

~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.2.2 2023 年 2 月

Copyright by JCCH Security Solution Systems Co., Ltd., All Rights reserved

- 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。

Copyright by JCCH Security Solution Systems Co., Ltd., All Rights reserved

目次

1. は	じめに5
1.1.	本書について5
1.2.	本書における環境5
2. サ・	- バ証明書発行とルート CA 証明書のダウンロード6
2.1.	サーバ証明書の発行6
2.1.1.	PKCS#12 形式での発行とダウンロード6
2.1.2.	CSR からの発行とダウンロード10
2.2.	ルート CA 証明書のダウンロード15
3. IIS	の設定16
3.1.	サーバ証明書の登録16
3.1.1.	PKCS#12 のサーバ証明書登録17
3.1.2.	CSR から発行したサーバ証明書の登録19
3.2.	ルート CA 証明書の登録21
3.2.1.	CTL の登録21
3.2.2.	信頼されたルート証明機関への登録 21
3.2.3.	ルート CA 証明書の確認22
3.3.	SSL ポートのバインド23
3.4.	クライアント証明書要求の有効化26
4. 動	乍確認27
5. そ(D他28
5.1.	接続時の「セキュリティ警告」について28
5.2.	失効検証の処理方法について 29
5.3.	失効情報をすぐに反映させたいとき 30
5.4.	失効の確認をしない方法 30
5.5.	ASP.NET(C#)でクライアント証明書の情報を取得する

1. はじめに

1.1.本書について

本書では、弊社製品「プライベート認証局Gléas」で発行したクライアント証明書サーバ 証明書を使用してMicrosoft Internet Information Services (IIS) 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。

- ▶ JS3 プライベート認証局Gléas (バージョン2.2.3)
 ※以後、「Gléas」と記載します
- ➤ Microsoft Windows Server 2022 Internet Information Services 10.0.20348.1 ※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

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. サーバ証明書発行とルート CA 証明書のダウンロード

本章では、後述の IIS の設定で使用するサーバ証明書、ルート CA 証明書について Gléas から発行、取得する手順を記載します。

2.1.サーバ証明書の発行

Gléas ではサーバ証明書を PKCS#12 形式または、IIS で生成した CSR を使用して発行す ることができます。以降にそれぞれの発行手順を記載します。

2.1.1. PKCS#12 形式での発行とダウンロード

Gléas の RA(管理画面)へログインし該当のサーバアカウントの詳細を表示します。 ※サーバアカウントの作成については代理店もしくは弊社へお問い合わせください。

アカウント]>詳細			1	コ認証局 ロログ 回管理者 ロヘル	Ź ₽ ₽ <u>₽₽₽</u> ₽	● サイドバー
アカウント	アカウント				■ <u>一覧に戻る</u>	▶ クイックナビ
	📄 iisdemo.spt-demo.loca	1			■ <u>Fv2</u>	8 ユーザ証明書
Group			10 AN - AR 40		A.	
証明書	2 アカワント情報・・・・・・	■ 改訂履歴	シ クループ情報			
Certificate	▶サーバ	登録日時:2022/12/20 15:04	▶ユーザグループ		■参加	IL LOLINGLONG
PR証デバイス Device	> ステータス:有効		> tal			
テンプレート	▶サーバ属性	最終更新:2022/12/20 15:04 <u>編集</u>	▶ロールグループ		日参加	
Template	> 木スト名:		> サーバ証明書		■削除	保存
アカウント操作						
カウントー覧	★ 証明書発行の履歴 ·····					▶ ドック ま アカウント (0)
録申請者一覧	▶1					<u> ★ 証明書 (0)</u>
カウント新規作成	# シリアル 開始	i 有効期限 ス	テータス 失効日	暗号種別トー	・ケン	
証明書発行		証明書は発行。	されていません。			
アカウント削除	トテンプレート構想					
ドックに入れる						
	種別		必須テンプレート	任意テンプレ	- 1-	
	一艘名(CN)	iisdemo.spt-demo.local				
	組織名(0)	JCCH Security Solution Syst	ems Co., Ltd.			
	ドメインコンボーネント(DC)	local			-	
	1511542541 4151 (50)	sunnort-v2			*	

サーバ属性の「編集」をクリックしホスト名に WEB サービスの FQDN を追加して「保存」 をクリックします。

'カウント」>詳細				証局 002 0管理者 0ヘルブ 002	<u>アウト</u> ● サイドバー
アカウント Account	אַכפֿוויי				<u>創に戻る</u> ▶ クイックナビ
グループ	IISdemo.spt-demo.local			D.	■ マシン証明書
Group	🖢 アカウント情報	▶ 改訂履歴	☞ グループ情報 ······		···
証明書 Certificate	▶サーバ	登録日時:2022/12/20 15:04	▶ユーザグループ	▶参加	☆認証局証明書
R証デバイス Device	> ステータス: 有効		> <i>t</i> al		
テンプレート	▶ サーバ届性	保存取り消し	▶ロールグループ	■参加	
femplate	> ホスト名:		> <u>サーバ証明書</u>		保存
カウント操作					A Parts
ウントー覧	★ 証明書発行の履歴・・・・・・				··· 1 アカウント (0)
申請者一覧	▶1				★証明書(0)
ウント新規作成	# シリアル 開始	有効期限 ス	テータス 天効日	暗号権別 トークン	
明書発行		alloh곱(3.9E1)(ゴロリオせん。		
カウント削除	▶ テンプレート情報 ······				
ックに入れる	▶サブジェクト				
	種別		必須テンプレート	任意テンプレート	
	一般名(CN)	iisdemo.spt-demo.local			
	組織名(0)	JCCH Security Solution Syst	ems Co., Ltd.		
		least			

左ペインの「証明書発行」をクリックします。

ウント]>詳細			1	■認証局 ■ログ ■管理者 ■ヘルズ ■ログ	アウト ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
カウント	アカウント			0 <u></u>	- <u>間に戻る</u> ▶ クイックナビ
ccount	📄 iisdemo.spt-demo.loca				<u>トック 8 ユーザ証明</u>
ルーフ roup					
明書	2 アカワント情報・・・・・・	■ 改訂履歴	シ クルーフ情報		
ertificate	▶サーバ	登録日時:2022/12/20 15:04	▶ユーザグループ	日参加	
証デバイス evice	≥ ステータス:有効		>tal		
シブレート	▶サーバ属性	最終更新: 2022/12/20 15:04 <u>編集</u>	トロールグループ	■参加	
mplate	> ホスト名: iisdemo.spt-demo.local		> <u>サーバ証明書</u>	図削除	保存
ウント操作					5. Durd
ントー覧	★ 証明書発行の履歴 ·····				・ ・ こ こ フカウント (0)
請者一覧	▶1				★証明書(0)
ント新規作成	# シリアル 開始	有効期限 ス・	テータス 失効日	暗号種別 トークン	
書発行		証明書は発行さ	さ れていません。		
ウント削除	▶ テンプレート情報				
クに入れる	N#-787-75				
	種別		必須テンプレート	任意テンプレート	
	一般宅(CN)	iisdemo.spt-demo.local			
	組織名(0)	JCCH Security Solution Syst	ems Co., Ltd.		
	ドリインティザーナンドのの	local			

「発行」をクリックします。

//////////////////////////////////////	明書発行	■ 認証局 ■ 日グ ■ 管理者 ■ ヘルブ ■	<u>ログアウト</u> ●サイドバー
アカウント	7 ກ່ຽንት		<u>一覧に戻る</u> ▶ クイックナビ
Account	🥃 iisdemo.spt-demo.local		
Group			
証明書	★ 証明書発行		
Certificate	この画面では証明書要求の作成を行います。 左側の「サブジェクト」と「属性」の内容で証明書要求を作成します。		THE STREET BEFORE
認証デバイス Device	右側のテンプレートの中から必要なものを選択して「発行」を押してください。		
テンプレート	▶評明書筆行	● 上級者向十	* ;
Template	下記の内容で証明書を発行します。よろしけわば「発行」を押してください。		保存
アカウント撮作			
カウント一覧		<u> </u>	▶ ドック
録申請者一覧	x 41-723 - b1	A 3940-Holert Az = Sudtill L	
カウント新規作成			
·証明書発行	CN=lisdemo.spi-demo.tocal Cn=lisdemo.spi-demo.tocal Cn=lisdemo.spi-demo.tocal	> 必須 デンオルPisz正 > 必須 サーバ部理素	
	> DC=local, support-v2	Comp name	
		▶選択可能なテンプレート	
	▶聶性	>なし	
	> 発行局:Support-v2		
	> 暗号アルゴリズム:RSA暗号		
	> 總長: 2048bit		

ステータスが発行依頼中となり、5分程で証明書が発行されます。

※画面の自動更新は行われないので時折画面更新などを行ってください。

 ○作業名: タスク13287 ○管理者: システム管 	<u>74</u> 理 <u>者</u>					プライベートCA	Gléäs	RA
[アカウント]>詳細					<u>ログ 回管理者</u>	■ <u>ヘルブ</u> ■ログアウト	O サイドバー	
アカウント Account	アカウント		_	_	_	□ <u>一覧に戻</u> る	> クイックナビ	۰.
ミ グループ	iisdemo.spt-demo.local					■Ev2	■ マシン証明書	
Group	🖢 アカウント情報・・・・・・・・	■改訂履歴	🖗 グルーフ	「情報・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		••••••	🗐 サーバ証明書	
Certificate	▶サーバ	登錄日時:2022/12/20 15:04	トユーザグル	ーブ		■参加	金 認証局証明書	
SEEデバイス Device	> ステータス:有効		> なし					
テンプレート	▶サーバ属性 最終	更新:2022/12/20 15:04 福集	▶ロールグル	ープ		■参加		
Template	> ホスト名:iisdemo.spt-demo.local		> <u>サーバ語明</u>	畫			保存	
●アカウント操作							▶ ドック	
アカウント一覧	東証明書発行の履歴・・・・・・						<u>まアカウント (0)</u>	-
登録申請者一覧	► 1 <u>Support-v2</u>					100 200 10070	★証明書_(0)	
アカウント新規作成		1908時後 ステータス	大知日	1日本(世方)	化红胡	164PHAJIL		
▶証明書発行	~1	3611183864		1582046(5118250)				
▶アカウント削除	▶ テンプレート情報 · · · · · · ·							
トックに入れる	▶サブジェクト							
	種別		必須テンプレート		任意	テンプレート		
	一般名(CN)	iisdemo.spt-demo.local						
	組織名(0)	JCCH Security Solution Sys	tems Co., Ltd.					
	ドメインコンボーネント(DC)	local support-v2						
操作問題 ブライベートCA Gié	25			Copyri	aht (C) 2010-2020 .	JCCH Security Solution Syst	ems Co. Ltd. All rights re	eserved.

証明書発行後に証明書をクリックして証明書詳細を開きます。

·管理者: <u>システム管理</u>	<u>理者</u>					AV-LCA	Gicas
アカウント]>詳細				■認証局 ■ログ		ルブ ロログアウト	●サイドバー
アカウント	アカウント					▶─前に戻る	る ▶ クイックナビ
Account	📄 iisdemo.spt-demo.loca	l i i i i i i i i i i i i i i i i i i i				■Ev2	<u>8 ユーザ証明書</u>
Group						-	
▲ 証明書	▶ アカウント情報・・・・・・	▶ 改訂風歴	を クルーフ情報				■ <u>サーバ証明書</u>
Certificate	▶サーバ	登録日時:2022/12/20 15:04	▶ユーザグループ			■参加	1211月11月末
認証デバイス Device	≥ ステータス:有効		>なし				
テンプレート	▶サーバ属性	最終更新:2022/12/20 15:04 編集	トロールグループ			n ætu	
Template	> 市スト名: iisdemo.spt-demo.local		いサーバに相思				保存
アカウント操作			· <u>· · · · · · · · · · · · · · · · · · </u>				
アカウントー覧	★ 証明書発行の履歴・・・・・						 ドック アカウレト (0)
1録申請者一覧	► 1 Support-v2						★証明書(0)
アカウント新規作成	# >บารน	開始有効期限	ステータス 失効日	暗号種別	秘密鍵	格納状況	
缸明書発行	<pre></pre>	2022/12/20 2025/12/20	有効	rsa2048(sha256)	•		
アカウント削除	▶ テンプレート情報						
ドックに入れる							
	種別		必須テンプレート		任意テンプ	∠ − ト	
	一般名(CN)	iisdemo.spt-demo.local					
	組織名(0)	JCCH Security Solution Sys	tems Co., Ltd.				
	ドッインコンボーネント(DC)	local					
	13.13 431 431 (30)	sunnort-v2	_		_		

「ダウンロード」をクリックし、表示されたダイアログでパスワードを入力して PKCS#12 形式の証明書をダウンロードします。

 ●作葉名: <u>タスク13287</u> ●管理者: <u>システム管理</u> 	7 <u>4</u> 理査 プライベートC	🗛 Gléås 🖪
[証明書]>詳細	◎湖荘局 ◎旦グ ◎管理者 ◎ヘルブ ◎旦グマ	한 (
アカウント Account そのup	2明書 미二組 Support-v2 CA#1080 미드2	□戻る ▶ クイックナビ 2 <u>8 ユーザ証明書</u> ■ <u>マンン証明書</u>
★ 証明書 Certificate	★ 証明書情報 ▶ <u>isdemo.spt.demo.local</u> ■ <u>isdemo.spt.demo.local</u> ■ <u>isdemo.spt.demo.local</u> ■ <u>isdemo.spt.demo.local</u> ■ <u>isdemo.spt.demo.local</u> ■ <u>isdemo.spt.demo.local</u>	 ■ サーバ証明書 ☆認証局証明書
SET	▶ サブジェクト	
テンプレート Template	>一統名:iisdemo.spt-demo.local >/作成日: 2022/12/20 15:20 >利効日数: 1006 >ドぶくつニンパーモンナ: 10cal >ドスペーロンパーモンナ: 10cal > 大知日:	保存
 証明書操作 証明書一覧 	>ドメインコンボーネント:support-v2 >失効理由:	▶ ドック
▶失効処理 ▶停止処理	> MPSR47 E1 E1 > 状態: 有効な証明書 > 処理の状態: 有効な証明書 > トークン必要:	<u>* 271ワント(0)</u> ★ 証明書(0)
▶ 秘密鍵の削除 ▶ドックに入れる	>)/i−ジョン: 4	
	▶ 証明法 新聞 > I認証局: <u>Supportv2 CA</u> > 培告アルニリズム::sa > ダイジェストアル・コリズム::sha256 > 建長: 2048 > 總用途: <u>電子墨名 線の短号化</u>	•
<u>操作履歴</u> プライベートCA Gléa	as Copyright (C) 2010-2020 JCCH Security Solution	Systems Co.,Ltd. All rights reserved.
	証明書を保護するためのバスワードを入力してください。 パスワードの入力 パスワード ···· ダウンロード キャンセル	

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

2.1.2. CSR からの発行とダウンロード

CSR からサーバ証明書を発行する際は IIS にて CSR を生成し、それを使用し Gléas から 発行します。

IIS を起動し左側ツリーの「サーバ名」をクリックし、「サーバ証明書」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。

💐 インターネット インフォメーション サービス	(ⅢS) マネージャー	- 🗆 X
← → ¶ → SPT-WIN2022	•	😰 🛛 🟠 🔞 •
ファイル(F) 表示(V) ヘルプ(H)		
接続 Image: Second state of the second sta	SPT-WIN2022 ホーム アイルター: * 検索(G) ・ ・ すべて表示(A) グループ化: IIS HTTP 応答ヘッダー MIME の理頭 エラーページ デイルクトリの参照 ハンドラーマッピング モ編 既定のドキュメント 出力キャッシュ 設証 要求フィルター 管理 *	操作 機能を開く サーバーの管理 再起動 開始 停止 アブリケーション ブールの表示 サイトの表示 新しい Web Platform コンボーネン トの取得 ヘルブ
準備完了		• .

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。

🍓 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			- 🗆 ×
←→ SPT-WIN2022	•			😰 🛛 🟠 🔞 🗸
ファイル(F) 表示(V) ヘルプ(H)				
接続	サーバー証明書 SSL に対して構成された Web サイトで の機能を使用します。	₹Webサーバーが使用できる証明書を	要求および管理するには、こ	操作 インボート 証明音の要求の作成 証明音の要求の完了
	フィルター:	🧊 検索(G) 🕞 🙀 すべて表示(A)	クループ化:	ドメイン証明書の作成
	名前 <	発行先	発行元	自己署名入り延明書の作成 更新された証明書の自動的な再 パインドを有効にする ② ヘルプ
< >>	□□□ 機能ビュー			
平備元了				S

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。

証明書の要求		?	×
識別名プロパティ			
証明書に必要な情報を指定します 用しないでください。	。都道府県および市区町村に闘する情報は、公式名称を指定してください。省略形	は使	
一般名(M):	iisdemo.spt-demo.local		
組織(O):	JCCH Security Solution Systems		
組織単位 (OU)(U):	Support		
市区町村(L)	Arakawa		
都道府県(S):	Tokyo		
国/地域(R):	~ 9t		
	前に戻る(P) 次へ(N) 終了(F)	キャンセル	

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」をクリックします。 ※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。

証明書の要求	?	×
晴号化サービス プロパイダーのプロパティ		
暗号化サービスプロバイダーおよびビット長を指定します。暗号化キーのビット長は、証明書の暗号化の強度を決定しま ット長が大きいほどセキュリティは高くなりますが、パフォーマンスが低下する可能性があります。 暗号化サービスプロバイダー(S):	t.Ľ	
Microsoft KSA Schannel Cryptographic Provider		
2048		
前に戻る(P) 次へ(N) 終了(F)	キャンセノ	ŀ

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。

証明書の要求	? ×
ファイル名	
証明巻の要求のファイル名を指定してください。この情報は署名のために証明機関に送信される可能性があります。 証明巻の要求ファイル名を指定してください(R):	
C:¥Users¥Administrator¥Desktop¥iisdemo.csr.txt	
前に戻3(P) 次へ(N) 終了(F)	キャンセル

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

Gléas の RA(管理画面)にログインして前手順でダウンロードした CSR からサーバ証明 書を発行します。

該当のサーバアカウントの詳細を開き「証明書発行」をクリックします。

※サーバアカウントの作成と証明書の発行については代理店または弊社へお問い合わせください。

○作業名: <u>タスク1489</u> ○管理者: <u>システム管</u>	<u>65</u> 理者			プライベートCA (Gléå's 🔼
[アカウント]>詳細			■ 認証局 ■ □ 2 ■ 2	理者 🏽 ヘルブ 🖬 ログアウト	O #4 FM- □
アカウント	アカウント (全 2件中 2件目)				▶ クイックナビ
Account	📄 iisdemo.spt-demo.local			■前 ■E22	<u> 오-ザ証明表</u>
Group				A	
🐞 証明書	2 アガリンド情報	図改訂履歴	シジルーノ情報		● 沙耳局詳細束
Certificate	トサーバ	登錄日時:2022/12/20 15:04	▶ ユーザクループ	■ 200	The second second second
認証デバイス Device	> ステータス: 有効		> なし		
テンプレート	▶サーバ腐性 弱	終更新:2022/12/20 15:04 編集	▶ロールグループ	■参加	
Template	> 木スト名: lisdemo.spt-demo.local		> <u>サーバ証明書</u>		保存
●アカウント操作					
アカウント一覧	★ 証明書発行の履歴 ······				▶ ドック 素 アカウント (0)
登録申請者一覧	►1 Support.v2			• 1919	★証明書 (2)
アカウント新規作成	# シリアル 開始	有効期限 ステータス	失効日 暗号種別 秘密鍵	格纳状况	Support-v2 CA#1080 Support-v2 CA#1087
▶証明書発行	▶ テンプレート情報 ·······				
L'un die 3 de 7	▶サブジェクト				
PPOPLARD	種別		必須テンプレート 行	E意テンプレート	
	一般名(CN)	iisdemo.spt-demo.local			
	組織名(O)	JCCH Security Solution Syste	ms Co., Ltd.		
	ドメインコンポーネント(DC)	local support-v2			
	► B5 #				
操作原度 プライベートCA Gir	695		Copyright (C) 2010-	2020 JCCH Security Solution System	ns Co.,Ltd. All rights reserved.

証明書詳細の「上級者向け設定」を開き「ファイルの選択」から CSR ファイルを指定し「発行」をクリックします。

※「CSR ファイルの内容を確認する」をチェックすると証明書発行操作後に CSR の内容を表示します。

 0作業名: <u>タスク14896</u> 0管理者: システム管 	<u>65</u> 理 <u>者</u>		プライベートCA	Gléås 🖪
[アカウント]>証明	書発行	c	3221日 ロログ ロ管理者 ロヘルブ ロログアウト	О #4 КЛ-
アカウント Account	プリシンド 『 iddemo.spt-demo.local iddemo.spt-demo.local // // // // // iddemo.spt-demo.local // //	防護統計でしません。 難行	O_HUEX OKOHUSE OKOHUSE	 ▶ ダイマクナビ ● ゴンズ目りま ● ゴンズ目りま ● ゴンズ目りま ● ゴンズ目りま ● ゴンバ目りま ● ゴンバ目りま ● ゴンバ目りま ● ゴンバ目りま ● ゴンバ目のま ● ゴンバーのま ● ゴンバー
▶臣時重発行	▶ サブジェクト > CN-lisdemo apt-demo local > 0=JCCH Security Solution Systems Co., Ltd. > DC-local, support-v2 ▶ 話社 > 解す方 (: Support-v2 > 培育アル-ジリズム :: RSAW書う		02068	Support-vz.Coartosr
操作服歴 ブライベートCA Gié	ias		Copyright (C) 2010-2020 JCCH Security Solution Syst	ems Co.,Ltd. All rights reserved.

「CSR ファイルの内容を確認する」をチェックした場合は CSR の詳細が表示されますので「この内容で発行する」をクリックします。

 ●作業名: タスク14896 ●管理者: システム管理 	5 星截	7774-1CA	Gléå's 🔼
[アカウント]>発行			O#4F//- □
アカウント Account ジループ Group 筆 証明書	■ Hisdemo.spt-demo.local 証明書要求(CSR)の確認 Cart Ficiate Resat: Data:	□ 二 知に戻る □ 土ヤンセル □ この内容で発行する	 > クイックナビ ③ ユーザ証明書 ■ マンン証明書 ■ サーバ証明書 ● サーバ証明書
Continicate ごをついていていていていていていていていていていていていていていていていていていて	Version: 0 (6.0) Dataciet (7.0) Dataciet (7.0) Dataciet (7.0) Dataciet (7.0) Philic How Alexen the realizery time Philic How Alexen the realizery time Philic How Alexen the realizery time Realizer Realizer (7.0) Realizer (7.0)	spt-deno, local	
	berdiar(1992)75:30-264 (2017)26-424 (2017)26-424 (2017) Bisalbicechedes(2017)27:303 (2016)31(3015)31(2016) Bisalbicechedes(2017)27:303 (2016)31(3015)31(2016) Bisalbicechede(2016)11(302)74(2016)31(3016) fibisal(2016)31(2016)31(3016)31(3016) fibisal(2016)31(2016)32(2016)32(2016)31(3016) fibisal(2016)31(2016)32(2016)32(2016)32(2016) Exponent: 50557 (2016)31(2016)32(2016)32(2016) Exponent: 50557 (2016)31(2016)32(2016)32(2016) Exponent: 50557 (2016)32(2016)32(2016)32(2016) Exponent: 50557 (2016)32(2016)32(2016)32(2016)32(2016) Exponent: 50557 (2016)32(2006)32(2006)32(2006)32(2006)32(2006)32(20		
操作履歴 プライベートCA Gié	25	Copyright (C) 2010-2020 JCCH Security Solution System	s Co.,Ltd. All rights reserved.

ステータスが発行依頼中となり、5分程で証明書が発行されます。

※画面の自動更新は行われないので時折画面更新などを行ってください。

adapted at 1					
プワント」>詳細				局 国ログ 国管理者 国本ルゼ 国ログス	マウト ●サイドバー
アカウント Account	アカウント (全 2件中 2件目)			D <u></u> 텂	に戻る ▶ クイックナビ
ガループ	iisdemo.spt-demo.local			Dii De	22 8 1-Jacoba
Group	● アカウント情報	网络打探乐	ち グループ情報		
証明書 Certificate		◎ - X61 A212	アフーボグループ	D & to	☆ 認証局証明書
課証デバイス	シフテータフ・有効	2380-011010101010-0		6224	
Device					
テンプレート Template	▶サーバ兩性	最終更新:2022/12/20 15:04 編集	▶ロールグループ	日参加	
	> 木スト名: iisdemo.spt-demo.local		> <u>サーバ証明書</u>	図記録	保存
アカウント操作	素可限素数にの原葉				▶ ドック
カウントー覧	★証明音先行の履歴			-	▲ アカウント_(0)
日本 日	▶1 <u>Support-V2</u> # S/Jアル RBH	- 有効調明	牛奶日 時長知知	+ 1813	★ 証明書(2) Support-v2 CA#1
印刷書発行	A 3	発行依赖中	rsa2048(sha256)		Support-v2 CA#1
アカウント削除					
「ックに入れる	▶ テンプレート情報 ······				
	▶サブジェクト (450)				
	(型5-1 一款名(CM)	iisdemo snt-demo local	心須ナノフレート	は息ナノフレート	
	相應名(O)	JCCH Security Solution Syste	ems Co., Ltd.		
	ドメインコンボーキント(DC)	local support-v2			

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

証明書発行後に証明書をクリックして証明書詳細を開きます。

りウント]>詳細								2 🛛 管理者 🕻	コヘルゴ ロログアウト	0 #4ドバー
アカウント	7カウント (全	2件中2件目)							日一間に戻	後 ▶ クイックナビ
Account	📄 iisde	mo.spt-demo.local							■煎 ■Ev2	8 ユーザ証明書
クルーフ Group		いた構成			10 AL					
证明書	2 F 755		244		0.01				FE 41 12	★ 2015月11月ま
日子バイフ	>7=-0	つ . 左か	22.34	304,2022/12/20 15:04	s tal.	-9-910-9			64 5220	
wice	7.01-2	A • 1820			2.00					
シブレート	▶サーバ8	勇性	最終更新:2	2022/12/20 15:04 🧱	▶□-	ルグループ			■参加	
	> ホスト名	: iisdemo.spt-demo.local			> 11 -	/ 1999書			図前期金	保存
ウント操作	4. er og e									▶ ドック
	* ELPHE	言先1107痕症							0000	2 アカウント(0)
「調査」見	# Supp	<u>シリアル</u>	開始	有効期限	ステータス	失幼日	暗号種別	16238	▲ 回应 格納状況	★証明書(0)
調発行	<u>\$2</u>	1091 (00:00:04:43)	2023/02/1	4 2026/02/14	有効		rsa2048(sha256)			
ウント削除										
クに入れる	727	レート情報・・・・・								
	▶ 5 09×	10P			水涌于1月1			任會于	<i>ল</i> 11 .−- Þ	
		一	iis	demo.spt-demo.local	12147556			12.2000		
		組織名(0)	JC	CH Security Solution Sy	stems Co., Ltd.					
		ドッインコンボーネント(DC)	loi	al						
		19119-1911-191(66)	su	pport-v2						

画面下方の証明書ファイル欄の「あり」リンクからサーバ証明書をダウンロードします。

証明書]>詳細		■ 認証局 ■ 日夕 ■ 管理者 ■ ヘルブ	■ <u>□ジアウト</u> ●サイドバー
アカウント Account	IIII IIII IIII IIII IIII IIII IIII IIII IIII		■ <u>一朝に戻る</u> ▶ クイックナビ
グループ	Support-v2 CA#1091	\$10=29214	
Group			▲ ■ サーバ証明書
Lib的書 Certificate	▶証明書情報		121551F48
認証デバイス	> ESEE局: Support-v2 CA		
Device	> 暗ちアルコリスム: rsa > ゼイジェストアルゴリズム: sha256		
テンフレート Template	> 練長: 2048		(277
17 月日 312 142 4 17	> 鍵用途: <u>電子署名</u> 鍵の暗号化		1417
明書一覧	> 拡張線用途: <u>SSLサーバ設証</u> <u>SSLクライアント認証</u> > NMG · DNOG vindeme and dame local		▶ ドック
失効処理	> 596 : DNS-E. Isdenio spi-demolicia		<u>* アカウント (0)</u> ● 1788年 (0)
停止処理	▶証明書ファイル	▶ 失効情報	× 310/352 (0)
ドックに入れる	> 証明書要求: <u>赤川</u>	> CDP : http://test1.jcch-sss.com/crl/ia1.crl	
	「毛成日時 2023/02/14 14:46 > 第78日 た: 赤川		
	作成		
	> 秘密鍵:なし		
	▶ テンプレート構成		
	デフォルト設定 サーバ証明書		

2.2. ルート CA 証明書のダウンロード

ルート CA 証明書は以下のURL ヘアクセスして Gléas からダウンロードします。 http://host名/crl/ia1.der

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. 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。

3.1.サーバ証明書の登録

サーバ証明書はPKCS#12形式の証明書の登録とCSRから発行した証明書の登録のいずれかで行います。

IIS を起動し、左側ツリーの「サーバ名」をクリックします。

「サーバ証明書」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。

♥゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚	– 🗆 X
	😰 🔤 🟠 🔞 -
7ァイル(F) 表示(V) ヘルプ(H)	
接続 SPT-WIN2022 ホーム ・ マクラードページ アイルター・ ・ マクラードページ アイルター・ ・ ア・ジ アイルシン ・ ア・ジ ・ ア・ジ ・ ア・ガ ・ ア・グ ・ ア・ガ ・ ア・ガ ・ ア・ガ ・ ア・ガ ・ ア・ガ ・ ア・ガ ・ ア・ガ ・ ア・ガ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	 操作 機能を聞く サーバーの管理 再起動 開始 停止 アブリケーションブールの表示 サイトの表示 新しいWeb Platform コンボーネントの取得 ヘルブ
华儀完了	¶.:

💐 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			– 🗆 X
← → ¶ → SPT-WIN2022	•			🐱 🗟 🔞 •
ファイル(F) 表示(V) ヘルプ(H)				
Fine (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	サーバー証明書 SL に対して準成されたWeb サイトで cの機能を使用します。 フィルター:	Web サーバーが使用できる証明書を ▼ 検索(G) 〜 〜 すべて表示(A) 発行先	要求および管理するには、 <i>グループ化:</i> _デ 発行元	センボート 証明會の要求の作成 証明會の要求の完了 ドメイン証明會の作成 自己署名入り証明會の作成 更新された証明會の自動的な再 パインドを有効にする ・
< >> 準備充了	< 「」「機能ビュー」 22テンツ ビュー		>	

以降の手順はサーバ証明書の種類に応じて「3.1.1PKCS#12のサーバ証明書登録」、「3.1.2CSR から発行したサーバ証明書の登録」の手順を進めて下さい。

3.1.1. PKCS#12 のサーバ証明書登録

本項では PKCS#12 形式のサーバ証明書を登録する方法を記載します。 IIS からサーバ証明書一覧を開き、操作メニュー内の「インポート」をクリックします。



「証明書のインポート」ダイアログが表示されるので、「2.1.1PKCS#12 形式での発行と

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

ダウンロード」でダウンロードした証明書ファイル (PKCS#12) のパス、および、PKCS#12 のパスワードを入力します。

※「証明書ストアの選択」は「個人」、「この証明書のエクスポートを許可する」はオフにしてください。

「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。

証明書のインポート	?	\times
証明書ファ <mark>イ</mark> ル (.pfx)(C):		
C:¥Users¥Administrator¥Desktop¥iisdemo.p12		
パスワード(P):		
••••		
証明書ストアの選択(S):		
個人		\sim
□ この証明書のエクスポートを許可する(A)		
OK	キャンセル	,

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。

3.1.2. CSR から発行したサーバ証明書の登録

本項では IIS で作成した CSR から発行した、サーバ証明書を登録する方法を記載します。 ※CSR からのサーバ証明書の発行は「2.1.2CSR からの発行とダウンロード」を参照してください。

IIS から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。

🍓 インターネット インフォメーション サービス	ス (IIS) マネージャー			– 🗆 X
← → ¶ → SPT-WIN2022	•			🐱 🛛 🟠 🔞 🗸
戻る ル(F) 表示(V) ヘルプ(H)				
(本) jµ(f) (ホス(V) (A)jµ(f) 接続 ④	サーバー証明書 SSL に対して構成された Web サイト の機能を使用します。 フパルター: 名前	で Web サーバーが使用できる証明魯を ■ 愛 換索(G) - 🕢 すべて表示(A) 発行先	要求および管理するには、こ グループ化: テ 発行元 >	
< >	🏢 機能ビュー 💦 コンテンツ ビュー			
準備完了				• <u>1</u> .

「証明機関の応答が含まれるファイルの名前」に、「2.1.2CSR からの発行とダウンロード」 でダウンロードした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。

証明書の要求を完了する	?	×
証明機関の応答を指定します		
証明機関からの応答が含まれるファイルを取得すると、以前に作成した証明書の要求が完了します。		
証明機関の応答が含まれるファイルの名前(R):		
C:¥Users¥Administrator¥Desktop¥download.crt		
フレンドリ名(近:		
iisdemo.spt-demo		
新しい証明書の証明書ストアを選択してください(S):		
個人 ~		
ОК	キャンセル	,

「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。

휔 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				-		×
← → ¶ → SPT-WIN2022 →					5	🖂 🟠	• (2)
ファイル(<u>F</u>) 表示(<u>V</u>) ヘルプ(<u>H</u>)							
接続	▲■ ++_バ_=元田聿			操作			
🔍 • 🔒 🖄 🔝	リーハー証明音			インオ	代−ト		
ジ >	SSL に対して構成された Web サイトで の機能を使用します。	・Web サーバーが使用できる証明書を	要求および管理するには、こ	証明 証明	書の要求の 書の要求の	作成 完了	
	71ルター:	▼ 検索(<u>G</u>) → 🔙 すべて表示(<u>A</u>)	グループ化:	FX1	ン証明書の	作成…	
	名前	発行先	発行元	5 <u></u>	署名入り証	明書の作	成
	iisdemo.spt-demo	iisdemo.spt-demo.local	Support-v2	更新 パイン	された証明詞 バを有効に プ	書の自動的 する	りな再

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

3.2. ルート CA 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CA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 ために利用します。

ルートCA証明書はCTLとコンピュータストアの両方に指定します。

※ルートCA証明書は「2.2ルートCA証明書のダウンロード」の手順でダウンロードします。

3.2.1. CTL の登録

Powershell(あるいは、コマンドプロンプト)を管理者起動し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CA証明書ファイル 例) certutil -f -addstore iis_client_trust ia1.der

3.2.2. 信頼されたルート証明機関への登録

CTLの登録と同様にコマンドを実行し、コンピュータストアの「信頼されたルート証明機 関」ヘルートCA証明書を追加します。

certutil -f -addstore [証明書ストア名] [ルートCA証明書ファイル] 例)certutil -f -addstore ROOT ia1.der

3.2.3. ルート CA 証明書の確認

Powershell(あるいは、コマンドプロンプト)より以下「certlm.msc」と入力してMMCを起動し、コンピュータストアの「信頼されたルート証明機関」および「CTL登録」で登録した証明書ストア(例:iis_client_trust)を確認し、ルートCA証明書がインポートされていることを確認します。



🚟 certlm - [証明書 - ローカル コンピュ-	-ター¥iis_client_trust	¥証明書]		—	×
ファイル(F) 操作(A) 表示(V) ヘノ	レプ(H)				
🗢 🔿 🙍 📅 🔏 🐂 🖉	1 📑 📔 🖬				
> 🖺 テストルート 🔹 🔺	発行先	^	発行者		有
✓ ¹ iis_client_trust □ 証明書	Support-v2		Support-v2		20
> 🧮 Local NonRemovable Cert					
> 🧮 リモート デスクトップ					
> 証明音の豆琢安水 、 スマート カードの信頼されたル・					
> 「 信頼されたパッケージ アプリの					
> 📔 信頼されたデバイス					
> 🧮 Web ホスティング					
> I Windows Live ID Token Iss					
> 📔 WindowsServerUpdateSer 🗸					
< >	<				>
iis_client_trust ストアには 1 個の証明書だ	があります。				

3.3. SSL ポートのバインド

Powershell(あるいは、コマンドプロンプト)を管理者起動し以下のコマンドを実行して作成した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] certstorename=MY clientcertnegotiation=enable sslctlstorename=[証明書ストア名]

例) netsh http add sslcert ipport=0.0.0.2:443

certhash=d3e2496dcb807a8a1db388b72ee1e17060cca6be certstorename=MY clientcertnegotiation=enable sslctlstorename=iis_client_trust

<u>Note:</u> 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」もしくは「SSL Certificate successfully added」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

Gertificate bindings:	
IP:port	: 0.0.0.0:443
Certificate Hash	: d3e2496dcb807a8a1db388b72ee1e17060cca6be
Application ID	: {0000000-0000-0000-0000000000000000000
Certificate Store Name	: MY
Verify Client Certificate R	evocation : Disabled
Verify Revocation Using Cac	hed Client Certificate Only : Disabled
Usage Check	: Enabled
Revocation Freshness Time	: 0
URL Retrieval Timeout	: 0
Ctl Identifier	: (null)
Ctl Store Name	: iis_client_trust
DS Mapper Usage	: 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レジストリ エディターより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:

 ${\tt HKLM} \verb"{\tt SYSTEM} \verb"{\tt CurrentControl} \verb"{\tt SecurityProviders} \verb"{\tt SCHANNEL}"$

SendTrustedIssuerList (REG DWORD) を追加し、1 を設定します。

 レジストリエディター ファイル(F) 「編集(E) 表示(V) お気に入り(A) 	AJ.	レプ(H)		- 0	×
	*	名前 ••••) (既定) •••••EventLogging •••••SendTrustedIssuerList	種類 REG_SZ REG_DWORD REG_DWORD	データ (値の設定なし) 0x00000001 (1) 0x00000001 (1)	
< >		<			>
コンピューター¥HKEY_LOCAL_MACHINE¥SYSTEM¥	Curr	entControlSet¥Control¥Security	Providers¥SCHANNEL		

IISマネージャーより左手のサイトを選択し、右手の操作より「バインド」をクリックしま

す。

a real terms and a second second		
← → 😌 ► SPT-WIN2022 ►	サイト > Default Web Site >	₩ ₩ ₩ W
ファイル(E) 表示(V) ヘルプ(H)		
8. ● ■ 2 ● 2 2 2 2 2 2 2 2 2 2 2 2 2	● Default Web Site ホーム 2 ペルター: ● ● 使衆(⑤ ● ⑤ すべて表示(Δ) グループ化: IIS HTTP 応答ヘッダー MIME の種類 SSL 設定 Iラー ページ ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	操作 〕 エクスプローラー アクセス許可の損集 サイトの編集 バインド ごバインド 塗るお沙え アブリケーションの表示 依地デイレクトリの表示 Web サイトの管理
	ディレクトリの参照 ハンドラ-マッピング モジュール ログ記録 ご ご ご ご 正確 既定のドキュメント 出力キャッシュ 認証 要求フィルター 管理 へ	 ご 再起動 ● 開始 ● 停止 Web サイトの参照 ● *:80 (http) 参照 ■ 詳細設定 構成 制限 HSTS ② ヘルブ
> E	罰 機能ビュー 🎇 コンテンツ ビュー	

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

種類に「https」、SSL証明書に前手順で設定したサーバ証明書(iisdemo.spt-demo)を選択し、「OK」をクリックします。

※TLS1.1以前を無効にする際は「レガシTLSを無効にする」をチェックします。

サイト バインドの追加	?	×
種類(T): IP アドレス(I): ポート(O): https ~ 未使用の IP アドレスすべて ~ 443		
ホスト名(H):		
□ サーバー名表示を要求する(N)		
□ TLS 1.3 over TCP を無効にする(B) □ QUIC を無効にします(A)		
✓ レガシ TLS を無効にする(G) HTTP/2 を無効にします(D)		
□ OCSP ステープリングを無効にします(S)		
SSL 証明書(F):		
iisdemo.spt-demo ~ 選択(L)	表示(V)	
ОК	キャンセル	

httpsが一覧に追加されたことを確認し「閉じる」をクリックします。

ţ	オトバイン	パ				?	×
	種類	ホスト名	ポート	IP アドレス	バインド情報	追加(<u>A</u>)	
	http https		80 443	*		 編集(<u>E</u>)	
						削除(<u>R</u>)	
						参照(<u>B</u>)	
						閉じる(<u>C</u>)	

3.4. クライアント証明書要求の有効化

IISマネージャーより左側ツリーのサイトを選択し、「SSL設定」アイコンをクリックします。



「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。



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。

4. 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 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。

Ę	support Support-v2 2022/12/27	
Ę	support_test1 Support-v2 2022/12/1	

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。

IIS Windows Server × -	+						-	0	×
← C බ ⊡ https://iisdemo.sp	t-demo.local				A 10 C3	ξ≡	œ	۲	
Windows Server									^
Internet Informa	ation Ser	rvices							
Welcome Bier	venue Tervet	tuloa							
ະ∋c≉ Benvenuto ສະຫຼ	Bienvenido	Hoş geldiniz	ברוכים הבאים			Welkom			
Bem-vindo	Καλώς ορίσατε	Välkommen	환영합니다	Добро пожаловать	Üdvözöljük				
				欢迎					

Note:

セキュリティ警告が表示される場合は、『5.1 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。* 5. その他

5.1.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 サーバヘ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。

- 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・・・

- 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。
- 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

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

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。

5.2.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、失効情報が記載されたデータを証 明書失効リスト(CRL)と言います。CRL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。CRL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。

5.3.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

5.4.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行わなくなります。

- 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] certstorename=MY clientcertnegotiation=enable 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。

5.5.ASP.NET(C#)でクライアント証明書の情報を取得する

以下にサンプルコードを記載します。

<%@ PAGE LANGUAGE="C#" %>
<html></html>
<script runat="server"></td></tr><tr><td>void Page_Load(object sender, EventArgs e) {</td></tr><tr><td>HttpClientCertificate cert = Request.ClientCertificate;</td></tr><tr><td>if (cert.IsPresent) {</td></tr><tr><td>Serial.Text = cert.SerialNumber;</td></tr><tr><td>Subject.Text = cert.Subject;</td></tr><tr><td>KeySize.Text = cert.SecretKeySize.ToString();</td></tr><tr><td>ValidFrom.Text = cert.ValidFrom.ToString("yyyy/MM/dd HH:mm:ss");</td></tr><tr><td>ValidUntil.Text = cert.ValidUntil.ToString("yyyy/MM/dd HH:mm:ss");</td></tr><tr><td>} else {</td></tr><tr><td>Summary.Text = "クライアント証明書が見つかりません";</td></tr><tr><td>}</td></tr><tr><td>}</td></tr><tr><td></script>
<body></body>
<asp:label id="Summary" runat="server"></asp:label>

シリアルNo:<asp:label id="Serial" runat="server"></asp:label>
サブジェクト:<asp:label id="Subject" runat="server"></asp:label>
鍵長:<asp:label id="KeySize" runat="server"></asp:label> bits
イii>有効期限の開始日:<asp:label id="ValidFrom" runat="server"></asp:label>
イii>有効期限の終了日:<asp:label id="ValidUntil" runat="server"></asp:label>

6. お問い合わせ

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