

CASIO®



CASSIOPEIA DT-10

DT-10M50SB 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。



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。

© 2007 カシオ計算機株式会社

Microsoft, MS, ActiveSync, Active Desktop, Outlook, Windows, Windows NT, および Windows ロゴは、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。Microsoft 社の製品は、OEM 各社に、Microsoft Corporation の 100%出資子会社である Microsoft Licensing, Inc.によりライセンス供与されています。

目次

1. はじめに	1
2. 無線LANのセキュリティに関して	2
2-1. セキュリティの必要性に関して	2
2-2. 従来のセキュリティ	3
2-3. 認証を伴う無線セキュリティ	4
3. 無線LANの設定・確認ツール (カシオオリジナル)	5
3-1. 設定ツール	5
3-2. 確認ツール	5
4. 無線LANの基本設定	6
4-1. 無線LANを有効にする	6
4-2. SSIDを設定する	6
4-3. IPアドレスを設定する	7
4-4. 設定を保存する	7
5. 簡単なセキュリティの設定	8
5-1. WEPオープン認証の場合	8
5-2. WPA-PSKの場合	9
6. 動的WEPを使用する(802.1x認証その1)	10
6-1. 設定画面	10
6-2. EAP-PEAP	11
6-2-1. 証明書の入手	11
6-2-2. ルート証明書のインポート	11
6-2-3. ワイヤレスプロパティの設定	12
6-2-4. 設定の保存	12
6-3. EAP-TLS	13
6-3-1. 証明書・秘密鍵のインポート	13
6-3-2. ルート証明書のインポート	13
6-3-3. クライアント証明書のインポート	14
6-3-4. 秘密鍵のインポート	14
6-3-5. ワイヤレスプロパティの設定	15
6-3-6. 設定の保存	15
7. WPAを利用する(802.1x認証その2)	16
7-1. EAP-PEAP	16
7-1-1. 証明書の入手	16
7-1-2. ルート証明書のインポート	16
7-1-3. ワイヤレスプロパティの設定	17
7-1-4. 設定の保存	17
7-2. EAP-TLS	18
7-2-1. 証明書・秘密鍵のインポート	18
7-2-2. ルート証明書のインポート	18
7-2-3. クライアント証明書のインポート	19
7-2-4. 秘密鍵のインポート	19
7-2-5. ワイヤレスプロパティの設定	20
7-2-6. 設定の保存	20
8. 無線LAN設定の確認方法	21
8-1. ネットサーチを起動する	21
8-2. 詳細情報を確認する	21
8-3. pingによる疎通テスト	22
8-4. SSIDが一覧に表示されない場合	22
9. IPアドレスの設定に関して	23

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-10M50SB シリーズ

上記対象機種では無線 LAN の設定を、カシオ製のオリジナルツールを用いて行います。
このマニュアルでは、

- 無線 LAN 設定 …… カシオ製の無線 LAN 設定ツール
- ネットサーチ …… カシオ製の無線 LAN 確認ツール

での無線 LAN の設定に関して解説を行っています。

合わせて、

- 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！>

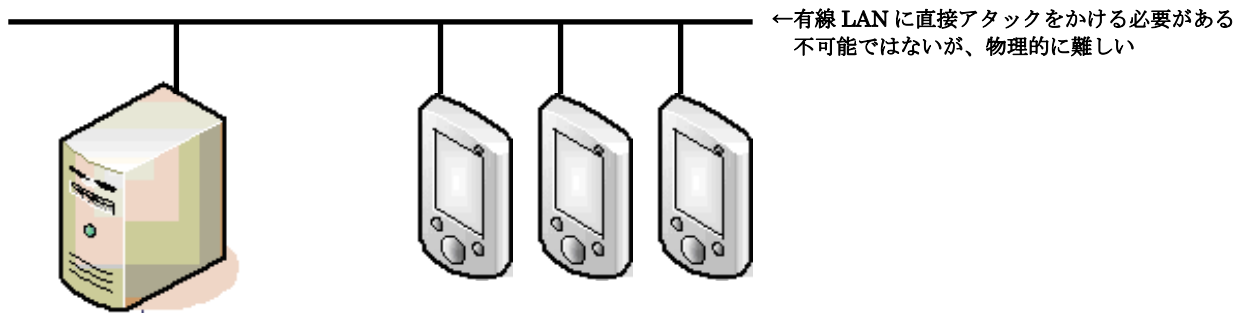
アクセスポイントの設定に関しては、ご使用のアクセスポイントの取扱説明書をご参照ください。
802.1x 認証を行う場合には、アクセスポイント側にも認証機能が必要です。
なお、弊社ではシスコ社製アクセスポイント『AIR-AP1121G-J-K9』を推奨しています。

2. 無線LANのセキュリティに関して

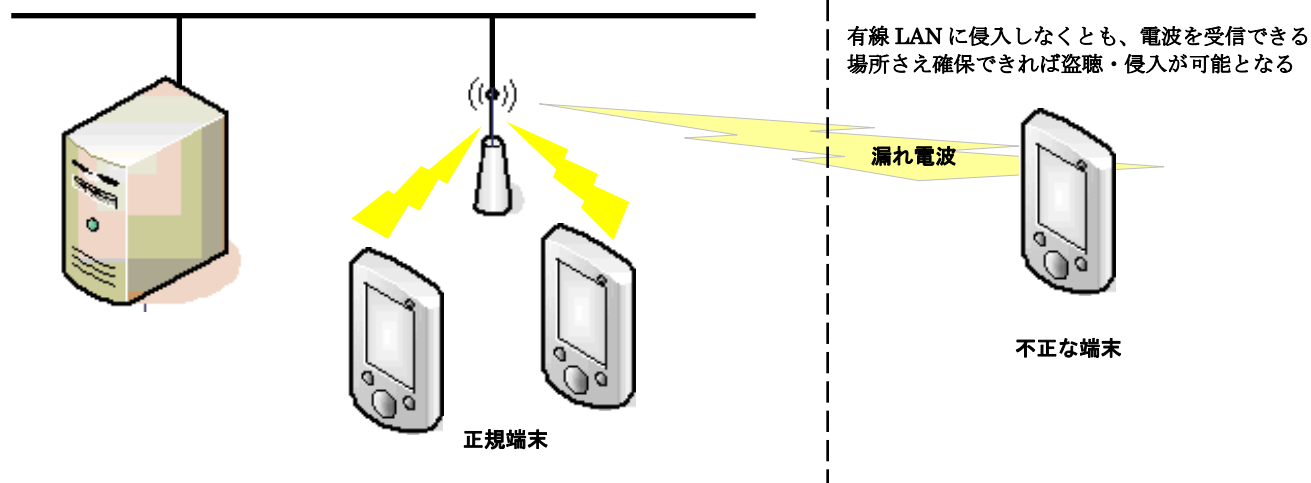
2-1.セキュリティの必要性に関して

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

従来より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 SSID 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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事が出来ない	<ul style="list-style-type: none"> 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 とい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 という手法を採用しており 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	<p>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</p> <p>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</p>	<ul style="list-style-type: none"> 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事が出来ない 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 の手軽さより安全な通信が可能となる 	<ul style="list-style-type: none"> 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

※電子証明書として、『.cer』形式の証明書、『.pvk』形式の秘密鍵をサポートしています。

他の形式の電子証明書はサポートしていません。

証明書と秘密鍵を一つにまとめた『.p12』形式などは使用できませんので、証明書の発行元より『.cer』形式と『.pvk』形式のファイルを入手してください。

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すが、無線 LAN の業界団体 Wi-Fi Alliance で規格化された WPA(Wi-Fi Protected Access)を使用する事をお勧めします。

※ 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-10M50SB で 802.1x 認証を使用する場合には、WPA(PEAP 又は TLS)での運用を推奨致します。暗号化に WEP(動的 WEP)を使用する事も可能ですが、お勧めいたしません。

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	<ul style="list-style-type: none"> ・ 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	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	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	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	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 と言えばこちらを意味します

ご注意

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」に対しても考慮する必要があります。

3. 無線LANの設定・確認ツール (カシオオリジナル)

3-1. 設定ツール

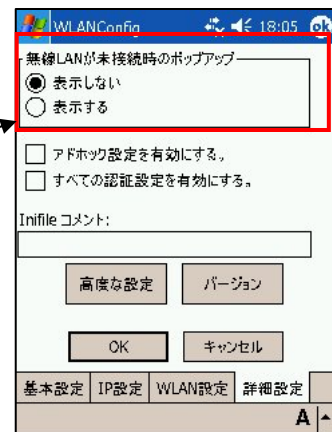
DT-10M50SB シリーズでは、カシオオリジナルの無線 LAN 設定ツールを搭載しています。



■ 特徴

- ・ 不揮発メモリに、無線 LAN の設定情報を記録する事で、電池切れなどが発生しても無線 LAN の設定は消えません。
- ・ 設定情報をコピーする事で、キッキング時の作業効率を上げる事が可能となります。
⇒設定情報は、基本的にテキストデータですが、セキュリティ事項に関しては暗号化しています。
- ・ 8021.x など高度なセキュリティに対応しています。
- ・ ご使用の電波環境に合わせて、ローミング閾値の変更やスキャン ch の制限などが可能です。

従来の DT-10 では、無線 LAN 接続のバールーン表示の抑制には、レジストリの設定、又はツールのインストールが必要でしたが、無線LAN設定ツール上の設定で抑制可能となりました。

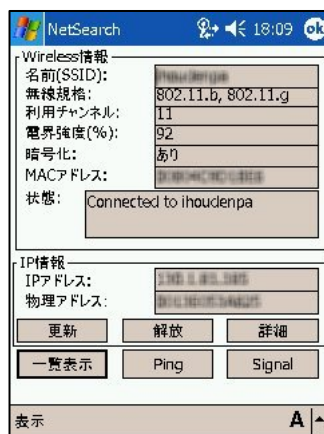


3-2. 確認ツール

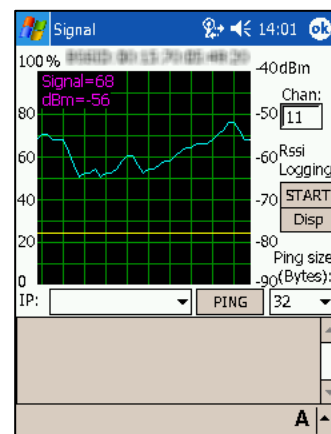
無線 LAN の確認ツールとして、ネットサーチを用意しています。ネットサーチで簡易的にアクセスポイントとの接続状態を確認する事が可能です。



周囲のアクセスポイントを一覧形式で確認できます。



接続しているアクセスポイントの詳細を確認する事が出来ます。



接続しているアクセスポイントの電波強度をグラフで表示する事が可能です。

■ ご注意：アクセスポイントが、SSIDを表示しない設定となっている場合、そのアクセスポイントのSSIDは一覧表示には表示されません。

4. 無線LANの基本設定

4-1. 無線LANを有効にする



- ①コントロールパネルから、システムタブを選択しします。
- ②CF電源設定を選択します。

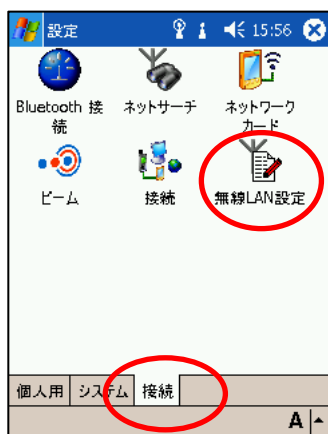


電源設定の画面が表示されます。

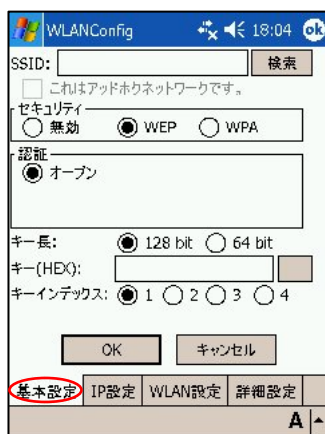
- ①W-LAN電源オンにチェックを入れます。
- ②OKボタンをタップします。

無線LANモジュールに電源が供給されていないと、無線LANが動作しないため、アクセスポイント一覧表示が出来ません。

4-2.SSIDを設定する



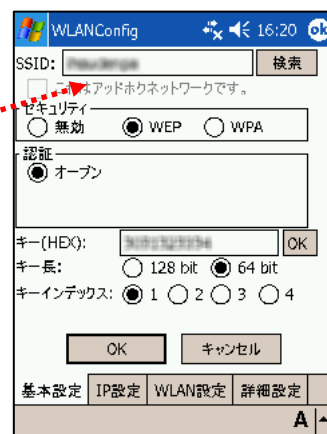
- ①コントロールパネルの接続タブを選択します。
- ②無線LAN設定を選択します



- ①基本設定のタブを選択してします。
- ②検索ボタンを選択します。



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。

アクセスポイント側でSSIDを表示しない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、SSIDを手入力してください。

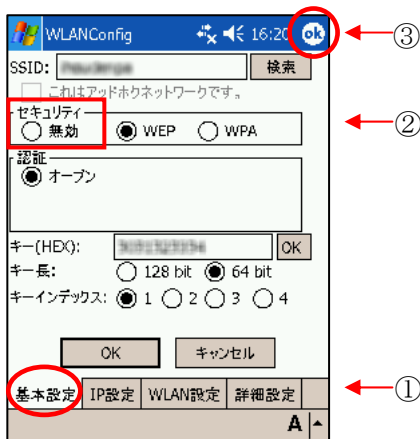
4-3.IPアドレスを設定する



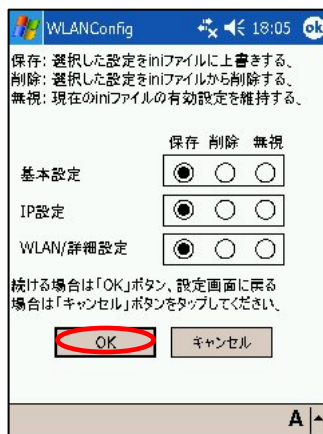
IP設定のタブを選択します。
必要に応じて、IPアドレスの設定を行ってください。

4-4.設定を保存する

セキュリティの設定を行わない場合は、これで終了です。
入力した設定情報をファイル化して保存します。
セキュリティの設定を行う場合は、以降のページの設定を行ってください。



- ①基本設定タブを選択します。
- ②セキュリティの設定を【無効】にします。
- ③OKボタンを押します。



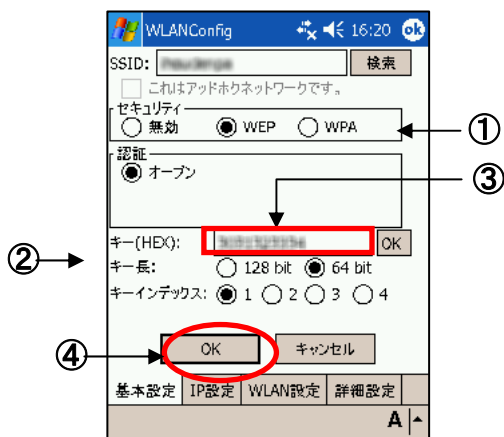
設定の保存の確認画面となります。
通常はそのままOKボタンを押します。



リセットの確認が出ます。
はいを押します。
自動的にリセットされます。

5. 簡単なセキュリティの設定

5-1.WEPオープン認証の場合



- キーは、64or128bitで選択が可能です。
必ずキー入力の前に選択してください。
キー長を変更する度にキーはクリアされます。
- キー長の自動判別はありません
必ずキー長の選択をして下さい。
- キー入力欄の隣の窓に入力桁が表示されます。
選択したキー長になるとOKと表示されます。
- ASCII⇄16進数の自動判別はありません
キーは、**必ず16進数で入力**してください。

例)

ASCII	a	b	c	A	B	C	1	2	3
16進	61	62	63	41	42	43	31	32	33

- ①セキュリティのWEPを選択します
- ②アクセスポイントに設定したキー長を選択します。
入力したキーデータからの自動判別機能はありません。
- ③アクセスポイントに設定したキーを入力します
キーは必ず16進で入力してください。ASCII入力は出来ません。
- ④OKボタンを押します。
必ず隣の表示がOKとなっている事を確認してください。

ご注意：WEPキー長について

WEPのキー長は
152bit
128bit
64bit
などがあります。

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。

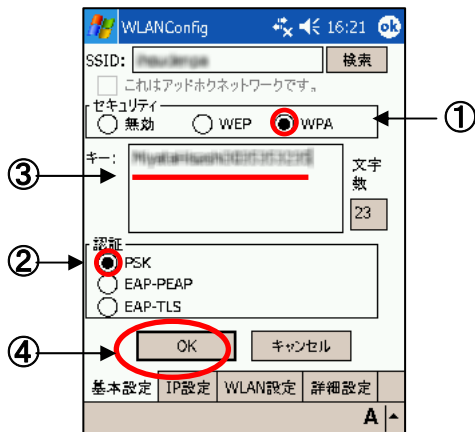
例えば、WEPキー152bitの入力データと、WEPキー128bitのキー長は
共に128bitです。

キー長	入力データ
152	128
128	104
64	40

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。

5-2.WPA-PSKの場合



- ①セキュリティでWPAを選択します
- ②認証でPSK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。

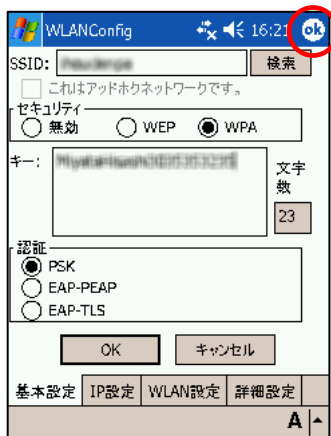
WPA-PSK の現状

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。

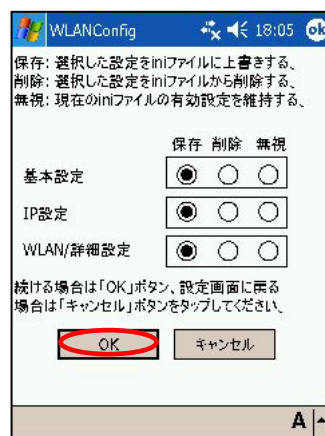
しかし、短いキーを使用した場合の脆弱性が指摘されており、キーの長さは**最低でも 21 桁以上を設定する事**が推奨されています。

5-3.設定を保存する

入力した設定情報をファイル化して保存します。



OKボタンを押します。



設定の保存の確認画面となります。通常はそのままOKボタンを押します。



リセットの確認が出ます。はいを押します。自動的にリセットされます。

6. 動的WEPを使用する(802.1x認証その1)

802.1x 認証を利用して動的 WEP を行います。

認証の方法は幾つもありますが、ここでは PEAP と、EAP-TLS を用いた方法の説明を行います。

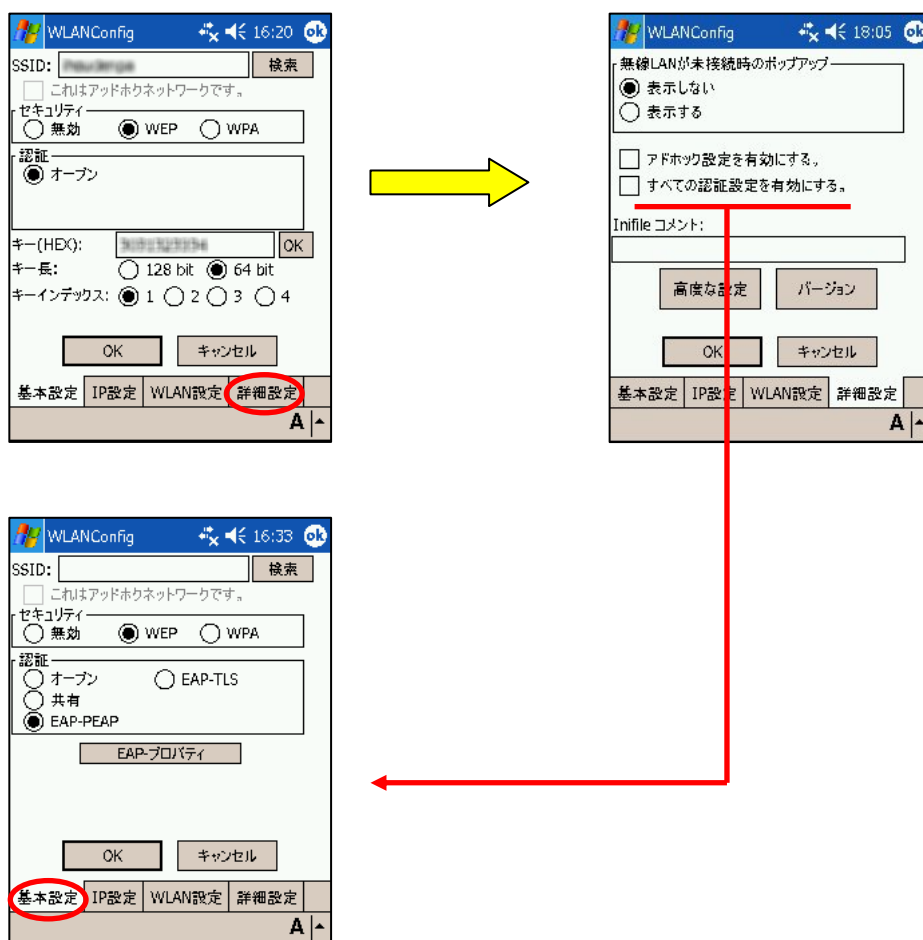
※ DT-10 では、WPA による 802.1x 認証が使用出来ます。

設定方法も殆ど同じ為、WPA を使用した 802.1x をご使用になる事を強くお勧めいたします。

6-1.設定画面

PEAP(WPA-EAP)でのワイヤレスプロパティ設定は、『セキュリティ』⇒【WEP】で行いますがデフォルトでは、オープン認証しか出来ません。下記の操作で、総ての認証方式を有効にして下さい。

- ① 詳細設定タブを選択します。
- ② すべての認証設定を有効にするに、チェックを入れます。
- ③ 基本設定タブを選択すると、認証設定の項目が増えています。
- ④ 認証で、EAP-PEAP を選択します。



6-2.PEAP

PEAP (WPA-EAP) は証明書とユーザ・パスワードを使用した認証でセキュア無線 LAN 環境を実現します。

PEAPはEAP-TLSとは異なりDT-10に*1ユーザ証明書をインポート (インストール) する必要はありませんがDT-10が認証サーバおよびAPを認証するためにサーバ証明書を使用します。

よって、DT-10にルート証明書のインポート (インストール) が必要となります。

設定手順としては、

ルート証明書をインポートした後、ワイヤレスLAN接続でのPEAP設定となります。

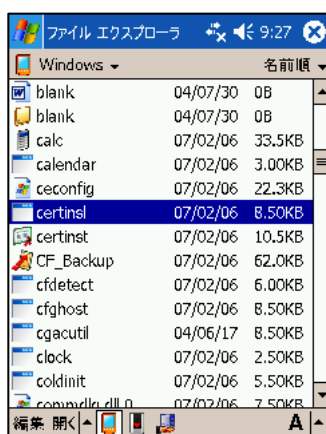
*1 認証サーバがDT-10を認証する手段はユーザ・パスワードを使用します。

6-2-1.証明書の入手

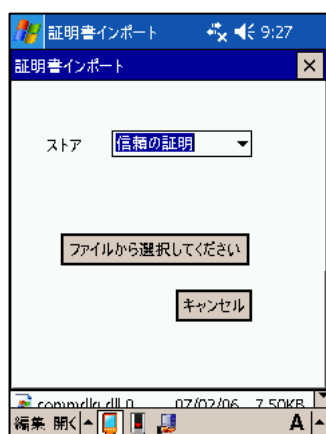
商用証明機関の証明書を購入するか、或いは自前のCAサーバを構築して証明書を作成します。

6-2-2.ルート証明書のインポート

証明書のインポートは専用ソフト【certinsl.exe】を使用します。



ファイルエクスプローラを起動して、マイデバイス → Windowsへと移動します。
Certinsl.exe を選択します。

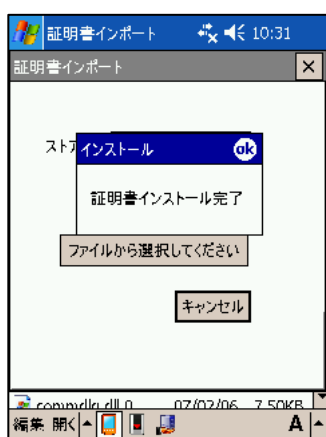


証明書インポート画面になります。

- ①【信頼の証明】を選択し、
- ②ファイルから選択してくださいをタップします。



証明書の一覧が表示されるのでインストールする証明書を選択します。

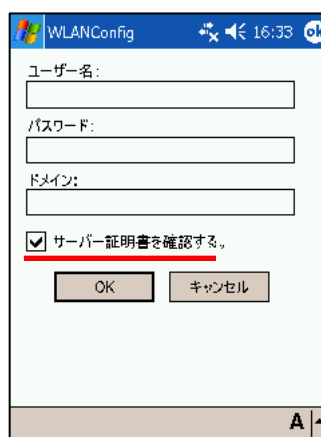
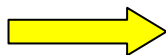


読み込みに成功すると、証明書インストール完了と、ダイアログが表示されます。
OK をタップするとプログラムが終了します。

6-2-3.ワイヤレスプロパティの設定



EAP-プロパティボタンをタップします。

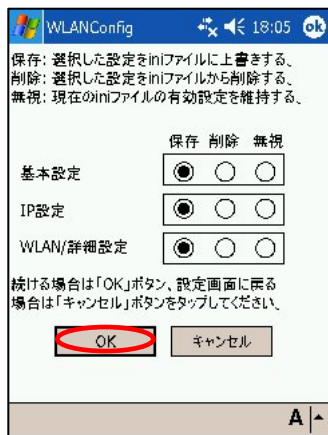


ここでは、接続時に入力するユーザ・パスワード情報をあらかじめ入力します。

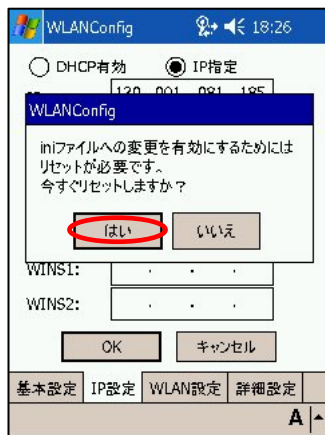
『サーバー証明書を確認する。』のチェックは、外さない事をお勧めします。このチェックが外れていると、サーバ証明書を確認なくなりセキュリティが大きく低下してしまいます。

6-2-4.設定の保存

入力した設定情報をファイル化して保存します。



設定の保存の確認画面となります。通常はそのままOKボタンを押します。



リセットの確認が出ます。はいを押します。自動的にリセットされます。

設定が終了すると、iniファイルへ保存するか聞いてきます。そのままOKとしてください。リセット後、設定が反映され使用可能となります。

6-3.EAP-TLS

EAP-TLS (WPA-EAP) は証明書を使用した認証でセキュア無線 LAN 環境を実現します。よって、まず DT-10 に証明書のインポート (インストール) が必須手順となります。設定手順としては、

DT-10 に証明書のインポート (インストール) が必要となります。

証明書・暗号鍵のインポート手順のあと EAP-TLS でのワイヤレス LAN 接続設定手順となります。

6-3-1.証明書・秘密鍵のインポート

商用認証機関の証明書を使用しない場合は、CAサーバを構築して以下の3つのファイルを作成します。

- ①ルート証明書
- ②ユーザ証明書 (クライアント証明書)
- ③^{※1} ユーザ証明書の秘密鍵

※1 ユーザ証明書 (クライアント証明書) のインポートの手順の流れで鍵のインポート時に使用します。ユーザ証明書と秘密鍵が一緒になったユーザ証明書をインポートする機能はありません。

証明書と秘密鍵は、下記の形式のファイルを別々にインポートする必要があります。

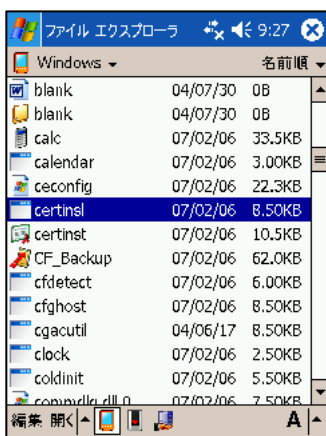
証明書の拡張子は .cer

秘密鍵の拡張子は .pvk

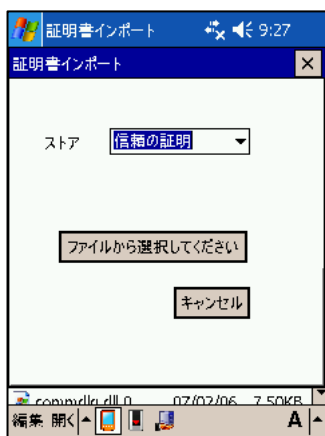
となります。

6-3-2.ルート証明書のインポート

証明書のインポートは専用ソフト【certinsl.exe】を使用します。



ファイルエクスプローラを起動して、マイデバイス → Windows へと移動します。Certinsl.exe を選択します。

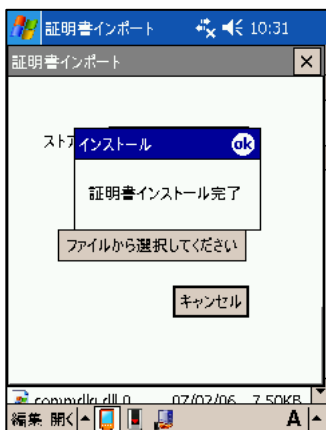


証明書インポート画面になります。

- ①【信頼の証明】を選択し、
- ②ファイルから選択してくださいをタップします。

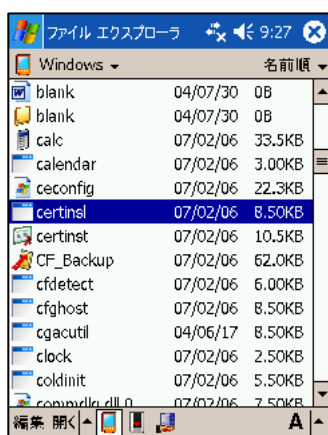


証明書の一覧が表示されるのでインストールする証明書を選択します。

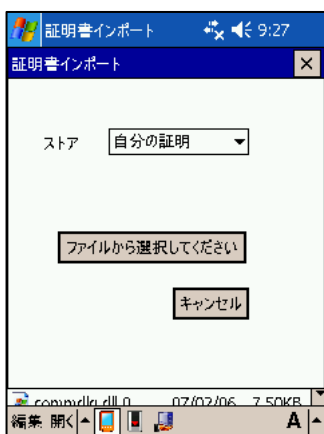


読み込みに成功すると、証明書インストール完了と、ダイアログが表示されます。OK をタップするとプログラムが終了します。

6-3-3.クライアント証明書のインポート



ファイルエクスプローラを起動して、マイデバイス → Windowsへと移動します。Certinsl.exe を選択します。

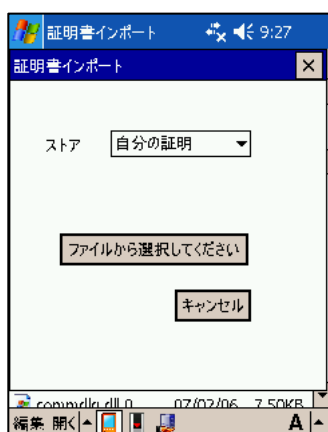


クライアント証明書をインストールします。自分の証明を選択して、ファイルから選択して下さい。をタップします。



種類 : Certificates を選択して証明書を読みます。

6-3-4.秘密鍵のインポート



秘密鍵をインストールします。自分の証明を選択して、『ファイルから選択して下さい』をタップします。



種類 : Private Keys を選択して秘密鍵を読み込んでください。

ご注意

秘密鍵にはパスワードをかけないで下さい。
DT-10 では、パスワードの掛かった秘密鍵は読み込めません。

6-3-5.ワイヤレスプロパティの設定

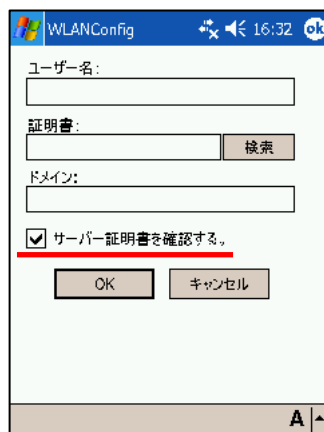
“セキュリティ” → “WEP”
“認証” → “EAP-TLS”

を選択します。

EAP-プロパティボタンをタップします。



EAPプロパティをタップします

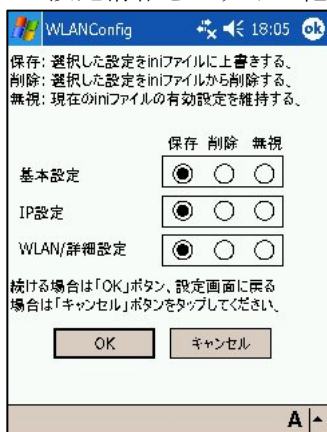


ユーザ名と、使用する証明書を選択します。

『サーバー証明書を確認する。』のチェックは、外さない事をお勧めします。このチェックが外れていると、サーバ証明書を確認なくなりセキュリティが大きく低下してしまいます。

6-3-6.設定の保存

入力した設定情報をファイル化して保存します。



設定の保存の確認画面となります。通常はそのままOKボタンを押します。



リセットの確認が出ます。はいを押してください。自動的にリセットされます。

設定が終了すると、iniファイルへ保存するか聞いてきます。そのままOKとしてください。リセット後、設定が反映され使用可能となります。

7. WPAを利用する(802.1x認証その2)

WPA を利用して 802.1x 認証を行います。

暗号化に WEP と比べより安全性の高い TKIP を使用している為、動的 WEP を使用するよりも WPAを使用することを強くお勧めします。

動的 WEP と同様に、PEAP と、EAP-TLS の二通りの認証方式を選択できます。

7-1.EAP-PEAP

PEAP (WPA-EAP) は証明書とユーザ・パスワードを使用した認証でセキュア無線 LAN 環境を実現します。

PEAPはEAP-TLSのようにDT-10 に*1ユーザ証明書をインポート (インストール) する必要はありませんがDT-10 が認証サーバおよびAPを認証するためにサーバ証明書を使用します。

よって、DT-10 にルート証明書のインポート (インストール) が必要となります。

設定手順としては、

ルート証明書をインポートした後、ワイヤレスLAN接続での PEAP 設定となります。

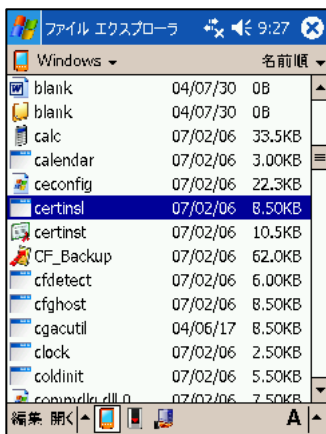
*1 認証サーバが DT-10 を認証する手段はユーザ・パスワードを使用します。

7-1-1.証明書の入手

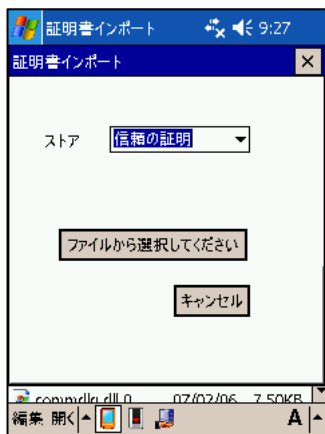
商用証明機関の証明書を購入するか、或いは自前の CA サーバを構築して証明書を作成します。

7-1-2.ルート証明書のインポート

証明書のインポートは専用ソフト【certinsl.exe】を使用します。



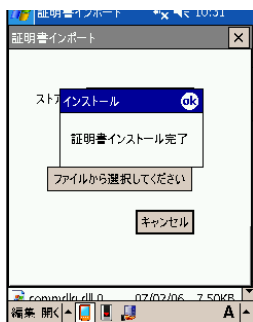
ファイルエクスプローラを起動して、マイデバイス → Windows へと移動します。Certinsl.exe を選択してください。



ルート証明書をインストールします。
【信頼の証明】を選択し、ファイルから選択してくださいをタップして下さい。

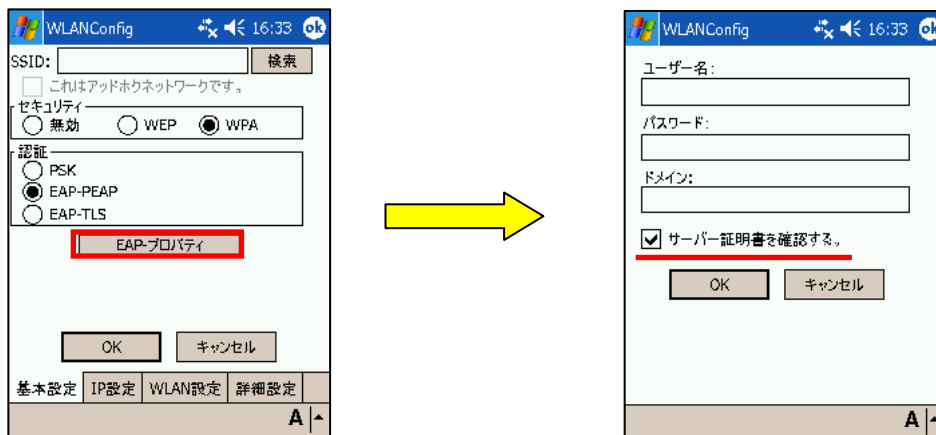


証明書の一覧が表示されるのでインストールする証明書を選択してください。



読み込みに成功すると、証明書インストール完了と、ダイアログが表示されます。OK をタップするとプログラムが終了します。

7-1-3.ワイヤレスプロパティの設定



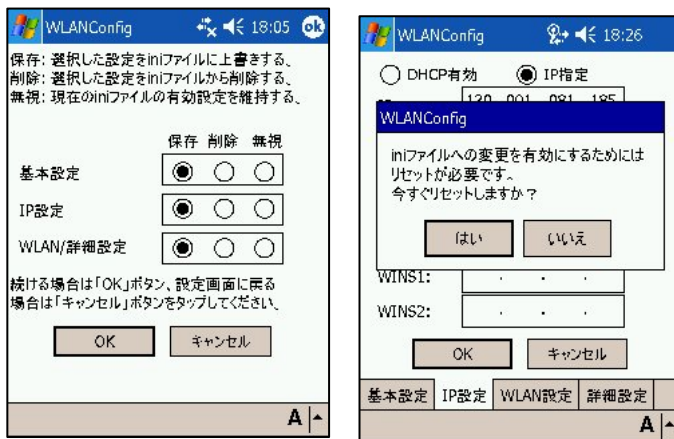
EAP-プロパティボタンをタップします。

ここでは、接続時に入力するユーザ・パスワード情報をあらかじめ入力します。

『サーバー証明書を確認する。』のチェックは、外さない事をお勧めします。
このチェックが外れていると、サーバ証明書を確認なくなりセキュリティが大きく低下してしまいます。

7-1-4.設定の保存

入力した設定情報をファイル化して保存します。



設定の保存の確認画面となります。
通常はそのままOKボタンを押してください。

リセットの確認が出ます。
はいを押してください。
自動的にリセットされます。

設定が終了すると、iniファイルへ保存するか聞いてきます。
そのままOKとしてください。
リセット後、設定が反映され使用可能となります。

7-2.EAP-TLS

EAP-TLS (WPA-EAP) は証明書を使用した認証でセキュア無線 LAN 環境を実現します。よって、まず DT-10 に証明書のインポート (インストール) が必須手順となります。設定手順としては、

DT-10 に証明書のインポート (インストール) が必要となります。

証明書・暗号鍵のインポート手順のあと EAP-TLS でのワイヤレス LAN 接続設定手順となります。

7-2-1.証明書・秘密鍵のインポート

商用認証機関の証明書を使用しない場合は、CAサーバを構築して以下の3つのファイルを作成します。

- ①ルート証明書
- ②ユーザ証明書 (クライアント証明書)
- ③^{※1} ユーザ証明書の秘密鍵

※1 ユーザ証明書 (クライアント証明書) のインポートの手順の流れで鍵のインポート時に使用します。ユーザ証明書と秘密鍵が一緒になったユーザ証明書をインポートする機能はありません。

証明書と秘密鍵は、下記の形式のファイルを別々にインポートする必要があります。

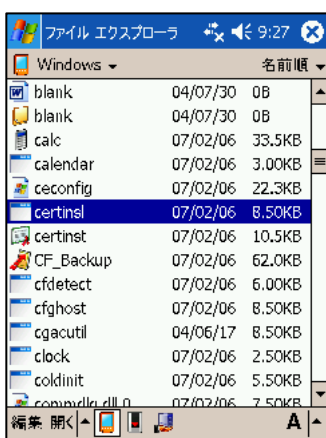
証明書の拡張子は .cer

秘密鍵の拡張子は .pvk

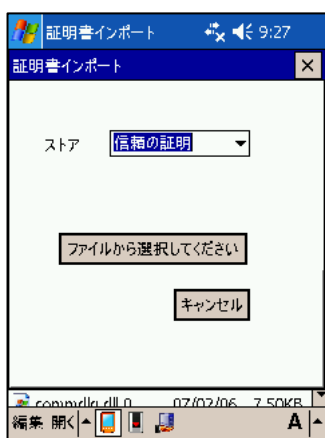
となります。

7-2-2.ルート証明書のインポート

証明書のインポートは専用ソフト【certinsl.exe】を使用します。



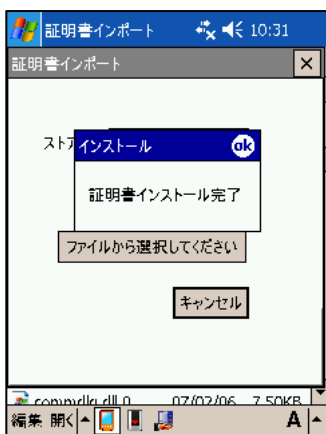
ファイルエクスプローラを起動して、マイデバイス → Windowsへと移動します。Certinsl.exe を選択してください。



ルート証明書をインストールします。【信頼の証明】を選択し、ファイルから選択してくださいをタップして下さい。

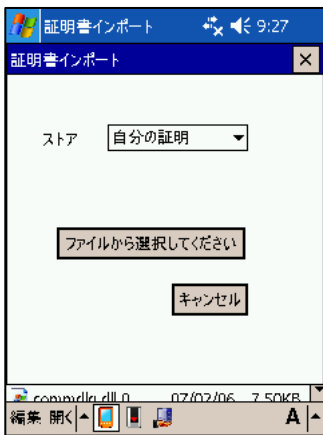


証明書の一覧が表示されるのでインストールする証明書を選択してください。



読み込みに成功すると、証明書インストール完了と、ダイアログが表示されます。OKをタップするとプログラムが終了します。

7-2-3.クライアント証明書のインポート

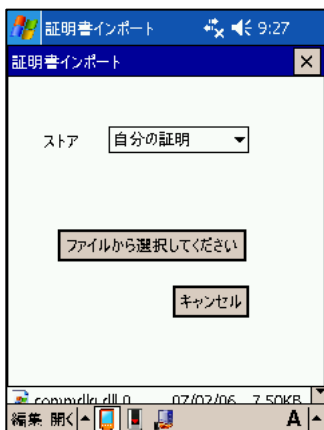


クライアント証明書をインストールします。
自分の証明を選択して、『ファイルから選択して下さい』
をタップします。



種類：Certificates を選択して
証明書を讀込んでください。

7-2-4.秘密鍵のインポート



秘密鍵をインストールします。
自分の証明を選択して、『ファイルから選択して下さい』
をタップします。



種類：Private Keys を選択して
秘密鍵を讀込んでください。

ご注意

秘密鍵にはパスワードをかけないで下さい。
現状では、パスワードの掛かった秘密鍵は讀込めません。

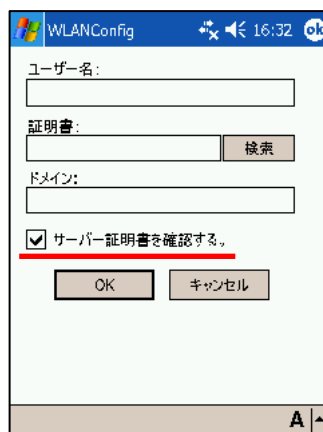
7-2-5.ワイヤレスプロパティの設定

“セキュリティ” → “WPA”
“認証” → “EAP-TLS”
を選択します。

EAP-プロパティボタンをタップします。



EAPプロパティをタップします

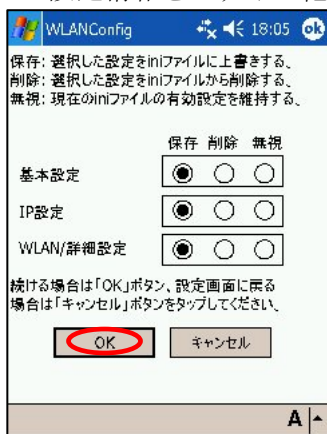


ユーザー名と、使用する証明書を
選択してください

『サーバー証明書を確認する。』のチェックは、外さない事をお勧めします。
このチェックが外れていると、サーバ証明書を確認なくなり
セキュリティが大きく低下してしまいます。

7-2-6.設定の保存

入力した設定情報をファイル化して保存します。



設定の保存の確認画面となります。
通常はそのままOKボタンを押して
ください。



リセットの確認が出ます。
はいを押してください。
自動的にリセットされます。

設定が終了すると、iniファイルへ保存
するか聞いてきます。
そのままOKとしてください。
リセット後、設定が反映され使用可能
となります。

8. 無線LAN設定の確認方法

ネットサーチを使用して、現存するアクセスポイントの一覧を表示したり接続しているアクセスポイントの電波強度を調べることが可能です。

8-1. ネットサーチを起動する

スタートメニューからネットサーチを選択します


ネットワークアイコンをダブルタップしてもネットサーチが起動します。



電界強度	局名 (SSID)	チャンネル
100	0 (%)	(ch)
88	ihoudenpa	11
0	WLANDST...	7

通信可能なアクセスポイントの一覧が表示されます。SSIDが緑ではさまれているアクセスポイントと接続しています。

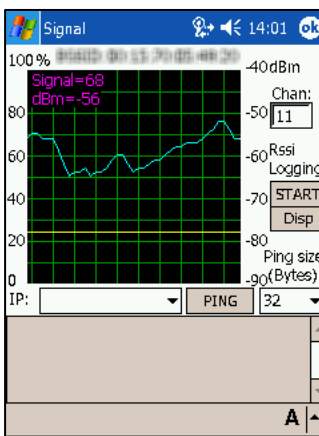
8-2. 詳細情報を確認する



Wireless情報
名前(SSID): ihoudenpa
無線規格: 802.11.b, 802.11.g
利用チャンネル: 11
電界強度(%): 92
暗号化: あり
MACアドレス: 00:0C:8C:00:00:00
状態: Connected to ihoudenpa

IP情報
IPアドレス: 192.168.1.100
物理アドレス: 00:0C:8C:00:00:00

更新 解放 詳細
一覧表示 Ping Signal



Signal

Signal=68
dBm=-56

Chan: 11

Rssi Logging
START
Disp

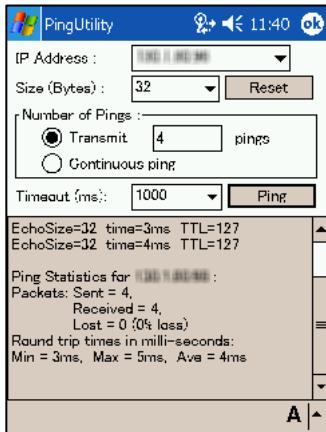
Ping size .go(Bytes):
IP: PING 32

使用中のSSIDを選択すると詳細情報が確認できます

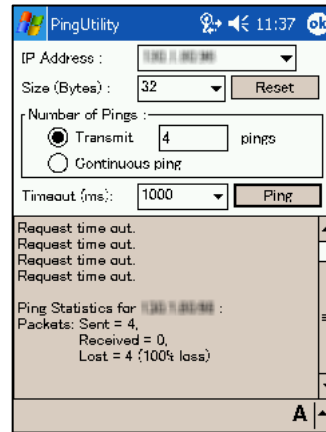
Signalボタンを選択すると電波強度の表示が出来ます

8-3.pingによる疎通テスト

ネットサーチを使用して Ping 疎通テストを行う事が可能です。

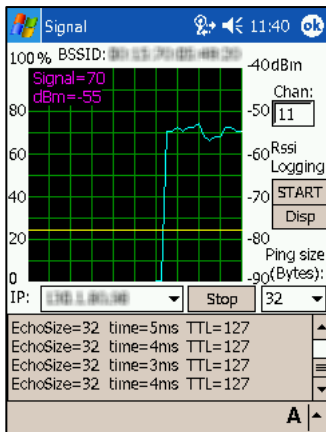


接続に成功している場合

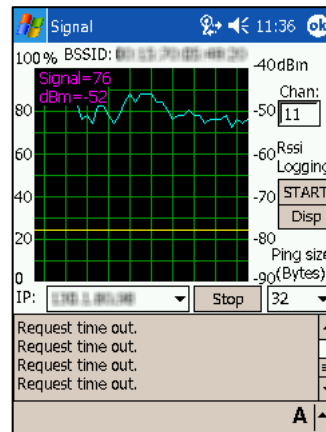


接続に失敗している場合

電波強度を表示している状態でも、Ping テストを行う事が可能です。

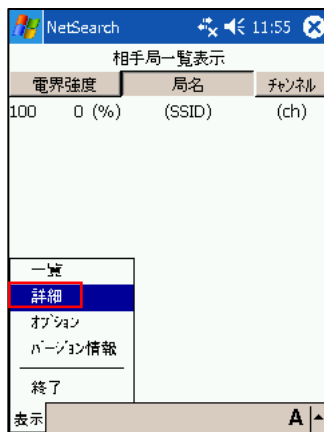


接続に成功している場合

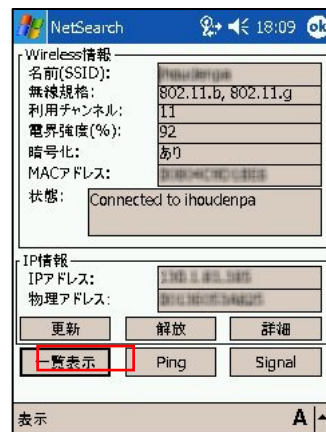


接続に失敗している場合

8-4.SSIDが一覧に表示されない場合



アクセスポイント側で SSID を表示しない設定になっている場合は、ネットサーチの一覧画面には SSID が表示されません。



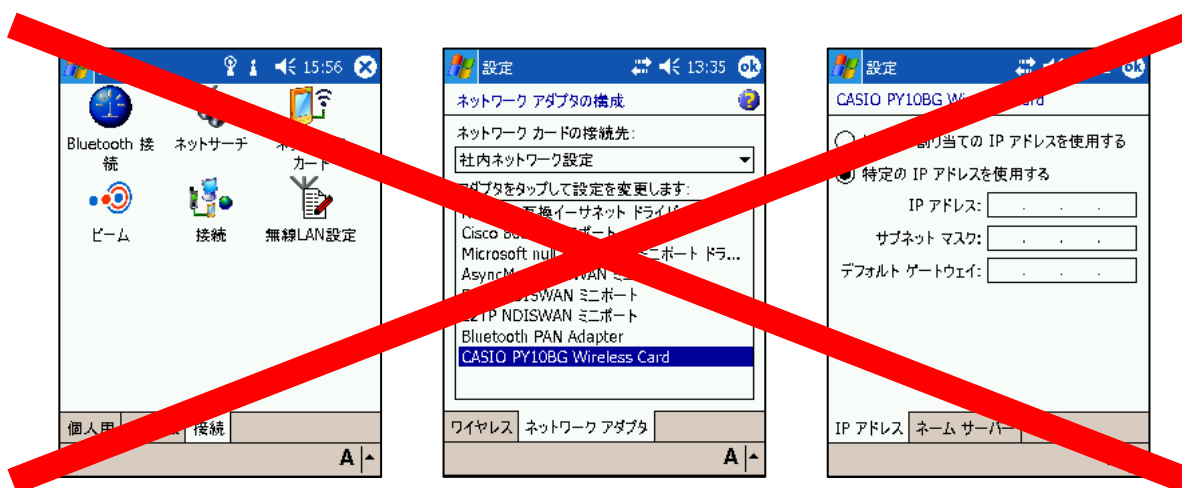
ネットサーチの詳細画面を表示することで現在接続中のアクセスポイントの情報と電波強度グラフの表示が可能となります。

9. IPアドレスの設定に関して

IPアドレスの設定は必ず無線 LAN 設定から行ってください。

スタート→設定→接続→ネットワークカード→ネットワークアダプタ

からも IP アドレスの設定は可能ですが、リセット後は無線 LAN 設定によって入力されたアドレスが有効になります。



こちらの設定は使用しないで下さい。

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

市内通話料でOK
ナビダイヤル 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)