電子証明書(秘密鍵ファイル)のインストール手順

Г

1. 発行サイトからダウンロードした『EndUser.p12』のファイル または、自身でエクスポートした「秘密鍵ファイル(拡張子が.pfxのファイル)」を開くと、インポートウィザード画面が表示されます。 保存場所は「現在のユーザ」を選択して、「次へ」をクリックしてください。

← 髪 証明書のインポート ウィザード	×
証明書のインポート 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。	
 保存場所 ● 現在のユーザー(C) 	
○ ローカル コンピューター(L) 続行するには、[次へ] をクリックしてください。	
なん(N) キャンチ	11.

2. ファイル名に 開いたファイルまでのパスが表示されていることを確認して「次へ」をクリックしてください。

	\times
← 🖉 証明書のインポート ウィザード	
インボートする証明書ファイル	
インポートするファイルを指定してください。	
	-
ファイル名(F):	
tEdgeDownloads¥ab4e7381-0582-4483-8fba-b7698f250ffb¥EndUser.p12 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)	
次へ(N) キャンセ	JL.

3. パスワードを入力します。

発行サイトからダウンロードした『EndUser.p12』のファイル を開いた場合は、「認証情報パスワード」を入力してください。 自身でエクスポートした秘密鍵ファイル(pfx ファイル)の場合は、エクスポート時のパスワードを入力してください。 インポートオプションは、

「このキーをエクスポート可能にする」と「すべての拡張プロパティを含める」にチェックを入れてください。 入力が終わったら「次へ」をクリックします。

秘密キーの保 セキュ	夏 リティを維持するために、*	秘密キーはパスワードで住	民護されています。		
秘密	ーのパスワードを入力して	てください。			
ーパスワ	- ド(P):				
	ハスワートの表示(D) 				
	秘密キーの保護を強力 このオプションを有効に?	にする(E) すると、秘密キーがアプリ	ケーションで使われる	たびに確認を求められ	ぇます。
	このキーをエクスポート可 キーのバックアップやトラ	「能にする(M) ンスポートを可能にします			1
	仮想化ベースのセキュリ	ティを使用して秘密キー	- を保護する(エクスポ-	-ト不可)(P)	L
	すべての拡張プロパティ	を含める(A)			L

「このキーをエクスポート可能にする」のオプションについて

初期値ではチェックが入っていません。チェック無の状態にすると、パソコンから秘密鍵(pfx ファイル)のエクスポートができなくなります。(エクスポートウィザードの画面で、「はい、秘密キーをエクスポートします」がグレーアウトして選択することができなくなります)

証明	書ストア						
	証明書に	ストアは、証明書	が保管される	システム上の領	域です。		
	Windov	vs に証明書スト:	アを自動的に追	瞿択させるか、	証明書の場所	を指定すること	ができます。
	01	正明書の種類に	甚づいて、自動	的に証明書	ストアを選択する	i(U)	
	0	IPPきたさべてと 証明者ストア:					
							参照(R)

5. 「完了」をクリックしてください。

← 参 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、証明書がインポートされます。	
次の設定が指定されました。 <mark>選択された証明者ストア</mark> ウィザードで自動的に決定されます	画面推移の途中で下記の画面が表示された場合は、
内容 PFX ファイル名 011 11 11 11 11 11 11 11 11 11 11 11 11	「はい」をクリックしてください。
	(この画面は表示されない場合もあります)
	セキュリティ警告
第7(f)	 発行者が次であると主張する証明機関 (CA) から証明書をインストールしようとしています: SECOM Passport for Member CA11 証明書が実際に "SECOM Passport for Member CA11" からのものであるかどうかを検証できません。"SECOM Passport for Member CA11" に 連絡して発行者を確認する必要があります。次の番号はこの過程で役立ちます: 押印 (1), Toologe ひのあります。次の番号はこの過程で役立ちます: 四ルート証明書をインストールすると、この CA によって発行された証明書は自動的に信頼されます。確認されていない拇印付きの証明書をインストールすることは、セキュリティ上、危険です。[はい] をクリックすると、この危険を認 助したことになります。 この証明書をインストールしますか?
	(はい(Y) いいえ(N)

6. 「OK」をクリックしてください。



以上で電子証明書のインストールは完了です。

「電子証明書の確認手順」を参照して、電子証明書がインストールされていることを確認してください https://www.medis.or.jp/6_pki/manual.html