

(参考資料としての利用に限る)

Microsoft IIS 8.x/10 サーバ証明書インストール方法 新規・更新

1. はじめに

IIS8.x/10環境下での、サーバ証明書インストール手順を以下に説明します。

大まかな手順は、以下のとおりです。

(1)証明書の受理とインストール準備

(2)サーバ証明書のインストール

(3)中間 CA 証明書のインストール

(4)サーバ証明書の適用

2. 証明書の受理とインストール準備

2.1 お客様のサーバ証明書の受理と保存

お客様のサーバ証明書(エンド証明書)は、発行時のメールに添付されていますので、名前をつけて保存します。

仮にファイル名はwww.jcert.biz.crtとし、Cドライブ直下へ保存しておきます。以後も同様としますが、 環境に合わせて読み替えてください。

2.2 中間 CA 証明書の受理と保存

サーバ証明書を使用するには、中間 CA 証明書が必要になります。

中間 CA 証明書は、「証明書を設定する前に(準備作業)」をご一読頂き、<u>中間証明書一覧から取得</u>してく ださい。 <u>https://www.jcert.co.jp/support/certificate/</u>



3. サーバ証明書のインストール お客様のサーバ証明書をインストールします。

3.1 サーバ証明書の選択

Windows キーを押して【スタートメニュー】を表示し右クリックから【すべてのアプリ】にアクセスします。

スター	- -		Administrate	or 🎴
		(în		
サーバー マネー ジャー	Windows PowerShell	管理ツール		
コンピューター	タスク マネージャー			
	e			
コントロール バネル	Internet Explorer			
テスクトップ	🖬 Madana Jaran (15)			
				JACOPTU

一覧画面から【インターネットインフォメーションサービスマネージャ】にアクセスします。





以下の画面が開きますので、【サーバ証明書】をダブルクリックします。

9			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
💽 🖣 🕨 WIN-04	1RRPE54478 •					
ファイル(F) 表示(V) ヘル	プ(H)					
接続 Q, • 🔜 / 2 8 。	🧤 win-o	D4RRPE54	478			
₩ 29-1-X-3 WIN-04RRPE54478	フィルター:	- 7	と検索(<u>G)</u> → 🔙 すべ	て表示(<u>A</u>) グル-	-プ化: _{領域}	-
	IIS HTTP 応答へッダー	MIME の種類	<u>(404</u>) エラー ページ	ブラン・ボック (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	ディレクトリの参照	マンドラー マッピング
	モジュール	ログ記録	<i>(</i> ワーカー プロセス	一日本語	していた 既定のドキュメント	出力キャッシュ
	3 認証	(1) 要求フィルター				
	管理 電子 機能の委任	〔 共有構成	構成エディター			

3.2 証明書要求の完了

右側の操作メニューの【証明書の要求の完了】をクリックします。





3.3 ファイルの指定

以下ウィザードが起動します。「証明機関の応答が含まれるファイルの名前」にダウンロードしたお客様のサーバ証明書を指定します。

「フレンドリ名」は任意の文字列を入力してください。わかりやすい文字列の入力をお勧めします。

【更新時】更新前の証明書のフレンドリ名とは異なる文字列を入力してください。

「新しい証明書の証明書ストアを選択してください」では【個人】のままにしておきます。 入力後【OK】をクリックします。

証明書の要求を完了する	?	x
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:¥www.jcert.biz.crt		
フレンドリ名(Y):		
www.jcert.biz		
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	ヤンセノ	۲

【SNI 利用の場合】SNI で IP を共有するすべての証明書は、「個人」 ストアではなく、「Web ホスティ ング」 ストアをインストール先として選択してください。

新しい証明書の証明書ストアを選択してください(S):				
Web ホスティング	~			



次に、中間 CA 証明書をインストールします。

【更新時】 既に SHA-2 中間証明書を設定済であれば、本章はスキップしてください。

4. 中間 CA 証明書のインストール

サーバ証明書を多くのブラウザで信頼を得るために、Web サーバに中間 CA 証明書をインストールしま す。上記 2 で準備した中間 CA 証明書をインストールしてください。

インストール方法は、「中間 CA 証明書インストール方法」をご参照ください。

https://www.jcert.co.jp/support/pdf/certificate/CA_install_iis8.pdf

5. サーバ証明書の適用

インストールしたお客様のサーバ証明書をサーバへ適用します。

5.1 バインド

サーバ証明書を適用したい Web サイトを選択し、右側の操作メニューの【バインド】をクリックします。

6	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	_ D X
€ • WIN-04	RRPE54478 → サイト → Default Web Site →	😰 🛛 🟠 🔞 🗸
ファイル(E) 表示(⊻) ヘル	プ(圧)	
接続 スタートページ WIN-O4RRPE54478 (WIN- マアリケーションブール サイト > Cefault Web Site	シロケンツ ビュー シロケンツ ビュー	操作 ♪ エクスプローラー アクセス許可の編集 サイトの編集 パインド 図 基本設定 アプリケーションの表示 仮想ディレクトリの表示 仮想ディレクトリの表示 砂糖 サイトの管理 ② 再起動 開始 停止 Web サイトの参照 詳細設定 構成 制限 ② へいブ オンライン ヘルブ
準備完了		• <u>1.</u> ;



5.2 サイトバインド

以下の画面が表示されますので、【追加】をクリックします。

		サイ	トバインド	? X
種類 http	ホスト名	ポート IP アドレス 80 *	バインド情報	追加(A) 編集(E) 削除(R) 参照(B)
				閉じる(C)

【更新時】 【編集】をクリックすることで表示される、前回利用した https 情報を選択してください。

			ታ ተኮ	バインド		? X
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		80	*		_	
https		443	*			編集(<u>E</u>)
						削除(<u>R</u>)
						参照(<u>B</u>)
						閉じる(<u>C</u>)



5.3 サイトバインドの追加(以下更新時は「追加」を「編集」と読替えてください)

以下画面が表示されますので、「種類」は『https』、「ポート」は『443(またはお客様が SSL で使用する ポート)』、「SSL 証明書」は『3.サーバ証明書のインストール でインストールした証明書』を選択し、【OK】 をクリックします。

(注)「SSL 証明書」には、3.3 で指定したフレンドリ名やコモンネームが表示されます。

サイト バインドの追	加 ? ×
種類(T): https ✓ ホスト名(H): □ サーバー名表示を要求する(N)	v (#43
SSL 証明書(F): www.jcert.biz イ	選択(L) 表示(V) OK キャンセル

5.4 サイトバインドの確認

以下画面が表示されますので、https が追加されていることを確認し、【閉じる】をクリックします。

		ታና	トバインド	? X
種類 http https	ホスト名	ポート IP アドレス 80 * 443 *	バインド情報	追加(A) 編集(E) 削除(R) 参照(B)
				閉じる(C)

以上でサーバ証明書の適用は完了です。



【追補】 SNI 利用の場合

SNI(Server Name Indication)の機能を利用することで1つのグローバル IP アドレスに複数の SSL 証明書 (ワイルドカードまたはマルチドメインをご利用の場合は1枚)を割り当てることが出来ます。

SNI 非対応のブラウザからはサイトが閲覧できませんので十分に考慮して利用して下さい。

一般的に利用されるブラウザの SNI への対応状況は以下になります。

✓ Internet Explorer 7 以降(OS は Windows Vista 以降)

- ✓ Mozilla Firefox 2.0 以降
- ✓ Google Chrome (OS は Windows Vista 以降)
- ✓ Android ブラウザ (Android 3.0 (Honeycomb) 以降)
- ✓ Opera 8.0 以降

これらのブラウザの最新の対応状況または、これら以外のブラウザのサポート状況は各ブラウザのサポ ートサイトをご確認下さい。

<mark>※以下の例は 2 つの異なる FQDN のサイトを 1 つのグローバル IP で提供する場合の例です。 手順通り証</mark> 明書を登録するには手順 3.2、3.3、4 で 2 枚目の証明書を「**Web ホスティング」ストアに追加**しておく 必要がございます。(ワイルドカードまたはマルチドメインをご利用の場合は 1 枚で足ります。)

追補1 サイトバインドの追加(1つ目)

手順5.15.2 と同様に操作しサイトバインドの追加画面を表示します。

以下画面が表示されますので、「種類」は『https』、「ポート」は『443(またはお客様が SSL で使用する ポート)』、「ホスト名」は『SSL 証明書に対応する FQDN』を入力、「サーバー名表示を要求する」のチェ ックを入れ、「SSL 証明書」は『3.サーバ証明書のインストール でインストールした証明書』を選択し、 【OK】をクリックします。

(注)「SSL 証明書」には、3.3 で指定したフレンドリ名やコモンネームが表示されます。

※「IP アドレス」について、同一 IIS に複数 IP を割り当てられている場合は、複数の証明書で共有す る特定の IP アドレスを指定するようにして下さい。

サイト バインドの追加	n ? ×
種類(T): https v IP アドレス(I): 未使用の IP アドレスすべて パスト名(H): □ サーバー名表示を要求する(N)	ポート(O): 443
SSL 証明書(F): www.jcert.biz v	選択(L) 表示(V) OK キャンセル



<mark>追補 2 同様に2つ目以降のサイトバインドの追加証明書(ワイルドカードまたはマルチドメインをご</mark> 利用の場合は1枚の同一証明書)を追加し、【OK】をクリックします。

(注)「SSL 証明書」には、3.3 で指定したフレンドリ名やコモンネームが表示されます。

※「IP アドレス」について同一 IIS に複数 IP を割り当てられている場合は、複数の証明書で共有する 特定の IP アドレスを指定するようにして下さい。

サイト バインドの追加 ? ?	x
種類(T): https v ホート(O): 未使用の IP アドレスすべて v 443	
www.site2.jcert.biz ✓ サーバー名表示を要求する(N)	
SSL 証明書(F)· www.site2.jcert.biz 選択(L) 表示(V)	
OK キャンセル	

追補3 サイトバインドの確認

以下の画面が表示されますので、追加分の2つの『種類』に「https」、『ポート』に「443」、『IP アドレス』が同じ設定となっていることを確認し、【閉じる】をクリックします。

(注)「SSL 証明書」には、3.3 で指定したフレンドリ名やコモンネームが表示されます。

※「IP アドレス」について同一 IIS に複数 IP を割り当てられている場合は、複数の証明書で共有する 特定の IP アドレスを指定するようにして下さい。

			ታイト バー	インド	? X
種類 http https	ホスト名 www.icert.biz	ポート 80 443	IP アドレス * *	バインド情報	追加(A) 編集(E)
https	www.site2.jcert.biz	443	*		削除(R)
					参照(B)
					閉じる(C)

以上で SNI を利用した複数のサーバ証明書の適用は完了です。



6. 証明書と秘密鍵のバックアップ

万一のサーバトラブルによる再設定や、ハード更新時の再インストールに備えて、証明書と秘密鍵をバックアップしておきます。 証明書と秘密鍵のバックアップについては、「Microsoft IIS8.x SSL サーバ証明書エクスポート方法」をご参照ください。

https://www.jcert.co.jp/support/pdf/faq3/inport_iis8.pdf

この文書に記載されている情報は予告なしに変更されることがあります。この文書に記載されている情報に従ってユーザーが操作を行った結果、ユーザーが被る損害については、ジェイサートでは一切責任を負いません。ユーザーは自己責任においてのみ、この文書を使用するものとします。