CASIO

アクティブセキュリティ
ユーザーズマニュアル

このマニュアルは、アクティブセキュリティの操作について記載します。

Ver. 1.12

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	ページ	説明
1.00	2009.07		新規作成
1.01	2009.09	4	インストール方法追加
		6	バージョン確認方法追加
		6-13	電池残量監視関連注釈追加
		17	電池残量監視機能追加
		25	背景画像ファイル名変更／追加
		2	NFC 認証タイムアウト時の挙動変更
		21-22	呼び出し関数の説明ににアドミン権限を追加 戻り値 0x0004 を追加
1.10	2010.03	-	リモートセキュリティの追加
		-	Windows Mobile 版の追加
1.12	2010.04	2	ユーザ切り替え時の注意書き追加
		34	アカウント情報ファイルパス追加

目次

1. 概要

カシオアクティブセキュリティは、次の2種類のセキュリティシステムを提供します。

セキュリティシステム種	役割
アクティブローカルセキュリティシステム （以下 ローカルセキュリティ）	特定のユーザのみが端末を利用可能とします。
アクティブリモートセキュリティシステム （以下 リモートセキュリティ）	遠隔地から SMS を介してデータの保護を行います。

また、ローカルセキュリティ支援として定義暗号化ツール、アカウント情報テーブル作成ツールを提供します。

以下に本システムで提供する基本機能と上記2種のセキュリティとの関係を記します。

番号	基本機能	内容	リモート セキュリティ	ローカル セキュリティ
1	端末ロック機能	端末内のデータ保護および漏洩防止のために、端末の操作を抑止する機能です。電源ボタン、タッチパネル、キーボードの操作のみ有効となり、アプリケーションの起動や ActiveSync によるファイルアクセスを禁止します。	○	○
2	ユーザ認証機能	ユーザ認証画面を表示します。デフォルトではNFC認証／パスワード認証機能を提供します。また、認証実装用 API を公開することで、別の認証機能を実装することを可能とします。	×	○
3	位置検索機能	端末のGPS位置情報を親端末に通知する機能です。	○	×
4	ファイル削除機能	指定回数以上の認証エラーが連続して発生した場合、指定のフォルダ／ファイルを削除します。	○	○

○:使用する　×:使用しない

1.1 ソフトウェア構成と動作環境

本システムを構成するソフトウェアとその動作環境について以下に記します。

【端末側動作環境】

項目	内容
ハードウェア	DT-5300 CE/WM
OS	Windows CE 6.0, Windows Mobile 6.5
対応ロケール	日本語/英語
必須ソフトウェア	.NETCompactframework2.0 以上
必須ライブラリ	業務ログライブラリ/WANGPRS ライブラリ/システムライブラリ/NFC ライブラリ

【端末側ソフトウェア一覧】

ソフトウェア	主要機能	対象機種	
		DT-5300CE	DT-5300WM
アクティブローカルセキュリティ	端末ロック／ユーザ認証／データ削除	○	○
アクティブセキュリティ設定	セキュリティ有効設定／誤認証許可回数設定／ログオフ有効時間設定／ソフトキーボード連携設定／削除ファイル・フォルダ設定／親端末電話番号設定	○	○
アクティブセキュリティアカウント設定	アカウント追加／削除、カードテスト、パスワードテスト	○	○
アクティブリモートセキュリティ	セキュリティスクリプト編集／削除、セキュリティスクリプト実行、セキュリティスクリプト実行結果表示、端末位置検索機能	×	○※

※ Professional 版のみ

※ アプリケーション動作中に、電源断やロック等のユーザ認証を必要とする操作を行った場合、セキュリティ保護のためにアプリケーションは強制的に終了します。

【PC 側動作環境】

項目	内容
ハードウェア	IBM PC/AT 互換機
OS	MS-DOS（Windows 内部コマンド）
対応ロケール	日本語/英語
必須ソフトウェア	なし

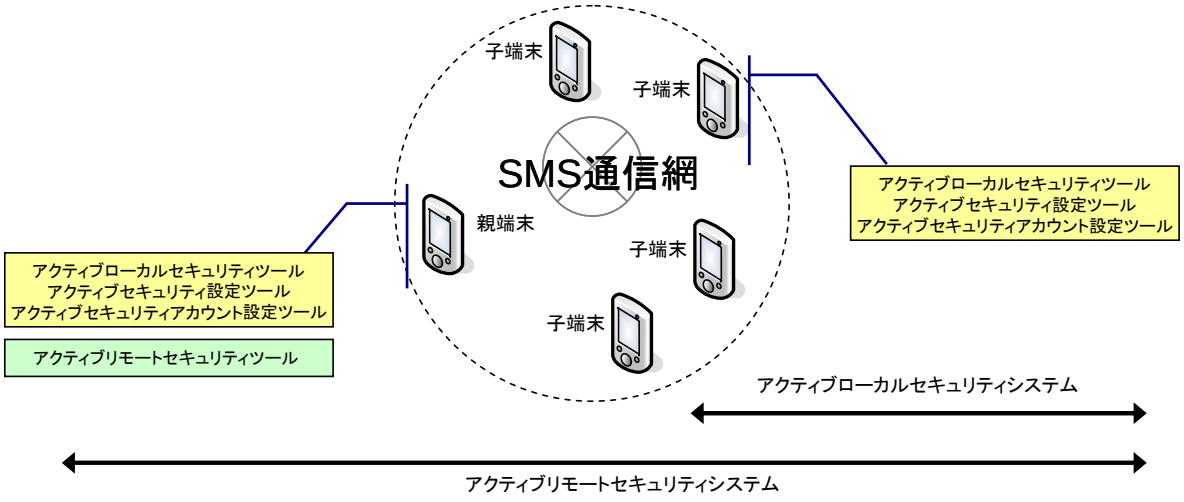
【PC 側ソフトウェア一覧】

ソフトウェア	主要機能
定義暗号化ツール	アクティブセキュリティで参照する定義ファイルを暗号化します。
アカウント作成ツール	CSV フォーマットファイル→アカウント情報テーブルファイルに変換します。

1.1.1　機器構成

ローカルセキュリティは、子端末のみで構成されます。
リモートセキュリティは、制御用親端末（最大 3 台）と、1 台以上の子端末により構成されます。

端末種	動作必須条件	役割
親端末	・NTT DOCOMO もしくは SOFTBANK の SMS/データ通信サービスが使用可能であること。 ・「アクティブリモートセキュリティツール」が動作すること。	「アクティブリモートセキュリティツール」上でセキュリティスクリプトを編集し、子端末に SM として送信します。また、子端末からの応答を受け取り、結果として表示します。
子端末	・NTT DOCOMO もしくは SOFTBANK の SMS が使用可能であること。 ・アクティブセキュリティ設定で親端末の電話番号を登録していること。	親端末から送信された SM を受信し、その内容に沿ったセキュリティ処理を行います。



機器構成と必要なソフトウェア

1.2 ローカルセキュリティについて

端末の電源を入れた後、ユーザを特定するために NFC 認証画面を表示します。
あらかじめ登録済みのユーザアカウント(「1.3ユーザアカウントについて」参照)に合ったカードをかざすか、パスワードを入力することで認証を行い、通常運用画面(デスクトップ)を表示します。
通常運用画面が表示されるまでは端末ロック状態(電源ボタン、タッチパネル、キーボードの操作のみ有効で、アプリケーションの起動や ActiveSync によるファイルアクセスは禁止)となります。
また、認証時に特定の条件を満たした場合にはファイル／フォルダ削除が行われます。
以下に電源 ON からユーザ認証を行い、通常運用画面表示を行うまでの流れを記します。

番号	項目	説明
①	NFC 認証画面	かざされたカードを読み込んで認証を行います。この画面では常に電波を出しています。10 秒間カードを読み込まなかった場合は②NFC 認証ﾀｲﾑｱｳﾄ画面に移行します。また、「パスワード認証画面へ>>」を押下することで③パスワード認証画面へ移行します。
②	NFC 認証ﾀｲﾑｱｳﾄ画面	この画面では電波を出していません。画面をタッチすることで①NFC 認証画面へ移行します。また、「パスワード認証画面へ>>」を押下することで③パスワード認証画面へ移行します。
③	パスワード認証画面	入力されたパスワードで認証を行います。「カード認証画面へ>>」を押下することで①NFC 認証画面へ移行します。

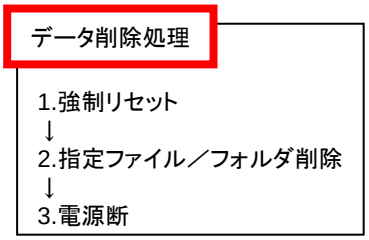
1.2.1　ファイル削除条件について

ファイル削除が適用される条件には以下の2つがあります。

- 認証 NG が指定許容回数以上発生した場合
- ログオフ状態が指定時間以上継続した場合

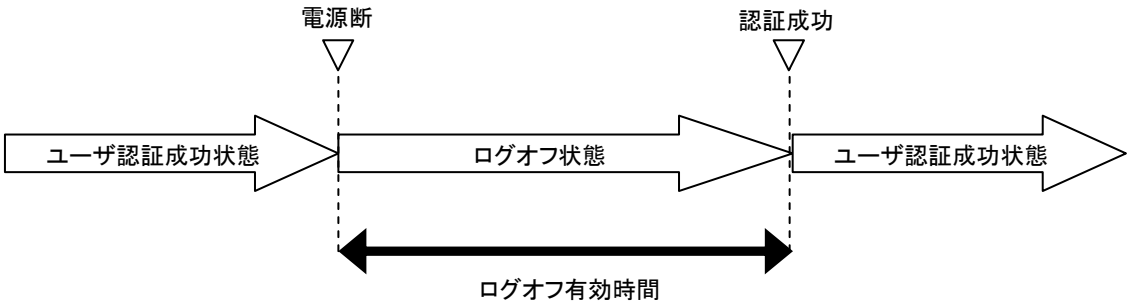
【指定許容回数以上の認証 NG が連続して発生した場合】

前図①NFC 認証画面および③パスワード認証画面で、認証 NG を連続して許容回数以上行った場合、指定したファイル／フォルダを削除します。



【ログオフ状態が指定時間以上継続した場合】

ログオフ有効時間以上のログオフ状態が継続した場合、指定したファイル／フォルダを削除します。



1.2.2　端末ロック状態で着信に応答するには

端末ロックまたは各認証画面状態で着信があった場合は、画面下部に表示される「応答」ボタンを押下するか F3 キーを押下します。

認証画面（着信中）

また、通話を切断する場合は F4 キーを押下してください。

1.3 ユーザアカウントについて

ユーザ認証で参照するユーザ情報をユーザアカウントと呼び、ユーザごとに NFC カードやパスワードでのユーザ認証が可能です。ユーザアカウントには2種類あり、それぞれ通常アカウント、アドミニストレータアカウントと呼びます。アクティブセキュリティ設定ツールやアクティブセキュリティアカウント設定ツール、アクティブリモートセキュリティツールはアドミニストレータ権限を持つアカウントでユーザ認証を行った場合のみ設定の変更が可能となります。アドミニストレータ権限を持つアカウントは必ず1名以上必要となります。1つのユーザアカウントは「アドミニストレータ権限フラグ」「ユーザ名」「パスワード」「NFCデータ」で構成されており、アカウント情報テーブルファイルにまとめて管理しています。（構造詳細は「5.2.3 CSV形式アカウント情報テーブルファイルフォーマット」参照）

このアカウント情報テーブルファイルは「アクティブセキュリティアカウント設定」を用いて端末上での編集を可能としているほか、PC上で作成したCSV形式のアカウント情報テーブルファイルをコンバートして使用する方法があります。（詳細については「5.2アカウント情報テーブル作成」参照）

1.4 動作設定について

本システムの動作に関しては、「アクティブセキュリティ設定ツール」にて設定を変更することが可能です。設定可能な項目を以下に記します。

設定機能	説明
有効無効設定	セキュリティを有効にした場合、セキュリティシステムが常にシステムを監視し、ローカルセキュリティ／リモートセキュリティの機能を提供します。無効とした場合、セキュリティシステムは動作しません。
連続誤認証許容回数設定	ユーザ認証にて参照する連続誤認証許容回数を設定します。 ここで設定した回数以上の誤認証を連続して行った場合は、ファイル削除処理を行います。
ログオフ有効時間設定	ログオフ状態継続可能時間を設定します。 ここで設定した時間以上のログオフ状態を継続した場合は、ファイル削除処理を行います。
ソフトウェアキーボード連携設定	文字入力を必要とする場合に自動的にソフトウェアキーボードを表示します。
削除ファイル／フォルダ設定	ファイル削除条件が適用された場合に削除するファイル／フォルダを設定します。
親端末電話番号設定	リモートセキュリティにおける親端末の電話番号を設定します。ここで設定した端末からの SM でのみ、セキュリティ処理を行います。

1.5 リモートセキュリティについて

制御用親端末で作成したセキュリティスクリプトを暗号化し、SM として子端末に送信します。セキュリティスクリプトの内容により、複数の SM に分割して送信されることがあります。
SM を受け取った子端末は、受信した SM からセキュリティスクリプトを復元し実行します。
セキュリティスクリプトとは、端末上で実行可能な処理（以下セキュリティコマンド）を順に記載した処理定義であり、以下の情報を含んでいます。

セキュリティスクリプト SM に含まれている情報について以下に記します。

番号	項目	説明
①	有効期限	セキュリティスクリプトの有効期限
②	ユニーク ID	セキュリティスクリプトごとに付与するユニークな ID
③	連番／全数	セキュリティスクリプトが複数の SM に分割された場合の番号および全体数
④	処理内容	セキュリティコマンドを処理順に列挙 セキュリティコマンドの詳細については「4.3セキュリティスクリプト編集」を参照してください。

また、通信状態と本体の電源状態およびリモートセキュリティ動作の関係を以下に記します。

No	通信+本体	親端末		子端末	
		子端末へ セキュリティ送信	子端末から 結果受信	親端末へ 結果送信	親端末から セキュリティ受信
①	圏内+本体 ON	○	○	○	○
②	圏内+本体 OFF	－	○ （※WakeOnSMS）	○	○ （WakeOnSMS）
③	圏外+本体 ON	エラー	圏内復帰で①へ	圏内復帰で①へ	圏内復帰で①へ
④	圏外+本体 OFF	－	圏内復帰で②へ	－	圏内復帰で②へ

※ WakeOnSMS　SM を受信することで本体の電源が入ります。

2. ユーザ認証について

端末起動時にユーザ認証を行い、端末の不正利用／データ漏洩防止を行います。
ユーザ認証中は、端末ロック（電源ボタン、タッチパネル、キーボードの操作のみ有効）となります。
ユーザ認証方式には NFC 認証とパスワード認証の2つの方式があります。

2.1 NFC認証方式とは

本体液晶部に NFC カードをかざすことで認証を行います。

NFC認証画面（認証有効）

NFC認証画面（認証待機）

NFC 認証画面（認証有効）時にカードをかざすことで認証を行います。
10 秒間カードを読み取ることができなかった場合は、NFC 認証画面（認証待機）へ移行します。
NFC 認証画面（認証待機）時に画面をタッチすることで NFC 認証画面（認証有効）へ移行します。
また、画面下位にある「パスワード認証画面へ」を押下することでパスワード認証へ移行します。

2.2 パスワード認証方式とは

パスワードを入力することで認証を行います。

パスワード認証画面

パスワードを入力し、「OK」を押下します。
入力した内容を一括して削除する場合は「クリア」を押下してください。
画面下位にある「カード認証画面へ」を押下することで NFC 認証画面（認証有効）へ移行します。

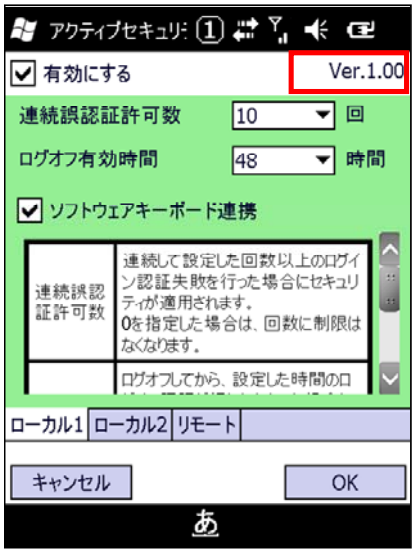
3. ローカルセキュリティを利用する

3.1 端末にインストールする

商品に含まれている以下のファイルを端末にコピーした後、端末上で実行してください。
ja_ActiveLocalSecurityWM.ARMV4I.CAB
※本ツールをアンインストールすることは出来ません。

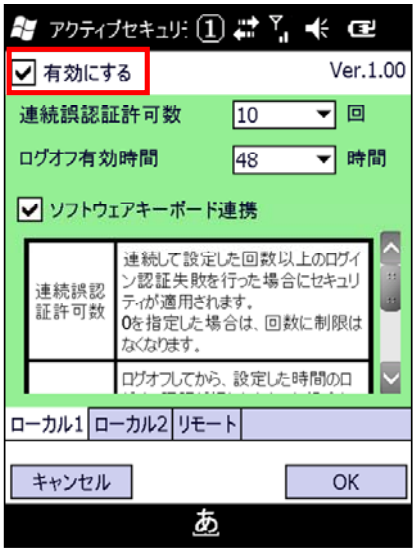
3.2 バージョン情報を確認する

ローカルセキュリティのバージョン情報を確認する場合は、「スタート」→「アクティブセキュリティ設定」を選択します。



3.3 アクティブセキュリティを有効にする

アクティブセキュリティの有効無効を変更する場合は、「スタート」→「アクティブセキュリティ設定」を選択します。

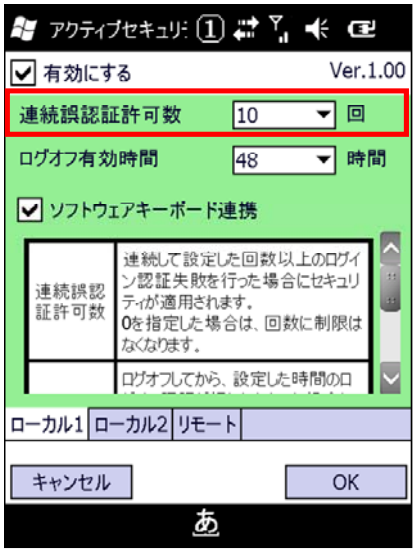


チェックあり：セキュリティ有効
チェックなし：セキュリティ無効

※ 「OK」ボタンを押下すると設定内容の保存および本体のリセットを行います。
※ セキュリティが有効で、かつ、アドミニストレータ権限のないユーザでユーザ認証を行った場合、設定内容を変更することは出来ません。

3.4 連続認証失敗の許容回数を設定する

「スタート」→「アクティブセキュリティ設定」を選択します。次に、アクティブセキュリティ設定画面の「ローカル1」タブを選択します。

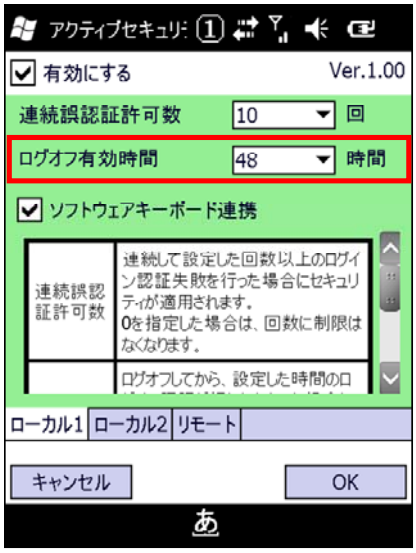


0～999の範囲で任意に設定可能です。しかし、数字以外の文字や範囲外を指定した場合は0となります。
0を指定した場合は、連続誤認証回数に制限がなくなります。

※ 「OK」ボタンを押下すると設定内容の保存および本体のリセットを行います。
※ アドミニストレータ権限のないユーザでユーザ認証を行った場合、設定内容を変更することは出来ません。

3.5 ログオフ有効時間を設定する。

「スタート」→「アクティブセキュリティ設定」を選択します。次に、アクティブセキュリティ設定画面の「ローカル1」タブを選択します。

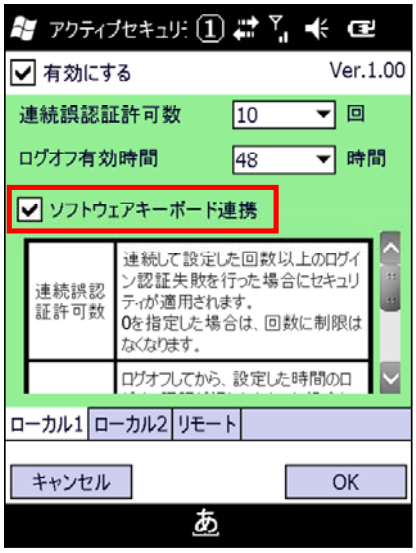


0～999の範囲で任意に設定可能です。しかし、数字以外の文字や範囲外を指定した場合は0となります。
0を指定した場合は、ログオフ有効時間に制限がなくなります。

※ 「OK」ボタンを押下すると設定内容の保存および本体のリセットを行います。
※ アドミニストレータ権限のないユーザでユーザ認証を行った場合、設定内容を変更することは出来ません。

3.6　ソフトウェアキーボードを自動的に表示する

「スタート」→「アクティブセキュリティ設定」を選択します。次に、アクティブセキュリティ設定画面の「ローカル1」タブを選択します。

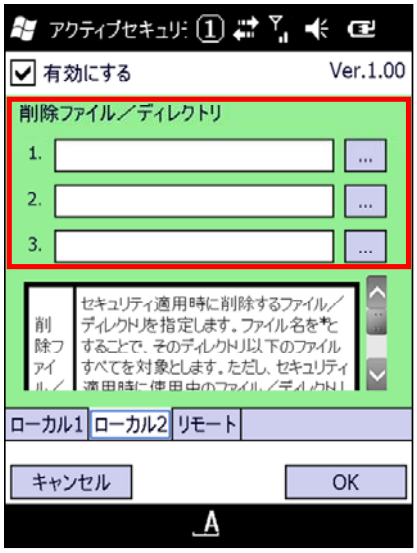


チェックあり：ソフトウェアキーボード制御する
チェックなし：ソフトウェアキーボード制御しない

※　「OK」ボタンを押下すると設定内容の保存および本体のリセットを行います。
※　アドミニストレータ権限のないユーザでユーザ認証を行った場合、設定内容を変更することは出来ません。

3.7　認証失敗時の削除ファイル／フォルダを設定する

「スタート」→「アクティブセキュリティ設定」を選択します。次に、アクティブセキュリティ設定画面の「ローカル2」タブを選択します。

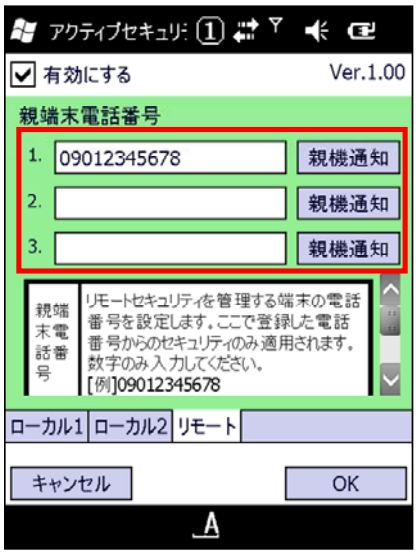


ファイル削除適用時に対象となるファイル／フォルダを
指定します。末尾にワイルドカード（＊）を使用することで
指定フォルダ下すべてのファイルを削除対象とします。

※　「OK」ボタンを押下すると設定内容の保存および本体のリセットを行います。
※　アドミニストレータ権限のないユーザでユーザ認証を行った場合、設定内容を変更することは出来ません。
※　使用中のファイルを削除することは出来ません。

3.8 親端末を設定する

リモートセキュリティにおいて、親端末の電話番号を最大 3 件まで登録できます。ここで設定した親端末からのセキュリティスクリプトのみ実行します。
「スタート」→「アクティブセキュリティ設定」を選択します。次に、アクティブセキュリティ設定画面の「リモート」タブを選択します。

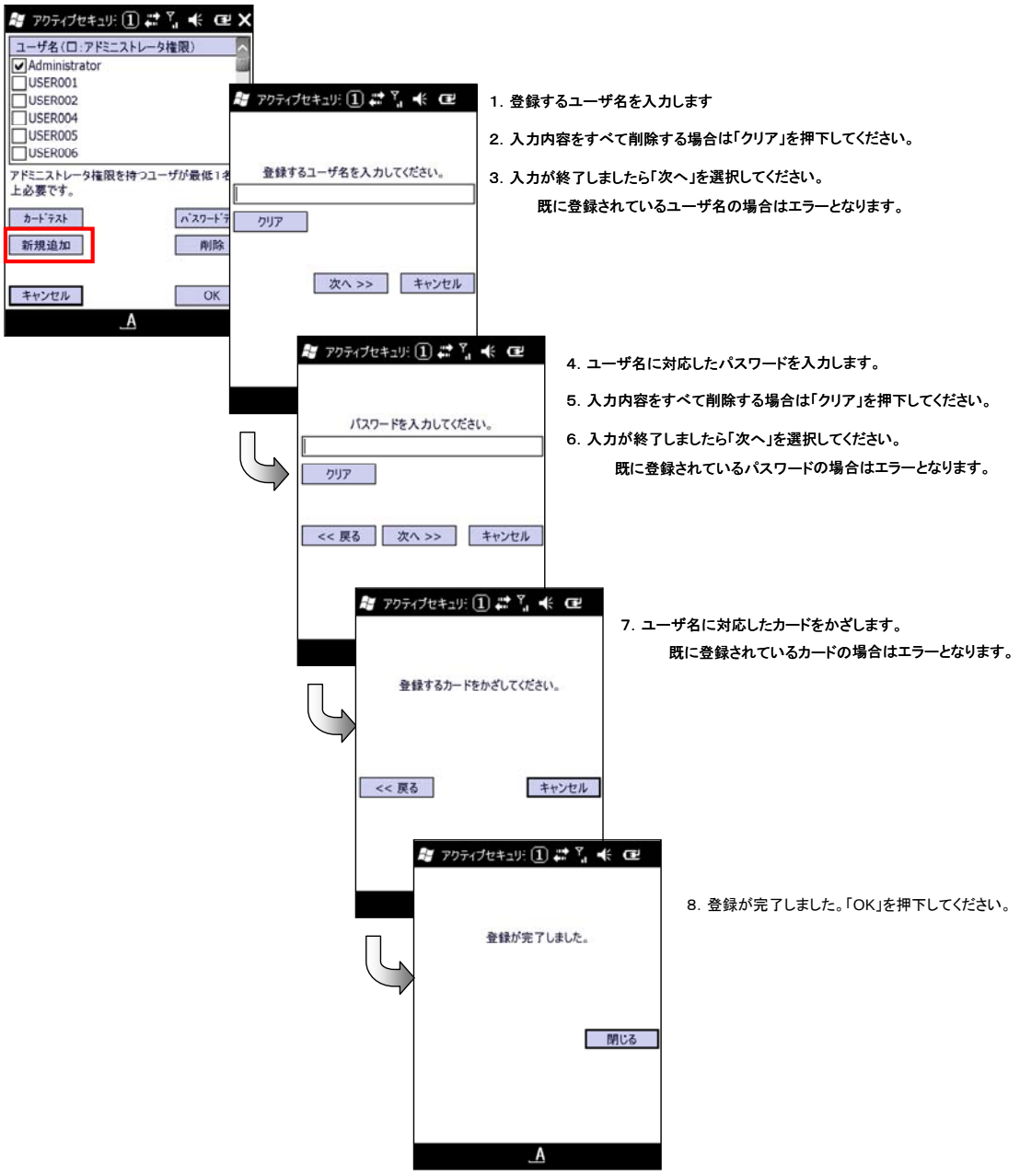


数字のみ入力可能です。
親機通知を押下することで、入力した電話番号に対して
登録用のSMを送信します。

※ 「OK」ボタンを押下すると設定内容の保存および本体のリセットを行います。
※ アドミニストレータ権限のないユーザでユーザ認証を行った場合、設定内容を変更することは出来ません。
※ SIM カードが未装着もしくは正常に認識できない場合、「リモート」タブは表示されません。

3.9 ユーザアカウントを追加する

標準認証で認証可能なユーザの追加を行います。
端末上で「スタート」→「アクティブセキュリティアカウント設定」を選択し、「新規追加」を押下してください。



1. 登録するユーザ名を入力します
2. 入力内容をすべて削除する場合は「クリア」を押下してください。
3. 入力が終了しましたら「次へ」を選択してください。
   既に登録されているユーザ名の場合はエラーとなります。
4. ユーザ名に対応したパスワードを入力します。
5. 入力内容をすべて削除する場合は「クリア」を押下してください。
6. 入力が終了しましたら「次へ」を選択してください。
   既に登録されているパスワードの場合はエラーとなります。
7. ユーザ名に対応したカードをかざします。
   既に登録されているカードの場合はエラーとなります。
8. 登録が完了しました。「OK」を押下してください。

※ アドミニストレータ権限のないユーザでユーザ認証を行った場合、本機能を利用することは出来ません。

3.10 ユーザアカウントを削除する

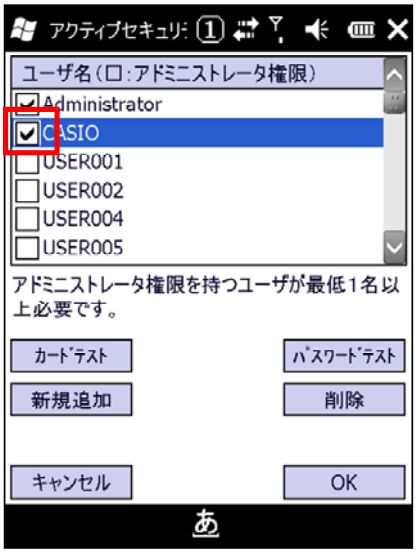
標準認証で認証可能なユーザの削除を行います。
端末上で「スタート」→「アクティブセキュリティアカウント設定」を選択してください。

1. 削除するアカウントのユーザ名を選択します。
2. 「削除」を押下します。
   削除対象が最後のアドミン権限保持ユーザの場合はエラーとなります。
3. 「はい」を押下してください。

※ アドミニストレータ権限のないユーザでユーザ認証を行った場合、本機能を利用することは出来ません。

3.11 ユーザアカウントにアドミニストレータ権限を設定する

アドミニストレータ権限とは、アカウントや設定に関する編集を可能とする権限であり、必ず1名以上のアドミニストレータ権限保持アカウントを必要とします。
端末上で「スタート」→「アクティブセキュリティアカウント設定」を選択してください。



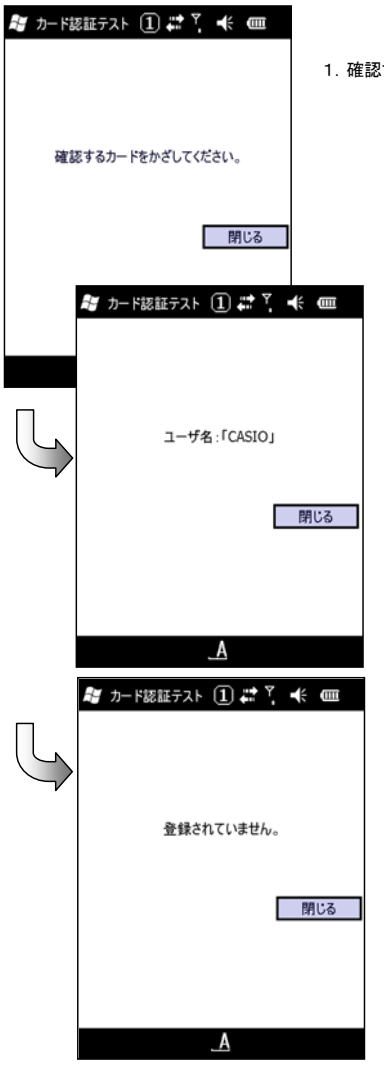
各ユーザ名左のチェックボックスでアドミニストレータ権限の有無を設定します。

※ アドミニストレータ権限のないユーザでユーザ認証を行った場合、本機能を利用することは出来ません。

3.12 カードの認証テストを行う

NFC カードを読み取り、登録済みアカウントか否かをテストします。登録済みの場合はそのユーザ名を表示します。

端末上で「スタート」→「アクティブセキュリティアカウント設定」を選択し、「カードテスト」を押下してください。



1. 確認するNFCカードをかざしてください。

2. かざしたカードはユーザ名「CASIO」で登録済みです。

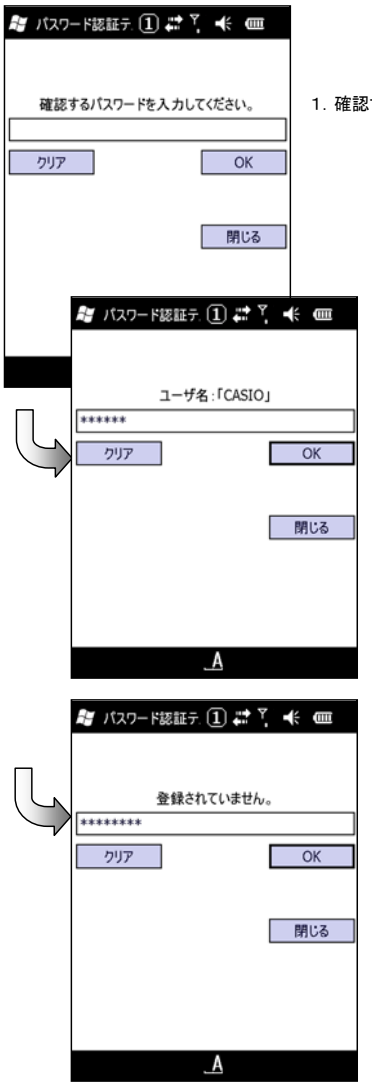
3. かざしたカードは未登録です。

※ アドミニストレータ権限のないユーザでユーザ認証を行った場合、本機能を利用することは出来ません。

3.13 パスワードの認証テストを行う

パスワードを入力し、登録済みアカウントか否かをテストします。登録済みの場合はそのユーザ名を表示します。

端末上で「スタート」→「アクティブセキュリティアカウント設定」を選択し、「パスワードテスト」を押下してください。



1. 確認するパスワードを入力してください。

2. 入力したパスワードはユーザ名「CASIO」で登録済みです。

3. 入力したパスワードは未登録です。

※ アドミニストレータ権限のないユーザでユーザ認証を行った場合、本機能を利用することは出来ません。

4. リモートセキュリティを利用する

4.1 端末にインストールする

商品に含まれている以下のファイルを端末にコピーした後、端末上で実行してください。
ja_ActiveRemoteSecurityWM.ARMV4I.CAB
※本ツールをアンインストールすることは出来ません。
※本ツールは親端末のみにインストールしてください。

4.2 リモートセキュリティメニューを表示する

端末上で「スタート」→「アクティブリモートセキュリティ」を選択してください。
本ツールでは以下の機能を提供します。

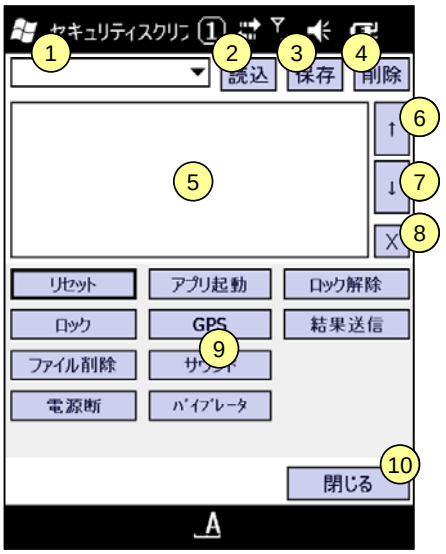
番号	機能	内容
①	セキュリティスクリプト編集	子端末で実行するセキュリティスクリプトを作成／編集します。
②	リモートセキュリティ実行	セキュリティ実行対象となる子端末上でセキュリティスクリプトを実行します。
③	リモートセキュリティ結果	実行したリモートセキュリティの内容や結果状況を表示します。

起動画面

※ アドミニストレータ権限のないユーザでユーザ認証を行った場合、本機能を利用することは出来ません。

4.3 セキュリティスクリプト編集

アクティブリモートセキュリティ画面で「セキュリティスクリプト編集」ボタンを押下してください。
子端末で実行するセキュリティスクリプトを作成／編集します。
以下に編集画面と各部位に関する説明を記します。



番号	機能	操作／内容
①	セキュリティスクリプトリスト	現在編集対象とするセキュリティスクリプト名を入力または選択します。
②	読込	セキュリティスクリプトリストで選択されているセキュリティスクリプトを読み込みます。現在編集中のセキュリティスクリプトが存在する場合は、確認ダイアログを表示します。
③	保存	現在編集中のセキュリティスクリプトをセキュリティスクリプトリストで選択されているセキュリティスクリプト名で保存します。
④	削除	セキュリティスクリプトリストで選択されているセキュリティスクリプトを削除します。
⑤	セキュリティスクリプト内容	実行順にセキュリティコマンドが並んだセキュリティスクリプトを表示します。 プロパティ設定が可能なセキュリティコマンドをダブルクリックすることで、プロパティ設定画面に移行します。
⑥	↑	セキュリティスクリプト内容で選択状態にあるセキュリティコマンドを1つ上に移動します。
⑦	↓	セキュリティスクリプト内容で選択状態にあるセキュリティコマンドを1つ下に移動します。
⑧	X	セキュリティスクリプト内容で選択状態にあるセキュリティコマンドを削除します。
⑨	セキュリティコマンドボタン （リセット、ロック、etc）	選択したセキュリティコマンドをセキュリティスクリプト最下行に追加します。 セキュリティスクリプトには最大 10 個のセキュリティコマンドを登録することが可能です。また実行回数に制限があるセキュリティコマンドは、その制限以上の登録はできません。 各セキュリティコマンドについての詳細は次表を参照してください。
⑩	閉じる	セキュリティスクリプト編集画面を閉じます。 現在編集中のスクリプトが未保存の場合は、確認ダイアログを表示します。

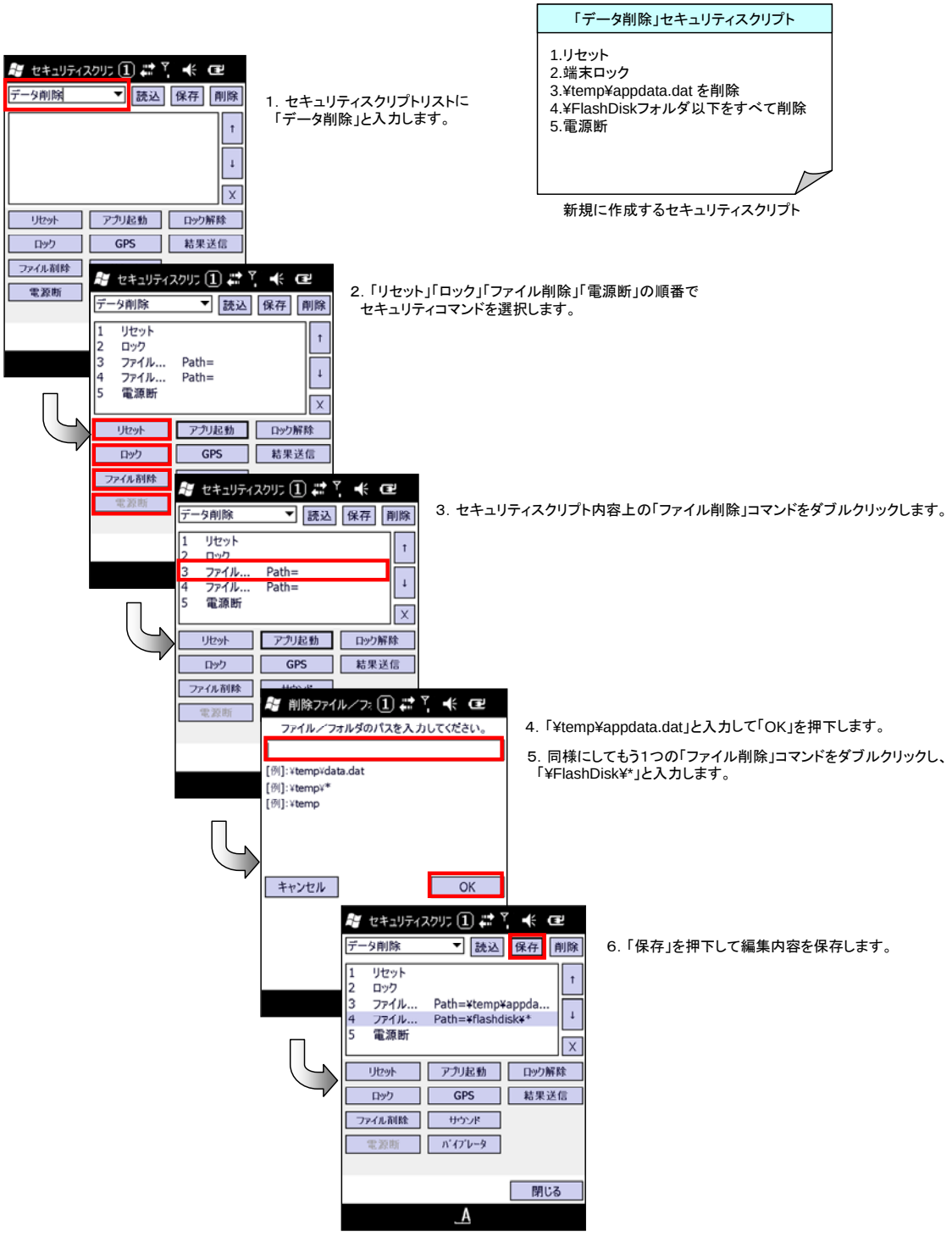
【セキュリティコマンド一覧】

セキュリティスクリプトで使用可能なセキュリティコマンドの一覧を下に記します。

番号	コマンド	プロパティ値	内容
①	リセット	(なし)	端末の状態に関わらずリセットを行います。 リセットから復帰後、続きのセキュリティコマンドを実行します。
②	ロック	(なし)	端末をロック状態にし、外部からのアクセスを禁止します。 端末が認証待ち状態の場合はリセットを行い、起動時にロック状態となります。 セキュリティコマンドでロック状態にした端末は、セキュリティコマンドでのロック解除でのみロックを解除することが出来ます。
③	ファイル削除	削除ファイル フォルダパス	指定したファイル／フォルダの削除を試みます。読み取り専用属性の場合は、属性を解除して削除を試みます。 使用中のファイル／フォルダを削除することは出来ません。よって、リセット直後に実行することをお勧めします。
④	電源断	(なし)	電源を落とします。 電源 ON 後、続きのセキュリティコマンドを実行します。 ※ セキュリティスクリプト内で1つだけ設定可能です。
⑤	アプリ起動	実行ファイルパス 引数オプション	指定したファイルを実行します。 あらかじめ、起動するアプリケーションを子端末上に配置しておく必要があります。 ※ 実行したプロセスの終了は監視しません。 ※ 起動の成否判定はしません。
⑥	GPS	タイムアウト値(秒)	GPS 測位を試みます。 指定したタイムアウト時間内に測位できなかった場合は、過去最近の位置情報を取得します。 ※ セキュリティスクリプト内で1つだけ設定可能です。
⑦	サウンド	サウンドファイルパス	指定したサウンドファイルを再生します。 あらかじめ、再生するファイルを子端末上に配置しておく必要があります。 ※ 再生の成否判定はしません。
⑧	バイブレータ	振動時間(秒)	指定した時間、振動します。 ※ 振動の成否判定はしません。
⑨	ロック解除	(なし)	端末のロックを解除します。 ※ セキュリティスクリプト内で1つだけ設定可能です。
⑩	結果送信	(なし)	セキュリティスクリプトの実行結果を親端末に送信します。 ※ セキュリティスクリプト内で1つだけ設定可能です。

4.3.1　セキュリティスクリプトを新規に作成する

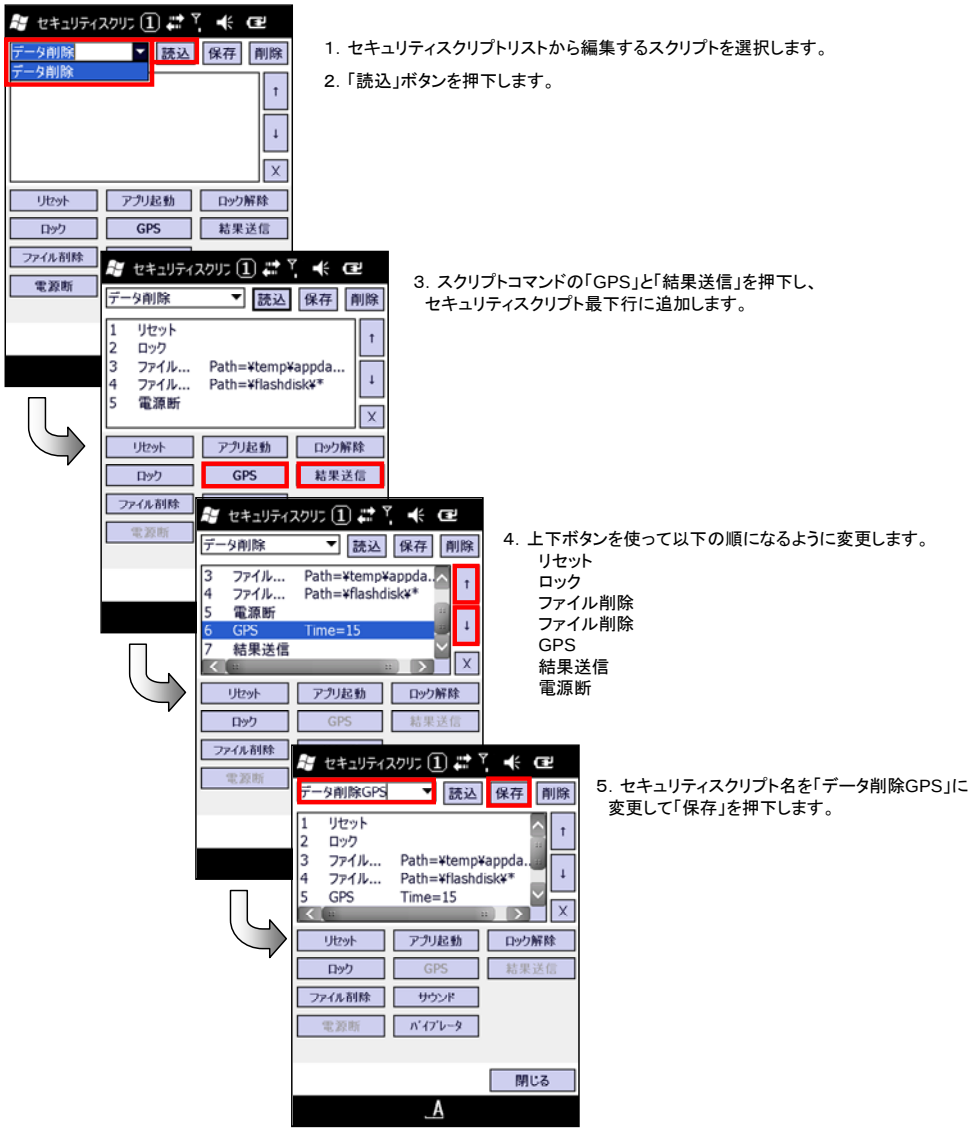
ここでは例として以下の動作を行うセキュリティスクリプトを新規に作成します。



※　セキュリティコマンドに関する詳細は「4.3セキュリティスクリプト編集」を参照してください。

4.3.2　セキュリティスクリプトをカスタマイズする

ここでは例として、「4.3.1 セキュリティスクリプトを新規に作成する」で作成したセキュリティスクリプトに「GPS」「結果送信」コマンドを追加し、別名で保存します。



※　セキュリティコマンドに関する詳細は「4.3セキュリティスクリプト編集」を参照してください

※　サンプルとして以下のセキュリティスクリプトを用意しています。目的に合わせてカスタマイズし、別名で保存後使用してください。サンプルのセキュリティスクリプトを削除／編集することはできません。

サンプル名称	登録内容
[e.g.]DeleteFile	ロック→リセット→ファイル削除(¥temp¥*)→ サウンド(¥Program Files¥CASIO¥ActiveSecurity¥WAV¥type04.wav)→結果送信→電源断
[e.g.]GPSSerach	GPS(60 秒)→結果送信
[e.g.]UnLock	ロック解除→結果送信

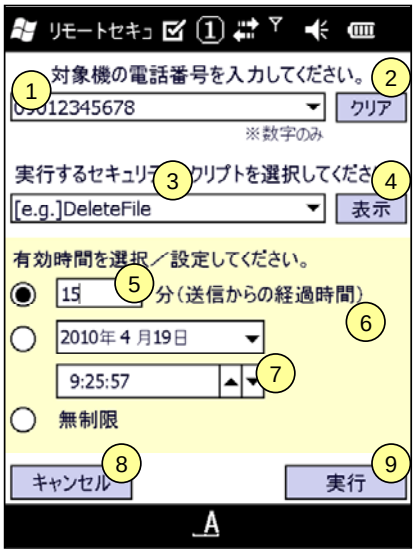
4.3.3　セキュリティスクリプトを削除する

ここでは例として、「4.3.1 セキュリティスクリプトを新規に作成する」で作成したセキュリティスクリプトを削除します。セキュリティスクリプトを削除しても、すでに実行したセキュリティスクリプトの実行結果表示が損なわれることはありません。

1. セキュリティスクリプトリストから「データ削除」を選択します。
2. 「削除」を押下します。
3. 削除確認ダイアログの「はい」を選択します。

4.4　リモートセキュリティ実行

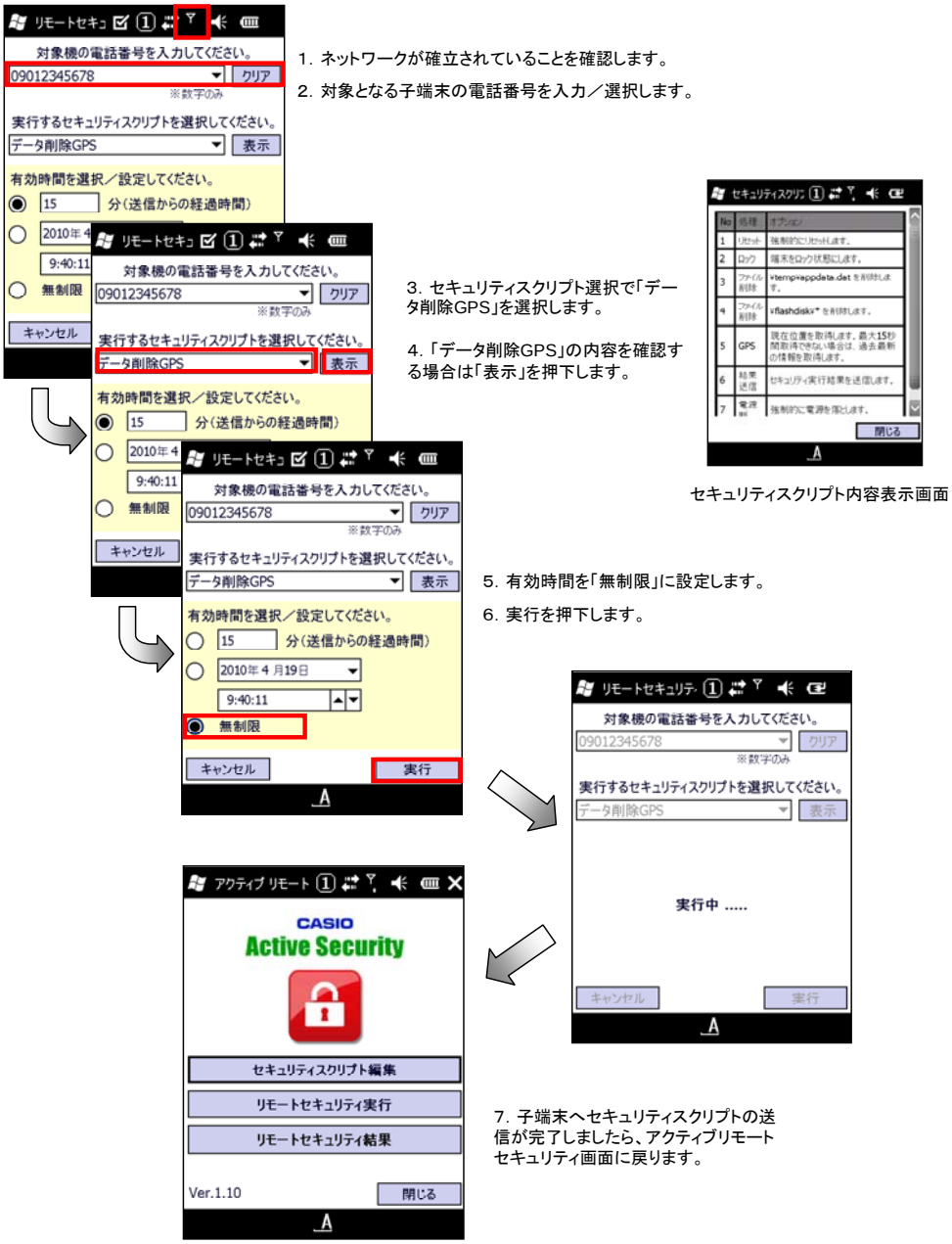
アクティブリモートセキュリティ画面で「リモートセキュリティ実行」ボタンを押下してください。
子端末でセキュリティスクリプトを実行します。
以下に実行画面と各部位に関する説明を記します。



番号	機能	操作／内容
①	子端末電話番号リスト	セキュリティスクリプトを実行する対象となる子端末の電話番号を入力/選択します。子端末側で親機登録時に本機を指定した場合、本リストに追加します。
②	クリア	子端末電話番号を削除します。
③	セキュリティスクリプト選択	子端末電話番号リストで入力/選択された子端末上で動作させるセキュリティスクリプトを選択します。
④	表示	セキュリティスクリプト選択で選択状態にあるセキュリティスクリプトの内容を表示します。
⑤	無制限	送信した時刻と子端末上で受け取った時刻との差に制限はありません。
⑥	経過時間制限	送信した時刻と子端末上で受け取った時刻との差が指定された時間以上は慣れていた場合は、セキュリティスクリプトを実行しません。
⑦	日付日時制限	子端末上で受け取った日時が指定された日時を経過していた場合は、セキュリティスクリプトを実行しません。
⑧	キャンセル	アクティブリモートセキュリティ画面に戻ります。
⑨	実行	指定内容にしたがって子端末にセキュリティスクリプトを送信します。 通信を確立できていない場合はエラーとなります。安定した通信環境下で実行してください。

4.4.1　リモートセキュリティを実行する

ここでは例として、「4.3.2 セキュリティスクリプトをカスタマイズする」で作成したセキュリティスクリプトを子端末（電話番号：09012345678）上で実行します。



1. ネットワークが確立されていることを確認します。
2. 対象となる子端末の電話番号を入力／選択します。
3. セキュリティスクリプト選択で「データ削除GPS」を選択します。
4. 「データ削除GPS」の内容を確認する場合は「表示」を押下します。

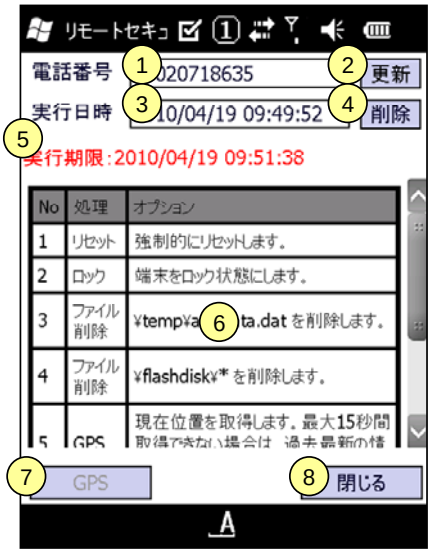
セキュリティスクリプト内容表示画面

5. 有効時間を「無制限」に設定します。
6. 実行を押下します。
7. 子端末へセキュリティスクリプトの送信が完了しましたら、アクティブリモートセキュリティ画面に戻ります。

※　既に子端末側でセキュリティスクリプトを実行している場合、送信したスクリプトは子端末上にスタックされ、順次実行します。ただし、スタックされたスクリプトは順不同で実行されます。

4.5　リモートセキュリティ結果

アクティブリモートセキュリティ画面で「リモートセキュリティ結果」ボタンを押下してください。
子端末で実行した結果を表示します。セキュリティスクリプトで「結果送信」コマンドを挿入していない場合や、ネットワークの影響で応答結果が得られなかった場合などは、実行したスクリプトの内容を表示します。
以下に結果画面と各部位に関する説明を記します。



結果応答がなかった場合

結果応答があった場合

番号	機能	操作／内容
①	電話番号	過去にセキュリティスクリプトを実行した子端末の電話番号の中から閲覧したい電話番号を選択します。
②	更新	電話番号で選択された子端末に関する結果情報を再読み込みし、更新します。
③	実行日時	過去に電話番号で選択された子端末上でセキュリティスクリプトを実行した日時の中から閲覧したい日時を選択します。
④	削除	電話番号で選択された子端末に関する応答結果情報を削除します。
⑤	結果状況	実行日時制限あり＋指定時刻に達していない場合：実行日時制限時刻を青文字で表示します。 実行日時制限あり＋指定時刻になっても子端末から実行結果が得られていない場合：実行日時制限時刻を赤文字で表示します。 実行日時制限なし＋子端末から実行結果が得られていない場合：青文字で無制限と表示します。 子端末から実行結果が得られている場合：青文字で「実行結果を表示します」と表示します。
⑥	セキュリティスクリプト内容	子端末から実行結果が得られている場合と得られていない場合で画面が異なります。上図を参照してください。
⑦	GPS	結果応答の中に GPS 測位情報が含まれていた場合に押下可能になります。 押下した場合は、その位置を表示します。
⑧	閉じる	アクティブリモートセキュリティ画面に戻ります。

4.5.1　リモートセキュリティ実行結果を確認する（GPS情報あり）

ここでは例として、「4.3.2 セキュリティスクリプトをカスタマイズする」で作成したセキュリティスクリプトを子端末上で実行させ、その実行結果を確認します。

1. 子端末から結果応答があった場合、アクティブリモートセキュリティ画面の「リモートセキュリティ結果」ボタンが点滅します。

2. 「リモートセキュリティ結果」を選択します。

3. 自動的に最も新しいセキュリティ実行結果を表示します。

4. 「GPS」を押下します。

4. 過去最近に測位した時刻とそのときの位置をGoogleマップ上に表示します。

※　GPS 測位時刻は、対象子端末のシステム時刻を元にしています。

5. アクティブローカルセキュリティ支援について

5.1 定義暗号化ツール

アクティブセキュリティで参照する定義ファイルを暗号化します。本ツールは PC 用アプリケーションです。
NFC データ参照定義ファイル（TXT 形式）を NFC データ参照定義ファイル（DAT 形式）に変換する場合に用います。

NFCデータ参照定義ファイル（TXT形式）:「7.2.1 NFCデータ参照定義ファイル（TXT形式）」参照
NFCデータ参照定義ファイル（DAT形式）:「7.2.2 NFCデータ参照定義ファイル（DAT形式）」参照

コマンドファイルプロパティ:

項目	内容
ファイル名	CASConfigPackager.exe
ファイルパス	商品に同梱されている同名ファイルを、実行する PC 上の任意の場所にコピーしてください。
ファイル形式	MS-DOS コマンド実行形式

5.1.1 コマンドライン書式

以下にコマンドラインでの書式について記載します。

CASConfigPackager.exe [/h] /i "Input config file" /o "Output config file"

オプション	内容
/h	コマンドライン詳細を表示します
/i	暗号化元ファイルパス指定宣言です。
"Input config file"	暗号化元ファイルパスです。
/o	暗号化出力ファイルパス指定宣言です。
"Output config file"	暗号化出力ファイルパスです。

※暗号化出力ファイルパスに既にファイルが存在していた場合は上書きします。

5.1.2 戻り値

終了コードとエラーメッセージ一覧を以下に記します。

終了状態	終了コード	メッセージ
正常終了	0	なし
異常終了	1	Parameter Error.
		Cannot find input file.
		Output file is read only.
		Cannot Open input file.
		Input file format error.

5.2 アカウント情報テーブル作成ツール

CSV フォーマットで記述されたアカウント情報テーブルファイルを、アクティブセキュリティ標準認証で直接参照可能なデータファイルに変換します。本ツールは PC 用アプリケーションです。

アカウント情報テーブルファイル:

項目	内容
ファイル名	ActSecAccount.dat
場所	¥Program Files¥CASIO¥ActiveSecurity

コマンドファイルプロパティ:

項目	内容
ファイル名	CASAccountConvertor.exe
ファイルパス	商品に同梱されている同名ファイルを、実行する PC 上の任意の場所にコピーしてください。
ファイル形式	MS-DOS コマンド実行形式

5.2.1 コマンドライン書式

以下にコマンドラインでの書式について記載します。

CASAccountConvertor.exe [/h] /i "Input account CSV file" /o "Output account file"

オプション	内容
/h	コマンドライン詳細を表示します。
/i	変換元 CSV 形式アカウント情報テーブルファイルパス指定宣言です。
"Input account CSV file"	変換元 CSV 形式アカウント情報テーブルファイルパスです。 本ファイルのフォーマットについては「5.2.3 CSV形式アカウント情報テーブルファイルフォーマット」を参照してください。
/o	アカウント情報テーブルファイル出力パス指定宣言です。
"Output account file"	アカウント情報テーブルファイル出力パスです。

※アカウント情報ファイル出力パスに既にファイルが存在していた場合は上書きします。

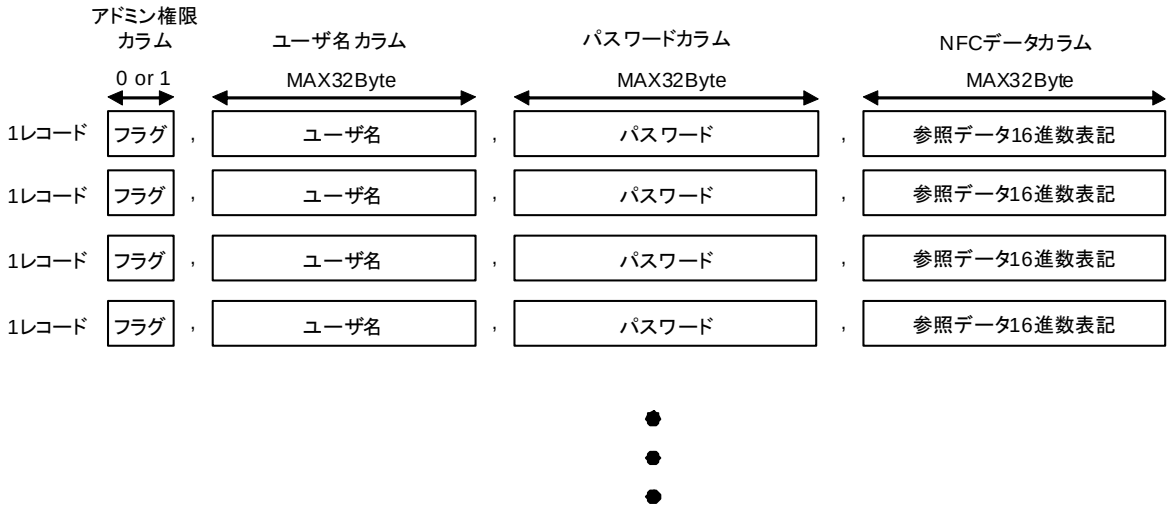
5.2.2 戻り値

終了コードとエラーメッセージ一覧を以下に記します。

終了状態	終了コード	メッセージ
正常終了	0	なし
異常終了	1	Parameter Error.
		Cannot find input file.
		Output file is read only.
		Cannot Open input file.
		Input file format error.

5.2.3　CSV形式アカウント情報テーブルファイルフォーマット

変換元となる CSV 形式（カンマ区切り）でのアカウント情報テーブルファイルフォーマットについて記します。



例：

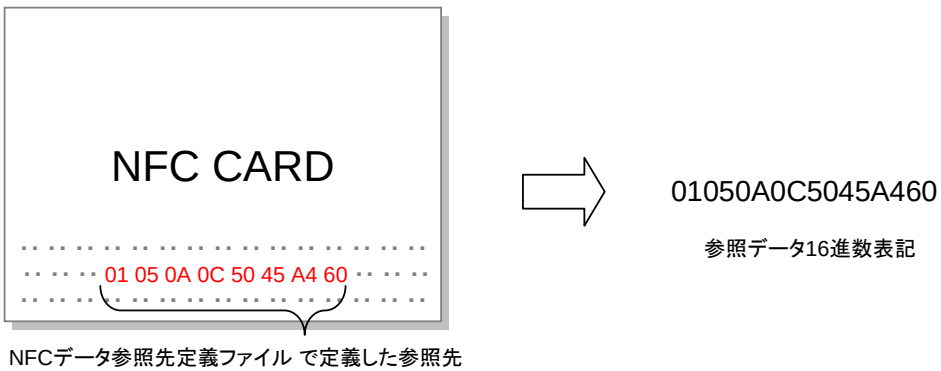
1,CASIO_A,11111,0A0B0C0　　*説明：アドミニストレータ権限有、パスワード「11111」、NFC データ「0A0B0C0」*

0,CASIO_B,11112,0B0C0D0　　*説明：アドミニストレータ権限無、パスワード「11112」、NFC データ「0B0C0D0」*

0,CASIO_C,11113,0C0D0E0　　*説明：アドミニストレータ権限無、パスワード「11113」、NFC データ「0C0D0E0」*

NFC データカラムについて

NFC データカラムに記載する参照データ 16 進数表記とは、「NFC データ参照定義ファイル」にて定義した場所に記載されているデータを 16 進数で表記した文字列となります。



6. 端末操作ログ

本システムでは端末で操作した内容を端末ログに出力しています。ログの種類と内容を以下に記します。
端末ログを閲覧するには「スタート」→「端末ログビューア」を起動してください。

6.1 ログ種類

6.1.1 ユーザ認証ログ

【実行ソース】 ActiveSecurity
【処理名】 Login

番号	種別	属性	メッセージ	説明
1	情報	情報	Load Standard Recognize DLL.	標準認証 DLL 読み込み
2	情報	情報	Load Extend Recognize DLL.	外部認証 DLL 読み込み
3	異常	エラー	DLL Load Error.（Error no）	認証 DLL 読み込み失敗
4	異常	エラー	Cannot find func Address in DLL. (Error no)	認証 DLL 公開関数未実装
5	経過	情報	Execute TODO Script.	残処理スクリプト実行
6	情報	情報	Unlock Machine.	端末操作ロック解除
7	情報	情報	Lock Machine. (Lock Mode)	端末操作ロック開始
8	情報	情報	System Resumed -> Call Main Recognize.	サスペンド検知＞メイン認証起動
9	開始	情報	Call Main Recognize.	メイン認証開始
10	終了	成功	Successes to login on Main Recognize.	メイン認証成功
11	終了	失敗	Login Missed in Main Recognize and leached MAX Count. Execute Local Security Script.	メイン認証失敗 許容回数オーバーによるセキュリティ発動
12	終了	失敗	Login Missed in Main Recognize.	メイン認証失敗
13	終了	エラー	Device Initialize Error in Main Recognized.	メイン認証でデバイス初期化エラー発生
14	終了	情報	Power Off in Main Recognized.	メイン認証から電源断要求
15	開始	情報	Call Sub Recognize.	サブ認証開始
16	終了	成功	Successes to login on Sub Recognize.	サブ認証成功
17	終了	失敗	Login Missed in Sub Recognize and leached MAX Count. Execute Local Security Script.	サブ認証失敗 許容回数オーバーによるセキュリティ発動。
18	終了	失敗	Login Missed in Sub Recognize.	サブ認証失敗
19	終了	エラー	Device Initialize Error in Sub Recognized.	サブ認証でデバイス初期化エラー発生
20	終了	情報	Power Off in Sub Recognized.	サブ認証から電源断要求
21	終了	失敗	Logoff period. Execute Local Security Script.	ログオフ有効時間超過のため、セキュリティ発動

6.1.2　設定変更ログ

【実行ソース】 ActiveSecurity
【処理名】 Setting

番号	種別	属性	メッセージ	説明
1	開始	情報	Start ActiveSecurity Setting.	本ツール起動開始
2	終了	情報	End ActiveSecurity Setting.	本ツール終了
3	情報	情報	Saved ActiveSecurity Setting. Times= [誤認証許容回数] Logoff=[ログオフ有効時間] Security=Enable / Disable DeleteFolder = [設定パス] DeleteFolder = [設定パス] DeleteFolder = [設定パス] ParentPhone = [親端末電話番号] ParentPhone = [親端末電話番号] ParentPhone = [親端末電話番号]	設定内容保存

6.1.3　アカウント操作ログ

【実行ソース】 ActiveSecurity
【処理名】 Account

番号	種別	属性	メッセージ	説明
1	開始	情報	Start ActiveSecurity Account Editor.	本ツール起動開始
2	情報	情報	Add new Account [USER NAME].	[USER NAME]を新規に追加
3	情報	情報	Delete [USER NAME].	[USER NAME]を削除
4	情報	情報	[USER NAME] is deprived the Administrator Authority.	[USER NAME]からアドミニストレータ権限を剥奪
5	情報	情報	[USER NAME] is given the Administrator Authority.	[USER NAME]にアドミニストレータ権限を授与
6	終了	情報	End ActiveSecurity Account Editor without save.	変更内容を保存せずに終了
7	終了	情報	End ActiveSecurity Account Editor.	変更内容を保存して終了

7. 運用にあわせたカスタマイズをする

7.1 ユーザ認証のカスタマイズについて

NFC認証では、MIFARE Standard／MIFARE Ultralight／FELICAのカード種からユーザの目的にあわせた選択が可能です。また、認証で参照する部分をそれぞれのカード種ごとに設定することが可能です。設定方法については「7.2NFCのデータ参照先を変更」を参照してください。

また、別途認証用アドインモジュールを用意していただくことで、デフォルトで用意している NFC 認証／パスワード認証の代わりに、運用にあわせた認証方式に変更することが可能です。
外部認証アドインは、下記ファイルを配置した後にリセットすることで有効となります。

外部認証アドインを実装する場合は以下のファイル仕様に従ってください。

項目	内容
ファイル名	CASRecogEx.dll
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥dll¥
ファイル形式	ダイアミックリンクライブラリ （アンマネージド DLL）

また、実装する認証内容については以下の仕様を満たしている必要があります。

項目	内容
画面構成	認証を促す画面およびユーザ通知画面は常に最前面の属性を持つこと。 現在の状況を正しくユーザに伝えること。 入力フォーカスが外れた場合は、速やかに自身の適切な場所に戻すこと。
認証方式	メイン認証方式とサブ認証方式を用意すること。 必要に応じてメイン認証の結果からサブ認証を呼び出す流れを構築すること。
処理	公開関数は、その戻り値が確定するまで処理を終了してはならない。 セキュリティ低下を招く処理を行ってはならない。

さらに、認証時には以下の公開関数を呼び出します。これは、外部認証アドインで実装する必要があります。

7.1.1　メイン認証呼び出し用関数

リセット後、最初に呼び出されます。本関数内で認証用画面出力および認証判定を行ってください。

```
[C++]
int CASMainRecognize()
```

解説

認証を開始する。認証が完了するまで、本関数を終了しないでください。
また、定期的に下記レジストリ値を参照し、0 以外の値の場合は終了コード:0x0030 で速やかに終了してください。

レジストリ場所:[HKLM]¥SOFTWARE¥CASIO¥ActiveSecurity

キー	型	説明
LASSStatus	DWORD	システムで使用

表示するダイアログには WS_EX_ABOVESTARTUP 属性が必要です。

戻り値

以下の認証結果を返します。呼び出し元である端末制御 HT アプリケーションは、この終了コードによって青字で示した処理を行います。

0x0000　：認証完了
　　：端末ロック状態を解除し、デスクトップ表示を行います。
0x0001　：メイン認証呼び出し依頼
　　：CASMainRecognize を呼び出します。
0x0002　：サブ認証方式呼び出し依頼
　　：CASSubRecognize を呼び出します。
0x0003　：認証失敗:メイン認証呼び出し依頼
　　：回数カウントアップ、最大許容回数判定実行します。
0x0004　：認証失敗:サブ認証方式呼び出し依頼
　　：回数カウントアップ、最大許容回数判定実行します。
0x0010　：デバイス初期化エラー
　　：電源断を行います。
0x0020　：電源断依頼
　　：電源断を行います。
0x0030　：システム処理移行
　　：以後の処理をシステムに移します。

7.1.2　サブ認証呼び出し用関数

メイン認証の戻り値によって呼び出されます。本関数内で認証用画面出力および認証判定を行ってください。

```
[C++]
int CASSubRecognize()
```

解説

認証を開始する。認証が完了するまで、本関数を終了しないでください。
また、定期的に下記レジストリ値を参照し、0 以外の値の場合は終了コード:0x0030 で速やかに終了してください。

レジストリ場所:[HKLM]¥SOFTWARE¥CASIO¥ActiveSecurity

キー	型	説明
LASSStatus	DWORD	システムで使用

表示するダイアログには WS_EX_ABOVESTARTUP 属性が必要です。

戻り値

以下の認証結果を返します。呼び出し元である端末制御 HT アプリケーションは、この終了コードによって青字で示した処理を行います。

0x0000　：認証完了
　　：端末ロック状態を解除し、デスクトップ表示を行います。
0x0001　：メイン認証呼び出し依頼
　　：CASMainRecognize を呼び出します。
0x0002　：サブ認証方式呼び出し依頼
　　：CASSubRecognize を呼び出します。
0x0003　：認証失敗:メイン認証呼び出し依頼
　　：回数カウントアップ、最大許容回数判定実行します。
0x0004　：認証失敗:サブ認証方式呼び出し依頼
　　：回数カウントアップ、最大許容回数判定実行します。
0x0010　：デバイス初期化エラー
　　：電源断を行います。
0x0020　：電源断依頼
　　：電源断を行います。
0x0030　：システム処理移行
　　：以後の処理をシステムに移します。

7.2 NFCのデータ参照先を変更する

NFC カードの参照先は「NFC データ参照定義ファイル」により定義されています。
本ファイルを運用環境／使用カード種にあわせて定義していただくことで、データ参照先を変更することが可能です。

本定義ファイルには2種類のフォーマットがあります。
1つは一般的な INI 形式のテキストファイルで指定する「NFC データ参照定義ファイル（TXT 形式）」、もう1つは、それを暗号化した「NFC データ参照定義ファイル（DAT 形式）」です。
それぞれのファイルがともに存在している場合は「NFC データ参照定義ファイル（TXT 形式）」を優先します。

7.2.1 NFCデータ参照定義ファイル（TXT形式）

NFC の認証データ参照部分を INI 形式で定義します。

ファイルプロパティ:

項目	内容
ファイル名	NFCConfig.ini
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥
ファイル形式	テキスト形式

ファイルフォーマット:

セクション名	キー名	説明
MIFARE_ST		MIFARE Standard 用設定です。
	KEYTYPE	参照ブロックのキータイプです。 A,B から選択します。
	KEYBLOCK	参照ブロックの認証キーブロック番号です。
	KEY	参照ブロックを閲覧するためのキーです。 16 進形式 6 桁で指定します。
	READBLOCK	参照ブロック番号です。
	STARTBYTE	参照ブロック先頭からの読み込み開始位置です。
	READCOUNT	STARTBYTE から読み込むバイト数です。 ブロックをまたがった参照はできません。
MIFARE_UL		MIFARE Ultralight 用設定です。
	READPAGE	参照ページ番号です。
	STARTBYTE	参照ページ先頭からの読み込み開始位置です。
	READCOUNT	STARTBYTE から読み込むバイト数です。 ページをまたがった参照はできません。
FELICA		FELICA 用設定です。
	SERVICECODE	読み込み対象のサービスコードです。
	BLOCKNUMBER	読み込み対象のブロック番号です。
	STARTBYTE	ブロック番号先頭からの読み込み開始位置です。
	READCOUNT	STARTBYTE から読み込むバイト数です。 ブロックをまたがった参照はできません。

※読み込み対象となるカード種のみ記載してください。

【記載例】

```
[MIFARE_ST]
KEYTYPE=A
KEYBLOCK=11
KEY=FFFFFFFFFFFF
READBLOCK=8
STARTBYTE=2
READCOUNT=10

[MIFARE_UL]
READPAGE=8
STARTBYTE=2
READCOUNT=10

[FELICA]
SERVICECODE=1009
BLOCKNUMBER=0
STARTBYTE=0
READCOUNT=16
```

※コメントアウト文字はありません。

7.2.2 NFCデータ参照定義ファイル(DAT形式)

定義暗号化ツール※を利用して「NFC データ参照定義ファイル(TXT 形式)」を変換します。

ファイルプロパティ:

項目	内容
ファイル名	NFCConfigCrypto.dat
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥
ファイル形式	バイナリ形式

※定義暗号化ツールについての詳細は「5.1定義暗号化」を参照してください。

7.3 背景を変更する

アクティブローカルセキュリティでは以下のファイルを背景用画像として表示しています。
これらのファイルを変更することで、運用にあわせた背景デザインの変更が可能です。

標準認証／外部認証共通 基底背景画面　NFC認証（認証有効）背景画面　NFC認証（認証待機）背景画面　パスワード認証背景画面

【標準認証／外部認証共通　基底背景画面　：　縦画面用】

項目	内容
ファイル名	LOCK_VBKGROUND.bmp
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥Images¥JA¥
ファイル形式	BMP 形式
サイズ	240x320（VGA 時 480x640 に自動伸張表示します）
色数	MAX 16bit

【標準認証／外部認証共通　基底背景画面　：　横画面用】

項目	内容
ファイル名	LOCK_HBKGROUND.bmp
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥Images¥JA¥
ファイル形式	BMP 形式
サイズ	320x240（VGA 時 640x480 に自動伸張表示します）
色数	MAX 16bit

【標準認証　NFC 認証（認証有効）背景画面　：　縦画面用】

項目	内容
ファイル名	NFC_VBKGROUND.bmp
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥Images¥JA¥
ファイル形式	BMP 形式
サイズ	240x320（VGA 時 480x640 に自動伸張表示します）
色数	MAX 16bit

【標準認証 NFC 認証(認証有効)背景画面 ： 横画面用】

項目	内容
ファイル名	NFC_HBKGROUND.bmp
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥Images¥JA¥
ファイル形式	BMP 形式
サイズ	320x240（VGA 時 640x480 に自動伸張表示します）
色数	MAX 16bit

【標準認証 NFC 認証(認証待機)背景画面 ： 縦画面用】

項目	内容
ファイル名	NFC_VBKGROUND_T.bmp
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥Images¥JA¥
ファイル形式	BMP 形式
サイズ	240x320（VGA 時 480x640 に自動伸張表示します）
色数	MAX 16bit

【標準認証 NFC 認証(認証待機)背景画面 ： 横画面用】

項目	内容
ファイル名	NFC_HBKGROUND_T.bmp
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥Images¥JA¥
ファイル形式	BMP 形式
サイズ	320x240（VGA 時 640x480 に自動伸張表示します）
色数	MAX 16bit

【標準認証 パスワード認証背景画面 ： 縦画面用】

項目	内容
ファイル名	PASSWD_VBKGROUND.bmp
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥Images¥JA¥
ファイル形式	BMP 形式
サイズ	240x320（VGA 時 480x640 に自動伸張表示します）
色数	MAX 16bit

【標準認証 パスワード認証背景画面 ： 横画面用】

項目	内容
ファイル名	PASSWD_HBKGROUND.bmp
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥Images¥JA¥
ファイル形式	BMP 形式
サイズ	320x240（VGA 時 640x480 に自動伸張表示します）
色数	MAX 16bit

7.4 認証時の効果音を変更する

標準認証では、認証が正常に行われた場合、タイムアウトが発生した場合、エラーが発生した場合に以下の効果音を再生しています。任意のサウンドファイルに置き換えることで効果音を変更することが可能です。効果音を鳴らさない場合は、以下のファイルをリネームするか削除してください。

【認証正常】

項目	内容
ファイル名	Type00.wav
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥wav
ファイル形式	端末で再生可能な WAV 形式

【認証タイムアウト】

項目	内容
ファイル名	Type01.wav
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥wav
ファイル形式	端末で再生可能な WAV 形式

【認証エラー】

項目	内容
ファイル名	Type02.wav
ファイルパス	¥Program Files¥CASIO¥ActiveSecurity¥wav
ファイル形式	端末で再生可能な WAV 形式

カシオ計算機お問い合わせ窓口

製品に関する最新情報

●製品サポートサイト（カシオペア・ハンディターミナル）

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）