

AirStation[™]Pro WAPM-APG300N/WAPM-AG300N 設定事例集

このたびは、弊社製AirStationProをお買い 求めいただき、誠にありがとうございます。 本書は、AirStationProの各種設定事例につ いて説明しています。ユーザーズマニュアル とあわせて本書をお読みください。

本書の使い方

本書を正しくお使いいただくための表記上の約束ごとを説明します。

■文中マーク/用語表記

- ▲注意マーク 製品の取り扱いにあたって注意すべき事項です。この注意事項に従わなかった場合、身体や製品に損傷を与えるおそれがあります。
- ▶ マーク 製品の取り扱いに関する補足事項、知っておくべき事項です。

▶参照 マーク 関連のある項目のページを記しています。

- ・文中[]で囲んだ名称は、操作の際に選択するメニュー、ボタン、テキストボックス、チェックボックスなどの名称を表わしています。
- ・文中「」で囲んだ名称は、ソフトウェアやダイアログボックスの名称を表わしています。
- ・本書では原則として弊社製無線アダプタを装着したパソコンを無線パソコン、本製品の設定に
 使用するパソコンを設定用パソコンと表記しています。
- ・ケーブルで接続された10/100/1000BASEのLANとケーブルを使用しない無線LANを明確に するために本書では次の用語を使用しています。

有線LAN…ケーブルで接続されたLAN

無線LAN…無線通信を使用したLAN

上記は、説明のために本書のみで便宜上使用する用語であり、一般的には使用されません。あら かじめご了承ください。

- ■本書の著作権は弊社に帰属します。本書の一部または全部を弊社に無断で転載、複製、改変などを行うことは禁じられております。
- BUFFALO™は、株式会社メルコホールディングスの商標です。AirStation™、AOSS™は、株式会社 パッファローの商標です。本書に記載されている他社製品名は、一般に各社の商標または登録商標です。 本書では™、®、©などのマークは記載していません。
- ■本書に記載された仕様、デザイン、その他の内容については、改良のため予告なしに変更される場合があり、現に 購入された製品とは一部異なることがあります。

■本書の内容に関しては万全を期して作成していますが、万一ご不審な点や誤り、記載漏れなどがありましたら、 お買い求めになった販売店または弊社サポートセンターまでご連絡ください。

- ■本製品は一般的なオフィスや家庭のOA 機器としてお使いください。万一、一般OA 機器以外として使用された ことにより損害が発生した場合、弊社はいかなる責任も負いかねますので、あらかじめご了承ください。
 - 医療機器や人命に直接的または間接的に関わるシステムなど、高い安全性が要求される用途には使用しない でください。
 - 一般OA 機器よりも高い信頼性が要求される機器や電算機システムなどの用途に使用するときは、ご使用になるシステムの安全設計や故障に対する適切な処置を万全におこなってください。
- ■本製品は、日本国内でのみ使用されることを前提に設計、製造されています。日本国外では使用しないでください。また、弊社は、本製品に関して日本国外での保守または技術サポートを行っておりません。
- ■本製品(付属品等を含む)を輸出または提供する場合は、外国為替及び外国貿易法および米国輸出管理関連法規等の規制をご確認の上、必要な手続きをおとりください。
- ■本製品の使用に際しては、本書に記載した使用方法に沿ってご使用ください。特に、注意事項として記載された 取扱方法に違反する使用はお止めください。
- 弊社は、製品の故障に関して一定の条件下で修理を保証しますが、記憶されたデータが消失・破損した場合については、保証しておりません。本製品がハードディスク等の記憶装置の場合または記憶装置に接続して使用するものである場合は、本書に記載された注意事項を遵守してください。また、必要なデータはパックアップを作成してください。お客様が、本書の注意事項に違反し、またはパックアップの作成を怠ったために、データを消失・破棄に伴う損害が発生した場合であっても、弊社はその責任を負いかねますのであらかじめご了承ください。
- ■本製品に起因する債務不履行または不法行為に基づく損害賠償責任は、弊社に故意または重大な過失があった 場合を除き、本製品の購入代金と同額を上限と致します。
- ■本製品に隠れた瑕疵があった場合、無償にて当該瑕疵を修補し、または瑕疵のない同一製品または同等品に交換 致しますが、当該瑕疵に基づく損害賠償の責に任じません。

目次

例1:AOSS/WPSを使って本製品と無線接続する	4
構成例	4
条件	4
使用機器	4
設定手順(Windows 7/Vista)	5
設定手順(Windows XP/2000)	6
CLI設定手順	8
AUSS/WPSで無線接続できないときは	8
例2:プロファイラーを使用する(タイマー)	9
構成例	9
条件	9
使用機器	9
設定手順	10
CLI設定手順	17
例2:部署問のわたっリティーを保たたい(マルチSSID)	10
例3:叩者间のピイエリティーを休らたい(マルテ33D) 構成例	۲۵ 18
	10 18
本口····································	18
没方候品	
CLI設定手順	
例4:部著間のセキュリティーを保ちたい(lagVLAN)	23
備以例	
余什	23
	24
設た于順(LZス1ッナ) 設立壬順(太制具)	24 20
設定于順(本表山) CII設定手順	23
例5:来客用フリースポットの設置(TagVLAN)	35
構成例	35
条件	35
使用機器	35
設定手順(L3スイッチのVLAN設定)	
設定手順(L3スイッチのハードウェアIPフィルター設定)	
設定 手順(不製品)	
ULI設定于順	48

例6:来客用フリースポットの設置(簡易ルーター機能)	49
構成例	49
条件	49
使用機器	49
設定手順(設定用パソコンの設定)	50
設定手順(本製品)	51
CLI設定手順	61
例7:802.1X無線認証を利用する(MACアドレスによる制 62	限の場合).

	62
	63
使用機器	63
設定手順(本製品)	63
CLI設定手順	67
設定手順(RADIUSサーバー)	68

例8:802.1X無線認証を利用する(内蔵RADIUSサーバー機能を₹	川用
する場合)	71
構成例	71
条件	71
使用機器	72
設定手順(本製品)	72
CLI設定手順	77
サプリカント側の設定例	77

例9:社内ネットワークの安全を自動的に保ちたい(Microsoft NAP) 78

構成例	
条件	
使用機器	79
設定手順(L2スイッチの設定)	79
設定手順(Windows Server 2008の設定)	
設定手順(本製品)	
クライアントの設定手順	
CL設定手順	111
例10:スパニングツリーを利用する	112
スパニングツリーについて	112
構成例	112
条件	113
使用機器	113
設定手順(本製品)	113
CL設定手順	116

 例11:マルチキャストスヌーピングを利用する 構成例 条件 使用機器 設定手順 CL設定手順 	117 117 117 117 118 122
例12:USBメモリーに本製品のログを記録する	123
構成例	123
条件	123
使用機器	123
設定手順	124
CLI 設定手順	125
ログ情報の確認方法	126
例13:リピーター機能でローミング環境を構築したい 構成例 条件 使用機器 設定手順(AP1~4共通の設定) 設定手順(AP2 3のリピーター機能の設定)	127 127 127 127 128 128
	130 122
CLI設定手順(AFI *4六/2000)に) CLI設定手順(AP2 2のリピーター機能の設定)	132
例14:リピーター機能で拠点間を無線接続したい 構成例 条件 設定手順	
CLI設定手順	

例1:AOSS/WPSを使って本製品と無線接続する

本製品はAOSS/WPS機能を搭載しており、これらの規格に対応した無線機器をかんたんに接続す ることができます。ここではAOSSもしくはWPS(PBC)を使って、新たに無線機器を本製品に接 続するための手順を紹介します。

構成例



条件

・本製品にすでにAOSS/WPS接続している無線機器がある環境に、新たな無線機器をAOSS/WPSを使って接続する。

・新たに無線機器を追加しても、既存の無線機器は接続と暗号化を維持できる。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・AOSS/WPSに対応したクライアントパソコン

○★モ クライアントパソコンには、あらかじめ「クライアントマネージャV」(Windows 7/ Vistaの場合)または「クライアントマネージャ3」(Windows XP/2000/Me/98SE)が インストールされている必要があります。

設定手順(Windows 7/Vista)

1 [スタート]-[すべてのプログラム]-[BUFFALO]-[エアステーションユー ティリティ]-[クライアントマネージャV]をクリックし、「接続先の作成」をク リックします。



3

画面にしたがって、本製品正面にあるAOSSボタンを5GHz/2.4GHzランプが点 滅するまで(約3秒間)押し続けます。



□ ▶ 〒 本製品正面のAOSSボタンの代わりに、本製品の設定画面([詳細設定]-[無線設定]-[AOSS])にあるAOSSボタンを押して接続設定をすることもできます。

4 接続に成功すると、30秒~1分程度してから、「接続が完了しました」と表示されます。 [保存して閉じる]をクリックします。



以上で接続は完了です。

接続完了後、「ネットワークの場所の設定」画面が表示された場合は、ご利用の環境にあった場所を 選択してください。

▶ 接続に失敗した場合は、5GHz/2.4GHzランプが点滅しますので、もう一度最初から接続をやり直してください。

設定手順(Windows XP/2000)

1 タスクトレイのアアイコンを右クリックし、「プロファイルを表示する」をクリックします。



2 「WPS/AOSS」 「WPS/AOSS」 ボタンをクリックします。



3 画面にしたがって、本製品正面にあるAOSSボタンを5GHz/2.4GHzランプが点滅するまで(約3秒間)押し続けます。



- ▲ 本製品正面のAOSSボタンの代わりに、本製品の設定画面([詳細設定]-[無線設定]-[AOSS])にあるAOSSボタンを押して接続設定をすることもできます。
- **4** 接続に成功すると、30秒~1分程度してから、「~完了しました」と表示されます。 ※Windows XPの場合は、[完了]をクリックして、画面を閉じてください。
- ▶ 接続に失敗した場合は、5GHz/2.4GHzランプが点滅しますので、もう一度最初から接続 をやり直してください。

以上で接続は完了です。

CLI設定手順

AOSS/WPS接続処理をCLIを使っておこなうには、以下のコマンドを入力します。

AOSS設定

```
(profile1)man$ airset aoss start Do you really want to start AOSS, continue? (y/n)y
```

WPS設定

(profile1)man\$ airset wps start

AOSS/WPSで無線接続できないときは...

AOSS/WPSで無線接続できないときは、以下の対策をおこなってください。

- ・本製品とパソコンとの距離が離れすぎていたり、壁や障害物等がある場合は、パソコンを本製品に近づけてからAOSS/WPS接続をおこなってください。
- ・他社製無線接続ツールがインストールされている場合は、削除した後、再度AOSS/WPS接続 をおこなってください。
- ・セキュリティーソフトを一時的に停止してから、AOSS/WPS接続をおこなってください。 AOSS/WPS接続が成功したらセキュリティーソフトを有効にしてください。
- ・無線LAN標準搭載パソコンをお使いの場合は、無線LAN機能がONになっているか、確認して ください。

例2:プロファイラーを使用する(タイマー)

プロファイラー機能とは、プロファイルごとに本製品に設定可能なパラメーターを複数設定でき、 自動もしくは手動で切り替えることができる機能です。この機能を使用することによって、時間帯 によってユーザーを制限したり、通信を制限したりすることができます。

構成例



条件

- ・平日の朝および昼間は本製品の無線機能をONにし、平日の夜間(23:00~30:00)と休日は本製品の無線機能をOFFにする。
- ・プロファイラー機能を使って、上記の切り替えが自動的におこなわれるように設定する。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・クライアントパソコン

設定手順

- 1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。
- 2 「詳細設定」をクリックします。



3 画面左側の[管理設定] – [時刻]をクリックします。 以下のように項目を設定して、[設定]をクリックします。

NTP機能 : 使用する(チェックあり)
 サーバー名 : 任意のNTPサーバーのIPアドレス(またはDNS解決可能なホスト名)
 確認時間 : 24時間毎

- ※ NTPサーバーを使用しない場合は、手動で日付や時刻を入力して[設定]をクリックして ください。
- ※ プロファイル機能有効時においても、本製品の内部時刻が正しくない場合(NTPサー バーもしくは手動で時刻が設定されていない状態)では、プロファイルの切り替えは開始 されません。

時刻/NTP/タイムゾーン 設定 🏼 🔽 ヘルプ

日付時刻設定 🔽 ヘルプ

 日付時刻
 2011 年
 10 月
 16 日
 13 時
 33 分
 24 秒

 設定
 現在の時刻を表示

 現在アクセス中のバソコンから時刻を取る

NTP機能設定 📪 ヘルプ

NTP機能	☑使用する	
サーバー名	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
確認時間	24 時間毎	
設定		



タイムゾーン 日本(GMT+09:00) 🗸 設定

4 画面左側の[管理設定] - [プロファイラ]をクリックします。 [プロファイル情報の編集]をクリックします。

プロファイラ	設定	? ヘルプ
現在、スケジュー	- ラは無効です	
スケジューラ	 ● 無効(手動ブロファイル ○ 有効(自動ブロファイル) 	切り替えモード) 切り替えモード)
現在のブロファイル	profile1 🔽	
設定		
スケジューラを 施されていないお ません。 時刻補正されるま プロファイルー 蜀	「効にしても、NTPもし 「態ではブロファイル :での間「管理ブロフ _こ 。 ・ ・ ・ ・ ・ ・ ・	しくは手動での時刻補正が実 の自動切り替えは開始され ァイル」が使用されます。
No. プロファイル名	色	
1 profile1 (管理)	(使用中)	
2 profile2		
4 profile4		
5 profile5		
6 profile6		
7 profile7		
8 profile8		
プロファイル情報の	編集	

5 コピー元に「profile1」、コピー先に「profile2」を選択し[プロファイルをコピー する]をクリックします。 「コピー先プロファイルの内容は上書きされます」と表示されたら、[設定]をク リックします。

-	10.	ファイラ設定	- プロ	ファイル情報の編集 🔽 ヘルプ
	編舞	を終了して前の画面	へ戻る	
ナロ	リファ	イル ? ヘ/	レプ	
No.	管理	ブロファイル名		色
1	۲	profile1	(使用中)	
2	0	profile2		
3	0	profile3		
4	0	profile4		
5	0	profile5		
6	0	profile6		
7	0	profile7		
8	0	profile8		
設定				
۲IJ ۱	<i>プロ</i> : 期化す	ファイルを初期化する るブロファイル: Pri	ofile1 💌	
	700	ファイルをコピーする		coffie?

プロファイルのコピーが終わったら、[編集を終了して前の画面へ戻る]をクリックします。

6 「現在のプロファイル」を「profile2」に変更して[設定]をクリックします。

プロファイラ	設定	? ヘルプ	
現在、スケジュー	ラは無効で	ब	
スケジューラ	 ● 無効(手動) ○ 有効(自動) 	パロファイル切り替えモー パロファイル切り替えモー	۲) ۲)
現在のプロファイル	profile1 🗸		
設定 スケジューラを有 での時刻補正が実 ファイルの自動切 時刻補正されるま が使用されます。	profile1 profile3 profile4 profile5 profile6 profile7 profile8 にい同一管	、NTPもしくは手乗 ない状態ではブロ 始されません。 理ブロファイル」)
ブロファイル一覧	? ヘル	プ	_
No. ブロファイル名	色		
1 profile1 (管理) ((使用中)		
2 profile2			
3 profile3			
4 profile4			
5 profile5			
6 profile6			
7 profile7			
8 profile8			
プロファイル 情報の	編集		

7 画面左側の[無線設定]-[(802.11aの)無線基本]をクリックします。 「無線機能」の「使用する」のチェックを外して、[設定]をクリックします。

無線基本設定(11a)	? ヘルブ
無線機能	□使用する
SSID	 エアステーションのMACアドレスを設定(XXXXXXXX_A) 値を入力:
VLAN ID	1
無線チャンネル	Auto(W52) (現在のチャンネル: 38+40) モード 倍速モード(40MHz) 🖌
[拡張設定]	
無線モード	11aと11nを同時利用する 🔽
	6Mbps: たし Rate BasicRate 9Mbps: たし Rate BasicRate 12Mbps: たし Rate BasicRate
RateSet (11a)	18Mbps: たし Rate BasicRate 24Mbps: たし Rate BasicRate 38Mbps: たし Rate BasicRate



手順7と同様に、802.11gの無線機能を無効にします。

9 画面左側の[管理設定] - [プロファイラ]をクリックします。 「スケジュール一覧」の[タイムテーブルの編集]をクリックします。

4 profile4
5 profile5
6 profile6
7 profile7
8 profile8
プロファイル情報の編集
スケジュール一覧 🤗 ヘルプ
No. 年 月 日 曜日指定 ブロファイル指定
日付指定のタイムテーブルは登録されていません
No. 曜日 開始時間 終了時間 ブロファイル名
曜日・時間指定のタイムテーブルは登録されていません
タイムテーブルの編集
2 ヘルプ
タイムテーフル
 週間スケジュール
スケジュール表示
○ 全てのスケシュール

10「タイムテーブルの新規追加」で、平日の夜間に無線機能がOFFになるよう、下記のように設定して、[新規追加]をクリックします。

指定方法	:	曜日・時間で指定する
曜日	:	月~金を有効(チェックあり)、日と土を無効(チェックなし)
設定時間	:	23時00分~30時00分
プロファイル	:	profile2

プロファイラ設定 - タイムテーブルの編集 🔽 ヘルプ

編集を終了して前の画面へ戻る

ダイムナーブルの新規追加 📕 🎫				
指定方法	○日付で指定する ④曜日・時間で指定する			
年月日	年 月 日			
曜日	 Ⅰ月火水木金土 ☑ ☑ ☑ ☑ ☑ □ 			
設定時間	23 💙時 00 💙分 ~ 30 💙時 00 💙分			
ブロファイルの選択	● プロファイルで指定する ○ 他の曜日の設定を使用する			
プロファイル	profile2 💌			
曜日を指定				

新規追加

11 手順10と同様に、「タイムテーブルの新規追加」で、休日に無線機能がOFFになる よう、下記のように設定して、[新規追加]をクリックします。

:	曜日・時間で指定する
:	月~金を無効(チェックなし)、日と土を有効(チェックあり)
:	06時00分~30時00分
:	profile2
	:

プロファイラ設定 - タイムテーブルの編集 🔽 ヘルプ

編集を終了して前の画面へ戻る					
タイムテーブルの新規追加 🧣 ヘルプ					
指定方法	○日付で指定する ● 曜日・時間で指定する				
年月日	年 月 日				
曜日					
設定時間	06 🗸時 00 🗸 分 ~ 30 🗸時 00 🗸 分				
ブロファイルの選択	● プロファイルで指定する ○ 他の曜日の設定を使用する				
プロファイル	profile2 💌				
曜日を指定					

新規追加

設定が終わったら、[編集を終了して前の画面へ戻る]をクリックします。

12「現在のプロファイル」で「profile1」を選択し、[設定]をクリックします。

プロファイラ	? ヘルプ		
現在、スケジュー	ラは無効	です	
スケジューラ	 ● 無効(手 ○ 有効(自 	動ブロファイル切り替えモード) 動ブロファイル切り替えモード)	
現在のブロファイル	profile2 🔽		
設定	profile1 profile2 profile3 profile4		
スケジューラを有 実施されていない されません。 時刻補正されるま	profile5 profile6 profile7 profile8 CVD[a] I	も、NTPもしくは手動で ブロファイルの自動切り 管理ブロファイル」が使	の時刻補正が 替えは開始 [用されま
ब .			

- 13「スケジューラ」で「有効(自動プロファイル切り替えモード)」を選択して、[設定] をクリックします。
 - ※ スケジューラーを有効にした場合、本製品の設定変更ができなくなることがあります。 その場合は、いったんスケジューラーを無効にし、必要なプロファイルに切り替えてから 設定を変更し、その後、スケジューラーを有効にしてください。

プロファイラ	? ヘルプ	
現在、スケジュー	ラは無効です	
スケジューラ	 (手動ブロファイル切り替えモード) (自動ブロファイル切り替えモード) 	
現在のブロファイル	profile1 🗸	
設定		
スケジューラを有 実施されていない されません。 時刻補正されるま す。	効にしても、NTPもしくは手動で 状態ではブロファイルの自動切り での間「管理ブロファイル」が6	の時刻補正が り替えは開始 使用されま

14 登録したスケジュールが「スケジュール一覧」と「タイムテーブル」に表示されていることを確認します。

スケジョ	1 – N –	·覧	? ^/	レプ							
No.年) 日付指定の	No. 年 月 日 曜日指定 ブロファイル指定 日付指定のタイムテーブルは登録されていません										
No. 曜日 1 日 月 2 日 月	 火水オ 火水オ	、金 土 < ☆ 土	開始時間 23:00 06:00] 終了時 30:00 30:00	潤 ブI pro pro	コファイ file2 file2	′ル名				
	テーブルロ	刀編集									
タイム き スケジュ	テー ブル ール表示	↓ ○辺 ○全	ヘルフ 間スケジョ てのスケジ	* - ール ジュール							
06	08	10	12	14	16	18	20	22	24	26	28
B											
月											
火											
水											
木											
金											
+											

以上で本製品の設定は完了です。

CLI設定手順

ここまでの設定をCLIを使っておこなうには、以下のコマンドを入力します。

NTPサーバー(例:ntp.buffalo.jp)から時刻を自動取得する場合 (profile1)man\$ setup ntp client enable server ntp.buffalo.jp interval 24 手動で時刻(2011年12月31日12時34分56秒)を設定する場合 (profile1)man\$ setup date 2011/12/31 12:34:56 (profile1)man\$ edit start profnum 1 (profile1)man[edit]\$ profile copy profname Profile1 to profname Profile2 force APXXXXXXXXXXXX (profile1) (profile1)man[edit]\$ profile switch profname profile2 force (profile2)man[edit]\$ airset 11a wireless disable (profile2)man[edit]\$ airset 11g wireless disable (profile2)man[edit]\$ profile schedule add week weekdays from 23:00 to 30:00 profname profile2 (profile2)man[edit]\$ profile schedule add week weekend from 6:00 to 30:00 profname profile2 (profile2)man[edit]\$ profile switch profname profile1 force (profile1)man[edit]\$ profile schedule enable force <再起動> Hello!

APXXXXXXXXXXX Welcome to BUFFALO CLI (profile1)man\$

例3:部署間のセキュリティーを保ちたい(マルチSSID)

本製品は1台で複数の無線ネットワークを設定することができます。この機能を利用すると、あた かも複数台のエアステーションが設置されているかのようなネットワークを構築することができ ます。

ここでは例として、VLANを使用せずに簡易的にネットワークを分ける方法を説明します。

構成例



条件

- ・無線でインターネットに接続できる環境で、人事部と営業部など他部署間での無線通信に制限を設ける。(他部署間では無線通信を禁止する)*
 ※
 ※
 (補留間では無線通信を禁止する)
- ・802.11a、802.11gともにメインの無線がすでに動作している。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

- ・クライアントパソコン
- ・有線側ネットワーク機器(例:スイッチ、ルーターなど)

設定手順

- 1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。
- 2 「詳細設定」をクリックします。



3 画面左側の[無線設定]-[(使用する無線規格の)マルチSSID]をクリックし、[マ ルチSSID登録情報の編集]をクリックします。

マルチSSID設定(11a) <u>?</u> ヘルプ	P
SSID YLAN ID 認証 暗号化 状態	
マルチSSIDの設定は登録されていません	
マルチSSD登録情報の編集	

4 営業部の設定をおこないます。 以下のように項目を設定して、[新規追加]をクリックします。

55ID	•	Elgyo
VLANID	:	1(変更なし)
無線の認証	:	WPA2-PSK
追加認証	:	追加認証を行わない
無線の暗号化	:	AES
WPA-PSK(事前共有キー)	:	abcdefgh(任意の値)、Key更新間隔:60(分)
ANY接続	:	許可する(チェックあり)
プライバシーセパレーター	:	SSIDセパレーター

編集を終了して前の画面へ戻る

SSID	Eigyo
VLAN ID	1
無線の認証	 記録正を行わたし、) IEEE802.1×/EAP WPA-PSK WPA/WFA2 mixedmode - PSK WPA-WFA2 mixedmode - PSK WPA-EAP WPA-WFA2 mixedmode - EAP
道力認忍証	 適加認証を行わない MACアドレスリストによる制限 MAC・アドレスリストルはよる制限 MAC・FADIUS認証 認証がスワード MAC・FADIUS認証 (MAC・FADIUS認証) MAC・FFレスを使う (次のパスワードを使う) (次のパスワードを使う) (加Gresoft WPを使用する) 制ICFネットワークに使用するいLAII: [4093
無線の暗号化	 ff 寄行化なし 𝔅𝔅𝔅(𝔅) 𝔅𝔅𝔅(𝔅) 𝔅𝔅(𝔅) 𝔅𝔅(𝔅) 𝔅𝔅 𝔅𝔅(𝔅) 𝔅𝔅 𝔅𝔅 𝔅𝔅 𝔅𝔅 𝔅𝔅 𝔅𝔅 𝔅𝔅 𝔅𝔅 𝔅𝔅 𝔅𝔅 𝔅 𝔅𝔅 𝔅𝔅 𝔅 𝔅𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅 𝔅
[拡張設定]	NOYX_4/IIB/NA
ANV接続	
11111356005	L 81 9 9

5 [設定]をクリックします。

6 人事部の設定をおこないます。 以下のように項目を設定して、[新規追加]をクリックします。

SSID	:	Jinji
VLANID	:	1(変更なし)
無線の認証	:	WPA2-PSK
追加認証	:	追加認証を行わない
無線の暗号化	:	AES
WPA-PSK(事前共有キー)	:	ijklmnop(任意の値)、Key更新間隔:60(分)
ANY接続	:	許可する(チェックあり)
プライバシーセパレーター	:	SSIDセパレーター

マルチSSID設定 - マルチSSIDの編集(11a) 🛛 🛛 🧣 ヘルプ

編集を終了して前の画面へ戻る

マルチSSID登録情報の	新規追加 💽 ヘルプ
SSID	Jinji
VLAN ID	1
無線の認証	○ 22212 老(न†/) ζ4(.) ○ 1742 E802.1 ×/EAP ○ 1874-75K
<u>这</u> 办吃228正	 ● 追加認知を行わない ● MACアドレスリストによる制限 ● MACアドレスリスト+MAC-RADIUS認証 ● MACアドレスを使う ● MACアドレスを使う ● Xのパスワードを使う ● MICrosoft NAPを使用する 割限ネットワーグに使用するVLAM: 4093
無線の暗号化	 日毎月になし ● 日年(前定信/k-e) ● 10(1) ● 10(1)<!--</th-->
[拡張設定]	
ANY接続	☑ 比可才ろ
ブライバシーセパレーター	SSEt231

新規追加

7 [設定]をクリックします。

以上で本製品の設定は完了です。

無線パソコンからそれぞれのSSIDを使って、ネットワークへ接続してください。接続手順は、無線 パソコンまたは無線子機のマニュアルを参照してください。

※ クライアントマネージャ3をお使いの場合は、プロファイルのインポート/エクスポート機能 を使うと、複数のパソコンへの設定が簡単におこなえます。プロファイルのインポート/エクス ポート機能については、クライアントマネージャ3のヘルプを参照してください。

CLI設定手順

ここまでの設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ airset 11a ssid add ssidname Eigyo vlanid 1
auth wpa2psk cipher aes rekey 60 key abcdefgh
(profile1)man[edit]$ airset 11a ssid privacy ssidname Eigyo ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Eigyo enable
(profile1)man[edit]$ airset 11a ssid add ssidname Jinji vlanid 1
auth wpa2psk cipher aes rekey 60 key ijklmnop
(profile1)man[edit]$ airset 11a ssid privacy ssidname Jinji ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Jinji enable
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Jinji enable
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

例4:部署間のセキュリティーを保ちたい(TagVLAN)

本製品は1台で複数の無線ネットワークを設定することができます。この機能を利用すると、あた かも複数台のエアステーションが設置されているかのようなネットワークを構築することができ ます。

ここでは例として、既存のVLANネットワークに本製品を追加する方法を説明します。



条件

- ・各階にTagVLANに対応したL2スイッチ(例:BS-G2024MR(別売))が導入されている。
- ・TagVLANを利用して、L2スイッチ同士を接続する。
- ・本製品の有線ポートとL2スイッチをTrunk接続する。
- ・本製品の管理をおこなう管理部と、本製品の管理VLANを統一する。
- ・各部署のサーバーにVLAN、SSIDを使用して接続できるようにする。
- ・他部署のサーバーやパソコンへは通信できないようにする。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・クライアントパソコン

・有線側ネットワーク機器(例:TagVLANに対応したL2スイッチなど)

設定手順(L2スイッチ)

Webブラウザーを使って、ネットワークからL2スイッチへログインし、TagVLANの設定をおこないます。(ここでは例として、BS-G2024MR(別売)を使用します)

本製品と接続



1 L2スイッチのマニュアルを参照して、L2スイッチの設定画面を表示します。

2 [詳細設定]-[VLAN設定]-[VLANステータス]をクリックします。

3 管理部のVLAN(101)を作成します。 以下のように項目を設定して、[追加]をクリックします。

VLAN ID	-	101
VLAN名	:	Kanri
VLAN Management	:	チェックあり
ポート	:	1~2を「Static Tagged」、3~8を「Static Untagged」、9~24を
		「Not Member」

VLANステータス

	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	VLAN 名
	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
I	PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged U:Static Untagged -:Not Member

新規VLAN 作成

VLAN ID:	1	01	(1-4	4094	4)																			
VLAN 名:	K	anri																						
VLAN Managemer	nt: 🖪																							
ボート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static Tagged	۲	۲	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\circ	\bigcirc														
Static Untagged	\bigcirc	\bigcirc	۲	۲	۲	۲	۲	۲	$^{\circ}$	\bigcirc														
Not Member	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲							

設定 再読込 クリア

4 人事部のVLAN(102)を作成します。 以下のように項目を設定して、[追加]をクリックします。

VLAN ID	:	102
VLAN名	:	Jinji
VLAN Management	:	チェックなし
ポート	:	1~2を「Static Tagged」、9~16を「Static Untagged」、3~8お
		よび17~24を「Not Member」

VLANステータス

VLAN 名	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	VLAN ID
	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	1
Kanri	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	U	U	U	U	U	U	Т	Т	101
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	PVID



新規VLAN 作成

VLAN ID:	102	(1-4094)
VLAN 名:	Jinji	
VLAN Management:		

ボート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static Tagged	۲	۲	\bigcirc																					
Static Untagged	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲	\bigcirc														
Not Member	\bigcirc	\bigcirc	۲	۲	۲	۲	۲	۲	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲							

設定 再読込 クリア

5 営業部のVLAN(103)を作成します。 以下のように項目を設定して、[追加]をクリックします。

VLAN ID	:	103
VLAN名	:	Eigyo
VLAN Management	:	チェックなし
ポート	:	1~2を「Static Tagged」、17~24を「Static Untagged」、3~
		16を「Not Member」

VLANステータス

VI	AN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	VLAN 名
	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
	101	Т	Т	U	U	U	U	U	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Kanri
	102	Т	Т	-	-	-	-	-	-	U	U	U	U	U	U	U	U	-	-	-	-	-	-	-	-	Jinji
	PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged	U:Static Untagged	-:Not Member
-----------------	-------------------	--------------

新規VLAN 作成

VLAN ID:	1	03	(1-	4094	4)																			
VLAN 名:	E	igyo																						
VLAN Managemer	nt: [
ボート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static Tagged	۲	۲	\bigcirc																					
Static Untagged	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲															
Not Member	\bigcirc	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	\bigcirc							
(設定) 「再読込」 ク	リア																							

6 [詳細設定]-[VLAN設定]-[VLANポート設定]をクリックします。

7 各ポートにPVIDを設定します。 以下のように項目を設定して、[設定]をクリックします。 ポート1~8 : 101 ポート9~16 : 102 ポート17~24 : 103

VLANボート設定

ボート	1	3	5	7	9	11	13	15	17	19	21	23
PVID	101	101	101	101	102	102	102	102	103	103	103	103
ボート	2	4	6	8	10	12	14	16	18	20	22	24
PVID	101	101	101	101	102	102	102	102	103	103	103	103

設定 再読込

- 8 [詳細設定]-[VLAN設定]-[VLANステータス]をクリックします。
- 9 VLANステータスに表示されているVLAN1の欄にある[編集]をクリックします。

10 VLAN1に所属するポートをすべて「Not Member」に設定します。 以下のように項目を設定して、[設定]をクリックします。

VLAN ID	:]
VLAN名	:	空欄
VLAN Management	:	チェックなし
ポート	:	1∼24を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
101	Т	Т	U	U	U	U	U	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
102	Т	Т	-	-	-	-	-	-	U	U	U	U	U	U	U	U	-	-	-	-	-	-	-	-	
103	Т	Т	-	-	-	-	-	-	-	-	-	-	-	-	-	-	U	U	U	U	U	U	U	U	
PVID	101	101	101	101	101	101	101	101	102	102	102	102	102	102	102	102	103	103	103	103	103	103	103	103	

T:Static Tagged U:Static Untagged -:Not Member

新規VLAN 作成

VLAN ID:	1		(1-	4094	1)																			
VLAN 名:	Ē		••		1																			
VLAN Managemer	nt: [
ボート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static Tagged	\bigcirc																							
Static Untagged	\bigcirc																							
Not Member	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲
【設定】 [再読込] [ク	リア																							

以上でL2スイッチの設定は完了です。 続いて、本製品の設定をおこないます。

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、VLANおよびマルチSSIDの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

糖能設定			
機能設定			
		■プロファイラ情報	
無 線		6	
無線LANの暗号化を設定する(WEP/TKIP/AES)		profile1	
無線LANの暗号化を設定する(RADIUSサーバーを使う)).		
※ 無線LANの基本設定をする		サブネット 情報	
インターネット		サブネット 1:[Manage	ement](VLAN 1)
※ <u>インターネット接続を設定する</u>		協調式能 未取得	
その他		(DHCP クラ	イアント:収得中)
ン エアステーションのファームウェアを更新する エフステ、ションの設定を知識化せる。		「解放」「書	さ換え
→ エアスフェンヨンの設定で初期目上する			
		■無線情報	
		IEEE 802.11a (Aut	to(W52) /
		36+40ch)	
		551U XXXXX	(XXXXXX_A
		記証万式 VPA-P S	SK
		暗号化 AES	
		マルチSSID 無効	
		IEEE 802.11g (Aut	io(1~11 ch) /
		11ch J	//////////
		初行士士 (104 日本 104 104 104 104 104 104 104 104 104 104	www.www.u
		BGBL/JJA、 ¥FA-F6 座空化 AE0	5K
		イルナ5510 売切	
	, i i i i i i i i i i i i i i i i i i i	Language	
		Japanese 🔽 🗌 Chan	se Language
		(([])) A055 AO	SS 設定画面へ

3 画面左側の[無線設定]-[(使用する無線規格の)マルチSSID]をクリックし、[マルチSSID登録情報の編集]をクリックします。

マルチSSID設定(11a) <u>?</u> ヘルプ
SSID VLAN ID 認証 暗号化 状態
マルチSSIDの設定は登録されていません
マルチSSD登録情報の編集

4 管理部の設定をおこないます。 以下のように項目を設定して、[新規追加]をクリックします。 SSID

33ID	•	Ndfiff
VLAN ID	:	101
無線の認証	:	WPA2-PSK
追加認証	:	追加認証を行わない
無線の暗号化	:	AES
WPA-PSK(事前共有キー)	:	abcdefgh(任意の値)、Key更新間隔:60(分)
ANY接続	:	許可する(チェックあり)
プライバシーセパレーター	:	SSIDセパレーター

マルチSSID設定 - マルチSSIDの編集(11a) 🛛 🛛 🤗 ヘルプ

編集を終了して前の画面へ戻る

マルノ 3310 豆 軒 旧 五	
SSID	Kanri
VLAN ID	101
無線の認証	記録基を行わたい IEEE802.1%だらP WPA-PSK WPA-PSK WPA-WWA2 mixedmode - PSK WPA-EAP WPA-EAP WPA-EAP WPA-EAP WPA-WPA2 mixedmode - EAP
迫力感恐奮正	 ・ 道加認証を行わない MACアドレスリストによる制限 MACアドレスリストによる制限 MAC-PAD1USIZ01 2001/2017 2001/2017<
無線の暗号化	 ● 昭号化なし ● 昭号化なし ● 取り(固定億key) ● 取り(固定億key) ● 自動夏邦kry長 ● WEP(自動起信key) ● 自動夏年間key2の供用 ● 研してい、● ● AES ● TKIP ● AES ● TKIP/AES elsed
[拡張設定]	······································
ANY接続	✓ 注示する
プライバシーヤバレー	

5 [設定]をクリックします。

WAPM-APG300N/WAPM-AG300N 設定事例集 31

7 [設定]をクリックします。

新規追加

無線の調整	● WPA2-PSK									
WARK-CORPORT	O WPA/WPA2 mixedmode - PSK									
	O WPA-EAP									
	O WPA2-EAP									
	○WPA/WPA2 mixedmode - EAP									
	 追加認証を行わない 									
	○ MACアドレスリストによる制限									
	○ MACアドレスリスト+MAC-RADIUS認証									
	 MAC-RADIUS設計 認識がスワード 									
追加認証	● MACアドレスを使う									
	○次のバスワードを使う									
	○ Microsoft NAPを使用する									
	制限ネットワークに使用するVLAN: 4093									
	 ・ ・ ・									
	○ WEP(固定値Key)									
	₩EP暗号化キー 文字入力・13文字(WEP128) ▼									
	○ WEP(自動配信Key)									
	自動更新Key長 WEP128 🗸									
無線の暗号化	WEP(固定値Key)の併用 併用しない 🗸									
WWW 000 0 10	暗号化キー									
	O TKIP									
	 AES 									
	○ TKIP/AES mixed ₩PA-PSK(事前共有キー):									
	•••••									
	Key更新間隔: 60 分									
[拡張設定]										
ANY接続	 評可する 									
ブライバシーセパレーター	SSIDセバレーター 🗸									

編集を終了して前の画面へ戻る

SSID

VLAN ID

マルチSSID登録情報の新規追加 🍞 ヘルプ

Jinji

102 ○ 認証を行わない ○ IEEE802.1×/EAP ○ WPA-PSK

マルチSSID設定 - マルチSSIDの編集(11a)

人事部の設定をおこないます。

6

以下のように項目を設定して、[新規追加]をクリックします。SSID: JinjiVLAN ID: 102無線の認証: WPA2-PSK追加認証: 追加認証を行わない無線の暗号化: AESWPA-PSK(事前共有キー): ijklmnop(任意の値)、Key更新間隔:60(分)ANY接続: 許可する(チェックあり)プライバシーセパレーター: SSIDセパレーター

? ヘルプ

8 営業部の設定をおこないます。 以下のように項目を設定して、[新規追加]をクリックします。 SSID : Eigyo VIAN ID : 103

VLAN ID	·	103
無線の認証	:	WPA2-PSK
追加認証	:	追加認証を行わない
無線の暗号化	:	AES
WPA-PSK(事前共有キー)	:	qrstuvwx(任意の値)、Key更新間隔:60(分)
ANY接続	:	許可する(チェックあり)
プライバシーセパレーター	:	SSIDセパレーター

マルチSSID設定 - マルチSSIDの編集(11a) 🛛 🛛 🥐 ヘルプ

編集を終了して前の画面へ戻る

マルチSSID登録情報の	新規追加 ? ヘルプ
SSID	Eigyo
VLAN ID	103
無線の認証	 ● 記録正を行行うない1 ● 記録正を行行うない1 ● IEEEB02、1x/EAP ● WPA-PSK ● WPA/WPA2 mixedmode - PSK ● WPA/WPA2 mixedmode - PSK ● WPA/EAP ● WPA2-EAP ● WPA2-EAP ● WPA2-EAP ● WPA2-EAP ● WPA2-EAP ● WPA2-EAP
這力吃認知	 ・ ・) 追加認証を行わない ・ MACアドレスリストによる制限 MACアドレスリストによる制限 MACアドレスリストにある MACアドレスフレド Z証証 1(フワード
無線の暗号化	 ● 暗号化なし ● FF(C)同注(前(e)) ● WEP(2) ● WEP(2) ● WEP(2) ● WEP(3) ● WEP(3) ● KLY ● KLY
[拡張設定]	1000 Section 100 PD
ANY接続	☑ 許元才ろ
ゴライバシーセパレーター	 Image: State St
	and C. D. N. L.

新規追加

9 [設定]をクリックします。

10 画面左側の[LAN設定]-[VLAN設定]をクリックします。

11 管理VLANと有線ポートのVLAN設定を以下のように変更して、[設定]をクリックします。

管理VLAN ID : 101 VLANモード : Tagged Port

VLANモード・ID設定 2 ヘルプ

インターフェース ¥LAN

インターフェース	VLANモード	VLAN ID
有線ボート(#1)	Tagged Port 💌	1
無線基本ボート(11a) SSID[XXXXXXXXXXXXA]	Untagged Port	1
無線マルチSSID(11a) SSID[Kanri]	Untagged Port	101
無線マルチSSID(11a) SSID[Jinji]	Untagged Port	102
無線マルチSSID(11a) SSID[Eigyo]	Untagged Port	103
無線基本ボート(11g) SSID[XXXXXXXXXXXX G]	Untagged Port	1

サブネット VLAN

サブネット名	サブネット種別	VLAN	ID
Management	管理サブネット	101	٦

設定

以上で本製品の設定は完了です。

本書のP24の図に合わせて、本製品とL2スイッチ、およびL2スイッチ同士を接続してください。 また、無線パソコンからそれぞれのSSIDを使って、ネットワークへ接続してください。接続手順 は、無線パソコンまたは無線子機のマニュアルを参照してください。

※ クライアントマネージャ3をお使いの場合は、プロファイルのインポート/エクスポート機能 を使うと、複数のパソコンへの設定が簡単におこなえます。プロファイルのインポート/エクス ポート機能については、クライアントマネージャ3のヘルプを参照してください。

CLI設定手順

ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ airset 11a ssid add ssidname Kanri vlanid 101
auth wpa2psk cipher aes rekey 60 key abcdefgh
(profile1)man[edit]$ airset 11a ssid privacy ssidname Kanri ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Kanri enable
(profile1)man[edit]$ airset 11a ssid add ssidname Jinji vlanid 102
auth wpa2psk cipher aes rekey 60 key ijklmnop
(profile1)man[edit]$ airset 11a ssid privacy ssidname Jinji ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Jinji enable
(profile1)man[edit]$ airset 11a ssid add ssidname Eigyo vlanid 103
auth wpa2psk cipher aes rekey 60 key qrstuvwx
(profile1) man[edit]$ airset 11a ssid privacy ssidname Eigyo ssid
(profile1)man[edit]$ airset 11a ssid anyscan ssidname Eigyo enable
(profile1)man[edit]$ ip lan vlan 101 force
(profile1)man[edit]$ ether port 1 vlan mode tagged
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```
例5:来客用フリースポットの設置(TagVLAN)

本製品は1台で複数の無線ネットワークを設定することができます。この機能を利用すると、あた かも複数台のエアステーションが設置されているかのようなネットワークを構築することができ ます。

ここでは例として、本製品を社内の無線アクセスポイント兼来客用フリースポットアクセスポイントとして使用する方法を説明します。

構成例

来客者用ネットワーク



条件

- ・ハードウェアIPフィルターに対応したL3スイッチ(例:BS-G3024MR(別売))が導入されている。
- ・TagVLANを利用して、本製品とL3スイッチを接続する。
- ・来客用フリースポットとして使用できるように本製品を設定する。
- ・来客用フリースポットからは、社内ネットワークにアクセスできないようにする。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・クライアントパソコン

・有線側ネットワーク機器(例:ハードウェアIPフィルターに対応したL3スイッチ、ルーターなど)

設定手順(L3スイッチのVLAN設定)

Webブラウザーを使って、ネットワークからL3スイッチへログインし、TagVLANの設定をおこないます。(ここでは例として、BS-G3024MR(別売)を使用します)



- 1 L3スイッチのマニュアルを参照して、L3スイッチの設定画面を表示します。
- 2 [基本設定]-[VLAN・IP設定]-[VLAN・IPステータス]をクリックします。

3 来客用(FreeSpot)のVLAN(10)を作成します。 以下のように項目を設定して、[追加]をクリックします。

VLAN ID	:	10
VLAN名	:	FreeSpot
Pアドレス	:	192.168.10.254
サブネットマスク	:	255.255.255.0/24
ポート	:	1~4を「Static Untagged」、5を「Static Tagged」、
		6~26& Not Member

VLANステータス

 VLAN ID
 1
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25
 26
 VLAN 名

 1
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U
 U

T:Static Tagge	UStatic Untagg						ł	-	:No1	t Me	embe	er														
新規VLAN 作成																										
VLAN ID:	10	(1-	409	4)																						
VLAN 名:	FreeS	pot																								
IPアドレス:	192.16	68.10	254																							
サブネットマスク:	255.2	55.25	5.0/2	24	~																					
ボート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	0	\bigcirc	\bigcirc	\bigcirc	۲	\bigcirc																				
Static Untagged	۲	\odot \odot \odot \odot \bigcirc \bigcirc						\bigcirc																		
Not Member	0	0	\bigcirc	\bigcirc	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲
設定 再読込	クリア																									

4 管理部のVLAN(25)を作成します。 以下のように項目を設定して、[追加]をクリックします。

VLAN ID	-	25
VLAN名	:	Kanri
IPアドレス	:	192.168.11.254
サブネットマスク	:	255.255.255.0/24
ポート	:	5を「Static Tagged」、6~12および25~26を「Static Untagged」、1~4お
		よび13~24を「Not Member」

VLANステータス

VLAN 名	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	VLAN ID	
	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	1	
FreeSpot	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Т	U	U	U	U	10	
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	PVID	

TO 1 T		
EStatic Lagged	U:Static Untagged	-:Not Member

新規VLAN 作成

VLAN ID:	25	(1-	4094	4)																						
VLAN 名:	Kanri																									
IPアドレス:	192.16	192.168.11.254																								
サブネットマスク:	255.2	55.25	5.0/2	24	*																					
ボート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
ボート Static Tagged	1	2 ()	3	4 ○	5 ⊙	6 ○	7 0	8	9 ()	10 ○	11 〇	12 ○	13 ()	14 〇	15 0	16 ○	17 ○	18 ()	19 ○	20 ○	21 〇	22 ○	23 ○	24 〇	25 〇	26 〇
ボート Static Tagged Static Untagged	1 0 0	2 〇	3 0	4 0 0	5 ⊙	6 ○	7 ○	8 ○	9 〇	10 ○	11 ○	12 ○	13 〇	14 〇	15 〇	16 〇	17 ○	18 〇	19 〇	20 〇	21 〇	22 ○	23 〇	24 〇	25 〇	26 〇
ボート Static Tagged Static Untagged Not Member	1 ○ ○	2 ○ ○	3 ○ ○	4 ○ ○	5 ③ 〇	6 ○ ⊙	7 0 0	8 ○ ⊙	9 () () ()	10 ○ ⊙	11 ○ ⊙	12 ○ ⊙	13 ○ ○	14 ○ ○	15 ○ ○	16 ○ ○	17 ○ ○	18 ○ ○	19 ○ ○	20 ○ ○	21 ○ ○	22 ○ ○	23 ○ ○	24 ○ ○	25 ○ ⊙	26 ○ ○

設定 再読込 クリア

社内ネットワークのVLAN(50)を作成します。 以下のように項目を設定して、[追加]をクリックします。

VLAN ID	:	50
VLAN名	:	Shanai
IPアドレス	:	192.168.50.254
サブネットマスク	:	255.255.255.0/24
ポート	:	5を「Static Tagged」、13~24を「Static Untagged」、
		1~4および6~12を「Not Member」

VLANステータス

5

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
10	U	U	U	U	Т	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	FreeSpot
25	-	-	-	-	Т	U	U	U	U	U	U	U	-	-	-	-	-	-	-	-	-	-	-	-	U	U	Kanri
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged U:Static Untagged -:Not Member

新規VLAN 作成

VLAN ID:	50 (1-4094)
VLAN 名:	Shanai
IPアドレス:	192.168.50.254
サブネットマスク:	255.255.255.0/24 💌

 Ti-h
 1
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25
 26

 Static Tagged
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0

設定 再読込 クリア

6 [基本設定]-[VLAN・IP設定]-[VLANポート設定]をクリックします。

7 各ポートにPVIDを設定します。

以下のように項目を設定して、[設定]をクリックします。

ポート1~4	: 10
ポート5~12および25~26	: 25
ポート13~24	: 50

VLANボート設定

ボート	1	3	5	7	9	11	13	15	17	19	21	23	25
PVID	10	10	25	25	25	25	50	50	50	50	50	50	25
ボート	2	4	6	8	10	12	14	16	18	20	22	24	26
PVID	10	10	25	25	25	25	50	50	50	50	50	50	25

設定 再読込

- 8 [基本設定]-[VLAN·IP設定]-[VLAN·IPステータス]をクリックします。
- 9 VLANステータスに表示されているVLAN 1の欄にある[編集]をクリックします。

10 VLAN 1に所属するポートをすべて「Not Member」に設定します。 以下のように項目を設定して、[設定]をクリックします。

VLAN ID	:	1
VLAN名	:	空欄
IPアドレス	:	192.168.1.254
サブネットマスク	:	255.255.255.0/24
ポート	:	1~26を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
10	U	U	U	U	Т	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	FreeSpot
25	-	-	-	-	Т	U	U	U	U	U	U	U	-	-	-	-	-	-	-	-	-	-	-	-	U	U	Kanri
50	-	-	-	-	Т	-	-	-	-	-	-	-	U	U	U	U	U	U	U	U	U	U	U	U	-	-	Shanai
PVID	10	10	10	10	25	25	25	25	25	25	25	25	50	50	50	50	50	50	50	50	50	50	50	50	25	25	

T:Static Tagged U:Static Untagged -:Not Member

新規VLAN 作成

VLAN ID:	1 (1-4094)		
VLAN 名:			
IPアドレス:	192.168.1.254		
サブネットマスク:	255.255.255.0/24	~	

ボート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	\bigcirc																									
Static Untagged	\bigcirc	$^{\circ}$	\bigcirc																							
Not Member	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲

設定 再読込 クリア

以上でL3スイッチのVLAN設定は完了です。 続いて、L3スイッチのハードウェアIPフィルター設定をおこないます。

設定手順(L3スイッチのハードウェアIPフィルター設定)

RS-232C(コンソール)接続でL3スイッチへログインし、ハードウェアIPフィルターの設定をおこないます。(ここでは例として、BS-G3024MR(別売)を使用します)

1 L3スイッチと設定用パソコンを、RS-232Cケーブルで接続します。

2 ターミナルソフトを次のとおりに設定し、L3スイッチにアクセスします。

- ・接続方法:COM1など
- ・データレート:9600bps
- ・データビット:8
- ・ストップビット:1
- ・パリティ:なし
- ・フロー制御:なし
- ・エミュレーション設定:VT100(または自動検出)
- ・キーの使いかた(ハイパーターミナル使用時):ターミナルキー
- 3 ターミナルが適切にセットアップできたら、ログインメニューが表示されます。 文字が表示されない場合は<Enter>を押してください。

BUFFALO - ハイパーターミナル ファイル() 編集() 表示() 通信() 転送() へルブ()	
W W W EEEEE L C C 0000 W W W EEEEE L C C 0 W W W EEEEE L C C 0 W W W EEEEE L C C 0 W W W EEEEE L C C 0	N M EEEEEE O MM MM E O MM H EEEEE O M M H E M M EEEEE O M M E
login:	

- **4** Login:にadminと入力し、<Enter>を押します。
- 5 Password:に、L3スイッチに設定されているパスワードを入力し、<Enter>を押します。 (BS-G3024MRの場合、初期設定ではパスワードは設定されていません)

以下のメニュー画面が表示されたら、<n>を押します。 <n>を押すと、CLIモードに切り替わります。

6

8

●BUFFALO - ハイパーターミナル □[フイバビ 編集日 表示() 油酸() 転送() ヘルプ() 日 ☞ ◎ 含 モ 珍 盛	
BUFFALO BS-G3024MR Main Menu	
a. System b. Port c. Rddress Table d. Spanning Tree e. VLAN f. Quality Of Service g. Security h. Trunk i. SNMP j. IGMP k. Difeasy k. Difeasy b. Consent Line o. Exit	
Hit <enter> to switch to a command line <tab> Move the Cursor <ctrl-l> Refresh <ctrl-w> Save</ctrl-w></ctrl-l></tab></enter>	

7 Global Configurationコマンドモードに入ります。

```
BS-G3024MR# configure
Configuring from terminal....
BS-G3024MR(config)#
```

「buffalo1」というアクセスリストを登録します。

```
BS-G3024MR(config)# access-list buffalo1
BS-G3024MR(config-access)#
```

9 アクセスリスト(buffalo1)に、来客用ネットワーク(192.168.10.0/24)から社 内ネットワーク(192.168.50.0/24)へのアクセスを禁止する内容を登録しま す。

```
BS-G3024MR(config-access)# deny 192.168.10.0/24 192.168.50.0/24
BS-G3024MR(config-access)#
```

10 アクセスリスト(buffalo1)に、社内ネットワーク(192.168.50.0/24)から来客 用ネットワーク(192.168.10.0/24)へのアクセスを禁止する内容を登録しま す。

```
BS-G3024MR(config-access)# deny 192.168.50.0/24 192.168.10.0/24
BS-G3024MR(config-access)#
```

11 Global Configurationコマンドモードに戻ります。

```
BS-G3024MR(config-access) # exit
BS-G3024MR(config) #
```

12 Interface Configurationコマンドモードに入り、ポート5の設定を開始します。

```
BS-G3024MR(config)# interface ethernet 5
BS-G3024MR(config-if)#
```

13 手順8~10で作成したアクセスリスト(buffalo1)の内容を、ポート5に適用します。

BS-G3024MR(config-if)# ip access-list buffalo1 inbound BS-G3024MR(config-if)#

14 Global Configurationコマンドモードに戻ります。

```
BS-G3024MR(config-if) # exit
BS-G3024MR(config) #
```

15 ここまでの設定内容を保存します。

BS-G3024MR(config) # system save

Saving Configuration ...

Configuration saved to NVRAM BS-G3024MR(config)#

16 exitコマンドを入力し、ログアウトします。

```
BS-G3024MR(config)# exit
BS-G3024MR# exit
```

以上でL3スイッチのハードウェアIPフィルター設定は完了です。 続いて、本製品の設定をおこないます。

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、TagVLANおよびマルチSSIDの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

BUJ-FFALO WARM-APG300N			ent Wireless LAN Access Poin Station $P_{\!rc}$
ТОР	詳細設定	システム情報	↓ <u>□グアウト</u>
機能設定		■プロファイラ情報	
無線		0	
無線LANの暗号化を設定する(WEP/TKIP/AES) 第線LANの暗号化を設定する(WEP/TKIP/AES)		profile1	
 ※ 無線LANの暗ちにで設定する(RADIUSリーバーで100) 新設は約の結本設定をする 			
1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		■サブネット 情報	
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		サブネット 1:[Mana	gement](VLAN 1)
その他		接続状態 (DHCPク	ライアント:取得中)
エアステーションのファームウェアを更新する		解放	書き換え
エアステーションの設定を初期化する			
		/+ /+ /-	
		■ 黒緑情報	
		IEEE 802.11a (A 36+40ch)	uto(W52) /
		SSID XXXX	XXXXXXXX A
		認証方式 ₽PA -	PSK
		暗号化 AES	
		マル手SSID 無効	
		11 ch)	uto(1~11cn)7
		SSID XXXX	XXXXXXXX_G
		認証方式 ♥PA-	PSK
		暗号化 AES	
		マルチSSID 無効	
	1	Japanese 🗸 🛛 Chi	ange Language
		(())) A055	40SS 設定画面へ
			WPS 設定画面へ
(C)2000-2009 BUF	FALO INC. All rights r	reserved.	

3 画面左側の[無線設定]-[(802.11gの)マルチSSID]をクリックし、[マルチSSID登録情報の編集]をクリックします。

マルチSSID設定 (11g) ? ヘルプ SSID VLAN ID 認証 暗号化 状態 マルチSSIDの設定は登録されていません

マルチSSID登録情報の編集

4 来客用ネットワークの設定をおこないます。 以下のように項目を設定して、[新規追加]をクリックします。

SSID	:	FreeSpot
VLANID	:	10
無線の認証	:	WPA2-PSK
追加認証	:	追加認証を行わない
無線の暗号化	:	AES
WPA-PSK(事前共有キー)	:	freespot(任意の値)、Key更新間隔:60(分)
ANY接続	:	許可する(チェックあり)
プライバシーセパレーター	:	STAセパレーター

編集を終了して前の画面へ戻る

マルチSSID登録情報の	新規追加 ? ヘルプ
SSID	FreeSpot
VLAN ID	10
無線の認証	● 記録正差(行わない) ● IEEEB02.1×/EAP ● WPA-PSK ● WPA/PSX ● WPA/WPA2 mixedmode - PSK ● WPA/EAP ● WPA2-EAP ● WPA2-EAP ● WPA/WPA2.mixedmode - EAP
迫力感認証	 適加認証を行わない MACアドレスリストドによる制限 MACアドレスリストドMAC-RADIUS認証 MACのアドレスを使う 次のパスワードを使う 次のパスワードを使う (MIcrosoft NAPを使用する) 制阪ネットワークに使用するYLAN: 4093
無線の暗号化	 ・ 暗号化なし ・ WEP(信)定(意味ey) WEP暗号化キー ・ 文字入力・13文字(WEP128) ・ ・ WEP(自動記(意key) 自動更新Kes長 WEP128 ・ WEP(信)定(個Key) の併用 併用しない ・ ・ ・
[拡張設定]	
ANY接続	✓ 許可する
プライバシーセバレーター	STAZ/IL-9-

新規追加

5 [設定]をクリックします。

6 画面左側の[無線設定]-[(802.11aの)マルチSSID]をクリックし、[マルチ SSID登録情報の編集]をクリックします。

マルチSSID設定(11a) <u>?</u> ヘルプ

SSID VLAN ID 認証 暗号化 状態 マルチSSIDの設定は登録されていません

マルチSSID登録情報の編集

7

社内ネットワークの設定をおこないます。 以下のように項目を設定して、[新規追加]をクリックします。

:	shanai
:	50
:	WPA2-PSK
:	追加認証を行わない
:	AES
:	buffalo-shanai(任意の値)、Key更新間隔:60(分)
:	許可する(チェックあり)
:	SSIDセパレーター

マルチSSID設定 - マルチSSIDの編集(11a) 🛛 🛛 🖓 ヘルプ

編集を終了して前の画面へ戻る

マルチSSID登録情報の	新規追加 ? ヘルプ
SSID	shanai
VLAN ID	50
無線の認証	● 記録正差行行かない ● IEEEB02.1×/EAP ● WPA-PSK ● WPA/WPA2 mixedmode - PSK ● WPA/WPA2 mixedmode - PSK ● WPA/WPA2 mixedmode - EAP ● WPA/WPA2 mixedmode - EAP
j皇力og之意正	 ・ 適加認証を行わない ・ 体のアドレスリストによる制限 ・ 体のアドレスリストはMC-RADIUS認証 ・ MACアドレスタレリスト4MAC-RADIUS認証 ・ MACアドレスを使う ・ かのパスワードを使う ・ 次のパスワードを使う ・ パムがく使用する ・ 制限ネットワークに使用するパムNI: ⁴⁰⁸³
兼線の暗号化	 ff若子(たなし WEP(高定(原key)) WEP(高定(原key)) eb動更新kes長 WEP128) wEP(自動記(高key)) 自動更新kes長 WEP128 ▼ WEP128 ▼
[拡張設定]	NOT WE NOT THE PARTY OF THE PAR
ANV 连结	
ゴライバシーセバレーター	(ビ) #+** 9 つつののでのです。
JUNU CAUTUR	

新規追加

8 [設定]をクリックします。

9 [LAN設定]-[VLAN設定]をクリックします。

10 VLANの設定をおこないます。 以下のように項目を設定して、[設定]をクリックします。

有線ポート	: Tagged Port
無線基本ポート(11a)	: VLAN ID 25
無線マルチSSID(11a)	: VLAN ID 50
無線基本ポート(11g)	: VLAN ID 25
無線マルチSSID(11g)	: VLAN ID 10
管理VLAN ID	: 25

VLANモード・ID設定 **? ヘルプ**

インターフェース ¥LAN

インターフェース	VLANモード	VLAN	IC
有線ボート(#1)	Tagged Port 💌	1	
無線基本ボート(11a) SSID[XXXXXXXXXXXXA]	Untagged Port	25	
無線マルチSSID(11a) SSID[shanai]	Untagged Port	50	
無線基本ボート(11g) SSID[XXXXXXXXXXXXX]G]	Untagged Port	25	
無線マルチSSID(11g) SSID[FreeSpot]	Untagged Port	10	

サブネット VLAN

サブネット名	「サブネット種別	VLAN	ID
Management	管理サブネット	25	

設定

以上で本製品の設定は完了です。

本書のP36の図に合わせて、本製品とL3スイッチを接続してください。 また、無線パソコンからそれぞれのSSIDを使って、ネットワークへ接続してください。接続手順 は、無線パソコンまたは無線子機のマニュアルを参照してください。

※ クライアントマネージャ3をお使いの場合は、プロファイルのインポート/エクスポート機能 を使うと、複数のパソコンへの設定が簡単におこなえます。プロファイルのインポート/エクス ポート機能については、クライアントマネージャ3のヘルプを参照してください。

CLI設定手順

ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

(profile1)man\$ edit start profnum 1 (profile1)man[edit]\$ (profile1)man[edit]\$ airset 11g ssid add ssidname FreeSpot vlanid 10 auth wpa2psk cipher aes rekey 60 key freespot (profile1)man[edit]\$ airset 11g ssid privacy ssidname FreeSpot station (profile1)man[edit]\$ airset 11g ssid anyscan ssidname FreeSpot enable (profile1)man[edit]\$ airset 11a ssid add ssidname Syanai vlanid 50 auth wpa2psk cipher aes rekey 60 key buffalo-syanai (profile1)man[edit]\$ airset 11a ssid privacy ssidname Syanai ssid (profile1)man[edit]\$ airset 11a ssid anyscan ssidname Syanai enable (profile1)man[edit]\$ ip lan vlan 25 force (profile1)man[edit]\$ ether port 1 vlan mode tagged (profile1)man[edit]\$ edit end Setting changed. Do you execute? (y/n)y

例6:来客用フリースポットの設置(簡易ルーター機能)

本製品は簡易ルーター機能を搭載しています。この機能を利用することでルーターを別途用意す ることなく、本製品1台で社内用無線アクセスポイントと来客用フリースポットを設定できます。 ここでは例として、本製品を社内の無線アクセスポイント兼来客用フリースポットアクセスポイ ントとして使用する方法を説明します。

構成例

来客者用フリースポット

(SSID : FreeSpot)



条件

- ・来客用フリースポットとして使用できるように本製品を設定する。
- ・来客用フリースポットからは、社内ネットワークにアクセスできないようにする。
- ・小規模での運用を想定。
- ・インターネット接続方法としてPPPoEを使用する。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

- ・AOSSに対応した設定用パソコン
 - ※ 設定用パソコンには、あらかじめクライアントマネージャV(Windows 7/Vistaの場合)また はクライアントマネージャ3(Windows XP/2000/Me/98SEの場合)がインストールされ ている必要があります。

設定手順(設定用パソコンの設定)

設定用パソコンのIPアドレスを固定し、設定用パソコンと本製品をAOSS接続します。

 設定用パソコンのIPアドレスを固定にします。 以下のように設定して、[OK]をクリックします。 (以下は、Windows XPの場合の画面です)

「次のIPアドレスを使う」 IPアドレス : 192.168.11.2 サブネットマスク : 255.255.255.0 デフォルトゲートウェイ : 空欄 「次のDNSサーバーのアドレスを使う」 優先DNSサーバー : 空欄 代替DNSサーバー : 空欄

インターネット プロトコル (TCP/IP)のプロ	ਮਿੰਡ 🛛 🤶 🔀
全般	
ネットワークでこの機能がサポートされている場 きます。サポートされていない場合は、ネットワ てください。	合は、IP 設定を自動的に取得することがで 一ク管理者に適切な IP 設定を問い合わせ
○ IP アドレスを自動的に取得する(<u>0</u>)	
○ 次の IP アドレスを使う(S):	
IP アドレス(I):	192 . 168 . 11 . 2
サブネット マスク(山):	255 . 255 . 255 . 0
デフォルト ゲートウェイ(<u>D</u>):	· · ·
○ DNS サーバーのアドレスを自動的に取得	导する(<u>B</u>)
○次の DNS サーバーのアドレスを使う(E)	
優先 DNS サーバー(<u>P</u>):	<u> </u>
代替 DNS サーバー(<u>A</u>):	· · ·
	[詳細設定(⊻)
	OK キャンセル

2 「例1:AOSS/WPSを使って本製品と無線接続する」(P4)を参照して、本製品と設定用パソコンをAOSSで接続します。

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、TagVLANおよびマルチSSIDの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

ТОР	詳細設定	システム	情報	₽ <u>µ/77</u>
機能設定		■プロファイラ	前報	
焦 線				
無線LAND暗号化を設定する(WEP/TKIP/AES)		pr pr	ofile1	
無線LANの暗号化を設定する(RADIUSサーバーを使う) 無線LANの増生やウオオス				
※ 無限LANU型本設定です○ 【 く、わ、 カ、 ↓		■サブネット	情報	
インターネット接続を設定する		サブネット 1	[Manage me	nt](VLAN 1)
子の他		接続状態 (:取得 DHCP クライア	ント:取得中)
 エアステーションのファームウェアを更新する 		1	解放 書き換け	۰
エアステーションの設定を初期化する				
		na dar óft dir dr		
		二二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二	4 - 1 - 4 - 4 - 124	F0) (
		36+40ch)	Ta (Auto(M	52)7
		SSID	*****	XXX_A
		認証方式	₩PA-PSK	
		暗号化	AES	
		マルチSSID	無効	
		IEEE 802.1	1 g (Auto(1	~11 ch) /
		SSID	******	YYY G
		認証方式	WPA-PSK	
		暗号化	AES	
		マルチSSID	無効	
			Change La	nauare
		- apra novo	E au	
			ANSEL AOSS E	定面面へ
			_	

3 画面左側の[LAN設定] – [サブネット設定]をクリックします。 [サブネットの編集]をクリックします。

サブネッ	ト設定	Ê					?	ヘルプ
サブネット名	VIAN T	レサブネット	、種別	ק קו	ドレフ軍	网络方法	オゴン	·=`/
Management	1	クレイン・ショ 管理サブネッ	가 보기가 기 분	n シ DHCPクラ	ライアン	л а лла Р	- デフォ.	ョン ルト経路)
サブネットの:	編集							

4 「サブネットの表示/操作」に登録されている「Management」欄の[編集]をクリックします。



設定

5 管理用サブネット (Management)を以下のように設定して、[修正保存]をクリックします。

:	Shanai
:	管理サブネット
:	1
:	手動設定 192.168.11.100
:	192.168.11.100(255.255.255.0)
:	ルーティング
:	空欄
:	空欄
:	受信「RIPv1」と「RIPv2」にのみチェックマークを付ける
:	使用しない
:	1500
:	サブネットにDHCPサーバー機能を提供する
:	192.168.11.10から30台

サブネット情報の編集 🎴 ヘルプ

サブネット名	Shanai					
サブネット種別	● 管理サブネット					
VLAN ID	1					
IP アドレスの取得方法	 ● 手動設定 ○ DHCP クライアント 					
	IP アドレス 192.168.11.100					
IF JFVA	サブネットマスク 255.255.255.0 💌					
ルーティング	ルーティング 💌					
デフォルトゲートウェイ	手動設定					
PNG	プライマリーサーバー:					
DNO	セカンダリーサーバー:					
希腊的白丝来早冬	送信: 🗌 RIPv1 🔲 RIPv2					
面的中心地变成品	受信: VRIPv1 VRIPv2					
UPnP IGD	使用しない 🔽					
MTU	1500					
	○使用しない					
	●サブネットICDHCPサーバー機能を提供する					
	○サブネットICDHCPサーバー機能をRelayする					
DHUP 9-7-	割り当て IP 192.168.11.10 から アドレス 30 合					
	除外アドレス					

修正保存

7 同様に、サブネットの編集画面で、来客用フリースポットのサブネットを追加します。

サブネット名	:	FreeSpot
サブネット種別	:	LANサブネット
VLAN ID	:	2
IPアドレスの取得方法	:	手動設定
IPアドレス	:	192.168.12.1 (255.255.255.0)
ルーティング	:	ルーティング
デフォルトゲートウェイ	:	空欄
DNS	:	空欄
動的経路	:	受信「RIPv1」と「RIPv2」にのみチェックマークを付ける
UPnP	:	使用しない
MTU	:	1500
DHCPサーバー	:	サブネットにDHCPサーバー機能を提供する
割り当てIPアドレス	:	192.168.12.10から30台

サブネット情報の編集 🔽 ヘルプ

サブネット名	FreeSpot
サブネット種別	⊙LAN サブネット ○Internet サブネット
VLAN ID	2
IP アドレスの取得方法	● 手動設定○ DHCP クライアント
IP アドレス	IP アドレス 192.168.12.1 サブネットマスク 255.255.0 ♥
ルーティング	ルーティング 💌
デフォルトゲートウェイ	手動設定
DNS	プライマリーサーバー: セカンダリーサーバー:
動的経路	送信: □RIPv1 □RIPv2 受信: ☑RIPv1 ☑RIPv2
UPnP IGD	使用しない 💙
MTU	1500
DHCP サーバー	 ●使用しない ●サブネットにDHCPサーバー機能を提供する ●サブネットにDHCPサーバー機能をRelayする 割り当て IP アドレス 192.168.12.10 から 30 台 除外アドレス

新規追加

8 画面左側の[無線設定]-[(802.11aの)マルチSSID]をクリックします。 [マルチSSID登録情報の編集]をクリックします。

マルチSSID設定 (11a) 🔽 ヘルプ

SSID VLAN ID 認証 暗号化 状態 マルチSSIDの設定は登録されていません

マルチSSID登録情報の編集



社内ネットワークのSSID設定を以下のように設定して、[新規追加]をクリック します。

SSID	:	Shanai
VLANID	:	1
無線の認証	:	WPA/WPA2 mixedmode-PSK
追加認証	:	追加認証を行わない
無線の暗号化	:	TKIP/AES mixed
WPA-PSK(事前共有キー)	:	abcdefgh(8~63文字の任意の値)
Key更新間隔	:	60分
ANY接続	:	許可する
プライバシーヤパレーター	:	SSIDセパレーター

マルチSSID登録情報の新規追加 🔽 ヘルプ

SSID	Shanai
VLAN ID	1
無線の認証	EVELE & F(+2) ∧ E(+) UPA-FAX VPA-FAX VPA-FAX
<u>这</u> 力呢???证	 通加認証を行わない MuCアドレスリストHuC-RADIUS認証 MuC-RADIUS認証 E認証がスワード MuCアドレスを使う 、次のパスワードを使う MuCアドレスを使う 次のパスワードを使う MuCア・レクを使用する MUCF・カッドワークに使用するVLAN: 4003
無線の暗号化	 ● 昭分化なし ● 昭分(名)定都(ev) ● 昭介電景化キー (文子入力・13文字(WEP128)) ● 御房町秋の長 (WEP128) ● 御房町秋の
[拡張設定]	
ANY接続	✓ 許可する
ブライバシーセバレーター	SSDセパレーター 💌

新規追加

10 [設定]をクリックします。

11 画面左側の[無線設定]-[(802.11gの)マルチSSID]をクリックします。 [マルチSSID登録情報の編集]をクリックします。

マルチSSID設定 (11g) 🔽 ヘルプ

SSID VLAN ID 認証 暗号化 状態 マルチSSIDの設定は登録されていません

マルチSSID登録情報の編集

12 来客用フリースポットのSSID設定を以下のように設定して、[新規追加]をクリックします。

SSID	:	FreeSpot
VLANID	:	2
無線の認証	:	WPA/WPA2mixedmode-PSK
追加認証	:	追加認証を行わない
無線の暗号化	:	TKIP/AESmixed
WPA-PSK(事前共有キー)	:	ijklmnop(8~63文字の任意の値)
Key更新間隔	:	60分
ANY接続	:	許可する
プライバシーセパレーター	:	STAセパレーター

マルチSSID登録情報の新規追加 🔽 ヘルプ

SSID	Shanai
VLAN ID	1
無線の認証	D2証を行わたい TEEEの21,1x/EP VPA-P3 VPA-P3 VPA-P3 VPA-P3 VPA-P4 VPA-EN VPA-EN VPA-EN VPA-EN VPA-EN VPA-EN
追为噶瑟証	 ③ 訪加認識を行わない ● MAC7 ドレスリストによる制限 ● MAC7 ドレスリストによる制限 ● MAC7-BADIUS認識 認識がスワード ● MAC7-BADIUS認識 (ADC7 ドレスを使う) ○ 法のがスワードを使う ○ 法のがスワードを使う ● MICresoft NUPS 使用する ■ MIRキットワーグに使用する*/LANE 4003
無線の暗号化	 日野代なし (PF(留定部key) WEP留号化キー 文字入力・13文字(WEP128) PEP(自動能(Eskey) 自動更新keg長 WEP128 VEP(自動能(Eskey) esp(128) WEP(国動能(Eskey) esp(128) WEP(国動能(Eskey) esp(128) WEP(国動能(Eskey) esp(128) WEP(国動能(Eskey) esp(128) WEP(国動能(Eskey) esp(128) WEP128) WEP(ISKE) Esp(128) WEP(ISKE) VEP(自動能(Eskey) WEP(ISKE) Fill WEP(ISKE) IST(P Esk(ISKE) IST(P Second Second Second Second Second Second Second Second Second Second Second Second Second Second
[拡張設定]	1997 August 1997 1977
ANV接続	V **=====
ゴニズバシーセパレーター	
	33DC/10 3 •
新規追加	

- 13 [設定]をクリックします。
- 14 画面左側の[TOP]をクリックします。

15 TOP画面の「インターネット接続を設定する」をクリックします。

ТОР	詳細設定
機能設定	
▲ 無	
≫ 無線LANの暗号化を設定する(WEP/TKIP/AES)	
≫ 無線LANの暗号化を設定する(RADIUSサーバーを使う)	
≫ 無線LANの基本設定をする	
▲ インターネット	
インターネット接続を設定する	
その他	
※ エアステーションのファームウェアを更新する	
エアステーションの設定を初期化する	

16 VLANモードを設定します。 以下のように項目を設定して、[進む]をクリックします。

VLANモード : UntaggedPort

> イン	ターネットボー	ト接続に使用する	ボートを指定しま	す 。					
		インターネット射 ードバンド回線力 ンターネット回線 フェースがTagge のVLAN IDを使用	競売を行うためにI N必要です。本ウ- 象として使用します dPortに設定されて しないよう注意し	t、モデムなどにき イザードではVLAN す。本製品のいずが ている場合は、他の てください。	接続 ID れか の 接	された F4094 のイン 続機者	: ブロ 」をイ !ター 話がこ		
		ボート名		YLAN モード	1	/LAN 1	D 選択		
		有線ボート(#1)	[Untassed Port]	Untagged Port	•	1	۲		
				r					

17 「PPPoEクライアント機能を使用する」をクリックします。



戻る

18 インターネット回線の接続先情報を設定します。 以下のように項目を設定して、「進む]をクリックします。

接続ユーザー名 : ご契約のプロバイダー指定のユーザー名 接続パスワード : ご契約のプロバイダー指定のパスワード

/メニネット回線の技:	就設走(FFF0E)	
🌣 インターネット接続のため	lに必要な情報を入力します。	
接続ユーザー名	xxx, xxx, xxx, xxx, xxx	
	•••••	
1800/1/2/2/1	•••••	(確認用)

19 設定内容を確認し、[接続開始]をクリックします。

定確認		
>> 以下の設定情報	#で、インターネット回線	泉の接続を試みます。
以下の設定で1 23 始」をクリックし1	マーネットへの接続を詰めてください。接続確認を開いた。	Jます。ようしければ、ホードにフロードハフト回線機器を接続し、「接続す 開始します。
※ 有線ボート(計) 信が切断される可能	のVLAN IDを4094 に変更 皆性があります。	Eします。現在このインターフェースを経由して設定を行っている場合は、ネ
※ 既存の「LAN サ IP アドレスの耳 ルーティング DHCP サーバー	ブネット」・「管理サブ 取得方法:「手動設定」 :「ルーティンク :「サブネットに	ネット」の設定の一部は以下のように変更されます。 フ」 DMCPサーバー機能を提供する」
	サブネット名	Internet-Subnet
	サブネット種別	Internet サブネット
	VLAN ID	4094
	IP アドレスの取得	方法 PPPoE クライアント
		接続先ユーザー名: xxxxxx®xxx.xxx.xxx
		接続先パスワード: #8##88##8
	PPPoE	サービス名 :
		キーブアライブ : on
	ルーティング	アドレス変換(NAPT)
	DNS	通知されたDNSを使用する
	動的経路	送信:使用しない 受信:RIPv1,RIPv2

戻る

接続開始

20 本製品が接続設定を確認しますので、画面が切り替わるまでしばらく待ちます。

10	ターネット 接続を設定	する		
接	続確認			
	>> 接続確認			
		DDD_F#, .5. OV	わ 共和法	
		確認中です	石則肝戌	
		PPPoEサーバー OK 確認中です	名前解決	

21 以下の画面が表示されたら接続設定は完了です。 [完了]をクリックしてください。

接続確認	
	PPPoEサーバー OK 名前解決 OK
	接续成功方式
	AirStationの設定は完了しました!
上の枠内に	:「接続成功です」と表示されないときは、 <u>こちら</u> で現象を確認してください。

22 手順1で変更した設定用パソコンのIPアドレス設定を元の設定に戻します。

以上で本製品の設定は完了です。

CLI設定手順

ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

(profile1)man\$ edit start profnum 1 (profile1) man[edit]\$ airset 11g ssid add ssidname FreeSpot vlanid 2 auth wpa2mixedpsk cipher mixed rekey 60 key abcdefgh (profile1)man[edit]\$ airset 11g ssid privacy ssidname FreeSpot station (profile1)man[edit]\$ airset 11g ssid anyscan ssidname FreeSpot enable (profile1)man[edit]\$ airset 11a ssid add ssidname Shanai vlanid 1 auth wpa2mixed cipher mixed rekey 60 key ijklmnop (profile1)man[edit]\$ airset 11a ssid privacy ssidname Shanai ssid (profile1)man[edit]\$ airset 11a ssid anyscan ssidname Shanai enable (profile1)man[edit]\$ ip subnet name Management address 192.168.11.100/24 (profile1)man[edit]\$ ip dhcp-server lease name Management mode server from 192.168.11.10 num 30 (profile1)man[edit]\$ ip subnet rename name Management Shanai (profile1)man[edit]\$ ip subnet add name FreeSpot type lan vlan 2 address 192.168.12.1/24 (profile1)man[edit]\$ ip dhcp-server lease name FreeSpot mode server from 192.168.12.10 num 30 (profile1)man[edit]\$ ip subnet add name Internet type inet vlan 4094 address pppoe user [PPPoE接続ユーザー名] pass [PPPoE接続パスワード] link alltime keepalive lcp (profile1)man[edit]\$ ip routing subnet name Internet forwarding enable napt outbound (profile1)man[edit]\$ ip defaultgw name Internet (profile1)man[edit]\$ ether port 1 vlan mode untagged vlan 4094 (profile1)man[edit]\$ edit end Setting changed. Do you execute? (y/n)y

例7:802.1X無線認証を利用する(MACアドレスによる制限の場合)

本製品はRADIUSサーバーを用いた無線パソコン認証に対応しており、強固なセキュリティーを 持つ無線ネットワークを構築することができます。RADIUSサーバーを利用した認証方式には次 のものがあり、パソコンの対応状況によって使い分けることができます。

: すべてのパソコンで利用可能
: IEEE802.1X/EAP準拠で、動的WEPキー配信をサポートしたパ
ソコンで利用可能
: WPA-EAP(Enterprise)に対応したパソコンで利用可能
: WPA2-EAP(IEEE802.11i)に対応したパソコンで利用可能

ここでは例として、RADIUSサーバーにMicrosoft Windows Server 2003搭載の認証サーバー (インターネット認証サービス)を使用する場合の手順を説明します。

暗号化の種別	セキュリティー強度	サプリカント	RADIUSサーバーの 対応
MAC-RADIUS	\bigtriangleup	不要	PAP対応
IEEE802.1X/EAP	0		
WPA-EAP WPA2-EAP WPA/WPA2 EAP	Ø	必要	EAP対応

構成例



無線パソコン

条件

- RADIUSサーバーには、インターネット認証サービス(IAS)が正常にインストールされ、認証 サービスが動作している。
 (インターネット認証サービスやRADIUSサーバーの設定などの詳細は、市販の書籍や各サー バーのマニュアルなどをご参照ください)
- ・接続をおこなうすべてのパソコンにサプリカントがインストールされ、必要な設定がおこなわれている。

(サプリカントのインストールや設定は、各ソフトウェアのマニュアルをご参照ください。 弊社製無線子機をお使いの場合、添付のクライアントマネージャ3のヘルプをご参照ください)

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

- ・RADIUSサーバー(Windows Server 2003)
- ・クライアントパソコン

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、認証の設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「無線LANの暗号化を設定する(RADIUSサーバーを使う)」をクリックします。



- 3 「11aと11gに共通の暗号化を設定する」をクリックします。
 - ※ 選択した規格の無線ポートのみ設定されます。選択されなかった無線規格については、 認証・暗号化設定をおこないません。

APM-APG300N	AirStatio	
機能設定		
線LANの暗号化を設定する(RAD	IUSサーバーを使う)	
音号化設定を行う無線規格	D 選択	
≫ 暗号化設定を行う無線規格を通	訳して下さい	
	11歳の増告号化を設定する	
暗号化設定を行う無線規格	<u>11sの暗号化を設定する</u>	
	<u>11aと11gに共通の暗号化を設定する</u>	
本エアステーションには複数の無 それぞれ別々の、または、共通の	線方式が存在します。 宿号化設定を行うことができます。	
戻る		
	(C)2000-2008 BUFFALO INC. All rights reserved.	

4

使用する暗号化方式をクリックします。

※ 接続する無線機器のすべてがサポート可能な暗号化方式を選択します。MAC-RADIUS 認証については、RADIUSサーバーが対応している必要があります。

eitzte	
LANの暗号化を	没定する(RADIUSサーバーを使う)
号化方式の選択	8
🌺 11aと11s共通の	暗号化方式を選択して下さい
暗号化方式	H4C-R40/US282 HEV/LEEUR/S.V/EAP) H2R/EAP(XE) H2R/EAP(XE) H2R/EAP(AES) H2R/EAP(AES) H2R/EAP(AES)
HED.	久/ 小海道) の経験で徳田できる暗黒ルモデッナ
TKIP:	9~00mmakaBellinできついならしたりできる。 WEPをさらに強固にした方式です。毎後DAU#照例もTKIPに対応している 必要があります。
AES:	TKIPより強固な次世代暗号化方式です。無線LAN機器側もAESに対応している必要があります。
MAC-RADIUS EZHE:	無線LAW機器のMACアドレスをユーザー名として、RADIUSサーバーに認証要求を行います。他の認証 方式をサポートしていない機器でも利用可能です。
IEEE802.1×/EAP:	無線uAW機器で用いられるMEPベースの認証方式です。RADIUSサーバーにはなADIUS/CAPプロトコルで 認証要求を行います。802.1×/CAP認証に対応したサブリカントが全ての無線LAN機器で必要となり まず。
WPA- EAP/WPA2- EAP:	TKIP/AESが利用可能な無線LAN機器の認証方式です。WPA,WPA2それぞれ対応したクライアントのみ 接続を行うことができます。
WPA/WPA2 nixednode-	WPA-EAPおよびWPA2-EAP,TKIP/AESをサポートした各クライアントが混在可能なモードです。但 し、ブロードキャスト資産の培気化についてはTKIPが用いられます。

2000-2009 DITEEALO INC. All viebto re-

・MAC-RADIUS認証を選択する場合は、次の画面が表示されますので任意のWEP暗号化 キーを入力してください。

(TCM)age1	
版化	
LANの暗号化を設定する((RADIUSサーバーを使う)
設定	
 11aと11g共通のNEP暗号(化キーを設定して下さい
	文字入力・13文字(WEP128) ▼
	⊙1: ••••••••
WEP暗号化牛一	02:
	03:
	04:
WEP暗号化キーは最大4つ登録 文字入力を選択剤は半角英語	禄すろことができ、そのうち1つを送信キーとして設定します。 数字または記号で入力し、
WEP暗号化キーは最大4つ登録 文字入力を選択時は半角英碁 16進数入力を選択時は16進	録することができ、そのうち1つを送信キーとして設定します。 好すまた1歳2号で入力し、 飲(0~4、A~Fまた1歳~f)で入力します。

5 RADIUSサーバー名とSharedSecretを入力して、[進む]をクリックします。 ※ ここで入力したSharedSecretは、RADIUSサーバー側にも同じ値を設定します。

M-APG300N	AirStation
設定	
LANの暗号化を設定する(RADI	USサーバーを使う)
IUS設定	
>> RADIUSサーバーの設定をして下	53L)
RADIUSサーバー	X00CX00CX00CX00C
SharedSecret	•••••
 無線LAH線器の認識などに用いられ RADIUSサーバーは通常エアステー エアステーションは私知(USサーバー) RADIUSサーバ RADIUSサーバー RADIUSサーバー SharedSecret: RADIUSサーバー 	2月840015サーバーの設定を行います。 ションの増更れぬしに設置し、 接続原本のあった無線LAM機器の設証を行います。 一から認証すが良い状態の無線LAM機器との通信を許可しません。 2付を行うサーバーを、IPアドレスもしくJ306%決可能なサーバー名で 設定するこ かかーバーをを入力することができます。 とすアステーションの思の声動をILT用いられる実体線(パスワード)です。 2回じあard Servetを持つエアステーションのみが、サーバーを使った認証を行う
半角の英数記号	2、1~255文平までの共有羅を設定することができます。



7 [設定完了]をクリックします。

以上で本製品の設定は完了です。 続いてRADIUSサーバーの設定をおこないます。

CLI設定手順

ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
MAC-RADIUS 認証の場合
(profile1)man[edit]$ airset 11a ssid security ssidnum 1 auth
none cipher wep fixed keytype asciil28 transmit 1 key abcdefghijklm
(profile1)man[edit]$ airset 11a ssid addsecurity ssidnum 1 mode
macradius authmac
IEEE802.1X/EAP 認証の場合
(profile1)man[edit]$ airset 11a ssid security ssidnum 1 auth
eap cipher wep rekey 60 key 128 addkey disable
WPA/WPA2-EAP 認証の場合
(profile1)man[edit]$ airset [11a ssid security ssidnum 1 auth
[wpaeap | wpa2eap | wpa2mixedeap] cipher aes rekey 60
(profile1)man[edit]$ radius primary enable server (RADIUS サーバー名)
secret (SharedSecret)
(profile1)man[edit]$ airset [11a | 11g] wireless enable
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

設定手順(RADIUSサーバー)

RADIUSサーバーヘログインし、本製品を登録します。

- 1 RADIUSサーバー(Microsoft Windows Server 2003)にログインします。
- 2 スタートメニューから[コントロールパネル]-[管理ツール]-[インターネット 認証サービス]をクリックします。
- 3 「RADIUSクライアント」を選択します。

🎾 インターネット認証サービス			_ 🗆 🗵
ファイル(E) 操作(<u>A</u>) 表示(V) ヘルプ(H)			
🍫 インターネット認証サービス (ローカル)	フレンドリ名	アドレス	プロトコル
 → 「RADUS 577/2/ト → リモ・アウセスのび ⇒ ジレモート アウセス ポリシー ⇒ ● 接続要求の処理 	•	このビューに表示する項目はありません。	Þ

- 4 ウィンドウ右側の空白部分を右クリックし、表示されたメニューから[新規作成] -[RADIUSクライアント]を選択します。
- 5 「名前とアドレス」設定で、「フレンドリ名」と「クライアントのアドレス」を設定し、[次へ]をクリックします。
 - ※ フレンドリ名には本製品を示す任意の名前を、クライアントのアドレスには、本製品の IPアドレス(またはホスト名)を入力してください。
- 6 「追加情報」設定で、「クライアントベンダ」・「共有シークレット」を入力します。
 - ※ クライアントベンダには「RADIUS Standard」を、共有シークレットには本製品に設定 した「Shared Secret」を入力してください。
- **7** [完了]をクリックします。
- **8** 「リモートアクセスポリシー」を選択します。

梦 インターネット認証サービス			J×
ファイル(E) 操作(A) 表示(V) ヘルプ(H)			
🔷 インターネット認証サービス (ローカル)	名前	順序	
ーー RADIUS クライアント	SIEEE8021 Wireless	1	
由 🧰 リモート アクセスのログ	🕼 Microsoft 🌾 ーティングとリモート アクセス サーバ	2	
一 🧐 リモート アクセス ポリシー	🕼 ほかのアクセス サーバーへの接続	3	
🖻 📄 接続要求の処理			

- 9 ウィンドウ右側から無線認証に使用するプロファイルを選択します。右クリックします。
- 10 選択した項目を右クリックし、[プロパティ]を選択します。
- 11 [プロファイルの編集]をクリックします。

IEEE802.11 Wirelessのプロパティ	? ×			
設定				
・ 接続要求が満たす必要のある条件を指定してください。				
ポリシー条件(<u>C</u>):				
INAS-Port-Type が次のものと一致: *ワイヤレス - その他 OR ワイヤレス -	IEEE 802.1			
	Þ			
追加(D) 編集(E) 削除(B)				
接続要求がこのポリシーで指定した条件を満たした場合、関連するプロファイ) 適用されます。	ルが接続に			
ブロファイルの編集(P)				
 ユーザー プロファイルで個々のアクセス許可が指定されない限り、このポリシーがネットワー クへのアクセスを制御します。				
接続要求が指定の条件を満たした場合:				
● リモート アクセス許可を拒否する(N)				
○ リモート アクセス許可を与える(④)				
	(本田(4)			
UK 49701	旭田(田)			

12 [認証]タブをクリックします。

13 認証の設定をおこないます。

・認証にMAC-RADIUSを使用する場合は、「暗号化されていない認証(PAP、SPAP)」に チェックマークをつけて、[OK]をクリックします。

ダイヤルイン フロファイルの編集	? ×	
ダイヤルインの制限 IP マルチリンク 認証 暗号化 詳細設定		
この接続に許可する認証方法のチェックボックスをオンにします。		
EAP メンクド(E)		
▼ Microsoft 暗号化認証バージョン 2(MS-CHAP v2)②		
🥅 パスワードの期限が切れた後、ユーザーがパスワードを変更する(<u>C</u>)		
└── Microsoft 暗号化認証 (MS-CHAP)(M)		
■ パスワードの其服徒が切れた後、ユーザーがパスワードを変更する(S)		
□ 暗号化認証 (CHAP)(N)		
↓ 暗号化されていない認証 (PAP、SPAP)(U)		
「認証されていないアクセス――	- II	
□ クライアントが認識正方法をネゴシェートせずに接続できるようにす(300)		
OK キャンセル 適用	æ	

・認証にEAP-TLS、EAP-PEAPを使用する場合は、[EAPメソッド]をクリックします。 EAP-TLSの場合は「スマートカードまたはその他の証明書」が、EAP-PEAPの場合は「保 護されたEAP(PEAP)」がそれぞれのリストの最上部に表示されていることを確認し、 [OK]をクリックします。

最上部にない場合は、項目を選択して[上へ移動]をクリックしてください。 PEAPの場合、次の追加設定をおこなってください。

- ・「保護されたEAP(PEAP)」を選択し、[編集]をクリック
- ・「セキュリティで保護されたパスワード(EAP-MSCHAPv2)」を選択し、[編集]をク リック
- ・「認証の再試行回数」を「0回」に設定

EAP プロバイダの選択	? ×
EAP の種類は表示されている順序でネゴシェートされます。	
EAP の種類(P):	
(栄養された EAP (PEAP) スマート カードまたはその他の時代日本	上へ移動(U)
	下へ移動(<u>D</u>)
追加(A) 編集(E) 削除(B) OK	キャンセル

14 [OK]をクリックし、設定を完了します。

以上でRADIUSサーバーの設定は完了です。
例8:802.1X無線認証を利用する(内蔵RADIUSサーバー機能を利用する場合)

本製品はRADIUSサーバーを用いた無線パソコン認証に対応しています。内蔵RADIUSサーバー 機能を使用することにより、RADIUSサーバー(Windows Server等)をお持ちでない環境におい ても強固なセキュリティーを持つ無線ネットワークを構築することができます。

ここでは例として、内蔵RADIUSサーバー機能を使用したネットワークを構築する方法を説明し ます。

構成例



無線パソコン

条件

・認証には本製品の内蔵RADIUSサーバーを使用し、内部認証にPEAP(MS-PEAP)を使用する。

・接続をおこなうすべてのパソコンにPEAP(MS-PEAP)方式の認証に対応したサプリカントがインストールされ、必要な設定がおこなわれている。
 (サプリカントのインストールや設定は、各ソフトウェアのマニュアルをご参照ください。

弊社製無線子機をお使いの場合、添付のクライアントマネージャ3またはクライアントマネー ジャVのヘルプをご参照ください)

- ○★ ・この設定事例ではアクセスポイントが自己発行サーバー証明書を使用するため、P77の 図1、図2のようにサプリカント側のサーバー証明書の検証を行わない設定にしてくだ さい。Verisign等の発行した証明書を用いて検証を行う場合は別途PKCS#12形式の 証明書をインポートする必要があります。
 - ・証明書ファイルには、「サーバー証明書(秘密鍵を含む)」、「CA証明書およびRoot証明書 までのChainを構成する全ての中間証明書」が含まれている必要があります。
 - ・本製品の内蔵RADIUSサーバーは内部認証にTLSを用いた認証にも対応しております。
 TLS方式で認証を行う場合、クライアント側の証明書に対応したPKCS#12形式の証明 書を新たにインポートする必要があります。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・クライアントパソコン

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、認証の設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。



3 画面左側の[無線設定]-[(802.11aの)無線セキュリティー]をクリックします。

4 以下のように設定して、[設定]をクリックします。

無線の認証: WPA/WPA2 mixedmode-EAP追加認証: 追加認証を行わない無線の暗号化: TKIP/AES mixedKey更新間隔: 60分ANY接続: 許可するプライバシーセパレーター: 使用しない

無線セキュリティー設定(11a)

? ヘルプ

無線の認証	 記録を行わない) ご目を認む、1×/EAP WPA-PSK WPA/WFA2 mixedmode - PSK WPA/WFA2 mixedmode - PSK WPA/EAP WPA2 = CAP WPA2 = CAP
迫力感忍難	 ● 追加型証を行わない ● MAC アドレスリスト+Lある制限 ● MAC アドレスリスト+MAC PADTUS認証 ● MAC PADTUS認証 12証±1(スワード ● MAC アドレスを使う ○ /次のパスワードを使う ● MAC アドレスを使う ● MAC PAC PAC PAC PAC PAC PAC PAC PAC PAC P
無線の暗号化	 ● 昭号化なし ● VEP(国定値Key) ■ 町町寄代上+- 文字入力・13文字(WEP128) ● ● 1: ② 2: ③ 3: ④ 4: ● WEP(自動配信Key) 自動更新key長 WEP128 ● ■ WEP(自動配信Key) ● 前販更新key長 WEP128 ● ■ WEP(国定値Key)の併用 併用しない ● ■ 新した+ ■ WFA-PS((事前共有キー): ■ Key更新智路: ⑥ ● 次
[拡張設定]	
ANY接続	✓ 許可する
プライバシーセパレーター	使用しない V

設定

5 画面左側の[ネットワーク設定]-[RADIUS設定]をクリックします。

以下のように設定して、[設定]をクリックします。

内蔵RADIUSサーバー	:	使用する
EAP内部認証	:	PEAP(MS-PEAP)
EAP証明書ファイル形式	:	PKCS#12(*.pfx/*.p12)
EAP証明書ファイル	:	空欄
EAP証明書ファイル・パスワード	:	空欄
Shared Secret	:	abcdefgh(任意の値)
Session-Timeout	:	3600秒
Termination-Action	:	再認証を行う(RADIUS-Request)

内蔵RADIUSサーバー 🎴 ヘルプ

内蔵RADIUSサーバー	☑ 使用する
EAP内部認証	PEAP(MS-PEAP)
EAP証明書ファイル形式	PKCS#12(*.pf× / *.p12)
EAP証明書ファイル	参照
EAP証明書ファイル・バスワード	
Shared Secret	•••••
Session-Timeout	3600 秒

設定

8

6

7 以下のように設定して、[新規追加]をクリックします。

サブネット サーバー	: Management(プライマリー) : 内蔵RADIUSサーバーを使用する
RADIUS設定	? ヘルプ
RADIUS設定の新規追加 🤗 ^	ヽルプ
サブネット Management(プライマリー)	×
サーバー ・ の 成 RADIUSサーバーを使 ・ の サブネット上のRADIUSサ	用する ーバーを使用する
新規追加	
画面左側の[管理設定] -	-[ユーザー管理]をクリックします。

9 [登録ユーザーリストの編集]をクリックします。



10 以下のように設定して、[新規追加]をクリックします。

ユーザー名	: username(任意の値)	
ユーザー管理設定 - 登録	ユーザーリストの編集	? ヘルプ
編集を終了して前の画面へ戻る		
登録ユーザーリストの新規追加	? ヘルブ	
ユーサー名 username		
		×

新規追加

11 登録ユーザーリストの[修正]をクリックします。

登録ユーザーリン	スト ? ヘルプ							
ユーザー名	操作							
username	修正削除							
全てのユーザーを削除								

1			
	_	いてんしていうしょ	
	- / .	し い トの ように 彩定して	

パスワード :	ijklmnop(任意の値)
ユーザー管理設定 - 登録ユ	ーザーリストの編集 <u>?</u> ヘルプ
編集を終了して前の画面へ戻る	
登録ユーザーリストの修正 🤗	ヘルプ
ユーザー名 username	
1/2/)-F	
修正保存	
登録ユーザーリスト 🛛 ? ヘルプ	
ユーザー名 操作 username 修正中	
全てのユーザー植削除	

13 画面左側の[無線設定]-[(802.11aの)無線セキュリティー]をクリックします。

14	以下のように設定して、 無線機能 SSID	[設定]をクリックします。 : 使用する : 値を入力 Shanai(任意の値)								
	無線基本設定(11a)	? ヘルプ								
	無線機能	✔使用する								
	SSID	 ○ エアステーションのMACアドレスを設定(X0000000000, A) ◎ 値を入力: Shanai 								
	VLAN ID	1								
	無線チャンネル	Auto(W52) ▼ ※0F8ありの場合、気象レーダー等を感知すると自動的にチャンネルが変更されます モード 倍速モード(40M+z) チャンネル変更検出間隔 15 分 一子概測値中でもチャンネルが変更する								

以上で本製品の設定は完了です。

CLI設定手順

ここまでの設定をCLIを使っておこなうには、以下のコマンドを入力します。

(profile1)man\$ edit start profnum 1 (profile1)man[edit]\$ (profile1)man[edit]\$ airset 11a ssid security ssidnum 1 auth wpa2mixedeap cipher mixed rekey 60 (profile1)man[edit]\$ radius internal_server enable eap peap secret abcdefgh (profile1)man[edit]\$ radius primary enable internal_server (profile1)man[edit]\$ setup authuser add username (profile1)man[edit]\$ setup authuser password username ijklmnop (profile1)man[edit]\$ airset 11a ssid rename ssidnum 1 Shanai (profile1)man[edit]\$ airset 11a wireless enable (profile1)man[edit]\$ edit end Setting changed. Do you execute? (y/n)y

サプリカント側の設定例

図1 クライアントマネージャ3の場合 認証プロファイル × ブロファイル名(N) profile EAPの種類(E) EAP-PEAP • ユーザー設定(サーバー証明書の検証) □ サーバー証明書を検証する(C) Windowsの証明書を使用する(W) ストアされた証明書を自動的に使用する 🔻 ■ 中間評明機関も対象とする(0) ○ ファイルから指定する(E) □ 次のサーバ(ご接続する(0) ○ 完全一致している場合のみ許可する(2) ● 後方が一致している場合に接続を許可する(1) キャンセル OK





例9:社内ネットワークの安全を自動的に保ちたい(Microsoft NAP)

本製品は、Microsoftネットワークアクセス保護(NAP:Network Access Protection)を用い た無線パソコン認証に対応しており、強固な無線ネットワークと社内ネットワーク等のイントラ ネットへ接続するクライアントパソコンの正常性ポリシー(※)の管理をおこなうことができま す。

※ 正常性ポリシーとは、ファイアウォール、セキュリティーソフトの有無、自動更新などのセキュ リティーセンターの設定内容をもとに、パソコンのセキュリティー設定が安全であるかを判断 するための基準です。

ここでは例として、ネットワークアクセス保護を利用して本製品を社内ネットワークに導入する 方法を説明します。



構成例

条件

- ・NAP検疫を設定してあるWindows Server 2008が導入されている。
- ・インターネットに接続できるルーターが導入されている。
- TagVLANに対応したL2スイッチ(例:BS-POE-2124GMR(別売))が導入されている。
- ・本製品の有線側とL2スイッチがTrunk接続する。
- ・本製品の管理をおこなう管理部と、本製品の管理VLANを統一する。
- ・各部署のサーバーにVLAN、SSIDを使用して接続できるようにする。
- ・各部署のサーバーやパソコンへは通信できないようにする。
- ・利用者は、Active Directory等で事前登録されている。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

- ・Windows Server 2008(NAP検疫用)
- ・有線側ネットワーク機器(例:TagVLANに対応したL2スイッチなど)
- ・クライアントパソコン

設定手順(L2スイッチの設定)

Webブラウザーを使って、ネットワークからL2スイッチヘログインし、PoE設定とVLAN設定をおこないます。(ここでは例として、BS-POE2124GMR(別売)を使用します)



- 1 L2スイッチのマニュアルを参照して、L2スイッチの設定画面を表示します。
- 2 [基本設定]-[PoE設定]-[PoEポート設定]をクリックします。

3 PoE設定をおこないます。

以下のようにポート2を設定して、[設定]をクリックします。 優先度 : 高 ハイパワー : afhigh-power (他の項目は、初期値のまま使用します)

PoEボート設定

ボート	PoE有効化	優先度	ハイバワー
1	ON 🔽	低 🖌	Disable 💌
2	ON 🔽	高 🖌	af high-power 💌
3	ON 🔽	低 🖌	Disable af high-power
4	ON 💌	低 🖌	Disable 💌
5	ON 💌	低 🖌	Disable 💌
6	ON 💌	低 🖌	Disable 💌
7	ON 💌	低 🗸	Disable 💌

4 [詳細設定]-[VLAN設定]-[VLANステータス]をクリックします。

5 企画部のVLAN(101)を作成します。

以下のように項目を設定して、[設定]をクリックします。

VLAN ID	:	101
VLAN名	:	Kikaku
VLAN Management	:	チェックなし
ポート	:	2& Static Tagged, 3~12& Static Untagged,
		1、13~26を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

tagged -:Not Membe	gged U:Static Untagged	-:Not Member
--------------------	------------------------	--------------

新規VLAN 作成

VLAN ID:	101 (1-4094)
VLAN 名:	Kikaku
VLAN Management:	

ボート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	\bigcirc	۲	\bigcirc	\bigcirc	\bigcirc	\circ	\bigcirc	\bigcirc	$^{\circ}$	\bigcirc																
Static Untagged	\bigcirc	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	\bigcirc													
Not Member	۲	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲										

設定 再読込 クリア

6 営業部のVLAN(102)を作成します。 以下のように項目を設定して、[設定]をクリックします。

VLAN ID	:	102
VLAN名	:	Eigyo
VLAN Management	:	チェックなし
ポート	:	2& Static Tagged, 13~22& Static Untagged,
		1、3~12、23~26を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
101	-	Т	U	U	U	U	U	U	U	U	U	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Kikaku
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged U:Static Untagged -:Not Member

新規VLAN 作成

VLAN ID:	102 (1-4094)
VLAN 名:	Eigyo
VLAN Management:	

ボート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	\bigcirc	۲	\bigcirc																							
Static Untagged	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	\bigcirc	\bigcirc	\bigcirc	\bigcirc											
Not Member	۲	0	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	0	0	\bigcirc	0	0	\bigcirc	0	\bigcirc	0	0	۲	۲	۲	۲

設定 再読込 クリア

7 NAP修復用のVLAN(1000)を作成します。 以下のように項目を設定して、[設定]をクリックします。

VLAN ID	:	1000
VLAN名	:	NAPrepair
VLAN Management	:	チェックなし
ポート	:	2を「Static Tagged」、23を「Static Untagged」、
		1、3~22、24~26を「Not Member」

VLANステータス

VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
101	-	Т	U	U	U	U	U	U	U	U	U	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Kikaku
102	-	Т	-	-	-	-	-	-	-	-	-	-	U	U	U	U	U	U	U	U	U	U	-	-	-	-	Eigyo
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged	U:Static Untagged	-:Not Member
-----------------	-------------------	--------------

新規VLAN 作成

VLAN ID:	1	000	(1-	4094	4)																					
VLAN 名:	N	APre	pair																							
VLAN Managemer	nt: [
_		_																								
ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	\bigcirc	۲	\bigcirc	\circ	\bigcirc																					
Static Untagged	\bigcirc	۲	\bigcirc	\bigcirc	0																					
Not Member	۲	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	\bigcirc	۲	۲	۲

設定
再読込
クリア

8 VLANステータスに表示されているVLAN 1の欄にある[編集]をクリックします。

管理部のVLAN(1)を作成します。 以下のように設定を変更して、[設定]をクリックします。

VLAN ID	:	1
VLAN名	:	Kanri
VLAN Management	:	チェックあり
ポート	:	2を「Static Tagged」、1、3~22、24~26を「Static Untagged」、23を
		「Not Member」

VLANステータス

9

VLA	U ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	VLAN 名
1		U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
10	1	-	Т	U	U	U	U	U	U	U	U	U	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Kikaku
10	2	-	Т	-	-	-	-	-	-	-	-	-	-	U	U	U	U	U	U	U	U	U	U	-	-	-	-	Eigyo
100	00	-	Т	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	U	-	-	-	NAPrepair
PVI	ID	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

T:Static Tagged	U:Static Untagged	-:Not Member

新規VLAN 作成

VLAN ID:	1 (1-4094)
VLAN 名:	Kanri
VLAN Management:	

ボート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Static Tagged	\bigcirc	۲	\bigcirc	0	0	\bigcirc																				
Static Untagged	۲	\bigcirc	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	\bigcirc	۲	۲	۲
Not Member	\bigcirc	$^{\circ}$	\bigcirc	۲	\bigcirc	\bigcirc	\bigcirc																			

設定 再読込 クリア

10 [詳細設定] – [VLAN設定] – [VLANポート設定]をクリックします。

11 各ポートにPVIDを設定します。

以下のように項目を設定して、[設定]をクリックします。

ポート1、2、24~26	:	1
ポート3~12	:	101
ポート13~22	:	102
ポート23	:	1000

VLANボート設定

ボート	1	3	5	7	9	11	13	15	17	19	21	23	25
PVID	1	101	101	101	101	101	102	102	102	102	102	1000	1
ボート	2	4	6	8	10	12	14	16	18	20	22	24	26
PVID	1	101	101	101	101	101	102	102	102	102	102	1	1

設定 再読込

以上でL2スイッチの設定は完了です。 続いて、Windows Server 2008の設定をおこないます。

設定手順(Windows Server 2008の設定)

Windows Server 2008を使用してNAP(Network Access Protection)機能を実現する方法を 提供するため、Windows Server 2008(以下サーバー)において以下の役割が構成されているこ とを確認してください。構成されていない場合は、追加インストールをおこなってください。 (設定に関しては、「サーバーマネージャ」を使用して説明します)

サーバーマネージャ役割

- Active Directory(ドメインサービス) 以下を参照してください。
- Active Directory(証明書サービス)
 エンタープライズのルートCAとして構成します。
- 3. DNSサーバー プライマリーDNSとして構成します。
- 4. ネットワークポリシーとアクセスサービス(NPS) 「NPS(シナリオウィザードを使用したNAPの構成)」(P86)を参照してください。

Active Directory(ドメインサービス設定)

- 1 [スタート]-[管理ツール]-[サーバーマネージャ]を選択します。
- 2 「サーバーマネージャ」が起動したら、[役割] [Active Directoryドメインサー ビス] – [Active Directoryユーザーとコンピューター] – [サーバー名(任意)] – [Users]を開きます。

3 [Users]内で右クリックし、ユーザー(例:NAPuser01)をウィザードの指示に したがって追加します。

※Windows Server 2008では、「パスワードは複雑さの要件を満たす必要がある」ポリ シーが初期設定で有効となっているため、簡単なパスワードは設定できません。パスワー ド設定時は、複雑なパスワードを設定するか、グループポリシーを変更してパスワードを 設定してください。

RADIUSクライアント

 「サーバーマネージャー」画面より、[役割] – [ネットワークポリシーとアク セスサービス] – [NPS(ローカル)] – [RADIUSクライアントとサーバー] – [RADIUSクライアント]を右クリックして[新規RADIUSクライアント]を選択 します。

2 以下のよう設定して、[OK]をクリックします。

フレンドリ名	: WAPM-APG300N
アドレス(IPまたはDNS)	: test_napserver.local
ベンダ名	: RADIUS Standard
共有シークレット	: nappassword(手動)
追加オプション	:「RADIUSクライアントがNAPに対応している」が有効

規 RADIUS クライアノト	
▼ この RADIUS クライアントを有効にする(E)	
名前とアドレス	
フレンドリ名(E):	
WAPM-APG300N	
, アドレス (IP または DNS)(<u>D</u>):	
test_napserver.local	確認(⊻)
∧`` <i>\</i> Å	
一般的な RADIUS クライアント用の RADIUS 標準を クライアント へンダを選択してください。 ペンダ名(M):	指定するか、一覧から RADIUS
RADIUS Standard	-
THE CASE AND ADDRESS OF THE AVAILABLE OF THE ADDRESS. INCL. 1 1997 ADDRESS	de objetiti - L objetite MV-7 El thérido ek
時(こも指定する必要があります。共有シークレットでは す。 ・ 手動(U) C 生成(G) サオシューカレット(S)	大文字と小文字が区別されま
時にも指定する必要があります。共有シークレットでは す。 ・ 手動(j) ・ 生成(g) 共有シークレット(S):	大文字と小文字が区別されま
時にも描定する必要があります。共有シークレットでは す。 ・ 手動(U) (* 生成(<u>G</u>) 共有シークレット(<u>S</u>): ●●●●●●●●●●●● 甘去:、	大文字と小文字が区別されま
はにも指定する必要があります。共有シークレットでは す ・ 手動(U) ○ 生成(G) 共有シークレット(S): 共有シークレットの確認入力(Q):	大文字と小文字加区別されま。
時にも指定する必要があります。共有シークレットでは す。	大文字と小文字が区別されま。
時(こち指定する必要があります。共有シークレットでは す。 チ教(山)	大文字と小文字が区別されま。
時にも指定する必要があります。共有シークレットでは ず。	大文字と小文字加区別にれま
時(こち指定する必要が恐ります。共有シークレットでは す。 デ 手動(U)	大文字と小文字が区別されま

※「共有シークレット」は、本製品の「RADIUS設定」にある「Shared Secret」と同じ値を設 定する必要があります。

NPS(シナリオウィザードを使用したNAPの構成)

1 「サーバーマネージャー」画面より、[役割] – [ネットワークポリシーとアクセス サービス] – [NPS(ローカル)]をクリックします。 2 「標準構成」で、「ネットワークアクセス保護(NAP)」を選択して[NAPを構成す る]をクリックします。



※ [NAPを構成する]をクリックすると、ウィザード画面が表示されます。

3 以下の内容を設定して、[次へ]をクリックします。

ネットワーク接続の方法	: IEEE802.1X(ワイヤレス)
アドレス(IPまたはDNS)	: test_napserver.local
ベンダ名	RADIUS Standard
共有シークレット	: nappassword(手動)
ポリシー名	: 任意のポリシー名
	(例:NAP802.1X(ワイヤレス)WAPM-APG300N)



4 「RADIUSクライアント」の手順2(P86)で追加したRADIUSクライアント (WAPM-APG300N)を選択して、[次へ]をクリックします。

NAP を構成する	×
802.1X 認証スイッチまたはアクセスポイントの指定	
RADIUS クライアントは、認証スイッチやワイヤレス、アクセス ポイントなどのネットワーク アクセス サー/ RADIUS クライアントはクライアント コンピュータではありません。 RADIUS クライアントを指定するには、[i自知]をクリックします。	৻৾৾৾৵৻ঢ়৾৾৽ঀ৾৾৾
RADIUS <i>D</i> 5/ <i>P</i> 2/KQ):	加(<u>A</u>) 集(E) 『除(E)
前へ(P) 茨へ(H) 売了(E) 年	ャンセル

5 「Active Directory(ドメインサービス設定)」の手順3(P85)で作成したユーザー グループを指定して、[次へ]をクリックします。

NAP を構成する	×		
ユーザーグループとコンピュー!	ヌグループの構成		
コンピュータのグループに対してアクセスを付与または拒否す。 す。ユーザーのグループに対してアクセスを付与または拒否す す。このポリシーに対し、コンピュータグループとユーザーグ	が場合は、ロンピュータグループ」(グループを追加しま グループの選択		? ×
グループを選択しないと、このポリシーはすべてのユーザーに コンピュータ グループ:	オブジェクトの種類を選択してください(S): グループ 場所を指定してください(F)		オブジェクトの種類(の)
	winserver2008.local 選択するオブジェクト名を入力してください (例)(E):		場所(」)
	Domain Users		名前の確認(<u>C</u>)
ユーザー グループ:		OK	
前へ(<u>P</u>)	次へ(N) 完了(E) キャンセル		

※使用する環境に合わせてグループを追加し、グループごとに設定を分けることもできます。

6 EAPの種類を設定して、[次へ]をクリックします。

EAPの種類 :セキュリティーで保護されたパスワード(PEAP-MS-CHAP)が有効

NAP を構成する	×
認証方法の構成	
PEAP (Innerted Extensible Authentication Protocol)は、ワイヤレスアクセフ、ポイントおよび認定なイッチで使用されな認定することで、AERA を構成するには、NFS サーバー上のサーバー証明書を確認し、認証の経緯を構成 考えに要素の分支す。 NFS サーバー証明書 場面の1音様でした。LEEPA#MEN(CA) まただからイアントコンドニータに含着されている公約 OA によって発 強軟のに含着が多た。LEEPA#E型数がないは、CaERI をかいたます(E) 強軟のに含着が多たがするに、CaERI をかいたます(E)	
ばた winserver/2008 local (2010/03/02 150403 まで有効) 表示(少). 遂沢(少). 産みの健整 FEAP の健整を選択してがさい。認知の種類によって、NISS がらか(ア)・ト・コンとコージまたはユー サーから受け入れる法格論解心理論(ユーザー名と1(イント、または証明者のハッイロか ガンまがます。 で たた・リーアへ「登録さればパワート(FEAP-Net-Orther VXS) の健康的変更では、証明時で、コーサーズン(ア)・ヘーズの点俗情報を入力できます。 「 マート・カードまたはその他の証明者(AP-N-マンタ) こが種類的変更では、注意相のに基づくレントーの名 見間すると素が多います。	
前へ(2) 洗へ(2) 売了(日 キャンセル	

※NPSサーバー証明書は、事前に追加したものが表示されます。

7 設定を変更せずに、そのまま[次へ]をクリックします。

NAP を構成する	õ				×
	仮想 LAN(VLAN	♦の構成			
RADIUS クライ のある制限付 を、RADIUS ク した指示に基づ VLAN を使用し 組織ネットワー 組織ネットワー	アント(スイッチおよびワイヤ ぎのネットワークおよび完全 ライアントに提供するよう NF いて適切なネットワークにト	レス アクセス ポイン なネットワーク アグ PS を構成できます ラフィックをルーティン 減する場合は、D: に提供するには、E	小を認識) が VLA セスを提供する細胞 。これにより、RAD ッグすることができま てへ] をクリックしてく 構成] をクリックしま	N をサポートする場 瓶ネットワークに開す US クライアントは、 す。 をさい。 す。	合、修復サーバ る VLAN 情報 NPS から受信
ー制成されたネー 制成されたネー	ットワークの VLAN ーーーー ットワークの VLAN 情報を	NPS (ご提供する).	[は、[構成] をクリッ		<u>構成(Q)</u>
		前へ(P)	;ħ<(<u>N</u>)		キャンセル

※上記は、NAP検疫後に接続する組織ネットワークのVLANと制限されたネットワークの VLANを設定する画面です。本設定事例では、上記の内容は設定しません。

8 NAP正常性ポリシーを設定して、[次へ]をクリックします。

システム正常性検証ツール : Windowsセキュリティー正常性検証ツール (「クライアントコンピュータの自動修復を有効にする」が有 効)

NAPに適合しないクライアントコンピューターのネットワークアクセス制限 : NAPに適合しないクライアントコンピュータの完全なネッ トワークアクセスを拒否する

					^
	NAP 正常性ポリシ	ーの定義			
インストールされて この正常性ポリシ	いるシステム正常性検証ッ ーで強制するシステム正常	ハールの一覧です(性検証ツールだけ	S) 「を選択してくださし	ho	
名前 Vindows 1	キュリティ正常性検証ツー)	16]			
↓ クライアント コ 選択した場合 イアント コンビ	ンピュータの自動修復を有外 、正常性ポリシーに洋拠しる ュータは、修復サーバーから	幼にする(E) ていないためにネッ ソフトウェア更新ブ	ットワークへのフル フ クログラムを取得で	?クセスを拒否された きます。	E NAP 対応クラ
選択しない場 完全なネット!	合、非準拠の NAP 対応り トーク アクセスは得られません	フライアント コンピ:	1一句は自動的に測	「新されず、手動で	更新されるまで
NAP に連合し	ないクライアント コンピュー	ータのネットワーク	アクセス制限:		
 NAP (こ適合 制限されたネ 	」ないウライアントコンピュー。 ットワークだけにアクセスを許	タの完全なネット! 可します。	フーク アクセスを拒	否する(<u>D</u>)	
C NAP (2適合	しないクライアント コンピュー	タレこ完全なネット「	フーク アクセスを許	ग वे थ्(प् र)	
		前へ(P))次へ(<u>N</u>)	完了(E)	キャンセル

※「システム正常性検証ツール」が複数インストールされている場合は、使用するものだけ にチェックマークを付けてください。



NAP を構成する 🛛 🛛
NAP 強制ポリシーおよび RADIUS クライアント構成の完了
次のポリシーが正常に作成され、次の RADIUS クライアントが正常に構成されました。
- 既定のフランサで構成の詳細を表示すない、「構成の詳細」をクリックしてださい。 - 構成を変更なには「調べ」をリックしてださい。 - 構成を保存してこのウ・ザードを閉じるには、「死了」をクリックしてください。
正常性ポリシー: NAP 8021X (ワイヤレス) WAPM-APG300N 迷蛇 NAP 8021X (ワイヤレス) WAPM-APG300N 非序地
接続要求ポリシー: NAP 802.1X (ワイヤレス) WAPM-APG300N
ネットワーク オリシー: NAP 6021× (ワイヤレス) WAPM-APG300N 連載 NAP 8021× (ワイヤレス) WAPM-APG300N 非原題 NAP 8021× (ワイヤレス) WAPM-APG300N NAP 非対応
1篇5式の註前版(0)
前へ(2) 次へ(1) 光7(E) キャンセル

システム正常性検証ツール

- 1 「サーバーマネージャー」画面より、[役割] [ネットワークポリシーとアクセス サービス] – [NPS(ローカル)] – [ネットワークアクセス保護] – [システム正常 性検証ツール]をクリックします。
- 2 画面右側の「Windowsセキュリティ正常性検証ツール」からプロパティ画面を表示させます。

			J .) >
システム正常性検証ツール		_	操作	
シューシュティーで学生検知りに用	(SUNA では MAR 対応力も(アントロンパットな)	の面から安また安全	- システム正常性検証ツール	
できます。SHVを使用する	には、SHVを構成して正常性ポリシーに1つ以上に	自加します。	表示	,
力并	(4-Feb 5		- 最新の情報に更新	
Windows セキュリティ正常性検	アソール 構成されました		- 🕜 ヘルプ	
			Windows セキュリティ正常性検証ツール	
			プロパティ	
			1 ANJ	

- 3 「Windowsセキュリティ正常性検証ツールのプロパティ」画面が表示されたら、 [構成]をクリックします。
- **4** Windows Vista/XPのポリシーにて、「ファイアウォール」と「自動更新」にのみ チェックマークを付けて、[OK]をクリックします。

ows セキュリティ正常性検証ツール	
dows Vista Windows XP	
下の設定を使用して、Windows セキュリティ正常性検証ツール ポリ す。	シーを定義します。ここで選択した内容により、ネットワークに接続するクライアントコンピュータの要件が定義され
<u>通信春報</u>	
ファイアウォール ▼ ネットワーク接続に対してファイアウォールが有効(<u>F)</u>	
マイルス対策 「ウイルス対策」	□ 点小口対策が最新の対能(T)
パイウェア対策 こ スパイウェア対策アプリケーションが有対(A)	▶ フレミイウェア対策が最新の状態(型)
自動更新 ▽ 自動更新が有効(<u>U</u>)	
2キュリティ更新ブログラムによる保護	
□ セキュリティ更新ブログラムのインストールが不十分なクライアントの	Dアクセスを制限する(R)
重要およびそれ以上	
クライアントによる最新のセキュリティ更新プログラムのチェックが必	要な間隔の時間数(S): 22
REPART IN THE PART OF A DATE OF A DATE OF A	パーコー・
ちょうしていたい。 を選択してください。	mアロソフムを4X19でであり。1861年に2月1007フロソフム4X1年元が必要な58音は、7X00パラ410月1つまたは4回方
☐ Windows Server Update Services	₩indows Update
	OK キャンセル 遠用(A

※ 上記は、接続クライアントに対する検疫のポリシーを設定する画面です。本設定事例で は、「ファイアウォール」と「自動更新」以外の内容は設定しません。

以上でWindows Server 2008の設定は完了です。

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、VLANおよびマルチSSIDの設定をお こないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

WAPM-APG300N		Air	Station P_{ℓ}
TOP	詳細設定	<u>システム情報</u>	<u>ا المحروم</u>
機能設定		フロファイフ情報	
		0	
一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一		profilel	
 新設に約0月日にと認定する(1001000 // と区ク/ 新線に約0基本設定をする 			
インターネット		サブネット 情報	
 インターネット接続を設定する 		サブネット 1:[Mana,	gement](VLAN 1)
その他		_{接続状態} 未取得 (DHCPク	ライアント:取得中)
 エアステーションのファームウェアを更新する 		解放	書き換え
ン エアステーションの設定を初期化する			
		■無線情報	
		IEEE 802.11a (A	uto(W52) /
		207400H) 2010	*****
		-71-7	00000000_H
		BOBLINE TRA-	FOR
		相传1C AES	
		マルチSSID 黒効	
		IEEE 802.11g (A	uto(1~11 ch) /
		11ch)	
			AAAAAAAA_U
		SGBE/J 丸 単PA-	POK
		相方1C AES	
		マルチSSID 無効	
		Language	
	[Japanese 🔽 🗌 Cha	ange Language
		(())) 2055 - J	4065 設定画面へ
			WPS 設定面面A

3 画面左側の[無線設定]-[(802.11aの)マルチSSID]をクリックし、[マルチSSID登録情報の編集]をクリックします。

マルチSSID設定(11a) <u>?</u> ヘルプ
SSID VLAN ID 認証 暗号化 状態
マルチSSIDの設定は登録されていません
マルチSSID登録情報の編集

4 企画部のネットワークの設定をおこないます。 以下のように項目を設定して、[新規追加]をクリックします。

SSID	:	Kikaku	
VLANID	:	101	
無線の認証	:	IEEE802.1x/EAP	
追加認証	:	Microsoft NAPを使用する	
		(制限ネットワークに使用するVLAN	1000)
無線の暗号化	:	WEP(自動配信Key)	
		(自動更新Key長 WEP128)	
ANY接続	:	許可する(チェックあり)	
プライバシーセパレーター	- :	SSIDセパレーター	

マルチSSID登録情報の新規追加 🔽 ヘルプ

0122	Kikala
ULAN TO	
VLAN IU	
無線の認証	22252 257(75724) 0 TEEE802.1x/EAP 0 WPA-PSK 0 WPA/WPA2 0 WPA/WPA2 0 WPA/WPA2 0 WPA/WPA2 0 WPA/WPA2 0 WPA/EAP 0 WPA/EAP 0 WPA/WPA2 0 WPA/WPA2
)最力08228E	 ● 追加認識を行わない ● MACアドレスリストによる事際 ● MACアドレスリスト+MAC-RADIUS認識 ● MACアドレスを使う ● MACアドレスを使う ● 次のパスワードを使う ● MACアドレスを使う ● MACアドレスを使用する ● MACREANA ● MACREANA
黒線の暗号化	 「時号化なし 「FF(間定値key) 「使用電号化キー (文字入力:13文字(WEP128)) ▼ 「 「WEP(自動配信key) 自動更新key長 (WEP128) ▼ 「 「 「WEP(自動配信key) (明用 併用しない ▼ 電号化キー 「
[始進設立]	107 C. # (IB) M . 2 77
	_
ANY接続	✓ 許可する
ブライバシーセバレーター	SSIDセバレーター 💌

新規追加

5 [設定]をクリックします。

同様に、営業部のネットワークの設定をおこないます。 以下のように項目を設定して、[新規追加]をクリックします。

SSID	:	Eigyo	
VLANID	:	102	
無線の認証	:	IEEE802.1x/EAP	
追加認証	:	Microsoft NAPを使用する	
		(制限ネットワークに使用するVLAN	1000)
無線の暗号化	:	WEP(自動配信Key)	
		(自動更新Key長 WEP128)	
ANY接続	:	許可する(チェックあり)	
プライバシーセパレーター	- :	SSIDセパレーター	

マルチSSID登録情報の新規追加 📪 ヘルプ

6

0075	
221D	Ligyo
VLAN ID	102
無線の認証	 ● 記録を行わたい() ● 訂EEE802.1x/EAP ● WPA-PSK ● WPA/WFA2 mixedmode - PSK ● WPA/WFA2 mixedmode - PSK ● WPA/EAP ● WPA/WFA2 mixedmode - EAP
追力略忍都正	 ③ 追加認証を行わない ● MACアドレスリストによる制限 ● MACアドレスリスト+MAC-RADIUS起証 ● MACアドレスを使う ● がのパスワードを使う ● MACアドレスを使う ● MACアドレスを使う ● MACアドレスを使う ● Microsoft NAPを使用する ● 創駅ネットワークに使用するVLAM: 1000
無線の暗号化	 ・ 時号化なし ・ (F)(御定信Key) ・ (安子入力: 13文字(WEP128)) ・ (WEP(信約)) ・ (動更有化キー (文字入力: 13文字(WEP128)) ・ ・ (中国の名称) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
[抗理設空]	NO CARBON DI
ANY按統	✓ 許可する
フライバシーセバレーター	SSDENU-9-

新規追加

7 [設定]をクリックします。

8 画面左側の[無線設定]-[(802.11aの)無線セキュリティー]をクリックします。

管理部の無線セキ	ュリティー設定をおこないます。 を設定して「新規追加]をクリックします
浜中のなりに項日 無線の認証 追加認証	 EEEE802.1x/EAP Microsoft NAPを使用する (制限ネットワークに使用する)/LAN 1000)
無線の暗号化	: WEP(自動配信Key) (自動更新Key長 WEP128)
ANY接続 プライバシーセパレ	: 許可する(チェックあり) ーター : 使用しない
無線セキュリティー	-設定(11a) ? ヘルブ
無線の認証	EZELE & CF47ball © IEEE802.1x/EAP WPA-PSK WPA-EAP WPA/WPA2 mixedmode - EAP
i鱼力og28亩	 通加認証を行わない MACアドレスリストHAC-RADIUS認証 MACアドレス以え HALC-RADIUS認証 MAC-RADIUS認証 MAC-RADIUS認証 MACアドレスを使う (次の)パスワードを使う (次の)パスワードを使う (次の)パスワードを使う (第8年ットワーク)に使用する 新駅キットワーク)に使用するVLAM: 1000
無線の暗号化	
[拡張設定]	,
ANY接続 プライバシーセバレーター	 ✓ 許可する 使用しない

設定

- 10 [設定]をクリックします。
- 11 画面左側の[無線設定]-[(802.11aの)無線基本]をクリックします。

12 管理部の無線基本設定をおこないます。 以下のように項目を設定して、[設定]をクリックします。

無線機能 : 使用する
 SSID : 値を入力する(Kanri)
 VLAN ID : 1
 (上記以外の設定値は、初期値のまま使用します)

無線基本設定(11a)	? ヘルプ
無線機能	☑ (使田才ス
TOPPING	
SSID	 ○ エア人ナーションOMACアドレ人を設定(X0000000000_A) ○ 値を入力: Kanri
VLAN ID	1
無線チャンネル	Auto(W52) マ (現在のチャンネル: 36+40) ※DFSありの場合、気象レーダー等を感知すると自動的にチャンネルが変更されます モード 倍速モード(40MHz) マ

- 13 [設定]をクリックします。
- 14 画面左側の[ネットワーク設定]-[RADIUS設定]をクリックします。
- 15 プライマリーサーバーを以下のように項目を設定して、[新規追加]をクリックします。

プライマリーサーバー : 使用する サーバー名 : RADIUSサーバーのIPアドレスまたはDNS解決可能なドメイン 名 Shared Secret : RADIUSサーバーと同じShared Secret

(上記以外の設定値は、初期値のまま使用します)

RADIUS設定	? ヘルプ			
RADIUS設定の新規追加 ? ヘルプ				
サブネット	Management(プライマリー) 💌			
サーバー名	PrimaryServer			
認証ボート	1812			
Accounting	☑ 使用する			
Account ingポート	1813			
Shared Secret	•••••			
Session-Timeout	3600 秒			
Termination-Action	□ Termination-Action 届性を使用する			

新規追加

16 同様にセカンダリーサーバーを以下のように項目を設定して、[新規追加]をクリックします。

セカンダリーサーバー	: 使用する
サーバー名	: RADIUSサーバーのIPアドレスまたはDNS解決可能なドメイン
	名
Shared Secret	: RADIUSサーバーと同じShared Secret
(上記以外の設定値は、	刃期値のまま使用します)
RADIUS設定	? ヘルブ

RADIUS設定の新規追加 🍱 ヘルノ			
サブネット	Management(セカンダリー) 🗸		
サーバー名	SecondaryServer		
認証ポート	1812		
Accounting	☑ 使用する		
Accountingボート	1813		
Shared Secret	•••••		
Session-Timeout	3600 秒		
Termination-Action	□ Termination-Action 属性を使用する		

r	#C+8`0 hn
L	新规追加

17 画面左側の[LAN設定]-[サブネット設定]をクリックします。 [サブネットの編集]をクリックします。



18「サブネットの表示/操作」に登録されている「Management」欄の[編集]をクリックします。



設定

19 管理用サブネット(Management)を以下のように設定して、[修正保存]をクリックします。

:	Management
:	管理サブネット
:	1
:	手動設定
:	192.168.11.100(255.255.255.0)
	(RADIUSクライアントとして登録したIPアドレス)
:	ルーティング
:	空欄
:	空欄
:	受信「RIPv1」と「RIPv2」にのみチェックマークを付ける
:	使用しない
:	1500
:	使用しない

サブネット情報の編集

? ヘルプ

編集を終了して前の画面へ戻る

サブネット情報の編集 🎴 ヘルプ

サブネット名	Management		
サブネット種別	● 管理サブネット		
VLAN ID	1		
IP アドレスの取得方法	● 手動設定○ DHCP クライアント		
	IP アドレス 192.168.11.100		
IF FFVA	サブネットマスク 255.255.255.0 💌		
ルーティング	ルーティング 💌		
デフォルトゲートウェイ	手動設定		
DNS	プライマリーサーバー:		
DNO	セカンダリーサーバー:		
£16452220	送信: 🗌 RIPv1 🔲 RIPv2		
副们中门地无作品	受信: VRIPv1 VRIPv2		
UPnP IGD	使用しない 🖌		
MTU	1500		
DHCP サーバー	 ●使用しない ●サブネットにDHCPサーバー機能を提供する ●サブネットにDHCPサーバー機能をRelayする 		

修正保存

20 [設定]をクリックします。

21 画面左側の[LAN設定] – [LANポート]をクリックします。

22 以下のように設定して、[設定]をクリックします。

VLAN モード :Tagged Port



23 [設定]をクリックします。

以上で本製品の設定は完了です。 続いて無線パソコンからそれぞれのSSIDを使ってネットワークに接続します。

クライアントの設定手順

NAP検疫をおこなうためにクライアント側の設定をします。Windowsドメイン参加を使用する場合、Windows端末はグループポリシーに従って自動的にNAPクライアントの設定が反映されます。 ここではドメイン参加をおこなわずに、手動設定にてNAPクライアントの設定をする方法を案内します。

※ NAP検疫に対応しているクライアント側のOSは、Windows Vista/XP(SP3以降)となります。

Windows Vistaの設定

クライアント側のOSがWindows Vistaの場合は、以下の手順で設定してください。

- 1 [スタート]-[アクセサリ]-[ファイル名を指定して実行]を選択します。
- 2 名前欄に「services.msc」と入力して、[OK]をクリックします。
- 3 サービス一覧から「Network Access Protection Agent」を右クリックし、[プロパティ]を選択します。
- 4 スタートアップの種類を「自動」に設定し、サービスの状態欄にある[開始]をクリックして、[OK]をクリックします。

表示名(N):	napagent Network Access Protection Agent		
脱明(D):	クライアント コンピュータ上のネットワーク アクセス保護 (NAP) 機能を有効にします		
実行ファイルのパス C:¥Windows¥Sys	(H): tem32¥svchost.exe -k NetworkService		
スタートアップの 種類(E): サービスのスタートT	自動 ▼		
サービスの状態:			
開始(S)	停止(T) 一時停止(P) 再開(R)		
	皆するときに適用する開始パラメータを指定してください。		

5 [スタート]ー[アクセサリ]ー[ファイル名を指定して実行]を選択します。

- **6** 名前欄に「mmc」と入力して、[OK]をクリックします。
- 7 コンソール1画面が表示されたら、「ファイル」ー「スナップインの追加と削除」を 選択します。
- 8 スナップインの追加と削除画面にて、「NAPクライアントの構成」と「グループポリシーオブジェクトエディタ」を追加し、[OK]をクリックします。



9

コンソール1の左画面にて、「コンソールルート」-「NAPクライアントの構成」-「実施クライアント」を選択し、右画面の「EAP検疫強制クライアント」を右クリッ クして、「有効」に設定します。

🔚 コンソール1 - [コンソー	ル ルート¥NAP クライアントの構成	(ローカル コンピュータ)¥実施クライアント	
🔚 ファイル(<u>E</u>) 操作(<u>A</u>)	表示(⊻) お気に入り(⊇) ウィン	ッドウ(W) ヘルプ(比)	_ 8 ×
🗢 🄿 🖄 📰 🚺			
 ◆ ● 2 m 経 m ○ コンソールルート ▲ 20 NB クライアント ○ 実施クライアン ○ 二 ジーザーインタ ○ 正常性登録の説 ○ 可一カル コンピュー 	 実施クライアント 名前 DHCP 検疫強制クライアント リモート アクセス検疫強制クライアント UFS ゲーレクス(検疫強制クライアント EAP 検疫強制クライアント EAP 検疫強制クライアント D. 79623 	状態 無効 無効 無効 有効	按作 実施クライアント ・ る示 ・ ここから新し 最新の情報に ヘルブ EAP 検疫強制クライ ▲ 協効 風新の情報に プロパティ マーハレブ
	名前: EAP れ 説明: FAP /	実変強制リライアント ドースの論制を NAP (ご得供します。	
	バージョン 10		
	ベンダ: Micros	soft Corporation	
< >	状態 有効		

- 10 コンソール1の左画面にて、「コンソールルート」-「ローカルコンピュータポリ シー」-「管理テンプレート」-「Windowsコンポーネント」-「セキュリティセン ター」を選択し、右画面の「セキュリティセンターをオンにする(ドメイン上のコ ンピュータのみ)」を右クリックして、[プロパティ]を選択します。
- 11 「有効」を選択して[OK]をクリックします。



- 12 コントロールパネル内の「ネットワーク共有センター」をダブルクリックし、「ワイヤレスネットワークの管理」をクリックします。
- 13 「追加」をクリックして、「ネットワークプロファイルを手動で作成します」を選択します。



14 以下の設定をおこなって、[次へ]をクリックします。

ネットワーク名 : 本製品に設定されているSSIDと同じ設定にします。 セキュリティの種類 : 本製品に設定されているセキュリティと同じ設定にします。 暗号化の種類 : 本製品に設定されている暗号化の種類と同じ設定にします。

セキュリティの種類(<u>S</u>):	000.4	
	802.1X	•
暗号化の種類(民):	WEP	~
セキュリティ キーまたは パスフレーズ(<u>C</u>):		□ パスフレーズ文* する(<u>D</u>)
☑ この接続を自動的に開始	台します(<u>エ)</u>	
■ ネットワークがブロー	ドキャストを行っていない	場合でも接続する(<u>0</u>)

- 15「接続の設定を変更します」をクリックします。
- 16 「セキュリティ」タブをクリックして、「ネットワークの認証方式の選択」で 「Microsoft:保護されたEAP(PEAP)」を選択し、[設定]をクリックします。
- 17 「サーバーの証明書を検証する」にチェックマークが付いていることを確認して「信頼されたルート証明書機関」にて使用するサーバーを選択します。
- 18 「認証方式を選択する」で「セキュリティで保護されたパスワード(EAP-MSCHAP v2)」を選択します。
- 19「すばやい再接続を有効にする」と「検疫のチェックを有効にする」にチェックマークを付け、[構成]をクリックします。

20 EAP MSCHAP v2のプロパティ画面にて、「Windowsのログオン名とパスワード(およびドメインがある場合はドメイン)を自動的に使う」のチェックマークを外します。



以上でWindows Vistaの設定は完了です。

Windows XPの設定

クライアント側のOSがWindows XPの場合は、以下の手順で設定してください。

- ┃ [スタート]−[ファイル名を指定して実行]を選択します。
- 2 名前欄に「services.msc」と入力して、[OK]をクリックします。
- 3 サービス一覧から「Network Access Protection Agent」を右クリックし、[プロパティ]を選択します。

4 スタートアップの種類を「自動」に設定し、サービスの状態欄にある[開始]をクリックして、[OK]をクリックします。

(ローカル コンピュー	タ) Network Access Protection Agent のプロパ ? 🗙	
全般 ログオン 回	11復 依存關係	
サービス:名:	napagent	
表示名(<u>N</u>):	Network Access Protection Agent	
見8月(<u>D</u>):	Windows クライアントにネットワーク アクセス保護への参加を許 可します。	
実行ファイルのパス(出): 〇単WINDOWS¥System32¥svchostexe -k netsvcs		
スタートアップの 種類(<u>E</u>):	自動	
サービスの状態:	開始	
開始(<u>S</u>)	停止① ─時停止 (2) 再開 (2)	
ここでサービスを開始するときに適用する開始パラメータを指定してください。		
開始4パラメータ(M):		
	OK キャンセル 通用(A)	

- 5 [スタート]ー[ファイル名を指定して実行]を選択します。
- **6** 名前欄に「mmc」と入力して、[OK]をクリックします。
- 7 コンソール1画面が表示されたら、「ファイル」ー「スナップインの追加と削除」を 選択します。
- 8 [追加]をクリックします。
- 9 「スタンドアロンスナップインの追加」画面が表示されたら、「グループポリシー」 を選択し、[追加]をクリックします。
- 10 グループポリシーオブジェクトの選択画面が表示されたら、[完了]をクリックします。
- 11 コンソール1の左画面にて、「コンソールルート」-「ローカルコンピュータポリ シー」-「コンピュータの構成」-「管理用テンプレート」-「Windowsコンポーネ ント」-「セキュリティセンター」を選択し、右画面の「セキュリティセンターを有 効にする(ドメイン上のコンピュータのみ)」を右クリックして、[プロパティ]を 選択します。

12「有効」を選択して、[OK]をクリックします。

セキュリティ センターを有効にする (ドメイン上のコンピュータのみ)のブロ ? 🔀
設定説明
🎒 セキュリティ センターを有効にする (ドメイン上のコンピュータのみ)
 ○ 未構成(Q) ○ 補助(E) ○ 無効(Q)
サポートされるパージョン: Microsoft Windows XP Professional, Windows Server 2003 ファミリ、またはそれ以
前の設定(P) 次の設定(N)
OK キャンセル 適用(A)

13 [スタート]ー[(すべての)プログラム]ー[アクセサリ]ー[コマンドプロンプト] を選択します。
14 EAP検疫強制クライアントを起動する「EAP Quarantine Enforcement Client」コマンドを実行します。

「netsh nap client set enforcement ID=79620 ADMIN="ENABLE" と入力し、 [Enter]キーを押します。

コマンドが実行されているかを確認するためには、「netsh nap client show state」と入力 し、[Enter]キーを押してください。

表示された「実施クライアントの状態」の中で、ENABLE設定したEAP Quarantine Enforcement Clientが「初期化済み=はい」となっていることを確認してください。

C:¥WINDOWS¥system32	¥cmd.exe	- 🗗 🗙
ID 名前 説明 バージョン ベンダ名 登録日 初期化済み	= 79620 = Wireless Eapol Quarantine Enforcement Client = Provides wireless Eapol based enforcement for NAP = 1.0 = Microsoft Corporation = = (\$1.0	
ID 名前 説明 バージョン ベンダ名 登録日 初期化済み	= 79621 = TS Gateway Quarantine Enforcement Client = Provides TS Gateway enforcement for NAP = 1.0 = Microsoft Corporation = ເມເບຊັ	
10 名前 説明 バージョン ベンダ名 登録日 初期化済み	= 79623 = EAP Quarantine Enforcement Client = EAP ベースの強制を NAP に提供します。 = 1.0 = Microsoft Corporation = = はい	

- 15 [スタート]ー[接続]を右クリックして、[開く]を選択します。
- 16 無線接続するデバイスを右クリックして、[プロパティ]を選択します。



17「ワイヤレスネットワーク」タブをクリックし、[追加]をクリックします。

🕹 ワイヤレス ネットワーク接続 3のプロパティ 🛛 🕐 🔀
全般 ワイヤレスネットワーク 詳細設定
✔ Windows でワイヤレス ネットワークの設定を構成する(W)
←利用可能なネットワーク(№):
範囲にあるワイヤレス ネットワークに接続、切断または詳細を表示するに は、下のボタンをクリックしてください。
ワイヤレス ネットワークの表示
優先ネットワーク(P): 下に、影まデジカも順に、利用コチャンシットロ、カに白色かけにはなします。
ドレー見表示された制度、利用可能なネットワークに自動的に接続します:
LAW .
<u>ワイヤレスネットワーク構成の設定</u> についての詳細を表示します。
 OK キャンセル

18「アソシエーション」タブにて以下の設定をします。

ネットワーク名(SSID) : 本製品に設定されているSSID

ネットワーク認証 : 本製品と同じ種類のセキュリティを設定します。 データの暗号化 : 本製品と同じ暗号化を設定します。

ワイヤレス ネットワークのプロパティ	? 🛛
アソシェーション 認証 接続	
ネットワーク名 (SSID)(N): NAP_buffalo	
□このネットワークがブロードキャストしていない 「ワイヤレス ネットワーク キー	場合でも接続する(<u>N</u>)
このネットワークでは)次のためのキーが必要:	
ネットワーク認証(A): オープン	/ システム 💌
データの暗号化(<u>D</u>): WEP	✓
ネットワーク キー(<u>K</u>):	
ネットワークキーの 確認入力(Q):	
キーのインデックス (詳細) 😒: 1 🔷	
▼キーは自動的に提供される(出)	
└──これはコンピュータ相互(ad hoc)のネットワーク ──ントを使用しないの)	で、 ワイヤレス アクセス ポイ
	OK キャンセル

19「認証」タブをクリックして、「EAPの種類」で「保護されたEAP(PEAP)」を選択し、「プロパティ」をクリックします。

ワイヤレス ネットワークのプロパティ 🛛 🕐 🔀
アソシェーション認証 接続
認証されたネットワーク アクセスをワイヤレスのイーサネットのネットワークで提供 するには、このオプションを遅んでください。
✓このネットワークで IEEE 802.1X 認証を有効にする(E)
EAP の種類(T): (保護された EAP (PEAP)
<u>לםולדּז(®</u>
✓コンピュータの情報が利用できるときは、コンピュータとして認証する(©)
□ ユーザーまたはコンピュータの情報が利用できないときは、 ゲストとして 認証する(④
 OK キャンセル

- 20「サーバーの証明書を検証する」にチェックマークが付いていることを確認して「信頼されたルート証明書機関」にて使用するサーバーを選択します。
- 21 「認証方式を選択する」で「セキュリティで保護されたパスワード(EAP-MSCHAP v2)」を選択します。

22「すばやい再接続を有効にする」と「検疫のチェックを有効にする」にチェックマークを付け、[構成]をクリックします。

保護された EAP のプロパティ ? 🔀
接続のための認証方法: ▼サーバーの証明書を検証する(⊻)
□)次のサーバー(ご接続する'Q):
信頼されたルート証明機関(R):
🔲 VeriSign Trust Network
VeriSign Trust Network
🔲 VeriSign Trust Network
VeriSign Trust Network
✓ winserver2008-DC-CA
🗌 Xcert EZ by DST 🥪
□新しいサーバーまたは信頼された証明機関を承認するようユーザーに求めな い(P)
認証方法を選択する(S):
セキュリティで保護されたパスワード(EAP-MSCHAP v2) 🛛 🖌 構成(C)
 ✓ すばやい再接続を有効にする(£) ✓ 検疫のチェックを有効にする(£) ✓ 検疫のチェックを有効にする(£) ✓ サーバーに暗号化バインドの TLV がない場合は切断する(£) ○ OK キャンセル

23 EAP MSCHAP v2のプロパティ画面にて、「Windowsのログオン名とパスワード(およびドメインがある場合はドメイン)を自動的に使う」のチェックマークを 外します。

EAP MSCHAPv2 ወታወለታፈ
接続のための認証方法:
合はドメイン)を自動的に使う(A)

以上でWindows XPの設定は完了です。

CL設定手順

ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

(profile1)man\$ edit start profnum 1 (profile1) man[edit]\$ airset 11a ssid add ssidname Kikaku vlanid 101 auth eap cipher wep rekey 60 key 128 (profile1)man[edit]\$ airset 11a ssid addsecurity ssidname Kikaku mode nap bgvlan 1000 (profile1)man[edit]\$ airset 11a ssid anyscan ssidname Kikaku enable (profile1) man[edit]\$ airset 11a ssid privacy ssidname Kikaku ssid (profile1)man[edit]\$ airset 11a ssid add ssidname Eigyo vlanid 102 auth eap cipher wep rekey 60 key 128 (profile1)man[edit]\$ airset 11a ssid addsecurity ssidname Eigyo mode nap bgvlan 1000 (profile1)man[edit]\$ airset 11a ssid anyscan ssidname Eigyo enable (profile1)man[edit]\$ airset 11a ssid privacy ssidname Eigyo ssid (profile1)man[edit]\$ airset 11a ssid rename ssidnum 1 Kanri (profile1)man[edit]\$ airset 11a ssid vlan ssidname Kanri vlanid 1 (profile1)man[edit]\$ airset 11a ssid security ssidname Kanri auth eap cipher wep rekey 60 key 128 (profile1)man[edit]\$ airset 11a ssid addsecurity ssidname Kanri mode nap bgvlan 1000 (profile1)man[edit]\$ airset 11a ssid anyscan ssidname Kanri enable (profile1)man[edit]\$ airset 11a ssid privacy ssidname Kanri ssid (profile1)man[edit]\$ airset 11a wireless enable (profile1)man[edit]\$ radius primary enable server [RADIUSプライマリー サーバー名] secret [SharedSecret] (profile1)man[edit]\$ radius secondary enable server [RADIUSセカンダ リーサーバー名] secret [SharedSecret] (profile1)man[edit]\$ ip lan address 192.168.11.100/24 force (profile1)man[edit]\$ ether port 1 vlan mode tagged (profile1)man[edit]\$ edit end Setting changed. Do you execute? (y/n)y

例10:スパニングツリーを利用する

スパニングツリーは、本製品や一部のネットワーク機器に搭載されている機能です。 ここでは、スパニングツリーを利用したネットワークの構成例を説明します。

スパニングツリーについて

利用用途

スパニングツリーに対応した機器(弊社製インテリジェントスイッチなど)と組み合わせることで、自動的にループ回避と冗長性を持ったネットワーク構成が可能になります。

おもな利点

- ・LANにおけるループ構成を自動で回避できます
- (ブロードキャストストームを回避したり、MACテーブルの学習が正常におこなえるように監視 します)
- ・ネットワーク構成に冗長性を持たせることができます
 (重要なパスが途切れた際にも代理として予備のリンクを検出しループを防ぎながら接続する ことができます)

スパニングツリーの種類(Legacy/Rapid)

Legacy(IEEE802.1D) : BPDUパケットを利用して、他のブリッジとスパニングツリープロト コルによるポート接続情報のやりとりをおこなうことで、ループの 検出や回避、冗長構成などを実現するための制御方法です。構成内容 によっては、収束するまでに時間がかかります。(最大で50秒間の通 信断が発生してしまいます)

Rapid (IEEE802.1w) : Legacyのスパニングツリーをより高速化させたプロトコルです。ただし、構成する機器がRapidスパニングツリーに対応していない場合は、Legacyとして扱われます。



条件

- ・すでにスパニングツリー機能を持ったネットワーク機器が設置、運用されている。
- ・本製品同士はリピーター機能(WDS)で接続する。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・スパニングツリー機能に対応したインテリジェントスイッチ(例:BS-G2024MR(別売)など) ・クライアントパソコン

設定手順(本製品)

Webブラウザーを使って、本製品の設定画面へログインし、スパニングツリーの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。



3 画面左側の[ネットワーク設定]-[ブリッジ]をクリックします。 以下のように項目を設定して、[設定]をクリックします。

Aging Time	:	300
スパニングツリー	:	使用する(チェックあり)
モード	:	RapidSTP
その他のパラメーター	:	初期設定のまま変更なし

※お使いの環境によっては、Hello TimeやMax Ageなど、パラメーターを個別に設定する 必要があります。

ブリッジ設定	
Aging Time	300
スパニングツリー	▼Spanning Tree Protocolをサポートする
モード	⊖STP ⊙ RapidSTP
Bridge Priority	32768
Forward Delay	15 秒
Hello Time	2 秒
Max Age	20 秒
Transmit Hold Count	6
Auto Edge	□ Auto Edgeを有効にする
設定	

ポートブリッジ情報の編集

ボート	Port Priority	Path Cost	Edgeポート	Point to Point
有線ポート(#1)	128	20		自動 🖌
無線基本ポート(11a) SSID[DODDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD	128	50		自動 🖌
無線基本ポート(11g) SSID[D000DDXXXXXXX_G]	128	50		自動 🖌

			£
	280	-	
. 8	Π.		

- 4 画面左側の[無線設定]-[(使用する無線規格の)無線基本]をクリックします。 「無線チャンネル」を「Auto」以外の固定のチャンネルに変更して、[設定]をク リックします。
 - ※リピーター機能(WDS)を使用するには、通信するエアステーションの無線チャンネルを すべて同じ設定にする必要があります。

無線基本設定(11g)	? ヘルプ
無線機能	☑使用する
SSID	 エアステーションのMACアドレスを設定(X00000000000,_G) 値を入力:
VLAN ID	1
無線チャンネル	Auto(1~11ch) ▼ 13 チャンネル 12 チャンネル 15 テンネル 11 チャンネル 15 分 10 チャンネル 5 + ンネルを変更する
[拡張設定]	8 チャンネル 7 チャンネル
無線モード	6 チャンネル 寺利用する 🗸
Contention Slot	ち ナャンイル 4 チャンネル
Preamble	3 チャンネル 2 チャンネル Auto(1~11ch) Auto(1~13ch) Urumuvs Z1L Rate BasicRate Z1L Rate BasicRate

5 画面左側の[無線設定]-[(使用する無線規格の)リピーター機能]をクリックします。 「リピーター機能(WDS)」を「使用する」に変更して、[設定]をクリックします。

リピーター機能(WDS)設定 (11g) ? ヘ ルプ
リビーター機能(WDS) 使用しない 使用してい 設定 WDS専用モードで使用する
※リビーター機能を使用するには通信する無線機と IPアドレスが重視しないようにして下さい。
通信可能なアクセスポイント マハノ MACアドレス 暗号化 VLAN ID 浅信可能なアクセスポイントが登録されていません 通信可能なアクセスポイントの編集
(木磯の無線側WACアドレス[XX:XX:XX:XX:XX]) [通信可能なアクセスポイントの編集]をクリックします。

7 下記のように変更して、[新規追加]をクリックします。 アクセスポイントの無線側MACアドレス:アクセスポイントの無線側MACアドレス VLANモード : Untagged Port 無線の暗号化 : AES WEP/PSK : 9876543210(任意の値)

リピーター機能(WDS)設定 - 通信可能なアクセスポイントの編集(11g) 🤶 ヘルプ

編集を終了して前の画面へ戻る

通信可能なアクセスポイントの衆	「規追加 🤗 ヘルブ
アクセスポイントの無線側MACアドレス	XXXXXXXXXXXXXX
VLAN モード	Untagged Port VLAN ID 1
暗号化	AES
WEP/PSK	•••••
	本機の無線側WACアドレス[XX:XX:XX:XX:XX:XX]

新規追加

6

 通信可能なアクセスポイント
 ペルブ
 MACアドレス 暗号化 VLAN ID 状態 操作 通信可能なアクセスポイントが登録されていません

8 通信相手側のエアステーションで、手順1~7までの手順をおこないます。

以上で本製品の設定は完了です。 設定が完了すると、Rapidスパニングツリープロトコルが動作し、ループ回避と冗長性を持った ネットワーク構成が自動的に設定されます。

CL設定手順

本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

(profile1)man\$ edit start profnum 1 (profile1)man[edit]\$ bridge aging 300 (profile1)man[edit]\$ bridge stp mode rstp (profile1)man[edit]\$ bridge stp enable (profile1)man[edit]\$ airset 11g channel 1 bandwith 20m (profile1)man[edit]\$ airset 11g wds enable (profile1)man[edit]\$ airset 11g wds add XX:XX:XX:XX:XX:XX (profile1)man[edit]\$ airset 11g wds security XX:XX:XX:XX:XX:XX wpapsk cipher aes key 9876543210 (profile1)man[edit]\$ edit end Setting changed. Do you execute? (y/n)y

例11:マルチキャストスヌーピングを利用する

本製品は、マルチキャストスヌーピング機能に対応しています。この機能を使用することで、マル チキャスト管理パケットの監視をおこない、不要なIPマルチキャストパケットのフラッディング を抑制することができるようになります。

ここでは例として、マルチキャストスヌーピング機能を使用したネットワーク設定について説明 します。

構成例



条件

- ・すでにネットワークにマルチキャストメディアサーバーやマルチキャストルーターが設置され ており、必要な設定がされている。
- ・会議資料などをマルチキャストメディアサーバーより無線パソコンへマルチキャスト配信する。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

- ・マルチキャストメディアサーバー(Windows Server 2003)
- ・マルチキャストルーター
- ・クライアントパソコン

設定手順

Webブラウザーを使って、本製品の設定画面へログインし、マルチキャストスヌーピングの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。



3 画面左側の[ネットワーク設定]-[マルチキャスト]をクリックします。

4 以下のように項目を設定して、[設定]をクリックします。

Snooping機能	:使用する(チェックあり)
Snooping対象プロトコル	:お使いの環境に合わせて設定
マルチキャスト無線LAN転送モード	:トンネル転送モードを有効にしない(チェックなし)
フィルタールール	:未学習のマルチキャストパケットを破棄しない
	(チェックなし)
マルチキャストAging Time	:300(秒)
Router Port	:有線ポート

 マルチキャスト設定
 アヘルブ

 Snooping 機能
 (使用する)

 Snooping 対象 プロトコル
 (□Pv4(100P))

 マルチキャスト無線LAN 転送モード
 □トンネル転送モードを有効にする

 フィルタールール
 □未学習のマルチキャストがケットを破壊する

 マルチキャスト Aging Time
 300 秒

 Router Port
 有線ボート(ま1) ♥

設定

5 画面左側の[無線設定]-[(使用する無線規格の)無線基本]をクリックします。 以下のように項目を設定して、[設定]をクリックします。

SSID	:	Multicast_11A
無線チャンネル	:	任意
モード	:	任意
Multicast Rate	:	お使いの環境に合わせて設定**

※マルチキャスト配信するコンテンツに応じて設定する必要があります。詳しくは、設定画 面のヘルプをご参照ください。

無線基本設定(11a)	? ヘルプ
無線機能	☑使用する
0122	○ エアステーションのMACアドレスを設定(XXXXXXXXXXXXXXXX)
0010	● 値を入力: Multicast_11A
VLAN ID	1
	Auto(W52)
	※DFSありの場合、気象レーダー等を感知すると自動的にチャンネルが変更されます ・ (佐連エード(40kul-)・
黒緑ナャンネル	
	テマノイル友史(映画)ppg 10 カ コース線通信曲でもエットングルズ亦画する
[扩建设定]	
東源モート	11a211n/2回时+1/用 9 合 🚩
	9Mone: fal Date BasicRate
	12Mhps: fri Pete PeoloPete
	18Mbps: til. Rate RasicRate
RateSet (11a)	24Mbps: ttt Rate BasicRate
	36Mbps: tu, Rate BasicRate
	48Mbps: フォレ. Rate @BasicRate
	54Mbps: つねし ORate @ BasicRate
	6.5~15Mbps : @ RateBasicRate
	13~30Mbps :)なし ④ Rate ○ BasicRate
	19.5~45Mbps: たし ® Rate BasicRate
RateSet (11n 1x)	26~60Mbps : tal Rate BasicRate
	520-120Mbps : True Rate BasicRate
	58.5~135Mbps: fri Pate PasiaPate
	65~150Mbps : til. Rate BasicRate
	13~30Mbps : trl. Rate Residente
	26~60Mbps : RateBasicRate
	39∼90Mbps :tal,RateBasicRate
RateSat (11n 2v)	52~120Hbps:)なし ③ Rate) BasicRate
Natebet (IIII 2X)	78~180Mbps: _ たし ® Rate BasicRate
	104~240Mbps: tal @Rate BasicRate
	11/~2/UMbps: tat Rate BasicRate
DCC DestaDet - Cot	6 10 04 hdbar
Guard Interval	0,12,24 Mbps
duard Interval	
Aggrogation	AMPDO V
hadreation	最大AMSDILLength 7935bytes >
フレームバースト	使用しない マ
802.11nプロテクション	マ使用する
DIIM Period	1
RTS Threshold	2947
Example Threshold	0046
rragment inresnoid	2340
Multicast Kate	Auto(BRS) V
ロートハランス(同時接続合数制限)	48 Mbps
端末キーブアライブ間隔	24 Mbps
802.11h送信バラメーター	18 Mbps
送信出力	9 Mbps
再送回数	6 Mbps Auto(BBS)
Beacon送信閒隔	100 Kus
SM PowerSave	無効
無線環境サーベイ	「サーベイを行う

設定

6 [設定]をクリックします。

7

画面左側の[無線設定]-[(使用する無線規格の)無線セキュリティー]をクリッ クします。

以下のように項目を設定して、[設定]をクリックします。

無線の認証	: WPA2-PSK
追加認証	: 追加認証を行わない
無線の暗号化	: AES
WPA-PSK(事前共有キー)	: 1234567890(任意の値)、Key更新間隔:60(分)
ANY接続	: 許可する(チェックあり)
プライバシーセパレーター	: 使用しない

? ヘルプ 無線セキュリティー設定(11a) ○認証を行わない O IEEE802.1×/EAP O WPA-PSK • WPA2-PSK 無線の認証 ○WPA/WPA2 mixedmode - PSK O WPA-EAP O WPA2-FAP ○WPA/WPA2 mixedmode - EAP ◉追加認証を行わない ○MACアドレスリストによる制限 ○ MACアドレスリスト+MAC-RADIUS認証 ○MAC-RADIUS認証 認証バスワード 追力唱忍証 ● MACアドレスを使う ○ 次のバスワードを使う ₩EP暗号化キー 文字入力・13文字(WEP128) ✔ . 1: 02: 03: O4: 無線の暗号化 自動更新Key長 WEP128 WEP (固定値Key)の併用 併用しない V 暗号化牛一 O TKIP AES WPA-PSX(事前共有キー): Key更新間隔: 60 分 [拡張設定] ✔ 許可する ANY接続 ブライバシーセバレーター 使用しない ~ 設定

8 [設定]をクリックします。

以上で本製品の設定は完了です。

CL設定手順

本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

(profile1)man\$ edit start profnum 1 (profile1)man[edit]\$ (profile1)man[edit]\$ bridge multicast snooping enable proto all rtport eth0 aging 300 defaultrule forward (profile1)man[edit]\$ bridge multicast tunnel disable (profile1)man[edit]\$ airset 11a ssid rename ssidnum 1 Multicast_11A (profile1)man[edit]\$ airset 11a channel auto_w52 bandwith 40m (profile1)man[edit]\$ airset 11a mrate 24 (profile1)man[edit]\$ airset 11a ssid security ssidnum 1 autu wpa2psk cipher aes rekey 60 key 1234567890 (profile1)man[edit]\$ edit end Setting changed. Do you execute? (y/n)y

例12:USBメモリーに本製品のログを記録する

本製品に搭載されているUSBポートに別売のUSBメモリーを取り付けると、本製品のログ情報を 記録することができます。

ここでは、USBメモリーに本製品のログ情報を記録するために必要な設定を説明します。

構成例



条件

- ・別売のUSBメモリーを使用する。
- ・ログ情報をUSBメモリーに記録する。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

・弊社製USBメモリー (対応USBメモリーについては、弊社ホームページをご参照ください)

設定手順

Webブラウザーを使って、本製品の設定画面へログインし、Syslog設定をおこないます。

- 1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。
- 2 「詳細設定」をクリックします。



3 画面左側の[機器診断]-[USB]をクリックします。 「USB機器名」にUSBメモリーの名称が表示されていることを確認します。

USBポート		? ヘルプ
接続ポート	USB	
USB機器名	USB Flash Disk	
消費電力	200mA	
ステータス		
イジェクト		

4 画面左側の[管理設定]-[ログ情報転送(syslog)]をクリックします。 USBメモリー転送機能の「使用する」にチェックマークをつけて、[設定]をクリッ クします。

ログ情報転送	(syslog)設定	? ヘルプ
ログ情報転送機能	□ 使用する syslogサーバー	
USBメモリー転送機能	☑使用する	
転送するログ情報	 パケットフィルター DHCPクライアント ROUTE AOSS ジジロファイラ NTPクライアント AOT 	 ✓ PPP₀Eクライアント ✓ DHCPサーバー ✓ US8 ✓ 無線クライアント ✓ 試定変更 ✓ システム起動 ✓ 有線リンク
設定全選択全	角郓余	

以上で本製品の設定は完了です。

CLI 設定手順

ここまでの設定をCLI を使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ usb show status
(profile1)man[edit]$ setup syslog client usb enable
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

ログ情報の確認方法

USBメモリーに転送されたログ情報の確認は、以下の手順でおこないます。

- 別冊の「ユーザーズマニュアル」を参照して、セキュリティーケースから本製品を 取り外します。
- 2 本製品正面のUSBイジェクトボタンを3秒以上押します。



3 USBランプが消灯したら、USBメモリーを抜き取ります。



4

USBメモリーをパソコンに挿して、記録されたログ情報を確認します。

D syslog.txt − Xモ帳	
ファイル(E) 編集(E) 書式(Q) 表示(V) ヘルプ(H)	
Oct 21 10:06:52 2008 [AP001650107447] : WIRED_ETH: et0: link down	^
Oct 21 10:06:57 2008 [AP001650107447] : WIRED_ETH: et0: link up(1000 Mbps Full duplex)	
Oct 21 10:07:04 2008 [AP001650107447] dhcpcd: Request: broadcasting DHCP_DISCOVER	
Oct 21 10:07:04 2008 L AP001650107447] dheped: broadcasting second DHCP_DISCOVER	
Oct 21 10:07:04 2008 [AP001650107447] dhcpcd: DHCP_OFFER received from (192.168.11.1)	
Oct 21 10:07:04 2008 [AP001650107447] dheped: broadcasting DHCP_REQUEST for 192.168.11.12	_
Oct 21 10:07:04 2008 [AP001650107447] dhcpcd: DHCP_ACK received from (192.168.11.1)	
Oct 21 10:07:04 2008 [AP001650107447] dhaped: Info : IP Address = 192.168.11.12	=
Oct 21 10:07:04 2008 L AP001650107447 dhcpcd: Info : Subnet Mask = 255.255.255.0	
Oct 21 10:07:04 2008 [AP001650107447] dhcpcd: Info : Default Gateway = 192.168.11.1	_
Oct 21 10:07:04 2008 L AP001650107447 dhcpcd: Info : DNSL1 = 192.168.11.1	
Oct 21 10:07:04 2008 [AP001650107447] dhaped: Info : DHCPSID = 192.168.11.1	
Oct 21 10:07:04 2008 L AP001650107447J dhcpcd: Info : DHCPGIADDR = 0.0.0.0	
Oct 21 10:07:04 2008 [AP001650107447] dhcpcd: Info : DHCPSIADDR = 0.0.0.0	
Oct 21 10:07:04 2008 L AP001650107447 dhcpcd: Info : DHCPCHADDR = XX:XX:XX:XX:XX:XX	
Oct 21 10:07:04 2008 [AP001650107447] dhcpcd: Info : DHCPSHADDR = XX:XX:XX:XX:XX:XX	
Oct 21 10:07:04 2008 [AP001650107447] dheped: Info : DHCPSNAME =	
Oct 21 10:07:04 2008 L AP001650107447 dhcpcd: Info : LEASETIME(172800) , RENEWALTIME(86400) ,	
REBINDTIME(151200)	
Oct 21 10:07:04 2008 L AP001650107447J dhcpcd: add resolve	~

以上でログ情報の確認は完了です。

例13:リピーター機能でローミング環境を構築したい

本製品のリピーター(WDS)機能を使用して、ローミング環境を構築する方法を説明します。

△注意 本設定事例では、802.11aと802.11gの同時通信が必要となりますので、WAPM-AG300Nをお使いの方は、本設定事例通りの設定はできません。

構成例



条件

- ・WAPM-APG300Nを使用している。
- ・AP1-AP2間、およびAP3-AP4間は、有線接続する。
- ・AP2-AP3間は、802.11gを使用してリピーター(WDS)通信する。
- ・各AP-無線パソコン間は、802.11aを使用して通信する。
- ・無線パソコンがローミングできるように、本製品の設定はすべて共通化する。

使用機器

対象機器

本製品(WAPM-APG300N)

必要機器

- ・クライアントパソコン
- ・有線側ネットワーク機器(例:スイッチなど)

設定手順(AP1~4共通の設定)

Webブラウザーを使って、本製品の設定画面ヘログインし、802.11aの設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。



3 画面

画面左側の[無線設定] – [(802.11aの)無線基本]をクリックします。 以下のように項目を設定して、[設定]をクリックします。

SSID : 無線チャンネル: モード :	Rainalsu Auto(W52)(任意のチャンネル) 倍速モード
無線基本設定(11a)	? ヘルブ
無線機能	☑使用する
SSID	 ○ エアステーションのMACアドレスを設定(X000XXX000XXX_A) ◎ 値を入力: kaihatsu
VLAN ID	1
無線チャンネル	AutoW20 家師の第10週後の「東京」レージー等を思知すると自動的なチャンネルが変更されます モード (招達モード(40M+b) ▼ チャンネル変更後出開発 15 分 一年級創作中でもチャンネルと変更する
[拡張設定]	
無線モード	11aと11nを同時利用する 💌

4 [設定]をクリックします。

5 画面左側の[無線設定]-[(802.11aの)無線セキュリティー]をクリックします。 以下のように項目を設定して、[設定]をクリックします。

無線の認証	:	WPA2-PSK
追加認証	:	追加認証を行わない
無線の暗号化	:	AES
WPA-PSK	:	1234567890(任意の値)、Key更新間隔:60(分)
ANY接続	:	許可する
プライバシーセパレーター	:	使用しない

無線セキュリティ	· 一設定 (11a) ? ヘルプ
無線の認証	EX322 & Z(+7) Z(L) EX322 & Z(+7) Z(L) WPA-2PK WPA-2PK WPA-2PK WPA-2PK WPA-2PK WPA-2PA WP
油力成認識	 ● は別成型目を行わない ● MACアドレスリストによる物理(● MACアドレスリストHub-FAADUSE2EE ● MACアトレスジスト・Hub-FAADUSE2EE ● MACアドレスダ(たう) ○ MACアドレスダ(たう) ○ MACアドレスダ(たう) ○ MACアドレスダ(たう) ○ MACアドレアトラー(たき(行う) ● MICreater (MAPを(行う)
煮練の暗号化	● 晴芳化なし ● UPU電音化本- 文字入力・15文字(WEP128) ● ● 1: 2: 3: 4: ● UPU(自由2)(ferm) 自動更新なの長 WEP128 ● WEP (自由2)(ferm) 自動更新なの長 WEP128 ● WEP (自由2)(ferm) ● 45: T127(ferm) (marked) WEALS T127(ferm) (m
Lat 25 (A ch 1	NOYOCATIBINE. 11 23
「仏」飯設定」	
ANY接続	 詳可する
プライバシーセパレータ-	- 使用しない 🔽

設定



以上でAP1~4共通の設定は完了です。 続けて、AP2とAP3にリピーター機能の設定をします。

設定手順(AP2、3のリピーター機能の設定)

Webブラウザーを使って、本製品の設定画面へログインし、リピーター機能の設定をおこないます。

1 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。

2 「詳細設定」をクリックします。

TOP	詳細設定	シフテレ	15.85	0.67
10 P	at HEAR AL	2810		• <u>1974</u>
200 ALEST			all de	
做形設定			7 IFI TR	
二 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一			ofile1	
※ 無線LANの暗号化を設定する(RADIUSサーバーを使う)			011101	
※ 無線LANの基本設定をする。		せつきゃん	iit aa	
インターネット		サブネット 1	Etternere mer	+](VLAN 1)
※ <u>インターネット接続を設定する</u>		ッフ ー ット 1.	ng得	ICJ(VL/AIN 1)
その他		接続状態(1	DHCP クライア	ント:取得中)
エアステーションのファームウェアを更新する			解放 書き換え	
エアステーションの設定を初期化する				
		兼線情報		
		IFFF 802 1	1a (Auto(W	52)/
		36+40ch)		
		SSID	******	XXX_A
	1	認証方式	₩PA-PSK	
	1	暗号化	AES	
		マルチSSID	無効	
		IEEE 802.1 11 ch)	1 g (Auto(1 ·	~11 ch) /
		SSID	XXXXXXXXX	XXX_G
	1	認証方式	₩PA-PSK	
	1	暗号化	AES	
		マルチSSID	無効	
		Language		
		Japanese 🔽	Change La	nguage
				STOLENES &
			4065 19	CELEBORIE V

3 画面左側の[無線設定]-[(802.11gの)無線基本]をクリックします。 以下のように項目を設定して、[設定]をクリックします。

無線チャンネル	:	1 チャンネル(Auto以外の任意のチャンネル)
モード	:	倍速モード

無線基本設定(11g)	3 ~1/7
無線機能	▼使用する
SSID	 エアステーションのMACアドレスを設定(X000X00000X_G) 値を入力:
VLAN ID	1
無線チャンネル	1 チャンネル V モード 倍速モード(40MHz, +5ch) V
[拡張設定]	
無線モード	11b, 11gと11nを同時利用する 🗸

- 4 [設定]をクリックします。
- 5 画面左側の[無線設定] [(802.11gの)リピーター機能]をクリックします。 「リピーター機能(WDS)」を「WDS専用モードで使用する」に変更して、[設定]を クリックします。

リビーター	·機能(#DS)設定 (11g) <u> へルラ</u>
リビーター機能(WDS) 使用しない 🔽
	使用しない
設定	WDS専用モードで使用する
※リビーター構	したいにには通信する無線機と
IF F F V X M	目板しないようにして下さい。
通信可能なアク	フセスポイント 🔽 ヘルプ
MACアドレス	暗号化 VLAN ID 状態
通信可能なアク	マセスポイントが登録されていません
通信可能な	アクセスポイントの編集

- 6 [設定]をクリックします。
- 7 [通信可能なアクセスポイントの編集]をクリックします。

8 画面左側の[無線設定]-[(802.11gの)リピーター機能]をクリックします。 以下のように項目を設定して、[新規追加]をクリックします。

アクセスポイントの無線側MACアドレス:アクセスポイントの無線側MACアドレス VLANモード : Untagged Port 無線の暗号化 : AES WEP/PSK : 9876543210(任意の値)

編集を終了して前の画面へ戻る 通信可能なアクセスポイントのま) 所知治加 ? ヘルブ
アクセスポイントの無線側MACアドレス	XXXXXXXXXXXXX
VLAN モード	Untagged Port VLAN ID 1
暗号化	AES
VEP /PSK	•••••
新規追加	本機の無線側WACアドレス[XX:XX:XX:XX:XX:XX]

9 もう1台のエアステーションにも同様の設定をおこないます。

以上で設定は完了です。

CLI設定手順(AP1~4共通の設定)

AP1~4の共通設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
(profile1)man[edit]$ airset 11a ssid rename ssidnum 1 kaihatsu
(profile1)man[edit]$ airset 11a channel auto_w52 bandwidth 40m
(profile1)man[edit]$ airset 11a ssid security ssidnum 1 auth wpa2psk
cipher aes rekey 60 key 1234567890
(profile1)man[edit]$ airset 11a ssid anyscan ssidnum 1 enable
(profile1)man[edit]$ airset 11a ssid ssidnum 1 privacy disable
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

CLI設定手順(AP2、3のリピーター機能の設定)

AP2、3のリピーター機能の設定をCLIを使っておこなうには、以下のコマンドを入力します。

(profile1)man\$ edit start profnum 1 (profile1)man[edit]\$ (profile1)man[edit]\$ airset 11g channel 1 40m subch 5 (profile1)man[edit]\$ airset 11g wds exclusive (profile1)man[edit]\$ airset 11g wds add XX:XX:XX:XX:XX: (profile1)man[edit]\$ airset 11g wds vlan 1 mode untagged vlanid 1 (profile1)man[edit]\$ airset 11g wds security XX:XX:XX:XX:XX: wpapsk cipher aes key 9876543210 (profile1)man[edit]\$ edit end Setting changed. Do you execute? (y/n)y

例14:リピーター機能で拠点間を無線接続したい

本製品のリピーター(WDS)機能を使用して、拠点間を無線接続する方法を説明します。

構成例



条件

- ・802.11a(W56帯)または802.11gを使用して、拠点間を無線接続する。
- ・暗号化はAESを使用する。
- ・本製品の屋内/屋外スイッチを「屋外」に切り替える。

使用機器

対象機器

本製品(WAPM-APG300N/WAPM-AG300N)

必要機器

- ・屋外設置アンテナ(WLE-HG-NDC/A(別売)やWLE-HG-DA/AG(別売)など)
- ・屋外アンテナ用同軸ケーブル(WLE-CCシリーズ(別売))
- ・同軸ケーブル変換コネクター(WLE-OP-RNC(別売))

設定手順

1 本製品前面の屋内/屋外スイッチを「屋外」に切り替えます。



- ▲注意・スイッチを「屋外」に設定すると、802.11a通信時にW56チャンネル(100/104/108/ 112/116/120/124/128/132/136/140ch)のみ使用可能となります。
 ・W52(36/40/44/48ch)およびW53(52/56/60/64ch)チャンネルを屋外で使用す ると、電波法違反となりますので、ご注意ください。
- 2 別冊の「ユーザーズマニュアル」を参照して、本製品の設定画面を表示します。
- 3 「詳細設定」をクリックします。



4 画面左側の[無線設定]-[(使用する無線規格の)無線基本]をクリックします。 以下のように項目を設定して、[設定]をクリックします。

無線チャンネル: 100チャンネル(AutoおよびW52/W53以外の任意のチャンネル) モード : 倍速モード

無線基本設定(11a)	? ヘルブ
無線機能	☑使用する
SSID	 エアステーションのMACアドレスを設定(XXXXXXXXXA) 値を入力:
VLAN ID	1
無線チャンネル	100 チャンネル/DFSあり) ▼ ※DFSありの場合、気象レーダー等を感知すると自動的にチャンネルが変更されます モード 倍速モード(40MHz, +104ch) ▼
[拡張設定]	
無線モード	11aと11nを同時利用する 🗸

- ▲注意 ・802.11aを使って拠点間を無線接続する場合は、必ずW56チャンネル(100/104 /108/112/116/120/124/128/132/136/140ch)をご使用ください。W52 (36/40/44/48ch)およびW53(52/56/60/64ch)チャンネルを使用すると、電波法 違反となります。
 - ・W56チャンネル使用時に本製品が中継機が気象レーダー等の発する電波検出すると、 同じ周波数帯を使わないよう無線チャンネルが自動的に変更されます。 (DFS(Dynamic Frequency Selection)機能) 無線チャンネル変更時は1分ほど通信ができなくなりますので、ご注意ください。
- 5 画面左側の[無線設定]-[(使用する無線規格の)リピーター機能]をクリックします。 「リピーター機能(WDS)」を「WDS専用モードで使用する」に変更して、[設定]を

クリックします。

リピーター機能(#DS)設定 (11a) 🔽 ヘルプ

リビーター機能(WDS)	使用しない	*
設定	使用しない 使用する WDS専用モードで使用す	5
※リビーター機能 IPアドレスが重複	を使用するには通信 しないようにして「	言する無線機と Fさい。
通信可能なアクセ	スポイント 🦻 ?	ヘルプ
MACアドレス 明	音号化 VLAN ID	状態
通信可能なアクセス	ポイントが登録されていま	ぜん
通信可能なアクt	2スポイントの編集)

(本機の無線側WACアドレス[XX:XX:XX:XX:XX:XX])

6 [設定]をクリックします。

7 [通信可能なアクセスポイントの編集]をクリックします。

8	画面左側の[無線設定]-[(使用する無線規格の)リピーター機能]をクリックします。
	以下のように項目を設定して、[新規追加]をクリックします。
	アクセスポイントの無線側MACアドレス:アクセスポイントの無線側MACアドレス VLANモード : Untagged Port 無線の暗号化 : AES
	WEP/PSK : 9876543210(任意の値)
	リピーター機能(WDS)設定 - 通信可能なアクセスポイントの編集 (11a) 🔽 ヘルプ

「「「「「「「」」」(「」」(「」」)(「」)(「」)(「」)(」)(」)(」)(」)(」)(」)(」)(」)(」)(」)(」)(」)(」	J
通信可能なアクセスポイントの衆	現追加 ? ヘルプ
アクセスポイントの無線側MACアドレス	000000000000000000000000000000000000000
VLAN モード	Untassed Port 🖌 VLAN ID 1
暗号化	AES
WEP/PSK	•••••
	本礎の無線側MACアドレス[XX:XX:XX:XX:XX:XX:XX]

新規追加

通信可能なアクセスポイント ペルブ MACアドレス 暗号化 VLAN ID 状態 操作 適信可能なアクセスポイントが登録されていません

緑体大約フレズ前の両面へ 更み しし

- 9 もう1台のエアステーションにも同様の設定をおこないます。
- 10 屋外アンテナのマニュアルを参照して、屋外アンテナを設置します。
- 11 別冊の「ユーザーズマニュアル」を参照して、本製品と屋外アンテナを同軸ケーブルで接続します。

以上で設定は完了です。

CLI設定手順

ここまでの本製品の設定をCLIを使っておこなうには、以下のコマンドを入力します。

```
(profile1)man$ edit start profnum 1
(profile1)man[edit]$
802.11aを使用する場合
(profile1)man[edit]$ airset 11a channel 100 40m subch 104
(profile1)man[edit]$ airset 11a wds exclusive
(profile1)man[edit]$ airset 11a wds add XX:XX:XX:XX:XX:XX
(profile1)man[edit]$ airset 11a wds vlan 1 mode untagged vlanid 1
(profile1)man[edit]$ airset 11a wds security XX:XX:XX:XX:XX:XX
wpapsk cipher aes key 9876543210
802.11gを使用する場合
(profile1)man[edit]$ airset 11g channel 1 40m subch 5
(profile1)man[edit]$ airset 11g wds exclusive
(profile1)man[edit]$ airset 11g wds add XX:XX:XX:XX:XX:XX
(profile1)man[edit]$ airset 11g wds vlan 1 mode untagged vlanid 1
(profile1)man[edit]$ airset 11g wds security XX:XX:XX:XX:XX:XX
wpapsk cipher aes key 9876543210
(profile1)man[edit]$ edit end
Setting changed. Do you execute? (y/n)y
```

35010638 ver.03

