



ePass2003 ユーザマニュアル

V1.2

変更履歴：

日付	バージョン	説明
May. 2011	V1.0	初版
Jan. 2012	V1.01	管理ツールの利用方法の内容追加
Dec 2012	V1.02	Windows 8 に対応
April 2017	V1.03	Windows 10 に対応
May. 2020	V1.04	[2.8 初期化 (管理者用のみ)] に「SO PIN 最大リトライ回数」、「ユーザ PIN 最大リトライ回数」の設定範囲を修正
May. 2020	V1.05	・Linux、MacOS 対応内容を追加 ・全体レイアウトの見直し
Aug. 2021	V1.06	サポートするプラットフォームを追加
Sep. 2024	V1.1	・サポートするプラットフォームの修正 ・「1.3.2 サイレントインストール版の利用手順」の追加 ・全体内容の調整
Nov. 2025	V1.2	・サポートするプラットフォームを追加

Software Developer's Agreement

All Products of Feitian Technologies Co., Ltd. (Feitian) including, but not limited to, evaluation copies, diskettes, CD-ROMs, hardware and documentation, and all future orders, are subject to the terms of this Agreement. If you do not agree with the terms herein, please return the evaluation package to us, postage and insurance prepaid, within seven days of their receipt, and we will reimburse you the cost of the Product, less freight and reasonable handling charges.

1...Allowable Use – You may merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. You may make archival copies of the Software.

2...Prohibited Use – The Software or hardware or any other part of the Product may not be copied, reengineered, disassembled, decompiled, revised, enhanced or otherwise modified, except as specifically allowed in item 1. You may not reverse engineer the Software or any part of the product or attempt to discover the Software's source code. You may not use the magnetic or optical media included with the Product for the purposes of transferring or storing data that was not either an original part of the Product, or a Feitian provided enhancement or upgrade to the Product.

3...Warranty – Feitian warrants that the hardware and Software storage media are substantially free from significant defects of workmanship or materials for a time period of twelve (12) months from the date of delivery of the Product to you.

4...Breach of Warranty – In the event of breach of this warranty, Feitian's sole obligation is to replace or repair, at the discretion of Feitian, any Product free of charge. Any replaced Product becomes the property of Feitian.

Warranty claims must be made in writing to Feitian during the warranty period and within fourteen (14) days after the observation of the defect. All warranty claims must be accompanied by evidence of the defect that is deemed satisfactory by Feitian. Any Products that you return to Feitian, or a Feitian authorized distributor, must be sent with freight and insurance prepaid.

EXCEPT AS STATED ABOVE, THERE IS NO OTHER WARRANTY OR REPRESENTATION OF THE PRODUCT, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5...Limitation of Feitian's Liability – Feitian's entire liability to you or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price you paid for the unit of the Product that caused the damages or are the subject of, or indirectly related to the cause of action. In no event shall Feitian be liable for any damages caused by your failure to meet your obligations, nor for

any loss of data, profit or savings, or any other consequential and incidental damages, even if Feitian has been advised of the possibility of damages, or for any claim by you based on any third-party claim.

6...Termination – This Agreement shall terminate if you fail to comply with the terms herein. Items 2, 3, 4 and 5 shall survive any termination of this Agreement.

目次

第 1 章	ランタイムライブラリのインストール	4
1.1	サポートするプラットフォーム	4
1.2	システム要件	4
1.3	ランタイムライブラリのインストール	5
1.3.1	手動インストール版の利用手順	5
1.3.2	サイレントインストール版の利用手順	8
1.4	ランタイムライブラリのアンインストール	8
第 2 章	管理ツールの使用方法	10
2.1	管理ツール使用の前提条件	10
2.2	概要	10
2.2.1	管理ツールの起動	10
2.2.2	トークンが接続された場合	11
2.2.3	管理ツールの機能	12
2.3	ログイン	12
2.4	証明書管理	14
2.4.1	証明書情報の表示	14
2.4.2	証明書ファイルのインポート	15
2.4.3	証明書ファイルのエクスポート	16
2.4.4	証明書の削除	17
2.5	トークン名の変更	18
2.6	ユーザ PIN の変更	18
2.7	PIN ブロックの解除（管理者用のみ）	21
2.8	初期化（管理者用のみ）	23
2.9	SO PIN の変更（管理者用のみ）	25
第 3 章	Windows における PIN 管理ツール	27
3.1	概要	27
3.2	Windows における EnterSafe ミニドライバの PIN 管理	27
3.2.1	ユーザ PIN の変更	27
3.2.2	Entersafe ミニドライバのブロック解除	30
付録・用語と略称		37

第1章 ランタイムライブラリのインストール

1.1 サポートするプラットフォーム

Windows :

- Windows 7/8/8.1 (32/64bit)
- Windows 10 (32/64bit)
- Windows 11 (64bit)
- Windows Server 2016 (32/64bit)
- Windows Server 2019 (64bit)
- Windows Server 2022 (64bit)
- Windows Server 2025 (64bit)

Linux : Ubuntu, CentOS, RedHat 等 kernel 2.6.x

Mac OS : macOS X 14.5 以前

1.2 システム要件

ePass2003 を利用するには、以下のシステム要件を満たしている必要があります。

- 前述 (1.1 参照) の OS のいずれかを使用していること
- USB ポート (USB1.1 または USB2.0) があること
- BIOS が USB をサポートし、且つ CMOS 設定上 USB が使用可能な状態になっていること
- USB の拡張またはハブが利用可能であること (オプション)
- ePass2003 トークンを利用すること

1.3 ランタイムライブラリのインストール

ePass2003 を使用する前に、ePass2003 のランタイムライブラリ（ドライバ）をインストールする必要があります。

ランタイムライブラリが SDK¥Windows¥PKI¥Redist に格納されて、手動インストール版（ePass2003-Setup.exe）とサイレントインストール版（ePass2003-Setup_silent.exe）の2種類があります。

以下に、Windows10 の環境での利用手順をそれぞれ説明します。

1.3.1 手動インストール版の利用手順

1. ePass2003-Setup.exe を起動し、ユーザーアカウント制御画面で [はい] をクリックします。
2. 言語選択画面で [OK] をクリックします。

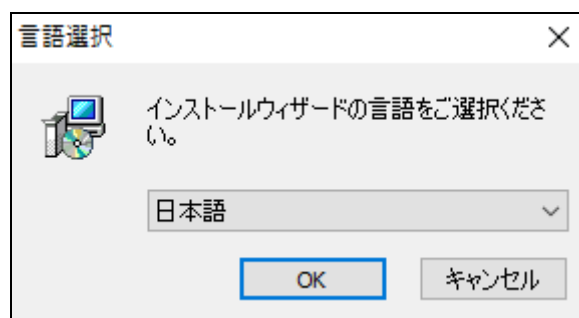


図1 言語の選択

3. [次へ] をクリックします。

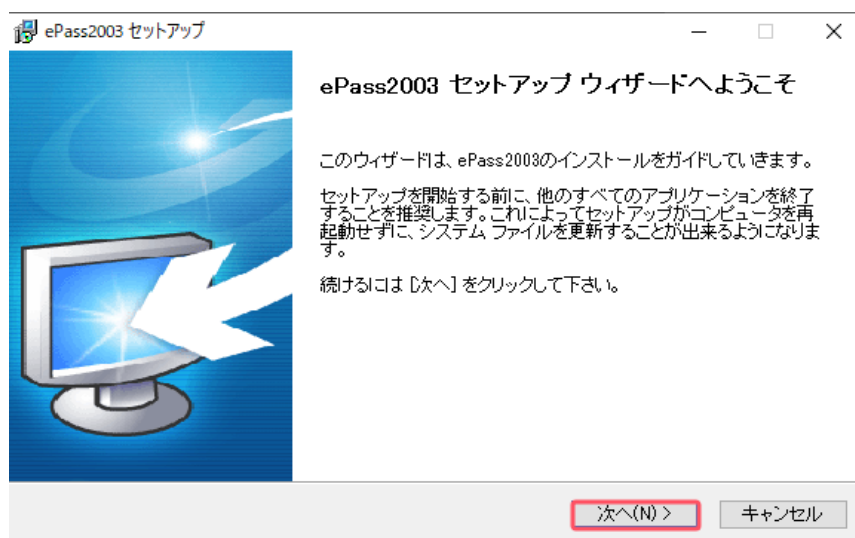


図2 インストールウィザード画面

4. [次へ] をクリックします。

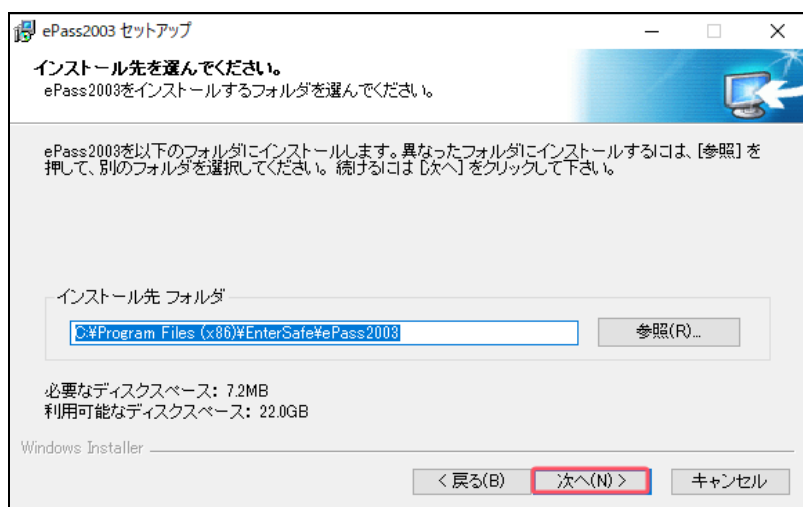


図3 インストールフォルダの選択画面

5. CSP タイプの選択画面が表示されます。デフォルトの [Private CSP] をお勧めします。[インストール] をクリックします。

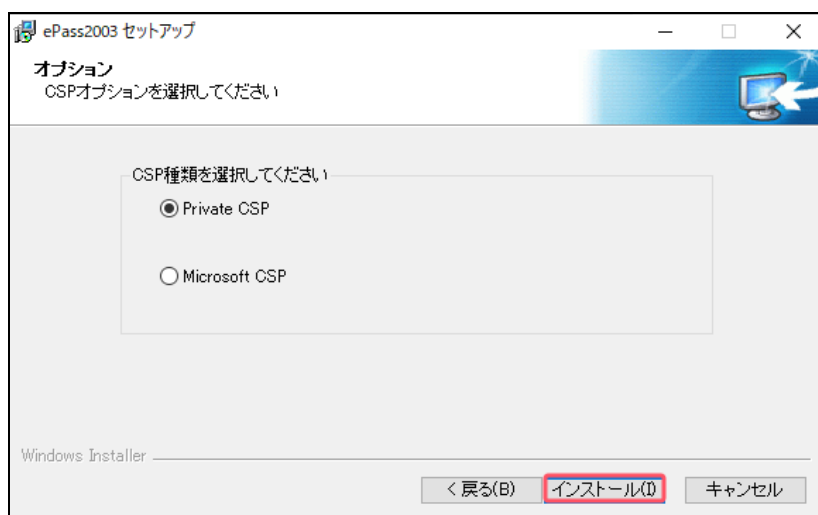


図4 CSP タイプの選択

ePass2003 は Private CSP と Microsoft CSP をサポートしています。

Private CSP は飛天が提供する CSP であり、カスタマイズや OEM 供給が可能です。

Microsoft CSP とは、Microsoft Base CSP (Microsoft Base Smart Card Crypto Provider)のことで、この CSP はミニドライバをサポートしており、複雑なインストールのプロセスを経ることなく、システムの更新だけでミドルウェアをインストールできます。また、インターネット環境のないユーザ向けのインストールパッケージも準備しています。

注意：

ミニドライバーは Windows7/8/8.1 では Windows Update より導入できます (Windows の自動アップデート機能を事前設定する必要があります)。

Visita/WinServer2008 の場合は Microsoft CSP をインストールする必要があります。

XP 以下の場合はまず KB909520 のパッケージをインストールしてから Microsoft CSP をインストールする必要があります。

6. 次のような画面が表示されてインストールします。

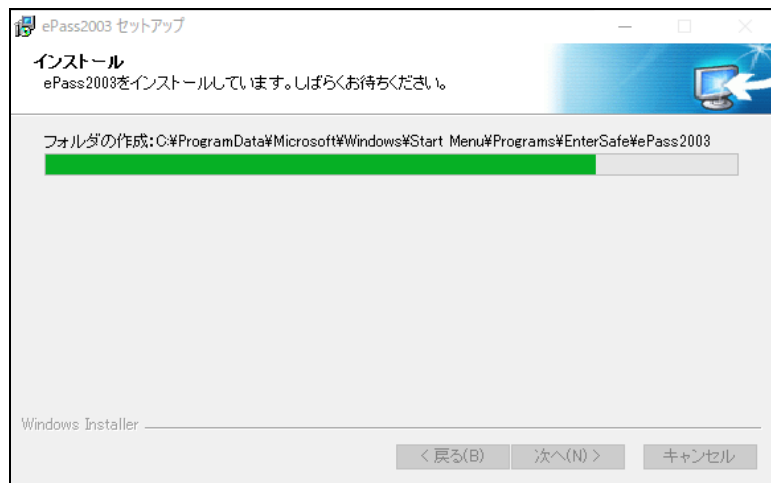


図 5 インストール実行画面

7. [完了] をクリックし、インストールが完了します。

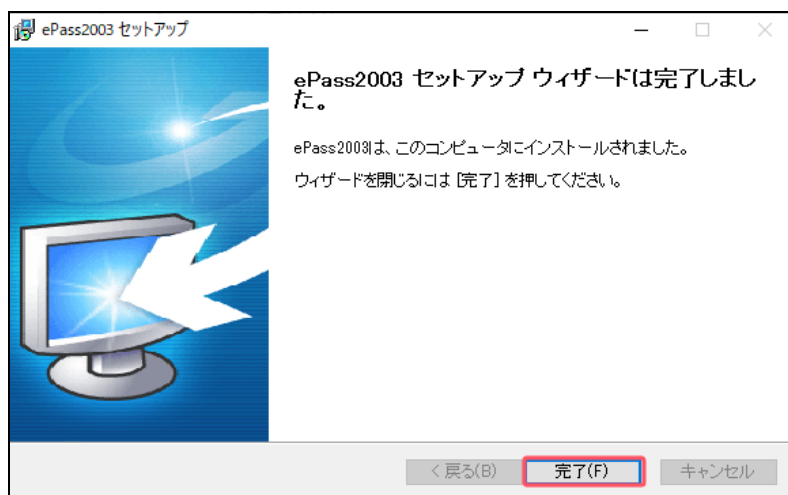


図 6 インストール完了画面

1.3.2 サイレントインストール版の利用手順

1. ePass2003-Setup_silent.exe をダブルクリックし、ユーザーアカウント制御画面に [はい] をクリックします。
2. 画面が表示せずに自動的にインストールされます。ePass2003 を接続し、利用可能になります。

1.4 ランタイムライブラリのアンインストール

1. 「コントロールパネル」→「プログラムのアンインストール」より“ePass2003”を選択し、「アンインストール」をクリックします。[ユーザーアカウント制御] 画面の [はい] をクリックします。
2. ePass2003 アンインストールのウィザードの [アンインストール] をクリックします。

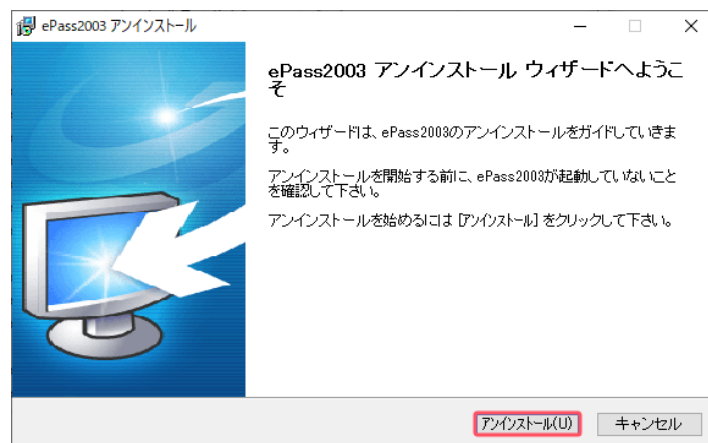


図7 アンインストールウィザード画面

3. アンインストールが開始されます。

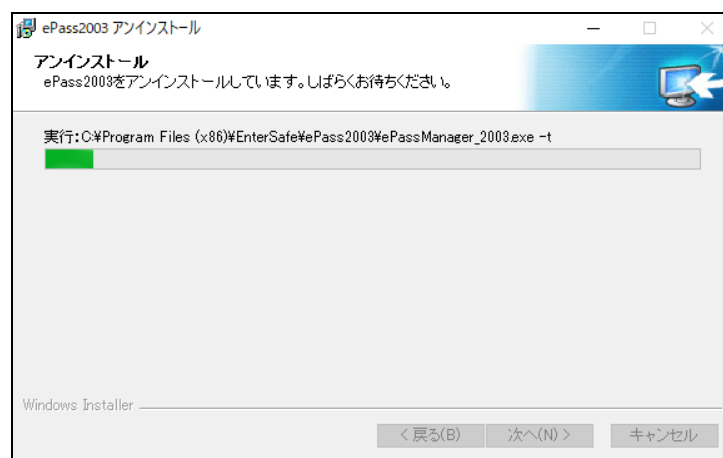


図8 アンインストール実行画面

4. [完了] をクリックし、アンインストールを完了します。



図 9 アンインストール完了画面

第2章 管理ツールの使用方法

管理ツールを使用して ePass2003 の様々な設定を変更できます。本章では、ePass2003 管理ツールの使用方法について説明します。

2.1 管理ツール使用の前提条件

管理ツールを利用する前に、ランタイムライブラリ（ドライバ）をインストールする必要があります。また、ePass2003 トークンを使用する前に、PKI の初期化を行う必要があります。（通常、工場出荷時に初期化されています。）

2.2 概要

管理ツールには「管理者用」と「エンドユーザ用」の 2 種類があります。

どちらのツールでも「ログイン」、証明書の「インポート」、「エクスポート」、「削除」、および「証明書情報の表示」、「ユーザ PIN の変更」、「トークン名の変更」が可能です。

ただし、管理者用ツールにはさらに「初期化」、「ユーザ PIN のブロック解除」、および「SO PIN 変更」機能が含まれています。エンドユーザ用にはこれらの機能は含まれていません。

ランタイムライブラリ（ドライバ）をインストールすると、エンドユーザ用の管理ツールは自動的にインストールされます。管理者用管理ツールは SDK に含まれています：

ePass2003_SDK¥Windows¥PKI¥Utilities¥ePassManagerAdm_2003.exe

以下では、Windows 10 環境でのエンドユーザ用管理ツール（略称：管理ツール）および管理者用管理ツールについて説明します。

2.2.1 管理ツールの起動

「スタート」→「EnterSafe」→「ePass2003 管理ツール」を選択して、管理ツールを起動します。

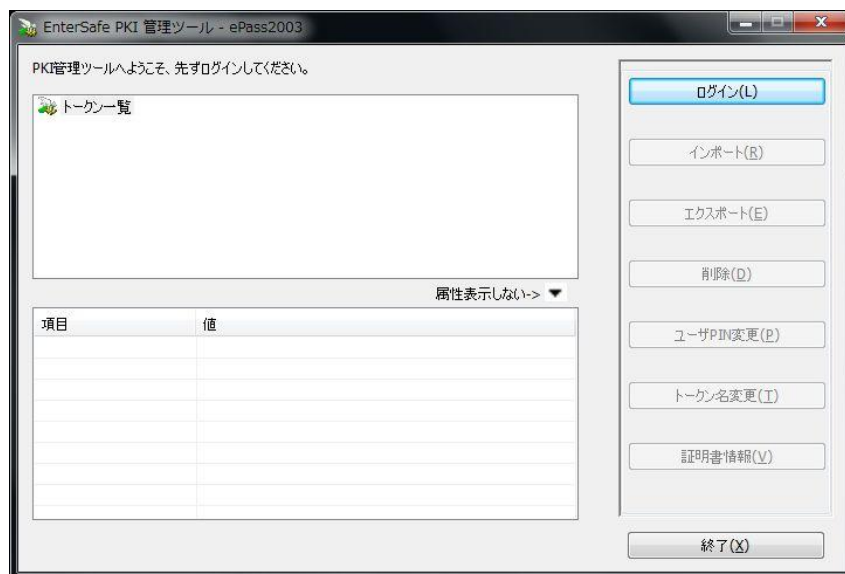


図 10 トークンが未接続の管理ツール画面

2.2.2 トークンが接続された場合

トークンが PC に接続された状態で管理ツールを起動すると、トークンの詳細情報が表示されます。下図は、トークン名「ePass2003」のトークンが接続された画面です。

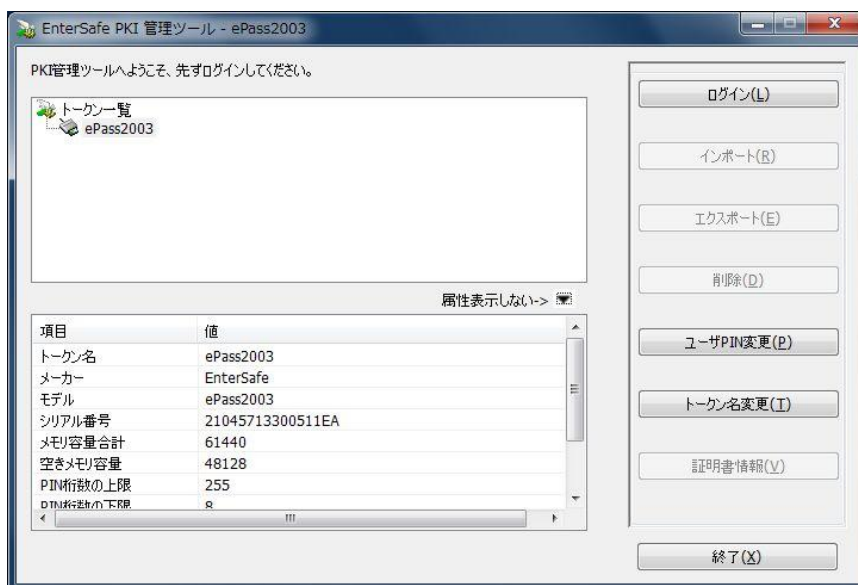


図 11 トークンが接続された管理ツール画面

注意：

メモリ領域は、PIN を参照するために保護されたエリアです。秘密鍵は非常に重要な情報であるため、COS によって管理され、メモリ領域には含まれていません。。

2.2.3 管理ツールの機能

管理ツールには「ログイン」、「インポート」、「エクスポート」、「削除」、「ユーザ PIN 変更」、「トークン名変更」、「証明書情報表示」、「終了」機能があります。

管理者用管理ツールには、さらに「PIN ブロック解除」、「初期化」、「SO PIN 変更」機能が含まれています。各機能の使用方法については、以下で説明します。

2.3 ログイン

管理ツールの左側の「トークン一覧」から ePass2003 トークンを 1 つ選び、「ログイン」ボタンをクリックすると、ユーザ PIN の入力画面が表示されます。



図 12 ユーザ PIN 入力画面

ユーザ PIN 入力画面で「ソフトキーボードを利用する」にチェックを入れると、下図のようにソフトキーボードが使用可能になります。

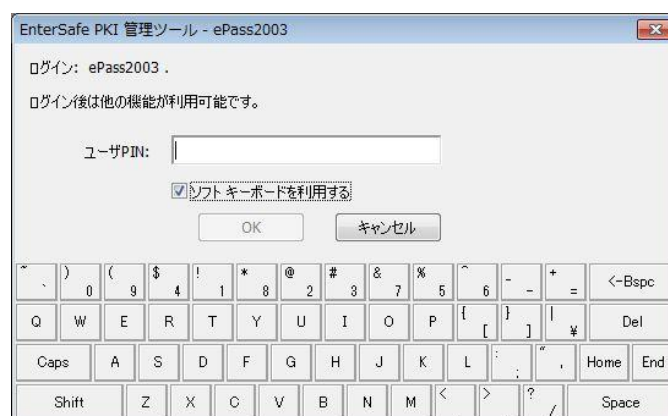


図 13 ユーザ PIN 入力画面（ソフトキーボード使用）

注意: 「ソフトキーボード」を利用する場合、物理キーボードの使用はできません。

PIN の入力後、画面の左上にトークン一覧が表示され、左下に選択されたトークンの詳細情報が表示されます。画面中央の「属性表示しない」ボタンをクリックすると、画面左下の属性一覧が「非表示」となります。ログイン後には、トークン内のメモリ容量の合計と空き容量を確認できます。また、「ログイン」ボタンは「ログアウト」に変更されます。「ログアウト」ボタンをクリックすると、安全にトークンからログアウトできます。

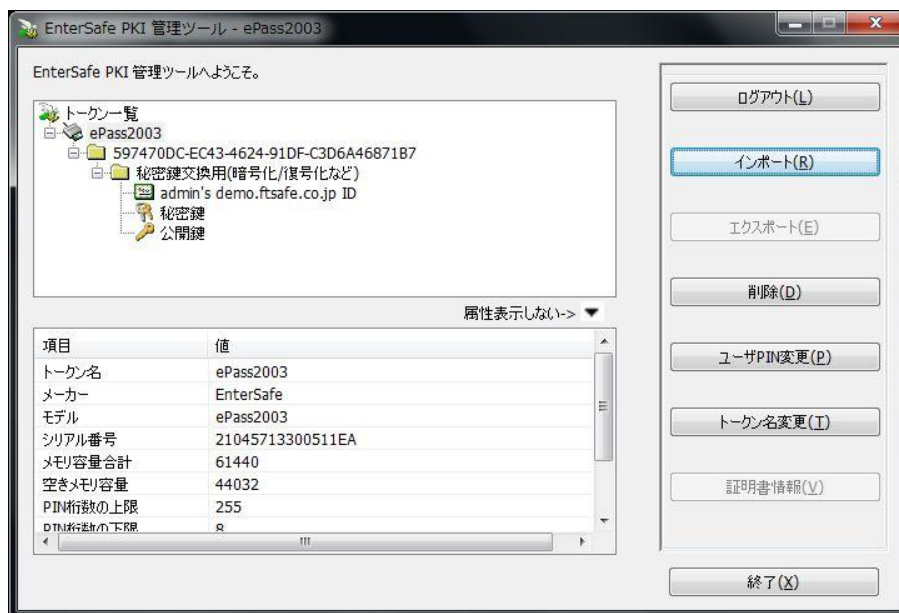


図 14 ログインされた管理ツール画面

間違った PIN を入力すると、エラーメッセージが表示されます。

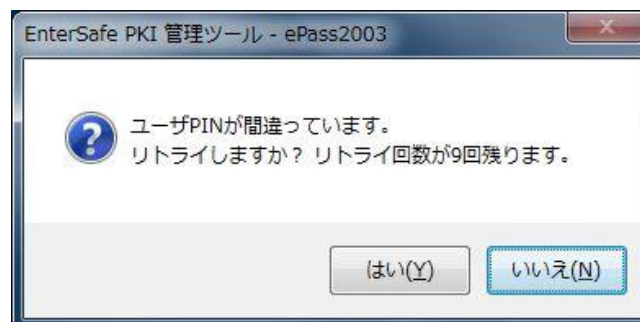


図 15 ログイン：エラーメッセージ画面

注意: PIN の入力回数には制限があり、最大で 10 回まで入力できます。リトライ回数がなくなると、トークンがロックされ使用できなくなりますので、注意してください。

2.4 証明書管理

秘密鍵および電子証明書は、セキュアに ePass2003 に格納できます。ePass2003 は X.509 v3 規格の電子証明書をサポートしています。管理ツールでログインすると、電子証明書の表示、インポート、エクスポート、削除が可能です。

2.4.1 証明書情報の表示

1. 管理ツール画面の左上から証明書を 1 つ選択すると、画面右の「証明書情報」ボタンが有効になります。

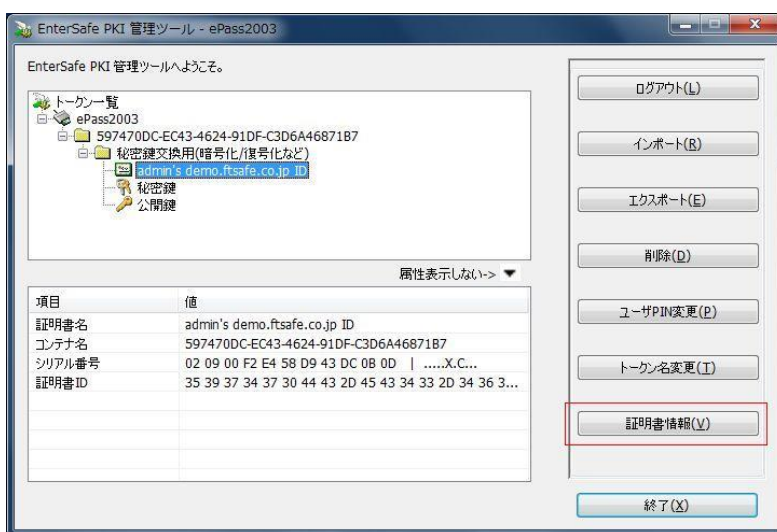


図 16 証明書情報表示画面

2. 証明書をダブルクリックするか、「証明書情報」ボタンをクリックすると、証明書の詳細情報が表示されます。

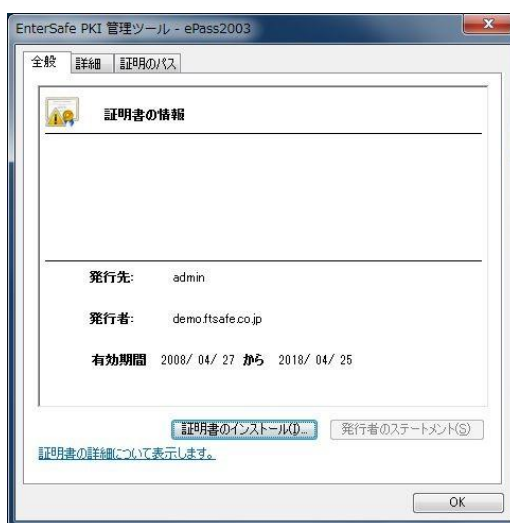


図 17 証明書情報（例）の表示画面

2.4.2 証明書ファイルのインポート

ePass2003 は P12、PFX、P7B、CRT、CER の 5 種類の証明書をサポートしています。P12 と PFX 証明書は公開鍵と秘密鍵のペアが含まれていますが、P7B、CRT、CER には含まれていません。以下に、PFX および P7B 証明書のインポート手順を説明します。

2.4.2.1 PFX 証明書のインポート

管理ツールの「インポート」ボタンをクリックすると、証明書のインポート画面が表示されます。

- ・ 「参照」ボタンをクリックして、PFX 証明書を選択します。証明書にパスワードが設定されている場合は、「証明書アクセスパスワード」にパスワードを入力します。
 - ・ 「全ての証明書」と「クライアント証明書のみ」のいずれかを選択できます。証明書チェーンを含める場合は、「全ての証明書」を選択してください。
 - ・ 証明書の保存場所は「コンテナの選択」で指定します。「新規のコンテナ」と「既存のコンテナ」のいずれかを選択できます。
 - ・ PFX 証明書には公開鍵と秘密鍵のペアが含まれています。用途として「秘密鍵交換」または「署名」のどちらかを選択します。「秘密鍵交換」を選択すると、インポートされた証明書は秘密鍵交換と電子署名の両方に使用できます。「署名」を選択した場合は、電子署名のみが利用可能で、秘密鍵交換は利用できません。
- ※特に特別な理由がない限り、「秘密鍵交換」を選択することをお勧めします。

「OK」ボタンをクリックして証明書をインポートします

注意：1つの証明書コンテナには、用途が異なる2つの証明書を保存可能です。同一用途の証明書をインポートすると、既存の証明書は上書きされます

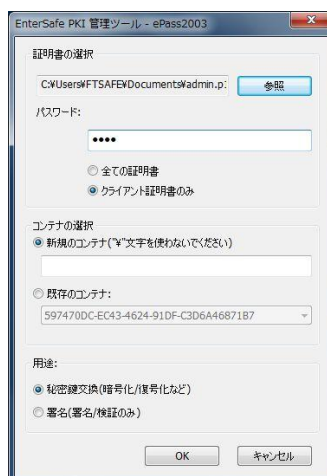


図 18 PFX 証明書のインポート画面

2.4.2.2 P7B 証明書のインポート

管理ツールの「インポート」ボタンをクリックすると、下図のような画面が表示されます。「参照」ボタンをクリックして、P7B 証明書を選択します。P7B 証明書は「新規のコンテナ」にのみ保存できます。P7B 証明書には公開鍵と秘密鍵のペアが含まれていないため、用途の選択は不要です。「OK」ボタンをクリックして証明書をインポートします。



図 19 P7B 証明書のインポート画面

2.4.3 証明書ファイルのエクスポート

管理ツールのエクスポート機能を使用して、トークンに保存された証明書をエクスポートし、ファイルとして保存できます。証明書を 1 つ選択して「エクスポート」ボタンをクリックすると、証明書保存場所を指定するダイアログボックスが表示されます。



図 20 証明書エクスポートダイアログボックス

ファイル名を入力し、「保存」をクリックします。正常に保存されると、下記のメッセージが表示されます。



図 21 証明書がエクスポートされた画面

注意: 管理ツールでのみ証明書をエクスポートできます。証明書の公開鍵と秘密鍵のペアはエクスポートできません

2.4.4 証明書の削除

1. 管理ツールで不要な証明書を削除できます。トークン一覧から削除したい証明書を選択し、「削除」ボタンをクリックすると、下記のメッセージ画面が表示されます。

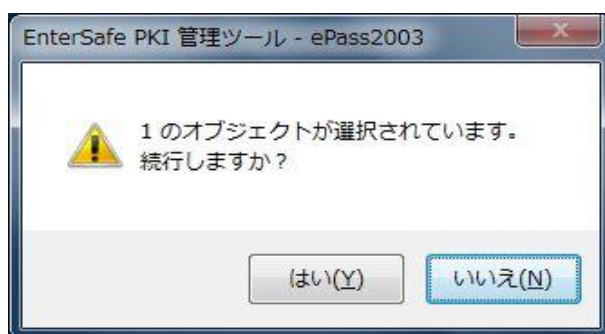


図 22 証明書の削除メッセージ画面

2. 「はい」ボタンをクリックすると、証明書が削除され、占有されていたメモリ領域が開放されます。同様の方法で、ePass2003 内の秘密鍵や証明書コンテナを選択し、「削除」ボタンをクリックすると、それらも削除されます。ePass2003 のトークン一覧を選択して「削除」ボタンをクリックすると、ePass2003 内のすべてのコンテナ、証明書、秘密鍵が削除されます。

2.5 トークン名の変更

トークンは内部に格納されているシリアル番号で区別されますが、シリアル番号は長くて覚えにくいいため、一般的にはトークン名で表示します。トークン名は管理ツールで変更することが可能です。

1. 管理ツール画面の「トークン名変更」ボタンをクリックすると、下記の画面が表示されます。

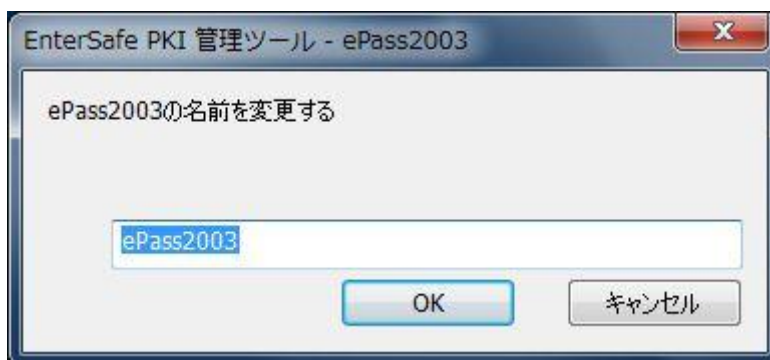


図 23 トークン名の変更画面

2. 新しいトークン名を入力し、「OK」ボタンをクリックすると、トークン名を変更できます。

注意: トークン名は最大 32 桁まで設定可能です。

2.6 ユーザ PIN の変更

トークンのユーザ PIN を個別に変更できます。ユーザ PIN を変更するには、管理ツールの「ユーザ PIN 変更」ボタンをクリックしてください。



図 24 ユーザ PIN 変更画面

「ソフトキーボード」にチェックを入れて、ソフトキーボードでユーザ PIN を入力します。ソフトキーボードを利用する場合、画面は下記のように表示されます。

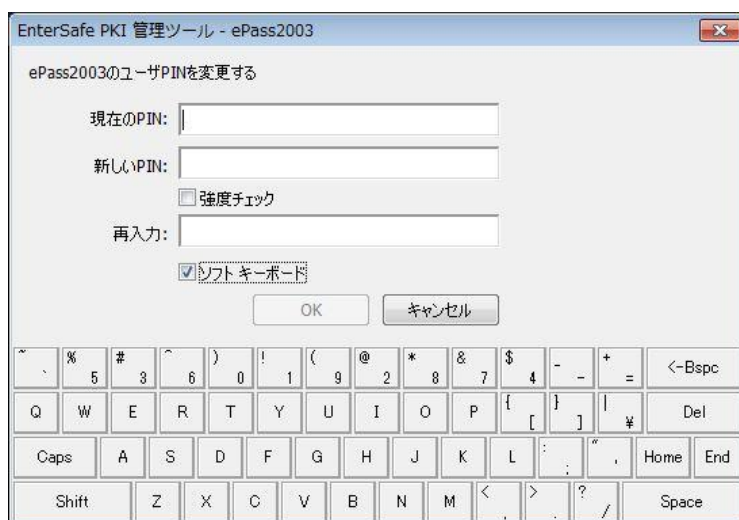


図 25 ユーザ PIN 変更画面（ソフトキーボード使用）

画面の「強度チェック」にチェックを入れると、新しいユーザ PIN の安全性強度をチェックできます。設定されたユーザ PIN の安全性が低い場合は、下図のように赤い「低」マークが表示されます。



図 26 ユーザ PIN 変更画面（安全性強度：低）

設定されたユーザ PIN の安全性強度がやや高い（中程度）場合は、下図のように表示されます。



図 27 ユーザ PIN 変更画面（安全性強度：中）

ユーザ PIN を設定する際は、適当な半角英数字（大文字、小文字、数字、記号）を組み合わせ、覚えやすく、できるだけ長いユーザ PIN を設定することを推奨します。設定範囲は 8～255 桁です。新しいユーザ PIN を 8 桁以下に設定すると「OK」ボタンがグレイアウトし、続行できません。また、255 桁以上の設定もできません。



図 28 ユーザ PIN 変更画面（安全性強度：高）

現在のユーザ PIN を入力し、下段の 2 つのボックスに新しいユーザ PIN を入力して、「OK」ボタンをクリックしてください。PIN の変更に成功すると、下記の画面が表示されます。



図 29 ユーザ PIN の変更が成功した際のメッセージ画面

注：工場出荷時のユーザ PIN は「12345678」です。現在のユーザ PIN の入力を誤ると、エラーメッセージが表示されます。制限回数を超えて入力を誤ると、ユーザ PIN がブロックされ（一時的にトークンが使用不可能になります）、ブロックされたトークンは管理者用管理ツールでのみ解除できます。

以上がエンドユーザ用管理ツールの説明になります。

次に管理者用管理ツールについて説明します。管理者用管理ツールには、いくつかの追加機能があります。次の図のように、メインの管理者画面には右下に（▲）ボタンがあります。

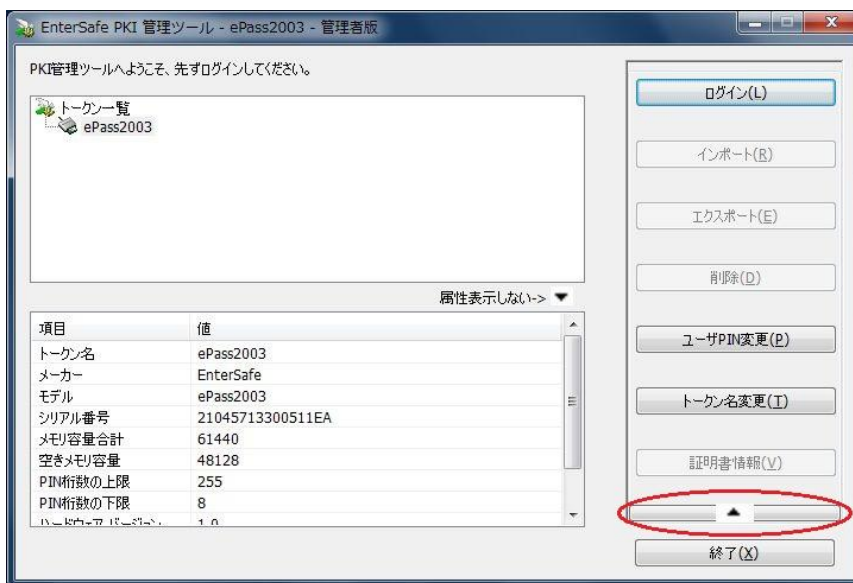


図 30 管理者画面 1

（▲）ボタンをクリックすると、以下のような管理者画面 2 が表示されます。

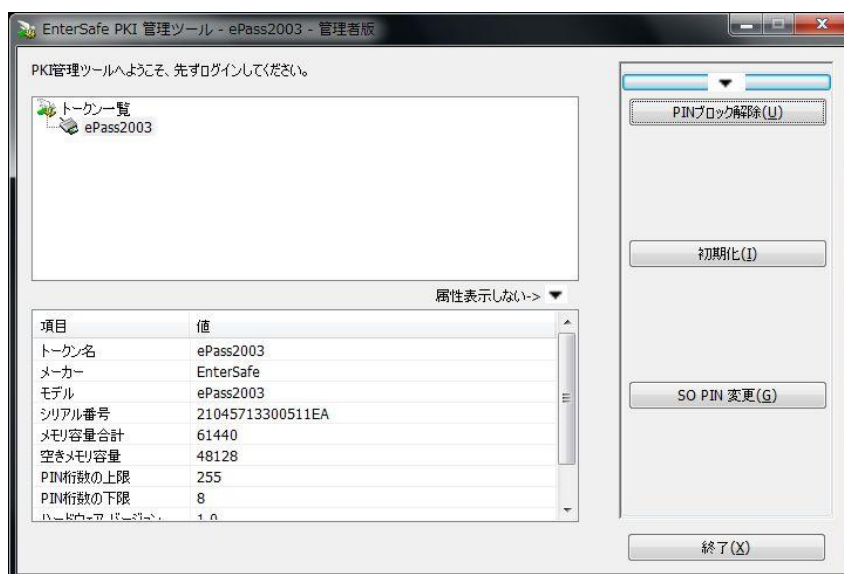


図 31 管理者画面 2

2.7 PIN ブロックの解除（管理者用のみ）

ユーザ PIN ブロックの解除は管理者用管理ツールでのみ行えます。ブロックを解除するには、画面の「PIN ブロックの解除」ボタンをクリックしてください。



図 32 PIN ブロックの解除

画面の「強度チェック」にチェックを入れて、入力された SO PIN の安全性強度をチェックします。使用方法は「2.6 ユーザ PIN の変更」の「強度チェック」をご参照ください。

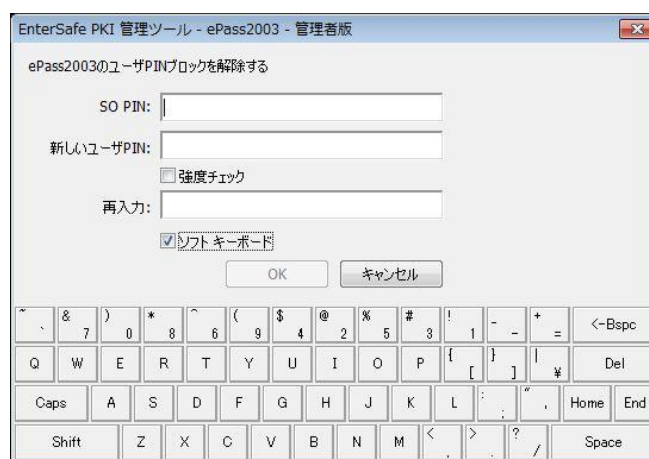


図 33 PIN ブロックの解除（ソフトキーボード使用）

SO PIN を入力して、新しいユーザ PIN（8～255 桁）を設定してください。「OK」ボタンをクリックすると、ユーザ PIN が再設定されます。変更成功すると、以下の画面が表示されます

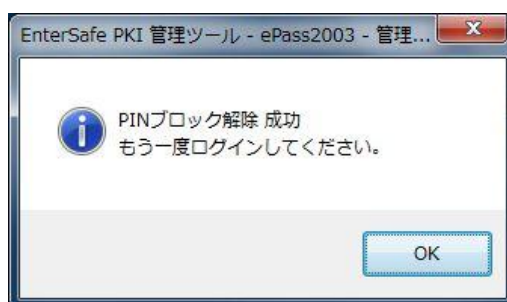


図 34 PIN ブロック解除メッセージ

注：工場出荷時の SO PIN は「entersafe」です。ユーザ PIN ブロックを解除するには、現在の SO PIN を正しく入力する必要があります。SO PIN の入力を 10 回誤ると、そのトークンは以後使用不能となりますので、十分ご注意ください。

2.8 初期化（管理者用のみ）

ePass2003 は使用前に初期化が必要です。初期化は管理者用管理ツールでのみ行うことができます。初期化時には、トークン名、SO PIN、ユーザ PIN、リトライ回数、タイムアウトを設定することができます。



図 35 トークンの初期化画面

注意：初期化を行うと、トークン内に保存されたすべてのデータが削除されます。初期化後は元に戻せません。

- 「トークン名」

トークン名には現在のトークン名が表示されます。変更する場合は、直接変更してください。後から「トークン名変更」機能を使ってトークン名を変更することもできます。

- 「SO PIN」と「再入力」

新しい SO PIN（8～255 桁）を入力してください。確認のために「再入力」フィールドにも再度入力してください。なお、後から「SO PIN 変更」機能（管理者用管理ツールのみ）で SO PIN を再度変更することができます。

- 「ユーザ PIN」と「再入力」

新しいユーザ PIN（8～255 桁）を入力してください。確認のために「再入力」フィールドにも再度入力してください。なお、後から「ユーザ PIN 変更」機能でユーザ PIN を再度変更することができます。

- 「SO PIN 最大リトライ回数」、「ユーザ PIN 最大リトライ回数」

SO PIN とユーザ PIN の最大リトライ回数を設定できます。設定範囲は 0～10 回で、デフォルトは 10 回に設定されています。

- 「タイムアウト」（単位：分）

タイムアウト時間（0～600 分）が設定できます。「0」を設定した場合は、タイムアウトなしとなります。

このタイムアウトはトークンの PIN 認証状態のタイムアウトを指します。トークンを一度 PIN 認証してから再度 PIN 認証が必要になるまでの時間です。

初期化時にタイムアウトを設定すると、PIN 認証後、一定時間内に操作が行われない場合、自動的にタイムアウト状態となります。タイムアウト状態でウェブページを更新すると、再度 PIN 認証が必要となります。

タイムアウト時間内に操作を行うと、その時点でタイムアウト時間が再計算されます。トークンのタイムアウト設定は、トークンを初期化する際に個別に設定できます。タイムアウト時間は 0～600 分の範囲で設定可能です。「0」を設定すると、タイムアウトなしを意味します。（出荷時のデフォルト設定は「0」：タイムアウトなしです。）

タイムアウト設定の例：

◎タイムアウト：10 分の場合

パターン 1：SSL 認証後、10 分間操作がないと、その後にページを更新すると再度 PIN 認証が行われます。

パターン 2：SSL 認証後、4 分後に再度ウェブページにアクセスすると、その時点から再度 10 分間のタイムアウトが設定されます。その後 10 分間操作がないと、タイムアウト状態になります。

◎タイムアウト：0 分（タイムアウトなし）の場合

SSL 認証時に最初の一回のみ PIN 認証が必要です。その後、ブラウザを閉じるまで再度 PIN 認証は不要です。

注：

トークンのタイムアウトが適用されるのは、アプリケーションがサーバにアクセスする際に毎回トークンの認証操作を行う場合に限りです（例えば、IE や Firefox での SSL 認証など）。一部の VPN クライアントソフトでは、最初の接続時のみトークンの PIN 認証を行うため、タイムアウトが適用されない場合があります。

初期化に失敗するとエラーメッセージが表示されます。エラーメッセージが表示された場合は、各項目が設定範囲内であるか確認してください。

設定変更後、各項目に問題がないか確認し、「初期化」ボタンをクリックすると確認画面が表示されます。

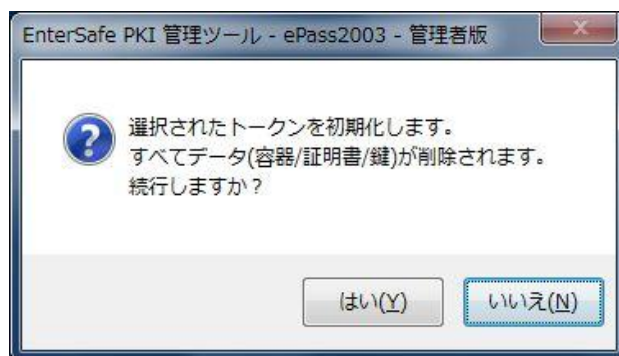


図 36 初期化確認画面

「はい」ボタンをクリックすると、初期化が行われます。初期化が成功すると、以下の画面が表示されます。設定された情報を有効にするには、再度ログインする必要があります。

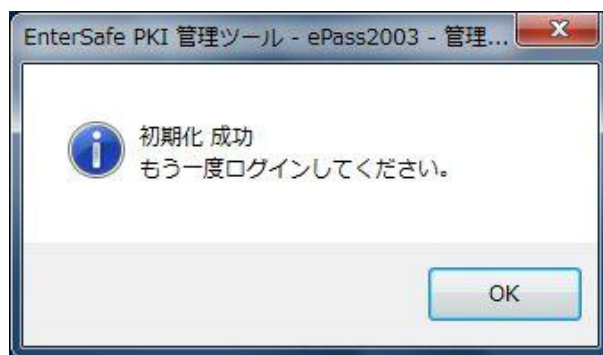


図 37 初期化成功メッセージ画面

2.9 SO PIN の変更（管理者用のみ）

管理者用管理ツールの「SO PIN 変更」ボタンをクリックすると、次のような SO PIN 変更のダイアログボックスが表示されます。



図 38 SO PIN 変更ダイアログボックス

「強度チェック」にチェックを入れると、入力された SO PIN の安全性強度をチェックできます。使用方

法は「2.6 ユーザ PIN の変更」の「強度チェック」をご参照ください。

入力された情報がスパイウェアで盗まれることを防ぐために、「ソフトキーボード」にチェックを入れ、ソフトキーボードで SO PIN を入力することができます。ソフトキーボードを利用する場合、画面は下記のように表示されます。



図 39 SO PIN の変更画面（ソフトキーボード使用）

SO PIN を変更するには、まず「現在の SO PIN」を入力し、次に「新しい SO PIN」と「再入力」を入力して、「OK」ボタンをクリックします。なお、SO PIN が 8 桁以下だと「OK」ボタンがグレースアウトし、クリックできません。

注意：工場出荷時の SO PIN は「entersafe」です。SO PIN を変更するには、現在の SO PIN を正しく入力する必要があります。SO PIN の入力を 10 回誤ると、そのトークンは以後使用不能となりますので、十分ご注意ください。

SO PIN が変更されると、下記画面が表示されます。



図 40 SO PIN 変更成功画面

第3章 Windows における PIN 管理ツール

3.1 概要

EnterSafe のミニドライバは、Microsoft Windows のスマートカードフレームワークによって EnterSafe が開発した新しいスマートカード・ミニドライバです。

この新しい Windows スマートカードのアーキテクチャは、最上位レイヤーにある共通の暗号化機能と最下位レイヤーにあるメーカー固有のスマートカード・ハードウェアとが分離しているという実態に対して効果を発揮するものです。現在の Windows には簡単なスマートカード・インターフェース・レイヤがあります。それはスマートカード・ミニドライバと呼ばれるものですが、Windows のプラットフォームに含まれている共通の暗号化コンポーネントに直接関係しています。

スマートカード用の暗号化技術は Windows Vista/2008 等の次世代暗号化技術(CNG : Cryptography API Next Generation)に実装されました。CAPI 用の CSP は、“Microsoft Base Smart Card Cryptographic Service Provider”と呼ばれ、CNG は“Microsoft Smart Card Key Storage Provider”と呼ばれます。Base CSP は旧 OS (WindowsXP 以下) ではサポートされていませんが、Windows Update 「KB909520」をインストールすることで利用可能となります。

Base CSP と KSP は共通のソフトウェア暗号化技術を提供します。アーキテクチャにおいて準拠しているミニドライバは、スマートカードのハードウェアとソフトウェアに簡単にアクセスするための機能を備えています。

アプリケーション開発者の視点から見ると、Base CSP と KSP および ミニドライバのインターフェースは、スマートカードの種類に関わらずスマートカードにアクセスする共通の手法を提供しています。

新しいアーキテクチャは既存のスマートカードのシナリオをサポートし、暗証番号(PIN)の管理ツールも提供しています。

3.2 Windows における EnterSafe ミニドライバの PIN 管理

3.2.1 ユーザ PIN の変更

通常、ユーザ PIN はトークン上のデータ保護のために使われるパスワードです。ユーザが Windows へのログオン、email の署名、email の暗号化や VPN 接続などの操作でプライベートな領域にアクセスする際、ユーザ PIN の入力が必要です。

トークン上のデータ保護の為、定期的にユーザ PIN を変更することを推奨します。ユーザ PIN を変更する為のインターフェースが Windows OS で提供されています。以降では OS ごとの、ユーザ PIN 変更方法について説明します。

3.2.1.1 Windows 2000, XP or Server 2003 でのユーザ PIN の変更

Windows 2000, XP or 2003 においてユーザ PIN を変更する場合は、事前に更新パッケージ「KB909520」をインストールして“Smart Card PIN Tool”を利用できるようにしておく必要があります。以下は、“Smart Card PIN Tool”を利用してユーザ PIN を変更する手順となります。

1. PC の USB ポートにユーザ PIN を変更したい ePass2003 を挿入して下さい。
2. 「スタート」→「ファイル名を指定して実行」に“PinTool”と入力し「スマートカード証明番号 (PIN) ツール」を起動すると、以下のような画面が表示されます。

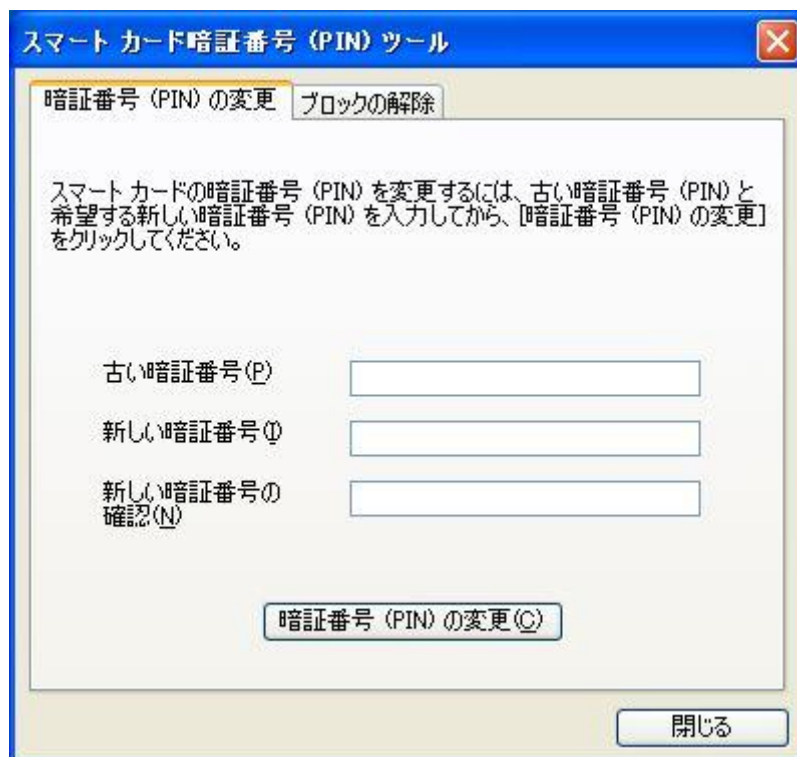


図 41 スマートカード暗証番号 (PIN) ツール – ユーザ PIN の変更

3. 上段に現在の PIN を入力し、中段に新しい PIN を入力し、下段に確認のため新しい PIN を再入力してください。
4. [暗証番号 (PIN) の変更] ボタンをクリックすると、ユーザ PIN の変更作業が完了します。

注意： ePass2003 のユーザ PIN のデフォルト値は “12345678” です。

3.2.1.2 Windows Vista, 2008, 7,8 でのユーザ PIN の変更

Windows Vista, 2008, 7, 8 の場合、ユーザは「セキュアデスクトップ」モードでスマートカードのユーザ PIN を変更することができます。

「セキュアデスクトップ」はオペレーティング・システムで最も信頼性の高い環境です。「セキュアデ

スクトップ」環境下では、ユーザは変更の可否を決定するまでコンピュータ上で他の作業を行うことができません。同様にプログラムを実行することもできません。「セキュアデスクトップ」が最も一般的に使われるのは Windows へのユーザログオンの時ですが、パスワードの変更やこれから説明するスマートカードの PIN 管理の操作にも使われます。

以下は、Windows Vista におけるスマートカードの PIN 変更の手順です。


1. [Ctrl+Alt+Delete]をクリックして、「セキュアデスクトップ」モード画面に入ります。
2. [パスワードの変更]を選択してください。
3. [他の資格情報]を選択してください。
4. PC の USB ポートに、ユーザ PIN を変更する ePass2003 を挿入してください。
5. スマートカードのアイコンを選択してください。
6. 下記のようにスマートカードの PIN 変更画面が表示されます。
7. 現在の(古い)暗証番号(PIN)を入力し、次に新しい暗証番号(PIN)を入力し、確認のため新しい暗証番号(PIN)を再入力してください。
8. 最後に、をクリックして完了です。



図 42 セキュアデスクトップ環境 – ユーザ PIN の変更

3.2.2 Entersafe ミニドライバのブロック解除

EnterSafe ミニドライバ上に保存されたデータは、ユーザ PIN によって保護されています。PIN のリトライ回数はハードウェアによって制限されています。設定されている制限値を超えるとミニドライバはブロックされます。一旦ブロックされると、正しいユーザ PIN を入力しても使えません。元に戻す唯一の手段が「**ブロック解除**」という方法です。

注意：EnterSafe ミニドライバの PIN のリトライ回数の最大値は、10 回となっています。

3.2.2.1 ブロック解除手続きの例

スマートカードのブロック解除機能では通常のエンドユーザには使用を許していない管理鍵が必要になります。ユーザはセキュリティ管理者にブロック解除を依頼する必要があります。

管理鍵の保護のため、エンドユーザに対して管理鍵を示すようなことは致しません。その代わりにチャレンジ&レスポンス認証方式が利用されます。

1. エンドユーザはスマートカードから暗号鍵(チャレンジ)を受け取ります。
2. エンドユーザはその暗号鍵(チャレンジ)を管理者に伝えます。
3. 管理者は、その暗号鍵(チャレンジ)(8 バイト)とそのユーザの管理鍵(24 バイト)を使って 3DES アルゴリズムの演算処理を施して値を生成します。この値がレスポンス(8 バイト)です。
4. 管理者は生成されたレスポンスをエンドユーザに送ります。
5. エンドユーザ側では、そのレスポンスの値が新しいユーザ PIN となります。
6. スマートカード側は、エンドユーザから入力されたレスポンスとスマートカードが自ら生成したレスポンスと照合し、二つのレスポンスの値が一致していればブロック解除処理が成功したことになります。そして新しいユーザ PIN が作成され、リトライ回数もリセットされます。

ユーザ PIN を検証する際の手続きのように、スマートカードのブロック解除の手続きも入力回数に制限値があります。一旦この制限値に達してしまうと、管理者もブロックを解除することはできません。スマートカードに格納されている全てのデータへのアクセスが永久にできなくなります。従いまして、ブロック解除の手続きは細心の注意が必要です。

ユーザ PIN 変更の手続きも同様ですが、スマートカードのブロック解除で使われるプロセスやツールは Windows Vista/2008 と旧 Windows OS とで異なります。

3.2.2.2 Windows 2000, XP, Server 2003 下におけるスマートカードのブロック解除

Windows 2000、XP、Server 2003 及びそれ以降のバージョンでは、“Smart Card PIN Tool”はユーザ PIN の変更のほかにスマートカードのブロック解除にも利用されます。

“PIN Tool”を利用するには PC にログオンが必要ですが、スマートカードは既にブロックされているのでユ

ユーザはログオンできません。そのような場合にユーザは、既にログオンされている他の PC で“PIN Tool”にアクセスして、スマートカードのブロック解除の手続きを行う必要があります。

以下は、“PIN Tool”を利用した時のブロック解除の画面です。

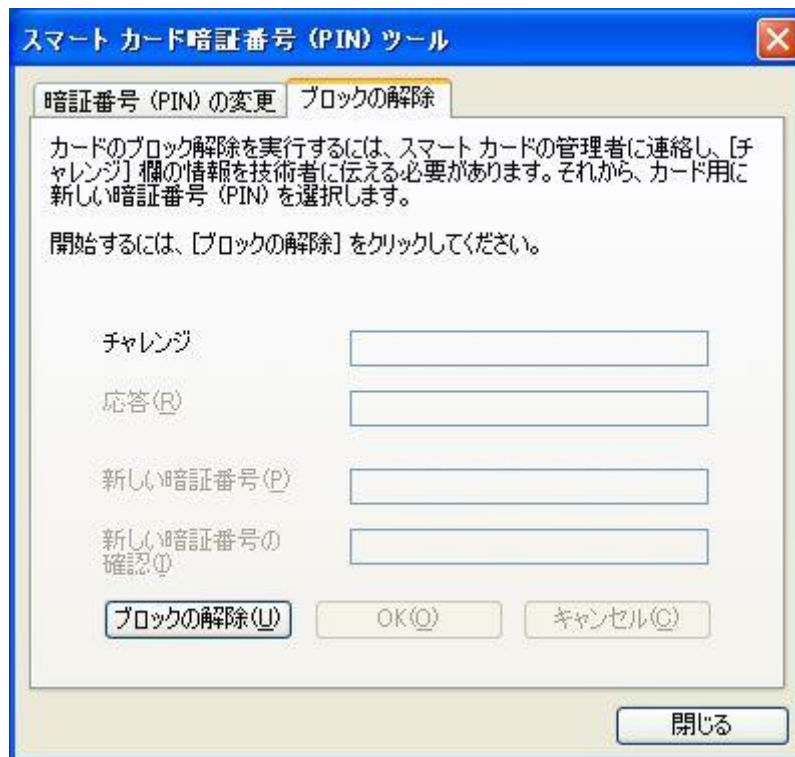


図 43 スマートカード暗証番号 (PIN) ツール – ブロックの解除

ブロックされたトークンを USB ポートに挿入して、[ブロックの解除]をクリックすると、スマートカードから 16 桁の暗号鍵(チャレンジ)が送られてきます。そして 3.2.2.1 で説明したようなプロセスで、ユーザが応答(レスポンス)、新しい暗証番号(PIN)、確認のための新しい暗証番号(PIN)の入力が可能になります。[OK]ボタンを押すと、応答(レスポンス)欄と新しい暗証番号(PIN)欄に入力された値がスマートカードに送られ、ブロック解除の手続きが完了します。

3.2.2.3 Windows Vista, 2008, 7, 8 下でのスマートカードのブロック解除

Windows Vista, 2008, 7, 8 でのスマートカードのブロック解除は、「セキュアデスクトップ」に統合されました。但し、デフォルトでは設定されていないので、「グループポリシー」(後述)を使って有効にする必要があります。この機能が有効になると、ブロックされたスマートカードを使ったログインがなされた時、スマートカードのブロック解除の画面が表示されます。

注意：

ブロック解除の手続きは、スマートカードがユーザの手に渡されるよりも以前に管理鍵を割当てられていることが必要です。また IT インフラストラクチャーとして、ユーザが支援を必要とする場合にこれらの鍵を安全に格納し、アクセスできる手段を備えていることも必要です。

3.2.2.3.1 Windows Vista, 2008, 7,8 下でのスマートカードのブロック解除を有効にする

Windows Vista, 2008,7,8 において「セキュアデスクトップ」モードでのユーザインターフェースのブロック解除機能はデフォルトで有効にはなっていません。有効にするには、管理者が **Microsoft Management Console (MMC)**でグループ ポリシー オブジェクト・エディタのスナップインを使って行います。

1. [スタート]ボタン→[ファイル名を指定して実行]欄に **MMC** と入力して、[Enter]キーを押してください。
2. ユーザアカウント制御のプロンプトが表示された場合は、[続行]をクリックしてください。コンソール 1 - [コンソール ルート]という **Microsoft Management Console** の画面が表示されます。
3. コンソール 1 の画面で、[ファイル]をクリックし、[スナップインの追加と削除]を選択してください。
4. [スナップインの追加と削除] 画面で、利用できるスナップインのリストの中のグループ ポリシー オブジェクト・エディタを選択して[追加]を押します。下記画面を参照してください。

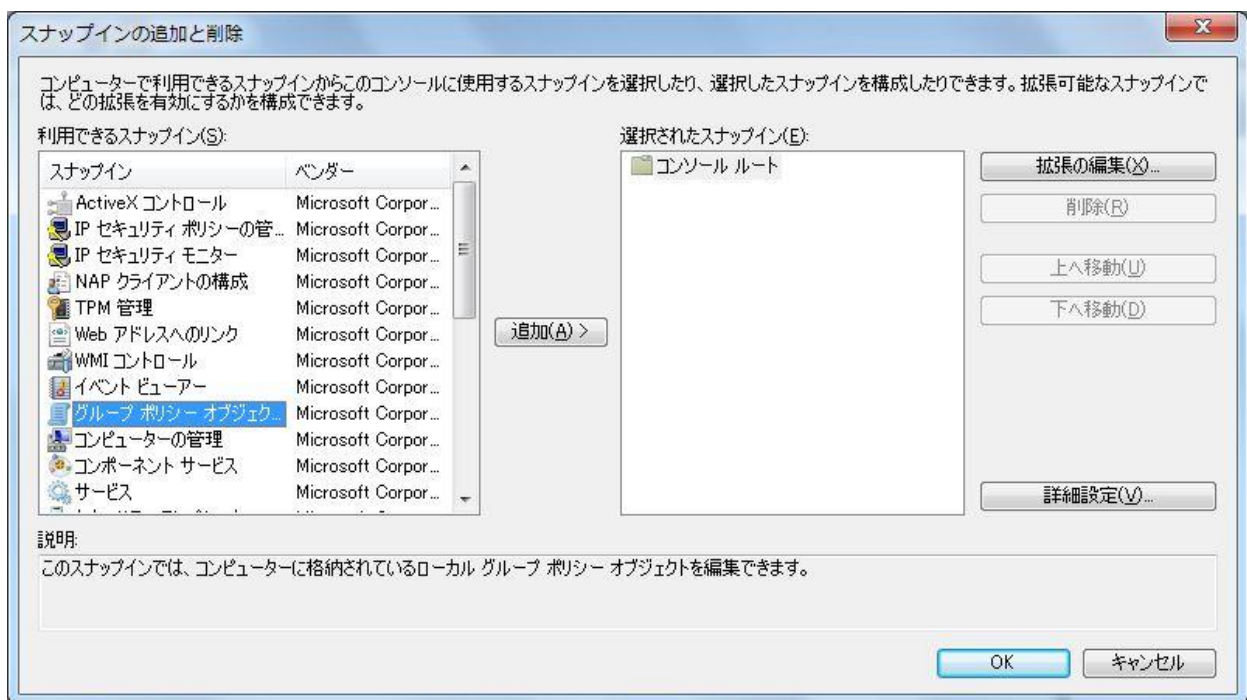


図 44 グループポリシーオブジェクト・エディタの追加

5. ブロック解除の機能はローカル PC 単体、またはドメイン下の全ての PC に対して有効にすることができます。
 - 1) ローカル PC 上でブロック解除を有効にするためには、管理者権限で行います。グループ ポリシー オブジェクトの中のローカルコンピュータポリシーを選択してください。[Finish] ボタンをクリックして、グループポリシーの選択を終了してください。
 - 2) ドメイン下の全ての PC 上でブロック解除を有効にするためには、ドメインコントローラに管理者権限でログインして行います。グループ ポリシー オブジェクトの中のデフォルト

ドメインポリシーを選択してください。[Finish]ボタンをクリックして、グループポリシーの選択を終了してください。

6. スナップインの追加と削除の画面で、[OK]をクリックして画面をクローズしてください。
7. 画面左側の一覧からローカルコンピュータポリシーをクリックし、[コンピュータの構成]→[管理用テンプレート]→[Windows コンポーネント]→[スマートカード]をクリックしてください。画面中央の設定のところで、[ログオン時に統合ブロック解除画面を表示する]選択し、ダブルクリックしてください。(次の画面を参照してください)

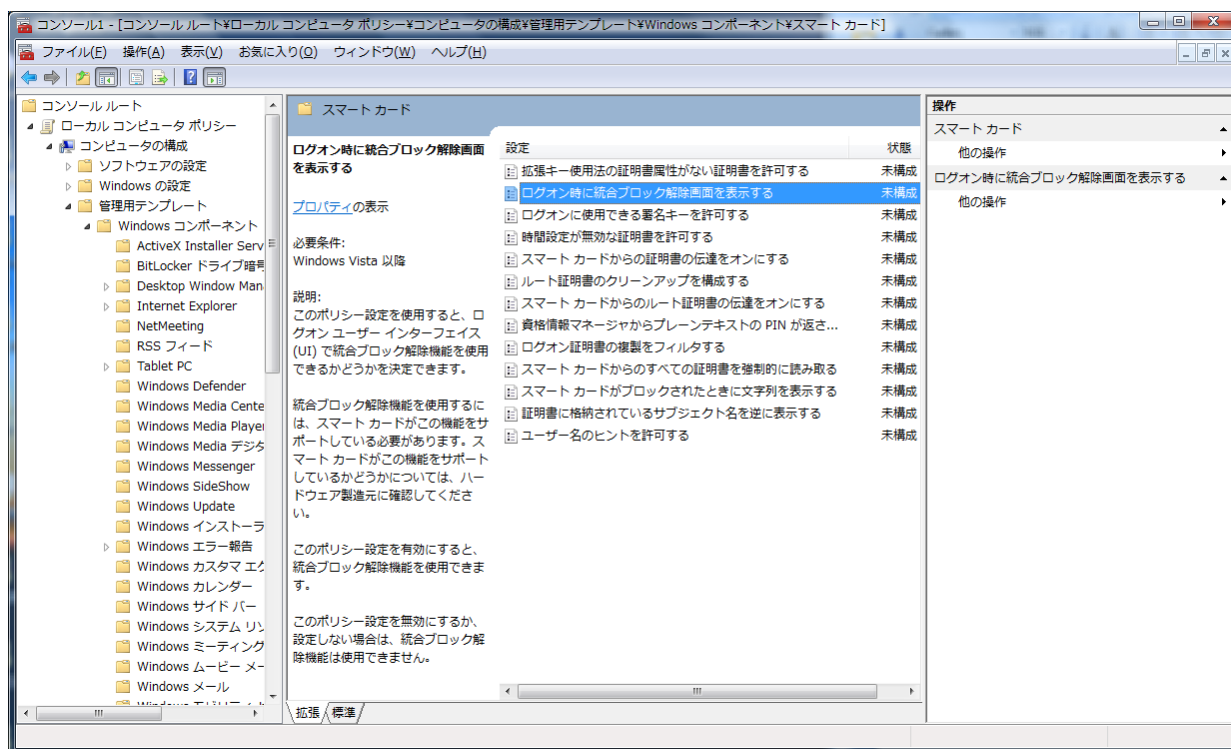


図 45 スマートカードの統合ブロック解除の設定

8. 次の画面のように、[有効]を選択してから、[OK]をクリックしてください。

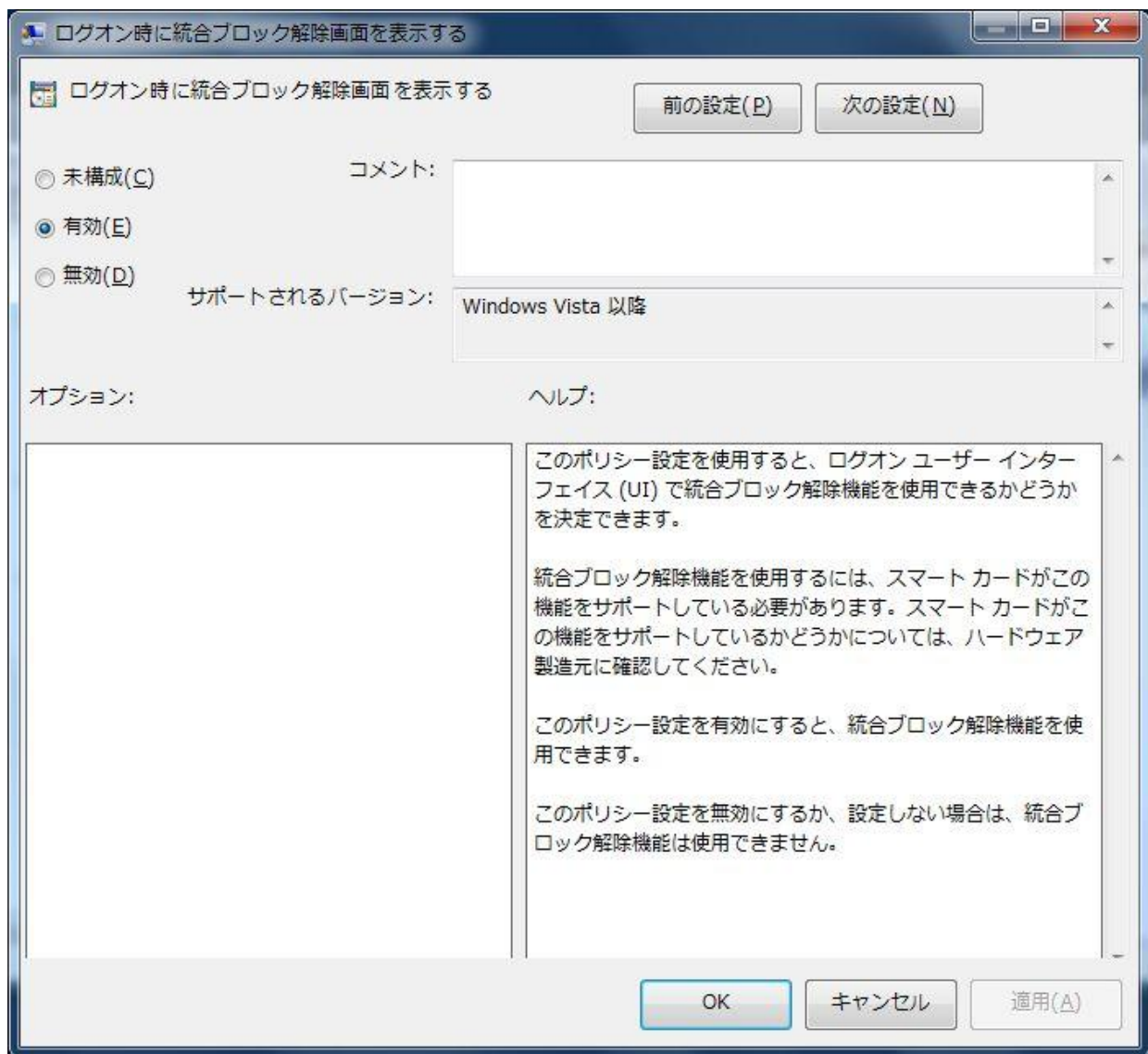


図 46 スマートカードの統合ブロック解除機能を有効にする

スマートカードのブロック解除の画面にはグループポリシーを介して固有のメッセージ等の文字列を作成することもできます。例えば管理者とチャレンジ&レスポンスのやり取りを行う際の電話番号等を記載するなどです。文字列の設定は次の手順で行います。

9. コンソール 1 の画面に戻り、[ローカル コンピュータ ポリシー] → [コンピュータの構成] → [管理用テンプレート] → [Windows コンポーネント] → [スマートカード]を選択してください。そして、画面中央の、[スマートカードがブロックされたときに文字列を表示する]を選択し、ダブルクリックしてください。
10. [有効]を選択してから、テキストボックスの中に表示させたいメッセージを入力してください。最後に[OK]をクリックしてください。(次の画面の例では、連絡先の電話番号が入力されています)

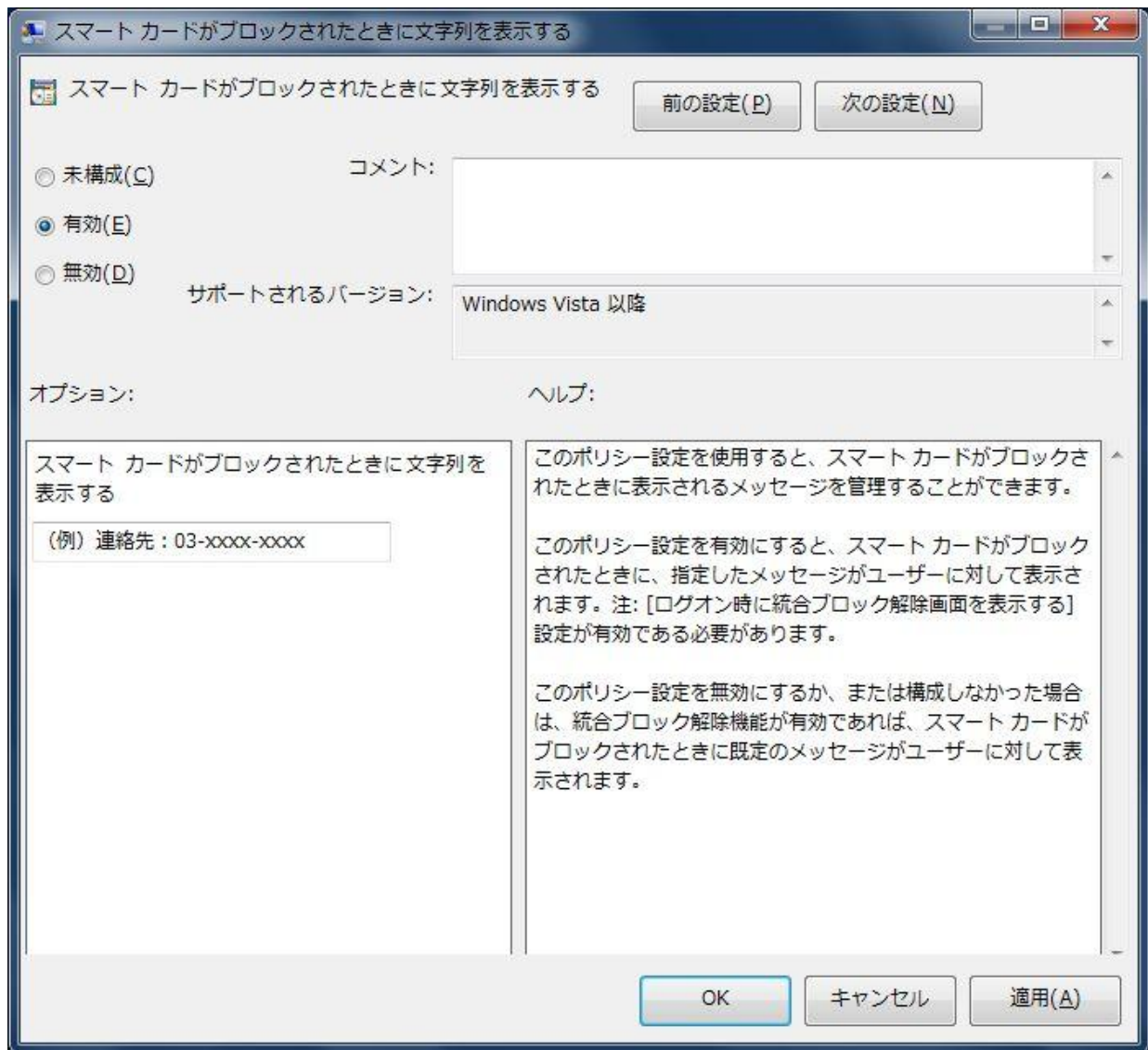


図 47 スマートカードがブロックされた時に案内文等の文字列を表示するか否かの設定

3.2.2.3.2 Windows Vista, 2008, 7, 8 下でのスマートカードのブロック解除

ユーザ PIN の変更の時と同様に、Windows Vista, 2008, 7, 8 ではスマートカードのブロック解除も「セキュアデスクトップ」に統合されています。但し、デフォルトでは設定されていないので、「グループポリシー」(3.2.2.3.1 参照)を使って有効にする必要があります。この機能が有効になっていると、ブロックされたスマートカードを使ってログインが行われた時に、ユーザにはスマートカードのブロック解除の画面が表示されます。

「セキュアデスクトップ」モードでのブロック解除の画面イメージは次の画面を参照ください。



図 48 セキュアデスクトップ – スマートカードのブロック解除

3.2.2.4 スマートカードのブロック解除用の管理ツール

スマートカードのブロック解除の手続きは、管理者がエンドユーザの持つスマートカードによって生成された暗号鍵（チャレンジ）からレスポンス値を生成し、それをユーザに通知するする必要があります。以下は管理者にて認識が必要な項目です。

1. 使用中の全てのスマートカードの管理鍵を知っているか、知る手段を把握していること
2. ユーザのスマートカードから与えられるチャレンジ値と管理鍵を使い、3DES のアルゴリズムツールにアクセスしてレスポンス値を生成できること

Windows OS はいずれのバージョンも、管理者がユーザのスマートカードの管理鍵を安全に保管するための手段を提供しておりません。提供されるのは、チャレンジ値に対するレスポンス値を計算するためのバックエンドツールとなります。

これらの機能は、一般向けには、Microsoft の Identity Lifecycle Manager(ILM)を含めた、商用の Base CSP compliant Card Management System (CMS)によって提供されます。

付録・用語と略称

用語・略称	説明
ePass2003	Feitian Technologies 社が開発した FIPS 認定モジュール搭載のスマートカードベースのトークンです。 PKI アプリケーション・システムのために設計されています。
CryptoAPI Interface (CAPI)	Microsoft 社が提供する暗号化、デジタル署名、認証などに関する API 群の総称です。 Windows のプラットフォーム上において、サードパーティのアプリケーションやユーザがこれらの API を利用してデータを暗号化したり、デジタル署名を付加したり、デジタル証明書の情報を取り出したりすることができます。
Smart Card Minidriver Interface	Microsoft 社によって提供された暗号化オペレーションのためのインターフェースです。 マイクロソフト・ベースのスマートカード暗号化プロバイダーおよびマイクロソフト・スマートカード鍵保管プロバイダーに対して、ハードウェアに依存しないか、ソフトウェアによってインプリメントされた暗号化アルゴリズムのカプセル化を提供します。
PKCS#11 Interface	PKCS#11 は、RSA Security 社が策定したプログラミングインターフェースです。ハードウェアに依存しない暗号化アクセラレータや、スマートカードなどの暗号化機能を持ったトークンに対するインターフェースです。