

# EINS/PKI for EDI 証明書

## <u>発行サービス</u>

## 証明書発行マニュアル

## (クライアント証明書/法人向け)

■ 第 3.08 版 2024 年 4 月 16 日

■ 株式会社 インテック



### ■ 更新履歴

Ver	更新日付	内容
1.00	2007/9/25	初版作成
2.00	2009/10/31	IEの設定変更の一部手順変更
2.01	2010/4/20	動作対象に Windows 7 を追加
2.02	2010/8/12	Windows 7、VISTA における証明書発行時のポップアップを修正
2.03	2010/11/8	鍵長が 1024bit 以下の場合の警告について追記
2.04	2010/11/19	IE のアドオン実行について修正
2.05	2011/6/7	証明書の鍵長が 2048bit に制限される点について追記
2.06	2013/4/1	動作対象に Windows 8 を追加
2.07	2014/1/6	・動作対象に Windows 8.1 を追加
		・for EDI リポジトリの URL 変更
		・ EINS/PKI 事務局の電話番号、E-mail アドレスの変更
2.08	2014/6/30	コーポレートマークの変更
2.09	2015/10/1	SHA-2 対応に合わせて画面のキャプチャを変更
2.10	2016/7/1	コーポレートマークの変更
2.11	2017/10/3	<ul> <li>・証明書発行画面変更に合わせて画面のキャプチャを変更</li> </ul>
		・ PIN ファイルの送付方法について変更
2.12	2019/6/7	・サービス名称変更に伴い、一部文言を修正
2.13	2019/11/27	・お客様専用マイページ開設に伴い、一部文言を修正
2.14	2020/9/16	・EINS/PKI 事務局の問合せフォーム URL を修正
2.15	2020/11/24	・EINS/PKI 公式サイト FAQ URL を修正
3.00	2022/6/14	・証明書発行用対応ブラウザ変更に伴う証明書ダウンロード手順の修
		正
3.01	2022/7/4	<ul> <li>クライアント証明書発行フローを修正</li> </ul>
3.02	2022/10/25	・「3. こんな時は」を追加
3.03	2022/12/1	・申請の流れを修正
3.04	2023/2/8	・ ルート認証局証明書、中間認証局証明書のインストール手順を追記
3.05	2023/3/22	・「個人」タブ部分の画像キャプチャ変更
3.06	2023/4/5	<ul> <li>         ・         証明書発行手順に追記         </li> </ul>
		・ 証明書発行後の確認について、題名を修正
		・証明書発行後の確認について、一部文言、画面を修正
3.07	2023/9/21	・証明書発行後の確認について、OpenSSL v3.1 系を使用するように
		一部文言、画面を修正



EINS/PKI for EDI 利用者証明書発行マニュアル

3.08 2024/4/16 ・ 証明書発行手順に証明書のバックアップの推奨を追加



### 目次

はじ	じめに	5
1.	利用者証明書の発行	7
2.	証明書発行後の確認	)
3.	こんな時は	3
3–1	OpenSSL をインストールする18	3
3–2	証明書ファイル(pfx 形式)から秘密鍵ファイルを取得する	1
3–3	証明書ファイル(pfx 形式)から秘密鍵を除いた証明書ファイル(pem 形式)を取得する 2	1
4.	トラブルシューティング	2



#### はじめに

EINS/PKI for EDIとは、株式会社インテックが運営し経済産業省・流通システム標準化事業にて規定されたセキュ リティ規格(共通認証局 証明書ポリシー)に準拠する認証局(以下、本認証局)による証明書発行サービスです。 本書ではクライアント証明書の発行手順についてご説明いたします。

※ サーバ証明書はメールにて証明書データを送付いたします。詳細は証明書申請マニュアルをご参照ください。

本手順による証明書発行は、次の流れになっております。

- ① 利用者証明書の発行
- ② 発行後の確認
- ※ ダウンロードした証明書ファイルを EDI アプリケーションにインストールする手順については 別途、EDI アプリケーションのマニュアルをご確認ください。

申請担当者様あてに E-mail にて送付しております、「EINS/PKI for EDI 証明書発行用データ送付のお知らせ」に 以下のものが添付されていることを確認してください。

● 証明書発行時の認証用 利用者 ID・PIN ファイル

また、証明書の発行を行うには、専用の Web サイトにアクセスする必要があります。 申請担当者様あてに「EINS/PKI for EDI 証明書発行用 URL のお知らせ」と書かれたメールをお送りしております ので、"<u>証明書発行用 URL</u>"をご確認ください。

本サービスのご利用に必要なブラウザにつきましては、以下の EINS/PKI 公式サイトをご確認ください。 ・EINS/PKI 公式サイト > よくある質問 > 「EINS/PKI サービスでサポートしている環境を教えてください。」 https://www.einspki.jp/new\_faq/



・クライアント証明書発行までのフロー





#### 1. 利用者証明書の発行

- 1) 利用者証明書の発行には、「利用者 ID」と「PIN」、並びに「証明書発行用 URL」の情報が必要になりま すので、事前にご確認ください。
  - ※ 「証明書発行用 URL」、「利用者 ID」、「PIN」は、申請担当者様あてに E-mail にて送付しております、「EINS/PKI for EDI 証明書発行用データ送付のお知らせ」に添付されている PIN ファイルに記載されています。
- 2) Microsoft Edge を使用して「証明書発行用 URL」にアクセスしてください。次の画面が表示されます。

EINS/PKI for EDI
証明書 ユーザー認証
この度はEINS/PKI for EDI証明書をご利用いただきありがとうございます。 下記の内容をご確認いただいてから証明書の発行をよろしくお願いいたします。
・ Microsoft Edge ・ Google Chrome ・ Firefox
※マイクロソフト社のサポートポリシーに則り、 EINS/PKI for EDIでの証明書発行用Webブラウザと して、Internet Explorer 11のサポートを終了しています。
※証明書発行に失敗してしまった場合はお問い合わせフォームよりEINS/PKI事務局まで お問い合わせください。
証明書発行
<ol> <li>利用者IDとPINをに入力します。</li> <li>「証明書発行処理 対象Webブラウザを確認し、証明書を発行します。」にチェックを入れて 「証明書発行」ボタンを押下してください。</li> <li>証明書発行画面が表示されます。         <u>「証明書ダウンロード」を押下して、発行された証明書をダウンロードしてください。</u></li> </ol>
利用者ID PIN (3)
□ <u></u>
※ ユーザ認証を5回失敗すると、 <u>ご使用のアカウントが使用不可</u> となりますのでご注意ください。 以上
Copyright © 2009 - 2022 INTEC Inc.



- 3) 利用者 ID の欄に「利用者 ID」、PIN の欄に「PIN」を入力してください。
- 4) 「証明書発行処理 対象 Web ブラウザを確認し、証明書を発行します。」にチェックをしてください。
- 5) 「証明書 発行」ボタンを押してください。
- 6) 証明書の発行が完了すると、次の画面が表示されます。

EINS/PKI for EDI	INTEC TIS INTEC Group
証明書 インストール	
証明書の発行が完了しました。 以下のボタンをクリックして証明書をダウンロードして、 証明書ファイル (client.pfx) がパソコン上に保存されたことをご確認ください。 ※PKCS#12保護パスワードは、証明書発行申請画面で入力したPINとなります 証明書 ダウンロード ◆ (7)	
Copyright © 20	09 - 2023 INTEC Inc.

- 7) 「証明書 ダウンロード」ボタンを押してください。証明書ファイルがダウンロードされます。
  - ※ 証明書ファイル[ファイル名:client.pfx]がダウンロードされたことを確認してください。また、証明書 ファイルをコピーして、バックアップを作成し別の媒体にて保存してください。
- 8) 申請担当者様、または証明書利用者様のE-mailメールアドレス宛てに証明書発行完了のメールを送付 いたしますので、メールが届いているかをご確認ください。
- 9) EDI アプリケーションに証明書ファイルのインストールをお願いいたします。
  - ※ 証明書ファイルのインストール手順は EDI アプリケーションのマニュアルをご参照ください。

電子証明書発行サービス EINS/PKI

#### 2. 証明書発行後の確認

※以下は証明書の内容を確認する手順となり、実施は任意となります。

1) ダウンロードした証明書ファイルをダブルクリックするとインポート ウィザードが開くため、「次へ」を押し て先に進みます。

÷	☞ 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)	
	○ □-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	

- 2) 秘密キーのパスワードには、証明書発行の際に使用した「PIN」を入力してください。
  - インポートオプションについては以下にチェックを入れてください。
    - ・このキーをエクスポート可能にする
    - ・すべての拡張プロパティを含める

<b>F-の保護</b> 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)
秘密キーのパスワードを入力してください。 パスワード( <u>P</u> ): 
パスワード( <u>P</u> ):  □ パスワードの表示( <u>D</u> )
インボートオブション(1): - 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。 - 「このキーをエクスポート可能にする(M) キーのパックアップやトランスポートを可能にします。 - 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(エクスポート不可)(P) - ダッイズの拡張プロパティを含める(A)



3) 「完了」を押すと証明書のインポートが完了します。

← 😺 証明書のインポート ウ	NJJ-K	×
証明書のインフ	ポート ウィザードの完了	
[完了] をクリックする	ると、証明書がインボートされます。	
次の設定が指定さ	halla:	
選択された証明書	コントア ウィザードで自動的に決定されます	
内容	PFX	
ファイル名	C:¥Users¥999000_115054¥Downloads¥client.pfx	
	完了(F) キャンセル	,

4) 「EINS/PKI for EDI リポジトリ」にアクセスしてルート認証局証明書、中間認証局証明書をダウンロードします。

https://www.einspki.jp/site\_repository/repository\_edi/

認証局証明書のダウンロード				
証明書ファイルへのリンクを右 ロードした証明書ファイルをダ をご確認ください。	クリックし、「対象をファイルに保存」よりダウンロードを行ってください。ダウン ブルクリックして表示し、『拇印』の項目がそれぞれの Finger Printと一致すること			
EINS/PKI for EDI ルー	¬認証局証明書(SHA-2)			
証明書のダウンロード	EINSPKI-EDI-ROOT_v2.cer 🗅			
有効期間 開始日	2015年4月28日 13:51:02			
有効期間 終了日	2035年4月23日 13:51:02			
Finger Print(SHA-1)	9b 74 13 6a d5 a5 2a 94 0e 36 a6 9f 8a 68 f9 74 fe 23 c8 0f			
EINS/PKI for EDI 中間	邵正局証明書(SHA-2)			
証明書のダウンロード	EINSPKI-EDI-CHAIN_V2.cer 🚹			
有効期間 開始日	2015年4月28日 13:58:26			
 有効期間 終了日	2035年4月23日 13:51:02			
Finger Print(SHA-1)	a1 ad 8a 80 9b 5d 2d ea ea f9 21 26 6d 51 65 97 e2 e6 7f 7e			





5) ダウンロードしたルート認証局証明書ファイルをダブルクリックすると証明書情報が開くため、「証明書 のインストール」を押して先に進みます。

📭 証明書	X
全般 詳細 証明のパス	
正明書の情報	
 この証明書の目的:	
• すべての発行ポリシー	
<ul> <li>すべてのアプリケーション ポリシー</li> </ul>	
発行先: EINS/PKI for EDI Root Certificate Authority V2	
発行者: EINS/PKI for EDI Root Certificate Authority V2	
有効期間 2015/04/28 から 2035/04/23	
び明典のイッフトール(N) 発行来のファートゼット(N)	
ОК	

6) インポート ウィザードが開くため、「次へ」を押して先に進みます。

←	~
証明書のインボート 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 します。	トアにコピー
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: 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 ム上の領域です。	テイで保護 れるシステ
保存場所 ● 現在のユーザー( <u>C</u> )	
○ 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。	



7)「証明書を全て次のストアに配置する」を選択して、参照ボタンを押し「信頼されたルート証明機関」を選 択後、「次へ」を押して先に進みます。

差 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(₽)
57-88→7 k 7.
信頼されたルート証明機関 参照(B)
Ver A /A D

8) 「証明書のインポート ウィザードの完了」が表示されるのを確認して「完了」を押します。

*	・ ᡒ 証明書のインポート ウィザード	×	
	証明書のインボ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。		
	ユーザーが選択した証明書ストア 信頼されたルート証明機関		
	内容 証明書		
		μ	
1			1





9) ダウンロードした中間認証局証明書ファイルをダブルクリックすると証明書情報が開くため、「証明書の インストール」を押して先に進みます。

<b>F</b>	证明 <del>者</del>	×
全化	受 詳細 証明のパス	
Γ	[]] 証明書の情報	
	この証明書の目的:	
	・すべてのアプリケーション ポリシー	
	発行先: EINS/PKI for EDI Certificate Authority V2	
	発行者: EINS/PKI for EDI Root Certificate Authority V2	
	有効期間 2015/04/28 から 2035/04/23	
	<b>証明書のインストール()</b> 発行者のステートメント(S)	
	ОК	

10) インポート ウィザードが開くため、「次へ」を押して先に進みます。

🔶 😺 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、さ します。	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
証明機関によって発行された証明書は、ユーザー されたネットワーク接続を提供すっための情報を含 ム上の領域です。	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 んでいます。証明者ストアは、証明者が保管されるシステ
保存場所 ③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( <u>N)</u> キャンセル



11)「証明書を全て次のストアに配置する」を選択して、参照ボタンを押し「中間証明機関」を選択後、「次へ」 を押して先に進みます。

÷	疑 証明書のインポート 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)	
	<u> 三明書 2 k z </u> 中間証明機関 参照(P)	
	次へ(N) キャンセ)	ŀ

12)「証明書のインポート ウィザードの完了」が表示されるのを確認して「完了」を押します。

← .	🐓 証明書のインボート ウィザード		×
	証明書のインボート 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。		
	ユーザーが選択した証明者ストア 中間証明機関 内容 証明者		
		完了(F) キャンセル	,





13) Microsoft Edge の画面右上にある「設定など("・・・"のアイコン)」を押し、「設定」を選択します。



#### 14)「プライバシー、検索、サービス」を開き、「証明書の管理」を開きます。

設定	Ē	ブラウザーの使用状況に関するオブションの診断データ、アクセスした Web サイトに関する情報、クラッシュ レボートを Microsoft に送信 して、Microsoft 製品の改善にご協力ください。
Q	設定の検索	EVENCIA: WINDOWS BOELT TO BUE IN A CARCELLARY
ċ	プライバシー、検索、サービス	自分に合わせてWeb エクスペリエンス <sup>⑦</sup> をカスタマイズする
59	外觀	データとその他の広告の設定は、 <u>Microsoft プライバシー グッシュボード</u> で管理します
	[スタート]、[ホーム]、および [新規] タブ	
Ē	共有、コピーして貼り付け	このアカウントでの閲覧履歴の使用 (広告、検索、ニュース、他の Microsoft サービスのパーソナル設定を目的とした使用)を Microsoft ●
T.	Cookie とサイトのアクセス許可	この設定を有効にするには、Microsoft アカウントでサインインする必要があります
6	既定のブラウザー	
$\downarrow$	ダウンロード	
양	ファミリー セーフティ	セキュリティ
At	言語	Microsoft Edge のセキュリティ設定を管理
Ø	プリンター	Storida e dátras
	システムとパフォーマンス	<b>証明香の管理</b> U HTTPS/SSLの証明告と設定を管理します
U	設定のリセット	
_	スマートフォンとその他のデバイス	Microsoft Defender SmartScreen
Ŷ	アクセシビリティ	Microson Detender Smanscreen を定って歩声をあるショートケンシロートでの体験9.9
9	Microsoft Edge について	<b>望ましくない可能性のあるアプリをブロックする</b> 予期しない動作を引き起こす可能性がある低評価のアプリのダウンロードをブロックします

15)「個人」タブのリストの中に、発行者が「<u>EINS/PKI for EDI Certificate Authority V2</u>」、「発行先」が証明書 ご利用者様のサーバ名、または個人名である証明書があることをご確認下さい。

証明書			<b></b>
目的(N):	<বৃন্দে>		•
個人 (動の人)中間語	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	Sれない発行元
発行先	発行者	有効期限 フレ	心闷名
www.intec.co.jp	EINS/PKI for EDI Cer	2018/08/ www	w.intec.co.jp

※「発行先」に表示される名称は証明書ごとに異なりますので、申請内容と照らし合わせてご確認ください。

16) 6)の一覧に表示された証明書情報をダブルクリックで開きます。「証明書」ダイアログが開きますので "<u>この証明書に対応する秘密キーを持っています</u>"と表示されていることをご確認ください。



証明書
全般 詳細 証明のパス
正明書の情報
この証明書の目的: ・リモート コンピューターの ID を保証する ・リモート コンピューター(こ ID を証明する ・電子メールを保護する
*詳細は、証明幾期のステートメントを参照してください。
<b>発行先:</b> www.intec.co.jp
<b>発行者:</b> EINS/PKI for EDI Certificate Authority V2
<b>右勃期四</b> 2015/ 08/ 21 协会 2018/ 08/ 21
📍 この証明書に対応する秘密キーを持っています。
発行者のステートメント(S) 駆動者の詳細について表示します。)
ОК





#### 3. こんな時は

EINS/PKI for EDI のクライアント証明書は、秘密鍵と証明書が単一のファイルに含まれる pfx 形式(拡張子: pfx、または p12)で発行、ダウンロードされます。

お使いの EDI 製品/EDI ソフトウェアによっては、証明書適用時に pfx 形式のクライアント証明書から秘密鍵 ファイル(拡張子:key)や秘密鍵を除いた pem 形式の証明書ファイル(拡張子:cer、または crt)を取得する必 要がある場合がございます。

この章では WindowsPC でフリーソフト OpenSSL を利用した場合の作業手順を掲載します。 本項の内容によって生じた結果の影響について、一切の責任を負いかねますこと予めご了承ください。

#### 3-1 OpenSSL をインストールする

 Shining Light Productions のダウンロードページ(<u>https://slproweb.com/products/Win32OpenSSL.html</u>)から OpenSSL Light 版 v3.1 系インストーラーをダウンロードします。

Win64 OpenSSL v3.1.2 Light       5MB Installer       Installs the most commonly used essentials of Win         EXE   MSI       5MB Installer       Installs the most commonly used essentials of Win         OpenSSL v3.1.2 (Recommended for users by the OpenSSL v3.1.2 (Recommended for users by the OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of installation.         Win64 OpenSSL v3.1.2       140MB Installer       Installs Win64 OpenSSL v3.1.2 (Recommended for users by the creators of OpenSSL v3.1.2 (Recommended for users)). Only installation.         Win32 OpenSSL v3.1.2 Light       140MB Installer       Installs the most commonly used essentials of Win openSSL v3.1.2 (Only install this if you need 32-b for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the gal agreement of users the subject to local and state laws. More information can be found in the gal agreement of the installation.         Win32 OpenSSL v3.1.2 Light       4MB Installer       Installs the most commonly used essentials of Win OpenSSL v3.1.2 (Only install this if you need 32-b for Windows. Note that this is a default build of OpenSSL v3.1.2 (Only install this if you need 32-b for Windows. Note that this is a default build of OpenSSL v3.1.2         Win32 OpenSSL v3.1.2       116MB Installer       Installs Win32 OpenSSL v3.1.2 (Only install this if 32-bit OpenSSL v3.1.2 (Only install this if 32-bit OpenSSL v3.1.2 (Only install this is a do f OpenSSL and is subject to local and state laws.		Туре	Description
Wind4 OpenSSL v3.1.2       140MB Installer       Installs Win64 OpenSSL v3.1.2 (Recommended for developers by the creators of <u>OpenSSL</u> ). Only insibit versions of Windows and targets Intel x64 chips that this is a default build of OpenSSL and is subjet that this is a default build of OpenSSL and is subjet that this is a default build of OpenSSL v3.1.2 Light         Win32 OpenSSL v3.1.2 Light       4MB Installer         EXE   MSI       Installs Installer         Win32 OpenSSL v3.1.2 Light       4MB Installer         Installs the most commonly used essentials of Wir OpenSSL v3.1.2 (Only install this if you need 32-b for Windows. Note that this is a default build of Op is subject to local and state laws. More information found in the legal agreement of the installation.         Win32 OpenSSL v3.1.2       116MB Installer         Installs Win32 OpenSSL v3.1.2       116MB Installer         OpenSSL v3.1.2       116MB Installer         Installs Win32 OpenSSL v3.1.2       116MB Installer	in64 OpenSSL v3.1.2 Light <u>KE   MSI</u>	5MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.1.2 (Recommended for users by the creators of <u>OpenSSL</u> ). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v3.1.2 Light       4MB Installer       Installs the most commonly used essentials of Wir OpenSSL v3.1.2 (Only install this if you need 32-b for Windows. Note that this is a default build of Op is subject to local and state laws. More information found in the legal agreement of the installation.         Win32 OpenSSL v3.1.2       116MB Installer       Installs Win32 OpenSSL v3.1.2 (Only install this if you need 32-b for Windows. Note that this is a default build of Op is subject to local and state laws. More information found in the legal agreement of the installation.         Win32 OpenSSL v3.1.2       116MB Installer       Installs Win32 OpenSSL v3.1.2 (Only install this if 32-bit OpenSSL for Windows. Note that this is a do of OpenSSL and is subject to local and state laws.	поч орепоза vз. г.z <u>KE   MSI</u>	140MB Installer	Installs Win64 OpenSSL v3.1.2 (Recommended for software developers by the creators of <u>OpenSSL</u> ). Only installs on 64- bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v3.1.2       116MB Installer       Installs Win32 OpenSSL v3.1.2 (Only install this if 32-bit OpenSSL for Windows. Note that this is a dof OpenSSL and is subject to local and state laws.	in32 OpenSSL v3.1.2 Light 4 KE   <u>MSI</u>	4MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v3.1.2 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
information can be found in the legal agreement or installation.	in32 OpenSSL v3.1.2 K <u>E</u>   <u>MSI</u>	116MB Installer	Installs Win32 OpenSSL v3.1.2 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

- 2) ダウンロードした EXE ファイルを起動し、OpenSSL をインストールします。
- 3) OpenSSL コマンドを利用できるよう、環境変数を追加します。
  - ① コントロールパネル > システム > システムの詳細設定 > 環境変数 をクリックします。



- ② 「Path」を選択した状態で「編集」をクリックします。
  - ※ その PC を利用する全ユーザに対して設定したい場合は「システム環境変数」から、ログインして いるユーザにのみ設定したい場合は「ユーザ環境変数」から選択してください。

12123029	1EE			
Path	<u>(</u>			
TMP XPRA_PDFIUM_PRINT	0		articity	
		新規(N)	編集(E)	削除(D)
ステム環境変数(S)	(H)			-
ステム環境変数(S) 変数 ComSpec	値			
ステム環境変数(S) 変数 ComSpec DriverData HOME HTTP_PROXY HTTPS_PROXY NUMBER_OF_PROCESSORS	١ <u>i</u>			

③「新規」を押下し、openssl.exe をダウンロードしたフォルダのパスを追加し、「OK」を押下します。
 「C:¥OpenSSL-Win32¥bin」に openssl.exe をダウンロードしている場合は以下のようになります。





4) コマンドプロンプトを起動し、OpenSSL のバージョンを確認します。バージョン正常に表示されるようであれば 正しくインストールされています。

> openssl version



#### 3-2 証明書ファイル(pfx 形式)から秘密鍵ファイルを取得する

- 1) コマンドプロンプトを起動します。
- 2) cd コマンドで pfx 形式のクライアント証明書ファイルが配置されているディレクトリへ移動します。
- 3) 次のコマンドを実行します。

> set OPENSSL\_MODULES=<openssl.exe をダウンロードしたフォルダのパス>

4) 次の OpenSSL コマンドを実行します。

> openssl pkcs12 -in <**クライアント証明書(pfx 形式)のファイル名**> -nocerts -nodes -out <**秘密鍵ファイ** ル名> -legacy

#### 入力例

> cd C:¥Users¥PKI

> set OPENSSL\_MODULES=C:¥OpenSSL-Win32¥bin

> openssl pkcs12 -in client.pfx -nocerts -nodes -out client.key -legacy

Enter Import Password: 証明書のインポートパスワードを入力する

## 3-3 証明書ファイル(pfx 形式)から秘密鍵を除いた証明書ファイル(pem 形式)を取得する

- 1) コマンドプロンプトを起動します。
- 2) cd コマンドで pfx 形式のクライアント証明書ファイルが配置されているディレクトリへ移動します。
- 3) 次のコマンドを実行します。

> set OPENSSL\_MODULES=<openssl.exe をダウンロードしたフォルダのパス>

4) 次の OpenSSL コマンドを実行します。

> openssl pkcs12 -in **<クライアント証明書(pfx 形式)のファイル名**> -clcerts -nokeys -out **<証明書(pem** 形式)ファイル名> -legacy

#### 入力例

> cd C:¥Users¥PKI

> set OPENSSL\_MODULES=C:¥OpenSSL-Win32¥bin

> openssl pkcs12 -in client.pfx -clcerts -nokeys -out client.cer -legacy

Enter Import Password: 証明書のインポートパスワードを入力する



#### 4. トラブルシューティング

正常に証明書が発行できない場合やご不明な点がございましたら、申請担当者様にて取りまとめの上、以下の URL のお問い合わせフォームからお問い合わせください。

https://www.einspki.jp/foredi\_mypage\_contact/