P3NK-4142-03Z0

FUJITSU Network SR-M
機能説明書

V02

FUJITSU

はじめに

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

2010年 4月初版
2013年 7月第2版
2014 年 8月第3版

目次

本書の構成と使いかた

本書では、一般的なネットワークの概要や本装置で使用できる便利な機能について説明しています。
また、CD-ROM の中の 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。

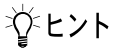
本書の構成

以下に、本書の構成と各章の内容を示します。

章タイトル	内　容
第 1 章　ネットワーク設計概念	この章では、一般的な IP ネットワークの設計概念について説明します。
第 2 章　機能概要	この章では、本装置の主な機能の概要を説明します。

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。



本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。

こんな事に気をつけて　本装置をご使用になる際に、注意していただきたいことを説明しています。

操作手順で説明しているもののほかに、補足情報を説明しています。

操作方法など関連事項を説明している箇所を示します。

本装置の機能を使用する際に、対象となる機種名を示します。

製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。

製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

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	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。

使用許諾条件

本製品には、カリフォルニア大学およびそのコントリビュータによって開発され、下記の使用条件とともに配付されているFreeBSDの一部が含まれています。
#　@(#)COPYRIGHT　8.2 (Berkeley) 3/21/94

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase "this text" refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase "This material" refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

本製品には、カリフォルニア大学バークレイ校において開発されたソフトウェアが含まれています。

Copyright © 1989 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

本製品には、スタンフォード大学よって開発され、下記の使用条件とともに配布されている mrouted の一部が含まれています。

The mrouted program is covered by the following license. Use of the mrouted program represents acceptance of these terms and conditions.

1. STANFORD grants to LICENSEE a nonexclusive and nontransferable license to use, copy and modify the computer software "mrouted" (hereinafter called the "Program"), upon the terms and conditions hereinafter set out and until Licensee discontinues use of the Licensed Program.
2. LICENSEE acknowledges that the Program is a research tool still in the development state, that it is being supplied "as is," without any accompanying services from STANFORD, and that this license is entered into in order to encourage scientific collaboration aimed at further development and application of the Program.
3. LICENSEE may copy the Program and may sublicense others to use object code copies of the Program or any derivative version of the Program. All copies must contain all copyright and other proprietary notices found in the Program as provided by STANFORD. Title to copyright to the Program remains with STANFORD.
4. LICENSEE may create derivative versions of the Program. LICENSEE hereby grants STANFORD a royalty-free license to use, copy, modify, distribute and sublicense any such derivative works. At the time LICENSEE provides a copy of a derivative version of the Program to a third party, LICENSEE shall provide STANFORD with one copy of the source code of the derivative version at no charge to STANFORD.
5. STANFORD MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED.By way of example, but not limitation, STANFORD MAKES NO REPRESENTATION OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED PROGRAM WILL NOT INFRINGE ANY PATENTS,COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. STANFORD shall not be held liable for any liability nor for any direct, indirect or consequential damages with respect to any claim by LICENSEE or any third party on account of or arising from this Agreement or use of the Program.
6. This agreement shall be construed, interpreted and applied in accordance with the State of California and any legal action arising out of this Agreement or use of the Program shall be filed in a court in the State of California.
7. Nothing in this Agreement shall be construed as conferring rights to use in advertising, publicity or otherwise any trademark or the name of "Stanford".
The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

本製品には、南カリフォルニア大学およびそのコントリビュータによって開発され、下記の使用条件とともに配布されている pimd の一部が含まれています。

Copyright (c) 1998-2001
University of Southern California/Information Sciences Institute.All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

$Id: LICENSE,v 1.5 2001/09/10 20:31:36 pavlin Exp $
Part of this program has been derived from mrouted.
The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

本製品には、オレゴン大学によって開発され、下記の使用条件とともに配布されている pimdd の一部が含まれています。

Copyright (c) 1998 by the University of Oregon.All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials,and other materials related to such distribution and use acknowledge that the software was developed by the University of Oregon.The name of the University of Oregon may not be used to endorse or promote products derived from this software without specific prior written permission.

THE UNIVERSITY OF OREGON DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING,

WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

IN NO EVENT SHALL UO, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT,TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH,THE USE OR PERFORMANCE OF THIS SOFTWARE.

Other copyrights might apply to parts of this software and are so noted when applicable.

Questions concerning this software should be directed to Kurt Windisch (kurtw@antc.uoregon.edu)

$Id: LICENSE,v 1.2 1998/05/29 21:58:19 kurtw Exp $

Part of this program has been derived from PIM sparse-mode pimd.
The pimd program is covered by the license in the accompanying file named "LICENSE.pimd".

The pimd program is COPYRIGHT 1998 by University of Southern California.

Part of this program has been derived from mrouted.

The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

Copyright (c) 1998 by the University of Southern California.All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials,and other materials related to such distribution and use acknowledge that the software was developed by the University of Southern California and/or Information Sciences Institute.
The name of the University of Southern California may not be used to endorse or promote products derived from this software without specific prior written permission.

THE UNIVERSITY OF SOUTHERN CALIFORNIA DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

IN NO EVENT SHALL USC, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT,TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH,THE USE OR PERFORMANCE OF THIS SOFTWARE.

Other copyrights might apply to parts of this software and are so noted when applicable.

Questions concerning this software should be directed to Pavlin Ivanov Radoslavov (pavlin@catarina.usc.edu)

$Id: LICENSE.pimd,v 1.1 1998/05/29 21:58:20 kurtw Exp $

Part of this program has been derived from mrouted.
The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

本製品には、RSA Data Security社が著作権を有しているMD5 Message-Digest Algorithmが含まれています。

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

本製品には、Eric Young 氏 (eay@cryptsoft.com) によって記述された暗号ソフトウェアが含まれています。

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

本製品には、OpenSSL ツールキットを使用するために OpenSSL Project (http://www.OpenSSL.org/) によって開発されたソフトウェアが含まれています。

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact licensing@OpenSSL.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

本製品には、Atsushi Onoe 氏、Video54 Technologies 社、Sam Leffler 氏および Errno Consulting 社によって記述された、以下の使用許諾に基づくソフトウェアが含まれています。

本製品には、Damien Bergamini 氏によって記述された、以下の使用許諾に基づくソフトウェアが含まれています。

本製品には、David Young 氏によって記述された、以下の使用許諾に基づくソフトウェアが含まれています。

本製品には、Jouni Malinen 氏、Sam Leffler 氏、Instant802 Networks 社および Devicescape Software 社によって記述された、以下の使用許諾に基づくソフトウェアが含まれています。

第1章 ネットワーク設計概念

この章では、一般的なIPネットワークの設計概念について説明します。

1.1　レイヤ 2 ネットワーク設計概念

適用機種　*SR-M20AP1, 20AP2*

1.1.1　VLAN

レイヤ 2 のネットワークは、MAC アドレスをもとに到達する先を制御します。レイヤ 2 のネットワークでは、VLAN と呼ばれる論理的なネットワークから構成されます。VLAN を使って複数の物理的な LAN から 1 つの論理的な LAN に構成したり、物理的に 1 つの LAN を複数の論理的な LAN に分けたりします。各 VLAN には VLAN ID（VID）をつけて管理します。

VLAN ID

各 VLAN には 10 進数で 1 から 4094 までの番号をつけて管理します。これを VLAN ID と言います。同じ VLAN ID を持つ VLAN に属している装置間では通信可能ですが、異なる VLAN ID を持つ VLAN に属している装置間では通信はできません。

VLAN の種類

SR-M20AP1 / 20AP2 の VLAN には以下の 2 つの種類があります。

- ポート VLAN
  ETHER ポートごとに「どの VLAN に所属するか」を設定するものです。
  その ETHER ポートのデータは、すべて指定された VLAN に属します。
- タグ VLAN
  1 つの物理回線上に複数の VLAN を設定する場合に使用します。IEEE802.1Q で標準化された方式で、VLAN ヘッダを Ethernet のフレームヘッダに挿入することによって、1 つの物理回線上に複数の VLAN を実現します。

この 2 つの種類は ETHER ポートごとに設定を変えることができます。つまり、VLAN ID が 10 の VLAN を、ETHER ポート 1 ではポート VLAN、ETHER ポート 2 ではタグ VLAN にするといったことができます。この場合、VLAN ID が 10 の VLAN のデータは、ETHER ポート 1 と ETHER ポート 2 で送受信され、ETHER ポート 1 ではタグのない通常のフレーム、ETHER ポート 2 ではタグ付きのフレームとして送受信されます。

1.2　本装置の設定の概要

適用機種　全機種

ネットワークと設定の関係

本装置に設定すべき情報としては、接続する回線に関する物理的な情報、接続するネットワークに関する論理的な情報、およびデータの振り分け条件である経路情報が必ず必要となります。また、ほかに装置固有の情報や、付加的なサービスの設定を必要に応じて行います。

本装置では、これらの情報の設定に関して、大きく以下のように分類しています。

- ether 定義
  本装置に接続する回線に関する物理的な情報を定義する命令群です。回線の種類や速度などに関する情報を定義します。
- ieee80211 定義
  本装置の無線 LAN に関する物理的な情報を定義する命令群です。無線 LAN の通信モード（IEEE802.11a/b/g/n）やチャネルなどに関する情報を定義します。
- wlan 定義
  本装置の無線 LAN インタフェースに関する情報を定義する命令群です。無線 LAN インタフェースごとに動作タイプ（アクセスポイント、WDS、スキャン専用）、SSID、認証・暗号化方式などに関する情報を定義します。
- vlan 定義（SR-M20AP1 / 20AP2 のみ）
  SR-M20AP1 / 20AP2 の VLAN に関する情報を定義する命令群です。静的な学習テーブルの情報などを定義します。
- lan 定義
  本装置に接続する LAN に関する論理的な情報を定義する命令群です。LAN の IP アドレスやネットワークの情報などを定義します。また、DHCP などの LAN に固有のサービスに関しても lan 定義によって定義します。
- その他の定義
  装置固有の情報や付加サービスの情報を必要に応じて定義する命令群です。ネットワーク管理に関する情報や時刻情報などの定義があります。

ネットワークインタフェースの定義

データ転送時の出口となるネットワークインタフェースには、その特性や接続されている回線によっていくつかの種別があります。

以下に、ネットワークインタフェースの種別について説明します。

- lo
  ループバックインタフェース
  装置の内部プログラムで折り返し通信を行う場合に利用されます。
- lan
  IP インタフェース
  IP を利用して通信する場合に利用するネットワークインタフェースです。lan 定義によって設定されます。

これらのインタフェース種別にインタフェース番号を付与したものがネットワークインタフェース名となります。

例：lo0,lan0,lan1,...

lan のネットワークインタフェースは lan 定義によって設定されます。lan 定義の定義番号とネットワークインタフェースのインタフェース番号は 1 対 1 に対応します。

経路情報の定義

経路情報は最終的に出口となるネットワークインタフェースを決定するために必要な情報を定義するものです。本装置では出口インタフェースに対応する定義内で経路情報を設定します。たとえば、lan0 から出力するための経路情報は lan0 内の定義に、lan1 から出力するための経路情報は lan1 内の定義に分けて設定します。

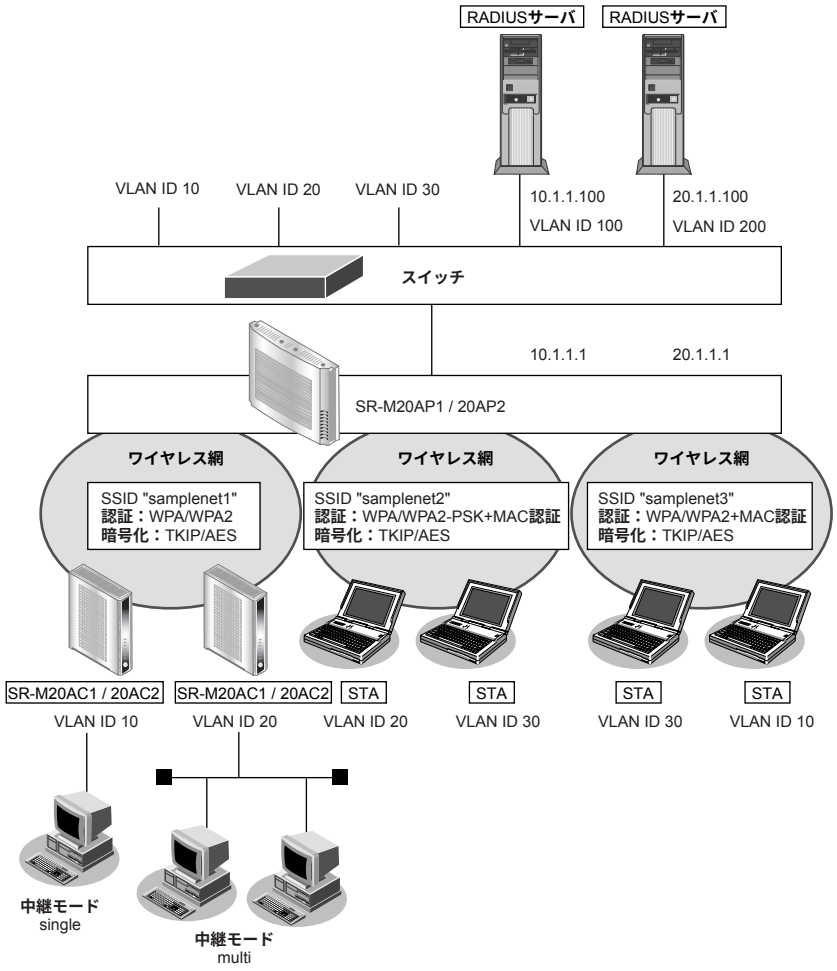
第２章　機能概要

この章では、本装置の主な機能の概要を説明します。

2.1　無線 LAN 機能

適用機種　全機種

IEEE802.11 に準拠した無線 LAN アクセスポイント動作、および、無線 LAN ステーション動作を行うことができます。



無線 LAN インタフェースでは、以下の動作をサポートしています。

○：対応している、-：対応していない

動作	SR-M20AP1 / 20AP2	SR-M20AC1 / 20AC2
アクセスポイント	○	-
ステーション	-	○

2.1.1　無線 LAN 通信規格

適用機種　全機種

IEEE802.11 準拠する以下の無線 LAN 通信規格をサポートします。
本装置は各規格での Wi-Fi 認定を取得しています。本装置に接続する機器は、相互接続性を確保するため Wi-Fi 認定を取得済みの機器とすることを推奨します。

- IEEE802.11b（1-14ch）
- IEEE802.11g（1-13ch）
- IEEE802.11a（W52：36/40/44/48ch）
- IEEE802.11a（W53：52/56/60/64ch）
- IEEE802.11a（W56：100/104/108/112/116/120/124/128/132/136/140ch）
- IEEE802.11n（2.4GHz）（1-13ch）
- IEEE802.11n（5GHz）（W52：36/40/44/48ch）
- IEEE802.11n（5GHz）（W53：52/56/60/64ch）
- IEEE802.11n（5GHz）（W56：100/104/108/112/116/120/124/128/132/136/140ch）

参照　コマンド設定事例集
「1.1 無線 LAN ネットワークを構築する」（P.8）、「1.2 無線 LAN ネットワークを構築する（IEEE802.11n）」（P.10）、
「2.1 無線 LAN ネットワークを構築する」（P.52）、「2.2 無線 LAN ネットワークを構築する（IEEE802.11n）」（P.54）

2.1.2　認証・暗号化機能

適用機種　全機種

無線 LAN 機能として IEEE802.11 標準の以下の認証・暗号化方式をサポートします。

補足
- SR-M20AC1 / 20AC2 では、PKI 証明書を使った IEEE802.1X 認証が併用できます。
- AES 暗号化は、ハードウェアによる暗号化を行います。

認証種別	認証方式	EAP プロトコル	EAP プロトコル内部認証	暗号化方式
OPEN 認証	-	-	-	
	IEEE802.1X 連携	MD5	-	
		TLS	-	WEP64, WEP128, なし
		TTLS	MSCHAPv2, PAP, CHAP	（SR-M20AC1 / 20AC2 は静的 WEP のみ）
		PEAP0	MSCHAPv2	
		PEAP1	MSCHAPv2	
SHARED 認証	共通鍵認証	-	-	
	IEEE802.1X 連携	MD5	-	
		TLS	-	WEP64, WEP128
		TTLS	MSCHAPv2, PAP, CHAP	（静的 WEP のみ）
		PEAP0	MSCHAPv2	
		PEAP1	MSCHAPv2	

認証種別	認証方式	EAP プロトコル	EAP プロトコル内部認証	暗号化方式
WPA 認証	事前共有キー認証	-	-	
	IEEE802.1X 連携	TLS	-	
		TTLS	MSCHAPv2, PAP, CHAP	TKIP, AES
		PEAP0	MSCHAPv2	
		PEAP1	MSCHAPv2	
WPA2 認証	事前共有キー認証	-	-	
	IEEE802.1X 連携	TLS	-	
		TTLS	MSCHAPv2, PAP, CHAP	TKIP, AES
		PEAP0	MSCHAPv2	
		PEAP1	MSCHAPv2	

こんな事に気をつけて

IEEE802.11n 通信を行うときは、wlan wpa cipher コマンドの WPA/WPA2 暗号化モード設定は、auto（TKIP または AES で自動判別）または aes（AES 暗号化）を指定してください。
また、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。

参照 コマンド設定事例集
「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」（P.17）、
「2.3 無線 LAN ネットワークで認証・暗号化する」（P.56）

2.1.3　SSID 非通知（ステルス機能）

適用機種 ***SR-M20AP1, 20AP2***

SSID 非通知は、無線 LAN の不正利用を防ぐための処置の 1 つで、ステルス機能と呼ばれます。

無線 LAN アクセスポイントから送信されるビーコンの中には SSID が含まれているため、電波が届く範囲にある無線 LAN 端末がビーコンを受信することで、無線 LAN アクセスポイントの存在と SSID を知ることができます。

第三者が無断で SSID を設定して使用してしまう危険性を少なくするため、ビーコンに SSID を含めないようにすることで無線 LAN アクセスポイントの存在を隠蔽することができます。

補足 SSID 非通知を有効にすると ANY 接続拒否が同時に動作します。

2.1.4　ANY 接続拒否（ANY キープロテクション）

適用機種 ***SR-M20AP1, 20AP2***

任意の無線 LAN アクセスポイントにも接続できる「ANY」接続という SSID を指定しない接続方法があり、無線 LAN 端末が SSID を指定しないで「ANY」とすることで周辺の無線 LAN アクセスポイントに接続できます。

このようなしくみを逆手にとり悪意のある第三者が無線 LAN を不正利用する危険性を少なくするため、「ANY」で接続を行おうとする無線 LAN 端末を接続拒否することができます。

補足 SSID 非通知を有効にすると同時に動作します。

2.1.5　MACアドレスフィルタ

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。

☛ 参照　コマンド設定事例集「1.10 MACアドレスフィルタリング機能を使う」（P.39）

2.1.6　端末台数制限／端末台数最低保証

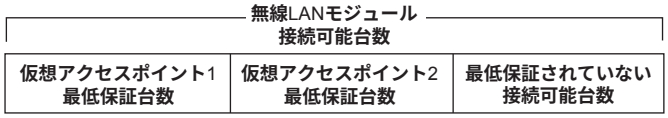
適用機種　***SR-M20AP1, 20AP2***

無線LAN端末の接続台数過多により発生する通信品質の低下などを防止するため、無線LANモジュールごとに無線LAN端末の接続台数を制限することができます。

また、仮想アクセスポイントを構築する場合に、接続台数の制限により保守用などの端末が接続不可となることがないように、仮想アクセスポイントごとに接続可能な無線LAN端末の台数を保証することができます。

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。**
- **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。**



☛ 参照　「2.1.9 仮想アクセスポイント機能（VAP）」（P.26）、
コマンド設定事例集
「1.6 端末台数制限機能を使う」（P.25）、
「1.7 端末台数最低保証機能を使う」（P.27）

2.1.7　WDS ブリッジ機能

適用機種　***SR-M20AP1, 20AP2***

WDS（Wireless Distribution System）ブリッジは、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。

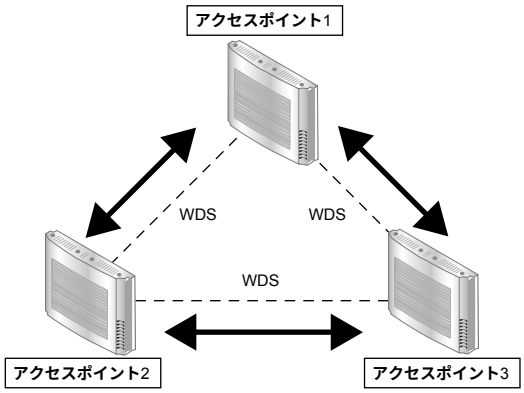
SR-M20AP1 / 20AP2 では WDS ブリッジのみで無線 LAN ネットワークを構築することができます。

こんな事に気をつけて

- **相手無線 LAN アクセスポイントと同じチャネル、通信モードで動作させてください。また、WDS のみで運用する場合、any 以外のチャネルを設定してください。**
- **WDS ブリッジの相手側無線 LAN インタフェースの MAC アドレスは正確に設定してください。**
  なお、SR-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 チャネルが W53/W56 で動作している場合、レーダを検出することがあります。レーダを検出した場合、チャネルが自動的に切り替わり、一時的に通信ができなくなるときがあります。WDS のみで運用している場合は、チャネルの切り替えは行われません。レーダを検出したチャネルは 30 分間使用することができないため、WDS のみで運用している場合は、レーダ検出後 30 分間動作を停止します。**
- **WDS を利用した以下の図のような冗長なネットワーク構成では、無線 LAN 上でのパケットのループが発生するため、このようなネットワーク構成は取らないでください。**



- **WDS ブリッジを行う無線 LAN アクセスポイント間では、IEEE802.11n 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。**

☛ 参照 コマンド設定事例集
「1.8 WDS ブリッジ機能を使う」（P.29）、
「1.9 VLAN ネットワークを WDS ブリッジ機能で接続する」（P.34）

2.1.8　プライバシープロテクション機能（AP ブリッジ）

適用機種　***SR-M20AP1, 20AP2***

プライバシープロテクションは、無線 LAN アクセスポイント内部でブリッジ（無線 LAN 端末間）を無効にする機能です。

同じ無線 LAN アクセスポイントに接続している無線 LAN 端末はお互いに通信できますが、プライバシープロテクション機能を利用する場合は、無線 LAN 端末間の通信をフィルタリングすることができます。

ほかの無線 LAN 端末からの個人情報の盗み見や共有フォルダへのアクセスを防御でき、ホットスポットサービスなどの不特定多数の利用者が存在する環境で各利用者のプライバシーを保護します。

本機能は仮想アクセスポイント利用時にも動作可能です。

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。

2.1.9　仮想アクセスポイント機能（VAP）

適用機種　***SR-M20AP1, 20AP2***

本装置では、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、無線 LAN インタフェースおよび有線 LAN インタフェースに対し、VLAN 機能を使うことによって、無線 LAN 端末のパケットを、有線 LAN 側に中継することができます。

無線 LAN ネットワークは無線 LAN インタフェースごとに定義でき、各無線 LAN インタフェースは仮想アクセスポイント（VAP）として使用することができます。仮想アクセスポイントには、同一または異なる SSID を割り当てることができ、また、異なるセキュリティポリシーを設定することができます。

仮想アクセスポイントに無線 LAN 端末が接続された際、パケットの中継に必須となる VLAN ID を割り当てる方式として、SR-M20AP1 / 20AP2 では固定 VLAN 割り当て方式および認証 VLAN 割り当て方式をサポートします。また、複数の仮想アクセスポイントに対する同一 VLAN の固定割り当ても可能です。

- 固定 VLAN 割当方式
  VAP に対してあらかじめ固定の VLAN ID を設定しておくことで、端末が接続された場合にその VLAN を固定的に割り当てる方式です。
  同一の VLAN が設定されたインタフェースに対してのみブリッジ中継が行われるため、無線 LAN に接続された端末を、仮想アクセスポイント（VAP）単位に VLAN を振り分けることができます。
- 認証 VLAN 割当方式
  IEEE802.1X や MAC アドレス認証を経て接続された端末に対して、RADIUS サーバから払い出された VLANID を割り当てる方式で、無線 LAN 端末単位に VLAN を振り分けることができます。
  VLANID は認証ごとに更新可能であり、払い出しがない場合は認証機能に設定された初期 ID を割り当てます。

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。

☛ 参照　コマンド設定事例集
「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」（P.12）、
「1.5 同一 SSID の複数アクセスポイントを構築する」（P.22）

2.1.10　WMM 機能（IEEE802.11e）

適用機種　全機種

WMM は、無線 LAN インタフェース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 種類の優先クラス Access Category（AC）に分類し、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、無線 LAN モジュールでは AC ごとに送信キューを持ち、送信キューにパケットが溜まっている場合は、優先度が高い AC の送信キューから優先的にパケットが送信されます。

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。**
- **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。**

本装置では振り分けに利用する DSCP 値は 6bit のうち先頭 3bit を参照し、以下の表に従って分類します。

また、ACL を利用することで特定パケットに対する優先クラスを任意に変更することもできます。

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

参照　コマンド設定事例集
「1.11 WMM 機能を使う」（P.41）、
「1.12 WMM 機能の Access Category 分類条件を変更する」（P.43）、
「2.6 WMM 機能を使う」（P.68）、「2.7 WMM 機能の Access Category 分類条件を変更する」（P.70）

2.1.11　ローミング機能

適用機種　***SR-M20AC1, 20AC2***

ローミングとは、無線 LAN 端末が複数の無線 LAN アクセスポイント間を移動することを可能にする機能です。

無線 LAN 端末が無線 LAN アクセスポイントの通信エリア外に移動した場合、別の無線 LAN アクセスポイントに接続を自動的に切り替えることで通信を維持しようとします。たとえば、ビルの各フロアに無線 LAN アクセスポイントを設置しておくことで、無線 LAN 端末がフロア間を移動しても設定の変更を意識することなくネットワークにアクセスすることができます。

補足　SR-M20AC1 / 20AC2 では、ビーコン受信タイムアウト検出／受信信号強度のしきい値／送信レートのしきい値により、ローミングすることができます。

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（デフォルト 5 分間隔）にスキャンします。このスキャンは全チャ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ネルがあらかじめ判明している場合は、スキャンチャネルリストでスキャンするチャネルを限定することをお勧めします。

参照　コマンド設定事例集「2.5 ローミング機能を使う」（P.66）

2.1.12　PMK キャッシュ機能

適用機種　全機種

PMK キャッシュ機能は、無線 LAN 接続時に利用される PMK（暗号鍵のマスター）を、無線 LAN アクセスポイント、無線 LAN 端末双方がキャッシュしておき、接続の際にキャッシュが一致した場合に IEEE802.1X 認証を省略とすることで、無線 LAN 端末の「再接続」に要する接続時間の短縮を可能とする機能です。

2.1.13　無線 LAN 中継機能

適用機種　***SR-M20AC1, 20AC2***

SR-M20AC1 / 20AC2 では、有線 LAN と無線 LAN 間をブリッジすることで、有線 LAN に接続された端末のパケットを、無線 LAN に中継することができます。無線 LAN インタフェースを搭載することができない PC やプリンタなどの端末を SR-M20AC1 / 20AC2 の有線 LAN に収容することで、新しく無線 LAN 対応 PC やプリンタなどの端末を購入しないで、簡単に無線 LAN ネットワークを構築することができます。

有線 LAN 側には 1 台の端末を収容するモードとスイッチを併用して、複数台の端末を収容するモードがあります。

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。

参照　コマンド設定事例集「2.4 無線 LAN 中継機能を使う」（P.65）

2.1.14　周辺アクセスポイント検出機能

適用機種　全機種

無線電波をスキャンすることにより、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。

ネットワークに不正（想定外）なアクセスポイントが存在すると通信に異常が起こることがあり、定期的に周辺アクセスポイントの状況を把握することで未然に問題を防ぐことができます。

- SR-M20AP1 / 20AP2

  手動スキャン、および自動スキャンによる周辺アクセスポイント検出が行えます。
  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を検出することができます。
  自動スキャンには、運用中スキャンモード、スキャン専用モードがあります。

  各モードについて以下に説明します。

  運用中スキャンモード

  無線 LAN アクセスポイントの運用をしながら無線電波をスキャンすることで、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。検出は現在運用中のチャネルだけで行います。
  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。
  また、電波干渉により近隣チャネルで動作している無線 LAN アクセスポイントも検出されることがあります。

  スキャン専用モード

  無線 LAN アクセスポイントの運用をしないでスキャン動作だけを行います。周辺の無線 LAN アクセスポイントを無線 LAN モジュールで利用可能なすべてのチャネルで検出することができます。
  レーダ検出などにより利用不可中のチャネルは検出の対象外となります。

こんな事に気をつけて

- **無線 LAN アクセスポイントの運用では、スループットが低下することがあります。**
- **電波干渉により近隣チャネルで動作している無線 LAN アクセスポイントも検出されることがあります。**
- **スキャン専用モードで使用する場合、無線 LAN 端末との接続はできません。**
- **レーダ検出などにより利用不可中のチャネルは検出の対象外となります。**

☛ 参照　コマンド設定事例集
「1.13 周辺アクセスポイント検出機能を使う」（P.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」（P.48）

- SR-M20AC1 / 20AC2

  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を検出することができます。

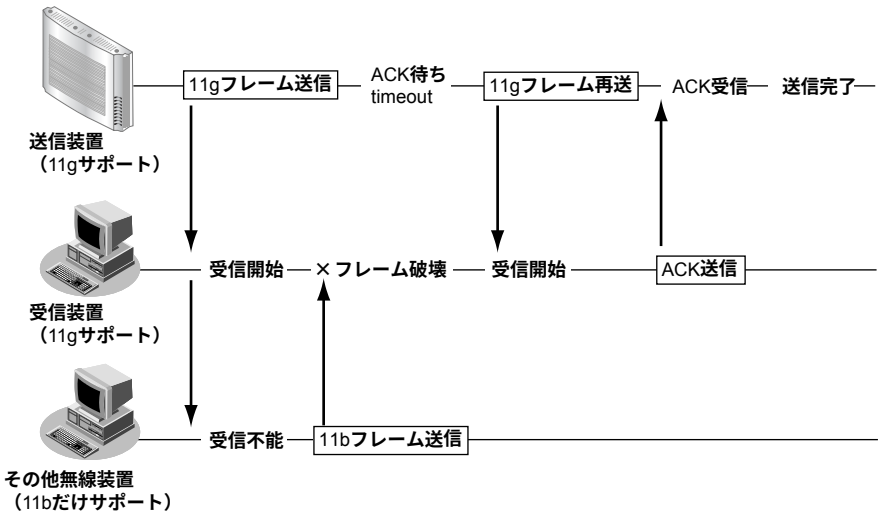
2.1.15　11g プロテクション機能

適用機種　全機種

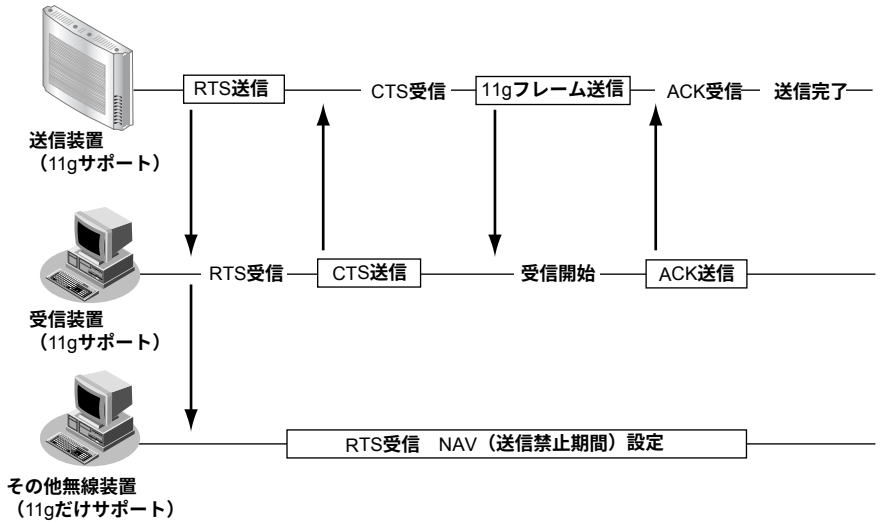
11g プロテクションとは、11b と 11g の装置が混在する環境で通信した場合に発生する、スループットの低下を抑止する機能です。

11b の装置は 11g での通信を理解できないため、11g の通信中に通信フレームを送信してしまう場合があります。この場合、フレーム破壊により通信がエラーとなり、再送が発生して結果 11g の装置のスループットが低下します。これを防ぐため、11g での通信に先立って、11b の装置が理解できる RTS または CTS-to-self のフレームを送信する機能が 11g プロテクションです。11b の装置に対し、RTS および CTS-to-self によってキャリアの占有時間を通知し、11g の通信が行われる間 11b の通信を抑止することで、11g の通信を保護することができます。

例）干渉が発生している場合



例）RTS/CTSでプロテクションを動作させた場合



こんな事に気をつけて

11g プロテクションを動作させた場合、11g の通信の前には RTS/CTS または CTS-to-self のフレームが付加されるため、動作させていない場合に比べてスループットが低下します。そのため、11g プロテクションは、実際に干渉によりスループットが低下している環境だけで動作させることを推奨します。

2.1.16　HT プロテクション機能

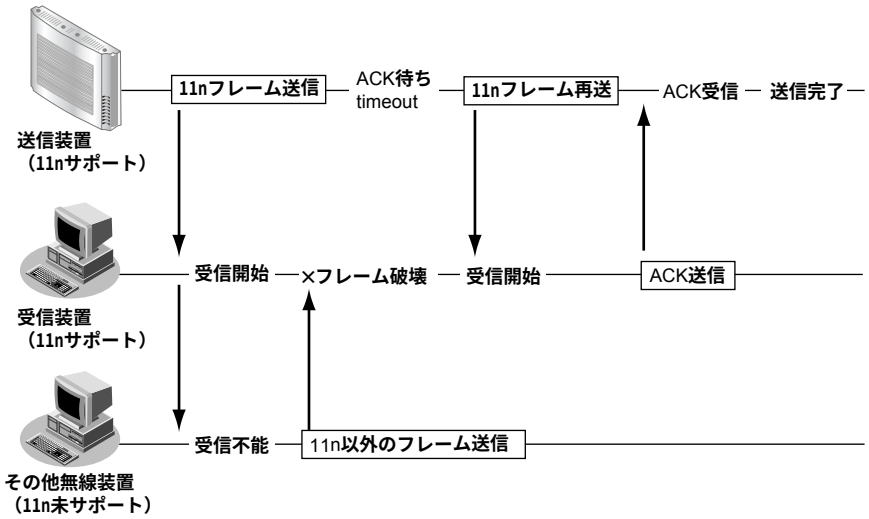
適用機種　全機種

HT プロテクションとは、11n と 11a/11b/11g の装置およびチャネルボンディング機能の使用・未使用の装置が混在する環境で通信した場合に発生する、スループットの低下を抑止する機能です。

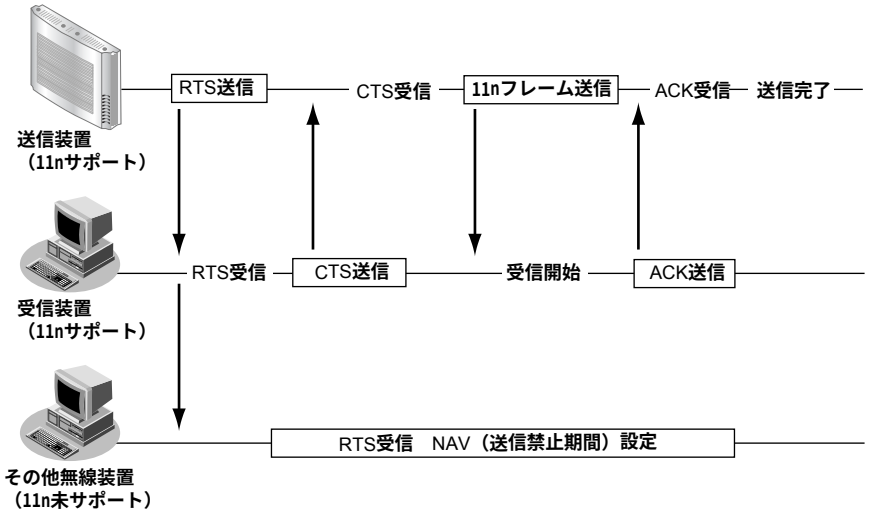
11a/11b/11g の装置は 11n での通信を理解できないため、11n の通信中に通信フレームを送信してしまう場合があります。この場合、フレーム破壊により通信がエラーとなり、再送が発生して結果 11n の装置のスループットが低下します。これを防ぐため、11n での通信に先立って、11a/11b/11g の装置が理解できる RTS または CTS-to-self のフレームを送信する機能が HT プロテクションです。11a/11b/11g の装置に対し、RTS および CTS-to-self によってキャリアの占有時間を通知し、11n の通信が行われる間 11a/11b/11g の通信を抑止することで、11n の通信を保護することができます。

チャネルボンディング機能の使用・未使用の混在時も、未使用の装置は 40MHz 幅での通信を理解できないため、同様のことが起こります。
この場合も HT プロテクションを利用することで、40MHz 幅での通信を保護することができます。

例）干渉が発生している場合



例）RTS/CTS でプロテクションを動作させた場合



こんな事に気をつけて

- **HT プロテクションを動作させた場合、11n および 40MHz 幅での通信の前には RTS/CTS または CTS-to-self のフレームが付加されるため、動作させていない場合に比べてスループットが低下します。そのため、HT プロテクションは、実際に干渉によりスループットが低下している環境だけで動作させることを推奨します。**
- **11b の装置が存在する環境で HT プロテクションを動作させる場合は、11g プロテクションの機能も設定してください。この場合、HT プロテクション用のフレームが、11b の装置も理解可能な低いレートで送信されるため、11g プロテクション未使用の場合に比べてスループットが低下します。**

2.1.17　ショートガードインターバル

適用機種　全機種

ショートガードインターバルとは、IEEE802.11n 規格のオプション機能で、11a/11g で 800 ナノ秒であったガードインターバルを 400 ナノ秒で使用するものです。
ショートガードインターバルを使用することで、800 ナノ秒のガードインターバルと比較して通信速度が約 1.1 倍に向上します。

こんな事に気をつけて

- **ショートガードインターバルは、無線 LAN アクセスポイントおよび無線 LAN クライアントの両方で有効である場合にだけ動作します。**
- **ショートガードインターバルは反射波の影響を受けやすいため、オフィスや家庭など無線 LAN アクセスポイントおよび無線 LAN クライアントの距離が近い環境での使用を推奨します。**

2.1.18　チャネルボンディング機能

適用機種　全機種

チャネルボンディングとは、IEEE802.11n 規格のオプション機能で、隣り合った 2 つのチャネルを束ねて通信する機能です。
従来の倍の 40MHz の帯域幅を使用するため、通信速度が 2 倍に向上します。

こんな事に気をつけて

- **チャネルボンディングを使用する場合、無線 LAN アクセスポイントおよび無線 LAN クライアントの両方でチャネルボンディングを有効にする必要があります。**
- **無線 LAN アクセスポイントでは、セカンダリチャネルに他 BSS のプライマリチャネルが存在する場合は自動的に 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 チャネルが 1 つしか確保できないことに加え、ほかのチャネルとの干渉が発生しやすいため、チャネルボンディングは 5GHz 帯での使用を推奨します。**

参照　コマンド設定事例集
「1.15 IEEE802.11n チャネルボンディング機能を使う」（P.50）、
「2.8 IEEE802.11n チャネルボンディング機能を使う」（P.72）

2.1.19　MIMO Power Save機能

適用機種 ***SR-M20AP1, 20AP2***

MIMO Power Saveとは、無線ネットワークのスループットと通信品質を向上するMIMO（Multiple Input Multiple Output）の電力消費を抑えるためのIEEE802.11n規格の機能です。
MIMOは複数のアンテナを利用するため、搭載するアンテナの数が多いほど、1本のアンテナしか利用しない旧規格の無線LANクライアントと比べ多くの電力を消費します。この電力消費を抑える機能として、無通信時に1つのアンテナを残して、ほかのアンテナの電源を切るMIMO Power Save機能があります。

本装置は、MIMO Power Save機能のDynamicモードまたはStaticモードで動作する無線LANクライアントとの接続をサポートすることにより、無線LANクライアントの電力を削減することができます。

こんな事に気をつけて

MIMO Power Save機能は本装置に接続する無線LANクライアントの電力消費を削減します。
本装置の電力消費を削減することはできません。

2.1.20　認証自動切替機能

適用機種 ***SR-M20AP1, 20AP2***

認証自動切替機能は、IEEE802.1X認証が定義された無線LANインタフェースが利用するRADIUSサーバの監視を行い、RADIUSサーバと通信ができなくなった場合に事前共有キー（PSK）認証へ認証を切り替えることで、無線LAN端末が接続できなくなることを回避し、無線LAN通信を継続することができます。
RADIUSサーバの定期監視に限らず、実際の認証要求で応答がない場合もバックアップへの切り替えが行われます。また、バックアップ側インタフェースはPSK認証に限らず、OPEN／SHARED認証とMACアドレス認証との組み合わせも可能です。

参照 「2.13 RADIUS機能」（P.55）、
コマンド設定事例集「7.2 認証自動切替機能を使う」（P.89）

2.1.21　ノイズ回避機能

適用機種 ***SR-M20AP1, 20AP2***

ノイズ回避機能は、運用チャネルに影響する一部のノイズを検出した場合に、チャネルを変更する機能です。
本機能により、ノイズによる通信影響を緩和できる場合があります。

こんな事に気をつけて

- **本機能を有効にすることにより無線LANと干渉する電波を検出した場合に運用チャネルの構成定義を自動的に変更し、かつ反映（commitコマンド実行）します。したがって構成定義を編集中の場合に予期しないタイミングで反映されてしまう場合があります。**
  構成定義を編集中の場合は本機能を一度無効化することをお勧めします。
- **本機能によって変更された無線LANチャネルの構成定義は自動的には保存されません。**
- **レーダーの検出状況により無線LANと干渉する電波を検出した場合であってもチャネルが切り替わらない場合があります。**

2.2　オートネゴシエーション機能

適用機種　全機種

オートネゴシエーション機能とは、IEEE802.3u に規定された 2 装置間のプロトコルであり、優先順位に従い通信速度、通信モード（全二重／半二重）の設定を自動的に行う機能です。

本装置が使用している 10/100/1000BASE-T ポートの相互接続について以下に示します。なお、表中の「100M/FULL」などの記述は、自装置と接続相手の通信モードの組み合わせの結果、リンク確立する接続モードを示します。記述がない場合は、リンク確立しません。

- オートネゴシエーション（Auto-Nego）どうしの接続は、相互に通信できるモードの中から、決められたアルゴリズムにより通信モードが設定されます。
- 固定どうしの接続は、同じ通信モードのときだけ正常に通信できます。

こんな事に気をつけて

- **一方がオートネゴシエーションで、他方が FULL（全二重）の固定で接続すると、通信モードは HALF（半二重）と認識されます。この場合、エラー率が高いなど正常な通信ができないことがありますので、通信モードを正しく設定してください。**
- **一方または両方の通信モードがオートネゴシエーションで、お互いが認識できない場合は、両方の通信モードを固定に設定してください。**
- **一方が 10M 固定、他方を 100M 固定で誤接続すると、片方の装置だけがリンク確立したり、通信状態によってはリンクが確立と切断を繰り返したりする場合があります。この場合は通信モードを正しく設定してください。**

○：接続可能、×：接続不能

自装置＼接続相手		Auto-Nego	10M 固定		100M 固定		1000M 固定
			FULL	HALF	FULL	HALF	FULL
Auto-Nego		○ 10M/FULL、10M/HALF 100M/FULL、100M/HALF、 1000M/FULL	×（※） 10M/HALF	○ 10M/HALF	×（※） 100M/HALF	○ 100M/HALF	○ 1000M/FULL
10M 固定	FULL	×（※） 10M/HALF	○ 10M/FULL	×	×	×	×
	HALF	○ 10M/HALF	×	○ 10M/HALF	×	×	×
100M 固定	FULL	×（※） 100M/HALF	×	×	○ 100M/FULL	×	×
	HALF	○ 100M/HALF	×	×	×	○ 100M/HALF	×
1000M 固定	FULL	○ 1000M/FULL	×	×	×	×	○ 1000M/FULL

※）リンク確立するが、通信設定が異常

2.3　AutoMDI/MDI-X機能

適用機種　全機種

AutoMDI/MDI-X機能とは、接続相手のポートがMDIかMDI-Xかを自動的に判断して接続する機能です。

本装置の10/100/1000BASE-Tポートでは、AutoMDI/MDI-X機能をサポートしています。

MDIの自動検出は、通信モードがAutoの場合のみ有効であり、10M/FULL固定、10M/HALF固定、100M/FULL固定、100M/HALF固定、1000M/FULL固定の場合は、MDIの自動検出を指定しても、システムログを出力してMDIとして動作します。

MDI/MDI-Xの指定（※） 通信モードの指定	auto	mdi	mdix
Auto	auto	mdi	mdix
固定	mdi	mdi	mdix

※）MDI/MDI-Xでは、以下の動作を指定できます。

auto　：MDIを自動検出
mdi　：MDIとして動作
mdix　：MDI-Xとして動作

2.4　フロー制御機能

適用機種　全機種

本装置では、全二重通信時は IEEE802.3x に基づく Pause フレーム、半二重通信時はバックプレッシャ機能によるフロー制御機能をサポートしています。
フロー制御の設定による各ポートの動作を以下に示します。

こんな事に気をつけて

フロー制御を適用した場合、接続相手が本装置の該当ポートにフレーム送信できなくなることがあります。この場合、接続相手のバッファ容量によって、本装置に設定している優先機能の優先度に関係なくフレーム廃棄されることがあります。このため、音声や画像などを使用するネットワークの場合は、フロー制御を無効にしてください。
また、接続相手によっては、データフレームの転送性能が劣化することがあります。

＜ Auto-nego モードの場合＞

フロー制御設定		システム動作
送信	受信	
off 設定	off 設定	IEEE802.3x に示されるフロー制御設定を、Pause= なし、送受信方向 = 対称（※ 1）としてオートネゴシエーションし、全二重モードでリンク確立した場合は、接続相手のフロー制御設定により処理を実行する（※ 2）。 半二重モードでリンク確立した場合は、半二重固定モードと同じ動作となる。
on 設定	off 設定	IEEE802.3x に示されるフロー制御設定を、Pause= なし、送受信方向 = 非対称（※ 1）としてオートネゴシエーションし、全二重モードでリンク確立した場合は、接続相手のフロー制御設定により処理を実行する（※ 2）。 半二重モードでリンク確立した場合は、半二重固定モードと同じ動作となる。
off 設定	on 設定	IEEE802.3x に示されるフロー制御設定を、Pause= あり、送受信方向 = 非対称（※ 1）としてオートネゴシエーションし、全二重モードでリンク確立した場合は、接続相手のフロー制御設定により処理を実行する（※ 2）。 半二重モードでリンク確立した場合は、半二重固定モードと同じ動作となる。
on 設定	on 設定	IEEE802.3x に示されるフロー制御設定を、Pause= あり、送受信方向 = 対称（※ 1）としてオートネゴシエーションし、全二重モードでリンク確立した場合は、接続相手のフロー制御設定により処理を実行する（※ 2）。 半二重モードでリンク確立した場合は、半二重固定モードと同じ動作となる。

※ 1）“Pause”は、Pause オペレーション能力のあり／なしを示し、“送受信方向”は、Pause オペレーション能力が送受信対称か、非対称かを示します。
フロー制御設定が、送信、受信共に on 設定の場合、送受信方向は対称となります。

※ 2）Auto-nego モード時のフロー制御設定は、接続相手のフロー制御設定により、以下の表のとおりに設定されます。

自装置のフロー制御設定		接続相手のフロー制御設定		Auto-Nego 結果	
送信	受信	Pause	送受信方向	pause 送信	pause 受信
off 設定	off 設定	D.C.	D.C.	N	N
on 設定	off 設定	なし	D.C.	N	N
		あり	対称	N	N
		あり	非対称	Y	N
off 設定	on 設定	なし	対称	N	N
		なし	非対称	N	Y
		あり	D.C.	N（※）	Y
on 設定	on 設定	なし	D.C.	N	N
		あり	対称	Y	Y
		あり	非対称	Y	Y

※）オートネゴシエーションの結果、送信 Pause=Y となるが、自設定に従って、送信 Pause=N とする。

- D.C. ：Don't Care
- Pause フレーム送信時
  Y　：フロー制御のために Pause フレームを送出する
  N　：Pause フレームを送出しない
- Pause フレーム受信時
  Y　：Pause フレームを受信することがあるため、その場合は受信処理（フロー制御）を行う
  N　：Pause フレームを受信しない（受信した場合は、Pause フレームを廃棄し、何も処理しない）

＜固定モードの場合＞

フロー制御設定		通信モード	システム動作	
送信	受信		送信方向	受信方向
off 設定	off 設定	全二重固定	Pause フレーム送出なし	Pause フレーム受信時は、フロー制御を実行しない（※ 1）
		半二重固定	バックプレッシャ送出なし	バックプレッシャ受信時は、データ送信停止（※ 2）
on 設定	off 設定	全二重固定	フロー制御のため Pause フレームを送出する	Pause フレーム受信時は、フロー制御を実行しない（※ 1）
		半二重固定	フロー制御のためバックプレッシャを送出する	バックプレッシャ受信時は、データ送信停止（※ 2）
off 設定	on 設定	全二重固定	Pause フレーム送出なし	Pause フレーム受信時は、フロー制御を実行する
		半二重固定	バックプレッシャ送出なし	バックプレッシャ受信時は、データ送信停止（※ 2）
on 設定	on 設定	全二重固定	フロー制御のため Pause フレームを送出する	Pause フレーム受信時は、フロー制御を実行する
		半二重固定	フロー制御のためバックプレッシャを送出する	バックプレッシャ受信時は、データ送信停止（※ 2）

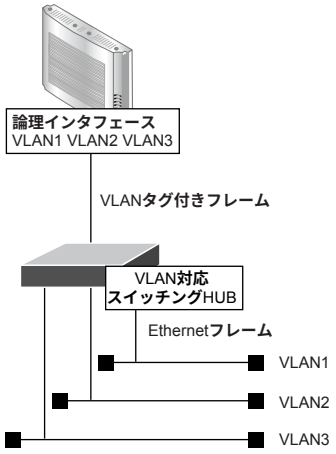
※ 1）Pause フレーム受信時は無視する。

※ 2）バックプレッシャとして送信停止するわけではなく、半二重動作としてデータ送信できない。

2.5　VLAN 機能

適用機種　***SR-M20AP1, 20AP2***

VLAN 機能とは、物理的な LAN を仮想的な複数の LAN に分割する機能です。



SR-M20AP1 / 20AP2 でサポートする VLAN 機能は、IEEE802.1q に準拠しています。
SR-M20AP1 / 20AP2 は VID=1 に、すべてのポートが VLAN1 のタグなしとして初期設定されていますが、各ポートを特定の VLAN のタグ付きまたはタグなしに設定を変更することができます。

VLAN とネットワークアドレス

VLAN 機能を使用した場合、ブリッジング通信はその VLAN 内に閉じたものになります。したがって、VLAN を定義するということは、MAC アドレスのレベルでブロードキャストフレームが届く範囲（ブロードキャストドメイン）を制限する、ということになります。

VLAN 種別

SR-M20AP1 / 20AP2 がサポートする VLAN 機能では、以下の単位で VLAN を分けることができます。

- ポート VLAN
  ポート単位でグループ化を行う機能です。
- タグ VLAN
  フレームに VLAN 番号を記したタグ情報を挿入し、フレーム単位で VLAN の区別を行う機能です。
- 認証 VLAN
  認証成功となった端末ごとに、RADIUS サーバから割り当てられた VLAN によって区別を行う機能です。

無線 LAN における VLAN

無線 LAN では SSID と VLAN を対応付け、有線 LAN ポートの VLAN とマッピングして、無線 LAN と有線 LAN ポート間の通信を実現します。認証 VLAN は端末ごとに VLAN を割り当てるため、認証に成功した端末は SSID に関係なく有線 LAN ポートの同一 VLAN へ通信が可能となります。

同一ポート上での VLAN の混在

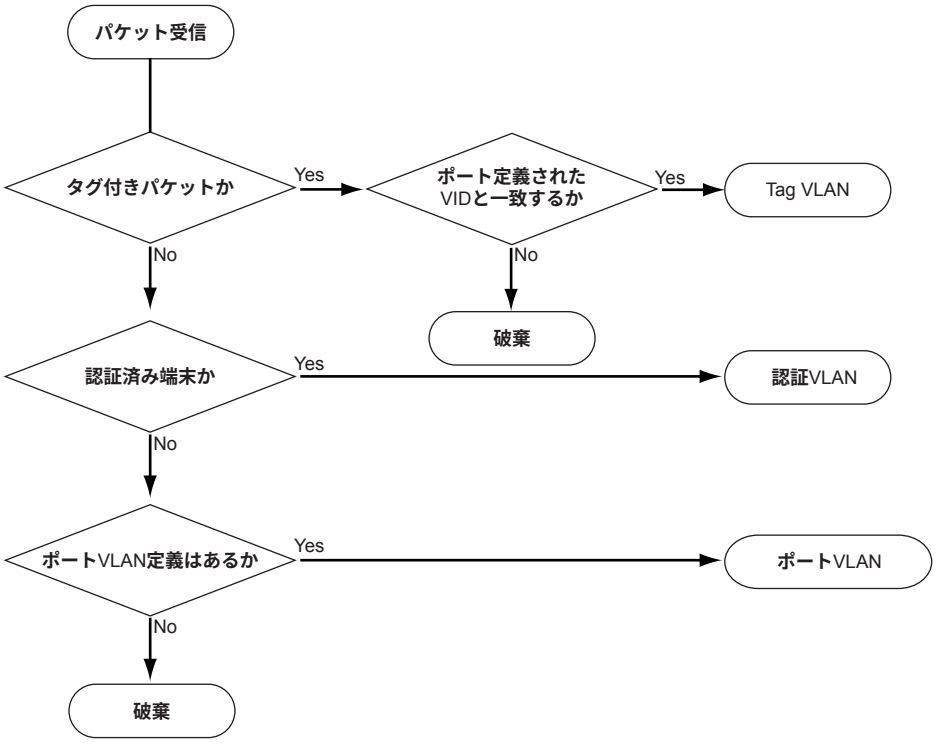
同一ポートには、ポート VLAN とタグ VLAN を同時に設定することはできません。同一ポートには、ポート VLAN だけ、またはタグ VLAN だけを設定してください。

Ethernet ポート上での同一 VLAN タグの設定

ポート VLAN、タグ VLAN ともに同一 VLAN を複数の Ethernet ポートに設定することはできません。ただし、Ethernet ポートでバックアップポート機能を使用する場合は、同一 VLAN を複数の Ethernet ポートに設定することができます。

パケット受信時の VLAN 判定

VLAN を設定したポートでパケットを受信した場合、受信したパケットの所属する VLAN の判定を以下の順序で行います。



パケット送信時の VLAN タグ

パケット送信時の VLAN タグの扱いは、送信するポートの Tagged ／ Untagged 設定に従って、Tagged ポートの場合は VLAN タグを付与し、Untagged ポートの場合は VLAN タグを付与しないで送信します。

2.6　ポート閉塞機能

適用機種　全機種

ポート閉塞機能とは、物理ポート（Ethernet）または論理インタフェース（無線 LAN インタフェース）のダウン状態（ポート閉塞状態）を online コマンド発行によるオペレータ指示があるまで保持する機能です。

障害要因によって、物理ポート（Ethernet）のリンクアップ、リンクダウンが繰り返し発生する可能性や、論理インタフェース（無線 LAN インタフェース）が通信できない状態になる可能性があります。そのような場合、本装置は意図的にダウン状態（ポート閉塞状態）を継続させることで、冗長経路が存在する場合は、安定した通信を保つことができます。

ポート閉塞状態への遷移は、以下で制御します。

- offline コマンド発行による手動閉塞（全機種）
- 通信制御機能の連携動作による自動閉塞（SR-M20AP1 / 20AP2 のみ）
- 接続ポートのリンク状態変化による自動閉塞（SR-M20AP1 / 20AP2 のみ）
- 認証自動切替機能による自動閉塞（SR-M20AP1 / 20AP2 のみ）

こんな事に気をつけて

- **offline コマンドは、管理者クラスだけ発行可能です。**
- **閉塞状態となったポートは、online コマンドの閉塞解除指定でポート閉塞を解除してください。**
- **認証自動切替機能の対象である無線 LAN インタフェースに対して閉塞が行われた場合、認証自動切替機能の対象であるすべての無線 LAN インタフェースが対象となります。**

offline コマンド発行による手動閉塞

offline コマンドは、以下を対象に閉塞状態に遷移することができます。

- 物理ポート（Ehternet）
  offline ether を発行することにより、対象ポートを閉塞状態とします。
- 論理インタフェース（無線 LAN インタフェース）
  offline wlan を発行することにより、対象無線 LAN インタフェースを閉塞状態とします。

通信制御機能の連携動作による自動閉塞

バックアップポート機能を使用した場合に、ポート閉塞状態への遷移指定が可能です。

☛ 参照 「2.7 バックアップポート機能」（P.42）

接続ポートのリンク状態変化による自動閉塞

接続ポートのリンク状態の変化を契機にポートを閉塞状態にすることを可能にします。

本装置でポート閉塞状態への遷移が可能なリンク状態変化は以下のとおりです。

- リンクダウンを契機にした無線 LAN インタフェースの連携閉塞（リンクダウンリレー閉塞（リンクインテグリティ））
  リンクダウン時に、構成定義で指定した連携無線 LAN インタフェース番号を同時に閉塞状態とします。
  また、リンクアップ状態へ復旧した場合に、連携無線 LAN インタフェースを同時に閉塞解除することも可能です。

参照 「2.8 リンクインテグリティ機能」（P.43）

認証自動切替による自動閉塞

認証自動切替機能を使用した場合、以下を契機に無線 LAN インタフェースを閉塞状態にします。

- RADIUS サーバからの応答を検出した場合、構成定義で backup 指定した無線 LAN インタフェースを閉塞状態とします。
- RADIUS サーバからの応答が検出できなかった場合、構成定義で master 指定した無線 LAN インタフェースを閉塞状態とし、backup 指定した無線 LAN インタフェースを閉塞解除します。

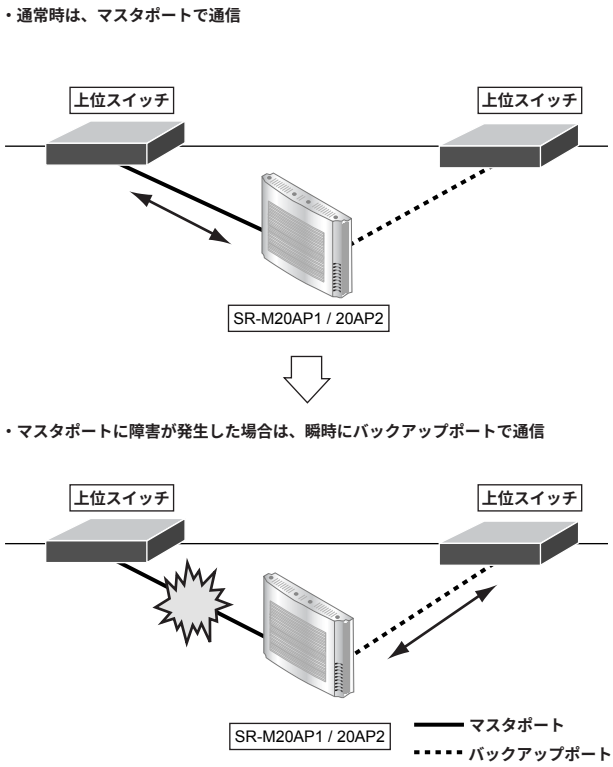
2.7　バックアップポート機能

適用機種　***SR-M20AP1, 20AP2***

バックアップポート機能とは、2 つのポートをグループ化し、片方のポートをマスタポート（優先ポート）、もう一方のポートをバックアップポート（待機ポート）として管理し、常にどちらか一方のポートだけを稼動させる機能です。

稼動中のポートになんらかの障害が発生した場合に、もう一方の待機ポートを瞬時に稼動ポートに切り替えることで、ネットワーク障害の影響を最小限に抑えることが可能です。

グループポートが共にリンクアップしている状態で、マスタポートを必ず優先使用するモードと、先にリンクアップしたポートを使用するモードの選択が可能です。



こんな事に気をつけて

- **バックアップポート機能では、障害発生時に稼動ポートを瞬時に切り替えることが可能ですが、各種プロトコルを使用した場合、通信が復旧するまでに各プロトコルでの復旧時間が必要となります。**
- **待機ポートの待機状態を offline と設定した場合、待機ポートはリンクダウンしているため、回線抜けなどの異常が発生しても検出はできません。切り替わり動作後に異常検出となります。**

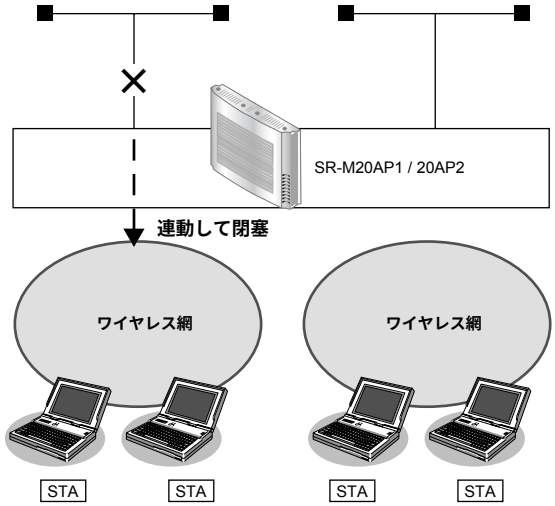
2.8　リンクインテグリティ機能

適用機種　***SR-M20AP1, 20AP2***

リンクインテグリティ（リンクダウンリレー）機能とは、指定したETHERポートがリンクダウンしたときに、連動して無線LANインタフェースを閉塞状態に遷移させ、強制的に無線LAN端末をほかのアクセスポイントにローミングさせる機能です。

リンクダウンしたETHERポートがリンクアップした場合、本機能で閉塞状態にした無線LANインタフェースを自動的に閉塞解除することができます。また、バックアップポート機能との併用により、指定したバックアップグループの優先／待機ポートの両方がダウン状態となったときに、連動して指定した無線LANインタフェースを閉塞状態にできます。

参照 「2.7 バックアップポート機能」（P.42）



こんな事に気をつけて

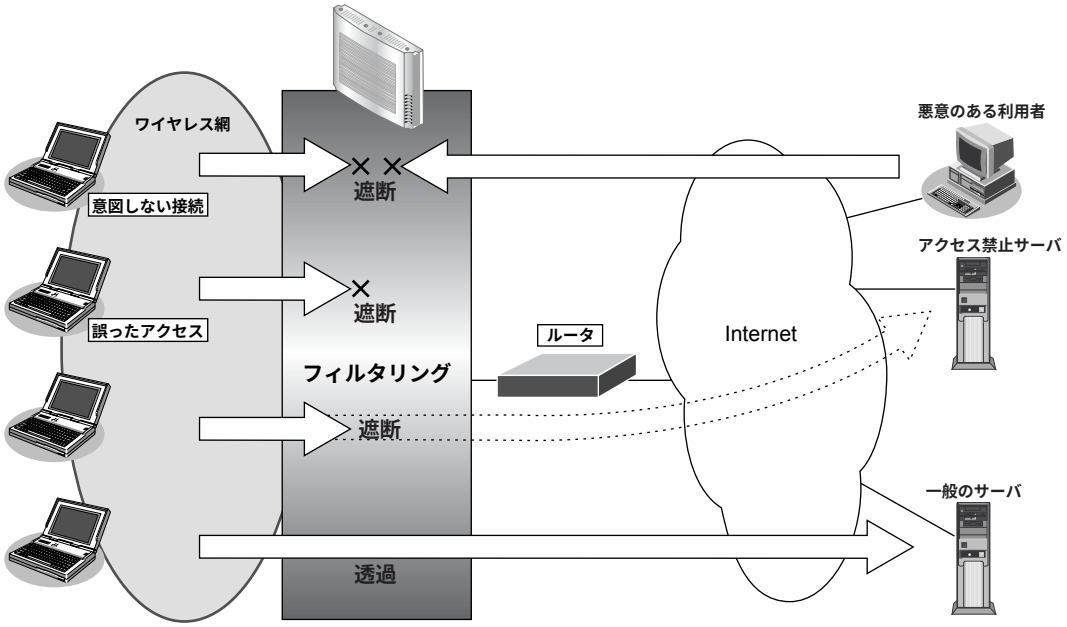
- **指定した無線LANインタフェースが使用されていない、または、すでにoffline状態のときは、自動的に閉塞解除することはできません。**
- **閉塞解除動作がコマンドによる閉塞解除の場合、閉塞された無線LANインタフェースはonlineコマンドで閉塞解除してください。**
- **ETHERポートの種別がバックアップポート指定、かつ、ether定義およびbackup定義でリンクダウンリレーの設定が行われている場合、ETHERポートに対する設定は無効となります。**

2.9　フィルタリング機能

適用機種　全機種

フィルタリング機能では、本装置を経由するパケットをMACアドレス、VLAN ID、IPアドレスやポート番号など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。

本装置では、Ethernetフレームに対するMACアドレスフィルタリング機能およびIPパケットに対するIPフィルタリング機能をサポートし、本装置に入力されたパケットが指定されたACL定義の“acl mac”定義、“acl ip”定義、“acl tcp”定義、“acl udp”定義または“acl icmp”定義に該当した場合、同一VLANに属するETHERポートおよび無線LANインタフェースに対して、フィルタリング処理を行います。



ネットワークのセキュリティを向上させるには、以下の要素について考える必要があります。

- ネットワークのセキュリティ方針
- 本装置以外の要素（ファイアーウォール、ユーザ認証など）

接続形態に応じてセキュリティ方針を決める

インターネットに接続する場合でもLANどうしを接続する場合でも、データの流れには「外部から内部へ」、「内部から外部へ」という2つの方向があります。セキュリティ方針を決める場合は、2つの方向について考慮する必要があります。

- **「外部から内部へ」流れるデータに対するセキュリティ方針の例**

  特定のパケットを受け取らないようにする。

  非公開ホストへのアクセスを拒否する。

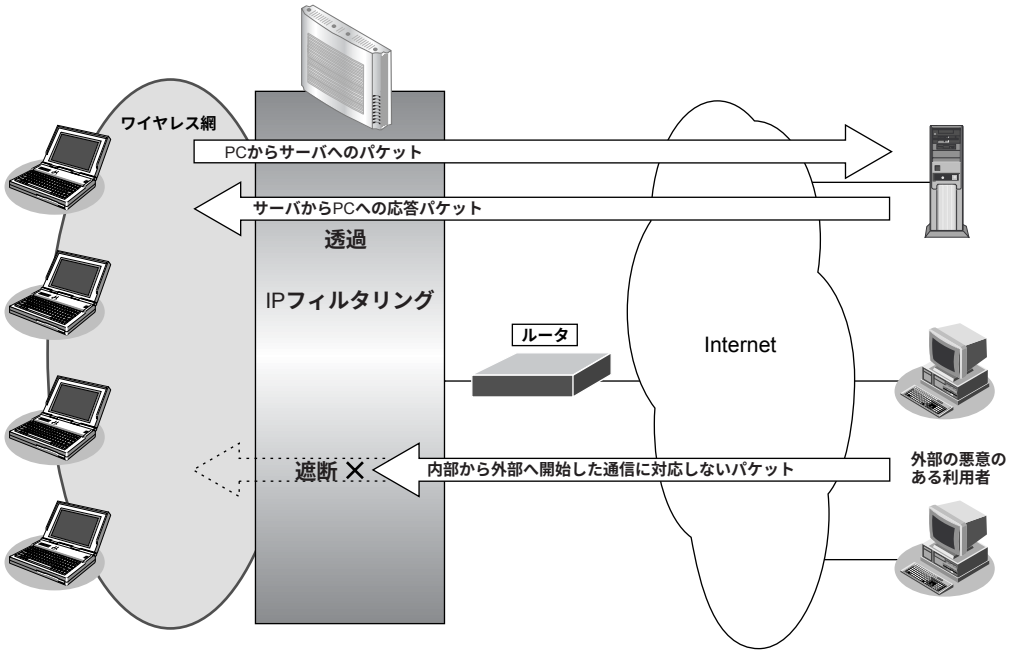
  内部ユーザによる不要なアクセスを防ぐ。

- **「内部から外部へ」流れるデータに対するセキュリティ方針の例**

  アクセス禁止サーバなどへのアクセスを制限する。

2.9.1　動的フィルタリング（SPI）

SPI は内部から外部へ通信を開始すると、これに対応するフィルタリングルールを自動的に作成し、外部からの応答パケットを透過させます。また、フィルタリングルールに対応しない外部から内部への通信を開始したパケットを遮断することができます。



補足　ブロードキャストアドレスやマルチキャストアドレスあてに SPI でフィルタリングを行うことはできません。DHCP などブロードキャストアドレスを用いる通信を SPI と併用する場合は、これらの通信を透過させるフィルタリングルールを設定してください。

ヒント

SPI によるフィルタリング対象は、構成定義で設定された IP フィルタリングを透過したパケットです。

こんな事に気をつけて

- ProxyDNS を設定している場合、ProxyDNS に対しての IP フィルタリングを設定しても効果はありません。
- 本装置でコンピュータウィルスの感染を防ぐことはできません。パソコン側でウィルス対策ソフトを使用するなど、別の手段が必要です。
- フィルタリングの対象となるのは本装置に入力されたパケットです。本装置より出力されるパケットは対象となりません。
- SPI 対象となるのは本装置に入力されたパケットです。そのため、本装置自身より送出されるパケットは対象となりませんので、本装置から外部側へ通信する場合は、必要な通信を透過させるフィルタリングルールを設定する必要があります。
- “vlan filter”、“serverinfo filter”、“wlan macfilter” コマンドなどの ACL を参照する定義は、参照可能上限数を超えた場合、適用されません。
- プライバシープロテクション機能が無効であり、同一仮想アクセスポイント内の端末どうしの通信が可能な場合、端末どうしの通信に対する VLAN のフィルタ設定は無効となります。

2.10 IEEE802.1X 認証機能

適用機種　全機種

IEEE802.1X 認証機能とは、外部に設置した RADIUS サーバによって認証を行います。

本装置では、IEEE802.1X に準拠した認証機能（802.1X 認証）をサポートしています（SR-M20AP1 / 20AP2 では無線 LAN インタフェースのみ。SR-M20AC1 / 20AC2 では ETHER ポートのみ）。

認証機能は、認証方式「EAP-MD5」、「EAP-TLS」、「EAP-TTLS」、「PEAP」に対応しています。認証を行うための認証データベースとして、自装置内の AAA 機能を用いたローカル認証と、外部に RADIUS サーバを設置したリモート認証が利用できます。ローカル認証を利用する場合は「EAP-MD5」のみで認証を行います。リモート認証を利用する場合は、ローカル認証に比べてより安全な「EAP-TLS」および「EAP-TTLS」などで認証を行います。

本機能を利用することで、認証許可のないユーザ端末の通信（認証要求を除く）をすべて遮断し、認証されたユーザ端末以外からのネットワークへの不当アクセスを防止します。

SR-M20AP1/ 20AP2 では RADIUS サーバに属性を設定することによって、認証時、ユーザ端末を VLAN に対応付けます。RADIUS サーバから VLAN ID が通知されなかった場合、“wlan dot1x vid” コマンドで設定された VID を割り当てます。

SR-M20AC1 / 20AC2 では、Supplicant の VLAN への対応付けは未サポートとなります。

本装置で動作確認が取れている RADIUS サーバは、富士通製「Safeauthor V3.6」です。

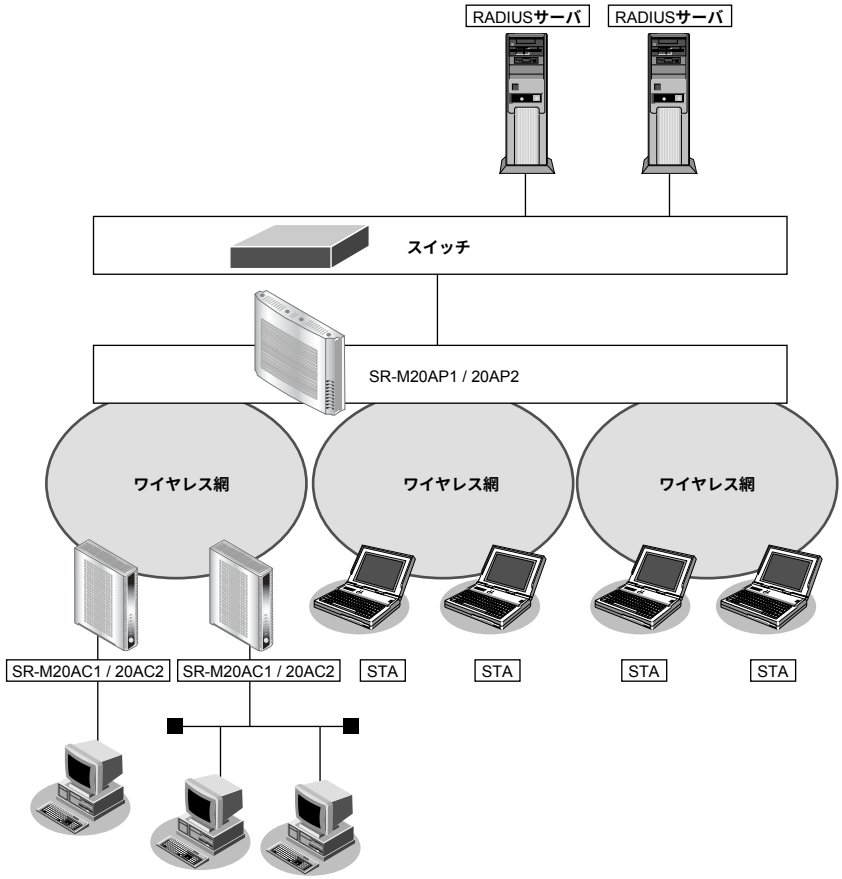
SR-M20AP1 / 20AP2 では、1 つの無線 LAN インタフェースで複数の端末を認証できます。

SR-M20AC1 / 20AC2 では、1 つの ETHER ポートで複数の端末を認証できます。この場合、ETHER ポートにスイッチング HUB などを接続し、そこに複数の端末を接続して、それぞれの端末で認証を行う運用が可能です。

1 つの ETHER ポートで複数の端末を認証する場合、“EAPOL 開始” メッセージを送信する Supplicant ソフトを使用してください。“EAPOL 開始” メッセージを送信しない Supplicant ソフトでは認証が開始されません。

無線 LAN での利用で動作確認が取れている Supplicant ソフトは、Juniper 製「Odyssey Client Manager3.10.0」、Microsoft 製「WindowsXP/Vista Zero Configuration」、Atheros 製「Atheros クライアントユーティリティー」です。

また、有線 LAN での利用で動作確認が取れている Supplicant ソフトは、富士通製「Systemwalker Desktop Inspection 802.1X サプリカント」です。



こんな事に気をつけて

- **本機能を利用するポートでは、事前に VLAN を設定できません。認証成功端末が認証成功時に割り当てられた VLAN で通信します。**
- **AAA 機能の課金情報としては通信累計時間のみサポートし、統計値（パケット数、データ量）は、常に 0 が通知されます。**

以下に、Windows® が標準で対応している EAP（Extensible Authentication Protocol）を示します。

○：対応、×：未対応

クライアント OS	対応 EAP			
	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP
Windows XP	○	○	×	×
Windows XP SP1、SP2、SP3	×	○	×	○
Windows Server 2003	○	○	×	○
Windows Vista	×	○	×	○
Windows 7	×	○	×	○

補足　また、無線 LAN の IEEE802.1X 認証では、暗号化に用いられる鍵情報の受け渡しも行われるため、Supplicant ソフトおよび認証（RADIUS）サーバともに無線 LAN での接続に対応している必要があります。

以下に、各 EAP の認証方式と特徴を示します。

認証方式	特徴
EAP-MD5	• ID、パスワードベースの認証規格である。 • ユーザ自身がパスワードを変更できるなど、管理者の負荷を軽減できる。
EAP-TLS	• 証明書内の情報（サブジェクト）による認証ができる。 • クライアント（ユーザ端末）とサーバの双方に登録されたデジタル証明書による双方向認証ができる。 • 期限切れのユーザ側証明書のチェックおよび拒否ができる。 • 証明書失効情報（CRL）を反映し、失効した証明書のアクセスを拒否できる。
EAP-TTLS	• ID、パスワードベースの認証規格である。 • ユーザ端末側で証明書が不要である。 • 導入時のコスト負担が少なく、高いセキュリティレベルを維持できる。
PEAP	• ID、パスワードベースの認証規格である。 • ユーザ端末側で証明書が不要である。 • 導入時のコスト負担が少なく、高いセキュリティレベルを維持できる。 • ユーザ自身がパスワードを変更できるなど、管理者の負荷を軽減できる。

VLAN ID 通知のための属性

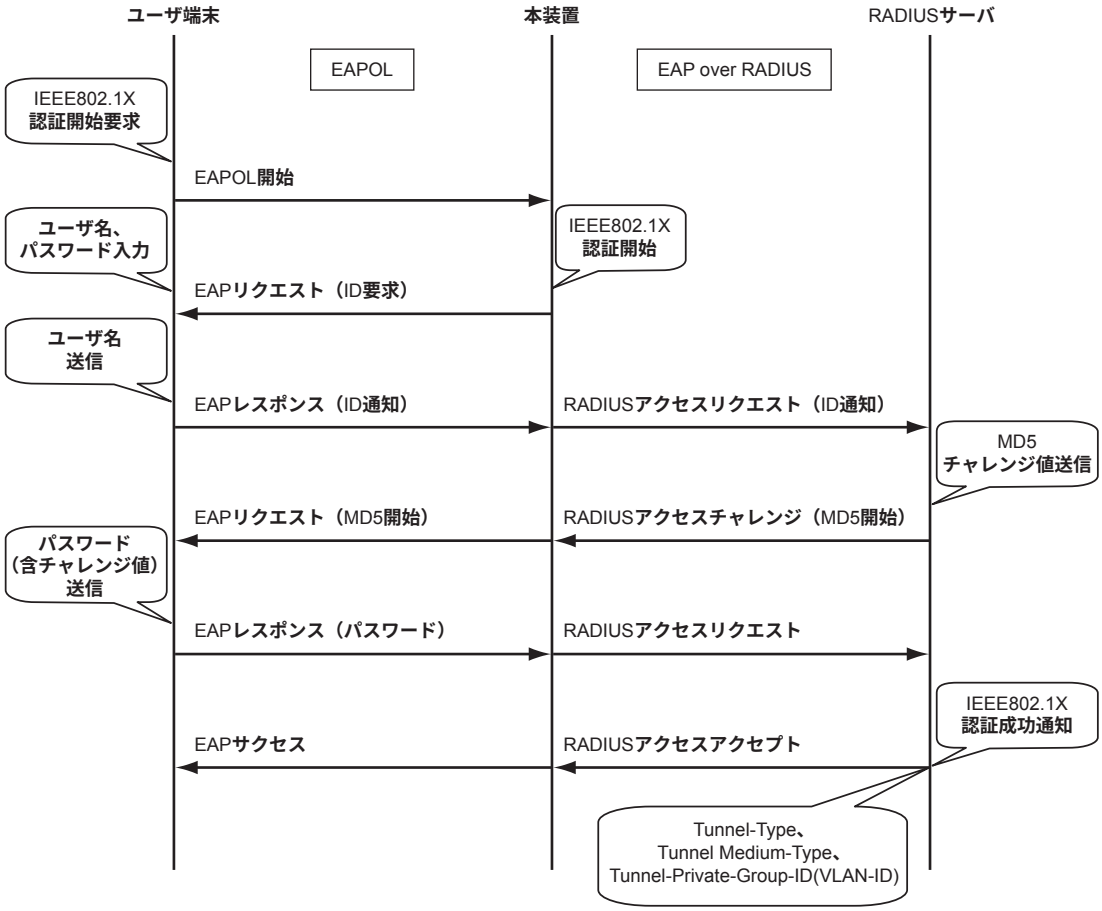
リモート認証時に Supplicant へ割り当てる VLAN ID を RADIUS サーバへ設定する際の属性情報を以下に示します。

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

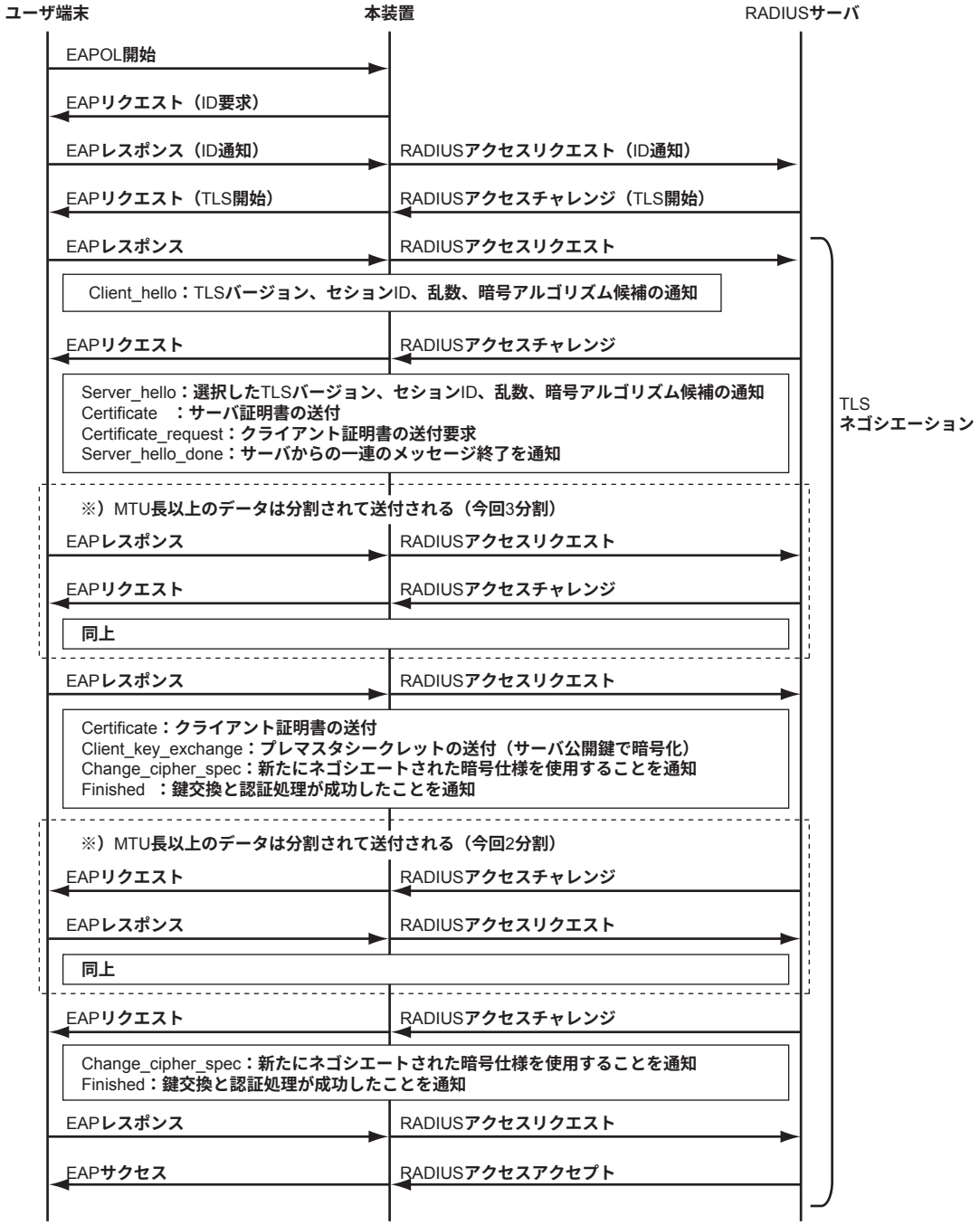
EAP-MD5 認証

EAP-MD5 認証とは、ユーザ端末と RADIUS サーバ間で共通のパスワードを持つことによって、認証する方式です。チャレンジ・レスポンスをやり取りし、MD5 ハッシュ関数によって暗号化して、RADIUS サーバがユーザの認証を行います。ローカル認証時は「RADIUS サーバ」の代わりに本装置内の「AAA 機能」が利用されます。
IEEE802.1X 機能の EAP-MD5 認証のシーケンスを以下に示します。



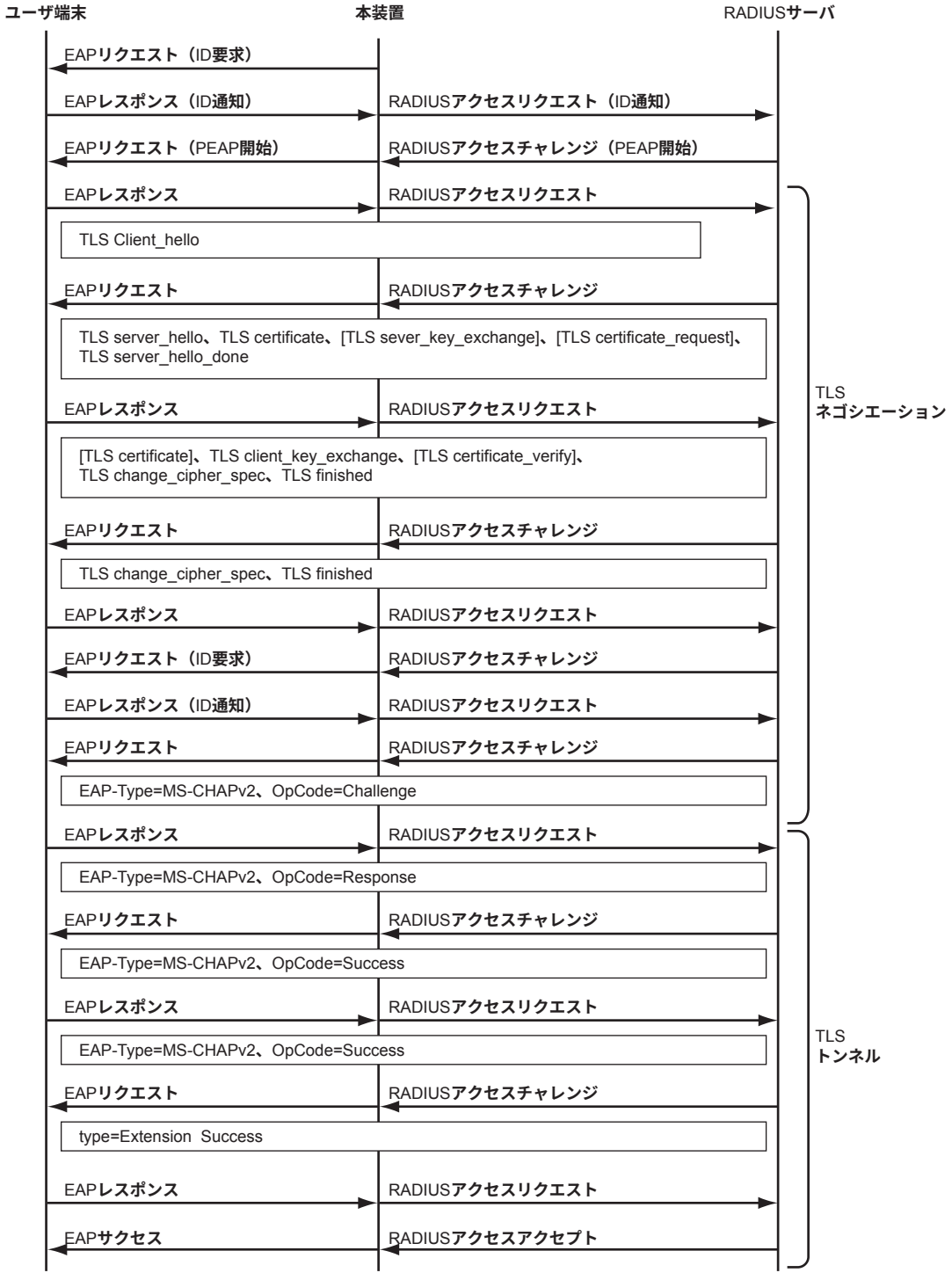
EAP-TLS 認証

EAP-TLS 認証とは、ユーザ端末と RADIUS サーバの双方に証明書を持つことによって、認証する方式です。
IEEE802.1X 機能の EAP-TLS 認証のシーケンスを以下に示します。



PEAP 認証（EAP-TTLS 認証も同様）

PEAP 認証とは、RADIUS サーバのみに証明書を持つことによって、認証する方式です。IEEE802.1X 機能の PEAP 認証のシーケンスを以下に示します。



2.11 MACアドレス認証機能

適用機種　全機種

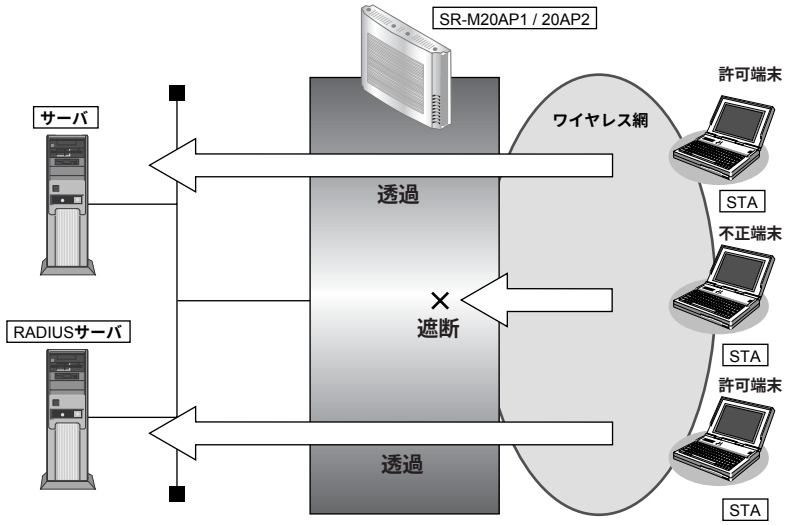
MAC アドレス認証機能とは、受信パケットの送信元 MAC アドレスで認証を行い、送信元の端末が接続を許可された端末であるか認証する機能です（SR-M20AP1 / 20AP2 は無線 LAN インタフェースのみ、SR-M20AC1 / 20AC2 は ETHER ポートのみ）。

本機能を利用することで認証許可のない不正端末を検知し、ネットワークへの不正アクセスを防止します。

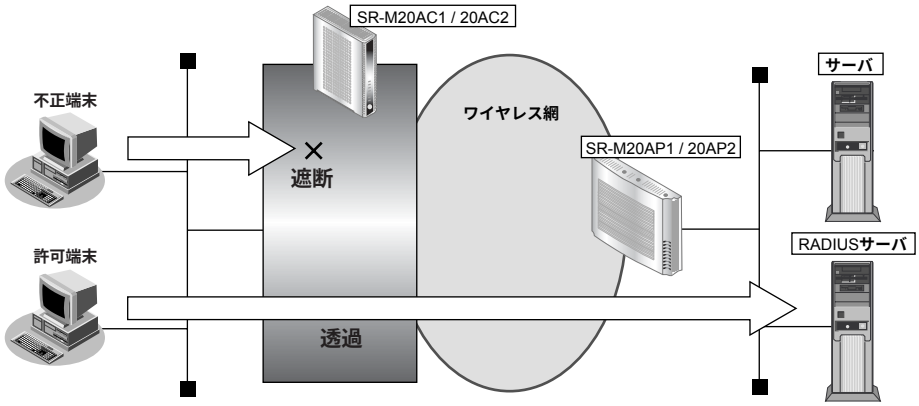
認証方式は「CHAP/PAP」に対応し、認証を行うための認証データベースとして、自装置内の AAA 機能を用いたローカル認証と、外部に RADIUS サーバを設置したリモート認証が利用できます。

SR-M20AP1 / 20AP2 では無線 LAN 側で受信した AUTHENTICATION フレームの送信元 MAC アドレスの認証を行い、成功した端末は認証で取得した VLAN ID の VLAN に収容されます。

SR-M20AC1 / 20AC2 では VLAN への対応付けはできません。



SR-M20AP1 / 20AP2 の MAC アドレス認証



SR-M20AC1 / 20AC2 の MAC アドレス認証

こんな事に気をつけて

- 本機能を利用する無線 LAN インタフェースでは、事前に VLAN を設定できません。認証成功端末が認証成功時に割り当てられた VLAN で通信します（SR-M20AP1 / 20AP2 のみ）。
- 本機能では、RADIUS アカウンティング機能は使用できません。
- 本機能では、端末からのパケット受信を契機とし認証を実施します。したがって、自発的にパケットを送信しない端末については、正常に認証できない場合があります。自発的にパケット送信しない端末を認証不要端末に設定することで、あらかじめ認証ポートに収容できます。

2.12 DHCP 機能

適用機種　全機種

2.12.1 IPv4 DHCP 機能

IPv4 DHCP 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（クライアント機能）です。

DHCP クライアント機能

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

ヒント

本装置でデフォルトルータの IP アドレスを受け取ると、自動的に優先度 1 のデフォルトルートがスタティック経路として生成されます。このスタティック経路は、スタティック経路情報の設定を行うことにより、デフォルトルート以外の任意のあて先や、優先度 1 以外に変更することができます。
このスタティック経路と、ほかの同じあて先への経路情報で冗長構成を行う場合は、それぞれの経路情報に 1 以外の値で優先度を設定してください。

参照　スタティック経路情報の設定については、コマンドリファレンス「lan ip route」を参照してください。

2.12.2 DHCP クライアント機能が使用できるインタフェース

DHCP クライアント機能が使用できるインタフェースが SR-M20AP1 / 20AP2 と SR-M20AC1 / 20AC2 では、以下のように異なります。

- SR-M20AP1 / 20AP2
  LAN インタフェースに属する有線ポート（Ethernet）でのみ DHCP クライアント機能が動作します。
- SR-M20AC1 / 20AC2
  LAN インタフェースに属する無線 LAN インタフェースでのみ DHCP クライアント機能が動作します。

2.13 RADIUS 機能

適用機種　全機種

RADIUS 機能は、AAA（Authentication, Authorization, Accounting）情報の管理を外部サーバ（RADIUS サーバ）を利用して行う機能です。複数の装置で同じ AAA 情報が必要な場合や、大量のユーザ情報を管理する場合など、ユーザの認証情報や設定情報、ユーザごとの接続時間を集約して管理することができます。

本装置では、RADIUS クライアント機能をサポートしています。

RADIUS クライアント機能は、以下の RADIUS サポート機能から AAA を経由して利用されます。

以下に、それぞれの機能で利用可能な AAA 情報を示します。

RADIUS サポート機能	認証方式（authentication）	ユーザ情報（authorization）	アカウンティング（accounting）
ログインユーザ認証	PAP 認証／CHAP 認証	使用しません	使用しません
IEEE802.1X 認証	EAP-MD5 認証、EAP-TLS 認証 EAP-TTLS 認証、PEAP 認証	使用しません	接続時間
MAC アドレス認証	PAP 認証／CHAP 認証 （※）	使用しません	使用しません

※）ユーザ名は MAC アドレス（区切り文字なし HEX12 文字）、パスワードは MAC アドレスまたは MAC アドレス認証情報で設定されたパスワードを使った認証となります。

本装置の RADIUS クライアント機能は、複数台の RADIUS サーバを使用したバックアップ構成または負荷分散構成が可能です。

RADIUS サーバとして定義された認証サーバおよびアカウンティングサーバは、alive 状態と dead 状態を持ちます。

それぞれの状態の意味は以下のとおりです。

- alive 状態
  サーバが使用可能である状態です。
  優先度が高い（定義上の数値が小さい）サーバから優先して使用されます。
  同じ優先度のサーバが複数存在する場合は、ランダムにサーバが選択されます。
- dead 状態
  サーバあてのリクエストがタイムアウトしたことにより、そのサーバの使用を一時的に停止している状態です。ほかに alive 状態のサーバが存在する場合、定義した優先度の値は使用されません。
  復旧待機時間で指定した時間が経過すると、自動的に alive 状態に復旧します。
  認証またはアカウンティングを行う場合、すべてのサーバが dead 状態になると、ランダムに 1 つのサーバで試行し、応答の得られたサーバは alive 状態に復旧します。

こんな事に気をつけて

- **RADIUS プロトコルの制約で、同時に認証およびアカウンティングが行える数は 256 です。同時に 257 以上の認証とアカウンティングを行った場合は、両方とも失敗します。**
- **RADIUS クライアント機能を定義しても、同じグループのユーザ情報は利用されます。AAA グループに RADIUS クライアント機能（aaa radius）とユーザ情報（aaa user）の両方を定義した場合、RADIUS クライアント機能で認証が行われます。RADIUS クライアント機能で認証が成功した場合はユーザ情報は利用されませんが、認証に失敗した場合は、次にユーザ情報で認証を行います。**

RADIUS サーバの監視

RADIUS サーバの監視は、以下のどちらかの方法で行うことができます。

- ICMP を使う方法
  RADIUS サーバが動作しているホストに対して、ICMP ECHO パケットを送受信することにより、そのホストの生存確認を行います。
- 認証を使う方法
  RADIUS サーバに対する定期的な認証要求を行うことにより、RADIUS サーバの生存確認を行います。監視は CHAP 方式を用いた認証で行いますが、認証結果にかかわらず、その応答による生存確認を行います。

2.14 DNS サーバ機能

適用機種　全機種

DNS サーバ機能とは、LAN インタフェース内の端末への DNS 要求に対して、上位 DNS サーバ（たとえば、プロバイダの DNS サーバ）を中継しないで、本装置が持っている情報を返すことができる機能です。

DNS サーバ機能を使用する場合、端末は DNS アドレスとしてルータの IP アドレスを設定します。端末が DHCP クライアントの場合は、DHCP サーバが通知する DNS アドレスとしてルータの LAN ポートの IP アドレスを通知する必要があります。

本装置には、以下の 2 種類の DNS サーバ機能があります。

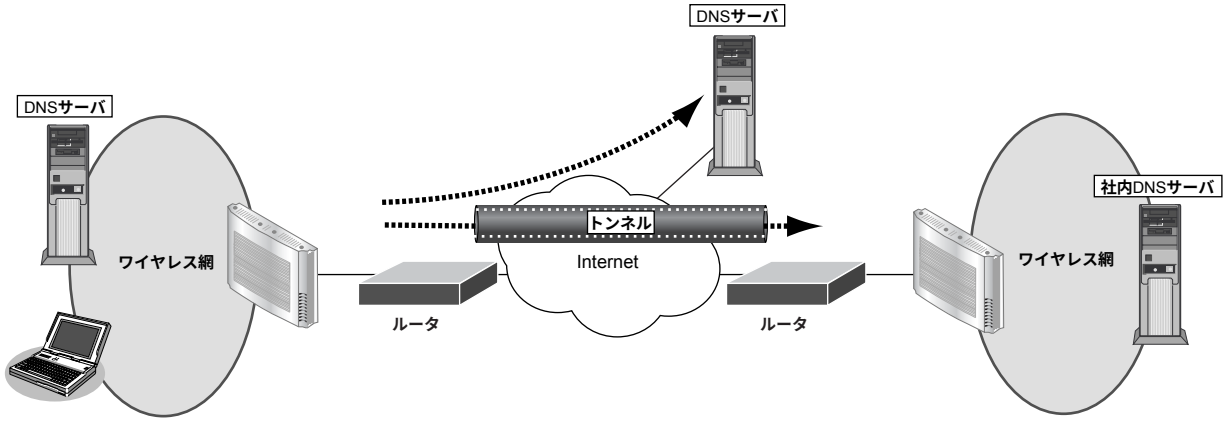
- DNS サーバ（スタティック）機能
- ProxyDNS（DNS 振り分け）機能

2.14.1 DNS サーバ（スタティック）機能

ドメイン名（FQDN：Fully Qualified Domain Name）と IP アドレスの組を静的に設定します。DNS クライアントからの問い合わせ（順引き、逆引き）に対し、設定したエントリを検索し、該当エントリが見つかった場合は応答します。見つからなかった場合は、上位 DNS サーバに問い合わせます。逆引き（IP アドレスから名前を応答）する場合は、応答パケット内に含まれる TYPE と CLASS を、TYPE を A（1 a host address）、CLASS を IN（1the Internet）とします。

2.14.2 ProxyDNS（DNS 振り分け）機能

ProxyDNS（DNS 振り分け）機能は、DNS 機能を使用した場合に問い合わせられた URL（順引き）または IP アドレス（逆引き）により、本装置が問い合わせ先の DNS サーバを自動的に割り振ることができます。そのため、DNS を使用しないで、以下のような環境をリモートサイト側に実現できます。



本装置が端末から DNS の Query メッセージを受信した場合、DNS 振り分けテーブル内に、問い合わせ先のドメイン名と一致するエントリが存在するかどうかをチェックします。一致するエントリが存在する場合は、その一致したエントリの DNS アドレスにメッセージを転送します。一致するエントリが存在しない場合は、デフォルト DNS アドレスにメッセージを転送します。

文字列の後ろから順に設定された文字列長を比較し、すべての文字列が一致している場合に、エントリと一致したと判断します。また、“＊”は特別な文字として、“＊”以降の比較は行わずに該当エントリを一致したと判断します。

設定例）

- ドメイン名　：DNS サーバアドレス
- www.fujitsu.co.jp　：1.1.1.1
- ftp.fujitsu.co.jp　：2.2.2.2
- *.is.fuku.fujitsu.co.jp　：3.3.3.3

デフォルト DNS サーバの設定ができ、上記でエントリを検索できなかった場合は、デフォルトサーバに問い合わせます。

☛ 参照　コマンド設定事例集「10 DNS サーバ機能を使う（ProxyDNS）」（P.104）

2.15 SNMP 機能

適用機種　全機種

SNMP（Simple Network Management Protocol）とは、IP 層および TCP 層レベルの情報を収集、管理するための IP 管理用のプロトコルです。

SNMP 機能では、管理する装置を SNMP マネージャ、管理される装置を SNMP エージェントと言います。

SNMP 機能でネットワークを管理する場合、管理する側は SNMP マネージャ機能を、管理される側は SNMP エージェント機能をサポートしている必要があります。

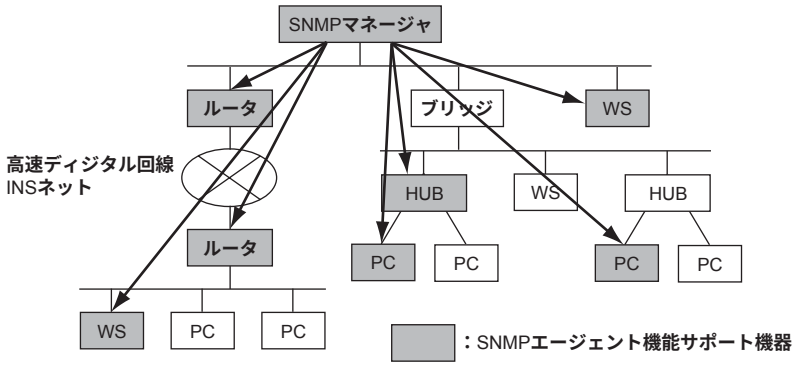
SNMP マネージャ機能は、ネットワーク上の端末の稼動状態や障害状態を一元管理します。SNMP エージェント機能は、SNMP マネージャの要求に対して MIB（Management Information Base：管理情報ベース）という管理情報を返します。

SNMP 機能は、この 2 つの機能を使用して、SNMP マネージャと SNMP エージェントとの間で MIB に定義されたパラメタを送受信してネットワークを管理します。

本装置では、SNMPv1、SNMPv2c および SNMPv3 をサポートします。また、標準 MIB および富士通拡張 MIB をサポートしています。

参照　仕様一覧「3.1 標準 MIB」（P.28）、「3.2 富士通拡張 MIB」（P.37）

SNMP 機能による管理



ヒント

◆ MIB とは

MIB には、装置のベンダに関係ない標準 MIB と装置ベンダ固有の拡張 MIB があります。RFC1213 などで定義される標準 MIB は、管理ノードのそれぞれの管理対象（オブジェクト）にアクセスするための仮想の情報領域です。RFC では、SNMP エージェントが取り付けるべき管理情報を定義しています。管理情報には、SNMP ノードとしてのシステム情報（システム名や管理者名など）や TCP/IP に関連する統計情報があります。しかし、RFC で定義されている項目では伝送路や HUB などを十分に管理できません。そのため、各種プロトコルの情報や各社の装置ごとのベンダ固有に合わせて MIB を拡張します。これを拡張 MIB と言います。

MIB は ASN.1（Abstract Syntax Notation 1）という形式で定義します。SNMP マネージャが拡張 MIB を管理するためには、SNMP エージェント側でその拡張 MIB を公開して、SNMP マネージャがその拡張 MIB の情報を収集するように定義する必要があります。

参照　コマンド設定事例集「12 SNMP エージェント機能を使う」（P.112）

ifIndex の割り当て

本装置の ifIndex の割り当てを以下に示します。

ifIndex	インタフェース／定義との対応
1～	ether ポート （ether ポート番号）
101～	無線 LAN モジュール （100 ＋無線 LAN モジュール定義番号）
10000～	wlan 定義 （10000 ＋無線 LAN インタフェース定義番号）
19000	loopback インタフェース
20000～	lan 定義 （20000 ＋ lan 定義番号）

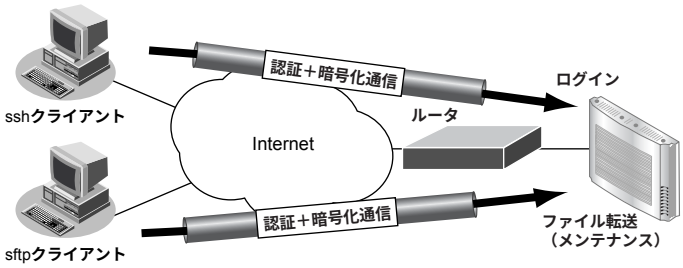
2.16 SSH サーバ機能

適用機種　全機種

SSH サーバ機能とは、TELNET サーバ機能と同じリモートログイン機能（ssh サーバ）と FTP サーバ機能と同じリモートファイル転送機能（sftp サーバ）をサポートしています。

TELNET サーバ機能および FTP サーバ機能では、平文テキストデータのまま通信するため、通信内容を傍受されたり、改ざんされる危険性があります。SSH サーバ機能では、ホスト認証および暗号化通信により、安全で信頼できるログイン機能およびファイル転送機能を利用することができます。

参照　本装置の SSH サーバ機能は、BSD ライセンスに基づいて公開されているフリーソフトウェアの OpenSSH を利用しています。詳しくは、公式サイト（http://www.openssh.com/ ）を参照してください。



※一時点ではどちらか一方の接続のみ

本装置の電源投入時およびリセット時に本装置の SSH ホスト認証鍵が生成されます。生成時間は、数十秒から数分です。SSH ホスト認証鍵生成開始時と完了時にシスログが出力され、生成完了した時点から本装置に SSH 接続することができます。

SSH クライアントソフトウェアにあらかじめ接続相手の SSH ホスト認証鍵を設定しておく必要がある場合は、本装置で show ssh server key dsa コマンドまたは show ssh server key rsa コマンドを実行して表示される SSH ホスト認証鍵を設定します。

本装置に SSH 接続した際に、本装置の SSH ホスト認証鍵が SSH クライアント側に送信されて、設定または保存されている鍵と異なる場合は、SSH 接続が拒否されます。したがって、装置交換などにより、SSH ホスト認証鍵が変更された場合は、SSH クライアントソフトウェアに設定または保存されている SSH ホスト認証鍵を再設定するか削除してから SSH 接続します。

そのあと、パスワード入力プロンプトが表示されますが、SSH ホスト認証などの処理により、表示されるまで多少時間がかかります。

本装置への SSH 接続は、同時に 1 接続しかできないため、SSH 接続中に新たな SSH 接続要求があった場合は、SSH ホスト認証をする前に切断されます。

また、serverinfo ssh/serverinfo sftp コマンドを off に設定することにより、SSH サーバ機能を完全に停止させることができます。

ssh クライアントと sftp クライアントは SSH ポートに接続するため、serverinfo コマンドの ssh または sftp のどちらかが on の場合、本装置の SSH ポートは接続できる状態のままであるため、off に設定した方はパスワード入力まで行われたあとに接続拒否されます。

こんな事に気をつけて

- SSH サーバ機能が完全に停止している状態で本装置を起動し、serverinfo コマンドで SSH 機能のどちらかを有効にして設定を反映した場合、SSH ホスト認証鍵の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。
- 本装置の SSH サーバ機能では、SSH プロトコルバージョン 2 だけをサポートしているため、SSH プロトコルバージョン 2 に対応した SSH クライアントソフトウェア（ssh クライアントソフトウェアおよび sftp クライアントソフトウェア）を使用してください。

以下に、ssh 接続と telnet 接続の相違点を示します。

項目	ssh 接続	telnet 接続
パスワード入力時無入力自動切断時間	2 分 （ログイン中は telnetinfo の設定に従う）	telnetinfo の設定に従う
シスログメッセージ（一部分抜粋）	login ユーザ名	logon telnet

以下に、sftp 接続と ftp 接続の相違点を示します。

項目	sftp 接続	ftp 接続
ユーザ ID 指定	接続前に指定 （一部の sftp クライアントは接続開始時に指定する）	接続後に指定 （一部の ftp クライアントは接続前に指定する）
バイナリモード指定	なし	あり
パッシブモード指定	なし	あり

本装置でサポートする SSH サーバ機能

項目	サポート内容
SSH プロトコルバージョン	SSH プロトコルバージョン 2 だけをサポート
SSH ポート番号／プロトコル	22 ／ TCP
IP プロトコルバージョン	IPv4
ホスト認証プロトコル	RSA
ホスト認証アルゴリズムの種類	ssh-rsa, ssh-dss
暗号方式の種類	aes128-cbc、3des-cbc、blowfish-cbc、cast128-cbc、arcfour、aes192-cbc、aes256-cbc、rijndael-cbc@lysator.liu.se、aes128-ctr、aes192-ctr、aes256-ctr
メッセージ認証コードの種類	hmac-md5、hmac-sha1、hmac-ripemd160、hmac-ripemd160@openssh.com、hmac-sha1-96、hmac-md5-96
同時接続数	1

2.17 USB メモリ機能

適用機種 ***SR-M20AP1, 20AP2***

USB メモリ機能とは、USB メモリに構成定義情報を保存したり、USB メモリから構成定義情報を転送するための機能です。

参照 動作検証済みの USB メモリ（富士通ホームページ）
http://fenics.fujitsu.com/products/manual/usb/

SR-M20AP1 / 20AP2 では以下のファイルシステムをサポートしています。

- FAT12（VFAT）
- FAT16（VFAT）
- FAT32（VFAT）

また、SR-M20AP1 / 20AP2 では以下の作業を行うことができます。

- USB メモリのフォーマット
- USB メモリからの構成定義の転送
- USB メモリへの構成定義の保存
- USB メモリからのファームウェアの更新
- USB メモリへのファームウェアの保存
- USB メモリへの tech-support の保存
- ファイル操作（ファイル一覧の表示、ファイルの削除、ファイルのコピー、ファイル名変更）

こんな事に気をつけて

- **SR-M20AP1 / 20AP2 は VFAT をサポートしているため、ロングファイル名を指定できます。ただし、日本語のファイル名は指定できません。**
- **USB メモリは、複数のパーティションに分割されたものを利用できますが、MS-DOS® の拡張パーティションは利用できません。**
- **ショートカットを利用することはできません。**
- **アクセス中に SR-M20AP1 / 20AP2 から USB メモリを抜いたり、電源切断やリセットを行うと、ファイルシステムが破壊されることがあります。この場合、Flash/Error ランプが橙色で点滅します。**
- **ファイルシステムの不整合を検出すると、Flash/Error ランプが橙色で点滅します。この場合は、USB メモリをフォーマットしてください。**
- **他社製品でフォーマットした USB メモリを利用して不都合が発生した場合は、SR-M20AP1 / 20AP2 でフォーマットし直してください。**
- **論理フォーマット時の FAT 種別（FAT12、FAT16、FAT32）は、USB メモリの容量に応じて自動的に判断されます。**
- **SR-M20AP1 / 20AP2 で USB メモリをフォーマットすると、保存されていた内容はすべて消去され、パーティションは単一になります。フォーマットするときは必要なファイルが残っていないか、十分に注意してください。**
- **USB ポートに、動作保証済み USB メモリ以外の媒体を挿入しないでください。**

2.17.1　構成定義の転送と保存

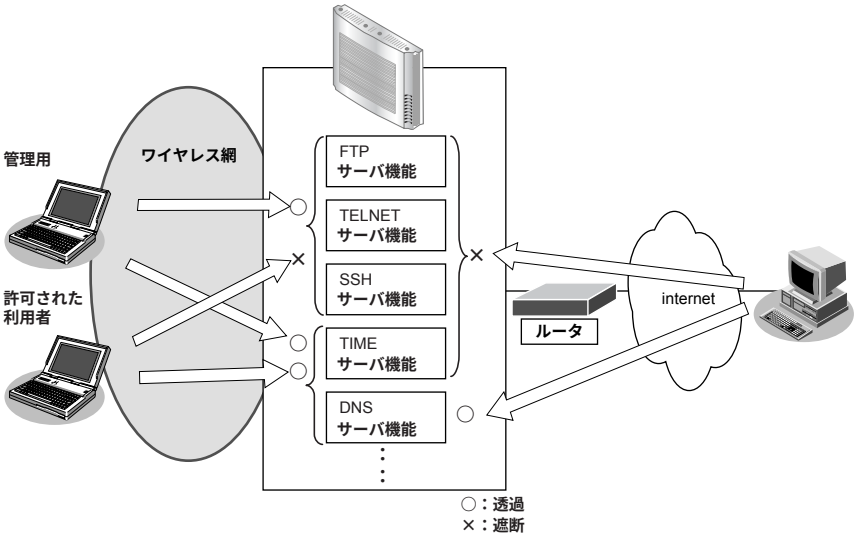
構成定義の転送および保存は、以下の方法で行います。

- copy コマンドで行う場合
  USB メモリのファイルは、/um0/<filename> でアクセスできます。たとえば、USB メモリに格納されている“config.txt”というファイルは、copy コマンドで /um0/config.txt のように指定します。
  USB メモリが複数パーティションに分割されている場合は、先頭のパーティションが利用されます。
  ディレクトリの区切り記号は / です。たとえば、USB メモリの“dir”というディレクトリに格納されている“config.txt”というファイルは、/um0/dir/config.txt のように指定します。
  同様にしてファームウェアの更新および保存ができます。
- Web で行う場合
  Web で行う場合の方法は、Web ユーザーズガイドの「3.3.4 USB メモリを使う」（P.36）を参照してください。

2.18 アプリケーションフィルタ機能

適用機種　全機種

アプリケーションフィルタ機能では、本装置で動作する各サーバ機能に対してアクセスを制限することができます。これにより、本装置のメンテナンスまたは本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することができます。



2.19 IDS機能

適用機種　全機種

IDS（IPv4 不正パケット検知）は、侵入などの不正アクセスによりセキュリティに影響を与えるパケットを検知する機能です。

本装置では、同一 VLAN に属する ETHER ポートおよび無線 LAN インタフェースに対して不正アクセスを検知した場合、システムログとして通知します。

検知対象一覧を以下に示します。

機能分類	検知内容
IP ヘッダ関連	Protocol フィールドが 134 以上のとき
	始点 IP アドレスと終点 IP アドレスが同じとき
	IP ヘッダの長さが length フィールドの長さよりも短いとき
	length フィールドと実際のパケットの長さが違うとき
IP オプションヘッダ関連	オプションヘッダの構造が不正であるとき
	Security and handling restriction header を受信したとき
	Loose source routing header を受信したとき
	Record route header を受信したとき
	Stream identifier header を受信したとき
	Strict source routing header を受信したとき
	Internet timestamp header を受信したとき
ICMP 関連	source quench を受信したとき
	timestamp request を受信したとき
	timestamp reply を受信したとき
	information request を受信したとき
	information reply を受信したとき
	address mask request を受信したとき
	address mask reply を受信したとき
UDP 関連	length フィールドの値が 8 よりも小さいとき
	UDP ヘッダの length フィールドの値が大き過ぎるとき
TCP 関連	フラグに何もセットされていないとき
	SYN と FIN が同時にセットされているとき
	ACK のない FIN を受信したとき
FTP 関連	PORT や PASV コマンドで指定されるポート番号が 1024 ～ 65535 の範囲でないとき

参照　メッセージ集「IDS のメッセージ」

こんな事に気をつけて

- システムログとして通知するためには、syslog pri コマンドでプライオリティ LOG_NOTICE を追加する必要があります。
- プライバシープロテクション機能が無効であり、同一仮想アクセスポイント内の端末どうしの通信が可能な場合、端末どうしの通信に対する VLAN の IDS 設定は無効となります。

2.20 ProxyARP 機能

適用機種　全機種

ProxyARP は、通信相手あての ARP 要求に対して本装置が代理で ARP 要求に応答する機能です。

ARP 要求パケットはネットワーク上にブロードキャストされるために、無線 LAN ネットワーク全体に負荷がかかることになります。ProxyARP 機能が有効な場合は、接続されている無線 LAN 端末の IP アドレスと MAC アドレス情報を管理し、ETHER ポート側から受信した無線 LAN 端末への ARP 要求パケットを無線 LAN ネットワーク側へ転送することはせず、本装置が該当する無線 LAN 端末の MAC アドレスを ARP 応答することで、ネットワーク負荷を軽減することができます。

本装置では、ARP 応答パケットの送信元 MAC アドレスに無線 LAN 端末の MAC アドレスを設定して代理応答する機能をサポートします。

こんな事に気をつけて

本装置に接続してからまったく通信していない無線 LAN 端末が存在する場合や、無線 LAN 端末に対するブリッジの学習テーブルエントリの生存時間が経過してエントリが削除された場合は、この無線 LAN 端末に対する ARP 要求は無線 LAN 端末側へ転送されます。

2.21 POE機能

適用機種　***SR-M20AP1, 20AP2***

IEEE802.3af に準拠したPOE（Power over Ethernet）による給電で動作可能です。

2 ポートから受電している場合は、1 ポートからの給電が停止しても動作を継続します。

2.22 PKI 機能

適用機種 ***SR-M20AC1, 20AC2***

PKI 機能とは、デジタル証明書の作成、登録、削除を行う機能です。

証明書とは、ITU-T 勧告の X.509 に定義されており、本人情報、公開鍵、有効期限、シリアルナンバ、シグネチャなどが含まれています。

PKI 機能を使用するアプリケーションは、以下のとおりです。

- 無線 LAN クライアント機能（EAP 認証方式）

こんな事に気をつけて

- SR-M20AC1 / 20AC2 の PKI 機能では、証明書について認証局（CA）に問い合わせることはできません。
- **認証局証明書は証明書の検証に利用されるため、設定した認証局証明書から発行されていない証明書の場合、検証に失敗することがあります。**
  詳しくは、各アプリケーションの説明を参照してください。
- SR-M20AC1 / 20AC2 は EAP 認証時に受信したデジタル証明書の有効期間を検証するため、システム時刻を正しく設定する必要があります。ご購入時のシステム時刻のままの場合、証明書の有効期限の検証に失敗することがあります。

参照 コマンド設定事例集「2.3 無線 LAN ネットワークで認証・暗号化する」（P.56）

2.23 無線 LAN 管理機能

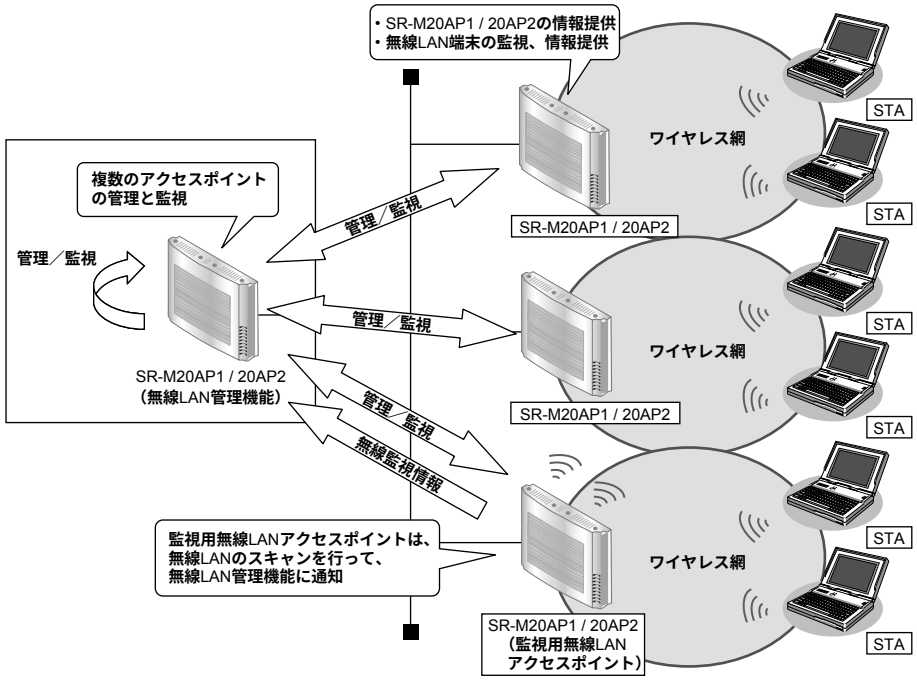
適用機種　***SR-M20AP1, 20AP2***

無線 LAN 管理機能として、以下の機能があります。

- アクセスポイントモニタリング機能
  - アクセスポイントをグループに分け、グループごとに設定、操作、表示を可能とします。
  - アクセスポイントの詳細な情報を表示します。
  - アクセスポイントのネットワーク稼動状況を監視し、状況を表示します。
- 周辺アクセスポイント検出機能
  - 無線 LAN の電波を監視し、周辺に存在するアクセスポイントを検出します。
- クライアントモニタリング機能
  - 無線 LAN の端末・電波強度を監視します。
- MAC アドレスフィルタ配布機能
  - 管理無線 LAN アクセスポイントでの無線 LAN 端末の接続可否をコントロールする MAC アドレスフィルタを集中管理して、配布する機能です。
- 電波出力自動調整機能
  - 管理無線 LAN アクセスポイントの無線送信出力を自動的に調整する機能です。
- 装置リセット機能
  - 管理無線 LAN アクセスポイントをリセットする機能です。
- チャネル自動調整機能
  - 稼動している無線 LAN モジュールに対して、最適な空チャネルまたは無線受信強度が比較的弱いチャネルを自動的に割り当てる機能です。

2.23.1 システム構成

無線 LAN 管理機能が対象とするシステム構成図を以下に示します。



2.23.2　アクセスポイントモニタリング機能

アクセスポイントモニタリング機能として、以下の機能があります。

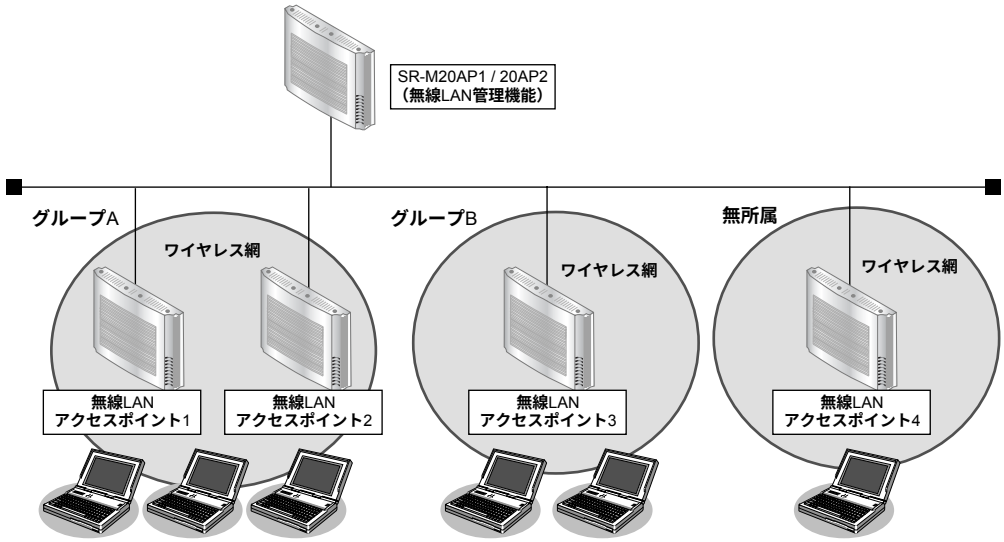
- 管理無線 LAN アクセスポイントのグループ化機能
  関連あるアクセスポイントをグループ単位にまとめて、管理、監視を容易にします。
- 稼動情報の収集機能
  管理無線 LAN アクセスポイントの設定情報を収集する機能です。収集した情報は、表示コマンドで参照することができます。
- 監視機能
  管理無線 LAN アクセスポイントの有線 LAN の監視、および、監視用無線 LAN アクセスポイントを使用して無線 LAN の監視を行います。

管理無線 LAN アクセスポイントのグループ化機能

一般家庭や小規模オフィスの無線 LAN とは異なり、無線 LAN 管理機能が対象とする無線 LAN ネットワークは多数のアクセスポイントによって構成されます。

管理無線 LAN アクセスポイントのグループ化機能は、多数あるアクセスポイントをグループ単位にまとめてることで、管理、監視を容易にさせる機能です。

管理無線 LAN アクセスポイントのグループ化の概念図を以下に示します。



管理グループの構成はネットワーク管理者の任意ですが、アクセスポイントへの設定・操作を効率よく行うために、部署ごと、フロアごとなど、共通の管理、設定をする単位でグループを作成することをお勧めします。

稼動情報の収集機能

管理機能で登録したアクセスポイントから、その稼動情報を収集します。収集する情報は、アクセスポイントの情報とアクセスポイントに接続している、または接続を拒否された無線 LAN 端末の情報です。

管理無線 LAN アクセスポイントに telnet でリモートログインして、コマンド実行により稼動情報の収集を行います。

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）。**

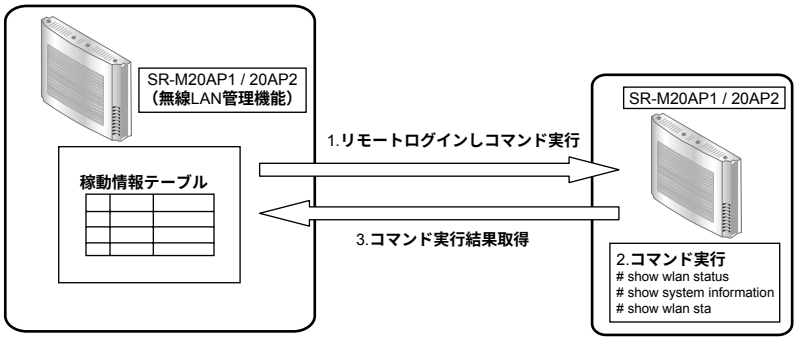
```
# nodemanager login service enable
```

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。**

稼動情報収集のしくみを以下に示します。



監視機能

監視機能は、アクセスポイントの有線 LAN ／無線 LAN の監視を行う機能です。

有線 LAN の監視は、対象となるアクセスポイントに ping を発行して有線 LAN のネットワーク状態を監視します。

無線 LAN の監視は、監視用無線 LAN アクセスポイントのスキャンレポートを取得・解析して、アクセスポイントの無線電波送信状態を監視します。

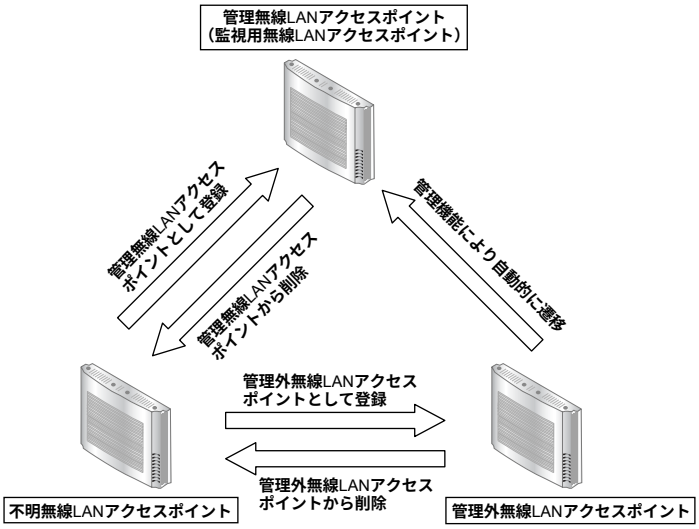
有線 LAN ／無線 LAN の監視結果は、ログとして装置内に一時保存し、その内容をコマンドで表示することができます。

無線 LAN アクセスポイントの種別

監視機能による無線 LAN の監視では、構成定義の設定内容に従って、監視で検出した無線 LAN アクセスポイントを以下に示す 3 つの種別のどれかに分類します。

No.	アクセスポイント種別	説明
1	管理無線 LAN アクセスポイント	無線 LAN 管理機能で監視対象となるアクセスポイントの呼称。 無線 LAN 管理機能は、複数ある管理無線 LAN アクセスポイントの有線 LAN ／無線 LAN の状態を集中監視する。 監視用の設定を行うことで、無線 LAN ネットワークの監視に使用する。
2	管理外無線 LAN アクセスポイント	使用している場所、目的などが明らかで監視する必要がないと判断したアクセスポイントの呼称。 無線 LAN 管理機能は、検出したアクセスポイントのうち、管理無線 LAN アクセスポイントに登録されていないものを、管理外無線 LAN アクセスポイントとして登録できる。
3	不明無線 LAN アクセスポイント	無線 LAN 管理機能で上記のどちらにも分類されないアクセスポイントの呼称。 無線 LAN 管理機能は、不明無線 LAN アクセスポイントの無線 LAN の状態を監視し、ネットワークのセキュリティに問題がないかを監視できる。

アクセスポイント種別の関係を以下に示します。

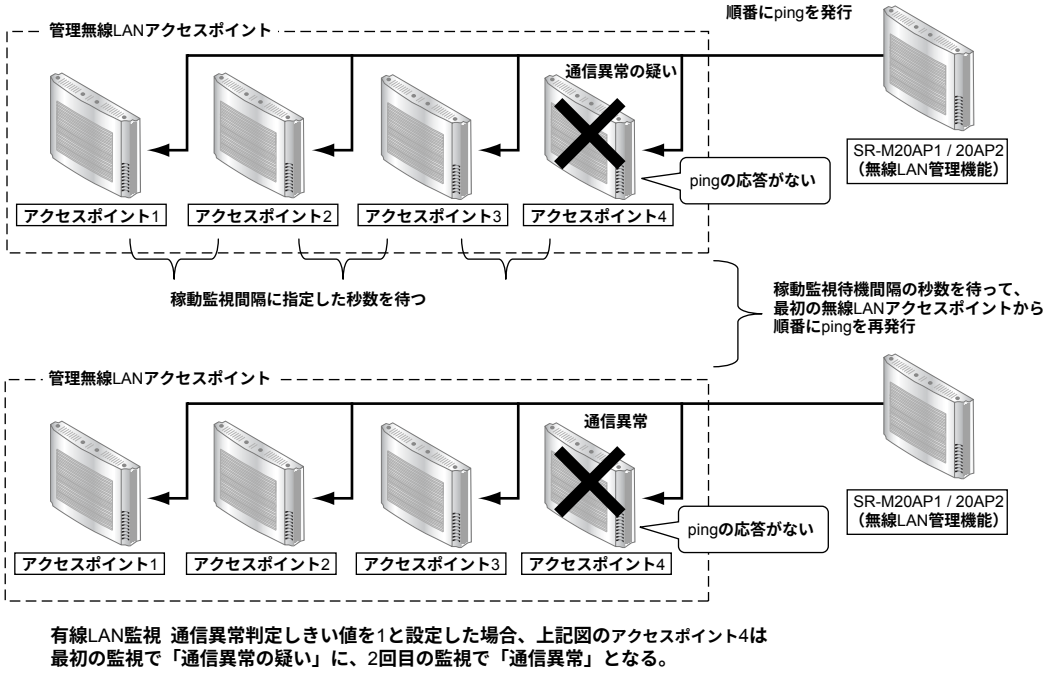


無線 LAN アクセスポイントの種別は、ネットワーク管理者による構成定義から決定されます。ただし、監視の結果、管理外で登録した MAC アドレスが管理無線 LAN アクセスポイントの MAC アドレスであると判明した場合、無線 LAN 管理機能は、自動的にその管理外無線 LAN アクセスポイントの登録を構成定義から削除します。

有線 LAN 監視の方法と監視状態

有線 LAN の通信状態の監視は、監視機能により ping を管理無線 LAN アクセスポイントに対して発行することで行います。監視機能は、その結果について以前の状態から変化があった管理無線 LAN アクセスポイントについて、「正常」、「通信異常の疑い」、「通信異常」の3つに分類して、監視ログとして装置内に保存し、その内容をコマンドで表示することができます。

有線 LAN の通信状態の監視の流れを以下に示します。



有線LAN監視 通信異常判定しきい値を1と設定した場合、上記図のアクセスポイント4は最初の監視で「通信異常の疑い」に、2回目の監視で「通信異常」となる。

無線 LAN 監視の方法と監視状態

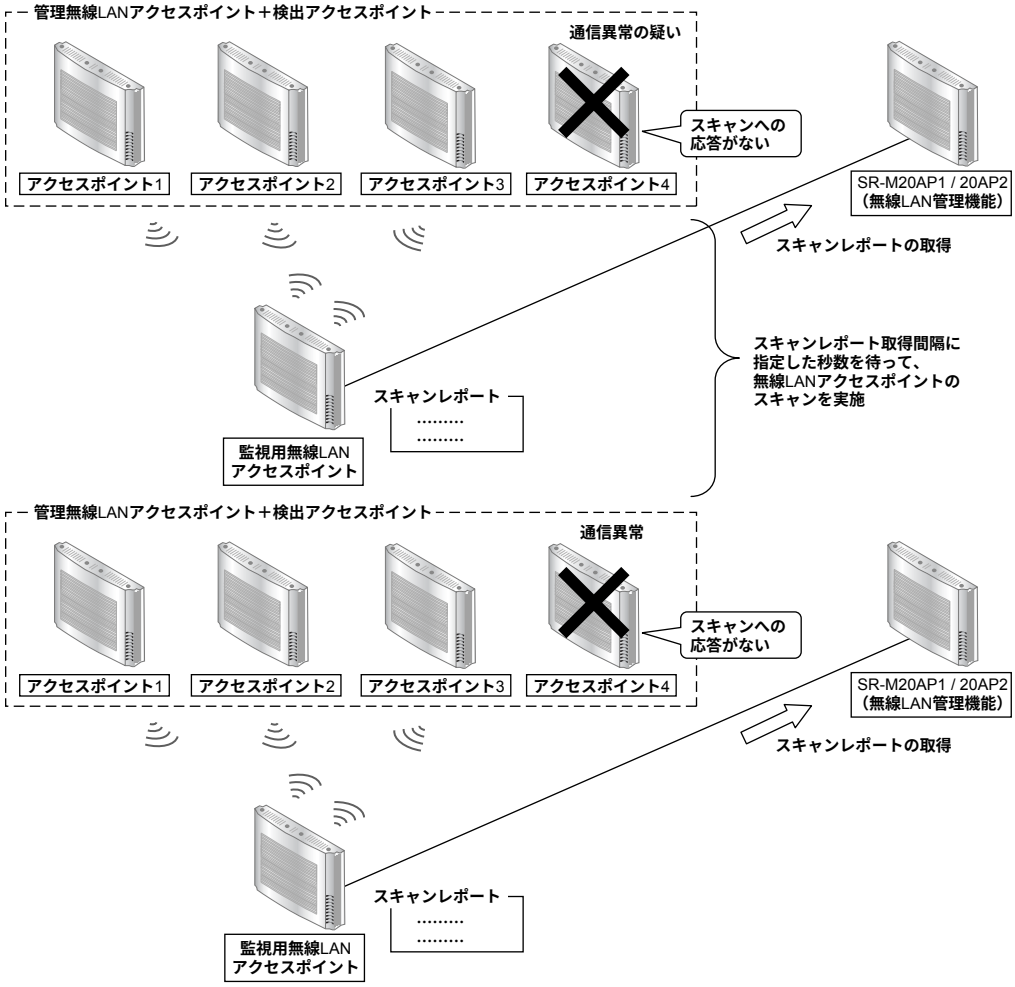
無線 LAN の通信状態の監視は、管理対象であるアクセスポイントの機能：周辺アクセスポイント検出機能（詳細は、「2.1.14 周辺アクセスポイント検出機能」（P.29）を参照）を使用して監視を行っています。監視機能により、監視用無線 LAN アクセスポイントからスキャンレポートを定期的に取得・解析して、「正常」、「通信異常の疑い」、「通信異常」の 3 つに分類したあと、監視ログとして装置内に保存し、その内容をコマンドで表示することができます。

こんな事に気をつけて

無線 LAN の監視できるチャネルの範囲は、周辺アクセスポイントの検出機能の設定に依存します。全チャネルの監視を実施したい場合、以下の環境を構築してください。

- **管理機器にスキャン専用モードに設定したアクセスポイントを加えて、効率的に配置する。**
- **上記の管理機器の構成定義で「管理機器用のスキャン要求の設定」を設定する。**

無線 LAN の通信状態の監視の流れを以下に示します。



無線LAN監視 通信異常判定しきい値を1と設定した場合、上記図のアクセスポイント4は「通信異常の疑い」、「通信異常」と状態が遷移する。

すべての管理無線 LAN アクセスポイントを監視用無線 LAN アクセスポイントに設定できますが、監視実行中は無線 LAN 端末との通信性能が低下しますので、設置する環境に応じて、監視用無線 LAN アクセスポイントを適切に配置してください。

2.23.3　周辺アクセスポイント検出機能

アクセスポイントモニタリングにより無線 LAN 監視を行うことで、周辺に存在するアクセスポイントを検出します。

検出したアクセスポイントは構成定義の設定内容に従って、管理無線 LAN アクセスポイント／管理外無線 LAN アクセスポイント／不明無線 LAN アクセスポイントのどれかに分類して表示します。

2.23.4　クライアントモニタリング機能

管理無線 LAN アクセスポイントと無線 LAN 端末の接続の関係について、以下のモニタリングを行うことができます。

- 無線 LAN インタフェースの無線 LAN 端末情報の表示
  管理無線 LAN アクセスポイントの無線 LAN インタフェースと接続が確立した無線 LAN 端末を確認することができます。
- 接続拒否の無線 LAN 端末情報の表示
  管理無線 LAN アクセスポイントに不正アクセスしようとした無線 LAN 端末の確認や、無線 LAN 端末の接続拒否原因の調査資料を取得することができます。
- 無線 LAN 通信のトレース情報の表示
  管理無線 LAN アクセスポイントの無線 LAN 通信のトレース情報を取得することができます。
- 無線 LAN 端末の RSSI 最大値／最小値一覧の表示
  管理無線 LAN アクセスポイントに接続している無線 LAN 端末からの電波の受信電波強度（RSSI）の状況を取得することができます。取得した情報は管理無線 LAN アクセスポイントの配置や電波出力の妥当性を判断する情報などに利用できます。

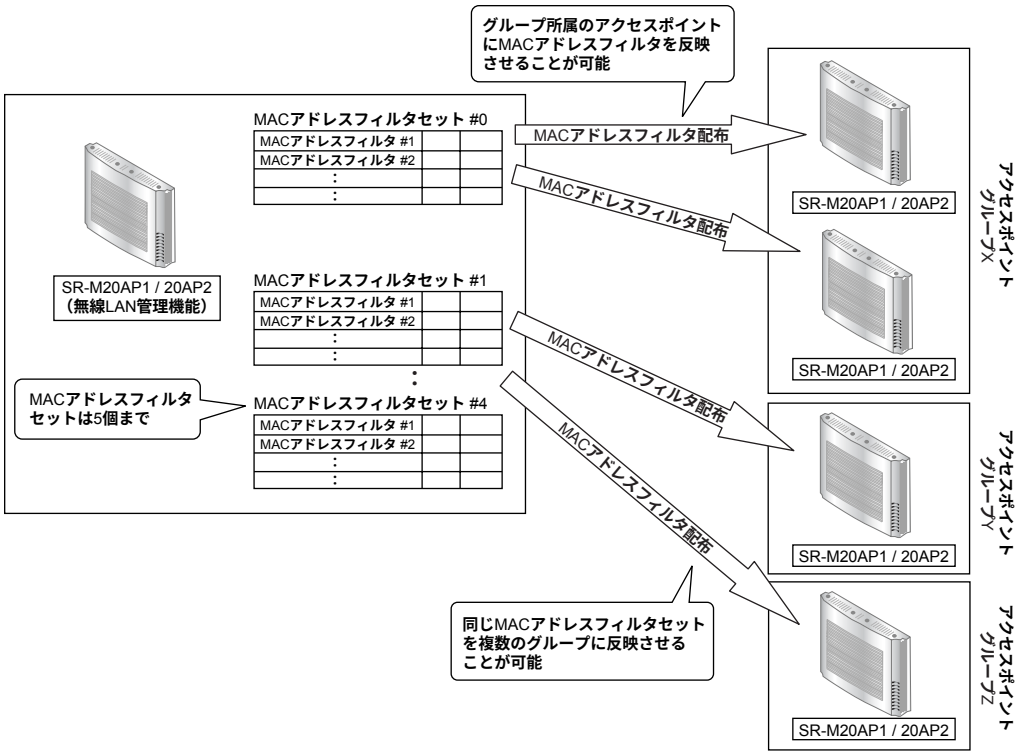
2.23.5　MACアドレスフィルタ配布機能

MACアドレスフィルタとはアクセスポイントが接続端末を制限するためのMACアドレスと処理方法を定義したものです。

無線LAN管理機能は、MACアドレスフィルタの管理、操作を容易にするため、複数のMACアドレスフィルタをまとめて管理するMACアドレスフィルタセットを提供しています。

MACアドレスフィルタ配布機能は、管理無線LANアクセスポイントに対して、MACアドレスフィルタセット単位でMACアドレスフィルタの配布を行います。

MACアドレスフィルタ配布機能のしくみを以下に示します。



2.23.6　電波出力自動調整機能

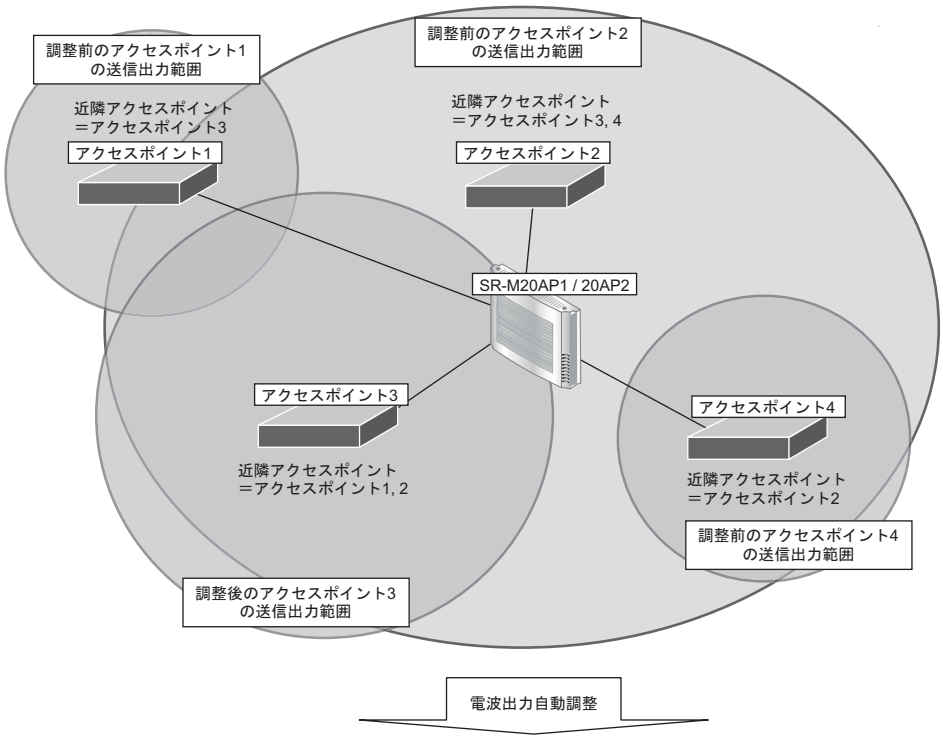
電波出力自動調整機能は、任意のアクセスポイントの無線送信出力を自動的に調整することで、その電波の到達範囲を必要最小限にする機能です。これにより無線LANの第三者による傍受を抑止します。

本機能は、調整対象アクセスポイントの近隣のアクセスポイントで調整対象アクセスポイントの電波を監視して、受信電波が十分に弱くなるまで、調整対象アクセスポイントの無線送信出力を変更します。本機能を利用する際には、近隣のアクセスポイントと、受信電波の強度しきい値を設定します。

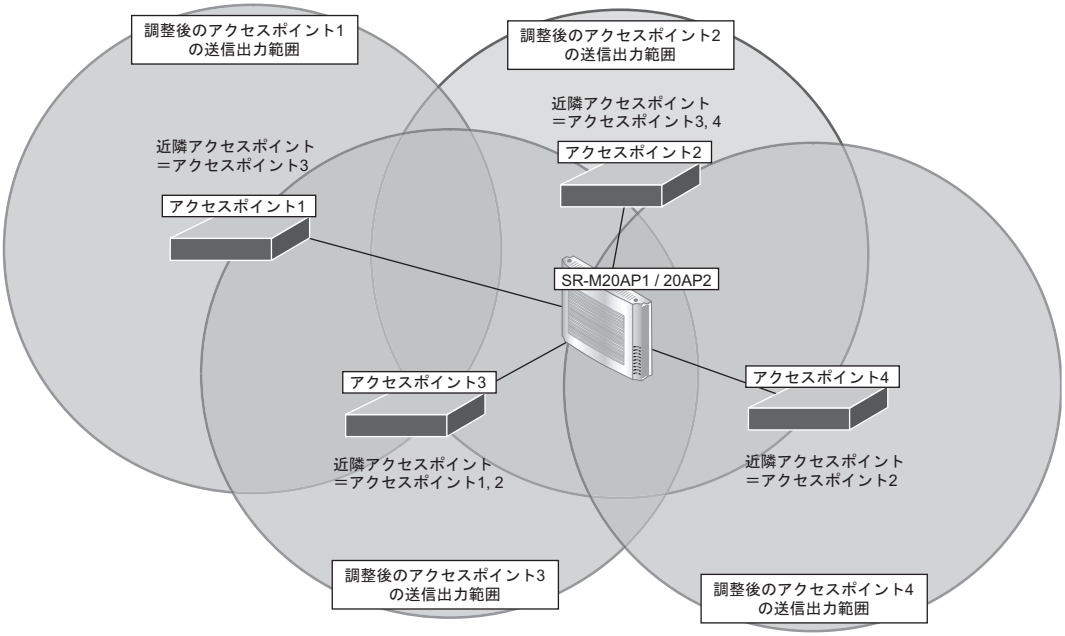
補足　電波出力自動調整機能を使用するには、管理無線LANアクセスポイントが2台以上必要です。

無線送信出力の調整前後の概要を以下に示します。

［無線送信出力の調整前］



［無線送信出力の調整後］



電波出力自動調整の結果、各アクセスポイントの無線送信は、近隣アクセスポイントに指定されたアクセスポイントで確認できるようになる。

電波出力自動調整中は、すべてのアクセスポイントでスキャン機能を頻繁に使用するため、無線 LAN 端末の通信品質が劣化する可能性があります。そのため、本機能は無線 LAN の運用開始前または無線 LAN のメンテナンス時など、無線 LAN の利用者がいないときに行う必要があります。

電波出力自動調整を行ったあとは、電波の届く範囲が調整前よりも狭くなる可能性があります。そのため、無線 LAN 管理者は接続不能になった端末がないか、ローミングを設定している環境でローミングが適切に行えるかを確認してください。

2.23.7　装置リセット機能

装置リセット機能は無線 LAN 管理機能で管理する複数のアクセスポイントに対し、まとめてリセットを行う機能です。

本機能により、構成変更やファームウェア更新後にアクセスポイントを一斉に再起動させることができます。リセット対象として、特定のアクセスポイントと管理グループを指定することができます。

2.23.8　チャネル自動調整機能

チャネル自動調整機能は、無線 LAN アクセスポイントが配置されている周りの無線状況をスキャンして、稼動している無線 LAN モジュール（2.4GHz、5GHz）のそれぞれに対して、最適な空チャネルまたは無線受信強度が比較的弱いチャネルを自動的に割り当てる機能です。

本機能で割り当てる無線 LAN チャネルの範囲は、制御コマンドで設定することが可能です。デフォルトの割り当てチャネルは以下となります。

- 2.4GHz 帯　：1, 6, 11 のチャネルを優先的に割り当てます。
- 5GHz 帯　　：W52, W53, W56 で規定されたチャネルを割り当てます。
- IEEE802.11n 通信で使用する帯域幅 : 20MHz

本機能は、設定対象の無線 LAN アクセスポイントの無線 LAN チャネルを変更しますので、無線 LAN の運用開始前または無線 LAN のメンテナンス時など、無線 LAN の利用者がいないときに行う必要があります。

索引

記号

A

D

E

F

H

I

L

M

P

R

S

T

U

V

W

あ

い

え

お

か

く

こ

し

す

せ

そ

た

ち

つ

て

と

に

の

は

ふ

ほ

ま

む

ゆ

り

ろ

SR-M　機能説明書

P3NK-4142-03Z0

発行日　　2014 年 8 月

発行責任　　富士通株式会社