(t cybertrust

# SureServer for SAKURA/SureServer for SAKURA(EV)

## Microsoft IIS7.0/7.5

# CSR 作成/証明書インストール手順書

## (新規•更新用)

Version 1.1

PUBLIC RELEASE

2015/04/21

IIS7.0/7.5 CSR 作成/証明書インストール作成手順書(新規・更新用)| Page 2

## <u> 改訂履歴</u>

日付	バージョン	内容
2014/12/10	1.0	初版リリース
2015/04/21	1.1	サイバートラストの WEB ディレクトリ変更に
		伴うリンク先 URL の修正



## <u>目次</u>

はじめに	4
CSR の作成	5
<ol> <li>CSR 作成前のご確認事項</li> <li>11 公開鍵長のご指定について</li> </ol>	6
1.2. CSR 作成時に指定する項目 (DN) について	6
<ol> <li>キーペア・CSR の作成</li> <li>2.1. 作成方法</li> </ol>	<b>7</b> 7
3. 証明書のお申し込み	11
証明書のインストール	12
4. 証明書のダウンロード	13
4.1. 中間 CA 証明書のダウンロード 4.2. SSL サーバー証明書のダウンロード	13 13
5. 証明書のインストール	15
5.1. 中間 CA 証明書のインストール 5.2. SSL サーバー証明書のインストール	15 23
6. SSL サーバー証明書の適用	25
7. 鍵ペアファイルのバックアップ	27
SSL 通信の確認	29
8. SSL 通信の確認	30



## はじめに

#### 【!】本手順書をご利用の前に必ずお読みください

本ドキュメントは、Microsoft 社の「Internet Information Services 7.0/7.5(以下、IIS7.0/7.5)」の環境下で サイバートラストのサーバー証明書をご利用いただく際の CSR 作成とサーバー証明書のインストール について解説するドキュメントです。

実際の手順はお客様の環境により異なる場合があり、IIS7.0/7.5 の動作を保証するものではございません。あらかじめご了承ください。

なお、このドキュメントは予告なく変更される場合があり、サイバートラスト株式会社はその内容に対して 責任を負うものではありません。

また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。

このドキュメントで説明するソフトウェアはライセンスに基づいて配布されるものであり、ライセンスの条 項に従った使用のみ許可されます。このドキュメントは、本来の使用目的のために発行され、公に発行 されるものではありません。

このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。

ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の 添付を条件として複製することができます。

サイバートラスト株式会社から事前に書面による合意を得ない限り、このドキュメントまたはその一部から直接的または間接的に知り得た内容または主題に関して、個々の企業やその従業員などの第三者に対し、口頭、文書、またはその他のいかなる手段によっても伝達することはできません。

cybertrust

IIS7.0/7.5 CSR 作成/証明書インストール作成手順書(新規・更新用)| Page 5

# <u>CSR の作成</u>



 $Copyright \ (C) \ Cybertrust \ Japan \ Co., \ Ltd. \ All \ Rights \ Reserved.$ 

## 1. CSR 作成前のご確認事項

CSR 作成前に以下についてご確認ください。

## 1.1. 公開鍵長のご指定について

公開鍵長は「2048bit」をご指定ください。

※2048bit 未満の鍵長をご指定の場合、証明書の申請時にエラーとなりますのでご注意ください。

### 1.2. CSR 作成時に指定する項目(DN)について

CSR 作成時に以下の項目を指定いただきますので、あらかじめ必要項目をご確認ください。

【!】以下の点についてご注意ください。

・●印がついている項目は必須設定項目です。

- ・各項目の最大文字数は半角64文字(半角スペースを含む)です。
- ・CSR に使用出来る文字は半角英数字(a~z, A~Z, 0~9)と記号(「"」「#」「;」「+」を除く)です。
- ・日本語は使用しないでください。
- ・個人事業主の方は入力項目が異なります。詳細につきましては、個人事業主のお申し込み方法をご参照ください。

	入力項目	内容	入力例
		実際に接続する URL の FQDN	https://www.cybertrust.ne.jp/index.html ⇒ www.cybertrust.ne.jp
•	コモンネーム(UN)	グローバル IP アドレス(※1)	https://212.xxx.xxx.xxx/index.html ⇒ 212.xxx.xxx.xxx
ullet	組織単位名(OU)	部署名(※2)	Technical Division
ullet	組織名(O)	申請組織の名称(英名)	Cybertrust Japan Co.,Ltd.
•	市町村名(L)	申請組織の事業所住所の「市町村名」(英名) ※東京は 23 区	Minato-ku
•	都道府県名 (S/ST)	申請組織の事業所住所の「都道府県名」(英名)	Tokyo
•	国名(C)	申請組織の国名(JP 固定)	JP

※1 SureServer for SAKURA(EV) は、コモンネームをグローバル IP アドレスとしてご指定いただけません。 ※2 申請法人以外の名称、屋号、商標、住所、場所、その他特定の自然人や法人を参照する値を指定することはできません。



## 2. <u>キーペア・CSR の作成</u>

Microsoft Windows Server 2008 の【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】を使って、SSL で使用するキーペア(公開鍵・秘密鍵のペア)と CSR を作成します。

### 2.1. 作成方法

- A) 【スタート】メニューから【コントロールパネル】→【管理ツール】→【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】を選択して起 動します。
- B)以下の画面から、【サーバー証明書】 をダブルクリックします。





#### C) 画面右側の操作メニューから【証明書の要求の作成】 をクリックしま す。



D)識別名プロパティを入力する画面が表示されますので、CSR に設定 する情報を入力して、【次へ】をクリックします。以下のルールに従っ て正確に入力してください。

※半角英数字で入力してください。 ※使用可能文字:スペース「a-z」「A-Z」「0-9」「'」「,」「.」「()」「:」「-」「?」「&」

入力項目	内容	入力例
一般名	完全なドメイン名(FQDN)	test.cybertrust.ne.jp
組織	申請組織の名称((英語)	Cybertrust Japan Co.,Ltd.
組織単位	「部署名」(※)	Test Unit
	申請組織の事業所住所の	
市区町村	「市町村名」(英語)	Minato-ku
	※東京は 23 区	
初送四间	申請組織の事業所住所の	Televe
即迫的乐	「都道府県名」(英語)	Токуо
国/地域	申請組織の国名	JP

(t

cybertrust

※申請法人以外の名称、屋号、商標、住所、場所、その他特定の自然人や法人を 参照する値を指定することはできません。

明書の要求	and the second	?
調 識別名プロ	<b>ሆ</b> የታ <i>1</i>	
証明書に必要な情報を指 ださい。省略形を使用しな	定します。都道府県および市区町村に関する情報は、公式なもので いでください。	を指定してく
一般名( <u>M</u> ):	test.cybertrust.ne.jp	
組織(_):	Cybertrust Japan Co.Ltd.	
組織単位 (OU)( <u>U</u> ):	Test Unit	- 10
市区町村(山)	Minato-ku	
都道府県(S):	Tokyo	
国/地域(R):	JP	न
		2
	前に戻る(P) 旅へ(N) 終了(E	) キャンセル

E)【暗号化サービス プロバイダ】は、表示された情報
 (Microsoft RSA Schannel Cryptographic Provider)
 を選択し、「ビット長」は「2048」と指定してください。

証明書の要求	? ×
暗号化サービス プロバイダのプロパティ	
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。暗号化キーのビット長は、証明書の暗号化の強度 を決定します。ビ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(S): Microsoft RSA SChannel Cryptographic Provider ビット長(B): 2048	
<b>前に戻る(P)</b> 終了(E) キャンセ	216



#### F) CSR のファイル名と保存先を指定し、【終了】をクリックします。



以上で、CSR の作成は完了です。



## 3. 証明書のお申し込み

作成した CSR をテキストエディタで開いて内容をコピーし、オンラインサインアップ の入力フォームに貼り付けて、お申し込みください。

<CSR サンプル> ※申請にはご利用いただけません。

-----BEGIN NEW CERTIFICATE REQUEST-----MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG A1UEBwwJTWIuYXRvLWt1MSIwIAYDVQQKDBIDeWJIcnRydXNOIEphcGFuIENvLixM dGQuMRIwEAYDVQQLDAIUZXNOIFVuaXQxHjAcBgNVBAMMFXRIc3QuY3IiZXJOcnVz 2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4R0cFsgrk05FgeUCaeDFyIIEST

----END NEW CERTIFICATE REQUEST-----

「-----BEGIN NEW CERTIFICATE REQUEST-----」から、「-----END NEW CERTIFICATE REQUEST-----」までをハイフンを含め、すべてコピーし申請画面 に貼り付けてください。

1 文字でも欠けるとフォーマットエラーとなりますのでご注意ください。

【!】CSR 作成後の注意事項

IIS7.0/7.5 では、CSR 作成後にキーペアのバックアップを取ることがで きない仕様となっております。そのため、SSL サーバー証明書のインス トールが完了するまでは、証明書の登録要求を絶対に削除しないでくだ さい。

※証明書の登録要求を削除されますと、元の CSR で発行した SSL サーバー証明 書のインストールができなくなり、弊社への再申請が必要になります。あらかじめ、 ご注意ください。

cybertrust

IIS7.0/7.5 CSR 作成/証明書インストール作成手順書(新規・更新用)| Page 12

# <u>証明書のインストール</u>

### 【!】本手順はサーバー証明書の発行後に行います。



## 4. 証明書のダウンロード

インストールが必要となる中間 CA 証明書・SSL サーバー証明書を事前にダウンロードします。

### 4.1. 中間 CA 証明書のダウンロード

サーバー証明書をご利用の際、お使いの機器へ中間 CA 証明書のインスト ールが必要となります。

ご選択いただいた商品により必要な証明書が異なりますので、証明書の種類をご確認のうえ、以下 URL からダウンロードしてください。

商品名	中間 CA 証明書
SureServer for SAKURA	https://www.cybertrust.ne.jp/sureserver/download/root_ca/PUBC AG3_sha2.txt
	中間 CA 証明書 1 https://www.cybertrust.ne.jp/sureserver/download/root.ca/evcag
	2_2_sha2.txt
SureServer or SAKURA(EV)	中間 CA 証明書 2
	https://www.cybertrust.ne.jp/sureserver/download/root_ca/evcag 2_sha2.txt

## 4.2. SSL サーバー証明書のダウンロード

(t cybertrust SSL サーバー証明書が発行されましたら、事前にダウンロードし、【.cer】や 【.txt】などの拡張子で保存してください。

- A) SSL サーバー証明書の発行後にお送りするメール(件名:[さくらインタ ーネット]《重要》SureServer サーバー証明書発行のお知らせ)に記載 されている URL にアクセスします。
- B) SSL サーバー証明書のダウンロード画面が表示されますので、お申し込み完了後にお送りしたメール(件名:【重要】お申込受付完了のお知らせ(ダウンロードパスワードご案内))に記載のパスワードを入力し、ダウンロードボタンをクリックしてください。

C) SSL サーバー証明書のダウンロード画面表示にならい、SSL サーバー 証明書を任意のフォルダに保存してください。



## 5. 証明書のインストール

中間 CA 証明書とSSL サーバー証明書のインストールを行います。

### 5.1. 中間 CA 証明書のインストール

中間 CA 証明書を「Microsoft 管理コンソール (Microsoft Management Console:MMC)」からインストールします。

※証明書更新時、すでに同じ内容の中間 CA 証明書がインストールされている場合は、 この手順をスキップしてください。

※SureServer for SAKURA(EV) では、同様の手順で「中間 CA 証明書 1」と「中間 CA 証 明書 2」をインストールしてください。

なお、必要な中間 CA 証明書のコモンネームが不明な場合は、サーバー証明書ファイルを開いて発行者のコモンネームの項目をご確認ください。

#### 【例】<u>SureServer for SAKURA(EV)の場合</u>

<b>証明書</b> ? 🔀
全般 詳細 証明のパス
副時書の情報
この証明書の目的: ・リモート コンピュータの ID を保証する
*詳細は、証明機関のステートメントを参照してください。 発行先: www.cybertrust.ne.jp
<b>発行者:</b> Cybertrust Japan EV CA G2
有効期間 2013/06/23 から 2015/06/23
こは明書のインストール①…   ※行者のステートメント(S)  OK

→必要な中間 CA 証明書のコモンネーム: Cybertrust Japan EV CA G2

(t cybertrust

#### A) 【スタート】メニューから【ファイル名を指定して実行】をクリックします。



#### B)【名前】へ「mmc」と入力して【OK】をクリックし、MMCを開きます。

📨 ファイノ	▶名を指定して実行 🛛 🔀
	実行するプログラム名、または開くフォルダやドキュメン ト名、インターネット リソース名を入力してください。
名前(0)	): mmc
	<ul> <li>このタスクは管理者特権で作成されます。</li> <li>OK キャンセル 参照(B)</li> </ul>



C) MMC 画面左上の【ファイル】メニューをクリックし、【スナップインの追 加と削除】をクリックします。

<u>אירבאיר (באיר איר איר איר איר איר איר איר איר איר </u>	
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)	×
新規作成N) Ctrl+N 問((0) Ctrl+O	
□ 上書き保存(S) Ctrl+S	操作
名前を付けて保存(A)に表示する項目はありません。	コンソール ルート 🔺
スナップインの這加と削IF家(M)_ Ctrl+M	他の操作 ▶
1773XI)	
終了(X)	
	I

D) 【利用できるスナップイン】から【証明書】を選択し、【追加】をクリックします。

フォルダ         Microsoft Corpor            オリシーの結果セット         Microsoft Corpor            メート デスクトップ         Microsoft Corpor            メーティングとリモート アクセニ         Microsoft Corpor            レーティングとリモート アクセニ         Microsoft Corpor            レーション・ジーゲーングレーブ         Microsoft Corpor            記述地域エクスプローラ         Microsoft Corpor            実有などび後期での管理         Microsoft Corpor            メーカショング         Microsoft Corpor            メーカンシーグ         Microsoft Corpor            ・         ・         Microsoft Corpor            ・         ・	けっけんし	10 M		TO A SHIELD AND A	500.#EM0.05
記憶数120.7月−う Microsoft Corpor_ 注共有と記憶板の管理 Microsoft Corpor_ 共有フルダ Microsoft Corpor_ HAT27ルダ Microsoft Corpor_	フォルダ オルシーの結果セット リモート デスクトップ レーティングとリモート アクセー ローカル ユーザーとグループ	Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_			新学校(P) 上へ移動(U) 下った時秋(V)
20日時代とビスーーフレスモニ Messed Coper 直信時代モニタ Microsoft Coper.	<ul> <li>記憶様エクスブローラ</li> <li>共和と記憶域の管理</li> <li>共和フォルダ</li> <li>研究オージャ</li> <li>理理理理</li> <li>(体験ないパラ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_	isto(A) >		
• • • • • • • • • • • • • • • • • • •		-			



#### E) 【コンピュータアカウント】を選択し、【次へ】をクリックします。



#### F) 【ローカルコンピュータ(このコンソールを実行しているコンピュータ)】 を選択し、【完了】をクリックします。

	: (このコンソールを実行しているコンと	(a-9)	4.777.783
「 おりのコンピュータ(A):			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を	変更できるようにする(W)	
これは、コンソールを1米	ほしに場合に切め週用されます。		



G) 【選択されたスナップイン】に【証明書(ローカルコンピュータ)】が追加 されていることを確認し、【OK】をクリックします。

スオックイン フォルダ フォルダ 動してト・デスクトップ し、ティングとリモート アクセー 第ローカル ユーザーとグループ 記憶域エクスプローラ 認共有に記憶域の管理 の 共有フルルダ	Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_ Microsoft Corpor_	▲ 	● コント・カット ② 証明書 (ローカル コンピュータ)	<b>拡張の編集(20</b> _ 育形(R) 上へ移動(U) 下へ移動(D)
日本12マネージャ ■ 証明書 ④ 信頼性とパフォーマンス モニー ■ 信頼性モニタ	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	•		【详细】改定(V)

H) コンソールルートへ【証明書(ローカルコンピュータ)】が追加されたことを確認し、【証明書(ローカルコンピュータ)】→【中間証明機関】→
 【証明書】をクリックします。



(t cybertrust



#### I) MMC 画面の左上の【操作】メニュー→【すべてのタスク】→【インポート】 の順にクリックします。

- ル1 -  -  -  -  -  -  -  -  -  -  -  -  -	- ロンソール ルート¥証明書([	コーカル コンピュータ)	¥中間証明機関¥証明書]
🚟 ファイル(F)	操作(A) 表示(V) お気に入り	り(0) ウィンドウ(W)	ヘルプ(H)
🗢 🔿 [ 👔	すべてのタスク(K) ・	インポートの…	
📔 א א-עעב	ここから新しいウィンドウ(W)	発行先 🔺	発行者
□ 🗊 証明書   □ 🗐 個人	新しいタスクパッド表示(T)		
<ul> <li>□ □ □</li> <li>□ □</li> <li>□ □</li> <li>□ □</li> <li>□ □</li> <li>□ □</li> <li>□ □</li> </ul>	最新の情報に更新(F) 一覧のエクスポート(L)		
	ヘルプ(H)	]	

J)証明書のインポートウィザードが表示されますので、【次へ】をクリック します。

証明書のインボート ウィザード		×
	証明書のインボート ウィザードの開始	
	このウィザードでは、証明書、証明書信頼リスト、および証明書失効リ ストをディスクから証明書ストアにコピーします。 証明機関によって発行された証明書は、ユーザー ID を確認し、データ を保護したり、またはセキュリティで保護されたネットワーク接続を提供 するための情報を含んでいます。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。 続行するには、D次へJ をクリックしてください。	
	< 戻る(日) (次へ(10)) キャンセル	



#### K)【参照】をクリックしてインストールする中間 CA 証明書を指定し、【次 へ】をクリックします。

ファイル名(E):				₩B(R)
はたいもの形式また	おみし 1 ~ の つ 二 / 11 ( - 5年)		**	
注意: 八切形式を防	EDE T JUJ771/WERE	祝の記明者を1本官でき 20 #40 / DEV D40)	97.9: 	
Personal Inform	mation Exchange- PKC	/5 #12 (.PFX.P12)	# ( 070)	
Cryptographic	Message Syntax Stan	dard- PKUS #/ 副型界	書(1978)	
Microsoft ジリア	小川とされた証明書人トノ	/(\$\$1)		
明書ファイルの形式の言	詳細について表示します。	2		

#### しし【次へ】をクリックします。

証明書ストアは、証明書が保管される	シシステム上の領域です。		
Windows に証明書ストアを自動的に	選択させるか、証明書のお	易所を指定すること	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ぶ	択する( <u>U</u> )	
● 証明書をすべて次のストアに配	】置する( <u>P</u> )		
証明書ストア:			
中間証明機関			参照( <u>R</u> )
証明書ストアの詳細を表示します			



M) 次の画面が表示されたら内容を確認して、【完了】をクリックします。

証明書のインボート ウィザード		×
	証明書のインポート ウィザードの完了	
	[完了] をクリックすると、証明書がインボートされます。 次の設定が指定されました:	
~	ユーザーが選択した証明書ストア 中間証明機関 内容 証明書	
	ファイル名 C¥Users¥ctj¥Desktop¥PUBCA	
3		
	< 戻る( <u>B</u> ) 完了 キャンセル	

N) インポート正常終了のメッセージが表示されますので、【OK】をクリッ クします。



(t cybertrust



O)証明書の一覧にインストールした中間 CA 証明書が表示されている ことを確認します。



P) 上記画面を閉じる際に、「コンソールの設定をコンソール 1 に保存し ますか?」と表示されますので、「いいえ」を選択して終了してください。

以上で中間 CA 証明書のインストールが完了します。

### 5.2. SSL サーバー証明書のインストール

SSL サーバー証明書のインストールを行います。

(t

cybertrust

A) 【スタート】メニューから【コントロールパネル】→【管理ツール】→【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】を選択して起 動し、以下の画面から、【サーバー証明書】をダブルクリックします。



#### B) 画面右側の操作メニューから【証明書の要求の完了】 をクリックしま す。



C) 【証明機関の応答が含まれるファイルの名前】に事前にダウンロード したお客様の SSL サーバー証明書ファイルを指定し、【OK】をクリッ クします。

※【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 をおすすめいたします。

証明書の	要求を完了する	?
	証明機関の応答を指定します	
書正日月相	期期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。	
	期の応答が含まれるファイルの名前(R): 20999999.cer	
וכער	型名( <u>)</u> :	
Cyber	trust Japan	
	<b>*</b> *2	ルレル
- 7° 55	Lサーバー証明書のインストールは完了です。	1211

(t cybertrust

## 6. SSL サーバー証明書の適用

インストールした SSL サーバー証明書をご利用の Web サイトへ適用します。

 A)【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】画面に 戻り、SSL サーバー証明書を適用したい Web サイトを選択し、画面 右側の操作メニューから【バインド】をクリックします。



#### ■ 新規の場合

B)「サイトバインド」画面が表示されますので、新規の場合は【追加】を クリックします。

種類	ホスト名	ポート	IP アドレス	二 形石	追加(A).
http		80	*		編集(E).
					削除(日)
100				and the second second	金服2(口)

#### ■ 更新の場合

(t

cybertrust

C)証明書更新の場合は既に https のバインド設定が存在しますので、 そちらを選択して【編集】をクリックします。

種類	ホスト名	ポート	IP アドレス	1542	追加( <u>A</u> )…
nαφ https		60 443	*		編集( <u>E</u> )
61					削除( <u>R</u> )
(				•	参照(B)

# D)【サイトバインドの追加】または【サイトバインドの編集】画面が表示されますので、以下の情報を選択して【OK】をクリックします。

サイト バイント	「の追加	?	×
種類(T):	IP アドレス(1): 未使用の IP アドレスすべて	<u>₩−ト(O):</u>	
ホスト名(日):			
」 SSL 証明書	(S):		
Cybertrust	Japan	▼ _表示(⊻)	
		OK キャンセル	

項目	入力内容
種類	https
IP アドレス	サーバー証明書を適用する
	Web サイトの IP アドレス
_10 1	443
	(もしくは、任意の SSL ポート番号)
	インストール時に指定したフレンドリ名や証明書
SSL 証明書	のコモンネームが表示されますので、適用した
	い SSL サーバー証明書を選択します。

以上で SSL サーバー証明書の適用は完了です。





鍵ペアファイルをバックアップします。

A) 【スタート】メニューから【コントロールパネル】→【管理ツール】→【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】を選択して起 動します。以下の画面から、【サーバー証明書】をダブルクリックしま す。



B) バックアップしたい SSL サーバー証明書を選択し、画面右側の操作 メニューから【エクスポート】をクリックます。





C) 【エクスポート先】に保存先のフォルダとファイル名を指定します。ファ イルの拡張子は【.pfx】を指定し、【パスワード】、【パスワードの確認 入力】に同じパスワードを入力し、【OK】をクリックします。

※指定するパスワードは任意の文字列です。証明書のインポート時に入力が必要 となります。

証明書のエクスポート	? :
エクスポート先(E):	
C:¥Backup.pfx	
パスワード( <u>P</u> ):	
•••••	
パスワードの確認入力(M):	
	キャンセル

以上で、鍵ペアファイルのバックアップは終了です。

【!】注意事項

- パスワードを紛失した場合には、バックアップに利用できなくなりますので、
   取り扱いには十分注意してください。
- バックアップファイルは必ず別なメディア(USB や CD 等)にコピーして、
   安全な場所に保管してください。
- 弊社がお客様の秘密鍵ファイルの情報を受け取ることはございません。
   あらかじめご了承ください。

Æ cybertrust

IIS7.0/7.5 CSR 作成/証明書インストール作成手順書(新規・更新用)| Page 29

# <u>SSL 通信の確認</u>



## 8. SSL 通信の確認

サーバー証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

SSL 通信の確認は設定を行っているサーバー以外の Web ブラウザや携帯電話、 スマートフォンなどの携帯端末、「<u>サーバー証明書の設定確認</u>」から行うことを推 奨します。



なお、接続時にセキュリティ警告やエラーが表示される場合は、以下よくある質問の「SSL 通信時のセキュリティ警告やエラーについて」をご参照ください。

≫ SSL 通信時のセキュリティ警告やエラーについて

(t cybertrust