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





# 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。

役割と破綻の追加ウィザード	×	_ 0 X		ーマネージャー	サーバー		5
公理を構成の追加のペゲート     このかが、ド東東市でと、特徴、特徴サービス または特徴をやうストールだき     のなえれると2600年後のシジューアング ニーズに立つて、イウストール下き後載し     での、     のなどの「「「「「「「」」」」」、     なのえたると2600年の「「」」     のないのないので、     ののないのないので、     ののないのないのないので、     ののないのないのないのない。     ののないのないのないのないのない。     ののないのないのないのないのないのない。     ののないのないのないのないのないのない。     ののないのないのないのないのないのないのない。     ののないのないのないのないのないのないのないのないのないのないのないのないのない	<ul> <li>た</li> <li>開始する前に</li> <li>現時であた</li> <li>インストールの理解</li> <li>サーバーの単純</li> <li>サーバーの単純</li> <li>ホロ</li> </ul>	■ ■ ▼ 第項(出) 9-4(1) 第三(0 Ab7(1)	<ul> <li>・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	- マネージャー - カル サーバーの 助と機能の追加 まするサーバーの追加 パー グループの作成 サーバーをクラウド サー *-バーの記録: 1 「「「AD DS ③ 「確認知 イベト サーズ」 パント サーズ」	サーバ・     ダンタンボード     ベムシンズ     シェンズ     シュンズ     シッシュズード     シッシュズード     シッシュズー     シッシュズー     シッシュズー     シッシュズー     シッシュ     シッシュ     シッシュ     シッシュ     シッシュ     シッシュ     シッシュ     ション     シー     シー     シー     ション     シー     ション     ション     ション     ション     ション     シー     ション     シー     シー	マネージヤー ・ ダ リーバー マネージャーへ (つ) (つ) (つ) (つ) (つ) (つ) (つ) (つ) (つ) (つ)	<ul> <li>●</li> <li>●</li></ul>

[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。

開始する前に	選択したサーバーにインストールする役割を1つ以上選択します。	-H00
サーバーの選択 サーバーの役割 機能 確認 結果	Veen     Veen	IIS Client Certificate Mapping Authentication uses client certificates to authenticate users. A client certificate is a digital ID from a trusted source. IIS offers two types of authentication using client certificate mapping. This type uses IIS to offer one-to-one or many-to-one certificate mapping. Native IIS mapping of certificates offers better performance.

「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。

🜇 コンソール1 - [コンソール ルート]			-	ΟX
🔂 ファイル(F) 操作(A) 表示(V) お気に入り(O) ウ	ィンドウ(W) ヘルプ(H)			- 8 ×
(+ - +   💼   🔒 📔 📷				
📔 コンソール ルート	名前	操作		
	このビューに表示する項目はありませ	コンソールル-	-ト	<b>^</b>
		他の操作	作	•

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。

2 どの拡張を有効にするかを構成でき 利用できるスナップイン(S):	5,750000,757,777 !ttp:		選択されたスナップイン(E):		
スナップイン ・ ActiveX 27トロール ● IP セキュリティ ポリシーの音… ● IP セキュリティ モニラー Oracle Instance Manager ■ TPM 管理 ● Web アドレスへのリンク ● Windows Server パックア… ● WMI コントロール ■ イントレビューアー ● インターネット インフオメーシ… ■ グループ ポリシー オブシェク… ■ コンターの音理	ペンダー Microsoft Corp Microsoft Corp	^	通知(A) >	<b>拡張の編集(X)</b> 削除(R) 上へ移動(U) 下へ移動(D)	
・ ジリー・ ネップインを ActiveX コントロール スナップインを	imicrosoft Corp 使うと、ActiveX コン	► ► □-J	しを含む結果とユーがある MMC ノードを追加できます。	ОК <i>+vуvµµ</i>	

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。

スナップインの追加と削除	×
コンビューターで利用できるスナップインからこのコンソールに使用するスナップインを選択したり、選択したスナップインを構成したりできます どの拡張を有効にするかを構成できます。	*。拡張可能なスナップインでは、
利用できるスナップイン(S): 選択されたスナップイン(E):	
スナップイン ベンダー ^ ニュンソール ルート	拡張の編集(X)
🖥 セキュリティの構成と分析 Microsoft Corp	
Ø タスクスケジューラ Microsoft Corp	削除(R)
ディスクの管理 Microsoft and V	
昌 デバイス マネージャー Microsoft Corp	上へ移動(U)
参テレフォニー Microsoft Corp	
N/フォーマンスモニター Microsoft Corp	下へ移動(D)
III フォルダー Microsoft Corp 追加(A) >	
」ポリシーの結果セット Microsoft Corp	
直ルーティングとリモート アクセス Microsoft Corp	
後ローカル バックアップ Microsoft Corp	
●ローカル ユーザーとグループ Microsoft Corp	
減 共有フォルダー Microsoft Corp	
運動 変形 マネージャー Microsoft Corp	
□ 🐺 証明書 Microsoft Corp 🗸	詳細設定(V)
5499.	
証明者ステックインを使うとユーリー、サービス、またはコンビューダーの証明者ストアの内容を閲覧できます。	
	OK thirth
	477 200

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。

証明書スナップイン			Х
このスナップインで管理する証明書:			
〇 ユーザー アカウント(M)			
○ サービス アカウント(S)			
● コンピューター アカウント(C)			
·			
	< 戻る(B)	次へ(N) >	キャンセル

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。

コンピューターの選択	×
このスナップインで管理するコンピューターを選択してください。 このスナップインで管理するコンピューター: ③ ローカル コンピューター(L): (このコンソールを実行しているコンピューター)          ○ 別のコンピューター(A):         □ コマンド ラインから起動したときは選択されたコンピューターを変更できるようにする(W) これは、コンソールを保存した場合にのみ適用されます。	参照(R)
これは、コノノールを体行した物白に切め適用されより。	
< 戻る(B) 完了	キャンセル

[OK]を押して終了すると MMC に証明書が追加されます。

🚟 コンソール1 - [コンソール ルート¥証明書 (ローカル コンピュー)	ワ−)¥クライアント認証発行者]			- 🗆 X
🚟 ファイル(F) 操作(A) 表示(V) お気に入り(O) ウィ	ンドウ(W) ヘルプ(H)			_ & ×
🔶 🎽 📰 📋 🔍 🗟 📝				
<ul> <li></li></ul>	オブジェクトの種類	このビューに表示する項目はありません。	操作           クライアント認 他の操	証発行者 <sup>作</sup> →
<ul> <li>スペート リードの追捕され ビルード</li> <li>信頼されたパッケージ アプリのインストール機関</li> <li>信頼されたデバイス</li> <li>留 Web ホスティング</li> <li>Windows Live ID Token Issuer</li> <li>WindowsServerUpdateServices</li> </ul>				
クライアント認証発行者 ストアには証明書がありません。			1	

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。

■ コンソール1 - 「コンソール ルート¥証明書(ローカル コンピュー)	マー)¥クライアント認証発行者1	– n x
ファイル(F) 操作(A) 表示(V) お気に入り(O) ワイ	ントワ(W) ヘルノ(H)	_ 8 ×
🗢 🔿 📶 📋 🧟 🗟 🥅		
📔 コンソール ルート	オブジェクトの種類	操作
→ 🙀 証明書 (ローカル コンピューター)		クライアント認証発行者
> 🦲 個人	このビューに表示する項目はありません。	体の操作
> 🧰 信頼されたルート証明機関		
> 一 中間証明機関		
>    信根された光11ル		
> ====================================		
◇ □ 信頼されたユーザー		
□ クライアント認証発(		
> 📋 プレビュー ビルドのル 証明書の検索( <u>N</u> )		
> □ テストルート すべてのタスク(K)	> 証明書の検索(N)	
> □ はかの入 > □ リモート デスクトップ 表示(⊻)	> インポート(J)	
> 📔 証明書の登録要求 ここから新しいウィンドウ(	<u>w</u> )	
> ニ スマートカードの信息 新しいタスクパッド表示(	D	
1目視されたデバイフ コード・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		
■ 18/8C1 NC2 / 11/2 最新の情報に更新(F)		
Windows Live ID 一覧のエクスポート(L)…		
> 🦳 WindowsServerU ヘルプ( <u>H</u> )		
証明書をストアに追加します		

7. [すべてのタスク(K)]を選択し、[インポート]を選択します。

「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。

インボートする証明書ファイル インボートするファイルを指定してください。 ファイル名(F): C:¥Program Files¥OpenSSL-Win64¥bin¥2022.sample.cer 注音: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます: Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B) Microsoft シリアル化された証明書ストア (.SST)	
インボートするファイルを指定してください。 ファイル名(F): C:¥Program Files¥OpenSSL-Win64¥bin¥2022.sample.cer 参照(R) 注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます: Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B) Microsoft シリアル化された証明書ストア (.SST)	/ボートする証明書ファイル
ファイル名(F): C:¥Program Files¥OpenSSL-Win64¥bin¥2022.sample.cer 参照(R) 注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます: Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B) Microsoft シリアル化された証明書ストア (.SST)	インボートするファイルを指定してください。
C:¥Program Files¥OpenSSL-Win64¥bin¥2022.sample.cer 参照(R) 注意:次の形式を使うと 1 つのファイルに複数の証明書を保管できます: Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B) Microsoft シリアル化された証明書ストア (.SST)	ファイル名(F):
注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます: Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B) Microsoft シリアル化された証明書ストア (.SST)	C:¥Program Files¥OpenSSL-Win64¥bin¥2022.sample.cer 参照(R)
Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B) Microsoft シリアル化された証明書ストア (.SST)	注意:次の形式を使うと1つのファイルに複数の証明書を保管できます:
Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B) Microsoft シリアル化された証明書ストア (.SST)	Personal Information Exchange- PKCS #12 (.PFX,.P12)
Microsoft シリアル化された証明書ストア (.SST)	Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)
	Microsoft シリアル化された証明書ストア (.SST)

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。

璹 コンソール1 - [コンソール ルート¥証明書 (ローカル コンピュー	·ター)¥クライアント認証発行者¥証明書]			— C	) X
🚟 ファイル(F) 操作(A) 表示(V) お気に入り(O) ウ	ィンドウ(W) ヘルプ(H)				_ 8 ×
🗢 🔿 📶 📋 🖸 🕞 🖬 📷					
🖆 בערב 📩 🔸	発行先 ^	発行者	有効期限	操作	
◇ □ 証明書(ローカル コンピューター)	GlobalSign GCC R3 PersonalSig	GlobalSign	2028/09/16	証明書	-
<ul> <li>ご 信頼されたルート証明機関</li> </ul>				他の操作	•
> 📔 エンタープライズの信頼					
> > 中間証明機関					
>					
> 📔 サードパーティルート証明機関					
> 🧰 信頼されたユーザー					
◇ □ 951 アント認証先11者					
> 📔 プレビュー ビルドのルート					
> 🔛 テストルート					
> 🔜 はかの人 > 🮬 リモート デスクトップ					
> 🧰 証明書の登録要求					
> 🧰 スマートカードの信頼されたルート					
> 信頼されたハッケーシ アノリのインストール機関 を頼されたデバイス					
> 📫 Web ホスティング					
S 🖾 Windows Live ID Token Issuer	<		>		
クライアント認証発行者ストアには1個の証明書があります。				1	

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。

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	ター・ソクライマント 認証 発行 キン証明書1			_	
	フニ/キンプ1 アフド86 証用1] 香辛証明音]			_	
🚟 ファイル(F) 操作(A) 表示(V) お気に入り(O) ウ	ィンドウ(W) ヘルプ(H)				_ & ×
🗢 🔿 🙍 🖬 📋 🖉 📾					
א-עעב 📔 🗠 🔨		発行者	有効期限	操作	
◇ 🗊 証明書 (ローカル コンピューター)	GlobalSign	GlobalSign	2029/03/18	証明書	<b>^</b>
> 🧰 個人	GlobalSign GCC R3 PersonalSig	GlobalSign	2028/09/16	(4の話/を	
> i 信頼されたルート証明機関		3		TEUJIPTE	· · · ·
> 二 エンターフライスの信頼					I
					I
<ul> <li>              ・ 1 信頼されに発行             ・ ごいたい             ・             ・</li></ul>					I
> 1 目積されていない証明者					
> ジー・ハージール 「・					I
> 10 パート・シート 「「「「「「」」」					I
					I
> 🗂 プレビュー ビルドのルート					I
> 📫 テストルート					
> 🔛 ほかの人					I
> 📔 リモート デスクトップ					I
> 🚞 証明書の登録要求					
> 📫 スマートカードの信頼されたルート					I
> 🧰 信頼されたパッケージ アプリのインストール機関					I
> 🧮 信頼されたデバイス					I
> 🔛 Web ホスティンク					
Windows Live ID Token Issuer	<		>		
クライアント認証発行者ストアには2個の証明書があります。				1	

## 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。

æ				コンピューターの管理	_ <b>_</b> X
ファイル(F) 操作(A)	表示(V)	へルプ(H)			
🦛 🔿 🙍 💽	à 🗟  🖬				
🌆 コンピューターの管理	(ローカル)	名前	フルネーム	説明	操作
▲ 🎁 システム ツール		Administr	a	Built-in account for administer	ユーザー 🔺
D 1 イベントビュ	- <i>P</i> -	St Guest		Built-in account for guest acce	他の操作・
▶ 100 共有フォルダ	1_ 10 1 E				
⊿ 28 ローカル ユー	-サーとクルーン				
🦰 グル-	新しいユー	-ザー(N)			
▶ 🔞 パフォーマ	表示(V)		•		
▲ 🤮 記憶域	最新の情報	報に更新(F)			
Windov	一覧のエク	ルスポート(L)			
■ ディスクの	へルプ(H)				
	/-/				

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。

iis-certUserの刀/(ディ ? ×	iis-certUserの刀Uパティ ? ×	1
リモート制御 リモート デスクトップ サービスのプロファイル ダイヤルイン 全般 所属するグループ プロファイル 環境 セッション	リモート制御 リモート デスクトップ サービスのプロファイル ダイヤルイン 全般 所属するヴループ プロファイル 環境 セッション	
iis-certüser	所属するグループ(M):	
フルネーム(E):         Pis-certUser           20時(D):         クライアンド間経をマルビングするユーザーです	2 Gard	
□ユーザーはが回らかっ待ににスラードの変更が必要(M) Øユーザーはバスラードを変更が必要(M) Øノスラードを無時間にする(2)		グループの選択 × オブジェクトの障害の選択(5):
フカウントを思想にする(m) アカウントを思想いずる(m) アカウントのCircleのプロド(Q)		グループ オブシェクトの種類(Q)… 場所の指定(E): WIN #7285()(200P #55(1)
	ユーザーダガルーブ メンパーシップに対する反要 注意(2) 利用(2) 利用(2) となりません。	通訳するオブシュクト名を入力してください(強)(E):         名前の確認(C)
OK         年ウンセル・         (A)         へんプ	OK         キャンセル         通用(点)         へみブ	詳細設定( <u>A</u> ) OK キャンセル

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。

¥_	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	_ <b>_</b> X
€ WIN-3E1	RRP80F4G ・ サイト ・ https	Web site 🔸		😳 📨 🟠 I 🕖 🔹
ファイル(E) 表示(⊻) ヘルフ	f( <u>H</u> )			
接続 ◎、・ 🔒   🖄   😣	(3) 認証	操作 (無効にする)		
スタート ページ WIN-3E1RRP80F4G (KJV8¥	グループ化: グループ化なし	•	and the state of the state	
- ⑦ アフルケーション ブール - ⑦ サイト ▷ ● Default Web Site ▷ ● https Web site	ARNET 偽装 Windows 認証 ダイジェスト認証 フォーム認証 基本認証 国名認証	<ul> <li>(人) 無効</li> <li>無効</li> <li>無効</li> <li>無効</li> <li>無効</li> <li>有効</li> </ul>	HTTP 401 チャレンジ HTTP 401 チャレンジ HTTP 302 ログイン/ソダ HTTP 401 チャレンジ	
< III >	■ 機能ヒュー / コンテンツ ビュー			
構成: 'localhost' applicationHo	ost.config、<場所のパス="https	Web site">		€ <u>∄</u> .:

# 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。

<b>V</b>	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	= <b>-</b> ×
€ WIN-3E	E1RRP80F4G → サイト → https Web site →	🔤 📧 🟠 🔞 🕶
ファイル(E) 表示(⊻) ヘル	ブ(圧)	
接続		操作
<ul> <li>         ・ □   2   8         </li> <li>スタート ページ         WIN-3E1RRP80F4G (KJV8¥     </li> </ul>	このページでは、Web サイトまたはアプリケーションの SSL 設定を変更することができます。	<ul> <li>■ 適用</li> <li>■ キャンセル</li> <li>● ant 7</li> </ul>
@ アブリケーション ブール ● サイト ▷ ● Default Web Site ▷ ● https Web site	<ul> <li>✓ SSL が必要(Q)</li> <li>クライアント証明書:</li> <li>○ 無視(I)</li> <li>○ 受理(A)</li> <li>● 必要(B)</li> </ul>	
		~
構成: 'localhost' application	Host.config 、<場所のパス="https Web site">	el.:

## 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。

<b>\$</b> ]	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	_ <b>D</b> X
€ S WIN-KT2BSCV	10QR ・ サイト ・ Default Web Site ・	😨 🗟 🏠 🔞 •
ファイル(E) 表示(⊻) ヘルプ(出)		
接続	様 成工ディター     なりとしていたり     なのの     なの     なの	<ul> <li>器件</li> <li>③ 適用</li> <li>③ 注かりてかり生成</li> <li>構成の検索</li> <li>セクション ④</li> <li>セクション ④</li> <li>セクション ④</li> <li>マクションのロック</li> <li>'(コレクション)' 要素 ④</li> <li>要素のロック</li> <li>項目の編集</li> <li>④ ヘルプ</li> </ul>
構成: Default Web Site Web.config		€ <u>⊒.:</u>

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

<b>V</b> j	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	_ 0	x
WIN-KT2BSCV	10QR ・サイト ・ Default Web Site ・		🙆 🖂 🟠	• •
ファイル(E) 表示(⊻) ヘルプ( <u>H</u> )				
	<ul> <li>構成エディター</li> <li>セクション(5): system.webServer/security/a</li> <li>最深のパス: MACHINE/WEBROOT/AF defaultLogonDomain enabled logonMethod manyToOneCertificateMappingsEnabled oneToOneCertificateMappingsEnabled oneToOneMappings</li> </ul>	u • 增所( <u>M</u> ): ApplicationHost.config <locati •<br=""><b>PHOST</b> <b>True</b> (ClearText True (Count=0) True (Count=0)</locati>	<ul> <li>操作</li> <li>違用</li> <li>キャンセル</li> <li>インブレの生成</li> <li>構成</li> <li>構成の検索</li> <li>セクション</li> <li>親構成に戻す</li> <li>セクションのロック部除</li> <li>「manyToOneMappings' 要素</li> <li>項目の編集</li> <li>ヘルブ</li> </ul>	
< III > 構成: ApplicationHost.config <locati< td=""><td>職能ビュー Mail コンテンツ ビュー     mon path='Default Web Site' /&gt;</td><td></td><td></td><td>€∃.:</td></locati<>	職能ビュー Mail コンテンツ ビュー     mon path='Default Web Site' />			€∃.:
and a spinor and a				11.::

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

コレク	ב גבפי	エディター - s	ystem.v	webServer/sec	urity/authe	entication	/iisClientCertificateMappingAu	uthentication/manyToC	DneMappings/ ?	-
項目:	:							操作:		
	name Uni	description ClientCe	enabled True	permissionMode Allow	userName iis-cert	password ******	גא נאכד	<b>コレクショ</b> ) 追加 すべて	<b>&gt;</b> פעל	9
								項目のプ	ับパティ เ	Ð
								項目( × 削除	ወወቃク	
עח'ר	( <del>,</del>							דעות 10 קעד 	f インヘルプ	
de	escripti	ion				ClientCertif	icateAuthentication			
er	nabled					True				
na	ame				8	UniqueNan	ne1			
pa	asswor	ď			1					
pe	ermissi	ionMode				Allow				
rı	iles				(	(Count=0)				
US	serNan	ne				iis-certUse	r			
rules	3									

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。

	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		
certificateField	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。		
contificatoSubEiold	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。		
CertificateSubField	証明書の発行者(Issuer)またはサブジェクト(Subject)のいずれかを通します。         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。         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 0、0Uに対して設定します。         照合内容を指定します。		
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。

コレクシ	ション エディター - sys	tem.webServe	r/security/authenticat	ion/iisClientCertificateMappingAuthent	ication/manyToOnel	Mappings/add/rules/	? ×
項目:						操作:	
certificateField certificateSubField ma Subject 0 Glo	matchCriteria GlobalSign K.K.	compareCaseSensitive True	IN UNC	コレクション 追加 すべてクリア		8	
						項目のプロパティ 項目のロック ※ 削除 ※ へいじプ オンライン ヘルプ	
プロパティ: certificateField			r Subject		,		
certificateSubFie compareCaseSer matchCriteria	ld hsitive		₹ O ₹ True ₹ GlobalSi	gn K.K.			
cartificataEiald							
Certificate Field デーク型:enum							

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。

目:	操作:				
certificateField certificateSubField Subject O Subject OU	matchCriteria GlobalSign K.K. Sales Div.	compareCaseSensitive True True	גאן ניאכד	コレクション 追加 すべてクリア	
					項目 のプロパティ
					項目のロック メ 剤除
					● ヘルプ オンライン ヘルプ
コパティ: certificateField			* Subject		
certificateSubFie	ld noithro		+ OU		
matchCriteria	ISICIVE		t Sales D	biv.	
rtificateField					

:						操作:	
name description enabled permissionMode userName Uni ClientCe True Allow iis-cert	userName lis-cert	password	גא ניז בז	<b>コレクション</b> 追加 すべてクリア			
						項目のプロパティ	
						 項目のロック X 削除	
						ペルプ オンライン ヘルプ	
パティ:							
lescription				C	lientCertificateAuthentication		
ame					rue IniqueName1		
assword							
ermission	Mode			F	llow		
ules				(	Count=2)		
omelamo				i	is-certUser		

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。
----	----	----	---	----	----

せイト バインドの編集			?	$\times$		
種類( <b>T):</b> 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):		1				
□ サーハー名表示を要 ✓ TLS 1.3 over TCP 3	:氷する(N) を無効にする(B) □ QUIC を無効にし	,ます(A)				
<ul> <li>□ レガシ TLS を無効にする(G)</li> <li>□ HTTP/2 を無効にします(D)</li> <li>□ OCSP ステープリングを無効にします(S)</li> </ul>						
SSL 証明書(F):		選択(L)	表示(V)			
		ОК	キャンセル			

■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)

Ę			Î
Ę			
Ē			
			~

【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

#### 值: 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。

🏬 レジストリ エディター				_	$\times$
ファイル(F) 編集(E) 表示(V) お気に入り(A)	ヘルプ(H)				
<ul> <li>Print</li> <li>PriorityControl</li> <li>ProductOptions</li> <li>RadioManagement</li> <li>SafeBoot</li> <li>ScEvents</li> <li>ScSiPort</li> <li>SecureBoot</li> <li>SecurePipeServers</li> <li>SecurityProviders</li> <li>SaslProfiles</li> <li>SCHANNEL</li> <li>Ciphers</li> </ul>	▲ 名前 ●)(既定) ●)EventLogging ●)SendTrustedIssu	種類 REG_SZ REG_DWORD REG_DWORD	データ (値の設定なし) 0×00000001(1) 0×00000001(1)		 



### 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 <u>https://jp.globalsign.com</u> (C) GMO GlobalSign K.K. All Rights Reserved.