NEC

自律型APモード設定ガイド

NA1000W/NA1000A

はじめに

このガイドは、自律型 AP モードでの本商品の設定方法および設定内容について詳しく説明します。

このモードは、機器の追加に制約のある既存システムへ、本商品を組み込む場合を想定したモードです。

自律型 AP モードの場合、本商品は、接続している有線ネットワークを経由してクライアントの無線接続を可能にするアクセスポイント(AP)として機能します。このモードでは、アクセスポイント(AP)はサーバーに接続しません。有線ネットワークに接続された独立デバイスとして動作し、この有線ネットワークを拡張します。

自律型 AP モードでのアクセスポイント(AP)動作

本商品が管理コンソールサーバーに接続して通信するモードを集中管理型 AP モードまたはセンサーモードと言います。集中管理型 AP モードまたはセンサーモードの場合、本商品は管理コンソールサーバーからそのコンフィグレーション設定を受け取ります。

ご注意：本商品を集中管理型 AP モードまたはセンサーモードでご利用になるには、別売りの管理コンソール（Management Console）が必要です。管理コンソール（Management Console）が無い場合は、自律型 AP モードのみのご利用となります。

また、本商品が管理コンソールサーバーに接続しないで、クライアントの無線接続を可能にするモードを自律型 AP モードと言います。自律型 AP モードに入る時は、はじめに適用された最後のコンフィグレーション設定を保存します。これらは、前に接続し通信していた管理コンソールサーバーから受信されたものです。本商品を集中管理型 AP モードまたはセンサーモードに変更した場合、または自律型 AP モードのアクセスポイント(AP)に新しいコンフィグレーション設定を適用するまで、これらのコンフィグレーション設定が利用されます。

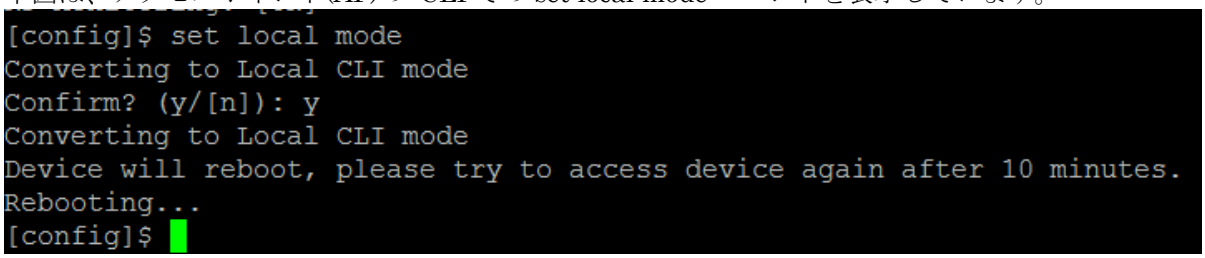
モードの変更は、本商品のコマンドラインインタフェース(CLI)によって行われます。本商品の CLI にログインし、[アクセスポイント(AP)に新しいコンフィグレーション設定を適用し、現在のコンフィグレーション設定を取得するために］モードを変更するそれぞれのコマンドを実行できます。本商品の CLI のデフォルトのユーザー認証は config（ユーザー名）と config（パスワード）です。デフォルトのユーザーを変更している場合は、CLI にログインするためにそれぞれの認証を使用します。

ご注意：CLI にログインするためのパスワードは必ずデフォルトから変更してください。

アクセスポイント(AP)を自律型 AP モードへ設定

集中管理型 AP モードまたはセンサーモードから自律型 AP モードにアクセスポイント(AP)のモードを変更するには、set local mode コマンドを使用します。モードが変更されたあとにデバイスが再起動します。

下図は、アクセスポイント(AP)の CLI での set local mode コマンドを表示しています。



自律型 AP モード用のコンフィグレーション設定を定義

自律型 AP モードのアクセスポイント(AP)に新しいコンフィグレーション設定を適用するために、set ap config コマンドを使用します。手動または通常のテキストファイルを使って新しい設定を適用できます。
ご注意：コンフィグレーションファイルまたは手動入力でのパラメータの値は 512 文字以下です。513 文字以上は任意の値が切り捨てられ、それに対応する機能が正しく動作しない可能性があります。パラメータ名と値の間にスペース、タブまたはその他の文字は入れないでください。
下記は、'AP_SSID' のパラメータとして 'test' を指定する場合の例です。
AP_SSID=test
コンフィグレーション設定が set ap config コマンドを経由して適用されると、デバイスは再起動されアクセスポイント(AP)に新しいコンフィグレーション設定を適用します。コンフィグレーション設定は、ラジオ設定、VAP 設定とグローバル設定で構成されています。VAP 設定は、SSID プロファイル設定、セキュリティ設定、ネットワーク、QoS 設定、ホットスポット 2.0 設定などを含みます。グローバル設定は、運用国、アンテナ情報、VLAN ID などの詳細情報を含みます。

下図は、テキストファイルを使用して、新しいコンフィグレーション設定の適用を表示しています。

```
[config]$ set ap config
Set AP config
Gets the AP configuration for Local CLI mode.

Select the method:
1. Save configuration through command prompt
2. Upload configuration from a URL
3. Exit
?
2
Enter the URL to download the configuration file: http://192.168.55.114/sensorim
ages/ap_conf_shailesh.txt
File saved
Rebooting...
```

下図は、set ap config コマンドを使用して新しいコンフィグレーション設定を手動入力する画面です。この画面が表示されたら、コンフィグレーションファイルのサンプルに記載された形式にしたがって、設定値を入力してください。

```
[config]$ set ap config
Set AP config
Gets the AP configuration for Local CLI mode.

Select the method:
1. Save configuration through command prompt
2. Upload configuration from a URL
3. Exit
?
1
Enter the AP configuration file contents:

Press '[Enter] [Ctrl + D] [Ctrl + D]' to exit the file
```

【ラジオ設定（Radio Settings）】

ラジオ設定は、無線関連のパラメータが含まれています。アクセスポイント(AP)が 2 つの無線を持っている場合、両方のラジオ設定をコンフィグレーションする必要があります。1 番目のラジオ設定は、[RADIO_START]

で始まり、 [RADIO_END]で終わります。アクセスポイント(AP)として機能できる無線が管理デバイス(Management Device)上に 2 つあります。2 番目のラジオ設定は、［RADIO_START=2］で始まり［RADIO_END=2］で終わります。
ラジオ設定セクションの内容は次のように表示されます。

```
[ RADIO_START ]
//Configuration parameters for radio settings
[ RADIO_END ]
```

次の表では、ラジオ設定について説明します。

パラメータ	説明	指定可能な値
WIRELESS_MODE	動作の周波数帯域 ユーザーは、IEEE802.11nまたはIEEE802.11acを有効に指定することも可能。	0（IEEE802.11b on 2.4GHz） 1（IEEE802.11g/b on 2.4GHz） 2（IEEE802.11a on 5GHz） 3（IEEE802.11n/g/b on 2.4GHz） 4（IEEE802.11n/a on 5GHz） 5（IEEE802.11ac/n/a on 5GHz）
AP_CHAN_WIDTH	無線のチャネル幅。 可能な値は、20MHzまたは20MHz/40MHzです。a/ n/ acデバイスの場合には、20/40/80 MHzが利用可能です。	1（20MHz） 2（40MHz） 3（80MHz）（11acのみ適用可能）
OP_CHANNEL	無線の動作チャネル。 デフォルトでは、自動的にチャネルを選択します（Auto）。手動で希望するチャネルを選択することもできます。手動で選択されたチャネルが周囲に存在しない場合、アクセスポイント(AP)は自動的にAutoモードに戻りチャネルを選択します。	0は自動チャネルを意味します。 それ以外は、設定モード(5GHz/2.4GHz)固有のチャネル番号です。 デフォルト値：0
FRAG_THRESH	フラグメンテーション閾値（バイト単位）。 このフィールドの許容値は、256～2346バイトです。このフィールドは、5GHz帯と2.4GHz帯のモードで適用可能です。	256～2346の値。 デフォルト値： 2346
RTSCTS_THRESH	RTS（Request to Send）閾値（バイト単位）。 アクセスポイント(AP)が送信にRTS/CTSハンドシェイクを使う必要があるフレームのサイズ以上の閾値を指定。このフィールドは、5GHz帯と2.4GHz帯のモードで適用可能です。 **ご注意：**閾値が非常に小さな値に設定されている場合は、無線チャネルが効率的に利用されません。この閾値は、ラージフレームに使用されます。	256～2347の値。 デフォルト値： 2347
BEACON_INT	アクセスポイント(AP)のビーコン送信間隔（ミリ秒単位）。	20～1000の値。 デフォルト値： 100
DTIM_PERIOD	DTIM（Delivery Traffic Indication Map）ピリオドの値は、ビーコンフレームにDTIMが含まれる頻度を決める数です。この数は各ビーコンフレームに含まれます。 DTIMは、アクセスポイント(AP)がブロードキャストまたはマルチキャストデータをバッファリン	1～10の値。 デフォルト値： 1

	グしているかどうかをクライアントデバイスに知らせるために、（DTIMピリオドに応じて）ビーコンフレームに含まれています。いずれかが存在する場合は、DTIMを含むビーコンフレームに続いて、アクセスポイント(AP)はバッファされたブロードキャストまたはマルチキャストデータを放出します。	
SHORT_GI	各OFDMシンボルの終わりから次の信号を送信するまでにかかる期間。これは、2つの連続するシンボル間の重複を防ぎます。従来のIEEE802.11a/g/bデバイスは、800nsのGIを使用します。400nsのGIは、IEEE802.11nのオプションです。このフィールドは、IEEE802.11n/ac固有です。	0（Full） 1（Half） デフォルト値： 1
AMPDUENABLE	フレームアグリゲーションの有効： このフィールドは、MPDU（MAC Protocol Data Unit）アグリゲーションの有効/無効を指定します。このフィールドは、IEEE802.11n/ac固有です。IEEE802.11ac無線の場合、フレームアグリゲーションはデフォルトで有効になっており、それを無効にすることはできません。	0（Disabled） 1（Enabled） デフォルト値： 1
AP_TRANSMIT_POWER	AP_TRANSMIT_POWER_ENABLED = 1 の場合のみ、AP_TRANSMIT_POWERは有効になります。 **ご注意**：実際の送信電力は、以下のうち最も低いものとなります ・ここで指定した値 ・規制地域で許容される最大値 ・無線でサポートされる最大電力	0～30dBmの値。 デフォルト値： 30
AP_TRANSMIT_POWER_ENABLED	アクセスポイント(AP)送信電力のカスタムを有効にします。	0（ユーザーによるカスタム無効） 1（ユーザーによるカスタム有効） デフォルト値： 0
BS_LOAD_BAL_THRESHOLD	バンドステアリング閾値： 5GHz帯のクライアントが2.4GHz帯のクライアントと設定された閾値を加算した数（すべてのSSID間でカウントされる）より少ない場合、新規のクライアントは5GHz帯に誘導されます。バンドステアリングがSSIDプロファイルで有効になっている場合のみ誘導が行われます。	0～50の値（クライアント数）。 デフォルト値： 10
NUM_OF_SPATIAL_STREAMS	無線の空間ストリーム数： アクセスポイント(AP)の無線通信における送受信の空間ストリーム数を設定します（ファームウェアバージョン1.3〈1.3.02〉以降に対応）。	1（1×1設定） 2（2×2設定） 3（3×3設定） デフォルト値： 3

【VAP 設定（Virtual AP Settings）】

物理的なアクセスポイント(AP)を、仮想 AP（VAP）に分けることができます。各 VAP は同一物理 AP 上の他の仮想 AP によって提供されるサービスに干渉しないで、独立したサービスを提供し異なる VLAN をサポートできます。

VAP のコンフィグレーション設定は、SSID プロファイルを経由して行われます。複数の SSID プロファイルをアクセスポイント(AP)に構成できます。1 つの SSID プロファイルを、アクセスポイント(AP)の任意の無線、または両方の無線に適用できます。各アクセスポイント(AP)の無線は、最高 8 つの SSID プロファイルのサポートができます。

両方の無線に同じ設定、または各無線に別の設定を適用できます。したがって、単一の物理 AP は、2 つの無線のそれぞれに最大 8 つの VAP に異なる設定が適用された場合、16VAP までの要求を満たすことができます。N 番目の VAP セクションは [VAP_START= N] で始まり、基本設定、セキュリティ設定、ネットワーク設定、ファイアウォール設定、キャプティブポータル設定、トラフィックシェーピングと QoS 設定、ホットスポット 2.0 設定のコンフィグレーションパラメータが続きます。セクションは [VAP_END= N] で終わります。

コンフィグレーションファイルの VAP セクションは、以下のとおりです。

```
[ VAP_START=N ]
//Configuration parameters for basic settings
//Configuration parameters for security settings
//Configuration parameters for network settings
//Configuration parameters for firewall settings
//Configuration parameters for captive portal settings
//Configuration parameters for traffic shaping and QoS settings
//Configuration parameters for Hotspot 2.0 settings
[ VAP_END=N ]
```

VAP セクションを構成する各コンフィグレーションパラメータを見てみましょう。

基本設定（Basic Settings）

基本設定は SSID ID、名前、RSSI 閾値、バンドステアリングステータス、許可されるアソシエーション数などから構成されます。これらの設定は必須です。

次の表では、基本設定について説明します。

パラメータ	説明	指定可能な値
SSID_PROFILE_ID	SSIDプロファイルの一意のID	1～256
AP_SSID	クライアントが接続するSSIDまたはネットワーク	最大32文字の任意の名前。
HIDESSID_BROADCAST	ビーコンフレームで、この仮想APでSSIDをブロードキャストするか否かを示します。有効にすると、この仮想APのビーコンは、SSIDを搬送します。	0（ビーコンでSSIDブロードキャストする） 1（ビーコンでSSIDをブロードキャストしない）
WMM_ENABLE	無線マルチメディアのためにQoSを有効にします。	0 (Disabled) 1 (Enabled)
ISOLATION_ENABLE	この仮想APの2つの無線クライアント間でクライアントアイソレーションを許可または禁止するかどうかを示します。値が1の場合、仮想APの無線クライアント間通信は無効になります。	0 (Disabled) 1 (Enabled)
RADIO_ID	各SSIDプロファイルを、一方の無線または両方の無線に適用可能です。	1 (SSIDプロファイルを無線1に適用) 2 (SSIDプロファイルを無線2に適用) 1, 2 (SSIDプロファイルを両方の無線に適用)
BS_BAND_STEERING_ENABLED	バンドステアリングを有効にすることで、ロードバランシング閾値のクライアント数は、このSSIDプロファイルが適用される無線のコンフィグレーションで使用されます。	0（バンドステアリング無効） 1（バンドステアリング有効）
BS_RSSI_THRESHOLD	アクセスポイント(AP)での受信信号がこの閾値より強いクライアントが5GHz帯に誘導されます。	-75 ～ -55 dBm
ENABLE_LIMIT_ON_ASSOC	このVAPのクライアントアソシエーション数の制限を有効にします。	0 (Disable) 1 (Enable)
ASSOC_LIMIT	アクセスポイント(AP)に許可されるアソシエーション数。	0～127の値。

セキュリティ設定（Security Settings）

セキュリティ設定は、VAP に適用されるセキュリティタイプを指定します。WEP が適用されている場合、WEP 関連の設定値を持つパラメータを指定する必要があります。WPA または混合（Mixed）設定が適用されている場合も同様に、対応するパラメータを指定する必要があります。
認証方法が RADIUS の場合は、RADIUS 関連のパラメータに対応する値を指定する必要があります。RADIUS アカウンティングが有効になっている場合は、RADIUS アカウンティングパラメータに対応する値を指定する必要があります。

次の表では、セキュリティ設定について説明します。

パラメータ	説明	指定可能な値
AP_SEC_MODE	アクセスポイント(AP)のセキュリティモード。 次のいずれかの値を持ちます。 **Open**: Openはセキュリティ設定が適用されていないことを意味します。これはデフォルトのセキュリティ設定です。 **WEP**: WEPは Wireless Equivalent Privacy の略称です。WEPは、IEEE802.11ネットワークで推奨されないセキュリティアルゴリズムです。これは、下位互換性の目的でのみ提供されています。 **WPA2**: WPA2は、より堅牢なセキュリティプロトコルです。IEEE802.11i規格を実装しています。 **WPA and WPA2 mixed mode**: これは、WPAとWPA2プロトコルの混在を意味します。 デフォルト値：Open	0 (Open) 1 (WEP) 3 (WPA2) 4 (WPA and WPA2 mixed mode)
WEPセキュリティ用のフィールド		
AP_WEP_TYPE	WEPタイプ **WEP40** ：40bitのWEPセキュリティを使用する場合 **WEP104** ：104bitのWEPセキュリティを使用する場合	WEP40 (40-bit key) WEP104 (104-bit key)
AP_KEY_TYPE	WEPキータイプ **ASCII** ：ASCII形式でWEPキーを入力する場合 **HEX** ：16進形式でWEPキーを入力する場合	ASCII （キーはASCII形式） HEX （キーは16進形式）
AP_WEP_MODE	認証タイプがオープンの場合は、Openを選択します。その場合、キーは暗号化のためにだけ使われます。 認証タイプが共有鍵の場合は、Sharedを選択します。その場合、キーは暗号化と認証に使われます。	1 (Open) 2 (Shared)
AP_WEP_KEY	WFPキーは、連続する16進の数字または文字です。WEPタイプがWEP40の場合は、選択したキーの種類に応じて、5文字のASCIIキーまたは10桁の16進数キーとしてキーを入力してください。 WEPタイプがWEP104の場合は、選択したキーの種類に応じて、13文字のASCIIキーまたは26桁の16進数キーとしてキーを入力してください。	・ AP_WEP_TYPEがWEP40で、AP_KEY_TYPEがASCIIの場合は、キーは5文字にする必要があります。 ・ AP_WEP_TYPEがWEP40で、AP_KEY_TYPEがHEXの場合は、キーは10桁の16進数にする必要があります。 ・ AP_WEP_TYPEがWEP140で、AP_KEY_TYPEがASCIIの場合は、キーは13文字にする必要があります。 ・ AP_WEP_TYPEがWEP140で、AP_KEY_TYPEがHEXの場合は、キーは26桁の16進数にする必要があります。

WPA/ WPA2/ WPA and WPA2 mixed modeのセキュリティに関連するフィールド		
AP_SECFILE	2種類の認証方式をサポートしています。 PSKおよびRADIUS認証。	PSK (Passphrase key) EAP (IEEE802.1x authentication)
PSK_KEY	認証方式がPSKの場合、このフィールドは必須です。PSKまたはパーソナル用共有鍵は、一般的に小規模オフィスのネットワークに使用されます。	8～63文字。
RADIUS認証関連のフィールド		
NAS_IDENTIFIER	ネットワークリソースにアクセスする1つのポイントとしてネットワークアクセスサーバー(NAS)が用いられる場合に、このフィールドが使われます。一般的に、NASは同時に何百ものユーザーをサポートします。RADIUSクライアントがNASに接続すると、NASはRADIUSサーバーへアクセス要求パケットを送信します。 これらのパケットは、NASのIPアドレスまたはNAS識別子のいずれかを含める必要があります。NAS IDまたはNAS識別子は、RADIUSサーバーでRADIUSクライアントを認証するために使用されます。NAS IDの文字列を指定できます。デフォルト値は %m-%s (%mはアクセスポイント〈AP〉のイーサネットMACアドレス、%sはWLANのSSIDを表示しています) です。これは、RADIUSサーバー上のNAS識別子の属性に対応します。NAS識別子のRADIUS属性の属性IDは32です。NAS IDがRADIUS認証セクションでRADIUSサーバーに設定された共有鍵と同じでないことを確認してください。	可変の文字列。
IEEE802_1X_RETRY_TIMEOUT	RADIUSリトライ設定 (N秒タイムアウト後のリトライ)	1～10秒の値。
IEEE802_1X_MAX_RETRIES	RADIUSのリトライ回数。	1～10の値。
DYNAMIC_VLAN_ENABLED	VLANのRADIUSベースの割り当てを有効にするには、ダイナミックVLANを有効にする必要があります。	0 (Disabled) 1 (Enabled)
DYNAMIC_VLAN_LIST	RADIUSユーザーがリダイレクトできるダイナミックVLANのカンマ区切りのリスト。ユーザーグループに特定のVLANが存在しない場合、デフォルトのVLANが使用されます。	VLAN IDのカンマ区切りのリスト。各VLAN IDは、0～4094の範囲。 [0：スイッチ上のVLAN番号に関わらず、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。]
AP_AUTH_SERVER	プライマリRADIUS認証サーバーのIPアドレス	有効なIPアドレス。

AP_AUTH_PORT	プライマリRADIUS認証サーバーのポート番号	有効なポート番号。
AP_AUTH_SECRET	プライマリRADIUS認証サーバーの共有鍵	可変の文字列。
AP_AUTH_SERVER2	セカンダリRADIUS認証サーバーのIPアドレス	有効なIPアドレス。
AP_AUTH_PORT2	セカンダリRADIUS認証サーバーのポート番号	有効なポート番号。
AP_AUTH_SECRET2	セカンダリRADIUS認証サーバーの共有鍵	可変の文字列。
AP_ACCT_ENABLED	RADIUSアカウンティングを有効にします。 以下のフィールドはRADIUSアカウンティングが有効になっている場合にのみ有効です。	0 （アカウンティング無効） 1 （アカウンティング有効）
AP_ACCT_SERVER	プライマリRADIUSアカウンティングサーバーのIPアドレス	有効なIPアドレス。
AP_ACCT_PORT	プライマリRADIUSアカウンティングサーバーのポート番号	有効なポート番号。
AP_ACCT_SECRET	プライマリRADIUSアカウンティングサーバーの共有鍵	可変の文字列。
AP_ACCT_SERVER2	セカンダリRADIUSアカウンティングサーバーのIPアドレス	有効なIPアドレス。
AP_ACCT_PORT2	セカンダリRADIUSアカウンティングサーバーのポート番号	有効なポート番号。
AP_ACCT_SECRET2	セカンダリRADIUSアカウンティングサーバーの共有鍵	可変の文字列。

ネットワーク設定（Network Settings）

すべてのネットワーク固有のパラメータは、ネットワーク設定で指定します。

次の表では、ネットワーク設定について説明します。

パラメータ	説明	指定可能な値
AP_VLAN	VAPが動作するVLAN ID。	0～4094の範囲。 [0：スイッチ上のVLAN番号に関わらず、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。]
VAP_IS_GUEST_SSID	アクセスポイント(AP)およびアクセスポイント(AP)とアソシエイトするクライアントが同じサブネット内にいることが可能な場合にブリッジネットワークが使用されます。 同様に、アクセスポイント(AP)とクライアントを別のサブネットにしたい場合は、ネットワークアドレス変換（NAT）にする必要があります。 NATでは、クライアントはプライベートIPアドレスプールを持つことができ、パブリックIPアドレスを必要としないためネットワークに複数のクライアントを容易に追加できます。	0　(Bridged AP) 1　(NAT AP)
NAT関連のパラメータ		
DHCPD_LEASE_TIME	DHCPリース時間（分単位） 最小値30分、最大値1440分。	30～1440
DHCPD_LOCAL_IP	DHCPアドレスプール外の選択されたネットワークID内のIPアドレス。このアドレスは、ゲスト無線ネットワークのゲートウェイアドレスとして使用されます。	有効なIPアドレス。
DHCPD_START_IP	選択したネットワークIDのDHCPアドレスプールの開始IPアドレス。	有効なIPアドレス。
DHCPD_END_IP	選択したネットワークIDのDHCPアドレスプールの終了IPアドレス。	有効なIPアドレス。
DHCPD_SUBNET_MASK	選択したネットワークIDのネットマスク。	有効なサブネットマスク。
DNS_SERVER_LIST	無線クライアントがDNSクエリを行うことができるDNSサーバー。3つのDNSサーバーを指定できます。	有効なIPアドレスのスペース区切りのリスト。

ファイアウォール設定（Firewall Settings）

ファイアウォールの設定はオプションです。複数のファイアウォールルールをSSIDプロファイルに設定できます。SSIDプロファイル用に定義されたファイアウォールルールは、トップダウン方式で評価されます。つまり、それぞれのホスト名と方向について一致するものが見つかるまで、最初のルールが評価され、次のルールと続きます。
特定のファイアウォールルールが定義されていない場合、IPアドレス、ホスト名、サブドメイン名またはドメイン名のいずれかの要求を許可またはブロックするために、デフォルトアクションを適用できます。ファイアウォールセクションがある場合、デフォルトのルールパラメータを指定する必要があります。

FIREWALL_ENABLEDパラメータが指定され値が1の場合は、少なくとも1つの他のルールとともにデフォルトのファイアウォールルールを指定する必要があります。

最初のルールは、番号0で示されます。したがって、N番目のルールは、N-1として示されます。
ファイアウォールのルールは、[FW_RULE_START=N]で始まり、コンフィグレーションパラメータが続きます。

セクションの最後は、[FW_RULE_END=N]で示されます。

ファイアウォールの設定内容は次のようになります。

```
[ FW_RULE_START=0 ]
//Configuration parameters for the firewall rule
[ FW_RULE_END=0 ]
…
[ FW_RULE_START=N ]
//Configuration parameters for the firewall rule
[ FW_RULE_END=N ]
FW_DEFAULT=2
```

次の表では、ファイアウォールの設定について説明します。

パラメータ	説明	指定可能な値
FIREWALL_ENABLED	ファイアウォールの有効／無効を設定します。ファイアウォールが有効になっている場合は、この表の下に明記されたパラメータを設定できます。	0（Disabled） 1（Enabled）
NAME	ユーザーがファイアウォールルールに付けた名前。	最大64文字。
TARGET	ルールが適用されるドメイン名、サブドメイン名、ホスト名、サブネットまたはIPアドレス。ここに複数のホスト名の空白区切りのリストを提示することができます。	有効なドメイン、サブドメイン名、ホスト名、サブネットまたはIPアドレス。 例： 192.168.8.173　www.xxxxxxxx.com 192.168.121.0/24
PROTOCOL	ネットワークプロトコル。 利用できるネットワークプロトコルは次のとおりです。 **TCP**：ルールが、TCPベースの通信のものである場合はTCPを選択します。 **UDP**：ルールが、UDPベースの通信のものである場合、UDPを選択します。 ルールがTCPおよびUDP以外のプロトコル通信用である場合は、そのプロトコル番号を指定します。 **Any**：ルールが特定のプロトコル通信用でない場合は、Anyを選択します。	0（Any） 1（TCP） 2（UDP） その他のプロトコルは、 Protocol Numberに + 3をした値を入れてください。 例：ICMP の場合 = 1 + 3 = 4
PORT	ポート番号。ポート番号またはポートの範囲をカンマ区切りのリストで提示することができます。	有効な値。 例： 20～22と80と443を設定したい場合 20:22,80,443
DIRECTION	ネットワークトラフィックの方向。 **Outgoing**：ルールがネットワークから出て行くデータ（つまり無線から有線）に適用される場合は、Outgoingを選択します。 **Incoming**：ルールがネットワークに入ってくるデータ（つまり有線から無線）に適用される場合は、Incomingを選択します。 **Any**：ルールが入出力の両トラフィックに適用される場合は、Anyを選択します。	0（Any） 1（Incoming） 2（Outgoing）

	例えば、無線ネットワークのユーザーが特定のWebサイトまたはドメインへのアクセスを許可または防ぎたい場合は、Outgoingの方向でそれぞれのルールを定義します。 同様に、特定のホストから無線ネットワークへのアクセスを防ぎたい場合は、Incomingの方向で、このホスト名またはドメイン名に固有のルールを定義できます。	
ACTION	ホストから、またはホストへのトラフィックを許可またはブロックできます。	1（Allow） 2（Block）
FW_DEFAULT	任意のタイプの要求を許可またはブロックします。	1（Allow） 2（Block）

次の表では、デフォルトのファイアウォールルール設定について説明します。

パラメータ	説明	指定可能な値
FW_DEFAULT	任意のタイプの要求を許可またはブロックします。	1（Allow） 2（Block）

キャプティブポータル設定（Captive Portal Settings）

自律型APモードでサポートされるキャプティブポータルのタイプは、次のとおりです。

・サインインまたはクリックスルーの外部スプラッシュページ
・RADIUS認証による外部スプラッシュページ

次の表では、キャプティブポータルの設定について説明します。

パラメータ	説明	指定可能な値
AP_IS_PORTAL_CONFIGURED	設定されるポータルのタイプです。	2（サインインまたはクリックスルーの外部スプラッシュページ） 3（RADIUS認証による外部スプラッシュページ）
EXTERNAL_PORTAL_URL	スプラッシュページのURLは、無線ユーザーを外部のポータルにリダイレクトするために使用されます。 このポータルは、無線ユーザーにユーザー名とパスワードを入力するよう促します。 共有鍵のためにこのパラメータを指定し、必要であればSSID-外部ポータル通信の共有鍵を指定してください。ウォールドガーデンの宛先にアクセスする前に、ゲストユーザーにスプラッシュページ上の利用規約に同意させたい場合は、ウォールドガーデンパラメータに制限アクセスを設定します。このパラメータが設定されていない場合、ゲストユーザーはスプラッシュページ上の利用規約に応じなくても、ウォールドガーデンの宛先にアクセス可能になります。	有効なURL 。
VALIDATE_PORTAL	ポータルを検証したい場合は、このパラメータを有効にします。このパラメータが有効になっている場合は、ポータルの共有鍵を指定します。	0（Disabled） 1（Enabled）

PORTAL_SECRET_KEY	このフィールドは、SSID-外部ポータル通信のための秘密鍵です。VALIDATE_PORTAL=1の時だけ指定できます。また、RADIUSサーバー設定を構成することもできます。アクセスポイント(AP)は、それを用いて無線ユーザーを実際に認証します。	可変のバイト単位のキー。 最大128バイト。
PORTAL_GATE1_AUTH	この機能を使用して、キャプティブポータル上の利用規約に同意しない限り、キャプティブポータルは、ウォールドガーデン内のサイトを含むインターネットアクセスを防ぐことができます。	0 (Disabled) 1 (Enabled)
詳細パラメータ：リクエスト属性		
REQUEST_TYPE_TO_PORTAL	リクエストタイプのフィールド名です。	可変の文字列。 例：REQUEST_TYPE_TO_PORTAL= res
CHALLENGE_TO_PORTAL	認証に使用されるランダムなテキストのフィールド名です。	可変の文字列。 例：CHALLENGE_TO_PORTAL=challenge
CLIENT_MAC_TO_PORTAL	クライアントのMACアドレス用のフィールド名です。	可変の文字列。 例:LIENT_MAC_TO_PORTAL=client_mac
AP_MAC_TO_PORTAL	外部のポータルと通信しているアクセスポイント(AP)のMACアドレスのフィールド名です。	可変の文字列。 例：AP_MAC_TO_PORTAL=ap_id
AP_IP_TO_PORTAL	外部のポータルと通信しているアクセスポイント(AP)のIPアドレスのフィールド名です。 これは、外部のポータルによって使用されるフィールド名と一致する必要があります。	可変の文字列。 例：AP_IP_TO_PORTAL=uamip
AP_PORT_TO_PORTAL	アクセスポイント(AP)と外部サーバーが通信するアクセスポイント(AP)のポート番号のフィールド名です。	可変の文字列。 例：AP_PORT_TO_PORTAL=uamport
FAILURE_COUNT_TO_PORTAL	失敗したログイン試行回数のカウント用のフィールド名です。	可変の文字列。 例： FAILURE_COUNT_TO_PORTAL=failure_count
USER_URL_TO_PORTALl	リクエストされたURLのフィールド名です。 アクセスポイント(AP)を通してクライアントによってリクエストされる(外部サーバーへの)URLです。	可変の文字列。 例： USER_URL_TO_PORTAL=userurl
LOGIN_URL_TO_PORTALl	ログインURLのフィールド名です。	可変の文字列。 例: LOGIN_URL_TO_PORTAL=login_url
LOGOFF_URL_TO_PORTAL	ログオフURLのフィールド名です。	可変の文字列。 例： LOGOFF_URL_TO_PORTAL=logoff_url
BLACKOUT_TIME_TO_PORTAL	残りのブラックアウト時間のフィールド名です。	可変の文字列。 例： BLACKOUT_TIME_TO_PORTAL=blackout_time
詳細パラメータ：レスポンス属性		
CHALLENGE_FROM_PORTAL	チャレンジのフィールド名です。	可変の文字列。 例： CHALLENGE_FROM_PORTAL=challenge
RESPONSE_TYPE_FROM_PORTAL	レスポンスタイプのフィールド名です。	可変の文字列。 例：RESPONSE_TYPE_FROM_PORTAL=res
CHALLENGE_RESPONSE_FROM_PORTAL	チャレンジレスポンスのフィールド名です。	可変の文字列。 例： CHALLENGE_RESPONSE_FROM_PORTAL=digest

REDIRECT_URL_FROM_PORTAL	リダイレクトURLのフィールド名です。	可変の文字列。 例： REDIRECT_URL_FROM_PORTAL=redirect
SESSION_TIMEOUT_FROM_PORTAL	ログインタイムアウトのフィールド名です。	可変の文字列。 例： SESSION_TIMEOUT=session_timeout
USER_NAME_FROM_PORTAL	ユーザー名のフィールド名です。	可変の文字列。 例:USER_NAME_FROM_PORTAL=username
PASSWORD_FROM_PORTAL	パスワードのフィールド名です。	可変の文字列。 例: PASSWORD_FROM_PORTAL=password
SPLASHLESS_ROAMING_ENABLED	無線クライアントが、あるアクセスポイント(AP)から別のものにローミングする場合に、スプラッシュページを表示しないようにする時は、このフィールドを有効にします。	0 (Disabled) 1 (Enabled)
BLACKOUT_TIME	ブラックアウト時間（分）です。 前回成功したセッションのタイムアウト後に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、ログインに成功し1時間後にタイムアウトします。このあと、30分間ログインできません。 30分経過後に再びログインできます。	0～1440
AUTH_TIMEOUT	ポータルページをサブミットしたあとに無線ユーザーがゲストネットワークにアクセスするためのログインタイムアウト（分単位）を指定します。タイムアウト後に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。ゲストネットワークへのアクセスを回復するためには、ポータルページをサブミットする必要があります。セッションタイムアウト前にゲストネットワークに対して切断したあと、再接続した場合は、 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。	10～525600
SERVICE_ID_TO_PORTAL	外部ポータルへサービス識別子の値を渡すために使用されるポータルパラメータの名前です。	可変の文字列。 例： SERVICE_ID_TO_PORTAL=service_id
PORTAL_SERVICE_ID	SERVICE_ID_TO_PORTALパラメータで定義した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自由形式のパラメータです。このパラメータは、SSIDプロファイル固有の機能を実装するために外部のポータルで使用できます。例えば、それぞれのSSIDは別々のポータルページを持つことができます。	可変の文字列または数字が使用可能
PORTAL_INTERNET_DOWN_ENABLED	インターネット接続の検出を有効にします。 インターネット接続をチェックし、インターネットの接続が失われた場合には、ポータルエラーページを表示します。インターネットがゲストSSIDで一時的に使用できない時にゲストにフィードバックを提供できます。	0 (Disabled) 1 (Enabled)
PORTAL_HOME_PAGE	リダイレクトURLです。 ユーザーがスプラッシュページを通過したあとにどこにリダイレクトされるかを定義します。	有効なURL。 例：http://googleplus.com/

ご注意：アクセスポイント(AP)によって使用される個々のフィールド名は、ポータルをホストしている外部のサーバーで使用されているフィールド名と一致する必要があります。同じパラメータの名前がお互いで異なる場合、アクセスポイント(AP)と外部サーバーは通信できない可能性があります。

ポータルタイプが**RADIUS認証による外部スプラッシュページ**である場合、以下にあるRADIUS設定のための追加パラメータを設定する必要があります。

次の表では、RADIUS 認証による外部スプラッシュページの設定について説明します。

パラメータ	説明	指定可能な値
PORTAL_RADIUS_CALLED_STATION_ID	Called station ID: アクセスポイント(AP)が認証プロセス中に、標準のRADIUSパラメータ。‘Called-Station-Id’で RADIUSサーバーに渡す自由形式のテキストパラメータです。特別な書式指定子‘%m’’、アクセスポイント(AP)のイーサネットMACアドレスに拡張され 指定できます。	可変の文字列。 Called station ID
PORTAL_RADIUS_NAS_ID	NAS ID: ネットワークリソースにアクセスする1つのポイントとしてネットワークアクセスサーバー（NAS）が使用される場合に、このフィールドが使われます。一般的に、NASは同時に何百ものユーザーをサポートします。RADIUSクライアントがNASに接続すると、NASはRADIUSサーバーへアクセス要求パケットを送信します。これらのパケットは、NASのIPアドレスまたはNAS識別子のいずれかを含める必要があります。NAS IDまたはNAS識別子は、RADIUSサーバーでRADIUSクライアントを認証するために使用されます。 NAS IDの文字列を指定できます。 デフォルト値は %m-%s（%mはアクセスポイント〈AP〉のイーサネットMACアドレス、%sはWLANのSSID）です。これは、RADIUSサーバー上のNAS識別子属性に対応します。NAS識別子のRADIUS属性の属性IDは32です。 NAS IDがRADIUS認証セクションでRADIUSサーバーに設定された共有鍵と同じでないことを確認してください。	可変の文字列。 NAS ID
プライマリ認証サーバーの詳細		
PORTAL_RADIUS_SERVER_IP	プライマリ認証サーバーのIPアドレスです。	有効なサーバーのIPアドレス。
PORTAL_RADIUS_SERVER_PORT	クライアントの要求を受け取るプライマリ認証サーバーのポート番号です。	有効なポート番号。
PORTAL_RADIUS_SECRET_KEY	アクセスポイント(AP)とプライマリ認証サーバー間の共有鍵です。	可変の文字列。
セカンダリ認証サーバーの詳細		
PORTAL_RADIUS_SERVER_IP_2	セカンダリ認証サーバーのIPアドレスです。	有効なサーバーのIPアドレス。
PORTAL_RADIUS_SERVER_PORT_2	クライアントの要求を受け取るセカンダリ認証サーバーのポート番号です。	有効なポート番号。
PORTAL_RADIUS_SECRET_KEY_2	アクセスポイント(AP)とセカンダリ認証サーバー間の共有鍵です。	可変の文字列。
PORTAL_RADIUS_ACCT_ENABLED	RADIUSアカウンティングの有効または無効です。	0 (Disabled) 1 (Enabled)

RADIUSアカウンティングパラメータ		
PORTAL_RADIUS_ACCT_INTERVAL	アカウンティング・インターバル（分単位）です。最小間隔は60秒（1分）、最大間隔は3600秒（60分）です。	秒単位のインターバル。 60～3600秒
プライマリ・アカウンティングサーバーのパラメータ		
PORTAL_RADIUS_ACCT_SERVER_IP	プライマリ・アカウンティングサーバーのIPアドレスです。	有効なサーバーのIPアドレス。
PORTAL_RADIUS_ACCT_SERVER_PORT	クライアントの要求を受け取るプライマリ・アカウンティングサーバーのポート番号です。	有効なポート番号。
PORTAL_RADIUS_ACCT_SECRET_KEY	アクセスポイント(AP)とプライマリ・アカウンティングサーバー間の共有鍵です。	可変の文字列。
セカンダリ・アカウンティングサーバーのパラメータ		
PORTAL_RADIUS_ACCT_SERVER_IP_2	セカンダリ・アカウンティングサーバーのIPアドレスです。	有効なサーバーのIPアドレス。
PORTAL_RADIUS_ACCT_SERVER_PORT_2	クライアントの要求を受け取るセカンダリ・アカウンティングサーバーのポート番号です。	有効なポート番号。
PORTAL_RADIUS_ACCT_SECRET_KEY_2	アクセスポイント(AP)とセカンダリ・アカウンティングサーバー間の共有鍵です。	可変の文字列。

ウォールドガーデン設定（Walled Garden Settings）

ウォールドガーデンは、インターネットへの制限付きアクセスを提供する方法です。 ウォールドガーデンの宛先は、スプラッシュページを表示せずに、指定したポート番号でアクセスできます。 またDomain（例：domain.com）は、そのサブドメイン（例：subdomain.domain.com)をカバーします。

除外されるドメイン、サブドメイン、IPアドレス範囲、およびポート番号のリストを設定します(例：192.168.1.0/24)。 これらのIPアドレス上のサービスは、ポータルページへのリダイレクトなしでアクセスできます。 ポータルページの一部分（イメージなど）がWebサーバーに配置されている場合、WebサーバーのIPアドレスをこのリストに入れる必要があります。

複数のウォールドガーデンの設定は、スペースで区切られたリストとして設定できます。各エントリには、1つのドメイン名または IP アドレス、カンマで区切られた複数のポート番号を設定できます。ドメイン名とポート番号は、コロン（:）で区切られます。

パラメータ	説明	指定可能な値
EXEMPTED_IP_PORT_LIST	ルールが適用されるドメイン名、サブドメイン名、ホスト名、サブネットまたはIPアドレスです。 例：google.com:20-22,81,443	有効なIPアドレス、ドメイン名およびポート番号。 例： 8.8.8.8:80,443,55 google.com:80,443,55 yahoo.com:20-22

トラフィックシェーピングと QoS 設定

次の設定をすることで、ネットワーク帯域幅を有効に利用できます。
ネットワークのアップロードおよびダウンロード制限の設定、クライアントアソシエーション数の制限、バンドステアリング、QoSパラメータを定義することです。ネットワークトラフィック、SSIDの上で使われるアプリケーションと使用中のアクセスポイント(AP)モデルに応じて、これらの方法から1つ以上を選んで設定できます。
次の表では、トラフィックシェーピングおよびQoSの設定について説明します。

パラメータ	説明	指定可能な値
TRAFFIC_SHAPING_UPLOAD	アップロード帯域幅（Kbps）です。	0～1048576の値。 0は無効を示します。

TRAFFIC_SHAPING_DOWNLOAD	ダウンロード帯域幅（Kbps）です。	0～1048576の値。 0は無効を示します。
TRAFFIC_SHAPING_STA_ENABLE	ユーザーごとの帯域制御を有効にします。	0（Disable） 1（Enable）
TRAFFIC_SHAPING_STA_DOWNLOAD	ユーザーのダウンロード帯域幅をKbps単位で制限します。	0～1048576 Kbpsの値。
TRAFFIC_SHAPING_STA_UPLOAD	ユーザーのアップロード帯域幅をKbps単位で制限します。	0～1048576 Kbpsの値。
VAP_MIN_RATE	最低ユニキャストデータ転送速度（Mbps）です。	0～54 Mbpsの値。
QOS_SSID_PRIORITY	条件に基づいてプライオリティを設定します。	0（Voice） 1（Video） 2（Best Video） 3（Background）
QOS_PRIORITY_TYPE	IEEE802.1pまたはIPヘッダーで示されるプライオリティに関わらず、このSSIDのすべてのトラフィックを、 選択されたプライオリティで送りたい場合は、プライオリティタイプで固定を選択します。このSSIDのトラフィックが選択されたプライオリティと同等か低い場合は、プライオリティタイプで上限を選択します。	0（上限） 1（固定）
QOS_DOWNSTR_MAP	ダウンストリームマッピングのタイプです。	0（IEEE802.1p） 1（DSCP） 2（TOS）
QOS_UPSTR_MARK_802_1p	IEEE802.1p マーキングです。	0（Disabled） 1（Enabled）
QOS_UPSTR_MARK_DSCP_TOS	DSCP/TOS マーキングです。	0（Disabled） 1（DSCP） 2（TOS）

Hotspot 2.0 設定（Hotspot 2.0 Settings）

アクセスポイント(AP)のHotspot 2.0設定は、一般設定、ローミングコンソーシアムリスト、場所設定、ドメイン名リスト、3GPPセルラーネットワーク情報リスト、NAIレルムリスト、WANメトリック、事業者フレンドリー名リスト、接続機能に分かれています。

一般設定

一般設定では、ネットワークアクセスタイプ、ネットワーク認証タイプエレメント、IPアドレスタイプなどのネットワーク設定をします。

次の表では、一般設定について説明します。

パラメータ	説明	指定可能な値
HS20_VAP_ENABLE	VAPがホットスポットとして機能しているかどうかを選択します。	1（Enable） 0（Disable）
HS20_L2TIF_ENABLE	レイヤ2トラフィック検査とフィルタリングを有効または無効にします。	1（Enable） 0（Disable）
BSS_LOAD_ENABLE	BSSロードを有効または無効にします。	1（Enable） 0（Disable）
PROXYARP_ENABLE	プロキシARPの設定を有効または無効にします。	1（Enable） 0（Disable）
PROXYARP_DGAF_DISABLE	DGAFを有効または無効にします。	1（Yes） 0（No）

P2P_XCONNECT_ENABLE	P2Pクロスコネクションを有効または無効にします。	1（Enable） 0（Disable）
HS20_ACCESS_NETWORK_TYPE	アクセスポイント(AP)のネットワークタイプ（利用可能なオプションのリストから1つ）を選択します。	0（PRIVATE） 1（PRIVATE_WITH_GUEST_ACCESS） 2（CHARGEABLE_PUBLIC） 3（FREE_PUBLIC） 4（PERSONAL_DEVICE） 5（EMERGENCY_SERVICES_ONLY） 14（TEST） 15（WILDCARD）
HS20_NETWORK_AUTH_TYPE	URLを持つネットワーク認証タイプ。	書式：<ネットワーク認証タイプインジケータ（1オクテット文字列）>[リダイレクトURL] ネットワーク認証タイプの値： 00　（利用条件の受諾） 01　（オンラインでの登録サポート） 02　（http/httpsリダイレクト） 03　（DNSリダイレクト） 例: HS20_NETWORK_AUTH_TYPE=02http://www.example.com/redirect/me/here/
HS20_IP_ADDR_TYPE_AVAILABILITY	IPv4とIPv6情報のビットマスク。	IPv4とIPv6情報のビットマスク。 書式：<16進文字列として符号化された1オクテットの値>(ipv4_type & 0x3f) << 2 | (ipv6_type & 0x3) IPv4_タイプ: 0（利用できないアドレスタイプ） 1（利用可能なパブリックIPv4アドレス） 2（利用可能なポート制限付きIPv4アドレス） 3（利用可能なシングルNAT変換されたプライベートIPv4アドレス） 4（利用可能なダブルNAT変換されたプライベートIPv4アドレス） 5（ポート制限付きIPv4アドレスおよび利用可能なシングルNAT変換IPv4アドレス） 6（ポート制限付きIPv4アドレスおよび利用可能なダブルNAT変換IPv4アドレス） 7（アドレスタイプの有効性が不明） IPv6_タイプ: 0（利用できないアドレスタイプ） 1（利用可能なアドレスタイプ）
HS20_INTERNET_ACCESS	ネットワークがアクセスポイント(AP)を経由してクライアントへのインターネットアクセスを提供する場合は、このパラメータを有効にします。	0（Disabled） 1（Enabled）

HS20_HESSID	HESSID（Homogenous Extended Service Set Identifier）。ホットスポットのアクセスポイント(AP)を識別するために使用されるオプションフィールドです。HESSIDが同じアクセスポイント(AP)は、Hotspot 2.0設定は同じになります。	デフォルト値：00:00:00:00:00:00

場所設定（Venue Settings）

場所設定は、アクセスポイント(AP)が配置される場所の詳細な構成を指定します。場所設定は、場所グループ（Venue Group）と場所タイプ（Venue Type）で構成されています。
次の表では、場所グループ（Venue Group）の設定について説明します。

パラメータ	説明	指定可能な値
HS20_VENUE_GROUP	利用可能なオプションから適切な場所グループを設定します。	0（未指定） 1（アセンブリ） 2（ビジネス） 3（教育機関） 4（工場および産業） 5（機関） 6（商業） 7（住居） 8（倉庫） 9（公共施設、その他） 10（乗り物） 11（屋外）
HS20_VENUE_TYPE	アクセスポイント(AP)が設置されている場所タイプを設定します。選択された場所グループに応じて、表示される内容は異なります。 例えば、教育機関として場所グループを選択すると、場所タイプには、未指定の教育機関・小学校・中学校・大学が利用可能です。	場所グループ0　： 0（未指定） 場所グループ1　： 0（未指定のアセンブリ） 1（アリーナ） 2（スタジアム） 3（乗客ターミナル〈空港、バス、フェリー、電車の駅など〉） 4（円形劇場） 5（アミューズメント パーク） 6（礼拝所） 7（会議場） 8（図書館） 9（博物館） 10（レストラン） 11（シアター） 12（バー） 13（喫茶店） 14（動物園または水族館） 15（緊急対応センター） 場所グループ2　： 0（未指定のビジネス） 1（医師または歯科医師のオフィス） 2（銀行） 3（消防署） 4（警察署） 6（郵便局） 7（専門家のオフィス）

		8（研究および開発施設） 9（弁護士事務所） 場所グループ3 ： 0（未指定の教育機関） 1（小学校） 2（中学校） 3（大学） 場所グループ4 ： 0（未指定の工場および産業） 1（工場） 場所グループ5 ： 0（未指定の公共機関） 1（病院） 2（長期看護施設〈療養所、ホスピスなど〉） 3（アルコールおよび薬物のリハビリテーション センター） 4（グループ ホーム） 5（刑務所または拘置所） 場所グループ6 ： 0（未指定の商業施設） 1（小売店） 2（食料品店） 3（自動車サービス ステーション） 4（ショッピング モール） 5（ガソリン スタンド） 場所グループ7 ： 0（未指定の居住施設） 1（個人の住居） 2（ホテルまたはモーテル） 3（寮） 4（宿泊施設） 場所グループ8 ： 0（未指定の倉庫） 場所グループ9 ： 0（指定の公共施設およびその他） 場所グループ10 ： 0（未指定の乗り物） 1（自動車またはトラック） 2（飛行機） 3（バス） 4（フェリー） 5（船またはボート） 6（電車） 7（モーター バイク）

		場所グループ11 ： 0（未指定の屋外） 1（自治体メッシュ ネットワーク） 2（都市公園） 3（休憩施設） 4（交通管制施設） 5（バス停留所） 6（売店）
HS20_VENUE_NAME_AND_LANG_CODE	このフィールドには、複数のエントリが、存在する場合があります。各場所のエントリは言語コードのあとに、コロン(:)と場所名が続きます。言語コードはISO639.2規格を参照してください。場所名の最大長は252バイトで、場所名には、最大32のエントリを追加できます。	有効な場所名 ： 252 bytes 有効な言語コード ： 3 bytes HS20_VENUE_NAME_AND_LANG_CODE=eng:test_venue

ローミングコンソーシアム

ネットワークは、ローミングコンソーシアムのメンバーやサービスプロバイダをサポートできます。エレメントは、一意の16進文字列かつ、1つ以上の組織識別子で構成されています。このエレメントに複数の組織識別子が含まれている場合は、ネットワークが複数のサービスプロバイダまたはコンソーシアムをサポートすることを意味します。最大32個のローミングコンソーシアムを、追加できます。リストにある最初の3つのローミングコンソーシアムが、ビーコンでアドバタイズされます。ローミングコンソーシアム文字列の長さは、3または5バイト（6または10の16進文字）にする必要があります。

次の表では、ローミングコンソーシアムの設定について説明します。

パラメータ	説明	指定可能な値
HS20_ROAMING_CONSORTIUM_OI	OI（組織識別子のリスト）と呼ばれる、複数のローミングコンソーシアム16進文字を使用して設定できます。リストにある最初の3つのローミングコンソーシアムがビーコンでアドバタイズされます。最大32個のローミングコンソーシアムを追加できます。ローミングコンソーシアムの文字列の長さは、3または5バイト（6または10の16進文字）にする必要があります。	例： HS20_ROAMING_CONSORTIUM_OI=0a1bdd

ドメイン名

ドメイン名リストはHotspot 2.0事業者のドメイン名リストを提供します。

次の表では、ドメイン名の設定について説明します。

パラメータ	説明	指定可能な値
HS20_DOMAIN_NAME	最高32のドメインを追加できます。ドメイン名のサイズは、最大255バイトです。	

3GPP セルラーネットワーク情報リスト

アクセスポイント(AP)によってサポートされているモバイルネットワークのリストを、3GPPセルラーネットワーク情報リストで設定できます。このリストには最大32のエントリを追加できます。

リストの各モバイルエレメントの開始と終了を、以下のとおりに構成できます。

```
[ HS20_CELLULAR_NETWORK_ENTRY_START=N ]
//Configuration parameters for 3GPP cellular network
[ HS20_CELLULAR_NETWORK_ENTRY_END=N ]
```

次の表では、3GPP セルラーネットワーク設定について説明します。

パラメータ	説明	指定可能な値
HS20_MOBILE_COUNTRY_CODE	3桁のモバイル国コードです。	
HS20_MOBILE_NETWORK_CODE	2～3桁のモバイルネットワークコードです。	

NAI レルムリスト

NAIレルムリストには、NAIレルムの要素が含まれています。NAIレルムの要素は、アクセスポイント(AP)を経由してアクセスできるネットワーク、サービスのサービスプロバイダ、他のエンティティに対応するネットワーク・アクセス識別子（NAI）要素のリストを提供します。1つ以上のEAPメソッドのリストが各NAIレルムに含まれています。

NAIレルムのセクションは、[HS20_NAI_REALM_ENTRY_START= N]で始まり、NAIレルムの設定パラメータが続きます。セクションは、[HS20_NAI_REALM_ENTRY_END= N] で終わります。

コンフィグレーションファイル内の NAI レルムセクションは、以下のとおりです。

```
[ HS20_NAI_REALM_ENTRY_START=N ]
//Configuration parameters for NAI realm
[ HS20_NAI_REALM_ENTRY_END=N ]
```

次の表では、NAI レルムの設定について説明します。

パラメータ	説明	指定可能な値
HS20_NAI_REALM	各セクションの長さが最大255バイトのレルムを最高32まで追加できます。	
HS20_EAP_METHOD	1つのレルムに最大4つのEAPメソッドを追加できます。EAPメソッドは、優先する順序で追加してください。最も優先されるEAPメソッドを最初に追加し、その後、2番目に優先されるメソッドと続きます。	0 (TLS) 1 (TTLS_MSCHAPv2) 2 (SIM) 3 (AKA)

事業者フレンドリー名リスト

事業者フレンドリー名リストには、言語コードと共に事業者フレンドリー名のリストを入力できます。

次の表では、オペレータフレンドリー名の設定について説明します。

パラメータ	説明	指定可能な値
HS20_OP_FRIENDLY_NAME_AND_LANG_CODE	事業者フレンドリー名リストの詳細です。 このフィールドには、複数のエントリがある場合があります。個々のエントリは、コロン（:）で区切られた2つのフィールドで構成されます。 例： HS20_OP_FRIENDLY_NAME_AND_LANG_CODE=eng ： name1 HS20_OP_FRIENDLY_NAME_AND_LANG_CODE=eng ： name2 HS20_OP_FRIENDLY_NAME_AND_LANG_CODE=eng ： name 言語コード:事業者フレンドリー名が指定された言語コードです。言語コードについてはISO	

	639.2規格を参照してください。 レルム名：異なる言語のHotspot 2.0事業者のフレンドリー名です。最大長は252バイト未満です。	

WANメトリック

WANメトリックでは、WLANを通じて利用可能なWAN接続の詳細を指定できます。リンクステータス、アップリンクとダウンリンクの速度はWANメトリックで指定できます。

次の表では、WANメトリックを説明します。

パラメータ	説明	指定可能な値
HS20_WAN_METRICS	パラメータの形式 <WAN Info>:<DL Speed>:<UL Speed>:0:0:0 コロン(:)で区切られた6つのフィールドで構成されています。 **(1) リンクステータス** 適切なオプションを設定します。 **Link up**：リンクがアップしている場合は、このオプションを設定します。 **Link down**：リンクがダウンしている場合は、このオプションを設定します。 **Link in test**：リンクがテスト中の場合は、このオプションを設定します。 **Not Configured**：リンクステータスが設定されていない場合、このオプションを設定します。 **(2) Kbps単位のダウンロード速度** **(3) Kbps単位のアップロード速度** **(4) Reserved (=0)** **(5) Reserved (=0)** **(6) Reserved (=0)**	リンクステータスのそれぞれの値は次のとおりです。 1 (LINK_UP) 2 (LINK_DOWN) 3 (LINK_IN_TEST) -100 (NOT_CONFIGURED)

接続機能

接続機能では、ネットワーク接続でサポートされているプロトコル、対応するポート番号、ポートが開いているか閉じているかを指定できます。これらの設定は、アクセスポイント(AP)が接続されている有線ネットワークの機能を表します。これらは、ホットスポット内で使用される通信プロトコルとポートの接続状態に関する情報を提供します。

ポート設定に基づき、Wi-Fiプロファイルのファイアウォール設定で適切なファイアウォールルールを設定していることを確認してください。

接続機能のセクションは、[HS20_CONNECTION_CAPAB_ENTRY_START=N]で始まり、接続機能の設定パラメータが続きます。セクションは、[HS20_CONNECTION_CAPAB_ENTRY_END=N] で終わります。

コンフィグレーションファイル内の接続機能セクションは、以下のとおりです。

```
[ HS20_CONNECTION_CAPAB_ENTRY_START=N ]
//Configuration parameters for connection capability
[ HS20_CONNECTION_CAPAB_ENTRY_END=N ]
```

次の表では、接続機能の設定について説明します。

パラメータ	説明	指定可能な値
HS20_PROTOCOL	プロトコル番号です。	1 (ICMP, 診断のために使用) 6 (FTP/SSH/HTTP/TLS/PPTP VPNs/VoIP) 17 (IKEv2/IPSec - NAT/VoIP) 50 (ESP, IPSec VPNで使用)
HS20_PORT_NO	ポート番号:上記で設定したプロトコルに対してのポート番号です。	プロトコル = 1 0 (ICMP, used for diagnostics) プロトコル = 6 次の値のいずれかが許可されます。 20 (FTP) 22 (SSH) 80 (HTTP) 443 (Used by TLS PPTP VPNs) 1723 (Used by PPTP VPNs) 5060 (VoIP) プロトコル = 17 次の値のいずれかが許可されます。 500 (Used by IKEv2 (IPSec VPN)) 4500 (May be used by IKEv2 (IPSec VPN)) 5060 (VoIP) プロトコル = 50 0 (ESP, used by IPSec VPNs)
HS20_PORT_STATUS	ポートのステータスです。	0 (Closed) 1 (Open) 2 (Unknown)

【グローバル設定（Global Settings）】

APデバイス固有のパラメータを含む各コンフィグレーションは、これらの設定からなる1つのグローバル設定セクションがあります。

グローバル設定セクションは、[GLOBAL START]で始まり、そのあとに、このセクションのコンフィグレーションパラメータが続きます。

静的IP設定が適用されている場合は、静的IP設定に関連した追加のパラメータを設定する必要があります。
グローバル設定の内容は、以下のとおりです。

```
[ GLOBAL_START ]
//Configuration parameters for global settings
[ GLOBAL_END ]
```

次の表では、グローバル設定について説明します。

パラメータ	説明	指定可能な値
VLAN_ID	ネットワーク設定が構成されるVLAN IDです。	0～4094の値 [0: スイッチのVLAN番号にかかわりなく、デバイスが接続してされるスイッチポートのタグなしVLANを示します。] デフォルト値 ：0
BOOTPROTO	下記のネットワークの設定を指定します。 DHCP: DHCP（ダイナミック・ホスト・コンフィグレーション・プロトコル）より設定を動的に受け取ります。 Static:静的またはユーザーにより手動で構成します。	dhcp（DHCPの設定を適用） static（静的設定を適用） デフォルト値：dhcp
スタティックIP 設定		
IP_ADDRESS	デバイスのIPアドレスです。	有効なIPアドレス。
NETMASK	ネットワークマスクです。	有効なネットワークマスク。
GATEWAY_IP	ゲートウェイIPアドレスです。	有効なゲートウェイIPアドレス。
PRIMARY_DNS	プライマリDNSサーバーです。	有効なDNSサーバー名またはIPアドレス。
SECONDARY_DNS	セカンダリDNSサーバーです。	有効なDNSサーバー名またはIPアドレス。
DNS_PREFIX	プライマリDNSサフィックスは、DNS名の登録とDNS名前解決で使用されます。	有効なドメイン名。

コンフィグレーションファイルのサンプル

ご注意：事前に設定内容が適切であることをご確認のうえ、設定してください。

以下は、コンフィグレーションファイルのサンプルです。

```
[ RADIO_START ]
WIRELESS_MODE=3
AP_CHAN_WIDTH=1
OP_CHANNEL=0
FRAG_THRESH=2346
RTSCTS_THRESH=2347
BEACON_INT=100
DTIM_PERIOD=1
SHORT_GI=0
AMPDUENABLE=1
AP_TRANSMIT_POWER=30
AP_TRANSMIT_POWER_ENABLED=0
BS_LOAD_BAL_THRESHOLD=5
[ RADIO_END ]
```

```
[ RADIO_START=2 ]
WIRELESS_MODE=5
AP_CHAN_WIDTH=3
OP_CHANNEL=44
FRAG_THRESH=2346
RTSCTS_THRESH=2347
BEACON_INT=100
DTIM_PERIOD=2
SHORT_GI=1
AMPDUENABLE=1
AP_TRANSMIT_POWER=30
AP_TRANSMIT_POWER_ENABLED=0
BS_LOAD_BAL_THRESHOLD=10
[ RADIO_END=2 ]

[ VAP_START=1 ]
AP_SSID=na1000w-g
HIDESSID_BROADCAST=0
WMM_ENABLE=0
ISOLATION_ENABLE=0
AP_VLAN=0
AP_SEC_MODE=0
VAP_IS_GUEST_SSID=0
AUTH_TIMEOUT=1440
PORTAL_HOME_PAGE=
DHCPD_LOCAL_IP=
DHCPD_LEASE_TIME=1440
EXEMPTED_IP_LIST=
DNS_SERVER_LIST=8.8.8.8
AP_IS_PORTAL_CONFIGURED=0
DHCPD_SUBNET_MASK=
DHCPD_START_IP=
DHCPD_END_IP=
BLACKOUT_TIME=0
FIREWALL_ENABLED=0
TRAFFIC_SHAPING_UPLOAD=0
TRAFFIC_SHAPING_DOWNLOAD=0
QOS_SSID_PRIORITY=0
QOS_PRIORITY_TYPE=0
QOS_DOWNSTR_MAP=1
QOS_UPSTR_MARK_802_1p=1
QOS_UPSTR_MARK_DSCP_TOS=0
ENABLE_LIMIT_ON_ASSOC=0
ASSOC_LIMIT=127
REQUEST_TYPE_TO_PORTAL=res
CHALLENGE_TO_PORTAL=challenge
CLIENT_MAC_TO_PORTAL=client_mac
AP_MAC_TO_PORTAL=ap_id
AP_IP_TO_PORTAL=uamip
AP_PORT_TO_PORTAL=uamport
FAILURE_COUNT_TO_PORTAL=failure_count
USER_URL_TO_PORTAL=userurl
LOGIN_URL_TO_PORTAL=login_url
LOGOFF_URL_TO_PORTAL=logoff_url
BLACKOUT_TIME_TO_PORTAL=blackout_time
CHALLENGE_FROM_PORTAL=challenge
```

```
RESPONSE_TYPE_FROM_PORTAL=res
CHALLENGE_RESPONSE_FROM_PORTAL=digest
REDIRECT_URL_FROM_PORTAL=redirect
SESSION_TIMEOUT_FROM_PORTAL=session_timeout
USERNAME_FROM_PORTAL=username
PASSWORD_FROM_PORTAL=password
VAP_MIN_RATE=0.0
SPLASHLESS_ROAMING_ENABLED=1
EXEMPTED_IP_PORT_LIST=
PORTAL_SERVICE_ID=
SERVICE_ID_TO_PORTAL=service_id
BS_BAND_STEERING_ENABLED=0
BS_RSSI_THRESHOLD=-75
PORTAL_INTERNET_DOWN_ENABLED=0
DYNAMIC_VLAN_ENABLED=0
TRAFFIC_SHAPING_STA_ENABLE=0
HS20_VAP_ENABLE=0
HS20_L2TIF_ENABLE=0
HS20_ACCESS_NETWORK_TYPE=15
HS20_VENUE_GROUP=0
HS20_VENUE_TYPE=0
HS20_HESSID=00:00:00:00:00:00
HS20_INTERNET_ACCESS=0
HS20_NETWORK_AUTH_TYPE=
HS20_IP_ADDR_TYPE_AVAILABILITY=00
BSS_LOAD_ENABLE=0
PROXYARP_ENABLE=0
PROXYARP_DGAF_DISABLE=0
P2P_XCONNECT_ENABLE=0
SSID_PROFILE_ID=10
RADIO_ID=1
AP_WEP_TYPE=WEP104
AP_KEY_TYPE=ASCII
AP_WEP_KEY=
AP_WEP_MODE=1
AP_SECFILE=PSK
AP_AUTH_SERVER=
AP_AUTH_PORT=1812
AP_AUTH_SECRET=
AP_AUTH_SERVER2=
AP_AUTH_PORT2=1812
AP_AUTH_SECRET2=
PSK_KEY=
AP_ACCT_ENABLED=0
[ VAP_END=1 ]

[ VAP_START=2 ]
AP_SSID=na1000w-a
HIDESSID_BROADCAST=0
WMM_ENABLE=1
ISOLATION_ENABLE=1
AP_VLAN=0
AP_SEC_MODE=3
AP_SECFILE=PSK
PSK_KEY=2991dfba28d65
VAP_IS_GUEST_SSID=1
AUTH_TIMEOUT=1440
```

```
PORTAL_HOME_PAGE=
DHCPD_LOCAL_IP=192.168.100.1
DHCPD_LEASE_TIME=1440
EXEMPTED_IP_LIST=
DNS_SERVER_LIST=8.8.8.8 192.168.100.1
AP_IS_PORTAL_CONFIGURED=0
DHCPD_SUBNET_MASK=255.255.255.0
DHCPD_START_IP=192.168.100.100
DHCPD_END_IP=192.168.100.200
BLACKOUT_TIME=0
FIREWALL_ENABLED=0
TRAFFIC_SHAPING_UPLOAD=0
TRAFFIC_SHAPING_DOWNLOAD=0
QOS_SSID_PRIORITY=0
QOS_PRIORITY_TYPE=0
QOS_DOWNSTR_MAP=1
QOS_UPSTR_MARK_802_1p=1
QOS_UPSTR_MARK_DSCP_TOS=0
ENABLE_LIMIT_ON_ASSOC=0
ASSOC_LIMIT=127
REQUEST_TYPE_TO_PORTAL=res
CHALLENGE_TO_PORTAL=challenge
CLIENT_MAC_TO_PORTAL=client_mac
AP_MAC_TO_PORTAL=ap_id
AP_IP_TO_PORTAL=uamip
AP_PORT_TO_PORTAL=uamport
FAILURE_COUNT_TO_PORTAL=failure_count
USER_URL_TO_PORTAL=userurl
LOGIN_URL_TO_PORTAL=login_url
LOGOFF_URL_TO_PORTAL=logoff_url
BLACKOUT_TIME_TO_PORTAL=blackout_time
CHALLENGE_FROM_PORTAL=challenge
RESPONSE_TYPE_FROM_PORTAL=res
CHALLENGE_RESPONSE_FROM_PORTAL=digest
REDIRECT_URL_FROM_PORTAL=redirect
SESSION_TIMEOUT_FROM_PORTAL=session_timeout
USERNAME_FROM_PORTAL=username
PASSWORD_FROM_PORTAL=password
VAP_MIN_RATE=0.0
SPLASHLESS_ROAMING_ENABLED=1
EXEMPTED_IP_PORT_LIST=
PORTAL_SERVICE_ID=
SERVICE_ID_TO_PORTAL=service_id
BS_BAND_STEERING_ENABLED=0
BS_RSSI_THRESHOLD=-75
PORTAL_INTERNET_DOWN_ENABLED=0
DYNAMIC_VLAN_ENABLED=0
TRAFFIC_SHAPING_STA_ENABLE=0
IEEE802_1X_RETRY_TIMEOUT=2
IEEE802_1X_MAX_RETRIES=4
HS20_VAP_ENABLE=0
HS20_L2TIF_ENABLE=1
HS20_ACCESS_NETWORK_TYPE=15
HS20_VENUE_GROUP=0
HS20_VENUE_TYPE=0
HS20_HESSID=00:00:00:00:00:00
HS20_INTERNET_ACCESS=0
```

```
HS20_NETWORK_AUTH_TYPE=
HS20_IP_ADDR_TYPE_AVAILABILITY=00
BSS_LOAD_ENABLE=0
PROXYARP_ENABLE=1
PROXYARP_DGAF_DISABLE=1
P2P_XCONNECT_ENABLE=0
SSID_PROFILE_ID=11
RADIO_ID=2
AP_WEP_TYPE=WEP104
AP_KEY_TYPE=ASCII
AP_WEP_KEY=
AP_WEP_MODE=1
AP_AUTH_SERVER=
AP_AUTH_PORT=1812
AP_AUTH_SECRET=
AP_AUTH_SERVER2=
AP_AUTH_PORT2=1812
AP_AUTH_SECRET2=
AP_ACCT_ENABLED=0
[ VAP_END=2 ]

[ VAP_START=3 ]
AP_SSID=bandsteering
HIDESSID_BROADCAST=0
WMM_ENABLE=1
ISOLATION_ENABLE=1
AP_VLAN=0
AP_SEC_MODE=4
AP_SECFILE=EAP
AP_AUTH_SERVER=192.168.10.100
AP_AUTH_PORT=1812
AP_AUTH_SECRET=radiuspass
VAP_IS_GUEST_SSID=0
AUTH_TIMEOUT=1440
PORTAL_HOME_PAGE=
DHCPD_LOCAL_IP=
DHCPD_LEASE_TIME=1440
EXEMPTED_IP_LIST=
DNS_SERVER_LIST=8.8.8.8
AP_IS_PORTAL_CONFIGURED=0
DHCPD_SUBNET_MASK=
DHCPD_START_IP=
DHCPD_END_IP=
AP_AUTH_SERVER2=
AP_AUTH_PORT2=1812
AP_AUTH_SECRET2=
AP_ACCT_ENABLED=1
AP_ACCT_SERVER=192.168.10.101
AP_ACCT_PORT=1813
AP_ACCT_SECRET=acountpass
AP_ACCT_SERVER2=
AP_ACCT_PORT2=1813
AP_ACCT_SECRET2=
BLACKOUT_TIME=0
FIREWALL_ENABLED=1
TRAFFIC_SHAPING_UPLOAD=10
TRAFFIC_SHAPING_DOWNLOAD=102400
```

QOS_SSID_PRIORITY=1
QOS_PRIORITY_TYPE=1
QOS_DOWNSTR_MAP=1
QOS_UPSTR_MARK_802_1p=1
QOS_UPSTR_MARK_DSCP_TOS=2
ENABLE_LIMIT_ON_ASSOC=1
ASSOC_LIMIT=32
REQUEST_TYPE_TO_PORTAL=res
CHALLENGE_TO_PORTAL=challenge
CLIENT_MAC_TO_PORTAL=client_mac
AP_MAC_TO_PORTAL=ap_id
AP_IP_TO_PORTAL=uamip
AP_PORT_TO_PORTAL=uamport
FAILURE_COUNT_TO_PORTAL=failure_count
USER_URL_TO_PORTAL=userurl
LOGIN_URL_TO_PORTAL=login_url
LOGOFF_URL_TO_PORTAL=logoff_url
BLACKOUT_TIME_TO_PORTAL=blackout_time
CHALLENGE_FROM_PORTAL=challenge
RESPONSE_TYPE_FROM_PORTAL=res
CHALLENGE_RESPONSE_FROM_PORTAL=digest
REDIRECT_URL_FROM_PORTAL=redirect
SESSION_TIMEOUT_FROM_PORTAL=session_timeout
USERNAME_FROM_PORTAL=username
PASSWORD_FROM_PORTAL=password
VAP_MIN_RATE=2.0
SPLASHLESS_ROAMING_ENABLED=1
EXEMPTED_IP_PORT_LIST=
PORTAL_SERVICE_ID=
SERVICE_ID_TO_PORTAL=service_id
BS_BAND_STEERING_ENABLED=1
BS_RSSI_THRESHOLD=-75
PORTAL_INTERNET_DOWN_ENABLED=0
DYNAMIC_VLAN_ENABLED=0
TRAFFIC_SHAPING_STA_ENABLE=1
TRAFFIC_SHAPING_STA_DOWNLOAD=5120
TRAFFIC_SHAPING_STA_UPLOAD=5
IEEE802_1X_RETRY_TIMEOUT=2
IEEE802_1X_MAX_RETRIES=4
HS20_VAP_ENABLE=0
HS20_L2TIF_ENABLE=1
HS20_ACCESS_NETWORK_TYPE=15
HS20_VENUE_GROUP=0
HS20_VENUE_TYPE=0
HS20_HESSID=00:00:00:00:00:00
HS20_INTERNET_ACCESS=0
HS20_NETWORK_AUTH_TYPE=
HS20_IP_ADDR_TYPE_AVAILABILITY=00
BSS_LOAD_ENABLE=1
PROXYARP_ENABLE=1
PROXYARP_DGAF_DISABLE=0
P2P_XCONNECT_ENABLE=0
NAS_IDENTIFIER=%m-%s
SSID_PROFILE_ID=12
RADIO_ID=1,2
FW_RULE_START=1
NAME=firewallname

```
TARGET=192.168.8.173
PROTOCOL=0
PORT=
DIRECTION=0
ACTION=2
FW_RULE_END=1
FW_DEFAULT=2
AP_WEP_TYPE=WEP104
AP_KEY_TYPE=ASCII
AP_WEP_KEY=
AP_WEP_MODE=1
PSK_KEY=
[ VAP_END=3 ]

[ GLOBAL_START ]
VLAN_ID=0
BOOTPROTO=dhcp
[ GLOBAL_END ]
```

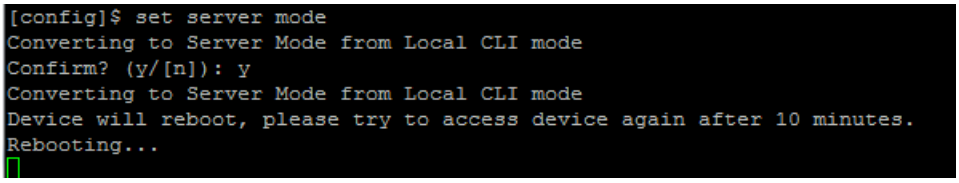
自律型 AP モードでコンフィグレーション設定を取得

自律型 AP モードでアクセスポイント(AP)の現在のコンフィグレーション設定を取得するには、get ap config コマンドを使用します。アクセスポイント(AP)の CLI にログインし、「get ap config」と入力してください。

アクセスポイント(AP)を集中管理型 AP モードまたはセンサーモードに設定

自律型 AP モードから集中管理型 AP モードまたはセンサーモードにアクセスポイント(AP)のモードを変更するには、set server mode コマンドを使用します。モードが変更されたあとにデバイスが再起動します。モードが集中管理型 AP モードまたはセンサーモードに変更されると、前回サーバーから受信したコンフィグレーション設定がデバイスに再度適用されます。モードが自律型 AP モードに変更された時に、最後のサーバーから受信したコンフィグレーション設定がバックアップされています。

下図は、アクセスポイント(AP)の CLI で set server mode コマンドを表示しています。



NECプラットフォームズ株式会社
自律型 AP モード設定ガイド　第 4 版

2018 年 4 月
AM1-002909-004