NASCA

User's Guide

目次

1　はじめに

「NASCA」は「NEC Authentication Agent」の略称です。

NASCA は、指紋、FeliCa カード、USB メモリなど、複数の認証デバイスを使用した高度な個人認証機能で、認証を受けていない人がコンピュータを使うことを防止したり、セキュリティチップを使用した強固なデータ保護をするセキュリティソフトウェアです。

「2　機能概要」、および「3　インストール／アンインストール」を読んだ後に、該当するページをご覧ください。

■本マニュアルで使用している記号／用語について

チェック　：してはいけないことや、注意していただきたいことを説明しています。
よく読んで注意を守ってください。場合によっては、作ったデータの消失、使用しているアプリケーションの破壊、パソコンの破損の可能性があります。また、全体に関する注意については、「注意事項」としてまとめて説明しています。

メモ　：利用の参考となる補足的な情報をまとめています。

参照　：マニュアルの中で関連する情報が書かれている所を示しています。

指紋センサ	：	内蔵指紋センサ（ライン型）を指します。
TPM	：	セキュリティチップを指します。
TPM PIN	：	セキュリティチップの基本ユーザーパスワードを指します。
TPM 認証	：	セキュリティチップを用いた暗号化に必要な認証を指します。 セキュリティチップの基本ユーザーパスワード(TPM PIN)を入力する必要があります。
Nasca-Admin	：	NASCA 管理者を指します。
バンクデータ	：	Web フォームバンクデータとアプリケーションバンクデータを指します。

■本マニュアルで使用しているアプリケーションなどの正式名称について

Windows Vista Business	：	Windows Vista® Business with Service Pack 1 (SP1)
Internet Explorer 7	：	Windows® Internet Explorer® 7
Word 2007	：	Microsoft® Office Word 2007
Excel 2007	：	Microsoft® Office Excel® 2007
Outlook 2007	：	Microsoft® Office Outlook ® 2007
PowerPoint 2007	：	Microsoft® Office PowerPoint® 2007

Adobe Reader	:	Adobe® Reader® 9.0 または Adobe® Reader® 9.1
Active Directory	:	Active Directory®
NASCA	:	NEC Authentication Agent

■動作環境について

本製品をインストールするには、次の環境が必要です。

[対応OS]

Windows Vista® Business with Service Pack 1 (SP1)

※日本語版のみ対応しています。
※32 ビット版のみ対応しています。
※記載されていない OS では使用できません。

■関連マニュアルについて

(お使いのモデルによっては添付されていない場合があります。)

指紋センサ
→『指紋センサ(ライン型)ユーザーズガイド』

FeliCa ポート
→『FeliCaポートマニュアル』

TPM
→『VersaPro/VersaPro J 電子マニュアル』の『セキュリティチップ ユーティリティ マニュアル』、
または『Mate/Mate J 電子マニュアル』の『セキュリティチップ ユーティリティ マニュアル』

２　機能概要

NASCA には次の機能があります。

■ユーザー情報管理機能

NASCA で使用する認証デバイスに関する情報や動作上のポリシーを管理します。

a） 認証デバイス／認証規則の管理（管理者用）

各ユーザーの認証で使用可能な認証デバイスや認証規則を管理します。

b） 認証情報／認証規則の設定

ユーザーの認証に使用する認証デバイスの情報（認証情報）と 認証デバイスの組み合わせ(認証規則)を設定します。

c） 認証ポリシーの設定

ユーザー認証を要求するタイミングを設定します。

■ユーザー認証機能

Windows パスワード以外の認証デバイス(指紋、FeliCa カード、USB メモリなど)によるデバイス認証機能を提供します。

a） Windows ログオン認証

Windows ログオン時にデバイス認証を要求します。

b） ユーザーアカウント制御

システムに変更を及ぼすアプリケーションやツール類を起動した際にデバイス認証を要求します。

c） ユーザー認証

NASCA のユーザー情報管理機能 ／Web フォームバンク機能／エクスポート機能等を使用する際にデバイス認証を要求します。

■TPM によるデータ保護

TPM を搭載した装置では、NASCA が管理するデータの一部を、TPM を用いて暗号化することができます。TPM を使用することで、より安全にデータを保護することができます。

■Web フォームバンク機能

任意の Web ページでユーザーが入力したデータを保存し、 ユーザーの入力処理を補助します。

■アプリケーションバンク機能

アプリケーションにユーザーが入力したデータを保存し、 ユーザーの入力処理を補助します。

■エクスポート／インポート機能

ユーザーの認証に関する情報やWebフォームバンクデータ、アプリケーションバンクデータをエクスポート／インポートします。

■バックアップ／リストア機能

バックアップ機能では、NASCA のデータベースの内容をファイルに保存することで、全ユーザー共通のデータやユーザーごとのデータを一括してバックアップすることができます。リストア機能では、ファイルにバックアップしたデータベースの内容を復元することができます。

■オプション機能

NASCA の設定を変更するためのオプション機能を提供します。

a)　ロック解除時の不正認証監視機能

不正なロック解除を防止するため、ロック解除時の認証試行回数を設定することができます。

b)　Windows ログオン認証画面の画像変更機能

「Windows ログオン認証」画面に表示される画像を変更することができます。

c)　個人認証デバイス利用強制機能

認証規則を設定していないユーザーに対して、Windows にログオンできる回数を制限することができます。

３　インストール／アンインストール

３－１　インストール

NASCA をインストール、または追加インストールする場合は、次の手順を行ってください。

チェック

- インストールは必ずコンピュータの管理者権限を持ったユーザー(ユーザー名は半角英数字)でログオンして行ってください。
- TPM をご使用になる場合、インストールを始める前に TPM の初期化を行ってください。初期化を行わない場合、インストール手順の途中で「登録したデータを保護するために TPM を使用します」設定を有効にできません。
- FeliCa ポートをご使用になる場合、インストールを始める前に「FeliCa Port Software」をインストールする必要があります。詳しくは、「FeliCa ポートマニュアル」をご覧ください。
- 指紋センサをご使用になる場合、インストールまたは追加インストールを行なうタイミングで、指紋センサが正しく認識されている必要があります。 デバイスの取り外しや無効化が行なわれていると指紋センサを認証デバイスとして使用できなくなる場合がありますので、ご注意ください。
- 「ユーザー情報管理機能」「エクスポート／インポート機能」「バックアップ／リストア機能」は、必ずインストールされます。
- NASCA は、ドメイン環境として Active Directory に対応しています。その他のドメイン環境では正常に動作しない可能性がありますので、ご注意ください。

3-1-1　NASCA 管理者

NASCA をお使いになるには、インストール中に NASCA の管理者(以下、「NASCA 管理者」)を設定する必要があります。

- ユーザー「Nasca-Admin」が NASCA 管理者として新規作成されます。
- NASCA 管理者は、管理者専用の機能（認証デバイス／認証規則の管理、バックアップ／リストア機能、ユーザーの初期化、オプション機能)を使用することができます。
- NASCA 管理者は、デバイスを使用した認証機能を使用することができません。

チェック

ユーザー「Nasca-Admin」がインストール前から既に存在する場合、このユーザーを管理者として設定します。 インストールを行う前に、このユーザーを管理者として設定して良いかどうかを確認してください。

3-1-2　インストール

初めて NASCA をインストールする場合は、次の手順でインストールを行ってください。

1. Windows を起動する
2. DVD/CD ドライブに「アプリケーション CD-ROM」をセットする
3. 「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「ファイル名を指定して実行」をクリック
4. 「名前」に「＜DVD/CD ドライブ名＞:¥NXSETUP.EXE」と入力して、「OK」ボタンをクリック
5. 「NEC Authentication Agent(NASCA)」を選択し、「インストール」ボタンをクリック
6. 「NASCA セットアップへようこそ」画面が表示されたら、「次へ」ボタンをクリック

7 「機能の選択」と表示されたら、インストールする機能を選択し、「次へ」ボタンをクリック

メモ

選択できる機能は、以下の通りです。

Windows ログオン認証	Windows にログオンする機能(Credential Provider)を提供します。詳しくは、「5-1　Windows ログオン認証」をご覧ください。
Web フォームバンク	Internet Explorer にツールバーを追加し、Web ページへのデータ入力を補助する機能を提供します。詳しくは、「7　Web フォームバンク機能」をご覧ください。
アプリケーションバンク	アプリケーションウィンドウへのデータ入力を補助する機能を提供します。詳しくは、「8　アプリケーションバンク機能」をご覧ください。

8 「セットアップタイプ　オプション選択」と表示されたら、オプションを選択し、「次へ」ボタンをクリック

メモ

TPM を使用しない場合は、Windows に搭載された暗号化機能によって登録したデータを保護します。TPM が搭載されている装置をお使いの場合は、セキュリティを高めるため TPM を使用することをおすすめします。

チェック

- TPM が搭載されていない装置をお使いの場合は、「登録したデータを保護するために TPM を使用します」を選択しないでインストールを行ってください。
- ここで選択したオプションの設定「登録したデータを保護するために TPM を使用します」は、インストール後に変更することができません。

9 「インストール準備の完了」と表示されたら、「インストール」ボタンをクリック

インストールが始まります。

10「管理者の設定」画面が表示されたら、「OK」ボタンをクリック

11「パスワードの設定」画面が表示されたらパスワードを入力して、「OK」ボタンをクリック

12「InstallShield Wizard の完了」と表示されたら、「完了」ボタンをクリック

13DVD/CD ドライブから「アプリケーション CD-ROM」を取り出し、Windows を再起動する

以上でインストールは完了です。

続いて、以下の設定を行ってください。

- 認証設定の管理
- バックアップの設定

参照

認証設定の管理

→「4-1　認証デバイス／認証規則の管理(管理者用)」

バックアップの設定

→「10-1　バンクデータ管理用のマスターコードの設定」、「10-2　バックアップの設定」

3-1-3 追加インストール

NASCA をインストールした後、インストールしていない機能を追加したい場合は、次の手順で追加インストールを行ってください。

1. Windows を起動する
2. DVD/CD ドライブに「アプリケーション CD-ROM」をセットする
3. 「スタート」ボタン→「コントロールパネル」をクリック
4. 「プログラム」にある「プログラムのアンインストール」をクリック
5. 「NASCA」を選択し、「変更」ボタンをクリック
6. 「ようこそ」と表示されたら、「変更」を選択し、「次へ」ボタンをクリック
7. 「機能の選択」と表示されたら、追加したい機能にチェックを入れて、「次へ」ボタンをクリック
   インストールが始まります。

8. 「メンテナンスの完了」と表示されたら、「完了」ボタンをクリック
9. DVD/CD ドライブから「アプリケーション CD-ROM」を取り出し、Windows を再起動する

以上でインストールは完了です。

３－２　アンインストール

NASCA を全てアンインストール、または一部機能をアンインストールする場合は、次の手順を行ってください。

チェック

アンインストールは必ずコンピュータの管理者権限を持ったユーザー(ユーザー名は半角英数字)でログオンして行ってください。

3-2-1　全てアンインストール

NASCA の全機能をアンインストールする場合は、以下の手順で全てアンインストールを行ってください。

1. Windows を起動する
2. 「スタート」ボタン→「コントロールパネル」をクリック
3. 「プログラム」にある「プログラムのアンインストール」をクリック
4. 「NASCA」を選択し、「アンインストール」ボタンをクリック
5. 「選択したアプリケーション、およびすべての機能を完全に削除します。」と表示されたら、「はい」ボタンをクリック
   アンインストールが始まります。
6. 「アンインストール完了」と表示されたら、「完了」ボタンをクリック
7. Windows を再起動する

以上でアンインストールは完了です。

3-2-2　一部機能をアンインストール

NASCA の一部機能をアンインストールする場合、以下の手順で一部機能をアンインストールしてください。

1. Windows を起動する
2. 「スタート」ボタン→「コントロールパネル」をクリック
3. 「プログラム」にある「プログラムのアンインストール」をクリック
4. 「NASCA」を選択し、「変更」ボタンをクリック
5. 「ようこそ」画面が表示されたら、「変更」を選択し、「次へ」ボタンをクリック
6. 「機能の選択」画面が表示されたら、削除したい機能のチェックを外して、「次へ」ボタンをクリック
   アンインストールが始まります。
7. 「一部の機能を削除します。続行しますか？」と表示されたら、「はい」ボタンをクリック
8. 「メンテナンスの完了」と表示されたら、「完了」ボタンをクリック
9. Windows を再起動する

以上でアンインストールは完了です。

４　ユーザー情報管理機能

ユーザー情報管理機能では次の情報を管理することができます。

- 認証デバイス／認証規則の管理(※)
- 認証情報／認証規則の設定
- 認証ポリシーの設定

(※は NASCA 管理者のみが情報を管理することができます)

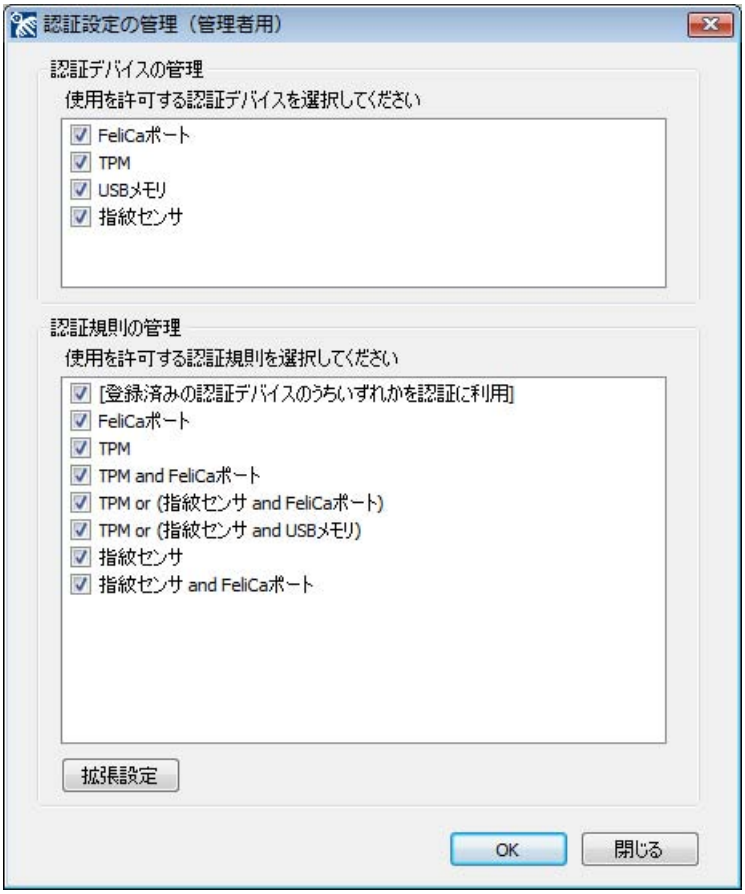
４－１　認証デバイス／認証規則の管理　(管理者用)

各ユーザーの認証に必要となる認証デバイスや認証規則を、あらかじめ用意されたものの中からひとつ以上選択し、“使用可能な”認証デバイスや認証規則を設定することができます。

「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「認証設定の管理(管理者用)」をクリック

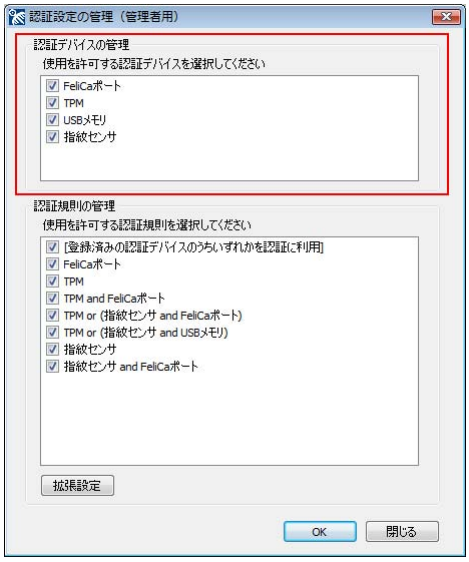
チェック

NASCA 管理者以外のユーザーでは「認証設定の管理(管理者用)」を起動できません。



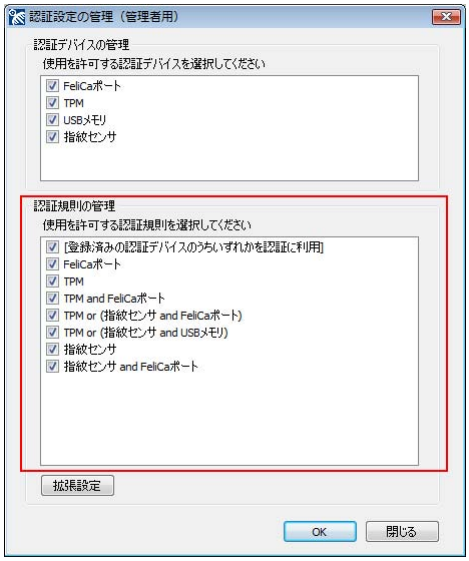
4-1-1　認証デバイスの管理

使用可能なデバイスを選択します。
ここで選択したデバイスのみ、Windows ログオン認証画面／ユーザーアカウント制御画面／ユーザー認証画面に表示されます。



4-1-2　認証規則の管理

使用可能な認証規則を選択します。
ここで選択した認証規則のみ、「4-2-3　認証規則の設定」で選択することができます。



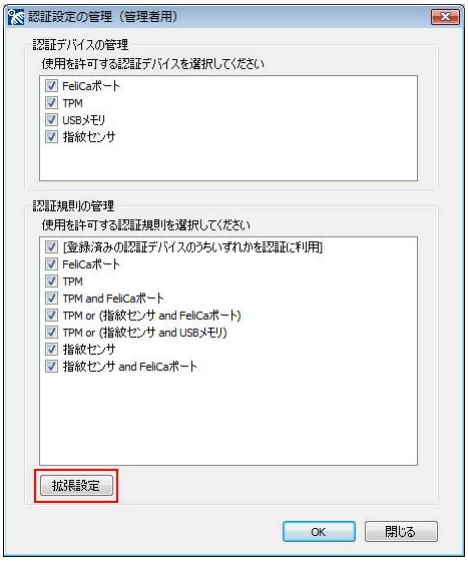
チェック

- 「4-1-1　認証デバイスの管理」で選択されていないデバイスを含む認証規則は選択することができません。
- 既に他のユーザーが設定している認証規則を、使用可能な認証規則から外した場合、そのユーザーは認証に成功しなくなりますので、ご注意ください。

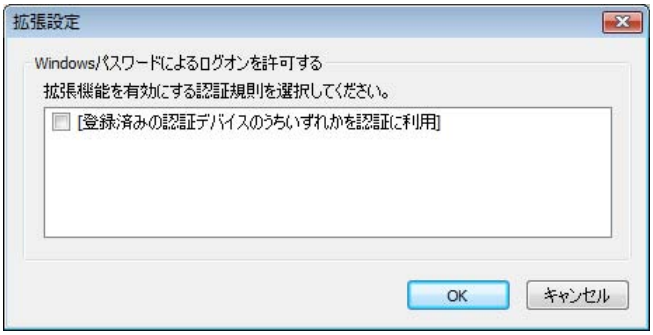
4-1-3　拡張機能の設定(管理者用)

使用可能な拡張機能を設定します。
ここで「Windows パスワードによるログオンを許可する」オプション設定を有効にした認証規則にのみ「4-2-3　認証規則の設定」で「Windows パスワードによるログオンを許可する」オプション設定を行うことができます。

1 「認証設定の管理(管理者用)」画面が表示されたら、「拡張設定」ボタンをクリック



2 「拡張設定」画面が表示されたら、「Windows パスワードによるログオンを許可する」オプション設定を有効にする認証規則を選択し、「OK」ボタンをクリック



チェック

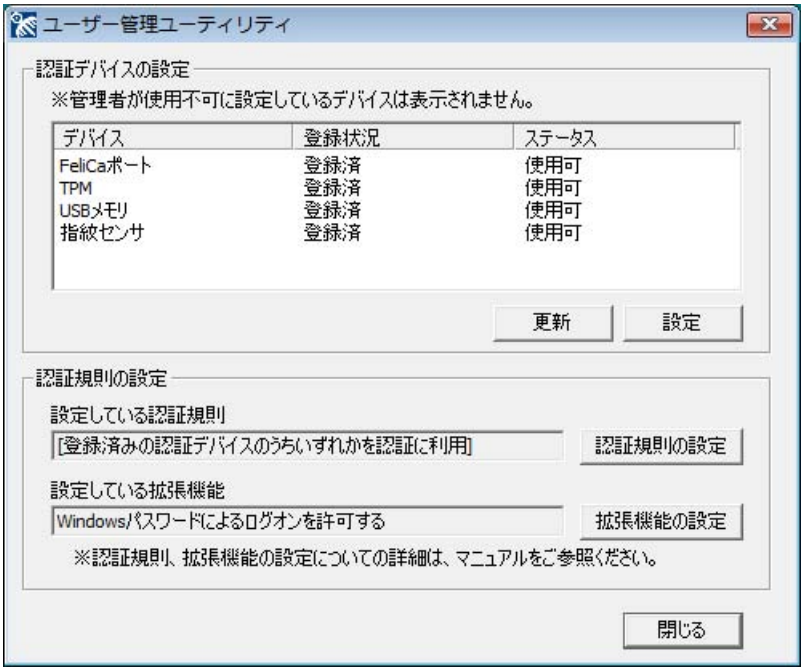
- 「Windows パスワードによるログオンを許可する」オプション設定に対応している認証規則は、「[登録済みの認証デバイスのうちいずれかを認証に利用]」のみです。

以上で拡張機能の設定は完了です。

４－２　認証情報／認証規則の設定

認証規則の選択と、認証に必要なデバイス情報の登録をユーザーごとに行います。

「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「ユーザー管理ユーティリティ」をクリック
「ユーザー管理ユーティリティ」が表示されます。



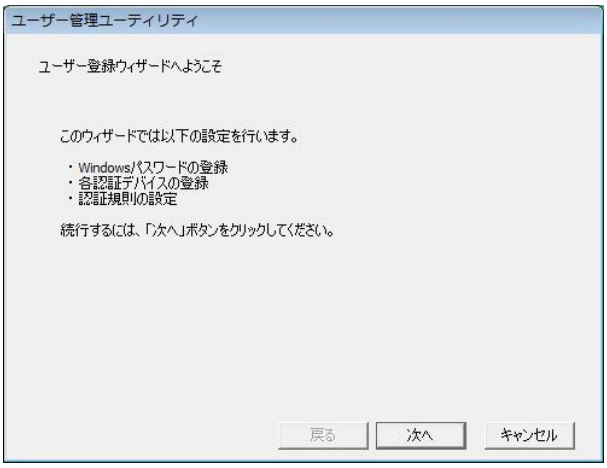
チェック

- NASCA 管理者は「ユーザー管理ユーティリティ」を起動できません。
- 初めて「ユーザー管理ユーティリティ」を起動した場合は、「ユーザー登録ウィザード」が表示されます。「4-2-1　ユーザー登録を行う」をご覧になり、ユーザーの登録を行ってください。
- ユーザー登録完了後は、「ユーザー管理ユーティリティ」起動時にユーザー認証が必要になります。

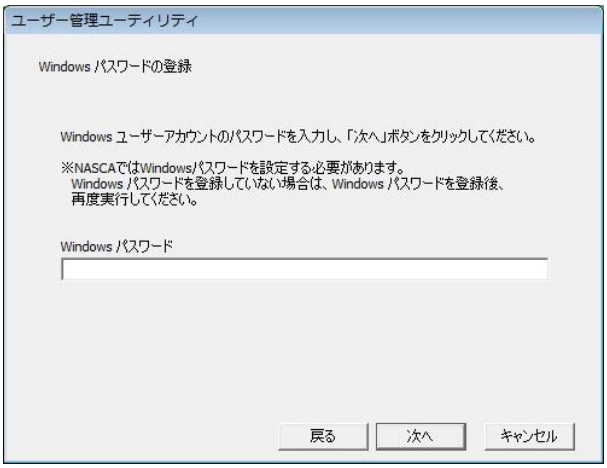
4-2-1　ユーザー登録を行う

初めて「ユーザー管理ユーティリティ」を起動した場合、「ユーザー登録ウィザード」が表示されます。

1　**「ユーザー登録ウィザードへようこそ」と表示されたら、「次へ」ボタンをクリック**



2　**「Windows パスワードの登録」と表示されたら、パスワードを入力し、「次へ」ボタンをクリック**



チェック

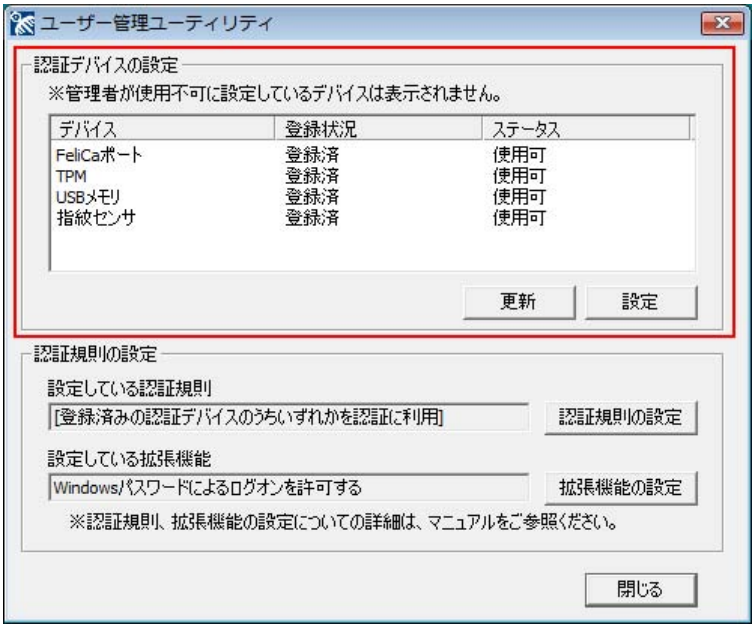
NASCA では、Windows パスワードを設定する必要があります。ユーザーの Windows パスワードが設定されていない場合は、いったん「ユーザー登録ウィザード」を閉じ、Windows パスワードの設定後、再度実行してください。

以上でユーザー登録は完了です。

引き続き、認証情報／認証規則の設定を行います。
詳細については、「4-2-2　認証情報の設定」、「4-2-3　認証規則の設定」、「4-2-4　拡張機能の設定」をご覧ください。

4-2-2　認証情報の設定

デバイス認証に使用するデバイスの認証情報を登録／削除／参照することができます。
認証情報を登録したいデバイスを選択し、「設定」ボタンをクリックし、各認証デバイスの設定を行います。



参照

設定方法については「4-3　認証デバイスの設定方法」をご覧ください。

チェック

「4-1-1　認証デバイスの管理」で選択されていない認証デバイスは表示されません。

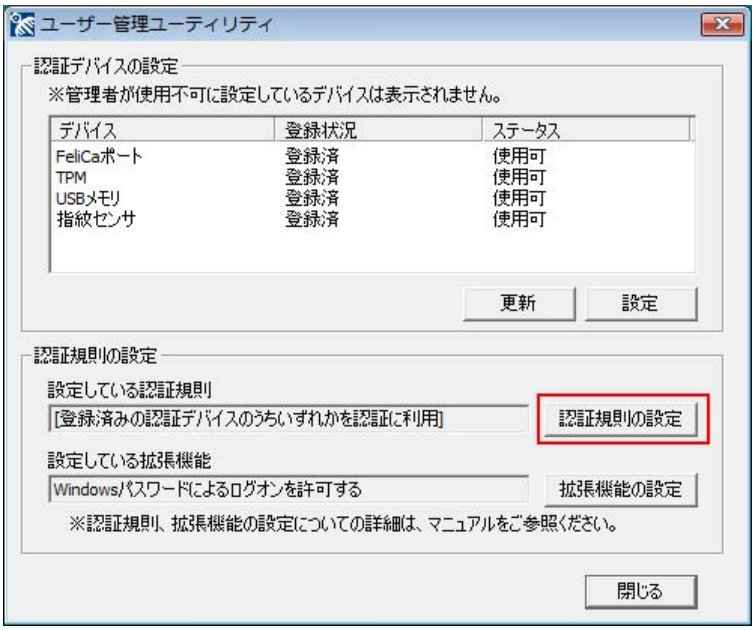
メモ

「ステータス」欄には、デバイスの使用可否状態が表示されます。「ユーザー管理ユーティリティ」起動中にデバイスを取り外すなどして、「ステータス」欄の表示状態と実際の状態に差が生じてしまった場合は、「更新」ボタンをクリックすることで表示を最新の状態に更新することができます。

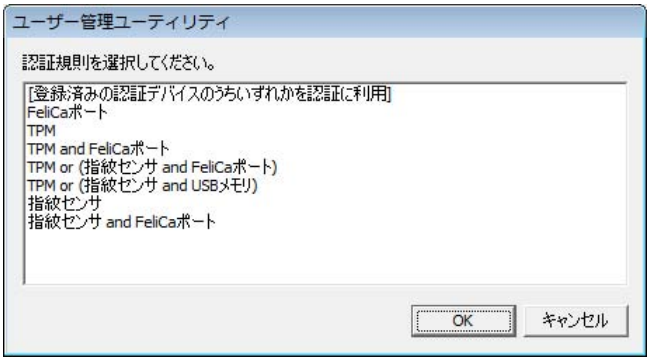
4-2-3 認証規則の設定

デバイス認証時に利用する認証規則を設定します。

1 「ユーザー管理ユーティリティ」画面で、「認証規則の設定」ボタンをクリック



2 認証規則を選択する画面が表示されたら、デバイス認証で使用する認証規則を選択し、「OK」ボタンをクリック



チェック

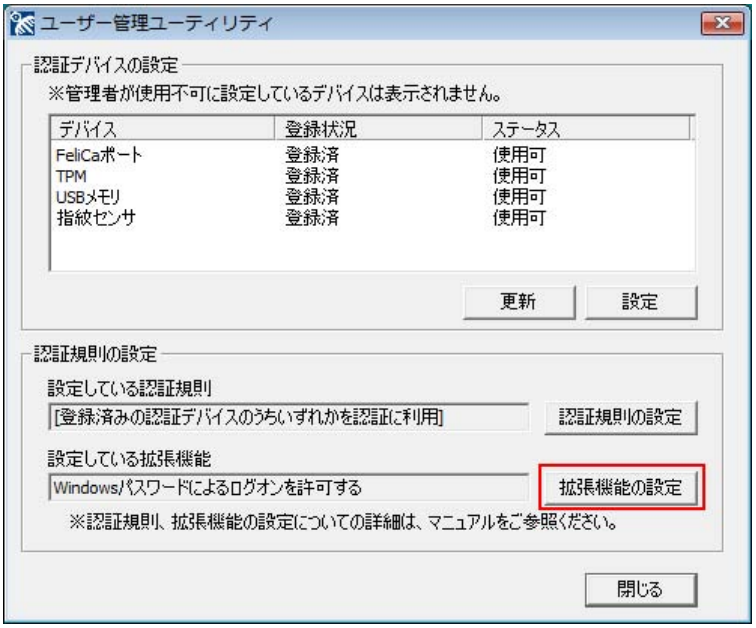
- 「4-1-2 認証規則の管理」で選択されていない認証規則は表示されません。
- 「4-2-2 認証情報の設定」で、認証情報の登録を行っていないデバイスを含む認証規則は表示されません。
- 認証規則は、初期状態では「未登録」となっているため、認証規則を設定しなければデバイス情報を登録しても、デバイス認証を利用することができません。

以上で認証規則の設定は完了です。

4-2-4 拡張機能の設定

認証規則に対する拡張機能の設定を行います。

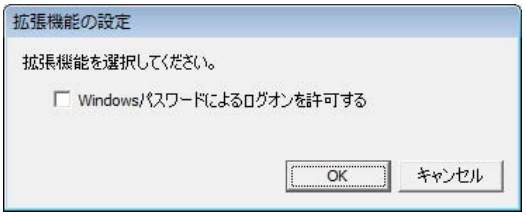
1 「ユーザー管理ユーティリティ」画面で、「拡張機能の設定」ボタンをクリック



チェック

- 「4-1-3 拡張機能の設定(管理者用)」でオプション設定を有効にしていない場合、「ユーザー管理ユーティリティ」画面に、「設定している拡張機能」と「拡張機能の設定」ボタンは表示されません。
- 認証規則を[登録済みの認証デバイスのうちいずれかを認証に利用]に設定していない場合、「拡張機能の設定」ボタンをクリックすることはできません。

2 「拡張機能の設定」画面が表示されたら、「Windows パスワードによるログオンを許可する」にチェックをし、「OK」ボタンをクリック



※ 初期状態では「Windows パスワードによるログオンを許可する」にチェックが入っていません。
※ 「Windows パスワードによるログオンを許可する」オプション設定を行った場合、Windows ログオン認証時に、認証規則の設定後も Windows パスワードによるログオンが可能になります。

チェック

- 「Windows パスワードによるログオンを許可する」オプション設定に対応している認証規則は、[登録済みの認証デバイスのうちいずれかを認証に利用]のみです。

- Windows ログオン認証時のみ、パスワードによる認証が可能になります。
  ユーザー管理ユーティリティ起動時などに要求される、Windows ログオン後のユーザー認証では、Windows パスワードによる認証はご利用になれません。

以上で拡張機能の設定は完了です。

メモ

認証情報を登録したデバイスを紛失したときに、Windows にログオンできなくなることを防ぐため、Windows パスワードによるログオン機能を利用することをおすすめします。

４－３　認証デバイスの設定方法

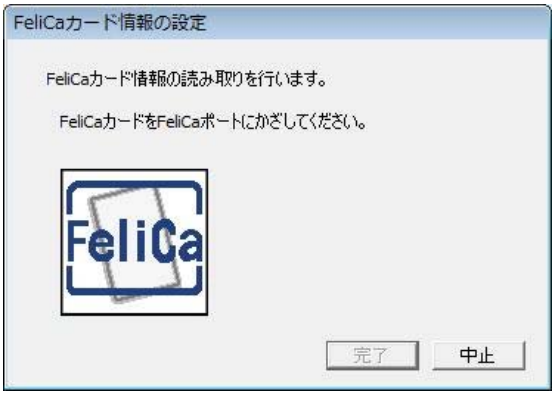
4-3-1　FeliCa カード情報の設定

ユーザーごとに3つまで、FeliCa カード情報の登録、削除、および名称変更を行うことができます。

チェック

現在 NASCA が対応しているのは、Edy 機能搭載カードのみです。

※　「登録情報」欄左部分にデバイス名称、右部分にデバイス情報が表示されます。
※　デバイス名称を設定していない場合は、デバイス名称部分は空白で表示されます。
※　デバイスを登録していない場合は、デバイス情報部分は“未登録”と表示されます。

登録	FeliCa カード情報を登録します。  認証デバイスとして登録するFeliCaカードを、FeliCaポートにかざしてください。カードが正常に認識されると、「この FeliCa カード情報を登録します。」と表示されます。

名称変更	登録した FeliCa カード情報に対して、名称を設定することができます。  FeliCa カード情報を登録していない場合は、名称を設定することができません。
削除	登録済みの FeliCa カードの情報を削除します。

チェック

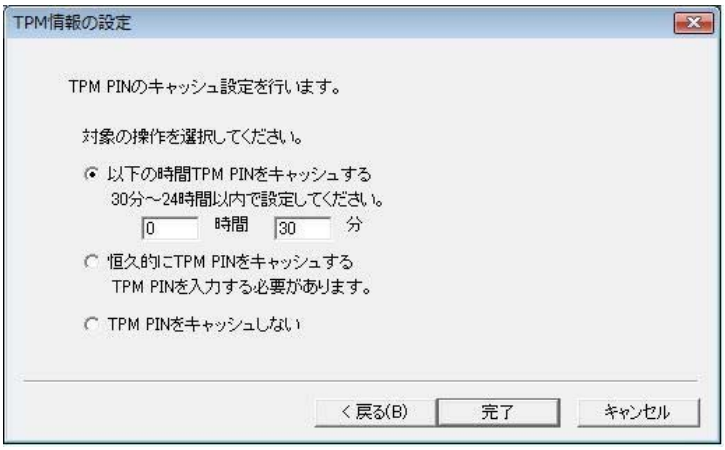
登録済みのFeliCaカード情報に対して名称を設定した状態で、登録済みのFeliCaカード情報の削除や上書きをすると、設定した名称も削除されます。

4-3-2 TPM 情報の設定

TPM PIN をキャッシュする時間の設定を行うことができます。

メモ

TPM 認証のために入力した TPM PIN はここで設定された時間内はキャッシュ(保存)されます。
TPM PIN がキャッシュされている間は、TPM 認証が自動的に行われるため、TPM によって保護されたデータにアクセスする場合でも、TPM PIN を入力する必要がなくなります。
TPM によるデータの保護については、「6 TPM によるデータ保護」をご覧ください。



以下の時間 TPM PIN をキャッシュする	30 分～24 時間以内で TPM PIN をキャッシュする時間を設定することができます。
恒久的に TPM PIN をキャッシュする	恒久的に TPM PIN をキャッシュします。 正しい TPM PIN を入力する必要があります。 
TPM PIN をキャッシュしない	TPM PIN をキャッシュしません。

チェック

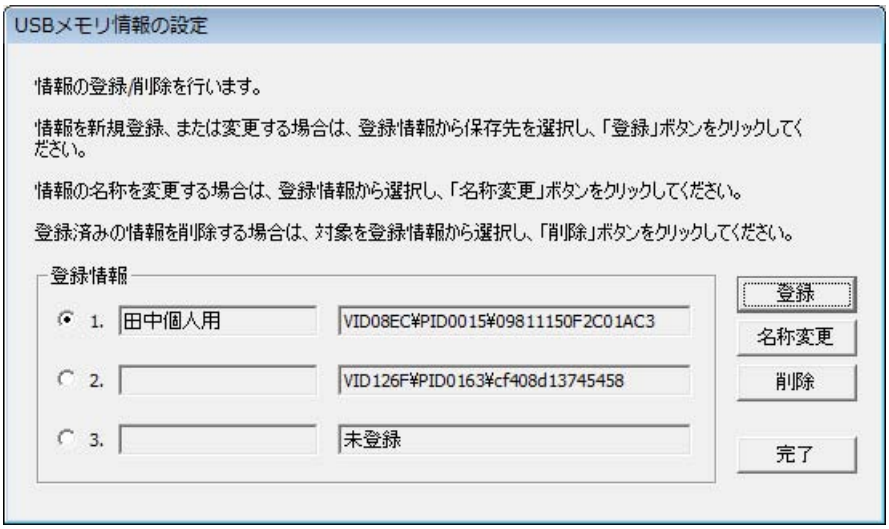
- TPM PIN がキャッシュされている状態で、TPM PIN を変更した場合は、必ずキャッシュ時間の設定をし直してください。
- ログオフやユーザーの切り替えを行うと、キャッシュが消去される場合があります。そのような場合は、必要に応じて再度 TPM PIN の入力をするか、あらかじめ恒久的に TPM PIN をキャッシュするように設定し直してください。

4-3-3 USB メモリ情報の設定

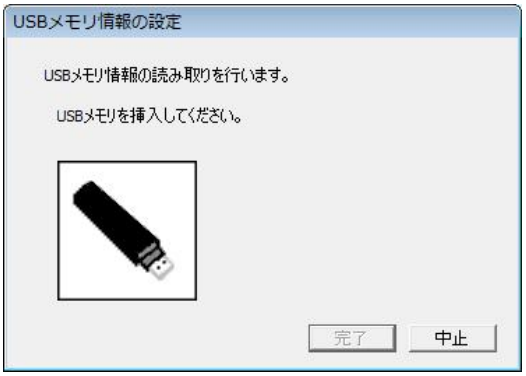
ユーザーごとに3つまで、USB メモリ情報の登録、削除、および名称変更を行うことができます。

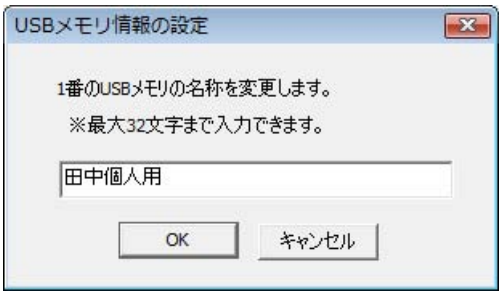
チェック

- 認証には、USB メモリの固有情報であるシリアルナンバーを利用します。シリアルナンバーを持たない USB メモリはご利用になれません。
- 特殊な機能（USB メモリへアクセスする際に認証を要求する機能など）を持った USB メモリは、認証デバイスとして正しく動作しない場合があります。
- 登録を行う際には、登録したい USB メモリ以外の USB メモリは取り外してください。
- USB メモリを4つ以上接続した場合は、認証デバイスとしては正しく動作しません。
- USB メモリをお使いになる場合は、本体の USB ポート、またはセレクションで用意されている USB キーボード本体の USB ポートに接続してください。



※ 「登録情報」欄左部分にデバイス名称、右部分にデバイス情報が表示されます。
※ デバイス名称を設定していない場合は、デバイス名称部分は空白で表示されます。
※ デバイスを登録していない場合は、デバイス情報部分は“未登録”と表示されます。

登録	USB メモリ情報を登録します。  認証デバイスとして登録するUSBメモリをUSBポートに挿入してください。USB メモリが正常に認識されると、「この USB メモリ情報を登録します。」と表示されます。

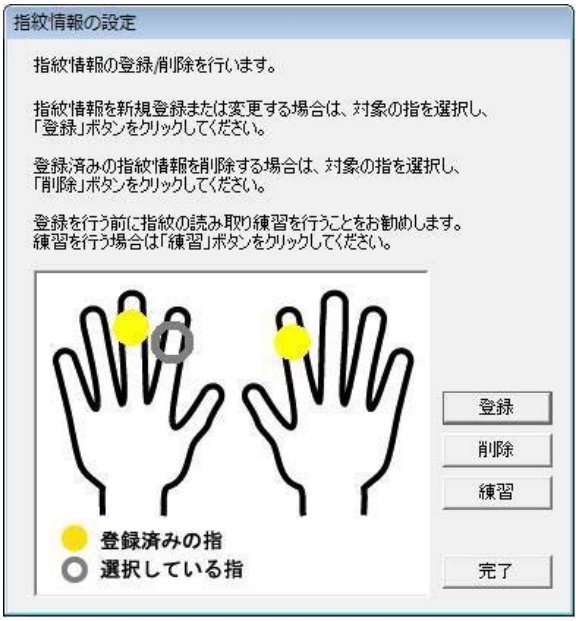
名称変更	登録した USB メモリ情報に対して、名称を設定することができます。  USB メモリ情報を登録していない場合は、名称を設定することができません。
削除	登録済みの USB メモリの情報を削除します。

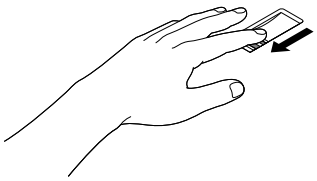
チェック

登録済みの USB メモリ情報に対して名称を設定した状態で、登録済みの USB メモリ情報の削除や上書きをすると、設定した名称も削除されます。

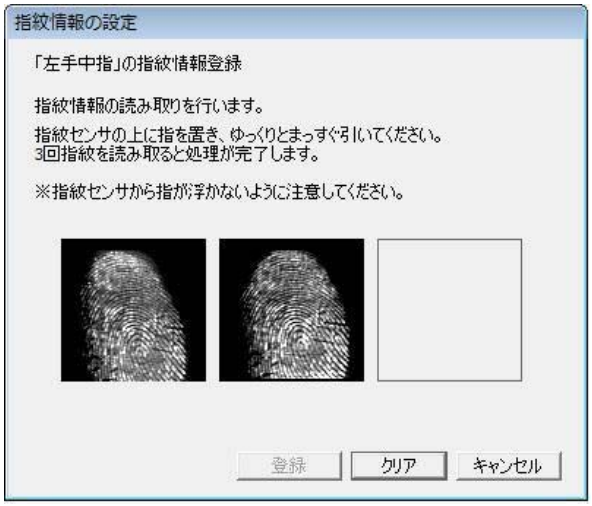
4-3-4 指紋情報の設定

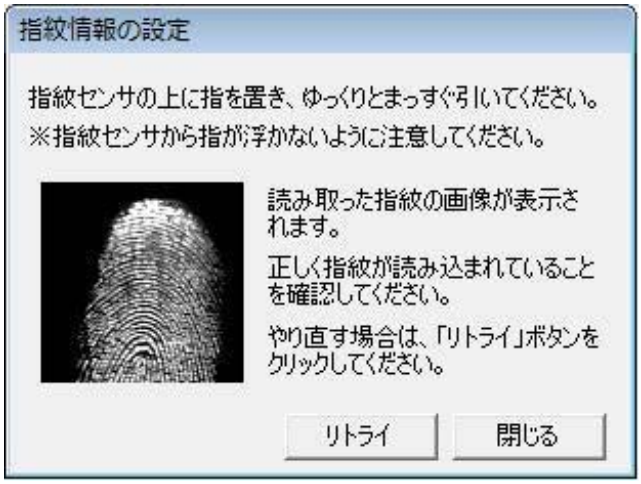
ユーザーごとに、各指の指紋情報の登録、削除を行うことができます。





※　既に登録が完了している指は、黄色で表示されます。

登録	指紋情報の登録を行います。  指紋の読み取りを 3 回行います。登録する指を 3 回読み取らせてください。 指紋情報が正常に読み取られると「指紋情報の読み取りが完了しました。」と表示されます。 3 回読み取れても、3 枚の画像の中で 1 枚でも画像が乱れたり、白くすれているような場合は、運用時の認識率低下につながる場合がありますので、「クリア」ボタンを押して登録し直してください。

削除	登録済みの指紋情報を削除します。
練習	指紋の読み取りの練習を行うことができます。 

メモ

指紋の登録は登録しやすい指を、複数本登録されることをおすすめします。

次のような場合は、指紋の登録が難しいことがあります。

- 汗や脂が多く、指紋の間が埋まっている
- 極端に乾いている
- 指紋が小さすぎる
- 指紋が大きすぎる
- 指紋が渦を巻いていない
- 手が荒れている
- 摩耗により指紋が薄い

汗や脂が多い場合には指をよく拭き、 手荒れや乾いている場合にはクリームなどを塗ることにより改善される場合があります。
また、指先が小さい場合は、なるべく大きな親指などで登録してください。
また、次のような場合には、指紋の特徴が変化し、照合時に不一致が起きやすくなります。

- 夏期など、汗や脂が多い場合
- 冬期など、極端に乾いている場合
- 手が荒れたり、けがをしたりした場合
- 急に太ったり、痩せたりした場合

登録が難しい場合は、照合時にも不一致がおきやすい傾向があります。
すべての指が登録しにくい場合には、同じ指を複数本登録することで、照合時の不一致がおきにくくなります。

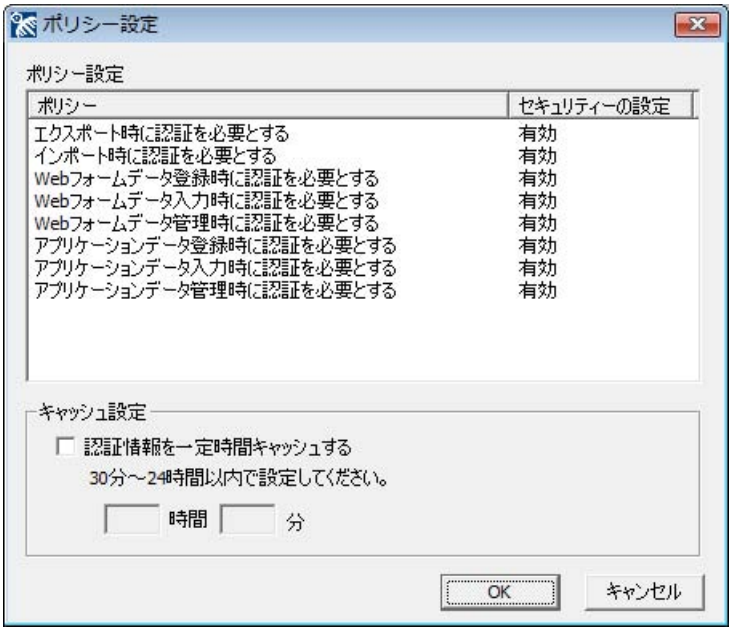
以上で認証デバイスの設定は完了です。

４－４　認証ポリシーの設定

NASCA を使用する上で、ユーザー認証を要求するタイミング、ユーザー認証のキャッシュ時間をユーザーごとに設定することができます。

「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「ポリシー設定」をクリック

「ポリシー設定」が表示されます。

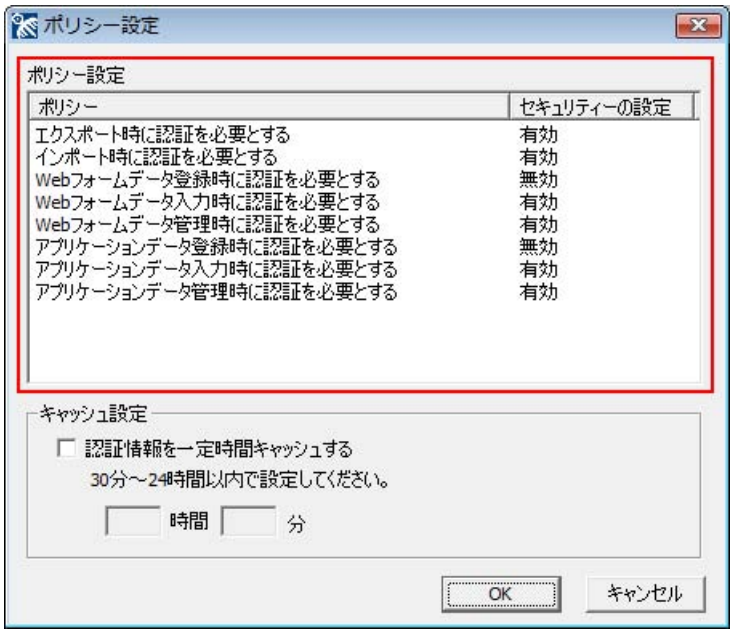


チェック

- NASCA 管理者は「ポリシー設定」を起動できません。
- ポリシー設定起動時には、必ずユーザー認証が要求されます。

4-4-1　認証ポリシーの設定

ユーザー認証を要求するタイミングを設定します。



※　初期状態では設定内容は全て有効となっています。

1　**「ポリシー設定」画面が表示されたら、設定を行うポリシーを選択し、ダブルクリック**
「詳細ダイアログ」が表示されます。

2　**ポリシーの設定を行い、「OK」ボタンをクリック**

3　**各ポリシーの設定を行ったら、「ポリシー設定」画面の「OK」ボタンをクリック**

以上で認証ポリシーの設定は完了です。

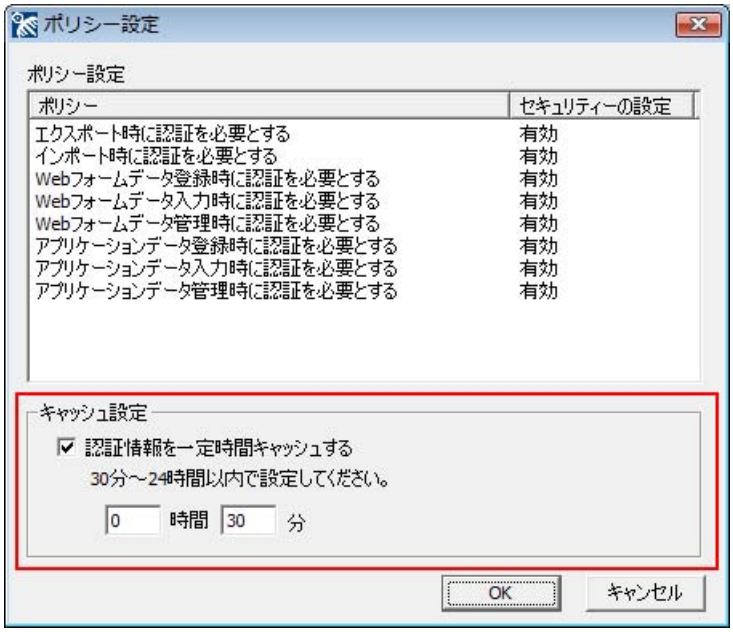
4-4-2 ユーザー認証のキャッシュ時間の設定

ユーザー認証のキャッシュ時間を設定します。

メモ

ユーザー認証のキャッシュ機能を有効にした場合、Windows ログオン認証やユーザー認証に成功した結果を、設定した時間内だけキャッシュ(保存)することができます。ユーザー認証がキャッシュされている間はポリシー設定で認証が必要とされている操作を行う場合でも、ユーザー認証が要求されなくなります。

1 「ポリシー設定」画面が表示されたら、「認証情報を一定時間キャッシュする」にチェックを入れ、認証情報のキャッシュ時間を 30 分～24 時間の範囲で入力します



※ 初期状態では、キャッシュ機能は無効です。

2 キャッシュの設定を行ったら、「ポリシー設定」画面の「OK」ボタンをクリック

メモ

- ユーザー認証のキャッシュ機能を利用しない場合は「認証情報を一定時間キャッシュする」のチェックを外してください。
- ログオフやユーザーの切り替えを行うと、キャッシュが消去される場合があります。

以上でユーザー認証のキャッシュ時間の設定は完了です。

５　ユーザー認証機能

５－１　Windows ログオン認証

Windows へログオンする際や、コンピュータのロックを解除する際に、様々な認証デバイスを使用することができます。

あらかじめ設定された認証規則に必要な認証情報の読み取りや、パスワードの入力が全て完了したら、矢印ボタンをクリックしてください。

- 認証デバイスからの認証情報の読み取りが完了すると、各デバイス名の横に［READ］と表示されます。
- 認証デバイスの状態が不正な場合、デバイス名の横に×が表示されます。また、TPM の状態が不正な場合、TPM の入力フォームは表示されません。
- TPM を認証に使用する場合は、その他のデバイスからの認証情報の読み取りが完了したあとで、TPM PIN を入力し、最後に矢印ボタンをクリックしてください。

メモ

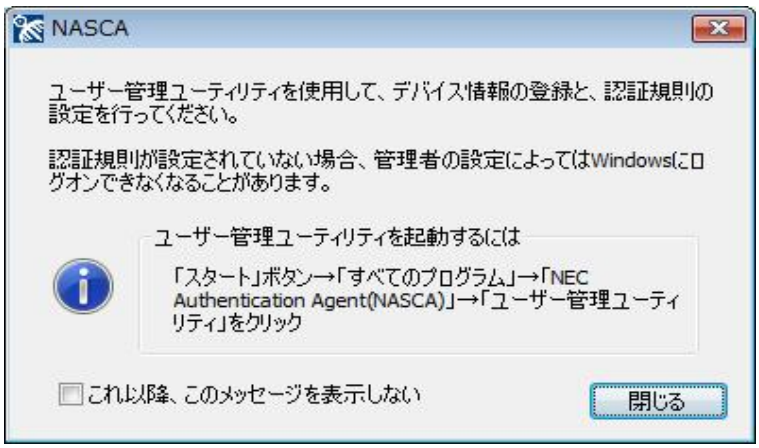
- 認証デバイスからの認証情報を読み取るには、以下の操作を行ってください。

指紋	指紋センサ上に指を置き、ゆっくりと引いてください。
USB メモリ	USB ポートに USB メモリを挿入してください。
FeliCa カード	FeliCa ポートに FeliCa カードをかざしてください。

- 認証に必要な情報の読み取りが全て正しく完了した場合、矢印ボタンをクリックせずに、自動的にログオンすることができる場合があります。 認証に必要な情報の読み取りが完了しても、自動的にログオンすることができない場合は、認証情報の読み取りを再度行うか、矢印ボタンをクリックしてください。
- USB メモリは、最大3つまで同時に接続した状態で認証を行うことができます。USB メモリを4つ以上接続した場合は、認証デバイスとしては正しく動作しません。
- Windows ログオン認証機能を使用するには、「Windows ログオン認証」をインストールする必要があります。詳しくは、「3-1 インストール」をご覧ください。

参照
- 認証情報／認証規則の登録方法については、「4 ユーザー情報管理機能」をご覧ください。
- 認証規則を設定していないユーザーのログオン制限の設定については、「11-3 個人認証デバイス利用強制機能」をご覧ください。

チェック
- 認証規則を設定していない場合（ユーザーの初回ログオン時含む）は Windows パスワードを入力して Windows へログオンしてください。
  - ✓ NASCA 管理者が、認証規則を設定していないユーザーのログオンを制限している場合、正しい Windows パスワードを入力しても Windows へログオンできない場合があります。詳しくは、「11-3 個人認証デバイス利用強制機能」をご覧ください。
  - ✓ 認証規則を設定していないユーザーでログオンすると、以下の画面が表示されます。この画面を非表示にするには、「ユーザー管理ユーティリティ」で認証規則を設定するか、ダイアログの「これ以降、このメッセージを表示しない」をチェックしてください。



- 認証規則を設定したアカウントは、初期状態では Windows パスワードは使用できません。Windows ログオン時に認証デバイスと併用して Windows パスワードを利用したい場合は「4-2-4 拡張機能の設定」をご覧ください。
- NASCA をインストールしたコンピュータへのリモートデスクトップ接続を利用したリモート接続を行う場合、認証で利用可能なデバイスは TPM に限られます。また、Windows パスワードによるログオンが許可されている場合は、Windows ログオン時のみ、Windows パスワードによる認証も利用可能です。
  接続先コンピュータのユーザーアカウントの認証規則が、TPM が利用可能な認証規則に設定されているか、または Windows パスワードによるログオンが許可されているか確認してください。
  認証規則の設定については、「4-2-3 認証規則の設定」をご覧ください。

なお、リモートデスクトップ接続は社内 LAN 等を想定した小規模なネットワーク環境での動作確認を行っています。インターネット網の経由など、ご利用のネットワーク環境によっては、リモート接続できない可能性があります。

- NASCA は、ドメイン環境として Active Directory に対応しています。その他のドメイン環境では正常に動作しない可能性がありますので、ご注意ください。

５－２　ユーザーアカウント制御

システムに変更を及ぼすアプリケーションやツール類を起動した際に、「ユーザーアカウント制御」画面が表示され、認証を要求される場合があります。「ユーザーアカウント制御」画面では、管理者権限を持ったユーザーで認証を行ってください。

Windows ログオン認証と同様に、認証に必要な情報の入力や、デバイスからの情報の読み取りを行い、「OK」ボタンをクリックしてください。

メモ

- NASCA をインストールしたコンピュータをドメインに参加させる場合なども、「ユーザーアカウント制御」画面と同様に NASCA の認証画面が表示される場合があります。
- 認証を行うユーザーのドメイン名が表示されていない場合は、ユーザー名を ”<ドメイン名>¥<ユーザー名>” の形式で入力してください。コンピュータをドメインに参加させる場合は、この形式で入力してください。

５－３　ユーザー認証

ユーザー管理ユーティリティなどで、ユーザーの機密情報(認証情報／認証規則)に関する設定を行う場合や、ポリシー設定で認証が必要とされている操作を行う際に、「ユーザー認証」画面が表示され、ユーザー認証が求められます。

Windows ログオン認証と同様に、認証に必要な情報の入力や、デバイスからの情報の読み取りを行い、「OK」ボタンをクリックしてください。

チェック

- 認証規則の設定が完了していない場合は、「ユーザー認証」画面右下の「パスワード＞＞」ボタンをクリックした後、パスワード欄に Windows パスワードを入力してください。
  なお、認証規則の設定が完了した後は、Windows パスワードによる認証はご利用になれません。
- ユーザー認証のキャッシュを設定している場合、ユーザー認証が要求されない場合があります。
  詳しくは「4-4-2 ユーザー認証のキャッシュ時間の設定」をご覧ください。

６　TPM によるデータ保護

TPM を搭載した装置では、NASCA が管理するデータの一部を、TPM を用いて暗号化することができます。TPM を使用することで、より安全にデータを保護することができます。

メモ

TPM によるデータ保護を行うかどうかは、インストール時のみ選択することができます。
詳しくは、「3-1　インストール」をご覧ください。

６－１　TPM 認証

Web フォームバンク機能／アプリケーションバンク機能で管理するデータの一部は、TPM を用いた暗号化によって保護されます。TPM を用いた暗号化を行うためには TPM 認証を行う必要があるため、以下の機能を使用中に「TPM 認証」画面が表示される場合があります。

- Web フォームバンク機能
- アプリケーションバンク機能
- インポート／エクスポート機能

正しい TPM PIN を入力し、「OK」ボタンをクリックしてください。
ただし TPM PIN がキャッシュされている場合は、認証は求められません。

参照

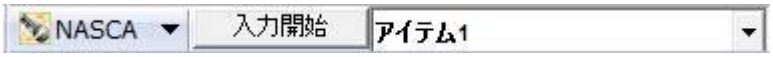
TPM PIN のキャッシュに関する設定方法は、「4　ユーザー情報管理機能」をご覧ください。

チェック

- インストール時に「登録したデータを保護するために TPM を使用します」を選択していない場合、TPM による暗号化が行われないため、TPM 認証は行われません。TPM を使用しない場合は、Windows に搭載された暗号化機能によって登録したデータを保護します。
- TPM の初期化が完了していない場合や、TPM が無効になっている場合は、Web フォームバンク機能／アプリケーションバンク機能を使用することができません。あらかじめ TPM が使用可能な状態であることを確認してください。
- TPM が破損してしまった場合やクリアされてしまった場合、Web フォームバンク機能／アプリケーションバンク機能が使用できなくなってしまう場合があります。 この場合でも TPM の復元を行うことによって、再度 Web フォームバンク機能／アプリケーションバンク機能が使用可能になる場合がありますので、TPM のバックアップを定期的に行うことをおすすめします。
  TPM のバックアップと復元については、TPM のマニュアルをご覧ください。

7　Web フォームバンク機能

Internet Explorer に追加される以下のツールバーを使用して、Web ページに入力されているデータを取得し、データベースに保存、管理する機能です。
データを保存した Web ページを表示した際に、以前保存したデータを自動的に入力することができます。



メモ

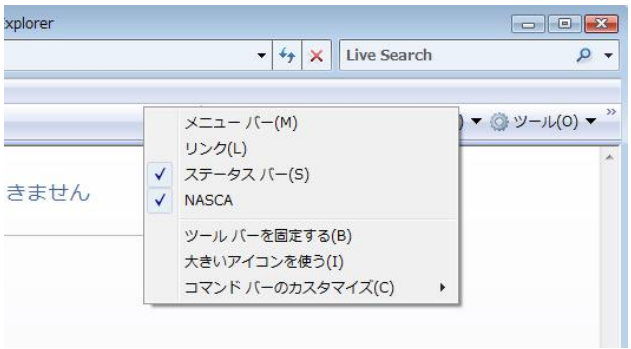
- Web フォームバンク機能を使用するには、「Web フォームバンク」をインストールする必要があります。詳しくは、「3-1 インストール」をご覧ください。
- インストール時に「登録したデータを保護するために TPM を使用します」を選択している場合、Web フォームバンク機能で管理するデータの一部は、TPM を用いた暗号化によって保護されます。TPM を用いた暗号化を行うためには、TPM 認証を行う必要があります。TPM 認証については、「6 TPM によるデータ保護」をご覧ください。
- Web フォームバンク機能をインストールした場合、ご使用の環境によっては Web サイトを表示するときに時間がかかる場合があります。
- Web フォームバンク機能は、Internet Explorer 7 で動作確認を行なっています。

チェック

Internet Explorer に NASCA のツールバーが表示されない場合は、以下の手順で設定を行ってください。

1 「スタート」ボタン→「Internet Explorer」をクリック
「Internet Explorer」が表示されます。

2 Internet Explorer のツールバー上で右クリックをし、メニューから「NASCA」を選択



チェック

Web フォームバンク機能をご使用になる前に、以下の手順で初期設定を行ってください。

1 Internet Explorer ツールバーより「オプション設定」メニューを選択
「オプション設定」が表示されます。

2 「オプション設定」で設定を確認し、必要があれば設定を変更

3 「OK」ボタンをクリック

７－１　Web フォームバンクデータ登録

Web フォームバンク機能で、以下のデータを登録することができます。

テキスト	テキストデータを保存します。
パスワード	パスワードを保存します。
ラジオボタン	ラジオボタンの選択情報を保存します。
チェックボックス	チェックボックスのチェックの有無を保存します。
選択メニュー	プルダウンメニューなどを保存します。
複数行テキスト	複数行に渡るテキストデータを保存します。

以下の手順で使用する機能を選択してください。

1 「スタート」ボタン→「Internet Explorer」をクリック
「Internet Explorer」が表示されます。

2 Internet Explorer のツールバーにある「NASCA ▼」をクリック

7-1-1 登録

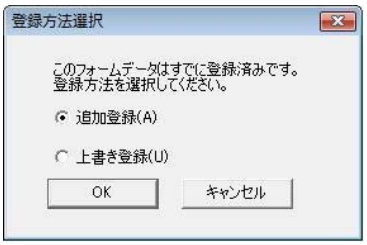
Internet Explorer ツールバーより「登録」メニューを選択すると、Web ページに入力されているデータの登録を行うことができます。

チェック

登録可能なデータがない Web ページを登録することはできません。

1 **表示中の Web ページ内にある Web フォームに必要なデータを入力し、Internet Explorer ツールバーの「登録」メニューを選択**

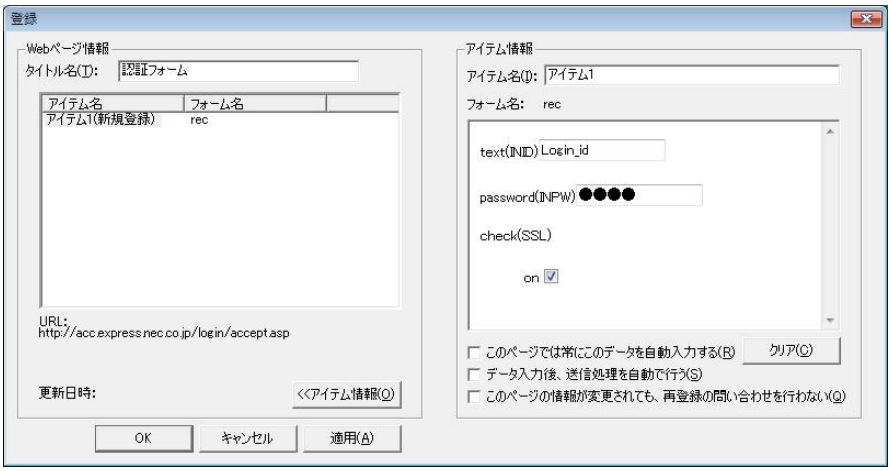
2 **「登録方法選択」画面が表示されたら、「追加登録」／「上書き登録」のどちらかを選択し、「OK」ボタンをクリック**



メモ

表示中の Web ページのデータを初めて登録する場合は、この画面は表示されません。

3 **「登録」画面が表示されたら、登録を行うアイテム名を選択する**



メモ

「クリア」ボタンをクリックすると、編集したアイテム情報が元に戻ります。

このページでは常にこのデータを自動入力する	この Web ページが表示された際に、このアイテムのデータを自動的に入力します。 1 つの Web ページに対して、1 つのアイテムのみ設定を行うことができます。その他のアイテムは同時に設定できません。新規に設定した場合、以前設定していたアイテムの「このページでは、常にこのデータを自動入力する」設定は無効になります。

データ入力後、送信処理を自動で行う	登録したデータの入力完了後、データの送信処理(「OK」／「送信」ボタンのクリック等)を自動的に行い、次の画面に進みます。
このページの情報が変更されても、再登録の問い合わせを行わない	このWebページのフォームの構成が変更された際に、再登録を行う問い合わせを行いません。

4 「アイテム情報」欄に必要なデータを入力する
5 「OK」ボタンをクリック

以上で登録は完了です。

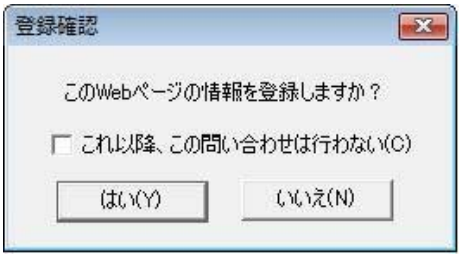
7-1-2 登録 (自動登録)

自動登録機能が有効になっている場合、 Internet Explorer ツールバーで「登録」メニューを選択しなくても、登録を行うことができます。

参照

自動登録機能の設定方法については、「7-1-5 オプション設定」をご覧ください。

1 Internet Explorer で登録したい Web ページを表示する
2 表示中の Web ページ内にある Web フォームに必要なデータを入力し、データの送信を実行(「OK」「送信」などのボタンをクリック)
3 「登録確認」画面が表示されたら、「はい」ボタンをクリック



メモ

- オプション設定「Web フォーム登録の問い合わせを行う」が有効になっていない場合、この画面は表示されません。
- 「これ以降、この問い合わせは行わない」を有効にすると、これ以降「登録確認」画面が表示されません。また、オプション設定「Web フォーム登録の問い合わせを行う」が無効になります。

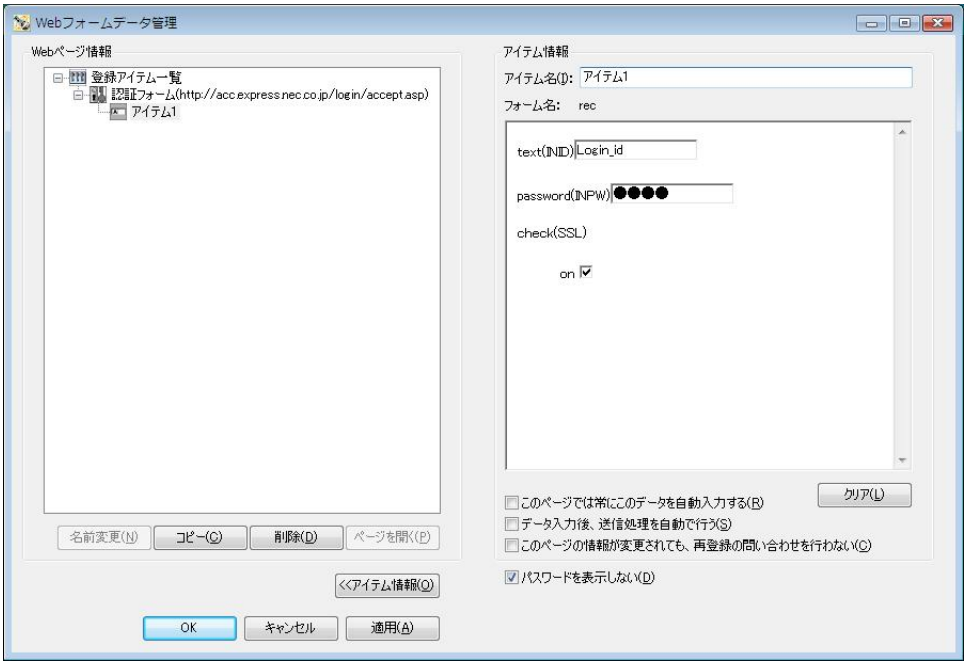
以降の手順は、「7-1-1 登録」をご覧ください。

7-1-3 データ管理

Internet Explorer ツールバーより「データ管理」メニューを選択すると、アイテムの一覧が表示され、アイテムの名前変更、コピー、削除、およびアイテム内の各データの編集を行うことができます。

メモ

「Web フォームデータ管理」は「スタート」メニューからも起動させることができます。
「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「Web フォームバンク設定」をクリックしてください。



Web ページ情報欄はツリー構造で表示されます。

Web ページを選択時	名前変更	名前を変更します。
	削除	Web ページを削除します。
	ページを開く	選択した Web にアクセスします。
アイテムを選択時	コピー	アイテムをコピーします。
	削除	アイテムを削除します。

メモ

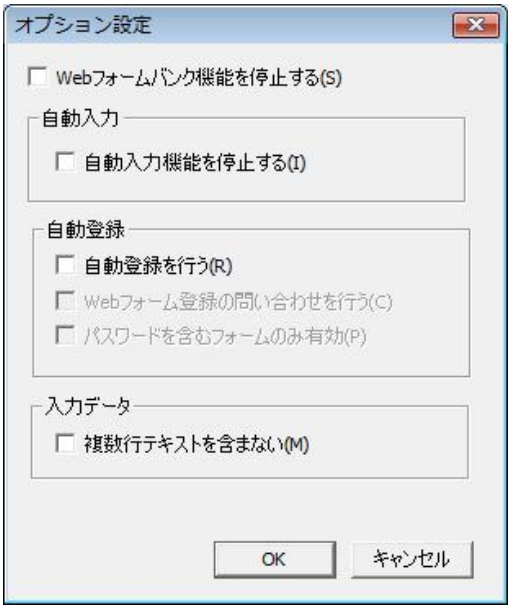
- 各チェックボックスの設定内容に関しては、「7-1-1 登録」をご覧ください。
- データを編集する際は、アイテム情報欄に表示されているフォームに直接入力してください。

7-1-4 機能停止／機能開始

Internet Explorer ツールバーより「機能停止」または「機能開始」メニューを選択することで、
自動入力、および自動登録機能の停止／開始を制御(オプション設定「Web フォームバンク機能を停止する」の有効／無効を変更)することができます。
インストール直後の設定では、Web フォームバンク機能が開始しているため、「機能停止」が表示されます。

7-1-5 オプション設定

Internet Explorer ツールバーより「オプション設定」メニューを選択すると、「オプション設定」画面が表示され、Web フォームバンクデータの自動登録等の設定を行うことができます。



※インストール直後は、上記のように設定されています。

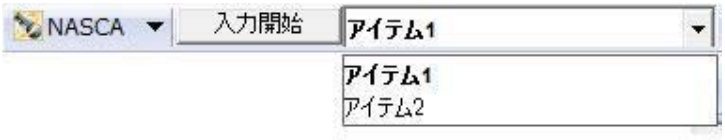
Web フォームバンク機能を停止する		自動入力、および自動登録機能を停止します。
自動入力	自動入力機能を停止する	自動入力を行いません。
自動登録	自動登録を行う	Web ページ上でデータを入力し、「OK」などのボタンを押すと、自動的に登録画面を表示させることができます。
	Web フォーム登録の問い合わせを行う	自動登録を行う前に、登録の続行を確認するダイアログを表示します。
	パスワードを含むフォームのみ有効	自動登録が有効な場合、パスワードを含むフォームの場合のみ、自動登録を行います。
入力データ	複数行テキストを含まない	複数行にわたるテキストを含むものは登録しません。

７－２　Web フォームバンクデータ入力補助

7-2-1　データ入力補助

以前登録を行った Web ページで、登録したデータを入力します。

1 「NASCA」ツールバーのプルダウンメニューからアイテムを選択する



2 「入力開始」ボタンをクリック

チェック

プルダウンメニューには、表示している Web ページに対して登録を行ったアイテムのみ表示されます。

7-2-2　自動入力機能

Web ページが表示された際に、登録したデータを Web ページに対して自動的に入力することができます。1 ページに対して 1 つのアイテムのみ設定を行うことができます。

メモ

「このページでは常にこのデータを自動入力する」設定が有効になっているアイテムは、強調表示されます。

チェック

自動入力設定時でも、登録時のフォームの構成が変更されている場合は登録済みのデータは入力されません。

８　アプリケーションバンク機能

アプリケーションに入力されているデータを取得し、データベースに保存、管理する機能です。
データを保存したアプリケーションを起動した際に、以前保存したデータを自動的に入力することができます。

メモ

- アプリケーションバンク機能を使用するには、「アプリケーションバンク」をインストールする必要があります。詳しくは、「3-1　インストール」をご覧ください。
- インストール時に「登録したデータを保護するために TPM を使用します」を選択している場合、アプリケーションバンク機能で管理するデータの一部は、TPM を用いた暗号化によって保護されます。TPM を用いた暗号化を行うためには、TPM 認証を行う必要があります。TPM 認証については、「6　TPM によるデータ保護」をご覧ください。

チェック

通知領域（タスクトレイ）にアプリケーションバンクアイコンが表示されていない場合は、以下の方法でアプリケーションバンク機能を起動してください。

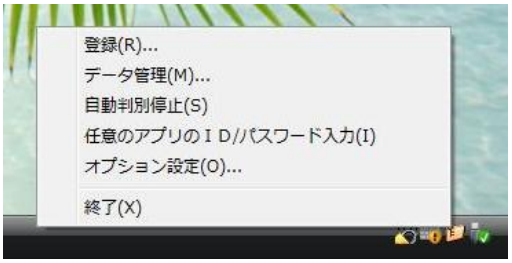
「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「アプリケーションバンク機能開始」をクリック

８－１　アプリケーションバンクデータ登録

アプリケーションバンク機能で、以下のデータを登録することができます。

テキスト	テキストデータを保存します。
パスワード	パスワードを保存します。
チェックボックス	チェックボックスのチェックの有無を保存します。

通知領域（タスクトレイ）に表示されているアプリケーションバンクアイコンを右クリックすると、メニュー（タスクトレイメニュー）が表示されます。タスクトレイメニューから使用する機能を選択してください。



8-1-1 登録

タスクトレイメニューより「登録」メニューを選択すると、アプリケーションに入力されているデータの登録を行うことができます。

メモ

アプリケーションバンク機能は以下のアプリケーションをサポートしています。

- Word 2007
- Excel 2007
- Outlook 2007
- PowerPoint 2007
- Internet Explorer 7
- Windows® メール
- Adobe Reader

チェック

以下の場合、登録ができない場合があります。

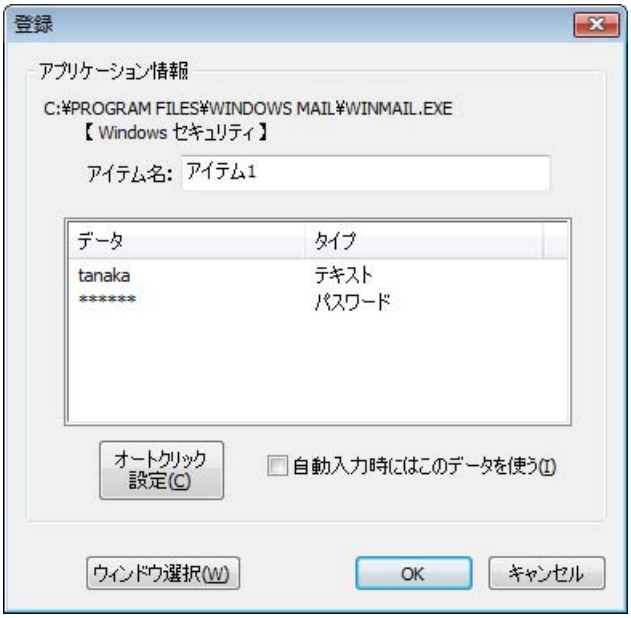
- アプリケーションのウィンドウに登録可能なデータがない場合
- アプリケーションのタイトルバーにタイトルがない場合
- 特殊な作りをしているウィンドウの場合
- サポートされていないアプリケーションの場合

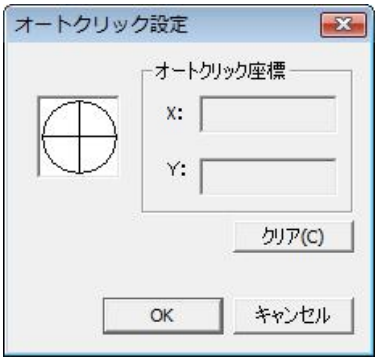
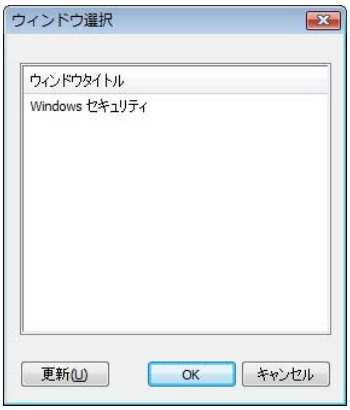
1 登録を行う対象アプリケーションにデータを入力する

2 通知領域（タスクトレイ）のアプリケーションバンクアイコンを右クリック

3 タスクトレイメニューから「登録」をクリック

登録画面が表示され、アプリケーションに入力したデータが表示されます。
また、登録対象アプリケーションのウィンドウが点滅します。



オートクリック設定	「8-2-1　データ入力補助」を行う際、登録したデータの入力完了後に、対象アプリケーションにあるボタンを自動的にクリック（オートクリック）することができます。  以下の方法でオートクリック設定を行ってください。 **1　選択カーソル（十字のアイコン）をクリック** **2　選択カーソルをクリックしたまま、オートクリックをするボタンへドラッグ＆ドロップ** **3　「OK」ボタンをクリック**
ウィンドウ選択	登録対象アプリケーションを変更することができます。  変更するアプリケーションのウィンドウタイトルを選択し、「OK」ボタンを押してください。 ウィンドウ選択画面の内容と実際の内容に差が生じてしまった場合は、「更新」ボタンをクリックすることで表示を最新の状態に更新することができます。
自動入力時にはこのデータを使う	このアプリケーションのウィンドウが表示された際に、このアイテムのデータを自動的に入力します。 1 つのアプリケーションのウィンドウに対して、1 つのアイテムのみ設定を行うことができます。その他のアイテムは同時に設定できません。新規に設定した場合、以前設定していたアイテムの「自動入力時にはこのデータを使う」設定は無効になります。
パスワードを表示しない	パスワード部分を「＊」で表示します。

4　「OK」ボタンをクリック

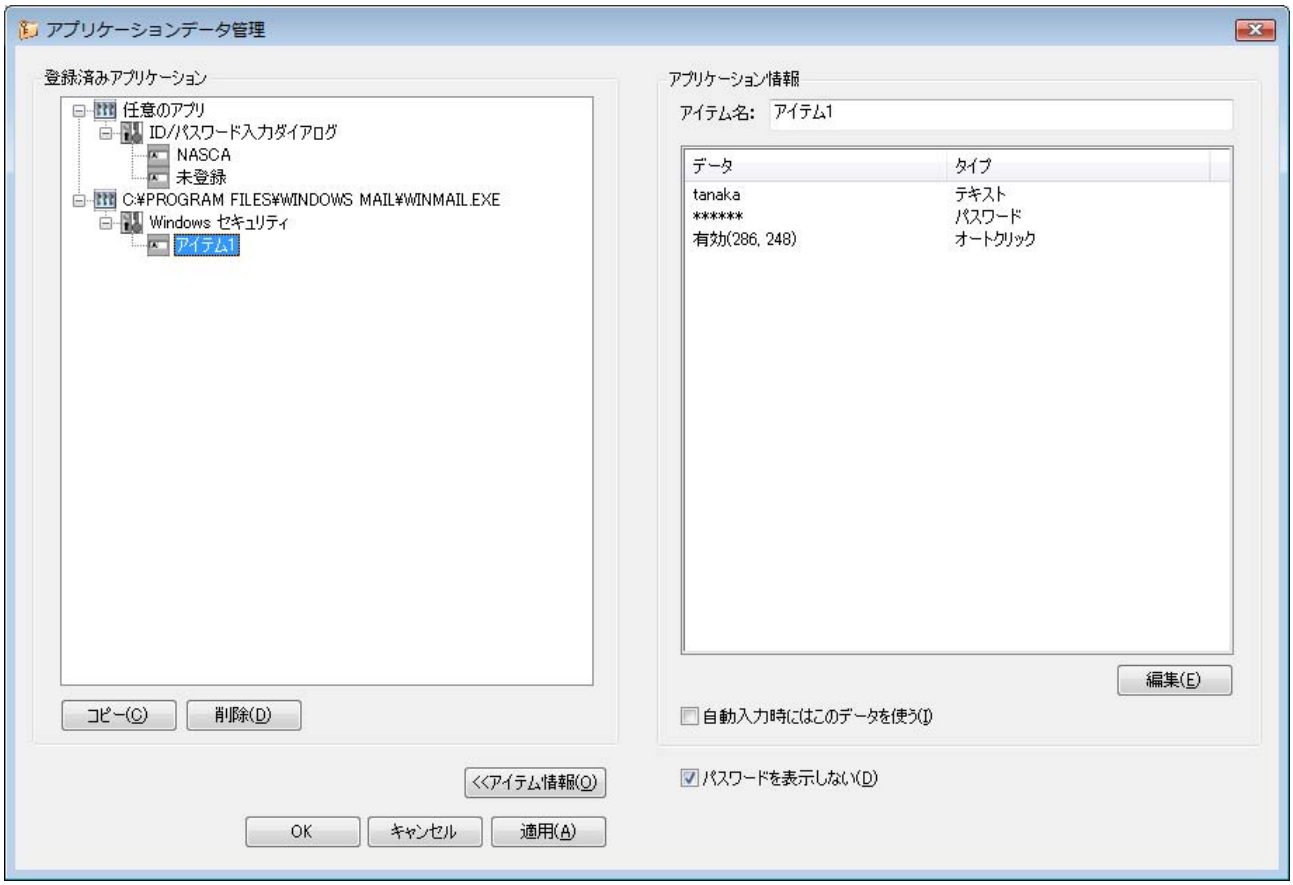
以上で登録は完了です。

8-1-2 データ管理

タスクトレイメニューより「データ管理」メニューを選択すると、アイテムの一覧が表示され、アイテムのコピー、削除、およびアイテム内の各データの編集を行うことができます。

メモ

「アプリケーションデータ管理」は「スタート」メニューからも起動させることができます。
「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「アプリケーションバンク設定」をクリックしてください。



登録済みアプリケーション欄はツリー構造で表示されます。

登録済みアプリケーション	コピー	アイテムをコピーします。
	削除	アイテムを削除します。
アプリケーション情報	編集	データを編集します。 編集するデータを選択して「編集」ボタンを押すと、タイプに応じた編集画面が表示されます。
	自動入力時にはこのデータを使う	「自動入力時にはこのデータを使う」設定を変更します。
パスワードを表示しない		パスワードを「＊」で表示します。

チェック

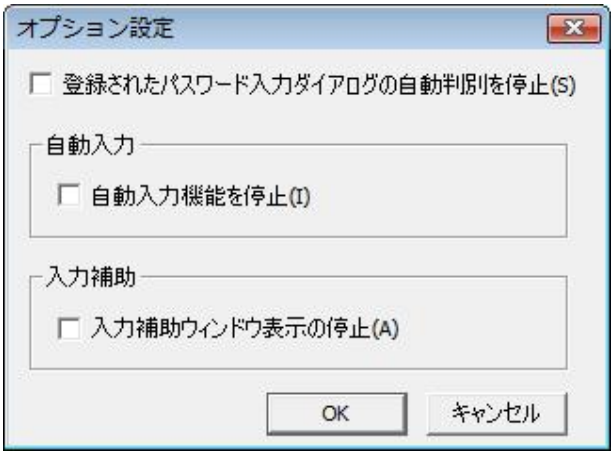
オートクリック設定の編集では、オートクリックの有効／無効の設定のみ変更することができます。オートクリックを行う座標を変更する場合は、アプリケーション情報を再登録する必要があります。

8-1-3 自動判別停止／自動判別開始

タスクトレイメニューより「自動判別停止」または「自動判別開始」メニューを選択することで、
自動入力、および入力補助機能の停止／開始を制御(オプション設定「登録されたパスワード入力ダイアログの自動判別を停止」の有効／無効を変更)することができます。
インストール直後の設定では、自動判別が開始されているため、「自動判別停止」が表示されます。

8-1-4 オプション設定

タスクトレイメニューより「オプション設定」メニューを選択すると、「オプション設定」画面が表示され、アプリケーションバンク機能の設定を行うことができます。



※インストール直後は、上記のように設定されています。

登録されたパスワード入力ダイアログの自動判別を停止		自動入力、および入力補助機能を停止します。
自動入力	自動入力機能を停止	自動入力を行いません。
入力補助	入力補助ウィンドウ表示の停止	入力補助ウィンドウを表示しません。

8-1-5 任意のアプリのID／パスワード入力

タスクトレイメニューより「任意のアプリの ID／パスワード入力」メニューを選択すると、任意のアプリケーションに対してあらかじめ登録したデータを入力することができます。詳しくは「8-3 任意のアプリのID／パスワード入力」をご覧ください。

8-1-6 終了

タスクトレイメニューより「終了」メニューを選択すると、アプリケーションバンク機能を終了させることができます。

メモ

アプリケーションバンク機能を再度起動させる際の手順は、「8 アプリケーションバンク機能」をご覧ください。

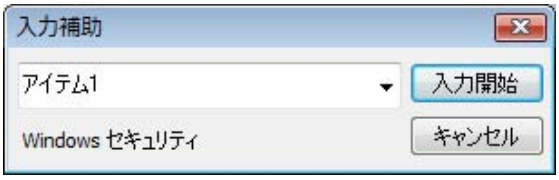
８－２　アプリケーションバンクデータ入力補助

8-2-1　データ入力補助

以前登録を行ったアプリケーションに、登録したデータを入力します。

1　データ入力補助を行う対象アプリケーションを起動する

デスクトップ画面の右下に、「入力補助」ウィンドウが表示されます。



2　プルダウンメニューからアイテムを選択する

3　「入力開始」ボタンをクリック

対象アプリケーションにアイテムのデータが入力されます。

チェック

- プルダウンメニューには、表示しているアプリケーションに対して登録を行ったアイテムのみ表示されます。
- 登録済みアプリケーションが起動していない場合、入力補助ウィンドウは表示されません。
- 入力補助ウィンドウが表示されるまでに、時間がかかる場合があります。

8-2-2　自動入力機能

以前登録を行ったアプリケーションのウィンドウが表示された際に、登録したデータをアプリケーションに対して自動的に入力することができます。1つのアプリケーションのウィンドウに対して、1 つのアイテムのみ設定を行うことができます。

メモ

「自動入力時にはこのデータを使う」設定が有効になっているアイテムは、強調表示されます。

８－３　任意のアプリのＩＤ／パスワード入力

ID とパスワード入力欄が表示されている任意のアプリケーションに対して、登録したデータを入力することができます。

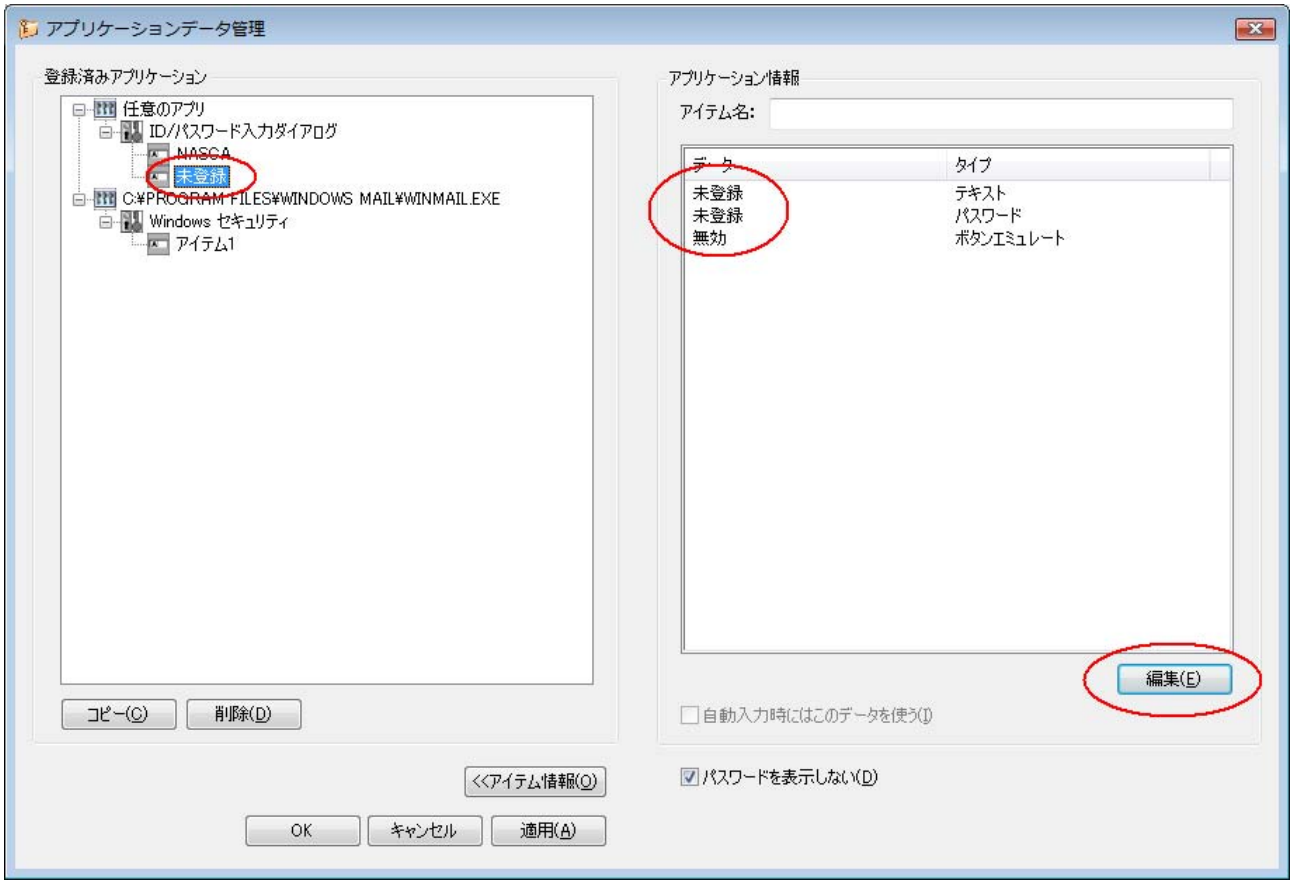
8-3-1　登録　（任意のアプリの ID／パスワード入力）

任意のアプリケーションに入力するデータを登録します。

1　通知領域（タスクトレイ）のアプリケーションバンクアイコンを右クリック

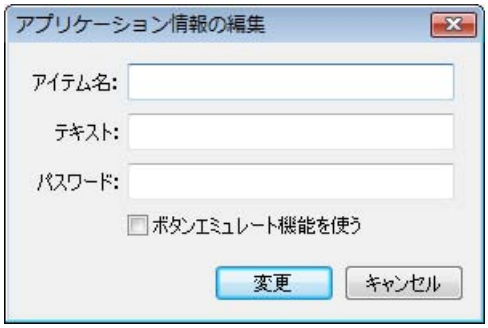
2　タスクトレイメニューから「データ管理」をクリック
データ管理画面が表示されます。

3　「登録済みアプリケーション」から、「任意のアプリ － ID／パスワード入力ダイアログ － 未登録」を選択



※　未登録を選択した場合、データ欄には“未登録”と表示されます。

4 「アプリケーション情報」のデータのいずれかを選択している状態で「編集」ボタンをクリックすると、「アプリケーション情報の編集」画面が表示されます。アイテム名、ID、パスワードのデータ、ボタンエミュレート機能の設定を行ってください。



メモ

- 登録可能なデータは、テキスト形式とパスワード形式の二つのデータです。
- 「ボタンエミュレート機能を使う」チェックを有効に設定した場合、登録したデータの入力完了後に、自動的に「OK」ボタンや「送信」ボタンをクリックします。
- データ入力を行う対象のアプリケーションによっては、ボタンエミュレート機能が正しく動作しない場合があります。

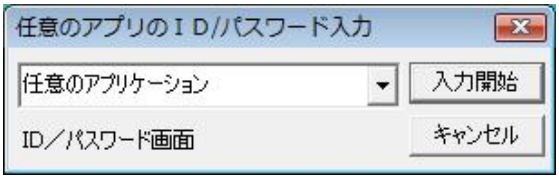
5 「OK」または「適用」ボタンをクリック

以上で登録は完了です。

8-3-2 データ入力補助 （任意のアプリの ID／パスワード入力）

テキスト形式とパスワード形式のフォームが含まれる任意のアプリケーションに対して、登録したデータを入力します。

1 データ入力補助を行う対象のアプリケーションを起動する
2 通知領域（タスクトレイ）のアプリケーションバンクアイコンを右クリック
3 タスクトレイメニューから「任意のアプリの ID／パスワード入力」をクリック
デスクトップ画面の右下に、「任意のアプリの ID／パスワード入力」ウィンドウが表示されます。



メモ

「任意のアプリの ID／パスワード入力」ウィンドウは、通知領域（タスクトレイ）にあるアプリケーションバンクアイコンをダブルクリックして表示させることもできます。

4 プルダウンメニューからアイテムを選択する
5 「入力開始」ボタンをクリック
対象アプリケーションにアイテムのデータが入力されます。

チェック

- テキスト形式とパスワード形式のフォームのいずれかが一つ以上含まれるアプリケーションのみ、データ入力補助が可能です。
- 対象アプリケーションにテキスト形式のフォームが2つ以上ある場合や、パスワード形式のフォームが2つ以上ある場合は、それぞれ1つのフォームにのみデータが入力されます。

９　エクスポート／インポート機能

エクスポート機能では、Web フォームバンクデータやポリシー設定などの各種データをファイルに保存することができます。インポート機能では、保存した各種データをファイルから取り込むことができます。

メモ

ログオンしているユーザーのデータのみ、エクスポート／インポートを行うことができます。

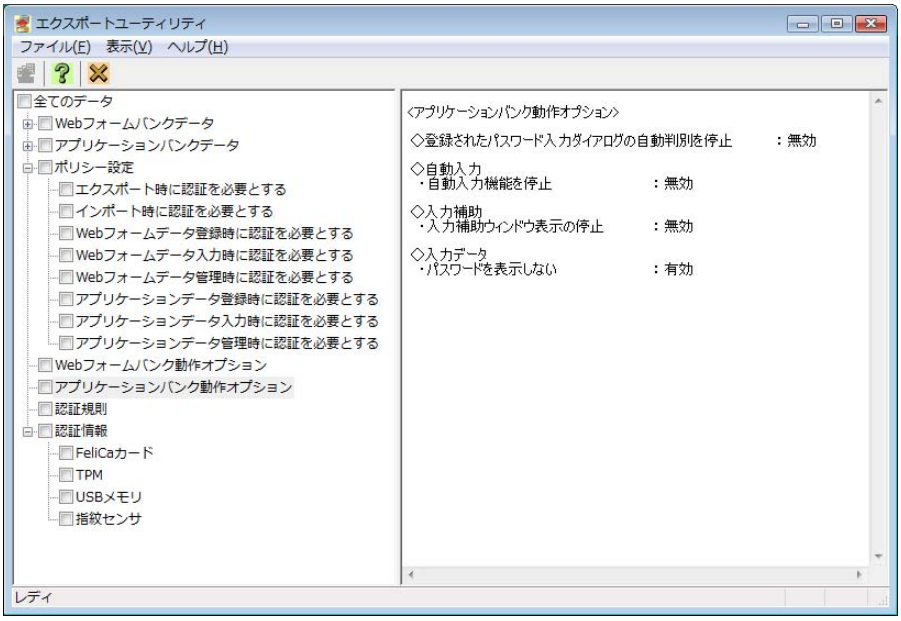
チェック

エクスポート時と異なる製品バージョンの NASCA がインストールされている場合はインポートを行うことが出来ない場合があります。NASCA の製品バージョンを確認する方法は、「12　Q&A」をご覧ください。

９-１　エクスポート

1　「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「エクスポートユーティリティ」をクリック

「エクスポートユーティリティ」が表示されます。



チェック

NASCA 管理者は「エクスポートユーティリティ」を起動できません。

メモ

「エクスポートユーティリティ」には、登録していないデータの項目は表示されません。

各項目の内容は次の通りです。

全てのデータ	Web フォームバンクデータ、アプリケーションバンクデータ、ポリシー設定、動作オプション、認証規則、認証情報をすべてエクスポートします。
Web フォームバンクデータ	アイテム名、URL、フォーム名、説明、パスワードなど、登録済みの Web フォームバンクデータをエクスポートします。
アプリケーションバンクデータ	アイテム名、アプリケーション名、パスワードなど、登録済みのアプリケーションバンクデータをエクスポートします。
ポリシー設定	ポリシー設定をエクスポートします。
Web フォームバンク動作オプション	Web フォームバンクのオプション情報をエクスポートします。
アプリケーションバンク動作オプション	アプリケーションバンクのオプション情報をエクスポートします。
認証規則	認証規則をエクスポートします。
認証情報	認証デバイスの情報をエクスポートします。

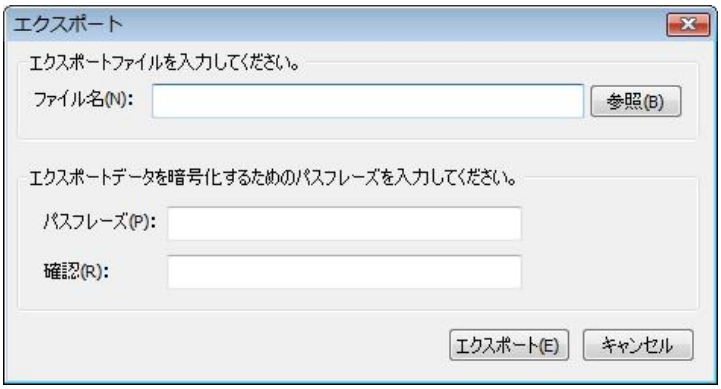
データをエクスポートする際に、ユーザーの機密情報部分(「Web フォームバンクデータのパスワード部分」、「アプリケーションバンクデータのパスワード部分」、「ユーザーの認証情報／認証規則」)を暗号化することができます。暗号化を行う場合は、復号化用のパスフレーズを設定する必要があります。

メモ

TPM PIN のキャッシュ設定が「恒久的に TPM PIN をキャッシュする」になっている場合、TPM の認証情報をエクスポートできません。

2 エクスポートする項目をチェックボックスで選択し、「ファイル」メニューの「エクスポート」をクリック

「エクスポート」画面が表示されます。



3 「エクスポート」画面が表示されたら、ファイル名、パスフレーズを入力し、「エクスポート」ボタンをクリック

※ データの暗号化を行わない場合は、パスフレーズを入力する必要はありません。

チェック

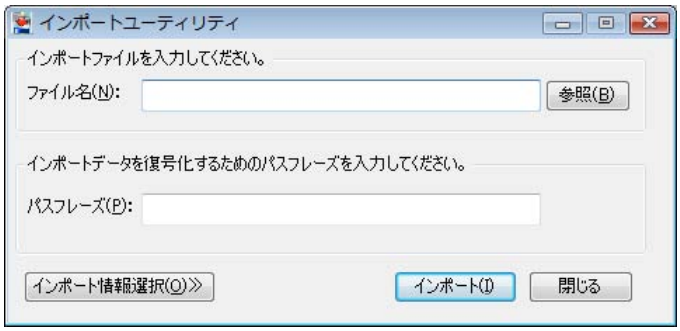
- パスフレーズはインポートする際に使用します。パスフレーズを正しく入力しない場合は、インポートできませんのでご注意ください。

- エクスポート処理では、セキュリティで保護された情報にアクセスするため、エクスポートユーティリティ起動時に、ユーザー認証・TPM 認証が必要となります。 認証に成功していない場合、保護された情報をエクスポートすることはできません。

以上でエクスポートは完了です。

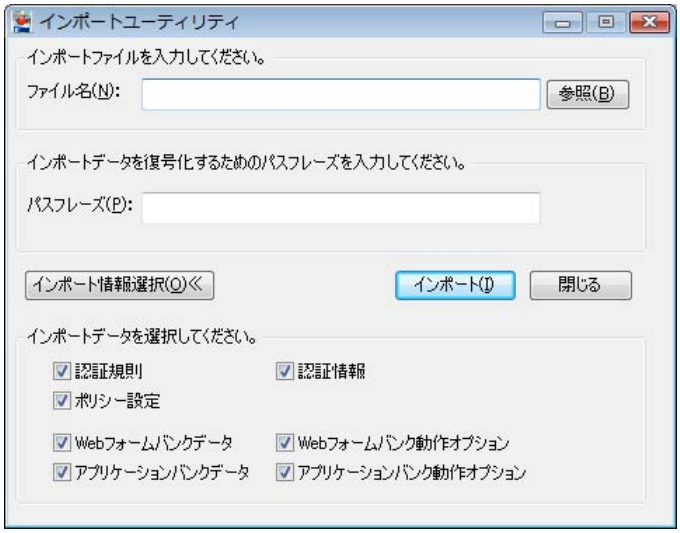
９－２　インポート

1 **「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「インポートユーティリティ」をクリック**
「インポートユーティリティ」が表示されます。



チェック
NASCA 管理者は「インポートユーティリティ」を起動できません。

2 **「インポートユーティリティ」画面が表示されたら、「インポート情報選択」ボタンをクリックし、インポートデータを選択します。**

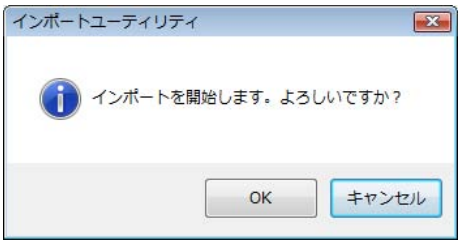


メモ

全てのデータをインポートする場合は、インポートデータを選択する必要はありません。

3 **インポートするファイル名、パスフレーズを入力、「インポート」ボタンをクリック**
※ エクスポート時にパスフレーズを設定していない場合は、入力する必要はありません。

4 **「インポートを開始します。よろしいですか？」と表示されたら、「OK」ボタンをクリック**

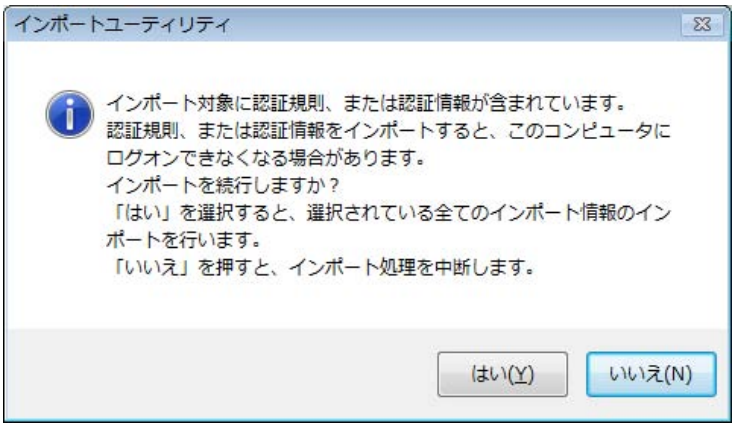


メモ

インポートすると、ファイルのデータが追加登録されます。ただし、同一項目のデータが存在する場合は、データが上書き登録されます。

チェック

- インポート処理では、セキュリティで保護された情報にアクセスする場合があるため、ユーザー認証・TPM 認証が複数回必要となる場合があります。 認証に成功していない場合、保護された情報をインポートすることはできません。
- NASCA 管理者が許可していない認証規則をインポートすることはできません。
- インポートデータに「認証規則」及び「認証情報」が含まれている場合は、以下の画面が表示されます。インポートファイルに含まれている認証規則や認証情報が不適切な場合、ログオンできなくなる場合があります。問題がないことを確認した上でインポートを行ってください。



以上でインポートは完了です。

１０　バックアップ／リストア機能

バックアップ機能では、NASCA のデータベースの内容をファイルに保存することで、全ユーザー共通のデータやユーザーごとのデータを一括してバックアップすることができます。リストア機能では、ファイルにバックアップしたデータベースの内容を復元することができます。
バックアップ／リストア機能は、NASCA 管理者のみ使用することができます。

チェック

- バンクデータ管理用マスターコードの設定と、ユーザーごとのバックアップ設定を行うことにより、ユーザー固有データの Web フォームバンクデータ、Web フォームバンク動作オプション、アプリケーションバンクデータ、アプリケーションバンク動作オプションをバックアップできます。詳しくは「10－1　バンクデータ管理用のマスターコードの設定」、「10－2　バックアップの設定」をご覧ください。
- 管理者によるバンクデータ管理用のマスターコードの設定を行っていない場合は、ユーザーごとのバックアップ設定を行うことはできません。
- バックアップ機能では、管理者によるバンクデータ管理用マスターコードの設定の有無に関わらず、ユーザー共通データの NASCA 基本データと認証設定の管理(管理者用)データ、ユーザー固有データの認証規則と認証情報、ポリシー設定がバックアップされます。

バックアップ可能なデータは、以下の通りです。

ユーザー共通データ	NASCA 基本データ	NASCA を使用する上で、必ず使用される基本データを指します。
	認証設定の管理（管理者用）データ	NASCA 管理者が使用を許可している認証デバイス／認証規則の設定データ、ログオン設定データを指します。詳しくは、「4-1　認証デバイス／認証規則の管理（管理者用）」、「11-3 個人認証デバイス利用強制機能」をご覧ください。
ユーザー固有データ	認証規則	デバイス認証で使用する認証規則を指します。詳しくは、「4-2-3　認証規則の設定」をご覧ください。
	認証情報	デバイス認証に使用する認証情報を指します。詳しくは、「4-2-2　認証情報の設定」をご覧ください。
	ポリシー設定データ	ユーザー認証を要求するタイミングを設定したデータを指します。詳しくは、「4-4　認証ポリシーの設定」をご覧ください。
	Web フォームバンクデータ	Web フォームバンク機能で登録したデータを指します。詳しくは「7-1　Web フォームバンクデータ登録」をご覧ください。
	Web フォームバンク動作オプション	Web フォームバンク機能のオプション情報を指します。詳しくは「7-1-5　オプション設定」をご覧ください。
	アプリケーションバンクデータ	アプリケーションバンク機能で登録したデータを指します。詳しくは「8-1　アプリケーションバンクデータ登録」をご覧ください。
	アプリケーションバンク動作オプション	アプリケーションバンク機能のオプション情報を指します。詳しくは「8-1-4　オプション設定」をご覧ください。

チェック

- リストアを行うと、バックアップを行った際の状態に戻ります。リストアを行う前の登録済みのデー

タは削除されますので、ご注意ください。

- ドメインサーバーと通信できない場合、NASCA 登録済みのドメインユーザーのデータをバックアップ／リストアができない可能性があります。ドメインサーバーと通信できることを確認してから、バックアップ／リストアを行ってください。
- バックアップ時と異なる製品バージョンの NASCA がインストールされている場合はリストアを行うことができませんので、ご注意ください。NASCA の製品バージョンを確認する方法は、「12 Q&A」をご覧ください。
- バックアップ／リストアを行う場合は実行中のアプリケーションウィンドウを全て閉じてください。通知領域（タスクトレイ）にアプリケーションバンクアイコンが表示されている場合は、タスクトレイメニューより「終了」メニューを選択し、アプリケーションバンク機能を終了させてください。

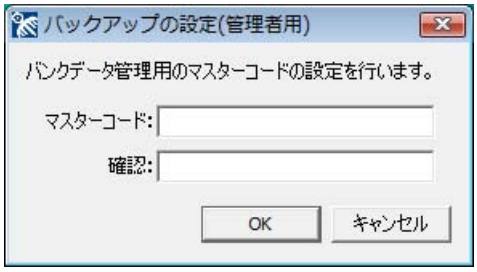
１０－１　バンクデータ管理用のマスターコードの設定

バンクデータ管理用のマスターコードを設定します。

10-1-1 バンクデータ管理用のマスターコードの初期登録

1 「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「バックアップの設定(管理者用)」をクリック

バンクデータ管理用のマスターコードの設定画面が表示されます。



チェック

- NASCA 管理者以外のユーザーでは「バックアップの設定（管理者用）」を起動できません。
- 初期登録が完了すれば、以後バンクデータ管理用のマスターコードを設定する必要はありません。

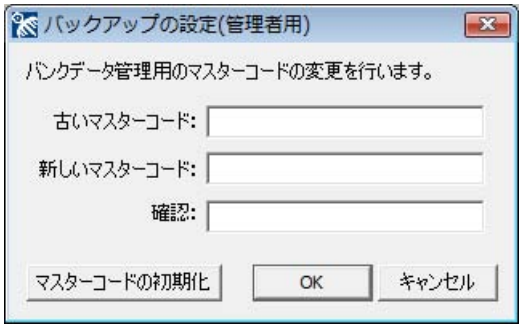
2 バンクデータ管理用のマスターコードの設定画面が表示されたら、マスターコードを入力し「OK」ボタンをクリック

以上でマスターコードの初期登録は完了です。

10-1-2 バンクデータ管理用のマスターコードの変更

1 「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「バックアップの設定(管理者用)」をクリック

バンクデータ管理用のマスターコードの変更画面が表示されます。



チェック

NASCA 管理者以外のユーザーでは「バックアップの設定(管理者用)」を起動できません。

2 バンクデータ管理用のマスターコードの変更画面が表示されたら、古いマスターコード、新しいマスターコードを入力し「OK」ボタンをクリック

メモ

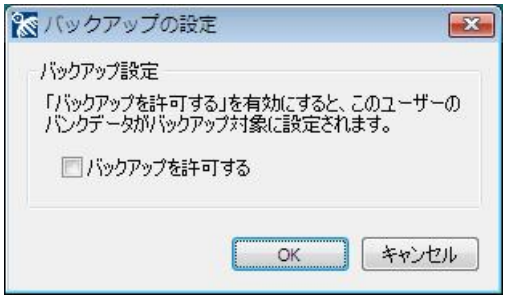
古いマスターコードを忘れてしまった場合は、「マスターコードの初期化」ボタンをクリックし、再度マスターコードを設定してください。マスターコードを初期化した場合、全てのユーザーのバックアップ設定が「バックアップを許可しない」設定に変更されるため、再度各ユーザーで設定を行う必要があります。バックアップ設定に関しては「10－2 バックアップ設定」をご覧ください。

以上でマスターコードの変更は完了です。

１０－２　バックアップの設定

ユーザーごとにバックアップ許可設定を行います。

1 NASCA 管理者以外のユーザーでログオンし「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「バックアップの設定」をクリック
「バックアップの設定」画面が表示されます。



2 「バックアップを許可する」チェックボックスにチェックを入れて、「OK」ボタンをクリック
3 TPM 認証が要求された場合は、正しい TPM 情報を入力して「OK」をクリック
※インストール時に、「登録したデータを保護するために TPM を使用します」設定を行っている場合のみ TPM 認証が要求される場合があります。

チェック

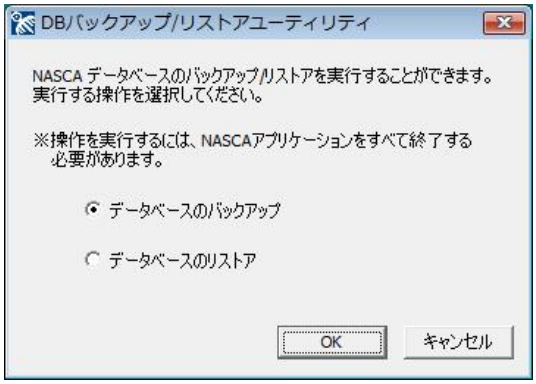
- 管理者によるバンクデータ管理用のマスターコードの設定を行っていない場合は、ユーザーごとの設定を行うことはできません。
- 本機能で「バックアップを許可する」設定を行っていないユーザーの Web フォームバンクデータ、Web フォームバンク動作オプション、アプリケーションバンクデータ、アプリケーションバンク動作オプションはバックアップの対象に含まれません。

以上でバックアップの設定は完了です。

１０－３　バックアップ

1 「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「バックアップユーティリティ（管理者用）」をクリック

「DB バックアップ／リストアユーティリティ」画面が表示されます。

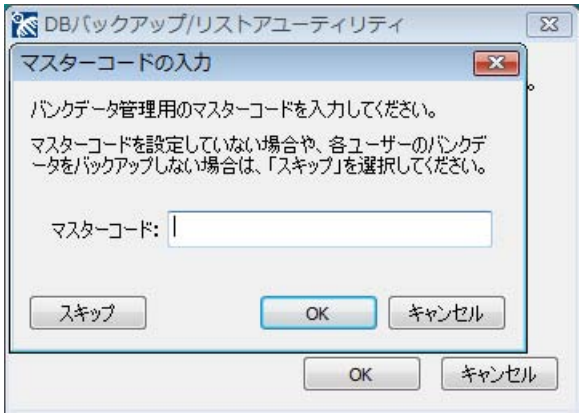


チェック

NASCA 管理者以外のユーザーでは「DB バックアップ／リストアユーティリティ」を起動できません。

2 「データベースのバックアップ」を選択し、「OK」ボタンをクリック

3 「マスターコードの入力」画面が表示されたら、バンクデータ管理用のマスターコードを入力し「OK」ボタンをクリック



メモ

Web フォームバンクデータ、Web フォームバンク動作オプション、アプリケーションバンクデータ、アプリケーションバンク動作オプションをバックアップする必要が無い場合は、「スキップ」ボタンをクリックしてください。

4 「バックアップファイルの設定」画面が表示されたら、バックアップファイルの保存先とファイル名を指定して「次へ」ボタンをクリック

5 「パスフレーズの設定」画面が表示されたら、パスフレーズを入力して「次へ」ボタンをクリック
6 「バックアップを開始しますか？」と表示されたら、「はい」ボタンをクリック
「バックアップ完了」画面が表示されます。
7 「完了」ボタンをクリック

以上でバックアップは完了です。

１０－４　リストア

1 「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「バックアップユーティリティ（管理者用）」をクリック
「DB バックアップ／リストアユーティリティ」画面が表示されます。

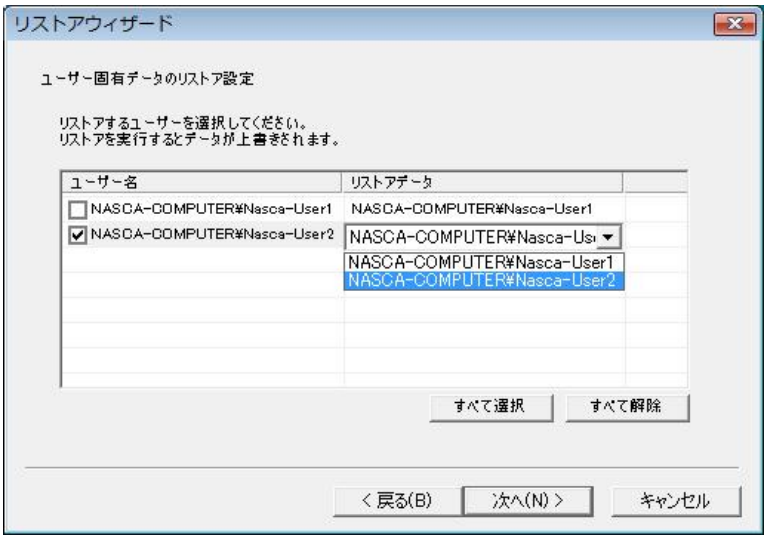
チェック
NASCA 管理者以外のユーザーでは「DB バックアップ／リストアユーティリティ」を起動できません。

2 「データベースのリストア」を選択し、「OK」ボタンをクリック
3 「リストアウィザードを開始します。」と表示されたら、「OK」ボタンをクリック
4 「バックアップファイルの入力」画面が表示されたら、リストアするバックアップファイルを指定して「次へ」ボタンをクリック
5 「パスフレーズの入力」画面が表示されたら、パスフレーズを入力して「次へ」ボタンをクリック
6 「ユーザー共通データのリストア設定」画面が表示されたら、リストアする項目を選択して、「次へ」ボタンをクリック
チェックボックスにチェックを入れた項目のみリストアされます。
「NASCA 基本データ」項目は必ずリストアされます。

7 「ユーザー固有データのリストア設定」画面が表示されたら、リストアするユーザーとリストアデータを選択して、「次へ」ボタンをクリック

チェックボックスにチェックを入れたユーザーに対して、リストアが行われます。

リストアデータ欄をクリックすると、バックアップファイルに保存されているユーザー名一覧が表示されます。ユーザー名を選択すると、そのユーザーの固有データをリストアすることができます。



8 「リストアを開始しますか？」と表示されたら、「はい」ボタンをクリック

「リストア完了」画面が表示されます。

メモ

リストアすると、データベースの内容がバックアップファイルのデータで上書きされます。

9 「完了」ボタンをクリック

その後、Windows を再起動してください。

以上でリストアは完了です。

１１　オプション機能

NASCA の設定を変更するためのオプション機能です。

１１－１　ロック解除時の不正認証監視機能

不正なロック解除を防止するため、ロック解除時の認証試行回数を設定することができます。設定後、認証に複数回失敗した場合、強制的に Windows を再起動させることができます。
設定は以下の手順で行ってください。

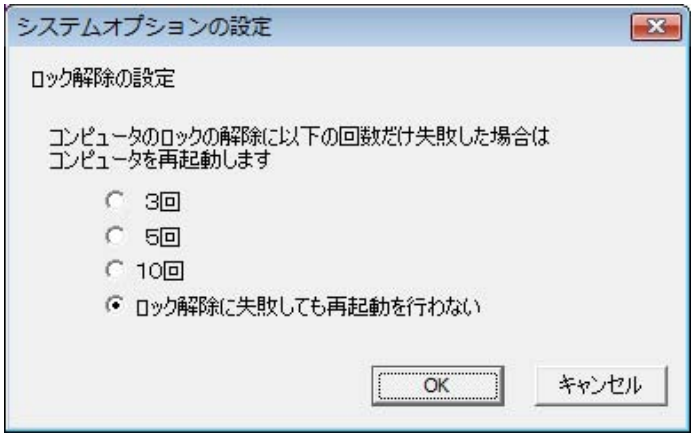
メモ

ロック解除時の不正認証監視機能を使用するには、「Windows ログオン認証」をインストールする必要があります。詳しくは、「3-1　インストール」をご覧ください。

チェック

- NASCA 管理者以外のユーザーでは「システムオプションの設定」を起動できません。
- ロック解除時に強制的に Windows の再起動が行われると、コンピュータをロックするまでに行っていた作業の内容は保存されませんのでご注意ください。

1 「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「ファイル名を指定して実行」をクリック
2 「名前」に「NscSetSysOption.exe」と入力して、「OK」ボタンをクリック
「システムオプションの設定」画面が表示されます。



※インストール直後は、「ロック解除に失敗しても再起動を行わない」に設定されています。

3 ロック解除時の認証の試行回数を選択し、「OK」ボタンをクリック
4 「設定を更新しました。設定を反映させるには、再起動が必要です。」と表示されたら、「OK」ボタンをクリック
5 Windows を再起動する

以上でロック解除時の不正認証監視機能の設定は完了です。

１１－２　Windows ログオン認証画面の画像変更機能

「Windows ログオン認証」画面に表示される画像を変更することができます。

メモ

画像変更ユーティリティを使用するには、「Windows ログオン認証」をインストールする必要があります。詳しくは、「3-1　インストール」をご覧ください。

チェック

NASCA 管理者以外のユーザーでは「画像変更ユーティリティ」を起動できません。

1 「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「ファイル名を指定して実行」をクリック

2 「名前」に「NscChgLogoImg.exe」と入力して、「OK」ボタンをクリック

「画像変更ユーティリティ」画面が表示されます。

3 「参照」ボタンをクリック

ファイルを選択する画面が表示されるので、画像を選択し「開く」ボタンをクリック

チェック

- 画像変更ユーティリティで指定できる画像は256 色のビットマップファイルのみです。256 色のビットマップファイル以外はサポートしていません。
- 画像変更ユーティリティで指定できる画像のサイズは「128×128(ピクセル)」です。

4 「画像変更ユーティリティ」画面で画像の変更を確認し、「OK」ボタンをクリック

以上で画像変更の設定は完了です。

１１－３　個人認証デバイス利用強制機能

認証規則を設定していないユーザーに対して、Windows にログオンできる回数を制限することができます。

「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「ログオンの設定(管理者用)」をクリック

「Windows ログオンの設定」画面が表示されます。

メモ

- 「ログオンの設定(管理者用)」を使用するには、「Windows ログオン認証」をインストールする必要があります。詳しくは、「3-1 インストール」をご覧ください。

チェック

- NASCA 管理者以外のユーザーでは「Windows ログオンの設定」を起動できません。
- ログオン可能回数の制限は、認証規則未登録のユーザーが対象です。

11-3-1 ログオン可能回数の設定 （一般設定）

認証規則を設定していない状態で、Windows にログオンできる回数を設定します。

1 「Windows ログオンの設定」が表示されたら、「認証規則未登録の状態での Windows ログオン回数を制限する」を選択

2 入力欄にログオン可能回数を入力

チェック

- ログオン可能回数は0～9999回を設定できます。
- 0回を設定した場合、認証規則登録済みのユーザー、詳細設定で個別にログオン可能回数が設定されたユーザーおよび NASCA 管理者のみログオン可能になります。その他のユーザーは Windows にログオンすることができません。

3 「OK」ボタンをクリック

以上で、ログオン可能回数の設定は完了です。

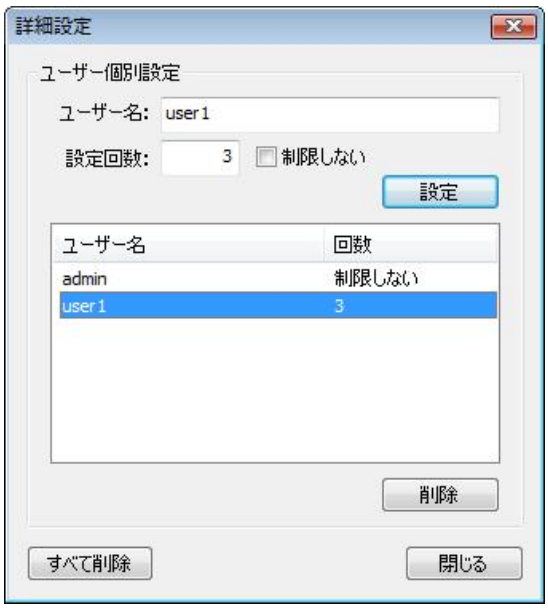
メモ

- 認証規則の登録をしているユーザーについては、Windows にログオンできる回数を設定することはできません。
- 個別にログオン可能回数が設定されたユーザー以外は、ここで設定した回数が適用されます。ユーザー個別にログオン回数を設定するには、「11-3-2 ログオン可能回数のユーザー個別設定」をご覧ください。

11-3-2 ログオン可能回数のユーザー個別設定

1 「Windows ログオンの設定」画面が表示されたら、「詳細設定」ボタンをクリック

「詳細設定」 画面が表示されます。



チェック

- 個別の設定を行っていないユーザーで Windows にログオンすると、一般設定の回数が自動的に登録されます。
- 「詳細設定」画面を表示するには、「**認証規則未登録の状態での Windows ログオン回数を制限する**」設定にする必要があります。

2 ユーザー名とログオン可能回数を入力し、「設定」ボタンをクリック

入力内容が一覧に反映されます。

チェック

- ログオン可能回数は0～9999回を設定できます。
- 0回を設定したユーザーは、認証規則未登録の状態ではログオンできなくなります。
- ドメインユーザーに対して設定する場合は、“<ドメイン名>¥<ユーザー名>”の形式でユーザー名を入力してください。

3 「閉じる」ボタンをクリック

「詳細設定」 画面が閉じます。

4 「Windows ログオンの設定」画面の「OK」ボタンをクリック

以上でログオン可能回数のユーザー個別設定は完了です。

１２　Q&A

１．ユーザー認証機能関連

Q1-1

Windows へログオンできない(ユーザー向け)

A1-1

認証デバイスの異常などにより Windows へログオンできない場合は、パスワードを入力して Windows へログオンしてください。
また、ネットワークの状態や、ドメインユーザーが作成されたタイミングによっては、新しいドメインユーザーによる Windows ログオンが一時的にできない場合があります。
このような場合は、一度 Windows を再起動してください。

チェック

正しいパスワードを入力しても Windows へログオンできない場合は、NASCA 管理者へ問い合わせてください。

メモ

認証規則を設定していないユーザーで、正しいパスワードを入力しても Windows へログオンできない場合は、NASCA 管理者によってログオン可能回数が制限されている可能性があります。

Q1-2

Windows へログオンできない(TPM を利用しているユーザー向け)

A1-2

TPM には辞書攻撃防御機能があり、何度も続けて認証に失敗した場合に、一定時間認証を受け付けない状態になります。そのため、TPM を使用した Windows ログオン認証や、ユーザー認証に成功しなくなる場合があります。
このような場合は、少し時間をおいてから、再度認証をお試しください。

参照

TPM の辞書攻撃防御機能についての詳細は、TPM のマニュアルをご覧ください。

Q1-3

Windows へログオンできない(NASCA 管理者向け)

A1-3

設定した認証デバイス、またはパスワードを使用しても Windows へログオンできない場合は、「ユーザー初期化ツール」を使用して、認証規則を初期化してください。

チェック

- 「ユーザー初期化ツール」を使用すると認証規則が初期化されます。認証規則の初期化後は必要に応じて再設定してください。
- 「ユーザー初期化ツール」は NASCA 管理者以外のユーザーでは起動できません。

1. 「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「ファイル名を指定して実行」をクリック
2. 「名前」に「NscResetUser.exe」と入力して、「OK」ボタンをクリック
3. 「ユーザー初期化ツール」画面が表示されたら、Windows にログオンできなくなったユーザーを選択して、「OK」ボタンをクリック
4. 「このユーザーの認証規則は消去されます。」と表示されたら、「OK」ボタンをクリック
5. 「認証規則の消去を完了しました。」と表示されたら、「OK」ボタンをクリック
6. 認証規則を削除したユーザーでパスワードを入力して Windows へログオンする

Windows へログオン後、必要に応じて認証規則を再設定してください。

Q1-4

ユーザー登録ウィザードや、ユーザー認証画面で、間違った Windows パスワードを何度も入力したら、その後正しい Windows パスワードを入力しても、認証に成功しなくなってしまった。

A1-4

これは NASCA の仕様によるものです。
何回か連続で Windows パスワード認証に失敗すると、Windows のシステム管理者が設定したポリシーによっては、アカウントがロックされてしまう場合があります。 この場合はシステム管理者に連絡し、アカウントのロックを解除してもらう必要があります。

Q1-5

デバイス認証から Windows パスワード認証へ、認証規則を切り替える方法は？

A1-5

認証規則の登録後、Windows パスワード認証(認証規則なし)に再度戻す場合は、ユーザーの認証規則を初期化する必要があります。
NASCA 管理者に連絡し、「ユーザー初期化ツール」を使用して認証規則を初期化してください。

NASCA 管理者は、以下の操作を実行してください。

チェック
「ユーザー初期化ツール」は NASCA 管理者以外のユーザーでは起動できません。

1. 「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「ファイル名を指定して実行」をクリック
2. 「名前」に「NscResetUser.exe」と入力して、「OK」ボタンをクリック
3. 「ユーザー初期化ツール」画面が表示されたら、パスワード認証に切り替えたいユーザーを選択して、「OK」ボタンをクリック
4. 「このユーザーの認証規則は消去されます。」と表示されたら、「OK」ボタンをクリック
5. 「認証規則の消去を完了しました。」と表示されたら、「OK」ボタンをクリック

以上で認証規則の初期化は完了です。

Q1-6

Windows ログオン認証時やコンピュータのロック解除時に、「DB パスワードの更新」という画面が表示される。

A1-6

この画面は、NASCA が保持しているユーザーの Windows パスワード情報と実際のパスワード情報に差分が検出された場合に表示されます。
ドメインユーザーのパスワードがサーバー側で変更された場合などに、この画面が表示されることがあります。
この画面で正しいパスワードを入力し直してください。

認証規則を設定済みのユーザーを OS 上から削除してしまった場合、削除されたユーザーによる Windows ログオン認証を行うと、この画面が表示される場合があります。
この場合は、一度キャンセルをし、正しいユーザーで認証をやり直してください。

Q1-7

Windows ログオン認証時、コンピュータのロック解除時、ユーザーアカウント制御の認証時の画面で、全てのデバイス名の横に「×」が表示されてしまい、デバイス認証ができない。

A1-7

NASCA に異常が発生している可能性があります。
このような状態になってしまった場合は、一度システムを再起動してください。
作業中の場合は、正しいログオンユーザー名と Windows パスワードを入力してログオンし、必要な情報の保存などを行ってからシステムを再起動してください。

Q1-8

休止状態・スリープ状態から復帰したら、認証デバイスを読み取らなくなってしまった。

A1-8

コンピュータが休止状態やスリープ状態から復帰すると、認証デバイスの動作が不安定になり、以下のような状態になる場合があります。

- 認証デバイスが不正な状態として認識される
- 認証情報の読み取りが正常に行えなくなる
- 正しい TPM PIN を入力しても、認証に成功しなくなる

この状態になってしまった場合、以下の方法でロックの解除をお試しください。

- Windows パスワードを入力し、「OK」ボタンをクリック
- コンピュータがバッテリ駆動中の場合は、AC アダプタを接続する
- もう一度スリープ状態に移行し、再度ロックの解除を試みる
- NASCA 管理者に連絡し、ユーザー"Nasca-Admin"でロックを解除する

メモ

ロックの解除の画面からスリープに移行する場合は、以下の操作を実行してください。

1. 「ユーザーの切り替え」ボタンをクリック
2. 「シャットダウンのオプション」ボタンをクリック
3. 「スリープ」をクリック

Q1-9

ログオン画面やユーザーアカウント制御画面などの認証画面に、デバイス名が表示されないことがある。

A1-9

NASCA 管理者が許可していないデバイスは、ログオン画面やユーザーアカウント制御画面に表示されません。どのデバイスが許可されているかについては NASCA 管理者に問い合わせてください。
デバイスが許可されているにも関わらず表示されていない場合は、以下のいずれかの方法をお試

しください。

- 「キャンセル」ボタンが表示されている場合、「キャンセル」ボタンを押下した後に、再び認証画面を表示させる
- 「ユーザーの切り替え」ボタンが表示されている場合、「ユーザーの切り替え」ボタンを押下する
- 一度「矢印ボタン（OK ボタン）」を押下し、認証を行う
- Windows を再起動する

Q1-10

ログオン画面が表示されるまでに時間がかかる。

A1-10

NASCA の Windows ログオン認証機能をインストールしている場合、ご利用の環境によっては、ログオン画面の表示に時間がかかる場合があります。

- 認証に使用するデバイスが使用可能な状態になるまで待機してからログオン画面の表示を行うため、ログオン画面の表示に時間がかかる場合があります。
- 認証に必要なドメイン情報などをネットワーク上から取得する必要があるため、接続しているネットワークの状態によってはログオン画面の表示に時間がかかる場合があります。
- Windows 起動時に実行される他のプログラムに影響して NASCA の動作が遅くなり、ログオン画面の表示に時間がかかる場合があります。

Q1-11

デバイスが正しく認識されず、ユーザー認証や認証情報の登録ができない。

A1-11

デバイスへのアクセスを制限する特殊なアプリケーションなどがインストールされている場合、このような現象が発生する可能性があります。

以下のような現象が起きる場合があります。

・ 認証用のデバイスが不正な状態として認識されてしまう。
・ 認証用のデバイスが正常な状態として認識されるが、認証情報の読み取りが行えない。

Q1-12

ユーザー名の変更を行ったが、変更後のユーザー名を入力しても Windows にログオンできない。

A1-12

ユーザーのフルネームのみが変更されており、ユーザー名は変更前のままである可能性があります。Windows ユーザーアカウントは、ユーザー名とフルネームの異なる2つの名前を持っている場合がありますが、NASCA で Windows ログオン認証を行う場合はユーザー名を入力する必要があります。このような場合は、変更前のユーザー名を入力し、Windows ログオン認証をお試しください。

メモ

ユーザー名とフルネームについての詳細は、Windows のヘルプなどを参照してください。

2. Web フォームバンク／アプリケーションバンク機能関連共通

Q2-1

Web フォームバンクデータ／アプリケーションバンクデータの入力補助機能が動作しなくなった。

A2-1

Web ページの構成／アプリケーションのウィンドウの構成が登録時から変更されている場合、データ入力補助や自動入力機能が使用できない可能性があります。その場合は、データの再登録を行ってください。

Q2-2

登録したパスワードが、バンクデータ入力時に入力されない。

A2-2

バンクデータを保護するための情報が、何らかの理由により利用できなくなってしまった可能性があります。このような場合には「データ保護機能の初期化ツール」を使用して、情報の初期化を行ってください。

1. 「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「ファイル名を指定して実行」をクリック
2. 「名前」に「NscUsrKeyGen.exe　/renew」と入力して、「OK」ボタンをクリック
   ユーザー認証が要求されます。
3. 「データ保護機能の初期化ツール」画面が表示されたら、「初期化」ボタンをクリック
4. 「データ保護機能の初期化を行います。よろしいですか?」と表示されたら「OK」ボタンをクリック
5. 「データ保護機能の初期化が完了しました。再起動してください。」と表示されたら「OK」ボタンをクリックし、再起動を行ってください。

以上でデータ保護機能の初期化は完了です。

チェック

- データ保護機能の初期化ツールを使用すると、Web フォームバンクデータ/アプリケーションバンクデータが全て削除されます。
- TPM が破損してしまった場合やクリアされてしまった場合は、データ保護機能の初期化が正常に完了しない場合があります。このような場合は、TPM の復元、または初期化を行ってから、データ保護機能の初期化を行ってください。

メモ

以下のような現象が起きている場合は、バンクデータを保護するための情報が破損している可能性があります。

- TPM 認証に成功しているが、Web フォームバンクデータ／アプリケーションバンクデータの管理画面で登録済みアイテムのパスワード情報部分のみ、正しく表示されない。

3．Web フォームバンク機能関連

Q3-1

Web フォームバンク機能で登録できない Web ページがある。

A3-1

その Web ページの構造に関係がある可能性があります。
Web フォームバンク機能では、標準的な HTML で作成された Web ページをサポートしています。
ただし、標準的な HTML で作成された Web ページにも数多くのパターンが存在しており、その Web ページの構造を正確に把握できないため、登録できない可能性があります。
Web ページの構造によっては、自動登録機能のみ動作しないなど、機能の一部のみに制限がかかる場合もありますので、登録手順を変えることによって問題が解決する可能性があります。

Q3-2

Web フォームバンク機能の「登録確認」画面で「いいえ」ボタンを押しても、同じ画面が複数回表示される。

A3-2

表示されている Web ページの構成が複雑な場合、「登録確認」画面で「いいえ」ボタンを押しても、同じ画面が複数回表示されることがあります。そのような場合は、「登録確認」画面が表示されなくなるまで「いいえ」ボタンを複数回押してください。もしくは、今後登録確認を行う必要がなければ、「これ以降、この問い合わせは行わない」にチェックしてから「いいえ」ボタンを押してください。

Q3-3

Webフォームバンク機能で登録済みのWebページを開いても、ツールバーに登録済みのアイテムが表示されない。

A3-3

Web フォームバンクデータの登録中、入力中、登録済み Web ページの表示直後に、別のウィンドウなどで登録済みの Web ページを表示させると、この現象が発生する場合があります。
また、お使いのコンピュータの動作が遅くなっている状態で、Web フォームバンク機能を使用すると以下のような状態になる場合があります。

- 登録済み Web ページを開いても、ツールバーに登録済みアイテムが表示されない。
- 「Web フォームデータ管理」画面を開くと Web フォームバンクデータが一つも表示されない。
- Web フォームバンクデータがエクスポートできない。

このような場合は表示中の Web ページをいったん閉じ、再度開き直すか、Internet Explorer を全て終了し、再度開き直してください。

４．アプリケーションバンク機能関連

Q4-1

アプリケーションバンク機能で登録できないアプリケーションがある。

A4-1

アプリケーションバンク機能がサポートしていないアプリケーションのデータを登録することはできません。また、サポートしているアプリケーションであっても、特殊な作りをしているウィンドウでは一部のデータを登録できない場合があります。
登録できないアプリケーションに対して、「任意のアプリのID／パスワード入力」機能によって入力補助を行うことができる場合があります。詳しくは「８　アプリケーションバンク機能」の「8-3　任意のアプリのID／パスワード入力」をご覧ください。

Q4-2

アプリケーションバンク機能で、登録済みのアプリケーションを開いても入力補助ウィンドウが表示されない。

A4-2

データの登録を行った時とは異なる手順でアプリケーションを起動した場合、以前登録を行ったアプリケーションとしては認識されず、入力補助ウィンドウが表示されないことがあります。
このような場合は、改めて登録を行うか、登録した時と同じ手順でアプリケーションを起動してください。

5. その他

Q5-1

NASCA をインストールしたコンピュータに対して、リモートデスクトップ接続などを使いリモート接続を試みたが、認証に成功しない。

A5-1

ご利用のネットワーク環境によっては、NASCA をインストールしたコンピュータに対して、リモート接続できない可能性があります。リモート接続できない場合は、接続先のコンピュータにインストールされている Windows ログオン認証機能をアンインストールしてください。一部機能をアンインストールする手順については、「3-2-2 一部機能をアンインストール」をご覧ください。

Q5-2

インストールされているNASCA の製品バージョンを調べたい。

A5-2

NASCA の製品バージョンを調べるには、以下の手順を行ってください。

1. **「スタート」ボタン→「すべてのプログラム」→「NEC Authentication Agent(NASCA)」→「インポートユーティリティ」をクリック**
2. **インポートユーティリティのタイトルバーを右クリック**
3. **メニューが表示されたら、「インポートユーティリティについて」をクリック**
   「インポートユーティリティについて」画面が表示されます。
   「インポートユーティリティについて」画面にて、NASCA の製品バージョンを確認することができます。製品バージョンは、画面中央に記載されています。

Q5-3

NASCA の挙動がおかしくなった。アプリケーションの起動やユーザー認証に成功しない。

A5-3

他のアプリケーションなどの動作によってシステムに高負荷がかかっている状況では、その影響で動作が遅くなる場合や正しく動作しなくなる場合があります。このような場合は、以下のいずれかの方法をお試しください。

- しばらく時間を置いてから再度操作を行う。
- Windows を再起動する。

それでも問題が解決しない場合は、NASCA のデータベースが破損している可能性があります。「データベース診断ユーティリティ」を使用して、データベースの診断と初期化を行ってください。

1. **「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「ファイル名を指定して実行」をクリック**
2. **「名前」に「NscChkDB.exe」と入力して、「OK」ボタンをクリック**
3. **「データベース診断ユーティリティ」画面が表示されたら、診断結果が「異常」となっているデータベースのチェックボックスをクリック**
4. **「初期化」ボタンをクリック**
5. **診断結果が「正常」になったことを確認して、「終了」ボタンをクリック**

以上でデータベースの初期化は完了です。
データベースの初期化後は、必要に応じて初期化されたデータを登録し直してください。

チェック

診断の結果、異常が検出されなかった場合やデータベースの初期化完了後も問題が解決しない場合は、NASCA 管理者に連絡し、ユーザー"Nasca-Admin"でログオン後に同じ手順でデータベースの診断を行ってください。

メモ

以下のような現象が起きている場合は、データベースが破損している可能性があります。

- Web フォームバンク機能を使用中に、「データベースオープンに失敗しました」と表示される
- エクスポートユーティリティ／インポートユーティリティが起動しない
- ポリシー設定機能を起動したときに、「情報の取得に失敗しました」と表示される
- ユーザー認証画面で、全デバイスのアイコンが表示されない。または全て「×」が表示されてしまう
- 「Windows へログオン」画面、「コンピュータのロックの解除」画面での認証中にパスワードの更新を要求されるが、パスワードの更新に成功しない