IIS8 (Windows Server 2012)での

クライアント証明書の設定方法

この手順書では、すでにサーバー証明書は設定されていることを前提として、Windows Server 2012 R2 上の Internet Information Services (IIS) 8.5 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。

サーバー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/csr/529.html?service=ssl サーバー証明書のインストール：

https://jp.globalsign.com/support/server/530.html?service=ssl

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(図１)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。(図２)

図１

図２

[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。

[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。

[次へ(N)>]を選択して、「サーバーの役割」(図 3)まで進みます。

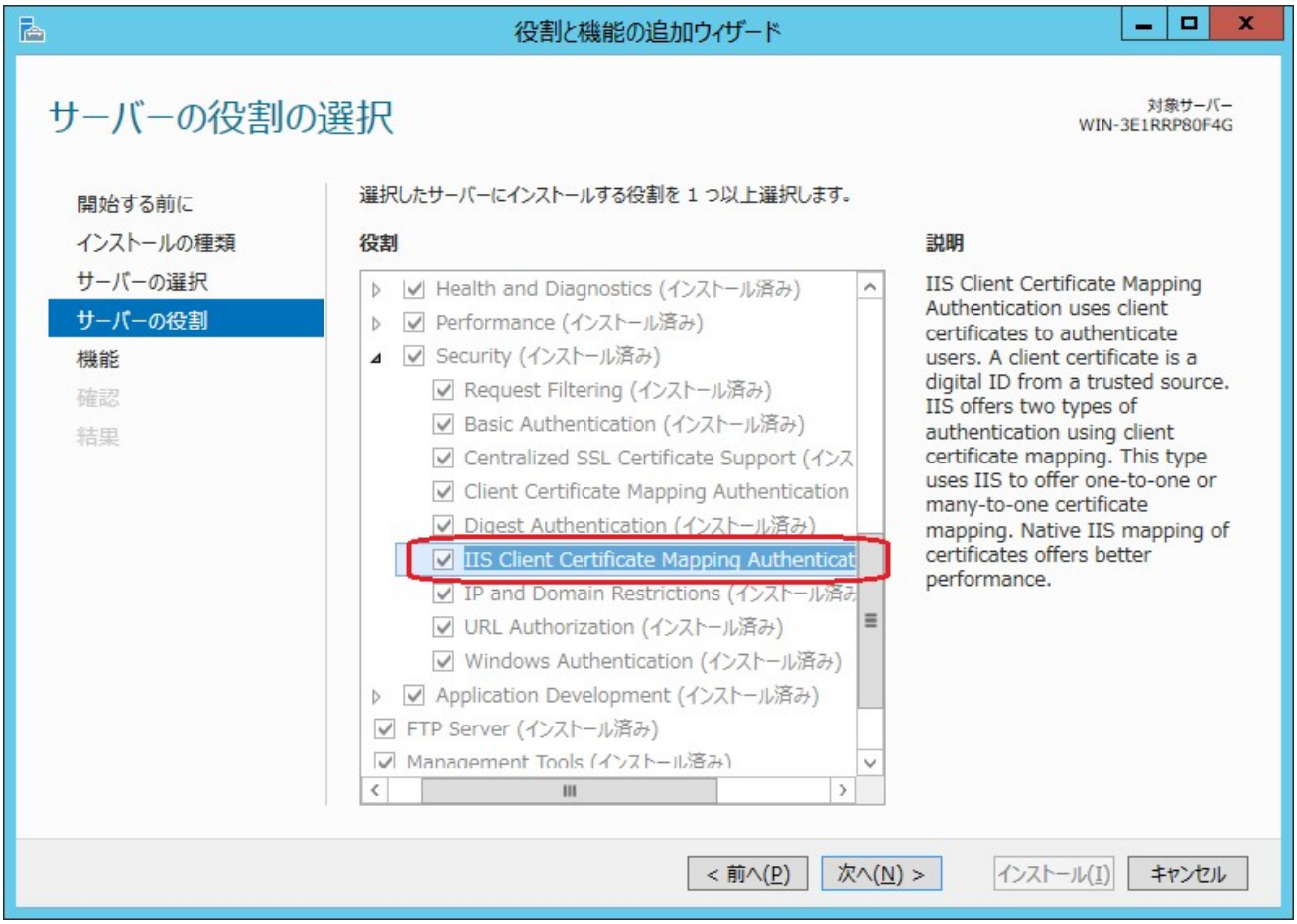


図 3

「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、「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に✔ を入れます。

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://technet.microsoft.com/ja-jp/library/ee431606.aspx

[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(図４)

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

図４

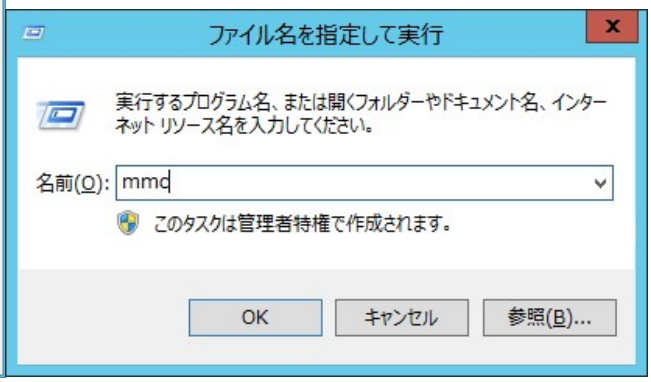
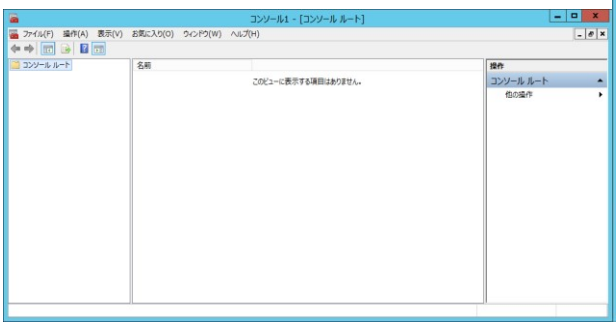


図５

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。(図５) 図 6 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。(図７)



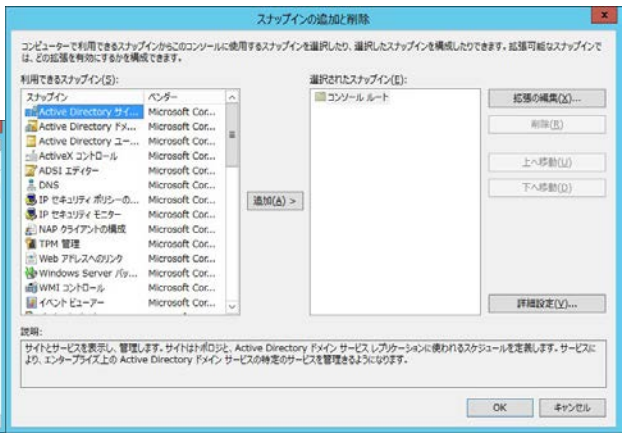


図 6

図７

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。(図８)

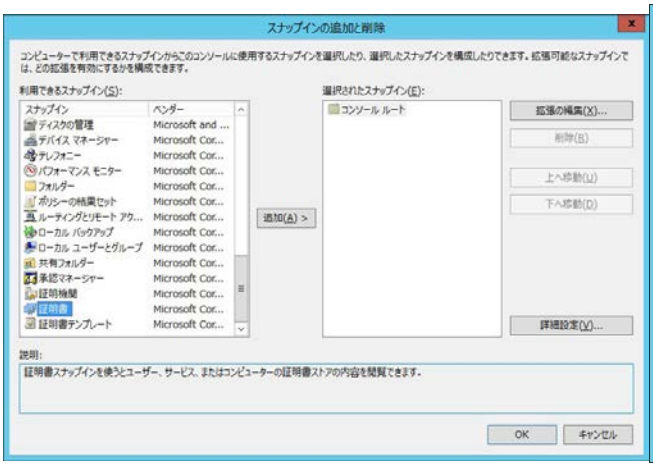


図８

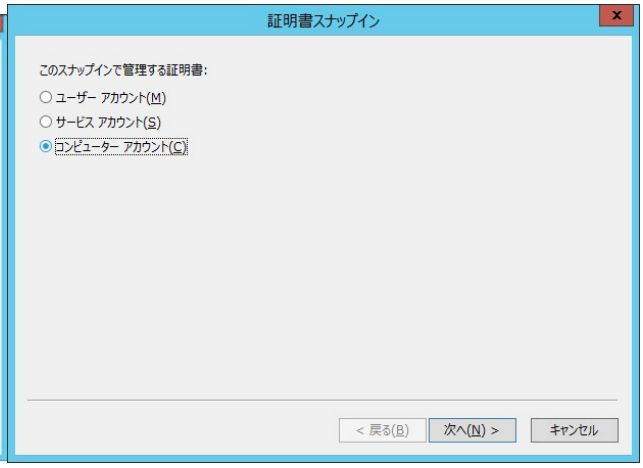


図９

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。(図９)

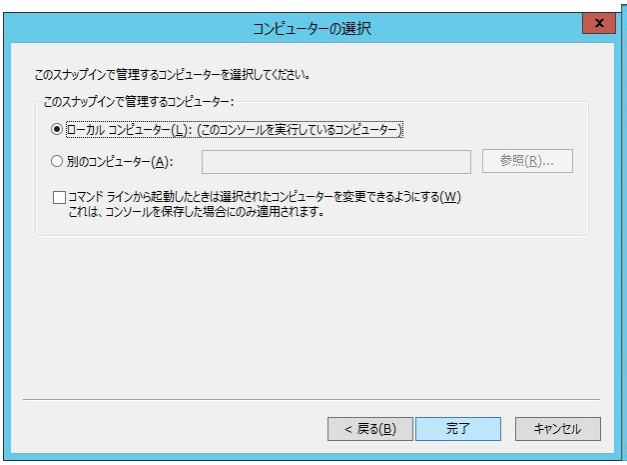


図１０

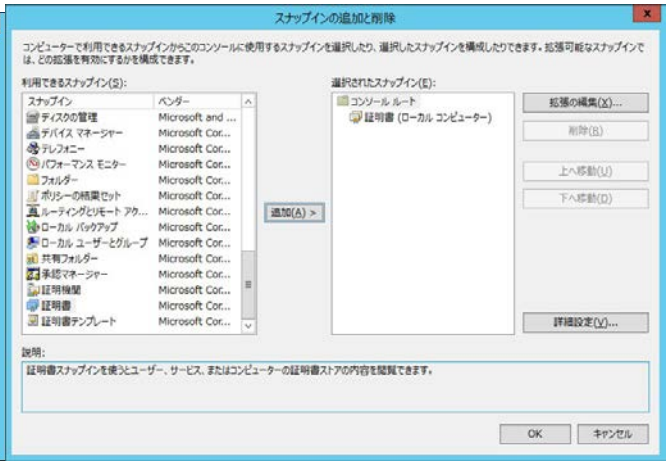


図１１

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１１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図１２のように MMC に証明書が追加されます。

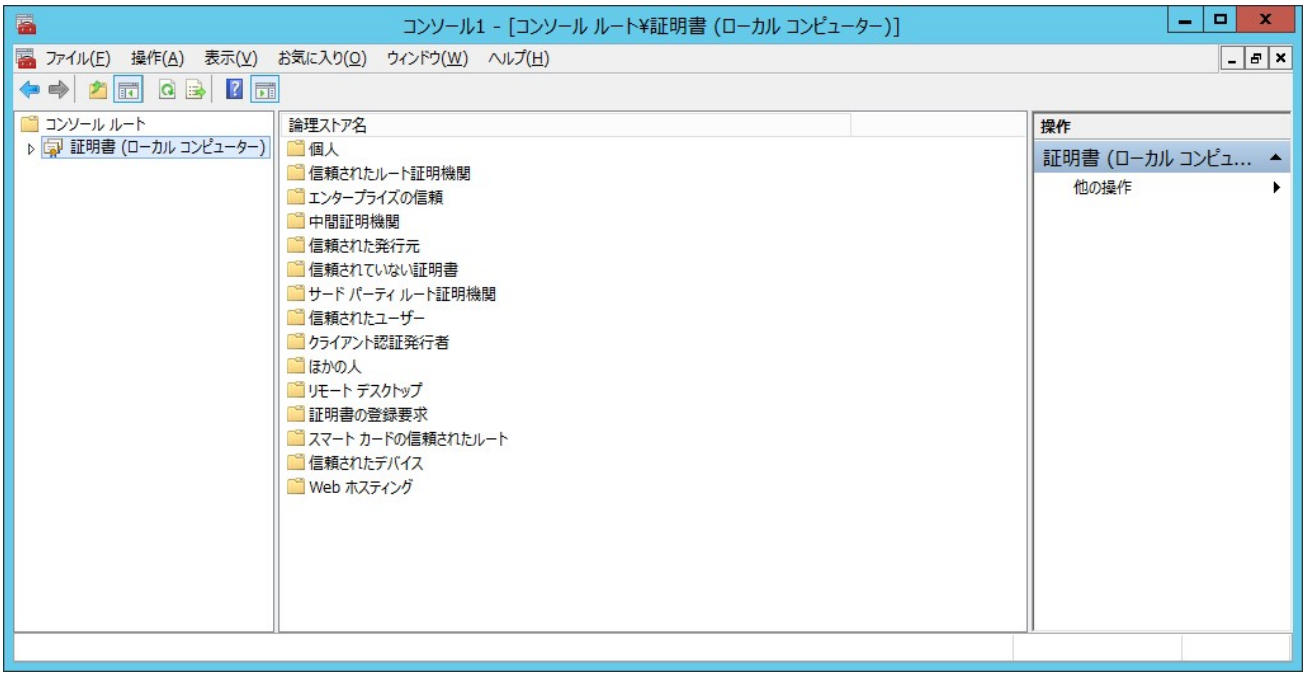


図１２

6. 左側ペインの「証明書」項目の左側にある”▷”をクリック、展開されたツリー表示中の「中間証明書」の”▷”をクリック。
7. その下の「証明書」を右クリックして、[すべてのタスク(K)]を選択、[インポート]を選択。(図１３)

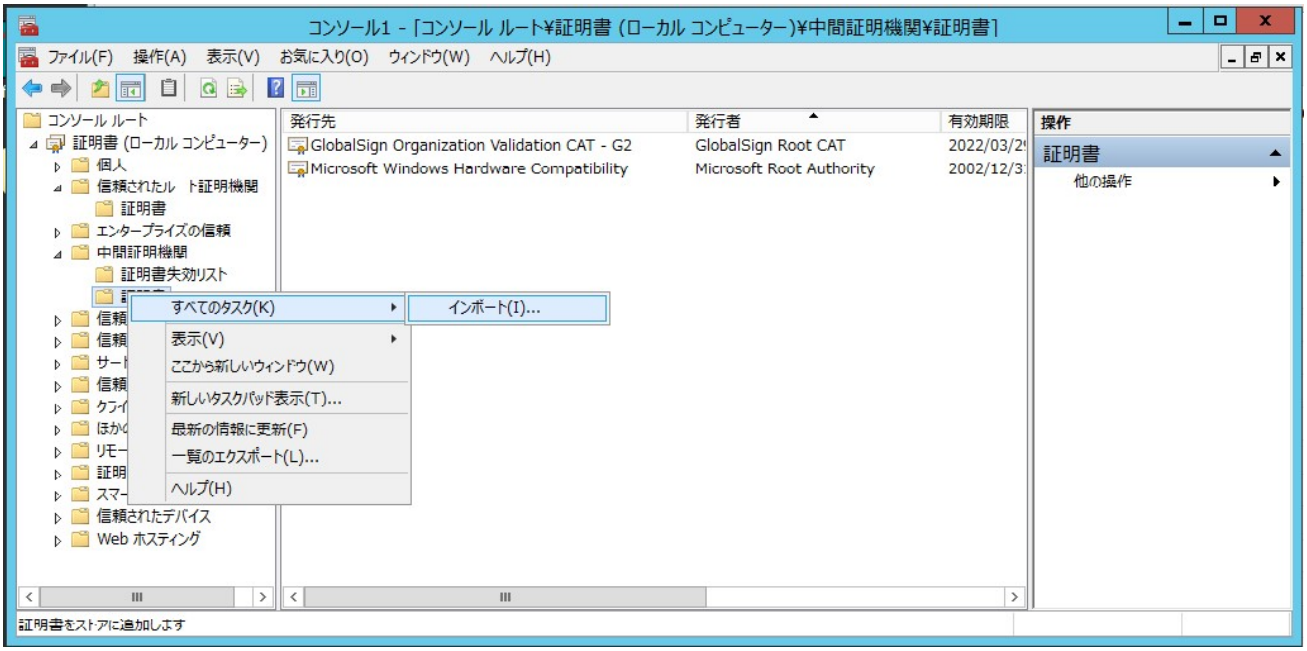


図１３

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。(図１４)

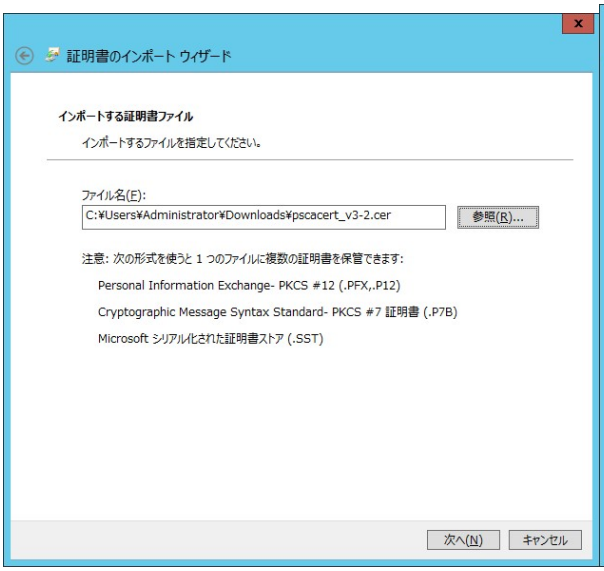


図１４

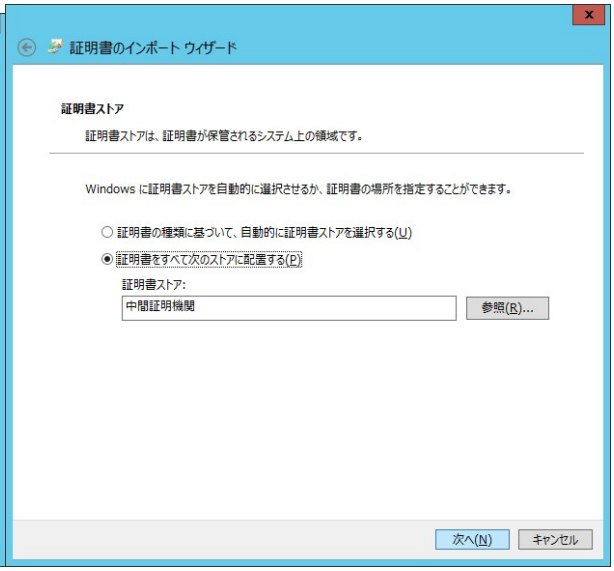


図１５

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「中間証明書」になっていることを確認して、[次へ(N)]を選択します。(図１５)
10. これで、中間証明書を導入することができました。(図１６)

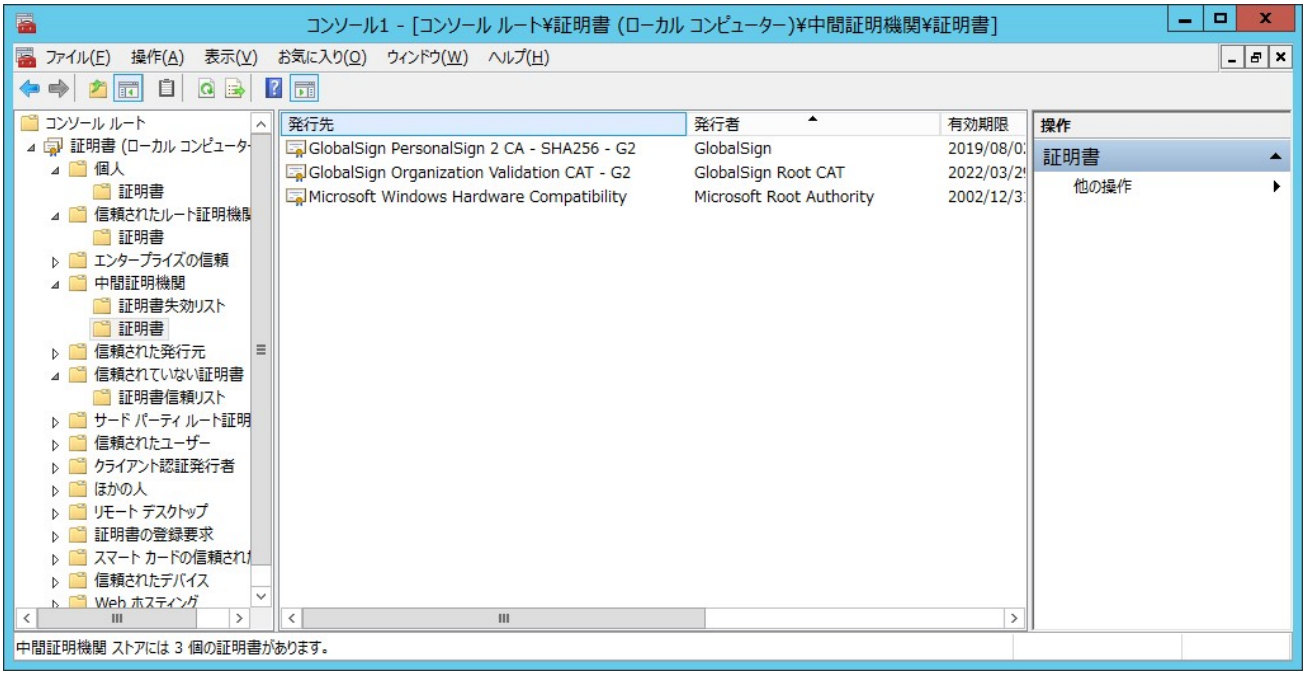


図１６

11. 同様にしてダウンロードしたルート証明書を「信頼されたルート証明機関」の配下の「証明書」にインポートします。

3. 認証局の信頼の設定

ご利用のクライアント証明書以外を信頼しないようにするため、証明書スナップインの「信頼されたルート証明機関」にある利用クライアント証明書に対応するルート証明書と「Microsoft Root Authority」以外のルート証明書を削除することをお勧めします。

4. ルート証明書の自動更新を停止する

1. 前述と同様に Microsoft 管理コンソール(MMC)を起動し、「グループ ポリシー オブジェクト エディター」をスナップインします。(図１７)

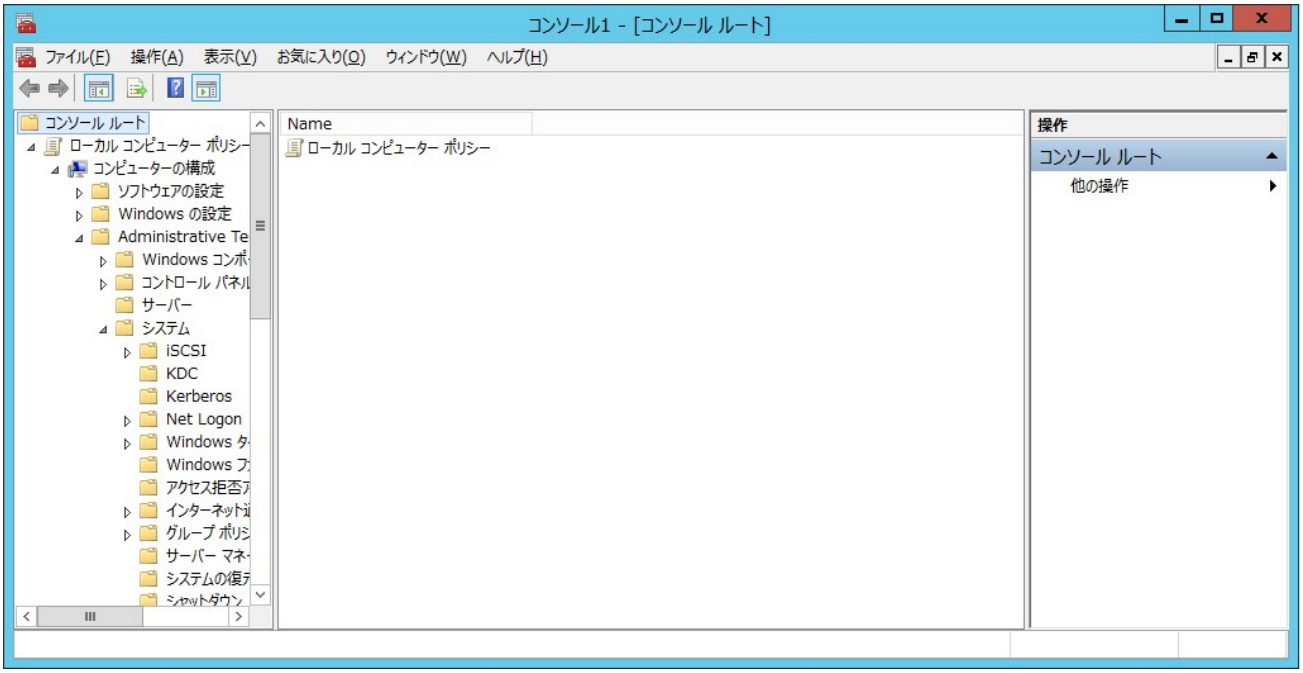


図１７

2. 表示された「ローカル コンピューター ポリシー」から順に"▷"をクリックして、「コンピューターの構成」＞「Administrative Templates (管理用テンプレート)」＞「システム」＞「インターネット通信の管理」＞「インターネット通信の設定」を選択し、「ルート証明書の自動更新をオフにする」の項目を「Enabled(有効)」にします。(図１８)

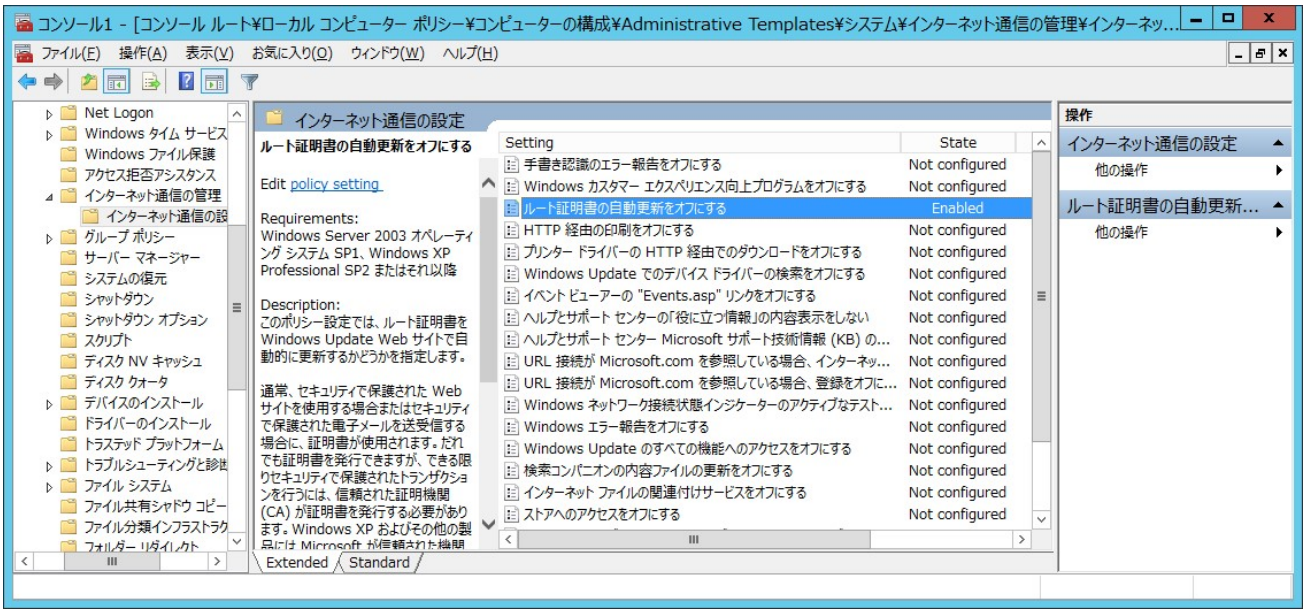


図１８

5. 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。

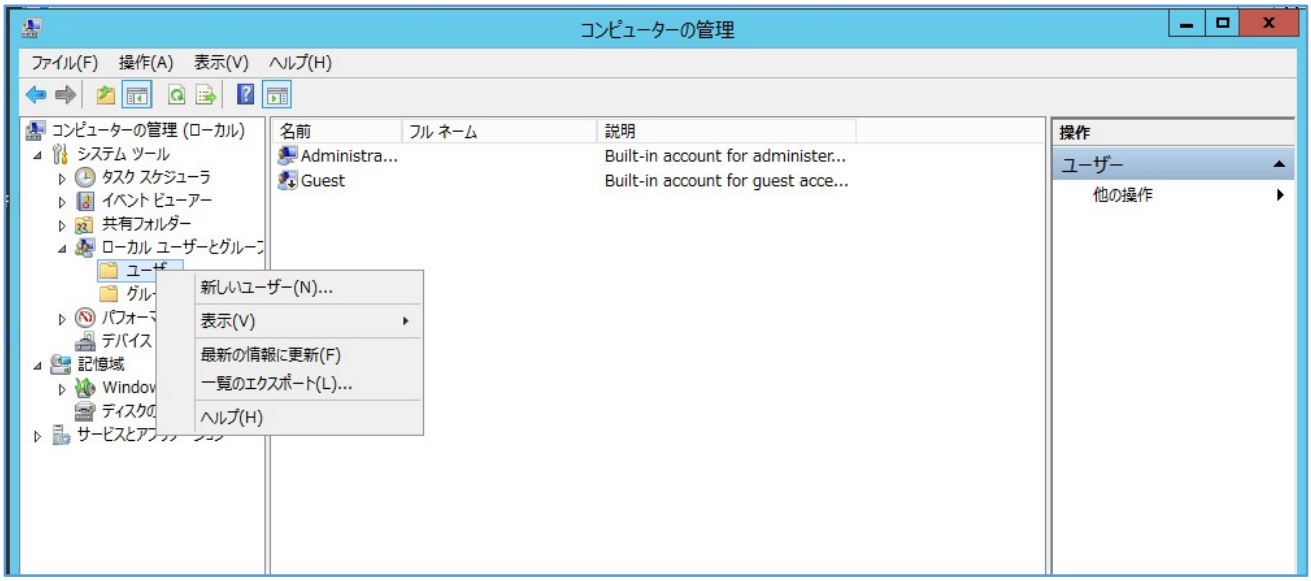
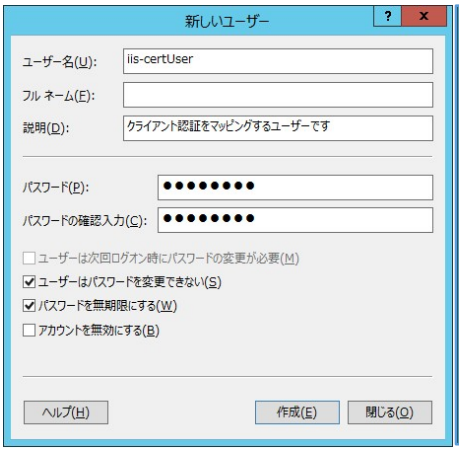


図１９

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、「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。（図１９）



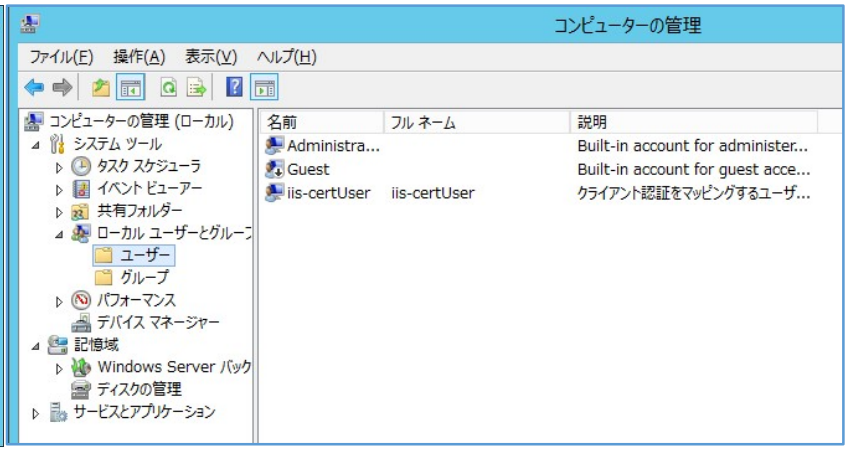


図２０　　図２１

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。(図２０)
[作成(E)]を選択すると、新しいユーザーが追加されました。（図２１）

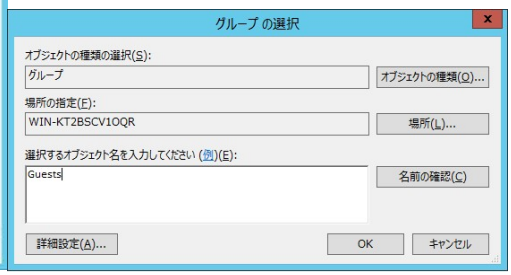


図２２　　図２３　　図２４

作成後、プロパティを確認し(図２２)、「所属するグループ」Users(図２３)で[追加(D)...]を選択して、Guests を追加します。(図２４)Users グループは削除します。

6. 匿名アクセスの無効化

IIS マネージャから「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。(図２５)

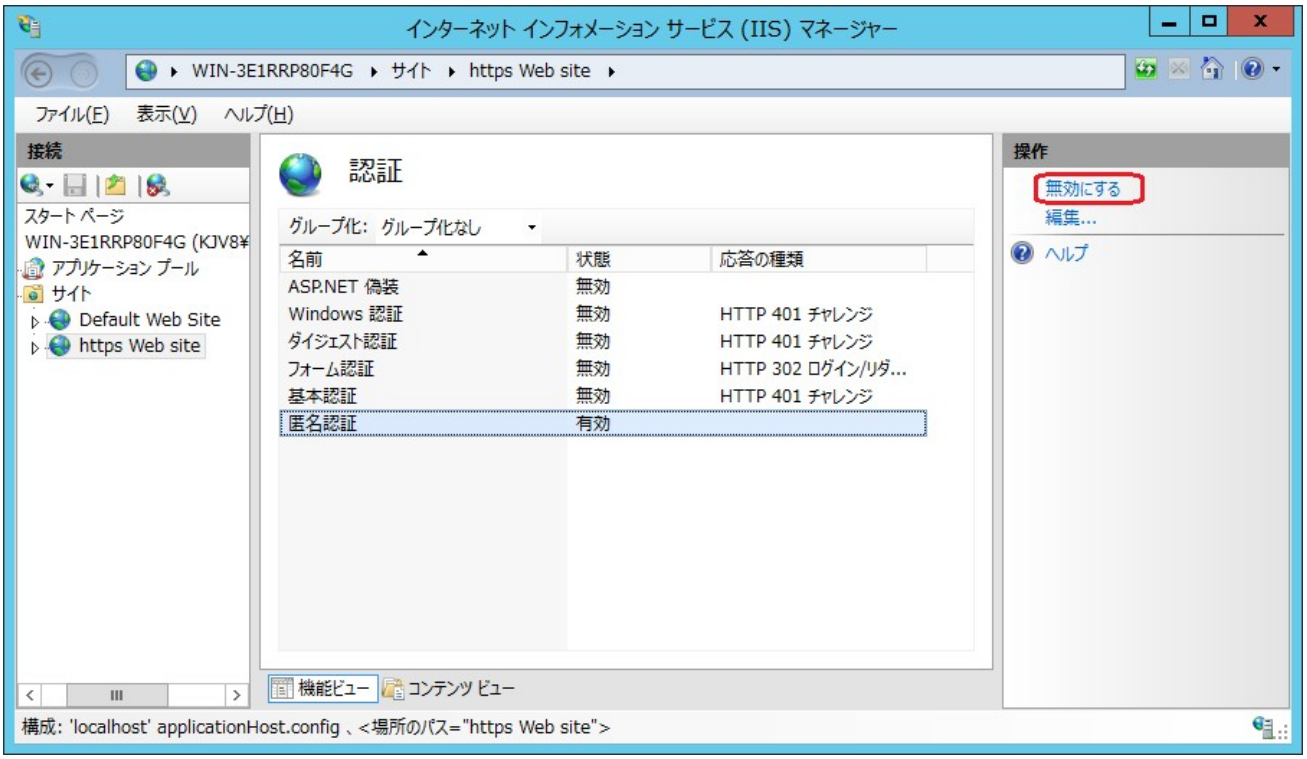


図２５

7. 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。

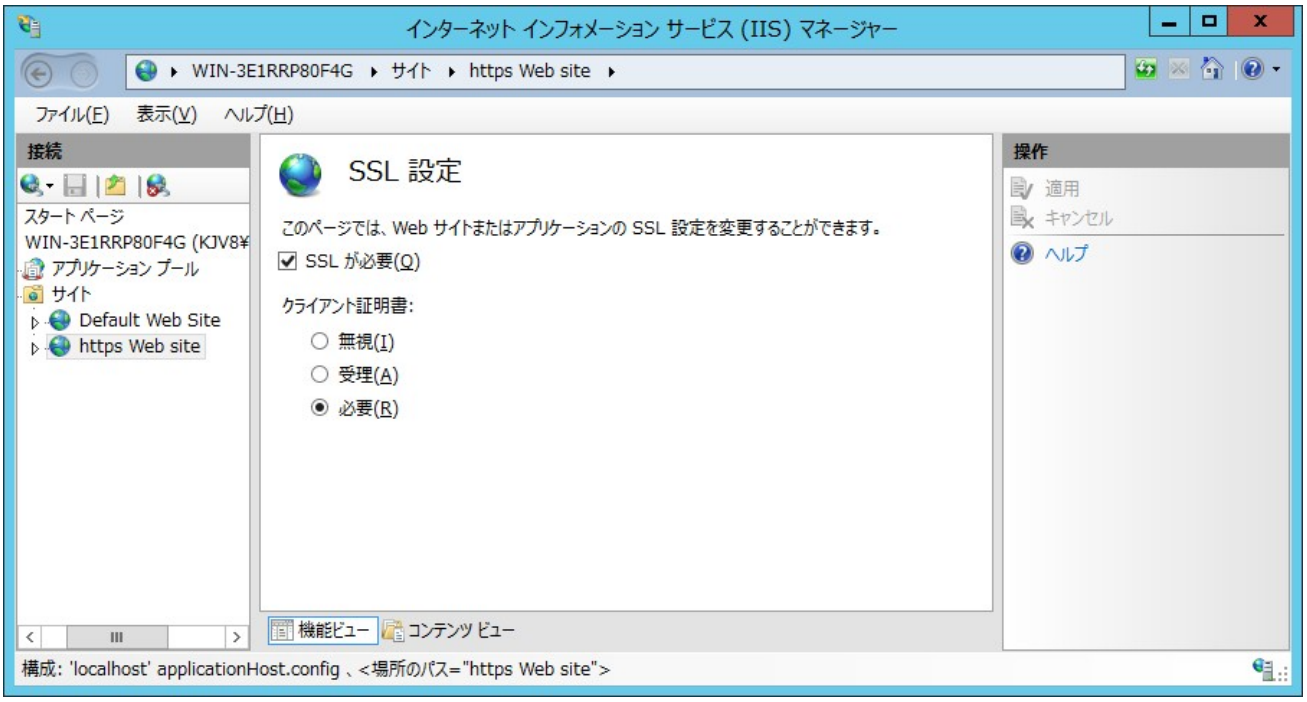


図２６

8. 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ーで認証させるかは基本的な設計で、サーバー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 サーバー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。それぞれについては下記のページを参考にしてください。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。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。

- 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

1. 構成エディターを起動する。
   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。(図２７)

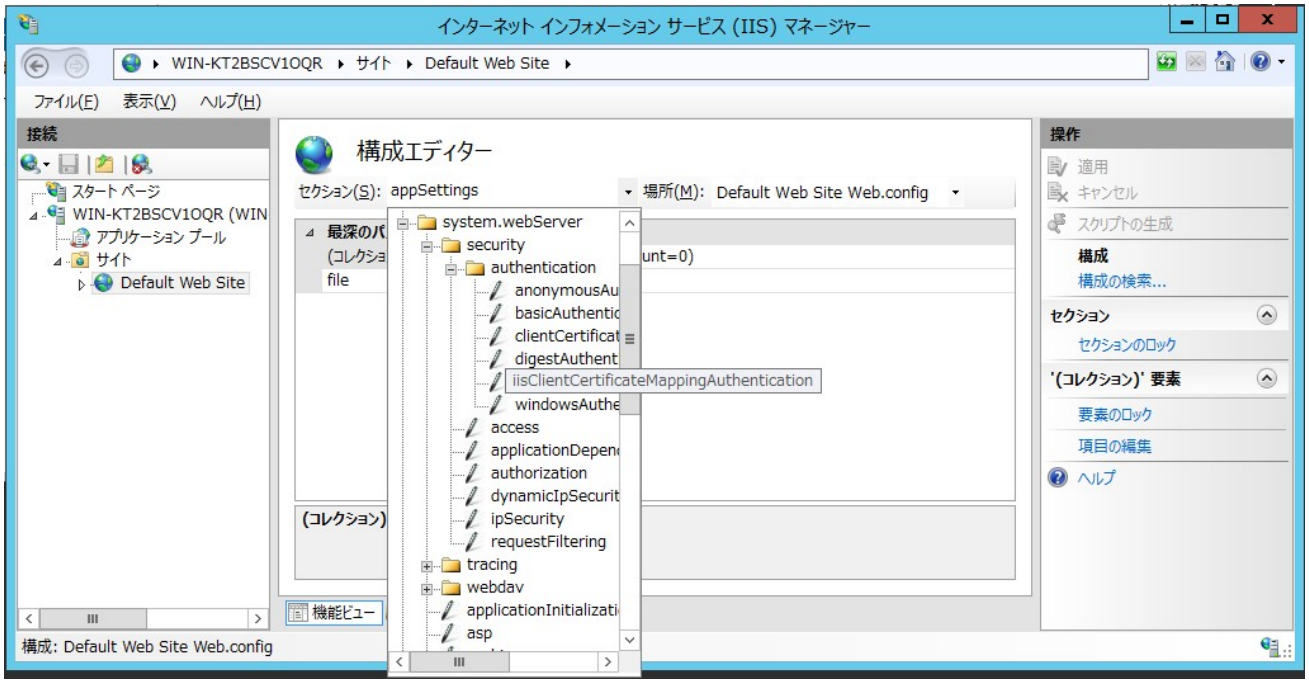


図２７

2. コレクション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設定を行います。図２８のようになります。 enabled: True
   manyToOneCertificateMappingsEnabled: True

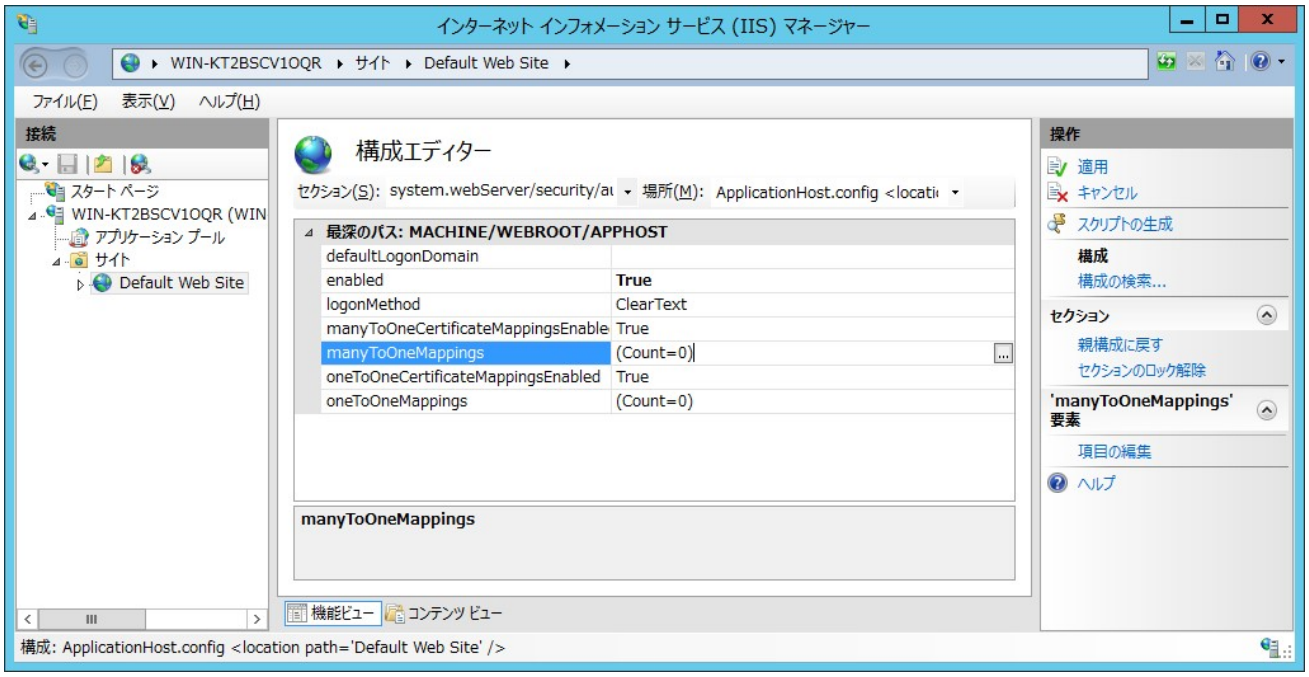


図２８

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コレクション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。図２９のようになります。

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

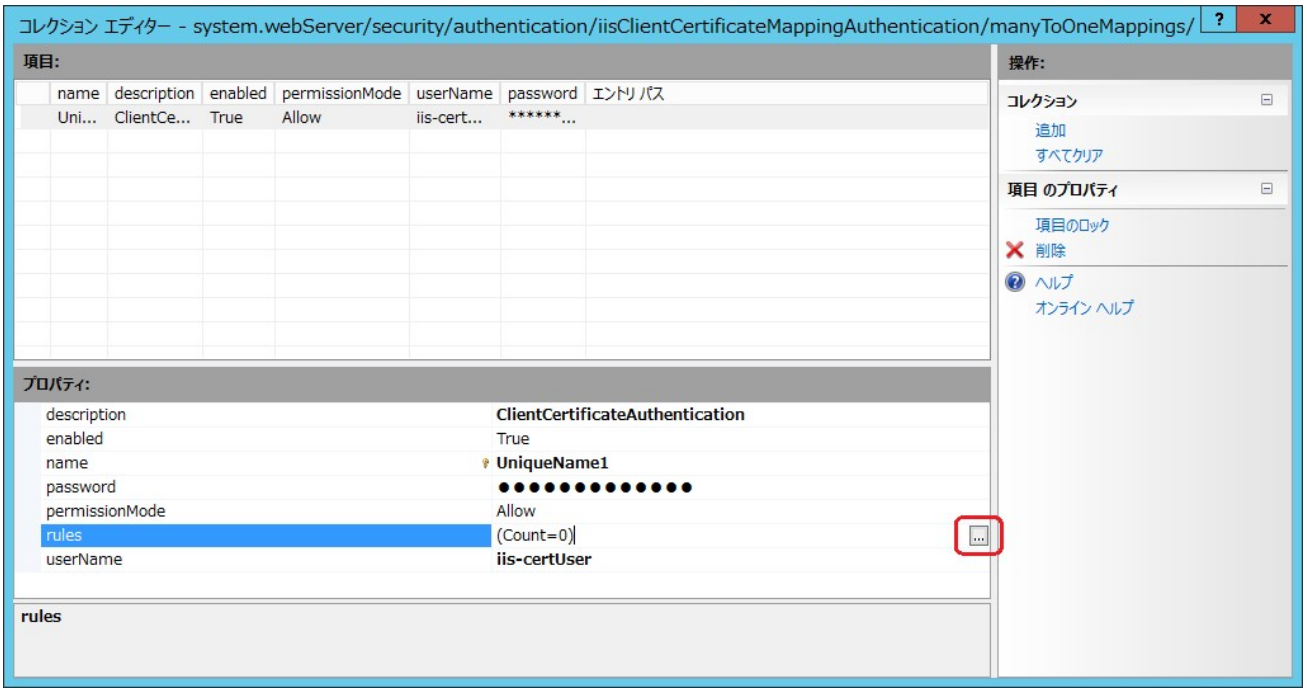


図２９

4. ルールの設定

「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、新たなコレクションエディターが開き、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”GlobalSign K.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。(図 30)

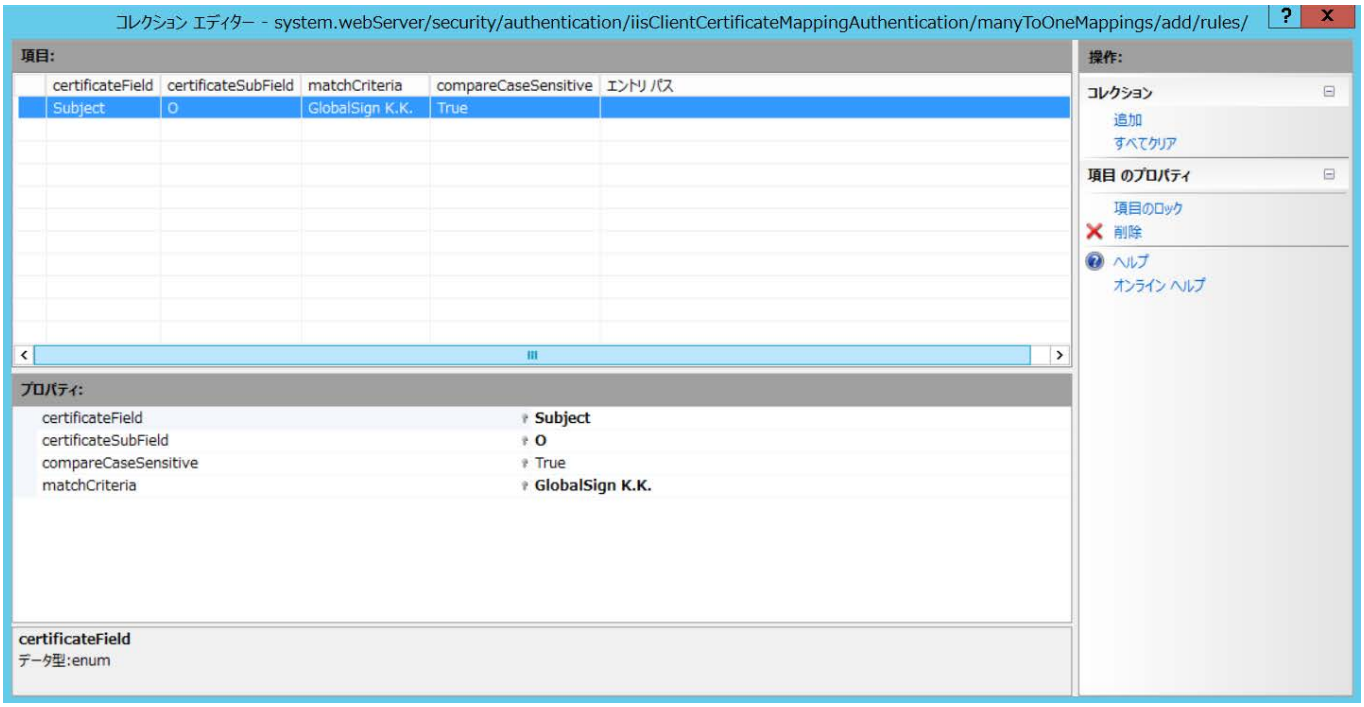


図３０

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。（図３１）

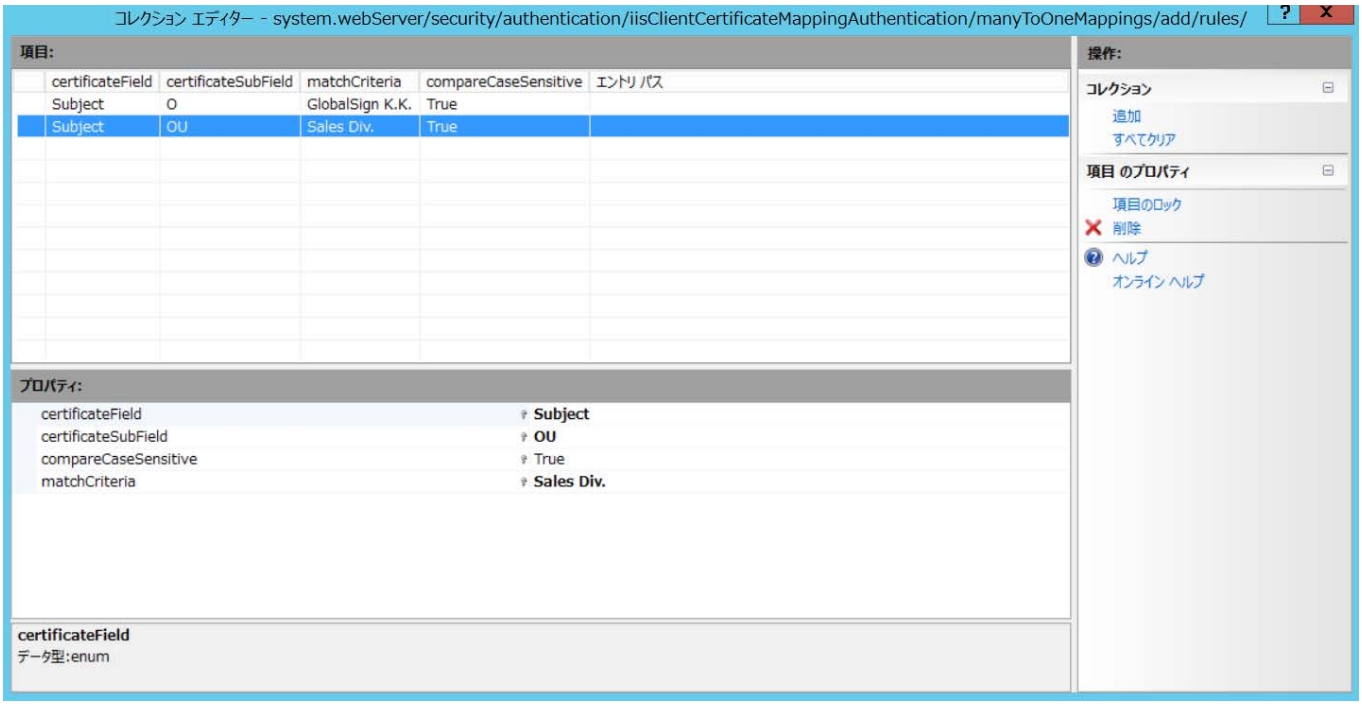


図３１

マッピングの設定が完了すると以下のようになります。（図３２）

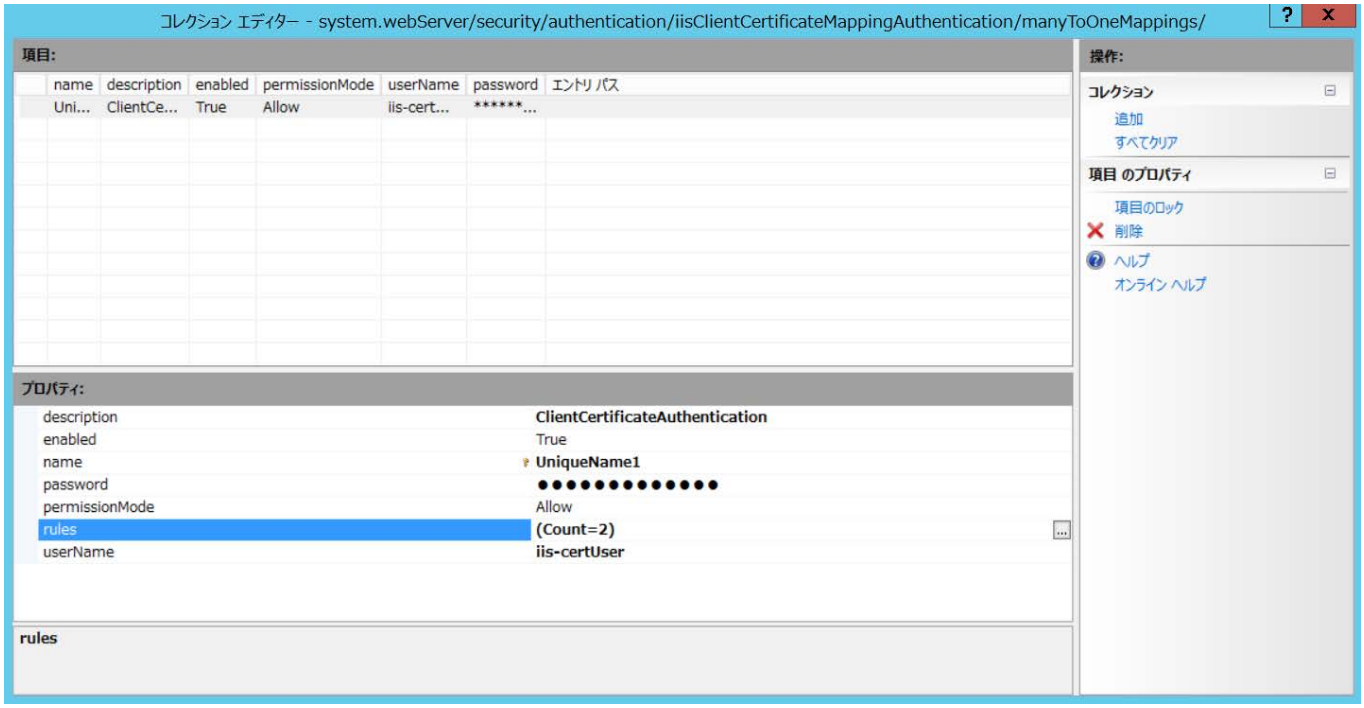


図３２

以上で設定は完了です。サービスのリスタートを行い、適切な証明書を使用して、認証の確認をしてください。