CASIO®

CASSIOPEIA

IT-300/9000/DT-5200/5300/X7/X8 シリーズ

無線 LAN セキュリティ

設定ガイド

概要説明

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。

Ver1.07

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	2007/03/21		正式公開版
1.01	2007/08/31		対象機種に、DT-X7 を追加
1.02	2008/02/08	5	PKCS#12 形式への対応に関して追記
1.02	2008/02/08	15	『.cer』形式と『.pvk』形式のみのサポートと明記
1.02	2008/02/08	30	『.cer』形式と『.pvk』形式のみのサポートと明記
1.02	2008/02/08	最終	情報機器コールセンターの電話番号を修正
1.03	2009/06/30	1	WPA2 に関して追記（DT-X7M50SB、DT-X7M52SB のみ対応）
1.03	2009/06/30	4	WPA2 に関して追記（DT-X7M50SB、DT-X7M52SB のみ対応）
1.03	2009/06/30	5	WPA2 に関して追記（DT-X7M50SB、DT-X7M52SB のみ対応）
1.03	2009/06/30	9	WPA2 に関して追記（DT-X7M50SB、DT-X7M52SB のみ対応）
1.03	2009/06/30	29	WPA2 に関して追記（DT-X7M50SB、DT-X7M52SB のみ対応）
1.03	2009/06/30	39	WPA2 に関して追記（DT-X7M50SB、DT-X7M52SB のみ対応）
1.04	2009/10/14		対象機種に、DT-5300 を追加
1.05	2010/09/17		操作画面例に、Windows Mobile を追加
1.06	2011/03/3		対象機種に、IT-300/DT-X8 を追加
1.06	2011/03/3		操作画面例に、アクティブメニュー を追加
1.06	2011/03/3	6	AES の説明を追加
1.06	2011/03/3	8	OS、アクティブメニュー画面の説明を追加
1.06	2011/03/3	74	Ping 操作の説明機種を DT-5300 から WM 機に変更
1.06	2011/03/3	75	Ping 操作の説明機種を DT-X7/8/5300CE に変更
1.06	2011/03/3	76	IP アドレスの設定の設定に関して DT-X8/IT300 を追加
1.07	2012/03/30		対象機種に IT-9000 を追加

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-5200M50 シリーズにサービスパックを適用したもの。
- ●DT-5200M60 シリーズ
- ●DT-X7 シリーズ
- ●DT-5300 シリーズ（WM シリーズは無線 LAN 設定ツールパッチを適用したもの。）
- ●DT-X8 シリーズ
- ●IT-300 シリーズ
- ●IT-9000 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、簡単に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**』及び『**AIR-AP1131AG**』にて
動作確認を行っております。

＜注意！＞
DT-X7 は、タッチパネルを搭載していません。
画面のボタンを操作する必要がある場合には、マウスエミュレート機能をご使用ください。
※Fn＋4 で本体 10 キーの動作モードの切り替えが可能となります。
　詳しくは、DT-X7 ファーストステップガイドをご覧ください。

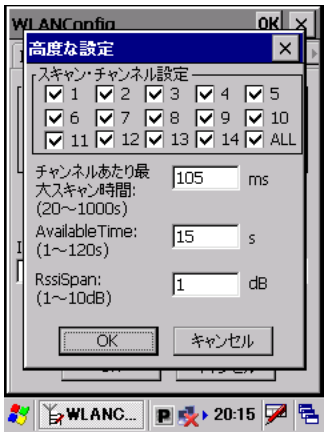
＜注意！＞
セキュリティ強化モデル **IT-300**、**IT-900**、**DT-X7M50SB**、**DT-X7M52SB**、**DT-X8 及び DT-5300** では無線 LAN の暗号化に AES を使用できます。
セキュリティの項目で、WPA を選択すると『TKIP』、WPA2 を選択すると『AES』が自動的に選択されます。
無線 LAN 設定ツールを使用する場合、WPA で『AES』を選択する事は出来ません。
WPA で『AES』を使用する場合は、無線 LAN の設定は、OS の設定ツール『NetUI』を使用してください。

2. 無線 LAN 設定ツール(カシオオリジナル)

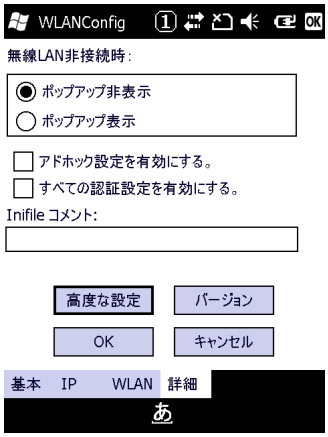
IT-300、IT-9000、DT-X7、DT-X8、DT-5200、DT-5300 では、無線 LAN の設定は、カシオオリジナルツールによる設定に変更となります。
※DT-5200M50 シリーズでは、サービスパックのインストールが必要です。

特徴

- 不揮発メモリに、無線 LAN の設定情報を記録する事で、電池切れなど不慮の事態に対応
- 設定情報をコピーする事で、キッティング時の作業効率を上げる事が可能となる
  ⇒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の設定に対応しています。
- ご使用の電波環境に合わせて、ローミング閾値の変更・スキャン ch の制限などが可能です。



CE 画面

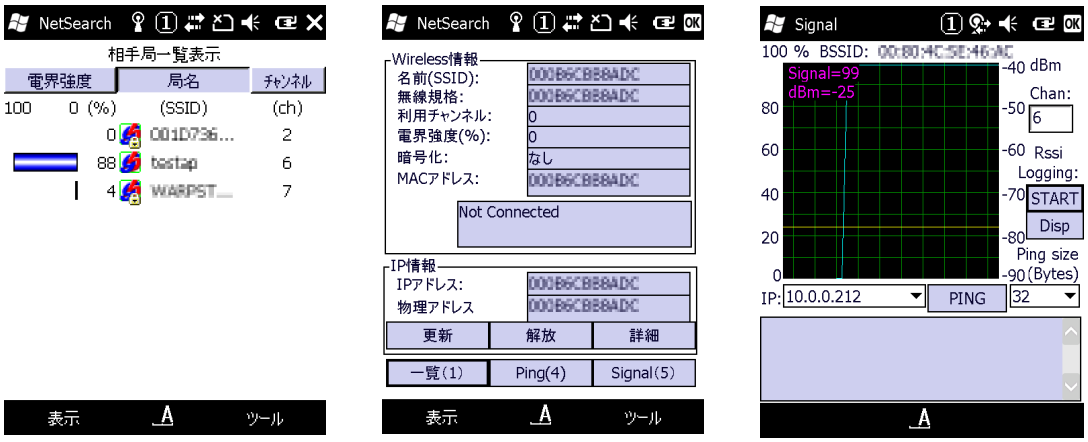


Windows Mobile 画面

- 必要に応じて、Windows 標準のツール(NetUI)を使用する事も可能です。
  特に必要が無ければ、カシオオリジナルツールでの設定を推奨します。

・　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。

CE 画面



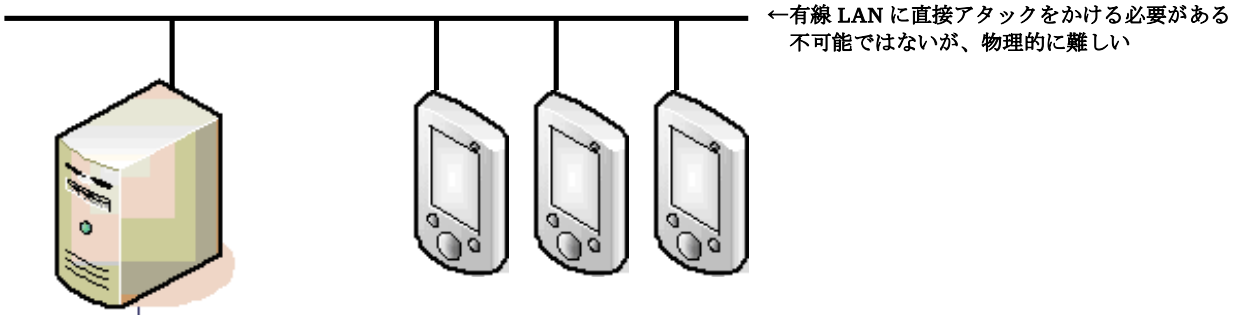
Windows Mobile 画面

3. 無線 LAN のセキュリティに関して

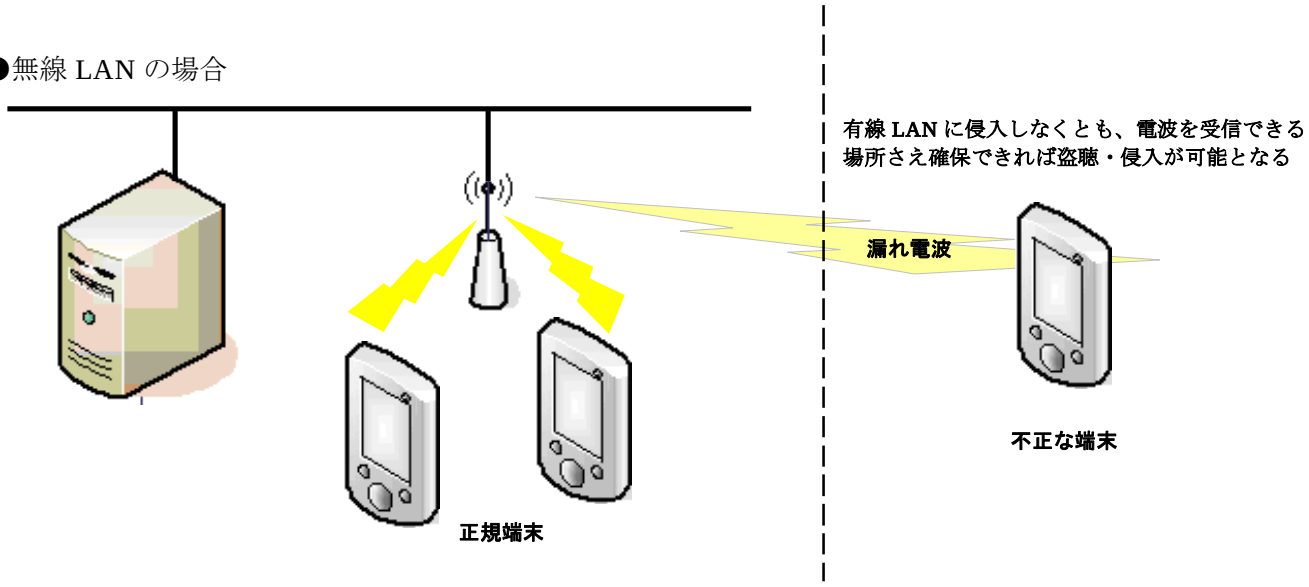
3-1.セキュリティの必要性

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。

3-2.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 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 ⇒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製品があります。
WPA-PSK では、暗号化に TKIP と言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	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。

また、セキュリティ機能強化モデルである、IT-300/IT-9000/DT-X7/DT-X7M50SB/DT-X7M52SB 及び
DT-5300 では、暗号化に AES が使用できるようになりました。
セキュリティで、WPA2 を選択する事により暗号化に AES が使用されるようになります。

	概要	期待される効果	脆弱性
WPA2 -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** **※最近の製品ならば、ほとんどサポートされている。**	・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 AES 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 ⇒大規模には向かない ⇒家庭用、小規模ネットワーク向け

3-3.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
・ セキュリティ強化モデルでは、WPA2 を選択する事により、暗号化方式に AES 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)** 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。

本機で、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、WEP の脆弱性を鑑み
極力 WPA または WPA2 をご使用になる事をお勧めします。

	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
WPA2-PSK	AES	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

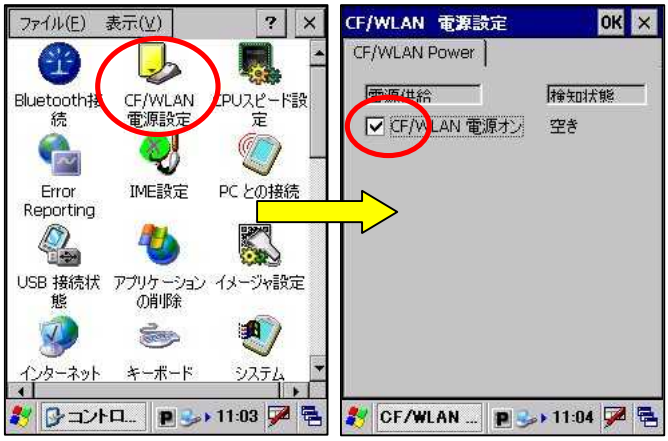
WPA2-PEAP	AES	802.1x RADIUS サーバが必要	一定時間で自動更新	サーバ証明書を使用して、認証を行う	無線暗号化に AES を使用し、サーバ認証に PEAP を使用します
WPA2-TLS	AES	802.1x RADIUS サーバが必要	一定時間で自動更新	サーバ証明書・クライアント証明書を使用して 相互に認証を行う	無線暗号化に AES を使用し、サーバ認証に TLS を使用します

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。

4. 無線 LAN の基本設定

4-1.無線 LAN を有効にする



CE 画面

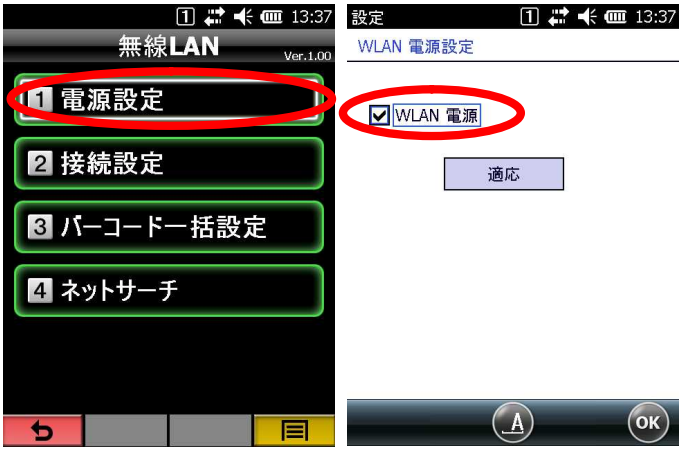
コントロールパネルから、CF/WLAN電源設定を選択して無線LANモジュールへ電源を供給します。

SSIDの設定時に、ネットサーチを使用するためです。
SSIDを手入力する場合にはこの作業は必要ありません。

Windows Mobile 画面

設定の接続から、WLAN電源設定を選択して無線LANモジュールへ電源を供給します。

SSIDの設定時に、ネットサーチを使用するためです。
SSIDを手入力する場合にはこの作業は必要ありません。



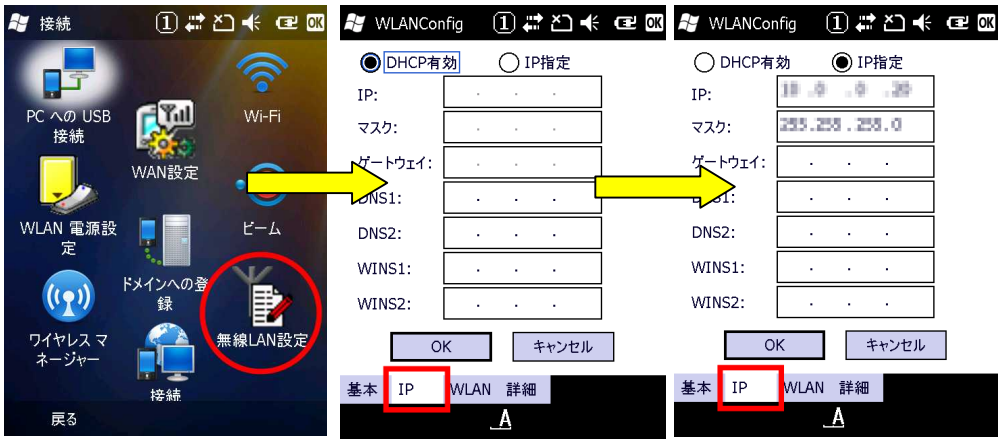
アクティブメニュー画面

アクティブメニューの設定→通信→無線LANから、電源設定を選択して無線LANモジュールへ電源を供給します。

CE_OS、WM_OS 6.0 と WM_OS 6.5 の画面は異なります。本資料では、操作説明画面例は表示項目や操作が同等の場合は CE_OS、WM_OS 6.0 の画面にて説明しています。
また、アクティブメニューは IT-300/9000,DT-X8 で利用可能なメニューシステムです。詳しくはアクティブメニューユーザーズガイドをご参照願います。

4-2.IP アドレスを設定する

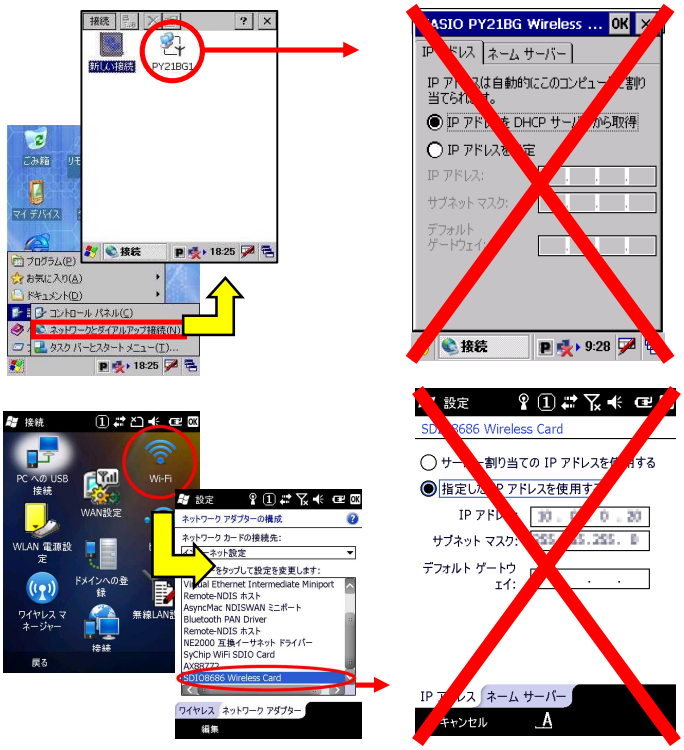
CE 画面



Windows Mobile 画面

アクティブメニュー画面

コントロールパネルから、無線LAN設定を選択します。
必要に応じて、IPアドレスの設定を行ってください。

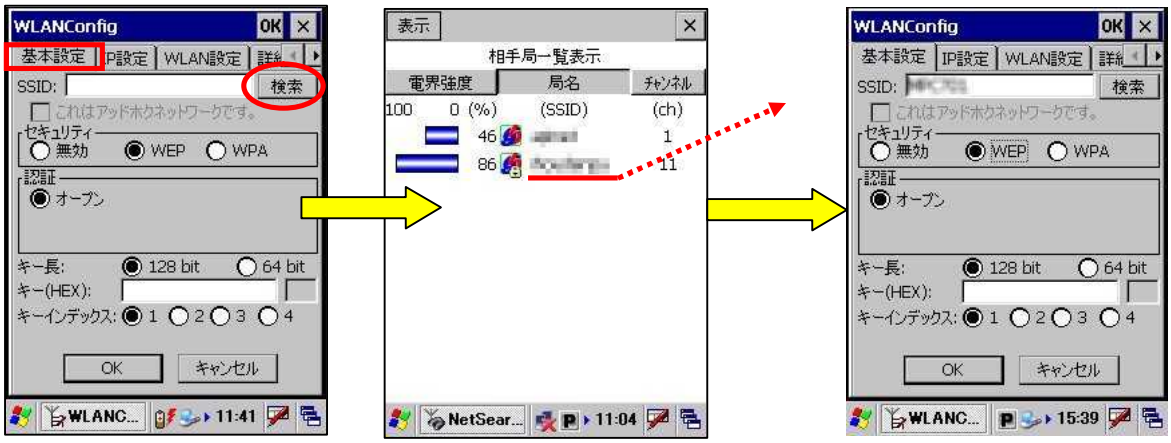


注意

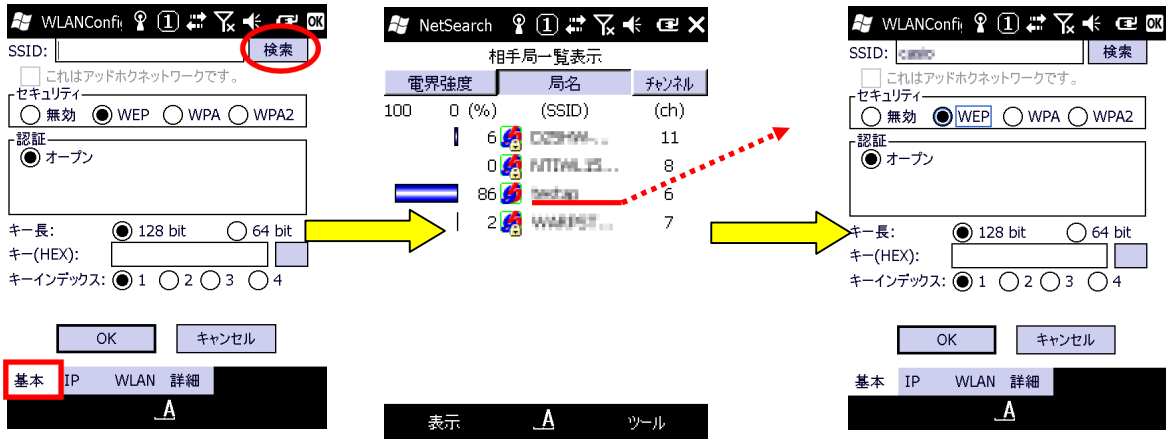
ネットワークとダイアルアップ接続から選択できる、IP アドレス設定画面でも IP アドレスの入力が出来ますが、こちらの画面は使用しないで下さい。

リセットの度に、無線 LAN 設定で指定したアドレスに書き換わってしまう事があります。

4-3.SSID を設定する



CE 画面



Windows Mobile 画面

基本設定タブを選択し、検索ボタンを押します

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ます。

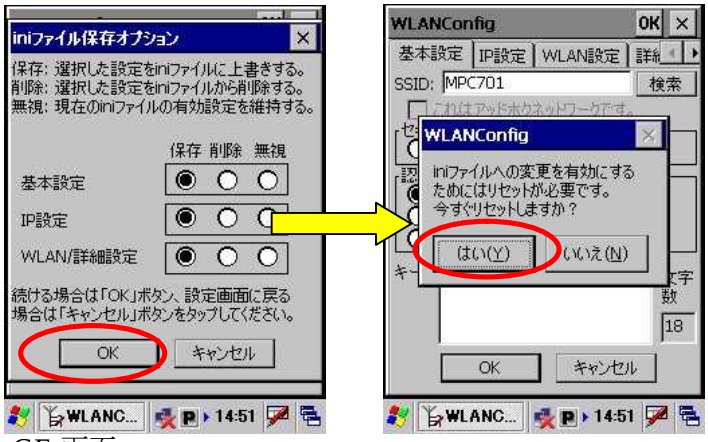
アクセスポイントのSSIDが入力されます。

注意

アクセスポイント側で SSID を隠す設定になっている場合には一覧表に表示されません。
その場合には、SSID を手入力してください。

4-4.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。
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。



CE 画面

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。
通常はそのままOKとしてください。
最後にリセットで、設定が反映され、無線LANが使用可能となります。

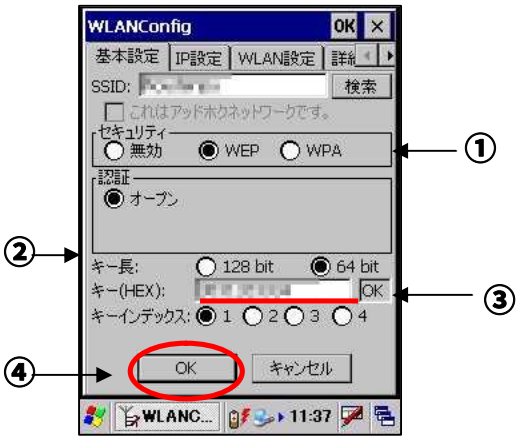
Windows Mobile 画面

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。

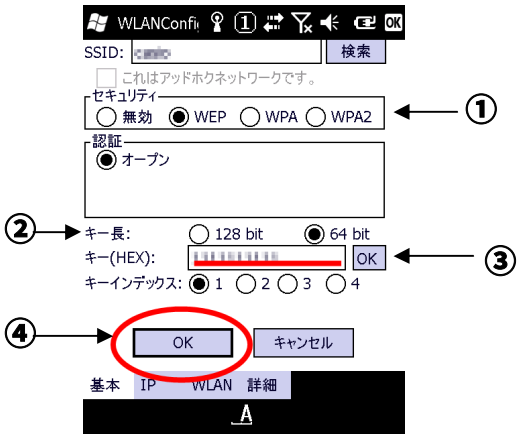
リセットの確認が出ます。
はいを押してください。
自動的にリセットされます。

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



CE 画面



Windows Mobile 画面

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。

・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

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。

無線LAN設定ツールでは、キー長128bitと64bitが選択できます

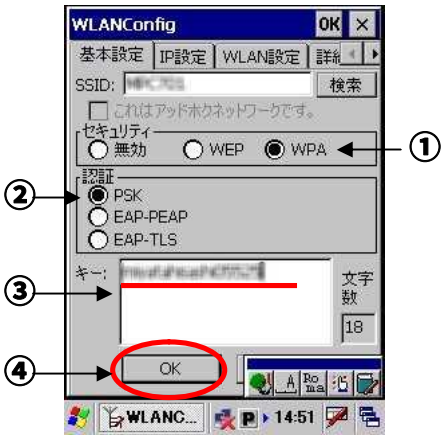
キーとして入力するデータは、キー長から24bitを引いた長さとなります。
キー長に付いての会話を行う場合、キー自体のbit長と入力データのbit長を
取り違え話しがかみ合わない場合がありますのでご注意ください。
特に、右の表のように、WEPキー152bitの入力データとWEPキー128bitでは
同じ128bitですので注意してください。

キー長	入力データ
152	128
128	104
64	40

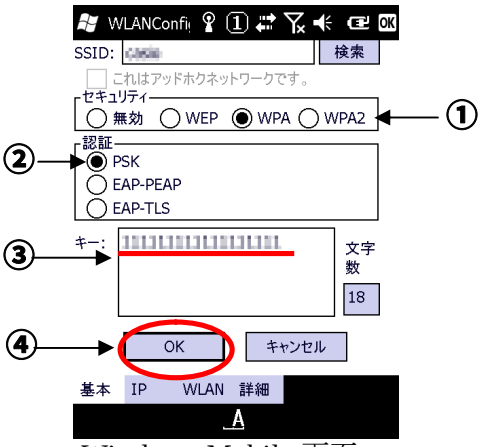
WEP の現状

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以降で説明する WPA-PSK または WPA2-PSK をご検討ください。

5-2.WPA -PSK の場合



CE 画面



Windows Mobile 画面

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
④SSIDを確認して問題が無ければ、
　OKボタンを押します。

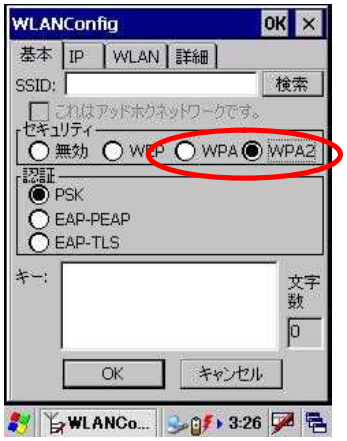
注意：DT -5200のWPA -PSKの設定

DT -5200のWPA -PSKの設定画面で、キーの入力を行うと、下記の動作になります。
※ DT-X7、5300では、発生しません。
１．SSIDを手入力する前に検索入力にしていた場合、検索入力したSSIDになる。
２．SSIDの手入力する前に検索入力にしていない場合、
・過去に無線LAN設定を実施している場合登録済のSSIDに置き換わってしまう。
・初めて無線LANの設定を行う場合には、SSIDが空白になってしまう。

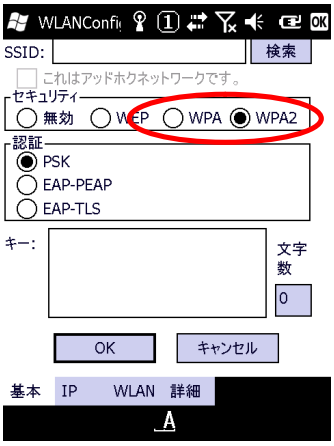
SSIDを検索して入力している場合は、問題ありませんが、手入力を行っている場合は、SSIDの入力は最後に行うようにしてください。

5-3.WPA2-PSK の場合（IT-300、IT-9000、DT-X8、DT-X7M50SB、DT-X7M52SB、DT-5300 が利用可能）

セキュリティ強化モデルである **IT-300/IT-9000/DT-X8/DT-X7M50SB/DT-X7M52SB 及び DT-5300** では、無線 LAN の暗号化に『AES』を使用する事が可能です。
セキュリティの項目に、追加された WPA2 を選択する事で、暗号に AES が使用されます。
WPA を選択した場合は、従来どおりに暗号には、TKIP が使用されます。



CE 画面



Windows Mobile 画面

WPA ⇒ 暗号化には TKIP が使用されます。
WPA2 ⇒ 暗号化には AES が使用されます。

ご注意：WPA で、AES は使用できません。
WPA-PSK で、AES を使う場合は、OS の無線 LAN 設定機能 NetUI を使用してください。

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。

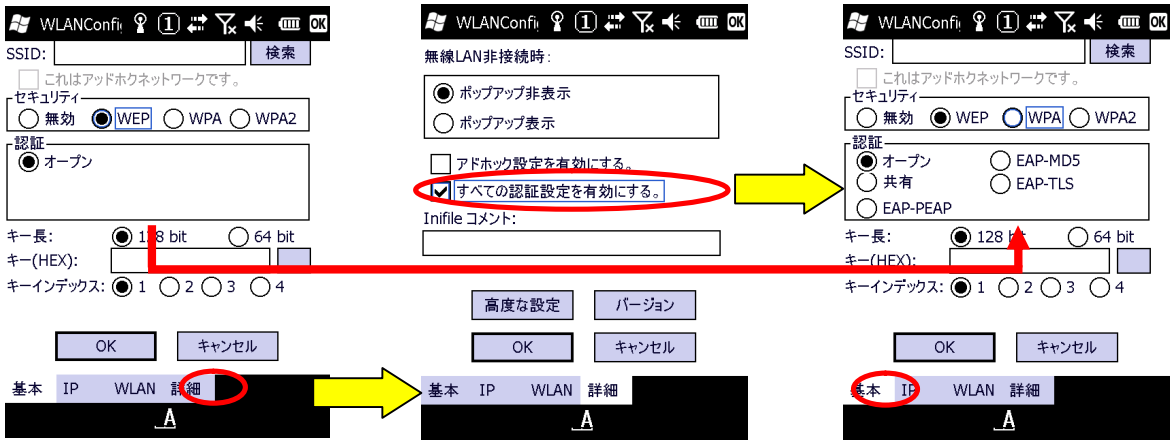
6. 動的 WEP を使用する(802.1x 認証その1)

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。
※ 本機では、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。

CE 画面



Windows Mobile 画面

6-2.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 のようにハンディターミナルに※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、ハンディターミナル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 認証サーバがハンディターミナル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

CE OS の証明書のインポートはコントロールパネルの証明書で行います。

CE 画面

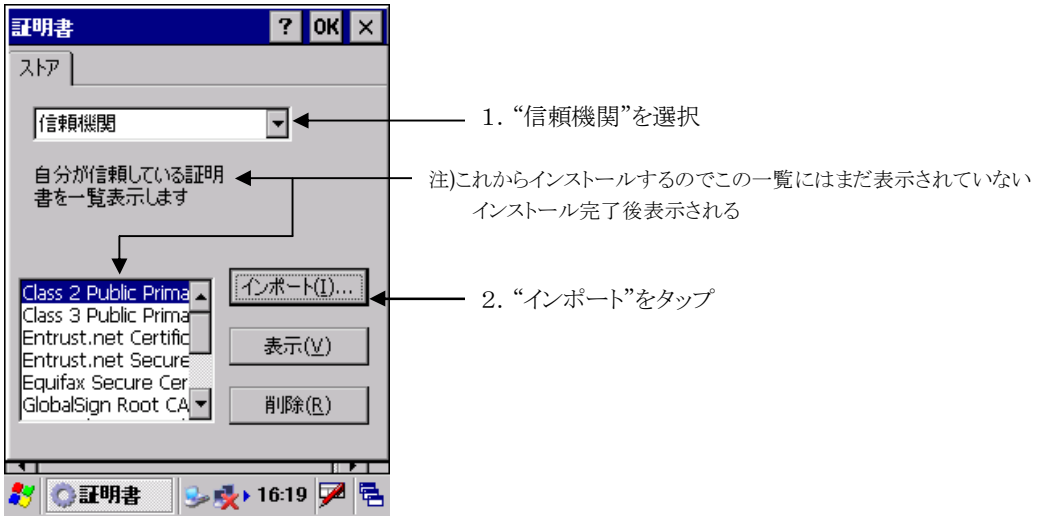
Windows Mobile OS の証明書のインポートは設定からシステムを選択し証明書インストールで行います。

Windows Mobile 画面

アクティブメニュー画面

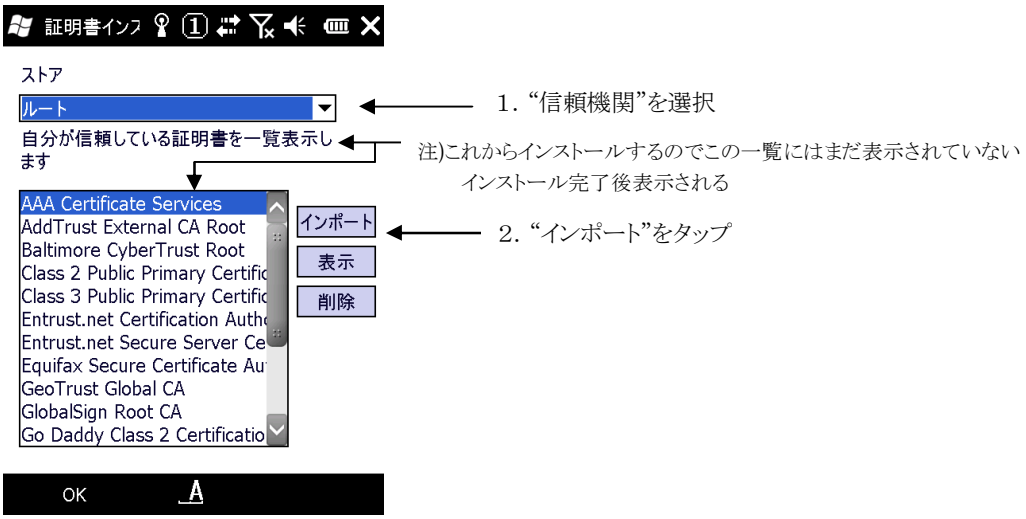
6-2-3.信頼証明の選択

CE OS のルート証明書のインポートは　“信頼期間”を選択して、“インポート”をタップします。



CE 画面

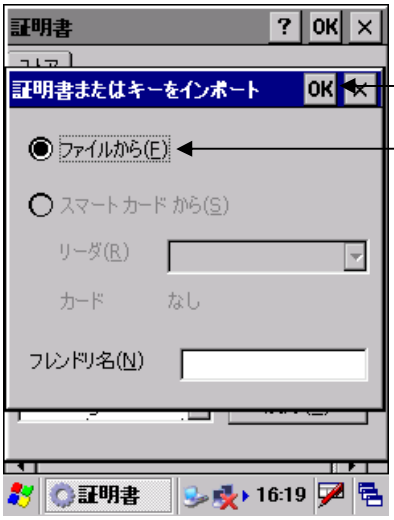
Windows Mobile OS のルート証明書のインポートは　“ルート”を選択して、“インポート”をタップします。



Windows Mobile 画面

6-2-4.ルート証明書ファイルの選択

CE OS は証明書をファイルからインポートするので“ファイルから”を選択して、“ＯＫ”をタップ。



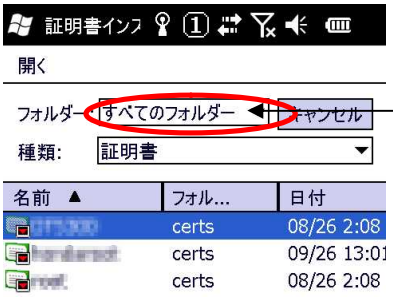
2. “ＯＫ”をタップ

1. “ファイルから”を選択

CE 画面

“ＯＫ”のタップで証明書が置かれているフォルダーの選択画面が表示されます。

Windows Mobile OS は証明書が存在するフォルダーを選択するか、“すべてのフォルダー”を選択します。

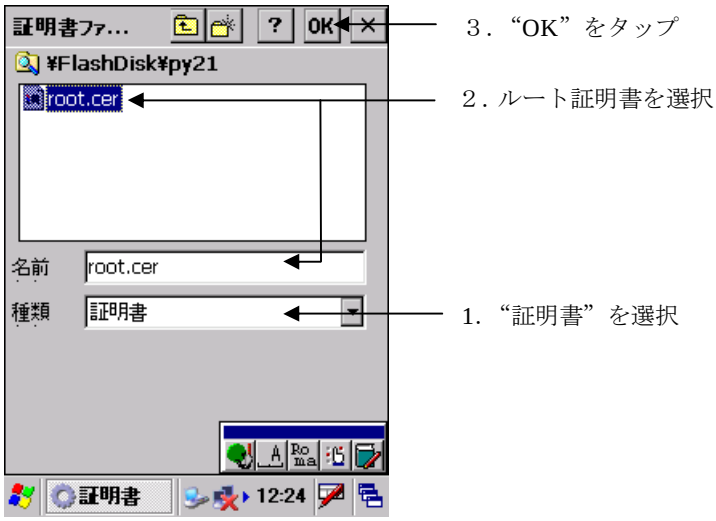


1. フォルダーを選択

Windows Mobile 画面

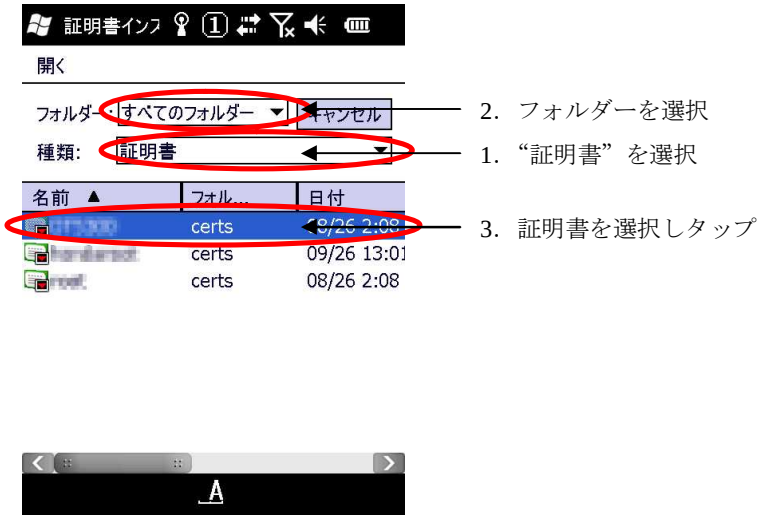
6-2-5.ルート証明書のインポート

CE OS は、種類を“証明書“にしてマイデバイスより、コピーした証明書ファイルのあるフォルダーを選択するとコピーした証明書の一覧が表示されます。
表示された証明書の一覧の中から、ルート証明書を選択し“ＯＫ”をタップします。



CE 画面

Windows Mobile OS は、種類を“証明書“にしてフォルダーを“すべてのフォルダー“、またはコピーした証明書ファイルのあるフォルダーを選択するとコピーした証明書の一覧が表示されます。
表示された証明書の一覧の中から、ルート証明書を選択しタップします。



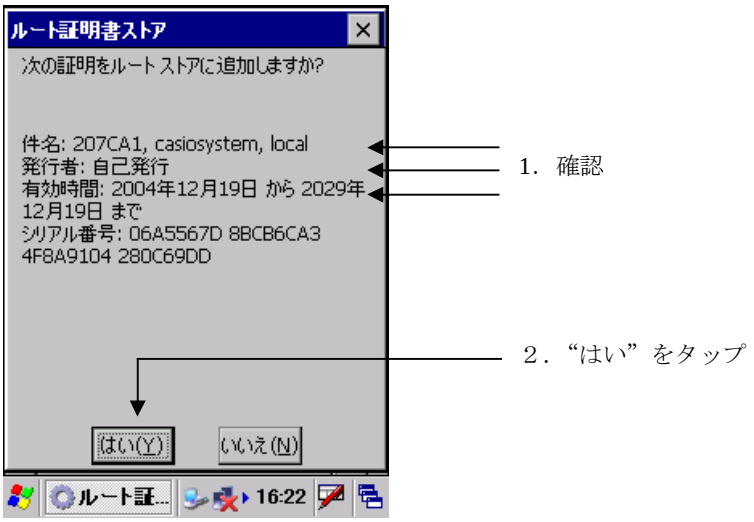
Windows Mobile 画面

6-2-6.ルート証明書の確認

CE OS は、ルート証明書ストアの確認画面が表示されます。

件名にルート証明書を作成した認証局の名前
発行者　本例の場合に内部のＣＡサーバで作成したので自己発行になっています
有効期間

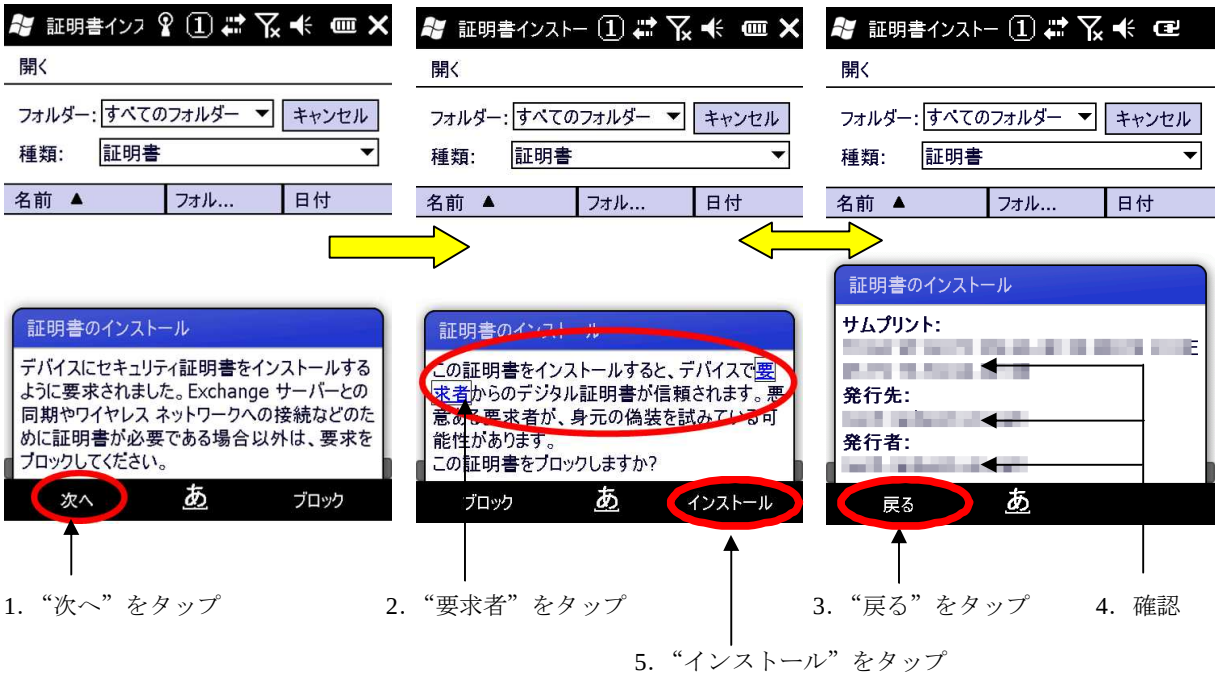
などが表示されます。
インポートする証明書に間違いがないか確認して“はい”をタップします。



Windows Mobile OS は、ルート証明書のインストールの確認画面が表示されます。
“次へ”をタップします。“要求者”をタップします。

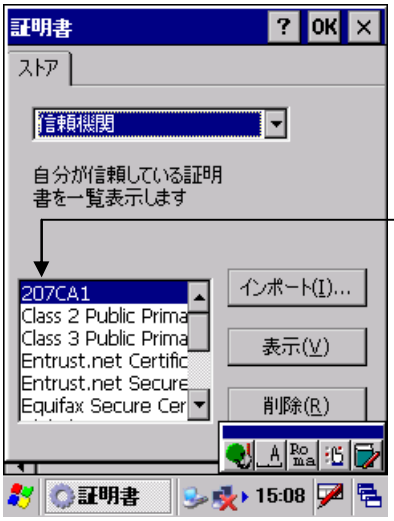
サムプリント
発行先
発行者

が表示されます。
インポートする証明書に間違いがないか確認して“戻る”をタップします。
“インストール”をタップします。



6-2-7.ルート証明書インポートの終了・確認

インポートが成功すると　信頼している証明書の一覧表示に表示されます。



インポートしたルート証明書が表示

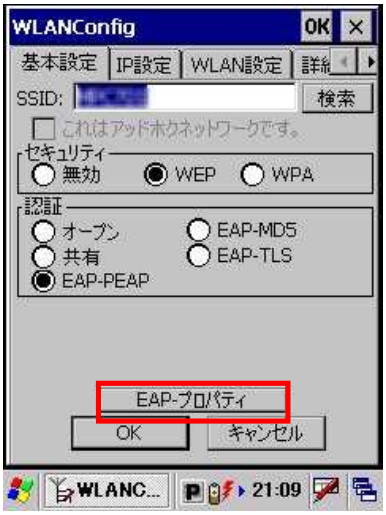
CE 画面

インポートしたルート証明書が表示

Windows Mobile 画面

6-2-8.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。

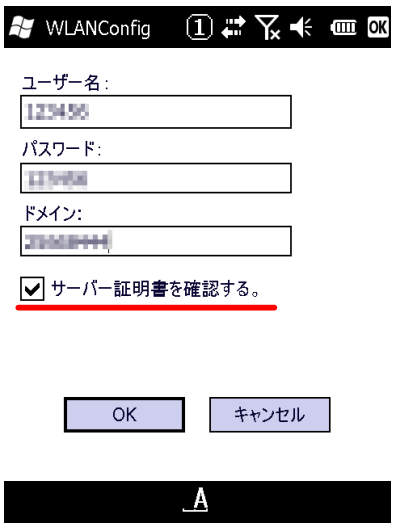


CE 画面

Windows Mobile 画面

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。

CE 画面



Windows Mobile 画面

『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しなくなり
セキュリティが大きく低下してしまいます。

6-3.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、ハンディターミナルに証明書のインポート（インストール）が必須となります。
設定手順としては、証明書･暗号鍵のインポートのあと EAP -TLS でのワイヤレス LAN 接続設定となります。

6-3-1.証明書・秘密鍵のインポート

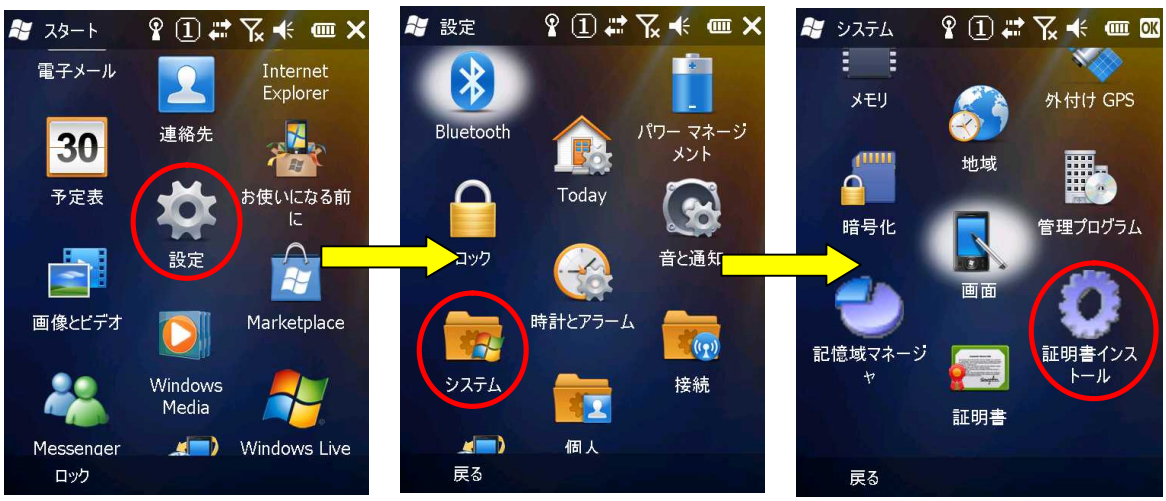
商用認証機関の証明書を使用しない場合は、CAサーバを構築して以下の3つのファイルを作成します。

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

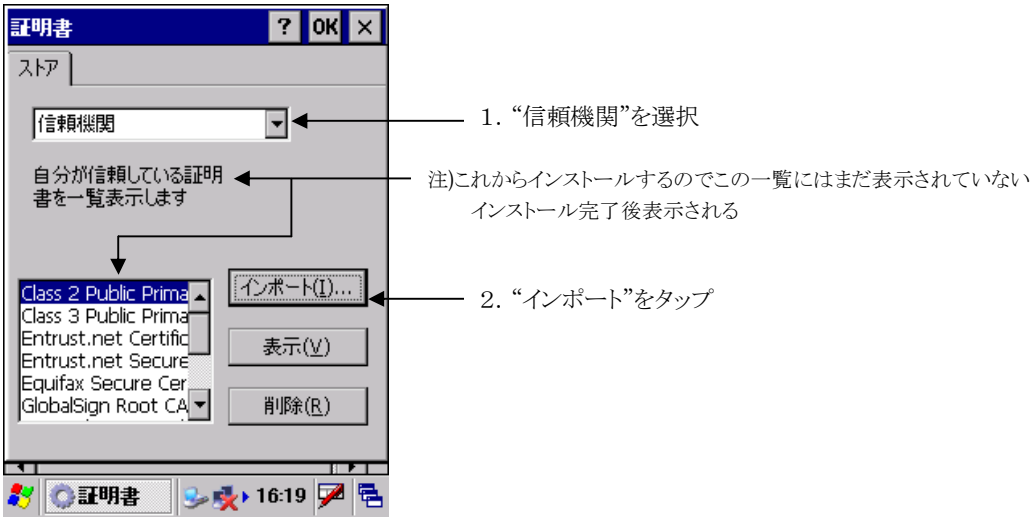
CE 画面



Windows Mobile 画面

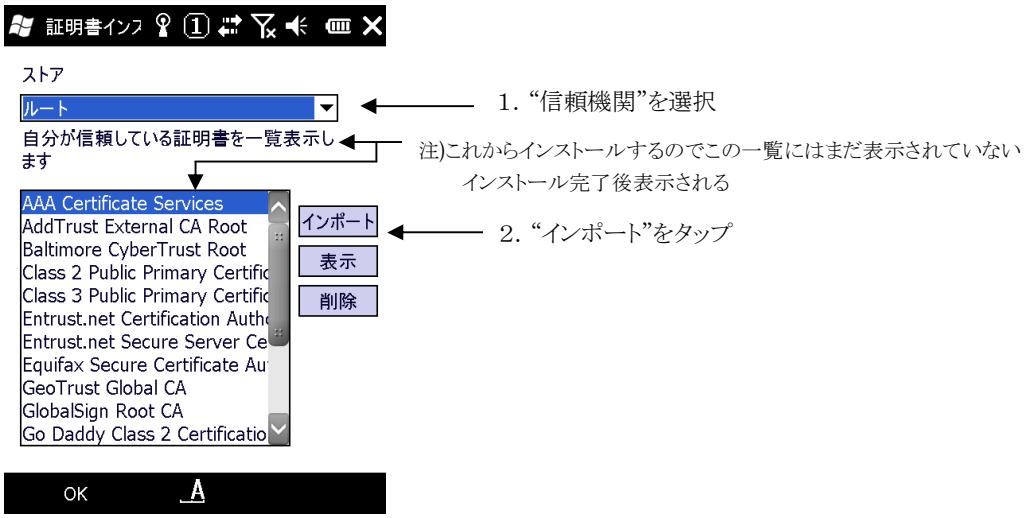
アクティブメニュー画面

CE OS のルート証明書のインポートは　“信頼期間”を選択して、“インポート”をタップし



CE 画面

Windows Mobile OS のルート証明書のインポートは　“ルート”を選択して、“インポート”をタップします。



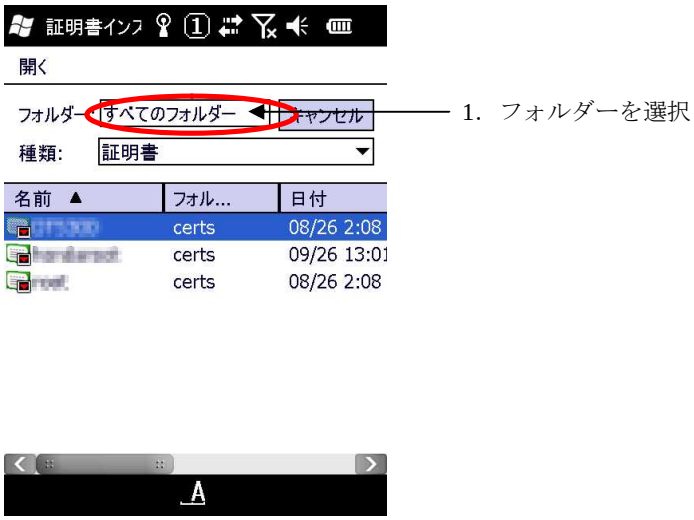
Windows Mobile 画面

ルート証明書ファイルの選択
CE OS は、証明書をファイルからインポートするので“ファイルから”を選択して、“ＯＫ”をタップします。

CE 画面

“ＯＫ”のタップで証明書が置かれているフォルダーの選択画面が表示されます。

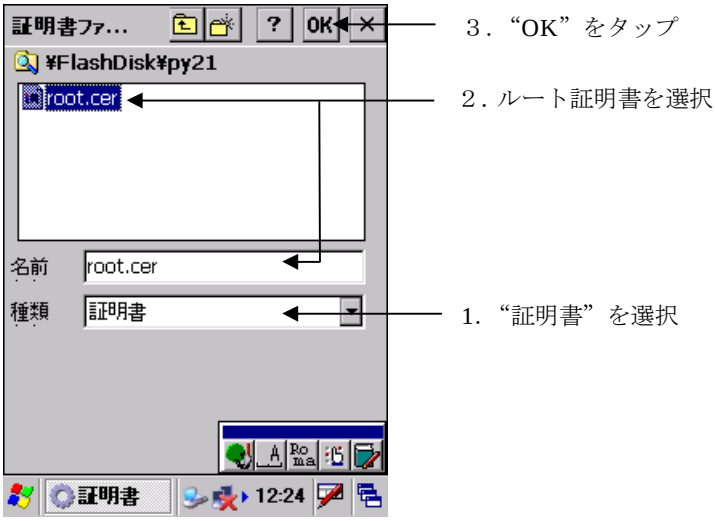
Windows Mobile OS は証明書が存在するフォルダーを選択するか、“すべてのフォルダー”を選択します。



Windows Mobile 画面

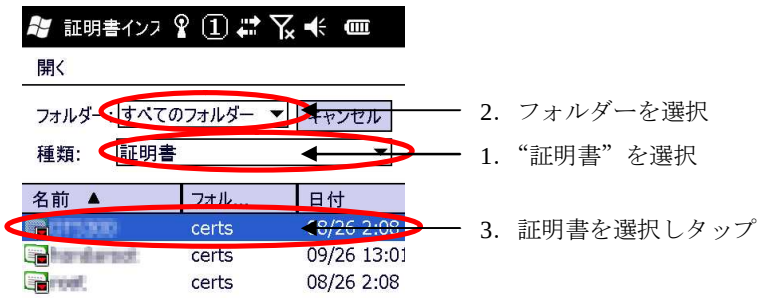
6-3-3.ルート証明書のインポート

CE OS は、種類を　“証明書“　にしてマイデバイスより、コピーした証明書ファイルのあるフォルダーを選択するとコピーした証明書の一覧が表示されます。
表示された証明書の一覧の中から、ルート証明書を選択し“ＯＫ”をタップします。



CE 画面

Windows Mobile OS は、種類を“証明書“にしてフォルダーを“すべてのフォルダー“、またはコピーした証明書ファイルのあるフォルダーを選択するとコピーした証明書の一覧が表示されます。
表示された証明書の一覧の中から、ルート証明書を選択しタップします。



Windows Mobile 画面

6-3-4.ルート証明書の確認

CE OS は、ルート証明書ストアの確認画面が表示されます。

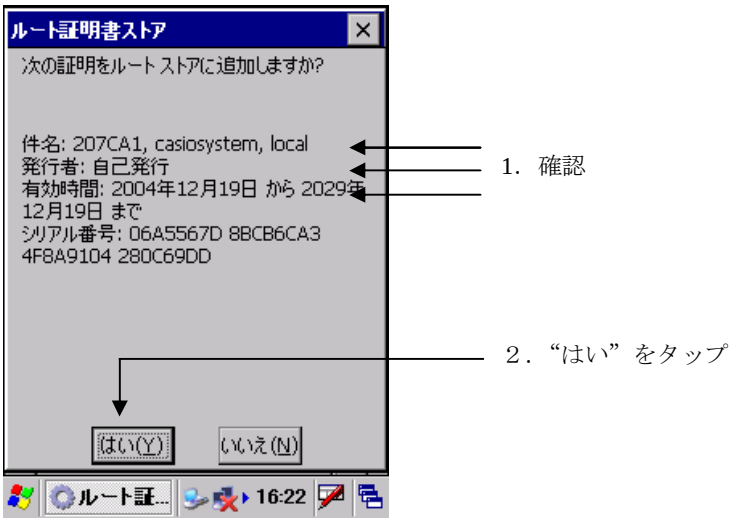
件名にルート証明書を作成した認証局の名前

発行者　本例の場合に内部のＣＡサーバで作成したので自己発行になっています

有効期間

などが表示されます。

インポートする証明書に間違いがないか確認して“はい”をタップします。



Windows Mobile OS は、ルート証明書のインストールの確認画面が表示されます。

“次へ”をタップします。“要求者”をタップします。

サムプリント

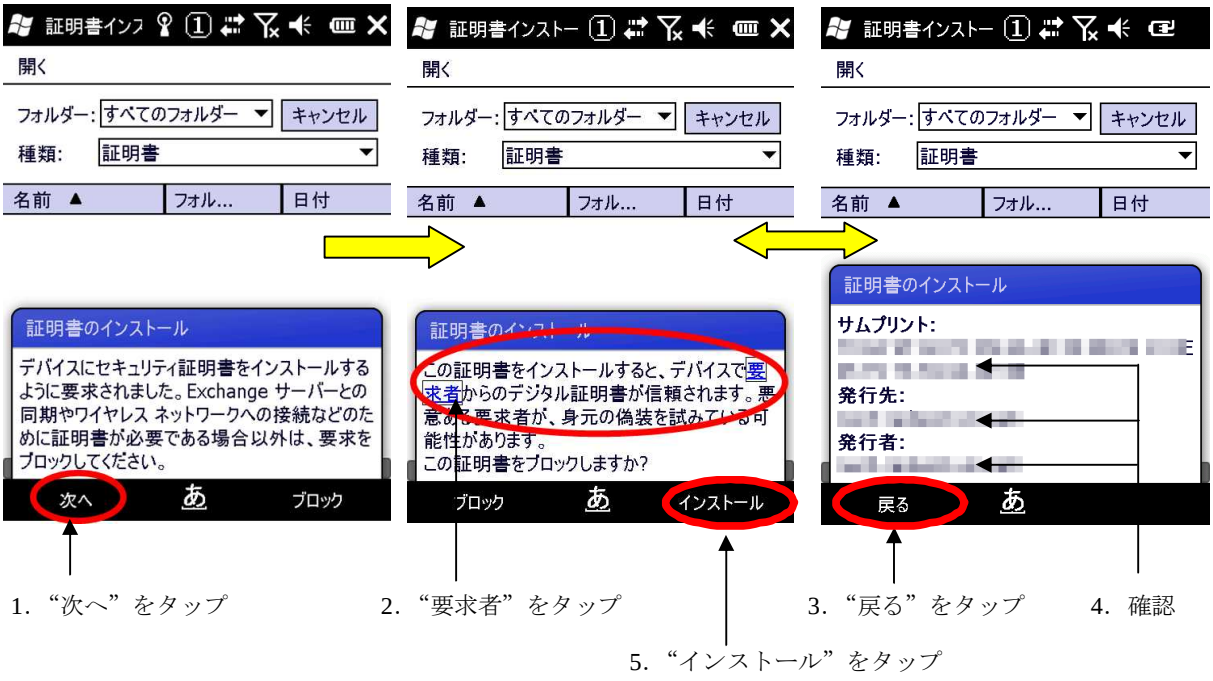
発行先

発行者

が表示されます。

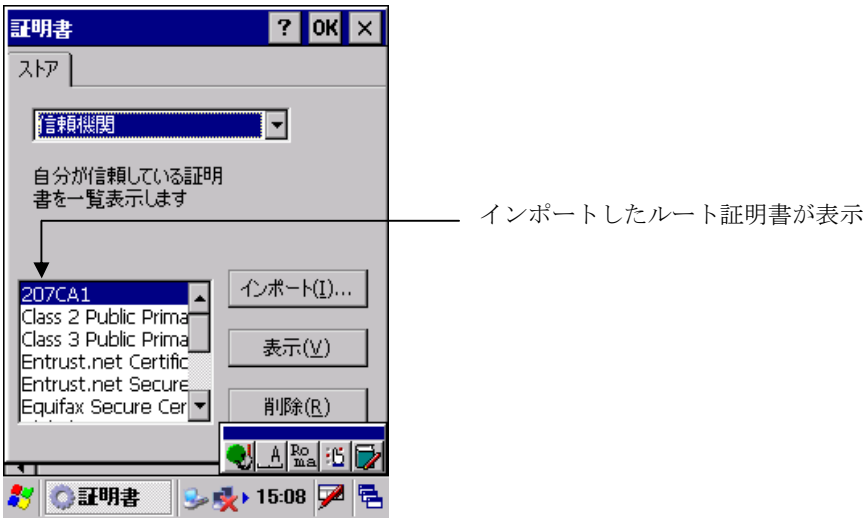
インポートする証明書に間違いがないか確認して“戻る”をタップします。

“インストール”をタップします。

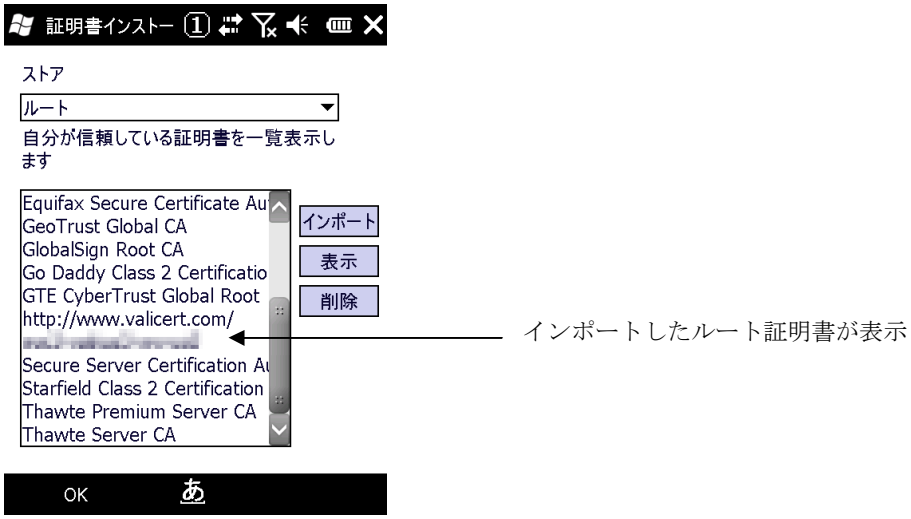


6-3-5.ルート証明書インポートの終了・確認

インポートが成功すると　信頼している証明書の一覧表示に表示されます



CE 画面



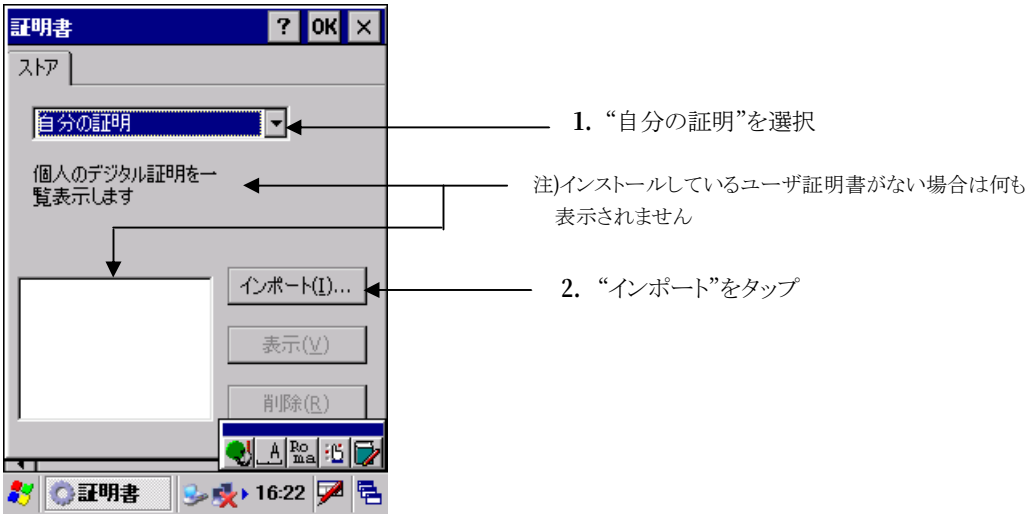
Windows Mobile 画面

6-3-6.ユーザ証明書のインポート

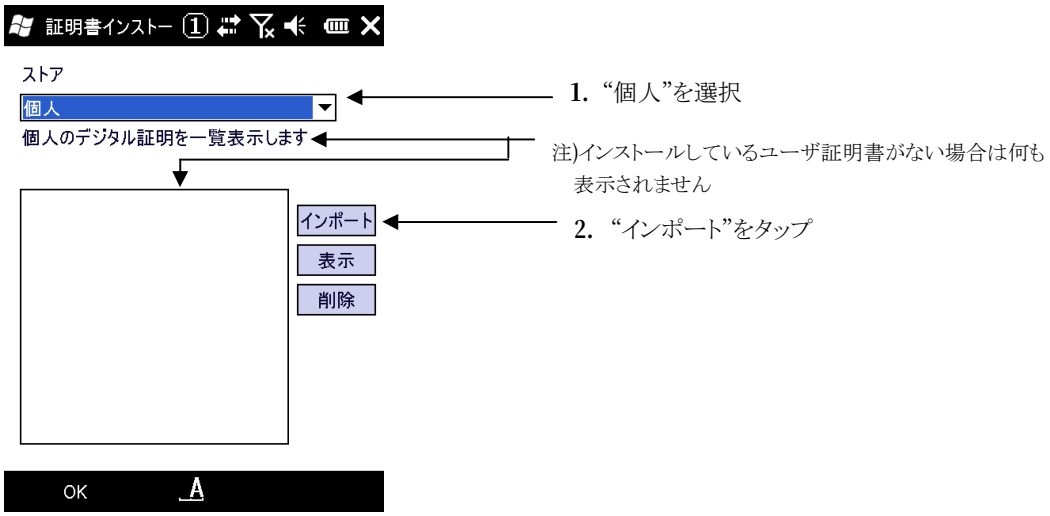
インポート手順として、初めにユーザ証明書をインポートし、後から秘密鍵をインポートします。

6-3-6- 1 個人デジタル証明の選択

ユーザ証明書のインポートは“自分の証明”を選択して、“インポート”をタップします。



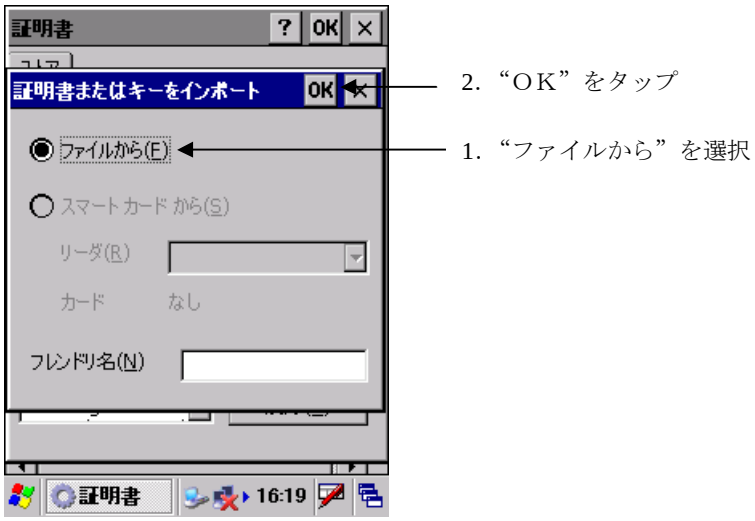
CE 画面



Windows Mobile 画面

6-3-6-２ユーザ証明書ファイルの選択

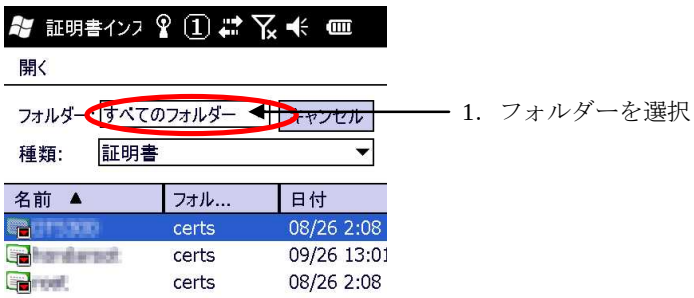
CE OS は、証明書をファイルからインポートするので“ファイルから”を選択して、“ＯＫ”をタップします。



CE 画面

“ＯＫ”のタップで証明書が置かれているフォルダーの選択画面が表示されます。

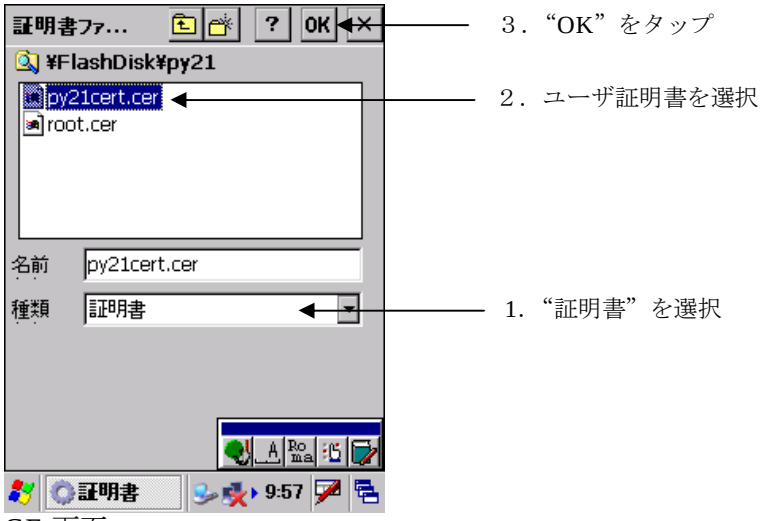
Windows Mobile OS は証明書が存在するフォルダーを選択するか、“すべてのフォルダー”を選択します。



Windows Mobile 画面

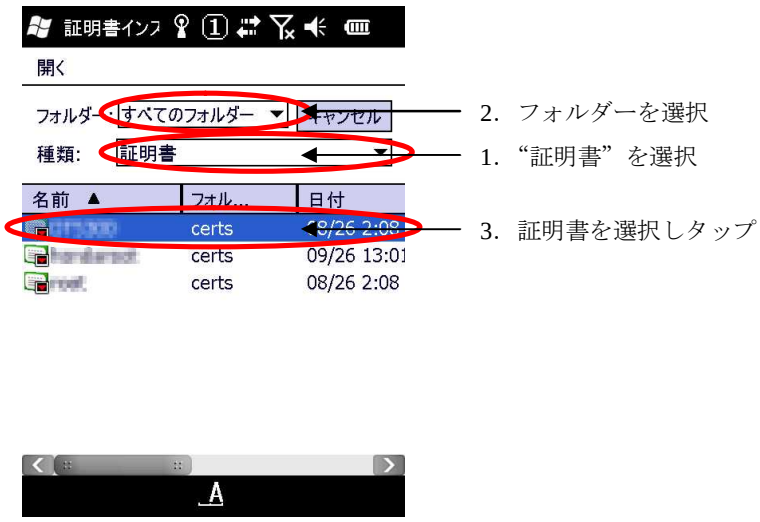
6-3-6-３ユーザ証明書のインポート

CE OS は、ルート証明書のインポートと同様に“ＯＫ”のタップで証明書が置かれているフォルダーの選択画面が表示されます。
種類を“証明書“　にして、コピーしたユーザ証明書ファイルのあるフォルダーを選択すると一覧が表示されます。
表示された証明書の一覧の中から、インポートするユーザ証明書を選択し“ＯＫ”をタップします。



CE 画面

Windows Mobile OS は、種類を“証明書“にしてフォルダーを“すべてのフォルダー“、またはコピーした証明書ファイルのあるフォルダーを選択するとコピーした証明書の一覧が表示されます。
表示された証明書の一覧の中から、ユーザ証明書を選択しタップします。



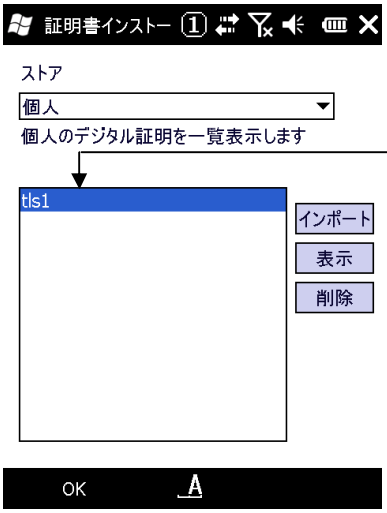
Windows Mobile 画面

6-3-6-４ユーザ証明書インポートの終了・確認

ユーザ証明書のインポートに成功すると、個人のデジタル証明の一覧に表示されます。

インポートしたユーザ証明書が表示されている

CE 画面

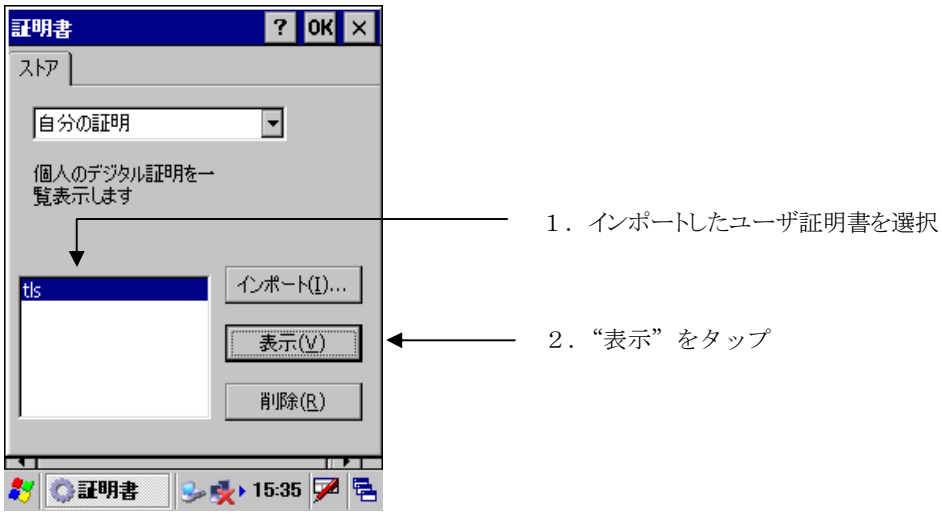


インポートしたユーザ証明書が表示されている

Windows Mobile 画面

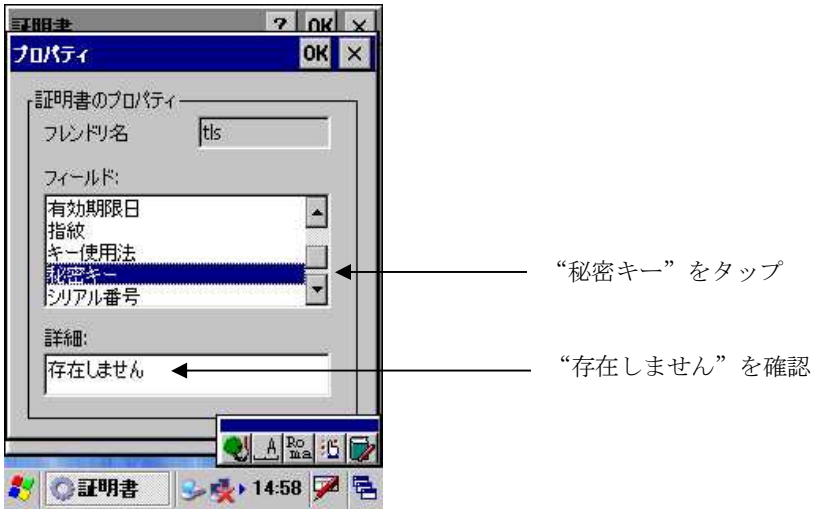
6-3-6- 5 秘密鍵インポートの確認

CE OS は、インポートしたユーザ証明書を表示し秘密鍵のインポートを確認します。
インポートしたユーザ証明書を選択して“表示”をタップします。

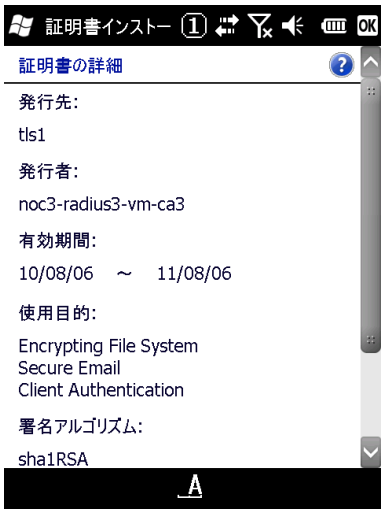


CE 画面

“秘密キー”を選択し、詳細を確認します。



CE 画面



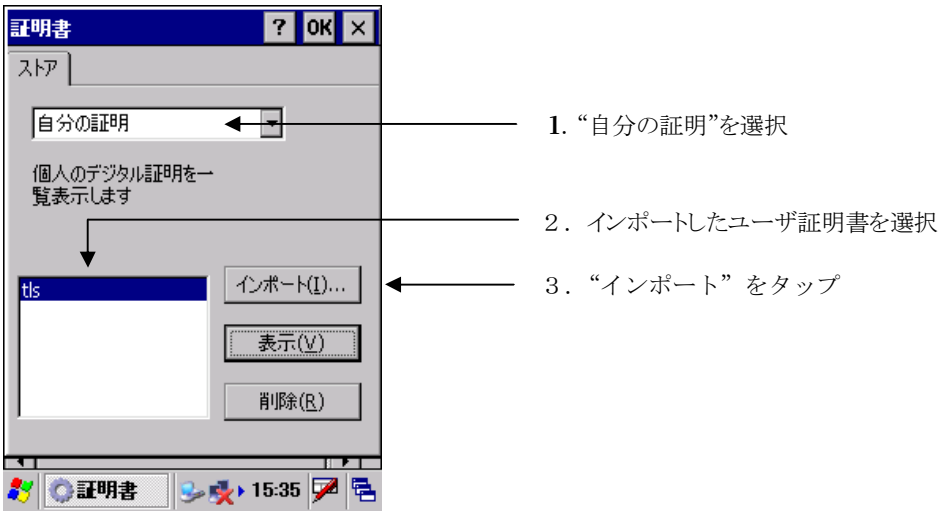
Windows Mobile 画面

Windows Mobile OSでは“表示”をタップしても秘密キーの項目が表示されません。

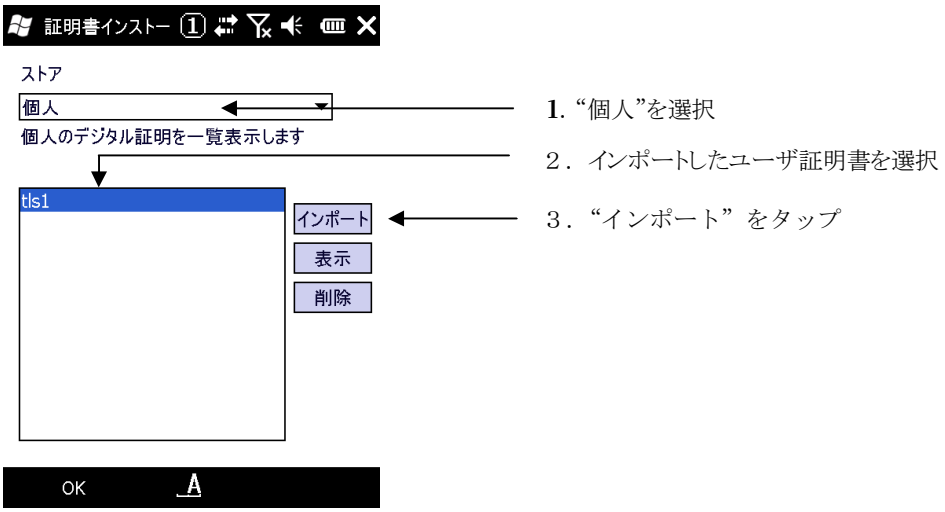
6-3-7.秘密鍵のインポート

6-3-7- 1 自分の証明のインポートを選択

インポートしたユーザ証明書に秘密鍵をインポートします。
CE OS は“自分の証明書”を Windows Mobile OS は“個人”を選択して、ユーザ証明書を選択し“インポート”をタップします。



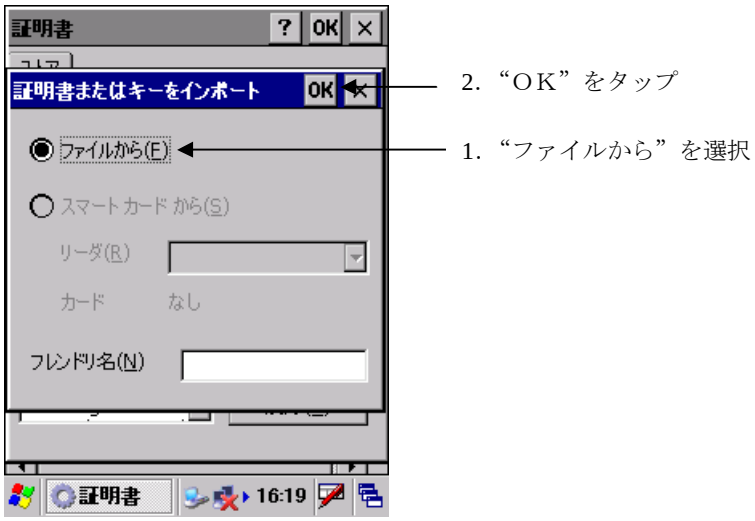
CE 画面



Windows Mobile 画面

6-3-7-２ユーザ証明書秘密鍵ファイルの選択

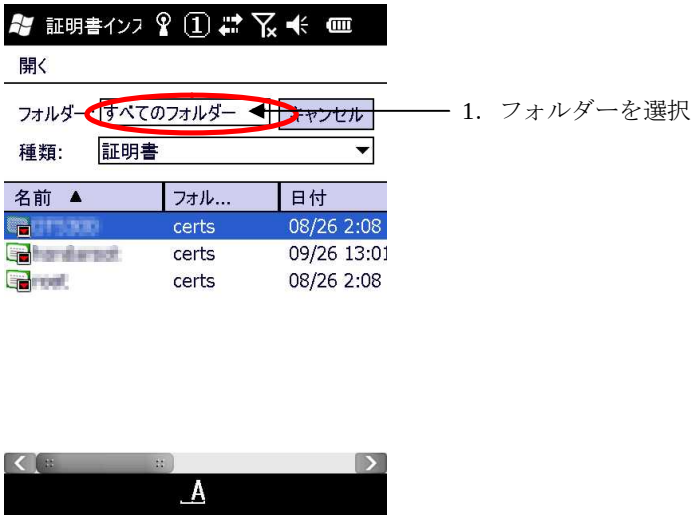
CE OS は、キーをファイルからインポートするので“ファイルから”を選択して、“ＯＫ”をタップします。



CE 画面

“ＯＫ”のタップで証明書が置かれているフォルダーの選択画面が表示されます。

Windows Mobile OS はキーが存在するフォルダーを選択するか、“すべてのフォルダー”を選択します。



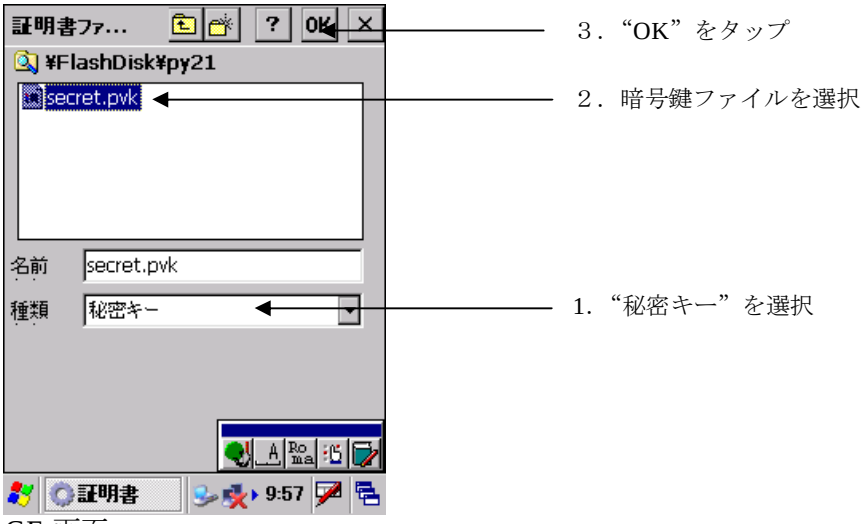
Windows Mobile 画面

6-3-7-３ユーザ証明書秘密鍵のインポート

CE OS は、証明書のインポートと同様に OK のタップで暗号鍵が置かれているフォルダーの選択画面が表示されます。

ファイルの種類を　“秘密キー“　にして、コピーした秘密鍵ファイルのあるフォルダーを選択すると一覧が表示されます。

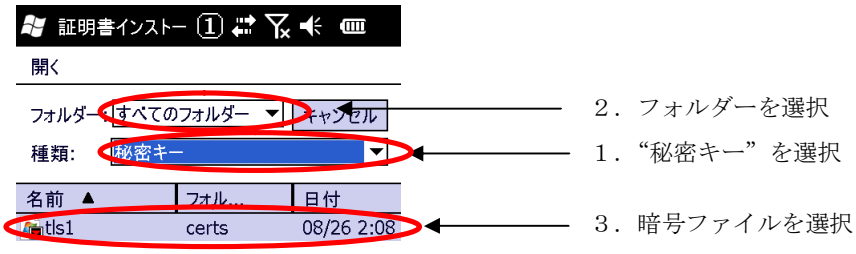
表示された証明書の一覧の中から、暗号鍵ファイルを選択し“ＯＫ”をタップします。



CE 画面

Windows Mobile OS は、種類を“秘密キー“にしてフォルダーを“すべてのフォルダー“、またはコピーした証明書ファイルのあるフォルダーを選択するとコピーした秘密鍵ファイルの一覧が表示されます。

表示された証明書の一覧の中から、秘密鍵ファイルを選択しタップします。

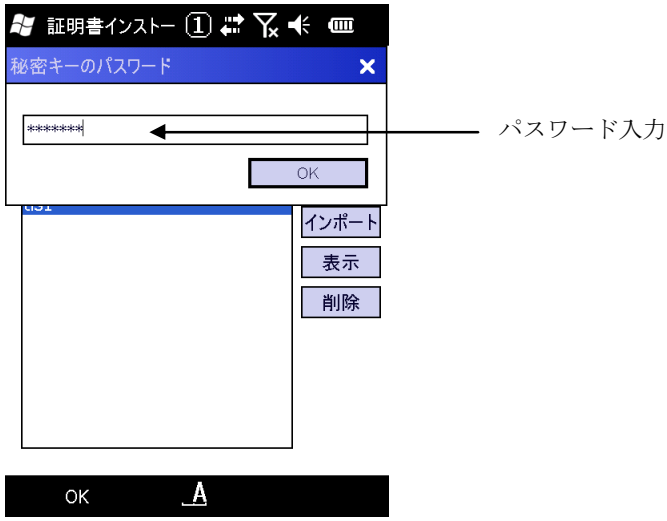


Windows Mobile 画面

6-3-7-４パスワード入力

ＣＡサーバ上で秘密鍵作成時に指定したパスワードを入力します。

CE 画面



Windows Mobile 画面

6-3-7-５ユーザ証明書暗号鍵インポートの終了

パスワード認証が成功すると証明書設定の画面に戻ります。

CE OS は、インポートした暗号鍵を確認するために証明書を表示させます。

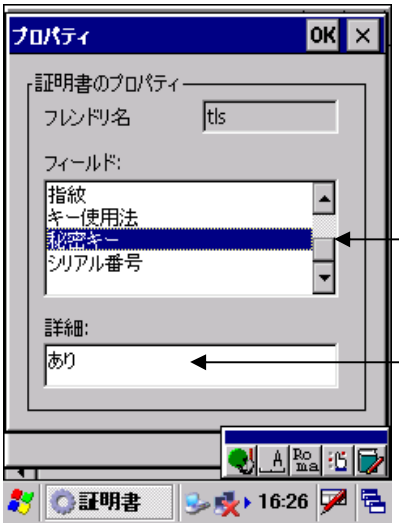
１．暗号鍵をインポートしたユーザ証明書を選択

２．“表示”をタップ

CE 画面

6-3-7-６ユーザ証明書暗号鍵インポートの確認

CE OS は“秘密キー”を選択して、詳細が“あり”になっていることを確認します。

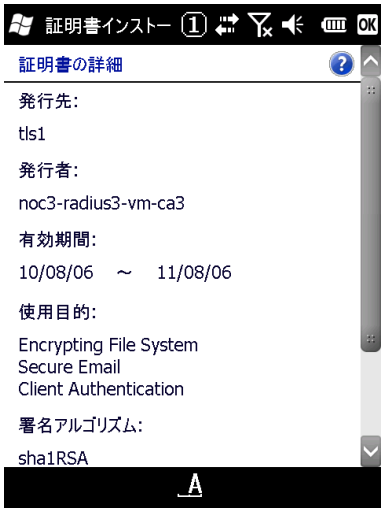


１．“秘密キー”をタップ

２．“あり”を確認

CE 画面

以上で、証明書のインポートは終了になります。



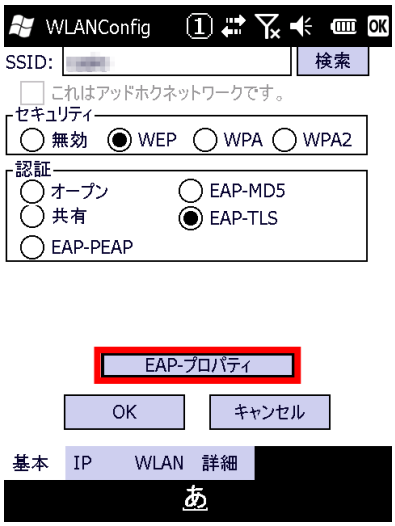
Windows Mobile OSでは“表示”をタップしても秘密キーの項目が表示されません。

Windows Mobile 画面

6-3-8.ワイヤレスプロパティの設定

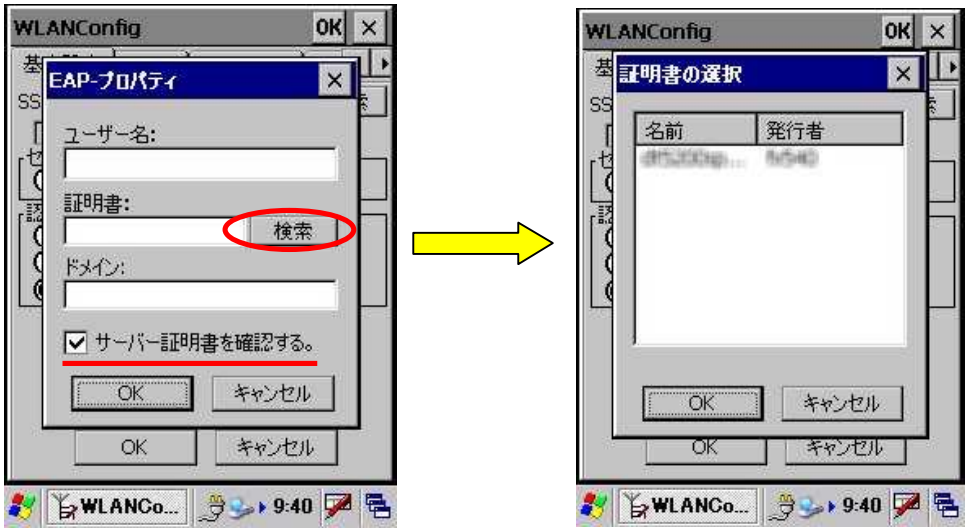
“セキュリティ” → “ WEP ”
“認証” → “ EAP-TLS ”
を選択します。
EAP-プロパティボタンをタップします。

CE 画面

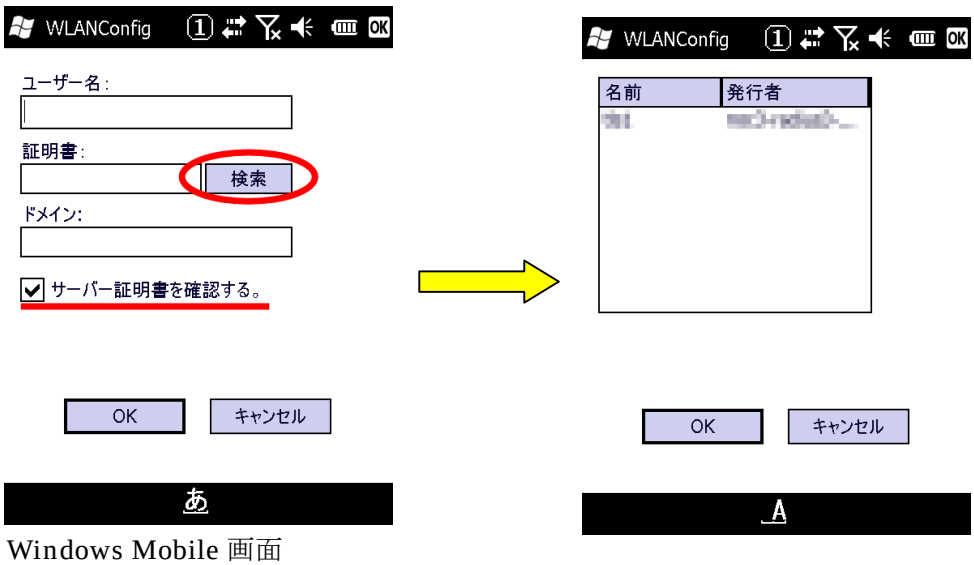


Windows Mobile 画面

証明書の選択
EAP－プロパティの認証で使用するユーザ証明書を選択します。
接続時に入力するユーザ・証明書・ドメイン情報を入力します。



CE 画面



Windows Mobile 画面

『サーバー証明書を確認する』のチェックを外すとサーバ証明書を確認しなくなり、
ユーザ証明書（と秘密鍵）でのみの認証になります。
セキュリティが弱くなるのでお勧めできません。
チェックを入れたままにする事をお勧めします。

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。

セキュリティ強化モデル IT-300/IT-9000/DT-X8/DT-X7M50SB、DT-X7M52SB、 DT-5300 シリーズでは、暗号化に TKIP よりも高度な AES を使用する事が可能です。
セキュリティで、WPA を選択すると暗号化に TKIP、WPA2 を選択すると暗号化に AES が選択されます。

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 のようにハンディターミナルに※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、ハンディターミナル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 認証サーバがハンディターミナル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

CE OS の証明書のインポートはコントロールパネルの証明書で行います。

CE 画面

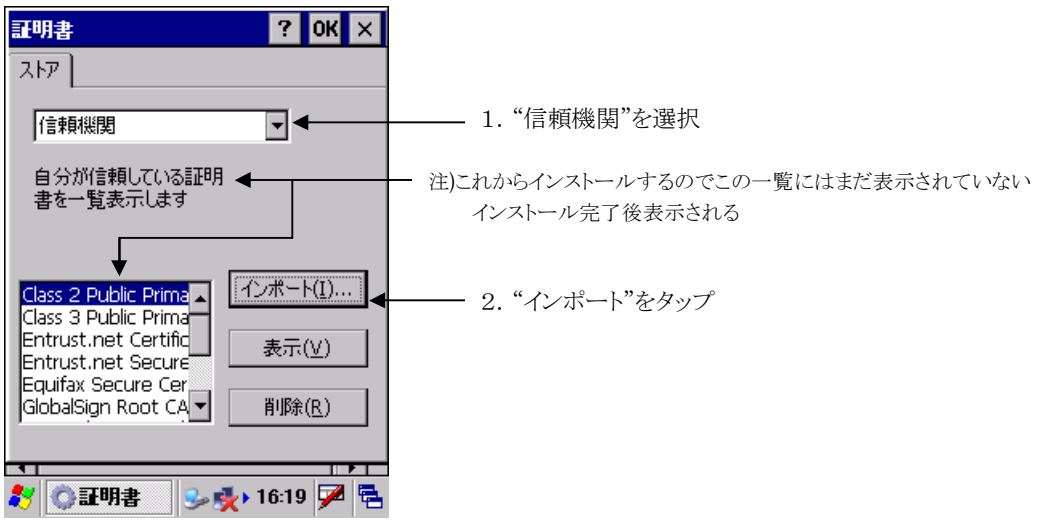
Windows Mobile OS の証明書のインポートは設定からシステムを選択し証明書インストールで行います。

Windows Mobile 画面

アクティブメニュー画面

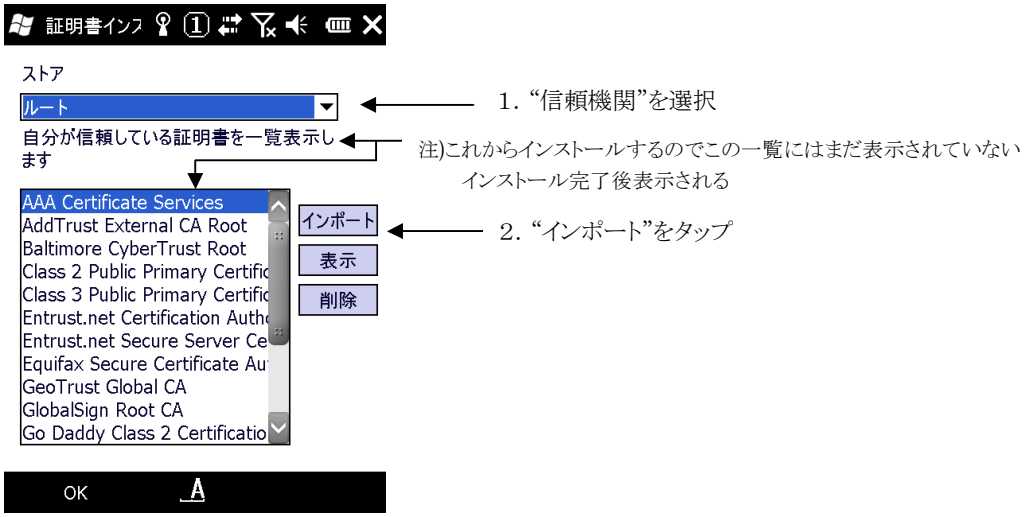
7-1-3.信頼証明の選択

CE OS のルート証明書のインポートは　“信頼期間”を選択して、“インポート”をタップします。



CE 画面

Windows Mobile OS のルート証明書のインポートは　“ルート”を選択して、“インポート”をタップします。



Windows Mobile 画面

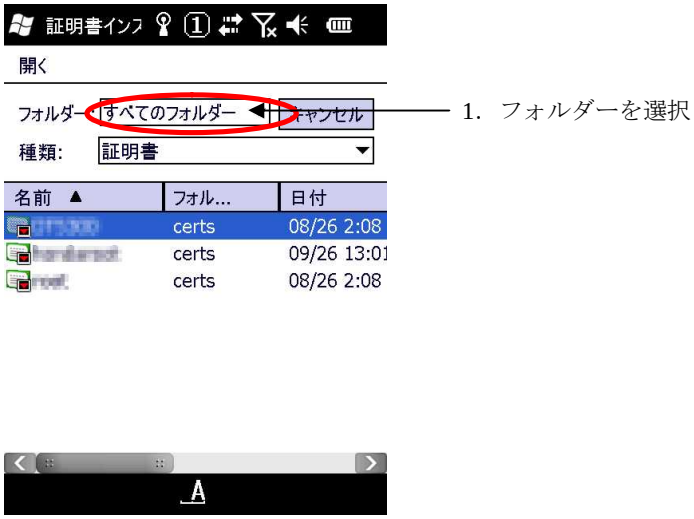
7-1-4.ルート証明書ファイルの選択

CE OS は、証明書をファイルからインポートするので“ファイルから”を選択して、“ＯＫ”をタップします。

CE 画面

“ＯＫ”のタップで証明書が置かれているフォルダーの選択画面が表示されます。

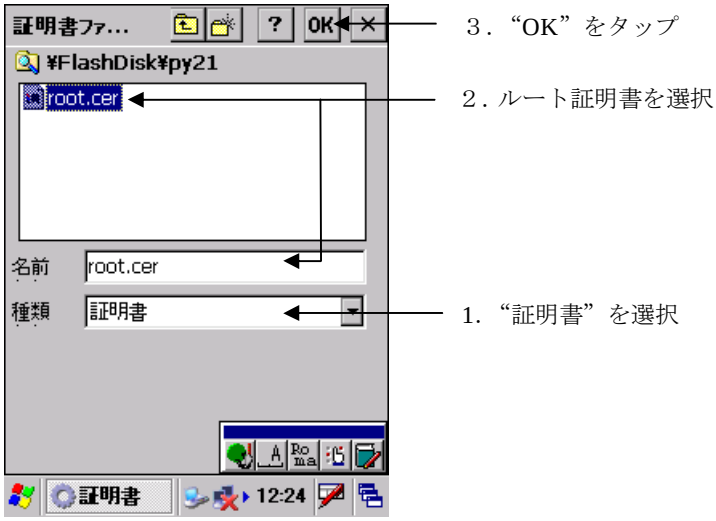
Windows Mobile OS は証明書が存在するフォルダーを選択するか、“すべてのフォルダー”を選択します。



Windows Mobile 画面

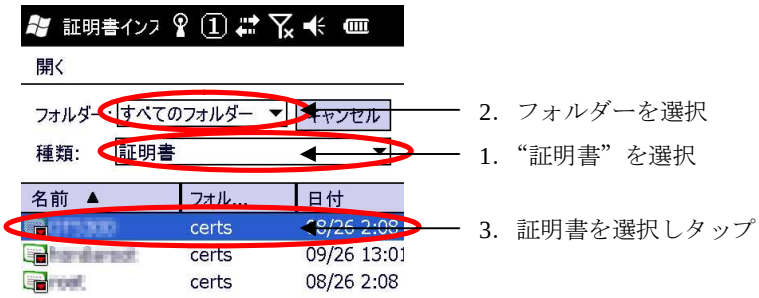
7-1-5.ルート証明書のインポート

CE OS は、種類を　“証明書“　にしてマイデバイスより、コピーした証明書ファイルのあるフォルダーを選択するとコピーした証明書の一覧が表示されます。
表示された証明書の一覧の中から、ルート証明書を選択し“ＯＫ”をタップします。



CE 画面

Windows Mobile OS は、種類を“証明書“にしてフォルダーを“すべてのフォルダー“、またはコピーした証明書ファイルのあるフォルダーを選択するとコピーした証明書の一覧が表示されます。
表示された証明書の一覧の中から、ルート証明書を選択しタップします。



Windows Mobile 画面

7-1-6.ルート証明書の確認

CE OS は、ルート証明書ストアの確認画面が表示されます。

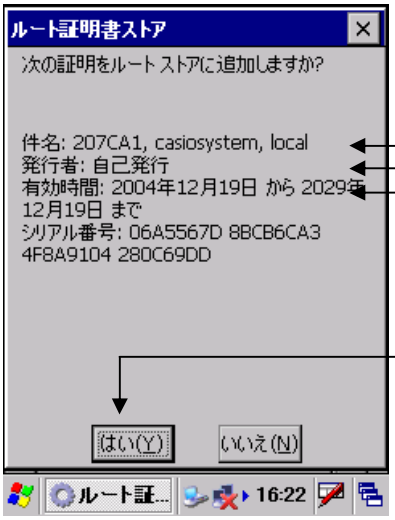
件名にルート証明書を作成した認証局の名前

発行者　本例の場合に内部のＣＡサーバで作成したので自己発行になっています

有効期間

などが表示されます。

インポートする証明書に間違いがないか確認して“はい”をタップします。



1．確認

2．“はい”をタップ

Windows Mobile OS は、ルート証明書のインストールの確認画面が表示されます。

“次へ”をタップします。“要求者”をタップします。

サムプリント

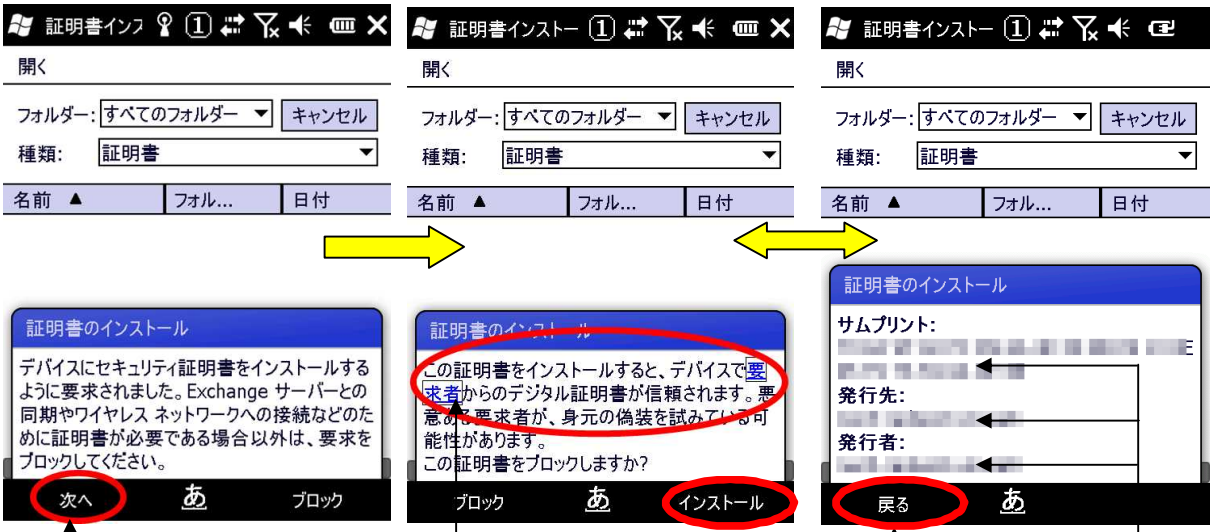
発行先

発行者

が表示されます。

インポートする証明書に間違いがないか確認して“戻る”をタップします。

“インストール”をタップします。



1．“次へ”をタップ

2．“要求者”をタップ

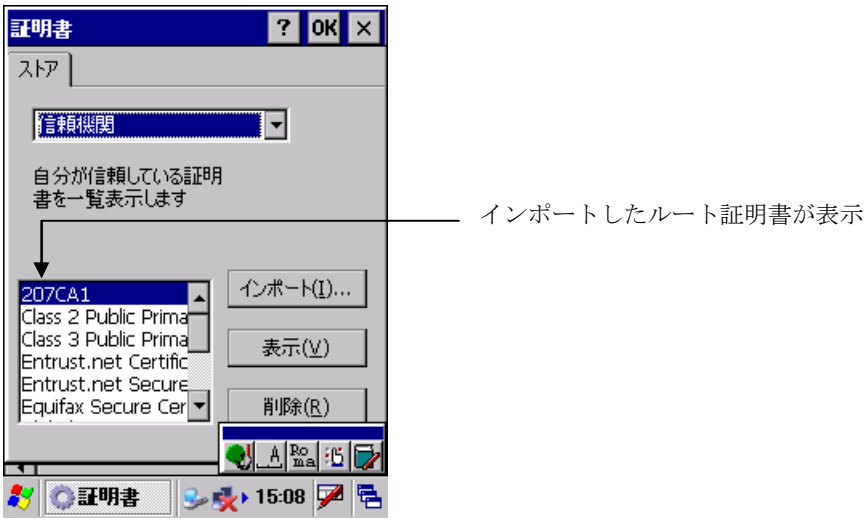
3．“戻る”をタップ

4．確認

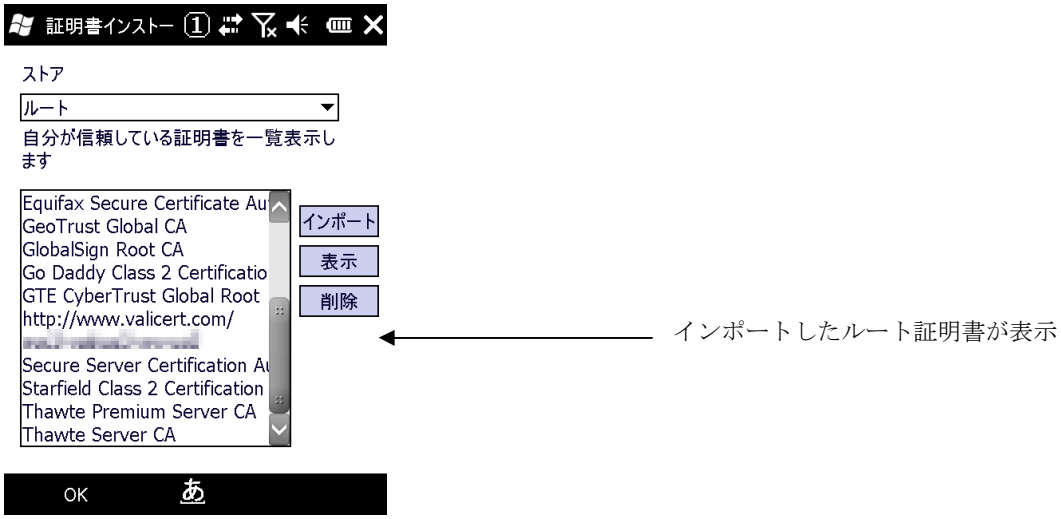
5．“インストール”をタップ

7-1-7.ルート証明書インポートの終了・確認

インポートが成功すると　信頼している証明書の一覧表示に表示されます。



CE 画面

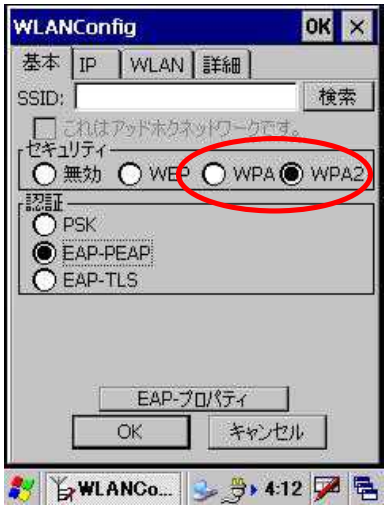


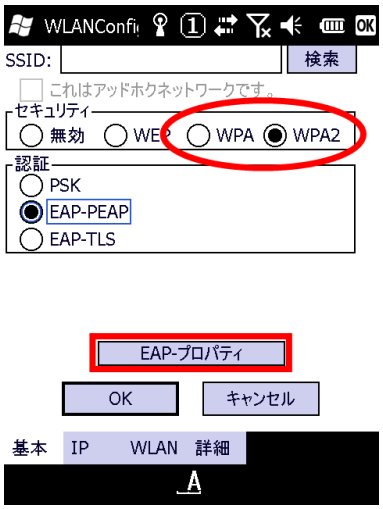
Windows Mobile 画面

7-1-8.ワイヤレスプロパティの設定

“セキュリティ” → “ WPA ”
“認証” → “ EAP-PEAP ”
を選択し、EAP-プロパティボタンをタップします。

CE 画面



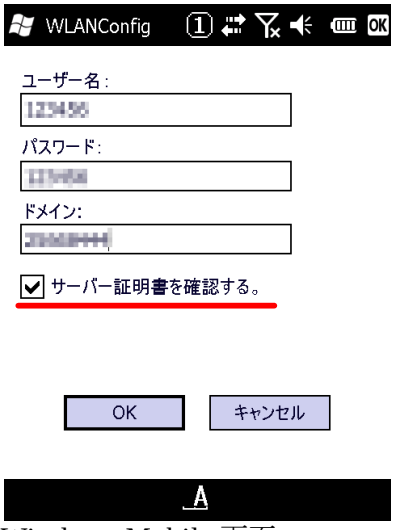


Windows Mobile 画面

IT-300/900、DT-X7M50SB、DT-X7M52SB、DT-5300 では、セキュリティで WPA2 を選択する事が出来ます。
WPA2 では暗号化に AES を使用します。
WPA を選択すると従来どおり TKIP が使われます。

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。

CE 画面



Windows Mobile 画面

『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しなくなり
セキュリティが大きく低下してしまいます。

7-2.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、ハンディターミナルに証明書のインポート（インストール）が必須となります。
設定手順としては、証明書･暗号鍵のインポートのあと EAP -TLS でのワイヤレス LAN 接続設定となります。

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

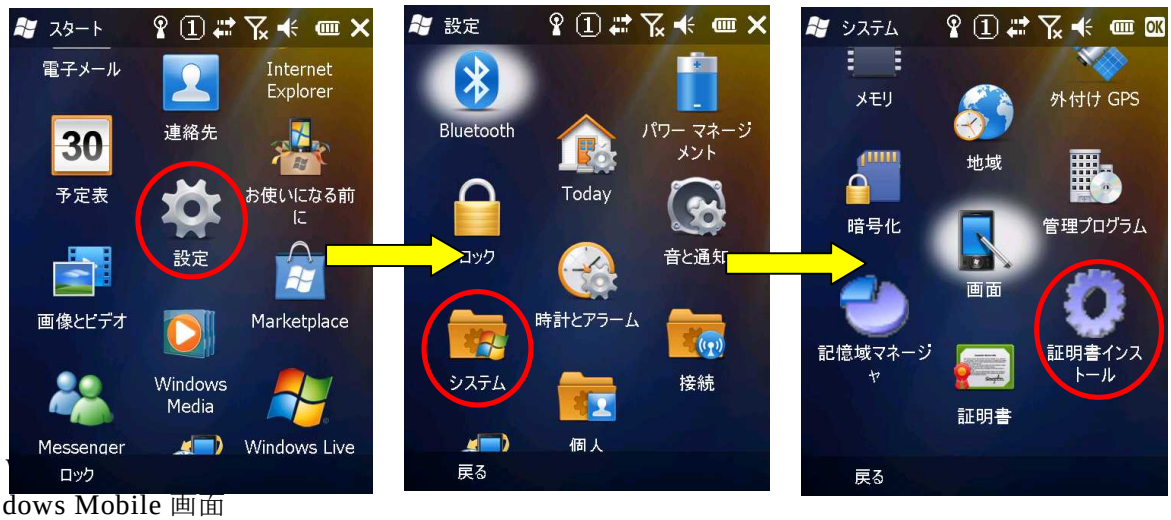
※1 ユーザ証明書（クライアント証明書）のインポートの手順の流れで鍵のインポート時に使用します。
ユーザ証明書と秘密鍵が一緒になったユーザ証明書をインポートする機能はありません。
証明書と秘密鍵は、下記の形式のファイルを別々にインポートする必要があります。
証明書の拡張子は　.cer
秘密鍵の拡張子は　.pvk
となります。

7-2-2.ルート証明書のインポート

CE OS の証明書のインポートはコントロールパネルの証明書で行います。

CE 画面

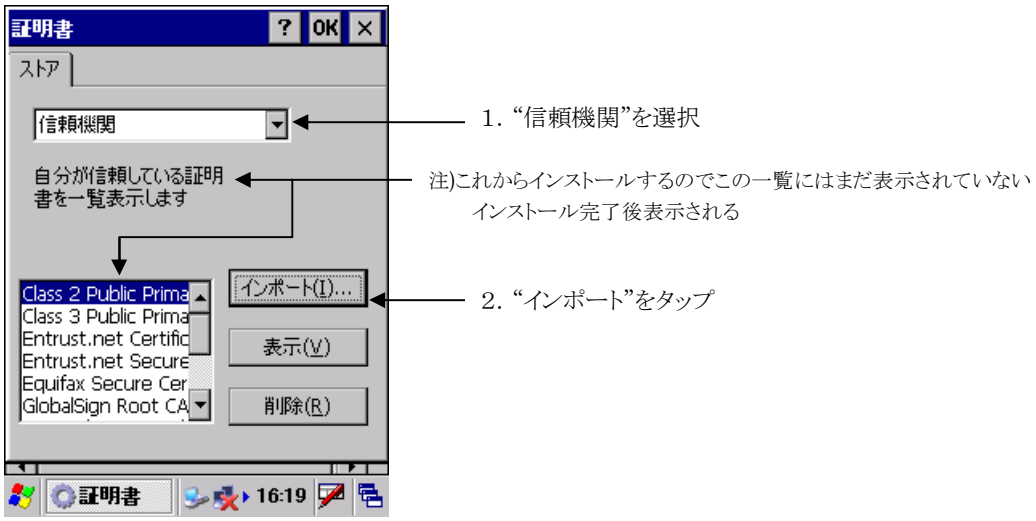
Windows Mobile OS の証明書のインポートは設定からシステムを選択し証明書インストールで行います。



Windows Mobile 画面

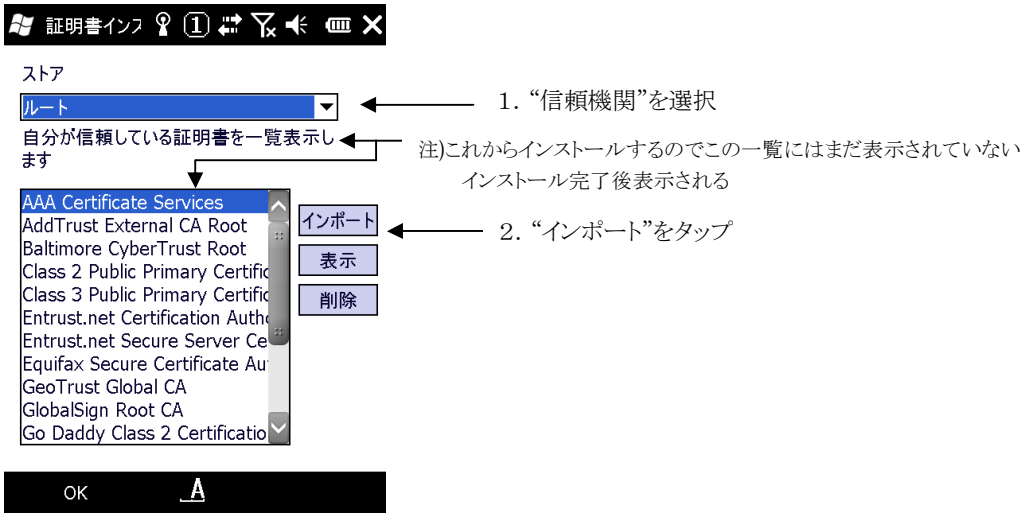
アクティブメニュー画面

ルート証明書のインポートは　“信頼期間”を選択して、“インポート”をタップします。



CE 画面

Windows Mobile OS のルート証明書のインポートは　“ルート”を選択して、“インポート”をタップします。



Windows Mobile 画面

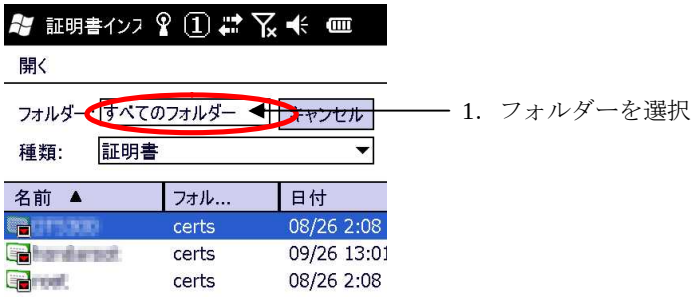
7-2-3.ルート証明書ファイルの選択

CE OS は、証明書をファイルからインポートするので“ファイルから”を選択して、“ＯＫ”をタップします。

CE 画面

“ＯＫ”のタップで証明書が置かれているフォルダーの選択画面が表示されます。

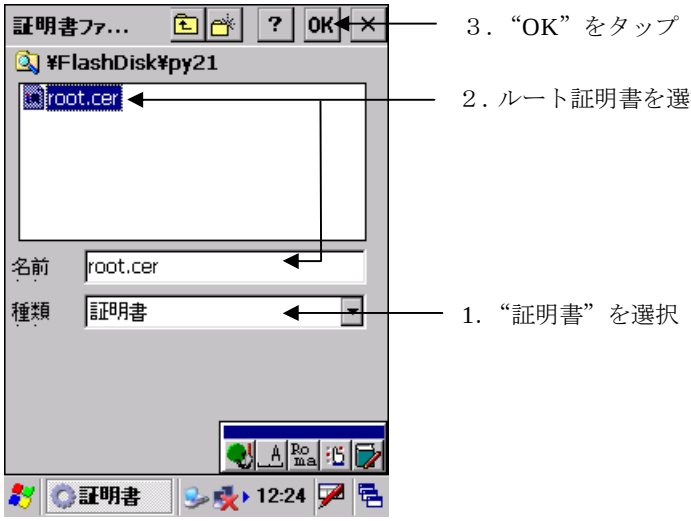
Windows Mobile OS は証明書が存在するフォルダーを選択するか、“すべてのフォルダー”を選択します。



Windows Mobile 画面

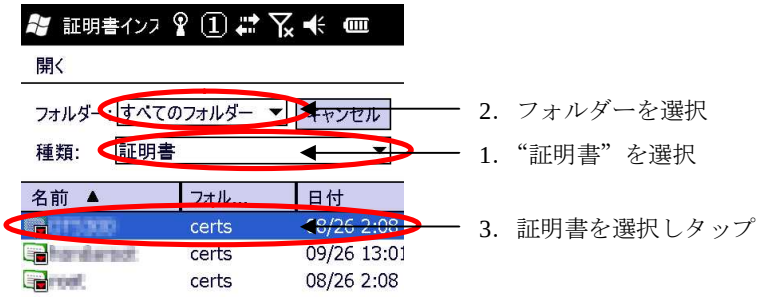
7-2-4.ルート証明書のインポート

CE OS は、種類を　“証明書“　にしてマイデバイスより、コピーした証明書ファイルのあるフォルダーを選択するとコピーした証明書の一覧が表示されます。
表示された証明書の一覧の中から、ルート証明書を選択し“ＯＫ”をタップします。



CE 画面

Windows Mobile OS は、種類を“証明書“にしてフォルダーを“すべてのフォルダー“、またはコピーした証明書ファイルのあるフォルダーを選択するとコピーした証明書の一覧が表示されます。
表示された証明書の一覧の中から、ルート証明書を選択しタップします。



Windows Mobile 画面

7-2-5.ルート証明の確認

CE OS は、ルート証明書ストアの確認画面が表示されます。

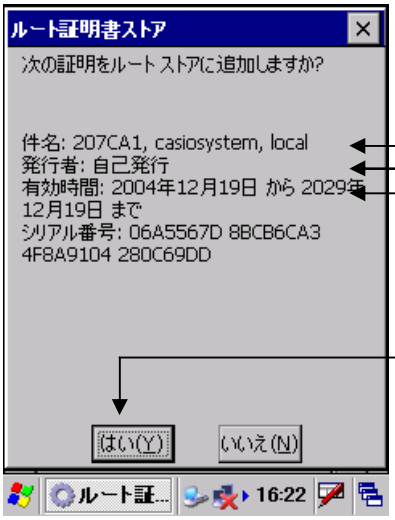
件名にルート証明書を作成した認証局の名前

発行者　本例の場合に内部のＣＡサーバで作成したので自己発行になっています

有効期間

などが表示されます。

インポートする証明書に間違いがないか確認して“はい”をタップします。



1．確認

2．“はい”をタップ

Windows Mobile OS は、ルート証明書のインストールの確認画面が表示されます。

“次へ”をタップします。“要求者”をタップします。

サムプリント

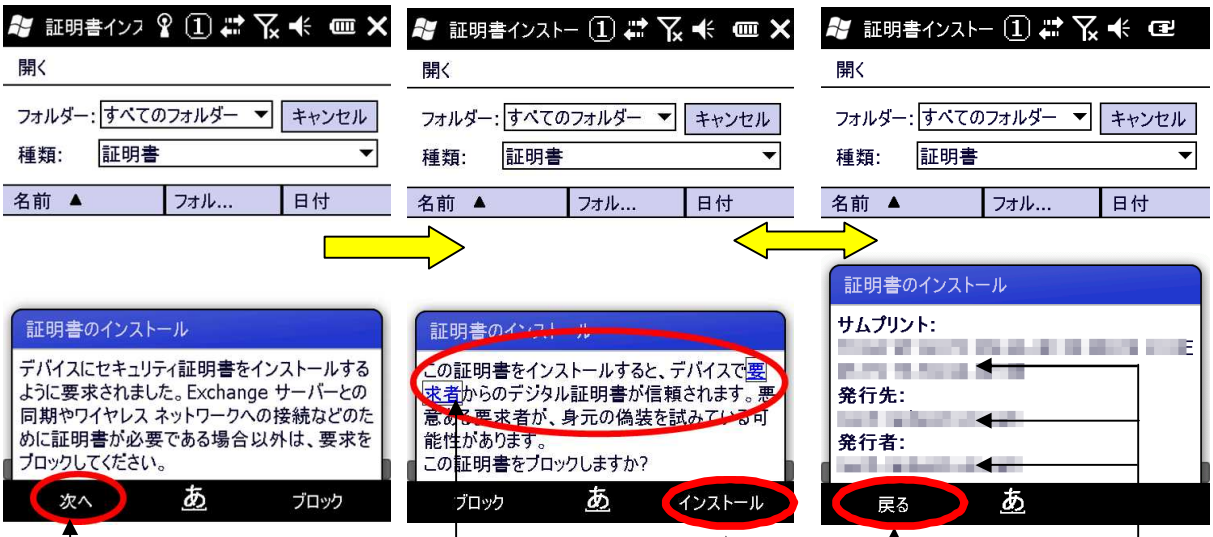
発行先

発行者

が表示されます。

インポートする証明書に間違いがないか確認して“戻る”をタップします。

“インストール”をタップします。

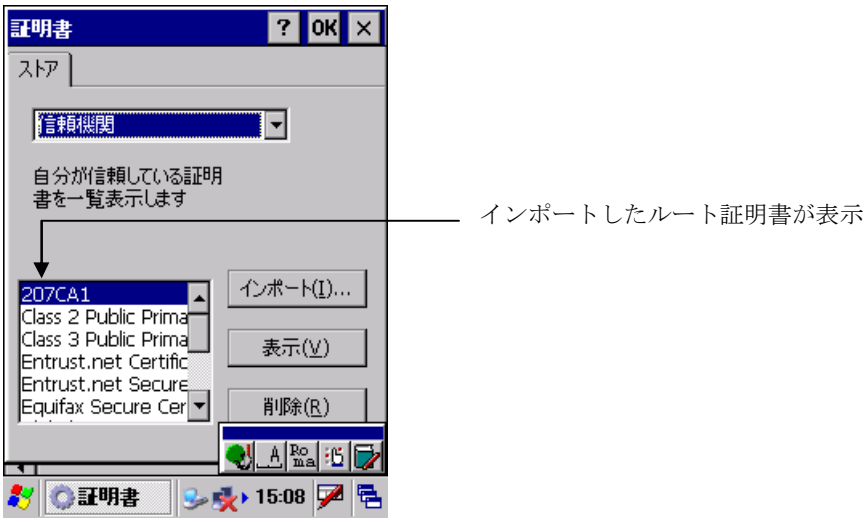


1．“次へ”をタップ　2．“要求者”をタップ　3．“戻る”をタップ　4．確認

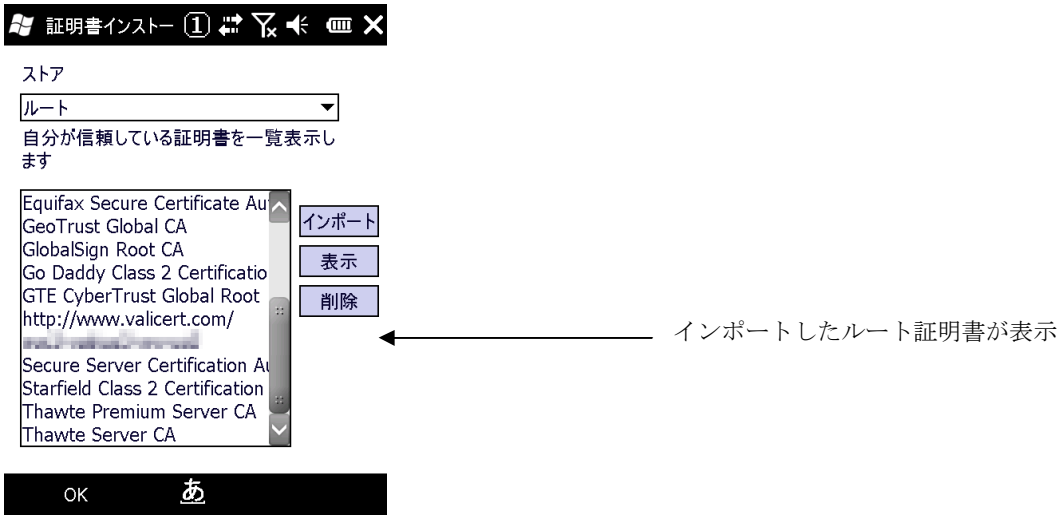
5．“インストール”をタップ

7-2-6.ルート証明書インポートの終了・確認

インポートが成功すると　信頼している証明書の一覧表示に表示されます。



CE 画面



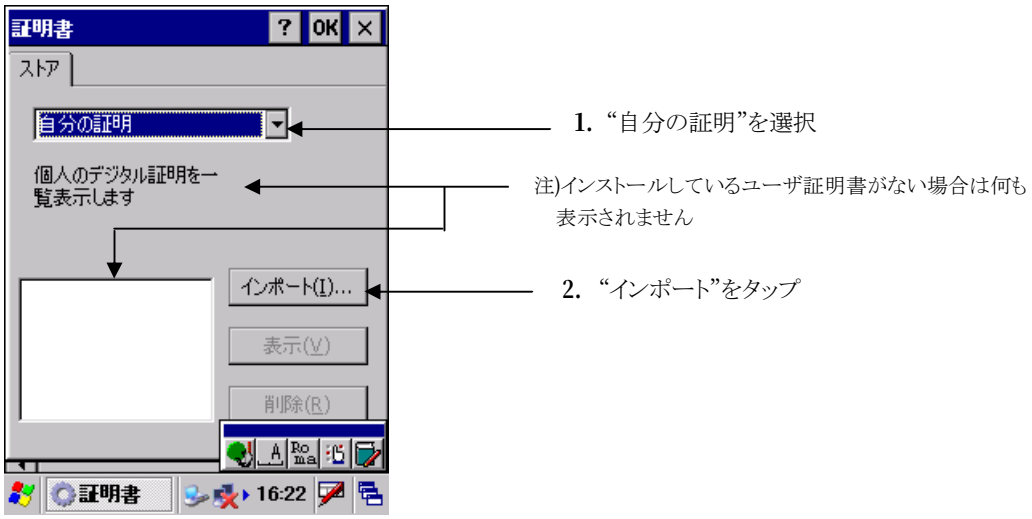
Windows Mobile 画面

7-2-7.ユーザ証明書のインポート

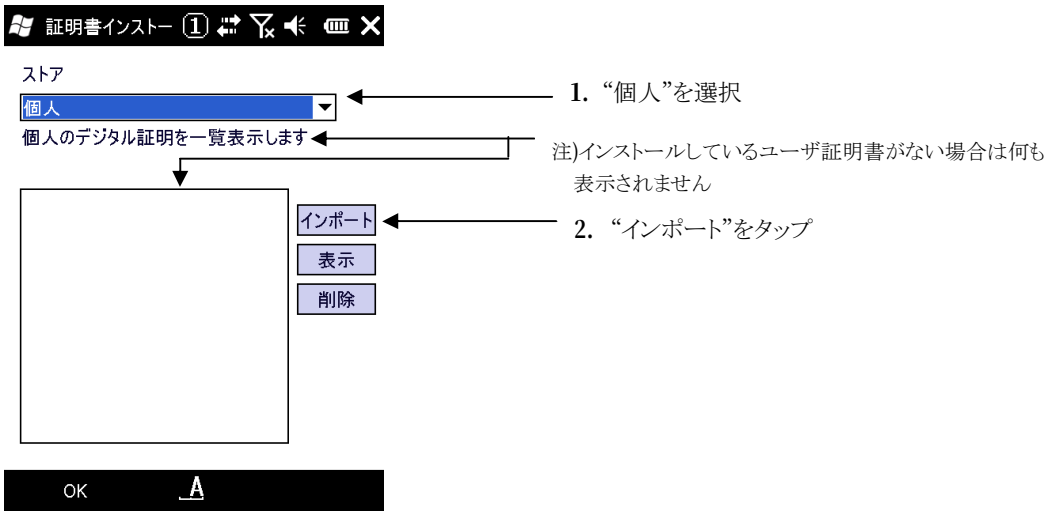
インポート手順として、初めにユーザ証明書をインポートし、後から秘密鍵をインポートします。

7-2-7- 1 個人デジタル証明の選択

ユーザ証明書のインポートは“自分の証明”を選択して、“インポート”をタップします。



CE 画面



Windows Mobile 画面

7-2-7-２ユーザ証明書ファイルの選択

CE OS は証明書をファイルからインポートするので“ファイルから”を選択して、“ＯＫ”をタップ。

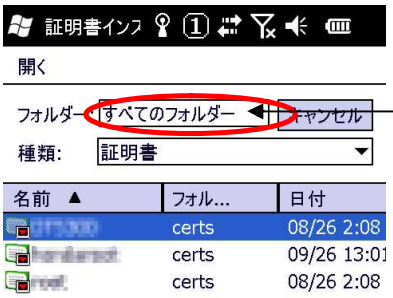
2. “ＯＫ”をタップ

1. “ファイルから”を選択

CE 画面

“ＯＫ”のタップで証明書が置かれているフォルダーの選択画面が表示されます。

Windows Mobile OS は証明書が存在するフォルダーを選択するか、“すべてのフォルダー”を選択します。



1. フォルダーを選択

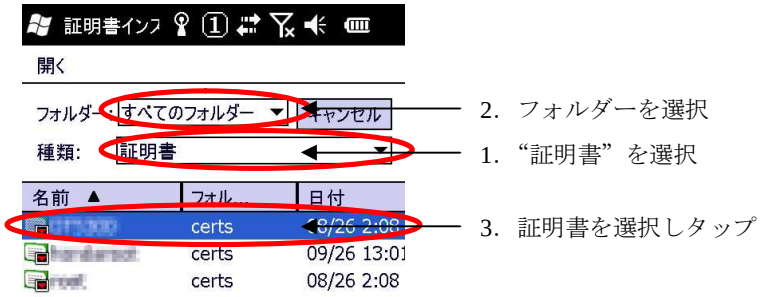
Windows Mobile 画面

7-2-7-３ユーザ証明書のインポート

CE OS は、ルート証明書のインポートと同様に“ＯＫ”のタップで証明書が置かれているフォルダーの選択画面が表示されます。
種類を“証明書“　にして、コピーしたユーザ証明書ファイルのあるフォルダーを選択すると一覧が表示されます。
表示された証明書の一覧の中から、インポートするユーザ証明書を選択し“ＯＫ”をタップします。

CE 画面

Windows Mobile OS は、種類を“証明書“にしてフォルダーを“すべてのフォルダー“、またはコピーした証明書ファイルのあるフォルダーを選択するとコピーした証明書の一覧が表示されます。
表示された証明書の一覧の中から、ユーザ証明書を選択しタップします。



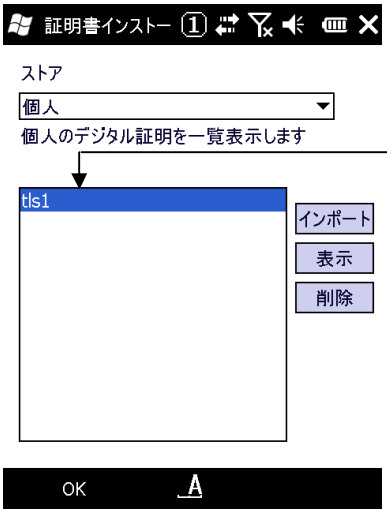

Windows Mobile 画面

7-2-7-４ユーザ証明書インポートの終了・確認

ユーザ証明書のインポートに成功すると、個人のデジタル証明の一覧に表示されます。

インポートしたユーザ証明書が表示されている

CE 画面

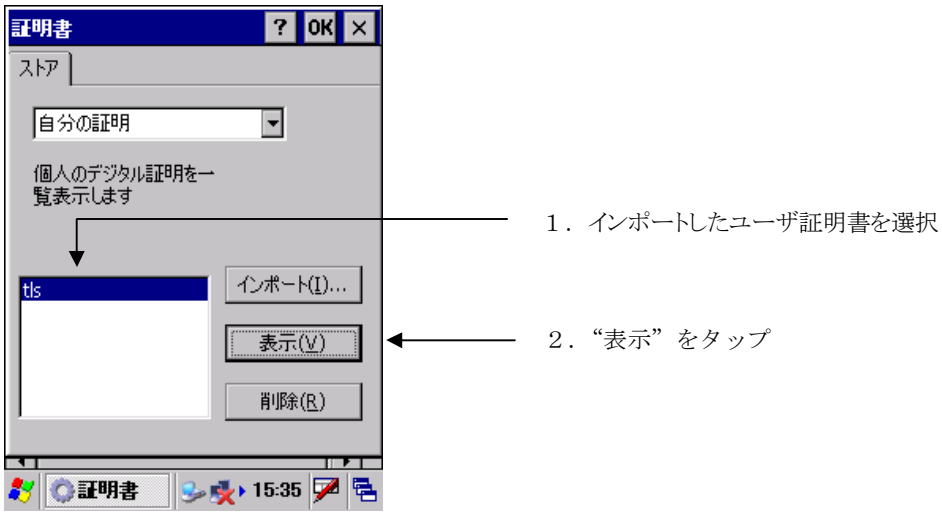


インポートしたユーザ証明書が表示されている

Windows Mobile 画面

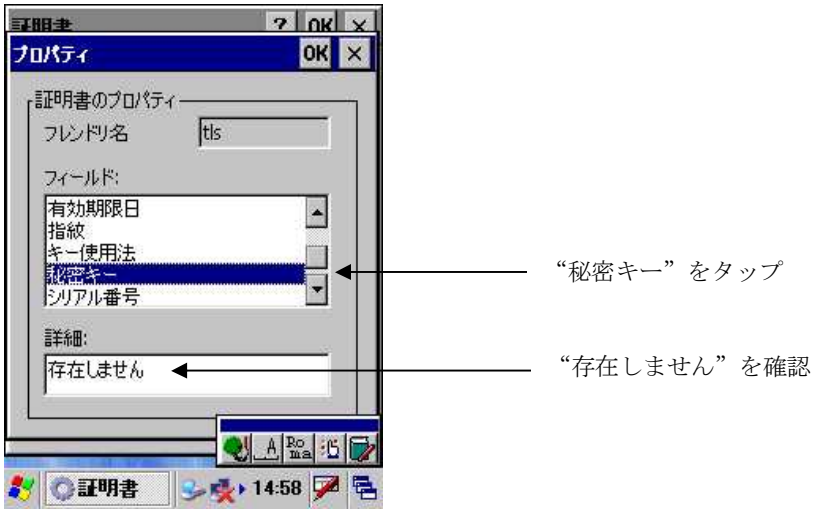
7-2-7-５秘密鍵インポートの確認

CE OS は、インポートしたユーザ証明書を表示し秘密鍵のインポートを確認します。
インポートしたユーザ証明書を選択して“表示”をタップします。

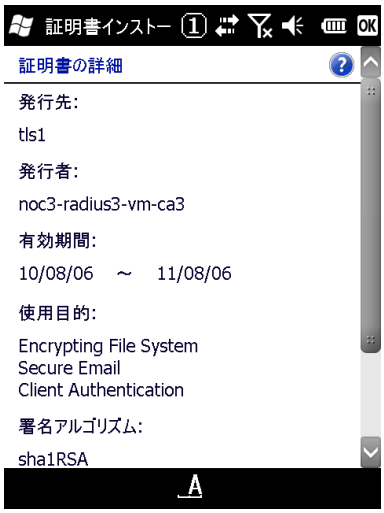


CE 画面

“秘密キー”を選択し、詳細を確認します。



CE 画面



Windows Mobile 画面

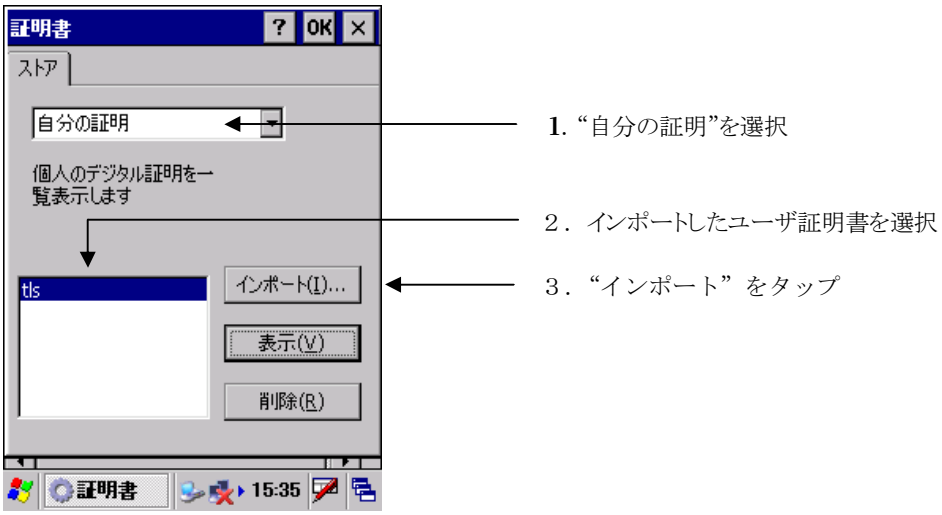
Windows Mobile OSでは“表示”をタップしても秘密キーの項目が表示されません。

7-2-8.秘密鍵のインポート

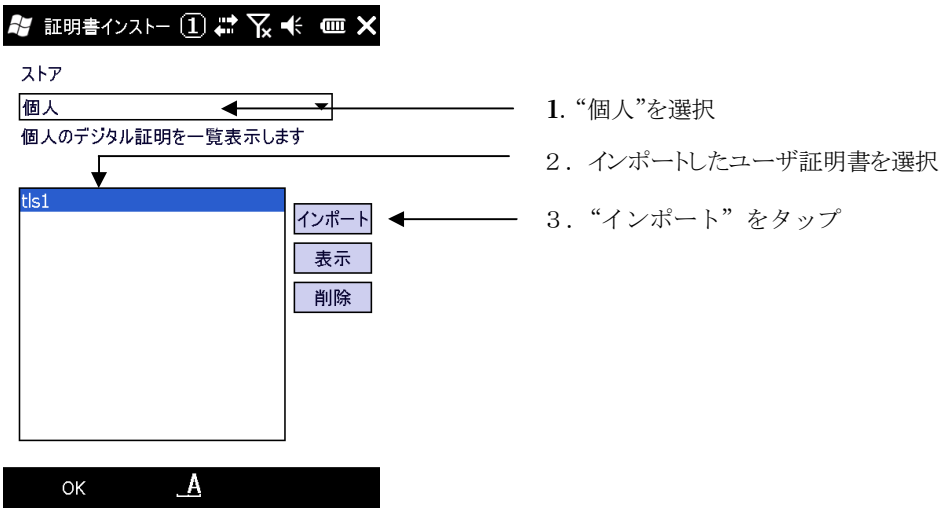
7-2-8- 1 自分の証明のインポートを選択

インポートしたユーザ証明書に秘密鍵をインポートします。

CE OS は“自分の証明書”を Windows Mobile OS は“個人”を選択して、ユーザ証明書を選択し“インポート”をタップします。



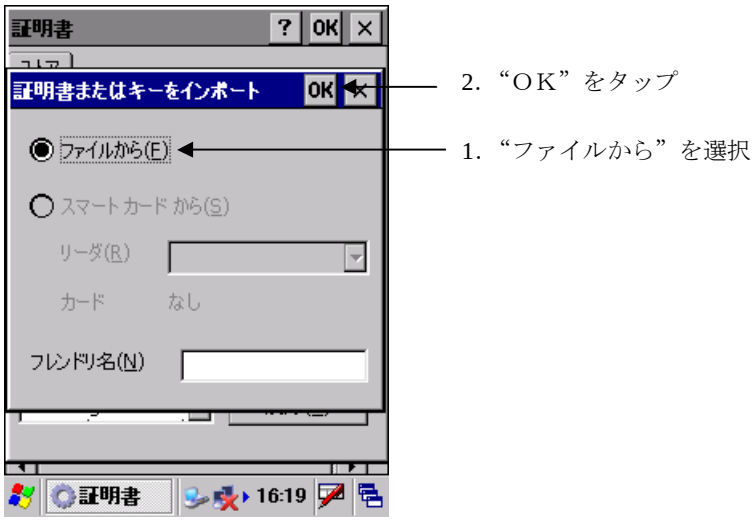
CE 画面



Windows Mobile 画面

7-2-8-２ユーザ証明書秘密鍵ファイルの選択

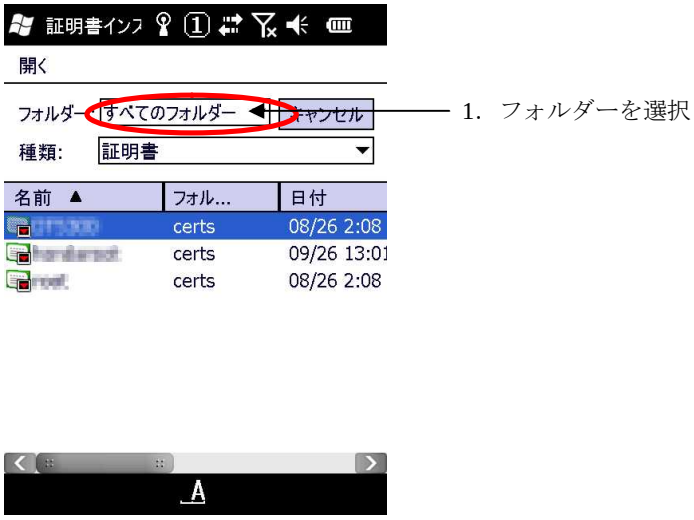
CE OS は、キーをファイルからインポートするので“ファイルから”を選択して、“ＯＫ”をタップします。



CE 画面

“ＯＫ”のタップで証明書が置かれているフォルダーの選択画面が表示されます。

Windows Mobile OS はキーが存在するフォルダーを選択するか、“すべてのフォルダー”を選択します。



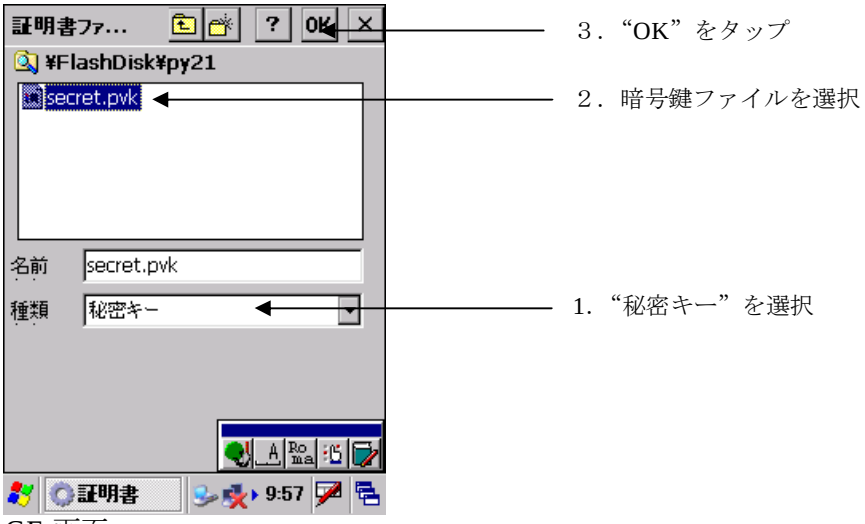
Windows Mobile 画面

7-2-8-３ユーザ証明書秘密鍵のインポート

CE OS は、証明書のインポートと同様に OK のタップで暗号鍵が置かれているフォルダーの選択画面が表示されます。

ファイルの種類を　“秘密キー“　にして、コピーした秘密鍵ファイルのあるフォルダーを選択すると一覧が表示されます。

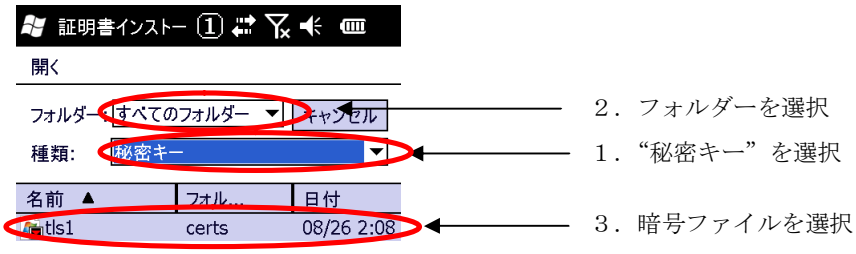
表示された証明書の一覧の中から、暗号鍵ファイルを選択し“ＯＫ”をタップします。



CE 画面

Windows Mobile OS は、種類を“秘密キー“にしてフォルダーを“すべてのフォルダー“、またはコピーした証明書ファイルのあるフォルダーを選択するとコピーした秘密鍵ファイルの一覧が表示されます。

表示された証明書の一覧の中から、秘密鍵ファイルを選択しタップします。

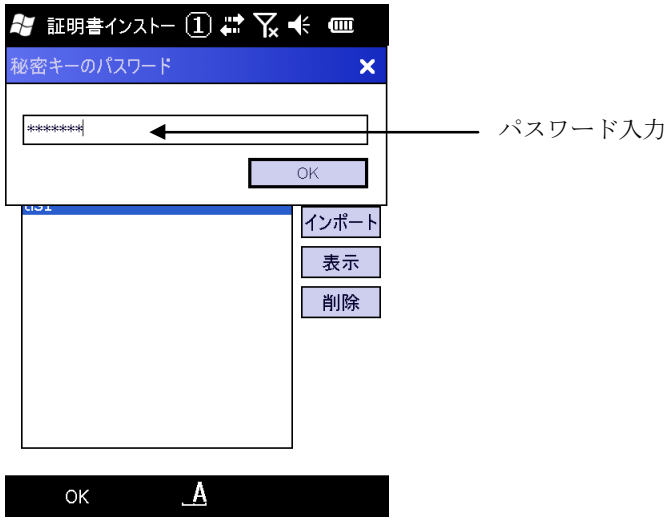


Windows Mobile 画面

7-2-8-４パスワード入力

ＣＡサーバ上で秘密鍵作成時に指定したパスワードを入力します。

CE 画面



Windows Mobile 画面

7-2-8-５ユーザ証明書暗号鍵インポートの終了

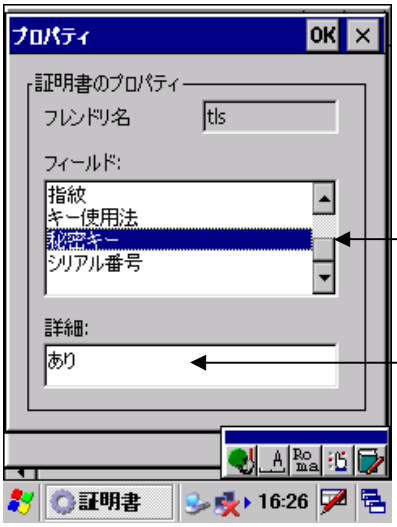
パスワード認証が成功すると証明書設定の画面に戻ります。
CE OS は、インポートした暗号鍵を確認するために証明書を表示させます。

１．暗号鍵をインポートしたユーザ証明書を選択

２．“表示”をタップ

7-2-8-６ユーザ証明書暗号鍵インポートの確認

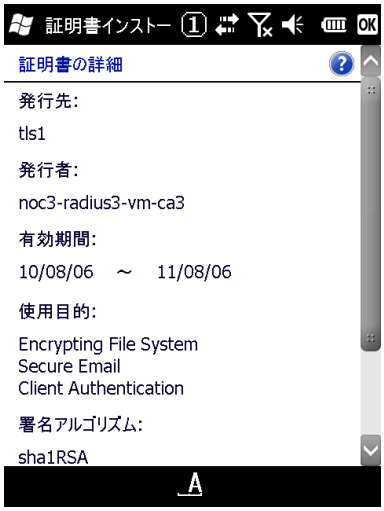
CE OS は“秘密キー”を選択して、詳細が“あり”になっていることを確認します。



１．“秘密キー”をタップ

２．“あり”を確認

以上で、証明書のインポートは終了になります。

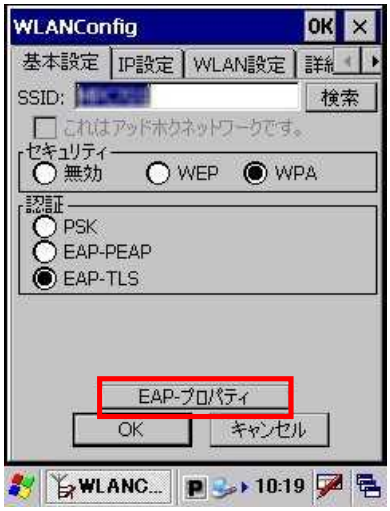


Windows Mobile 画面

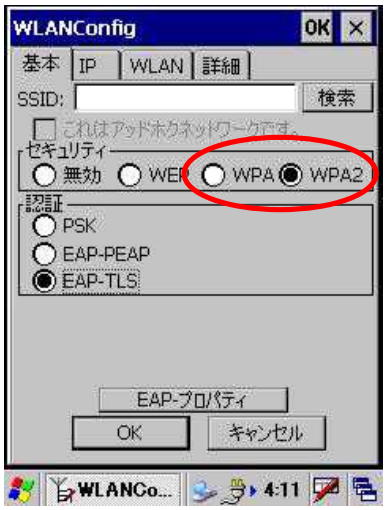
Windows Mobile OSでは“表示”をタップしても秘密キーの項目が表示されません。

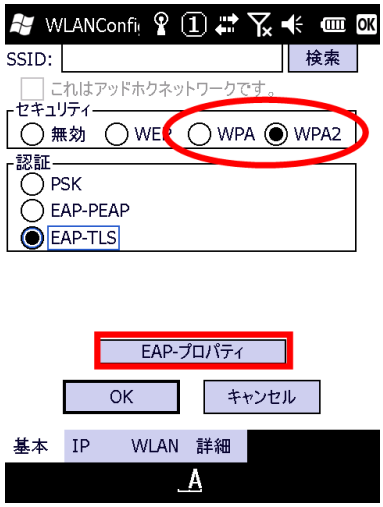
7-2-9.ワイヤレスプロパティの設定

“セキュリティ” → “ WPA ”
“認証” → “ EAP-TLS ”
を選択し、EAP-プロパティを選択します。



CE 画面

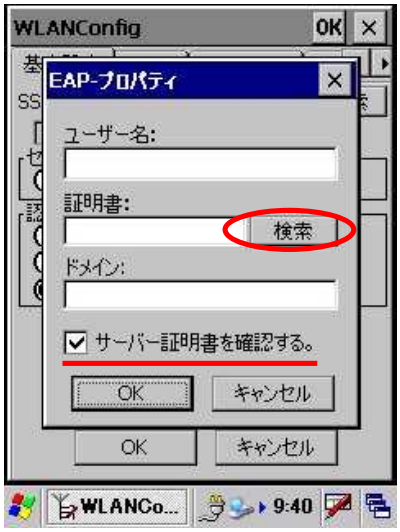




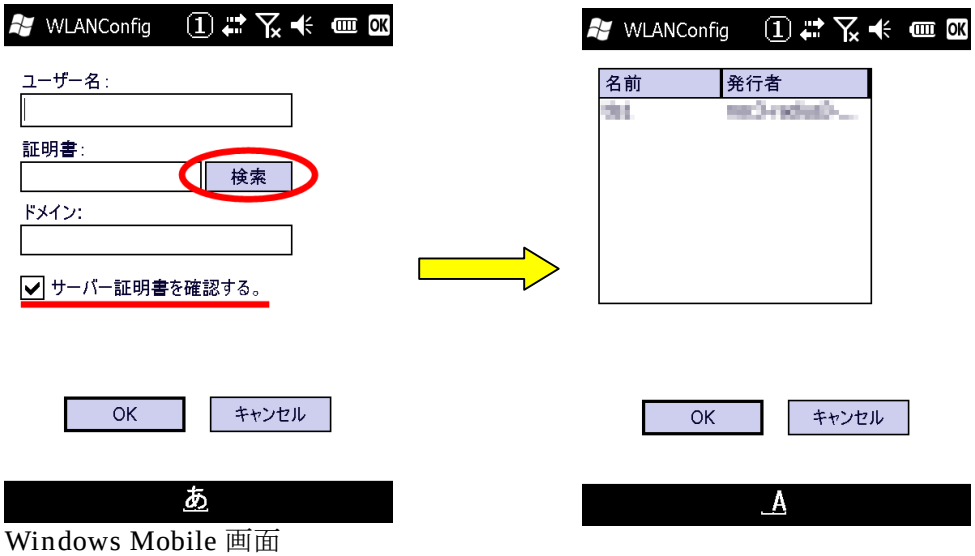
Windows Mobile 画面

IT-300/9000 、 DT-X7M50SB 、 DT-X7M52SB 、 DT-5300 では、セキュリティで WPA2 を選択する事が出来ます。
WPA2 では暗号化に AES を使用します。
WPA を選択すると従来どおり TKIP が使われます。

証明書の選択
EAP－プロパティの認証で使用するユーザ証明書を選択します。
接続時に入力するユーザ・証明書・ドメイン情報を入力します。



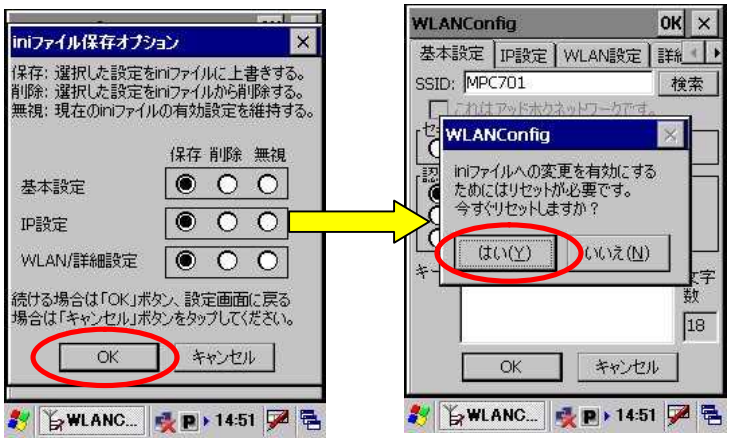
CE 画面



Windows Mobile 画面

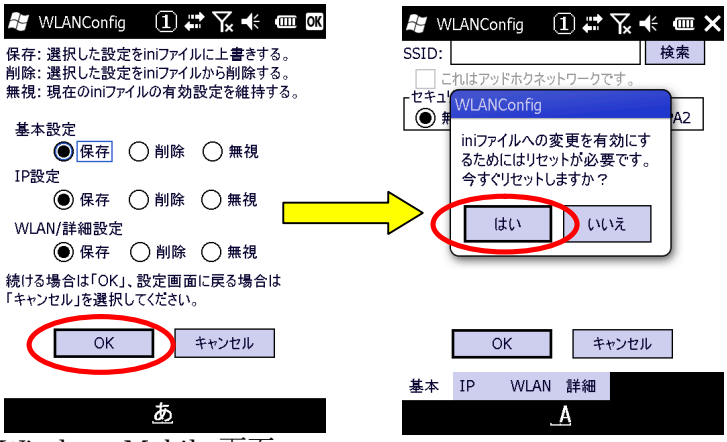
『サーバー証明書を確認する』のチェックを外すとサーバ証明書を確認しなくなり、
ユーザ証明書（と秘密鍵）でのみの認証になります。
セキュリティが弱くなるのでお勧めできません。
チェックを入れたままにする事をお勧めします。

8. 設定の保存



CE 画面

設定が終了すると、inファイルへ保存するか聞いてきます。
通常はそのまま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。



Windows Mobile 画面

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。
自動的にリセットします。

9. 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。

9-1.ネットサーチを起動する

CE　OS

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。

DT-5200の初期画面

その他機器の初期画面

DT-X7 では、10 キーでの操作が可能です。

【1】⇒相手局一覧表示
【2】⇒詳細画面

以下の操作で、画面呼び出しを行います。
【4】⇒ping 操作画面
【5】⇒電波強度グラフ表示

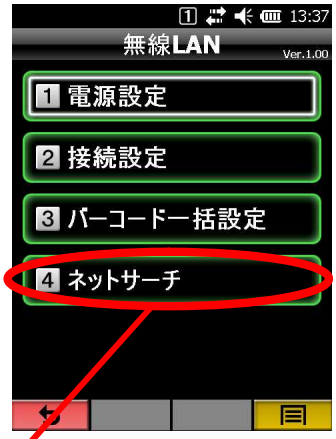
【0】⇒ネットサーチ終了

一覧表示画面では、
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。

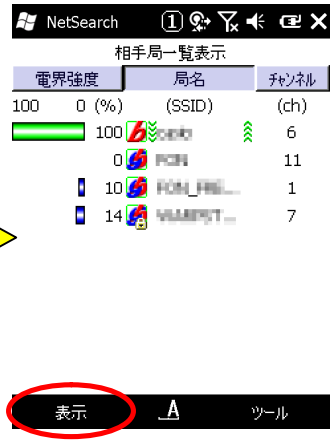
Windows Mobile OS

スタートメニューからネットサーチを選択します

アクティブメニューからネットサーチを選択します

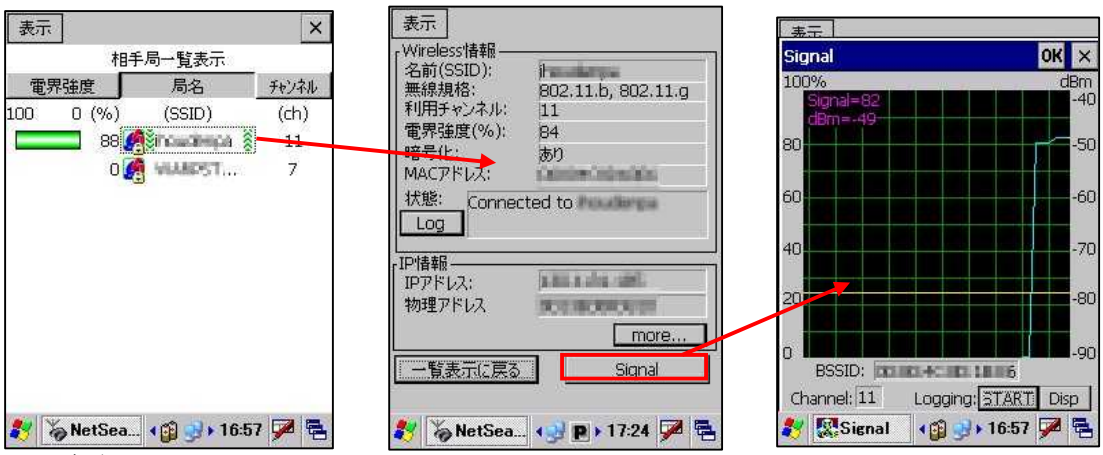


WMの初期画面

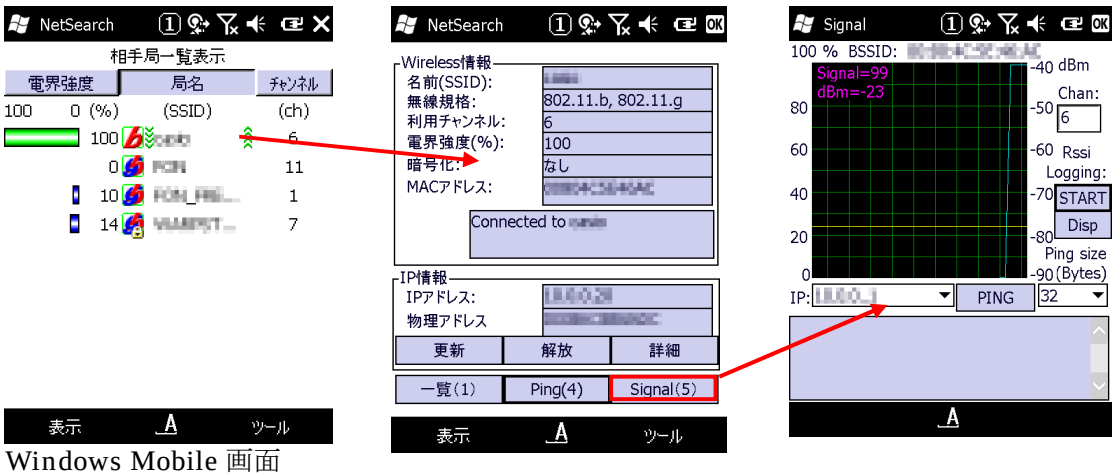


一覧表示画面では、
SSIDが緑ではさまれているアクセスポイントと接続しています。

9-2.詳細情報を確認する



CE 画面



Windows Mobile 画面

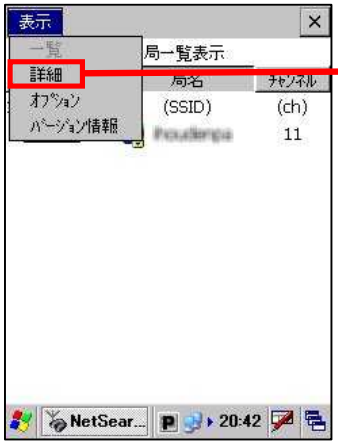
使用中のSSIDを選択すると詳細情報が確認できます

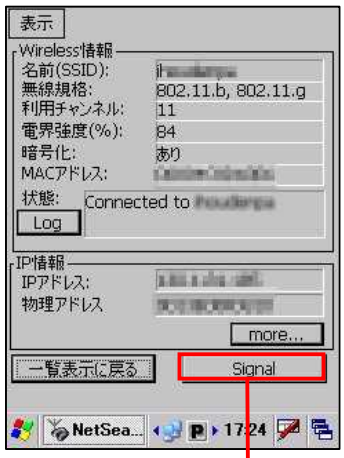
Signalボタンを選択すると電波強度の表示が出来ます

電波強度や、ローミング閾値がグラフで確認できます
※DT-X7では、10キーの【5】で画面を表示します。

DT-X7 では、10 キーの【1】で『一覧画面』
【2】で『詳細画面』へ切替が出来ます。
【0】でネットサーチを終了します。

9-3.SSID が一覧に表示されない場合

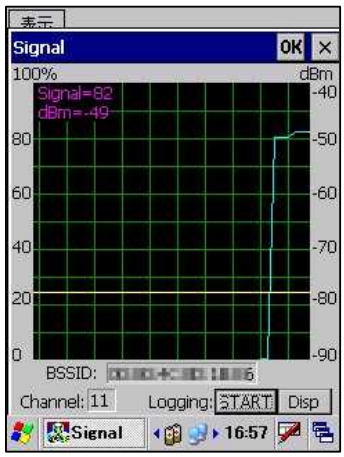




アクセスポイント側で SSID を隠す設定になっている場合

DT-5200 では、ネットサーチの一覧画面に 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。



9-4.ping 疎通テストによる通信の確認

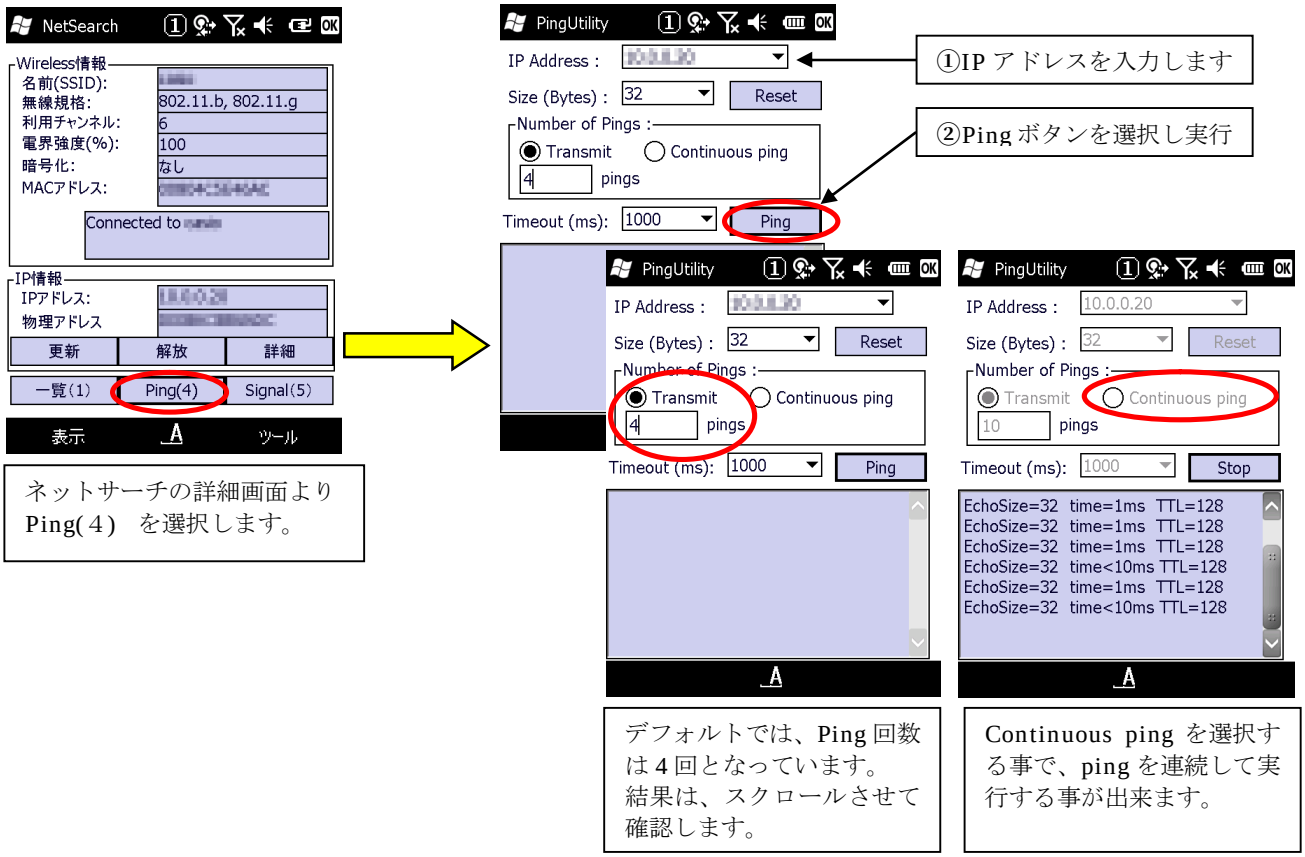
9-4-1.DT-5200 シリーズでの場合

コマンドプロンプトで、【ping】コマンドを使用します。
コマンドの入力は、『Fn+0』で、ソフトキーボードを表示して入力します。

ping 結果の表示は、画面に収まりきらないので、
スクロールさせて表示を確認します。

9-4-2.Windows Mobile シリーズでの場合

Windows Mobile では、コマンドプロンプトの【ping】コマンドありません。
ネットサーチの詳細画面で,【Ping(4)】ボタンを選択する事で、PingUtility が起動します。
テンキーの『4』を選択するか、『Ping(4)』ボタンをタップします。



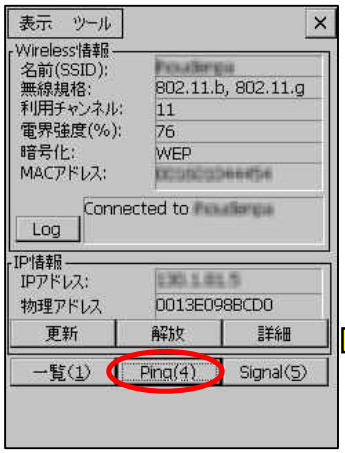
ネットサーチの詳細画面より
Ping(4) を選択します。

デフォルトでは、Ping 回数は 4 回となっています。
結果は、スクロールさせて確認します。

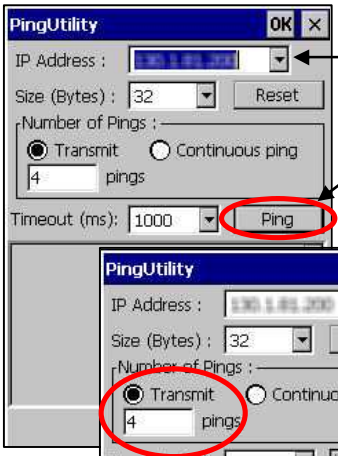
Continuous ping を選択する事で、ping を連続して実行する事が出来ます。

9-4-3.Windows CE シリーズでの場合

Windows CE では、コマンドプロンプトの【ping】コマンドありません。
ネットサーチの詳細画面で,【Ping(4)】ボタンを選択する事で、PingUtility が起動します。
テンキーの『4』を選択するか、マウスエミュレートモードで『Ping(4)』ボタンを選択します。

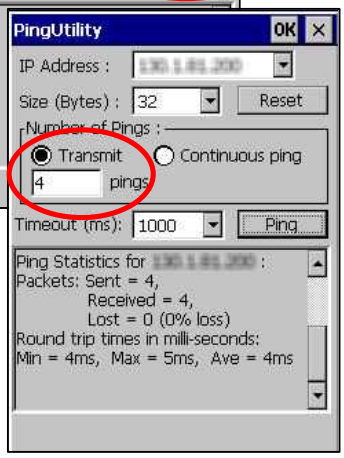


ネットサーチの詳細画面より
Ping(４)　を選択します。

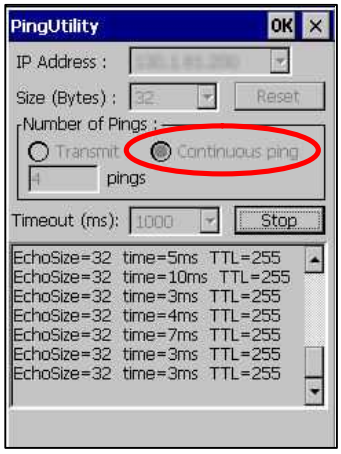


①IP アドレスを入力します

②Ping ボタンを選択し実行



デフォルトでは、Ping 回数は 4 回となっています。
結果は、スクロールさせて確認します。



Continuous ping を選択する事で、ping を連続して実行する事が出来ます。

10. ご注意

10-1.DT-5200M50 をサービスパックリリース以前よりご使用の場合

・ **NetUI(OS 提供の無線設定ツール)をご使用の場合**

　無線 LAN が設定済の DT-5200 にサービスパックを導入しただけでは設定が消える心配はありませんが下記の点にご注意ください。
サービスパックインストール後に、無線設定を行い、設定を保存すると
リセット後に、保存した無線 LAN の設定が有効になり、以前の設定は消えてしまいます。
サービスパックのインストール後には、必ず無線 LAN 設定ツールを使用し、
無線 LAN の設定をやり直していただけるようお願い致します。

・ **ネットサーチツール(カシオ提供の無線 LAN 設定ツール)をご使用の場合**

　無線 LAN の設定は、『¥FlashDisk¥SystemSettings¥wlancfg.ini』に保存されています。
サービスパックインストール後に、無線 LAN 設定を行う場合、以前の設定を修正(引継ぐ)事が可能となります。

・ **従来より DT-5200 をご使用で、サービスパック未適用で運用されている場合**

　事前に十分なテストを行った上でサービスパックをご利用頂けるようお願い致します。
従来からの物にサービスパックを適用するか、修理機のサービスパックを削除してから導入するなどサービスパックの適用の有無が混在しないようご配慮をお願い致します。
※カシオでは、サービスパックをインストールした状態で運用頂く事を推奨いたします。
※サービスパックをご使用にならない場合には、ご使用になるソフトウェアをインストールする前に、FlashiDisk\CE\ARM フォルダーの『ServicePackDT5200.102.CAB』を削除の後フルリセットをかけてください。

10-2.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→ネットワークとダイヤルアップ接続 から以下の無線アイコンを選択する。
Windows Mobile ではワイアレスマネージャーから設定する。

・PY21BG1(DT-5200)
・PY55BG1(DT-X7)
・SDIO86861(DT-5300)
・WLZX_SD1(DT-5300 a 準拠モデル)
・SDIO86861(DT-X8)
・SDIO8686 Wirless Card(IT-300)
・SDIO8686 Wirless Card(IT-9000)

事で 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。

カシオ計算機お問い合わせ窓口

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/ht/

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)