IIS10.0 (Windows Server 2022)
クライアント証明書の設定方法

GlobalSign by GMO

IIS10.0 (Windows Server 2022)でのクライアント証明書の設定方法

この手順書では、すでにサーバ証明書は設定されていることを前提として、Windows Server 2022上のInternet Information Services (IIS) 10.0でのクライアント証明書の設定方法について記載します。

サーバ証明書の設定については、以下のサイトを参考に設定を行ってください。

■証明書署名要求（CSR） の生成：

https://jp.globalsign.com/support/ssl/manual-csr/iis10.html

■サーバ証明書のインストール：

https://jp.globalsign.com/support/ssl/manual-install/iis10.html

1. IIS の構成

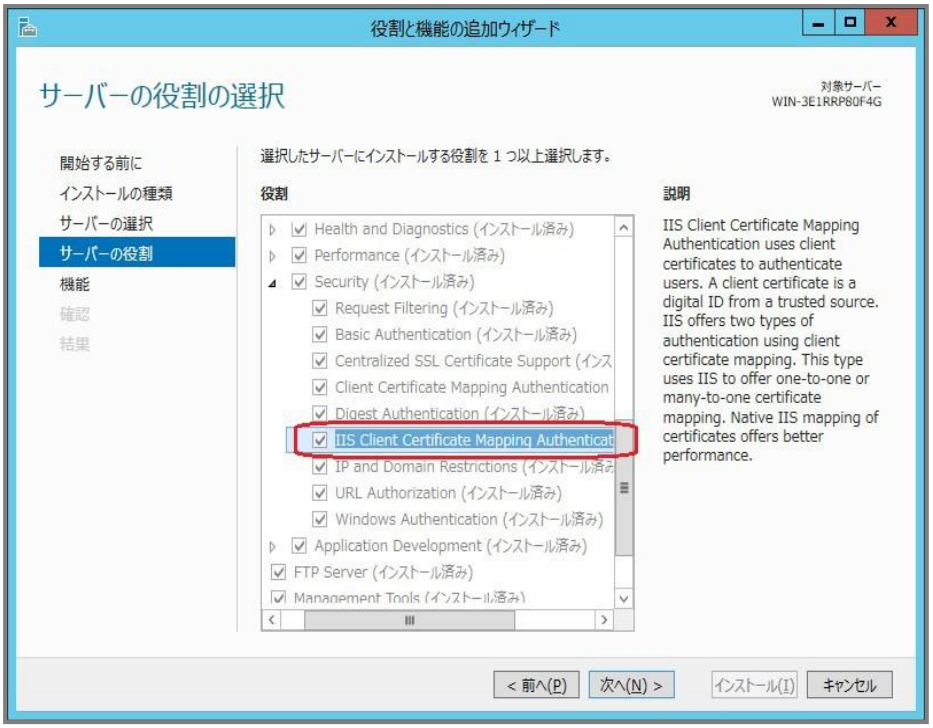
IIS がクライアント認証を利用できるように設定します。

サーバーマネージャー・ダッシュボードから「役割と機能の追加」を選択し、[役割と機能の追加ウィザード]を起動します。

[次へ(N)>]を選択して、「インストールの種類」では「役割ベースまたは機能ベースのインストール」を選択します。

続いて、[次へ(N)>]を選択して、「サーバーの選択」ではこれからクライアント証明書を設定しようとしているサーバーを選択します。

最後に、[次へ(N)>]を選択して、「サーバーの役割」まで進みます。



「役割」のチェックボックスで「Web Server (IIS)」の前の三角マークをクリックし、

「Security」の前の三角マークをクリックして、「IIS Client Certificate Mapping Authentication（IIS クライアント証明書マッピング認証)」のチェックボックスを✓します。

※すでにインストールされている場合には、すでに✓されています。

ほぼ同じ名前の「Client Certificate Mapping Authentication
（クライアント証明書マッピング認証)」がありますが、
違いについては以下のページを参照ください。
https://learn.microsoft.com/ja-jp/previous-versions/ee431606(v=technet.10)?redirectedfrom=MSDN

[次へ(N)>]を数回選択し、[インストール(I)]が選択できるようになれば選択し、
必要な役割や機能をインストールします。
[次へ(N)>]を押し続けることができなければ、必要な役割・機能は
すでにインストールされていますので、[キャンセル]を押して終了してください。

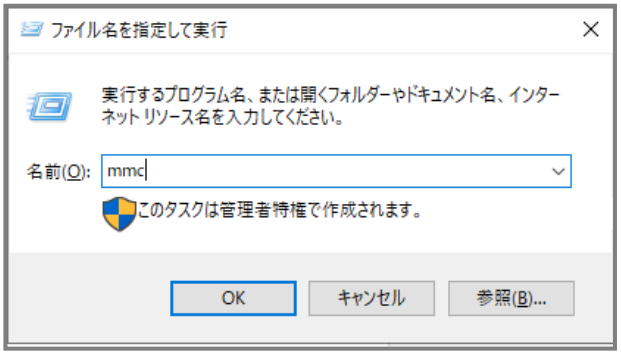
2. クライアント証明書の中間証明書・ルート証明書の設定

GlobalSign の下記リポジトリから、必要となるルート証明書、中間 CA 証明書を取得してください。

GMO グローバルサイン リポジトリ・ページ

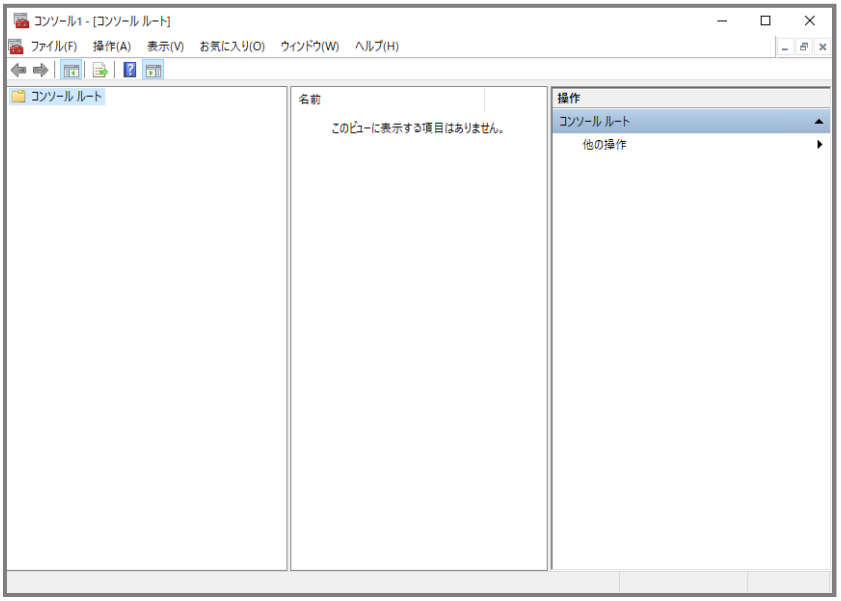
https://jp.globalsign.com/repository/

以下、Microsoft 管理コンソール(MMC)を利用して、証明書の導入を行います。



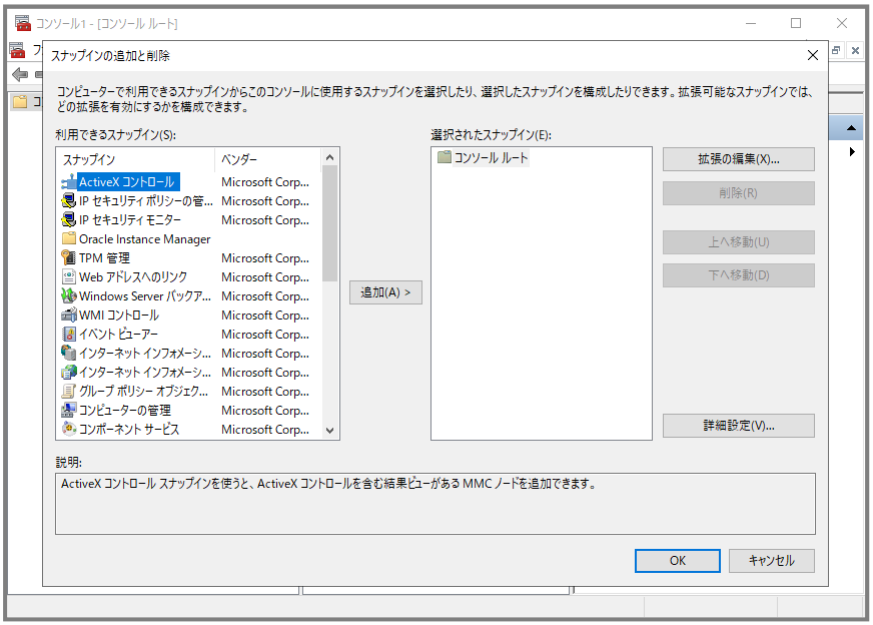
1. 「ファイル名を指定して実行」コマンドで”mmc”と入力。

以下 のようなMicrosoft 管理コンソールが開きます。

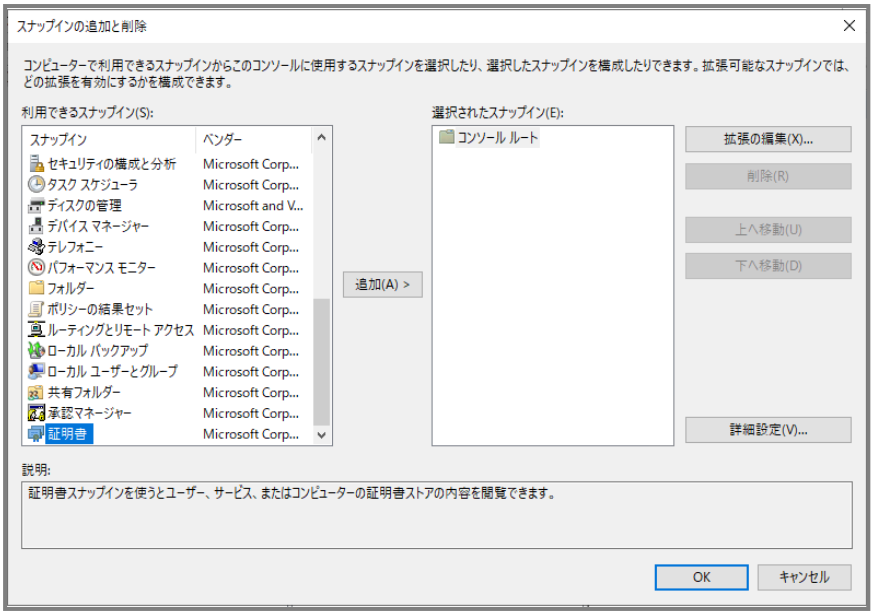


2. ファイル> スナップインの追加と削除(M)…を選択すると、

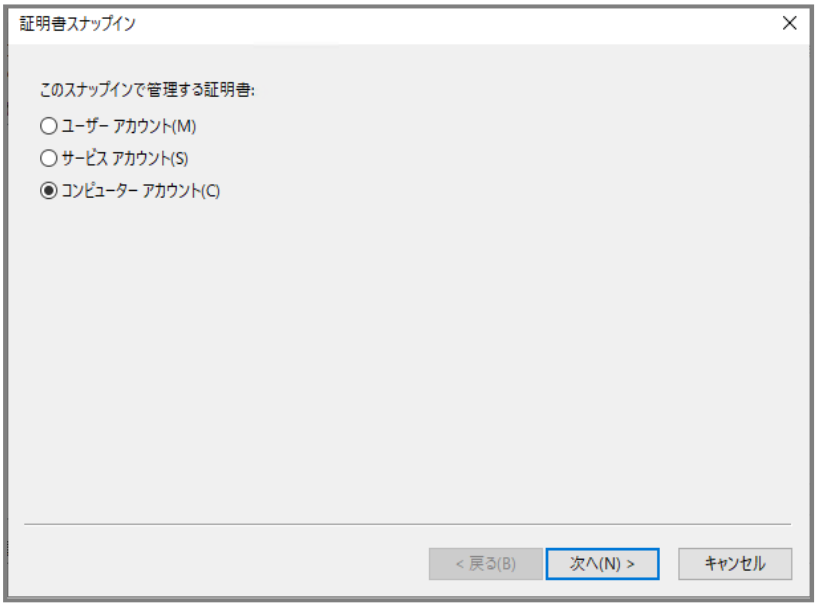
「スナップインの追加と削除」ウィンドウが開きます。



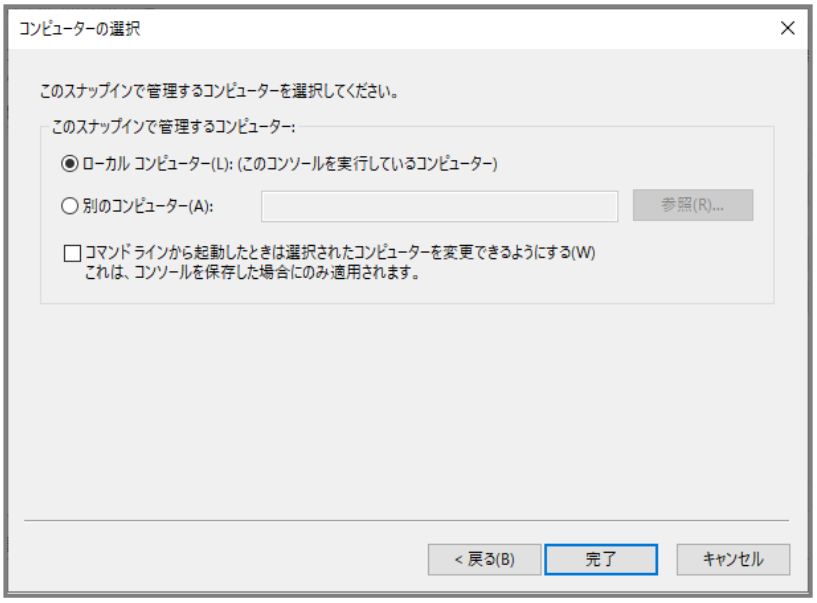
3. 「利用できるスナップイン(S)」から証明書を選択し、[追加]ボタンを選択します。



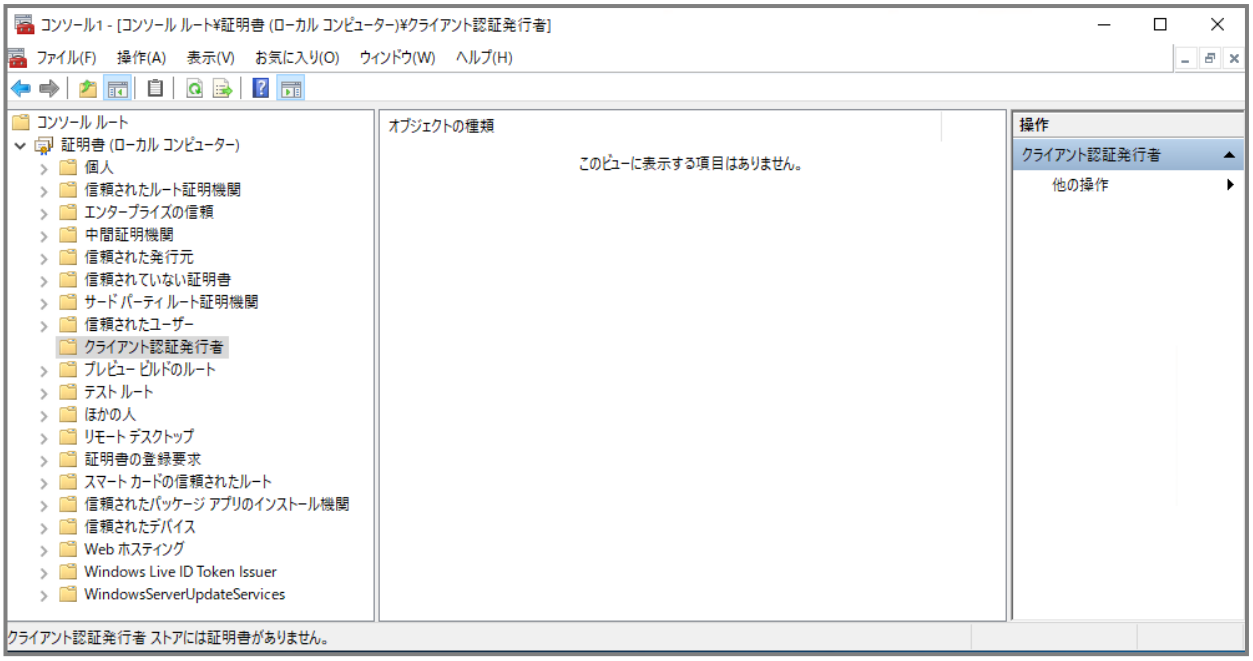
4. 「証明書スナップイン」のウィンドウが開くので、「コンピューター アカウント」の
ラジオボタンを選択して[次へ(N)>]を選択します。



5. 「コンピュータの選択」のウィンドウで[完了]を選択すると、
図のように、「選択されたスナップイン」に証明書のスナップインが追加されます。

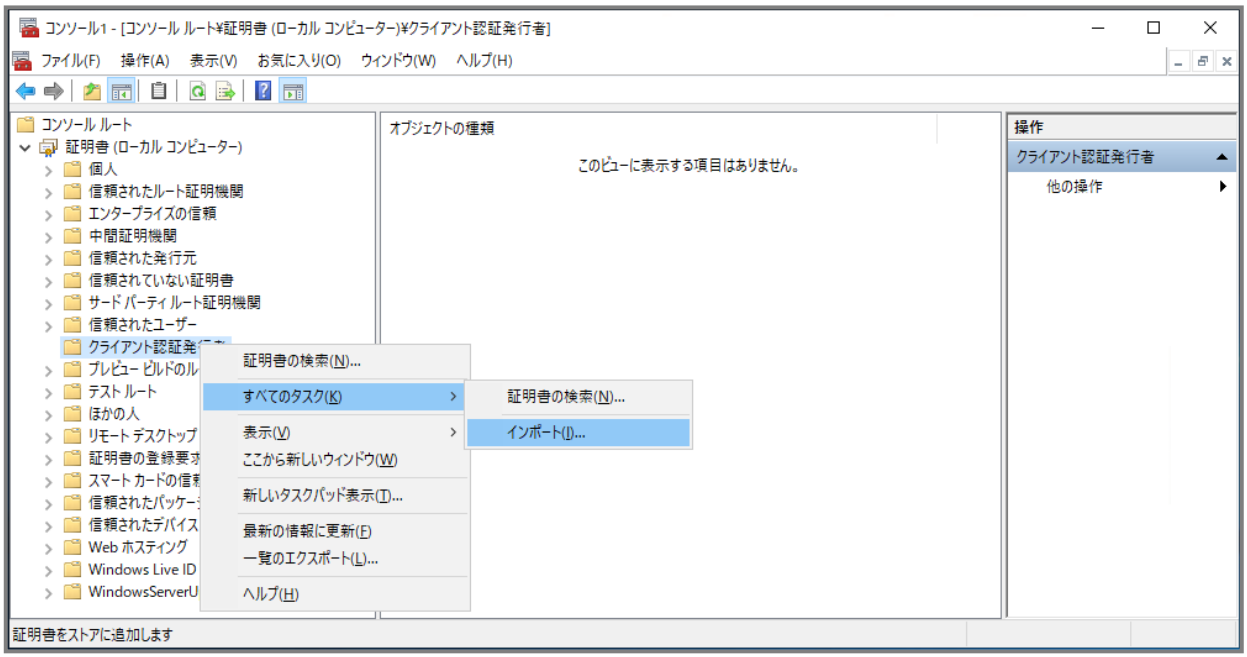


[OK]を押して終了すると MMC に証明書が追加されます。



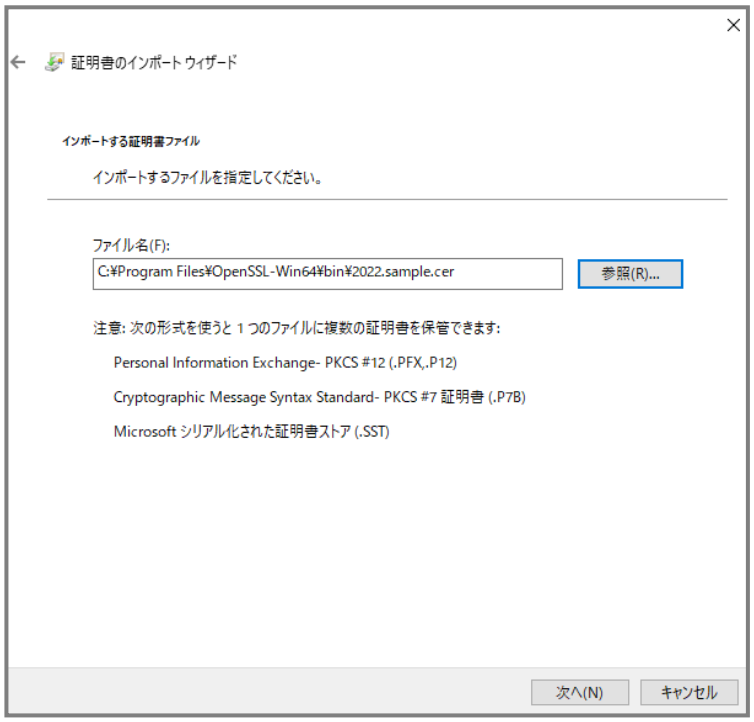
6. 左側ペインの「証明書」項目の左側にある”▷”をクリックし、

   展開されたツリー表示中の「クライアント認証発行者」を右クリックします。

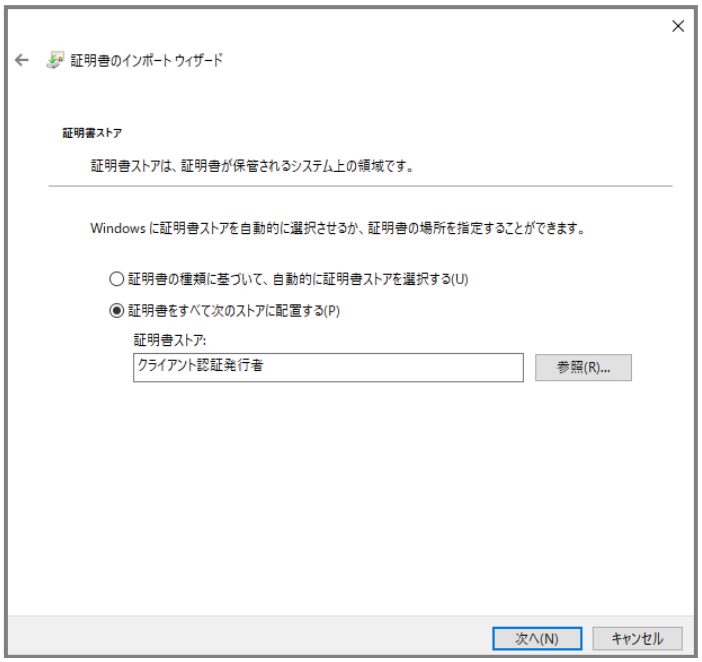


7. [すべてのタスク(K)]を選択し、[インポート]を選択します。

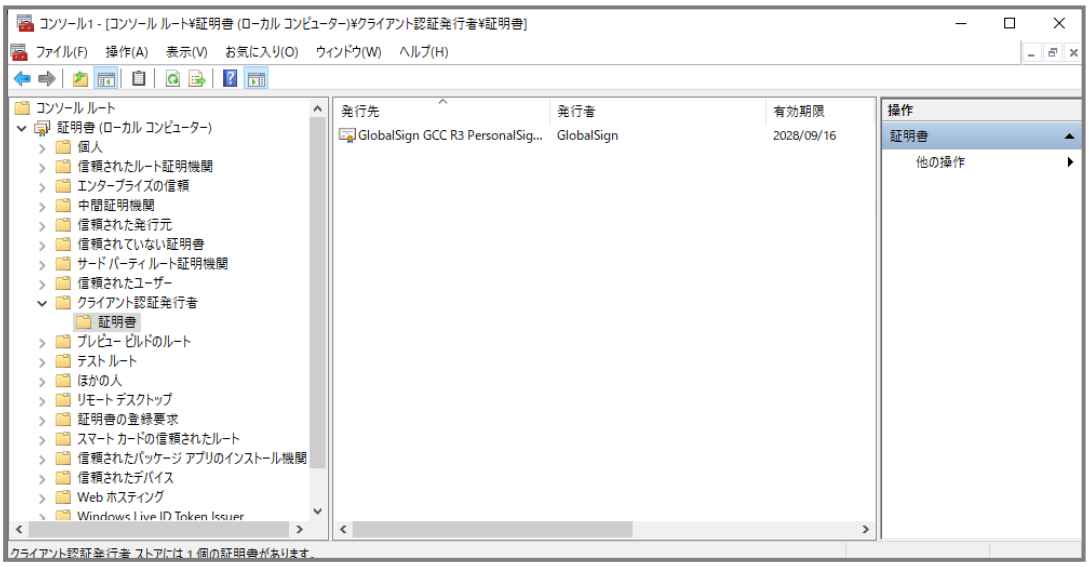
8. 「証明書のインポートウィザード」の 2 つ目のウィンドウ「インポートする証明書ファイル」の
[参照(R)…]ボタンで、ダウンロードした中間証明書を選択し、
先ほどダウンロードしたファイルを指定して、[次へ(N)]を選択します。



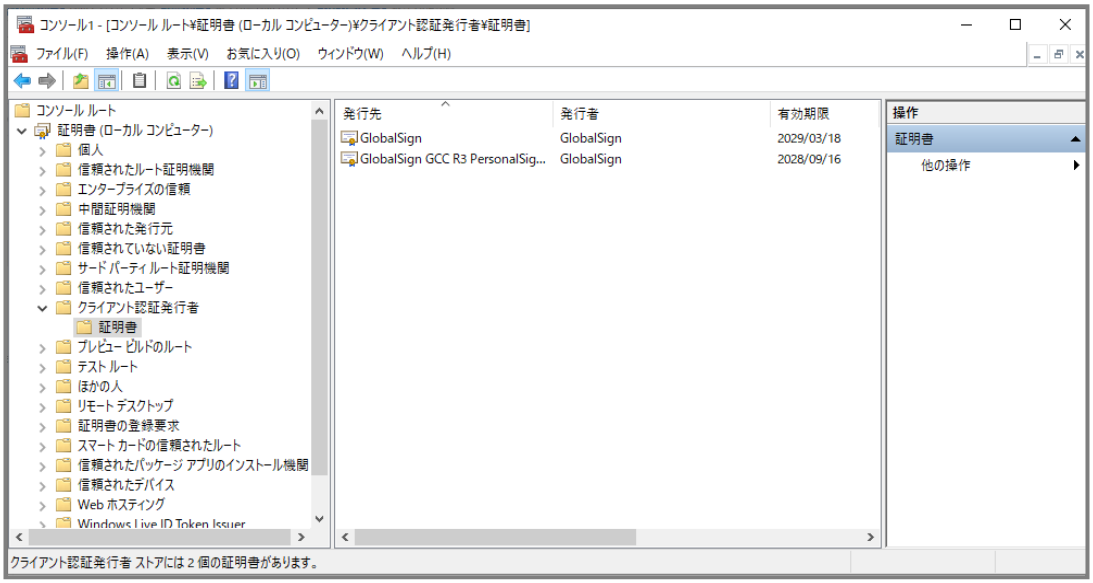
9. 証明書のストア（証明書を保管する場所の指定）ウィンドウでは、証明書ストアが
「クライアント認証発行者」になっていることを確認して、[次へ(N)]を選択します。



10. これで、中間証明書を導入することができました。



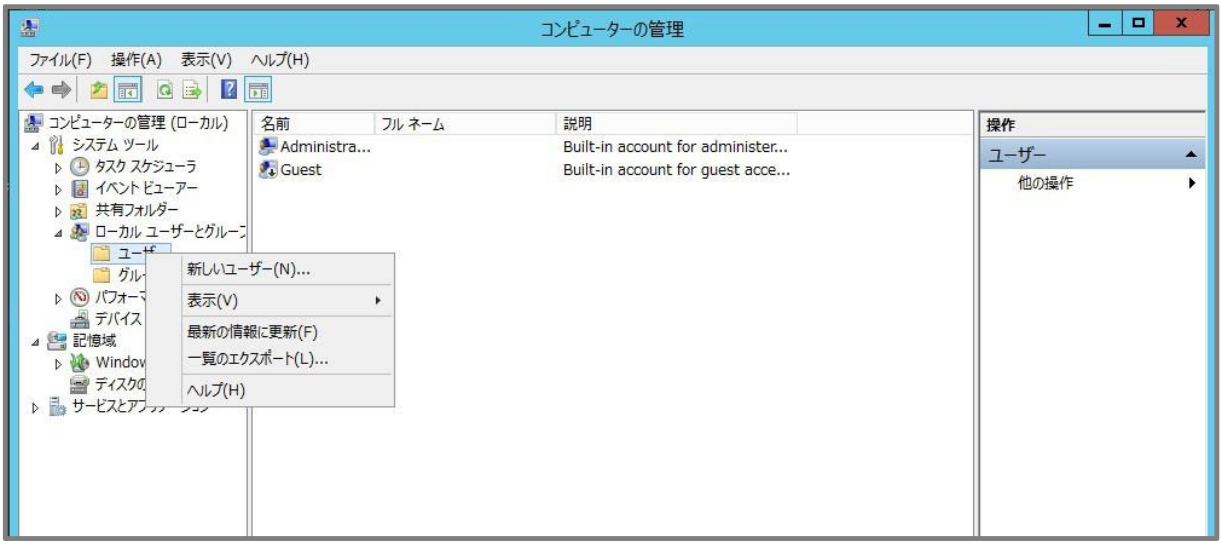
11. 同様にしてダウンロードしたルート証明書を「クライアント認証発行者」の配下の「証明書」にインポートします。



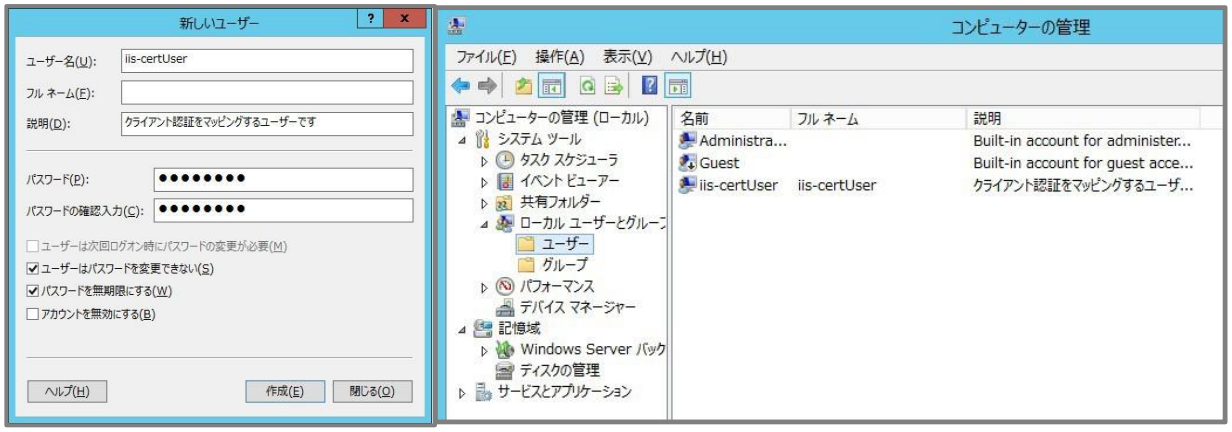
3. IIS アカウントの設定

クライアント認証はアクセスするクライアント証明書を IIS のユーザアカウントと
マッピングする必要があります。

サーバーマネージャーの「ツール」＞「コンピューターの管理」を選択して、
「コンピューターの管理」のウィンドウを開きます。



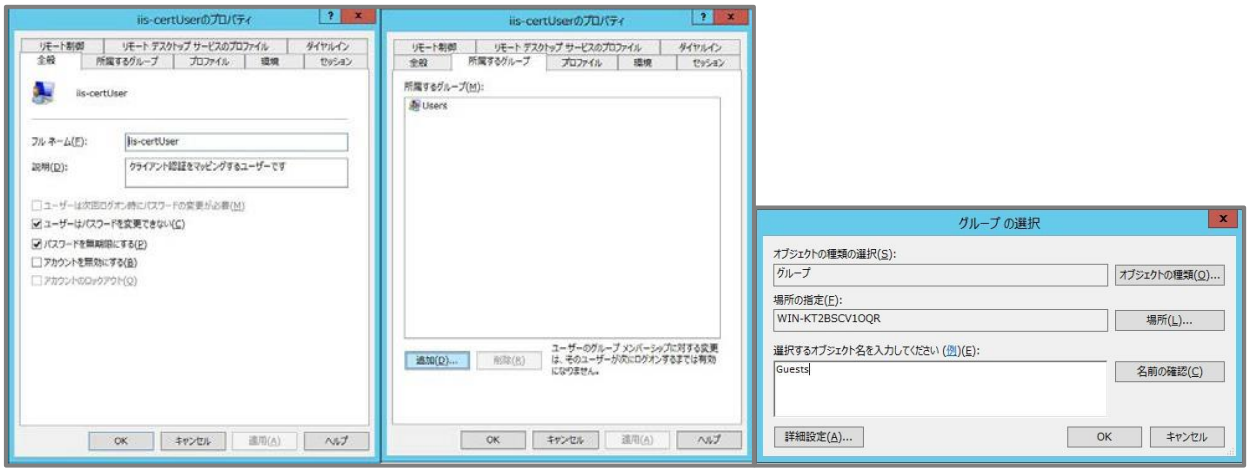
左ペインの「コンピューターの管理(ローカル)」下の「システムツール」の”▷”をクリックし、
「ローカルユーザーとグループ」の”▷”をクリック。
「ユーザー」ホルダを右クリックして「新しいユーザー(N)…」選択します。



ユーザー名、パスワードは任意です。

「ユーザーはパスワードを変更できない」、「パスワードを無期限にする」に✓を入れます。

[作成(E)]を選択すると、新しいユーザーが追加されました。



作成後、プロパティを確認し、「所属するグループ」Usersで[追加(D)…]を選択して、

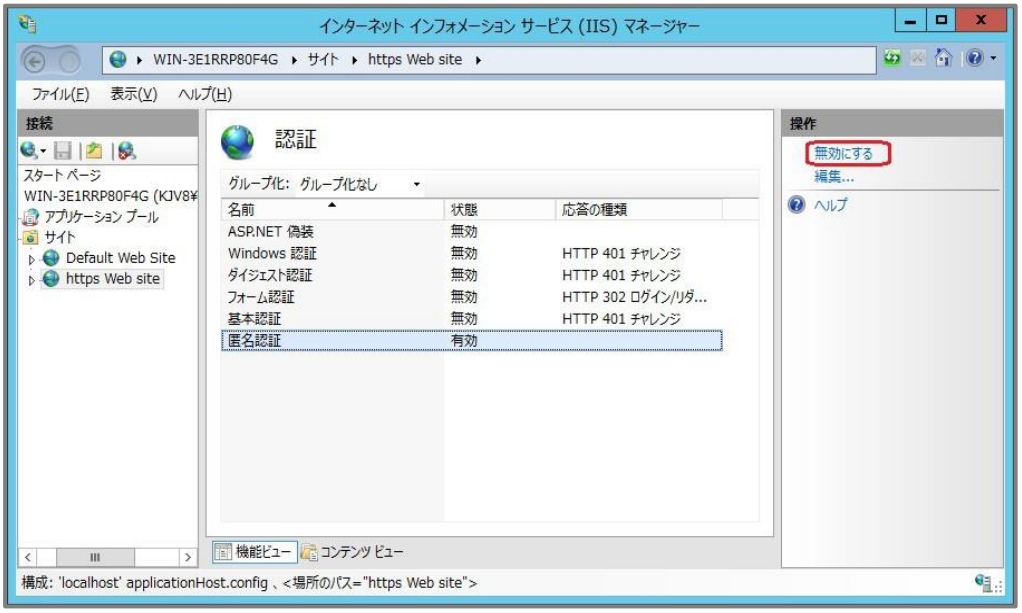
Guests を追加します。Users グループは削除します。

※作成したユーザーのお取り扱いには十分ご注意ください。

4. 匿名アクセスの無効化

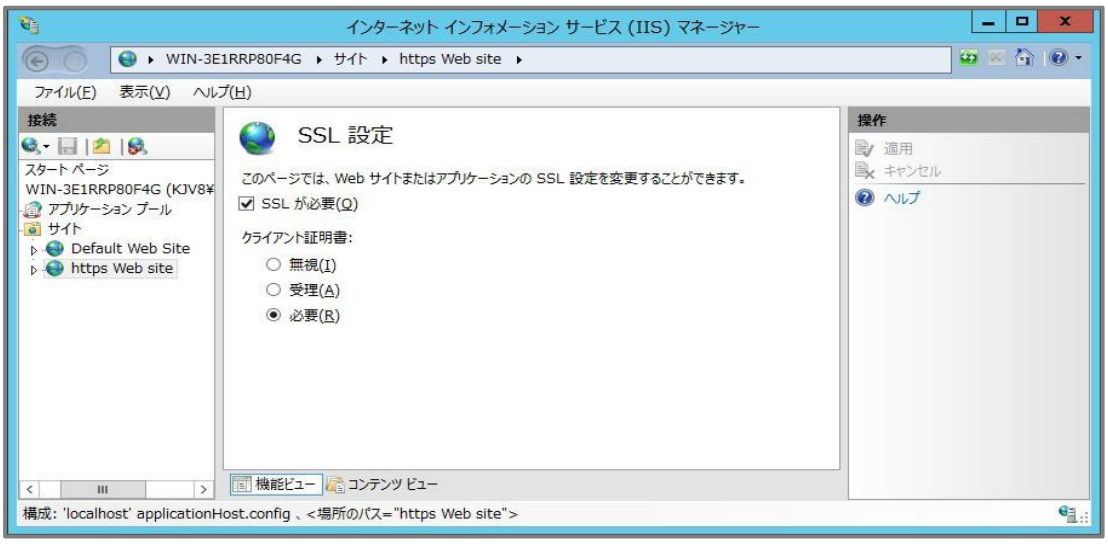
IIS マネージャーから「認証」のアイコンをクリックすると、認証の設定ペインが表示されます。

匿名認証を無効にします。



5. SSL アクセスの有効化

IIS マネージャーにて「SSL 設定」のアイコンをダブルクリックすると、SSL 設定のペインが表示されます。「SSL が必要」に✓を入れ、「クライアント証明書」は「必要」のラジオボタンを選択します。



6. クライアント証明書を多対一にマップする

本来、クライアント証明書のユーザーをどのようにサーバで認証させるかは基本的な設計で、
サーバ設定以前にどのようにユーザー認証するかを設計しておく必要があります。
ここでは、もっとも一般的なクライアント証明書による認証について説明します。
それぞれの選択肢については、参考のためのリンクを掲載するにとどめます。

Windows サーバのクライアント証明書認証には IIS を使用するもの、Active Directory を利用して認証するものの 2 種類があります。

ここでは IIS を使用したクライアント証明書マッピング認証の設定について説明します。

■IIS を使用したクライアント証明書マッピング認証
https://technet.microsoft.com/ja-jp/library/ee431606.aspx

■Active Directory を使用したクライアント証明書マッピング認証
https://technet.microsoft.com/ja-jp/library/ee431573.aspx

また、クライアント証明書 1 枚と 1 ユーザーを 1 対 1 で対応させるoneToOneMappings と、
複数のクライアント証明書を 1 ユーザーに多対 1 で対応させる manyToOneMappings があります。

それぞれの詳細については下記のページを参考にしてください。

■複数のクライアント証明書を 1 ユーザーに対応させる
https://technet.microsoft.com/ja-jp/library/ee431621.aspx

■クライアント証明書 1 枚と 1 ユーザーを 1 対 1 で対応させる
https://technet.microsoft.com/ja-jp/library/ee431627.aspx

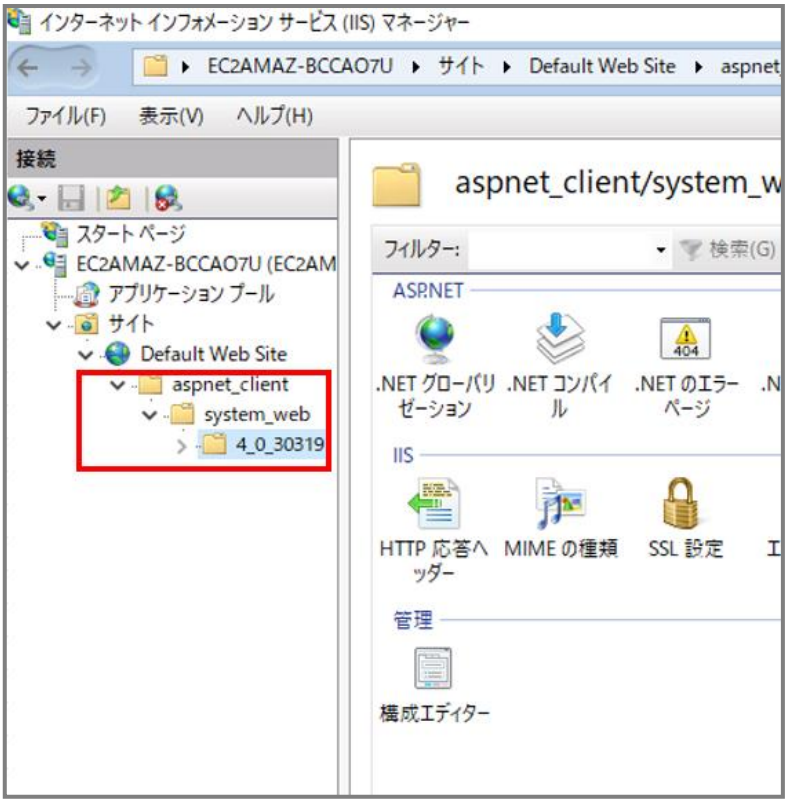
ここでは、多対 1 で対応させる manyToOneMappings の設定について説明します。

IISクライアント証明書マッピング認証の制約について

クライアント証明書を使用した、O/OUによるマッピング認証は、「サイト」単位で有効です。

ディレクトリに対しては正しく動作しませんので、ご注意ください。

例：赤枠のディレクトリに対しても構成エディターが設けられていますが、機能しません。

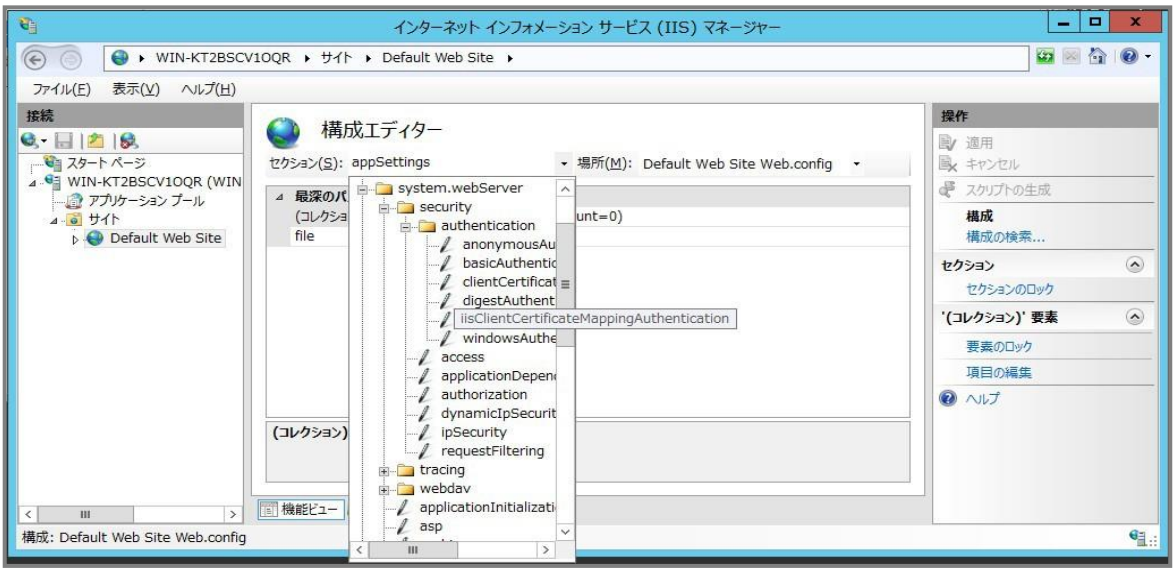


あくまで、「サイト」単位でマッピング認証を設定することが可能です。

1. ISS マネージャーから「構成エディター」を起動します。

   中央のペインに構成エディターが開きます。

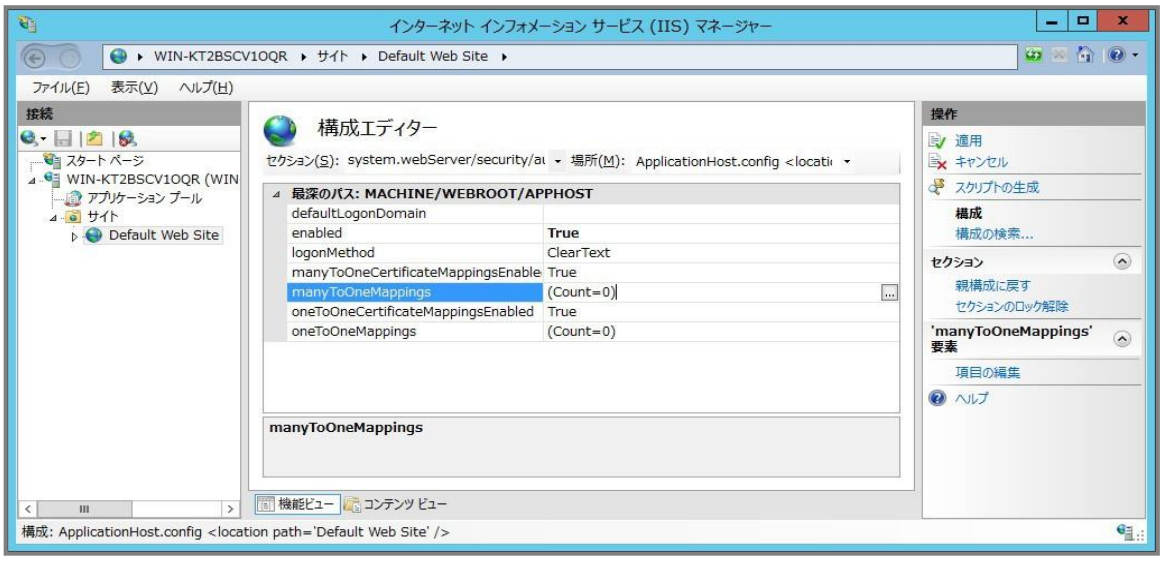
   「セクション」の項目から system.webServer > security > authentication > iisClientCertificateMappingAuthenticationを選択します。



2. 構成エディターでクライアント証明書認証の設定表示された画面で、

   以下の様な値になります。

   manyToOneCertificateMappingsEnabled: True



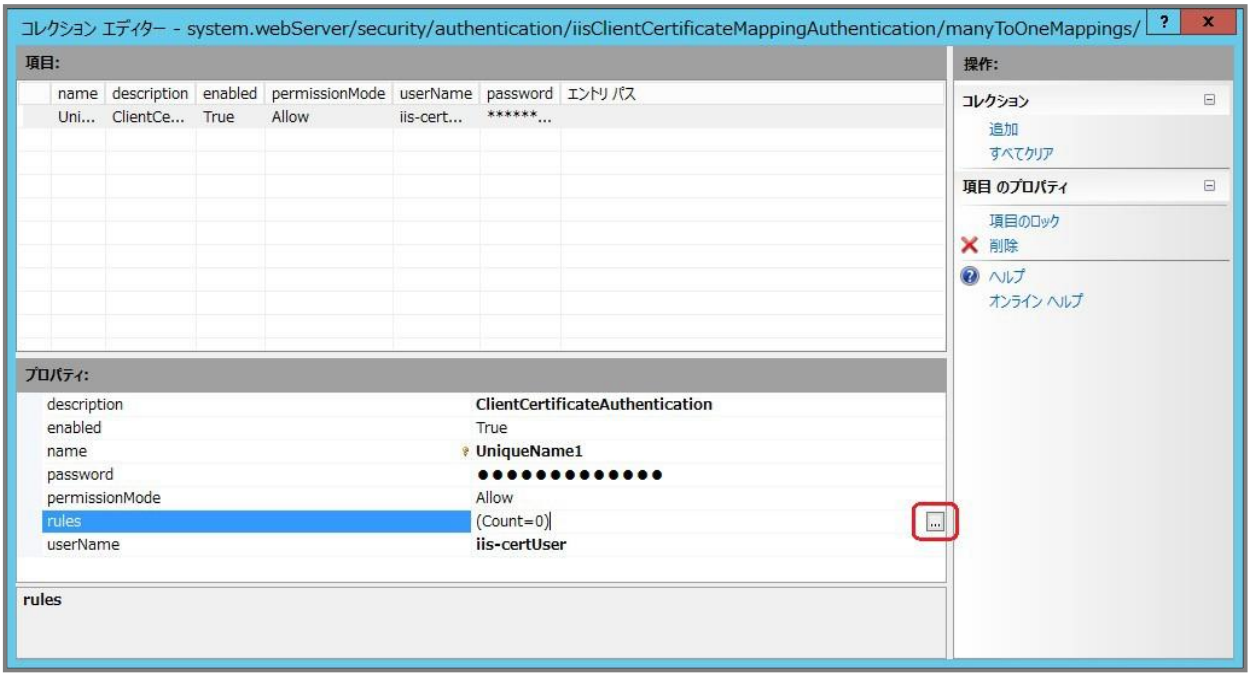
3. 多対１マッピング認証の設定 manyToOneMappings の項目にカーソルを置くと、

項目に右端に[…]マークが表示されます。

これをクリックして構成エディターを開きます。

右ペインの「追加」を選択して以下のようにプロパティを入力します。

description	このルールの説明
enabled	True
name	このルールに設定する任意のユニーク名前
password	クライアント証明書認証を割り当てる **IIS アカウントのパスワード**
userName	クライアント証明書認証を割り当てる **IIS アカウントのユーザ名**



4. ルールの設定をします。

「rules」の項目にカーソルが来るとその項目の右端に[…]が現れます。

これをクリックすると、新たな構成エディターが開き、マッピングのルールを設定することができます。

右ペインの「追加」を選択して、証明書項目の条件を設定します。

認証条件の設定には、通常クライアント証明書の発行の際に

「専用 BaseDN」で指定したO（組織名）やOU（部門名）を設定します。

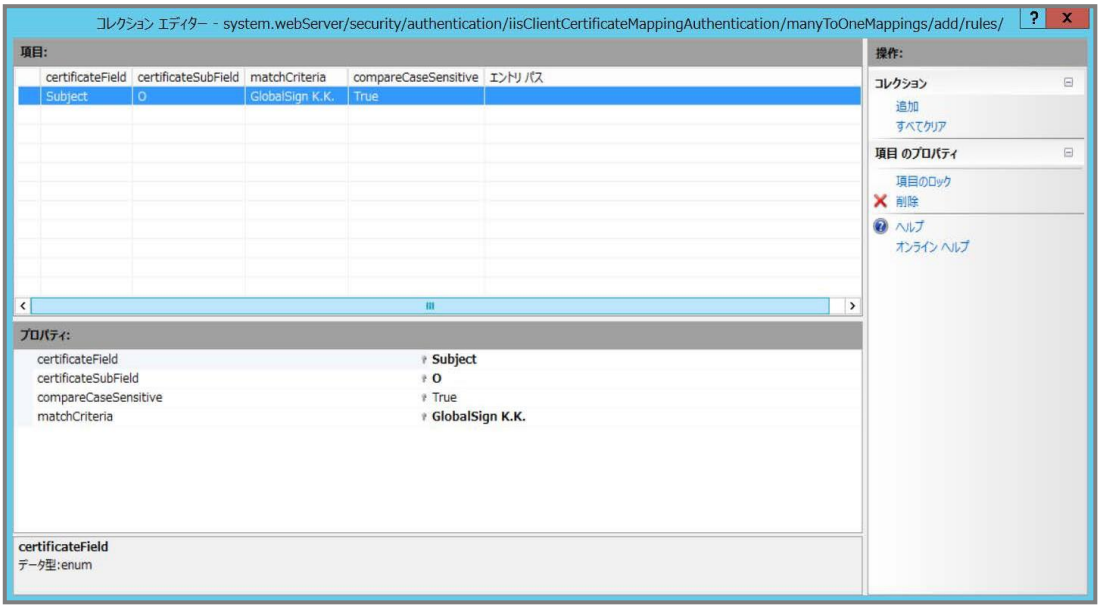
例えば、O に”GlobalSignK.K.”、OU に”Sales Div.”を設定された証明書を認証する場合には、

ここでこれらの2つの条件を設定します。

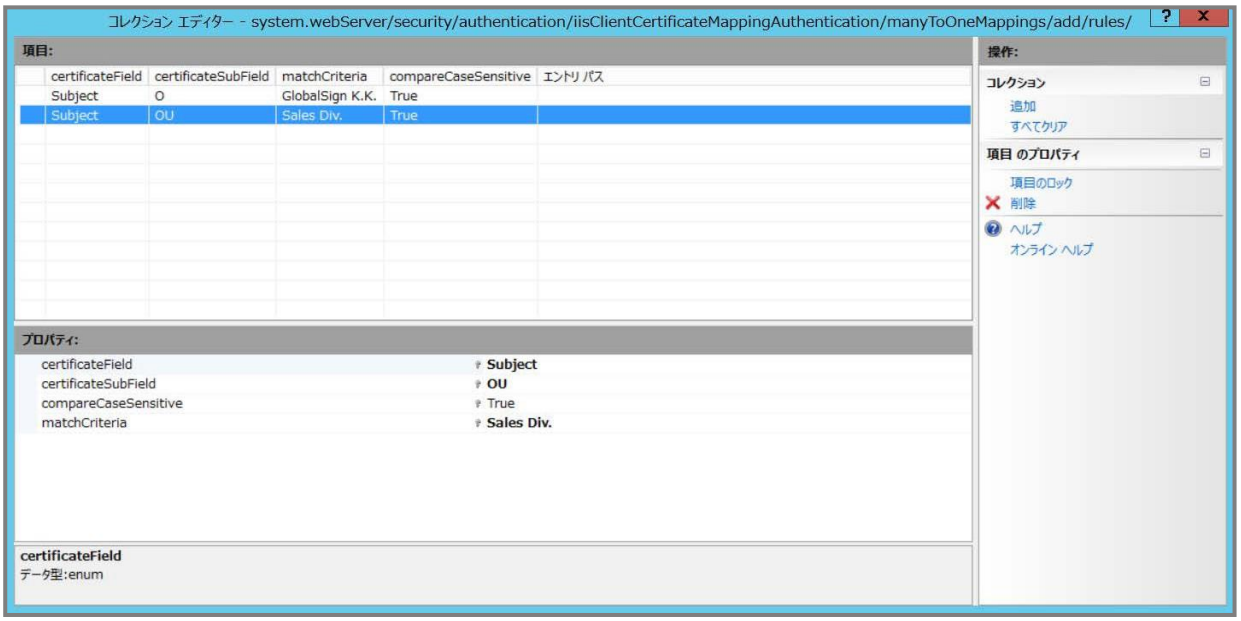
certificateField	証明書の発行者(Issuer)またはサブジェクト(Subject)のいずれかを選択します。 証明書の他のフィールドを条件に設定することはできません。
certificateSubField	上で指定したフィールドに対するサブフィールドを指定します。 通常 O、OU に対して設定します。
matchCriteria	照合内容を指定します。

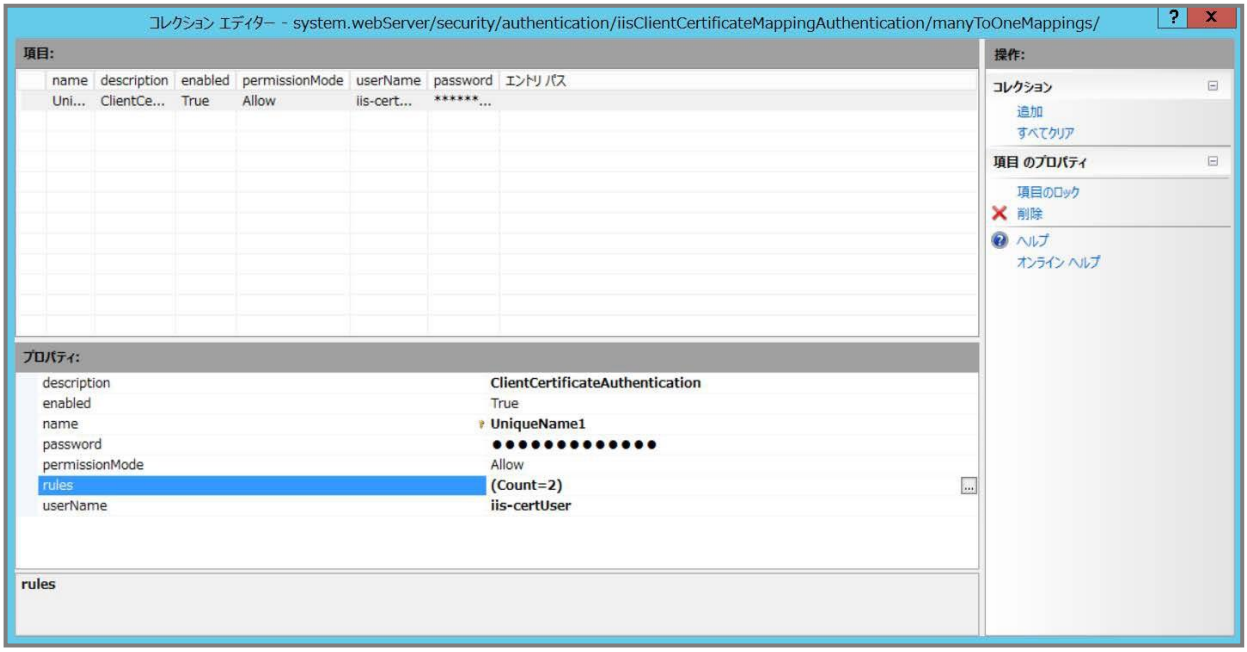
以下の図では、Subject のO に”GlobalSign K.K.” を設定することで、

証明書のサブジェクトの O（組織名）が”GlobalSign K.K.”である証明書を認証する例を示します。



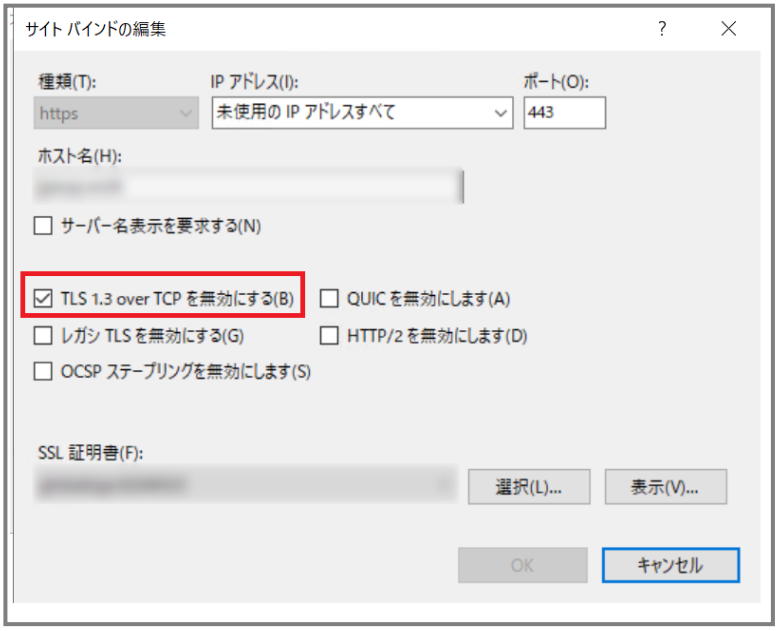
更に、「追加」から以下のように Subject の OU に”Sales Div.”を追加設定することで、
証明書のサブジェクトの O（組織名）が”GlobalSign K.K.”であり、
なおかつ OU（部門名） が”Sales Div.”である証明書を認証する例を示します。





マッピングの設定が完了すると上記のようになります。
以上で設定は完了です。

※注意：Windows Server 2022のIISにおいて、クライアント証明書認証で
うまく接続できない場合があります。
その際は、バインド編集から「TLS 1.3 over TCPを無効にする」にチェックを入れて再度お試しください。



■クライアント認証の動作について

サーバ側に設定した CA のチェーン以外の証明書も選択肢に表示されます。

レジストリエディタから、SendTrustedIssuerList を有効にすることで回避できますので、以下の設定をお試しください。（必須の設定ではありません）

【レジストリの編集（値の追加）】

レジストリは Windows システムの非常に重要なファイルです。

レジストリの編集を誤ると、Windows が起動しなくなるなど、

リカバリー再セットアップを余儀なくされるような事態が発生する恐れがあります。

こちらの変更作業によって、万一不具合が生じました場合も弊社では責任を負いかねます。

慎重にご実施ください。

レジストリを編集する際には、あらかじめレジストリキーを保存しておくことをお勧めいたします。

SendTrustedIssuerList を設定して、CTL を送信する構成に設定します。

1) IIS サーバに管理者権限をもつユーザーでログオンします。

2) [ファイル名を指定して実行] を開き、regedit と入力して [OK] をクリックします。

3) 以下のレジストリにレジストリを設定します。

レジストリキー：**HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel**

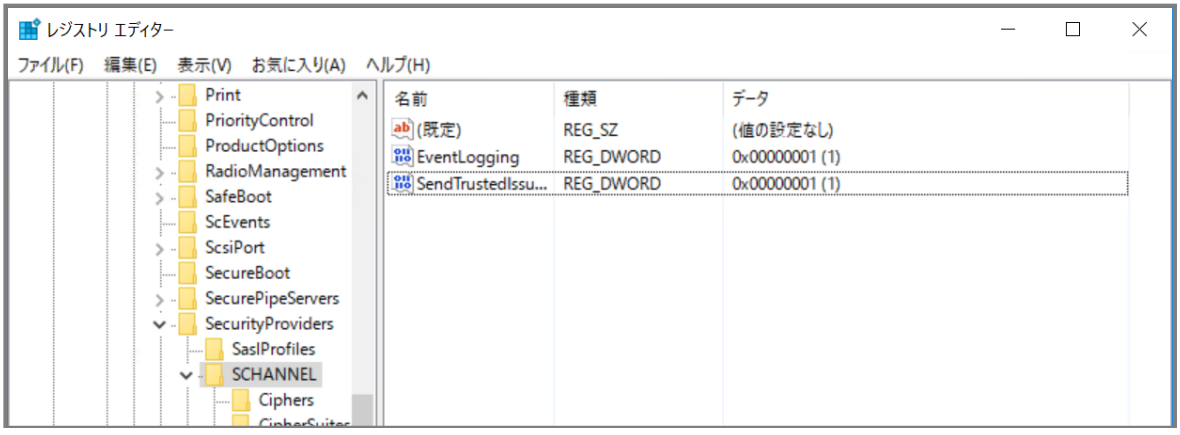
名前: **SendTrustedIssuerList**

型: **REG_DWORD**

値: **1**

※SendTrustedIssuerList は既定では存在しないレジストリ値となります。

レジストリエディタ上で値を新規作成して、レジストリを設定してください。



GMO グローバルサイン株式会社

〒150-0043 東京都渋谷区道玄坂 1-2-3　渋谷フクラス

TEL：03-6370-6500　https://jp.globalsign.com