

SureServer/SureServer EV

Microsoft IIS6.0

証明書インストール手順書

(サーバ移行用)

Version 1.4

PUBLIC RELEASE

2016/12/15

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

<u> 改訂履歴</u>

日付	バージョン	内容
2012/6/22	1.0	初版リリース
2013/8/2	1.1	Cybertrust Japan Public CA G3 の提供開始 に伴う修正
2014/1/6	1.2	SureServer(1024bit)の終了に伴う修正
2015/2/9	1.3	クロスルート証明書の変更に伴う修正
2016/12/15	1.4	「はじめに」の記述内容を修正



<u>目次</u>

じめ		4
±=	- 	F
争用	川华1	
1.1.	中間 CA 証明書のダウンロード	5
1.2.	pfx ファイルの保存	5
証明	月書のインストール	6
2.1.	MMC の起動	6
2.2.	スナップインの追加	7
2.3.	中間 CA 証明書のインストール	11
2.4.	pfx ファイルのインストール	14
2.5.	SSL サーバ証明書の適用	19
pfx	ファイルのバックアップ	23
SSI	_ 通信の確認	23
	じめ 事前 1.1. 1.2. 2.1. 2.2. 2.3. 2.4. 2.5. pfx SSI	じめに 事前準備 1.1. 中間 CA 証明書のダウンロード 1.2. pfx ファイルの保存 証明書のインストール 2.1. MMC の起動 2.2. スナップインの追加 2.3. 中間 CA 証明書のインストール 2.4. pfx ファイルのインストール 2.5. SSL サーバ証明書の適用 pfx ファイルのバックアップ SSL 通信の確認



はじめに

(t cybertrust

【!】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 6.0(以下、IIS6.0)」の環境下で pfx ファ イルと中間 CA 証明書ファイルをインストールする手順について解説するドキュメントです。

IIS6.0 単独での動作確認ができていることを前提としております。

実際の手順はお客様の環境により異なる場合があり、IIS6.0 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。

1.<u>事前準備</u>

IIS6.0 ヘインストールする中間 CA 証明書ファイルと pfx ファイル(SSL サーバ証明 書ファイルと秘密鍵ファイル)を準備します。

1.1. 中間 CA 証明書のダウンロード

サーバ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、以下弊社ホームページからダウンロードしてください。

≫ <u>ルート・中間 CA 証明書のダウンロード</u>

また、ご利用商品や必要な証明書の種類がご不明の場合は、以下をご覧く ださい。

≫ どの中間 CA 証明書をダウンロードすればよいですか?

1.2. pfx ファイルの保存

インストールする pfx ファイルを IIS6.0 の任意のディレクトリへ保存します。



2. 証明書のインストール

「Microsoft 管理コンソール (Microsoft Management Console:MMC)」から中間 CA 証明書と pfx ファイル (SSL サーバ証明書と秘密鍵ファイル)のインストールを行います。

2.1. MMC の起動

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、「Microsoft 管理コンソー ル」を開きます。

ファイル名	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(<u>O</u>):	mmc
	OK キャンセル 参照(<u>B</u>)



2.2. スナップインの追加

A) 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。



B) 【スナップインの追加と削除】内の【追加】をクリックします。

スナップインの追加と削除 ? ×
スタンドアロン 拡張
このページを使ってコンソールにスタンドアロン スナップインを追加または削除します。
スナップインの追加先 (S): 🔄 コンソール ルート 📰
[見8月
追加(D) 肖印除(R) バージョン情報(B)
OK ++++++++++++++++++++++++++++++++++++
OKキャンセル



C) 【利用できるスタンドアロン スナップイン】の中から【証明書】を選択し、 【追加】をクリックします。

スタンドアロン スナップインの追加		? ×
利用できるスタンドアロン スナップイン:		
スナップイン	ベンダ	
重ルーティングとリモート アクセス	Microsoft Corporation	
🔣 ローカル ユーザーとグループ	Microsoft Corporation	
Τ ワイヤレス モニタ	Microsoft Corporation	
📄 📄 共有フォルダ	Microsoft Corporation	
▲ 「夜認マネージャ	Microsoft Corporation	
	Microsoft Corporation	_
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Microsoft Corporation	
副 記明書テンプレート	Microsoft Corporation	
🍰 分散ファイル システム	Microsoft Corporation	-
Allows you to configure the NET Framework	k 11	
	× 1.1	
ſ	追加(<u>A</u>) 閉じる	©

D) 【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。

証明書スナップイン			×
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(M)			
· · · · · · · · · · · · · · · · · · ·	C		
	< 戻る(日	次へ(N) >	キャンセル



E) 【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。



F) 【利用できるスタンドアロン スナップイン】の【閉じる】をクリックします。

ス	タンドアロン スナップインの追加		? ×
	利用できるスタンドアロン スナップイン:		
	スナップイン	ベンダ	
	篁 ルーティングとリモート アクセス	Microsoft Corporation	
	🔝 ローカル ユーザーとグループ	Microsoft Corporation	
	Τ ワイヤレス モニタ	Microsoft Corporation	
	🔁 共有フォルダ	Microsoft Corporation	
	🚋 承認マネージャ	Microsoft Corporation	
	1201111月機関	Microsoft Corporation	
	圖 証明書	Microsoft Corporation	
	1220 証明書テンプレート	Microsoft Corporation	
	🍰 分散ファイル システム	Microsoft Corporation	-
	, 「 記印月 ———————————————————————————————————		
	証明書スナップインを使うとユーザー、サービス、ま を表示できます。	たはコンピュータの証明書ストアの	の内容
		<u>(道加(A)</u> 開じる	©]



G) 【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。

スナップインの追加と削除 21×
スタンドアロン 拡張
このページを使ってコンソールにスタンドアロン スナップインを追加または削除します。
スナップインの追加先(S): 🔄 コンソール ルート 💌 💼
THER
説明 証明書スナップインを使うとユーザー、サービス、またはコンピュータの証明書ストアの内容を
3077 C 28 9 0
OK ##\/#/



2.3. 中間 CA 証明書のインストール

A) 【証明書(ローカルコンピュータ)】→【中間証明機関】→【証明書】の順 にクリックします。

※証明書が未登録の場合は【証明書】が表示されないため、【中間証明書機関】をク リックします。



B) 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。

י ארעב 🚡	- עעבו	ル ルート¥証明	唐 ([コーカル コンピュータ))¥中間証明機関¥証明書]	
🚡 ファイル(E)	操作(<u>A</u>)	表示──お	気に入り	10) ウィンドウ(W)	ヘルプ(圧)	
⇔ ⇒ 🖻	すべての	タスク(<u>K)</u>	•	インポートΦ		
间 א ערב 📋	ここから親	fしいウィンドウ	<u>N</u>		発行先 △	
□□··· 🗐 証明書 □□··□□ 個人	新しいタ	スクパッド表示(Ţ)			
⊡… 🧰 信頼	最新の情	鰆報(こ更新(<u>F</u>)				
비 효율 파네	- 一覧のI	.クスポート(<u>し</u>)				
	明書	••••				
白… 🧰 信頼	⊡ 信頼された発行元					
王… 🔜 信頼	きれていない	温明書			1	



C)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。



D) 【ファイル名】ヘインストールする中間 CA 証明書ファイル名を指定し、 【次へ】をクリックします。

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。	
ファイル名(E): C:¥PUBCAG3.cer	
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)	
	-
〈戻る(B) 次へ(N) > キャンセル	



E)証明書ストアに【中間証明機関】が表示されていることを確認し、【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。	
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(1)	
< 戻る(四) 次へ(1)> キャンセル	

F)証明書のインポート ウィザードの完了画面の表示内容を確認し、【完 了】をクリックします。

証明書のインボート ウィザード		×
	証明書のインボート ウィザードの完了	
	証明書のインポート ウィザードが正常に完了しました。	
	70-19-752択した計明者ストア 中間証明機関 内容 証明書	
	ファイル名 C¥PÜBCAG3.cer	
and the second		
	,	
	〈戻る(B) 完了 キャンセル	



G) 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】を押して終 了となります。

証明書の	インボート ウィザード	×
(į)	正しくインボートされまし	た。
	OK	

※SureServer EV[2048bit]・SureServer EV[SHA-2]、および、SureServer[2048bit]用クロ スルート方式では、同様の手順で「クロスルート用中間 CA 証明書」と「中間 CA 証明書」 をインストールしてください。

以上で中間 CA 証明書のインストールは完了です。

2.4. pfx ファイルのインストール

pfx ファイル(SSL サーバ証明書と秘密鍵ファイル)のインストールを行います。

A) 【証明書(ローカルコンピュータ)】→【個人】→【証明書】の順にクリック します。

※証明書が未登録の場合は【証明書】が表示されないため、【個人】をクリックします。





B) 画面の左上の【操作】メニュー→【すべてのタスク】→【インストール】の 順にクリックします。



C)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たへ] をクリックしてください。	
	< 戻る(四) (次へ)(10) キャンセル	_



D) 【ファイル名】ヘインストールする pfx ファイル名を指定し、【次へ】をクリ ックします。

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。	
ファイル名(E):	
C.¥backup.pfx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)	
	_
< 戻る(B) (次へ(N))> キャンセル	

E) 【パスワード】へ pfx ファイルに設定されているパスワードを入力し、【次 へ】をクリックします。

※パスワードは pfx ファイルの作成・エクスポート時に設定した任意の文字列です。
※SSL サーバ証明書のエクスポートを許可する場合は、【このキーをエクスポート
可能にする】にチェックを入れてください。

証明書	ወインボート ウィザード
K7	ワード セキュリティを維持するために、秘密キーはパスワードで保護されていました。
	秘密キーのパスワードを入力してください。
	■ 秘密キーの(保護を建力にする(E)
	このオブションを有外にすると、秘密キーカアブリケーションに使われるたいに睡眠なな状態のれます。
	回 このキーをエカ2 ポート可能(こすろ(M)
	そのバックアップやトランスポードを可能にします。
	< 戻る(B) 「万へ(Q)) キャンセル



F)証明書ストアに【個人】が表示されていることを確認し、【次へ】をクリッ クします。

証明書ストア 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。
Windows (こ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(山)
● 証明書をすべて)次のストア(:配置する(P)
個人 参照(B)
< 戻る(B) (ア次へ(M)) キャンセル キャンセル

G)証明書のインポート ウィザードの完了画面の表示内容を確認し、【完 了】をクリックします。

証明書のインボート ウィザード	×
	証明書のインボート ウィザードの完了
	証明書のインボート ウィザードが正常に完了しました。
	コンザーが選択した証明書ストア 個人
	内容 PFX ファイル名 C¥backup.pfx
and the second	
	< 戻る(B) (三元7) キャンセル



H) 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】を押して 終了となります。



以上で pfx ファイル(SSL サーバ証明書と秘密鍵ファイル)のインストールは 完了です。



2.5. SSL サーバ証明書の適用

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

- A) 【スタート】メニューから【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、IIS マネージャを起動します。
- B) SSL サーバ証明書を適用する Web サイトを選択し、プロパティを表示 します。
- C) 【ディレクトリ セキュリティ】タブ→【サーバー証明書】をクリックして、
 Web サーバー証明書ウィザードを起動します。

既定の Web サイトのブロパティ	<u>? ×</u>
Web サイト イ バフォーマンス ISAPI フィルタ ホーム ディレクトリ ドキュメント ディレクトリ セキュリティ HTTP ヘッダー カスタム エラー	
- 認証とアクセス制御 医名アクセスを有効にし、このリソースの認証方法 を編集します。	
IP アドレスまたはインターネット ドメイン名を使用して このリソースへのアクセス許可を切り替えます。	
·····································	
」 セキュリティで保護された通信	
このリソースへのアクセス時に、セキュリティで保護さ れた通信を要求し、クライアント証明書を有効に します。 このリソースへのアクセス時に、セキュリティで保護さ サーバー証明書(S)… します。 証明書の表示(V)…	
OK キャンセル 適用(A) ヘルプ	



D) Web サーバー証明書ウィザードが表示されますので、【次へ】をクリック します。



E) 【既存の証明書を使用】を選択して【次へ】をクリックします。

IIS 証明書ウィザード	×
サーバー証明書 以下は、Web サイトに証明書を割り当てる方法です。	
この Web サイトに使用する方法を選択してください: 証明書の新規作成(Q) 既存の証明書を使用(A) キー マネージャのバックアップ ファイルから証明書をインボート(Q) .pfx ファイルから証明書のインボート(M) リモート サーバーからこのサイトへの証明書のコピーまたは移動(Y) 	
	キャンセル



F) インストールした SSL サーバ証明書を指定し、【次へ】をクリックします。

IIS 証 使用	明書ウィザード 可能な証明書 Web サーバーに使用可能	な証明書のリストはよ	以下のとおりです。		×
	記明書を選択してください	1			
	発行先	発行元	有効期限	使用目的	フレンド 🔺
	www.cybertrust.ne.jp	Cybertrust Jap	2014/01/11	サーバー認証、ク	dummy
					_
	•				
			< 戻る(B)	次へ(№)>	キャンセル

G) SSL 接続を行う TCP ポート(SSL 接続では通常 443 ポート)を入力し、 【次へ】をクリックします。

IS 証明書ウィザード	×
SSL ボート この Web サイトが使用する TCP ボートを指定してくださ	n. 🚱
この Web サイトが使用する TCP ボート(<u>L</u>): 443	
	戻る(B) (万大へ(M)) キャンセル



H) 適用する SSL サーバ証明書の内容が表示されますので、確認後、【次 へ】をクリックします。

IIS 証明書ウィザード	x
証明書の概要 既存の証明書をインストールします。	
以下の証明書が Web サーバーにインスト・ い。 証明書の詳細: 発行先 発行元 有効期限 使用目的 フレンドリ名 国/地域 都道所県 市区町村 組織 組織単位 (OU)	-ル可能です。インストールするには、D次へ]をクリックしてくださ www.cybertrust.ne.jp Cybertrust.Japan Public CA G3 2014/01/11 サーバー認証.クライアント認証 dummy_site JP Tokyo Minato-ku Cybertrust.Japan Co.Ltd. Technical Devision
	< 戻る(B) (次へ(M)) キャンセル

I) Web サーバー証明書ウィザードの完了の画面が表示されますので、 【完了】をクリックします。



以上で SSL サーバ証明書の設定は完了です。



3. pfx ファイルのバックアップ

pfxファイルは、万が一に備えて必ず別のメディア(CDやUSB等)にコピーして安全な場所に保管してください。

なお、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。

4. <u>SSL 通信の確認</u>

(t cybertrust サーバ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、「サーバ証明書の設定確認」から行うことを推奨しま す。

■ <u>設定確認例</u>
Internet Explorer 8
<sureserver ev[2048bit]=""></sureserver>
🔊 https://ev2048.cybertrust.ne.jp/ 🛛 🙀 🔒 Cybertrust Global Root
<sureserver[2048bit](クロスルート方式を含む)></sureserver[2048bit](クロスルート方式を含む)>
🖉 https://mobile2018.cybertrust.ne.jp/ 🛛 🔒
• Firefox 12.0
<sureserver ev[2048bit]=""></sureserver>
Gybertrust Japan (JP) https://ev2048.cybertrust.ne.jp 🦙 🗸 🧭
< SureServer[2048bit](クロスルート方式を含む)>
cybertrust.ne.jp https://mobile2025.cybertrust.ne.jp 🔶 🔻 🗃
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