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. 1.01

**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。

© 2009 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。

# 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<br>戻り値 0x0004 を追加 |

# 目次


1. 概要 1

2. 認証機能 2
2.1 NFC 認証 2
2.2 パスワード認証 3

3. 導入と運用 4
3.1 インストールする 4
3.1.1 PC にインストールする 4
3.1.2 HT にインストールする 4
3.2 バージョンを確認する 6
3.3 アクティブセキュリティの有効無効を切り替える 6
3.4 セキュリティ条件（誤認証回数）を変更する 7
3.5 セキュリティ動作（削除ファイル／フォルダ）を変更する 8
3.6 ユーザアカウントを追加する 9
3.7 ユーザアカウントを削除する 10
3.8 ユーザアカウントにアドミン権限を与える 11
3.9 カード認証のテストをする 12
3.10 パスワード認証のテストをする 13
3.11 定義を暗号化する 14
3.11.1 コマンドライン書式 14
3.11.2 戻り値 14
3.12 アカウント情報テーブルを作成する 15
3.12.1 コマンドライン書式 15
3.12.2 戻り値 15
3.12.3 CSV 形式アカウント情報テーブルファイルフォーマット 16

4. 電池残量低下時の動作について 17

5. ログを参照する 18
5.1 ユーザ認証ログ 18
5.2 設定変更ログ 19
5.3 アカウント操作ログ 19

6. カスタマイズをする 20
6.1 認証方法を変更する 20
6.1.1 メイン認証呼び出し用関数 21
6.1.2 サブ認証呼び出し用関数 22
6.2 NFC のデータ参照先を変更する 23
6.2.1 NFC データ参照定義ファイル（TXT 形式） 23
6.2.2 NFC データ参照定義ファイル（DAT 形式） 24
6.3 背景をカスタマイズする 25
6.4 認証サウンドをカスタマイズする 27
6.5 ソフトキーボードの自動表示を切り替える 28

# 1. 概要

本書は、CASIO Active Security を利用していただくための操作マニュアルです。

CASIO Active Security では、端末にユーザ認証機能を持たせることで、特定のユーザのみが利用可能な環境を提供します。また、別途アドオンを用意することでユーザ認証方式を変更することが可能であり、運用ごとに最適なセキュリティ環境を実現できます。

以下に本システムで提供する機能の一覧を記します。

| 機能 | 概要説明 |
|---|---|
| 認証機能 | 標準で提供する認証方法です。（標準認証と呼びます） |
| NFC 認証 | NFC カードを使用した認証を行います。 |
| パスワード認証 | パスワード入力による認証を行います。 |
| セキュリティ設定機能 | セキュリティに関する設定を行います。 |
| 有効無効設定 | セキュリティの ON/OFF を設定します。 |
| 誤認証回数設定 | セキュリティが発動する誤認証回数を設定します。 |
| 削除ファイル／フォルダ設定 | 連続して誤認証した回数が設定値を超過した場合に削除するファイル／フォルダを指定します。 |
| ユーザアカウント編集機能 | ユーザアカウントに関する編集を行います。<br>※標準認証でのみ有効です。 |
| ハンディ用 | |
| ユーザアカウントの追加 | ユーザアカウントを新規に追加します。 |
| ユーザアカウントの削除 | ユーザアカウントを削除します。 |
| アドミン権限の設定 | ユーザに**アドミン権限**※の設定を行います。 |
| カード認証テスト | NFC カードが登録済みか否かを調べます。 |
| パスワード認証テスト | パスワードが登録済みか否かを調べます。 |
| PC 用 | |
| アカウント情報テーブル作成機能 | アカウント情報テーブルファイルを作成します。 |
| 電池残量監視機能 | 認証中に電池残量低下を検出した場合、電源を落とします。 |
| カスタマイズ機能 | 標準認証を運用にあわせてカスタマイズします。 |
| 認証方法カスタマイズ | 標準認証の代わりに別の認証を用いて認証を行います。 |
| NFC 参照先カスタマイズ | NFC カードの読み込み部分を変更します。 |
| 背景カスタマイズ | 背景画像を変更します。 |
| サウンドカスタマイズ | 認証時の効果音を変更します。 |
| ソフトキーボード自動表示 | ソフトキーボード自動表示を設定します。 |
| 定義暗号化機能 | 定義ファイルを暗号化します。（PC 用ツール） |
| ログ機能 | アカウント操作に関する端末ログを出力します。 |

※ アドミン権限とは、アカウントに関する編集を可能とする権限です。
※ 本マニュアル上の画面デザインは変更する場合があります。

# 2. 認証機能

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、電源ボタン、タッチパネル、キーボードの操作を行うことは可能ですが、ActiveSync やエクスプローラによるファイルアクセスはできません。
ユーザ認証には NFC 認証とパスワード認証の2つの認証方式があります。

## 2.1 NFC 認証

本体液晶部に NFC カードをかざすことで認証を行います。

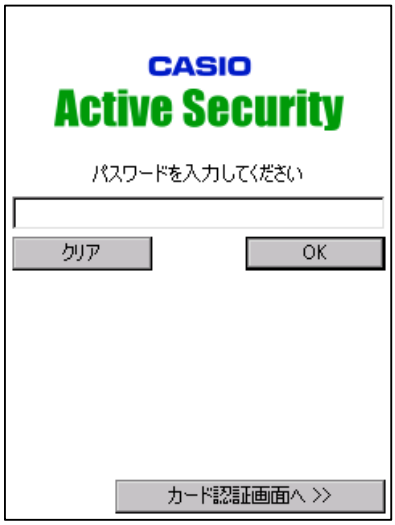
NFC認証画面（認証有効）

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）へ遷移します。
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）へ遷移します。
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遷移します。

## 2.2 パスワード認証

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 認証へ遷移します。

# 3. 導入と運用

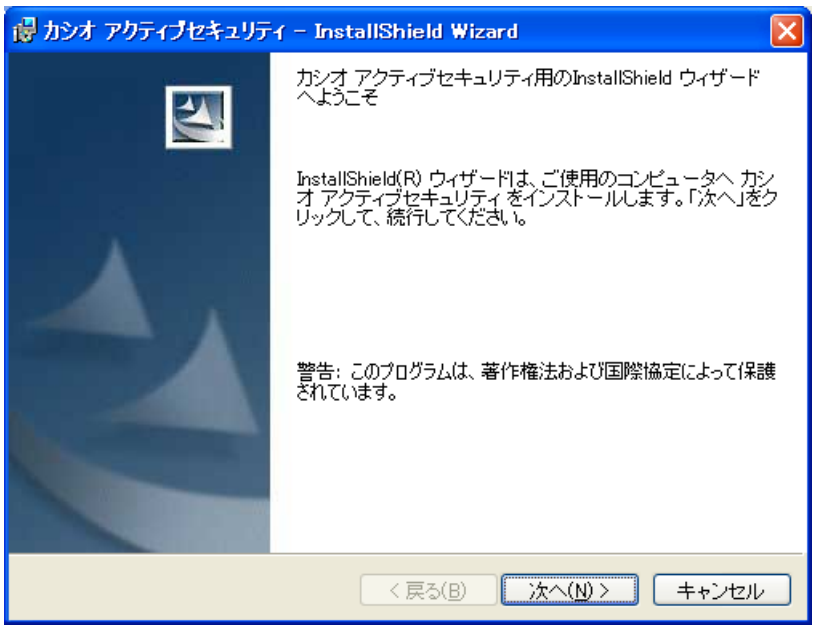
## 3.1 インストールする

### 3.1.1 PC にインストールする

アクティブセキュリティの環境を構築するためには、まず PC へ「カシオ アクティブセキュリティ」をインストールする必要があります。

1. 商品 CD にある setup.exe を実行してください。

2. 画面の指示に従ってインストールを実行してください。




### 3.1.2 HT にインストールする

【Windows XP でインストールする場合】

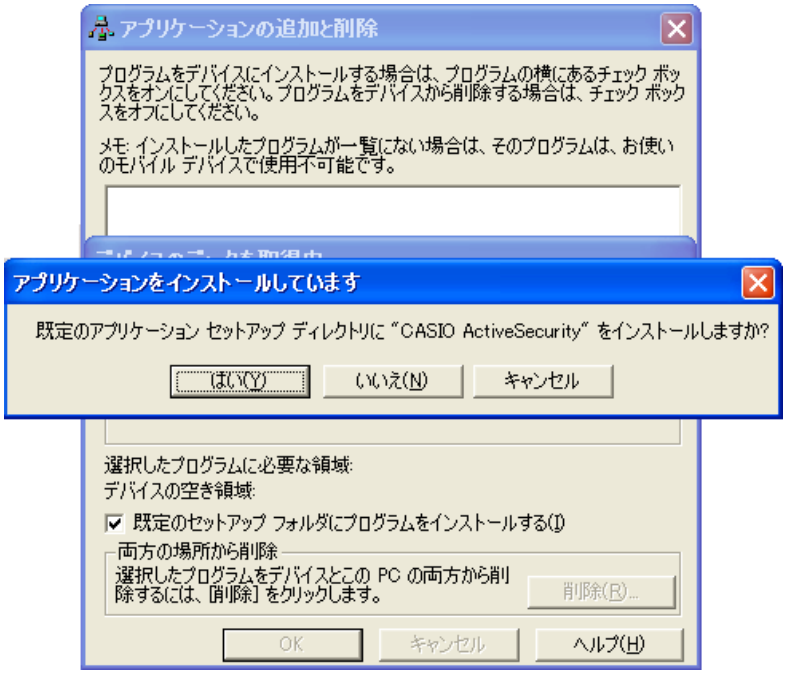
インストール元となる PC に「カシオ アクティブセキュリティ」がインストール済みで、インストール先となる HT とは ActiveSync で接続されている状態であることを前提とします。

1. インストール先となる HT 上で既にアクティブセキュリティを実行している場合は、HT 上のアクティブセキュリティを無効に設定し(「3.3アクティブセキュリティの有効無効を切り替える」参照)、リセットを行います。

2. PC 上のスタートメニューより、以下のメニューを選択して実行します。

   [スタート]→[プログラム]→[カシオ アクティブセキュリティ]→[クライアントモジュールを転送(ARMV4I)]

3. 画面の指示に従ってインストールを実行してください。




4. インストールが完了しましたら、端末をリセットします。

5. 次回起動時に認証画面が表示されることを確認してください。

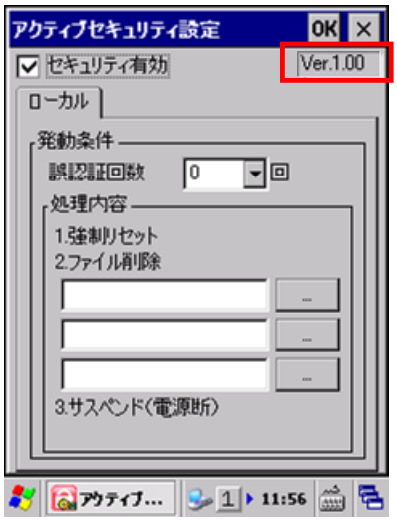
※ 初回インストール直後では、NFC 認証を行うことはできません。パスワード認証で「casio」と入力してください。ユーザ名:「Administrator」で認証します。セキュリティ保護のため、「3.6ユーザアカウントを追加する」「3.7ユーザアカウントを削除する」を参照してアカウントの編集を行ってください。
※ 一度インストールされますと、セキュリティ保護のためアンインストールを行うことはできません。

【Windows Vista でインストールする場合】

Windows Mobile Device Center を利用して端末側に以下のモジュールを送信し端末側で実行してください。
[¥Program Files]¥CASIO¥ActiveSecurity¥CAB¥ja_ActiveSecurity.ARMV4I.CAB

## 3.2 バージョンを確認する

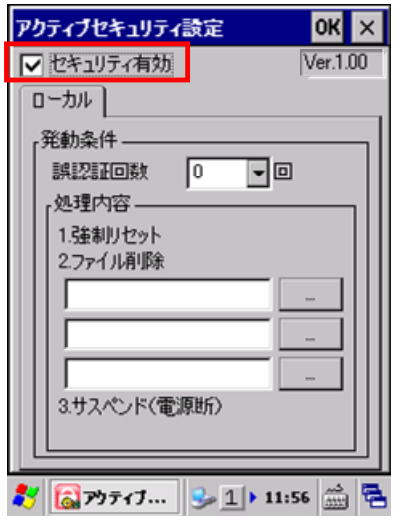
アクティブセキュリティのバージョン情報を確認する場合は、「プログラム」→「ユーティリティ」→「アクティブセキュリティ設定」を選択します。




※ アクティブセキュリティ設定起動中は電源を落とさないでください。

## 3.3 アクティブセキュリティの有効無効を切り替える

アクティブセキュリティの有効無効を変更する場合は、「プログラム」→「ユーティリティ」→「アクティブセキュリティ設定」を選択します。

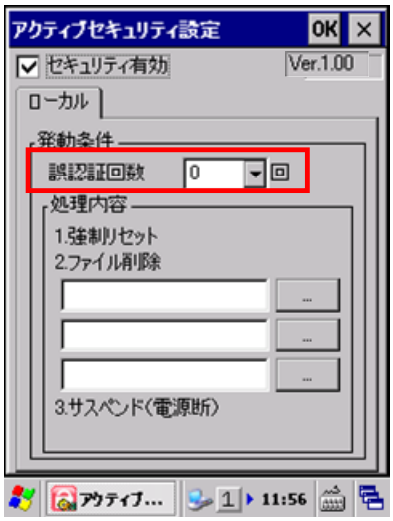



チェックあり：セキュリティ有効
チェックなし：セキュリティ無効

※ 次回リセット時から有効となります。
※ セキュリティが有効で、かつ、アドミン権限のないユーザが本ツールを起動した場合、設定の変更はできません。
※ アクティブセキュリティ設定起動中は電源を落とさないでください。
※ アクティブセキュリティ設定起動中はオートパワーオフ無効となります。

## 3.4 セキュリティ条件（誤認証回数）を変更する

連続誤認証回数を変更する場合は、「プログラム」→「ユーティリティ」→「アクティブセキュリティ設定」を選択します。

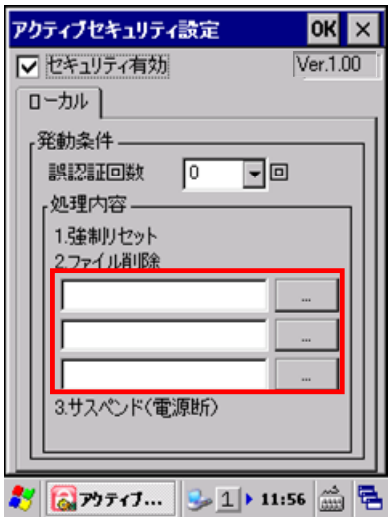



0～999の範囲で任意に設定可能です。しかし、数字以外の文字や範囲外を指定した場合は0となります。
0を指定した場合は、連続誤認証回数に制限がなくなります。

※ 設定保存時から有効となります。
※ セキュリティが有効で、かつ、アドミン権限のないユーザが本ツールを起動した場合、設定の変更はできません。
※ アクティブセキュリティ設定起動中は電源を落とさないでください。
※ アクティブセキュリティ設定起動中はオートパワーオフ無効となります。

## 3.5　セキュリティ動作（削除ファイル／フォルダ）を変更する

連続誤認証回数を超過した場合に削除するファイル／フォルダを変更する場合は、「プログラム」→「ユーティリティ」→「アクティブセキュリティ設定」を選択します。

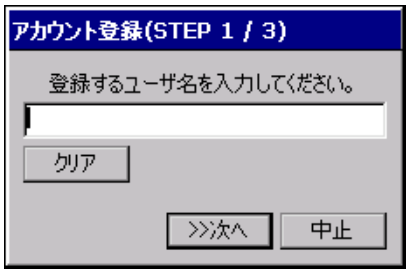



連続誤認証回数を超過した場合に削除するファイル／フォルダを指定します。末尾にワイルドカード（＊）を使用することで指定フォルダ下すべてのファイルを削除対象とします。

※ 設定保存時から有効となります。
※ セキュリティが有効で、かつ、アドミン権限のないユーザが本ツールを起動した場合、設定の変更はできません。
※ アクティブセキュリティ設定起動中は電源を落とさないでください。
※ アクティブセキュリティ設定起動中はオートパワーオフ無効となります。
※ システムファイル／フォルダを指定した場合は、セキュリティ動作後に正常に起動できなくなる場合があります。

## 3.6 ユーザアカウントを追加する

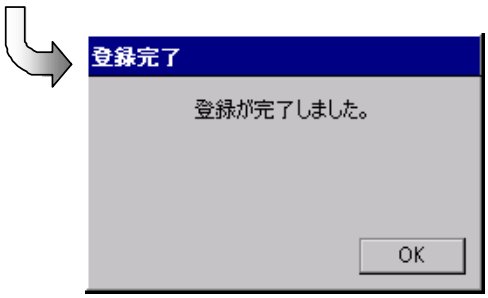
標準認証で認証可能なユーザの追加を行います。
端末上で「プログラム」→「ユーティリティ」→「アクティブセキュリティアカウント設定」を選択し、「**新規追加**」を押下してください。




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。

※ アクティブセキュリティアカウント設定起動中は電源を落とさないでください。
※ アクティブセキュリティアカウント設定起動中はオートパワーオフ無効となります。

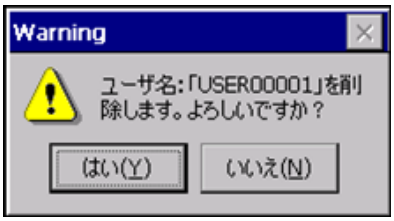
## 3.7 ユーザアカウントを削除する

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「プログラム」→「ユーティリティ」→「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. 「OK」を押下してください。

※ アクティブセキュリティアカウント設定起動中は電源を落とさないでください。
※ アクティブセキュリティアカウント設定起動中はオートパワーオフ無効となります。

## 3.8 ユーザアカウントにアドミン権限を与える

アドミン権限とは、アカウントに関する編集を可能とする権限であり、必ず1名以上のアドミン権限保持アカウントを必要とします。

端末上で「プログラム」→「ユーティリティ」→「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ン権限の有り無しを設定します。

アドミン権限のないユーザで本ツールを起動した場合、アカウントの操作はできません。

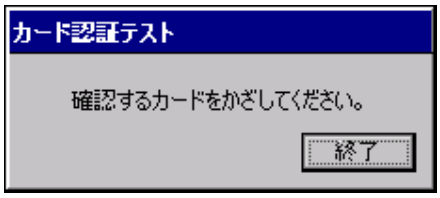
アドミン権限のないユーザで起動した場合

※ アクティブセキュリティアカウント設定起動中は電源を落とさないでください。
※ アクティブセキュリティアカウント設定起動中はオートパワーオフ無効となります。

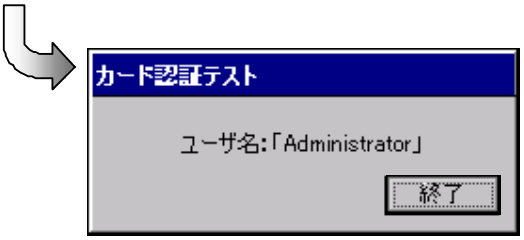
## 3.9 カード認証のテストをする

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。

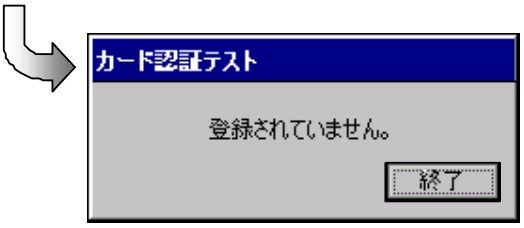
端末上で「プログラム」→「ユーティリティ」→「アクティブセキュリティアカウント設定」を選択し、「**カード認証テスト**」を押下してください。




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「Administrator」で登録済みです。



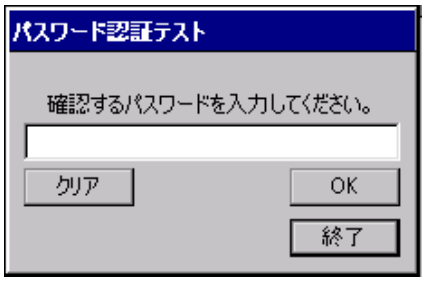

3. かざしたカードは未登録です。

※ アクティブセキュリティアカウント設定起動中は電源を落とさないでください。
※ アクティブセキュリティアカウント設定起動中はオートパワーオフ無効となります。

## 3.10 パスワード認証のテストをする

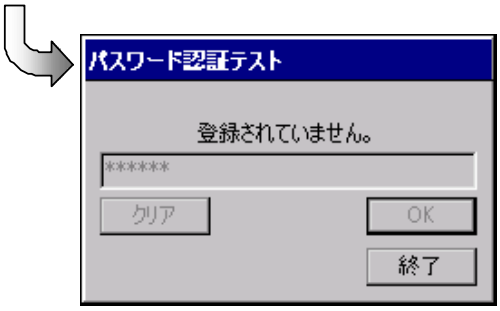
パスワードを入力し、登録済みアカウントか否かをテストします。登録済みの場合はそのユーザ名を表示します。

端末上で「プログラム」→「ユーティリティ」→「アクティブセキュリティアカウント設定」を選択し、「**パスワード認証テスト**」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「Administrator」で登録済みです。




3. 入力したパスワードは未登録です。

※ アクティブセキュリティアカウント設定起動中は電源を落とさないでください。
※ アクティブセキュリティアカウント設定起動中はオートパワーオフ無効となります。

## 3.11 定義を暗号化する

以下の PC 用コマンドを用いて、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。
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。

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 | [Program Files]¥CASIO¥ActiveSecurity¥Command¥ |
| ファイル形式 | MS-DOS コマンド実行形式 |

### 3.11.1 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。

### 3.11.2 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. |

## 3.12 アカウント情報テーブルを作成する

以下の PC 用コマンドを用いて、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。

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 | [Program Files]¥CASIO¥ActiveSecurity¥Command¥ |
| ファイル形式 | MS-DOS コマンド実行形式 |

### 3.12.1 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。<br>本ファイルのフォーマットについては「3.12.3 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。

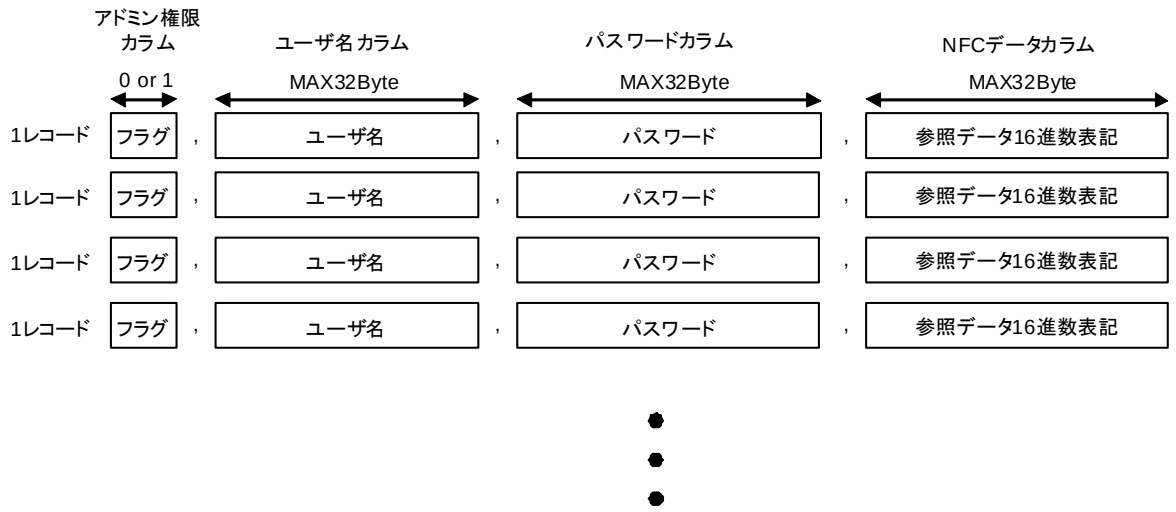
### 3.12.2 戻り値

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. |

### 3.12.3 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。

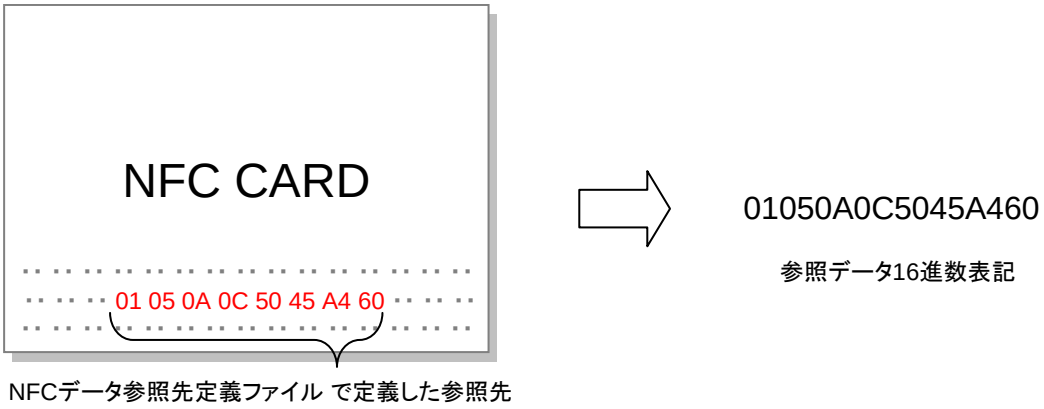



例：

1,CASIO_A,11111,0A0B0C0　*説明：アドミン権限有、パスワード「11111」、NFC データ「0A0B0C0」*
0,CASIO_B,11112,0B0C0D0　*説明：アドミン権限無、パスワード「11112」、NFC データ「0B0C0D0」*
0,CASIO_C,11113,0C0D0E0　*説明：アドミン権限無、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。



## 4. 電池残量低下時の動作について

認証中に電池残量低下を検出した場合は、以下のダイアログを表示し、10 秒後に電源を落とします。
ダイアログ表示中に AC による電源供給を行った場合は、認証画面に戻ります。

# 5. ログを参照する

本システムでは操作内容を端末ログに出力しています。以下に出力フォーマットを記します。
端末ログを閲覧するには「プログラム」→「ユーティリティ」→「端末ログビューア」を起動してください。

## 5.1 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<br>誤認証回数超過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<br>誤認証回数超過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 |

## 5.2 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. | [USER NAME]を新規に追加 |
| 3 | 情報 | 情報 | Saved ActiveSecurity Setting. Saved ActiveSecurity Setting.<br>Times= [誤認証回数]<br>Security=Enable / Disable<br>DeleteFolder = [設定パス]<br>DeleteFolder = [設定パス]<br>DeleteFolder = [設定パス] | 設定内容 |

## 5.3 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]からアドミン権限を剥奪 |
| 5 | 情報 | 情報 | [USER NAME] is given the Administrator Authority. | [USER NAME]にアドミン権限を授与 |
| 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 |

# 6. カスタマイズをする

## 6.1 認証方法を変更する

アクティブセキュリティでは、別途アドイン(「外部認証アドイン」と呼びます)を用意していただくことで、運用環境に適した認証方式を実装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¥ActiveSecurity¥dll¥ |
| ファイル形式 | ダイアミックリンクライブラリ |

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全画面／前面の属性を持つこと。<br>現在の状況を正しくユーザに伝えること。 |
| 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。<br>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。<br>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。

### 6.1.1　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()
```

```
[Visual Basic]
Public Shared Function CASMainRecognize() As Int32
```

```
[C#]
public static Int32 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、認証完了時（戻り値：0x0000）、認証したアカウントにアドミン権限を持たせる場合は以下のレジストリを設定する必要があります。

[HKEY_LOCAL_MACHINE¥SOFTWARE¥CASIO¥ActiveSecurity]

| キー名 | タイプ | 内容 |
|---|---|---|
| Admin | DWORD | 0：アドミン権限を持たないアカウント<br>1：アドミン権限を持つアカウント |

**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：メイン認証方式呼び出し依頼
誤認証回数カウントアップ、誤認証回数判定を実行します。
0x0004　：認証失敗：サブ認証方式呼び出し依頼
：誤認証回数カウントアップ、誤認証回数判定を実行します。
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。

### 6.1.2　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()
```

```
[Visual Basic]
Public Shared Function CASSubRecognize() As Int32
```

```
[C#]
public static Int32 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、認証完了時（戻り値：0x0000）、認証したアカウントにアドミン権限を持たせる場合は以下のレジストリを設定する必要があります。

[HKEY_LOCAL_MACHINE¥SOFTWARE¥CASIO¥ActiveSecurity]

| キー名 | タイプ | 内容 |
|---|---|---|
| Admin | DWORD | 0：アドミン権限を持たないアカウント<br>1：アドミン権限を持つアカウント |

**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：メイン認証方式呼び出し依頼
誤認証回数カウントアップ、誤認証回数判定を実行します。
0x0004　：認証失敗：サブ認証方式呼び出し依頼
：誤認証回数カウントアップ、誤認証回数判定を実行します。
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。

## 6.2 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。

### 6.2.1 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¥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。<br>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。<br>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。<br>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。<br>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。<br>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。

### 6.2.2　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¥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「3.11定義を暗号化する」を参照してください。

## 6.3 背景をカスタマイズする

アクティブ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¥ActiveSecurity¥Images |
| ファイル形式 | BMP 形式 |
| サイズ | 240x320（VGA 時 480x640 に自動伸張表示する） |
| 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¥ActiveSecurity¥Images |
| ファイル形式 | BMP 形式 |
| サイズ | 320x240（VGA 時 640x480 に自動伸張表示する） |
| 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¥ActiveSecurity¥Images |
| ファイル形式 | BMP 形式 |
| サイズ | 240x320（VGA 時 480x640 に自動伸張表示する） |
| 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 | ¥¥ Files¥ActiveSecurity¥Images |
| ファイル形式 | BMP 形式 |
| サイズ | 320x240（VGA 時 640x480 に自動伸張表示する） |
| 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¥ActiveSecurity¥Images |
| ファイル形式 | BMP 形式 |
| サイズ | 240x320（VGA 時　480x640 に自動伸張表示する） |
| 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 | ¥¥ Files¥ActiveSecurity¥Images |
| ファイル形式 | BMP 形式 |
| サイズ | 320x240（VGA 時　640x480 に自動伸張表示する） |
| 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¥ActiveSecurity¥Images |
| ファイル形式 | BMP 形式 |
| サイズ | 240x320（VGA 時　480x640 に自動伸張表示する） |
| 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¥ActiveSecurity¥Images |
| ファイル形式 | BMP 形式 |
| サイズ | 320x240（VGA 時　640x480 に自動伸張表示する） |
| 色数 | MAX 16bit |

## 6.4 認証サウンドをカスタマイズする

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サウンドを再生しています。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¥ActiveSecurity¥wav |
| ファイル形式 | 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¥ActiveSecurity¥wav |
| ファイル形式 | 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¥ActiveSecurity¥wav |
| ファイル形式 | WAV 形式 |

## 6.5 ソフトキーボードの自動表示を切り替える

パスワード認証時やアカウント編集でのユーザ名／パスワード入力時等、キーボードを使用して入力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。

この機能を抑止する場合は、以下のレジストリの内容を変更してください。

[HKEY_LOCAL_MACHINE¥SOFTWARE¥CASIO¥ActiveSecurity]

| キー名 | タイプ | 内容 |
|---|---|---|
| SIPControl | DWORD | 0: ソフトキーボードを表示しません。<br>1: ソフトキーボードを表示します。 |

# カシオ計算機お問い合わせ窓口

**製品に関する最新情報**

**●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)