CASIO

CASSIOPEIA
DT-10

DT-10M50S シリーズ
無線 LAN セキュリティ
設定ガイド

無線 LAN を使用するにあたって 802.1x など、
より高度なセキュリティ設定の方法に関して
説明しています。

Ver1.00

ご注意

- このソフトウェアおよびマニュアルの一部または全部を無断で使用、複製することはできません。
- このソフトウェアおよびマニュアルは、本製品の使用許諾契約書のもとでのみ使用することができます。
- このソフトウェアおよびマニュアルを運用した結果の影響については、一切の責任を負いかねますのでご了承ください。
- このソフトウェアの仕様、およびマニュアルに記載されている事柄は、将来予告なしに変更することがあります。
- このマニュアルの著作権はカシオ計算機株式会社に帰属します。
- 本書中に含まれている画面表示は、実際の画面とは若干異なる場合があります。予めご了承ください。

変更履歴

バージョン	日付	頁	説明
1.00	2008/02/08		Ver1.00 公開

目次

1. はじめに

このマニュアルは以下の機種を対象として記述されています。

<<対象機種>>
●DT-10M50S シリーズ

無線 LAN の簡単な設定方法に加え
●無線 LAN に関しての一般的なセキュリティ対策に関して
●802.1x 認証を用いた方法に関して
に対しても解説を行っています。

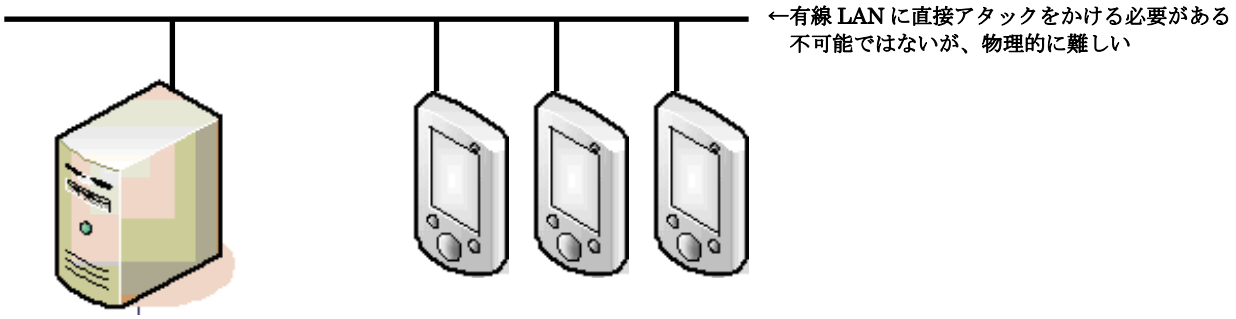
＜注意！＞
アクセスポイントの設定に関しては、ご使用のアクセスポイントの取扱説明書をご参照ください。
802.1x 認証を行う場合には、アクセスポイント側にも認証機能が必要です。
なお、弊社ではシスコ社製アクセスポイント『AIR-AP1121G-J-K9』を推奨しています。

2. 無線LANのセキュリティに関して

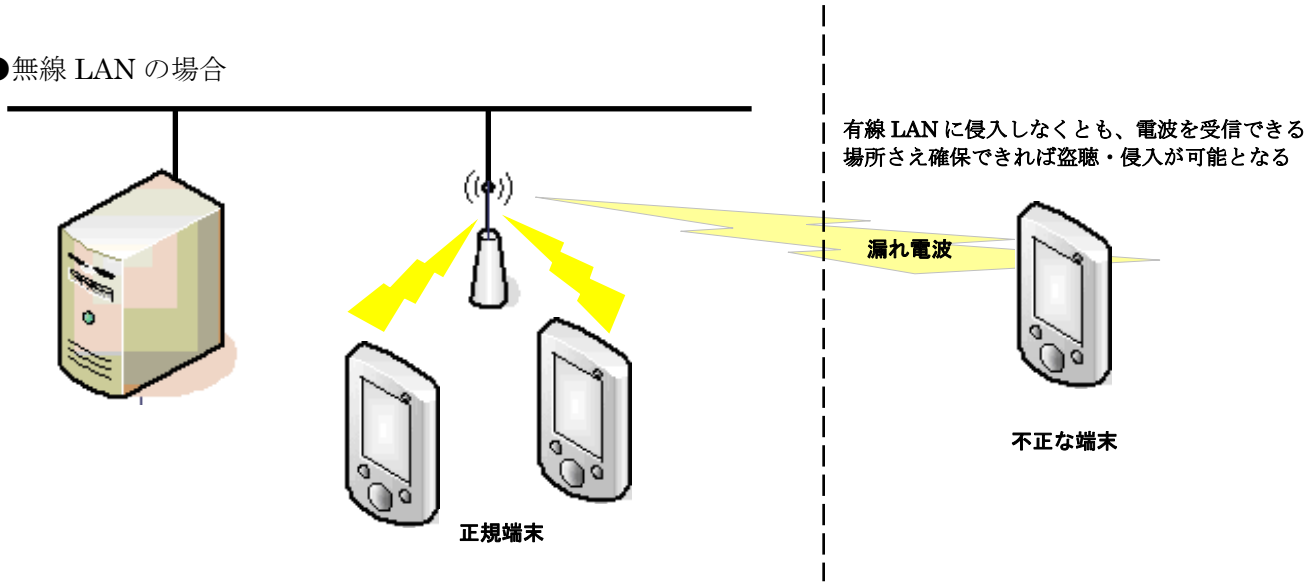
2-1.セキュリティの必要性に関して

無線 LAN は、ケーブルの設置が不要な為、モバイル端末には最適な通信方法と言えますが、
無線電波が想定作業エリア外に漏れてしまいそれを第三者に盗聴されてしまう危険性があります。
無線 LAN を使用する際は、十分セキュリティに対して考慮する必要があります。

●有線 LAN の場合



●無線 LAN の場合



上記の例でもわかるように、有線 LAN に不正に侵入する為には、実際に LAN ケーブルに接触する必要があります。
それに比較して、無線 LAN の場合には、電波を使用した通信である為、電波が届く範囲であれば盗聴自体は比較的容易です。

無線 LAN を使用する場合には、何らかのセキュリティを使用して、

①ネットワークに侵入されないようにする
②無線を盗聴されてもデータを解析されないようにする

などの対策を行う必要があります。

2-2.従来のセキュリティ

従来から一般的に行われてきたセキュリティの設定には下記の物があります。

	概要	期待される効果	脆弱性
SSID	アクセスポイントと端末で 同一の SSDI の場合のみ通信可能とする	アクセスポイントの SSID を非公開に設定することで、 外部の端末からアクセスポイントが見えなくなり、 ネットワークに侵入できなくなる	・たとえ隠していても SSID は簡単に見る事が可能 ⇒セキュリティでは無く ネットワークの識別機能と考えるべき
MAC アドレス フィルタリング	アクセスポイント側で、 特定の MAC アドレスにのみ接続可能な設定を行う	MAC アドレスは、無線 LAN 端末毎に異なる その為無関係な端末はアクセスポイントに 接続が出来なくなる	・盗聴を防ぐ事は出来ない ・端末の MAC アドレスは、盗聴などで判別出来る ・MAC アドレスの詐称は容易に行う事が可能
固定 WEP	アクセスポイントと、端末に 同じキーを設定することで データを暗号化し通信を行う	通信データが暗号化される為盗聴されても データを見ることが出来ない	・WEP キーは固定である為、時間をかければ キーの解読が可能 ・総ての端末で同じキーを使用するため端末数が 多くなるほど、解読され易くなる。 ⇒定期的にキーを変更するのが望ましい ・WEP キーの更新は、アクセスポイントと 端末総てで行う必要があり 端末が多い場合は保守に手間がかかる

現存するほぼ総てのアクセスポイントと端末では、上記の手法がサポートされていますが、
現状では、SSID や MAC アドレスフィルタリング単体では、セキュリティとは言えない状況となっています。
最低でも固定 WEP による暗号化は必須といえますが、上記のとおり万全のセキュリティとはいえません。
強いて言えば、固定 WEP で、キーを頻繁に変更する運用が、次善の策となります。

又、現在のアクセスポイントでは、固定 WEP に変わるセキュリティとして WPA-PSK と言う
セキュリティを使用できる物があります。
WPA-PSK では、暗号化に TKIP を採用しており WEP より解読が難しくなっています。

	概要	期待される効果	脆弱性
WPA-PSK	アクセスポイントと端末に設定してある 事前共有鍵（Pre-Shared Key） の一致で認証に代える **アクセスポイント・端末でのサポートが必要** **※古い製品ではサポートされていない**	・通信データが暗号化される為盗聴されても データを見ることが出来ない ・暗号化に TKIP を使用しているため アクセスポイントと端末が対応していれば 固定 WEP の手軽さとより安全な通信が可能となる	・キーが短いと解読されてしまう危険性が高い ⇒21 桁以上のキーを設定することが望ましい ・盗聴による暗号解析は難しいが、 端末の盗難など事前共有鍵（Pre-Shared Key）の 流出が発生した場合には、総ての端末と アクセスポイントに対して再設定を行う必要がある ⇒大規模ネットワークには向かない ⇒家庭用、小規模ネットワーク向け

現在 WEP によるセキュリティを行っている場合は、アクセスポイントで WPA-PSK が
サポートされている場合は、WEP から WPA-PSK へ変更することをお勧めします。

2-3.認証を伴う無線セキュリティ

上記のとおり、固定 WEP では、暗号キーが解読され易いと言うセキュリティ上の問題があります。
又、WPA-PSK では、事前共有鍵(Pre-Shared Key)が流出した場合にはそのネットワーク全体が危険にさらされます。
これを解決する為に、802.1x 認証と暗号化を組み合わせる方法が考えられます。

802.1x では、電子証明書と認証サーバを利用した認証を行います。効果としては、
・ 不正な端末によるネットワークへの侵入の防止
・ 不正なアクセスポイントによる『なりすまし』の防止
暗号化に関しては、
・ 動的 WEP を使用する事が可能となり接続毎に暗号キーを自動変更する事が可能
・ WEP よりも安全な暗号化方式 TKIP の利用が可能
となります。

802.1x では、認証方法・暗号化に関しては細かく規定をしていませんが、
無線 LAN の業界団体 Wi-Fi Alliance で規格化された **WPA(Wi-Fi Protected Access)**が、
標準的に使用されるようになって来ています。
※ **WPA** は、暗号化方式の **WEP(Wired Equivalent Privacy)**と字面は似ていますが、
全く意味は全く異なりますのでご注意ください。

DT-10M50S では、WPA-PEAP に対応しています。

	暗号化方式	認証	暗号化キー	概要	特徴
WPA-PSK	TKIP	なし アクセスポイントと 端末に設定してある 事前共有鍵 (Pre-Shared Key) の一致で認証に代える	一定時間で自動更新	固定 WEP を改善した物 アクセスポイントと端末が対応していれば 固定 WEP の手軽さとより安全な通信が可能となる	・認証サーバが不要で手軽に使用できる ・キーが短いと解読されてしまう危険性が高い ⇒21 桁以上のキーを設定することが望ましい ・認証サーバを使用せず、総ての端末で同一の キーを使用しているため、定期的にキーの 変更を行う事が望ましい ・盗聴による暗号解析は難しいが、 端末が盗まれた場合には、 残りの総ての暗号キーを再設定する必要がある ・キーの変更には総ての端末と アクセスポイントに対して行う必要がある ⇒大規模ネットワークには向かない ⇒家庭用、小規模ネットワーク向け
EAP-PEAP 動的 WEP	WEP	802.1x RADIUS サーバが必要	接続毎に変更	サーバ証明書を使用して、認証を行う	設定は、WPA と殆ど変わりません。 WEP の脆弱性を鑑み、 WPA を選択する事をお勧めします。
EAP-TLS 動的 WEP	WEP	802.1x RADIUS サーバが必要	接続毎に変更	サーバ証明書・クライアント証明書を使用して 相互に認証を行う	設定は、WPA と殆ど変わりません。 WEP の脆弱性を鑑み、 WPA を選択する事をお勧めします。
WPA-PEAP	TKIP	802.1x RADIUS サーバが必要	一定時間で自動更新	サーバ証明書を使用して、認証を行う	通常、PEAP と言えばこちらを意味します
WPA-TLS	TKIP	802.1x RADIUS サーバが必要	一定時間で自動更新	サーバ証明書・クライアント証明書を使用して 相互に認証を行う	通常、TLS といえばこちらを意味します

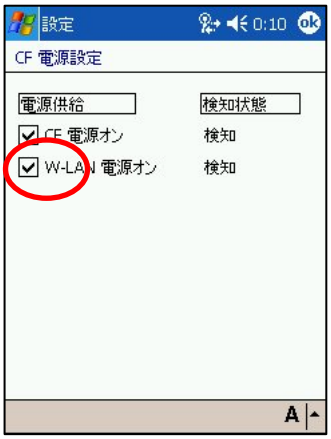
注意

802.1x 認証での運用を行う場合、認証サーバの運用が必須となります。
導入計画を行う場合、サーバ導入のハードウェア・ソフトウェアのコストのみでは無く、
サーバを運用する為の「事前検証」「導入」「運用」に対する「日程」「コスト」「人員」に関しても
考慮する必要があります。

3. 無線LANの基本設定

3-1.無線LANを有効にする

コントロールパネルから、システムタブを選択し、CF電源設定を選択します。



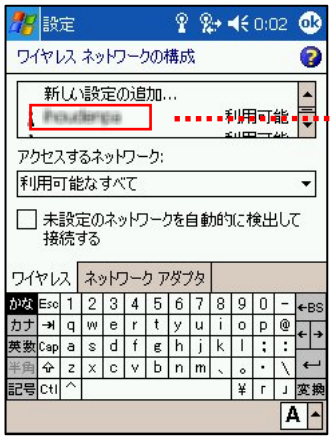
W-LAN電源オンにチェックを入れ、無線LANモジュールへ電源を供給します。

注意

無線LANモジュールに電源が供給されていないと無線LANの設定が行えません。

3-2.SSIDを設定する

コントロールパネルの接続タブから、ネットワークカードを選択します



アクセスポイントの一覧が表示されます。
接続したいアクセスポイントを選んでダブルタップして下さい。

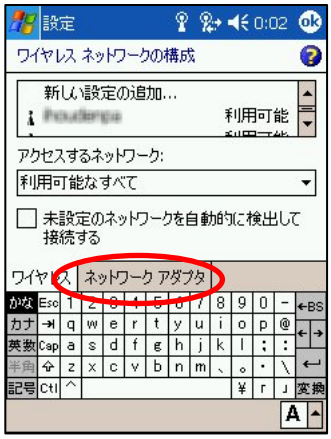
アクセスポイントのSSIDが入力されます。
名前を確認したら、OKで画面を閉じてください

SSIDが隠し設定になっている場合は一覧にSSIDが表示されません。
その場合は、新しい設定の追加を選択して、SSIDを手入力してください。

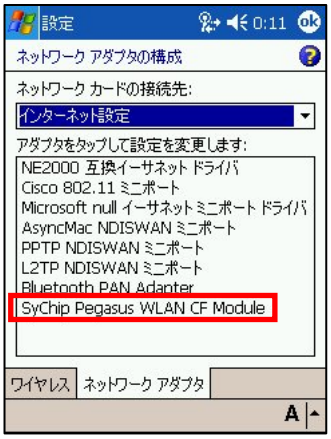
SSIDを手入力します。
その後、OKを選択して画面を閉じてください。

3-3.IPアドレスを設定する

6

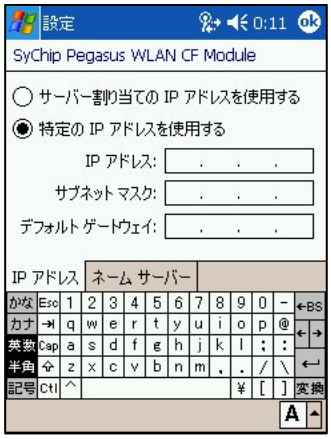


ネットワークアダプタの
タブを選択します。



無線LANアダプタを選択します。

SyChip Pegasus WLAN CF Module
を選択してください。



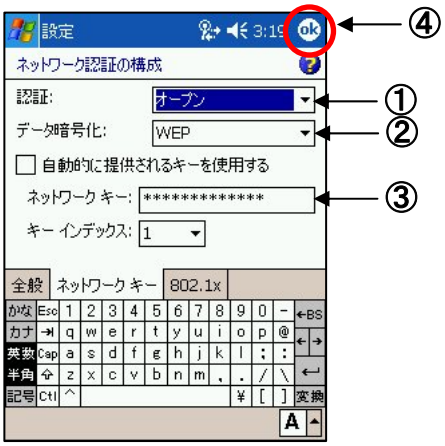
ご使用の環境に合わせて
IPアドレスの設定を行って
ください。

3-4.設定を保存する

入力した設定情報を保存します。
セキュリティの設定を行わない場合は、これでおしまいです。

4. 簡単なセキュリティの設定

4-1.WEPオープン認証



①認証は、オープンを選択します。
②セキュリティのWEPを選択します
③アクセスポイントに設定したキーを入力します。
④OKボタンを押します。

・キーは、64or128bitで選択が可能です。
・キー長は自動判別されます。
・ASCII⇔16進数は、自動判別されます。

ご注意:WEPキー長に付いて

WEPのキー長は
152bit
128bit
64bit
などがあります。

キー長	入力データ
152	128
128	104
64	40

DT-10では、キー長128bitと64bitが選択できます

WEPの暗号鍵は、初期ベクタ(24bit)＋暗号鍵(入力データ)で構成されます。
従って入力するデータ自体は、キー長から24bitを引いた物となります。
WEPキー長では、キー長と入力データ長を取り違えない様にして下さい。

例えば、WEPキー152bitの入力データと、WEPキー128bitのキー長は
共に128bitです。

WEP の現状

WEP では、アクセスポイントと端末側に設定したキーを使用して通信データを暗号化します。
現存する殆どのアクセスポイントで使用できる方法ですが、既にセキュリティの脆弱性が
指摘されており、現状ではお勧めできるセキュリティ方式とは言えなくなって来ています。
止むを得ない場合以外は次項で説明する WPA-PSK をご検討ください。

4-2.WPA-PSK

①認証でWPA-PSKを選択します
②データ暗号化でTKIPを選択します
③アクセスポイントに設定した
　キーを入力します
④OKボタンを押します。

WPA-PSK の現状

WPA-PSK は、脆弱性を指摘されている WEP から比べると強固な暗号方式となっています。
最近のアクセスポイントでは、殆どサポートされています。

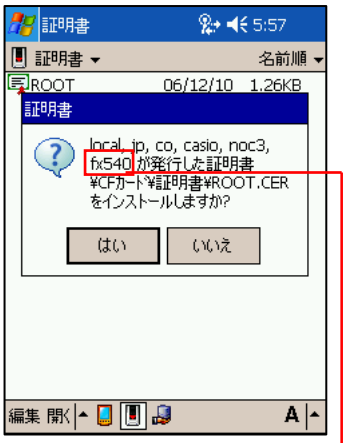
しかし、短いキーを使用した場合の脆弱性が指摘されており、
キーの長さは**最低でも 21 桁以上を設定する事**が推奨されています。

5. 802.1x認証を使用する(WPA-PEAP)

無線 LAN の設定を行う前に、証明書のインストールを行います。

5-1.証明書のインストール

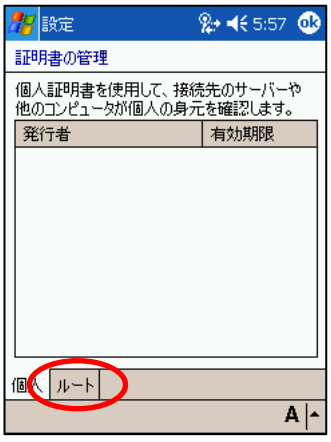
購入もしくは作成した証明書を
DT-10 にコピーし、
ファイルエクスプローラで
表示します。



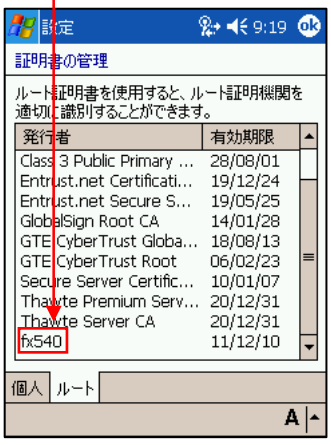
証明書を選択すると、インストー
ルを行うか聞いてきますので、
『はい』を選択してください。

5-2.証明書のインストールの確認

コントロールパネルの
システムタブを選択します。



ルートタブを選択します。

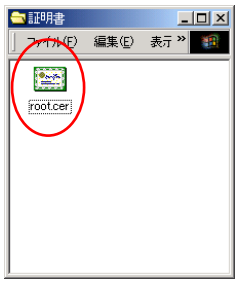


インストールした証明書が
表示されている事を確認します。

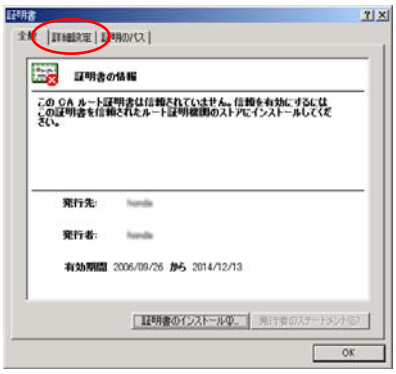
5-3.証明書が読込めない場合の対処方法

Windows Server 以外で作成された証明書では、
読込に失敗する事があります。
この様な場合は、PC を使用して下記の手順で
証明書のコピーを作成してください。

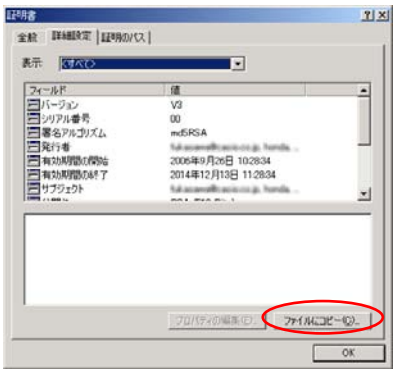
証明書のコピー方法



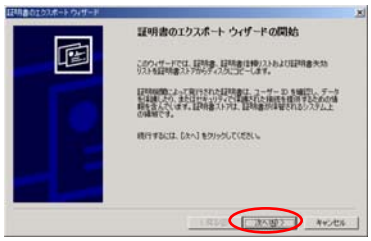
PC のファイルエクスプローラで、
ルート証明書を表示して
ダブルクリックします。



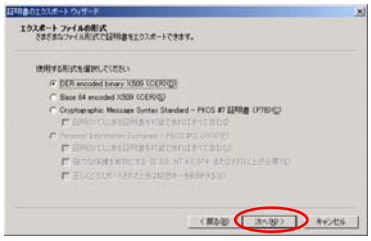
証明書のインストール画面が起動しますので、
詳細設定のタブを選択します。



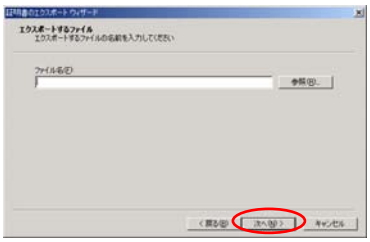
ファイルにコピーのボタンを選択します。



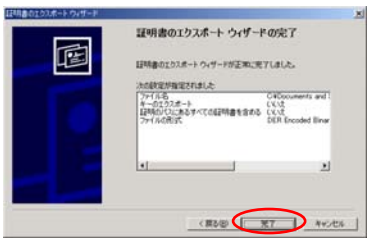
証明書のエクスポートウィザード画面
になります。
次へボタンをクリックしてください。



エクスポート形式を聞いてきます。
DER encoded binary x509(デフォルト)を
選択してください



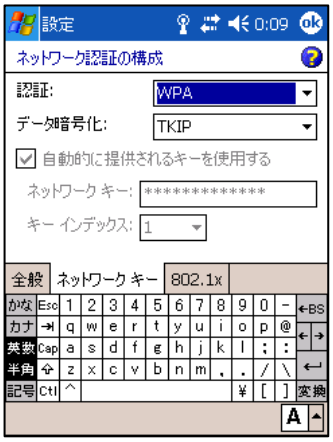
証明書のコピー先とファイル名を
入力します。



証明書のコピーを作成します。
OK ボタンをクリックしてください。
ここで作成された証明書を
DT-10 で使用します。

5-4.無線LANの設定

①コントロールパネルのシステムタブを選択します。
②ネットワークカードを選択します。
③ワイヤレスのタブを選択します。
④接続したいアクセスポイントを選択します。



①ネットワークキーのタブを選択します。
②認証は、WPAを選択します。
③データ暗号化はTKIPを選択します。

①802.1xのタブを選択します。
②EAPの種類は、PEAPを選択します。

5-5.接続

接続したいアクセスポイントを選択し、長押しをすると、接続メニューが表示されます。
接続を選択してください。

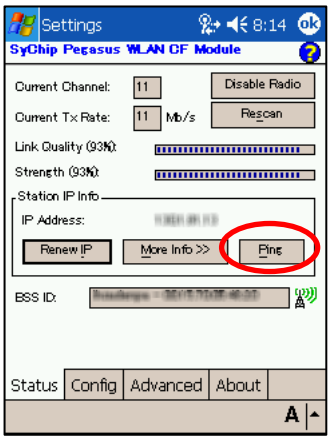
ユーザ名とパスワードを入力します。

アクセスポイントが、接続済みになっている事を確認してください。

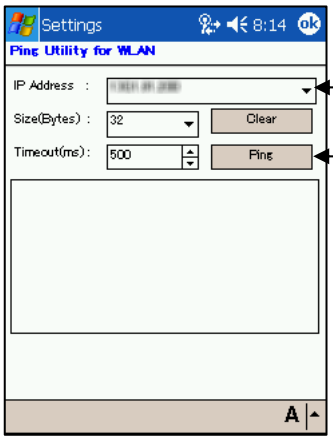
6. 無線LAN設定の確認

無線 LAN の接続の確認には、Pegasus Settings を使用します。

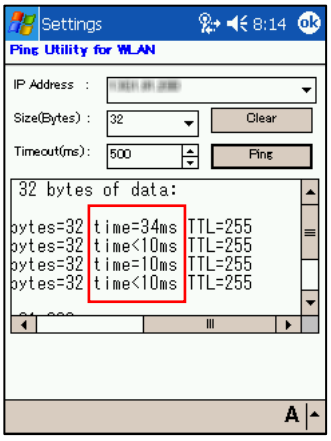
コントロールパネルの接続から
Pegasusu Settings を選択します。



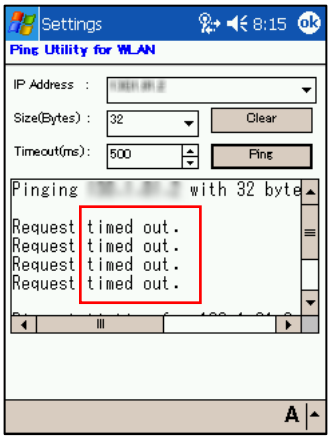
コントロールパネルの接続から
Pegasusu Settings を選択します。



①接続先の IP アドレスを入力ます。
②Ping を実行します。



接続先から応答が返っていれば
正常に接続されています。



応答が返っていない場合は、
タイムアウトとなります。
今までの設定を見直してください。

カシオ計算機お問い合わせ窓口

※平成 20 年 2 月現在

製品に関する最新情報
●法人向け製品サイト
http://casio.jp/business/

●カシオ製品サポートサイト
http://casio.jp/support/pa/

製品の取扱い方法のお問い合わせ
●情報機器コールセンター
0570-022066
市内通話料金でご利用いただけます。
携帯電話・PHS 等をご利用の場合、**048-233-7241**

カシオ計算機株式会社
〒151-8543　東京都渋谷区本町 1-6-2
TEL 03-5334-4638(代)