**]>[**デバッグログ**]の順に移動します。

2. 左端のメニューアイコン ⋮ をクリックし、[**ダウンロード**]または[**削除**]を選択します。

注意：デバッグログの参照できる時間は、キャプチャしてから30分のみ保存されます。

2.15.9 アクセスポイント Webシェル

Webシェルは、SSH経由でアクセスポイントにリモートでログインするためのオンラインインターフェースです。管理者(Administrator)、または、スーパーユーザーのみ、AIRRECT APのWebシェルを利用することができます。WebシェルのURLは、アクセスポイントごとに異なります。URLをブックマークすると、アクセスポイントに直接シェルセッションを開くことができます。

設定パラメータで定義された制限に応じて、1つのアクセスポイントに対して同時に複数のWebシェルセッションを開くことができます。Webシェルは非アクティブなアクセスポイントでは利用できません。

※アクセスポイントがデータの多い操作で過負荷になっている場合、進行中のWebシェルセッションに遅延が生じたり、新しいWebシェルが開かないことがあります。たとえば、Webシェルですでにタスクを実行している状態で、パケットキャプチャやデバッグログの生成、または、ライブクライアントのトラブルシューティングなどのデータ量の多い操作を開始した場合、Webシェルに遅延が発生することがあります。ライブクライアントのデバッグ（または同様のデータ量の多い操作）を実行しているときにWebシェルを開こうとすると、エラーが発生してWebシェルが開かないことがあります。

アクセスポイント Webシェルへのナビゲーション

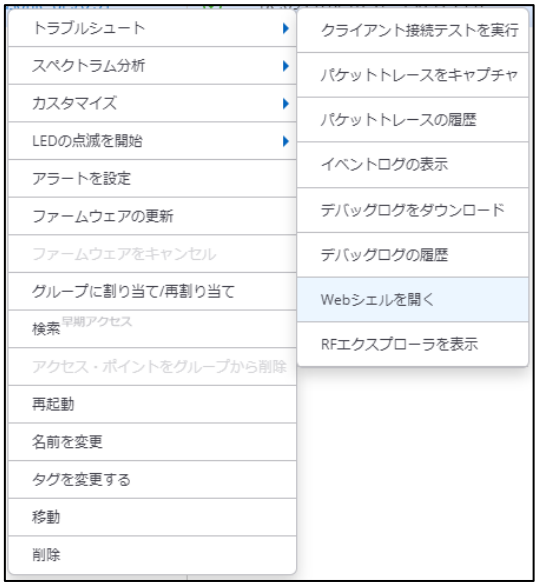
アクセスポイント Webシェルには、以下の場所からアクセスすることができます。

・[モニター]>[Wi-Fi]>[アクセスポイント]
・[モニター]>[WIPS]>[管理対象Wi-Fiデバイス]
・[フロアプラン]

アクセスポイント Webシェルを開く

アクセスポイント Webシェルを開くには以下の手順で行います。

1. [モニター]>[Wi-Fi]>[アクセスポイント]と進みます。
2. 該当のアクセスポイントを右クリックし、[トラブルシュート]>[Webシェルを開く]を選択します。Webシェルは新しいタブで開きます。



3. rootの認証情報を入力します。

これで、AP-CLIコマンドを入力できるようになります。
セッションを終了するには、ブラウザを閉じてください。
※AP-CLI コマンドの一覧は、「CLI リファレンス」を参照してください。

2.15.10 スペクトラム分析

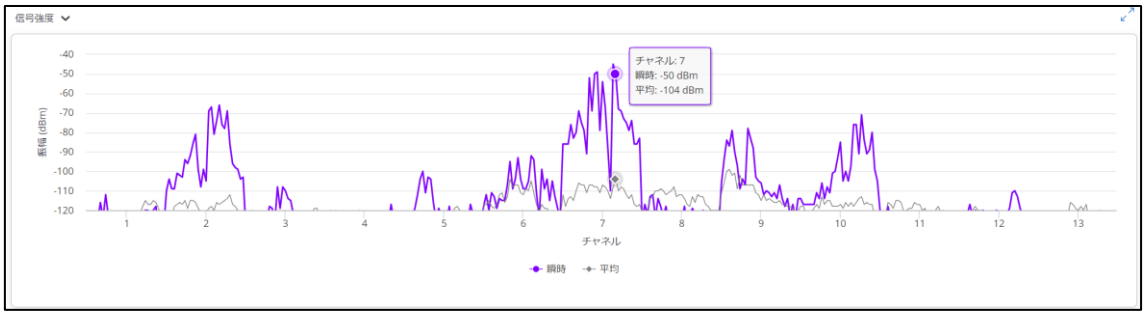
スペクトラム分析は、使用率とスペクトラム密度、各チャネルのパワーレベルの解析情報を表示することで、無線 LAN 以外の電波干渉などを確認することができます。[**スペクトラム分析**]画面を表示するには以下の手順を実行します。

1．[**モニター**]>[WiFi]>[**アクセスポイント**]順にクリックします。
2．アクセスポイントを右クリックし、[**スペクトラム分析**]>[**スペクトル・スキャンを実行**]をクリックします。

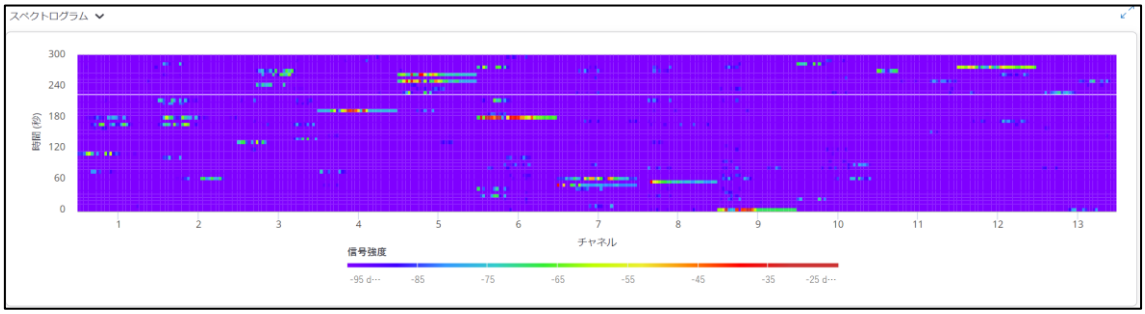
3．[**周波数帯**]を選択し[**実行**]をクリックします。

スペクトラム分析ではチャネルを基盤にフィルタリングできます。

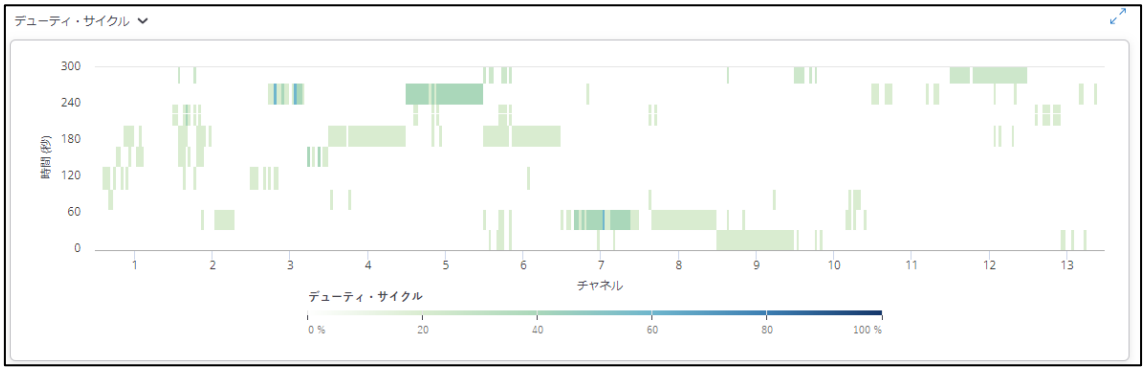
信号強度：Wi-Fi ソースに対してリアルタイムでチャネルごとの周囲の信号強度と、設定した期間での平均強度を示します。信号強度グラフの横軸(x)は[**チャネル**]縦軸(y)は[**振幅（dBm）**]です。



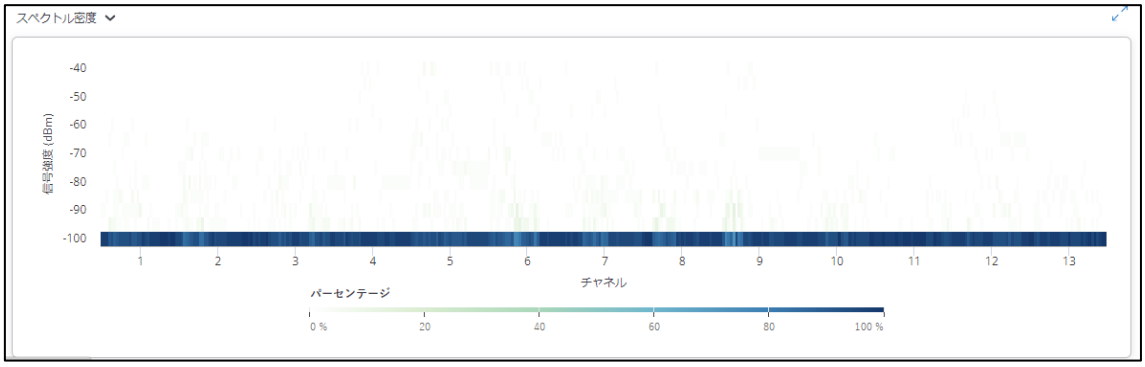
スペクトログラム：信号強度軸でチャネルごとの干渉波を色で区分し表示します。スペクトログラムグラフの横軸(x)は[**チャネル**]縦軸(y)は[**時間（秒）**]です。



デューティ・サイクル：リアルタイムでチャンネルのアクティブ水準や混雑度を確認できます。デューティ・サイクルグラフの横軸(x)は[**チャネル**]縦軸(y)は[**時間（秒）**]です。



スペクトル密度：信号強度軸でチャネルごとの干渉波を図式化します。スペクトル密度グラフの横軸(x)は[**チャネル**]縦軸(y)は[**信号強度（dBm）**]です。



2.15.11 イベントログの一覧表示

[**トラブルシュート**]>[**イベントログ**]から、選択したロケーションにあるすべてのアクセスポイントとクライアントのイベントログ一覧を確認することが出来ます。

[**アクセスポイント**]タブには、アクセスポイントのイベントログが保持されます。ログはアクセスポイントに関するものであり、クライアントやその接続情報に関連するデータは含まれていません。これらのイベントは アクセスポイントからリアルタイムで送信され、AIRRECT Cloudに保存されます。

イベントログに関する詳細は、以下の通りです。

パラメータ	概要
時刻	イベントが発生したタイムスタンプを表します。
名前	イベントが発生したAIRRECT APの名前を表します。
説明	イベントに関する説明を表します。
MACアドレス	イベントが発生したAIRRECT APのMACアドレスを表します。
場所	イベントが発生したロケーションを表します。
カテゴリ	イベントのカテゴリ(システム/無線通信/ネットワーク/SSID)を表します。
タイプ	イベントの重大度（重要/デバック/アラート/情報/エラー）を表します。

フィルタを使用すると、指定期間中の**アクセスポイントのイベントログ**の詳細が取得できます。

以下は、アクセスポイントに関するログ記録が残るイベントの種類です。
●アクセスポイント メモリステータス
●アクセスポイント 再起動
●アクセスポイント IPアドレスの競合
●アクセスポイント システムサービスクラッシュ
●アクセスポイント イーサーネットポートの状況
●アクセスポイント アップグレードの成功/失敗
●アクセスポイント コマンドラインを使用しての構成変更
●アクセスポイント DHCPのリース状況、その他

また、[**モニター**]>[Wi-Fi]>[**アクセスポイント**]の順に進み [**アクセスポイント**]を右クリックして[**トラブルシュート**]>[**イベントログの表示**]オプションをクリックすることでも、同様のイベントログを表示することができます。

イベントログに関する詳細は、以下の通りです。

パラメータ	概要
カテゴリ	イベントのカテゴリを表します。
タイプ	イベントの種類を表します。
説明	イベントに関する説明です。
日付	イベントが発生したタイムスタンプを表します。

アクセスポイントのイベントログと同様に、[**クライアント**]タブを選択すると、そのロケーションのクライアントイベント一覧が表示されます。表示内容の詳細は、『**クライアント・イベント**』をご参照ください。

2.15.12 ACS/DCSのメカニズムとレポート

Wi-Fi の干渉が多い場合、ネットワークの性能が低下する可能性があります。ACS(Auto Channel Selection)/DCS(Dynamic Channel Selection)計測とレポートは、アクセスポイントがチャネルを選択する際、電波干渉を感知/防止する機能です。レポートには、チャネル変更のイベント情報と変更要因のパラメータ情報が含まれます。
ACS は、起動時に実行され、最適なパフォーマンスを維持するために、以下のように最初と動作中に最適なチャネルを見つけます。

●起動時 ACS:隣接 AP が同じチャネルを選択する可能性を最小限に抑えるため、起動時にランダム化された時間間隔でチャネルをスキャンします。
●定期 ACS:無線環境を調査して、変更するのに最適なチャネルを見つけ、必要に応じて新しいチャネルを選択します。ACS の周期は設定変更が可能で、デフォルトは 12 時間です。

ACS チャネル選択の仕組みとしては、アクセスポイントが各チャネルをスキャンし、スキャンしたすべてのチャネルをランク付けしてより良いスコアのチャネルを優先的に選択します。チャネルの選択は、以下の手順で行われます。

1. チャネルのスキャン
2. チャネルフィルタリング
   Bluetooth・LTE 通信・電子レンジなどの Wi-Fi 機器を除いた周波数を発する機器のチャネルを使用している割合（非 Wi-Fi 使用率）が 40%を超えるとアクセスポイントはそのチャネルを破棄します。
3. チャネルランキング
   電波干渉状況をスコアリングし、ランク付けします。
   ●BSSID の数と強度：BSSID が少なければアクセスポイント間の競合が少なくなるため、良いスコアになります。その際には、受信強度も加味されてスコアリングされます。
   ●チャネルのオーバーラップ、チャネルボンディング： 隣接するチャネルがオーバーラップしており、干渉の影響がある場合はスコアが低くなります。
4. チャネルの選択
   他の AIRRECT AP で利用されていない、最もスコアが低いチャネルが選択されます。

チャネルが変更となるしきい値については、CLI から変更することも可能です。

通信品質を維持する仕組み

AIRRECT AP は、通信用アンテナとは別の、多機能アンテナを使用してチャネルをスキャンします。AP は常時 1ch あたり 120 ミリ秒のスキャンを行います。全周波数帯の継続的な監視は、非常に短いスキャンサイクルを実現でき、電波干渉を素早く回避することができます。1 スキャンサイクル、つまりチャネルスキャンにかかる時間は下記となります。

周波数帯	チャネル数	バックグラウンドスキャン（参考値）	多機能アンテナスキャン
2.4GHz	13 個	78 秒	1.56 秒
5GHz	20 個	120 秒	2.4 秒
6GHz	24 個	144 秒	2.88 秒

また、以下の仕組みにより通信中のアプリケーションが途切れないようになります。

●チャネルスイッチアナウンス（CSA）

定期 ACS の間、AP は、新しいチャネルに切り替える前に、チャネルスイッチアナウンス（CSA）をクライアントに送信します。AP は、新しいチャネルに切り替える前にクライアントに「新しいチャネルは X になります」と通知します。これにより、クライアントはどのチャネルに切り替える必要があるかを認識したあとに、チャネルを切り替えます。

●クライアント対応 ACS

定期 ACS で AP がチャネルを変更したことにより、アプリケーションを使用しているクライアントの接続性が低下する可能性があります。リアルタイムアプリケーションには厳しいタイミング要件がありますので（Voice over Wi-Fi の場合、一方向の遅延は 50 ミリ秒未満である必要があります）、突然のチャネル変更により、通話の音声の途切れや、動画のフリーズが発生する恐れがあります。これを回避するために、AP は、アドミッションコントロール中に TSpec（Traffic Spec）を使用して音声またはビデオコールを識別します。定期 ACS によってチャネルの変更が要求された際に、音声またはビデオコールがアクティブな場合、AP はチャネルの変更を延期することで、サービス品質（QoS）が保証されます。

チャネルスコアの確認

チャネルのスコアについてはインサイト機能より確認ができます。
ACS/DCS レポートを表示するには、以下の手順を実行します。

1. [**モニター**]>[WiFi]>[**アクセスポイント**]をクリックします。
2. アクセスポイントを右クリックし、[**トラブルシュート**]>[**イベントログの表示**]をクリックします。
   または、[**トラブルシュート**]>[**イベントログ**]の[**アクセスポイント**]タブの一覧から確認します。

3. チャネルログの[ ]をクリックすると、[**インサイト**]情報が表示されます。

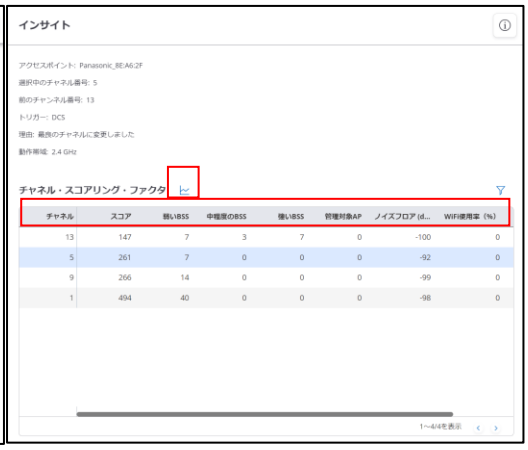
4．インサイトでは[**チャネル・スコアリング・ファクタ**]がテーブル表示されます。

チャネル	スコア	弱いBSS	中程度のBSS	強いBSS	管理対象AP	ノイズフロア (d...	WiFi使用率（%）
5	280	2	0	13	1	-85	11
9	302	5	0	3	0	-98	24
13	387	0	8	6	0	-96	10
1	1015	40	19	4	0	-96	21

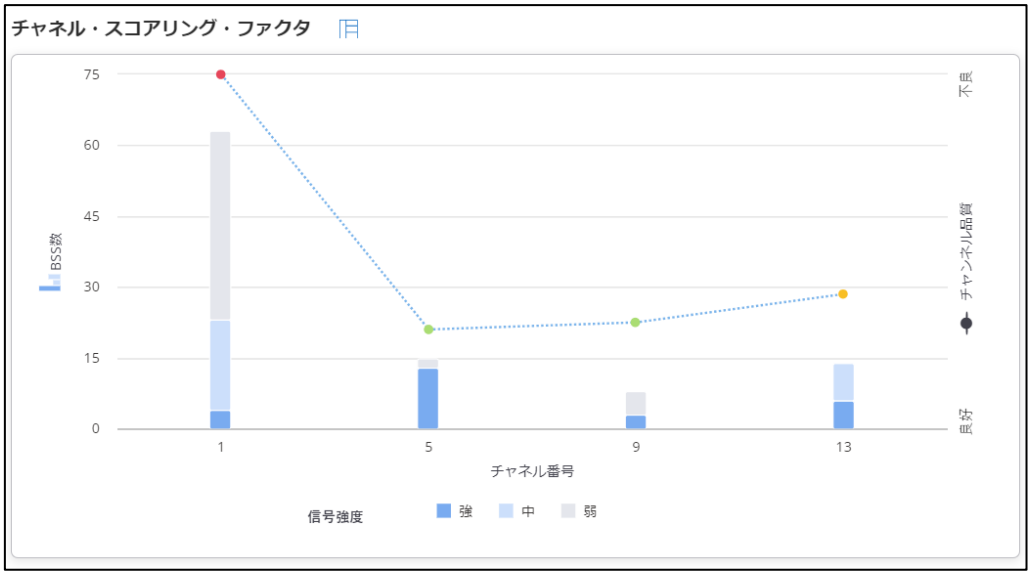
[**チャネル・スコアリング・ファクタ**]では、フィルタにより各情報が表示されます。

パラメータ	概要
チャネル	チャネル番号を表します。
スコア	チャネルのスコアを表します。
弱い BSS	35dBm<SNR の BSS 数
中程度の BSS	15dBm<SNR<=35dBm の BSS 数
強い BSS	15dBm<=SNR の BSS 数
管理対象 AP	チャネルに表示されるアクセスポイント数を表します。
ノイズフロア（dBm）	デバイスで作られるノイズの量を表します。（dBm）
WiFi 使用率（%）	Wi-Fi のチャネル使用率を表します。

スコアリングデータは、グラフ表示に切り替えることも可能です。



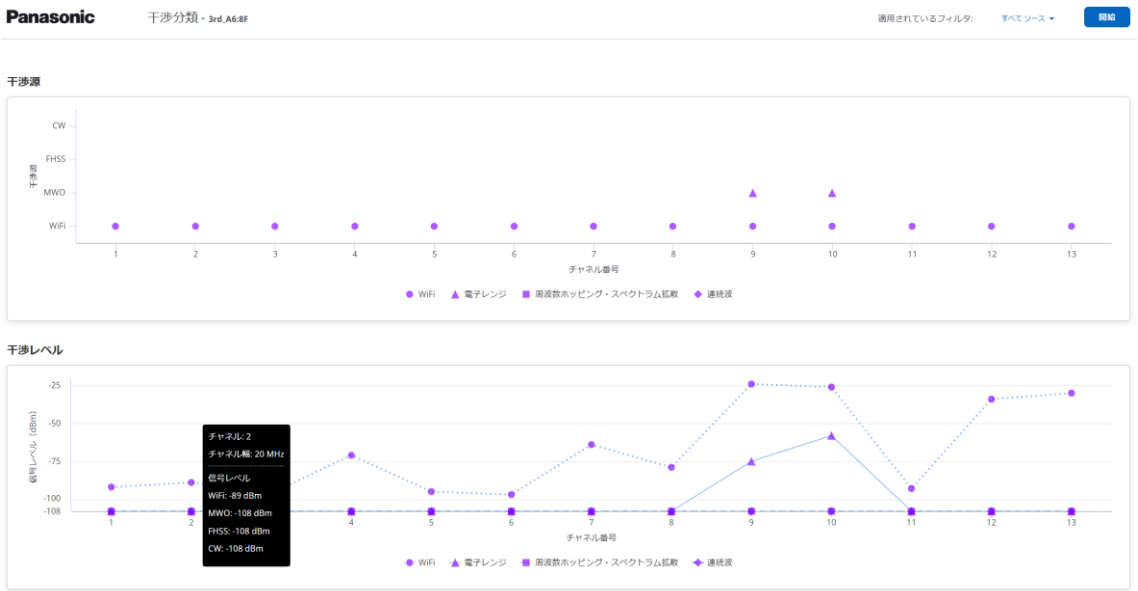
チャンネルスコアリングは、アルゴリズムを使用してスキャンされたすべてのチャネルの良好な順位を設定し、新しいチャンネルを選択する際に利用します。チャネルのスコアリングは下のように折れ線グラフで表示され、低いほど良好な値となります。



2.15.13 干渉分類

RF環境で問題が発生する原因の1つとしてWiFi以外の干渉があります。
干渉分類では、特定の帯域またはチャネルをスキャンし、WiFi、電子レンジ(MWO)、周波数ホッピングスペクトラム拡散(FHSS)、連続波(CW)の4つのカテゴリに分類し干渉度を調べることができます。

干渉分類を実行するには以下の手順を行います。
1.[モニター]>[Wi-Fi]>[アクセスポイント]の順に移動します。
2.干渉分類の開始するアクセスポイント名を右クリックします。
3.スキャンを実施する[周波数帯]または[チャネル]を選択の後、オプション設定を行います。
4.[開始]ボタンをクリックすると、別タブにて干渉分類の結果が表示されます。



グラフ上のプロットにカーソルを合わせると、分類ごとに信号強度が表示されます。

2.15.14 アクセスポイントのデバイス証明書

アクセスポイントのデバイス証明書とCA証明書を一元管理する機能です。
RadSecやアップリンクポート認証など、アクセスポイントのTLS認証が必要となる機能では、本セクションにてTLSデバイス証明書のアップロード操作が必要となります。

証明書を作成する前に、次の点に注意してください。

- 証明書データのサポート形式はPEMです。
- 最大5つのCA信頼チェーンの証明書をアップロードできます。
- デバイス証明書とCA証明書のアップロード箇所は異なります。（CA証明書のアップロード箇所：[**システム**]>[**詳細設定**]>[**CA証明書**]>[**CA証明書のアップロード**]）
- CSRを再生成した場合も、新しい署名済みデバイス証明書がアクセスポイントにアップロードされるまではアップロード済みの既存の証明書は削除されません。

<u>デバイス証明書アップロードまでのフロー</u>

1. **CSRを生成します。**
   a.新しい証明書タグを生成する場合は、[**新しい証明書タグを追加**]をクリックし、タグの名前を設定します。（グローバル証明書メニューからのみ可能）
   b.既存の証明書タグを生成する場合は、[**証明書タグを選択**]をクリックし、タグを選択します。

CSRは[**CSR設定**]にて設定した情報を基に生成されます。

2. **生成したCSRをダウンロードします。**
   ダウンロードしたいCSRを含む証明書タグを選択します。
   ダウンロードしたCSRは証明書発行機関へ提出し、デバイス（TLS）証明書発行の後、認証局による署名を行います。
   ※AIRRECT Cloudは証明書発行機関、認証局を提供しておりません。

3. **発行した署名済みデバイス証明書をアップロードします。**

証明書アクション

[モニター]>[Wi-Fi]>[アクセスポイント]タブに表示されるすべてのアクセスポイント、または各アクセスポイントに対し、証明書に関連する操作を実行します。
すべてのアクセスポイントに対する操作を行う場合には、グローバル証明書メニューから証明書アクションを実行します。

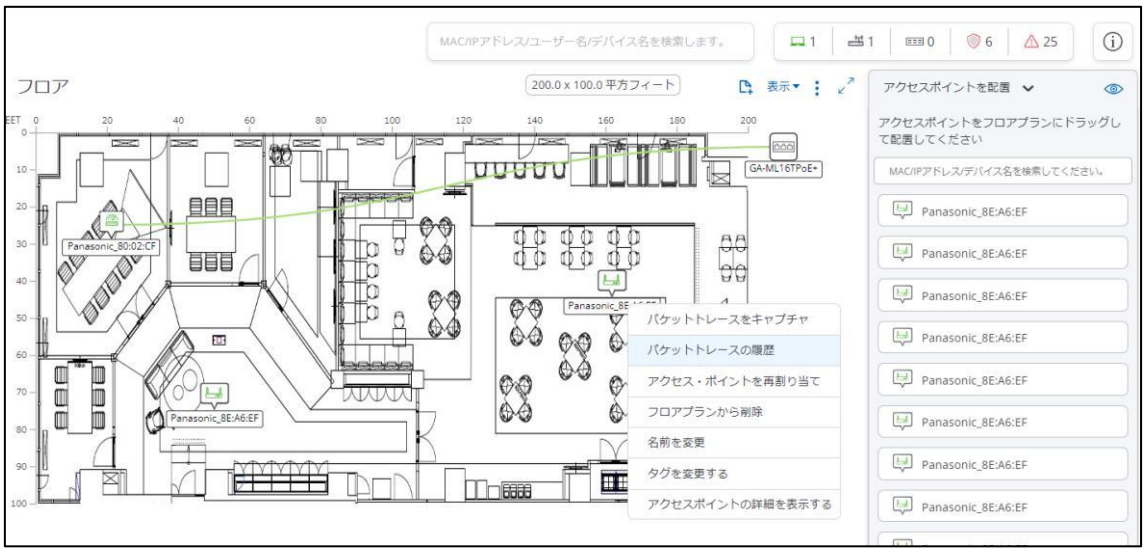
各アクセスポイントに対する操作を行う場合には、三点メニュー（⋮）から証明書アクションを実行します。

以下は、証明書アクションのパラメーター一覧とその概要です。

パラメータ	概要
CSRの生成	CSRを生成します。 生成時には、生成先となる証明書タグを設定、選択します。
CSRのダウンロード	生成したCSRをダウンロードします。 ダウンロード時には、ダウンロードしたい証明書タグを選択します。
デバイス証明書をアップロード	署名済みデバイス証明書をアップロードします。 アップロード時には、アップロード先となる証明書タグを選択します。
証明書を管理	アクセスポイントが持つすべての証明書タグを表示します。 証明書タグの名前、直近の証明書アクションログ（アイコン）、証明書ステータス（アイコン）、証明書の有効期限が表示されます。表内の三点メニュー（⋮）では各証明書タグに対する証明書アクションが可能です。 三点メニュー（⋮）でのみ使用可能です。
証明書の削除	アップロードした署名済みデバイス証明書を削除します。 削除時には、削除したい証明書タグを選択します。
証明書の再プッシュ	署名済みデバイス証明書を再アップロードします。 再プッシュ時には、プッシュしたい証明書タグを選択します。 アクセスポイントの誤動作により、アクセスポイントとアップロード済みデバイス証明書との関連付けに失敗した場合に使用します。削除済みデバイス証明書は再プッシュできません。
すべての証明書タグを削除	アクセスポイントが持つすべての証明書タグを削除します。 削除時には、削除したい証明書タグを選択します。 三点メニュー（⋮）でのみ使用可能です。
CSR設定	CSR設定を行います。 CSRは本セクションで設定した内容を基に生成されます。 グローバル証明書メニューでのみ使用可能です。
直近のユーザーアクションログをダウンロード	直近の証明書アクションログをダウンロードします。 グローバル証明書メニューでのみ使用可能です。

2.16 フロアプラン

ロケーションにフロアプランを追加し、アクセスポイントをフロアプランにドラッグアンドドロップすることで簡単にアクセスポイントの登録ができます。また、登録したアクセスポイントに対して複数の操作を実行することができます。
これにより、フロア内にあるアクセスポイントで複数の操作を実行する際に効率的に行えます。例えばネットワーク接続に関する問題がある場合やユーザー付近にあるアクセスポイントのパケットトレース履歴を閲覧したい場合は、フロアプランでアクセスポイントを右クリックし[**トラブルシュート**]>[**パケットトレースの履歴**]の順に進むと、パケットトレース履歴が表示されます。



AIRRECT Cloudの任意のロケーションで、そのロケーションのフロアプランとその直接の子ロケーションのフロアプランのみのカードビューを表示できます。ロケーション階層のさらに下にあるロケーションの平面図は表示されません。

2.16.1 フロアプランの設定

フロアプランの追加

AIRRECT Cloudのロケーションに、平面図のフロアプランを追加することができます。フロアプランを追加するには、以下の手順を実行します。

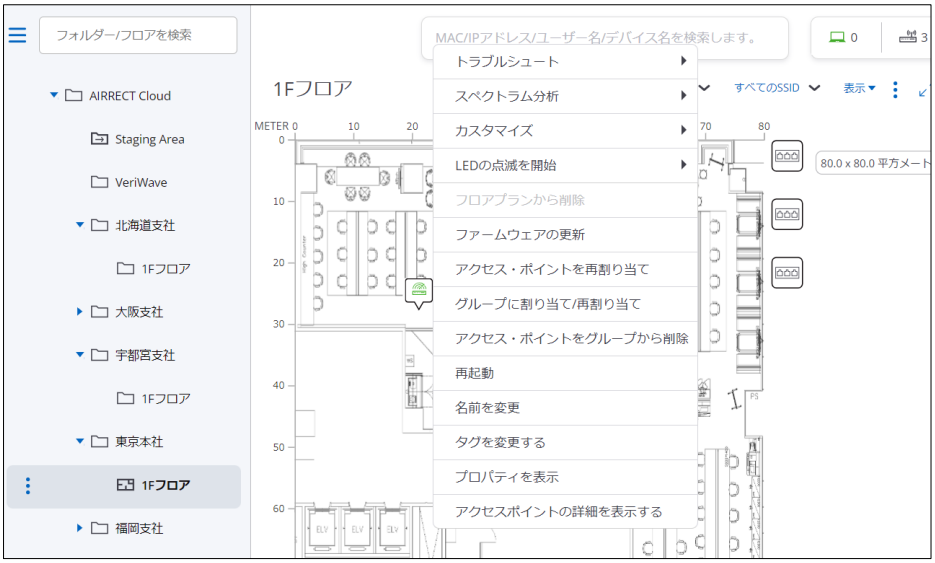
1. ロケーション階層で、フロアプランを追加するロケーションに移動します。[**フロアプランを追加**]をクリックします。

2. [**フロアプラン名**]を入力します。
3. [**イメージをアップロード**]から、アップロードするファイルを選択します。
4. [**フロアプランの寸法**]を設定します。
5. [**保存**]をクリックすると、フロアプランが保存されます。

フロアプランからアクセスポイントの操作をする

フロアプランのアクセスポイントでは、さまざまな操作を実行することができます。フロアプランのアクセスポイントの操作を実行するには、以下の手順を実行します。

1. ロケーション階層で、フロアプランのロケーションに移動します。
2. 平面図をクリックして開きます。
3. 右側パネルに表示されているアクセスポイントを、フロアプランの好きなロケーションにドラッグアンドドロップします。表示できるアクセスポイントは、管理しているAIRRECT Cloudと、任意に設定した認定アクセスポイントです。
4. 操作を実行したいアクセスポイントを右クリックし、実行したい操作を選択します。



2.16.2 ヒートマップ

ヒートマップにより、ユーザーがフロアプランに配置されたデバイスのカバレッジ、リンク速度、およびチャネルを視覚化できます。
また、フロアプランのさまざまなビューを選択して、フロアプランのデバイス配置、APカバレッジ、APリンクスピード、APチャネルカバレッジも視覚化できます。
デフォルトビューには、フロアプランとフロアに配置されたデバイスが表示されます。

1. 左側のパネルにある [**フロアプラン**]タブをクリックします。
2. デフォルトビューを表示する既存のフロアプランをクリックします。
3. 画面右上のメニュークリックし [**RFヒートマップ**]を選択します。

4. フロアプランのデフォルトビューとなる、[**既定のビュー**]が表示されます。

ヒートマップビューイング

選択したフロアプランの、以下のステータスがヒートマップで表示できます。
また、各タイプのヒートマップを選択すると、カラーパレットと、解像度、周波数帯域などを選択できるフローティングウインドウが表示されます。

●APカバレッジ
　フローティングウインドウで[**最小RSSI**]チェックボックスを選択すると、スケールバーで設定されているRSSIしきい値に従って、RSSIカバレッジを表示することができます。

●APリンクスピード

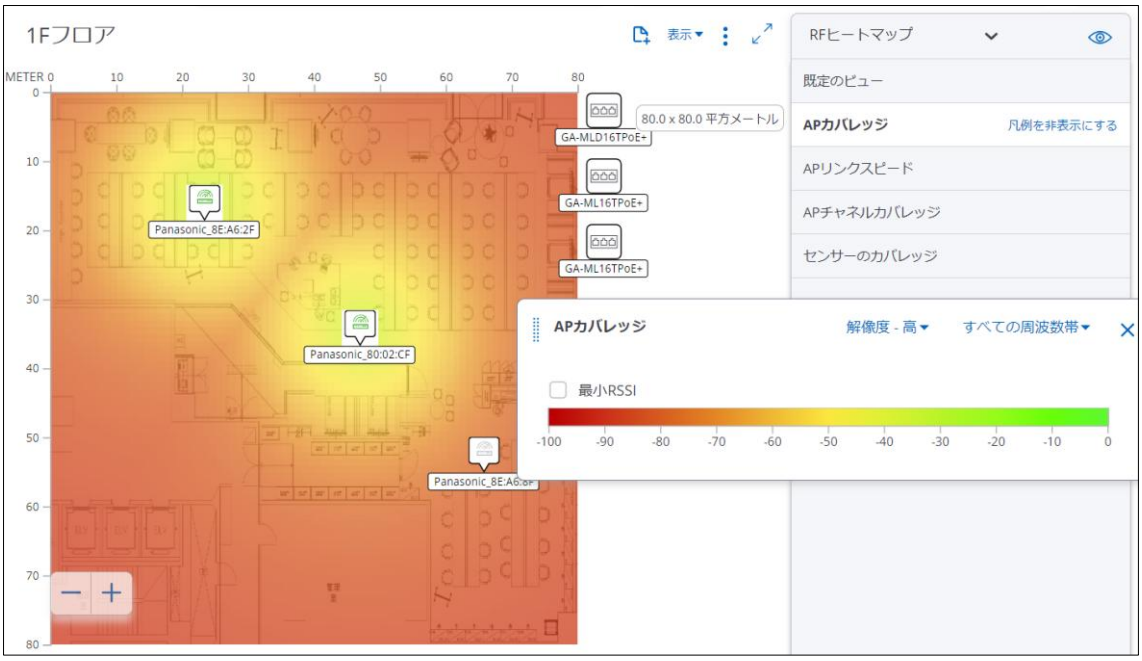
●APチャネルカバレッジ

●センサーのカバレッジ
　フローティングウインドウで不正端末の検出、または防御を行うカバレッジを表示します。検出感度で設定したセンサーのRSSIしきい値に従って、カバレッジを表示することができます。

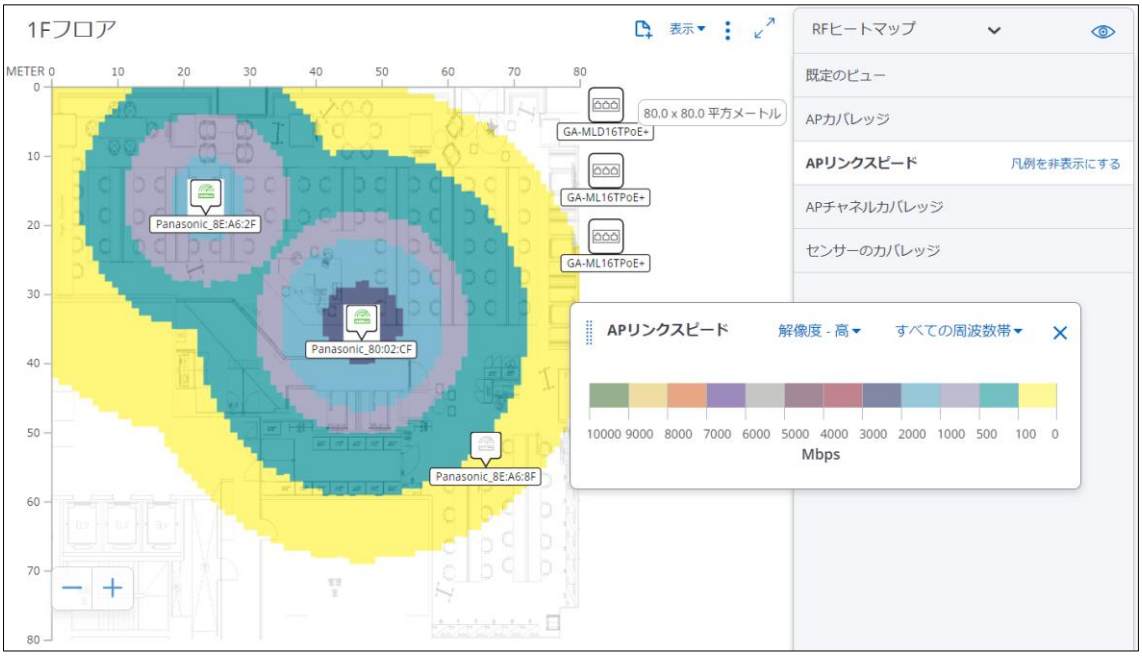
各フィルタの詳細については、『解像度と周波数フィルタ』を参照してください。

各ヒートマップビューを開くには、以下の手順を実行します。
1. 左側のパネルの [**フロアプラン**]タブをクリックします。
2. APカバレッジを表示したいフロアプランを選択します。
3. 右側のパネルから[**RFヒートマップ**]オプションを選択します。
4. 確認したいオプションを選択すると、フロアプランに情報が表示されます。

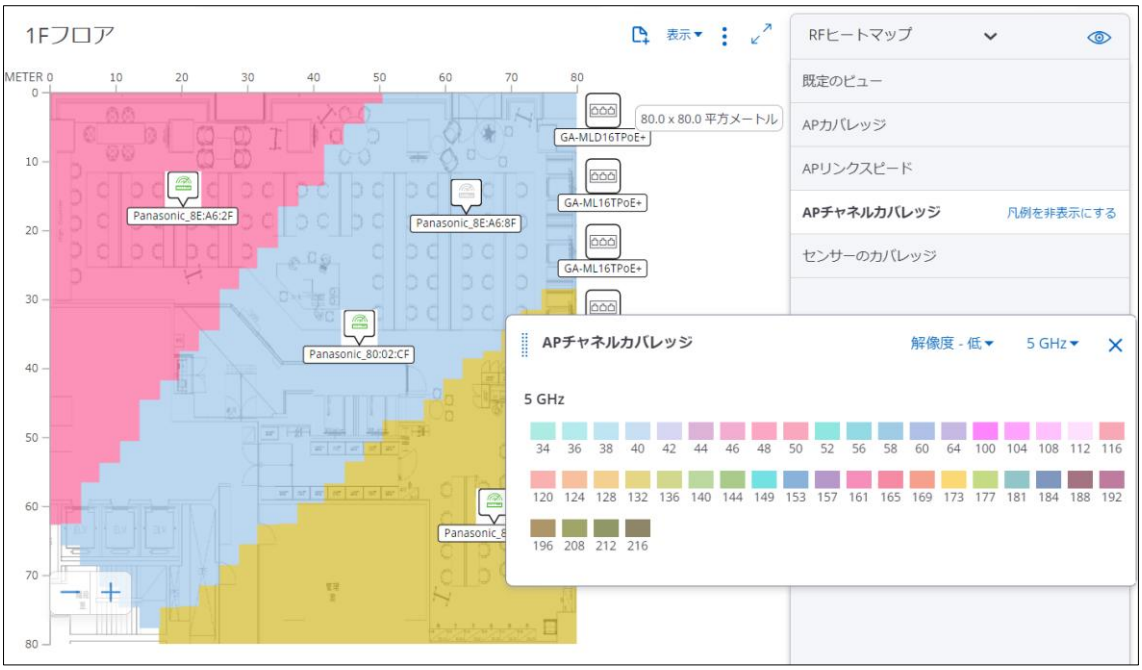
●APカバレッジビュー表示例



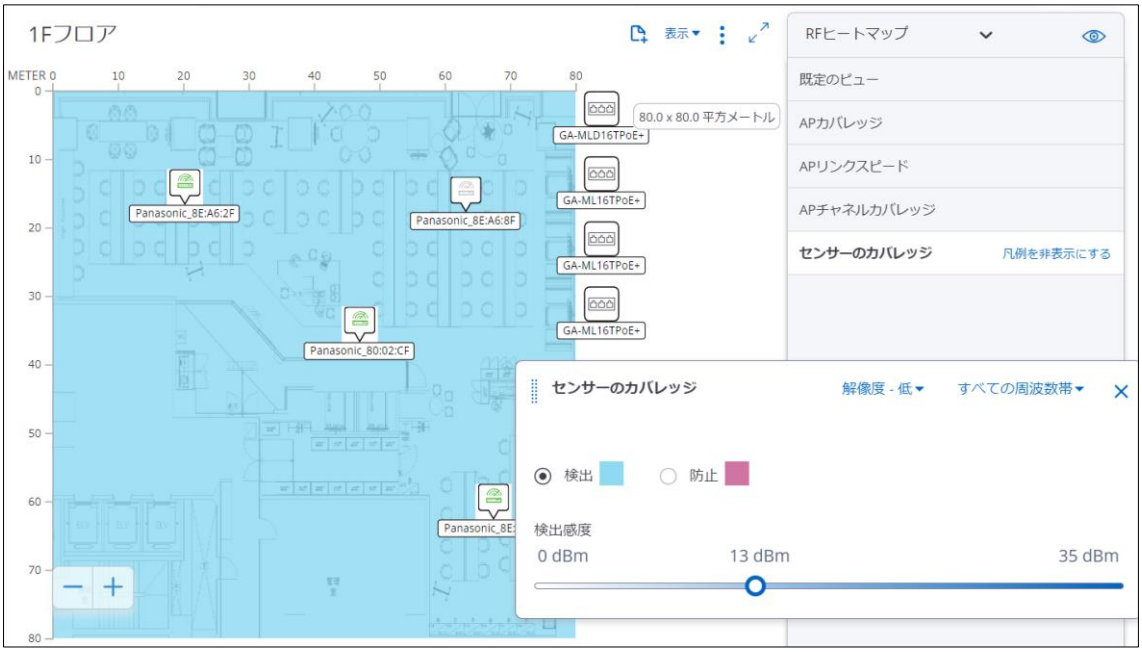
●AP リンクスピードビュー表示例



●APチャネルカバレッジビュー表示例



●センサーのカバレッジビュー表示例



解像度と周波数フィルタ

解像度と周波数は、ヒートマップで利用可能な2つのフィルタです。これらのフィルタは、[**既定のビュー**]を除くすべてのビューで使用できます。

解像度フィルタ

解像度フィルタは、フロアプランの解像度設定を設定するために使用されます。 解像度設定には、以下の3つの種類があります。

●低：計算と視覚化の精度は低いですが、結果が表示されるまでの時間は短くなります。

●中：計算と視覚化の精度は中程度で、結果が表示されるまで適度な時間がかかります。

●高：計算と視覚化の精度が最も高くなりますが、結果が表示されるまでに最大の時間がかかります。

周波数フィルタ

周波数フィルタは、アクセスポイントが動作している周波数に基づいてデータをフィルタリングするために用います。3つの基準に基づいて、データがフィルタリングされます。

●すべての周波数帯：2.4 GHz、5GHz、6GHzのデータが表示されます。

●2.4GHz：2.4GHzのデータが表示されます。

●5GHz：5GHzのデータが表示されます。

●6GHz：6GHzのデータが表示されます。

2.16.3 アクセスポイントとクライアントの検索

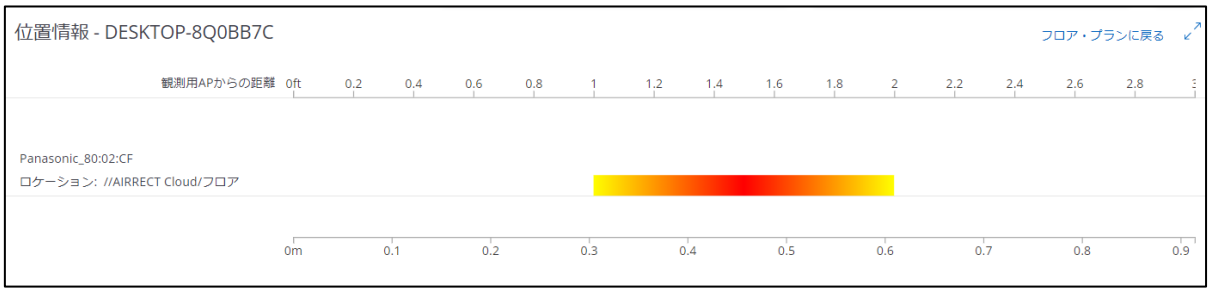
フロアプランに追加された特定のアクセスポイントやクライアントをUIから検索して探すことができます。また、この機能を使って、フロアプラン内の不正なアクセスポイントやクライアントを探すことができます。ただし、複数のデバイスまたはクライアントを検索することはできません。アクセスポイントやクライアントの位置の特定には、三角測量法を使用します。
AIRRECT Wi-Fiの以下の画面からデバイスの位置を検索し特定することができます。
●[フロアプラン]
●[モニター]>[Wi-Fi]>[クライアント]
●[モニター]>[Wi-Fi]>[アクセスポイント]
●[モニター]>[WIPS]>[管理対象Wi-Fiデバイス]
●[モニター]>[WIPS]>[アクセスポイント]
●[モニター]>[WIPS]>[クライアント]

アクセスポイントとクライアントの検索
サーバーが位置探知アルゴリズムを実行することで、アクセスポイントが別のアクセスポイントやクライアントのRSSIを報告します。アクセスポイントが別のアクセスポイントやクライアントを検出できるかどうかは、以下の 3 つの基準によります。
1. アクセスポイントまたはクライアントがアクティブである必要があります。
   ●位置探知を行うためには、クライアントはデータパケットを積極的に送信する必要があります。
   ●センサーモードで動作する配置されていない管理対象デバイスを見つけることはできません。
2. デバイスは、3台以上のアクセスポイントに認識されている必要があります。フロアにアクセスポイントが2つしかない場合、フロアプランでデバイスを見つけることはできません。代わりに、近接ビューが表示されます。

検索機能で使われる各デバイスの名称の意味は以下のとおりです。
●**管理対象デバイス：**アクセスポイントモード、または、専用WIPSモードで構成されたAIRRECT APです。当デバイスはフロアプラン上に配置することができます。
●**非管理対象デバイス：**管理対象デバイスの近くにあり、かつ管理対象デバイスから認識可能なWi-Fiデバイス（スマートフォンやアクセスポイントなど）です。
これらのデバイスはフロアプラン上に配置することはできませんが、デバイス間のデータトラフィックがあれば、位置を特定することができます。非管理対象デバイスは承認済み、不正（ローグ）、ゲスト、または外部のいずれかのカテゴリに分類されます。

●**配置されたデバイス：**フロアプラン上に配置された管理対象デバイスです。

配置されたアクセスポイントがない、またはフロアに配置されているアクセスポイントが3台未満でデバイスを見つけることができない場合は、デバイスの近接ビューが表示されます。[**近接**]ページには、他のアクセスポイントに対するデバイスのおおよその距離が表示されます。

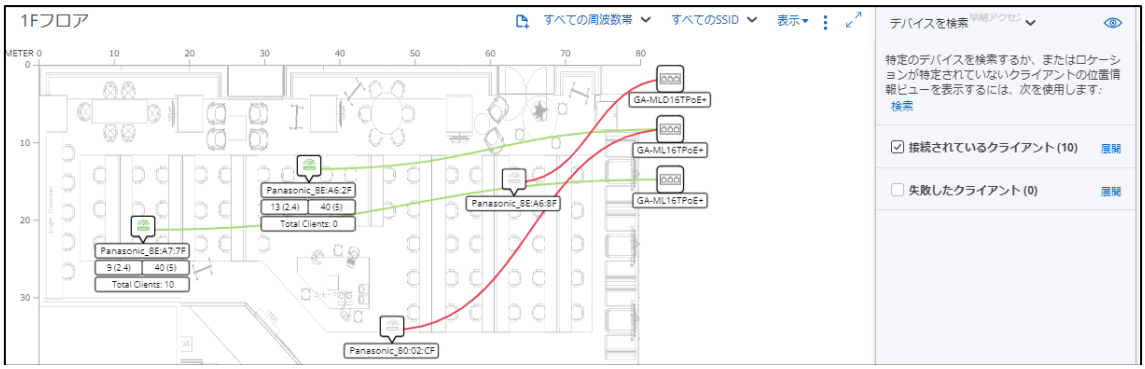


アクセスポイントとクライアントの検索方法

●フロアプランから探す(1)

管理されているクライアントやデバイスは、[**接続されているクライアント**]と[**失敗したクライアント**]のチェックボックスを使って探すことができます。管理されていない、配置されていないデバイスやクライアント、特にWIPSクライアントやデバイスを探すには、右パネルの[**検索**]オプションを使用します。また、[**検索**]を使用して、フロアプラン上で位置を特定できなかったクライアントの近接ビューを見ることができます。

1. [**フロアプラン**]をクリックして、[**ナビゲーター**]を展開します。
2. ロケーションツリーからロケーションを選択します。
3. 右側のパネルのドロップダウンメニューから[**デバイスを検索**]を選択します。
4. [**接続されているクライアント**]チェックボックスを選択して、フロアプラン内の管理対象デバイスとクライアントのリストを表示します。



●フロアプランから探す(2)

[**フロアプラン**]からアクセスポイントまたはクライアントの詳細ページに遷移することができます。[**フロアプラン**]でアクセスポイントを右クリックし、[**アクセスポイントの詳細を表示する**]をクリックすると、そのデバイスの詳細ページにリダイレクトされます。
リダイレクトされたページでは、アクセスポイントのプロパティと、現在アソシエーションされているクライアントと、対象のアクセスポイントが情報を共有している別のAIRRECT AP情報が表示されます。

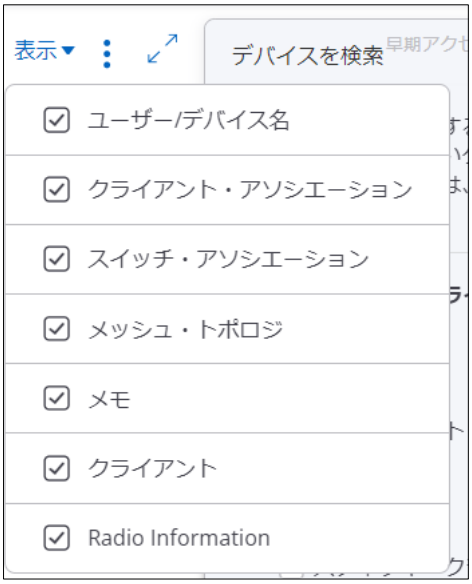
特定のデバイスを探知する

管理対象の配置済みアクセスポイント、管理対象外の配置済みアクセスポイント、単一のクライアントなどの特定のデバイスを探知することができます。
例として、不正であると思われる特定のクライアントを監視する場合は、このオプションを使用してクライアントを特定します。
アクセスポイントを見つけるには、以下の手順を実行します。

1. [**モニター**]>[Wi-Fi]>[**アクセスポイント**]をクリックします。
2. リストからアクセスポイントを選択し、右クリックします。
3. [**検索**]をクリックします。
   アクセスポイントが配置されているフロアプランに移動します。 デバイスが見つからない場合は、[**近接ビュー**]ページに移動します。同様に、[**モニター**]>[Wi-Fi]>[**クライアント**]からクライアントを探すことができます。
   ※非アクティブなデバイスの場合、または複数のデバイスが選択されている場合、[**検索**]メニューは無効になります。

フロアプランに表示される内容

画面右上の[表示]フィルターから、フロアマップに表示させる情報の変更ができます。



●[**ユーザー/デバイス名**]：クライアントのユーザー名とアクセスポイントのデバイス名を表示します。

●[**クライアント・アソシエーション**]：どのクライアントがどのアクセスポイントにアソシエートされているかを表示します。

●[**スイッチ・アソシエーション**]：どのスイッチがどのアクセスポイントと接続されているかを表示します。スイッチの表示については、『スイッチのトポロジー表示』をご参照ください。

●[**メッシュ・トポロジ**]：アクセスポイント間のメッシュリンクを表示します。
本フィルタは「デバイスを検索」を有効化しているときのみ選択できます。

●[**クライアント**]：アクセスポイントが接続しているクライアント数を表示します。

●[**無線情報**]: 無線電波が2.4GHz/5GHz/6GHz帯のどのチャネルで動作しているか表示します。

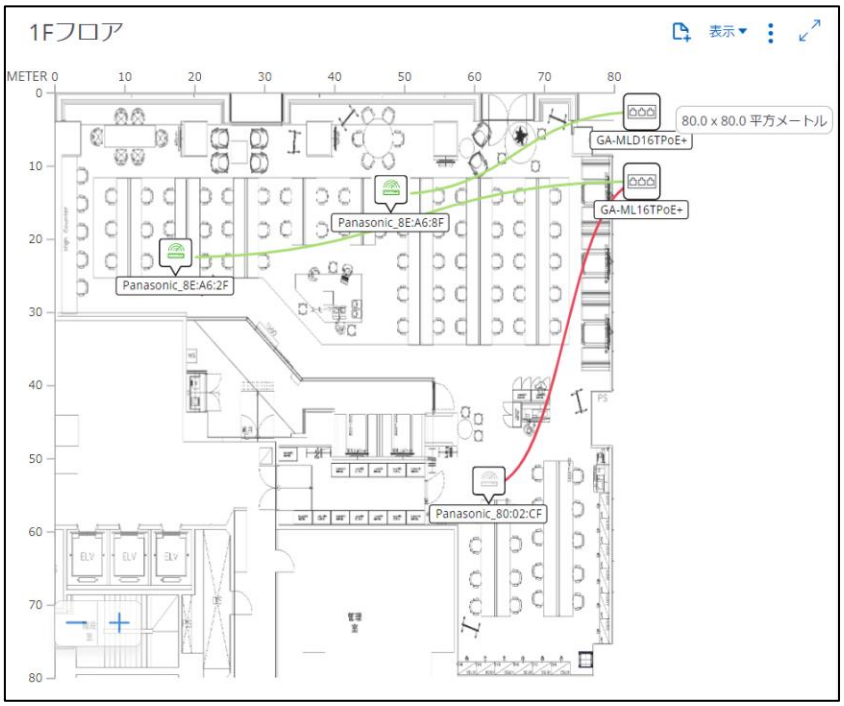
●[**メモ**]：作成したメモアイコンを表示します。メモは、[**表示**]フィルタ左のアイコンをクリックすることで、作成が可能です。

●[**接続されているクライアント**]と、[**低RSSI**]や[**低データレート**]などの接続状態

●[**失敗したクライアント**]と、[**アソシエーション失敗**]や[**認証失敗**]などの失敗の理由

2.16.4 スイッチのトポロジー表示

フロアマップを登録しておくことで、アクセスポイントに接続しているスイッチングハブをフロアに表示・配置することができます。これにより、どのアクセスポイントがどのスイッチングンハブに接続しているか、また、接続が正常にできているか確認することができます。アクセスポイントが正常にスイッチングハブと接続できているときは緑色の線で接続が示され、通信断などによりスイッチングハブと接続されていない場合は赤色の線で示されます。トポロジーは、任意のフロア右上の[**表示**]フィルタリングから、[**スイッチ・アソシエーション**]を有効化することで表示されます。



また、アクセスポイントにカーソルを合わせると詳細情報が表示されるので、スイッチングハブのどのポートにアクセスポイントが接続されているか等の確認をすることができます。

注意：スイッチングハブを表示させるには、スイッチングハブのLLDPが有効になっている必要があります。また、スイッチングハブのアイコンは自動で表示され、変更することが出来ません。当社製スイッチングハブの場合、デフォルトでLLDPが無効のため、CLIにて以下の設定が必要です。

【設定例：GA-MLシリーズ、MGA-ML4TWPoE++共通】

⑴スイッチ名設定　｜　(config)# snmp-server name <switch name>

➡スイッチ名が設定済みの場合は⑴はスキップして下さい。

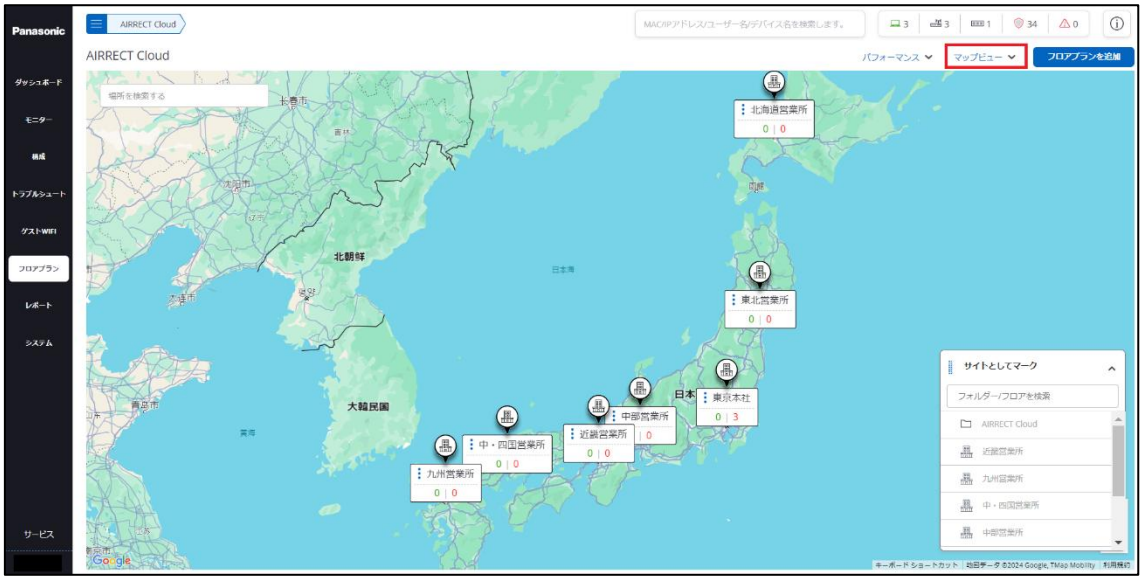
⑵LLDP有効化　｜　(config)# lldp run

⑶スイッチ名の表示 ｜　(config-if)# lldp tlv-select system-name

その他の機種のコマンドについては、各スイッチングハブのCLIリファレンスをご確認ください。

2.16.5 マップビューの表示

[フロアプラン]>[マップビュー]画面では、Google マップ上へフォルダを配置することができ、配置した各フォルダのネットワーク状況を瞬時に把握することができます。
※フロアやグループを配置することはできません。



Google マップを操作する

マウスホイールで拡大/縮小表示、ダブルクリックで拡大表示、ドラッグ&ドロップ、またはキーボード（←↑↓→）で移動、UI 左上の「**場所を検索する**」で住所検索が可能です。

フォルダを Google マップへ配置する

UI 右下の「**サイトとしてマーク**」に表示されているフォルダをドラッグ&ドロップにより Google マップへ配置することができます。
※別フォルダの Google マップへ既に配置済みのフォルダは再配置できません。

配置済みフォルダを Google マップから削除する

[⋮]>[サイトを削除する]で削除します。

フォルダを正確な位置に配置する

[⋮]>[サイト座標の編集]を選択します。
「**場所を検索する**」へ住所を入力した後、「**保存**」を選択します。

各フォルダのネットワーク状況を確認する

画面右上のプルダウンにて、確認したい情報を選択します。

緑色は正常なデバイス数、赤色は異常なデバイス数を示します。

●**接続**：SSID 接続プロセス結果を表示します。

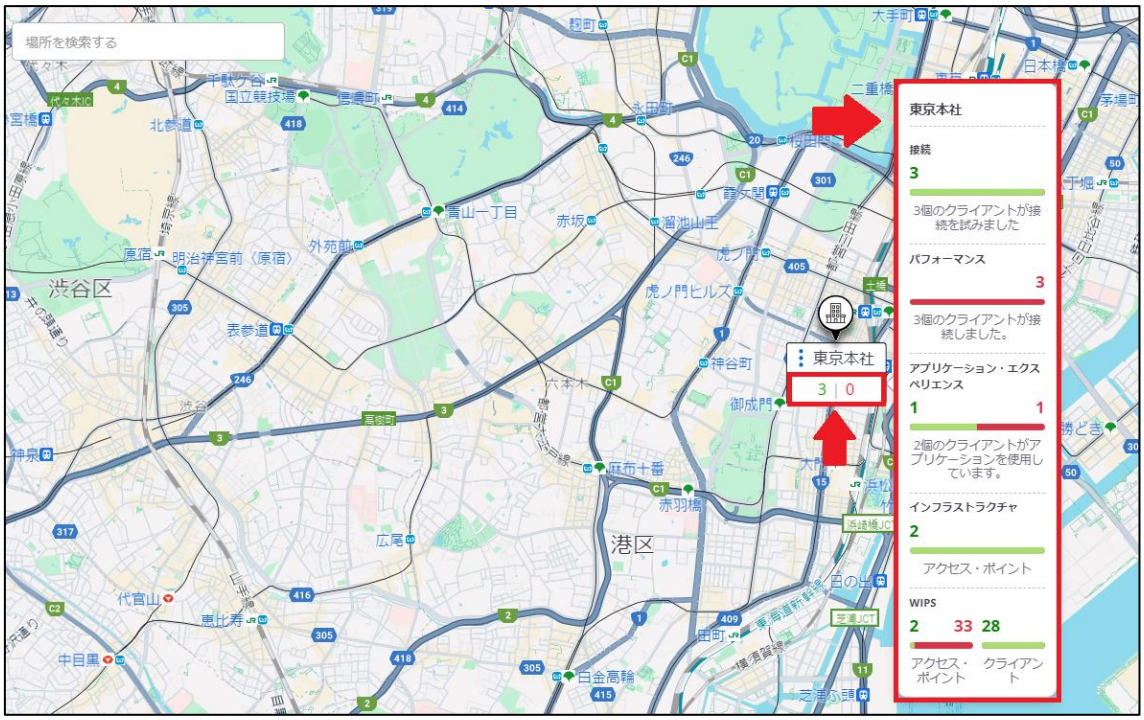
●**パフォーマンス**：Wi-Fi 環境のパフォーマンスを表示します。

●**アプリケーションエクスペリエンス**：Wi-Fi 通信の品質を表示します。

●**インフラストラクチャ**：アクセスポイントの負荷を表示します。

●**WIPS**： WIPS アンテナにより検出されたデバイスを表示します。

表示数値のクリックで、他情報も合わせて表示させることができます。



2.17 レポート

メニューの[**レポート**]タブから、現在のネットワーク状況をHTMLまたはExcelでレポート出力することができます。HTMLで出力したレポートは、PDFでも保存できます。また、レポートは定期的なスケジュールを組むことで、AIRRECT Cloud内にデータを蓄積することができます。レポートの種類としては、WiFi、WIPS、アラート、コンプライアンスに大きく分類されます。

レポートはそれぞれ、以下の情報を出力します。

レポートの分類	レポートの種類	概要
WiFi＞インベントリ	WiFiアクセスポイント	[**モニター**]>[**WiFi**]>[**アクセスポイント**]の情報が出力されます。
	WiFiトンネル	[**モニター**]>[**WiFi**]>[**トンネル**]の情報が出力されます。
	WiFiクライアント	[**モニター**]>[**WiFi**]>[**クライアント**]の情報が出力されます。
	WiFiアクセスポイント詳細	[**モニター**]>[**WiFi**]>[**アクセスポイント**]>[**アクセスポイントエクスプローラー**]の情報が出力されます。
	WiFi無線	[**モニター**]>[**WiFi**]>[**無線通信(無線へのアクセス)**]の情報が出力されます。
	WiFi多機能ラジオ - 瞬時	[**モニター**]>[**WiFi**]>[**無線通信(多機能無線機)**]の情報が出力されます。
WiFi＞接続	クライアント特性	[**モニター**]>[**WiFi**]>[**クライアント**]>[**クライアントエクスプローラー**]の情報が出力されます。
	クライアント接続履歴	特定のクライアントが過去に接続した回数や接続に失敗した履歴、周波数帯ごとの接続回数等が出力されます。

レポートの分類	レポートの種類	概要
WiFi＞接続	クライアントアソシエーション	指定した期間での以下のクライアント情報が出力されます。 ●クライアントMAC ●プロトコル ●接続/切断時間とセッション時間 ●ロケーション ●データ転送量と転送速度 ●アクセスしたドメイン
	クライアントの可視性	指定した期間での以下のクライアント情報が出力されます。 ●クライアントMAC ●接続したロケーション ●最大RSSI値とその時のBSSIDのMAC ●接続/切断時間とセッション時間 ●接続したアクセスポイントMAC ●クライアントのランダムMAC有効/無効
WiFi＞アプリケーション	アプリケーションエクスペリエンスレポート	[**ダッシュボード**]>[**アプリケーション**]の[**アプリケーションエクスペリエンス**]の情報が出力されます。
WIPS＞インベントリ	WIPS管理対象WiFiデバイス	[**モニター**]>[WIPS]>[**管理対象WiFiデバイス**]の情報が出力されます。
	WIPSネットワーク	[**モニター**]>[WIPS]>[**ネットワーク**]の情報が出力されます。
	管理対象WiFiデバイスのインベントリ	各モデルごとのアクセスポイント数やアクティブなアクセスポイント数などの概要情報、およびロケーション、IPアドレス等の基本情報を含む、管理対象WiFiデバイスの概要が出力されます。
	WIPSクライアント	[**モニター**]>[WIPS]>[**クライアント**]の情報が出力されます。
	WIPSアクセスポイント	[**モニター**]>[WIPS]>[**アクセスポイント**]の情報が出力されます。

レポートの分類	レポートの種類	概要
WIPS＞ポリシー適用	無線空間リスク評価	利用しているネットワークに、オープンなSSIDやアドホックネットワークなどの脆弱性のある設定、クライアント接続の有無が出力されます。
	ワイヤレス脆弱性評価	不正クライアントからのアクセスやハニーポッド攻撃、DOS攻撃などのネットワークに関して脆弱性の有無とサマリーとして出力されます。
	セキュリティステータス	どのロケーションでどのようなセキュリティアラートがおきているかが出力されます。
	ワイヤレス侵入防止の概要	WIPS機能によって接続防止されたアクセスポイントまたはクライアントの情報とアラート情報が出力されます。
	アクセスポイントの分類	検出された認定AP、ローグAP、未分類AP、外部APのサマリーと、各アクセスポイントの詳細情報が出力されます。
	クライアントの分類	検出された認定クライアント、ローグ・クライアント、ゲスト・クライアント、外部クライアント、未分類クライアントのサマリーと、各クライアントの詳細情報が出力されます。
	WIPSアラート	[モニター]>[アラート]>[WIPS]の情報が出力されます。
アラート	システムアラート	[モニター]>[アラート]>[システム]の情報が出力されます。
	WiFiアラート	[モニター]>[アラート]>[WiFi]の情報が出力されます。
	WIPSアラート	[モニター]>[アラート]>[WIPS]の情報が出力されます。

レポートの分類	レポートの種類	概要
コンプライアンス	SOXワイヤレス・コンプライアンス	SOX法に要件に準拠に必要な無線環境条件と、現在の環境が条件を満たしているかの評価レポートが出力されます。
	PCI DSSワイヤレス・コンプライアンス	Payment Card Industry Data Security Standard（PCI DSS）: カード会員データを保護するための推奨セキュリティ・コントロールを規定に対して、無線環境の脆弱性要件と現在の環境が条件を満たしているかの評価レポートが出力されます。
	GLBAワイヤレス・コンプライアンス	米国GLBA法に要件に準拠に必要な無線環境条件と、現在の環境が条件を満たしているかの評価レポートが出力されます。
	PCI DSSワイヤレス・コンプライアンスの内部監査レポート	PCI DSSワイヤレス・コンプライアンスに加えて、違反の可能性のある内容についてもレポートとして出力されます。
	HIPAAワイヤレス・コンプライアンス	米国HIPAA法に要件に準拠に必要な無線環境条件と、現在の環境が条件を満たしているかの評価レポートが出力されます。
	DoD指令8100.2コンプライアンス	米国DoD指令8100.2法に要件に準拠に必要な無線環境条件と、現在の環境が条件を満たしているかの評価レポートが出力されます。
	MITSワイヤレス・コンプライアンス	カナダ連邦MITS法に要件に準拠に必要な無線環境条件と、現在の環境が条件を満たしているかの評価レポートが出力されます。

レポートの手動生成

[**レポートを生成します**]アイコンをクリックすると、画面右側にパネルが開き、下図のように設定パラメータが表示されます。

●レポート形式レポートの形式としては、HTML上での表示と、csvファイルでの出力が可能です。HTMLの画面右上のアイコンから、PDF出力または印刷を行うことができます。

●レポートデータの範囲
固定：任意の設定した時間から、現在までの無線環境データを出力します。
カスタム：レポートを出力する期間を選択します。

●レポートをアーカイブする
レポートをアーカイブして、あとで表示することができます。ユーザーのレポートアーカイブストレージは最大30MBまで保存されます。容量を超えた場合、過去のレポートを削除しないとレポートをアーカイブできなくなります。アーカイブされたレポートは、自動的に削除する日付を定義することもできます。

アーカイブされたレポートは、AIRRECT Wi-Fiの[**レポート**]>[**アーカイブ済み**]>[**保存**]から表示できます。アーカイブされたレポートは、レポート生成をしたユーザーの権限に応じて表示されます。

各ユーザーレベルのアクセス権限は、以下の通りです。
●スーパーユーザー：アーカイブされたすべてのレポートを表示できます。
●管理者：管理者がアーカイブしたレポートを表示できます。
●オペレーター：自分がアーカイブしたレポートを表示できます。
●ビューア：アーカイブの実施/アーカイブされたレポートの表示ができません。

任意のレポート名を右クリックすると、レポート名の変更、自動削除設定の変更、レポートの削除ができます。

また、レポート名の横のチェックボックスを選択し右クリックすると、まとめてアーカイブを削除することができます。まとめて削除する場合、アーカイブ数によっては処理に時間がかかる場合がありますが、削除処理中は、AIRRECT Cloudの操作はできなくなります。

レポートのスケジューリング生成

定期的なレポート生成をスケジューリングできます。管理者またはオペレーターの権限を持つユーザーは本機能によりスケジューリングできますが、閲覧者ユーザーはスケジュールされたレポートのみを閲覧できます。以下のように[**レポートをスケジュール設定します**]アイコンをクリックすると、画面の右側にパネルが開き、ユーザー設定可能なパラメータのセットが表示されます。

レポートのオンデマンド生成と同様に、レポート形式とレポートデータ範囲の設定と、定期保存する頻度を設定します。
設定頻度としては、以下の設定が可能です。
●1回：一度だけ、任意の日時で設定を行います
●定期：任意の期間内、生成間隔でレポートをアーカイブします。

レポートが正常にスケジュールされると、データは[**レポート**]>[More]>[**保存**]に格納されます。また、スケジュールされたレポートを配信するメールには、レポートの URL とその JSON バンドルが含まれています。デフォルトでは、レポート URL は一定期間利用できます。有効期限が切れたら、JSON バンドルをレポートレンダリングアプリケーションにアップロードして、レポートを表示できます。
アーカイブ設定が[**削除しない**] に設定されている場合、電子メールで送信された URL は、レポートが[**レポート**]>[More]>[**保存**]ページから手動で削除されるまで常に有効になります。

2.18 サードパーティサーバーの連携

サードパーティのサーバーとAIRRECT Cloudの統合は、システムレベルの操作であり、ネットワーク全体に適用されます。サードパーティーシステムと連携を行うと、AIRRECT Cloudからリアルタイムで登録したサーバーにデータが送信されます。また、サードパーティサーバーがローカルネットワーク上に設置されている場合には、CIPモードのAPが必要となります。

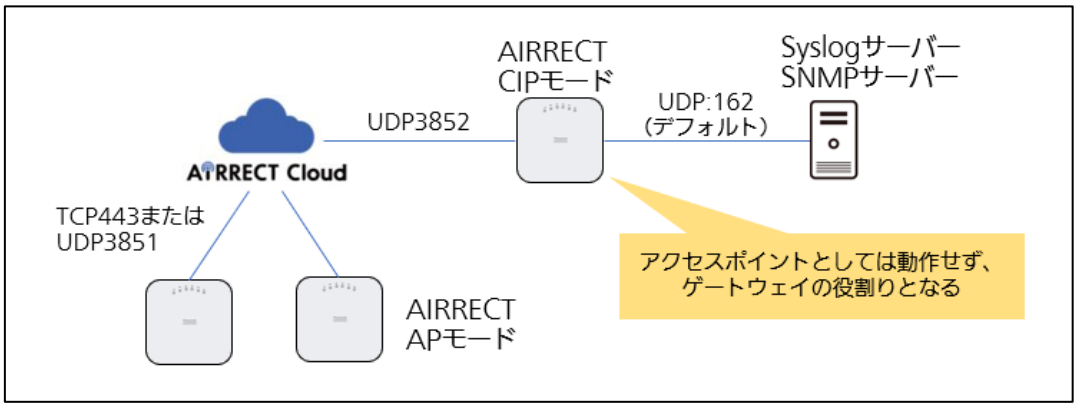
2.18.1 CIP(Cloud Integration Point)モード

AIRRECT APをCIPモードに切り替えることにより、AIRRECT Cloudをローカルで設置している各デバイスと統合し、以下のサードパーティ・サービスを既存のインフラを継続利用することができます。

●Syslogサーバー統合
●SNMPサーバー統合
●Cisco無線LANコントローラー（WLC）
●Arubaモビリティ・コントローラー

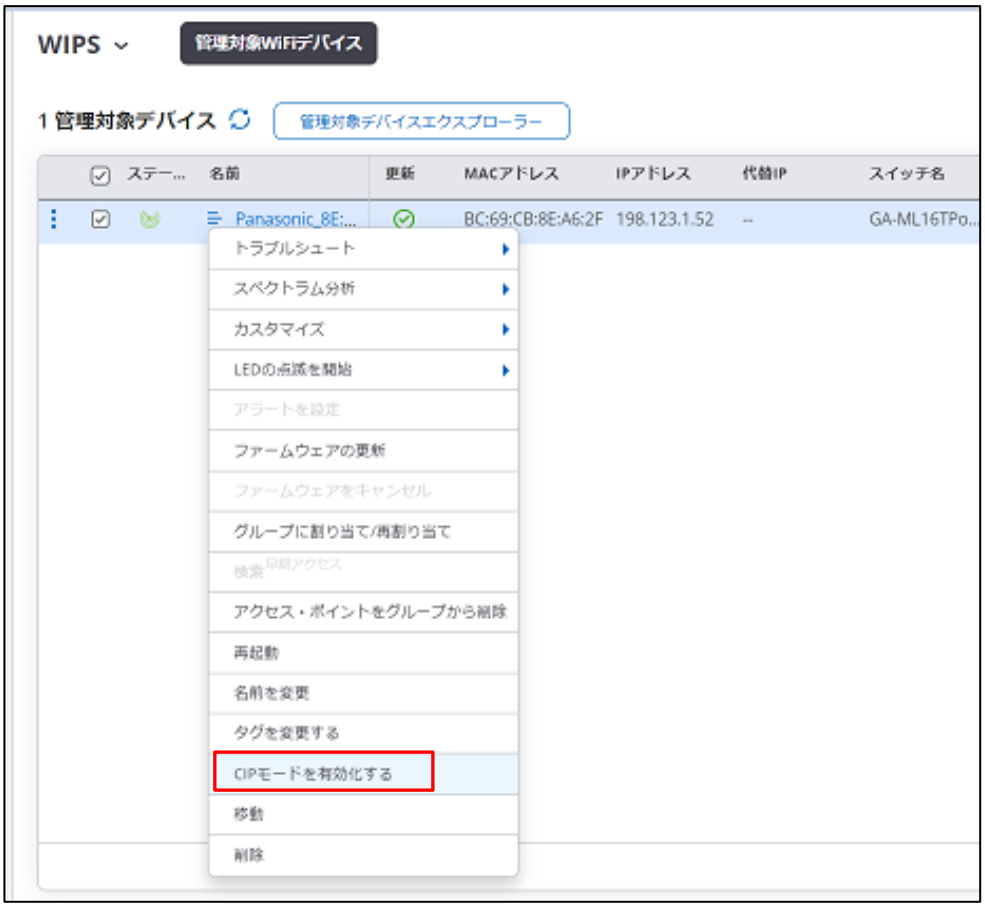
AIRRECT Cloud は、転送先のサードパーティサーバーがグローバル IP アドレスを持つ場合には直接通信が可能ですが、ローカル IP アドレスを持つ場合には直接通信できないため、ゲートウェイとなる CIP が必要となります。

CIPは、UDP3852を使用して、AIRRECT CloudとセキュアなOpenVPNトンネルを作成します。データはすべて OpenVPN トンネルを介して交換され、AES-256-CBC で暗号化、保護されます。CIPは、プライマリとセカンダリのペアで冗長構成が可能です。



CIPモードへの変更は以下の手順で実行します。

1. [モニター]>[WIPS]>[管理対象Wi-Fiデバイス]に移動します。
2. アクセスポイントを右クリックして「CIPモードを有効にする」を選択します。



2.18.2 Google統合設定

AIRRECT CloudとGoogle Workspaceアカウントで設定したChromebook等のデバイス情報を統合することが出来ます。
Google統合を行うことで、ネットワーク管理者はデバイスがネットワークに接続しようとしたときに、SSIDで設定したクライアント認証機能によってデバイスを承認または拒否できます。また、ロールベース制御により任意のポリシーを制御できます。Google統合したデバイスとの接続については、「クライアント認証の設定」を参照してください。

Google 統合を設定するには、以下の手順を実行します。

1. [**システム**]>[**サードパーティーのサーバー**]>[**Google統合**]の順にクリックします。
2. [**JSON キーファイルをアップロード**]をクリックすると、ファイル選択ウィンドウを開きます。
3. GoogleからダウンロードしたJSONキーファイルを選択し、[**開く**]をクリックします。JSONファイル名が AIRRECT Cloudの画面に表示されます。
4. [**管理者のメールアドレス**]を入力します。
   ※Googleで作成されたサービスアカウントのJSONキーにアソシエーションされたメールアドレスです。
5. [**クライアントリストの同期**]をクリックして、クライアントのリストを Google サーバーと同期すると、Google Workspace のクライアントリストが更新されます。

2.18.3 SNMPサーバー統合

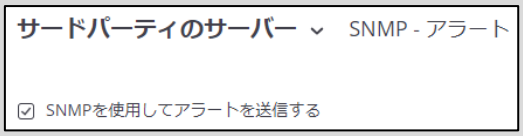
1 つまたは複数の SNMP サーバーに SNMP トラップで SNMP サーバーにアラートを送信することができます。
アラート用のSNMPサーバーを追加するには、[**システム**]>[**サードパーティのサーバー**]>[SNMP - **アラート**]の順に進み、[**宛先 SNMPサーバー**]テーブルで[**追加**]をクリックすると、画面右側に[SNMP Trap **送信先サーバーを追加する**]設定パネルが開きます。

以下の表では、各設定と概要が説明されています。

設定	概要
有効化する	AIRRECT CloudとSNMPサーバー間の通信を有効にする場合に選択します。
SNMP Trap 送信先サーバー IP/Hostname	SNMPサーバーのIPアドレスまたはホスト名を入力します。 ※SNMPサーバーがプライベートIPアドレスを使用する場合、クラウド統合ポイント(CIP)を選択する必要があります。
ポート番号	SNMPサーバーとAIRRECT Cloud通信のポート番号を示します。
プライマリ クラウド統合 ポイント（CIP）	ドロップダウンリストから、SNMPサーバーのプライマリクラウド統合ポイント(CIP)として使用するAIRRECT APを選択します。 ※CIPからAIRRECT Cloudへのネットワークでポート番号3852を開く必要があります。
セカンダリ クラウド統合 ポイント (CIP)	ドロップダウンリストから、SNMPサーバーのセカンダリクラウド統合ポイント（CIP）として使用するデバイスを選択します。プライマリCIPがダウンした場合、セカンダリCIPはサービスのクラウドへの接続を保証します。
SNMP バージョン	AIRRECT Cloudサーバーとコントローラーとの通信にSNMP v2、または、v3を選択します。
コミュニティ 文字列	SNMP v2の場合、SNMPサーバーで認証するカスタムコミュニティストリングを定義します。コミュニティストリングを必ず変更してください。
ユーザー名	SNMP V3の場合、AIRRECT CloudがSNMPサーバーにログインするための自動生成されたユーザー名を表します。
認証パスワード	SNMP v3サーバーで認証するためのパスワードを表します。
認証プロトコル	SNMP v3に使用される認証プロトコルを表します。

設定	概要
プライバシーパスワード	SNMP v3ベースのトラップの暗号化に使用されるシークレットキーを表します。
プライバシープロトコル	SNMP v3ベースのトラップの暗号化に使用される方法を表します。

注意: 個々のSNMPサーバーがすべて「有効」であっても、**[SNMPを使用してアラートを送信する]**チェックボックスが選択されていない限り、AIRRECT Cloudによってアラートは送信されません。



2.18.4 Syslogサーバー設定

AIRRECT CloudからSyslogサーバーを設定することで、本システムからメッセージを送信しサードパーティのSyslogサーバーに保存することができます。
Syslogサーバーを構成するには、以下の手順を実行します。

1. **[システム]>[サードパーティのサーバー]>[Syslog]**の順に進みます。
2. 「Syslog統合ステータス」は、Syslogサーバーのステータスを表しています。
   現在のステータスには、実行中、停止、エラーのステータス表示がされます。
3. **[Syslogサーバーを有効にする]**をクリックすると、AIRRECT CloudとSyslogサーバーの統合が有効に設定されます。
4. **[追加]**をクリックすると、 **[Syslogサーバーを追加する]**ウィンドウが表示されます。
5. **[Syslogサーバーを追加する]**ウィンドウで、詳細の設定を入力します。

設定	概要
有効化にする	AIRRECT Cloudと、このSyslogサーバー間の通信を有効にする場合に選択します。
Syslogサーバー IP /Hostname	SyslogサーバーのIPアドレスまたはホスト名を指定します。 ※SNMPサーバーがプライベートIPアドレスを使用する場合、クラウド統合ポイント(CIP)を選択する必要があります。
ポート番号	システムがアラートを送信するSyslogサーバーのポート番号を指定します。 初期値：514
プライマリクラウド統合ポイント (CIP)	AIRRECTとSyslogの統合を有効にするプライマリCIPを選択します。CIPでデバイスが選択されているSyslogサーバーはCIP宛先と呼ばれ、CIP対応のAIRRECT APのCIP宛先としてリストされます。
セカンダリクラウド統合ポイント（CIP）	Syslogサーバーのセカンダリクラウド統合ポイント（CIP）として使用するAIRRECT APを選択します。プライマリCIPがダウンした場合、セカンダリCIPはサービスのクラウドへの接続を保証します。
メッセージ形式	アラートを送信する形式を指定します。利用可能なオプションは、以下の通りです。 ・PLAIN ・IDMEF（侵入検知メッセージ交換フォーマット）
BOMヘッダーを追加する	バイトオーダーマークをSyslogサーバーエントリに追加します。これはプレーンテキストファイルの場合に関係があります。

イベントを送付する	[構成]>[アラート]で「通知」を選択したイベントをSyslogサーバーに転送します。
監査ログを送付する	監査ログをSyslogサーバーに送信します。 プレーンテキスト形式でのみ監査ログを転送できます。 注意：csvファイルは文字コードUTF-8で保存されます。

6. [**保存**]をクリックします。

2.18.5 Webフック

Webフックを使用すると、アラート通知をWebフック対応アプリケーション（Teams、Slackなど）へ通知することができます。

Webフックを設定するには以下の手順を行います。
1.[**システム**]>[**サードパーティサーバー**]>[**Webフック**]に移動します。
2.[**Webhookを有効にする**]を選択します。

3.[**エンドポイントを追加**]をクリックします。
注意：エンドポイントは最大4つまで追加可能です。
4.[**基本**]タブで次の設定を行います。

設定	概要
有効	Webフックのステータスを有効にする場合に選択します。
名前	Webフックの名前を入力します。
エンドポイントURL	エンドポイントURLを入力します。 注意：HTTP URLとIPv6アドレスはサポートしていません。必ずHTTPS URLを使用してください。
メソッドタイプ	HTTPメソッドタイプ（POST、PUT、GET）を選択します。デフォルトはPOSTです。GETメソッドがサポートする[**リクエストデータタイプ**]はフォームデータのみです。
要求ヘッダー	Webフックリクエストのリクエストヘッダーを追加する場合は、[**新しい行を追加**]をクリックし、キーと値のペアを設定します。最大10行まで追加可能です。

5.[**その他の設定**] タブで次の設定を行います。

設定	概要
SSL証明書の検証	SSL証明書の署名検証を行う場合に選択します。デフォルトは有効です。
応答タイムアウト	指定した時間が経過してもエンドポイントから応答が受信できない場合、リクエストを失効します。
再試行回数	エンドポイントへのリクエストの再試行回数を設定します。
固定クエリパラメータ	Webフックリクエストのクエリパラメータを追加する場合は、[**新しい行を追加**]をクリックし、キーと値のペアを設定します。最大10行まで追加可能です。
リクエストデータタイプ	フォームデータ：アラート内容をキーと値のペアで送信します。[**新しい行を追加**]をクリックし、キーと値のペアを設定、選択します。 ロウボディ：アラート内容を [{{field_name}}]で囲まれたフィールドとテキストを組み合わせで送信します。プレーンテキスト、JSON、XMLのいずれかの形式で設定可能です。
プライマリクラウド統合ポイント(CIP)	プライマリクラウド統合ポイント(CIP)として指定するアクセスポイントを選択します。エンドポイントがインターネット上に設置されている（グローバルIPアドレスを持つ）場合には設定不要です。
セカンダリクラウド統合ポイント(CIP)	セカンダリCIPを追加する場合は、[セカンダリクラウド統合ポイント(CIP)]をクリックし、セカンダリCIPとして指定するアクセスポイントを選択します。

6.[**完了**]をクリックします。

2.19 ホットスポットSSID

企業ネットワーク付近には、ホットスポットSSIDを出力するアクセスポイントが存在する可能性があります。企業クライアントが既知のホットスポットSSIDを認識した場合、ユーザが気づかないうちに接続している危険性があります。望ましくない接続が発生する可能性の高い、このようなSSIDをホットスポットSSIDとして分類できます。

ホットスポットSSIDを追加するには、以下の手順を行います。

1.[**システム**]>[**詳細設定**]に移動します。

2.[**ホットスポットSSID**]をクリックします。

3.[**追加**]をクリックします。

4.SSID名を入力し、[OK]をクリックします。

2.20 脆弱なSSID

企業ネットワーク付近には、デフォルト（工場出荷状態の名前）のSSIDを出力するアクセスポイントが存在する可能性があります。企業クライアントが既知のデフォルトSSIDを認識した場合、ユーザーが気づかないうちに接続している危険性があります。望ましくない接続が発生する可能性の高い、このようなSSIDを脆弱なSSIDとして分類できます。

脆弱なSSIDを追加するには、以下の手順を行います。

1.[**システム**]>[**詳細設定**]に移動します。

2.[**脆弱なSSID**]をクリックします。

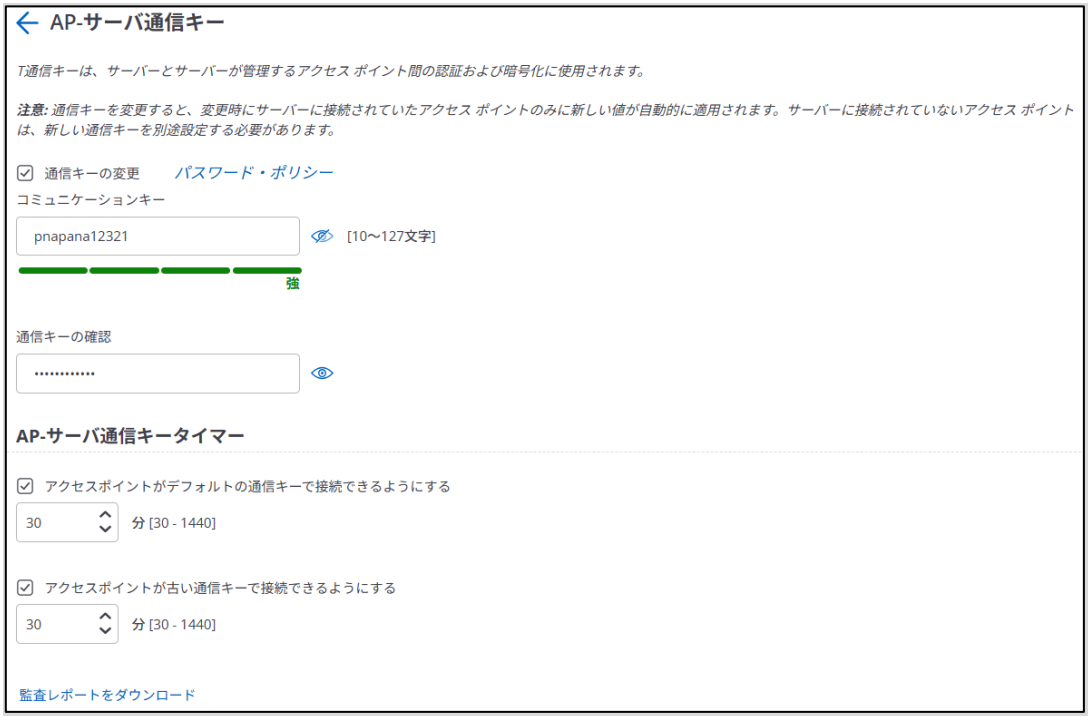
3.[**追加**]をクリックします。

4.SSID名を入力し、[OK]をクリックします。

2.21 AP-サーバ通信キー

サーバーとアクセスポイント間の認証および暗号化に使用する通信キー（共有鍵）を設定します。サーバーとアクセスポイントの双方が所有している通信キーが一致した場合のみ接続が許可され、不一致の場合には接続が拒否されます。通信キーを変更した場合、変更時にサーバーに接続していたアクセスポイントのみが変更後の通信キーを取得できます。

注意：デフォルト（工場出荷状態）の通信キーへの復元はできません。



新規アクセスポイントなど、現在設定中の通信キーを所有していないアクセスポイントをサーバーに接続したい場合、「**AP-サーバ通信キータイマー**」を使用します。

設定	概要
デフォルトの通信キーで接続できるようにする	デフォルトの通信キーを所有するアクセスポイントのサーバー接続を一時的に（設定した時間）許可します。
古い通信キーで接続できるようにする	変更前の通信キーを所有するアクセスポイントのサーバー接続を一時的に（設定した時間）許可します。

「**AP-サーバ通信キータイマー**」により接続したアクセスポイントは現在設定中の通信キーを自動で取得します。

監査レポートをダウンロード

過去 6 か月間の AP-サーバ通信キータイマーの履歴と、その間に接続されたアクセスポイントの情報を CSV ファイルでダウンロードできます。（接続履歴は AP-6810 のみ）

注意：デフォルト（工場出荷状態）の通信キーに関しまして、アクセスポイントには一意の値が設定されておりますが、サーバーは AIRRECT Cloud の契約年により異なります。
●2024 年以前にご契約の方
サーバーは、アクセスポイントと同じ通信キーが設定されております。
※すべてのアクセスポイント（AIRRECT AP）のサーバー接続が許可されますので、通信キーの変更を推奨（UI へ橙色マークを出現）しております。

●2025 年以降にご契約の方
サーバーは、アクセスポイントとは異なるランダムな通信キーが設定されております。新規アクセスポイントをサーバー（クラウド）に接続する場合は「**AP-サーバ通信キータイマー**」を使用する必要がございます。

3. 管理者設定

Launchpadの画面上部にある管理者タブから、AIRRECT Cloud管理に関する様々な設定ができます。AIRRECT Cloudにログインして利用できるユーザーはライセンス購入時に登録した管理者ユーザーとなりますが、任意に追加の管理者の設定や、ユーザー管理に関する詳細設定を行えます。

3.1 Launchpadユーザーの管理

Launchpadから、クラウド上のさまざまなサービスにアクセス可能なユーザーの作成や、許諾権限の付与をすることができます。各ユーザーにはプロファイルが割り当てられ、プロファイルにはそれぞれのLaunchpadサービス上で操作を行うための許諾権限が定義されています。

3.1.1 プロファイルの種類

Launchpadには、初期値で以下のシステム定義プロファイルがあります。

●Admin：Admin(管理者)プロファイルは、最も高い権限を有しています。管理者プロファイルを持つユーザーは、他のユーザーの管理、キー管理、機器登録、およびLaunchpad設定の管理をすることができます。また、他のLaunchpadサービスや使用可能なツールにおいて、最高位の許諾権限を割り当てられています。各サービスにおいてユーザーに割り当てられている個々の許諾権限または役割は、修正することができません。

●Custom：初期設定で新規ユーザーに割り当てられているプロファイルです。カスタムプロファイルには、定義されている許諾権限がありません。カスタムプロファイルを割

り当てたユーザーには、ユーザーの許諾権限を個々のサービスで設定する必要があります。そのため、カスタムプロファイルを持つ異なるユーザーが、使用するサービスによって異なる許諾権限を有していることがあります。

下記の表は、割り当てられたプロファイルによって、新規ユーザーがLaunchpadサービスで持つことのできる権限の詳細を示します。

プロファイル	Launchpad サービスにおける役割/権限			
	Launchpad	無線管理	キャプティブポータル	パケット解析
Admin	ユーザー管理/キー管理/設定/機器登録	Superuser	Administrator	User
Custom	ユーザーに権限を設定する	サービス有効時に、役割を設定する		

ユーザーアカウント情報の追加、編集、削除にはユーザー管理権限が必要です。他のユーザーやキーに対して行える変更は、ログインしているユーザーや、編集対象のユーザーやキーのプロファイルによって変わります。下記の表で、ログインしているユーザーが他のユーザーやキーに対して行える行為の詳細を示します。

他のユーザーを編集するユーザーのプロファイル	編集されるユーザー/キーのプロファイル	
	Admin	Custom
Admin	●アカウント情報/キー名称の編集 ●プロファイルの変更 ●ユーザー/キーのロック ●ユーザー/キーの削除 ●キーの値のリセット	●アカウント情報/キー名称の編集 ●プロファイルの変更 ●ユーザー/キーのロック ●ユーザー/キーの削除 ●サービスにおける許諾権限の変更 ●キーの値のリセット
Custom	---	●アカウント情報/キー名称の編集 ●プロファイルの変更 ●ユーザー/キーのロック ●ユーザー/キーの削除 ●共通サービスにおける許諾権限の変更 ●キーの値のリセット

上述のシステム定義プロファイルの他にも、Launchpadではユーザー定義プロファイルの作成が容易に行えます。ユーザー定義プロファイルについての詳細は、『ユーザー定義プロファイルの管理』をご参照ください。ローカルユーザーは、Launchpad上で限定的に認証されたユーザーです。

3.1.2 ユーザー管理の構成

ユーザーの追加

ユーザーを追加するためには、まずユーザーのアカウント情報を定義する必要があります。初期設定では、ユーザーにカスタムプロファイルが割り当てられています。ユーザーアカウント情報を保存後、ユーザーにサービス特権を割り当てる必要があります。

Launchpadでは、ユーザー（ローカルユーザー）をユーザー名とパスワードの組み合わせにより認証します。ユーザーが所属しているカスタマーの二要素認証が有効であれば、ローカルユーザーを二要素認証で認証できます。二要素認証の詳細については、『二要素認証の管理』を参照ください。

備考：ユーザーアカウントの最大登録数は、権限に関係なく25アカウントまでです。

ユーザーアカウント情報の追加は、下記の手順で行います。

1. [**管理者**]から、[**ユーザー**]タブをクリックします。既存ユーザーの一覧が表示されます。
2. [**ユーザー追加**]をクリックして、ユーザーを追加します。

3. アカウント情報を入力します。

パラメータ	概要
ログインID	ユーザーのログインID **注意**：ログインIDはEメール形式である必要があります。
Eメール	ユーザーのEメールID（自動入力）
姓	ユーザーの苗字
名	ユーザーの名前
タイムゾーン	ユーザーのタイムゾーン

4. [**保存**]をクリックします。

新規ユーザーが追加されると、アカウントのパスワードを設定するよう促す登録メールがユーザーに送信されます。メールを受け取ったユーザーは、メール内のリンクをクリックすることでパスワードを設定できます。

※登録メールは、[**EメールID**]に入力されたEメールへ送信されます。

プロファイルの割り当て
ユーザーの追加後、そのユーザーにプロファイルを割り当てる必要があります。
ユーザーへのプロファイル割り当ては、下記の手順で行います。
1. [**管理者**]から、[**ユーザー**]タブをクリックすると、既存ユーザーの一覧が表示されます。
2. 該当ユーザーの行右端のメニューマーク⋮をクリックし、[**サービス特権**]を選択します。
3. 必要なプロファイルを選択します。
4. [**保存**]をクリックします。
ユーザーへのサービス特権割り当てについての詳細は、『ユーザーのサービス特権の管理』を参照ください。

プロファイルを管理者からカスタムに変更する際に、カスタムプロファイル用に新たなルールが定義されるまで、Launchpadサービスに対するそれまでの許諾権限はすべて維持されます。カスタムから管理者にプロファイルを変更すると、ユーザーはすべてのLaunchpadサービスにおいて最高位の許諾権限を持ちます。

ユーザーの編集
ユーザーアカウント情報の編集には、ユーザー管理権限が必要です。 また、ユーザーのログインID、EメールIDは編集することはできません。他のフィールドはすべて編集可能です。
ユーザーアカウント情報の編集は、下記の手順で行います。
1. [**管理者**]から、[**ユーザー**]タブを選択すると、既存ユーザーの一覧が表示されます。
2. 該当ユーザーの行をクリックし編集します。
3. アカウント情報を修正します。
4. [**保存**]をクリックします。
ユーザーアカウント情報の変更は、次回ログイン時、つまりLaunchpadから一度ログアウトしログインした後に反映されます。

ユーザー認証形態の変更
ユーザーの認証形態には、ローカルユーザーがあります。
ローカルユーザー：Launchpad情報に基づいてLaunchpadへ認証されるユーザー

ユーザーのロック/ロック解除
ユーザーを予め定義して管理を行う準備をしておき、Launchpadへのアクセス権限を後ほど行いたい場合や、すでに有効なユーザーのLaunchpadへのアクセスを制限したい場合、または、特定のユーザーを削除せずにブロックしたい場合など、ユーザーアカウントをロックすることで、そのユーザーのLaunchpadへのアクセスを拒否することができま

す。ロックしたユーザーは、いつでもロック解除できます。ユーザーをロックすると、南京錠　アイコンがユーザーの[**姓名**]の右横に表示されます。
ユーザーのロックとロック解除は下記の手順で行います。
1. [**管理者**]から[**ユーザー**]タブをクリックすると、既存ユーザーの一覧が表示されます。
2. ロックまたはロック解除したいユーザーの行のメニューマークをクリックします。
3. [**ロック/ロック解除**]をクリックします。

リセットパスワード
ユーザー管理権限があれば、ユーザーのパスワードをリセットすることができます。
ユーザーパスワードをリセットすると、アカウントの新しいパスワードを設定するよう促すEメールがユーザーに送信されます。ユーザーは、通知されたEメール内のリンクをクリックすることで新たなパスワードを設定できます。
ユーザーパスワードのリセットは、下記の手順で行います。
1. [**管理者**]から、[**ユーザー**]タブをクリックすると、既存ユーザーの一覧が表示されます。
2. パスワードをリセットしたいユーザーの行をクリックします。
3. [**パスワードのリセット**]のチェックボックスを選択します。
4. [**保存**]をクリックします。
新しいパスワードを設定するためのEメールがユーザーのEメール IDに送信されます。

ユーザーの検索
ログインID、氏名、Eメール、最終ログイン、またはプロファイルからユーザーを検索できます。

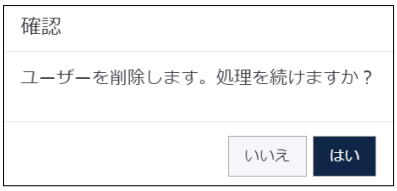
ユーザーの検索は、下記の手順で行います。
1. [**管理者**]から、[**ユーザー**]タブをクリックします。
2. 右上のユーザー検索ボックスに、検索キーワードをタイプします。
検索キーワードをタイプするごとに、マッチするユーザーの一覧が表示されます。

ユーザーの削除

ローカルユーザーを削除することができます。

ユーザーアカウント情報の削除は、下記の手順で行います。

1. [**管理者**]から、[**ユーザー**]タブをクリックすると、既存ユーザーの一覧が表示されます。
2. 削除したいユーザーの行のメニューマーク⋮をクリックします。
3. 表示されたポップアップメニューで[**削除**]をクリックすると、削除を確定させるメッセージが表示されます。



4. [**はい**]をクリックして、ユーザーを削除します。

※該当ユーザーのサービスに関連するデータの削除中にLaunchpad上で問題が起こった場合、ユーザーの削除は中断されます。

ユーザーアカウント一時停止ポリシー

[**管理者**]>[**設定**]の[**アカウントロックアウトポリシー**]で、続けてログインに失敗した後にLaunchpadユーザーアカウントを停止する設定ができます。

このオプションを設定するためには、以下の項目を設定する必要があります：

項目	概要
ログイン試行の最大失敗数	続けてログインに失敗した回数。
アカウントロック期間	分単位の時間。続けてログインに失敗するとこのポリシーが有効になる。
アカウントロックアウト時に表示されるメッセージ	続けてログインに失敗し、アカウントが一時停止されると表示されるメッセージ。
最小のパスワードの文字数	パスワード設定に必要な最低文字数。
二要素認証	2つの異なる情報による認証。詳しくは、『二要素認証の管理』を参照ください。
二要素認証を強制	二要素認証を強制するため。詳しくは、『二要素認証の強制』を参照ください。

3.2 ユーザー定義プロファイルの管理

ユーザー定義プロファイルの追加

ユーザー管理またはキー管理の許諾権限を有している場合、プロファイルタブが管理者セクションに表示されます。初期設定では、ユーザー定義プロファイルは、カスタムタイプです。プロファイルを追加する場合、プロファイル名が他と重複しないようにご注意ください。また、プロファイル名は空欄にできません。

ユーザープロファイルの追加は以下の手順で行います。

1.[**プロファイル**]タブをクリックします。
   システム定義プロファイルとユーザー定義プロファイルの一覧が表示されます。
2. [**新しいプロファイル**]をクリックして、新しいプロファイルを追加します。
3. [**プロファイル名**]を入力します。
4. [**保存**]をクリックします。プロファイルの保存後、プロファイルに応じた権限を設定できます。
5. [Launchpad]や[**パケット解析**]等の権限を設定し、再度[**保存**]をクリックします。

ユーザー定義プロファイルの編集

作成済みのシステム定義プロファイルの許諾権限に基づいて、ユーザー定義プロファイルの許諾権限を編集できます。自分に割り当てられたプロファイルは編集できません。

ユーザー定義プロファイルの編集は以下の手順で行います。

1. [**プロファイル**]タブをクリックします。
   システム定義プロファイルとユーザー定義プロファイルが入った一覧が表示されます。
2. 既存プロファイルのひとつをクリックします。
3. 必要なサービスのロールを設定後、[**保存**]をクリックします。

ユーザー定義プロファイルの削除

割り当てられているユーザーがいなければ、以下を除きユーザー定義プロファイルを削除することができます。

●ユーザー定義プロファイルに1人以上のユーザーが割り当てられている場合

●システム定義プロファイル

ユーザー定義プロファイルの削除は以下の手順で行います。

1. [**プロファイル**]タブをクリックします。
2. 削除対象のユーザー定義プロファイルの右端にある⋮アイコンをクリックします。
3. [**削除**]をクリックします。確認メッセージで[**はい**]をクリックし、プロファイルの削除を確定します。

プロファイルのユーザー/キー一覧表示

プロファイルに割り当てられているユーザーとキーの一覧を閲覧できます。Launchpadでは、プロファイルの下に、システム定義およびユーザー定義のプロファイルが一覧で表示されます。割り当てられているユーザーとキーの数が、それぞれのプロファイル名に対して表示されます。この数値はハイパーリンクになっています。数値のハイパーリンクをクリックすると、関連するユーザーまたはキーのページへとジャンプします。プロファイルに割り当てられているユーザーとキーの詳細を閲覧できます。

下図では、管理者プロファイルに割り当てられたユーザーの詳細が示されています。

下図では、カスタムプロファイルに割り当てられたキーの詳細が示されています。

3.3 ユーザーのサービス特権の管理

[**管理者**]からAIRRECT Cloudを利用する新規ユーザーを作成する場合、新規ユーザー作成完了後に、そのユーザーにサービス権限を割り当てます。サービス権限には、以下の種類があります。

●Admin：すべての操作が可能な最高権限をもつユーザー

●Custom：権限の範囲を任意に決めることで、操作を制限したいユーザー

3.3.1 Launchpadでの権限割り当て

Customプロファイルを持つユーザーにユーザー管理権限を割り当てると、そのユーザーは他のユーザーを追加、編集、削除ができるようになり、サービス特権を割り当てると、そのユーザー用に有効になっているサービスにアクセスできます。ユーザーにサービス特権を割り当てる場合、利用させたい個々のサービスを有効にしておく必要があります。また、そのユーザーにそれぞれのサービスに特有な役割を割り当てておく必要があります。Customプロファイルを持つユーザーのサービス特権は何度でも変更できます。

権限が割り当てられたユーザーは、アカウントロックアウトポリシーやパスワードポリシーといったカスタマーレベルのオプションを[**設定**]タブから設定できます。

サービス特権の割り当ては、下記の手順で行います。

1. [**ユーザー**]、[**キー**]、または、[**プロファイル**]タブをクリックします。既存のユーザー、キー、またはプロファイルの一覧が表示されます。
2. アイコン⋮をクリックして、[**サービス権限**]を選択します。
3. Launchpad関連のサービス特権を割り当てるには、[Launchpad]のタイルをクリックします。Launchpadの許諾権限画面に、[**ユーザー管理**]、[**キー管理**]、[**設定**]、[**機器登録**]のチェックボックスがそれぞれ表示されます。

4. ユーザーに割り当てたい権限に応じて、該当項目のチェックボックスを選択します。
各項目の詳細は以下のとおりです。

パラメータ	概要
ユーザー管理	Launchpadユーザーの管理をユーザーに許可します。
キー管理	第三者アプリがAPIコール経由でLaunchpadへアクセスするのに使用するキーの管理をユーザーに許可します。
設定	Launchpadユーザーに対するアカウントロックアウトポリシーやパスワードポリシーといった、カスタマーレベルのオプション管理をユーザーに許可します。
機器登録	LaunchpadサービスにおけるAIRRECT APの登録管理をユーザーに許可します。

5. [**保存**]をクリックし、ユーザーに割り当てた権限を保存します。

AIRRECT Cloudを利用する場合、ポータルやロケーションごとに権限を割り当てることができます。サービス権限読込後の2時間、ポータルとロケーションの一覧がサーバーのキャッシュに保管されています。最近作成したポータルやロケーションが一覧に表示されない場合は、更新アイコンをクリックして、リストを再読込してください。更新アイコンは、状況に応じてポータルまたはロケーションのリストの右上に表示されます。

3.3.2 キャプティブポータルでのサービス権限割り当て

キャプティブポータルでは、ゲストの管理やアナリティクスを行うことができます。キャプティブポータルでは、Administrator、Guestbook Operator、Analystといったユーザーの役割を定義できます。

●Administratorは、キャプティブポータルアカウントにおいて完全なアクセス権を持ちます。さらにポータル管理権限を持ち、アナリティクスやログにアクセスできます。

●Guestbook Operatorのアクセス権は非常に限定的です。自分が割り当てられているポータルでのみゲストユーザーの管理ができます。

●Analystは、すべてのポータルでアナリティクスを閲覧することができます。

※役割にあるMarketing Executiveは将来的な拡張機能です。
V.11.0.1では利用しません。

下記の表で、ユーザー種別のユーザー権限を、機能ごとに示します。

機能	操作	Administrator	Guestbook Operator	Analyst
ユーザーの管理	ユーザーの閲覧	可	不可	不可
	ユーザーの作成	可	不可	不可
	ユーザーの編集	可	不可	不可
	ユーザーの削除	可	不可	不可
ポータルの管理	ポータルの閲覧	可	不可	不可
	ポータルの作成	可	不可	不可
	ポータルの編集	可	不可	不可
	ポータルの設定	可	不可	不可
	ソーシャルメディアへの プラグイン設定	可	不可	不可
	ポータルの削除	可	不可	不可
Wi-Fi/WIPSサーバー管理	サーバーの追加	可	不可	不可
	サーバーの編集	可	不可	不可
	サーバーの同期	可	不可	不可
	同期設定の構成	可	不可	不可
	サーバーの削除	可	不可	不可
ゲストの管理	ゲストブックの設定	可	不可	不可
	ゲストユーザーの作成	可	可	不可
	ゲストユーザーの閲覧	可	可	不可
	ゲストユーザーの修正	可	可	不可
	ゲストユーザーの削除	可	可	不可
	ゲストユーザーの インポート/エクスポート	可	可	不可
	ゲストユーザーの 有効化/無効化	可	可	不可
	ゲストユーザーパッチの作成	可	可	不可
	ゲストユーザーパッチの エクスポート	可	可	不可
	ゲストユーザーパッチの閲覧	可	可	不可
	ゲストユーザーパッチの削除	可	可	不可

機能	操作	Administrator	Guestbook Operator	Analyst
Analytics	グラフの閲覧	可	不可	可
	ビジターログの閲覧	可	不可	可
	ビジターログのダウンロード	可	不可	可
ログの管理	ゲストアクセスログのダウンロード	可	不可	不可
	ユーザー監査ログのダウンロード	可	不可	不可
	SMSログのダウンロード	可	不可	不可
ダッシュボード	ダッシュボードの閲覧	可	不可	可
	ダッシュボードをPDFファイルでダウンロード	可	不可	可
	ダッシュボードレポートの予定作成	可	不可	可
レポート	レポートの作成	可	不可	可
	レポートの予定作成	可	不可	可
	レポートの複製	可	不可	可
	レポートのダウンロード	可	不可	可
	レポートのEメール送信	可	不可	可
	レポートの削除	可	不可	不可

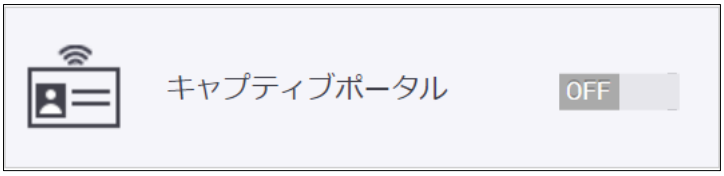
キャプティブポータルでのサービス権限の割り当ては、下記の手順で行います。

1. [**管理者**]から、[**ユーザー**]、[**キー**]、または[**プロファイル**]タブをクリックします。

既存のユーザー、キー、またはプロファイルの一覧が表示されます。

2.メニューアイコンをクリックして、[**サービス権限**]を選択します。

3. キャプティブポータルのタイルをクリックします。



4. [**ユーザーロール**]のドロップダウンリストから、割り当てたい役割を選択します。

ユーザーの役割としてGuestbook Operatorを選択する場合は、ポータルを選択します。

5. [**保存**]をクリックし、そのサービスでの設定を保存します。

3.3.3 無線管理でのサービス権限割り当て

無線管理では、Superuser、Administrator、Operator、Viewerという4つのユーザーが定義されます。Superuserはすべての権限を持っています。これに対してViewerの権限は最も限定的な権限です。
下記表に、Superuser、Administrator、Operator、Viewer のユーザー権限を機能ごとに示します。

機能ごとのユーザー権限					
機能	操作	Superuser	Administrator	Operator	Viewer
システム設定と運用ポリシー	システム設定のオプション	可	可	不可	不可
	アクセスポイント自動分類	可	可	不可	不可
	クライアント自動分類	可	可	不可	不可
	侵入防止	可	可	不可	不可
	LEDの点滅	可	可	可	可
イベント、デバイス、ロケーション	生成イベントの閲覧	可	可	可	可
	生成イベントの修正	可	可	可	不可
	生成イベントの削除	可	可	可	不可
	デバイスの閲覧	可	可	可	可
	アクセスポイント、クライアントの修正	可	可	可	不可
	アクセスポイント、クライアントの削除	可	可	可	不可
	ロケーションの閲覧	可	可	可	可
	ロケーションの追加	可	可	可	不可
	ロケーションの修正	可	可	可	不可
	ロケーションの削除	可	可	可	不可
レポート	共有レポートの生成	可	可	可	可
	共有レポートの予定作成	可	可	可	不可

選択したロケーションで、Wi-Fiアクセス管理機能、WIPS管理機能、またはその両方をユーザー向けに提供できます。
下記の表で、[**Wi-Fiアクセス管理**]を選択した場合にAdministratorおよびOperatorに割り当て可能な権限の一覧を示します。

機能ごとのユーザー権限			
機能	**操作**	Administrator	Operator
WIPS	認定済みWLANポリシー	不可	不可
	アクセスポイント自動分類	不可	不可
	クライアント自動分類	不可	不可
	禁止デバイスリストの管理	不可	不可
	侵入防止	不可	不可
	侵入防止機能の有効化	不可	不可
	WLAN統合/Aruba、WLC端末統合の管理	不可	不可
	デバイスリストロックの管理	不可	不可
	禁止デバイスリストの管理	不可	不可
Wi-Fiアクセス管理	デバイステンプレートの管理	可	不可
	SSIDプロファイルの管理	可	不可
	ネットワークインターフェイスの管理	可	不可
	デバイス詳細からのカスタム無線設定	可	不可
アクセスポイントの動作設定	禁止リストへの追加/からの削除	不可	不可
	隔離されたアクセスポイント	不可	不可
	カテゴリーの変更	不可	不可
	隔離ステータスの変更	不可	不可
	認知済みまたは外部デバイスとしてマーク/マーク解除	不可	不可
クライアントの操作	グループの変更	不可	不可
	隔離された端末	不可	不可
	禁止リストへのデバイス追加/からのデバイス削除	不可	不可
	不正端末の自動隔離	不可	不可

下記の表で、[WIPS管理]を選択した場合にAdministratorおよびOperatorユーザーに割り当て可能な権限の一覧を示します。

機能ごとのユーザー権限			
機能	操作	Administrator	Operator
WIPS	認定済みWLANポリシー	可	不可
	アクセスポイント自動分類	可	不可
	クライアント自動分類	可	不可
	禁止デバイスリストの管理	可	不可
	侵入防止	可	不可
	侵入防止機能の有効化	可	不可
	WLAN統合HP、Aruba、WLC統合の管理	可	不可
	デバイスリストロックの管理	可	不可
	禁止デバイスリストの管理	可	不可
Wi-Fiアクセス管理	デバイステンプレートの管理	不可	不可
	SSIDプロファイルの管理	不可	不可
	ネットワークインターフェイスの管理	不可	不可
	デバイス詳細からのカスタム無線設定	不可	不可
アクセスポイントの動作	禁止リストへの追加/からの削除	可	可
	隔離されたアクセスポイント	可	可
	カテゴリーの変更	可	可
	隔離ステータスの変更	可	可
	認知済みまたは外部デバイスとしてマーク/マーク解除	可	可
クライアントの操作	グループの変更	可	可
	隔離された端末	可	可
	禁止リストへのデバイス追加/からのデバイス削除	可	可
	不正端末の自動隔離	可	可

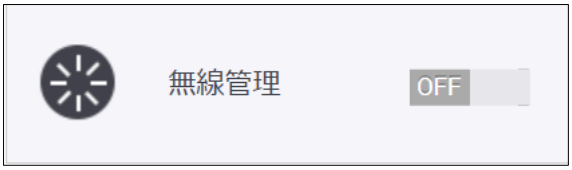
AIRRECT Cloudでのサービス権限の割り当ては、下記の手順で行います。

1. [**管理者**]から、[**ユーザー**]、[**キー**]、または[**プロファイル**]タブをクリックします。

既存のユーザー、キー、またはプロファイルの一覧が表示されます。

2.メニューアイコン⋮をクリックして、[**サービス権限**]を選択します。

3. [**無線管理**]のタイルをクリックします。



4. [**ユーザーロール**]のドロップダウンリストから、割り当てたいロールを選択します。

5. [**許可されたロケーション**]で、役割を割り当てたいロケーションのチェックボックスを選択します。
6. ユーザー用にWi-Fiアクセス管理機能を有効にしたい場合は、[**Wi-Fi アクセス管理**]のチェックボックスを選択します。
7. ユーザー用にWIPS管理機能を有効にしたい場合は、[**WIPS管理**]のチェックボックスを選択します。
8. 役割を割り当てられたユーザーにアクセスを許可するロケーションを、同じ画面上に表示されているロケーションツリーで選択します。
9. [**保存**]をクリックし、そのサービスでの設定を保存します。

3.3.4 パケット解析でのサービス権限割り当て

パケット解析は、キャプチャした802.11ワイヤレスパケットファイルの読取・分析を行うウェブベースのWi-Fiネットワーク・トラブルシューティングツールです。パケットキャプチャファイル内にあるフレーム関連の情報を画像化し、パケットキャプチャの解釈を容易にします。この機能では、UserとViewerという2種類のユーザー役割を定義できます。下記の表で、UserおよびViewerに割り当てできる権限を示します。

機能	User	Viewer
トレースをアップロード	可	不可
トレースを削除	可	不可
ダッシュボードの閲覧	可	可
グラフの閲覧	可	可
共有可能なリンクの作成	可	不可
フィードバックの送信	可	可
LaunchpadにPackets特有の許諾権限を割り当て/割り当て解除	可	不可

パケット解析でのサービス特権の割り当ては、下記の手順で行います。

1. [**管理者**]から、[**ユーザー**]、[**キー**]、または[**プロファイル**]タブをクリックします。既存のユーザー、キー、またはプロファイルの一覧が表示されます。

2.メニューアイコン⋮をクリックして、[**サービス権限**]を選択します

3. [**パケット解析**]のタイルをクリックします。

4. [**ユーザーロール**]ドロップダウンリストから、割り当てたいロールを選択します。

5. [**保存**]をクリックし、そのサービスでの設定を保存します。

3.4 キーの管理

サードパーティ製アプリがLaunchpadサービスから認証を受け、APIコール経由で通信ができるように、キーIDとキー値のペアを生成するものです。これらのキーIDとキー値のペアは、[**キー**]の管理内のサービス権限で管理できます。
※キー検証サービスをサポートするLaunchpadサービスのみ、サードパーティ製アプリからAPIコール経由でアクセスできます。
キーIDとキー値のペアは、ユーザー名とパスワードの組み合わせと同じように、Launchpadサービスへの認証やLaunchpadサービスとの通信に使用できますが、APIコールを通じてのみ使用可能です。キーIDとキー値のペアは、Launchpad UIへのアクセスには使用できません。
ユーザーアカウントと同様に、キーにプロファイルを割り当てることができます。プロファイルについての詳細や、プロファイルによって割り当て可能な権限についての詳細は、『ユーザー定義プロファイルの管理』を参照ください。
ひとつのキーは、キー名、キーID、キー値、そしてプロファイルで構成されます。キー名は、ユーザーが定義するキーを識別するための名称です。キーIDとキー値は、システムによって生成され、サードパーティ製アプリがLaunchpadサービスへアクセスする際に使用されます。また、キーの追加、編集、削除にはキー管理権限が必要です。

注意：管理プロファイル全体で登録できる数は25となっているため、
キーを登録した分だけ、登録できるユーザーアカウント数が減少します。

キー値の閲覧

キー値は、以下の要件を満たすユーザーにのみ表示されます。

●ユーザーのプロファイルがキーのプロファイルと同等またはそれ以上である。
●そのサービスにおいてユーザーの持っている許諾権限がキーの許諾権限と同等またはそれより高い権限である。

キーの追加

キーを追加すると、初期設定ではカスタムプロファイルが割り当てられています。キーを保存後、キーにサービス特権を確実に割り当てる必要があります。キーへのサービス特権割り当ては、ユーザーへのサービス権限割り当てと同様に行うことができます。キーへのサービス特権割り当てについての詳細は『ユーザーのサービス権限の管理』を参照ください。

キーのプロファイルと同様またはそれより高い権限のプロファイルを持つユーザーのみが、キーを編集できます。編集で修正できるのは、キー名とプロファイル名のみです。キーIDは変更できませんが、キー値のリセットはできます。キー値をリセットすると、新たな値が自動生成されます。既存のキーIDとキー値のペアをすでに使用中のアクティブセッションは影響を受けませんが、新たなセッションを始めるためにLaunchpadサービスへアクセスするサードパーティ製アプリは、新たなキーIDとキー値ペアを使用する必要があります。

キー情報の追加は、下記の手順で実行します。

1. [**管理者**]から、[**キー**]タブをクリックします。
2. [**キー追加**]をクリックして、キーを追加します。
3. キー名を入力し、Enterキーを押します。

APIのベースURL

API にてアクセスする設定のベース URL は「Wi-Fi 統合監視」から確認できます。

[**API のベース URL**]を表示するには以下の手順を実行します。

1. [**システム**]>[**詳細設定**]>[**API のベース URL**]の順にクリックします。

2. [**設定と管理**]と[**ゲスト分析**]の URL が表示されます。

3.4.1 キーのロック/ロック解除

キーを定義しているが、Launchpadサービスへのアクセス授与は後で行いたい場合や、すでに有効なキーによるLaunchpadサービスへのアクセスを制限したい場合、または特定のキーを削除せずにブロックしたい場合など、キーをロックすることで、Launchpadサービスへアクセスしないようにできます。
ロックしたキーは、いつでもロック解除できます。キーをロックすると、南京錠のアイコンが表示されます。
キーのロックとロック解除は下記の手順で行います。
1. [**管理者**]から、[**キー**]タブをクリックすると、キーの一覧が表示されます。
2. ロックまたはロック解除したいキーの行のメニューマーク⋮をクリックします。
3. [**ロック/ロック解除**]をクリックします。

キーの検索
キーID、キー名、またはプロファイルからキーを検索できます。検索を行うには、右上にあるユーザー検索ボックスに、検索キーワードをタイプします。 検索キーワードをタイプするごとに、マッチするキーの一覧が表示されます。

キーの削除

キーIDとキー値のペアの削除は、下記の手順で行います。

1. [**管理者**]から、[**キー**]タブをクリックすると、既存キーの一覧が表示されます。
2. 削除したいユーザーの行のメニューマーク⋮をクリックします。
3. 表示されたポップアップメニューで[削除]をクリックすると、削除を確定させるメッセージが表示されます。
4. [**はい**]をクリックして、ユーザーを削除します。

※該当キーのサービスに関連するデータの削除中にLaunchpad上で問題が起こった場合、キーの削除は中断されます。

3.5 設定の管理

設定を管理するには、設定サービス特権が必要です。設定により、ユーザーのLaunchpadへの最大ログイン試行回数を管理できます。また、指定されたログイン試行回数後、ユーザーがLaunchpadからロックアウトされる時間の長さを管理できます。ロックアウト時に表示されるメッセージもここで指定できます。設定で、最低パスワード長も指定できます。

それ以外にも、顧客や組織向けの二要素認証の有効化や強制化も[**設定**]タブから行えます。二要素認証の有効化や強制については、『二要素認証の構成』を参照ください。

グローバル設定の構成や編集は、下記の手順で行います。

1. [**管理者**]から[**設定**]タブをクリックします。

   下記テーブルのアカウントロックアウトポリシーを設定します。

オプション	概要
ログイン試行の最大失敗数	許可される最大ログイン試行回数と、試行を繰り返せる時間の長さ。
アカウントロックアウト期間	指定した時間内に続けてログインに失敗した後、ユーザーがログインできなくなる分単位でのロックアウト期間。
アカウントロックアウト時に表示されるメッセージ	ロックアウト期間中にログインを試行した場合に表示されるメッセージ。

パスワードポリシー

オプション	概要
最小の パスワード 文字数	●パスワードの長さ：最小の長さは8文字です。 ●パスワードの複雑さ：少なくとも1文字以上の小文字英字がパスワードに必要とするにはこのオプションを選択してください。 ●少なくとも1文字以上の数字がパスワードに必要とするにはこのオプションを選択してください。 ●少なくとも1つ以上の特殊記号 (! @ # $ % ^ & * ( ) = + { } : ; < > , ` ~ ? _ | .) がパスワードに必須です。 ●少なくとも1文字以上の大文字英字がパスワードに必須です。 ●ユーザー名と異なるパスワードが必須です。
パスワードの 期限/一意性	●**パスワードの期限を有効にする**：パスワードの期限を設定するにはこのオプションを選択します。最小値は1日です。 ●**ユニークなパスワード制限を有効にする。**：[**パスワードの期限を有効にする**]オプションを選択すると、このオプションも自動的に選択されます。パスワードが最後の[指定の個数]のパスワードと一致しないように指定できます。

※パスワードポリシーの設定は、ユーザーのパスワードの期限が切れた場合、
またはユーザーが既存パスワードを変更した場合に有効になります。

オプトアウト

オプション	概要
Panasonicが管理者として自分のアカウントにアクセスすることを許可しない。	トラブルシュートや技術的問題を解決するために、当社がお客様のアカウントに、管理者権限でアクセスする場合があります。問題解決を迅速に進めるために、初期設定では当社サポートセンターがアクセス可能な設定がされていますが、このオプションを選択することで、当社は管理者権限でお客様のアカウントにアクセスできなくなります。ただし、当社はメンテナンスを目的とした制限付きのアクセス権「Viewer only (閲覧のみ)」を維持します。この制限付きアクセスは、お客様のネットワークにおけるネットワークキー、　パスワード、ワイヤレスユーザーID等が開示されることはありません。

二要素認証

二要素認証は、管理者(Admin)ユーザーが2つの異なる認証情報で認証する方法です。

オプション	概要
二要素認証	二要素認証を有効化する場合に選択します。詳細については『二要素認証の有効化』を参照ください。
二要素認証を強制する	二要素認証を強制する場合に選択します。詳細については『二要素認証の強制』を参照ください。

ログインを許可されたIPv4アドレス

管理者ユーザーは、Launchpadや他サービスへのアクセスを、ユーザーセッションのIPアドレスに応じて制限できます。利用可能なオプションは以下のとおりです。

注意：グローバルIPアドレスのみ制限可能です。ローカルIPアドレスの制限はできません。

●**[特定のIPアドレス]**：Launchpadへのログインとアクセスが許可されるIPv4アドレスのリストを入力するにはこのオプションを選択します。IPアドレスを許可済みIPアドレスのリストに追加するには、IPアドレスを入力し、**[追加]**をクリックします。このリストに記載のあるIPアドレスから発生するユーザーセッションのみ、アクセスが許可されます。

●**[IPアドレスの範囲]**：Launchpadへのログインとアクセスが許可されるIPアドレスの範囲を入力するにはこのオプションを選択します。IPアドレス範囲を許可済みIPアドレスのリストに追加するには、先頭および終端のIPアドレスを入力し、**[追加]**をクリックします。この範囲内のIPアドレスから発生するユーザーセッションのみ、アクセスが許可されます。

注意：IPアドレス、IPアドレス範囲の登録数の上限は25です。

●**[ユーザーがログインするIPアドレスにセッション制限します。]**：特定のIPアドレスにユーザーセッションを制限するにはこのオプションを選択します。ユーザーが一度Launchpadへログインすると、AIRRECT Launchpadまたはその他サービスへアクセスするユーザーセッションが、ユーザーがログインしたIPアドレスからのものに限定されます。ユーザーセッションの発生元であるIPアドレスが変更されると、ユーザーは一度ログアウトし再度ログインするよう促されます。

※現在IPアドレスは、Launchpadから発生するアクションでのみ検証されています。

●**[同じユーザーアカウントからの同時ログインを防止します。]**：同じユーザーが同じ情報を使って二重にログインするのを防ぐために、ログイン済みのユーザーからのアクセスを拒否するには、このオプションを選択します。このオプションが設定されると、ユーザーは同時に2つ以上のアクティブセッションを持つことができません。

※これらの設定を有効化する間、すでにアクティブなユーザーセッションは、これらの変更の影響を受けません。

3.5.1 二要素認証の構成

二要素認証は、ユーザーが2つの異なる認証情報で認証されるという認証手順です。
Launchpadでは、パスワードとユーザー名の組合せとユーザーアカウント用のワンタイムパスワードがサポートされます。ワンタイムパスワードは、Google認証やAuthyといったタイムベースのワンタイムパスワード生成アプリケーションで生成できます。スマートフォンやタブレット端末が利用できない場合は、ワンタイムパスワードを電子メールでEメールIDへ送信できます。
ユーザーは、パスワードとユーザー名の組合せとワンタイムパスワードとの両方が、そのユーザーの設定値と一致してはじめてLaunchpadにログインできます。
Adminの役割または権限を持つユーザーが、二要素認証を有効化または強制できます。
Launchpadでは、組織がそのユーザーに対し、二要素認証を有効化または強制できるようになっています。二要素認証が有効の場合、Adminユーザーの決定により、Launchpadへアクセスする際の二要素認証を一部またはすべてのユーザーに対して有効化できます。二要素認証が強制されると、組織の全ユーザーがLaunchpadを使ったLaunchpadサービスへのログイン時に二要素認証を使用する必要があります。
Launchpadで二要素認証を実行する手順は以下の通りです。

1. Adminユーザーが二要素認証を有効化または二要素認証を強制します。
2. Launchpadへのログイン時に、ユーザーはそれぞれ自身のワンタイムパスワードを生成します。ワンタイムパスワードは、Google認証などのタイムベースのワンタイムパスワード生成アプリケーションを使って生成できます。またはLaunchpadを使って生成し、電子メールでユーザーに届けることができます。アカウントに電子メールでワンタイムパスワードを届けるには、ログインページで、Eメールで届けるためのリンクをクリックする必要があります。

二要素認証の有効化

Adminユーザーとして、カスタマーレベルでの二要素認証を有効化できます。カスタマーレベルで二要素認証が有効化されると、各ユーザーにとっては二要素認証がオプションとなります。カスタマーレベルで二要素認証が有効化された後、Launchpadで二要素認証ログインをさせたいユーザーに二要素認証を有効化する必要があります。
二要素認証を有効化するには、下記の手順で行います。

1. [**管理者**]>[**設定**]をクリックします。
2. [**二要素認証**]のチェックボックスを選択します。
3. [**保存**]をクリックします。

二要素認証の強制

Adminユーザーとして、カスタマーレベルでの二要素認証を強制できます。カスタマーレベルで二要素認証を強制している場合、そのカスタマーのすべてのローカルユーザーにおいてLaunchpadへ二要素認証ログインが必須となります。二要素認証を強制するには、カスタマーにおいて二要素認証を有効化しておくことが必要です。二要素認証を強制すると、自動的にそのカスタマーのすべてのローカルユーザーに対して有効化および強制されます。

カスタマーレベルでの二要素認証の強制は、下記の手順で行います。

1. [**管理者**]>[**設定**]をクリックします。
2. [**二要素認証**]のチェックボックスを選択します。
3. [**二要素認証を強制する**]のチェックボックスを選択します。
4. [**保存**]をクリックします。

二要素認証をカスタマーレベルで強制すると、その配下のすべてのローカルユーザーは二要素認証を使ってLaunchpadに認証されるよう強制されます。初めてのログインでは、各ユーザーはEメール IDに届けられたワンタイムパスワードを使って認証されます。その後、ユーザーはタイムベースのワンタイムパスワード生成アプリケーションを使ってワンタイムパスワードを生成することもできます。この設定は、ユーザーが自らのアカウント設定で行います。詳細については『自身のアカウント設定の管理』を参照ください。

3.5.2 自身のアカウント設定の管理

姓、名、パスワード、タイムゾーン、二要素認証といった自身のLaunchpadアカウント設定を管理できます。自身のアカウント設定を管理するには、自身のユーザー情報でログインする必要があります。アカウント設定での変更は、次回ログイン時に適用されます。

個人情報/パスワードの管理

姓、名、タイムゾーンなどの個人情報やパスワードは何度でも変更できます。パスワードの変更はローカルユーザーのみが行えます。

注意：Eメール IDは変更することができません。

名前の変更は、下記の手順で行います。

1. Launchpadにログインします。
2. 画面右上の自身のユーザー名をクリックします。
3. [**アカウント設定**]のリンクをクリックします。
4. 必要な情報を修正します。
5. [**保存**]をクリックします。

二要素認証の管理

二要素認証の管理はローカルユーザーのみが行えます。

二要素認証が組織レベルで有効化されている場合、ログイン時の二要素認証を有効化できます。有効化した後、新たなキーを自身で生成できます。生成したキーは、二要素目の認証に使用できます。新たなキーを生成すると、キーとQRコードが生成されます。このキーを使用するか、Google認証やAuthyといったタイムベースのワンタイムパスワード生成アプリケーションでそのQRコードをスキャンできます。Google認証やAuthyは、スマートフォンにインストールできます。Google認証やAuthyでは、定期的にワンタイムパスワードが生成されます。そのパスワードを、Launchpadへのログイン時の二要素目の認証として使用できます。

ワンタイムパスワードを生成する前に、ご使用のスマートフォンの日時をインターネット経由でアップデートしておく必要があります。

キー生成用アプリケーションを使いたくない場合は、Launchpadでワンタイムパスワードを生成し、それをEメールIDに送信する方法もあります。

二要素認証の管理は、下記の手順で行います。

1. Launchpadにログインします。
2. 画面右上にある自身のユーザー名をクリックします。
3. [**アカウント設定**]のリンクをクリックします。
4. 二要素認証の下にある[**有効**]のチェックボックスを選択します。
5. Google認証やAuthyでQRコードをスキャンします。Google認証アプリでワンタイムパスワードが生成されます。
6. Google認証で生成されたワンタイムパスワードを、二要素認証の下にあるワンタイムパスワードに入力します。
7. 現在のパスワードを入力します。
8. [**保存**]をクリックします。ここで入力されたワンタイムパスワードを、Launchpadへの次回ログイン時の二要素目の認証として使用できます。

3.6 ユーザーアクションログ

Launchpadでは、ユーザーのアクションログが記録されており、csvファイル形式でダウンロードすることができます。ユーザーアクションログの日時は、ユーザーのタイムゾーンに依存します。また、ユーザーアクションログを削除することもできます。
ユーザーアクションログは以下のいずれかの方法でダウンロードできます。
●指定の日付範囲でダウンロード
●数時間、数日、または数か月前にさかのぼってダウンロード
csvファイルには、以下のようなパラメータが表示されます。

パラメータ	概要
Date	ユーザーアクションが発生した日時
Host Adress	ユーザーのログイン元であるクライアントのIPアドレス
Login Name	アクションのあったカスタマー名
Type	Access,Settingなどのユーザーアクションタイプ
Message	ユーザーのアクション内容詳細

ユーザーアクションログのダウンロードは、以下の手順で行います。

1. [**管理者**]から[**ログ**]タブをクリックします。
2. 以下のいずれかの方法で、ユーザーアクションログの出力範囲を選択します。
   a) 上のfrom - toのチェックボックスを選択し、いつからいつまでの日時のユーザーアクションログをダウンロードするか指定します。
   b) 過去数時間、数日、または数か月分のユーザーアクションログをダウンロードしたい場合は、下のチェックボックスを選択したあと、時間/日/月の数値（幅）を指定し、プルダウンメニューから時間/日/月のいずれかを選択します。

3. [**ダウンロード**]をクリックします。

注意：csvファイルは文字コードUTF-8で保存されます。

ユーザーアクションログの削除

画面右上のごみ箱アイコンをクリックすることで、ユーザーアクションログを削除できます。削除には、User Management以上の権限が必要です。ログは1か月間保存されます。その後、ログを削除するまでの期間を選択することができます。

ユーザーアクションログの削除の手順は以下のとおりです。

1. **画面右上のごみ箱**アイコンをクリックすると、ログを削除したい期間を問われます。
2. [**以前のｘ月**]で月数を選択し、[**適用**]をクリックします。またはすべてのログを削除したい場合は、[**すべて削除**]をクリックし、ログをすべて削除します。

3.7 権限レポート

ユーザー権限レポート

Launchpadでは、以下のユーザー権限に関するレポート生成が可能です。

●各ユーザーに割り当てられた個々のサービス、および各サービスにおいて割り当てられた役割についての詳細情報

●ユーザーに割り当てられているサービスがロックされているか、または利用可能かの状態表示

●該当ユーザーのプロファイル名とタイムゾーン名

レポート生成には、選択カスタマーのManagement許諾権限が必要です。

ユーザー権限レポートの生成は、下記の手順で行います。

1. [**管理者**]から[**ユーザー**]タブをクリックします。
2. ページ右上にあるユーザー権限レポートのアイコンをクリックします。
   ユーザー権限レポートが、HTML形式で生成されます。

キー権限レポート

Launchpadでは、サービスまたはカスタマーごとのキー権限について以下のような詳細レポートを得ることができます。

●選択した顧客のすべてのサービスにおけるプロファイルと許諾権限情報

●各キーに割り当てられている個々のサービス機能の詳細

●キーに割り当てられているサービスがロックされているか、利用可能かの状態表示

●キー名、キーID、およびプロファイル名が示されます。

キー権限レポートは、選択したカスタマーごとに生成されます。カスタマーツリーのルート部分を選択しレポートを生成すると、そこで作成されたキーに関連するサービスが、レポートに含まれます。

※キー検証サービスをサポートしているAIRRECTサービスのみが、キー権限レポートに掲載されます。また、キー権限レポートの生成には、選択したカスタマーのManagement許諾権限が必要です。

キー権限レポートの生成は、下記の手順で行います。

1. [**管理者**]から[**キー**]タブをクリックします。
2. ページ右上にあるキー権限レポートのアイコンをクリックします。

キー権限レポートが、HTML形式で生成されます。

プロファイル権限レポート

Launchpadでは、サービスまたはカスタマーごとのプロファイル権限について以下のような詳細レポートを得ることができます。

●選択したカスタマーのユーザー定義プロファイルと、すべてのサービスに対してそのカスタマーが持つ権限の情報

●各プロファイルに割り当てられている、個々のサービス機能の詳細情報

●プロファイルに割り当てられているサービスがロックされているか、利用可能かの状態表示

●割り当てられているユーザーやキーの数が記載されます。

プロファイル権限レポートの生成

プロファイル権限レポートの生成には、選択したカスタマーのUser ManagementまたはKey Management権限が必要です。

プロファイル権限レポートの生成は、下記の手順で行います。

1. [**管理者**]から[**プロファイル**]タブをクリックします。
2. ページ右上にあるプロファイル権限レポートのアイコンをクリックします。

   プロファイル権限レポートが、HTML形式で生成されます。

3.8 Wi-Fi統合監視の初期値一覧

ライセンス購入時に、Wi-Fi 統合監視ツールに設定されている初期値を以下に示します。

■構成＞WiFi 設定

項目	設定内容	初期値
SSID 設定（初期状態では SSID は未作成。以下、SSID 作成時の初期値）		
基本	SSID タイプ	プライベート
	SSID を非表示	無効
セキュリティ	セキュリティレベル	オープン
ネットワーク	VLAN ID	0(Untag)
	ネットワークモード	ブリッジ
	AP 間コーディネーション	付近の RF
	SSID VLAN でクライアントアソシエーションをアドバタイズ	有効
	DHCP オプション 82	無効
アクセス制御	クライアント認証	無効
	ロールベースの制御	無効
	DHCP フィンガープリント・ベースのアクセス制御	無効
	Bonjour ゲートウェイ	無効
	リダイレクト	無効
	許可リクエストおよび拒否リストの Wi-Fi クライアント	無効
	クライアント分離	無効
アナリティクス	アソシエーション	無効
	アプリケーションの可能性	有効
	アプリケーション QoE 監視	有効
	分析結果をサードパーティーサーバーにプッシュ	無効
キャプティブポータル	キャプティブポータル	無効

項目	設定内容	初期値
SSID 設定（初期状態では SSID は未作成。以下、SSID 作成時の初期値）		
RF 最適化	スマートクライアントのロードバランシング	無効
	スマートステアリング	無効
	最小 RSSI ベースのアソシエーション	無効
	バンドステアリング	有効
	ステアリングを強制	有効
	付近の 802.11k リスト	無効
	802.11v　BBS 移行	無効
	ブロードキャスト/マルチキャスト制御	無効
	IGMP スヌーピング	有効
	スヌーピングのタイムアウト	5 分
	マルチキャストをユニキャストに変換	無効
SSID スケジューリング	タイムスロットを選択	無効
トラフィックシェーピングと QoS	同時アソシエーションの最大数を次に制限	無効
	SSID の最大アップロード帯域幅を次に制限	無効
	SSID の最大ダウンロード帯域幅を次に制限	無効
	ユーザー一人当たりの最大アップロード帯域幅を次に制限	無効
	ユーザー一人当たりの最大ダウンロード帯域幅を次に制限	無効
	QoS	有効
	WMM 受付制御を強制	無効
	SSID 優先度	音声
	優先度のタイプ	上限
	ダウンロードストリームマッピング	DSCP
	802.1p マーキング	有効
	DSCP/TOS マーキング	無効
	マルチキャスト、ブロードキャスト、管理トラフィックのデータレートを次に設定	6Mbps
	最大ユニキャスト・トラフィック・データ・レートを制限	無効
	最小ユニキャスト・トラフィック・データ・レートを制限	無効
	802.11n 以上を含むすべてのクライアントに適用	無効

項目	設定内容	初期値
無線接続設定（2.4GHz）		
チャネル設定	チャネル選択	自動
	候補チャネル	1,5,9,13
	選択モード	スケジュール
	セカンド ACS タイムスロット	無効
	ファーストタイムスロット（HH:MM）	04:00
	動的チャネル選択	無効
機能	プロトコル	802.11ax
	チャネル幅	20/40MHz
	ガード・インターバル	0.8 マイクロ秒
802.11ax の機能強化	ダウンリンクの MU-MIMO	有効
	アップリンクの MU-MIMO	有効
	ダウンリンクの OFDMA	有効
	アップリンクの OFDMA	有効
	BSS カラー	有効
	Spatial Reuse (SR)	無効
送信電力選択	送信電力選択	自動
	ラウドネス RSSI	-75dBm
	ネイバー数	3
	最小 EIRP	8dBm
	最大 EIRP ※電波法の最大値に制限されます。	36dBm
	外部アンテナを使用する	無効
スマートステアリング	ローミング開始間隔	10 秒
	ローミング開始パケットのしきい値	5 パケット
スマートクライアントのロードバランシング	最小クライアント負荷	30 クライアント
	最小クライアントの負荷の差	5 クライアント
バンドステアリング	バンドステアリングクライアント負荷の差	25 クライアント
WMM 受付制御ポリシー	受付制御必須	無効
フレームアグリゲーション	A-MSDU	有効
	A-MPDU	有効
無線通信詳細設定	RTS のしきい値	2347
	DTIM 期間	1 ビーコン
	同期間隔	10 秒

項目	設定内容	初期値
無線接続設定（5GHz）		
チャネル設定	チャネル選択	自動
	候補チャネル	すべての非 DFS チャネル、36、40、44、48
	選択モード	スケジュール
	セカンド ACS タイムスロット	無効
	ファーストタイムスロット（HH:MM）	04:00
	動的チャネル選択	無効
	チャネル選択で DFS 履歴を使用	無効
機能	プロトコル	802.11ax
	チャネル幅	20/40MHz
	ガード・インターバル	0.8 マイクロ秒
802.11ax の機能強化	ダウンリンクの MU-MIMO	有効
	アップリンクの MU-MIMO	有効
	ダウンリンクの OFDMA	有効
	アップリンクの OFDMA	有効
	BSS カラー	有効
	Spatial Reuse (SR)	無効
送信電力選択	送信電力選択	自動
	ラウドネス RSSI	-75dBm
	ネイバー数	3
	最小 EIRP	12dBm
	最大 EIRP ※電波法の最大値に制限されます。	36dBm
	外部アンテナを使用する	無効
スマートステアリング	ローミング開始間隔	10 秒
	ローミング開始パケットのしきい値	5 パケット
スマートクライアントのロードバランシング	最小クライアント負荷	30 クライアント
	最小クライアントの負荷の差	5 クライアント
WMM 受付制御ポリシー	受付制御必須	無効
フレームアグリゲーション	A-MSDU	有効
	A-MPDU	有効
無線通信詳細設定	RTS のしきい値	2347
	DTIM 期間	1 ビーコン

項目	設定内容	初期値
無線接続設定（6GHz）		
チャネル設定	チャネル選択	自動
	候補チャネル（UNII - 5）	すべてのチャネル、1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93
	選択モード	スケジュール
	セカンド ACS タイムスロット	無効
	ファーストタイムスロット（HH:MM）	04:00
	動的チャネル選択	無効
機能	プロトコル	802.11ax
	チャネル幅	20/40/80MHz
	ガード・インターバル	0.8 マイクロ秒
802.11ax の機能強化	ダウンリンクの MU-MIMO	有効
	アップリンクの MU-MIMO	有効
	ダウンリンクの OFDMA	有効
	アップリンクの OFDMA	有効
	BSS カラー	有効
	Spatial Reuse (SR)	無効
送信電力選択	送信電力選択	自動
	ラウドネス RSSI	-75dBm
	ネイバー数	3
	最小 EIRP	12dBm
	最大 EIRP ※電波法の最大値に制限されます。	36dBm
	外部アンテナを使用する	無効
スマートステアリング	ローミング開始間隔	10 秒
	ローミング開始パケットのしきい値	5 パケット
スマートクライアントのロードバランシング	最小クライアント負荷	30 クライアント
	最小クライアントの負荷の差	5 クライアント
WMM 受付制御ポリシー	受付制御必須	無効

項目	設定内容	初期値
無線接続設定（6GHz）		
フレームアグリゲーション	A-MSDU	有効
	A-MPDU	有効
無線通信詳細設定	RTS のしきい値	2347
	DTIM 期間	1 ビーコン

項目	設定内容	初期値
無線接続設定（共通）		
クライアントステアリングの共通パラメーター	ステアリング RSSI	-70dBm
	最大ステアリング試行回数	2
	ステアリングブラックアウト期間	15 分
	クライアントステアリングのアクセスポイント同期	有効
	同期間隔	10 秒

■構成＞デバイス設定

項目	設定内容	初期値
デバイス設定		
デバイス	アクセスポイントを専用 WIPS センサーに変換	無効
	バックグラウンドスキャン	通常
	WiFi スキャンの長さ	100 ミリ秒
	WiFi アクセスの長さ	60 秒
	WiFi セキュリティ機能	無効
	クライアント RSSI の更新間隔	60 秒
	VLAN 拡張機能	無効
	リンクアグリゲーション	無効
	ユーザー名　※変更不可	config
	パスワード	ランダムな英数字 ※クラウド接続前は config
	デバイスログを Syslog サーバーに送信	無効
	SSH バナーを表示	無効
	SSH アイドル・タイムアウト	有効、5 分
	IPv4/IPv6 デュアルスタック	有効
	SSH IP 許可リストの有効化	無効
	LED の無効化	無効
	縮小機能の LED 表示を無効化する	無効
	可視性分析をサードパーティ・サーバーにプッシュ	無効
	周波数帯を選択	2.4Hz
	アクセスと WIPS センサーモードの両方を有効化	無効
	アンテナ設定タイプを選択	内蔵

項目	設定内容	初期値
セキュリティ		
VLAN モニタリング	SSID VLAN モニタリング	有効
	VLAN 自動モニタリング	無効
	監視する VLAN を追加	無効
オフラインモード	オフラインモード	有効
	デバイスが接続の喪失を検出した後にオフラインモードに切り替える時間	15 分
デバイス分類ポリシー	ネットワーク接続された AP を次として分類	無効、ローグ
	ネットワーク接続されていない AP を「外部」として分類	有効
	認定 AP とアソシエートされているクライアントを「認定」として分類	無効
	ローグ AP とアソシエートされているクライアントを「不正」として分類	有効
	外部 AP とアソシエートされているクライアントを「不正」として分類	有効
侵入防止ポリシー	侵入防止レベル	デグレード
	ローグ AP	無効
	ネットワークに接続されている未分類ＡＰ	無効
	「認定」と分類されているが、セキュリティ対策を施していないＡＰ（Open）	無効
	「認定」と分類されているが、弱いセキュリティ対策を施していないＡＰ（WEP）	無効
	「外部」と分類された AP への認定クライアント接続	無効
	「認定」と分類された AP への不正クライアント接続	無効
	「認定」と分類された AP への未分類クライアント接続	無効
	アドホック・ネットワークに参加する認定クライアント	無効
	ハニーポット/Evil Twin AP	無効

項目	設定内容	初期値
セキュリティ		
チャネル設定【監視するチャネル】	2.4GHz	1~14
	5 GHz	34,36,38,40,42,44,46,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144,149,153,157,161,165,208,212,216
	6 GHz（UNII - 5）	1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93
	6 GHz（UNII - 6）	97,101,105,109,113
	6 GHz（UNII - 7）	117,121,125,129,133,137,141,145,149,153,157,161,165,169,173,177,181,185
	6 GHz（UNII - 8）	189,193,197,201,205,209,213,217,211,225,229,233

項目	設定内容	初期値
セキュリティ		
チャネル設定【防御するチャネル】	2.4GHz	1~13
	5GHz	36,40,44,46,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144,
	6GHz（UNII - 5）	1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93

■構成＞アラート

アラートのアクティブ化		
有効		
項目	設定内容	初期値
アラートを設定		
WiFi	接続	無効
	パフォーマンス	無効
	ベースライン	無効
	クライアント接続テスト	無効
システム＞ サーバー	サーバーが起動しました	●表示 ●重要度　低
	サーバーが停止しました	●表示 ●通知 ●セキュリティ・ステータスに影響する ●重要度　高
	データベース・バックアップ結果	●表示 ●重要度　高
	データベース復元結果	●表示 ●重要度　高
	自動削除が実行されました	●表示 ●重要度　低
	デバイス接続が拒否されました。ライセンス数の制限に達しました。	●表示 ●通知 ●重要度　低
	非アクティブなクライアントが検出されました	●表示 ●重大度　中
システム＞ デバイス	CPU 使用率が越えています	●表示 ●メール ●通知 ●重大度　高
	メモリ使用率が越えています	●表示 ●メール ●通知 ●重大度　高
	サーバーがアクセス・ポイントに少なくとも到達できていない時間設定	●表示 ●メール ●重大度　高

項目	設定内容	初期値
アラートを設定		
システム＞ デバイス	ファームウェア・アップデートが失敗したアクセス・ポイントの数の基準設定	●表示 ●メール ●重大度　高
	認可された AP が非アクティブです	無効
	認定 AP がネットワークから切断されました	無効
	新しいネットワークが検出されました	●表示 ●通知 ●重大度　高
	互換性のないバージョンが AP に検出されました	●表示 ●通知 ●重大度　中
	管理対象 WiFi デバイスの認証が失敗しました。	●表示 ●通知 ●セキュリティ・ステータスに影響する ●重大度　高
	デバイスがフェイルセーフ・モードで動作しています。	●表示 ●メール ●通知 ●重大度　高
	新しいデバイスがサーバーに接続しました	●表示 ●メール ●通知 ●重大度　低
	デバイスがサーバーから切断されました	●表示 ●通知 ●セキュリティ・ステータスに影響する ●重大度　高
	古いファームウェア・バージョンのデバイスが検出されました。	●表示 ●通知 ●セキュリティ・ステータスに影響する ●重大度　中

項目	設定内容	初期値
アラートを設定		
システム＞ デバイス	デバイスのファームウェア・アップデートが失敗しました。	●表示 ●通知 ●重大度　中
	デバイスのファームウェア・バージョンを使用できません	●表示 ●通知 ●重大度　中
	トンネル・エンドポイントが切り替わりました	●表示 ●メール ●通知 ●重大度　高
	トンネル・エンドポイントがダウンしています（13.0 より前の AP ビルドに適用）	●表示 ●メール ●通知 ●重大度　高
	トンネルエンドポイントが理由によりダウンしました（AP ビルド 13.0 以降に適用）	●表示 ●メール ●通知 ●重大度　高
	RADIUS サーバーが応答していません。	●表示 ●メール ●通知 ●重大度　高
	認証 RADIUS サーバーが切り替わりました。	●表示 ●メール ●通知 ●重大度　高
	ネットワーク・プロファイルに関してアップしている VAP	●表示 ●メール ●通知 ●重大度　高
	ネットワーク・プロファイルに関してダウンしている VAP	●表示 ●メール ●通知 ●重大度　高

項目	設定内容	初期値
アラートを設定		
システム＞ デバイス	アクセス・ポイントの再起動	●表示 ●通知 ●重大度　高
	VLAN の最大上限に達しました	●表示 ●メール ●通知 ●重大度　高
	アクセスポイントのアップリンクポートの認証に失敗しました	●表示 ●メール ●通知 ●重大度　高
	ローカル認証	●表示 ●重大度　中
	非準拠のファームウェアバージョンのアクセスポイントが検出されました	●表示 ●メール ●通知 ●セキュリティ・ステータスに影響する ●重大度　高
WIPS> ローグ AP	不正 AP が許可されていないチャンネルで動作しています	●表示 ●重大度　低
	禁止 AP がアクティブです	●表示 ●メール ●通知 ●セキュリティ・ステータスに影響する ●重大度　高
	ローグ AP がアクティブです	●表示 ●メール ●通知 ●セキュリティ・ステータスに影響する ●重大度　高
	オフラインモード：ローグ AP が検出されました	●表示 ●重大度　低
	不確定 AP がアクティブです	無効

項目	設定内容	初期値
アラートを設定		
WIPS>誤認定 AP	認定 AP が許可されていないチャンネルで動作しています	●表示 ●重大度　低
	誤設定されている認定 AP がアクティブです	●表示 ●メール ●通知 ●セキュリティ・ステータスに影響する ●重大度　低
	WDS モードの認定 AP	無効
	認定されている可能性がある AP がアクティブです	●表示 ●重大度　中
WIPS>誤動作クライアント	オフラインモード: 認定クライアントとローグ AP のアソシエーションが検出されました	●表示 ●重大度　低
	オフラインモード: 認定クライアントと外部 AP のアソシエーションが検出されました	●表示 ●重大度　低
	オフラインモード: 認定クライアントとハニーポット AP のアソシエーションが検出されました	●表示 ●重大度　低
	オフラインモード: 不正/未分類クライアントと認定 AP とのアソシエーションが検出されました	●表示 ●重大度　低
	オフラインモード: 不正/未分類クライアントとローグ AP とのアソシエーションが検出されました	●表示 ●重大度　低
	オフラインモード: ソフト AP が検出されました	無効
	認定 AP のゲスト SSID への認定クライアント接続	●表示 ●重大度　中
	禁止クライアントがアクティブです	●表示 ●メール ●通知 ●セキュリティ・ステータスに影響する ●重大度　高

項目	設定内容	初期値
アラートを設定		
WIPS>誤動作クライアント	ブリッジング/ICS 構成のクライアント	●表示 ●メール ●通知 ●セキュリティ・ステータスに影響する ●重大度　中
	ローグ・クライアントがアクティブです	●表示 ●メール ●通知 ●セキュリティ・ステータスに影響する ●重大度　高
	ゲスト・クライアントの誤アソシエーション	無効
	ゲスト SSID への不正クライアント接続	無効
	認定クライアントの誤アソシエーション	●表示 ●通知 ●セキュリティ・ステータスに影響する ●重大度　高
	ソフト・モバイル・ホットスポット AP または Windows 7 の仮想 AP がアクティブです	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
	クライアントが非準拠の認証タイプを使用して認証されました	●表示 ●重大度　高
	認定アクセスポイントへの不正クライアント接続	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
WIPS>中間者攻撃	ハニーポット/Evil Twin がアクティブです	●表示 ●メール ●セキュリティ・ステータスに影響する ●重大度　高

項目	設定内容	初期値
アラートを設定		
WIPS>中間者攻撃	ハニーポット/Evil Twin がアクティブです	●表示 ●メール ●セキュリティ・ステータスに影響する ●重大度　高
	オフラインモード: ハニーポット AP が検出されました	●表示 ●重大度　低
	PS-Poll 攻撃が進行中です	無効
WIPS>アドホック・ネットワーク	オフラインモード: 認定クライアントがアドホック接続モードで検出されました	●表示 ●重大度　低
	認定クライアントがアドホック・ネットワークに参加しています	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
WIPS>防止	AP が最大防止キャパシティに達しました。	●表示 ●重大度　中
	AP を防止する必要があります	●表示 ●重大度　高
	クライアントを防止する必要があります	●表示 ●重大度　高
WIPS>DoS	オフラインモード: DoS 攻撃が検出されました	●表示 ●重大度　低
	アソシエーション解除フラッド攻撃が進行中です	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
	アソシエーション解除ブロードキャスト攻撃が進行中です	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
	偽クライアントが検出されました	無効
	認証解除フラッド攻撃が進行中です	●表示 ●セキュリティ・ステータスに影響する ●重大度　高

項目	設定内容	初期値
アラートを設定		
WIPS>DoS	認証解除ブロードキャスト攻撃が進行中です	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
	認証フラッド攻撃が進行中です	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
	EAPOL Logoff フラッド攻撃が進行中です	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
	EAPOL Start フラッド攻撃が進行中です	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
	Premature EAP Success 攻撃が進行中です	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
	Premature EAP Failure 攻撃が進行中です	●表示 ●セキュリティ・ステータスに影響する ●重大度　高
	偽 AP が検出されました	無効
	RTS/CTS フラッド	無効
WIPS>探索	過度の NULL プローブが検出されました	無効
自動削除		
サーバ上に保存するアラート数	セキュリティ・アラート数	50000
	システムアラート数	1000
アラートをサーバー上に保存する期間		30 日間
E メールの受信者		
設定なし		

■構成＞WIPS

項目	設定内容	初期値
アクセス・ポイントの自動分類		
外部アクセス・ポイント	未分類リストの外部の可能性がある AP を「外部」として自動的に分類（推奨）	有効
ローグ・アクセス・ポイント	未分類リストのローグの可能性がある AP を「ローグ」として自動的に分類（推奨）	有効
クライアントの自動分類		
初期クライアント分類	このロケーションで新たに検出されたクライアントを自動的に分類	無効
認定アクセス・ポイントに接続せいているクライアント	未分類クライアントを分類	有効 (認定)
	外部クライアントを再分類	無効
	ゲスト・クライアントを再分類	無効
	誤設定されている認定アクセスポイントに接続せいているクライアント	有効
	有線ネットワークに接続されていないアクセスポイントを接続しているクライアント	無効
ローグ・アクセス・ポイントに接続せいているクライアント	ローグ・アクセス・ポイントに接続する認定クライアント以外のクライアントを「ローグ」として再分類する	有効
	ローグの可能性があるアクセス・ポイントに接続する認定クライアント以外のクライアントを「ローグ」として再分類する	有効

項目	設定内容	初期値
クライアントの自動分類		
ゲスト SSID に接続しているクライアント	外部クライアントを「ゲスト」として再分類する	有効
	未分類クライアントを「ゲスト」として再分類する	有効
	誤設定されているゲストアクセスポイントに接続しています	有効
	有線ネットワークに接続されていないアクセスポイントと接続しているクライアント	無効
外部アクセス・ポイントに接続しているクライアント	外部アクセス・ポイントに接続するすべての未分類クライアントが「外部」として分類されます	有効
	外部の可能性があるアクセス・ポイントに接続するすべての未分類クライアントが「外部」として分類されます	無効
	外部アクセス・ポイントに接続するすべてのゲスト・クライアントが「外部」として分類されます	無効
	外部の可能性があるアクセス・ポイントに接続するすべてのゲスト・クライアントが「外部」として分類されます	無効
コーポレート・ネットワークへのブリッジング	有線ネットワークに WiFi をブリッジングしている場合、認定以外のクライアントを「ローグ」として再分類します。	有効
	RSSI ベースのクライアント分類	無効
自動侵入防止		
自動侵入防止		無効
自動侵入防止レベル	現在の侵入防止レベル	中断
アクセス・ポイントの防止	ローグ・アクセス・ポイント	有効
	誤設定されている認定アクセス・ポイント	有効
	ローグの可能性があるアクセス・ポイント	無効
	認定されている可能性があるアクセス・ポイント	有効
	不確定アクセス・ポイント	無効
	禁止アクセス・ポイント	有効
認定クライアントの誤アソシエーション	ゲスト SSID	無効
	外部または外部の可能性があるアクセス・ポイント	有効
	不確定アクセス・ポイント	有効
	拒否 SSID	有効
ゲスト・クライアントの誤アソシエーション	外部または外部の可能性があるアクセス・ポイント	無効
	不確定アクセス・ポイント	無効

項目	設定内容	初期値
クライアントの自動分類		
認定アクセスポイントへの不正アソシエーション	認定アクセスポイントへの不正クライアント接続	無効
ゲスト SSID への不正アソシエーション	ゲストアクセスポイントへのローグクライアント接続	有効
	ゲストアクセスポイントへの未分類クライアント接続	無効
	ゲストアクセスポイントへの外部クライアント接続	無効
禁止クライアント	認定またはゲストアクセスポイント	有効
	不確定アクセスポイント	無効
ローグ・クライアント	接続を許可していないネットワークにあるアクセスポイントへのクライアント接続	無効
（クライアントのすべての接続での）クライアントのブリッジング/ICS	ブリッジング/ICS 構成の認定クライアント	有効
	ブリッジング/ICS 構成のゲスト・クライアント	無効
	ブリッジング/ICS 構成のローグ・クライアント	有効
	ブリッジング/ICS 構成の外部/未分類クライアント	無効
	エンタープライズ・モニタリング・サブネットに接続しているブリッジング/ICS クライアント	有効
アドホック接続	アドホック・ネットワークに参加している認定クライアント	有効
	アドホック・ネットワークに参加しているゲスト・クライアント	無効
	アドホック・ネットワークに参加しているローグ・クライアント	無効
MAC スプーフィング	認定アクセス・ポイントの MAC アドレスのスプーフィング	無効
ハニーポット/Evil Twin アクセス・ポイント	ハニーポット/Evil Twin アクセス・ポイントに接続している認定クライアント	有効
サービス拒否（DoS）攻撃	WiFi サービス拒否（DoS）攻撃	無効

項目	設定内容	初期値
認定 WiFi ポリシー		
ロケーションで設定した SSID 以外の無線通信を誤設定アクセスポイントに分類する		有効
詳細設定 (アクセスポイントの事前分類)	モニタリング対象サブネットに接続するアクセス・ポイントを「認定の可能性がある」または「ローグ」として事前分類します。	有効
	信号強度がしきい値より大きいアクセス・ポイントを「認定の可能性がある」または「ローグ」として事前分類します。	無効
認定 WiFi プロファイル		無効

■システム＞監査ログ

項目	初期値
監査ログポリシー	
ユーザーアクションの保存期間	7 日

4. Wi-Fi簡易設定

Wi-Fi 簡易設定は、SSID 設定やキャプティブポータルなどの代表的な設定を簡易的に行うことができるアプリケーションです。スマートフォンに最適化した画像デザインとなっているため、パソコンから操作ができない場合や、簡易的な設定を行いたい場合に最適です。管理しているアクセスポイントやクライアントの状況確認や、ゲスト Wi-Fi を使った分析機能による簡易的なマーケティング調査も可能です。分析機能に関しては、Wi-Fi 簡易設定からのみ閲覧が可能です。Wi-Fi 簡易設定は「Wi-Fi 統合管理」の簡易版となっており、互いで行った設定は連動します。

Wi-Fi簡易設定は [**ダッシュボード**]>[**Wi-Fi簡易設定**]のクリックで起動できます。

注意：Wi-Fi 簡易設定の操作対象はルートフォルダ(フォルダ名:AIRRECT Cloud)のみとなります。カスタマイズフォルダは操作することができません。

Wi-Fi簡易設定からサインアウト

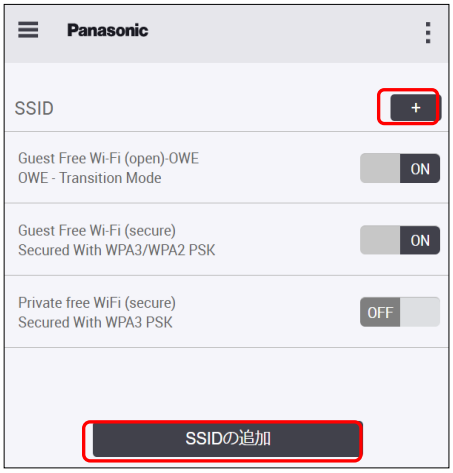
[**Wi-Fi簡易設定**]からサインアウトするには、以下の手順を実行します。

1. 画面左上のメニューアイコン≡をクリックします。
2. [**サインアウト**]をクリックするとログアウトされ、サインインページに移行します。

4.1 SSIDの基本設定

Wi-Fi簡易設定でSSIDの設定を行うには、以下の手順を実行します。

1. SSIDの一覧画面の[＋]アイコン、または[**SSIDの追加**]をクリックします。

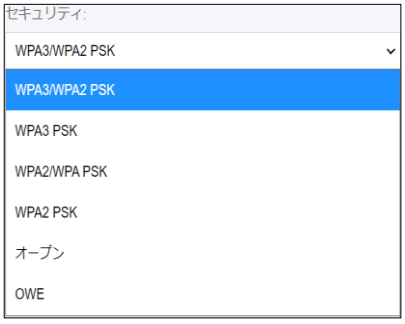


2. [**SSIDを設定する**]画面が表示されるので、[BASIC]タブで基本情報を入力します。

   ●**SSID 名**：SSID 名を入力します。

   ●**セキュリティ**：セキュリティモードを選択します。

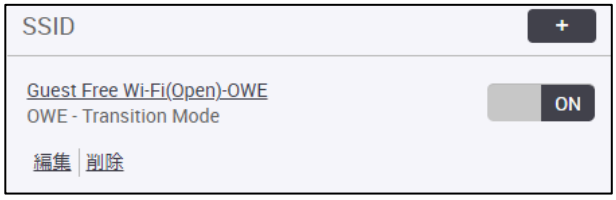
   ●**パスワード**：パスワードを入力します。



3. [**保存**]をクリックします。

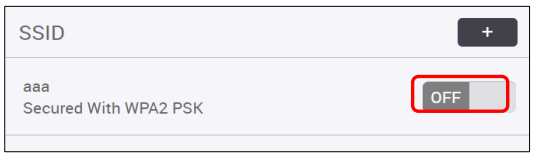
SSIDの編集/削除

SSIDをクリックすると、SSIDを[**編集**]、[**削除**]できます。



SSIDの有効化/無効化

SSID 情報の右側にある[OFF/ON]アイコンのクリックで、SSID ステータス（ON/OFF）を切り替えることができます。



各用語の確認

ポータル画面右上のメニューボタン⋮の[**リファレンスガイド**]画面から当アプリ内の用語の定義を参照できます。

4.2 SSIDのネットワークタイプ

[**SSID を設定する**]の[**ネットワークタイプ**]で、SSID のタイプを選択できます。
選択するネットワークタイプにより、設定可能な内容が異なります。
●**プライベート**：社内環境内での従業員用の SSID の場合。
●**ゲスト**：店舗/ホテルなどでのゲスト用の SSID の場合。

4.2.1 ADVANCED共通設定

ネットワークタイプ（プライベート/ゲスト）共通の設定項目は以下になります。
●**DHCP**：NAT SSID を使用する場合は ON に設定します。
●**コンテンツフィルタリング**：「DHCP」が[ON]の場合、コンテンツフィルタリングを設定できます。詳細は『コンテンツフィルタリングのポリシー設定』をご参照ください。
●**SSID スケジューリング**：SSID スケジュールを設定できます。詳細は『SSID スケジューリングの設定』をご参照ください。

コンテンツフィルタリングのポリシー設定
コンテンツフィルタリングを設定するには以下の手順を実行します。
1. [**コンテンツフィルタリング**]を[ON]にします。

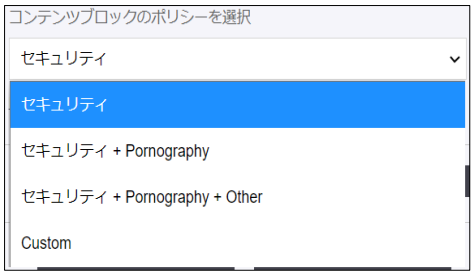
3. [**コンテンツブロックのポリシーを選択**]からポリシーを選択します。

●**セキュリティ**：マルウェア、フィッシング、詐欺サイトをブロックします。

●Pornography：性的コンテンツを含むサイトをブロックします。

●Other：成人向けコンテンツ、中絶、アルコール、犯罪、麻薬、ファイル共有、ギャンブル、ヘイト、自殺、タバコ、暴力を含むサイトをブロックします。

●Custom：カスタム設定します。

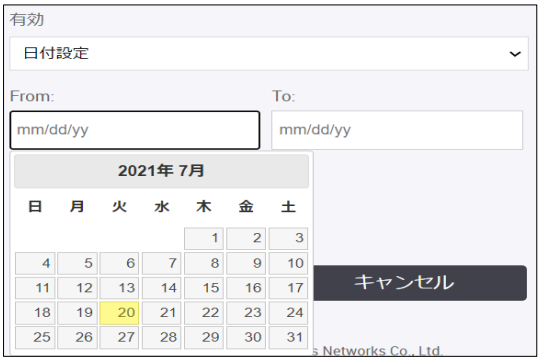


SSIDスケジューリングの設定

SSID スケジューリングを設定するには以下の手順を実行します。

1. [**SSID スケジューリング**]の[**編集**]をクリックします。
2. [**編集**]画面が表示されるので、各項目を設定します。

●[**有効**]：[**無期限**]、または[**日付設定**]を選択します。[**日付設定**]を選択した場合、表示される以下の画面から[From] [To]の日付を入力します。



●[**カスタムタイムスロット**]：決まった曜日/時間にスケジューリングしたい場合、
この項目にチェックを入れ、曜日/時間のセルをタップして設定します。

3. スケジュールの設定をした後、[**スケジュール設定**]をクリックして、設定を保存します。

4.2.2 ADVANCEDゲスト設定

ゲスト Wi-Fi 設定固有の設定項目は以下になります。
●ゲストアクセスポータル
●ゲスト帯域幅制限

ゲストアクセスポータルの設定
ゲストアクセスポータルを設定するには以下の手順を実行します。
1. [**ゲストアクセスポータル**]を[ON]にします。

2. 各項目を設定します。

●[**スプラッシュページをデザインする**]：画面のテキストをクリックすると[**スプラッシュページテンプレート**]が開きます。

設定の詳細は『スプラッシュページのデザイン』を参照ください。

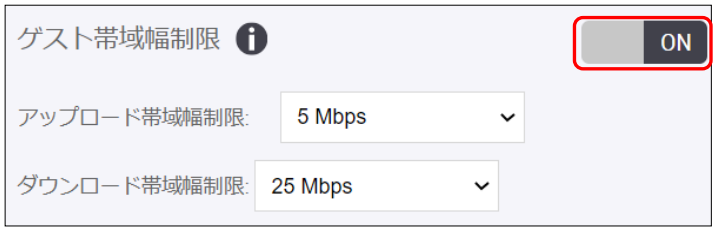
●[**リダイレクト URL**]、[**ログインタイムアウト**]、[**ブラックアウトタイム**]：ゲストログイン後の設定をします。設定の詳細は『キャプティブポータルの基本構成』を参照ください。

ゲスト帯域幅制限の設定

ゲスト帯域幅制限は、業務上で使用する通信帯域を確保したい場合など、利用可能な合計帯域幅をゲスト Wi-Fi 通信で圧迫させないために設定します。

ゲスト帯域幅制限を設定するには以下の手順を実行します。

1. [**ゲスト帯域幅制限**]を[ON]にします。



2. 各項目を設定します。

●[**アップロード帯域幅制限**]、[**ダウンロード帯域幅制限**]：利用環境に応じて、データアップロード/ダウンロードの通信速度を設定します。

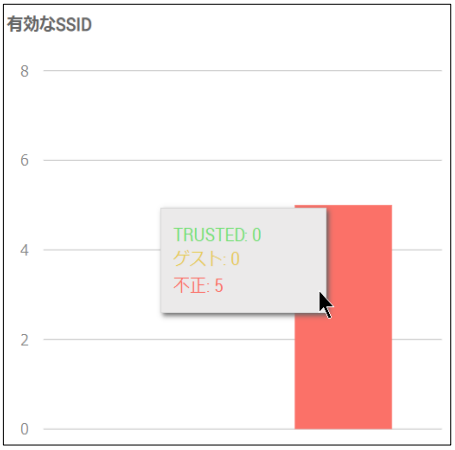
4.3 稼働状況/ゲストアクセス解析

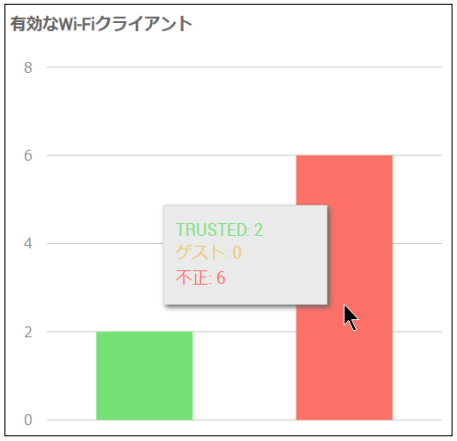
Wi-Fi簡易設定では、簡易的なWi-Fi統計情報も参照できます。
●接続デバイスの稼働状況
●ゲストアクセスの解析
これらの値は、フォルダ/フロアごとではなく、ネットワーク全体の統計情報です。
ネットワークの現状を、スマートフォンなどからスピーディに確認したい際に役立ちます。

4.3.1 接続デバイスの稼働状況

[WiFi ネットワーク]>[ダッシュボード]画面から、管理しているアクセスポイントの全てのロケーションの SSID および、接続されているデバイスの稼働状況を参照できます。
※個別のデバイス状況を確認したい場合は、Wi-Fi 統合管理から確認が必要です。

接続デバイスの稼働状況を参照するには以下の手順を実行します。
1. 画面左上の≡アイコンをクリックします。
2. [WiFi ネットワーク]>[ダッシュボード]の順に移動します。
3. [有効な SSID]と[有効な WiFi クライアント]の稼働状況が表示されます。





デバイスの分類に応じて色分けされたグラフが表示されます。
●緑色：認定 SSID/クライアント
●黄色：ゲスト SSID/ゲスト SSID に接続されたクライアント
●赤色：不正 SSID/クライアント
グラフの上にカーソルを置くとデバイス数が表示されます。

4.3.2 ゲストアクセスの解析

AIRRECT AP では、ゲスト用の SSID(ゲスト Wi-Fi)に接続したクライアントだけでなく、ゲスト Wi-Fi に接続していない近くのクライアントも認識し、そのクライアント情報を保持します。

[解析]機能は、それらのクライアント情報を、自動で簡易的なグラフとして表示することで、小売店等におけるマーケティングに役立つ情報を提供することを目的としています。

ゲストアクセスの解析には以下の 2 種類の情報があります。

●**インサイト：** 小売店などに来店をしたユーザーが、店舗にどの程度の頻度で来店しているか、またゲスト Wi-Fi を利用しているかを、周囲のクライアント履歴から分析した情報から統計し表示します。
店舗に来店しているかどうかは、RSSI 値と滞在時間で判別されます。
AIRRECT AP がクライアント認識する-70dBm 以上の強度のパケットを、5 分以上受信した場合には店内の顧客と認識され、それ以外の場合は外部の Wi-Fi クライアントと認識します。

●**アナリティクス：**ゲスト用 Wi-Fi に接続したユーザーの、接続時間帯やゲスト Wi-Fi の利用をするためのログイン方法、来客数や来客頻度などを統計し、マーケティングで利用できるように視覚化します。

インサイトの確認

インサイトの情報を参照するには以下の手順を実行します。

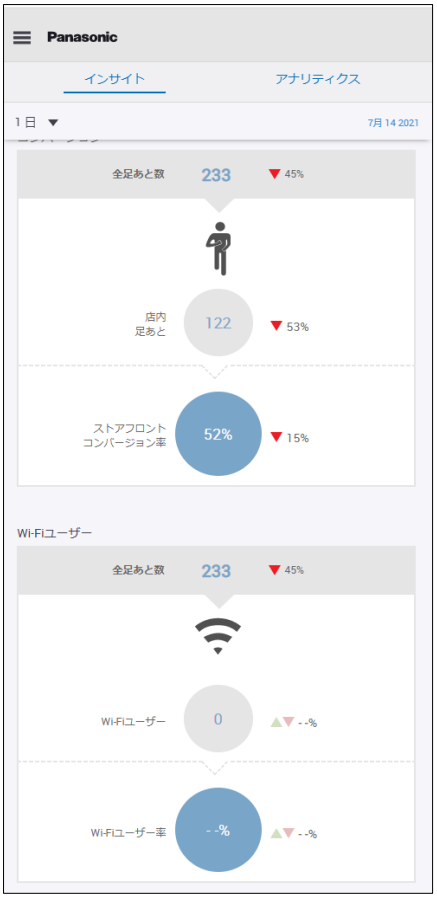
1. 画面左上の≡アイコンをクリックします。
2. **[ゲスト情報]>[ダッシュボード]**をクリックします。
3. **[インサイト]**タブにゲストのアクセス状況が表示されます。画面下へスクロールすると追加の情報が表示されます。

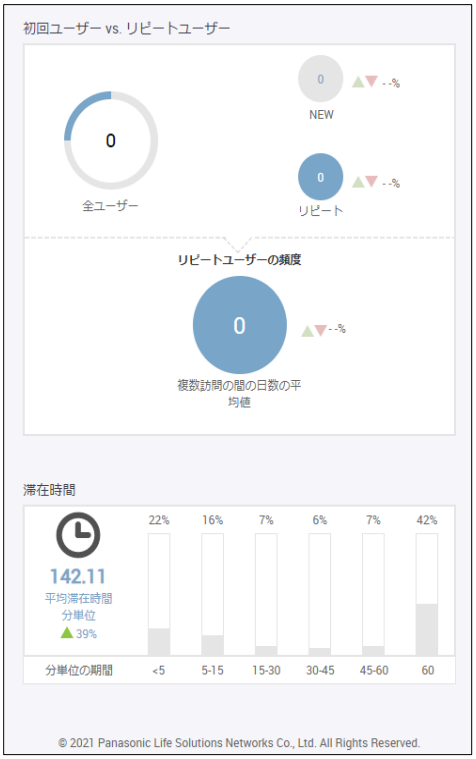
訪問者数、ユーザーの分類、ユーザーの滞在時間などの情報が視覚的に表示されます。
各情報の詳細は以下のパラメータを参照してください。

インサイトのパラメータ

項目	説明
店内足あと	入店したWi-Fiデバイスの台数を表します。
ストアフロント コンバージョン率	通過するWi-Fiデバイスのうち、何台が店舗やゾーンに入ったのかを表します。
Wi-Fiユーザー率	ゲストWi-Fiを使用する訪問者の割合を表します。
初回ユーザー	初めてゲストWi-Fiを使用した訪問者を表します。
リピートユーザー	複数回、ゲストWi-Fiを使用した訪問者を表します。
滞在時間	店舗やゾーンに入ったWiFiデバイスの滞在時間を表します。

また、統計期間を 1 日、7 日、30 日からフィルタリングにすることも可能です。



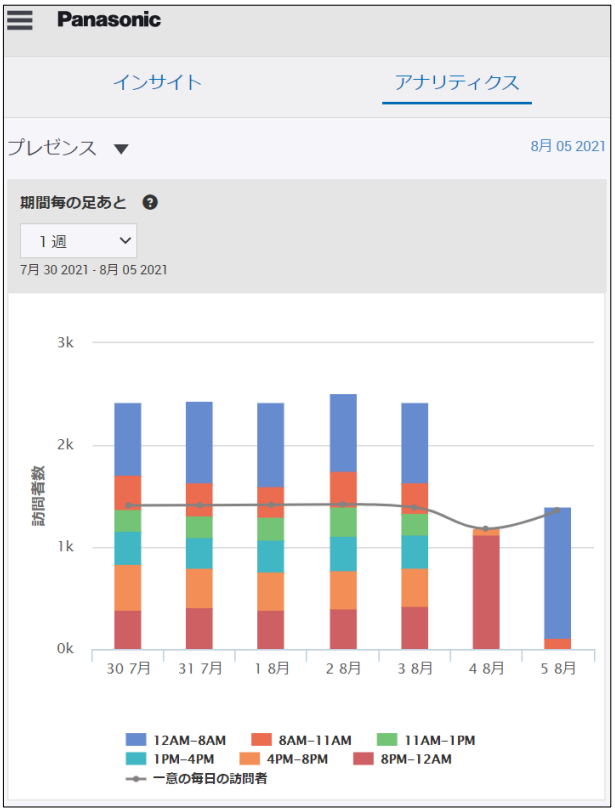


アナリティクスの確認

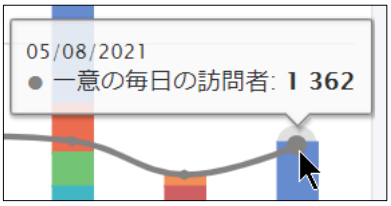
アナリティクスの情報を参照するには以下の手順を実行します。

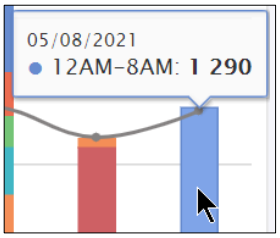
1. 画面左上の≡アイコンをクリックします。
2. [**ゲスト情報**]>[**解析**]をクリックします。
3. [**アナリティクス**]タブ>[**プレゼンス**]を選択します。

時間帯に応じて色分けされたグラフが表示されます。



グラフの上にカーソルを置くと訪問者数が表示されます。

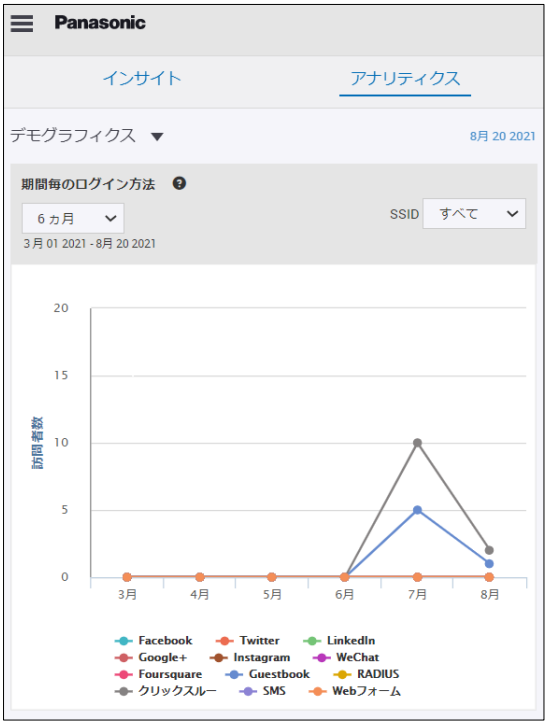




デモグラフィクス

キャプティブポータルがソーシャルメディアアカウントを介したログイン用に構成されている場合、[**デモグラフィクス**]では、インターネットへのアクセスに使用されるソーシャルメディアアカウントに基づいて、ゲストユーザーの数を数値およびグラフィックで表現することにより、Wi-Fiの使用状況を分析できます。

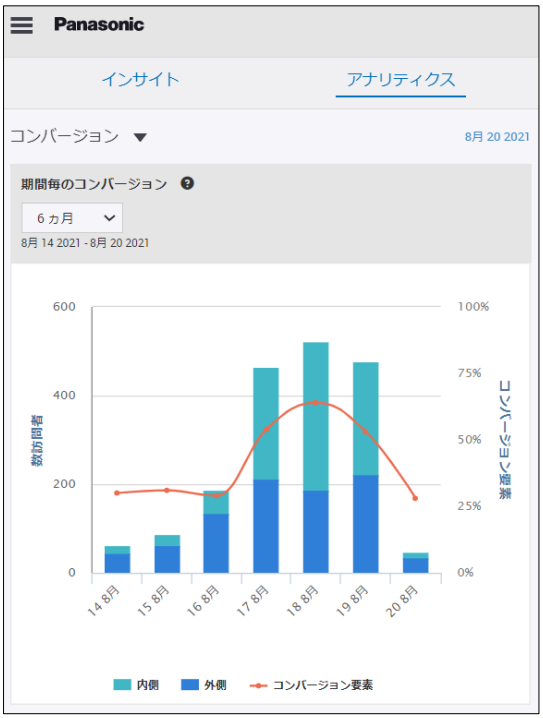
表示するには[アナリティクス]タブ>[デモグラフィクス]を選択します。



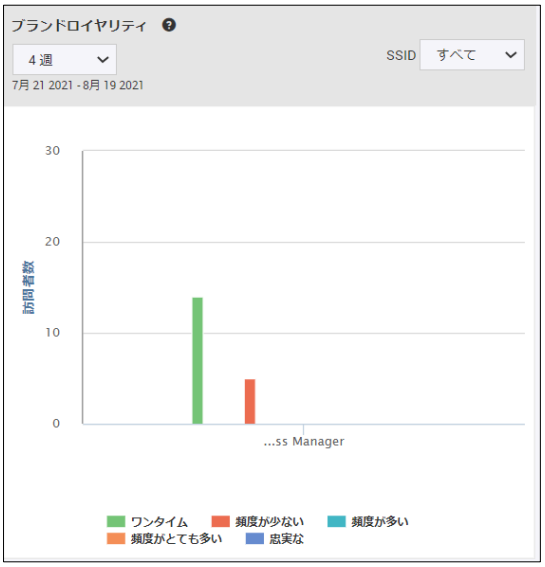
コンバージョン

[コンバージョン]は、RSSI 値に基づいて、何人のゲストがコンバージョン（来店）したかを示すコンバージョン分析グラフを表示します。

表示するには[アナリティクス]タブ>[コンバージョン]を選択します。



また、画面下部のブランドロイヤリティでは、ストアやブランドへのゲストの来店頻度を表すロイヤリティー分析グラフを表示します。
ロイヤルティ分析グラフは、[分析]> [コンバージョン]で表示できます。
これは、フィルタリングしたSSIDに対して、期間中に1回以上Wi-Fiにアクセスしたゲストユーザーの訪問頻度と訪問者の数を示す棒グラフです。 グラフは、ゲストの総数に基づいてプロットします。



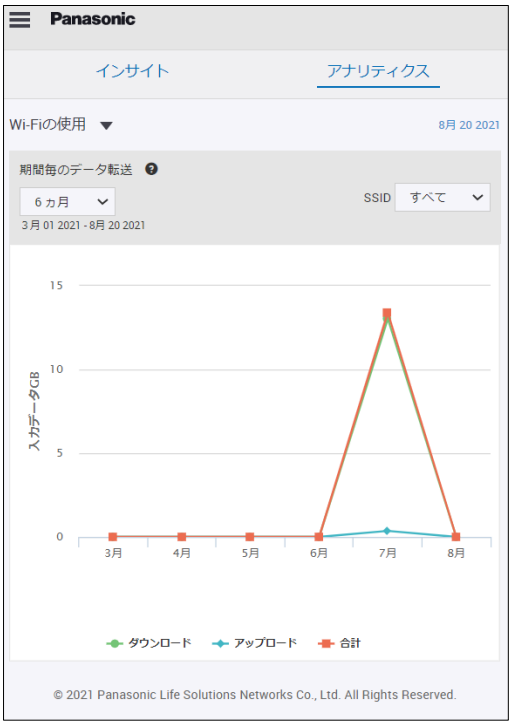
訪問頻度に応じて、以下のように分類されます。

訪問頻度	訪問回数/7 日間,14 日間	訪問回数/30 日間
ワンタイム	1 回	1 回
頻度が少ない	2 回	2～4 回
頻度が多い	3 回	5～7 回
頻度がとても多い	4 回	8～15 回
ロイヤルカスタマー	4 回以上	15 回以上

Wi-Fiの使用

[Wi-Fiの使用]では、日別、場所別の受信データ、送信データ、総データ交換量をグラフで表示します。

表示するには[アナリティクス]タブ>[Wi-Fiの使用]を選択します。

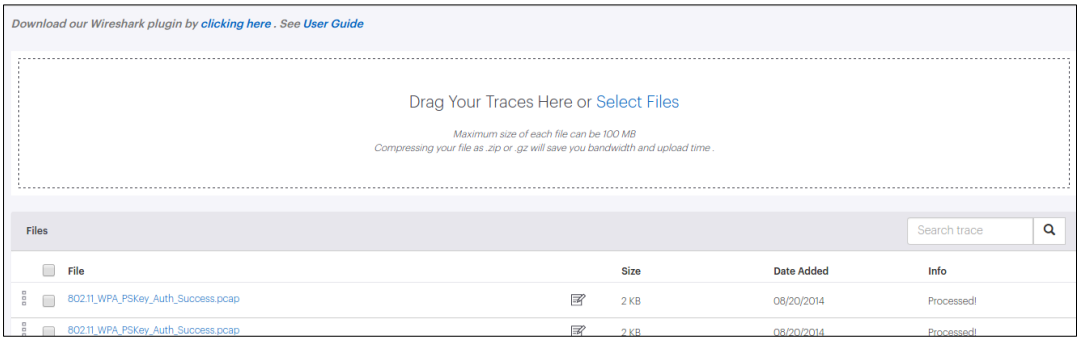


5. パケット解析 - 導入ガイド

パケット解析機能は、AIRRECT Cloudで保存されたログデータ解析を、直感的な操作で実行できます。本章では、パケット解析の簡易的な操作方法を記載します。
パケット解析は、Launchpadの [**ダッシュボード**]>[**パケット解析**]から移行します。

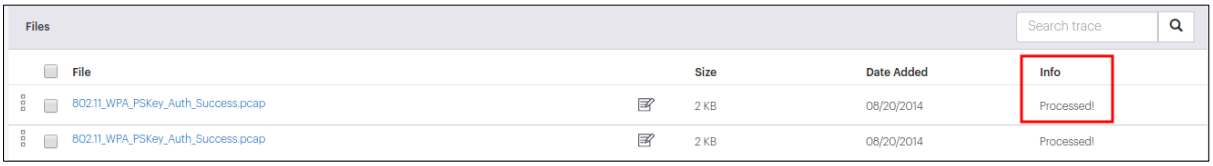
5.1 トレースファイルの分析

[**パケット解析**]タイルを選択すると、新たなトレースのアップロードや、アップロード済みトレースを管理できます。



トレースファイルのアップロード

新しいトレースは、 [Drag Your Traces]とマークされたセクションにドラッグアンドドロップするか、[Select Files]テキストをクリックして、ファイルブラウザを使用してアップロードファイルを参照/選択することでアップロードできます。
ファイルがアップロードされると、[Info]列の下に結果が表示されます。

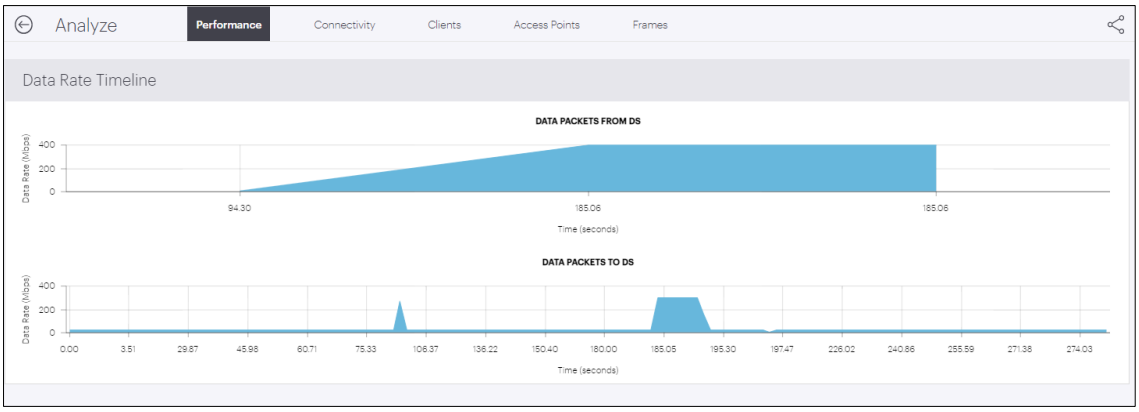


ファイル名をクリックすると、[Analyze]ページに移動します。

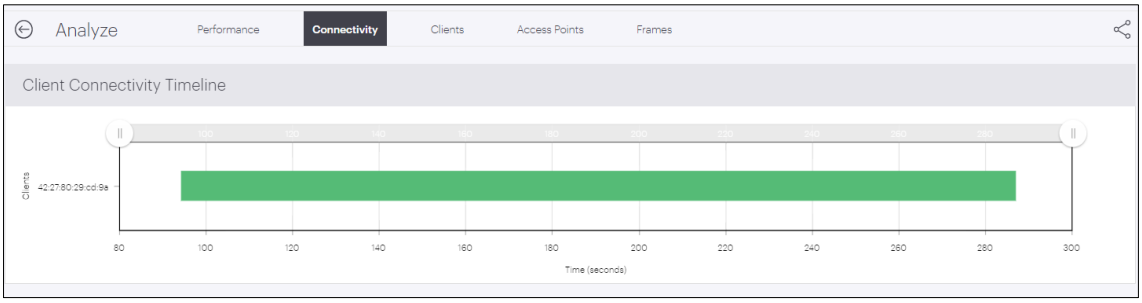
グラフとチャートの分析

[Analyze]ページには、グラフ、チャート、および表を含むさまざまなタブがあります。

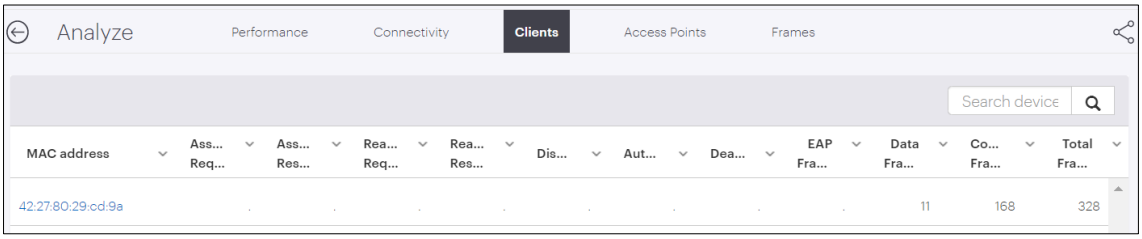
●[Performance]タブ：トレース内のクライアントとAPのパフォーマンス測定に関連するグラフが表示されます。これには、データレート、接続遅延、再試行レート、通信時間、RSSI、ブロードキャスト/マルチキャストパケットなどのパラメータが含まれます。さまざまな測定の統計と割合は、以下のページで確認できます。



●[Connectivity]タブには、トレース期間中のさまざまなクライアントの接続状態に関連するチャートとグラフが表示されます。これには、接続期間、障害、SSID、アクセスポイント、チャネルなどのパラメータが含まれます。グラフ内のクライアントをクリックすると、グラフの下のテーブルに移動し、そのクライアントの接続状態に関する詳細と統計が表示されます。



●[Clients]タブと[Access Points]タブには、トレースで検出された各クライアントとアクセスポイントの統計が表示されます。この統計には、各デバイスで見つかったさまざまなフレームタイプの数などの詳細情報が含まれます。また、分析したいデバイスの MAC を特定するためにも非常に有用です。



デバイスの選択

[Analyze]ページのさまざまなチャートと表に、トレースの接続性とパフォーマンス状況の概要が表示されます。特定のクライアント、または、アクセスポイントの詳細な分析については、任意のデバイスからそのMACアドレスをクリックしてください。これにより、[Visualize]ページに移動します。

デバイスのフレームの視覚化

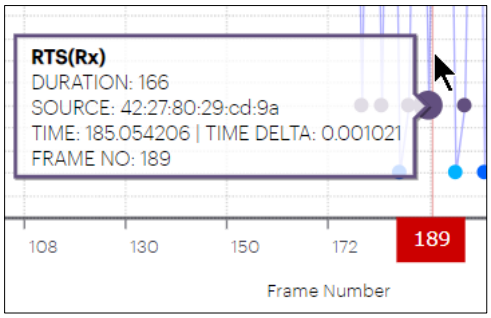
選択したMACに基づいて、ツールはトレースを処理し、[Visualize]ページを表示します。このページには、選択したデバイスのみに固有のグラフと表が含まれています。

Visualizeページ内のタブ表示について

当ページには[Frame View]、[Time View]、[Frames]の3つのタブがあります。
これらのタブに関する説明を以下に記します

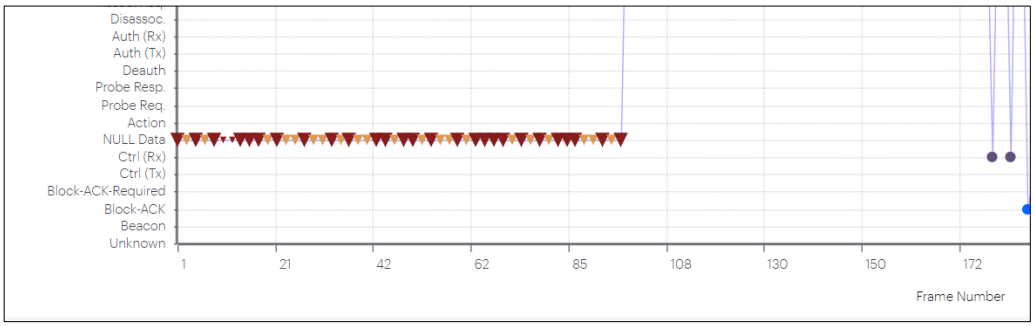
●このグラフは動的な特性を持ち、グラフ上の各マーカーはトレースの各フレームを表します。選択したクライアントMACに対応するフレームのみがグラフに表示されます。
マーカーの詳細情報は、『マーカー一覧』を参照ください。

●グラフの特定箇所にカーソルを合わせると、その特定のフレームに関する詳細情報を表示するツールチップが表示されます。

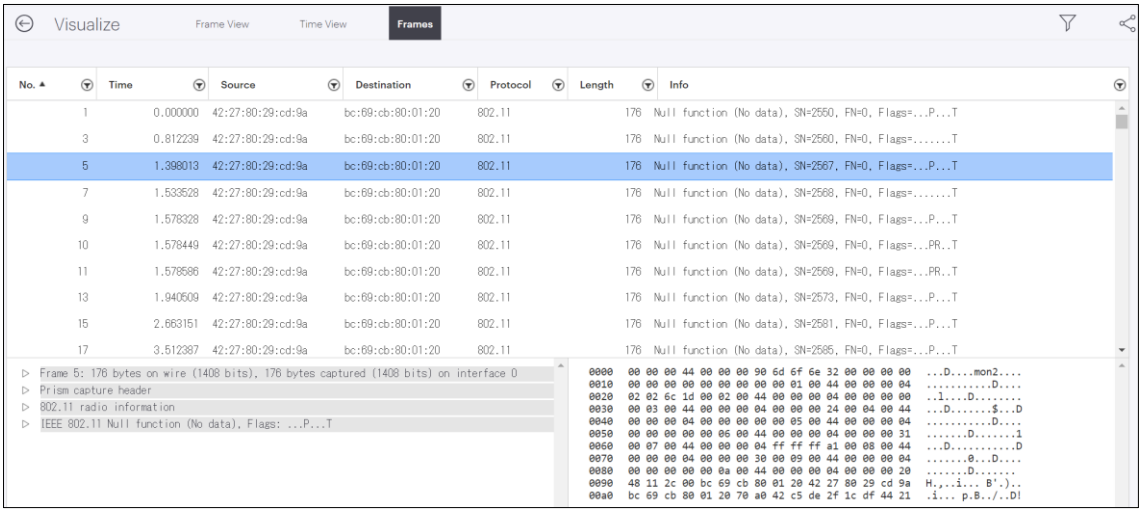


●異なるタイプ/サブタイプの異なるフレームは、グラフ上で異なる色と異なるY軸レベルで表示されます。通常の接続ハンドシェイクの後で発生するフレームタイプ/サブタイプは、前に発生したものよりも高いレベルで表示されます。この考え方は、トレース内の　接続ハンドシェイクパターンをすばやく理解するために有用です。

●X軸は、トレースにキャプチャされたフレームの実際のフレーム番号を示します。Y軸は、さまざまなフレームタイプ/サブタイプに割り当てられたさまざまな論理レベルに対応します。



●グラフとは別に[Frame]タブを使用することで、Wiresharkと同様のビュー表示をすることができます。



5.2 マーカー一覧

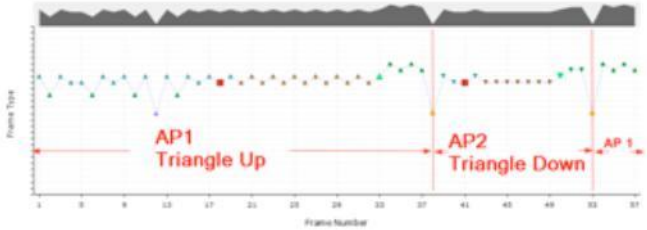
Frame Viewで表示されるマーカーは、色と形、サイズによってフレームの種類、状態が分類されます。

マーカーの色とY軸の高さ

Y軸に割り当てられている論理レベルと表示される色			フレーム種類	Wireshark フィルタ
0		000000	Beacon	wlan.fc.type_subtype==0x08
1		796B8F	ACK(Tx)/(Rx)	wlan.fc.type_subtype==0x1d
2		8A868F	PS-Poll(Tx)	wlan.fc.type_subtype==0x1a
2		624F7F	RTS(Tx)	wlan.fc.type_subtype==0x1b
2		876DAF	CTS(Tx)	wlan.fc.type_subtype==0x1c
2		583F7F	CF End(Tx)	wlan.fc.type_subtype==0x1e
2		5E536F	CF End+CF Ack(Tx)	wlan.fc.type_subtype==0x1f
3		8A868F	PS-Poll(Rx)	wlan.fc.type_subtype==0x1a
3		624F7F	RTS(Rx)	wlan.fc.type_subtype==0x1b
3		876DAF	CTS(Rx)	wlan.fc.type_subtype==0x1c
3		583F7F	CF End(Rx)	wlan.fc.type_subtype==0x1e
3		5E536F	CF End+CF Ack(Rx)	wlan.fc.type_subtype==0x1f
4		CC6600	空データ(Tx)	wlan.fc.type_subtype==0x2c || wlan.fc.type_subtype==0x2d || wlan.fc.type_subtype==0x2e || wlan.fc.type_subtype==0x24 || wlan.fc.type_subtype==0x25 || wlan.fc.type_subtype==0x26 || wlan.fc.type_subtype==0x27
4		DF9853	空データ(Rx)	wlan.fc.type_subtype==0x2c || wlan.fc.type_subtype==0x2d || wlan.fc.type_subtype==0x2e || wlan.fc.type_subtype==0x24 || wlan.fc.type_subtype==0x25 || wlan.fc.type_subtype==0x26 || wlan.fc.type_subtype==0x27
5		98AFC7	アクションフレーム(Tx)	wlan.fc.type_subtype==0x0d
5		12395F	アクションフレーム(Rx)	wlan.fc.type_subtype==0x0d
6		6699CC	プローブ要求	wlan.fc.type_subtype==0x04

Y 軸に割り当てられている論理レベルと表示される色			フレーム種類	Wireshark フィルタ
7		66CCCC	プローブ返信	wlan.fc.type_subtype==0x05
8		E42217	認証解除(Tx)	wlan.fc.type_subtype==0x0c
9		E42217	認証解除(Rx)	wlan.fc.type_subtype==0x0c
10		3333CC	認証(Tx)/(Rx)	wlan.fc.type_subtype==0x0b
11		E42217	アソシエーション解(Tx)/(Rx)	wlan.fc.type_subtype==0x0a
12		C25283	アソシエーションリクエスト	wlan.fc.type_subtype==0x00
13		7D2252	アソシエーション返信	wlan.fc.type_subtype==0x01
14		9966FF	再アソシエーションリクエスト	wlan.fc.type_subtype==0x02
15		9933FF	再アソシエーション返信	wlan.fc.type_subtype==0x03
16		990000	ATIM	wlan.fc.type_subtype==0x09
17		9933	EAPOL(Tx)	eapol
18		9933	EAPOL(Rx)	eapol
19		3B9C9C	EAP(Tx)	eap
19		996633	SSL(Tx)	ssl
20		3B9C9C	EAP(Rx)	eap
20		996633	SSL(Rx)	ssl
21		9933	EAPOL-K(Tx)	eapol.type == 3
22		9933	EAPOL-K(Rx)	eapol.type == 3
23		660000	データ(Tx)	データ
24		660000	データ(Rx)	データ

マーカーの形

形		使用方法/意味
	円	この形は、AP でクライアントが認証される前に交換されたフレームを示すのに使われます。例：プローブ要求、プローブ返信
	四角	この形は、なんらかの失敗をしたフレームを示すのに使われます。 例：認証解除、アソシエーション解除
	上向き三角	この形は、AP でクライアントが認証された時 (プローブ段階の後)、またはその後に交換されたフレームを示すのに使われます。 例：認証、アソシエーションリクエストなど
	下向き三角	この形は、*上向き三角*と同様に使われますが、トレースキャプチャした期間においてクライアントが異なる BSSID に移動していた場合にのみ使われます。BSSID が変わるとすぐに*上向き三角*は*下向き三角*に変わり、再度 BSSID が変わるまでそのままとなります。このように、この形はクライアントホッピングを視覚的に示すために、*上向き三角*と共に使われます。 例：例えばあるクライアントが AP1 から AP2 へ、そしてまた AP1 へホッピングしたとします。この場合、AP1 と交換されたフレームはすべて上向き三角となり、AP2 と交換されたフレームはすべて下向き三角となります。 
	星	この形は、クライアントがアソシエイトを試みている AP の MAC と異なる MAC を Current AP フィールドに持つ、特別な再アソシエーションフレームを示すのに使われます。つまり、この形はホッピングを示す再アソシエーションフレームを示すのに使われます。

マーカーのサイズ

すべてのマーカーは下記の3つのケースを除き同じサイズです：

1. 失敗を示すフレーム (認証解除やアソシエーション解除フレーム)
2. 成功を示すフレーム (EAP-成功フレーム)
3. リトライフレーム (リトライビットを1に設定)

1, 2のケースでは、フレームの重要さを強調するためにマーカーのサイズが他より少し大きくなります。

3のケースでは、以前のフレームのリトライであることを示すために、マーカーのサイズが他より少し小さくなります。

© Panasonic Electric Works Networks Co., Ltd. 2022-2025

パナソニックEWネットワークス株式会社

〒105-0021　東京都港区東新橋2丁目12番7号　住友東新橋ビル2号館4階
TEL 03-6402-5301 / FAX 03-6402-5304
URL: https://panasonic.co.jp/ew/pewnw/

P0422-21105