

導入・操作の手引  
Installation and Operation Manual

---

SSL 証明書管理ソフトウェア

# Smart Cert Manage

第3版

2023年10月16日

U00147356803

セイコーソリューションズ株式会社

---

Windows、.NET Framework は米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。

本書に記載されている会社名、製品名はそれぞれ各社の商標および登録商標です。

(C) Copyright Seiko Solutions Inc. 2023

1. セイコーソリューションズ株式会社の文書による許可なく、本書の全部または一部の複製・転載および改変等を行う事は出来ません。
2. 本書の内容については将来予告なしに変更する事があります。

# 目 次

1. はじめに .....	6
1.1. SSL 証明書管理ソフトウェア「SmartCertManage」概要 .....	6
1.2. 機能一覧 .....	7
1.3. システム要件 .....	9
1.3.1. ハードウェア要件 .....	9
1.3.2. システム要件 .....	9
1.4. ユーザー権限 .....	10
2. インストール .....	11
3. アンインストール .....	23
4. バージョンアップ .....	31
5. 初期設定 .....	32
5.1. 初期設定 .....	33
6. 共通設定 .....	42
6.1. ダッシュボード .....	42
6.1.1. サービスの稼働状態画面 .....	44
6.1.2. バージョン照会画面 .....	45
6.2. 一般設定 .....	46
6.2.1. プロキシ設定 .....	46
6.2.2. 各プロセス完了待ちタイマー設定 .....	46
6.3. ユーザーグループ設定 .....	47
6.3.1. ユーザーグループ選択 .....	47
6.3.2. 通知設定テーブル選択 .....	47
6.3.3. 所属メンバー設定 .....	48
6.4. ユーザー一覧 .....	49
6.5. ユーザー設定 .....	50
6.5.1. ユーザーID 設定 .....	50
6.5.2. ユーザー権限設定 .....	50
6.5.3. ユーザーパスワード設定 .....	51
6.5.4. ユーザー連絡先設定 .....	51
6.5.5. ユーザー追加/更新/削除 .....	51
6.6. メール送信設定 .....	52
6.6.1. 発信元メールアドレス設定 .....	52
6.6.2. メールサーバーアドレス設定 .....	52
6.6.3. メールサーバポート番号設定 .....	52
6.6.4. SMTP 認証設定 .....	52
6.6.5. SMTP 認証ユーザー設定 .....	52
6.6.6. SMTP 認証パスワード設定 .....	53
6.7. メール通知設定 .....	54
6.7.1. 証明書期限メール送信設定 .....	55
6.7.2. 証明書更新メール送信設定 .....	55
6.7.3. 申請メール送信設定 .....	55
6.7.4. メール宛先設定 .....	55

6.7.5.	メールタイトル設定.....	55
6.7.6.	メール本文設定.....	55
<b>7.</b>	<b>証明書の管理.....</b>	<b>56</b>
7.1.	サービス一覧.....	56
7.2.	サービス情報詳細設定.....	58
7.2.1.	サービス名称の設定.....	59
7.2.2.	有効/無効 設定.....	59
7.2.3.	証明書コモンネーム設定.....	59
7.2.4.	公開鍵情報設定.....	59
7.2.5.	有効期限ステータス.....	59
7.2.6.	更新ステータス.....	59
7.2.7.	証明書情報.....	59
7.2.8.	認証局への自動申請設定.....	59
<b>8.</b>	<b>認証局への申請.....</b>	<b>60</b>
8.1.	認証局申請情報の設定.....	60
8.1.1.	認証局申請名称.....	60
8.1.2.	申請認証局.....	61
8.1.3.	認証局 API キー.....	61
8.2.	申請者情報 / EV 申請者情報の設定.....	62
8.2.1.	申請者情報テーブル名称.....	63
8.2.2.	ユーザーID で申請する.....	63
8.2.3.	データを入力する.....	63
8.3.	組織の編集.....	64
8.3.1.	組織名称.....	64
8.3.2.	組織番号.....	64
8.3.3.	備考.....	65
8.4.	認証局への自動申請の設定.....	66
8.4.1.	証明書申請ステータス.....	66
8.4.2.	申請メッセージ.....	66
8.4.3.	証明書の種類.....	67
8.4.4.	ライセンス数.....	67
8.4.5.	前回申請時のオーダーID.....	67
8.4.6.	組織選択.....	68
8.4.7.	認証局申請情報選択.....	68
8.4.8.	申請者情報選択.....	68
8.4.9.	証明書申請開始.....	68
8.5.	公開鍵情報の設定.....	69
8.5.1.	暗号スイート指定.....	69
8.5.2.	鍵長.....	69
8.5.3.	国名.....	69
8.5.4.	都道府県.....	69
8.5.5.	市区町村.....	69
8.5.6.	組織名.....	70
8.5.7.	部門.....	70
8.5.8.	メールアドレス.....	70
8.6.	証明書関連設定.....	71
8.6.1.	CSR ファイル関連設定.....	72

8.6.2.	認証局申請設定 .....	75
8.6.3.	証明書入出力業務 .....	76
<b>9.</b>	<b>サーバー・ロードバランサーへの適用 .....</b>	<b>80</b>
9.1.	サービス情報詳細（ノード一覧） .....	80
9.1.1.	ノード名称の設定 .....	82
9.1.2.	ノードの拠点設定 .....	82
9.1.3.	ノード有効・無効の設定 .....	82
9.1.4.	ノード確認方法の設定 .....	83
9.1.5.	ノード種別設定 .....	85
9.1.6.	アクセス情報設定 .....	87
9.1.7.	適用スケジュール設定 .....	88
9.1.8.	適用ステータス .....	88
9.2.	Windows サーバー側の設定 .....	89
9.2.1.	WinRM の有効化 .....	89
9.2.2.	グループの追加 .....	90
9.2.3.	ファイアウォール .....	91
<b>10.</b>	<b>ログ表示 .....</b>	<b>92</b>
10.1.	ログの表示 .....	92
10.2.	ソフトウェア全体ログの表示 .....	93
10.3.	サービス毎のログ表示 .....	94
<b>11.</b>	<b>メンテナンス .....</b>	<b>95</b>
11.1.	ライセンスキーの入力 .....	95
11.1.1.	ハードウェア情報の取得 .....	95
11.1.2.	ライセンスキーの発行申請 .....	95
11.1.3.	ライセンスキーの入力 .....	96
11.1.4.	ライセンス情報の確認 .....	97
11.2.	バックアップとリストア .....	98
11.2.1.	バックアップファイル .....	98
11.2.2.	バックアップ .....	98
11.2.3.	リストア .....	109
11.3.	DB のリフレッシュ .....	116
11.3.1.	リフレッシュ .....	116
11.4.	テクニカルサポートファイルの生成 .....	118
11.4.1.	テクニカルサポートファイルの生成 .....	118
<b>12.</b>	<b>付録 .....</b>	<b>121</b>
12.1.	ログメッセージ一覧 .....	121
12.2.	送信メール内容 .....	128
12.2.1.	証明書期限メール .....	128
12.2.2.	証明書申請メール .....	128
12.2.3.	証明書適用メール .....	129

## 1. はじめに

### 1.1. SSL 証明書管理ソフトウェア「SmartCertManage」概要

本製品 SSL 証明書管理ソフトウェア (SmartCertManage) は、SSL サーバー証明書の管理業務の省力化を実現するソフトウェアです。

サーバー証明書の情報を一元管理し、全ての SSL 証明書を見える化します。更新期限が近付いたらメールでお知らせします。

鍵と CSR の作成から認証局への申請、証明書の取得については、本ソフトウェアが認証局の API 経由で代行します。

また、サーバーやロードバランサーへのインストール・適用作業、適用後の更新確認も行います。

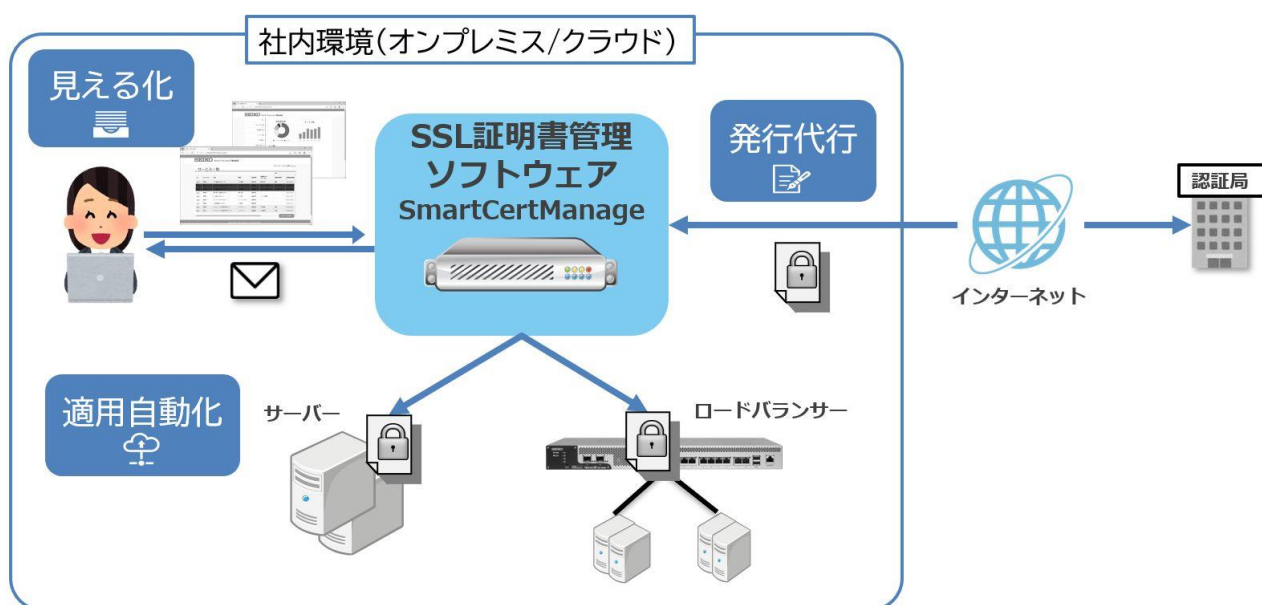


図1.1 製品概要図

## 1.2. 機能一覧

機能	項目	内容
基本機能	企業	拠点ごとの証明書管理
	ユーザーグループ/ユーザー	ユーザーグループごとの証明書管理 ユーザー2段階権限（管理者/一般）
	バックアップ/リストア	設定/証明書のバックアップ/リストア
	ログ照会	ログ一覧の表示（全体/サービス単位）※ <sup>1</sup>
見える化	サービス（証明書）管理	サービス表示（一覧/詳細表示） サービス有効/無効 証明書管理（2世代/2つの中間証明書+サーバー証明書） 証明書ステータス（有効期限/更新） 証明書のインポート/エクスポート（PEM形式）
	通知	SMTP送信（SMTP認証、STARTTLSによるSSL暗号化通信） 期限時（90日/60日/30日/15日/失効時を選択） 申請時（申請開始/申請中/申請終了） 適用時（適用開始/適用終了）
	CSRファイル	鍵/CSRファイル作成 CSRインポート（PEM形式、ファイル/貼り付け）
代行申請	対応認証局/証明書種別	digicert(セキュアサーバーOV/EV、グローバルサーバーOV/EV、ジオトラスト トゥルービジネス ID/トゥルービジネス withEV)※ <sup>2</sup>
	認証局申請設定	組織/認証局申請/申請者情報/EV承認者情報/ライセンス数 設定
	スケジュール申請	日時を指定して申請/今すぐ申請
適用	適用対象	Linux Apache(2.4.6 / 2.4.8~)※ <sup>3</sup> ※ <sup>4</sup> Windows IIS※ <sup>4</sup> F5 BIG-IP シリーズ※ <sup>3</sup> ※ <sup>4</sup>
	設定	Apache（証明書ファイル/中間証明書ファイル/鍵ファイル/作業フォルダ）※ <sup>6</sup> IIS（IIS マネージャーサイト名/バインドホスト名）※ <sup>5</sup> F5 BIG-IP（SSL プロファイル名/インポート名称）
	アクセス設定	IP アドレス ポート番号 ※ <sup>6</sup> ログインID/パスワード ※ <sup>7</sup> 実行ID/パスワード ※ <sup>7</sup>
	適用後の確認方法	IP アドレス/ポート番号（FQDN 指定） URL 指定 確認しない
	ロールバック	適用時のエラー時※ <sup>8</sup>

**注意**

- ※1 内部ログ出力のために TCP ポート 9020 をオープンします。  
9020 ポートを使用している場合、本ソフトウェアは起動できません。
- ※2 組織認証、ドメイン認証は、Certcentral で事前に申請要請および承認がされていることが条件となります。
- ※3 Linux Apache の対象バージョンは 2.4.6、2.4.8 以降となります。  
F5 BIG-IP の対象バージョンは 11 となります。
- ※4 Linux/BIG-IP の場合は、Linux/BIG-IP 上に管理されている鍵は適用に利用できません。適用を行う場合は、鍵ファイルを必ずインポートしてください。  
Windows IIS の場合も同様に、インポートした鍵ファイルと対となるサーバー証明書にて適用することが可能です。  
Windows 上で鍵・CSR を生成した場合は、その CSR をもとに作成した SSL サーバー証明書を適用することも可能です。この場合 Windows 上にある鍵を利用するため鍵ファイルのインポートは不要です。また、この場合は、証明書を管理するサービスに、適用を実施する Windows ノードは 1 つのみ登録してください。
- ※5 事前に対象の Windows に、WinRM サービス有効の設定をしてください
- ※6 Linux Apache のみ有効となります。Windows の場合は winRM の標準ポート番号(5985)、F5 は RestAPI の標準ポート番号 (443) を利用します。
- ※7 Windows IIS は、ログイン ID として administrator の権限をもつユーザーを設定してください。  
F5 BIG-IP は、ログイン ID として administrator の権限をもつユーザーを設定してください。  
Linux Apache は、ログイン ID (ログイン ID に付与できない環境では実行 ID) としてフォルダおよびファイル作成/apache のリスタートが行える権限のユーザーを指定してください。
- ※8 Linux Apache のみ有効となります。



## 1.3. システム要件

### 1.3.1. ハードウェア要件

パソコン	1.3.2 システム要件に記載している OS が正常に動作する機種
ハードディスク	本製品導入の為に、8GB 以上の空きが必要です。
メモリ	8GB 以上で空きメモリが 2GB 以上
ネットワーク	100/1000BASE のネットワークボードが 1 枚以上
CPU	1.3.2 システム要件に記載している OS が正常に動作する CPU 64 ビット (x64) のプロセッサ
ディスプレイ解像度	1920 x 1080 以上 1677 万色以上

### 1.3.2. システム要件

OS	Windows Server 2019 Standard (日本語版 64bit) <b>注意</b> WindowsUpdateは最新の状態にしてください。
ソフトウェア	本製品を動作させる前に以下のソフトウェアをインストールする必要があります。 Microsoft .NET Framework 4.6.1 Microsoft .NET Framework 4.8 Microsoft Access DatabaseEngine 2010 Microsoft Visual C++ 2015-2022 Redistributable(x86) Microsoft Visual C++ 2017 Redistributable Package(x64) Python 3.10.4(x86) Python 3.10.4(x64) Win64 OpenSSL-1.1.1t Light postgresql 14.4-1 Windows(x64) <b>注意</b> Microsoft Office2010 以降の 64bit 版が導入されている環境では本製品は動作しません。
その他	認証局に申請を行う場合や、SSL証明書の確認をインターネット経由で行う場合は、本ソフトウェアがインターネットに接続する必要があります。 プロキシが必要とする環境の場合は、本製品にプロキシの設定をお願いいたします。 ファイアウォールをご使用の場合は、本製品がインストールされた Windows の IP アドレスから HTTPS クライアントとして宛先 443 等のパケットを透過する設定をいれてください。

## 1.4. ユーザー権限

本製品は2種類のユーザー（管理者、一般）でログインすることができます。

管理者ではすべての操作が可能です。一般では設定/状態の参照が可能です。設定の変更はできません。

## 2. インストール

### 注意

- ・インストールを実行するには Windows OS の管理者権限が必要です。
- ・ネットワークドライブからのインストールには対応していませんので、ローカルディスクにコピーして下さい。
- ・本製品の動作に必要な NET Framework4.6.1/4.8 と Microsoft Access DatabaseEngine 2010 はインストーラーから導入する事が可能ですが、.NET Framework4.6.1/4.8 インストール後に再起動する場合があります。導入時に PC の再起動をさせたくない場合、事前に導入してください。
- ・1 つのマシンに本製品は 1 台のみインストール可能です。

製品フォルダ内の Setup.exe を実行します。

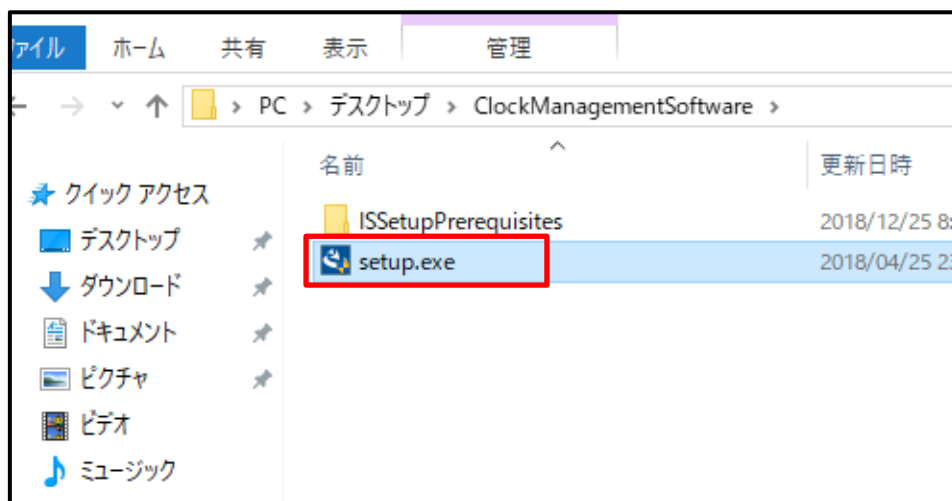


図 2.1 インストーラーの実行

インストーラーを実行すると、図 2.2 のような画面が表示されます（既にインストールされている項目については、要件として出力されません）。

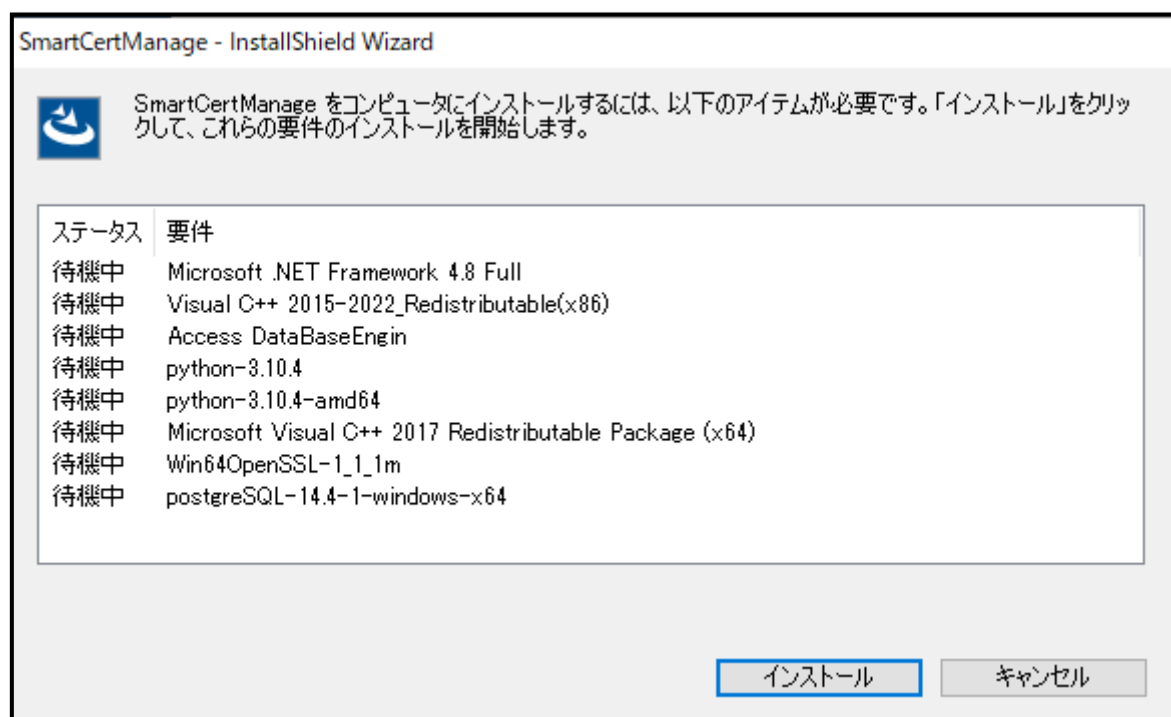


図 2.2 各項目インストール確認画面

<インストール>: 表示されているソフトウェアのインストールを開始します。

<キャンセル>: インストーラーは終了します。

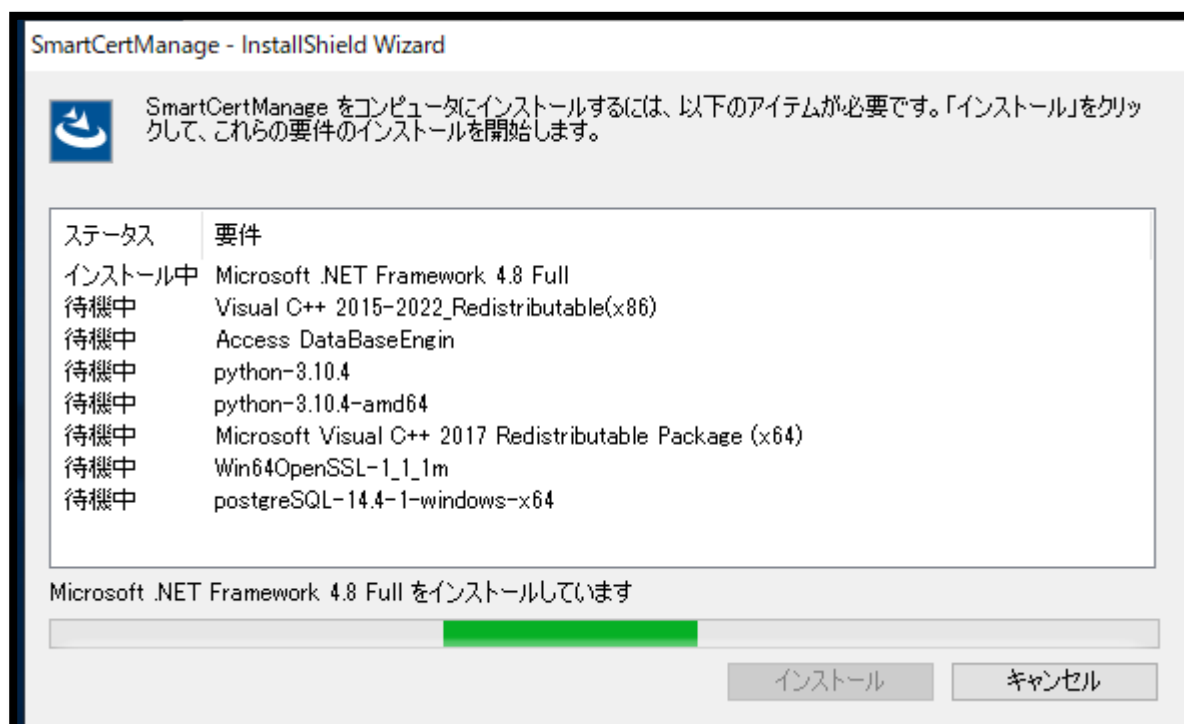


図 2.3 各項目インストール画面

<インストール>ボタンを選択すると、図 2.3 のように表示され各項目がインストールされます。

Microsoft Access DataBaseEngine 2010 をインストールする場合、図 2.4 が表示されます。  
、< 次へ>ボタンを選択します。

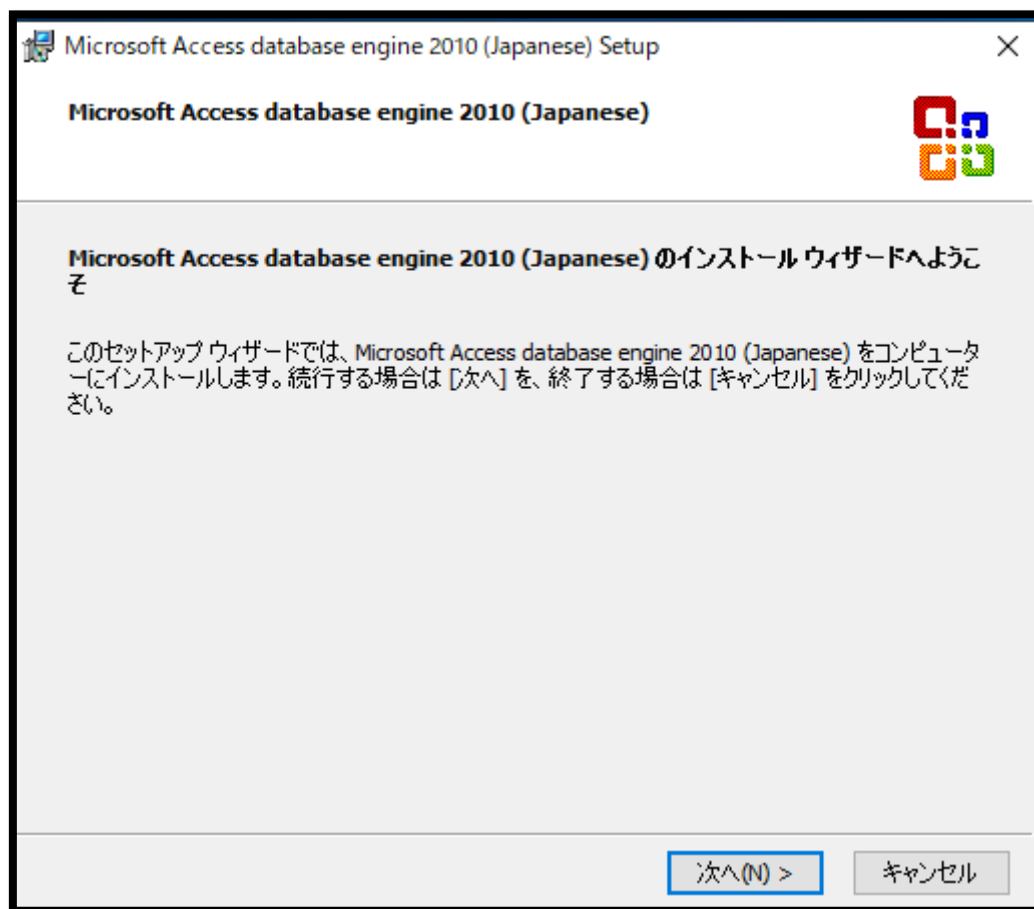


図 2.4 Microsoft Access DataBaseEngine 2010 インストール開始

使用許諾を確認し、<…に同意します>にチェックを入れ、< 次へ>ボタンを選択します。

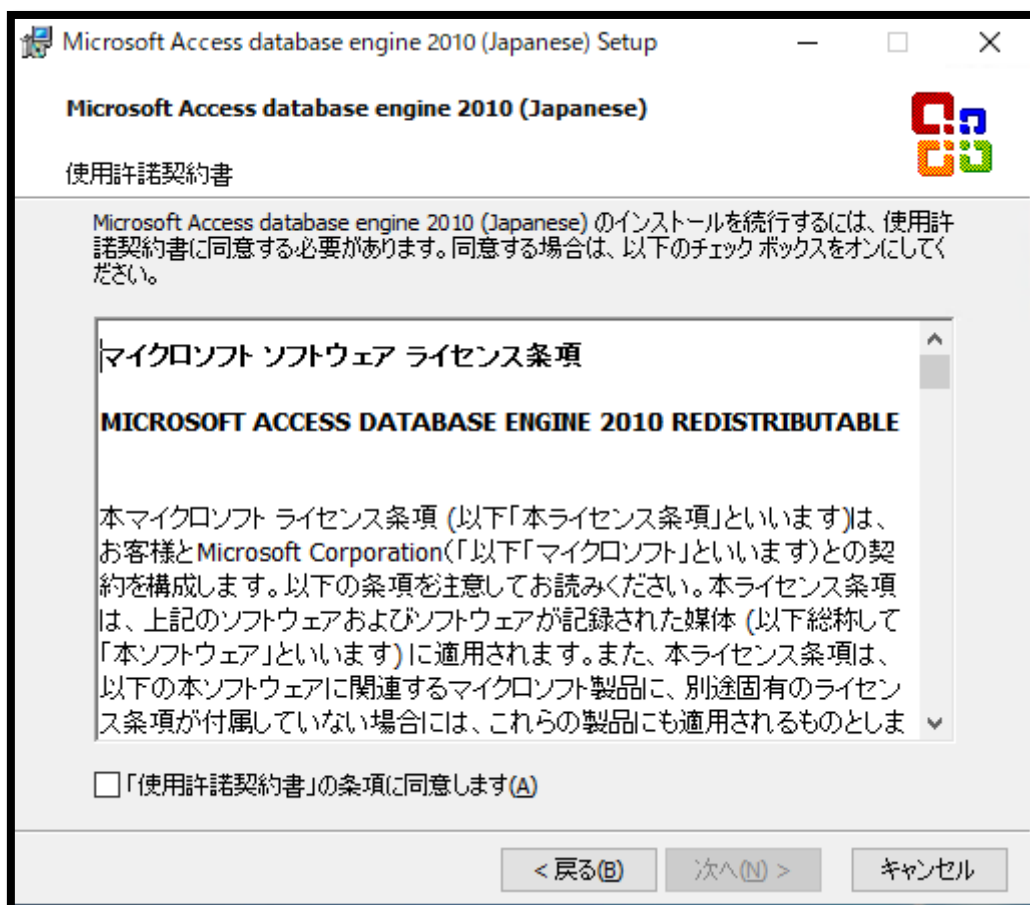


図 2.5 Microsoft Access DataBaseEngine 2010 使用許諾

インストール先をデフォルトから変更する場合は<参照>ボタンを選択し、フォルダを選択してください。インストール先を指定したら、<次へ>ボタンを選択します。

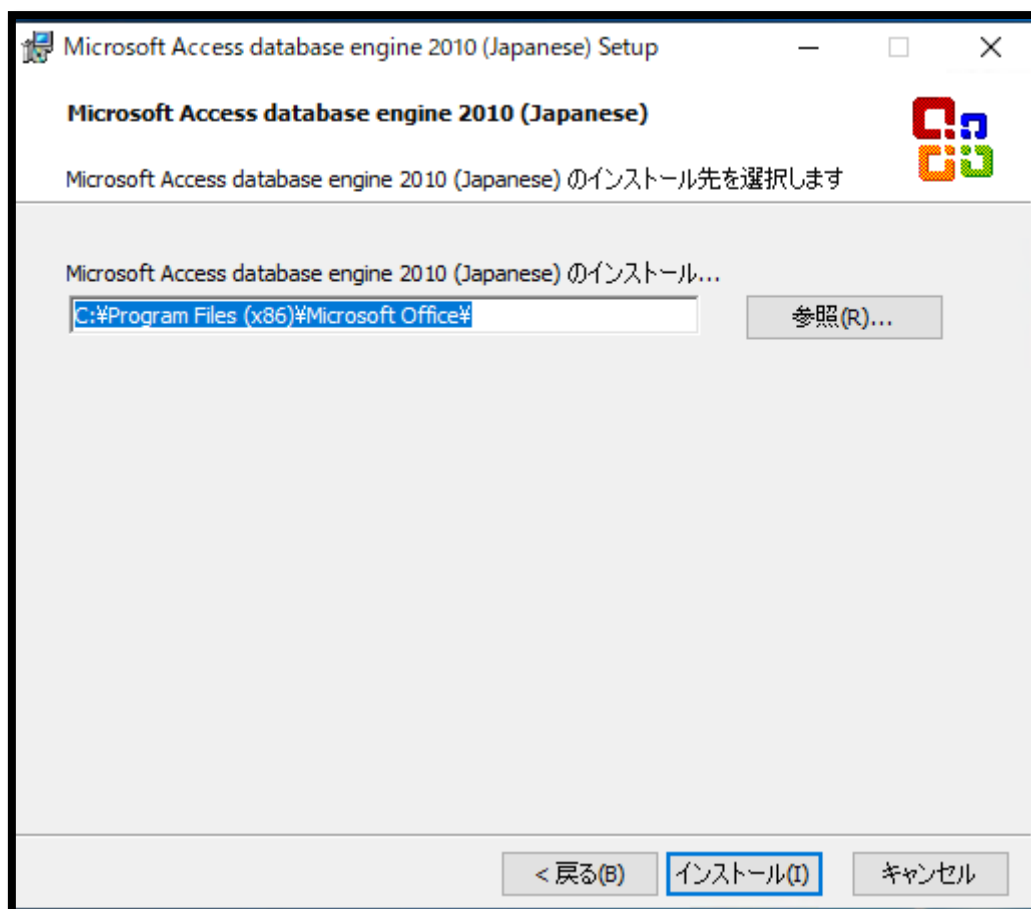


図 2.6 Microsoft Access DataBaseEngine 2010 インストール先選択



インストールが開始されます。

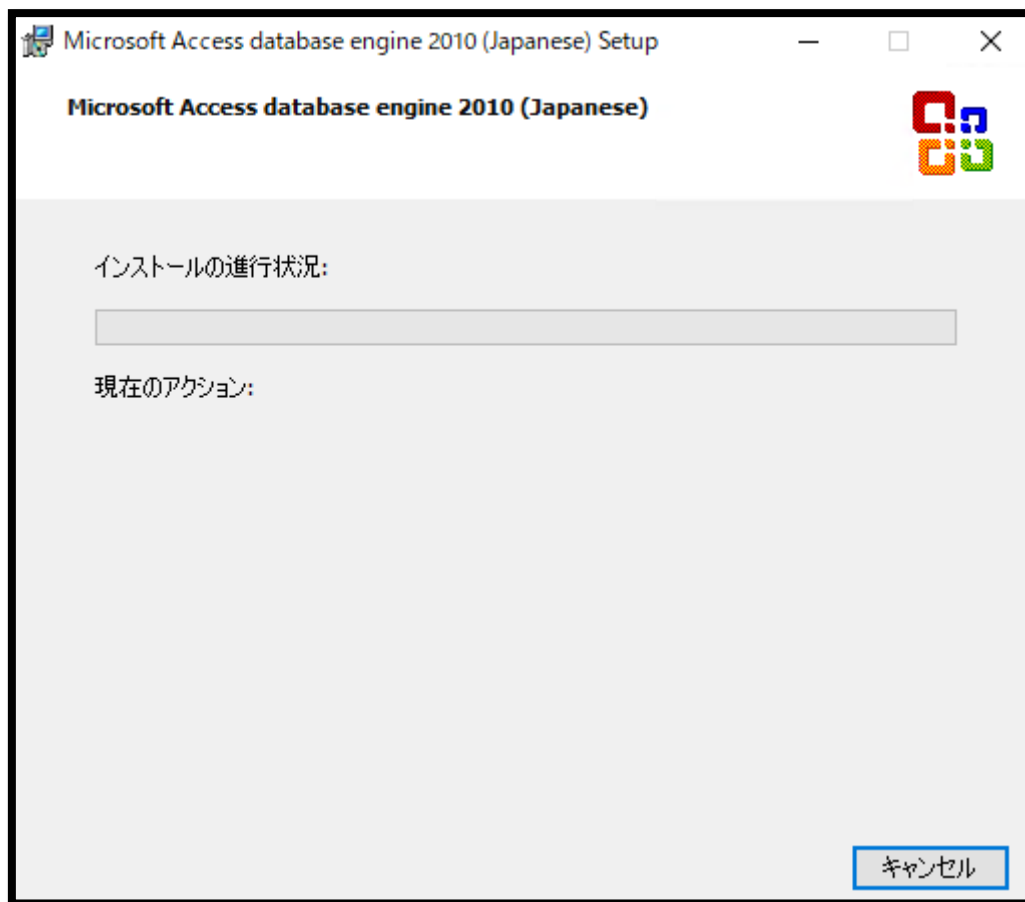


図 2.7 Microsoft Access DataBaseEngine 2010 インストール中

インストールが完了すると図 2.8 が表示されるので、<OK>ボタンを選択します。

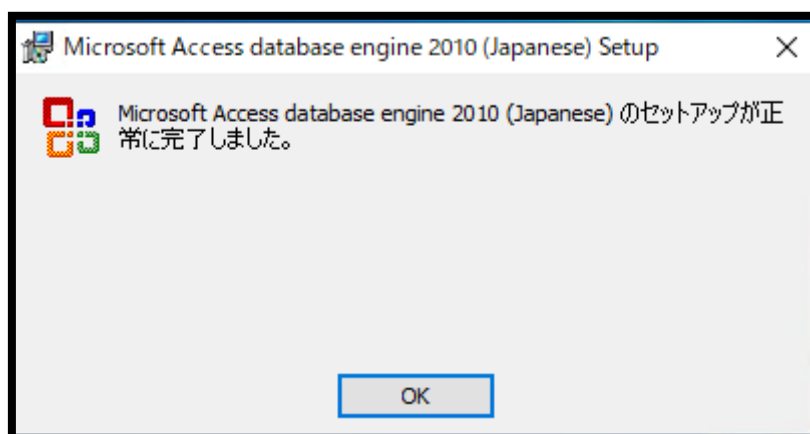


図 2.8 Microsoft Access DataBaseEngine 2010 インストール完了

各項目のインストールが完了すると **Smart Cert Manage** のインストール画面 (0) が表示されます。  
インストール開始画面が表示されたら<次へ>ボタンを選択します。

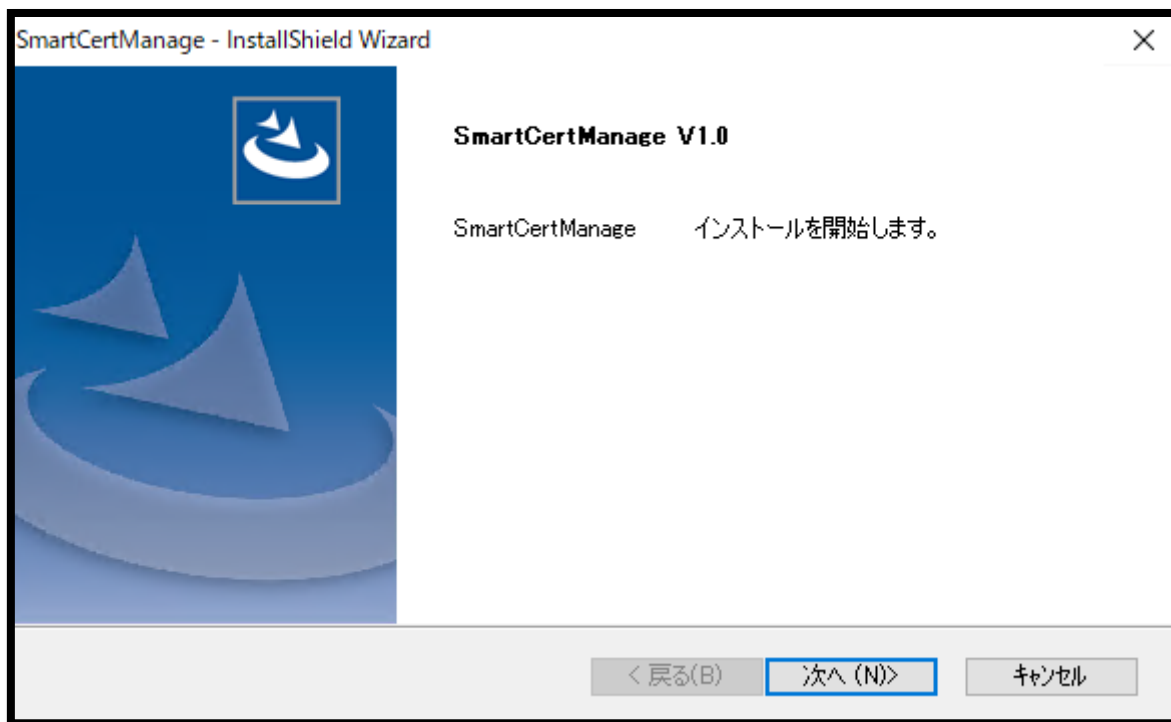


図 2.9 インストール画面

インストール設定が表示されます。<次へ>ボタンを選択します。

**注意**

インストール先は C:\SCM にだけ対応しております。インストール先はインストーラーの設定のままでインストール作業をすすめてください。

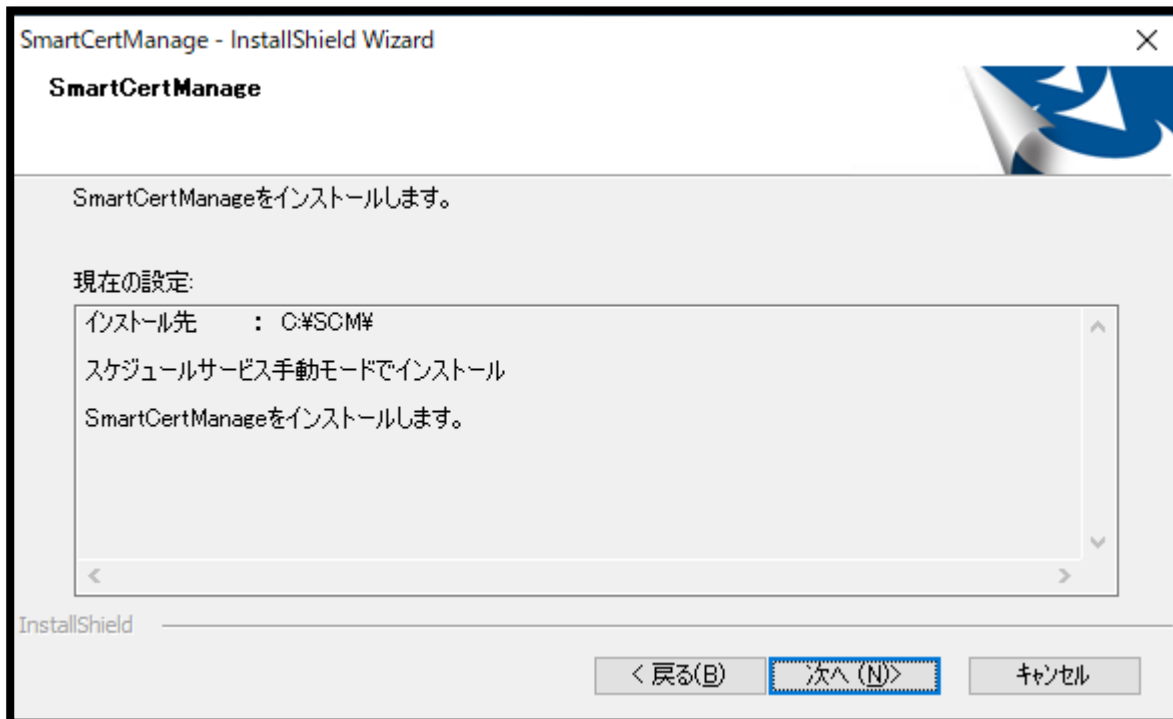


図 2.10 インストール設定確認画面

インストールが開始されます。

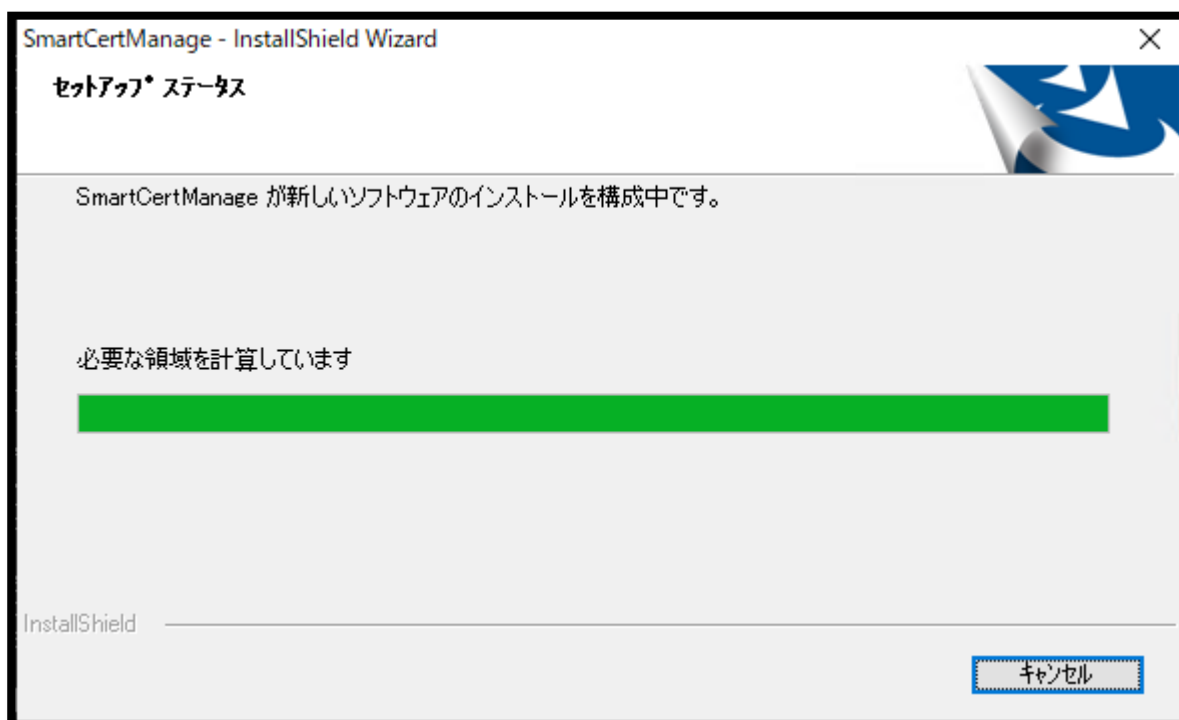
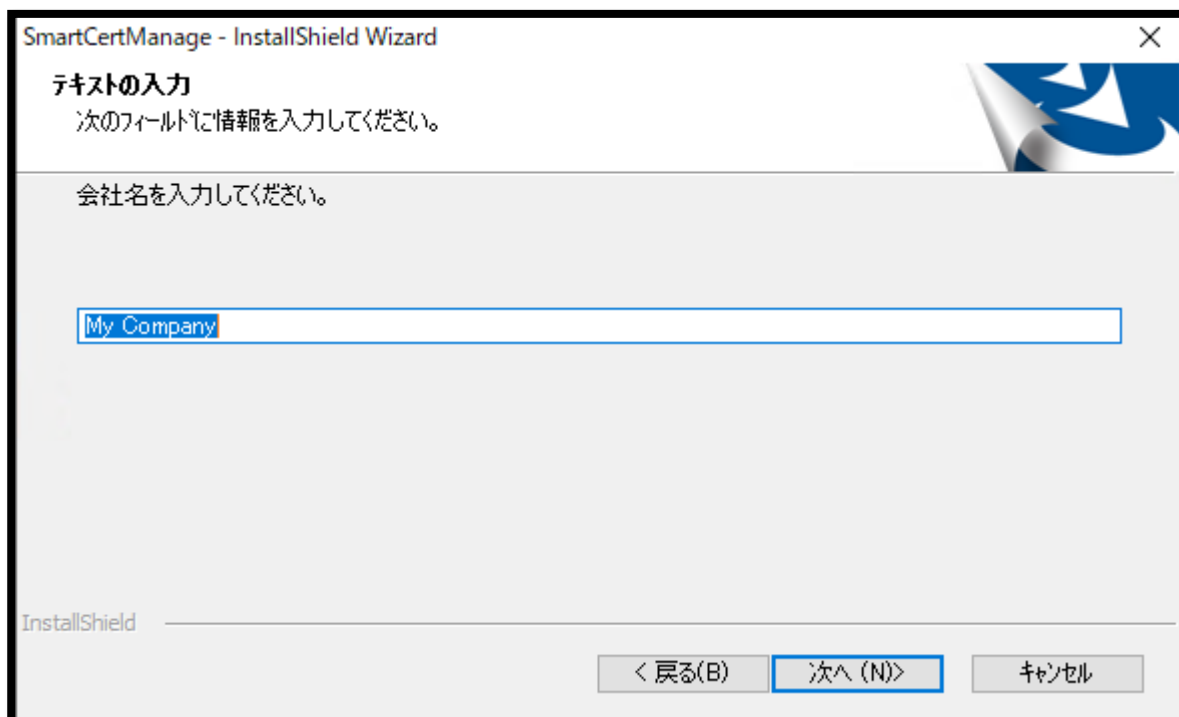


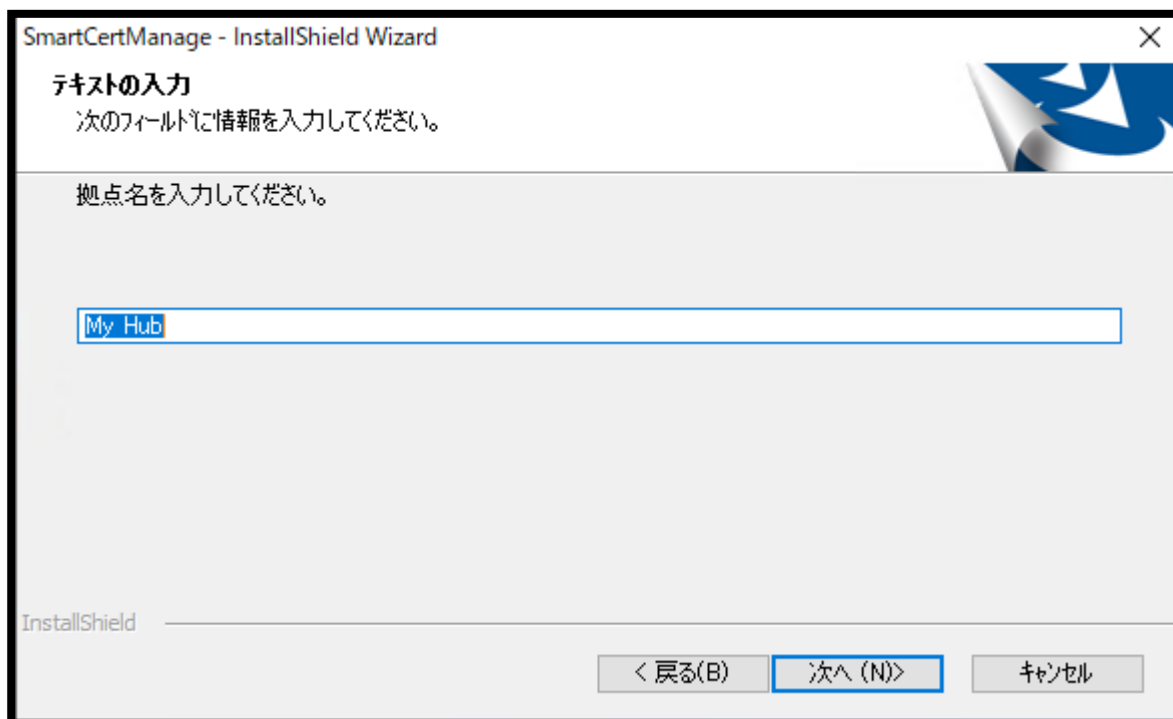
図 2.11 インストール中画面

会社名を入力する画面が出力されます。

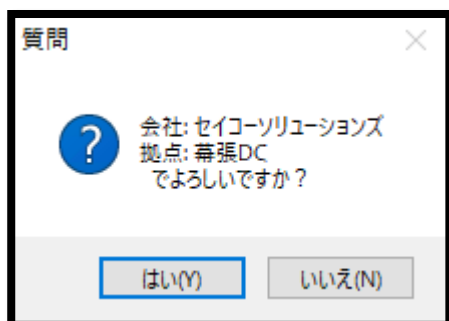
会社名を入力したら、<次へ>ボタンを選択します。



拠点名を入力する画面が出力されます。  
拠点名を入力したら、<次へ>ボタンを選択します。



会社名と拠点名を確認します。  
内容で OK の場合は、<はい>を選択します。



インストールが完了すると以下の画面が表示されます。<完了>ボタンを選択するとインストール画面は終了します。

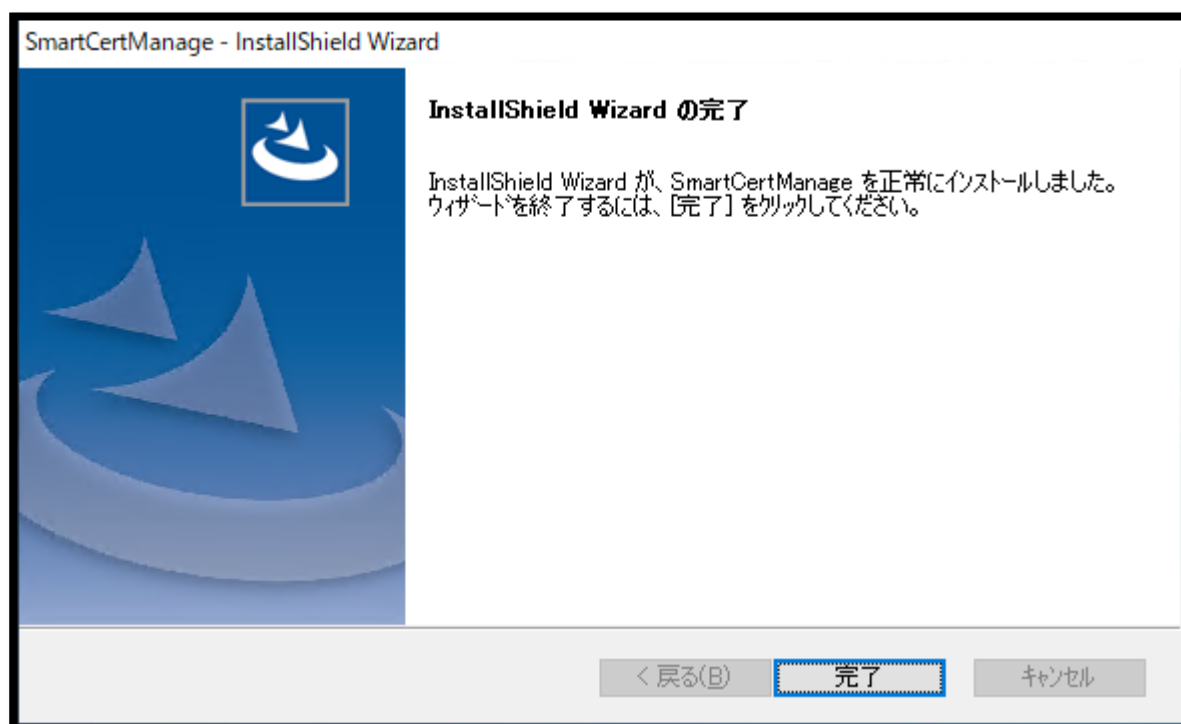


図 2.12 インストール終了画面

<完了>ボタンクリックでインストール完了です。

### 3. アンインストール

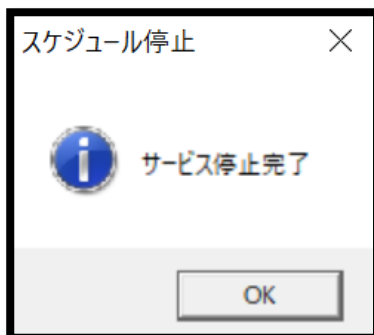
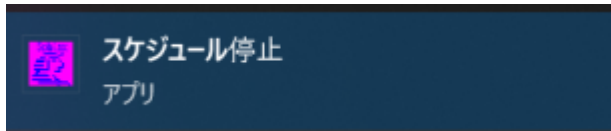
**注意**

アンインストール後、新しいバージョンをインストールする場合は、あらかじめデータのバックアップをしておいてください。データのバックアップは 11.2.2 バックアップを参照してください。

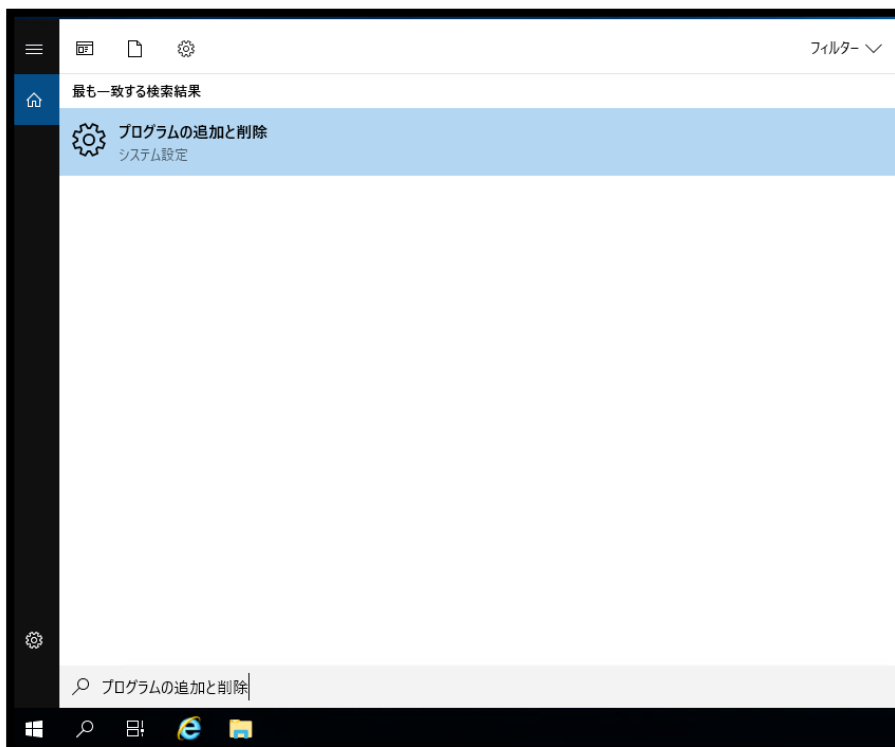
アプリケーションが起動している場合は事前に終了させてください。

スケジュールが開始されている場合は、事前に停止させてください。

Windows 検索窓で「スケジュール停止」を入力し、スケジュール停止 アプリを起動します。



Windows の検索窓で「プログラムの追加と削除」を入力し、プログラムの追加と削除を選択します。



SmartCertManage を右クリックし、<アンインストール>を選択します。

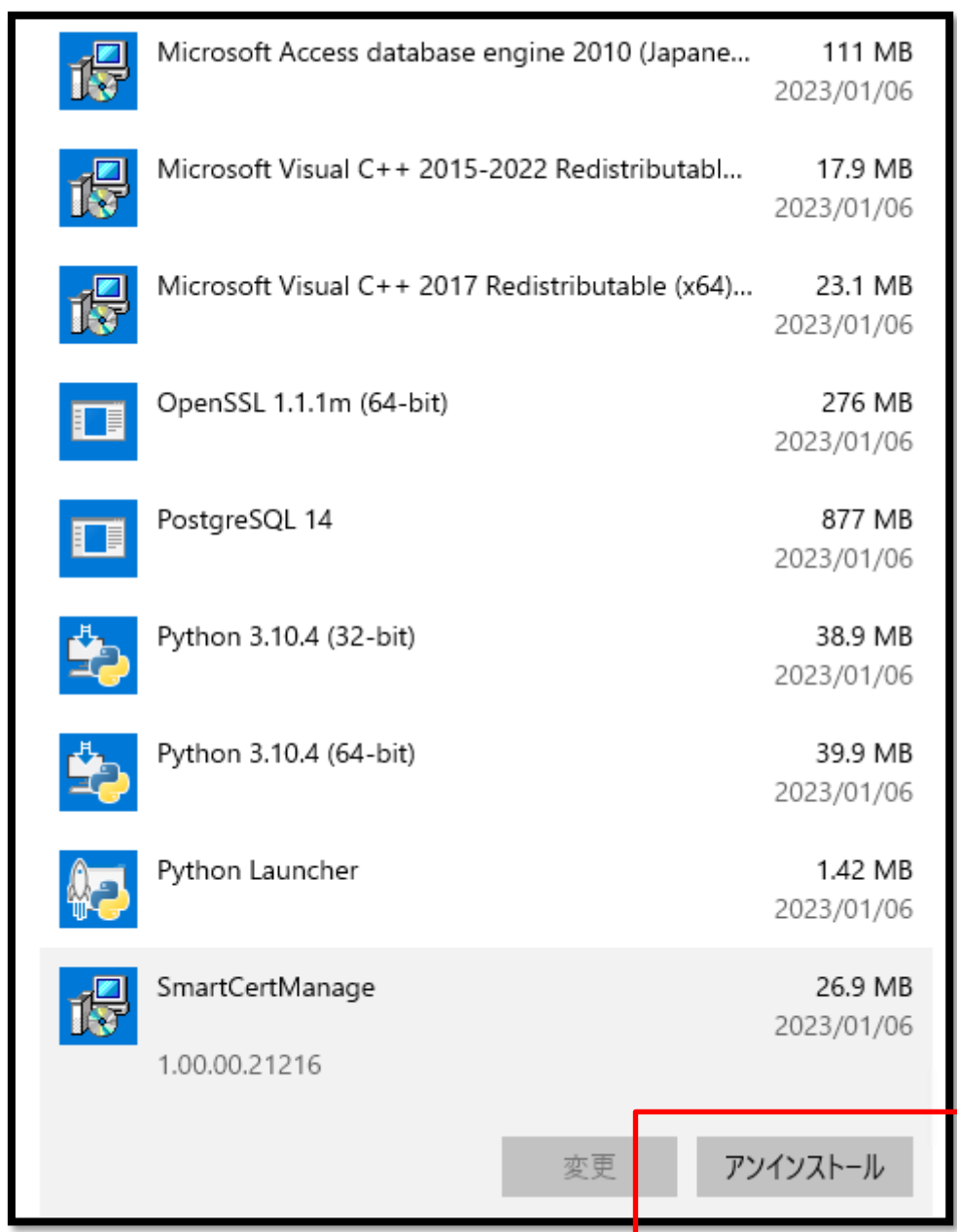


図 3.1 プログラムのアンインストール

0 のメッセージが表示されます。<はい>ボタンを選択します。

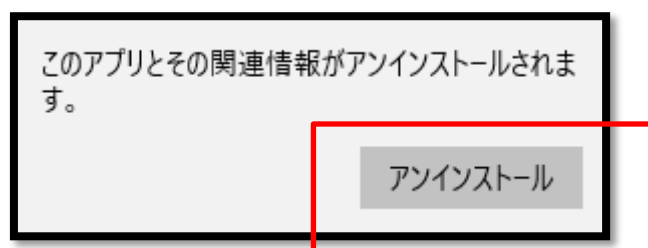


図 3.2 アンインストール確認メッセージ



図 3.2 のメッセージが表示されます。<はい>ボタンを選択するとアンインストールが実行されます。

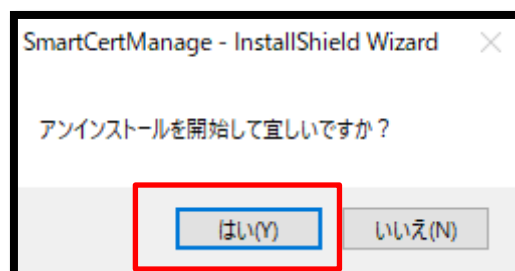


図 3.3 アンインストール実行中

アンインストールが完了すると以下の画面が表示されます。

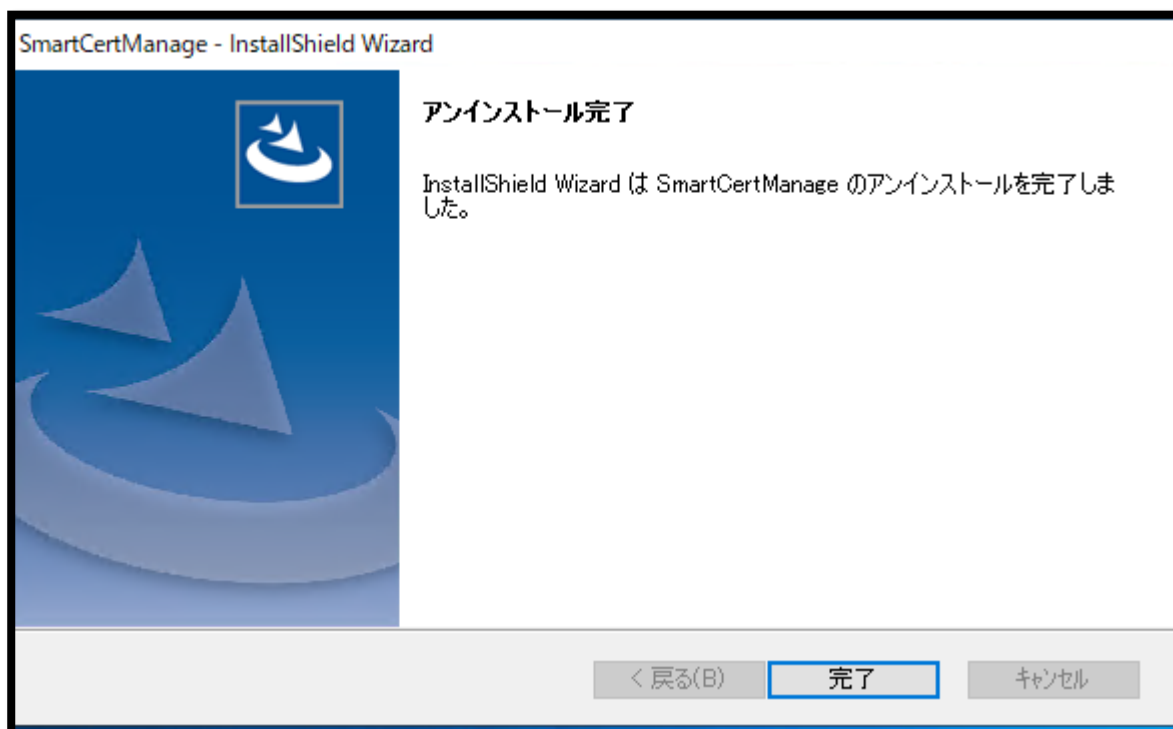


図 3.4 アンインストール終了画面

ユーザーディレクトリーは削除されません。不要な場合は手動で削除して下さい。

**注意**

本ソフトウェアをインストーラーでアンインストールした状態では、証明書ファイルや証明書管理情報は残されたままの状態です。

ソフトウェアをバージョンアップする目的でアンインストールする場合は、インストールフォルダを手動で削除しないでください。

**注意**

ユーザーディレクトリーを削除する場合は、Python をアンインストールしてから削除してください。新しく SmartCertManage をインストールすることができなくなります。

ソフトウェアが生成したデータベースも含めて削除する場合は、以下の手順を実行してください。

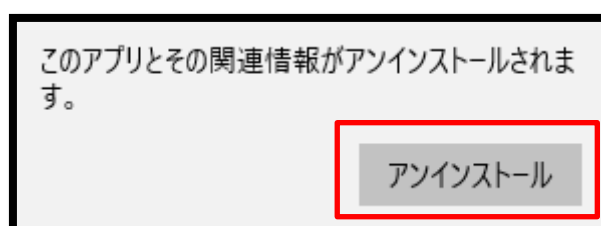
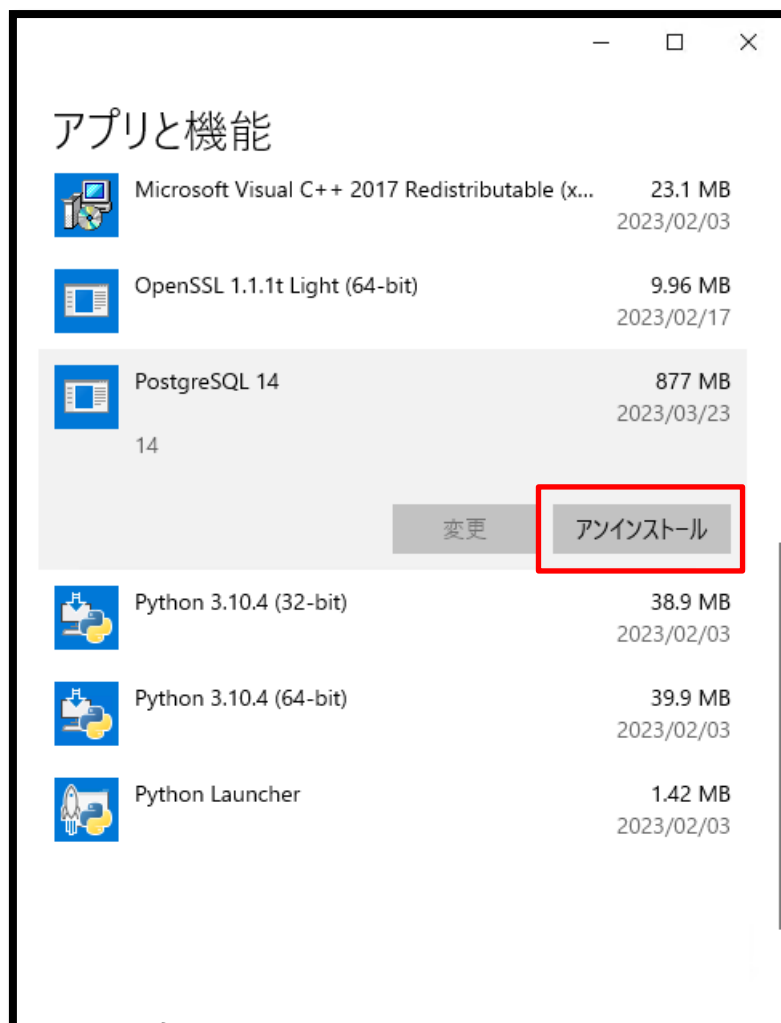
**注意**

ソフトウェアが生成したデータベースを削除すると、新しいバージョンをインストールした場合でも、それまでに利用していたデータは復旧できません。

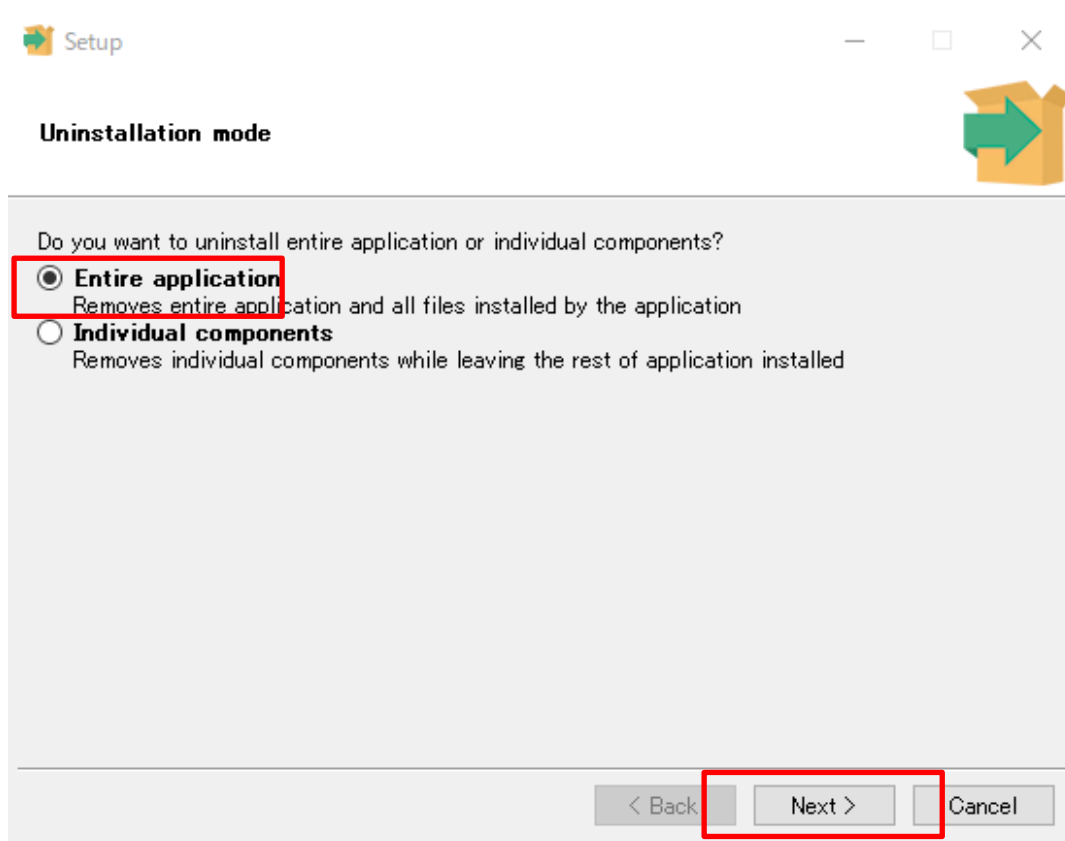
ソフトウェアをバージョンアップする目的でアンインストールをする場合は、以下の手順は行わないでください。

まず、PostgreSQL をアンインストールします。

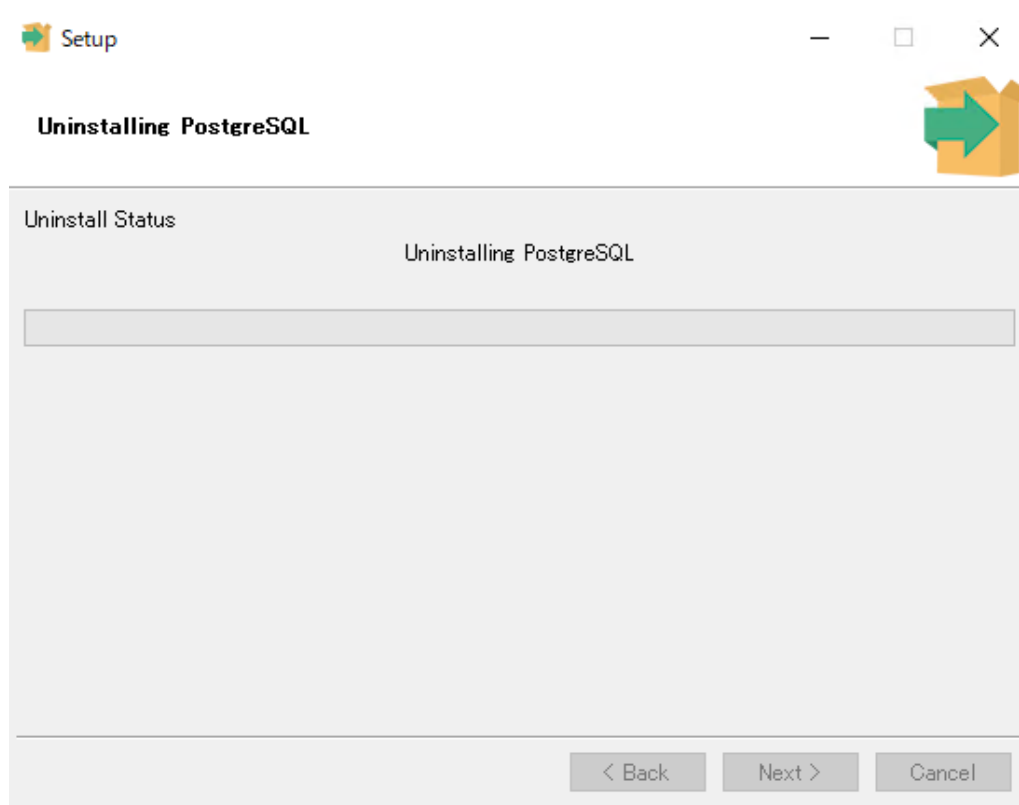
Windows の検索窓で「プログラムの追加と削除」を入力し、プログラムの追加と削除を選択します



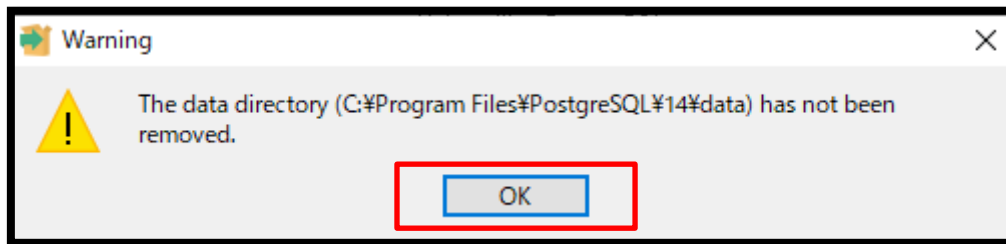
アンインストール画面で、「Entire application」を選び、Next ボタンを選択します。



アンインストールが開始されます。



データを削除していないメッセージが出力されます。OK を選択します。

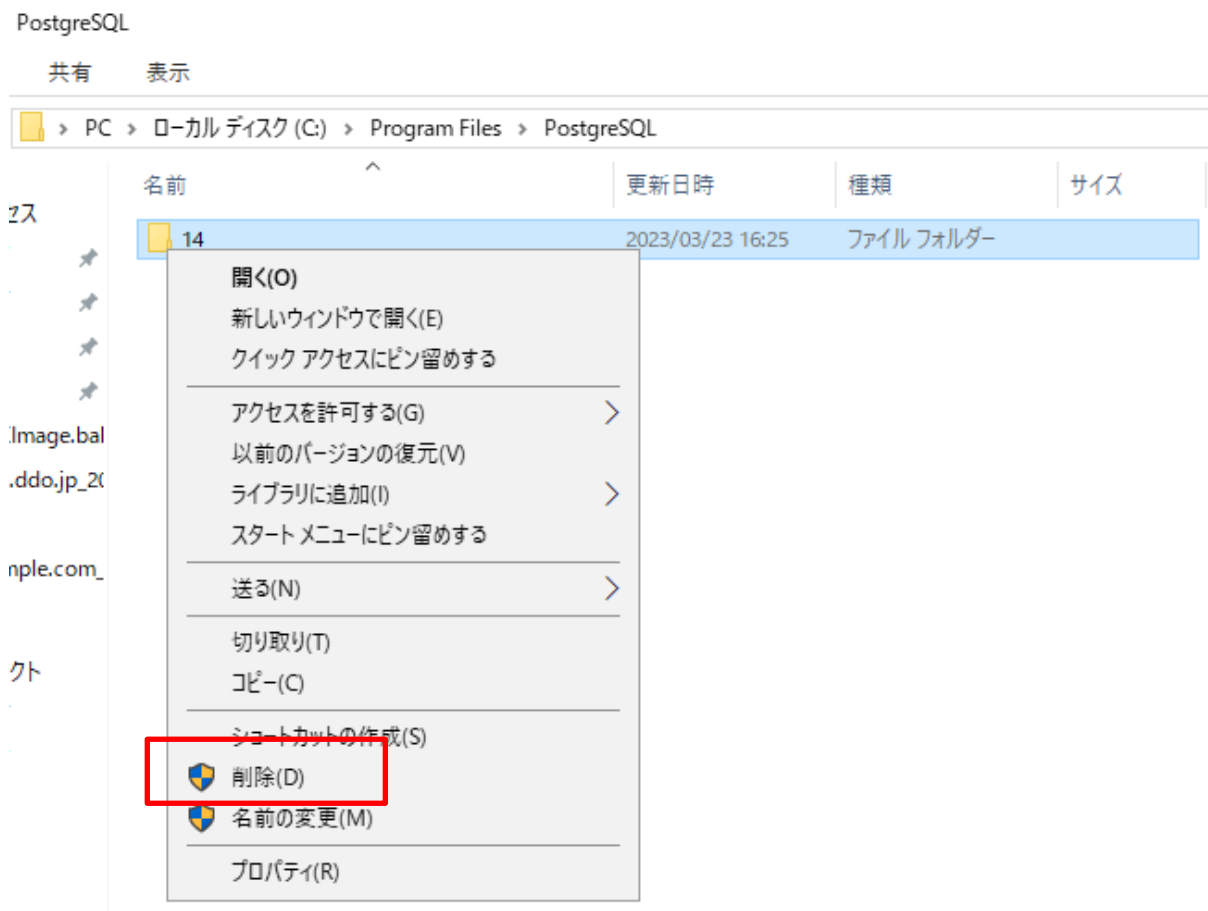


つぎに、データベースがあるファイルを削除します。

エクスプローラーで、postgreSQL のインストールディレクトリ (C:\Program Files\PostgreSQL)

に行き、「14」のディレクトリで右クリックを押下します。

プロンプトにある「削除」を選択します。



これで、データベースの削除が完了しました。

**注意**

新しいバージョンをインストールせずに、情報を完全に削除する場合は、2つの python をそれぞれアンインストールした後に、インストールフォルダ（デフォルトは、C:\SCM\ ）を手動で削除してください。

## 4. バージョンアップ

本ソフトウェアのバージョンアップを行う場合は、新しいバージョンのインストーラーをご用意のうえ

3 アンインストール

2 インストール

の順に実行してください。

### 注意

本ソフトウェアがインストールした状態の更新インストールは実施できません。

必ずアンインストール後に、新しいバージョンのインストーラーにてインストールを実施してください。

### 注意

本ソフトウェアをインストーラーでアンインストールした状態では、証明書ファイルや証明書管理情報は残されたままの状態です。新しいバージョンのインストーラーでインストールすることで、新しいバージョンのソフトウェアに情報は引き継がれます。

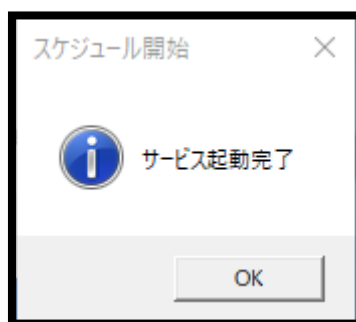
## 5. 初期設定

スケジュール機能の開始や、ライセンスキーの入力、管理者ユーザーの初期設定、デフォルトグループ名の変更を行います。

スタートメニューの SmartCertManager から、”スケジュール開始” (図 5.1) を実行します。



図 5.1 スケジュール開始画面



スケジュール開始画面(図 5.1)が表示されます。



## 5.1. 初期設定

スタートメニューの SmartCertManager から、” SCM クライアント” (図 5.2 起動画面) を実行します



図 5.2 起動画面

ログイン画面が表示されます。

初期状態では、管理者として登録されているメールアドレス「admin@example.com」を入力し、<ログイン>を選択してください。

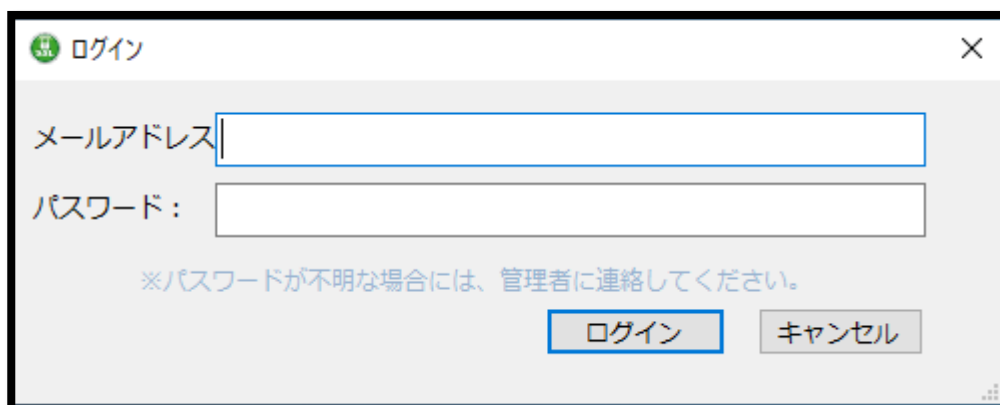


図 5.3 ログイン画面

初期パスワードを設定します。

<OK>を選択した後、新しいパスワードとパスワード再入力に、それぞれ同じパスワードを設定して、<パスワードを設定してログイン>を選択してください。

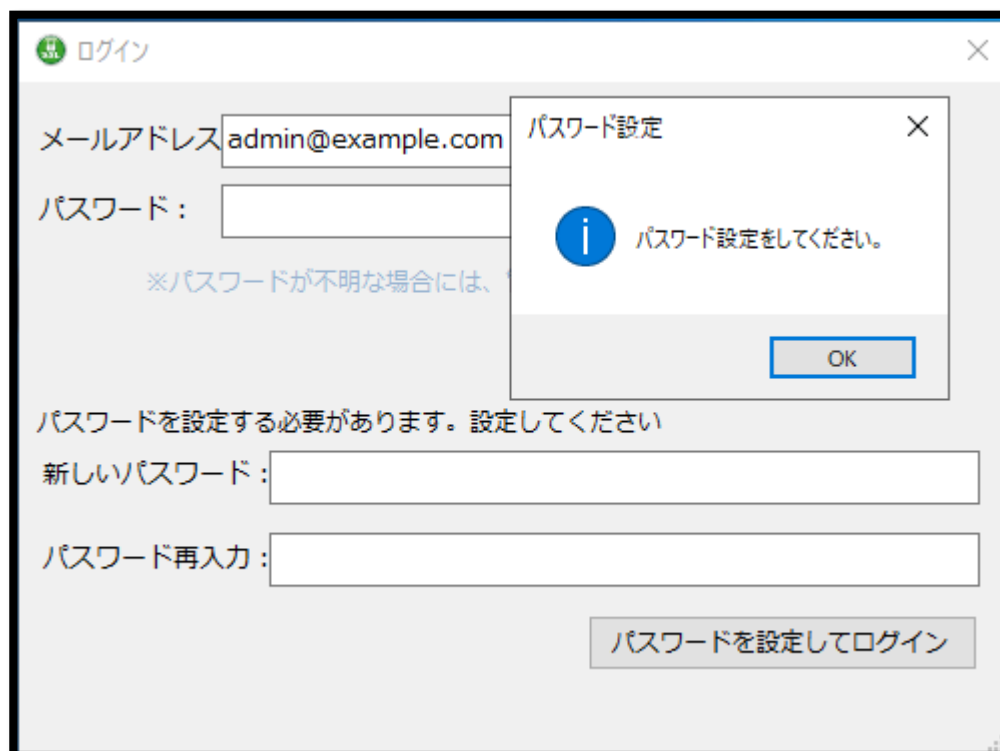


図 5.4 初期パスワード設定画面

**注意**

正式ライセンスキーを取得している場合は、以降の設定を行う前にライセンスの入力を行います。ライセンスの入力については、11.1 ライセンスキーの入力 を参照ください

管理者ユーザーを登録します。

ダッシュボードが表示されたら、右上の<ユーザー情報>を選択してください。



図 5.5 ダッシュボード画面

ユーザー一覧画面が表示されたら、<ユーザー追加>ボタンを選択してください。



図 5.6 ユーザー管理画面

新しく管理者ユーザーのログイン用メールアドレスを登録します。

ユーザーID にメールアドレスを入力します。

権限選択は、管理者を選択します。

パスワードと、パスワード（再入力）に、同じパスワードを入力します。次回ログイン時にパスワードを設定する場合は、パスワードを入力せずに、次回ログイン時にパスワードを設定する、をレ点チェックします。

入力が終わりましたら、<追加>ボタンを選択します。



ユーザー情報編集

ユーザーID(メールアドレス) : admin@seiko-sol.co.jp

権限選択 :  一般ユーザー  管理者

パスワード : \*\*\*\*\*

パスワード(再入力) : \*\*\*\*\*

次回ログイン時にパスワードを設定する  パスワードを見せる

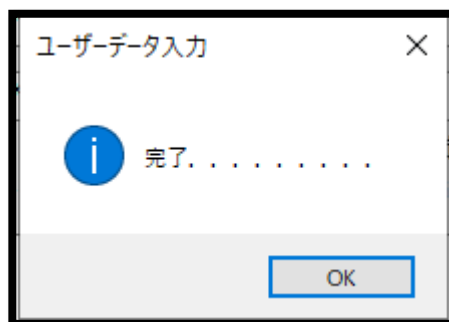
※パスワードを変更した場合には、再入力エリアにも新しいパスワードを入力してください。

連絡先 :

追加 キャンセル

図 5.7 管理者ユーザー登録画面

入力内容に間違いがなければ、完了と出力されます。<OK>ボタンを選択します。



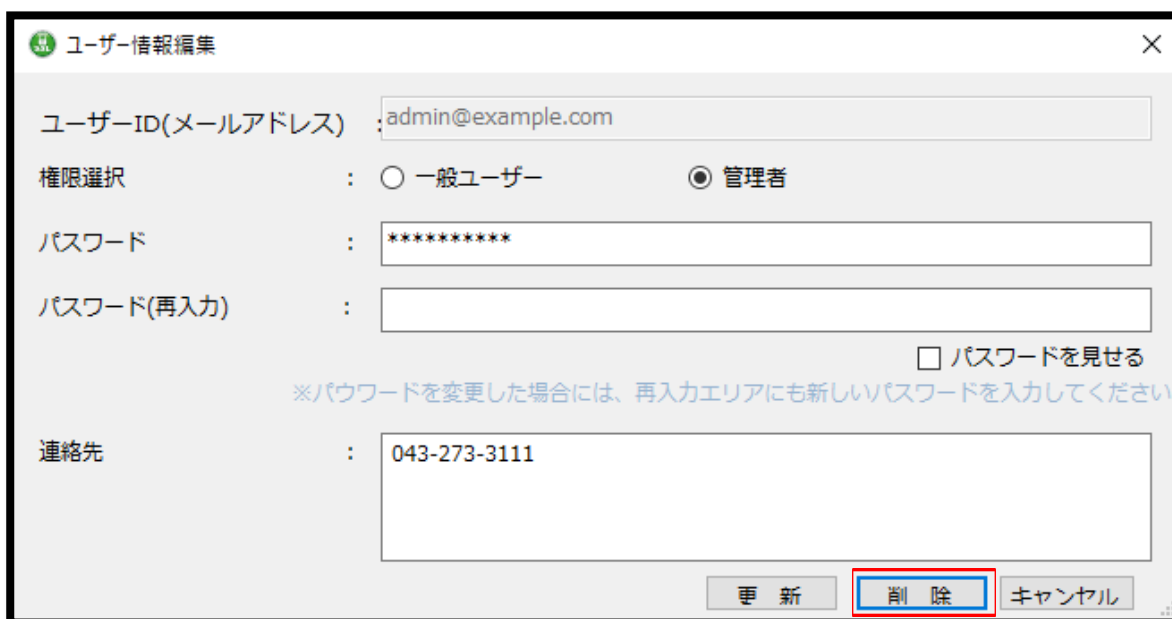
初期の管理者ユーザ ([admin@example.com](mailto:admin@example.com)) を削除する場合は、ユーザー一覧画面で、対象ユーザーの行の<編集する>を選択します。

**注意**

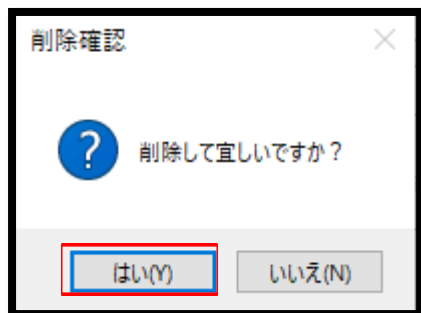
ログインしているユーザーは削除できません。削除するユーザーと異なる管理者ユーザーでログインしてください。



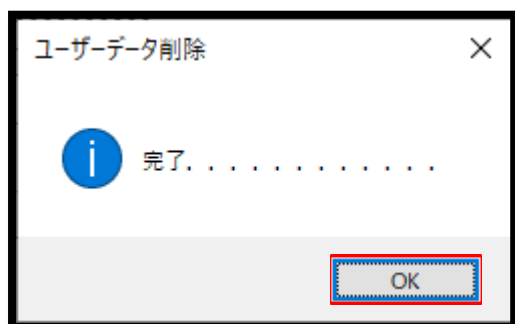
右下にある<削除>ボタンを選択します。



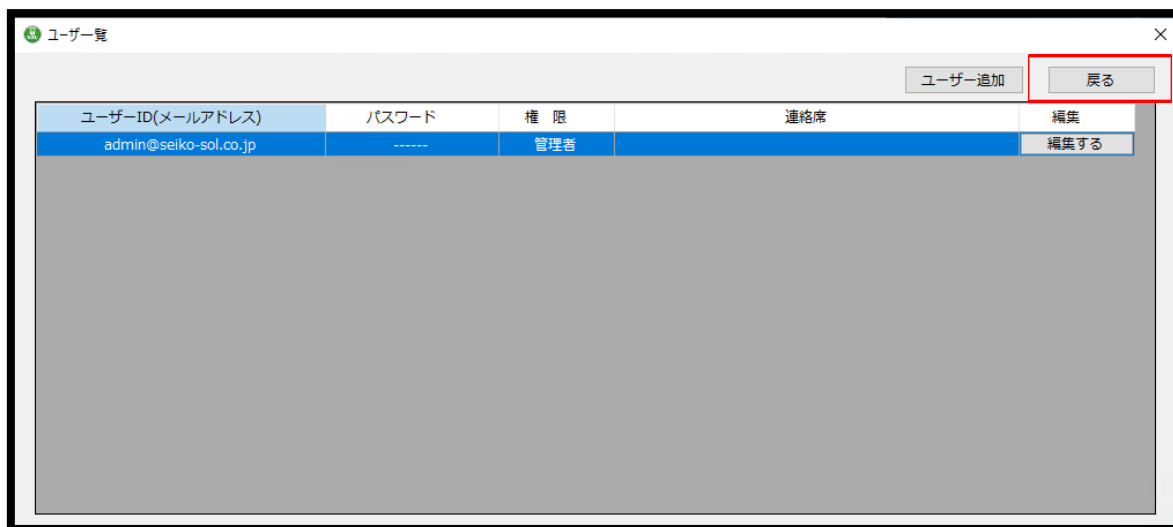
<はい>を選択すると、削除されます。



<OK>を選択します。



初期ユーザーが削除されていることを確認します。  
<戻る>ボタンを選択します。



次に、ユーザーグループの名称を変更します。  
ダッシュボード画面右上の<グループ情報>ボタンを選択します。



初期グループの名称が「samplegroup」になっています。  
右上の<名称変更>ボタンを選択します。

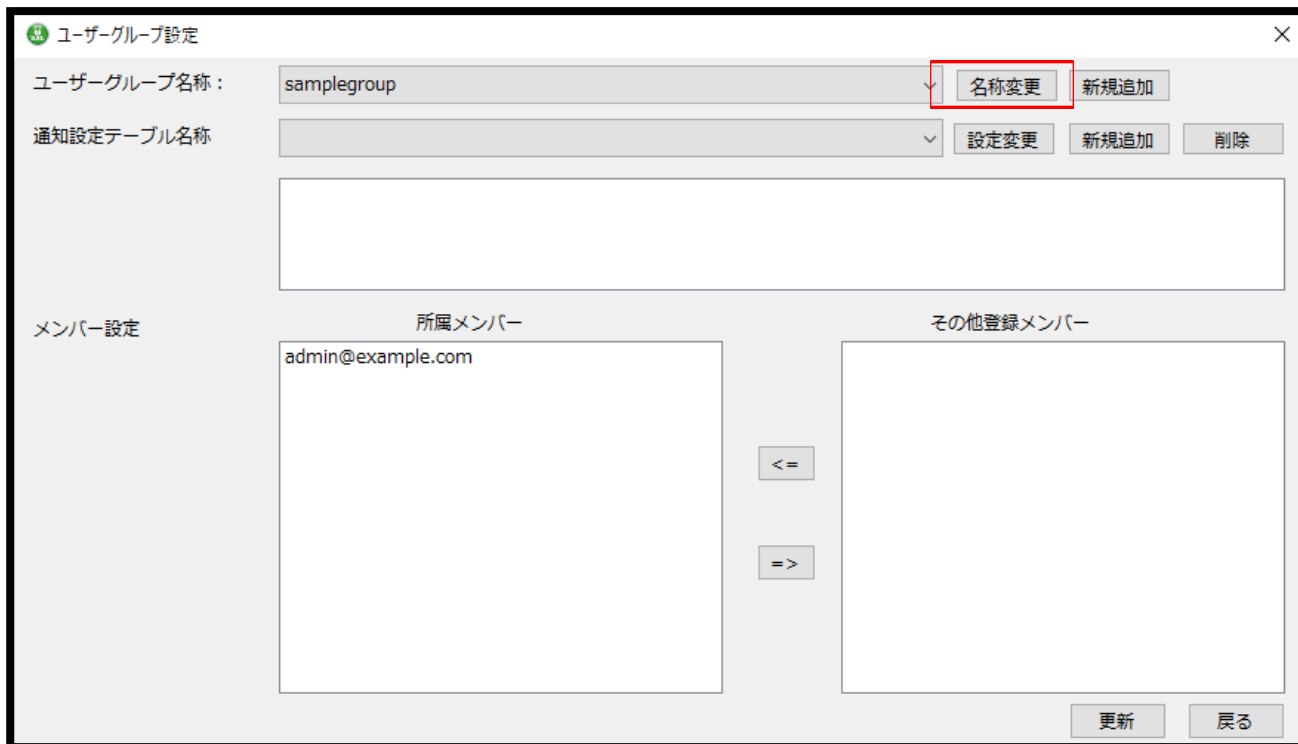


図 5.8 ユーザーグループ設定画面

ユーザーグループ名を入力し、<更新>ボタンを選択します。

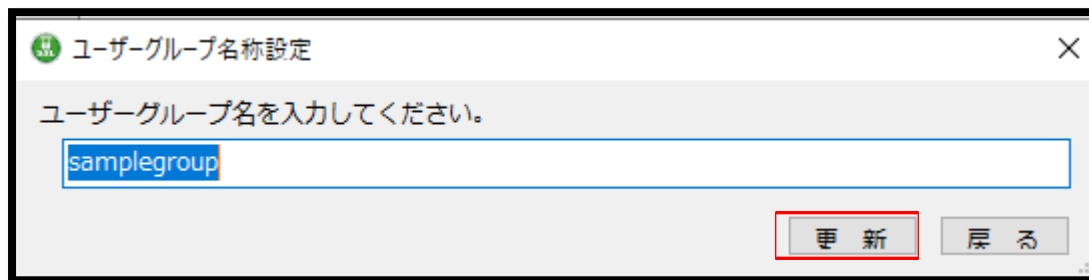


図 5.9 ユーザーグループ名入力画面



ユーザーグループ名が変更されていることを確認します。  
右下の<戻る>ボタンを選択します。

ユーザーグループ設定

ユーザーグループ名称: サイト運用チーム

通知設定テーブル名称

メンバー設定

所属メンバー

admin@seiko-sol.co.jp

其他登録メンバー

<=

=>

これで、初期設定は終了となります。  
アプリケーションを一度終了し、再度起動した後、新しく作成したユーザアカウントでログインできることを確認してください。

## 6. 共通設定

本章では、本製品をご利用する際に、共通で行う画面と設定を説明します。

### 6.1. ダッシュボード

ログインすると最初に表示される画面となります。



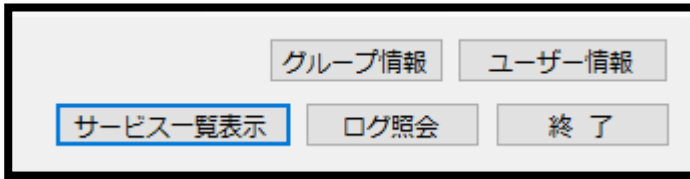
図 6.1 ダッシュボード画面

画面左上に、会社名とログイン名が表示されます。

画面中央には、以下のように情報がそれぞれ出力されます。

- ・エラー情報：赤色文字
    - 期限管理：証明書失効情報
    - 申請：申請エラー情報
  - ・ワーニング情報：黄色文字
    - 期限管理：90日未満/60日未満/30日未満/15日未満の各情報
    - 適用：サービス所属ノードの適用エラー情報
  - ・インフォメーション情報：黒色文字
    - 申請：申請待ち（スケジュール済）情報、申請中情報
- 各情報は、サービス詳細ページ等へのリンクとなっております。

画面右には、ボタンが配置されています。



以下のボタンはそれぞれ対応する画面へ遷移します。

- ・グループ情報：ユーザーグループ設定画面への遷移
- ・ユーザー情報：ユーザー一覧画面への遷移
- ・一覧表示：サービス一覧画面への遷移

(左上メニューの 表示→一覧表示 を選択した場合も、同様の動作となります)

ログ照会ボタンを選択すると、全体のログが表示されます。

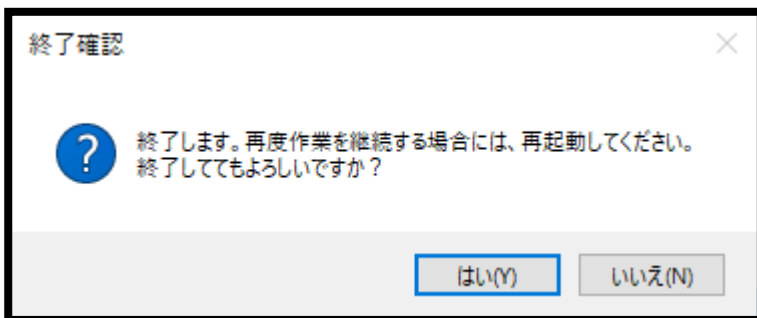
左上メニューの、メンテナンス→ログ照会 を選択した場合も、同様の動作となります。

ログ照会については、10.ログ表示をご参照ください。

終了ボタンを選択すると、アプリケーションは終了します。

右上メニューの、ファイル→終了 を選択した場合や、Windows 画面右上の「×」を選択した場合も、同様の動作となります。

はい(Y)、を選択すると、アプリケーションが終了します。



左上のメニューの設定では、以下のように画面に遷移します。

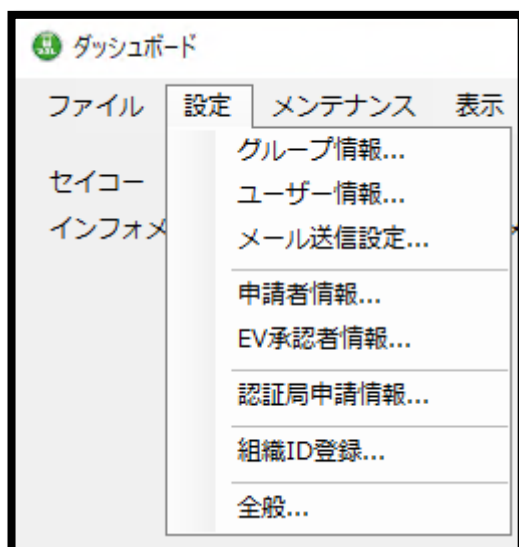
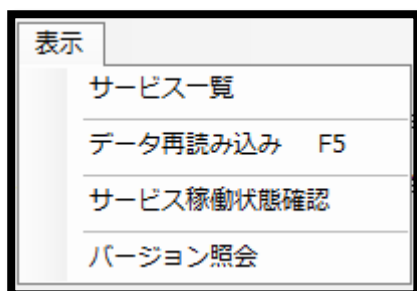


図 6.2 設定メニュー

- ・グループ情報：ユーザーグループ設定画面への遷移
- ・ユーザー情報：ユーザー一覧画面への遷移
- ・メール送信設定：メール送信設定画面への遷移
- ・申請者情報：認証局申請者情報画面への遷移
- ・EV 申請者情報：認証局申請者情報画面への遷移
- ・認証局申請情報：認証局申請情報画面への遷移
- ・組織 ID 登録：組織 ID 編集画面への遷移
- ・全般：一般設定画面への遷移

左上の表示では、以下のように画面遷移します。



- ・サービス一覧：サービス一覧画面への遷移
- ・データ再読み込み：データの再読み込みの実施
- ・サービス稼働状態確認：サービスの稼働状態画面への遷移
- ・バージョン照会：バージョン照会画面への遷移

### 6.1.1. サービスの稼働状態画面

本ソフトウェアのサービス状態を確認することが可能です。

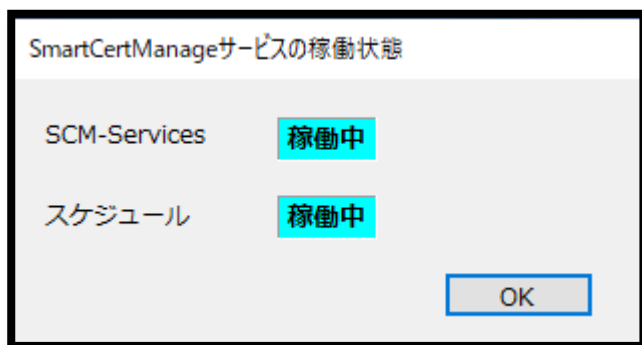


図 6.3 サービス稼働状態画面

#### 注意

全てのサービスが稼働中でない場合、本ソフトウェアは正常に動作しません。  
SCM-Service が稼働していない場合は、Windows を再起動してください。  
スケジュールが稼働していない場合は、5.1 初期設定を参考にして起動してください。

### 6.1.2. バージョン照会画面

製品バージョンとライセンス情報を確認することが可能です。ライセンス更新については、11.1 ライセンスキーの入力を参照ください。



図 6.4 バージョン照会画面

## 6.2. 一般設定

ダッシュボードのメニューから、設定→全般 で一般設定画面に遷移します。  
 プロキシの設定やタイマーの設定をします。  
 更新ボタンを選択すると、設定が完了します。

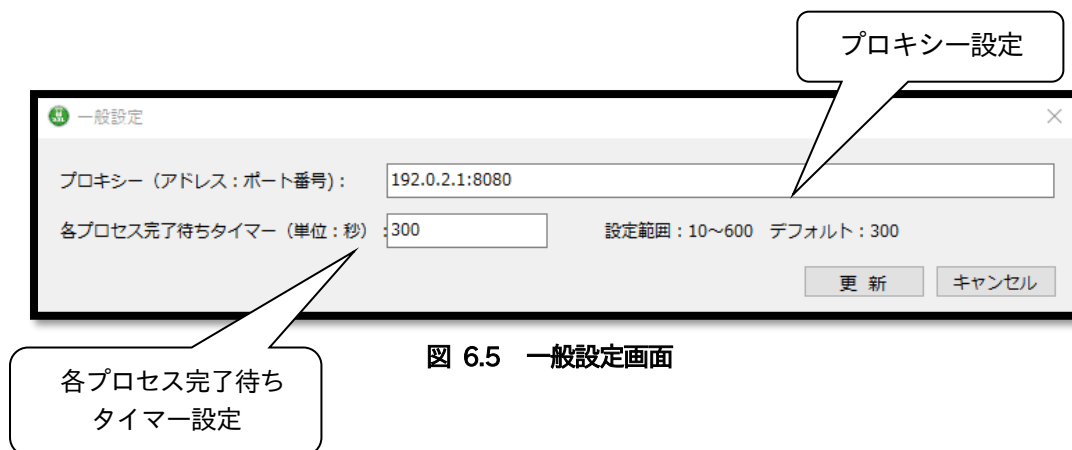


図 6.5 一般設定画面

### 6.2.1. プロキシ設定

プロキシとポート番号の設定をします  
 プロキシサーバーを IPv4 アドレス（またはニーモニック）とポート番号を、コロン（:）区切りで指定します。  
 省略した場合、プロキシを経由せずに通信します。

**注意**

プロキシを設定した場合、以下の通信がプロキシ経由の通信となります。

- ・サーバー証明書の確認のための、TLS 通信
- ・サーバー証明書を認証局へ申請、及び申請後の確認のための、restAPI 通信

**注意**

プロキシをニーモニックで入力する場合は、URL の FQDN 部分のみを入力してください  
 （例： example.proxy:8080 ）。

### 6.2.2. 各プロセス完了待ちタイマー設定

内部プロセスの完了待ちのタイマーを設定します。  
 申請する認証局のレスポンスや、適用するサーバーやロードバランサーのレスポンスなどの環境に応じて変更します。  
 通常はデフォルトのまま利用してください。

## 6.3. ユーザーグループ設定

ダッシュボードのグループ情報ボタン、またはダッシュボードのメニューから、設定→グループ情報、でユーザーグループ設定画面に遷移します。

ユーザーグループを複数設定することで、各グループに所属するユーザーは、それぞれユーザーグループに所属する証明書/サービスだけを管理・確認することが可能です。

更新ボタンを選択すると、変更した情報が設定されます。

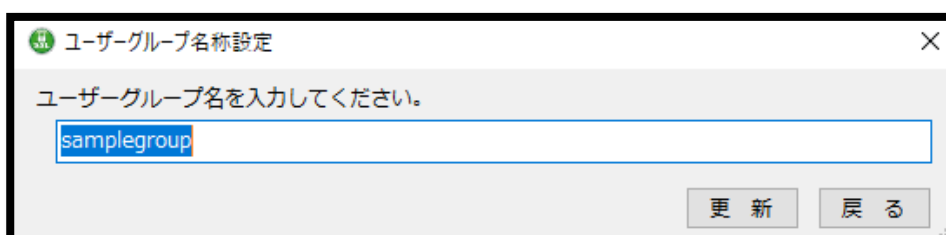


図 6.6 ユーザーグループ設定画面

### 6.3.1. ユーザーグループ選択

設定したいユーザーグループを選択します。

初期状態は1つのグループのみ設定してあります。



グループ名称を変更する場合は、名称変更ボタンを選択します。

グループを新しく追加する場合は、新規追加ボタンを選択します。

### 6.3.2. 通知設定テーブル選択

イベントをメール等で通知する場合、通知設定テーブルを選択します。

初期状態は通知設定テーブルが設定してありません。

通知設定テーブルを新しく追加する場合は、新規追加ボタンを選択すると、メール通知設定画面に遷移します。

詳しくは、6.7 メール通知設定を参照ください。

### 6.3.3. 所属メンバー設定

ユーザーグループに所属するメンバーを設定します。

左のその他登録メンバー枠にいるメンバーを選択し、<=ボタンを選択することで所属メンバーに入れます。

左の所属メンバー枠にいるメンバーを選択肢、=>ボタンを選択することで所属メンバーから外します。



## 6.4. ユーザー一覧

ダッシュボードのユーザー情報ボタン、またはダッシュボードのメニューから、設定→ユーザー情報、でユーザー一覧画面に遷移します。

既に登録されているメンバーが一覧表示されます。

ユーザーID(メールアドレス)	パスワード	権限	連絡先	編集
admin@example.com	-----	管理者	043-273-3111	編集する
admin@example.co.jp	-----	管理者		編集する
normal@example.com	-----	一般		編集する
normal@example.co.jp	-----	一般		編集する

図 6.7 ユーザー一覧画面

ユーザーを新規追加する場合は、ユーザー追加ボタンを選択します。

登録されているメンバーを変更する場合は、対象となるユーザー行の編集するボタンを選択します。

どちらかを選択した場合、ユーザー情報編集画面に遷移します。

各項目は以下のとおりです

- ・ユーザーID：本ソフトウェアにログインするアカウント名（メールアドレス）
- ・パスワード：
  - ：パスワード設定済
  - 未設定：パスワード未設定（次回ログイン時にパスワードを設定します）
- ・権限：
  - 管理者：管理者ユーザー
  - 一般：一般ユーザー
- ・連絡先：連絡先内容

## 6.5. ユーザー設定

ユーザー情報編集画面では、ユーザーID の設定、権限、パスワード、連絡先が設定可能です。  
更新ボタンを選択すると、変更した情報が設定されます。  
削除ボタンを選択すると、ユーザー情報が削除されます。

The image shows two screenshots of the 'ユーザー情報編集' (User Information Edit) form. The top screenshot shows the form with callouts for each field: 'ユーザーID設定' (User ID setting) pointing to the 'ユーザーID(メールアドレス)' field, 'ユーザー権限設定' (User Authority setting) pointing to the '権限選択' radio buttons, 'ユーザーパスワード設定' (User Password setting) pointing to the 'パスワード' and 'パスワード(再入力)' fields, and 'ユーザー連絡先設定' (User Contact Information setting) pointing to the '連絡先' field. The bottom screenshot shows the same form with callouts for the '追加' (Add) button, '更新' (Update) button, and '削除' (Delete) button.

図 6.8 ユーザー情報編集画面

### 6.5.1. ユーザーID 設定

ユーザーID をメールアドレスで設定します。  
新規追加の場合にのみ設定が可能です。

### 6.5.2. ユーザー権限設定

ユーザー権限を設定します。  
一般ユーザーは、設定情報や各種状態、ログを確認することは可能ですが、認証局への申請設定、サーバーやロードバランサーへの適用設定、その他の設定は、これを行うことができません。  
管理者ユーザーは、上記設定を行うことが可能です。

### 6.5.3. ユーザーパスワード設定

パスワードを設定します。同じパスワードを上下2つに入力して設定します。

入力したパスワードを確認する場合は、パスワードを見せる、を選択します。

新規追加の場合、次回ログイン時にパスワードを設定する、を選択すると、新規ログイン時にパスワードを設定することが可能です。

### 6.5.4. ユーザー連絡先設定

ユーザーの連絡先を設定します。

連絡先として入力する内容に制限はありません。

### 6.5.5. ユーザー追加/更新/削除

ユーザーを更新する場合は更新ボタンを選択します。

ユーザーを削除する場合は削除ボタンを選択します。

新規追加の場合、追加ボタンを選択します。

※ログインしている管理者ユーザーは削除できません。別の管理者ユーザーでログインして削除してください。

## 6.6. メール送信設定

ダッシュボードのメニューから、設定→メール送信設定 でメール通知設定画面に遷移します。本ソフトウェアからメールを送信するためのサーバアドレスやポート番号、SMTP 認証設定を行います。設定ボタンを選択すると、設定が完了します。

図 6.9 メール通知設定画面

### 6.6.1. 発信元メールアドレス設定

送信するメールの発信元のメールアドレスを、メールアドレス形式で設定します。

### 6.6.2. メールサーバアドレス設定

メールを送信するサーバーの IP アドレスを、IPv4 アドレス形式で設定します。メールを送信するサーバーのアドレスを、IPv4 アドレス形式、またはニーモニックで指定します。ニーモニックで指定する場合は、事前に Windows の名前解決設定を行ってください。

### 6.6.3. メールサーバポート番号設定

メールを送信するサーバーのポート番号を設定します。SMTP 認証設定のあり/なしに関わらず、この設定のポート番号で送信するメールサーバーに接続します。

### 6.6.4. SMTP 認証設定

送信するメールサーバーが SMTP 認証を行う場合は、SMTP 認証ありにレ点を設定します。SMTP 認証をありに設定した場合で、送信するメールサーバーが暗号化された接続が必要な場合、TLS 暗号による暗号化通信を試みます。TLS 通信は STARTTLS で行うため、対象のメールサーバーが STARTTLS に対応している必要があります。TLS 通信においてサーバー証明書の情報をチェックするために、Windows に登録されてある信頼している CA リストを参照します。

SMTP 認証を行う場合は、このあとの SMTP 認証ユーザー設定、及び SMTP 認証パスワード設定をします。

### 6.6.5. SMTP 認証ユーザー設定

SMTP 認証を行うユーザーを、メールアドレス形式で設定します。

### 6.6.6. SMTP 認証パスワード設定

SMTP 認証を行うユーザーのパスワードを設定します。

## 6.7. メール通知設定

ユーザーグループ設定画面で、通知設定テーブル設定にて設定変更ボタンまたは新規追加ボタンを選択することで、メール通知設定画面に遷移します。



メール送信をする条件設定、メールの宛先やメール内容を設定することが可能です。更新ボタンを選択すると、変更した情報が設定されます。

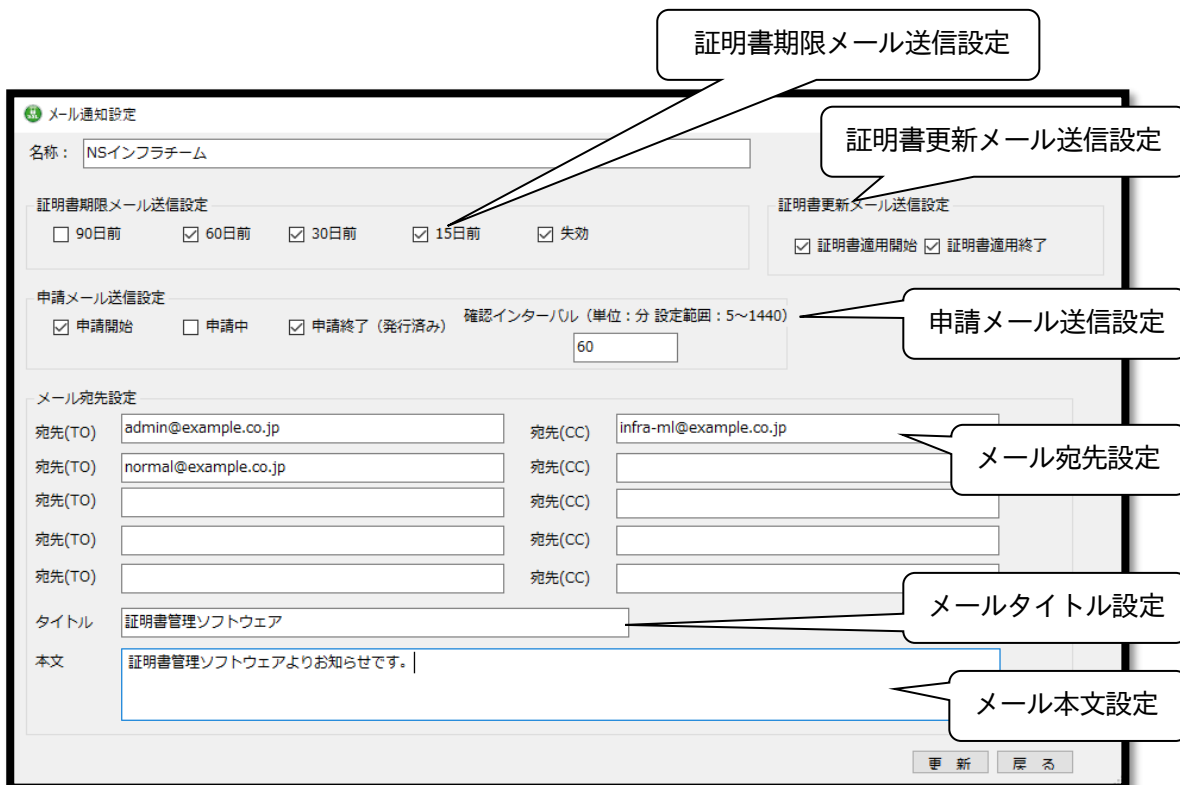


図 6.10 通知設定画面

### 6.7.1. 証明書期限メール送信設定

管理しているサーバー証明書の期限が設定した条件になった場合、メールを送信します。  
設定したい条件にレ点を設定します。

### 6.7.2. 証明書更新メール送信設定

サーバー証明書をサーバーやロードバランサーに適用する場合、その適用開始や適用終了時にメールを送信します。  
設定したいタイミングにレ点を設定します。

### 6.7.3. 申請メール送信設定

認証局に申請する場合、その申請開始や申請途中の確認した時点、また申請終了時にメールを送信します。  
設定したいタイミングにレ点を設定します。  
また、認証局に対して確認を行うインターバルを設定します。

#### 注意

メールが送信されるタイミングは以下となります。

申請開始：初回申請を実施した場合

申請中：

申請がエラーとなった場合

(ただし、エラー結果が同じ場合は、リトライ時のエラーのメールは送信されません)

申請が認証局に受理された場合

申請終了：

証明書を取得した場合

認証局から（リトライできない）終了通知があった場合

### 6.7.4. メール宛先設定

送信するメールの宛先を設定します。

TO フィールドに 5 個、CC フィールドに 5 個、あわせて 10 個のメールアドレスが設定可能です。

### 6.7.5. メールタイトル設定

送信するメールのタイトルを設定します。

### 6.7.6. メール本文設定

送信するメールの本文を設定します。

## 7. 証明書の管理

本ソフトウェアは、サービスによってサーバー証明書を管理します。  
 サービスは、1つの証明書を世代管理していくものであり、最大2世代を管理します。  
 コモンネームが同じ場合でも、別々の証明書を複数管理する場合は、サービスもそれぞれ別々に作成することになります。  
 本章では、このサーバー証明書を管理するサービスの設定について説明します。

### 7.1. サービス一覧

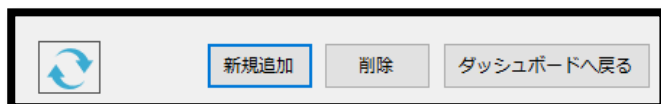
ダッシュボードの一覧表示ボタン、またはダッシュボードのメニューから、表示→一覧表示、でサービス一覧画面に遷移します。



図 7.1 サービス一覧画面

一覧表示では、1つのサービスが1行で表示されます。  
 サービスで管理している証明書が、ワーニング状態である場合は黄色に、エラー状態である場合は赤色に、それぞれ行の色が変化します。

画面右上には、ボタンが配置されています。  
 以下のボタンはそれぞれ以下の動作をします。



- ・更新ボタン（下の図）：最新のデータ読み込みと再表示
- ・新規追加：サービス情報詳細画面（新規追加）への遷移
- ・削除：選択した行の削除
- ・ダッシュボード：ダッシュボード画面への遷移

各行についての説明は以下のとおりです。

No. : 通し No.

サービス名称 : サービスの名称



コモンネーム：サービスに登録されている証明書の CN (コモンネーム)

有効期限：サーバー証明書が管理されている場合、その管理されている最新のサーバー証明書の有効期限

証明書・CSR ボタン：証明書関連設定画面への遷移

ログ照会：そのサービスに関するログを抽出したログ表示

対象の行をダブルクリックすることで、サービス情報詳細画面に遷移します。

## 7.2. サービス情報詳細設定

サービス一覧画面から新規追加ボタンの選択、または対象サービスの行をダブルクリックすることでサービス情報詳細設定画面に遷移します。

サービス情報詳細設定画面では、サービス名称の設定、管理するサーバー証明書の基本情報の設定と状態の確認、認証局に申請を行う場合の申請情報の選択が行えます。

認証局に申請を行う場合の申請情報についての説明は、8.認証局への申請を参照ください。

管理するサーバー証明書が適用されているサーバーやロードバランサーを、本ソフトウェアではノードとして管理します。

サービス情報詳細画面では、下方にサーバー証明書が適用されるノードを、一行に1つのノードでまとめて表示します。詳細ボタンを選択するとノード情報画面に遷移します。

サービス情報詳細画面のノード情報部分、ならびにノード情報画面については、9.サーバー・ロードバランサーへの適用を参照ください。

サービス名称の設定

公開鍵情報設定

有効/無効 設定

証明書コモンネーム設定

有効期限ステータス

更新ステータス

証明書情報

認証局への自動申請設定

8.認証局への申請で説明します

9.サーバー・ロードバランサーへの適用で説明します

ノード名称	有効・無効	サーバー種別	適用ステータス	シリアルNo	詳細
server_01	有効	Linux Apache	正常		詳細
server_02	有効	Linux Apache	正常		詳細

### 7.2.1. サービス名称の設定

サービスの名称を設定します。

他のサービスと区別するために、わかりやすい名称にしてください。

### 7.2.2. 有効/無効 設定

サービスの有効・無効を設定します。

このサービスは無効です

無効に設定した場合、このサービスに紐づいたサーバー証明書は、管理の対象外となり、申請・適用・期限管理は行われなくなります。

### 7.2.3. 証明書コモンネーム設定

サーバー証明書のコモンネームを設定します。

サーバー証明書の CN と同じ名称にしてください

証明書の申請やインポート、SSL 通信による確認では、実際のサーバー証明書と同一であることを確認します。

マルチ証明書の場合は、SAN にある FQDN を、下のテキストボックスに 1 行 1 FQDN として入力してください。

最大文字数は 64 バイト分となります。

### 7.2.4. 公開鍵情報設定

対象のサーバー証明書の申請のために CSR を本ソフトウェアで作成する場合、設定が必要となります。

公開鍵情報設定ボタンを選択すると、公開鍵情報画面に遷移します。

公開鍵情報の設定は、8.5 公開鍵情報の設定を参照ください。

### 7.2.5. 有効期限ステータス

証明書を管理している場合、管理している最新の証明書の有効期限がどのようなステータスであるかを表示します。

### 7.2.6. 更新ステータス

認証局へ自動申請をする場合、その更新ステータスを表示します。

### 7.2.7. 証明書情報

管理しているサーバー証明書の情報を表示します。

有効期限、シリアル番号、上位の CA 証明書（中間証明書やルート証明書）、などの情報を表示します。

本ソフトウェアでは、一つのサーバー証明書では 2 世代まで管理します。

サーバー証明書がどのノードからも参照されていない場合、古い証明書は自動的に削除されます。

また、2 つサーバー証明書を管理している状態で、サーバー証明書をインポートしたり申請していたサーバー証明書を認証局から取得した場合、2 つあるサーバー証明書のうち古い証明書を削除します。

証明書ファイルと中間証明書は別です、を選択すると、証明書ファイルのインポート時に、サーバー証明書と中間証明書を別ファイルとして取り扱います。

### 7.2.8. 認証局への自動申請設定

認証局へ自動申請をする、を選択した場合、本ソフトウェアにて認証局への申請を行います。

認証局へ自動申請をしない、を選択した場合、本ソフトウェアにて認証局への申請を行いません。

認証局への自動申請をする設定など詳細は、8. 認証局への申請を参照ください。



### 8.1.2. 申請認証局

申請を行う認証局を設定します。

### 8.1.3. 認証局 API キー

認証局 API キーを入力します。

認証局によってキーの取得方法は異なります。

#### 8.1.3.1. 認証局がデジサートの場合

認証局がデジサートの場合、CERTCENTRAL の WEB 画面左メニューから、自動化→API キーより API を発行してください。

ユーザーは、対象の証明書を管理できるアカウントを選び、API キー制限には、Orders が許可されている項目を選択してください。



図 8.3 デジサート API キー追加画面

API キーが発行されますので、このキーをコピーし、本ソフトウェアにコピーします。



図 8.4 デジサート API キー発行画面

## 8.2. 申請者情報 / EV 申請者情報の設定

ダッシュボードのメニューから、設定→申請者情報、もしくは、設定→EV 申請者情報を選択することで、認証局申請者情報画面に遷移します（サービス情報詳細から申請者情報編集ボタンを選択することで、選択した認証局申請者情報画面に遷移します）。

申請者情報/EV 申請者情報の設定画面はどちらも同じですが、選んだ情報により内部で別々に管理されます。EV 証明書を申請する場合は、EV 申請者情報も別に登録してください。

### 注意

認証局がデジサートの場合、申請者情報/EV 申請者情報は、対応する組織を選択することで、CERTCENTRAL に登録されている情報を参照して申請することが可能です。

また本項目を設定した場合、CERTCENTRAL 上の対象の組織に紐づく、申請者情報/EV 申請者情報を更新することになります。

認証局がデジサートの場合、できるかぎり CERTCENTRAL に登録されている情報を参照して申請することをお勧めします。

認証局申請者情報

テーブル名称: NSサポート部申請

申請者情報テーブル名称

ユーザーIDで申請する

ユーザーIDで申請する

データを入力する

名前 : 姓 \_\_\_\_\_ 名 \_\_\_\_\_

国コード : \_\_\_\_\_

郵便番号: \_\_\_\_\_ ハイフンなしで入力してください

都道府県: \_\_\_\_\_ 市区町村: \_\_\_\_\_

住所1 : \_\_\_\_\_

住所2 : \_\_\_\_\_

電話番号: \_\_\_\_\_ ハイフンなしで入力してください

役職: \_\_\_\_\_

メールアドレス: \_\_\_\_\_

更新 終了

図 8.5 認証局申請者情報画面(ユーザ ID 利用)

認証局申請者情報

テーブル名称: NSサポート課申請

申請者情報テーブル名称

ユーザーIDで申請する

データを入力する

名前 : 姓 聖子 名 セイコー

国コード : 日本国

郵便番号: 2618507 ハイフンなしで入力してください

都道府県: 千葉県 市区町村: 千葉市

住所1 : 美浜区中瀬

住所2 : 1-8

電話番号: 0482733111 ハイフンなしで入力してください

役職: 課長

メールアドレス: seiko.seiko@seiko-sol.co.jp

更新 終了

データを入力する

図 8.6 認証局申請者情報画面(個別入力)

### 8.2.1. 申請者情報テーブル名称

申請者情報のテーブル名称を設定します。

### 8.2.2. ユーザーIDで申請する

#### 8.2.2.1. デジサートの場合

CERTCENTRAL の対象ユーザーID を設定することで、設定申請者情報を直接入力する代わりにCERTCENTRAL の設定を参照します。

CERTCENTRAL に設定してあるユーザーID を設定する場合は、CERTCENTRAL の API 経由でユーザーID を取り出す必要があります。詳しくは弊社サポートにお問い合わせください。

### 8.2.3. データを入力する

申請者の情報を直接入力します。

情報は以下となります。

名前

国コード

郵便番号

住所1

住所2

電話番号

役職

メールアドレス

## 8.3. 組織の編集

### 注意

認証局がデジサートの場合に設定が必要となります。

ダッシュボードのメニューから、設定→組織 ID 登録、を選択することで、組織の編集画面に遷移します。組織の編集を行います。

新しく登録する場合は、新規作成ボタンを選択します。

既に設定されている組織を変更する場合は、編集ボタンを選択します。

変更を反映する場合は、更新ボタンを選択します。

削除したい場合は、削除ボタンを選択します。

組織ID編集

データを変更する場合には、データ選択後【編集】ボタンをクリックします。  
データを削除するためには、データ選択後【編集】ボタンをクリックしデータ確認後【削除】ボタンをクリックします。

ID	名称	組織番号	備考
001	NS	123456789	

組織ID編集

組織名称 : NS

組織番号 : 123456789

備考 :

削除 更新 中止

新規作成 編集

終了

図 8.7 組織 ID 編集画面

### 8.3.1. 組織名称

組織名称を設定します。

わかりやすい名称を登録してください。

### 8.3.2. 組織番号

#### 8.3.2.1. デジサートの場合

CERTCENTRAL の WEB 画面左メニューから、証明書→組織を選択します。対象となる組織の組織番号と同じ値を設定してください。





図 8.8 デジサート 組織番号取得画面

### 8.3.3. 備考

組織に紐づく情報を設定します。設定内容に制限はありません。

## 8.4. 認証局への自動申請の設定

認証局への自動申請をしたい証明書を管理するサービス情報詳細画面の申請情報の部分を設定します。認証局へ自動申請する、を選択することで、設定が可能となります。

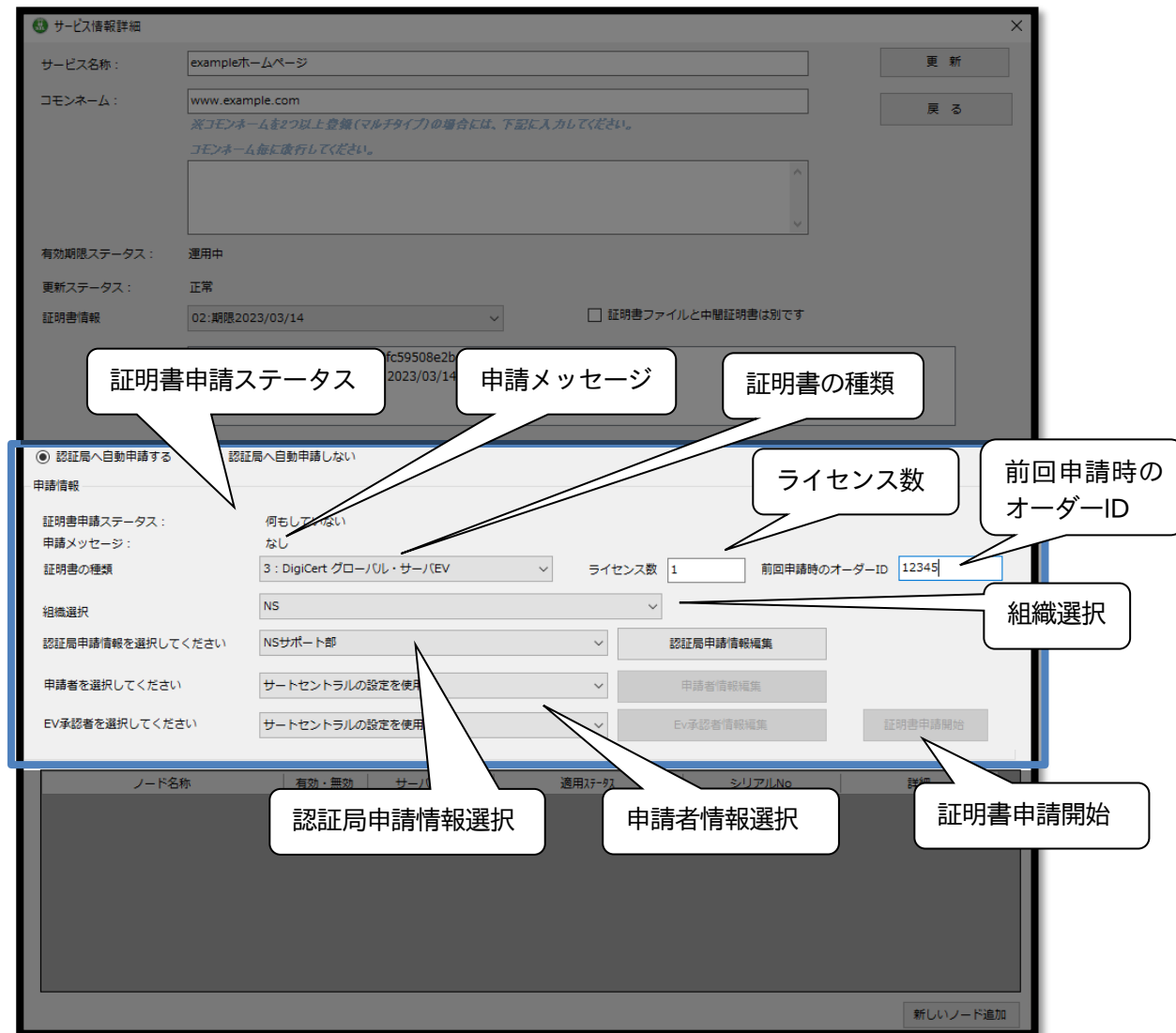


図 8.9 認証局への自動申請設定画面

### 8.4.1. 証明書申請ステータス

認証局へ自動申請をする場合、その更新ステータスを表示します。

### 8.4.2. 申請メッセージ

申請時のメッセージとなります。

### 8.4.3. 証明書の種類

申請を行うサーバー証明書の組織を選択します。

以下より選択します。

- 0:Digicert セキュア・サーバーOV
- 1:Digicert セキュア・サーバーEV
- 2:Digicert グローバル・サーバーOV
- 3:Digicert グローバル・サーバーEV
- 10:GeoTrust トゥルービジネス ID
- 11:GeoTrust トゥルービジネス ID with EV

### 8.4.4. ライセンス数

対象のサーバー証明書の必要ライセンス数を設定します。

#### 8.4.4.1. デジサートの場合

Digicert 社のサーバー証明書の場合、証明書が適用されるサーバーやロードバランサーの数に応じて設定します。

詳しくは、以下のリンク先をご参照ください。

<https://knowledge.digicert.com/ja/jp/solution/SO22948.html>

### 8.4.5. 前回申請時のオーダーID

前回申請時のオーダーID を指定します。

#### 8.4.5.1. デジサートの場合

##### 注意

認証局がデジサートの場合で更新の場合には、設定が必要となります。

CERTCENTRAL の WEB 画面左メニューから、証明書→オーダーを選択します。

対象となる証明書のオーダーの数値と同じ値を設定してください。

オーダー	証明書名	オーダーステータス
347232046 クイックビュー	d.sslsslsslssl.ddo.jp	発行済み
347224686 クイックビュー	c.sslsslsslssl.ddo.jp	発行済み

図8.1 デジサート 組織番号取得画面

#### 8.4.6. 組織選択

対象のサーバー証明書に紐づく、組織を選択します。  
組織はあらかじめ設定する必要があります。  
詳細については、8.3.組織の編集を参考にしてください。

#### 8.4.7. 認証局申請情報選択

対象のサーバー証明書に紐づく、認証局申請情報を選択します。  
認証局申請情報はあらかじめ設定する必要があります。認証局申請情報編集ボタンを選択すると、選択した情報を編集することが可能です。  
詳細については、8.1. 認証局申請情報の設定を参照ください。

#### 8.4.8. 申請者情報選択

対象のサーバー証明書に紐づく、申請者情報を選択します。  
申請者情報はあらかじめ設定する必要があります。申請者情報編集ボタンを選択すると、選択した情報を編集することが可能です。  
詳細については、8.2. 申請者情報 / EV 申請者情報の設定を参照ください。

##### 8.4.8.1. デジサートの場合

認証局がデジサートの場合は、本設定項目は CERTCENTRAL の設定を参照することが可能です。選択した組織に紐づく申請者情報/EV 申請者情報を参照します。  
サートセントラルの設定を使用、を選択してください。

#### 注意

本申請により、CERTCENTRAL の申請者情報/EV 申請者情報の設定を修正することになります。デジサートの場合はできるだけ、サートセントラルの設定を使用する事を推奨します。

#### 8.4.9. 証明書申請開始

認証局へ申請を開始します。  
証明書関連設定画面の認証局申請で、今すぐ申請を選択し申請開始ボタンを選択した場合と同じ動作を行います。

## 8.5. 公開鍵情報の設定

本ソフトウェアで CSR を作成する場合は、公開鍵情報画面で設定します。

### 注意

認証局がデジサートの場合で更新の場合には、設定が必要となります。

CSR ファイルをインポートする場合、または CSR を貼り付ける場合は、不要となります。  
更新ボタンを選択すると、変更が設定されます。

公開鍵情報(サービス名: exampleホームページ)

暗号スイート指定	rsa	暗号スイート指定
鍵長	4096	鍵長
国名	日本国	国名
都道府県	千葉県	都道府県
市区町村	Chiba	市区町村
組織名	Seiko Solutions Inc.	組織名
部門	NS	部門
メールアドレス	seiko.seiko@seiko-sol.co.jp	メールアドレス

更新 キャンセル

図 8.10 公開鍵情報画面

### 8.5.1. 暗号スイート指定

鍵の暗号スイートになります。

### 8.5.2. 鍵長

鍵長を設定します。2048 / 4096 から選択します。

### 8.5.3. 国名

日本国を設定します。

### 8.5.4. 都道府県

組織が所属している都道府県を設定します。  
最大文字数は 128 バイト分となります。

### 8.5.5. 市区町村

組織が所属している市区町村を、アルファベットで設定します。  
最大文字数は 128 バイト分となります。

### 8.5.6. 組織名

組織名を、アルファベットで設定します。

最大文字数は 64 バイト分となります。

### 8.5.7. 部門

部門を、アルファベットで設定します。部門を設定しない場合は、空欄にしてください。

最大文字数は 64 バイト分となります。

### 8.5.8. メールアドレス

メールアドレスを、アルファベットで設定します。メールアドレスを設定しない場合は、空欄にしてください。

最大文字数は 128 バイト分となります。

## 8.6. 証明書関連設定

サービス一覧画面の対象サービス行の証明書・CSR ボタンを選択すると、証明書関連設定画面に遷移します。証明書関連設定画面ではサーバー証明書の申請のための、CSR ファイル管理、認証局への証明書申請の実施、サーバー証明書ファイルのインポート・エクスポート、が行えます。

The screenshot shows the '証明書関連設定' (Certificate-related Settings) window. It is divided into three main sections:

- CSRファイル関連 (CSR File Related):** Contains radio buttons for '作成' (Create) and 'CSRインポート' (CSR Import). The '作成' option is selected. Buttons include '鍵・CSRファイルを作成する' (Generate Key/CSR File), 'CSRファイルエクスポート' (Export CSR File), 'ファイルインポート' (File Import), and '入力データインポート' (Import Input Data).
- 認証局申請 (CA Application):** Contains radio buttons for '今すぐ申請' (Apply Now) and '日時を指定して申請' (Apply with Date/Time). The '今すぐ申請' option is selected. Fields for date (2022/12/14) and time (18:42) are present, along with an '申請開始' (Start Application) button.
- 証明書入出力業務 (Certificate Import/Export Business):** Contains instructions and buttons for '証明書エクスポート' (Export Certificate) and '証明書ファイルインポート' (Import Certificate File).

Callouts point to the following elements:

- 'CSR ファイル関連設定' (CSR File Related Settings) points to the CSR File Related section.
- '認証局申請設定' (CA Application Settings) points to the CA Application section.
- '証明書入出力業務' (Certificate Import/Export Business) points to the Certificate Import/Export Business section.

図 8.11 証明書関連設定画面

### 8.6.1. CSR ファイル関連設定

CSR ファイル関連設定では、認証局に申請する CSR ファイルの準備を行います。



図 8.12 証明書関連設定(CSR 作成)



図 8.13 証明書関連設定(CSR インポート)



### 8.6.1.1. CSR 作成

CSR ファイル・鍵ファイルを作成します。

鍵・CSR ファイルを作成するボタンを選択することで作成されます。

作成したファイルは、CSR ファイルエクスポートボタンを選択することでエクスポートします。

鍵・CSR ファイルの内容については、8.5.公開鍵情報の設定で予め設定してください。

### 8.6.1.2. 貼り付けによる CSR インポート

PEM 形式の CSR 内容を貼り付けることによりインポート処理を行います。

openssl コマンドの場合、以下のようなオプションで実行することで PEM 形式が出力されます。

例として、以下のようにコマンドを実行した場合、出力された Server\_csr.pem ファイルの内容をコピーし、本ソフトウェアに貼り付けることでインポートが行えます。オプションは証明書にあわせて変更してください。

```
openssl req -new -subj "/C=JP/ST=Tokyo/O=Seiko/CN=$COMMON" -out Server_csr.pem -key Server_key.pem
```

● CSRインポート

```
MIIDBzCCAe8CAQAwYoxGTAXBgNVBAMMEGNvbW1vbk5hbWUuY28uanAxZjBjNV
BAYTAmpwMQ4wDAYDVQQIDAVjaGliYTESMBAGA1UEBwwJbWloYW1hLWt1MRlwEAYD
VQQKDAIzZWlrby1zb2wxZCzAJBgNVBAsMAm5zMRswGQYJKoZIhvcNAQkBFgxc2xA
bWFpbC5jb20wgqEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCtwsHc93+c
WrVOGHFYazPW1kIkI62mK9y/PPnp9R9PRKY8HSSJs09OI0NJ6AxFF4vTUTInzj4
LjJBrmyC1MXnEEWxeqr748iskHqrSPwKxb+8Beyqy8ZXHPEzIYFmPymvJKon9oYp
R5TWRRVWmTn39bkb8Pdw6dihBVMSEPWfVrcftS4zIno0KKmQXmXtYKulSAPjEsS
PFnizO8A/by5t8ttm6OsSH9ceyMdTkOzAJaHpXtWRP6p/vlchwWPitDj6i1rdaHT
gcQ3L883QOLBhdWwx95/FbwdLX68ZwwPy5S5FF1HTa/jKdS//X5DIUsNRpInQQ6u
KRrlLpzF1+LZAgMBAAGgNzA1BgkqhkiG9w0BCQ4xKDAmMCQGA1UdEQQdMBuCB2Fh
YS5jb22CB2JiY5jb22CB2NjYy5jb20wDQYJKoZIhvcNAQELBQADggEBAETnwGVg
0hV1imlBjevFLq/fnMv0rw9MbkBm+eDq6uvNd4di/lb7JVLBqSKoc6li99BXYjKY
EZvF1qNCmgzsFU6Mz3AMdNKdvj8x29tgHFTi6QCNHix21v5782tj+3a4RgJrXf8j
FjbxKMw95V0HgSWMSmkLU+iKMr2zaoFr6FgEWor00XIXgeOIM4zANiA1AvcSEZhk
EKzMqvtAHizd1g9Tkhpy22tgA7X5cG1CCc4nnNMYk8No+A2WwJ8wHU8hn1HKZd3
DRb4bNnUnmMGtDgboCJMmsAgICFFnoe25xJZZZIIHC88nOU09PazUALX+raYuaL
9Rbmuoc6R/VVXE=
-----END CERTIFICATE REQUEST-----
|
```

ファイルインポート      入力データインポート

貼り付け後に、入力データインポートボタンを押すことでインポートされます。

### 8.6.1.3. ファイルによるインポート

PEM 形式の CSR ファイルでインポートします。

ファイルインポートボタンを選択すると、ファイル選択画面に遷移します。

対象の CSR ファイルを選択して開くボタンを選択します。

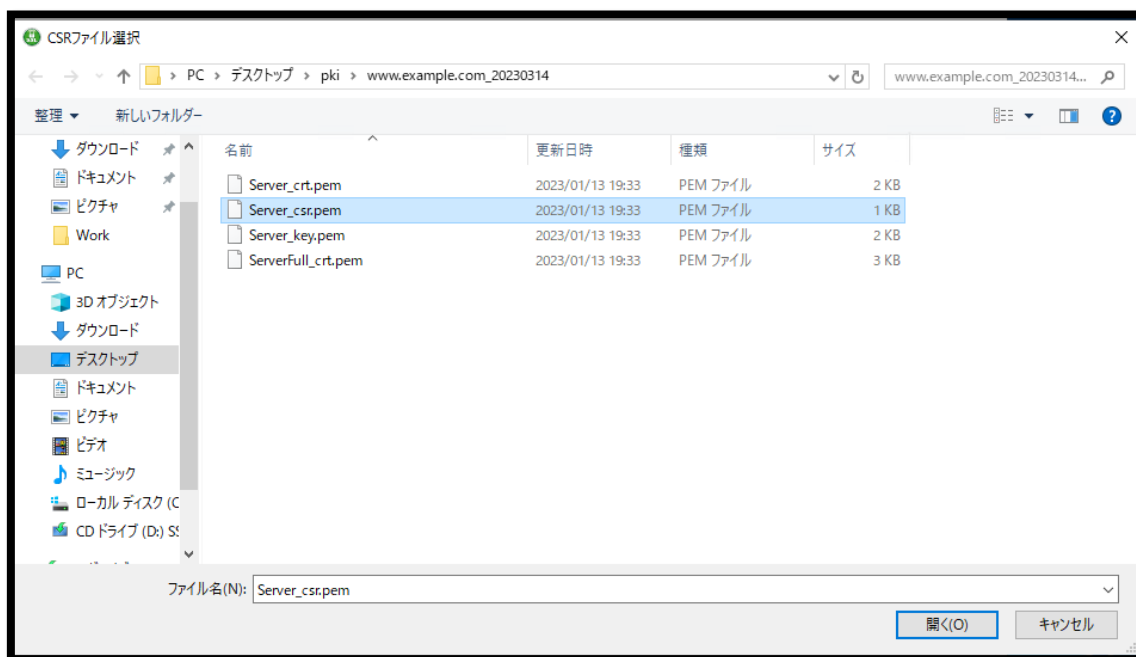


図 8.14 CSR ファイル選択画面

#### 8.6.1.4. 認証局申請時に作成

CSR ファイル・鍵ファイルを申請時に同時に作成します。

鍵・CSR ファイルの内容については、8.5 公開鍵情報の設定で予め設定してください。

## 8.6.2. 認証局申請設定

認証局に申請を実施します。

申請開始ボタンを選択すると、選択したタイミングで申請が開始されます。

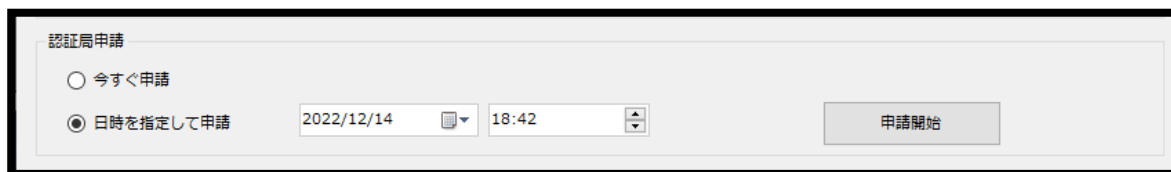


図 8.15 認証局申請設定画面

今すぐ申請を選択した場合、認証局への申請はすぐに実施されます。

日時を指定して申請を選択した場合、指定した日時に申請が実施されます。

どちらの場合でも、申請時に情報が間違っていた場合や不足している場合はエラーとして、一定時間後に申請を実施します。

予約中の場合は申請をキャンセルボタンが表示されます。キャンセルボタンを選択すると、申請していた予約をキャンセルすることが可能です。

### 注意

申請時にエラーであるかどうかはサービスのログを確認します。エラー内容をもとに、認証局への申請設定を見直して修正をしてください。

### 注意

申請中は、以下の処理が行えません。申請開始する前に確認をしてください。

- ・ サービス情報詳細 申請情報の設定変更
- ・ 証明書関連設定 CSR ファイル関連の設定および認証局申請の設定

### 8.6.3. 証明書入出力業務

証明書入出力業務では、証明書のエクスポートとインポートが行えます。

証明書をインポートした場合、既に管理されている証明書がある場合、より期限が古い証明書が削除されます（1つだけ管理されている場合は削除しません）。また、インポートされた証明書も含めて、期限がより新しい証明書がサービスの最新証明書に設定されます。

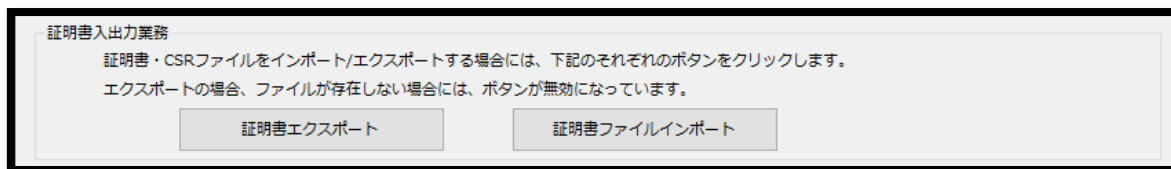


図 8.16 証明書入出力業務画面

#### 8.6.3.1. 対象の証明書ファイルについて

選択されている証明書が、エクスポートの対象となる証明書となります（選択しない限りは、最新証明書に設定されています）。

また、サービス詳細画面の、証明書ファイルと中間証明書ファイルは別です、がチェックされている場合は、サーバー証明書ファイルと中間証明書ファイルは別々にインポートすることになります。

1つのファイルにサーバー証明書と中間証明書ファイルが一緒の環境では、証明書ファイルと中間証明書ファイルは別です、のチェックは外してください。

#### 注意

ここで選択したファイルが、以下の実施で対象となります。

- ・証明書エクスポート
- ・サーバーやロードバランサーへの適用

通常は最新証明書（期限がより新しい証明書）が選択されていますので、確認のために設定を変更した場合は、期限がより新しい証明書に選択をするようにしてください。

#### 注意

インポートできる証明書ファイル・鍵ファイルの形式は PEM 形式となります。ファイル内容が PEM 形式であれば拡張子に関係なく読み込むことが可能です。

エクスポートする証明書ファイル・鍵ファイルの形式は PEM 形式となります。

### 8.6.3.2. 証明書ファイルエクスポート

認証局から申請していたサーバー証明書を本ソフトウェアが受け取った場合に、本ソフトウェアからサーバー証明書ファイルをエクスポートする場合には、証明書エクスポートボタンを選択します。

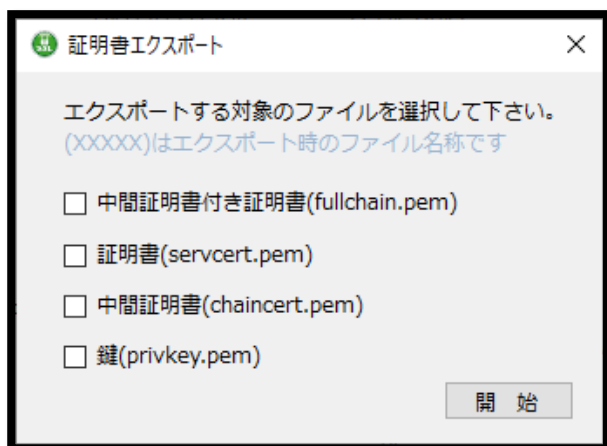
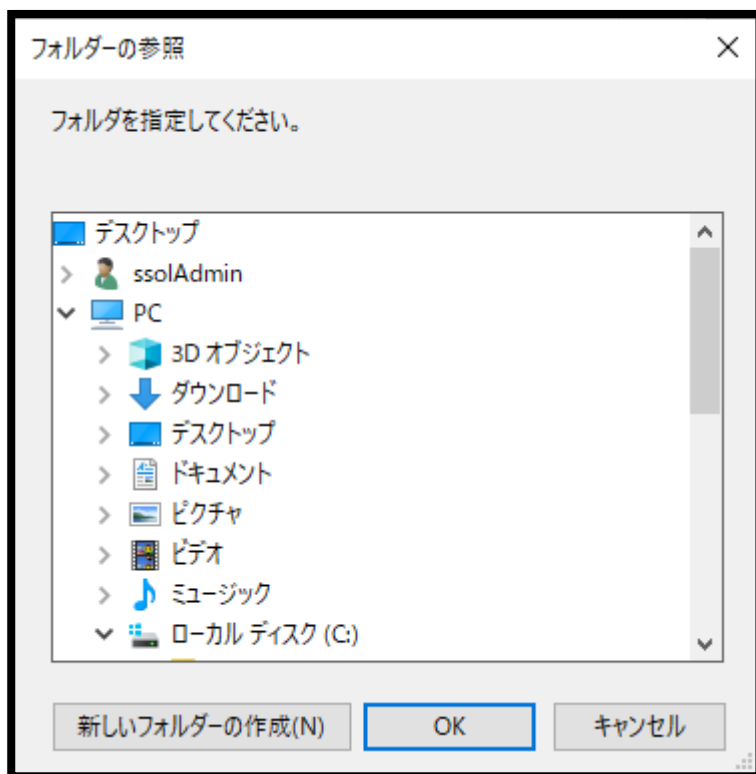


図 8.17 証明書エクスポート画面

エクスポートしたいファイルを選択し、開始ボタンを選択します。



フォルダーの参照画面に遷移しますので、エクスポートするフォルダを選択します。＜新しいフォルダの作成＞ボタンを選択することで、フォルダを新規作成します。

OKボタンを選択すると、選んだフォルダに証明書ファイルがエクスポートされます。

### 8.6.3.3. 証明書ファイルインポート

本ソフトウェアでサーバーやロードバランサーに適用のために、事前にサーバー証明書ファイルや鍵ファイルをインポートすることが可能です。

#### 注意

サービスに証明書が2件ある状態で証明書のインポートをするとインポートの成功/失敗(異常)にかかわらず古い証明書の登録が削除されます。失敗した場合登録は1件となります。

証明書申請も同様に2件ある状態では成功/失敗にかかわらず、古い証明書の登録を削除します

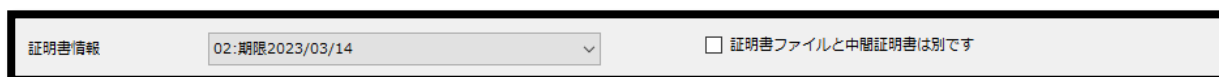
#### 注意

以下の条件の場合、証明書ファイルインポートは失敗します。

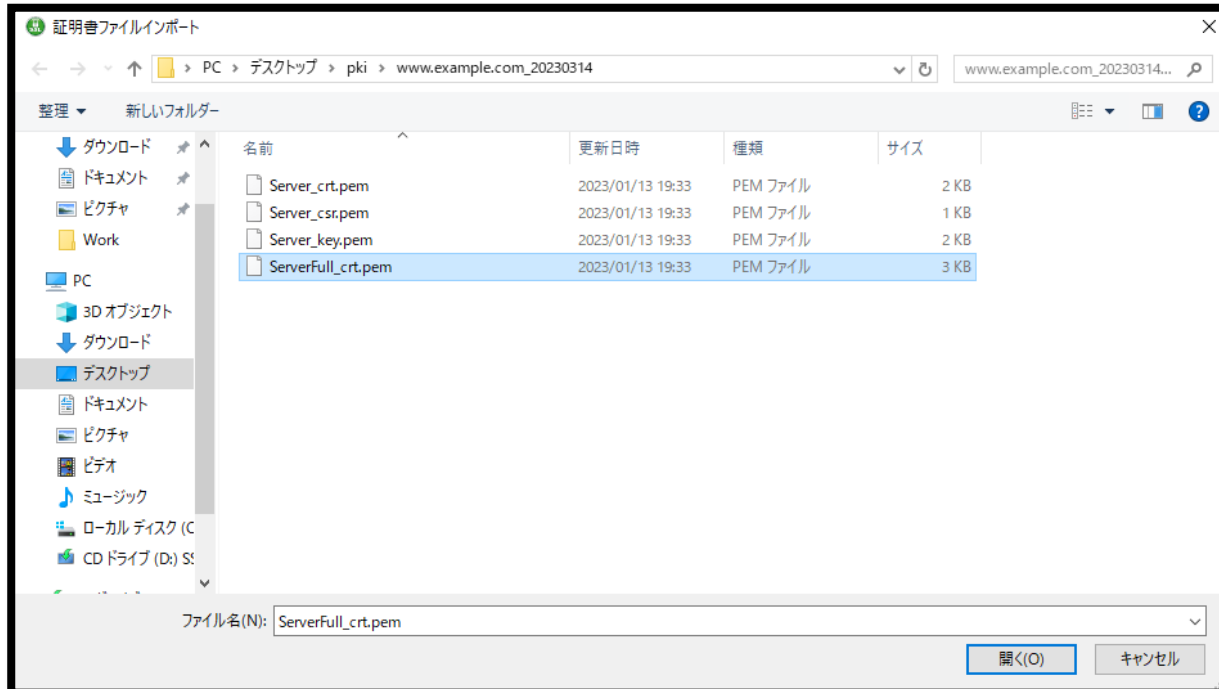
- ・ コモンネーム不一致
- ・ 一つの証明書チェーンとならない。  
重複した証明書やチェーンにならない証明書が含まれている
- ・ PEM形式以外の証明書形式

インポートの方式として、サーバー証明書と中間証明書を1つのファイルで行う方式と、別々のファイルで行う方式とを選ぶことが可能です。

これらは、サーバー証明書の証明書情報にある証明書情報で事前に設定します。

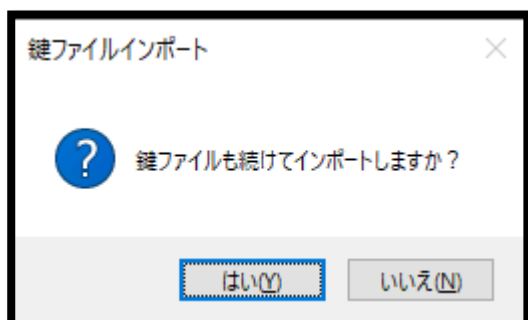


サーバー証明書ファイルや鍵ファイルをインポートするには、証明書ファイルインポートボタンを選択します。



証明書ファイルインポート画面に遷移します。

証明書ファイルを指定して開くボタンを選択すると、サーバー証明書ファイルとしてインポートされます。



続けて鍵ファイルのインポートも行う場合は、〈はい(Y)〉ボタンを選択します。  
秘密鍵インポート画面に遷移しますので、証明書ファイルと同じように、〈鍵ファイルを指定して開く〉ボタンを選択すると、鍵ファイルとしてインポートされます。

## 9. サーバー・ロードバランサーへの適用

### 9.1. サービス情報詳細(ノード一覧)

サービス情報詳細画面の下方に、ノード一覧が表示されます。

ノードは、管理しているサーバー証明書を適用・SSL通信で確認する単位となります。

ノード名称	有効・無効	サーバー種別	適用ステータス	シリアルNo	詳細
server_01	有効	Linux Apache	正常		詳細
server_02	有効	Linux Apache	正常		詳細

図 9.1 サービス情報詳細(ノード一覧)

ノードを新規追加する場合は、新しいノード追加ボタンを選択します。

登録されているノードの詳細を確認・変更する場合は、対象となるノード行の詳細ボタンを選択します。

どちらかを選択した場合、ノード情報画面に遷移します。

各項目は以下のとおりです

- ・ノード名称：登録名称
- ・有効・無効
  - 有効：適用のスケジュール設定やシリアルの確認を行う
  - 無効：適用のスケジュール設定やシリアルの確認を行わない



- ・サーバー種別：
  - Linux Apache : Linux の apache が対象
  - F5 : F5 ロードバランサーが対象
  - Windows IIS : Windows の IIS が対象
- ・適用ステータス：
  - 適用のステータスが表示されます。
- ・シリアル No :
  - 適用後に SSL 通信を行い確認をした SSL サーバー証明書のシリアル No.が表示されます。

## ノード情報

サービス詳細画面から新しいノード追加ボタンの選択、または対象ノード行の詳細ボタンの選択をすることでノード情報画面に遷移します。

ノード情報画面では、ノード名称の設定、有効無効の設定、SSL 通信による確認方法の設定、適用するサーバ種別と種別毎の詳細設定、アクセス情報の設定、更新実施のスケジュール設定が行えます。

サービス情報へ戻るボタンを選択すると、更新を確認するプロンプトが表示されます。はい(Y)を選択すると更新が反映されます。

このノード削除ボタンを選択すると、表示されているノード情報を削除します。

The screenshot shows the 'Node Information' (ノード情報) configuration page. It includes the following fields and callouts:

- ノード名称の設定**: Points to the '名称' (Name) input field containing 'server\_01'.
- ノードの拠点設定**: Points to the '拠点' (Location) dropdown menu set to '標準DC'.
- ノード有効・無効の設定**: Points to the '有効・無効' (Status) dropdown menu set to '有効'.
- ノード確認方法の設定**: Points to the '確認方法' (Verification Method) dropdown menu set to '1:IPアドレス'.
- ノード種別設定**: Points to the '種別' (Type) dropdown menu set to '0:Linux Apache'.
- アクセス情報設定**: Points to the '証明書ファイル' (Certificate File) input field containing '/www/cert/apache/cert\_full.pem'.
- 適用スケジュール設定**: Points to the '更新予定日' (Update Scheduled Date) field showing '2023/01/16 18:42'.

Other visible fields include 'このノード削除' (Delete this node), 'サービス情報へ戻る' (Return to service information), 'IPアドレス' (192.168.2.100), 'ポートNo.' (443), 'FQDN' (www.example.com), '作業フォルダー' (/usr/local/scm/), and '適用ステータス' (Normal).

図 9.2 ノード情報設定画面

### 9.1.1. ノード名称の設定

ノードの名称を設定します。  
他のノードと区別するために、わかりやすい名称にしてください。

### 9.1.2. ノードの拠点設定

ノードがある拠点を選択します。

### 9.1.3. ノード有効・無効の設定

ノードの有効・無効を設定します。  
有効とした場合、適用のスケジュール設定や SSL 通信による証明書シリアルの確認は行いません。

### 9.1.4. ノード確認方法の設定

ノードに対して SSL 通信を行い、得られたサーバー証明書が、管理している新しいサーバー証明書であるかを確認するための、確認方法を設定します。

SSL 通信によるサーバー証明書の確認は、以下のタイミングで実施されます。

- ・本ソフトウェアによる自動適用の実施後

#### 9.1.4.1. URL による確認方法

確認方法に 0:URL を選択すると、URL による選択方法になります。

この方式を使う場合は、主にインターネット経由で SSL 通信を行い確認する場合同じになります。

確認方法 : 0:URL

URL : www.example.com

注意：URLのFQDN部分のみ入力して下さい

図 9.3 ノード確認方法の設定画面(URL)

URL には、SSL 通信するサーバーの URL アドレスを設定します。

確認時には、設定された URL アドレスに対して SSL 通信を行います。

TLS1.2 の場合は、URL アドレスの FQDN をもとにした SNI 指定にてサーバー証明書を要求します。

#### 注意

URL の FQDN 部分のみを入力してください (例： www.example.com )。

#### 9.1.4.2. IP アドレスによる確認方法

確認方法に 1:IP アドレスを選択すると、IP アドレスによる選択方法になります。

この方式を使う場合は、主にイントラネット内で SSL 通信を行い確認する場合同じになります。

確認方法 : 1:IPアドレス

IPアドレス : 192.168.2.100      ポートNo : 443

FQDN : www.example.com

図 9.4 確認方法の設定画面(IP アドレス)

IP アドレスには、SSL 通信するサーバーの IP アドレスを設定します。

ポート No には、SSL 通信するサーバーのポート番号を設定します。

FQDN に設定した内容で、SNI 指定にてサーバー証明書を要求します。FQDN を指定しない場合は、SNI 指定を行いません。

#### 9.1.4.3. 確認しない

サーバー証明書を適用した後の SSL 通信による確認は行いません。

確認ができない条件下の場合に選択します。

例えば、管理ポートからは SSL 通信が許可されていない場合で、グローバル/インターネット経由では確認できない場合や、ロードバランサー配下のサーバーの場合など、があります。

確認を行わない場合、ノード一覧に証明書のシリアル No.は出力されません。

### 9.1.5. ノード種別設定

サーバー証明書を適用するノードの種別を設定します。  
ノードの種別により、適用するための設定が異なります。

#### 9.1.5.1. Linux Apache

種別に、0:Linux Apache を選択すると、Linux 上の Apache 用の設定となります。

図 9.5 Linux Apache 用設定画面

証明書ファイルには、サーバー証明書ファイルを格納したファイルパスを設定します。SSLCertificateFile ディレクティブの設定内容となります。

鍵ファイルには、サーバー証明書の鍵ファイルを格納したファイルパスを設定します。SSLCertificateKeyFile ディレクティブの設定内容となります。

Apache 2.4.7 以前の場合は、中間証明書ファイルは別ファイルとして設定する必要があります。中間証明書ファイルに中間証明書ファイルパスを設定します。SSLCertificateChainFile ディレクティブの設定内容となります。

作業フォルダーには、本ソフトウェアが証明書を管理するワークホルダーを指定します。このフォルダーに、設定されていたサーバー証明書と新しい証明書の2世代の鍵・証明書のペアを管理します。

#### 注意

各ファイルの設定項目、並びに作業フォルダーは、全角文字や空白文字（ブランク）は設定しないでください。

#### 9.1.5.2. F5 BIG-IP

種別に、20:F5 BIG-IP を選択すると、F5 社製ロードバランサーBIG-IP 用の設定となります。

図 9.6 F5 BIGIP 用設定画面

SSL プロファイル名には、BIG-IP 上で対象となるプロファイル名称を設定します。

インポート名称には、BIG-IP 上で対象となるインポート名称を設定します。

インポート名の有効文字は、大文字/小文字アルファベット、数字、ハイフン（-）、ドット（.）、アンダーバー（\_）です。

## 9.1.5.3. Windows Server IIS

種別に、WindowsServer xxxx IIS ( xxxx 内は、2012 / 2012 R2 / 2016 / 2016 R2 / 2019/ 2022 )を選択すると、Microsoft 社製 Windows IIS 用の設定となります。

IIS マネージャーサイト名には、IIS のマネージャーサイト名を設定します。

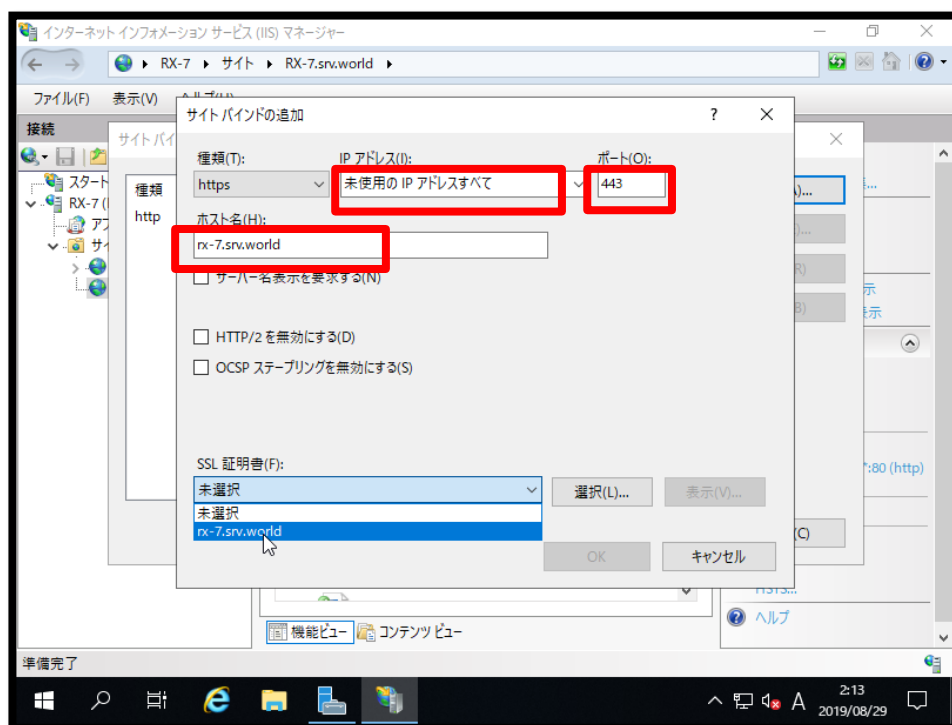
バインドホスト名には、Windows のバインドホスト名を設定します。

バインドホストは、Windows の IIS マネージャーからバインドの編集を開き、サイトバインド画面にある

- ・ホスト名
- ・IP アドレス
- ・ポート

を、弊社ソフトウェアの  
ノード編集>バインドホスト名  
に「:」区切りで指定してください。

IP アドレスが「未使用の IP アドレスすべて」の場合は「\*」を指定します。  
下の画像の場合は、 rx-7.srv.world:\*:443 となります



**注意**

Windows 上で鍵・CSR を生成した場合は、その CSR をもとに作成した SSL サーバー証明書を適用することも可能です。この場合 Windows 上にある鍵を利用するため鍵ファイルのインポートは不要です。また、この場合は、証明書を管理するサービスに、適用を実施する Windows ノードは 1 つのみ登録してください。

### 9.1.6. アクセス情報設定

アクセス情報設定ボタンを選択すると、アクセス情報画面に遷移します。  
更新ボタンを選択することで、更新内容が反映されます。

図 9.7 情報設定画面

#### 9.1.6.1. アクセス名称

アクセス情報の名称を設定します。  
他のノード情報とは別のアクセス情報名称を設定してください。

#### 9.1.6.2. アクセス用 IP アドレス

ノードにアクセスする IP アドレスを IPv4 アドレス形式で設定します。

#### 9.1.6.3. アクセス用ポート No

適用時にノードにアクセスするポート番号を設定します。  
Linux Apache の場合、SSH アクセスによる接続を行います。サーバーに設定してある SSH サーバーのポート番号を設定します。空白の場合は、22 番ポートに対してアクセスを行います。

**注意**

F5 BIG-IP の場合、Rest-API(https)による接続を行います。常に 443 番ポートに対してアクセスを行いますので、本設定による影響はありません。

Windows IIS の場合、WinRM による接続を行います。常に 5985 番ポートに対してアクセスを行いますので、本設定による影響はありません。

#### 9.1.6.4. ログイン ID / パスワード

ログイン ID には、SSH や Rest-API、WinRM で接続するログイン用の ID を設定します。  
パスワードには、ログイン ID に対応したパスワードを設定します。  
パスワードを見えるようにする、を設定すると、パスワードを確認することができます。

#### 9.1.6.5. 実行 ID / パスワード

Linux Apache の場合、SSH のログイン ID とは別に apache のデーモンの再起動など管理者（root など）の実行権限が必要な場合、その実行 ID を設定します。パスワードには、実行 ID に対応したパスワードを設定します。

#### 注意

ログイン ID のユーザーがそのまま実行できる権限が付与されている場合は、本設定は省略可能です。

#### 注意

F5 BIG-IP や、Windows IIS の場合、本設定は必要ありません。

#### 9.1.7. 適用スケジュール設定

サーバーやロードバランサーへ適用をスケジュール実行する場合は、その適用を実施する予定日時を設定します。左記の日時で自動更新設定ボタンを選択することで、スケジュールされます。  
いますぐ実行ボタンを選択すると、適用がすぐに実行されます。

#### 9.1.8. 適用ステータス

本ソフトウェアが、対象のサーバーやロードバランサーに適用を実施したステータスを表示します。  
表示は以下となります。



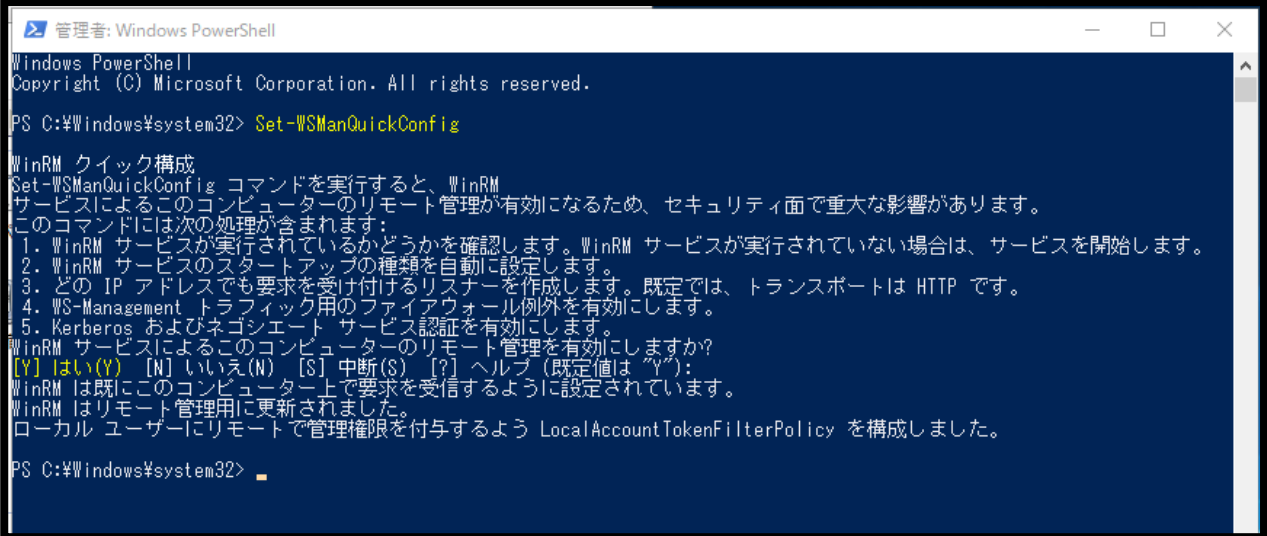
## 9.2. Windows サーバー側の設定

証明書を適用するサーバーが Windows の場合、Windows サーバー側に、WinRM 通信を有効化・通信許可する設定が必要となります。

本項目の手順により、対象サーバーの設定を実施してください。

### 9.2.1. WinRM の有効化

powershell(管理者)より『Set-WSManQuickConfig』を実行します  
有効化の確認はそのままリターン(“Y” 選択)



```
管理: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Set-WSManQuickConfig

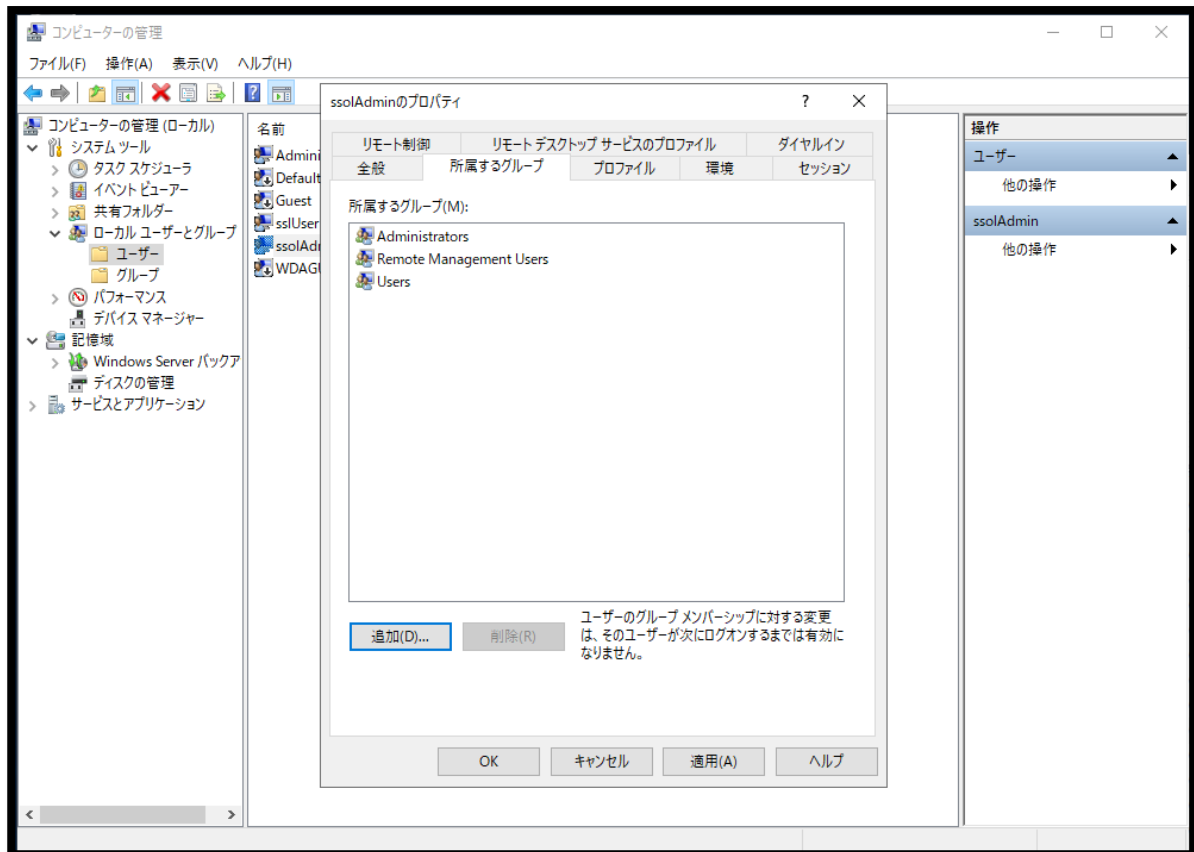
WinRM クイック構成
Set-WSManQuickConfig コマンドを実行すると、WinRM
サービスによるこのコンピューターのリモート管理が有効になるため、セキュリティ面で重大な影響があります。
このコマンドには次の処理が含まれます:
1. WinRM サービスが実行されているかどうかを確認します。WinRM サービスが実行されていない場合は、サービスを開始します。
2. WinRM サービスのスタートアップの種類を自動的に設定します。
3. どの IP アドレスでも要求を受け付けるリスナーを作成します。既定では、トランスポートは HTTP です。
4. WS-Management トラフィック用のファイアウォール例外を有効にします。
5. Kerberos およびネゴシエート サービス認証を有効にします。
WinRM サービスによるこのコンピューターのリモート管理を有効にしますか?
[Y] はい(Y) [N] いいえ(N) [S] 中断(S) [?] ヘルプ (既定値は "Y"):
WinRM は既にこのコンピューター上で要求を受信するように設定されています。
WinRM はリモート管理用に更新されました。
ローカル ユーザーにリモートで管理権限を付与するよう LocalAccountTokenFilterPolicy を構成しました。

PS C:\Windows\system32>
```

WinRM 実行時の画面

### 9.2.2. グループの追加

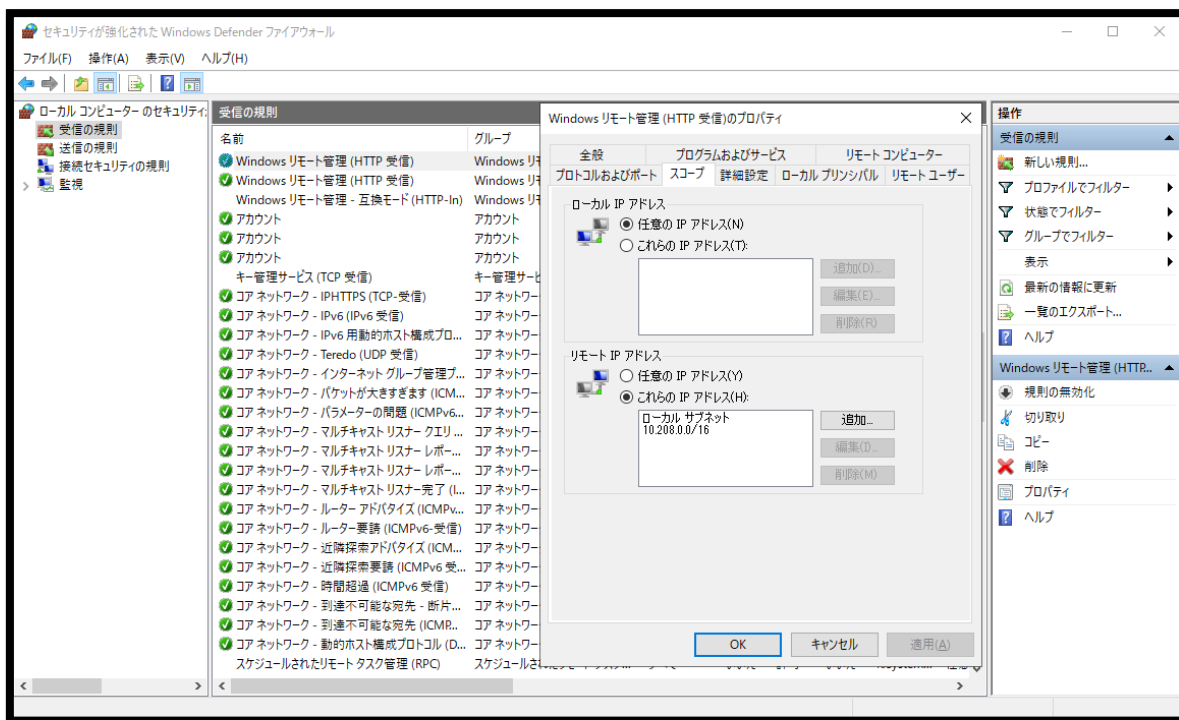
証明書適用に使用する管理者権限を持つアカウントに「Remote Management Users」グループを追加します



グループの追加画面

### 9.2.3. ファイアウォール

環境により個別にファイアウォールを設定する必要があります。  
スコープのリモート IP に接続元を追加してください。



ファイアウォール画面

## 10. ログ表示

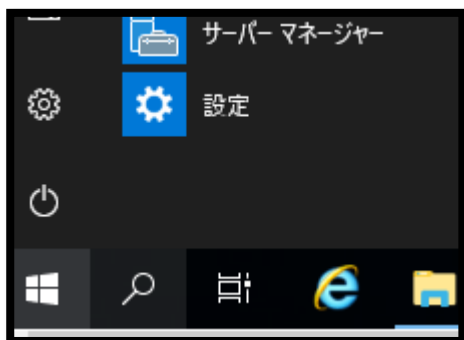
### 10.1. ログの表示

本ソフトウェアのログは、ファイルとして Windows ファイルシステム上に保存されます。

ログファイルは、拡張子「.txt」ファイルとなります。ログ照会ボタンなどを選択すると、関連付けした Windows 上のアプリケーションで開きます。

お使いのテキストエディタを、拡張子「.txt」で関連付けしてください。

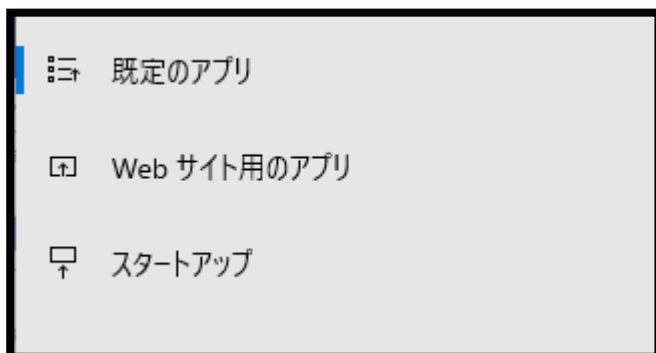
スタートメニューから設定を開きます



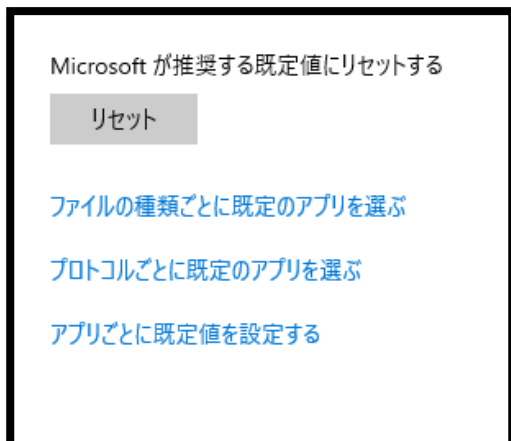
アプリを選択します



左メニューの規定のアプリを選択します



ファイルの種類ごとに規定のアプリを選ぶ、を選択します。



.txt テキストドキュメントの、規定を選ぶを選択します。



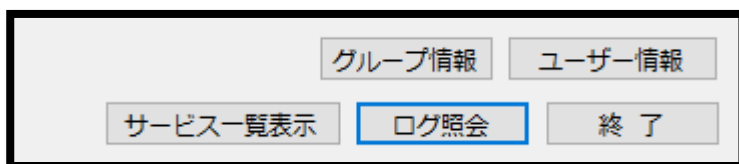
アプリケーションを選択します。

この種類のファイルやプロトコルに対応したアプリがインストールされていません。と出力される場合は、アプリケーションから選択してください。

## 10.2. ソフトウェア全体ログの表示

本ソフトウェア全体のログを表示するには、以下の方法を行ってください。

- ・ダッシュボードの、メニューのメンテナンス→ログ照会、を選択
- ・ダッシュボードの、ログ照会ボタンを選択



下図のように全体ログが表示されます。

```

2022-12-20 11:12:17.173 launchApp <10000> 00000 AMSLaunchApp Ver=1.00 module start.
2022-12-20 12:07:28.884 AMSregCERT <10000> 00001 AMSregCERT Ver=1.00 module start.
2022-12-20 12:07:29.040 AMSregCERT <10026> 00001 証明書を登録します。シリアルNo(001)=0x2751011081a0e613d7711fbaeb69660
2022-12-20 12:07:29.057 AMSregCERT <10027> 00001 データの更新を要求します。
2022-12-20 12:07:29.057 AMSregCERT <11658> 00001 証明書を登録が終了しました。
2022-12-20 12:07:29.057 AMSregCERT <10099> 00001 AMSregCERT module end.
2022-12-20 12:07:29.502 periodic <10000> 00001 AMSperiodic Ver=1.00 module start.
2022-12-20 12:07:29.580 periodic <11708> 00001 適用ステータスを更新します。test1
2022-12-20 12:07:29.612 periodic <10099> 00001 AMSperiodic module end.
2022-12-20 14:20:56.644 createParam <10000> 00001 AMScreateParam Ver=1.00 module start.
2022-12-20 14:20:56.741 createParam <12801> 00001 適用要求の生成に成功しました[000010100001000000100001]。サービス名: test1, 拠点名: NS開発部, ノード名: test
2022-12-20 14:20:56.795 createParam <10024> 00001 証明書適用ステータスを更新しました。[test:103]
2022-12-20 14:20:56.833 createParam <12802> 00001 適用要求を要求します。拠点: NS開発部
2022-12-20 14:20:56.860 createParam <W0022> 00001 通知情報が取得できませんでした。(ID=1)
2022-12-20 14:20:56.861 createParam <10099> 00001 AMScreateParam module end.
2022-12-20 14:20:59.465 apply <10000> 00001 AMSapply Ver=1.00 module start.
2022-12-20 14:20:59.468 apply <11801> 00001 適用処理を開始します[000010100001000000100001]。
2022-12-20 14:21:04.239 apply <11802> 00001 適用処理を終了しました。[000010100001000000100001]
2022-12-20 14:21:04.243 apply <10099> 00001 AMSapply module end.
2022-12-20 14:21:05.213 regResult <10000> 00001 AMSregResult Ver=1.00 module start.
2022-12-20 14:21:05.285 regResult <11801> 00001 適用の結果の更新を開始します。ノード: test, シリアル番号: 0x2751011081a0e613d7711fbaeb69660
2022-12-20 14:21:05.300 regResult <11802> 00001 適用の結果を更新しました。ノード: test
2022-12-20 14:21:05.300 regResult <10027> 00001 データの更新を要求します。
2022-12-20 14:21:05.312 regResult <W0022> 00001 通知情報が取得できませんでした。(ID=1)
2022-12-20 14:21:05.313 regResult <10099> 00001 AMSregResult module end.
2022-12-20 14:21:05.652 periodic <10000> 00001 AMSperiodic Ver=1.00 module start.
2022-12-20 14:21:05.814 periodic <10099> 00001 AMSperiodic module end.
2022-12-20 15:21:00.678 createParam <10000> 00001 AMScreateParam Ver=1.00 module start.

```

図 9.8 全体ログの表示例

### 10.3. サービス毎のログ表示

サービス毎に抽出したログを表示するには、以下の方法を行ってください。

- ・サービス一覧画面の、対象のサービス行にある ログ照会ボタンを選択



対象サービスにログが無い場合には、メッセージを表示しデータは表示されません。

## 11. メンテナンス

### 11.1. ライセンスキーの入力

ライセンスキーを本ソフトウェアに入力することで、ライセンス利用期間までライセンスに応じた証明書申請やサーバー適用を行うことが可能となります。

ライセンス利用期間を超えて継続して利用する場合は、新たにライセンスキーを取得し本手続きを行います。

#### 11.1.1. ハードウェア情報の取得

本ソフトウェアをインストールしたサーバーのハードウェア情報を取得します。

本ソフトウェアのダッシュボードから、メニュー→表示→バージョン照会を選択します。



ハードウェアキー の行にある、8桁の文字列がハードウェア情報になります。

#### 11.1.2. ライセンスキーの発行申請

ハードウェア情報の取得で確認したハードウェアキー（8桁の文字列）を購入先に送付ください。ご契約頂いているソフトウェア利用ライセンスに基づいた、ライセンスキーが発行されます。

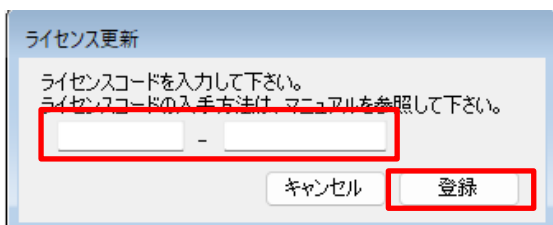
### 11.1.3. ライセンスキーの入力

本ソフトウェアに発行されたライセンスキーを入力します。

本ソフトウェアのダッシュボードから、メニュー→表示→バージョン紹介を選択します。



バージョン照会画面からライセンス更新ボタンを選択します。



ライセンス更新画面で、ライセンスキーを入力し、登録ボタンを選択します。



#### 11.1.4. ライセンス情報の確認

本ソフトウェアに入力されているライセンスを確認します。

本ソフトウェアのダッシュボードから、メニュー→表示→バージョン照会を選択します。



バージョン紹介画面で出力されている、有効期限、最大登録可能サービス数、最大登録可能ノード数、がライセンス情報となります。

ご契約されているライセンス情報と同じ内容であることを確認してください。

## 11.2. バックアップとリストア

本章では、バックアップとリストアの方法について記載します。

本ソフトウェアが管理している内容と証明書については、バックアップとリストアすることが可能です。

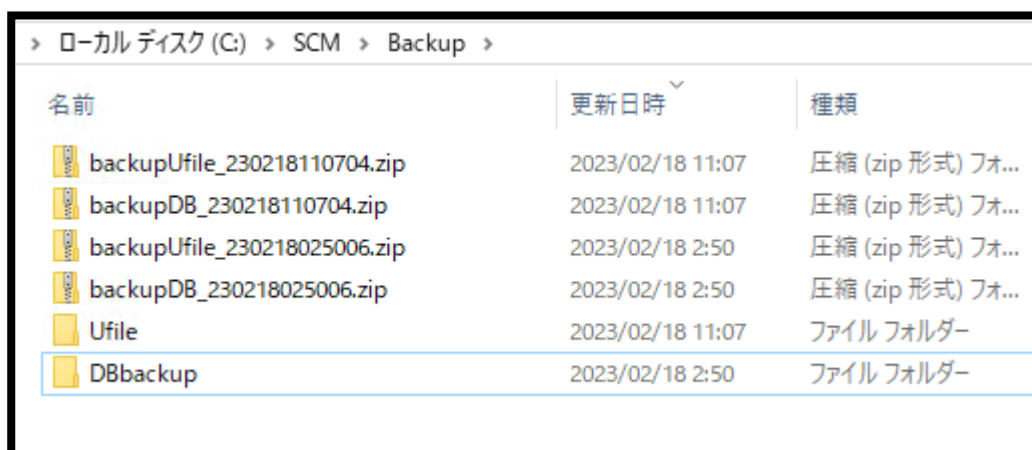
以下のようなシチュエーションにて本機能をご活用いただけます。

- ・本ソフトウェアを、現状のサーバーと異なるサーバーで運用する場合
  - ① 現状のサーバーでバックアップを実施
  - ② 新サーバーで本ソフトウェアをインストール
  - ③ ①でバックアップしたファイルにて新サーバーでリストアを実施
- ・定期的にバックアップを行い、運用しているサーバーが利用不可となったときに別のサーバーで構築する場合
  - ① 現状のサーバーで定期バックアップを実施
  - ② バックアップファイルを別のサーバー・ネットワークフォルダに配置
  - ③ 運用しているサーバーが利用不可となったときに新サーバーで本ソフトウェアをインストール
  - ④ ②でバックアップしたファイルにて新サーバーでリストアを実施

### 11.2.1. バックアップファイル

バックアップを実施すると、インストールしたディレクトリ（デフォルトは C:\scm）の配下に、Backup フォルダが作成されます。

このフォルダ配下にバックアップのフォルダとファイルが作成されます。



バックアップしたファイルは、以下の2つのフォルダとして作成されます。

- ・DBbackup：データベースの内容となります。主に管理情報となります。
- ・Ufile：ファイルの内容となります。主にサーバー証明書や中間証明書、ログ、等となります。

この2つのフォルダは、バックアップを実施したタイミングで、更新されます。

また、バックアップしたタイミングで、上記2つのフォルダの zip ファイルがそれぞれ作成されます。

この zip ファイルは、バックアップを実行した年月日時分秒の入ったファイル名となり、バックアップ実施ごとに作成されます。

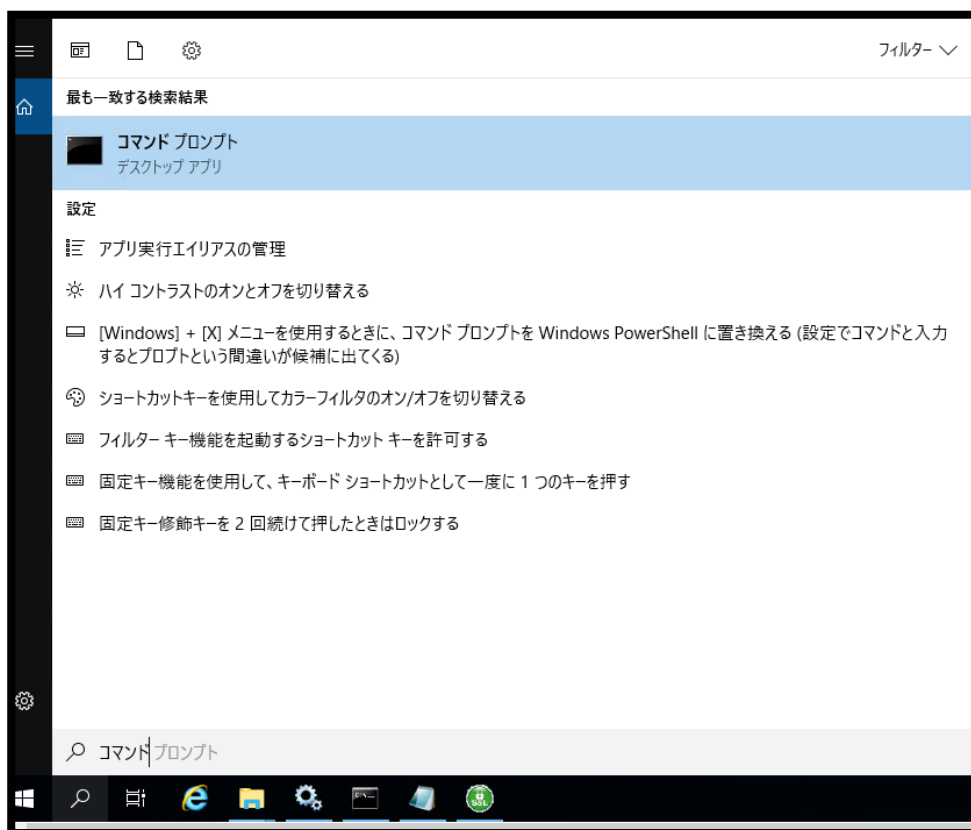
zip ファイルはバックアップ実行ごとに作成されますので、定期バックアップを行う場合は、適宜削除をしてください。

### 11.2.2. バックアップ

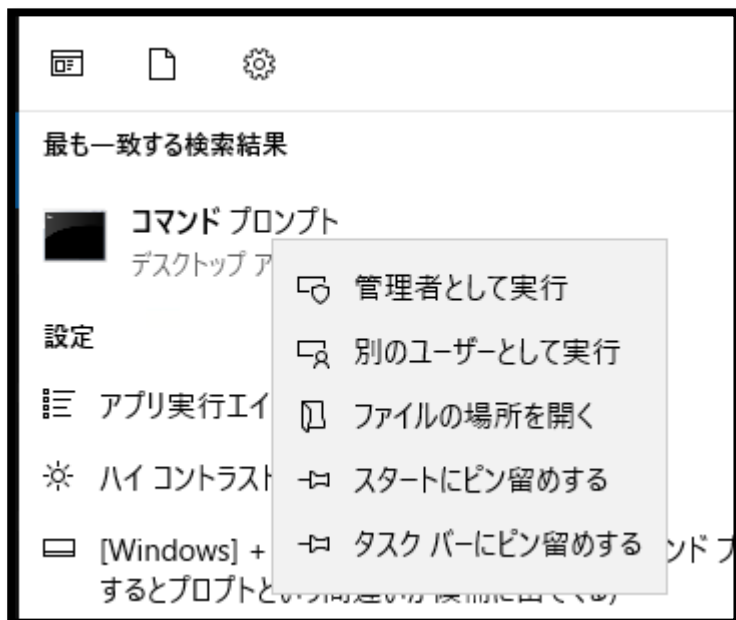
#### 11.2.2.1. バックアップコマンドの実行

バックアップの実行を、コマンドプロンプトで実行します。

Windows の左下の 🔍 窓にて、「コマンド」と入力します。



コマンドプロンプトで、マウスを右クリックし、「管理者として実行」を選択します。



コマンドプロンプトで、インストールしたディレクトリ（標準では C:\SCM）に移動します。  
バックアップを行うコマンドは、SSLbackupDB.bat となります。  
オプションを「backup」で実行します。

```

コマンドプロンプト
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ssol\Admin>cd C:\¥SCM

C:\¥SCM>.\¥SSLbackupDB.bat
"Usage: { backup | restore | support } [ <backup_folder> ]"

C:\¥SCM>.\¥SSLbackupDB.bat backup_

```

.\¥SSLbackupDB.bat backup

と入力し、Enter キーを入力することで、バックアップが実行されます。

```

C:\¥SCM>.\¥SSLbackupDB.bat backup
Backup¥ folder not exist...creating."
DBbackup¥ folder not exist...creating."
COPY 0
COPY 0
COPY 2
COPY 1
COPY 1
COPY 0
COPY 1
COPY 1
COPY 1
COPY 2
COPY 0
COPY 2
COPY 0
COPY 3
COPY 1
COPY 1
zipファイル DBbackup_230130120825.zip を作成します。"
Backup¥¥file folder not exist...creating."
powershell -NoProfile -ExecutionPolicy Unrestricted Compress-Archive -Path DBbackup¥ -DestinationPath DBbackup_230130120825.zip -Force
xcopy /e /y Ufile "Backup¥"¥Ufile
Ufile¥SpXSchedule.accdb
Ufile¥SpXSchedule.laccdb
:
:
Ufile¥USERLOG¥SVLOG¥SCH25.txt
Ufile¥USERLOG¥SVLOG¥SCH26.txt
Ufile¥Work¥C0000001.bat
Ufile¥Work¥RC0000001.txt
Ufile¥Work¥RT0000002.txt
Ufile¥Work¥RT0000003.txt
Ufile¥Work¥T0000002.bat
Ufile¥Work¥T0000003.bat
51 個のファイルをコピーしました
zipファイル Ufilebackup_230130120825.zip を作成します。"
powershell -NoProfile -ExecutionPolicy Unrestricted Compress-Archive -Path Ufile -DestinationPath Ufilebackup_230130120825.zip -Force
C:\¥SCM>_

```

Windows のエクスプローラーにて、バックアップフォルダ/ファイルが作成されていることを確認してください。

名前	更新日時	種類	サイズ
backupUfile_230218111848.zip	2023/02/18 11:19	圧縮 (zip 形式) フォ...	
backupDB_230218111848.zip	2023/02/18 11:18	圧縮 (zip 形式) フォ...	
Ufile	2023/02/18 11:18	ファイル フォルダー	
DBbackup	2023/02/18 11:18	ファイル フォルダー	

**注意**

バックアップしたファイル自体については、本ソフトウェアは管理をしておりません。ローカルに保存したままの場合、HDD 故障により失われる場合も考えられます。ストレージを冗長化する、他のファイルサーバー上に適宜移動する、などバックアップファイル管理の実施をお願いいたします。

**11.2.2.2. 定期バックアップの設定**

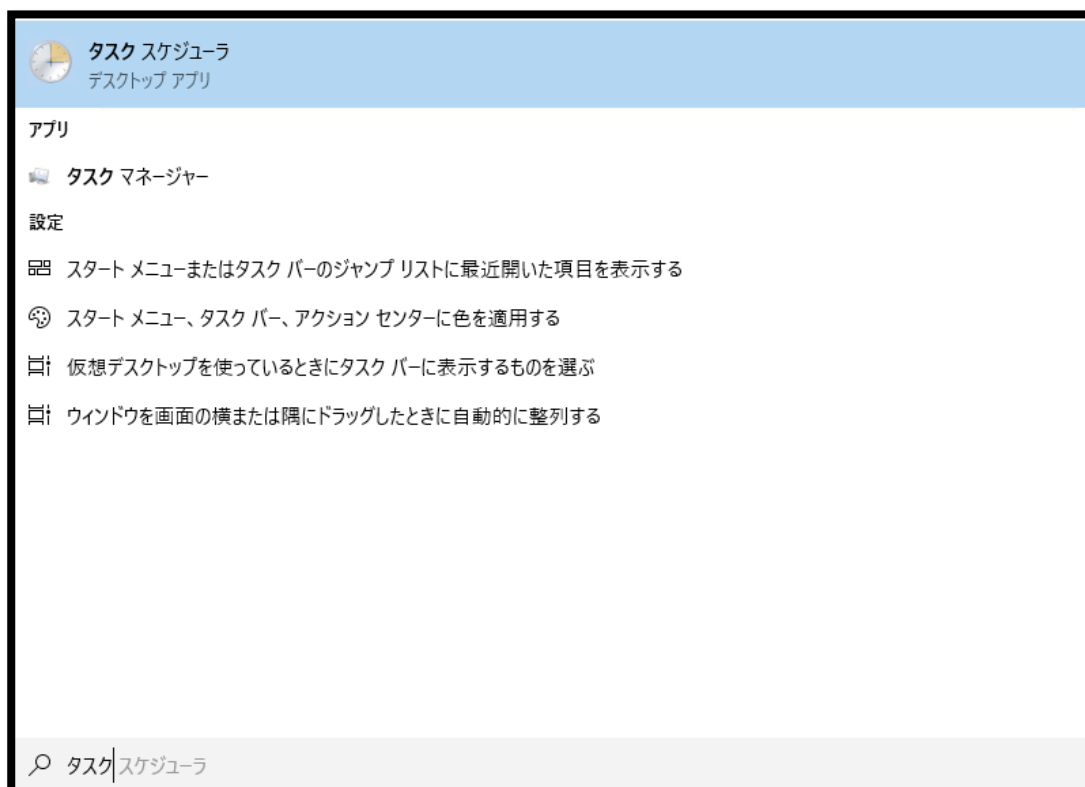
定期バックアップを設定するには、バックアップコマンドを定期実行します。Windows 標準の機能であるタスクスケジューラーに、バックアップコマンドを登録することで定期実行が行えます（他に、コマンドを定期実行するサービスを利用することも可能です）。

**注意**

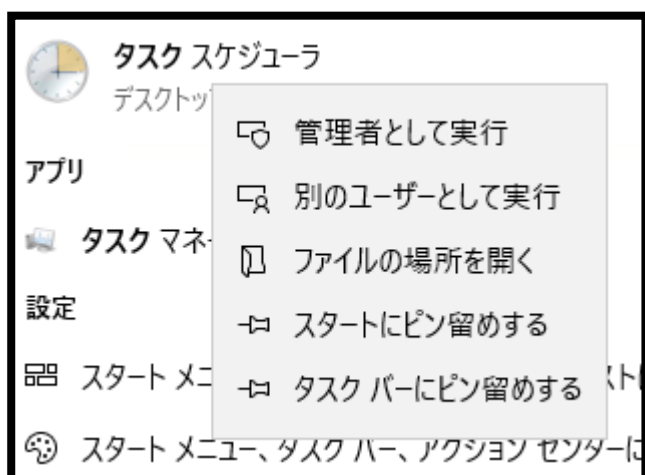
定期バックアップを設定すると、実行毎に、バックアップしたフォルダの zip ファイルが作成されます。定期的に古い zip ファイルは削除するようにしてください。

ここでは、タスクスケジューラーに登録する方法を説明します。

Windows の左下の 窓にて、「タスク」と入力します。

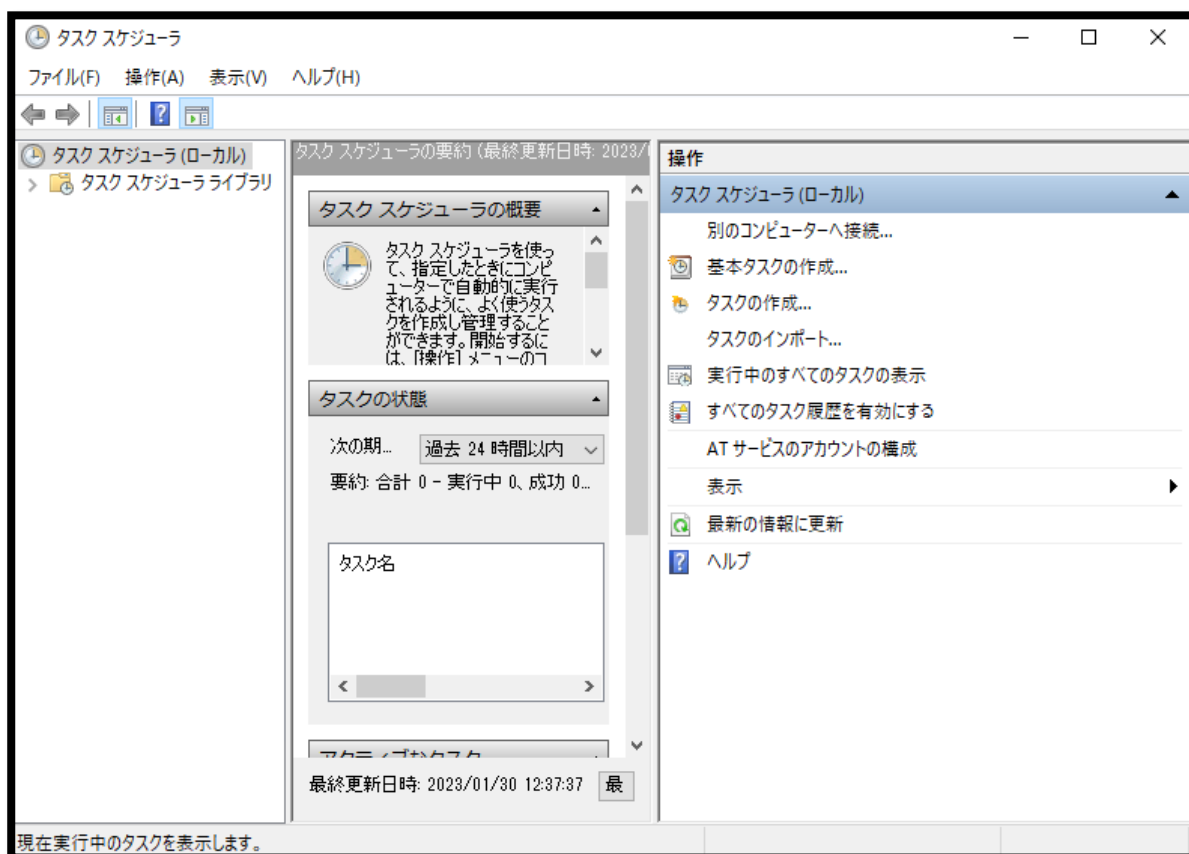


タスクスケジューラーを右クリックし、「管理者として実行」を選択します。



タスクスケジューラーが起動します。

右窓の「基本タスクの作成」を選択します。



スケジューラーの名称を設定します。わかりやすい名前にしてください。

The screenshot shows a dialog box titled '基本タスクの作成ウィザード' (Basic Task Creation Wizard) with a close button (X) in the top right corner. The main title is '基本タスクの作成' (Basic Task Creation). On the left, there is a vertical navigation pane with four items: '基本タスクの作成' (selected), 'トリガー' (Trigger), '操作' (Operation), and '完了' (Completed). The main area contains the following text: 'このウィザードでは、よく使うタスクをすばやくスケジュールします。複数のタスク操作やトリガーなどの詳細オプションや設定は、[操作] ペインの [タスクの作成] コマンドを使ってください。' (This wizard allows you to quickly schedule commonly used tasks. For detailed options and settings such as multiple task operations and triggers, please use the [Task Creation] command in the [Operation] pane.) Below this text, there are two input fields: '名前(A):' (Name) containing 'SSL証明書管理ソフトウェア定期バックアップ' (SSL Certificate Management Software Regular Backup) and '説明(D):' (Description) which is currently empty. At the bottom right, there are three buttons: '< 戻る(B)' (Back), '次へ(N) >' (Next), and 'キャンセル' (Cancel).

タスク開始間隔を設定します。  
毎日または毎週など、環境に応じて設定してください。

The screenshot shows the same dialog box, now at the 'タスクトリガー' (Task Trigger) step. The left navigation pane has 'タスクトリガー' selected. The main area contains the text 'いつタスクを開始しますか?' (When do you want to start the task?). Below this text is a list of radio button options: '毎日(D)' (Daily) - selected, '毎週(W)' (Weekly), '毎月(M)' (Monthly), '1回限り(O)' (One-time only), 'コンピューターの起動時(H)' (At computer startup), 'ログオン時(L)' (At logon), and '特定イベントのログへの記録時(E)' (At recording to log for specific events). At the bottom right, there are three buttons: '< 戻る(B)' (Back), '次へ(N) >' (Next), and 'キャンセル' (Cancel).

詳細の実施時刻などを設定します。

The screenshot shows the '基本タスクの作成ウィザード' (Basic Task Creation Wizard) dialog box. The title bar includes a close button (X). The main area is titled '毎日' (Daily) and features a clock icon. Below the title, there are fields for '基本タスクの作成' (Basic Task Creation) and 'トリガー' (Trigger). The '開始(S):' (Start) field is set to '2023/01/30' and '12:41:01'. A checkbox for 'タイムゾーン間で同期(Z)' (Synchronize across time zones) is present. The '間隔(C):' (Interval) is set to '1' day. The '操作' (Operation) section is currently empty. At the bottom, there are three buttons: '< 戻る(B)' (Back), '次へ(N) >' (Next), and 'キャンセル' (Cancel).

操作では、「プログラムの開始」を選択します。

The screenshot shows the '基本タスクの作成ウィザード' (Basic Task Creation Wizard) dialog box in the '操作' (Operation) step. The title bar includes a close button (X). The main area is titled '操作' and features a clock icon. Below the title, there are fields for '基本タスクの作成' (Basic Task Creation) and 'トリガー' (Trigger). The 'トリガー' is set to '毎日' (Daily). The '操作' section is titled 'タスクでどの操作を実行しますか?' (Which operation do you want to perform for the task?). There are three radio button options: 'プログラムの開始(T)' (Start the program) is selected, '電子メールの送信 (非推奨)(S)' (Send email (not recommended)), and 'メッセージの表示 (非推奨)(M)' (Display message (not recommended)). At the bottom, there are three buttons: '< 戻る(B)' (Back), '次へ(N) >' (Next), and 'キャンセル' (Cancel).



プログラムは、インストールフォルダ（標準では C:\SCM）にある、SSLbackupDB.bat を選択します。  
引数は「backup」を指定します。

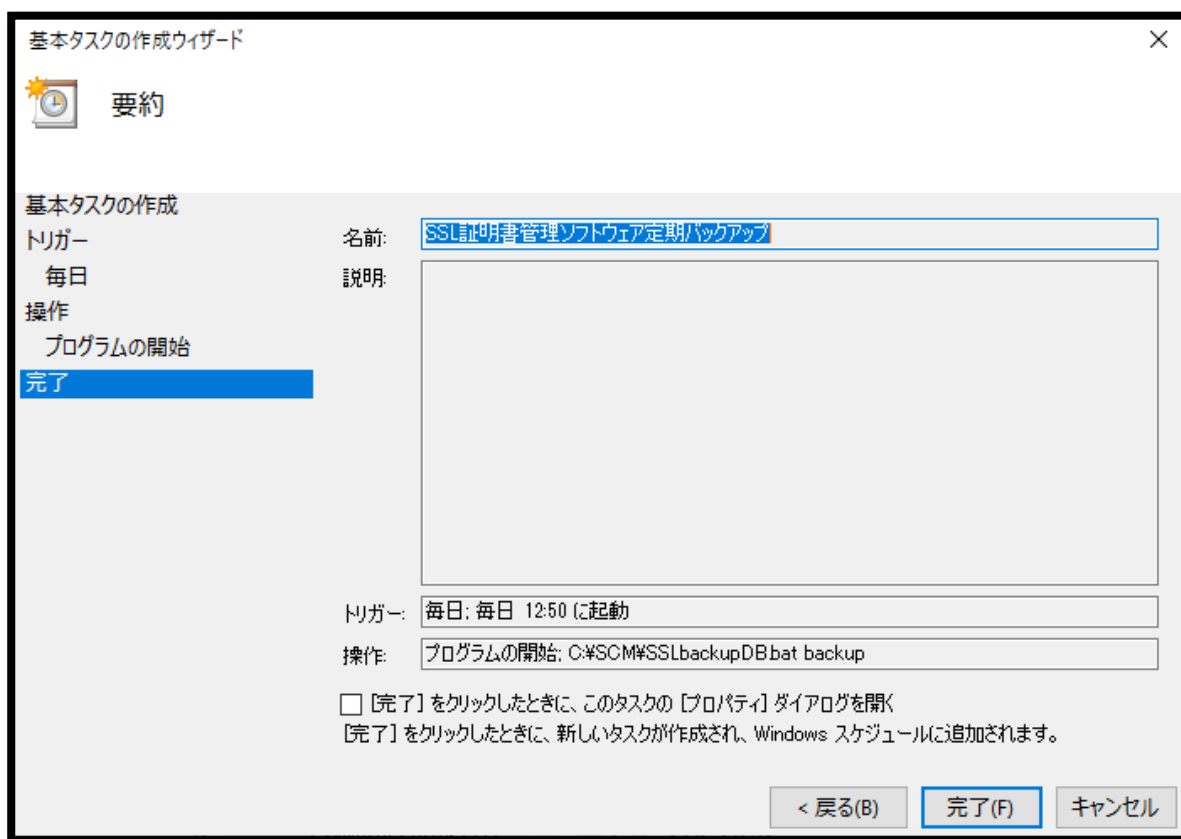
開始（プログラムを実行するパス）は、インストールフォルダ（標準では C:\SCM）を指定します。

The screenshot shows the 'Basic Task Wizard' dialog box, titled '基本タスクの作成ウィザード'. The current step is 'プログラムの開始' (Program Start), indicated by a blue highlight in the left-hand navigation pane. The main area is titled '基本タスクの作成' (Basic Task Creation) and contains the following fields:

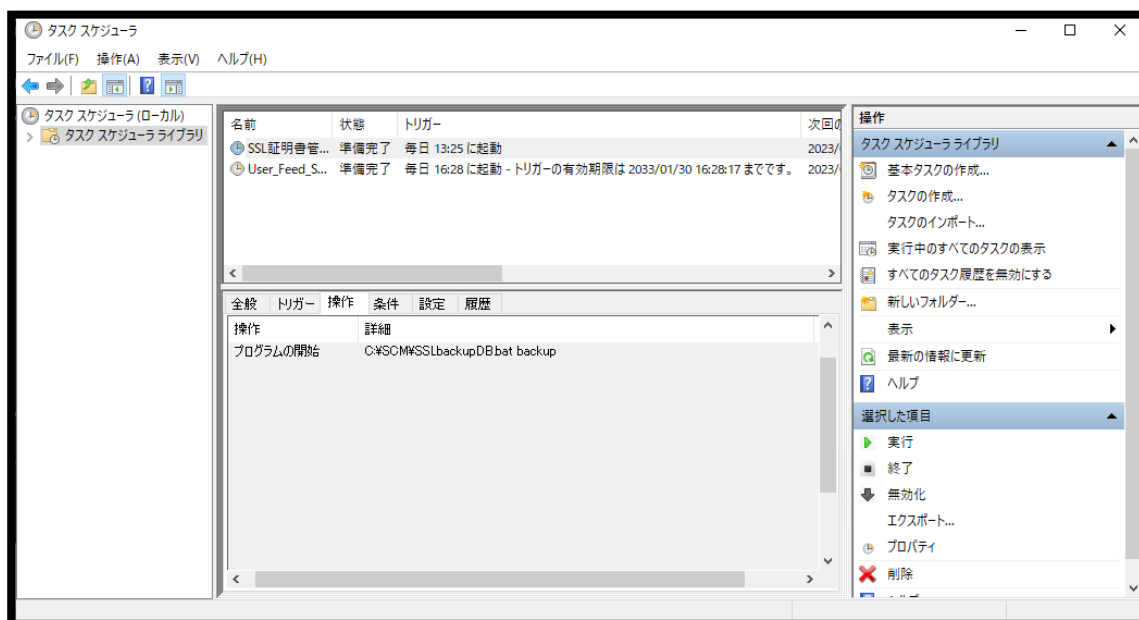
基本タスクの作成	プログラム/スクリプト(P):	引数の追加 (オプション)(A):	開始 (オプション)(T):
トリガー			
毎日	C:\SCM\SSLbackupDB.bat	backup	C:\SCM\
操作			
プログラムの開始			
完了			

Buttons at the bottom: < 戻る(B) (Back), 次へ(N) > (Next), キャンセル (Cancel).

完了を選択してください。

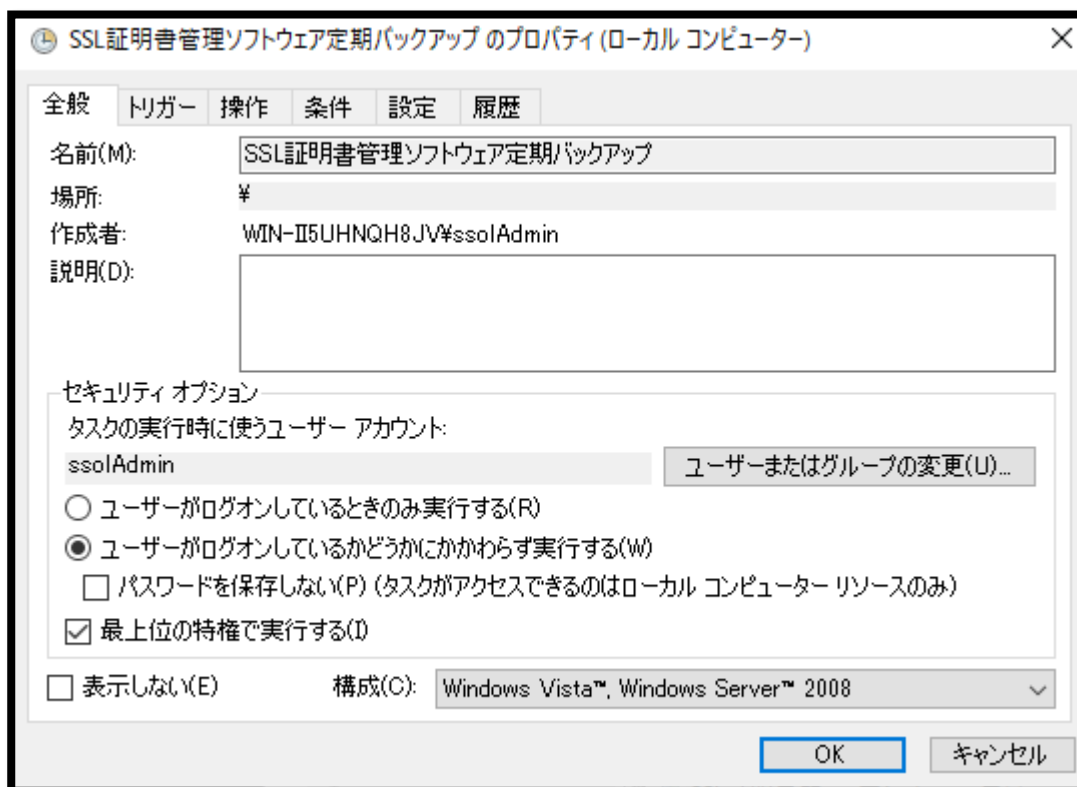


タスクスケジューラーで、真ん中の窓に、設定したスケジューラーがあることを確認してください。



右クリックしてプロパティを選択します。

「全般」タブで、「ユーザーがログインしているかどうかにかかわらず実行する」「最上位の特権で実行する」を選択してください。



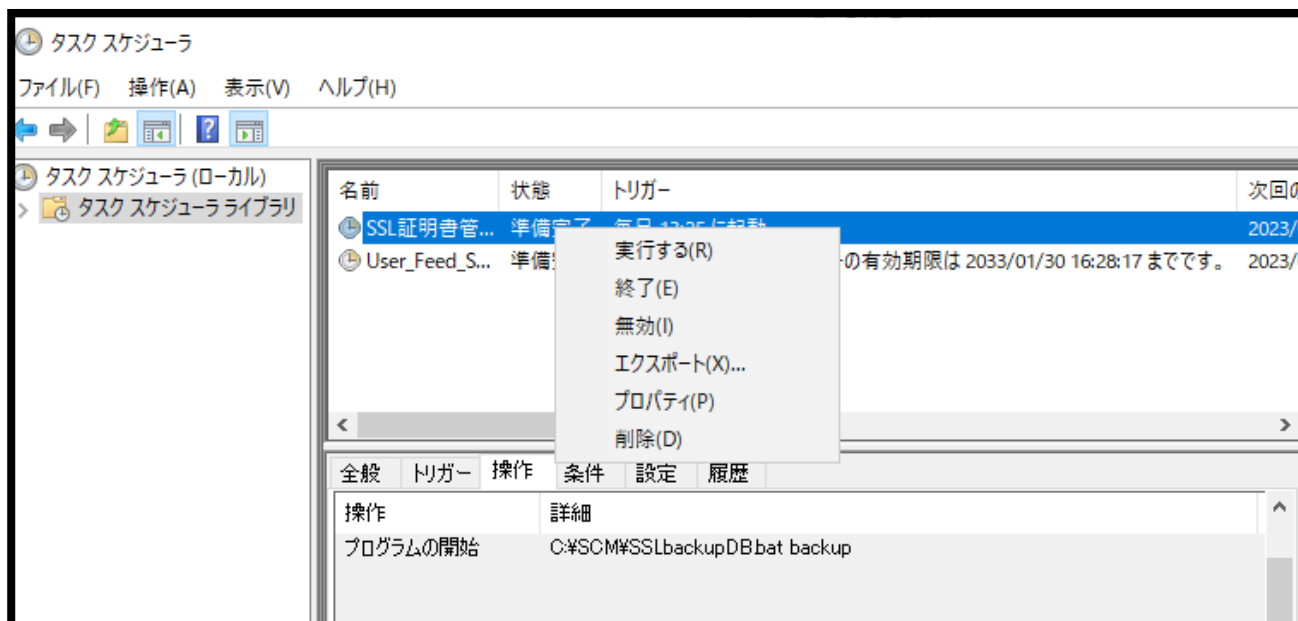
これで設定が完了しました。

動作することを確認します。

設定した時間経過後に Windows のエクスプローラーで、バックアップフォルダやファイルが作成されていることを確認してください。



すぐに確認する場合は、タスクスケジューラーの画面で、対象のスケジューラー項目で右クリックし「実行する」を選択します。



### 11.2.3. リストア

インストールを実施したソフトウェアに、バックアップファイルのリストアします。

#### 注意

リストアが行える条件は以下となります。条件が異なる場合、設定が一部リストアされません。

- ・同じソフトウェアバージョンでバックアップしたファイルが対象となります。
- ・ソフトウェアをインストールしたら、他の設定を行う前にリストアを実行してください。

#### 注意

リストア時は、以下の状態で行ってください。

- ・インストール作業をした直後（SSL 証明書管理ソフトウェアにて新しい設定を行っていない状態）
- ・SSL 証明書管理ソフトウェアが起動していない状態
- ・スケジューラーが停止している状態

#### 注意

以下の情報はリストアされません。

- ・インストール時に作成した企業名と拠点名はリストアの対象外となります（インストール時の設定を引き継ぎます）。前環境で利用していた企業名/拠点名をインストール時に入力してください。
- ・初期グループ（samplegroup または sampblegroup の名称を変えたグループ）はリストアの対象外となります。リストアを行うとインストール時に作られている sampblegroup に設定を引き継ぎますので、リストア後に名称を変更してお使いください。
- ・初期ユーザー（[admin@example.com](mailto:admin@example.com)）はリストアの対象外となります。リストアを行うとインストール時に作られている [admin@example.com](mailto:admin@example.com) に設定を引き継いでいます。前環境で利用していた場合はパスワードを再設定してお使いください。

#### 注意

リストアを実行すると、ライセンスの有効期限が失効されます。

リストア実行後は、ライセンスキーの入力を実施してください。

ライセンスキーの入力は 11.1 ライセンスキーの入力を参照ください。

#### 11.2.3.1. DB のリストア

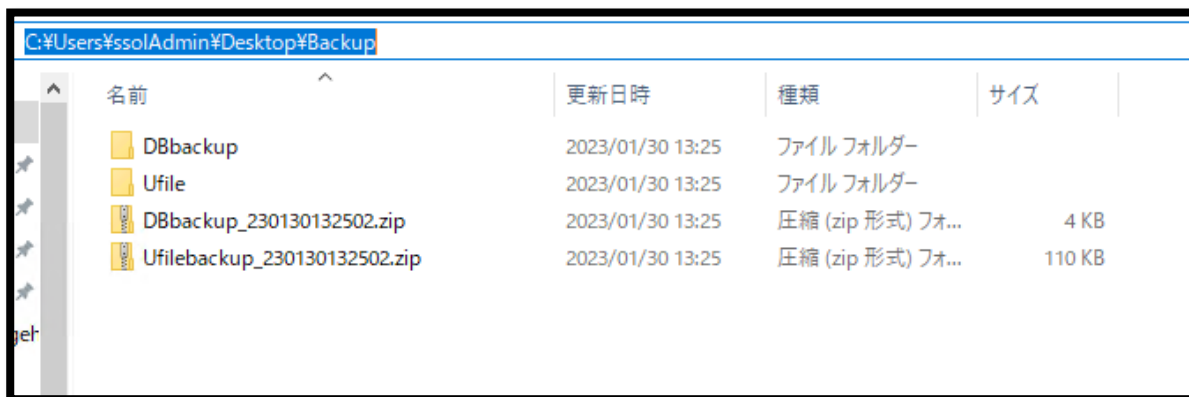
DB のリストアを実施します。

DB のリストア元のフォルダをコピーにて配置します。

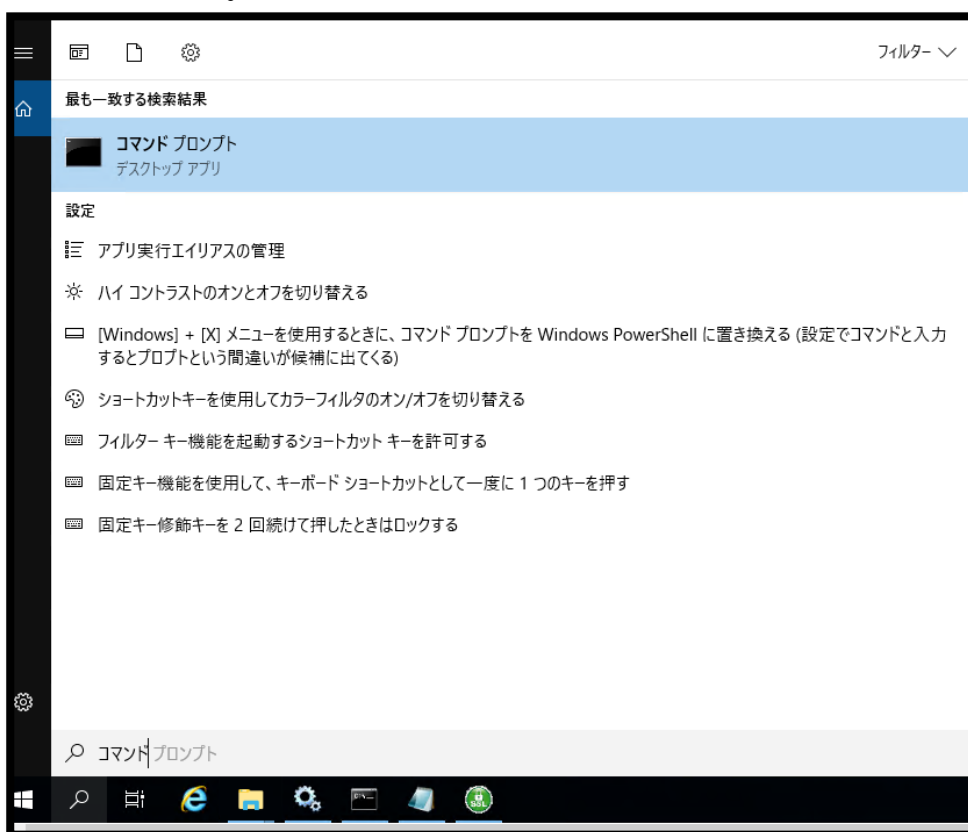
インストールディレクトリ（標準では C:\¥SCM）に、「Backup」フォルダーを作成します。

作成した「Backup」フォルダに、バックアップしてある「DBbackup」フォルダを配置します。

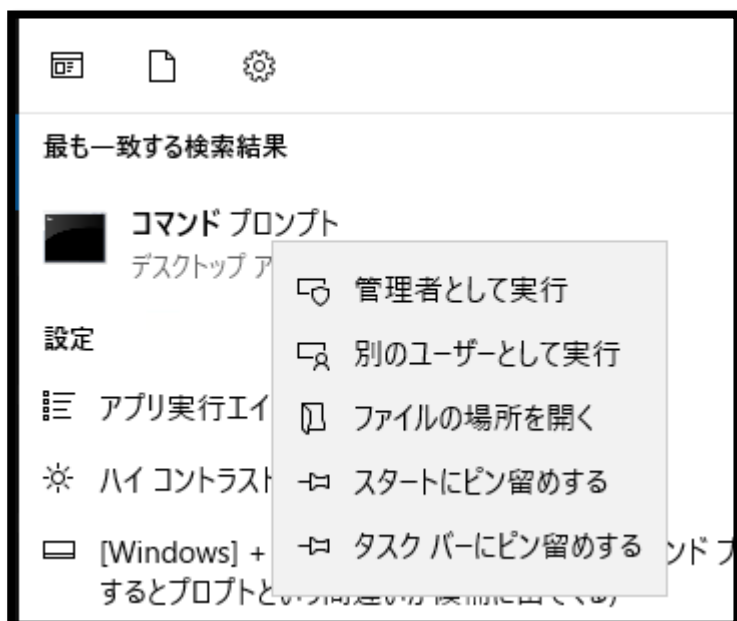
DBbackup フォルダは、バックアップ操作にて作成されたフォルダ、または、DBbackup\_xxxx.zip ファイルから解凍したフォルダを配置してください。



この状態で、バックアップコマンドを実行します。  
 バックアップコマンドは、コマンドプロンプトから管理者権限で実行します。  
 Windows の左下の 🔍 窓にて、「コマンド」と入力します。



コマンドプロンプトで、マウスを右クリックし、「管理者として実行」を選択します。



コマンドプロンプトで、インストールしたディレクトリ（標準では C:\SCM）に移動します。  
 バックアップを行うコマンドは、SSLbackupDB.bat となります。  
 オプションを「restore」で実行します。

```

CAL コマンドプロンプト
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:¥Users¥ssolAdmin>cd C:¥SCM

C:¥SCM> .¥SSLbackupDB.bat
"Usage: { backup | restore | support } [ <backup_folder> ]"

C:¥SCM> .¥SSLbackupDB.bat restore_

```

.\SSLbackupDB.bat restore

と入力し、Enter キーを入力することで、リストアが実行されます。

```
コマンドプロンプト
file%Master%periodic.bat
) 個のファイルをコピーしました
zipファイル Ufilebackup_230204183434.zip を作成します。”
powershell -NoProfile -ExecutionPolicy Unrestricted Compress-Archive -Path Ufile -DestinationPath Ufilebackup_230204183
134.zip -Force

::%SCM>
::%SCM>
::%SCM>. %SSLbackupDB.bat restore
Backup%
COPY 0
COPY 0
COPY 1
COPY 0
COPY 1
COPY 0
COPY 0
COPY 0
COPY 0
COPY 0
COPY 100
COPY 0
COPY 0
COPY 100
COPY 9
COPY 29
ノストア処理実施しました。
rem
rem
::%SCM>
```

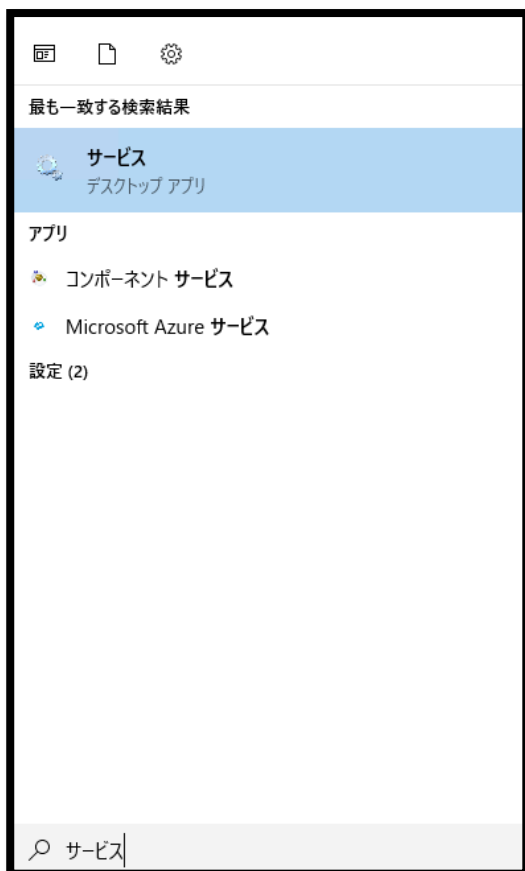


### 11.2.3.2. 証明書ファイル等のリストア

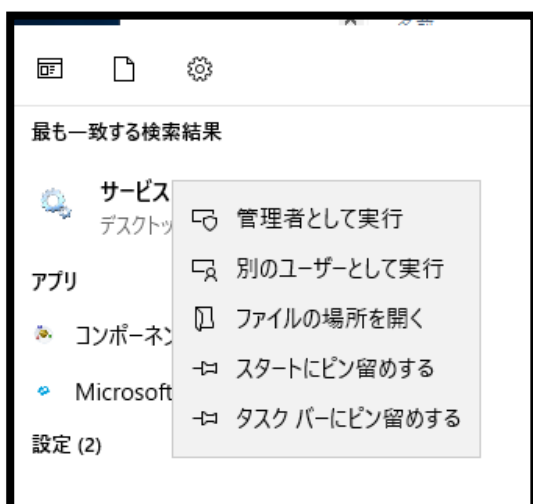
つづいて、証明書ファイル等のリストアを実施します。

実行する前に、SCM Service を停止します。

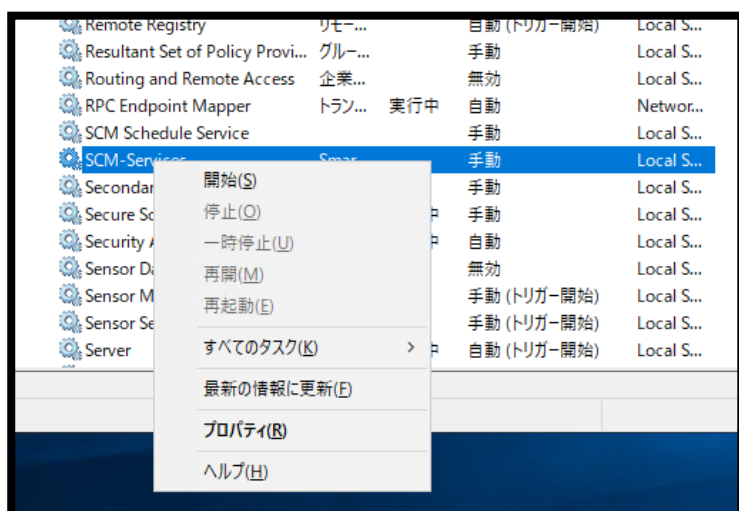
Windows の左下の $\text{\textcircled{O}}$ 窓にて、「サービス」と入力します。



サービスを右クリックし、「管理者として実行」を選択します。

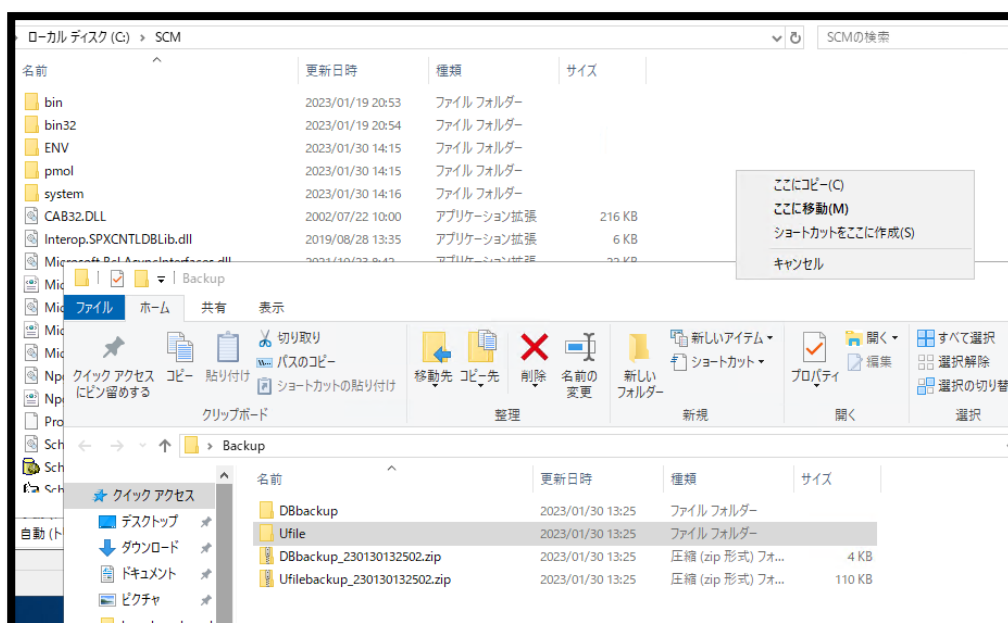


サービスから、SCM-Services を右クリックし、停止を実施します。



リストア元の backup フォルダにある Ufile フォルダをコピーにて配置します。  
 かならず、DB のフォルダと同じタイミングでバックアップした Ufile フォルダをコピーしてください。

コピー先の場所は、インストールフォルダ (標準では C:\SCM) の直下になります。  
 インストール直後は、すでに Ufile フォルダがありますので、一度 Ufile フォルダを削除し、バックアップして  
 いた Ufile フォルダを配置してください。  
 Windows エクスプローラーで行ってください。



これでリストア処理は実施済です。  
 サービスの起動を行うため、一度 Windows を再起動してください。  
 Windows が起動したら、スケジューラーを起動し、SSL 証明書管理ソフトウェアを起動して、リストア内容  
 を確認してください。

### 11.2.3.4. リストア後の設定

必要に応じて、以下の設定を行ってください

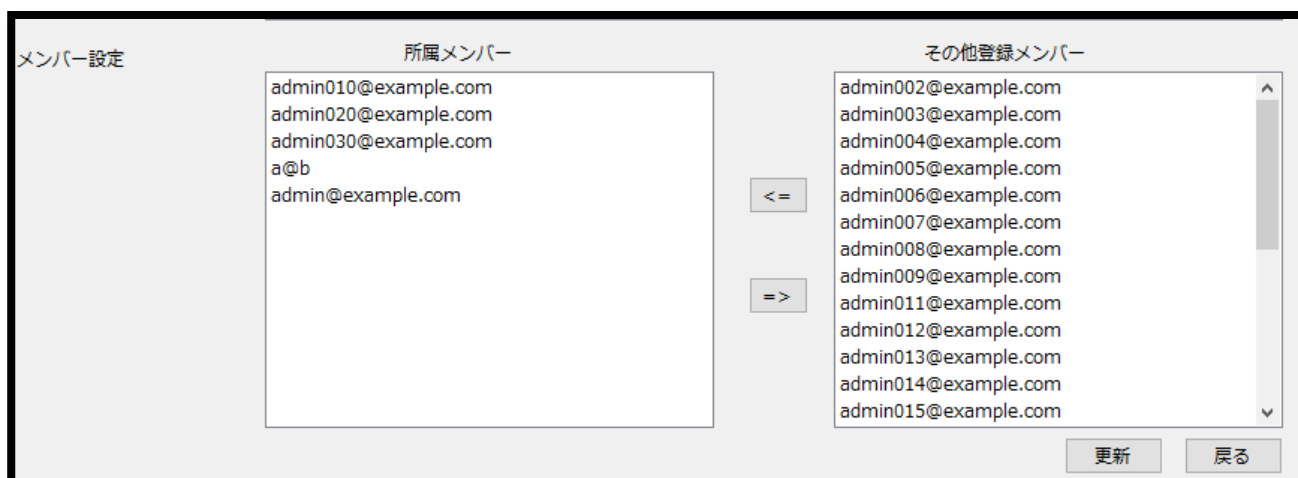
#### 11.2.3.4.1. 初期ユーザーの削除

初期ユーザーを削除して利用している環境では、リストア時に再作成した初期ユーザーを削除してください。削除については、2 インストールを参照してください。

#### 11.2.3.4.2. ユーザーのユーザーグループ所属修正

初期ユーザー（または初期ユーザーを削除した場合は別のユーザー）は、リストア時に初期グループの所属になります。

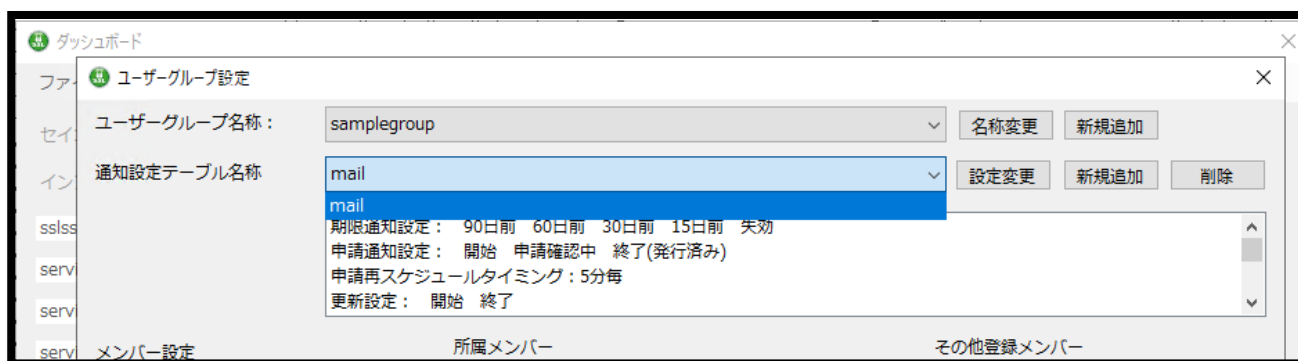
ダッシュボードから、グループ情報を選択し、対象のユーザーを適切なユーザーグループ所属に変更してください。



#### 11.2.3.4.3. メール通知設定のグループ設定

ユーザーグループに紐づくメール通知設定が解除されている場合があります。

ダッシュボードから、グループ情報を選択し、ユーザーグループごとに通知設定テーブルを括りつけてください。



### 11.3. DBのリフレッシュ

本ソフトウェアを利用している環境においては、定期的に内部DBをリフレッシュすることで、ソフトウェアのレスポンスが向上します。


以下の環境では、定期的にDBのリフレッシュをお願いします。

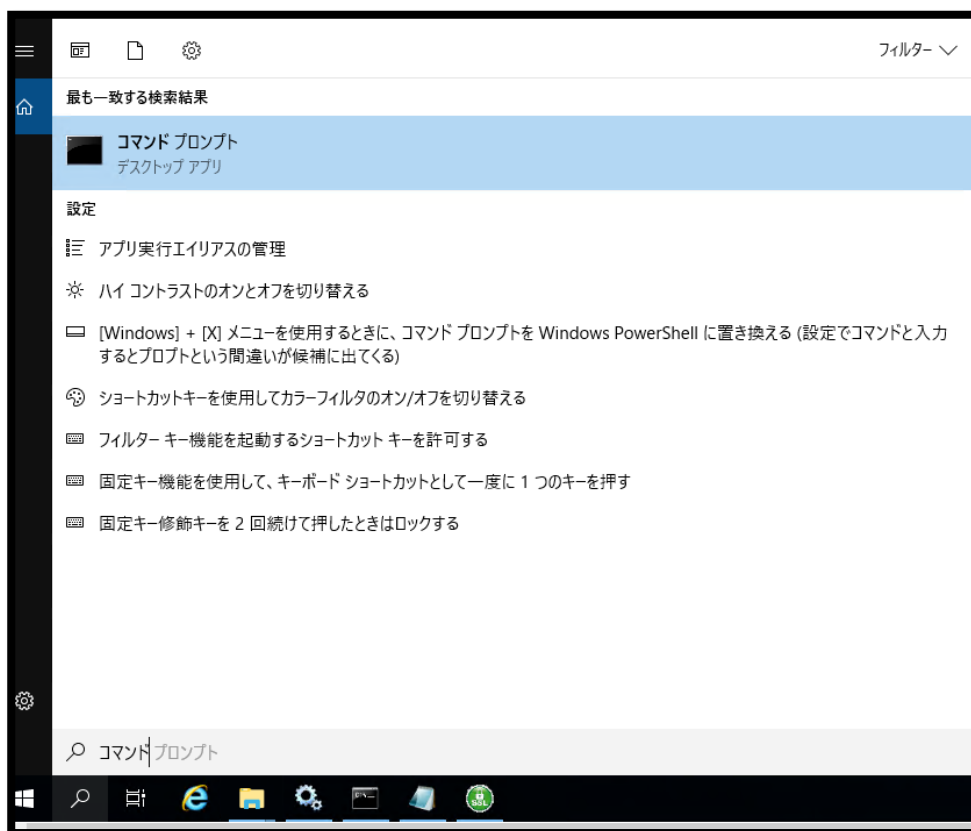
- ・比較的多いサービスを設定・管理している（数百程度）
- ・比較的多いノードを設定・管理している（数百程度）
- ・ソフトウェアのレスポンスがインストール直後と比較して顕著に遅くなってきている

#### 11.3.1. リフレッシュ

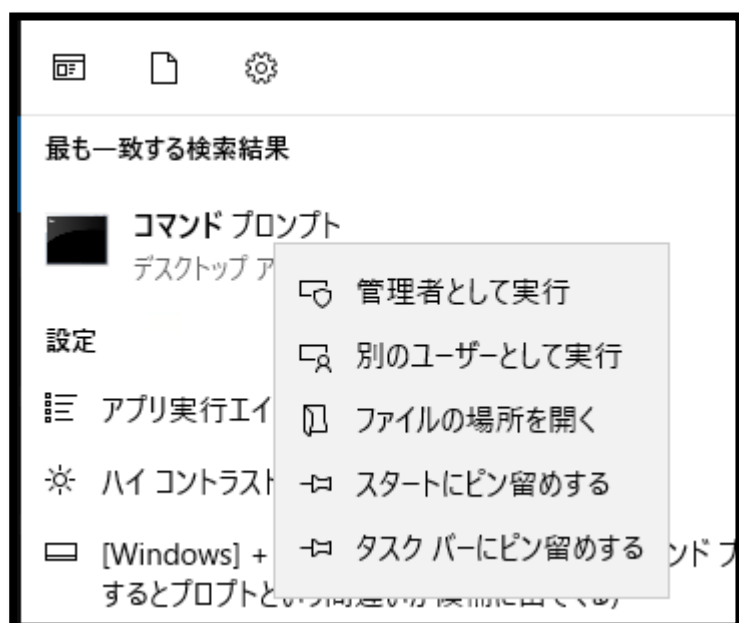
DBのリフレッシュを実施します。

リフレッシュは、コマンドプロンプトから管理者権限でコマンド実行します。

Windowsの左下の窓にて、「コマンド」と入力します。



コマンドプロンプトで、マウスを右クリックし、「管理者として実行」を選択します。



コマンドプロンプトで、インストールしたディレクトリ（標準では C:\SCM）に移動します。  
 バックアップを行うコマンドは、SSLcontrolDB.bat となります。  
 オプションを「cleanup」で実行します。

```
.\SSLbackupDB.bat cleanup
```

と入力し、Enter キーを入力することで、リストアが実行されます。

```
c:\$SCM>.\SSLcontrolDB.bat
"Usage: [ cleanup ]"

c:\$SCM>.\SSLcontrolDB.bat cleanup
vacuumdb: データベース"SSLDB"をVACUUMしています

c:\$SCM>_
```

## 11.4. テクニカルサポートファイルの生成

本ソフトウェアの技術サポートを受ける場合に必要となるテクニカルサポートファイルを生成します。

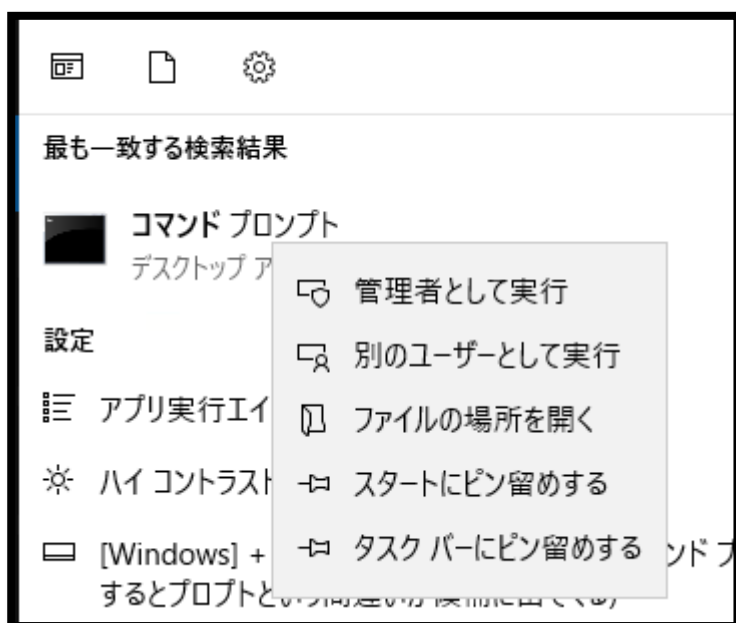
### 11.4.1. テクニカルサポートファイルの生成

コマンドプロンプトで実行します。

Windows の左下の $\text{\textcircled{P}}$ 窓にて、「コマンド」と入力します。



コマンドプロンプトで、マウスを右クリックし、「管理者として実行」を選択します。



コマンドプロンプトで、インストールしたディレクトリ（標準では C:\SCM）に移動します。テクニカルサポートファイルの生成を行うコマンドは、SSLbackupDB.bat となります。オプションを「support」で実行します。

```

CA: コマンドプロンプト
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:¥Users¥ssolAdmin>cd C:¥SCM

C:¥SCM>.¥SSLbackupDB.bat
"Usage: { backup | restore | support } [ <backup_folder> ]"

C:¥SCM>.¥SSLbackupDB.bat support_

```

.\SSLbackupDB.bat support

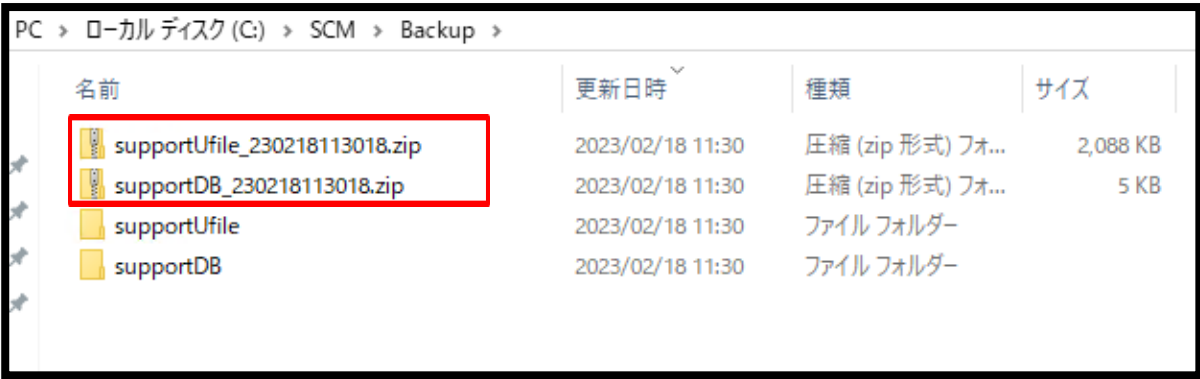
と入力し、Enter キーを入力することで、テクニカルサポートファイルが生成されます。

```

C:¥SCM>.¥SSLbackupDB.bat support
Backup¥
"Backup¥ folder not exist...creating."
supportDB
"supportDB folder not exist...creating."
COPY 2
COPY 0
COPY 1
COPY 1
COPY 1
COPY 0
COPY 1
COPY 0
COPY 1
COPY 2
COPY 1
COPY 1
COPY 1
COPY 200
COPY 10
COPY 31
"zipファイル supportDB_230218113018.zip を作成します。"
""Backup¥¥supportUfile folder not exist...creating."
powershell -NoProfile -ExecutionPolicy Unrestricted Compress-Archive -Path supportDB -DestinationPath supportDB_230218113018.zip -Force
xcopy /e /y Ufile ""Backup¥¥supportUfile"
Ufile¥SpXSchedule.accdb
Ufile¥SpXSchedule.laccdb
Ufile¥00001¥01¥appconf¥000001_update.json
:
:
削除したファイル - C:¥SCM¥Backup¥supportUfile¥00001¥CertData¥s00199¥002¥privkey.pem
削除したファイル - C:¥SCM¥Backup¥supportUfile¥00001¥CertData¥s00200¥001¥privkey.pem
削除したファイル - C:¥SCM¥Backup¥supportUfile¥00001¥CertData¥s00200¥002¥privkey.pem
"zipファイル supportUfile_230218113018.zip を作成します。"
powershell -NoProfile -ExecutionPolicy Unrestricted Compress-Archive -Path supportUfile -DestinationPath supportUfile_230218113018.zip -Force"
C:¥SCM>_

```

Windows のエクスプローラーにて、テクニカルサポートファイルが作成されていることを確認してください。



名前	更新日時	種類	サイズ
supportUfile_230218113018.zip	2023/02/18 11:30	圧縮 (zip 形式) フォ...	2,088 KB
supportDB_230218113018.zip	2023/02/18 11:30	圧縮 (zip 形式) フォ...	5 KB
supportUfile	2023/02/18 11:30	ファイル フォルダー	
supportDB	2023/02/18 11:30	ファイル フォルダー	

コマンド実行時に生成された以下の2つのファイルを、弊社サポート宛に送付してください。

supportUfile\_XXXXXXXXXX.zip ファイル

supportDB\_XXXXXXXXXX.zip ファイル



## 12. 付録

### 12.1. ログメッセージ一覧

#### 注意

%%に囲まれた範囲は、その状況に対応した文字列に置き換えられます。

ID	メッセージ
0000	%モジュール名% Ver=%モジュール名%module start.
0001	指定のフォルダに誤りがあります。[%パラメータ名称%:パラメータ指定値%]
0002	ログ要求 パラメータ件数の誤り [args=%パラメータ件数%] errno=%要求 ID%
0003	ログ要求 メッセージ番号の誤り errno=%要求 ID%
0004	ファイルが見つかりません。[%ファイル名%]
0005	フォーマットが異常です。[%ファイル名%] Line=%異常行%
0006	設定値の取得に失敗しました。key=%キーワード%
0007	ファイルの削除に失敗しました。[%失敗理由%]
0008	フォルダの生成に失敗しました。[%失敗理由%]
0009	ファイルの圧縮に失敗しました。[%失敗理由%]
0010	ファイルの解凍に失敗しました。[%失敗理由%]
0011	DB 読込に失敗しました。[%失敗理由%]
0012	DB 書込に失敗しました。[%失敗理由%]
0013	有効なサービスが見つかりません。
0014	ファイルの保存に失敗しました。[%失敗理由%]
0015	ファイルの移動失敗 [%失敗理由%]
0016	ファイルの複写失敗 [%失敗理由%]
0017	要求処理の登録に失敗しました。
0018	要求処理の取得に失敗しました。
0019	ファイルまたはフォルダが見つかりません。[%フォルダー名%]
0020	書き込み先フォルダーが使用中です。[%フォルダー名%]
0021	メールを要求します。[%要求メールのサブジェクト%]
0022	メール送信関連の情報が取得できませんでした。(ID=%サービス ID%)
0023	証明書申請ステータスを更新しました。%サービス名%:%更新値%

0024	証明書適用ステータス更新しました。%ノード名%:%更新値%
0025	証明書の登録をクリアしました。シリアル No(%001 or 002%)=%シリアル番号%
0026	証明書を登録します。シリアル No(%001 or 002%)=%シリアル番号%
0027	データの更新を要求します。
0028	証明書または秘密鍵の形式が不正です[%1]。
0029	%SSL 接続異常時のシステムメッセージ%
0030	エラーコードファイルを読み込みました。%読込ファイル区分%
0098	%例外メッセージ%
0099	%モジュール名% module end.
1201	取得したイベントが未定義の為削除しました。[%削除フォルダ名%]
1202	コマンドの終了待ちタイムアウトが発生しました。[%実行コマンド%]
1601	適用の結果の更新を開始します。ノード:%ノード名%, シリアル番号:%シリアル番号%
	確認の結果の更新を開始します。ノード:%ノード名%, シリアル番号:% %シリアル番号%
1602	適用の結果を更新しました。ノード:%ノード名%
	確認の結果を更新しました。ノード:%ノード名%
1603	適用の結果を更新はありません。ノード:%ノード名%
	確認の結果を更新はありません。ノード:%ノード名%
1604	申請結果の更新を開始します[%要求 ID%]。
1605	申請結果を更新しました[%要求 ID%]。
1606	サービスに未登録の証明書が見つかりました(適用)。ノード:%ノード名%, シリアル番号:%シリアル番号%
	サービスに未登録の証明書が見つかりました(適用)。ノード:%ノード名%, シリアル番号:%シリアル番号%
1607	ノードが追加されました。(確認)。ノード:%ノード名% ※ 未使用
1608	ノードが見つかりません(適用)。ID:%要求 ID%
	ノードが見つかりません(確認)。ID:%要求 ID%
1609	サービスに証明書が登録できません。[No Empty]
1610	申請の登録に失敗しました[%エラーコード%]。
1611	未定義の認証局です。
1612	証明書申請のスケジュール登録をしました。
1613	証明書申請のスケジュール登録に失敗しました。%異常メッセージ% 異常メッセージ 'Not32bit' : 32bit 以外の動作モード

	'readDLL' : dll 読込失敗 'noneMode' : モードなし 'faileDB' : DB 登録失敗 'execution' : 想定外のエラー
1614	適用の結果に有効なデータがありません。
	確認の結果に有効なデータがありません。
	申請の結果に有効なデータがありません。
1615	ノード : %ノード名%は無効設定です。
1651	証明書と秘密鍵のペアの確認ができません。
1652	コモンネームが一致しません。
1653	サービスが見つかりません[%サービス ID%]。
1654	証明書が申請中または申請待ちの為に登録できません。
1655	指定された証明書は登録済みです。指定された証明書で更新します[%1 or 2%]。
1656	証明書と登録秘密鍵のペアの確認ができません。
1657	証明書情報を登録する為の空きがありません。
1658	証明書を登録しました。
	証明書を登録しました。【証明書登録なし】
1659	指定された証明書に重複または未関係の証明書が含まれています。
1660	指定された証明書ファイルに複数の証明書が含まれています。
1701	%サービス名称%の証明書の有効期限が 15 日をきりました。
	%サービス名称%の証明書の有効期限が 30 日をきりました。
	%サービス名称%の証明書の有効期限が 60 日をきりました。
	%サービス名称%の証明書の有効期限が 90 日をきりました。
1702	%サービス名称%の証明書の有効期限が終了しました。
1703	%サービス名称%の証明書情報(%1 または 2%)をクリアします
1704	サーバー証明書登録更新 サービスの登録がありません。
	サーバー証明書登録更新 サービスの登録がありません。(ID=%ID%)
	サーバー証明書有効期限確認 サービスの登録がありません。(ID=%ID%)
	サーバー証明書有効期限確認 サービスの登録がありません。(ID=%ID%)
1705	通知情報が取得できませんでした。(ID=%サービス ID%)
1706	証明書の登録確認を開始します。 %サービス名称%

1707	証明書の登録確認を終了します。 %サービス名称%
	証明書の登録確認を終了します。 %サービス名称%有効なノードなし
1708	適用ステータスを更新します。 %サービス名称%
1801	適用処理を開始します[%ID%]。
1802	適用処理を終了しました。 [%ID%]
1803	要求ファイルのセル数が異常です。 line=%異常行%
1804	要求ファイル、適用モードが異常です。 line=%異常行%
1805	要求ファイルのセル数が異常です。
1810	ssh 接続で応答待ちタイムアウトが発生しました。 TM=%タイマー値%
1811	ログインに失敗しました。 [%ログインユーザー名%]
1812	コマンド実行が失敗しました。 [%実行コマンド%]
1813	アカウント情報が見つかりません。
1814	適用後の確認情報が見当たりません。
1815	適用後の確認に失敗しました。
1816	証明書リストアに失敗しました。 [%詳細%]
1817	パーミッションの変更に失敗しました。 [%対象パス名%]
1818	標準エラー出力メッセージ [%メッセージ%]
1819	%SSL 接続失敗メッセージ%
1820	RestAPI を要求します。 [request=%メソッド%, url=%URL%]
1821	要求に失敗しました。 [%異常メッセージ%]
1822	レスポンスが異常です。 [%応答コード%]
1839	%RestAPI 接続失敗メッセージ%
1840	ファイルの削除に失敗しました。 [%削除ファイル名%]
1841	ファイルの転送に失敗しました。(送信)[%転送ファイル名%]
1842	ファイルの転送に失敗しました。(受信)[%転送ファイル名%]
1843	pkcs12 形式の変換に失敗しました。 [%詳細%]
1849	接続に失敗しました。 [%WinRM 詳細メッセージ%]
1850	SSL 接続が成功しました。 [%接続アドレス%]
1851	フォルダを作成しました。 [%作成フォルダ名%]
1852	ファイルを転送しました。 [%転送ファイル名%]

1853	証明書／秘密鍵ファイルをバックアップしました。
1854	証明書／秘密鍵ファイルを置き換えました。
1855	Apache の再起動を要求しました。
1857	証明書を確認しました。シリアル No:%シリアルNo.%
1858	古い証明書を削除します。[%削除フォルダ%]
1859	証明書の適用が終了しました。
1860	SSL 接続を切断しました。
1861	適用に失敗した為にロールバックを実施します。
1862	証明書／秘密鍵ファイルを復元しました。
1863	転送したファイルを削除しました。
1864	作成したフォルダを削除しました。
1865	インポートしました。[%インポート名%]
1866	プロファイルを更新しました。[%プロファイル名%]
1867	サイトを更新しました。[%サイト名%]
2001	CSR の作成に失敗しました。
2002	未対応の暗号スイートです。
2003	CSR 情報の収取に失敗しました。[%1]
2101	CSR ファイルの読込に失敗しました。[%ファイル名%]
2102	RestAPI を要求します。[%要求コマンド%]
2103	要求に失敗しました。[%システム出力メッセージ%]
2104	異常応答を受信しました。[%応答コード%]
2105	想定外の内容の応答を受信しました。[%システム出力メッセージ%]
2106	組織の認証が確認できません。[%詳細%]
2107	ドメインの認証が確認できません。[%詳細%]
2108	複数のレスポンス応答を受信しました [requests(%件数%)]
2109	証明書申請状態 [%結果状態%]
2110	要求ファイルのセル数が異常です。line=%異常行%
2111	要求情報が不足しています。line=%異常行%[%異常内容%]
2112	申請処理を開始します[%要求 ID%]。[%コモンネーム%]
2113	申請処理を終了しました。[%要求 ID%]

2199	応答詳細[%エラーコード%:%エラーメッセージ%]
2201	メール送信に失敗しました。[%異常時のシステムメッセージ%]
2202	登録情報が不足しています。[%不足項目%]
2203	SMTP は暗号化されていません。[%メッセージ%]
2401	要求ファイルのセル数が異常です。line=%異常行%
2402	要求ファイル、ホスト情報が異常です。line=%異常行%
2403	要求ファイル、検索モードが異常です。line=%異常行%
2404	証明書が見つかりません。
2405	確認開始 Addr<%宛先%> host<%要求宛先%> FQDN<%要求 FQDN%> port<%要求ポート%> mode< 1 >
2406	確認終了 Addr<%宛先%> host<%要求宛先%> FQDN<%要求 FQDN%> port<%要求ポート%> mode< 1 >
2410	ssh 接続で応答フォーマットが異常です。
2411	証明書が受信できません。
2412	ssh 接続で応答待ちタイムアウトが発生しました。TM=%タイマー値%
2413	名前解決に失敗しました。[%ホスト名%]
2420	アカウント情報が見つかりません。
2421	ログインに失敗しました。
2422	証明書が見つかりません。
2423	コマンド実行が失敗しました。[%コマンド%]
2429	%コマンド実行例外メッセージ%
2601	適用要求の生成に%成功または失敗%しました[%コード%]。サービス名:%サービス名% 拠点名:%拠点名% ノード名:%拠点名% %失敗時のメッセージ%
	適用要求の生成に%成功または失敗%しました[%コード%]。サービス名:%サービス名% 拠点名:%拠点名% ノード名:%拠点名% %失敗時のメッセージ%
	申請要求の生成に%成功または失敗%しました[%コード%]。サービス名:%サービス名% %失敗時のメッセージ%
2602	適用要求を要求します。拠点:%拠点名%
	確認要求を要求します。拠点:%拠点名%
	申請要求を要求します。拠点:%拠点名%
2603	適用結果の要求しました。拠点:%拠点名%
	確認結果の要求しました。拠点:%拠点名%
	申請結果の要求しました。拠点:%拠点名%
2605	要求された条件に一致するノードが見つかりません。S%サービス ID%

	要求された条件に一致するノードが見つかりません。H%拠点 ID%
	要求された条件に一致するノードが見つかりません。N%ノード ID%
	要求された条件に一致するノードが見つかりません。C%企業 ID%
2606	要求された条件に一致するサービスが見つかりません。S%サービス ID%
	要求された条件に一致するサービスが見つかりません。C%企業 ID%
2607	申請要求を要求します。サービス：%サービス名%
2608	申請結果の要求しました。サービス：%サービス名%
2609	CSR ファイルの作成を要求します。
2610	証明書情報を登録する為の空きがありません。
2611	無効のノードに適用が要求されました。[%ノード名%]

## 12.2. 送信メール内容

本ソフトウェアで送信されるメール内容を例文で記載します。

メール通知設定、および対象拠点・サービス・ノード名称は以下としています。

タイトル	SSL 証明書管理 SW
本文	SSL 証明書管理 SW からお知らせ
拠点名	幕張 DC
サービス名	service001
ノード名	ServerABC

### 12.2.1. 証明書期限メール

#### 12.2.1.1. 90 日前

90 日前、60 日前、30 日前、15 日前は、日付以外は同じ文面となります。

Subject: SSL 証明書管理 SW 証明書の有効期間が 90 日未満です[service001]

Body:

SSL 証明書管理 SW からお知らせ

service001 の証明書の有効期間が 90 日未満です。

有効期間終了日 : 20230226

#### 12.2.1.2. 失効

Subject: SSL 証明書管理 SW 証明書の有効期間が失効中です[service001]

Body:

SSL 証明書管理 SW からお知らせ

service001 の証明書の有効期間が失効中です。

有効期間終了日 : 20230216

### 12.2.2. 証明書申請メール

#### 12.2.2.1. 申請開始

Subject: SSL 証明書管理 SW 申請を開始しました[service001]

Body:

SSL 証明書管理 SW からお知らせ

service001 への申請を開始しました。



### 12.2.2.2. 申請中

Subject: SSL 証明書管理 SW 申請が申請中です[service001]  
Body:  
SSL 証明書管理 SW からお知らせ

service001 への申請が申請中です。  
orders <I2109> 00001 証明書申請状態 [pending]

### 12.2.2.3. 申請終了

Subject: SSL 証明書管理 SW 証明書の有効期間が失効中です[service001]  
Body:  
SSL 証明書管理 SW からお知らせ

service001 への申請が完了しました。

Subject: SSL 証明書管理 SW 申請が異常完了しました[service001]  
Body:  
SSL 証明書管理 SW からお知らせ

テスト環境(1)への申請が異常完了しました。  
orders <E2109> 00001 証明書申請状態 [rejected]

## 12.2.3. 証明書適用メール

### 12.2.3.1. 適用開始

Subject: SSL 証明書管理 SW 適用を開始しました[service001:ServerABC]  
Body:  
SSL 証明書管理 SW からお知らせ

ServerABC への適用を開始しました。  
サービス名 : service001  
拠点名 : 幕張 DC

## 12.2.3.2. 適 用 終 了

Subject: SSL 証明書管理 SW 適用が終了しました[service001:ServerABC]

Body:

SSL 証明書管理 SW からお知らせ

ServerABC への適用が終了しました。

サービス名 : service001

拠点名 : 幕張 DC

トレースメッセージ :

証明書の適用処理開始[Windows IIS] 2023/02/19 03:35:06

apply <I1852> 00001 ファイルを転送しました。 [\$env:TEMP\s001\fullchain.pfx]

apply <I1867> 00001 サイトを更新しました。 [interop]

apply <I1857> 00001 証明書を 確認 しました。 シリアル  
No:0x784d7fa871eb0fc59508e2bc01a82708289f0ee2

apply <I1859> 00001 証明書の適用が終了しました。

証明書の適用処理終了[Windows IIS] 2023/02/19 03:35:11

Subject: SSL 証明書管理 SW 適用が終了しました[service001]

Body:

SSL 証明書管理 SW

ServerABC への適用が失敗しました。

サービス名 : service001

拠点名 : 幕張 DC

メッセージ : apply <E1811> 00001 ログインに失敗しました。 [root]

トレースメッセージ :

証明書の適用処理開始[Apache] 2023/02/21 02:46:19

apply <E1811> 00001 ログインに失敗しました。 [root]

apply <I1860> 00001 SSH 接続を切断しました。

証明書の適用処理終了[Apache] 2023/02/21 02:46:23

apply <I1861> 00001 適用に失敗した為にロールバックを実施します。

証明書のロールバック処理開始[Apache] 2023/02/21 02:46:23

apply <E1811> 00001 ログインに失敗しました。 [root]

apply <I1860> 00001 SSH 接続を切断しました。

証明書のロールバック処理終了[Apache] 2023/02/21 02:46:26

セイコーソリューションズ株式会社

〒261-8507 千葉県千葉市美浜区中瀬 1-8

[support@seiko-sol.co.jp](mailto:support@seiko-sol.co.jp)