P3NK-5502-03Z0

Fujitsu Network SR-M
コマンド設定事例集

V03

FUJITSU

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
無線LANを使用した安全なネットワークを構築するために、本装置をご利用ください。

2016年 6月初版
2017年 7月第2版
2023年 5月第3版

目次

本書の使いかた

本書では、ネットワークを構築するために、代表的な接続形態や本装置の機能を活用した接続形態について説明しています。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

ネットワーク設定を初めて行う方でも「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

 ヒント	本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。
こんな事に気をつけて	本装置をご使用になる際に、注意していただきたいことを説明しています。
	操作手順で説明しているもののほかに、補足情報を説明しています。
	操作方法など関連事項を説明している箇所を示します。
	本装置の機能を使用する際に、対象となる機種名を示します。
	製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。
	製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

設定例の記述について

コマンド例では configure コマンドを実行して、構成定義モードに入ったあとのコマンドを記述しています。
また、プロンプトは設定や機種によって変化するため、“#” に統一しています。

本書における商標の表記について

Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

製品名称	本文中の表記
Microsoft® Windows® 7 64bit Home Premium	Windows 7 および Windows
Microsoft® Windows® 7 32bit Professional	

本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
SR-M50AP1　ご利用にあたって	SR-M50AP1の設置方法やソフトウェアのインストール方法を説明しています。
コマンドユーザーズガイド	構成定義コマンド、運用管理コマンド、およびその他のコマンドの項目やパラメタの詳細な情報を説明しています。
コマンドリファレンス	コマンドの項目やパラメタの詳細な情報を説明しています。
コマンド設定事例集（本書）	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード／ソフトウェア仕様とMIB/Trap一覧を説明しています。
Webユーザーズガイド	Web画面を使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
Webリファレンス	Web画面の項目の詳細な情報を説明しています。

1　無線 LAN 機能を使う（SR-M50AP1）

適用機種　*SR-M50AP1*

1.1　無線 LAN を構築する

適用機種　*SR-M50AP1*

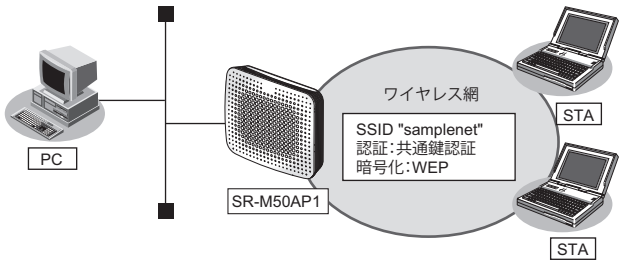
ここでは、既存の有線 LAN ネットワークを無線化する場合を例に説明します。

無線 LAN によるネットワークのワイヤレス化を行い、LAN ケーブルの配線なしに無線通信によるネットワークを構築することができます。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおりに設定しても通信できないことがあります。

☛ 参照　マニュアル「SR-M50AP1　ご利用にあたって」



● 設定条件

無線 LAN を使ってアクセスポイントを構築する

- 利用する無線 LAN モジュール　：ieee80211 1
- 利用する無線 LAN インタフェース：wlan 1
- 通信モード　：IEEE802.11b/g
- 11b/g チャネル　：6
- SSID　：samplenet
- 認証モード　：共通鍵認証
- 暗号化モード　：WEP
- WEP キー　：テキストで“abcdefghijklm”

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 6

アクセスポイントを設定する
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth shared
# wlan 1 wep mode enable
# wlan 1 wep key 1 text abcdefghijklm
# wlan 1 wep send 1

設定終了
# save
# commit
```

1.2　無線 LAN を構築する（IEEE802.11n）

適用機種　***SR-M50AP1***

本装置は IEEE802.11n 規格に準拠しています。IEEE802.11n を使用することにより、高速な無線通信が実現できます。

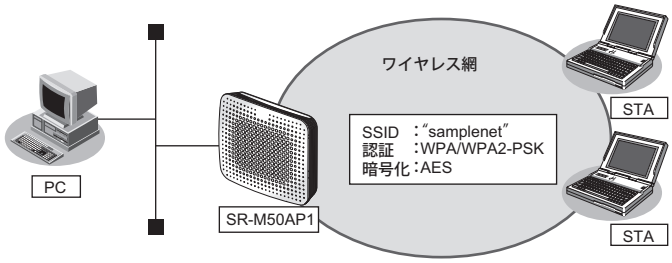
こんな事に気をつけて

- 無線 LAN クライアントが IEEE802.11n に対応している必要があります。
- 暗号化方式として WEP および TKIP は使用できません。定義した場合は無効な設定として無線 LAN インタフェースが使用できません。
- IEEE802.11n 未対応の無線装置が同一チャネルに存在している場合、スループットが低下する場合があります。

  ☛ 参照　マニュアル「機能説明書」

- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおりに設定しても通信できないことがあります。

  ☛ 参照　マニュアル「SR-M50AP1　ご利用にあたって」



● 設定条件

無線 LAN を使ってアクセスポイントを構築する

- 利用する無線 LAN モジュール　：ieee80211 2
- 利用する無線 LAN インタフェース：wlan 9
- 通信モード　：IEEE802.11a/n
- チャネル　：52
- SSID　：samplenet
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：AES
- 事前共有キー（PSK）　：テキストで "abcdefghijklmnopqrstuvwxyz"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a/n
# ieee80211 2 channel 52

無線LANインタフェースを設定する
# wlan 9 use on
# wlan 9 ssid samplenet
# wlan 9 auth wpa/wpa2-psk
# wlan 9 wpa cipher aes
# wlan 9 wpa psk text abcdefghijklmnopqrstuvwxyz

設定終了
# save
# commit
```

1.3　無線 LAN を構築する（IEEE802.11ac）

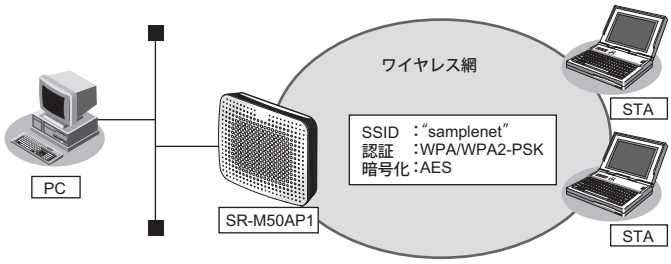
適用機種　***SR-M50AP1***

本装置は IEEE802.11ac 規格に準拠しています。IEEE802.11ac を使用することにより、高速な無線通信が実現できます。

こんな事に気をつけて

- 無線 LAN クライアントが IEEE802.11ac に対応している必要があります。
- 暗号化方式として WEP および TKIP は使用できません。定義した場合は無効な設定として無線 LAN インタフェースが使用できません。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおりに設定しても通信できないことがあります。

☛参照　マニュアル「SR-M50AP1　ご利用にあたって」



● 設定条件

無線 LAN を使ってアクセスポイントを構築する

- 利用する無線 LAN モジュール　：ieee80211 2
- 利用する無線 LAN インタフェース：wlan 9
- 通信モード　：IEEE802.11a/n/ac
- チャネル　：52
- SSID　：samplenet
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：AES
- 事前共有キー（PSK）　：テキストで "abcdefghijklmnopqrstuvwxyz"

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a/n/ac
# ieee80211 2 channel 52

無線LANインタフェースを設定する
# wlan 9 use on
# wlan 9 ssid samplenet
# wlan 9 auth wpa/wpa2-psk
# wlan 9 wpa cipher aes
# wlan 9 wpa psk text abcdefghijklmnopqrstuvwxyz

設定終了
# save
# commit
```

1.4　仮想アクセスポイントにより複数の無線 LAN ネットワークを構築する

適用機種　***SR-M50AP1***

仮想アクセスポイントを使用することで、1つの無線 LAN モジュールで複数の無線 LAN ネットワークを構築することができます。それぞれの無線 LAN インタフェースに VLAN ID を割り当てることで、ネットワークのグループ化を行うことができます。

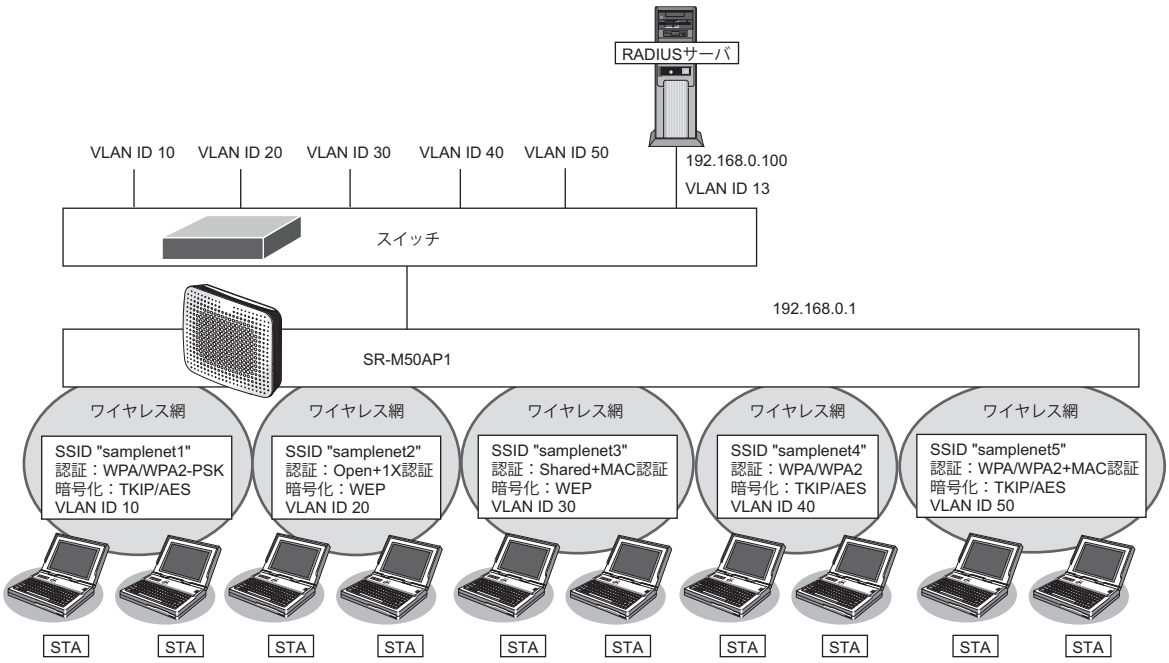
IEEE802.1X 認証機能または MAC アドレス認証機能を使用すると、認証サーバを利用して、無線 LAN ネットワークに接続する端末またはユーザが、ネットワークへのアクセス権限を持っているかを認証することもできます。

同一の無線 LAN ネットワークを 2.4GHz 帯および 5GHz 帯の両方で動作させるには、両方の無線 LAN デバイスに対する無線 LAN インタフェースに同じ VLAN ID の定義を行ってください。

こんな事に気をつけて

- プライバシープロテクション機能は、同一仮想アクセスポイント内の端末どうしの通信を防止するものであり、同機能が有効な場合であっても同一の VLAN ID を指定した複数の無線 LAN インタフェース間の通信については可能です。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおりに設定しても通信できないことがあります。

☛ 参照　マニュアル「SR-M50AP1　ご利用にあたって」



● 設定条件

有線 LAN を使ってネットワークに接続する

- 利用するポート　：ether1
- IP アドレス　：192.168.0.1/24

無線 LAN を使用する（共通）

- 利用する無線 LAN モジュール　：ieee80211 1 および ieee80211 2
- 通信モード　：IEEE802.11b/g および IEEE802.11a
- チャネル　：10（11b/g）および 52（11a）

仮想アクセスポイント（SSID：samplenet1）を構築する

- 利用する無線LANインタフェース：wlan 1およびwlan 9
- SSID：samplenet1
- 認証モード：WPA/WPA2-PSK自動判別認証
- 暗号化モード：TKIP/AES自動判別
- 事前共有キー（PSK）：テキストで“abcdefghijklmnopqrstuvwxyz”
- VLAN ID：10

仮想アクセスポイント（SSID：samplenet2）を構築する

- 利用する無線LANインタフェース：wlan 2およびwlan 10
- SSID：samplenet2
- 認証モード：オープン認証
- 暗号化モード：WEP
- WEPキー：テキストで“abcdefghijklm”
- IEEE802.1X認証：有効
- IEEE802.1X認証（サーバ）：aaa1
- VLAN ID：20

仮想アクセスポイント（SSID：samplenet3）を構築する

- 利用する無線LANインタフェース：wlan 3およびwlan 11
- SSID：samplenet3
- 認証モード：共通鍵認証
- 暗号化モード：WEP
- WEPキー：テキストで“nopqrstuvwxyz”
- MACアドレス認証：有効
- MACアドレス認証（サーバ）：aaa1
- VLAN ID：30

仮想アクセスポイント（SSID：samplenet4）を構築する

- 利用する無線LANインタフェース：wlan 4およびwlan 12
- SSID：samplenet4
- 認証モード：WPA/WPA2自動判別認証
- 暗号化モード：TKIP/AES自動判別
- IEEE802.1X認証：有効
- IEEE802.1X認証（サーバ）：aaa1
- VLAN ID：40

仮想アクセスポイント(SSID:samplenet5)を構築する

- 利用する無線LANインタフェース：wlan 5およびwlan 13
- SSID：samplenet5
- 認証モード：WPA/WPA2自動判別認証
- 暗号化モード：TKIP/AES自動判別
- IEEE802.1X認証：有効
- IEEE802.1X認証（サーバ）：aaa1
- MACアドレス認証：有効

- MACアドレス認証（サーバ）　：aaa1
- VLAN ID　：50

認証サーバをAAA定義で指定する

- aaa定義番号　：aaa1
- 認証サーバIPアドレス　：192.168.0.100
- 認証サーバシークレットキー　：passwd

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
IEEE802.1X認証を使用する
# dot1x use on

MACアドレス認証を使用する
# macauth use on

RADIUSサーバのVLANを設定する
# lan 0 vlan 13
# lan 0 ip address 192.168.0.1/24 3

ETHER1ポートを設定する
# ether 1 vlan tag 10,13,20,30,40,50

無線LANモジュールを設定する（IEEE802.11b/g）
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10

無線LANモジュールを設定する（IEEE802.11a）
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 52

仮想アクセスポイント（SSID：samplenet1）を設定する
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 1 vlan untag 10
# wlan 9 use on
# wlan 9 ssid samplenet1
# wlan 9 auth wpa/wpa2-psk
# wlan 9 wpa cipher auto
# wlan 9 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 9 vlan untag 10

仮想アクセスポイント（SSID：samplenet2）を設定する
# wlan 2 use on
# wlan 2 ssid samplenet2
# wlan 2 auth open
# wlan 2 wep mode enable
# wlan 2 wep key 1 text abcdefghijklm
# wlan 2 wep send 1
# wlan 2 dot1x use on
# wlan 2 dot1x aaa 1
# wlan 2 dot1x vid 20
# wlan 2 dot1x vlan assign disable
```

```
# wlan 10 use on
# wlan 10 ssid samplenet2
# wlan 10 auth open
# wlan 10 wep mode enable
# wlan 10 wep key 1 text abcdefghijklm
# wlan 10 wep send 1
# wlan 10 dot1x use on
# wlan 10 dot1x aaa 1
# wlan 10 dot1x vid 20
# wlan 10 dot1x vlan assign disable

仮想アクセスポイント（SSID：samplenet3）を設定する
# wlan 3 use on
# wlan 3 ssid samplenet3
# wlan 3 auth shared
# wlan 3 wep mode enable
# wlan 3 wep key 1 text nopqrstuvwxyz
# wlan 3 wep send 1
# wlan 3 macauth use on
# wlan 3 macauth aaa 1
# wlan 3 macauth vid 30
# wlan 3 macauth vlan assign disable
# wlan 11 use on
# wlan 11 ssid samplenet3
# wlan 11 auth shared
# wlan 11 wep mode enable
# wlan 11 wep key 1 text nopqrstuvwxyz
# wlan 11 wep send 1
# wlan 11 macauth use on
# wlan 11 macauth aaa 1
# wlan 11 macauth vid 30
# wlan 11 macauth vlan assign disable

仮想アクセスポイント（SSID：samplenet4）を設定する
# wlan 4 use on
# wlan 4 ssid samplenet4
# wlan 4 auth wpa/wpa2
# wlan 4 wpa cipher auto
# wlan 4 dot1x use on
# wlan 4 dot1x aaa 1
# wlan 4 dot1x vid 40
# wlan 4 dot1x vlan assign disable
# wlan 12 use on
# wlan 12 ssid samplenet4
# wlan 12 auth wpa/wpa2
# wlan 12 wpa cipher auto
# wlan 12 dot1x use on
# wlan 12 dot1x aaa 1
# wlan 12 dot1x vid 40
# wlan 12 dot1x vlan assign disable

仮想アクセスポイント（SSID：samplenet5）を設定する
# wlan 5 use on
# wlan 5 ssid samplenet5
# wlan 5 auth wpa/wpa2
# wlan 5 wpa cipher auto
# wlan 5 dot1x use on
# wlan 5 dot1x aaa 1
# wlan 5 dot1x vid 50
# wlan 5 dot1x vlan assign disable
# wlan 5 macauth use on
# wlan 5 macauth aaa 1
```

```
# wlan 5 macauth vid 50
# wlan 5 macauth vlan assign disable
# wlan 13 use on
# wlan 13 ssid samplenet5
# wlan 13 auth wpa/wpa2
# wlan 13 wpa cipher auto
# wlan 13 dot1x use on
# wlan 13 dot1x aaa 1
# wlan 13 dot1x vid 50
# wlan 13 dot1x vlan assign disable
# wlan 13 macauth use on
# wlan 13 macauth aaa 1
# wlan 13 macauth vid 50
# wlan 13 macauth vlan assign disable

認証サーバを AAA 定義で指定する
# aaa 1 name aaasvr
# aaa 1 radius service client auth
# aaa 1 radius client server-info auth 0 secret passwd
# aaa 1 radius client server-info auth 0 address 192.168.0.100
# aaa 1 radius client server-info auth 0 source 192.168.0.1

設定終了
# save
# commit
```

1.5　IEEE802.1X 認証および MAC アドレス認証により VLAN を管理する

適用機種　***SR-M50AP1***

IEEE802.1X 認証機能または MAC アドレス認証機能を使用した場合、認証データベースで、ユーザごとに所属する VLAN ID を設定すると、認証端末またはユーザが所属するネットワークを指定することができます。

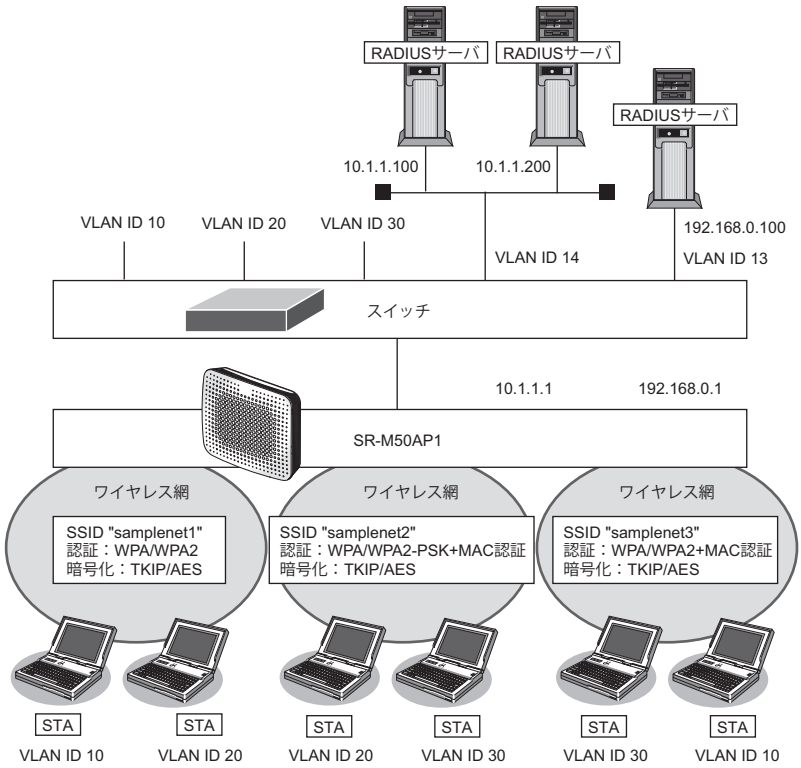
これにより、ネットワークへのアクセスを認証端末またはユーザごとに管理することができます。

☛ 参照　マニュアル「機能説明書」

こんな事に気をつけて

- IEEE802.1X 認証、MAC アドレス認証を利用する無線 LAN インタフェースでは事前に VLAN を設定できません。
- IEEE802.1X 認証、MAC アドレス認証で利用する AAA のグループ ID を正しく設定してください。
- 複数の認証を併用した場合は、それぞれの認証が完了した時点で、払い出された VLAN ID で上書きされていきます。
- 認証サーバに VLAN ID が設定されていない場合、wlan dot1x vid コマンド、および wlan macauth vid コマンドで設定された VLAN ID が使用されます。
- プライバシープロテクション機能を有効にした場合でも、無線 LAN インタフェース間で同一の VLAN ID が割り当てられた端末どうしの通信は可能です。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおりに設定しても通信できないことがあります。

☛ 参照　マニュアル「SR-M50AP1　ご利用にあたって」



● 設定条件

有線 LAN を使ってネットワークに接続する

- 利用するポート　：ether1
- IP アドレス　：192.168.0.1/24、10.1.1.1/24

無線 LAN を使用する（共通）

- 利用する無線 LAN モジュール　：ieee80211 1 および ieee80211 2
- 通信モード　：IEEE802.11b/g および IEEE802.11a
- チャネル　：10（11b/g）および 52（11a）

仮想アクセスポイント（SSID：samplenet1）を構築する

- 利用する無線 LAN インタフェース　：wlan 1 および wlan 9
- SSID　：samplenet1
- 認証モード　：WPA/WPA2 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- IEEE802.1X 認証　：有効
- IEEE802.1X 認証（サーバ）　：aaa1

仮想アクセスポイント（SSID：samplenet2）を構築する

- 利用する無線 LAN インタフェース　：wlan 2 および wlan 10
- SSID　：samplenet2
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで “abcdefghijklmnopqrstuvwxyz”
- MAC アドレス認証　：有効
- MAC アドレス認証（サーバ）　：aaa2

仮想アクセスポイント（SSID：samplenet3）を構築する

- 利用する無線 LAN インタフェース　：wlan 3 および wlan 11
- SSID　：samplenet3
- 認証モード　：WPA/WPA2 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- IEEE802.1X 認証　：有効
- IEEE802.1X 認証（サーバ）　：aaa3
- MAC アドレス認証　：有効
- MAC アドレス認証（サーバ）　：aaa3

認証／課金サーバを AAA 定義で指定する

- aaa 定義番号　：aaa1
- 認証サーバ（プライマリ）IP アドレス　：10.1.1.100
- 認証サーバ（プライマリ）シークレットキー　：passwd
- 認証サーバ（セカンダリ）IP アドレス　：10.1.1.200
- 認証サーバ（セカンダリ）シークレットキー　：passwd
- 課金サーバ（プライマリ）IP アドレス　：10.1.1.100
- 課金サーバ（プライマリ）シークレットキー　：passwd
- 課金サーバ（セカンダリ）IP アドレス　：10.1.1.200

- 課金サーバ（セカンダリ）シークレットキー　：passwd

- aaa 定義番号　：aaa2
- 認証サーバ（プライマリ）IP アドレス　：10.1.1.200
- 認証サーバ（プライマリ）シークレットキー　：passwd
- 認証サーバ（セカンダリ）IP アドレス　：10.1.1.100
- 認証サーバ（セカンダリ）シークレットキー　：passwd

- aaa 定義番号　：aaa3
- 認証サーバ IP アドレス　：192.168.0.100
- 認証サーバシークレットキー　：passwd
- 課金サーバ IP アドレス　：192.168.0.100
- 課金サーバシークレットキー　：passwd

こんな事に気をつけて

RADIUS サーバにはユーザに VLAN ID を割り当てるために、以下の属性を設定してください。
設定方法については、RADIUS サーバのマニュアルを参照してください。

名前	番号	属性値（※）
Tunnel-Type	64	VLAN（13）
Tunnel-Media-Type	65	802（6）
Tunnel-Private-Group-ID	81	VLAN ID（10 進数表記を ASCII コードでコーディング）

※）（）内の数字は属性として設定される 10 進数の値

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
IEEE802.1X 認証を使用する
# dot1x use on

MAC アドレス認証を使用する
# macauth use on

RADIUS サーバの VLAN を設定する
# lan 0 vlan 13
# lan 0 ip address 192.168.0.1/24 3
# lan 1 vlan 14
# lan 1 ip address 10.1.1.1/24 3

ETHER1 ポートを設定する
# ether 1 vlan tag 10,13,14,20,30

無線 LAN モジュールを設定する（IEEE802.11b/g）
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10

無線 LAN モジュールを設定する（IEEE802.11a）
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 52
```

仮想アクセスポイント（SSID：samplenet1）を設定する
wlan 1 use on
wlan 1 ssid samplenet1
wlan 1 auth wpa/wpa2
wlan 1 wpa cipher auto
wlan 1 dot1x use on
wlan 1 dot1x aaa 1
wlan 9 use on
wlan 9 ssid samplenet1
wlan 9 auth wpa/wpa2
wlan 9 wpa cipher auto
wlan 9 dot1x use on
wlan 9 dot1x aaa 1

仮想アクセスポイント（SSID：samplenet2）を設定する
wlan 2 use on
wlan 2 ssid samplenet2
wlan 2 auth wpa/wpa2-psk
wlan 2 wpa cipher auto
wlan 2 wpa psk text abcdefghijklmnopqrstuvwxyz
wlan 2 macauth use on
wlan 2 macauth aaa 2
wlan 10 use on
wlan 10 ssid samplenet2
wlan 10 auth wpa/wpa2-psk
wlan 10 wpa cipher auto
wlan 10 wpa psk text abcdefghijklmnopqrstuvwxyz
wlan 10 macauth use on
wlan 10 macauth aaa 2

仮想アクセスポイント（SSID：samplenet3）を設定する
wlan 3 use on
wlan 3 ssid samplenet3
wlan 3 auth wpa/wpa2
wlan 3 wpa cipher auto
wlan 3 dot1x use on
wlan 3 dot1x aaa 3
wlan 3 macauth use on
wlan 3 macauth aaa 3
wlan 11 use on
wlan 11 ssid samplenet3
wlan 11 auth wpa/wpa2
wlan 11 wpa cipher auto
wlan 11 dot1x use on
wlan 11 dot1x aaa 3
wlan 11 macauth use on
wlan 11 macauth aaa 3

認証／課金サーバをAAA定義で指定する
aaa 1 name aaasvr1
aaa 1 radius service client both
aaa 1 radius client server-info auth 0 secret passwd
aaa 1 radius client server-info auth 0 address 10.1.1.100
aaa 1 radius client server-info auth 0 source 10.1.1.1
aaa 1 radius client server-info auth 1 secret passwd
aaa 1 radius client server-info auth 1 address 10.1.1.200
aaa 1 radius client server-info auth 1 priority 1
aaa 1 radius client server-info auth 1 source 10.1.1.1
aaa 1 radius client server-info accounting 0 secret passwd
aaa 1 radius client server-info accounting 0 address 10.1.1.100
aaa 1 radius client server-info accounting 0 source 10.1.1.1
aaa 1 radius client server-info accounting 1 secret passwd

```
# aaa 1 radius client server-info accounting 1 address 10.1.1.200
# aaa 1 radius client server-info accounting 1 priority 1
# aaa 1 radius client server-info accounting 1 source 10.1.1.1
# aaa 2 name aaasvr2
# aaa 2 radius service client auth
# aaa 2 radius client server-info auth 0 secret passwd
# aaa 2 radius client server-info auth 0 address 10.1.1.200
# aaa 2 radius client server-info auth 0 source 10.1.1.1
# aaa 2 radius client server-info auth 1 secret passwd
# aaa 2 radius client server-info auth 1 address 10.1.1.100
# aaa 2 radius client server-info auth 1 priority 1
# aaa 2 radius client server-info auth 1 source 10.1.1.1
# aaa 3 name aaasvr3
# aaa 3 radius service client auth
# aaa 3 radius client server-info auth 0 secret passwd
# aaa 3 radius client server-info auth 0 address 192.168.0.100
# aaa 3 radius client server-info auth 0 source 192.168.0.1
# aaa 3 radius client server-info accounting 0 secret passwd
# aaa 3 radius client server-info accounting 0 address 192.168.0.100
# aaa 3 radius client server-info accounting 0 source 192.168.0.1

設定終了
# save
# commit
```

1.6　同一SSIDの複数アクセスポイントを構築する

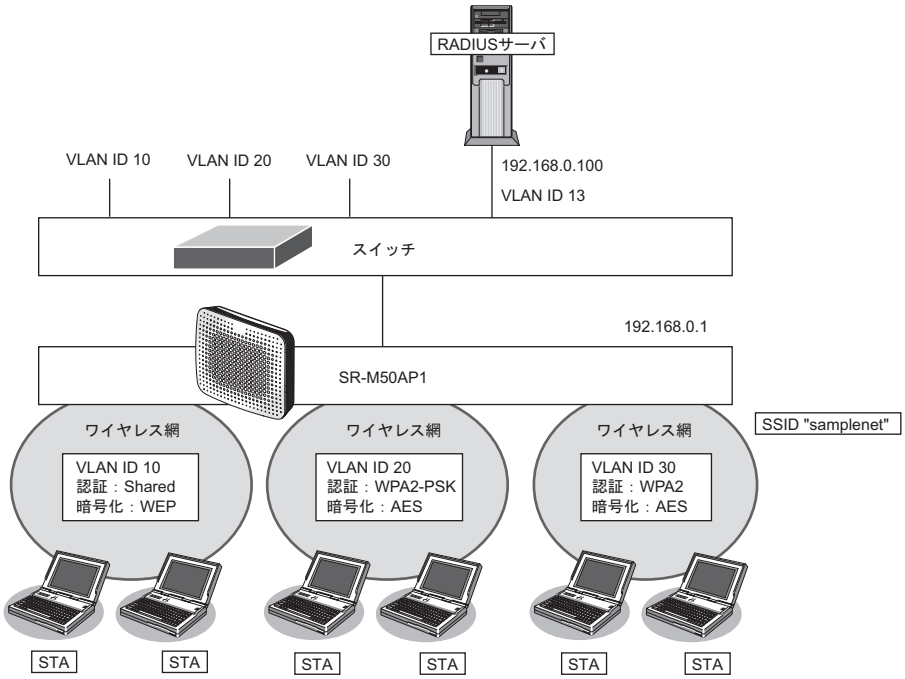
適用機種　***SR-M50AP1***

同一SSIDの仮想アクセスポイントを構築することにより、接続の際の認証・暗号化方式によって端末が属するネットワークを分けることができます。

こんな事に気をつけて

- 同一のSSIDかつ同一の認証・暗号化方式の仮想アクセスポイントを設定した場合、どちらの仮想アクセスポイントに接続されるかは不定となります。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおりに設定しても通信できないことがあります。

☛ 参照　マニュアル「SR-M50AP1　ご利用にあたって」



● 設定条件

有線LANを使ってネットワークに接続する

- 利用するポート　：ether1
- IPアドレス　：192.168.0.1/24

無線LANを使用する（共通）

- 利用する無線LANモジュール　：ieee80211 1およびieee80211 2
- 通信モード　：IEEE802.11b/gおよびIEEE802.11a
- チャネル　：10（11b/g）および52（11a）

仮想アクセスポイント（共通鍵認証）を構築する

- 利用する無線LANインタフェース　：wlan 1およびwlan 9
- SSID　：samplenet
- 認証モード　：共通鍵認証
- 暗号化モード　：WEP

- WEP キー　：テキストで“abcdefghijklm”
- VLAN ID　：10

仮想アクセスポイント（WPA2-PSK）を構築する

- 利用する無線 LAN インタフェース：wlan 2 および wlan 10
- SSID　：samplenet
- 認証モード　：WPA2-PSK
- 暗号化モード　：AES
- 事前共有キー（PSK）　：テキストで“abcdefghijklmnopqrstuvwxyz”
- VLAN ID　：20

仮想アクセスポイント（WPA2）を構築する

- 利用する無線 LAN インタフェース：wlan 3 および wlan 11
- SSID　：samplenet
- 認証モード　：WPA2
- 暗号化モード　：AES
- IEEE802.1X 認証　：有効
- IEEE802.1X 認証（サーバ）　：aaa1
- VLAN ID　：30

認証／課金サーバを AAA 定義で指定する

- aaa 定義番号　：aaa1
- 認証サーバ IP アドレス　：192.168.0.100
- 認証サーバシークレットキー　：passwd
- 課金サーバ IP アドレス　：192.168.0.100
- 課金サーバシークレットキー　：passwd

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
IEEE802.1X 認証を使用する
# dot1x use on

RADIUS サーバの VLAN を設定する
# lan 0 vlan 13
# lan 0 ip address 192.168.0.1/24 3

ETHER1 ポートを設定する
# ether 1 vlan tag 10,13,20,30

無線 LAN モジュールを設定する（IEEE802.11b/g）
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10

無線 LAN モジュールを設定する（IEEE802.11a）
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 52
```

仮想アクセスポイント（共通鍵認証）を設定する
wlan 1 use on
wlan 1 ssid samplenet
wlan 1 auth shared
wlan 1 wep mode enable
wlan 1 wep key 1 text abcdefghijklm
wlan 1 wep send 1
wlan 1 vlan untag 10
wlan 9 use on
wlan 9 ssid samplenet
wlan 9 auth shared
wlan 9 wep mode enable
wlan 9 wep key 1 text abcdefghijklm
wlan 9 wep send 1
wlan 9 vlan untag 10

仮想アクセスポイント（WPA2-PSK）を設定する
wlan 2 use on
wlan 2 ssid samplenet
wlan 2 auth wpa2-psk
wlan 2 wpa cipher aes
wlan 2 wpa psk text abcdefghijklmnopqrstuvwxyz
wlan 2 vlan untag 20
wlan 10 use on
wlan 10 ssid samplenet
wlan 10 auth wpa2-psk
wlan 10 wpa cipher aes
wlan 10 wpa psk text abcdefghijklmnopqrstuvwxyz
wlan 10 vlan untag 20

仮想アクセスポイント（WPA2）を設定する
wlan 3 use on
wlan 3 ssid samplenet
wlan 3 auth wpa2
wlan 3 wpa cipher aes
wlan 3 dot1x use on
wlan 3 dot1x aaa 1
wlan 3 dot1x vid 30
wlan 3 dot1x vlan assign disable
wlan 11 use on
wlan 11 ssid samplenet
wlan 11 auth wpa2
wlan 11 wpa cipher aes
wlan 11 dot1x use on
wlan 11 dot1x aaa 1
wlan 11 dot1x vid 30
wlan 11 dot1x vlan assign disable

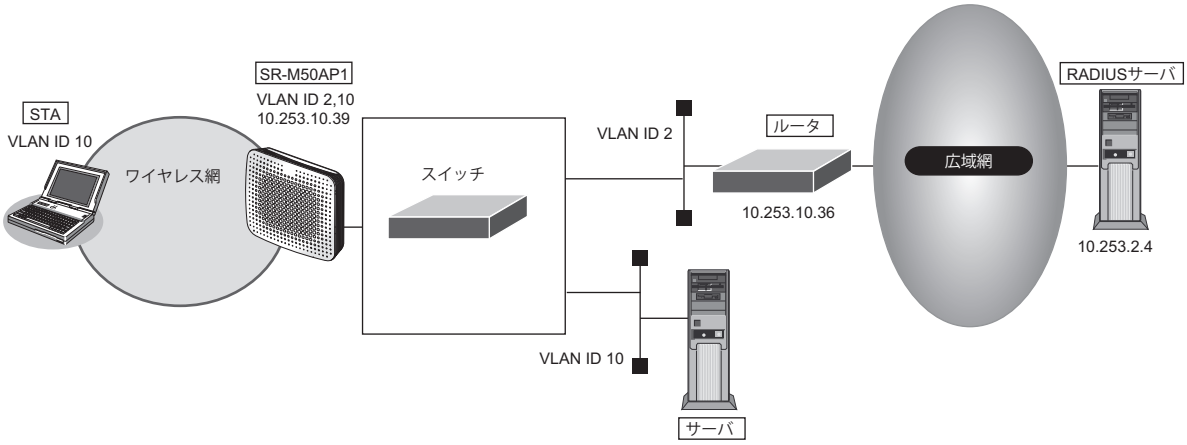
認証／課金サーバをAAA定義で指定する
aaa 1 name aaasvr
aaa 1 radius service client both
aaa 1 radius client server-info auth 0 secret passwd
aaa 1 radius client server-info auth 0 address 192.168.0.100
aaa 1 radius client server-info auth 0 source 192.168.0.1
aaa 1 radius client server-info accounting 0 secret passwd
aaa 1 radius client server-info accounting 0 address 192.168.0.100
aaa 1 radius client server-info accounting 0 source 192.168.0.1

設定終了
save
commit

1.7　認証自動切替機能を使う

適用機種　***SR-M50AP1***

ここでは、RADIUS サーバの稼動状況を監視し RADIUS サーバからの応答がない場合に、認証方式を IEEE802.1X 認証から共有鍵認証へ自動切り替えを行う場合の設定方法を説明します。



こんな事に気をつけて

- RADIUS サーバの監視には、ICMP を使う方法と、認証を使う方法があります。
- ICMP で監視を行う場合は、RADIUS サーバが動作しているホストの生存確認だけを行います。
- 認証で監視を行う場合は、CHAP 方式を用いた認証で監視を行います。認証結果は監視しないため、RADIUS サーバが認証失敗を通知しても切り替えは発生しません。
- RADIUS サーバ側でログを採取する場合は、大量の監視用の認証成功または失敗のログが出力される可能性があります。監視間隔の設定、RADIUS サーバ側のログ採取の設定には注意してください。
- wlan dot1x backup コマンドで IEEE802.1X 認証のバックアップ解除を自動復旧しない（manual）設定とした場合、無線 LAN インタフェースはバックアップからマスタに自動復旧はしません。dot1xctl backup recovery コマンドでバックアップ解除を行ってください。

☛ 参照　マニュアル「コマンドリファレンス」の「dot1xctl backup recovery」

補足　認証自動切替機能使用時に、RADIUS サーバの監視異常により IEEE802.1X 認証方式から切り替わっている場合、READY ランプが橙色で点滅します。

● 設定条件

有線 LAN を使ってネットワークに接続する

- 利用するポート　：ether1
- IP アドレス　：10.253.10.39/24
- デフォルトルート　：10.253.10.36/24

無線 LAN を使用する（共通）

- 利用する無線 LAN モジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：10（11b/g）

仮想アクセスポイント（SSID：samplenet1）を構築する

- 利用する無線 LAN インタフェース：wlan 1
- SSID　：samplenet1
- 認証モード　：WPA/WPA2 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- IEEE802.1X 認証　：有効
- IEEE802.1X 認証（サーバ）　：aaa1
- 認証自動切替の設定　: マスタとして動作
- バックアップ切り戻し時間
  （RADIUS サーバ復旧を検出後のバックアップからマスタへの切り戻し時間）
  : 10 秒
- VLAN ID　: 10

仮想アクセスポイント（SSID：samplenet2）を構築する

- 利用する無線 LAN インタフェース：wlan 2
- SSID　：samplenet2
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで “abcdefghijklmnopqrstuvwxyz”
- IEEE802.1X 認証　：無効
- 認証自動切替の設定　：バックアップとして動作
- 認証自動切替のバックアップ対象インタフェース
  ：wlan 1
- VLAN ID　：10

認証／課金サーバを AAA 定義で指定する

- aaa 定義番号　：aaasrv1
- 認証サーバ IP アドレス　：10.253.2.4
- 認証サーバシークレットキー　：passwd
- 課金サーバ IP アドレス　：10.253.2.4
- 課金サーバシークレットキー　：passwd

認証サーバの監視を設定する

- 認証サーバ監視方法　：認証による監視（監視時間はデフォルト値）
- 認証サーバ監視用認証 ID　：user00
- 認証サーバ監視用パスワード　：passwd

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
IEEE802.1X認証を使用する
# dot1x use on

管理用VLANを設定する
# lan 0 ip address 10.253.10.39/24 3
# lan 0 vlan 2

デフォルトルートを設定する
# lan 0 ip route 0 default 10.253.10.36 1

ETHER1ポートを設定する
# ether 1 vlan tag 2,10

無線LANモジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10

仮想アクセスポイント（SSID：samplenet1）を設定し、認証自動切替のマスタとして動作させる
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa/wpa2
# wlan 1 wpa cipher auto
# wlan 1 dot1x use on
# wlan 1 dot1x aaa 1
# wlan 1 dot1x backup master 10s
# wlan 1 dot1x vlan assign disable
# wlan 1 dot1x vid 10

仮想アクセスポイント（SSID：samplenet2）を設定し、認証自動切替のバックアップとして動作させる
# wlan 2 use on
# wlan 2 ssid samplenet2
# wlan 2 auth wpa/wpa2-psk
# wlan 2 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 2 wpa cipher auto
# wlan 2 dot1x backup backup 1
# wlan 2 vlan untag 10

認証／課金サーバをAAA定義で指定する
# aaa 1 name aaasvr1
# aaa 1 radius service client both
# aaa 1 radius client server-info auth 0 secret passwd
# aaa 1 radius client server-info auth 0 address 10.253.2.4
# aaa 1 radius client server-info auth 0 source 10.253.10.39
# aaa 1 radius client server-info accounting 0 secret passwd
# aaa 1 radius client server-info accounting 0 address 10.253.2.4
# aaa 1 radius client server-info accounting 0 source 10.253.10.39

認証サーバの監視を設定する
# aaa 1 radius client server-info auth 0 watch type auth
# aaa 1 radius client server-info auth 0 watch user user00 passwd

設定終了
# save
# commit
```

1.8　端末台数制限機能を使う

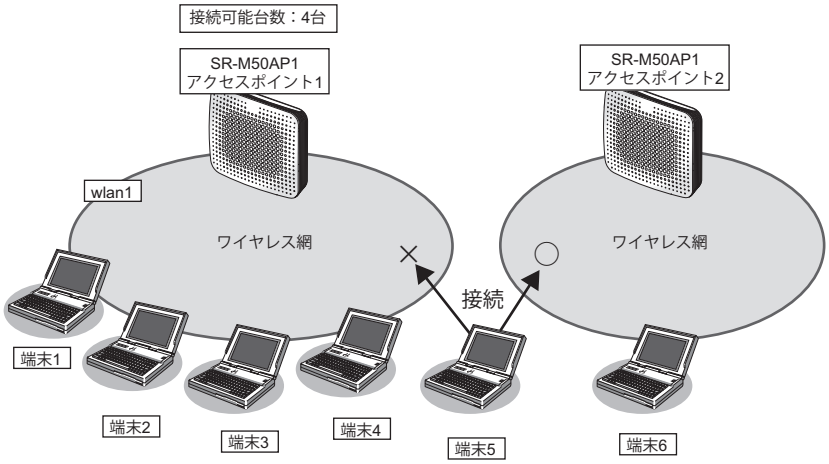
適用機種　***SR-M50AP1***

端末台数制限機能として、接続する端末の台数を制御することにより、通信速度の低下を防ぎます。

無線LAN端末は設定した制限数を超えて無線LANアクセスポイントに接続することはできません。接続に失敗した無線LAN端末には、その理由として端末台数制限によるものであることを伝えることで、ほかの無線LANアクセスポイントへの接続を促します。

こんな事に気をつけて

- 端末台数最低保証機能の最低保証台数が設定されていた場合、最低保証台数分は本機能の接続可能台数の中から確保されます。そのため、接続可能台数に到達する前に無線LAN端末が接続できなくなることがあります。
  最低保証されていない接続可能な無線LAN端末台数を増やすには、本機能の接続可能台数を増やしてください。
- 無線LAN端末が端末台数制限により接続に失敗し、接続先をほかの無線LANアクセスポイントへ変更する動作については、SR-M50AP1は失敗理由を伝えて変更を促すだけとなります。実際に接続先が変更されるには、無線LAN端末が接続先を切り替える動作をサポートしている必要があります。
- 2.4GHz帯でTKIP認証端末を複数台接続する場合、認証キーの割り当て数上限超過により、端末可能台数に到達する前に無線LAN端末が接続できなくなることがあります。



● 設定条件

無線LANを使用する

- 利用する無線LANモジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：10
- 接続可能台数　：4

仮想アクセスポイントを構築する

- 利用する無線LANインタフェース：wlan 1
- SSID　：samplenet
- 認証モード　：WPA/WPA2-PSK自動判別認証
- 暗号化モード　：TKIP/AES自動判別
- 事前共有キー（PSK）　：テキストで“abcdefghijklmnopqrstuvwxyz”

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10

接続可能台数を設定する
# ieee80211 1 sta limit 4

仮想アクセスポイントを設定する
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz

設定終了
# save
# commit
```

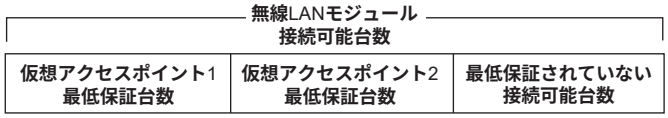
1.9　端末台数最低保証機能を使う

適用機種　***SR-M50AP1***

端末台数最低保証機能とは、仮想アクセスポイントごとに、最低でも接続可能な無線LAN端末の台数を保証する機能です。

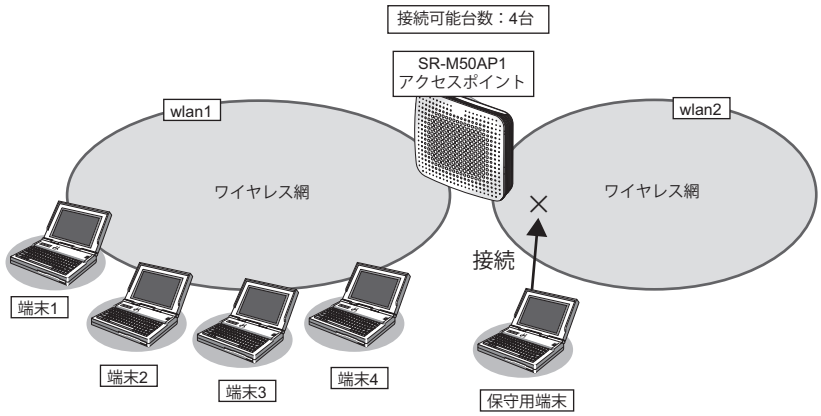
こんな事に気をつけて

- ある無線LANモジュールの仮想アクセスポイントすべてに設定されている最低保証台数の合計が、同無線LANモジュールの端末台数制限機能による接続可能台数を超えないように設定してください。
- 最低保証する台数は、端末台数制限機能の接続可能台数の中から確保されます。そのため、接続可能台数に到達する前に無線LAN端末が接続できなくなることがあります。

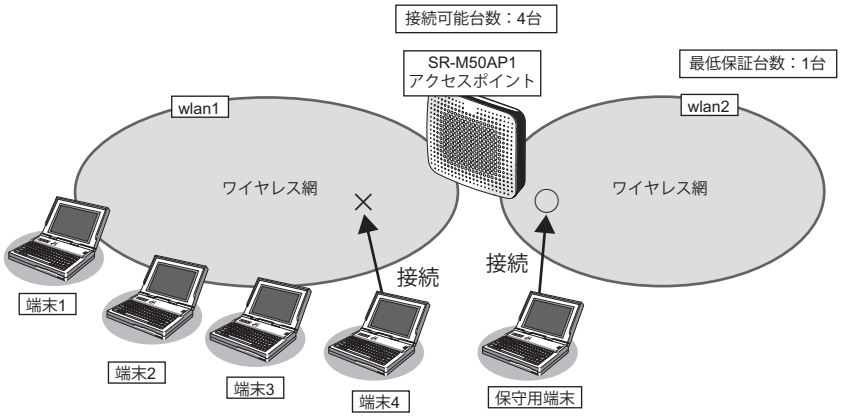


本機能は以下のような場合に有用です。

本機能を利用していない場合、保守用などの無線LAN端末がSR-M50AP1の端末台数制限機能により接続不可となる場合があります。



ここで、保守用の無線LAN端末の接続先である仮想アクセスポイントに、本機能によって最低保証する台数を1台設定しておくことで、保守用の無線LAN端末は必ず接続することができます。



● 設定条件

無線 LAN を使用する

- 利用する無線 LAN モジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：10
- 接続可能台数　：4

仮想アクセスポイント 1 を構築する

- 利用する無線 LAN インタフェース：wlan 1
- SSID　：samplenet1
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで “abcdefghijklmnopqrstuvwxyz”

仮想アクセスポイント 2 を構築する

- 利用する無線 LAN インタフェース：wlan 2
- SSID　：samplenet2
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで “ABCDEFGHIJKLMNOPQRSTUVWXYZ”
- 最低保証台数　：1

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線 LAN モジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10
# ieee80211 1 sta limit 4

仮想アクセスポイント 1 を設定する
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz

仮想アクセスポイント 2 を設定する
# wlan 2 use on
# wlan 2 ssid samplenet2
# wlan 2 auth wpa/wpa2-psk
# wlan 2 wpa cipher auto
# wlan 2 wpa psk text ABCDEFGHIJKLMNOPQRSTUVWXYZ

仮想アクセスポイント 2 に最低保証台数を設定する
# wlan 2 sta guarantee 1

設定終了
# save
# commit
```

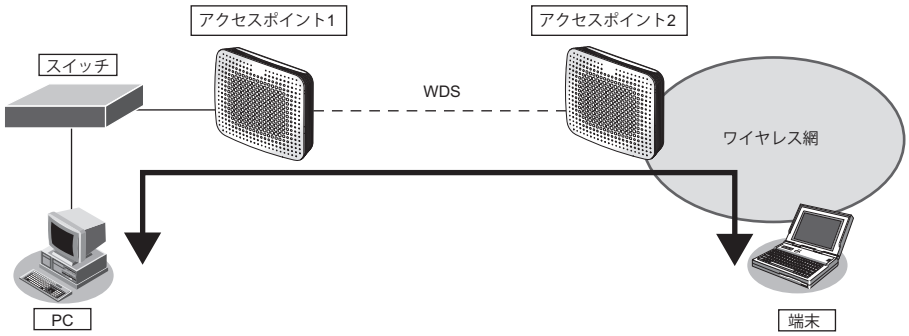
1.10　WDSブリッジ機能を使う

適用機種　***SR-M50AP1***

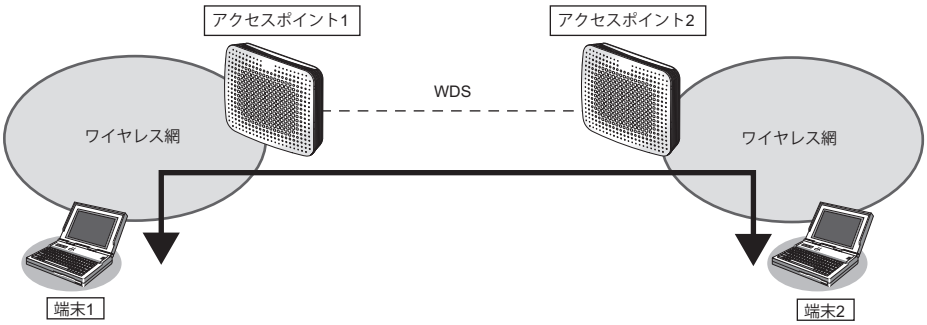
WDSブリッジとは、無線LANアクセスポイントどうしの通信を可能にする機能です。ある無線LANアクセスポイントを中継して別の無線LANアクセスポイントとデータの送受信を行うことができるため、単一の無線LANアクセスポイントを使用した場合に比べて広い範囲での通信が可能となります。

SR-M50AP1ではWDSブリッジのみで無線LANネットワークを構築することができます。

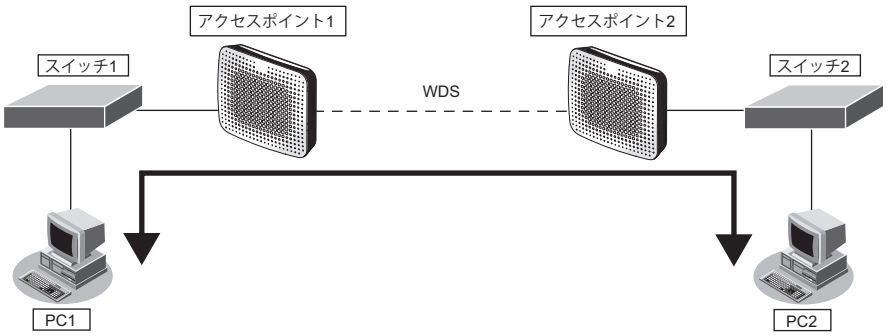
- 有線LANと無線LAN端末間の通信



- 無線LAN端末間の通信



- 有線LAN間の通信

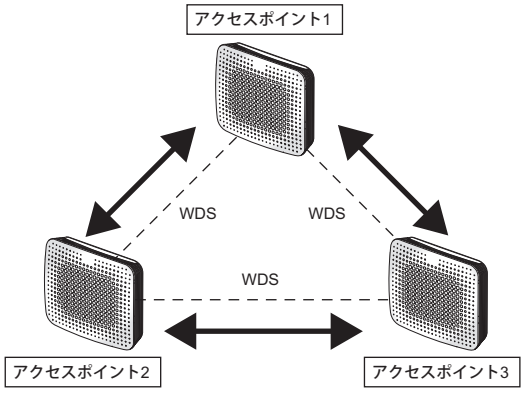


こんな事に気をつけて

- 相手無線 LAN アクセスポイントと同じチャネル、通信モードで動作させてください。また、WDS のみで運用する場合、any 以外のチャネルを設定してください。
- WDS ブリッジの相手側無線 LAN インタフェースの MAC アドレスは正確に設定してください。
  なお、SR-M50AP1 の無線 LAN の MAC アドレスは、show system information コマンドで確認することができます。
  wlan コマンドで定義した無線 LAN インタフェースについて、インタフェース番号が小さいものから順に連続した値の MAC アドレスが割り当てられます。
  動作中の無線 LAN インタフェースの MAC アドレスは、show wlan status コマンドで確認することができます。

  ☛参照　マニュアル「コマンドリファレンス」の「show system information」、「show wlan status」

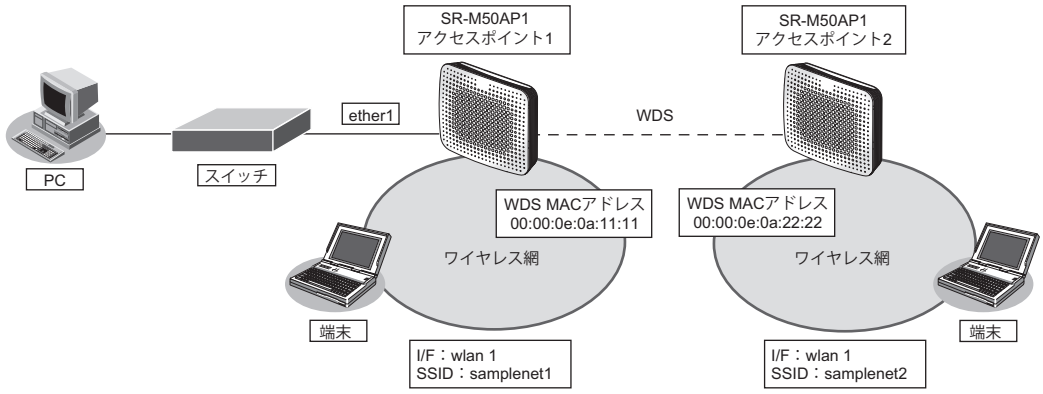
- 本機能のブリッジ処理は、同一の VLAN に割り当てられたインタフェース間でのみ行われます。WDS ブリッジ機能を使用する場合は、WDS 用のインタフェースを含み、対象のインタフェース（ether、wlan など）が同一の VLAN となるように設定してください。
- 他社の無線 LAN アクセスポイントとの接続はできません。
- WDS ブリッジを行う無線 LAN アクセスポイント間では、接続認証、接続要求などの手順は行いません。また、利用できる暗号化方式は WEP 暗号化のみです。
- 無線 LAN アクセスポイント 1 台との WDS ブリッジには、無線 LAN インタフェース 1 つを WDS 用のインタフェースとして使用します。そのため、WDS 用のインタフェースを生成した数だけ、仮想アクセスポイントとして利用できる無線 LAN インタフェースが減少することになります。
- 無線 LAN チャネルが W53/W56 で動作している場合、レーダを検出することがあります。レーダを検出した場合、チャネルが自動的に切り替わり、一時的に通信ができなくなるときがあります。WDS のみで運用している場合は、チャネルの切り替えは行われません。レーダを検出したチャネルは 30 分間使用することができないため、WDS のみで運用している場合は、レーダ検出後 30 分間動作を停止します。
- WDS を利用した以下の図のような冗長なネットワーク構成では、無線 LAN 上でのパケットのループが発生するため、このようなネットワーク構成は取らないでください。



- WDS ブリッジを行う無線 LAN アクセスポイント間では、IEEE802.11n および IEEE802.11ac を使用することはできません。
  設定された場合、無線通信モードが 11a/n および 11a/n/ac のときは 11a で動作し、無線通信モードが 11b/g/n および 11g/n のときは 11g で動作します。

WDS ブリッジを行う場合の設定方法を説明します。

参照 VLAN を利用したい場合は、「1.11 VLAN ネットワークを WDS ブリッジ機能で接続する」（P.39）を参照してください。



● 設定条件

[アクセスポイント 1]

有線 LAN を使ってネットワークに接続する

- 利用するポート　：ether1

仮想アクセスポイントを構築する

- 利用する無線 LAN モジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：1（11b/g）
- 利用する無線 LAN インタフェース　：wlan 1
- SSID　：samplenet1
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで“abcdefghijklmnopqrstuvwxyz”

WDS 用の無線 LAN インタフェースを構築する

- 利用する無線 LAN モジュール　：ieee80211 2
- 通信モード　：IEEE802.11a
- チャネル　：36（11a）
- 利用する無線 LAN インタフェース　：wlan 9
- 暗号化モード　：WEP
- WEP キー　：テキストで“ABCDEFGHIJKLM”
- 相手無線 LAN アクセスポイント MAC アドレス　：00:00:0e:0a:22:22

[アクセスポイント2]

仮想アクセスポイントを構築する

- 利用する無線LANモジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：11（11b/g）
- 利用する無線LANインタフェース　：wlan 1
- SSID　：samplenet2
- 認証モード　：WPA/WPA2-PSK自動判別認証
- 暗号化モード　：TKIP/AES自動判別
- 事前共有キー（PSK）　：テキストで“zyxwvutsrqponmlkjihgfedcba”

WDS用の無線LANインタフェースを構築する

- 利用する無線LANモジュール　：ieee80211 2
- 通信モード　：IEEE802.11a
- チャネル　：36（11a）
- 利用する無線LANインタフェース　：wlan 9
- 暗号化モード　：WEP
- WEPキー　：テキストで“ABCDEFGHIJKLM”
- 相手無線LANアクセスポイントMACアドレス　：00:00:0e:0a:11:11

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[アクセスポイント1]

```
仮想アクセスポイントを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 1
# wlan 1 use on
# wlan 1 ssid samplenet1
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz

WDS用の無線LANインタフェースを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 36
# wlan 9 use on
# wlan 9 type wds
# wlan 9 wep mode enable
# wlan 9 wep key 1 text ABCDEFGHIJKLM
# wlan 9 wep send 1
# wlan 9 wds neighbor 00:00:0e:0a:22:22

高速転送モードを無効にする
# system bridge acceleration mode disable

設定終了
# save
# commit
```

[アクセスポイント2]

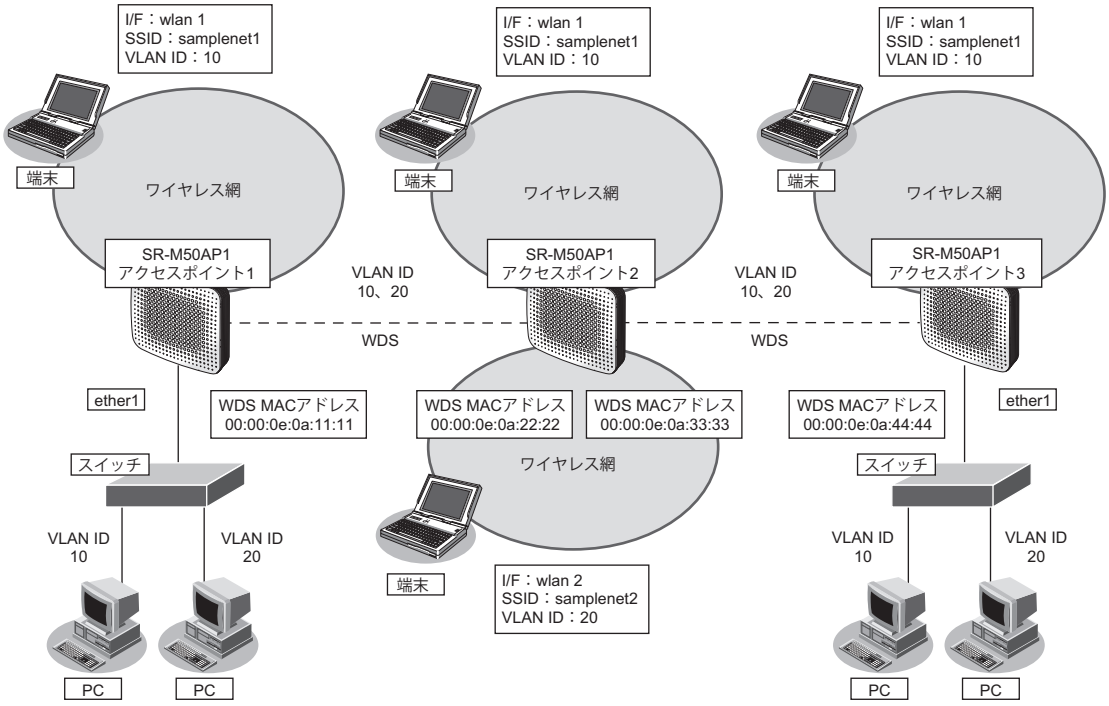
```
仮想アクセスポイントを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 11
# wlan 1 use on
# wlan 1 ssid samplenet2
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text zyxwvutsrqponmlkjihgfedcba

WDS用の無線LANインタフェースを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 36
# wlan 9 use on
# wlan 9 type wds
# wlan 9 wep mode enable
# wlan 9 wep key 1 text ABCDEFGHIJKLM
# wlan 9 wep send 1
# wlan 9 wds neighbor 00:00:0e:0a:11:11

高速転送モードを無効にする
# system bridge acceleration mode disable

設定終了
# save
# commit
```

1.11　VLAN ネットワークを WDS ブリッジ機能で接続する

適用機種　***SR-M50AP1***

WDS ブリッジに利用する無線 LAN インタフェースをタグ付きのインタフェースとして設定することで、WDS ブリッジは VLAN ネットワークどうしを接続することができます。

ここでは、3 台の SR-M50AP1 のそれぞれの VLAN ネットワークを、WDS ブリッジによって接続する場合の設定方法を説明します。



● 設定条件

[アクセスポイント 1]

有線 LAN を使ってネットワークに接続する

- 利用するポート　：ether1
- VLAN ID　：10、20

仮想アクセスポイントを構築する

- 利用する無線 LAN モジュール　：ieee80211 2
- 通信モード　：IEEE802.11a
- チャネル　：36（11a）
- 利用する無線 LAN インタフェース　：wlan 9
- SSID　：samplenet1
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで “abcdefghijklmnopqrstuvwxyz”
- VLAN ID　：10

WDS 用の無線 LAN インタフェースを構築する

- 利用する無線 LAN モジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：1（11b/g）
- 利用する無線 LAN インタフェース　：wlan 1
- 暗号化モード　：WEP
- WEP キー　：テキストで “ABCDEFGHIJKLM”
- 相手無線 LAN アクセスポイント MAC アドレス　：00:00:0e:0a:22:22
- VLAN ID　：10、20

[アクセスポイント 2]

仮想アクセスポイント 1 を構築する

- 利用する無線 LAN モジュール　：ieee80211 2
- 通信モード　：IEEE802.11a
- チャネル　：40（11a）
- 利用する無線 LAN インタフェース　：wlan 9
- SSID　：samplenet1
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで “abcdefghijklmnopqrstuvwxyz”
- VLAN ID　：10

仮想アクセスポイント 2 を構築する

- 利用する無線 LAN モジュール　：ieee80211 2
- 通信モード　：IEEE802.11a
- チャネル　：40（11a）
- 利用する無線 LAN インタフェース　：wlan 10
- SSID　：samplenet2
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで “zyxwvutsrqponmlkjihgfedcba”
- VLAN ID　：20

WDS 用の無線 LAN インタフェース 1 を構築する

- 利用する無線 LAN モジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：1（11b/g）
- 利用する無線 LAN インタフェース　：wlan 1
- 暗号化モード　：WEP
- WEP キー　：テキストで “ABCDEFGHIJKLM”
- 相手無線 LAN アクセスポイント MAC アドレス　：00:00:0e:0a:11:11
- VLAN ID　：10、20

WDS 用の無線 LAN インタフェース 2 を構築する

- 利用する無線 LAN モジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：1（11b/g）
- 利用する無線 LAN インタフェース　：wlan 2
- 暗号化モード　：WEP
- WEP キー　：テキストで “ZYXWVUTSRQPON”
- 相手無線 LAN アクセスポイント MAC アドレス　：00:00:0e:0a:44:44
- VLAN ID　：10、20

[アクセスポイント 3]

有線 LAN を使ってネットワークに接続する

- 利用するポート　：ether1
- VLAN ID　：10、20

仮想アクセスポイントを構築する

- 利用する無線 LAN モジュール　：ieee80211 2
- 通信モード　：IEEE802.11a
- チャネル　：44（11a）
- 利用する無線 LAN インタフェース　：wlan 9
- SSID　：samplenet1
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで “abcdefghijklmnopqrstuvwxyz”
- VLAN ID　：10

WDS 用の無線 LAN インタフェースを構築する

- 利用する無線 LAN モジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：1（11b/g）
- 利用する無線 LAN インタフェース　：wlan 1
- 暗号化モード　：WEP
- WEP キー　：テキストで “ZYXWVUTSRQPON”
- 相手無線 LAN アクセスポイント MAC アドレス　：00:00:0e:0a:33:33
- VLAN ID　：10、20

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[アクセスポイント1]

```
ETHER1 ポートを設定する
# ether 1 vlan tag 10,20

仮想アクセスポイントを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 36
# wlan 9 use on
# wlan 9 ssid samplenet1
# wlan 9 auth wpa/wpa2-psk
# wlan 9 wpa cipher auto
# wlan 9 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 9 vlan untag 10

WDS 用の無線 LAN インタフェースを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 1
# wlan 1 use on
# wlan 1 type wds
# wlan 1 wep mode enable
# wlan 1 wep key 1 text ABCDEFGHIJKLM
# wlan 1 wep send 1
# wlan 1 wds neighbor 00:00:0e:0a:22:22
# wlan 1 vlan tag 10,20

高速転送モードを無効にする
# system bridge acceleration mode disable

設定終了
# save
# commit
```

[アクセスポイント2]

```
仮想アクセスポイント 1 を設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 40
# wlan 9 use on
# wlan 9 ssid samplenet1
# wlan 9 auth wpa/wpa2-psk
# wlan 9 wpa cipher auto
# wlan 9 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 9 vlan untag 10

仮想アクセスポイント 2 を設定する
# wlan 10 use on
# wlan 10 ssid samplenet2
# wlan 10 auth wpa/wpa2-psk
# wlan 10 wpa cipher auto
# wlan 10 wpa psk text zyxwvutsrqponmlkjihgfedcba
# wlan 10 vlan untag 20

WDS 用の無線 LAN インタフェース 1 を設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 1
# wlan 1 use on
```

```
# wlan 1 type wds
# wlan 1 wep mode enable
# wlan 1 wep key 1 text ABCDEFGHIJKLM
# wlan 1 wep send 1
# wlan 1 wds neighbor 00:00:0e:0a:11:11
# wlan 1 vlan tag 10,20

WDS 用の無線 LAN インタフェース 2 を設定する
# wlan 2 use on
# wlan 2 type wds
# wlan 2 wep mode enable
# wlan 2 wep key 1 text ZYXWVUTSRQPON
# wlan 2 wep send 1
# wlan 2 wds neighbor 00:00:0e:0a:44:44
# wlan 2 vlan tag 10,20

高速転送モードを無効にする
# system bridge acceleration mode disable

設定終了
# save
# commit
```

[アクセスポイント 3]

```
ETHER1 ポートを設定する
# ether 1 vlan tag 10,20

仮想アクセスポイントを設定する
# ieee80211 2 use on
# ieee80211 2 mode 11a
# ieee80211 2 channel 44
# wlan 9 use on
# wlan 9 ssid samplenet1
# wlan 9 auth wpa/wpa2-psk
# wlan 9 wpa cipher auto
# wlan 9 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 9 vlan untag 10

WDS 用の無線 LAN インタフェースを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 1
# wlan 1 use on
# wlan 1 type wds
# wlan 1 wep mode enable
# wlan 1 wep key 1 text ZYXWVUTSRQPON
# wlan 1 wep send 1
# wlan 1 wds neighbor 00:00:0e:0a:33:33
# wlan 1 vlan tag 10,20

高速転送モードを無効にする
# system bridge acceleration mode disable

設定終了
# save
# commit
```

1.12　MACアドレスフィルタリング機能を使う

適用機種　***SR-M50AP1***

MACアドレスフィルタリング機能は、無線LAN端末のMACアドレスを判別し、無線LANアクセスポイントへの接続を制御することでセキュリティを向上させることができます。

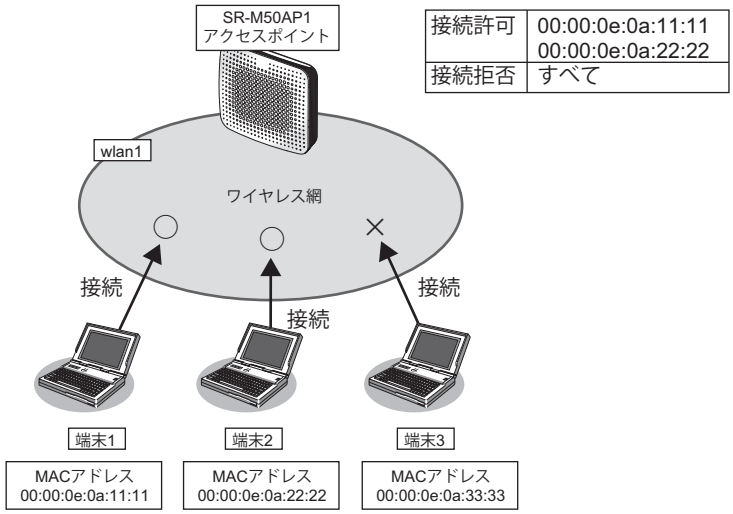
SR-M50AP1では、送信元MACアドレス（無線LAN端末のMACアドレス）のみをフィルタリングの対象とします。

無線LANアクセスポイントのMACアドレスフィルタリングの設計方針には、以下の2つがあります。

- 基本的に無線LAN端末の接続をすべて拒否し、特定の端末だけ接続を許可する
- 基本的に無線LAN端末の接続をすべて許可し、特定の端末だけ接続を拒否する

ここでは、特定の端末だけ接続を許可する設定例について説明します。

特定の端末だけ接続を拒否するには、以下のフィルタリングのポリシーを逆にした設定を行います。



● 設定条件

無線LANを使用する

- 利用する無線LANモジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- 11b/gチャネル　：11

仮想アクセスポイントを構築する

- 利用する無線LANインタフェース　：wlan 1
- SSID　：samplenet
- 認証モード　：WPA/WPA2-PSK自動判別認証
- 暗号化モード　：TKIP/AES自動判別
- 事前共有キー（PSK）　：テキストで“abcdefghijklmnopqrstuvwxyz”
- 接続を許可する無線LAN端末のMACアドレス　：00:00:0e:0a:11:11
  ：00:00:0e:0a:22:22
- 接続を拒否する無線LAN端末のMACアドレス　：その他すべて

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 11

仮想アクセスポイントを設定する
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz

MACアドレス00:00:0e:0a:11:11の無線LAN端末からの接続を許可する
# acl 0 mac 00:00:0e:0a:11:11 any
# wlan 1 macfilter 0 pass acl 0

MACアドレス00:00:0e:0a:22:22の無線LAN端末からの接続を許可する
# acl 1 mac 00:00:0e:0a:22:22 any
# wlan 1 macfilter 1 pass acl 1

残りの無線LAN端末からの接続をすべて拒否する
# acl 2 mac any any
# wlan 1 macfilter 2 reject acl 2

設定終了
# save
# commit
```

1.13　WMM機能を使う

適用機種　***SR-M50AP1***

WMM機能とは、無線LAN端末に送出するパケットの優先制御を行う機能です。

本機能を利用することで、トラフィックが多い場合でも、音声やビデオなどのパケットを優先的に送出することができ、通信の途切れを軽減することができます。

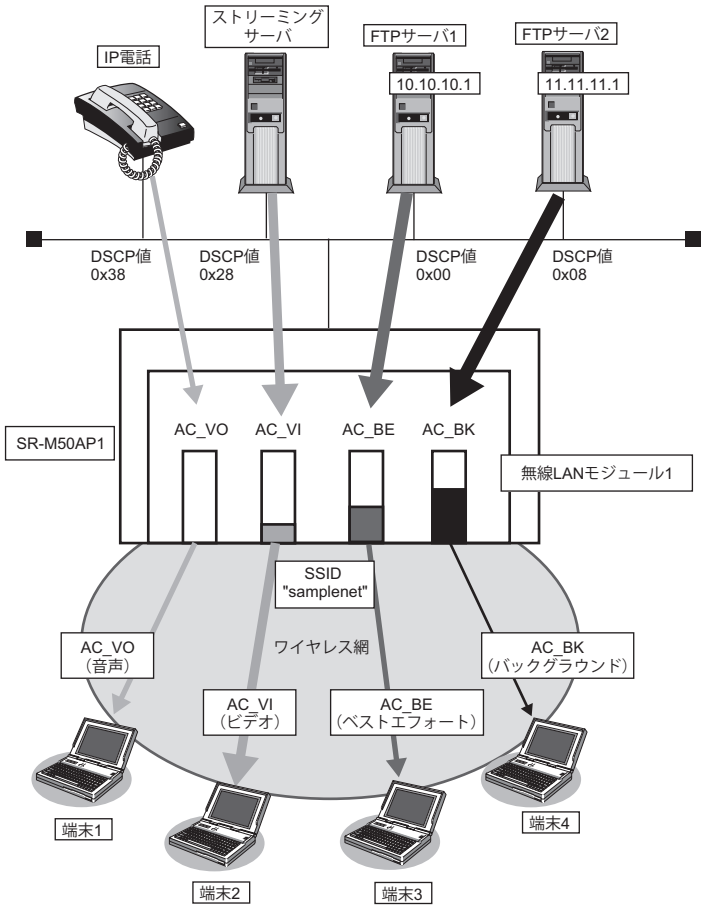
無線に送出するパケットはIPパケットのDSCP値を元に、4種類のAccess Category（AC）に分類されます。ACは優先度が高い方から、AC_VO（音声）、AC_VI（ビデオ）、AC_BE（ベストエフォート）、AC_BK（バックグラウンド）であり、ACごとに送信キューを持ちます。送信キューにパケットがたまっている場合は、優先度の低いACより優先度の高いACの送信キューから優先的にパケットが送出されます。

こんな事に気をつけて

- 以下のパケットは常に同じACに分類されます。

種別	AC
EAPOLパケット	AC_VO
ARPパケット	AC_VO
IPヘッダを含まないパケット	AC_BE
WMMに対応していない端末あてのパケット	AC_BE

- 本機能は無線LANモジュール単位で制御するため、本機能の有効化／無効化を仮想アクセスポイントごとに設定することはできません。同一の無線LANモジュールを使用しているほかの仮想アクセスポイントのトラフィックの状況によっては、優先度の高いパケットでも送出が遅れる場合があります。



以下に、DSCP 値と AC の分類の対応表を示します。

DSCP 値は 6 ビットのうち、先頭 3bit だけが AC の分類に使用されます。

DSCP 値			AC 分類
	10 進数の値	先頭 3bit の値	
0x38 ～ 0x3f 0x30 ～ 0x37	56 ～ 63 48 ～ 55	7 6	AC_VO
0x28 ～ 0x2f 0x20 ～ 0x27	40 ～ 47 32 ～ 39	5 4	AC_VI
0x18 ～ 0x1f 0x00 ～ 0x07	24 ～ 31 0 ～ 7	3 0	AC_BE
0x10 ～ 0x17 0x08 ～ 0x0f	16 ～ 23 8 ～ 15	2 1	AC_BK

● 設定条件

無線 LAN を使用する

- 利用する無線 LAN モジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：1
- WMM 機能　：有効にする

仮想アクセスポイントを構築する

- 利用する無線 LAN インタフェース：wlan 1
- SSID　：samplenet
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで “abcdefghijklmnopqrstuvwxyz”

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線 LAN モジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 1

WMM 機能を設定する
# ieee80211 1 wmm mode enable

仮想アクセスポイントを設定する
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz

設定終了
# save
# commit
```

1.14　WMM機能のAccess Category分類条件を変更する

適用機種　*SR-M50AP1*

WMM機能で利用されるAccess Category（AC）の分類条件を変更することができます。

本機能を利用することで、端末ごとの優先度の設定や、ネットワーク全体でQoSのポリシーの統一を行うことができます。

書き換え条件

以下の条件を指定することによって、AC分類条件を指定することができます。どの条件にも一致しなかったパケットは、「1.13 WMM機能を使う」（P.46）の動作に従って分類されます。

- ACLのIP定義で指定した以下の情報
  - 送信元IP情報（IPアドレス／アドレスマスク）
  - あて先IP情報（IPアドレス／アドレスマスク）
  - プロトコル番号
  - TOS値、DSCP値

ここでは、以下の場合を例に説明します。

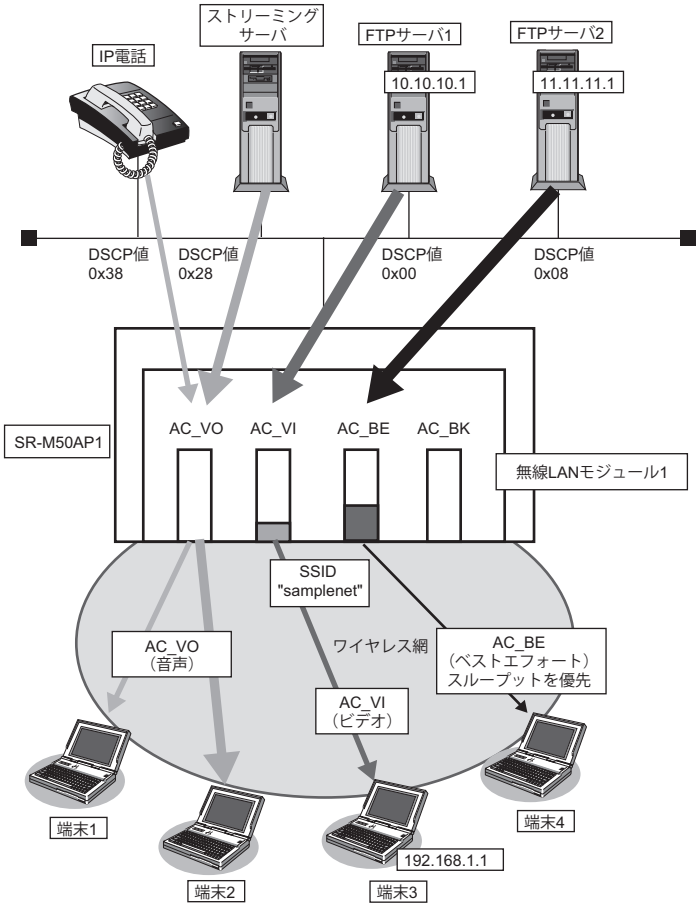
- ビデオのトラフィックは、ACを音声に分類する
- 端末3あてのトラフィックは、ACをビデオに分類する
- FTPサーバ2からのトラフィックは、ベストエフォートに分類する
- IP電話からのトラフィックはACを変更しない
- ベストエフォートのトラフィックは、スループットを優先する

こんな事に気をつけて

- 以下のパケットはACLで指定した条件にかかわらず、常に同じACに分類されます。

種別	AC
EAPOLパケット	AC_VO
ARPパケット	AC_VO
IPヘッダを含まないパケット	AC_BE
WMMに対応していない端末あてのパケット	AC_BE

- 5GHz帯の通信モードにおいて、Access Category分類条件の変更は動作しません。



● 設定条件

無線 LAN を使用する

- 利用する無線 LAN モジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：6
- WMM 機能　：使用する
- ACK 応答要求の設定　：AC_BE で送信するデータに対する ACK 応答を要求しない

仮想アクセスポイントを構築する

- 利用する無線 LAN インタフェース　：wlan 1
- SSID　：samplenet
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで“abcdefghijklmnopqrstuvwxyz”
- AC 分類条件　：DSCP 値が 0x28（10 進数で 40）の場合、AC_VO に分類する
  あて先 IP アドレスが 192.168.1.1/32 の場合、AC_VO に分類する
  送信元 IP アドレスが 11.11.11.0/24 の場合、AC_BE に分類する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 6

WMM機能を設定する
# ieee80211 1 wmm mode enable

ACK応答要求を設定する
# ieee80211 1 wmm ack besteffort disable

仮想アクセスポイントを設定する
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz

AC分類条件を設定する
# wlan 1 wmm aclmap 0 ac voice 0
# wlan 1 wmm aclmap 1 ac video 1
# wlan 1 wmm aclmap 2 ac besteffort 2

ACLを設定する
# acl 0 ip any any any dscp 40
# acl 1 ip any 192.168.1.1/32 any any
# acl 2 ip 11.11.11.0/24 any any any

設定終了
# save
# commit
```

1.15　周辺アクセスポイント検出機能を使う

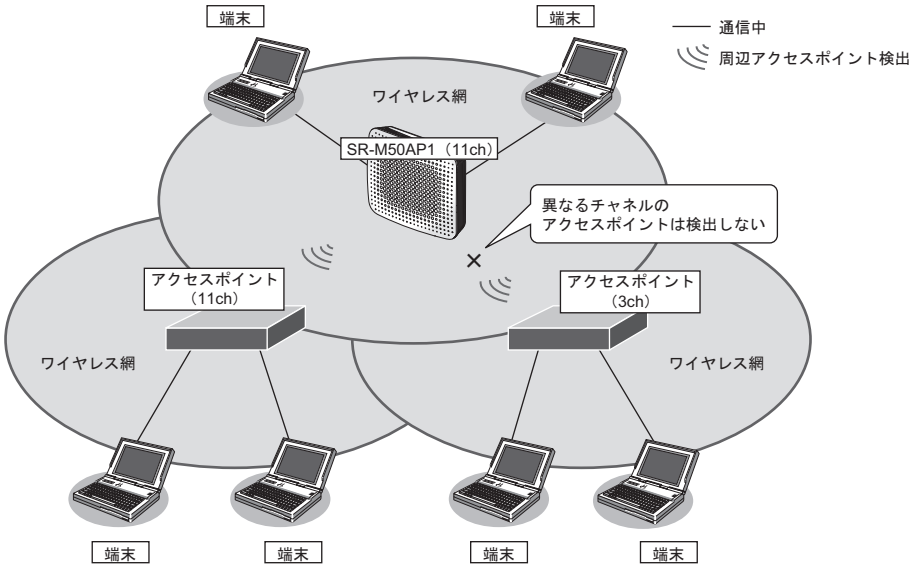
適用機種　***SR-M50AP1***

無線LANアクセスポイントの運用をしながら無線電波を検出することで、SR-M50AP1周辺の無線LANアクセスポイントを検出することができます。周辺アクセスポイントの検出は現在運用中のチャネルだけで行います。
また、手動スキャンを実施することで最新の周辺アクセスポイント情報を知ることができます。

☛参照　マニュアル「コマンドリファレンス」の「周辺アクセスポイント情報の取得、表示」

こんな事に気をつけて

- 無線LANアクセスポイントの運用では、スループットが低下することがあります。
- 電波干渉により近隣チャネルで動作している無線LANアクセスポイントも検出されることがあります。



● 設定条件

無線LANを使用する

- 利用する無線LANモジュール　：ieee80211 1
- 通信モード　：IEEE802.11b/g
- チャネル　：11
- 周辺アクセスポイント検出の動作モード　：enable

仮想アクセスポイントを構築する

- 利用する無線LANインタフェース　：wlan 1
- SSID　：samplenet
- 認証モード　：WPA/WPA2-PSK 自動判別認証
- 暗号化モード　：TKIP/AES 自動判別
- 事前共有キー（PSK）　：テキストで “abcdefghijklmnopqrstuvwxyz”

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 11

周辺アクセスポイント検出機能を有効にする
# ieee80211 1 apscan mode enable

仮想アクセスポイントを設定する
# wlan 1 use on
# wlan 1 ssid samplenet
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz

設定終了
# save
# commit
```

1.16　監視専用装置として周辺アクセスポイント検出機能を使う

適用機種　***SR-M50AP1***

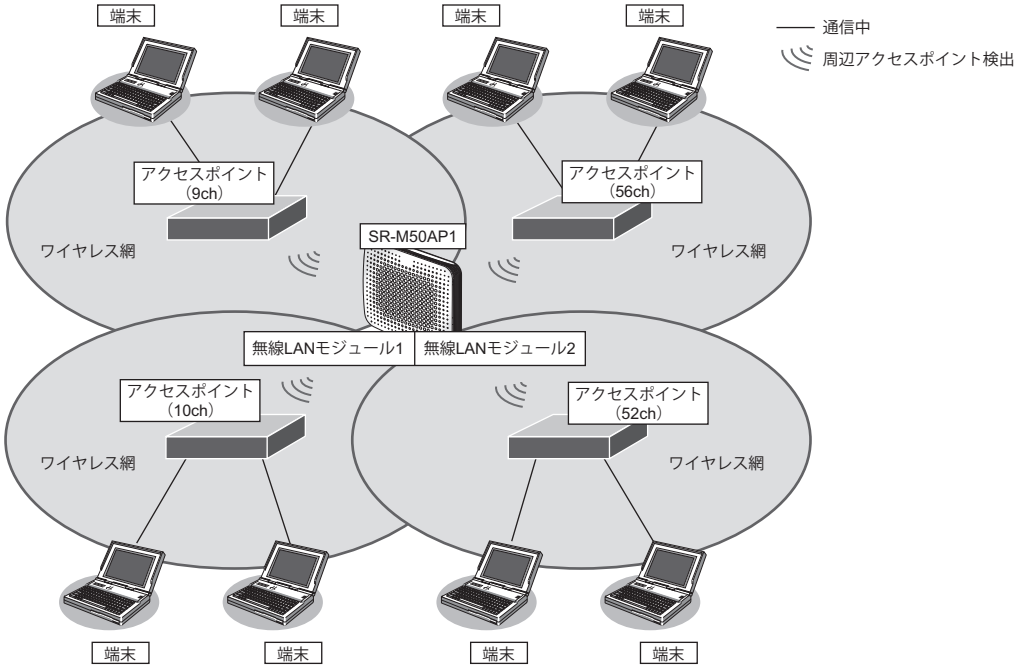
無線LANアクセスポイントの運用をしないで検出だけを行います。SR-M50AP1周辺の無線LANアクセスポイントを無線LANモジュールで利用可能なすべてのチャネルで検出することができます。

また、手動スキャンを実施することで最新の周辺アクセスポイント情報を知ることができます。

参照　マニュアル「コマンドリファレンス」の「周辺アクセスポイント情報の取得、表示」

こんな事に気をつけて

- 無線LAN端末との接続はできません。
- レーダ検出などにより利用不可中のチャネルは検出の対象外となります。



● 設定条件

無線LANを使用する

- 利用する無線LANモジュール　：ieee80211 1およびieee80211 2
- 通信モード　：IEEE802.11b/gおよびIEEE802.11a
- 周辺アクセスポイント検出の動作モード　：enable

無線LANインタフェースを設定する

- 利用する無線LANインタフェース　：wlan 1およびwlan 9
- 無線LANインタフェースの動作タイプ　：scanonly

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LANモジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 2 use on
# ieee80211 2 mode 11a

周辺アクセスポイント検出機能を有効にする
# ieee80211 1 apscan mode enable
# ieee80211 2 apscan mode enable

無線LANインタフェースを設定する
# wlan 1 use on
# wlan 1 type scanonly
# wlan 9 use on
# wlan 9 type scanonly

設定終了
# save
# commit
```

1.17　IEEE802.11n チャネルボンディング機能を使う

適用機種　***SR-M50AP1***

チャネルボンディングとは、隣り合った2つのチャネルを束ねて通信する機能です。従来の倍の40MHzの帯域幅を使用し、通信速度を向上させることができます。

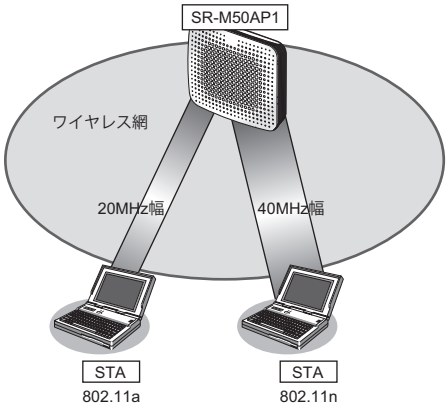
こんな事に気をつけて

- チャネルボンディングを使用する場合、無線LANクライアントでチャネルボンディングを有効にする必要があります。
- 2.4GHz帯の場合、セカンダリチャネルに他BSSのプライマリチャネルが存在するときは、自動的に20MHz幅のBSSを開始します。
- 5GHz帯の場合、他BSSのプライマリチャネル、セカンダリチャネルの存在有無に関わらず、自動的に40MHz幅のBSSを開始します。
- 5GHz帯の場合、無線LANアクセスポイントが運用を開始したあとは、他無線LAN装置と電波干渉が発生しても、帯域幅を20MHzに縮退動作することはありません。
- 2.4GHz帯では重なり合わない40MHzチャネルが1つしか確保できないことに加え、ほかのチャネルとの干渉が発生しやすいため、チャネルボンディングは5GHz帯での使用を推奨します。

チャネルボンディング機能を利用できるチャネルの組み合わせはIEEE802.11n規約によって制限されており、プライマリチャネル番号とセカンダリチャネル番号を正しく設定する必要があります。
本装置では、使用するセカンダリチャネルを、プライマリチャネル番号のオフセットとして指定します。
プライマリチャネル番号（無線LANチャネル番号）とセカンダリチャネルオフセットが有効となる組み合わせは以下のとおりです。

周波数帯	プライマリチャネル番号	セカンダリチャネルオフセット	セカンダリチャネル番号
2.4GHz	1	above	5
	2	above	6
	3	above	7
	4	above	8
	5	above	9
		below	1
	6	above	10
		below	2
	7	above	11
		below	3
	8	above	12
		below	4
	9	above	13
		below	5
	10	below	6
	11	below	7
	12	below	8
	13	below	9
W52	36	above	40
	40	below	36
	44	above	48
	48	below	44
W53	52	above	56
	56	below	52
	60	above	64
	64	below	60

周波数帯	プライマリチャネル番号	セカンダリチャネル オフセット	セカンダリチャネル番号
W56	100	above	104
	104	below	100
	108	above	112
	112	below	108
	116	above	120
	120	below	116
	124	above	128
	128	below	124
	132	above	136
	136	below	132



● 前提条件

- SR-M50AP1、無線 LAN クライアントで、チャネルボンディング以外は、正しく設定されている。

● 設定条件

- チャネルボンディング　　：使用する（40MHz の帯域を使用する）
- プライマリチャネル番号　　：52 チャネル
- セカンダリチャネル番号　　：56 チャネル

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
チャネルボンディング機能を設定する
# ieee80211 2 channel 52
# ieee80211 2 bandwidth 40
# ieee80211 2 secondary-channel above

設定終了
# save
# commit
```

1.18　IEEE802.11ac チャネルボンディング機能を使う

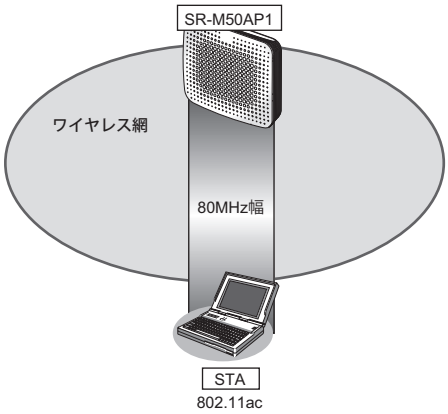
適用機種　***SR-M50AP1***

チャネルボンディングとは、隣り合った2つのチャネルを束ねて通信する機能です。

IEEE802.11 n では従来の倍の40MHzの帯域幅を使用しますが、IEEE802.11acでは従来の4倍の80MHzの帯域幅を使用し、通信速度を向上させることができます。

こんな事に気をつけて

- チャネルボンディングを使用する場合、無線LANクライアントでチャネルボンディングを有効にする必要があります。
- 802.11acでチャネルボンディングを使用する場合、セカンダリチャネル番号の設定は必要ありません。



● 前提条件

- SR-M50AP1、無線LANクライアントで、チャネルボンディング以外は、正しく設定されている。

● 設定条件

- チャネルボンディング　　：使用する（80MHzの帯域を使用する）
- プライマリチャネル番号　　：52チャネル

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
チャネルボンディング機能を設定する
# ieee80211 2 channel 52
# ieee80211 2 bandwidth 80
```

2　VLAN 機能を使う

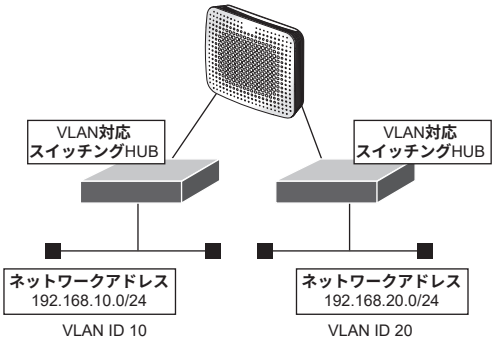
適用機種　*SR-M50AP1*

参照　マニュアル「機能説明書」

2.1　ポート VLAN 機能を使う

適用機種　*SR-M50AP1*

ここでは、ポート単位でグループ化したタグなしパケットをポート VLAN で送受信する場合の設定方法を説明します。



● 設定条件

- ETHER1、2 ポートを使用する
- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：10　　ネットワークアドレス：192.168.10.0/24
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

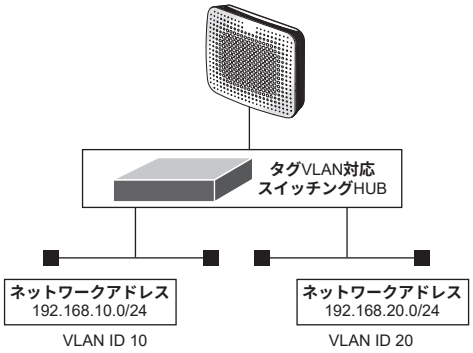
● コマンド

```
ETHER1 ポートを設定する
# ether 1 vlan untag 10

ETHER2 ポートを設定する
# ether 2 vlan untag 20

192.168.10.1/24 のネットワークを設定する
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 10

192.168.20.1/24 のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

2.2　タグ VLAN 機能を使う

適用機種　***SR-M50AP1***

ここでは、1つのポートで、2つのVLANからのタグ付きパケットを、それぞれのVLANで送受信する場合の設定方法を説明します。



● 設定条件

- ETHER1 ポートだけを使用する
- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：10　　ネットワークアドレス：192.168.10.0/24
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

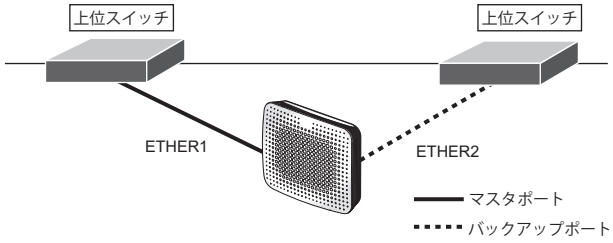
● コマンド

```
ETHER1 ポートを設定する
# ether 1 vlan tag 10,20

ETHER2 ポートを未設定にする
# ether 2 use off

192.168.10.1/24 のネットワークを設定する
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 10

192.168.20.1/24 のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

3　バックアップポート機能を使う

適用機種　***SR-M50AP1***

ここでは、バックアップポートを利用する場合の設定方法について説明します。
対象となるポートをそれぞれ異なるスイッチに接続することで、冗長接続形態を取ることができます。



● 設定条件

- ETHER1、2 ポートをバックアップポートとして使用する
  （ETHER1 をマスタポート、ETHER2 をバックアップポートとする）
- マスタポートを優先的に使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

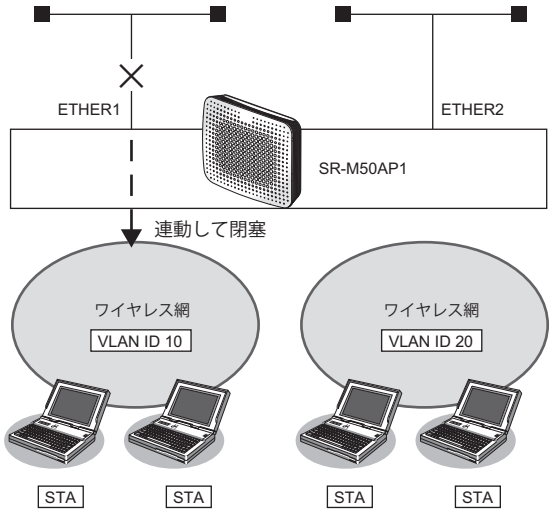
● コマンド

```
ETHER1 ポートをバックアップポート（グループ 1）のマスタポートに設定する
# ether 1 type backup 1 master

ETHER2 ポートをバックアップポート（グループ 1）のバックアップポートに設定する
# ether 2 type backup 1 backup

バックアップグループ 1 をマスタポート優先モードに設定する
# backup 1 mode master

設定終了
# save
# commit
```

4　リンクインテグリティ機能を使う

適用機種　***SR-M50AP1***

ここでは、ETHER ポートがリンクダウンした場合、連動して指定した無線 LAN インタフェースを閉塞させる場合の設定方法について説明します。



● 設定条件

- ETHER1 ポートに連動して無線 LAN インタフェース 1 ～ 8 を閉塞させる
  利用する無線 LAN インタフェース ：wlan 1 ～ wlan 8
  VLAN ID　：10
- ETHER2 ポートに連動して無線 LAN インタフェース 9 ～ 16 を閉塞させる
  利用する無線 LAN インタフェース ：wlan 9 ～ wlan 16
  VLAN ID　：20

上記の設定条件に従って設定を行う場合のコマンド例を示します。

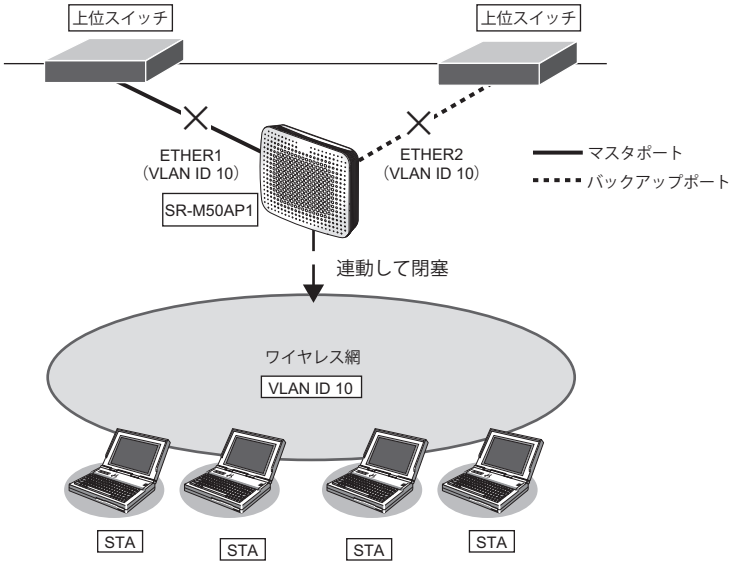
● コマンド

```
ETHER1 ポートを設定する
# ether 1 vlan tag 10

ETHER2 ポートを設定する
# ether 2 vlan tag 20

ETHER1 ポートがリンクダウンした場合、WLAN1 ～ 8 が連動して閉塞状態になるように設定する
# ether 1 downrelay wlan 1-8

ETHER2 ポートがリンクダウンした場合、WLAN9 ～ 16 が連動して閉塞状態になるように設定する
# ether 2 downrelay wlan 9-16

自動的に閉塞解除するモードに設定する
# ether 1 downrelay recovery mode auto
# ether 2 downrelay recovery mode auto

設定終了
# save
# commit
```

4.1　バックアップポートでリンクインテグリティ機能を使う

適用機種　***SR-M50AP1***

ここでは、バックアップポート機能に連動して、指定した無線LANインタフェースを閉塞させる場合の設定方法について説明します。



● 設定条件

- バックアップポート機能に連動して無線LANインタフェース1～16を閉塞させる
  利用する無線LANインタフェース：wlan 1～wlan 16
  VLAN ID　：10

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

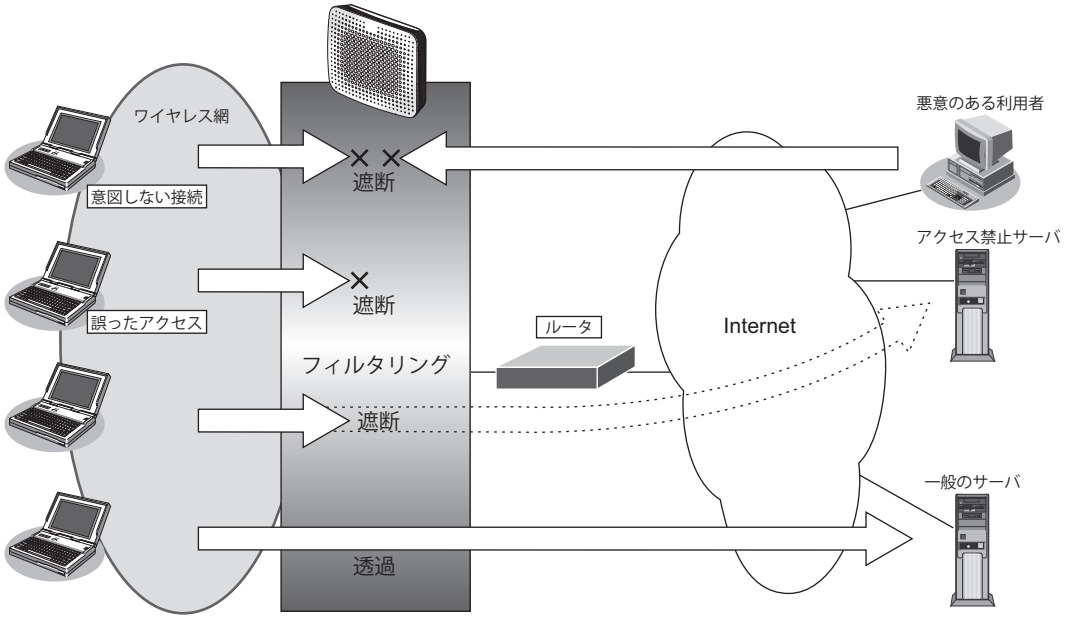
```
ETHER1 ポートを設定する
# ether 1 vlan tag 10

ETHER2 ポートを設定する
# ether 2 vlan tag 10

ETHER1 ポートをバックアップポート（グループ 1）のマスタポートに設定する
# ether 1 type backup 1 master

ETHER2 ポートをバックアップポート（グループ 1）のバックアップポートに設定する
# ether 2 type backup 1 backup

バックアップポートダウンした場合、WLAN1～16 が連動して閉塞状態になるように設定する
# backup 1 downrelay wlan 1-16

自動的に閉塞解除するモードに設定する
# backup 1 downrelay recovery mode auto

設定終了
# save
# commit
```

5　フィルタリング機能を使う

適用機種　***SR-M50AP1***

本装置を経由するパケットを、MACアドレス、VLAN ID、IPアドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティの向上や、ネットワークへの負荷を軽減することができます。

☛参照　マニュアル「機能説明書」



フィルタリングの条件

本装置では、ACL番号で指定したACL定義の中で、以下の条件を指定することによってデータの流れを制御できます。

- 送信元MAC情報（MACアドレス）
- あて先MAC情報（MACアドレス）
- VLAN ID
- 送信元情報（IPアドレス／アドレスマスク／ポート番号）
- あて先情報（IPアドレス／アドレスマスク／ポート番号）
- プロトコル
- TCP・UDPのポート番号
- TCP接続要求
- ICMPのTYPE/CODE
- IPパケットのTOS値／DSCP値

ヒント

◆ IP アドレスとアドレスマスクの決め方

IP フィルタリング条件の要素には「IP アドレス」と「アドレスマスク」があります。制御対象となるパケットは、本装置に届いたパケットの IP アドレスとアドレスマスクの論理積の結果が、指定した IP アドレスと一致したものに限ります。

◆ TCP 接続要求とは？

TCP プロトコルでのコネクション確立要求を、フィルタリングの対象にするかどうかを指定するものです。フィルタリングの動作に透過、プロトコルに TCP を指定した場合に有効です。TCP プロトコルはコネクション型であるため、コネクション確立要求を発行し、それに対する応答を受信することによってコネクションを開設します。そのため、一方からのコネクションを禁止する場合でも、コネクション確立要求だけを遮断し、その他の応答や通常データなどを透過させるように設定しないと通信できません。

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の 2 つがあります。

A. 基本的にパケットをすべて遮断し、特定の条件のものだけを透過させる

B. 基本的にパケットをすべて透過させ、特定の条件のものだけを遮断する

ここでは、設計方針 A の例として、以下の設定例について説明します。

- 特定サービスへのアクセスだけを許可する

また、設計方針 B の例として、以下の設定例について説明します。

- 特定サーバへのアクセスだけを禁止して SPI を併用する
- 特定の MAC アドレス間の通信だけを禁止する

なお、設定例はデフォルト VLAN（VLAN ID = 1）での通信を前提として説明します。

こんな事に気をつけて

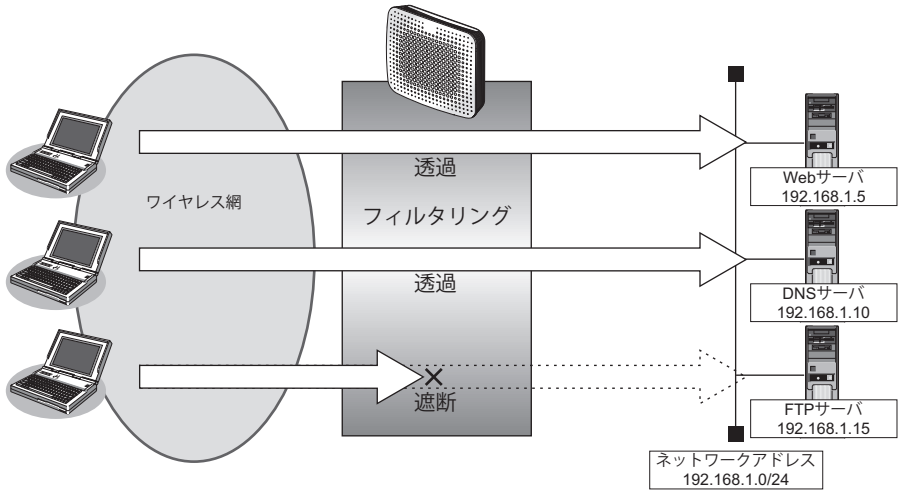
- IP フィルタリングで DHCP（ポート番号 67、68）でのアクセスを制限する設定を行った場合、DHCP 機能が使用できなくなる場合があります。
- フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。
- 高速転送モード機能が有効の場合、フィルタ設定は無効となります。

5.1　特定サービスへのアクセスだけを許可する

適用機種　***SR-M50AP1***

ここでは、すべてのWeb サーバに対してアクセスすることだけを許可し、ほかのサーバ（FTP サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、Web サーバ名を解決するために、DNS サーバへのアクセスは許可します。

補足　DNS サーバに問い合わせが発生する場合、DNS サーバへのアクセスを許可する必要があります。
DNS サーバへのアクセスを許可することによって、Web サービス以外でドメイン名を指定した場合もDNS サーバへの発信が発生します。あらかじめ接続するWeb サーバが決まっている場合は、本装置のDNS サーバ機能を利用することによって、DNS サーバへの発信を抑止することができます。



● フィルタリング設計

- 無線LAN 側（192.168.1.0/24）からWeb サーバへのアクセスを許可
- 無線LAN 側（192.168.1.0/24）からDNS サーバへのアクセスを許可
- ICMP の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- Web サーバへのアクセスを許可するには
  (1) 192.168.1.0/24 の任意のポートから、任意のWeb サーバのポート80（http）へのTCP パケットを透過させる
- DNS サーバへのアクセスを許可するには
  (1) 192.168.1.0/24 の任意のポートから、DNS サーバのポート53（domain）へのUDP パケットを透過させる
- ICMP の通信を許可するためには
  (1) ICMP パケットを透過させる
- その他をすべて遮断するには
  (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

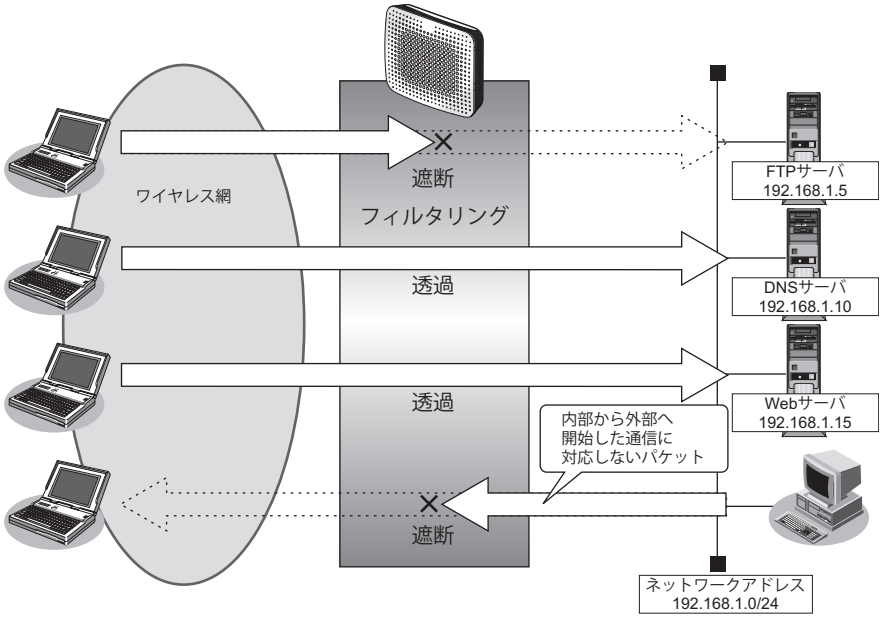
● コマンド

```
任意のWebサーバのポート80へのTCPパケットを透過させる
# acl 0 ip 192.168.1.0/24 any 6 any
# acl 0 tcp any 80 yes
# vlan 1 filter 0 pass 0

Webサーバからの応答パケットを透過させる
# acl 1 ip any 192.168.1.0/24 6 any
# acl 1 tcp 80 any no
# vlan 1 filter 1 pass 1

DNSサーバのポート53へのUDPパケットを透過させる
# acl 2 ip 192.168.1.0/24 192.168.1.10/32 17 any
# acl 2 udp any 53
# vlan 1 filter 2 pass 2

DNSサーバからの応答パケットを透過させる
# acl 3 ip 192.168.1.10/32 192.168.1.0/24 17 any
# acl 3 udp 53 any
# vlan 1 filter 3 pass 3

ICMPのパケットを透過させる
# acl 4 ip any any 1 any
# acl 4 icmp any any
# vlan 1 filter 4 pass 4

残りのパケットをすべて遮断する
# acl 5 ip any any any any
# vlan 1 filter 5 reject 5

高速転送モードを無効にする
# system bridge acceleration mode disable

設定終了
# save
# commit
```

5.2　特定サーバへのアクセスだけを禁止してSPIを併用する

適用機種　***SR-M50AP1***

ここでは、FTPサーバに対するアクセスを禁止する場合の設定方法を説明します。



● フィルタリング設計

- 無線LAN側からLAN上のFTPサーバ（192.168.1.5）へのアクセスを禁止

● フィルタリングルール

- FTPサーバへのアクセスを禁止するには

  (1) 192.168.1.5のポート21（ftp）へのTCPパケットを遮断する

- 無線LAN側からLAN側へのアクセスは許可し、その他をすべて遮断するには

  (1) 残りのパケットにSPIを利用してIPフィルタリングを行う

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
無線LAN端末から192.168.1.5へのFTPのパケットを遮断する
# acl 0 ip any 192.168.1.5/32 6 any
# acl 0 tcp any 21 yes
# vlan 1 filter 0 reject 0

残りのパケットにSPI（無線LAN側を内側とみなす）を利用してIPフィルタリングを行う
# vlan 1 filter default spi wlan 5m

高速転送モードを無効にする
# system bridge acceleration mode disable

設定終了
# save
# commit
```

5.3　特定の MAC アドレス間の通信だけを禁止する

適用機種　***SR-M50AP1***

● フィルタリング設計

- VLAN1でのMACアドレス00:0b:01:02:03:04のホストとMACアドレス00:0b:11:12:13:14のホスト間のTCP通信だけを禁止

上記のフィルタリング設計に従って設定を行う場合のコマンド例を示します。

● コマンド

送信元MACアドレスが00:0b:01:02:03:04、あて先MACアドレスが00:0b:11:12:13:14であるTCPパケットを遮断する
```
# acl 0 mac 00:0b:01:02:03:04 00:0b:11:12:13:14
# acl 0 ip any any 6 any
# vlan 1 filter 0 reject 0
```

送信元MACアドレスが00:0b:11:12:13:14、あて先MACアドレスが00:0b:01:02:03:04であるTCPパケットを遮断する
```
# acl 1 mac 00:0b:11:12:13:14 00:0b:01:02:03:04
# acl 1 ip any any 6 any
# vlan 1 filter 1 reject 1
```

高速転送モードを無効にする
```
# system bridge acceleration mode disable
```

設定終了
```
# save
# commit
```

6　DHCP 機能を使う

適用機種　*SR-M50AP1*

本装置の IPv4 DHCP には、以下の機能があります。

- DHCP クライアント機能

参照　マニュアル「機能説明書」

6.1　DHCP クライアント機能を使う

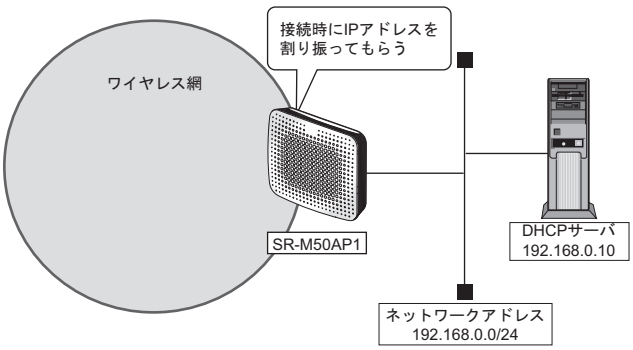
適用機種　*SR-M50AP1*

DHCP クライアント機能は、DHCP サーバから IP アドレスなどの情報を取得する機能です。使用する場合は、DHCP サーバが動作している LAN に接続する必要があります。利用者は、IP アドレスを意識することなくネットワークを利用できます。

本装置の DHCP クライアント機能は、以下の情報を受け取って動作します。

- IP アドレス
- ネットマスク
- リース期間
- デフォルトルータの IP アドレス
- DNS サーバの IP アドレス
- TIME サーバの IP アドレス
- NTP サーバの IP アドレス
- ドメイン名
- リース更新時間

ここでは、DHCP クライアント機能を使用する場合の設定方法を説明します。



● 設定条件

SR-M50AP1

- ETHER1 ポートを使う
- ETHER1 を ポート VLAN（untag 1）に設定する
- 無線 LAN を使って仮想アクセスポイントを構築する
  - 利用する無線 LAN モジュール　：ieee80211 1
  - 利用する無線 LAN インタフェース　：wlan 1
  - 通信モード　：IEEE802.11b/g
  - チャネル　：10（11b/g）
  - SSID　：samplenet
  - 認証モード　：OPEN 認証
- 本装置の IP アドレス　：有線ポート経由で DHCP サーバから取得する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

SR-M50AP1

```
ETHER1 ポートを設定する
# ether 1 use on
# ether 1 vlan untag 1

無線 LAN モジュールを設定する
# ieee80211 1 use on
# ieee80211 1 mode 11b/g
# ieee80211 1 channel 10

仮想アクセスポイントを設定する
# wlan 1 use on
# wlan 1 ssid samplenet

DHCP 機能を設定する
# lan 0 ip dhcp service client
# lan 0 vlan 1

設定終了
# save
# commit
```

7　DNS サーバ機能を使う（ProxyDNS）

適用機種　*SR-M50AP1*

本装置の ProxyDNS には、以下の機能があります。

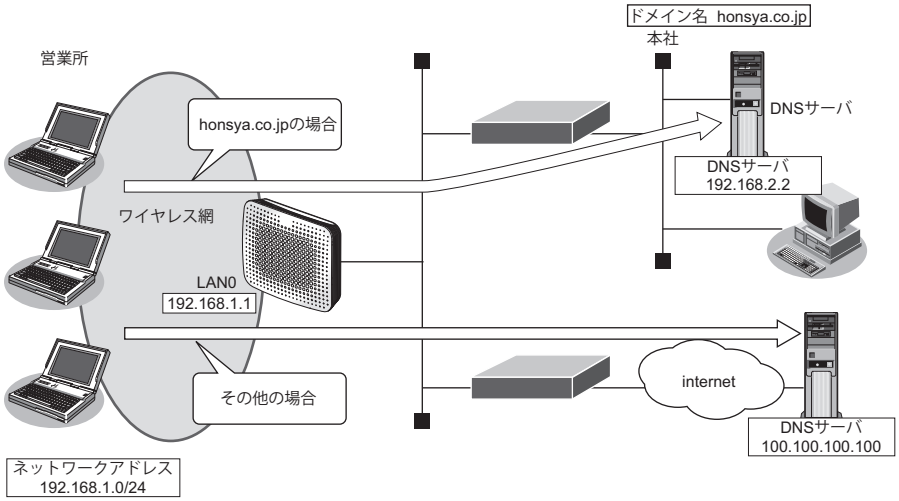
- DNS サーバの自動切り替え機能
- DNS 問い合わせタイプフィルタ機能
- DNS サーバ機能

☛ 参照　マニュアル「機能説明書」

7.1　DNS サーバの自動切り替え機能（順引き）を使う

適用機種　*SR-M50AP1*

ProxyDNS は、パソコン側で本装置の IP アドレスを DNS サーバの IP アドレスとして登録するだけで、ドメインごとに使用する DNS サーバを切り替えて中継できます。ここでは、順引きの場合の設定方法を説明します。



● 設定条件

- 会社の DNS サーバを使用する場合
  使用するドメイン　　：honsya.co.jp
  DNS サーバの IP アドレス　　：192.168.2.2
- インターネット上の DNS サーバを使用する場合
  使用するドメイン　　：honsya.co.jp 以外
  DNS サーバの IP アドレス　　：100.100.100.100

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　マニュアル「コマンドユーザーズガイド」の「コマンドで入力できる文字一覧」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
DNS サーバ自動切り替え機能（順引き）を設定する
# proxydns domain 0 any *.honsya.co.jp any static 192.168.2.2
# proxydns domain 1 any * any static 100.100.100.100

設定終了
# save
# commit
```

パソコン側の設定を確認する

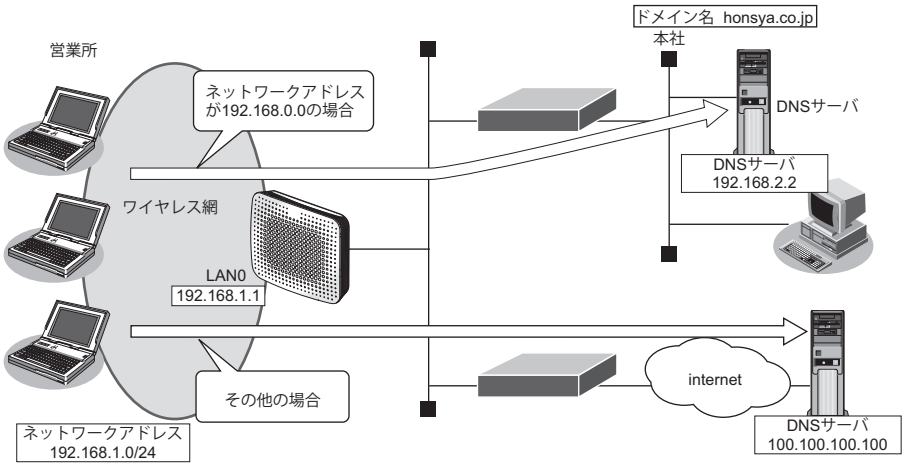
1. パソコン側が DHCP クライアントかどうか確認します。

DHCP クライアントでない場合は設定します。

7.2　DNS サーバの自動切り替え機能（逆引き）を使う

適用機種　***SR-M50AP1***

ProxyDNS は、先に説明した順引きとは逆に、IP アドレスごとに使用する DNS サーバを切り替えて中継できます。ここでは、逆引きの場合の設定方法を説明します。



● 設定条件

- 会社の DNS サーバを使用する場合
  逆引き対象のネットワークアドレス　：192.168.0.0
  DNS サーバの IP アドレス　：192.168.2.2
- インターネット上の DNS サーバを使用する場合
  逆引き対象のネットワークアドレス　：192.168.0.0 以外
  DNS サーバの IP アドレス　：100.100.100.100

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　マニュアル「コマンドユーザーズガイド」の「コマンドで入力できる文字一覧」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
DNS サーバ自動切り替え機能（逆引き）を設定する
# proxydns address 0 192.168.0.0/24 static 192.168.2.2
# proxydns address 1 any static 100.100.100.100

設定終了
# save
# commit
```

パソコン側の設定を確認する

1.　パソコン側が DHCP クライアントかどうか確認します。

DHCP クライアントでない場合は設定します。

7.3　DNS問い合わせタイプフィルタ機能を使う

適用機種　***SR-M50AP1***

端末が送信するDNSパケットのうち、特定の問い合わせタイプ（QTYPE）のパケットを破棄することができます。

こんな事に気をつけて

ProxyDNS機能を使用する場合、問い合わせタイプがA（1）のDNS問い合わせパケットを破棄するように指定にすると、正常な通信が行えなくなります。

● 設定条件

- ドメイン名　：＊
- 問い合わせタイプ　：SOA（6）
- 動作　：破棄する

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　マニュアル「コマンドユーザーズガイド」の「コマンドで入力できる文字一覧」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
DNS問い合わせパケット破棄を設定する
# proxydns domain 0 6 * any reject

設定終了
# save
# commit
```

パソコン側の設定を行う

ここでは、Windows 7の場合を例に説明します。

1. ［スタート］－［コントロールパネル］をクリックします。
2. ［ネットワークとインターネット］をクリックします。
3. ［ネットワークと共有センター］をクリックします。
4. ［アダプターの設定の変更］をクリックします。
5. ［ローカルエリア接続］アイコンを右クリックし、［プロパティ］ボタンをクリックします。
   ［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。
6. 一覧から「インターネットプロトコルバージョン4（TCP/IPv4）」を選択します。

7. ［プロパティ］ボタンをクリックします。
［インターネットプロトコルバージョン4（TCP/IPv4）のプロパティ］ダイアログボックスが表示されます。

8. 「次のDNSサーバーのアドレスを使う」を選択します。

9. 「優先DNSサーバー」に、本装置のIPアドレスを入力します。

10. ［OK］ボタンをクリックします。
［ローカルエリア接続のプロパティ］ダイアログボックスに戻ります。

11. ［閉じる］ボタンをクリックします。
設定した内容が有効になります。

7.4　DNSサーバ機能を使う

適用機種　***SR-M50AP1***

本装置のホストデータベースにホスト名とIPアドレスを登録します。登録したホストに対してDNS要求があった場合は、ProxyDNSがDNSサーバの代わりに応答します。

● 設定条件

- ホスト名　：host.com
- IPv4アドレス　：192.168.1.2

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

参照　マニュアル「コマンドユーザーズガイド」の「コマンドで入力できる文字一覧」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
ホストデータベース情報を設定する
# host 0 name host.com
# host 0 ip address 192.168.1.2

設定終了
# save
# commit
```

補足　ホストデータベース情報は「DNSサーバ機能」で使われており、それぞれ必要な項目だけを設定します。

パソコン側の設定を行う

パソコン側の設定を行います。

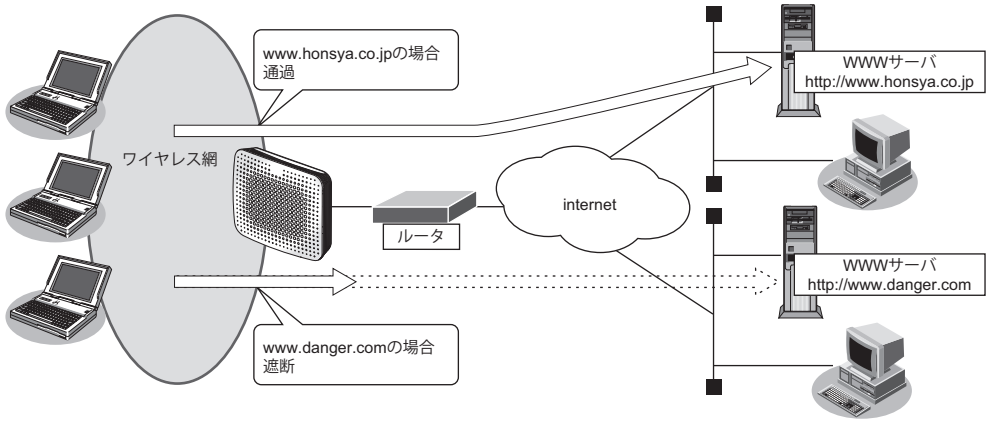
設定方法は、「7.3 DNS 問い合わせタイプフィルタ機能を使う」（P.74）の「 パソコン側の設定を行う」（P.74）を参照してください。

8　特定のURLへのアクセスを禁止する（URLフィルタ機能）

適用機種　***SR-M50AP1***

URLフィルタ機能は、特定のURLへのアクセスを禁止することができます。本機能を使用する場合は、ProxyDNS情報で設定します。

以下にURLフィルタを行う場合の設定方法を説明します。



☛参照　マニュアル「機能説明書」

ここでは、会社のネットワークとプロバイダがすでに接続されていることを前提とします。また、ProxyDNS情報は何も設定されていないものとします。

● 設定条件

- アクセスを禁止するドメイン名　：www.danger.com
- DNSサーバのIPアドレス　：100.100.100.100

こんな事に気をつけて

- URLフィルタ機能を使用する場合は、LAN内のパソコンが本装置のIPアドレスをDNSサーバのIPアドレスとして登録する必要があります。
- コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛参照　マニュアル「コマンドユーザーズガイド」の「コマンドで入力できる文字一覧」

ヒント

◆「＊」は使えるの？

たとえば「www.danger.com」と「XXX.danger.com」の両方をURLフィルタの対象とする場合は「＊.danger.com」と指定することで両方を対象にできます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

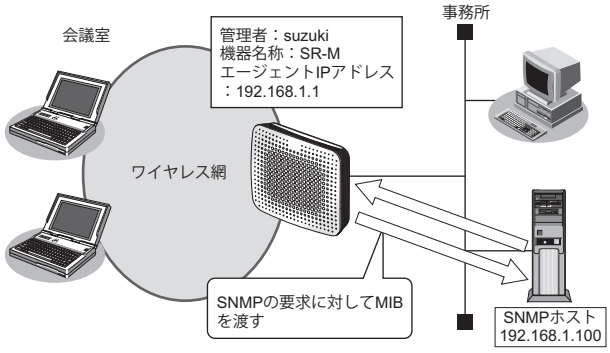
● コマンド

```
URL の情報を設定する
# proxydns domain 0 any www.danger.com any reject
# proxydns domain 1 any * any static 100.100.100.100

設定終了
# save
# commit
```

9　SNMP エージェント機能を使う

適用機種　***SR-M50AP1***

本装置は、SNMP（Simple Network Management Protocol）エージェント機能をサポートしています。
ここでは、SNMP ホストに対して MIB 情報を通知する場合の設定方法を説明します。



参照　マニュアル「機能説明書」

ヒント

◆ SNMP とは？

SNMP（Simple Network Management Protocol）は、ネットワーク管理用のプロトコルです。SNMP ホストは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMP エージェントは、SNMP ホストの要求に対して MIB（Management Information Base）という管理情報を返します。

また、特定の情報についてはトラップという機能を用いて、SNMP エージェントから SNMP ホストに対して非同期通知を行うことができます。

参照　マニュアル「仕様一覧」

こんな事に気をつけて

- エージェントアドレスには、本装置に設定されたどれかのインタフェースの IP アドレスを設定します。
  誤った IP アドレスを設定した場合は、SNMP ホストとの通信ができなくなります。
- 認証プロトコルとパスワード、暗号プロトコルとパスワードは、SNMP ホストの設定と同じ設定にします。誤ったプロトコルとパスワードを設定した場合は、SNMP ホストとの通信ができなくなります。
- SNMPv3 での認証／暗号プロトコルを使用する場合、snmp 設定反映時の認証／暗号鍵生成に時間がかかります。
  このとき、セッション監視タイムアウトが発生するなど、ほかの処理に影響する可能性があります。
- SNMPv3 で使用される snmpEngineBoots 値は、装置再起動時に初期化（初期値：1）されます。そのため、MIB 情報取得中に装置が再起動されると、SNMP ホストによっては継続した MIB 情報の取得ができないことがあります。

SNMPv1 または SNMPv2c でアクセスする場合の情報を設定する

SNMPv1 または SNMPv2c でアクセスする場合は、以下の情報を設定します。

● 設定条件

- SNMP エージェント機能を使用する
- 管理者　：suzuki
- 機器名称　：SR-M
- 機器設置場所　：1F（1 階）
- エージェントアドレス　：192.168.1.1（自装置 IP アドレス）
- SNMP ホストアドレス　：192.168.1.100
- コミュニティ名　：public00

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname SR-M
# snmp agent location 1F
# snmp agent address 192.168.1.1

SNMP ホスト情報を設定する
# snmp manager 0 192.168.1.100 public00 off disable

SNMP エージェント機能を使用する
# snmp service on

設定終了
# save
# commit
```

SNMPv3 でアクセスする場合の情報を設定する

SNMPv3 でアクセスする場合は、以下の情報を設定します。

● 設定条件

- SNMP エージェント機能を使用する
- 管理者　：suzuki
- 機器名称　：SR-M
- 機器設置場所　：1F（1 階）
- エージェントアドレス　：192.168.1.1（自装置 IP アドレス）
- SNMP ホストアドレス　：192.168.1.100
- トラップ通知ホストアドレス　：192.168.1.100
- ユーザ名　：user00
- 認証プロトコル　：MD5
- パスワード　：auth_password
- 暗号プロトコル　：DES

- パスワード　　：priv_password
- MIB ビュー　　：MIB 読み出しは system、interfaces グループのみ許可。
  トラップ通知は linkDown、linkUp トラップのみ許可。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname SR-M
# snmp agent location 1F
# snmp agent address 192.168.1.1

SNMPv3 情報を設定する
# snmp user 0 name user00
# snmp user 0 address 0 192.168.1.100
# snmp user 0 notification 0 192.168.1.100

認証・暗号プロトコルを設定する
# snmp user 0 auth md5 auth_password
# snmp user 0 priv des priv_password

MIB ビュー情報を設定する
# snmp user 0 read view 0
# snmp user 0 notify view 0
# snmp view 0 subtree 0 include system
# snmp view 0 subtree 1 include interfaces
# snmp view 0 subtree 2 include linkdown
# snmp view 0 subtree 3 include linkup

SNMP エージェント機能を使用する
# snmp service on

設定終了
# save
# commit
```

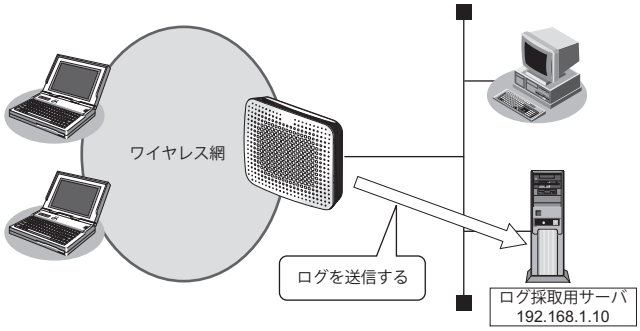
10　システムログを採取する

適用機種　***SR-M50AP1***

本装置では、各種システムログ（回線の接続／切断など）をネットワーク上のシステムログサーバに送信することができます。また、セキュリティログとして以下のログを採取することができます。

- IDS（検知した不正パケット）
- URL フィルタ（遮断したパケット）

ここでは、システムログを採取する場合の設定方法を説明します。



● 設定条件

- 以下のプライオリティを設定する
  - プライオリティ LOG_ERROR
  - プライオリティ LOG_WARNING
  - プライオリティ LOG_NOTICE
  - プライオリティ LOG_INFO
- 以下のセキュリティログを採取する
  - IDS
  - Proxy DNS
- ログ受信用サーバの IP アドレス　：192.168.1.10

上記の設定条件に従ってシステムログを採取する場合のコマンド例を示します。

● コマンド

```
# syslog server 0 address 192.168.1.10

システムログを設定する
# syslog pri error,warn,notice,info
# syslog security ids,proxydns

設定終了
# save
# commit
```

採取したシステムログを確認する

採取したシステムログの確認方法は、お使いのサーバによって異なります。

11　スケジュール機能を使う

適用機種　***SR-M50AP1***

本装置のスケジュール機能は、以下のとおりです。

- 構成定義情報切り替え予約
  本装置は、内部に２つ構成定義情報を持つことができます。運用構成の変更に備え、あらかじめ構成定義情報を用意し、指定した日時に新しい構成定義に切り替えることができます。

こんな事に気をつけて

設定前に本装置の内部時刻を正しくセットしてください。

☛参照　マニュアル「コマンドユーザーズガイド」

11.1　構成定義情報の切り替えを予約する

適用機種　***SR-M50AP1***

本装置は、内部に構成定義情報を２つ持つことができます。

ここでは、2016年1月1日6時30分に構成定義情報を構成定義情報１から構成定義情報２に切り替える場合の設定方法を説明します。

● 設定条件

- 実行日時　　：2016年4月1日　6時30分
- 構成定義情報切り替え　　：構成定義情報１の構成定義情報→構成定義情報２の構成定義情報

上記の設定条件に従って構成定義情報を切り替える場合のコマンド例を示します。

● コマンド

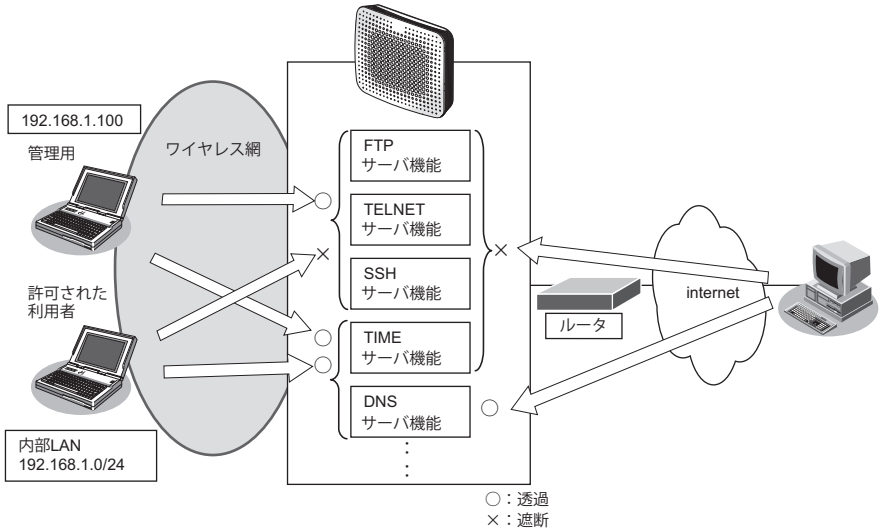
```
構成定義を切り替える
# addact 0 1604010630 reset config2

設定終了
# save
# commit
```

12　アプリケーションフィルタ機能を使う

適用機種　***SR-M50AP1***

本装置上で動作する各サーバ機能に対してアクセス制限を行うことができます。

これにより、装置をメンテナンスまたは装置のサーバ機能を使用する端末を限定し、セキュリティを向上させることができます。



ここでは、アプリケーションフィルタを利用して各サーバ機能へのアクセスを制限する場合の設定方法を説明します。

● 設定条件

- 管理用のホスト（192.168.1.100）からだけ TELNET/FTP/SSH サーバ機能へのアクセスを許可する
- 内部 LAN のホスト（192.168.1.0/24）からだけ TIME サーバ機能へのアクセスを許可する
- その他のサーバ機能は制限しない

こんな事に気をつけて

IP フィルタリングにより自装置へのパケットを遮断している場合、アプリケーションフィルタで許可する設定を行っていてもアクセスはできません。

上記の設定条件に従ってアプリケーションフィルタを設定する場合のコマンド例を示します。

● コマンド

```
制限するサーバ機能に対し、デフォルトのアクセスを遮断する
# serverinfo ftp filter default reject
# serverinfo telnet filter default reject
# serverinfo ssh filter default reject
# serverinfo time filter default reject

管理用のホストからのFTP/TELNET/SSHサーバ機能へのアクセスを許可する
# acl 0 ip 192.168.1.100/32 any any any
# serverinfo ftp filter 0 accept acl 0
# serverinfo telnet filter 0 accept acl 0
# serverinfo ssh filter 0 accept acl 0

内部LANのホストからのTIMEサーバ機能へのアクセスを許可する
# acl 1 ip 192.168.1.0/24 any any any
# serverinfo time filter 0 accept acl 1

設定終了
# save
# commit
```

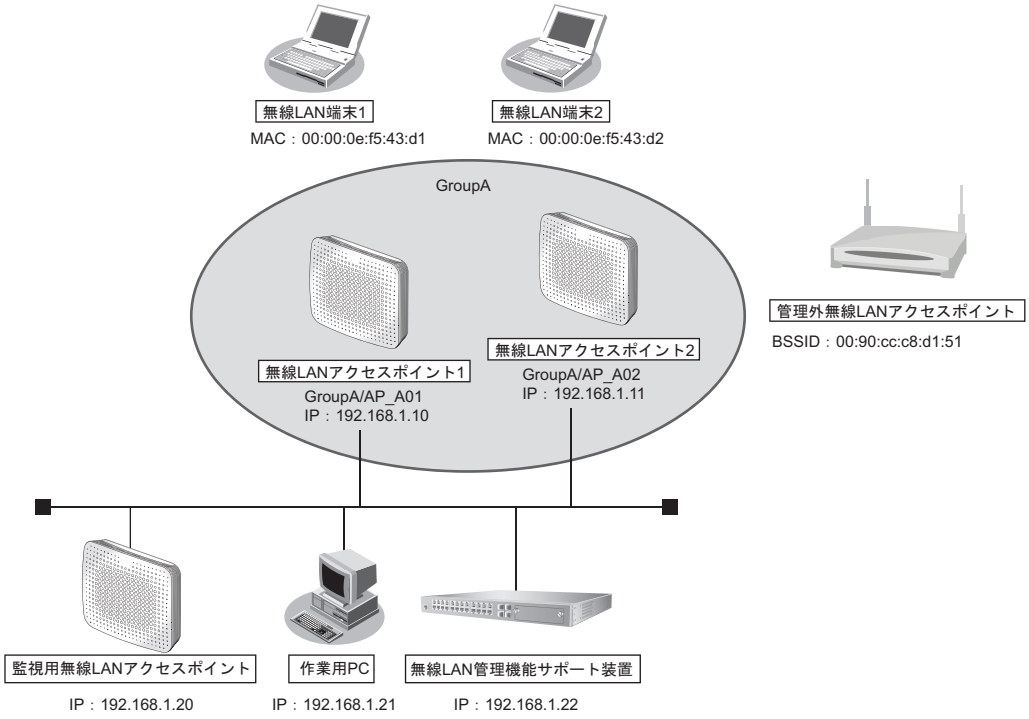
13　無線 LAN 管理機能を使う

適用機種　*SR-M50AP1*

13.1　無線 LAN 管理機能の環境を設定する

適用機種　*SR-M50AP1*

ここでは、複数の無線 LAN アクセスポイントによって構成されたネットワークを無線 LAN 管理機能で管理する場合の設定方法を説明します。



補足　無線 LAN の監視を実施する場合は、1 台以上の無線 LAN アクセスポイントを監視用に設定してください。

無線 LAN 管理機能で監視できる無線 LAN のチャネルは、周辺アクセスポイント検出機能の設定に依存します。周辺アクセスポイント検出機能の設定方法は、「1.16 監視専用装置として周辺アクセスポイント検出機能を使う」（P.53）を参照してください。

監視用無線 LAN アクセスポイントの無線 LAN モジュールは、監視する無線 LAN のチャネルによってその稼動を選択することができます。無線 LAN モジュールの設定方法は、「1.1 無線 LAN を構築する」（P.8）を参照してください。

こんな事に気をつけて

- 管理機器のログイン時の入力プロンプトは、システムデフォルト（Login:）のままとしてください。
  管理機器のログイン時の入力プロンプトを変更した場合、無線LAN管理機能の動作は不定となります。
- 無線LANアクセスポイントを管理機器として動作させるには、無線LANアクセスポイントで以下のコマンドを設定する必要があります。コマンド設定により無線LAN管理機能からのリモートログインが可能となります（コマンドの詳細は、マニュアル「コマンドリファレンス」の「無線LAN管理 ログイン情報」を参照してください）。

  ```
  # nodemanager login service enable
  ```

  なお、管理機器のセキュリティを確保するために、以下のコマンドでユーザ：nodemgrのパスワードを設定することを推奨します（コマンドの詳細は、マニュアル「コマンドリファレンス」の「パスワード情報」を参照してください）。

  ```
  # password nodemgr set <password>
  ```

- 無線LAN管理機能で、「アクセスポイントモニタリング機能」「電波出力自動調整機能」「チャネル自動調整機能」を使用する場合は、無線LANアクセスポイントで以下のコマンドを設定する必要があります（コマンドの詳細は、マニュアル「コマンドリファレンス」の「無線LANモジュール情報」を参照してください）。

  ```
  # ieee80211 <number> apscan mode enable
  ```

- 管理機器でユーザ：nodemgrのパスワード情報を設定した場合、無線LAN管理機器側の情報も同時に設定するようにしてください。
- ログインは1セッションのみです。そのため、管理されるアクセスポイント側にログインしていない必要があります。

● 設定条件

- 無線LAN管理対象
  管理グループ
  　グループ名　：GroupA
  無線LANアクセスポイント1
  　管理機器名　：AP_A01
  　IPアドレス　：192.168.1.10
  　アカウント　：ユーザID：nodemgr、パスワード：nodemgr1
  無線LANアクセスポイント2
  　管理機器名　：AP_A02
  　IPアドレス　：192.168.1.11
  　アカウント　：ユーザID：nodemgr、パスワード：nodemgr2
- 監視用無線LANアクセスポイント
  周辺アクセスポイント検出機能をスキャン専用モードで運用
  使用する無線LANモジュール　：ieee80211 1、ieee80211 2
  　管理機器名　：Watcher
  　IPアドレス　：192.168.1.20
  　監視用アカウント　：ユーザID：nodemgr、パスワード：nodemgr3
- 管理外無線LANアクセスポイント
  　MACアドレス　：00:90:cc:c8:d1:51
- アクセスポイント情報取得の時間パラメタ（アクセスポイントモニタリング用）
  情報取得間隔　：10秒
  情報取得待機間隔　：10秒
  情報取得タイムアウト時間　：5秒
- 監視のパラメタ（アクセスポイントモニタリング用）
  有線LAN
  　稼動監視間隔　：10秒
  　稼動監視待機間隔　：10秒
  　稼動監視タイムアウト時間　：5秒
  　稼動監視 通信異常判定しきい値　：6回

無線LAN
　スキャンレポート取得間隔　　：10秒
　スキャンレポート取得待機間隔　　：10秒
　スキャンレポート取得タイムアウト時間　　：1分
　無線LAN監視 通信異常判定しきい値　　：6回

- 監視ログのパラメタ（アクセスポイントモニタリング／クライアントモニタリング用）
  監視ログ保持件数　　：100件
- 無線LAN端末のRSSI監視のパラメタ（クライアントモニタリング用）
  RSSI評価母数　　：10個
  RSSI最低しきい値　　：20

上記の設定条件に従って設定を行う場合のコマンド例を示します。

無線LANアクセスポイント1の設定

● コマンド

```
nodemgrアカウントを有効にし、パスワードを設定する
# password nodemgr set nodemgr1
# nodemanager login service enable

設定終了
# save
# commit
```

無線LANアクセスポイント2の設定

● コマンド

```
nodemgrアカウントを有効にし、パスワードを設定する
# password nodemgr set nodemgr2
# nodemanager login service enable

設定終了
# save
# commit
```

監視用無線LANアクセスポイントの設定

● コマンド

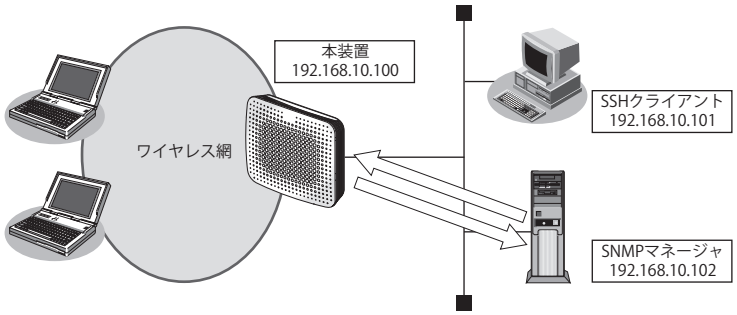
```
nodemgrアカウントを有効にし、パスワードを設定する
# password nodemgr set nodemgr3
# nodemanager login service enable

設定終了
# save
# commit
```

14　装置を保護する

適用機種　***SR-M50AP1***

本装置に対するセキュリティ対策として、以下の設定を行います。

- 管理者 (admin) 用パスワードの設定
- 自動切断（オートログアウト）の設定
- Telnet/SSH および SNMP 接続に対するアクセス制限
- 不要なサービスの停止



● 設定条件

本装置に対するセキュリティ対策として、以下の設定を行います。

- 管理者 (admin) パスワードの設定　：srm_admin-2022
- IP アドレス　：192.168.10.100
- 自動切断（オートログアウト）の設定
  （ログインしたままの状態で指定時間無操作だった際に、自動切断を行う）
  コンソールのオートログアウト時間
  ：5 分
  SSH のオートログアウト時間　：5 分
- SNMP 設定
  アクセス許可する SNMP マネージャ
  ：192.168.10.102
  コミュニティ名　：private
  マネージャからの書き込み　：許可しない
- SSH 接続を許可するホストの IP アドレス
  ：192.168.10.101
- Telnet 接続　：禁止
- 不要なサーバ機能はすべて停止
  # serverinfo < サーバ機能名 > ip off

● コマンド

```
adminパスワードをsrm_admin-2022に設定
# password admin set srm_admin-2022

コンソール接続のオートログアウト時間を5分に設定
# consoleinfo autologout 5m

SSHのオートログアウトまでの無操作時間を5分に設定
# telnetinfo autologout 5m

自装置IPアドレスとVLANの設定
# lan 0 ip address 192.168.10.100/24 3
# lan 0 vlan 1

SNMPを有効、コミュニティ名をprivate、書き込み許可しない
# snmp service on
# snmp manager 0 192.168.10.102 private v1 disable

許可するホストからのSSH接続のみ許可する
# acl 0 ip 192.168.10.101/32 any any any
# serverinfo ssh filter 0 accept acl 0
# serverinfo ssh filter default reject

不要なサーバ機能はすべて停止
# serverinfo telnet ip off
# serverinfo ftp ip off
# serverinfo sftp ip off
# serverinfo http ip off
# serverinfo sntp ip off
# serverinfo time ip tcp off
# serverinfo time ip udp off

設定終了
# save
# commit
```

索引

ほ

ま

む

ゆ

り

SR-M　コマンド設定事例集

P3NK-5502-03Z0

発行日　　2023年5月

発行責任　　富士通株式会社