

SREX-FSU4



ユーザーズマニュアル

第1.0版



指紋認証システム導入ガイド

本製品は Windows10 のログオン認証機能である【Windows Hello】、または製品 CD-ROM に収録されている指紋認証ソフトウェア【OmniPassSE】にてご利用可能です。

本マニュアルの第 2 章では Windows Hello での使用について、第 3 章からは OmniPassSE での使用について説明を行っています。

※ Windows Hello と OmniPassSE を同時に使用することはできません。

目次

第1章 はじめに

1-1.製品の特徴	5 頁
1-2.安全にお使い頂くために	9 頁
1-3.マニュアルの構成	11 頁
1-4.製品に関するお問い合わせ	12 頁

第2章 Windows Hello での使用

2-1.ドライバーインストール	13 頁
2-2.指紋登録と認証	17 頁

第3章 OmniPassSE のインストールと登録

3-1.Windows ログオンパスワード作成	20 頁
3-2.OmniPassSE インストール	21 頁
■OmniPassSE のインストール	
■OmniPassSE のアンインストール	
3-3.OmniPassSE ユーザー登録	25 頁
■OmniPassSE ユーザー登録	
■OmniPassSE 認証ダイアログ	

第4章 OmniPassSE の使用

4-1.アカウント情報の記憶	30 頁
■Web ログオンパスワードの記憶	
■アプリケーションログオンパスワードの記憶	
■ID の管理	
4-2.暗号化と復号化	39 頁
■暗号化	
■復号化	
■暗号化ファイルの共有	

第5章 OmniPassSE の管理と設定

5-1.ユーザーの追加と削除	44 頁
■ユーザーの追加	
■ユーザーの削除	
5-2.アカウント情報の管理	47 頁

5-3.プロファイルのバックアップと復元	49 頁
----------------------	------

- ユーザープロファイルのバックアップ

- ユーザープロファイルの復元

5-4. OmniPassSE コントロールセンターその他の設定	53 頁
----------------------------------	------

- ユーザーのデバイス登録の変更

- 認証デバイスの必須設定

- 緊急ポリシーオーバーライド機能を有効にする

- OmniPassSE へのログオン設定

- 暗号化／復号化の設定

- サウンドの設定

- タスクバーヒントの設定

- 認証ウィンドウの設定

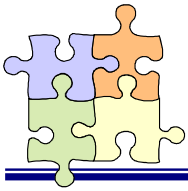
第6章 付録

6-1.アプリケーション API	63 頁
------------------	------

- OmniPassSE 認証サンプルプログラム概要

- API 呼び出し方法

- API インターフェイス仕様



本章では SREX-FSU4 指紋センサーおよび付属ソフトウェアの製品の特徴と使用上の注意点について説明しています。

SREX-FSU4 について

■ 場所をとらないUSB ドングルタイプ

ノートパソコンの USB ポートに装着したまま持ち運べるコンパクトデザインの指紋センサーです。

本体側面の 11(W)×5(L)mm の黒色部分がセンサーエリアで、弊社ロゴの下部には指紋センサーの動作状態を示す LED を装備。小型でも使いやすい設計になっています。



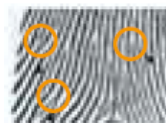
■ ハイブリッド方式で確実な個人認証が可能

指紋認証エンジンにバイオメトリックス技術「特徴点抽出方式」を採用。指紋の特徴点 6 か所以上の照合をおこないます。さらに、本製品の特長である小型のセンサーエリアにて、6 か所以上の特徴点を照合しきれないケースにおいては、パターン・マッチング方式により指紋の形状特徴を追加して照合をおこないます。特徴点抽出方式とパターン・マッチング方式とのハイブリッド方式で照合を行うことにより、他人受入率 (FAR) 0.002%以下、他人拒否率 (FRR) 2.95%以下と高性能な指紋識別能力を実現しています。



特徴点抽出方式とは

指紋の切れ目 (端点) や分かれ目 (分岐点) などの特徴のある箇所を、相対座標、方向性、種類などで照合する方式です。



分岐点

端点

○: 特徴点



■ 360 度どの向きからのタッチでも指紋照合

従来製品は決まった方向でのタッチが必要でしたが、本製品では向きの制限がありません。ノートパソコン、デスクトップパソコンの USB ポートの向きとらわれず、タッチしやすい向きで利用できる製品です。

■ 1 秒以内の高速認証

指紋認証を高速化する「Smart Learning」アルゴリズム搭載により、指紋認証をおこなうたびに最良の指紋イメージに更新することで、認証照合の高速化を図っています。

■ Windows Hello 対応

Windows10 のログオン認証機能である【Windows Hello】には、指紋認証機能でのログオンがサポートされました。

SREX-FSU4 は Windows Hello の指紋認証デバイスとして動作します。

Windows の基本機能から指紋登録を行い、Windows Hello で認証を行うことが可能です。

■ 認証ソフトウェアのデファクトスタンダード OmniPassSE8.0 採用

SREX-FSU4 指紋センサーと OmniPassSE を統合することにより、コンピューター、アプリケーション、Web サイト、その他のパスワードで保護されたリソースへのアクセスを制限する強固なセキュリティ認証システムの実現が可能です。OmniPassSE は下記の機能を提供します。

●指紋認証による Windows ログオン

指紋認証により Windows にログオンします。ユーザー名とパスワードを入力する必要はありません。

スタンバイからの復帰時、パスワード対応スクリーンセーバーロックの解除時も指紋認証によるログオンが可能です。

●ファイルの暗号化と共有

ファイルもしくはフォルダーを選ぶだけで指紋認証を使ったファイルの暗号化と復号化を行うことができます。個人情報、機密情報のセキュリティ保護を行うことができます。

暗号化したファイルを他のユーザーと共有する機能も提供しています。

●アカウント情報の管理

アカウント情報を要求する Web サイトやアプリケーションのアカウント情報（ユーザー名やパスワード）を無制限に記憶させることができます。一度 OmniPassSE にアカウント情報を記憶させることにより、以後指紋認証を利用してログオンすることが可能になります。複数のアカウント情報を覚えておくことができ、毎回入力する必要はありません。

●一台のパソコンを複数のユーザーで利用することが可能

複数ユーザーの指紋を登録し利用することができます。暗号化ファイルの共有設定も可能です。

●ユーザー作成アプリケーションから認証呼び出し

ユーザーが作成したアプリケーションプログラムに OmniPassSE 指紋認証ダイアログを呼び出すための API を公開しています。簡単に指紋認証を組み込むことができます。

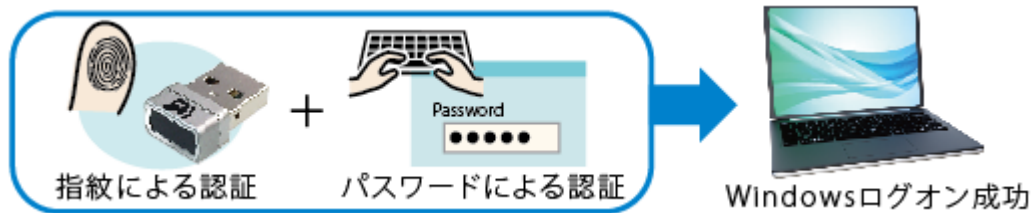
■ 複数人で使用 OK

1 つのアカウントで最大 10 本までの指紋を登録することができますので、最大で 10 人まで同一アカウントの共用が可能です。

また、複数の Windows のアカウントを作成いただくことで複数アカウントでの登録も可能です。

■ 総務省ガイドラインで求められる「二要素認証」に対応

認証条件を指紋認証とパスワード入力の両方必須とすれば、総務省の情報セキュリティに関するガイドラインでも求められている「二要素認証」となります。指紋認証ソフトウェア「OmniPass SE」の「認証規則の設定」でパスワード認証と指紋認証の両方にチェックすると、パソコンに指紋とパスワードの二要素認証を追加することができます。



■ パッケージの内容

本製品のパッケージには、次のものが同梱されています。不足の場合は、お手数ですが販売店または弊社サポートセンターまでご連絡ください。

- 指紋センサー本体
- CD-ROM(OmniPassSE 指紋認証ソフトウェア・マニュアル PDF)
- インストールガイド
- 保証書

■ OmniPassSE8.0 製品仕様






[OmniPassSE 8.01.xx]

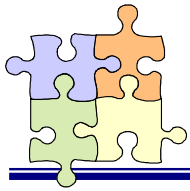
対応 OS	Windows 10/8.1/7 ※32ビット/64ビット両対応
対応ブラウザ	Internet Explorer 11.x

■ SREX-FSU4 製品仕様

製品名	USB 指紋認証システムセット・タッチ式
型番	SREX-FSU4
指紋センサー	センサー方式：静電容量式タッチ式センサー センサーエリア：11(W)mm×5(L)mm、密度：363DPI 階調：256色(8bit/pixel) グレースケール
インターフェイス	USB2.0 Full Speed Compliant
電源仕様	5V (USBバスパワーから取得)
消費電流	動作時：10mA(TYP)、待機時：4mA(TYP)、サスペンド時：0.5mA(TYP)
ESD 耐圧	12kV (IEC61000-4-2 Level 3)
保証動作環境	温度：0～40℃ 湿度：20～80%(ただし結露なきこと)
外形寸法・重量	約 14(W) × 8(H) × 21(D) mm (突起部含む)・約 5g
照 合 精 度	他人受入率(FAR):0.002%以下、本人拒否率(FRR):2.95%以下 認証速度：1sec.以下(Smart Learning アルゴリズム搭載)
対応 OS	Windows 10/8.1/7 ※32ビット/64ビット両対応

■ LED について

青点灯		ドライバーが正しく適用されて正常な状態
青点滅		ユーザーの指紋のタッチを待っている状態
緑点灯		認証成功(指紋登録時は正しく指紋が読めたときに点灯)
赤点灯		認証失敗(指紋登録時は指紋が正しく読み込めないときに点灯)
無点灯		PC がスリープモードあるいはデバイスが正しく認識されていない (デバイスマネージャーで！がついている等)



第1章 はじめに

1-2. 安全にお使い頂くために

本製品を安全にお使いいただくために、以降の記述内容を必ずお守りください。

本マニュアルでは、いろいろな表示をしています。これは、本製品を安全に正しくお使いいただき、あなたや他の人々に加えられるおそれのある危害や損害を未然に防止するために目安となるものです。その表示と意味は次のようになっています。内容をよくご理解の上、お読みください。



この表示を無視して誤った取り扱いをすると、データを失ったり、機密を要するデータが公開されたり、システムへのアクセスを拒否される等の危険があります。



この表示を無視して誤った取り扱いをすると、本製品の機能が損なわれ、本マニュアルに記載された手順通りの動作ができなくなる可能性があることを示しています。

ご使用上の注意事項

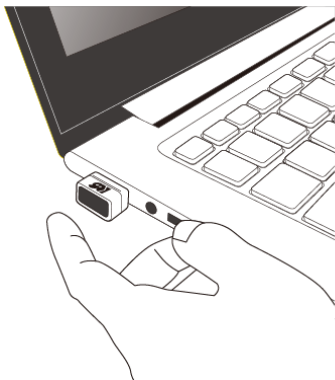
■接続時のご注意

- ①1台のパソコンに同一の指紋センサーを複数接続しないでください。
- ②USBハブに接続して使用する場合は、セルフパワー電源タイプ（ACアダプターなどで電源が供給されるタイプ）のハブに接続し、直列接続は2段以内にしてください。
- ③他社製の指紋センサーがインストールされている場合は、そのソフトウェアをアンインストールしてから本指紋センサーを接続してください。
- ④指紋認証中に本指紋センサーの取り外しを行わないでください。

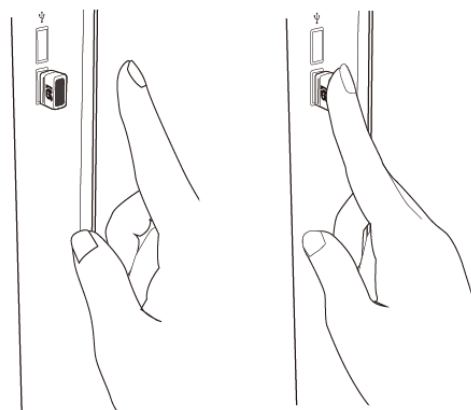
■SREX-FSU4 指紋取得方法について

360度どの向きからのタッチでも指紋照合可能ですが、指紋センサーの認識率や照合率の精度を保つために、下図を参考に指を置いてください。

指の腹の部分センサー面の中央に押し当て、指紋取得が完了するまで触れてください。



【センサーが横向きの場合】












【センサーが縦向きの場合】

※次の場合は指紋を認識できない場合や、照合率が低下することがあります。

- 指が乾燥している場合
- 指が汗や水で濡れている場合
- 皮膚が荒れている場合
- 泥や油で指が汚れている場合
- 指紋が薄い場合
- センサー面にホコリや汚れや水分がある場合

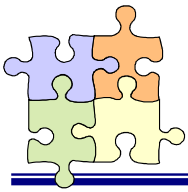
その他のご注意

	①指紋認証技術は完全な本人認証・照合を保証するものではありません。当社では本製品を使用されたこと、または使用できなかったことによって生じるいかなる損害に関しても、一切責任を負いかねますのであらかじめご了承ください。
	②本製品はパソコン用周辺機器として設計されております。人命に関わる用途、または高度な信頼性、安全性を要する用途での使用は考慮されておりません。このような用途で使用される設備、機器、システム等への組み込みは避けてください。
	③本書の内容に関しましては、将来予告なしに変更することがあります。 また、本書の内容につきましては万全を期して作成しましたが、万一不審な点や誤りなどお気づきになりましたらご連絡願います。
	④本製品は日本国内仕様となっており、海外での保守およびサポートは行っておりません。
	⑤本製品は電子機器ですので、静電気を与えないでください。
	⑥ラジオやテレビ、オーディオ機器の近く、モータなどノイズを発生する機器の近くでは誤動作することがあります。必ず離してご使用ください。
	⑦高温多湿の場所、温度差の激しい場所、チリやほこりの多い場所、振動や衝撃の加わる場所、スピーカ等の磁気を帯びたものの近くでの保管は避けてください。
	⑧製品の分解や改造等は、絶対に行わないでください。
	⑨無理に曲げる、落とす、傷つける、上に重いものを載せることは行わないでください。

この装置は、クラスB機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

V C C I - B



第1章 はじめに

1-3. マニュアルの構成

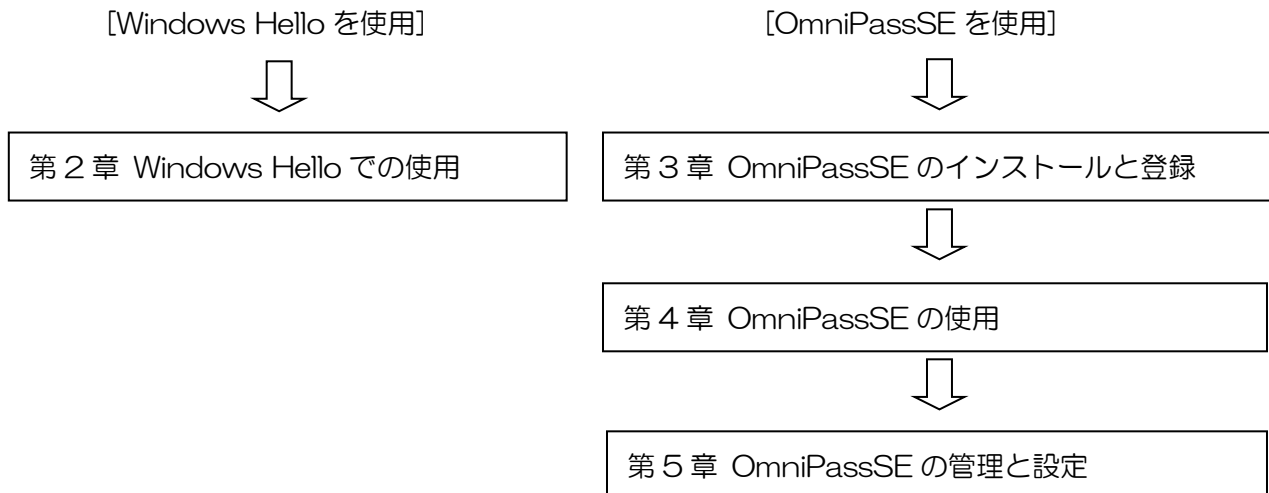
本製品では、Windows10 のログオン認証機能である【Windows Hello】と、製品 CD-ROM に収録されている【OmniPassSE】にてご利用可能です。

使用する OS や機能により選択してください。

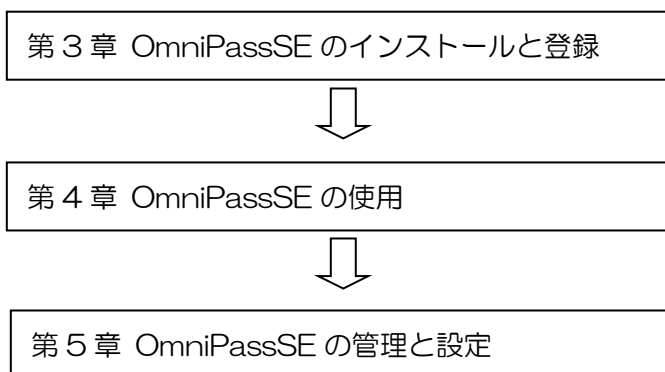
	Windows Hello	OmniPassSE
対応 OS	Windows10	Windows10/8.1/7
機能	Windows ログオン	Windows ログオン パスワード認証 Web ページ ファイル・フォルダーの暗号化

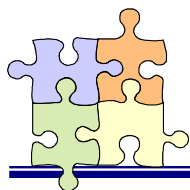
■ Windows10 でご使用の場合

Windows Hello または OmniPassSE のどちらかを使用します。



■ Windows8.1/7 でご使用の場合





第1章 はじめに

1-4. 製品に関するお問い合わせ

本製品に関するご質問がございましたら、下記までお問い合わせください。お問い合わせの際には、巻末の「質問用紙」に必要事項をご記入の上、下記 FAX 番号までお送りください。折り返し弊社より電話または FAX、電子メールにて回答いたします。

ご質問に対する回答は、下記営業時間内となりますのでご了承ください。また、ご質問の内容によりましてはテスト・チェック等の関係上、時間がかかる場合もございますので予めご了承ください。

ラトックシステム株式会社 サポートセンター

〒556-0012 大阪市浪速区敷津東 1-6-14 朝日なんばビル

TEL 06-6633-6741

月～金 10:00～13:00、14:00～17:00

土曜、日曜および祝日を除く

FAX 06-6633-8285

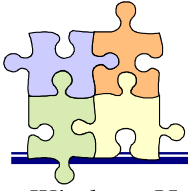
電子メール：<https://web1.ratocsystems.com/mail/support.html>

ホームページで最新の情報をお届けしております。

<http://www.ratocsystems.com>

個人情報取り扱いについて

ご連絡いただいた氏名、住所、電話番号、メールアドレス、その他の個人情報は、お客様への回答など本件に関する業務のみに利用し、他の目的では利用致しません。



第2章 Windows Hello での使用

2-1. ドライバーインストール

Windows Hello で使用するためには、下記手順によりドライバーをインストールする必要があります。

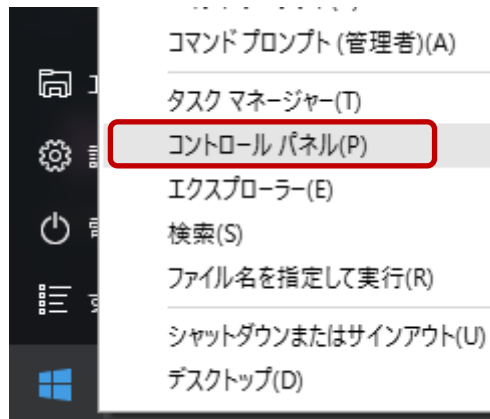


ドライバーをインストールするには、インターネットに接続する必要があります。

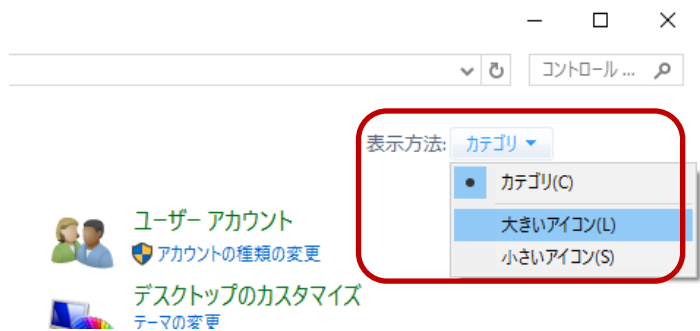
OmniPassSE はインストールしないでください。

2-1-1.

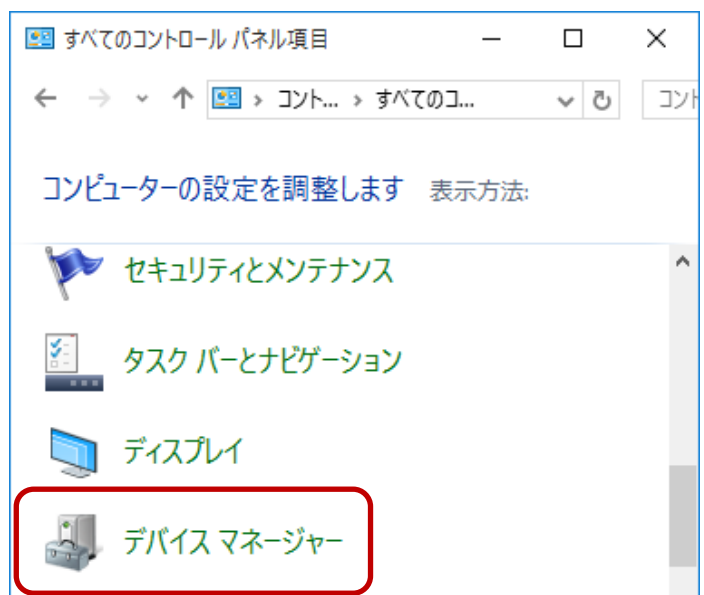
Windows スタートボタンを右クリックし、[コントロールパネル]を開きます。



表示方法を[大きいアイコン]に変更します。

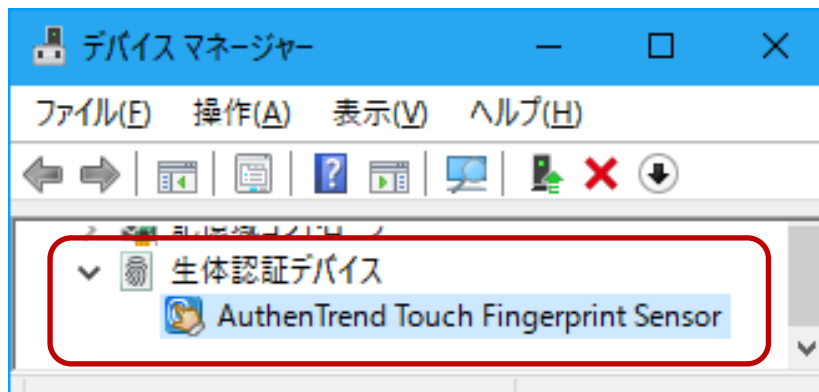


デバイスマネージャーを開きます。

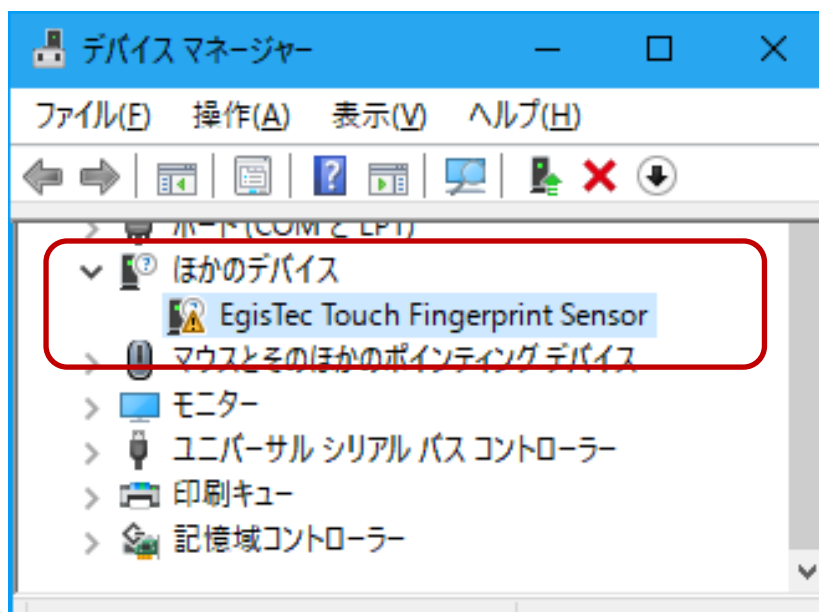


2-1-2.

下図のように「AuthenTrend Touch Fingerprint Sensor」と正常に認識している場合は、「2-2. 指紋登録と認証」へ進んでください。

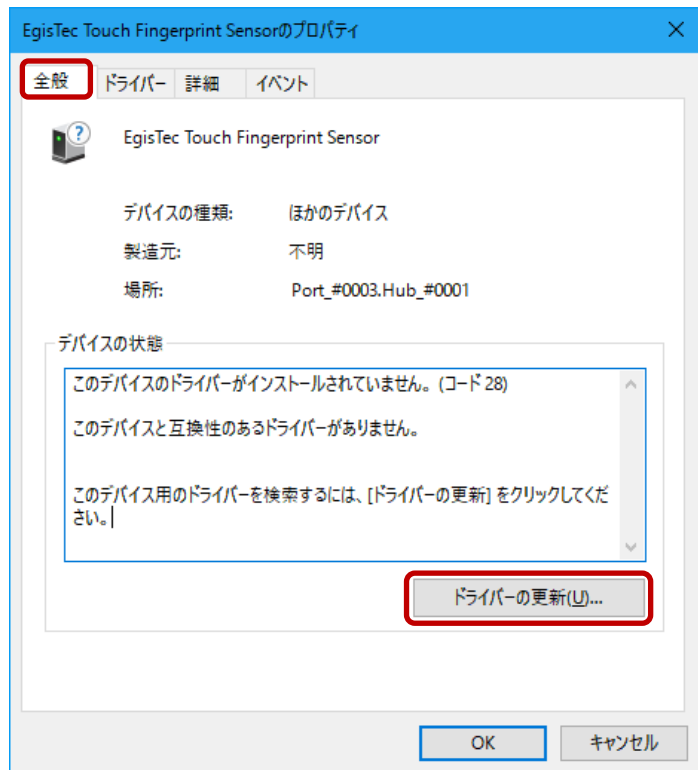


「?!」EgisTec Touch Fingerprint Sensor」と正常に認識していない場合は、右クリックしてプロパティを開きます。



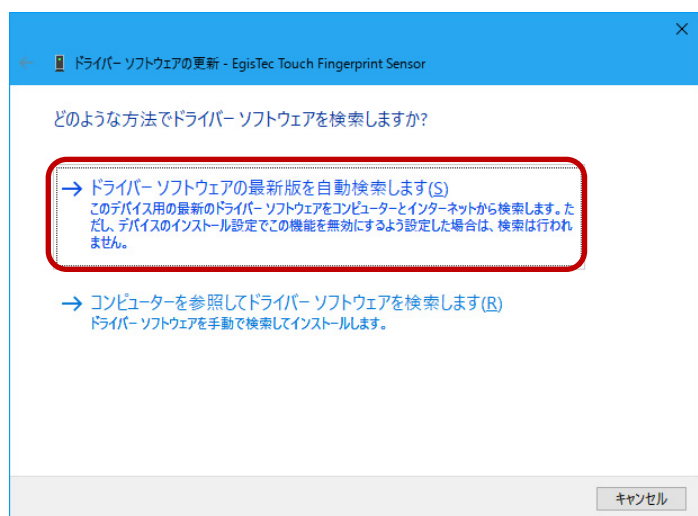
2-1-3.

「ドライバーの更新」をクリックします。



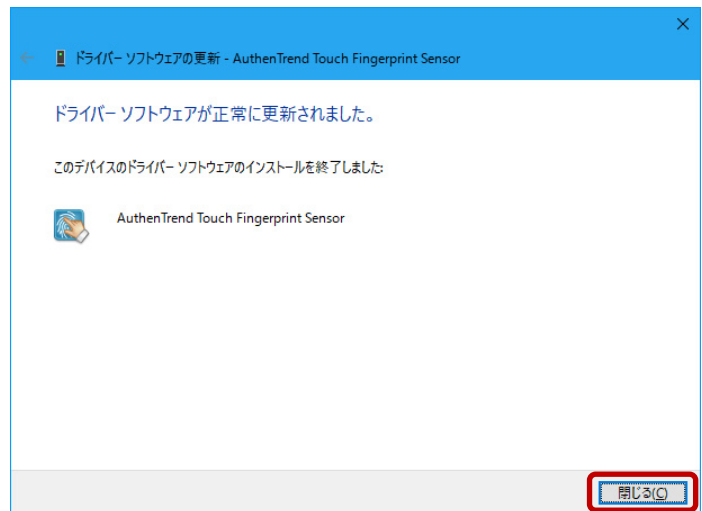
2-1-4.

インターネットに接続できることを確認し、「ドライバーソフトウェアの最新版を自動検索します」をクリックします。



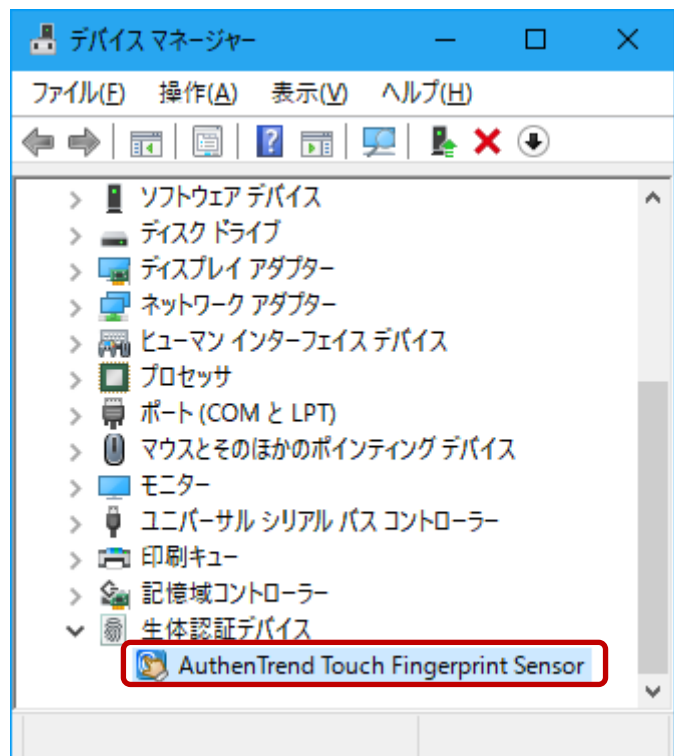
2-1-5.

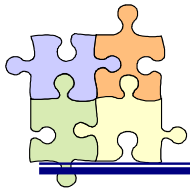
以上で Windows Hello 用のドライバーインストールは完了です。



2-1-6.

デバイスマネージャー上で「AuthenTrend Touch Fingerprint Sensor」と認識していることを確認し、「2.2 指紋登録と認証」へ進みます。





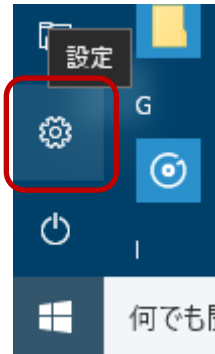
第2章 Windows Hello での使用

2-2. 指紋登録と認証

Windows Hello を使用するには、Windows パスワードと暗証番号(PIN)の設定が必要です。

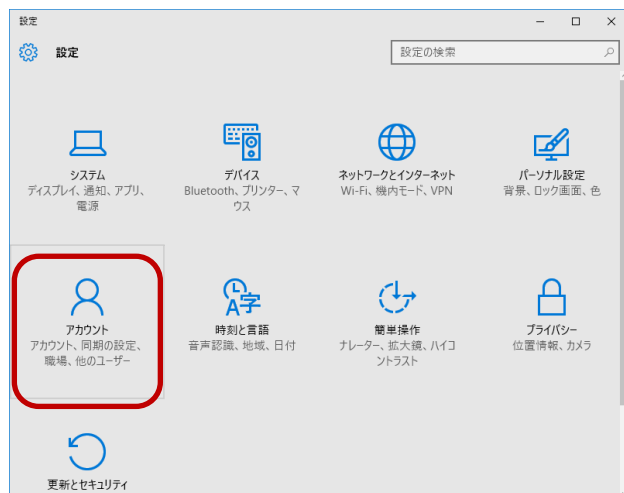
2-2-1.

Windows スタートメニューの[設定]をクリックします。



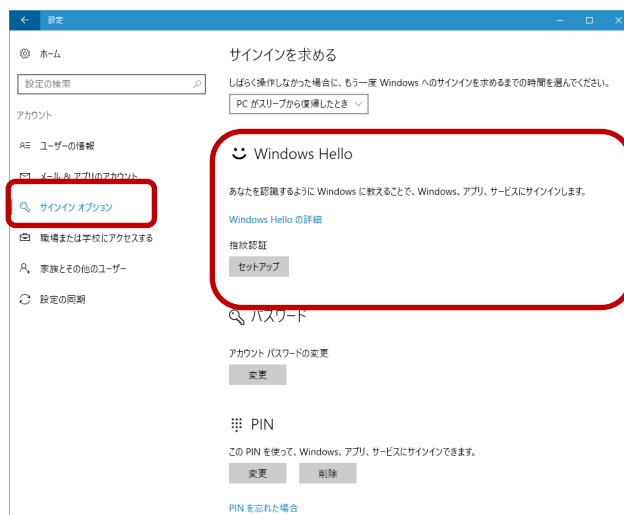
2-2-2.

[アカウント]をクリックします。



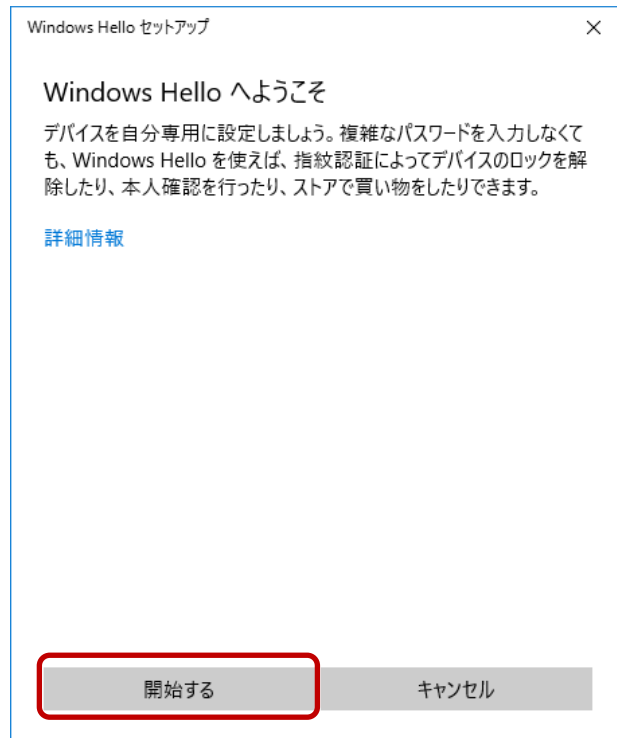
2-2-3.

[サインイン オプション]を選択し、[パスワード] [暗証番号(PIN)]の設定後に [Windows Hello]の「セットアップ」をクリックします。



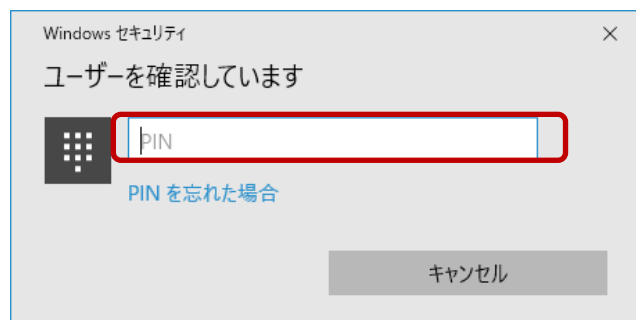
2-2-4.

「開始する」をクリックします。



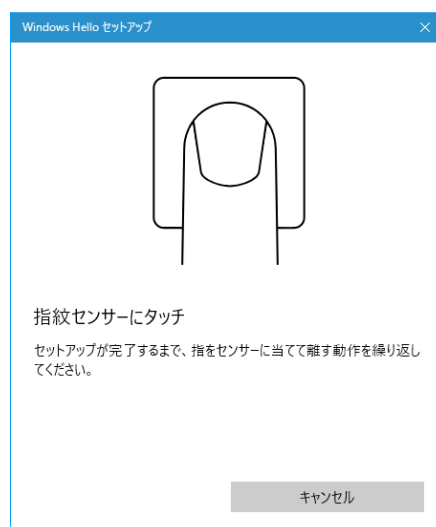
2-2-5.

設定した暗証番号(PIN)を入力します。



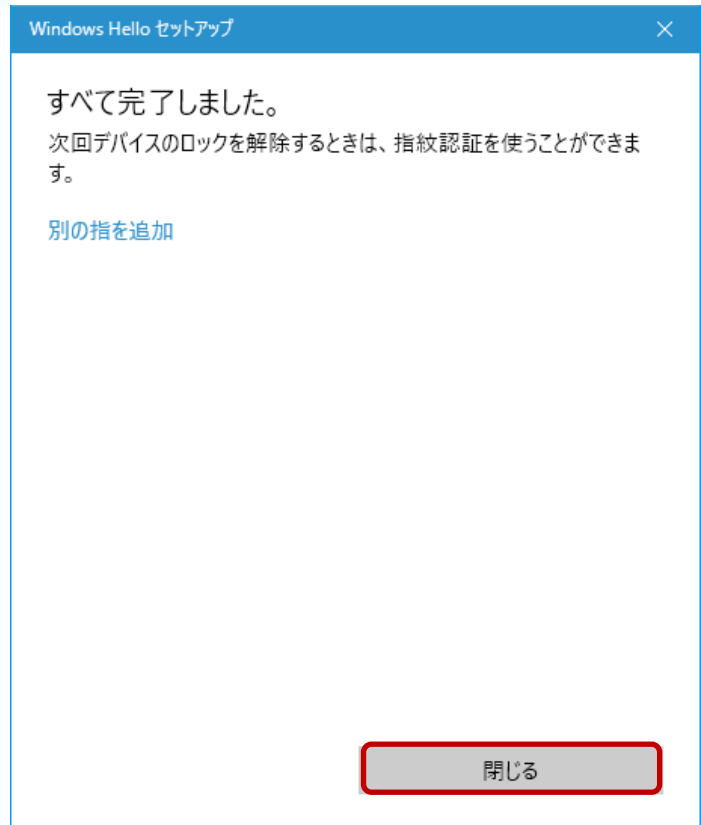
2-2-6.

画面の指示にしたがい、指紋の登録を行います。



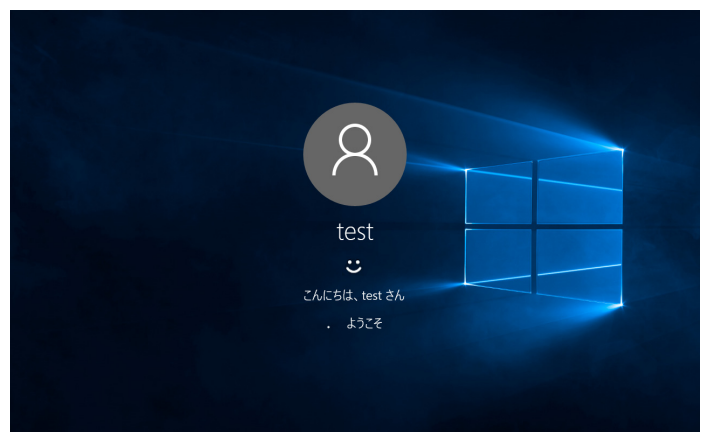
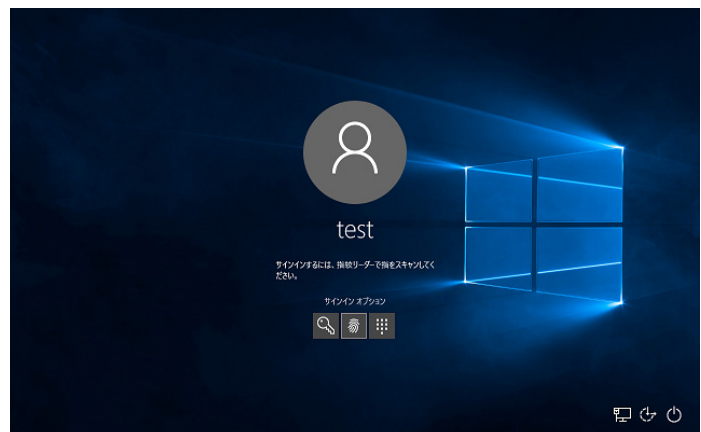
2-2-7.

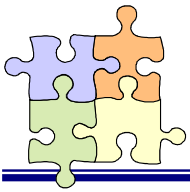
以上で指紋登録は完了です。
別の指紋を登録する場合は「別の指を追加」をクリックし追加で登録を行います。



2-2-8.

Windows ログオン時に登録した指紋をスキャンすることで、自動的にログオンすることができます。



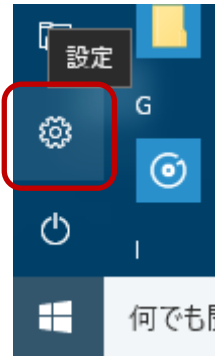


3-1. Windows ログオンパスワード作成

OmniPassSE ユーザー登録では Windows ログオン時のユーザー名とパスワードが必要になります。OmniPassSE ユーザー登録を行う前に、必ず Windows のログオンパスワードを作成してください。(下記は Windows10 での説明画面となります)

3-1-1.

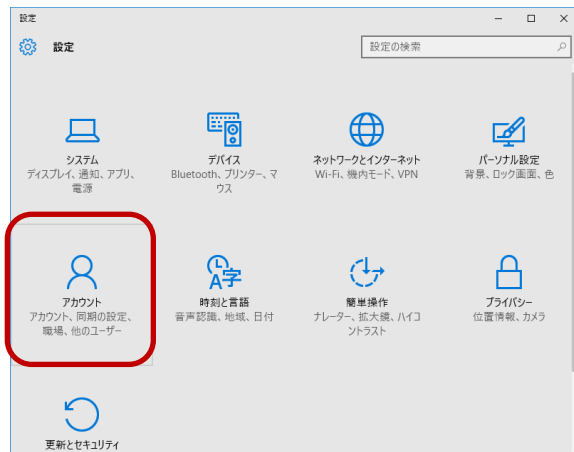
Windows スタートメニューの[設定]をクリックします。



3-1-2.

[アカウント]をクリックします。

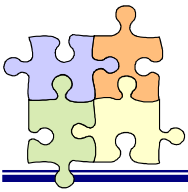
(Windows10 以外の OS では、Windows スタートメニューをクリックし、[コントロールパネル]-[ユーザーアカウント]より設定します。)



3-1-3.

[サインイン オプション]を選択し、[パスワード]の「追加」をクリックします。





3-2. OmniPassSE インストール

OmniPassSE のインストール・アンインストールについて説明します。

本製品を USB ポートに接続して OmniPassSE のインストールを行ってください。

OmniPassSE をインストールすることで本製品のドライバーも自動的にインストールされます。

■OmniPassSE のインストール

3-2-1.

製品付属 CD-ROM の OmniPass フォルダー内にある下記フォルダーに収録されているセットアッププログラム「SETUP.EXE」を起動します。

[OmniPass¥OP_x32] ⇒ 10/8.1/7 用 (32 ビット版)

[OmniPass¥OP_x64] ⇒ 10/8.1/7 用 (64 ビット版)

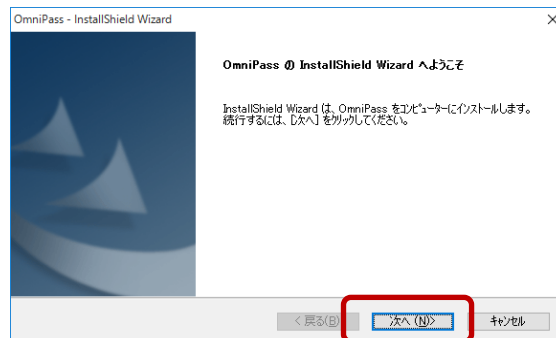
ユーザーアカウント制御の画面が表示される場合は、「はい」をクリックします。



OmniPassSE をインストールするユーザーはシステムに対して管理者権限を持っている必要があります。

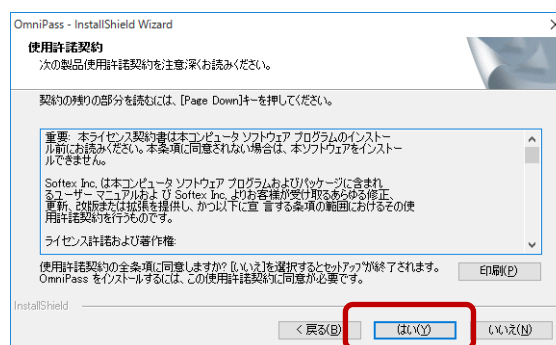
3-2-2.

「OmniPass セットアップへようこそ」の画面で「次へ(N)」をクリックします。



3-2-3.

使用許諾書の内容をご確認頂き、同意をいただいた上で「はい(Y)」をクリックします。

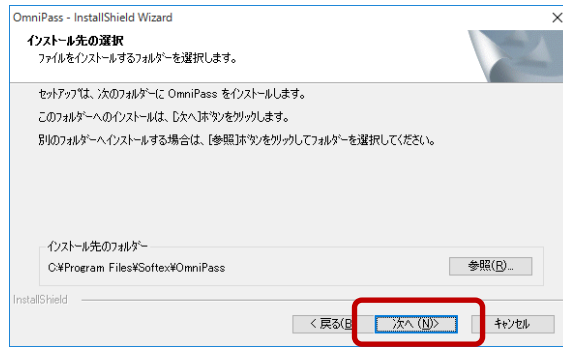


3-2-4.

インストール先の選択を行います。「次へ(N)」をクリックします。



ルートディレクトリ（例えば、C:\）にインストールしないでください。OmniPassSE をインストールしたディレクトリの下層でファイルやフォルダの暗号化はできません。



3-2-5.

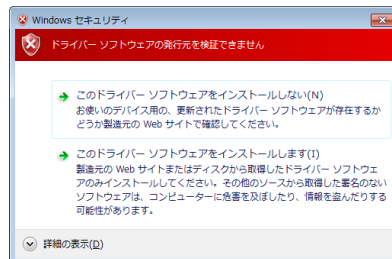
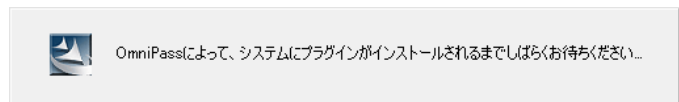
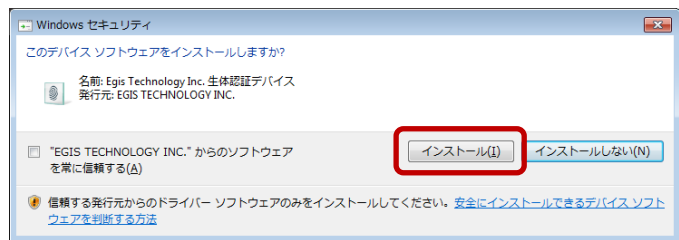
「このデバイスソフトウェアをインストールしますか?」と表示される場合は「インストール(I)」をクリックします。



Windows7 でのご注意

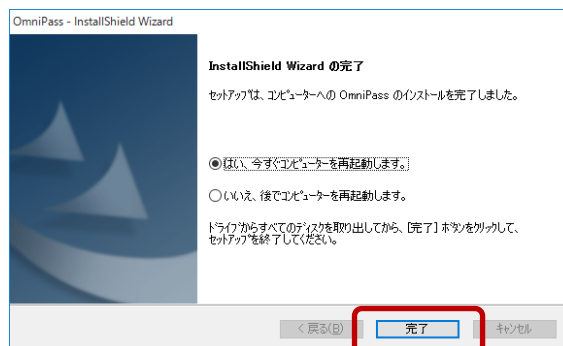
インストール中に「ドライバーソフトウェアの発行元を検証できません」と表示される場合は、Windows アップデートを行ってから、OmniPassSE を再セットアップしてください。

KB3033929(SHA-2 署名および検証機能のサポートを追加する更新プログラム)のインストールが必要です。



3-2-6.

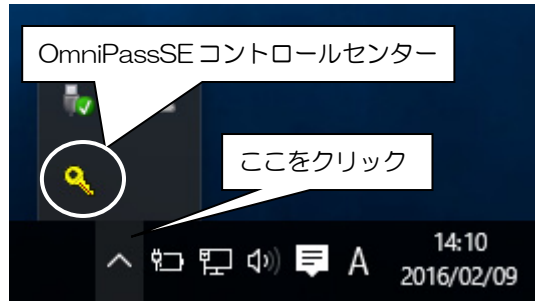
「はい、今すぐコンピューターを再起動します。」を選択し、「完了」をクリックします。



3-2-7.

再起動後、タスクバーに鍵マークの OmniPassSE コントロールセンターのアイコンが表示されます。

「3-3. OmniPassSE ユーザー登録」にある OmniPassSE 登録画面が自動的に表示されますので、登録を行います。



■OmniPassSE のアンインストール

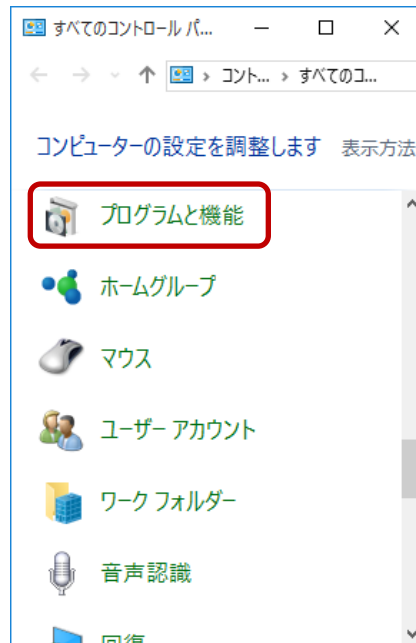


OmniPassSE のアンインストールを行うと、OmniPassSE で暗号化されたファイルは復号化することができなくなります。また、保存されたパスワードと情報は全て失われます。アンインストールを行う前に、必ず以下の操作を行ってください。

- (1) 全ての OmniPassSE 暗号化ファイルを復号化する。
- (2) OmniPassSE のユーザープロファイルをバックアップする。
- (3) 記憶させた Web およびアプリのアカウント・パスワード情報のメモを取っておく。

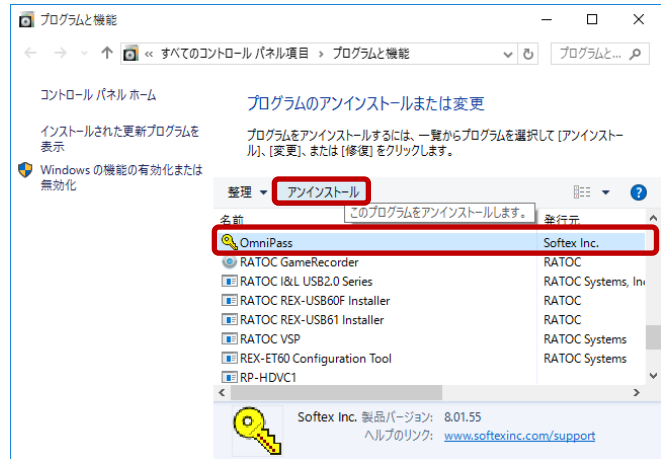
3-2-8.

[コントロールパネル]の「プログラムと機能」を開きます。



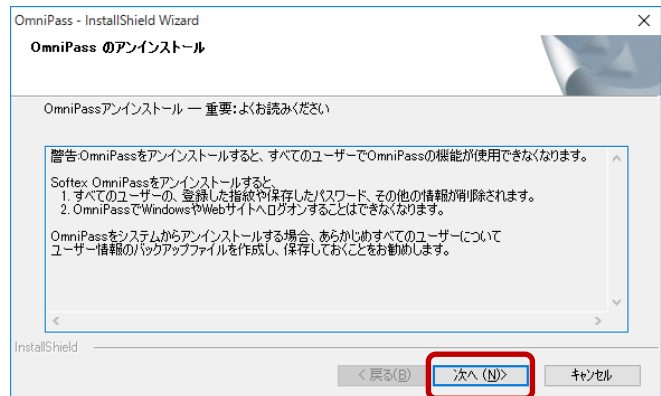
3-2-9.

インストールされたプログラムの一覧より「OmniPass」を選択し、「アンインストール」をクリックします。



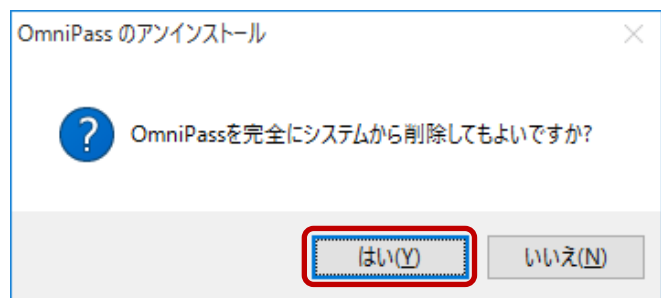
3-2-10.

アンインストール時の警告内容をご確認頂き、アンインストールする場合は「次へ(N)」をクリックします。



3-2-11.

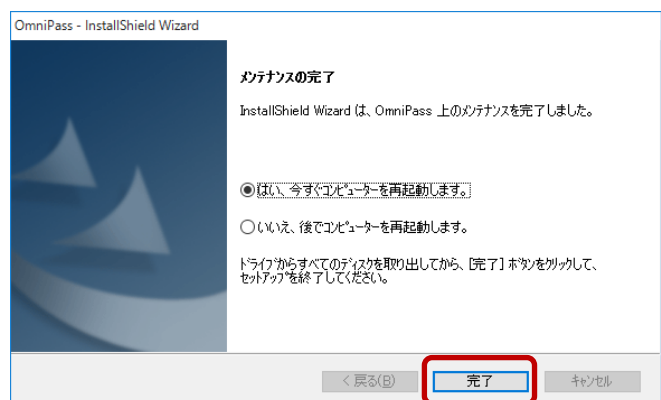
アンインストールの最後の確認です。実行する場合は「はい(Y)」をクリックします。

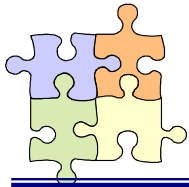


3-2-12.

アンインストールは完了です。「はい、今すぐコンピューターを再起動します。」を選択して、「完了」をクリックします。

以上の操作でアンインストール作業は完了です。





OmniPassSE ユーザー登録では Windows ログオン時のユーザー名とパスワードが必要になります。登録を行う前に、必ず Windows のログオンパスワードを作成してください。

■OmniPassSE ユーザー登録

3-3-1.

OmniPass 登録ウィザードから、「開始」ボタンをクリックします。



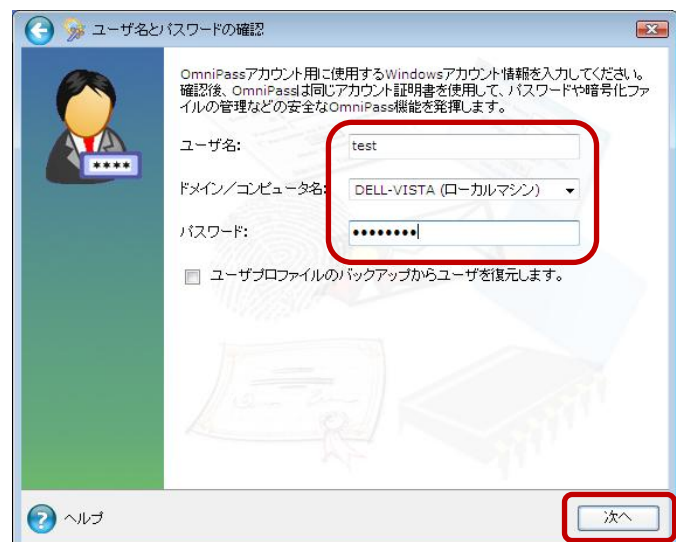
3-3-2.

[ユーザ名][ドメイン/コンピュータ名][パスワード]を入力して、「次へ」をクリックします。



Windows にログオンするときと同じユーザー名とパスワードを入力します。ドメインは通常、コンピュータ名になります。

企業環境などで、ドメインへログオンしている場合は[ドメイン/コンピュータ名]は、Windows のコンピュータ名ではありません。システム管理者にお問い合わせください。



3-3-3.

認証で使用する指をイラスト上で選択し、「次へ」をクリックします。



指の選択画面には「練習」ボタンがあります。クリックすると、指紋のキャプチャを練習できます。



3-3-4.

指紋の読み取りを開始します。画面の表示に従って指紋の読み取りを行います。指紋の読み取りは約 12 回行う必要があります。

読み取りが正常に行われた場合は、指紋画像が緑色で表示され、失敗した場合は、指紋画像が赤色で表示されます。



読み取った指紋との確認を行いますので、もう一度、同じ指の指紋の読み取りを行います。「選択した指が OmniPass に登録されました。」と表示されましたら、「次へ」をクリックします。

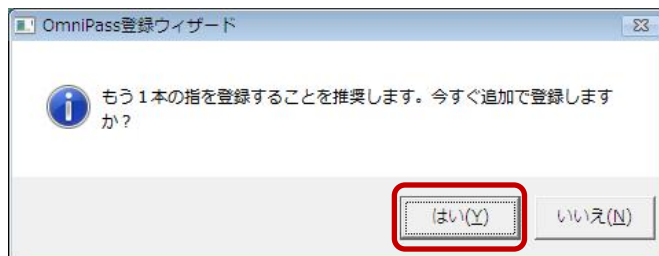
登録に失敗した場合は、画面左上の「←(戻る)」をクリックし、再登録を行います。



3-3-5.

「もう 1 本の指を登録することを推奨します。今すぐ追加で登録しますか?」というメッセージが表示されますので、他の指も登録する場合は「はい(Y)」をクリックします。

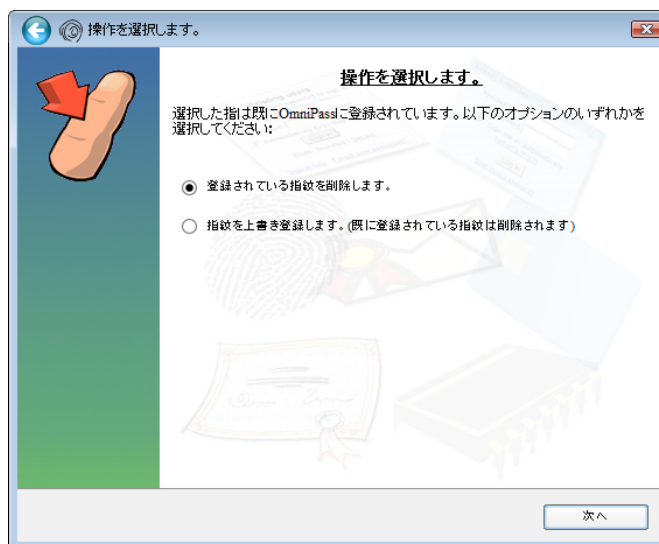
手順 3-3-3.の操作に戻り、異なる指で登録操作を繰り返します。



(登録済みの指を選択した場合)

登録済みの指紋情報を削除するか、上書き登録を行うかを選択することができます。

画面左上の「←(戻る)」をクリックすると登録指を選択する画面に戻ります。



3-3-6.

サウンドプロンプトの設定、タスクバーヒントの設定および認証ウィンドウの設定を行います。設定内容を確認して、「次へ」をクリックします。



OmniPassSE が各種の OmniPassSE イベントをユーザーに通知する方法を選択できます。OmniPassSE の操作方法に慣れるまで、初心者モードのタスクバーヒントおよびサウンドプロンプトをオンにすることをお勧めします。

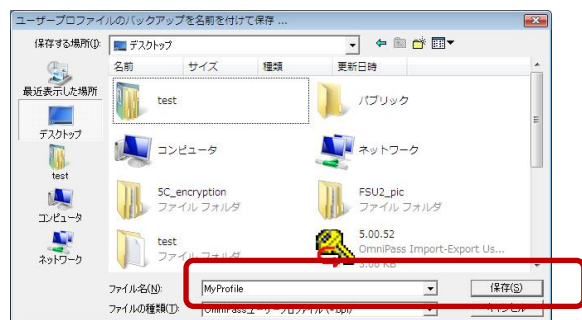
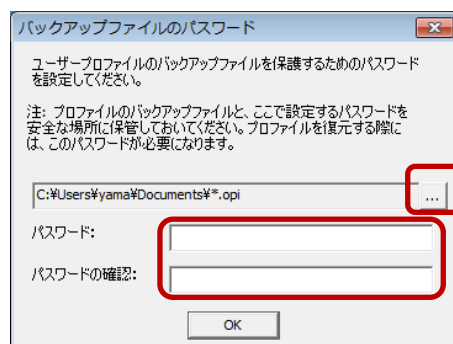


3-3-7.

作成したユーザープロファイルのバックアップファイルを保存します。「今すぐバックアップ」をクリックします。



バックアップファイルのパスワードを入力し、保存先を指定後に「OK」ボタンをクリックします。



3-3-8.

以上で OmniPassSE のユーザー登録作業は終了です。

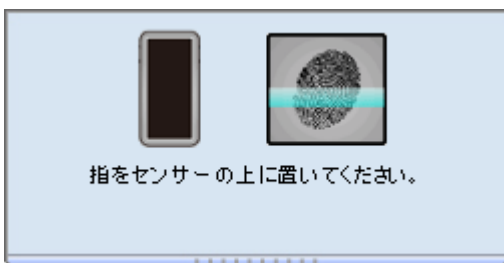
「完了」ボタンをクリックします。



■OmniPassSE 認証ダイアログ

Windows を再起動すると、従来の Windows のログオンでは表示されなかった OmniPassSE 認証ダイアログが表示されます。これは、OmniPassSE 認証システムが呼び出されると常に表示されます。OmniPassSE 認証システムは、以下の場合に呼び出されます。

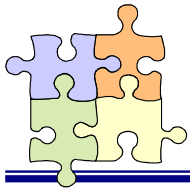
- (1) Windows のログオン時
- (2) OmniPassSE のログオン時
- (3) ワークステーションのロック解除時
- (4) スリープまたは休止状態からの復帰時 (OmniPassSE とは別に設定が必要です)
- (5) パスワード対応のスクリーンセーバーのロック解除時
- (6) パスワード等を OmniPassSE に記憶したサイトを開いた時
- (7) ファイルまたはフォルダーの暗号化・復号化実行時



OmniPassSE 認証ダイアログの プルダウンボタンをクリックすると、各指紋センサーと「マスターパスワードの認証」の選択バーが表示されます。

右図で各認証方法をクリックすると、選択した認証画面が表示されます。





4-1. アカウント情報の記憶

OmniPassSE アカウント情報の記憶を行うことにより、アカウント入力（ユーザ ID、パスワード）が必要な Web サイトに指紋認証により自動的にログオンすることができます。何種類ものパスワードを覚えておく必要はありません。



OmniPassSE8.01.xx が対応しているブラウザは Microsoft Internet Explorer 11.x です。

■Web ログオンパスワードの記憶

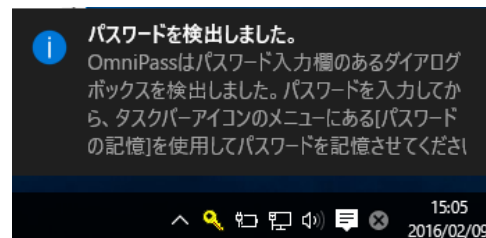
4-1-1.

アカウント入力を要求する Web サイトが開かれると、OmniPassSE はアカウント入力が要求されたことを自動検出し、「パスワードを検出しました。」というメッセージを表示します。

Google アカウント
メール:
パスワード:
 次回から入力を省略します。

[パスワードをお忘れの方](#)

Google アカウントをお持ちでない方は [こちらから今すぐアカウントを作成](#)



4-1-2.

アカウント情報（右の Web サイトでは、ユーザーのメールアドレスとパスワード）を入力した状態にします。



アカウント情報（ユーザーID、メールアドレス、パスワード等）にかな漢字コードを使用できない場合があります。

Google アカウント
メール:
パスワード:
 次回から入力を省略します。

[パスワードをお忘れの方](#)

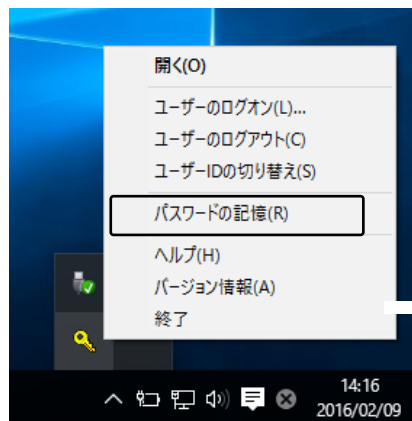
Google アカウントをお持ちでない方は [こちらから今すぐアカウントを作成](#)

ルズ

保護モード: 有効 100%

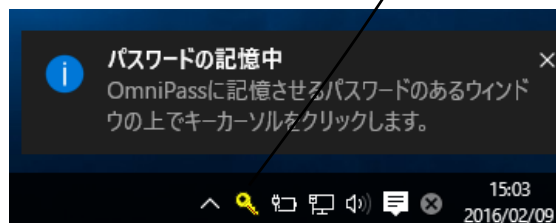
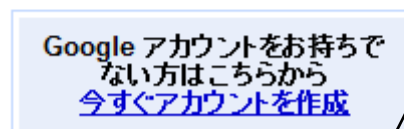
4-1-3.

タスクバーの OmniPassSE コントロールセンターを右クリックし、右クリックメニューより「パスワードの記憶 (R)」を選択します。



4-1-4.

「パスワードの記憶中」が表示された状態で、OmniPassSE キー（右図の鍵マーク）をログオンプロンプト（アカウント入力ダイアログ）の近くにドラッグします。

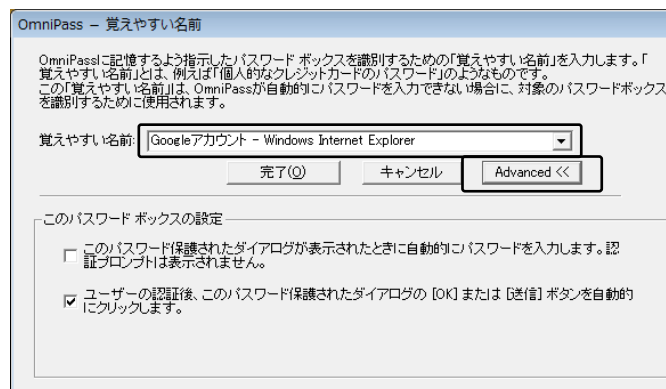


4-1-5.

OmniPassSE がアカウント情報を記憶すると、「覚えやすい名前」のダイアログが表示されます。「覚えやすい名前」を編集入力し、「完了(Q)」ボタンをクリックします。

OmniPassSE に記憶させたアカウント情報は「パスワードの管理」に保管されています。

「Advanced」をクリックするとパスワードの入力方法を設定することができます。



すでに OmniPassSE に記憶させた Web サイトに対して「パスワードの記憶」を再実行すると、OmniPassSE は現在記憶している Web サイトのアカウント情報（ユーザーID やパスワード）を上書き更新します。

例えば、アカウントページのパスワードを XXXXXX で、すでに OmniPassSE に記憶させていたとします。ところが、ある日、新しいパスワード：YYYYYY への更新案内が送られてきて、今後は新しいパスワード：YYYYYY でログオンしなければいけなくなったと仮定します。その場合、アカウントページにアクセスして、OmniPassSE にログオンさせる代わりに新しいパスワード：YYYYYY を入力します。その後「ログオン」をクリックしないで、パスワードの記憶を使用してカーソルを OmniPassSE キーに変え、ログオンプロンプトの近傍をクリックします。OmniPassSE は確認を要求し、続いてアカウント情報を上書きします。上記の操作により、OmniPassSE に記憶させたユーザーID は同じですが、パスワードは XXXXXX から YYYYYY へ更新されます。

■アプリケーションログオンパスワードの記憶

OmniPassSE はアカウント入力が必要とするホームページ以外に、「パスワードセットアップウィザード」の機能を使って、アカウント入力が必要とする Windows プログラムのアカウント情報も記憶することができます。

4-1-6.

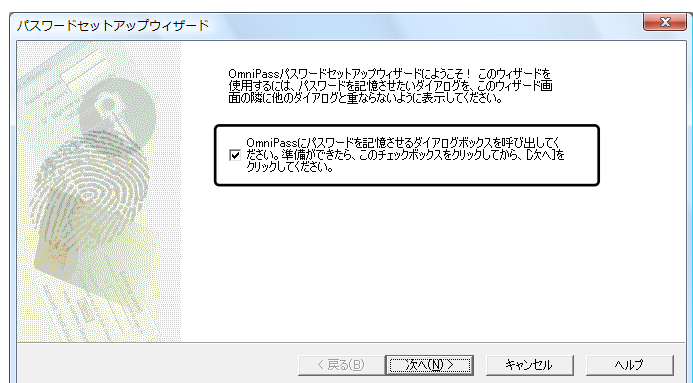
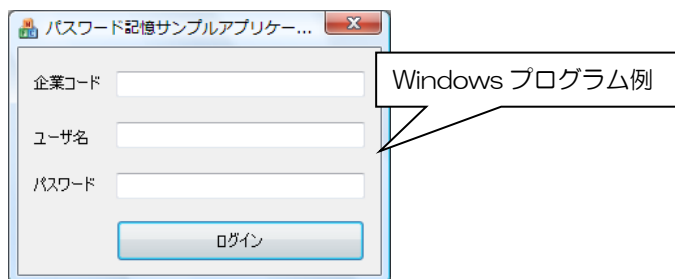
OmniPassSE コントロールセンターを起動し、[アクション]メニューより、「パスワードウィザード」を選択します。



4-1-7.

Windows プログラムのアカウント情報入力画面を「パスワードセットアップウィザード」の近くに表示させてから、

「OmniPass にパスワードを記憶させるダイアログボックスを呼び出してください。・・・」をチェックし、「次へ(N)」をクリックします。

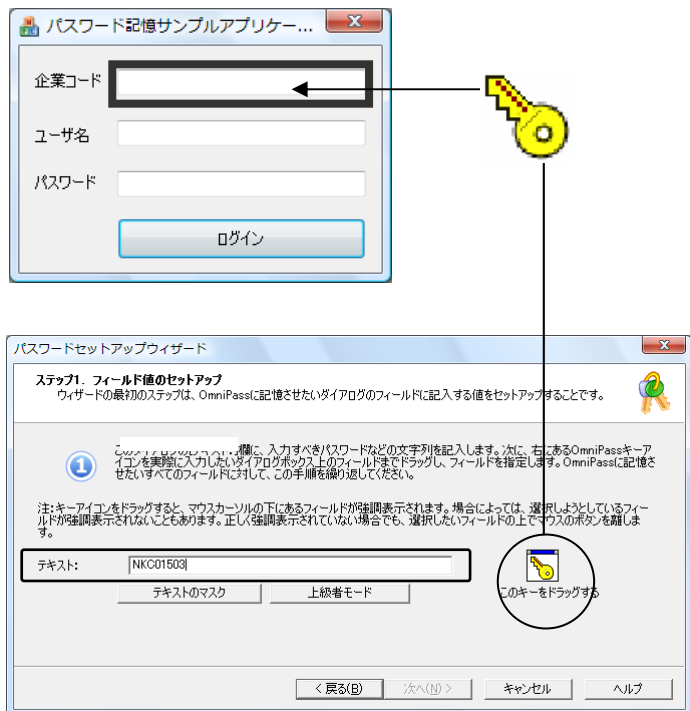


4-1-8.

パスワードセットアップウィザードの「テキスト」欄に適切なアカウントデータを入力し、「このキーをドラッグ」をドラッグし、Windows プログラムの該当入力欄の上へドロップします。右 Windows プログラムの例では、最初に企業コードのフィールド設定を行っています。



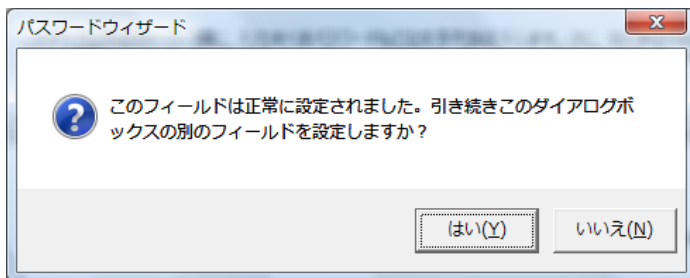
Windows プログラムの入力欄へ直接入力しないでください。



4-1-9.

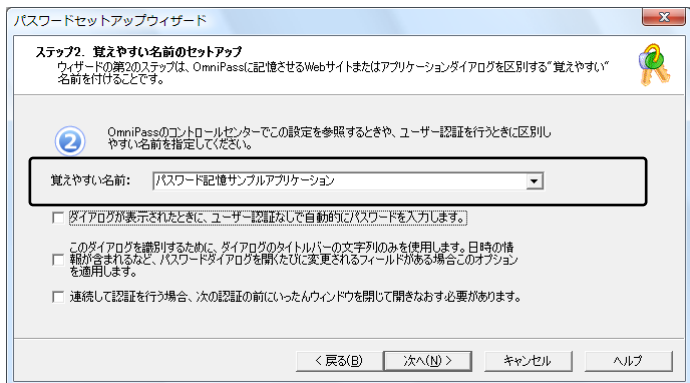
一つのフィールドの設定が終了すると右確認メッセージが表示されます。引き続きフィールド入力を行う場合は「はい (Y)」をクリックします。右の例では、企業コードの次に「ユーザ名」と「パスワード」の設定が必要です。

全ての入力が完了したら、「いいえ (N)」をクリックします。



4-1-10.

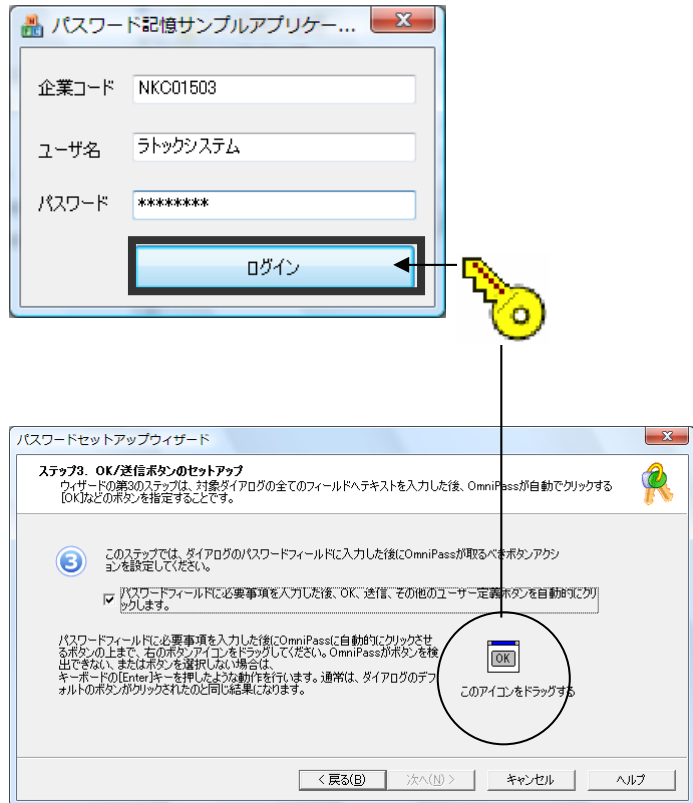
Windows プログラムの名前を「覚えやすい名前」に入力し、「次へ (N)」をクリックします。



4-1-11.

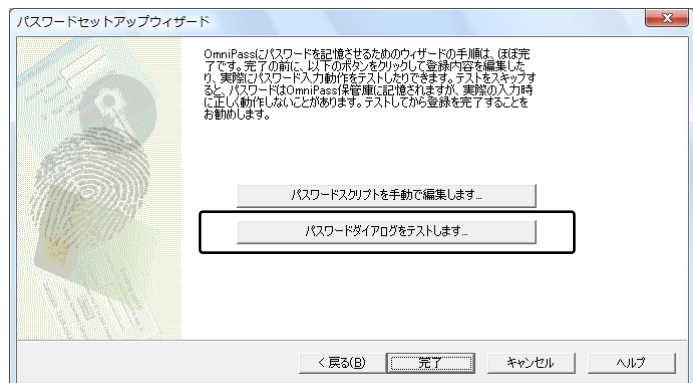
Windows プログラムで最後に操作するボタンを指定します。「このアイコンをドラッグ」をドラッグし、操作するボタンの上へドロップします。OmniPassSE への記憶操作は以上で終了です。

「次へ(N)」をクリックします。



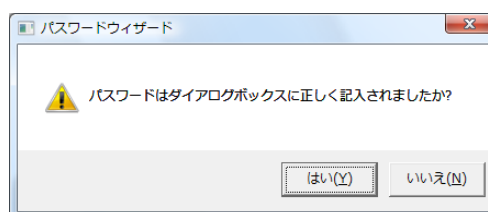
4-1-12.

「パスワードダイアログをテストします」をクリックします。



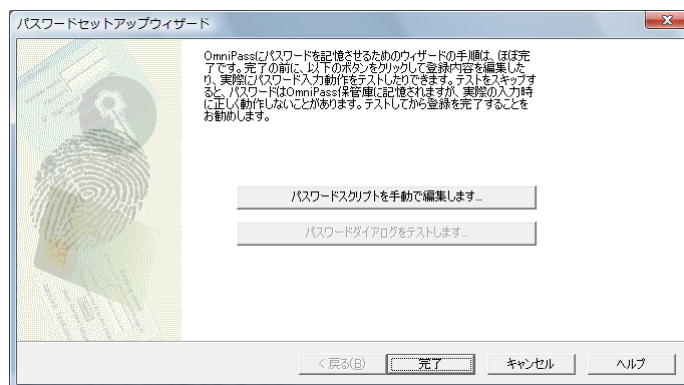
4-1-13.

テスト結果に問題がなければ、「はい(Y)」をクリックします。



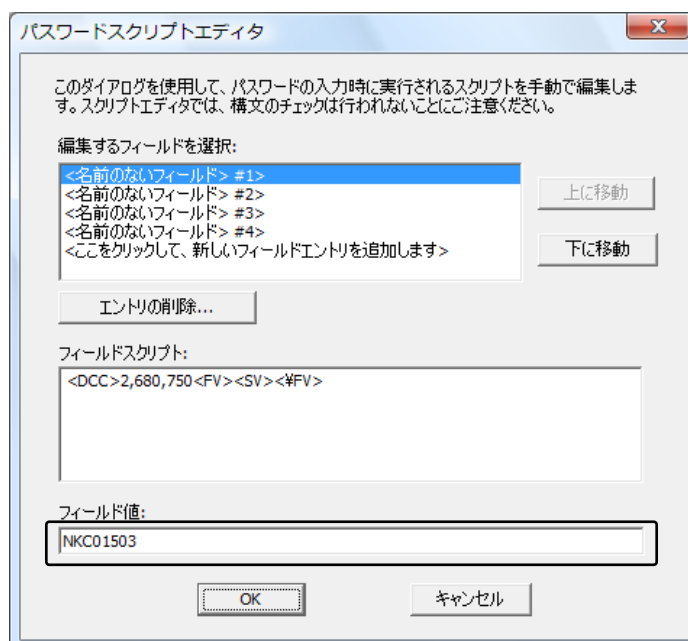
4-1-14.

最後に「完了」をクリックします。

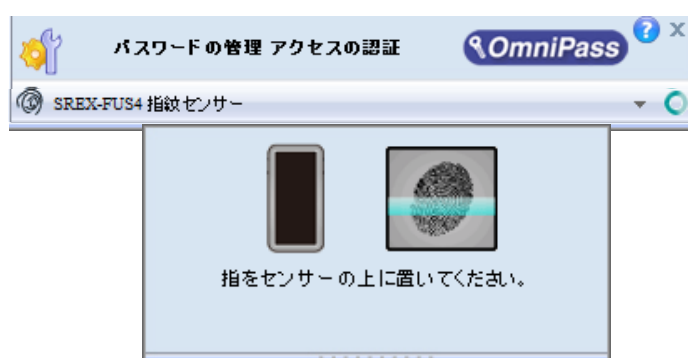


4-1-15.

手順 4-1-12 で「パスワードスクリプトを手動で編集します」をクリックすると、右スクリプト編集画面が表示されます。編集が必要な場合は、ここで編集することができます。



次回より、Windows プログラムのアカウント入力が表示されると、OmniPassSE 指紋認証ダイアログが表示されます。アカウント情報を入力する代わりに、OmniPassSE の指紋認証だけでログオンすることができます。

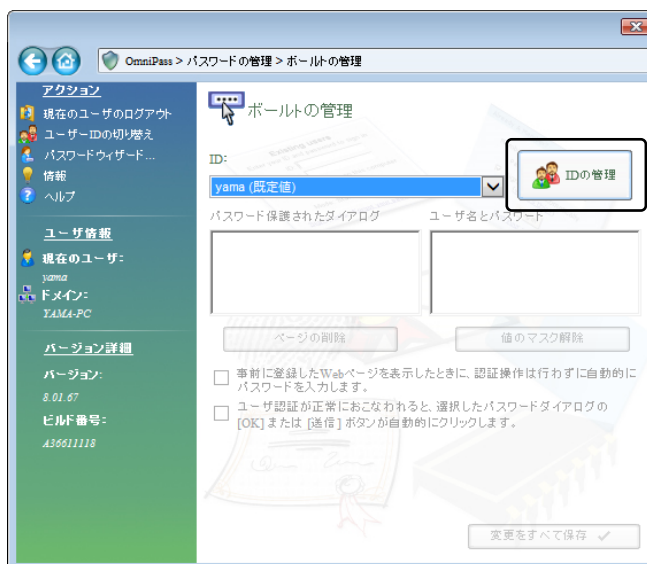


■IDの管理

一人の人が同一の Web サイトで複数のアカウントを取得している場合についても、OmniPassSE にアカウント情報を記憶させて OmniPassSE 指紋認証機能を使用することができます。複数のアカウントを管理する場合は、一人のユーザーに対して複数の ID を作成し、それぞれの ID に一つのアカウント情報を設定します。

4-1-16.

OmniPassSE コントロールセンターを起動し、「パスワードの管理」を選択し、「IDの管理」をクリックします。

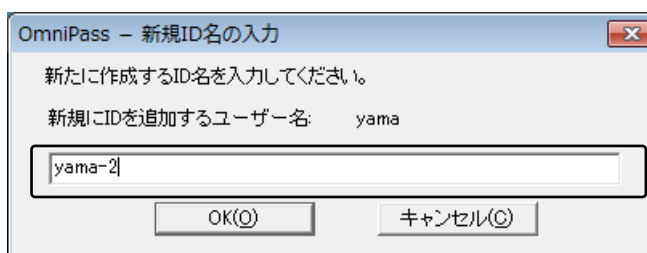


新しい ID を追加する場合は、「新規 ID」をクリックします。



4-1-17.

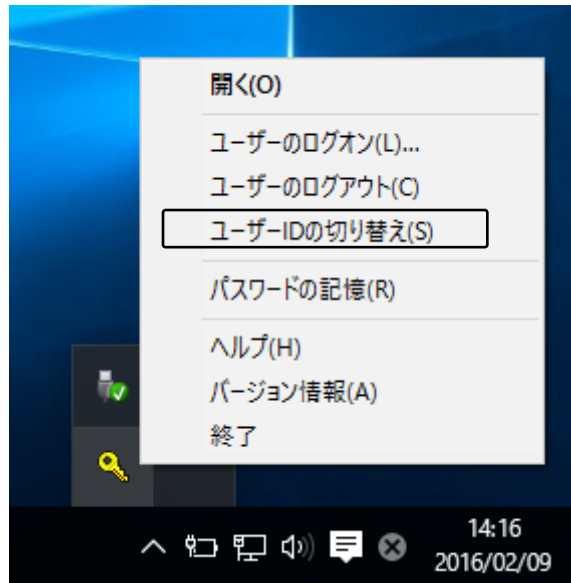
「ユーザー名に対する新規 ID」を入力し、「OK(O)」をクリックします。前項の画面で「変更をすべて保存」をクリックして設定は完了です。



4-1-18.

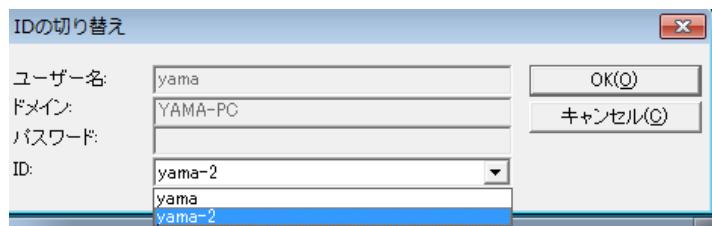
同一の Web サイトで複数のアカウント情報を記憶させる場合は、「ログオンパスワードの記憶」を行う前に「ユーザーID の切り替え(S)」を行い、ユーザーID ごとに一つのアカウントを記憶させます。

ユーザーID の変更は、タスクバーの「OmniPassSE コントロールセンター」を右クリックし、「ユーザーID の切り替え(S)」を選択します。



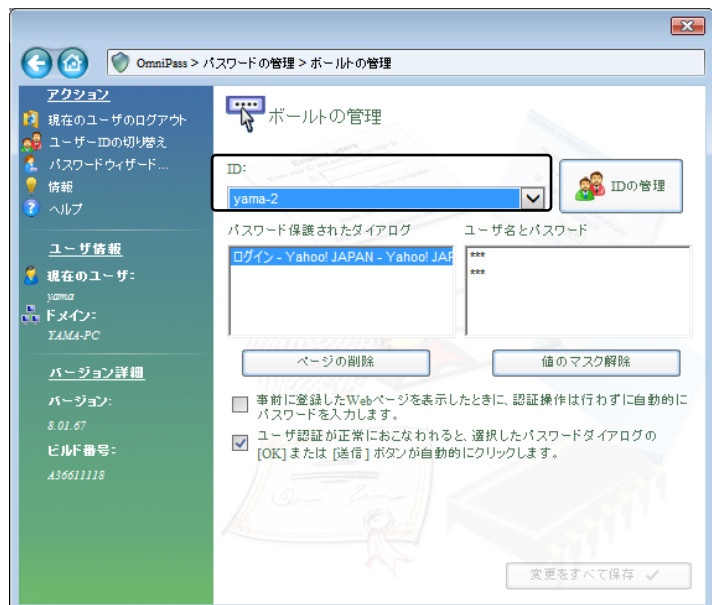
4-1-19.

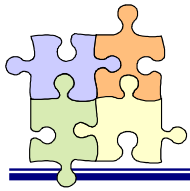
「ID の切り替え」ダイアログより、変更したい ID を選択します。ID 変更後、Web ログオンパスワードの記憶を実行します。



4-1-20.

各ユーザーID の「パスワード管理」は、OmniPassSE コントロールセンターの[パスワードの管理]-[ポールの管理]のページより行うことができます。画面上の「ID」を切り替えることにより、ID ごとに記憶されたパスワード情報等が表示されます。





OmniPassSE はフォルダー単位・ファイル単位での暗号化と復号化を行うことができます。

また、OmniPassSE 暗号化ファイルは複数の OmniPassSE 登録ユーザーと共有することができます。

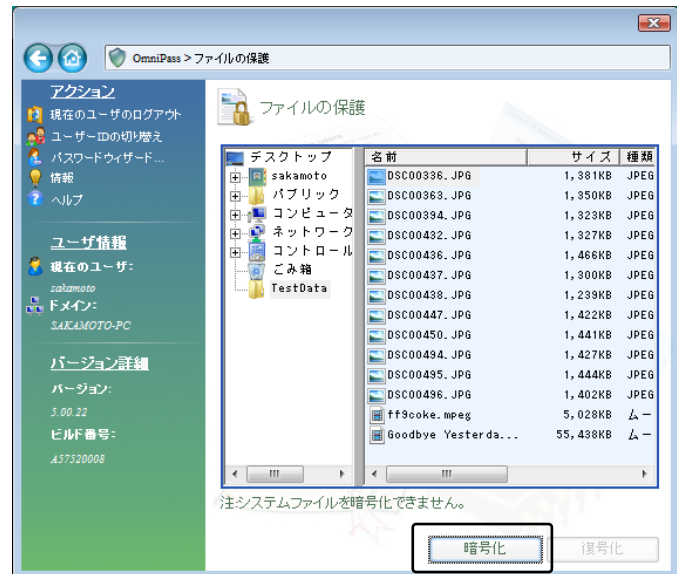
■暗号化

4-2-1.

OmniPassSE コントロールセンターを起動し、「ファイルの保護」を選択します。

暗号化を行うフォルダーもしくはファイルを選択し、「暗号化」をクリックします。

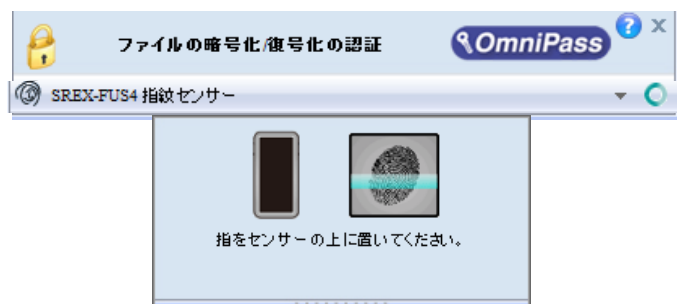
※ 64 ビット版 OS では OmniPassSE コントロールセンターにこの機能はありません。暗号化する場合は本項目の手順 4-2-6 をご参照ください。



“C:\Windows” に格納された Windows のシステムファイル、“C:\Program Files” にインストールされたプログラム、OmniPassSE がインストールされているフォルダーは、暗号化することができません。

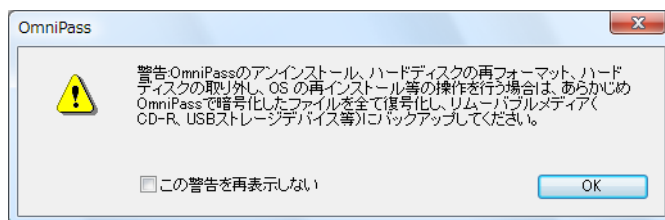
4-2-2.

暗号化のための認証を行います。



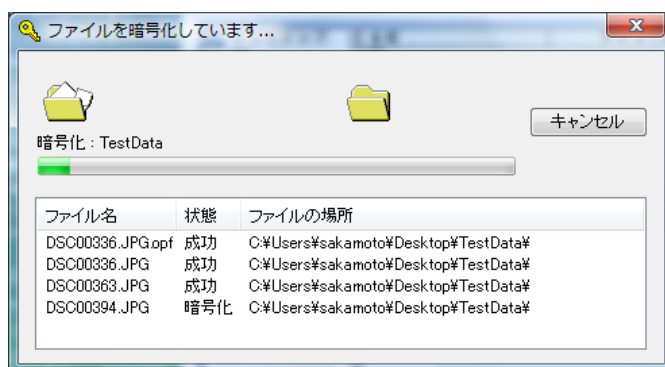
4-2-3.

暗号化を行うための認証が完了すると警告メッセージが表示されます。内容を確認して「OK」をクリックします。



4-2-4.

暗号化が行われます。



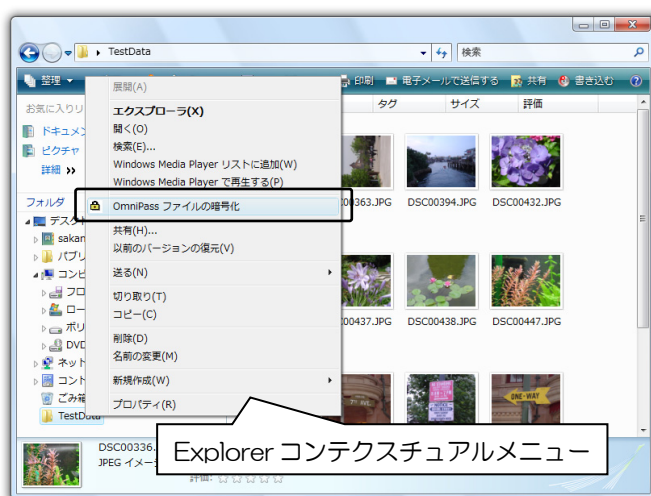
4-2-5.

暗号化を行ったフォルダーもしくはファイルは鍵の付いた新しいアイコンで表示されます。ファイルの拡張子は「.opf」、フォルダーの拡張子は「.opef」に変換されます。



4-2-6.

暗号化の操作は Windows Explorer から行うこともできます。マウスの右クリックでコンテキストメニューを表示し、「OmniPass SE ファイルの暗号化」を選択すると上記と同じ暗号化の操作を行うことができます。



■復号化

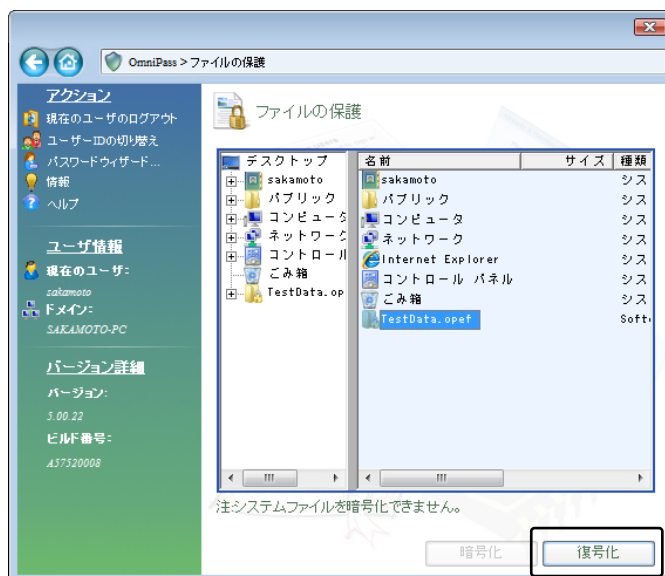
4-2-7.

OmniPassSE コントロールセンターを起動し、「ファイルの保護」のページを選択します。

復号化を行いたいフォルダーもしくはファイルを選択し、「復号化」をクリックします。

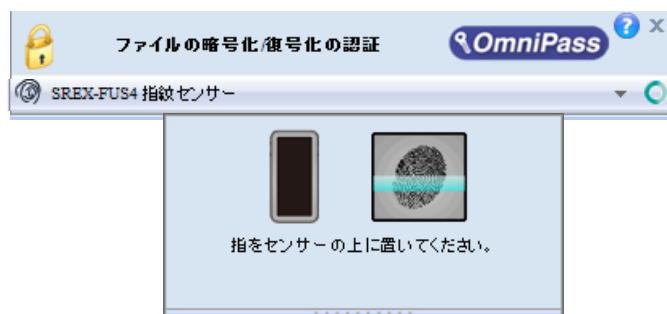
マウスの右クリックでコンテキストメニューを表示し、「OmniPassSE ファイルの復号化」を選択して、復号化の操作を行うこともできます。

※ 64 ビット版OSでは OmniPassSE コントロールセンターにこの機能はありません。復号化する場合は右クリックより行ってください。



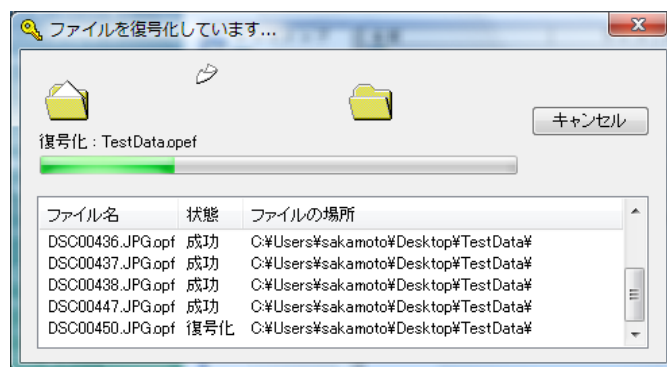
4-2-8.

復号化のための認証を行います。



4-2-9.

認証に成功すると自動的に復号化が行われます。



復号化を行う方法として、Explorer に表示された暗号化ファイル・暗号化フォルダーをマウスから直接ダブルクリックする方法があります。

フォルダーをダブルクリックすると暗号化フォルダーは一旦復号化されますが、フォルダー内の暗号化ファイルを編集し、フォルダーを閉じると暗号化された状態になります。

暗号化ファイルの場合、ダブルクリックで開くと復号化されます。

■暗号化ファイルの共有

4-2-10.

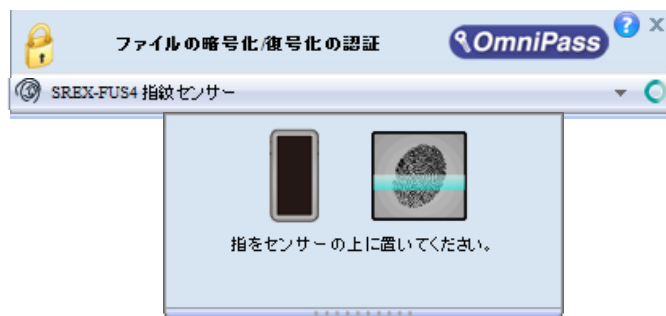
Windows Explorer からマウスの右クリックでメニューを表示し、

「OmniPassSE 暗号化ファイルの共有」を選択します。



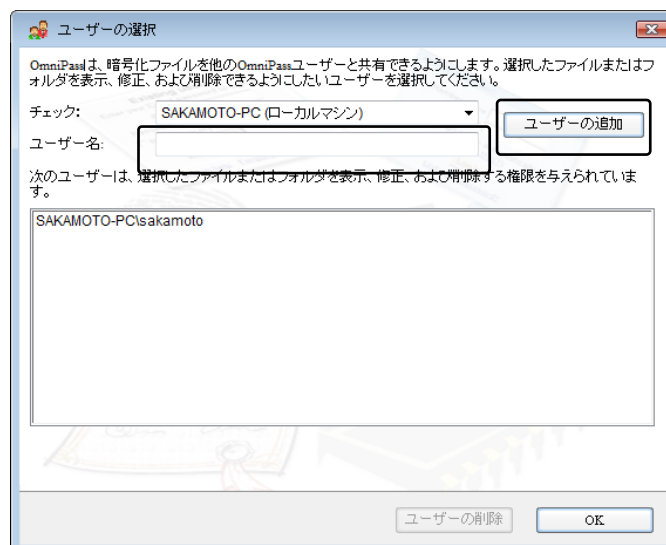
4-2-11.

暗号化ファイル共有のための認証を行います。



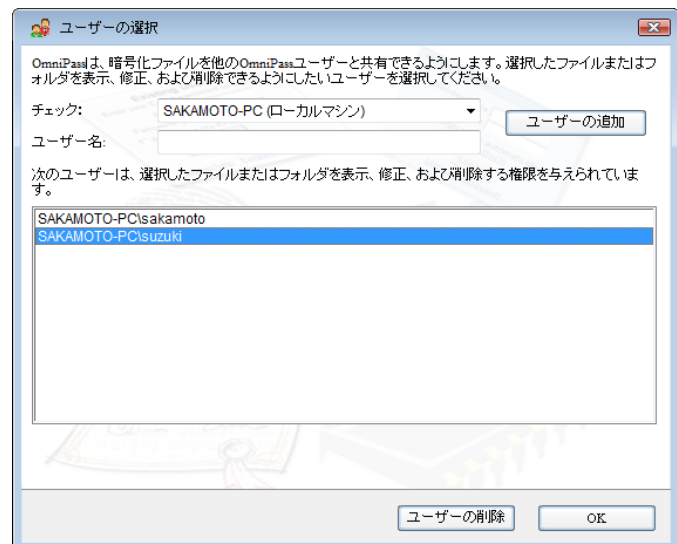
4-2-12.

暗号化ファイルの共有を行いたい
OmniPassSE に登録されたユーザー名
を入力し、「ユーザーの追加」のボタン
をクリックします。



4-2-13.

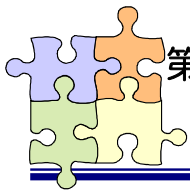
下部の一覧に共有化を許可するユーザーが追加されます。



OmniPassSE 暗号化ファイルやフォルダーを共有すると、共有するユーザーとの間で共有されたリソースを効果的に制御することができます。一旦共有の許可を行うと、許可されたユーザーはすべてのファイルのコピー・編集を行うことができ、更には OmniPassSE ユーザーのリストから全てのユーザーを排除することができます。許可を与えたユーザーが暗号化されたリソースの制御をできないようにすることも可能となりますので、注意してください。



ファイルの共有を許可されたユーザーが復号化の操作を行う場合は、ユーザーは OmniPassSE にログオンする必要があります。OmniPassSE にログオンしていない状態で、ファイルの復号化を行うことはできません。

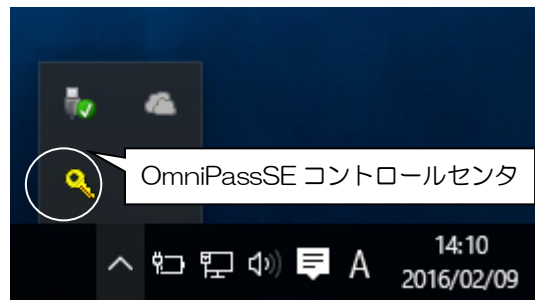


OmniPassSE ユーザーの追加ではユーザー名とパスワードが必要になります。ユーザーの追加を行う場合は、先に追加するユーザーの Windows ログオンパスワードを作成してください。

■ユーザーの追加

5-1-1.

タスクバーに格納された鍵マーク (OmniPassSE コントロールセンター) をダブルクリックします。



5-1-2.

「ユーザー管理ウィザードの実行」を選択します。



5-1-3.

次に「新規ユーザを OmniPass に追加」を選択します。

以降の操作は、「3-3.OmniPassSE ユーザー登録」で説明されている手順 3-3-2 から従ってユーザー登録を行います。



■ユーザーの削除

ユーザーを削除すると、そのユーザーに関連付けられた OmniPassSE データは自動的に破棄されます。また、そのユーザーが暗号化したファイルは復号化できなくなります。

削除を行う前に、必ず以下の操作を行ってください。

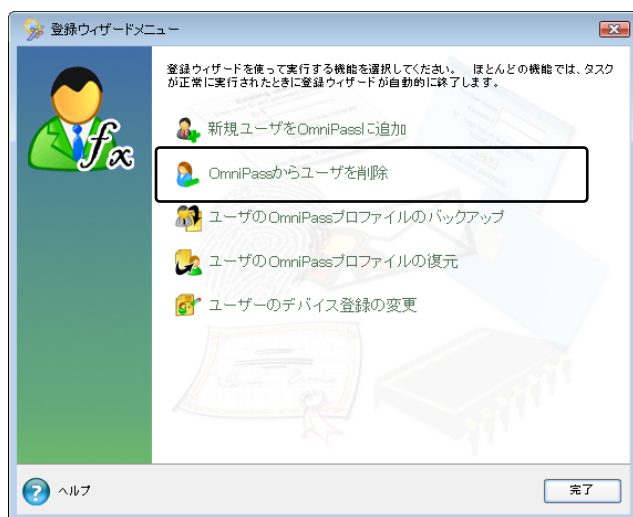


- (1) OmniPassSE ユーザープロファイルのバックアップを行う。
- (2) 全ての OmniPassSE 暗号化ファイル・フォルダーを復号化する。
- (3) 記憶させた Web およびアプリのアカウント・パスワード情報のメモを取っておく。

5-1-4.

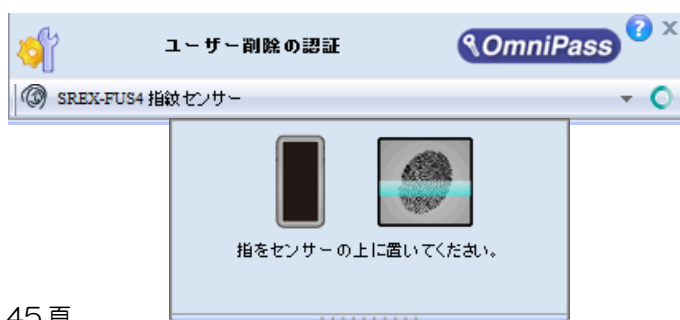
OmniPassSE コントロールセンターを起動し、「登録ウィザードの実行」を選択します。

右画面より「OmniPass からユーザを削除」をクリックします。



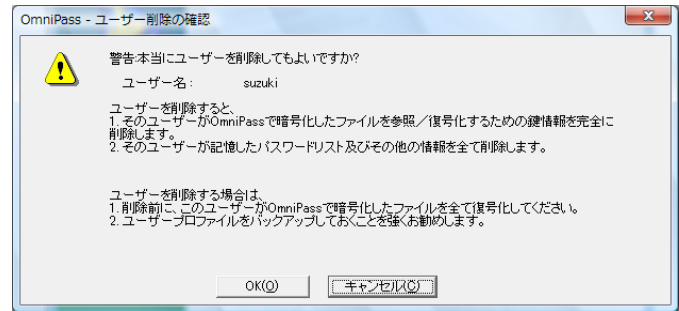
5-1-5.

削除を行うユーザーの指紋認証を行います。

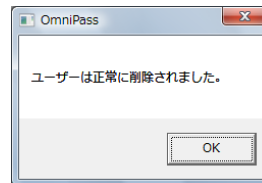


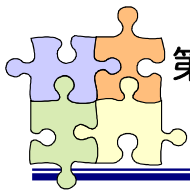
5-1-6.

削除されるユーザー名と警告の内容を確認して、事前に適切な処置を行った後、問題がなければ「OK(O)」をクリックします。



削除完了確認画面が表示されます。「OK」ボタンをクリックします。





5-2. アカウント情報の管理

「ログオンパスワードの記憶」で OmniPassSE に記憶させたパスワード情報をパスワードの管理で参照することができます。万が一、パスワードを忘れた場合にも確認できます。

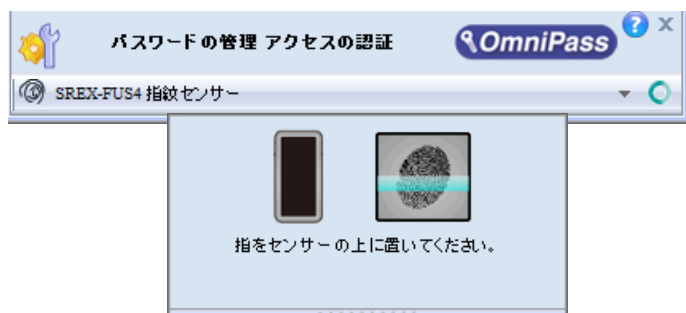
5-2-1.

OmniPassSE コントロールセンターを起動し、「パスワードの管理」を選択します。



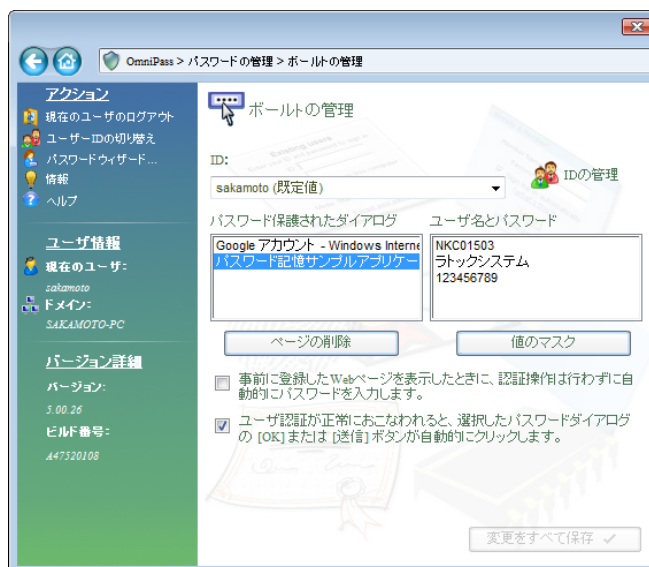
5-2-2.

「パスワードの管理」を開くためには、右の認証作業を行います。



5-2-3.

「ボルトの管理」頁が開きます。
「パスワード保護されたダイアログ」にOmniPassSEが記憶したWebサイトおよびWindowsプログラムの名前が表示されます。「ユーザー名とパスワード」に各サイトのアカウント情報が表示されます。「値のマスク解除」をクリックしてパスワードの内容を確認できます。
また、「ページの削除」をクリックして、記憶した情報を削除することができます。

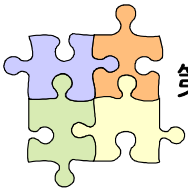


OmniPassSE による記憶されたサイトの処理方法には、下記の 3 つの設定があります。

- (1) 「事前に登録した Web ページを表示したときに、認証操作は行わずに自動的にパスワードを入力します。」
- (2) 「ユーザー認証が正常におこなわれると、選択したパスワードダイアログの「OK」または「送信」ボタンを自動的にクリックします。」
- (3) 上記のいずれにもチェックを入れない設定。

4-1. アカウント情報の記憶の手順 4-1-4 で設定した内容が表示されます。

- (1) の設定は、あまり安全ではありません。(1) の設定を有効にすると、このサイトに移動するたびに、OmniPassSE は認証を要求せずにサイトに自動的にログインします。
- (2) の設定にすると、OmniPassSE に記憶されたサイトを開くたびに、ユーザー認証が要求されます。認証に成功すると、このサイトに自動的にログインします。
- (3) の設定にすると、OmniPassSE に記憶されたサイトを開くたびに、ユーザー認証を要求します。認証に成功すると、サイトの入力位置へアカウント情報（ユーザ ID やパスワード）は自動的に記入されますが、サイトにログインするためには、Web サイトの OK、送信、またはログインボタンをクリックする必要があります。



5-3. プロファイルのバックアップと復元

ユーザープロファイルのバックアップにより、OmniPassSE に記憶させたサイトのアカウント情報をバックアップすることができます。OmniPassSE のアンインストールを行う前に、必ずユーザープロファイルのバックアップを行ってください。



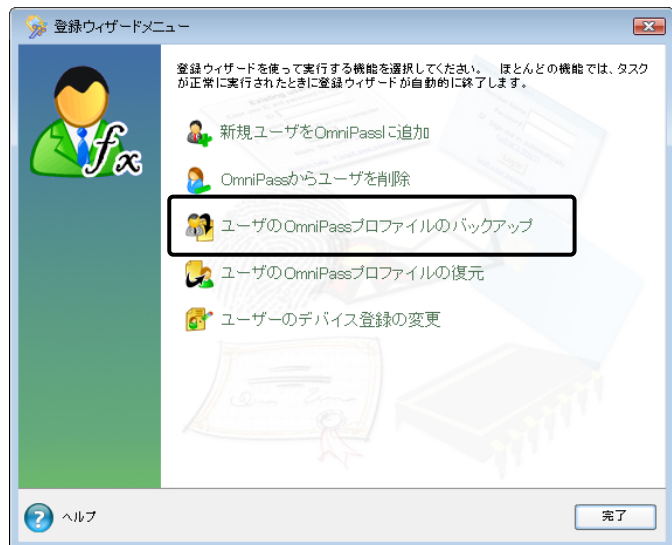
ユーザープロファイルのバックアップでは、「登録されている指紋データ」および「認証規則の設定(54頁 認証デバイスの必須設定)」は保存されません。

ユーザープロファイルを復元後に指紋認証を使用するには、指紋の再登録が必要です。

■ユーザープロファイルのバックアップ

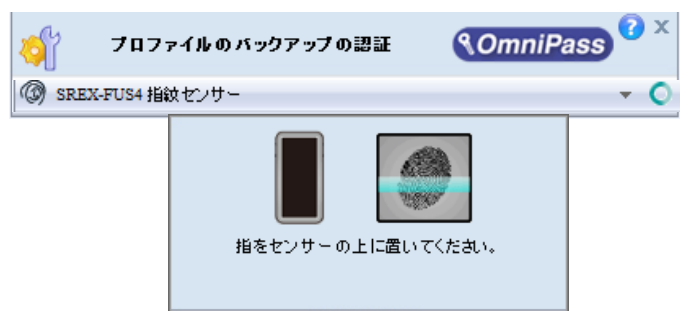
5-3-1.

OmniPassSE コントロールセンターを起動し、「ユーザー管理ウィザードの実行」を選択します。
右画面より「ユーザの OmniPass プロファイルのバックアップ」をクリックします。



5-3-2.

バックアップのための認証を行います。

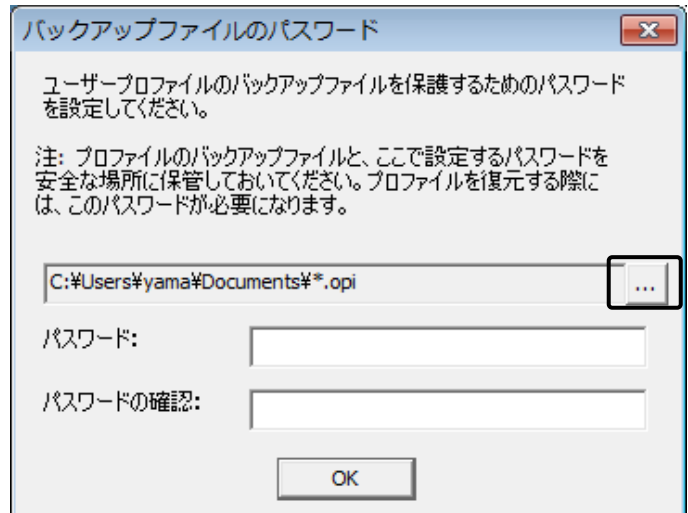


5-3-3.

バックアップファイルの保存先を選択しパスワードを設定します。

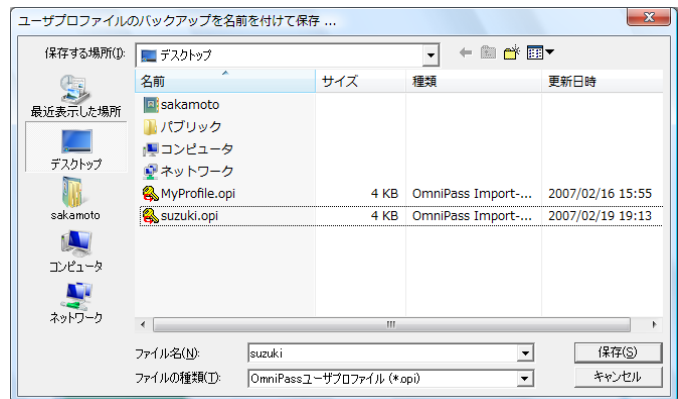


このパスワードは復元の際に使用しますので、必ず他の場所に記録しておくようにします。



5-3-4.

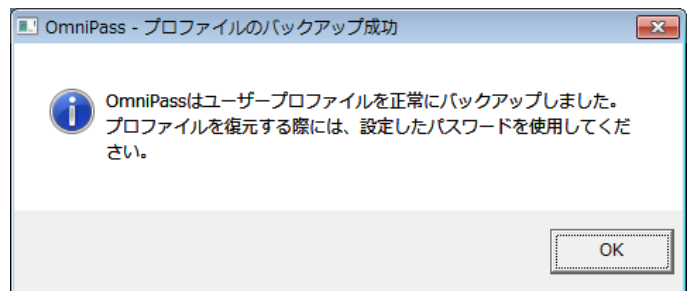
バックアップファイルの名前と保存先を指定します。



5-3-5.

「プロフィールのバックアップ成功」のメッセージが表示されます。「OK」をクリックします。

保存した場所に「xxx.opi」ファイルが作成されます。



■ユーザープロファイルの復元

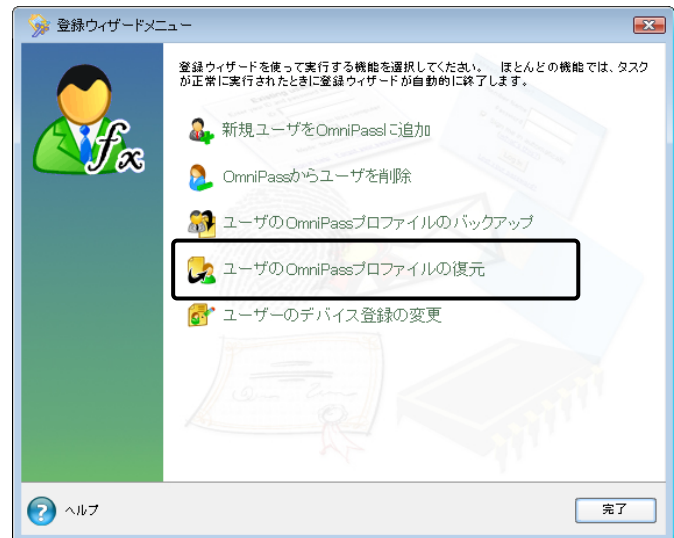
5-3-6.

OmniPassSE コントロールセンターを起動し、「登録ウィザードの実行」を選択します。

右画面より「ユーザの OmniPass プロファイルの復元」をクリックします。

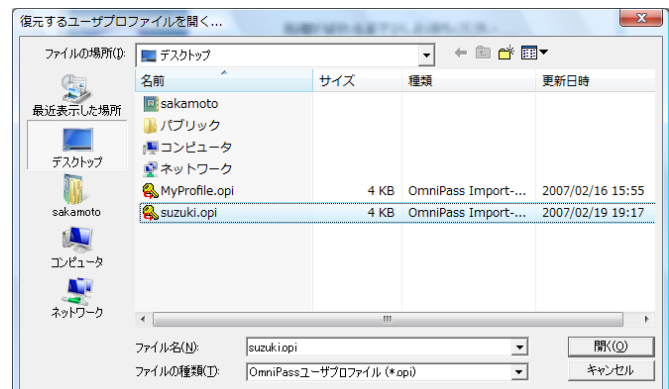


同じ名前のユーザーが既に登録されている場合、プロファイルを復元することはできません。



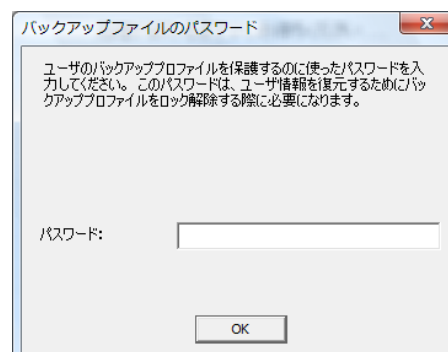
5-3-7.

復元したいユーザープロファイルが保存されている場所とファイル名を指定し、「開く(O)」をクリックします。



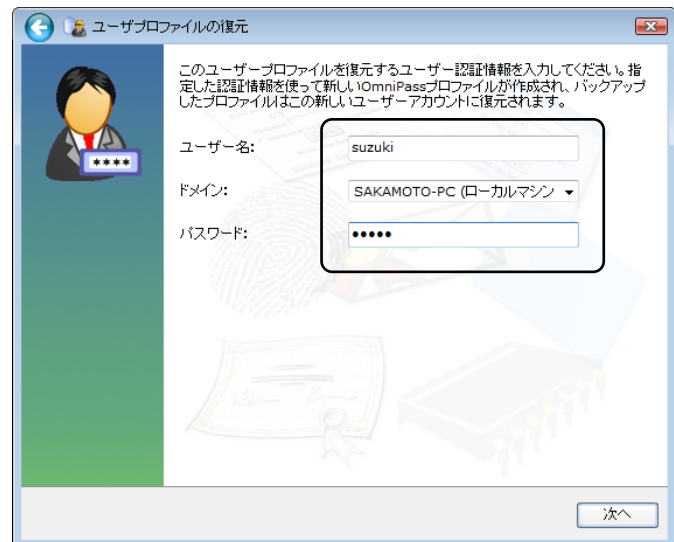
5-3-8.

ユーザープロファイルのバックアップを行ったときに設定したパスワードを入力し、「OK」をクリックします。



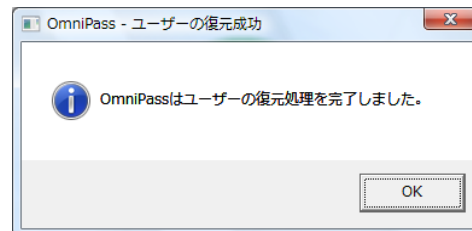
5-3-9.

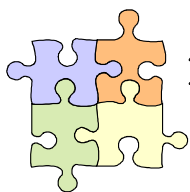
ユーザープロファイルのバックアップを行った時に使用していた「ユーザー名」・「ドメイン名」・「パスワード」を入力して「次へ」をクリックします。



5-3-10.

「ユーザーの復元処理完了」のメッセージが表示されます。
「OK」をクリックします。





OmniPassSE のその他の設定機能について説明します。

■ユーザーのデバイス登録の変更

「認証デバイスの登録」は、既に登録されたユーザーについて、別の指の指紋データも追加登録したい場合に使用します。将来、OmniPassSE で別の認証デバイスが追加サポートされた場合に、「認証デバイスの登録」よりそのデバイスを登録して、認証に使用することができます。

5-4-1.

OmniPassSE コントロールセンターを起動し、「登録ウィザードの実行」を選択します。

右画面より「ユーザーのデバイス登録の変更」をクリックします。

以後の操作は、「3-2.OmniPassSE ユーザー登録」の3-2-3からの手順と同じです。

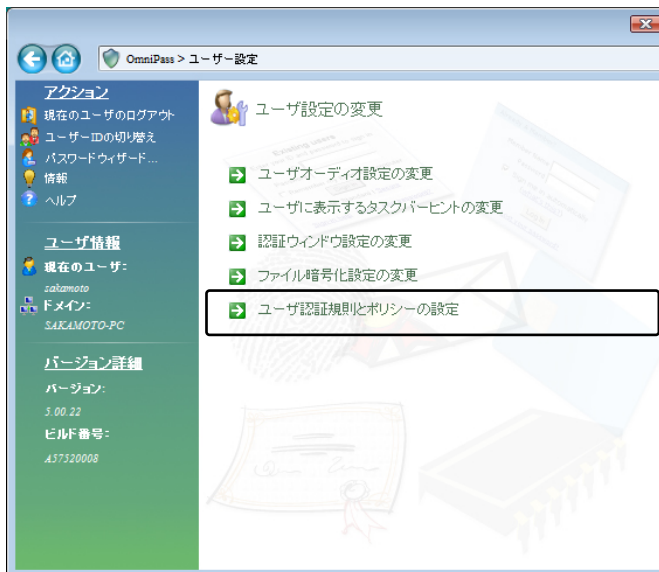


■ 認証デバイスの必須設定

5-4-2.

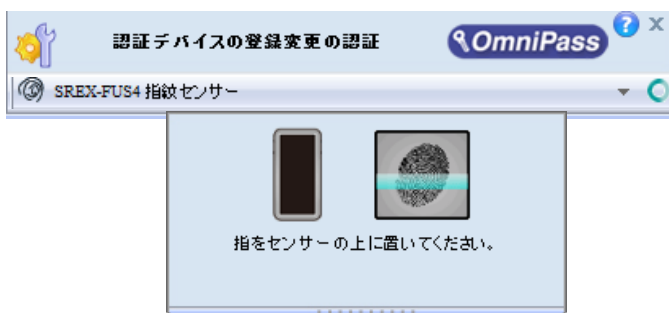
OmniPassSE コントロールセンターを起動し、「ユーザー設定の変更」を選択します。

右画面より「ユーザー認証規則とポリシーの設定」をクリックします。



5-4-3.

認証規則の設定のための認証を行います。

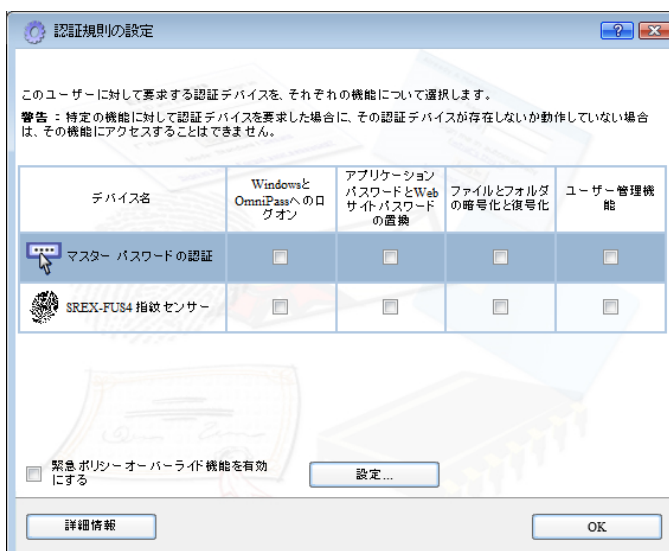


5-4-4.

認証デバイスの必須設定では、

- ① Windows と OmniPass へのログオン
- ② アプリケーションパスワードと Web サイトパスワードの置換
- ③ ファイルとフォルダの暗号化と復号化
- ④ ユーザー管理機能

を行う際に、それぞれの認証方式(指紋認証/パスワード認証)を必須とするか否かの設定を行うことができます。

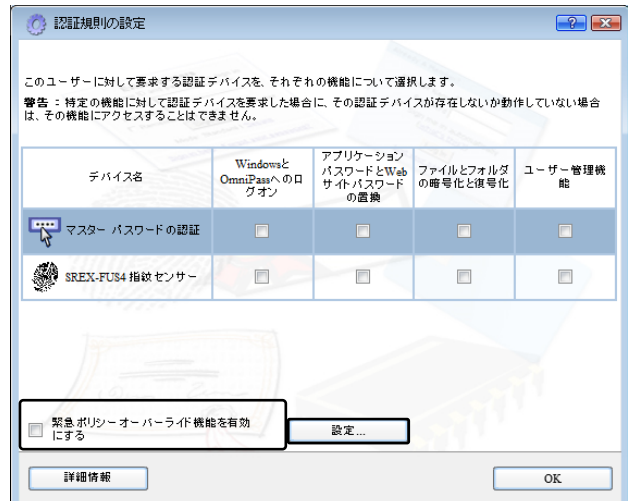


■緊急ポリシーオーバーライド機能を有効にする

「緊急ポリシーオーバーライド機能を有効にする」にチェックを入れると、認証が必要な操作で認証できない場合に、設定した回答を入力することで認証作業を回避することができます。

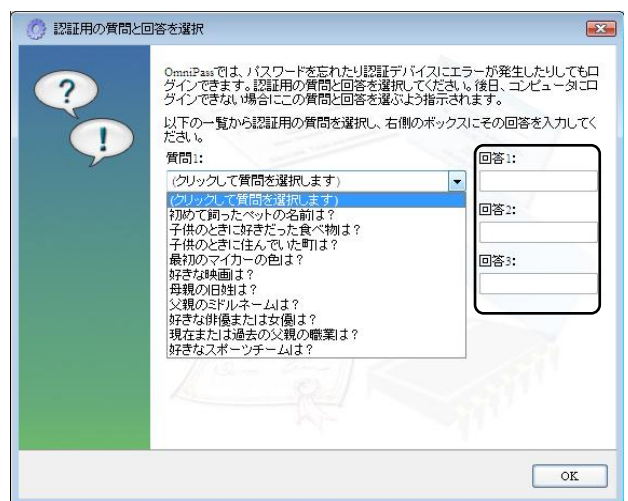
設定方法は以下の通りとなります。

「認証規則の設定」ダイアログで「設定」ボタンをクリックします。



「認証用の質問と回答を選択」ダイアログが出力されますので、質問 1~3 を選択し、回答 1~3 に回答を入力します。

「OK」ボタンをクリックします。



使用方法は以下の通りとなります。

認証画面の「ログインできません」をクリックします。



「緊急ポリシーオーバーライド」ダイアログが出力されますので、ユーザー名とドメイン名を入力し「OK」ボタンをクリックします。



設定した回答 1~3 を入力し「OK」ボタンをクリックします。

認証用の質問と回答を選択

OmniPassでは、パスワードを忘れたり認証デバイスにエラーが発生したりしてもログインできます。以前に設定した認証用の質問の回答を入力してください。

質問の右側にあるボックスに以下の質問の回答を入力してください。

質問1:	初めて飼ったペットの名前は？	回答1:	
質問2:	子供のときに好きだった食べ物？	回答2:	
質問3:	子供のときに住んでいた町は？	回答3:	

OK

■OmniPassSE へのログオン設定

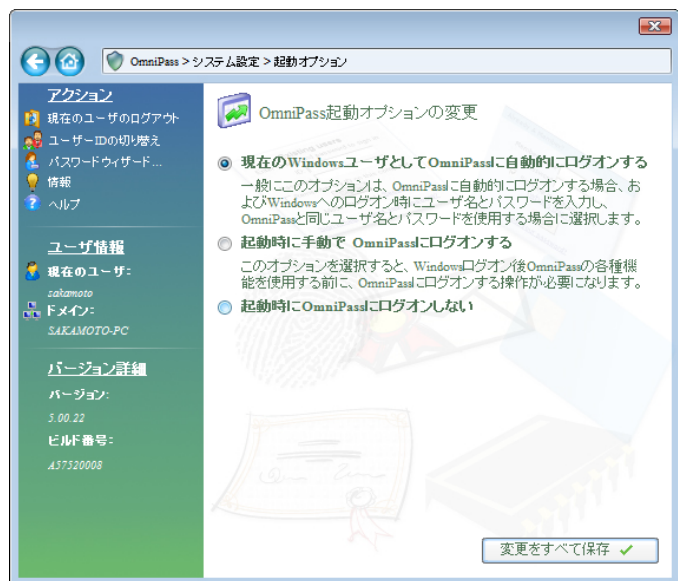
Windows ログオンユーザーが OmniPassSE の機能を使用するためには、OmniPassSE へログオンする必要があります。

OmniPassSE コントロールセンターを起動します。右画面より、「システム設定の変更」メニューを選択し「OmniPass 起動オプションの変更」をクリックします。



「起動オプション」より3種類の OmniPassSE へのログオン方法を選択することができます。

- (1) 現在の Windows ユーザーとして OmniPass に自動的にログオンする (デフォルト値)
- (2) 起動時に手動で OmniPass にログオンする
- (3) 起動時に OmniPass にログオンしない

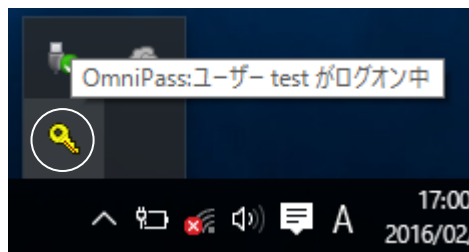


(1) の設定が選択されていると、Windows にログオンした後、Windows 起動後に OmniPassSE に自動的にログオンします。

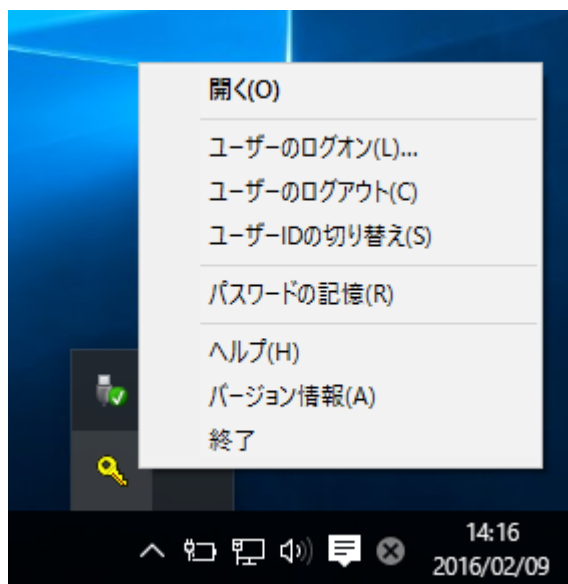
(2) の設定が選択されていると、OmniPassSE は Windows 起動後にユーザーに OmniPassSE にログオンするように要求します。

(3) の設定が選択されていると、OmniPassSE はユーザーに OmniPassSE にログオンするように要求しません。

タスクバーに登録された鍵マークの OmniPassSE 上にカーソルを移動することにより、現在 OmniPassSE にログオンしているユーザー名を確認することができます。

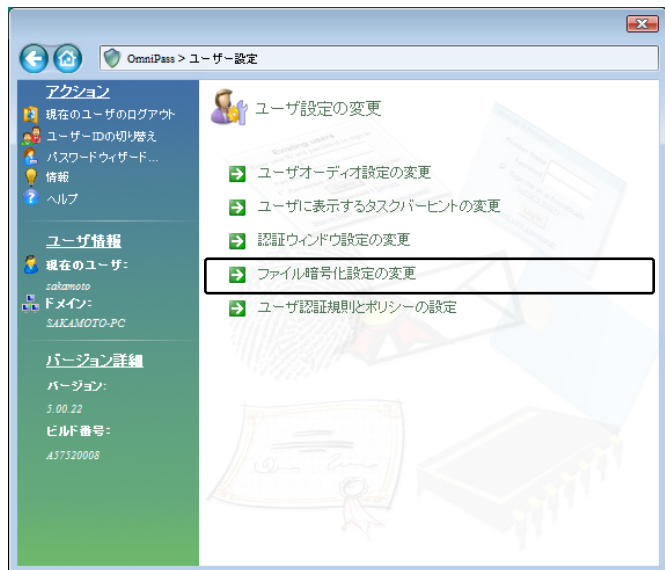


同様にマウス右クリックより、「ユーザーのログオン(L)」もしくは「現在のユーザーのログアウト(C)」を選択することにより、Windows を起動したまま OmniPassSE ログオンユーザーを切り替えることができます。

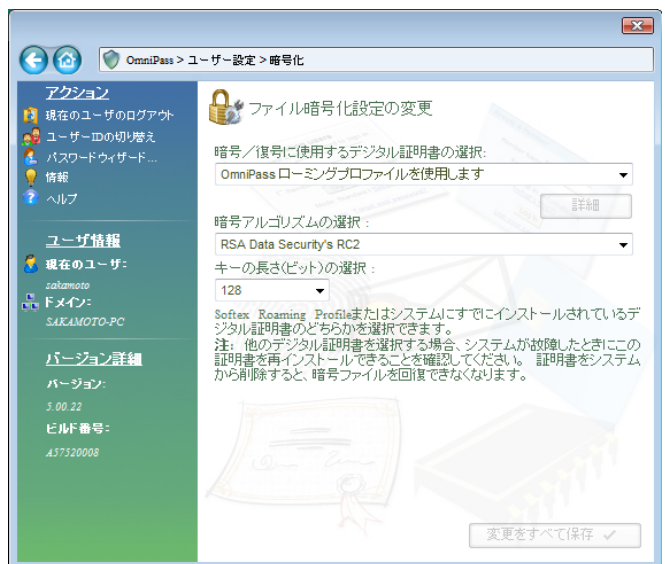


■暗号化／復号化の設定

OmniPassSE コントロールセンターを起動し、「ユーザー設定の変更」を選択します。右画面より「ファイル暗号化設定の変更」をクリックします。

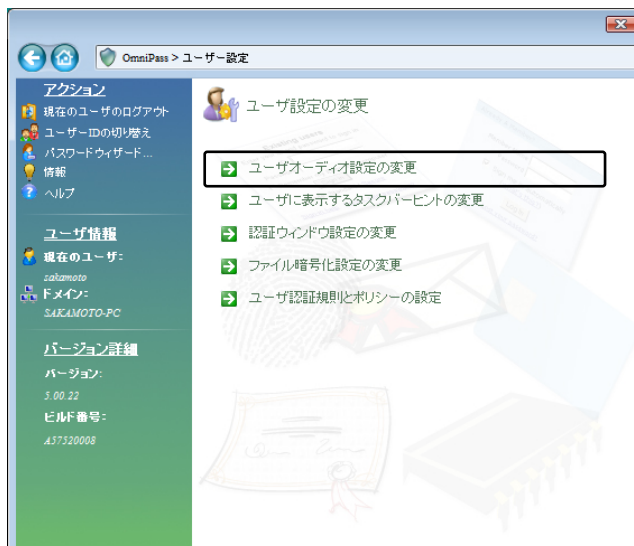


「アルゴリズムの選択」から、
➤RSA Data Security's RC2
➤RSA Data Security's RC4
➤Data Encryption Standard (DES)
➤Two Key Triple DES
➤Three Key Triple DES
を選択することができます。上から下の順で暗号化セキュリティの信頼性は高くなりますが、暗号化・復号化に要する時間は長くなります。



■サウンドの設定

OmniPassSE コントロールセンターを起動し、「ユーザー設定の変更」を選択します。
右画面より「ユーザーオーディオ設定の変更」をクリックします。

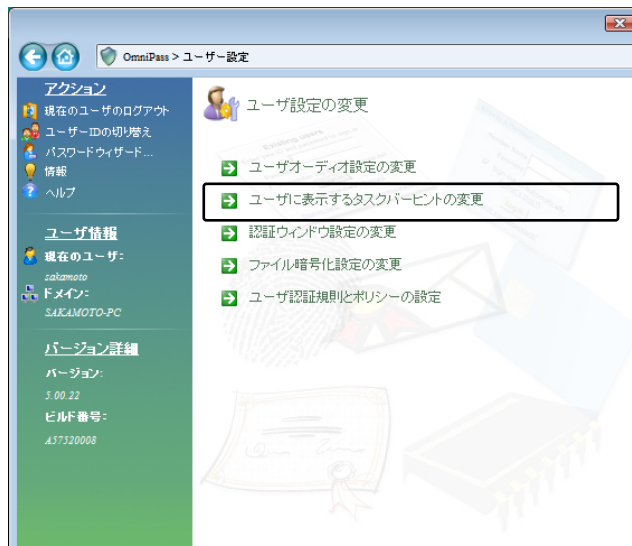


OmniPassSE のイベント（例えば、ログオン認証に成功した時、認証が拒否されたときなど）をサウンドでユーザーに通知する方法を設定できます。

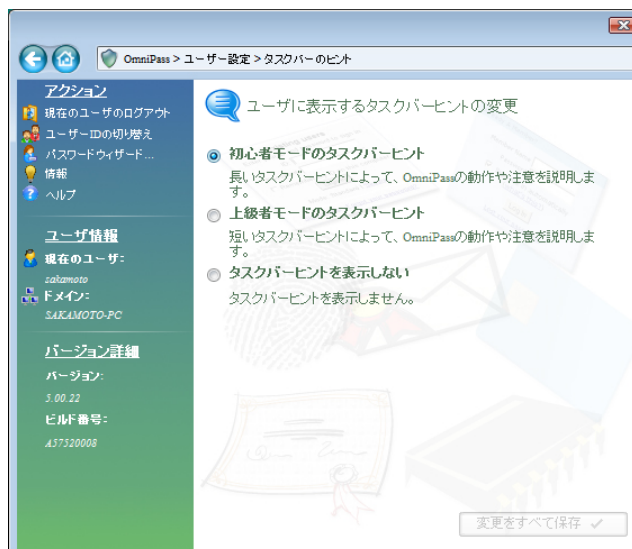


■タスクバーヒントの設定

OmniPassSE コントロールセンターを起動し、「ユーザー設定の変更」を選択します。
右画面より「ユーザに表示するタスクバーヒントの変更」をクリックします。

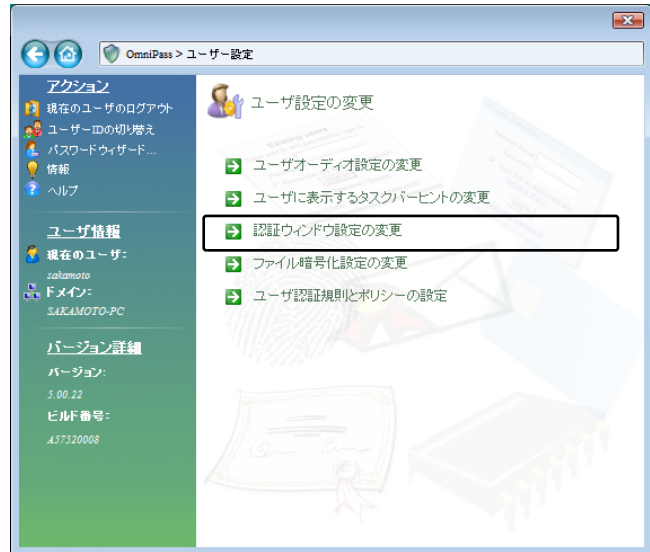


タスクバーのヒントを表示するという設定にしていれば、OmniPassSE は「パスワードを記憶」できるタイミングを常に通知しますので、ユーザーにログオンを要求する任意の認証イベントを記憶することができます。

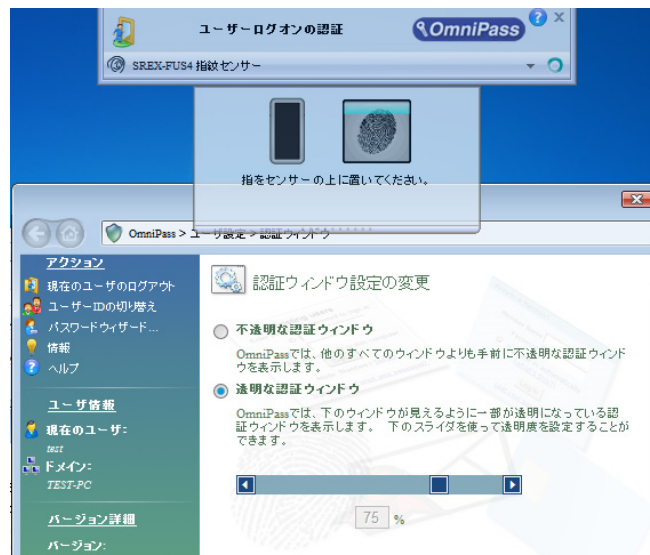


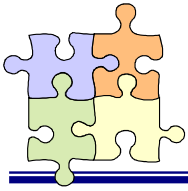
■ 認証ウィンドウの設定

OmniPassSE コントロールセンターを起動し、「ユーザー設定の変更」を選択します。
右画面より「認証ウィンドウ設定の変更」をクリックします。



「透明な認証ウィンドウ」を選択すると、認証画面の透明度を設定することができます。





6-1. アプリケーション API

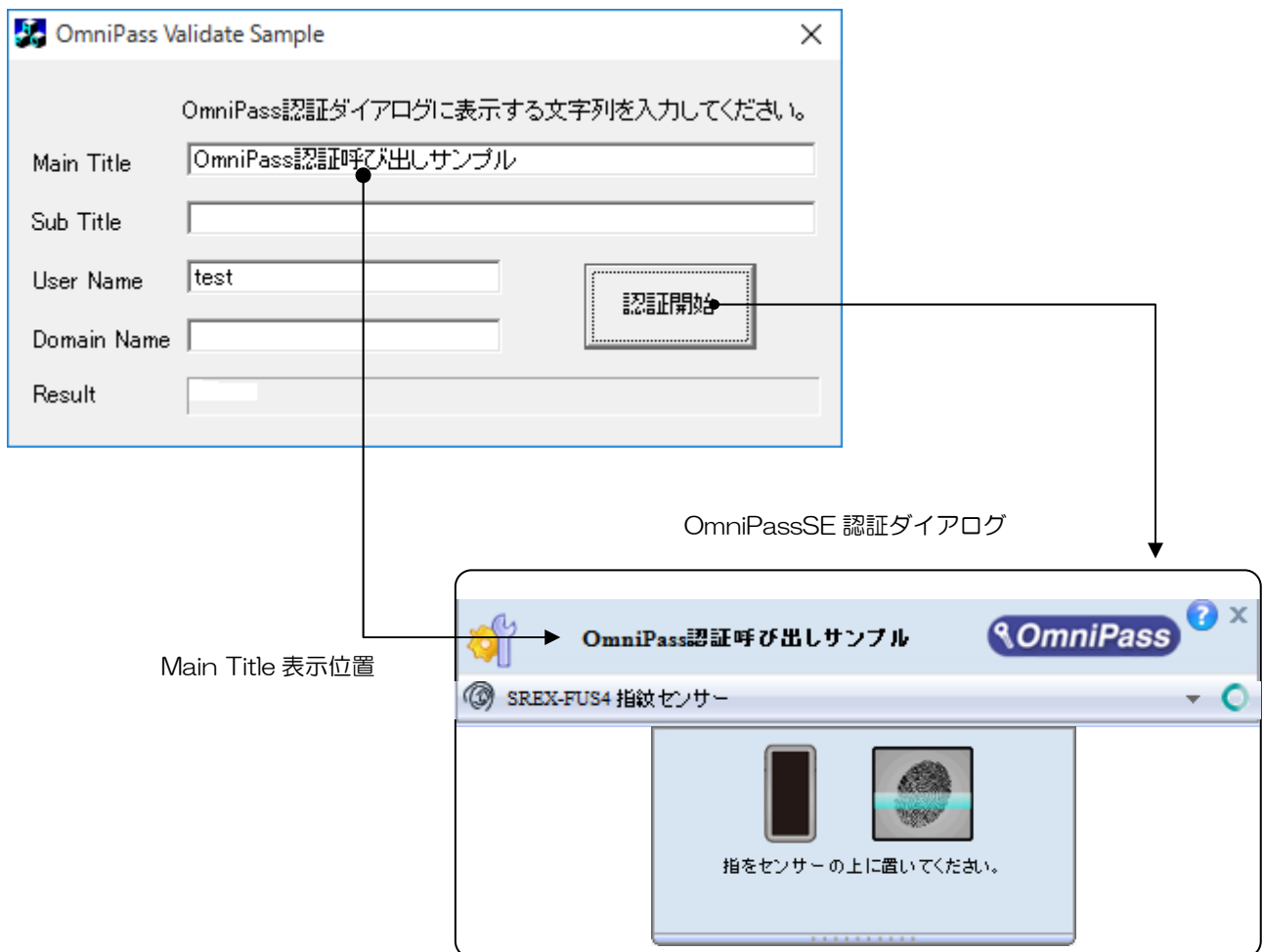
アプリケーションプログラムから OmniPassSE が提供している指紋認証ダイアログを呼び出し、指紋認証を行うプログラム作成方法について説明します。

■OmniPassSE 認証サンプルプログラム概要

製品付属 CD-ROM の「SDK¥OPSDK_x32」「SDK¥OPSDK_x64」フォルダーに、アプリケーションプログラムから OmniPassSE が提供する指紋認証ダイアログを呼び出してユーザー認証を行うサンプルプログラムが格納されています。

(「OPSDK_x32」は 32bit 用、「OPSDK_x64」は 64bit 用となります。)

サンプルプログラム OPValidate.exe を呼び出すと下記のダイアログが表示されます。Main Title 欄に OmniPassSE 認証ダイアログに表示したい文字列を入力し、User Name 欄に認証を行うユーザー名をセットします。「認証開始」ボタンをクリックすると、OmniPassSE 認証ダイアログが表示されます。OmniPassSE 認証ダイアログで指紋認証を行うと、認証結果が Result 欄に表示されます。



■API 呼び出し方法

アプリケーションから OmniPassSE の指紋認証機能呼び出すための準備として、

- (1) OmniPassSE をインストールします。

ダイナミックリンクライブラリ OP3INTC.DLL は、OmniPassSE をインストールすると自動的にコピーされます。

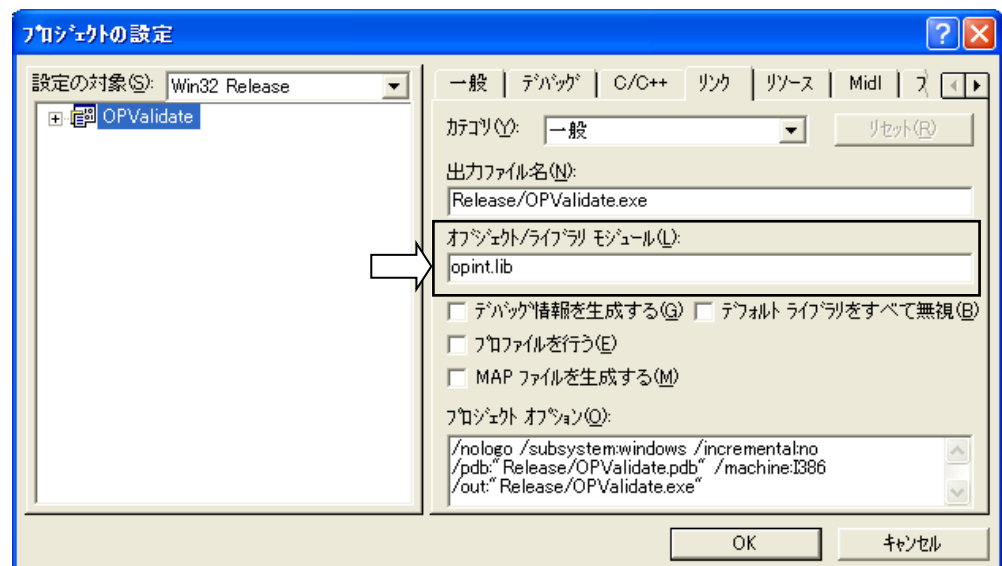
- (2) OPINT.LIB ライブラリモジュールをアプリケーションのプロジェクトに追加

スタティックライブラリ OPINT.LIB は製品添付 CD-ROM の「SDK¥Lib」フォルダーに格納されています。OPINT.LIB をアプリケーションのプロジェクトにコピーし、プロジェクトの設定より「リンク」ページを開いて、「オブジェクト/ライブラリモジュール(L)」に追加します。

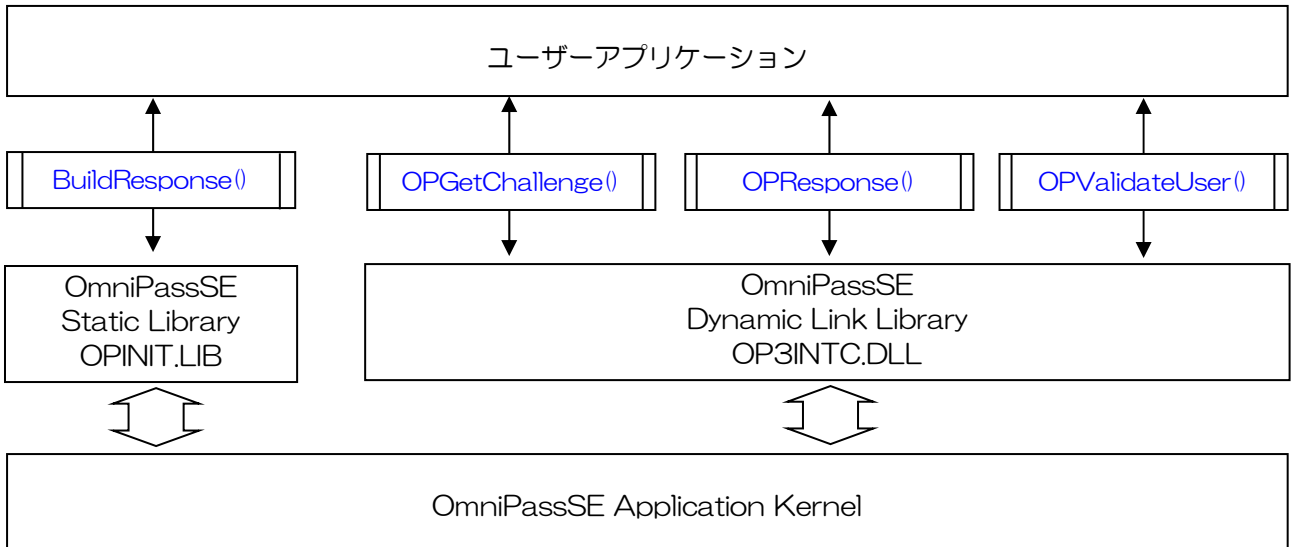
- (3) 製品添付 CD-ROM の「SDK¥Include」フォルダーに格納されている「OmniPass.h」をアプリケーションのプロジェクトにコピーし、アプリケーションにインクルードします。

- (4) アプリケーションの初期化部分で OP3INTC.DLL が提供する OPGetChallenge()、OPResponse()と OPValidateUser()ファンクションのアドレスを取得します。

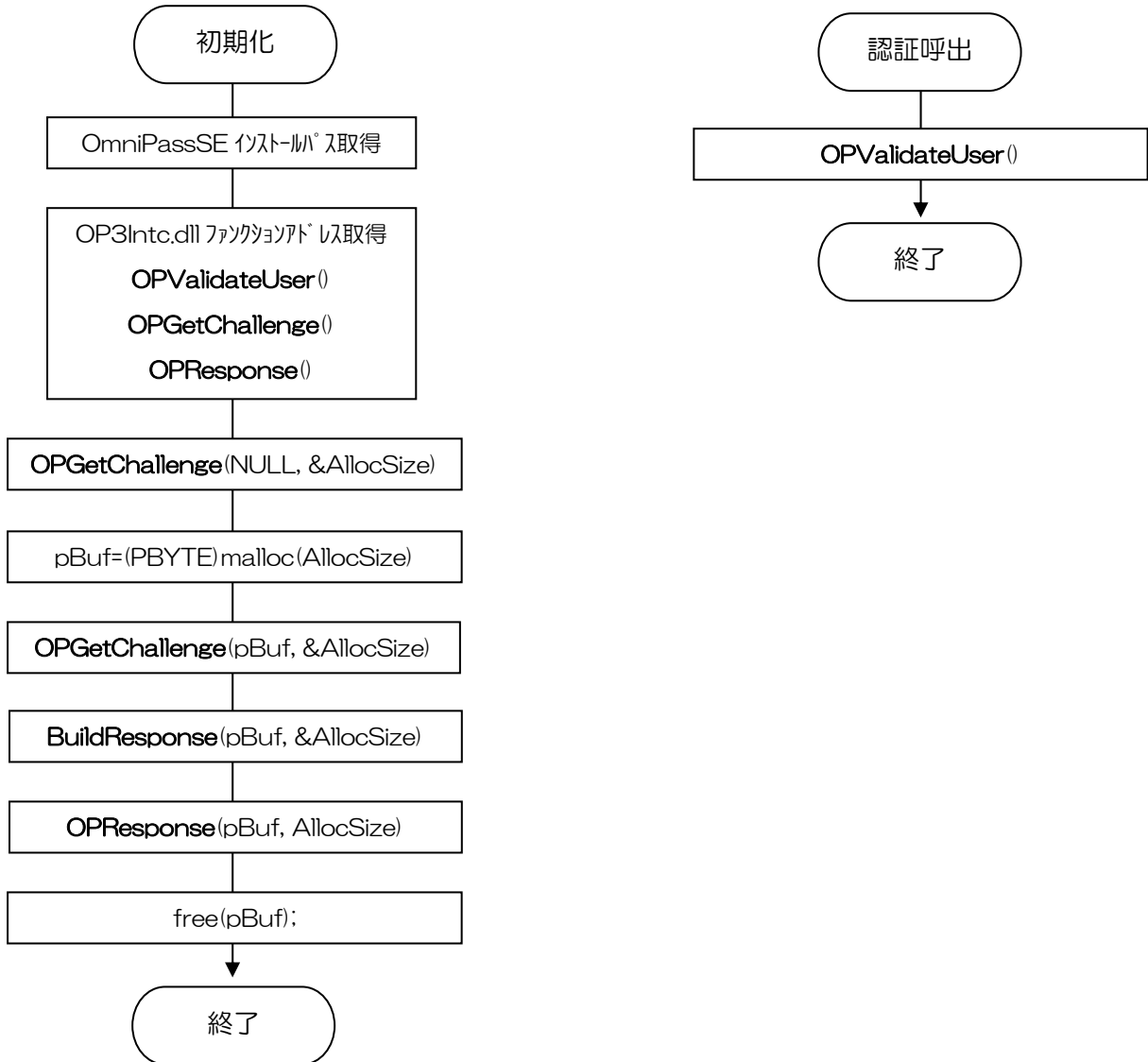
以上で、アプリケーションから各 API を呼び出すための準備は完了です。OPValidateUser()の呼び出しを行うまでのプログラミングフローを次ページに示します。エラー処理等の詳細に関しては、添付のサンプルソースコード「OPValidate」を参照してください。



■OmniPassSE インターフェイスアーキテクチャ



■プログラミングフロー



■API インターフェイス仕様

OPValidateUser	OmniPassSE 認証ダイアログ表示
-----------------------	-----------------------------

DWORD OPValidateUser (

PCHAR UserName, 認証ユーザー名
PCHAR authTitle, 認証ダイアログに表示するメインタイトル
PCHAR authSubTitle —
)

引数

UserName OmniPassSE 認証を行うユーザー名が格納されているバッファのアドレスを指定します。ASCII 文字列の終端は NULL ターミネートとしてください。

authTitle OmniPassSE 認証ダイアログのメインタイトルに表示する文字列が格納されているバッファのアドレスを指定します。

authSubTitle 必ず、NULL を指定してください。

戻り値

この関数は下記の DWORD 値を返します。

OP_RET_USER_VALIDATION_SUCCESSFUL (0)	ユーザーが正常に認証されました。
OP_RET_VALIDATE_CALLINGAPP_FAILED (1)	呼び出しアプリケーションが認証されていません。 OPGetChallenge()/OPResponse() でエラーがないか確認してください。
OP_RET_NOT_INSTALLED (2)	OmniPassSE がインストールされていません。
OP_RET_INSTALLATION_CORRUPT (3)	OmniPassSE が正しくインストールされていません。
OP_RET_USER_NOT_ENROLLED (4)	指定されたユーザーは OmniPassSE に登録されていません。
OP_RET_USER_VALIDATION_FAILED (5)	ユーザー認証に失敗しました。
OP_RET_GENERIC_ERROR (6)	その他のエラーが発生しました。

解説

OmniPassSE は指定されたユーザーの認証を行います。ユーザー名格納バッファが NULL の場合は、現在 Windows にログオンしているユーザーの認証を行います。

ユーザー名をセットする場合は、下記のフォーマットで認証を行うユーザーの名前を指定してください。

ローカルユーザの場合：“. ¥ユーザー名”

ドメインユーザの場合：“ドメイン名¥ユーザー名”

```

ULONG OPGetChallenge (
    PBYTE pBuffer,
    PULONG pLength
)
    
```

引数

pBuffer		アプリケーションでアロケーションしたバッファへのポインタをセットします。NULL 以外の値がセットされた場合は、格納されるデータの場所を示します。
pLength		ULONG データへのポインタをセットします。pBuffer に NULL がセットされている場合は、このパラメータは無視されます。pBuffer に有効な値がセットされている場合は、pBuffer が示すバッファのサイズをセットしてください。関数が正常に終了した場合は、pBuffer に返されたデータのサイズがセットされます。

戻り値 この関数は下記の ULONG 値を返します。

<code>ERROR_NONE</code>	<code>(0x0000)</code>	正常終了したことを示します。
<code>ERROR_INTERNAL</code>	<code>(0x00F1)</code>	OmniPassSE で内部エラーが発生したことを示します。
<code>ERROR_INVALID_PARAM</code>	<code>(0x00F2)</code>	無効なパラメータがセットされたことを示します。
<code>ERROR_INVALID_SIZE</code>	<code>(0x00F3)</code>	指定のパラメータが無効であるか、必要となるサイズを満足していないことを示します。

解説

この関数は OmniPassSE の認証関数 OPValidateUser () を使用する前に、手順に従って 2 回呼び出す必要があります (API 呼び出しフロー図を参照してください)。初回の呼び出しでは、pBuffer に NULL をセットして呼び出しを行い、pLength に返される必要バッファのサイズを取得します。その後、pLength で指定された大きさのバッファを確保し、pBuffer に確保したバッファへのポインタ、pLength には確保したバッファサイズをセットし、再度この関数を呼び出します。関数が正常に終了した場合は、このバッファに BuildResponse () に引き渡すデータがセットされます。

```

ULONG OPResponse (
    PBYTE pBuffer,
    PULONG pLength
)

```

引数

pBuffer アプリケーションでアロケーションしたバッファへのポインタをセットします。このバッファには BuildResponse() で返されたデータが格納されている必要があります。

pLength pBuffer に格納された有効データのサイズをセットします。

戻り値

この関数は下記の ULONG 値を返します。

ERROR_NONE	(0x0000)	正常終了したことを示します。
ERROR_INTERNAL	(0x00F1)	OmniPassSE で内部エラーが発生したことを示します。
ERROR_INVALID_PARAM	(0x00F2)	無効なパラメータがセットされたことを示します。
ERROR_INVALID_SIZE	(0x00F3)	指定のパラメータが無効であるか、必要となるサイズを満足していないことを示します。

解説

この関数は OmniPassSE 認証関数 OPValidateUser() の初期化処理として使用します。この関数の戻り値が ERROR_NONE の場合は、OPValidateUser() の呼び出しの準備が整ったことを意味します。ERROR_NONE 以外の場合は、OPValidateUser() を呼び出すことはできません。

```

ULONG BuildResponse (
    PBYTE pBuffer,
    PULONG pLength
)

```

引数

pBuffer アプリケーションでアロケーションしたバッファへのポインタをセットします。このバッファには OPGetChallenge () で返されたデータが格納されている必要があります。

pLength pBuffer に格納された有効データのサイズをセットします。OPGetChallenge () で返されたデータ長をセットしてください。

戻り値

この関数は下記の ULONG 値を返します。

ERROR_NONE	(0x0000)	正常終了したことを示します。
ERROR_INTERNAL	(0x00F1)	OmniPassSE で内部エラーが発生したことを示します。
ERROR_INVALID_PARAM	(0x00F2)	無効なパラメータがセットされたことを示します。
ERROR_INVALID_SIZE	(0x00F3)	指定のパラメータが無効であるか、必要となるサイズを満足していないことを示します。

解説

この関数は OmniPassSE 認証関数 OPValidateUser () の初期化処理として使用します。この関数の戻り値が ERROR_NONE の場合は、レスポンスバッファ pBuffer が正常にビルドされたことを意味します。このバッファは、OPResponse () に引き渡してください。

RATOC SREX-FSU4 質問用紙

●下記情報をご記入願います。

法人登録の方のみ	会社名・学校名			
	所属部署			
ご担当者名				
E-Mail				
住所	〒			
TEL		FAX		
製品型番		シリアルNo.		
ご購入情報	販売店名		購入日	

●下記運用環境情報とお問い合わせ内容をご記入願います。

【パソコン/マザーボードのメーカー名と機種名】
【ご利用のOS】
【OmniPassSE バージョン】
【お問合せ内容】
【添付資料】



個人情報取り扱いについて

ご連絡いただいた氏名、住所、電話番号、メールアドレス、その他の個人情報は、お客様への回答など本件に関わる業務のみに利用し、他の目的では利用致しません。

