

FUJITSU Network SR-M コマンド設定事例集

V02

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。

2010年 4月初版
2013年 7月第2版
2014年 8月第3版

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。
従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。
Microsoft Corporationのガイドラインに従って画面写真を使用しています。
Copyright FUJITSU LIMITED 2010 - 2014

目次

| | |
|--|----|
| はじめに | 2 |
| 本書の使いかた | 5 |
| 本書の読者と前提知識 | 5 |
| 本書における商標の表記について | 6 |
| 本装置のマニュアルの構成 | 7 |
| 1 無線 LAN 機能を使う (SR-M20AP1 / 20AP2) | 8 |
| 1.1 無線 LAN ネットワークを構築する | 8 |
| 1.2 無線 LAN ネットワークを構築する (IEEE802.11n) | 10 |
| 1.3 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 | 12 |
| 1.4 IEEE802.1X 認証および MAC アドレス認証により VLAN を管理する | 17 |
| 1.5 同一 SSID の複数アクセスポイントを構築する | 22 |
| 1.6 端末台数制限機能を使う | 25 |
| 1.7 端末台数最低保証機能を使う | 27 |
| 1.8 WDS ブリッジ機能を使う | 29 |
| 1.9 VLAN ネットワークを WDS ブリッジ機能で接続する | 34 |
| 1.10 MAC アドレスフィルタリング機能を使う | 39 |
| 1.11 WMM 機能を使う | 41 |
| 1.12 WMM 機能の Access Category 分類条件を変更する | 43 |
| 1.13 周辺アクセスポイント検出機能を使う | 46 |
| 1.14 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 | 48 |
| 1.15 IEEE802.11n チャンネルボンディング機能を使う | 50 |
| 2 無線 LAN 機能を使う (SR-M20AC1 / 20AC2) | 52 |
| 2.1 無線 LAN ネットワークを構築する | 52 |
| 2.2 無線 LAN ネットワークを構築する (IEEE802.11n) | 54 |
| 2.3 無線 LAN ネットワークで認証・暗号化する | 56 |
| 2.3.1 OPEN 認証 IEEE802.1X 連携 EAP-MD5 認証 | 56 |
| 2.3.2 SHARED 認証 IEEE802.1X 連携 EAP-MD5 認証 | 57 |
| 2.3.3 WPA 事前共有キー (PSK) 認証 | 57 |
| 2.3.4 WPA IEEE802.1X 連携 EAP-TLS 認証 | 58 |
| 2.3.5 WPA IEEE802.1X 連携 EAP-TTLS 認証 | 62 |
| 2.3.6 WPA IEEE802.1X 連携 EAP-PEAP 認証 | 63 |
| 2.4 無線 LAN 中継機能を使う | 65 |
| 2.5 ローミング機能を使う | 66 |
| 2.6 WMM 機能を使う | 68 |
| 2.7 WMM 機能の Access Category 分類条件を変更する | 70 |
| 2.8 IEEE802.11n チャンネルボンディング機能を使う | 72 |
| 3 VLAN 機能を使う | 74 |
| 3.1 ポート VLAN 機能を使う | 74 |
| 3.2 タグ VLAN 機能を使う | 75 |
| 4 バックアップポート機能を使う | 76 |
| 5 リンクインテグリティ機能を使う | 77 |
| 5.1 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 | 78 |
| 6 フィルタリング機能を使う | 79 |
| 6.1 特定サービスへのアクセスだけを許可する | 81 |
| 6.2 特定サーバへのアクセスだけを禁止して SPI を併用する | 83 |
| 6.3 特定の MAC アドレス間の通信だけを禁止する | 84 |
| 7 IEEE802.1X 認証機能を使う | 85 |
| 7.1 無線 LAN で IEEE802.1X 認証機能を使う | 86 |
| 7.2 認証自動切替機能を使う | 89 |
| 7.3 有線 LAN で IEEE802.1X 認証機能を使う | 92 |
| 7.4 IEEE802.1X 認証機能を設定したポートに Wake On LAN パケットを転送する | 93 |

| | | |
|-----------------|--|------------|
| 8 | MAC アドレス認証機能を使う | 95 |
| 8.1 | 無線 LAN で MAC アドレス認証機能を使う | 95 |
| 8.2 | 有線 LAN で MAC アドレス認証機能を使う | 98 |
| 8.3 | MAC アドレス認証機能を設定したポートに Wake On LAN パケットを転送する | 99 |
| 9 | DHCP 機能を使う | 101 |
| 9.1 | DHCP クライアント機能を使う | 101 |
| 10 | DNS サーバ機能を使う (ProxyDNS) | 104 |
| 10.1 | DNS サーバの自動切り替え機能 (順引き) を使う | 104 |
| 10.2 | DNS サーバの自動切り替え機能 (逆引き) を使う | 106 |
| 10.3 | DNS 問い合わせタイプフィルタ機能を使う | 107 |
| 10.4 | DNS サーバ機能を使う | 108 |
| 11 | 特定の URL へのアクセスを禁止する (URL フィルタ機能) | 110 |
| 12 | SNMP エージェント機能を使う | 112 |
| 13 | システムログを採取する | 115 |
| 14 | スケジュール機能を使う | 116 |
| 14.1 | 構成定義情報の切り替えを予約する | 116 |
| 15 | アプリケーションフィルタ機能を使う | 117 |
| 16 | 無線 LAN 管理機能を使う | 119 |
| 16.1 | 無線 LAN 管理機能の環境を設定する | 119 |
| 16.2 | アクセスポイントモニタリングを行う | 123 |
| 16.3 | クライアントモニタリングを行う | 124 |
| 16.4 | 無線 LAN アクセスポイントに MAC アドレスフィルタを配布する (MAC アドレスフィルタ配布) | 125 |
| 16.5 | 無線 LAN アクセスポイントの電波出力を調整する (電波出力自動調整) | 126 |
| 16.6 | 無線 LAN アクセスポイントの無線 LAN チャンネルを調整する | 128 |
| 索引 | | 129 |

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。

また、CD-ROM 中の README ファイルには大切な情報が記載されていますので、併せてお読みください。

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。



補足 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。



参照 操作方法など関連事項を説明している箇所を示します。



適用機種 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。



警告 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。



注意 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

Microsoft、MS-DOS、Windows、Windows Server および Windows Vista 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。

Adobe および Reader は、Adobe Systems Incorporated（アドビシステムズ社）の米国ならびに他の国における商標または登録商標です。

Netscape は、米国 Netscape Communications Corporation の商標です。

UNIX は、米国およびその他の国におけるオープン・グループの登録商標です。

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® XP Professional operating system | Windows XP |
| Microsoft® Windows® XP Home Edition operating system | |
| Microsoft® Windows Server® 2003, Standard Edition | Windows Server 2003 |
| Microsoft® Windows Server® 2003 R2, Standard Edition | |
| Microsoft® Windows Server® 2003, Enterprise Edition | |
| Microsoft® Windows Server® 2003 R2, Enterprise Edition | |
| Microsoft® Windows Server® 2003, Datacenter Edition | |
| Microsoft® Windows Server® 2003 R2, Datacenter Edition | |
| Microsoft® Windows Server® 2003, Web Edition | |
| Microsoft® Windows Server® 2003, Standard x64 Edition | |
| Microsoft® Windows Server® 2003 R2, Standard Edition | |
| Microsoft® Windows Server® 2003, Enterprise x64 Edition | |
| Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition | |
| Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based systems | |
| Microsoft® Windows Server® 2003, Datacenter x64 Edition | |
| Microsoft® Windows Server® 2003 R2, Datacenter x64 Edition | |
| Microsoft® Windows Vista® Ultimate operating system | Windows Vista |
| Microsoft® Windows Vista® Business operating system | |
| Microsoft® Windows Vista® Home Premium operating system | |
| Microsoft® Windows Vista® Home Basic operating system | |
| Microsoft® Windows Vista® Enterprise operating system | |
| Microsoft® Windows® 7 64bit Home Premium | Windows 7 |
| 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-M20AP1 ご利用にあたって | SR-M20AP1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。 |
| SR-M20AP2 ご利用にあたって | SR-M20AP2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。 |
| SR-M20AC1 ご利用にあたって | SR-M20AC1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。 |
| SR-M20AC2 ご利用にあたって | SR-M20AC2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。 |
| 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。 |
| コマンドユーザーズガイド | コマンドを使用して、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。 |
| 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。 |
| 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。 |
| 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-M20AP1 / 20AP2)

適用機種 SR-M20AP1, 20AP2

1.1 無線 LAN ネットワークを構築する

適用機種 SR-M20AP1, 20AP2

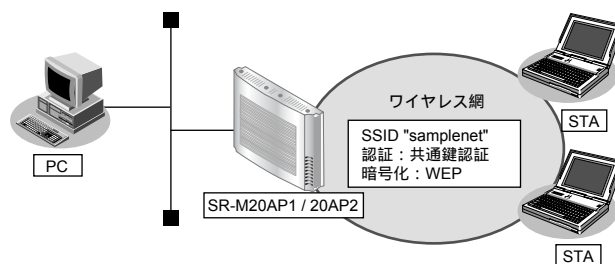
ここでは、既存の有線 LAN ネットワークを無線化する場合を例に説明します。

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つ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 SR-M20AP1 ご利用にあたって「[3.3.2 本装置をご購入時の状態に戻す](#)」(P.61)
- SR-M20AP2 ご利用にあたって「[本装置をご購入時の状態に戻す](#)」(P.72)



● 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 チャンネル : 10
- 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 10
```

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 ネットワークを構築する (IEEE802.11n)

適用機種 SR-M20AP1, 20AP2

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

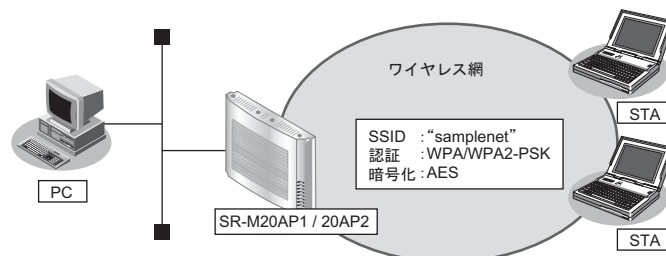
- 無線 LAN クライアントが IEEE802.11n に対応している必要があります。
- 暗号化方式として WEP および TKIP は使用できません。定義した場合は無効な設定として無線 LAN インタフェースが使用できません。
- IEEE802.11n 未対応の無線装置が同一チャンネルに存在している場合、スループットが低下する場合があります。

☛ 参照 機能説明書 「2.1.16 HT プロテクション機能」 (P31)

- 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つ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 SR-M20AP1 ご利用にあたって 「3.3.2 本装置をご購入時の状態に戻す」 (P61)

SR-M20AP2 ご利用にあたって 「本装置をご購入時の状態に戻す」 (P72)



● 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
- チャンネル : 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 "abcdefghijklmnopqrstuvwxyzyz"

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 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-M20AP1, 20AP2

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。

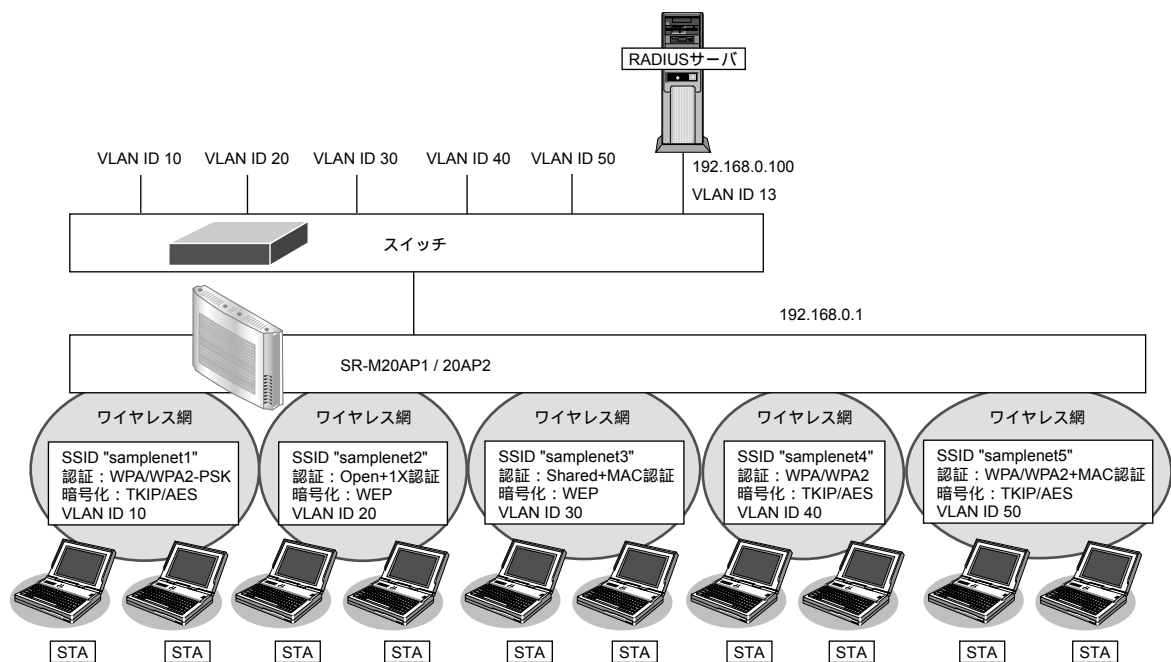
IEEE802.1X認証機能またはMACアドレス認証機能を使用すると、認証サーバを利用して、無線LANネットワークに接続する端末またはユーザが、ネットワークへのアクセス権限を持っているかを認証することもできます。

同一の無線LANネットワークをIEEE802.11b/gおよびIEEE802.11a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つ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 SR-M20AP1 ご利用にあたって「[3.3.2 本装置をご購入時の状態に戻す](#)」(P61)
- SR-M20AP2 ご利用にあたって「[本装置をご購入時の状態に戻す](#)」(P72)



● 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
- ・ チャンネル : 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
```


1.4 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-M20AP1, 20AP2

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。

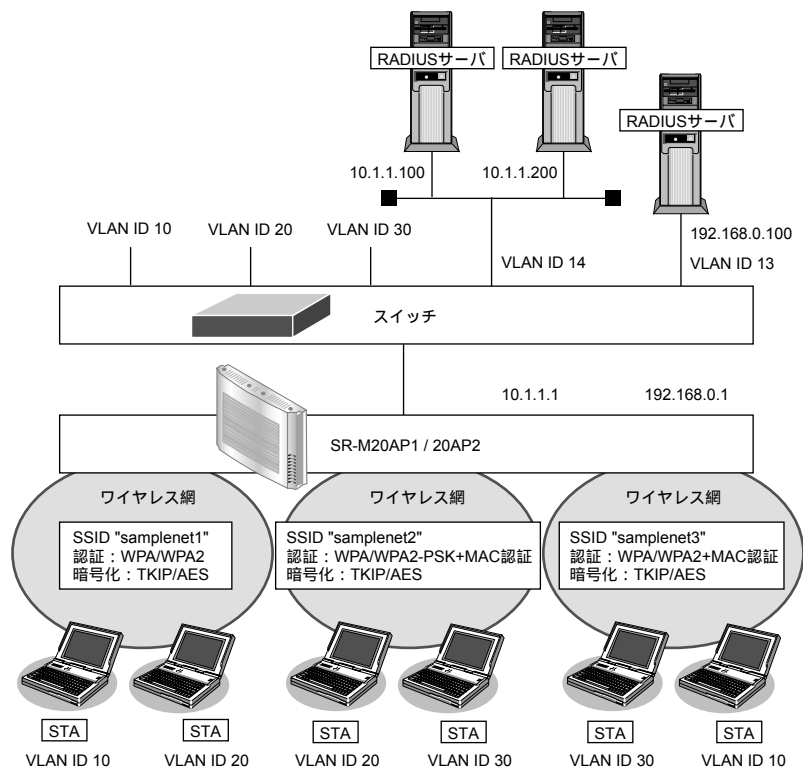
☛ 参照 機能説明書 [2.10 IEEE802.1X 認証機能] (P46)

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つ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 SR-M20AP1 ご利用にあたって [3.3.2 本装置をご購入時の状態に戻す] (P61)

SR-M20AP2 ご利用にあたって [本装置をご購入時の状態に戻す] (P72)



● 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
- チャンネル : 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 "abcdefghijklmnopqrstuvwxy"
- 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
```

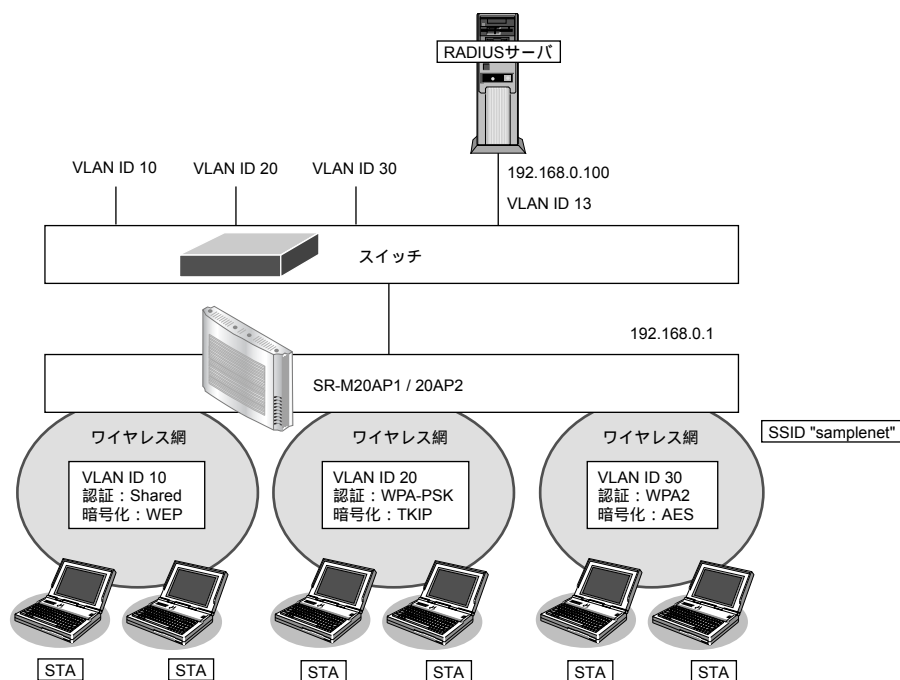
1.5 同一 SSID の複数アクセスポイントを構築する

適用機種 SR-M20AP1, 20AP2

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つ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 SR-M20AP1 ご利用にあたって「[3.3.2 本装置をご購入時の状態に戻す](#)」(P61)
SR-M20AP2 ご利用にあたって「[本装置をご購入時の状態に戻す](#)」(P72)



● 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
- チャンネル : 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 (WPA-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 : WPA-PSK
- 暗号化モード : TKIP
- 事前共有キー (PSK) : テキストで “abcdefghijklnopqrstuvwxyz”
- 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 (WPA-PSK) を設定する

```
# wlan 2 use on
# wlan 2 ssid samplenet
# wlan 2 auth wpa-psk
# wlan 2 wpa cipher tkip
# wlan 2 wpa psk text abcdefghijklmnopqrstuvwxyz
# wlan 2 vlan untag 20
# wlan 10 use on
# wlan 10 ssid samplenet
# wlan 10 auth wpa-psk
# wlan 10 wpa cipher tkip
# 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
```


1.6 端末台数制限機能を使う

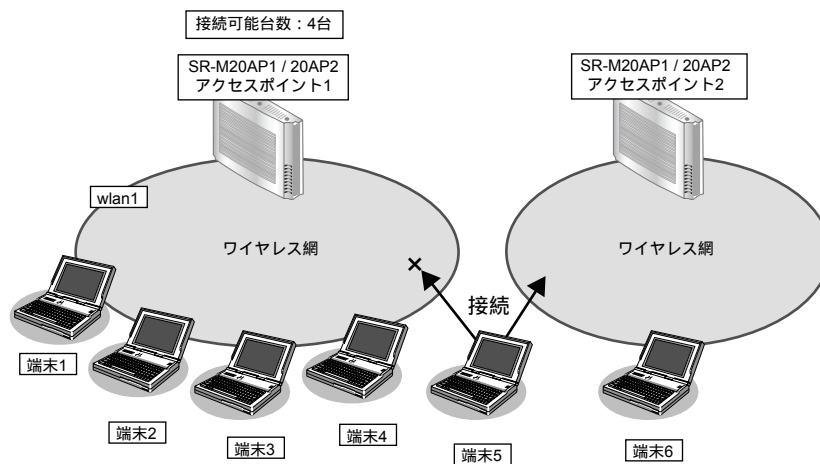
適用機種 SR-M20AP1, 20AP2

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-M20AP1 / 20AP2 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。



● 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
- チャンネル : 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
```

1.7 端末台数最低保証機能を使う

適用機種 SR-M20AP1, 20AP2

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。

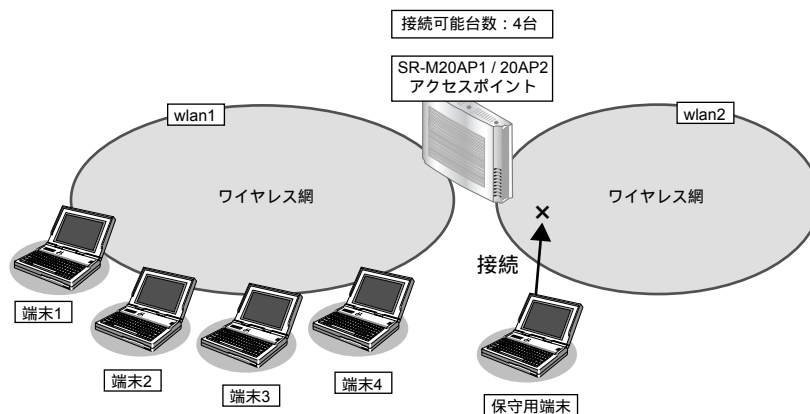
こんな事に気をつけて

- 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。

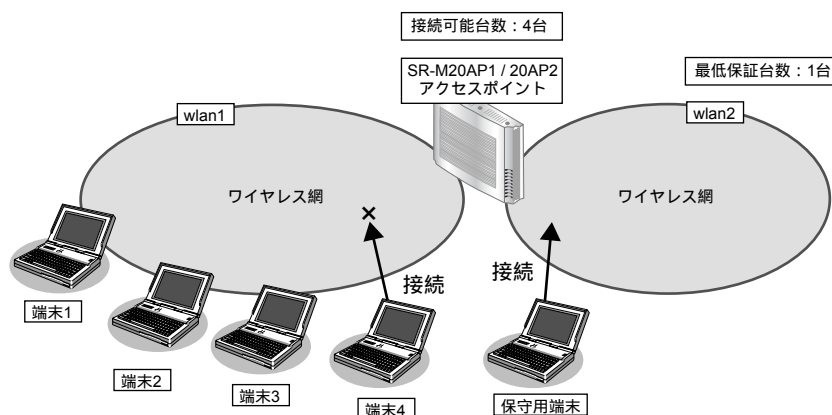
| 無線LANモジュール 接続可能台数 | | |
|-----------------------|-----------------------|----------------------|
| 仮想アクセスポイント1 最低保証台数 | 仮想アクセスポイント2 最低保証台数 | 最低保証されていない 接続可能台数 |

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-M20AP1 / 20AP2 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
- チャンネル : 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
```

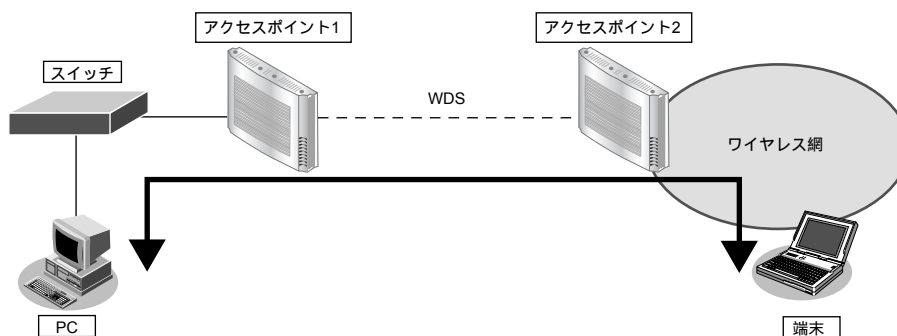
1.8 WDSブリッジ機能を使う

適用機種 SR-M20AP1, 20AP2

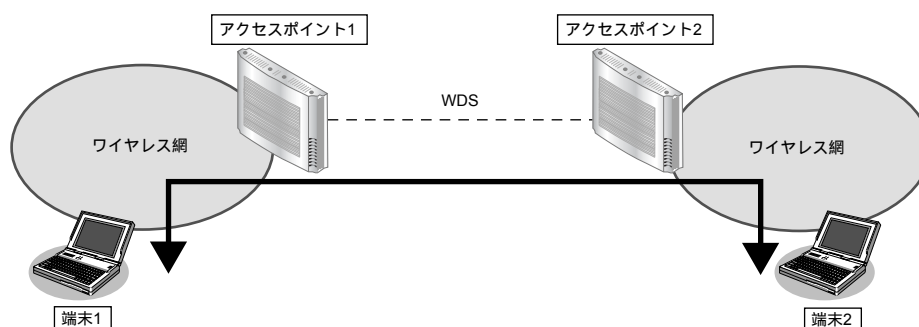
WDSブリッジとは、無線LANアクセスポイントどうしの通信を可能にする機能です。ある無線LANアクセスポイントを中継して別の無線LANアクセスポイントとデータの送受信を行うことができるため、単一の無線LANアクセスポイントを使用した場合に比べて広い範囲での通信が可能となります。

SR-M20AP1 / 20AP2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。

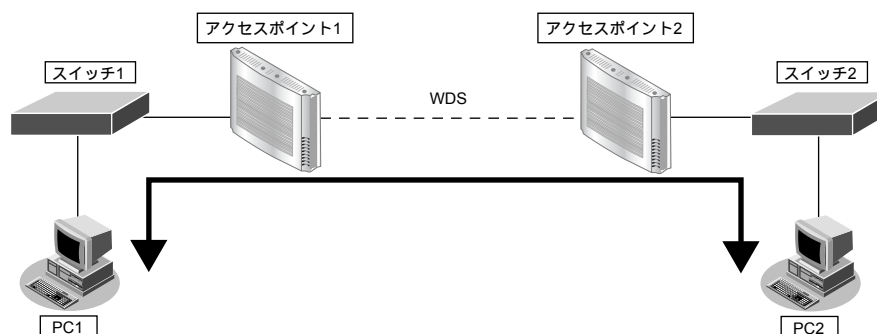
- 有線LANと無線LAN 端末間の通信



- 無線LAN 端末間の通信



- 有線LAN 間の通信

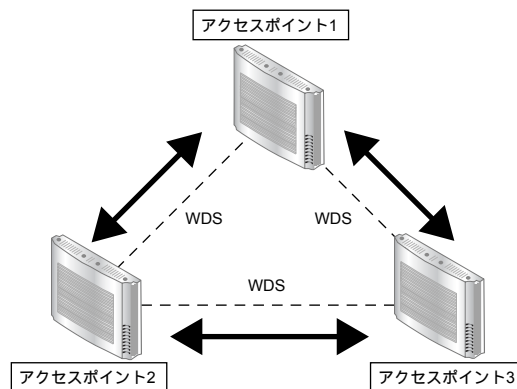


こんな事に気をつけて

- 相手無線 LAN アクセスポイントと同じチャンネル、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 以外のチャン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-M20AP1 / 20AP2 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 [コマンドリファレンス](#) 「show system information」、「show wlan status」

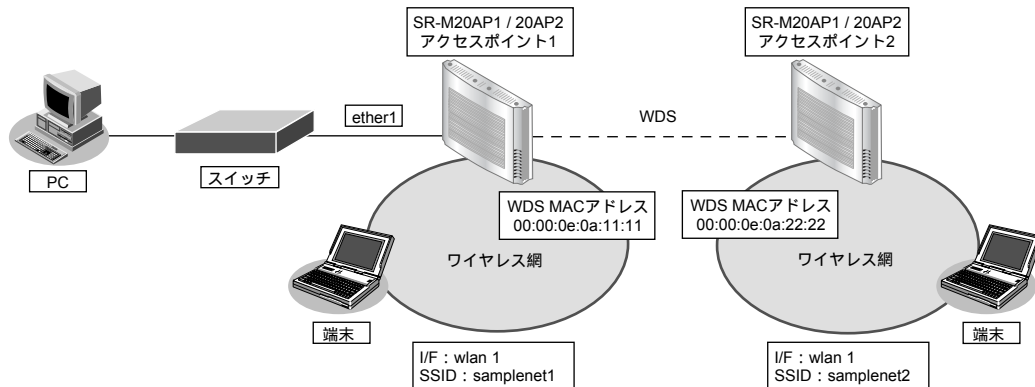
- 本機能のブリッジ処理は、同一の VLAN に割り当てられたインタフェース間でのみ行われます。WDS ブリッジ機能を使用する場合は、WDS 用のインタフェースを含み、対象のインタフェース (ether, wlan など) が同一の VLAN となるように設定してください。
- 他社の無線 LAN アクセスポイントとの接続はできません。
- WDS ブリッジを行う無線 LAN アクセスポイント間では、接続認証、接続要求などの手順は行いません。また、利用できる暗号化方式は WEP 暗号化のみです。
- 無線 LAN アクセスポイント 1 台との WDS ブリッジには、無線 LAN インタフェース 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 チャンネルが 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、チャン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ことがあります。WDS のみで運用している場合は、チャンネルの切り替えは行われません。レーダを検出したチャンネルは 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 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 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、「1.9 VLANネットワークをWDSブリッジ機能で接続する」(P34)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

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
- チャンネル : 10

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 : 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 "abcdefghijklmnopqrstuvwxy"

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インタフェース : wlan 2
- 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]**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
- チャンネル : 10

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 : 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 インタフェース : wlan 2
- 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]****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 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

```
# wlan 2 use on
# wlan 2 type wds
# wlan 2 wep mode enable
# wlan 2 wep key 1 text ABCDEFGHIJKLM
# wlan 2 wep send 1
# wlan 2 wds neighbor 00:00:0e:0a:22:22
```

設定終了

```
# save
# commit
```


[アクセスポイント2]**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 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

```
# wlan 2 use on  
# wlan 2 type wds  
# wlan 2 wep mode enable  
# wlan 2 wep key 1 text ABCDEFGHIJKLM  
# wlan 2 wep send 1  
# wlan 2 wds neighbor 00:00:0e:0a:11:11
```

設定終了

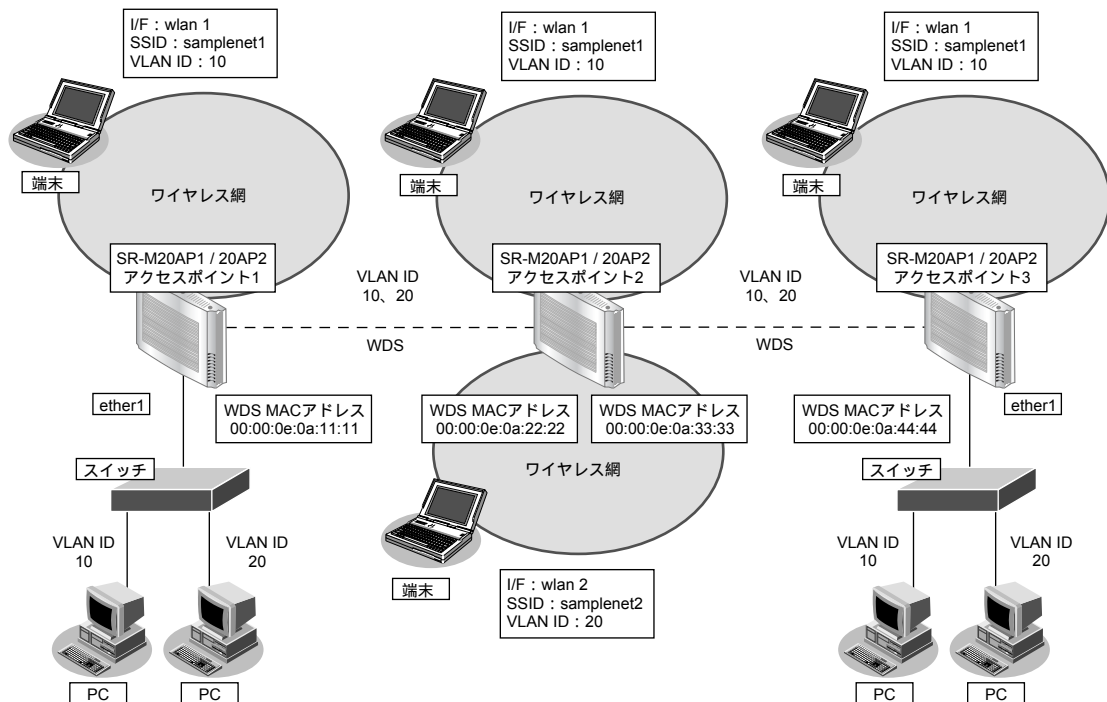
```
# save  
# commit
```

1.9 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-M20AP1, 20AP2

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-M20AP1 / 20AP2 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

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
- チャンネル : 10

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 : 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 "abcdefghijklmnopqrstuvwxy"
- 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 インタフェース : wlan 2
- 暗号化モード : WEP
- WEP キー : テキストで "ABCDEFGHJKLMN"
- 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]**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
- チャンネル : 10

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 "abcdefghijklmnopqrstuvwxy"
- 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 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 "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 インタフェース : wlan 3
- 暗号化モード : WEP
- WEP キー : テキストで "ABCDEFGHJKLMN"
- 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 インタフェース : wlan 4
- 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

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
- チャンネル : 10

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 : 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 "abcdefghijklmnopqrstuvwxyx"
- 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 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: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
```

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 samplenet1
# wlan 1 auth wpa/wpa2-psk
# wlan 1 wpa cipher auto
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyx
# wlan 1 vlan untag 10
```

WDS 用の無線 LAN インタフェースを設定する

```
# wlan 2 use on
# wlan 2 type wds
# wlan 2 wep mode enable
# wlan 2 wep key 1 text ABCDEFGHIJKLM
# wlan 2 wep send 1
```

```
# wlan 2 wds neighbor 00:00:0e:0a:22:22
# wlan 2 vlan tag 10,20
```

```
設定終了
# save
# commit
```

【アクセスポイント2】

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 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
# wlan 1 vlan untag 10
```

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 zyxwvutsrqponmlkjihgfedcba
# wlan 2 vlan untag 20
```

WDS 用の無線 LAN インタフェース 1 を設定する

```
# wlan 3 use on
# wlan 3 type wds
# wlan 3 wep mode enable
# wlan 3 wep key 1 text ABCDEFGHIJKLM
# wlan 3 wep send 1
# wlan 3 wds neighbor 00:00:0e:0a:11:11
# wlan 3 vlan tag 10,20
```

WDS 用の無線 LAN インタフェース 2 を設定する

```
# wlan 4 use on
# wlan 4 type wds
# wlan 4 wep mode enable
# wlan 4 wep key 1 text ZYXWVUTSRQPON
# wlan 4 wep send 1
# wlan 4 wds neighbor 00:00:0e:0a:44:44
# wlan 4 vlan tag 10,20
```

```
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
```

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 samplenet1
```

```
# wlan 1 auth wpa/wpa2-psk
```

```
# wlan 1 wpa cipher auto
```

```
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz
```

```
# wlan 1 vlan untag 10
```

WDS用の無線 LAN インタフェースを設定する

```
# 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:33:33
```

```
# wlan 2 vlan tag 10,20
```

設定終了

```
# save
```

```
# commit
```

1.10 MAC アドレスフィルタリング機能を使う

適用機種 SR-M20AP1, 20AP2

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。

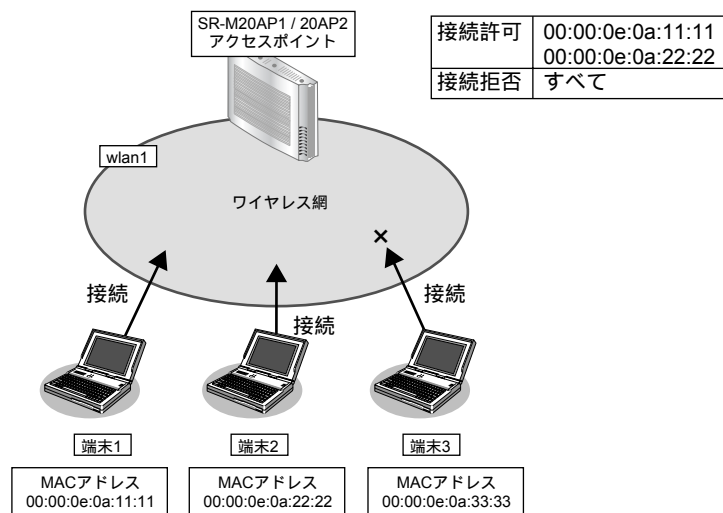
SR-M20AP1 / 20AP2 では、送信元 MAC アドレス（無線 LAN 端末の MAC アドレス）のみをフィルタリングの対象とします。

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
- チャンネル : 10

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 "abcdefghijklmnopqrstuvwxy"
- 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 10
```

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
```


1.11 WMM 機能を使う

適用機種 SR-M20AP1, 20AP2

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。

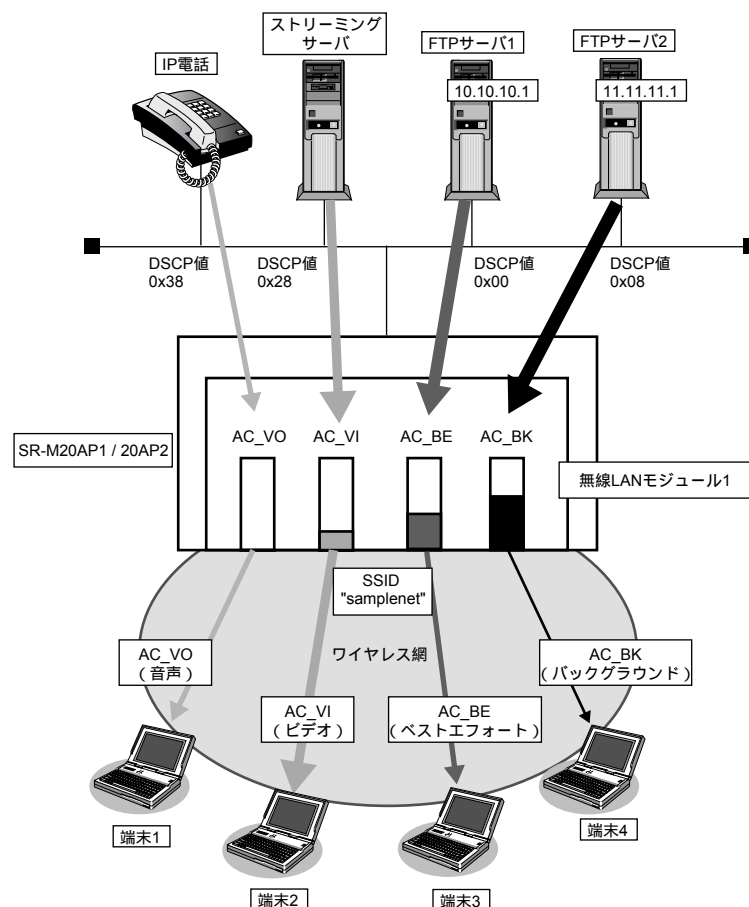
無線に送出するパケットは IP パケットの DSCP 値を元に、4 種類の Access Category (AC) に分類されます。AC は優先度が高い方から、AC_VO (音声)、AC_VI (ビデオ)、AC_BE (ベストエフォート)、AC_BK (バックグラウンド) であり、AC ごとに送信キューを持ちます。送信キューにパケットがたまっている場合は、優先度の低い AC より優先度の高い AC の送信キューから優先的にパケットが送出されます。

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
- チャンネル : 10
- 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 10
```

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
```

1.12 WMM機能の Access Category 分類条件を変更する

適用機種 SR-M20AP1, 20AP2

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、「[1.11 WMM機能を使う](#)」(P41) 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

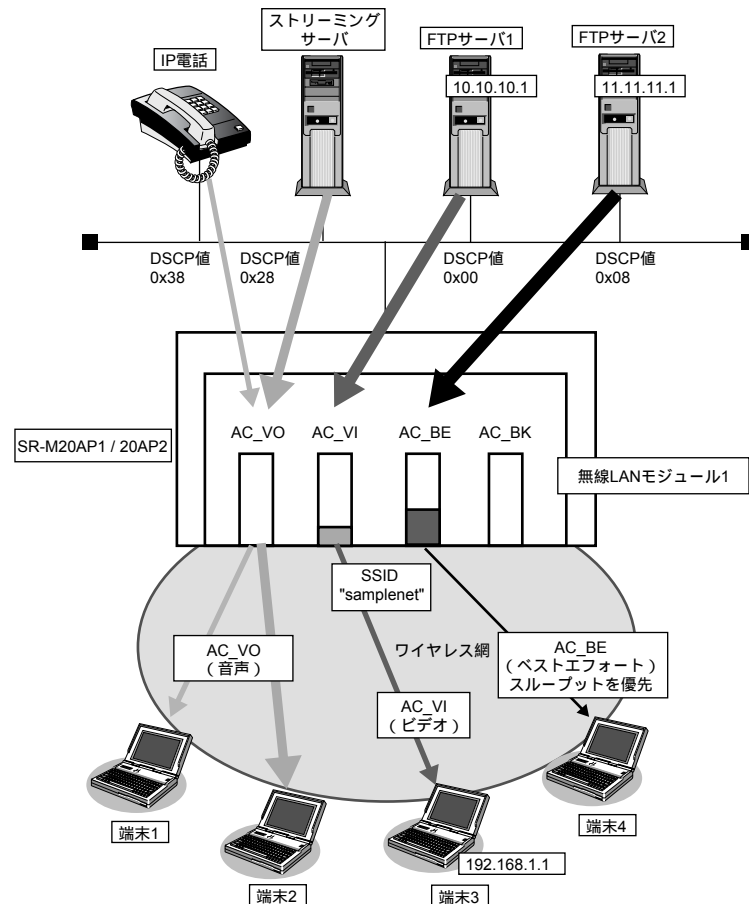
ここでは、以下の場合を例に説明します。

- 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、スルーブットを優先する

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 |



● 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
- チャンネル : 10
- 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 "abcdefghijklmnopqrstuvwxy"
- 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 10
```

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
```

1.13 周辺アクセスポイント検出機能を使う

適用機種 SR-M20AP1, 20AP2

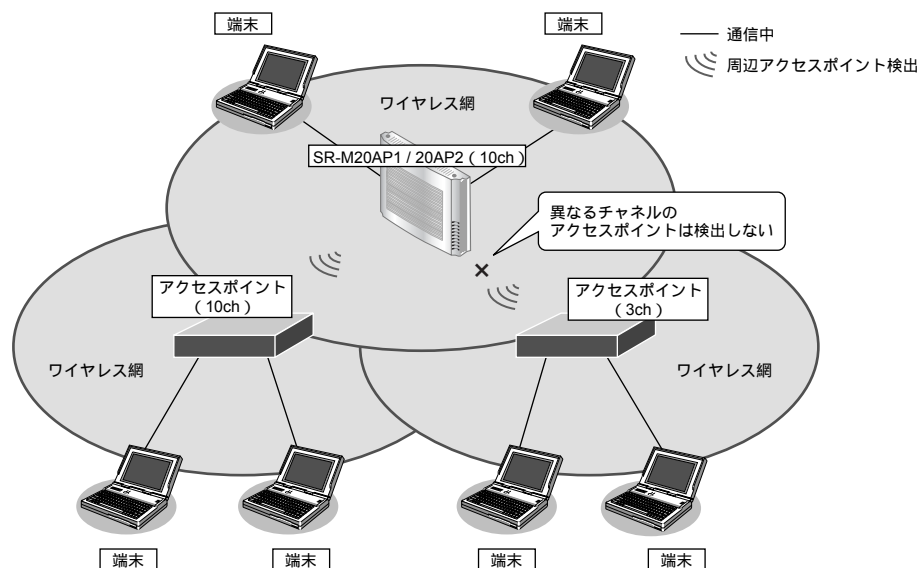
無線 LAN アクセスポイントの運用をしながら無線電波を検出することで、SR-M20AP1 / 20AP2 周辺の無線 LAN アクセスポイントを検出することができます。周辺アクセスポイントの検出は現在運用中のチャンネルだけで行います。

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 [コマンドリファレンス](#) 「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ン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
- チャンネル : 10
- 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 "abcdefghijklmnopqrstuvwxyzz"

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
```

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
```

1.14 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-M20AP1, 20AP2

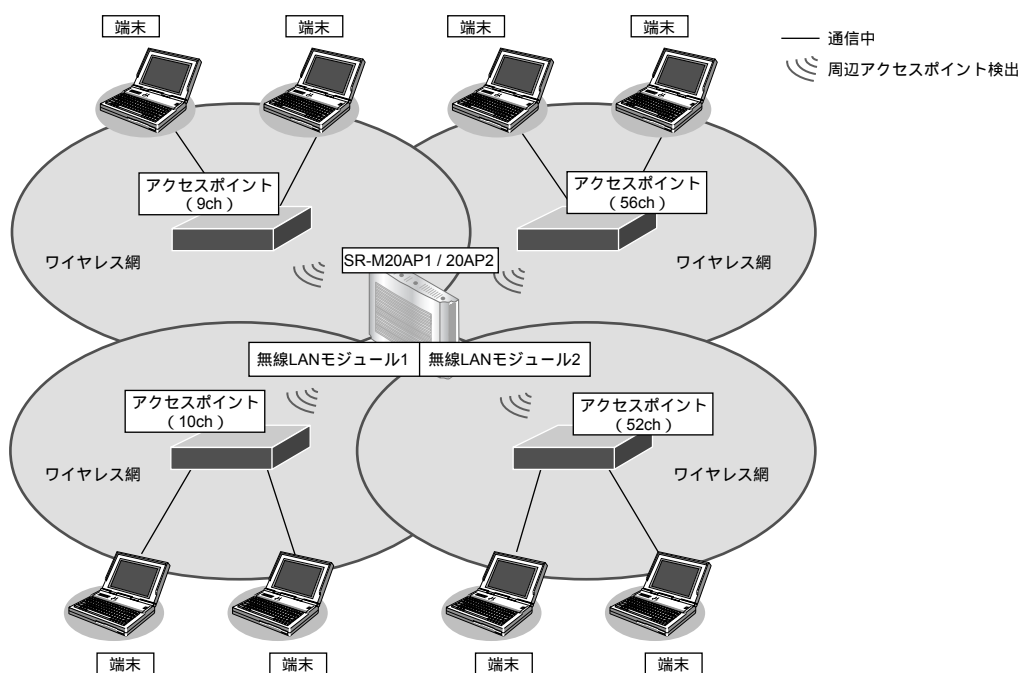
無線 LAN アクセスポイントの運用をしないで検出だけを行います。SR-M20AP1 / 20AP2 周辺の無線 LAN アクセスポイントを無線 LAN モジュールで利用可能なすべてのチャンネルで検出することができます。

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 [コマンドリファレンス](#) 「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ン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
```

1.15 IEEE802.11n チャンネルボンディング機能を使う

適用機種 SR-M20AP1, 20AP2

チャンネルボンディングとは、隣り合った2つのチャン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

- チャン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ンネルボンディングを有効にする必要があります。
- セカンダリチャンネルに他BSSのプライマリチャンネルが存在する場合は、自動的に20MHz幅のBSSを開始します。
- 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チャンネルが1つしか確保できないことに加え、ほかのチャンネルとの干渉が発生しやすいため、チャンネルボンディングは5GHz帯での使用を推奨します。

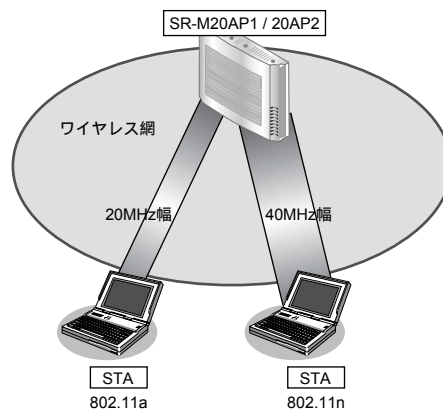
チャンネルボンディング機能を利用できるチャンネルの組み合わせはIEEE802.11n規約によって制限されており、プライマリチャンネル番号とセカンダリチャンネル番号を正しく設定する必要があります。

本装置では、使用するセカンダリチャンネルを、プライマリチャンネル番号のオフセットとして指定します。

プライマリチャンネル番号（無線LANチャンネル番号）とセカンダリチャン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 | プライマリチャンネル番号 | セカンダリチャンネル オフセット | セカンダリチャンネル番号 |
|--------|--------------|---------------------|--------------|
| 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 | プライマリチャンネル番号 | セカンダリチャンネルオフセット | セカンダリチャンネル番号 |
|------|--------------|-----------------|--------------|
| 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-M20AP1 / 20AP2、無線 LAN クライアントで、チャン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

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

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

```

チャン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

```

2 無線 LAN 機能を使う (SR-M20AC1 / 20AC2)

適用機種 SR-M20AC1, 20AC2

2.1 無線 LAN ネットワークを構築する

適用機種 SR-M20AC1, 20AC2

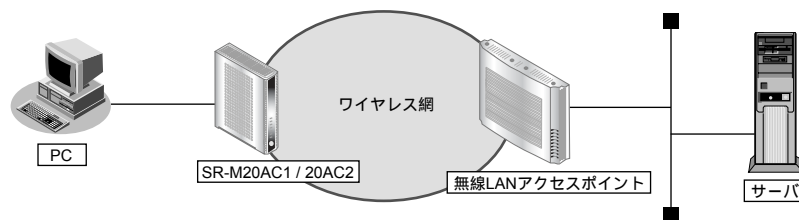
無線 LAN によるネットワークのワイヤレス化を行い、LAN ケーブルの配線なしに無線通信によるネットワークを構築することができます。

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。

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 SR-M20AC1 ご利用にあたって「[3.3.2 本装置をご購入時の状態に戻す](#)」(P.42)
- SR-M20AC2 ご利用にあたって「[本装置をご購入時の状態に戻す](#)」(P.51)



● 設定条件

無線 LAN を使ってネットワークを構築する

- 利用する無線 LAN モジュール : ieee80211 1
- 通信モード : IEEE802.11b/g
- 11b/g チャンネル : 10
- 利用する無線 LAN インタフェース : wlan 1
- SSID : samplenet
- 認証モード : 共通鍵認証
- WEP 使用の設定 : WEP を使用する無線アクセスポイントとだけ通信する
- WEP キー : 64-bit キーのテキストで "abcde"
- 使用する WEP キー : 2

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
```

無線 LAN インタフェースを設定する

```
# wlan 1 use on  
# wlan 1 ssid samplenet  
# wlan 1 auth shared  
# wlan 1 wep mode enable  
# wlan 1 wep key 2 text abcde  
# wlan 1 wep send 2
```

設定終了

```
# save  
# commit
```

2.2 無線 LAN ネットワークを構築する (IEEE802.11n)

適用機種 SR-M20AC1, 20AC2

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

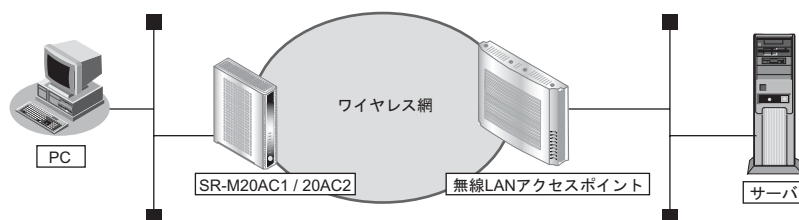
- 無線 LAN クライアントが IEEE802.11n に対応している必要があります。
- 暗号化方式として WEP および TKIP は使用できません。定義した場合は無効な設定として無線 LAN インタフェースが使用できません。
- IEEE802.11n 未対応の無線装置が同一チャンネルに存在している場合、スループットが低下する場合があります。

☛ 参照 機能説明書 「2.1.16 HT プロテクション機能」 (P31)

- 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つ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 SR-M20AC1 ご利用にあたって 「3.3.2 本装置をご購入時の状態に戻す」 (P42)

SR-M20AC2 ご利用にあたって 「本装置をご購入時の状態に戻す」 (P51)



● 設定条件

無線 LAN を使ってネットワークを構築する

- 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 : IEEE802.11a/n
- チャンネル : 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 1 use on  
# ieee80211 1 mode 11a/n  
# ieee80211 1 channel 52
```

無線 LAN インタフェースを設定する

```
# wlan 1 use on  
# wlan 1 ssid samplenet  
# wlan 1 auth wpa/wpa2-psk  
# wlan 1 wpa cipher aes  
# wlan 1 wpa psk text abcdefghijklmnopqrstuvwxyz
```

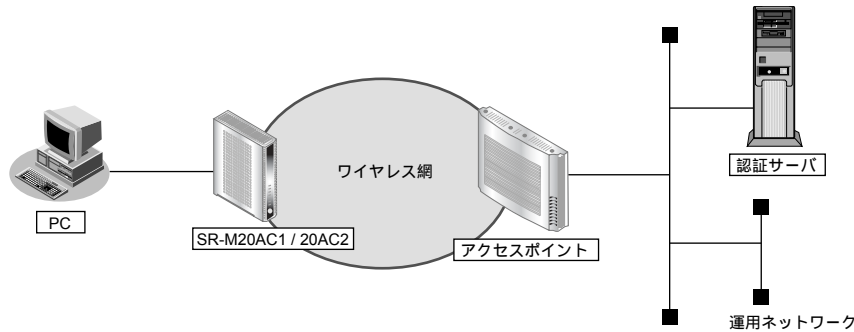
設定終了

```
# save  
# commit
```

2.3 無線 LAN ネットワークで認証・暗号化する

適用機種 SR-M20AC1, 20AC2

SR-M20AC1 / 20AC2 とアクセスポイント間（ワイヤレス網）を認証・暗号化することができます。
以下にその設定例について説明します。



● 前提条件

- SR-M20AC1 / 20AC2、アクセスポイントで、認証・暗号関連以外は、正しく設定されている
- 認証サーバの設定は、適切な設定がなされる

2.3.1 OPEN 認証 IEEE802.1X連携 EAP-MD5 認証

● 設定条件

- 認証モード : open
- EAP プロトコル : EAP-MD5
- EAP ID : user@example.com
- EAP パスワード : abcdefg

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

```

サブリカント情報を設定する
# supplicant dot1x use on

無線 LAN インタフェース（認証、暗号化関連）を設定する
# wlan 1 auth open
# wlan 1 supplicant dot1x use on
# wlan 1 supplicant eap protocol md5
# wlan 1 supplicant eap id user@example.com
# wlan 1 supplicant eap password abcdefg

設定終了
# save
# commit

```


2.3.2 SHARED 認証 IEEE802.1X 連携 EAP-MD5 認証

● 設定条件

- 認証モード : SHARED
- EAP プロトコル : EAP-MD5
- EAP ID : user@example.com
- EAP パスワード : abcdefg
- WEP 使用の設定 : WEP を使用する無線アクセスポイントとだけ通信する
- WEP キー : 64-bit キーのテキストで “abcde”
- 使用する WEP キー : 2

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

```

サブリカント情報を設定する
# supplicant dot1x use on

無線 LAN インタフェース（認証、暗号化関連）を設定する
# wlan 1 auth shared
# wlan 1 supplicant dot1x use on
# wlan 1 supplicant eap protocol md5
# wlan 1 supplicant eap id user@example.com
# wlan 1 supplicant eap password abcdefg
# wlan 1 wep mode enable
# wlan 1 wep key 2 text abcde
# wlan 1 wep send 2

設定終了
# save
# commit

```

2.3.3 WPA 事前共有キー（PSK）認証

● 設定条件

- 認証モード : wpa-psk
- 暗号化モード : TKIP
- 事前共有キー（PSK） : 16進数で “12345abc”

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 インタフェース（認証、暗号化関連）を設定する
# wlan 1 auth wpa-psk
# wlan 1 wpa cipher tkip
# wlan 1 wpa psk hex 12345abc

設定終了
# save
# commit

```

2.3.4 WPA IEEE802.1X 連携 EAP-TLS 認証

● 設定条件

自装置証明書、秘密鍵を準備する

- 鍵ペア識別番号 : 0
- 鍵長 : 1024bit
- 証明書要求で使用するハッシュアルゴリズム : md5
- 国名 : JP
- 都道府県 : Kanagawa
- 市区町村 : Kawasaki
- 組織または会社名 : Fujitsu Limited
- 組織ユニットまたは部門 : Tech Div.
- ホスト名 : shisya.fujitsu.com
- メールアドレス : shisya@fujitsu.com

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。

自装置証明書要求を作成 (鍵ペアの作成) する

● コマンド

自装置証明書要求 (鍵ペア) の作成を行う

```
# crypto certificate generate
RSA key pair number[0-4] :0
generate RSA key pair.
Are you sure?[y/n] :y
key bit(512-2048) :1024
certificate request hash(sha1 or md5) :md5
Country Name(2 letter code) :JP
State or Province Name :Kanagawa
Locality Name :Kawasaki
Organization Name :Fujitsu Limited
Organizational Unit Name :Tech Div.
Common Name :shisya.fujitsu.com
Email Address :shisya@fujitsu.com
```

以下のようなコマンドが表示され、自装置証明書要求 (鍵ペア) の設定が行われます。

Please wait to create RSA private key and Certificate request.

```
certificate private 0 line 0 riUB@No/fTnpCpEt5EF0cCIRdgTiDnB5n4DLemM5Lr1D8@zQQAL90cFFlCgzCY7P@W3ddbEokoMnHTc@6SP7VOyisD2
certificate private 0 line 1 qC0dBKfQC1TpoWDZtPlUkK5cU1YilubYxhA5V2dudYwB0xAcjflFvsNRzF/xcoi5FnKiOdZjzWxv75NjYMY@nzuVnL6
certificate private 0 line 2 w27xcCjoF1paovWVw1aA4rXXY2L4DGW30rs04sDWCnERcL855Mqw0@Xz0raGv@g8MfKGX3bnEaDImiyAIFflbxRVFsQU
certificate private 0 line 3 xM5/V6omhXp2WaRn6Xi/04wipg357HvboVnJKaiQpY6AbeAftpphz47KFPKnMDaMuxlPY2w@15Obr1KUM1Vkn0U/YTP
certificate private 0 line 4 cfsRgjZ8kEbsUEsNzfnTKATIbtDSBqIZ5Bo46RwRIBkpkJ9dlVv30dJ7cdfnJi9hX@faJbpP3@F3NZP4yKAE3CWtqF
certificate private 0 line 5 jk31xZd750HuAGNPWsvEVEVMA6Kt@YpkpV9zwWGdlmOKBs8XgTA8Y5hg8Ut@THKIRI0TgdM4avfQaYwwXVWwCFxvUHh
certificate private 0 line 6 KsrHISB2rYuTnCYCm2sYNdVXaVrMv6VqkNfYnrOwfwu0QoczYUZEDNOYSkP2tLDqBoO47nNWmJWObe2BOex1ujZktW/
certificate private 0 line 7 59UMtzcr44eZToKjXqU2JHi3ukoKHi4FETYeljZ2MRMoz0DAflVspeddmCjmA0F7SvHh1egTyF0u9GFxW6kTmBy6/lgc
certificate private 0 line 8 7Vjmfca4QXaAW4MROzjMMmT2kM0phwZ35MNeg977kXr2E2vznOh9Wlk4JmBYplxkw@OHo54sC9@HTYy8PNJcP1nSs
certificate private 0 line 9 pn21UfTKuk7eVv7WHuxeEznr0V7Wom0FA8Y0u0yQTX5Ebef7DZMgNgrCxpH@jilClmgstpyehofYUc3KFvNmx2ujLJQ
certificate private 0 line 10 uittrerb9m0JxHmle91wPzGZqMwCy5HFL2IUIn/cuv0y1sh8qC20unS26tO0iv87dpWwccEqAlwt3PGZHM339Y77Cp
certificate private 0 line 11 i0q8WeYLk4sSb9vcsnicFdINAYl9wrWBaZjQIV09vSleN26oTDNBxvmCbJmQyJjUxcDntSiyrylUPthzziagC@SLet
certificate private 0 line 12 WbejnbFwGh/Y6RxCav38qx6@04Eb1bfVaubC/zDH9rLwgr10N/10Rzli0ZqzJ63oL
certificate request 0 line 0 MIICMDCCAZkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEWhLYW5hZ2F3YTER
certificate request 0 line 1 MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGItaXRIZDESMBAG
certificate request 0 line 2 A1UECXMJVGVjaCBEaXYuMRswGQYDVQDEExJzaGlzeWEuZnVqaXRzdS5jb20xHzAD
certificate request 0 line 3 BgkqhkiG9w0BCQEWEWhvZ2VhZnVqaXRzdS5jb20wZ3wZ8wDQYJKoZIhvcNAQEBBQAD
certificate request 0 line 4 y0AMIGJAOGBAJ6514c4JqfTA1Y43xnEj3UwGPb/I9yaAuR9ZB/TTIglLUw7nHj
certificate request 0 line 5 Eu+i2RSudi7YhH70YQgMdBG81CtelqV2zP+xx/9507lqs5YyJkHYzqyS4E4+KOAQg
certificate request 0 line 6 fs/o1JlcpEPD2iAqW0rkXGVocRjNuxN7FdhfDiwsUUNAXX3CyHQ/x0LAgMBAAGg
certificate request 0 line 7 UDBOBgkqhkiG9w0BCQ4xQTA/MasGA1UdDwQEAWiChDAPBgNVHREEDCAGhwTAqAEB
```

```
certificate request 0 line 8 MB8GA1UdEQQYMBaCFHNoaXN5Y51hLmZ1aml0c3UuY29tMA0GCSqGSib3DQEBAUA
certificate request 0 line 9 A4GBADod3PXDfWBjOmrUNdeODdrlKakzNtmEx6py42t92reStv3Lx903TJ503QqQ
certificate request 0 line 10 Zzs7YoyRK2BZCkdRuzrs7eAmMPO41/tRNalR6lkDXcL5xw0JKU79rlsYllGboCJa
certificate request 0 line 11 CzIBS/z/+Rkq72KHOWQa/lqZZRMEJAAN4tqbCv6EnNHAAn3L
Created RSA private key and Certificate request.
#
```

自装置証明書要求（鍵ペア）の作成終了

```
# save
```

自装置証明書要求（鍵ペア）の表示

```
# show crypto certificate base64 candidate
```

```
[Certificate Request]
```

```
[1] Number : 0
```

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIcMDCCAzkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEWhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGltaxRIZDESMBAG
A1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
BgkqhkiG9w0BCQEWEGhvZ2ZVAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAJ6514c4JqfTA1Y43xnEji3UwGPb/I9yaAuR9ZB/TTlgkLUw7nHj
Eu+i2RSudi7YhH70YOGMdBG81CtelqV2zP+x/95O7lqs5YyJkHYzqyS4E4+KOAQG
fs/o1JicpEPD2iAqW0rkXGVocRjNuxN7FdhfDiwsUUNAXXI3CyHQ/x0LAGMBAAgG
UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAghwTAqAEB
MB8GA1UdEQQYMBaCFHNoaXN5Y51hLmZ1aml0c3UuY29tMA0GCSqGSib3DQEBAUA
A4GBADod3PXDfWBjOmrUNdeODdrlKakzNtmEx6py42t92reStv3Lx903TJ503QqQ
Zzs7YoyRK2BZCkdRuzrs7eAmMPO41/tRNalR6lkDXcL5xw0JKU79rlsYllGboCJa
CzIBS/z/+Rkq72KHOWQa/lqZZRMEJAAN4tqbCv6EnNHAAn3L
```

```
-----END CERTIFICATE REQUEST-----
```

```
#
```

表示された自装置証明書要求の証明書部分「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」の最後の改行までをカット&ペーストで端末（パソコンなど）に保存します。

保存した自装置証明書要求は端末で、FTP や HTTP などにて認証局（CA）と交換します。

次に認証局で発行された自装置証明書を FTP や HTTP などにて認証局から端末（パソコンなど）に保存します。

自装置証明書を取り込む

● コマンド

```
# crypto certificate local 0 name my-cert0
```

```
Please input.
```

端末（パソコンなど）に保存した自装置証明書を貼り付けます。

```
-----BEGIN CERTIFICATE-----
```

```
MIIcCrzCCAahCAQEWdQYJKoZIhvcNAQEEBQAwwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaxRIZDESMBAGA1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2ZVAZnVqaXRzdS5jb20wHhcN
MDYwNjA1MDIyMjE1WhcNMDCwMTAxMDIyMjE1WjCBnzELMAkGA1UEBhMCSIAxETAP
BgNVBAGTCeEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwIuZWNoIERpdj4xGzAZBgNVBAMTEEnNoaXN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSib3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBkgqhkiG9w0BAQEFAAOBjQAwgYkCgYEAocGCIVZtO1Tool3eIltbmsOxhK3
KIOqwZhDM11sOGIQUvT6ImpyL25NcoQIJbN9mT31MWWpp1nfirBB3LenaT3X/MEo
vveD9FJ1VbnENjbuEmmjhvxnj7/MHDvQ1D3163BpsIkOIVs1dauO+uOZ6R1iIM4G
Kypoad0ukW05f9ECAwEAATANBgkqhkiG9w0BAQQFAAOBgQBHokgsMEIT5CJbozH7
rX4u+dLwb0Y48rkfuTmITrfx+eVniPVCdaUxV0Ih361RaWtta/8116OxHylmHCnt
LOLEscckXxnU0ArYBNjyYlrXwurBJYtIVZPOPqRDq7gSez4zp1IPkt14DrTRSGOh
3rQwOpmTcYT9Uu4iddD9CmUrA==
```

```
-----END CERTIFICATE-----
```

以下のようなコマンドが表示され、自装置証明書の設定が行われます。

```
certificate local 0 name my-cert0
```

```

certificate local 0 line 0 MIICITCCA4CAQAwDQYJKoZIhvcNAQEEBQAwwZlxCzAJBgNVBAYTAkpQMREwDwYD
certificate local 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMla2F3YXNha2kxEDA0BgNVBAoTB3NjYyBM
certificate local 0 line 2 dGQxDALBgNVBAsTBGRhaTlxGDAWBgNVBAMTD0hpcm9mdW1pIEthc3VnYTEiMCAG
certificate local 0 line 3 CSqGSib3DQEJARYTa2FzdWdAc2NjLWluYy5jby5qcDAeFw0wNjAxMDQwNzUwNTNa
certificate local 0 line 4 Fw0wNjAyMDMwNzUwNTNaMIGSMQswCQYDVQQGEwJKUDERMA8GA1UECBMIS2FuYWdh
certificate local 0 line 5 d2ExETAPBgNVBACTCGthd2FzYWtpMRAwDgYDVQQKEwdzY2MgTHRkMQ0wCwYDVQQL
certificate local 0 line 6 EwRkYwkyMRGwFgYDVQQDEw9laXJvZnVtaSBLYXN1Z2ExIjAgBgkqhkiG9w0BCQEW
certificate local 0 line 7 E2thc3VnQHJyY1pbmMuY28uanAwgZ8wDQYJKoZIhvcNAQEEBQAwwZlxCzAJBgNVBAYTAkpQMREwDwYD
certificate local 0 line 8 AM5sXoNnzM4FQrYnF/ekLWYfH3w0yZl1qtGUpoWRZIGWiAs4rx/1RgGtnQnjNBc
certificate local 0 line 9 8tD9tG2Uo2ngiNsKNvRB39j7EGFIgdPJwwfAaKqA7rgRzQo7jyH7rE5CATVBAnYI
certificate local 0 line 10 HUOIhUAOzDy851u5p4ZjADdlcsPu+5FUqgMgVZ7/B/sdAgMBAAEwDQYJKoZIhvcN
certificate local 0 line 11 AQEEBQADgYEAwpvly/Ak6d1vMgdtclYY5S14jQKd2tnB9CtHz+byG4I75lgqh2uF
certificate local 0 line 12 xZlpbYuSGvVOS+zll1yilexM5p7QPUs/BAWU1ePUmrlrasetEbgIFX0pXylWF8C
certificate local 0 line 13 bW08H9SMIDfkd6dindxpKA3VmVIPQKSwCkaAF2kA+LAao0lasskjm04=
#

```

自装置証明書の設定終了

```
# save
# reset
```

● 設定条件

認証局証明書を準備する

- 認証局証明書識別名 : ca-cert0

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。

認証局証明書を設定する

認証局で発行された認証局証明書をFTPやHTTPなどで認証局から端末（パソコンなど）に保存します。

端末（パソコンなど）に保存した認証局証明書を貼り付けます。

● コマンド

```

# crypto certificate ca 0 name ca-cert0
Please input.
----BEGIN CERTIFICATE-----
MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGItXRIZDESMBAGA1UECXMJVGvjaCBEaXYuMRswGQYDVQQDEExJob25zeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAxETAP
BgNVBAGTCEthbnFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRlwEAYDVQQLEwIjUZWNoIERpdia4xGzAZBgNVBAMTEmhvbnN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSib3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwwZkCgYEAua6liSE7sVwzRHhfUnUrwnQay45L
3nQ4/7zfeAk5uEcXM69NqL+XoSSzmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
mVOTGe1ovNGcjp6T73v5MJHivp69Vhc8a25KE7BSaTbsAkvTOPAJt83QE4aXJIZx
zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
/9AqZo3mV7b/uXDdljRMBlg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
Wiv3s5KaqrjACyTVnCHU7RKqQjpnJ6TNwSKUIAxDrqSNM5zzg4AgIX+uE8XY5fE
VAupZ2q7za3Slq6GikoN+tXc4Q==
-----END CERTIFICATE-----

```

以下のようなコマンドが表示され、認証局証明書の設定が行われます。

```

certificate ca 0 name ca-cert0
certificate ca 0 line 0 MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate ca 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate ca 0 line 2 c3UgTGItXRIZDESMBAGA1UECXMJVGvjaCBEaXYuMRswGQYDVQQDEExJob25zeWEu
certificate ca 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN

```

```

certificate ca 0 line 4 MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIxETAP
certificate ca 0 line 5 BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate ca 0 line 6 aXRzdSBMaW1pdGVkMRlwEAYDVQQLewlUZWNolERpdj4xGzAZBgNVBAMTEmhvbnN5
certificate ca 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate ca 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwnQay45L
certificate ca 0 line 9 3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
certificate ca 0 line 10 mVOTGe1ovNGcpj6T73v5MJHivp69Vhc8a25KE7BSaTbsAkVTOPAJt83QE4aXJIZx
certificate ca 0 line 11 zeFdGj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
certificate ca 0 line 12 /9AqZo3mV7b/uXDdljRMblg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
certificate ca 0 line 13 Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUIAxDrgSNM5zzg4AgIX+uE8XY5fE
certificate ca 0 line 14 VAupZ2q7za3Slq6GikoN+tXc4Q==

```

認証局証明書の設定終了

```

# save
# reset

```

● 設定条件

- 認証モード : wpa
- 暗号化モード : TKIP
- EAP プロトコル : EAP-TLS
- EAP ID : user@example.com
- 認証局証明書情報 : 認証局証明書識別番号 0 の証明書を使用する
- 自装置証明書情報 : 自装置証明書識別番号 0 の証明書を使用する
- 秘密鍵識別番号 : 秘密鍵識別番号 0 の秘密鍵を使用する

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

無線 LAN インタフェース (認証、暗号化関連) を設定する

```

# wlan 1 auth wpa
# wlan 1 wpa cipher tkip
# wlan 1 supplicant eap protocol tls
# wlan 1 supplicant eap id user@example.com
# wlan 1 supplicant certificate ca 0
# wlan 1 supplicant certificate local 0
# wlan 1 supplicant certificate private_key 0

```

設定終了

```

# save
# commit

```

2.3.5 WPA IEEE802.1X 連携 EAP-TTLS 認証

● 設定条件

認証局証明書を準備する

- 認証局証明書識別名 : ca-cert1

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。

認証局証明書を設定する

認証局で発行された認証局証明書を FTP や HTTP など認証局から端末（パソコンなど）に保存します。
端末（パソコンなど）に保存した認証局証明書を貼り付けます。

● コマンド

```
# crypto certificate ca 1 name ca-cert1
Please input.
-----BEGIN CERTIFICATE-----
MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaxRIZDESMBAGA1UECXMJVGvjaCBEaXYuMRswGQYDVQQDEExJob25zeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAxETAP
BgNVBAGTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwIUZWNolERpdi4xGzAZBgNVBAMTEmhvbnN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBkgqhkiG9w0BAQEFAAOBjQAwGykCgYEAua6liSE7sVwzRHhfUnUrwnQay45L
3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwwgjbG/ogzQePq1m
mVOTGe1ovNGcjp6T73v5MJHivp69Vhc8a25KE7BSaTbsAkVTOPAJt83QE4aXJIZx
zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
/9AqZo3mV7b/uXDdljRMblg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUIAxDrqSNM5zzg4AgIX+uE8XY5fE
VAupZ2q7za3Slq6GikoN+tXc4Q==
-----END CERTIFICATE-----
```

以下のようなコマンドが表示され、認証局証明書の設定が行われます。

```
certificate ca 1 name ca-cert1
certificate ca 1 line 0 MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate ca 1 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate ca 1 line 2 c3UgTGltaxRIZDESMBAGA1UECXMJVGvjaCBEaXYuMRswGQYDVQQDEExJob25zeWEu
certificate ca 1 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate ca 1 line 4 MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAxETAP
certificate ca 1 line 5 BgNVBAGTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate ca 1 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwIUZWNolERpdi4xGzAZBgNVBAMTEmhvbnN5
certificate ca 1 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate ca 1 line 8 nzANBkgqhkiG9w0BAQEFAAOBjQAwGykCgYEAua6liSE7sVwzRHhfUnUrwnQay45L
certificate ca 1 line 9 3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwwgjbG/ogzQePq1m
certificate ca 1 line 10 mVOTGe1ovNGcjp6T73v5MJHivp69Vhc8a25KE7BSaTbsAkVTOPAJt83QE4aXJIZx
certificate ca 1 line 11 zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
certificate ca 1 line 12 /9AqZo3mV7b/uXDdljRMblg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
certificate ca 1 line 13 Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUIAxDrqSNM5zzg4AgIX+uE8XY5fE
certificate ca 1 line 14 VAupZ2q7za3Slq6GikoN+tXc4Q==
```

認証局証明書の設定終了

```
# save
# reset
```

● 設定条件

- 認証モード : wpa2
- 暗号化モード : AES
- EAP プロトコル : EAP-TTLS
- EAP ID : user@example.com
- EAP 匿名 ID : デフォルトの匿名 ID “anonymous” を使用
- EAP パスワード : abcdefg
- EAP 内部認証プロトコル : CHAP
- 認証局証明書情報 : 認証局証明書識別番号 1 の証明書を使用する

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

無線 LAN インタフェース (認証、暗号化関連) を設定する

```
# wlan 1 auth wpa2
# wlan 1 wpa cipher aes
# wlan 1 supplicant eap protocol ttls
# wlan 1 supplicant eap id user@example.com
# wlan 1 supplicant eap password abcdefg
# wlan 1 supplicant eap inner protocol chap
# wlan 1 supplicant certificate ca 1
```

設定終了

```
# save
# commit
```

2.3.6 WPA IEEE802.1X 連携 EAP-PEAP 認証

● 設定条件

認証局証明書を準備する

- 認証局証明書識別名 : ca-cert2

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。

認証局証明書を設定する

認証局で発行された認証局証明書を FTP や HTTP など認証局から端末 (パソコンなど) に保存します。

端末 (パソコンなど) に保存した認証局証明書を貼り付けます。

● コマンド

```
# crypto certificate ca 2 name ca-cert2
Please input.
-----BEGIN CERTIFICATE-----
MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQIIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1amI0
c3UgTGltaxRIZDESMBAGA1UECzMJVGVjaCBEaXRYuMRswGQYDVQQDEExJob25zeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA2MDczNTIzWhcNMDczMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAxETAP
BgNVBAGTCeThbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMMPRnVq
aXRzdSBMaW1pdGVkMRlwEAYDVQQLEwIUZWNolERpdj4xGzAZBgNVBAMTEmhvbnN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
```

```

nzANBqkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwnQay45L
3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
mVOTGe1ovNGcjp6T73v5MJHivp69Vhc8a25KE7BSaTbsAkVTOPAJt83QE4aXJIZx
zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
/9AqZo3mV7b/uXDdljRMblg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
Wiv3s5KaqrjACyTVnCHU7RKqQjpnJ6TNwSKUIAxDrqSNM5zzg4AgIX+uE8XY5fE
VAupZ2q7za3Slq6GikoN+tXc4Q==
-----END CERTIFICATE-----

```

以下のようなコマンドが表示され、認証局証明書の設定が行われます。

```

certificate ca 2 name ca-cert2
certificate ca 2 line 0 MIIcCrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate ca 2 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate ca 2 line 2 c3UgTGltXRIZDESMBAGA1UECXMJVGVjaCBEaXYuMRswGQYDVQDEExJob25zeWEu
certificate ca 2 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate ca 2 line 4 MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAXETAP
certificate ca 2 line 5 BgNVBAGTCeThbmFnYXdhMREwDwYDVQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate ca 2 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLewlUZWNolERpdj4xGzAZBgNVBAMTEmhvbnN5
certificate ca 2 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate ca 2 line 8 nzANBqkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwnQay45L
certificate ca 2 line 9 3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
certificate ca 2 line 10 mVOTGe1ovNGcjp6T73v5MJHivp69Vhc8a25KE7BSaTbsAkVTOPAJt83QE4aXJIZx
certificate ca 2 line 11 zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
certificate ca 2 line 12 /9AqZo3mV7b/uXDdljRMblg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
certificate ca 2 line 13 Wiv3s5KaqrjACyTVnCHU7RKqQjpnJ6TNwSKUIAxDrqSNM5zzg4AgIX+uE8XY5fE
certificate ca 2 line 14 VAupZ2q7za3Slq6GikoN+tXc4Q==

```

認証局証明書の設定終了

```

# save
# reset

```

● 設定条件

- 認証モード : wpa/wpa2 自動判別
- 暗号化モード : TKIP/AES 自動判別
- EAP プロトコル : EAP-PEAP
- EAP ID : user@example.com
- EAP パスワード : abcdefg
- PEAP バージョン : バージョン 0 を使用
- 内部認証プロトコル : MSCHAPv2
- 認証局証明書情報 : 認証局証明書識別番号 2 の証明書を使用する

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

無線 LAN インタフェース (認証、暗号化関連) を設定する

```

# wlan 1 auth wpa/wpa2
# wlan 1 wpa cipher auto
# wlan 1 supplicant eap protocol peap
# wlan 1 supplicant eap id user@example.com
# wlan 1 supplicant eap password abcdefg
# wlan 1 supplicant eap peapversion 0
# wlan 1 supplicant eap inner protocol mschapv2
# wlan 1 supplicant certificate ca 2

```

設定終了

```

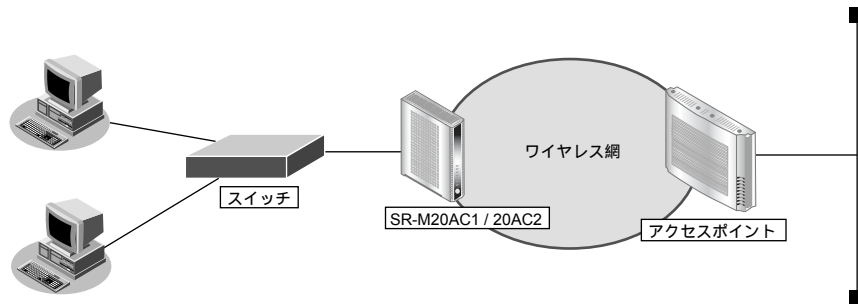
# save
# commit

```


2.4 無線 LAN 中継機能を使う

適用機種 SR-M20AC1, 20AC2

SR-M20AC1 / 20AC2 の有線 LAN にスイッチを併用することにより複数の PC を収容できます。
以下にその設定例について説明します。



● 前提条件

- SR-M20AC1 / 20AC2 で、無線 LAN 中継定義以外は、正しく設定されている

● 設定条件

- 無線 LAN 中継機能の動作モード : マルチクライアントモード
- ノード管理テーブルの有効期限 : 1 日

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 インタフェース（無線 LAN 中継関連）を設定する

```
# wlan 1 relay multi
# wlan 1 relay expire 1d
```

設定終了

```
# save
# commit
```

こんな事に気をつけて

マルチクライアントモードを使用する場合、中継可能なフレームは以下になります。

- IPv4、ARP、DHCP、WOL

ただし、DHCPは、有線 LAN 側の DHCP クライアントが、無線 LAN 側にいる DHCP サーバおよびリレーエージェントにアドレスをもらう形態は中継可能ですが、無線 LAN 側の DHCP クライアントが有線 LAN 側の DHCP サーバにと
いう形態は中継されません。

2.5 ローミング機能を使う

適用機種 SR-M20AC1, 20AC2

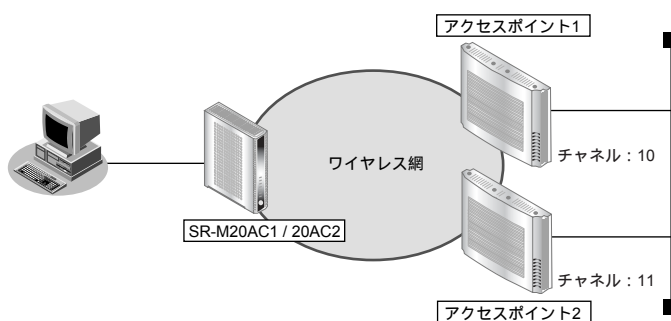
接続先アクセスポイントが複数台ある環境で、SR-M20AC1 / 20AC2 を設置した場合、アクセスポイントとの受信信号強度や送信レート、ビーコン喪失によるローミングを行うことができます。

ローミングを設定することにより、接続中アクセスポイントとの受信信号強度や送信レートが設定したしきい値を下回った場合、より通信状態のよいアクセスポイントへ接続を行います。なお、アクセスポイントから受信するビーコンを連続喪失した場合も、より通信状態のよいアクセスポイントへ接続を行います。

以下にその設定例について説明します。

こんな事に気をつけて

ローミング動作を有効に設定した場合、周辺アクセスポイント情報を定期的（5分間隔）にスキャンします。このスキャンは全チャンネルに対して行うため、通信に影響を与える場合があります。通信するアクセスポイントのチャンネルがあらかじめ判明している場合は、スキャンチャンネルリストでスキャンするチャンネルを限定することをお勧めします。



受信信号強度しきい値から dBm への変換方法は、以下のとおりです。

| 単位 | 変換式 |
|-----|-------------------|
| dBm | (受信信号強度しきい値) - 95 |

● 前提条件

- SR-M20AC1 / 20AC2 で、ローミング定義以外は、正しく設定されている
- 通信モードは、802.11b とする

● 設定条件

- ローミング動作 : 有効
- ローミング受信信号強度のしきい値 : 10
- ローミング送信レートのしきい値 : 2Mbps
- ビーコン喪失回数のしきい値 : 5回
- スキャンチャンネルリスト : 10 と 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

無線 LAN インタフェース (ローミング関連) を設定する

```
# wlan 1 roaming mode enable  
# wlan 1 roaming threshold rssi 11b 10  
# wlan 1 roaming threshold rate 11b 2  
# wlan 1 roaming threshold bmiss 5
```

無線 LAN モジュール (スキャンチャンネル) を設定する

```
# ieee80211 1 chanlist 10,11
```

設定終了

```
# save  
# commit
```

2.6 WMM 機能を使う

適用機種 SR-M20AC1, 20AC2

WMM 機能とは、無線 LAN アクセスポイント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。

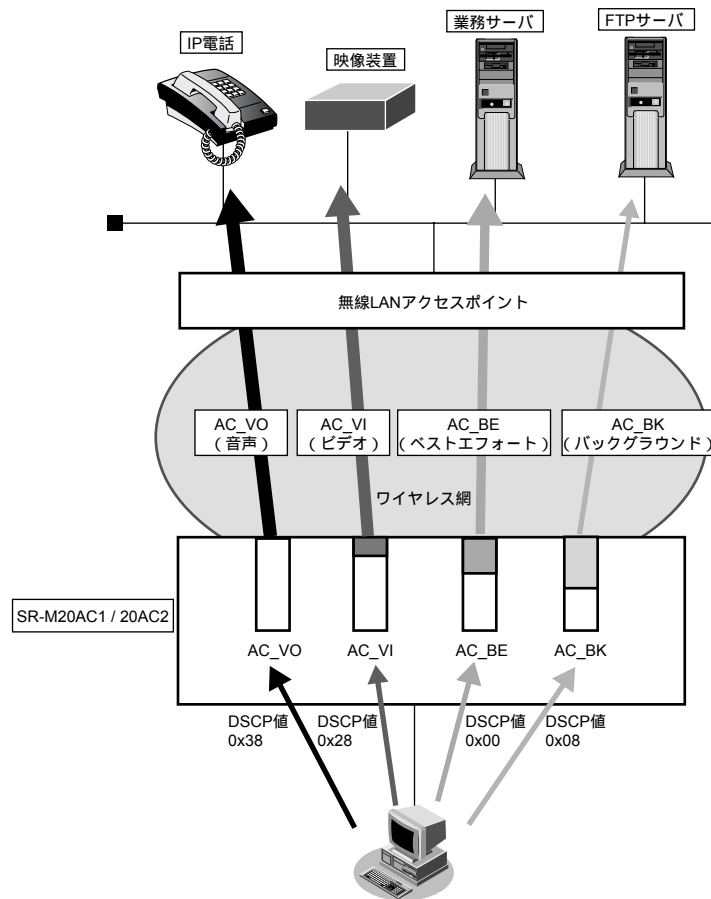
無線に送出するパケットは IP パケットの DSCP 値を元に、4 種類の Access Category (AC) に分類されます。AC は優先度が高い方から、AC_VO (音声)、AC_VI (ビデオ)、AC_BE (ベストエフォート)、AC_BK (バックグラウンド) であり、AC ごとに送信キューを持ちます。送信キューにパケットがたまっている場合は、優先度の低い AC より優先度の高い AC の送信キューから優先的にパケットが送出されます。

● 前提条件

- SR-M20AC1 / 20AC2 で、WMM 定義以外は、正しく設定されている

こんな事に気をつけて

WMM 機能を使うためには、無線 LAN アクセスポイントの WMM 機能も有効にする必要があります。



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

- WMM 優先制御 : 有効にする

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 (WMM 機能) を設定する
# ieee80211 1 wmm mode enable
```

```
設定終了
# save
# commit
```

2.7 WMM機能の Access Category 分類条件を変更する

適用機種 SR-M20AC1, 20AC2

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、[\[2.6 WMM機能を使う\] \(P68\)](#) 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

● 前提条件

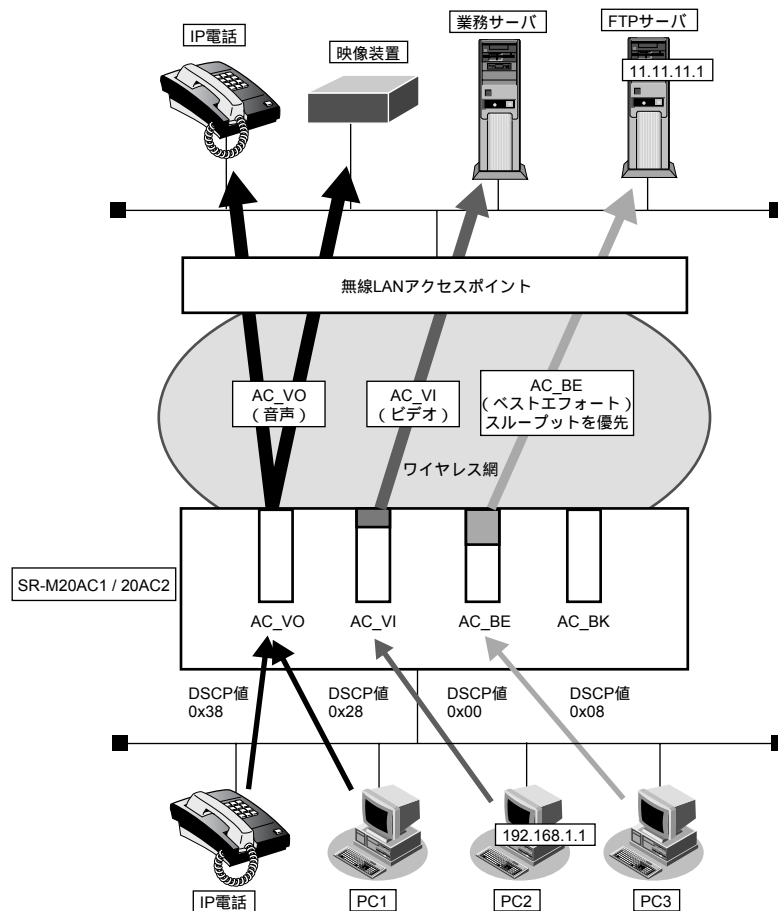
- SR-M20AC1 / 20AC2 で、WMM 定義以外は、正しく設定されている

ここでは、以下の場合を例に説明します。

- ベストエフォートのトラフィックは、スルーットを優先する
- PC1 からのトラフィック (DSCP 値 : 0x28) は、AC を音声に分類する
- PC2 からのトラフィックは、AC をビデオに分類する
- FTP サーバあてのトラフィックは、ベストエフォートに分類する

こんな事に気をつけて

WMM 機能を使うためには、無線 LAN アクセスポイントの WMM 機能も有効にする必要があります。



● 設定条件

- WMM 優先制御 : 有効にする
- 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
- AC 分類条件 : DSCP 値が 0x28 (10 進数で 40) の場合、AC_VO に分類する
送信元 IP アドレスが 192.168.1.1/32 の場合、AC_VI に分類する
あて先 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 (WMM 関連) を設定する

```
# ieee80211 1 wmm mode enable
# ieee80211 1 wmm ack besteffort disable
```

無線 LAN インタフェース (WMM 関連) 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 192.168.1.1/32 any
# acl 2 ip any 11.11.11.0/24
```

設定終了

```
# save
# commit
```

2.8 IEEE802.11n チャンネルボンディング機能を使う

適用機種 SR-M20AC1, 20AC2

チャンネルボンディングとは、隣り合った2つのチャン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

- チャンネルボンディングを使用する場合、無線LANアクセスポイントでチャンネルボンディングを有効にする必要があります。
- 2.4GHz帯では重なり合わない40MHzチャンネルが1つしか確保できないことに加え、ほかのチャンネルとの干渉が発生しやすいため、チャンネルボンディングは5GHz帯での使用を推奨します。

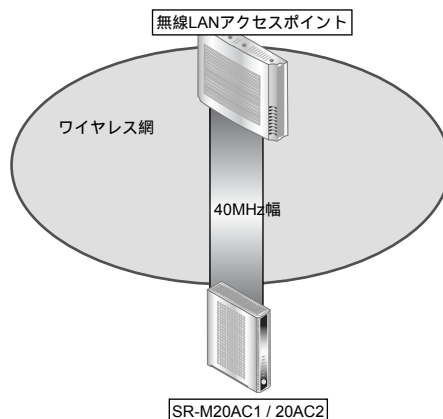
チャンネルボンディング機能を利用できるチャンネルの組み合わせはIEEE802.11n規約によって制限されており、プライマリチャンネル番号とセカンダリチャンネル番号を正しく設定する必要があります。

本装置では、使用するセカンダリチャンネルを、プライマリチャンネル番号のオフセットとして指定します。

プライマリチャンネル番号（無線LANチャンネル番号）とセカンダリチャン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 | プライマリチャンネル番号 | セカンダリチャンネル オフセット | セカンダリチャンネル番号 |
|--------|--------------|---------------------|--------------|
| 2.4GHz | 1 | above | 5 |
| | 2 | above | 6 |
| | 3 | above | 7 |
| | 4 | above | 8 |
| | 5 | above | 9 |
| | 6 | below | 1 |
| | 6 | above | 10 |
| | 7 | below | 2 |
| | 7 | above | 11 |
| | 8 | below | 3 |
| | 8 | above | 12 |
| | 9 | below | 4 |
| | 9 | above | 13 |
| 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 | プライマリチャンネル番号 | セカンダリチャンネルオフセット | セカンダリチャンネル番号 |
|------|--------------|-----------------|--------------|
| 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-M20AC1 / 20AC2、無線LANアクセスポイントで、チャン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

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

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

```

チャンネルボンディング機能を設定する
# ieee80211 1 channel 52
# ieee80211 1 bandwidth 40
# ieee80211 1 secondary-channel above

設定終了
# save
# commit

```

3 VLAN 機能を使う

適用機種 SR-M20AP1, 20AP2

こんな事に気をつけて

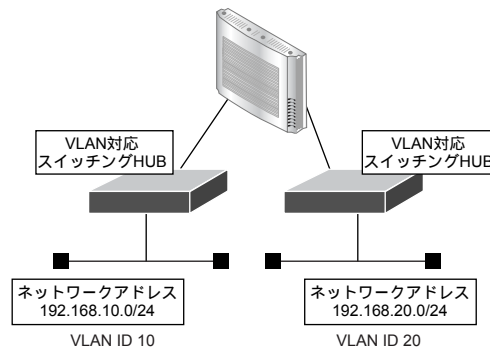
ETHER1とETHER2に同一VLAN IDを設定して運用することはできません。
必ず、異なるVLAN IDを設定する必要があります。

☞ 参照 機能説明書 [2.5 VLAN 機能] (P38)

3.1 ポートVLAN機能を使う

適用機種 SR-M20AP1, 20AP2

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
```

```

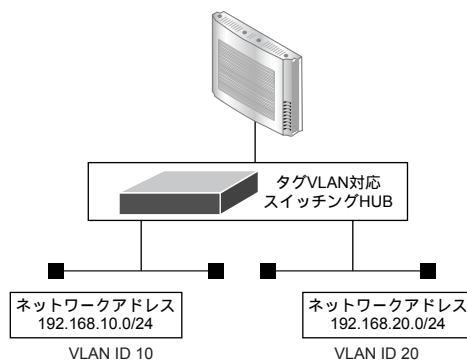
設定終了
# save
# commit

```

3.2 タグVLAN機能を使う

適用機種 SR-M20AP1, 20AP2

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

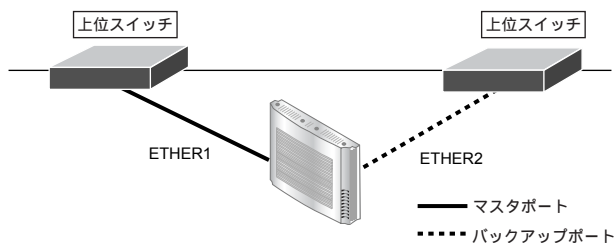
設定終了
# save
# commit

```

4 バックアップポート機能を使う

適用機種 SR-M20AP1, 20AP2

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をマスターポート、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）のマスターポートに設定する
# 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

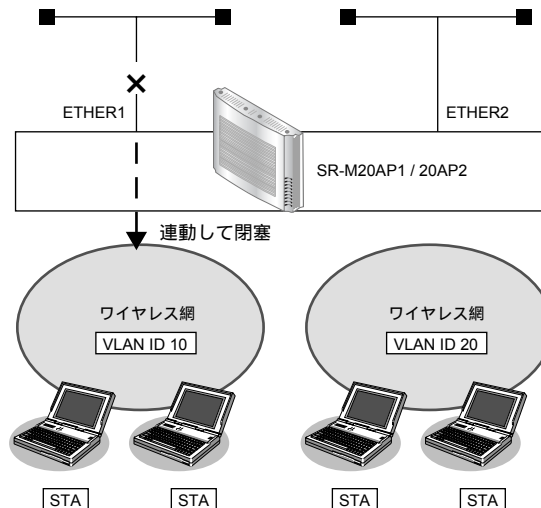
バックアップグループ1をマスターポート優先モードに設定する
# backup 1 mode master

設定終了
# save
# commit
```

5 リンクインテグリティ機能を使う

適用機種 SR-M20AP1, 20AP2

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

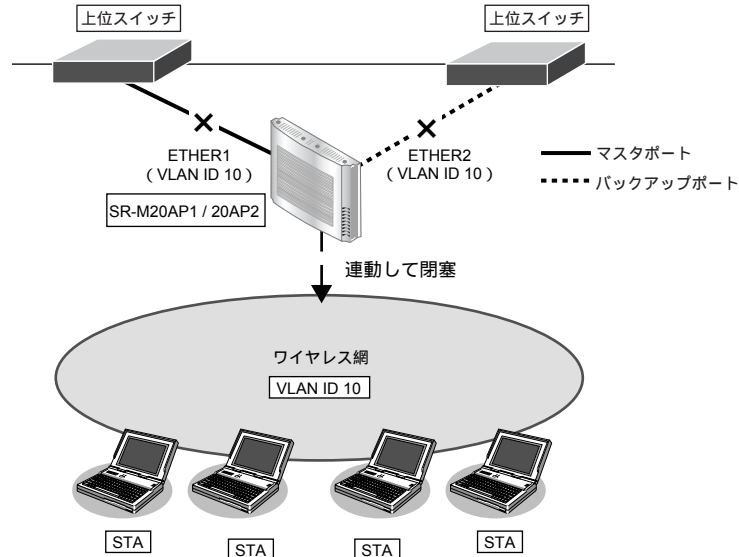
自動的に閉塞解除するモードに設定する
# ether 1 downrelay recovery mode auto
# ether 2 downrelay recovery mode auto

設定終了
# save
# commit
```

5.1 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-M20AP1, 20AP2

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) のマスターポートに設定する
# 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

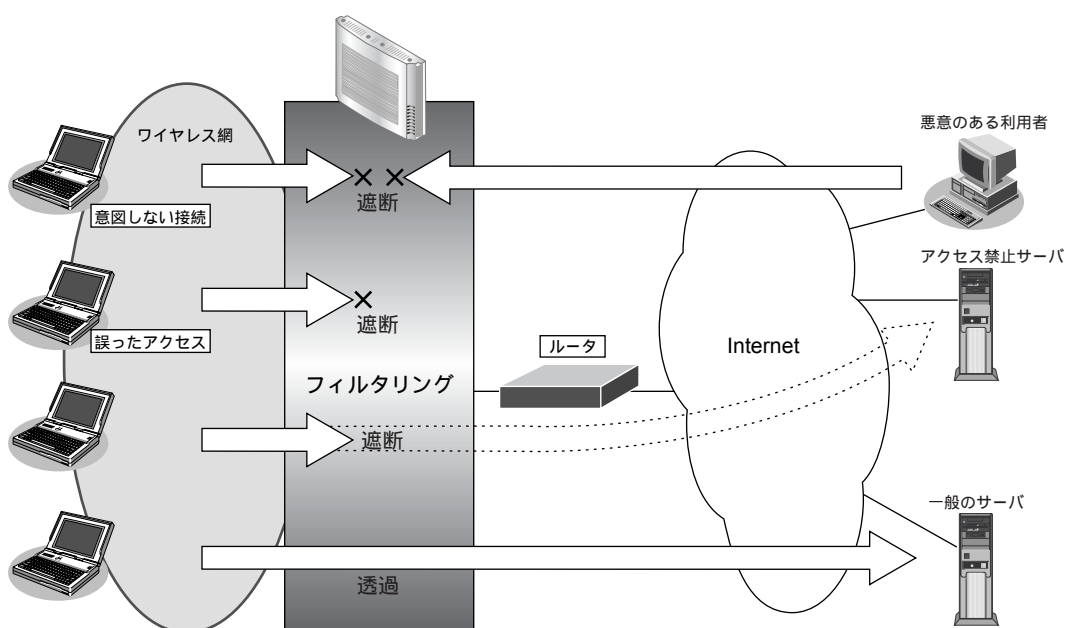
設定終了
# save
# commit
```

6 フィルタリング機能を使う

適用機種 全機種

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。

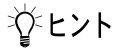
☞ 参照 機能説明書「2.9 フィルタリング機能」(P.44)



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



◆ 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です。

◆ 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。

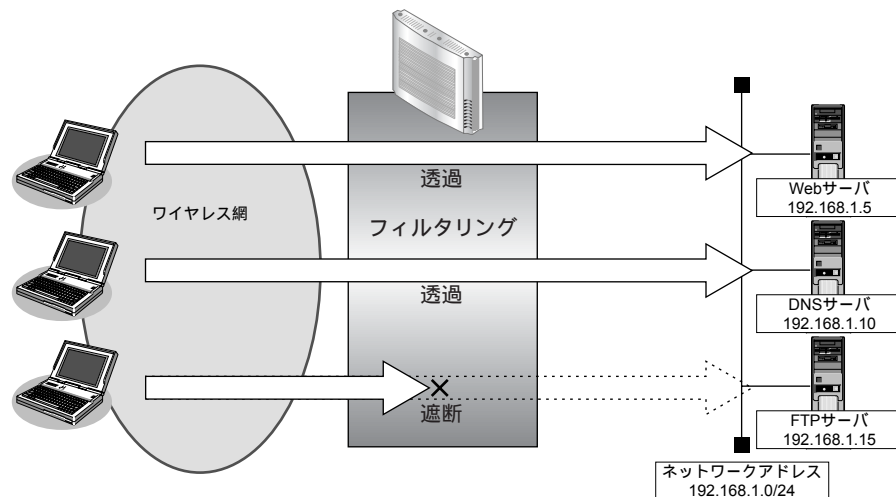
6.1 特定サービスへのアクセスだけを許可する

適用機種 全機種

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。



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制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
```

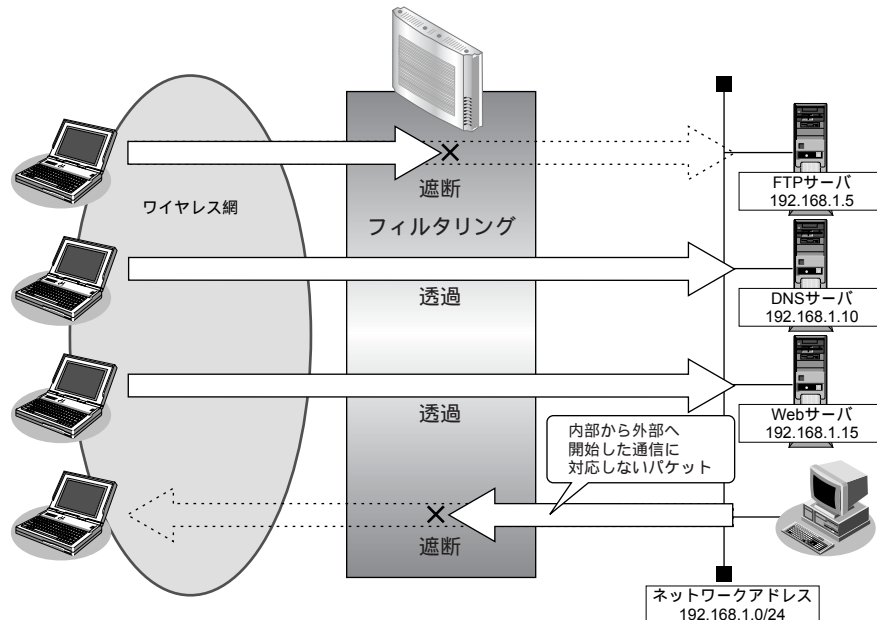
設定終了

```
# save
# commit
```

6.2 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 全機種

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
 - 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
 - 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
```

設定終了

```
# save
# commit
```

6.3 特定のMACアドレス間の通信だけを禁止する

適用機種 全機種

● 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

設定終了
# save
# commit
```

7 IEEE802.1X 認証機能を使う

適用機種 全機種

IEEE802.1X 認証を使用すると、本装置に接続する端末ユーザがネットワークへのアクセス権を持っているかを認証することができます。

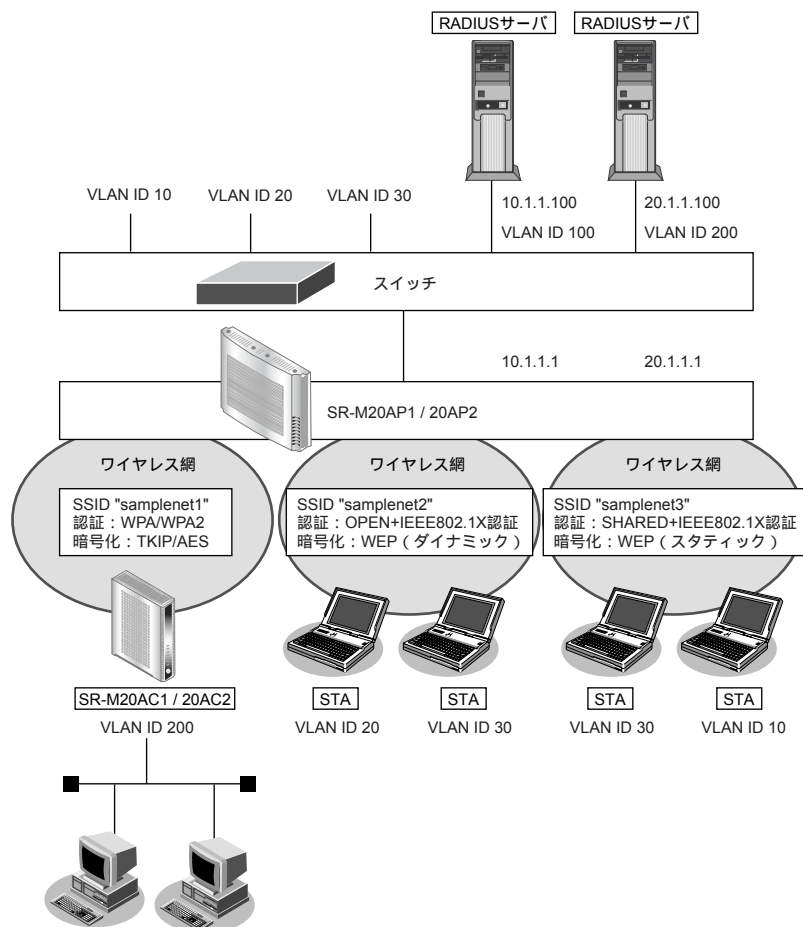
また、SR-M20AP1 / 20AP2 では認証データベースで、ユーザごとに所属する VLAN ID を設定すると、認証されたユーザが所属するネットワークも同時に管理できます。

これらの機能により、ネットワークへのアクセスをユーザ単位で制御でき、ネットワークのセキュリティを向上させることができます。

☛ 参照 機能説明書 [2.10 IEEE802.1X 認証機能] (P46)

こんな事に気をつけて

- IEEE802.1X 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 (SR-M20AP1 / 20AP2)。
- 認証サーバに VLAN ID が設定されていない場合、wlan dot1x vid コマンドで設定された VLAN ID が使用されます (SR-M20AP1 / 20AP2)。
- IEEE802.1X 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。
- ローカル認証で利用できる認証方式は EAP-MD5 だけです。



7.1 無線 LAN で IEEE802.1X 認証機能を使う

適用機種 SR-M20AP1, 20AP2

ここでは、無線 LAN インタフェースで IEEE802.1X 認証を行う場合の設定方法を説明します。

● 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 : 10.1.1.1/24、20.1.1.1/24

無線 LAN を使用する (共通)

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

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 : オープン認証
- 暗号化モード : WEP (ダイナミック)
- 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 : samplenet3) を構築する

- 利用する無線 LAN インタフェース : wlan 3
- SSID : samplenet3
- 認証モード : 共通鍵認証
- 暗号化モード : WEP (スタティック)
- WEP キー : テキストで "abcdefghijklm"
- IEEE802.1X 認証 : 有効
- IEEE802.1X 認証 (サーバ) : aaa1

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 : 10.1.1.100
- 認証サーバシークレットキー : passwd
- 課金サーバ IP アドレス : 10.1.1.100
- 課金サーバシークレットキー : passwd

※) 本装置がサポートする課金情報と対応する属性を以下に示します。

- 接続時間 : Acct-Session-Time

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
```

RADIUS サーバの VLAN を設定する

```
# lan 0 vlan 100
# lan 0 ip address 10.1.1.1/24 3
# lan 1 vlan 200
# lan 1 ip address 20.1.1.1/24 3
```

ETHER1 ポートを設定する

```
# ether 1 vlan tag 10,20,30,100,200
```

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、IEEE802.1X 認証を有効にする

```
# 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
```

仮想アクセスポイント (SSID : samplenet2) を設定し、IEEE802.1X 認証を有効にする

```
# wlan 2 use on
# wlan 2 ssid samplenet2
# wlan 2 auth open
# wlan 2 wep mode enable
# wlan 2 wep type dynamic 128 rekey 10m
# wlan 2 dot1x use on
# wlan 2 dot1x aaa 1
```

仮想アクセスポイント (SSID : samplenet3) を設定し、IEEE802.1X 認証を有効にする

```
# wlan 3 use on
# wlan 3 ssid samplenet2
# wlan 3 auth shared
# wlan 3 wep mode enable
# wlan 3 wep key 1 text abcdefghijklm
# wlan 3 wep send 1
```

```
# wlan 3 dot1x use on  
# wlan 3 dot1x aaa 1
```

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 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
```

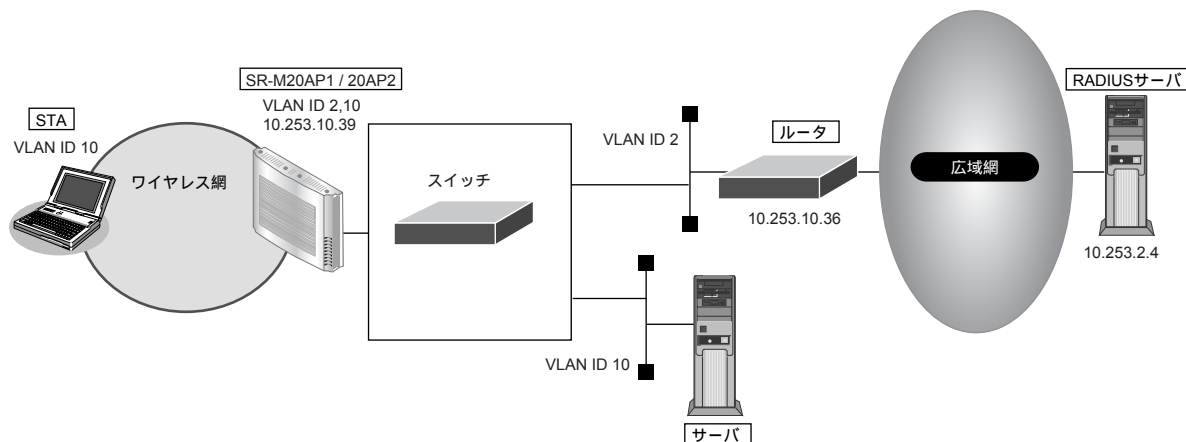
設定終了

```
# save  
# commit
```


7.2 認証自動切替機能を使う

適用機種 SR-M20AP1, 20AP2

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 [コマンドリファレンス](#) [dot1xctl backup recovery]



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、Check ランプが緑色で点滅します。

● 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
- チャンネル : 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
```

7.3 有線LANでIEEE802.1X認証機能を使う

適用機種 SR-M20AC1, 20AC2

ここでは、有線LANでIEEE802.1X認証を行う場合の設定方法を説明します。

なお、SR-M20AC1 / 20AC2とSR-M20AP1 / 20AP2との接続はすでに設定されているものとします。

● 前提条件

- SR-M20AC1 / 20AC2とSR-M20AP1 / 20AP2との接続設定がされている
- SR-M20AP1 / 20AP2において、SR-M20AC1 / 20AC2とRADIUSサーバが同じVLANに所属している
- IPアドレスとして、20.1.1.10/24が設定されている

● 設定条件

認証／課金サーバをAAA定義で指定する

- aaa定義番号 : aaa0
- 認証サーバIPアドレス : 20.1.1.100
- 認証サーバシークレットキー : passwd
- 課金サーバIPアドレス : 20.1.1.100
- 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
```

有線ポートでIEEE802.1X認証を有効にする

```
# ether 1 dot1x use on
# ether 1 dot1x aaa 0
```

認証／課金サーバをAAA定義で指定する

```
# aaa 0 name aaasvr0
# aaa 0 radius service client both
# aaa 0 radius client server-info auth 0 secret passwd
# aaa 0 radius client server-info auth 0 address 20.1.1.100
# aaa 0 radius client server-info auth 0 source 20.1.1.10
# aaa 0 radius client server-info accounting 0 secret passwd
# aaa 0 radius client server-info accounting 0 address 20.1.1.100
# aaa 0 radius client server-info accounting 0 source 20.1.1.10
```

設定終了

```
# save
# commit
```

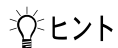
7.4 IEEE802.1X 認証機能を設定したポートに Wake On LAN パケットを転送する

適用機種 SR-M20AC1, 20AC2

SR-M20AC1 / 20AC2 の有線ポートに接続されている端末が Wake On LAN 機能に対応している場合、SR-M20AC1 / 20AC2 が Wake On LAN パケット (Magic Packet) を転送することで端末を遠隔操作で起動させることができます。

しかし、有線ポートに IEEE802.1X 認証機能を設定した場合、認証済み端末が存在しないときは Wake On LAN パケットを転送することができません (認証済み端末が存在する場合は、転送が可能です)。

本機能を設定することにより、認証済み端末が存在しない場合でも Wake On LAN パケットを転送することができます。



◆ Wake On LAN 機能とは？

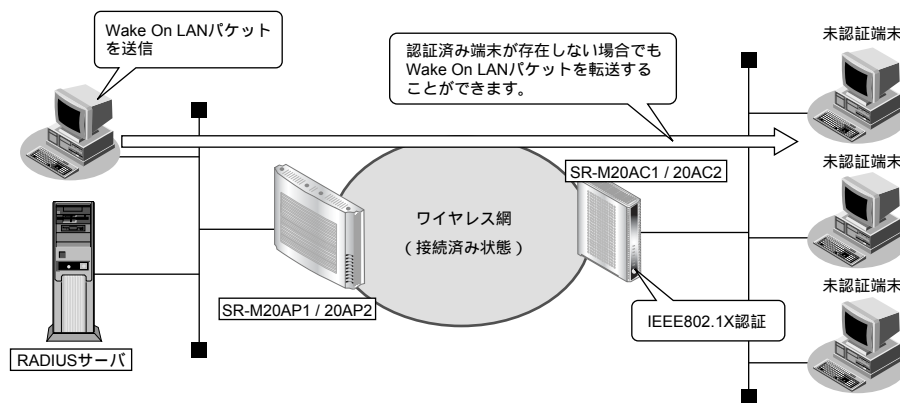
AMD 社が開発したネットワーク上の電源 OFF 状態のパソコンを遠隔操作で起動する機能です。

起動は Magic Packet と呼ばれる Wake On LAN 機能特有のパケットを送付して行います。

なお、Wake On LAN 機能はパソコンを起動するだけで電源 OFF は行いません。電源 OFF する場合は、別途、電源制御用ソフトウェアが必要になります。

こんな事に気をつけて

本機能は、Wake On LAN に対応したパソコンだけで利用できます。Wake On LAN 対応機種については、パソコンのメーカーにお問い合わせください。



● 前提条件

- SR-M20AC1 / 20AC2 の有線インターフェースで IEEE802.1X 認証が設定されており、Wake On LAN パケット転送モード定義以外は、正しく設定されている

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

```
Wake On LANパケット転送モードを有効にする  
# ether 1 dot1x wol enable
```

```
設定終了  
# save  
# commit
```



パソコンがWake On LANパケットを受信してから起動が完了するまで、数十秒から数分かかります（お使いの機種やOSによって異なります）。

8 MAC アドレス認証機能を使う

適用機種 全機種

MAC アドレス認証機能を使用すると、本装置を経由する端末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ができます。

また、SR-M20AP1 / 20AP2 では認証データベースにユーザごとに所属する VLAN ID を設定することで、認証されたユーザが所属するネットワークも同時に管理できます。

これらの機能により、ネットワークへのアクセスをユーザ単位で制御でき、ネットワークのセキュリティを向上させることができます。

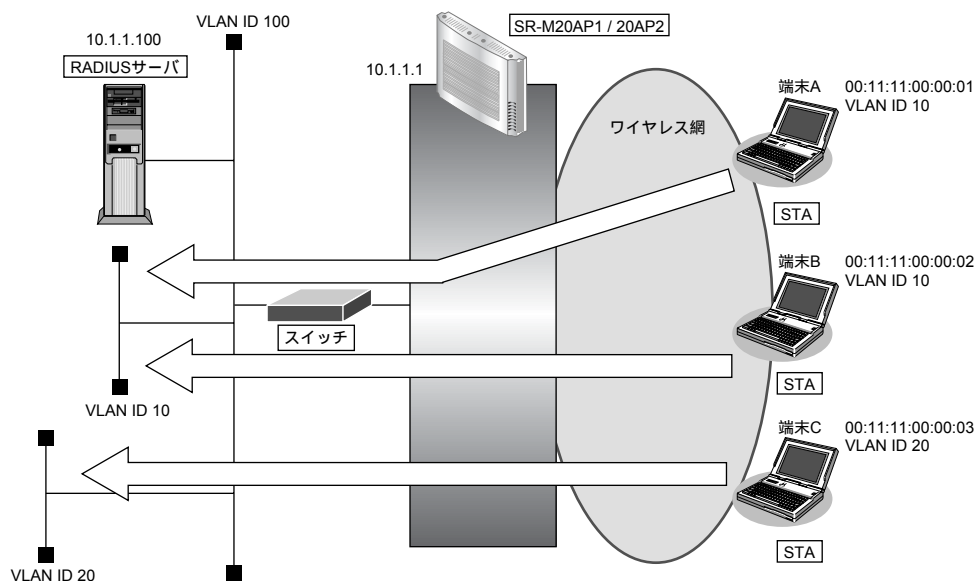
こんな事に気をつけて

- 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 (SR-M20AP1 / 20AP2)。
- 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。

8.1 無線 LAN で MAC アドレス認証機能を使う

適用機種 SR-M20AP1, 20AP2

ここでは、無線 LAN インタフェースで MAC アドレス認証を行う場合の設定方法を説明します。



● 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 : ether 1
- IP アドレス : 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
- 通信モード : IEEE802.11b/g
- チャンネル : 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 : WPA2-PSK
- 暗号化モード : AES
- 事前共有キー (PSK) : テキストで “abcdefghijklmnopqrstuvwxyz”
- MAC アドレス認証 : 有効
- AAA 情報 : aaa 1

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 : WPA2-PSK
- 暗号化モード : AES
- 事前共有キー (PSK) : テキストで “zyxwvutsrqponmlkjihgfedcba”
- MAC アドレス認証 : 有効
- AAA 情報 : aaa 2

AAA 定義で RADIUS 認証サーバ利用を指定する

- aaa 定義番号 : aaa 1
- 認証サーバ IP アドレス : 10.1.1.100
- 認証サーバシークレットキー : passwd
- 利用可能なユーザは以下のとおり

| MAC アドレス | 割り当てる VLAN ID |
|-------------------|---------------|
| 00:11:11:00:00:01 | VLAN 10 |
| 00:11:11:00:00:02 | VLAN 10 |

AAA 定義でローカル認証情報利用を指定する

- aaa 定義番号 : aaa 2
- 利用可能なユーザは以下のとおり

| MAC アドレス | 割り当てる VLAN ID |
|-------------------|---------------|
| 00:11:11:00:00:03 | VLAN 20 |

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

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 100
```

```
# lan 0 ip address 10.1.1.1/24 3
```

ETHER1 ポートを設定する

```
# ether 1 vlan tag 10,20,100
```

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、MAC アドレス認証を有効にする

```
# wlan 1 use on
```

```
# wlan 1 ssid samplenet1
```

```
# wlan 1 auth wpa2-psk
```

```
# wlan 1 wpa cipher aes
```

```
# wlan 1 wpa psk text 1234567890123
```

```
# wlan 1 macauth use on
```

```
# wlan 1 macauth aaa 1
```

仮想アクセスポイント (SSID : samplenet2) を設定し、MAC アドレス認証を有効にする

```
# wlan 2 use on
```

```
# wlan 2 ssid samplenet2
```

```
# wlan 2 auth wpa2-psk
```

```
# wlan 2 wpa cipher aes
```

```
# wlan 2 wpa psk text abcdefghijklm
```

```
# wlan 2 macauth use on
```

```
# wlan 2 macauth aaa 2
```

AAA 定義を設定する

```
# aaa 1 name aaasvr1
```

```
# 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 10.1.1.100
```

```
# aaa 1 radius client server-info auth 0 source 10.1.1.1
```

```
# aaa 2 name localAuth
```

```
# aaa 2 user 0 id 001111000003
```

```
# aaa 2 user 0 password 001111000003
```

```
# aaa 2 user 0 supplicant vid 20
```

設定終了

```
# save
```

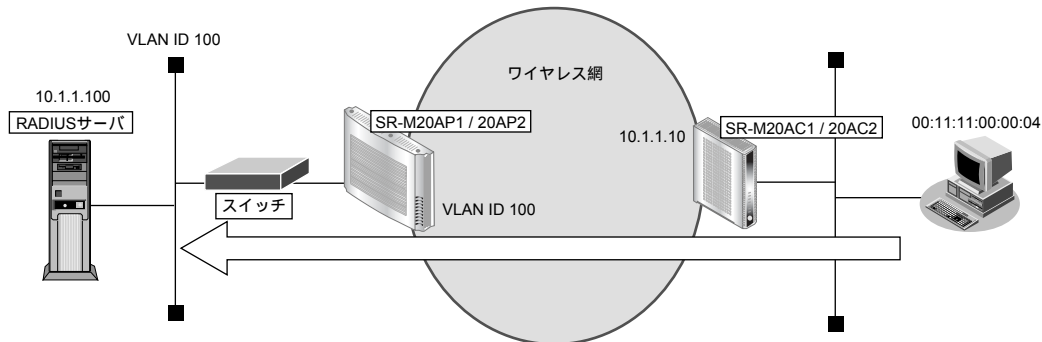
```
# commit
```

8.2 有線LANでMACアドレス認証機能を使う

適用機種 SR-M20AC1, 20AC2

ここでは、有線LANでMACアドレス認証を行う場合の設定方法を説明します。

なお、SR-M20AC1 / 20AC2 と SR-M20AP1 / 20AP2 との接続はすでに設定されているものとします。



● 前提条件

- SR-M20AC1 / 20AC2 と SR-M20AP1 / 20AP2 との接続設定がされている
- SR-M20AP1 / 20AP2 において、SR-M20AC1 / 20AC2 と RADIUS サーバが同じ VLAN に所属している
- IP アドレスとして 10.1.1.10/24 が設定されている

● 設定条件

認証サーバを AAA 定義で指定する

- aaa 定義番号 : aaa 0
- 認証サーバ IP アドレス : 10.1.1.100
- 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

```

MAC アドレス認証を使用する
# macauth use on

有線ポートで MAC アドレス認証を有効にする
# ether 1 macauth use on
# ether 1 macauth aaa 0

認証サーバを AAA 定義で指定する
# aaa 0 name aaasvr
# aaa 0 radius service client auth
# aaa 0 radius client server-info auth 0 secret passwd
# aaa 0 radius client server-info auth 0 address 10.1.1.100
# aaa 0 radius client server-info auth 0 source 10.1.1.10

設定終了
# save
# commit

```

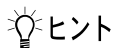
8.3 MACアドレス認証機能を設定したポートにWake On LANパケットを転送する

適用機種 SR-M20AP1, 20AP2

SR-M20AP1 / 20AP2の有線ポートに接続されている端末がWake On LAN機能に対応している場合、SR-M20AP1 / 20AP2がWake On LANパケット (Magic Packet) を転送することで端末を遠隔操作で起動させることができます。

しかし、有線ポートにMACアドレス認証機能を設定した場合、認証済み端末が存在しないときはWake On LANパケットを転送することができません (認証済み端末が存在する場合は、転送が可能です)。

本機能を設定することにより、認証済み端末が存在しない場合でもWake On LANパケットを転送することができます。



◆ Wake On LAN機能とは？

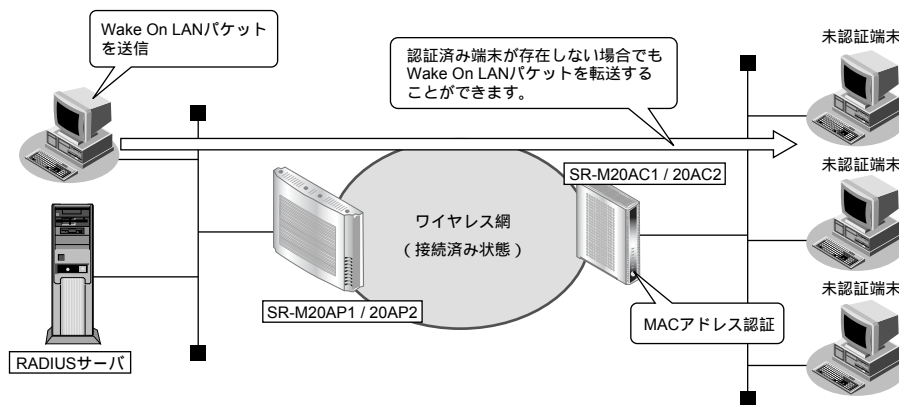
AMD社が開発したネットワーク上の電源OFF状態のパソコンを遠隔操作で起動する機能です。

起動はMagic Packetと呼ばれるWake On LAN機能特有のパケットを送付して行います。

なお、Wake On LAN機能はパソコンを起動するだけで電源OFFは行いません。電源OFFする場合は、別途、電源制御用ソフトウェアが必要になります。

こんな事に気をつけて

本機能は、Wake On LANに対応したパソコンだけで利用できます。Wake On LAN対応機種については、パソコンのメーカーにお問い合わせください。



● 前提条件

- SR-M20AP1 / 20AP2の有線インターフェースでMACアドレス認証が設定されており、Wake On LANパケット転送モード定義以外は、正しく設定されている

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

```
Wake On LANパケット転送モードを有効にする  
# ether 1 macauth wol enable
```

```
設定終了  
# save  
# commit
```



パソコンがWake On LANパケットを受信してから起動が完了するまで、数十秒から数分かかります（お使いの機種やOSによって異なります）。

9 DHCP 機能を使う

適用機種 全機種

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 機能説明書 [2.12 DHCP機能] (P54)

9.1 DHCPクライアント機能を使う

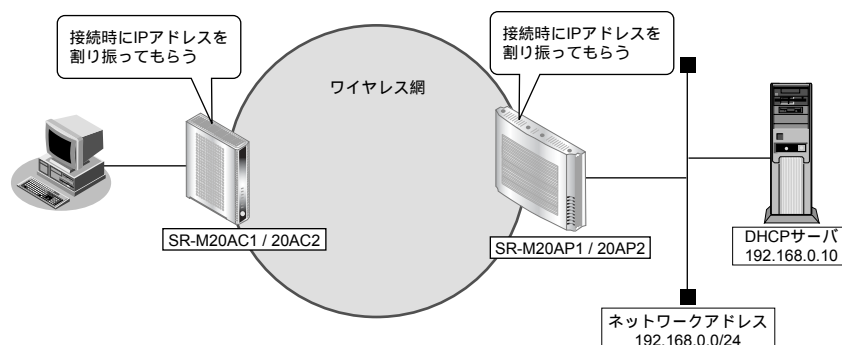
適用機種 全機種

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-M20AP1 / 20AP2

- 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
 - チャンネル : 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

SR-M20AC1 / 20AC2

- ETHER1 ポートを使う
- 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
 - チャンネル : 10 (11b/g)
 - SSID : samplenet
 - 認証モード : OPEN 認証
- 本装置の IP アドレス : 無線 LAN インタフェース経由で 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-M20AP1 / 20AP2

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
```

SR-M20AC1 / 20AC2

ETHER1 ポートを設定する
ether 1 use on

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

設定終了
save
commit

10 DNSサーバ機能を使う (ProxyDNS)

適用機種 全機種

本装置のProxyDNSには、以下の機能があります。

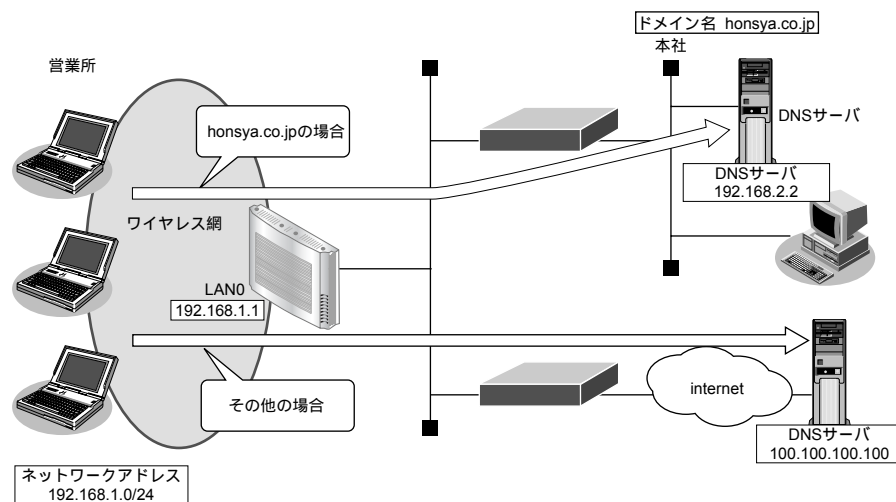
- DNSサーバの自動切り替え機能
- DNS問い合わせタイプフィルタ機能
- DNSサーバ機能

☞ 参照 機能説明書「2.14 DNSサーバ機能」(P57)

10.1 DNSサーバの自動切り替え機能 (順引き) を使う

適用機種 全機種

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 コマンドユーザズガイド「1.7 コマンドで入力できる文字一覧」(P27)

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

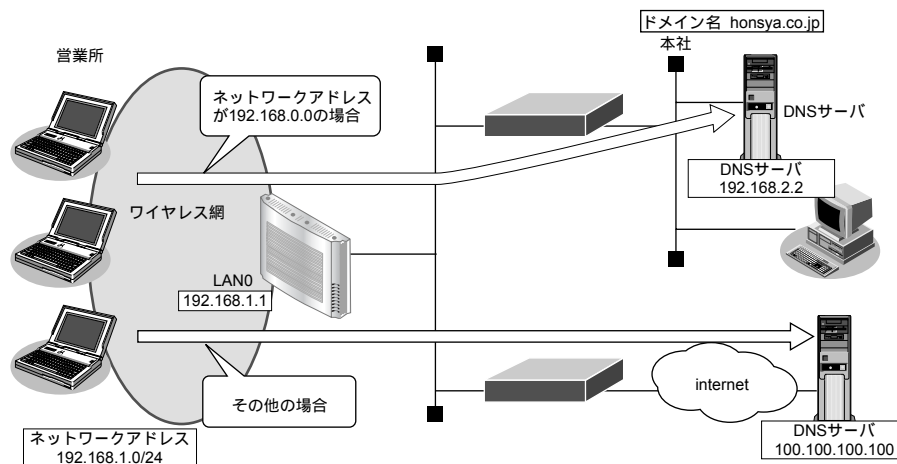
1. パソコン側がDHCPクライアントかどうか確認します。

DHCPクライアントでない場合は設定します。

10.2 DNS サーバの自動切り替え機能（逆引き）を使う

適用機種 全機種

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 コマンドユーザズガイド「1.7 コマンドで入力できる文字一覧」(P27)

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。

10.3 DNS 問い合わせタイプフィルタ機能を使う

適用機種 全機種

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 コマンドユーザズガイド 「1.7 コマンドで入力できる文字一覧」 (P27)

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 Vista の場合を例に説明します。

1. [コントロールパネル] ウィンドウで [ネットワークとダイヤルアップ接続] アイコンをクリックします。
2. [ネットワークと共有センター] をクリックします。
3. [ネットワーク接続の管理] をクリックします。
4. [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] 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。
5. 一覧にインターネットプロトコルバージョン 4 (TCP/IPv4) が含まれていることを確認します。
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. [OK] ボタンをクリックします。
パソコンを再起動するかを確認するメッセージが表示されます。
12. [はい] ボタンをクリックし、パソコンを再起動します。
設定した内容は、再起動後に有効になります。

10.4 DNS サーバ機能を使う

適用機種 全機種

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サーバー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 コマンドユーザズガイド「[1.7 コマンドで入力できる文字一覧](#)」(P27)

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。

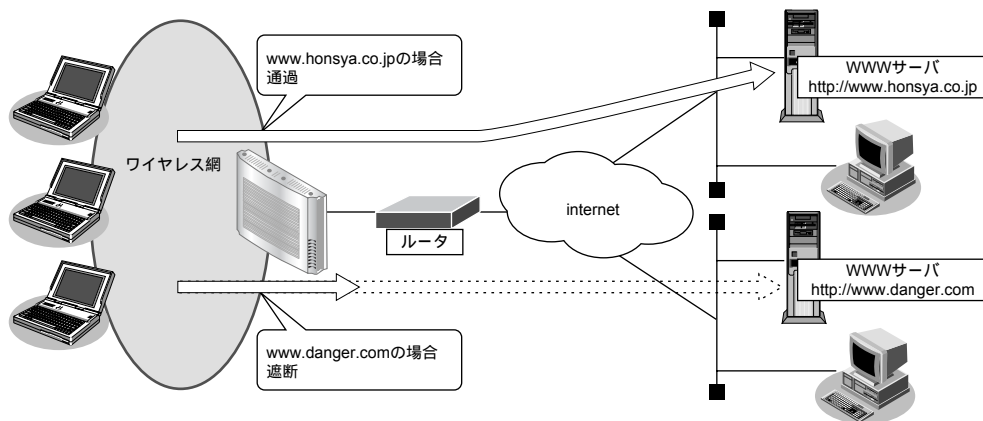
設定方法は、「[10.3 DNS 問い合わせタイプフィルタ機能を使う](#)」(P.107) の「[パソコン側の設定を行う](#)」(P.107) を参照してください。

11 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 全機種

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 機能説明書 [2.14 DNSサーバ機能] (P57)

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 コマンドユーザズガイド [1.7 コマンドで入力できる文字一覧] (P27)

💡 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
```

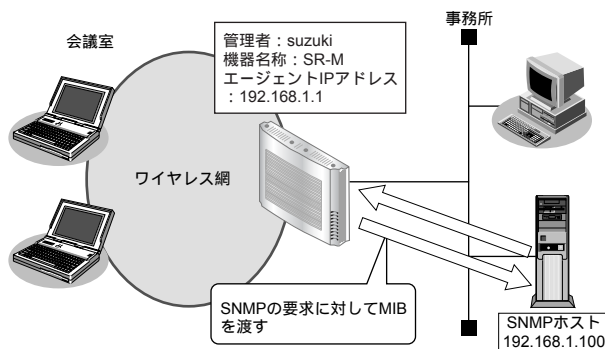
設定終了

```
# save  
# commit
```

12 SNMP エージェント機能を使う

適用機種 全機種

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 機能説明書 [2.15 SNMP機能] (P59)

💡 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 仕様一覧 [3.1 標準 MIB] (P28)、[3.2 富士通拡張 MIB] (P37)、[3.3 Trap 一覧] (P38)

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
```

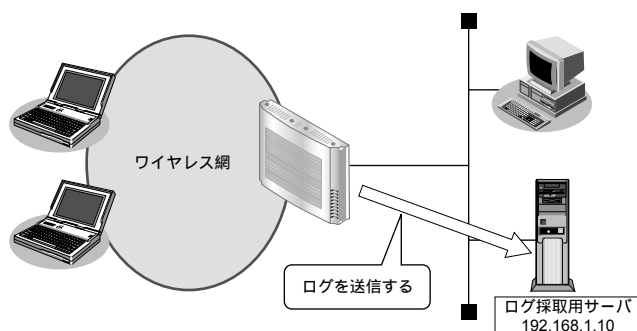
13 システムログを採取する

適用機種 全機種

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。

14 スケジュール機能を使う

適用機種 全機種

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 コマンドユーザズガイド「1.2 時刻を設定する」(P12)

14.1 構成定義情報の切り替えを予約する

適用機種 全機種

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、2010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 : 2010年1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 1001010630 reset config2

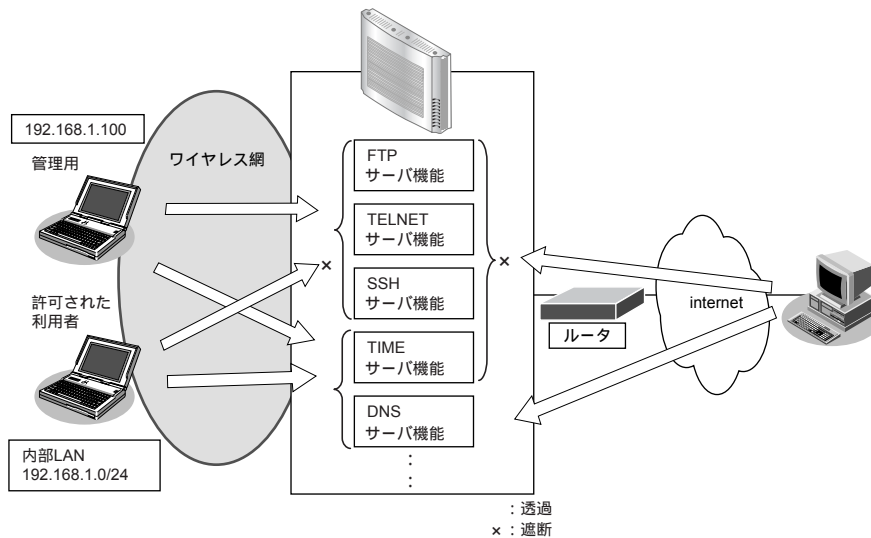
設定終了
# save
# commit
```

15 アプリケーションフィルタ機能を使う

適用機種 全機種

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
```

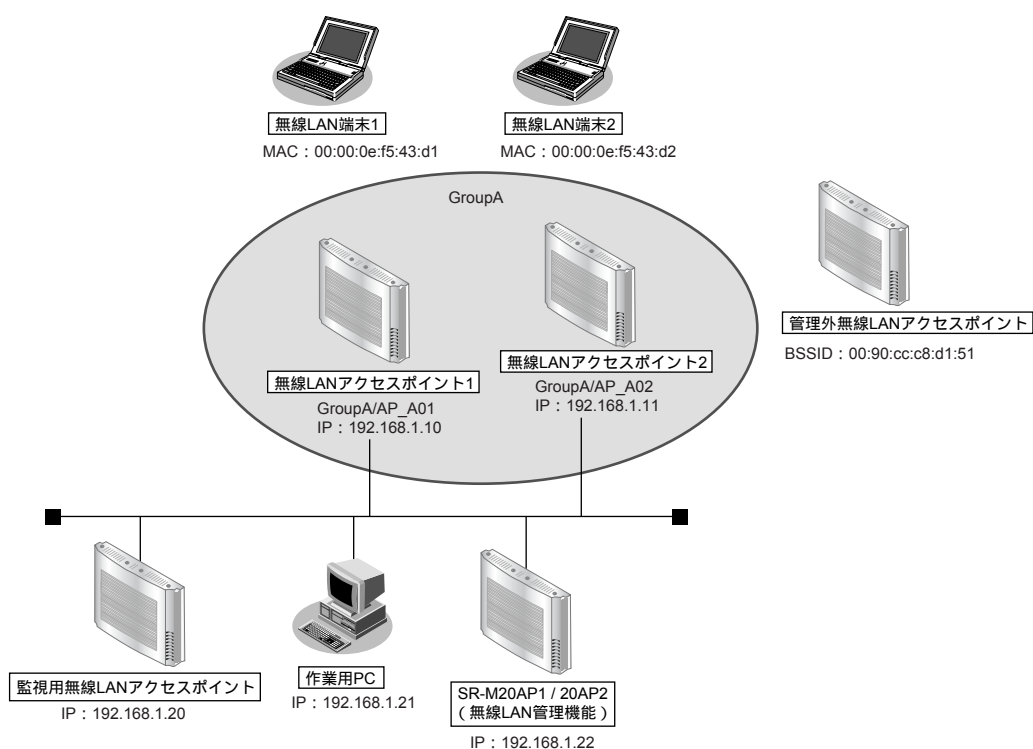
16 無線 LAN 管理機能を使う

適用機種 SR-M20AP1, 20AP2

16.1 無線 LAN 管理機能の環境を設定する

適用機種 SR-M20AP1, 20AP2

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。



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 のチャンネルは、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、「[1.14 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](#)」(P48)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 のチャン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、「[2.1 無線 LAN ネットワークを構築する](#)」(P52)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、[コマンドリファレンス「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、[コマンドリファレンス「パスワード情報」](#)を参照してください)。

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

- 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
```

SR-M20AP1 / 20AP2 (無線 LAN 管理機能) の設定

● コマンド

管理グループを設定する

```
# nodemanager group 0 name GroupA
```

無線 LAN アクセスポイントを設定する

```
# nodemanager node 0 name AP_A01
# nodemanager node 0 group 0
# nodemanager node 0 address 192.168.1.10
# nodemanager node 0 user nodemgr nodemgr1
# nodemanager node 0 wlan scan disable
# nodemanager node 1 name AP_A02
# nodemanager node 1 group 0
# nodemanager node 1 address 192.168.1.11
# nodemanager node 1 user nodemgr nodemgr2
# nodemanager node 1 wlan scan disable
```

監視用無線 LAN アクセスポイントを設定する

```
# nodemanager node 4 name Watcher
# nodemanager node 4 address 192.168.1.20
# nodemanager node 4 user nodemgr nodemgr3
# nodemanager node 4 wlan scan enable
# nodemanager node 4 wlan sta disable
```

管理外無線 LAN アクセスポイントを設定する

```
# nodemanager wlan scan unmanaged 0 UMAP01 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を設定する

```
# nodemanager collect interval 10s 10s 5s
```

有線 LAN、無線 LAN の監視パラメタを設定する

```
# nodemanager icmpwatch interval 10s 10s 5s
# nodemanager icmpwatch threshold 6
# nodemanager wlan scan interval 10s 10s 1m
# nodemanager wlan scan error threshold 6
```

監視ログのパラメタを設定する

```
# nodemanager log 100
```

無線 LAN 端末の RSSI 監視のパラメタを設定する

```
# nodemanager wlan sta rssi 10 20
```

設定終了

```
# save
# commit
```

16.2 アクセスポイントモニタリングを行う

適用機種 SR-M20AP1, 20AP2

無線 LAN 管理機能は、アクセスポイントモニタリングをすることができます。



- モニタリングは各管理機器にアクセスして収集した結果を出力していますので、構成定義の設定直後や、ネットワークの状況によっては収集が完了しておらず、途中の状態が表示される場合があります。この場合は、しばらく時間を置いたあと、再度モニタリング結果を表示してみてください。
- 使用目的が明確で管理不要な無線 LAN アクセスポイントを管理外無線 LAN アクセスポイントとして設定すると、不明無線 LAN アクセスポイントのモニタリングが容易となります。

ここでは、「16.1 無線 LAN 管理機能の環境を設定する」(P.119) で構築した環境に対するアクセスポイントモニタリングのコマンド例を示します。

☛ 参照 各コマンドの表示結果については、「コマンドリファレンス」を参照してください。

● コマンド

管理無線 LAN アクセスポイントのモニタリング結果の一覧を表示する

```
# show nodemanager logging wlan scan managed brief
```

管理無線 LAN アクセスポイントの有線 LAN、無線 LAN のモニタリング結果を表示する

```
# show nodemanager node node 0
```

```
# show nodemanager node node 1
```

管理無線 LAN アクセスポイントの無線 LAN のモニタリング結果を表示する

```
# show nodemanager logging wlan scan managed group 0
```

管理外無線 LAN アクセスポイントのモニタリング結果を表示する

```
# show nodemanager logging wlan scan unmanaged
```

不明無線 LAN アクセスポイントのモニタリング結果を表示する

```
# show nodemanager logging wlan scan unknown
```

監視ログを表示する

```
# show nodemanager logging wlan scan
```

16.3 クライアントモニタリングを行う

適用機種 SR-M20AP1, 20AP2

無線 LAN 管理機能は、無線 LAN アクセスポイントと接続している無線 LAN 端末のクライアントモニタリングをすることができます。



モニタリングは各管理機器にアクセスして収集した結果を出力していますので、構成定義の設定直後や、ネットワークの状況によっては収集が完了しておらず、途中の状態が表示される場合があります。この場合は、しばらく時間を置いたあと、再度モニタリング結果を表示してみてください。

ここでは、「[16.1 無線 LAN 管理機能の環境を設定する](#)」(P.119) で構築した環境に対するクライアントモニタリングのコマンド例を示します。

☛ **参照** 各コマンドの表示結果については、「[コマンドリファレンス](#)」を参照してください。

● コマンド

無線 LAN 端末の受信信号強度のモニタリング結果を表示する

```
# show nodemanager logging wlan sta rssi group 0
```

無線 LAN 端末の接続状況をモニタリングする

```
# show nodemanager logging wlan sta group 0
```

無線 LAN 端末の接続拒否情報をモニタリングする

```
# show nodemanager logging wlan reject group 0
```

無線 LAN インタフェースのトレース情報をモニタリングする

```
# show nodemanager logging wlan trace group 0
```

監視ログを表示する

```
# show nodemanager logging wlan scan
```

16.4 無線 LAN アクセスポイントに MAC アドレスフィルタを配布する (MAC アドレスフィルタ配布)

適用機種 SR-M20AP1, 20AP2

無線 LAN 管理機能は、無線 LAN アクセスポイントへの無線 LAN 端末の (MAC アドレスによる) 接続許可情報を一括管理して配布することができます。

補足 管理機器の MAC アドレスフィルタをクリアしたい場合は、MAC アドレスフィルタを設定していない MAC アドレスフィルタセットを配布してください。

● 設定条件

- 無線 LAN の接続を許可する端末
 - 無線 LAN 端末 1 (MAC アドレス : 00:00:0e:f5:43:d1)
 - 無線 LAN 端末 2 (MAC アドレス : 00:00:0e:f5:43:d2)
- 無線 LAN の接続を拒否する端末
 - 上記以外
- MAC アドレスフィルタの配布先
 - 無線 LAN アクセスポイント 1
 - 無線 LAN アクセスポイント 2

ここでは、「16.1 無線 LAN 管理機能の環境を設定する」(P.119) で構築した環境に対する MAC アドレスフィルタ配布のコマンド例を示します。

参照 各コマンドの実行結果については、「コマンドリファレンス」を参照してください。

● コマンド

```
接続を許可する無線 LAN 端末の MAC アドレスを MAC アドレスフィルタに設定する
# nodemanager wlan filterset 0 filter 0 mac 00:00:0e:f5:43:d1 pass
# nodemanager wlan filterset 0 filter 0 description STATION_001
# nodemanager wlan filterset 0 filter 1 mac 00:00:0e:f5:43:d2 pass
# nodemanager wlan filterset 0 filter 1 description STATION_002
# nodemanager wlan filterset 0 filter 2 mac any reject
```

```
設定完了
# save
# commit
```

```
無線 LAN アクセスポイントに MAC アドレスフィルタを配布する
# nodemanagerctl update wlan filterset 0 group 0
```

16.5 無線 LAN アクセスポイントの電波出力を調整する (電波出力自動調整)

適用機種 SR-M20AP1, 20AP2

無線 LAN 管理機能は、無線 LAN アクセスポイントの電波出力を調整することができます。



近隣管理機器には、電波出力自動調整機能で設定対象の無線 LAN アクセスポイントの無線を到達させたい無線 LAN アクセスポイントを設定します。ただし、電波出力自動調整による送信出力の調整には時間がかかりますので、必要以上に近隣管理機器を設定しないようにしてください。電波出力自動調整は、構成定義で設定した“電波自動調整の RSSI 最低しきい値”に近い値になるまで、以下の処理を繰り返します。

1. 近隣管理機器での周辺アクセスポイント情報の取得
必要時間：約 60 秒×近隣管理機器の台数
2. 電波出力の確認
RSSI 最低しきい値に近い値であれば終了
3. 無線 LAN アクセスポイントの無線送信出力の設定
必要時間：約 10 秒
4. 無線送信出力の安定待ち
必要時間：約 90 秒
5. 手順 1. の処理から繰り返し

こんな事に気をつけて

- 電波出力自動調整は、無線 LAN インタフェースの動作タイプが AP のみ（未設定を含む）で構成される無線 LAN アクセスポイントを対象とするようにしてください。
- 電波出力自動調整の近隣機器には、以下の条件を満たす無線 LAN アクセスポイントを指定してください。
 - 調整対象と同じ無線 LAN モジュールが動作している。
 - その無線 LAN モジュールの動作タイプは、AP、SCANONLY または未設定のみから構成される。
- 電波出力自動調整の実施中は、無線の状態が不安定になる可能性があります。よって、メンテナンスなどの通常運用時以外で電波出力自動調整を行うようにしてください。

● 設定条件

- 電波出力を調整する無線 LAN アクセスポイント
無線 LAN アクセスポイント 1
無線 LAN アクセスポイント 2
- 無線 LAN アクセスポイント 1 の近隣管理機器
無線 LAN アクセスポイント 2、監視用無線 LAN アクセスポイント
- 無線 LAN アクセスポイント 2 の近隣管理機器
無線 LAN アクセスポイント 1、監視用無線 LAN アクセスポイント
- 電波出力自動調整の RSSI の最低しきい値 : 20

ここでは、「16.1 無線 LAN 管理機能の環境を設定する」(P.119) で構築した環境に対する電波出力自動調整のコマンド例を示します。

参照 各コマンドの実行結果については、「コマンドリファレンス」を参照してください。

● コマンド

近隣管理機器を設定する

```
# nodemanager node 0 wlan neighbor 1 4
```

```
# nodemanager node 1 wlan neighbor 0 4
```

電波出力自動調整のRSSIの最低しきい値を設定する

```
# nodemanager wlan autotxpower rssi 20
```

設定完了

```
# save
```

```
# commit
```

電波出力自動調整を行う

```
# nodemanagerctl wlan autotxpower group 0
```

16.6 無線 LAN アクセスポイントの無線 LAN チャンネルを調整する

適用機種 SR-M20AP1, 20AP2

無線 LAN 管理機能は、無線 LAN アクセスポイントの無線 LAN チャンネルを自動的に調整することができます。

こんな事に気をつけて

無線 LAN チャンネル自動調整の実施中は、無線の状態が不安定になる可能性があります。よって、メンテナンスなどの通常運用時以外で無線 LAN チャンネル自動調整を行うようにしてください。

● 設定条件

- 5GHz 帯のチャンネル自動調整の割り当て範囲 : w52/53/56
- 2.4GHz 帯のチャンネル自動調整の判定用 RSSI しきい値 : 20
- 2.4GHz 帯のチャンネル自動調整のレイアウト
 - 開始チャンネル : 1
 - チャンネル割り当て間隔 : 5
- IEEE802.11n 通信時に使用する帯域幅 : 40

ここでは、「16.1 無線 LAN 管理機能の環境を設定する」(P.119) で構築した環境に対する無線 LAN チャンネル自動調整のコマンド例を示します。

☞ **参照** 各コマンドの実行結果については、「[コマンドリファレンス](#)」を参照してください。

● コマンド

```
5GHz 帯のチャンネル自動調整の割り当て範囲を設定する
# nodemanager wlan autochannel channel w52/53/56

2.4GHz 帯のチャンネル自動調整の判定用 RSSI しきい値を設定する
# nodemanager wlan autochannel rssi 20

2.4GHz 帯のチャンネル自動調整のレイアウトを設定する
# nodemanager wlan autochannel layout 1 5

IEEE802.11n 通信時の通信帯域幅を設定する
# nodemanager wlan autochannel bandwidth 40

設定終了
# save
# commit

無線 LAN アクセスポイントの使用チャンネルを自動調整する
# nodemanagerctl wlan autochannel group 0
```


索引

A

| | |
|-----------------------|--------|
| Access Category | 43, 70 |
| ACL 番号 | 79 |

D

| | |
|------------------------------|-----|
| DHCP 機能 | 101 |
| DHCP クライアント機能 | 101 |
| DNS サーバ機能 | 108 |
| DNS サーバの自動切り替え機能 (逆引き) | 106 |
| DNS サーバの自動切り替え機能 (順引き) | 104 |
| DNS 問い合わせタイプフィルタ機能 | 107 |

I

| | |
|-----------------------|--------|
| IEEE802.11n | 10, 54 |
| IEEE802.1X 認証機能 | 85 |
| IP アドレス | 80 |

M

| | |
|-------------------------|-----|
| MAC アドレス認証機能 | 95 |
| MAC アドレスフィルタ配布 | 125 |
| MAC アドレスフィルタリング機能 | 39 |
| MIB | 112 |

P

| | |
|----------------|-----|
| ProxyDNS | 104 |
|----------------|-----|

S

| | |
|---------------------|-----|
| SNMP | 112 |
| SNMP エージェント機能 | 112 |

U

| | |
|------------------|-----|
| URL フィルタ機能 | 110 |
|------------------|-----|

V

| | |
|---------------|----|
| VLAN 管理 | 17 |
| VLAN 機能 | 74 |

W

| | |
|----------------------|--------|
| Wake On LAN 機能 | 93, 99 |
| WDS ブリッジ機能 | 29, 34 |
| WMM 機能 | 41, 68 |

あ

| | |
|----------------------|-----|
| アクセスポイントモニタリング | 123 |
| アドレスマスク | 80 |
| アプリケーションフィルタ機能 | 117 |

か

| | |
|------------------|----|
| 仮想アクセスポイント | 12 |
|------------------|----|

き

| | |
|-----------|-----|
| 逆引き | 106 |
|-----------|-----|

く

| | |
|--------------------|-----|
| クライアントモニタリング | 124 |
|--------------------|-----|

こ

| | |
|--------------------|-----|
| 構成定義情報切り替え予約 | 116 |
|--------------------|-----|

し

| | |
|----------------------|--------|
| システムログ | 115 |
| システムログの確認 | 115 |
| 周辺アクセスポイント検出機能 | 46, 48 |
| 順引き | 104 |

す

| | |
|------------------|-----|
| スイッチング HUB | 74 |
| スケジュール機能 | 116 |

せ

| | |
|--------------|----|
| 制御 | 79 |
| セキュリティ | 79 |

た

| | |
|------------------|----|
| タグ VLAN 機能 | 75 |
| 端末台数最低保証機能 | 27 |
| 端末台数制限機能 | 25 |

ち

| | |
|---------------------|--------|
| チャンネルボンディング機能 | 50, 72 |
|---------------------|--------|

て

| | |
|----------------|-----|
| 電波出力自動調整 | 126 |
|----------------|-----|

と

ドメイン 104

に

認証・暗号化 56

は

バックアップポート機能 76

ふ

フィルタリング機能 79

フィルタリングの条件 79

フィルタリングの設計方針 80

複数アクセスポイント 22

ほ

ポート VLAN 機能 74

ホストデータベース 108

ま

マニュアル構成 7

む

無線 LAN 管理機能 119

無線 LAN 機能 8, 52

無線 LAN チャンネルの自動調整 128

無線 LAN 中継機能 65

無線 LAN ネットワーク 8, 52

無線通信 8

ゆ

優先順位 80

り

リンクインテグリティ機能 77

ろ

ローミング機能 66

SR-M コマンド設定事例集

P3NK-4192-03Z0

発行日 2014年8月

発行責任 富士通株式会社

- 本書の一部または全部を無断で他に転載しないよう、お願いいたします。
- 本書は、改善のために予告なしに変更することがあります。
- 本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、損害については、弊社はその責を負いません。