

無線 LAN 対応ケーブルモデム

CBW38G4J

上級者権限マニュアル



<目次>

1	安全にお使いいただくには.....	3
2	機器の各種設定について.....	4
2.1	ログイン方法.....	4
2.2	モデム情報.....	5
2.3	基本設定.....	6
2.4	上級者設定.....	8
2.5	無線設定.....	12



注意事項)

※本マニュアルに関する、設定方法の詳細について、弊社ではご案内が出来かねます。

※本マニュアルの設定、変更により生じた不具合・不利益に関しまして、弊社では保障を致しかねます。

1 安全にお使いいただくには

本製品を安全にお使いいただくには、下記の安全上の注意を必ずお読みいただき、ご使用下さい。

	警告	取り扱いを誤った場合、使用者が死亡または負傷する可能性が想定される場合。
	注意	取り扱いを誤った場合、使用者が障害を負う危険が想定される場合、及び物的損傷の発生が想定される場合。



警告

- ・ 電源は AC100V(50Hz/60Hz)を使用してください。
電源は電源コンセントから直接取り、タコ足配線は避けてください。
火災・感電の原因になります。
- ・ 本機に水が入ったり、本機がぬれたりしないようご注意ください。
本機の上に薬品や水などの入った容器を置かないでください。
- ・ ぬれた手で電源プラグを抜き差ししないでください。
感電の原因になります。
- ・ AC アダプタは、必ず付属の製品を使用してください。
- ・ 電源コードを傷つけたり、無理な力を加えたりしないでください。
電源プラグを抜くときは、必ずプラグを持って抜いてください。
電源コードが破損し、火災・感電の原因になります。
- ・ 本機を分解しないでください。内部に調整箇所はありません。
お客様による修理は危険ですから絶対おやめください。
点検・修理は販売店にご依頼ください。
- ・ 煙が出ている、異臭がするなどの異常状態のまま使用すると、火災・感電の原因になります。
異常に気付いた場合は、すぐに電源プラグをコンセントから抜いて、ご加入のケーブルテレビ事業者またはサービス会社に修理をご依頼ください。
- ・ 異物が本機の内部に入った場合は、電源プラグをコンセントから抜いて、ご加入のケーブルテレビ事業者またはサービス会社に修理をご依頼ください。そのまま使用すると火災・感電の原因になります。



注意

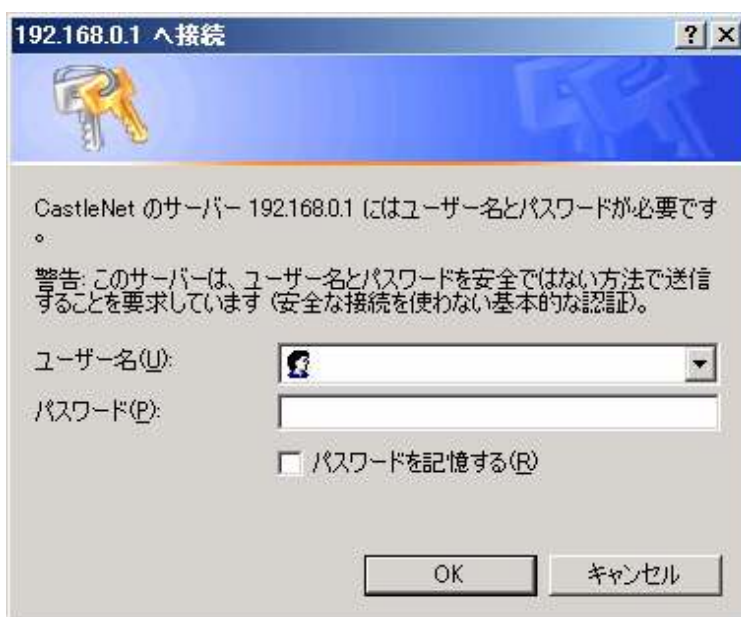
- ・ 極端な高温や低温の場所での使用や保存は避けてください。故障の原因になります。使用温度範囲は 0~40°C です。
- ・ ぐらついた台の上や、傾いた所など不安定な場所に置かないでください。
落下してけがの原因になります。
- ・ 衝撃や連続的な振動の加わる場所には設置しないでください。故障の原因になります。
- ・ 本機の上にものを載せないでください。
- ・ 直射日光の当たる場所や暖房器具などの熱器具の近くには設置しないでください。また、湿度の高い場所やほこりの多い場所は避けてください。
- ・ 本機の通気孔をふさいだり、他の機器と積み重ねて使用しないでください。
内部の温度が上がり、故障の原因になります。
- ・ 長期間ご使用にならない場合は電源プラグをコンセントから抜いてください。

2. 機器の各種設定について

本機器はパソコンと LAN ケーブルにて接続し、WEB ブラウザから設定することで、機器の状態の確認や、各種の設定を行うことができます。

2.1 ログイン方法

1. 本機器が正常に動作していることを確認し、パソコンを LAN ケーブルにて接続されている状態で、WEB ブラウザを起動させます。
2. WEB ブラウザのアドレス入力欄に <http://192.168.0.1> を入力し、移動します。
3. 下記のような、ユーザー名とパスワードの入力を求める画面が表示されます。必要な権限でのユーザー名とパスワードを入力します。



権限		出荷時設定	変更時のメモ
上級者権限	ユーザー名	admin	
	パスワード	admin	
初心者権限	ユーザー名	user	
	パスワード	user	

2.2 モデム情報

2.2.1 初期設定



モデムへのログインパスワードを変更する場合に使用します。

◇パスワードの変更方法

1. 「①変更するユーザ ID 名」に、利用するユーザー名を入力します。
2. 「②新しいパスワード」「新しいパスワードの再入力」のそれぞれに設定したい新しいパスワードを入力します。

※パスワードは16桁までの英数字が設定できます。空欄でも設定できてしまいますので注意！

3. 「③現在のパスワード」に、変更前のパスワードを入力します。
4. 画面下の【設定】ボタンをクリックします。
5. 再度ログインの画面が出ます。ユーザー名と**新しいパスワード**を入力し【OK】をクリックします。



6. 最初の「初期設定」画面に戻り、変更完了となります。

2.3 基本設定

2.3.1 基本設定情報

画面上側【基本設定】→画面左側【基本設定情報】を選択すると表示されます。

The screenshot shows a web browser window with the address bar displaying "192.168.0.1/RgSetup.asp". The page title is "Residential Gateway Configuration: Basic - Set". The navigation menu at the top includes "モデム情報", "基本設定" (highlighted), "上級者設定", and "無線設定". On the left sidebar, "基本設定情報" and "DHCP" are visible. The main content area is titled "基本設定" and "基本設定情報", with a subtitle "上位の接続とRFゲートウェイの基本的な設定情報". Below this, the "ネットワーク設定" section is shown, including "WAN" settings:

IPアドレス:	221.118.67.122
MACアドレス:	00:1c:7b:6d:f5:23
リース時間	D: 01 H: 00 M: 00 S: 00
リース期限:	Wed Aug 10 04:36:20 2011
IPv4 DNS Servers:	211.1.192.244 211.1.192.245

2011 Castlenet Technology. All rights reserved.

接続に関する基本内容が表示されます。

モデムが取得している IP アドレス、モデムの MAC アドレスなどが記載されています。

2.3.2 DHCP

画面上側【基本設定】→画面左側【DHCP】を選択すると表示されます。



LAN 側の内蔵 DHCP サーバの設定について記載されています。

基本的に設定を変更する必要はありません。

○DHCP サーバ機能

DHCP サーバ機能を有効にするのか、無効にするのかを設定します。

○ローカルアドレスのスタート値

DHCP にて配布する IP アドレスの最初のアドレス番号を設定します。

○払い出しアドレス数

DHCP サーバ機能にて、IP アドレスを配布する総数
(IP アドレスは、「ローカルアドレスのスタート値」から始まるアドレス番号の連番となります。)

○リースタイム

IP アドレスの貸し出し時間(リースタイム)を秒単位で指定します。

○DHCP クライアント

過去にこのモデムに接続され、記録されている機器(パソコンなど)のリストが表示されます。

→モデム内で割り振られている IP アドレスを変えたい、などの場合は、リスト右端の「選択」にチェックを入れ、【強制削除】ボタンをクリックすると、リストから削除できます。

2.4 上級者設定

2.4.1 IP アドレスフィルタ

画面上側【上級者設定】→画面左側【IP アドレスフィルタ】を選択すると表示されます。



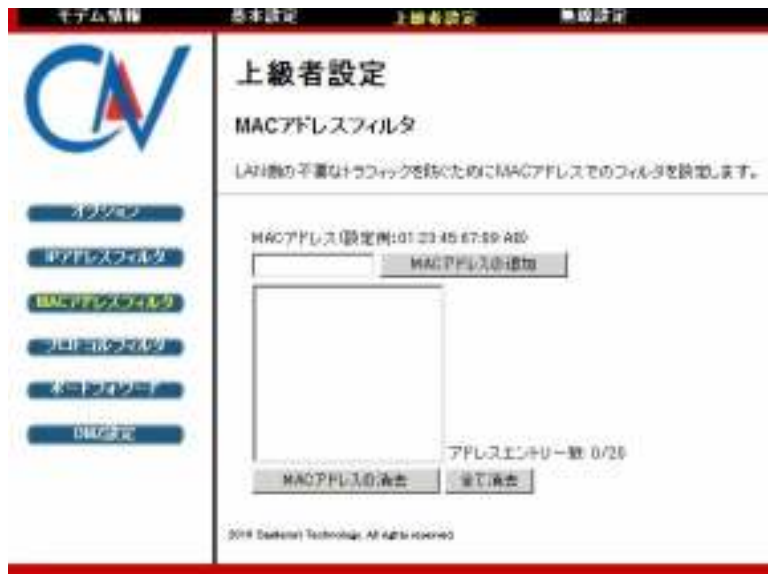
この画面で設定した「特定の IP アドレス」から外部への通信を遮断する機能です。

◇フィルタ設定を行うには

1. 「先頭アドレス」「終了アドレス」のそれぞれの値を入力します。
2. 一覧の右端の「有効化」にチェックを入れます。
3. 【設定】ボタンをクリックすると、入力された内容が反映されます。

2.4.2 MAC アドレスフィルタ

画面上側【上級者設定】→画面左側【MAC アドレスフィルタ】を選択すると表示されます。



LAN 側で利用する機器の中で、一部にフィルタをかけて、特定の接続機器の接続を遮断します。

◇フィルタ設定を行うには

- 「MAC アドレス」のすぐ下の入力欄に、フィルタをかけたい機器の MAC アドレスを入力し、【MAC アドレスの追加】ボタンをクリックします。リストに追加されたら、設定が反映されます。

2.4.3 プロトコルフィルタ

画面上側【上級者設定】→画面左側【プロトコルフィルタ】を選択すると表示されます。



LAN 側での特定のポート番号の範囲の通信を遮断します。

◇フィルタ設定を行うには

- 「先頭番号」「終了番号」を入力し、「種類」を TCP・UDP・両方のいずれかを選択します。その後、「有効化」にチェックを入れ、【設定】ボタンをクリックすると設定が反映されます。

2.4.4 ポートフォワード

上級者設定

ポートフォワード

Webサーバ、FTPサーバ等の特定のポート番号上に入ってくるリクエストを可能にします。これにより公共のインターネットからアクセス可能にします。

IPアドレス	先頭番号	終了番号	種類	有効化
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>
192.168.0.0	0	0	両方	<input type="checkbox"/>

Application	Port
HTTP	80
FTP	21
TFTP	69
SMTP	25
POP3	110
NNTP	119
Telnet	23
IRC	164
SNMP	161
Finger	79
Duress	70
Whois	43
radius	107
LDAP	389
UUCP	540

設定

特定のプロトコル番号の範囲で通信を端末に転送することが出来ます。

プロトコルの種類は、TCP もしくは UDP か、その両方を選択することが出来ます。

ポート開放を行う際などに利用します。

◇設定を行うには

- ・「IP アドレス」欄に、転送の為に利用する IP アドレスを入力します。
- ・「先頭番号」「終了番号」にて、設定するポート番号の範囲を指定します。
- ・「種類」にてプロトコルの種類を【TCP】【UDP】【両方】から選択します。
- ・「有効化」にチェックを入れ、下部の【設定】をクリックすると設定が反映されます。

2.4.5 DMZ 設定

画面上側【上級者設定】→画面左側【DMZ 設定】を選択すると表示されます。



DMZ を公開する際に設定します。

◇設定を行うには

画面上の IP アドレスを入力し、【設定】ボタンをクリックすると設定が反映されます。

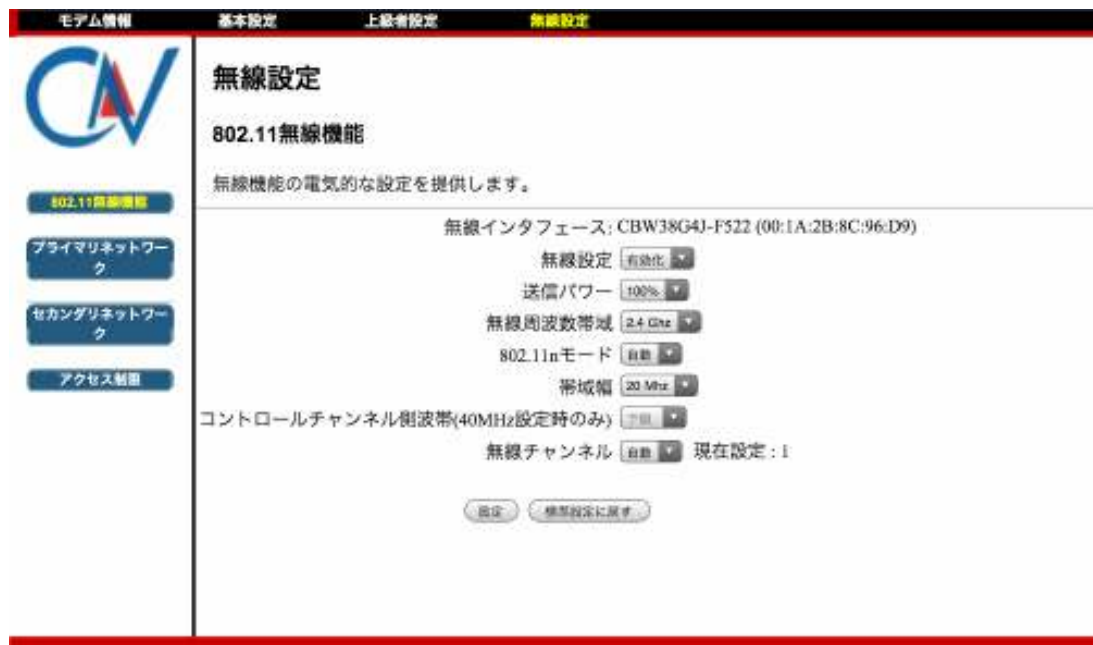
※DMZ…DeMilitarized Zone(非武装地帯)の略。

内部ネットワークと、外部ネットワークの間に設定されている、隔離された中間のネットワーク領域(サブネットワーク)のこと。コンピュータセキュリティの一種で、外部からのアクセスに対し、内部ネットワークに直接アクセスできないようにする。主にホームページサーバやメールサーバの運用に利用される。

2.5 無線設定

2.5.1 802.11 無線機能

画面上部【無線設定】→画面左部【802.11 無線機能】をクリック



無線に関する、設定の確認・変更が可能です。通常は、変更の必要はありません。

※設定を変更する場合は、各設定を選択した後【設定】ボタンをクリックします。

設定を元に戻したい場合は、そのまま【標準設定に戻す】をクリックします。

- ・無線設定（初期値:有効化）

基本的に「**有効化**」のままにします。

万が一、無線 LAN を使用したくない場合は「無効化」を選択します。

- ・送信パワー（初期値:100%）

本機器の無線送信パワーを調整します。基本、変更の必要はありません。

- ・無線周波数帯域（初期値:2.4GHz）

本機器は 802.11b/g/n 対応なので、2.4GHz 専用であり変更は出来ません。

- ・802.11n モード（初期値:自動）

802.11n 対応端末を利用する場合に設定します。基本は「自動」のままとしてください。

- ・帯域幅（初期値:20MHz）

本来は、数字が大きいほど、利用する帯域が広がり、速度が出やすくなる性質があります。

ただし、現在は、他の機器の無線通信と干渉しやすくなり、逆に速度が遅くなる可能性が高い為、基本は「20MHz」のほうが安定して速度が出ると考えられます。

- ・コントロールチャンネル側波帯(40MHz 設定時のみ)

帯域幅 40MHz 設定時に、上側か下側のどちらにチャンネルを配置するかを選択できます。

他に無線 LAN 機器がある場合、お互いの干渉を避けるために調整することが出来ます。

- ・無線チャンネル（初期値:自動）

通信する無線チャンネルを変更することが出来ます。基本は「自動」で問題ありません。

2.5.2 プライマリネットワーク

画面上部【無線設定】→画面左部【プライマリネットワーク】をクリック



LAN 側と同一ネットワークであるプライマリな無線ネットワークの設定を提供します。無線接続のネットワークの設定とセキュリティ設定について、暗号化・認証方式の変更や、暗号化キーの変更などを行うことができます。

主な機能説明

プライマリネットワーク

プライマリネットワークによるセキュリティー設定で無線接続を行うか否か設定します。

基本は【有効化】としてください。

ネットワーク名 (SSID)

32 文字までの英数字で、接続の際に利用する ID 名を設定します。

なるべく第三者が安易に想定できない SSID にすることをお奨めします。

無線端末間の通信

無線接続端末が複数存在した場合、それらの端末間での通信を許可または禁止します。

WPA (もしくは WPA2)

暗号化及び認証に別途 RADIUS サーバを使う方式です。

WPA (もしくは WPA2)-PSK

暗号化のために共有鍵を使う方式です。共有鍵自身は、WPA 暗号化キーで入力します。

WPA/WPA2 暗号化方式

暗号化の方式を選択しますが、汎用性と処理速度を考慮して AES の選択を推奨します。

WPA 暗号化キー

WPA による暗号化を行うキーを入力します。キーは8~63文字の英数字を入力します。

入力した文字は、●に置き換わりますが、入力欄の右にある“Show Key”をチェックすることで可視化出来ます。

RADIUS サーバの IP アドレス

認証に RADIUS サーバを用いる際のサーバ IP アドレス

RADIUS サーバのポート番号

認証に RADIUS サーバを用いる際のサーバ待ち受けポート番号

RADIUS サーバのキー

認証に RADIUS サーバを用いる際のサーバキー

グループキーの交換間隔

グループキーの交換間隔を秒単位で指定します。

WPA/WPA2 再認証間隔

WPA/WPA2 再認証間隔を秒単位で指定します。

WEP 暗号化

WEP を利用する場合の、暗号化キーの長さを設定します。

対応する端末のサポートできる最長のキーを選択することを推奨します。

公開鍵認証

任意: 認証の初期段階では暗号化を行わない方式。

必須: 認証の初期段階から WEP 暗号化を行って通信確立を行う方式。(推奨)

802.1x 認証

802.1x 認証を行う場合には“有効化”、行わない場合には“無効化”を選択します。

ネットワークキー

WEP 認証用のキーを入力します。キーは下記の入力規則があります。

	ASCII 設定	16進数設定
使用可能文字(数字)	半角英数	0-9、a-f
64bit 設定時	5文字	10桁
128bit 設定時	13文字	26桁

標準ネットワークキー

4セット存在するネットワークキーの内、実際に使用するネットワークキー番号

パスフレーズ

パスフレーズに、32文字以下の半角英数字を入力し、【WEP キーの生成】ボタンを押すことで、自動的にネットワークキーを生成することができます。

○ 自動セキュリティー機能

WPS(Wi-Fi Protected Setup)を使用し、対応したゲーム機などとの間で簡単にセキュリティー設定が可能です。接続する端末機器の操作方法は、接続する端末機器のマニュアルをご確認下さい。本機能を使用しない場合は“無効化”を選択します。

・ 押しボタン方式

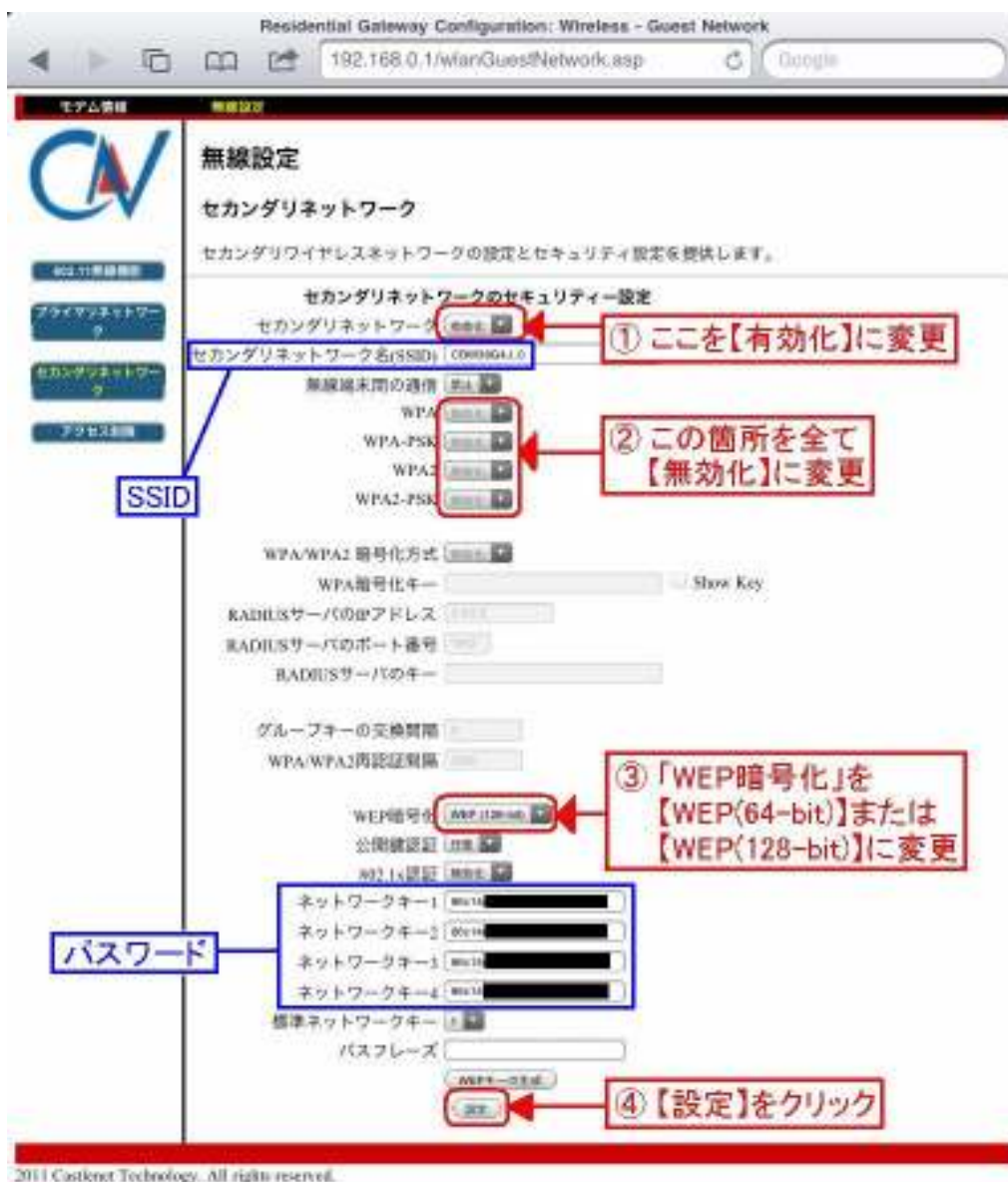
本機器の押しボタンを2秒程度押し、LED を点滅状態にします。また、同時に接続する端末機器を押しボタン方式を選択することで、自動的にセキュリティー設定が完了します。

・ PIN 入力方式

WPS 端末の追加方法を PIN と選択し、PIN の入力欄に接続する端末機器が発行する PIN 番号を入力し【追加】ボタンを押します。同時に接続する端末機器を PIN 方式を選択すると、自動的にセキュリティー設定が完了します。

2.5.3 セカンダリネットワーク

画面上部【無線設定】→画面左部【セカンダリネットワーク】をクリック



LAN 側とは別の独立したセカンダリな無線ネットワークの設定を提供します。
IP アドレスの配布はプライマリネットワークとは異なる 192.168.1.0/24 が提供されます。
各項目の詳細については『2.4.2 プライマリネットワーク』をご参照下さい。

※主に WEP しか対応していない任天堂 DS・DSLite を接続する際などに利用します。

- ① 「セカンダリネットワーク」を【有効化】に変更する
- ② 「WPA」「WPA-PSK」「WPA2」「WPA2-PSK」を全て【無効化】に変更する
- ③ ②が終わると「WEP 暗号化」が変更可能になるので、ここを【WEP(64-bit)】
または【WEP(128-bit)】に変更する
- ④ 「ネットワークキー」が自動に入力されるので、「SSID」と「ネットワークキー」をわかりやすい
書面などにメモします。【設定】をクリックして完了です
設定が完了したら、DS・DSLite にて接続設定が可能となります。

2.5.4 アクセス制限

画面上部【無線設定】→画面左部【アクセス制限】をクリック

無線設定

アクセス制限

ワイヤレスネットワークへアクセスする端末をMACアドレスで制御する設定を提供します。

無線インターフェース CBW38G4J-FE22 (00:1A:2B:8C:99:D8)

MAC限定方法 無効化

MACアドレス(例: 00:11:22:33:44:55)

接続端末	MACアドレス	Agent	BSSID/BSSID	IP Addr	Host Name	Mode	Speed (Mbps)
Android	00:11:22:33:44:55	32.0	0	192.168.0.16	yr	iPad n	65000
Android	00:11:22:33:44:55	1.92	34	0	192.168.0.11	u u n	65000

無線 LAN で接続する端末を MAC アドレスでアクセス制限できます。

各機能説明

無線インターフェース

プライマリネットワーク・セカンダリネットワークのどちらの設定を行うかを切り替えます。

なお、各ネットワークは有効化されてなければ表示されません。

インターフェース名は SSID が表示されます。

MAC 限定方法

以下の登録する MAC アドレスに対する限定のしかたを設定します。

無効化: MAC アドレスのリストを無視してアクセス制限しません。

許可: MAC アドレスリストに該当する端末のみ通信を許可します。

拒否: MAC アドレスリストに該当する端末は通信を拒否します。

MAC アドレス(例: 00:11:22:33:44:55)

各無線インターフェース毎に限定する MAC アドレスを例のようにコロン区切りで入力します。