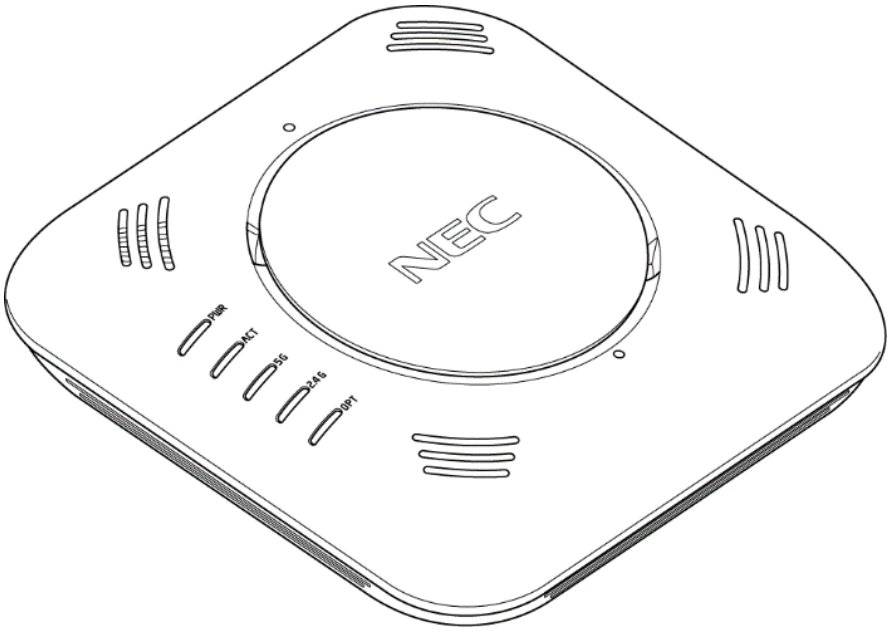
IEEE802.11ac 対応無線 LAN アクセスポイント

NA1500A



設定事例集

第 3.0.1 版

ご注意

本装置をご使用の前に、本書をよくお読みください。

お読みになったあとは、いつでもご覧になれる場所に必ず保管してください。

＜はじめに＞

このたびは IEEE802.11ac 対応無線 LAN アクセスポイント NA1500A をご利用いただき、まことにありがとうございます。

本書では、本装置に搭載されている各機能の詳細について説明します。

各コマンドの詳細については、「コマンドリファレンスガイド」を参照してください。
なお、本書は NA1500A ソフトウェアバージョン 3.0 に対応しています。

【ご注意】

(1) 本書の内容の一部または全部を無断転載･無断複写することは禁止されています。
(2) 本書の内容については、将来予告なしに変更することがあります。
(3) 本書の内容については万全を期して作成いたしましたが、万一ご不審な点や誤り･記載もれなどお気づきの点がありましたらご連絡ください。
(4) 本商品の故障・誤動作・天災・不具合あるいは停電などの外部要因によって通信などの機会を逸したために生じた損害などの純粋経済損失につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。
(5) セキュリティ対策をほどこさず、あるいは、無線 LAN の仕様上やむをえない事情によりセキュリティの問題が発生してしまった場合、当社は、これによって生じた損害に対する責任はいっさい負いかねますのであらかじめご了承ください。
(6) せっかくの機能も不適切な扱いや不測の事態（例えば落雷や漏電など）により故障してしまっては能力を発揮できません。「取扱説明書」をよくお読みになり、記載されている注意事項を必ずお守りください。

＜目次＞

第1章　　コンフィグレーションモード

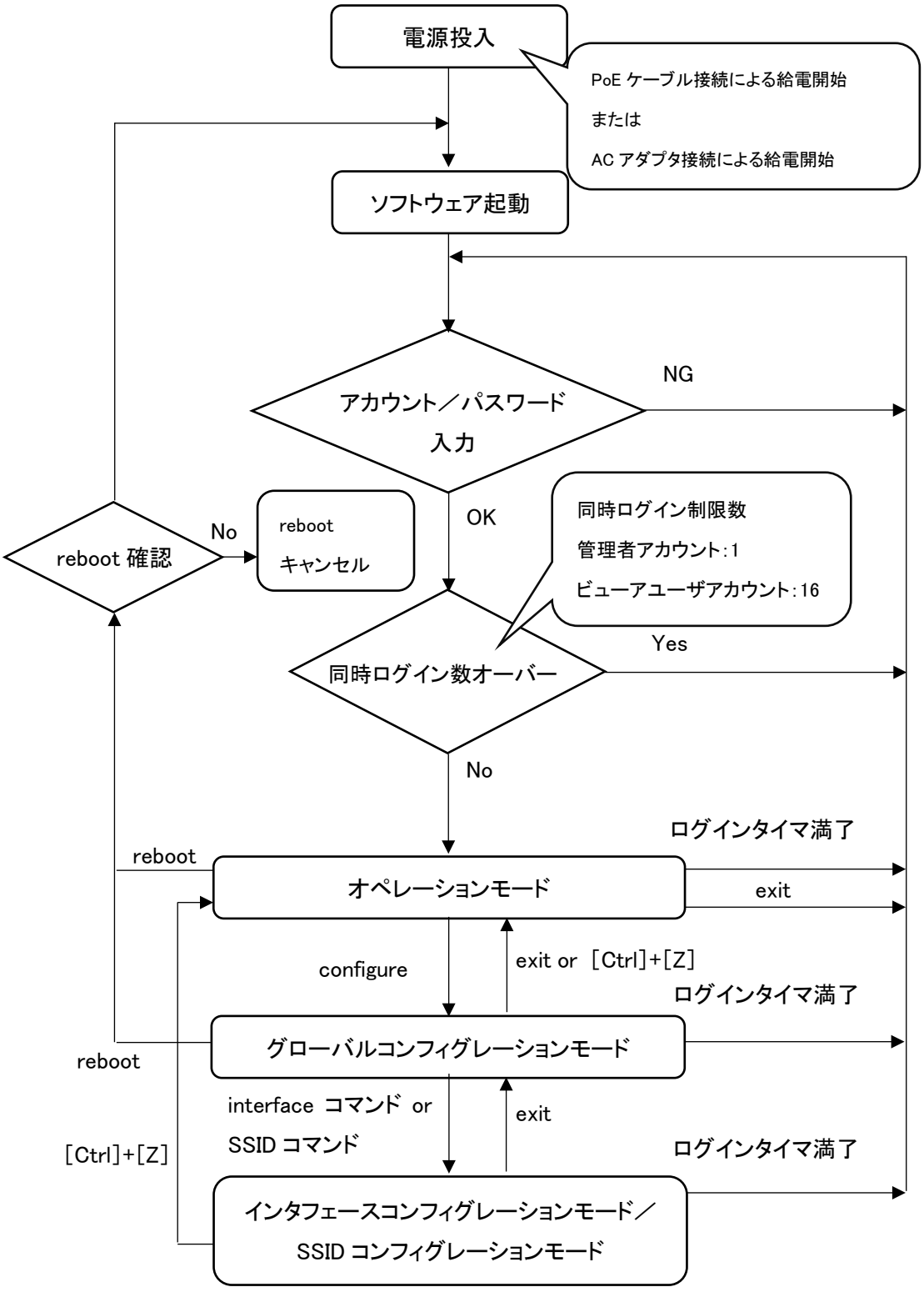
本章は、各インタフェースの設定とコンフィグレーションモードの関係について説明します。

1.1. インタフェースとコンフィグレーションモードについて

本書は、ネットワーク構成図と設定例をもとに記述しています。
ご利用いただけるインタフェース名ならびに対応するコンフィグレーションモード名は、
以下となります。

物理／論理インタフェース名称	コンフィグレーションモード名
VLAN インタフェース （論理インタフェース）	VLAN インタフェースコンフィグレーションモード
LAN1/PoE ポート （物理／基本インタフェース）	GigaEthernet0 インタフェースコンフィグレーションモード
LAN1/PoE ポート （仮想インタフェース）	GigaEthernet0.<Virtual Interface ID> インタフェースコンフィグレーションモード Virtual Interface ID は、1～16 で、最大 16 個まで使用可能
LAN2 ポート （物理／基本インタフェース）	GigaEthernet1 インタフェースコンフィグレーションモード
LAN2 ポート （仮想インタフェース）	GigaEthernet1.<Virtual Interface ID> インタフェースコンフィグレーションモード Virtual Interface ID は、1～16 で、最大 16 個まで使用可能
5GHz 帯無線インタフェース	radio0 インタフェースコンフィグレーションモード
2.4GHz 帯無線インタフェース	radio1 インタフェースコンフィグレーションモード
SSID	SSID コンフィグレーションモード

1.2. モード遷移


電源投入
PoE ケーブル接続による給電開始
または
AC アダプタ接続による給電開始
ソフトウェア起動
アカウント／パスワード
入力
NG
OK
同時ログイン制限数
管理者アカウント：1
ビューアユーザアカウント：16
reboot 確認
No
reboot
キャンセル
同時ログイン数オーバー
Yes
No
ログインタイマ満了
reboot
オペレーションモード
exit
configure
exit or ［Ctrl］+[Z]
ログインタイマ満了
グローバルコンフィグレーションモード
reboot
interface コマンド or
SSID コマンド
exit
[Ctrl]+[Z]
ログインタイマ満了
インタフェースコンフィグレーションモード／
SSID コンフィグレーションモード

第2章　　ログイン

本章は、ログイン方法について説明します。

2.1. 管理者アカウントで利用する

管理者アカウントで使用する場合

初回ログイン時

login config

Password config

初回ログインするとユーザ名とパスワードの変更を求められます。

変更後、write memory を必ず行ってください。

write memory 後、新たなユーザ名、パスワードにてログインしてください。

ログインすると以下のプロンプトが表示され、オペレーションモードが表示されます。

AP#

2.2. ビューアユーザアカウントで利用する

登録済みビューアユーザのアカウント／パスワードで、ログインします。

例

login: Taro_XXXX　　登録済みビューアユーザアカウント

Password: XXXXXXXXXX　　登録済みビューアユーザパスワード

ログインすると以下のプロンプトが表示され、オペレーションモードが表示されます。

AP#

ビューアユーザのアカウントで使用できるコマンド一覧

オペレーションモード	グローバルコンフィグレーションモード
configure exit show copyright	exit ?(help 相当) show arp entry show arp statistics show associations show buffers show clock show copyright show error-log show hardware show interfaces show ip filter show led show logging show mac filter show memory show ntp show power inline show processes show radio-noll show rogue ap show snmp-agent community show ssh-server sessions show terminal show uptime show version

2.3. グローバルコンフィグレーションモードに遷移する

以下コマンドにて、グローバルコンフィグレーションモードに移行ができます。

```
AP# configure
Enter configuration commands, one per line. End with CTRL+Z.
AP(config)#
```

上記のとおり、プロンプトが変化します。

第3章　　共通設定

本章は、システムの共通設定について説明します。

3.1. システム設定（装置共通の設定）

3.1.1. ターミナルの表示長さの制限を変更する

以下コマンドにて、ターミナルの表示長さ制限を変更できます。

100 行に制限する場合

```
AP(config)# terminal length 100
AP(config)# write memory
```

長さ制限を行わない場合

```
AP(config)# terminal length 0
AP(config)# write memory
```

3.1.2. ターミナルのログインタイムアウト値を変更する

以下コマンドにて、ターミナルのログインタイムアウト値を変更できます。

タイムアウト時間を 10 分に設定する場合

```
AP(config)# terminal timeout 10
AP(config)# write memory
```

タイムアウトしないようにする場合

```
AP(config)# terminal timeout 0
AP(config)# write memory
```

3.1.3. バージョンを確認する

以下コマンドにて、バージョンの確認ができます。

```
AP(config)# show ver
Boot ver.       : Boot Version X.X.X
FW
   Boot side            : normal
   FW ver.              : Y.Y.Y
   FW ver.(backup)   : Z.Z.Z
```

3.1.4. 日時を設定する

以下コマンドにて、日時の設定ができます。

```
AP(config)# clock 17 20 0 31 5 2018
% Thu May 31 17:20:00 JST 2018
```

日時設定項目は、以下のとおりです。
clock HOUR MINUTE SECONDS [DATE [MONTH [YEAR]]]

3.1.5. ホスト名を設定する

以下コマンドにて、ホスト名表示を変更できます。

```
AP(config)# hostname na1500a
AP(config)# write memory
```

3.2. ビューアユーザを登録する

ビューアユーザアカウントは、1 つだけ作成できます。
以下のビューアユーザ名／ビューアユーザパスワードを登録したい場合、
次の設定を行います。

例　　ユーザ名:　　Taro_XXXX
　　パスワード:　　Taro_XXXX_abcd_12345678

AP(config)# username Taro_XXXX Taro_XXXX_abcd_12345678
AP(config)# write memory

登録に使用できる文字は、以下のとおりです。
ユーザ名
　　アスキー文字列。大文字／小文字は区別されます。
　　範囲: 8～16 文字
　　　　使用できる文字
　　　　アルファベット半角大文字（A～Z）
　　　　アルファベット半角小文字（a～z）
　　　　数字半角（0～9）
　　　　記号半角「-（ハイフン）」、「_（アンダースコア）」
　　　　※ただし、先頭文字に ″-″(ハイフン) は利用不可です。
パスワード
　　アスキー文字列。大文字／小文字は区別されます。
　　範囲: 8～249 文字
　　　　使用できる文字
　　　　アルファベット半角大文字（A～Z）
　　　　アルファベット半角小文字（a～z）
　　　　数字半角（0～9）
　　　　記号半角（わかりやすくするために全角で表示しています。）

!	“	#	$	%	&	(	)
*	+	、	ー	.	／	:	;
<	=	>	@	[	＼	]	^
_	{	|	}	～			

第4章　　設定事例

各種機能の設定について説明します。

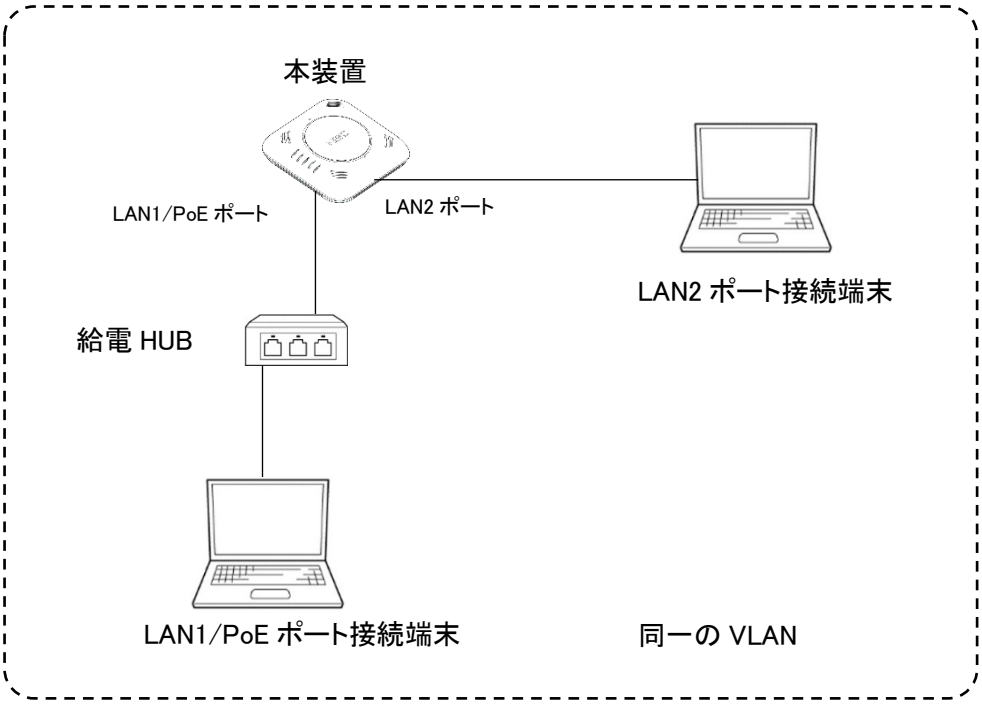
4.1. 設定事例 1 LAN1/PoE ポートと LAN2 ポートの利用

1 つの VLAN 内に

LAN1/PoE ポート

LAN2 ポート

の構成を登録して利用する場合の事例です。



4.1.1. VLAN を作成する

以下のコマンドにて、設定可能 VLAN_id を確認できます。

```
AP(config)# interface vlan ?
  <1-4094>  -- config_interface_vlan
  u         -- config_interface_vlan
```

ソフトウェアバージョンにより同時に使用できる VLAN の組み合わせが異なります。

ソフトウェアバージョン 1.0 は、Untagged-VLAN（vlan_id は、u）または、Tagged-VLAN（vlan_id は、1～4094）のいずれかしか設定できません。
そのため、複数の VLAN を同時に使用したい場合は、Tagged-VLAN を使用します。
（Tagged パケットによる使用）

ソフトウェアバージョン 2.0 以降は、Untagged-VLAN（vlan_id は、u）と Tagged-VLAN（vlan_id は、1～4094）を、同時に使用できます。

いずれのソフトウェアバージョンでも Untagged-VLAN は、1 つまでしか使用できません。

4.1.1.1. Untagged-VLAN を設定する

使用する装置の IP アドレスを

・固定設定する場合

・DHCP による自動割り当てを使用する場合

・IP アドレスを割り当てない

のいずれかにより、次の設定を行ってください。

IP アドレスは、複数の VLAN を使用する場合、いずれかの VLAN にて、1 つまで設定が可能です。

（1）　IP アドレスを固定設定する

以下は、IP アドレスを固定で使用する場合の例です。

```
AP(config)# interface vlan u
AP(config-vlan u)# ip address 192.168.1.245/24
AP(config-vlan u)# ip route 192.168.1.1
AP(config-vlan u)# dns server 192.168.1.1
AP(config-vlan u)# vlan enable
AP(config-vlan u)# exit
AP(config)# write memory
```

（2）　IP アドレスの DHCP による自動割り当てを使用する

以下は、IP アドレス、ゲートウェイアドレス、DNS サーバアドレスの DHCP による自動割り当てを使用する場合の例です。

```
AP(config)# interface vlan u
AP(config-vlan u)# ip address dhcp
AP(config-vlan u)# dns server dhcp
AP(config-vlan u)# vlan enable
AP(config-vlan u)# exit
AP(config)# write memory
```

DNS サーバは、複数設定が可能です。
使用しない DNS サーバは、以下のコマンドで削除が可能です。
登録済み DNS サーバ(192.168.1.1)を削除する場合は、以下のとおりです。

```
AP(config)# interface vlan u
AP(config-vlan u)# no dns server 192.168.1.1
AP(config-vlan u)# exit
AP(config)# write memory
```

4.1.1.2. Tagged-VLAN（例 vlan_id=2）を設定する

使用する装置の IP アドレスを

・固定設定する場合

・DHCP による自動割り当てを使用する場合

・IP アドレスを割り当てない

のいずれかにより、次の設定を行ってください。

IP アドレスは、複数の VLAN を使用する場合、いずれかの VLAN にて、1 つまで設定が可能です。

（1） IP アドレスを固定設定する

以下のコマンドにて、VLAN に固定アドレスを設定することができます。

```
AP(config)# interface vlan 2 ・・・・・・・・vlan_id=2 を指定
AP(config-vlan 2)# ip address 192.168.1.245/24
AP(config-vlan 2)# ip route 192.168.1.1
AP(config-vlan 2)# dns server 192.168.1.1
AP(config-vlan 2)# vlan enable
AP(config-vlan 2)# exit
AP(config)# write memory
```

（2） IP アドレスの DHCP による自動割り当てを使用する

以下は、IP アドレス、ゲートウェイアドレス、DNS サーバアドレスの DHCP による自動割り当てを使用する場合の例です

```
AP(config)# interface vlan 2
AP(config-vlan 2)# ip address dhcp
AP(config-vlan 2)# dns server dhcp
AP(config-vlan 2)# vlan enable
AP(config-vlan 2)# exit
AP(config)# write memory
```

DNS サーバは、複数設定が可能です。
使用しない DNS サーバは、以下のコマンドで削除が可能です。
登録済み DNS サーバ(192.168.1.1)を削除する場合は、以下のとおりです。

```
AP(config)# interface vlan 2
AP(config-vlan u)# no dns server 192.168.1.1
AP(config-vlan u)# exit
AP(config)# write memory
```

4.1.2. LAN1/PoE ポートと LAN2 ポートを設定する

以降、LAN1/PoE ポート（GigaEthernet0）インタフェースを例に説明します。
LAN2 ポート（GigaEthernet1）を設定したい場合は、GigaEthernet0 を GigaEthernet1 に読み替えて設定します。

4.1.2.1 LAN1/PoE ポートの物理インタフェースを設定する

以下のコマンドにて、物理インタフェースの設定を行うことができます。

```
AP(config)# interface GigaEthernet0
AP(config-if-GigaEthernet0)# port-speed auto  ･･･スピード/Duplex を Auto に設定
AP(config-if-GigaEthernet0)# no port-mdi-mdix  ･･･････Mdi/Mdix を Auto に設定
AP(config-if-GigaEthernet0)# no port-shutdown  ･･･････ポートをアクティブに設定
AP(config-if-GigaEthernet0)# exit
AP(config)# write memory
```

4.1.2.2 LAN1/PoE ポートの VLAN を登録する

4.1.2.2.1 LAN1/PoE ポートの VLAN を Untagged-VLAN に接続設定する

以下のコマンドにて、VLAN の設定を行うことができます。

```
AP(config)# interface GigaEthernet0
AP(config-if-GigaEthernet0)# vlan u  ・・・・・・・・・・作成済みの Untagged-VLAN の ID
AP(config-if-GigaEthernet0)# no shutdown
AP(config-if-GigaEthernet0)# exit
AP(config)# write memory
```

4.1.2.2.2 LAN1/PoE ポートの VLAN を Tagged-VLAN に接続設定する

Tagged_VLAN を使用する場合は、下記、仮想インタフェース ID(X)を使用します。

GigaEthernet0.X

下記では、仮想インタフェース ID に「1」を使用します。

```
AP(config)# interface GigaEthernet0.1
AP(config-if-GigaEthernet0.1)# vlan 2  ・・・・・・作成済みの Tagged-VLAN の ID
AP(config-if-GigaEthernet0.1)# no shutdown
AP(config-if-GigaEthernet0.1)# exit
AP(config)# write memory
```

4.1.2.3 LAN2 ポートの物理インタフェースを設定する

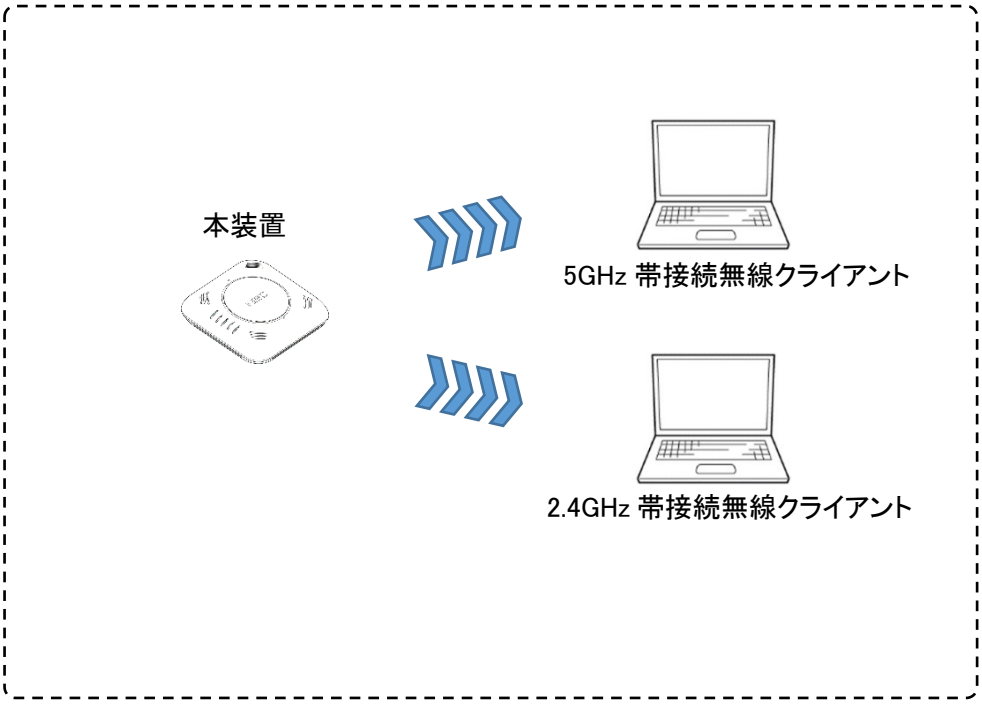
「4.1.2.1 LAN1/PoE ポートの物理インタフェースを設定する」を
LAN2 ポート(GigaEthernet1)に読み替えて設定します。

4.1.2.4 LAN2 ポートの VLAN を登録する

「4.1.2.2 LAN1/PoE ポートの VLAN を登録する」を
LAN2 ポート(GigaEthernet1)に読み替えて設定します。

4.2.　設定事例 2　無線インタフェースの利用

無線インタフェースの設定、SSID 設定についての事例です。



4.2.1. 無線インタフェースを設定する

4.2.1.1. 5GHz 帯無線インタフェース（radio0）を設定する

例 1）以下の内容を設定します。

Channel　　36 固定
通信規格（モード） 11ac を使用
バンド幅　　80MHz

```
AP(config)# interface radio0
AP(config-if-radio0)# channel 36 mode 11ac bandwidth 80
AP(config-if-radio0)# exit
AP(config)# write memory
```

例 2）以下の内容を設定します。

Channel　　36 固定
通信規格（モード） 11ac を使用
バンド幅　　40MHz

```
AP(config)# interface radio0
AP(config-if-radio0)# channel 36 mode 11ac bandwidth 40
AP(config-if-radio0)# exit
AP(config)# write memory
```

例 3）以下の内容を設定します。

Channel　　36 固定
通信規格（モード） 11ac を使用
バンド幅　　20MHz

```
AP(config)# interface radio0
AP(config-if-radio0)# channel 36 mode 11ac bandwidth 20
AP(config-if-radio0)# exit
AP(config)# write memory
```

4.2.1.2. 2.4GHz 帯無線インタフェース（radio1）を設定する

例 1）以下の内容を設定します。

Channel　　1 固定
通信規格（モード）11ng を使用
バンド幅　　40MHz

```
AP(config)# interface radio1
AP(config-if-radio1)# channel 1 mode 11ng bandwidth 40
AP(config-if-radio1)# exit
AP(config)# write memory
```

例 2）以下の内容を設定します。

Channel　　1 固定
通信規格（モード）11ng を使用
バンド幅　　20MHz

```
AP(config)# interface radio1
AP(config-if-radio1)# channel 1 mode 11ng bandwidth 20
AP(config-if-radio1)# exit
AP(config)# write memory
```

4.2.2. SSID を設定する

4.2.2.1. 5GHz 帯無線インタフェース（radio0）専用 SSID を作成する

例）以下の内容を設定します。

SSID 名	test_5G
無線クライアント許容台数	10 台
認証モード	WPA2-PSK
暗号化	AES
パスフレーズ	12345678
接続先 VLAN_id	u
使用周波数	5GHz 帯（radio0）

SSID を作成し SSID コンフィグレーションモードにて設定します。

```
AP(config)# ssid test_5G
AP(config-ssid test_5G)# max-associations 10
AP(config-ssid test_5G)# vlan u・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・vlan_id を指定
AP(config-ssid test_5G)# encryption mode wpa2 aes・・・・・・・・・・・・・・・・・wpa2-aes 指定
AP(config-ssid test_5G)# authentication type psk・・・・・・・・・・・・・・・・・・・・psk 指定
AP(config-ssid test_5G)# encryption wpa-psk-key ascii 12345678・・・パスフレーズ設定
AP(config-ssid test_5G)# radio-device radio0・・・・・・使用する無線インタフェースの指定
AP(config-ssid test_5G)# enable-ssid
AP(config-ssid test_5G)# exit
AP(config)# write memory
```

4.2.2.2. 2.4GHz 帯無線インタフェース（radio1）専用 SSID を作成する

例）以下の内容を設定します。

SSID 名	test_2G
無線クライアント許容台数	10 台
認証モード	WPA2-PSK
暗号化	AES
パスフレーズ	12345678
接続先 VLAN_id	u
使用周波数	2.4GHz 帯（radio1）

SSID を作成し SSID コンフィグレーションモードにて設定します。

```
AP(config)# ssid test_2G
AP(config-ssid test_2G)# max-associations 50
AP(config-ssid test_2G)# vlan u・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・vlan_id を指定
AP(config-ssid test_2G)# encryption mode wpa2 aes・・・・・・・・・・・・・・・・・wpa2-aes 指定
AP(config-ssid test_2G)# authentication type psk・・・・・・・・・・・・・・・・・・・・psk 指定
AP(config-ssid test_2G)# encryption wpa-psk-key ascii 12345678・・・パスフレーズ設定
AP(config-ssid test_2G)# radio-device radio1・・・・・・使用する無線インタフェースの指定
AP(config-ssid test_2G)# enable-ssid
AP(config-ssid test_2G)# exit
AP(config)# write memory
```

4.2.2.3. 5GHz 帯(radio0)/2.4GHz 帯(radio1)用 SSID を作成する

例）以下の内容を設定します。

SSID 名	test_dual
無線クライアント許容台数	10 台
認証モード	WPA2-PSK
暗号化	AES
パスフレーズ	12345678
接続先 VLAN_id	u
使用周波数	5GHz 帯および 2.4GHz 帯（both）

SSID を作成し SSID コンフィグレーションモードにて設定します。

```
AP(config)# ssid test_dual
AP(config-ssid test_dual)# max-associations 10
AP(config-ssid test_dual)# vlan u・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・vlan_id を指定
AP(config-ssid test_dual)# encryption mode wpa2 aes・・・・・・・・・・・・・・・wpa2-aes 指定
AP(config-ssid test_dual)# authentication type psk・・・・・・・・・・・・・・・・・・psk 指定
AP(config-ssid test_dual)# encryption wpa-psk-key ascii 12345678・・パスフレーズ設定
AP(config-ssid test_dual)# radio-device both・・・・・・使用する無線インタフェースの指定
AP(config-ssid test_dual)# enable-ssid
AP(config-ssid test_dual)# exit
AP(config)# write memory
```

4.2.3. 無線インタフェースを有効設定する

4.2.3.1. radio0(5GHz 帯)のみを有効にする

以下のコマンドにて、有効設定ができます。

```
AP(config)# radio-enable radio0
AP(config)# write memory
```

4.2.3.2. radio1(2.4GHz 帯)のみを有効にする

以下のコマンドにて、有効設定ができます。

```
AP(config)# radio-enable radio1
AP(config)# write memory
```

4.2.3.3. radio0(5GHz 帯)/radio1(2.4GHz 帯)とも、有効にする

以下のコマンドにて、有効設定ができます。

```
AP(config)# radio_enable both
AP(config)# write memory
```

4.2.4. ステルス機能を使用する

ステルス機能は、SSID ごとに設定を行います。

設定は、SSID コンフィグレーションモードにて、SSID 単位で行います。
以下のとおり、作成済み SSID にステルス機能を設定します。
SSID 名 :test をステルスにする場合

```
AP(config)# ssid test
AP(config-ssid test)# hide bssid
AP(config-ssid test)# exit
AP(config)# write memory
```

5GHz 帯/2.4GHz 帯にて同一の SSID を使用している場合は、該当 SSID に設定すると
5GHz 帯/2.4GHz 帯両方の該当 SSID に適用されます。
ステルスを解除したい場合は、SSID コンフィグレーションモードで、以下の例のとおり
「no hide bssid」を設定します。

```
AP(config)# ssid test
AP(config-ssid test)# no hide bssid
AP(config-ssid test)# exit
AP(config)# write memory
```

4.2.5. レーダ波検出時のチャネル遷移を無効にする

W53 帯または W56 帯の固定チャネル設定を使用しての動作中に限り、レーダ波を検出した際のチャネル利用について固定チャネルの継続利用を設定することができます。

dfs channel fix コマンドを使用することで、W53 帯または W56 帯の固定チャネルで動作中にレーダ波を検出したとき、他のチャネル利用をしないよう制限することができます。
本コマンドを有効にして W53 帯または W56 帯の固定チャネル使用中、レーダ波を検出すると現在使用のチャネルが、「NOL」にある間は、無線を停波します。
そして「NOL」リストから該当チャネルが消えると同一に使用していた固定チャネルにて無線復旧します。
本コマンドは、動作モードを設定する channel コマンドの内容にて、W53 帯または W56 帯の固定チャネルを設定した場合のみ有効です。

channel コマンドの設定とレーダ波検出時のチャネル遷移動作は、以下のとおりです。

<table>
<tr><td>Channel コマンドで
設定した動作モード</td><td>dfs channel fix 設定時
（固定有効）
レーダ波検出時のチャネル遷移動作</td><td>no dfs channel fix 設定時
（固定無効 = 初期値）
レーダ波検出時のチャネル遷移動作</td></tr>
<tr><td>W52 帯のいずれかの
固定チャネル設定時</td><td colspan="2">W52 帯での使用中は、レーダ波を検出しません。</td></tr>
<tr><td>W53 帯のいずれかの
固定チャネル設定時</td><td rowspan="2">チャネル遷移は行わず、無線停波。
「NOL」リストから該当チャネルが消えると同一固定チャネルにて復旧します。</td><td>W53 帯のいずれかのチャネルに遷移します。</td></tr>
<tr><td>W56 帯のいずれかの
固定チャネル設定時</td><td>W56 帯のいずれかのチャネルに遷移します。</td></tr>
<tr><td>auto-w52 設定時</td><td colspan="2">W52 帯での使用中は、レーダ波を検出しません。</td></tr>
<tr><td>auto-w53 設定時</td><td colspan="2">W53 帯のいずれかのチャネルに遷移します。</td></tr>
<tr><td>auto-w56 設定時</td><td colspan="2">W56 帯のいずれかのチャネルに遷移します。</td></tr>
<tr><td>auto-w52-w53 設定時</td><td colspan="2">W53 帯にて通信時、W52/W53 帯のいずれかのチャネルに遷移します。
（W52 帯での使用中は、レーダ波を検出しません。）</td></tr>
<tr><td>auto-w52-w56 設定時</td><td colspan="2">W56 帯にて通信時、W52/W56 帯のいずれかのチャネルに遷移します。
（W52 帯での使用中は、レーダ波を検出しません。）</td></tr>
<tr><td>auto-w53-w56 設定時</td><td colspan="2">W53/W56 帯のいずれかのチャネルに遷移します。</td></tr>
<tr><td>Auto 設定時</td><td colspan="2">W52/W53/W56 帯のいずれかのチャネルに遷移します。
（W52 帯での使用中は、レーダ波を検出しません。）</td></tr>
</table>

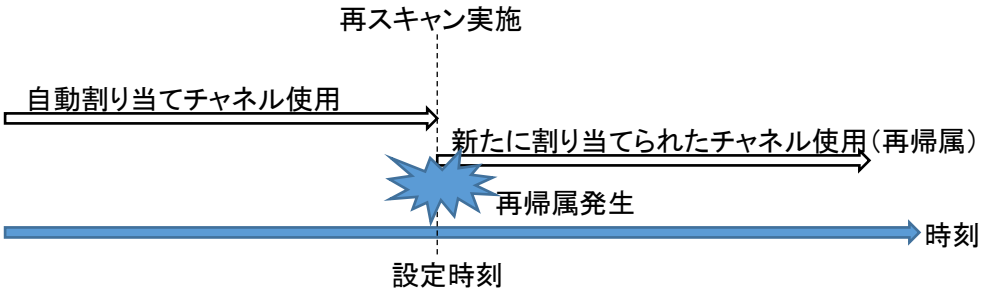
本設定は、5GHz 帯の radio0 インタフェースコンフィグレーションモードのみ設定できます。

AP(config) interface radio0・・・・・・・radio0 インタフェースコンフィグレーションモード移行
AP(config-if-radio0)# dfs channel fix・・・・固定チャネル使用有効を設定
AP(config-if-radio0)# exit

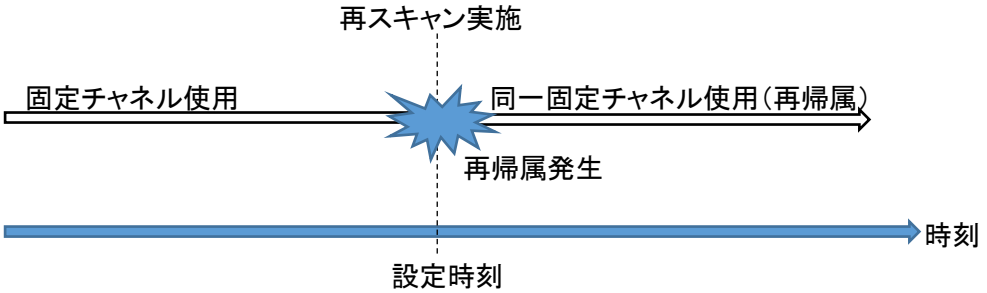
4.2.6. チャネル自動再スキャンスケジュールを設定する

設定した時刻に空きチャネルを自動的に再スキャンすることができます。
無線インタフェース(radio0／radio1)ごとに、最大 2 つまで時刻を設定することができます。
また、設定時刻の時点で、帰属無線クライアントがある場合、初期状態では再スキャンを行わない設定ですが、再スキャンを強制的に行う設定も可能です。
自動チャネル割り当てにて使用中、再スキャンを強制的に行う設定になっている場合、設定時刻にいったん帰属が外れ、無線クライアントの再帰属が発生します。
固定チャネル使用時、再スキャンを強制的に行う設定になっている場合、設定時刻にいったん帰属が外れますが、無線クライアントは、再度同一固定チャネルにて使用を開始します。

チャネル自動設定の場合(channel-scan-schedule force 有効時)



固定チャネル設定の場合(channel-scan-schedule force 有効時)



本設定は、radio0 または radio1 のインタフェースコンフィグレーションモードにて設置が可能です。

AP(config)# interface radio0・・・・・・・・・インタフェースコンフィグレーションモードに遷移
AP(config-if-radio0)# channel-scan-schedule add 23:30
・・・・・・・・再スキャン時刻 23:30 に設定
AP(config-if-radio0)# no channel-scan-schedule force
・・・・・・・・帰属無線クライアントがある場合、
再スキャンを実施しない
AP(config-if-radio0)# channel-scan-schedule enable
・・・・・・・・自動再スキャンスケジュール有効
AP(config-if-radio0)# exit

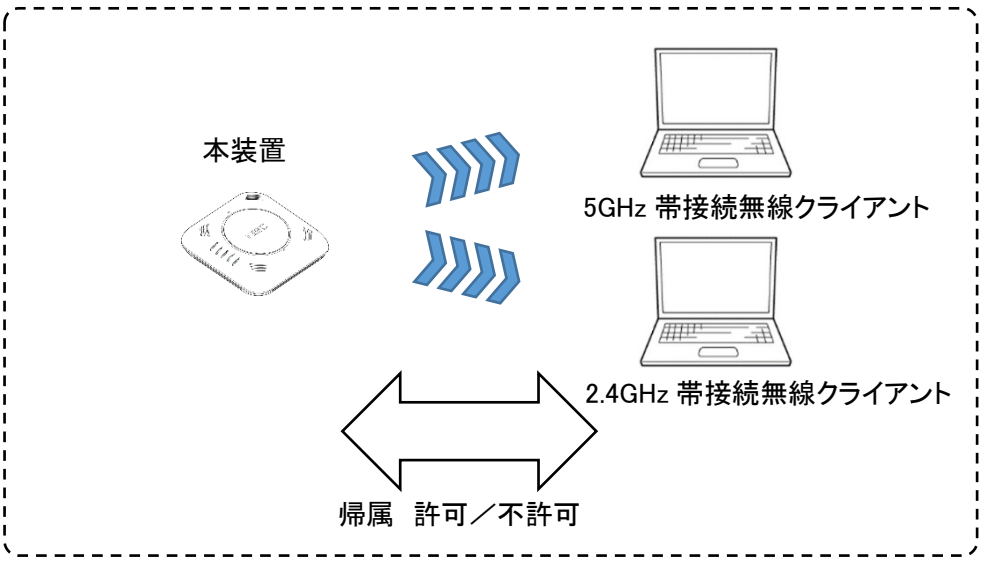
4.3.　設定事例 3　無線クライアントの帰属管理

無線クライアントの帰属管理は、
無線クライアント用 MAC アドレスフィルタリング機能を使用します。
設定／リスト変更／解除には、おのおの以下のステップを行います。
また、変更後、「write memory」と「reboot」による再起動を実行することで、適用されます。

＜設定＞
① MAC アクセスリストの登録
② フィルタの設定適用
③ write memory 実行
④ reboot 実行

＜リスト変更（フィルタの設定適用済み）＞
① MAC アクセスリストの追加／削除
② write memory 実行
③ reboot 実行

＜解除＞
① フィルタの設定無効
② MAC アクセスリストの削除（再度同じ内容で使用する場合は、削除不要）
③ write memory 実行
④ reboot 実行



4.3.1. MAC アクセスリストを登録／削除する

MAC アドレスフィルタリング機能は、無線クライアントの帰属管理に使用します。
そのため、MAC アクセスリストならびに適用設定は、SSID 単位で行います。
5GHz 帯/2.4GHz 帯にて同一の SSID を使用している場合は、該当 SSID に設定すると
5GHz 帯/2.4GHz 帯両方に適用されます。
MAC アクセスリストの登録／削除には、「write memory」と「reboot」による再起動が必要です。

4.3.1.1. MAC アクセスリストに無線クライアントを登録する

登録対象 SSID	test
登録 MAC アドレス	AA:AA:AA:AA:AA:AA
	BB:BB:BB:BB:BB:BB
	E4:B3:18:A5:7B:E3

以下のコマンドにて、対象の無線クライアントを追加します。
MAC アクセスリストの登録には、write memory だけでなく、再起動が必要です。

```
AP(config)# ssid test
AP(config-ssid test)# mac access-list add AA:AA:AA:AA:AA:AA
AP(config-ssid test)# mac access-list add BB:BB:BB:BB:BB:BB
AP(config-ssid test)# mac access-list add E4:B3:18:A5:7B:E3
AP(config-ssid test)# exit
AP(config)# write memory
AP(config)# reboot
Are you want to reboot the AP? (Yes or [No]): y
# reboot....
```

4.3.1.2. MAC アクセスリストから無線クライアントを削除（個別）する

削除対象 SSID	test
削除 MAC アドレス	E4:B3:18:A5:7B:E3

以下のコマンドにて、対象の無線クライアントをリストから個別に削除します。
MAC アクセスリストの削除には、write memory だけでなく、再起動が必要です。

```
AP(config)# ssid test
AP(config-ssid test)# mac access-list del E4:B3:18:A5:7B:E3
AP(config-ssid test)# exit
AP(config)# write memory
AP(config)# reboot
Are you want to reboot the AP? (Yes or [No]): y
# reboot....
```

4.3.1.3. MAC アクセスリストから無線クライアントを削除（一括）する

削除対象 SSID	test
削除 MAC アドレス	登録している MAC アドレスすべて

以下のコマンドにて、リストに登録している無線クライアントの MAC アドレスを一括削除します。
MAC アクセスリストの一括削除には、「write memory」と「reboot」による再起動が必要です。

```
AP(config)# ssid test
AP(config-ssid test)# no mac access-list
AP(config-ssid test)# exit
AP(config)# write memory
AP(config)# reboot
Are you want to reboot the AP? (Yes or [No]): y
# reboot....
```

4.3.2. MAC アクセスリストを適用する

SSID 単位で、MAC アクセスリストは、1 つずつ持つことができます。
登録した MAC アクセスリストに対して、

allow	:アクセスリストに登録した無線クライアントの接続を許可します。
deny	:アクセスリストに登録した無線クライアントの接続を不許可にします。
disable	:アクセスリストによるチェック機能を無効にします。

を行うことができます。
本コマンドは、「write memory」のみで反映されます。「reboot」による再起動は必要ありません。

4.3.2.1. 登録した無線クライアントの帰属を許可する

mac access-list に登録した無線クライアントに帰属を許可します。

```
AP(config)# ssid test
AP(config-ssid test)# mac filter allow
AP(config-ssid test)# exit
AP(config)# write memory
```

4.3.2.2. 登録した無線クライアントの帰属を不許可にする

mac access-list に登録した無線クライアントに帰属を不許可にします。

```
AP(config)# ssid test
AP(config-ssid test)# mac filter deny
AP(config-ssid test)# exit
AP(config)# write memory
```

4.3.2.3. 登録した無線クライアントアクセスリストを無効にする

mac access-list を無効にします。
本設定を行っても、MAC アクセスリストの設定内容は、消去されません。

```
AP(config)# ssid test
AP(config-ssid test)# mac filter disable
AP(config-ssid test)# exit
AP(config)# write memory
```

または、

```
AP(config)# ssid test
AP(config-ssid test)# no mac filter
AP(config-ssid test)# exit
AP(config)# write memory
```

4.3.3. MAC アクセスリストの適用状態を確認する

下記コマンドにて、MAC アクセスリストの設定内容ならびに適用状態を確認できます。

```
AP(config)# show mac filter
```

アクセスリストおよび適用状態の設定後の読み出し例は次のとおりです。
以下の例は、5GHz 帯/2.4GHz 帯で、同一の SSID を使用して、許可設定を行った場合の内容になります。

```
AP(config)# show mac filter
[radio0]
SSID:test
   AccessType:allow
      aa:aa:aa:aa:aa:aa
      bb:bb:bb:bb:bb:bb
      e4:b3:18:a5:7b:e3

[radio1]
SSID:test2
   AccessType:allow
      aa:aa:aa:aa:aa:aa
      bb:bb:bb:bb:bb:bb
      e4:b3:18:a5:7b:e3
```

4.4.　設定事例 4　RADIUS サーバ認証の設定

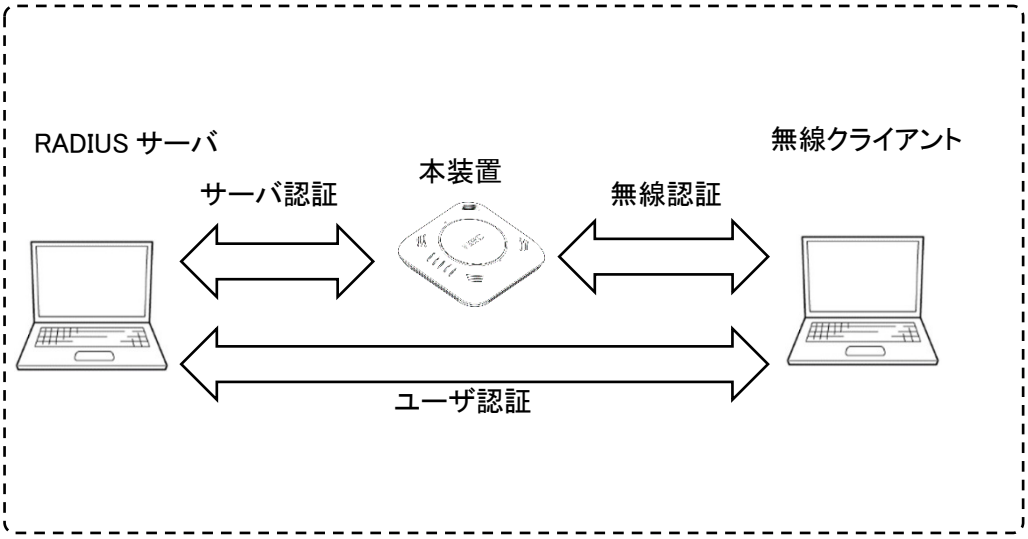
RADIUS サーバを用いて認証を行うための各種設定は、SSID 単位で行います。
ここでは、

サーバ認証　　RADIUS サーバと NA1500A 間の認証
無線認証　　無線クライアントと NA1500A 間の無線暗号化と認証

を説明します。

RADIUS サーバのユーザ認証は、各無線クライアントと RADIUS サーバ間で実施します。
無線クライアントのユーザ設定、RADIUS サーバ側の認証設定、ユーザ設定は、
ご使用になっている RADIUS サーバの説明書などを参照してください。

ソフトウェアバージョン 2.0 以降は、RADIUS サーバを 2 台まで接続可能です。



4.4.1. 使用するプライマリ RADIUS サーバを設定する

無線認証関連設定例は、以下のとおりです。

SSID 名	test_radius
無線クライアント許容台数	10 台
認証モード	WPA2 エンタープライズ-802.1X
暗号化	AES

サーバ認証関連設定例は、以下のとおりです。

RADIUS サーバの IP アドレス	192.168.1.11
アカウンティングポート	ポート 1813
認証ポート	ポート 1812
最大送信回数（初回含む）	5 回
再送時のタイムアウト時間	3 秒
共有鍵が、平文 or 暗号	平文
事前共有鍵	87654321

SSID を作成し SSID コンフィグレーションモードにて設定します。
以下は最低限の設定になります。
接続先無線インタフェースならびに接続先 VLAN インタフェース等に関する設定は、
「4.2.設定事例 2　無線インタフェースの利用」を参照してください。

```
AP(config)# ssid test_radius・・・・・・・・・・・・・・・・・・・・・・・・RADIUS サーバ認証用 SSID
AP(config-ssid test_radius)# max-associations 10・・・・・・無線クライアント接続許容台数
AP(config-ssid test_radius)# encryption mode wpa2 aes・・・・①
AP(config-ssid test_radius)# authentication type dot1x・・・・・①
                                                    無線クライアントとの認証／暗号設定
                                                    （WPA2 エンタープライズ-802.1X/AES）
AP(config-ssid test_radius)# radius host ip 192.168.1.11 ・・・
                                                        プライマリ RADIUS サーバの
                                                        IP アドレス
                                                acct-port 1813 ・・アカウンティングポート
                                                        アカウンティング機能を使用し
                                                        ない場合は、0 を入力します。
                                                        本オプション省略時は、
```

前の状態を引き継ぎます。
auth-port 1812 ・・認証ポート
認証機能を使用しない場合
は、0 を入力します。
本オプション省略時は、
前の状態を引き継ぎます。
retransmit 5 ・・・・・最大送信回数（初回含む）[回]
timeout 3 ・・・・・・・再送時のタイムアウト時間[秒]
key 0 ・・・・・・・・・共有鍵が、平文か暗号か指定
暗号化は将来予定となります。
87654321・・・・・・・事前共有鍵

```
AP(config-ssid test_radius)# radio-device radio0・・・・5GHz 帯無線インタフェース使用
AP(config-ssid test_radius)# enable-ssid・・・・・・・・・・・・・SSID 有効
AP(config-ssid test_radius)# exit
AP(config)# write memory
AP(config)#
```

4.4.2. 使用するセカンダリ RADIUS サーバを設定する

ソフトウェアバージョン 2.0 以降は、RADIUS サーバを 2 台まで登録することができます。
また、「4.4.1.使用するプライマリ RADIUS サーバを設定する」を先に設定を行わないとセカンダリ RADIUS サーバを設定することはできません。

セカンダリ RADIUS サーバは、SSID コンフィグレーションモードにて設定します。
以下は最低限の設定になります。

```
AP(config)# ssid test_radius・・・・・・・・・・・・・・・・・・・・・・・・RADIUS サーバ認証用 SSID
AP(config-ssid test_radius)# radius secondary-host ip 192.168.1.11・・・・
                                                    セカンダリ RADIUS サーバの
                                                    IP アドレス
                                  acct-port 1813 ・・アカウンティングポート
                                                    アカウンティング機能を使用し
                                                    ない場合は、0 を入力します。
                                                    本オプション省略時は、
                                                    前の状態を引き継ぎます。
                                  auth-port 1812 ・・認証ポート
                                                    認証機能を使用しない場合
                                                    は、0 を入力します。
                                                    本オプション省略時は、
                                                    前の状態を引き継ぎます。
AP(config-ssid test_radius)# radio-device radio0・・・・・・5GHz 帯無線インタフェース使用
AP(config-ssid test_radius)# enable-ssid・・・・・・・・・・・・・SSID 有効
AP(config-ssid test_radius)# exit
AP(config)# write memory
AP(config)#
```

4.4.3. RADIUS サーバへのアクセスブロックを設定する

ソフトウェアバージョン 2.0 以降は、RADIUS サーバを 2 台まで登録することができます。
RADIUS サーバを 2 台使用する場合に限りプライマリ RADIUS サーバへのアクセスブロックを設定することができます。
本設定値は、プライマリサーバ／セカンダリサーバで共通に使用します。
プライマリサーバで認証エラーとなった場合、設定した期間は、プライマリ RADIUS サーバとの認証を行わず、セカンダリサーバと認証を行います。
期間満了時にはプライマリサーバへ認証先の切り戻しを行います。
この設定はセカンダリサーバが設定されている場合にのみ有効です。

RADIUS サーバへのアクセスブロックは、SSID コンフィグレーションモードにて設定します。
以下は最低限の設定になります。

```
AP(config)# ssid test_radius・・・・・・・・・・・・・・・・・・・・・・・・RADIUS サーバ認証用 SSID
AP(config-ssid test_radius)# radius deadtime 10・・・・・・・・アクセスブロック時間 10 分
AP(config-ssid test_radius)# radio-device radio0・・・・・・5GHz 帯無線インタフェース使用
AP(config-ssid test_radius)# enable-ssid・・・・・・・・・・・・・SSID 有効
AP(config-ssid test_radius)# exit
AP(config)# write memory
AP(config)#
```

4.4.4. RADIUS サーバへの再認証間隔を設定する

RADIUS サーバへ再認証する時間間隔を設定します。
本設定値は、プライマリサーバ／セカンダリサーバで共通に使用します。

RADIUS サーバへの再認証間隔は、SSID コンフィグレーションモードにて設定します。
以下は最低限の設定になります。

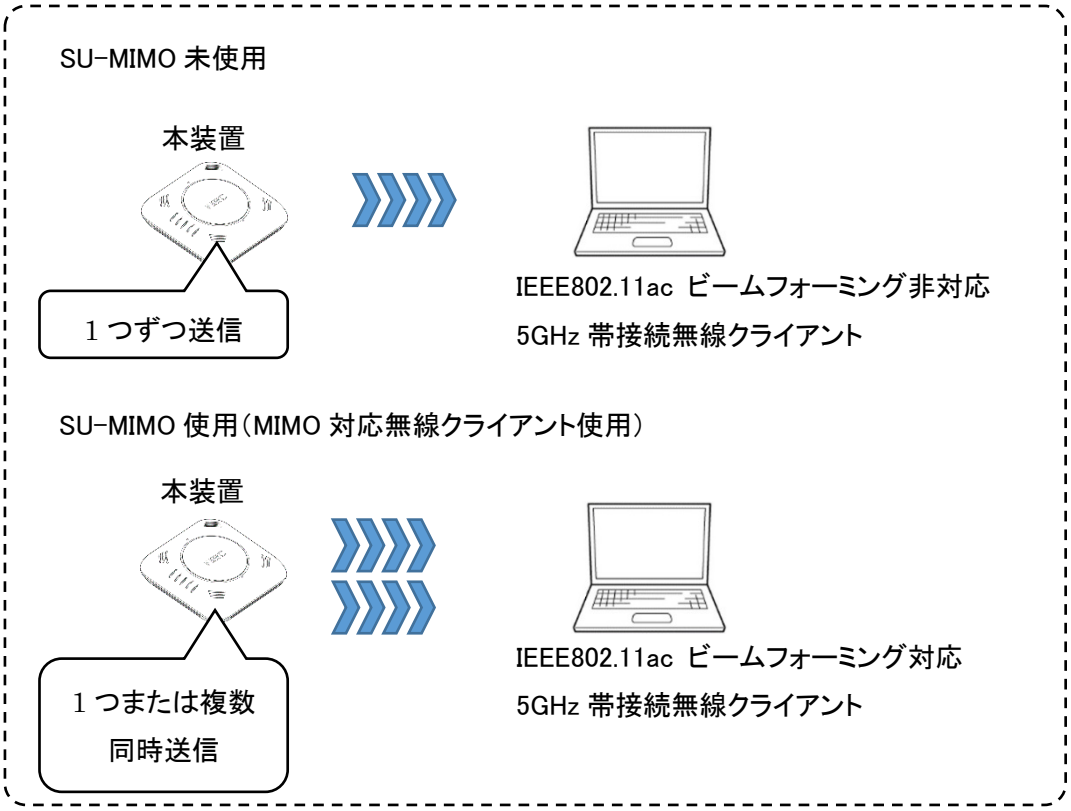
```
AP(config)# ssid test_radius・・・・・・・・・・・・・・・・・・・・・・・・RADIUS サーバ認証用 SSID
AP(config-ssid test_radius)# radius reauthentication 30・・再認証間隔時間  30 分
AP(config-ssid test_radius)# radio-device radio0・・・・・5GHz 帯無線インタフェース使用
AP(config-ssid test_radius)# enable-ssid・・・・・・・・・・・・・SSID 有効
AP(config-ssid test_radius)# exit
AP(config)# write memory
AP(config)#
```

4.5.　設定事例 5　送信ビームフォーミングの設定

本装置は、初期状態では、送信ビームフォーミング（SU-MIMO/MU-MIMO）が、無効設定になっています。
次の設定を行うことで、送信ビームフォーミングを有効にし、スループットを向上させることが可能です。
ただし、本機能を使用する場合、接続する無線クライアントも MIMO 機能を有する必要があります。
MIMO 機能に対応していない無線クライアントを使用する場合、スループットは向上せず、低下する場合があります。
また、本機能は、IEEE802.11ac 以外のモードでは、使用できません。

4.5.1. SU-MIMO を設定する

SU-MIMO 機能は、一度に 1 台の無線クライアントに対し、1 つまたは複数の送信を
同時に行うことができます。

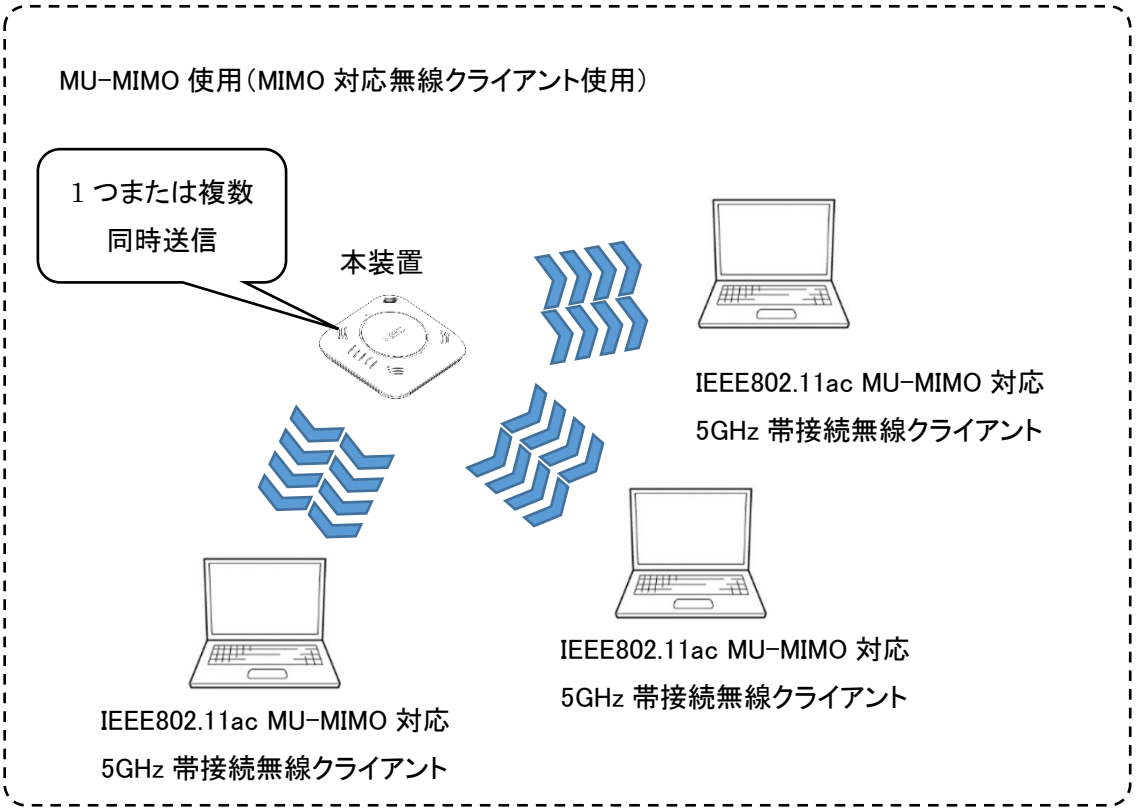


IEEE802.11ac を設定した radio0 インタフェースのみ設定が可能です。

AP(config)# interface radio0
AP(config-if-radio0)# tx-beamform-enable・・・・・・・SU-MIMO 有効
AP(config-if-radio0)# exit
AP(config)# write memory

4.5.2. MU-MIMO を設定する

MU-MIMO は、一度に複数の無線クライアントに対し、1 つまたは複数の送信を
同時に行うことができます。



IEEE802.11ac を設定した radio0 インタフェースのみ設定が可能です。

```
AP(config)# interface radio0
AP(config-if-radio0)# tx-beamform-enable 3・・・・・・・MU-MIMO 有効
AP(config-if-radio0)# exit
AP(config)# write memory
```

4.6.　設定事例 6　リンクインテグリティの設定

リンクインテグリティの機能を使用することで、

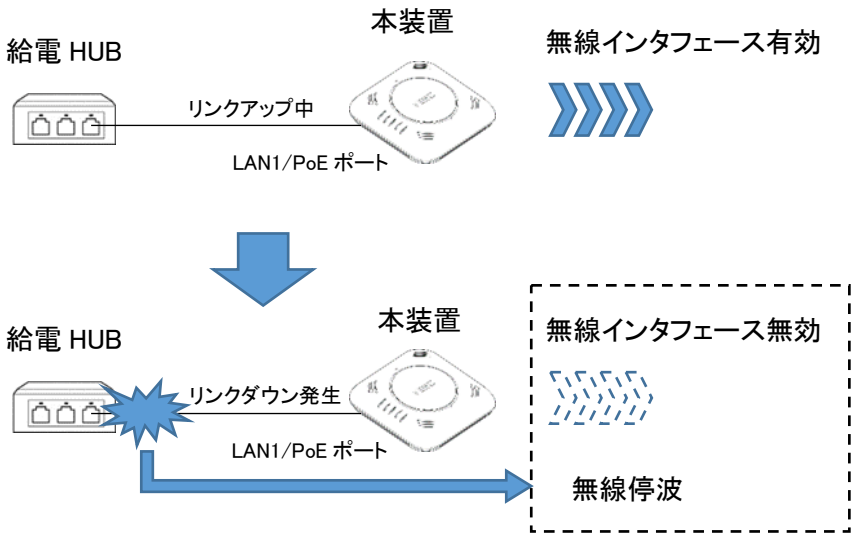
・有線インタフェースのリンク状態

・有線インタフェースに接続したホストとの通信状態

を監視し、無線インタフェースの有効／無効を連動して制御することができます。

有線インタフェース（LAN1/PoE ポート）のリンク状態と無線インタフェースの有効／無効の制御動作は以下のとおりです。

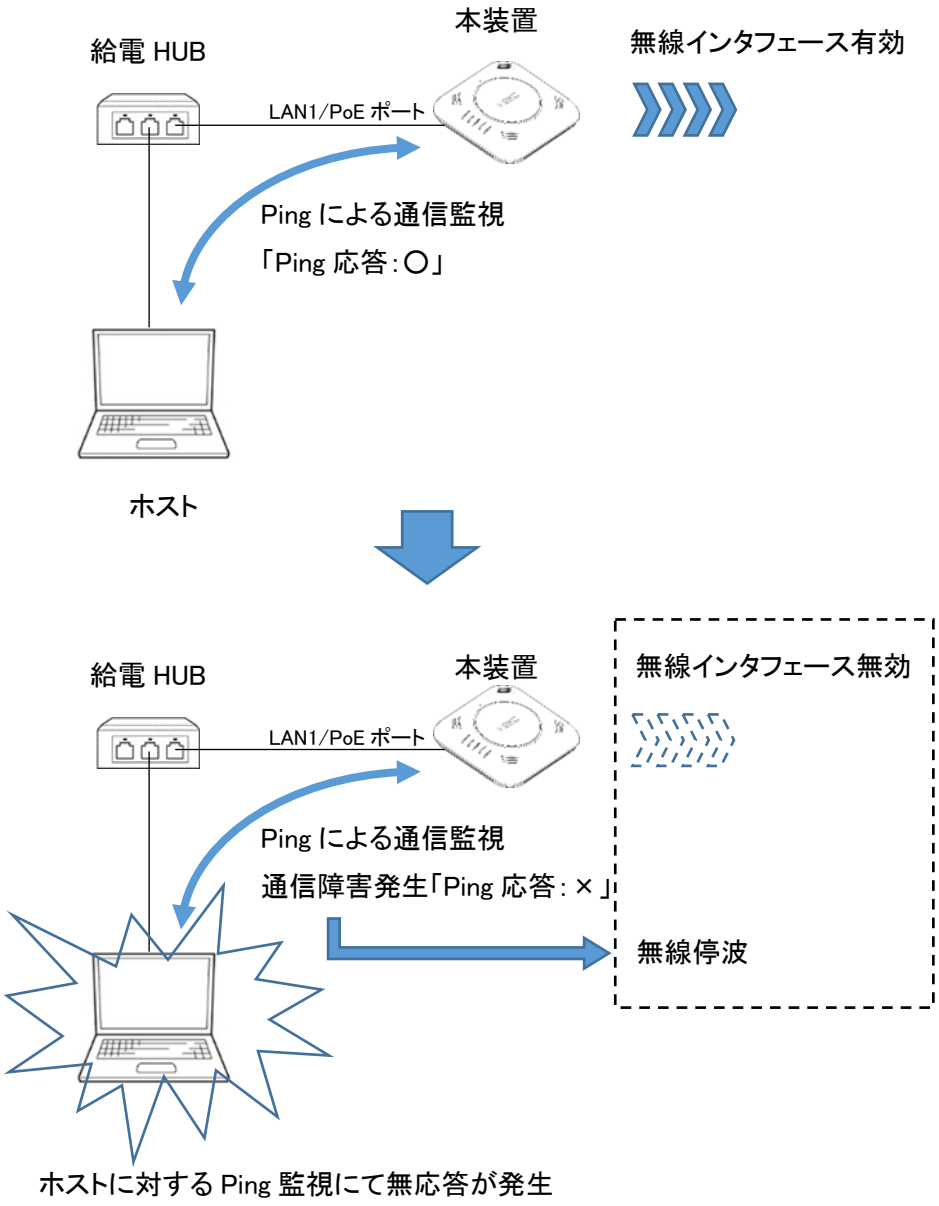
有線インタフェース（LAN1/PoE ポート）が動作中にリンクダウンが発生した場合



LAN1/PoE ポートのリンクダウンを検出すると
無線インタフェースを無効にし、無線を停波します。

有線インタフェースに接続したホストとの通信状態と無線インタフェースの有効／無効の制御動作は以下のとおりです。

有線インタフェース（LAN1/PoE ポート）にネットワーク経由で接続されたホストとの間を Ping にて通信状態監視中、ホストとの間で通信不通が発生した場合



4.6.1. イーサネットインタフェースのリンク監視を設定する

GigaEthernet インタフェースのリンク監視条件を設定します。
リンク監視条件の個別追加／個別削除および clear watchlist interface を行うことで、一括削除を行うことができます。
また、設定を残したまま機能の有効／無効の切り替えを行うことができます。

リンクインテグリティ動作開始条件

指定したインタフェースのリンクダウン継続状態が MONITOR-CYCLE 秒間継続した場合に動作を開始します。

対象インタフェースは GigaEthernet0 のみで、GigaEthernet1 は将来拡張予定です。

リンクインテグリティ動作解除条件

指定したインタフェースがリンクアップになった時点で動作を解除します。

本設定は、管理用 VLAN の VLAN インタフェースコンフィグレーションモードにて設定します。

```
AP(config)# interface vlan u
                        ・・・・・・・・管理用 VLAN インタフェースコンフィグレーションモード移行
AP(config-vlan u)# watchlist interface add  GigaEthernet0
                        ・・・・・・・監視対象のインタフェースを設定
AP(config-vlan u)# watchlist interface enable・・・・・・・リンク監視機能の有効設定
AP(config-vlan u)# exit
```

4.6.2. 通信監視ホストのアドレスと監視条件を設定する

通信監視を行うホストの IP アドレスまたはホスト名を、リストに登録します。
VLAN あたり 4 つまでホストの登録が可能です。
通信監視を行うホストの 個別追加／個別削除および clear watchlist host-ip を行うことで、一括削除を行うことができます。
また、設定した通信監視を行うホストの監視条件を watchlist host-monitor を行うことで、設定することができます。
ホストの通信監視は、設定を残したまま機能の有効／無効の切り替えを行うことができます。

本設定は、管理用 VLAN の VLAN インタフェースコンフィグレーションにて設定します。

```
AP(config)# interface vlan u
                        ・・・・・・・・管理用 VLAN インタフェースコンフィグレーションモード移行
AP(config-vlan u)# watchlist host-ip add 192.168.1.1・・・・・・・・・監視対象のホストを登録
AP(config-vlan u)# watchlist host-monitor monitor-cycle 30 monitor-retry 4
                        ・・・・・・・・Ping 監視周期は、30 秒
                                        Ping 失敗時の再送回数は、4 回
                                        の場合の設定
AP(config-vlan u)# watchlist host-ip enable・・・・・・ホスト通信監視の有効設定
AP(config-vlan u)# exit
```

4.6.3. 無線インタフェースの停止条件を設定する

リンク監視条件ならびに通信監視条件がマッチした場合の、無線側停止条件の有効／無効を設定することができます。
本設定を無効にしている場合は、リンク監視条件ならびに通信監視条件がマッチした場合でも無線側は、停止しません。
ただし、条件を検出した内容のログを残すことはできます。

本設定は、管理用 VLAN の VLAN インタフェースコンフィグレーションにて設定します。

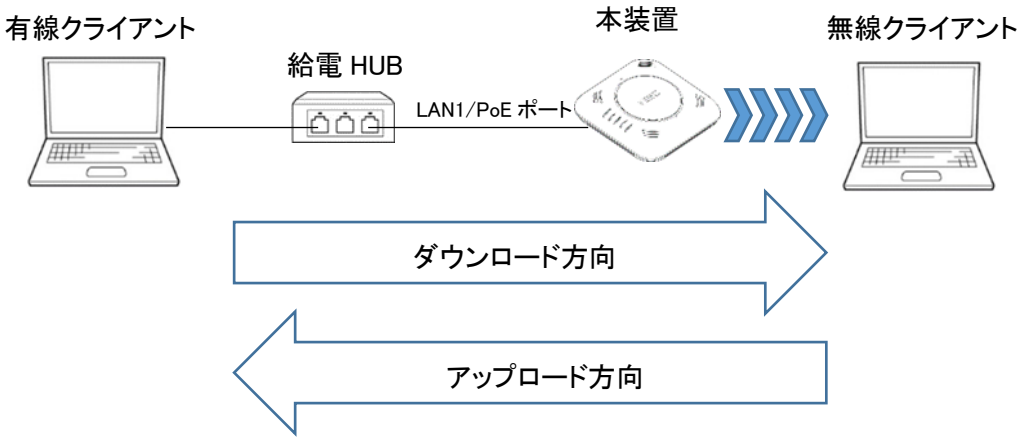
```
AP(config)# interface vlan u
                    ・・・・・・・・・管理用 VLAN インタフェースコンフィグレーションモード移行
AP(config-vlan u)# watchlist action shutdown
                    ・・・・・・・・・リンク監視条件ならびに通信監視条件がマッチした場合
                                      radio0（5GHz 帯）／radio1（2.4GHz 帯）
                                      両方のインタフェースを停止します。
AP(config-vlan u)# exit
```

4.7.　設定事例 7 トラフィックシェーピングの設定

SSID 単位のトラフィックシェーピングを設定することができます。
シェーピングは、「total-upload」を使用して無線インタフェースの SSID から有線インタフェースへのアップロード帯域を指定できます。また、「total-download」を使用して有線インタフェースから無線インタフェースの SSID へのダウンロード帯域を設定することができます。
両方向の帯域設定をする場合は、「total-upload」と「total-download」を同時に使用します。

設定可能数は、以下のとおりです。
「total-upload TU（アップロード帯域シェーピング）」設定は、最大 8 つの SSID まで設定可能です。
「total-download TD（ダウンロード帯域シェーピング）」設定は、最大 8 つの SSID まで設定可能です。
使用する SSID が、radio-device both 設定し、2 つのインタフェースにて使用する場合は、使用数は、2 つとしてカウントします。

シェーピングの方向は以下のとおり



本設定は、SSID コンフィグレーションモードにて設定します。

```
AP(config)# ssid ict・・・・・・・・・・・・・・・・・SSID コンフィグレーションモードに移行
AP(config-ssid ict)# traffic-shaping total-upload 10000 total-download 20000
                                        ・・・・・・・・・アップロード帯域を 10Mbps に設定
                                                          ダウンロード帯域を 20Mbps に設定
                                                          省略時は、前の状態を継続します。
AP(config-ssid ict)# exit
```

4.8.　設定事例 8　送信 AMPDU の設定

SSID の送信 AMPDU の有効／無効の設定ならびに有効時のサブフレーム数設定を行うことができます。
送信 AMPDU は、初期状態では有効になっていますが、無効にすることができます。

本設定は、SSID コンフィグレーションモードにて設定します。

```
AP(config)# ssid ict・・・・・・・・・・・・・・・・・・・・・・・・SSID コンフィグレーションモードに移行
AP(config-ssid ict)# no tx-ampdu-enable・・・・・送信 AMPDU　無効
AP(config-ssid ict)# exit
```

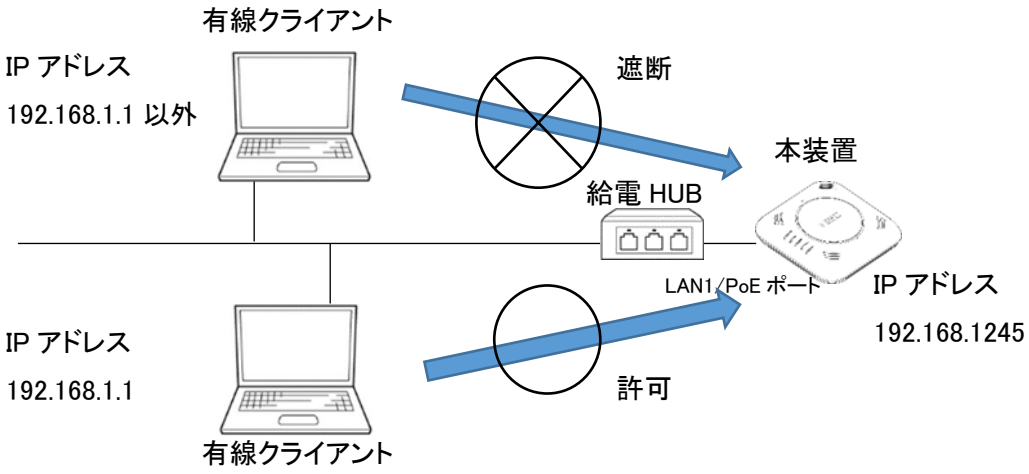
また、送信 AMPDU 有効時、のサブフレーム数を変更することができます。

```
AP(config)# ssid ict・・・・・・・・・・・・・・・・・・・・・・・・SSID コンフィグレーションモードに移行
AP(config-ssid ict)# tx-ampdu-subframes-limit 64・・・・・・サブフレーム数 64 に設定
                                                          （初期値は、64）
AP(config-ssid ict)# tx-ampdu-enable・・・・・・・・・・送信 AMPDU　有効
AP(config-ssid ict)# exit
```

4.9.　設定事例 9　IP フィルタリングの設定

4.9.1.　特定の有線クライアント以外からの CLI へのアクセスを遮断する

GigaEthernet インタフェースに接続され、かつ管理用 VLAN に属しているすべての有線クライアントは、Tenlet または SSH を用いて、CLI へアクセスを行うことができます。
ソフトウェアバージョン 3.0 以降では、特定の IP アドレスのクライアント以外からのアクセスを遮断することができます。
以下は、GigaEthernet0 の管理用 VLAN に接続された IP アドレス 192.168.1.1 のクライアントからは、CLI へのアクセスを許可するが、
192.168.1.1 以外のクライアントからのアクセスを遮断する場合の設定です。

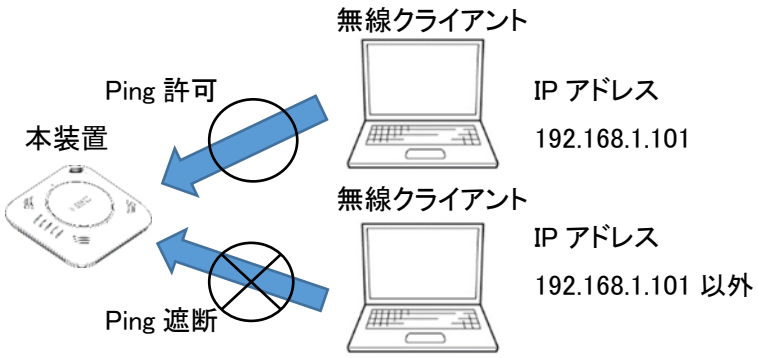


アクセスリスト test1 に許可条件、test2 に遮断条件を設定します。

```
AP(config)# ip access-list test1 permit ip src 192.168.1.1/32 dest any
                                        ・・・192.168.1.1 への IP 通信許可
AP(config)# ip access-list test2 deny ip src any dest any
                                        ・・・他の無線クライアントからの IP 通信遮断
AP(config)# interface GigaEthernet0
AP(config-if-GigaEthernet0)# ip filter test1 1 rcv     ・・・シーケンス No.1 にて許可指定
AP(config-if-GigaEthernet0)# ip filter test2 2 rcv     ・・・シーケンス No.2 にて遮断指定
AP(config-if-GigaEthernet0)# !
AP(config)# write memory
```

4.9.2. 無線クライアントから本装置への Ping を許可する

初期状態において、無線インタフェースに接続されているすべての無線クライアントは、本装置への Ping を許可されていません。
ソフトウェアバージョン 3.0 以降では、無線インタフェースに接続され、かつ管理用 VLAN に属しているすべてまたは、特定の無線クライアントから本装置への Ping を許可することができます。
以下は、radio0 の管理用 VLAN に接続された IP アドレス 192.168.1.101 のクライアントからは、本装置への Ping を許可するが、
192.168.1.101 以外の無線クライアントからのアクセスを遮断する場合の設定です。



アクセスリスト test1 に許可条件を設定します。

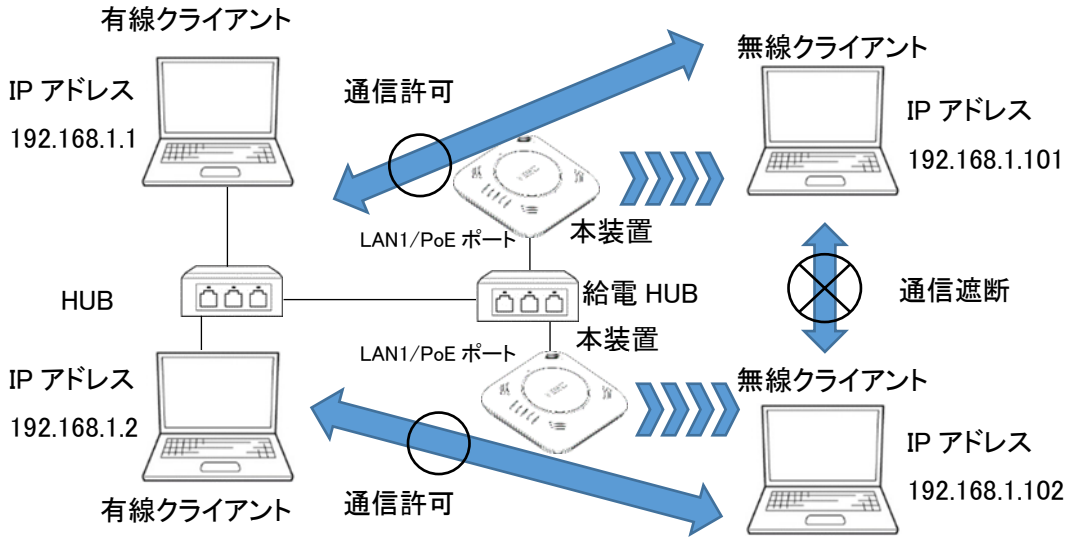
```
AP(config)# ip access-list test1 permit icmp src 192.168.1.101/32 dest any
                                        ・・・192.168.1.101/32 からの Ping を許可
AP(config)# interface radio0
AP(config-if-radio0)# ip filter test1 1 rcv        ・・・シーケンス No.1 にて許可指定
AP(config-if-radio0)# !
AP(config)# write memory
```

以下は、radio0 の管理用 VLAN に接続されたすべてのクライアントから本装置への Ping を許可する設定です。

```
AP(config)# ip access-list test1 permit icmp src any dest any
                                        ・・・すべてのクライアントからの Ping を許可
AP(config)# interface radio0
AP(config-if-radio0)# ip filter test1 1 rcv        ・・・シーケンス No.1 にて許可指定
AP(config-if-radio0)# !
AP(config)# write memory
```

4.9.3. 無線クライアントと有線クライアント間のみ通信を許可する

以下は、同一 VLAN 内に NA1500A を 2 台接続し、有線クライアントは HUB を経由して 2 台の NA1500A に接続、そして無線クライアントは、おのおのの NA1500A に 1 台ずつ接続された環境において、有線クライアント(192.168.1.1/192.168.1.2)からは、
無線クライアント(192.168.1.101/192.168.1.102)への通信を許可するが無線クライアント間の通信は遮断する場合の設定です。

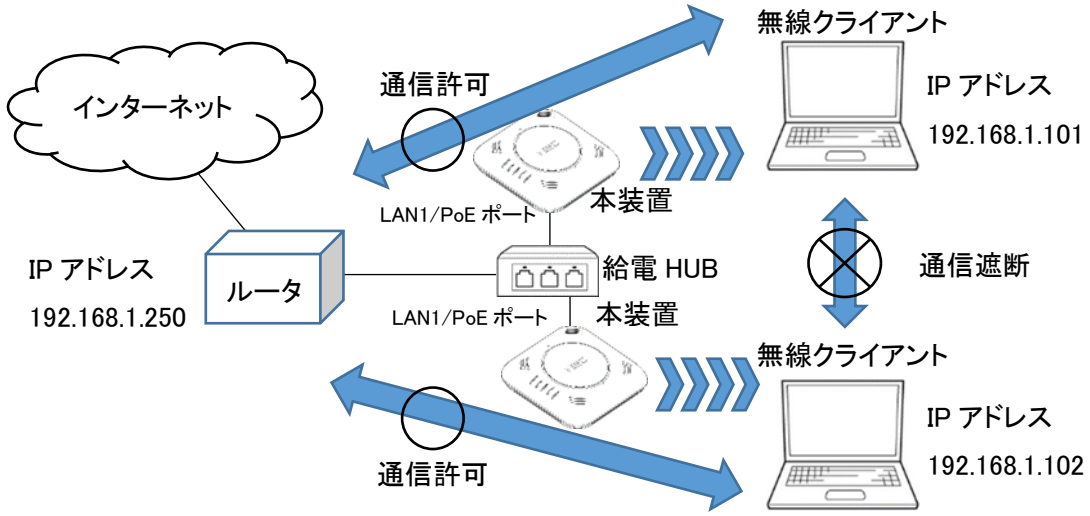


各装置に同一の内容を設定します。
アクセスリスト test1 に許可条件、test2 に遮断条件を設定します。

```
AP(config)# ip access-list test1 permit ip src any dest 192.168.1.1/32
                                                    ・・・192.168.1.1 への通信許可
AP(config)# ip access-list test1 permit ip src any dest 192.168.1.2/32
                                                    ・・・192.168.1.2 への通信許可
AP(config)# ip access-list test2 deny ip src any dest any
                                                    ・・・その他への通信は遮断
AP(config)# interface radio0
AP(config-if-radio0)# ip filter test1 1 in          ・・・シーケンス No.1 にて許可指定
AP(config-if-radio0)# ip filter test2 2 in          ・・・シーケンス No.2 にて遮断指定
AP(config-if-radio0)# !
AP(config)# write memory
```

4.9.4. 無線クライアントからルータを経由した通信のみを許可する

以下は、同一 VLAN 内に NA1500A を 2 台接続し、ルータは HUB を経由して 2 台の NA1500A に接続、そして無線クライアントは、おのおのの NA1500A に 1 台ずつ接続された環境において、無線クライアント(192.168.1.101/192.168.1.102)からは、ルータ(192.168.1.250)を経由した通信(インターネットなどへの通信)を許可するが無線クライアント間の通信は遮断する場合の設定です。
(各クライアントに設定する DNS サーバ/ゲートウェイのアドレスがルータの IP アドレスの場合)

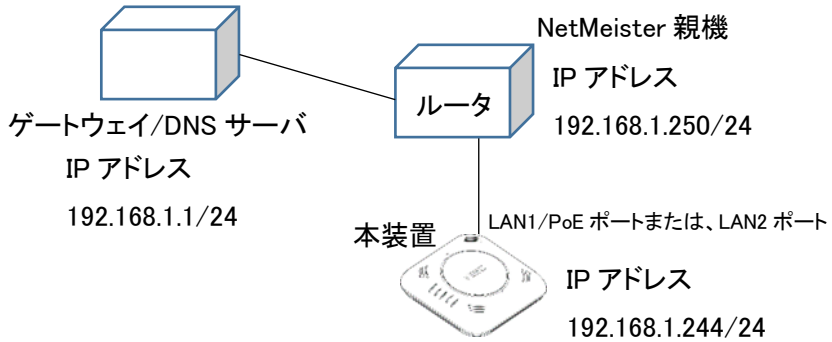


各装置に同一の内容を設定します。
アクセスリスト test1 に許可条件、test2 に遮断条件を設定します。

```
AP(config)# ip access-list test1 permit ip src any dest 192.168.1.250/32
                                                    ・・・ルータへの通信許可
AP(config)# ip access-list test2 deny ip src any dest 192.168.1.0/24
                                                    ・・・指定サブネット遮断
AP(config)# interface radio0
AP(config-if-radio0)# ip filter test1 1 in          ・・・シーケンス No.1 にて許可指定
AP(config-if-radio0)# ip filter test2 2 in          ・・・シーケンス No.2 にて遮断指定
AP(config-if-radio0)# !
AP(config)# write memory
```

4.10.　設定事例 10　NetMeister クライアントの設定

NetMeister クライアント機能を使用するためには、NetMeister 親機となる機器が必要です。
以下は、NetMeister 親機（ルータ）を使用した場合の設定になります。



本装置の NetMeister 親機側に NetMeister 関連設定がされている必要があります。
本構成における設定例は、以下のとおりです。

```
AP(config)# hostname NA1500A-1      ・・・自ホスト名を固有なものに設定
AP(config)# nm enable               ・・・NetMeister クライアント機能を有効に設定
AP(config)# nm account abcdefg password plain 12345678
                                    ・・・NetMeister 登録済みの GROUP-ID とパスワードを登録
AP(config)# nm parent ip 192.168.1.250 port 443
                                    ・・・NetMeister 親機の IP アドレスおよびポート番号を設定
AP(config)# nm https-server ip port 443        ・・・自ポート番号を設定
AP(config)# no nm proxy             ・・・Proxy 経由の接続の場合指定
AP(config)# no nm suppress-feature alarm
                                    ・・・アラーム送信を抑制しない場合の設定
```

本装置を固定アドレスにて NetMeister クライアント機能を使用する場合、
NetMeister 親機が指定するゲートウェイならびに DNS サーバを本装置にも設定する必要があります。

```
AP(config)# interface vlan u                    ・・・Untagged-VLAN を使用する場合
AP(config-vlan u)# ip address 192.168.1.244/24      ・・・本装置 IP アドレス
AP(config-vlan u)# ip route 192.168.1.1             ・・・ゲートウェイの IP アドレス
AP(config-vlan u)# dns server 192.168.1.1           ・・・DNS サーバの IP アドレス
AP(config-vlan u)# vlan enable
!
```

第5章　　付録

商標、ライセンス、コピーライト

- NEC ロゴは、日本およびその他の国における日本電気株式会社の商標および登録商標です。
- NetMeister は、NECプラットフォームズ株式会社の登録商標です。
- Wi-Fi、Wi-Fi Alliance、WPA および WPA2 は、Wi-Fi Alliance の商標または登録商標です。
- その他、各会社名、各製品名およびサービス名などは各社の商標または登録商標です。

IEEE802.11ac 対応無線 LAN アクセスポイント

NA1500A

設定事例集

NWA-A06495-003-00

第 3.0.1 版　2019 年 10 月