デジサート Class1 S/MIME 証明書取得手順

1. 最初に以下のようなメールがご利用になられるメールアドレスに届きます。

Confirm your email address: DigiCert order
no-reply@digitalcertvalidation.com
We have received a request to validate this e-mail address for inclusion in a DigiCert certificate.
Email Address: Account ID:
Ordered on:
What is next?
Before we can issue your certificate, approve the request to verify that you control this email address.
View the details and complete the request here (link is valid for 24 hours): https://www.digicert.com/link/request-approval/mailbox.php?t
Contact us if you have questions or need to reject the request here: https://www.digicert.com/contact-us/
Thank you, DigiCert Customer Support https://www.digicert.com/contact-us/

「View the details and complete the request here (link is valid for 24 hours):」の下の リンクをクリックして、表示される以下のサイトで「Approve」をクリックしてください。 ※メール内のリンクは受信後24時間以内という期限がございますのでご注意ください。

Please confirm the email mailbox control verification request The email address below was submitted to SSL/TLS Certificate Authority as part of a certificate request. Your confirmation is required before the certificate can be issued. If you find any errors or if you wish to reject this request, please contact SSL/TLS Certificate Authority by phone or email.
Request Details
Email Date Submitted
Approve mailbox control validation request
Your click on the button below will be logically associated with this request and subscriber authorization and in accordance with applicable law will be a legally binding signature indicating you reviewed this request and do represent and warrant that the information provided is true and correct and that you take such action with authority of the Organization/Applicant.
Approve
If this request contains any errors or you want to reject the request, please contact us at +1-801-441-7230 or no-reply@dcv.digitalcertvalidation.com.

2. 次にこのようなメールがご利用になられるメールアドレスに届きます。

	デジサート Class 1 S/MIME 証明書の承認が完了しました
digicert	DigiCert <admin@digicert.com></admin@digicert.com>
	digicert
	Nippon Jimuki Co.,Ltd.
	様
	デジサート 個人用証明書(Class 1 S/MIME)が承認されました。
	次のURLにアクセスし、お早めにデジサート 個人用証明書を取得してください:
	https://www.digicert.com/link/pid-install.php?token=
	∽ 返信み 転送

3.メール内のリンクをクリックしてください。Webブラウザが起動します。 (特にブラウザの制限はありません)

Gener	ate your DigiCe	rt Premium C	ertific	ate		
or techni	cal assistance or to make	corrections, contact yo	our admin	strator.		
DigiCe	rt Personal ID Details					
	名前:					
	Eメールアドレス:					
	組織:					
	サプスクライバー契約:	マスターサービス契約		I agree to the	terms of the subscr	iber agreement
1	Certificate Password:	••••••				
	バスワードの確認:	•••••				
Your Pe you wil	ersonal ID will be valid for I need to contact your org	1 年 from the time it i anization administrato	s issued. or to requ	You have until May 1 est a new email.	7, 2022 to generate	this certificate or
If your v DigiCert	veb server is configured to SHA2 Assured ID CA, as	require "Client Authe well as DigiCert Assure	ntication" ed ID CA-	, you may need to co L.	nfigure it to allow o	lient certs issued by
	new security standards, ar	y client certificate exp	iring on o	r after January 1, 20	20, will be issued u	sing SHA-2 regardless

画面の"名前"、"Eメールアドレス"に間違いがないかご確認ください。

4. マスターサービス契約を確認し、「利用規約に同意する」をチェックします。
Certificate Password(証明書のパスワード)を入力します。
※このパスワードは任意の値をご入力いただけますが、証明書をクライアント環境に インストールする時に使用します。
パスワードを忘れると証明書をインストールできませんのでご注意ください。

5. 証明書を生成する(Generate Certificate)を押下します。 ※完了画面に変わるまでそのままお待ちください。

以下の画面に変わりましたら証明書ファイルの取得は完了です。
 任意のファイル名.p12の証明書ファイルがダウンロードされたことをご確認ください。
 ※p12ファイルは pfxファイル(PKCS#12形式)です。



こちらの画面にならなくても、p12ファイルがダウンロードされていれば完了です。 ブラウザは閉じていただいて問題ありません。

ダウンロードした**p12**ファイルをクライアント環境にインストールする手順は次ページを ご確認ください。 1. ダウンロードされたp12ファイルをダブルクリックします。



2. 起動した証明書インポートウィザードで「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、および証明書夫効リストをディスクから証明書ストアにコピー します。	
	証明機關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。	
	次へ(N) キャンセノ	ŀ

3. インポートするファイル名を指定する画面で「次へ」をクリックします。



4. 証明書取得時に設定したパスワードを入力します。

「このキーをエクスポート可能にする」チェックをONにして「次へ」をクリックします。

秘密	パーの保護 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す。
	秘密キーのパスワードを入力してください。
	- パスワード(P):
	•••••
	パスワードの表示(D)
	インポート オブション(I):
	□ 秘密キーの保護を強力にする(E) このオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。
	ごのキーをエクスポート可能にする(M) キーのバックアップやトランスポートを可能にします。
	✓ すべての拡張プロパティを含める(A)

5.「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」を選び、「次へ」を クリックします。

🛃 証明書のインポー	トウイザード			
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き	t.,	
Windows (2	証明書ストアを自動的(に選択させるか、証明	きの場所を指定すること	ができます。
● 証明書	身の種類に基づいて、自	動的に証明書ストアを	選択する(U)	
○ 証明書	身をすべて次のストアに配	已置する(P)		
証明	書ストア:			
				参照(R)

6.「証明書インポートウィザードの完了」画面が表示されますので、「次へ」をクリックします。

← 夢 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: 	
完了(F) キャンセル	

7.「証明書インポートウィザード」画面が表示されますので、「OK」をクリックします。



クライアント環境への証明書ファイルのインポートは完了です。

メールソフトへの設定については以下のメーカーFAQサイトをご確認ください。

(参考)一般的なメーラーで利用するための参考手順書(デジサート・ジャパンサイト) https://knowledge.digicert.com/ja/jp/solution/SO23911.html