



Soliton KeyManager

Windows 版 Soliton KeyManager V1.4
説明書

Soliton[®]

株式会社ソリトンシステムズ 2017年12月

Soliton KeyManager は、株式会社ソリトンシステムズの商標です。

その他、本書に記載の会社名、製品名等は、各社の商標または登録商標です。

本文中に ™、®、©は明記していません。

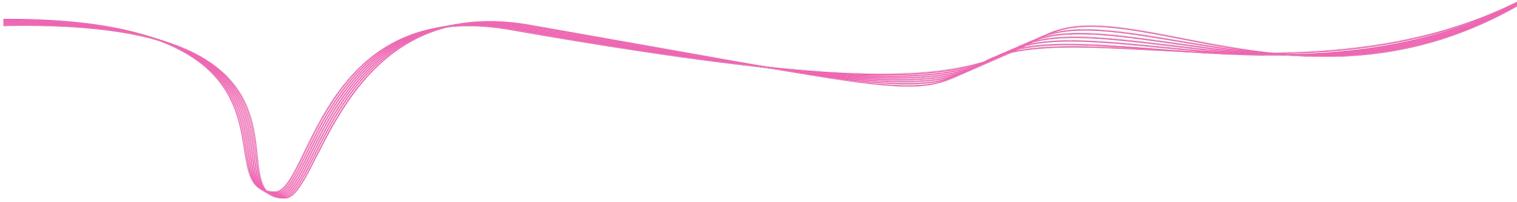
Copyright © 2013-2017, Soliton Systems K.K., All rights reserved.

目次

はじめに	5
本書の表記規則	6
本書で使用される用語	7
1 KeyManager の概要	8
1.1 KeyManager の機能概要	8
2 セットアップ	9
2.1 動作環境	9
2.2 KeyManager をインストールする	10
2.2.1 インストール方法	10
2.2.2 アップデート方法	15
2.2.3 アンインストール方法	18
2.2.4 修復方法	18
3 KeyManager の使用方法	19
3.1 画面構成	19
3.2 証明書をインストールする	22
3.2.1 証明書を申請する	22
3.2.2 デバイスを登録する	31
3.3 証明書を確認/削除/更新する	33
3.3.1 証明書を確認する	33
3.3.2 証明書を削除する	35
3.3.3 証明書を更新する	37
3.4 有効期限の通知機能を使用する	38
3.4.1 デフォルトの設定を変更する	38
3.4.2 証明書単位で通知設定を変更する	39
4 KeyManager 情報の確認方法	42
4.1 APID を確認する	42
4.2 MAC アドレスを確認する	44
4.3 バージョンを確認する	44



5	トラブルシューティング	45
	5.1 申請・デバイス登録に失敗する	45
	5.1.1 プロキシサーバー	45
	5.2 互換オプション	46
	5.3 診断情報	47
	5.3.1 診断情報を取得する	47



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。

Windows 版 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、Windows 版 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

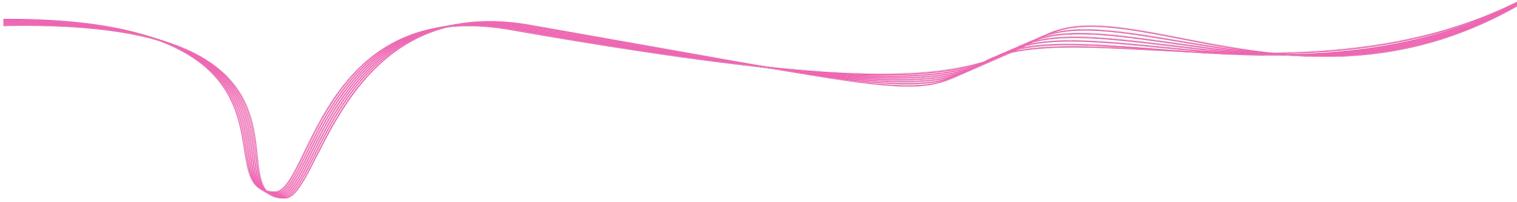
表記例	意味
[Shift]キー	キーは、大カッコ ([]) で囲んであらわします。
[F]→[O]キー	キーが右矢印 (→) で区切られている場合は、それぞれのキーを順に押すことをあらわします。この例では、[F]キー、[O]キーを順に押すことをあらわしています。
[Ctrl]+[A]キー	2つのキーの間にあるプラス記号 (+) は、最初のキーを押しながら2番目のキーを押すことをあらわします。この例では、[Ctrl]キーを押しながら、[A]キーを押すことをあらわしています。
矢印キー	[→]キー、[←]キー、[↑]キー、[↓]キーの総称です。

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の製品です。

□ 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 または Soliton ID Manager (以降、ID Manager) 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、プロファイルの適用、証明書の確認、削除機能を提供します。

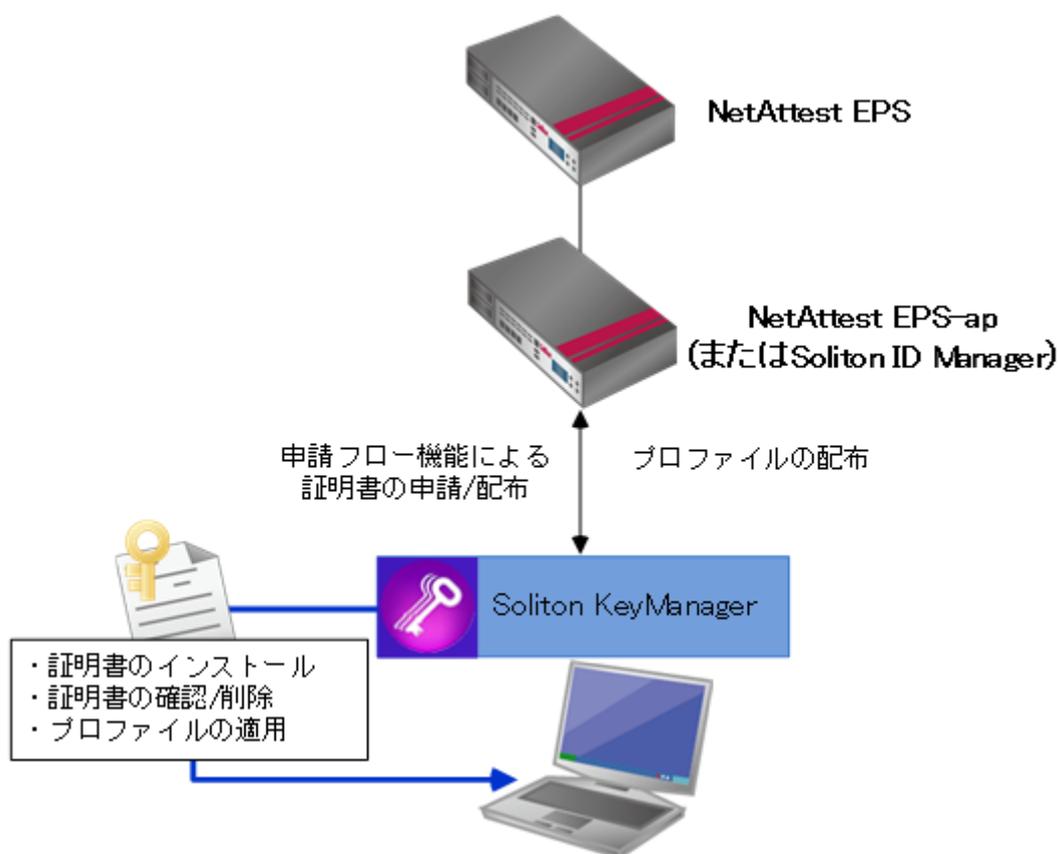


図 1.1.1 機能概要

NetAttest EPS、NetAttest EPS-ap および ID Manager の設定方法については、「NetAttest EPS-ap スタートアップガイド」または「ID Manager リファレンスガイド (プロファイル発行機能)」を参照してください。本書では、連携する機器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。

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 V1.4 の動作環境は、以下のとおりです。

表 2.1 動作環境

項目	内容	
機種	PC/AT 互換機	
OS	32 ビット	64 ビット
Windows 7	Home Premium (SP1) Professional (SP1) Enterprise (SP1) Ultimate (SP1)	Home Premium (SP1) Professional (SP1) Enterprise (SP1) Ultimate (SP1)
Windows 8.1	Core edition (SP なし) Pro (SP なし) Enterprise (SP なし)	Core edition (SP なし) Pro (SP なし) Enterprise (SP なし)
Windows 10	Home (SP なし) Pro (SP なし) Enterprise (SP なし)	Home (SP なし) Pro (SP なし) Enterprise (SP なし)
言語	日本語/英語	
その他	以下の製品が必要です。 ・ NetAttest EPS V4.6.0 以降 V4.6.3 以降を推奨します。 V4.6.0～V4.6.2 においては一部注意事項があります。 詳しくは、弊社の Web サイト内の FAQ を参照してください。 ・ NetAttest EPS-ap V2.0.2 以降 ・ Soliton ID Manager V2.2.0 以降	



- **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。**
- **Windows 7 については、Windows XP Mode はサポート対象外です。**
- **Windows RT はサポート対象外です。**
- **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。**

2.2 KeyManager をインストールする

ここでは 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 KeyManager V1.4.x 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 インストール方法

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。

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. 弊社の Web サイトからダウンロードした「SolitonKeyManagerV14x_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「SolitonKeyManagerV14x.exe」を実行してください。



図 2.2.1 SolitonKeyManagerV14x.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てから、<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、インストール後にデスクトップにショートカットが作成されます。

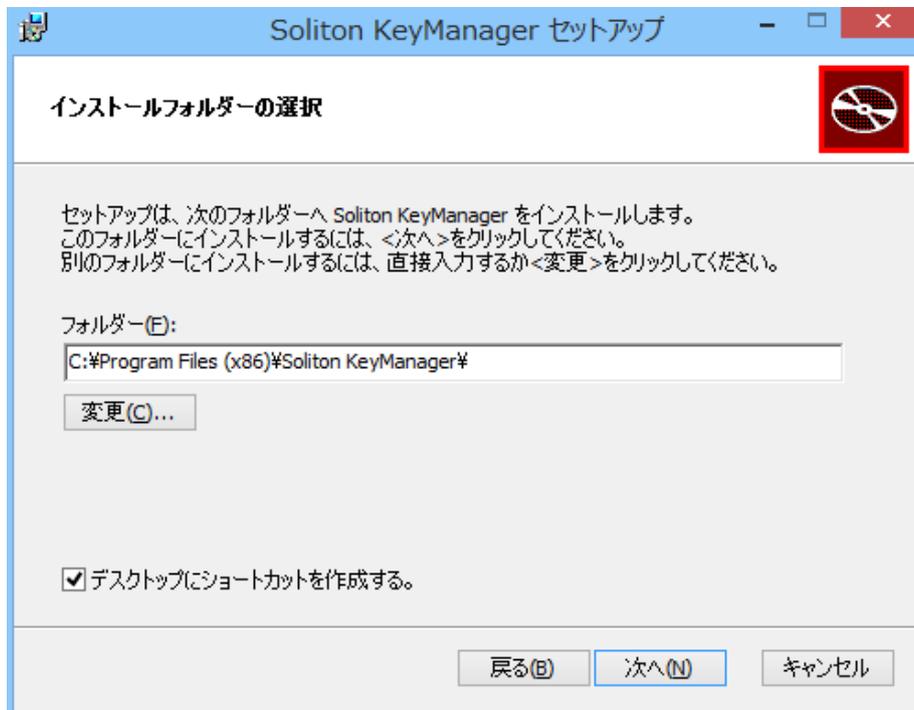


図 2.2.5 インストールフォルダーの選択

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。

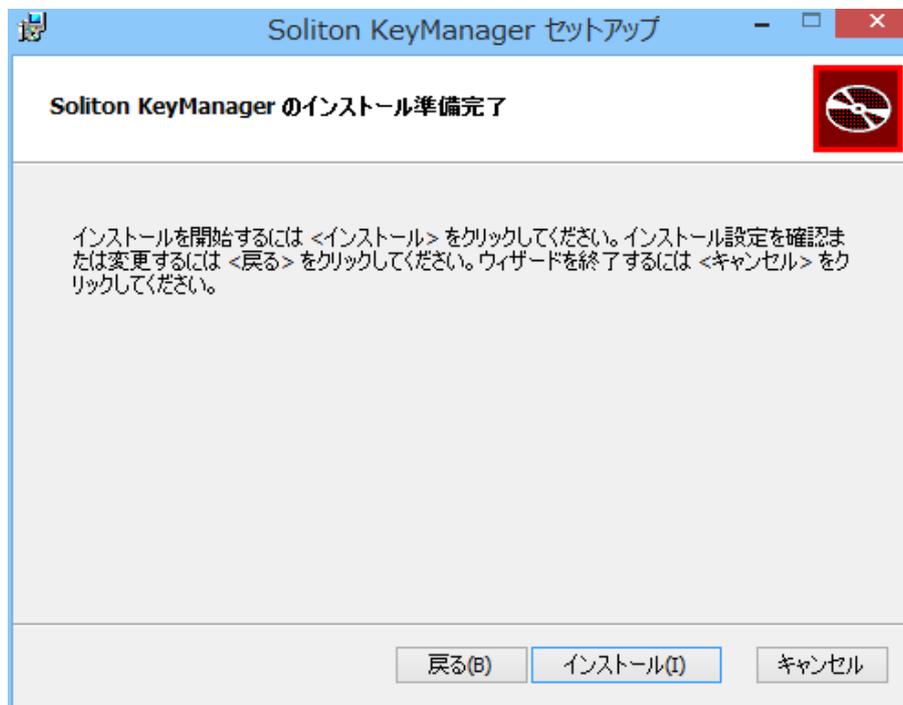


図 2.2.6 インストール準備完了

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。[Soliton KeyManager を起動する] がチェックされている場合は、この画面を閉じた後に KeyManager が起動します。



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、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、SolitonKeyManagerV14x.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¥SolitonKeyManagerV14x.exe -s
```



サイレントインストールを行った場合は、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。

サイレントインストールを行った場合は、「デスクトップにショートカットを作成する」オプションが変更できません。サイレントインストールでは、初期値が有効であるため、デスクトップにショートカットが作成されます。

またサイレントインストールを行った場合は、「Soliton KeyManager を起動する」オプションも変更できません。ただし「Soliton KeyManager を起動する」オプションの初期値は有効ですが、サイレントインストールを行った場合には、インストール後に KeyManager を起動しません。

2.2.2 アップデート方法

KeyManager のアップデートは、以下の手順で行ってください。



KeyManager V1.0 がインストールされている場合は、KeyManager V1.0 をアンインストールしてから、「2.2.1 インストール方法」を参考に KeyManager V1.2.0 以降をインストールしてください。この作業により、KeyManager V1.0 の以下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 (V1.0.1)

また、各証明書ストアに格納した証明書が削除されることはありません。

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「SolitonKeyManagerV14x_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「SolitonKeyManagerV14x.exe」を実行してください。



図 2.2.9 SolitonKeyManagerV14x.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 KeyManager が起動していた場合、強制的に OS が再起動されます。
- KeyManager V1.2.x 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

2.2.3 アンインストール方法

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。

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「SolitonKeyManagerV14x.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、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、SolitonKeyManagerV14x.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¥SolitonKeyManagerV14x.exe -s -uninstall
```



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、Wi-Fi プロファイルを使用した Wi-Fi に関する設定、各証明書ストアに格納された証明書は削除されません。

2.2.4 修復方法

KeyManager は、以下のいずれかの方法で修復を行う事ができます。

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「修復」を選択して、KeyManager を修復してください。
- インストール時に使用した「SolitonKeyManagerV14x.exe」をダブルクリックし、「Soliton KeyManager セットアップ」で[修復]を選択して、KeyManager を修復してください。



KeyManager V1.2.0 以降がインストールされている環境に誤って V1.0.1 以前の KeyManager をインストールしてしまった場合、古い KeyManager をアンインストールした後、V1.2.0 以降のインストーラーで修復を実施してください。

3 KeyManager の使用方法

KeyManager の画面構成、証明書のインストールおよび削除方法について説明します。

3.1 画面構成

「Soliton KeyManager」のアイコンをクリックすると KeyManager が起動し、図 3.1.1 が表示されます。

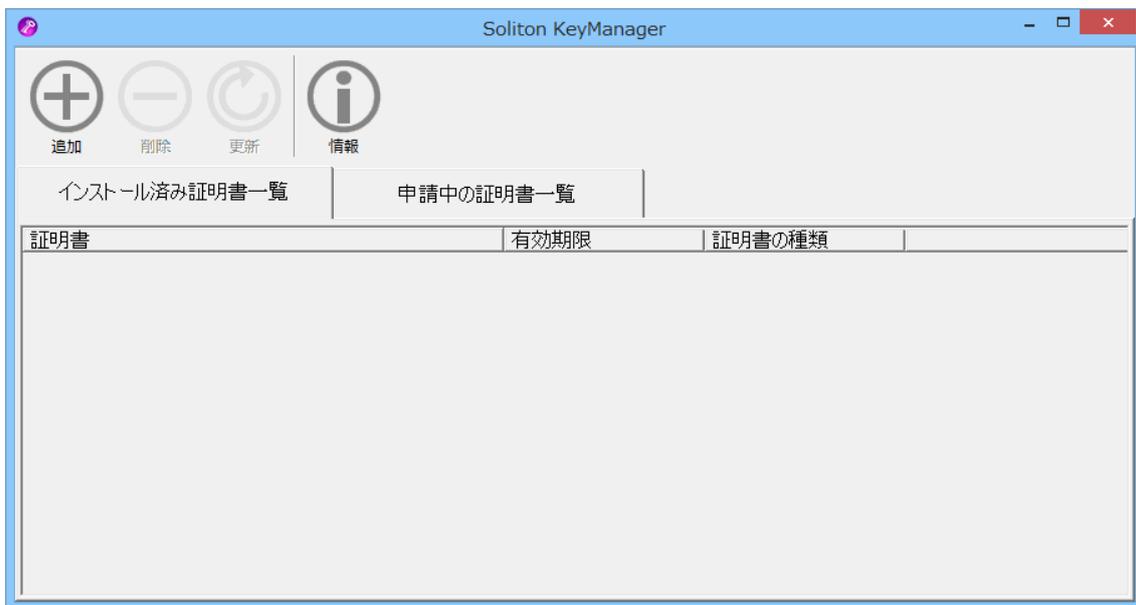


図 3.1.1 KeyManger

KeyManager は、画面上部のツールバーと、インストール済み証明書一覧画面、申請中の証明書一覧画面で構成されています。

一覧画面は、それぞれのタブをクリックすることで表示を切り替えることができます。

□ ツールバー

KeyManager の画面上部に表示されます。

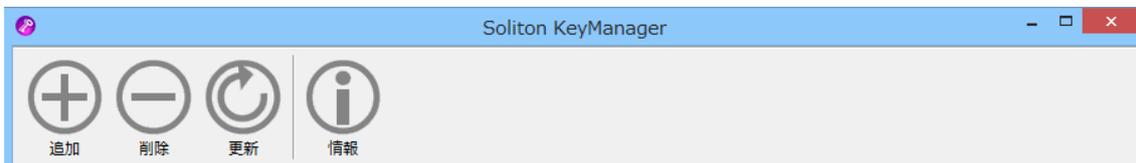


図 3.1.2 ツールバー

表 3.1.1 ツールバー

項目	説明
 追加	証明書の申請や取得を行う際に使用します。

項目	説明
 削除	証明書の削除、および証明書申請の削除、取り下げを行う際に使用します。 一覧に表示されている証明書、または証明書申請を選択している場合に有効になります。
 更新	証明書の更新、および証明書申請の最新状態を表示する際に使用します。 一覧に表示されている証明書、または証明書申請を選択している場合に有効になります。
 情報	APID の確認、および証明書の有効期限通知に関するデフォルトの設定を変更することができます。また KeyManager のバージョンを確認できます。 APID については「4.1 APID を確認する」を参照してください。証明書の有効期限の通知設定については「3.4 有効期限の通知機能を使用する」を参照してください。バージョンの確認については「4.3 バージョンを確認する」を参照してください。

□ インストール済み証明書一覧

KeyManager を使用してインストールした証明書が一覧表示されます。

インストール済みの証明書の確認や削除、および更新を行うことができます。なお、削除した証明書は、一覧には表示されません。

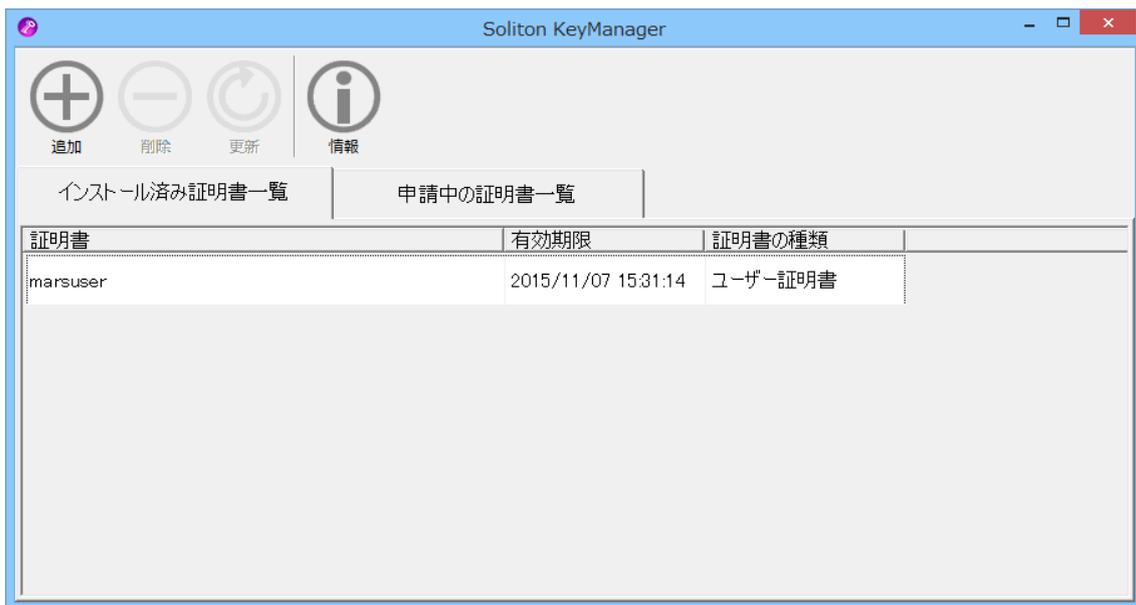


図 3.1.3 インストール済み証明書一覧

表 3.1.2 インストール済み証明書一覧

項目	説明
証明書	インストール済み証明書の CN (コモンネーム) が表示されます。
有効期限	インストール済み証明書の有効期限が表示されます。
証明書の種類	インストール済み証明書の種類が表示されます。 ・ユーザー証明書 ・コンピューター証明書

□ 申請中の証明書一覧

KeyManager から行った証明書の申請情報が一覧表示されます。

証明書の申請、申請内容の変更や取り下げ、デバイス登録を行うことができます。なお、取り下げを行った申請情報、およびデバイス登録まで完了した申請情報は、一覧には表示されません。

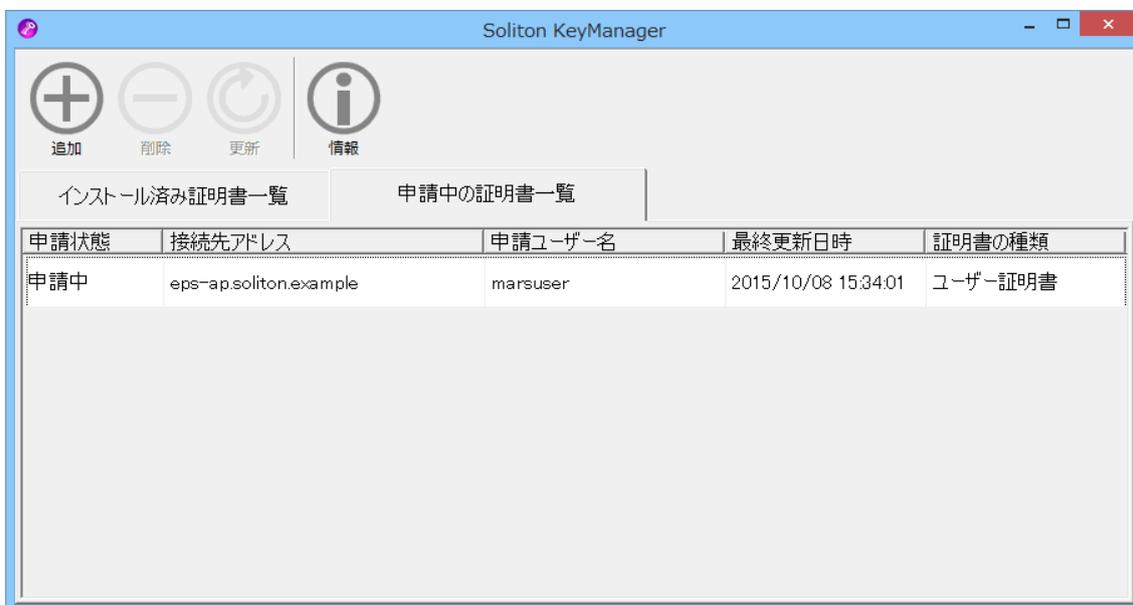


図 3.1.4 申請中の証明書一覧

表 3.1.3 申請中の証明書一覧

項目	説明
申請状態	証明書申請の状態を表示します。 <ul style="list-style-type: none"> ・未申請 : 申請を行っていない状態です。 証明書の申請が却下された場合も申請状態は未申請になります。 ・申請中 : 申請は完了し、承認者による承認待ちの状態です。 ・承認済 : 承認者による承認が完了した状態です。
接続先アドレス	申請時に指定した、接続先のホスト名または IP アドレスが表示されます。
申請ユーザー名	申請時に指定したユーザー ID が表示されます。
最終更新日時	最後に申請先へ接続し、証明書の申請状態を取得した日時が表示されます。
証明書の種類	申請時に指定した証明書の種類が表示されます。 <ul style="list-style-type: none"> ・ユーザー証明書 ・コンピューター証明書

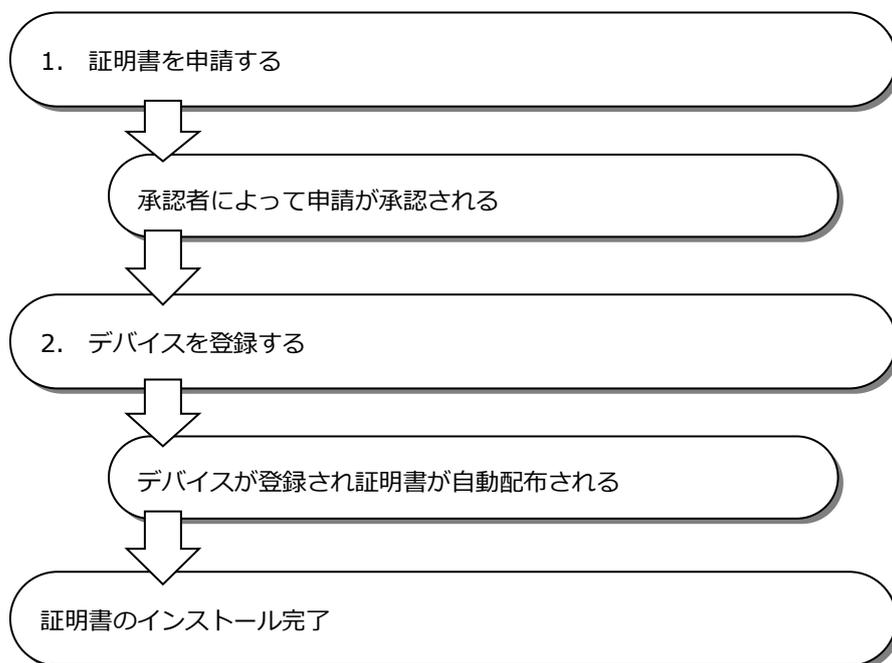
3.2 証明書をインストールする

KeyManager を使用した証明書のインストール方法について説明します。

弊社の NetAttest EPS / NetAttest EPS-ap または ID Manager と連携することで、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や、「プロファイル」として登録されている設定項目を適用することができます。CA 証明書がインストールされていない場合は、同時に CA 証明書のインストールも行います。

なお、SCEP 以外の設定項目は、証明書のインストール後に適用されます。Windows に対応する「プロファイル」の設定項目については、接続先機器の製品マニュアル、およびリリースノートを参照してください。

申請フローの流れは、以下のとおりです。



3.2.1 証明書を申請する

KeyManager を使用して、証明書の申請、申請内容の確認および変更、申請の取り下げを行うことができます。

3.2.1.1 証明書の申請

証明書の申請は、以下の手順で行ってください。

1. KeyManager を起動してください。

2. [申請中の証明書一覧]タブをクリックすると、図 3.2.1 が表示されます。ツールバーの<追加>をクリックしてください。

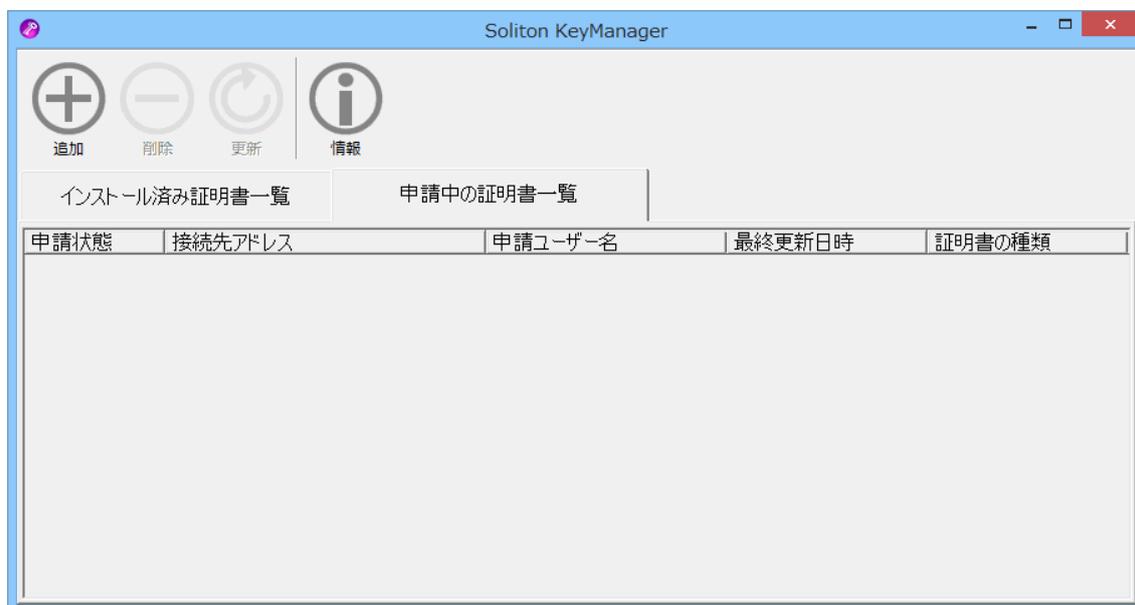


図 3.2.1 申請中の証明書一覧

3. 図 3.2.2 が表示されます。ユーザー証明書を申請する場合は<ユーザー証明書>、コンピューター証明書を申請する場合は<コンピューター証明書>をクリックしてください。

※ここで選択した証明書の種類は、NetAttest EPS-ap および ID Manager 接続後に変更することはできません。

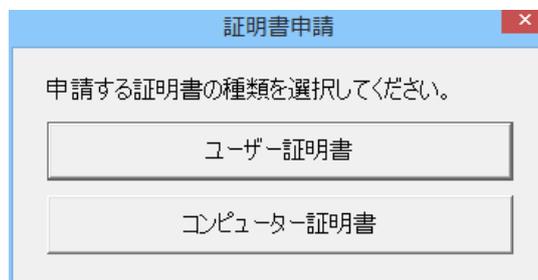


図 3.2.2 証明書申請

4. 図 3.2.3 が表示されます。「ホスト名または IP アドレス」、「ユーザーID」、「パスワード」を入力し、<接続>をクリックしてください。

図 3.2.3 接続

表 3.2.1 接続

項目	説明
ホスト名または IP アドレス (必須)	<p>接続先のホスト名または IP アドレスを指定してください。 使用可能文字：半角英数字（英字は小文字のみ）、コロン(:)、ドット(.)、ハイフン(-)</p> <p>形式：ホスト名の場合は FQDN、 IP アドレスの場合は 10 進ドット形式で指定してください。 ポート番号を指定する場合、ホスト名または IP アドレスとポート番号をコロン (:) で区切って指定してください。 ポート番号は接続先の HTTPS サービスポートを指定してください。 ポート番号の指定がない場合は、443 番ポートが使用されます。</p> <p>デフォルト：設定なし 文字数：最大 64 文字</p>
ユーザーID (必須)	<p>証明書を申請するユーザーID を指定してください。 接続先が ID Manager の場合は、以下の形式で決められたサイト識別子も指定してください。</p> <p>形式 (ID Manager) : ユーザーID@サイト識別子 例 test@example.com</p> <p>デフォルト：設定なし 文字数：最大 64 文字</p>
パスワード (必須)	<p>証明書を申請するユーザーのパスワードを指定してください。</p> <p>デフォルト：設定なし 文字数：最大 253 文字</p>

※NetAttest EPS-ap への接続後、10 分経過するとセッションタイムアウトになります。その場合は、再度接続を行ってください。

5. 図 3.2.4 が表示されます。「通知先メールアドレス」と、必要に応じて「承認者へのメモ」を入力し、<申請開始>をクリックしてください。

※NetAttest EPS-ap にて自動承認が有効に設定されている場合や、ID Manager で申請がすでに承認されている場合、図 3.2.4 の証明書申請画面ではなく、デバイス登録画面が表示されます。この場合は「3.2.2 デバイスを登録する」の手順 4 に進んでください。

図 3.2.4 証明書申請

表 3.2.2 証明書申請

項目	説明
通知先メールアドレス	承認者からの通知メールを受信するメールアドレスを指定してください。 使用可能文字：半角英数字、アスタリスク(*)、アットマーク(@)、アンダーバー(_)、アンパサンド(&)、イコール(=)、エクスクラメーション(!)、クエスチョン(?)、シングルクォーテーション(')、スラッシュ(/)、ダラー(\$)、チルダ(~)、中カッコ({})、ドット(.)、ナンバー(#)、ハイフン(-)、ハット(^)、バッククォーテーション(`)、パイプ()、パーセント(%)、プラス(+) ・接続先が NetAttest EPS-ap の場合 デフォルト：NetAttest EPS に登録されているメールアドレス ・接続先が ID Manager の場合 デフォルト：ID Manager に登録されているメールアドレス 文字数：最大 256 文字
承認者へのメモ	承認者に連絡しておく情報がある場合に入力してください。 デフォルト：[コンピューター名 (「user」 or 「comp」)]： ※「承認者へのメモ」にデフォルトの文字列は表示されません。 ※デフォルトの文字列は申請する際、自動的に付け足されます。 ※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。 文字数：最大 1024- (コンピューター名の文字数+9) 文字 例 コンピューター名が「EXAMPLE-PC」(10 文字) の場合 1024- (10+9) = 最大 1005 文字
証明書の種類	図 3.2.2 で選択した証明書の種類が有効になっています。 変更することはできません。

項目	説明
管理者の連絡先	
メールアドレス	管理者によって連絡先メールアドレスが設定されている場合のみ表示されます。管理者にメールで問い合わせを行う場合には、このメールアドレスを使用してください。
電話番号	管理者によって連絡先電話番号が設定されている場合のみ表示されます。管理者に電話で問い合わせを行う場合には、この電話番号を使用してください。

※図 3.2.4 で<キャンセル>をクリックした場合は証明書申請がキャンセルされ、申請中の証明書一覧に [申請状態]が「未申請」の状態で作成されます。申請中の証明書一覧に保存されている情報を変更する場合は、「3.2.1.2 申請内容の確認、変更」を参照してください。

6. 図 3.2.5 が表示されます。<OK>をクリックしてください。

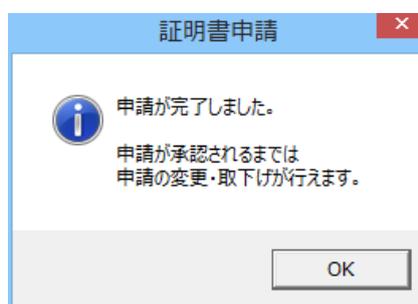


図 3.2.5 証明書の申請完了

7. 図 3.2.6 が表示されます。申請した情報が表示されていることを確認してください。

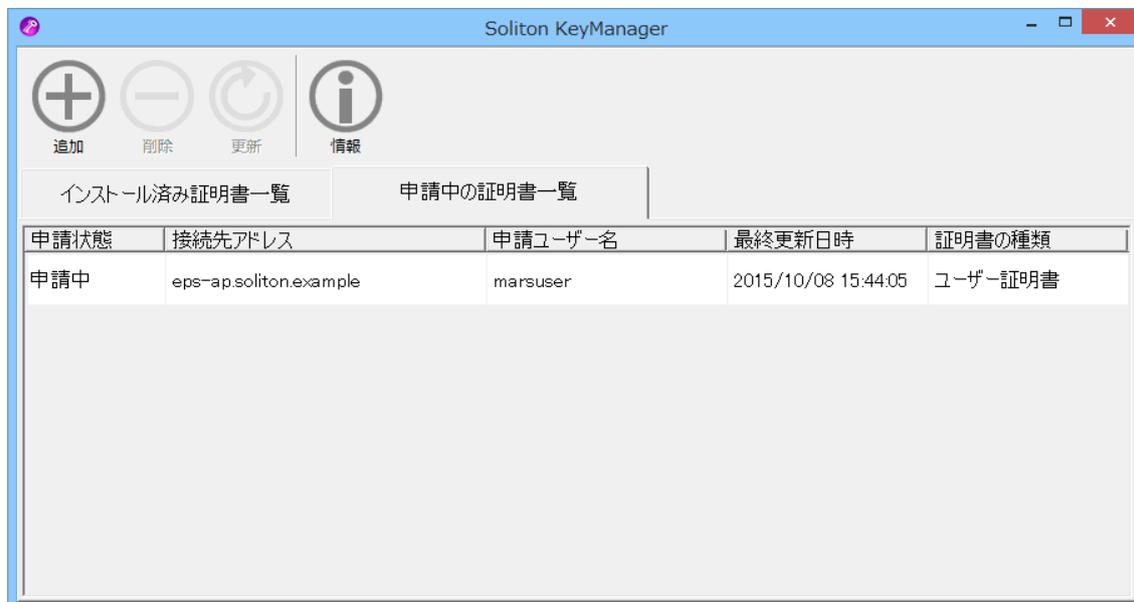


図 3.2.6 申請中の証明書一覧

3.2.1.2 申請内容の確認、変更

証明書の申請内容および申請状況は、申請中の証明書一覧から確認することができ、承認者によって承認されるまでは変更することができます。

申請内容の確認、変更は、以下の手順で行ってください。

1. KeyManager を起動してください。
2. [申請中の証明書一覧]タブをクリックすると、図 3.2.7 が表示されます。確認または変更を行う証明書申請をダブルクリックしてください。

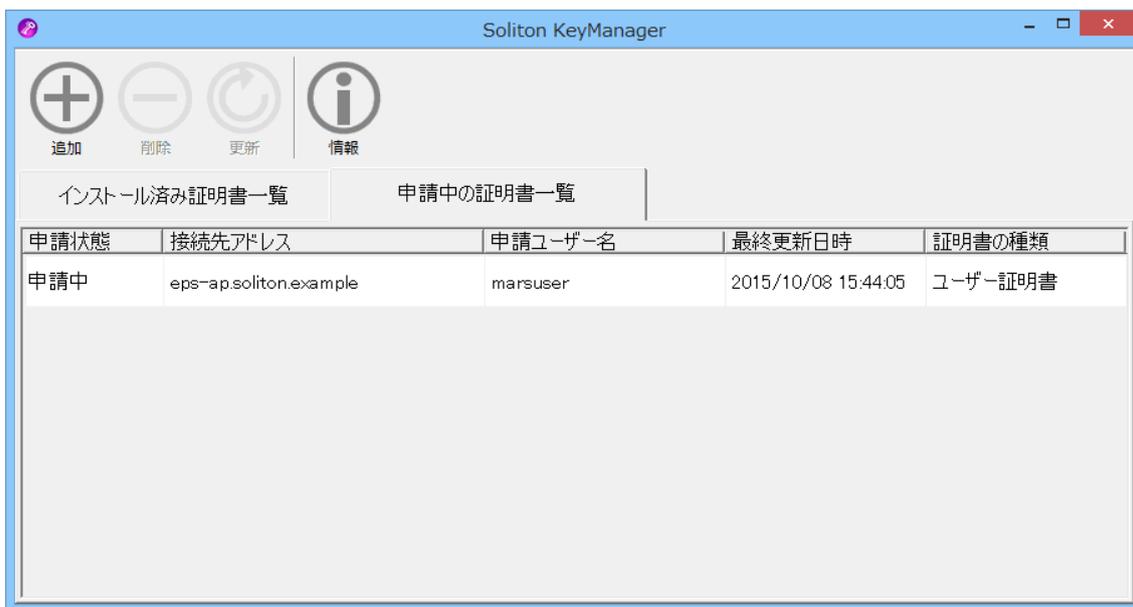


図 3.2.7 申請中の証明書一覧

3. 図 3.2.8 が表示されます。申請時に指定した「ホスト名または IP アドレス」と「ユーザーID」が編集不可の状態を設定されます。「パスワード」を入力し<接続>をクリックしてください。

※KeyManager 起動後、2 回目以降の接続時には、前回接続時のパスワードが設定され、自動で接続を行います。

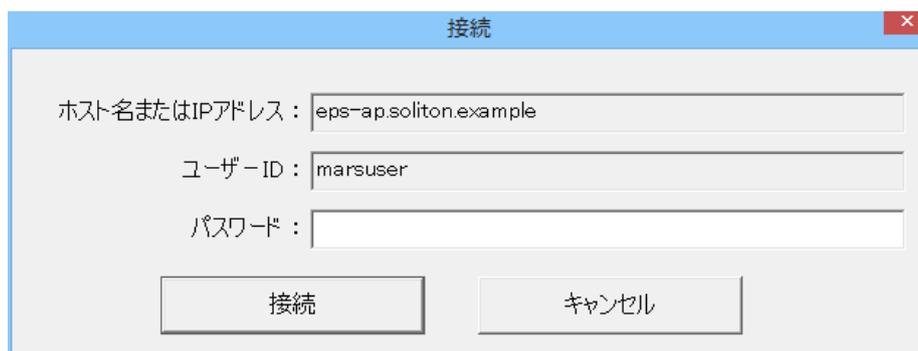


図 3.2.8 接続

4. 図 3.2.9 が表示されます。必要に応じて申請内容を変更し<申請内容の変更>をクリックしてください。

申請内容に変更がない場合は、<キャンセル>をクリックしてください。<申請を取上げる>をクリックすると、申請を取り下げることができます。



図 3.2.9 申請内容確認

5. 図 3.2.9 で<申請内容の変更>をクリックすると確認メッセージが表示されます。<はい>をクリックすると図 3.2.10 が表示されます。<OK>をクリックしてください。

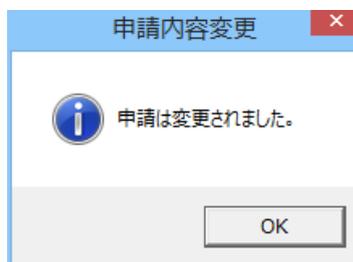


図 3.2.10 申請内容の変更完了

3.2.1.3 申請の取り下げ

証明書の申請は、デバイスの登録を行うまで取り下げることができます。

申請の取り下げは、以下の手順で行ってください。

1. KeyManager を起動してください。
2. [申請中の証明書一覧]タブをクリックすると、図 3.2.11 が表示されます。取り下げる証明書申請を選択し、ツールバーの<削除>をクリックしてください。



図 3.2.11 申請中の証明書一覧

3. 図 3.2.12 が表示されます。<はい>をクリックしてください。

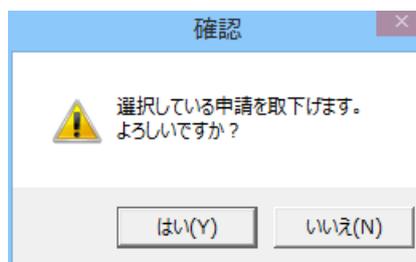


図 3.2.12 取り下げ確認

※申請状態が「未申請」である場合は、図 3.2.13 が表示されます。<はい>をクリックしてください。NetAttest EPS-ap または ID Manager への接続は行わずに、申請中の証明書一覧から削除されます。

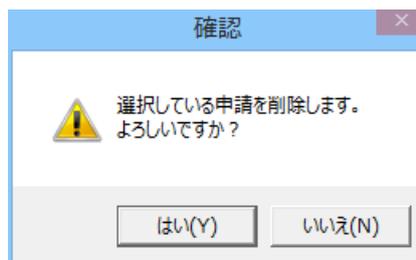


図 3.2.13 削除確認

4. 図 3.2.14 が表示されます。申請時に指定した接続先とユーザーID が編集不可の状態を設定されます。「パスワード」を入力し<接続>をクリックしてください。

※KeyManager 起動後、2 回目以降の接続時には、前回接続時のパスワードが設定され、自動で接続を行います。

※NetAttest EPS-ap または ID Manager への接続が行えない状態で申請中の証明書一覧から申請を削除した場合、KeyManager から申請を取り下げることができなくなります。

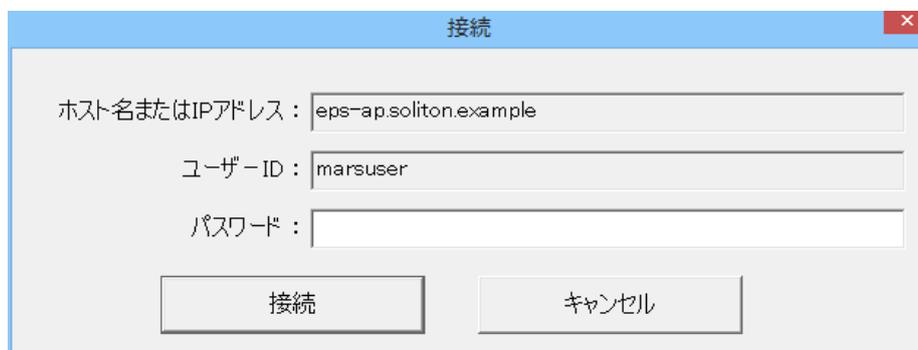


図 3.2.14 接続

5. 図 3.2.15 が表示されます。<OK>をクリックしてください。取り下げた証明書申請は、申請中の証明書一覧から削除されます。

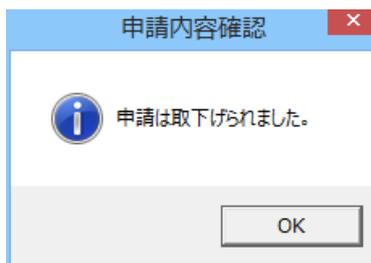


図 3.2.15 申請の取り下げ完了

証明書の申請は、申請内容確認画面で内容を確認してから取り下げることができます。手順については、「3.2.1.2 申請内容の確認、変更」を参照してください。

3.2.2 デバイスを登録する

承認者によって申請が承認された場合、デバイス登録を行うことで証明書をインストールすることができます。

CA 証明書がインストールされていない場合は、CA 証明書も同時にインストールされます。ただし、CA 証明書については KeyManager から確認、削除することはできません。

なお、管理者によって通知メールが設定されている場合は、証明書の申請時に指定した「通知メールアドレス」宛てに送信されるメールにて、承認者による承認または却下を確認することができます。

デバイスの登録および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. KeyManager を起動してください。
2. [申請中の証明書一覧]タブをクリックすると、図 3.2.16 が表示されます。申請状態が「承認済」の証明書申請をダブルクリックするか、証明書申請を選択しツールバーの<更新>をクリックしてください。

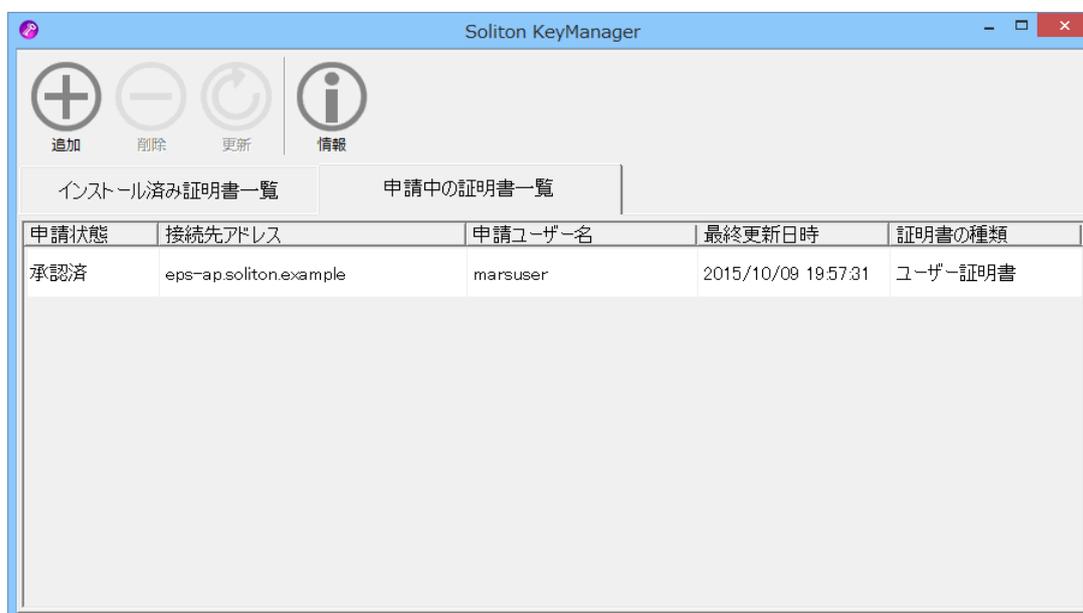


図 3.2.16 申請中の証明書一覧

3. 図 3.2.17 が表示されます。申請時に指定した「ホスト名または IP アドレス」と「ユーザー ID」が編集不可の状態を設定されます。「パスワード」を入力し<接続>をクリックしてください。

※KeyManager 起動後、2 回目以降の接続時には、前回接続時のパスワードが設定され、自動で接続を行います。

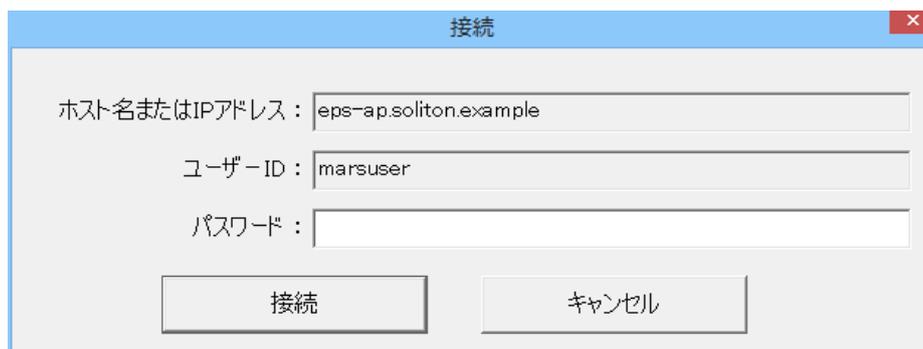


図 3.2.17 接続

4. 図 3.2.18 が表示されます。<デバイス登録開始>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。

なお、<キャンセル>をクリックするとデバイス登録のキャンセル、<申請を取下げると証明書申請の取り下げを行うことができます。



図 3.2.18 デバイス登録

5. CA 証明書がインストールされていない場合は、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。
6. プロファイルに Wi-Fi 設定項目を含む場合は、図 3.2.19 が表示されます。<OK>をクリックしてください。このメッセージは、プロファイルに設定されている SSID ごとに表示されます。

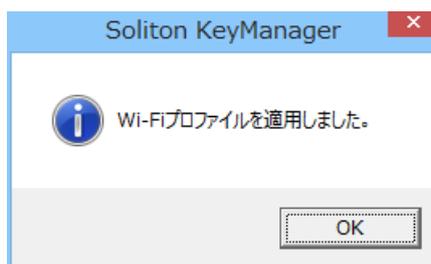


図 3.2.19 プロファイルの適用完了

7. 図 3.2.20 が表示されます。<OK>をクリックしてください。

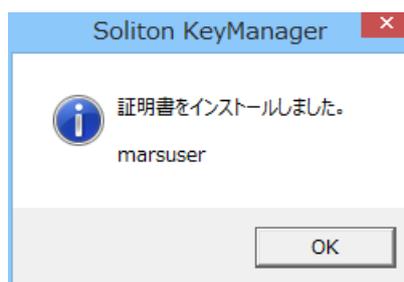


図 3.2.20 証明書のインストール完了

8. 図 3.2.21 が表示されます。インストール済み証明書一覧にインストールした証明書が表示されていることを確認してください。

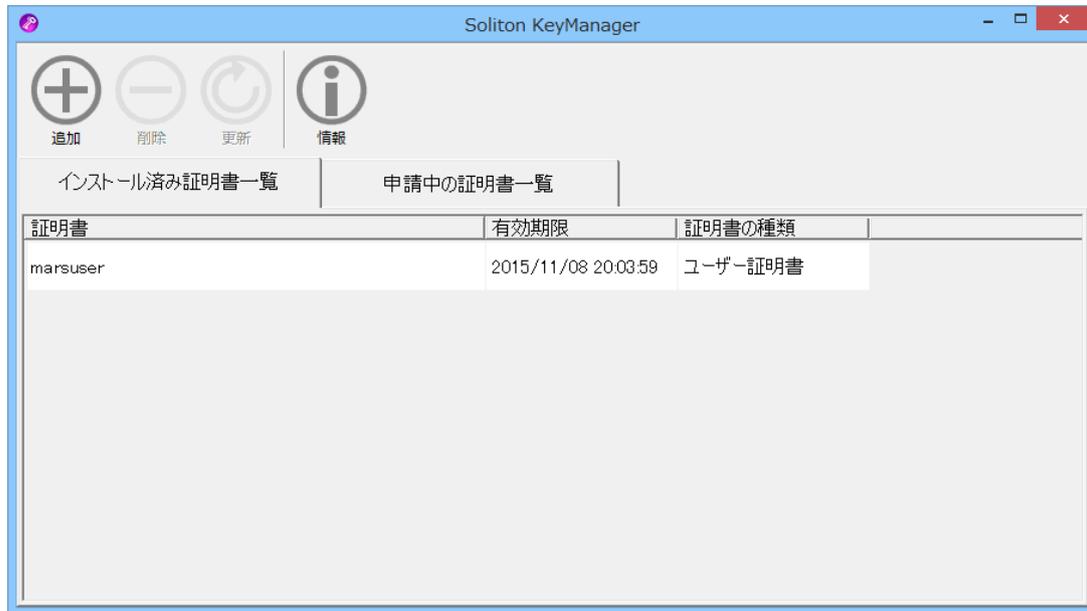


図 3.2.21 インストール済み証明書一覧



証明書の申請が承認者によって却下された場合、申請中の証明書一覧の[申請状況]が「未申請」に更新されます。必要に応じて申請内容を修正し、再度申請を行ってください。

3.3 証明書を確認/削除/更新する

KeyManager を使用してインストールした証明書の確認および削除、有効期限が近くなった場合などに証明書を更新する方法について説明します。

3.3.1 証明書を確認する

証明書の確認は、以下の手順で行ってください。

1. KeyManager を起動してください。

2. 図 3.3.1 が表示されます。確認する証明書をダブルクリックしてください。または、証明書を右クリックして表示されるメニューから[詳細表示]をクリックしてください。

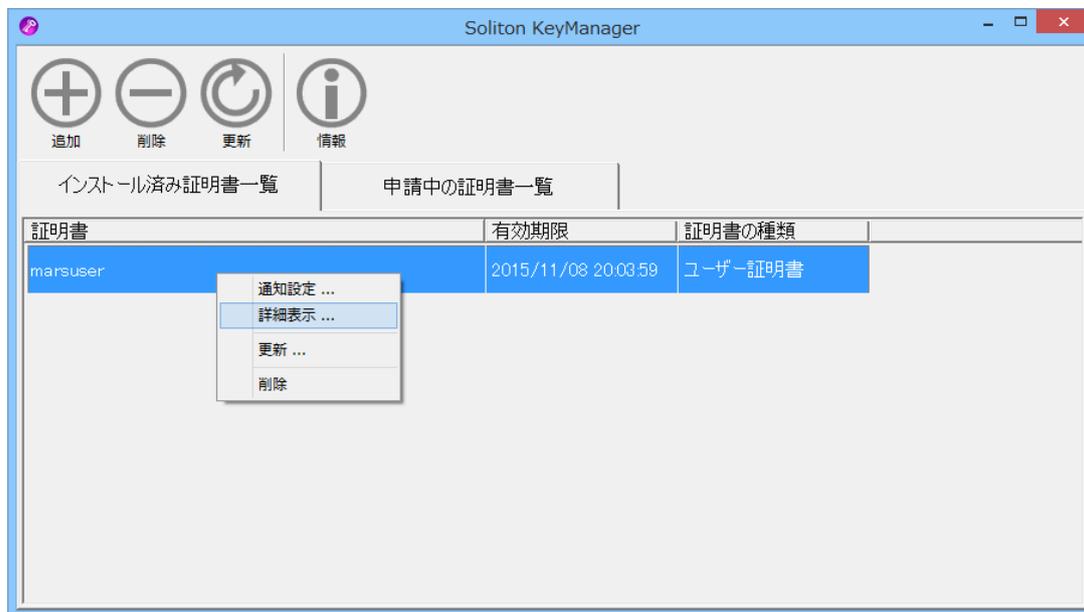


図 3.3.1 インストール済み証明書一覧

3. 図 3.3.2 が表示されます。証明書を閉じる場合は、<OK>をクリックしてください。

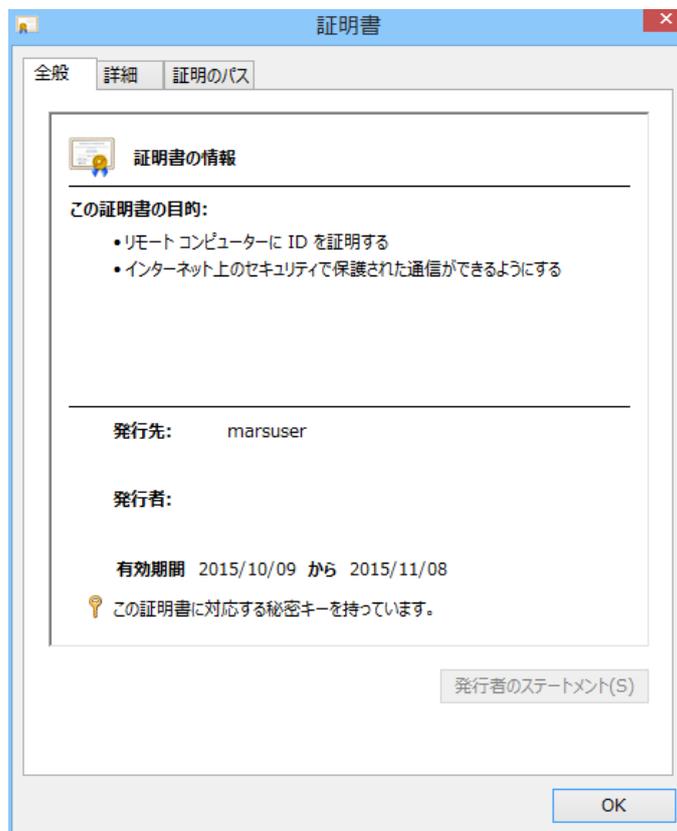


図 3.3.2 証明書

3.3.2 証明書を削除する

証明書の削除は、以下の手順で行ってください。

1. KeyManager を起動してください。
2. 図 3.3.3 が表示されます。削除する証明書を選択し、ツールバーの<削除>をクリックしてください。または、証明書を右クリックして表示されるメニューから[削除]をクリックしてください。

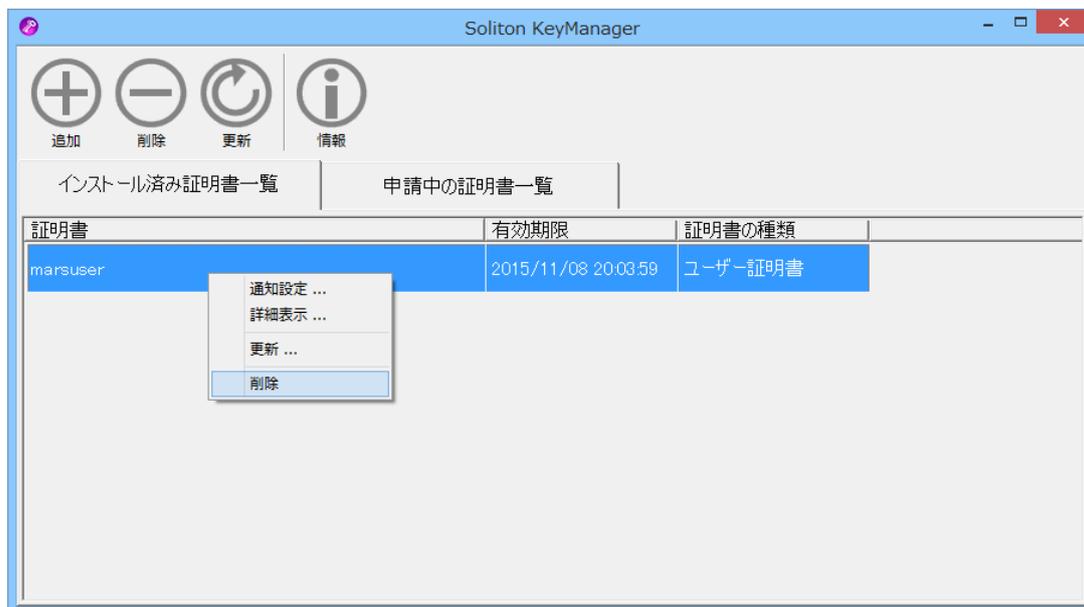


図 3.3.3 インストール済み証明書一覧

3. 図 3.3.4 が表示されます。<はい>をクリックしてください。

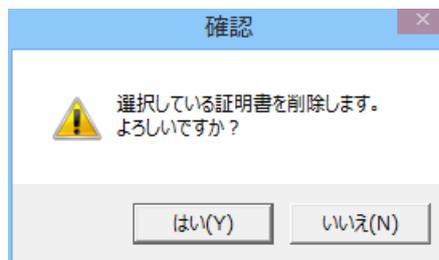


図 3.3.4 削除確認メッセージ

4. 図 3.3.5 が表示されます。<OK>をクリックしてください。

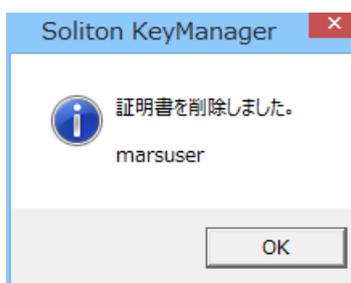


図 3.3.5 証明書の削除完了

5. 図 3.3.6 が表示されます。インストール済みの証明書一覧に、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。

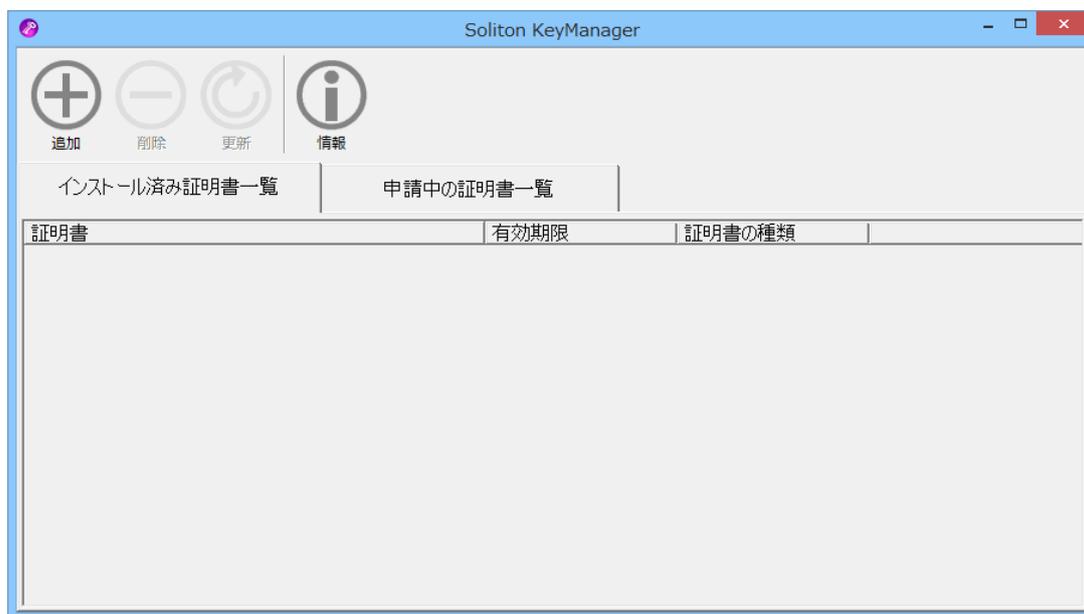


図 3.3.6 インストール済み証明書一覧



インストール済み証明書一覧にある証明書情報を削除すると証明書ストアに格納された証明書が削除されます。コンピューター証明書を削除した場合は、該当するコンピューター証明書を利用した端末内の他のユーザーにも影響するためご注意ください。

3.3.3 証明書を更新する

有効期限が近くなった証明書などは、申請時の情報を使用して証明書を再申請することができます。

証明書の更新は、以下の手順で行ってください。

1. KeyManager を起動してください。
2. 図 3.3.7 が表示されます。更新する証明書を選択し、ツールバーの<更新>をクリックしてください。または、証明書を右クリックして表示されるメニューから[更新]をクリックしてください。

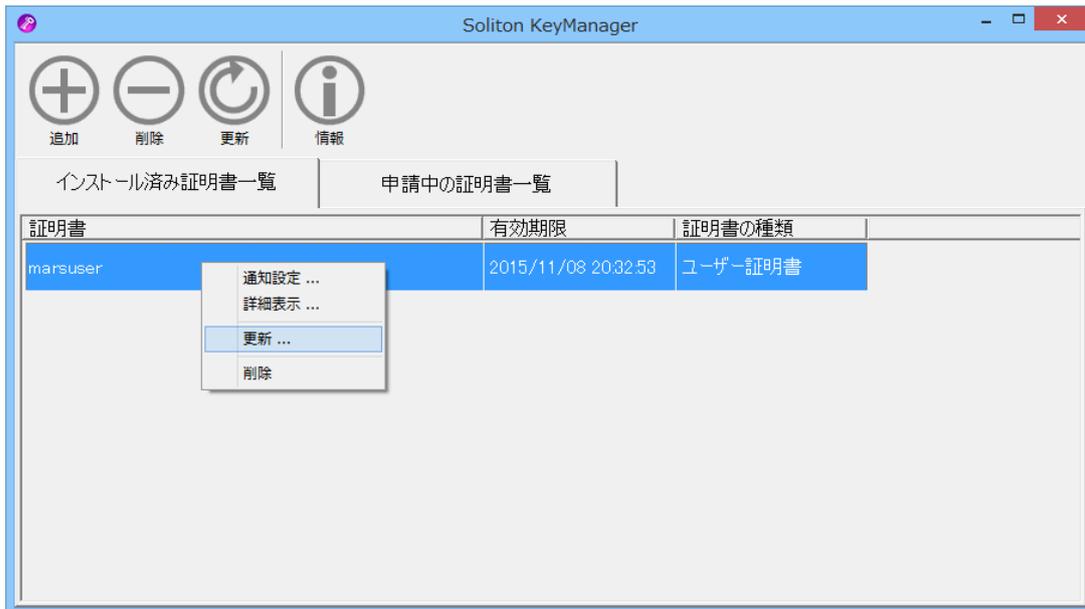


図 3.3.7 インストール済み証明書一覧

3. 図 3.3.8 が表示されます。「パスワード」を入力し、<接続>をクリックしてください。
以降の手順は証明書を申請する際と同様です。「3.2.1.1 証明書の申請」の手順 5 に進んでください。
なお、証明書の更新を行った場合、古い証明書（図 3.3.7 で選択した証明書）は自動で削除されます。



図 3.3.8 接続



図 3.3.8 の「ホスト名または IP アドレス」「ユーザーID」は V1.2.3 以降の KeyManager で取得した証明書を更新する際に入力済みの状態になります。

3.4 有効期限の通知機能を使用する

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。

ユーザー証明書の場合は、該当するユーザー証明書をインストールしているユーザーに対してのみ通知され、コンピューター証明書の場合は、全ユーザーに対して通知が行われます。

3.4.1 デフォルトの設定を変更する

インストールまたは更新する証明書の、有効期限通知に関するデフォルトの設定を変更することができます。

以降、インストールまたは更新する証明書には、ここで設定した内容が反映されるようになります。

証明書の有効期限通知に関するデフォルトの設定を変更する手順は、以下のとおりです。

1. KeyManager を起動し、ツールバーの<情報>をクリックしてください。
2. [通知設定]タブにて証明書の有効期限通知に関する設定を行い、<OK>をクリックしてください。

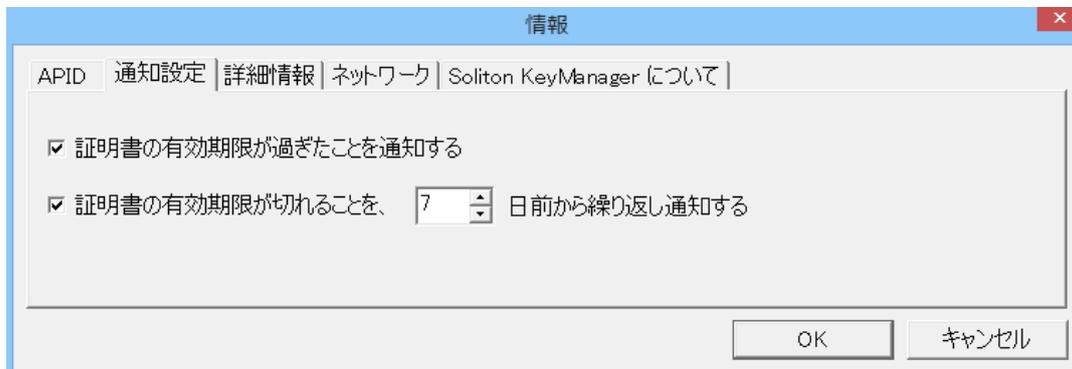


図 3.4.1 通知設定タブ

表 3.4.1 通知設定タブ

項目	説明
証明書の有効期限が過ぎたことを通知する	証明書の有効期限が過ぎたことを通知する場合は、チェックしてください。 デフォルト：チェックあり（通知する）
証明書の有効期限が切れることを、～日前から繰り返し通知する	証明書の有効期限切れを事前に通知する場合は、チェックしてください。 デフォルト：チェックあり（通知する）
～日前	[証明書の有効期限が切れることを、～日前から繰り返し通知する]を チェックしている場合に有効になります。 有効期限の何日前から通知を開始するか指定してください。 デフォルト：7 日前 設定可能範囲：1～120 日前

3.4.2 証明書単位で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。

1. KeyManager を起動してください。
2. 図 3.4.2 が表示されます。設定を変更する証明書を右クリックし、表示されるメニューから[通知設定]をクリックしてください。

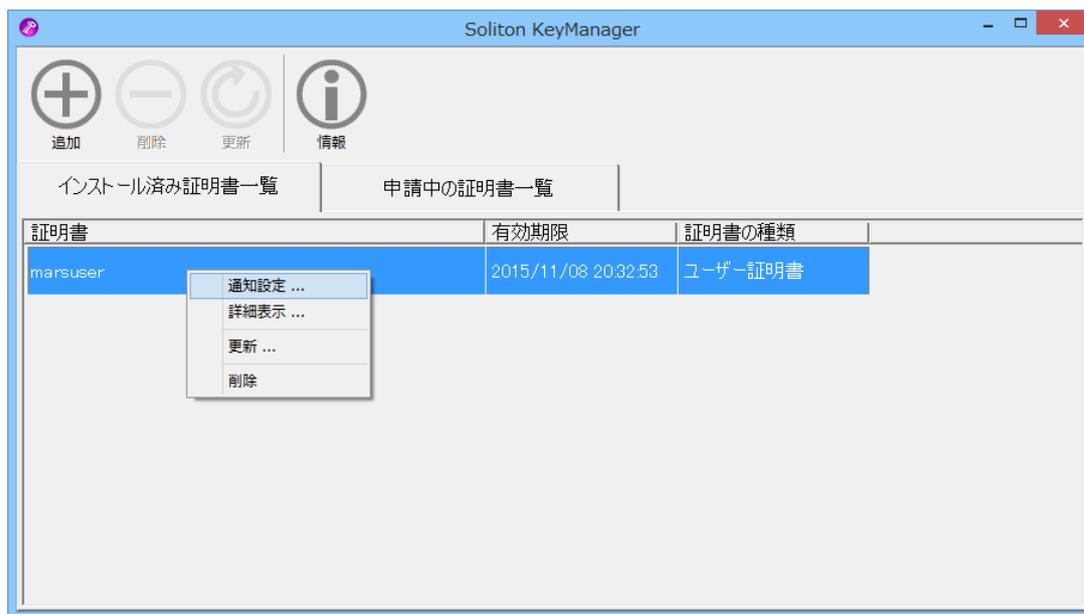


図 3.4.2 インストール済み証明書一覧

3. 図 3.4.3 が表示されます。設定項目および入力仕様は、図 3.4.1 と同様です。証明書の有効期限通知に関する設定を行い、<OK>をクリックしてください。

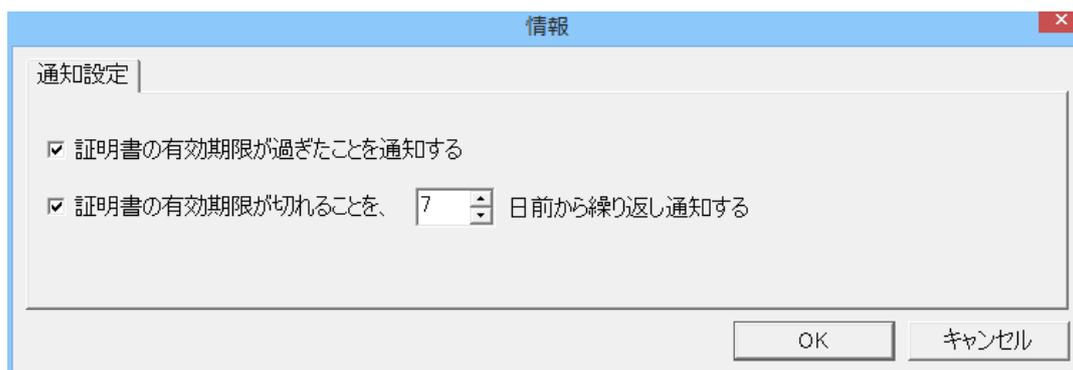


図 3.4.3 通知設定タブ

□ 有効期限切れ間近のメッセージ通知例

証明書の有効期限切れ間近になった場合、KeyManager が起動し、図 3.4.4 のメッセージが表示されます。



図 3.4.4 期限切れ間近のメッセージ通知例

表 3.4.2 期限切れ間近のメッセージ通知例

項目	説明
証明書	証明書の CN (コモンネーム) が表示されます。
有効期限	証明書の有効期限が表示されます。
証明書の種類	証明書の種類が表示されます。 ・ユーザー証明書 ・コンピューター証明書

また、KeyManager のインストール済み証明書一覧では、有効期限切れ間近になった証明書は赤色で表示されるようになります。

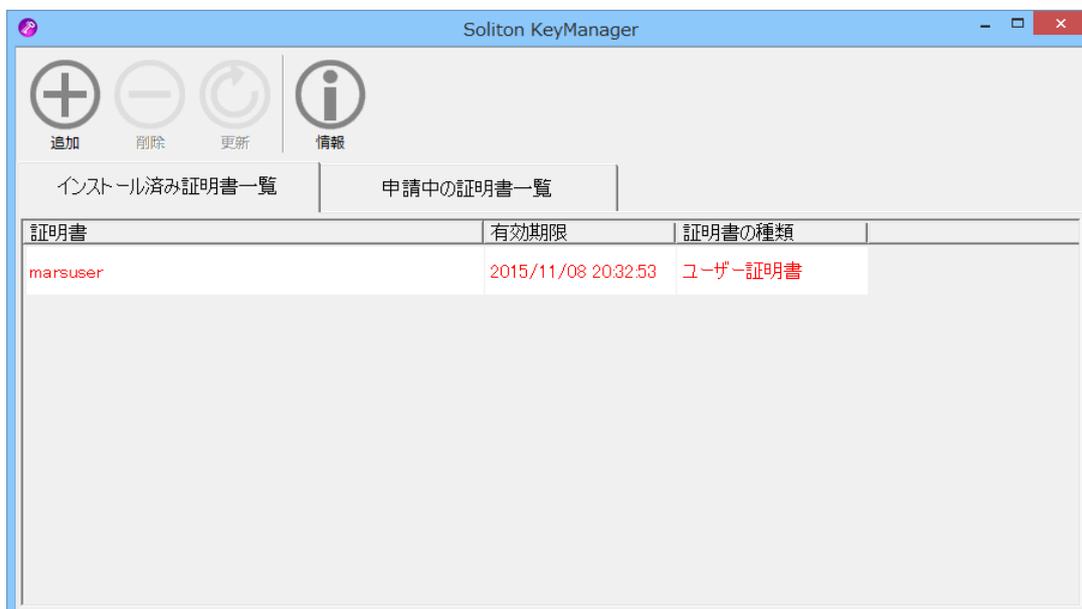


図 3.4.5 インストール済み証明書一覧

□ 有効期限切れのメッセージ通知画面例

証明書の有効期限が切れた場合、KeyManager が起動し、図 3.4.6 のメッセージが表示されます。表示される項目は、有効期限切れ間近のメッセージと同様です。



図 3.4.6 有効期限切れのメッセージ通知例

また、KeyManager のインストール済み証明書一覧では、有効期限が切れた証明書は灰色で表示されるようになります。

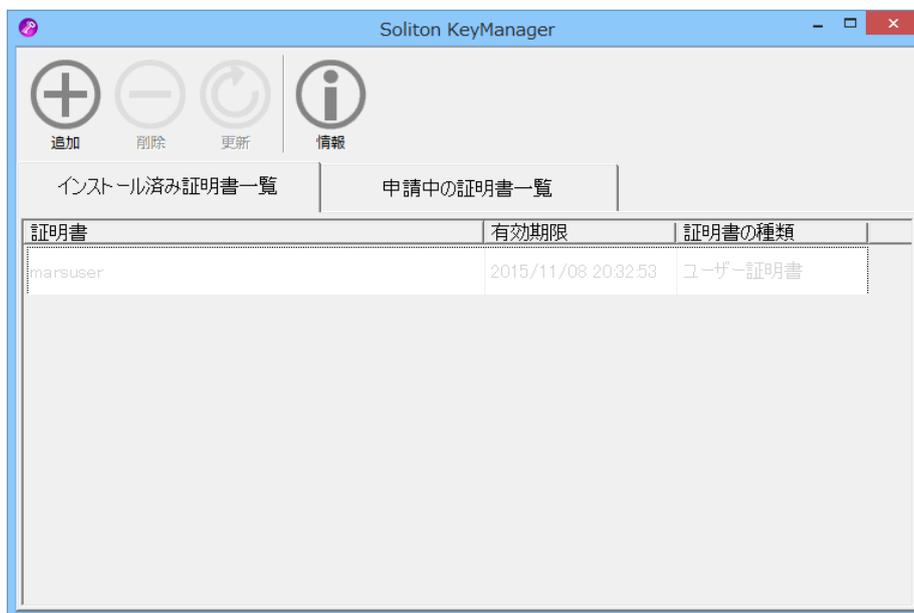


図 3.4.7 インストール済み証明書一覧



- 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間に通知されます。
- 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を考慮し、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。
- 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。

4 KeyManager 情報の確認方法

KeyManager の APID の確認および APID をメールで送信する方法、バージョンの確認方法について説明します。

4.1 APID を確認する

KeyManager の APID を確認する方法、メールで送信する方法について説明します。

APID は、NetAttest EPS-ap または ID Manager に登録するデバイスを一意に識別するための ID です。UDID/APID チェックが有効に設定されている場合、デバイスを登録する前に APID の登録が必要になります。KeyManager では、管理者に APID をメールで送信することができます。



KeyManager V1.0.0 で証明書申請を行う際に使用された APID は、KeyManager V1.0.1 以降の「APID (コンピューター)」と同一です。既に KeyManager V1.0.0 でユーザー証明書をインストールしている環境で新たに KeyManager V1.0.1 以降でコンピューター証明書を申請した場合、利用するユーザーID によって以下のような動作となります。

- ユーザー証明書をインストールしたユーザーID とコンピューター証明書を申請したユーザーID が同じ場合、同一のユーザーID/APID からの申請と判断され、デバイス登録情報が上書きされます。
- ユーザー証明書をインストールしたユーザーID とコンピューター証明書を申請したユーザーID が異なる場合、コンピューター証明書は取得できません。異なるユーザーID でコンピューター証明書を取得するためには、KeyManager V1.0.0 で登録したデバイス情報を削除してください。

APID の確認およびメールで送信する手順は、以下のとおりです。

1. KeyManager を起動し、ツールバーの<情報>をクリックしてください。
2. 図 4.1.1 が表示され、[APID]タブにて APID を確認することができます。

APID(ユーザー) : ユーザー証明書申請時に登録する APID です。

APID(コンピューター) : コンピューター証明書申請時に登録する APID です。

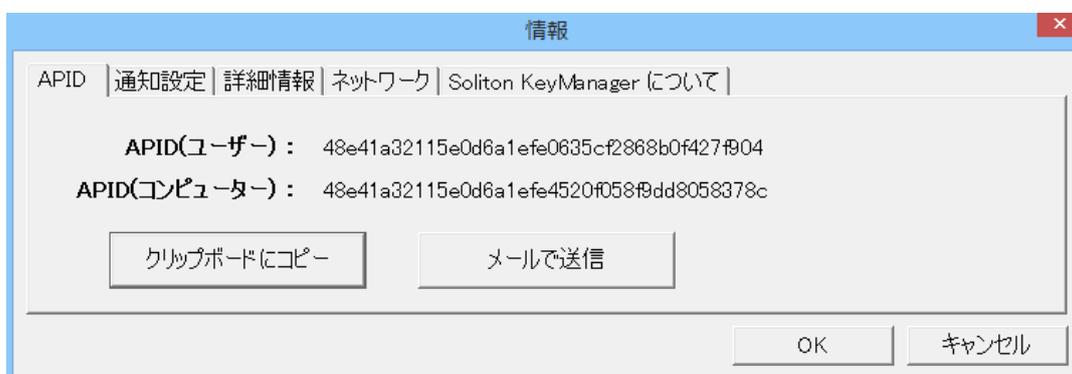


図 4.1.1 APID タブ

□ APID をクリップボードにコピーしたい場合

図 4.1.1 で<クリップボードにコピー>をクリックすると図 4.1.2 が表示され、[APID]、および [Information](「コンピューター名」「ログインユーザーID」)をクリップボードにコピーすることができます。

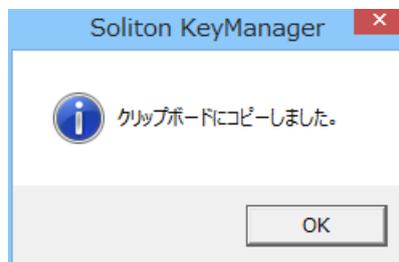


図 4.1.2 クリップボードにコピー

□ APID をメールで送信したい場合

図 4.1.1 で<メールで送信>をクリックすると、コンピューターにデフォルト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[API]と[Information](「コンピューター名」「ログインユーザーID」)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。

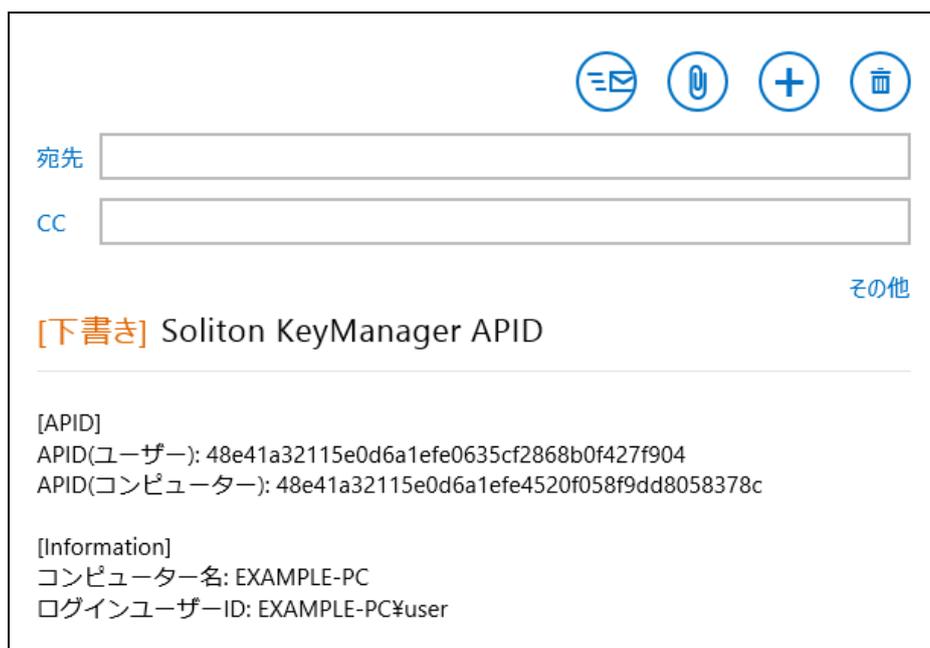


図 4.1.3 メール作成画面(例)

4.2 MAC アドレスを確認する

KeyManager が取得した MAC アドレスの確認方法について記載します。

1. KeyManager を起動し、ツールバーの<情報>をクリックしてください。
2. [詳細情報]タブにて MAC アドレスを確認することができます。

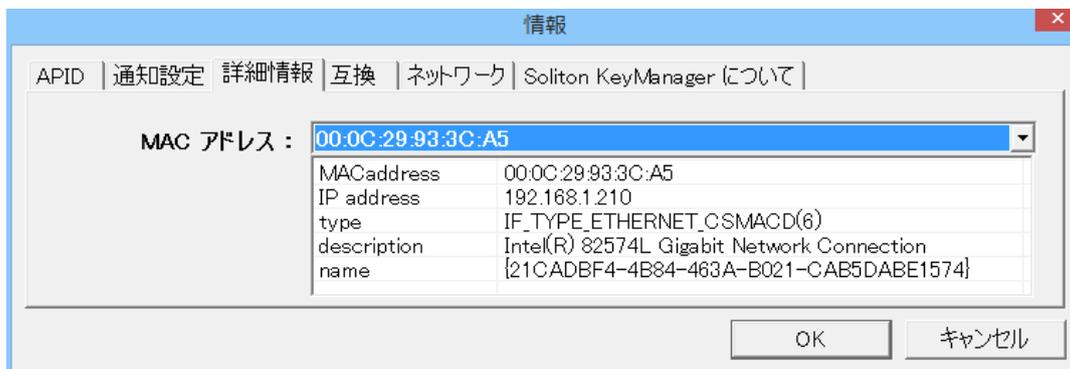


図 4.2.1 詳細情報

4.3 バージョンを確認する

KeyManager のバージョン確認方法について説明します。

1. KeyManager を起動し、ツールバーの<情報>をクリックしてください。
2. [Soliton KeyManager について]タブにてバージョンを確認することができます。



図 4.3.1 Soliton KeyManager について

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してください。

Soliton FAQ

<http://faq1.soliton.co.jp/>

5.1 申請・デバイス登録に失敗する

KeyManager からの通信が正常に行うことができない環境では、申請やデバイス登録に失敗する場合があります。

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

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、申請やデバイス登録に失敗します。例外設定などにより通信を阻害しないように構成してください。

KeyManager が使用する通信ポートについては FAQ を参照してください。

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

<http://faq1.soliton.co.jp/faq/show/5896>

5.1.1 プロキシサーバー

ネットワーク上にプロキシサーバーがある環境にて、プロキシサーバーの構成や設定により申請やデバイス登録が行えない場合があります。

ここでは KeyManager からの通信をプロキシサーバー経由させない場合の設定方法を記載します。

通常は、設定を変更する必要はありません。

1. KeyManager を起動し、ツールバーの<情報>をクリックしてください。
2. [ネットワーク]タブをクリックしてください。図 5.1.1 が表示されます。

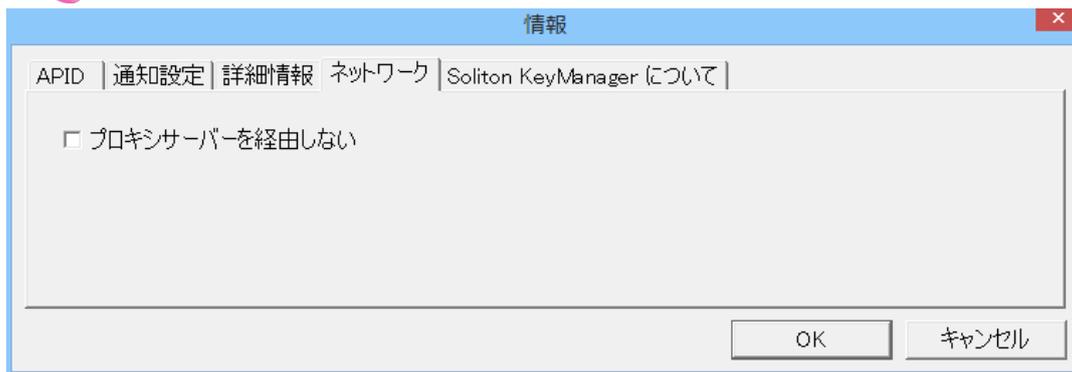


図 5.1.1 ネットワーク

3. [プロキシサーバーを経由しない]にチェックを入れ、<OK>をクリックしてください。

5.2 互換オプション

KeyManager V1.2.1 から APID の生成方法が変わったため、V1.2.0 以前の APID をデバイスチェック機能などで使用している場合、証明書取得時に問題が発生する可能性があります。互換オプションを有効にすることで V1.2.0 以前と同じ方法で APID を生成します。

互換オプションを有効にする手順は、以下の通りです。

1. KeyManager を起動し、ツールバーの<情報>をクリックしてください。
2. [互換]タブをクリックしてください。図 5.2.1 が表示されます。

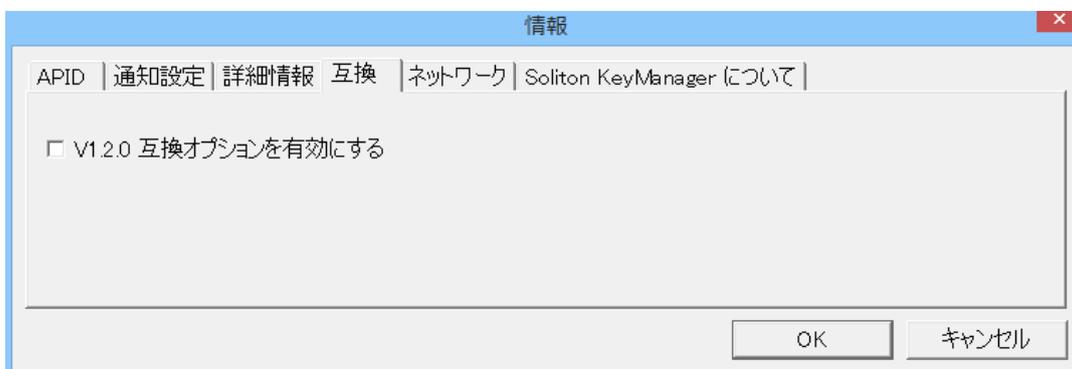


図 5.2.1 互換

3. [V1.2.0 互換オプションを有効にする]にチェックを入れると図 5.2.2 が表示されます。内容を確認し <OK>をクリックしてください。

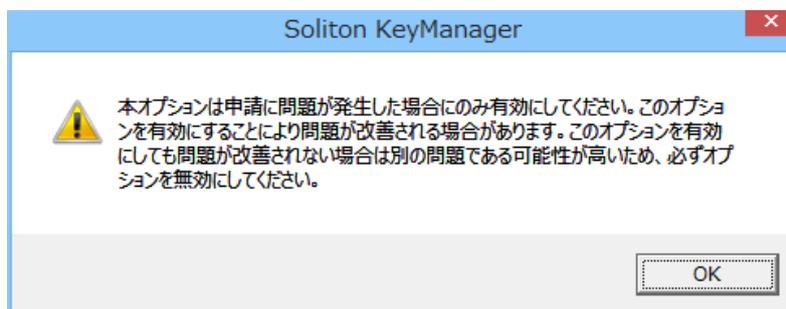


図 5.2.2 互換オプション説明



- V1.2.0 から V1.2.1 以降にアップデートした場合、[V1.2.0 互換オプションを有効にする]のデフォルト値は有効です。V1.2.1 以降を新規にインストールした場合、[V1.2.0 互換オプションを有効にする]のデフォルト値は無効になります。
- 互換オプションが無効の状態でも V1.2.3 以降にアップデートした場合、[互換]タブは非表示になります。

5.3 診断情報

KeyManager を使用中に障害が発生した場合などに、発生した障害を解析するために必要となる動作環境、動作状況などの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、お客様に環境を伺う、状況を調べていただくなどのお客様にかかる手間を軽減することができます。

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。

5.3.1 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. KeyManager を起動し、ツールバーの<情報>をクリックしてください。
2. [Soliton KeyManager について]タブをクリックしてください。

3. 図 5.3.1 が表示されます。<診断情報取得>をクリックしてください。



図 5.3.1 Soliton KeyManager について

4. 図 5.3.2 が表示されます。[同意する]をチェックし、<次へ>をクリックしてください。

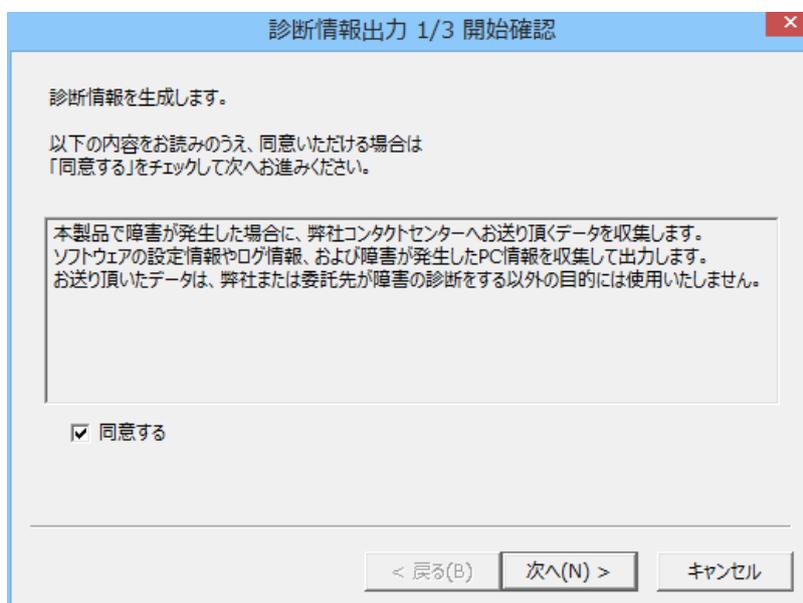


図 5.3.2 診断情報出力(1/3)

5. 診断情報の収集が終了すると図 5.3.3 が表示されます。<次へ>をクリックしてください。
※診断情報の収集には数分かかることがあります。



図 5.3.3 診断情報出力(2/3)

6. 図 5.3.4 が表示されます。必要に応じて診断情報ファイルの保存先を変更してください。<完了>をクリックすると zip 形式で圧縮した診断情報が指定した保存先へ出力されます。

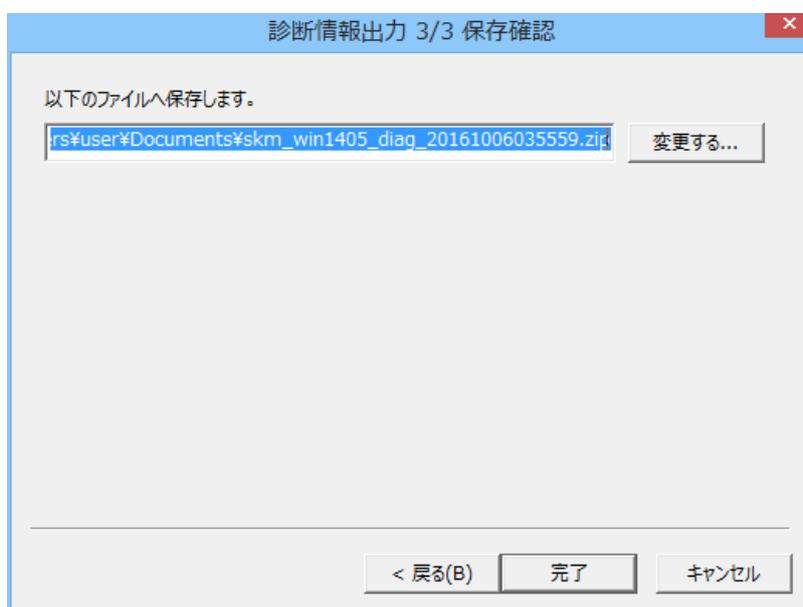


図 5.3.4 診断情報出力(3/3)



Soliton KeyManager

Windows 版 Soliton KeyManager V1.4 説明書

2016年10月15日	第1版
2017年01月17日	第2版
2017年12月07日	第3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

<http://www.soliton.co.jp/>

Copyright © 2013-2017, Soliton Systems K.K., All rights reserved.



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。

本書の一部または全部について株式会社ソリトンシステムズの承諾を得ずに、いかなる方法においても複写・複製・転載・加工等これらに類する行為を禁じます。