Soliton KeyManager

Soliton KeyManager V2.2　説明書

Soliton

株式会社ソリトンシステムズ　2026 年 4 月

目　次

はじめに

このたびは、株式会社ソリトンシステムズ オリジナルセキュリティ製品「Soliton KeyManager」をご利用いただき、誠にありがとうございます。

Soliton KeyManager（以降、KeyManager）は、弊社のアプリケーションが使用するデジタル証明書のインストールを行うためのツールです。

本ツールを使用することで、弊社の製品と連携して SCEP を使用した証明書のインストールおよびプロファイルの適用、インストールした証明書の確認、削除などを行うことができます。

本書は、Soliton KeyManager のセットアップ方法、および操作方法について説明しています。

本書の表記規則

本書は、次に示す一定の表記規則にしたがって書かれています。

一般

表記例	意味
メニューの [ファイル]-[開く]	メニューのコマンドの選択経路をあらわします。この例では、[ファイル]メニューに含まれている[開く]コマンドをあらわしています。
<OK>、<次へ> <OK>または<適用>	コマンドボタン名は、山カッコ（<>）で囲んであらわします。
「ファイル名」、「入力値」 「画面名」「ダイアログ名」 「参照場所」	構文中のかぎカッコ（「」）で囲んである部分は、ファイル名や入力値などをあらわします。また、画面名やダイアログ名、参照する場所などを示す場合も、かぎカッコ（「」）で囲んであらわします。
チェックする、チェックしない、チェックをはずす	メニューのコマンドやダイアログのチェックボックスなどを ON（または OFF）することをあらわします。

キー操作

表記例	意味
[Shift]キー	キーは、大カッコ（[]）で囲んであらわします。
[F]→[O]キー	キーが右矢印（→）で区切られている場合は、それぞれのキーを順に押すことをあらわします。この例では、[F]キー、[O]キーを順に押すことをあらわしています。
[Ctrl]+[A]キー	2 つのキーの間にあるプラス記号（+）は、最初のキーを押しながら 2 番目のキーを押すことをあらわします。この例では、[Ctrl]キーを押しながら、[A]キーを押すことをあらわしています。
矢印キー	[→]キー、[←]キー、[↑]キー、[↓]キーの総称です。

記号

記号	意味
	「注意事項」を意味します。使用方法などに関する注意事項や、設定を行う際の注意事項を説明しています。
	「関連」を意味します。設定を行う際の関連箇所を説明しています。
※	「注釈」を意味します。簡単な補足説明などのコメントを記述しています。

その他

項目	規則
操作方法	特に記載がない限り、マウスを使用した操作方法で説明しています。
ログイン/ログアウト	特に記載がない限り、「ログイン/ログアウト」「ログオン（サインイン）/ログオフ（サインアウト）」の操作および機能名称については、「ログイン/ログアウト」を使用して説明しています。

本書で使用される用語

- NetAttest EPS

  プライベート証明機関機能を備えた、IEEE802.1X 認証サーバーの機能を提供する弊社のアプライアンス製品です。

- NetAttest EPS-ap

  NetAttest EPS のオプション製品です。NetAttest EPS と連携し、コンピューターやスマートデバイスへの証明書配布と利用ポリシーの適用を自動化することができます。

- Soliton ID Manager

  NetAttest EPS と連携し、コンピューターやスマートデバイスへの証明書配布と利用ポリシーの適用を自動化することができる弊社製品です。(V2.2.12 以降は証明書の発行機能は廃止されるため利用できません)

- Soliton OneGate

  Soliton OneGate（以降、OneGate）は、クラウドサービスの ID 管理とシングルサインオン、多要素認証を簡単にかつセキュアに行える弊社の認証基盤サービスです。

- APID

  Soliton KeyManager が独自に持つ識別番号です。

- ワンタッチ証明書配布

  OneGate や NetAttest EPS-ap からの招待メールに記載された KeyManager 用の URL を使用して証明書を取得する方法です。

- ゼロタッチ証明書配布

  Soliton KeyManager のコマンドラインを利用した証明書配布方法(Windows)です。

1　KeyManager の概要

この章では、KeyManager の概要について説明します。

1.1　KeyManager の機能概要

KeyManager は、NetAttest EPS-ap、Soliton ID Manager（以降、ID Manager）、Soliton OneGate（以降、OneGate）の申請フロー機能による SCEP を使用した証明書のインストール、証明書の確認、削除機能を提供します。

本書では、連携する機器（NetAttest EPS、NetAttest EPS-ap、ID Manager、OneGate）で必要な設定がされていることを前提として説明します。連携機器の設定方法については、各製品マニュアルを参照してください。

- Windows 版

  Wi-Fi、VPN での証明書認証用の他、Soliton SecureBrowser II など、その他アプリで利用する証明書のインストールを行います。

2　セットアップ

この章では、KeyManager のセットアップ方法について説明します。

2.1　動作環境

KeyManager V2.2 の動作環境は、以下のとおりです。

表 2.1　動作環境（Windows）

項目	内容
OS	Windows 11
言語*1	日本語/英語
その他	以下の製品および環境が必要です。 ・NetAttest EPS V5.2.x/V5.0.x/V4.10.x ・NetAttest EPS-ap V2.6.x ・Soliton ID Manager V2.2.0 以降（V2.2.12 以降は利用できません） ・Soliton OneGate ・.Net Framework 4.6.1 以降

*1　OS の言語設定に合わせて表示します。未対応言語の場合は「英語」で表示します。

- **Windows 版 KeyManager について**
  - **.Net Framework 4.6.1 以降が必要です。**
  - **on ARM は、サポート対象外です。**
  - **IA64 は、サポート対象外です。**
  - **64 ビット OS については、WOW64 上での動作をサポートします。**
  - **SSL/TLS 暗号やプロキシサーバーに関する動作は OS の設定に依存します。**
- **各 OS での最新の対応状況については弊社 Web サイトをご確認ください。**

  「各種 OS、仮想化環境、ウイルス対策ソフトウェアへの対応状況」

  https://www.soliton.co.jp/support/win_virus.html
- **Soliton ID Manager V2.2.12 以降では証明書発行機能が廃止されるため KeyManager から利用できません。**

2.2　KeyManager のインストール

ここでは KeyManager のインストール方法について説明します。

- **弊社 Web サイトより最新バージョンのリリース状況をご確認ください。**

  https://www.soliton.co.jp/support/soliton/hardware/skm/

2.2.1　Windows 版

Windows 版 KeyManager のインストール、アップデート、アンインストール方法について説明します。

例として Windows 版 KeyManager V2.2.0 を使用して説明します。各手順内のバージョン表記部分は、実際にインストールするバージョンに読み替えてください。

2.2.1.1　インストールする

Windows 版 KeyManager は、弊社の Web サイトからダウンロードすることができます。

Windows 版 KeyManager のインストールは、以下の手順で行ってください。

1. KeyManager をインストールするコンピューターに、Administrator 権限のユーザーでログインしてください。
2. ダウンロードした「SolitonKeyManagerV220_Windows.zip」を、任意の場所に解凍してください。
3. 解凍したフォルダー内の「SolitonKeyManagerV220.exe」を実行してください。

図 2.2.1　SolitonKeyManagerV220.exe

4. 図 2.2.2 が表示されます。<インストール>をクリックしてください。

※ユーザーアカウント制御の画面が表示された場合は、<はい>をクリックしてください。

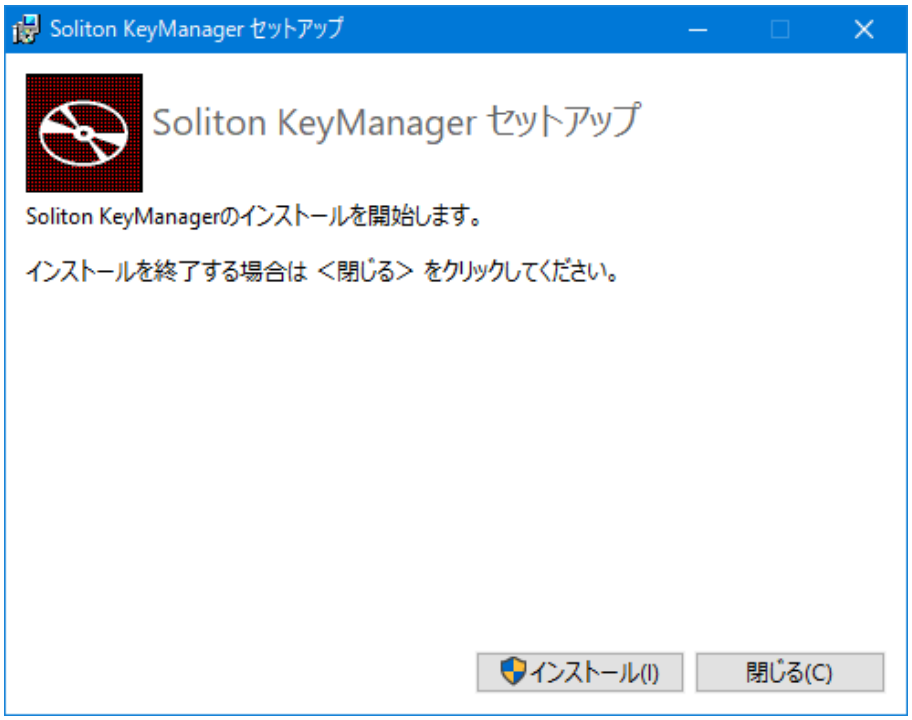

図 2.2.2　セットアップ

5. 図 2.2.3 が表示されます。<次へ>をクリックしてください。

図 2.2.3　ようこそ

6. 図 2.2.4 が表示されます。使用許諾契約の内容を確認したうえで[使用許諾契約書に同意します]をチェックし、<次へ>をクリックしてください。

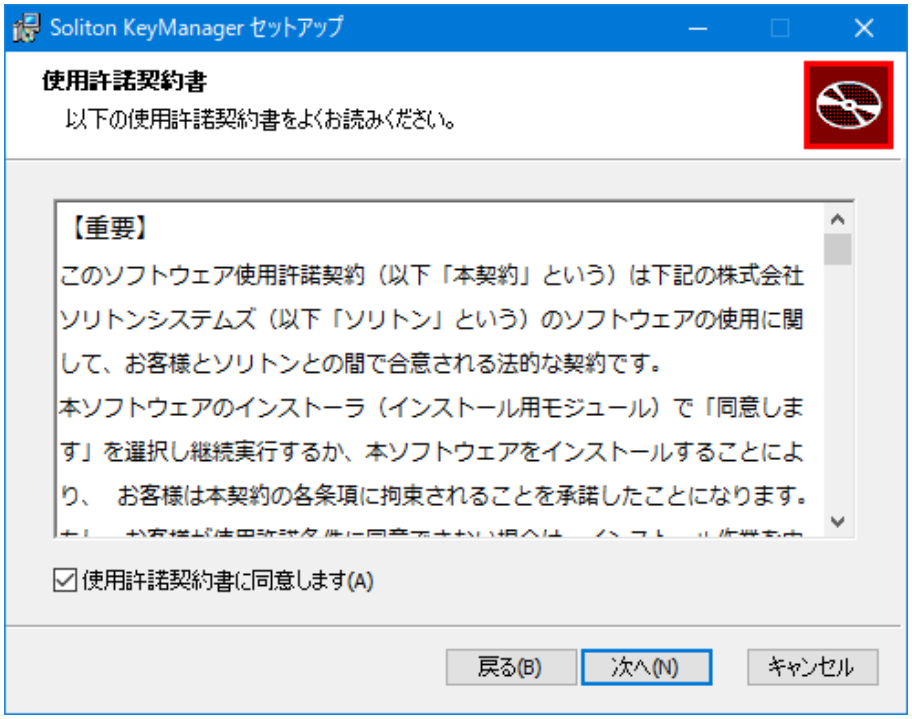

図 2.2.4　使用許諾契約書

7. 図 2.2.5 が表示されます。インストール先のフォルダーを変更する場合は、<変更>をクリックしインストール先のフォルダーを指定し、<次へ>をクリックしてください。[デスクトップにショートカットを作成する。]がチェックされている場合、インストール後デスクトップにショートカットが作成されます。

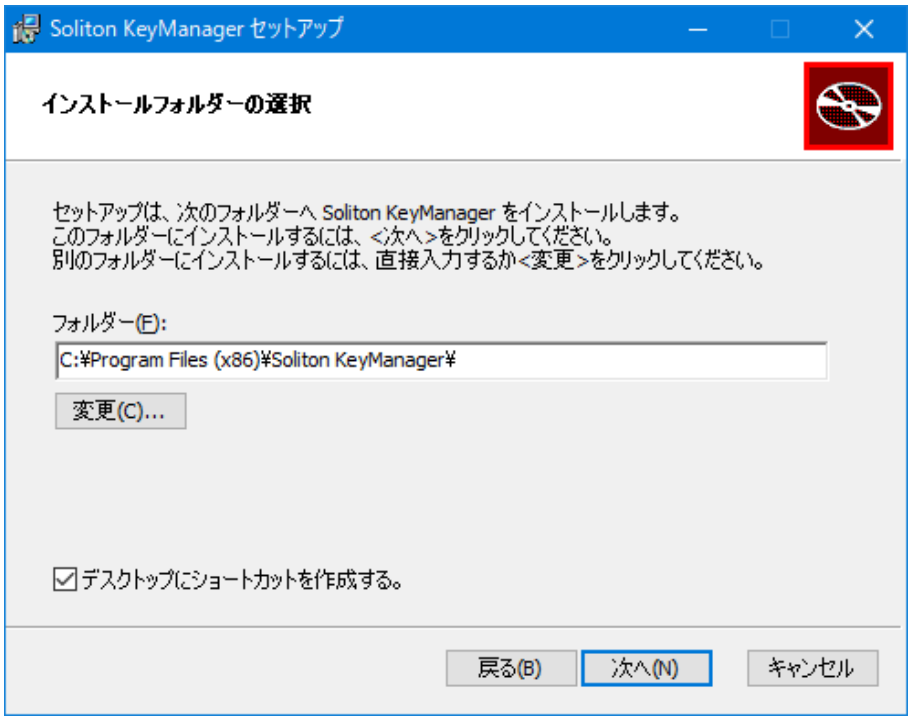

図 2.2.5　インストールフォルダーの選択

8. 図 2.2.6 が表示されます。<インストール>をクリックしてください。

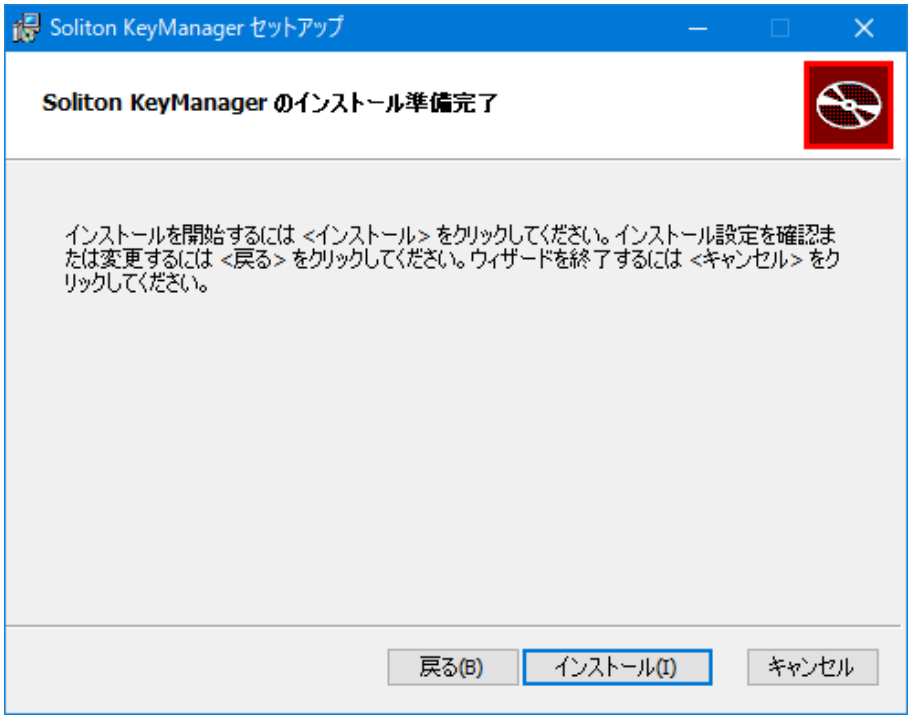

図 2.2.6　インストール準備完了

9. 図 2.2.7 が表示されます。<閉じる>をクリックしてください。

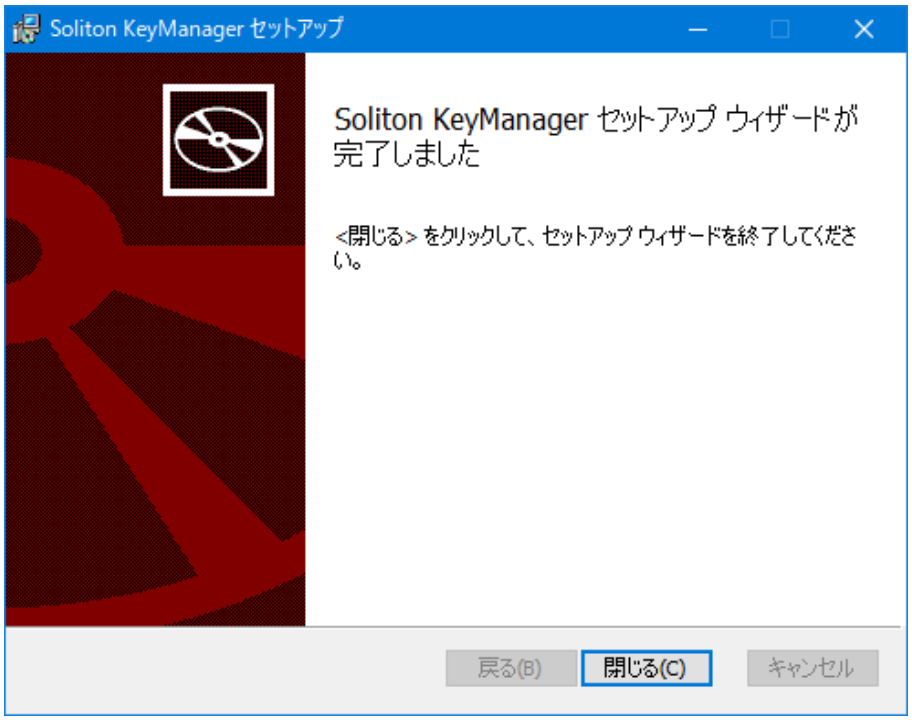

図 2.2.7　セットアップウィザード完了

10. 図 2.2.8 が表示されます。<終了する>をクリックしてください。

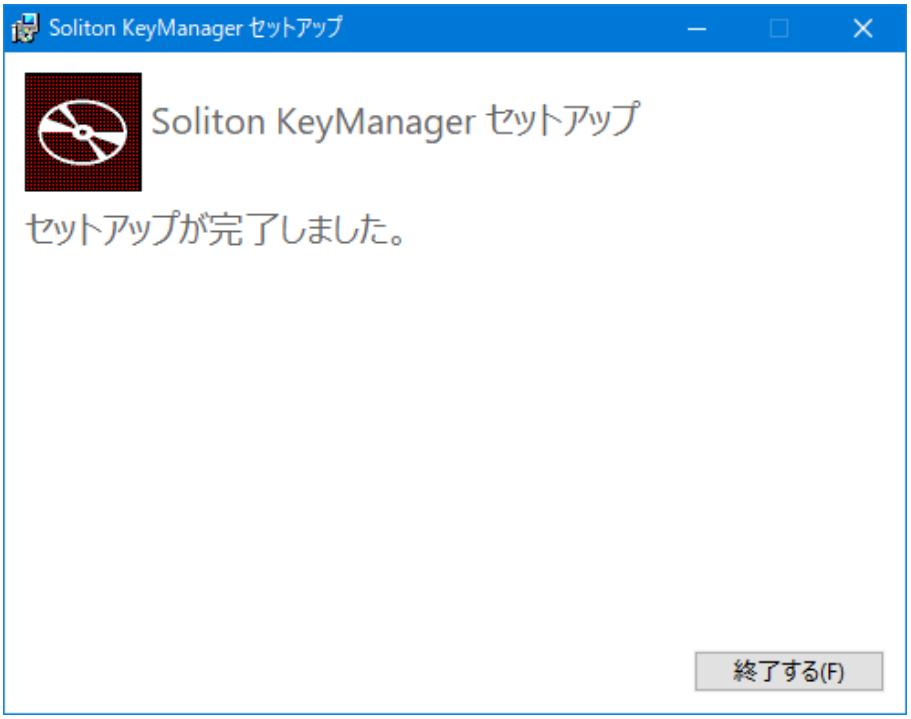

図 2.2.8　セットアップ完了

❑ サイレントインストール

コマンドオプションを指定することで、Windows 版 KeyManager をサイレントインストールすることができます。ここでは、SolitonKeyManagerV220.exe が「C:¥work」フォルダーにある場合を例として記載します。

```
>C:¥work¥SolitonKeyManagerV220.exe -s
```

デフォルトではサイレントインストールでは「デスクトップにショートカットを作成する」オプションは有効になるため、デスクトップにショートカットが作成されます。

「デスクトップにショートカットを作成する」オプションを無効にするにはコマンドオプションを指定してください。

```
>C:¥work¥SolitonKeyManagerV220.exe -s installdesktopshortcut=0
```

「installdesktopshortcut」を「0」に指定することで「デスクトップにショートカットを作成する」オプションが無効になります。「1」に指定すると有効になります(デフォルト)。

- **サイレントインストールを行った場合、本製品の使用許諾契約に同意したことになります。サイレントインストールでは、使用許諾契約書が表示されず、使用許諾契約に同意するための確認画面も表示されません。**

❑ キッティングインストール

キッティングインストールは、OS のディスクイメージを使用した端末展開を実施する際に利用する機能です。コマンドオプションを指定することで、Windows 版 KeyManager をキッティング用にインストールすることができます。

ここでは、SolitonKeyManagerV220.exe が「C:¥work」フォルダーにある場合を例として記載します。

```
>C:¥work¥SolitonKeyManagerV220.exe kitting=1
```

- **キッティングインストールは Windows 版 KeyManager V2.0.4 以降から利用できます。**
- **キッティングインストールを行った場合、APID の生成を行わずにインストールを完了することができます。**

  キッティングインストール後、アプリの起動、PC 再起動など、その他の作業は行わずに速やかに PC を終了し、マスターとなる OS のディスクイメージを作成してください。

  KeyManager が正しくキッティング、イメージ展開されているか確認するには、展開した 2 台以上のクライアントコンピューターで KeyManager を起動し、APID を比較してください。

  クライアントコンピューター毎に異なる APID が割り当てられていれば正常なイメージ展開が行われています。
- **キッティングインストールを行った場合、すでに生成済みの APID は削除されます。APID が読み込めずに KeyManager が起動しない問題などが発生した場合は、アンインストール後キッティングインストールを実施してください。**

2.2.1.2　アップデートする

Windows 版 KeyManager のアップデートは、以下の手順で行ってください。

- **Windows 版 KeyManager V1.4.3 以前がインストールされている場合は、V1.4.4 を経由してから V2.2.0 へアップデートしてください。**

1. KeyManager をアップデートするコンピューターに、Administrator 権限のユーザーでログインしてください。
2. 弊社の Web サイトからダウンロードした「SolitonKeyManagerV220_Windows.zip」を、任意の場所に解凍してください。
3. 解凍したフォルダー内の「SolitonKeyManagerV220.exe」を実行してください。

図 2.2.9　SolitonKeyManagerV220.exe

4. 図 2.2.10 が表示されます。<インストール>をクリックしてください。
   ※ユーザーアカウント制御の画面が表示された場合は、<はい>をクリックしてください。

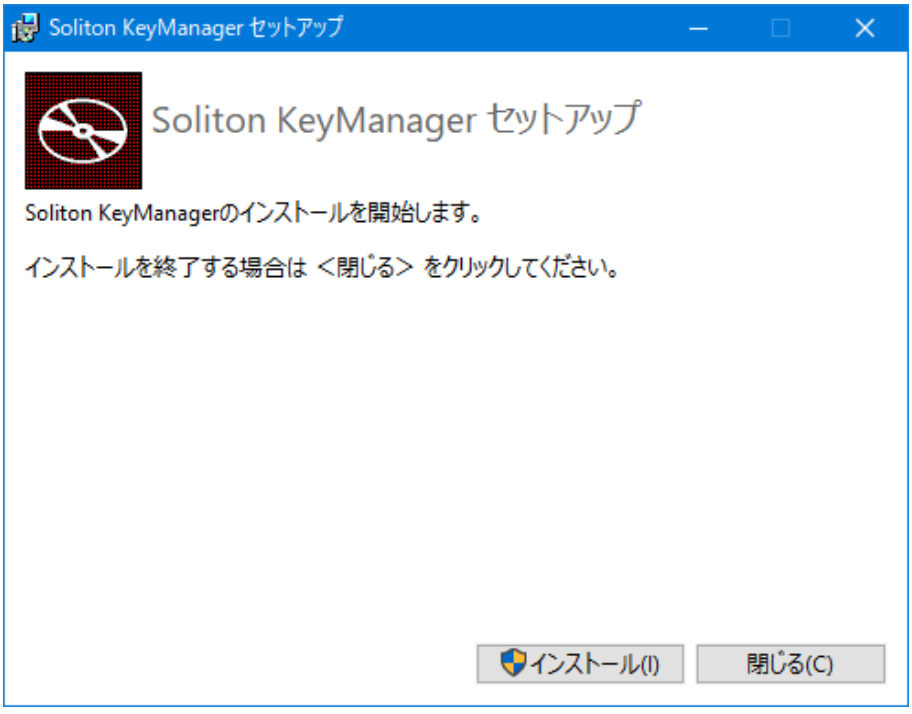

図 2.2.10　セットアップ

5. 図 2.2.11 が表示されます。<閉じる>をクリックしてください。

図 2.2.11　セットアップウィザード完了

6. 図 2.2.12 が表示されます。<終了する>をクリックしてください。

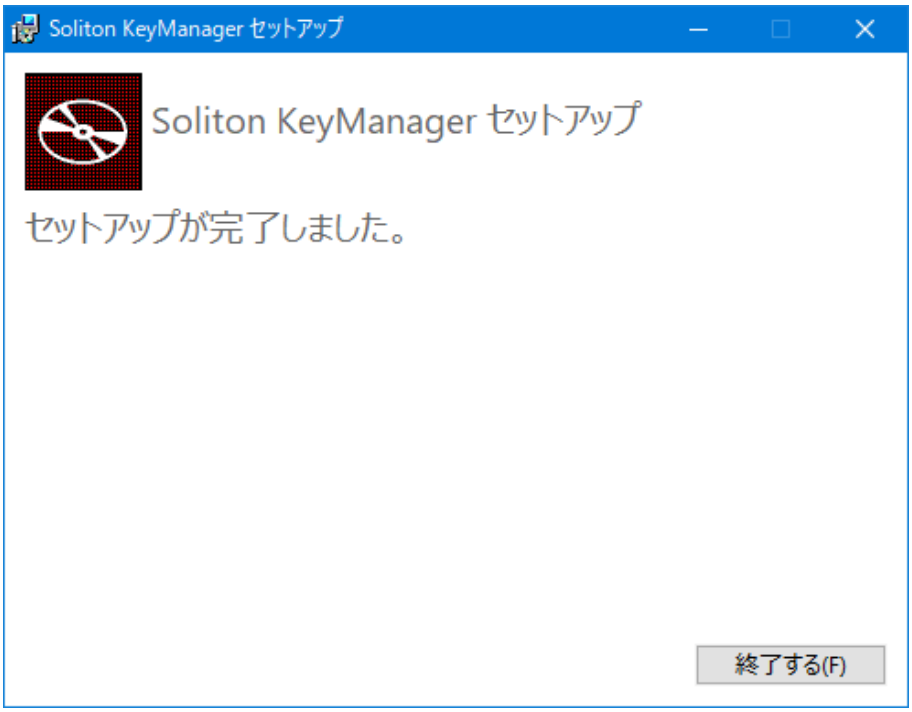

図 2.2.12　セットアップ完了

- **サイレントインストールを実施した際に Windows 版 KeyManager が起動していた場合、強制的に OS が再起動されます。**
- **アップデートした場合、以下の情報が変化する事はありません。**
  - **証明書一覧の情報**
  - **申請中の証明書の情報**
  - **設定情報**
  - **APID**

2.2.1.3 アンインストールする

Windows 版 KeyManager は、以下のいずれかの方法でアンインストールを行うことができます。

Windows 版 KeyManager がインストールされているコンピューターに Administrator 権限のユーザーでログインしてください。

- 「プログラムと機能」を起動して「Soliton KeyManager」を選択し、<アンインストールと変更>をクリックしてください。「Soliton KeyManager セットアップ」で「削除」を選択して、KeyManager をアンインストールしてください。
- インストール時に使用した「SolitonKeyManagerV220.exe」をダブルクリックし、「Soliton KeyManager セットアップ」で[削除]を選択して、KeyManager をアンインストールしてください。

❑ サイレントアンインストール

コマンドオプションを指定することで、Windows 版 KeyManager をサイレントアンインストールすることができます。ここでは、SolitonKeyManagerV220.exe が「C:¥work」フォルダーにある場合を例として記載します。

```
>C:¥work¥SolitonKeyManagerV220.exe -s -uninstall
```

- **Windows 版 KeyManager をアンインストールした場合、通知設定や申請情報、証明書の一覧情報は削除されますが、各証明書ストアに格納された証明書は削除されません。**

  またアンインストールを行っても、APID は保持されます。

3　KeyManager の使用方法

ここでは KeyManager を使用した申請の手順、承認状況の確認、アクティベーション(利用開始手続き)の進め方、証明書の更新、および APID の確認方法について説明します。

3.1　アプリの起動

KeyManager の起動方法について説明します。

3.1.1　PC

1.　「Soliton KeyManager」のアイコンをタップまたはクリックしてください。

図 3.1.1　KeyManager

2.　図 3.1.2 が表示され、KeyManager が起動します。

図 3.1.2　ホーム画面

3.2　APID

KeyManager の APID を確認する方法について説明します。

APID は、デバイスを一意に識別するため KeyManager が割り当てた独自の ID です。NetAttest EPS-ap や ID Manager または OneGate の UDID/APID チェックが有効に設定されている場合、アクティベーションを行う前に APID を登録する必要があります。

3.2.1　PC

1. 「Soliton KeyManager」のアイコンをタップまたはクリックして KeyManager が起動し、ホーム画面の右上にある<APID>ボタンをタップまたはクリックしてください。

図 3.2.1　ホーム画面-APID ボタン

2. APID が表示されます。

図 3.2.2　APID

❑ クリップボードにコピー

APID 画面で<クリップボードにコピー>をタップまたはクリックすると、表示されている APID をクリップボードにコピーすることができます。

❑ メールで送信

APID 画面で<メールで送信>をタップまたはクリックすると、OS のデフォルトに設定されているメールアプリケーションを使用して、件名に「Soliton KeyManager APID」、本文に APID が設定された状態でメール作成画面を表示します。

3.3　新しい証明書

KeyManager を使用して新規に証明書を取得するための申請手順について説明します。

3.3.1　PC

1. ホーム画面で<新しい証明書>をタップまたはクリックしてください。

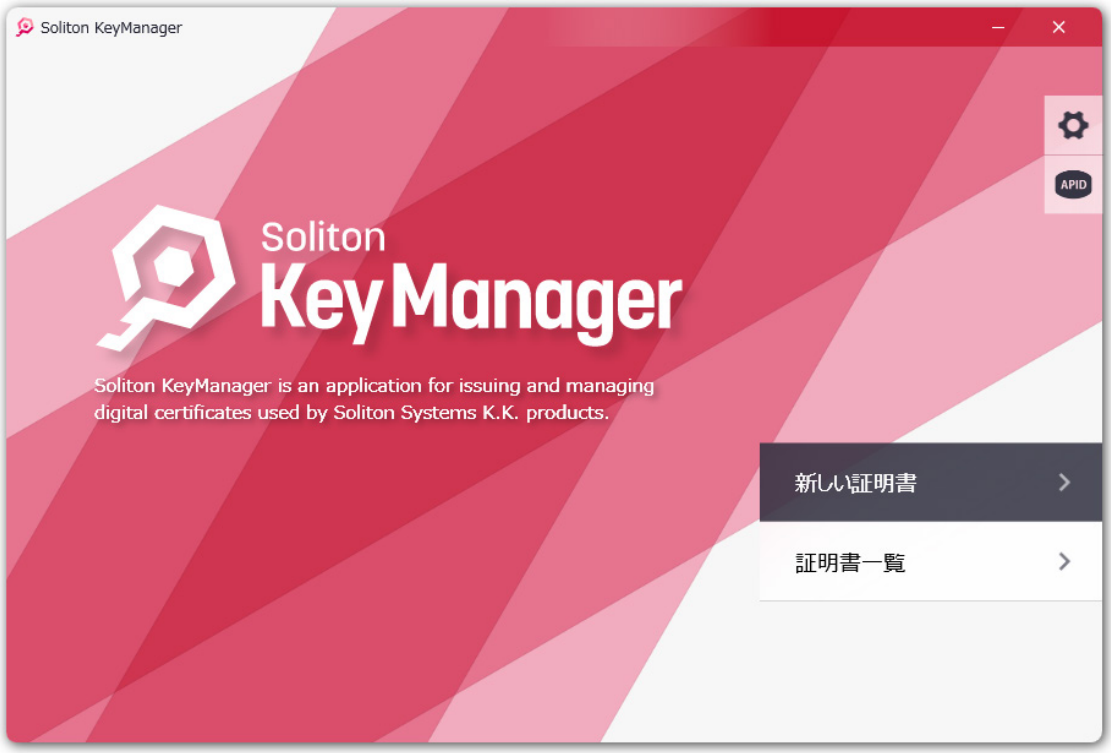

図 3.3.1　ホーム画面

2. 図 3.3.2 が表示されます。ホスト名または IP アドレス、ポート番号を入力し<次へ>をタップまたはクリックしてください。

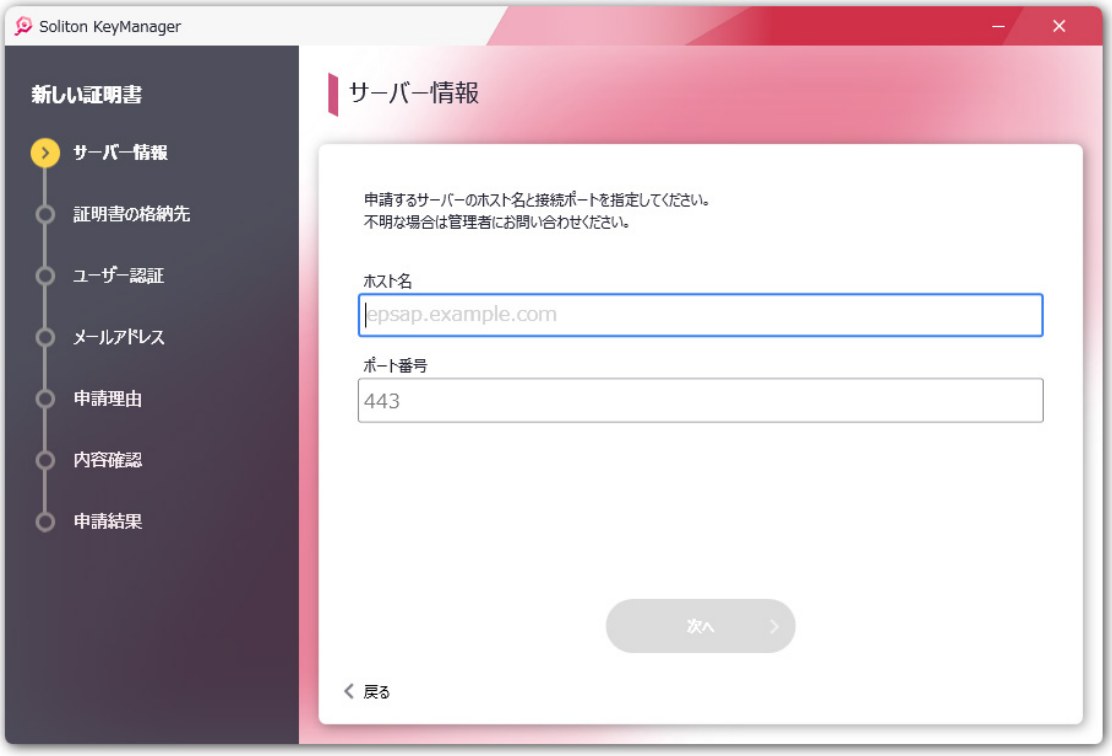

図 3.3.2　サーバー情報

3. 接続先が信頼されていない場合、図 3.3.3 の警告メッセージが表示されます。接続を続けるには<OK>をタップまたはクリックしてください。

   ※接続先が信頼されている場合、図 3.3.3 は表示されません。手順 4 に進んでください。

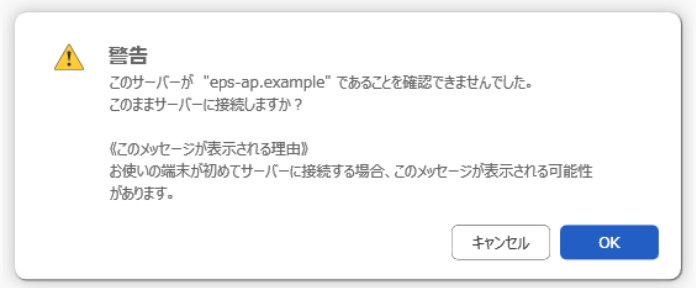

図 3.3.3　警告メッセージ

4. サーバーの配布する CA 証明書がインストールされていない場合、CA 証明書をダウンロードしてインストールを行います。

   ※CA 証明書がすでにインストールされている場合は、手順 5 に進みます。

- **CA 証明書のダウンロード、インストール手順は「付録 1-1　CA 証明書取得手順（Windows）」を参照してください。**

5. 図 3.3.4 が表示されます。証明書の用途に合わせて格納先を選択してください。

図 3.3.4　証明書の格納先

6. 図 3.3.5 が表示されます。「ユーザーID」「パスワード」を入力して<次へ>をタップまたはクリックしてください。

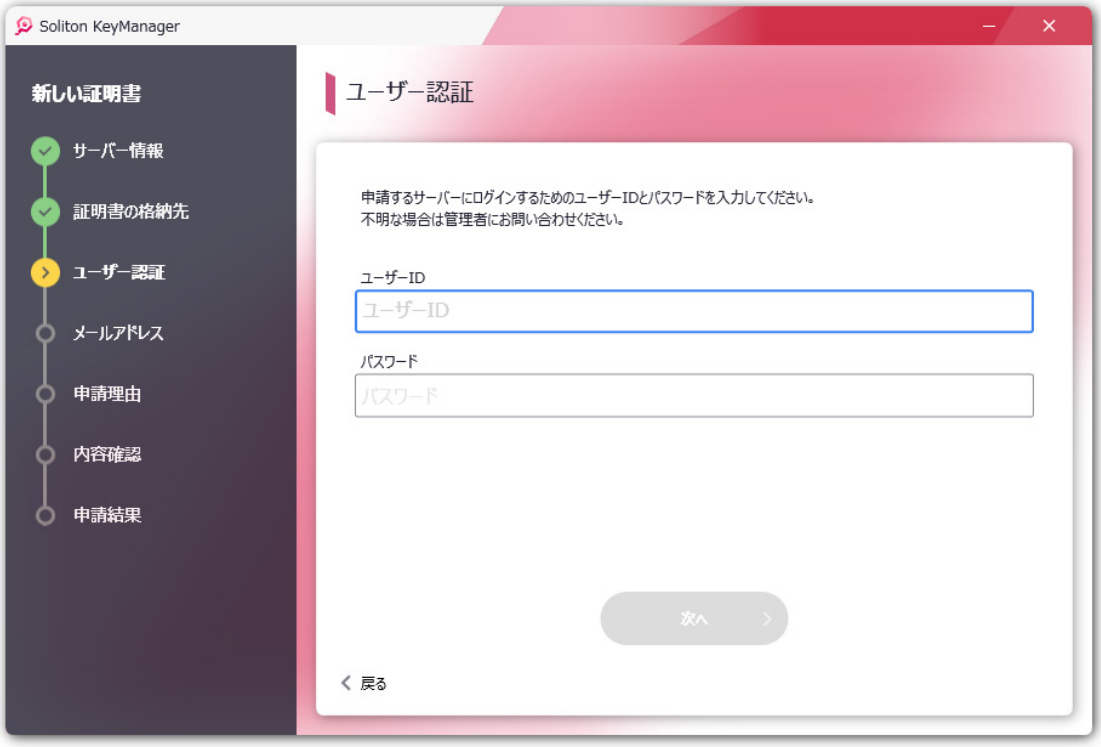

図 3.3.5　ユーザー認証

7. 図 3.3.6 が表示されます。必要に応じて「メールアドレス」を入力し<次へ>、または<スキップ>をタップまたはクリックしてください。

   ※接続先の設定や承認状況により、図 3.3.6 は表示されません。本項の「招待コードを入力」「デバイスの任意情報の入力」または、「3.4　アクティベーション -3.4.1　PC-手順 4」を参考にアクティベーションを行ってください。

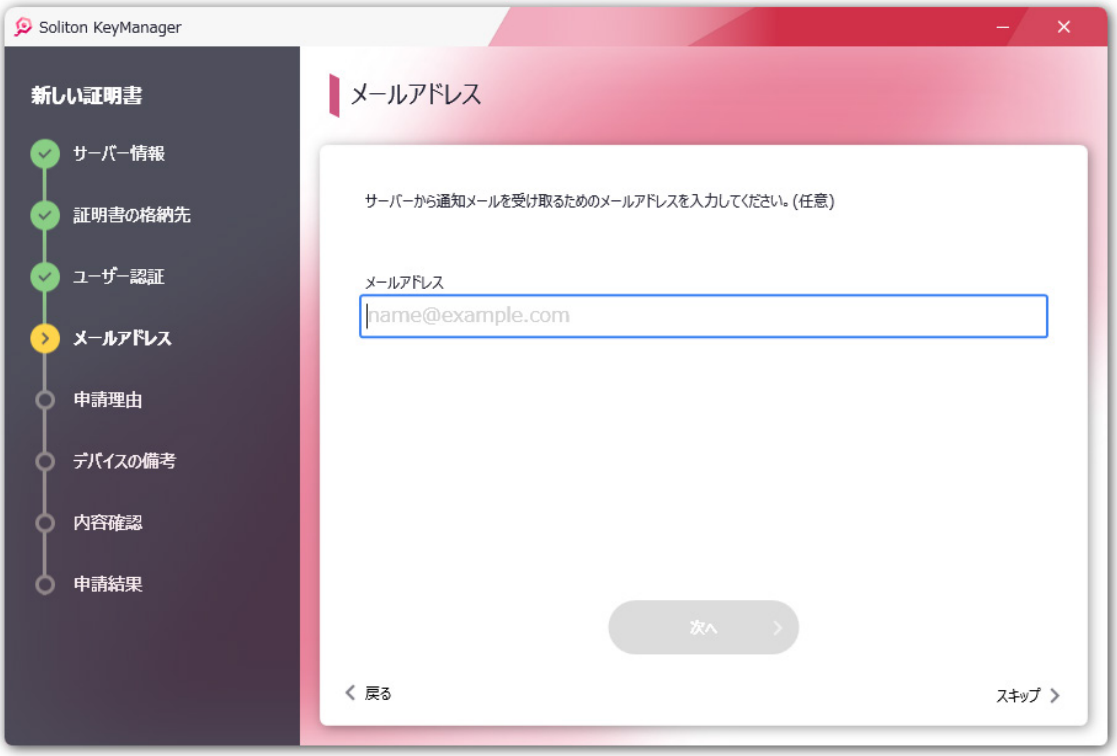

図 3.3.6　メールアドレス

- **メールアドレスに指定できる文字数は 128 文字までです。**

8. 図 3.3.7 が表示されます。必要に応じて「申請理由」を入力し<次へ>、または<スキップ>をタップまたはクリックしてください。

図 3.3.7　申請理由

9. 図 3.3.8 が表示されます。申請内容を確認し<申請>をタップまたはクリックしてください。

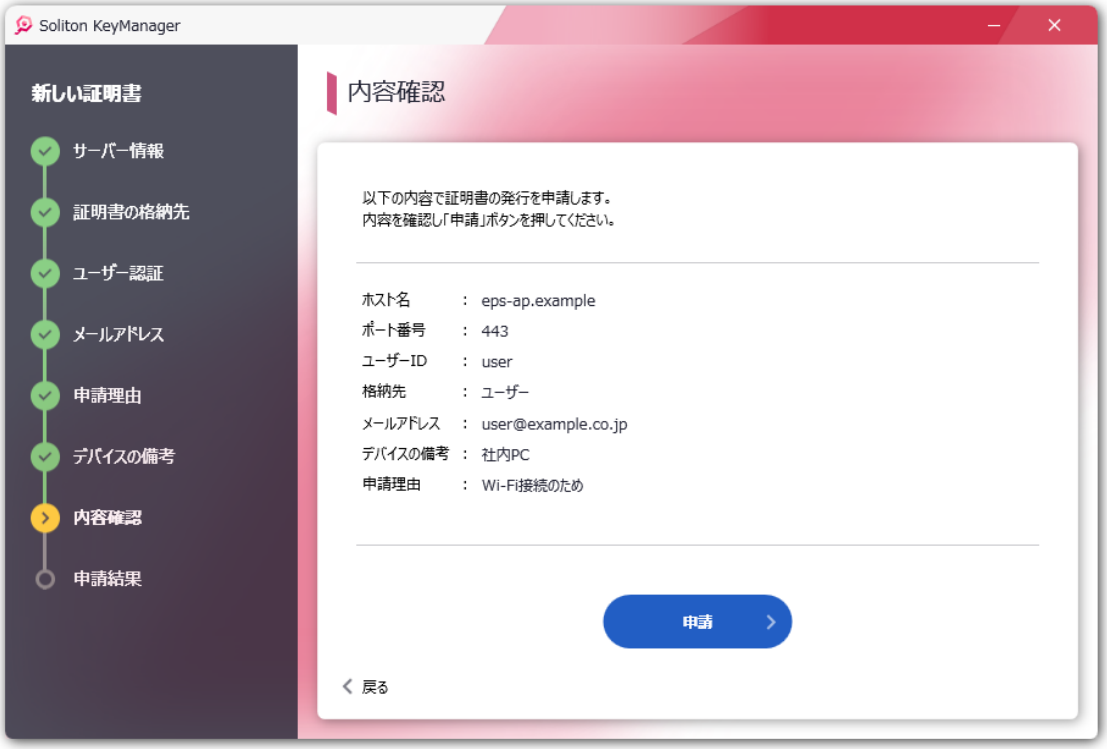

図 3.3.8　内容確認

10. 申請が完了すると図 3.3.9 が表示されます。<ホームに戻る>をタップまたはクリックしてください。
承認状況の確認手順は「3.4　アクティベーション」を参照してください。

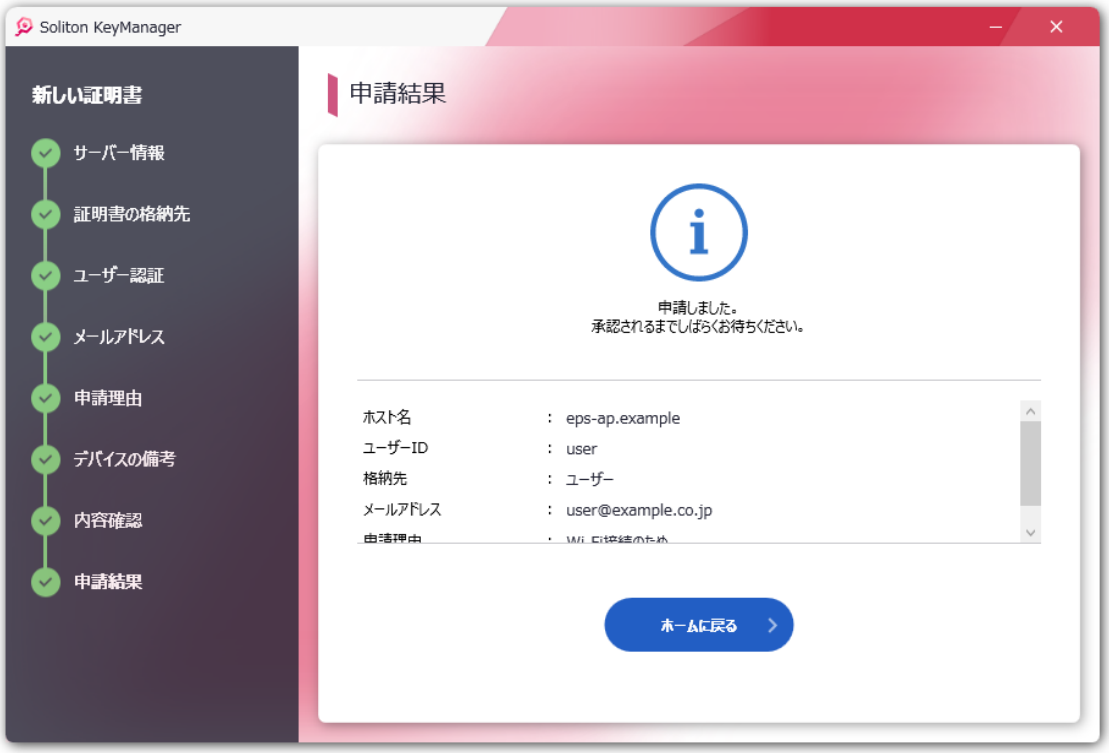

図 3.3.9　申請結果

接続先の設定により、図 3.3.8 の表示の前に「デバイスの備考」画面が表示されます。本項の「デバイスの任意情報の入力」を参考に入力を行ってください。

❑ 招待コードを入力

招待メールを受け取ったユーザーID でアクセスすると、承認状況に合わせて招待コードの入力画面が表示されます。

1. 適切な招待コードを入力し<次へ>をタップまたはクリックしてください。

図 3.3.10　招待コード

2. 図 3.3.11 が表示されます。本書の「3.4　アクティベーション -3.4.1　PC-手順 4」を参考にアクティベーションを行ってください。

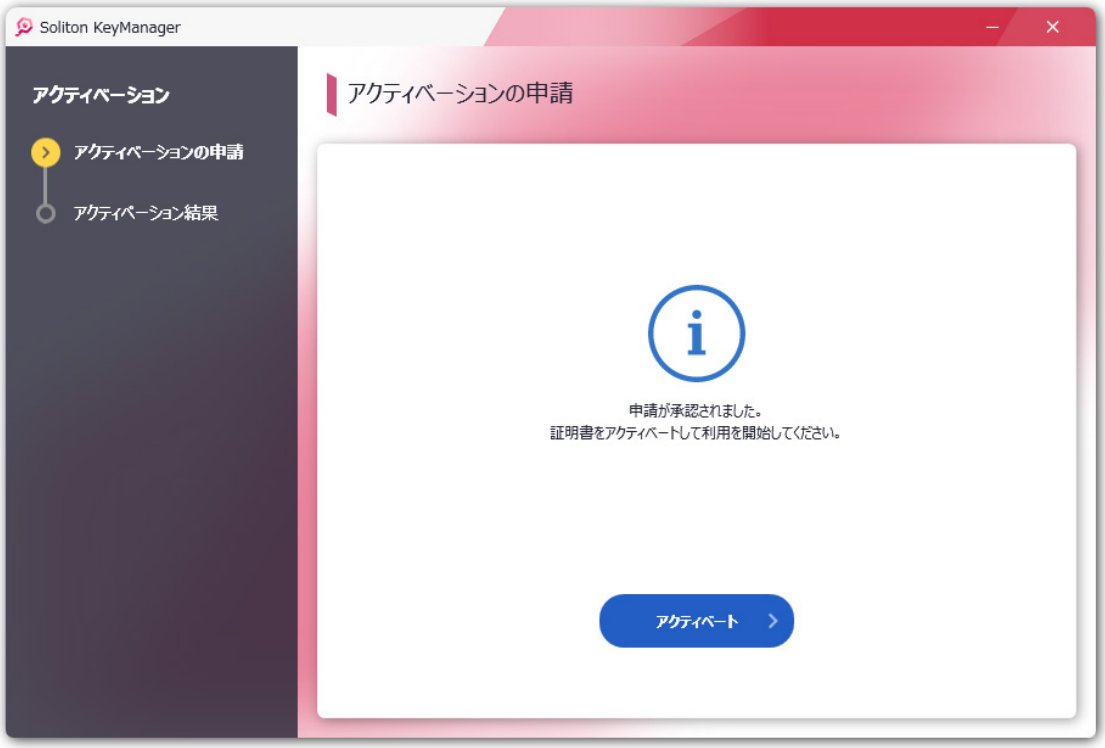

図 3.3.11　アクティベーションの申請

❑ デバイスの任意情報の入力

接続先の設定に合わせて図 3.3.12 が表示されます。

1. 必要に応じて任意情報を入力し<次へ>、または<スキップ>をタップまたはクリックしてください。

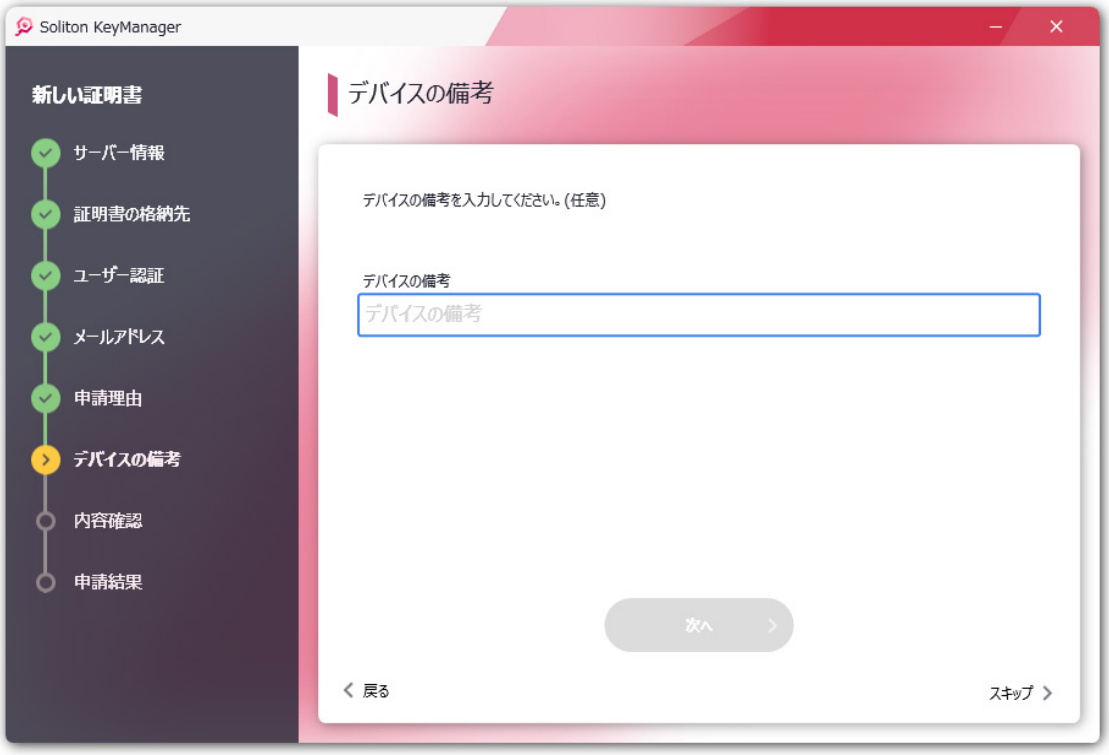

図 3.3.12　デバイスの備考

本書では接続先のデフォルト設定である「デバイスの備考」という項目名で表示されていますが、任意入力欄の項目名は接続先の設定によって変更されます。

2. 画面の指示に従い、本書の「3.3　新しい証明書-3.3.1　PC-手順 9」または「3.4　アクティベーション-3.4.1　PC-手順 4」を参考にアクティベーションを行ってください。

3.4　アクティベーション

申請の承認状況を確認してアクティベーションを行う手順について説明します。

招待モードや自動承認の場合は、申請後に自動的に「アクティベーションの申請」画面が表示されます。

- **申請の承認完了後の操作について、KeyManager V2.0 の画面およびドキュメントでは「利用開始手続き」と表現していましたが、V2.2 では「アクティベーション」「アクティベート」という表現に変更になりました。**

3.4.1　PC

1.　申請中の申請は証明書一覧に追加されます。<証明書一覧>をタップまたはクリックしてください。

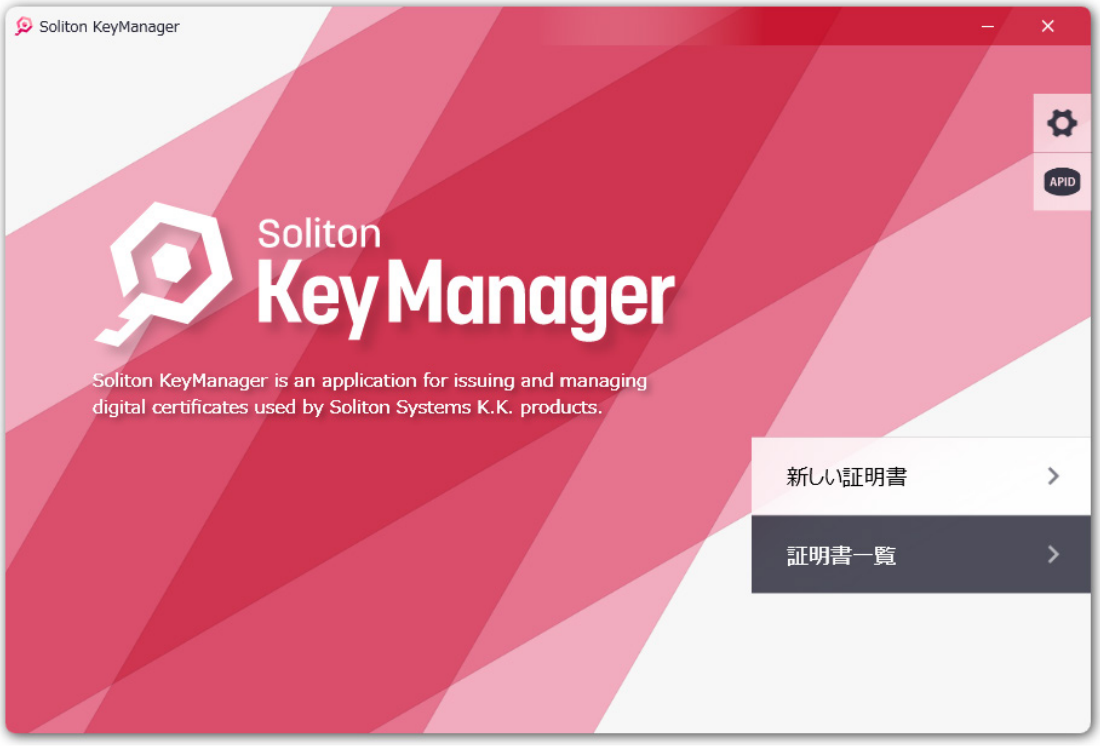

図 3.4.1　ホーム画面-証明書一覧

2. 図 3.4.2 が表示されます。申請の<アクティベート>をタップまたはクリックしてください。

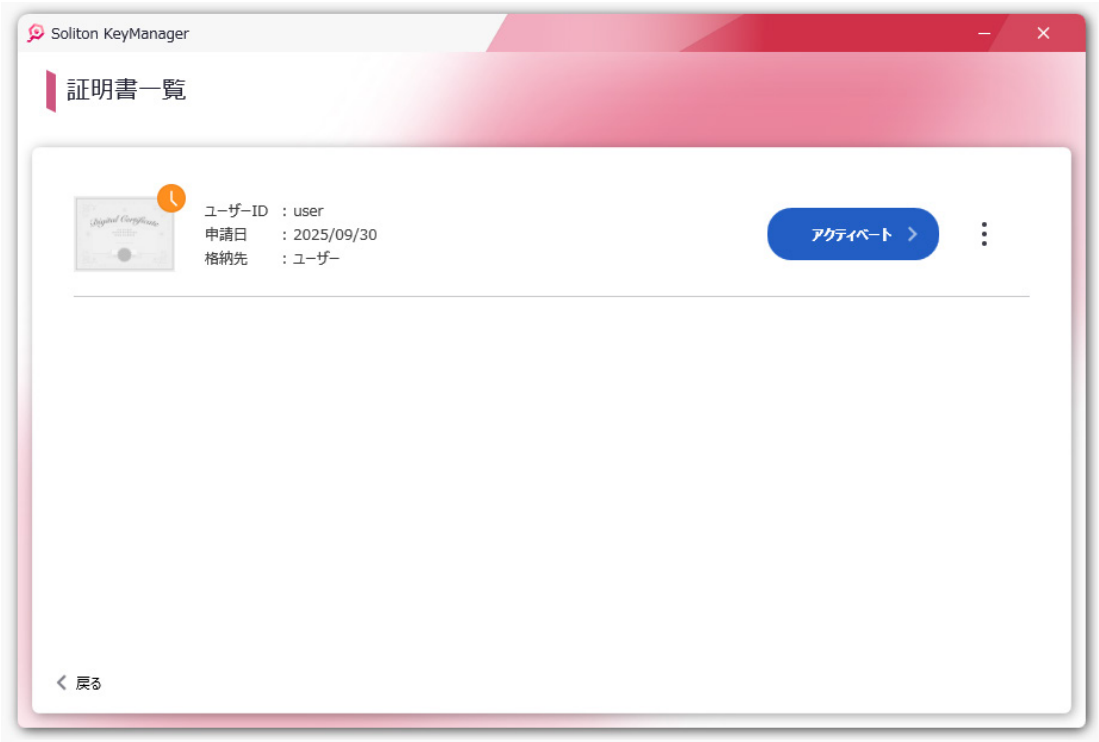

図 3.4.2　証明書一覧–申請

3. 図 3.4.3 が表示されます。「パスワード」を入力し<次へ>をタップまたはクリックしてください。

図 3.4.3　ユーザー認証-アクティベーション

4. 承認が完了していると図 3.4.4 が表示されます。<アクティベート>をタップまたはクリックしてください。

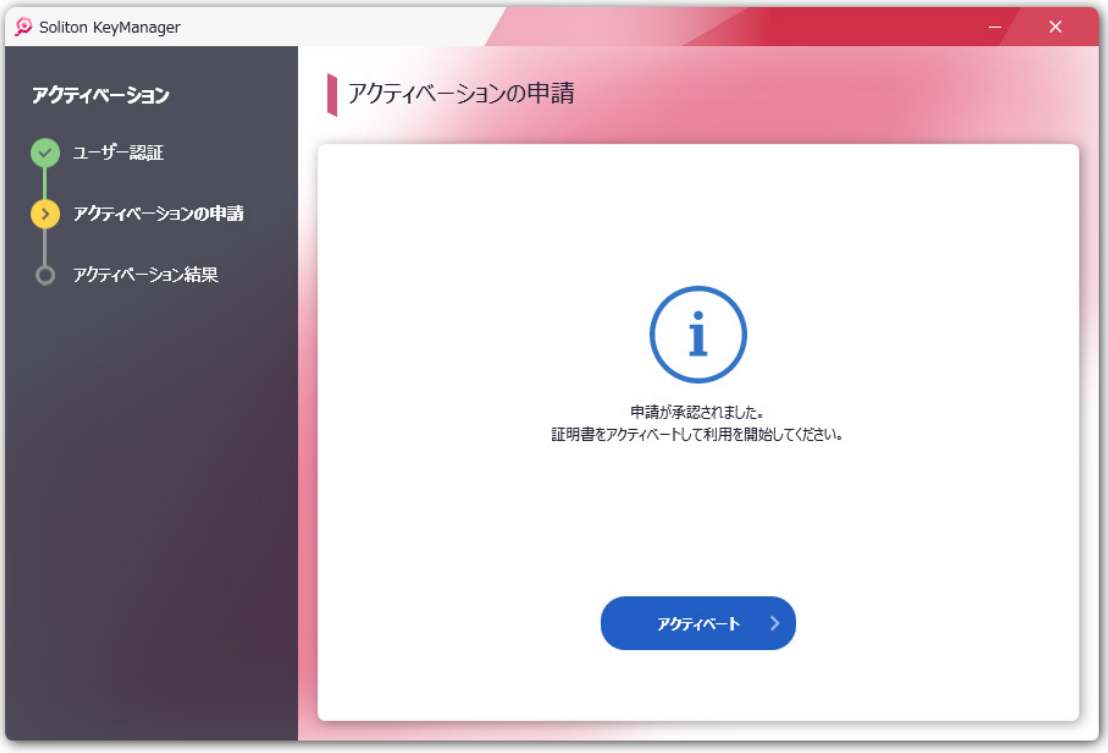

図 3.4.4　アクティベーションの申請

5. 証明書がインストールされるとアクティベーションが完了します。

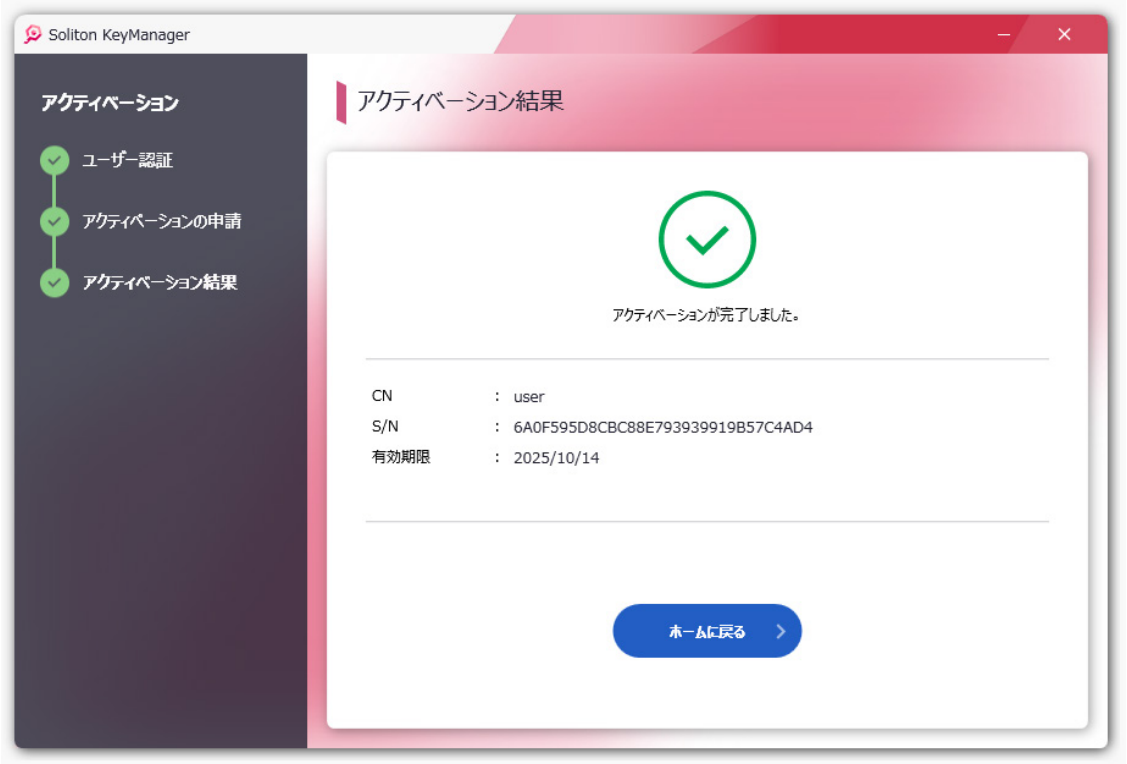

図 3.4.5　アクティベーション結果-完了

- **Windows 版 KeyManager でコンピューターストアに証明書を格納する際、「NetAttest RA Client Admin Module」というアプリを使用します。証明書の格納先に「コンピューター」を選択した場合、「NetAttest RA Client Admin Module」が行うデバイスへの操作を許可するユーザーアカウント制御の画面が表示される場合があります。パスワードの入力等、必要な操作を行い「NetAttest RA Client Admin Module」の操作を許可してください。**
- **Windows 版 KeyManager ではアクティベーション時に、接続先の設定により「CA 証明書配付設定(資格情報)」や、「Wi-Fi 設定」が適用されます。**

❑ 申請が未承認の場合

接続先で申請の承認が完了されていない場合は、図 3.4.5 は表示されず、図 3.4.6 が表示されます。

承認が完了するまでお待ちいただくか、承認者(管理者)に確認してください。

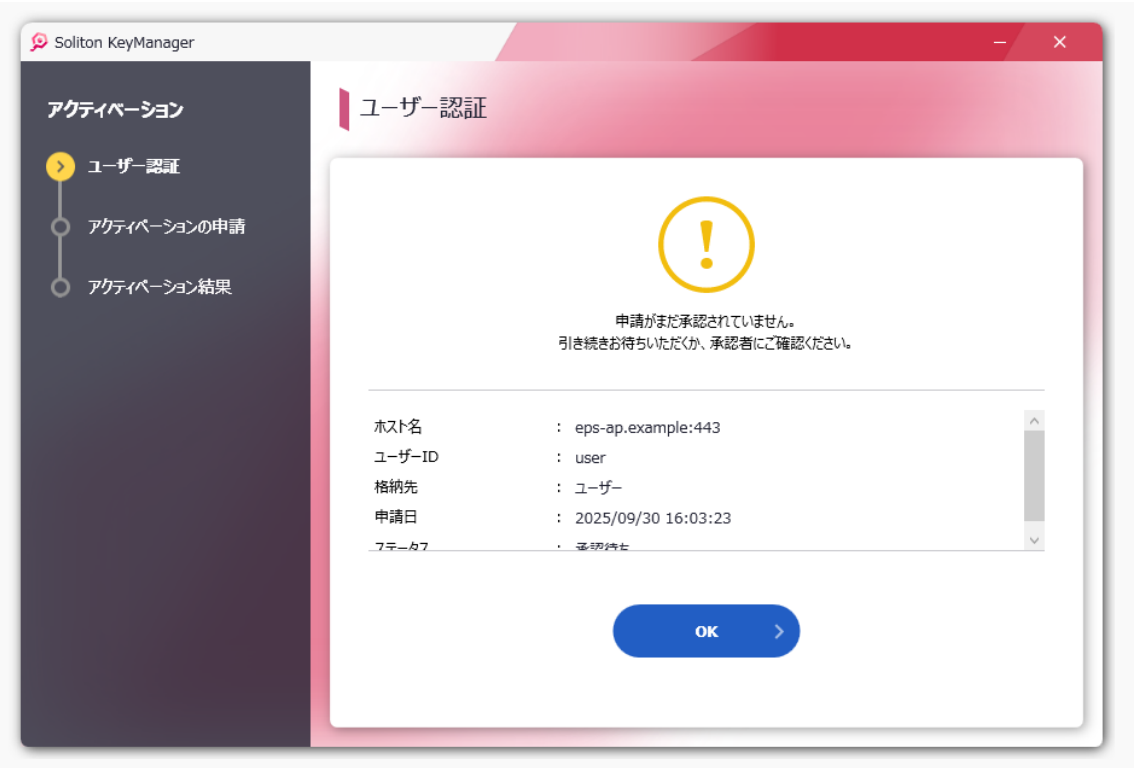

図 3.4.6　未承認-アクティベーション

❑ 申請の取り下げ

申請を取り下げする手順を説明します。申請の取り下げを行うことで接続先の申請が取り下げられます。

1. 申請中の申請は証明書一覧に追加されます。証明書一覧から取り下げたい申請の<⋮>をタップまたはクリックして表示されるメニューから<取り下げ>を選択してください。

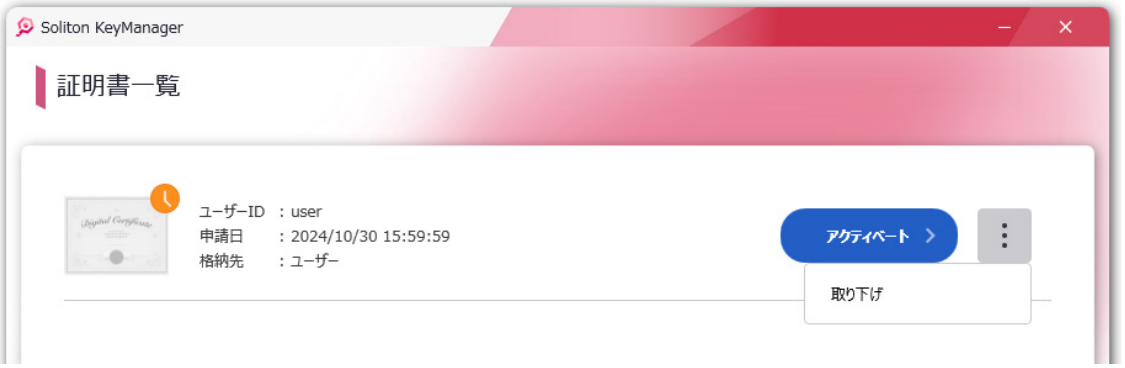

図 3.4.7　取り下げ

2. 図 3.4.8 の申請の取り下げの確認ダイアログが表示されます。<OK>をタップまたはクリックしてください。

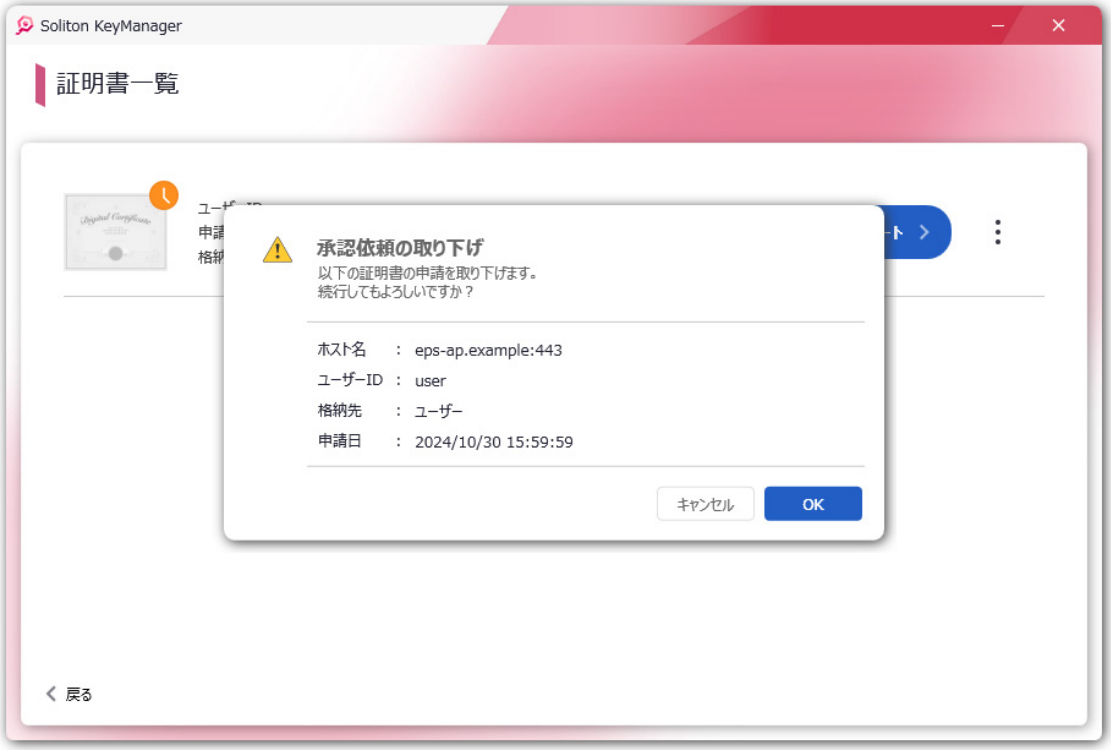

図 3.4.8　確認ダイアログ-取り下げ

3. 図 3.4.9 が表示されます。「パスワード」を入力し<次へ>をタップまたはクリックしてください。

※接続先の設定により、図 3.4.9 はスキップされて図 3.4.10 が表示されます。

図 3.4.9　ユーザー認証-取り下げ

4. 取り下げが完了すると図 3.4.10 が表示されます。

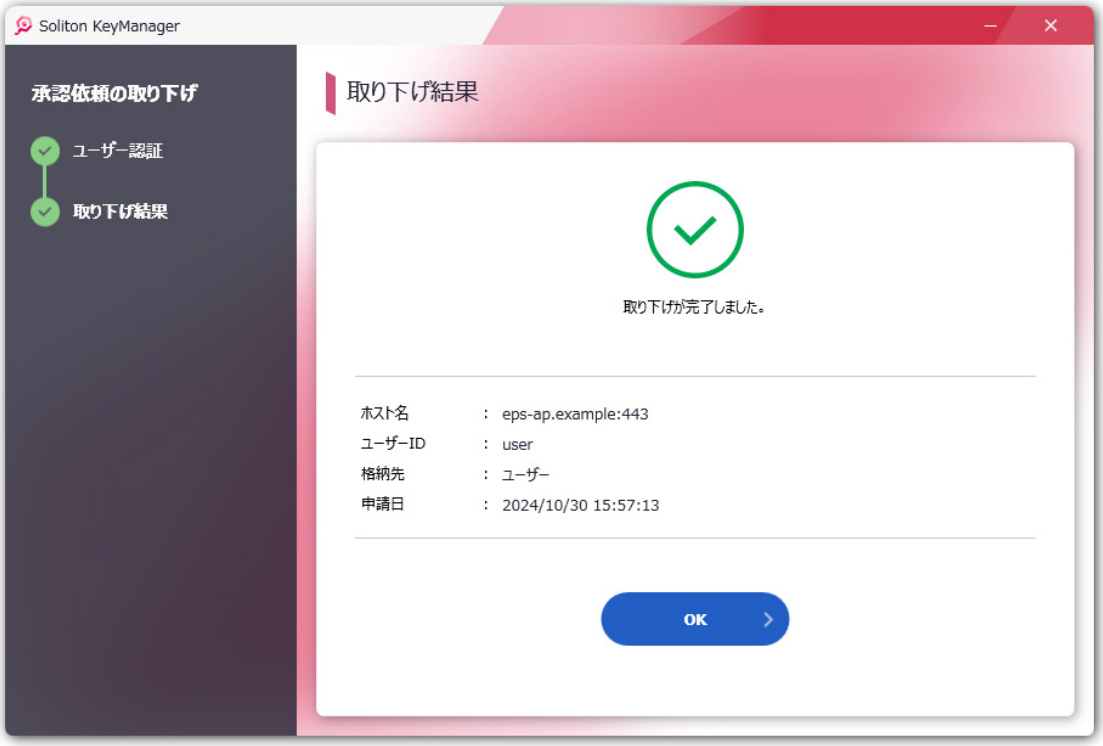

図 3.4.10　取り下げ結果

- 証明書一覧の取り下げ済みの申請は、<⋮>をタップまたはクリックして表示されるメニューから「再申請」、「削除」を行うことができます。
  - <再申請>をタップまたはクリックすると、取り下げた申請と同じ内容で再度申請することができます。
  - <削除>をタップまたはクリックすると、取り下げた申請の情報を端末から削除します。

  申請時にエラーが発生して失敗した際には、取り下げ後に再度新しく申請を行っても同じエラーで失敗する場合があります。その場合は失敗した申請を「取り下げ」後に「削除」を行うようにしてください。

3.5　証明書の更新

証明書の更新は、以下の手順で行ってください。

3.5.1　PC

1. ホーム画面の<証明書一覧>をタップまたはクリックしてください。

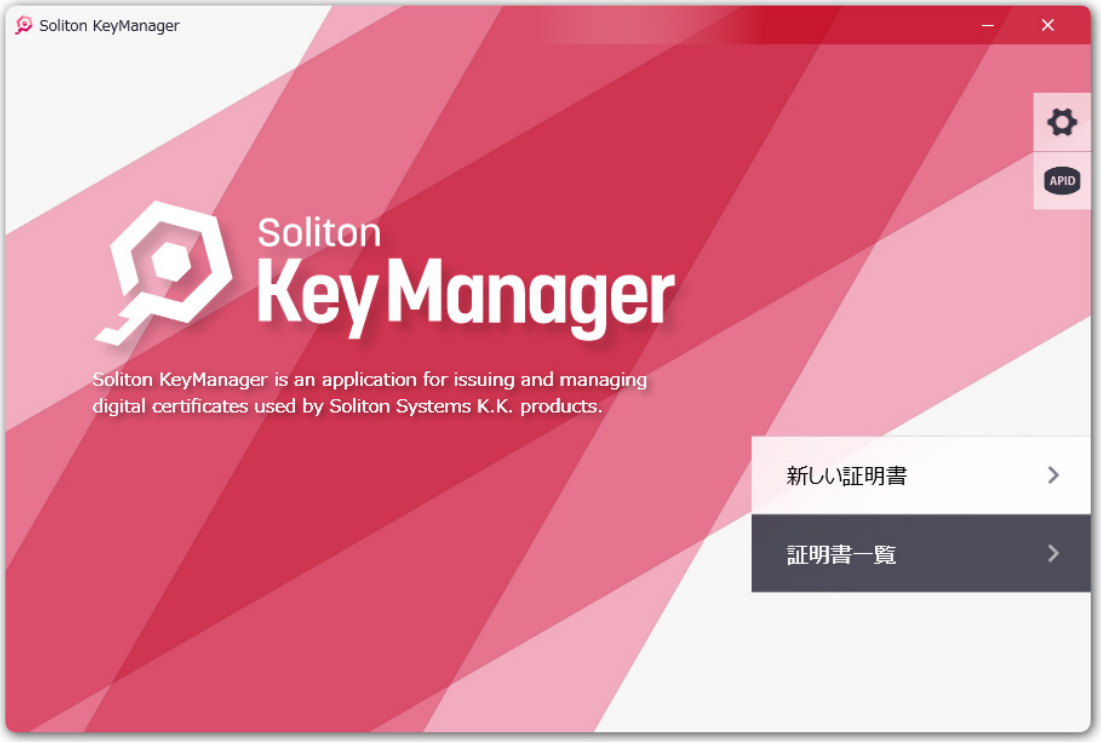

図 3.5.1　ホーム画面-証明書一覧

2. 証明書を取得している場合、更新対象となる証明書の一覧が表示されます。有効期限が近づいている証明書には<更新>ボタンが表示されますので、更新したい証明書の<更新>をタップまたはクリックしてください。

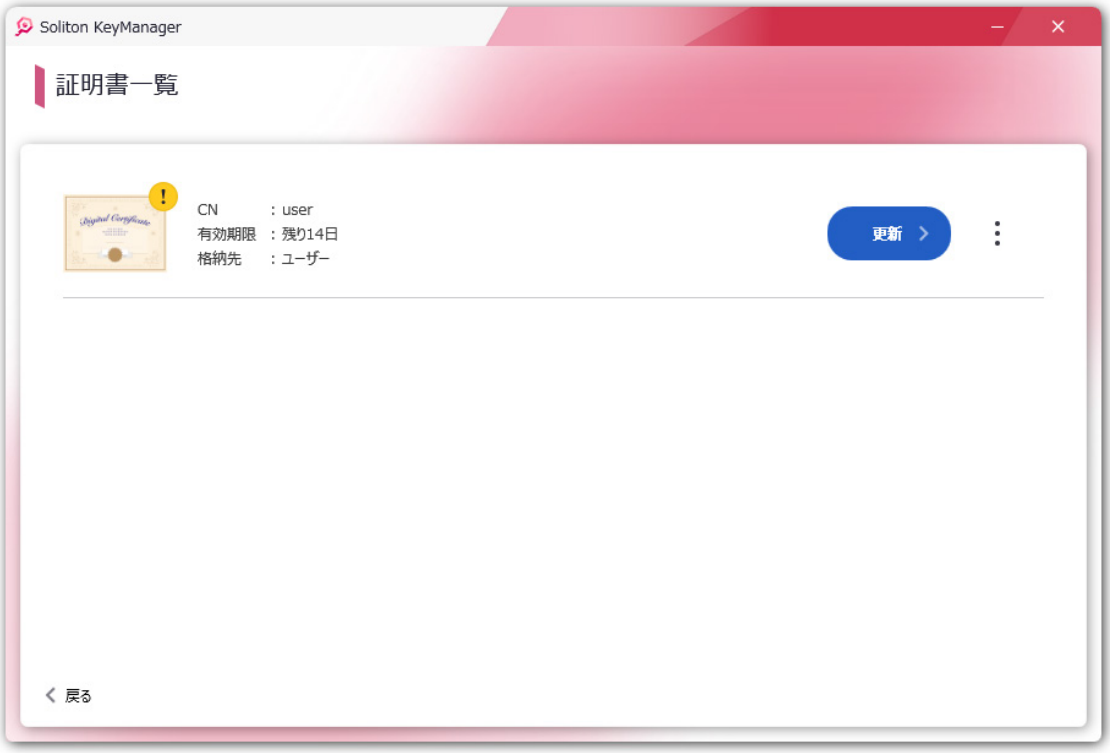

図 3.5.2　証明書一覧-更新

3. 有効期限が近づいていない証明書を更新するには、<⋮>をタップまたはクリックして表示されるメニューから<更新>を選択してください。

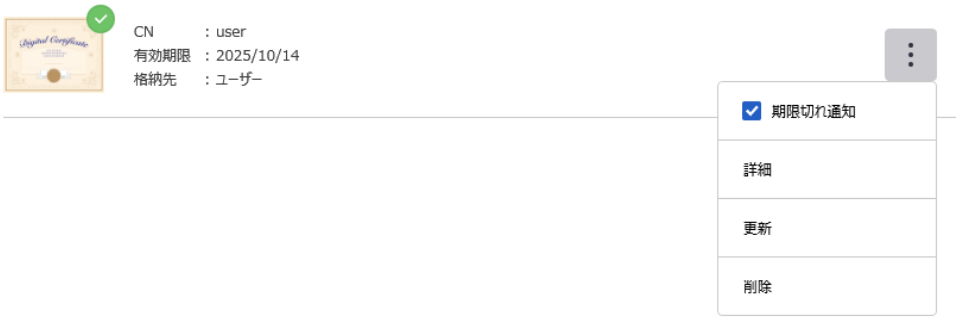

図 3.5.3　証明書一覧-更新(メニュー)

4. 図 3.5.4 の証明書の更新の確認ダイアログが表示されます。<OK>をタップまたはクリックしてください

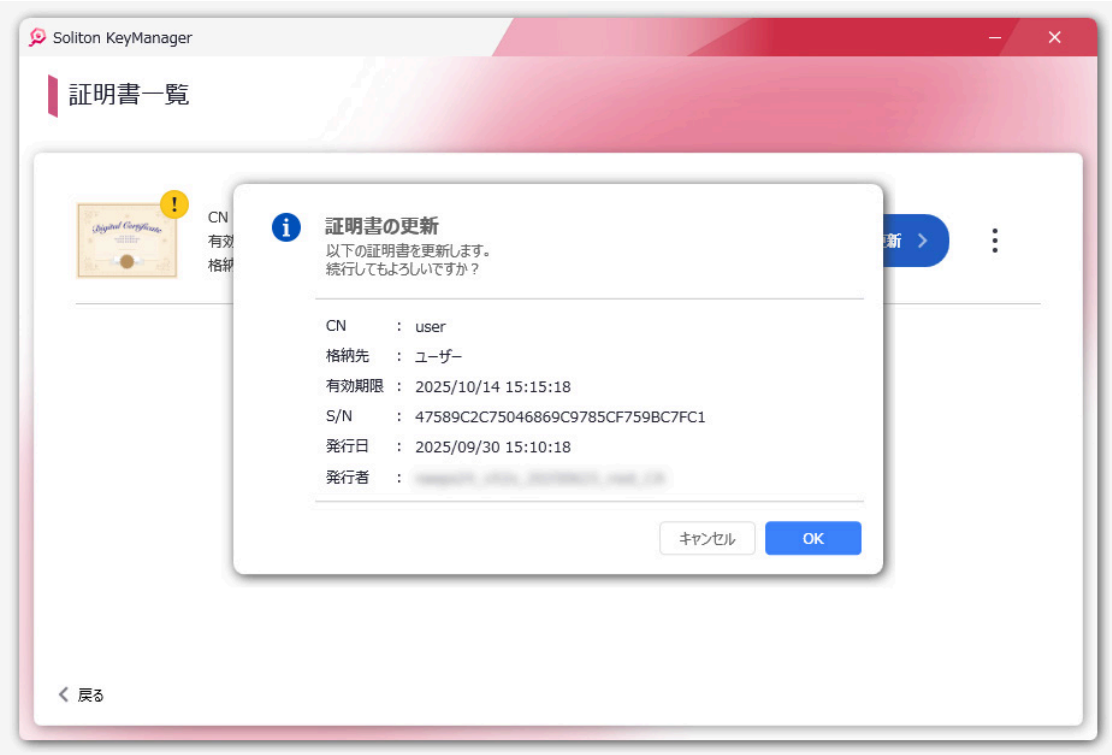

図 3.5.4　確認ダイアログ-証明書の更新

5. 図 3.5.5 が表示されます。パスワードを入力し<次へ>をタップまたはクリックしてください。

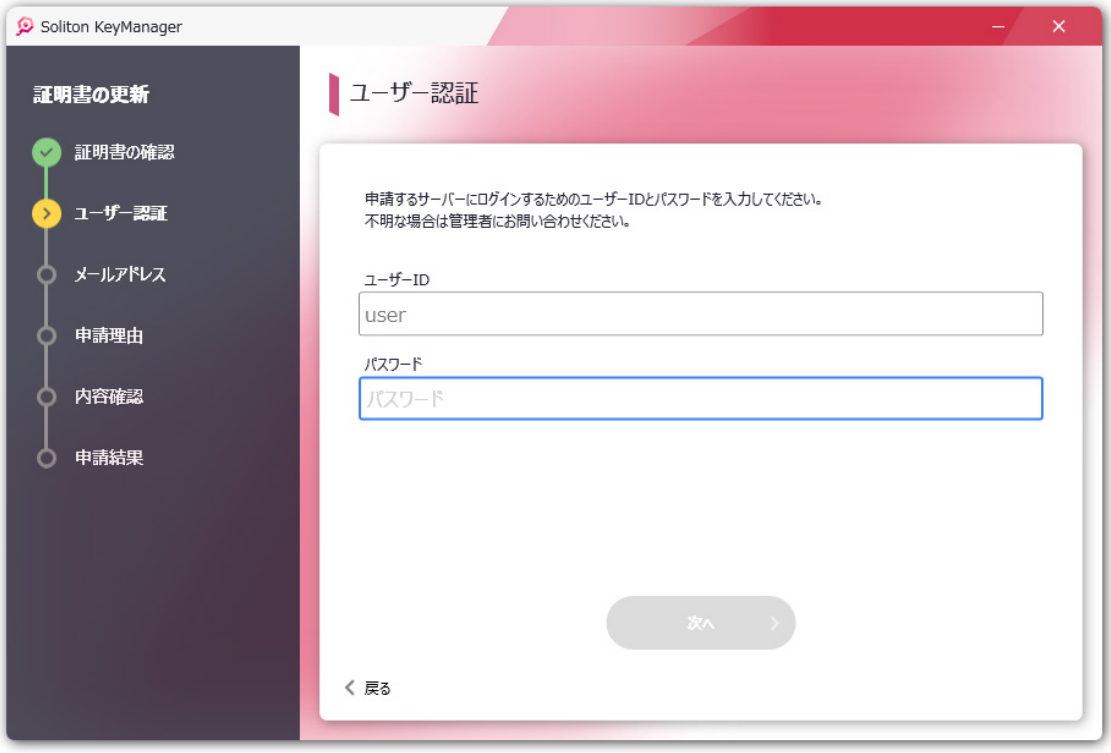

図 3.5.5　ユーザー認証-証明書の更新

6. これ以降の操作は「3.3　新しい証明書」と同じ手順で証明書の更新を完了してください。

❑ アプリ通知からの更新

表示されたアプリ通知から更新を行った場合の操作を説明します。

アプリ通知は証明書の有効期限が近づいた際に、また証明書の有効期限が切れた際に表示されます。ここでは証明書の有効期限が近づいた際に表示されるアプリ通知からの更新の手順について記載します。

通知設定については「4.3 通知設定」を参照してください。

1. 有効期限が近づくと以下のようなアプリ通知が表示されます。<OK>をタップまたはクリックしてください。

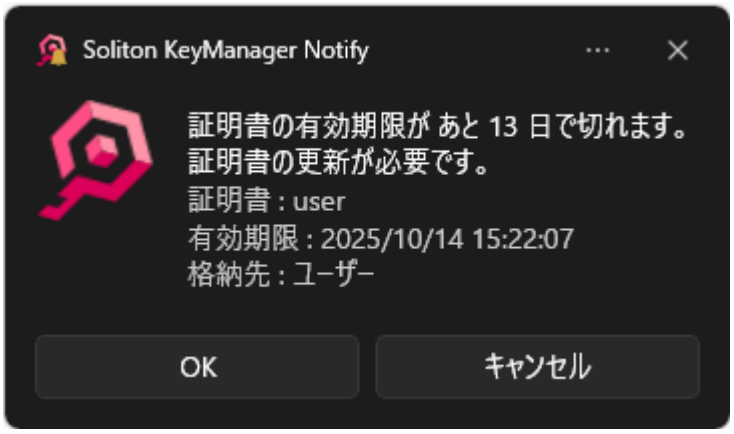

図 3.5.6　アプリ通知

2. 図 3.5.7 が表示されます。<次へ>をタップまたはクリックしてください。

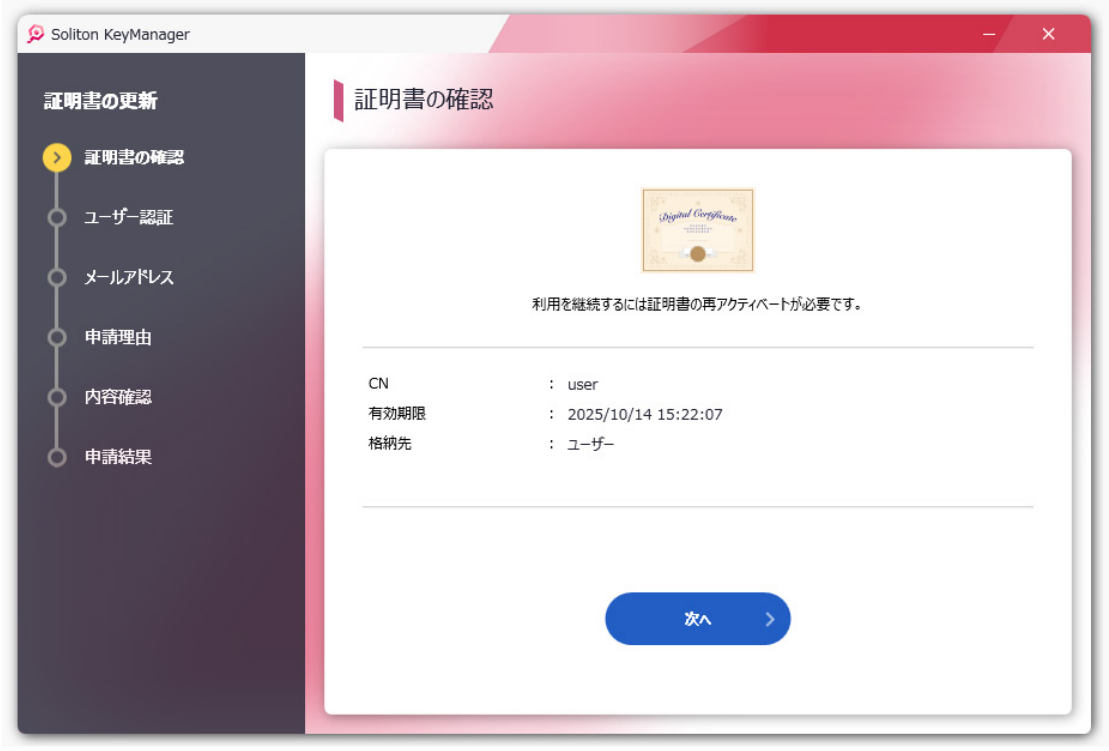

図 3.5.7　アプリ通知からの更新

3. 図 3.5.8 が表示されます。パスワード」を入力し<次へ>をタップまたはクリックしてください。

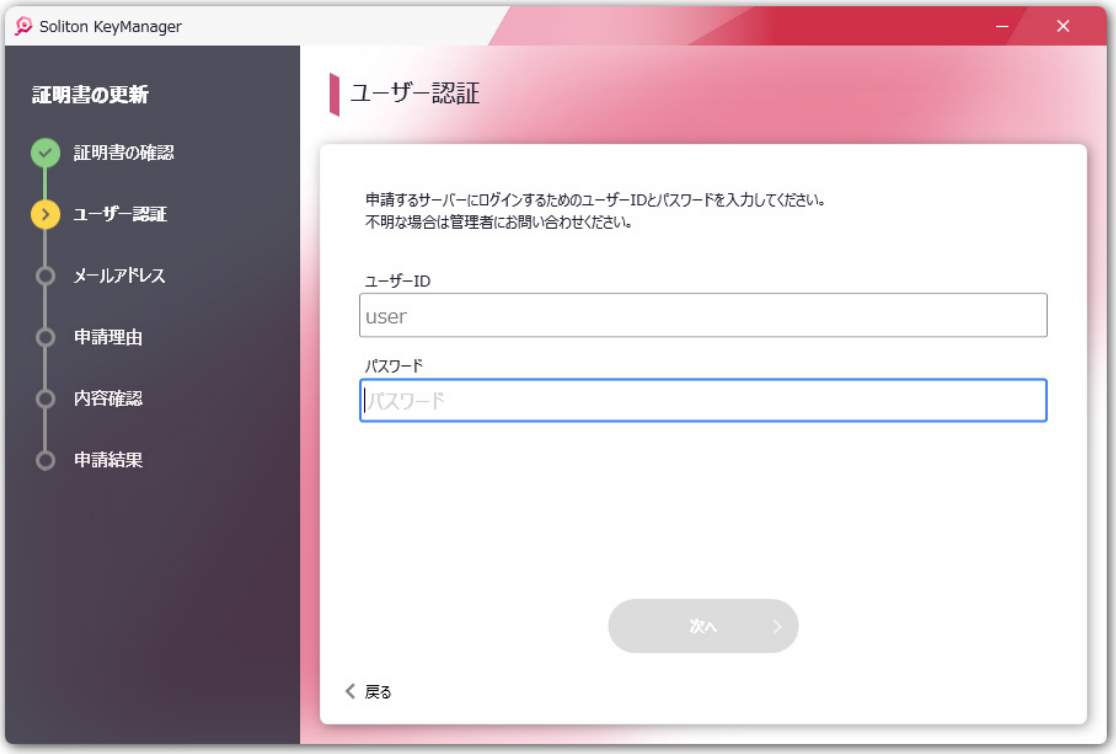

図 3.5.8　ユーザー認証-アプリ通知からの更新

4. これ以降の操作は「3.3　新しい証明書」と同じ手順で証明書の更新を完了してください。

3.6　URL からの申請（ワンタッチ証明書配布）

接続先からの招待メールに記載された KeyManager 用の URL を使用して証明書をインストール・更新することができます。ここではパスワードレスが有効な接続先からの招待メールに記載された KeyManager 用の URL から申請する手順について説明します。

3.6.1　PC

1. 招待メールに記載の KeyManager 用の URL をタップまたはクリックしてください。KeyManager が起動して申請が実行されます。

   ※接続先の設定により URL に証明書の格納先が指定されていない場合は「3.6.1　PC - 証明書の格納先を選択」を参照してください。またパスワードレスが有効でない場合は「3.6.1　PC - パスワードレスが無効」を参照してください。

図 3.6.1　申請 - URL からの申請

2. 申請～アクティベーション(証明書インストール)まで自動的に行われます。

図 3.6.2　アクティベート - URL からの申請

3. アクティベーションが完了します。<閉じる>をタップまたはクリックしてください。通常の KeyManager を起動するには<アプリを開く>をタップまたはクリックしてください。

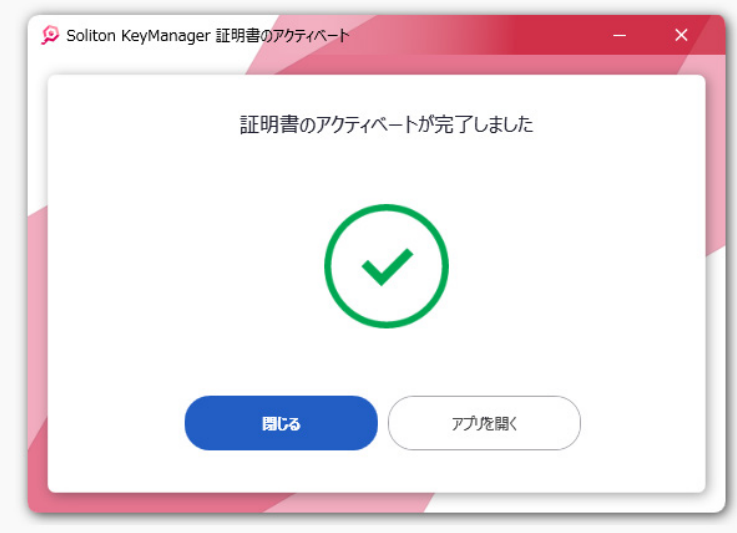

図 3.6.3　アクティベート完了 - URL からの申請

❑ 接続先が信頼されていない場合

接続先が信頼されていない場合、申請時に図 3.6.4 の警告メッセージが表示されます。接続を続けるには<OK>をタップまたはクリックしてください。

サーバーの配布する CA 証明書がインストールされていない場合、CA 証明書をダウンロードしてインストールを行います。

※接続先が信頼されている場合、図 3.6.4 は表示されません。

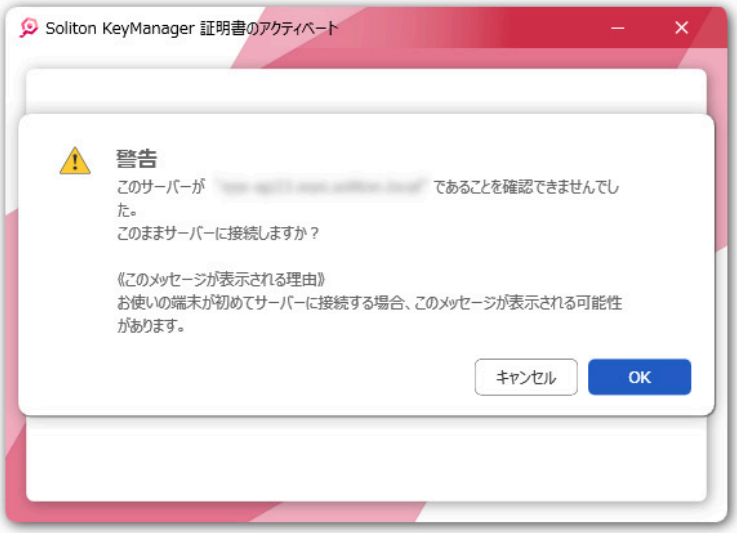

図 3.6.4　警告メッセージ-URL からの申請

- **このメッセージは、接続先の Web サーバー証明書が信頼できない場合に表示されます。**
- **CA 証明書のダウンロード、インストール手順は「付録 1-1　CA 証明書取得手順（Windows）」を参照してください。**

❑ パスワードレスが無効

接続先の設定でパスワードレスが無効の場合は、URL から起動すると図 3.6.5 が表示されます。パスワードを入力して<次へ>をタップまたはクリックしてください。

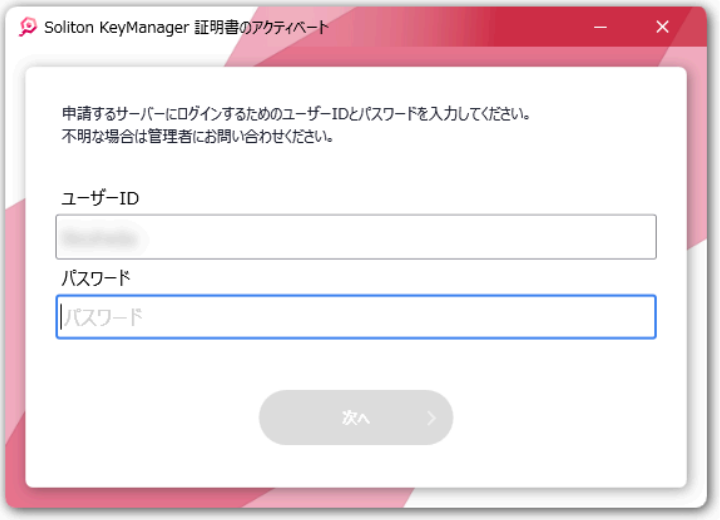

図 3.6.5　ユーザー認証-URL からの申請

❑ 証明書の格納先を選択

接続先の設定で招待に証明書の格納先が指定されていない場合は、URL から起動すると格納先の選択画面が表示されます。格納先を選択してください。

図 3.6.6　証明書の格納先-URL からの申請

4　証明書の操作

ここでは KeyManager を経由してインストールした証明書の確認、削除、通知設定について説明します。

4.1　証明書の確認

KeyManager を使用してインストールした証明書の確認方法について説明します。

4.1.1　PC

1.　ホーム画面の<証明書一覧>をタップまたはクリックしてください。

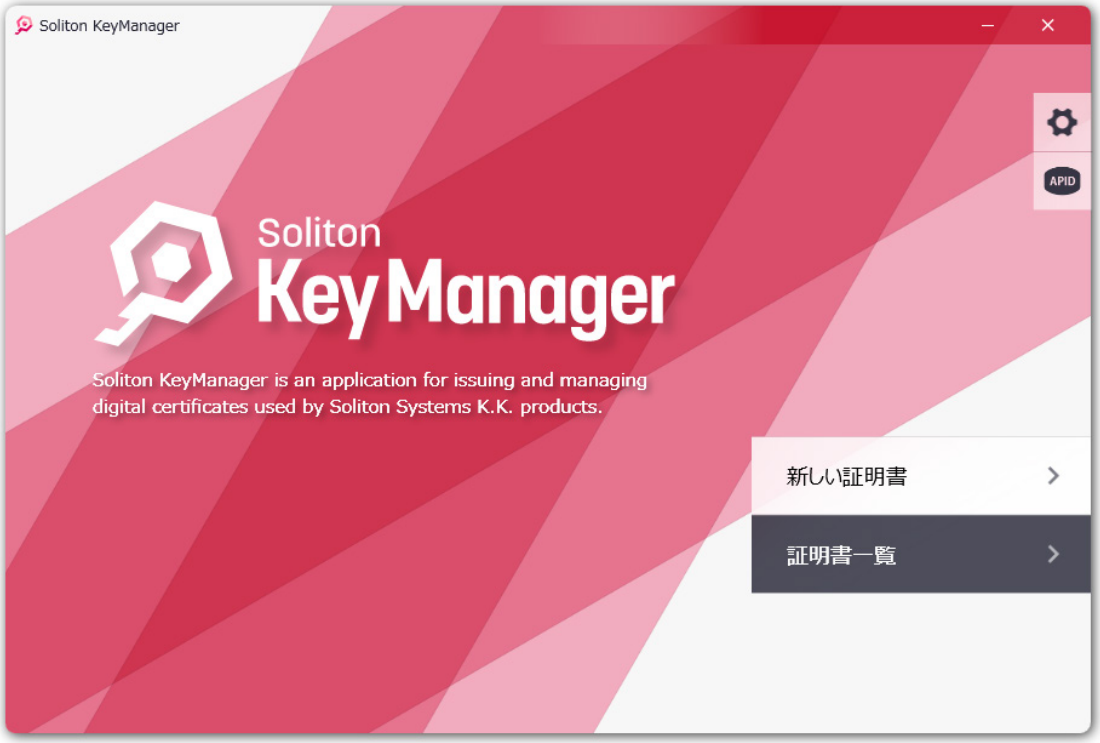

図 4.1.1　ホーム画面-証明書一覧

2. 証明書一覧画面が表示されます。削除したい証明書の<⋮>をタップまたはクリックしてください。

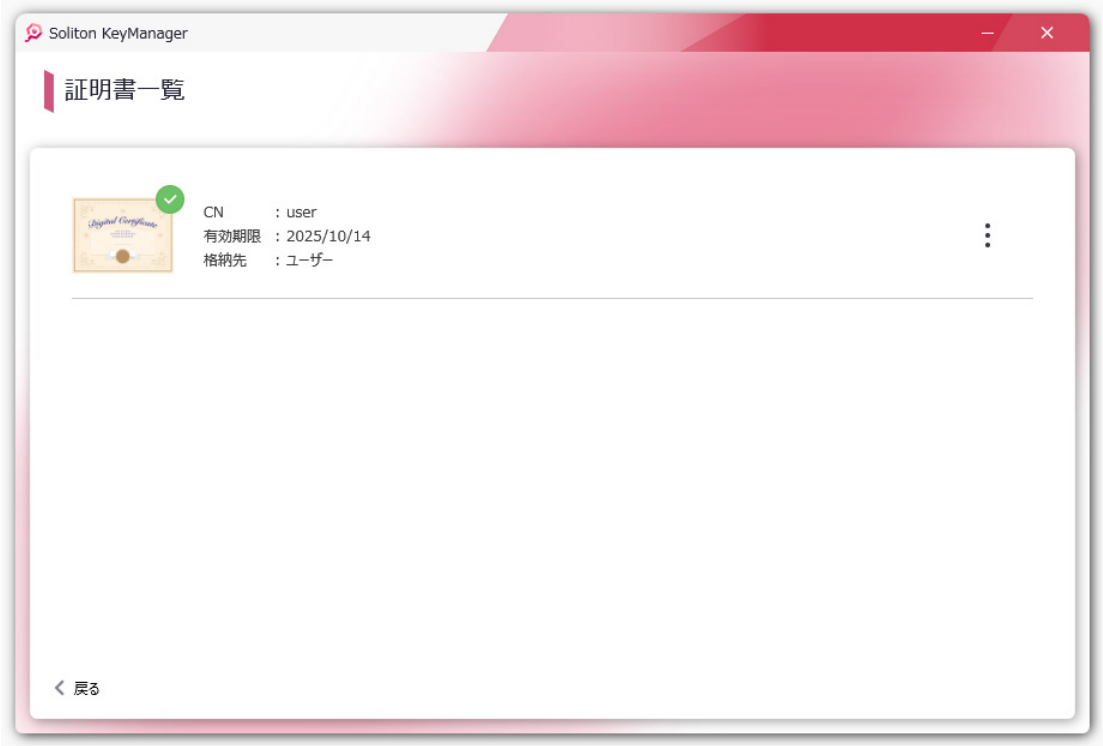

図 4.1.2　証明書一覧

3. 証明書メニューが表示されます。<詳細>をタップまたはクリックしてください。

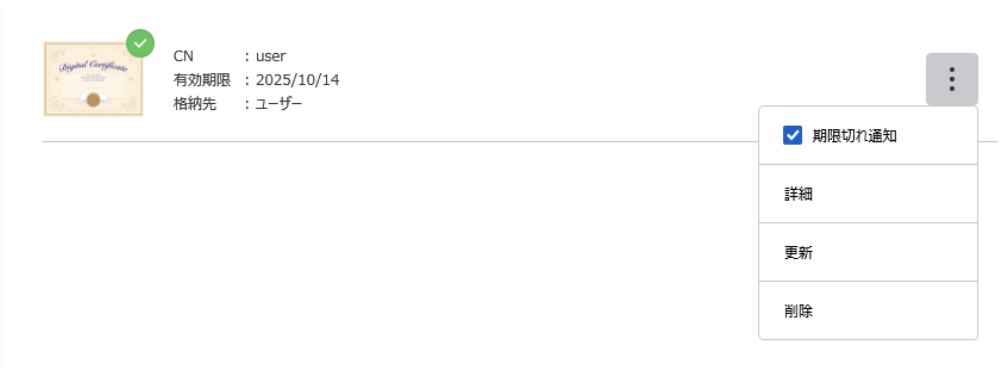

図 4.1.3　証明書メニュー

4. 証明書の詳細が表示されます。<証明書情報>をタップまたはクリックすることでより詳細な情報を確認できます。

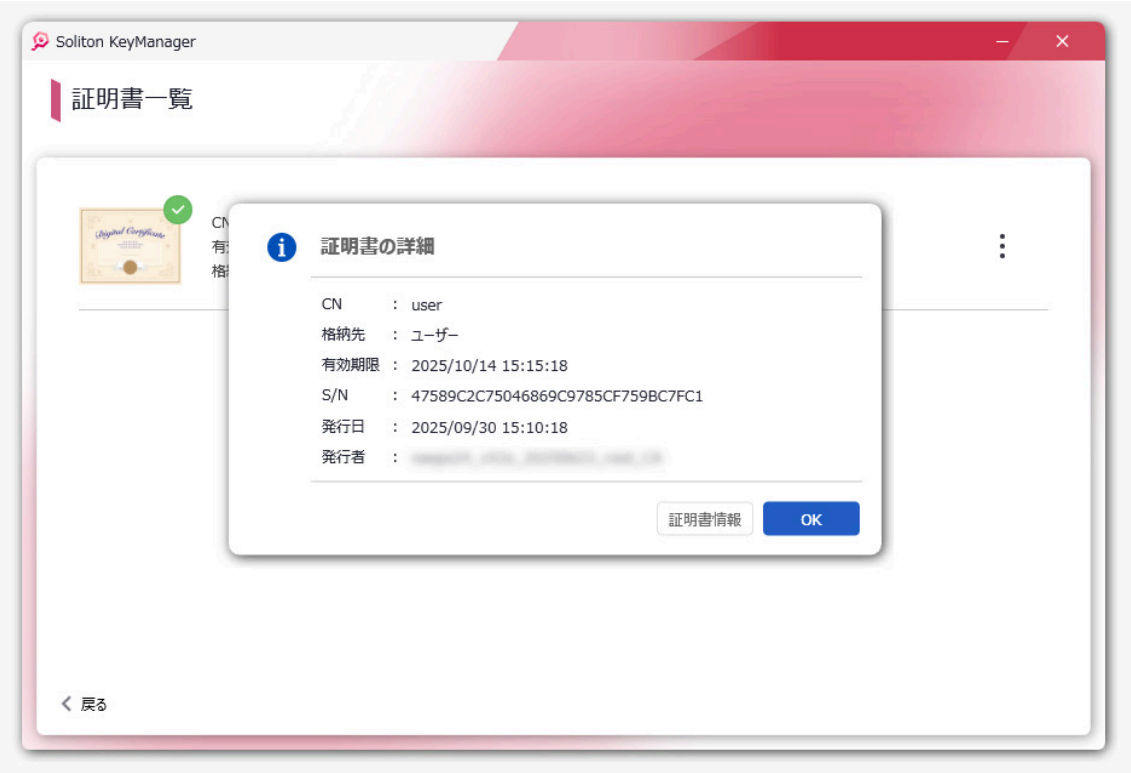

図 4.1.4　証明書の詳細

4.2　証明書の削除

KeyManager を使用してインストールした証明書の削除方法について説明します。

4.2.1　PC

1. ホーム画面の<証明書一覧>をタップまたはクリックしてください。

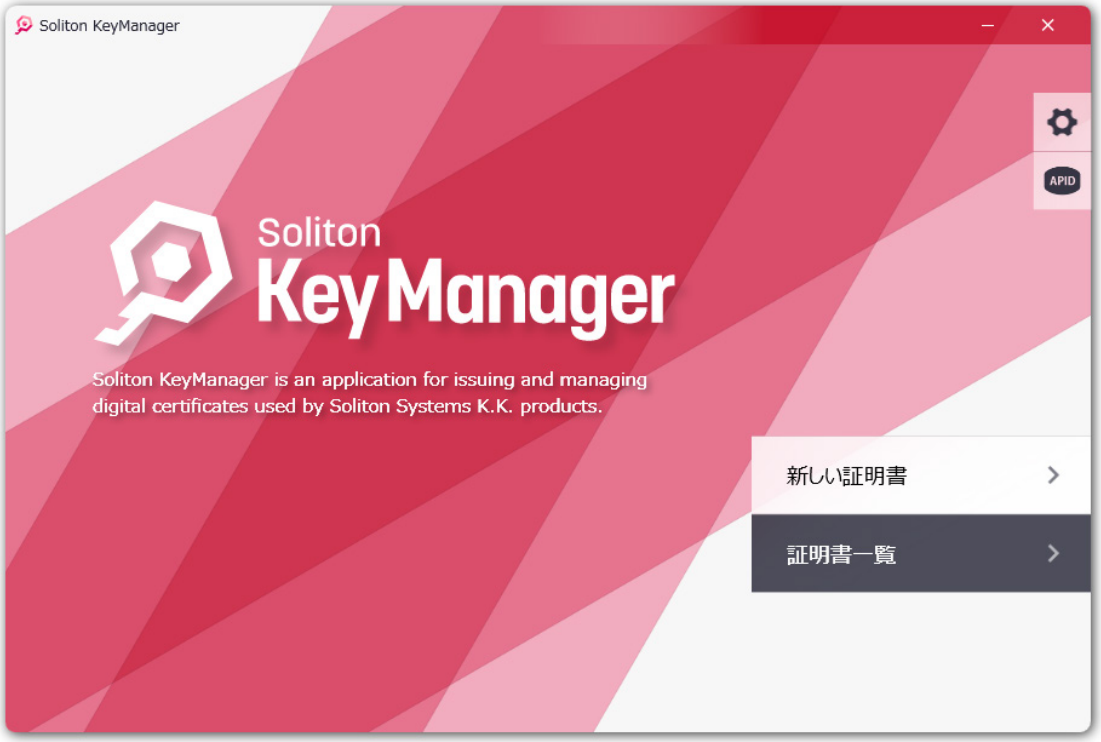

図 4.2.1　ホーム画面-証明書一覧

2. 証明書一覧画面が表示されます。削除したい証明書の<⋮>をタップまたはクリックしてください。

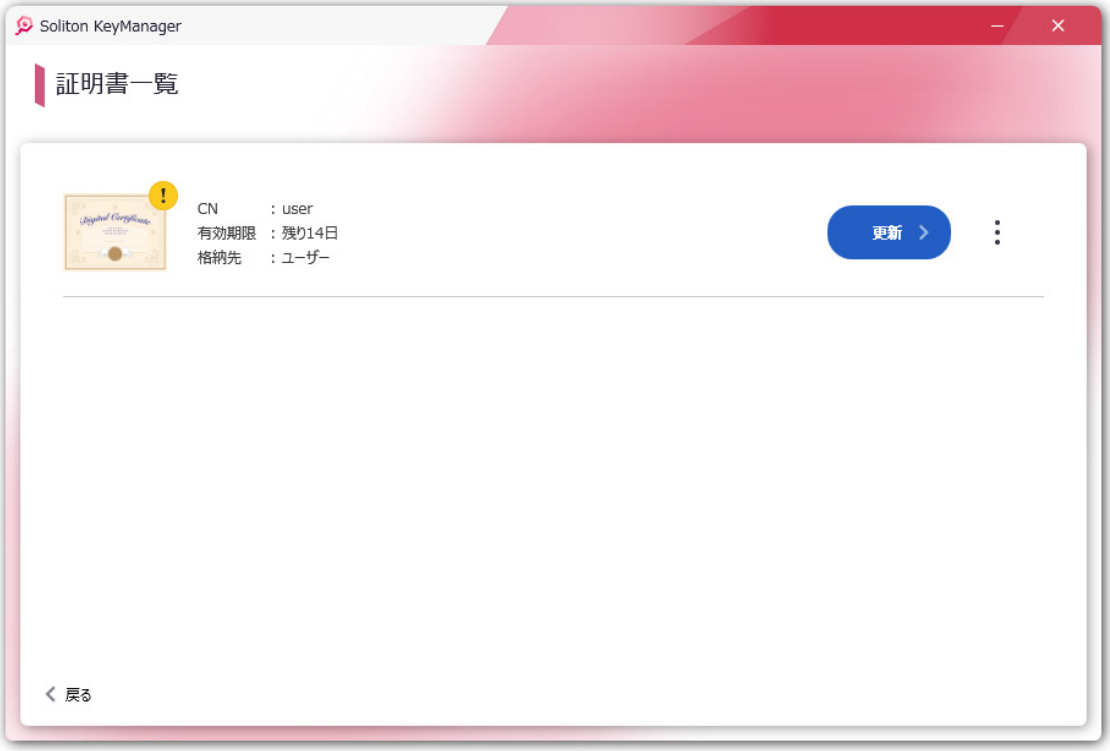

図 4.2.2　証明書一覧

3. 証明書メニューが表示されます。<削除>をタップまたはクリックしてください。

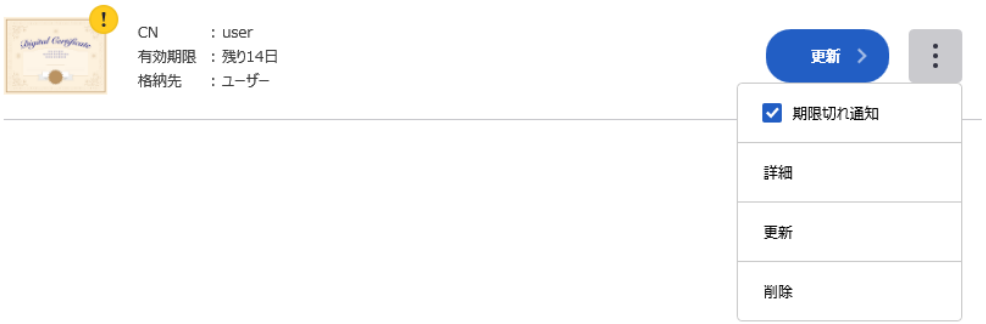

図 4.2.3　証明書メニュー

4. 削除の確認ダイアログが表示されます。<はい>をタップまたはクリックしてください。

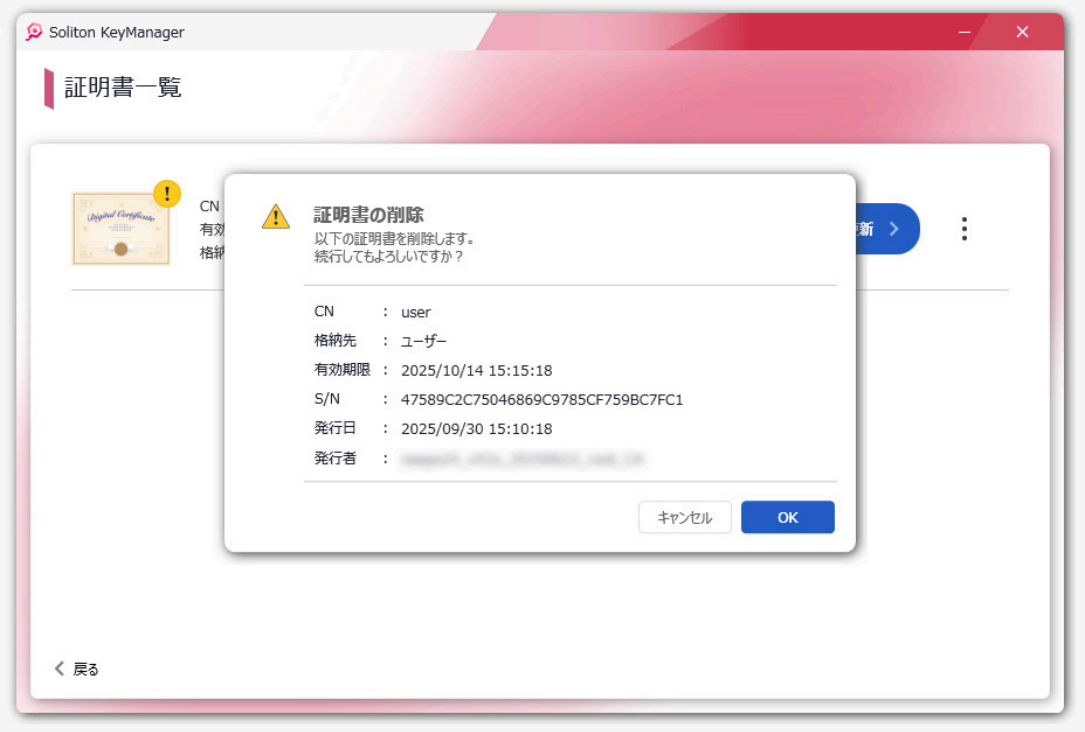

図 4.2.4　削除確認ダイアログ

- **Windows 版では、証明書の格納先がコンピューターの証明書を削除する場合にユーザーアカウント制御のダイアログが表示されます。**
- **KeyManagerから証明書を削除すると実際の証明書ストアからも削除されますのでご注意ください。**

4.3　通知設定

KeyManager を使用してインストールした証明書の有効期限が近づいた際や、有効期限が切れた際に表示される、通知メッセージ機能の設定方法について説明します。

4.3.1　設定を変更する

証明書の有効期限切れ通知に関する設定を変更します。

既にインストール済みの証明書および以降にインストールした証明書は、ここで指定した設定が反映されます。

4.3.1.1　PC

1. ホーム画面上部にある歯車アイコンをタップまたはクリックしてください。

図 4.3.1　設定-ホーム画面

2. 図 4.3.2 の設定画面が表示されます。必要に応じて「通知設定」の「証明書の有効期限が切れた際に通知する」、および「証明書の有効期限が近づいた際に通知する」の設定を変更してください。

   ※ユーザーアカウント制御の画面が表示された場合は、<はい>をタップまたはクリックしてください。

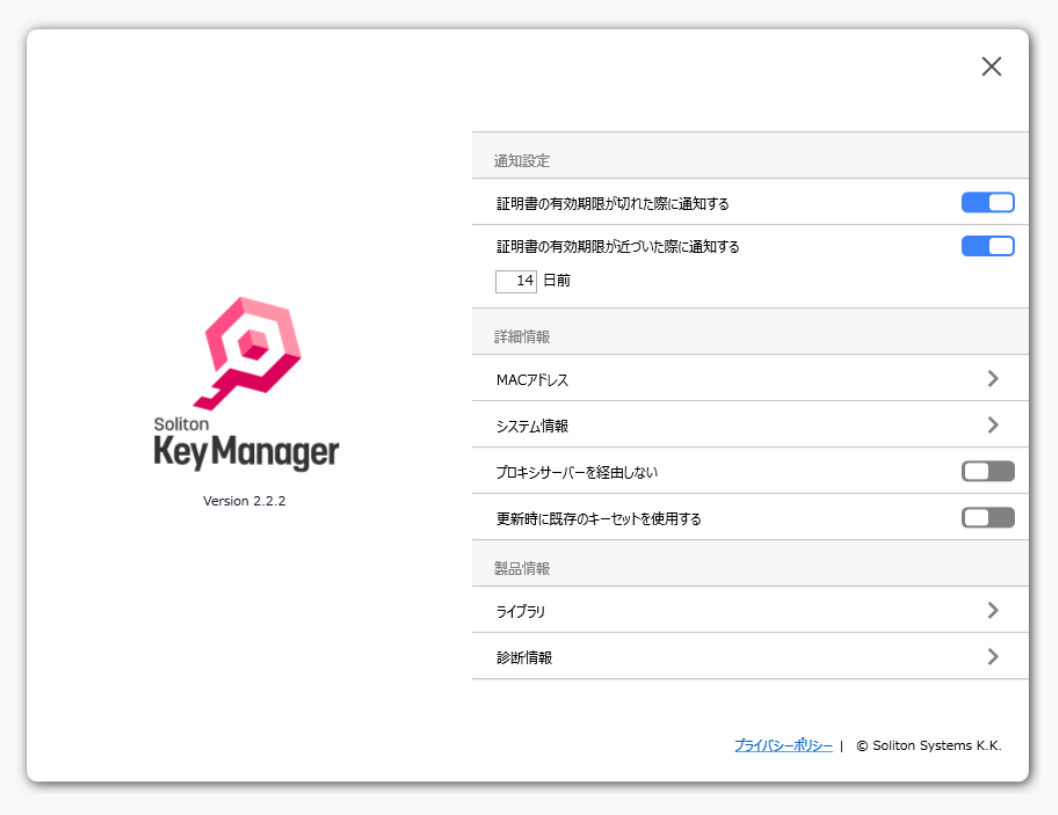

図 4.3.2　通知設定-設定

表 4.3.1　通知設定

項目		説明
証明書の有効期限が切れた際に通知する		証明書の有効期限が過ぎたことを通知する設定です。
	設定	証明書の有効期限が過ぎたことを通知する場合は、ON にしてください。 デフォルト：ON（通知する）
証明書の有効期限が近づいた際に通知する		証明書の有効期限が近づいたことを通知する設定です。
	設定	証明書の有効期限が近づいた際に通知する場合は、ON にしてください。 デフォルト：ON（通知する）
	～日前	証明書の有効期限の何日前に通知するか指定してください。 デフォルト：14 日前 設定可能範囲：1～120 日前

- **証明書の格納先がコンピューターの証明書がインストールされている場合は、通知設定の変更が反映されるタイミングでユーザーアカウント制御のダイアログが表示されます。**

4.3.2　証明書別に通知設定を変更する

インストール済みの証明書は、個別に有効期限切れ通知を行うかどうか指定することができます。

証明書単位で有効期限切れ通知の設定を変更する手順は、以下のとおりです。

4.3.2.1　PC

1.　ホーム画面の<証明書一覧>をタップまたはクリックしてください。

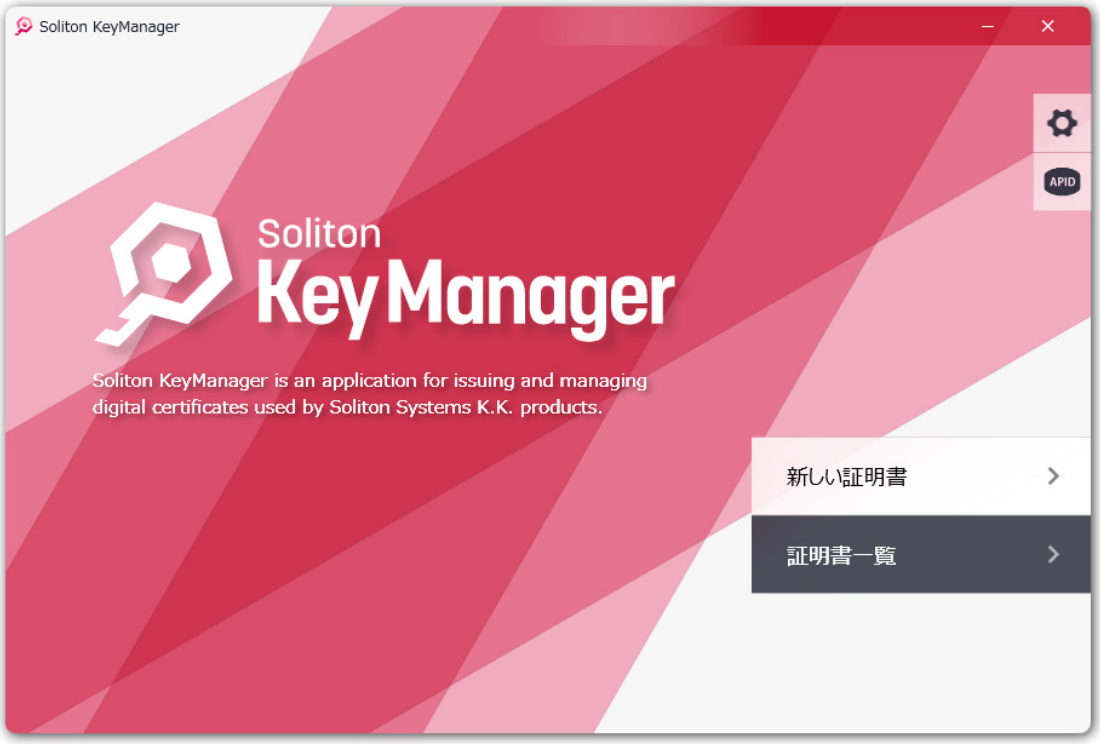

図 4.3.3　証明書一覧-ホーム画面

2. 図 4.3.4 の証明書一覧が表示されます。通知設定を変更したい証明書の<⋮>をタップまたはクリックしてください。

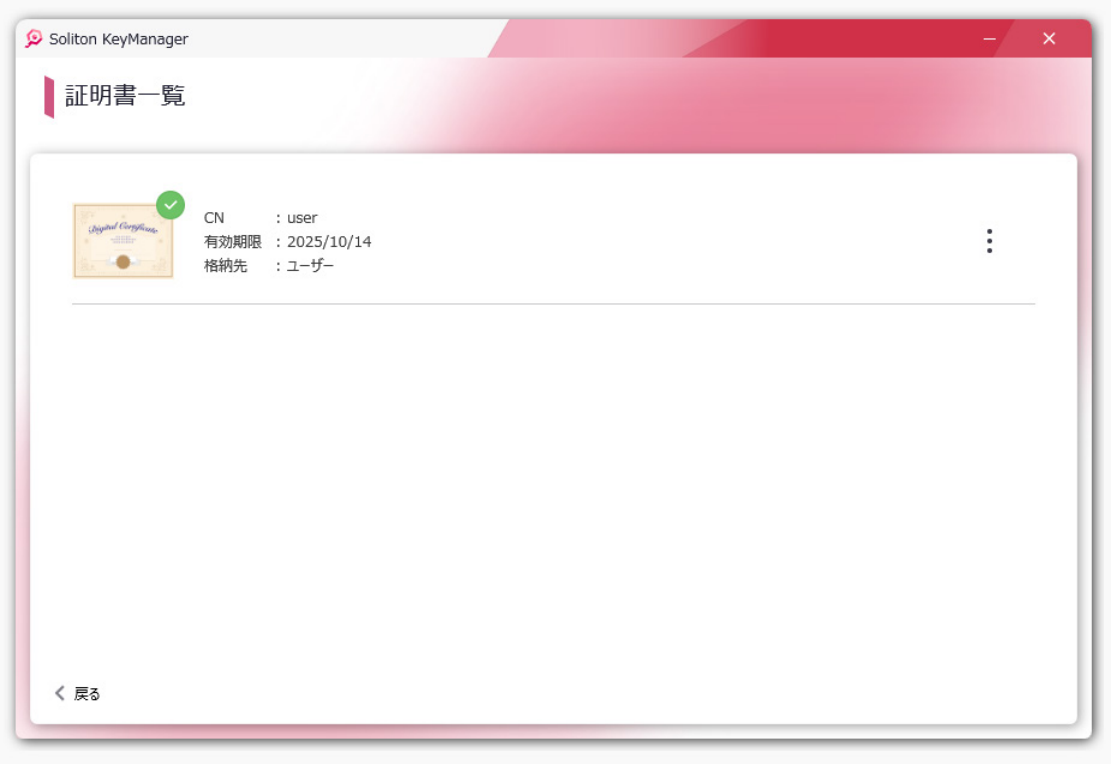

図 4.3.4　設定メニュー

3. 図 4.3.5 が表示されます。必要に応じて「期限切れ通知」のチェックボックスを変更してください。証明書単位に通知を表示するかどうかを指定できます。

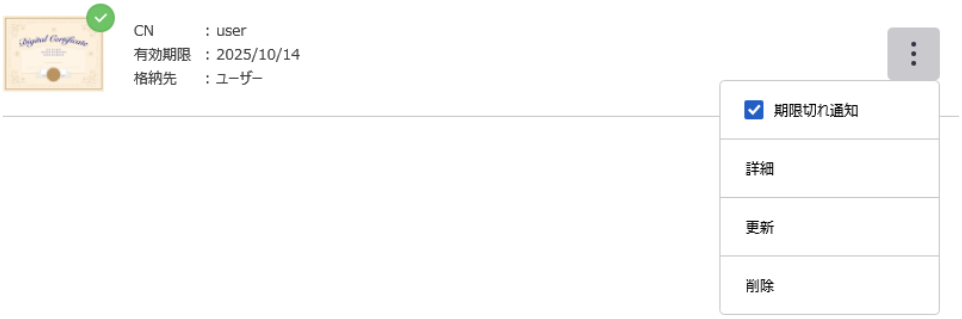

図 4.3.5　証明書一覧

表 4.3.2　個別の通知設定

項目		説明
期限切れ通知		この証明書の有効期限切れ通知を表示するかどうかを指定する設定です。
	チェックボックス	証明書の有効期限切れ通知を表示する場合は、ON にしてください。 OFF にすると「証明書の有効期限が切れた際の通知」および「証明書の有効期限が近づいた際の通知」どちらの通知メッセージも非表示になります。 この設定を ON にしても、設定にて通知設定が有効になっていない場合は表示されません。 デフォルト：ON（通知する）

- **Windows 版の場合、「証明書の有効期限が近づいた際の通知」のメッセージは、有効期限が切れるまで 1 日 1 回、証明書の有効期限が切れる時刻と同じ時間に通知します。**
- **Windows 版において、通知時間にコンピューターを起動していない、またはログインしていない場合、ユーザーがログインした際に証明書の有効期限を確認し、通知条件に該当するとメッセージを通知します。**
- **Windows 版の場合、ログイン時の有効期限切れのメッセージは、ログインする度に通知されます。有効期限切れの通知メッセージを停止するには、該当する証明書の更新、削除、または証明書一覧の「期限切れ通知」の設定を解除してください。**

5　トラブルシューティング

KeyManager のトラブル時に役立つ操作について説明します。

また、弊社 Web サイトの FAQ では本製品に関する最新の情報を提供しています。

お困りの際はこちらをご参照ください。

Soliton FAQ

https://faq1.soliton.co.jp/

- **KeyManager から正常に通信できない環境では、申請やアクティベーションに失敗する場合があります。**

  通信できない場合は、ルータや VPN などの中継地点、DMZ のネットワーク機器、ファイアウォール、クライアントのセキュリティソフトの通信/制限許可設定など確認してください。

  ネットワーク機器やセキュリティソフトにより KeyManager の通信がブロックされた場合、申請やアクティベーションに失敗します。例外設定等、通信を阻害しないような構成をご検討ください。

5.1　よくある質問

☞ FAQ No:5896「Soliton KeyManagerが使用する通信ポートを教えてください。」

https://faq1.soliton.co.jp/faq/show/5896

5.2　診断情報

KeyManager を使用中に障害が発生した場合、発生した障害の解析を行うため、動作環境や動作状況といった情報収集を目的として、弊社より診断情報のご提供をお願いする場合があります。診断情報を提供していただくことで、環境や状況の共有をスムーズに行います。

通常は、診断情報を取得する必要はありません。診断情報の取得は、管理者より指示があった場合のみ行ってください。

5.2.1　診断情報を取得する

診断情報を取得する手順は、以下のとおりです。

1. ホーム画面上部にある歯車アイコンをタップまたはクリックしてください。
2. 製品情報にある<診断情報の送信>または<診断情報>をタップまたはクリックしてください。

付録

付録 1　Windows

Windows 版 KeyManager 固有の動作について説明します。

ここでは Windows11 の PC を例に説明します。

1-1　CA 証明書取得手順（Windows）

1. サーバーの配布する CA 証明書がインストールされていない場合、KeyManager が自動的に CA 証明書をダウンロードし、セキュリティ警告の画面が表示されます。<はい>をクリックし CA 証明書をインストールしてください。

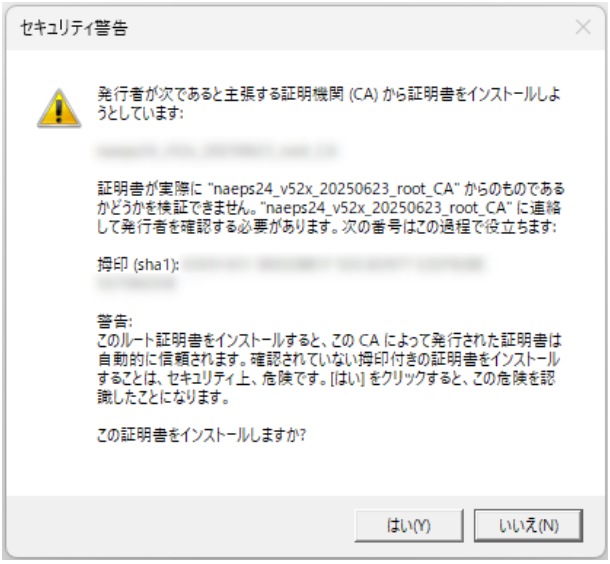

図 A1.1　セキュリティ警告

2. CA 証明書をインストールすると次の画面に進みます。

1-2　MAC アドレスの確認

アクティベーション中、デバイスチェックに使用する MAC アドレスの確認方法について記載します。

1. ホーム画面上部にある歯車アイコンをタップまたはクリックしてください。
2. 図 A1.2 が表示されます。「詳細設定」の<MAC アドレス>をタップまたはクリックしてください。

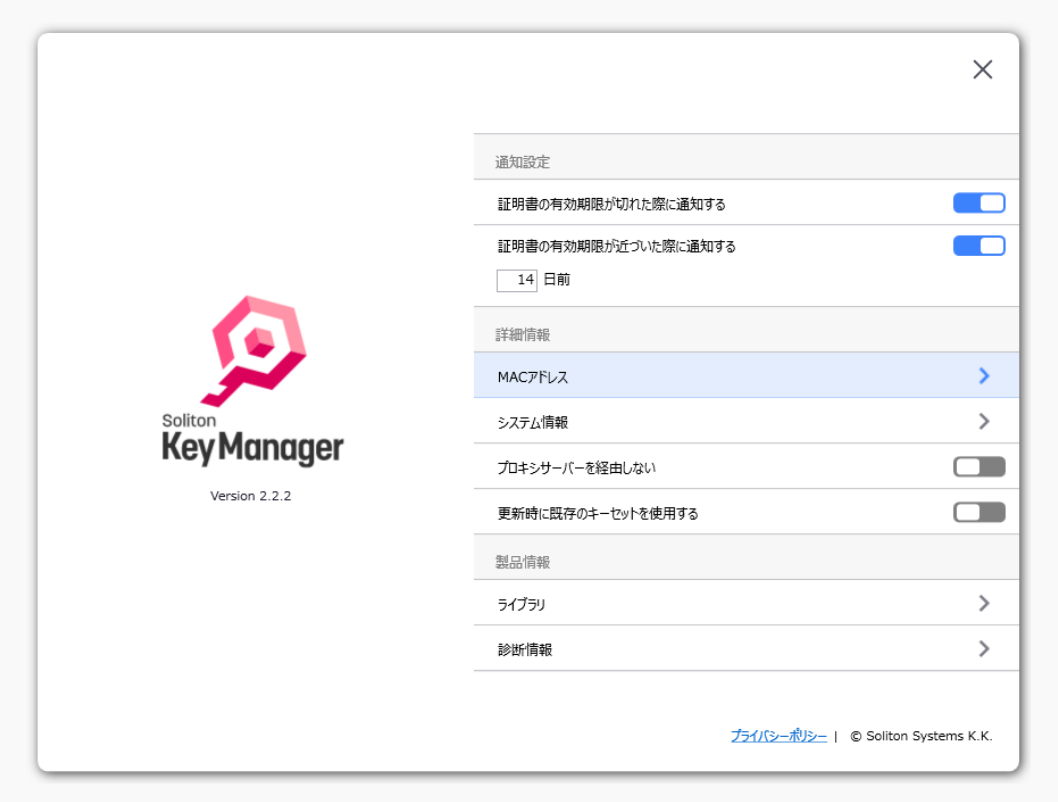

図 A1.2　設定

3. 図 A1.3 が表示され、MAC アドレスを確認することができます。

図 A1.3　MAC アドレス

1-3　プロキシサーバーを経由しない

Windows 版 KeyManager からの通信をプロキシサーバー経由にしない場合の設定方法を記載します。

1. ホーム画面上部にある歯車アイコンをタップまたはクリックしてください。
2. 図 A1.4 が表示されます。「詳細設定」の「プロキシサーバーを経由しない」にチェックを入れてください。

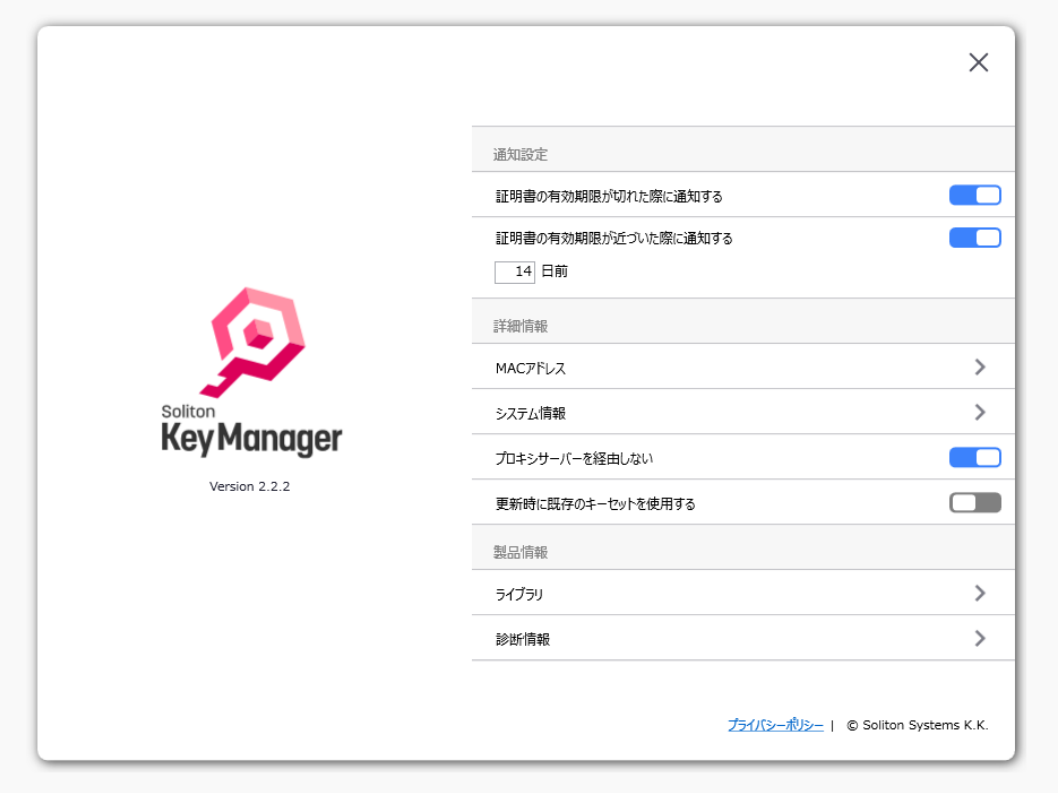

図 A1.4　設定

1-4　申請理由の初期値

NetAttest EPS-ap(申請モード(手動承認))に対して Windows 版 KeyManager から申請を行うと、申請理由に下記文字列が自動的に付与され、ユーザーが「申請理由」に設定した値は下記文字列以降に続けて送信されます。

```
[コンピューター名]/[ドメイン名]/[ユーザーID]/[Mac アドレス]/[格納先]:
```

- **申請理由が送信されるのは EPS-ap 申請モードの手動承認の場合のみ。**
- **[格納先]には、格納先として「ユーザー」を選択した場合は「user」が、「コンピューター」を選択した場合は「comp」が入ります。**
- **[ドメイン名]には、コンピューターが参加しているドメイン名が付加されます。ログインしているユーザーのドメイン情報ではありません。コンピューターがドメインに参加していない場合、[ドメイン名]には「WORKGROUP」が入ります。**

1-5　コンピューター名を送信する

アクティベーションを行うとコンピューター名をサーバーに送信します。

1-6　ドメイン情報を送信する

Windows 版 KeyManager は、利用ユーザーが参加しているドメイン名をアクティベーション中にサーバーへ送信しています。

サーバーが証明書の配布先をドメイン名で制限している場合、適切なドメインに参加していないユーザーやローカルユーザーでは証明書の取得が行えません。

Windows 版 KeyManager V2.2.3 以降で Active Directory 環境に加えて、Entra Join 環境でもドメイン名を送信できるようになりました。

1-7　シリアル番号/ベンダー名を送信する

Windows 版 KeyManager V2.2.2 以降では、アクティベーションを行うと端末のシリアル番号とベンダー名をサーバーに送信しています。

送信しているシリアル番号とベンダー名、およびコンピューター名は以下の方法で確認できます。

1. ホーム画面上部にある歯車アイコンをタップまたはクリックしてください。
2. 図 A1.5 が表示されます。「詳細設定」の<システム情報>をタップまたはクリックしてください。

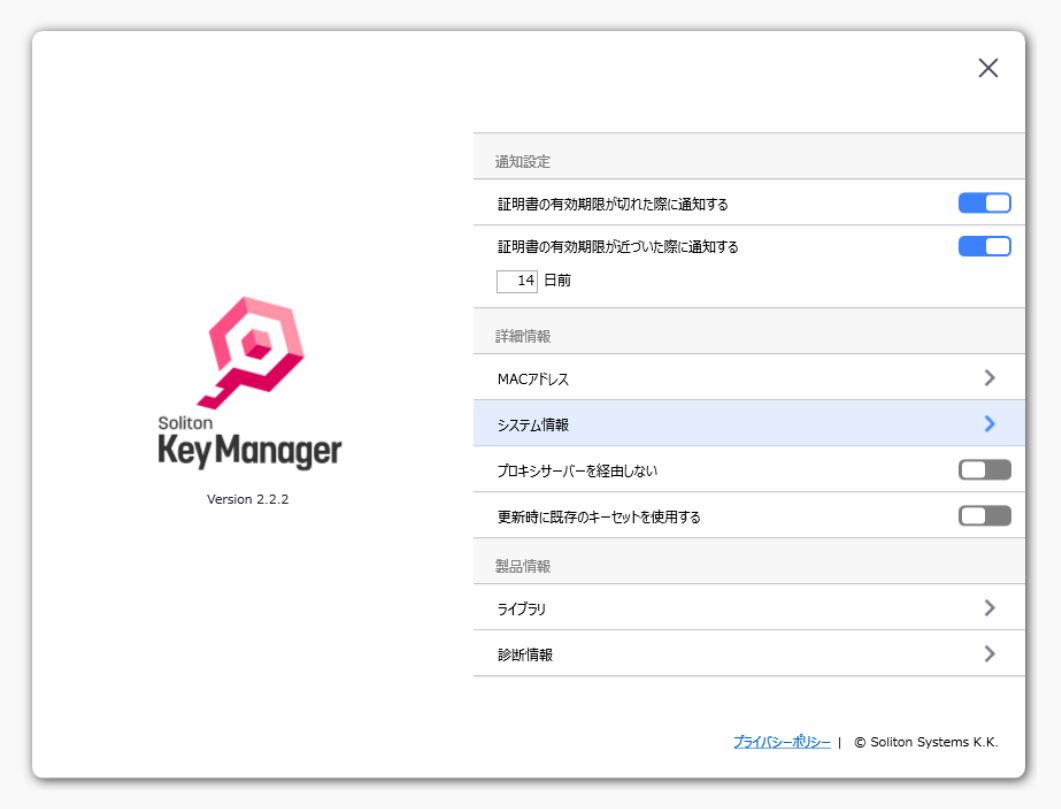

図 A1.5　設定

3. 図 A1.6 が表示され、システム情報を確認することができます。

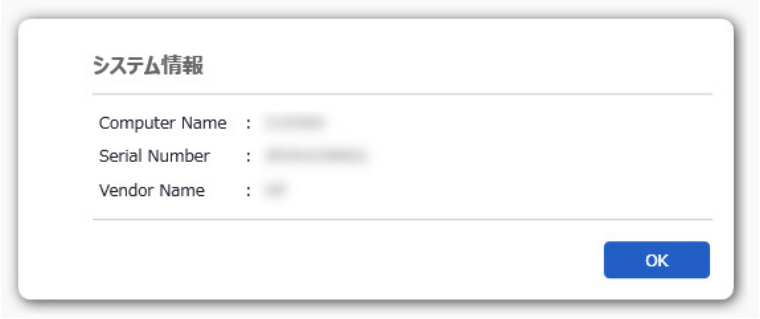

図 A1.6　システム情報

1-8　コマンドラインによる証明書インストール

KeyManager をコマンドラインで実行して、証明書をインストールする機能です。

管理者が Active Directory や資産管理ソフトなどを利用してコマンドを実行することで、利用者が意識することなくゼロタッチ(※)で安全に利用者の PC に証明書をインストールできます。

※使用するコマンドや環境によっては利用者の操作が必要な場合があります。ご利用の環境で事前に十分な確認を行ってください。

❑　対象バージョン

Windows 版 KeyManager　V2.0.11 以降(一部機能は V2.2.0 以降対応)

❑　対応環境

NetAttest EPS-ap 申請モード(自動承認)

Soliton OneGate(デバイス予約方式)

- **本機能は NetAttest EPS-ap が「申請モード」でかつ「自動承認」が「有効」の場合に利用できます。「自動承認」が「無効」の場合や「招待モード」の場合は利用できません。**
- **本機能は Soliton OneGate が「デバイス予約方式」の場合に利用できます。**

❑　コマンド形式

以下の形式でコマンドオプションを指定して実行してください。

```
keymanager.exe /cl [option] [option]
```

❑ コマンドオプション一覧

コマンドラインで指定するコマンドオプションの一覧です。

表 A1.1　コマンドオプション

オプション	説明
/cl	必須項目です。 コマンドラインで実行します。コマンドラインで実行する場合は必ずこのオプションを指定してください。
/h <host name or IP address>	必須項目です。 接続するサーバーのホスト名または IP アドレスを指定してください。
/hp <port>	接続するサーバーのポート番号を指定してください。 指定しない場合はデフォルトのポート番号が使用されます。 デフォルト：443
/u <user id>	申請ユーザーを指定してください。 指定しない場合および/wl オプションを指定していない場合は入力ダイアログが表示されます。入力ダイアログは Windows にログオンしていない場合は表示されません。
/p <password>	申請ユーザーのパスワードを指定してください。 指定しない場合および/ep オプションを指定していない場合は入力ダイアログが表示されます。入力ダイアログは Windows にログオンしていない場合は表示されません。
/ep <password>	申請ユーザーの暗号化されたパスワードを指定してください。 パスワードを暗号化するには「パスワードを暗号化する」を参照してください。 /ep オプションと/p オプションは同時に指定できません。
/sc /su	格納先を指定します。 /sc：コンピューター /su：ユーザー 指定しない場合は格納先として「ユーザー」が使用されます。

オプション	説明
/new	強制的に「新規」で申請します。 指定しない場合は、接続先と申請ユーザーおよび格納先が同じ証明書が既にインストールされている環境では「更新」（上書き）されます。インストールされていない環境は「新規」で申請します。 ※V2.2.0 以降では、/new を指定しない場合に有効期限が通知日数の範囲であれば「更新」します。通知日数の範囲外の場合は更新が不要として更新はスキップされます。
/wl	申請ユーザーとして Windows にログオンしているユーザーID を取得して使用する。 連携している認証サーバーが Active Directory と連携しているなど、Windows のログオンユーザーを申請ユーザーとして利用できる環境で使用できます。
/cn	証明書の CN の値を以下で上書きします。 ・コンピューター証明書の CN にコンピューター名を使用する。 ・ユーザー証明書の CN に Windows ログオンユーザーID を使用する。
/np	プロキシサーバーを経由せずに通信を行います。 指定していない場合は UI の設定「プロキシサーバーを経由しない」が無効として動作します。 ※V2.2.1 以前では UI の設定に従って動作します。
/usk	証明書更新時に既存のキーセットを使用します。 指定しない場合は証明書更新時に新しいキーセットが生成します。キーサイズの変更をともなう証明書更新の場合には指定しないでください。 このオプションは証明書更新時のみ有効です。 /new オプション指定時は無視されます。 ※このオプションは V2.2.2 以降で利用可能。
/debug	デバッグモードを有効にします。

❑ パスワードを暗号化する

/pe オプションを使用することで、入力した平文のパスワードを暗号化してコマンドラインに出力します。

コマンド内のパスワードを暗号化することで、バッチファイルを配布するケースで共通のアカウントを使用する場合などに、平文のパスワードが見えてしまうことを回避することができます。

暗号化されたパスワードは/ep オプションで使用します。

/ep オプションで指定した暗号化されたパスワードは、KeyManager で復号化してサーバーに送信されます。

パスワードを暗号化するには/pe オプションを指定して単体で実行してください。/cl オプションで実行

されるコマンドと併用できません。

```
keymanager.exe /pe 〈password〉
```

表 A1.2　コマンドオプション(パスワードを暗号化)

オプション	説明
/pe <password>	入力したパスワード(平文)を暗号化します。 空白や記号「<>」が含まれる場合は「"(ダブルクォート)」で囲んでください。パスワード文字列として「"(ダブルクォート)」は使用できません。

❑ コマンド実行結果を確認する

コマンドラインの実行結果の確認方法について説明します。

ユーザーは以下の方法でコマンドラインにより証明書のインストールが行えているか確認できます。

➢ アプリ通知

ログオン中のユーザーにアプリ通知(トースト通知)で結果が通知されます。

表 A1.3　アプリ通知

結果	メッセージ
成功	証明書をインストールしました。(ユーザー) 証明書をインストールしました。(コンピューター)
失敗	証明書のインストールに失敗しました。(ユーザー) 証明書のインストールに失敗しました。(コンピューター)

スタートアップスクリプトなど Windows にユーザーがログオンしていない場合は表示されません。

SYSTEM 権限で実行している場合はログオンユーザーに対して表示を試みます。

利用する資産管理ソフトの仕様や、実行方法によってはアプリ通知が表示されない場合があります。

アプリ通知は OS の設定で通知を無効にすることができます。また集中モードが有効な場合に直接アクションセンターに格納される場合があります。

アプリ通知が表示されない場合でも、証明書のインストールは実行されます。

➢ KeyManager を起動して確認する

KeyManager の証明書一覧にインストールした証明書が表示されます。コマンドラインでインストールした証明書を KeyManager の UI から更新・削除を行うことができます。

➢ 結果ファイルを確認する

直前のコマンドラインの実行結果が、結果ファイル（Command_result.txt）に保存されます。

格納先がコンピューターの場合は Program Data フォルダーに保存されます。ユーザーの場合はユーザープロファイルに保存されます。結果ファイルは診断情報に含まれます。

(例)

格納先「コンピューター」: C:¥ProgramData¥Soliton Systems¥Soliton KeyManager

格納先「ユーザー」: C:¥Users¥<ログオンユーザー>¥AppData¥Local¥Soliton KeyManager

《結果ファイル 例》

```
Date:2024/02/01 11:15:000
Result: succeeded
UserID: user01
Store: computer
CN: user01
S/N: 12345
Expires: 2025/02/01 11:20:000
```

表 A1.4　結果ファイル

項目	説明
Date	コマンド実行日時
Result	コマンドの実行結果 succeeded：成功 failed：失敗 canceled：中止(ユーザー操作) no executed：実行をスキップ
UserID	申請ユーザー
Store	格納先
CN	インストールした証明書の CN ※成功時にのみ
S/N	インストールした証明書のシリアル番号 ※成功時にのみ
Expires	インストールした証明書の有効期限 ※成功時にのみ

➢ ERRORLEVEL で確認する

直前のコマンドラインの実行結果を ERRORLEVEL により確認できます。

ERRORLEVEL を取得することで実行したコマンドの終了コードを確認できるため、それによりバッチファイルにて処理を分岐することもできます。

例)

```
@keymanager.exe /cl /su /h <ホスト名または IP アドレス> /hp 443 /u admin01 /p password
@echo %ERRORLEVEL%
```

表 A1.5　終了コード

終了コード	結果
0	成功
100	KeyManager で失敗（実行権限が不足、コマンドが不正など）
110	更新をスキップ(更新不要)
120	ユーザー操作による終了(パスワード入力をキャンセルなど)
200	サーバーとの通信に失敗（ホスト名やポート番号が不正など）
300	サーバーからエラーが返されて失敗（認証失敗など）
1000	その他、想定していないエラー

- **ERRORLEVEL は KeyManager V2.2.0 以降で利用できます。**

  KeyManager V2.0.11 では ERRORLEVEL に対応していないため、実行に失敗しても必ず「0(成功)」となります。

  コマンドプロンプトから KeyManager を直接コマンドで実行した場合に、KeyManager のプロセスの終了を待たずに制御が戻るため正しく ERRORLEVEL が取得できません。

  コマンドプロンプトから KeyManager をコマンドで実行して ERRORLEVEL を取得したい場合は、「start /wait」コマンドによりプロセスの終了を待つように指定して実行してください。

例)

```
 >start /wait keymanager.exe /cl /su /h <ホスト名または IP アドレス> /hp 443 /u admin01 /p
password
 >echo %errorlevel%
0
```

制約事項

- **接続する NetAttest EPS-ap が「申請モード」でかつ「自動承認」が「有効」の場合に本機能を利用できます。**
- **接続する Soliton OneGate が「デバイス予約方式」の場合に本機能を利用できます。**
- **言語は日本語/英語のみ**
- **コマンドラインは実行したユーザーの権限で実行されます。**

UI の場合では管理者権限が必要な場合は昇格ダイアログが表示されますが、コマンドラインの場合は実行途中での昇格は行われません。格納先をコンピューターに指定した場合は、実行したユーザーに権限が不足していると失敗で終了します。格納先をコンピューターに指定する場合は管理者権限のあるユーザーまたは SYSTEM ユーザーで実行してください。

- **スタートアップスクリプトを使用したコマンドライン実行について**

スタートアップスクリプトはコンピューターの起動時に SYSTEM ユーザーで実行されます。そのため以下の制限事項があります。

・ /wl オプションは使用できません。

・ 指定できる格納先は「コンピューター」のみ(/SC オプション)

・ 入力ダイアログは表示されません。/u オプション、/p(/ep)オプションを使用して申請ユーザー情報を指定してください。

・ アプリ通知は表示されません。

- **ユーザーストアの信頼されたルート証明機関に CA 証明書をインストールする場合はセキュリティ警告が表示されます。**
- **Active Directory や資産管理ソフトなどで一斉にコマンドを実行する場合、端末台数が多いとサーバー側の申請の処理に遅延が発生して、KeyManager で処理が失敗する場合があります。しばらく待ってから再度実行してください。**
また、Active Directory や資産管理ソフト側でコマンドを実行するタイミングを分散させるなどの運用を検討してください。安定して同時に実行できる端末台数は、20～30 台程度が目安となります。

スクリプトでコマンドラインの実行を行う場合は、「timeout」コマンドと環境変数「%random%」を使用して実行タイミングを分散させることができます。

例）0 から 3600 秒の範囲でコマンド実行を待機させる例

```
set /A timeout=%random%*3600/32767
timeout /T %timeout% > NUL

"C:¥Program Files (x86)¥Soliton KeyManager¥KeyManager.exe" /cl /su /h <ホスト名または IP アドレス> /hp 443 /u <ユーザーID> /p <パスワード> /cn
```

※　環境変数「%random%」は 0 から 32767 の間の整数値を返します。

※　コマンド実行の待機する秒数の範囲については、実行する環境に応じて調整してください。

❑　　配布シナリオ例

ここではコマンドラインで証明書を配布するシナリオの例を紹介します。

NetAttest EPS/NetAttest EPS-ap や Soliton OneGate を利用して、**「共通のアカウント」**を使用して同時に申請を行う運用を想定している場合は、必ず以下の**注意事項**を参照してください。

- **「共通のアカウント」は利用者に登録してください。管理者はこのアカウントをコマンドに埋め込みユーザーに実行させることでユーザーのパスワード入力なしに申請を行うことができます。**
- **Soliton OneGate を利用している場合、利用者から「共通のアカウント」を削除すると、このアカウントを使用したコマンドで発行されたすべての証明書が失効されます。**

- **NetAttest EPS/EPS-ap で「共通のアカウント」を使用して複数の端末から同時にコマンドを実行する場合の注意事項**

NetAttest EPS/EPS-ap を使用して、「共通のアカウント」で同時に申請して証明書インストールを行う場合の注意事項について説明します。

SCEP の MDM チャレンジはユーザーID ごとに生成され保持されます。SCEP リクエストに含まれる MDM チャレンジがこれと一致すれば証明書が自動的に発行されます。

しかし同一ユーザーID で複数端末から同時に申請を行われると、後から実施した申請の MDM チャレンジが上書きされて、先に行われた申請の SCEP リクエストが自動発行されずに証明書の取得に失敗します。

「共有のアカウント」をコマンドに埋め込んで配布したスクリプトなどで同時に実行された場合に、この問題が発生する可能性があります。

※Soliton OneGate ではこの問題は発生しません。

ゼロタッチを実現するためにコマンドに「共通のアカウント」を使用した運用を行う場合には、次の POINT に注意して配布環境を構築してください。

●POINT●

(1) 共通のアカウントを 1 つ用意する

ここでは例として「admin01」とします。

(2) コマンドの「/u」で指定するユーザーID を「共通のアカウント」+「ログオンユーザーID またはコンピューター名」で指定する

例)コンピューター名が SALES-PC の場合

```
/u admin01%COMPUTERNAME%

→　NetAttest EPS-ap に送信される申請ユーザーID は　「admin01SALES-PC」となる
```

例)ログインユーザーID が user01 の場合

```
/u admin01%USERNAME%

→ NetAttest EPS-ap に送信される申請ユーザーID は 「admin01user01」となる
```

(3) NetAttest EPS で「共通のアカウント」+「ログオンユーザーID またはコンピューター名」のユーザーID でも「共通のアカウント」として認証が成功するように構成する

NetAttest EPS のサービス管理ページの[RADIUS > 詳細設定]の「アドバンス設定」で、RADIUS Hints file(hints_added.in)を以下のように編集してください。

例)「admin01%COMPUTERNAME%」や「admin01%USERNAME%」を「admin01」として認証させたい場合

・hints_added.in

```
# RADIUS Hints file
DEFAULT User-Name =~ "admin01.*"
  Just-User-Name := admin01
#
```

(4) 「/CN」オプションを指定する

「/CN」オプションを使用することで証明書の CN をユーザー名またはコンピューター名に指定することができます。

「/CN」オプションを使用しない場合、「CN＝ユーザーID」で証明書が発行されます（NetAttest EPS-ap のデフォルト）。このユーザーID は申請で「/u」で指定したユーザーID となります。例えば「/u admin01%COMPUTERNAME%」で申請すると「CN= admin01winpc01」となります。

「/CN」オプションを使用することで実際に利用するユーザーに紐づいた CN で証明書を取得することができます。

例）利用者「user01」のクライアント PC「SALES-PC」にユーザー証明書をインストールする。証明書の CN には利用者のユーザーID になるように/cn オプションを指定。申請には共通のアカウント「admin01」にコンピューター名を付加して使用する。

```
"C:¥Program Files (x86)¥Soliton KeyManager¥KeyManager.exe" /cl /su /h <ホスト名または IP アドレス> /hp 443 /u admin01%COMPUTERNAME% /p password /cn
```

このコマンドでは以下のような内容で申請される。

・申請時のユーザーID：admin01SALES-PC

・認証に使用されるユーザーID：admin01

・発行された証明書の CN：user01

➢ シナリオ例 1：ログオンスクリプトでユーザー証明書をインストールする(Soliton OneGate)

Active Directory のログオンスクリプトを利用して、利用者の PC にユーザー証明書を Solton OneGate から取得するケース。ログオンスクリプトは、ログオンしたユーザーの権限で実行されます。

[環境例]

Soliton OneGate

ログインユーザー：user01

共通のアカウント：admin01

(1) バッチファイルの準備

ログオンスクリプトでコマンドを実行するバッチファイルを準備します。

例）利用者のクライアント PC にユーザー証明書をインストールする。証明書の CN には利用者のユーザーID になるように/cn オプションを指定。申請には共通のアカウントを使用する。また実行タイミングを 0～3600 秒の範囲で遅らせる。

```
set /A timeout=%random%*3600/32767
timeout /T %timeout% > NUL

"C:¥Program Files (x86)¥Soliton KeyManager¥KeyManager.exe" /cl /su /h <OneGate のホスト名> /hp 443 /u admin01 /p password /cn
```

(2) Active Directory の操作

グループポリシーのログオンスクリプトにバッチファイルを登録する。

(3) クライアント PC の操作

Windows に「user01」でログオンする。

Windows にログオン後にログオンスクリプトが実行される。

(4) 結果

利用者が操作することなく、クライアント PC のユーザーストアに「CN=user01」のユーザー証明書がインストールされる。

➢ シナリオ例 2：ログオンスクリプトでユーザー証明書をインストールする（NetAttest EPS/EPS-ap）

Active Directory のログオンスクリプトを利用して、利用者の PC にユーザー証明書を NetAttest EPS/EPS-ap から取得するケース。ログオンスクリプトは、ログオンしたユーザーの権限で実行されます。

[環境例]

NetAttest EPS/NetAttest EPS-ap

ログインユーザー：user01

共通のアカウント：admin01

(1) NetAttest EPS のアドバンス設定を行う

共通のアカウントで複数同時に申請できるように NetAttest EPS のアドバンス設定を追加します。

例）「admin01%USERNAME%」を「admin01」として認証させる

・hints_added.in

```
# RADIUS Hints file
DEFAULT User-Name =~ "admin01.*"
  Just-User-Name := admin01
#
```

(2) バッチファイルの準備

ログオンスクリプトでコマンドを実行するバッチファイルを準備します。

例）利用者のクライアント PC にユーザー証明書をインストールする。

証明書の CN には利用者のユーザーID になるように/cn オプションを指定。申請には共通のアカウントを使用する。また実行タイミングを 0～3600 秒の範囲で遅らせる。

```
set /A timeout=%random%*3600/32767
timeout /T %timeout% > NUL

"C:¥Program Files (x86)¥Soliton KeyManager¥KeyManager.exe" /cl /su /h <EPS-ap のホスト名または IP アドレス> /hp 443 /u admin01%USERNAME% /p password /cn
```

(3) Active Directory の操作

グループポリシーのログオンスクリプトにバッチファイルを登録する。

(4) クライアント PC の操作

Windows に「user01」でログオンする。

Windows にログオン後にログオンスクリプトが実行される。

(5) 結果

利用者が操作することなく、クライアント PC のユーザーストアに「CN=user01」のユーザー証明書がインストールされる。

➢ シナリオ例 3：スタートアップスクリプトでコンピューター証明書をインストールする（NetAttest EPS/EPS-ap）

Active Directory のスタートアップスクリプトを利用して、利用者の PC にコンピューター証明書を NetAttest EPS/EPS-ap から取得するケース。スタートアップスクリプトは、SYSTEM 権限で実行されます。

[環境例]

NetAttest EPS/NetAttest EPS-ap

クライアント PC：SALES-PC

共通のアカウント：admin01

(1) NetAttest EPS のアドバンス設定を行う

共通のアカウントで複数同時に申請できるように NetAttest EPS のアドバンス設定を追加します。

例）「admin01%COMPUTERNAME%」を「admin01」として認証させる

・hints_added.in

```
# RADIUS Hints file
DEFAULT User-Name =~ "admin01.*"
  Just-User-Name := admin01
#
```

(2) バッチファイルの準備

ログオンスクリプトでコマンドを実行するバッチファイルを準備します。

例）利用者のクライアント PC にコンピューター証明書をインストールする。

証明書の CN には利用者のクライアント PC のコンピューター名になるように/cn オプションを指定。申請には共通のアカウントを使用する。また実行タイミングを 0～3600 秒の範囲で遅らせる。

```
set /A timeout=%random%*3600/32767
timeout /T %timeout% > NUL

"C:¥Program Files (x86)¥Soliton KeyManager¥KeyManager.exe" /cl /sc /h <EPS-ap のホスト名または IP アドレス> /hp 443 /u admin01%COMPUTERNAME% /p password /cn
```

(3) Active Directory の操作

グループポリシーのスタートアップスクリプトにバッチファイルを登録する。

(4) クライアント PC の操作

Active Directory と通信が行える環境でクライアント PC を起動する。

Windows 起動後にスタートアップスクリプトが実行される。

(5) 結果

利用者が操作することなく、クライアント PC のコンピューターストアに「CN= SALES-PC」のコンピューター証明書がインストールされる。

1-9　サイレントインストールを利用する

「2.2.1　Windows 版 - サイレントインストール」を参照してください。

1-10　OS のディスクイメージをマスター展開した環境で利用する（キッティングインストール）

「2.2.1　Windows 版 - キッティングインストール」を参照してください。

1-11　証明書更新時に既存のキーセットを使用する

証明書更新時に更新元の証明書のキーセットを使用して更新したい場合の設定方法を記載します。

KeyManager V2.2.2 以降では証明書更新時に新規のキーセットを生成します。更新元の証明書のキーセットを使用したい場合はこの設定を有効にしてください。

1. ホーム画面上部にある歯車アイコンをタップまたはクリックしてください。
2. 図 A1.7 が表示されます。「詳細設定」の「更新時に既存のキーセットを使用する」にチェックを入れてください。（デフォルトは無効）

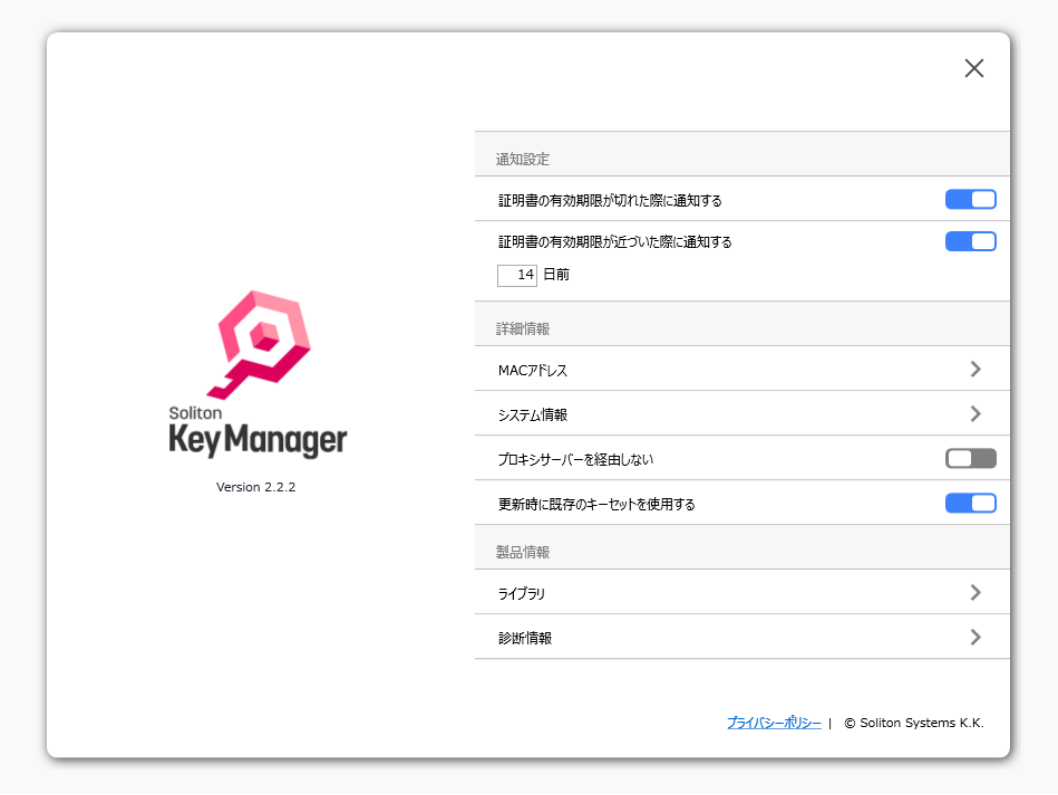

図 A1.7　設定

- **「更新時に既存のキーセットを使用する」が有効の場合は、キーサイズの変更をともなう証明書の更新を行うことはできません。例えば 2048bit の証明書を 4096bit に更新しようとしてもアクティベーション時に失敗します。**

  キーサイズの変更をともなう証明書の更新を行いたい場合は、「更新時に既存のキーセットを使用する」を無効にしてください。

Soliton KeyManager

Soliton KeyManager V2.2　説明書

2024 年 11 月 30 日	第 1 版
2025 年 2 月 1 日	第 2 版
2025 年 10 月 30 日	第 3 版
2026 年 4 月 3 日	第 4 版

株式会社ソリトンシステムズ
〒160-0022　東京都新宿区新宿 2-4-3
https://www.soliton.co.jp/

本書に記載されている情報、事項、データは、予告なく変更されることがあります。

本書に記載されている情報、事項、データは、誤りがないように最善の注意を払っていますが、本書に記載されている情報、事項、データによって引き起こされた遺失行為、傷害、損害等について、弊社は一切、その責任を負いません。

Soliton®