UPKI 電子証明書発行サービス

利用の手引き (Ver 1.0)

国立情報学研究所

改訂履歴

バージョン	改訂内容	改訂者
Ver 1.0	初版作成	事務局
		作成日:
		2014/11/20

UPKI 電子証明書発行サービス利用の手引き 目次

1. UPKI 電子証明書サービスの概要	5
1-1. サービスの概念図	5
1-2. UPKI 電子証明書発行サービスで使用する用語の役割	6
2. サービスへの利用申請	7
2-1. サービス利用条件等	7
2-1-1. サービス利用機関	7
2-1-2. 申請単位	7
2-1-3. 利用条件	7
2-1-4. 規程等の理解と承諾	7
2-2. サーバ証明書の発行・利用条件等	8
2-2-1 . サーバ証明書の発行条件	8
2-2-2. 動作確認済みサーバアプリケーション	8
2-2-3. 推奨する Web ブラウザ	8
2-3. 事務局	9
3. 事務フローと各種申請手続の概要	10
3-1. 事務フロー全体の概要	10
3-2. 各種申請手続きの概要	10
4. サービス利用申請手続(機関責任者向け)	11
4-1. サービス利用申請と事務の流れ	11
4-2. サービス利用申請書の記入方法	13
4-3. ドメイン申請書(表面)の記入方法	15
4-4. ドメイン申請書(裏面)の記入方法	17
4-5. 確認実施手順調査票の記入方法	18
5. サーバ証明書発行申請手続(登録担当者,利用管理者向け)	19
5-1. サーバ証明書発行申請の手続きと事務の流れ	19
5-2. 発行申請 TSV ファイルの作成について(利用管理者向け)	$\dots 20$
5.3. 発行申請 TSV ファイル作成支援ツールの使い方について	$\dots 20$
5.3.1. TSV 作成支援ツールへのアクセス	$\dots 20$
5.3.2. CSR の送信	20
5.3.3. サーバ証明書作成データの入力	22
5.3.4. 発行申請 TSV ファイルの出力	22
6. サーバ証明書失効申請手続(登録担当者,利用管理者向け)	23
6-1. サーバ証明書失効申請手続と事務の流れ	$\dots 23$
6-2. 失効申請 TSV ファイルの作成について(利用管理者向け)	$\dots 25$
6-3. 失効申請 TSV ファイル作成支援ツールの使い方について(利用管理者向け)	$\dots 25$
6.3.1. TSV 作成ツールへのアクセス	25

6.3.2. 失効する証明書の送信	25
6.3.3. 失効に必要なデータの入力	
6.3.4. 失効申請 TSV ファイル出力	
7. サーバ証明書更新申請手続(登録担当者,利用管理者向け)	
7.1. サーバ証明書更新申請手続と事務の流れ	
7-2. 更新申請 TSV ファイル作成支援ツールの使い方について	30
7.2.1. TSV 作成支援ツールへのアクセス	30
7.2.2. シリアル番号の確認	30
7.2.3. CSR の送信	30
7.2.4. 更新申請に必要なデータの入力	
7.2.5. 更新申請 TSV ファイルの出力	
参考資料等	33

1. UPKI 電子証明書サービスの概要

1-1. サービスの概念図

サービス全体の概要(サービス利用申請から証明書発行まで)は以下の図のとおりです。



【概要説明】

①各機関の機関責任者は、登録担当者を任命する。

この際、機関責任者は、登録担当者の実在性、本人性を確認することが必須です。

②サービス参加申請/承認

機関責任者は,サービス利用申請書に必要事項を記載し,機関の長を示す公印を押印した サービス参加申請書を事務局宛てに郵送することにより,サービスへの参加申請を行いま す。

③発行申請ファイル(TSV 形式)提出

利用管理者は、登録担当者に対して、証明書発行申請ファイルを TSV 形式で作成し、提出 します。

④利用管理者の審査

登録担当者は、利用管理者について実在性、本人性について審査します。

⑤TSV ファイルのアップロード

利用管理者から証明書申請ファイルを受け取った登録担当者は,申請内容に間違いがない かどうかを確認した後,証明書自動発行支援システムにアップロードする。 ⑥ダウンロード URL 通知(システム→利用管理者)

証明書発行後,支援システムから直接利用管理者宛てにダウンロード URL の通知を行い ますので,利用管理者は,当該 URL にアクセスして証明書をダウンロードします。

1-2. UPKI 電子証明書発行サービスで使用する用語の役割

以下に、本説明資料で使用する用語について説明いたします。

組 織	用語	説明
		本サービスで使用する、電子証明書を発行する
		ための認証局。Web Trust for CA に準拠してお
	認証局	り,世界的に信頼できる証明書の発行が可能で
		す。また、この証明書は主要な環境で、商用の
		電子証明書と同様に使用することが可能です。
		Web ブラウザで本システムにアクセスすること
NII	証明書自動発行支援シス	によって,登録担当者からの証明書発行申請や、
	テム	利用管理者・利用者による証明書ダウンロード
		などの機能をご利用いただけます。
		本サービスでは, 証明書発行要求 (CSR) や失
		効申請, その他の各種申請について TSV ファイ
	TSV ファイル	ルというタブ区切りファイルを作成いただき、
		システムに投入していただくこととなります。
	事務局	サービスの利用申請や証明書発行申請にあた
		り、審査業務等を実施する事務窓口です。
		本サービスの利用申請にあたり、各機関で選出
	機関責任者	いただく代表者の方です。課長相当職または准
		教授相当職以上の常勤教職員の方にお願いいた
		します。
		本サービスの参加機関側の事務的な窓口及び利
各大学	登録担当者	用管理者の審査業務の一部をお願いする方で
		す。大学の規模に応じて複数名選出いただくこ
		とも機関責任者が兼務することも可能です。
		電子証明書を管理する方です。サービス参加機
	利用管理者	関内の常勤教職員の方であれば、どなたでも利
		用管理者となることが可能です。

2. サービスへの利用申請

2-1. サービス利用条件等

本サービスでは、別紙「国立情報学研究所 UPKI 電子証明書発行サービス利用規程」第2条 に定める機関を対象として実施します。また、参加にあたっては次のような条件等があります ので、ご確認ください。

2-1-1. サービス利用機関

- 1. 大学, 短期大学, 高等専門学校, 大学共同利用機関
- 国立大学法人、大学共同利用機関法人および公立大学法人、ならびに、学校法人であって学校教育法(昭和二十二年法律第二十六号)第八十三条に定める大学もしくは同法第百十五条に定める高等専門学校を設置する機関
- 3. 国公立試験研究機関,ならびに,高等教育機関の教育研究活動支援を目的とする法人
- 4. 第一号から第三号に該当する大学・研究機関等が設置する機関
- 5. その他、本サービスの利用が必要であると研究所が認めた機関

2-1-2. 申請単位

本サービスへは,機関ごとの利用申請をお願いします。キャンパス毎や研究室毎のサー ビス利用申請は認められません。キャンパスや研究室が持つドメインを利用したい場合 は、サービス利用申請完了後に、ドメイン申請を行って下さい。

2-1-3. 利用条件

- 1. サービスの趣旨に賛同し,証明書利用の結果についてフィードバック調査にご協力い ただけること。
- 証明書申請について責任を全うできること。(利用管理者の本人性確認,実在性確認, 利用管理者が管理するサーバの実在性確認等)
- 3. 登録担当者は以下のいずれかの環境を利用できること。
- Microsoft Internet Explorer 8 (Windows) 以上
- · Firefox 24.0 (Windows, OS X) 以上

2-1-4. 規程等の理解と承諾

以下の規程類等について理解し、承諾したうえでサービスに参加すること。

- 1. UPKI 電子証明書発行サービス利用規程
- 2. UPKI 電子証明書発行サービス利用細則
- 3. 国立情報学研究所オープンドメイン認証局2証明書ポリシ
- 4. 国立情報学研究所運用支援認証局証明書ポリシ
- 5. セコム電子認証基盤認証運用規程
- 6. 情報・システム研究機構個人情報保護規程

2-2. サーバ証明書の発行・利用条件等

本サービスで発行するサーバ証明書には,次のような発行・利用条件等がありますのでご確 認ください。

2-2-1. サーバ証明書の発行条件

- ・対象とするサーバ
 - 所属する機関が所有するまたは管理するサーバ
 - サーバ認証を必要とするサーバ
 - ※特定少数の検証者のみを対象としたサーバや検証者ルート証明書の配布が容易に実 現できる場合は対象外とさせていただきます。
- ・ドメイン

- 所属する機関が保有または管理するドメイン

※ドメイン申請書で申請したドメインであること。

- ・CSR 作成上の注意事項
 - 鍵長は 2048bit 以上とします。

2-2-2. 動作確認済みサーバアプリケーション

本サービスでは、次のアプリケーションでの動作確認を実施しています。

- 1. Apache(mod ssl) 1.3
- 2. Apache(mod ssl) 2.0
- 3. Apache-SSL(1.3.33+1.55)
- 4. Microsoft Internet Information Server 6.0
- 5. Microsoft Internet Information Server 7.0
- 6. Microsoft Internet Information Server 7.5
- 7. Microsoft Internet Information Server 8.0
- 8. Microsoft Internet Information Server 8.5
- 9. IBM HTTP Server 7.0
- 10. Jakarta Tomcat 5
- 11. Apache Tomcat 6
- 12. Apache Tomcat 7

2-2-3. 推奨する Web ブラウザ

本サービスでは、次の Web ブラウザで動作確認を行っています。

- 1. Microsoft Internet Explorer 8 以上
- 2. Firefox 24.0 以上
- 3. Opera 12.15 以上
- 4. Apple Safari 6.0 以上
- 5. Google Chrome 34.0.1847.116 以上
- 6. iOS 用 Safari 4.0 以上

7. Android 4.0 以降に対応した Google Chrome

8. 平成 21 年 1 月から平成 26 年 8 月までに日本の携帯電話事業者(「(株)NTT ドコモ」、「ソフトバンクモバイル(株)」、「KDDI(株)」、「(株)ウィルコム」、「イー・アクセス(株)」) で発売 された携帯電話に搭載された Web ブラウザで、ルート認証局証明書の鍵長 RSA2048bit に 対応したブラウザ

最新情報は下記 Web ページをご参照ください。 https://certs.nii.ac.jp/join/

2-3. 事務局

UPKI 電子証明書発行サービス事務局は、本サービスに関する事務等の受付やお問い合わせ 窓口となっております。各種手続やお問い合わせについては、以下までご連絡ください。

〒101-8430 東京都千代田区一ツ橋2丁目1番2号 国立情報学研究所 学術基盤推進部 学術基盤課 総括・連携基盤チーム UPKI電子証明書発行サービス 事務局

 TEL: 03-4212-2216 /
 FAX: 03-4212-2230

 E-Mail: certs@nii.ac.jp

 $\pi - \varDelta \sim - \vec{v}$: https://certs.nii.ac.jp/

3. 事務フローと各種申請手続の概要

3-1. 事務フロー全体の概要

本サービスで発生する各種申請手続については、次のとおりです。

- プロジェクト参加申請
 - ▶ 4. サービス利用申請手続(機関責任者向け)で説明します。
- 証明書発行·更新
 - 5. サーバ証明書発行申請手続(登録担当者,利用管理者向け)で説明します。
 - 7. サーバ証明書更新申請手続(登録担当者,利用管理者向け)で説明します。
- 証明書失効
 - 6. サーバ証明書失効申請手続(登録担当者,利用管理者向け)で説明します。

3-2. 各種申請手続きの概要

本サービスで発生する各種申請手続きについては、以下のとおりです。

手続き	概要・処理の流れ			
	機関ごとにサービスの利用申請が必要となります。機関責任者は、サ			
	ービス利用申請書に必要事項を記載し,機関の長を示す公印を押印し			
サービフ	たサービス参加申請書を事務局宛てに郵送することにより,サービス			
リーレス	への参加申請を行います。			
个小开 中 詞	またサービス参加審査を円滑に行うため、作成した申請書について			
	は、事前に事務局宛てに、電子ファイル(Excel 形式)でメール送信			
	してください。ファイル送信宛先 : certs@nii.ac.jp			
電子証明書	サービス利用機関において,新規に電子証明書の発行を必要とする場			
発行申請	合は、証明書発行申請を行います。また、既に発行した電子証明書の			
	主体者 DN を変更する場合も発行申請を行います。			
電子証明書	有効期限に関わらず発行済証明書に対して証明書を再発行したい場			
更新申請	合や,電子証明書の記載事項(主体者 DN を除く)について変更が必			
	要な場合に更新申請を行います。			
	(各電子証明書の有効期限については,有効期限終了の1ケ月前に事			
	務局から利用管理者に対して電子メールで通知します。)			
	電子証明書が不要になった場合や秘密鍵が危殆化した場合等には,失			
電子証明書	効申請を行います。また,主体者 DN を変更後に旧証明書を失効する			
失効申請	場合にも失効申請を行います。(利用管理者から失効申請 TSV ファイ			
	ルの提出を受けて、登録担当者は支援システムに TSV ファイルをア			
	ップロードする必要があります。)			

4. サービス利用申請手続(機関責任者向け)

4-1. サービス利用申請と事務の流れ

サービス利用申請から証明書の取得までの流れは次のとおりです。



サービス利用にあたって機関責任者の方は、本サービス利用規程、同細則についてよく理解した うえでサービス利用申請を行っていただくこととなります。 その際,

-本サービスには機関ごとに参加いただく必要があること。

一機関責任者の方が作成し、機関の長を示す公印を押印したサービス参加申請書(および確認 実施調査票)を、事務局まで提出(電子媒体と本紙の両方)する必要があること。

- 旧プロジェクト(UPKI オープンドメイン証明書自動発行検証プロジェクト)参加機関の皆 様についても,新サービスで定めるサービス利用申請書のご提出が必要となること。

にご注意くださいますようお願いします。

なお、ご提出いただきましたサービス利用申請書の記載内容について、事務局から直接、機関 責任者の方にお問い合わせさせていただくことがございます。予めご了承ください。

また,登録担当者の方には,サービス参加後の電子証明書発行申請時に利用管理者の本人性及 び実在性を確認していただく必要がございますので,サービス利用申請書と同時にご提出いただ きます「確認実施手順調査票」に記載した手順に基づき,同様に確認を実施するようにしてくだ さい。

作成したサービス利用申請書は、本紙を事務局までお送りいただく前に、電子媒体を事務局ま で電子メールにてお送りくださいますよう、ご協力お願いします。

なお、サービスの利用までに必要な日数は参加審査を実施する必要上、機関により異なります が、サービス利用申請が事務局に到着してから、概ね 1.5~2 ヶ月程度となりますので、予めご 了承ください。

サービス利用申請が完了しましたら、事務局より機関責任者の方および登録担当者の方宛てに 電子メールでサービスご利用開始日をご連絡させていただきます。その後は,登録担当者の方が 実際に支援システムを利用して,サーバ証明書の発行,失効,更新等の作業を行っていただくこ ととなります。

4-2. サービス利用申請書の記入方法

サービス利用にあたりご提出いただくサービス利用申請書は次のとおりです。このサービス利 用申請書は機関責任者の方にご記入いただく必要があります。また,機関の長を示す公印の押印 が<u>必要</u>となりますので,ご注意ください。

				平成年月日
		UPKI電子証明書発行サービ	ころ 利用申請書	
国立情報学研	究所長 殿			
		· · · · · · · · · · · · · · · · · · ·		
		申請 百役 職 由 請 者 氏 名		
UPKI電子証明書 のとおり申請しま	『発行サービス0 ます。 ┃= のセッキクロ	D利用について「国立情報学研究所し	JPKI電子証明書発行サー	ビス利用規程」を遵守し,次
<u> </u>	このセルをクリー機関名	ックし (リストから参加裡別を選択し)		
	(日本語表記)			
所属機関	機関名 (英語表記)			
	所在地	₸		
	氏名		所属	
機關責任者	職名		電話番号	
	E-Mail			
	所属住所	〒 (所属機関所在地と同じ場合は省略可)		
機関の区分		このセルをクリックして、様	関の区分を選択してください	
構成員数	このセルをクリッ	クして、構成員数を選択してください。		
利用開始希望日	平反	え 27 年	1月	1日
	氏名		担当部所(役職)	
経理担当者	職名		電話番号	
	E-Mail		FAX	
	請求書送付先	〒 (所属機関所在地と同じ場合は省略可)		
備老				
PLD - 7				

(欄外向かって右上)

1)申請者役職

機関の長である申請者の役職名を記入してください。

2)申請者氏名

申請者の記名押印(機関の長を示す公印を押印)をお願いします。

(記入欄内)

1)所属機関

- 1-1)機関名(日本語表記):貴機関の正式名称を記入してください。
- 1-2)機関名(英語表記): 貴機関の正式名称を英語表記で記入してください。

この機関名は証明書の Organization(O)に記載されますので正確にご記入く ださい。

1-3) 所在地: 貴機関の所在地を記入してください。なお, 複数のキャンパス等に分かれて いる場合には,大学本部の所在する住所を記入してください。

2)機関責任者

- 2-1)氏名:機関責任者の氏名を記入してください。
- 2-2) 所属:機関責任者の所属名称を記入してください。
- 2·3) 職名:機関責任者の職名を記入してください。なお,機関責任者に必要な要件については, UPKI 電子証明書発行サービス利用規程第6条をご参照ください。
- 2-4) 電話番号:機関責任者と直接連絡可能な電話番号を記入してください。
- 2-5) E-Mail:機関責任者と連絡可能な電子メールアドレスを記入してください。
- 2-6) 所属住所:上欄 1-3)で記載した所属機関の所在地と異なる場合に記入してください。

3)機関の区分

UPKI 電子証明書発行サービス利用規程第2条の対象機関のうち、貴機関がいずれに該当するかを選択してください。

4)構成員数

構成員数を、リストから選択してください。構成員数とは、機関の常勤の教員と研究者の人 数となります。

5)利用開始希望日

サービスの利用開始希望日を、リストから選択して指定してください。なお、申請からサービス利用開始までは、1.5 ヶ月から2ヶ月を要します。

6) 経理担当者

- 4-1)氏名:経理担当者の氏名を記入してください。
- 4-2) 担当部署(役職):経理担当者の所属名称または役職を記入してください。
- 4-3)職名:経理担当者の職名を記入してください。
- 4·4) 電話番号:経理担当者と連絡可能な電話番号を記入してください。
- 4-5) FAX:経理担当者と連絡可能な FAX 番号を記入してください。
- 4-6) E-Mail: 経理担当者本人の電子メールアドレス¹を記入してください。
- 4-7)請求書送付先:上欄 1-3 で記載した所属機関の所在地と異なる場合に記入してくださ

 \flat

※登録担当者の記入方法については機関責任者と同様です。 機関責任者および登録担当者のメールアドレスは、所属機関が保有または管理するドメインのも

¹ やむを得ず共用の電子メールアドレスを利用する場合には、事前に事務局宛にご相談ください。

のをご記入ください。

また、サービス利用申請書の2シート目にある、「取引先マスタ登録依頼書」も必ず記入してく ださい。記入例については、3シート目をご参照ください。

4-3. ドメイン申請書(表面)の記入方法

サービス利用のためのドメイン申請時に作成していただくドメイン申請書は次のとおりです。 このドメイン申請書は、機関責任者の自署押印が必要になりますので,ご注意ください。

(表)					平成	年	月日
	UP	KI電子証明書	発行サービス	、ドメイン申請書			
国立情報学研	究所 御中						
) 広馬(彼) (周) (周) (周) (周) (周) (周) (周) (周) (周) (周	。 新(自 署)			E
次のとおりUPKI	電子証明書発行	サービスのドメイン	利用を申し込み	ゝ ます。			
申請種別	このセルをクリッ	ックして、申請種別	を選択してくださ	い			
	機関名 (日本語表記)						
所属機関	機関名 (英語表記)						
	所在地	∓					
対象ドメイン							
対象ドメインの 用途							
	氏名			所 属			
	ローマ字			17/ N±6			
登録担当者1	職名			電話番号	- :	-	
	E-Mail			FAX		-	
	所属住所	〒(所属機関所在地と	同じ場合は省略可)				
	氏名						
	ローマ字			所属			
登録担当者2	職名			電話番号		-	
	E-Mail			FAX		_	
	所属住所	〒(所属機関所在地と	同じ場合は省略可)				
	氏名						
	ローマ字			所属			
登録担当者3	職名		•	電話番号		_	
	E-Mail			FAX		_	

(欄外向かって右上)

1)所属機関名

貴機関の正式名称を記入してください。

2)機関責任者

機関責任者の方の自筆で氏名を記入したうえで、押印(組織之印であれば尚良)ください。

(記入欄内)

1)所属機関

- 1-1)機関名:貴機関の正式名称を記入してください。
- 1-2)機関名(英語表記): 貴機関の正式名称を英語表記で記入してください。 この機関名は証明書の Organization(O)に記載されますので正確にご記入く ださい。
- 1-3) 所在地: 貴機関の所在地を記入してください。なお, 複数のキャンパス等に分かれて いる場合には,大学本部の所在する住所を記入してください。

2)対象ドメイン

本サービスで利用するドメイン名を記入してください。

3)対象ドメインの用途

本サービスで利用するドメイン名の用途を記入してください。

4)登録担当者1

- 4-1)氏名:登録担当者の氏名を記入してください。
- 4-2)所属:登録担当者の所属名称を記入してください。
- 4-3)職名:登録担当者の職名を記入してください。
- 4-4) 電話番号:登録担当者と連絡可能な電話番号を記入してください。
- 4-5) FAX:登録担当者と連絡可能な FAX 番号を記入してください。
- 4-6) E-Mail:登録担当者本人の電子メールアドレス2を記入してください。

4-7)所属住所:上欄 1-3 で記載した所属機関の所在地と異なる場合に記入してください。 ※登録担当者 2 以降も同様です。3 名以上登録したい場合は、適宜記入欄を複製してください。 用紙が 2 枚におよんでもかまいません。

² やむを得ず共用の電子メールアドレスを利用する場合には、事前に事務局宛にご相談ください。

4-4. ドメイン申請書(裏面)の記入方法

ドメイン申請書の裏面には,機関責任者に確認していただく事項について記載しています。各々 の設問についてご確認いただき,確認欄にご回答いただく必要があります。

(裹) 機関責任者確認事項
記 入 日 平成 年 月 日 機 関 名 称 機 関 責 任 者
(1)以下の項目について確認の上, 確認欄から該当する選択肢を選んでください。
確認欄 ドメイン登録担当者への確認(ドメインの本人性確認) 対象ドメインでのサーバ証明書発行を,機関責任者及び登録担当者が担当することについ て,ドメイン登録担当者[1]の承諾を得た。
確認欄
確認欄 登録担当者の記載内容の確認(登録担当者の実在性確認) 参加申請書に記載した全ての登録担当者情報について,事実と相違ないことを確認した。
確認欄 確認実施手順調査票の確認 確認実施手順調査票に記載した全ての情報について、事実と相違ないことを確認した。
(2)その他(事務局への連絡事項などありましたらご記入ください)
[1] ドメイン登録担当者とは, ドメイン名の保有に対して責任を持つ者である。JPRSが提供するWhoisサービスにおいて「登録担当者」と呼ばれ る。

ドメイン申請書の裏面では、機関責任者がサービス利用にあたり、確認する事項についてお伺いしています。機関責任者の方は、各事項をご確認いただき、確認済みの項目について各々確認欄に「OK」、「NG」をリストから選択してください。

- 1)ドメイン登録担当者への確認(ドメインの本人性の確認)
 - 本サービスで利用するドメインでサーバ証明書の発行申請を行うことについて,機関責任者及 び登録担当者が担当することを,「ドメイン登録担当者³」から承諾を得ているかどうかについ て確認してください。確認いただき「ドメイン登録担当者」の承諾を得ている場合には確認欄 のリストから「OK」を選択してください。
- ³ JPRS が提供する Whois サービスでは、 m. [登録担当者] に該当する方になります。

2)登録担当者からの承諾(登録担当者の本人性の確認)

確認実施手順調査票で定めた手順をもとに,登録担当者がサービス利用規程を理解し,規程第 7条に定める事項について承諾していることを確認してください。確認いただき登録担当者の 承諾が得られている場合には確認欄のリストから「OK」を選択してください。

3)登録担当者の記載内容の確認(登録担当者の実在性確認)

参加申請書に記載した全ての登録担当者情報について事実と相違ないことを確認してください。 確認いただき事実に相違ない場合には確認欄のリストから「OK」を選択してください。

4)確認実施手順調査票の確認

「確認実施手順調査票」に記載した全ての情報が事実と相違ないことを確認してください。確認いただき、事実と相違ない場合には確認欄のリストから「OK」を選択してください。

5)その他

その他、事務局への連絡事項等がありましたら、記載欄にご記入ください。

4-5. 確認実施手順調査票の記入方法

ドメイン申請時に、「確認実施手順調査票」をご提出いただく必要があります。

確認実施手順調査票の記入については,別シートの記入例を参考としながら自大学の状況に沿った状況についてご記入ください。また,自機関において,どのような組織体制でサービスを利用されているかについて、体制図を体制図シートに記載いただく必要があります。記入の際には, 機関責任者と登録担当者及び利用管理者がどのような体制で運用されているのかについて明示す るようにしてください。

ご提出いただく際には、お手数をお掛けいたしますが、確認実施手順調査票と体制図が表裏 1 枚となるように印刷のうえ、事務局までお送りくださいますようお願いいたします。

なお、記載いただきました確認実施手順調査票につきましては、事前にサービス参加申請書と ともに電子媒体で事務局(certs@nii.ac.jp)までお送りくださいますよう、併せてお願いいたします。

5. サーバ証明書発行申請手続(登録担当者,利用管理者向け)

5-1. サーバ証明書発行申請の手続きと事務の流れ

サーバ証明書発行申請から証明書が発行・取得されるまでの流れは次のとおりです。



サービス参加の後,サーバ証明書の発行申請を行っていただくわけですが,利用管理者は「サ ーバ証明書発行申請ファイル」をTSV形式で作成し,登録担当者に提出していただく必要があり ます。(TSVファイルとは,各データの区切りにタブ文字を利用したファイルのことです。)利用 管理者から登録担当者へのTSVファイルの提出方法については本サービスでは特に規定しませ ん。各機関の規程にもとづいてそれぞれ提出をお願いします。

この作成いただいた TSV ファイルを登録担当者が自動発行支援システムにアップロードする と,認証局でサーバ証明書が発行された後,直接利用管理者宛てに証明書取得 URL がメールで 送信され,証明書を取得することが可能となります。

サーバ証明書発行申請ファイルは,事務局が提供している「サーバ証明書発行申請ファイル作 成支援ツール」という Web アプリケーションを利用して作成することが可能となっています。本 ツールの操作方法は,後述いたします。

さて,登録担当者側では,確認実施手順にもとづいて提出した利用管理者の本人性・実在性確 認等を行います。そして、利用管理者から提出されたサーバ証明書発行申請ファイルについて, 申請内容等(対象ドメインや FQDN 等)に間違いがないか確認を行い,問題がなければ支援シス テムにアップロードし,サーバ証明書発行申請を行うこととなります。

登録担当者によるサーバ証明書発行申請ファイルの確認のポイントは次のとおりとなります。

- 主体者 DN
 - OU が含まれる場合、利用管理者の所属部局名または当該サーバの所管部局であること
- 利用管理者氏名
 - ▶ FQDNのサーバの管理者氏名であること
- 利用管理者 E-mail
 - ▶ 利用管理者のメールアドレスに間違いないこと
 - 間違えると証明書取得 URL が正しく通知されず、証明書の発行を受けることができません
- FQDN
 - ▶ サービスに申請したドメインであること
 - ▶ 自機関に存在する FQDN であること
 - ▶ 自機関が管理しているサーバであること

5-2. 発行申請 TSV ファイルの作成について(利用管理者向け)

発行申請 TSV ファイルを作成するにあたり,後述の作成支援ツールを利用して発行申請に必要 な TSV ファイルを作成していただくことが可能です。

手作業で作成する場合には、「支援システム操作手順書(利用管理者用)」に記載のサーバ証明 書発行申請 TSV ファイル形式に基づき、データ間の区切りを「タブ」にした TSV ファイルを作 成して、登録担当者宛てに提出してください。

5.3. 発行申請 TSV ファイル作成支援ツールの使い方について

発行申請 TSV ファイルは事務局が提供する「TSV ファイル作成支援ツール」という Web アプ リケーションを利用して作成することが可能です。以降で簡易な利用方法をご説明いたします。 TSV 作成支援ツール使用方法の詳細については、以下の URL をご参照ください。

TSV ツール(Web アプリ版)の使い方

https://upki-portal.nii.ac.jp/docs/odcert/software/tsvtool

5.3.1. TSV 作成支援ツールへのアクセス

以下の URL にアクセスして、ツールを表示してください。 https://tsvtool.nii.ac.jp/cgi⁻bin/tsvtool.cgi

5.3.2. CSR の送信

前項の URL にアクセスすると以下のようなページが表示されますので、TSV 作成支援ツ

ールの TSV 種別のドロップダウンリストが「発行申請 TSV」になっていることを確認した 上で「CSR ファイルから」の行の「参照」をクリックして,既に作成済みの CSR を選択し 「CSR 送信」をクリックしてください。

TSVツール α版

サーバ上に個人情報を残さないために、操作を完了させるかもしくは途中で やめる場合はキャンセルをクリックしてください。



5.3.3. サーバ証明書作成データの入力

次図のように「CSR」「主体者 DN」「サーバ FQDN」フィールドが埋められた入力フォー ムが表示されますので、以下のテキストボックスに必要事項を入力してください。

通常は「dNSName」は空白のままで構いません。入力が終了しましたら右下の【完了】 ボタンをクリックしてください。

発行申請TSV		
CSR		
BEGIN CERTI	FICATE REQUEST	
		P P P P P P P P P P P P P P P P P P P
4mmvnivieiu4Z8W37	/TB2	
END CERTIFI	CATE REQUEST	
 主体者DN	C	
サーバFQDN	u <u>eti en talini in j</u> p	
dNSName		
加入者Email		
加入者氏名		
加入者所属		
ソフトウェア名等		
キャンセル		このレコードを再チェック 完了
末尾に新しいレコー CSRから ロクイック送信 新規作成	トを追加: 参照 OSR送信	

TSVツール α版

5.3.4. 発行申請 TSV ファイルの出力

次図のとおり前項で入力したデータが画面に表示されますので【ダウンロード】ボタンを 押してください。サーバ証明書発行申請 TSV ファイルがダウンロードされます。

TSVツール α版									
1件の発行申請TSVレコードの一覧	1です。								
主体者DN	証明書ブ ロファイ ルID	d3 d4 d5 d	6CSR	加入者	加入者所属	加入者Email	サーバFQDN	ソフトウェ ア名等	dNSName
(°N⊢,1:	1		###		222.7 h- 44 6 m	q	upli portalnikacij e	Apache 2.2.3	
作成したTSVファイルをダウンロー 再編集したい場合は一旦ダウンロ 終了	-ドするには ۱ードしたファ	このボタン [:] ァイルを再度	をクリッ 度アッフ	ックして< プロードし	ださい。 <u> </u>	<u> </u>			

ダウンロード終了後には、左下の【終了】をクリックしてください。

6. サーバ証明書失効申請手続(登録担当者,利用管理者向け)

6-1. サーバ証明書失効申請手続と事務の流れ

サーバ証明書失効の流れは次のとおりです。



利用管理者は、証明書発行申請時と同様に失効申請 TSV ファイルを作成し、登録担当者に提出 します。登録担当者は、提出されたファイルに間違いがないか確認したうえで支援システムにア ップロードします。

支援システム側で失効処理が終了すると,登録担当者及び利用管理者の両方に失効完了通知が 電子メールで送信されます。

利用管理者の異動や退職等の都合により,失効すべきサーバ証明書の失効申請が当該利用管理 者より行うことが困難な場合には,登録担当者が代理して,当該サーバ証明書の失効申請を行う ことができますが,その場合でも,証明書発行申請時の利用管理者メールアドレス宛てに本失効 申請完了のメールが送信されることとなります。

もし,利用管理者メールアドレスを変更あるいは不要になった場合には,別途,登録担当者から事務局宛てに直接ご相談くださいますよう,お願いします。

なお、失効申請についても発行申請と同様に、利用管理者が失効申請 TSV ファイルを作成し、 登録担当者宛てに提出する必要があります。TSV ファイル作成時の注意点は、次のとおりです。

失効申請 TSV ファイル記載情報の注意点(利用管理者向け)

● 主体者 DN

◆ 失効対象となる証明書の DN と同一であること

- 失効対象証明書シリアル番号
 - ◆ 失効対象となる証明書のシリアル番号と同一であること
- 失効理由

◆ 以下を基準に失効理由を指定してください。

1: keyCompromise	秘密鍵の紛失・漏洩等が発生した場合
3: affiliationChanged	主体者DN(OUなど)を変更するために旧証明書を失効する場合
4: superseded	主体者DN以外の証明書記載項目を変更するために旧証明書を失効する 場合(有効期限の延長のみの場合も含む)
5: cessationOfOperation	証明書の利用を終了する場合
0: unspecified	その他の理由により失効する場合

● 利用管理者 mail

◇ 利用管理者メールアドレスが発行申請時と異なる場合は必ず入力してください。記入がない場合、失効完了通知は発行申請時の利用管理者メールアドレス(および登録担当者)に対して行われます。

失効申請 TSV ファイルでは、失効の対象となる証明書のシリアル番号を 10 進法で記入するこ とにご注意ください。(証明書のシリアル番号は通常 16 進法で表記されています。) 16 進数で表 記されたシリアル番号を 10 進数に変換したい場合は、Windows 標準で付属している「電卓」の 機能を利用して変換することが可能です。以下の手順をお試しください。

【16 進数→10 進数の変換手順】
1.「スタート」-「すべてのプログラム」-「アクセサリ」-「電卓」を実行する。
2. メニューから「表示」-「関数電卓」を選択。
3.「電卓」の左上のオプションが「16 進」になっていることを確認したうえで、16 進数の 証明書シリアル番号を入力し、オプションを「10 進」に切り替える。
以上の手順で、16 進数のシリアル番号を 10 進数の番号に変換することが可能です。

利用管理者から失効申請 TSV ファイルの提出を受けた登録担当者は,次の確認ポイントに基づき記載内容について不備が無いことを確認したうえで,証明書自動発行支援システムにアップロードします。

失効申請 TSV ファイル記載情報の確認ポイント(登録担当者向け)

- 失効理由
 - O(unspecified)が指定されている場合、他の失効理由に該当しないことがわかる 失効理由コメントが適切に記入されていること
 - ◆ 良い例: 鍵ペアファイルを誤って消去したため
 - ◆ 悪い例: 証明書が不要になったため
 → 5 (cessationOfOperation) が正解

加入者 mail

▶ 加入者メールアドレスに間違いないこと

その後,証明書が失効された旨については,システムから登録担当者及び利用管理者に対して 電子メールで通知されることとなります。

6-2. 失効申請 TSV ファイルの作成について(利用管理者向け)

失効申請 TSV ファイルを作成するにあたり,作成支援ツールを利用して失効申請に必要な TSV ファイルを作成していただくことが可能です。

手作業で作成する場合には、「支援システム操作手順書(利用管理者用)」に記載のサーバ証明 書失効申請 TSV ファイル形式に基づき、データ間の区切りを「タブ」にした TSV ファイルを作 成して、登録担当者宛てに提出してください。

6-3. 失効申請 TSV ファイル作成支援ツールの使い方について(利用管理者向け)

6.3.1. TSV 作成ツールへのアクセス

以下の URL にアクセスして,ツールを表示してください。 https://tsvtool.nii.ac.jp/cgi⁻bin/tsvtool.cgi

6.3.2. 失効する証明書の送信

次図のようなページが表示されますので TSV 作成支援ツールの TSV 種別のドロップダ ウンリストから「失効申請 TSV」を選択し「証明書ファイルから」の行の「参照」をクリ ックして失効させたい証明書ファイルを選択し「証明書送信」をクリックしてください。

TSVツール α版

サーバ上に個人情報を残さないために、操作を完了させるかもしくは途中で やめる場合はキャンセルをクリックしてください。



6.3.3. 失効に必要なデータの入力

次図のとおり「主体者 DN」「シリアル番号」が埋められた入力フォームが表示されますので、それ以降の必要事項を入力してください。

なお「失効理由」については

- 1. 秘密鍵の紛失,漏洩等が発生した場合
- 3. 主体者 DN (OU など) を変更する場合
- 4. 主体者 DN 以外の証明書記載項目を変更するために証明書を失効する場合(有効期 限の更新のみの場合も含む)
- 5. 証明書の利用を終了する場合
- 0. その他

上のいずれかの理由を選択し、左端の数字を入力してください。0の場合は「失効理由コメント」に失効申請に至った理由を128文字以内で入力してください。

なお,失効理由で4を選択した場合で直後に新証明書の発行を予定している場合には「失 効申請」ではなく「更新申請」として申請してください。

入力が終了しましたら,右下の【完了】ボタンをクリックしてください。

TSVツール α版

失効申請TSV		
主体者DN シリアル番号	c**_,**, ******;, *** *, ****************	<u> </u>
加入者Email 失効理由 生効理由コンム		
大火ル重田コンクト		このレコードを再チェック 完了
末尾に新しいレコー CSRから 証明書から	ート [*] を追加: 参照 CSR送信 参照 証明書送信	
 □ クイック送信 新規作成 		

6.3.4. 失効申請 TSV ファイル出力

次図のとおり 6.2.3 で入力したデータが表示されますので確認の上【ダウンロード】ボタンをクリックしてください。失効申請に必要な TSV ファイルがダウンロードされます。

TSVツール α版

1件の失効申請TSVレコードの一覧です。

主体者DN	d2 d3	シリアル番号	失効 理由	失効理由 コメント	d7 d8	d9	加入者Email	d11	d12 d1	13
Си- и и и и и и и и и и и и и и и и и и	515	0 170000 1001 25007	1							
作成したTSVファイルをダウンロードする(再編集したい場合は一旦ダウンロードした	 こはこのボタ .ファイルをŦ	いをクリックしてくださし 再度アップロードしてく	e gr	א-סעל						

終了しましたら【終了】ボタンをクリックしてください。

7. サーバ証明書更新申請手続(登録担当者,利用管理者向け)

7.1. サーバ証明書更新申請手続と事務の流れ

サーバ証明書更新申請手続については,前章までの発行申請手続きと失効申請手続きを一部組 み合わせたような形となります。全体の流れは次のとおりです。



利用管理者が作成した更新申請 TSV ファイルを登録担当者が確認し、システムにアップロード することにより、システムからダウンロード用の URL が利用管理者宛てに通知され、その URL から更新後の証明書を利用管理者が直接ダウンロードし利用管理者サーバにインストールします。

ここで,発行申請手続きでは,証明書発行完了通知をシステムから登録担当者宛てに電子メールで送信するのですが,更新申請手続きでは証明書発行(更新)完了通知とともに,失効申請 TSV ファイルを一緒に添付した形で登録担当者宛てに電子メールが送信されます。

その後登録担当者は、利用管理者から更新後の証明書に旧証明書を置換した旨の連絡を待って、 連絡受領後、先に受信した失効申請 TSV ファイルをシステムにそのままアップロードします。

その後は失効申請手続きと同様に登録担当者及び利用管理者宛てに失効完了通知をシステムか ら受信し、本手続きは完了することとなります。

TSV ファイル作成時の注意点は、次のとおりです。

更新申請 TSV ファイル記載情報の注意点(加入者向け)

- 主体者 DN
 - ▶ 更新前サーバ証明書の主体者 DN と同一であること
- 失効対象証明書シリアル番号
 - ▶ 失効対象となる証明書のシリアル番号と同一であること
- 失効理由
 - ▶ 更新時は失効理由を指定しないでください。
 - ◇ (自動的に「主体者 DN 以外の証明書記載項目を変更するために旧サーバ 証明書を失効する場合(4: superseded)」が失効理由として設定されます。)
- 利用管理者氏名·利用管理者所属
 - 更新前サーバ証明書の利用管理者氏名と同一かどうかにかかわらず必ず入力してください
- 利用管理者 E-mail
 - ▶ 利用管理者メールアドレスに間違いないこと
 - ▶ 間違えると証明書取得 URL が加入者に正しく通知されません。

利用管理者から更新申請 TSV ファイルの提出を受けた登録担当者は、次の確認ポイントに基づき記載内容について不備が無いことを確認したうえで、証明書自動発行支援システムにアップロードします。

更新申請TSVファイル記載情報の確認ポイント(登録担当者向け)

- 加入者氏名
 - ▶ 加入者氏名が申請時点における加入者 FQDN のサーバの管理者氏名であること
- 加入者所属

▶ 加入者の所属に間違いないこと

- 加入者 E-mail
 - ▶ 加入者メールアドレスに間違いないこと
 - ▶ 間違えると証明書取得 URL が加入者に正しく通知されません。
- 加入者 FQDN
 - ▶ 更新の場合にも、新規発行申請時同様、以下の点を必ず確認してください。
 - ◆ 自機関に存在する FQDN であること
 - ◆ 自機関で管理しているサーバであること
- 7-2. 更新申請 TSV ファイル作成支援ツールの使い方について

【ご注意】どのような理由であっても旧証明書の鍵ペアは更新申請には使用できません。改めて鍵ペアを生成し同じ主体者 DN で CSR を作成してください。CSR 作成方法の詳細については、以下の URL を参照してください。

サーバ証明書インストールマニュアル

https://certs.nii.ac.jp/archive/manuals/#_495

7.2.1. TSV 作成支援ツールへのアクセス

以下の URL にアクセスして,ツールを表示してください。 <u>https://tsvtool.nii.ac.jp/cgi⁻bin/tsvtool.cgi</u>

7.2.2. シリアル番号の確認

更新申請には更新しようとする旧証明書のシリアル番号が必要です。シリアル番号が不明 な場合には、失効申請 TSV の作成手順に従って、旧証明書ファイルをアップロードして、旧 証明書のシリアル番号を確認してください。

7.2.3. CSR の送信

TSV 作成ツールにアクセスすると、下のようなページが表示されますので「TSV 作成ツール」の右側のドロップダウンリストから「更新申請 TSV」を選択し、「CSR ファイルから」の行の「参照」をクリックして、新しい証明書のために作成した CSR を選択して【CSR 送信】をクリックしてください。

TSVツール α版

サーバ上に個人情報を残さないために、操作を完了させるかもしくは途中で やめる場合はキャンセルをクリックしてください。



7.2.4. 更新申請に必要なデータの入力

次図のとおり「CSR」「主体者 DN」「サーバ FQDN」が埋められた入力フォームが表示さ れますので、まず 5.2.2「シリアル番号の確認」で確認したシリアル番号を「旧証明書シリア ル番号」に入力してください。あとは、サーバ証明書発行申請と同じ要領で、以下の必要事 項について入力してください。

通常は「dNSName」は空白のままで構いません。入力が終了したら【完了】ボタンをク リックしてください。 TSVツール α版

更新中請ISV	
旧証明書シリアル番 □ or 6進数:	
CSRBEGIN CERTIFICATE REQUEST	
k r	IV.
	- K
c	,U
c	X
-	6
E	z
Fauguri wipping conversion	
END CERTIFICATE REQUEST	
主体者DN C** .** : : : : : : : : : : : : : : : : :	Norman and the state of the sta
サーバFQDN]
dNSName カルメギロー・	-
加入者氏名	
加入者所属	
ソフトウェア名等	-
++>U/	[200J-F8用+199][元]
末尾に新しいレコードを追加:	
CSRから 参照 CSR送信	
証明書から 参照… 証明書送信	
□クイック送信	
新規作成	

7.2.5. 更新申請 TSV ファイルの出力

次図のとおり入力されたデータが表示されますので、確認の上【ダウンロード】ボタン をクリックしてください。更新申請に必要な TSV ファイルがダウンロードされます。



終了しましたら【終了】ボタンをクリックしてください。

参考資料等

以下資料につきましては UPKI 電子証明書発行サービスのサイト上に掲載しております。ご参照ください。

https://certs.nii.ac.jp/

【規程類】

- -UPKI 電子証明書発行サービス利用規程
- -UPKI 電子証明書発行サービス利用細則
- -国立情報学研究所オープンドメイン認証局2証明書ポリシ(Certificate Policy: CP)
- -国立情報学研究所運用支援認証局証明書ポリシ(Certificate Policy: CP)
- ーセコム電子認証基盤認証運用規程(Certificate Practice Statement: CPS)
- 情報・システム研究機構個人情報保護規程

【申請書類】

- -UPKI 電子証明書発行サービス利用申請書、ドメイン申請書、変更届
- -UPKI 電子証明書発行サービス 確認実施手順調査票

【マニュアル等】

- -UPKI 電子証明書発行サービス 証明書自動発行支援システム操作手順書(登録担当者用)
- -UPKI 電子証明書発行サービス 証明書自動発行支援システム操作手順書(利用管理者用)
- -証明書自動発行支援システムサーバ証明書インストールマニュアルー式

[FAQ]

-UPKI 電子証明書発行サービス FAQ

https:// certs.nii.ac.jp/faq/

【TSV 作成支援ツール】

-TSV ツール(Web アプリ版)

https://tsvtool.nii.ac.jp/cgi-bin/tsvtool.cgi

-TSV ツール(Web アプリ版)の使い方

https://upki-portal.nii.ac.jp/docs/odcert/software/tsvtool

以上