

書類提出用 端末要件

平成 25 年 6 月

金融庁 総務企画局 企業開示課

- ◆Microsoft Corporation のガイドラインに従って画面写真を使用しています。
- ♦Microsoft、Windows、Windows Vista は、米国 Microsoft Corporationの米国及びその他の国における登録商標又は商標です。
- ◆Oracle と Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文 中の社名、商品名等は各社の商標又は登録商標である場合があります。
- Adobe® product screen shots reprinted with permission from Adobe Systems Incorporated.
- ◆Adobe、Adobe Photoshop、Adobe Illustrator は、Adobe Systems Incorporated の登録商標又は商標です。
- ◆その他、記載されている会社名及び製品名は、各社の登録商標又は商標です。
- ◆本文中では、TM、®、©は省略しています。
- ◆本文及び添付のデータファイルで題材として使用している個人名、団体名、商品名、ロゴ、連絡先、メールアドレス、場所、出来事等は、全て架空のものです。実在するものとは一切関係ありません。
- ◆本書に掲載されている内容は、平成25年6月現在のもので、予告なく変更される可能性があります。
- ◆本書は、構成、文章、プログラム、画像、データ等の全てにおいて、著作権法上の保護を受けています。本書の一部あるいは全部について、いかなる方法においても複写、複製等、著作権法上で規定された権利を侵害する行為をすることは禁じられています。
- ◆本書に記載の会社名及び製品名について、金融庁はそれらの会社、製品等を推奨するものではありません。

4

1 操作環境について

2	事前準	備	5
	2-1	EDINET 利用時の操作環境 ····································	5
	2–2	信頼済みサイトへの登録	6
	2-3	証明書の設定	8
		2-3-1 証明書設定の必要性確認	8
		2-3-2 証明書の設定	0
	2-4	JRE の設定	1
	2-5	電子メールの設定	2
	2-6	フィルタリングソフトを導入している場合	2
3	電子署	名	3
	3-1	電子証明書について1	3
	3–2	公的個人認証サービスのセットアップ	5
		3-2-1 IC カードリーダのドライバセットアップ	6
		3-2-2 署名機能クライアントのセットアップ	6
		3-2-3 公的個人認証証明書登録ツールのセットアップ	!5
	3–3	商業登記	81

3-3-1	事前準備	31
3-3-2	証明書の登録	31

本書について

本書は、「**開示書類等提出者のサイト**」を利用するためのコンピュータの事前準備及び必要な設定変更について説明しています。

EDINET を御利用いただくために

EDINET に開示書類を提出するための前提知識として、一般的な Web ブラウザを使用し、 インターネットが御利用いただける方を対象としています。

本書の表記について

本書は次の環境で作成されています。

OS	Microsoft Windows 7 SP1
ソフトウェア	Microsoft Internet Explorer 9
	JRE Version7 Update7
	Adobe Reader X

本書内に記載されている記号は、次のような意味があります。

表示	意味		表	示	意味
	操作に関連するポイントについ て説明しています。	_			画面の入力又は選択する項目 等を指します。
MEMO	知っておいていただきたいことに ついて説明しています。				画面で表示された項目を指しま す。
③重要	重要事項について説明していま す。必ずお読みください。		K	»	画面の項目名を指します。 例:《EDINET コード》をクリックします。
[]	画面名を指します。 例:[提出者検索画面]が表示されます。		ľ]	キーを押す操作を指します。 例:【F5】キーを押します。

製品名の記載について

本書では、次の略称を使用しています。

名称	略称
Windows 7	Windows 7 又は Windows
Windows Vista	Windows Vista 又は Windows
Windows XP	Windows XP 又は Windows
Windows Internet Explorer 9	Internet Explorer 9 又は Internet Explorer
Windows Internet Explorer 8	Internet Explorer 8 又は Internet Explorer
Windows Internet Explorer 7	Internet Explorer 7 又は Internet Explorer
Adobe Reader X	Adobe Reader X 又は Adobe Reader

<<EDINET の利用に当たって>> EDINET を装い、ユーザ ID、パスワード等の個人情報を盗もうとする偽の Web サイトに注意してください。 このような Web サイトに誘導するメールが届いても、リンク先にアクセスし たり、添付ファイルを開いたりしないように注意してください。 EDINET からメールで個人情報を照会することは一切ありません。 なお、ウィルス対策ソフトを最新の状態にするなど、御利用環境のセキュ リティ対策をおすすめします。

1 操作環境について

「開示書類等提出者のサイト」を利用する場合の、コン ピュータ環境について説明します。

EDINET は、下表に記載のオペレーティングシステム、Web ブラウザ及び「JRE (Java Runtime Environment)」の組合せで動作を確認しています。なお、JRE については JRE7 の 最新バージョンを設定することを推奨しています。

JREの設定手順については、「2-4 JREの設定」を参照してください。

<ハードウェア>

ディスプレイ解像度: 1024×768 以上

くソフトウェアン

	Web ブラウザ			
オペレーティングシステム	Internet	Internet	Internet	
	Explorer 9	Explorer 8	Explorer 7	
	(32bit)			
Windows7 SP1(32bit、64bit のいずれも可)	\bigcirc	\bigcirc	—	
Windows Vista SP2	\bigcirc	0	0	
Windows XP SP3	_	0	0	
JRE	V	ersion7 Update	e7	

※上の表の組合せ以外で EDINET を利用する場合、画面の表示が操作ガイドと一部異なるときがあります。
※EDINET を利用するためには、事前に政府認証基盤(GPKI)のホームページから「アプリケーション認証局の自己署名証明書」を入手する必要があります。手順は「2-3-2 証明書の設定」(p.10)を確認してください。

※PDFの書類を閲覧するためのソフトウェア(例:AdobeReader)が必要です。

2 事前準備 EDINET を利用する前に、御利用いただくコンピュータに事 前準備が必要です。事前準備の手順について説明します。

2-1 EDINET利用時の操作環境

EDINET に接続する際に、御利用いただいているコンピュータで、初期設定から変更する箇所について説明します。



2-2 信頼済みサイトへの登録

Internet Explorer を起動し、[開示書類等提出者のサイト]を「信頼済みサイト」に登録します。「信頼済みサイト」には安全であることがわかっている Web サイトの URL を登録しておくことで、登録された Web サイトからのダウンロード及び実行時の警告が表示されず、また、実行時の制限を受けないようにできます。EDINET の[開示書類等提出者のサイト]を正しく動作するように利用していただくために、信頼済みサイトへ登録します。

1

Internet Explorer を起動します。

2 メニューバーの《ツール》から《インター ネット オプション》をクリックします。



[**インターネット オプション**]が表示され ます。セキュリティの設定をします。





[信頼済みサイト]が表示されます。

5

《次の Web サイトをゾーンに追加する》 に「https://submit.edinet-fsa.go.jp/」と 入力します。

6

7

8

す。

<u>追加(A)</u> (追加)をクリックしま す。

が追加されたことを確認します。

信頼済みサイト
このゾーンに Web サイトを追加/削除できます。このゾーンのすべての Web サイトに、このゾーンのセキュリティの設定が適用されます。
この Web サイトをゾーン(お追加する(D):
https://submit.edinet-fsa.go.jp/
Web サイト(W):
↓ ▼このゾーンのサイトにはすべてサーバーの確認(https:)を必要とする(S)
閉じる(C)



[**インターネット オプション**]に戻りま す。



インターネット オプション ? 💌			
全般 セキュリティ プライバシー コンテンツ 接続 プログラム 詳細設定			
セキュリティ設定を表示または変更するゾーンを選択してください。			
🗌 🥥 🗳 🗸 🚫 📲			
インターネット ローカル イントラネッ 信頼済みサイト 制限付きサイト ト			
このソーンには、コンピューターやファイルに損害を与えない しのシーン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・			
このゾーンに届する Web サイトがあります。			
このゾーンのセキュリティのレベル(L)			
このゾーンで許可されているレベル: すべて			
- 大署名の ActiveX コントロールはダウンロードやる前に言言します。			
🔤 保護モードを有効にする (Internet Explorer の再起動が必要)(P)			
レベルのカスタマイズ(C) 既定のレベル(D)			
すべてのゾーンを既定のレベルにリセットする(R)			

2-3 証明書の設定

EDINET を利用するには、「ルート証明書の更新」プログラムが有効である必要がありま す。「ルート証明書の更新」プログラムが有効でない方は、政府認証基盤(GPKI)のホー ムページから「アプリケーション認証局の自己署名証明書」をダウンロードし、御利用いた だくコンピュータに設定してください。

設定の要否については、「2-3-1 証明書設定の必要性確認」の操作をし確認します。確認した結果、設定が必要である場合は、「2-3-2 証明書の設定」の操作をします。

2-3-1 証明書設定の必要性確認

EDINET の [開示書類等提出者のサイト] に接続し、「アプリケーション認証局の自己署名証 明書」を手動で設定する必要があるかを確認します。



3

[セキュリティの警告]が表示される場 合は、「2-3-2 証明書の設定」の操作 が必要です。

《ここをクリックしてこの Web ページを閉 じる》をクリックして Web ブラウザを終了 します。





OK

2-3-2 証明書の設定

政府認証基盤(GPKI)のホームページから、「アプリケーション認証局の自己署名証明書」 をダウンロードし、御利用いただくコンピュータに設定します。

1

Web ブラウザを起動します。

2

政府認証基盤(GPKI)のホームページ に接続し、「アプリケーション認証局の 自己署名証明書」をダウンロードし、設 定します。

《アプリケーション認証局》をクリックし、 以降の操作は、画面の指示に従ってく ださい。

政府認証基盤(GPKI)の ホームページ

MEMO

政府認証基盤(GPKI)のホームページの URL は、https://www.gpki.go.jp/ です。

政府認証基盤(GPKI)のホームページ及 び「アプリケーション認証局の自己署名 証明書」の設定に関する質問は、政府認 証基盤(GPKI)のホームページに記載さ れている、《お問い合わせ》より確認して ください。



※本画面は 2013 年 3 月現在のものです。

2-4 JREの設定

EDINET に書類提出する場合は、事前に Oracle Corporation の「JRE(Java Runtime Environment)」のインストールが必要です。

^{*}● JRE(Java Runtime Environment)のダウンロードサイト

JRE(Java Runtime Environment)は、次のホームページからダウンロードできます。

※次のホームページは Oracle Corporation で運営されており、金融庁が運営しているものではありません。このアドレスは 2013 年 3 月時点のものです。

http://www.java.com/ja/download/

1

Internet Explorer を起動し、Java のダ ウンロードサイトを表示します。

2

画面中央にある「無料 Java のダウン ロード」ボタンをクリックします。

3

以降の操作は、表示される画面の指示 に従ってください。



インストールができない場合は、自社の システム管理者に御相談ください。



2-5 電子メールの設定

EDINET では、電子メールを利用して、開示書類等提出者に迅速情報を提供します。御 利用のコンピュータから利用が可能な電子メールアドレスを開示書類等提出者ごとに取 得してください。電子メールアドレスは、EDINET利用届出時に入力が必要になります。

2-6 フィルタリングソフトを導入して いる場合

フィルタリングソフトを導入している場合で、EDINET に書類を提出するときは、次の URL がアクセスできるように設定してください。

<EDINET>

http://submit.edinet-fsa.go.jp/

https://submit.edinet-fsa.go.jp/

https://submit-sorry.edinet-fsa.go.jp/

<政府認証基盤(GPKI)>

https://www.gpki.go.jp/

また、EDINET での書類提出にあたり、JRE (Java Runtime Environment) 及び Adobe Reader が必要となります。御利用いただくコンピュータに事前にインストールしておくか、又は それぞれのダウンロードサイトをアクセスできるように設定してください。



EDINET に書類提出する際に、電子署名を付与して提出す る場合の電子証明書、事前準備について説明します。 ※なお、書類提出時の電子署名の付与は任意です。

3-1 電子証明書について

書類提出時に、電子署名を付けて提出する場合は、事前に電子証明書を入手しておく必要があります。

電子証明書は「政府認証基盤(GPKI: Government Public Key Infrastructure)」が相互認証 した次の民間認証局から発行されている電子証明書を使用してください。

民間認証局の一覧(2	2013 年 3 月時点)
------------	---------------

認証局(会社名)	サービス名	証明書タイプ
電子認証登記所	商業登記認証局	
日本電子認証株式会社	AOSign サービスに係る認証局	IC カード
東北インフォメーション・システムズ	TOiNX 電子入札対応認証サービスに係る	
株式会社	認証局	
	TDB 電子認証サービス TypeA に係る認	
	証局	
	セコムパスポート for G-ID に係る認証	
	局	$FD, IC \mathcal{N} = F$
ジャパンネット株式会社	電子入札コアシステム用電子認証サー	IC h - K
	ビスに係る認証局	
地方公共団体による公的個人認証	地方公共団体による公的個人認証サー	
サービス	ビス	
	CTI 電子入札及び申請届出対応電子認証	
株式云社中電シーティーティ	サービスに係る認証局	
	税理士証明書発行サービスに係る認証	
口平饥埕上建百云	局	
株式会社 NTT ネオメイト	e-Probatio PS2 サービスに係る認証局	IC カード

認証局(会社名)	サービス名	証明書タイプ
	日本土地家屋調査士会連合会認証サー	
口本工地家座調査工会建立会	ビスに係る認証局	

3-2 公的個人認証サービスのセット アップ

EDINET に書類提出する際に、公的個人認証サービスから発行された署名を付与して提出する場合の事前準備について説明します。

事前に次のドライバ又はアプリケーションソフトウェアを準備します。

事前に準備するもの	説明
□ IC カードリーダドライバ	IC カードリーダをパソコンで使用できるようにする
	ファイルを「 IC カードリーダドライバ 」といいます。パ
	ソコンに接続すると、自動セットアップされる場合が
	あります。その場合は不要です。IC カードリーダの
	ホームページ、取扱説明書等で確認し、入手してくだ
	さい。
□ 署名機能クライアント	EDINET の [開示書類等提出者のサイト] から入手しま
	す。
□ 公的個人認証証明書登録ツー	EDINET の [開示書類等提出者のサイト] から入手しま
μ	す。

事前に準備したものを使用し、次の手順でセットアップを進めます。

1 IC カードリーダドライバのセットアップ

電子証明書が登録された IC カードを読み込むためのカードリーダをセットアップします。メーカーによってはカードリーダをパソコンに接続すると、自動セットアップされる場合があります。

2 署名機能クライアントのセットアップ

EDINET の[**開示書類等提出者のサイト**]から署名機能クライアントをダウンロードし、 セットアップします。

3 公的個人認証証明書登録ツールのセットアップ

EDINET の [開示書類等提出者のサイト] から公的個人認証証明書登録ツールをダウン ロードし、セットアップします。

3-2-1 ICカードリーダのドライバセットアップ

IC カードリーダのドライバをセットアップし、使えるようにします。 使用するパソコンに、IC カードリーダを接続すると自動セットアップされる場合があ ります。自動セットアップの場合は、しばらく待つとドライバのセットアップが完了しま す。それ以外の場合は、IC カードリーダを提供しているメーカーのホームページ又は取 扱い説明書を確認して、手順に従ってドライバをセットアップしてください。

3-2-2 署名機能クライアントのセットアップ

EDINET からダウンロードした「署名機能クライアント」をセットアップします。

「署名機能クライアント」は、EDINET の[開示書類等提出者のサイト]にある「トップメニュー」 の「推奨端末仕様」から「署名機能クライアントダウンロード」をクリックし、ダウンロード します。



セットアップの手順は次のとおりです。

- (1) ダウンロードした「Client.zip」を解凍します。
- (2) セットアップファイルの署名を確認します。
- (3) 署名機能クライアントをセットアップします。

(1) ダウンロードした「Client.zip」の解凍

解凍ツールを利用する場合は、ツールの手順に従ってください。



「setup.exe」ファイルが表示されま す。



POINT

Windows の設定が、ファイルの拡張子を 表示する設定になっている場合は右の 図のように「setup.exe」と表示され、ファ イル名の後ろに拡張子「.exe」が表示さ れます。表示しない設定の場合「setup」 と表示されます。



(2) セットアップファイルの署名の確認

セットアップを実行するファイル(setup 又は setup. exe)の発行元が正しいことを確認します。ClientCS 及び ClientUS のそれぞれの setup ファイルを確認してください。

1

「ClientCS」フォルダ又は「ClientUS」 フォルダにある「setup.exe」ファイルを 右クリックし、ショートカットメニューの 《プロパティ》をクリックします。

※本項では、「ClientCS」フォルダの setup ファ イルの署名を確認する手順のみを説明して います。「ClientUS」フォルダも同じ手順で確 認してください。



[setup.exe のプロパティ] が表示され ます。

2

《デジタル署名》タブをクリックし、《署名 の一覧》から署名をクリックします。

3

______詳細(D)_____(詳細)をクリックしま す。

Setup.exeのプロパティ
全般 互換性 デジタル署名 セキュリティ 詳細 以前のバージョン
署名の一覧
署名者名: 電子メール アド タイムスタンプ
Financial Servic利用不可 利用不可
[詳細(D)
OK キャンセル 適用(A)

[デジタル署名の詳細]が表示されま す。

4

《全般》タブを表示します。《署名者の情 報》の《名前》が「Financial Services Agency」となっていることを確認し、 証明書の表示(V) リックします。

デジタル署名の詳細		? 💌
全般 詳細設定		
デジタル署 このデジタル	名情報 署名は問題ありません。	
- 署名者の情報(S)		
名前:	Financial Services Agency	
電子メール:	利用不可	
署名時刻:	利用不可	
	証明書の表示の	v)
-副署名(U)		
署名者名:	電子メール アド タイムスタンプ	
	======(D)	
		OK

[証明書] が表示されます。

5

《全般》タブの「発行先」が「Financial Services Agency」となっていることを確 認します。

6

《証明のパス》タブをクリックします。

証明書					
全般 詳細 記明のパス					
正明書の情報					
この証明書の目的:					
 ソフトウェアがソフトウェア発行者の送信であるか確認する 公開後のソフトウェアの変更を禁止する 					
ZAMARY////JI/V/SCCTTL/O					
*詳細は、証明機関のステートメントを参照してください。					
発行先 : Financial Services Agency					
発行者: ApplicationCA					
有効期間 2012/12/19 から 2015/12/18					
· 証明書のインストール(D 発行者のステートメント(S)					
証明書の詳細について表示します。					

[証明のパス] タブが表示されます。

7 《証明のパス》の《Japanese Government ApplicationCA》を選択し 証明書の表示(V) (証明書の表示)を クリックします。



[証明書] が表示されます。

8

《 全 般 》タブ の《 発 行 先 》が 「ApplicationCA」となっていることを確認 します。

9

《詳細》タブをクリックします。

証明書	x
全般 詳細 証明のパス	
正明書の情報	1
この証明書の目的:	
 ソフトウェアがソフトウェア発行者の送信であるか確認する 公開後のソフトウェアの変更を禁止する 	
発行先 : ApplicationCA	
発行者: ApplicationCA	
有効期間 2007/12/13 から 2017/12/13	
発行者のステートメント(S)	
証明書の詳細について表示します。 	
ОК	

[詳細] タブが表示されます。

10 一覧から《拇印》をクリックします。 表示される拇印の内容を確認します。

操作1 に戻り、同様の手順で 「ClientUS」フォルダのセットアップ ファイルの署名も確認します。

証明書		×
全般 詳細 証明のパス		
表示(S): <すべて>	•	
フィールド	値	*
■ キー使用法 ■ 基本制限 ■ 共和ロルゴルブム	Certificate Signing, Off-line C Subject Type=CA, Path Lengt shal	
時印	7f 8a b0 cf d0 51 87 6a 66 f3	
□ フレフトリ名 □ 拡張キー使用法 (プロパティ)	Japanese Government Applic サーバー認証、クライアント認証、	E
7f 8a b0 cf d0 51 87 6a 66 f3 36	i Of 47 c8 8d 8c d3 35 fc 74	
証明書の詳細について表示します。	「プロパティの編集(E)) ファイル	(ट⊐ピー(C)
		ОК

(3) 署名機能クライアントのセットアップ

署名機能クライアントをセットアップします。

「ClientCS」フォルダのセットアップを実行後、「ClientUS」フォルダのセットアップを 実行します。

1

「ClientCS」フォルダの「setup.exe」をダ ブルクリックします。

※本項では、「ClientCS」フォルダの setup ファ イルのセットアップ手順のみを説明していま す。「ClientUS」フォルダも同じ手順でセット アップしてください。



POINT

Windows の設定が、ファイルの拡張子を 表示する設定になっている場合は右の 図のように「setup.exe」と表示され、ファ イル名の後ろに拡張子「.exe」が表示さ れます。表示しない設定の場合「setup」 と表示されます。

整理 • 📑 開く 書き込む	- 45	しいフォルダー			III • 📶	
🚖 お気に入り	-	名前	更新日的	橙圳	サイズ	
🎉 ダウンロード		🛃 setup.exe	2013/03/21 19:46	アプリケーション	5,317 KB	٦.
デスクトップ 10日 最近表示した場所				3		
🧊 ライブラリ						
◎ ドキュメント						
10000	E					
🚼 ビデオ						
1 ミュージック						
帰 コンピューター						
🏝 ローカル ディスク (C:)						
□= ローカル ディスク (D:)						
🗣 ネットワーク						

「Formcoordinator クライアント部品(署 名共通) ウィザードへようこそ] が表示 されます。

2 次へ(N)> (次へ)をクリックします。



[Formcoordinator クライアント部品(署 **名共通) セットアップタイプ** が表示さ れます。

名共通) セットアッフタイフ」 か表示されます。	セットアップ タイブ ご利用方法に合わせて最適なセットアップ タイプを選択してください。		
3 《セットアップタイプ》は「すべて」を選択 し、 <u>沐へ(N)></u> (次へ)をクリックしま す。	セットアップ タイプを選択してください。		
אַגאָא POINT			
インストール機能又はインストール先を 指定できます。	InstallShield < 戻る(B) 次へ(N) > キャンセル		

🗒 Formcoordinatorクライアント部品(署名共通) - InstallShield Wizard

×

4

インストールを開始します。 インストール(1) (インストール)をクリック します。



インストールが開始されます。

😸 Formcoo	ordinatorクライアント部品(署名共通) - InstallShield 👝 💿 🕰
Formcoord 選択した	linatorクライアント部品(署名共通) をインストールしています ・プログラム機能をインストールしています。
1	InstallShield ウィザードは、Formcoordinatorクライアント部品(署名共通) をインストールしています。しばらくお待ちください。
	ステータス:
InstallShield –	< 戻る(B) 次へ(N) > キャンセル

インストールが完了すると、「ウィザー ドを完了しました」とメッセージが表示 されます。

5 インストールを終了します。 <u>
完了(F)</u>(完了)をクリックします。

署名機能クライアント (ClientCS) の セットアップが完了しました。

操作 1 に戻り、同様の手順で、 「ClientUS」をセットアップします。







署名機能クライアントソフトが不要になった場合は、アンインストールします。

コントロールパネルの「プログラムのインストールまたは変更」から「Formcoordinator クライアント部品(署名機能)」 を選択し、アンインストールします。



3-2-3 公的個人認証証明書登録ツールのセットアップ

EDINET からダウンロードした「公的個人認証証明書登録ツール」をセットアップします。 「公的個人認証証明書登録ツール」は、EDINET の[開示書類等提出者のサイト] にある 「トップメニュー」の「推奨端末仕様」をクリックし、ダウンロードします。



セットアップの手順は次のとおりです。

- (1) ダウンロードした「JPKIRegistCert.zip」を解凍します。
- (2) セットアップファイルの署名を確認します。
- (3)「JPKIAppli02-04.exe」で利用者クライアントソフトをセットアップします。
- (4) IC カードリーダを設定します。
- (5)「JPKIRegistCert.exe」で IC カードの電子証明書を Web ブラウザに登録します。

(1) ダウンロードした「JPKIRegistCert.zip」の解凍

解凍ツールを利用する場合は、ツールの手順に従ってください。



JPKIAppli02-04 及び JPKIRegistCert

POINT

両方をセットアップします。セットアップす る順序は「JPKIAppli02-04」をセットアッ プ後、「JPKIRegistCert」をセットアップし ます。

拡張子の表示

2 偏の項目

ネットワーク

POINT

Windows の設定が、ファイルの拡張子を表示する設定になってい る場合は上の図のように「JPKIAppli02-04.exe」と表示され、ファイ ル名の後ろに拡張子「.exe」が表示されます。表示しない設定の 場合「JPKIAppli02-04」と表示されます。

(2) セットアップファイルの署名の確認

セットアップを実行するファイル(JPKIAppli02-04 及び JPKIRegistCert)の発行元が 正しいことを確認します。操作の手順は「(2) セットアップファイルの署名の確認」(p.18) を参照してください。

(3) 利用者クライアントソフトのセットアップ

利用者クライアントソフトをセットアップします。

利用者クライアントソフトのセットアップは、「公的個人認証サービス ポータルサイト (http://www.jpki.go.jp/index.html)」の「利用者クライアントソフトのダウンロード (http://www.jpki.go.jp/download/index.html)」を参照してください。

▶ 事前の準備	○ 利用者クライアント ソフトのダウンロード	◎ 電子申請にあたって	 パスワードの失念や 紛失、有効期間等 		
<u>-ップページ</u> > 利用者クライアントソフト	のダウンロード				
▶ 利用者クライアントソフトの ダウンロード	step1 住基カード取得 電子証	step3 ICカードリーダ ライタの用意	TEP4 パソコンのセット アップ		
ダウンロードとインストール (Windowsをご利用の方)	↓ 利田老クライアン	トソフトのダウンロー	3		
ダウンロードとインストール (Macintoshをご利用の方)		利用者クライアントソフトとは、	- 公的個人認証サービスを利用した行		
利用者クライアントソフトの利用 ▶ 方法(Windowsをご利用の方)		政手続き等を行うときに住民基本台帳カード(ICカード)に記録され た電子証明書を利用するためのソフトウェアです。			
利用者クライアントソフトの利用 う法(Macintoshをご利用の方)					
▶ 公的個人認証サービスとは	7				
▶ よくあるご質問		 利用者クライアントソフト 	に関するお知らせ		
▶ お問い合わせ					
	ダウンロードとイン	ストール			
	ご利用のパソコン環境に合っ	た利用者クライアントソフトをダウン	ノロードしてください。		
	•				



公的個人認証証明書登録ツールの利用者クライアントソフトが不要になった場合は、アンインストールします。 アンインストールの手順は、「利用者クライアントソフトのダウンロード(http://www.jpki.go.jp/download/index.html)」 を参照してください。

(4) IC カードリーダの設定

利用者クライアントソフトで IC カードリーダを設定します。IC カードリーダをコン ピュータに接続し、IC カードをセットします。

1	₩ マニュアル	ミュージック	
《スタート》から「公的個人認証サービ	 メンテナンス リンタッチボタン設定 	コンピューター	
ス」の「ユーティリティ」の「IC カードリー	→ 公的個人認証サービス	コントロール パネル	
ダライタ設定」をクリックします。	JPKI利用者ソフト Jューティリティ	デバイスとプリンター	
	ICカードリーダライタ設定 は、lava実行環境への登録	既定のプログラム	
	いたいのでは、1000000000000000000000000000000000000	ヘルプとサポート	
	▲ 前に戻る		
	プログラムとファイルの検索	シャットダウン ▶	

[ICカードリーダライタ設定]が表示され ます。

2

使用する IC カードリーダライタの種類を 選択します。 ※ここでは USB 経由で接続する IC カードリー ダライタを選択します。





確認メッセージが表示されます。





(5) IC カードの電子証明書を Web ブラウザに登録

接続された IC カードリーダに IC カードを挿入し、IC カードに登録されている電子証 明書を Web ブラウザに登録します。「(1) ダウンロードした「JPKIRegistCert.zip」の解凍」 (p.26) でダウンロードした「JPKIRegistCert」ファイルを使用して登録をします。



[**ログイン**]が表示されます。

3 IC カードの《パスワード》を入力し、 □K (OK)をクリックします。



メッセージ画面が表示され、自動的に 閉じられます。

証明書が Web ブラウザに登録された ことを確認します。



4

Web ブラウザを起動し、メニューバーの 《ツール》から《インターネット オプショ ン》をクリックします。



[インターネット オプション]が表示され ます。

5

《コンテンツ》タブをクリックします。

6 証明書(C) (証明書)をクリッ クします。

インターネット オプション
全般 セキュリティ プライバシー コンテンツ 接続 プログラム 詳細設定
保護者による制限
閲覧できるインターネットのコンテンツを指 保護者による制限(P) 定します。
コンテンツ アドバイザー
規制システムを使用すると、このコンピューターで閲覧できるインターネットの 内容を指定することができます。
- · · · · · · · · · · · · · · · · · · ·
[] 証明書 ———————————————————————————————————
暗号化された接続と識別のための証明書を設定します。
SSL 状態のクリア(S) 証明書(C) 発行元(B)
オートコンプリート
オートコングリートによって、Web ページで前回 入力した内容を、入力中に補完できます。
フィードと Web スライス
フィードと Web スライスは、Web サイトの更新さ 設定(N) れたコンテンツを Internet Explorer やその他の プログラムで表示します。
OK キャンセル 適用(A)

[証明書]が表示されます。 IC カードの電子証明書が一覧に追加 されていることを確認します。

証明書					×
目的(N)): (<	<i>ব</i> ে<>			•
個人	ほかの人 中間証明	明機関 信頼されたルート	那根関 信	頼された発行元 信	頼されない発行元
発行	行先	発行者	有効期限	フレンドリ名	
-	098098098098090 nim.	Registrar of Tokyo Lo	2014,(01,((1 26)	
5	2012	the Governor of Kana	2015/12/		
· · ·					
「インポ	ペート(D) エクスポ・	ート(E) 肖邶余(R)			詳細設定(A)
			_		
<すべ	T>				
	-				表示(V)
証明書	の詳細について表示し	<u>ます。</u>			閉じる(C)

3-3 商業登記

EDINET に書類提出する際に、商業登記の署名を付与して提出する場合の事前準備について説明します。

3-3-1 事前準備

電子証明書を事前に入手してください。 既に入手済みの方は、証明書の期限切れ、失効等がないか、確認してください。 ※証明書が期限切れ、失効等している場合、書類に署名を付与する操作の際にエラーとなります。

3-3-2 証明書の登録

証明書を Web ブラウザに登録します。





< 戻る(B) 次へ(N) >

キャンセル

[インポートする証明書ファイル]が表示 されます。

6

参照(B)...(参照)をクリックし、Web ブラウザに登録する証明書の保存先を 指定します。



[パスワード]が表示されます。 ※表示されない場合は操作9に進みます。

8

証明書のパスワードの指定が必要な場合は、パスワード入力画面が表示されます。《パスワード入力画本表示されます。《パスワード》を入力し、 (次へ(N)> (次へ)をクリックします。

エット・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	1 リート 書ファイル イルを指定してください。	
ファイル名(E): D:¥cert¥sha1-2	06goodp12	
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)		
証明書ファイルの形式の	「詳細について表示します。	
	< 戻る(B) 次へ(N) > キャンセル	

証明書のインポート ウィザード	
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す。 	
秘密キーのパスワードを入力してください。	
紀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。	
フライベート キーの保護の詳細について表示します。	
(戻る(B) 次へ(N) > キャンセル	1

[証明書ストア]が表示されます。

9

証明書を配置するストアを指定し、 (次へ(N)> (次へ)をクリックします。



POINT

指定がなければ、既定のまま操作を続けてください。

証明書のインボートウィザード	x
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 (ご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。	
◎ 証明書の種業額に基づいて、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	
個人 参照(R)	
証明書ストアの詳細を表示します。	
< 戻る(B) 次へ(N) > キャンセル	

[証明書のインポートウィザードの完了] が表示されます。

10 証明書のインポートが完了します。 <u>完了</u>(完了)をクリックします。



[セキュリティ警告]が表示されます。

11

内容を確認し、<u>(はい(Y)</u>(はい)をクリックします。

ルート証明書のインストール POINT

電子証明書発行者の証明機関からルー ト証明書がインストール済みの場合は、 本メッセージは表示されません。 操作 12 に進んでください。本メッセージ が表示された場合は、本メッセージ内に ある拇印をメモし、操作 13 以降の手順で 拇印を確認してください。



確認メッセージが表示されます。





[証明書] が表示されます。

13

《個人》タブをクリックし、一覧に証明書 が登録されていることを確認します。

14

証明書の内容を確認します。証明書名 をダブルクリックします。

証明書				
目的(N): (3 個人 ほかの人 中間調明)	すべて> 月機関 信頼されたルート記	[明機関│信9	頼された発行元	▼
発行先	発行者 Registrar of Tokyo Le	有効期限 2014/01/…	フレンドリ名 くなし>	
インボート(0) 「エクスボー	-ト(E) 肖耶余(R)]		[詳細設定(A)
証明書の目的		_		
				表示(V)
証明書の詳細について表示し	<u>‡す。</u>			開じる(C)

[証明書] が表示されます。

15

《証明書のパス》タブをクリックします。

16

《証明書のパス》のルート証明書をク リックし、 証明書の表示(V) (証明書 の表示)をクリックします。

証明書 文字
全般 詳細 証明のパス
- 証明のパス(P)
Registrar of Tokyo Legal Affairs Bureau
証明書の表示(∨)
証明書の状態(S):
この証明書は問題ありません。
」 証明書のパスの詳細について表示します。
ОК

[証明書] が表示されます。

17

《全般》タブの《発行先》を確認します。

18

《詳細》タブをクリックします。



19

ー覧から《拇印》をクリックします。 表示される拇印の内容を確認します。

20

確認を終了します。

証明書				
全般 詳細 証明のパス				
表示(S): <すべて>	•			
フィールド	值			
 新キー使用法 秘密キーの使用期間 基本制限 1.2.392.100300.1.1.2 毎日アルリズム 	Digital Signature, Key Enciph 30 22 80 0f 32 30 31 31 30 3 Subject Type=CA, Path Lengt 0c 18 e6 9d b 1 e4 ba ac e6 b sha1 ==			
	e7 f2 38 2f d7 a2 af e4 2d 50			
e7 f2 38 2f d7 a2 af e4 2d 50 a8 41 c6 9f 93 8a fc ab 90 24				
<u>証明書の詳細について表示します。</u>	プロパティの編集(E)) ファイルにコピー(C)			
	ОК			







(次世代 EDINET 案)

平成 25 年 6 月