

## ■ AIRRECT Cloud ver.14.0.0 主要追加機能

本ドキュメントは ver14.0.0 での主な追加機能および仕様変更の概要を記載します。

その他、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.	追加機能
1	Spatial Reuse 機能(チャンネル干渉空間でのクライアント同時通信の改善)
2	自動 DFS チャンネル候補リスト管理機能
3	自動チャンネル選択スケジュール機能
4	UPSK (Unique PSK) 機能
5	キャプティブポータルの認証プラグインに SAML 方式、OpenID Connect 方式を追加
6	クラウド設定情報のチェックポイント機能(保存、復元、比較)
7	クラウド管理画面の UI、デザインの改善
8	フロアプランにスイッチ情報を表示する機能
9	アクセスポイントのステータスを統合表示する機能
10	クライアントイベントログの統合管理機能
11	クライアントエクスプローラー機能
12	キャプティブポータルのゲストブック機能の改善
13	WIPS のデバイスインポート機能
14	BSSID 検索/表示機能の改善
15	NAC クラスター設定における CoA リクエスト機能
16	RADIUS ダイナミックリダイレクト機能
17	カスタマイズされたロケーションフォルダの表示機能
18	クライアント接続テストに結果パラメータ表示機能
19	Wi-Fi レポート機能の拡張 (「クライアント特性」「WiFi 無線」)
20	ビーコンにアクセスポイント名の表示機能
21	設定メニューの項目最適化
22	パスワードポリシー変更
23	パスワードポリシーチェックのバー表示機能

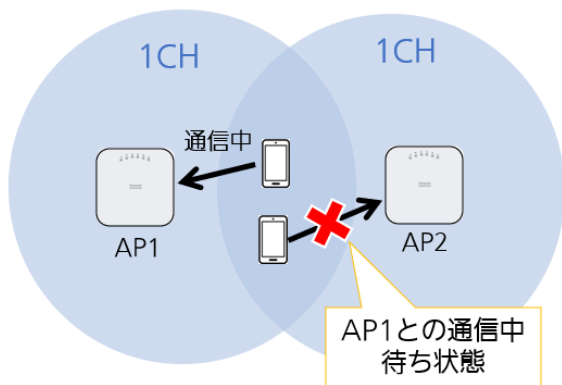
## 1. Spatial Reuse 機能(チャンネル干渉空間でのクライアント同時通信の改善)

従来対応していた 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。BSS Color とは、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。

これまでの干渉回避方式の CSMA/CA は、同一チャン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。

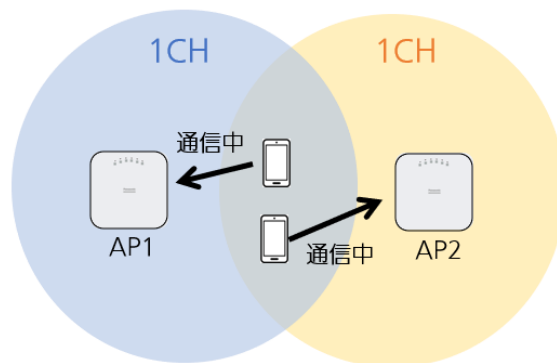
### 【CSMA/CA 方式】

同じチャン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。



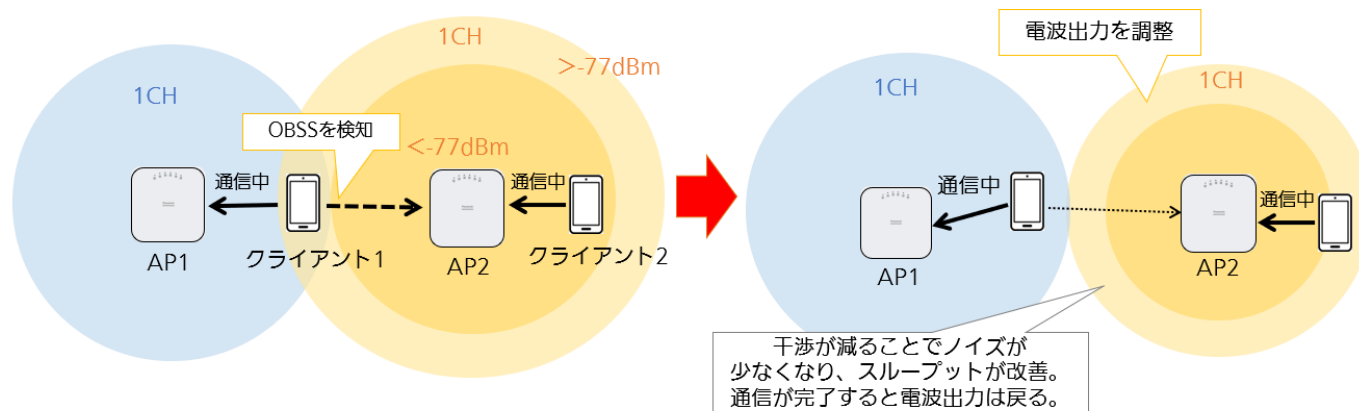
### 【BSS Color】

同一チャンネルであっても、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、同じチャン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。

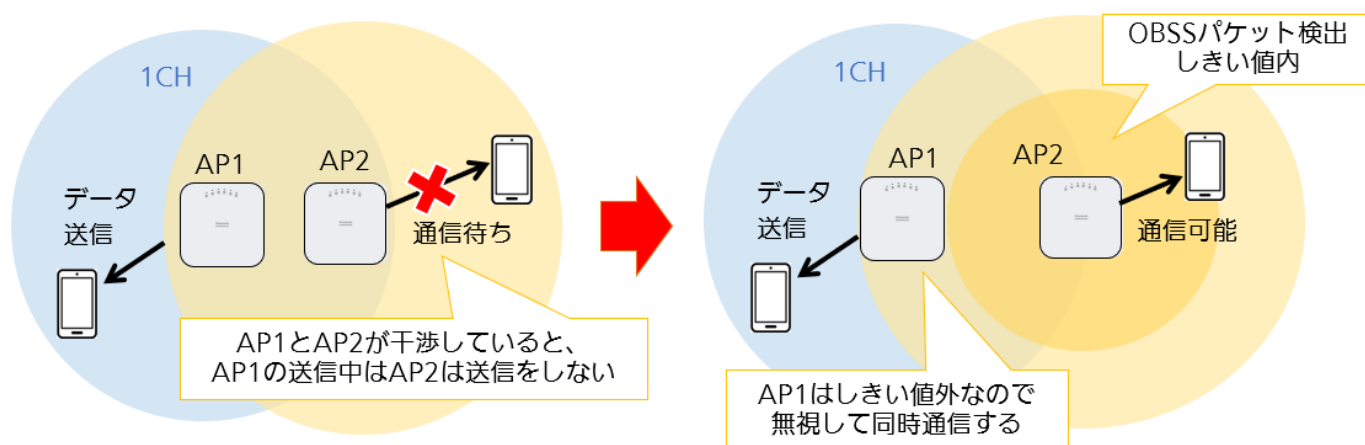
#### OBSS/パケット検出のしきい値

-77



dBm [-81～-62]

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。



## 2. DFS チャンネル履歴 リスト管理機能

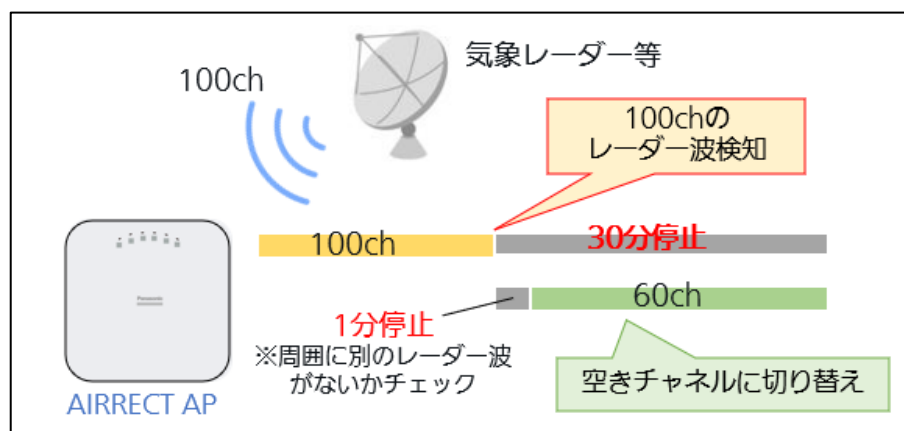
過去のレーダーヒット率(チャンネルスコア)に基づき、DFS※チャンネル候補リストを自動生成することができます。アクセスポイントの運用を継続し学習させることで、レーダーを避ける最適なチャンネルが選択されることで、DFS による問題が解消されます。

※DFS : Dynamic Frequency Selection の略。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ンネルを調べて移動する一連の処理のこと。

- チャンネルごとのレーダーヒット率は、再起動後も有効です。
- DFS チャンネルのレーダーヒット率は、近隣のアクセスポイントと共有します。

[DFS による問題]

- 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、その後別のチャンネルに切り替える。
- 電波停止を避けるため、使っているチャンネルを制限することにより干渉が発生。
- 問題発生時は、周囲の AP がカバレッジを調整し、隣接するアクセスポイントにローミングまたは、2.4GHz 帯にステアリングされる。

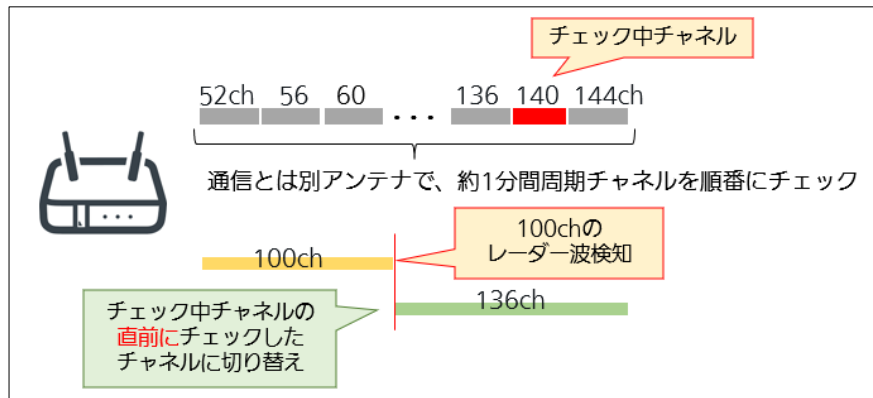


## [一般的な DFS 回避機能との差分]

一般的な DFS 回避機能のメカニズムとして、レーダー派を検知する前に別のチャン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。

- ・検知するレーダー派が多数あると、頻繁にチャンネル変更が発生する可能性がある。
- ・チャン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。



## 3. 自動チャンネル選択スケジュール機能

自動チャンネル選択の実行タイミングの選択肢が拡張されました。動的チャンネル変更を設定されている場合、環境によってはチャンネルが頻繁に発生してしまうことがあります。その場合はクライアントへの影響を最小限にするため、動的チャンネル変更ではなく、影響が少ない時間帯でのみ変更をする設定が必要です。V12 までは、チャンネルスキャンを行う時間間隔のみ設定が可能でしたが、本機能拡張によって、時間帯の指定が 2 つまで可能となりました。

### チャンネル設定

チャンネル選択  
☒ 自動 ☐ 手動

候補チャンネル  

☐ すべてのチャンネル

☐ すべての非DFSチャンネル

<input type="checkbox"/> 36	<input type="checkbox"/> 40	<input type="checkbox"/> 44	<input type="checkbox"/> 48	<input checked="" type="checkbox"/> 52	<input checked="" type="checkbox"/> 56
<input checked="" type="checkbox"/> 60	<input checked="" type="checkbox"/> 64	<input checked="" type="checkbox"/> 100	<input checked="" type="checkbox"/> 104	<input checked="" type="checkbox"/> 108	<input checked="" type="checkbox"/> 112
<input checked="" type="checkbox"/> 116	<input checked="" type="checkbox"/> 120	<input checked="" type="checkbox"/> 124	<input checked="" type="checkbox"/> 128	<input checked="" type="checkbox"/> 132	<input checked="" type="checkbox"/> 136
<input checked="" type="checkbox"/> 140	<input checked="" type="checkbox"/> 144				

選択モード \*  
☒ スケジュール ☐ 定期的

☒ セカンドACSタイムスロット

ファーストタイムスロット (HH:MM) \*  

04

00

セカンドタイムスロット (HH:MM)  

12

00

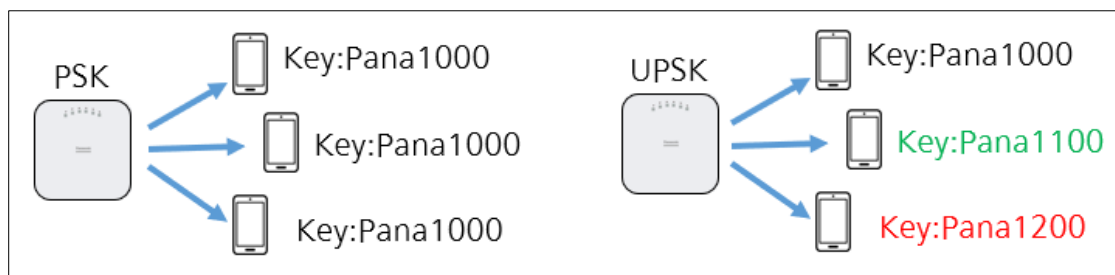
備考：選択されているロケーションのタイムゾーンに従います。

☐ 動的チャンネル選択

☐ チャンネル選択でDFS履歴を使用

## 4. Unique PSK(UPSK)機能

通常の PSK では 1 つの SSID に対して 1 つのパスワードとなりますが、UPSK によって同じ SSID でもデバイスごとに複数のパスワードが設定できるようになります。



※本機能を利用するには、別途 NAC(Network Access Control)サーバーが必要となります。

サードパーティとして、Cisco ISE、Aruba Clearpass 等との連携に対応しております。

また、ランダム/ ローカライズされた MAC アドレスを使用するクライアントでは、UPSK は未サポートです。

### 【UPSK のユースケース】

#### ●新入生のオンボーディング

1. 新入生が、デフォルトの PSK（管理者が共有）でログイン
2. デバイスの MAC アドレスを Radius に登録するためのポータルサイトにリダイレクト
3. MAC アドレスを登録後、学生はデバイス用に自動生成された、または管理者が設定した UPSK を取得
4. 学生は UPSK を使用して Wi-Fi にログインし、学生のネットワークにアクセス

類似機能としては、PPSK 機能がありますが、PPSK は AIRRECT Cloud のみで設定が可能です。

PPSK との差分は、PPSK は複数のグループの PSK を作成するのに対し、UPSK はデバイス一台ごとに効率よく異なるパスワードを設定することができます。

## 5. キャプティブポータルの認証プラグインに SAML 方式、OpenID Connect 方式を追加

サードパーティの SAML/OpenID Connect システムと AIRRECT Cloud を連携することで、SAML/OpenID Connect サーバーで登録しているユーザー名、パスワードで SSID にログインできる仕組みを搭載しました。

Okta社 設定UI

ユーザー名/パスワードが一致しており、且つシステムで登録されているユーザがログイン可能

## 6. クラウド設定情報のチェックポイント機能(保存、復元、比較)

現時点(チェックポイント)の AIRRECT Cloud 設定項目の保存・復元が可能となります。

それにより、設定変更後に不具合等が発生した際に、元の設定に戻したり、保存したチェックポイントの項目差分を確認することができます。

チェックポイントを作成

カスタム・ポリシー、デバイス設定、SSIDプロファイルなどの設定を保存するためのチェックポイントを作成します。

チェックポイント名

初期設定

説明

2023年5月のネットワーク環境

キャンセル

作成

チェックポイントは、差分比較を実施するとツリー表示され、異なる設定の特長ごとに背景色で示されます。

チェックポイントを比較

2個の差分が見つかりました。

設定変更1

デバイス設定1

configs: {  
 globalPolicies: { }  
 locationConfigsTree: { }  
 type: globalcheckpointconfig  
}  
referencedFileConfigs: []  
referencedInheritedConfigs: []  
}

customDeviceSettings: {}  
policies: {  
 AP\_LIST\_LOCKING\_POLICY: { }  
 BLE\_SETTINGS: { }  
 CLIENT\_LIST\_LOCKING\_POLICY: { }  
 DEVICE\_CONFIG: {  
 applyToExistingDevices: true  
 defaultTemplateId: 18  
 policyCreatedAtLocId: {  
 id: S1  
 type: locallocationid  
 }  
 policyType: DEVICE\_CONFIG  
 }  
 DEVICE\_UPGRADE: { }  
}

profiles: { }

customDeviceSettings: {}  
policies: {  
 AP\_LIST\_LOCKING\_POLICY: { }  
 BLE\_SETTINGS: { }  
 CLIENT\_LIST\_LOCKING\_POLICY: { }  
 DEVICE\_UPGRADE: { }  
 EVENT\_ACTIVATION\_POLICY: { }  
 INTRUSION\_PREVENTION\_ACTIVATION: { }  
 LOC\_NAMED\_VLANS\_POLICY: { }  
 LOCATION\_THRESHOLD: { }  
 LOCATION\_TIMEZONE: { }  
}

チェックポイントは3種類があり、それぞれ以下の設定が保存可能です。

- 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 設定などを保存する。
- 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する。
- 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を全ての設定を保存する。  
グローバルチェックポイントは、比較用であり復元はできない。

制限事項: 1. Captive portal(ゲスト WiFi 設定)は保存できません。

- 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なくなります。

※メジャーアップデートのみに適用されます。復元はできませんが、設定項目の比較は可能です。



## 7. クラウド管理画面の UI、デザインの改善

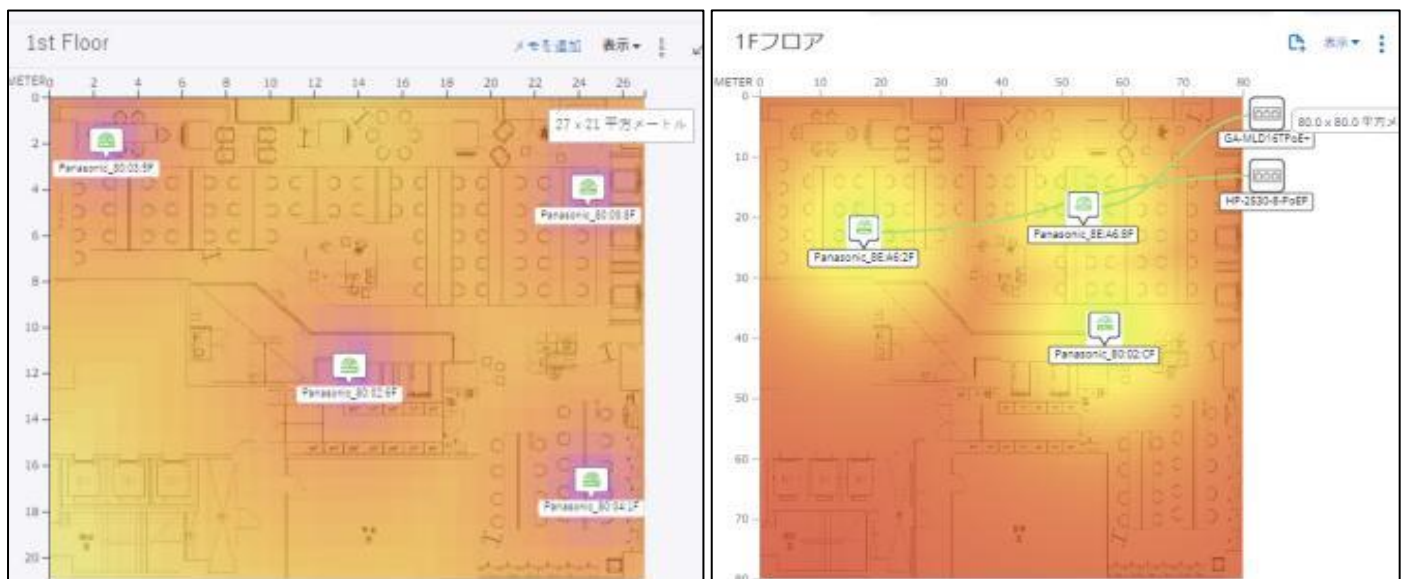
視認性をアップさせる目的で、画面解像度の向上、Web UI のフォント/アイコンデザイン等が変更となりました。操作性については、今までと変更ありません。

[デザイン比較 画面例]

●ダッシュボード 上：旧デザイン、下：新デザイン



●ヒートマップ 左：旧デザイン、右：新デザイン



## 8. フロアプランにスイッチ情報を表示する機能

フロアプラン外に、アクセスポイントと接続されているスイッチが表示されるように機能拡張したことにより、ネットワークポロジの確認がより効率的に行えるようになります。

### ●リンク状況が色で判断可能：

アクセスポイントがアクティブであれば緑色、非アクティブとなったら、赤色となる

### ●接続のステータス状況（リンク速度、電源、ポート情報など）の確認が可能

The screenshot displays a floor plan of the 1st floor (1Fフロア) with a grid from 0 to 80 meters. Various network devices are plotted, including access points (Panasonic\_8E:A6:2F, Panasonic\_8E:A6:8F, Panasonic\_80:02:CF) and switches (GA-MLD16TPoE+, GA-ML16TPoE+). A red box highlights the Panasonic\_80:02:CF access point, and a red arrow points from it to a detailed status popup window.

画面のアクセスポイントを選択

ステータス	非アクティブ
名前	Panasonic_80:02:CF
モデル	AP-6810
更新	デバイスのファームウェアは最新です
MACアドレス	BC:69:CB:80:02:CF
IPアドレス	10.0.1.21
代替IP	—
ビルド	13.0.2-28.39
切断日時	16:17
最終起動日	15:37
グループ	—
リンク速度	1 Gbps
電源	PoE+
接続しているポート	Gi1/0/3

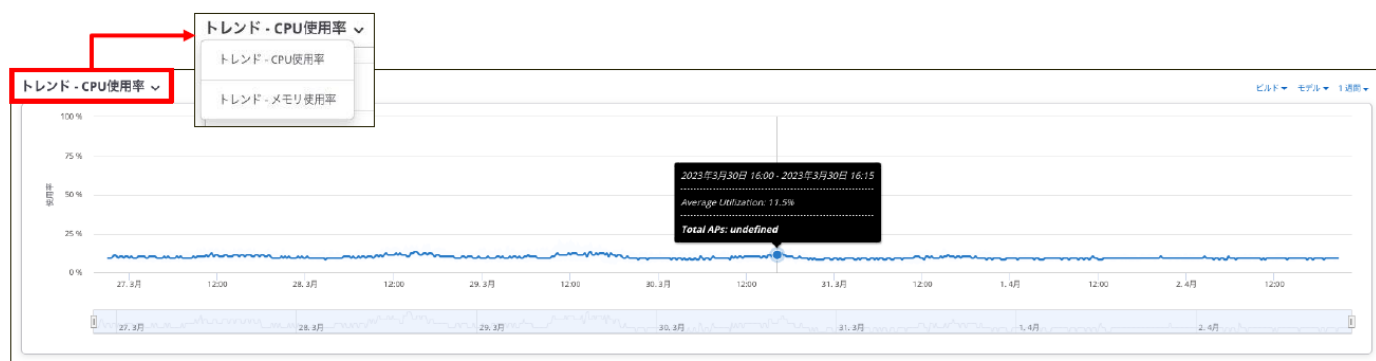
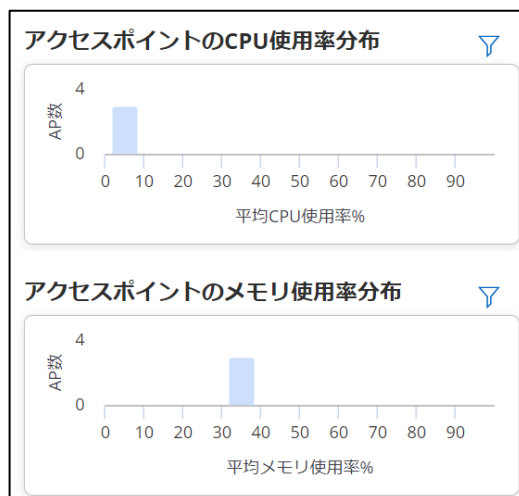
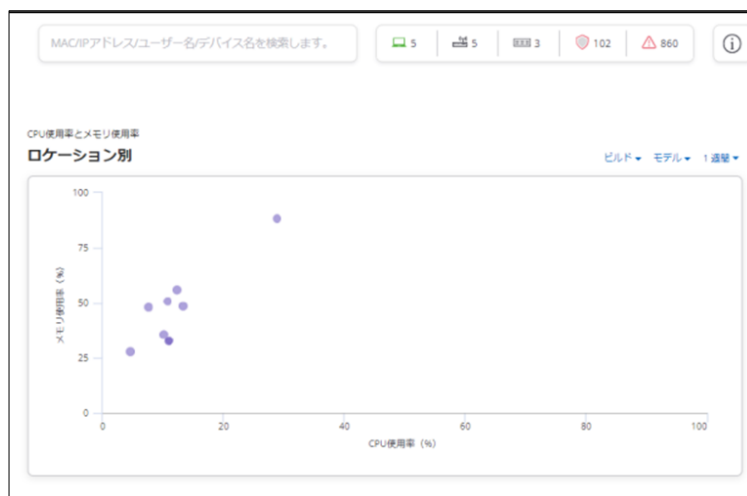


## 9. アクセスポイントのステータス統合表示機能

Ver12 以前は CPU 使用率、メモリ使用率等のハードウェアの健全性は個々のアクセスポイントに確認が必要でしたが、一元表示可能なグラフで表示される、インフラストラクチャタブがダッシュボードに追加されました。

各ロケーションごとの情報を集約し、以下のチャートを表示が可能です。

- アクセスポイント単位でのチャート
- ロケーション単位でのチャート
- CPU/メモリ使用率単位でのグラフ
- CPU/メモリ利用率のトレンド



## 10. クライアントイベントログの統合管理機能

Ver12 以前は、クライアントイベントログは[モニター]>[クライアント]から、任意のクライアント選択をするなどして、各クライアント単位でしか可視化ができませんでしたが、特定のロケーション等の単位で一括閲覧が可能となりました。それにより、問題のある端末やネットワークの接続傾向などが効率よく確認可能となります。

時刻 ↓	MACアドレス	イベント	AP名	BSSID	SSID
2023年4月27日 14:58:09.603	4A:2B:4F:21:71:CA	成功	Panasonic_8E:A6:2I	bc:69:cb:8e:a6:11	empl
2023年4月27日 14:56:02.196	4A:2B:4F:21:71:CA	[IPアドレス] クライアントがIPアドレス 10.0.1.50 を受信しました。	Panasonic_8E:A6:2I	bc:69:cb:8e:a6:11	empl
2023年4月27日 14:56:02.189	4A:2B:4F:21:71:CA	[IPアドレス] クライアントがIPアドレス fe80::34:80a5:5fa0:c755 を受信し...	Panasonic_8E:A6:2I	bc:69:cb:8e:a6:11	empl
2023年4月27日 14:56:02.095	4A:2B:4F:21:71:CA	[VLAN] クライアントにVLAN 0が割り当てられています	Panasonic_8E:A6:2I	bc:69:cb:8e:a6:11	empl
2023年4月27日 14:55:56.218	5A:A4:A0:0D:FD:03	成功	Panasonic_8E:A6:2I	bc:69:cb:8e:a6:02	empl
2023年4月27日 14:55:56.211	5A:A4:A0:0D:FD:03	[DNS] クライアントは、IPv4 DNSクエリに対する応答を正常に受信しまし...	Panasonic_8E:A6:2I	bc:69:cb:8e:a6:02	empl
2023年4月27日 14:55:56.060	5A:A4:A0:0D:FD:03	[IPパケット] クライアントは、IP10.0.1.48を使用して開始しています。	Panasonic_8E:A6:2I	bc:69:cb:8e:a6:02	empl
2023年4月27日 14:55:53.314	5A:A4:A0:0D:FD:03	[IPアドレス] クライアントがIPアドレス 10.0.1.48 を受信しました。	Panasonic_8E:A6:2I	bc:69:cb:8e:a6:02	empl
2023年4月27日 14:55:53.214	5A:A4:A0:0D:FD:03	[IPアドレス] クライアントがIPアドレス fe80::1c1d:d8bf:86cb:37fa を受信...	Panasonic_8E:A6:2I	bc:69:cb:8e:a6:02	empl

## 11. クライアントエクスプローラー機能

現在接続中、または WIPS で検出されたクライアント情報をグラフィカルに表形式で表示可能です。  
フィルター機能も搭載されているため、管理者は該当するクライアント情報とその総数の把握が容易になった。

### ●フィルター機能

Wi-Fi クライアント：接続中 AP 名、接続中 SSID 名、周波数帯、チャンネル、プロトコル、ベンダー名、OS、  
Google 認証状況、ロール適用状況、接続不良の種類

WIPS クライアント：接続中 AP 名、接続中 SSID 名、周波数帯、チャンネル、プロトコル、ベンダー名、  
グループ名

設定を行う項目の手順の仕様が以下の通り変更となります。



## 12. キャプティブポータルのゲストブック機能の改善

Ver12.0.1 以前は、ゲストブックの設定をした後に編集したい場合、再度該当の SSID の編集画面で、再設定を行う必要がありました。ゲストブック機能自体を、SSID の編集画面に加えてメニュー画面からも一括管理できるように改善することで、効率的にゲストユーザー管理ができるようになります。

また、以前は英語表記のみ対応でしたが、日本語にも対応しました。

編集するゲスト情報の  
SSID 選択を行える

ステータス	電子メール・ステータス	バッチID	SMSステータス	作成日付	から有効	まで有効
Guest Wi-Fi2 [ Guest Wi-Fi2 ]	バッチ	--	--	5月 15, 2023 18:18	5月 15, 2023 18:18	5月 16, 2023 18:18
Guest Wi-Fi1 [ Test Captive S2 ]	バッチ	--	--	5月 15, 2023 18:18	5月 15, 2023 18:18	5月 16, 2023 18:18
Test Userb	バッチ	--	--	5月 15, 2023 18:18	5月 15, 2023 18:18	5月 16, 2023 18:18
Test Userp	バッチ	--	--	5月 15, 2023 18:18	5月 15, 2023 18:18	5月 16, 2023 18:18
Test Userj	バッチ	--	--	5月 15, 2023 18:18	5月 15, 2023 18:18	5月 16, 2023 18:18
Test Userrr	バッチ	--	--	5月 15, 2023 18:18	5月 15, 2023 18:18	5月 16, 2023 18:18
Test Userc	バッチ	--	--	5月 15, 2023 18:18	5月 15, 2023 18:18	5月 16, 2023 18:18
thomyjrLD...	個別	--	--	5月 15, 2023 18:18	5月 15, 2023 18:18	5月 16, 2023 18:18
lgx7zdugnBv...	個別	--	--	4月 26, 2023 13:52	4月 26, 2023 13:52	4月 27, 2023 13:52
lgvni14ox3...	個別	送信済み	--	4月 25, 2023 11:32	4月 25, 2023 11:31	4月 26, 2023 11:31

## 13. WIPS のデバイスインポート機能

WIPS 機能において、認定アクセスポイント、不正アクセスポイント等の設定は今までは Web UI から個々に行う必要がありましたが、CSV で一括インポートすることができ作業効率化が図れるようになりました。

①テンプレートのダウンロード

A	B	C	D	E
*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。				
*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。				
*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。				
*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。				
*区切り記号の有無にかかわらず空白行は無視されます。				
MAC Address	IP Address	Device Name	Location	Location Name
aa:bb:cc:dd:ee:f1	192.168.8.180	Device 1	-1	//AIRRECT Cloud/Staging Area
aa:bb:cc:dd:ee:f1	192.168.8.180	Device 1	0	//AIRRECT Cloud
aa:bb:cc:dd:ee:f1	192.168.8.180	Device 1	49	//AIRRECT Cloud/宇都宮支社
aa:bb:cc:dd:ee:f1	192.168.8.180	Device 1	50	//AIRRECT Cloud/宇都宮支社/1Fフロア
aa:bb:cc:dd:ee:f1	192.168.8.180	Device 1	51	//AIRRECT Cloud/東京本社
aa:bb:cc:dd:ee:f1	192.168.8.180	Device 1	52	//AIRRECT Cloud/東京本社/1Fフロア

②編集/インポート

14. BSSID 検索/表示機能の改善

グローバルサーチの検索バーと、各アクセスポイントの詳細画面からBSSID 情報を確認可能となりました。今までは、[モニター]>[アクセスポイント]の一覧画面にある SSID タブからしか確認不可であったため、検索効率化が出来るようになります。

【アクセスポイント詳細画面】



【グローバルサーチ画面】



Panasonic\_8E:A6:8F

10 BSSIDs

ステータス	BSSID	周波数帯	Wi-Fi規格	アソシエーション件数	Tx.電力 (dBm)	SSID	セキュリティ
	BC:69:CB:8E:A6:60	5 GHz	WIFI 6	6	23	employee_wifi	WPA3, WPA2
	BC:69:CB:8E:A6:61	5 GHz	WIFI 6	1	23	S_test	WPA3, WPA2
	BC:69:CB:8E:A6:70	2.4 GHz	WIFI 6	0	23	employee_wifi	WPA3, WPA2
	BC:69:CB:8E:A6:71	2.4 GHz	WIFI 6	0	23	S_test	WPA3, WPA2
	BC:69:CB:8E:A6:62	5 GHz	WIFI 6	0	23	Home Wi-Fi	WPA3, WPA2
	BC:69:CB:8E:A6:63	5 GHz	WIFI 6	0	23	VLAN840	WPA2
	BC:69:CB:8E:A6:64	5 GHz	WIFI 6	0	23	Guest WIFI	Open
	BC:69:CB:8E:A6:65	5 GHz	WIFI 6	0	23	Test	Open
	BC:69:CB:8E:A6:72	2.4 GHz	WIFI 6	0	23	Home Wi-Fi	WPA3, WPA2
	BC:69:CB:8E:A6:73	2.4 GHz	WIFI 6	0	23	VLAN840	WPA2

## 15. NAC クラスター設定における CoA リクエストの許可機能

Ver.12 以前は RADIUS サーバーとして設定している IP からの CoA リクエストしか処理できませんでしたが、RADIUS サーバーとして設定していない IP アドレスからのリクエストでも処理が可能となりました。

※CoA : Change of Authorization の略。RADIUS プロトコルを利用して、認証後のネットワーク接続に対して、アクセス制御情報を変更するための機能。CoA リクエストは、NAC クラスター内の NAC 装置が、CoA リクエストを受け取った場合に、他の NAC 装置にも同じアクセス制御情報の変更を要求するもの。

☒ 承認の変更 (CoA)

追加のCoAサーバーIPアドレス

## 16. RADIUS ダイナミックリダイレクト機能

ロールプロファイル設定にて、RADIUS 認証成功後、認証済端末を管理者が指定した URL へリダイレクトさせることが可能となります。(リダイレクト先設定は Radius サーバーにて指定します。また、同 Web サイトをワールドガーデンリストに事前登録が必要です。)

ネットワーク・プロファイル ▾ **ロールプロファイル**

このロール・プロファイルに変更すると、このロール・プロファイルを使用するすべてのSSIDに影響

← roll test

☒ リダイレクト

☐ 静的リダイレクト ☒ 動的リダイレクト

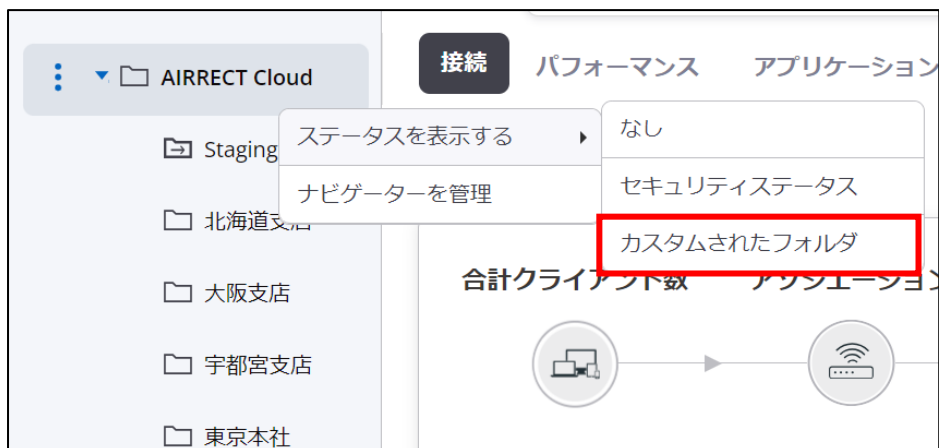
☐ HTTPSリダイレクト



承認前にアクセスできるWebサイト \*

panasonic.co.jp:80,443 ✕

## 17. カスタマイズされたロケーションフォルダの表示機能

フォルダのカスタマイズ設定をした場合、以前はどのフォルダがカスタマイズされており、どのフォルダがルートフォルダを継承しているかが設定したかが分かりにくい問題がありました。本アップデートにより、カスタマイズした項目が色分けされ一目で分かるように改善されました。

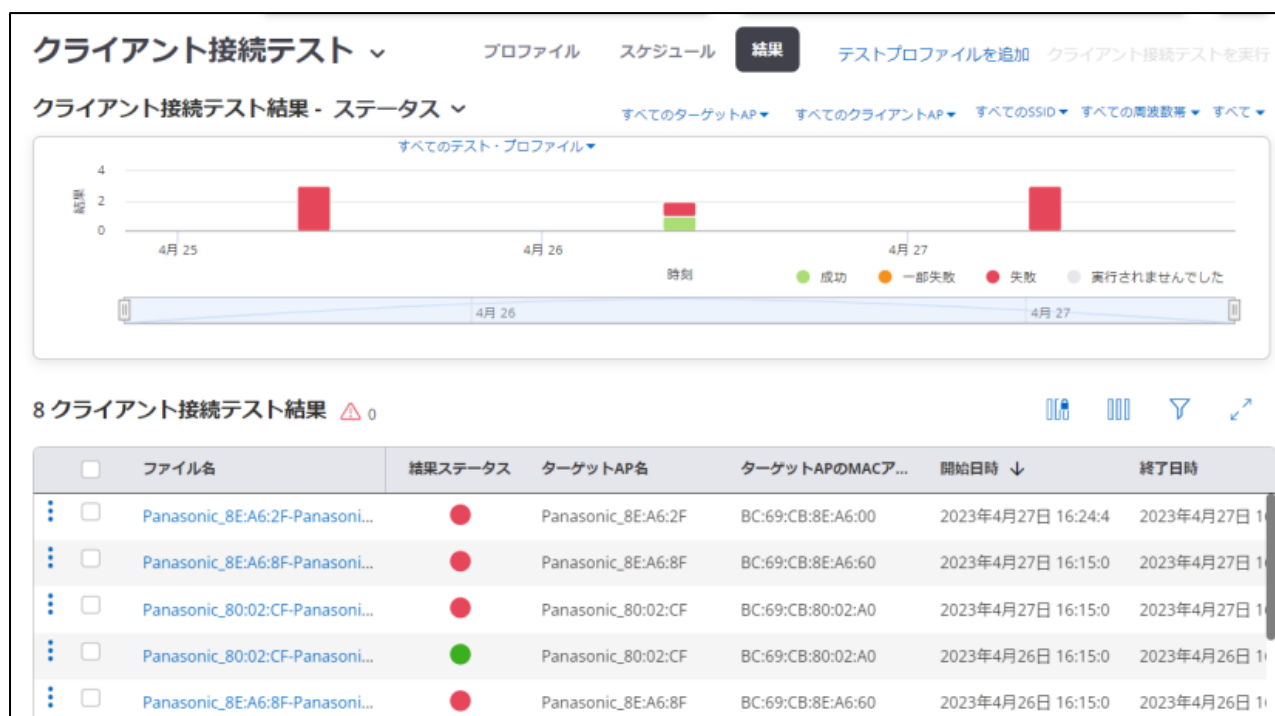


-  ...カスタマイズされたロケーション
-  ...上位フォルダの設定を継承



## 18. クライアント接続テストに結果パラメータ表示機能

アクセスポイント間で通信試験を行うクライアント接続テストにおいて、結果のサマリー表示画面しました。これにより、遅延時間やスループット等の状態推移によるトラブルシューティングの効率化ができます。



## 19. Wi-Fi レポート機能拡張（「クライアント特性」「WiFi 無線」）

以下の二種類のレポートを追加しました。

### 1. 「クライアント特性」レポート

- ・接続している Wi-Fi 規格、周波数帯のサマリー
- ・クライアント情報詳細

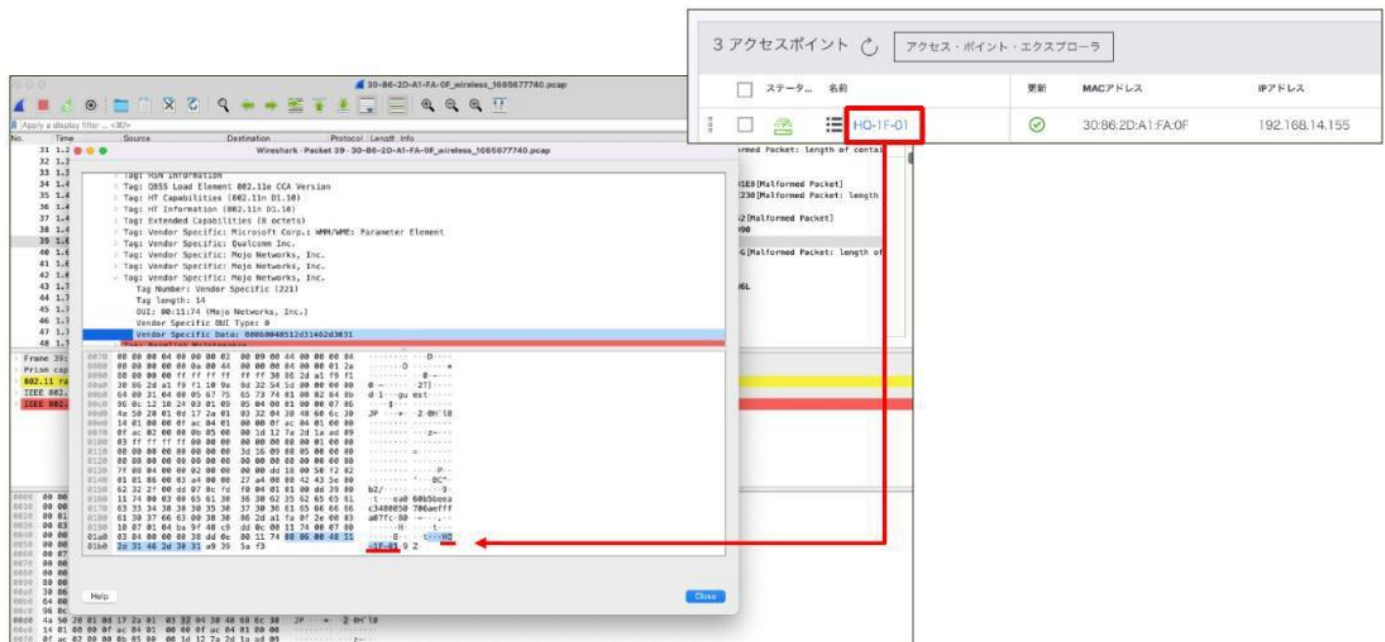
### 2. 「WiFi 無線」レポート

- ・2.4GHz および 5GHz 帯で動作するアクティブな SSID リスト表示
- レポートメニューだけでなく、[モニター]>[WiFi]>[無線通信]からもダウンロード可能

## 20. ビーコンにアクセスポイント名の表示機能

ビーコンにアクセスポイント名を付加することが可能になったことにより、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、アクセスポイントの特定、識別が容易になる。

※専用ソフト(WireShark など)を使用した場合のみ、ユーザーはビーコン(AP 名)を認識可能。



## 20. 設定メニューの項目の最適化

設定を行う項目の手順の仕様が以下の通り変更となります。

設定項目	現在 (v12.0.1)	ver.14
Radius	左メニュー[構成]>[WiFi]>[Radius]タブ	左メニュー[構成]>[ネットワークプロファイル]>[Radius]タブ
トンネルインターフェース	左メニュー[構成]>[WiFi]>[トンネルインターフェース]タブ	左メニュー[構成]>[ネットワークプロファイル]>[トンネルインターフェース]タブ
ロールプロファイル	左メニュー[構成]>[WiFi]>[ロールプロファイル]タブ	左メニュー[構成]>[ネットワークプロファイル]>[ロールプロファイル]タブ
無線通信設定	左メニュー[構成]>[WiFi]>[無線通信]タブ	左メニュー[構成]>[デバイス]>[アクセスポイント]>[WiFi無線]タブ
デバイス	左メニュー[構成]>[デバイス設定]>[デバイス]タブ	左メニュー[構成]>[デバイス]>[アクセスポイント]>[全般的]タブ
セキュリティ (WIPS)	左メニュー[構成]>[デバイス設定]>[セキュリティ]タブ	左メニュー[構成]>[デバイス]>[アクセスポイント]>[セキュリティ]タブ
レポート - インベントリ	左メニュー[レポート]>[インベントリ]タブ	左メニュー[レポート]>[WiFi]>[インベントリ]タブ
レポート - WIPS	左メニュー[レポート]>[WIPS]タブ	左メニュー[レポート]>[WIPS]>[ポリシー適用]タブ
レポート - アラート	左メニュー[レポート]>[アラート]タブ	左メニュー[レポート]>[アラート]
レポート - コンプライアンス	左メニュー[レポート]>[コンプライアンス]タブ	左メニュー[レポート]>[コンプライアンス]
レポート - クライアント	左メニュー[レポート]>[クライアント]タブ	左メニュー[レポート]>[WiFi]>[接続]タブ
レポート - アーカイブ済み	左メニュー[レポート]>[アーカイブ済み]タブ	左メニュー[レポート]>[More]>[保存]
レポート - スケジュール済み	左メニュー[レポート]>[スケジュール済み]タブ	左メニュー[レポート]>[More]>[スケジュール]
レポート - アナリティクス	左メニュー[レポート]>[アナリティクス]タブ	-

## 21. 設定メニューの項目の最適化

AIRRECT Cloud のログインパスワードのポリシー強度が変更となりました。

- ・少なくとも 1 つ以上の小文字が含まれること
- ・少なくとも 1 つ以上の数字が含まれること

※以下は以前よりあったポリシー

- ・パスワードの最小文字数は 8 文字
- ・少なくとも 1 つの大文字を含むこと
- ・少なくとも 1 つの特殊文字を含むこと
- ・ユーザー名、ファーストネーム、ラストネームを含まないこと
- ・パスワードの強度は十分でなければいけないため、推測可能な単語や文字列を含むことは不可

尚、今まで利用してたパスワードは変更せずに利用可能です。

## 22. セキュリティポリシーチェックのバー表示機能

AIRRECT AP の CLI パスワード、SSID のパスフレーズキー入力時に「弱」「中」「良」「強」の 4 段階で表示されるようになりました。

※AIRRECT Cloud へのログイン以外は、高いセキュリティポリシーでのパスワード設定は強制ではありません。

「弱」であっても設定は可能です。

☐ アクセスポイントを専用WIPSセンサーに変換

デバイスのパスワード

パスワード・ポリシー

ユーザー名

config

パスワード\*

.....

👁

パスワードの確認\*

.....

👁

有効なパスワードは以下の通りです。

- 最低9文字、最大32文字
- 1文字以上の大文字が必要
- 1文字以上の特殊文字 (!@#\$%^&\*()=+{};:;<>~`\_/. ) が必要
- よく使われる語句や英数字の並びを含めることはできません

強