クライアント証明書利用説明書
外部からのWebメール利用(多要素認証)準備

農林水産研究情報総合センター

Ver.1.6 2020/01/21

目次

1. はじめに 1
   1.1. 前提条件 1
2. クライアント証明書インストールまでの流れ 2
   2.1. Soliton KeyManagerインストール 3
3. Windows編 4
   3.1. Soliton KeyManager インストール 4
   3.2. APID確認・申請 4
      3.2.1. APIDの確認 4
      3.2.2. APIDの申請 4
   3.3. クライアント証明書インストール 5
      3.3.1. 認証局証明書(CA)インストール 5
      3.3.2. クライアント証明書取得申請 7
      3.3.3. クライアント証明書インストール確認 8
4. macOS編 9
   4.1. Soliton KeyManager インストール 9
   4.2. APID確認・申請 9
      4.2.1. APIDの申請 9
   4.3. クライアント証明書インストール 10
      4.3.1. 認証局証明書(CA)インストール 10
      4.3.2. クライアント証明書取得申請 12
      4.3.3. クライアント証明書インストール確認 13
5. Android編 14
   5.1. Soliton KeyManager インストール 14
   5.2. Android 6系、7系 14
      5.2.1. APID確認・申請 14
      5.2.2. クライアント証明書インストール 15
   5.3. Android 8系、9系、10系 18
      5.3.1. APID確認・申請 18
      5.3.2. クライアント証明書インストール 19
6. iOS編 25
   6.1. UDID確認・申請 25
      6.1.1. iTunes で確認 25
      6.1.2. Windowsデバイスマネージャ(iPhone XS/XR/11/11pro) 26
      6.1.3. Macシステムレポート(iPhone XS/XR/11/11pro) 27
      6.1.4. UDIDの申請 28
   6.2. クライアント証明書インストール 28
      6.2.1. 認証局証明書(CA)インストール 28
      6.2.2. 証明書信頼設定の有効化 32
      6.2.3. クライアント証明書取得申請 32
      6.2.4. クライアント証明書インストール確認 34
7. 証明書の更新 36
8. 証明書の削除 37
   8.1. クライアント証明書の削除(Windows) 37
   8.2. クライアント証明書の削除(macOS) 38
   8.3. クライアント証明書の削除(Android) 39

8.4. クライアント証明書の削除(iOS) 40
9. 通知設定 41
9.1. クライアント証明書の有効期限の通知機能(Windows) 41
9.2. クライアント証明書の有効期限の通知機能(macOS) 42
9.3. クライアント証明書の有効期限の通知機能(Android) 42
9.4. クライアント証明書の有効期限の通知機能(iOS) 44

1. はじめに

本書の目的

本手順書では、農林水産研究情報総合センターのクライアント証明書発行基盤を利用しクライアント証明書をインストールするにあたって、最低限必要となる項目について記載しております。本手順書に記載されていない内容等については、製品のマニュアルを参考にしていただくか、農林水産研究情報総合センターにお問い合わせください。

1.1. 前提条件

クライアント証明書をインストールする際に利用するアプリケーションと対応OSは下記のとおりです。

- Soliton KeyManager（Windows版）
  - 動作環境: 「別紙：Soliton KeyManager V2 説明書 第5版」のP9を参照してください。
  - ダウンロード先: https://www.soliton.co.jp/support/soliton/hardware/skm/
- Soliton KeyManager（Mac版）
  - 動作環境: 「別紙：Soliton KeyManager V2 説明書 第5版」のP9を参照してください。
  - ダウンロード先: https://www.soliton.co.jp/support/soliton/hardware/skm/
- Soliton KeyManager（Android版）
  - 動作環境: 「別紙：Soliton KeyManager V2 説明書 第5版」のP9を参照してください。
  - ダウンロード先: https://www.soliton.co.jp/support/soliton/hardware/skm/
    アプリケーションはGoogle Playよりダウンロードしてください。
- Mobile Safari（iOS版）
  - 動作環境: 「本書：6.2. クライアント証明書インストール」を参照してください。

本書では説明にあたって、KeyManager・Safariの名称を用います。 また、クライアント証明書をインストールする装置（パソコン、スマートデバイス等）を総称して、「端末」と表記します。 手順を進めるにあたって以下を確認してください。

- 対象端末の電源が投入されていること
- 対象端末がネットワークに接続され、配布サーバ[1]にネットワーク経由でアクセス可能なこと



[1] 配布サーバ: クライアント証明書申請の際に接続するサーバ

2. クライアント証明書インストールまでの流れ

クライアント証明書のインストールにあたっては、利用者の端末OSの違いによって、手順が異なります。 下記はクライアント証明書インストールまでの全体フロー図となっています。

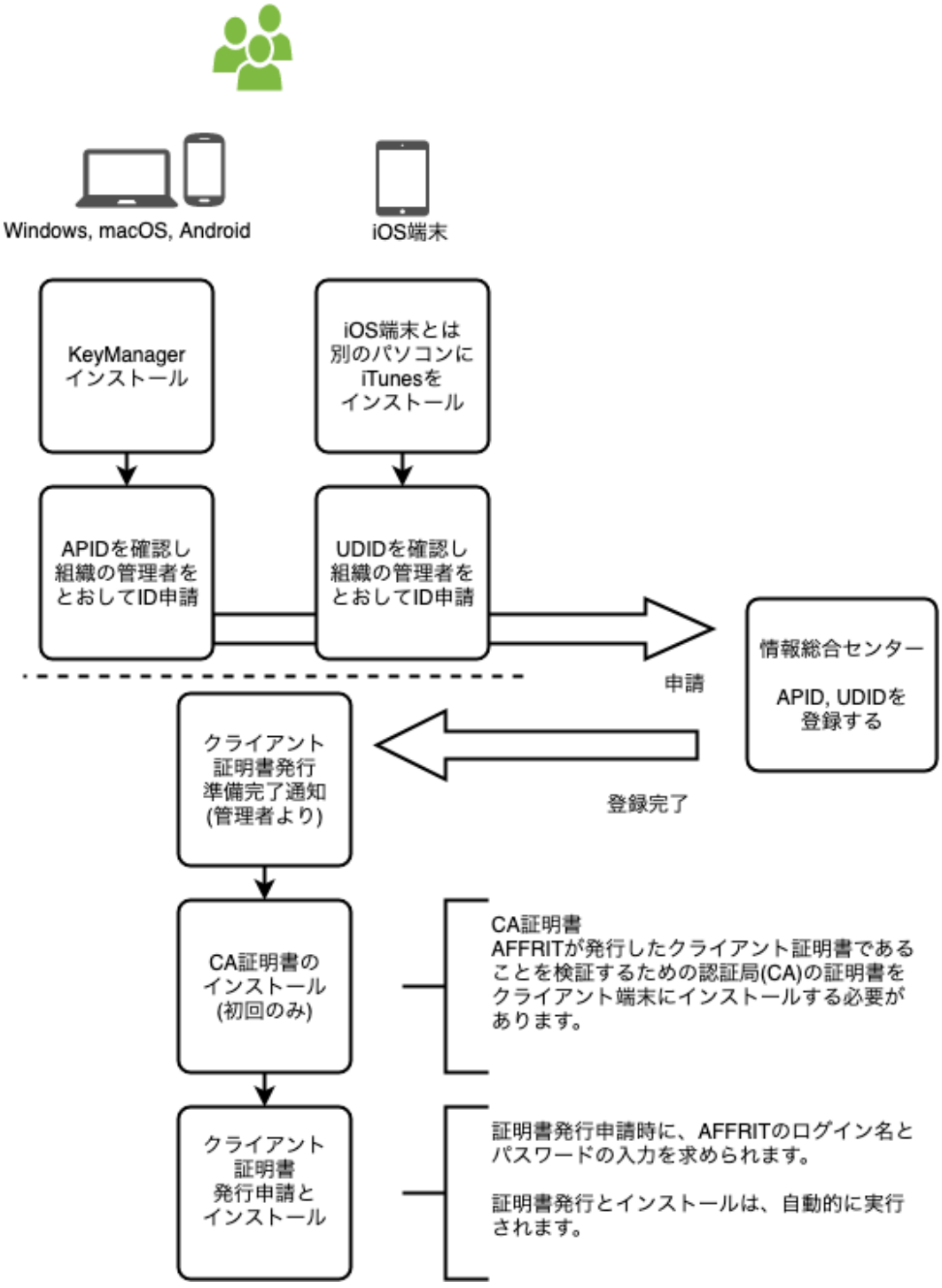


図 1. クライアント証明書インストールまでの流れ

大きく分けて2つの場合があります。

- 端末OSがWindows, macOS, Androidの場合
- 端末OSがiOSの場合

【事前準備】

端末へのアプリケーションのインストールとAPID/UDID申請を行います。
APID/UDID申請を実施しないとクライアント証明書発行申請ができませんので、ご注意ください。
APID及びUDIDは端末を一意に識別するためのIDであり、クライアント証明書発行基盤で利用します。
APIDはKeyManagerで確認でき、UDIDはiTunes上で確認できます。

【クライアント証明書インストール】

クライアント証明書の発行準備が整い次第、メールで通知されます。
利用者はKeyManagerまたはSafariを用いてクライアント証明書を取得し、インストールします。

2.1. Soliton KeyManagerインストール

クライアント証明書をインストールする端末へのKeyManager及びSafariのインストール作業は各利用者にて実施していただきます。手順に関しては下記に示すとおり、別紙を参照してください。

- Soliton KeyManager（Windows版）
  インストール手順「別紙：Soliton KeyManager V2 説明書 第5版」のP15-22を参照してください。
- Soliton KeyManager（Mac版）
  インストール手順「別紙：Soliton KeyManager V2 説明書 第5版」のP11-14を参照してください。
- Soliton KeyManager（Android版）
  インストール手順「別紙：Soliton KeyManager V2 説明書 第5版」のP10を参照してください。
- Mobile Safari
  本アプリケーションはiOS標準となっております。インストールされていない場合は、各利用者にて対応をお願いいたします。

Soliton KeyManagerのインストールの際の注意点

- アプリケーションは最新版のインストールが推奨です。既にSoliton KeyManagerがインストールされている場合は、旧バージョンをアンインストールしてから最新バージョンをインストールしてください。
- クライアント証明書発行基盤の利用開始後、アプリケーションの不具合等で再インストールが必要になった場合も同様に旧バージョンをアンインストールしてから最新バージョンをインストールしてください。

3. Windows編

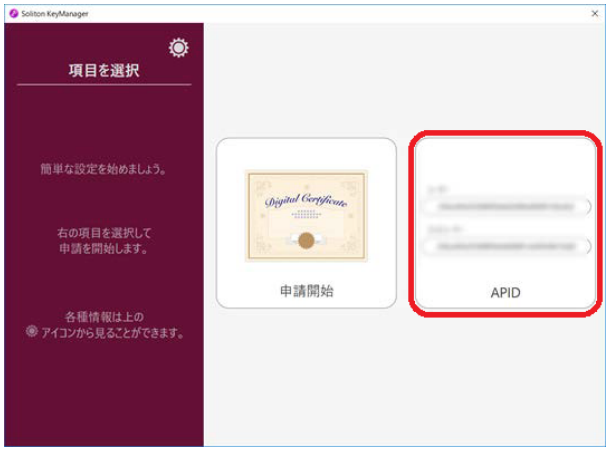
3.1. Soliton KeyManager インストール

- Soliton KeyManager（Windows版）
  - 動作環境: 「別紙：Soliton KeyManager V2 説明書 第5版」のP9を参照してください。
  - ダウンロード先: https://www.soliton.co.jp/support/soliton/hardware/skm/

3.2. APID確認・申請

3.2.1. APIDの確認

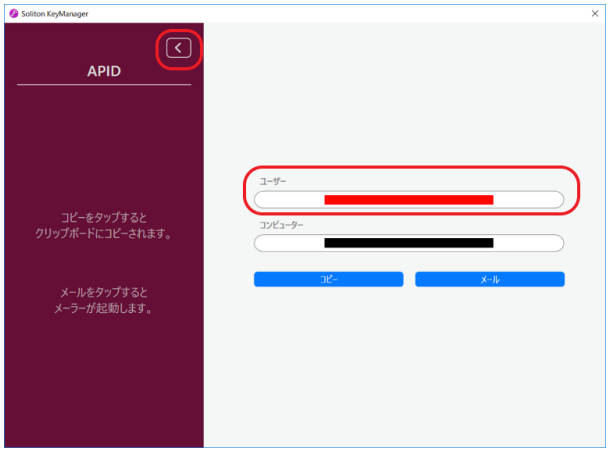
1 KeyManagerを起動すると、トップページが表示されます。
[APID]をクリックします。



2 [ユーザー]と表示されている右横の文字列が今回利用するAPIDです。

[コピー]をクリックして、メモや申請様式等にペーストします。

[閉じる]をクリックし、表示を 終了します。



3.2.2. APIDの申請

利用者は取得した「APID」と「情報総合センターの利用者ID」を管理者へ申請します。 この申請を実施しないとクライアント証明書発行申請ができませんので、ご注意ください。

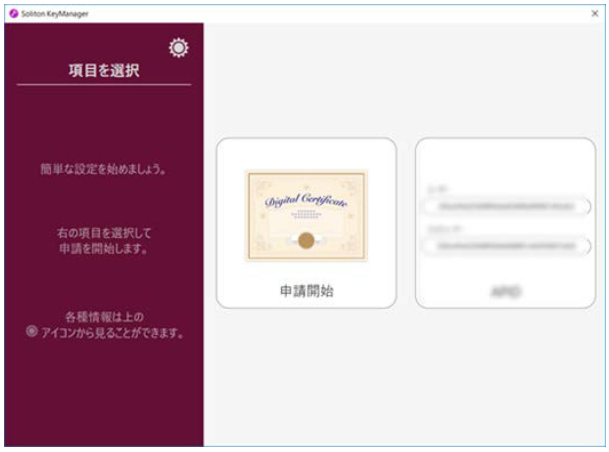
確認事項

- APIDを申請する際、英文字「A～Z」を小文字「a～z」に変更してください。

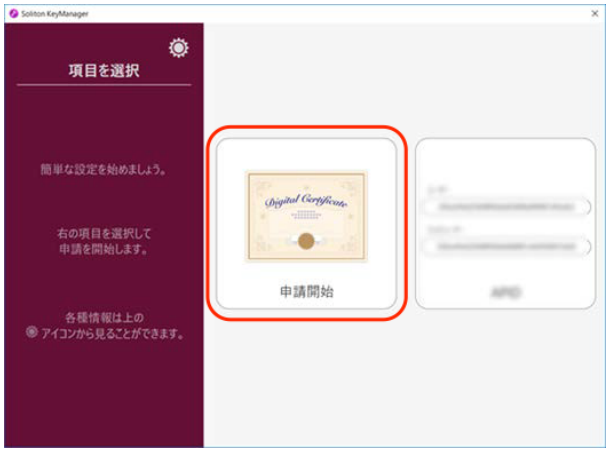
3.3. クライアント証明書インストール

3.3.1. 認証局証明書(CA)インストール

1　KeyManagerを起動すると、トップページが表示されます。

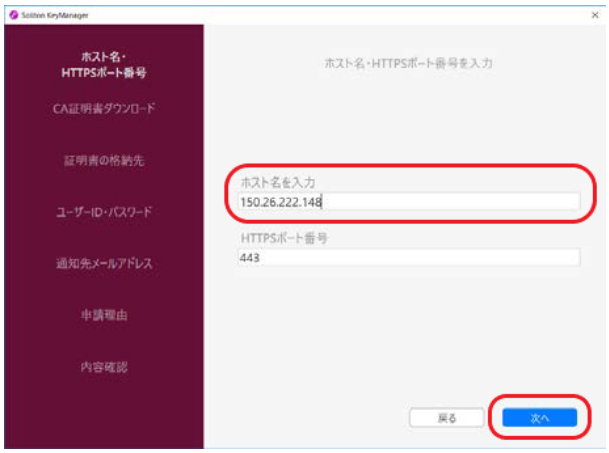


2　[申請開始]をクリックします。



3　[配布サーバ]への接続情報を入力します。
ホスト名を入力: 150.26.222.148
[HTTPSポート番号]:
([デフォルト値から変更なし)
443

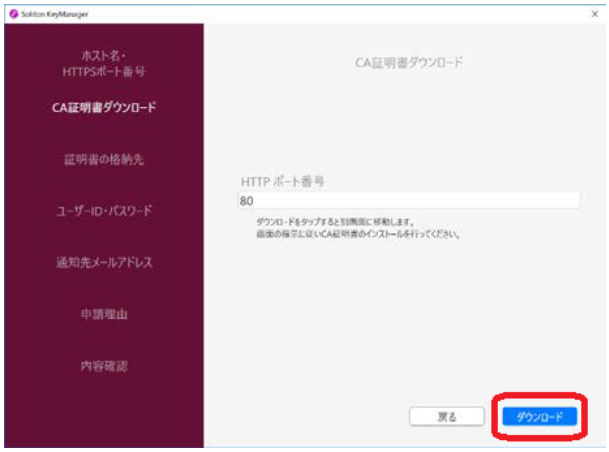
[次へ]をクリックします。



4　クライアント証明書の初回インストール時には、CA証明書のインストールも必要となります。(4～8の手順)

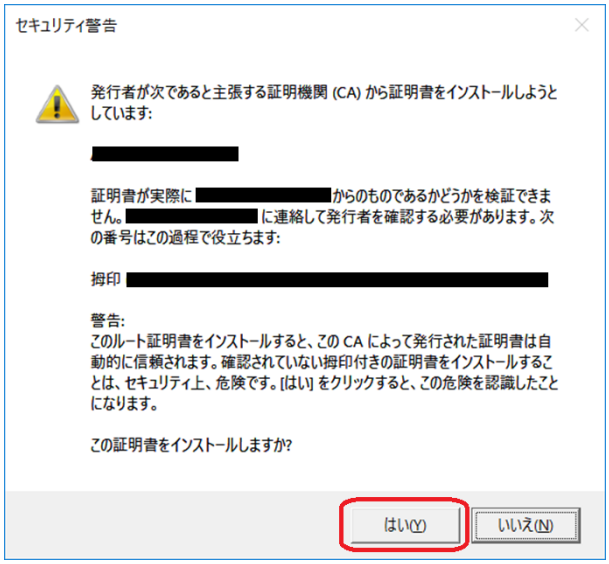
[HTTPポート番号]:
([デフォルト値から変更なし)
80

[ダウンロード]をクリックします。



5　クライアント証明書の初回インストール時には、ルートCA証明書のインストールも必要となります。
この際、「セキュリティ警告」という右図のようなポップアップが表示されます。

[はい]をクリックして手順を進めてください。



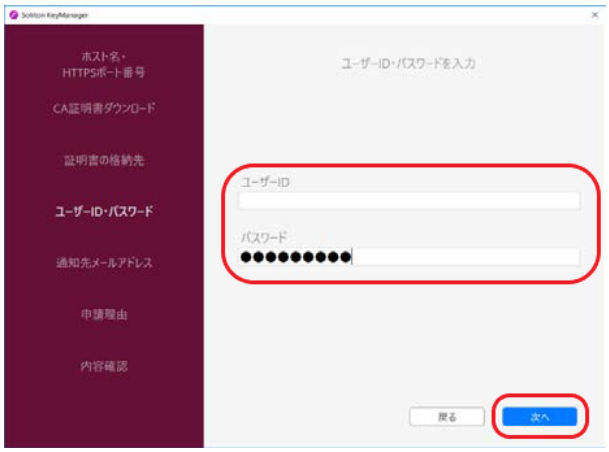
3.3.2. クライアント証明書取得申請

6　正常に接続されると、証明書の格納先画面が表示されますので、[ユーザー]をクリックします。

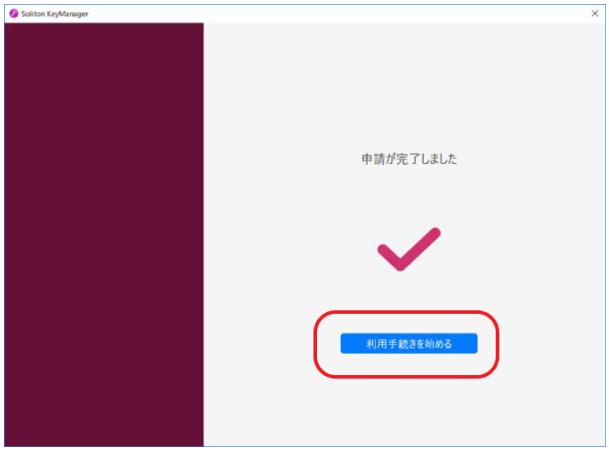


7　情報を入力し[次へ]をクリックします。

[ユーザーID]:
情報総合センターの利用者ID
[パスワード]:
情報総合センターの利用者パスワード

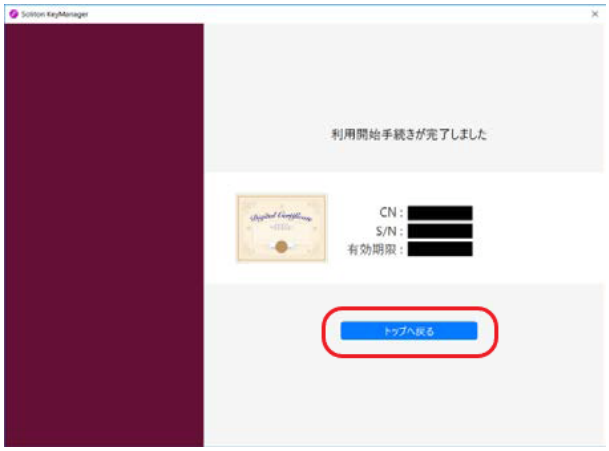


8　[利用手続きを始める]をクリックします。

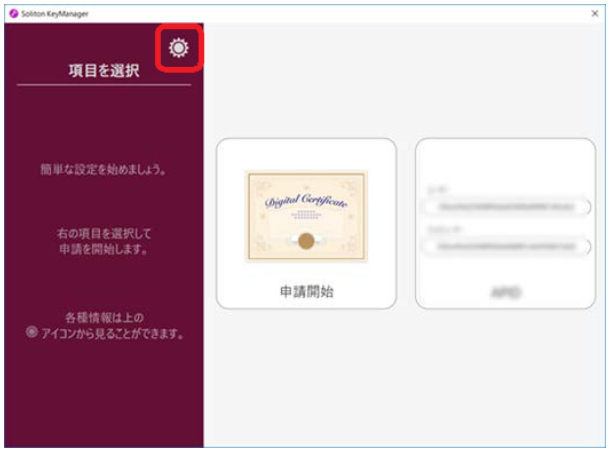


3.3.3. クライアント証明書インストール確認

9　証明書のインストールが完了しましたので、
[トップへ戻る]をクリックします。



10　左上の歯車アイコンをクリックします。



11　インストールした証明書の一覧が確認できます。
[詳細]をクリックすると、証明書の
詳細情報を参照できます。



4. macOS編

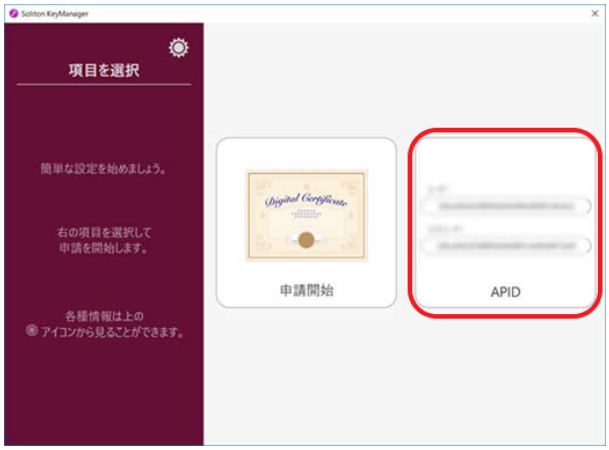
4.1. Soliton KeyManager インストール

- Soliton KeyManager（Mac版）
  - 動作環境: 「別紙：Soliton KeyManager V2 説明書 第5版」のP9を参照してください。
  - ダウンロード先: https://www.soliton.co.jp/support/soliton/hardware/skm/

4.2. APID確認・申請

Soliton KeyManagerを起動して、APIDを確認します。

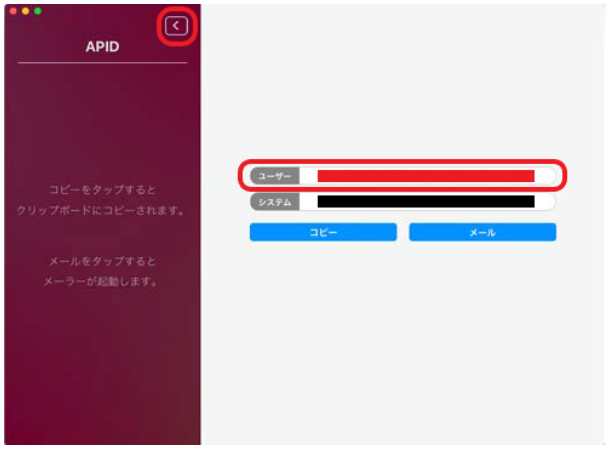
1 KeyManagerを起動すると、トップページが表示されます。 [APID]をクリックします。



2 [ユーザー]と表示されている右横の文字列が今回利用するAPIDです。

[コピー]をクリックして、メモや申請様式等にペーストします。

[閉じる]をクリックし、表示を終了します。



4.2.1. APIDの申請

利用者は取得した「APID」と「情報総合センターの利用者ID」を管理者へ申請します。 この申請を実施しないとクライアント証明書発行申請ができませんので、ご注意ください。

確認事項

- APIDを申請する際、英文字「A～Z」を小文字「a～z」に変更してください。

4.3. クライアント証明書インストール

4.3.1. 認証局証明書(CA)インストール

1　KeyManagerを起動すると、トップページが表示されます。



2　[申請開始]をクリックします。



3　[配布サーバ]への接続情報を入力します。
ホスト名を入力: 150.26.222.148
[HTTPSポート番号]:
(デフォルト値から変更なし)
443

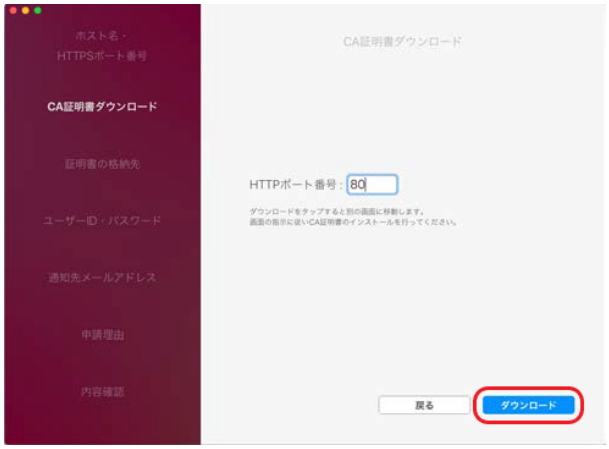
[次へ]をクリックします。



4　クライアント証明書の初回インストール時には、CA証明書のインストールも必要となります。(4～8の手順)

[HTTPポート番号]:
(デフォルト値から変更なし)
80

[ダウンロード]をクリックします。



5　新規の「プロファイル」ウィンドウが立ち上がりますので、[続ける]をクリックします。

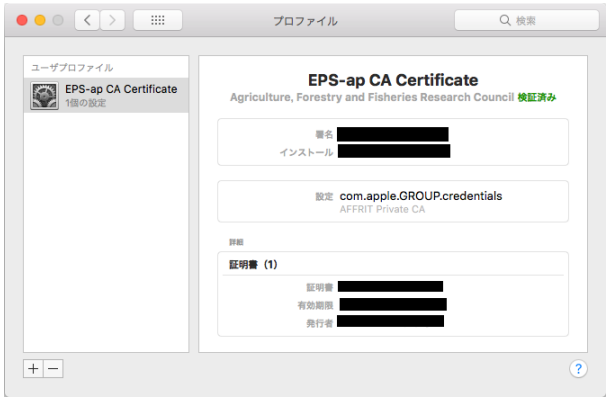


6　[インストール]をクリックします。



7　CA 証明書のインストールが完了します。

「プロファイル」ウィンドウは閉じていただき、 KeyManager の画面を開いてください。



4.3.2. クライアント証明書取得申請

8　配布サーバへの接続情報が入力されている事を確認 し、[次へ]をクリックします。
[ホスト名を入力]: 150.26.222.148
[HTTPS ポート番号] :
(デフォルト値から変更なし)
443



9　正常に接続されると、証明書の格納先画面が表示さ
れますので、[ユーザー]をクリックします。

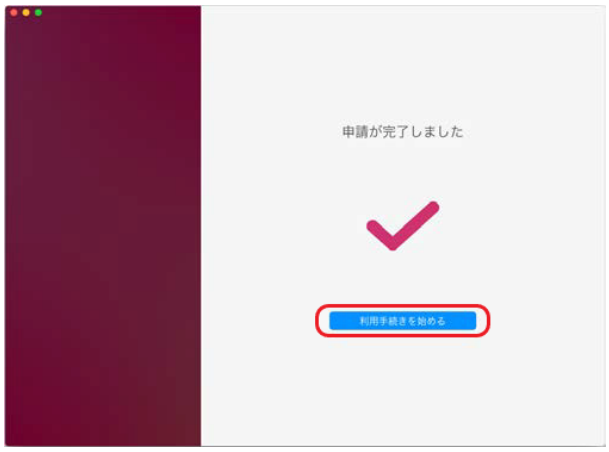


10　情報を入力し[次へ]をクリックします。

[ユーザーID]:
情報総合センターの利用者 ID
[パスワード]:
情報総合センターの利用者パスワード

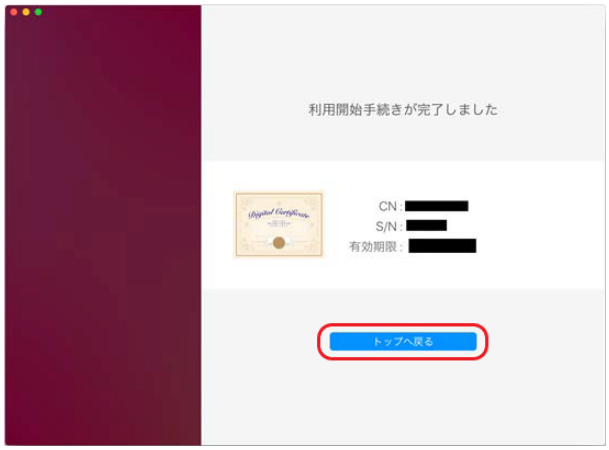


11　[利用手続きを始める]をクリックします。



4.3.3. クライアント証明書インストール確認

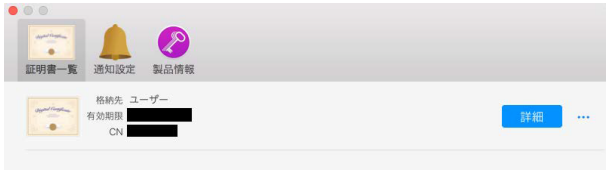
12　証明書のインストールが完了しましたので、[トップへ戻る]をクリックします。



13　左上の歯車アイコンをクリックします。



14　インストールした証明書の一覧が確認できます。
[詳細]をクリックすると、証明書の詳細情報を参照で きます。



5. Android編

5.1. Soliton KeyManager インストール

- Soliton KeyManager（Android版）
  - 動作環境: 「別紙：Soliton KeyManager V2 説明書 第5版」のP9を参照してください。
  - 開発元サイト: https://www.soliton.co.jp/support/soliton/hardware/skm/
    アプリケーションはGoogle Playよりダウンロードしてください。



Android 7系以前のOSをご利用の場合は、以下Android 6系、7系を参照してください。
Android 8, 9, 10系をご利用の場合は、Android 8系、9系、10系を参照してください。

5.2. Android 6系、7系

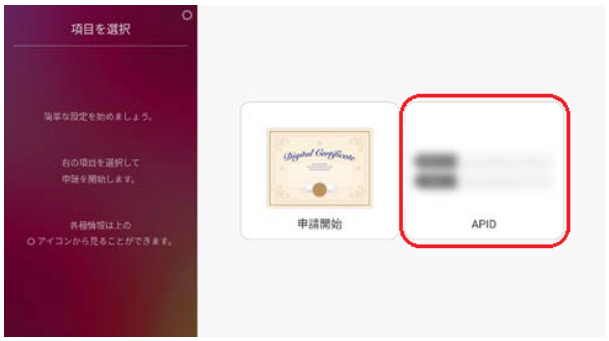
5.2.1. APID確認・申請

APIDの確認

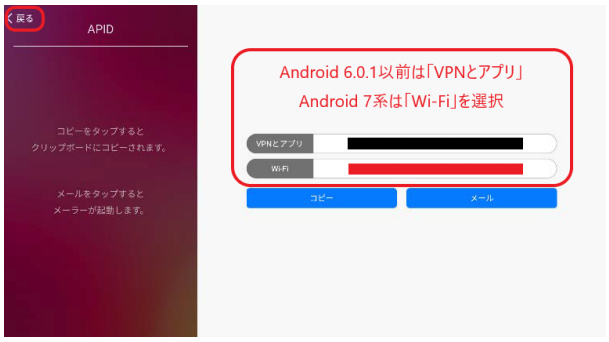
1 KeyManager
の初回起動時、権限に関するダイアログが表示されます。
[許可]をタップします。



2 KeyManager
のトップページが表示されます。
[APID]をタップします。



3 Android 6.0.1 以前の場合は、[VPNとアプリ]と表示されている文字列が、今回利用するAPID です。
Android 7 系の場合は、[Wi-Fi]と表示されている文字列が、今回利用するAPID です。
[戻る]をタップし、トップページに戻ります。



APIDの申請

利用者は取得した「APID」と「情報総合センターの利用者ID」を管理者へ申請します。 この申請を実施

しないとクライアント証明書発行申請ができませんので、ご注意ください。

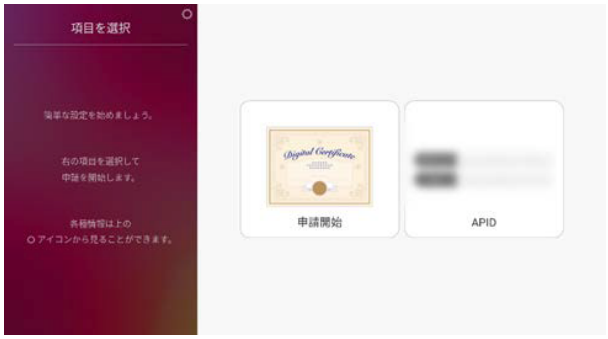
確認事項

- APIDを申請する際、英文字「A～Z」を小文字「a～z」に変更してください。

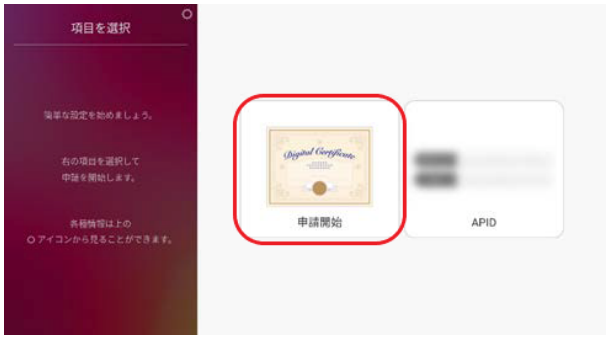
5.2.2. クライアント証明書インストール

認証局証明書(CA)インストール

1 KeyManagerを起動すると、トップページが表示されます。



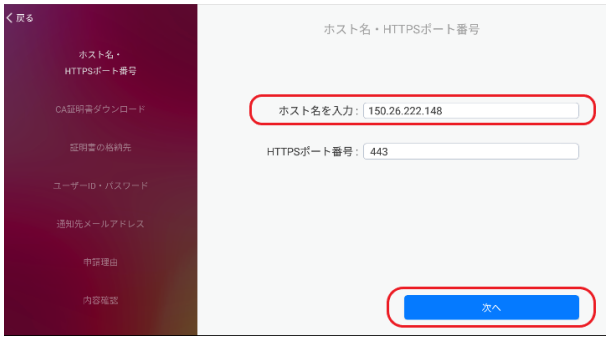
2 [申請開始]をタップします。



3 [配布サーバ]への接続情報を入力します。

ホスト名を入力: 150.26.222.148
[HTTPSポート番号]:
(デフォルト値から変更なし)
443

[次へ]をタップします。



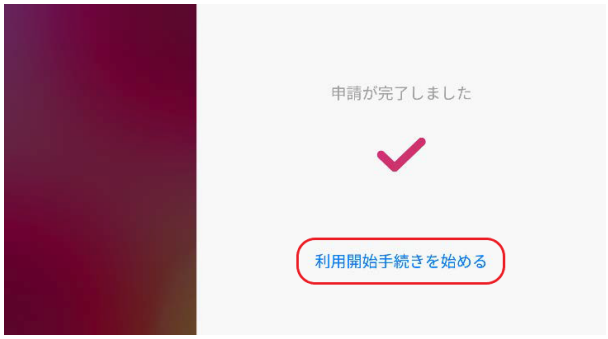
4　正常に接続されると、証明書の格納先画面が表示されます。
Android 6.0.1 以前は、[VPNとアプリ]、
Android 7 系の場合は、[Wi-Fi]を 選択します。



5　情報を入力し[次へ]をタップします。
[ユーザーID]: 情報総合センターの利用者ID
[パスワード]:
情報総合センターの利用者パスワード



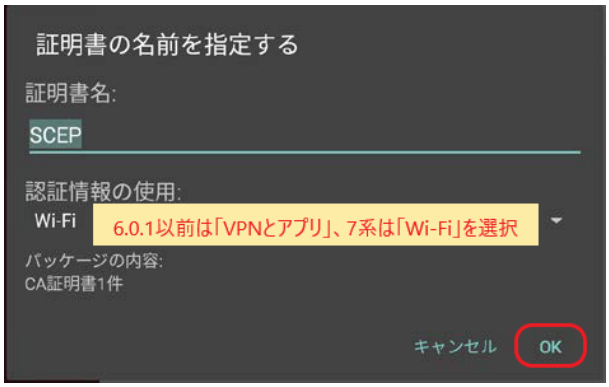
6　[利用開始手続きを始める]をタップします。



クライアント証明書インストール確認

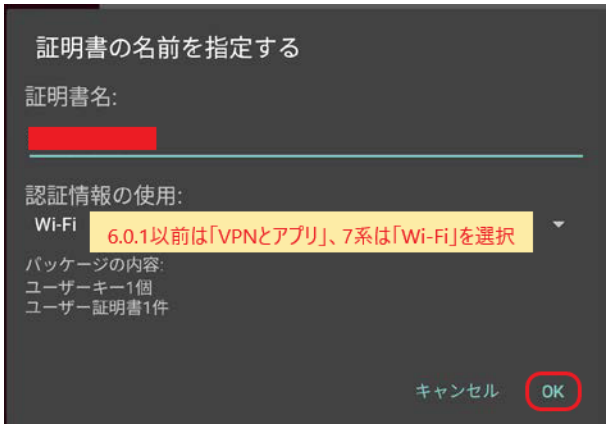
7　正常に接続されると、[証明書の名前を指定する]の画面が表示されます。
下記の情報を入力し、[OK]をタップします。

[証明書名]: 変更なし
[認証情報の使用]:
Android
6.0.1以前の場合はVPNとアプリを選択
Android 7系の場合は、Wi-Fiを選択



8　続けてクライアント証明書のインストール画面へ移ります。
下記の情報を入力し、[OK]をタップします。

[証明書名]: 変更なし
[認証情報の使用]:
Android
6.0.1以前の場合はVPNとアプリを選択
Android 7系の場合は、Wi-Fiを選択



9　[利用開始手続きが完了しました]と表示され、インストールは完了です。

[トップへ戻る]をタップします。



5.3. Android 8系、9系、10系

5.3.1. APID確認・申請

APIDの確認

1 KeyManager
を起動するとトップページが表示されます。

[APID]をタップします。



2 Android 8、9、10の場合は、[VPNとアプリ]
と表示されている文字列が、今回利用する
APID です。



APIDの申請

利用者は取得した「APID」と「情報総合センターの利用者ID」を管理者へ申請します。 この申請を実施しないとクライアント証明書発行申請ができませんので、ご注意ください。

確認事項

- APIDを申請する際、英文字「A～Z」を小文字「a～z」に変更してください。

5.3.2. クライアント証明書インストール

認証局証明書(CA)インストール

1 KeyManagerを起動すると、トップページが表示されます。

[申請開始]をタップします。



2 [配布サーバ]への接続情報を入力します。
ホスト名を入力: 150.26.222.148
[HTTPSポート番号]:
(デフォルト値から変更なし)
443

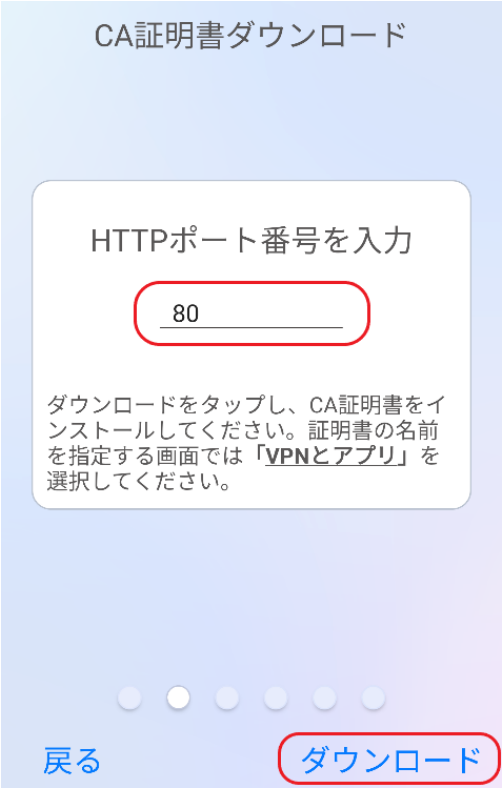
[次へ]をタップします。



3　CA証明書ダウンロードのため、[配布サーバ]の接続情報を入力します。
[HTTPポート番号]:
(デフォルト値から変更なし)
80

[ダウンロード]をタップします。

※Android10の場合、表示されません。そのまま5へ進んでください。





4　正常に接続されると、[証明書の名前を指定する]の画面が表示されます。
下記情報を入力し、そのまま[OK]をタップします。

[証明書名]: 変更なし
[認証情報の使用]: VPNとアプリを選択



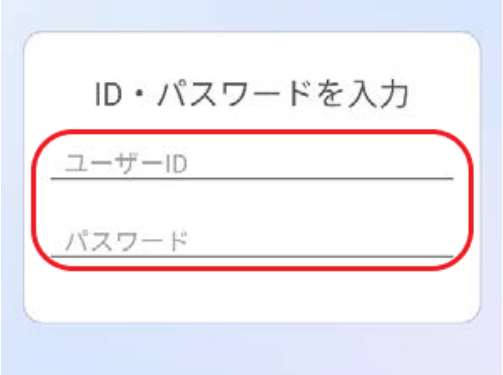
5　正常に接続されると、証明書の格納先画面が表示されます。

[VPNとアプリ]を選択します。

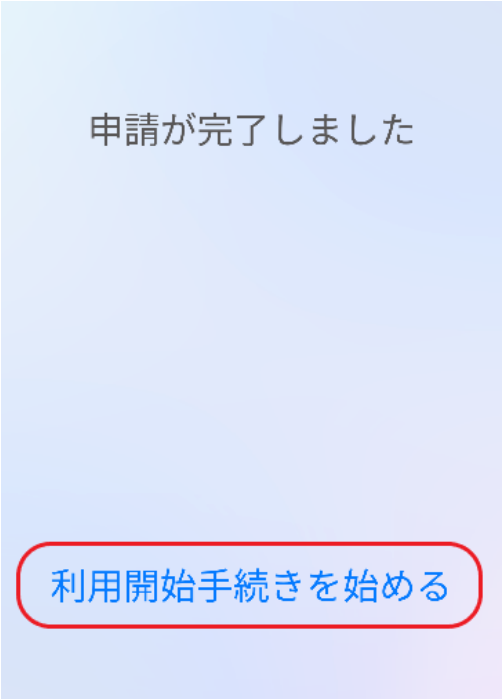


6　情報を入力し[次へ]をタップします。

[ユーザーID]: 情報総合センターの利用者ID
[パスワード]:
情報総合センターの利用者パスワード

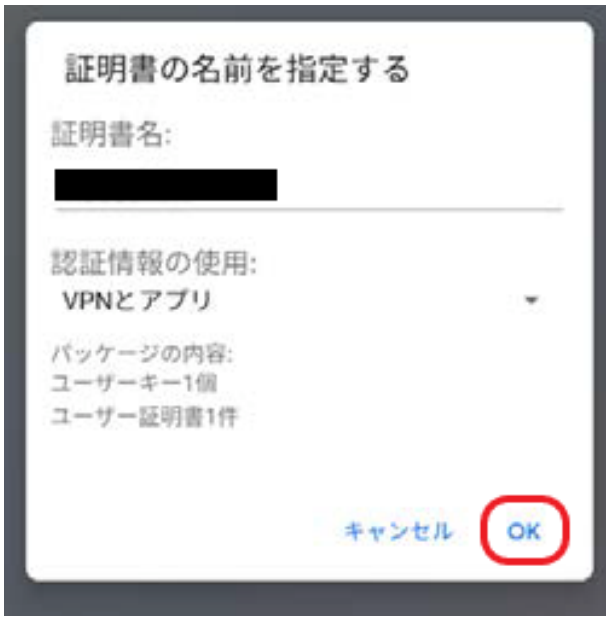


7　[利用開始手続きを始める]をタップします。



クライアント証明書インストール確認

8　正常に接続されると、[証明書の名前を指定する]の画面が表示されます。
下記情報を入力し、[OK]をタップします。
[証明書名]:
変更なし(デフォルト値はAFFRITアカウント)
[認証情報の使用]:
VPNとアプリを選択



9　[利用手続きが完了しました]と表示され、インストールは完了です。

[トップへ戻る]をタップします。



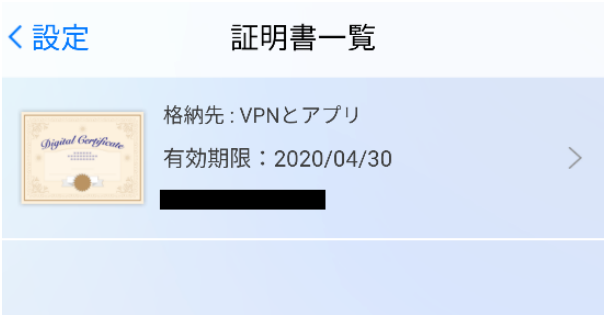
10　右上の歯車アイコンをタップします。



11　[証明書一覧]をタップします。



12　インストールした証明書の一覧が確認できます。



6. iOS編

6.1. UDID確認・申請



2018年9月以降にリリースされたiOS端末の場合、UDIDがハイフン入りの25桁の文字列に仕様が変更されています。
また、UDIDをiTunesで確認できない場合がありますので、iTunes以外での確認方法につきましては、Windowsデバイスマネージャ(iPhone XS/XR/11/11pro)、Macシステムレポート(iPhone XS/XR/11/11pro)を参照してください

6.1.1. iTunes で確認

1 iTunes(Apple社)がインストールされている端末を準備し、iOS端末を接続します。
iTunesが自動起動しない場合は、手動で起動させてください。

<No Image>

2 端末を選択し、[概要]タブをクリックします。



3 [シリアル番号]をクリックします。

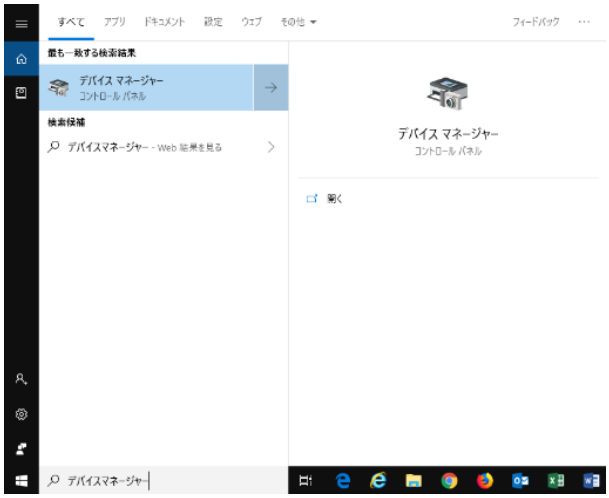


4 [シリアル番号]の表示が切り替わり、[端末識別番号]となります。
UDIDが40桁の場合、申請の際にUDIDの大文字[A-Z]を小文字[a-z]に変更してくだ さい。
(UDIDが、25桁の場合は、そのまま申請してください。)

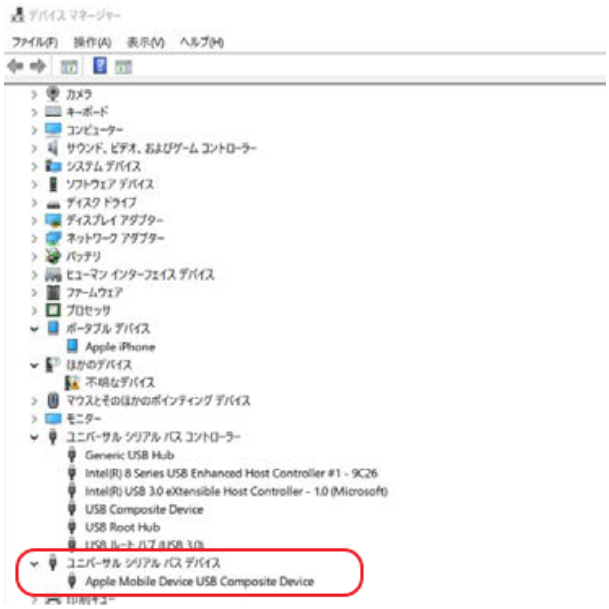


6.1.2. Windowsデバイスマネージャ(iPhone XS/XR/11/11pro)

1　Windows端末に、iOS端末を接続し、デバイスマネージャを起動します。
([検索ボックス]に、[デバイスマネージャ]と入力し、起動します。)

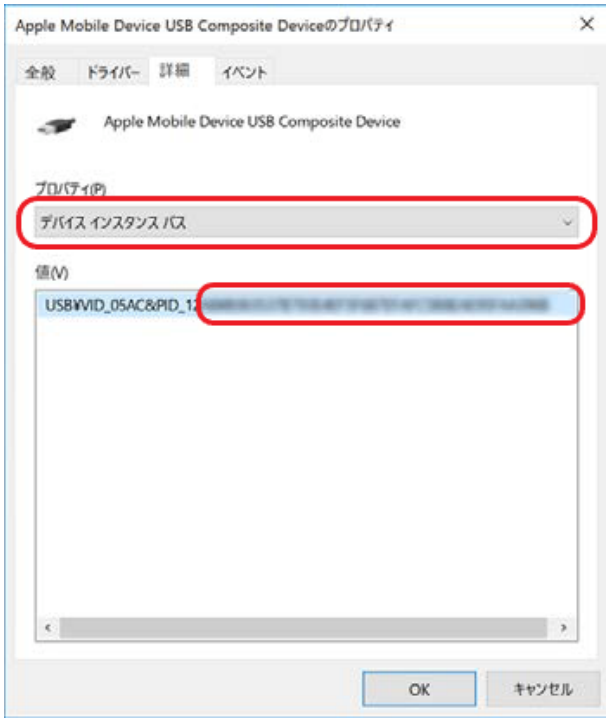


2　[ユニバーサルシリアルバスデバイス]より、接続したiOS機器が認識されているか確認してください。
表示された端末をダブルクリックし、プロパティを開いてください。



3　端末のプロパティ表示後、[詳細]タブをクリックします。
プロパティの[デバイスインスタンスパス]を選択すると値の右側部分に接続したiOS機器のUDID(ハイフン入り25桁)が表示されます。

UDIDが25桁の場合は、大文字[A-Z]のまま申請してください。



6.1.3. Macシステムレポート(iPhone XS/XR/11/11pro)

1　MacにiOS端末を接続します。
接続したあと、Macの画面左上部にありますAppleアイコンのメニューを開き、[このMacについて]をクリックします。



2　[システムレポート]をクリックします。



3 [ハードウェア]セクションにある[USB]をクリックします。
画面右側の[USB装置ツリー]にiOS端末情報が表示されるので、これを選択し、下に表示された項目の中から[シリアル番号]にUDID(ハイフン入り25桁)が表示されますので、こちらを利用します。

UDIDが25桁の場合は、大文字[A-Z]のまま申請してください。



6.1.4. UDIDの申請

利用者は取得した「UDID」と「情報総合センターの利用者ID」を管理者へ申請します。
この申請を実施しないとクライアント証明書発行申請ができませんので、ご注意ください。

確認事項

- UDIDを申請する際、英文字「A～Z」を小文字「a～z」に変更してください。(40桁の場合)
- 2018年9月以降にリリースされたiOS端末の場合、UDIDがハイフン入りの25桁の文字列に仕様が変更されています。
  UDIDが25桁の場合は、大文字[A-Z]のままで申請してください。

6.2. クライアント証明書インストール

iOSでのクライアント証明書の取得・インストールは、iOS 12以降のWebブラウザ(Mobile Safari)で行います。

対応Webブラウザ

- iOS 12以降のMobile Safari

確認事項

- iOSの[設定]-[Safari]-[Cookieをブロック]を[常にブロック]以外に設定してください。
- iOS 10.3以降ではクライアント証明書が標準で信頼されなくなります。このため手動にて有効にする必要がありますので、ご注意ください。(手順11証明書信頼設定の有効化参照)

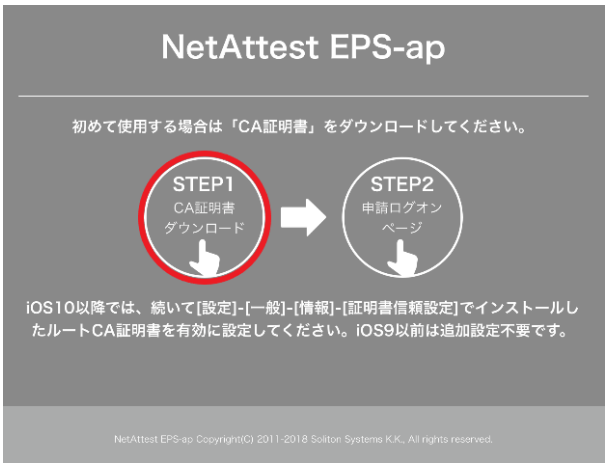
6.2.1. 認証局証明書(CA)インストール

1　端末のWebブラウザ(Safari)で、以下のURLを入力して接続してください。
http://
<配布サーバのIPアドレスまたはホスト名> /
http://150.26.222.148/

※[設定]-[Safari]-
[デスクトップ用Webサイトを表示]にて[すべてのWebサイト]が有効になっていると、「http」と入力してもhttpsページにリダイレクトされてしまいます。必ず上記設定が[無効]であることを確認してから、Webブラウザにアクセスしてください。



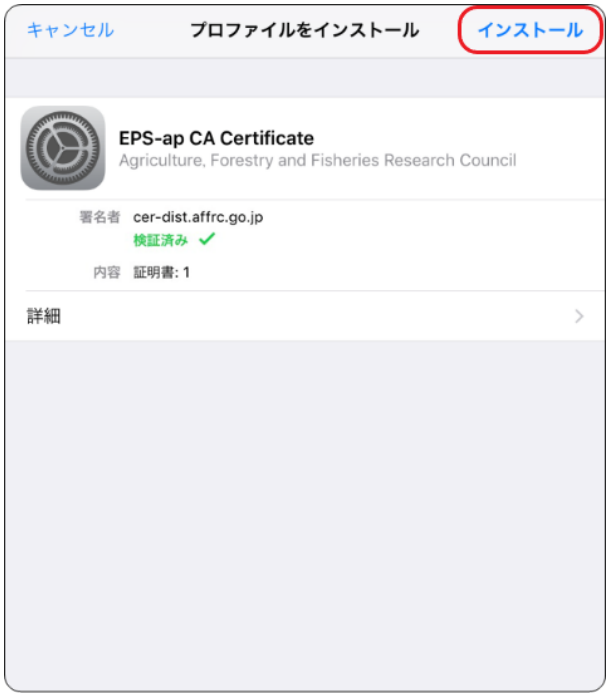
2　申請Webサービスのトップページが表示されます。
[STEP 1 CA証明書ダウンロード]をタップします。



3　正常に接続されると、構成プロファイル(CA証明書プロファイル)の表示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。



4　CA証明書をインストールするため、プロファイルのインストール画面に移ります。
[インストール]をタップします。



5　端末のパスコードを設定している場合は、パスコードを入力し[完了]をタップします。



6　証明書信頼設定の警告画面が表示されます。
内容を確認し、[インストール]をタップします。

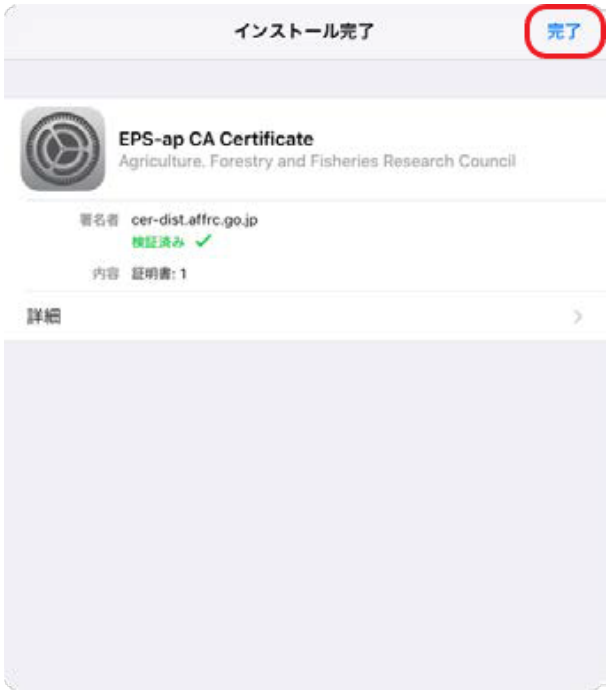
iOS 10.3以降では、クライアント証明書が標準で信頼されなくなりました。
このため、手動にて有効にする必要がありますので、ご注意ください。
(手順11証明書信頼設定の有効化を参照)



7　確認のため再度表示されますので、
[インストール]ボタンをタップします。



8　インストール完了が表示されますので、
[完了]ボタンをタップします。



9　[設定]-[一般]-[プロファイル]
(または[プロファイルとデバイス管理])を
選択します。
プロファイルに、認証局証明書(EPS-ap CA
Certificate)があることを確認します。



10 証明書の詳細を確認するには、EPS-ap CA Certificateをタップします。



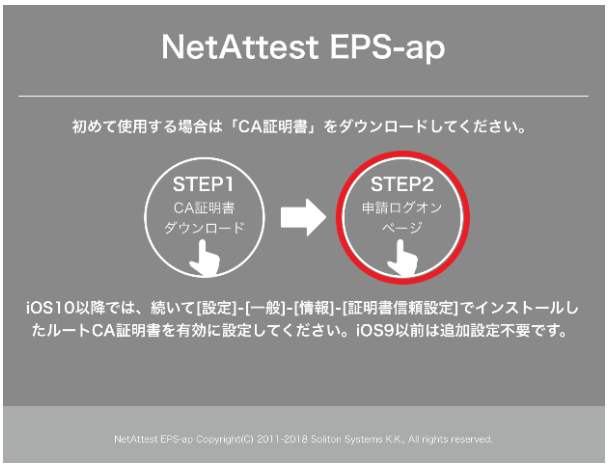
6.2.2. 証明書信頼設定の有効化

11 [設定]-[一般]-[情報]-[証明書信頼設定]の順に選択し、[ルート証明書を全面的に信頼する]で、[AFFRIT Private CA]を有効にします。



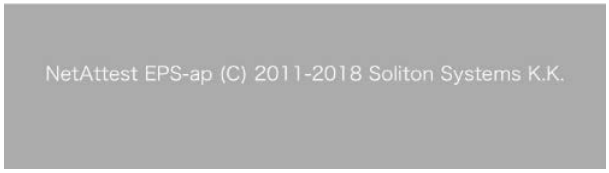
6.2.3. クライアント証明書取得申請

12 CA証明書プロファイルのインストール後、Webブラウザに申請Webサービスのトップページが表示されます。[STEP 2 申請ログオンページ]をタップします。



13 [利用開始]ボタンをタップします。

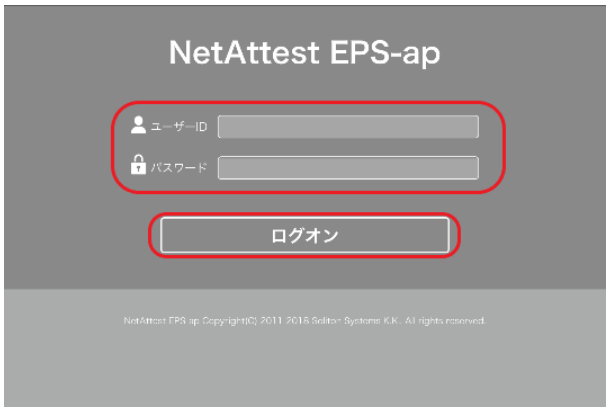




14 構成プロファイル(CA証明書プロファイル)の表示に関するダイアログが表示されます。
[許可]をタップしてください。



15 申請ログオンのトップページが表示されます。
下記情報を入力して、[ログオン]ボタンをタップします。
[ユーザーID]: 情報総合センターの利用者ID
[パスワード]:
情報総合センターの利用者パスワード



16 [利用開始]ボタンをタップします。

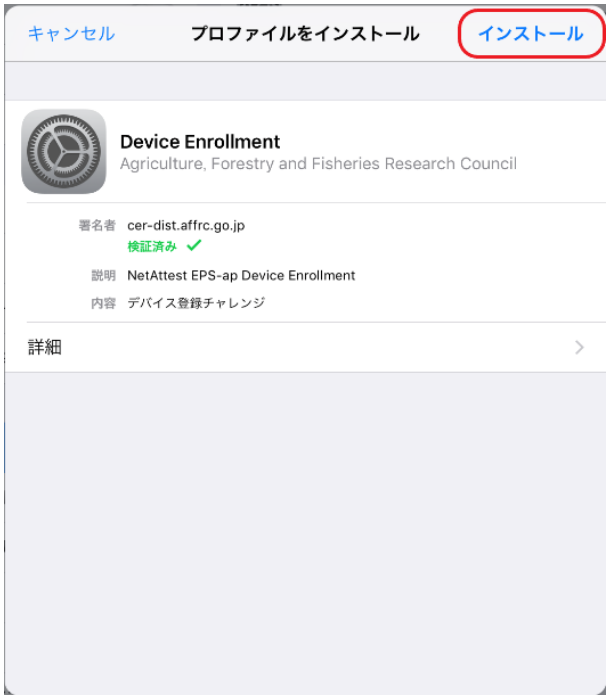


17 再度、構成プロファイル(CA証明書プロファイル)の表示に関するダイアログが表示されます。
[許可]をタップしてください。



6.2.4. クライアント証明書インストール確認

18 クライアント証明書(Device Enrollment)のインストールが始まります。
プロファイルのインストール画面において、[インストール]ボタンをタップします。



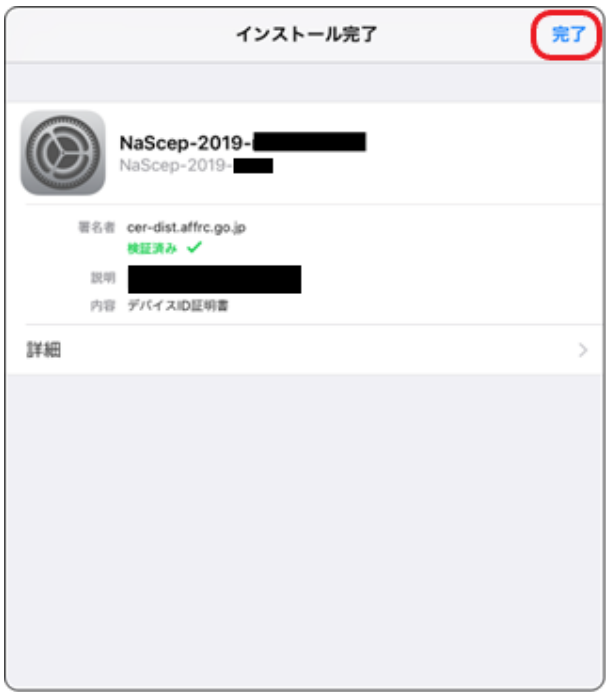
19 端末のパスコードを設定している場合は、パスコードを入力後、[完了]をタップします。



20 再度確認を求められますので、[インストール] ボタンをタップします。



21 インストール完了が表示されますので、[完了]をタップします。



22 クライアント証明書は、[設定]-[一般]-[プロファイル]で確認できます。

<No Image>

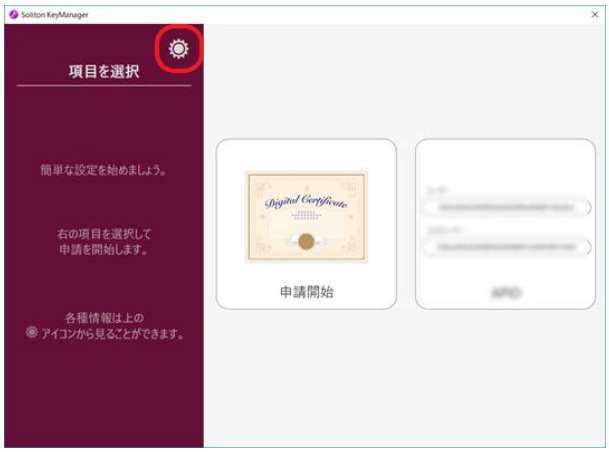
7. 証明書の更新

- クライアント証明書の有効期限は翌年度4月末までとします（4月一ヶ月は失効猶予期間です）。このため、翌年度の利用継続を希望する登録端末は、当該年度の継続申請受付期間（2月～3月）において、新規利用申請と同様（利用誓約書の提出は不要）に所属組織を通して申請手続きを行ってください。（新たな証明書を発行しますので申請端末にインストールしてください）
- クライアント証明書のインストールについては、それぞれのOSの「クライアント証明書インストール」手順を参照してください。(認証局証明書(CA)は、インストール済みですので作業は不要です。)
- 新たな証明書をインストールし、動作の確認ができたら、古い証明書は削除可能です。古い証明書を削除していない場合、証明書の有効期限内であれは使用可能ですので、使用する証明書を選択する必要がありますのでご注意ください。

8. 証明書の削除

8.1. クライアント証明書の削除(Windows)

1　KeyManagerを起動すると、トップページが表示されます。
左上の歯車のアイコンをクリックします。



2　削除したい証明書の[…]をクリックすると、削除と通知設定のメニューが表示されるので[削除]をクリックします。



3　削除の確認が表示されるので[はい]をクリックします。

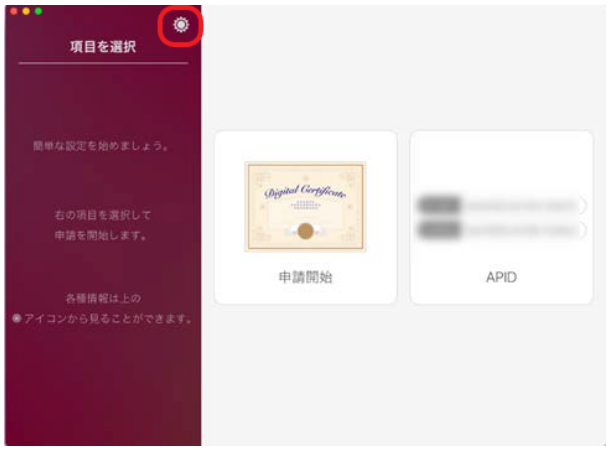


4　証明書一覧に、削除した証明書が表示されていないことを確認してください。



8.2. クライアント証明書の削除(macOS)

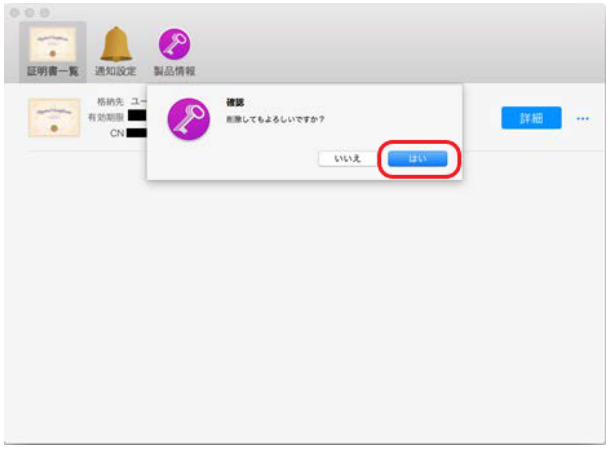
1　KeyManagerを起動すると、トップページが表示されます。
左上の歯車のアイコンをクリックします。



2　削除したい証明書の[…]をクリックすると、削除と通知設定のメニューが表示されるので[削除]をクリックします。



3　削除の確認が表示されるので[はい]をクリックします。



4　証明書一覧に、削除した証明書が表示されていないことを確認してください。



8.3. クライアント証明書の削除(Android)

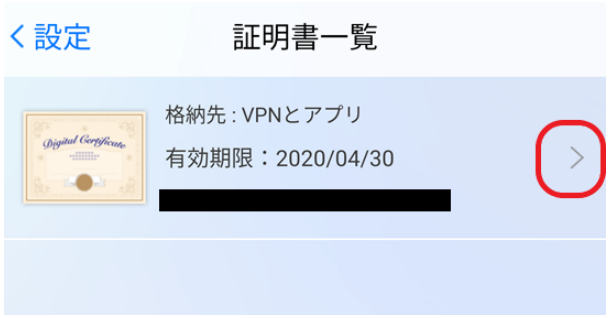
1　KeyManagerを起動すると、トップページが表示されます。
右上の歯車のアイコンをタップします。



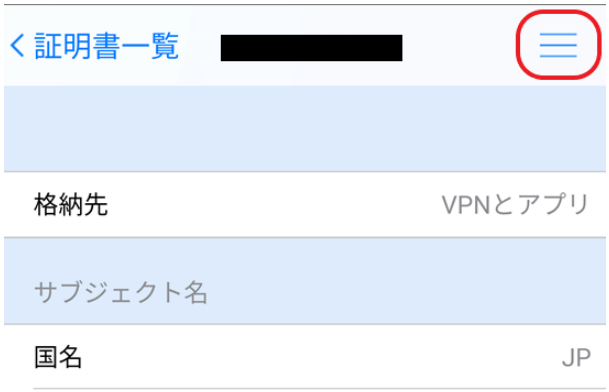
2　[証明書一覧]をタップします。



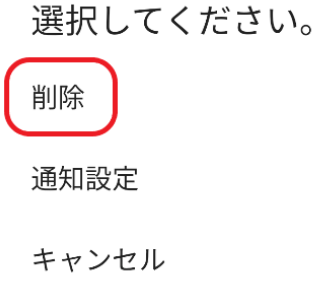
3　削除したい証明書が表示されていることを確認し、[>]をタップします。



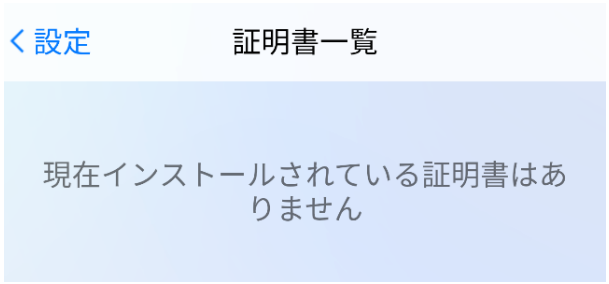
4　証明書の詳細情報が表示されますので、右上の[≡]をタップします。



5　証明書に対する操作ができますので、[削除]をタップします。
確認のダイアログが表示されますので、[はい]をタップします。



6　証明書一覧に、削除した証明書が表示されていないことを確認してください。



8.4. クライアント証明書の削除(iOS)

1　「設定」ー「一般」ー「プロファイル」で、インストールされているプロファイルを確認します。

対象のプロファイルを選択し、削除します。
端末のパスコードの入力が求められますので、パスコードを入力してください。

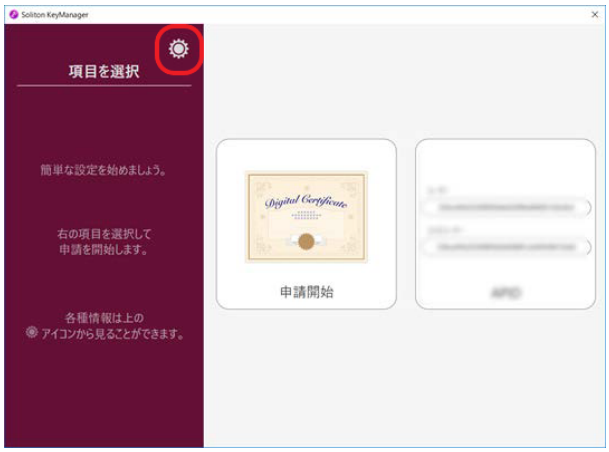


9. 通知設定

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、以下に示します。

9.1. クライアント証明書の有効期限の通知機能(Windows)

1　KeyManagerを起動すると、トップページが表示されます。
左上の歯車のアイコンをクリックします。



2　[通知機能]タブをクリックすると、通知に関する設定項目が表示されます。
証明書の有効期限が過ぎた通知を表示させる場合、[期限切れの際に通知を許可]にチェックを入れてください。

証明書の有効期限切れ間近に通知を表示させる場合、[期限切れ間近に通知を許可]にチェックを入れ、日数を設定してください。
デフォルト: 7日前
設定可能範囲: 1～120日前

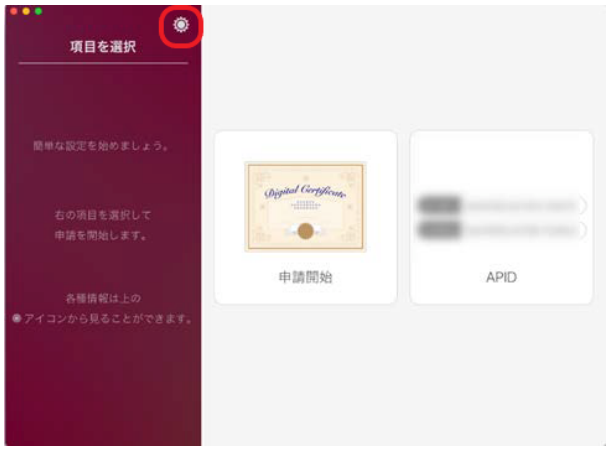


通知機能に関する補足事項

- 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されます。
- 有効期限切れのメッセージは、証明書の有効期限に表示されている時刻に通知されます。
- 通知時間にコンピュータを起動していない、またはログオン(サインイン)していない場合を考慮し、ユーザがログオン(サインイン)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。
- ログオン(サインイン)時の有効期限切れのメッセージは、ログオン(サインイン)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。

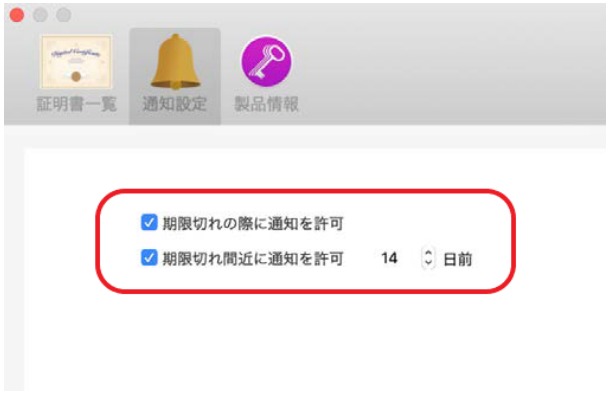
9.2. クライアント証明書の有効期限の通知機能(macOS)

1　KeyManagerを起動すると、トップページが表示されます。
左上の歯車のアイコンをクリックします。



2　[通知機能]タブをクリックすると、通知に関する設定項目が表示されます。
証明書の有効期限が過ぎた通知を表示させる場合、[期限切れの際に通知を許可]にチェックを入れてください。

証明書の有効期限切れ間近に通知を表示させる場合、[期限切れ間近に通知を許可]にチェックを入れ、日数を設定してください。
デフォルト: 7日前
設定可能範囲: 1～120日前



9.3. クライアント証明書の有効期限の通知機能(Android)

1　KeyManagerを起動すると、トップページが表示されます。
右上の歯車のアイコンをタップします。



2　[通知機能]タブをタップすると、通知に関する設定項目が表示されます。



3　証明書の有効期限が過ぎた通知を表示させる場合、 [期限切れ通知 > 通知]をオンにしてください。

証明書の有効期限切れ間近に通知を表示させる場合、 [期限切れ間近通知 > 通知]をオンにし、日数を設定してください。
デフォルト: 7日前
設定可能範囲: 1～120日前



9.4. クライアント証明書の有効期限の通知機能(iOS)

iOSに関しては、通知機能は実装されておりません。