秘密鍵のエクスポート手順

秘密鍵のエクスポートは何回でも行うことができます。エクスポートするたびにパスワードを変更することができます。

秘密鍵のファイルは

- ◆法人代表者証明書の場合・・・EDI ツールへの設定、または R3 署名・暗号化ツールへの設定に必要なファイル
- ◆個人証明書の場合・・・申請電子データシステム(ゲートウェイシステム)を利用するパソコンにインポートするために 必要なファイル
- 1. 「個人」タブに表示されている一覧の中から、エクスポートする証明書を選択して「エクスポート」をクリックします。 下記画面の表示の手順は、

「電子証明書の確認手順(MicrosoftEdge 又は GoogleChrome)」 https://www.medis.or.jp/6_pki/manual.html を参照してください。

証明書			×
目的(<u>N</u>):	<すべて>		~
個人 ほかの人	中間証明機関 信頼されたルート	証明機関 信頼された発行元	信頼されない発行元
発行先	発行者	有効期限	フレンドリ名
medis8060	medis8060	2116/10/08	<なし>
TEST MEDIS	SECOM Passport for Me	ember CA11 2019/05/02	<なし>
< インポート(j) 証明書の目的	エクスボート(E)]	> 詳細設定(<u>A</u>)
<\$\`(\)			表示(⊻)
			閉じる(<u>C</u>)

2. 証明書のエクスポートウィザードが表示されたら、「次へ」をクリックします。

← <i>疑</i> 証明書のエクスポート ウィザード	×		
証明書のエクスポート 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証明書ストアからディスクにコピ 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、「次へ」をクリックしてください。			
次へ(N) キャン	セル		

3. 証明書のエクスポートウィザードが表示されたら、「はい、秘密キーをエクスポートします」を選択して、 「次へ」をクリックします。

← ジ 証明書のエクスポート ウィザード	×
秘密キーのエクスボート 秘密キーを証明書と一緒にエクスポートすることができます。	
秘密キーはパスワードで保護されています。秘密キーを証明書と一緒にエクスポートする場合は、パスワードを 入力する必要があります。 証明書と一緒に秘密キーをエクスポートしますか? ●はい、秘密キーをエクスポートします(Y) ○いいえ、秘密キーをエクスポートしません(O)	
次へ(N) キャン	セル

4.「Personal Information Exchange-PKCS #12(.pfx)」を選択し、

「証明のパスにある証明書を可能であればすべて含む」と「すべての拡張プロパティをエクスポートする」 にチェックを入れて「次へ」をクリックします。

※「正しくエクスポートされたときは秘密キーを削除する」にはチェックを入れないでください。

エクフボート ファイルの形 チ		
さまざまなファイル形式で証明書をエクスポートできます。		
使用する形式を選択してください:		
O DER encoded binary X.509 (.CER)(D)		
Base 64 encoded X.509 (.CER)(S)		
〇 Cryptographic Message Syntax Standard - PKCS #7 証	明書 (.P7B)(C)	
□ 証明のパスにある証明書を可能であればすべて含む(I)		
Personal Information Exchange - PKCS #12 (.PFX)(P)		
✓ 証明のパスにある証明書を可能であればすべて含む(U)		
□ 正しくエクスポートされたときは秘密キーを削除する(K)		
✓ すべての拡張プロパティをエクスポートする(A)		
□ 証明書のプライバシーを有効にする(E)	-	
○ Microsoft シリアル化された証明書ストア (.SST)(T)		

5. パスワードにチェックを入れて、任意のパスワードを入力してください。パスワードの確認の欄にも同じパスワードを入力します。 ここで入力したパスワードは忘れないようにしてください。忘れてしまうと、エクスポートした証明書が使用できなくなります。

(その下にある「暗号化」は、そのままで結構です)

セキュリティ セキュリティを維持するために、セキュリティプリンシバルで秘密キーを保護するかパスワードを使用しなけれ げかりません
追加(A)
削除(R)
✓ パスワード(P):
•••••
パスワードの確認(C):
暗号化: TripleDES-SHA1 ✓
次へ(N) キャンセル

6. 参照ボタンをクリックして、任意の保存先とファイル名を指定してください。

<	☞ 証明書のエクスポート ウィザード	×
	エクスポートするファイル 	
	エクスボートするファイルの名前を入力してください	_
	ファイル/名(F): 参照(R)	
	次八(N) キャンセ ノ	,

7. 保存先とファイル名を入れて「保存」をクリックします。

下図は、保存先:デスクトップ ファイル名:秘密鍵 とした例です

 名前を付けて保存 			Х
	ٽ ~	,○ デスクトップの検索	
整理 ▼ 新しいフォルダー		• = = = • = = =	- ?
 ▲ 21ックアクセス ■ デスクトップ * ● ダウンロード * (音) ドキュメント * ■ ピクチャ * 	更新日時	種類	<u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>
			>
ファイル名(り): 秘密鍵			~
ファイルの種類(1): Personal Information Exchange (*.pfx)			~
▲ フォルダーの非表示		保存(S) キ・	ャンセル

- 8. ファイル名に指定した保存先とファイル名が表示されていることを確認して「次へ」をクリックします。
- 9.「完了」をクリックして、「正しくエクスポートでされました」の表示画面で「OK」をクリックします。

← 夢 証明書のエクスポート ウィザード	×	÷	- 🛷 証明書のエクスボート ウィザード		×
エクスポートするファイル エクスポートするファイルの名前を入力してください				証明書のエクスポート ウィザードの完了	
ファイル名(F): C:¥Users¥medis2005¥Desktop¥秘密键.pfx 参照(R)				証明書のエクスポート ウィザードが正常に完了しました。 次の設定が指定されました: <mark>ファイル名 C.YUSersYmedis200</mark> キーのエクスポート はい 証明のパンにあるすべての証明書を含める はい ファイルの形式 Personal Informatic く ▶	
(N) [キー	ンセル			完了(F) 年ャンセ	ะม

指定した場所にファイルが保存されていることを確認してください。 ファイル名の後につく拡張子は『.pfx 』になります。 秘密鍵のファイルは右記のアイコンで表示されます。ファイル容量は 3KB 程度です。 このファイルをバックアップファイルとして保存する場合は、 エクスポート時のパスワードとともに保管してください。

法人代表者証明書について

秘密鍵の拡張子が『.pfx』でも署名暗号化ツールの設定には支障ありません