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:

<u>https://jp.globalsign.com/support/csr/529.html?service=ssl</u>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。



「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/



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。

- 「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 1. 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)

						スナップイ	/ンの違加と削除	×
				コンピューターで利用できるスナック は、どの拡張を有効にするかを構た	プインからこのコンソール 成できます。	こ使用するスナップイ	ンを道訳したり、道訳したスナップインを構成	したりできます。拡張可能なスナップインで
				利用できるスナップイン(5):			道訳されたスナップイン(E):	
				スナップイン	15-5-	^	111 コンソール ルート	535の編集(区)
	コンソール1 - [コンソール ルート]		- • ×	Active Directory Fx	Microsoft Cor	-		前降(医)
イル(F) 操作(A) 表示	i(V) お気に入り(O) りィンドウ	2(W) ∧JLプ(H)	_ 0 ×	Active Directory 1	Microsoft Cor			
	1			ACOVEX J/FU-//	Microsoft Cor			上へ移動(以)
1-4, JI-46	名相	マクジュール車帯する7回時はもりませい	操作 1754-11-11-15	L DNS	Microsoft Cor			下へ時動(D)
				◎ IP セキュリティモニター Mic ALP クライアントの構成 Mic TPM 智理 Mic Windows Server / Sy Mic Windows Server / Sy Mic WMI コントロール Mic II イベント ビューアー Mic EI ALP ビューアー Mic	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	v		詳細設定(火)
				説明: サイトとサービスを表示し、管理し より、エンタープライズ上の Activ	Jます。サイトはトポロジ e Directory ドメイン	と、Active Directo サービスの特定のサ	ny ドメイン サービス レプリケーションに使わ ービスを管理きるようになります。	れるスケジュールを定義します。サービスに
				-				OK キャンセル
		6				図 7	7	

図 7

「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)

	スナップイン	の追加と削除	×		証明書スナップイン	x
コンピューターで利用できなスケップインからこのコンソールに留 は、2023編集制用にするが実現成できます。 利用できるスケップイン(5): スケップイン スケップイン スケップイン プケップイン デケップイン マケッショー Microsoft Cor マケッショー Microsoft Cor マケッショー Microsoft Cor マケッショー フォルダー フォルダー フォルダー Microsoft Cor マケッショー Microsoft Cor マケッショー フォルダー フォルダー フォルダー Microsoft Cor マケッショー フォルダー Microsoft Cor マケッショー フォルダー バータング・シング Microsoft Cor マケッショー フォルダー Microsoft Cor マケッショー フォルダー Microsoft Cor マケッショー バータング・シング Microsoft Cor マケッショー メージク・シング Microsoft Cor マケッショー メージク・シング Microsoft Cor マケッショー メージク・シング Microsoft Cor マケッショー レージクシー Microsoft Cor マケッショー レージ レージ レージ マケッショー メージ マケッショー メージ アイレ マケッショー メージ アイン マケッシー メージ マク・シン マケッシー Microsoft Cor マケッショー メージ マク・シン マク・ メージ アイン マク・ マク・ マク・ マク・ マク・ マク・ マク・ マク・	8月1762/19/14/21 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	○ 国内したり、国内したスナップイン(点): 国内2011とスナップイン(点): □ コンソールルート トアの内容を開解できます。	構成したりできます。転獲可能なスキップインで	このスナップインで管理する証明書: ○ ユーザー アカウント(<u>M</u>) ○ サービス アカウント(<u>S</u>) ④ <u>ロンビューター アカウント(C)</u>	< 戻る(B) 次へ(N) > キャン 1	セル
				図 8		买 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)

コンピューターの選択	スナップインの追加と削除
コンピューターの選択 ス 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(たさい。 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) ③ 別のコンピューター(L): 参照(R) □ 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(M) これは、コンソールを保存した場合にのみ週用されます。	D221-9CHA開できるスサップインがあ2022/9-ルに使用するスサップインを選択したスサップインを選択したりてきます。記述可能なスサップインで は、との認識を物かにするかを構成できます。 HTT できるスサップイン(5): フサップク・ ディススの管理 Microsoft Coc の (754 - 72 X ES-P Microsoft Coc の (754 - 72 X ES-P Microsoft Coc の (754 - 73 X ES-P Microsoft Coc 0
< 戻る(日) 完了 キャンセル	ОК. +17>СЛ.
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。

🖀 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	x
□ ファイル(E) 操作(A) 表示(Y) お気に入り(Q) ウィンドウ(W) ヘルプ(H)	_ & ×
 ▲ コンソール ルート 論理ストア名 ● 個人 ● 信頼されたルート証明機関 ● エンタープライズの信頼 ● 中間証明機関 ● 信頼された光行元 ● 信頼された発行元 ● 信頼された光公い証明書 ● サードパーディールート証明機関 ● 信頼されたユーザー ● クライアント認証発行者 ● ほかの人 ● 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 ● 信頼されたデバイス ● Web ホスティング 	操作 証明書 (ローカル コンピュ ▲ 他の操作 →

- 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。
- 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)

🗟 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)¥中間証明機関¥証明書]								
🧱 ファイノレ(F) 操作(A) 表示(V) お気に入り(O) ウィンドウ(W) ヘノレプ(H)								
📔 コンソール ルート	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 Or	ganization Validation CAT - G2	GlobalSign Root CAT	2022/03/2!	証明書			
▶ ■ 10人 ▲ ● 信頼されたル ト証明機関	Microsoft Win	dows Hardware Compatibility	Microsoft Root Authority	2002/12/3:	他の操作	•		
▷ ○ エンタープライズの信頼								
▲ ● 中間町明機関 ● 証明書失効リスト								
「日本」 すべてのタスク(K) +	インボート(I)						
▷ 1 信頼 ▷ 1 信頼 表示(V)	•							
▶ 2 サート ここから新しいウィ	rンドウ(W)							
▷ □ 信頼	表示(T)							
▶ 🗀 ほかく 最新の情報に更	新(F)							
▶ 🗋 リモー 一覧のエクスポー	٠٢(L)							
▷ 🔤 スマー ヘルプ(H)								
▶ 📔 信頼されたデバイス								
▶ ● Web ホステインク								
		ш						
11日本をフレマに追わりします。						1		

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)

■ 証明書のインポート ウィザード	× ● ● 証明書のインボート ウィザード
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。	延明書ストア 証明書ストアは、証明書が保管されるシステム上の領域です。
ファイル名(E): C:¥Users¥Administrator¥Downloads¥pscacert_v3-2.cer 建意: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)	Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。 () 証明書の種類に基づいて、自動的に証明書ストアを選択する(少) () 証明書をすべて次のストアに配置する(P) 証明書入下7: 中間証明機関 参照(<u>k</u>)
次へ(N) キャンセル	次へ(N) キャンセル

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)

□>ソール1 - [コ>ソール ルート¥証明書 (ローカル コンピューター)¥中間証明機関¥証明書]								
Zァイル(E) 操作(A) 表示(Y) お気に入り(Q) ウィンドウ(W) ヘルプ(H)								
📔 コンソール ルート 📃 🔨	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・	🔄 GlobalSign PersonalSign 2 CA - SHA256 - G2	GlobalSign	2019/08/0:	証明書				
⊿ 🧰 個人	🔄 GlobalSign Organization Validation CAT - G2	GlobalSign Root CAT	2022/03/2!	他の場作				
	🛱 Microsoft Windows Hardware Compatibility	Microsoft Root Authority	2002/12/3:	IB0/3#TF	,			
▲ 11日根(1)レート証明版例								
▶ ■ エンタープライズの信頼								
⊿ 📫 中間証明機関								
📔 証明書失効リスト								
🖺 証明書								
▶ 🧰 信頼された発行元 🛛 🗏								
⊿ 🧰 信頼されていない証明書								
▶ サート ハーナイ ルート証明								
▶ ■ 15根C1 いにユーリー								
ト 🎬 ほかの人								
▶ 📫 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1								
▶ 🧰 信頼されたデバイス								
▶ <u>◎ Web ホスティンガ</u> × < Ⅲ >	<		>					
中間証明機関 ストアには 3 個の証明書が	っ あります。			1				

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)

🖷 בא-עכב] - 11–עכב	_ D X							
福 ファイル(E) 操作(A) 表示(Y) お気に入り(Q) ウィンドウ(W) ヘルプ(H)	_ 8 ×							
Name	操作							
▲ 道 ローカル コンビューター ホリシー 道 ローカル コンビューター ポリシー	コンソール ルート 🔺							
▶ □ ソフトウェアの設定	他の操作・・							
▶ 🧰 Windows の設定								
⊿ G Windows ⊐>d								
▷ □ Vindows J Xi ▷ □ J>h□-ル パネル								
サーバー								
SCSI CC								
🗎 Kerberos								
> 🔛 Net Logon								
▶ Windows 9								
1 アクセス拒否す								
> 🛄 129-7-91								
▶ <u>></u> クループ ポリミ 「 + - バー フネー								
STATE STATE STATE STATE								
ירי¢איעל ≈ 🔁								
	1							

図17

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)

🖀 コンソール1 - [コンソール ルート¥ローカル コンピューター ポリシー¥コンピューターの構成¥Administrative Templates¥システム¥インターネット通信の管理¥インターネッ 💻 🗖 💌									
□ ファイル(E) 操作(A) 表示(V)	37-バル(E) 操作(A) 表示(Y) お気に入り(Q) ウィンドウ(W) ヘルプ(H)								
🗢 🏟 🙇 📰 🗟 🖬 🦻	7								
▷ I Net Logon	□ インターネット通信の設定				操作				
▶ Mindows タイム サービス	ルート証明書の自動更新をオフにする	Setting	State	^	インターネット通信の設定 ▲				
Windows JP1ル保護 アクセス拒否アシスタンス	Edit policy setting	目 手書き認識のエラー報告をオフにする ▲ 目 Windows カスタマー エクスペリエンス向上プログラムをオフにする	Not configured Not configured		他の操作 ▶				
▲ 129-ネット通信の管理		目ルート証明書の自動更新をオフにする	Enabled		ルート証明書の自動更新 ▲				
	Requirements: Windows Server 2003 オペレーティ ング システム SP1, Windows XP Professional SP2 またはそれ以降 Description: このポリシー設定では、ルート証明書を Windows Update Web サイトで目 動的に更新するかとうかを指定します。 通常、セキュリティで保護された、Web サイトを使用する場合またはセキュリティ で保護された電子メールを送受信する 場合に、証明書が使用されます。たれ でも証明書を発行できますが、できる限 りセキュリティで保護されたトランザのショ えを行うには、信頼された証明機関 (CA)が証明書を発行できますが、できる限 ります。Windows XP およびその他の製 品には Microsoft が信頼された地間 Extended Standard	 E HTTP 経由の印刷をオフにする E ブリンタードライバーの HTTP 経由でのダウンロードをオフにする E ブリンタードライバーの HTTP 経由でのダウンロードをオフにする E ゲルントビューアーの "Events.asp" リンクをオフにする E イルントビューアーの "Events.asp" リンクをオフにする E ヘルブとサポート センターの「役に立つ清解しの内容表示をしない E ヘルブとサポート センターの「役に立つ清解しの内容表示をしない E ヘルブとサポート センター Microsoft むの 参照している場合、 センターネッ E URL 接続が Microsoft.com を参照している場合、 センターネッ E URL 接続が Microsoft.com を参照している場合、 登録をオフに… E Windows エラー報告をオフにする E Windows Update のすべての機能へのアクセスをオフにする E 検索コンパニオンの内容アイルの更添をオフにする E ストアへのアクセスをオフにする C 	Not configured Not configured		他の操作 →				
					,				

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 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	_ _ X				
ファイル(F) 操作(A)	ファイル(F) 操作(A) 表示(V) ヘノレプ(H)								
🗢 🄿 🙍 📅 🧕	🗟 🛛								
🜆 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	_	Administ	tra	Built-in account for administer	ユーザー				
▷ (-) タスク スケジュ ▷ (-) タスク スケジュ	-7	💱 Guest		Built-in account for guest acce	他の操作 ▶				
▶ 20 共有フォルダー					100 M 100				
⊿ 🌆 ローカル ユー	ザーとグルーン								
□ ユーザ □ グル・	新しいユー	ษ์–(N)							
▷ 🔞 パフォーマ	表示(V)		•						
- デバイス ・ 🕞 記憶域	最新の情報	報に更新(F)							
≥ Windov	一覧のエク	ヮスポート(L)							
📄 ディスクの	へルプ(H)								
▷ 📷 Ħ-ビスとアン→→	1-1								

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)

	iis-certUserの元バティ ? ×	iis-certUserのプロバティ ? ?	
リモート制御 金般 所	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 賞するグループ プロファイル 道境 セッション	リモート制卵 リモート デスクトップ ワーじスのプロファイル ダイヤルイン 金穀 所属するグループ プロファイル 環境 セッション 所属するグループ(M):	
is-cert	user	A Users	
フル ネーム(E):	lis-certUser		
說明(<u>D</u>):	クライアント認証をマッピングするユーザーです		
□ ユーザーは次回ロ 図 ユーザーは/スク・ 図 パスワードを無期 □ アカウントを局効 □ アカウントのロック1	がわったににフードの変更が必要(M) ドマ変更をない(C) 聴いする(2) にする(B) ドクド(Q)	ユーザーのグループ メンバーシップに対する反映	グループの選択 × オブジェクトの種類の選択(S): グループ グループ オブジェクトの種類(Q) 場所の指定(E): WIN-KT285CV10QR 週泊するオブシェクト&き 入力L ポくたさい (例)(FE): 温前するオブシェクト&き 入力L ポくたさい (例)(FE):
		通加(D) 利用(R) になりません。	Guests 名称の確認(C)
	OK キャンセル 道用(A) ヘルプ	OK キャンセル 道川(点) へルプ	詳細設定(<u>A</u>)
	22	叉 2 3	図24

 $2\ 2$

图 2 4

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)

8										
WIN-3E1	🕞 💿 🔮 、 WIN-3E1RRP80F4G 、 サイト 、 https Web site 🔸									
ファイル(E) 表示(⊻) ヘルブ	ファイル(E) 表示(⊻) ヘルプ(出)									
接続	認証			操作 無効にする						
WIN-3E1RRP80F4G (KJV8¥ ③ アブリケーション ブール ● ● Default Web Site ● ● https Web site	クルーブ化: ケルーブ化なし 名前 ASP.NET 偽装 Windows 認証 ダイジェスト認証 フォーム認証 基本認証 匿名認証	状態 無効 無効 無効 無効 有効	応答の種類 HTTP 401 チャレンジ HTTP 401 チャレンジ HTTP 302 ログイン/リグ HTTP 401 チャレンジ							
構成: 'localhost' applicationHo	ost.config、<場所のパス="https	s Web site">		• <u>1</u> .:						

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。



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 <u>https://technet.microsoft.com/ja-jp/library/ee431606.aspx</u>
- 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)

・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	_ D X
 ・ WIN-KT2BSCV10QR → サイト → Default Web Site → ファイル(E) 表示(Y) ヘルプ(E) 接続 ・ ・ ・	월 ≥ 合 0 •
Constraints of the formation of t	■/ 週用 ■、キャンセル スクリプトの生成 構成の検索 セクション ② セクション) ② (コレクション) 愛素 ③ 要素のロック 項目の編集 ③ ヘルプ
構成: Default Web Site Web.config ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	e _{l.:}

図27

 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

6	インターネット インフォメー	ーション サービス (IIS) マネージャー			x
WIN-KT2BSCV	V10QR ・ サイト ・ Default Web Site ・			🖸 🔤 🙆	• •
ファイル(E) 表示(⊻) ヘルプ(H)					
接続	1#c+		Ħ	₽ / F	
 ● ●<td>(点)、エディター セクション(ら): system.webServer/security/ar</td><td></td><td colspan="2">■ 適用 ■ キャンセル</td>	(点)、エディター セクション(ら): system.webServer/security/ar		■ 適用 ■ キャンセル		
👔 アプリケーション プール	△ 最深のパス: MACHINE/WEBROOT/AP	PHOST	9	「大クリノトの主成	
⊿ · 🔞 サイト ▷ 😜 Default Web Site	enabled		構成 構成の検索		
	logonMethod	ClearText	t	2クション	
	many IoOneCertificateMappingsEnable manyToOneMappings oneToOneCertificateMappingsEnabled	True (Count=0) True		親構成に戻す セクションのロック解除	
	oneToOneMappings (Count=0)	3	manyToOneMappings' 要素	۲	
				項目の編集	
) ハルプ	
	manyToOneMappings				
< III >	🏢 機能ビュー 🎼 コンテンツ ビュー				
構成: ApplicationHost.config <locat< td=""><td>tion path='Default Web Site' /></td><td></td><td></td><td></td><td>•</td></locat<>	tion path='Default Web Site' />				•

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2.0のようにな

「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

							操作:	
name Uni	description ClientCe	enabled True	permissionMode Allow	userName iis-cert	password	גאו עאכד	コレクション 追加 すべてクリア	
							項目 のプロパティ	Ξ
							 項目のロック X 削除	
パティ:							♥ ヘルフ オンライン ヘルプ	
lescripti enabled name	on			- - -	ClientCertif True UniqueNan	icateAuthentication ne1		
asswor	d			1		•••••		
permissi	onMode				Allow			
ules	ne				iis-certUse	r		

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)

コレクション エディター - syste	em.webServer/sec	curity/authenticati	ion/iisClientCertificateMappingAuthentication/manyToOne	Mappings/add/rules/	? X
項目:				操作:	
certificateField certificateSubField t Subject 0	matchCriteria cor GlobalSign K.K. Tru	mpareCaseSensitive Je	דאן האר דער ארצ	コレクション 追加 すべてクリア	Ξ
				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	
< ז'וווּלק: certificateField		₩ ₹ Subject			
certificateSubField compareCaseSensitive matchCriteria		₹ O ₹ True ₹ GlobalSi	gn K.K.		
certificateField データ型:enum					

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)

コレクシ	ション エディター - sys	stem.webServe	r/security/authentica	tion/iisClientCertificateMappingAuthe	entication/manyToOneMapp	pings/add/rules/	X
項目:					操作	P:	
certificateField Subject Subject	certificateSubField O OU	matchCriteria GlobalSign K.K. Sales Div.	compareCaseSensitive True True	גא ניאכד	ישב	ンション 追加 すべてクリア	0
					× 9	項目のロック 削除 ヘルプ オンライン ヘルプ	
プロパティ: certificateField			r Subject	1			
certificateSubFie	ld		P OU				
matchCriteria	Isitive		* Inde * Sales D	iv.			
certificateField データ型:enum							

図31

		עב	クション エ	ディター - system	webServe	/security,	authentication/iisClientCertificateMappingAu	thentication/manyT	oOneMappings/	? X
項	∃:								操作:	
	name Uni	description ClientCe	enabled True	permissionMode Allow	userName lis-cert	password ******	גא נאכד		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 剤除 ヘルプ オンライン ヘルプ 	
プロ	リパティ:									
	descripti enabled name passwor permiss	ion d ionMode				C T U 4 A	lientCertificateAuthentication rue iniqueName1			
	rules userNan	ne				(Count=2) s-certUser			
rul	es									

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。