クライアント証明書登録手順書

株式会社電算システム

2010年4月 第一版

(t cybertrust

2011 年 4 月 第二版(証明書更新作業用)

■はじめに

1. クライアント証明書とは

1-1. クライアント証明書概要



 ・パソコンにクライアント証明書を登録頂く事で弊社のASPサービス を利用する際にサーバ側で証明書の有無を確認し、サービスを利用す る権限を判断します。

(クライアント証明書が無いとサービスが利用できません。) 又、情報を暗号化することにより、セキュリティを強固にします。

2. 本手順書の目的

Ct cvbertrust ・上記のようにクライアント証明書をパソコンに登録(インストール) 頂かないと今後はサービスが利用できません。
 お客様には、弊社より「クライアント証明書 登録のお願い」がメールにてご案内されます。
 本手順書は、本メールが通知された後、早期に登録が完了できるように、どのようにクライアント証明書を登録するかを記載しています。

本手順書をご活用頂き、登録期限までの完了を頂ければ幸いです。



■クライアント証明書更新登録手順

本手順書は、InternetExplorer6~8を前提に作成さ せて頂いています。

1. ご案内メールについて

2通のメールがお手元に届きます。

1-1. 証明書発行通知メール

クライアント証明書発行の準備ができたお知らせです。

※このメールは株式会社電算システムのマネージド PKI サービスへ お申し込みいただいた方へ送信しています。 ※お心当りのない方は大変お手数ですが、その旨をご返信ください。

お申し込みの内容に基づきクライアント証明書が発行されました。 以下のアドレスにアクセスしてクライアント証明書を取得してください。

1

【証明書取得申請先 URL】 http://www.dsk-idc.jp/dskmpki/b3

2

【証明書情報】

Common Name: dscaXXXXX Subject: C=JP, OU=[XXX], CN=dscaXXXXX Serial Number: XXXX

cybertrust

(株)電算システム データセンター 認証局担当< ca-sys@densan-s.co.jp >

①をダブルクリックすると『電算システム マネージドPKI』の画面に移ります。この画面は作業を行う為の入口になります。
 ②は、その際に必要となる、リクエストIDです。

1-2.証明書登録依頼メール

クライアント証明書登録の作業のお願いです。

【クライアント証明書更新登録のお願い】

平素は弊社サービスのご利用を賜り、厚く御礼申し上げます。 さて、昨今、個人情報保護法や内部統制対応に見られるコンプライア ンスの取り組み等、企業を取り巻く環境が変化し、企業に求められる 責任もより大きな物となっています。

弊社と致しましてもこの社会環境の変化に対応すべく、現在、ご提供しているサービス に対してクライアント証明書を用いたセキュリティ対策を平成22年5月11日より施し、強化させて頂きました。

この度は、クライアント証明書導入後ほぼ1年が経ち、現在、ご利用 頂いているパソコンのクライアント証明書を更新頂く作業が必要となり ました。

つきましては、下記 URL より手順書を御取得頂き、平成23年4月 30日までに作業を完了させて頂きます様、よろしくお願い致します。 尚、今回は本メールを配布させて頂きましたお客様のみが対象となりま す。他に弊社の他サービスやクライアント証明書を用いたサービスをご 利用頂いていても本メールが届いていないお客様は対象外ですので、本 作業は不要です。

又、今回以降は3年に1度の更新とさせて頂きます。 お忙しい折、大変恐縮ですが、よろしくお願い致します。

【ご連絡事項】

ID: * * * * パスワード: × × × × ※お客様ごとに変わります。

・手順書は、InternetExplorerのバージョン6から8を対象にご用意しています。

※手順書は下記 URL より御取得下さい。

http://www.dsk-idc.jp/dskmpki/manual/dsk-mpki-manual-02.pdf

・お問合せについては、以下までお願いします。

問合せ先 : 株式会社電算システム サポート課

電話番号 : TEL058-279-3458

対応時間 : 祝祭日を除く月曜日から金曜日の午前8:50~12:00、 午後1:00~5:50

(㈱電算システム クライアント証明書登録手順書 | Page 4

(t cybertrust 2. 登録手順

2-1. 登録作業に着手する。

・登録作業は大きく以下の4つの作業です。

- 1) ユーザ認証=証明書を登録できる方の確認(認証) Page5の 2-1 項
- 2) 鍵の取得から保存 Page6~8の2-2項
- 3) 鍵の登録 (ブラウザへのインストール) Page9~11 の 2-3 項
- 4) 『ログアウト』で完了です。 ※2)3)が、クライアント証明書の登録に必要な作業です。
- ・スタートです。 · Page3の証明書発行通知メールに記載されている①アドレスをダブ ルクリックすると以下の画面に移ります。

		tps://ca45	i managedpk	i.ne.jp/De	ensanSys	temCertific	ation Author	ity/pages/		8 4	× 3	Google			5
ァイル(<u>E</u>)	編集(E)	表示(⊻)	お気に入り)(<u>A</u>) ッ	/-ル(<u>T</u>)	ヘルプ(円)						1 97400			
お気に入	0 0	https://c	a45.managed	pki.ne.jp	/DensanS	iystemCerti	f		1	🔄 • 6	3 - 🖃	•	ページ(<u>P</u>)・	・ セーフティ(S)・	· ツール(<u>0</u>) •
SK	株式会	社電	算シフ	ステレ	4										
							ユ -	サ認	耻						
					選択さ	れたポリシ	では、証明	書の発行に	ユーザ認証	[が必要で	きす。				
					ユーサ	f ID とバス	フードを入力	うしてください	10						
					7-+	f ID									
					; _:/75	7					_				
					<u>, , , , , , , , , , , , , , , , , , , </u>			Login							
								LOBIN							
															9
															J
														cybe	ertrust
初期素子	されました											インカーネ	wh		▼ 100%
	21100012							-	2 12 1	the de		122.4	210	* B	10070



(t

2-2. 鍵の取得 ・クライアント認証を行う為の鍵を取得します。 『鍵の取得』を選びます。



『鍵の取得』の画面に移ります。

Ct cvbertrust



・「リクエストID」「パスワード」「パスワードの確認」を入力し、 「Submit」をクリックします。

<u>「リクエスト ID」</u>は、Page3 の証明書発行通知メールにある <u>リクエスト ID</u>を入力します。

<u>「パスワード」</u>は、Page4の証明書発行登録依頼メールにて通知されているパスワードを入力します。

「パスワードの確認」では、上記「パスワード」として入力したものと同じ 内容を入力します。<u>(2度同じパスワードを入力します。)</u>

・次の画面に移ります。

「Download」をクリックします。

🏉 電算システム マネージドPKI - こ利用者をま向け画面 - Windows Internet Explorer	
🚱 👽 🐧 https://ca45 managedpkine.jp/DensanSystemCertificationAuthority/pages/ 🗹 🔒 🐼 🐼 🔀 Google	P+
ファイル(E) 編集(E) 表示(W) お気に入り(A) ツール(D) ヘルブ(H)	
🖕 お気に入り 電算システム マネージドPKI - ご利用者さま向け画面 🍡 🖓 🔹 🖾 - 🖾 🖶 ページ(P) * セーフティ	<u>s)・ ツール(0)・ @・</u>
DSK 株式会社 電算システム	トップへ
	ログアウト
TTD 4.9% /~ rh 2#	
中請储報 <u>一覧</u>	
鍵をタワンロードします。鍵のタワンロードまたはインストールを行うには、 証明書の管理 「Download」ボタンをクリックしてください。	
証明書の取得	
- 鍵の取得 	
あ知らせ	
間、哈拉世連絡先	
ca45.managemki.me.jp	
secured site	
2010-08-30 09:57 JST	
save-key.jsp 😜 インターネット	🚡 🔹 🔍 100% 🔹 💡

- ※ 鍵の取得は、セキュリティ確保の目的から、以下の条件により、証明 書発行から一定期間経過後ロックされ、取得できなくなります。ご注 意ください。
 - 鍵取得後3日経過

Ct

cybertrust

• 証明書発行後30日経過

次の画面に移ります。

「保存」をクリックします。

ファイルの	ダウンロード 🛛 🔀
20771	(ルを聞くか、または保存しますか?
	名前: 200807240000157p12
	種類: Personal Information Exchange
	発信元: mpkidemo
	開K((0) (保存(S) キャンセル
🗹 この種	(類のファイルであれば常に警告する(<u>W</u>)
0	インターネットのファイルは役に立ちますが、ファイルによってはコンピュータに問題を 起こすものもあります。発信元が言頼できない場合は、このファイルを開いたり保 存したりしないでください。 <u>危険性の説明</u>

・保存場所を指定(ご自身でわかりやすい場所=デスクトップ、マイドキュ メント等)し、「保存」をクリックします。

名前を付けて保存					? 🔀
保存する場所(I):	🔁 Sample		~	3 👂 🖻 🛄	
して 最近使ったファイル					
び デスクトップ					
ک ۲۲ ۴キュメント					
ער אד דארב אד					
マイ ネットワーク	ファイル名(<u>N</u>):	200807240000157p12		~	保存(<u>S</u>)
	ファイルの種類(工):	Personal Information Exchange		*	



2-3. 鍵の登録インストール

・次に取得した鍵情報(PKCS#12 ファイル)をブラウザにインストールします。 (Internet Explorer での証明書ストアへの登録)

先ほどPage8で保存した鍵情報(PKCS#12ファイル)をダブルクリックします。下 記のようなダイアログ画面が表示されますので「次へ」をクリックします。



・「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(<u>F</u>):	
C¥bulkdata sample¥sample¥200704200000426.p12 参照(B)	
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)	
〈戻る個) (次へ他) キャンセル	



・PKCS#12ファイルの暗号化パスワードを入力して「次へ」をクリックします。

ここの「パスワード」は、Page7「鍵の取得」で入力したPage4の証明書発行 登録依頼のパスワードです。

証明書のインボート ウィザード	R
パスワード 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。 パスワード(P):	
□ 秘密・マーのFRBを運んにすると、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ます。 このオプションを有効にすると、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ます。	
□こ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。	
〈 戻る 個 (次へ 個) キャンセル	

※他のチェックボックスについてチェックは不要です。

・「次へ」をクリックします。

(t cybertrust

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(U)
○ 証明書をすべて)次のストアに配置する(P)
証明書ストア:
参照(<u>R</u>)
< 戻る(B) (次へ(M)) キャンセル

※ ラジオボタンについては上記のままで問題ありません。

・「完了」をクリックします。

証明書のインボート ウィザード		X
	証明書のインボート ウィザートの完了	
	証明書のインボート ウィザードが正常に完了しました。	
	次の設定が指定されました:	
	選択された証明書ストア ウィザードで自動的に決定されます	
	内容 PFX	
	ノアイ ル2 UUUUU420.p12	
	〈戻る(四) 完了 キャンセル	

「はい」をクリックします。

セキュリテ	(警告) 🛛 🗡
	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:
	Densan System Certification Authority
	証明書が実際に "Densan System Certification Authority" からのものであるかどうかを検証できません。 "Densan System Certification Authority" (ご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:
	提印 (sha1):
	警告: この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。確認されていない相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。ほい1をクリックすると、この危険を認識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?

※上記セキュリティ警告は環境によって表示されない場合があります。

・下記のダイアログが表示されれば完了です。



(t cybertrust

・最後に右上の『ログアウト』をクリック頂き、『ログアウト完了』画面が

でれば作業は完了です。





- 《 ご参考 / クライアント証明書更新登録後の操作 》
 - ・ 証明書の更新作業を正しく完了すると更新前の証明書の有効期限が切れるまで、利用時に以下のように旧・新の 2 つの証明書が選択画面に表示されます。 旧証明書の有効期限が切れるまでの間「dscaXXXXX」の番号の大きい方をご 選択下さい。

ジタル副	明書の選択	?
1	表示しようとしている 書を選択してください	Web サイトでは、ID が必要とされています。証明 [\] 。
	名前	発行者
	dsca00480 dsca00065	Densan System Certification Authority Densan System Certification Authority
		■詳細情報(M) 証明書の表示(V)

※上記、名前はご参考で実際のものとは異なります。

・OKを選択してください。この操作以降は、いつもの利用手順と同じです。

以上

