



JCCH・セキュリティ・ソリューション・システムズ

# プライベートCA Gléas ホワイトペーパー

～IISにおけるクライアント証明書を利用した

ユーザ認証の設定手順～

Ver.2.2

2023年2月

- ・ JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- ・ その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- ・ Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

## 目次

1. はじめに .....	5
1.1. 本書について.....	5
1.2. 本書における環境 .....	5
2. サーバ証明書発行とルート CA 証明書のダウンロード .....	6
2.1. サーバ証明書の発行.....	6
2.1.1. PKCS#12 形式での発行とダウンロード.....	6
2.1.2. CSR からの発行とダウンロード.....	10
2.2. ルート CA 証明書のダウンロード.....	15
3. IIS の設定 .....	16
3.1. サーバ証明書の登録.....	16
3.1.1. PKCS#12 のサーバ証明書登録 .....	17
3.1.2. CSR から発行したサーバ証明書の登録 .....	19
3.2. ルート CA 証明書の登録.....	21
3.2.1. CTL の登録.....	21
3.2.2. 信頼されたルート証明機関への登録.....	21
3.2.3. ルート CA 証明書の確認 .....	22
3.3. SSL ポートのバインド.....	23
3.4. クライアント証明書要求の有効化.....	26
4. 動作確認 .....	27
5. その他.....	28
5.1. 接続時の「セキュリティ警告」について .....	28
5.2. 失効検証の処理方法について .....	29
5.3. 失効情報をすぐに反映させたいとき .....	30
5.4. 失効の確認をしない方法 .....	30
5.5. ASP.NET(C#)でクライアント証明書の情報を取得する .....	31

プライベート CA Gléas ホワイトペーパー  
IIS におけるクライアント証明書を利用したユーザ認証の設定手順

6. お問い合わせ .....32

## 1. はじめに

### 1.1. 本書について

本書では、弊社製品「プライベート認証局Gléas」で発行したクライアント証明書サーバ証明書を使用してMicrosoft Internet Information Services (IIS) でクライアント証明書認証をおこなう環境を構築するための設定例を記載します。

主な対象とするユーザは、公開鍵暗号基盤 (PKI) を利用したクライアント証明書による認証を検討しているWebサイト管理者、および、Webプログラマーをターゲットとしています。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

### 1.2. 本書における環境

本書における手順は、以下の環境で作成しています。

- JS3 プライベート認証局Gléas (バージョン2.2.3)
  - ※以後、「Gléas」と記載します
- Microsoft Windows Server 2022
  - Internet Information Services 10.0.20348.1
  - ※以後、「IIS」と記載します

以下については、本書では説明を割愛します。

- Windows ServerやIISの基本的な設定
  - クライアントから、`http://{Webサーバのホスト名}/` として接続できることを前提としています。
- クライアント証明書の端末へのインポート方法

## 2. サーバ証明書発行とルート CA 証明書のダウンロード

本章では、後述の IIS の設定で使用するサーバ証明書、ルート CA 証明書について Gléas から発行、取得する手順を記載します。

### 2.1. サーバ証明書の発行

Gléas ではサーバ証明書を PKCS#12 形式または、IIS で生成した CSR を使用して発行することができます。以降にそれぞれの発行手順を記載します。

#### 2.1.1. PKCS#12 形式での発行とダウンロード

Gléas の RA（管理画面）へログインし該当のサーバアカウントの詳細を表示します。

※サーバアカウントの作成については代理店もしくは弊社へお問い合わせください。

The screenshot displays the Gléas RA management interface. The main content area shows details for the account 'iisdemo.spt-demo.local'. It includes sections for 'アカウント情報' (Account Information), 'グループ情報' (Group Information), '証明書発行の履歴' (Certificate Issuance History), and 'テンプレート情報' (Template Information).

**アカウント情報**

- サーバ: iisdemo.spt-demo.local
- 登録日時: 2022/12/20 15:04
- ステータス: 有効
- サーバ属性: 最終更新: 2022/12/20 15:04
- ホスト名:

**グループ情報**

- ユーザグループ: なし
- ロールグループ: なし

**証明書発行の履歴**

#	シリアル	開始	有効期限	ステータス	失効日	暗号種別	トークン
証明書は発行されていません。							

**テンプレート情報**

種別	必須テンプレート	任意テンプレート
一般名(CN)	iisdemo.spt-demo.local	
組織名(O)	JCCH Security Solution Systems Co., Ltd.	
ドメインコンポーネント(DC)	local	support2

## プライベート CA Gléas ホワイトペーパー IIS におけるクライアント証明書を利用したユーザ認証の設定手順

サーバ属性の「編集」をクリックしホスト名に WEB サービスの FQDN を追加して「保存」をクリックします。

作業名: タスク132874  
管理者: システム管理者

プライベートCA Gléas RA

[アカウント] > 詳細

アカウント: iisdemo.spt-demo.local

アカウント情報

- サーバ: 登録日時: 2022/12/20 15:04
- ステータス: 有効
- サーバ属性: [保存](#) [再読み込み](#)
- ホスト名: iisdemo.spt-demo.local

グループ情報

- ユーザグループ: [追加](#)
- なし
- ロールグループ: [追加](#)
- サーバ証明書: [削除](#)

証明書発行の履歴

#	シリアル	開始	有効期限	ステータス	失効日	暗号種別	トークン
証明書は発行されていません。							

テンプレート情報

種別	必須テンプレート	任意テンプレート
一般名(CN)	iisdemo.spt-demo.local	
組織名(O)	JCCH Security Solution Systems Co., Ltd.	
ドメインコンポーネント(DC)	local	support2

操作メニュー: アカウント一覧, 登録申請書一覧, アカウント新規作成, 証明書発行, アカウント削除, ドックに入れる

ドック: アカウント (0), 証明書 (0)

操作: 保存

操作履歴: プライベートCA Gléas

Copyright (C) 2010-2020 JCCH Security Solution Systems Co., Ltd. All rights reserved.

左ペインの「証明書発行」をクリックします。

作業名: タスク132874  
管理者: システム管理者

プライベートCA Gléas RA

[アカウント] > 詳細

アカウント: iisdemo.spt-demo.local

アカウント情報

- サーバ: 登録日時: 2022/12/20 15:04
- ステータス: 有効
- サーバ属性: 最終更新: 2022/12/20 15:04 [編集](#)
- ホスト名: iisdemo.spt-demo.local

グループ情報

- ユーザグループ: [追加](#)
- なし
- ロールグループ: [追加](#)
- サーバ証明書: [削除](#)

証明書発行の履歴

#	シリアル	開始	有効期限	ステータス	失効日	暗号種別	トークン
証明書は発行されていません。							

テンプレート情報

種別	必須テンプレート	任意テンプレート
一般名(CN)	iisdemo.spt-demo.local	
組織名(O)	JCCH Security Solution Systems Co., Ltd.	
ドメインコンポーネント(DC)	local	support2

操作メニュー: アカウント一覧, 登録申請書一覧, アカウント新規作成, **証明書発行**, アカウント削除, ドックに入れる

ドック: アカウント (0), 証明書 (0)

操作: 保存

操作履歴: プライベートCA Gléas

Copyright (C) 2010-2020 JCCH Security Solution Systems Co., Ltd. All rights reserved.

## プライベート CA Gléas ホワイトペーパー IIS におけるクライアント証明書を利用したユーザ認証の設定手順

「発行」をクリックします。



ステータスが発行依頼中となり、5分程で証明書が発行されます。

※画面の自動更新は行われないので時折画面更新などを行ってください。



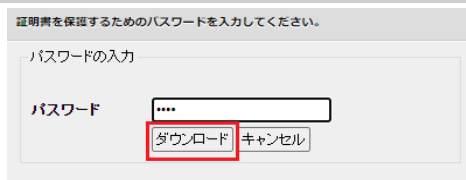
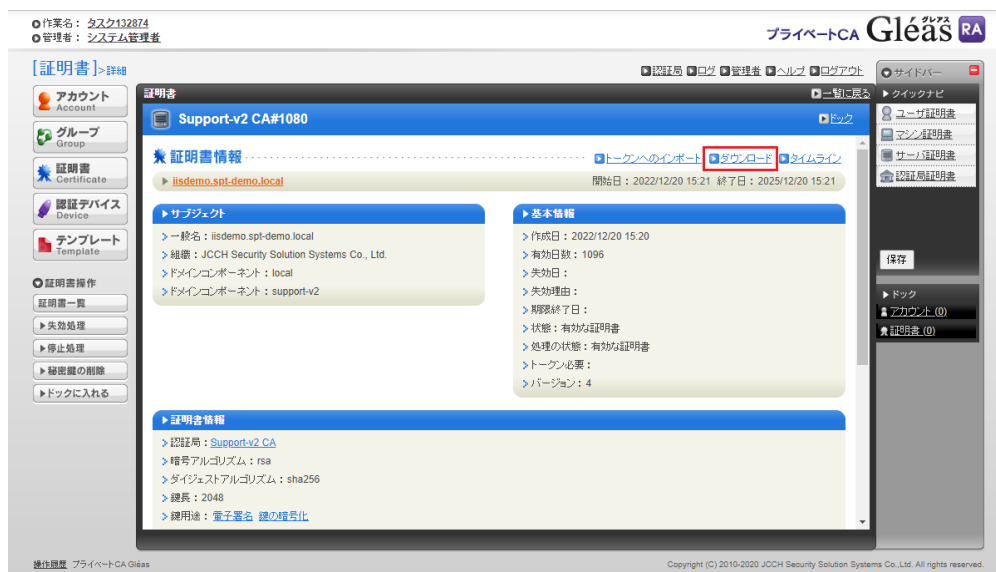


## プライベート CA Gléas ホワイトペーパー IIS におけるクライアント証明書を利用したユーザ認証の設定手順

証明書発行後に証明書をクリックして証明書詳細を開きます。



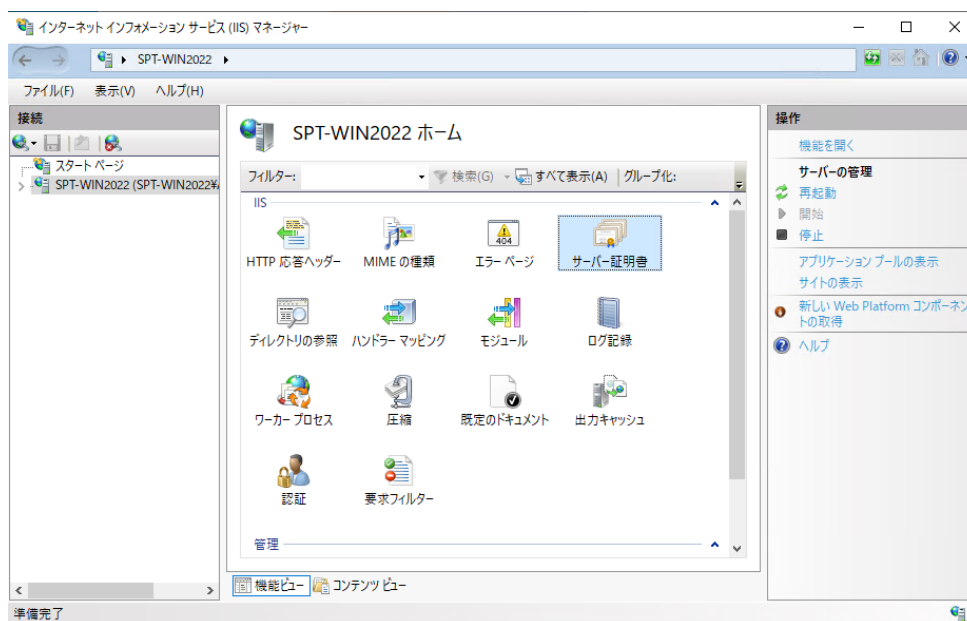
「ダウンロード」をクリックし、表示されたダイアログでパスワードを入力して PKCS#12 形式の証明書をダウンロードします。



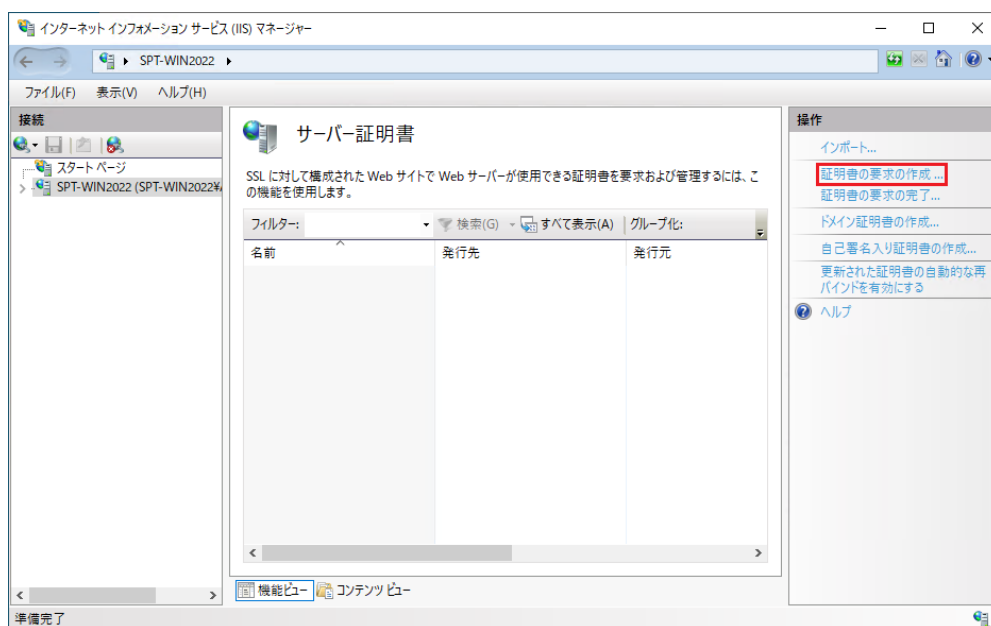
## 2.1.2. CSR からの発行とダウンロード

CSR からサーバ証明書を発行する際は IIS にて CSR を生成し、それを使用し Gléas から発行します。

IIS を起動し左側ツリーの「サーバ名」をクリックし、「サーバ証明書」アイコンをクリックすると、現在登録されているサーバ証明書が一覧表示されます。




操作メニュー内の「証明書の要求の作成」をクリックします。



プライベート CA Gléas ホワイトペーパー  
IIS におけるクライアント証明書を利用したユーザ認証の設定手順

各項目を入力して、「OK」ボタンをクリックします。一般名には、Web サーバの FQDN を入力してください。

証明書の要求 ? ×

 識別名プロパティ

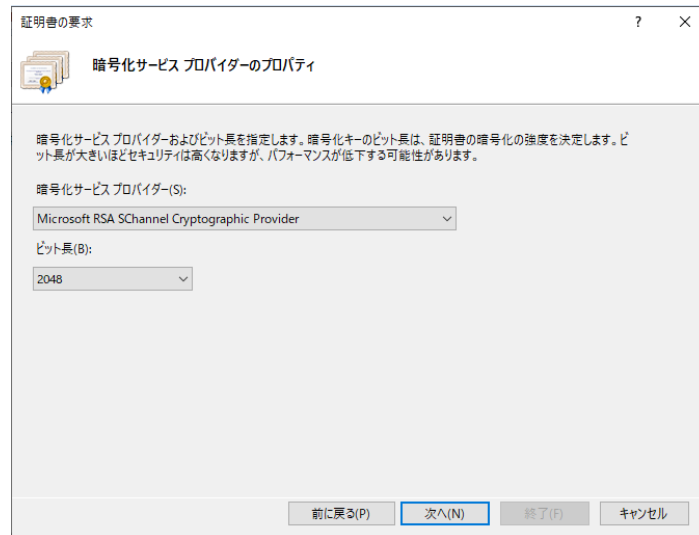
証明書に必要な情報を指定します。都道府県および市区町村に関する情報は、公式名称を指定してください。省略形は使用しないでください。

一般名(M):	<input type="text" value="iisdemo.spt-demo.local"/>
組織(O):	<input type="text" value="JCH Security Solution Systems"/>
組織単位 (OU)(U):	<input type="text" value="Support"/>
市区町村(L)	<input type="text" value="Arakawa"/>
都道府県(S):	<input type="text" value="Tokyo"/>
国/地域(R):	<input type="text" value="JP"/>

前に戻る(P) 次へ(N) 終了(F) キャンセル

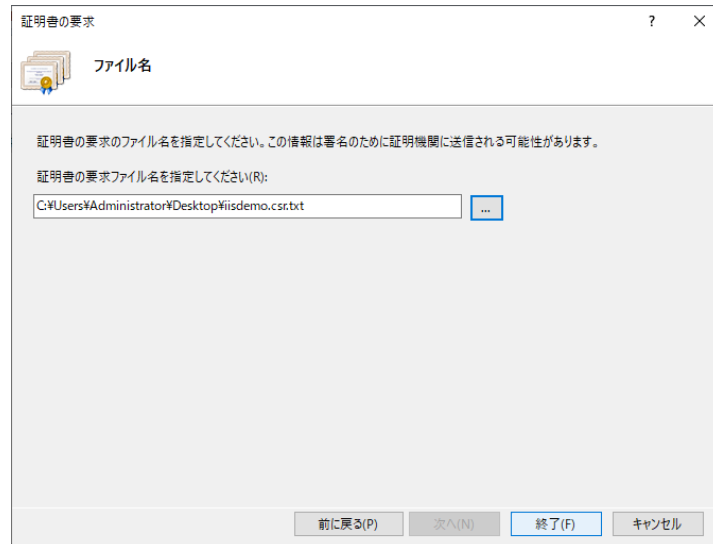
プライベート CA Gléas ホワイトペーパー  
IIS におけるクライアント証明書を利用したユーザ認証の設定手順

暗号化サービスプロバイダ、および、ビット長を指定します。「次へ」をクリックします。  
※IIS のデフォルト値は、1024bit ですが、Gléas では 2048bit 以上を推奨しているため、2048bit 以上を選んでください。



The screenshot shows a dialog box titled '証明書の要求' (Certificate Requirements) with a sub-title '暗号化サービス プロバイダーのプロパティ' (Encryption Service Provider Properties). The main text reads: '暗号化サービスプロバイダーおよびビット長を指定します。暗号化キーのビット長は、証明書の暗号化の強度を決定します。ビット長が大きいほどセキュリティは高くなりますが、パフォーマンスが低下する可能性があります。' (Specify the encryption service provider and bit length. The bit length of the encryption key determines the strength of the certificate encryption. The larger the bit length, the higher the security, but performance may decrease). Below this, there are two dropdown menus: '暗号化サービスプロバイダー(S):' (Encryption Service Provider(S):) set to 'Microsoft RSA SChannel Cryptographic Provider' and 'ビット長(B):' (Bit Length(B):) set to '2048'. At the bottom, there are four buttons: '前に戻る(P)' (Back), '次へ(N)' (Next), '終了(F)' (Finish), and 'キャンセル' (Cancel).

CSR の保存先を指定するダイアログが表示されるので、デスクトップ等に保存してください。



The screenshot shows the same dialog box '証明書の要求' (Certificate Requirements) but with the sub-title 'ファイル名' (File Name). The main text reads: '証明書の要求のファイル名を指定してください。この情報は署名のために証明機関に送信される可能性があります。' (Specify the file name for the certificate request. This information may be sent to the certificate authority for signing). Below this, there is a text input field for '証明書の要求ファイル名を指定してください(R):' (Specify the certificate request file name(R):) containing the path 'C:\Users\Administrator\Desktop\iisdemo.csr.txt' and a browse button '...' to its right. At the bottom, there are four buttons: '前に戻る(P)' (Back), '次へ(N)' (Next), '終了(F)' (Finish), and 'キャンセル' (Cancel).

## プライベート CA Gléas ホワイトペーパー IIS におけるクライアント証明書を利用したユーザ認証の設定手順

Gléas の RA (管理画面) にログインして前手順でダウンロードした CSR からサーバ証明書を発行します。

該当のサーバアカウントの詳細を開き「証明書発行」をクリックします。

※サーバアカウントの作成と証明書の発行については代理店または弊社へお問い合わせください。



証明書詳細の「上級者向け設定」を開き「ファイルの選択」から CSR ファイルを指定し「発行」をクリックします。

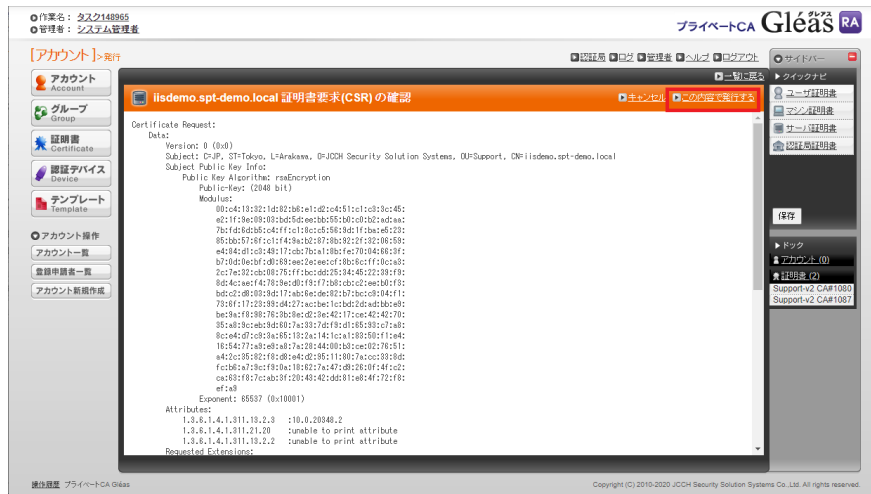
※「CSR ファイルの内容を確認する」をチェックすると証明書発行操作後に CSR の内容を表示します。



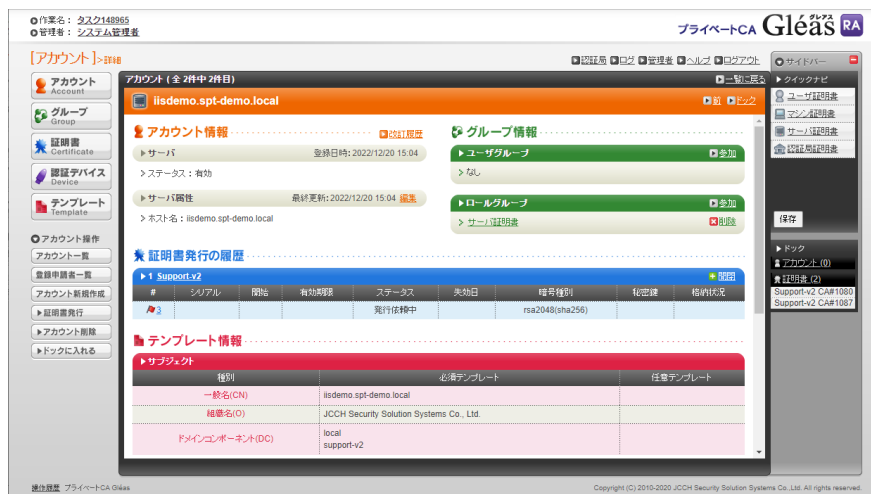
# プライベート CA Gleas ホワイトペーパー

## IIS におけるクライアント証明書を利用したユーザ認証の設定手順

「CSR ファイルの内容を確認する」をクリックした場合は CSR の詳細が表示されますので「この内容で発行する」をクリックします。



ステータスが発行依頼中となり、5分程で証明書が発行されます。  
※画面の自動更新は行われないので時折画面更新などを行ってください。



## プライベート CA Gléas ホワイトペーパー IIS におけるクライアント証明書を利用したユーザ認証の設定手順

証明書発行後に証明書をクリックして証明書詳細を開きます。



画面下方の証明書ファイル欄の「あり」リンクからサーバ証明書をダウンロードします。



## 2.2. ルート CA 証明書のダウンロード

ルート CA 証明書は以下の URL へアクセスして Gléas からダウンロードします。

<http://host名/crl/ia1.der>

## 3. IIS の設定

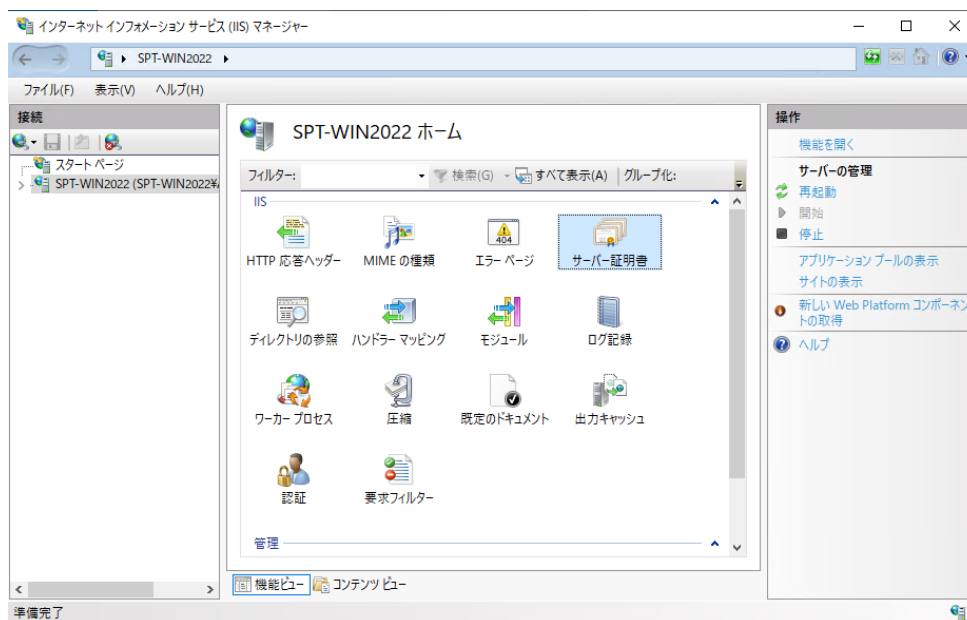
本章では、インターネット インフォメーション サービス (IIS) マネージャーを利用して IIS の設定を行います。

### 3.1. サーバ証明書の登録

サーバ証明書は PKCS#12 形式の証明書の登録と CSR から発行した証明書の登録のいずれかで行います。

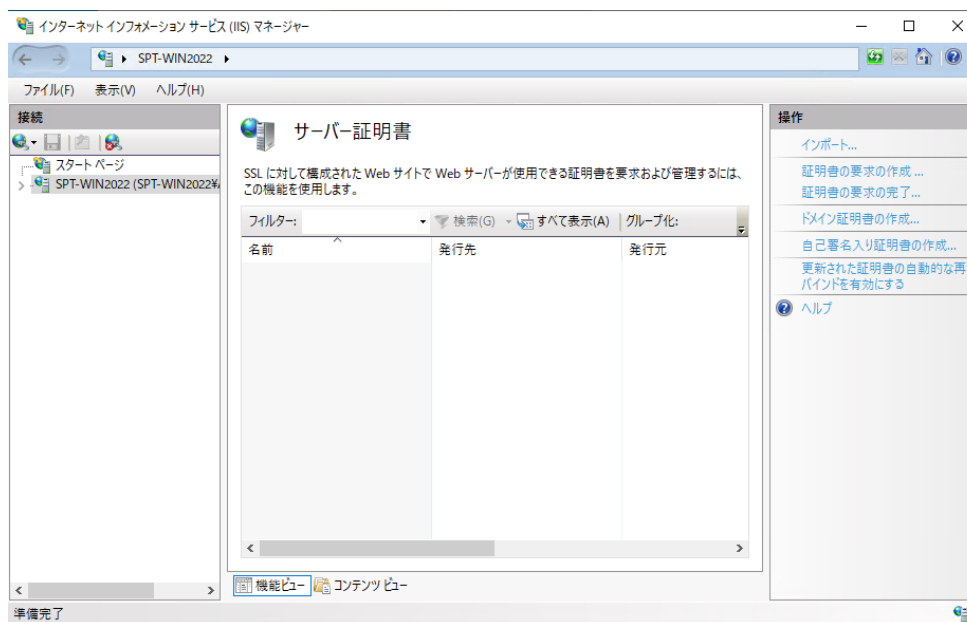
IIS を起動し、左側ツリーの「サーバ名」をクリックします。

「サーバ証明書」アイコンをクリックすると、現在登録されているサーバ証明書が一覧表示されます。





## プライベート CA Gléas ホワイトペーパー IIS におけるクライアント証明書を利用したユーザ認証の設定手順

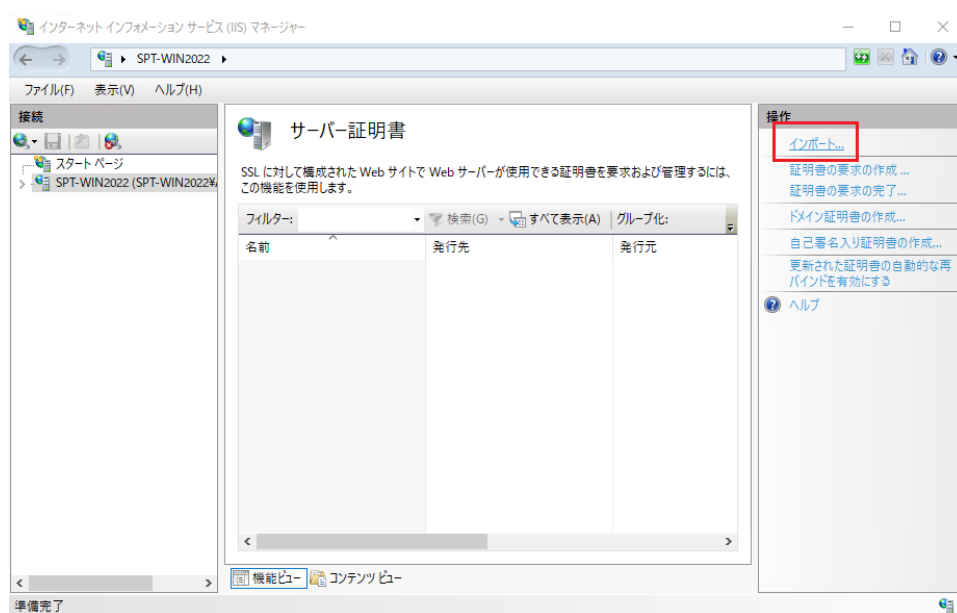


以降の手順はサーバ証明書の種類に応じて「3.1.1PKCS#12 のサーバ証明書登録」、「3.1.2CSR から発行したサーバ証明書の登録」の手順を進めて下さい。

### 3.1.1. PKCS#12 のサーバ証明書登録

本項では PKCS#12 形式のサーバ証明書を登録する方法を記載します。

IIS からサーバ証明書一覧を開き、操作メニュー内の「インポート」をクリックします。



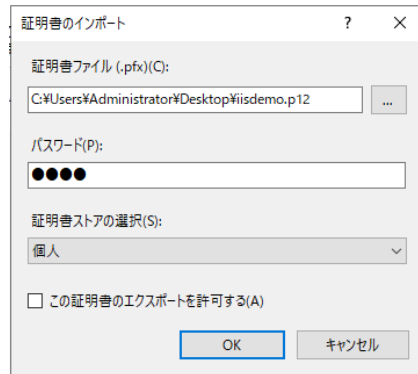
「証明書のインポート」ダイアログが表示されるので、「2.1.1PKCS#12 形式での発行と

プライベート CA Gléas ホワイトペーパー  
IIS におけるクライアント証明書を利用したユーザ認証の設定手順

ダウンロード」でダウンロードした証明書ファイル (PKCS#12) のパス、および、PKCS#12 のパスワードを入力します。

※「証明書ストアの選択」は「個人」、「この証明書のエクスポートを許可する」はオフにしてください。

「OK」ボタンをクリックすると、インポートされたサーバ証明書が一覧に追加されます。



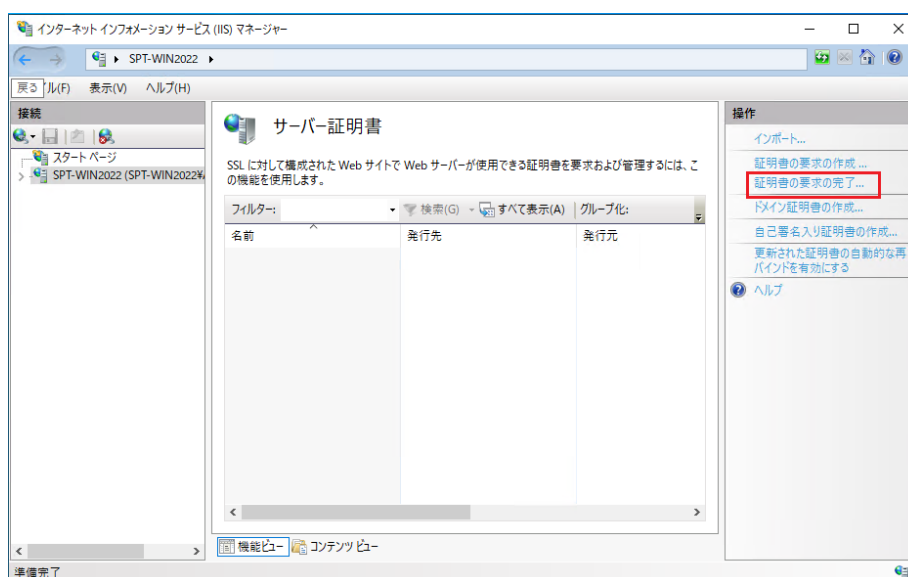
Note:

PKCS#12 ファイルの拡張子には、.p12 と .pfx があります。IIS の証明書のインポートダイアログには、.pfx を指定するように書かれていますが、拡張子が.p12 ファイルのファイルも指定可能です。

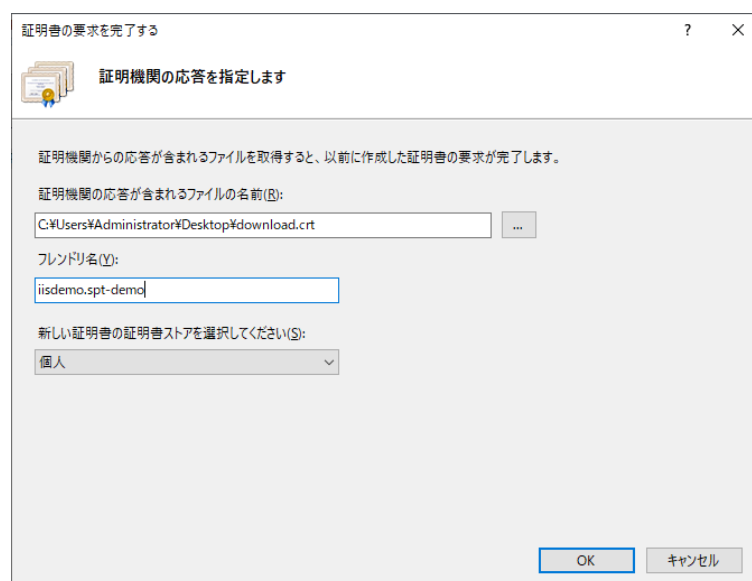
### 3.1.2. CSR から発行したサーバ証明書の登録

本項では IIS で作成した CSR から発行した、サーバ証明書を登録する方法を記載します。  
※CSR からのサーバ証明書の発行は「2.1.2CSR からの発行とダウンロード」を参照してください。

IIS からサーバ証明書の一覧画面を開き、操作メニュー内の「証明書の要求の完了」をクリックします。

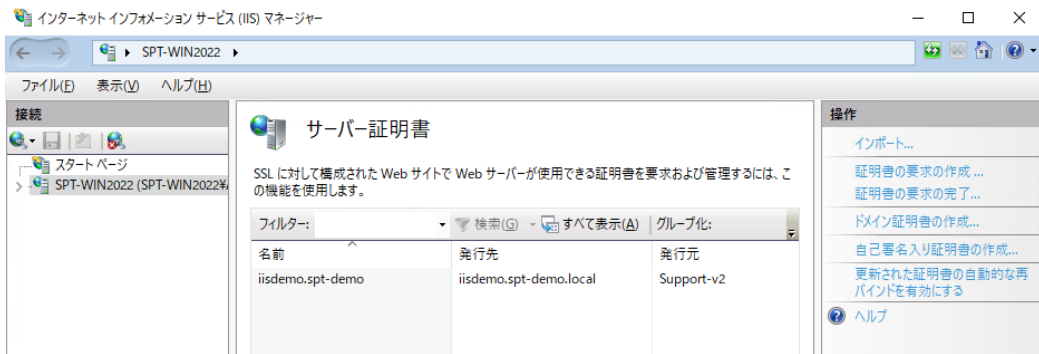


「証明機関の応答が含まれるファイルの名前」に、「2.1.2CSR からの発行とダウンロード」でダウンロードしたサーバ証明書のパスを指定します。  
フレンドリ名には、識別用の任意の文字列を入力します。



プライベート CA Gléas ホワイトペーパー  
IIS におけるクライアント証明書を利用したユーザ認証の設定手順

「OK」ボタンをクリックすると、サーバ証明書の一覧に追加されます。



## 3.2. ルート CA 証明書の登録

クライアント証明書によるSSL認証を利用するためには、ルートCA証明書の登録が必要です。これは、クライアントPCから提示されるクライアント証明書が正しいことを検証するために利用します。

ルートCA証明書はCTLとコンピュータストアの両方に指定します。

※ルートCA証明書は「2.2ルートCA証明書のダウンロード」の手順でダウンロードします。

### 3.2.1. CTL の登録

Powershell(あるいは、コマンドプロンプト)を管理者起動し以下のコマンドを実行し、CTL (証明書信頼リスト) を作成します。CTLを使うことで、Gléasから発行したクライアント証明書だけをクライアントに提示させることが可能となります。

```
certutil -f -addstore [証明書ストア名] [ルートCA証明書ファイル]
```

例) certutil -f -addstore iis\_client\_trust ia1.der

### 3.2.2. 信頼されたルート証明機関への登録

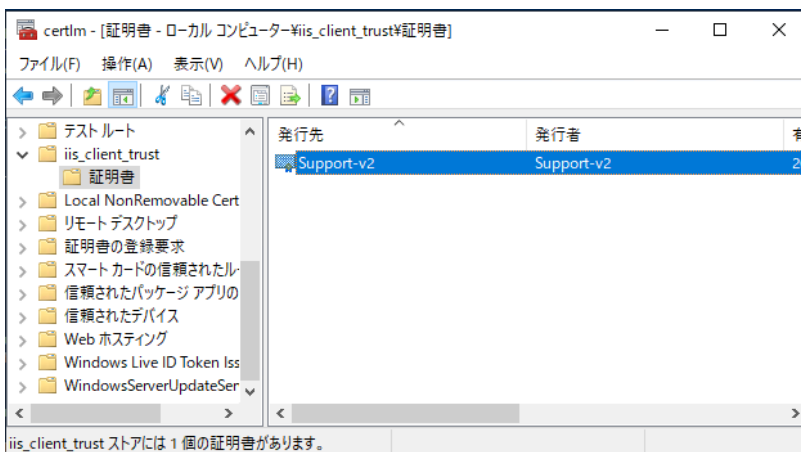
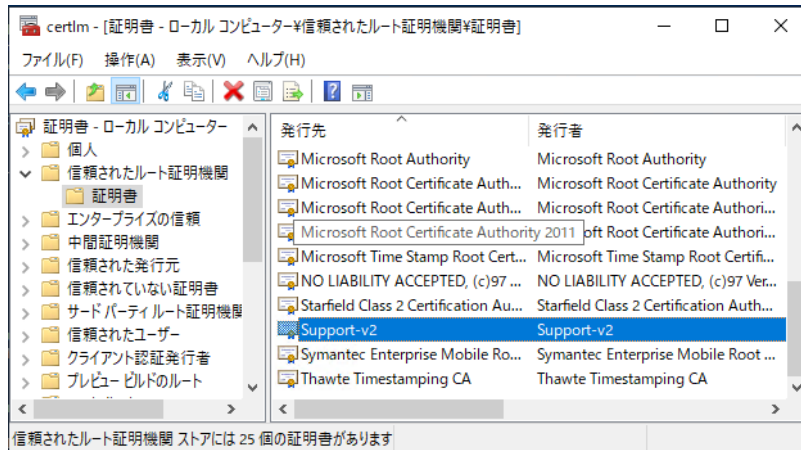
CTLの登録と同様にコマンドを実行し、コンピュータストアの「信頼されたルート証明機関」へルートCA証明書を追加します。

```
certutil -f -addstore [証明書ストア名] [ルートCA証明書ファイル]
```

例) certutil -f -addstore ROOT ia1.der

### 3.2.3. ルート CA 証明書の確認

Powershell(あるいは、コマンドプロンプト)より以下「certlm.msc」と入力してMMCを起動し、コンピュータストアの「信頼されたルート証明機関」および「CTL登録」で登録した証明書ストア（例：iis\_client\_trust）を確認し、ルートCA証明書がインポートされていることを確認します。



### 3.3. SSL ポートのバインド

Powershell(あるいは、コマンドプロンプト)を管理者起動し以下のコマンドを実行して作成したCTLを指定し、SSLバインドを設定します。

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=[サーバ証明書の拇印] certstorename=MY  
clientcertnegotiation=enable sslctlstorename=[証明書ストア名]
```

例) netsh http add sslcert ipport=0.0.0.0:443  
certhash=d3e2496dcb807a8a1db388b72ee1e17060cca6be certstorename=MY  
clientcertnegotiation=enable sslctlstorename=iis\_client\_trust

Note:

上記では、サーバの IP アドレスを指定していますが、ホスト名で指定することも可能です。その場合は *ipport* の代わりに *hostnameport* を指定します。

サーバ証明書の拇印は以下のコマンドで確認できます。

```
Get-ChildItem Cert:\LocalMachine\My
```

正常に終了すると、「SSL 証明書を正常に追加しました」もしくは「SSL Certificate successfully added」と表示されます。

実施した結果は以下コマンドで確認可能です。

```
>netsh http show sslcert
```

```
SSL Certificate bindings:  
-----  
  
IP:port                : 0.0.0.0:443  
Certificate Hash       : d3e2496dcb807a8a1db388b72ee1e17060cca6be  
Application ID        : {00000000-0000-0000-0000-000000000000}  
Certificate Store Name : MY  
Verify Client Certificate Revocation : Disabled  
Verify Revocation Using Cached Client Certificate Only : Disabled  
Usage Check           : Enabled  
Revocation Freshness Time : 0  
URL Retrieval Timeout : 0  
Ctl Identifier        : (null)  
Ctl Store Name        : iis_client_trust  
DS Mapper Usage       : Disabled
```

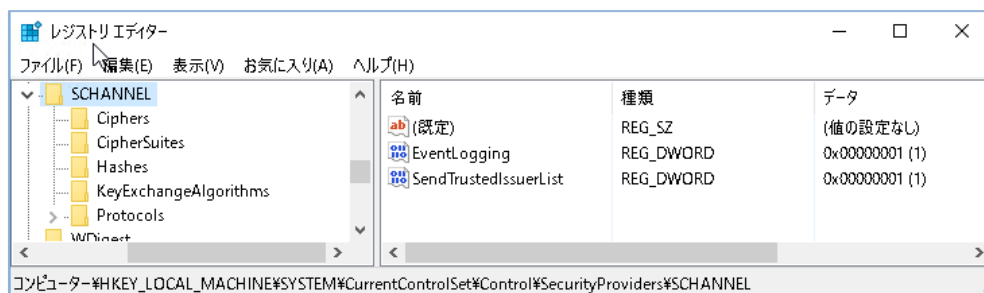
プライベート CA Gléas ホワイトペーパー  
IIS におけるクライアント証明書を利用したユーザ認証の設定手順

CTLに登録した信頼済み発行者（認証局）をクライアントに送信するためにはレジストリエディターより以下のレジストリエントリの作成が必要となります。

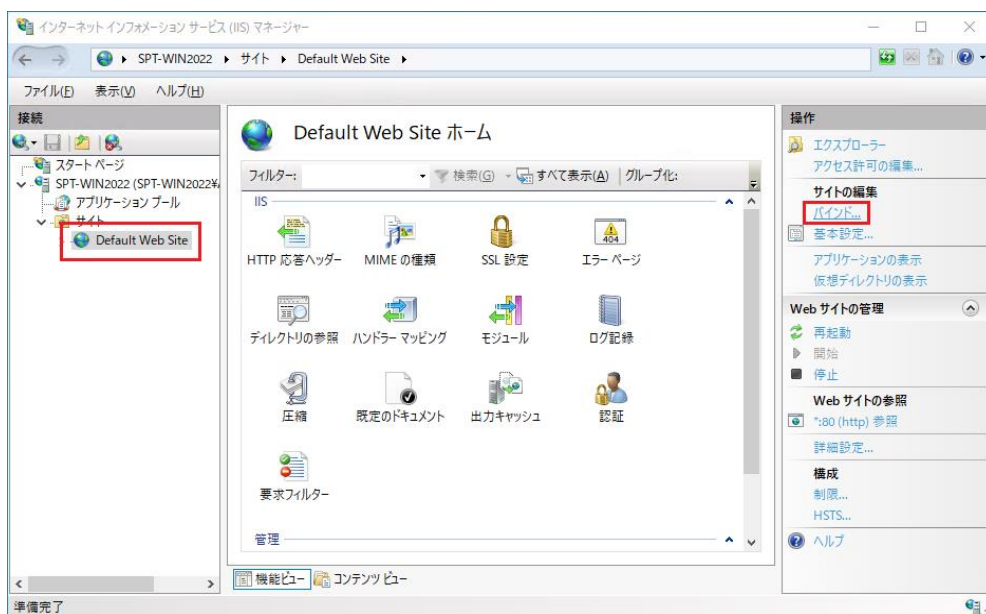
レジストリパス：

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL

SendTrustedIssuerList (REG\_DWORD) を追加し、1 を設定します。



IISマネージャーより左手のサイトを選択し、右手の操作より「バインド」をクリックします。





プライベート CA Gléas ホワイトペーパー  
IIS におけるクライアント証明書を利用したユーザ認証の設定手順

種類に「https」、SSL証明書に前手順で設定したサーバ証明書（iisdemo.spt-demo）を選択し、「OK」をクリックします。

※TLS1.1以前を無効にする際は「レガシTLSを無効にする」をチェックします。

サイトバインドの追加

種類(T): https IP アドレス(I): 未使用の IP アドレスすべて ポート(O): 443

ホスト名(H):

サーバー名表示を要求する(N)

TLS 1.3 over TCP を無効にする(B)  QUIC を無効にします(A)

レガシ TLS を無効にする(G)  HTTP/2 を無効にします(D)

OCSP ステージングを無効にします(S)

SSL 証明書(F): iisdemo.spt-demo 選択(L)... 表示(V)...

OK キャンセル

httpsが一覧に追加されたことを確認し「閉じる」をクリックします。

サイトバインド

種類	ホスト名	ポート	IP アドレス	バインド情報
http		80	*	
https		443	*	

追加(A)...

編集(E)...

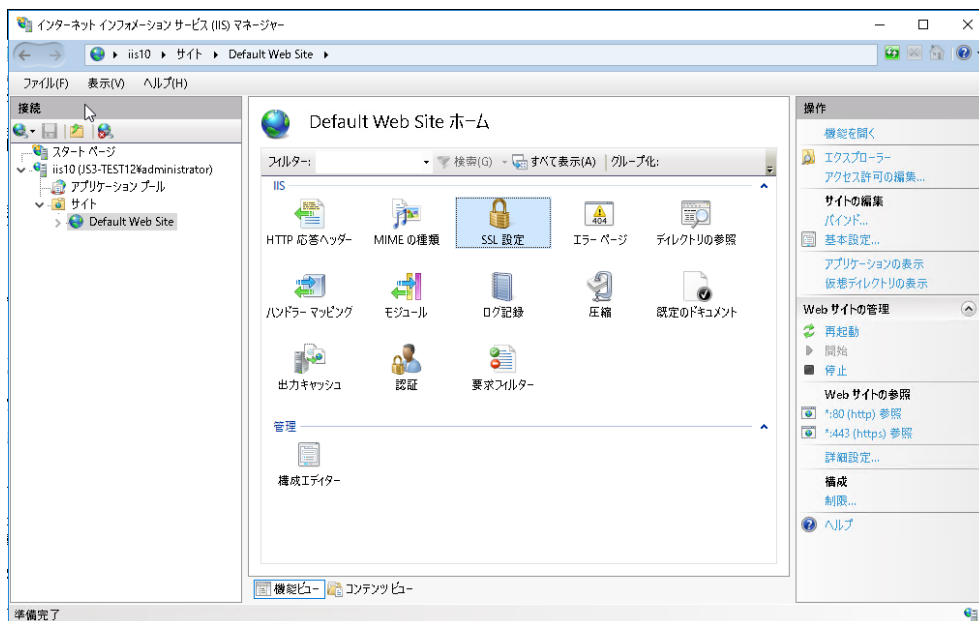
削除(D)

参照(B)

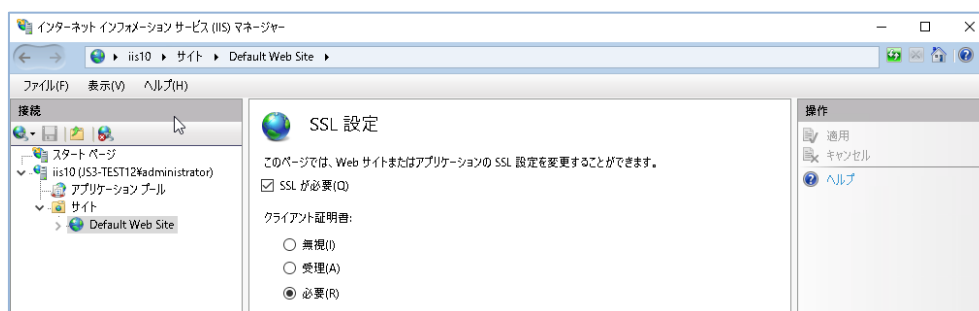
閉じる(C)

### 3.4. クライアント証明書要求の有効化

IIS マネージャーより左側ツリーのサイトを選択し、「SSL 設定」アイコンをクリックします。



「SSLが必要」のチェックボックスを有効にし、クライアント証明書の「必要」をクリックして有効化します。



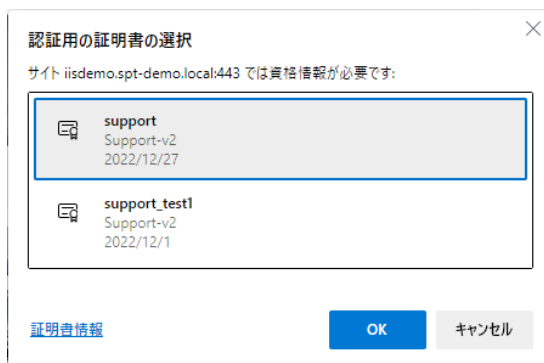
右側メニューの「適用」をクリックすると、SSL 設定の変更内容が確定します。  
以上で IIS の設定は終了です。

## 4. 動作確認

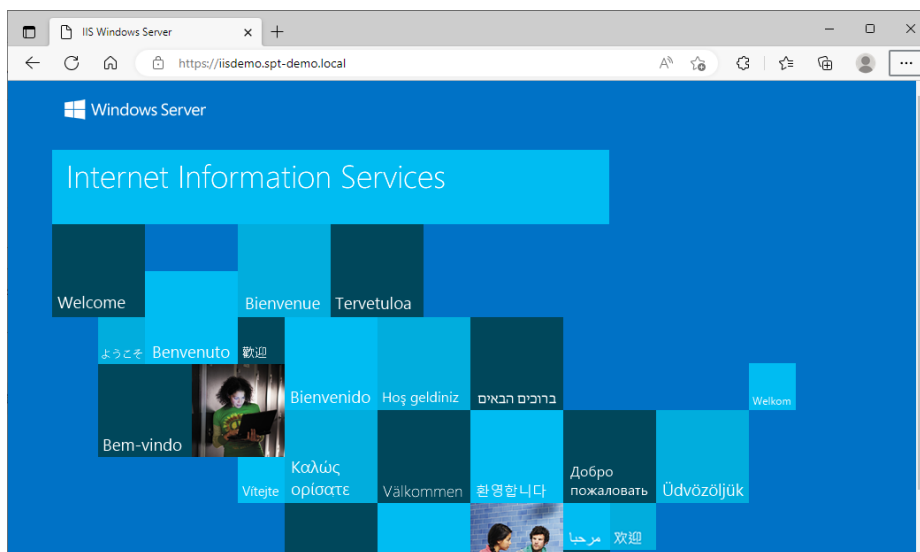
クライアント証明書がインポートされた端末でインターネットエクスプローラを起動して、<https://{Web サーバのホスト名}/> にアクセスします。

(スクリーンショットは Edge のものとなります)

クライアント証明書を選ぶダイアログが表示されるので、「OK」ボタンを押下します。



クライアント証明書による認証が実施され、ウェブページが表示されます。



Note:

セキュリティ警告が表示される場合は、『5.1 接続時の「セキュリティ警告」について』を参照してください。

## 5. その他

### 5.1. 接続時の「セキュリティ警告」について

Web サーバへの接続時、クライアント PC は Web サーバへサーバ証明書の提示を求めます。クライアント PC は提示されたサーバ証明書の検証を行い、不備があった場合に「プライバシーエラー」を表示します。



サーバ証明書の検証では、以下の項目を確認しています。

- ① 自身が信頼した認証局から発行された証明書であるか（サーバ証明書の署名検証ができるか）
- ② サーバ証明書の有効期限
- ③ 接続先 URL(ホスト名部分)と、サーバ証明書のホスト名の一致

※プライバシーエラーが表示されないようにするには・・・

- ① 信頼された認証局から発行された証明書であるかサーバ証明書の発行元を信頼できるかどうかを、クライアントが確認できない場合に表示されます。  
パブリック認証局で発行されたサーバ証明書を Web サーバに搭載するか、中間証明書を Web サーバに搭載する、もしくは、拇印を確認して CA 証明書をクライアントの「信頼されたルート証明機関」に登録することで解決します。  
クライアントの OS やブラウザによって表示されたり、されなかったりする場合は、IIS に中間証明書が正しく指定されているか確認します。
- ② 有効期限の確認  
アクセス時のクライアントの時刻が、サーバ証明書に記載されている有効期限の開始日と終了日の間ではないときに発生します。  
クライアントの時刻が正しいか確認し、時刻が正しい場合はサーバ証明書の有効期限が切れていないか確認し、切れている場合は新たなサーバ証明書を準備し搭載し

ます。

③ 接続先とサーバ証明書の一致確認

接続先ホスト名 (Internet Explorer のアドレスバーの「https://」から次の「/(スラッシュ)」まで) とサーバ証明書の発行先サブジェクトの「CN」やサブジェクトの別名の「DNS Name」が異なっている場合に発生します。証明書の発行先は、証明書の詳細パネルから確認することができます。

サーバ証明書のサブジェクトの「CN」、もしくはサブジェクトの別名の「DNS Name」が正しいか確認してください。正しくない場合は、サーバ証明書を再発行してください。また、サーバ証明書の CN がホスト名で書かれている場合は、IP アドレスでアクセスした場合も発生します。

## 5.2. 失効検証の処理方法について

証明書の利用を停止することを、証明書の失効と言い、失効情報が記載されたデータを証明書失効リスト(CRL)と言います。CRLの中には失効した証明書のシリアル番号の全て(または一部)が記載されています。CRLは、特定の証明書の利用を停止させたい時などに利用します。証明書の利用を停止することで、その証明書を所有しているユーザのアクセスを禁止させることができます。

クライアント証明書の有効性を検証する機器によって、失効検証の処理方法は異なりますが、IISのデフォルトの動作では、クライアント証明書に記載されたCRL配布ポイントを自動的に参照する仕組みになっています。

※失効に関する注意点

認証局で失効操作を行っても、認証局がCRLを更新しそれをIISが取得するまで失効は反映されません。

CRLには「次の更新予定」という項目でCRLの次の更新日時が記されています。IISはこの項目を CRLの有効期限として扱い、この日時を過ぎると全てのユーザのアクセスを拒否します。また、一度取得したCRLはローカルにキャッシュとして保持されるため、有効期限が過ぎるまでCRLを新たに取得することはありません。

### 5.3.失効情報をすぐに反映させたいとき

以下の手順を実施すると、CRLのキャッシュ終了時間を即時にクリアするため失効情報を即時にIISに反映することが可能です。

(動作確認時には、ブラウザのキャッシュクリアを先におこないます)

```
certutil -urlcache crl delete  
certutil -setreg chain¥ChainCacheResyncFiletime "@now"  
net stop cryptsvc  
net start cryptsvc
```

### 5.4.失効の確認をしない方法

前述のとおり、IISのデフォルトの動作では、クライアント証明書に記載されたCRL配布ポイントを自動的に参照して、CRLを取得して利用するしくみになっています。CRL配布ポイントに指定されたURLにCRLが存在しない場合や存在しても有効期限が過ぎている場合は、すべてのクライアントの接続を拒否します。

以下の設定を実施するとクライアント証明書の失効確認を行わなくなります。

1. SSLバインドを解除する

```
netsh http delete sslcert ipport=0.0.0.0:443
```

2. 失効確認を無効にして、SSLバインドを再設定する

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=[サーバ証明書の拇印]  
certstorename=MY clientcertnegotiation=enable sslctlstorename=[証明書ストア名]  
verifyclientcertrevocation=disable
```

失効確認を有効にする場合は、`verifyclientcertrevocation` に `enable` を指定してSSLバインドを再設定します。

## 5.5.ASP.NET(C#)でクライアント証明書の情報を取得する

以下にサンプルコードを記載します。

```
<%@ PAGE LANGUAGE="C#" %>
<html>
<script runat="server">
void Page_Load(object sender, EventArgs e) {
    HttpClientCertificate cert = Request.ClientCertificate;
    if (cert.IsPresent) {
        Serial.Text = cert.SerialNumber;
        Subject.Text = cert.Subject;
        KeySize.Text = cert.SecretKeySize.ToString();
        ValidFrom.Text = cert.ValidFrom.ToString("yyyy/MM/dd HH:mm:ss");
        ValidUntil.Text = cert.ValidUntil.ToString("yyyy/MM/dd HH:mm:ss");
    } else {
        Summary.Text = "クライアント証明書が見つかりません";
    }
}
</script>
<body>
<asp:Label id="Summary" runat="server" />
<ul>
<li>シリアル No : <asp:Label id="Serial" runat="server" /></li>
<li>サブジェクト : <asp:Label id="Subject" runat="server" /></li>
<li>鍵長 : <asp:Label id="KeySize" runat="server" /> bits</li>
<li>有効期限の開始日 : <asp:Label id="ValidFrom" runat="server" /></li>
<li>有効期限の終了日 : <asp:Label id="ValidUntil" runat="server" /></li>
</ul>
</body>
</html>
```

## 6. お問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■本書に関するお問い合わせ先

株式会社JCCH・セキュリティ・ソリューション・システムズ

Tel: 050-3821-2195

Mail: sales@jcch-sss.com