Soliton KeyManager

Soliton KeyManager V2　説明書

Soliton®

株式会社ソリトンシステムズ　2024 年 2 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。

- 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。

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。

- iOS/iPadOS 版

  Soliton SecureBrowser Pro や Soliton SecureDesktop Client など、Soliton 社製アプリで使用する証明書のインストールを行います。

- Android 版

  Wi-Fi、VPN での証明書認証用の他、Soliton SecureBrowser Pro 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。

  また、EPS-ap の MDM オプションを利用すれば、デバイス管理できるよう構成することができます。

- Mac 版

  Wi-Fi、VPN での証明書認証用の他、Soliton SecureBrowser Pro 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。

- Windows 版

  Wi-Fi、VPN での証明書認証用の他、Soliton SecureBrowser Pro 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 V2.0 の動作環境は、以下のとおりです。

表 2.1　動作環境（iOS/iPadOS、Android、Mac）

項目	内容		
OS	iOS/iPadOS 15.0~17.3	Android 10~14	macOS 12~14
言語*1	日本語/英語/デンマーク語/ドイツ語/スペイン語/フランス語/韓国語/オランダ語/ロシア語/スウェーデン語/中国語（簡体字）/中国語（繁体字）/ベトナム語		
その他	以下の製品が必要です。 ・NetAttest EPS V4.8.14 以降、NetAttest EPS-ap V2.0.16 以降 ・NetAttest EPS V4.8.14 以降、Soliton ID Manager V2.2.0 以降 ・Soliton OneGate		

*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。

表 2.2　動作環境（Windows）

項目	内容	
OS	Windows 10	Windows 11
言語*1	日本語/英語/デンマーク語/ドイツ語/スペイン語/フランス語/韓国語/オランダ語/ロシア語/スウェーデン語/中国語（簡体字）/中国語（繁体字）	
その他	以下の製品および環境が必要です。 ・NetAttest EPS V4.8.14 以降、NetAttest EPS-ap V2.0.16 以降 ・NetAttest EPS V4.8.14 以降、Soliton ID Manager V2.2.0 以降 ・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

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　iOS/iPadOS 版

iOS/iPadOS 版 KeyManager は、App Store からダウンロードすることができます。App Store から「Soliton KeyManager」をダウンロードし、インストールしてください。

一般的なアプリケーションと同様の手順で、アンインストールすることができます。

2.2.2　Android 版

Android 版 KeyManager は、Google Play からダウンロードすることができます。Google Play から「Soliton KeyManager V2」をダウンロードし、インストールしてください。

一般的なアプリケーションと同様の手順で、アンインストールすることができます。ただし、MDM 対象のデバイスとして構成した場合、本書の「付録 2-4　MDM プロファイルの削除」を参照し、プロファイルを削除してからアンインストールしてください。

2.2.3　Mac 版

Mac 版 KeyManager のインストール、アンインストール方法について説明します。

例として Mac 版 KeyManager V2.0.0 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。

2.2.3.1　インストールする

Mac 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。

Mac 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、管理者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「SolitonKeyManagerV200_Mac.dmg」を開いてください。
3. 展開したフォルダー内の「Soliton KeyManager.pkg」を実行してください。

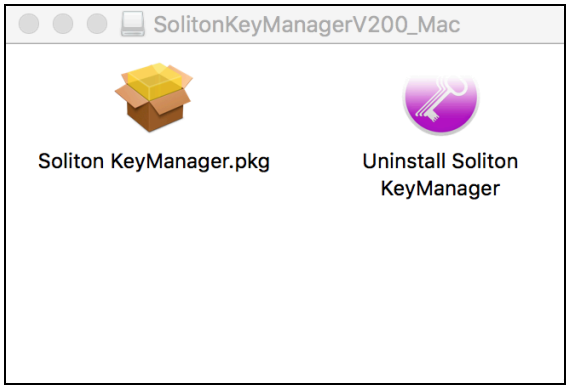

図 2.2.1　SolitonKeyManagerV2xx_Mac.dmg（展開後）

4. 図 2.2.2 が表示されます。<続ける>をクリックしてください。

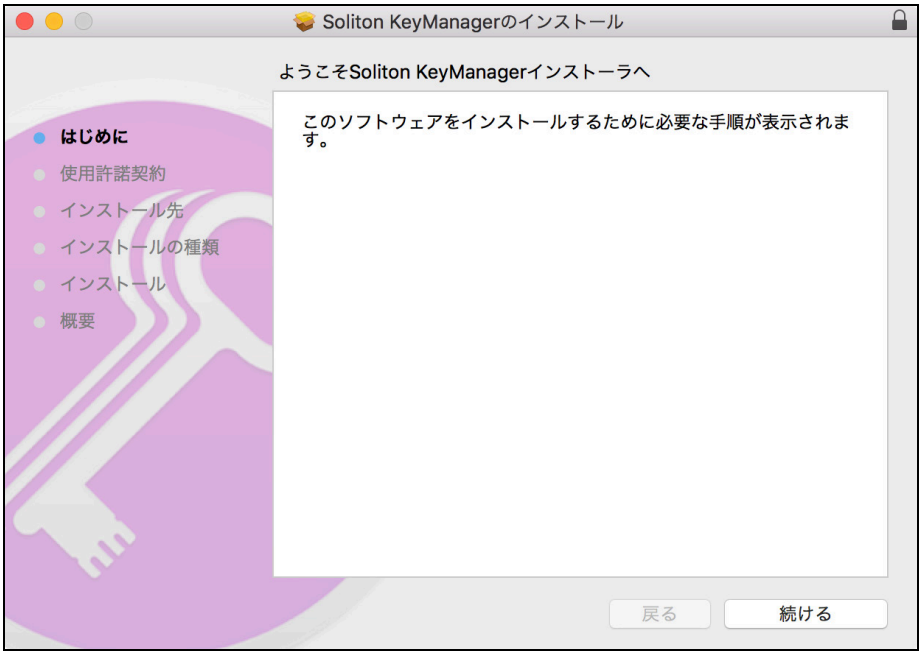

図 2.2.2　ようこそ

5. 図 2.2.3 が表示されます。使用許諾契約の内容を確認したうえで<続ける>をクリックしてください。

図 2.2.3　使用許諾契約

6. 図 2.2.4 が表示されます。<同意する>をクリックしてください。

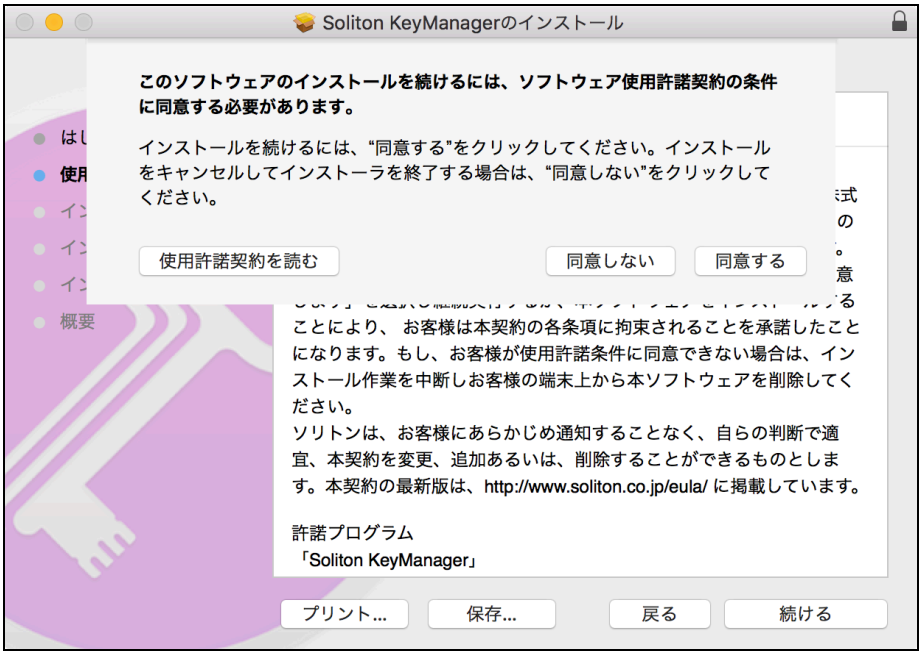

図 2.2.4　使用許諾契約の同意

7. 図 2.2.5 が表示されます。<インストール>をクリックしてください。標準インストールした場合、KeyManager はアプリケーションフォルダーにインストールされます。

※管理者権限の許可を求めるダイアログが表示された場合は、<ソフトウェアをインストール>をクリックしてください。

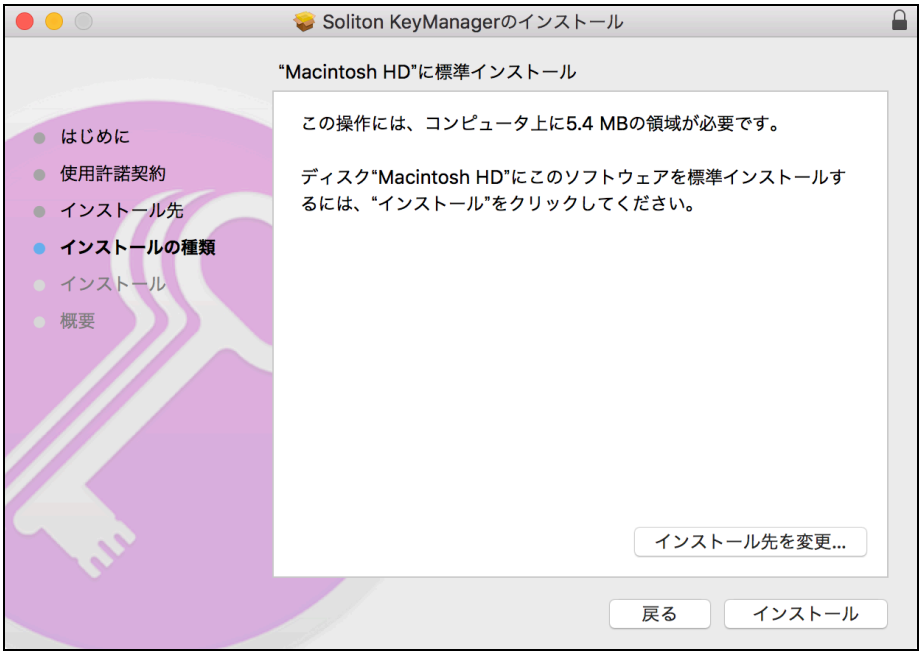

図 2.2.5　インストール

8. 図 2.2.6 が表示されます。<閉じる>をクリックしてください。

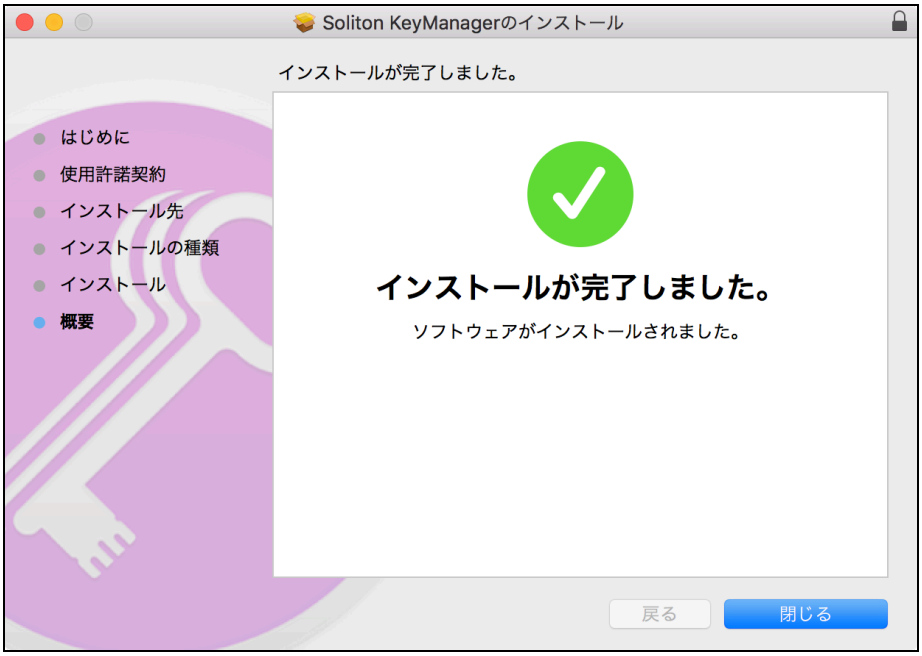

図 2.2.6　インストール完了

2.2.3.2　アンインストールする

Mac 版 KeyManager のアンインストールは、以下の手順で行ってください。

1. KeyManager をアンインストールするコンピューターに、管理者権限のユーザーでログインしてください。
2. インストール時に展開したフォルダー内の「Uninstall Soliton KeyManager」を実行してください。

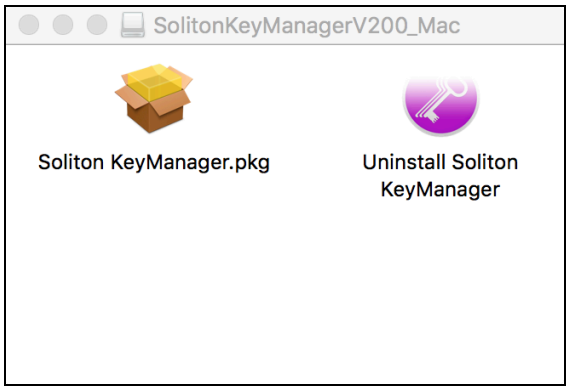

図 2.2.7　SolitonKeyManagerV2xx_Mac.dmg（展開後）

3. 図 2.2.8 が表示されます。<アンインストール>をクリックしてください。

   ※管理者権限の許可を求めるダイアログが表示された場合は、<OK>をクリックしてください。

図 2.2.8　アンインストール確認

4. 図 2.2.9 が表示されます。<OK>をクリックしてください。

図 2.2.9　アンインストール完了

キーチェーンに保存された証明書やプロファイル登録された CA 証明書は削除されません。

2.2.4　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 V2.0.0 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。

2.2.4.1　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「SolitonKeyManagerV200_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「SolitonKeyManagerV200.exe」を実行してください。

2.2.10　SolitonKeyManagerV200.exe

4. 図 2.2.11 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。

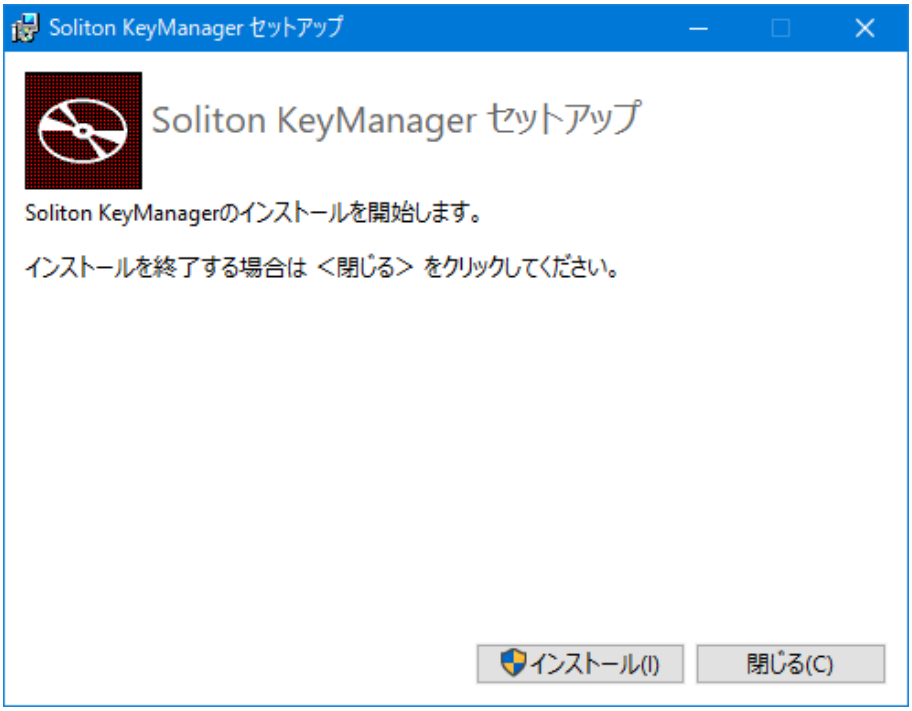

図 2.2.11　セットアップ

5. 図 2.2.12 が表示されます。<次へ>をクリックしてください。

図 2.2.12　ようこそ

6. 図 2.2.13 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。

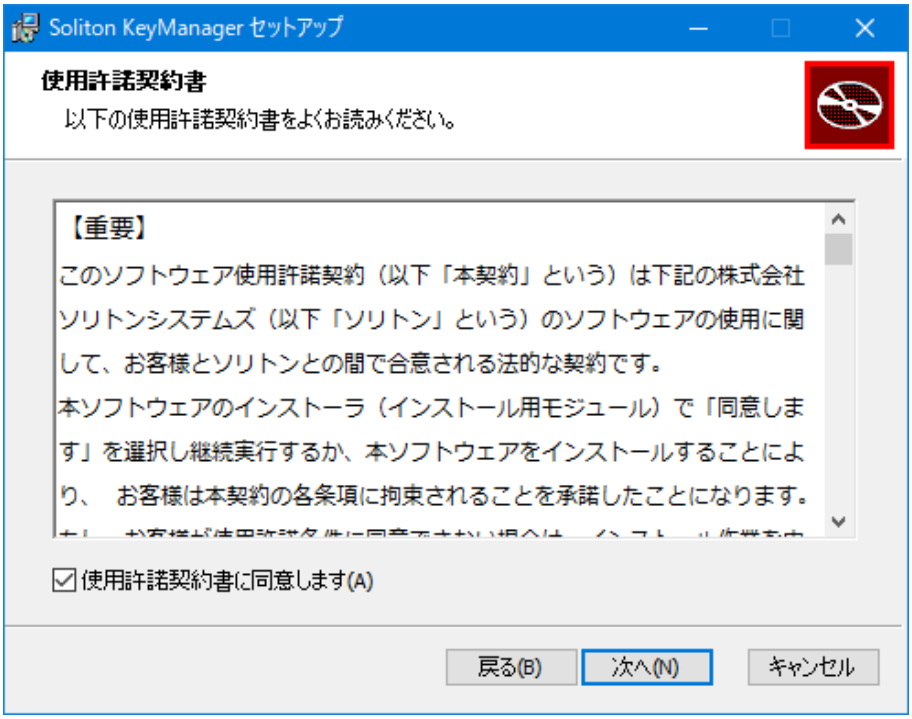

図 2.2.13　使用許諾契約書

7. 図 2.2.14 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。

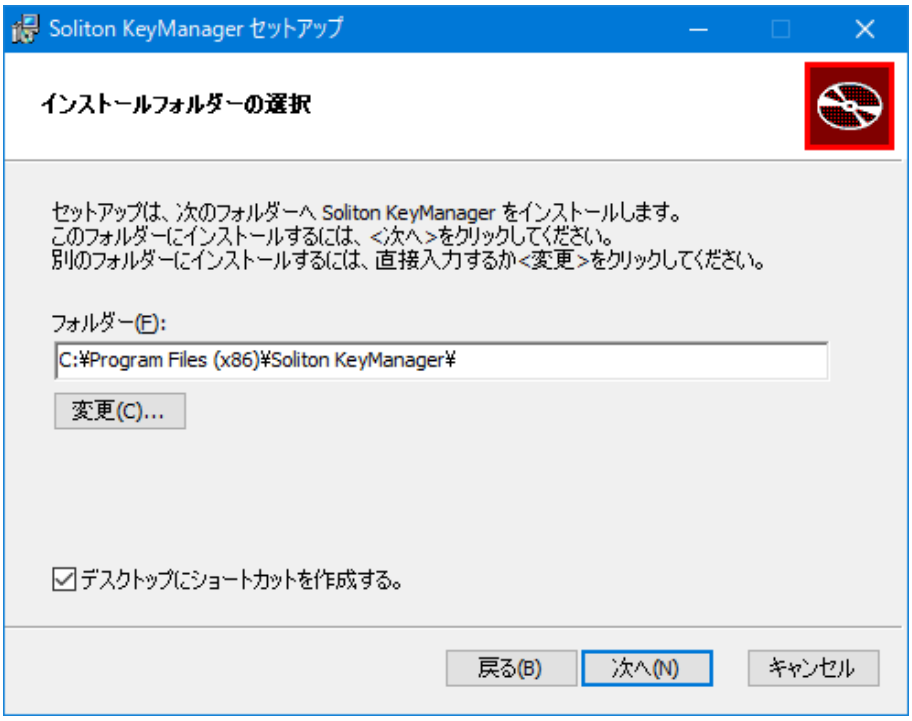

図 2.2.14　インストールフォルダーの選択

8. 図 2.2.15 が表示されます。<インストール>をクリックしてください。

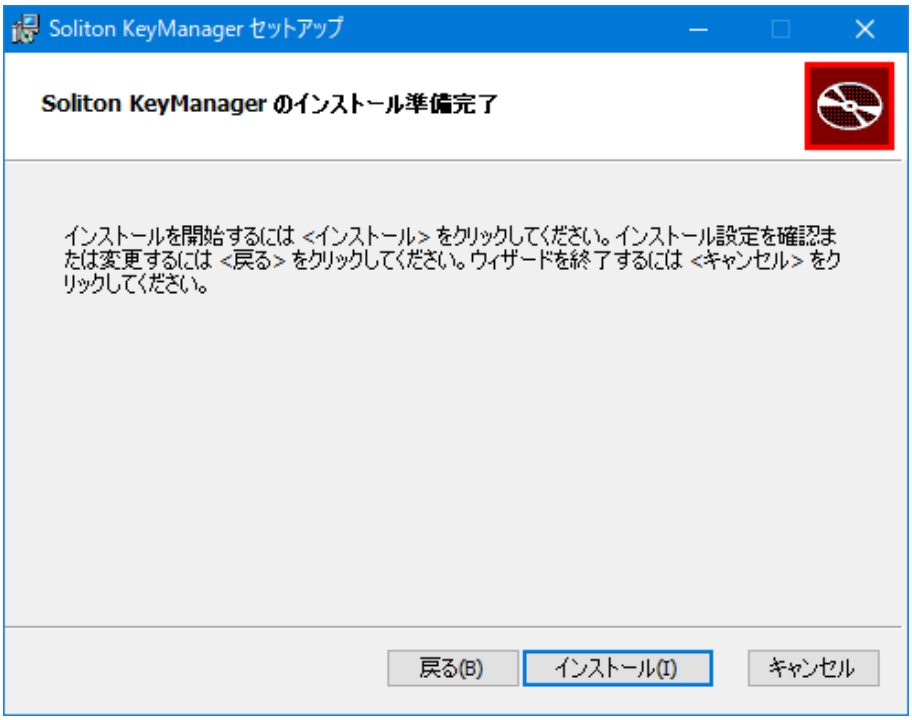

図 2.2.15　インストール準備完了

9. 図 2.2.16 が表示されます。<閉じる>をクリックしてください。

図 2.2.16　セットアップウィザード完了

10. 図 2.2.17 が表示されます。<終了する>をクリックしてください。

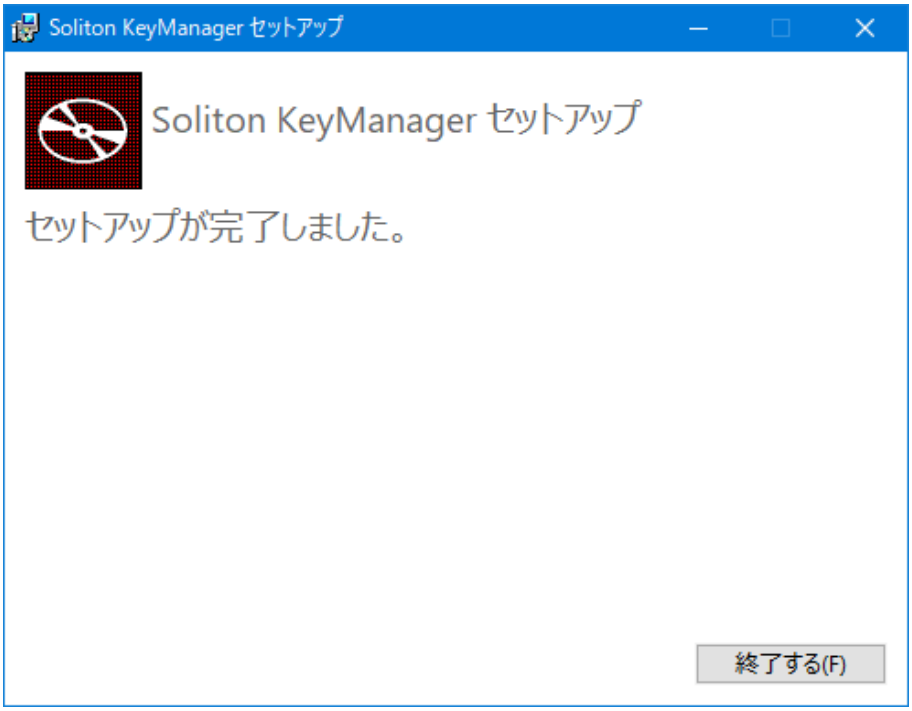

図 2.2.17　セットアップ完了

❑ 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、SolitonKeyManagerV200.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¥SolitonKeyManagerV200.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¥SolitonKeyManagerV200.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、SolitonKeyManagerV204.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¥SolitonKeyManagerV204.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。

2.2.4.2　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 V2.0.0 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「SolitonKeyManagerV200_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「SolitonKeyManagerV200.exe」を実行してください。

図 2.2.18　SolitonKeyManagerV200.exe

4. 図 2.2.19 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。

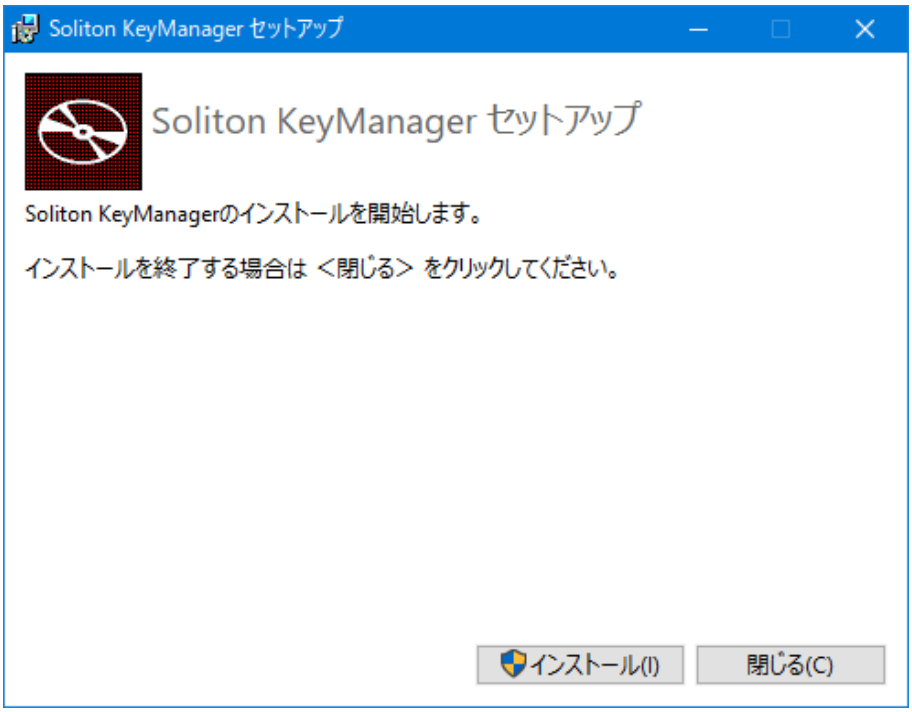

図 2.2.19　セットアップ

5. 図 2.2.20 が表示されます。<閉じる>をクリックしてください。

図 2.2.20　セットアップウィザード完了

6. 図 2.2.21 が表示されます。<終了する>をクリックしてください。

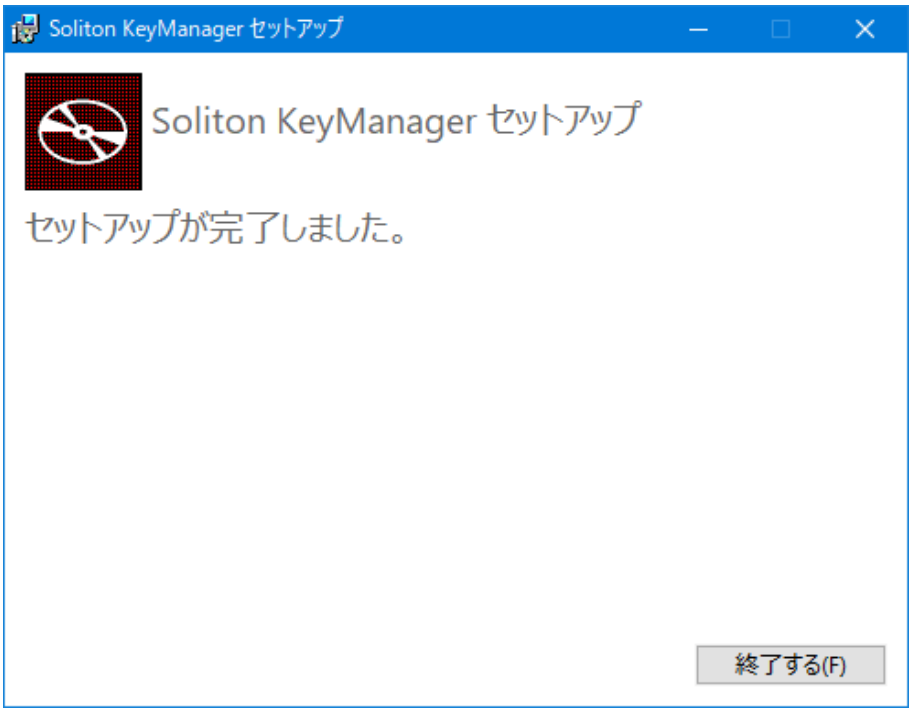

図 2.2.21　セットアップ完了

- **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。**
- **Windows 版 KeyManager V1.4.4 から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。**
  - **「インストール済み証明書一覧」の情報**
  - **「申請中の証明書一覧」の情報**
  - **「通知設定」の情報**

2.2.4.3 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「SolitonKeyManagerV200.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、SolitonKeyManagerV200.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¥SolitonKeyManagerV200.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。

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、利用開始手続きの進め方、および APID の確認方法について説明します。

KeyManager はスマートフォン、タブレット端末、PC といったデバイスの種類によって画面構成が異なります。

iOS、Android を搭載したスマートフォンを利用している場合は「スマートフォン」、iOS、iPadOS、Android を搭載したタブレット端末を利用している場合は「タブレット」、macOS、Windows を搭載した PC を利用している場合は「PC」を参照してください。

本章では、例として「スマートフォン」に Android 版、「タブレット・PC」には Mac 版を使用して説明します。特に記載がない限り、OS による内容の違いはありません。

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　スマートフォン

1.　「KeyManager」のアイコンをタップしてください。

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　起動画面

初回起動時、KeyManager に付与する権限に関するダイアログ（図 3.1.3、図 3.1.4）が表示されます。必ず<許可>を選択してください。

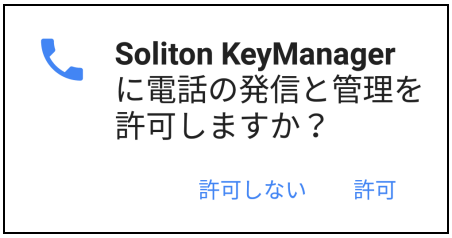

図 3.1.3　権限ダイアログ-Android

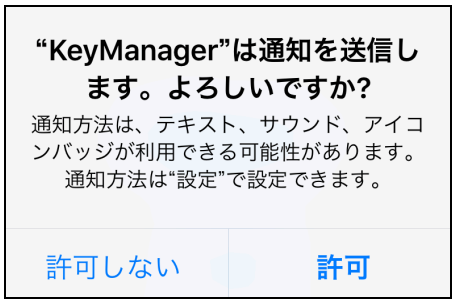

図 3.1.4　権限ダイアログ-iOS

3.1.2　タブレット・PC

1.　「KeyManager」のアイコンをタップしてください。

図 3.1.5　KeyManager

2. 図 3.1.6 が表示され、KeyManager が起動します。

図 3.1.6　起動画面

iOS、iPadOS、Android 環境では初回起動時、KeyManager に付与する権限に関するダイアログ（図 3.1.7、図 3.1.8）が表示されます。必ず<許可>を選択してください。

図 3.1.7　権限ダイアログ-Android

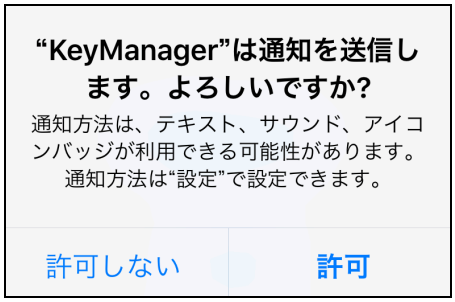

図 3.1.8　権限ダイアログ-iOS

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 または ID Manager の UDID/APID チェックが有効に設定されている場合、利用開始手続きを行う前に APID を登録する必要があります。

3.2.1　スマートフォン

1. 「KeyManager」のアイコンをタップすると KeyManager が起動し、図 3.2.1 が表示されます。<APID>をタップしてください。

図 3.2.1　起動画面

2. APID が表示されます。

図 3.2.2　APID

3. APID をタップすると APID メニューが表示されます。

図 3.2.3　APID メニュー

❑ クリップボードにコピー

APID メニューで<クリップボードにコピー>をタップすると、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 メニューで<メールで送信>をタップすると、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することができます。

Android 版の場合、アプリケーションの選択メニューが表示されます。適切なアプリケーションを選択してください。

3.2.2　タブレット・PC

1.　「Soliton KeyManager」のアイコンをクリックすると KeyManager が起動し、図 3.2.4 が表示されます。<APID>をクリックしてください。

図 3.2.4　起動画面

2. APID が表示されます。

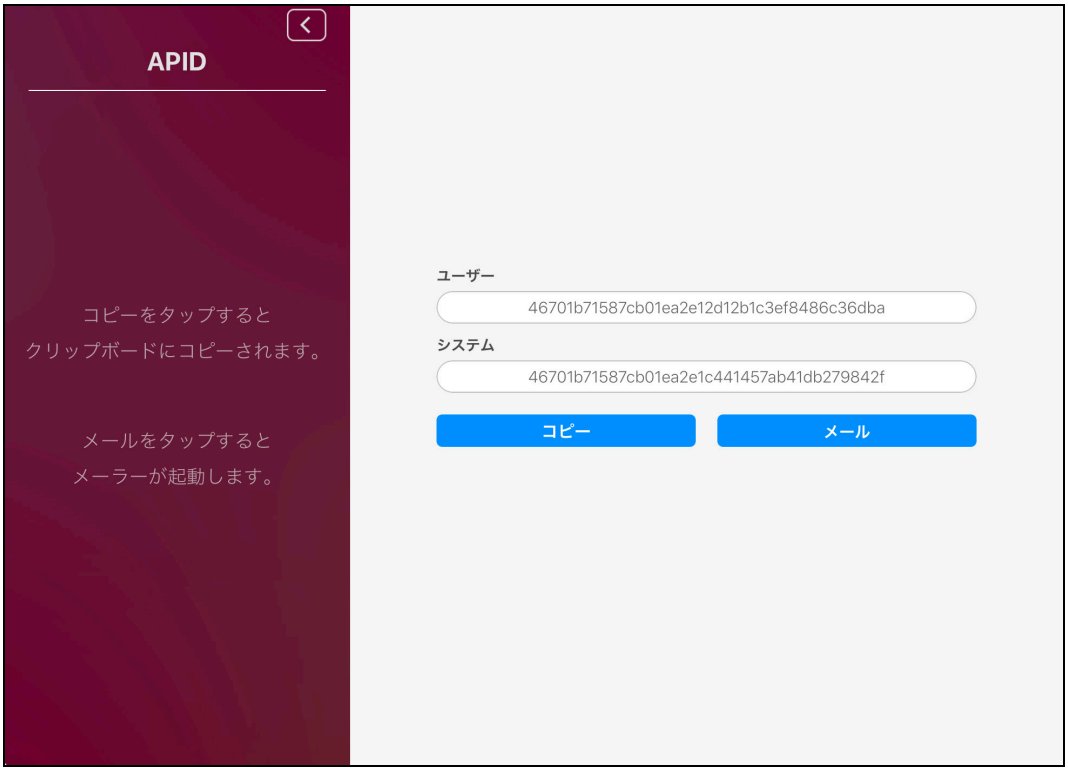

図 3.2.5　APID

❑ コピー

APID 画面で<コピー>をクリックすると、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

APID 画面で<メール>をクリックすると、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。

Android 版の場合、アプリケーションの選択メニューが表示されます。適切なアプリケーションを選択してください。

3.3　申請開始

KeyManager を使用した利用申請の手順について説明します。

3.3.1　スマートフォン

1. 起動画面で<申請開始>をタップしてください。

図 3.3.1　起動画面

2. 接続先の入力画面が表示されます。ホスト名または IP アドレス、ポート番号を入力し<次へ>をタップしてください。

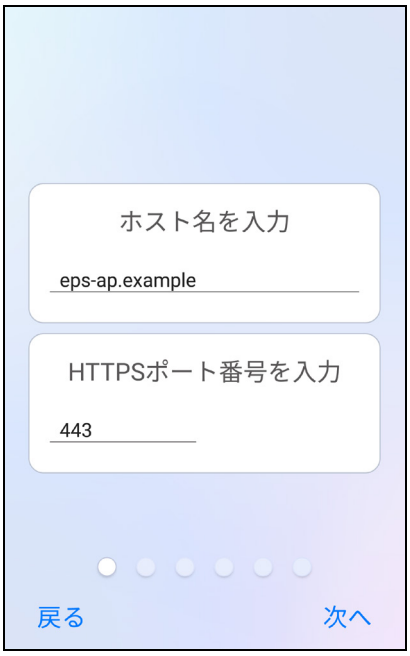

図 3.3.2　申請開始

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。

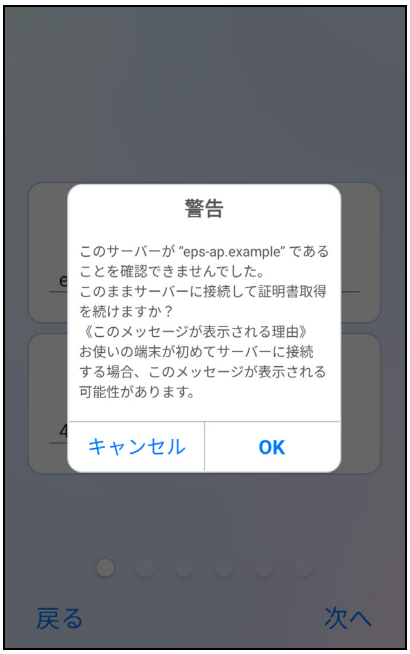

図 3.3.3　警告メッセージ

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。

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 証明書のダウンロードを行います。

   ※CA 証明書がインストールされている場合、CA 証明書はダウンロードされません。手順 5 に進んでください。

- **CA 証明書のダウンロード、インストール手順は OS によって異なります。詳しくは「付録 2-1　CA 証明書取得手順（Android）」または「付録 2-2　CA 証明書取得手順（Android 11 以降）」を参照してください。**
- **iOS 版は CA 証明書の自動ダウンロードをおこないません。CA 証明書のダウンロード、インストールについては「付録 1-1　CA 証明書取得手順（iOS）」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。
   iOS は証明書の格納先を選択しません。手順 6 に進んでください。

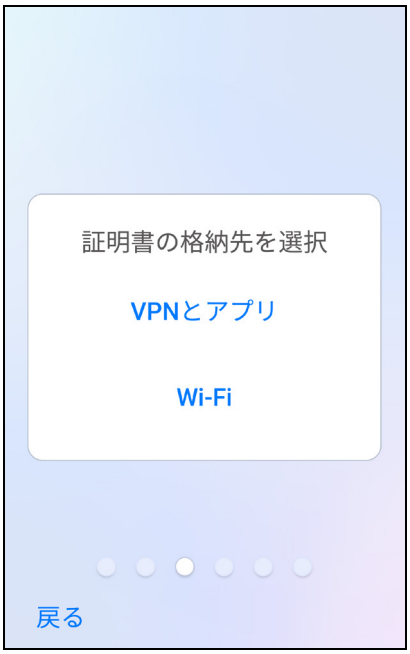

図 3.3.4　証明書の格納先

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>をタップしてください。

図 3.3.5　ID・パスワード

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

※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」「任意情報の入力」または、「3.4　承認確認-3.4.1　スマートフォン-手順 4」を参考に利用開始手続きを行ってください。

図 3.3.6　通知先メールアドレス

通知先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>をタップしてください。

※接続先の設定により、図 3.3.8 は表示されません。本項の「任意情報の入力」を参考に申請を行ってください。

図 3.3.8　申請内容確認

10. 図 3.3.9 が表示され利用申請が完了します。<トップに戻る>をタップしてください。

承認状況の確認手順は「3.4　承認確認」を参照してください。

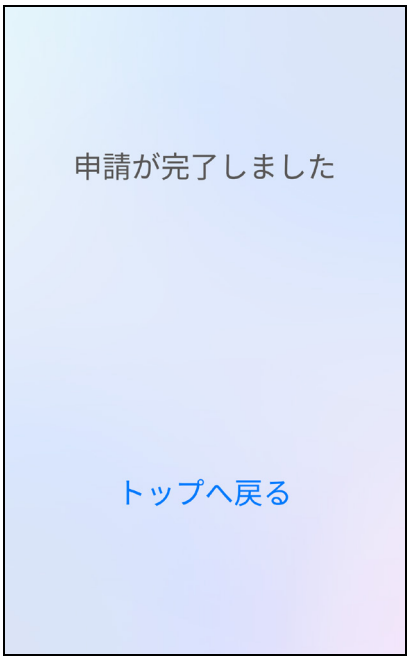

図 3.3.9　申請完了

❑ 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>をタップしてください。

図 3.3.10　招待コードを入力

2. 図 3.3.11 が表示されます。本書の「3.4　承認確認-3.4.1　スマートフォン-手順 4」を参考に利用開始手続きを行ってください。

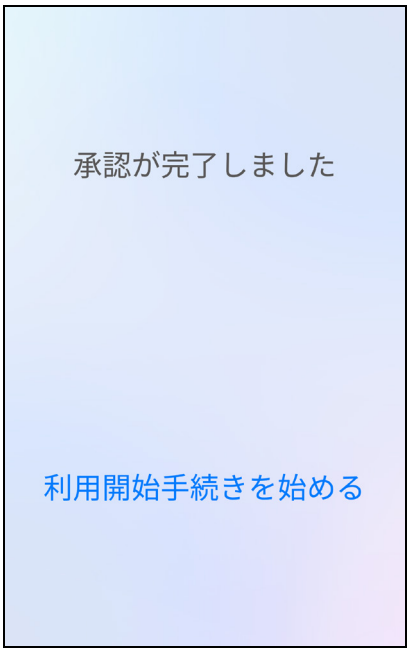

図 3.3.11　利用開始手続きを始める

❑ 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>をクリックしてください。

図 3.3.12　任意情報入力

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、項目名は接続先の設定によって変更されます。

画面の指示に従い、本書の「3.3　申請開始-3.3.1　スマートフォン-手順９」または「3.4　承認確認-3.4.1　スマートフォン-手順４」を参考に利用開始手続きを行ってください。

3.3.2　タブレット・PC

1.　起動画面で<申請開始>をクリックしてください。

図 3.3.13　起動画面

2. 図 3.3.14 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>をクリックしてください。

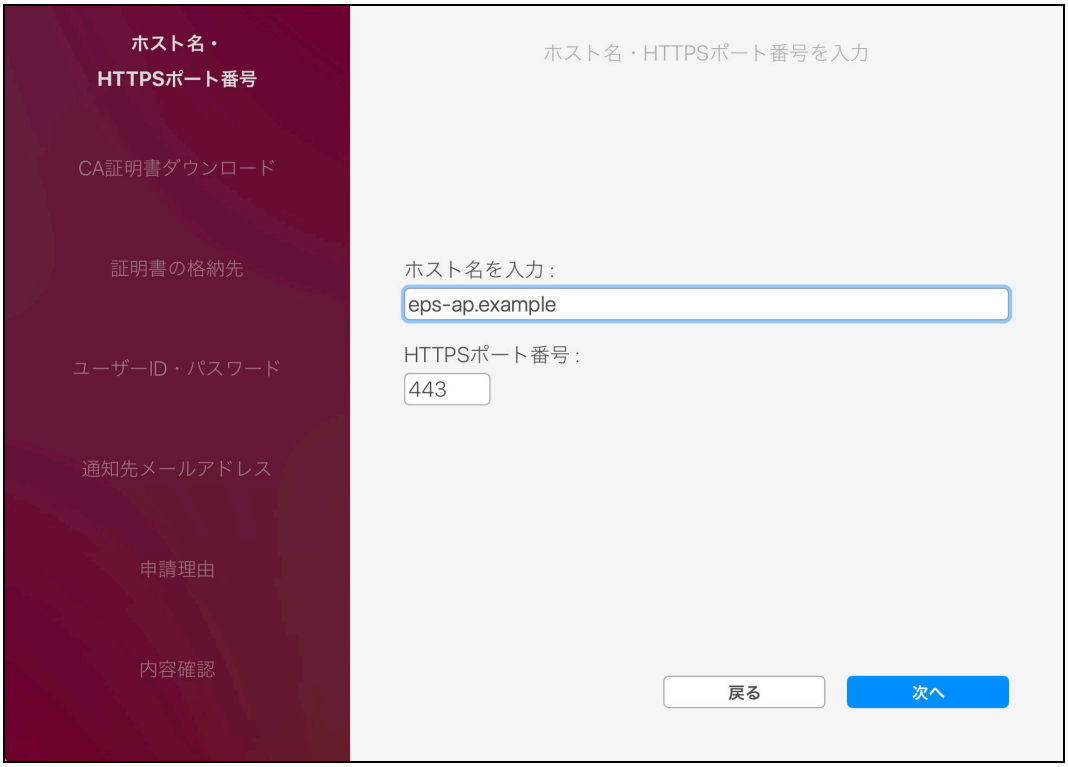

図 3.3.14　申請開始

3. 接続先が信頼されていない場合、図 3.3.15 の警告メッセージが表示されます。接続を続けるには<OK>をタップしてください。

   ※接続先が信頼されている場合、図 3.3.15 は表示されません。手順 4 に進んでください。

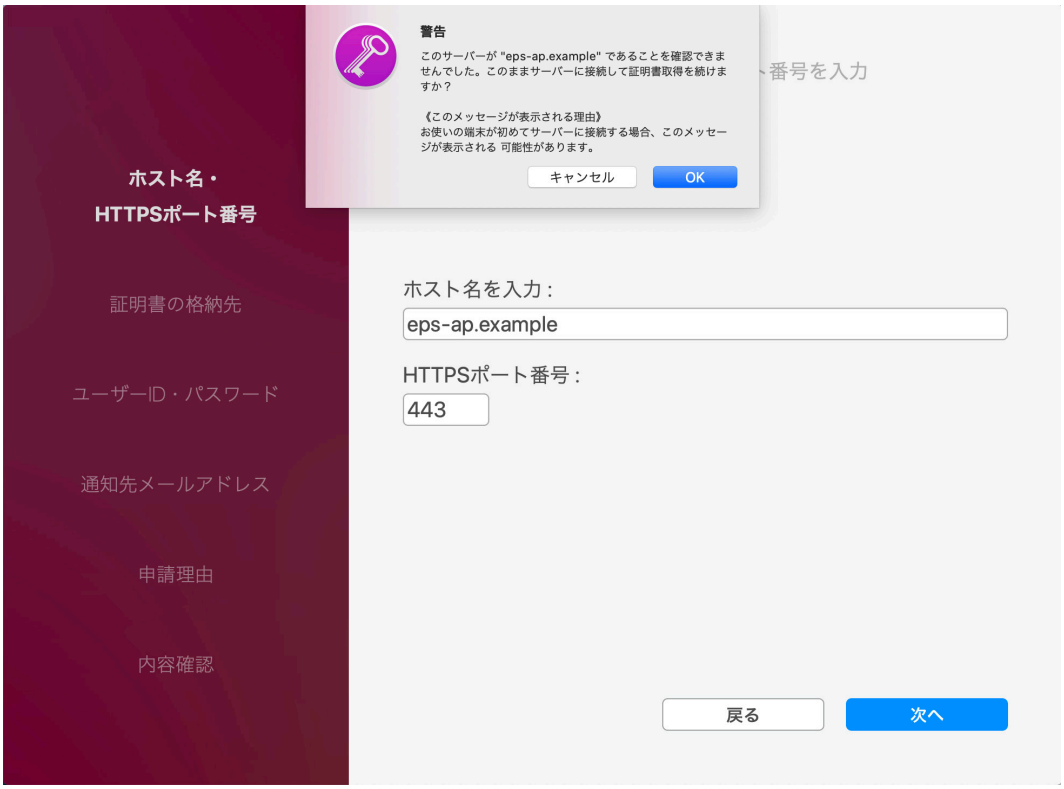

図 3.3.15　警告メッセージ

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。

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 証明書のダウンロードを行います。

   ※CA 証明書がインストールされている場合、CA 証明書はダウンロードされません。手順 5 に進んでください。

- **CA 証明書のダウンロード、インストール手順は OS によって異なります。詳しくは「付録 2-1　CA 証明書取得手順（Android 10 以前）」、「付録 2-2　CA 証明書取得手順（Android 11 以降）」、「付録 3-1　CA 証明書取得手順（Mac）」または「付録 4-1　CA 証明書取得手順（Windows）」を参照してください。**
- **iOS 版は CA 証明書の自動ダウンロードをおこないません。CA 証明書のダウンロード、インストールについては「付録 1-1　CA 証明書取得手順（iOS）」を参照してください。**

5. 図 3.3.16 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。
   iPadOS は証明書の格納先を選択しません。手順 5 に進んでください。

図 3.3.16　証明書の格納先

6. 図 3.3.17 が表示されます。「ユーザーID」「パスワード」を入力して<次へ>をクリックしてください。

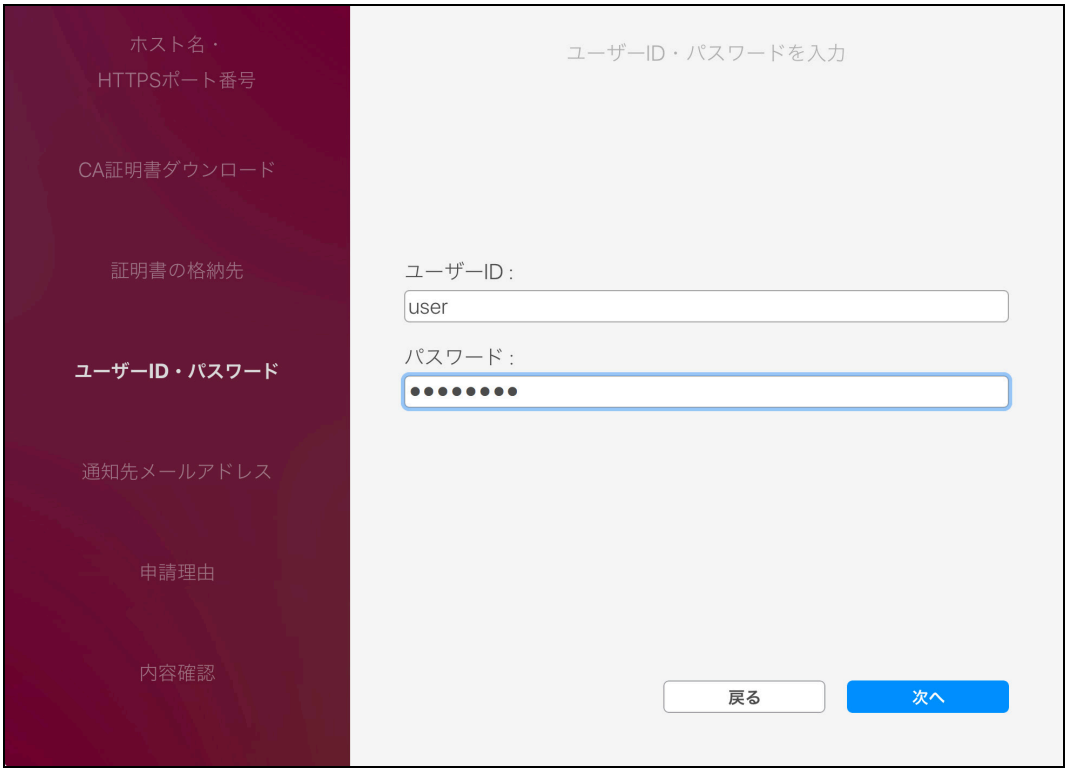

図 3.3.17　ID・パスワード

7. 図 3.3.18 が表示されます。必要に応じて「通知先メールアドレス」を入力し<次へ>、または<スキップ>を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 3.3.18 は表示されません。本項の「招待コードを入力」「任意情報の入力」または、「3.4　承認確認-3.4.2　タブレット・PC-手順 4」を参考に利用開始手続きを行ってください。

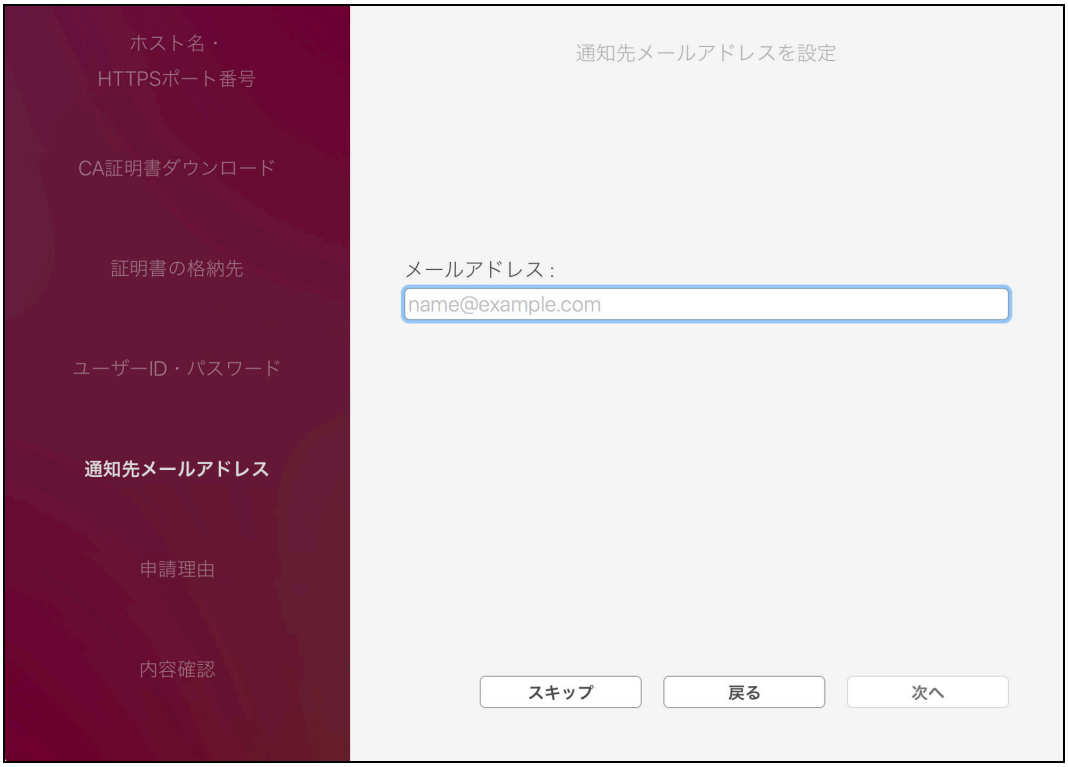

図 3.3.18　通知先メールアドレス

通知先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 3.3.19 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>をクリックしてください。

図 3.3.19　申請理由

9. 図 3.3.20 が表示されます。申請内容を確認し<申請>をクリックしてください。

※接続先の設定により、図 3.3.20 は表示されません。本項の「任意情報の入力」を参考に申請を行ってください。

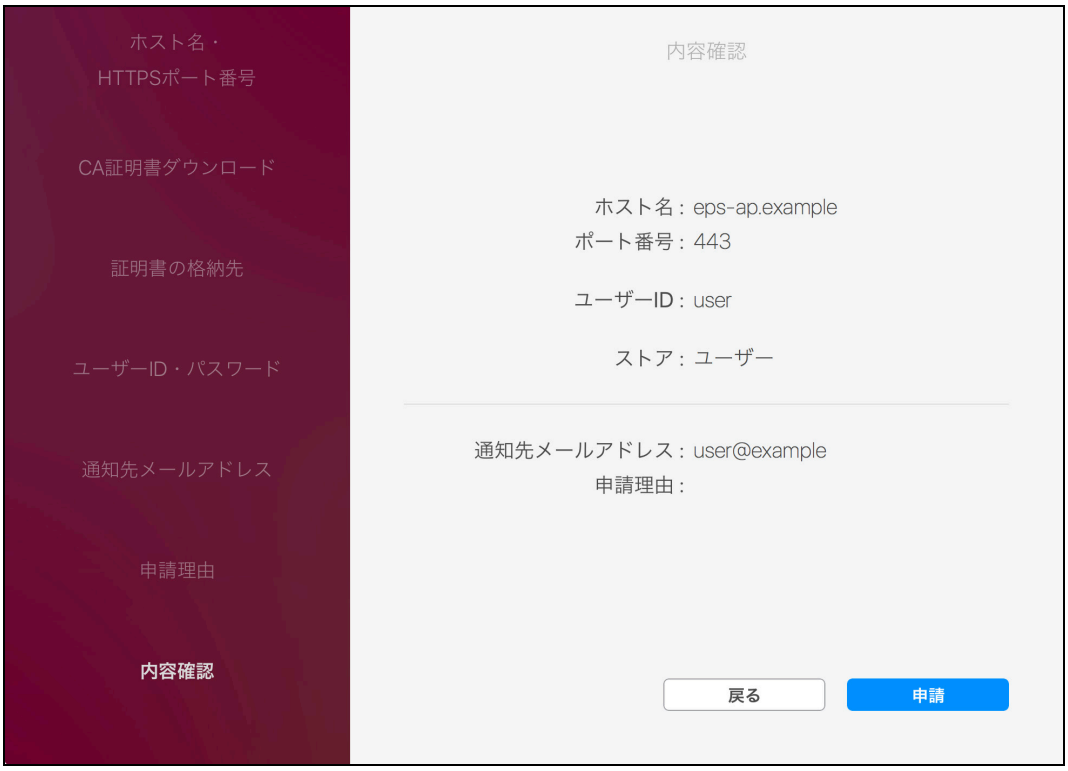

図 3.3.20　内容確認

10. 申請が完了すると図 3.3.21 が表示されます。<トップに戻る>をクリックしてください。
    承認状況の確認手順は「3.4　承認確認」を参照してください。

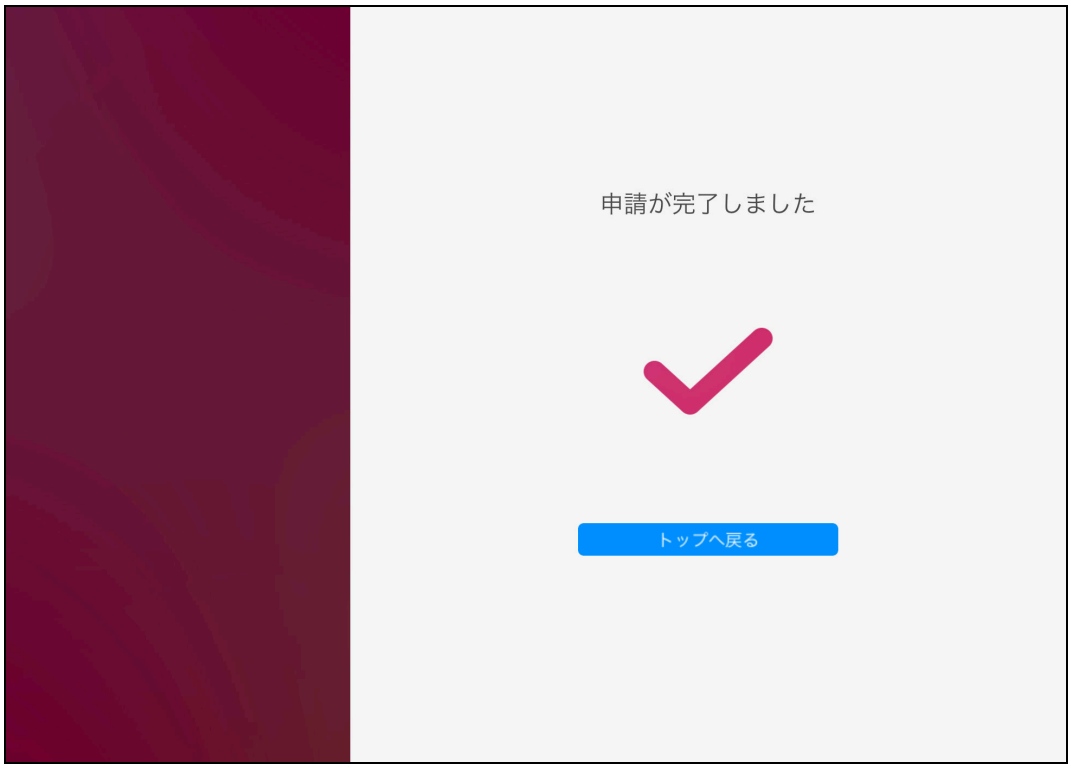

図 3.3.21　申請完了

❑ 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>をクリックしてください。

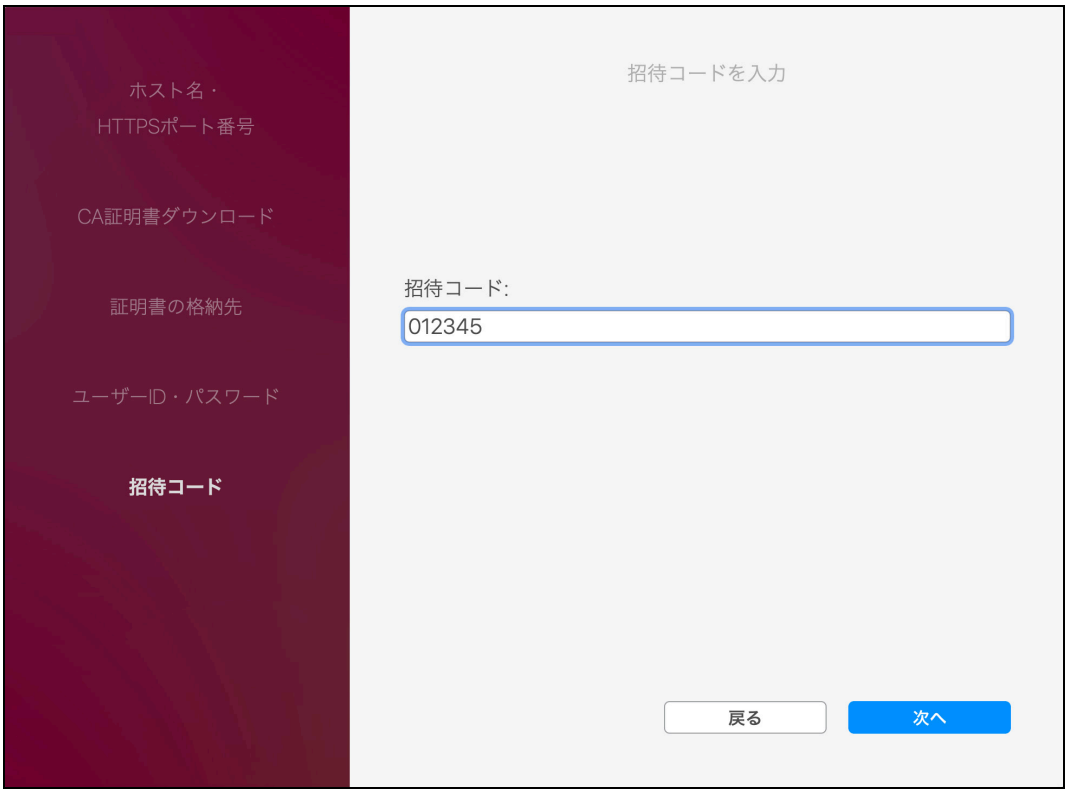

図 3.3.22　招待コードを入力

2. 図 3.3.23 が表示されます。本書の「3.4　承認確認-3.4.2　タブレット・PC-手順 4」を参考に利用開始手続きを行ってください。

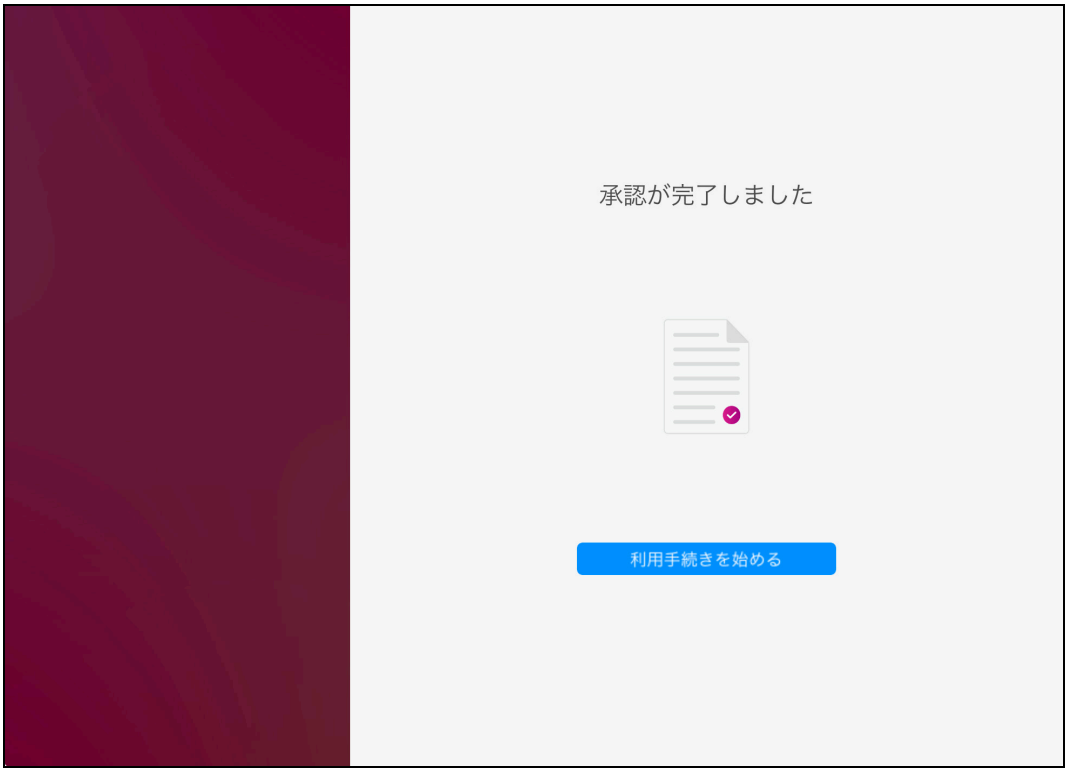

図 3.3.23　利用開始手続きを始める

❑ 任意情報の入力

接続先の設定に合わせて図 3.3.24 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>をクリックしてください。

図 3.3.24　任意情報入力

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、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　申請開始-3.3.2　タブレット・PC-手順９」または「3.4　承認確認-3.4.2 タブレット・PC-手順４」を参考に利用開始手続きを行ってください。

3.4　承認確認

申請の承認状況を確認する手順について説明します。

3.4.1　スマートフォン

1.　申請中は起動画面に<承認確認>が表示されます。<承認確認>をタップしてください。

図 3.4.1　起動画面-承認確認

2.　図 3.4.2 が表示されます。<承認状況を確認する>をタップしてください。

図 3.4.2　承認確認

3. 図 3.4.4 が表示されます。「パスワード」を入力し<次へ>をタップしてください。

図 3.4.4　パスワード-承認確認

4. 承認が完了していると図 3.4.5 が表示されます。<利用開始手続きを始める>をタップしてください。

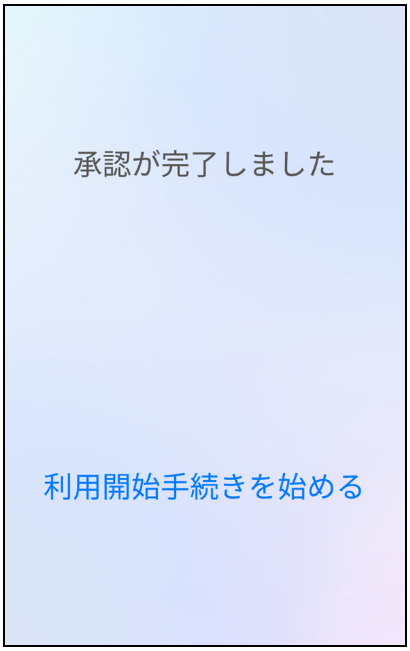

図 3.4.5　利用開始手続きを始める

5.　利用開始手続きが完了すると証明書がインストールされます。

図 3.4.6　利用開始手続き完了

Android 版の場合、証明書の利用目的ごとに格納先を指定する必要があります。証明書名の指定画面にある「認証情報の使用」では申請時に選択した証明書の格納先と同じ設定を指定してください。

- **VPN とアプリ**

  Android 版 Soliton SecureBrowser Pro など、Wi-Fi 接続以外の用途で証明書を使用する場合に選択してください。

- **Wi-Fi**

  Wi-Fi 接続で証明書を使用する場合に選択してください。Wi-Fi を選択した場合は、CA 証明書とユーザー証明書の両方を「認証情報の使用：Wi-Fi」に格納してください。

3.4.2　タブレット・PC

1.　申請中は起動画面に<承認確認>が表示されます。<承認確認>をクリックしてください。

図 3.4.7　起動画面-承認確認

2. 図 3.4.8 が表示されます。<承認状況を確認する>をクリックしてください。

図 3.4.8　承認確認

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

図 3.4.9　パスワード-承認確認

4. 承認が完了していると図 3.4.10 が表示されます。<利用開始手続きを始める>をクリックしてください。

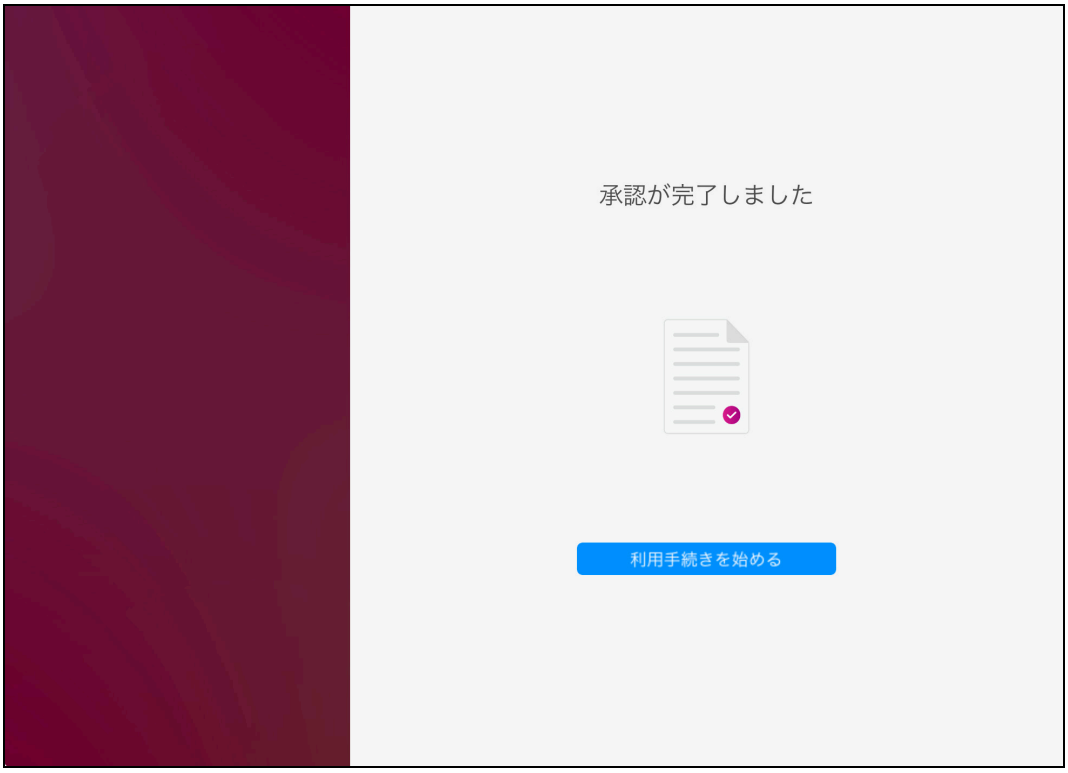

図 3.4.10　利用開始手続きを始める

5. 利用開始手続きが完了すると証明書がインストールされます。

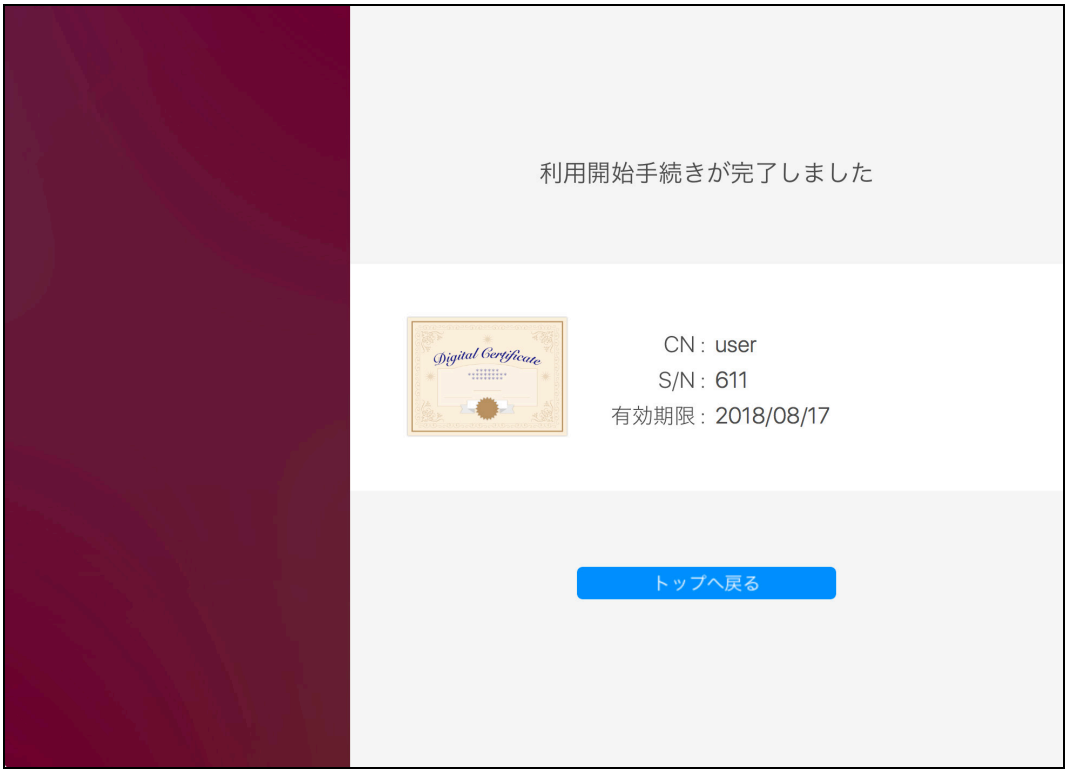

図 3.4.11　利用開始手続き完了

Android 版 KeyManager の場合、証明書の利用目的ごとに格納先を指定する必要があります。証明書名の指定画面にある「認証情報の使用」では申請時に選択した証明書の格納先と同じ設定を指定してください。

- **VPN とアプリ**

  Android 版 Soliton SecureBrowser Pro など、Wi-Fi 接続以外の用途で証明書を使用する場合に選択してください。

- **Wi-Fi**

  Wi-Fi 接続で証明書を使用する場合に選択してください。Wi-Fi を選択した場合は、CA 証明書とユーザー証明書の両方を「認証情報の使用：Wi-Fi」に格納してください。

Mac 版 KeyManager ではシステムキーチェーンに証明書を保存する際、「Soliton KeyManager HelperTool」というツールを使用します。証明書の格納先に「システム」を選択した場合、「Soliton KeyManager HelperTool」のインストール、および利用のため管理者権限を求めるダイアログが表示されます。パスワードを入力し、インストール、および利用許可を行ってください。

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。

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　スマートフォン

1. 起動画面の<申請開始>をタップしてください。

図 3.5.1　起動画面

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。更新したい証明書の<申請>をタップしてください。

図 3.5.2　申請開始-更新申請

3. 図 3.5.3 が表示されます。パスワードを入力し<次へ>をタップしてください。

図 3.5.3　パスワード-更新申請

4. 図 3.5.4 が表示されます。必要に応じて「通知先メールアドレス」を入力し<次へ>、または<スキップ>をタップしてください。

   ※接続先の設定や承認状況により、図 3.5.4 は表示されません。本書の「3.4　承認確認-3.4.1　スマートフォン-手順 4」を参考に利用開始手続きを行ってください。

図 3.5.4　通知先メールアドレス-更新申請

5. 図 3.5.5 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>をタップしてください。

図 3.5.5　申請理由-更新申請

6. 図 3.5.6 が表示されます。申請内容を確認し<申請>をタップしてください。

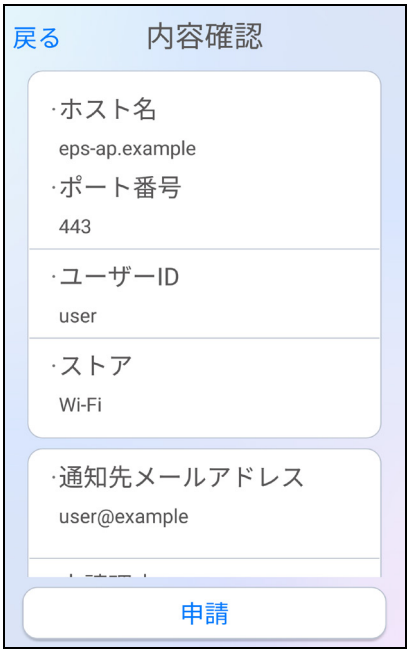

図 3.5.6　内容確認

7. 申請が完了すると図 3.5.7 が表示されます。<トップに戻る>をタップしてください。
承認状況の確認手順は「3.4　承認確認」を参照してください。

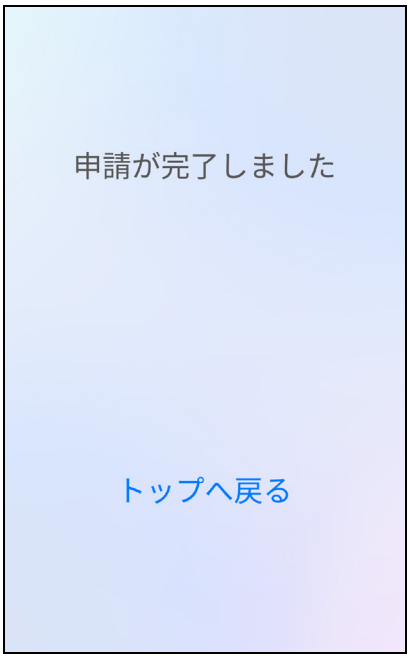

図 3.5.7　申請完了

3.5.2　タブレット・PC

1. 起動画面の<申請開始>をクリックしてください。

図 3.5.8　起動画面

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。更新したい証明書の<申請>をクリックしてください。

図 3.5.9　申請開始-更新申請

3. 図 3.5.10 が表示されます。パスワードを入力し<次へ>をクリックしてください。

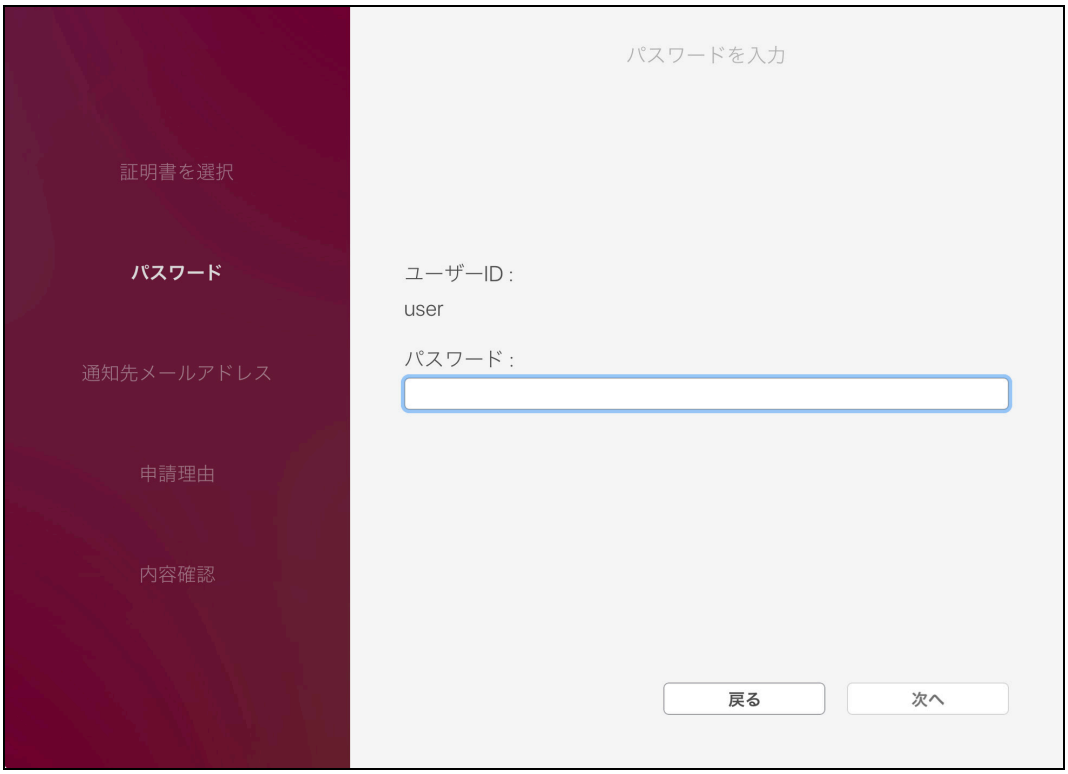

図 3.5.10　パスワード-更新申請

4. 図 3.5.11 が表示されます。必要に応じて「通知先メールアドレス」を入力し<次へ>をクリック、または<スキップ>を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 3.5.11 は表示されません。本書の「3.4　承認確認-3.4.2　タブレット・PC-手順 4」を参考に利用開始手続きを行ってください。

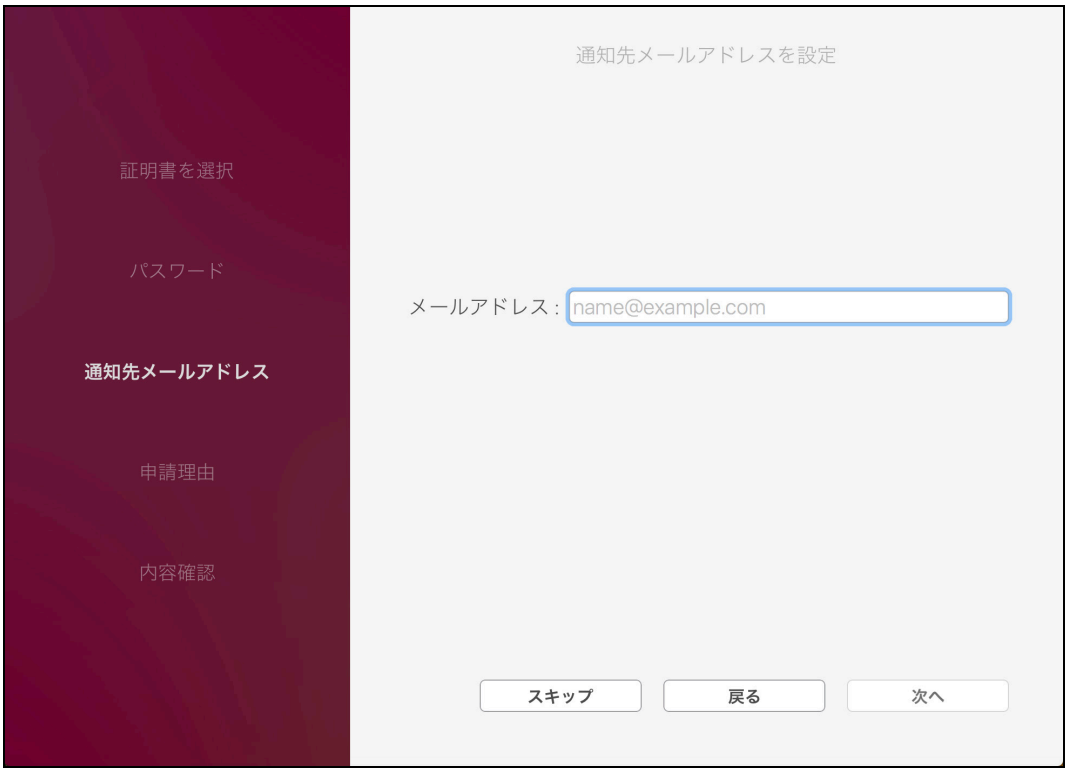

図 3.5.11　通知先メールアドレス-更新申請

5. 図 3.5.11 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>をクリックしてください。

図 3.5.11　申請理由-更新申請

6. 図 3.5.12 が表示されます。申請内容を確認し<申請>をクリックしてください。

図 3.5.12　内容確認

7. 申請が完了すると図 3.5.13 が表示されます。<トップに戻る>をクリックしてください。
   承認状況の確認手順は「3.4　承認確認」を参照してください。

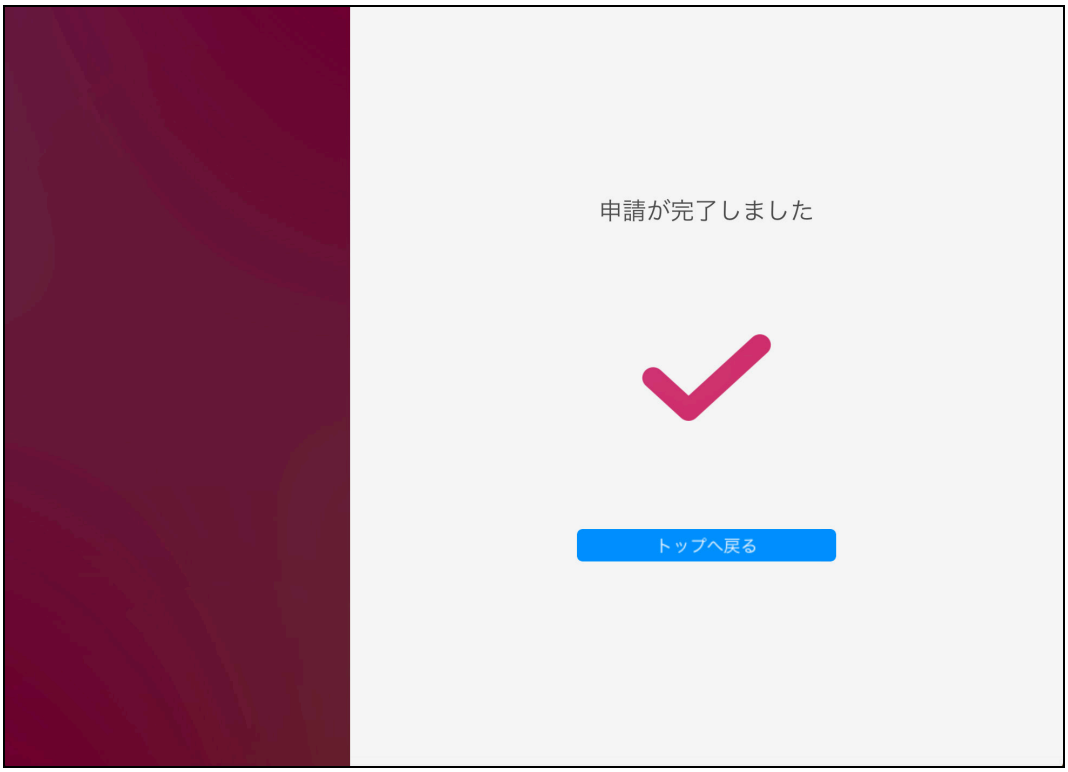

図 3.5.13　申請完了

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。

KeyManager はスマートフォン、タブレット端末、PC といったデバイスの種類によって画面構成が異なります。

iOS、Android を搭載したスマートフォンを利用している場合は「スマートフォン」、iOS、iPadOS、Android を搭載したタブレット端末を利用している場合は「タブレット」、macOS、Windows を搭載した PC を利用している場合は「PC」の項を参照してください。

例として「スマートフォン・タブレット」には Android 版、「PC」には Mac 版を使用して説明します。

4.1　証明書の確認・削除

KeyManager を経由してインストールした証明書の確認・削除方法について説明します。

4.1.1　スマートフォン・タブレット

1. 起動画面上部にある歯車アイコンをタップしてください。
2. 図 4.1.1 が表示されます。<証明書一覧>をタップしてください。

図 4.1.1　設定メニュー

- **iOS/iPadOS 版の場合、設定メニューに「iTunes から証明書をインストール」が表示されます。**
- **Android 版 KeyManager を利用し MDM 対象デバイスとして構成している場合、設定メニューに[MDM]-[プロファイル]が表示されます。**

3. インストールした証明書一覧が表示されます。詳細の確認、または削除したい証明書をタップしてください。

図 4.1.2　証明書一覧

4. 証明書の詳細が表示されます。画面右上のメニューアイコンをタップしてください。

図 4.1.3　証明書詳細

5. 証明書メニューが表示されます。<削除>をタップしてください。

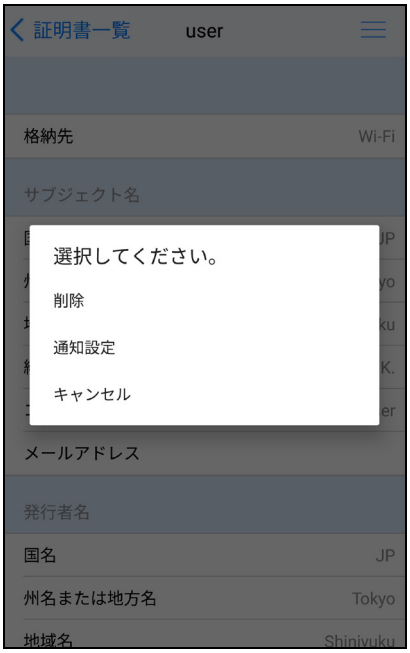

図 4.1.4　証明書メニュー

6. 確認ダイアログが表示されます。<はい>をタップしてください。

図 4.1.5　削除確認

Android 版の場合、OS の証明書ストアに格納されている証明書の実体は削除されません。

7. 削除が完了し証明書一覧画面に遷移します。

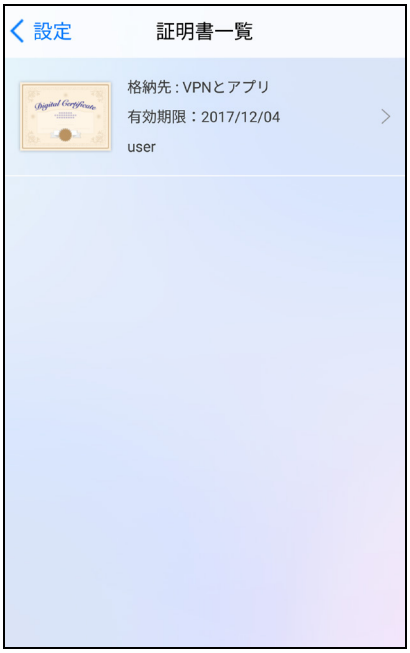

図 4.1.6　証明書一覧（削除後）

4.1.2　PC

1. 起動画面上部にある歯車アイコンをクリックしてください。
2. 証明書一覧画面が表示されます。削除したい証明書の<…>をタップしてください。

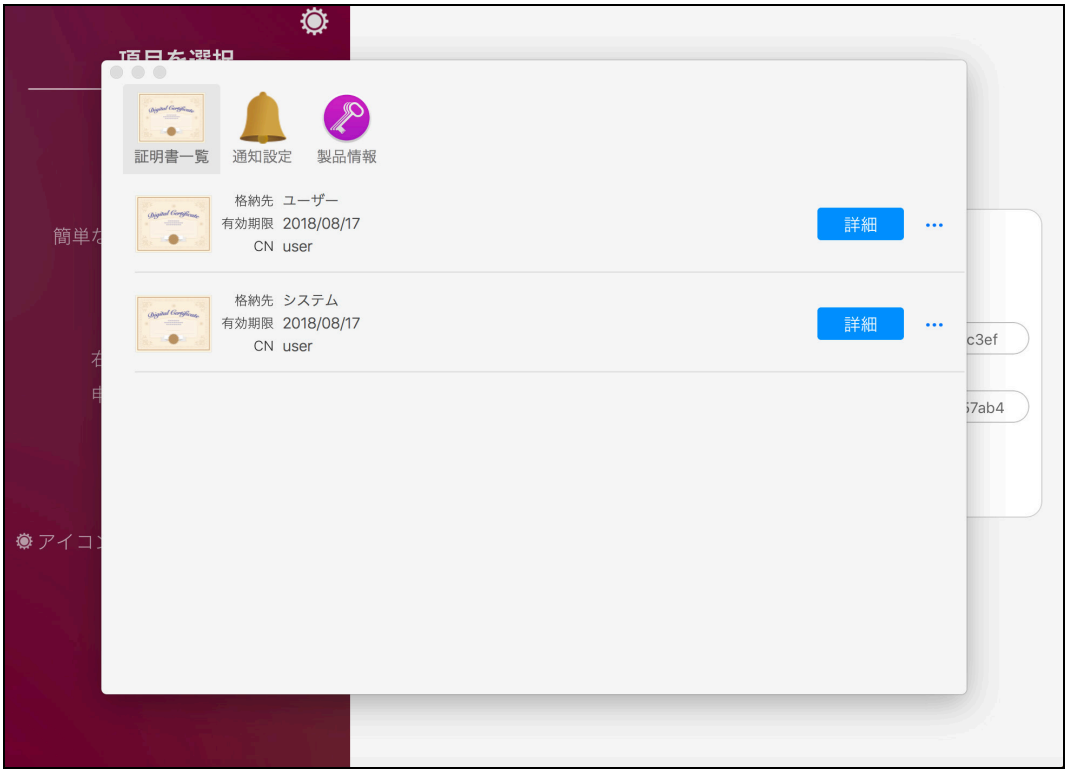

図 4.1.7　設定（PC）

3. 証明書メニューが表示されます。<削除>をクリックしてください。

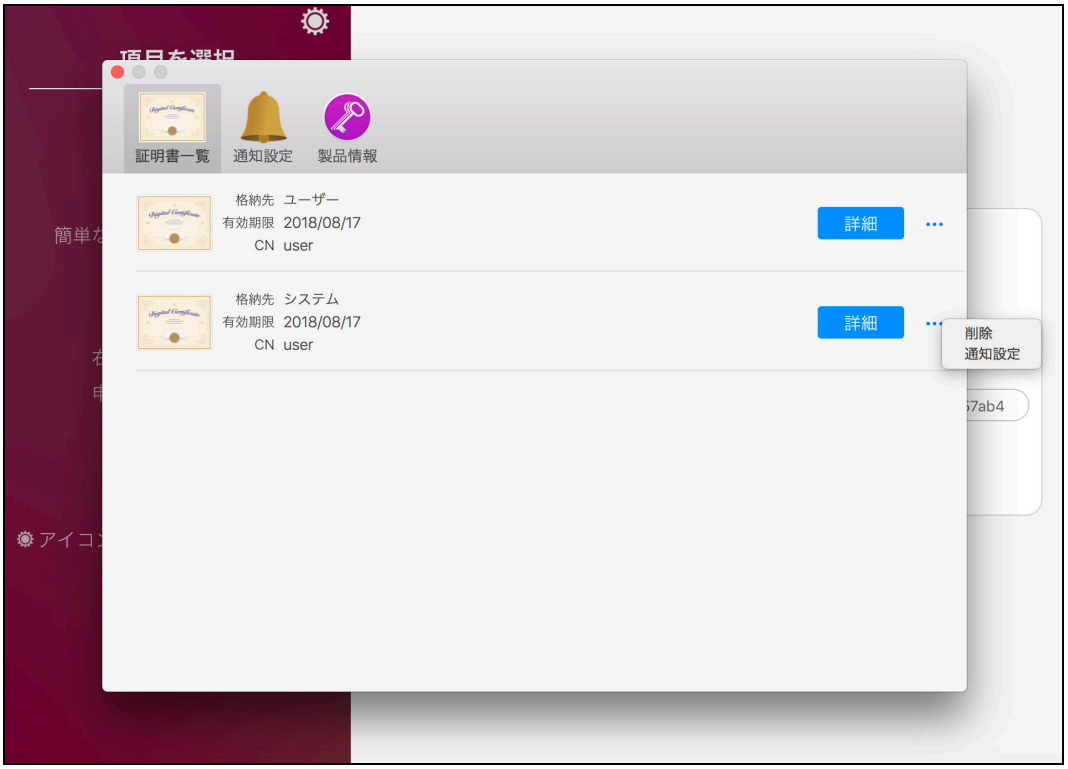

図 4.1.8　証明書メニュー

4. 削除の確認ダイアログが表示されます。<はい>をクリックしてください。

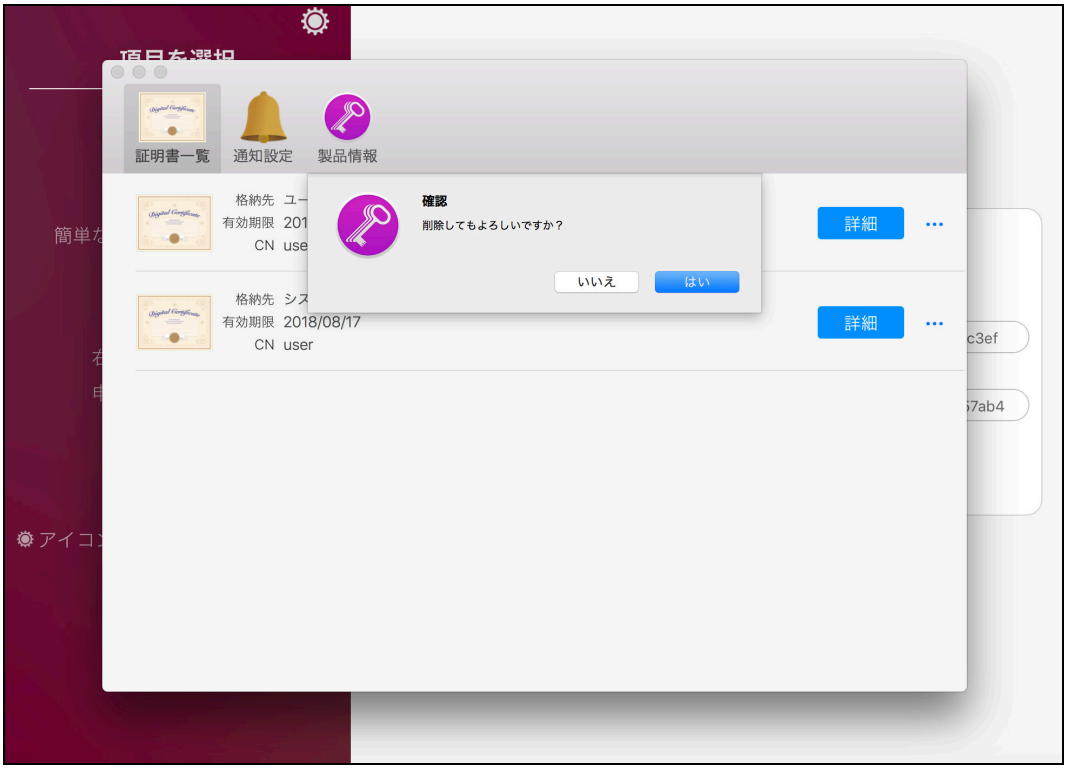

図 4.1.9　削除確認メッセージ

削除する証明書の[格納先]が「システム（Mac)」または「コンピューター（Windows)」の場合、証明書を削除するために管理者権限の許可を求めるダイアログ（ユーザーアカウント制御）が表示されます。

4.2　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り、有効期限が切れたりした場合に表示される、通知メッセージ機能の設定方法について説明します。

例として「スマートフォン・タブレット」には Android 版、「PC」には Mac 版を使用して説明します。

4.2.1　デフォルト設定を変更する

インストールする証明書の有効期限通知に関する設定を変更します。

以降、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。

4.2.1.1　スマートフォン・タブレット

1. 起動画面上部にある歯車アイコンをタップしてください。
2. 図 4.2.1 が表示されます。<通知設定>をタップしてください。

図 4.2.1　設定メニュー

3. 図 4.2.2 が表示されます。必要に応じて期限切れ通知、および期限切れ間近通知の設定を変更してください。

図 4.2.2　通知設定

表 4.2.1　通知設定

項目		説明
期限切れ通知		証明書の有効期限が過ぎたことを通知する設定です。
	通知	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）
期限切れ間近通知		証明書の有効期限切れを事前に通知する設定です。
	通知	証明書の有効期限切れを事前に通知する場合は、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

4.2.1.2　PC

1. 起動画面上部にある歯車アイコンをクリックしてください。
2. 証明書一覧画面が表示されます。<通知設定>をクリックしてください。

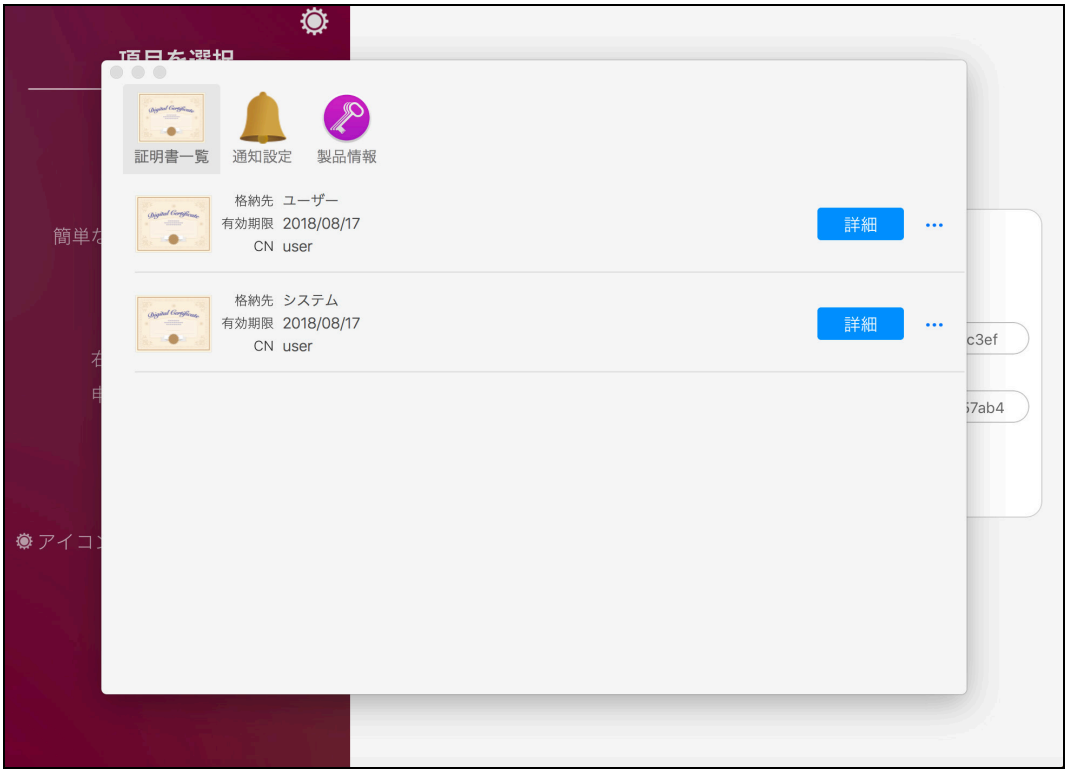

図 4.2.3　設定メニュー

3. 図 4.2.4 が表示されます。必要に応じて期限切れ通知、および期限切れ間近通知の設定を変更してください。

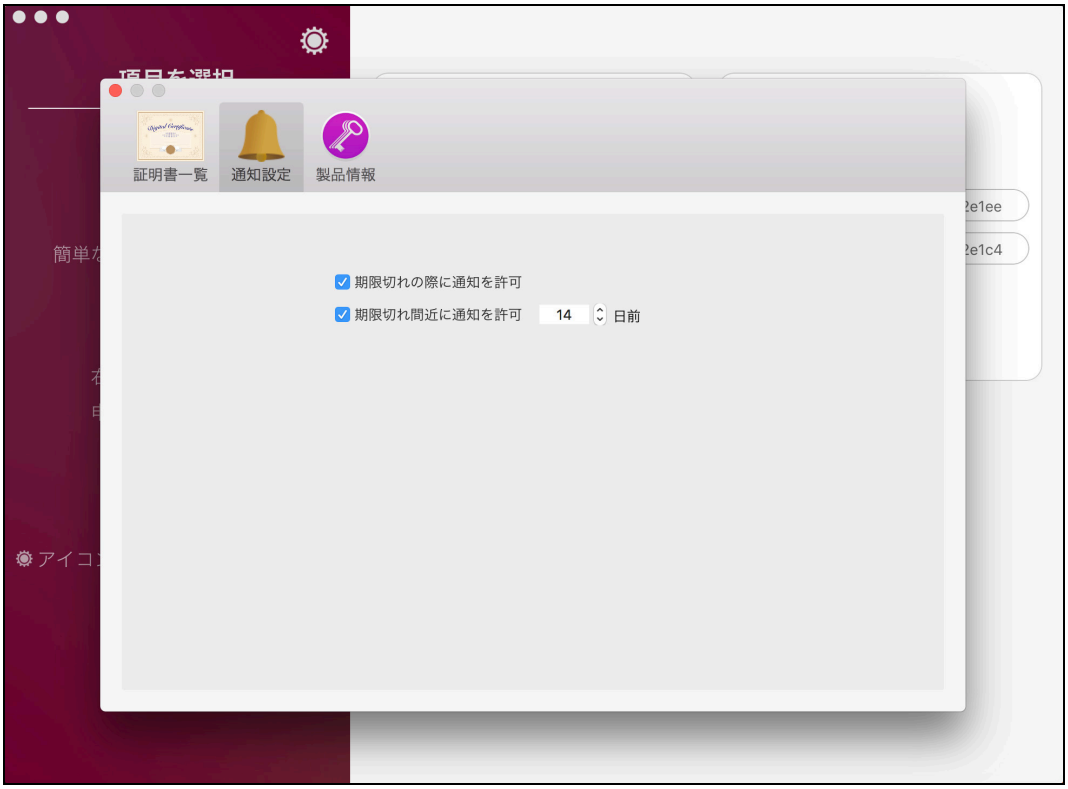

図 4.2.4　通知設定

表 4.2.2　通知設定

項目		説明
期限切れ通知		証明書の有効期限が過ぎたことを通知する設定です。
	通知	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）
期限切れ間近通知		証明書の有効期限切れを事前に通知する設定です。
	通知	証明書の有効期限切れを事前に通知する場合は、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

4.2.2　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、個別に有効期限通知の設定を変更することができます。

証明書単位で有効期限通知の設定を変更する手順は、以下のとおりです。

4.2.2.1　スマートフォン・タブレット

1. 起動画面上部にある歯車アイコンをタップしてください。

2. 図 4.2.5 が表示されます。<証明書一覧>をタップしてください。

図 4.2.5　設定メニュー

3. 図 4.2.6 が表示されます。通知設定を変更したい証明書をタップしてください。

図 4.2.6　証明書一覧

4. 図 4.2.7 が表示されます。画面右上のメニューボタンをタップしてください。

図 4.2.7　証明書詳細

5. 図 4.2.8 が表示されます。<通知設定>をタップしてください。

図 4.2.8　証明書メニュー

6. 図 4.2.9 が表示されます。必要に応じて期限切れ通知、および期限切れ間近通知の設定を変更してください。

図 4.2.9　通知設定

4.2.2.2　PC

1. 起動画面上部にある歯車アイコンをクリックしてください。
2. 図 4.2.10 が表示されます。通知設定したい証明書の<…>をクリックしてください。

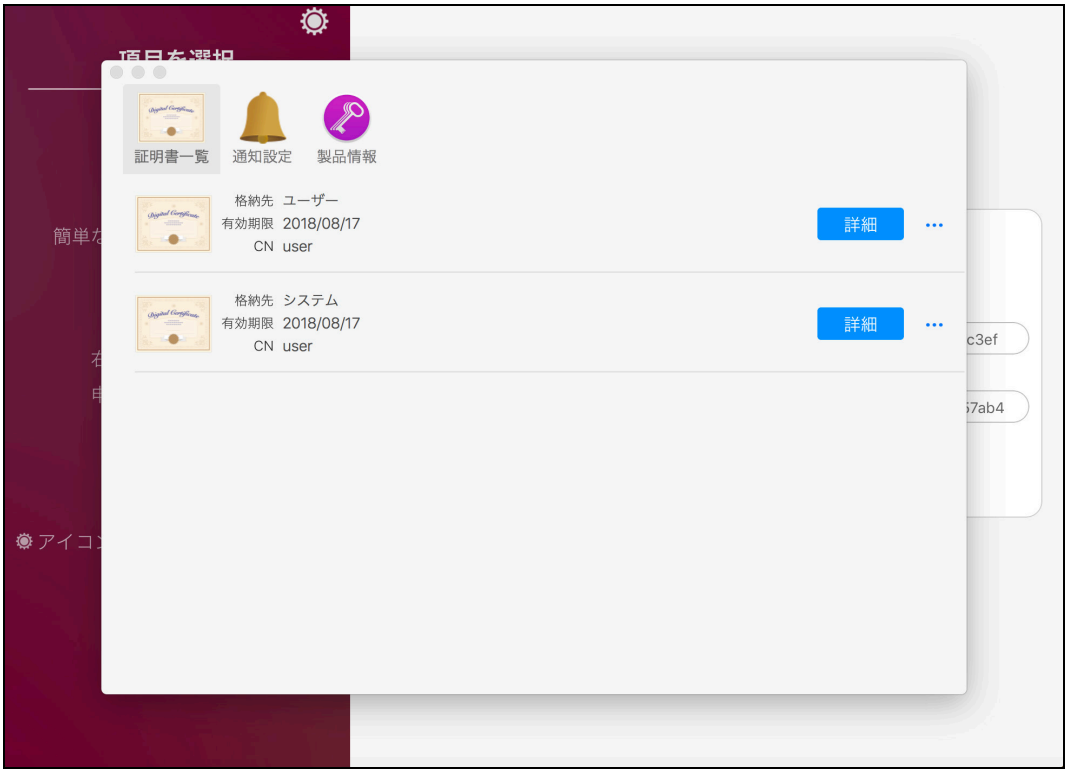

図 4.2.10　設定メニュー

3. 図 4.2.11 が表示されます。<通知設定>をクリックしてください。

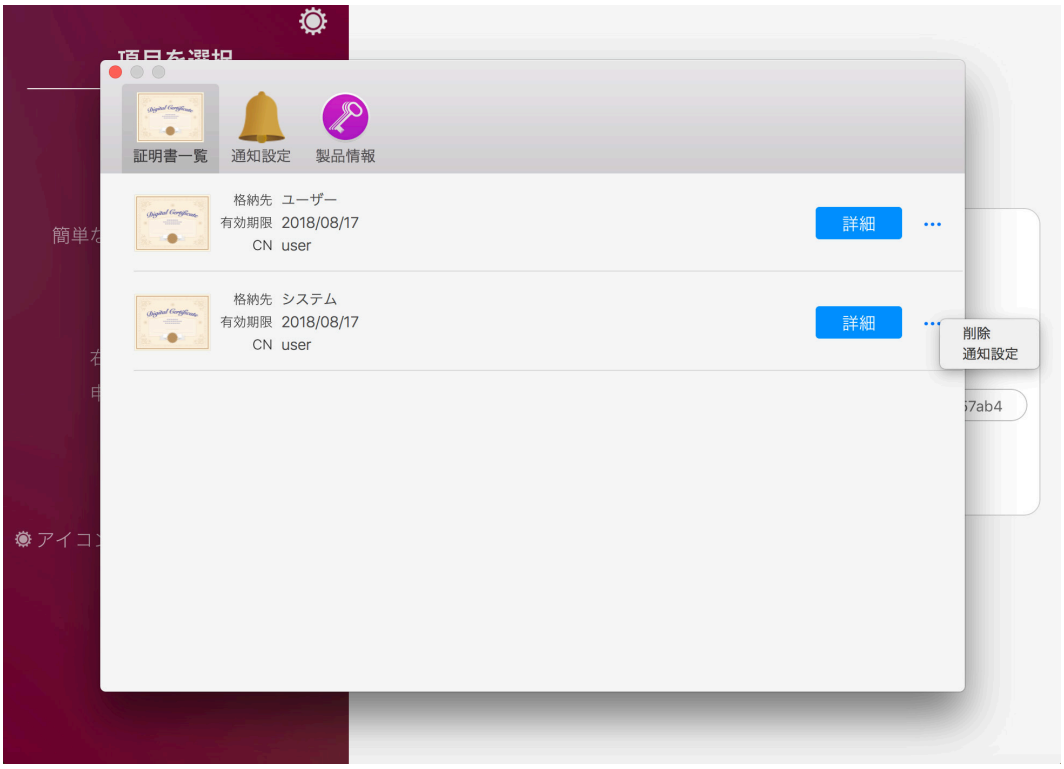

図 4.2.11　証明書一覧

4. 図 4.2.12 が表示されます。必要に応じて期限切れ通知、および期限切れ間近通知の設定を変更してください。証明書単位に通知設定が変更されます。

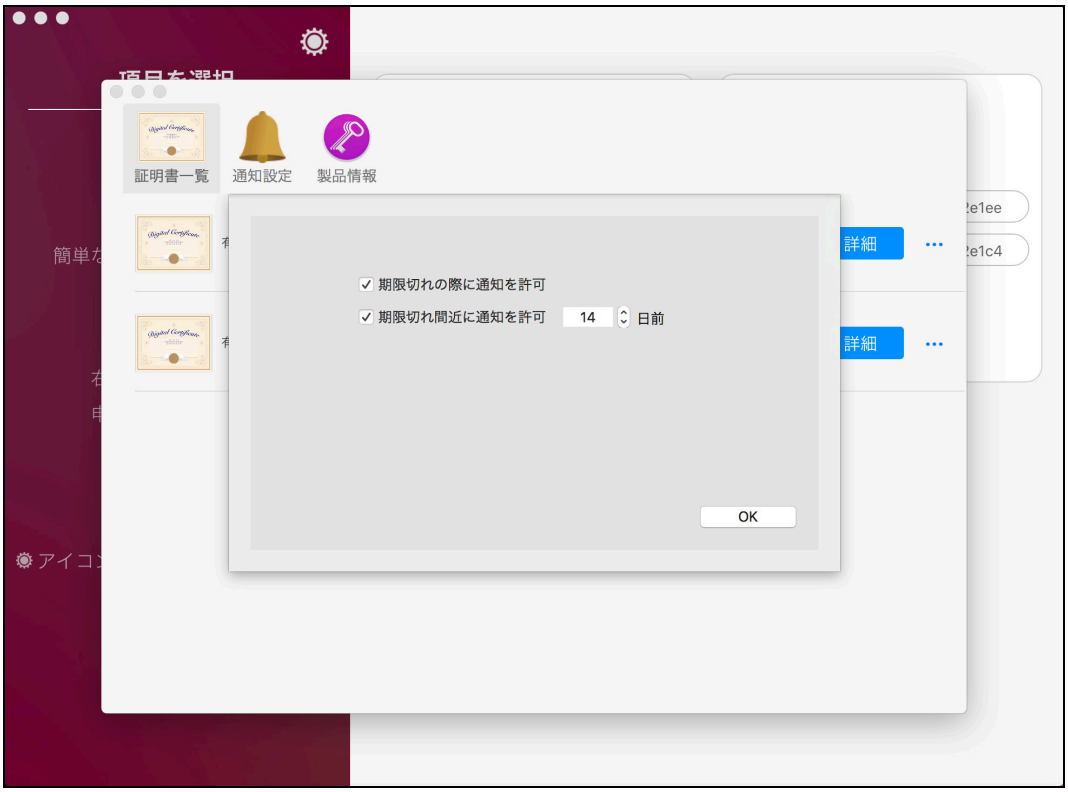

図 4.2.12　通知設定

- **Windows 版の場合、有効期限切れ間近のメッセージは、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、または通知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、申請や利用開始手続き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、申請や利用開始手続きに失敗します。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

☞ FAQ No:9698「最新のiOS/Androidバージョンに対応していますか？」

https://faq1.soliton.co.jp/faq/show/9698

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. 起動画面上部にある歯車アイコンをクリックしてください。
2. [製品情報]をクリックしてください。
3. <診断情報の送信>または<診断情報>をクリックしてください。

付録

付録 1　iOS/iPadOS

iOS 版 KeyManager 固有の動作について説明します。

ここでは iOS14 のスマートフォンを例に説明します。

1-1　CA 証明書取得手順（iOS）

1. ブラウザ（MobileSafari）を起動し、下記 URL へアクセスすると図 A1.1 が表示されます。

   http://<接続先の FQDN>

図 1.1　EPS-ap Web サービスページ

接続先が Soliton ID Manager の場合は図 A1.2 が表示されます。<証明書ダウンロード>から構成プロファイル（CA 証明書プロファイル）をダウンロードしてください。

図 A1.2　プロファイル発行サービス

2. <STEP1　CA 証明書ダウンロード>をタップすると構成プロファイル（CA 証明書プロファイル）のダウンロードに関するダイアログが表示されます。<許可>をタップしてください。

図 A1.3　構成プロファイルダウンロード

3. ダウンロードメッセージが表示されます。<閉じる>をタップしてください。

図 A1.4　ダウンロードメッセージ

4. [設定]App の[プロファイルがダウンロードされました]をタップすると、構成プロファイルのインストール画面が表示されます。<インストール>をタップしてください。

図 A1.5　プロファイルインストール

5. 警告画面が表示されます。内容を確認し<インストール>をタップしてください。

図 A1.6　警告

6. 図 A1.6 が表示されます。<インストール>をタップしてください。

図 A1.7　警告-インストール

7. インストールが完了したら<完了>をタップしてください。

図 A1.8　インストール完了

ルート CA 証明書インストール後に、[設定]-[一般]-[情報]-[証明書信頼設定]でインストールしたルート CA 証明書を有効にしてください。

1-2　iTunes から証明書をインストール

iTunes のファイル共有機能を使用して証明書のインストールを行うことができます。

以下の拡張子の証明書ファイルが対象です。

- .p12（.P12）
- .pfx（.PFX）

証明書のインストールは、以下の手順で行ってください。

1. iOS をコンピューターに接続し、iTunes を起動してください。
2. 接続している iOS デバイスの[ファイル共有]を選択してください。
3. [ファイル共有]セクションの[App]で「KeyManager」を選択してください。
4. 「KeyManager の書類」で<ファイルを追加>をクリックし、インストールする証明書ファイルを選択してください。
5. iOS で KeyManager を起動し、起動画面上部の歯車アイコンをタップしてください。
6. 図 A1.9 が表示されます。<iTunes から追加した証明書>をタップしてください。

図 A1.9　設定メニュー

7. iTunes から追加した証明書ファイルが表示されます。インストールする証明書をタップしてください。画面右上の<編集>をタップすると、iTunes からコピーした証明書ファイルを手動で削除することができます。

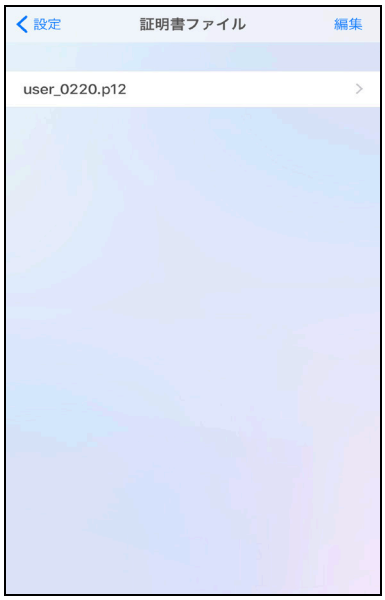

図 A1.10　証明書ファイル

8. パスワード入力画面が表示されます。証明書に設定されているパスワードを入力し、画面右上の<インストール>をタップしてください。

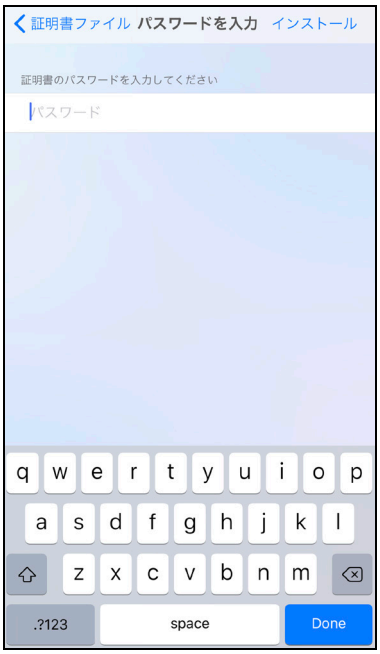

図 A1.11　パスワード入力

9. 証明書がインストールされます。証明書一覧にインストールした証明書が表示されます。

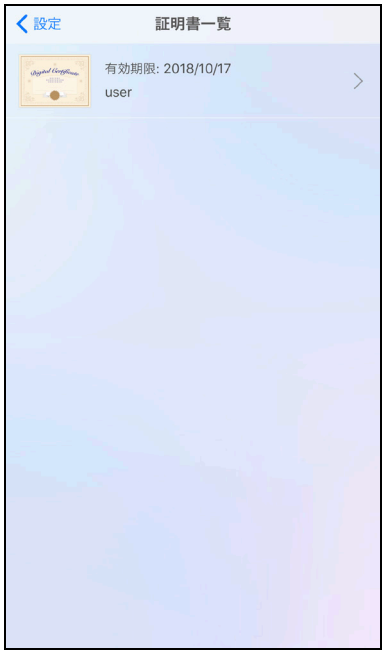

図 A1.12　証明書一覧

1-3　メールから証明書をインストール

メールに添付された証明書のインストールを行うことができます。

以下の拡張子の証明書ファイルが対象です。

- .p12（.P12）
- .pfx（.PFX）
- .pkcs12（.PKCS12）

証明書のインストールは、以下の手順で行ってください。

1. iOS でメーラーを起動し、証明書が添付されたメールを開いてください。
2. 図 A1.13 が表示されます。インストールする証明書ファイルをロングタップしてください。

A1.13　証明書ファイル添付メール

3. 共有メニューが表示されます。<KeyManager にコピー>をタップしてください。

A1.14　共有メニュー

共有メニューに<KeyManager にコピー>がない場合、<その他>からアクティビティリストを表示し、「KeyManager にコピー」を有効にしてください。

4. 図 A1.15 が表示されます。<保存>をタップしてください。

図 A1.15　証明書をコピー

5. KeyManager を起動し、起動画面上部の歯車アイコンをタップしてください。
6. 図 A1.16 が表示されます。<iTunes から追加した証明書>をタップしてください。

図 A1.16　設定メニュー

7. コピーした証明書ファイルが表示されます。インストールする証明書をタップしてください。

図 A1.17　証明書ファイル

8. パスワード入力画面が表示されます。証明書に設定されているパスワードを入力し、画面右上の<インストール>をタップしてください。

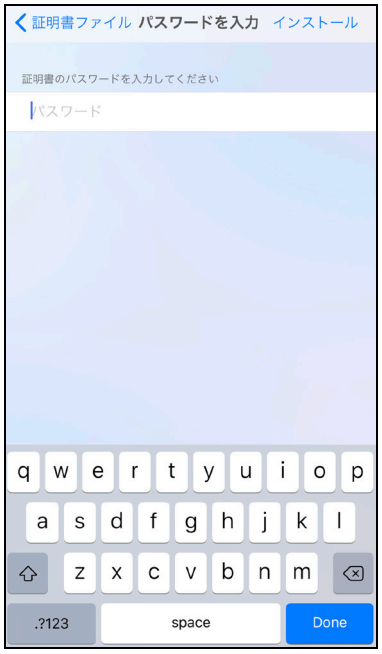

図 A1.18　パスワード入力

9. 証明書がインストールされます。証明書一覧にインストールした証明書が表示されます。

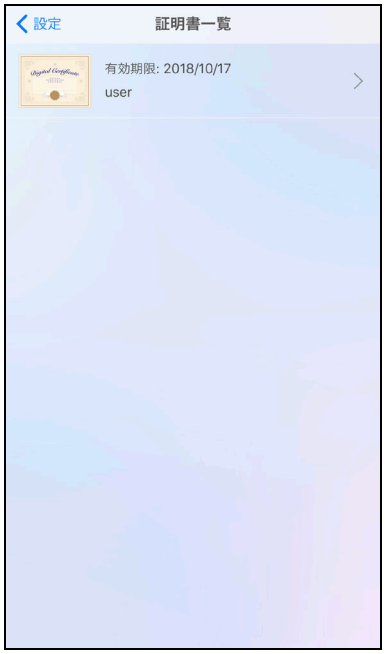

図 A1.19　証明書一覧

1-4　デバイス名を送信する

利用開始手続きを行うと[設定]アプリ-[一般]-[名前]に登録されている値をサーバーに送信します。

付録 2　Android

Android 版 KeyManager 固有の動作について説明します。

特に記載がない限り、ここでは Android 11 のスマートフォンを例に説明します。

2-1　CA 証明書取得手順（Android 10 以前）

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ます。
2. 画面ロックがかかっている場合、画面ロック解除に必要なコードの入力が求められます。適切なコードを入力してください。
3. 証明書名の指定画面が表示されます。「認証情報の使用」に「VPN とアプリ」を選択し、<OK>をタップしてください。

図 A2.1　証明書名指定画面

端末により「証明書名」が自動入力されない場合があります。

4. 画面ロックがかかっていない場合、画面ロックの設定を求められます。画面の指示に従い、画面ロックを設定してください。画面ロックが設定済みの場合は手順 5 に進んでください。

5. CA 証明書のインストールに成功すると図 A2.2 が表示されます。

図 A2.2　証明書の格納先

2-2　CA 証明書取得手順（Android 11 以降）

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、ダウンロードフォルダーに保存します。

図 A2.3　CA 証明書インストール

図 A2.3 の場合、「cacert1_20200925154743.cer」というファイル名で CA 証明書をダウンロードしています。メッセージ内容を確認し<OK>をタップしてください。

2. [設定]アプリに遷移します。[設定]アプリの[セキュリティ]-[暗号化と認証情報]-[証明書のインストール]-[CA 証明書]を選択してください。

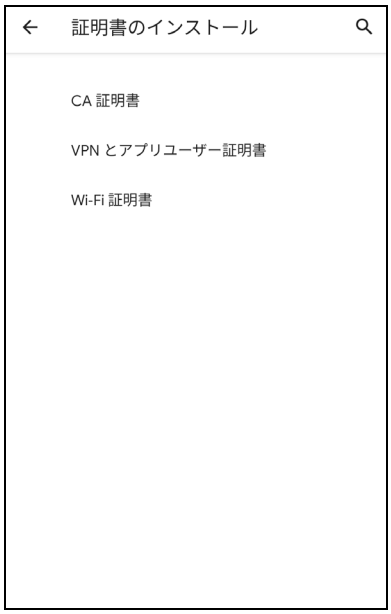

図 A2.4　証明書のインストール

3. CA 証明書インストールに関するメッセージが表示されます。内容を確認の上、<インストールする>をタップしてください。

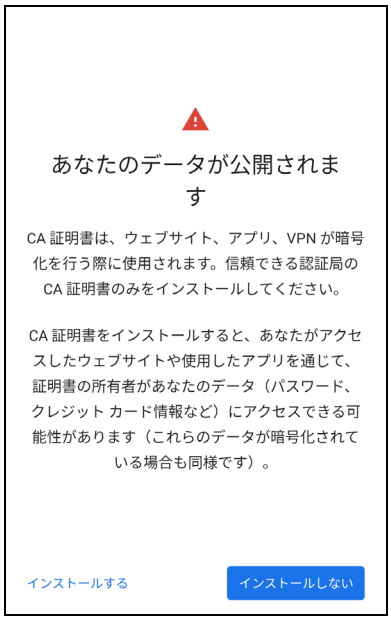

図 A2.5　CA 証明書インストールに関するメッセージ

4. 画面ロックがかかっている場合、画面ロック解除に必要なコードの入力が求められます。適切なコードを入力してください。

5. ダウンロードした CA 証明書を選択し、CA 証明書をインストールしてください。

図 A2.6　証明書選択

❑ Wi-Fi 接続時にサーバー証明書を検証する

Wi-Fi 接続時にサーバー証明書を検証する場合は、以下の手順でダウンロードした CA 証明書を「Wi-Fi 証明書」ストアにインストールしてください。

1. [設定]アプリの[セキュリティ]-[暗号化と認証情報]-[証明書のインストール]-[Wi-Fi 証明書]を選択してください。

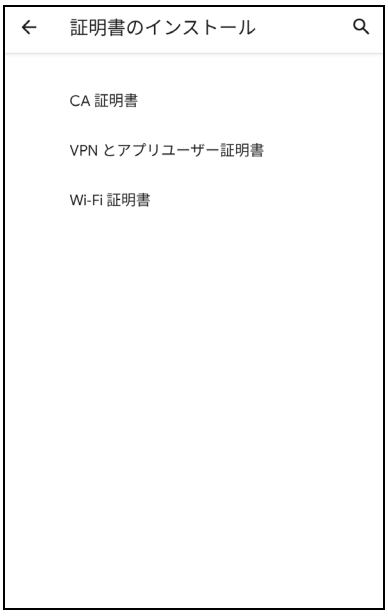

図 A2.7　証明書のインストール

2. ダウンロードした CA 証明書を選択してください。

図 A2.8　証明書選択

3. 図 A2.7 が表示されます。証明書の名前を指定して<OK>をタップしてください。

図 A2.9　CA 証明書名の指定（Wi-Fi 証明書）

2-3　利用開始手続き中の証明書格納先（Android 10 以前）

利用開始手続き中に表示される証明書名の指定画面では、証明書の利用目的ごとに格納先（「認証情報の使用」）を指定する必要があります。

「認証情報の使用」は申請した際に選択した「証明書の格納先」（図 3.3.4　証明書の格納先）と同じ設定を指定してください。

❑ VPN とアプリ

1. 利用開始手続きを開始すると図 A2.10 が表示されます。「認証情報の使用」に「VPN とアプリ」が選択されていることを確認し<OK>をタップしてください。

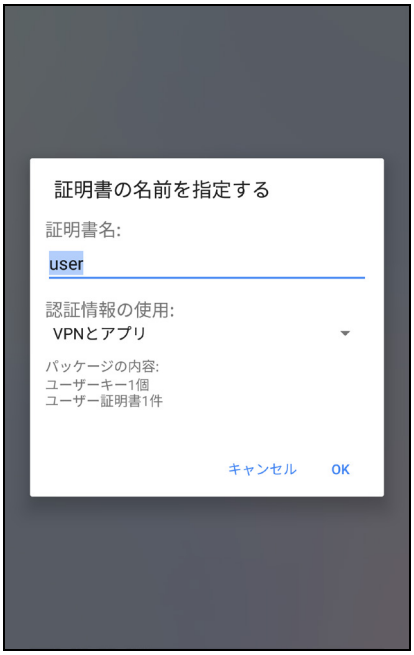

図 A2.10　認証情報の使用-VPN とアプリ

❑ Wi-Fi

1. 利用開始手続きを開始すると図 A2.11 が表示されます。「認証情報の使用」に「Wi-Fi」を選択し<OK>をタップしてください。

図 A2.11　認証情報の使用-Wi-Fi（CA）

2. 図 A2.12 が表示されます。「認証情報の使用」に「Wi-Fi」を選択し<OK>をタップしてください。

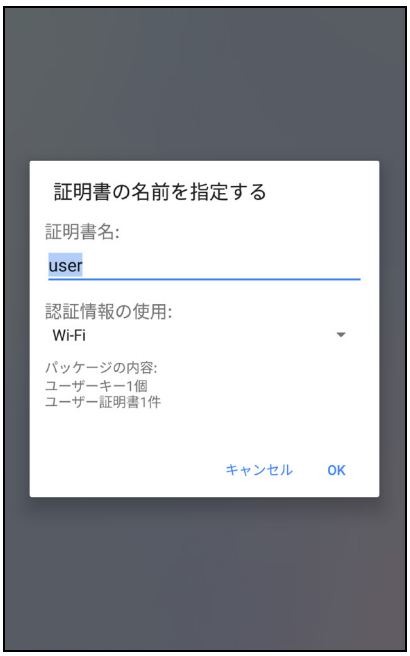

図 A2.12　認証情報の使用-Wi-Fi（ユーザー）

端末により「証明書名」が自動入力されない場合があります。

2-4　利用開始手続き中の証明書格納先（Android 11 以降）

利用開始手続き中に表示される「証明書の種類の選択」画面では、証明書の利用目的ごとに格納先を指定する必要があります。

「証明書の種類」は申請した際に選択した「証明書の格納先」（図 3.3.4　証明書の格納先）と同じ設定を指定してください。

❑ VPN とアプリ

1. 利用開始手続きを開始すると図 A2.13 が表示されます。「証明書の種類」に「VPN とアプリユーザー証明書」が選択されていることを確認し<OK>をタップしてください。

図 A2.13　証明書の種類-VPN とアプリユーザー証明書

2. 図 A2.14 が表示されます。証明書の名前を指定して<OK>をタップしてください。

図 A2.14　証明書名の指定（VPN とアプリユーザー証明書）

❑ Wi-Fi

3. 利用開始手続きを開始すると図 A2.15 が表示されます。「証明書の種類」に「Wi-Fi 証明書」を選択し<OK>をタップしてください。

図 A2.15　証明書の種類-Wi-Fi 証明書

4. 図 A2.16 が表示されます。証明書の名前を指定して<OK>をタップしてください。

図 A2.16　証明書名の指定（Wi-Fi 証明書）

端末により「証明書名」が自動入力されない場合があります。

2-5　MDM プロファイルのインストール

1. MDM の対象デバイスとして構成する場合、利用開始手続き中に MDM 構成に必要なプロファイルが配布され、図 A2.17 が表示されます。<この端末管理アプリを有効にする>をタップしてください。

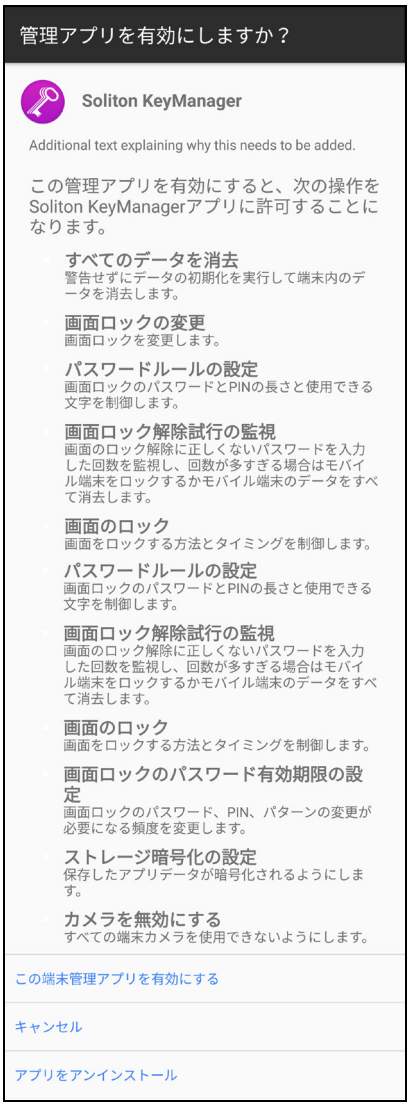

図 A2.17　管理アプリの有効化

2-6　MDM プロファイルの削除

1. MDM プロファイルをインストールすると設定メニューに[MDM]-[プロファイル]が追加されます。<プロファイル>をタップしてください。

図 A2.18　設定メニュー

2. 図 A2.19 が表示されます。<削除>をタップしてください。

図 A2.19　プロファイル

3. A2.20 が表示されます。<削除>をタップしてください。

図 A2.20　削除ダイアログ

4. MDM プロファイルが削除され、設定メニューから MDM に関連するメニューが削除されます。

図 A2.21　設定メニュー

2-7　デバイス名を送信する

利用開始手続きを行うと[設定]アプリ-[デバイス情報]-[デバイス名]に登録されている値をサーバーに送信します。

付録 3　Mac

Mac 版 KeyManager 固有の動作について説明します。

ここでは macOS Catalina の PC を例に説明します。

3-1　CA 証明書取得手順（Mac）

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、ブラウザ（Safari）を起動し、下記 URL へ自動的にアクセスします。

   https://<接続先 FQDN>/cacert.php

2. 接続先が信頼されていない場合、ブラウザが警告メッセージを表示します。[詳細を表示]-[この Web サイトを閲覧]-<Web サイトを閲覧>をタップし構成プロファイル（CA 証明書プロファイル）をダウンロードしてください。

   ※接続先が信頼されている場合、警告メッセージは表示されません。手順 3 に進んでください。

図 A3.1　警告メッセージ（Safari）

3. ファイルのダウンロードに関するダイアログが表示されます。<許可>をタップしてください。

※当該サイトからのファイルダウンロード許可をすでに行っている場合、確認ダイアログは表示されません。手順 4 へ進んでください。

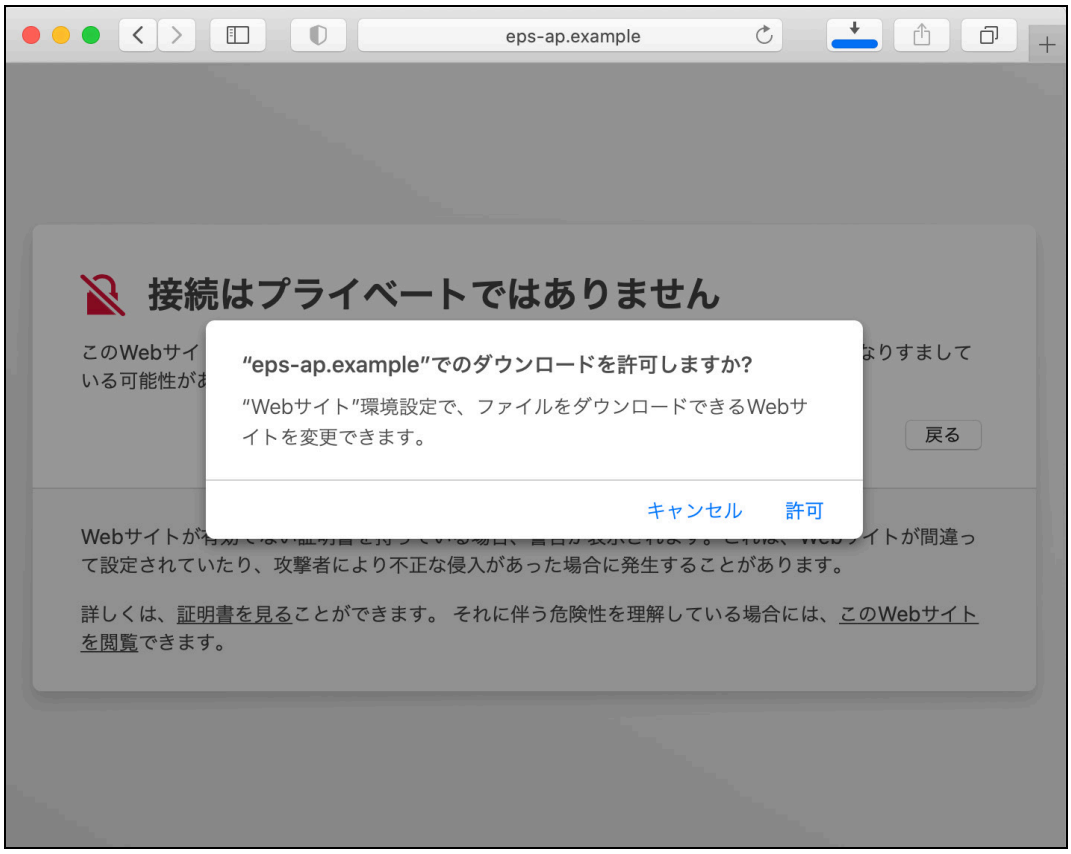

図 A3.2　ファイルダウンロードダイアログ

4. 別ウィンドウで図 A3.3 が表示されます。<続ける>をクリックしてください。

図 A3.3　インストール確認ダイアログ

5. 図 A3.4 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 A3.4　プロファイルインストール

6. CA 証明書のインストールが完了すると、図 A3.5 が表示されます。

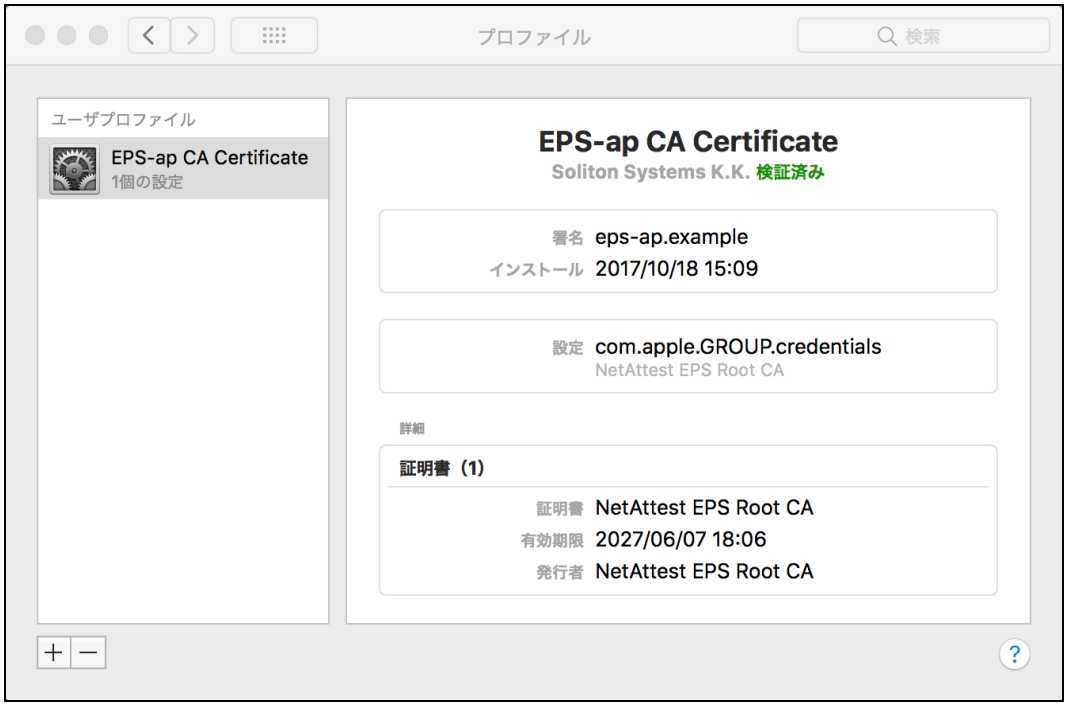

図 A3.5　インストール完了

3-2　コンピューター名を送信する

利用開始手続きを行うと[システム環境設定]-[共有]-「コンピューター名」に登録されている値をサーバーに送信します。

付録 4　Windows

Windows 版 KeyManager 固有の動作について説明します。

ここでは Windows10 の PC を例に説明します。

4-1　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。

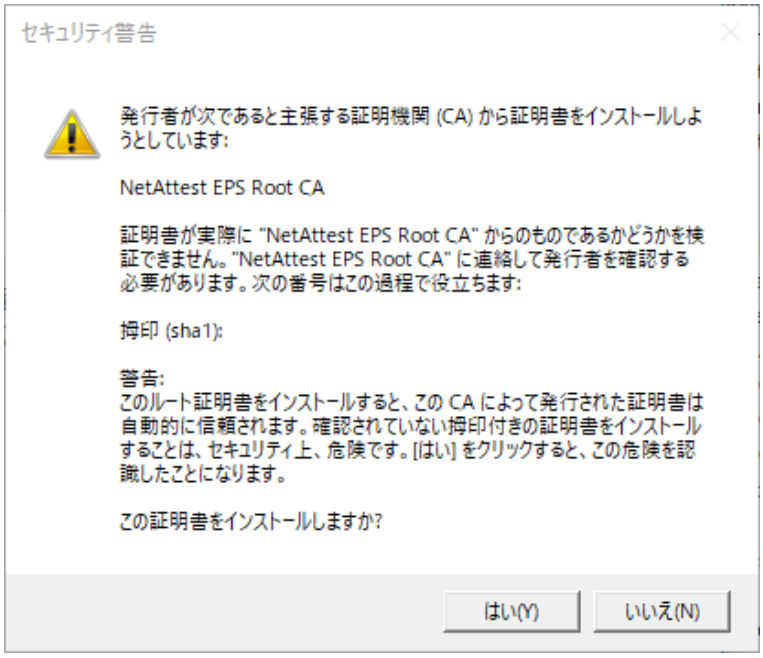

図 A4.1　セキュリティ警告

2. CA 証明書をインストールするとホスト名・HTTPS ポート番号入力画面に戻ります。

4-2　Mac アドレスの確認

利用開始手続き中、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. 起動画面上部にある歯車アイコンをタップしてください。
2. 図 A4.2 が表示されます。<詳細情報>をクリックしてください。

図 A4.2　設定

3. 図 A4.3 が表示され、Mac アドレスを確認することができます。

図 A4.3　詳細情報

4-3　プロキシサーバーを経由しない

Window 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. 起動画面上部にある歯車アイコンをタップしてください。
2. 図 A4.4 が表示されます。<詳細情報>をクリックしてください。

図 A4.4　設定

3. 図 A4.5 が表示されます。「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 A4.5　詳細情報

4-4　申請理由の初期値

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]/[ユーザーID（ドメイン名付き）]/[Mac アドレス]/[「user」or「comp」]:
```

選択した証明書種類がユーザー証明書の場合「user」、コンピューター証明書の場合「comp」が付け足されます。

4-5　Legacy APID の確認

Windows 版 KeyManager は V2.0.4 にて APID 生成ロジックを変更しました。ここでは V2.0.3 以前の旧生成ロジック（Legacy APID）の APID を確認する手順を記載します。

- **V2.0.3 以前からアップデートしている場合、APID は変更されずに Legacy APID を継続して利用します。**
- **Legacy APID が利用開始手続き中のデバイスチェック等で利用されることはありません。**

❑ UI で確認

1. 起動画面で<APID>をクリックしてください。
2. 図 A4.6 が表示されます。右ペインの背景を 10 秒以内に 7 回クリックしてください。

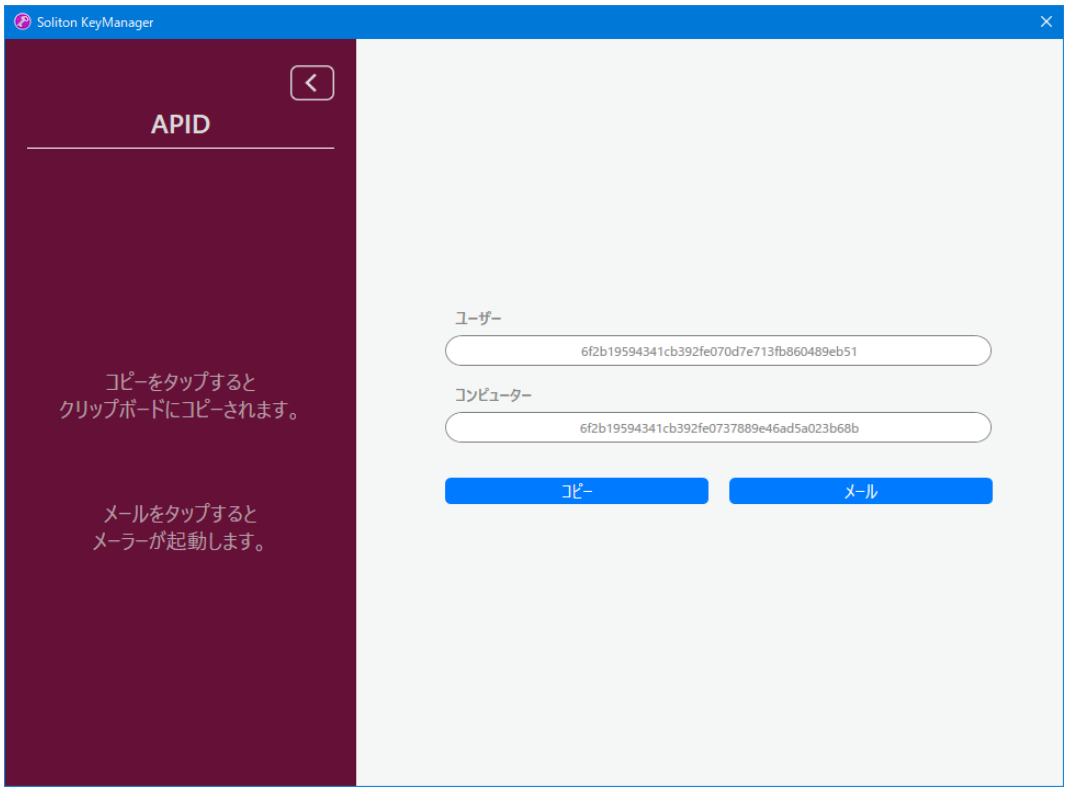

図 A4.6　APID

3. 図 A4.7 が表示され、Legacy APID が確認できます。

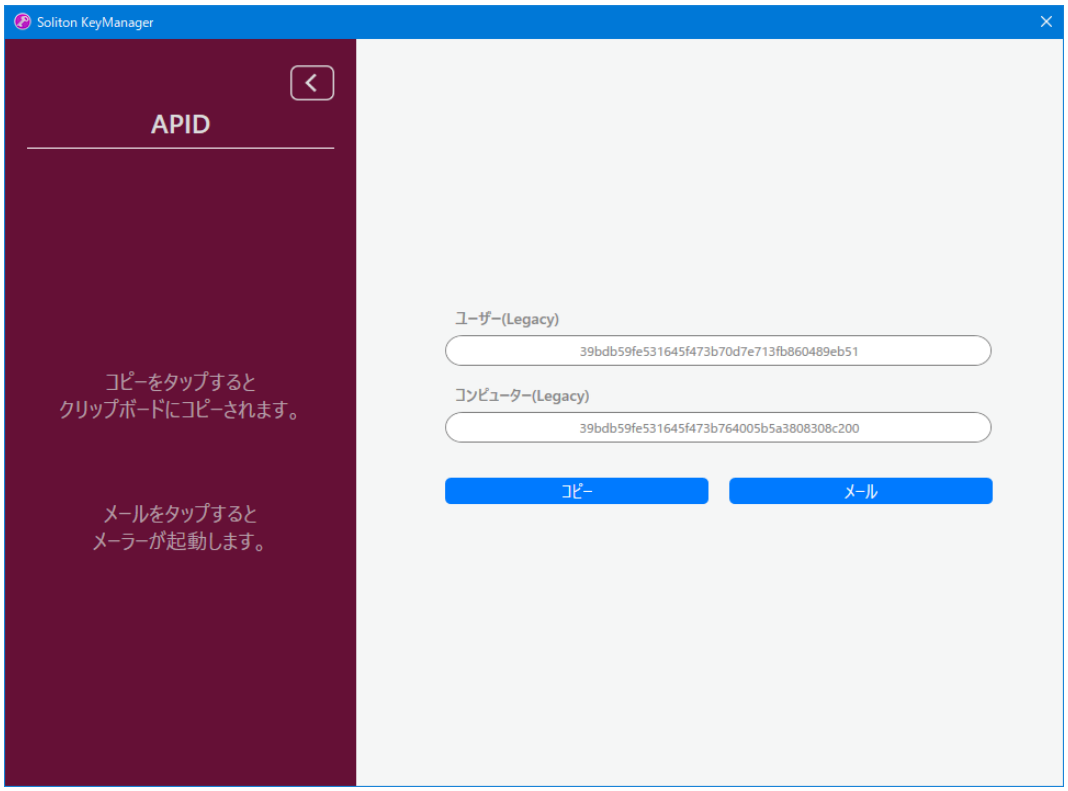

図 A4.7　APID(Legacy)

❑ クリップボードにコピー

[APID]画面の<コピー>をクリックすると、クリップボードに以下の内容をコピーします。

```
[APID]
APID(ユーザー): 6f2b19594341cb392fe070d7e713fb860489eb51
APID(コンピューター): 6f2b19594341cb392fe0737889e46ad5a023b68b

[APID(Legacy)]
APID(ユーザー): 39bdb59fe531645f473b70d7e713fb860489eb51
APID(コンピューター): 39bdb59fe531645f473b764005b5a3808308c200

[Information]
コンピューター名: DESKTOP-SAMPLE
ログインユーザーID: DESKTOP-SAMPLE¥USER
MAC アドレス: EC:8E:B5:77:7D:2B
```

❑ メールにコピー

[APID]画面の<メール>をクリックすると、以下内容のメールを作成します。

```
件名：Soliton KeyManager APID

本文：
[APID]
APID(ユーザー)： 6f2b19594341cb392fe070d7e713fb860489eb51
APID(コンピューター)： 6f2b19594341cb392fe0737889e46ad5a023b68b

[APID(Legacy)]
APID(ユーザー)： 39bdb59fe531645f473b70d7e713fb860489eb51
APID(コンピューター)： 39bdb59fe531645f473b764005b5a3808308c200

[Information]
コンピューター名： DESKTOP-SAMPLE
ログインユーザーID： DESKTOP-SAMPLE¥USER
MAC アドレス： EC:8E:B5:77:7D:2B
```

4-6　コンピューター名を送信する

利用開始手続きを行うとコンピューター名をサーバーに送信します。

4-7　ドメイン情報を送信する

Windows 版 KeyManager は、利用ユーザーの参加しているドメイン名を利用開始手続き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取得が行えません。

4-8　コマンドラインによる証明書インストール

コマンドラインにより KeyManager を実行して NetAttest EPS-ap に接続し、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。

❑ 対応環境

NetAttest EPS-ap 申請モード(自動承認)

❑ 対象バージョン

Windows 版 KeyManager　V2.0.11 以降

- **本機能は接続する NetAttest EPS-ap が「申請モード」でかつ「自動承認」が「有効」の場合にのみ利用できます。**
- **※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。**

❑ 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 4.8.1　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 NetAttest EPS-ap のホスト名または IP アドレスを指定してください。

オプション	説明
/hp <port>	接続する NetAttest EPS-ap のポート番号を指定してください。 指定しない場合は NetAttest EPS-ap の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。
/new	強制的に「新規」で申請します。 指定しない場合は、KeyManager でまだ証明書を取得していない場合は「新規」で申請します。既に同じ格納先に証明書がインストールされている場合は「更新」（上書き）します。
/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。 NetAttest EPS-ap と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が NetAttest EPS-ap の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」の設定に従います。
/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 EPS-ap 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 4.8.2　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 4.8.3　結果ファイル

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行えています。

➢ 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 4.8.4 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 Faild：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

❑ 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

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インストールするケース。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]

利用者アカウント：user01

管理者アカウント：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。申請には共通の管理者アカウントを使用する。

```
"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 /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：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

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インストールするケース。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]

クライアント PC：SALES-PC

利用者アカウント：user01

管理者アカウント：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。申請には共通の管理者アカウントを使用する。

```
"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 /p password /cn
```

(2) 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。

(3) 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。

(4) 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。

制約事項

- **本機能は接続する NetAttest EPS-ap が「申請モード」でかつ「自動承認」が「有効」の場合にのみ利用できます。**
- **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。
- **KeyManager はコマンドラインで指定された内容でそのまま実行します。そのためコマンドラインが実行されるたびに証明書が取得（更新）されますのでお気をつけください。**
- **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。**

Soliton KeyManager

Soliton KeyManager V2　説明書

2017 年 10 月 28 日　　第 1 版

2024 年 2 月 5 日　　第 11 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/

Soliton®