

■AIRRECT Could Ver16.1.0 主要追加機能

本ドキュメントは Ver16.1.0 での主要な追加機能および仕様変更の概要を記載します。

軽微な機能追加や仕様変更、不具合修正に関しては、リリースノートをご参照ください。

No.	機能
1	クライアントイベントログのエクスポート
2	アクセスポイントイベントログの保存期間拡大
3	アラート通知タイプの一括全選択-解除
4	ダイナミック VLAN - 自動
5	証明書アクション
6	フロアプラン - 無線ごとのクライアント数
7	CPU/メモリ閾値超過アラート
8	アップリンクポート認証失敗アラート
9	ダッシュボード - 概要
10	ACS/TPC フリーズ
11	RadSec(Radius over TLS)
12	アップリンクポート認証
13	ホットスポット SSID/脆弱な SSID
14	干渉分類
15	Ekahau 統合
16	フォルダープラン - Google マップビュー
17	Web フック

1. クライアントイベントログのエクスポート

CSV出力により、クライアントイベントログのローカル保存が可能となります。

※エクスポート操作はクライアント単位での実施となります。

●画面遷移：[モニター]>[WiFi]>[クライアント]>クライアント名のクリック>[イベントログのエクスポート(アイコン)]

#	A	B	C	D	E	F	G	H	I	J
	タイムスタンプ	イベント	説明	BSSID	AP名	ロケーション	SSID	信号強	チャンネル	パケット
1	2024年5月21日 10:57:03.095	Success	成功	bc:69:cb:8 1st_A7:1F	//AIRREC #1			5 GHz	144	
2	2024年5月21日 10:57:03.087	Intermediate	クライアントは、IPv4 DNSクエリに	bc:69:cb:8 1st_A7:1F	//AIRREC #1			5 GHz	144	
3	2024年5月21日 10:57:02.424	Intermediate	クライアントは、IP192.168.1.32を	bc:69:cb:8 1st_A7:1F	//AIRREC #1			5 GHz	144	
4	2024年5月21日 10:57:02.424	Intermediate	クライアントには IP アドレス	bc:69:cb:8 1st_A7:1F	//AIRREC #1			5 GHz	144	
5	2024年5月21日 10:57:02.423	Intermediate	クライアントには IP アドレス	bc:69:cb:8 1st_A7:1F	//AIRREC #1			5 GHz	144	
6	2024年5月21日 10:57:02.423	Intermediate	クライアントにVLAN 0が割り当て	bc:69:cb:8 1st_A7:1F	//AIRREC #1			5 GHz	144	
7	2024年5月21日 10:57:02.423	Intermediate	クライアントにVLAN 0が割り当て	bc:69:cb:8 1st_A7:1F	//AIRREC #1			5 GHz	144	
8	2024年5月21日 10:57:02.379	Intermediate	クライアントが正常に(再)アソシ	bc:69:cb:8 1st_A7:1F	//AIRREC #1			5 GHz	144	
9	2024年5月21日 10:57:02.379	Intermediate	クライアントにVLAN 0が割り当て	bc:69:cb:8 1st_A7:1F	//AIRREC #1			5 GHz	144	
10	2024年5月21日 10:57:02.371	Intermediate	AP がクライアントから認証要求	bc:69:cb:8 1st_A7:1F	//AIRREC #1			5 GHz	144	
11	2024年5月21日 03:01:44.955	Intermediate	クライアントは、IPv4 DNSクエリ	bc:69:cb:8 2nd_A7:AF	//AIRREC #1			5 GHz	132	
12	2024年5月21日 02:50:18.847	Success	成功	bc:69:cb:8 2nd_A7:AF	//AIRREC #1			5 GHz	132	
13	2024年5月21日 02:48:25.722	Intermediate	クライアントには IP アドレス	bc:69:cb:8 2nd_A7:AF	//AIRREC #1			5 GHz	132	
14	2024年5月21日 02:48:15.799	Intermediate	クライアントは、IP192.168.1.32	bc:69:cb:8 2nd_A7:AF	//AIRREC #1			5 GHz	132	
15	2024年5月21日 02:48:15.799	Intermediate	クライアントには IP アドレス	bc:69:cb:8 2nd_A7:AF	//AIRREC #1			5 GHz	132	
16	2024年5月21日 02:48:15.692	Intermediate	クライアントにVLAN 0が割り当て	bc:69:cb:8 2nd_A7:AF	//AIRREC #1			5 GHz	132	
17	2024年5月21日 02:48:15.682	Intermediate	クライアントは、IP192.168.1.32	bc:69:cb:8 2nd_A7:AF	//AIRREC #1			5 GHz	132	
18	2024年5月21日 02:48:15.682	Intermediate	クライアントには IP アドレス	bc:69:cb:8 2nd_A7:AF	//AIRREC #1			5 GHz	132	
19	2024年5月21日 02:48:15.681	Intermediate	クライアントにVLAN 0が割り当て	bc:69:cb:8 2nd_A7:AF	//AIRREC #1			5 GHz	132	

2. アクセスポイントイベントログの保存期間拡大

アクセスポイントイベントログの保存期間は“1 週間”から“1 カ月”へ拡大します。

●画面遷移：[トラブルシューティング]>[イベントログ]>[アクセスポイント]

時刻 ↓	名前	説明
2024年5月23日 08:43:18.183	2nd_A7:AF	自動チャンネル選択が開始されました。APは動作モード11AXG HE20でチャンネル
2024年5月23日 08:43:18.175	2nd_A7:AF	Periodic ACSハンドラーがチャンネル12/バンド2.4 GHzでトリガーされました。
2024年5月23日 08:35:10.165	1st_A7:1F	SSID #0 (2.4 Ghz) の出力：UP.
2024年5月23日 08:35:10.165	1st_A7:1F	SSID #1 (2.4 Ghz) の出力：UP.
2024年5月23日 08:35:10.158	1st_A7:1F	APが、動作モード11AXG HE20でチャンネルを9に 変更しました。
2024年5月23日 08:35:09.291	1st_A7:1F	Periodic ACSハンドラーがチャンネル13/バンド2.4 GHzでトリガーされました。

3. アラート通知タイプの一括全選択-解除

アラート通知タイプ(表示/メール/通知)の選択、および選択解除の一括で操作できるようになりました。
このフィールドは各アラートカテゴリ画面に設けております。

- 画面遷移：[構成]>[アラート]>[アラートを設定]



4. ダイナミック VLAN – 自動 VLAN

ダイナミック VLAN を利用する場合、これまでは動的割り当てを行う VLAN を事前に指定する必要がありましたが、『自動 VLAN』では、この VLAN 指定の手間を省くことができます。

- 画面遷移：SSID プロファイル>[セキュリティ] or [アクセス制御]



5. 証明書アクション

RadSec やアップリンクポート認証機能を利用する場合、証明書によるアクセスポイント自身の認証が必要となります。アクセスポイントに対する証明書関連の操作(CSR 生成/CSR 出力/証明書入力など)は証明書アクションへ集約されております。

※証明書の発行や証明書への署名はできません。

●画面遷移：[モニター]>[WIPS]>[管理対象 WiFi デバイス]>[証明書アクション(アイコン)]

The screenshot displays the '証明書アクション' (Certificate Action) menu in the Panasonic AIRRECT Cloud interface. The menu items are:

- CSRを生成
- CSRをダウンロード
- デバイス証明書をアップロード
- 証明書を削除
- 証明書を再アップロード
- CSR設定
- 過去のユーザー・アクションのログをダウンロード

Three modal windows are shown:

- CSRを生成**: A dialog for generating a CSR, with a dropdown menu set to 'RadSec' and a '生成' (Generate) button.
- CSRをダウンロード**: A dialog for downloading a CSR, with a dropdown menu for selecting a certificate tag and a 'ダウンロード' (Download) button.
- デバイス証明書をアップロード**: A dialog for uploading a device certificate, with a dropdown menu set to 'RadSec' and a 'ファイルを選択' (Select File) button.

6. フロアプラン - 無線ごとのクライアント数

フロアプランへ表示できる情報として、『無線ごとのクライアント数』が追加されました。アクセスポイントへの接続台数を、周波数帯(2.4GHz 帯/5GHz 帯)ごとに確認することができます。

※カッコ内の数値が周波数帯を示します。

●画面遷移：[フロアプラン]>フロアへアクセス>[:]>[無線ごとのクライアント数]

The screenshot shows a floor plan view in the Panasonic AIRRECT Cloud interface. A callout box points to an access point with the text '5GHzに3台接続中' (3 devices connected to 5GHz). The right-hand sidebar shows a list of filters, with '無線ごとのクライアント数' (Client count by wireless band) highlighted in red.

7. CPU/メモリ閾値超過アラート

アクセスポイントのCPU/メモリ平均使用率が閾値を超過した場合にアラートを受け取ることができます。閾値はカスタマイズが可能です。

- 画面遷移：[構成]>[アラート]>[アラートを設定]>[デバイス]

The screenshot shows the 'Alerts' configuration page in the Panasonic AIRRECT Cloud interface. The 'Device' section is highlighted with a red box, showing two alert rules:

- CPU:** CPU使用率が超過しています. Threshold: 3% (min), 15% (max). [15~120].
- Memory:** メモリ使用率が超過しています. Threshold: 40% (min), 15% (max). [15~120].

Red arrows labeled 'CPU' and 'Memory' point to these respective settings. A green arrow labeled '閾値超過時' (Threshold Exceeded) points to the 'システム' (System) tab in the alert list below. The alert list shows two alerts:

ID	優先度	ステータス	概要
28647	LOW	🟡	AP [BC-69:CB-8E-A7-AF]のメモリ使用率が15分以上40パーセントを超過しました。
28646	LOW	🟡	AP [BC-69:CB-8E-A7-AF]のCPU使用率が15分以上3パーセントを超過しました。

8. アップリンクポート認証失敗アラート

アクセスポイントのアップリンクポート認証に失敗した場合にアラートを受け取ることができます。

- 画面遷移：[構成]>[アラート]>[アラートを設定]>[デバイス]

The screenshot shows the 'Alerts' configuration page in the Panasonic AIRRECT Cloud interface. The 'Device' section is highlighted with a red box, showing one alert rule:

- Uplink Port:** 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.

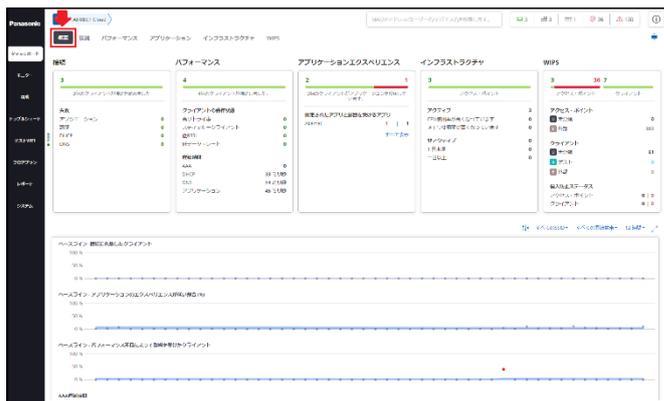
A red arrow points to this setting. A green arrow labeled '認証失敗' (Authentication Failure) points to the 'システム' (System) tab in the alert list below. The alert list shows one alert:

ID	優先度	ステータス	概要
9965	HIGH	🔴	デバイス [BC-69:CB-80:68:CF] についてアップリンクポート認証の失敗が報告されました。

9. ダッシュボード - 概要

AIRRECT Cloud の新しいスタート画面です。各ダッシュボード(接続/パフォーマンス/アプリケーション/インフラストラクチャ/WIPS)からピックアップした主要な情報が1つの画面に集約されています。ユーザーはログインしてすぐに、現在は勿論、過去1カ月のネットワーク状況を様々な観点で可視化、把握することができます。

●画面遷移：[ダッシュボード]>[概要]



10. ACS/TPC フリーズ

TPC(送信電力制御)や ACS(自動チャンネル選択)が動作するロケーションにて、特定のアクセスポイントの送信電力やチャンネルを簡単にフリーズ(固定化)させることができます。フリーズ中のアクセスポイントは送信電力やチャンネルの変更は発生しません。フリーズはいつでも解除することができます。

※DFS は ACS フリーズ中も発生します。

●画面遷移：[モニター]>[WiFi]>[無線通信]

ステータス	アクセスポイント	チャンネル	チャンネル選択モード	Tx.電力 (dBm)	送信電力モード
無線を無効化する	1st_A7:1F	144	カスタマイズされていません	23	カスタマイズされていません
ACSをフリーズ	1st_A7:1F	9	カスタマイズされていません	23	カスタマイズされていません
TPCをフリーズ	2nd_A7:AF	108	カスタマイズされていません	23	カスタマイズされていません
	2nd_A7:AF	1	カスタマイズされていません	23	カスタマイズされていません

11. RadSec(Radius over TLS)

RadSec では、アクセスポイントと Radius サーバー間の RADIUS 通信が TLS により暗号化されます。従来の UDP を使用した平文の Radius 通信の弱点を強化することができます。

●画面遷移：[構成]>[ネットワークプロファイル]>[RADIUS]



12. アップリンクポート認証

アクセスポイント自身のネットワークへの参加を IEEE802.1X(EAP-TLS)認証によりセキュアに実施することができます。認証前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、認証成功時は企業 VLAN を、認証失敗時はゲスト VLAN を提供するなどがあります。

●画面遷移：[構成]>[デバイス]>[アクセスポイント]>[LANポート]>[アップリンクポートの認証]



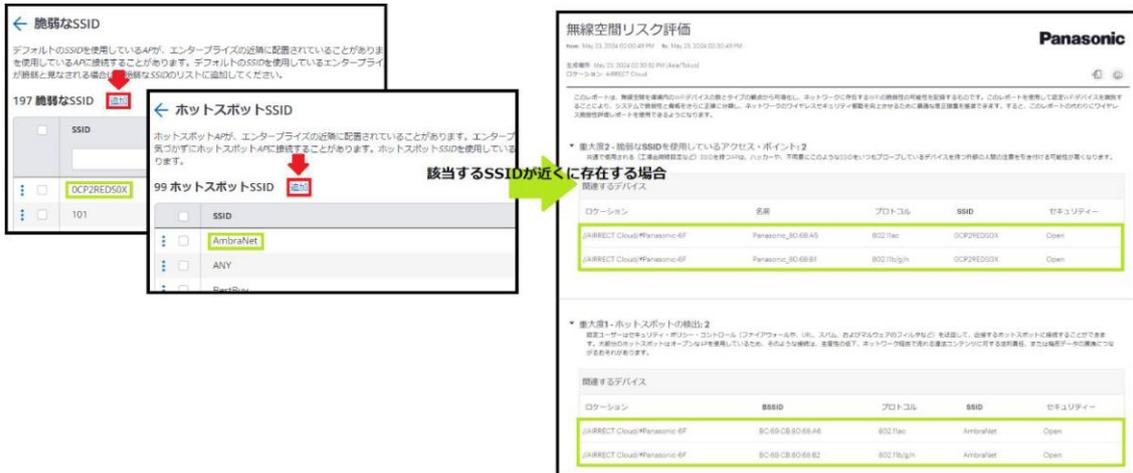
例)



13. ホットスポット SSID/脆弱な SSID

セキュリティリスクとなるホットスポット SSID や脆弱な SSID を自在に定義できるようになりました。定義した SSID 名を出力するアクセスポイントが企業ネットワーク付近に存在する場合、WIPS レポート (“無線空間リスク評価”または“ワイヤレス脆弱性評価”)により、その存在を把握することができます。

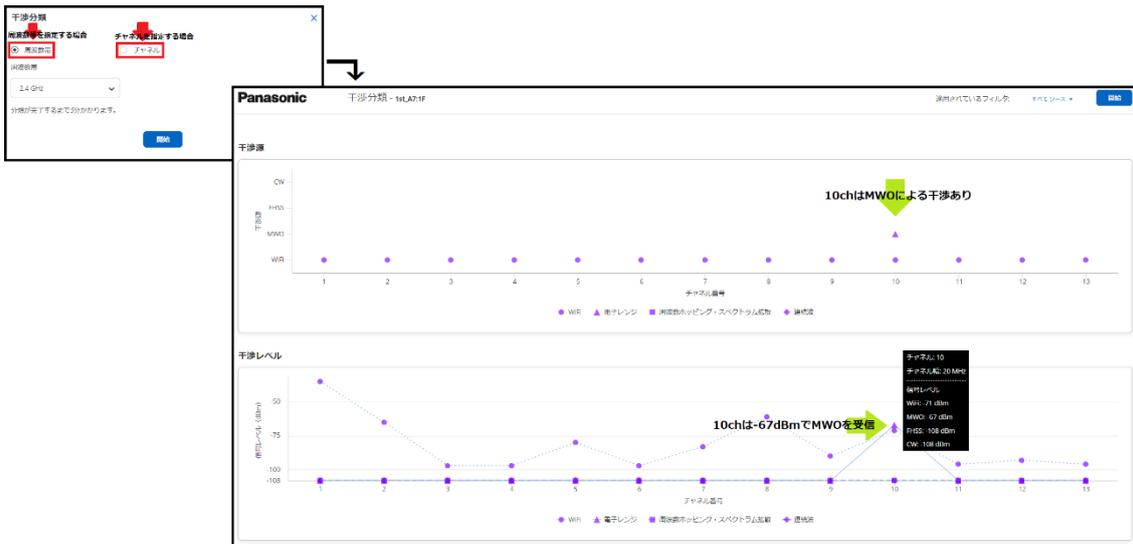
●画面遷移：[システム]>[詳細設定]>[ホットスポット SSID] or [脆弱な SSID]



14. 干渉分類

Wi-Fi 電波へ悪影響を与えるのは、Wi-Fi デバイスだけではありません。電子レンジ、Bluetooth 機器などの家電製品の電磁波も干渉の原因となります。干渉分類では、各チャンネルに存在する干渉物をリアルタイムで分類、特定することができます。分類は、Wi-Fi(Wi-Fi デバイス)、MWO(電子レンジなど)、FHSS(Bluetooth, ZigBee など)、CW(レーダーなど)の4つです。

●画面遷移：[モニター]>[WiFi]>[アクセスポイント]>[：]>[トラブルシューティング]>[干渉分類を開始]



15. Ekahau 統合

Ekahau Cloud にて作成したフロアプランを、AIRRECT Cloud のフロアプランとしてインポートすることができます。画像入力、寸法入力、アクセスポイントの配置。これら全て自動化されます。

- 画面遷移：[フロアプラン]>[フロアプランの追加]>[Ekahau からインポート]



16. フォルダープラン - Google マップビュー

Google マップへ拠点(フォルダー)を配置することができます。

拠点の正確な位置に加え、現在のネットワーク状況を拠点ごとに把握することができます。

- 画面遷移：[フロアプラン]>[マップビュー]



17. Web フック

アラートを、Google Chat、Microsoft Teams、Slack などのアプリケーションで受け取ることができます。

アラートの文書はカスタマイズが可能です。

※アラート通知タイプで“通知”を選択しているアラートが Web フックの対象となります。

●画面遷移：[システム]>[サードパーティーのサーバー]>[Webhook]

