



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.2.0

2020年12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。

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

目次

1. はじめに .....	4
1.1. 本書について .....	4
1.2. 本書における環境 .....	4
2. IIS の設定 .....	4
2.1. サーバ証明書の登録 .....	5
2.1.1. PKCS#12 をインポートする方法 .....	6
2.1.2. 証明書の要求の作成/登録.....	7
2.2. ルート証明書の登録 .....	10
2.3. SSL ポートのバインド .....	11
2.4. クライアント証明書要求の有効化.....	12
3. 動作確認 .....	13
4. その他 .....	14
4.1. 接続時の「セキュリティ警告」について.....	14
4.2. 失効検証の処理方法について.....	15
4.3. 失効情報をすぐに反映させたいとき.....	16
4.4. 失効の確認をしない方法 .....	16
4.5. ASP.NET(C#)でクライアント証明書の情報を取得する方法 .....	16
5. 問い合わせ .....	17

## 1. はじめに

### 1.1. 本書について

本書では、Microsoft Internet Information Services 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。

- Microsoft Windows Server 2016  
Internet Information Services 10.0  
※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. IISの設定

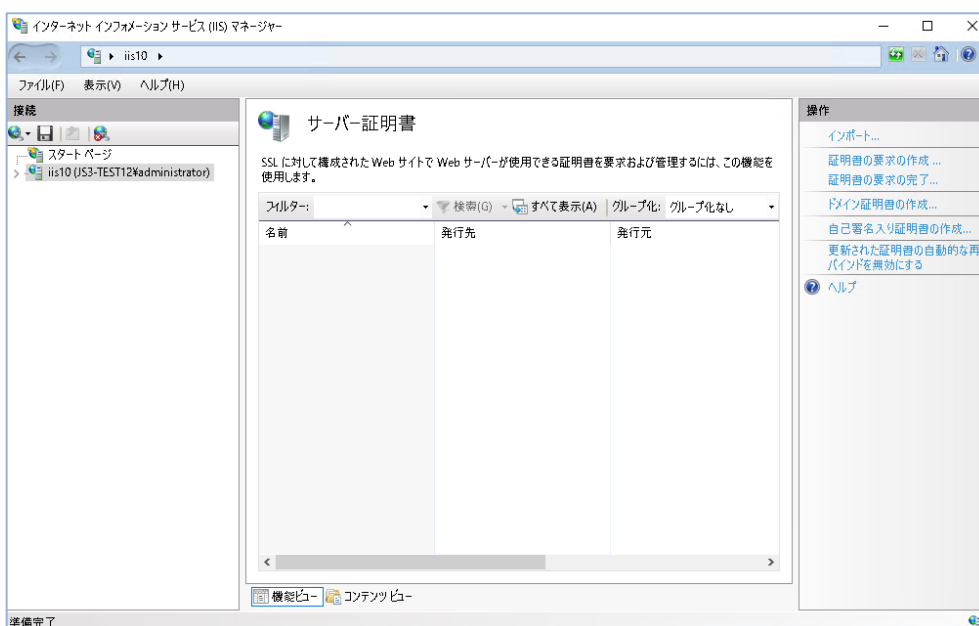
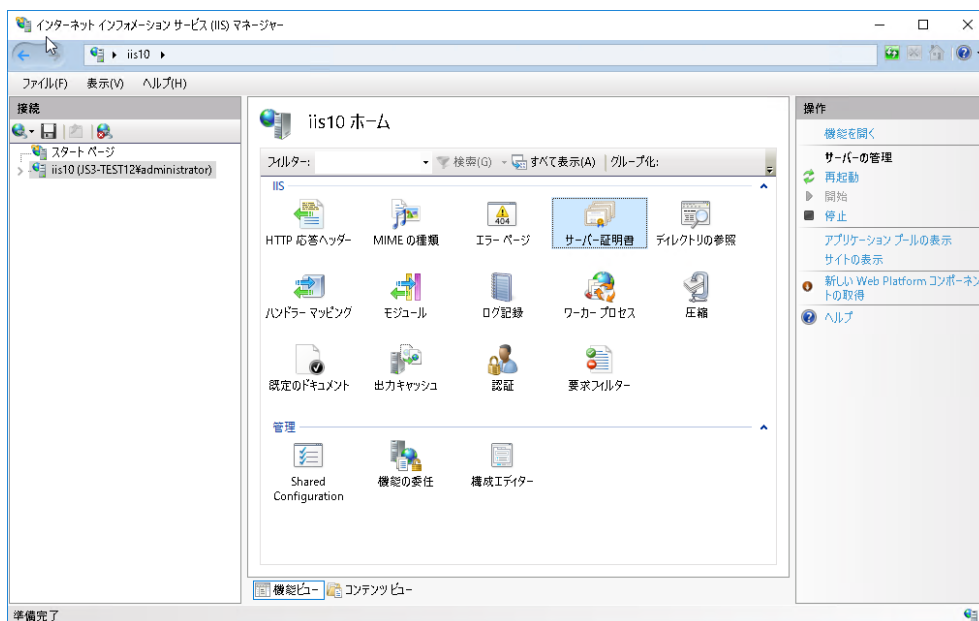
本章では、インターネット インフォメーション サービス (IIS) マネージャーを利用して IIS の設定を行います。

インターネット インフォメーション サービス (IIS) マネージャーは、スタートメニューの「管理ツール」より起動します。

## 2.1. サーバ証明書の登録

左側ツリーの「サーバ名」をクリックします。

「サーバー証明書」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。



※既にサーバ証明書を登録済みであれば、『2.3 SSL ポートのバインド』に進んでください

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

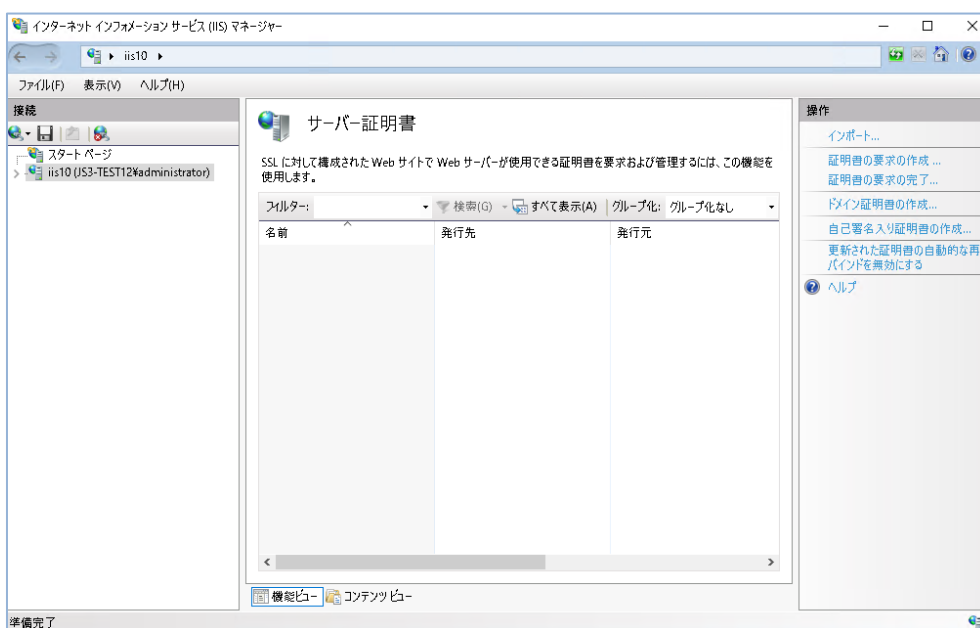
サーバ証明書を新規に登録する場合、操作メニュー内の「インポート」を選び PKCS#12 をインポートするか、または「証明書の要求の作成」を選び CSR を作成後、認証局で発行した証明書を登録します。

ここでは、PKCS#12 をインポートする方法と CSR の作成/登録の方法を記載します。

### 2.1.1. PKCS#12 をインポートする方法

ここでは、認証局から受け取った PKCS#12 をインポートする方法を記載します。CSR を利用する場合は、『2.1.2 証明書の要求の作成/登録』を参照してください。

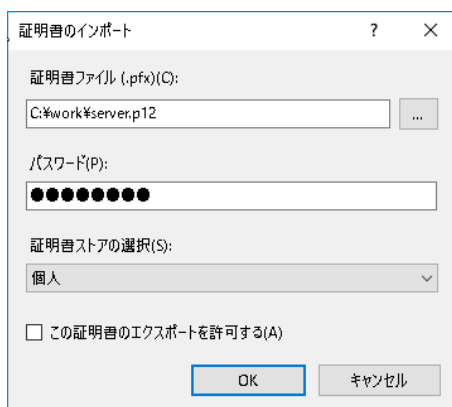
1. 操作メニュー内の「インポート」をクリックします。



2. 「証明書のインポート」ダイアログが表示されるので、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。

「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。

## 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



### Note:

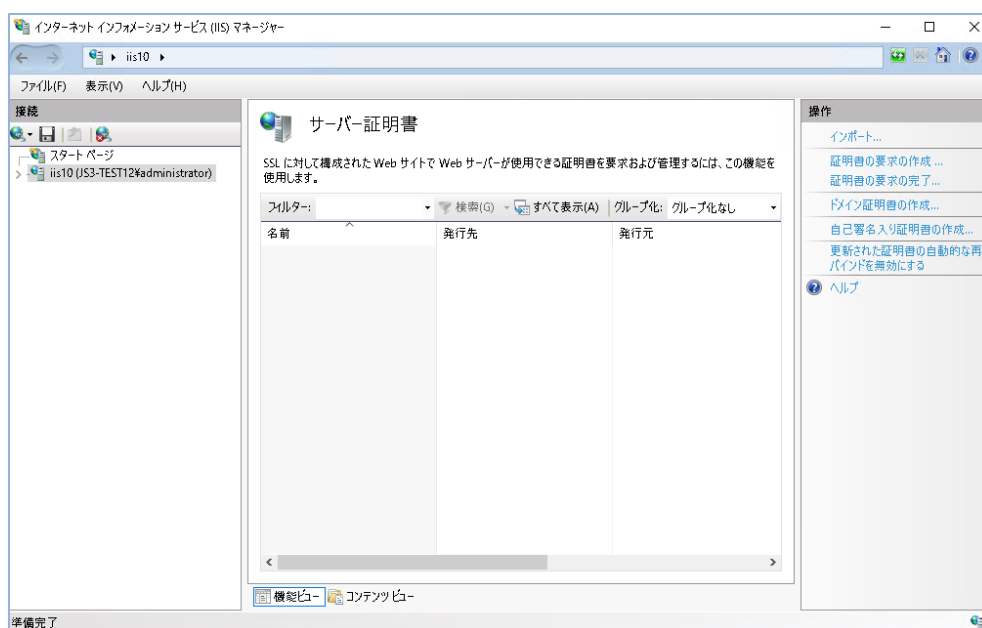
PKCS#12 ファイルの拡張子には、.p12 と .pfx があります。IIS の証明書のインポートダイアログには、.pfx を指定するように書かれていますが、拡張子が.p12 ファイルのファイルも指定可能です。

## 2.1.2. 証明書の要求の作成/登録

ここでは、IIS で証明書の要求を作成する方法、および、認証局から受け取ったサーバ証明書を登録する方法を記載します。

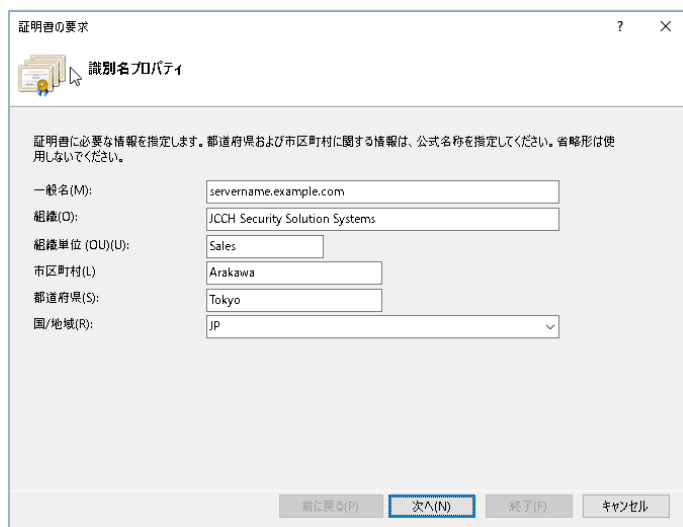
PKCS#12 をインポートする場合は、『2.1.1 PKCS#12 をインポートする方法』を参照してください。

1. 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

2. 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。

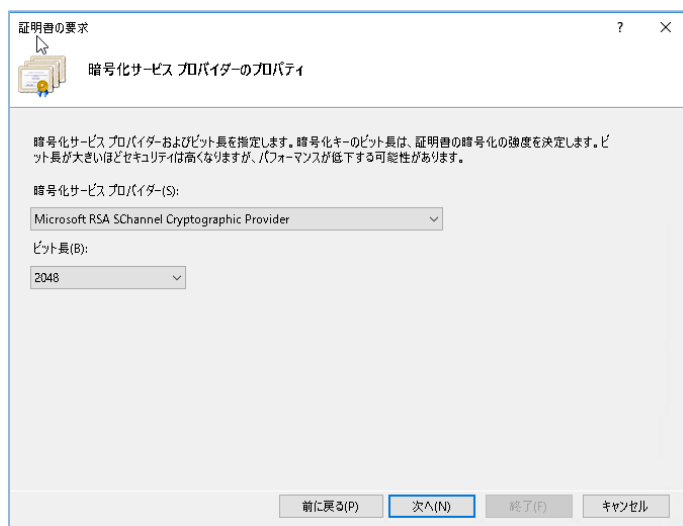


The screenshot shows a Windows dialog box titled '証明書の要求' (Certificate Request) with a sub-title '識別名プロパティ' (Identification Properties). The dialog contains several input fields for identifying the certificate request:

- 一般名 (M): servename.example.com
- 組織 (O): JCCH Security Solution Systems
- 組織単位 (OU) (U): Sales
- 市区町村 (L): Arakawa
- 都道府県 (S): Tokyo
- 国/地域 (R): JP

At the bottom, there are four buttons: '前に戻る(P)' (Previous), '次へ(N)' (Next), '終了(F)' (Finish), and 'キャンセル' (Cancel). The '次へ(N)' button is highlighted.

3. 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」をクリックすると、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 '証明書の要求' dialog box, but with the sub-title '暗号化サービスプロバイダのプロパティ' (Encryption Service Provider Properties). The dialog contains the following settings:

- 暗号化サービスプロバイダ (S): Microsoft RSA SChannel Cryptographic Provider
- ビット長 (B): 2048

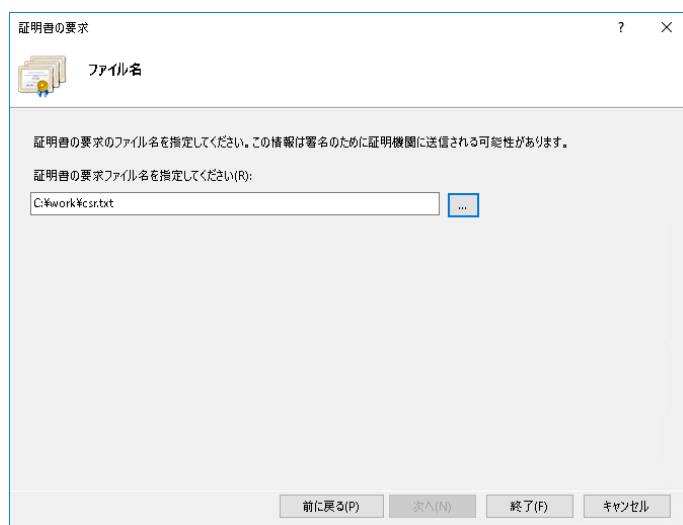
At the bottom, there are four buttons: '前に戻る(P)' (Previous), '次へ(N)' (Next), '終了(F)' (Finish), and 'キャンセル' (Cancel). The '次へ(N)' button is highlighted.

プライベート CA Gléas をご利用のお客様へ:

Gléas で CSR を署名する際、テンプレートで指定した秘密鍵の鍵長と上記ビット長が一致している必要があります。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。



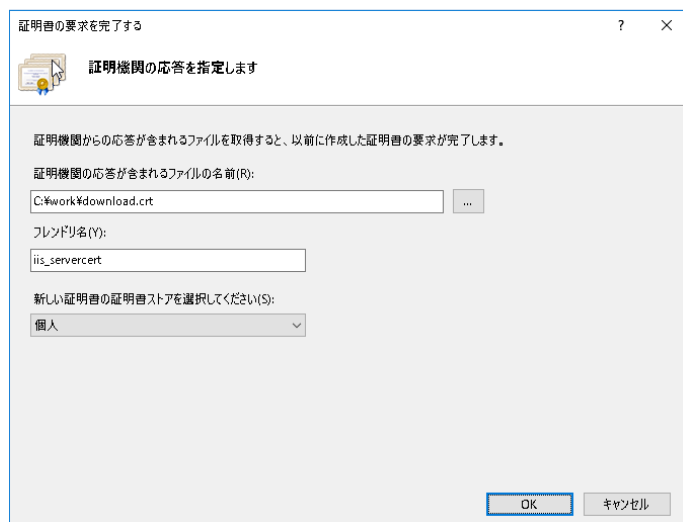
プライベート CA Gléas ホワイトペーパー  
IIS におけるクライアント証明書を利用したユーザ認証の設定手順



4. 3で保存した CSR ファイルは、プライベート CA Gléas に渡して、サーバ証明書を取得してください。サーバ証明書を取得したら、次に進んでください。

5. サーバ証明書を IIS に登録します。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。

6. 「証明機関の応答が含まれるファイルの名前」に、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。「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。



## 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



### 2.2. ルート証明書の登録

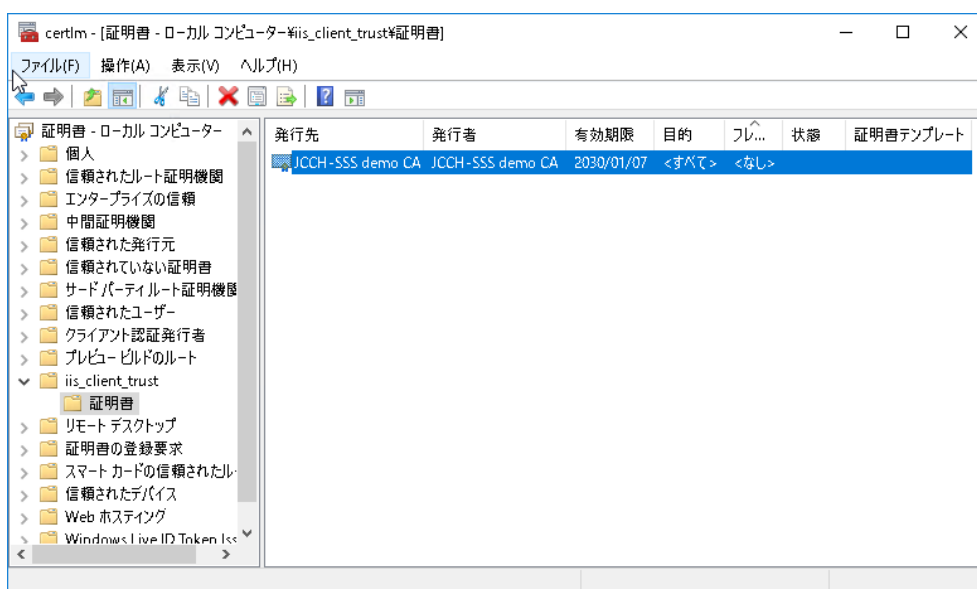
クライアント証明書によるSSL認証を利用するためには、ルート証明書の登録が必要です。これは、クライアントPCから提示されるクライアント証明書が正しいことを検証する際に利用するためです。

Powershell(あるいは、コマンドプロンプト)より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] [ルート証明書ファイル]
```

```
例) certutil -f -addstore iis_client_trust ial.cer
```

MMCで証明書ストアを見ると (certlm.msc)、ストアが作成されているのが分かります。



## 2.3. SSL ポートのバインド

以下のコマンドを実行し、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]
appid='{4dc3e181-e14b-4a21-b022-59fc669b0914}' certstorename=MY
sslctlstorename=[証明書ストア名]
```

### 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」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 証明書のバインド:

```
-----
IP:ポート                : 0.0.0.0:443
証明書ハッシュ           : 84e957e4b19e2b5c658fcd39b3bf754d8ba95f41
アプリケーション ID     : {4dc3e181-e14b-4a21-b022-59fc669b0914}
証明書ストア名          : MY
クライアント証明書の失効状態の検証: Enabled
キャッシュされたクライアント証明書のみを使用した失効状態の検証: Disabled
使用法のチェック        : Enabled
失効リストの更新を確認する間隔: 0
URL 取得のタイムアウト  : 0
Ctl 識別子               : (null)
Ctl ストア名             : iis_client_trust
DS マッパーの使用法      : Disabled
クライアント証明書のネゴシエート: Disabled
接続の拒否              : Disabled
```

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
```

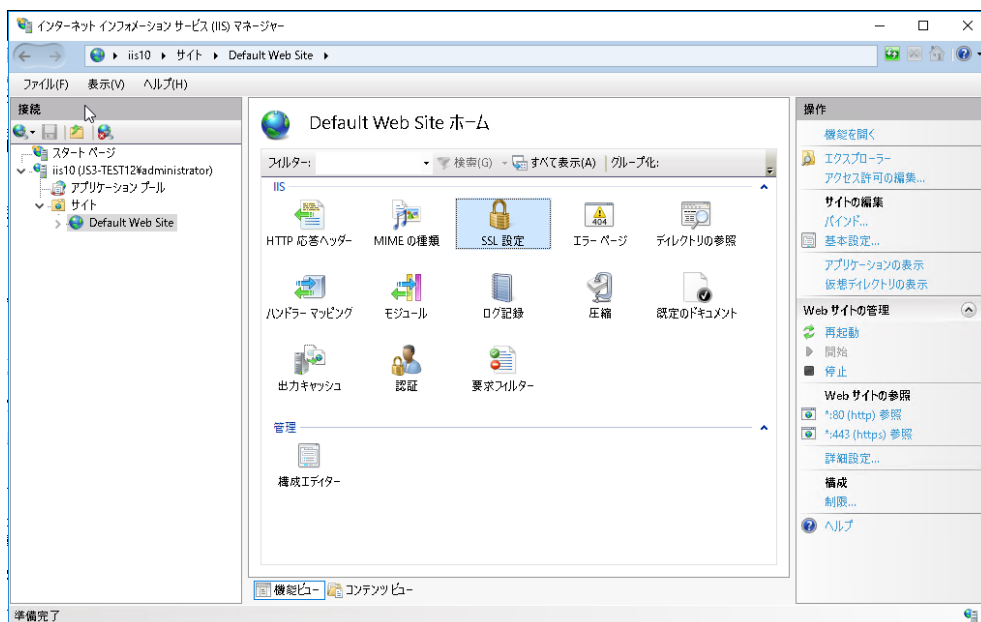
`SendTrustedIssuerList` (REG\_DWORD) を追加し、1 を設定します。

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

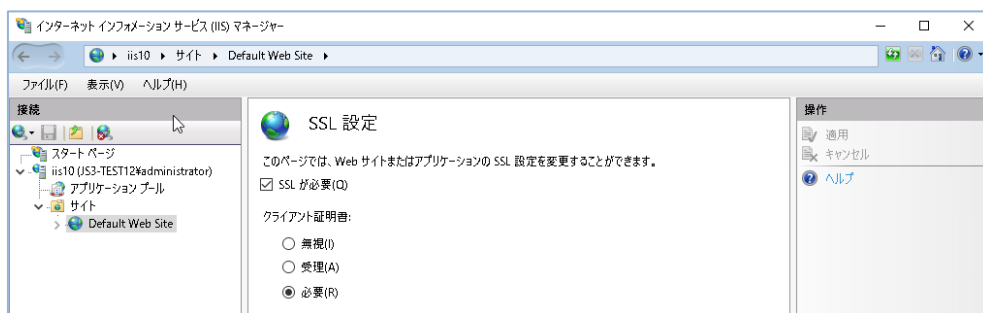


## 2.4. クライアント証明書要求の有効化

1. 左側ツリーの「Default Web Site」がクリックされた状態で、「SSL設定」アイコンをクリックします。



2. 「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。



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

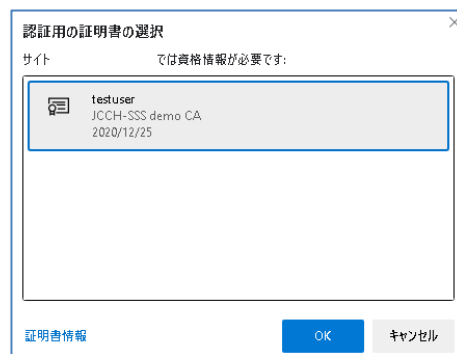
3. 右側メニューの「適用」をクリックすると、SSL設定の変更内容が確定します。

以上でIISの設定は終了です。

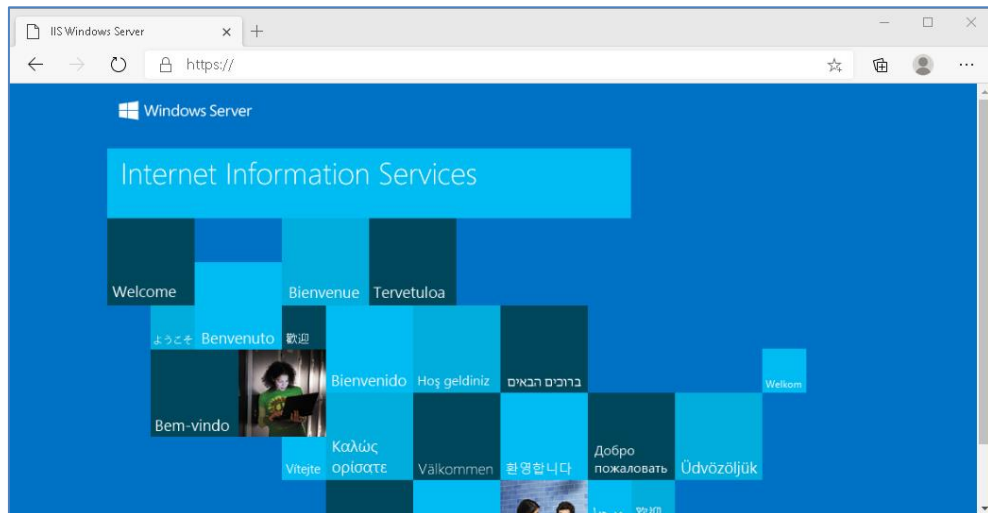
### 3. 動作確認

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Chromium版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、『4.1 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。

## 4. その他

### 4.1. 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。

## 4.2. 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ます。失効情報が記載されたデータを証明書失効リストと言います。証明書失効リスト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。証明書失効リストは、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。

### 4.3. 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
```

### 4.4. 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しなくなります。

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]
appid='{4dc3e181-e14b-4a21-b022-59fc669b0914}' certstorename=MY
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。

### 4.5. ASP.NET(C#)でクライアント証明書の情報を取得する方法

以下にサンプルコードを記載します。



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

```
<%@ 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>
```

## 5. 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