

WIRELESS LAN BRIDGE
SB-520

IEEE802.3af規格PoE受電専用

おもな機能について

1

おもな機能の設定について

2

設定画面について

3

保守について

4

ご参考に

5



Icom Inc.

はじめに

このたびは、本製品をお買い上げいただきまして、まことにありがとうございます。

本製品は、[IEEE802.11g]規格と[IEEE802.11b]規格の2.4GHz帯無線LAN規格に対応し、異なる有線LAN同士を最高54Mbpsで無線ブリッジ接続する屋外用WIRELESS LAN BRIDGEです。

イーサネット電源供給ユニットを付属していますので、近くに電源がない場所にも設置できます。

ご使用前に、この取扱説明書をよくお読みいただき、本製品の性能を十分発揮していただくとともに、末長くご愛用くださいますようお願い申し上げます。

※本製品が対応する無線LAN規格は、以下のとおりです。

IEEE802.11b:11Mbps(2.4GHz帯)

IEEE802.11g:54Mbps(2.4GHz帯)

※[IEEE802.11g]規格は、[IEEE802.11b]規格と互換性があります。

※[IEEE802.11]規格(ch14)には対応していません。

※2010年10月現在、本製品は、Wi-Fiの認証を取得していません。

登録商標について

アイコム株式会社、アイコム、Icom Inc.、アイコムロゴ、WAVEMASTERは、アイコム株式会社の登録商標です。Microsoft、Windows、Windows Vistaは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

Adobe、Adobe Readerは、Adobe Systems Incorporated(アドビシステムズ社)の登録商標です。

Atherosは、Atheros Communications, Inc.の登録商標または商標です。

Wi-Fi、WPAは、Wi-Fi Allianceの商標または登録商標です。

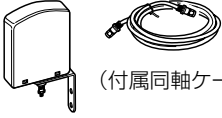
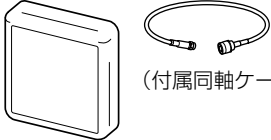
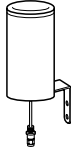
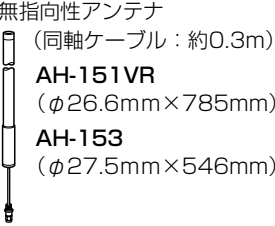
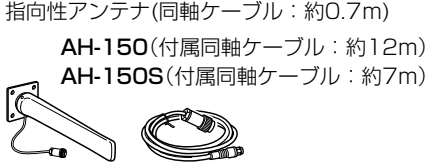
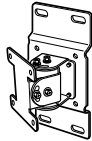


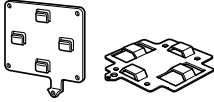
その他、本書に記載されている会社名、製品名は、各社の商標および登録商標です。

本製品の概要について

- ◎ SB-520本体(SA-4を除く)は、樹脂成形の防水構造JIS保護等級4相当(防まつ形)を採用していますので、屋内外を問わず設置が可能です。
- ◎ 内蔵アンテナ、および外部アンテナ(弊社別売品)の使用を選択できます。
- ◎ 設置場所や通信障害を調査、診断の目安になるサイトサーベイ機能を搭載しています。
- ◎ 本製品の電源供給は、PoE機能に対応しています。
付属のイーサネット電源供給ユニット(SA-4)をすることで、本製品に電源を供給できます。
- ◎ 無線ブリッジ簡易設定機能を搭載していますので、通信相手の登録が簡単です。
- ◎ 無線アクセスポイント機能を設定すると、無線ブリッジ機能と併用できます。
- ◎ [IEEE802.11g(54Mbps)]規格の無線LANには、地上波デジタルテレビジョン放送と同じ変調(OFDM)方式を採用していますので、マルチパスによる影響を受けにくく、高速で安定性に優れています。
- ◎ 無線ブリッジで使用しているときは、スパンニングツリー機能を設定することにより、ネットワークループによるネットワーク障害を防止できます。
- ◎ ルーティング機能を設定すると、無線LANと有線LAN間をルーティングできます。
- ◎ 無線アクセスポイント通信には、MACアドレスフィルタリング機能、ネットワーク(オープンシステム/共有キー)認証、IEEE802.1X認証、WPA(Wi-Fi Protected Access)暗号化方式など、高度なセキュリティーを搭載しています。
- ◎ ネットワーク管理機能にはSNMPをサポートしています。
- ◎ 有線LANは、10BASE-T/100BASE-TX(自動切り替え)に対応しています。
- ◎ 設定は、すべてWWWブラウザからできます。
- ◎ 技術基準適合証明を取得していますので、無線局の免許は不要です。

はじめに

別売品について

AH-104 ：平面アンテナ  (付属同軸ケーブル：約3m)	AH-166 ：平面アンテナ(高利得仕様)  (付属同軸ケーブル：約0.5m)	AH-154 ：カージオイド型アンテナ (同軸ケーブル：約0.3m) 
無指向性アンテナ (同軸ケーブル：約0.3m) AH-151VR (φ26.6mm×785mm) AH-153 (φ27.5mm×546mm) 	指向性アンテナ(同軸ケーブル：約0.7m) AH-150 (付属同軸ケーブル：約12m) AH-150S (付属同軸ケーブル：約7m) 	MB-89 ：仰角金具 調整範囲 上30/下30度 左30/右30度 
OPC-2113 ：同軸延長ケーブル (5D-HFA：約10m) AH-166以外のアンテナに 接続するときは、変換コネク ター(市販品)が必要です。 	OPC-1222A ：LANケーブル (約20m) 既存のLANケーブ ルと付け替えが必 要です。 	MB-91 ：壁面取付プレート 

【別売品についてのご注意】

弊社製別売品は、本製品の性能を十分に発揮できるように設計されていますので、必ず弊社指定の別売品をお使いください。

弊社指定以外の別売品とのご使用が原因で生じるネットワーク機器の破損、故障あるいは動作や性能については、保証対象外とさせていただきますので、あらかじめご了承ください。

本書の表記について

本書は、次の表記規則にしたがって記述しています。

[]表記：オペレーティングシステム(OS)の各ウィンドウ(画面)、ユーティリティ、設定画面の各メニューとそのメニューに属する設定画面の名称を([])で囲んで表記します。

[]表記：タブ名、アイコン名、テキストボックス名、チェックボックス名、各設定画面の設定項目名を([])で囲んで表記します。

< >表記：ダイアログボックスのコマンドボタンなどの名称を(<>)で囲んで表記します。

※ Microsoft® Windows® 7 Ultimate、Microsoft® Windows® 7 Professional、Microsoft® Windows® 7 Home Premiumは、Windows 7と表記します。

Microsoft® Windows Vista® Home Basic、Microsoft® Windows Vista® Home Premium、Microsoft® Windows Vista® BusinessおよびMicrosoft® Windows Vista® Ultimateは、Windows Vistaと表記します。
Microsoft® Windows® XP Professional、Microsoft® Windows® XP Home Editionは、Windows XPと表記します。

※ 本書は、Ver.1.03のファームウェアを使用して説明しています。

※ 本書中の画面は、OSのバージョンや設定によって、お使いになるパソコンと多少異なる場合があります。
また、説明のため、実際に表示される画面とは異なる場合があります。

はじめに	2
登録商標について	2
本製品の概要について	3
別売品について	4
本書の表記について	4

第 1 章

おもな機能について 7

1. 各部の名称と機能	8
2. PoE機能について	9
3. 無線通信モードについて	10
4. ローミング機能について	12
5. 暗号化方式について	12
6. スパニングツリー機能について	13
7. ルーティング機能について	13
8. VLAN機能について	14

第 2 章

おもな機能の設定について 15

1. DHCPサーバー機能を使用するには	16
2. 無線LANと有線LANのあいだをルーティングするには	17
3. [WEP RC4/OCB AES]暗号化を設定するには	20
4. [WPA-PSK(TKIP)/(AES)]暗号化を設定するには	25
5. [IEEE802.11b]規格の通信を制限するには	26
6. スパニングツリー機能を使用するには	27
7. 設定画面へのアクセスを制限するには	29

もくじ

第3章

設定画面について 31

1. 設定画面の名称と機能について 32
2. 「ネットワーク設定」メニュー 33
3. 「無線設定」メニュー 43
4. 「システム設定」メニュー 61
5. 「情報表示」メニュー 66

第4章

保守について 71

1. 設定内容の確認または保存 72
2. 保存された設定の書き込み 73
3. 設定を出荷時の状態に戻すには 74
4. ファームウェアをバージョンアップする 76

第5章

ご参考に 79

1. Telnetで接続するには 80
2. 設定画面の構成について 81
3. 定格について 82
4. 本製品以外の機器との無線ブリッジ接続について 83
5. 弊社製無線LAN端末との通信について 83
6. 本製品で使用しているソフトウェアのライセンス情報について 84

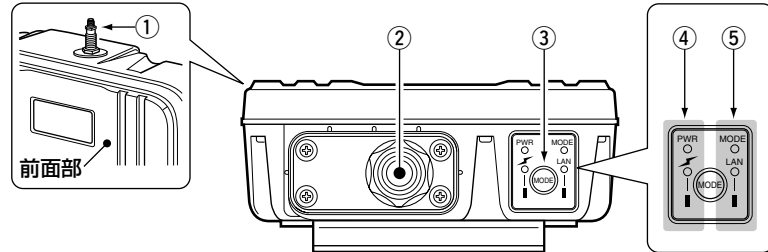
この章では、
本製品のおもな機能について説明しています。



1. 各部の名称と機能	8
■ SB-520	8
■ SA-4	9
2. PoE機能について	9
3. 無線通信モードについて	10
4. ローミング機能について	12
5. 暗号化方式について	12
6. スパニングツリー機能について	13
7. ルーティング機能について	13
8. VLAN機能について	14

1 おもな機能について

1. 各部の名称と機能

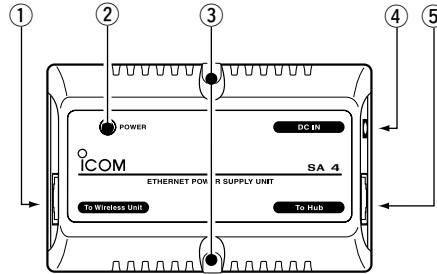
■ SB-520



- ① アンテナコネクタ 外部アンテナ(弊社別売品)を接続します。
※ アンテナを接続しない(内蔵アンテナを使用する)場合は、本製品の設定画面でアンテナの設定(※P44)を「内蔵アンテナ」に変更し、アンテナコネクタキャップ(付属品)を取り付けます。
※ 出荷時や全設定を初期化した場合、使用できるアンテナは、「外部アンテナ」に設定されます。
- ② LANケーブル SA-4(付属品)の[To Wireless Unit]ポート、または[IEEE802.3af]対応のHUBなどと接続します。
- ③ <MODE>ボタン 本製品の設定を初期化するボタンです。
※ 押しつづけると、[PWR](緑)ランプと[MODE](緑)ランプが、約5秒間、同時点滅します。すべてのランプが点灯したとき、ボタンから手をはなすと、自動的に設定を出荷時の状態に戻して再起動します。
- ④ [PWR](緑)/
[](赤)ランプ **[PWR](緑)ランプ**
点灯: 本製品に電源が供給されているとき
点滅: 初期化のため、<MODE>ボタンを押しつづけているとき
[](赤)ランプ
点灯: 本製品と無線通信を確立、または通信中のとき
消灯: 通信相手が存在しない、または無線通信しない状態がつづいたとき
※ 消灯までの時間は、通信状態によって異なります。
- ⑤ [MODE](緑)/
[LAN](赤)ランプ **[MODE](緑)ランプ**
点滅: 初期化のため、<MODE>ボタンを押しつづけているとき
スパニングツリー機能で経路を作成中のとき
[LAN](赤)ランプ
点灯: 有線LANへの接続が正常なとき
消灯: LANケーブルが未接続のとき
点滅: データを送受信しているとき

1. 各部の名称と機能(つづき)

■ SA-4

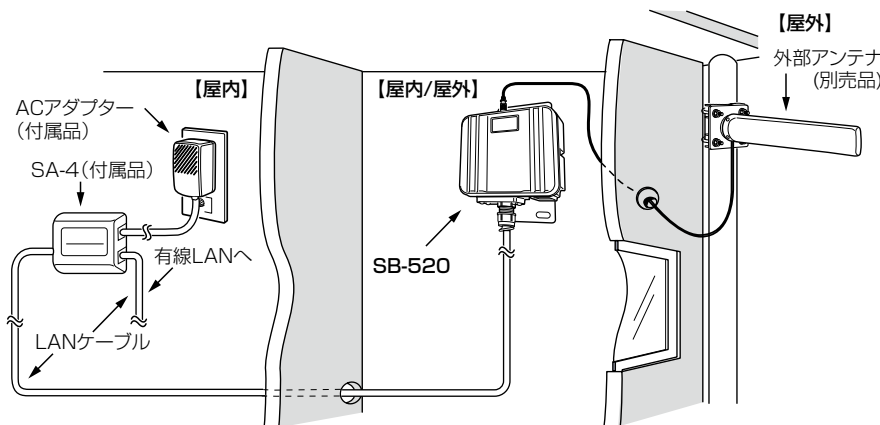


- ① [To Wireless Unit]ポート 本製品のLANケーブルと接続します。
- ② [POWER]ランプ 点灯:本製品とSA-4が接続されたとき
点滅:本製品とSA-4が未接続のとき
- ③ 壁面固定用ネジ穴 付属のタッピングネジ(AO-3×16:2本)でSA-4を固定する穴です。
- ④ [DC IN]ポート 本製品に付属のACアダプターを接続します。
- ⑤ [To Hub]ポート LANケーブル(市販品)で、有線LANと接続します。

2. PoE機能について

イーサネット電源供給ユニット(SA-4)、または[IEEE802.3af]規格対応のHUBを使用して、本製品のLANケーブルから電源を供給する機能です。

※SA-4の接続について詳しくは、別紙の「設定ガイド」をご覧ください。



SA-4の設置場所には十分ご注意ください。
 SA-4の通気口をふさいだり、極端に狭い場所や壁とのすき間など、風通しの悪い場所に設置したりしないでください。
 強力な磁界(電磁波)や静電気の発生する場所、温度、湿度が、本書に記載の使用環境を超えるところでは使用しないでください。
 発熱して故障の原因になることがあります。

1 おもな機能について

3. 無線通信モードについて

本製品は、次の4種類(3モード+OFF)が設定できます。

◎ 「Wireless Bridge(無線ブリッジ)」モード

(出荷時のモード)

対向する本製品同士が無線ブリッジ(レイヤー2)接続することで、お互いの有線LANを無線で接続するネットワーク形態です。

※無線ブリッジとして収容できる本製品の台数は、最大63台までですが、10台以下となることをおすすめします。

推奨台数や伝送速度は、環境により異なります。

※2010年10月現在、本製品以外と無線ブリッジ接続できる弊社製機器は、SB-510、SB-510EA、SB-5100です。

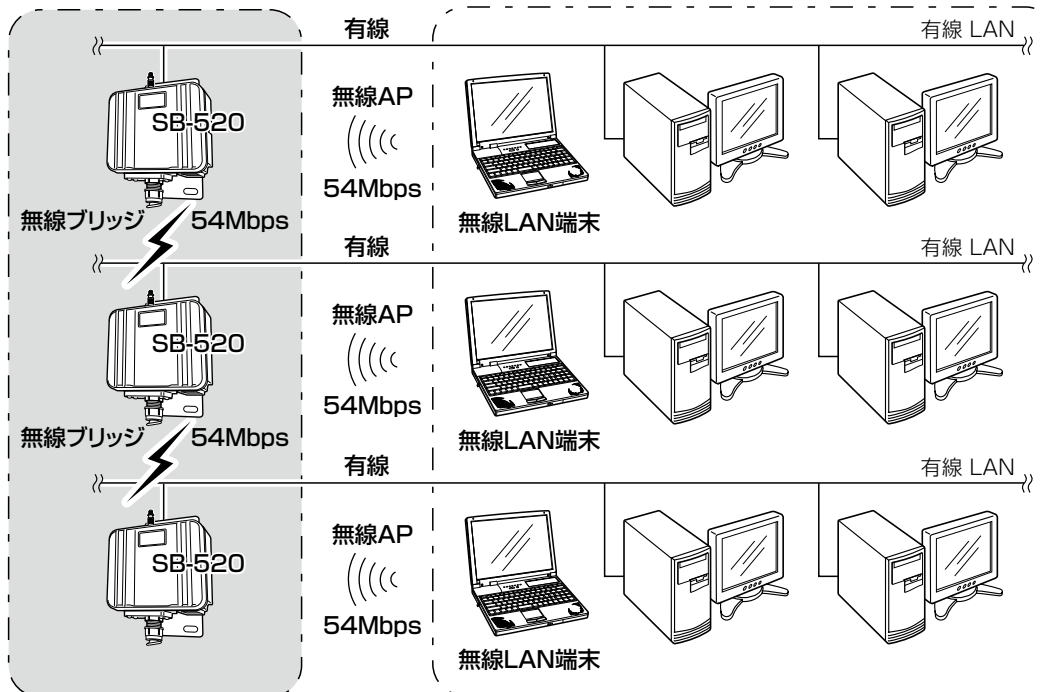
◎ 「Access Point(無線アクセスポイント)」モード

無線LAN端末が本製品を介して通信するネットワーク形態で、「Wireless Bridge」モードによるネットワーク形態と併用できます。

※収容できる無線LAN端末の台数は、本製品1台につき、10台以下となることをおすすめします。

推奨台数や伝送速度は、環境により異なります。

※説明では、SA-4を省略しています。



63台まで収容可能
(推奨台数:10台)

[1024台]★-[本製品の使用台数]まで収容可能
(本製品1台につき、無線LAN端末:10台を推奨)
★1024台は、無線LAN端末を含む台数です。

3. 無線通信モードについて(つづき)

◎「Site Survey(サイトサーベイ)」モード

ほかの無線LAN機器と電波干渉★しない最適な場所に設置されているかを確認できます。

本製品の無線伝送エリア内で稼働する無線LAN機器を自動で検出でき、その機器が使用する[無線チャンネル]、[電波強度(RSSI)]、[BSSID]、[暗号化方式]、[SSID]を最大64件分表示します。

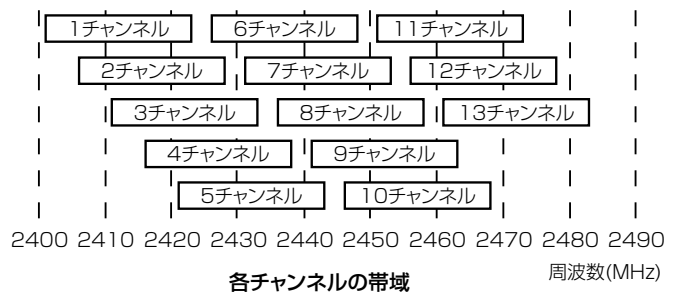
※「Site Survey」モード設定中、無線接続は停止します。

調査が終了したら、「Wireless Bridge」モード、または「Access Point」モードに設定してください。

★電波干渉について

電波干渉を防止するため、本製品の[無線チャンネル]は、別の無線ネットワークグループと4チャンネル以上空けて設定してください。

それ以下のときは、右図に示すように、帯域の1部が重複するため、近くに[IEEE802.11b/g]規格の無線アクセスポイントやビル間通信機器が存在するときは、電波干渉することがあります。たとえば、異なる無線ネットワークグループの[無線チャンネル]を、「01CH(2412MHz)」-「06CH(2437MHz)」-「11CH(2462MHz)」に設定すると電波干渉しません。



下記の画面は、本製品の設置場所でサイトサーベイ(通信環境調査)を実行した例で、本製品の「無線チャンネル」を「6」に設定するとよいという目安になります。

【サイトサーベイ表示例】

下記の通信環境調査例で、「07CH(2442MHz)」と「08CH(2447MHz)」については、表示された[電波強度(RSSI)]が弱い(数値が小さい)ため、「06CH(2437MHz)」と電波干渉する影響はありません。

また、「06CH(2437MHz)」が使用されている場合でも、そのチャンネルの無線アクセスポイントが少なく[電波強度(RSSI)]が弱い(数値が小さい)場合、影響しない場合もあります。

- ◎ 最大64件を表示します。
- ◎ チャンネル番号の小さい順に表示します。
- ◎ 同じチャンネルで使用されている場合は、検索された順番に表示します。

No	チャンネル	RSSI	BSSID	暗号化	SSID
1	01CH(2412MHz)	2800	90-C7-...	WEP	Wireless_A
2	07CH(2442MHz)	100	90-C7-...	WPA-PSK(TKIP)	Wireless_B
3	08CH(2447MHz)	500	90-C7-...	WPA-PSK(AES)	Wireless_C
4	11CH(2462MHz)	2800	90-C7-...	暗号なし	Wireless_D
5	12CH(2467MHz)	100	90-C7-...	WEP	Wireless_E
6	13CH(2472MHz)	500	90-C7-...	WEP	

◎「OFF」

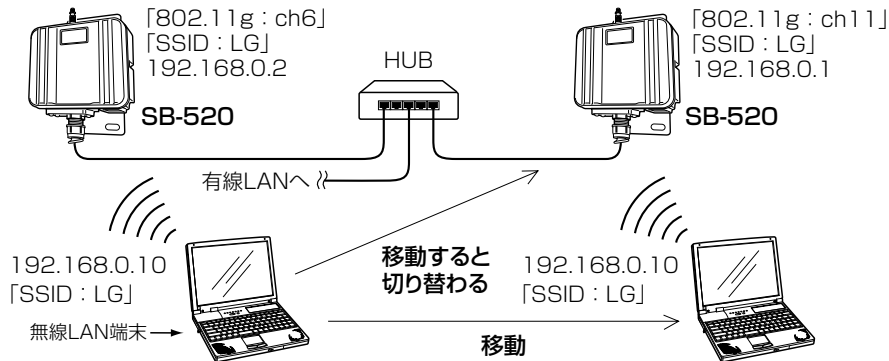
本製品の保守などで、無線通信機能を停止させるとき設定します。

1 おもな機能について

4. ローミング機能について

本製品を有線LAN上に、無線伝送エリアが重なるように複数設置することで、無線LAN端末は移動しながら複数の無線伝送エリアにまたがった通信が可能になるため、無線伝送エリアを拡大できます。

ローミング機能を使用する場合は、「Access Point」モードに変更してください。



【ローミング機能をご使用になるときの注意】

- ◎ 出荷時や全設定初期化時は、本製品のDHCPサーバー機能(☞P16、P35)は、「しない」に設定されています。本製品と同じネットワーク上に、DHCPサーバーが複数存在すると、IPアドレスが重複して不測の事態になりますので、DHCPサーバー機能の使用にはご注意ください。
- ◎ 無線LAN端末は、[IEEE802.11b]規格、および[IEEE802.11g]規格の無線内蔵型、および弊社製無線LANカードやWIRELESS LAN UNIT(☞P83)を装着してご使用ください。
- ◎ 本製品が無線通信で利用できるチャンネル(☞P46)は、01CH～13CHです。
- ◎ 移動する無線伝送エリア内では、すべての無線LAN端末とローミング機能で使う本製品の[SSID](☞P45)や「暗号化方式」(☞P51)は、すべて同じ設定値にしてください。
[SSID]や「暗号化方式」が異なるとローミングできません。
- ◎ ローミング機能とルーティングモード(☞P13、P17)は、併用できません。
ルーティングモードの場合、本製品に設定された本体IPアドレスのネットワーク部が1台ごとに異なるため、ローミング機能は使用できません。
- ◎ 電波干渉を避けるため、電波の利用状況や最適な設置場所の選定は、サイトサーベイ機能(☞P10、P69、P70)で表示される結果を参考にしてください。

5. 暗号化方式について

「WEP RC4」、「OCB AES」、「TKIP」、「AES」の暗号化方式から選択できます。

「TKIP」方式と「AES」方式は、無線ブリッジ接続機能による通信には使用できません。

無線アクセスポイント機能による通信では、すべての暗号化方式が使用できます。

「Access Point」モードに設定して、無線ブリッジ接続と併用するときは、「WEP RC4」方式、または「OCB AES」方式でご使用ください。

※ 通信相手と暗号化方式や暗号鍵(キー)の設定が異なるときは、通信できません。

※ 暗号化方式の設定について詳しくは、本書51ページをご覧ください。

6. スパニングツリー機能について

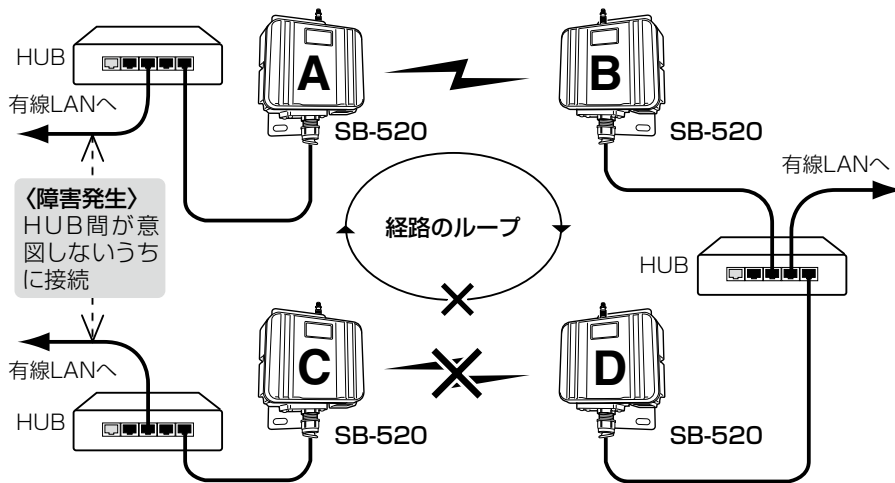
経路のループを検出し、パケットが無限に循環するのを回避して、最適な経路を作成する機能です。

下記のネットワーク例で、スパニングツリー機能を本製品(図:A~D)に設定した場合、有線LAN同士の意図しない接続(図:A-C間)が起こったとき、経路のループを検出して重複する経路のうち優先度の低い方(例、図:C-D間)を遮断します。

経路を遮断することで、ネットワークの正常な稼働が保たれます。

※スパニングツリー機能は、本製品すべて(図:A~D)に設定する必要があります。

※スパニングツリー機能の設定例などについて詳しくは、本書27ページをご覧ください。



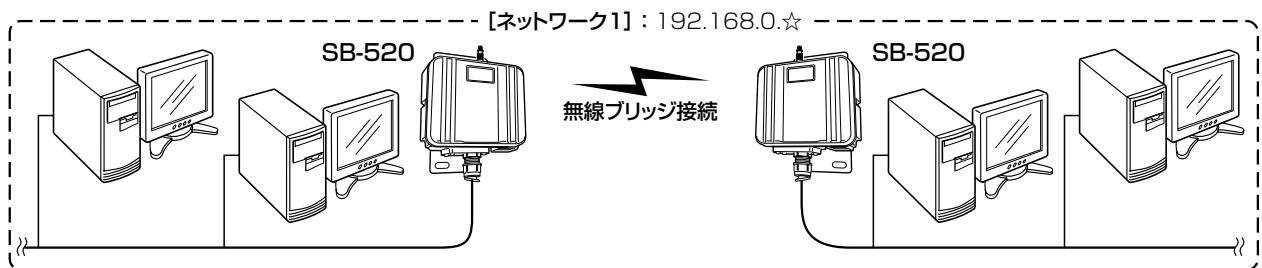
※説明では、内蔵アンテナを使用し、SA-4を省略しています。

7. ルーティング機能について

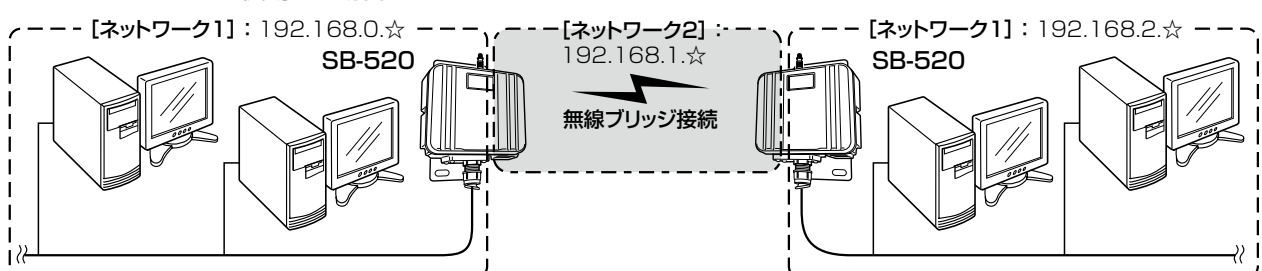
ルーティングモードを使用すると、無線LANと有線LANのネットワークグループを別々に構成でき、それらのネットワークグループ間をルーティングできます。(P17)

※下記の図は、ルーティングモードを使用しない場合(上段)と使用する場合(下段)の例です。

ルーティングモードを使用しない場合



ルーティングモードを使用する場合



※IPアドレスの「ホスト部」は、☆で表記しています。
説明では、内蔵アンテナを使用し、SA-4、HUBを省略しています。

1 おもな機能について

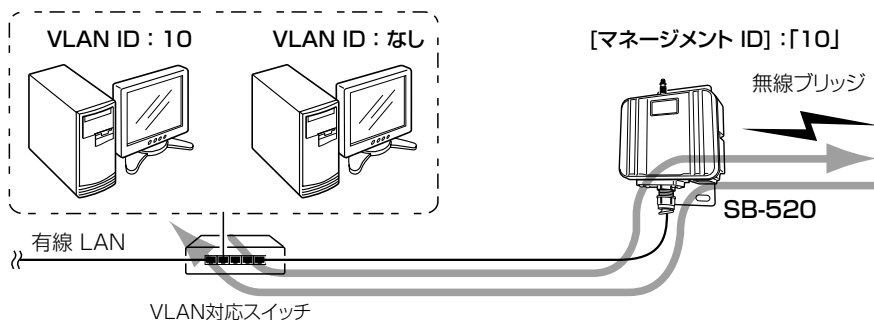
8. VLAN機能について

本製品をルーティングモード(☞P13、P17)で使用する場合は、VLAN機能が設定されていても無効になります。同じ[マネージメントID]で使用するネットワークグループ中に管理者を置く場合は、本書29ページに記載の方法を併せて使用できます。

【無線ブリッジ接続の場合】

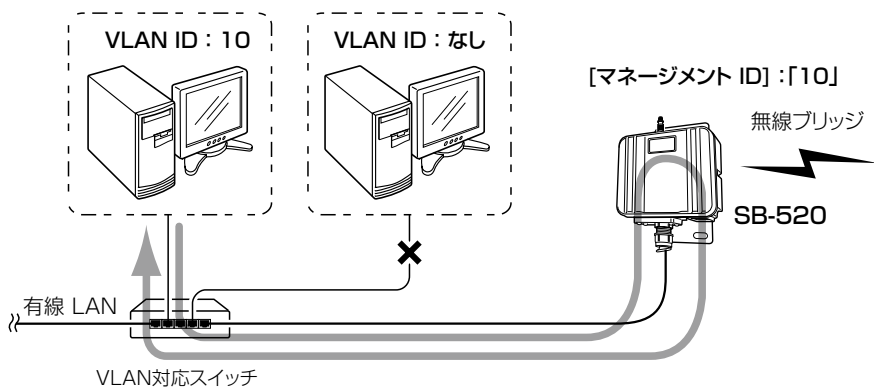
(説明では、内蔵アンテナを使用し、SA-4を省略しています。)

[VLAN ID]の有無に関係なく、すべてのパケットが無線ブリッジ接続で通信できます。



【本製品にアクセスする場合】

本製品の[マネージメントID] (例: 10)と同じ番号の[VLAN ID] (例: 10)に設定されたパケットだけが、本製品の設定画面などに直接アクセスできます。



この章では、
本製品のおもな機能について、その設定手順を説明しています。

1. DHCPサーバー機能を使用するには	16
2. 無線LANと有線LANのあいだをルーティングするには	17
■ ルーティングの設定例	17
3. [WEP RC4/OCB AES]暗号化を設定するには	20
■ 暗号鍵(キー)の入力について	20
■ 16進数で暗号鍵(キー)を入力するには	21
■ ASCII文字で暗号鍵(キー)を入力するには	22
■ ASCII文字→16進数変換表	23
■ 暗号鍵(キー)値の設定例	23
■ 暗号鍵(キー)を生成するには	24
4. [WPA-PSK(TKIP)/(AES)]暗号化を設定するには	25
■ 鍵(キー)を入力するには	25
5. [IEEE802.11b]規格の通信を制限するには	26
6. スパニングツリー機能を使用するには	27
7. 設定画面へのアクセスを制限するには	29

2 おもな機能の設定について

1. DHCPサーバー機能を使用するには

DHCPサーバー機能を使用するときは、下記の手順でDHCPサーバー機能と自動割り当て開始IPアドレスを設定してください。

※本製品のネットワーク上にDHCPサーバが存在するときは、必要ありません。

※下記の設定例は、ルーティングモード(※P13、P17)を使用しない場合の設定例です。

ルーティングモードと併せて使用する場合は、[ネットワーク2]側のDHCPサーバー機能を設定します。

※自動割り当て開始IPアドレスの[ネットワーク部(例: 192.168.0.)]が、本製品のIPアドレスのネットワーク部と同じになるように設定してください。

※設定後は、本製品のDHCPサーバからIPアドレスを自動的に取得できるように、有線または無線LAN端末のIPアドレス設定を変更してください。

【設定のしかた】

②クリック

①クリック

⑤クリック

③クリック

④変更する

	ネットワーク1	ネットワーク2
DHCPサーバー機能を使用	<input checked="" type="radio"/> しない <input checked="" type="radio"/> する	<input checked="" type="radio"/> しない <input type="radio"/> する
割り当て開始IPアドレス	192.168.0.10	192.168.1.10
割り当て個数	10 個	10 個
サブネットマスク	255.255.255.0	255.255.255.0
リース期間	72 時間	72 時間
ドメイン名		
デフォルトゲートウェイ		
プライマリDNSサーバー		
セカンダリDNSサーバー		
プライマリWINSサーバー		
セカンダリWINSサーバー		

静的DHCPサーバー設定

登録の追加			
MACアドレス	IPアドレス	ネットワーク1	ネットワーク2
<input type="text"/>	<input type="text"/>	<input type="button" value="追加"/>	<input type="button" value="追加"/>

現在の登録

MACアドレス	IPアドレス	ネットワーク1	ネットワーク2
<input type="text"/>	<input type="text"/>		

[ルーティングモードを使用]欄(※P17)で、チェックマークを入れない場合は、無効です。

【DHCPサーバー機能について】

本製品のDHCPサーバー機能を有効にすると、パソコンが本製品に接続したときに、本製品からIPアドレスを自動的に取得できます。

本製品を既存のLANと接続する場合、本製品がパソコンに自動で割り当てるIPアドレスの範囲が、パソコンなどのネットワーク機器に固定で割り当てたIPアドレスと重複しないように設定してください。

2. 無線LANと有線LANのあいだをルーティングするには

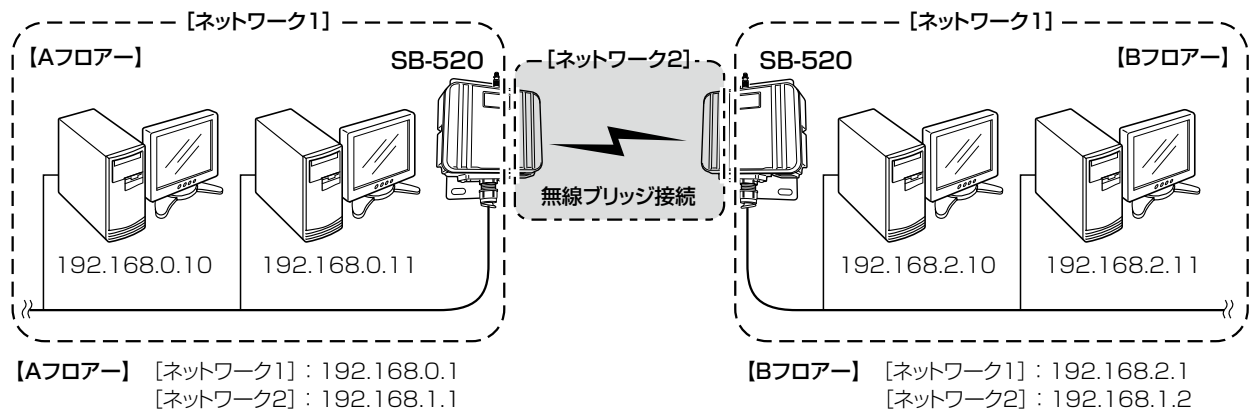
ルーティングモードを使用して、無線LANと有線LANのネットワークグループを別々に構成するための設定手順について、下記の図を例に説明します。

※無線ブリッジ接続の設定は、完了しているものとして説明しています。

■ ルーティングの設定例

次のネットワーク構成を例に、経路を動的に作成する場合と静的に作成する場合の設定例を説明します。

※無線ブリッジ接続の設定は、完了しているものとして説明しています。



※説明では、内蔵アンテナを使用し、SA-4、HUBを省略しています。

【Aフロアー】側：ルーティングモードとIPアドレスの設定

[フロアーA]側の[ネットワーク1]と[ネットワーク2]の設定します。

※本製品のDHCPサーバー機能を使用しない場合を例としています。

この場合、パソコンには、デフォルトゲートウェイとして、「192.168.0.1」を設定してください。

①クリック → ネットワーク設定 | LAN側IP | DHCP | ブリッジ | RIP | ルーティング |

④クリック → 無線設定 | 登録 | 取消 | 登録して再起動

②クリック → システム設定 | 本体名称 | VLAN設定 | ルーティングモード設定

③入力する → IPアドレス設定

	ネットワーク1	ネットワーク2
IPアドレス	192.168.0.1	192.168.1.1
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ		

※ネットワーク2側の設定はルーティングモード時のみ有効。

再起動が完了(約30秒)するまで、クリックしても戻りません。

↓

本体を再起動しています。
本体の起動を確認後、[Back]をクリックしてください。

⑤クリック

2 おもな機能の設定について

2. 無線LANと有線LANのあいだをルーティングするには

■ ルーティングの設定例(つづき)

【Bフロアー】側：ルーティングモードとIPアドレスの設定

前ページの図を例に、[フロアーB]側の[ネットワーク1]と[ネットワーク2]の設定します。

※本製品のDHCPサーバー機能を使用しない場合を例としています。

この場合、パソコンには、デフォルトゲートウェイとして、「192.168.2.1」を設定してください。

①クリック → ネットワーク設定

④クリック → 登録して再起動

②クリック → ルーティングモード設定

③入力する → IPアドレス設定

	ネットワーク1	ネットワーク2
IPアドレス	192.168.2.1	192.168.1.2
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ		

※ネットワーク2側の設定はルーティングモード時のみ有効。

経路を静的に作成する場合の設定

【設定のしかた】：[フロアーA]側

※経路を動的に作成する場合は、次ページの設定をご覧ください。

①クリック → ネットワーク設定

②クリック → ルーティング

④クリック → スタティックルーティング設定

③入力する → 登録の追加

⑤確認する → 現在の登録

宛先	サブネットマスク	ゲートウェイ
192.168.2.0	255.255.255.0	192.168.1.2

宛先	サブネットマスク	ゲートウェイ
192.168.2.0	255.255.255.0	192.168.1.2

2. 無線LANと有線LANのあいだをルーティングするには

■ ルーティングの設定例

経路を静的に作成する場合の設定(つづき)

【設定のしかた】:[フロアーB]側

①クリック

②クリック

④クリック

③入力する

⑤確認する

インターフェース リスト			
インターフェース	IPアドレス	サブネットマスク	
kse0	192.168.0.1	255.255.255.0	

スタティックルーティング設定			
登録の追加			
宛先	サブネットマスク	ゲートウェイ	
192.168.0.0	255.255.255.0	192.168.1.1	
追加			
現在の登録			
宛先	サブネットマスク	ゲートウェイ	
192.168.0.0	255.255.255.0	192.168.1.1	
削除			

経路を動的に作成する場合の設定

【設定のしかた】

[フロアーA]と[フロアーB]側の「RIP」画面に下記を設定します。

◎ [RIP設定] :「RIP」

◎ [RIP動作] :「受信も送信も行う」

※ 経路を静的に作成する場合は、前ページの設定をご覧ください。

②クリック

①クリック

④クリック

③選択する

RIP設定		
	ネットワーク1	ネットワーク2
RIP設定	RIP	RIP
RIP動作	受信も送信も行う	受信も送信も行う
認証キー		

再起動が完了(約30秒)するまで、
クリックしても戻りません。

本体を再起動しています。
本体の起動を確認後、[Back]をクリックしてください。

⑤クリック

2 おもな機能の設定について

3. [WEP RC4/OCB AES]暗号化を設定するには

[WEP RC4/OCB AES]の暗号鍵(キー)による設定は、次のとおりです。

- ◎ 16進数で暗号鍵(キー)を直接入力する(☞P21)
- ◎ ASCII文字で暗号鍵(キー)を直接入力する(☞P22)
- ◎ [キージェネレーター]に入力した文字列から暗号鍵(キー)を生成する(☞P24)

■ 暗号鍵(キー)の入力について

[暗号化方式]と[入力モード]の設定によって、暗号鍵(キー)に入力する桁数および文字数が、下記のように異なります。

ネットワーク認証		暗号化方式	入力モード	
オープンシステム	共有キー		16進数(HEX)	ASCII文字
○	○	WEP RC4 64(40)ビット	10桁	5文字(半角)
○	○	WEP RC4 128(104)ビット	26桁	13文字(半角)
○	○	WEP RC4 152(128)ビット	32桁	16文字(半角)
○	×	OCB AES 128(128)ビット	32桁	16文字(半角)

【不正アクセス防止のアドバイス】

本製品に設定する暗号鍵(WEPキー/Pre-Shared Key)は、容易に推測されないものにしてください。
数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵を変更すると有効です。

【通信する相手側の設定について】

通信する相手のワイヤレス LAN BRIDGEや無線LAN端末にも同じ暗号鍵(キー)に設定するとアクセスできます。
通信相手間で[キーインデックス]が異なる場合でも、暗号鍵(キー)は、相手と同じ番号のテキストボックスに、同じ暗号鍵(キー)を設定してください。
※通信相手間で暗号鍵(キー)の内容が異なると通信できません。

【キージェネレーターについて】

入力モードが、「16進数」(出荷時の設定)のときに使用できます。
任意の文字列を入力すると、暗号鍵(キー)を各キー番号のテキストボックスに自動生成できます。
各キー番号のテキストボックスに生成される桁数、および文字数は、選択する[暗号化方式]によって異なります。
※[キージェネレーター]は、弊社以外の機器と互換性はありません。

【OCB AES暗号化方式のネットワーク認証について】

「OCB AES」暗号化方式を設定するときは、「オープンシステム」認証を選択してください。
※「オープンシステム・共有キー」認証を選択しても、「オープンシステム」認証が登録されます。

3. [WEP RC4/OCB AES]暗号化を設定するには(つづき)

■ 16進数で暗号鍵(キー)を入力するには

出荷時や全設定初期化時、暗号化は設定されていません。

次の条件で設定する場合を例に説明します。

- ◎ [ネットワーク認証]:「オープンシステム・共有キー」(出荷時の設定)
- ◎ [暗号化方式] :「WEP RC4 128(104)」ビット
- ◎ [キーインデックス]:「1」(出荷時の設定)
- ◎ [入力モード] :「16進数」(出荷時の設定)
- ◎ [WEPキー 1] :「0~9」、および「a~f(またはA~F)」を使用して、26桁を入力

※「暗号鍵(キー)の入力について」(P20)、「暗号鍵(キー)の設定例」(P23)と併せてご覧ください。

【設定のしかた】

②クリック → 暗号化

①クリック → 無線設定

④クリック → ネットワーク認証

⑥クリック → キージェネレーター

③選択する → オープンシステム・共有キー

⑤入力する → 16進数

【ご参考】
IEEE802.1X認証するときは、設定が必要です。
この場合、[WEPキー]は設定できません。

出荷時の設定であることを確認します。

再起動が完了(約30秒)するまで、
クリックしても戻りません。

↓

本体を再起動しています。
本体の起動を確認後、[Back]をクリックしてください。

⑦クリック → [Back]

【不正アクセス防止のアドバイス】
本製品に設定する暗号鍵(WEPキー/Pre-Shared Key)は、容易に推測されないものにしてください。
数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵を変更すると有効です。

2 おもな機能の設定について

3. [WEP RC4/OCB AES]暗号化を設定するには(つづき)

■ ASCII文字で暗号鍵(キー)を入力するには

出荷時や全設定初期化時、暗号化は設定されていません。

次の条件で設定する場合を例に説明します。

- ◎ [ネットワーク認証]:「オープンシステム・共有キー」(出荷時の設定)
- ◎ [暗号化方式] :「WEP RC4 128(104)」ビット
- ◎ [キーインデックス]:「1」(出荷時の設定)
- ◎ [入力モード] :「ASCII文字」
※「ASCII文字→16進数変換表」(P23)と併せてご覧ください。
- ◎ [WEPキー 1] :「LANWAVEMASTER」
※「暗号鍵(キー)の入力について」(P20)と併せてご覧ください。

【設定のしかた】

再起動が完了(約30秒)するまで、
クリックしても戻りません。

再起動が必要な項目が変更されています。

出荷時の設定であることを確認します。

【ご参考】
IEEE802.1X認証するときは、設定
が必要です。
この場合、[WEPキー]は設定でき
ません。

再起動が完了(約30秒)するまで、
クリックしても戻りません。

本体を再起動しています。
本体の起動を確認後、[Back]をクリックしてください。

【不正アクセス防止のアドバイス】

本製品に設定する暗号鍵(WEPキー/Pre-Shared Key)は、容易に推測されないものにしてください。
数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵を変更すると有効です。

3. [WEP RC4/OCB AES]暗号化を設定するには(つづき)

■ ASCII文字→16進数変換表

相手が指定する[入力モード]で暗号鍵(キー)を設定できない場合は、下記の変換表を参考に指示された暗号鍵(キー)に対応する記号や英数字で入力してください。

[例] 16進数入力で「4153434949」(10桁)を設定している場合、ASCII文字では、「ASCII」(5文字)になります。

ASCII文字	!	"	#	\$	%	&	'	()	*	+	,	-	.	/	
16進数	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f
ASCII文字	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
16進数	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f
ASCII文字	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16進数	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f
ASCII文字	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
16進数	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f
ASCII文字	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16進数	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f
ASCII文字	p	q	r	s	t	u	v	w	x	y	z	{		}	~	
16進数	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	

■ 暗号鍵(キー)値の設定例

[WEP RC4 128(104)]ビットの暗号化方式を例に、暗号鍵(キー)を16進数(26桁)で直接入力する場合を説明します。

[例] 下記のように入力します。

キーインデックス「2」:[48-6F-74-73-70-6F-74-41-63-63-65-73-73]

キーインデックス「3」:[57-41-56-45-4D-41-53-54-45-52-4C-41-4E]

(※「- (ハイフン)」の入力を省略しても設定できます。)

1. キーインデックス「2」のWEPキー(値)が同じなので通信できます。

	本製品側	無線LAN端末側
キーインデックス	2	2
WEPキー	入力モード：16進数	入力モード：16進数
1	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
2	48-6f-74-73-70-6f-74-41-63-63-65-73-73	48-6f-74-73-70-6f-74-41-63-63-65-73-73
3	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
4	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

2. キーインデックス「2」と「3」のWEPキー(値)が同じなので通信できます。

	本製品側	無線LAN端末側
キーインデックス	2	3
WEPキー	入力モード：16進数	入力モード：16進数
1	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
2	48-6f-74-73-70-6f-74-41-63-63-65-73-73	48-6f-74-73-70-6f-74-41-63-63-65-73-73
3	57-41-56-45-4D-41-53-54-45-52-4C-41-4E	57-41-56-45-4D-41-53-54-45-52-4C-41-4E
4	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

3. キーインデックス「2」と「3」のWEPキー(値)が異なるので通信できません。

	本製品側	無線LAN端末側
キーインデックス	2	3
WEPキー	入力モード：16進数	入力モード：16進数
1	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
2	48-6f-74-73-70-6f-74-41-63-63-65-73-73	57-41-56-45-4D-41-53-54-45-52-4C-41-4E
3	57-41-56-45-4D-41-53-54-45-52-4C-41-4E	48-6f-74-73-70-6f-74-41-63-63-65-73-73
4	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

【不正アクセス防止のアドバイス】

本製品に設定する暗号鍵(WEPキー/Pre-Shared Key)は、容易に推測されないものにしてください。
数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵を変更すると有効です。

2 おもな機能の設定について

3. [WEP RC4/OCB AES]暗号化を設定するには(つづき)

■ 暗号鍵(キー)を生成するには

出荷時や全設定初期化時、暗号化は設定されていません。

次の条件で設定する場合を例に説明します。

- ◎ [ネットワーク認証] : 「オープンシステム・共有キー」(出荷時の設定)
- ◎ [暗号化方式] : 「WEP RC4 128(104)」ビット
- ◎ [キージェネレーター] : 「SB520」
- ◎ [キーインデックス] : 「1」(出荷時の設定)
- ◎ [入力モード] : 「16進数」(出荷時の設定)

【設定のしかた】

②クリック

①クリック

⑤クリック

⑦クリック

③選択する

④入力する

⑥確認する

再起動が完了(約30秒)するまで、
クリックしても戻りません。

本体を再起動しています。

本体の起動を確認後、**[Back]** をクリックしてください。

⑧クリック

【不正アクセス防止のアドバイス】

本製品に設定する暗号鍵(WEPキー/Pre-Shared Key)は、容易に推測されないものにししてください。

数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵を変更すると有効です。

4. [WPA-PSK(TKIP)/(AES)]暗号化を設定するには

[WPA-PSK(TKIP)/(AES)]の共有鍵(キー)による設定は、次の2とおりです。

- ◎ 16進数で64桁を入力する
- ◎ ASCII文字で8～63文字を入力する

■ 鍵(キー)を入力するには

出荷時や全設定初期化時、暗号化は設定されていません。

次の条件で設定する場合を例に説明します。

- ◎ [ネットワーク認証] : [WPA-PSK]
- ◎ [暗号化方式] : [TKIP]
- ◎ [PSK(Pre-Shared Key)] : [wavemaster](ASCII文字の場合)
- ◎ [キー更新間隔] : [120]分(出荷時の設定)

【設定のしかた】

②クリック → ネットワーク設定 | 無線LAN | **暗号化** | MACフィルタリング | 無線ブリッジ |

①クリック → 無線設定

⑥クリック → システム設定

④選択する → ネットワーク認証

③選択する → PSK(Pre-Shared Key)

⑤入力する → キー更新間隔

【ご参考】
WPA認証するときは、設定が必要です。
この場合、[PSK(Pre-Shared Key)]は設定できません。

再起動が完了(約30秒)するまで、
クリックしても戻りません。

本体を再起動しています。
本体の起動を確認後、[Back]をクリックしてください。

⑦クリック → [Back]

【不正アクセス防止のアドバイス】
本製品に設定する暗号鍵(WEPキー/Pre-Shared Key)は、容易に推測されないものにしてください。
数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵を変更すると有効です。

2 おもな機能の設定について

5. [IEEE802.11b]規格の通信を制限するには

[IEEE802.11g]規格と[IEEE802.11b]規格で本製品にアクセスする無線LAN端末が混在する環境で、[IEEE802.11g]規格との通信を優先または、[IEEE802.11g]規格との通信だけに限定することで、混信による通信速度の低下を防止および緩和できます。

※[11g保護機能]の設定によって、図のような通信ができます。

※「無線LAN」メニューにある「無線LAN」画面で設定できます。

[11g保護機能]の設定が「有効」のとき(出荷時の設定)

※IEEE802.11b規格との混在により、IEEE802.11g規格の速度が低下するのを防止でき、極端に通信速度が遅い場合にだけ効果があります。



[11g保護機能]の設定が「無効」のとき



[11g保護機能]の設定が「g専用」のとき



※説明では、内蔵アンテナを使用し、SA-4を省略しています。

6. スパニングツリー機能を使用するには

スパニングツリー機能の設定について、下記の図を例に説明します。

下記に示す接続障害例は、本製品[A]のHUBと本製品[C]のHUBが意図しないうちに接続されてしまったネットワークで、本製品のすべてにスパニングツリー機能が設定されているため、本製品[C]-[D]間の無線ブリッジ接続を停止して、同一ネットワークグループ内の経路ループを阻止している状態の図です。

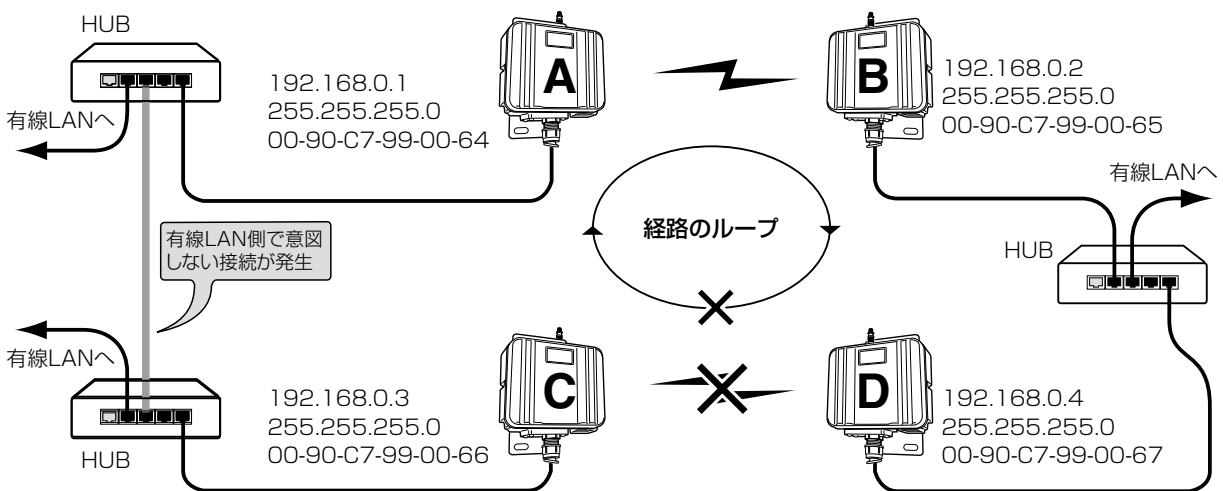
※本製品[A~D]の中で、[D]の[MACアドレス]が最小とします。

[MACアドレス]は、「情報表示」メニューの「ネットワーク」画面に表示されています。

図中では、各機器(A~D)の設定値を上から[IPアドレス]、[サブネットマスク]、[BSSID]の順に記載しています。

説明では、内蔵アンテナを使用し、SA-4を省略しています。

【設定のしかた】



Step1.本製品[A]-本製品[B]間の設定

- ① 本体IPアドレスとサブネットマスクを設定(☞P34)します。
 - ◎ 本製品[A]: 192.168.0.1/255.255.255.0
 - ◎ 本製品[B]: 192.168.0.2/255.255.255.0
 - ② 通信相手と同じ[チャンネル]を設定(☞設定ガイド)します。(例: 11 (2462MHz))
 - ③ 通信相手の[BSS ID]を自分の機器に登録(☞設定ガイド)します。
 - ◎ 本製品[A]には、「例: 00-C7-90-99-00-65」を登録します。
 - ◎ 本製品[B]には、「例: 00-C7-90-99-00-64」を登録します。
- ※ 本製品[A]と本製品[B]の[通信速度]の設定は、「自動」とします。

Step2.本製品[C]-本製品[D]間の設定

- ① 本体IPアドレスとサブネットマスクを設定(☞P34)します。
 - ◎ 本製品[C]: 192.168.0.3/255.255.255.0
 - ◎ 本製品[D]: 192.168.0.4/255.255.255.0
 - ② 通信相手と同じ[チャンネル]を設定(☞設定ガイド)します。(例: 6 (2437MHz))
 - ③ 通信相手の[BSS ID]を自分の機器に登録(☞設定ガイド)します。
 - ◎ 本製品[C]には、「例: 00-C7-90-99-00-67」を登録します。
 - ◎ 本製品[D]には、「例: 00-C7-90-99-00-66」を登録します。
- ※ 本製品[C]と本製品[D]の[通信速度]の設定は、「自動」とします。

2 おもな機能の設定について

6. スパニングツリー機能を使用するには(つづき)

Step3.スパニングツリー機能を設定する

①クリック → ネットワーク設定 | LAN側IP | DHCP | **ブリッジ** | RIP | ルーティング |

②クリック → 無線設定 | 登録 | 取消 | 登録して再起動

④クリック → システム設定 | **ブリッジ設定**

③クリック → 情報表示

スパニングツリー機能を使用		<input type="radio"/> しない	<input checked="" type="radio"/> する
ブリッジ優先度(Bridge Priority)		32768	
エージングタイム(Aging Time)		300 秒	
マックスエイジ(Max Age)		20 秒	
ハロータイム>Hello Time)		2 秒	
転送遅延(Forward Delay)		15 秒	
パスコスト(Path Cost)	有線LAN	19	
	無線LAN	100	
ポート優先度(Port Priority)	有線LAN	128	
	無線LAN	128	



再起動が完了(約30秒)するまで、
クリックしても戻りません。

本体を再起動しています。

本体の起動を確認後、**[Back]**をクリックしてください。

⑤クリック

ご参考に-優先度について

ブリッジ接続された本製品の経路優先度は、ブリッジ優先度→パスコスト→ポート優先度の順に決定され、各設定値の小さい方が優先されます。

ご使用のネットワークの形態によって、これらの設定値で優先度を設定してください。

本書での接続例の場合、ブリッジ優先度は、本製品[A~D]すべてが同じ設定値「32768(出荷時の設定)」のため、MACアドレスの小さい本製品[D]を優先します。

本製品[D]のパスコストは、[無線LAN]の設定値「100(出荷時の設定)」より[有線LAN]の設定値「19(出荷時の設定)」のほうが小さいため、有線LANの経路が優先され、無線LANの通信を停止させます。

ポート優先度は、この場合、[有線LAN]と[無線LAN]の設定値が同じ設定値「128(出荷時の設定)」のため比較の対象にはなりません。

7. 設定画面へのアクセスを制限するには

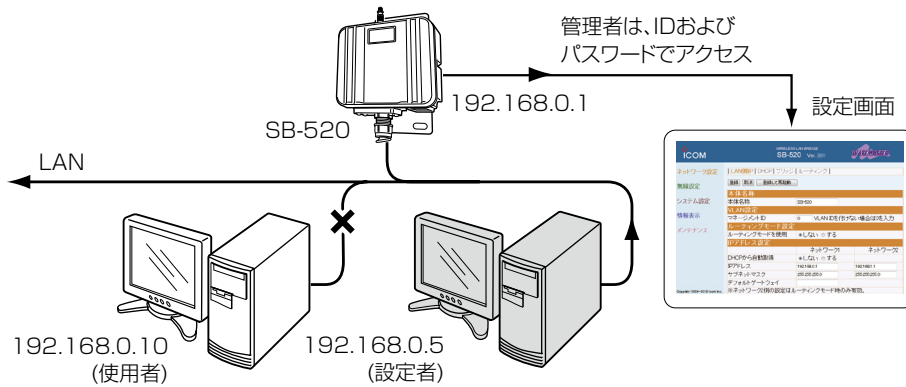
設定者用の[管理者パスワード]、および[管理者IP]を設定することで、設定者以外がWWWブラウザから本製品の設定画面にアクセスできないようにします。

※ [管理者IPアドレス]は、設定者が使用するパソコンに固定IPアドレスを設定してください。

設定すると、登録したIPアドレス以外のパソコンは、本製品の設定画面にアクセスできなくなります。

※説明では、内蔵アンテナを使用し、SA-4を省略しています。

【設定のしかた】

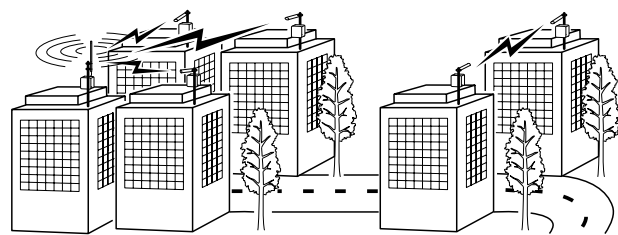


	ネットワーク設定	本体管理 時計 SYSLOG SNMP
④クリック	無線設定	登録 取消
		登録後は、[ユーザー名]と[パスワード]を求める画面を表示します。
①クリック	システム設定	管理者ID設定
	情報表示	管理者ID admin
②入力する	メンテナンス	管理者パスワード
		確認入力
③入力する		管理者IP設定
		管理者IP1 192.168.0.5
		管理者IP2
		管理者IP3
		管理者IP4
		管理者IP5
		管理者IP6
		管理者IP7
		管理者IP8

【不正アクセス防止のアドバイス】

本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。

数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものにし、さらに定期的にパスワードを変更するなどが有効です。



この章では、

各メニューの設定画面について説明します。

※「メンテナンス」メニューについては、「保守について」(P4章)で、操作方法と併せて説明しています。

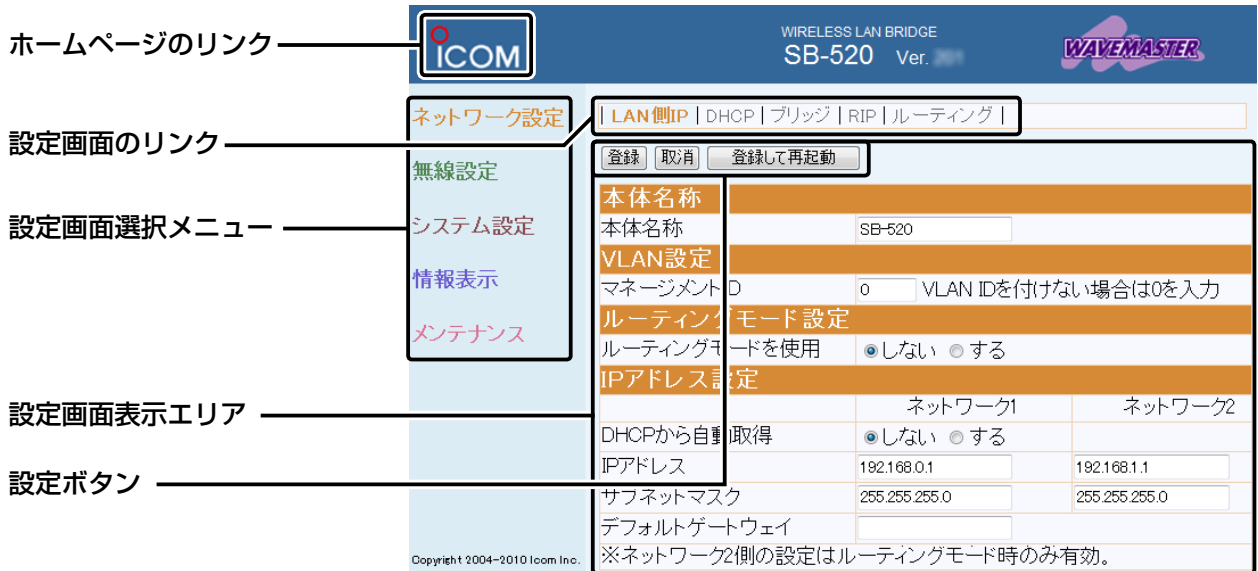
※設定画面は、各メニューとして用途ごとに分類されていますので、「設定画面の構成について」(P81)と併せてご覧ください。

1. 設定画面の名称と機能について	32
2. 「ネットワーク設定」メニュー	33
■ 本体名称	33
■ VLAN設定	33
■ ルーティングモード設定	33
■ IPアドレス設定	34
■ DHCPサーバー設定	35
■ 静的DHCPサーバー設定	37
■ ブリッジ設定	38
■ RIP設定	40
■ インターフェース リスト	41
■ IP経路情報	41
■ スタティックルーティング設定	42
3. 「無線設定」メニュー	43
■ BSSID	43
■ 無線LAN設定	44
■ 暗号化設定	51
■ RADIUS設定	56
■ WEPキー	57
■ 無線端末間通信設定	57
■ MACアドレスフィルタリング設定	58
■ BSSID	59
■ ステーションリスト	59
■ 登録済み端末リスト	60
4. 「システム設定」メニュー	61
■ 管理者ID設定	61
■ 管理者IP設定	62
■ 自動時計設定	63
■ 内部時計設定	64
■ SYSLOG設定	64
■ SNMP設定	65
5. 「情報表示」メニュー	66
■ インターフェース リスト	66
■ インターフェース情報	66
■ 本体MACアドレス	66
■ 無線UNIT	67
■ パケット情報	67
■ 端末情報	68
■ サイトサーベイ	69
■ サイトサーベイの調査例について	70
■ SYSLOG	70

3 設定画面について

1. 設定画面の名称と機能について

本製品の設定画面の名称と各画面に含まれる項目を説明します。
設定画面の構成について詳しくは、本書57ページをご覧ください。



ホームページのリンク

インターネットに接続できる環境で、アイコンをクリックすると、弊社のホームページを閲覧できます。

設定画面のリンク

クリックした名前の画面を[設定画面表示エリア]に表示します。

設定画面選択メニュー

各メニューのタイトル上にマウスポインターを合わせ、そのメニュー名をクリックすると、そのメニューに含まれる画面名を[設定画面のリンク]の部分に表示します。

設定画面表示エリア

[設定画面のリンク]からクリックした名前の画面を表示します。

設定ボタン

設定した内容の登録や取り消しをします。
<登録>をクリックして、「再起動が必要な項目が変更されています。」と表示されるとき、<登録して再起動>をクリックすると、画面上で確定された内容が再起動後に有効となります。
再起動中は、下記の画面を表示します。

本体を再起動しています。
本体の起動を確認後、[Back]をクリックしてください。

- ※ 再起動が完了(約30秒)するまで、[Back]と表示された文字の上にマウスポインターを移動してクリックしても、設定画面に戻りませんので、しばらくしてから再度クリックしてください。
- ※ 表示画面によって、表示されるボタンの種類や位置が異なります。

2. 「ネットワーク設定」メニュー

■ 本体名称

「ネットワーク設定」-「LAN側IP」

本製品の名称を設定します。

本体名称	
本体名称	SB-520

本体名称…………… 「Telnet」で本製品に接続したとき、ここで設定した本体名称を表示します。
 (出荷時の設定: SB-520)
 ※アルファベットで始まる半角英数字(a～z, A～Z, 0～9, -)を31文字以内で設定します。
 なお、それ以外の文字は、登録できない場合があります。

■ VLAN設定

「ネットワーク設定」-「LAN側IP」

VLAN機能(※P14)についての設定です。

VLAN設定	
マネージメントID	0 VLAN IDを付けたい場合は0を入力

マネージメントID …………… 本製品に設定された同じID番号を持つネットワーク上の機器からのアクセスだけを許可できます。
 (出荷時の設定: 0)
 設定できる範囲は、「0～4094」です。
 ※VLAN IDを使用しないネットワークから本製品にアクセスするときは、「0」を設定します。
 ※不用意に設定すると、本製品の設定画面にアクセスできなくなりますのでご注意ください。
 ※本製品をルーティングモードで使用する場合、VLAN機能の設定は、無効になります。
 ※無線ネットワークのVLAN IDは、「無線設定」メニューの「無線LAN」画面にある[VLAN ID]欄(※P45)で設定できます。

■ ルーティングモード設定

「ネットワーク設定」-「LAN側IP」

無線LANと有線LAN間のルーティングを設定します。

ルーティングモード設定	
ルーティングモードを使用	<input checked="" type="radio"/> しない <input type="radio"/> する

ルーティングモードを使用…………… ルーティングモードで使用する時設定します。
 (出荷時の設定: しない)
 ※ルーティングモードで使ったときの透過プロトコルは、IPv4だけです。
 ※「する」を設定したときは、本製品の無線LANネットワークを有線LANネットワークと異なるサブネットとして構成できます。(※P13、P17)
 ※ルーティングモードを使用すると、不要なブロードキャストなどのトラフィックを抑えた通信ができます。

3 設定画面について

2. 「ネットワーク設定」メニュー(つづき)

■ IPアドレス設定

「ネットワーク設定」-「LAN側IP」

本製品のLAN側IPアドレスを設定します。

IPアドレス設定		
	① ネットワーク1	ネットワーク2
IPアドレス	② 192.168.0.1	192.168.1.1
サブネットマスク	③ 255.255.255.0	255.255.255.0
デフォルトゲートウェイ	④	

※ネットワーク2側の設定はルーティングモード時のみ有効。

① ネットワーク1/ネットワーク2

.....

- ルーティングモードを使用しない場合
無線LANを有線LANと同じネットワーク(ネットワーク1)で構成するため、[ネットワーク2]側の列にある各欄の設定は、無効になります。
- ルーティングモードを使用する場合
無線LANを有線LANと異なるネットワーク(ネットワーク2)で構成するため、[ネットワーク2]側の列にある各欄は無線LAN側の設定、[ネットワーク1]側の列にある各欄は有線LAN側の設定になります。

② IPアドレス

- 本製品のIPアドレスを設定します。
(出荷時の設定: ネットワーク1→192.168.0.1
ネットワーク2→192.168.1.1)
※本製品の有線LANは、ルーティングモードの設定(※P13、P17)に関係なく、[ネットワーク1]側の列で設定します。

③ サブネットマスク

- 本製品のサブネットマスク(同じネットワークで使用するIPアドレスの範囲)を設定します。
(出荷時の設定: 255.255.255.0)
※本製品を現在稼働中のネットワークに接続するときなど、そのLANに合わせたサブネットマスクに変更してください。

【例:「255.255.255.248」に設定する場合】

同じネットワークで使用するIPアドレスの範囲は、「192.168.0.0～192.168.0.7」になります。
この場合、端末に割り当てできるIPアドレスの範囲は、「192.168.0.2～192.168.0.6」です。
なお、端末に割り当てできないIPアドレスは次のようになります。
「192.168.0.0」: ネットワークアドレス
「192.168.0.1」: 本製品のIPアドレス
「192.168.0.7」: ブロードキャストアドレス

④ デフォルトゲートウェイ ...

- 本製品のネットワーク部が異なる接続先と通信する場合、パケット転送先機器のIPアドレスを入力します。
※本製品の[ネットワーク1]側と同じIPアドレスは登録できません。

2. 「ネットワーク設定」メニュー(つづき)

■ DHCPサーバー設定

「ネットワーク設定」-「DHCP」

DHCPサーバー機能についての設定です。

DHCPサーバー設定			
	①	ネットワーク1	ネットワーク2
DHCPサーバー機能を使用	②	<input checked="" type="radio"/> しない <input type="radio"/> する	<input checked="" type="radio"/> しない <input type="radio"/> する
割り当て開始IPアドレス	③	192.168.0.10	192.168.1.10
割り当て個数	④	10 個	10 個
サブネットマスク	⑤	255.255.255.0	255.255.255.0
リース期間	⑥	72 時間	72 時間
ドメイン名	⑦		
デフォルトゲートウェイ	⑧		
プライマリDNSサーバー	⑨		
セカンダリDNSサーバー	⑩		
プライマリWINSサーバー	⑪		
セカンダリWINSサーバー	⑫		

① ネットワーク1/ネットワーク2

.....

◎ルーティングモードを使用しない場合

無線LANを有線LANと同じネットワーク(ネットワーク1)で構成するため、[ネットワーク2]側の列にある各欄の設定は、無効になります。

◎ルーティングモードを使用する場合

無線LANを有線LANと異なるネットワーク(ネットワーク2)で構成するため、[ネットワーク2]側の列にある各欄は無線LAN側の設定、[ネットワーク1]側の列にある各欄は有線LAN側の設定になります。

② DHCPサーバー機能を使用

DHCPサーバー機能の使用を設定します。 (出荷時の設定: しない)
 「する」に設定すると、③～⑫の設定が有効になり、本製品に有線および無線で接続している端末がTCP/IP設定を「IPアドレスを自動的に取得する」にしている場合、本製品のDHCPクライアントになります。

③ 割り当て開始IPアドレス ...

本製品に有線および無線で接続する端末へ、IPアドレスを自動で割り当てるときの開始アドレスを設定します。

(出荷時の設定: ネットワーク1→192.168.0.10
 ネットワーク2→192.168.1.10)

④ 割り当て個数

本製品が自動割り当てできるIPアドレスの個数を設定します。

(出荷時の設定: 10)

[割り当て開始IPアドレス] (③) 欄に設定されたIPアドレスから連続で自動割り当てできるIPアドレスの最大個数は、0～128(無線LANで接続する端末を含む)までです。

※128を超える分については設定できませんので、手動でクライアントに割り当ててください。

※「0」を設定したときは、自動割り当てをしません。

3 設定画面について

2. 「ネットワーク設定」メニュー

■ DHCPサーバー設定(つづき)

「ネットワーク設定」-「DHCP」

DHCPサーバー設定			
	①	ネットワーク1	ネットワーク2
DHCPサーバー機能を使用	②	<input checked="" type="radio"/> しない <input type="radio"/> する	<input checked="" type="radio"/> しない <input type="radio"/> する
割り当て開始IPアドレス	③	<input type="text" value="192.168.0.10"/>	<input type="text" value="192.168.1.10"/>
割り当て個数	④	10 個	10 個
サブネットマスク	⑤	<input type="text" value="255.255.255.0"/>	<input type="text" value="255.255.255.0"/>
リース期間	⑥	72 時間	72 時間
ドメイン名	⑦	<input type="text"/>	<input type="text"/>
デフォルトゲートウェイ	⑧	<input type="text"/>	<input type="text"/>
プライマリDNSサーバー	⑨	<input type="text"/>	<input type="text"/>
セカンダリDNSサーバー	⑩	<input type="text"/>	<input type="text"/>
プライマリWINSサーバー	⑪	<input type="text"/>	<input type="text"/>
セカンダリWINSサーバー	⑫	<input type="text"/>	<input type="text"/>

- ⑤ サブネットマスク …………… [割り当て開始IPアドレス] (③) 欄に設定されたIPアドレスに対するサブネットマスクです。
(出荷時の設定: 255.255.255.0)
- ⑥ リース期間 …………… DHCPサーバーが、ローカルIPアドレスを定期的に自動で端末に割り当てなおす期限を時間で指定します。
(出荷時の設定: 72)
設定できる範囲は、「1～9999(時間)」です。
- ⑦ ドメイン名 …………… 指定のドメイン名を設定する必要があるときは、DHCPサーバーが有線で接続する端末に通知するネットワークアドレスのドメイン名を127文字(半角英数字)以内で入力します。
- ⑧ デフォルトゲートウェイ …… [割り当て開始IPアドレス] (②) 欄のIPアドレスとネットワーク部が異なる接続先と通信する場合、パケット転送先機器のIPアドレスを入力します。
- ⑨ プライマリDNSサーバー …… DNSサーバーのアドレスが2つある場合は、優先したい方のアドレスを入力します。
入力すると、設定したDNSサーバーアドレスをDHCPクライアントに通知します。
- ⑩ セカンダリDNSサーバー …… [プライマリDNSサーバー] (⑨) 欄と同様、DNSサーバーのアドレスが2つある場合は、DNSサーバーアドレスのもう一方を入力します。
- ⑪ プライマリWINSサーバー …… Microsoftネットワークを使ってWINSサーバーを利用する場合は、WINSサーバーアドレスを入力します。
WINSサーバーのアドレスが2つある場合は、優先したい方のアドレスを入力します。
- ⑫ セカンダリWINSサーバー …… [プライマリWINSサーバー] (⑪) 欄と同様、WINSサーバーのアドレスが2つある場合は、残りの一方を入力します。

2. 「ネットワーク設定」メニュー(つづき)

■ 静的DHCPサーバー設定

「ネットワーク設定」-「DHCP」

固定IPアドレスを特定の端末に割り当てる設定です。

静的DHCPサーバー設定			
登録の追加 ①			
MACアドレス	IPアドレス	ネットワーク1	ネットワーク2
<input type="text"/>	<input type="text"/>	<input type="button" value="追加"/>	<input type="button" value="追加"/>
現在の登録 ②			
MACアドレス	IPアドレス	ネットワーク1	ネットワーク2

- ① 登録の追加 …………… 端末のMACアドレスとIPアドレスの組み合わせを登録します。
登録するときは、[ネットワーク1] 欄、または[ネットワーク2] 欄の〈追加〉をクリックします。
※本製品のDHCPサーバー機能(☞P16)を使用する場合に有効です。
※最大32個の組み合わせを登録できます。
登録するIPアドレスは、DHCPサーバー機能による割り当て範囲、および本製品のIPアドレスと重複しないように設定してください。
※ルーティングモード(☞P13、P17)を使用する場合は、[ネットワーク2] 欄の登録が有効になります。

- ② 現在の登録 …………… 登録した内容を表示します。

【登録例】

登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

現在の登録			
MACアドレス	IPアドレス	ネットワーク1	ネットワーク2
00-90-C7- <input type="text"/>	192.168.0.20	<input type="button" value="削除"/>	
00-90-C7- <input type="text"/>	192.168.1.20		<input type="button" value="削除"/>

3 設定画面について

2. 「ネットワーク設定」メニュー(つづき)

■ ブリッジ設定

「ネットワーク設定」-「ブリッジ」

スパニングツリー機能を設定します。

ブリッジ設定		
スパニングツリー機能を使用	①	<input checked="" type="radio"/> しない <input type="radio"/> する
ブリッジ優先度(Bridge Priority)	②	32768
エージングタイム(Aging Time)	③	300 秒
マックスエイジ(Max Age)	④	20 秒
ハロータイム(Hello Time)	⑤	2 秒
転送遅延(Forward Delay)	⑥	15 秒
パスコスト(Path Cost)	⑦	有線LAN 19
		無線LAN 100
ポート優先度(Port Priority)	⑧	有線LAN 128
		無線LAN 128

- ① **スパニングツリー機能を使用** 経路のループを検出し、パケットが無限に循環するのを回避して、最適な経路を作成する機能です。 (出荷時の設定: しない)
経路作成中は、本製品の[MODE]ランプが点滅します。
スパニングツリー機能を設定すると、経路障害のないときは、経路のループを検出して重複する経路のうち優先度の低い方を遮断します。
ブリッジ間で経路障害が起きると、正常時に遮断されていた経路を使用して、ネットワークの正常な稼働を保ちます。
- ② **ブリッジ優先度**…………… ブリッジで通信する本製品の優先度を決定する値で、設定値が小さいほど、優先度が高くなります。 (出荷時の設定: 32768)
設定できる範囲は「0~65535」で、一番優先度が高い本製品が、そのネットワークのルートブリッジになります。
※同じ値が設定された機器がある場合は、MACアドレスの小さい機器の優先度が高くなります。
※出荷時の設定でご使用になることを推奨します。
- ③ **エージングタイム** …………… 本製品が自動学習したMACアドレスをアドレステーブルに記憶しておく時間を指定します。 (出荷時の設定: 300)
設定できる範囲は、「15~1000000(秒)」です。
※無通信状態がこの欄に設定された時間つづくと、アドレステーブルから削除されます。
※出荷時の設定でご使用になることを推奨します。
- ④ **マックスエイジ** …………… BPDU(Bridge Protocol Data Unit)を指定します。 (出荷時の設定: 20)
設定できる範囲は、「6~40(秒)」です。
※出荷時の設定でご使用になることを推奨します。

2. 「ネットワーク設定」メニュー

■ ブリッジ設定(つづき)

「ネットワーク設定」-「ブリッジ」

- ⑤ **ハロータイム** 本製品がルートブリッジとして動作するとき、本製品からBPDU情報を送出する間隔を設定します。 (出荷時の設定:2)
設定できる範囲は、「1~10(秒)」です。
※出荷時の設定でご使用になることを推奨します。
- ⑥ **転送遅延** ネットワークの再編成中に学習したMACアドレスの有効期限を指定します。 (出荷時の設定:15)
設定できる範囲は、「4~30(秒)」です。
※出荷時の設定でご使用になることを推奨します。
- ⑦ **パスコスト** ネットワーク全体のブリッジとルートブリッジ間の優先データパスの決定に利用される値で、各ポートからルートブリッジまでの経路コストが小さいブリッジが優先されます。 (出荷時の設定:有線LAN→19
無線LAN→100)
※設定できる範囲は、「1~65536」です。
※出荷時の設定でご使用になることを推奨します。
- ⑧ **ポート優先度** ブリッジで通信する本製品のポートごとに優先度を決定する値で、設定値が小さいほど、ポート優先度が高くなります。 (出荷時の設定:有線LAN→128
無線LAN→128)
設定できる範囲は、「0~255」です。
※各ポートで同じ値が設定されている場合は、物理的なポート番号の小さい順に優先度が高くなります。
※出荷時の設定でご使用になることを推奨します。

3 設定画面について

2. 「ネットワーク設定」メニュー(つづき)

■ RIP設定

「ネットワーク設定」-「RIP」

隣接ルーターやアクセスポイントと経路情報を交換して、経路を動的に作成するときの設定です。

RIP設定		
①	ネットワーク1	ネットワーク2
RIP設定 ②	使用しない ▼	使用しない ▼
RIP動作 ③	受信のみ ▼	受信のみ ▼
認証キー ④	<input type="text"/>	<input type="text"/>

① ネットワーク1/ネットワーク2

.....

◎ルーティングモードを使用しない場合

無線LANを有線LANと同じネットワーク(ネットワーク1)で構成するため、[ネットワーク2]側の列にある各欄の設定は、無効になります。

◎ルーティングモードを使用する場合

無線LANを有線LANと異なるネットワーク(ネットワーク2)で構成するため、[ネットワーク2]側の列にある各欄は無線LAN側の設定、[ネットワーク1]側の列にある各欄は有線LAN側の設定になります。

② RIP設定

RIPの種類を選択します。 (出荷時の設定:使用しない)

◎使用しない :RIPを使用しないときの設定です。

◎RIP :RIPの「Version1」を使用します。

◎RIP2 :RIPの「Version2」を使用して、マルチキャストアドレスにパケットを送信します。

【RIP2について】

RIP2は、可変長サブネットマスクに対応していますので、イントラネット環境でも利用できます。

受信については、ブロードキャスト/マルチキャストの区別なく受け入れます。

③ RIP動作

RIPを使用する場合に有効な設定で、隣接ルーターなどの機器と経路情報を動的に交換する動作をネットワークごとに「受信のみ」、または「受信も送信も行う」から選択します。 (出荷時の設定:受信のみ)

④ 認証キー

[RIP設定](②)欄で、「RIP2」を設定している場合、そのRIP動作を認証するためのキーを入力します。

[RIP設定]欄で、「RIP」または「使用しない」を選択している場合は、設定しても無効になります。

※キーは、大文字/小文字の区別に注意して、半角31文字以内で入力します。

※認証キーの入力は、他のルーターやアクセスポイントに設定されている認証キーと同じ設定にします。

※認証キーを設定すると、「RIP」を設定しているゲートウェイと、異なる認証キーを設定している「RIP2」および、認証キーを設定していない「RIP2」ゲートウェイからのRIPパケットを破棄します。

2. 「ネットワーク設定」メニュー(つづき)

■ インターフェース リスト

「ネットワーク設定」-「ルーティング」

[IP経路情報]項目に表示された[経路]について、その詳細を表示します。

※「情報表示」メニューの「ネットワーク」画面でも確認できます。(※P66)

インターフェース リスト		
インターフェース	IPアドレス	サブネットマスク
atheros0	192.168.1.1	255.255.255.0
kse0	192.168.0.1	255.255.255.0
lo0	127.0.0.1	255.0.0.0

※上図は、ルーティングモードを使用したときの表示例です。

■ IP経路情報

「ネットワーク設定」-「ルーティング」

[IP経路情報]項目に表示された[経路]について、その詳細を表示します。

IP経路情報				
①宛先	②サブネットマスク	③ゲートウェイ	④経路	⑤作成
192.168.0.0	255.255.255.0		kse0	misc
192.168.1.0	255.255.255.0		atheros0	misc

- ① 宛先 ルーティングの対象となるパケットの宛先IPアドレスを表示します。
- ② サブネットマスク ルーティングの対象となるパケットの宛先IPアドレスに対するサブネットマスクを表示します。
- ③ ゲートウェイ ルーティングの対象となるパケットの宛先IPアドレスに対するゲートウェイを表示します。
- ④ 経路 ルーティングの対象となるパケットの宛先IPアドレスに対する転送先インターフェースを表示します。
 ◎kse0 :ルーティングモードを使用しないとき、転送先インターフェースが[ネットワーク1](有線LANと無線LAN)の場合です。
 ルーティングモードを使用するとき、転送先インターフェースが[ネットワーク1](有線LAN)の場合です。
 ◎atheros0 :ルーティングモードを使用するとき表示され、転送先インターフェースが[ネットワーク2](無線LAN)の場合です。
 ※経路の詳細は、[インターフェース リスト]項目に表示します。
- ⑤ 作成 どのように経路情報が作成されたかを表示します。
 ◎static :スタティック(定義された)ルートで作成
 ◎rip :ダイナミック(自動生成された)ルートで作成
 ◎misc :ブロードキャスト関連のフレーム処理で作成

3 設定画面について

2. 「ネットワーク設定」メニュー(つづき)

■ スタティックルーティング設定

「ネットワーク設定」-「ルーティング」

パケットの中継経路を最大32件まで登録できます。

スタティックルーティング設定			
登録の追加			
① 宛先	② サブネットマスク	③ ゲートウェイ	④
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="追加"/>
現在の登録 ⑤			
宛先	サブネットマスク	ゲートウェイ	

- ① 宛先 対象となる相手先のIPアドレスを入力します。
- ② サブネットマスク 対象となる宛先のIPアドレスに対するサブネットマスクを入力します。
- ③ ゲートウェイ パケット転送先ルーターのIPアドレスを入力します。
- ④ <追加> 入力内容が登録され、[現在の登録] (⑤)欄に表示します。
- ⑤ 現在の登録 登録した内容を表示します。

【登録例】

登録した内容を取り消すときは、該当する欄の<削除>をクリックします。

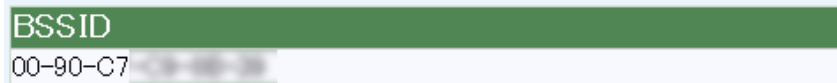
現在の登録			
宛先	サブネットマスク	ゲートウェイ	
192.168	255.255.255.0	192.168	<input type="button" value="削除"/>

3. 「無線設定」メニュー

■ BSSID

「無線設定」－「無線LAN」

本製品のBSSIDを表示します。
無線ブリッジ接続する相手側の機器に登録します。



- ※「無線ブリッジ」画面(☞P59)に表示される内容と同じです。
- ※「情報表示」メニューの「ネットワーク」画面(☞P66)に表示される[本体MACアドレス]とは異なります。
- ※[無線LAN]項目の[使用モード]欄が「OFF」に設定されている場合は、「無線UNITを使用していません。」と表示され、本製品の無線通信機能を停止しています。
- ※[無線LAN]項目の[使用モード]欄で「Site Survey」が設定されている場合は、BSSIDが表示されていますが、無線接続は停止していますので、ご注意ください。

3 設定画面について

3. 「無線設定」メニュー(つづき)

■ 無線LAN設定

「無線設定」-「無線LAN」

本製品に内蔵された無線LANカードに対する設定です。

※ ★印の設定は、無線LAN端末との通信に使用される機能です。

無線LAN設定		
使用モード	①	Wireless Bridge ▼
アンテナ	②	<input checked="" type="radio"/> 外部アンテナ <input type="radio"/> 内蔵アンテナ
SSID	③	LG
VLAN ID	④ ★	0 <small>VLAN IDを付けない場合は0を入力</small>
ANY接続拒否	⑤ ★	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑥	11CH (2462 MHz) ▼
Rts/Ctsスレッシュホールド	⑦	なし ▼
11g保護機能	⑧	有効 ▼
11gベーシックレート	⑨	802.11b ▼
パワーレベル	⑩	高 ▼
接続端末制限	⑪ ★	63
ビーコン間隔	⑫ ★	100 ミリ秒
DTIM間隔	⑬ ★	1
長距離通信モードを使用	⑭	<input checked="" type="radio"/> しない <input type="radio"/> する

- ① 使用モード 本製品の無線通信モードを切り替えます。(出荷時の設定: Wireless Bridge)
- ◎「Wireless Bridge」
「無線ブリッジ(ビル間通信)」機能を使用するとき設定します。
 - ◎「Access Point」
「無線ブリッジ(ビル間通信)」機能と「無線アクセスポイント」機能を併用するとき設定します。
 - ◎「Site Survey」
電波環境調査をするとき設定します。
ほかの無線LAN機器と電波干渉しない最適な場所への設置を確認できます。
※無線接続は、停止しますのでご注意ください。
 - ◎「OFF」
本製品の無線通信機能を停止させるとき設定します。
[BSSID]項目には、「ユニットを使用していません」を表示し、(②～⑭)欄の設定が無効になります。
- ② アンテナ 本製品で使用するアンテナを設定します。 (出荷時の設定: 外部アンテナ)

3. 「無線設定」メニュー

■ 無線LAN設定(つづき)

「無線設定」-「無線LAN」

- ③ SSID 無線ブリッジ接続(ビル間通信)する相手のBSSIDを自動検出するとき、設定します。 (出荷時の設定:LG)
 ※大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。
 ※設定したSSIDと同じ機器を検出すると、BSSIDを「無線ブリッジ」画面にある[ステーションリスト]項目の[自動検出された端末]欄(☞P59)に表示します。
 ※「Access Point」モード(☞P44)で使用するときは、本製品と同じ[SSID]が設定された無線LAN端末のグループと通信できます。
 無線ブリッジ接続と併用する場合は、自動検出された無線ブリッジ接続する相手側の[BSSID]を本製品に登録後、無線LAN端末との接続に使用する[SSID]に変更してください。
 ※相手のBSSIDを自動検出するとき、近くに、同じSSIDの弊社製無線アクセスポイントが存在する場合は、その無線アクセスポイントのBSSIDも表示されますのでご注意ください。
 ※[SSID]と[ESSID]は、同じ意味で使用しています。
 本製品以外の無線LAN機器では、[ESSID]と表記されている場合があります。
- ④ VLAN ID [SSID](③)欄の無線グループにID番号を設定します。 (出荷時の設定:0)
 設定したID番号と同じ端末(有線/無線)だけがVLANグループを構成できます。
 設定できる範囲は、「0~4094」です。
 ID番号を付けないときは、「0」を設定します。
 ※SB-520本体のVLAN IDは、「ネットワーク設定」メニューにある「LAN側IP」画面の[VLAN設定]項目(☞P33)で設定できます。

3 設定画面について

3. 「無線設定」メニュー

■ 無線LAN設定(つづき)

「無線設定」-「無線LAN」

※★印の設定は、無線LAN端末との通信に使用される機能です。

無線LAN設定		
使用モード	①	Wireless Bridge ▼
アンテナ	②	<input checked="" type="radio"/> 外部アンテナ <input type="radio"/> 内蔵アンテナ
SSID	③	LG
VLAN ID	④ ★	0 VLAN IDを付けない場合は0を入力
ANY接続拒否	⑤ ★	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑥	11CH (2462 MHz) ▼
Rts/Ctsスレッシュホールド	⑦	なし ▼
11g保護機能	⑧	有効 ▼
11gベーシックレート	⑨	802.11b ▼
パワーレベル	⑩	高 ▼
接続端末制限	⑪ ★	63
ビーコン間隔	⑫ ★	100 ミリ秒
DTIM間隔	⑬ ★	1
長距離通信モードを使用	⑭	<input checked="" type="radio"/> しない <input type="radio"/> する

⑤ **ANY接続拒否:** …………… ANY接続を許可するように設定されている無線LAN端末からの検索や接続の拒否についての設定です。 (出荷時の設定: しない)

出荷時の設定では、接続が簡単になるように、無線LAN端末からの検索や接続を許可しています。

この設定を「する」にした場合、ANY接続を許可するように設定されている無線LAN端末が使用する「Windows標準のワイヤレスネットワーク接続」や「弊社製無線LANカードに付属の設定ユーティリティ」から検索されません。

⑥ **チャンネル** …………… 本製品の無線通信に使用するチャンネルを設定します。

(出荷時の設定: 11 (2462MHz))

※無線ブリッジ接続する相手と同じ設定にします。

※無線LAN端末は、本製品のチャンネルを自動的に検知して通信します。

※近くに2.4GHz帯(IEEE802.11b/g規格)の無線アクセスポイントやビル間通信機器が存在するときは、電波干渉を避けるため、本製品の「チャンネル」は、それらの無線ネットワークグループと4チャンネル以上空けて設定してください。

それ以下のときは、図に示すように帯域の1部が重複するため混信することがあります。

たとえば、隣接する無線ネットワークグループを1-6-11チャンネルに設定すると混信しません。

※本製品は、14チャンネルに対応していません。

※[無線LAN]項目の[使用モード]欄が「OFF」に設定されている場合は、選択できるチャンネルを表示しません。

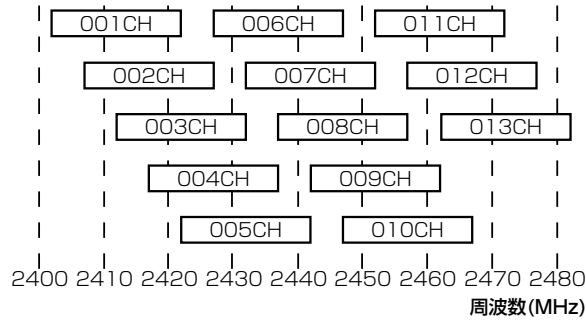
3. 「無線設定」メニュー

■ 無線LAN設定(つづき)

「無線設定」-「無線LAN」

⑦ チャンネル(つづき) ………

【各チャンネルの帯域】



⑦ Rts/Ctsスレッシュホールド ……………

RTS/CTSスレッシュホールドとは、RTS/CTS信号を送信するしきい値のことです。 (出荷時の設定:なし)

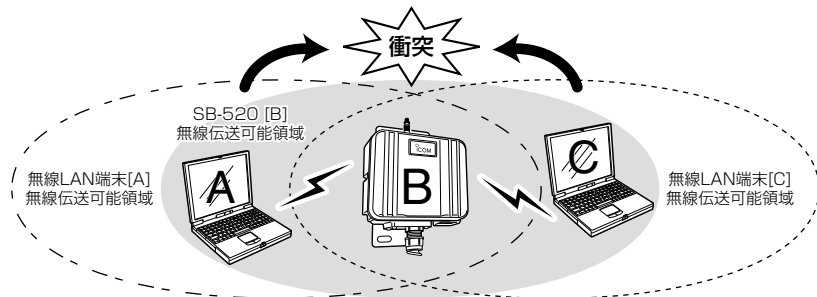
データサイズがしきい値を超えると、互いの通信状態を打診・交渉(ネゴシエーション)するためにRTS/CTS信号を送信して「隠れ端末」の影響による通信速度の低下を防止します。

しきい値は、通信環境やデータの転送量などにあわせて「500バイト」または「1000バイト」から選択します。

※「なし」を設定したときは、RTS/CTS信号を送信しません。

【隠れ端末とは】

下図のように、それぞれが無線LAN端末[B]と通信できても、互いが直接通信できない無線LAN端末[A]-[C]同士([A]に対して[C]、[C]に対して[A])のことを隠れ端末と呼びます。



※説明では、外部アンテナやSA-4を省略しています。

通信の衝突を防止するには、無線端末[A]から送信要求(Rts)信号を受信した本製品[B]が、無線伝送可能領域内にある無線端末[A]および[C]に送信可能(Cts)信号を送り返すことで、Rts信号を送信していない無線端末[C]に本製品[B]が隠れ端末と通信中であることを認識させます。

これにより、Rts信号を送信していない無線端末[C]は、本製品[B]から受信完了通知(ACK)を受信するまで本製品[B]へのアクセスを自制して、通信の衝突を防止できます。

3 設定画面について

3. 「無線設定」メニュー

■ 無線LAN設定(つづき)

「無線設定」-「無線LAN」

※★印の設定は、無線LAN端末との通信に使用される機能です。

無線LAN設定		
使用モード	①	Wireless Bridge ▼
アンテナ	②	<input checked="" type="radio"/> 外部アンテナ <input type="radio"/> 内蔵アンテナ
SSID	③	LG
VLAN ID	④ ★	0 <small>VLAN IDを付けない場合は0を入力</small>
ANY接続拒否	⑤ ★	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑥	11CH (2462 MHz) ▼
Rts/Ctsスレッシュホールド	⑦	なし ▼
11g保護機能	⑧	有効 ▼
11gベーシックレート	⑨	802.11b ▼
パワーレベル	⑩	高 ▼
接続端末制限	⑪ ★	63
ビーコン間隔	⑫ ★	100 ミリ秒
DTIM間隔	⑬ ★	1
長距離通信モードを使用	⑭	<input checked="" type="radio"/> しない <input type="radio"/> する

- ⑧ 11g保護機能 …………… 異なる無線LAN規格(IEEE802.11b/g)が混在する環境で発生する通信速度低下を緩和する機能です。 (出荷時の設定:有効)
- ◎「無効」 : [IEEE802.11b/g]規格のどちらかに統一された無線LAN環境で使用するときを設定します。
- ◎「有効」 : [IEEE802.11b/g]規格の無線LAN機器が混在する環境で、[IEEE802.11g]規格の無線LAN機器の通信速度が極端に低下するときを設定します。
- ◎「g専用」 : [IEEE802.11g]規格の無線LAN機器だけ接続を許可します。 [IEEE802.11b]規格だけに対応した無線LAN機器は接続できなくなります。
- ⑨ 11gベーシックレート …… [IEEE802.11g]規格でのベーシックレートを設定します。 (出荷時の設定:802.11b)
- [IEEE802.11g]規格でのみ有効です。
各無線LAN規格が対応できる速度は、下記ようになります。
- ◎「802.11」 : 「1/2」Mbps
- ◎「802.11b」 : 「1/2/5.5/11」Mbps
- ◎「802.11g」 : 「1/2/5.5/11/6/12/24」Mbps
- ◎「OFDM」 : 「6/12/24」Mbps
- ※設定を変更すると、正常に通信できないことがあります。
特に必要がない場合は、工場出荷時の状態でご使用ください。

3. 「無線設定」メニュー

■ 無線LAN設定(つづき)

「無線設定」→「無線LAN」

- ⑩ **パワーレベル** …………… 本製品に内蔵された無線LANカードの送信出力を設定します。
高/中/低(3段階)の中から選択できます。 (出荷時の設定:高)
本製品の最大伝送距離は、パワーレベルが「高」の場合です。
パワーレベルを低くすると、それに比例して伝送距離も短くなります。
- 【パワーレベルを低くする目的について】**
 ◎本製品から送信される電波が広範囲に届くのを軽減したいとき
 ◎通信エリアを制限してセキュリティを高めたいとき
 ◎比較的狭いエリアに複数台の無線ブリッジが設置された環境で、近くの無線LAN機器との電波干渉をなくして、通信速度の低下などを軽減したいとき
- ⑪ **接続端末制限** …………… 本製品に同時接続できる無線LAN端末の台数を設定します。
設定できる範囲は、「1～63」です。 (出荷時の設定:63)
※接続制限を設定すると、接続が集中するのを防止(本製品の負荷を分散)できますので、接続集中による通信速度低下を防止できます。
- ⑫ **ビーコン間隔** …………… 本製品から一定間隔で送信されるパケット(ビーコン)の送信間隔(ミリ秒)を設定します。 (出荷時の設定:100)
設定できる範囲は、「20～1000(ミリ秒)」です。
ビーコンとは、無線ネットワークを同期させるための信号です。
※[DTIM間隔](⑬)を掛けた値が、「5000」を超えないように設定してください。
※設定を変更すると、正常に通信できないことがあります。
特に必要がない場合は、工場出荷時の状態でご使用ください。
- ⑬ **DTIM間隔** …………… DTIM(Delivery Traffic Indication Message)を送信されたビーコンに挿入する間隔を設定します。 (出荷時の設定:1)
設定できる範囲は、「1～250」です。
DTIMとは、パケットの送信待ちを伝えるメッセージのことです。
※[ビーコン間隔](⑫)を掛けた値が、「5000」を超えないように設定してください。
※設定を変更すると、正常に通信できないことがあります。
特に必要がない場合は、工場出荷時の状態でご使用ください。

3 設定画面について

3. 「無線設定」メニュー

■ 無線LAN設定(つづき)

「無線設定」-「無線LAN」

※★印の設定は、無線LAN端末との通信に使用される機能です。

無線LAN設定		
使用モード	①	Wireless Bridge ▼
アンテナ	②	<input checked="" type="radio"/> 外部アンテナ <input type="radio"/> 内蔵アンテナ
SSID	③	LG
VLAN ID	④ ★	0 <small>VLAN IDを付けない場合は0を入力</small>
ANY接続拒否	⑤ ★	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑥	11CH (2462 MHz) ▼
Rts/Ctsスレッシュホールド	⑦	なし ▼
11g保護機能	⑧	有効 ▼
11gベーシックレート	⑨	802.11b ▼
パワーレベル	⑩	高 ▼
接続端末制限	⑪ ★	63
ビーコン間隔	⑫ ★	100 ミリ秒
DTIM間隔	⑬ ★	1
長距離通信モードを使用	⑭	<input checked="" type="radio"/> しない <input type="radio"/> する

- ⑭ **長距離通信モードを使用** … 相手との通信距離が4Km以上で、極端に通信速度が遅い場合に設定します。
(出荷時の設定: しない)
- ※長距離通信モードは、対向する相手側の本製品にも設定することで有効になります。
- ※通信相手との距離が4Km未満の場合は、出荷時の設定でご使用ください。
4Km未満で長距離通信モードを使用すると、通信速度低下の原因になります。
- ※無線ブリッジ接続する相手以外の[BSSID]が複数登録されている場合は、速度低下の原因になります。
- ※長距離通信をする場合、直線の見通し距離だけでなく、電波の反射や干渉の影響、およびフレネルゾーンなどを考慮して、アンテナを設置する必要があります。
- 長距離通信モードを設定しても改善されない場合は、これらも原因と考えられます。
- ※「フレネルゾーンについて」や「地球の影響について」は、本製品に同梱の設置工事説明書をご覧ください。

3. 「無線設定」メニュー(つづき)

■ 暗号化設定

「無線設定」-「暗号化」

無線通信を暗号化するための設定です。

※ ★印の設定は、無線LAN端末との通信に使用される機能です。

暗号化設定		
ネットワーク認証	①	オープンシステム・共有キー
暗号化方式	②	なし
キージェネレーター	③	
PSK(Pre-Shared Key)	④★	半角英数字で8-63文字、もしくは16進数で64桁を入力
キー更新間隔	⑤★	120 分
キーインデックス	⑥	1

- ① ネットワーク認証 …………… [暗号化方式] (②) 欄で選択された暗号化方式を使用する無線LAN端末からのアクセスに対する認証方式を選択します。
 (出荷時の設定: オープンシステム・共有キー)
 ※異なる認証方式の相手とは互換性がないので、通信をする相手間で同じ設定にしてください。
 ※弊社製無線LAN機器によっては、「認証モード」と記載されています。
 ※「WPA-PSK」、「WPA2-PSK」、「WPA-PSK・WPA2-PSK」の認証方式は、無線ブリッジ接続機能による通信には使用できません。

【認証方式について】

- オープンシステム・共有キー
 「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、「オープンシステム」と「共有キー」を自動認識しますので、本製品と暗号鍵(キー)が同じであれば通信できます。
- オープンシステム
 「WEP RC4」、「OCB AES」暗号化方式による無線LAN端末からのアクセスに対して、暗号鍵(キー)の認証をしません。
- 共有キー
 「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、本製品と無線LAN端末の暗号鍵(キー)が同じかどうかを認証します。
- IEEE802.1X
 「WEP RC4」暗号化方式を使用して、RADIUSサーバーによるIEEE802.1X認証するときの設定です。
 ※ [RADIUS設定] 項目 (P56) と併せて設定してください。

【ネットワーク認証と暗号化方式の対応について】						
	オープンシステム	共有キー	オープンシステム・共有キー	WPA WPA2	WPA-PSK WPA2-PSK	IEEE802.1X
WEP RC4	○	○	○	×	×	○
OCB AES	○	×	×	×	×	×
TKIP	×	×	×	○	○	×
AES	×	×	×	○	○	×

3 設定画面について

3. 「無線設定」メニュー

■ 暗号化設定(つづき)

「無線設定」-「暗号化」

※★印の設定は、無線LAN端末との通信に使用される機能です。

暗号化設定		
ネットワーク認証	①	オープンシステム・共有キー ▼
暗号化方式	②	なし ▼
キージェネレーター	③	<input type="text"/>
PSK(Pre-Shared Key)	④★	<input type="text"/> 半角英数で8-63文字、もしくは16進数で64桁を入力
キー更新間隔	⑤★	120 分
キーインデックス	⑥	1 ▼

- ① ネットワーク認証(つづき)
 - ◎WPA(Wi-Fi Protected Access)
「TKIP」/「AES」暗号化方式を使用して、RADIUSサーバーによるIEEE802.1X認証をするときの設定です。
※ [IEEE802.1X] 認証より強力で、「TKIP」暗号化方式の使用を標準規格とする認証方式です。
※ [RADIUS設定] 項目(☞P56)と併せて設定してください。
 - ◎WPA2
ネットワーク認証方式にWPA2を使用します。
※ [WPA] 認証より強力な「AES」暗号化方式の使用を標準規格とする認証方式で、「PMKIDキャッシュ」により、再接続による認証が不要です。
※ 「WPA2」認証に対応したクライアントが必要です。
※ [RADIUS設定] 項目(☞P56)と併せて設定してください。
 - ◎WPA・WPA2
「WPA」認証と「WPA2」認証を自動認識します。
 - ◎WPA-PSK(Pre-Shared Key)
共有鍵(キー)で認証します。
RADIUSサーバーを利用しない簡易的な「TKIP」/「AES」暗号化の認証方式で、本製品と無線LAN端末の共有鍵(キー)が同じかどうかを認証します。
 - ◎WPA2-PSK
ネットワーク認証方式にWPA2-PSKを使用します。
※ 「WPA2-PSK」認証に対応した無線LAN端末が必要です。
 - ◎WPA-PSK・WPA2-PSK
「WPA-PSK」認証と「WPA2-PSK」認証を自動認識します。

【不正アクセス防止のアドバイス】

本製品に設定する暗号鍵(WEPキー/Pre-Shared Key)は、容易に推測されないものにし、さらに定期的に暗号鍵を変更すると有効です。
数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵を変更すると有効です。

3. 「無線設定」メニュー

■ 暗号化設定(つづき)

「無線設定」—「暗号化」

- ② 暗号化方式 …………… 無線伝送データを暗号化する方式を選択します。 (出荷時の設定:なし)
 対応する暗号化方式は、「WEP RC4」、「OCB AES」、「TKIP」、「AES」です。
 異なる暗号化方式の相手とは互換性がないので、暗号化方式は、通信をする相手間で同じ設定にしてください。
 ※「TKIP」方式と「AES」方式は、無線ブリッジ接続機能による通信には使用できません。
 ※「WEP RC4 152(128)」、「OCB AES」方式での接続は、弊社製無線LANカードに付属の設定ユーティリティをご利用いただくか、弊社製ワイヤレスLANユニットをご用意ください。

【暗号化方式について】

◎なし

データを暗号化しないで通信します。

◎WEP RC4

無線通信で一般によく使用されるセキュリティです。

※暗号鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

※[ネットワーク認証](①)欄で、「オープンシステム・共有キー」、または「オープンシステム」、「共有キー」、「IEEE802.1X」を選択したとき使用できます。

※「WEP RC4 152(128)」方式は、Windows標準のワイヤレスネットワーク接続を使用して本製品に接続できません。

◎OCB AES

「WEP RC4」より強力な暗号化方式で、暗号化するデータのブロック長と暗号鍵(キー)の長さは、128ビットです。

※[ネットワーク認証](①)欄で、「オープンシステム」を選択したとき使用できます。

※Windows標準のワイヤレスネットワーク接続を使用して本製品に接続できません。

◎TKIP(Temporal Key Integrity Protocol)

暗号鍵(キー)を一定間隔で自動更新しますので、「WEP RC4」より強力です。

Windows 7、Windows Vista、Windows XPの端末で使用できます。

※[ネットワーク認証](①)欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

◎AES(Advanced Encryption Standard)

暗号化の強化、および暗号鍵(キー)を一定間隔で自動更新しますので、「TKIP」より強力な暗号化方式です。

※[ネットワーク認証](①)欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

◎TKIP・AES

無線LAN端末からのアクセスに対して、「TKIP」と「AES」を自動認識します。

3 設定画面について

3. 「無線設定」メニュー

■ 暗号化設定(つづき)

「無線設定」-「暗号化」

※★印の設定は、無線LAN端末との通信に使用される機能です。

暗号化設定		
ネットワーク認証	①	オープンシステム・共有キー
暗号化方式	②	なし
キージェネレーター	③	
PSK(Pre-Shared Key)	④★	
キー更新間隔	⑤★	120 分
キーインデックス	⑥	1

- ③ キージェネレーター …………… [暗号化方式] (②) 欄で、「WEP RC4」、または「OCB AES」を選択したとき、暗号化、および復号に使用する暗号鍵(キー)を [WEPキー] 項目 (※P57) に生成するための文字列を設定します。
(出荷時の設定: 空白(何も設定されていません。))

次のように文字列を設定すると、暗号鍵(キー)が生成されます。

1. [暗号化方式] (②) を選択します。
 2. 大文字/小文字の区別に注意して、文字列を31文字以内(任意の半角英数字/記号)で入力します。
※入力する文字列は、通信する相手(弊社製機器)側のキージェネレーターと同じ文字列を設定してください。
他社製の機器とは互換性がないので、ご注意ください。
 3. <登録>をクリックします。
 - 入力した文字列より生成された暗号鍵(キー)を [WEPキー] 項目のテキストボックスに表示します。
- ※ [WEPキー] 項目の [入力モード] 欄が、「ASCII文字」に設定されている場合は、[キージェネレーター] を使用できません。
- ※ [WEPキー] 欄に生成される暗号鍵(キー)の桁数、および文字数は、選択する [暗号化方式] によって異なります。(※P20)
- ※ キージェネレーターから生成された暗号鍵(キー)が通信相手間で異なる場合、暗号化されたデータを復号できません。
- ※ 暗号鍵(キー)を直接設定するときは、[WEPキー] 項目で設定してください。

- ④ PSK(Pre-Shared Key) …… 共有鍵(キー)を半角英数字で入力します。
[暗号化方式] (②) 欄で「TKIP」、または「AES」方式を選択してから、[ネットワーク認証] (①) 欄で「WPA-PSK」、「WPA2-PSK」、「WPA-PSK・WPA2-PSK」を選択します。
※同じ暗号化方式を使用する相手と、同じ共有鍵(キー)を設定してください。
※16進数で設定するときは、64桁を入力してください。
※ASCII文字で設定するときは、大文字/小文字の区別に注意して、8~63文字を入力してください。

3. 「無線設定」メニュー

■ 暗号化設定(つづき)

「無線設定」-「暗号化」

- ⑤ キー更新間隔 …………… [ネットワーク認証] (①) 欄で、「WPA」、「WPA2」、「WPA・WPA2」、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK・WPA2-PSK」を選択したとき、暗号鍵(キー)の更新間隔を分で設定します。 (出荷時の設定: 120)
設定できる範囲は、「0~1440(分)」です。
※「0」を設定すると、更新しません。
- ⑥ キーインデックス …………… [暗号化方式] (①) 欄で、「WEP RC4」、または「OCB AES」を選択したとき、[WEPキー] 欄 (P57) のテキストボックスに設定された暗号鍵(キー)のうち、送信データの暗号化に使用する鍵(キー)を「1」~「4」の番号で指定します。 (出荷時の設定: 1)
※「1」~「4」のすべてに設定された暗号鍵(キー)の内容が通信相手と同じであれば、通信する相手間で異なる番号を指定しても通信できます。
※本製品に無線LANで接続する端末のキーインデックスを設定するとき、Windows XP (Service Pack適用時を除く) 標準のワイヤレスネットワーク接続を使用する場合は、本製品とは異なり選択範囲が「0」~「3」ですのでご注意ください。
本製品で「1」を選択した場合は、Windows XPの[キーインデックス(詳細)(X)]で「0」を設定することと同じ意味になります。
※弊社製無線LAN機器によっては、「キーID」と記載されています。

3 設定画面について

3. 「無線設定」メニュー(つづき)

■ RADIUS設定

「無線設定」-「暗号化」

RADIUSサーバーを使用してWPA認証、またはIEEE802.1X認証するときの設定です。

※EAP-TLSとEAP-TTLS、EAP-PEAPに対応しています。

RADIUS設定		
	プライマリー	セカンダリー
① アドレス	<input type="text"/>	<input type="text"/>
② ポート	<input type="text" value="1812"/>	<input type="text" value="1812"/>
③ シークレット	<input type="text"/>	<input type="text"/>
④ 再認証間隔	<input type="text" value="120"/> 分	

- ① **プライマリー/セカンダリー** [プライマリー]列に設定したサーバーから応答がない場合、その次にアクセスさせるRADIUSサーバーがあるときは、[セカンダリー]列にそのRADIUSサーバーアドレスを設定します。
- ② **アドレス** 対象となるRADIUSサーバーのIPアドレスを入力します。
- ③ **ポート** 対象となるRADIUSサーバーの認証ポートを設定します。
(出荷時の設定: 1812)
※設定できる範囲は、「1~65535」です。
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。
- ④ **シークレット** 本製品とRADIUSサーバーの通信に使用するキーを設定します。
RADIUSサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。
- ⑤ **再認証間隔** [暗号化設定]項目の[ネットワーク認証](①)欄(☑P51)で、「IEEE802.1X」を選択したとき、RADIUSサーバーに再度認証を要求する間隔を分で設定します。
(出荷時の設定: 120)
設定できる範囲は、「0~9999(分)」です。
※「0」を設定したときは、再認証しません。

3. 「無線設定」メニュー(つづき)

■ WEPキー

「無線設定」-「暗号化」

「WEP RC4」、または「OCB AES」方式の暗号化で使用する暗号鍵(キー)の設定です。

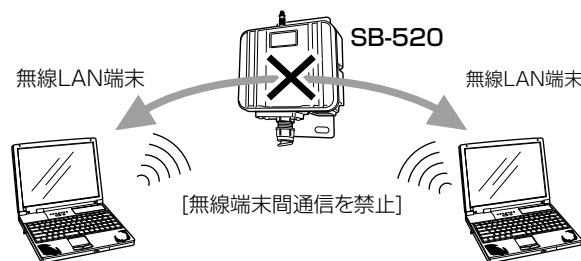
- ① 入力モード 暗号鍵(キー)の入力モードを選択します。 (出荷時の設定: 16進数)
 ※入力モードを変更したときは、「暗号化」画面の「登録」をクリックしてから、暗号鍵(キー)を入力してください。
 ※ASCII文字が設定されているときは、[暗号化設定]項目(※P54)の[キージェネレーター]を使用できません。

- ② 鍵(キー)入力用ボックス ... [キージェネレーター]を使用しない場合は、暗号化および復号化に使用する暗号鍵(キー)を16進数で直接入力します。 (出荷時の設定: 00-00-00-00-00)
 ※16進数で設定するときは、「0~9」および「a~f(またはA~F)」の半角文字を入力してください。
 ※ASCII文字で設定するときは、大文字/小文字の区別に注意して、任意の半角英数字を入力してください
 ※暗号鍵(キー)は、通信する相手間で、すべての[キーインデックス(1~4)]値に対して同じ設定にすることをおすすめします。
 異なる設定の場合、通信相手間で[キーインデックス]値の設定が異なると、通信できません。

■ 無線端末間通信設定

「無線設定」-「MACフィルタリング」

無線LAN端末同士の通信についての設定です。



※説明では、内蔵アンテナを使用し、SA-4を省略しています。

- 無線端末間通信を禁止..... 無線LAN端末同士が本製品を介して通信するのを禁止する場合に設定します。 (出荷時の設定: しない)
 ※本製品を無線ホットスポット接続に利用するときなどは、「する」に設定すると、本製品を介して無線LAN端末同士が通信することを禁止できます。

3 設定画面について

3. 「無線設定」メニュー(つづき)

■ MACアドレスフィルタリング設定

「無線設定」－「MACフィルタリング」

本製品に接続できる無線LAN端末を制限する設定です。

MACアドレスフィルタリング 設定			
MACアドレスフィルタリングを使用 ①		<input checked="" type="radio"/> しない <input type="radio"/> する	
登録の追加 ②			
MACアドレス		<input type="text"/>	<input type="button" value="追加"/>
現在の登録 ③			
登録済みの端末	受信中の端末	通信状況	

① MACアドレスフィルタリングを使用

…………… 本製品に無線LAN端末のMACアドレスを登録して、本製品と接続できる無線LAN端末を制限する設定です。
(出荷時の設定: しない)
※「する」に設定すると、[現在の登録]欄に登録されていないMACアドレスの無線LAN端末は、本製品とアクセスできません。

② 登録の追加 ……………

接続を許可する無線LAN端末のMACアドレスを入力して、〈追加〉をクリックします。
※登録されたMACアドレスは、[登録済みの端末]欄に表示され、MACアドレスフィルタリングが有効なとき、そのMACアドレスを持つ無線LAN端末とだけ通信できます。
※最大256台分のMACアドレスを登録できます。
※入力は、半角英数字で12桁(16進数)を入力します。
※2つの入力例は、同じMACアドレスになります。
(入力例: 00-90-c7-47-00-00、0090c7470000)

③ 現在の登録 ……………

無線LAN端末の登録と通信状況を表示します。
登録されていないMACアドレスを持つ無線LAN端末についても[受信中の端末]欄にMACアドレスを表示しますので、〈追加〉をクリックして、追加登録できます。

【登録例】

登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

現在の登録			
登録済みの端末	受信中の端末	通信状況	
00-90-C7- 00-00-00	00-90-C7- 00-00-00	通信中	<input type="button" value="削除"/>
00-90-C7- 00-00-00		登録済	<input type="button" value="削除"/>

3. 「無線設定」メニュー(つづき)

■ BSSID

「無線設定」－「無線ブリッジ」

本製品のBSSIDを表示します。
無線ブリッジ接続する相手側の機器に登録します。



- ※「無線LAN」画面(☞P43)に表示される内容と同じです。
- ※「情報表示」メニューの「ネットワーク」画面(☞P66)に表示される[本体MACアドレス]とは異なります。
- ※「無線LAN」項目の[使用モード]欄が「OFF」に設定されている場合は、「無線UNITを使用していません。」と表示され、本製品の無線通信機能を停止しています。
- ※「無線LAN」項目の[使用モード]欄で「Site Survey」が設定されている場合は、BSSIDが表示されていますが、無線接続は停止していますので、ご注意ください。

■ ステーションリスト

「無線設定」－「無線ブリッジ」

無線ブリッジ接続(ビル間通信)する相手の[BSSID]に登録します。



※上図は、自動検出例です。

- ① **登録の追加** 登録しない相手とは、無線ブリッジ接続できません。
<追加>をクリックすると、ここで入力した[BSSID]と[最大通信速度]が登録されます。
- [BSSID]** 無線ブリッジ接続する相手の[BSSID]を、12桁(16進数)の半角英数字で入力します。
※最大256台分の[BSSID]が登録できます。
※下記の入力例は、同じ[BSSID]として処理されます。
(入力例:00-90-C7-99-00-00、0090C7990000)
- [最大通信速度]** 登録した相手と通信する速度を設定します。(出荷時の設定:自動)
※「自動」のときは、環境の変化などで通信が不安定になると、通信が続行可能な速度に自動で切り替わります。
※数値を指定したときは、環境の変化などで通信が不安定になると、指定した数値以下の速度に自動で切り替わります。

3 設定画面について

3. 「無線設定」メニュー

■ ステーションリスト(つづき)

「無線設定」－「無線ブリッジ」

ステーションリスト		
登録の追加 ①		
BSSID	最大通信速度	
<input type="text"/>	自動 ▼	<input type="button" value="追加"/>
自動検出された端末 ②		
BSSID	最大通信速度	
00-90-C7- 00-12-18	自動 ▼	<input type="button" value="追加"/>

※上図は、自動検出例です。

- ② 自動検出された端末 …………… [チャンネル]と[SSID]が、本製品と同じ設定の弊社製ビル間通信ユニットを検出すると、その機器の[BSS ID]を表示します。
検出された機器とビル間通信する場合は、この欄の右に表示された〈追加〉をクリックすると、検出された[BSS ID]を登録できます。
※検出結果を最大64件まで表示します。
※近くに、同じ条件の弊社製無線アクセスポイントや無線AP間通信する機器が存在する場合は、それらの機器の[BSS ID]と併せて検出されますのでご注意ください。

■ 登録済み端末リスト

「無線設定」－「無線ブリッジ」

[ステーションリスト]項目から登録した[BSSID]と[最大通信速度]を表示します。

登録済み端末リスト			
BSSID	最大通信速度	信号強度	
00-90-C7- 00-12-18	自動 ▼ <input type="button" value="変更"/>	5	<input type="button" value="削除"/>
00-90-C7- 00-12-11	自動 ▼ <input type="button" value="変更"/>	0	<input type="button" value="削除"/>

- このリストに表示する[BSSID]を持つ弊社製ビル間通信ユニットと、設定した速度で無線ブリッジ接続できます。
通信中に表示される[信号強度]は、「15」以上であれば、正常に通信可能です。
※登録を削除するときは、該当する欄の右端にある〈削除〉をクリックします。
※登録した相手との送信速度を変更するときは、数値を選択後、〈変更〉をクリックします。
※無線ブリッジ接続する相手の[BSSID]だけを登録してご使用ください。
それ以外の相手の[BSSID]が複数登録されている場合は、速度低下の原因になります。

4. 「システム設定」メニュー

■ 管理者ID設定

「システム設定」－「本体管理」

本製品の設定画面にアクセスするためのパスワードを変更します。

管理者ID設定		
管理者ID	①	admin
管理者パスワード	②	<input type="text"/>
確認入力	③	<input type="text"/>

- ① **管理者ID** 本製品の設定画面にアクセスしたとき、ユーザー名の入力を求められますので、そこに[管理者ID]として、「admin」を入力します。
※本製品の[管理者ID]は、変更できません。
- ② **管理者パスワード** [管理者ID]に対するパスワードを設定します。
大文字/小文字の区別に注意して、任意の英数字(半角31文字以内)で入力します。
[管理者パスワード]を設定すると、次回のアクセスからパスワードの入力を求められますので、そこに[管理者パスワード]を入力します。
入力中の文字は、すべて「●(黒丸)」で表示します。
- ③ **確認入力** 確認のために、パスワードを再入力します。

【不正アクセス防止のアドバイス】

本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。

数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものにし、さらに定期的にパスワードを変更するなどが有効です。

【ご注意】

管理者パスワードを忘れた場合、設定を確認できなくなりますので、忘れないように注意してください。

※お忘れの場合、本製品の<MODE>ボタンを押して、設定を工場出荷時(初期化)に戻していただくことになります。

初期化のしかたについて詳しくは、別紙の「設定ガイド」をご覧ください。

3 設定画面について

4. 「システム設定」メニュー(つづき)

■ 管理者IP設定

「システム設定」－「本体管理」

本製品の設定画面へのアクセスをIPアドレスで制限する設定です。

管理者IP設定	
管理者IP1	<input type="text"/>
管理者IP2	<input type="text"/>
管理者IP3	<input type="text"/>
管理者IP4	<input type="text"/>
管理者IP5	<input type="text"/>
管理者IP6	<input type="text"/>
管理者IP7	<input type="text"/>
管理者IP8	<input type="text"/>

管理者IP1～管理者IP8 ………

本製品の設定画面へのアクセスを制限するために、本製品にアクセスを許可する端末のIPアドレスを8台まで登録できます。（入力例: 192.168.0.5）
※ [管理者IP]を設定すると、IPアドレスが登録された端末以外は、次回のアクセスから本製品の設定画面にアクセスできなくなります。
※ 空白の場合は、本製品に接続するすべての端末が設定画面にアクセスできます。

4. 「システム設定」メニュー(つづき)

■ 自動時計設定

「システム設定」-「時計」

本製品の内部時計を自動設定するとき、アクセスするタイムサーバーの設定です。

自動時計設定	
自動時計設定を使用 ①	<input checked="" type="radio"/> しない <input type="radio"/> する
NTPサーバー IPアドレス ②	210.173.160.27
アクセス時間間隔 ③	1 日

- ① 自動時計設定を使用 …………… 本製品の自動時計設定機能を設定します。 (出荷時の設定: しない)
「する」に設定すると、インターネット上に存在するタイムサーバーに日時の問い合わせをして、内部時計を自動設定します。
- ② NTPサーバ IPアドレス …… アクセスするタイムサーバーのIPアドレスを入力します。
(出荷時の設定: 210.173.160.27)
※初期に参照しているNTPサーバーは、インターネットマルチフィード株式会社(<http://www.jst.mfeed.ad.jp/>)のものです。
- ③ アクセス時間間隔 …………… タイムサーバーにアクセスする間隔を設定します。
設定できる範囲は、「0~7(日)」です。 (出荷時の設定: 1)
※「0」を設定すると、問い合わせをしません。
※設定した日数でアクセスできなかったときは、さらに設定した日数が経過するまで問い合わせをしません。
※自動時計設定機能は、NTPサーバーへの問い合わせ先(経路)を設定する必要があります。
経路を設定しないときは、問い合わせできません。
「ネットワーク設定」メニュー→「LAN側IP」画面→「IPアドレス設定」項目にある「デフォルトゲートウェイ」欄(※P34)、または「ルーティング」画面→「スタティックルーティング設定」項目(※P42)で、ルーティングテーブルを設定してください。

3 設定画面について

4. 「システム設定」メニュー(つづき)

■ 内部時計設定

「システム設定」-「時計」

本製品の内部時計を設定します。

内部時計設定						
本体の時刻 ①	2010年	1月	1日	11時	20分	③
設定する時刻 ②	2010年	10月	7日	12時	00分	時刻設定

- ① **本体の時刻** 本製品に設定されている時刻を表示します。
- ② **設定する時刻** 本製品の設定画面にアクセスしたときの時刻を、最初に表示します。
※WWWブラウザの〈更新〉をクリックすると、端末の時計設定を取得して表示します。
- ③ **〈時刻設定〉** [設定する時刻] (②) 欄に表示された時刻を本製品に設定するボタンです。
※時刻を正確に設定するときは、本製品の設定画面に再度アクセスしなおすか、WWWブラウザの〈更新〉をクリックしてから、〈時刻設定〉をクリックしてください。

■ SYSLOG設定

「システム設定」-「SYSLOG」

指定したホストにログ情報などを出力するための設定です。

SYSLOG設定	
DEBUGを使用 ①	<input checked="" type="radio"/> しない <input type="radio"/> する
INFOを使用 ②	<input type="radio"/> しない <input checked="" type="radio"/> する
NOTICEを使用 ③	<input type="radio"/> しない <input checked="" type="radio"/> する
ホストアドレス ④	<input type="text"/>

- ① **DEBUGを使用** 各種デバッグ情報をSYSLOGに出力する設定です。(出荷時の設定: しない)
- ② **INFOを使用** INFOタイプのメッセージをSYSLOGに出力する設定です。
(出荷時の設定: する)
- ③ **NOTICEを使用** NOTICEタイプのメッセージをSYSLOGに出力する設定です。
(出荷時の設定: する)
- ④ **ホストアドレス** SYSLOG機能を使用する場合、SYSLOGを受けるホストのアドレスを入力します。
※ホストは、SYSLOGサーバー機能に対応している必要があります。

4. 「システム設定」メニュー(つづき)

■ SNMP設定

「システム設定」-「SNMP」

TCP/IPネットワークにおいて、ネットワーク上の各ホストから本製品の情報を自動的に収集してネットワーク管理するときの設定です。

SNMP設定	
SNMP設定を使用 ①	<input type="radio"/> しない <input checked="" type="radio"/> する
コミュニティID(GET) ②	public
名前 ③	
場所 ④	
連絡先 ⑤	

- ① **SNMPを使用** …………… 本製品のSNMP機能を設定します。(出荷時の設定: する)
「する」に設定すると、本製品の設定情報をSNMP管理ツール側で管理できません。
- ② **コミュニティID(GET)** …… 本製品の設定情報をSNMP管理ツール側から読み出すことを許可するIDを、半角31文字以内の英数字で入力します。
- ③ **名前** …………… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される名前を入力します。
(出荷時の設定: public)
※半角127文字以内の英数字で入力します。
- ④ **場所** …………… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される場所を、半角127文字以内の英数字で入力します。
- ⑤ **連絡先** …………… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される連絡先を、半角127文字以内の英数字で入力します。

3 設定画面について

5. 「情報表示」メニュー

■ インターフェース リスト

「情報表示」-「ネットワーク」

「ネットワーク設定」メニュー→「ルーティング」画面→[IP経路情報]項目(☞P41)に表示された[経路]について、その詳細を表示します。

インターフェース リスト		
インターフェース	IPアドレス	サブネットマスク
atheros0	192.168.1.1	255.255.255.0
kse0	192.168.0.1	255.255.255.0
lo0	127.0.0.1	255.0.0.0

※上図は、ルーティングモードを使用したときの表示例です。

■ インターフェース情報

「情報表示」-「ネットワーク」

本製品のポートごとに、通信状況とパケットの数を表示します。

インターフェース情報		
インターフェース	情報	
atheros0 ①	状況	通信中
	受信パケット数	0
	送信パケット数	1
kse0 ②	状況	通信中
	受信パケット数	118
	送信パケット数	83

① atheros0 [無線LAN]ポートでの通信状況と、そのときの送信と受信のパケット数を表示します。

② kse0 [有線LAN]ポートでの通信状況と、そのときの送信と受信のパケット数を表示します。

■ 本体MACアドレス

「情報表示」-「ネットワーク」

本製品のMACアドレスを表示します。

本体MACアドレス	
00-90-C7-	XXXXXXXXXX

※本製品のケースに貼られているシリアルシールにも同じ内容が記載されています。

※「無線設定」メニューの「無線LAN」画面(☞P43)と「無線ブリッジ」画面(☞P59)に表示される[BSS ID]とは異なります。

5. 「情報表示」メニュー(つづき)

■ 無線UNIT

「情報表示」-「無線UNIT」

本製品に内蔵の無線LANユニットの動作状況を表示します。

無線UNIT	
情報	WIRELESS UNIT ANALOGUE
BSSID	00-90-C7-12-34-56
動作モード	54Mbps (802.11g)
チャンネル	2462MHz (11CH)

※「無線設定」メニュー→「無線LAN」画面→[無線LAN設定]項目→[使用モード]欄(P44)を「OFF」に設定されているときは、「無線UNITを使用していません。」を[情報]欄に表示します。

このとき、本製品の無線通信機能は、停止していることを示しています。

※「無線設定」メニュー→「無線LAN」画面→[無線LAN設定]項目→[使用モード]欄を「Site Survey」に設定されているときは、[無線UNIT]項目が表示されません。

■ パケット情報

「情報表示」-「無線UNIT」

本製品に内蔵の無線LANユニットが送受信したデータの中で、パケットの種類ごとに情報を表示します。

パケット情報					
	総数	マルチキャスト	管理フレーム	エラー	
受信	369097		39	2232	1337
送信	741305		1323	1380	0

※「無線設定」メニュー→「無線LAN」画面→[無線LAN設定]項目→[使用モード]欄(P44)を「Site Survey」に設定されているときは、[パケット情報]項目が表示されません。

3 設定画面について

5. 「情報表示」メニュー(つづき)

■ 端末情報

「情報表示」-「無線UNIT」

各無線LAN端末との通信情報を表示します。

※「無線設定」メニュー→「無線LAN」画面→「無線LAN設定」項目→「使用モード」欄(※P44)を「Site Survey」に設定されているときは、「端末情報」項目が表示されません。

端末情報				
① AID	② RSSI	③ 受信レート	④ MACアドレス	⑤ 能力
1	32	11Mbps (802.11g)	00-90-C7- 99-4D-79	PrivacyInvoked ▼

- ① **AID** 無線LAN端末の識別ID(Association-ID)を表示します。
- ② **RSSI** 無線LAN端末から受信した電波の強さを表示します。
※数値が大きいほど、電波強度が強いことを示しています。
- ③ **受信レート** 無線LAN端末からの受信レートを表示します。
- ④ **MACアドレス** 無線LAN端末のMACアドレスを表示します。
- ⑤ **能力** 無線LAN端末が使用できる機能を一覧で表示します。
※一覧を見るときは、テキストボックスの▼をクリックします。
PrivacyInvoked : データ通信に暗号化を使用できます。
ShortPreamble : ショートプリアンプルを使用できます。
ShortSlotTime : ショートスロットタイムを使用できます。

【ショートプリアンプルについて】

プリアンプルは、送信データへ付加する同期信号のことです。

「ショートプリアンプル」と「ロングプリアンプル」があり、「ショートプリアンプル」を使用すると通信効率は向上しますが、ノイズなどの影響を受けやすくなります。

【ショートスロットタイムについて】

802.11gでもオプションによりスロットタイムを802.11aと同じ9 μ sに設定することで(標準は20 μ s)、802.11aと同じ実効速度を実現する機能です。

5. 「情報表示」メニュー(つづき)

■ サイトサーベイ

「情報表示」-「無線UNIT」

サイトサーベイ(電波環境調査)の結果を表示する画面です。

※「無線設定」メニュー→「無線LAN」画面→「無線LAN設定」項目→「使用モード」欄(☞P44)を「Site Survey」に設定したとき表示されます。

① No	② チャンネル	③ RSSI	④ BSSID	⑤ 暗号化	⑥ SSID
1	01CH (2412 MHz)	2800-90-C7-		WEP	WirelessA
2	02CH (2417 MHz)	100-90-C7-		WEP	WirelessB

- ① No チャンネル番号の小さい順に表示します。
※チャンネル番号が同じ場合は、電波を検出した順に表示します。
- ② チャンネル 検出された機器の無線チャンネルを表示します。
- ③ RSSI 検出された機器から受信した電波の強さを表示します。
※数値が大きいほど、電波強度が強いことを示しています。
- ④ BSSID 検出された機器の[BSSID]を表示します。
- ⑤ 暗号化 検出された機器が通信で使用する暗号化方式を表示します。
※「WEP RC4」、または「OCB AES」のときは、「WEP」と表示します。
- ⑥ SSID 検出された機器の[SSID]を表示します。

【サイトサーベイについて】

- ◎最大64件を表示します。
- ◎同じチャンネルで使用されている無線LAN機器は、検索された順番に表示します。
- ※「Wireless Bridge」モード、「Access Point」モード、「OFF」では、使用できません。
- ※「Site Survey」モード設定中、無線接続は停止します。

3 設定画面について

5. 「情報表示」メニュー(つづき)

■ サイトサーベイの調査例について

「情報表示」—「無線UNIT」

下記の画面は、本製品の設置場所でサイトサーベイ(電波環境調査)を実行した例です。

※「無線設定」メニュー→「無線LAN」画面→「無線LAN設定」項目→「使用モード」欄(※P44)を「Site Survey」に設定したとき表示されます。

No	チャンネル	RSSI	BSSID	暗号化	SSID
1	01CH (2412 MHz)	28	00-90-C7-...	WEP	WirelessA
2	02CH (2417 MHz)	1	00-90-C7-...	WEP	WirelessB
3	02CH (2417 MHz)	8	00-90-C7-...	WEP	WirelessC
4	07CH (2442 MHz)	3	00-90-C7-...	WEP	WirelessD
5	08CH (2447 MHz)	5	00-90-C7-...	WPA-PSK(TKIP)	WirelessE
6	11CH (2462 MHz)	25	00-90-C7-...	WPA-PSK(AES)	WirelessF
7	11CH (2462 MHz)	5	00-90-C7-...	暗号なし	WirelessG
8	11CH (2462 MHz)	5	00-90-C7-...	暗号なし	WirelessH
9	12CH (2467 MHz)	17	00-90-C7-...	WEP	WirelessI
10	12CH (2467 MHz)	17	00-90-C7-...	WEP	WirelessJ

※上記の画面は、調査結果の表示例です。
実際の結果は、設置環境によって異なります。

上記画面の調査例では、本製品の無線チャンネルを「06CH(2437MHz)」に設定するとよいという目安になります。

なお、「07CH(2442MHz)」と「08CH(2447MHz)」チャンネルについては、表示された[電波強度(RSSI)]が弱い(数値が小さい)ため、「06CH(2437MHz)」チャンネルと電波干渉する影響はありません。

※「06CH(2437MHz)」チャンネルが使用されている場合でも、そのチャンネルの無線アクセスポイントが少なく[電波強度(RSSI)]が弱い(数値が小さい)場合、影響しない場合もあります。

※実際に本製品を設置する場所で調査してください。

※電波状況は、時間帯によって変化することがありますので、設置前と設置後に、ある程度間隔をおきながら数回ずつ調査することをおすすめします。

■ SYSLOG

「情報表示」—「SYSLOG」

本製品がホストに出力するログ情報を表示します。

SYSLOG	
日付・時間	内容
01/01 09:25:47	httpd: tthttpd starting on port 80
01/01 09:25:48	snmpd: NET-SNMP version 5.0.9
01/01 09:25:49	root: SB-520 Ver. 1.02 Copyright 2004-2010 Icom Inc.
01/01 09:25:49	root: System is ready.

※上記の画面は、ログ情報の表示例です。

この章では、

本製品の設定内容の保存、初期化やファームウェアのバージョンアップを確認する手順などについて説明しています。

1. 設定内容の確認または保存	72
■ 確認と保存のしかた	72
2. 保存された設定の書き込み	73
■ 書き込みかた	73
3. 設定を出荷時の状態に戻すには	74
A 〈MODE〉ボタンを使用する	74
B 設定画面を使用する	75
4. ファームウェアをバージョンアップする	76
■ ファームウェアについて	76
■ バージョンアップについてのご注意	76
■ ファイルを指定して更新する	77

4 保守について

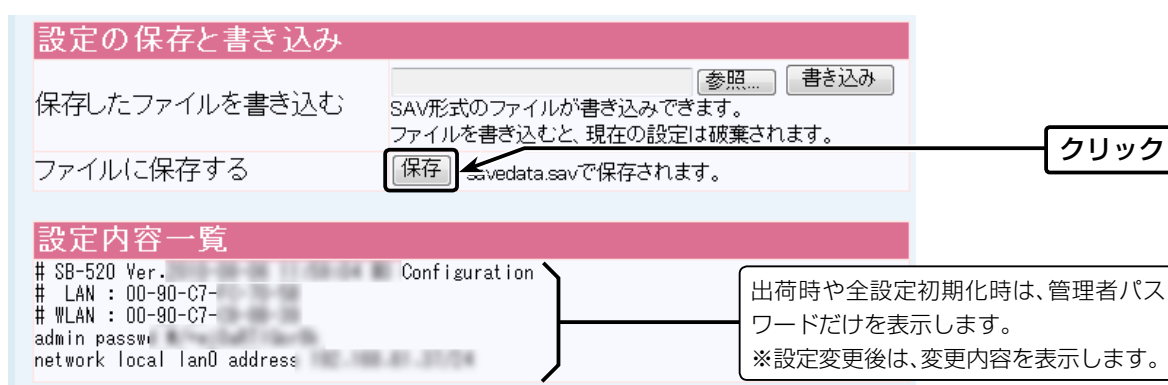
1. 設定内容の確認または保存

本製品の設定画面で変更された内容を確認して、その内容を設定ファイルとしてパソコンに保存できます。
※設定を保存しておくこと、誤って設定内容が失われたときなどに利用できます。

■ 確認と保存のしかた

「メンテナンス」→「設定保存」

- 1 本製品の設定画面にアクセスします。
- 2 「メンテナンス」メニューをクリックします。
「設定保存」画面を表示します。
- 3 [ファイルに保存する]欄の〈保存〉をクリックします。
「ファイルのダウンロード」画面(別画面)を表示します。



- 4 「ファイルのダウンロード」画面の〈保存(S)〉をクリックします。
「名前を付けて保存」画面(別画面)を表示します。
- 5 保存する場所に変更がない場合は、〈保存(S)〉をクリックします。
「.sav」の拡張子がついた設定ファイルが、選択した場所に保存されます。

2. 保存された設定の書き込み

保存した設定ファイル(※P72)を本製品に書き込む手順を説明します。

■ 書き込みかた

「メンテナンス」→「設定保存」

- 1 本製品の設定画面にアクセスします。
- 2 「メンテナンス」メニューをクリックします。
「設定保存」画面を表示します。
- 3 設定ファイルの保存先を指定するため、〈参照...〉をクリックします。
「アップロードするファイルの選択」画面(別画面)を表示します。

設定の保存と書き込み

保存したファイルを書き込む SAV形式のファイルが書き込みできます。ファイルを書き込むと、現在の設定は破棄されます。

ファイルに保存する 保存 savedata.savで保存されます。

設定内容一覧

```
# SB-520 Ver. Configuration
# LAN : 00-90-C7-
# WLAN : 00-90-C7-
admin passw
network local lan0 address
```

出荷時や全設定初期化時は、管理者パスワードだけを表示します。
※設定変更後は、変更内容を表示します。

- 4 保存された設定ファイルを指定して、〈開く(O)〉をクリックします。
「保存したファイルを書き込む」欄のテキストボックスに、保存先が表示されます。
- 5 「保存したファイルを書き込む」欄の〈書き込み〉をクリックします。
設定ファイルの内容を本製品に書き込みます。

設定の保存と書き込み

保存したファイルを書き込む SAV形式のファイルが書き込みできます。ファイルを書き込むと、現在の設定は破棄されます。

ファイルに保存する 保存 savedata.savで保存されます。

指定した設定ファイルの保存先(拡張子:sav)を表示します。

- 6 書き込み完了(約30秒)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。
※設定画面に戻らないときは、再起動中ですので、しばらくして再度クリックするか、下記の画面を閉じて、設定画面にアクセスしなおしてください。

本体を再起動しています。

本体の起動を確認後、[Back]をクリックしてください。

【ご注意】

本製品の設定ファイルを本製品以外の機種に書き込まないでください。
本製品の設定ファイルを本製品以外の機器に組み込んだ場合や、改変や分解したことによる障害、および本製品の故障、誤動作、不具合、破損、データの消失あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益または第三者からのいかなる請求についても当社は一切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。

4 保守について

3. 設定を出荷時の状態に戻すには

ネットワーク構成を変更するときなど、本製品の設定をはじめからやりなおすときや、既存の設定データをすべて消去したいときなど、設定内容を出荷時の状態に戻せます。

そのときの状況に応じて、次の2とおりの方法があります。

A 〈MODE〉ボタンを使用する

本製品に設定されたIPアドレスが不明な場合など、設定画面にアクセスできないとき

B 設定画面を使用する(※P75)

本製品に設定されたIPアドレスがわかっていて、そのIPアドレスで設定画面にアクセスできるとき

A 〈MODE〉ボタンを使用する

初期化すると、すべての設定項目が出荷時の状態になります。

※パソコンに設定されたIPアドレスのネットワーク部が本製品(出荷時の設定: 192.168.0.1)と異なると、本製品にアクセスできなくなりますので、必要に応じてパソコンのIPアドレスを変更してください。

- 1 SA-4(別売品)、または[IEEE802.3af]規格対応のHUBで接続された本製品の電源を入れます。

[PWR](緑)ランプの点灯と、[LAN](赤)ランプの消灯を確認します。

※SA-4、またはHUBを除くすべてのネットワーク機器を本製品からはずしてください。

- 2 ランプが全点灯(赤/緑)するまで、〈MODE〉ボタンを押します。
[PWR](緑)ランプと[MODE](緑)ランプが数回同時点滅したのち、全点灯(赤/緑)します。

※同時点滅しないときは、はじめからやりなおしてください。

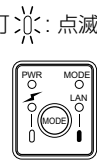
- 3 〈MODE〉ボタンから手をはなします。
ランプが全点滅(赤/緑)して、設定初期化を開始します。

- 4 [PWR](緑)ランプの点灯を確認します。
設定初期化が完了です。

【ランプの状態】

●: 消灯 ○: 点灯 ◐: 点滅

電源投入
[点灯(緑)]



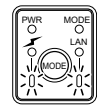
長押し
[同時点滅(緑)]



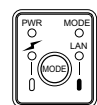
[全点灯(赤/緑)]



初期化開始
[全点滅(赤/緑)]



初期化完了
[点灯(緑)]



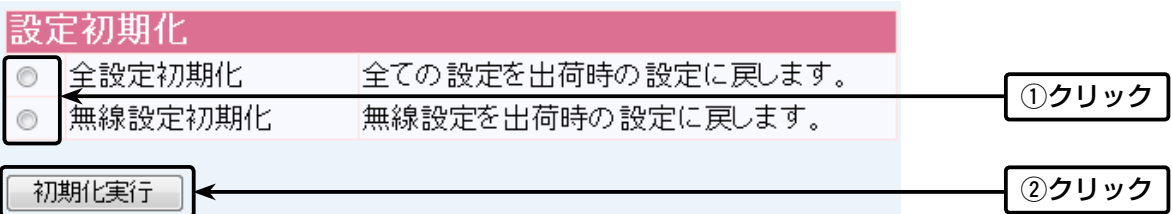
3. 設定を出荷時の状態に戻すには(つづき)

B 設定画面を使用する

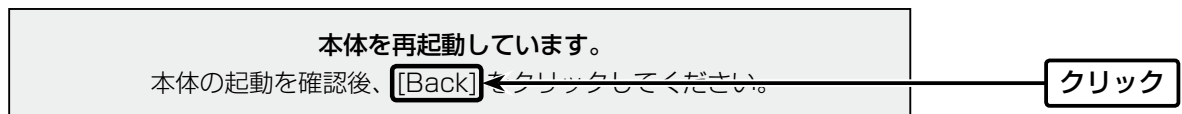
「メンテナンス」→「設定初期化」

IPアドレスが不明な場合など、設定画面にアクセスできないときは、本書74ページをご覧ください。

- 1 本製品の設定画面にアクセスします。
- 2 「メンテナンス」メニュー、「設定初期化」の順にクリックします。
「設定初期化」画面を表示します。
- 3 初期化したい条件をクリックして、「初期化実行」をクリックします。
クリックした条件に該当する設定内容が出荷時の設定に戻ります。



- 4 書き込み完了(約30秒)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。
※設定画面に戻らないときは、再起動中ですので、しばらくして再度クリックするか、下記の画面を閉じて、設定画面にアクセスしなおしてください。



【初期化の条件について】

◎ 全設定初期化をクリックした場合

本製品に設定されたすべての内容を出荷時の状態に戻します。

初期化実行後は、「192.168.0.1 (出荷時の設定)」で動作します。

初期化によって、パソコンに設定されたIPアドレスのネットワーク部が本製品と異なったときは、アクセスできなくなりますので、必要に応じてパソコンのIPアドレスを変更してください。

◎ 無線設定初期化をクリックした場合

「無線設定」メニューで設定した内容だけを出荷時の状態に戻します。

初期化実行後は、SSIDが「LG (出荷時の設定)」、暗号化が「なし」の状態で作動します。

初期化によって、パソコンに設定されたSSIDや暗号化設定が本製品と異なったときは、アクセスできなくなりますので、必要に応じて、「無線設定」メニュー、および無線LAN端末の設定を変更してください。

4 保守について

4. ファームウェアをバージョンアップする

本製品の設定画面からファームウェアをバージョンアップ(更新)できます。

■ ファームウェアについて

ファームウェアは、本製品を動作させるために、出荷時から本製品のフラッシュメモリーに書き込まれているプログラムです。

このプログラムは、機能の拡張や改良のため、バージョンアップをすることがあります。

バージョンアップの作業をする前に、本製品の設定画面にアクセスして、次のフレーム内に表示するバージョン情報を確認してください。

バージョンアップをすると、機能の追加など、本製品を最良の状態にできます。



■ バージョンアップについてのご注意

- ◎ ファームウェアの更新中は、絶対に本体の電源を切らないでください。
更新中に電源を切ると、動作しなくなるおそれがありますので、更新後、自動的に再起動するまでそのままの状態でお待ちください。
- ◎ ご使用のパソコンでファイアウォール機能が動作していると、バージョンアップできないことがあります。
バージョンアップできない場合は、ファイアウォール機能を「無効」にしてください。
- ◆ 記載する操作の結果については、自己責任の範囲となりますので、次のことを守って操作をはじめてください。
弊社ホームページ <http://www.icom.co.jp/> より提供される本製品のアップデート用ファームウェアファイルを、本製品以外の機器に書き込み、改変や分解したことによる障害、および本製品の故障、誤動作、不具合、破損、データの消失あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益、または第三者からのいかなる請求についても当社は一切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。

4. ファームウェアをバージョンアップする(つづき)

■ ファイルを指定して更新する

「メンテナンス」-「ファームウェアの更新」

バージョンアップの前に、現在の設定ファイルの保存をおすすめします。(☞P72)

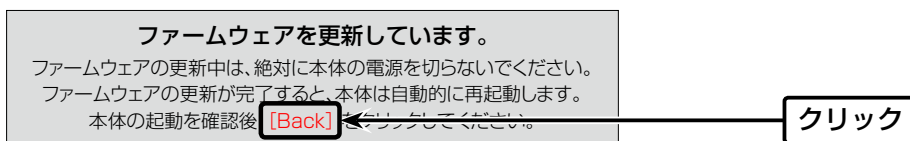
※バージョンアップ後、既存の設定内容が初期化されるファームウェアファイルがありますので、ダウンロードするときは、弊社ホームページに記載の内容をご確認ください。

※日常、設定者以外の端末からバージョンアップできないように、設定画面へのアクセス制限の設定(☞P29)をおすすめします。

- 1 本製品の設定画面にアクセスします。
- 2 「メンテナンス」メニュー、「ファームウェアの更新」の順にクリックします。
「ファームウェアの更新」画面を表示します。
- 3 <参照...>をクリックして、弊社ホームページよりダウンロードしたファームウェアファイル(拡張子:dat)の保存先を指定してから、<更新>をクリックします。



- 4 更新完了(約30秒)後、[Back]と表示された文字の上にマウスポインターを移動してクリックすると、設定画面に戻ります。



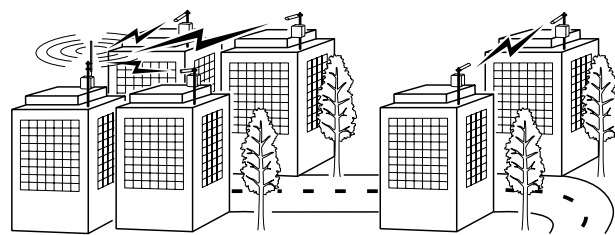
設定画面に戻らないときは、ファームウェアファイルの更新中ですので、しばらくしてから再度クリックしてください。(接続するパソコンや本製品の電源は、絶対に切らないでください。)

【ご注意】

[Back]の操作(☞手順4.)で、設定画面に戻るようになるまで、ご使用のパソコンや本製品の電源を絶対に切らないでください。

途中で電源を切ると、データの消失や誤動作の原因になります。

※出荷時の設定内容に戻るような注意書きがあるバージョンアップ用ファームウェアの場合は、[Back]をクリックしても設定画面に戻れませんので、接続するパソコンのIPアドレスを「例:192.168.0.10」に設定してから、本製品の設定画面にアクセスしなおしてください。



この章では、
設定画面の構成、設定項目の初期値、仕様などを説明しています。

1. Telnetで接続するには	80
■ Windows Vista/Windows 7の場合	80
■ オンラインヘルプについて	80
2. 設定画面の構成について	81
3. 定格について	82
一般仕様	82
有線部	82
無線部	82
SA-4(付属品)	82
4. 本製品以外の機器との無線ブリッジ接続について	83
5. 弊社製無線LAN端末との通信について	83
6. 本製品で使用しているソフトウェアのライセンス情報について	84
GNU GPL に関するお知らせ	84

1. Telnetで接続するには

Telnetでの接続について説明します。

ご使用のOSやTelnetクライアントが異なるときは、それぞれの使用方法をご確認ください。

■ Windows Vista/Windows 7の場合

お使いいただくときは、「コントロールパネル」→「プログラム」→「Windows の機能の有効化または無効化」から、「Telnetクライアント」を有効にしてから、下記の手順で操作してください。

【設定のしかた】

- ① Windowsを起動します。
- ② [スタート](ロゴボタン)から[プログラムとファイルの検索]を選択します。
名前欄に「Telnet.exe」と入力し、[Enter]キーを押します。
※ Windows Vistaをご使用の場合は、[スタート](ロゴボタン)から[検索の開始]を選択します。
- ③ Telnetクライアントが起動しますので、下記のように入力します。
Microsoft Telnet>open 本製品のIPアドレス(入力例:open 192.168.0.1)
- ④ 下記を入力して[ENTER]キーを押すと、ログインできます。
login:admin
password:空白(何も入力しない)
※ 出荷時や全設定初期化時は、本製品のPasswordを設定していません。
※ passwordは、本製品の設定画面にある「システム設定」メニューで設定された内容と同じです。
- ⑤ ログインメッセージ(SB-520 #)が表示されます。

■ オンラインヘルプについて

Telnetを使用したターミナルソフトの接続では、オンラインで、コマンドリファレンスを参照できます。

コマンド一覧……………	[Tab]キーを押すと、使用できるコマンドの一覧が表示されます。 コマンド名の入力につづいて[Tab]キーを押すと、サブコマンドの一覧が表示されます。
コマンドヘルプ……………	コマンドの意味を確認したいときは、コマンド名の入力につづけて[?]キーを押すとコマンドのヘルプが表示されます。
コマンド名の補完……………	コマンド名を先頭から数文字入力し[Tab]キーを押すと、コマンド名が補完されます。 入力した文字につづくコマンドが1つしかないときは、コマンド名を最後まで補完します。 例) d[Tab]→date 複数のコマンドがあるときは、コマンドの候補を表示します。 例) s[Tab]→save system

2. 設定画面の構成について


本製品の全設定を初期化したとき、WWWブラウザに表示される画面構成です。

設定メニュー	設定画面	設定項目	
ネットワーク設定	LAN側IP	本体名称	
		VLAN設定	
		ルーティングモード設定	
		IPアドレス設定	
	DHCP	DHCPサーバー設定	
		静的DHCPサーバー設定	
	ブリッジ	ブリッジ設定	
	RIP	RIP設定	
	ルーティング	インターフェース リスト	IP経路情報
			スタティックルーティング設定
無線設定	無線LAN	BSSID 無線LAN設定	
	暗号化	暗号化設定	
		RADIUS設定	
		WEPキー	
	MACフィルタリング	無線端末間通信設定 MACアドレスフィルタリング設定	
無線ブリッジ	無線ブリッジ	BSSID ステーションリスト 登録済み端末リスト	
システム設定	本体管理	管理者ID設定 管理者IP設定	
	時計	自動時計設定 内部時計設定	
	SYSLOG	SYSLOG設定	
	SNMP	SNMP設定	
情報表示	ネットワーク	インターフェース リスト インターフェース情報	
	無線UNIT	無線UNIT パケット情報 端末情報	
SYSLOG	SYSLOG		
メンテナンス	設定保存	設定の保存と書き込み 設定内容一覧	
	設定初期化	設定初期化	
	ファームウェアの更新	ファームウェアの更新	

5 ご参考に

3. 定格について

一般仕様

電	源: PoE (IEEE802.3af 準拠 最大10W) ※SA-4(付属品)使用時は、AC100V±10% 最大20W
使 用 環 境	温度-20~50℃(電源投入、1時間放置後★)、0~50℃(コールドスタート時) ★-20℃~0℃の環境で電源を入れたときは、[PWR(緑)]ランプの点灯、または設定画面へのアクセスを確認後、通信を開始する前に1時間以上放置してから、本製品をリセット(再起動)すること 湿度5~95%(結露状態を除く)
外 形 寸 法	140(W)×120(H)×53.5(D)mm ※取り付け金具、突起物を除く
適 合 マ ス ト 径	φ40~60mm
重	量: 約830g(本体接続LANケーブル/取り付け金具を含む)
適 合 規 格	クラスA情報技術装置(VCCI)
インターフェース	状態表示ランプ[PWR(緑)、MODE(緑)、LAN(赤)、  (赤)]、<MODE>ボタン
防 水 レ ベ ル	JIS保護等級4(防まつ形)相当

有線部

通 信 速 度	10/100Mbps(自動切り替え/半二重)
インターフェース	RJ-45型プラグ×1(LANケーブル5m付き) ※極性(クロス/ストレート)自動認識 ※IEEE802.3/10BASE-T準拠 ※IEEE802.3u/100BASE-TX準拠 ※IEEE802.3af準拠
透過プロトコル	IPv4(ルーティングモード時)

無線部

国 際 規 格	IEEE802.11b/g準拠
国 内 規 格	ARIB STD-T66
インターフェース	アンテナコネクタ(SMA-J型×1)
使用周波数範囲	2412~2472MHz
通信速度(理論値)	最大54Mbps(IEEE802.11g規格) 最大11Mbps(IEEE802.11b規格)

SA-4(付属品)

入 力 電 圧	DC12V±5% ※付属のACアダプターを使用時
出 力 電 圧	DC48V±10%
接 地 方 式	マイナス接地
使 用 環 境	温度0~40℃、湿度5~95%(結露状態を除く)
外 形 寸 法	110(W)×36(H)×71(D)mm(突起物を除く)
重	量: 約130g(本体のみ)
インターフェース	[POWER]ランプ [LAN]ポート(RJ-45型)×2 ※IEEE802.3ab/100BASE-T準拠 ※IEEE802.3/10BASE-T準拠 ※IEEE802.3u/100BASE-TX準拠

※定格・仕様・外観などは、改良のため予告なく変更する場合があります。

4. 本製品以外の機器との無線ブリッジ接続について

(2010年10月現在)

本製品以外と無線ブリッジ接続できる弊社製機器は、SB-510、SB-510EA、SB-5100だけです。

5. 弊社製無線LAN端末との通信について

(2010年10月現在)

本製品の「Access Point」モードで「IEEE802.11b/g」規格の無線LAN端末と通信するとき、パソコンに装着する無線LANカードやWIRELESS LAN UNITは、下記の弊社製品がご使用いただけます。

◎「IEEE802.11b/g」規格準拠製品

SE-800、SE-80M、SE-80、SE-56W、SE-50W、SE-50、SU-80、SU-50W、SL-5300W、SL-5200W、SL-5200、SL-5100、SL-5000XG

◎「IEEE802.11b」規格準拠製品

SU-12、SL-5000、SL-120、SL-110、SL-12、SL-11

【暗号化対応表】

弊社製無線LANカードやWIRELESS LAN UNITが対応する暗号化方式は、下記のとおりです。

無線LAN製品	暗号化方式 なし	WEP RC4			OCB AES	TKIP	AES
		64bit	128bit	152bit	128bit		
SL-11/SL-110	○	○	○	×	×	×	×
SL-12/SL-120	○	○	○	×	×	×	×
SU-12	○	○	○	×	×	×	×
SL-5000	○	○	○	○	○	×	×
SL-5000XG	○	○	○	○	○	×	×
SL-5100	○	○	○	○	○	×	×
SL-5200	○	○	○	○	○	○	○
SL-5200W	○	○	○	○	○	○	○
SL-5300W	○	○	○	○	○	○	○
SE-50/SE-50W	○	○	○	○	○	○	○
SE-56W	○	○	○	○	○	○	○
SE-80/SE-80M	○	○	○	○	×	○	○
SE-800	○	○	○	○	×	○	○
SU-50W	○	○	○	○	○	○	○
SU-80	○	○	○	○	×	○	○

※ 今後弊社から発売される無線LAN製品については、弊社サポートセンターにお問い合わせください。

6. 本製品で使用しているソフトウェアのライセンス情報について

GNU GPL に関するお知らせ

本製品には、以下のGNU GENERAL PUBLIC LICENSE Version2に基づきライセンスされるルーティングソフトウェアとして、zebraが含まれています。

お客様は、これらのソフトウェアソースコードの入手、改変、再配布の権利があることをお知らせします。

ライセンス情報については、下記の内容をご確認ください。

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

6.本製品で使用しているソフトウェアのライセンス情報について

GNU GPL に関するお知らせ(つづき)

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

6.本製品で使用しているソフトウェアのライセンス情報について

GNU GPL に関するお知らせ(つづき)

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.本製品で使用しているソフトウェアのライセンス情報について

GNU GPL に関するお知らせ(つづき)

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

6.本製品で使用しているソフトウェアのライセンス情報について

GNU GPL に関するお知らせ(つづき)

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
<one line to give the program's name and a brief idea of what it does.>  
Copyright (C) 19yy <name of author>
```

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

6.本製品で使用しているソフトウェアのライセンス情報について

GNU GPL に関するお知らせ(つづき)

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

【ソースコードの入手方法について】

本製品で使用されているGPLライセンスのソースコードの入手先については、下記の弊社サポートセンターにお問い合わせください。

お問い合わせ先： アイコム株式会社 サポートセンター
0120-156-313 (フリーダイヤル)
◆携帯電話・PHS・公衆電話からのご利用は、
06-6792-4949 (通話料がかかります)
受付 (平日 9:00~17:00)
電子メール:support_center@icom.co.jp
アイコムホームページ:http://www.icom.co.jp/

なお、これらのソフトウェアのソースコードの内容についてのご質問には、お答えしかねますのであらかじめご了承ください。

また、弊社が所有権を持つソフトウェアコンポーネントについては、ソースコードの開示対象ではありません。

高品質がテーマです。

