

UPKI オープンドメイン証明書
自動発行検証プロジェクト

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 0.98	<ul style="list-style-type: none"> ・ TSV ツールを Web アプリケーション版に変更 Ver0.96 で説明した EXCEL 版 TSV 作成支援ツールは EXCEL2003 及びそれ以前の EXCEL を利用して鍵長が 2048bit 以上の CSR を扱う場合に不具合があることが確認されたため。(EXCEL 版は今後公開終了予定) ・ FAQ, TSV 作成支援ツールに関する利用方法の URL を巻末に追加 	事務局 更新：2009/06/19
Ver 1.0	<ul style="list-style-type: none"> ・ 機関責任者が登録担当者を兼務できることを明記 ・ 1 機関複数ドメイン対応 ・ 対応携帯電話の表現変更 ・ 場合によって更新申請でなく発行申請を行う必要があることを明記 ・ 参加申請書電子媒体は郵送前に送信すること ・ 参加承認メールは機関責任者と登録担当者両方に送信される ・ 失効理由コメントは全角半角にかかわらず 128 文字 ・ 巻末資料に変更申請書・変更届を追加 ・ 誤植の修正 	事務局 更新：2009/11/02

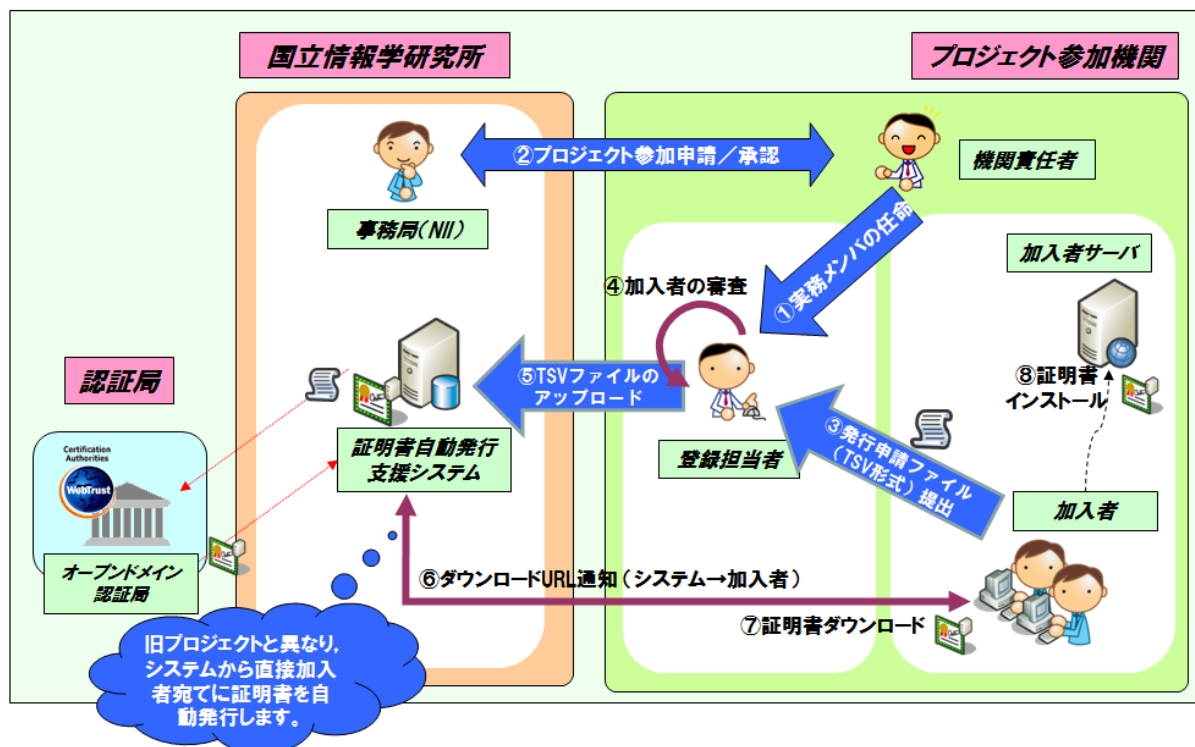
UPKI オープンドメイン証明書自動発行検証プロジェクト利用の手引き 目次

1. プロジェクトの概要	
1-1. プロジェクトの概念図	・・・ 4
1-2. プロジェクトで使用する用語と役割	・・・ 5
2. プロジェクトへの参加	
2-1. プロジェクト参加条件等	・・・ 6
2-2. サーバ証明書の発行・利用条件等	・・・ 7
2-3. プロジェクト事務局	・・・ 8
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	・・・ 9
3-2. 各種申請手続きの概要	・・・ 9
4. プロジェクト参加申請手続（機関責任者向け）	
4-1. プロジェクト参加申請と事務の流れ	・・・ 11
4-2. プロジェクト参加申請書（表面）の記入方法	・・・ 13
4-3. プロジェクト参加申請書（裏面）の記入方法	・・・ 15
4-4. 確認実施手順調査票の記入方法	・・・ 17
5. 発行申請手続（登録担当者，加入者向け）	
5-1. 発行申請手続きと事務の流れ	・・・ 18
5-2. 発行申請 TSV ファイル作成について（加入者向け）	・・・ 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	・・・ 20
6. 失効申請手続（登録担当者，加入者向け）	
6-1. 失効申請手続きと事務の流れ	・・・ 22
6-2. 失効申請 TSV ファイルの作成について（加入者向け）	・・・ 24
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	・・・ 24
7. 更新申請手続（登録担当者，加入者向け）	
7-1. 更新申請手続きと事務の流れ	・・・ 27
7-2. 更新申請 TSV ファイルの作成支援ツールの使い方について	・・・ 29
参考資料等	・・・ 32

1. プロジェクトの概要

1-1. プロジェクトの概念図

プロジェクト全体の概要（プロジェクト参加から証明書発行まで）は以下図のとおりです。



【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プロジェクト参加申請/承認

機関責任者は、別添のプロジェクト参加申請書に必要事項を記載し、自署・押印のうえ、本申請書を事務局に郵送します。

③発行申請ファイル (TSV 形式) 提出

加入者は、登録担当者に対して、サーバ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加入者の審査

登録担当者は、加入者について実在性、本人性について審査します。

⑤TSV ファイルのアップロード

加入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, ⑦ダウンロード URL 通知 (システム→加入者), 証明書ダウンロード

サーバ証明書発行後、支援システムから直接加入者宛てにダウンロード URL の通知を行いますので、加入者は、当該 URL にアクセスして証明書をダウンロードします。

⑧証明書インストール

加入者は、加入者サーバに発行されたサーバ証明書をインストールします。

1-2. プロジェクト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
NII	オープンドメイン認証局	本プロジェクトで使用する、サーバ証明書を発行するための認証局。Web Trust for CA に準拠しており、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ウェブブラウザ等で、商用のサーバ証明書と同様に使用することが可能です。
	証明書自動発行支援システム	Web ブラウザで本システムにアクセスすることによって、登録担当者からの証明書発行申請や加入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。
	TSV ファイル	本プロジェクトでは、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	プロジェクトの参加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。
各大学	機関責任者	本プロジェクトの参加にあたり、各機関で選出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をお願いいたします。
	登録担当者	本プロジェクトの参加機関側の事務的な窓口及び加入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。
	加入者	サーバを管理し、実際にサーバ証明書を利用される方です。プロジェクト参加機関内の常勤教職員の方であれば、どなたでも加入者となることが可能です。
	加入者サーバ	加入者の方が管理するサーバです。本プロジェクトで発行したサーバ証明書を実際にインストールして使用するサーバのことです。

2. プロジェクトへの参加

2-1. プロジェクト参加条件等

本プロジェクトでは、別紙「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要領」第4条に定める機関を参加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. 参加対象機関

1. SINET に加入する大学，短期大学，高等専門学校，大学共同利用機関
2. SINET に加入する大学共同利用機関法人，独立行政法人，地方独立行政法人，学校法人，公益法人，または国公立試験研究機関
3. 日本学術会議協力学術研究団体で，本プロジェクトが対象とするドメイン名を保有し部会が認めた団体
4. 1. または 2. に該当する機関の長が設置する組織で，本プロジェクトが対象とするドメイン名を保有し，当該ドメイン名でのサーバ証明書の利用が必要であると部会が特に認めたもの

2-1-2. 参加単位

本プロジェクトへの参加単位は，各機関ごとの参加申込でお願いします。キャンパス毎や研究室毎のプロジェクト参加は認められません。

2-1-3. 参加条件

1. プロジェクトの趣旨に賛同し，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。
2. 証明書申請について責任を全うできること。（加入者の本人性確認，実在性確認，加入者サーバの実在性確認）
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。
 - ・ Internet Explorer 5.5 SP2 以降
 - ・ Firefox 2.0 以降
 - ・ Netscape 7.1 以降

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，承諾したうえでプロジェクトに参加すること。

- ・ 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要領
- ・ 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に関する事務手続き要領
- ・ UPKI オープンドメイン証明書利用に係る申合せ
- ・ 国立情報学研究所オープンドメイン認証局 2 証明書ポリシー
- ・ 国立情報学研究所運用支援認証局証明書ポリシー
- ・ セコム電子認証基盤認証運用規程

2-2. サーバ証明書の発行・利用条件等

本プロジェクト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
 - －所属する機関の主たるドメインおよびそれに準ずるドメイン
 - ※プロジェクト参加申請書に記載したドメインであること。
- ・CSR 作成上の注意事項
 - －鍵長は 1024bit 以上(2048bit 以上を推奨)とします。

2-2-2. 動作確認済みサーバアプリケーション

本プロジェクトでは、次のアプリケーションでの動作確認を実施しています。

- ・ Apache (mod_ssl-2.8.25-1.3.34)
- ・ Apache-SSL (1.3.33+SSL_1.55)
- ・ Microsoft Internet Information Server5.0
- ・ Microsoft Internet Information Server6.0
- ・ IBM HTTP Server 6.02 以上
- ・ Jakarta Tomcat (4.1.31, 5.0.30)

2-2-3. 推奨する Web ブラウザ

本プロジェクトでは、次の Web ブラウザで動作確認を行っています。

- ・ Microsoft Internet explorer 5.5 以上
- ・ Firefox1.0.8 以上
- ・ Opera8.0 以上
- ・ Apple Safari3.0.4 以上
- ・ Google Chrome0.2.149 以上

※携帯電話への対応は「2006年6月以降に日本で発売された携帯電話で、2048bit RSA 鍵のルート証明書の検証ができるもの」であれば利用可能です。

最新情報は下記 Web ページをご参照ください。

<https://upki-portal.nii.ac.jp/docs/odcert/howto/intro#software>

2-3. プロジェクト事務局

プロジェクト事務局は、本プロジェクト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 基盤企画課 総括・連携システムチーム

UPKI オープンドメイン証明書自動発行検証プロジェクト 事務局

TEL : 03-4212-2218, 2226 / FAX : 03-4212-2230

E-Mail : cerpj2@nii.ac.jp

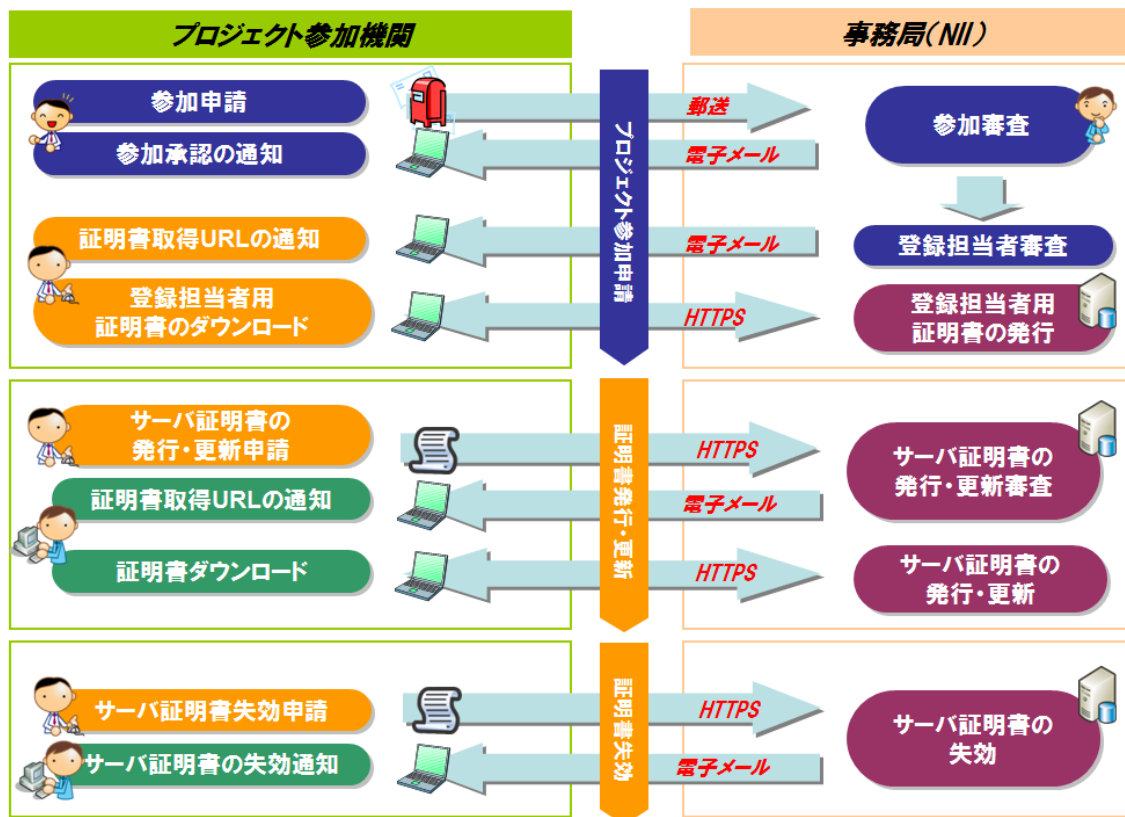
ホームページ : <https://upki-portal.nii.ac.jp/docs/odcert>

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

本プロジェクトで発生する各種申請手続については、次のとおりです。

事務フロー全体の概要



3-2. 各種申請手続きの概要

本プロジェクト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。

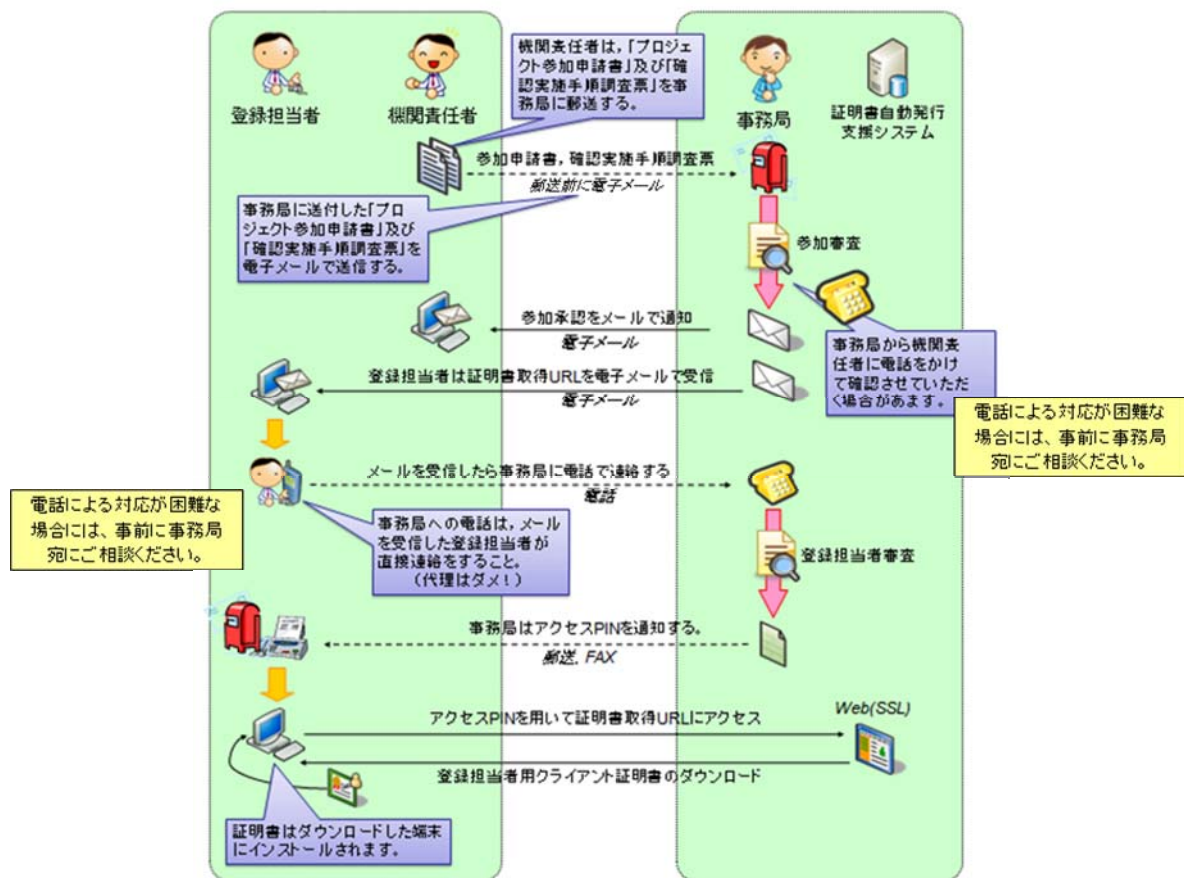
手続き	概要・処理の流れ
プロジェクト参加申請	<p>機関ごとにプロジェクトへの参加申請が必要となります。機関責任者は、プロジェクト参加申請書に必要事項を記載し、自署及び押印のうえ、事務局宛てに参加申請書を郵送することにより、プロジェクトへの参加申請を行います。</p> <p>またプロジェクト参加審査を円滑に行うため、作成した参加申請書については、事前に事務局宛てに、電子ファイルでメール送信してください。ファイル送信宛先：cerpj2@nii.ac.jp</p>
サーバ証明書発行申請	<p>プロジェクト参加機関において、新規にサーバ証明書の発行を必要とする場合に証明書発行申請を行います。また、既に発行したサーバ証明書の主体者 DN を変更する場合も発行申請を行います。</p>
サーバ証明書	<p>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</p>

更新申請	<p>合や、サーバ証明書の記載事項（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。</p> <p>（サーバ証明書の有効期限については、有効期限終了の 1 ヶ月前に事務局から加入者に対して電子メールで通知します。）</p>
サーバ証明書失効申請	<p>サーバ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場合にも失効申請を行います。（加入者から失効申請 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。）</p>

4. プロジェクト参加申請手続（機関責任者向け）

4-1. プロジェクト参加申請と事務の流れ

プロジェクト参加申請から証明書の取得までの流れは次のとおりです。



プロジェクト参加にあたって機関責任者の方は、本プロジェクト参加要領、事務手続き要領についてよく理解したうえでプロジェクト参加申請を行っていただくこととなります。

その際、

- サーバ証明書プロジェクトには機関ごとに参加いただく必要があること。
 - 機関責任者の方が、自署捺印したプロジェクト参加申請書（および確認実施調査票）を事務局まで電子媒体と本紙の両方を提出する必要があること。
 - 旧プロジェクト（サーバ証明書発行導入における啓発・評価研究プロジェクト）参加機関の皆様についても、新プロジェクトで定める参加申請書のご提出が必要となること。
- ご注意くださいますようお願いいたします。

なお、ご提出いただきました参加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、プロジェクト参加後のサーバ証明書発行申請時に加入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、参加申請書と同時に提出いただきます「確認実施手順調査票」に記載した手順に基づき、同上確認を実施するようにしてください。

作成した参加申請書は、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、ご協力をお願いします。

プロジェクト参加までの流れは次表のとおりです。

No.	項目	担当	説明
1	登録担当者への応募	機関責任者 登録担当者	次の書類を十分に確認し、お送りください。 <ul style="list-style-type: none"> プロジェクト参加要領および申請手続書要領 サーバ証明書利用に係る申合せ オープンメインフレーム2 証明書ポリシー (Certificate Policy) 運用支援センター 証明書ポリシー (Certificate Policy) セコム電子認証基盤 認証利用指針 (Certification Practice Statement)
2	登録担当者の任命	機関責任者	機関責任者の方は、 登録担当者の本人性・現在社を離脱のうえ 、任命を行ってください。
3	プロジェクト参加申請書の送付	機関責任者 ↓ 事務局	プロジェクト参加申請書および申請手続書に必要事項をご記入の上、事務局宛てに郵送してください。 なお、プロジェクト申請書には機関責任者の署名及び捺印が必須となります。郵送入票は後述
4	機関責任者への連絡	事務局 ↓ 機関責任者	事務局から機関責任者および登録担当者様宛てに、電子メールでプロジェクト参加申請書の送達についてご連絡させていただきます。
5	登録担当者への連絡	事務局 ↓ 登録担当者	事務局から登録担当者様宛てに、電子メールでプロジェクト参加申請書の結果と、登録担当者用証明書ダウンロードに必要な証明書取扱いについてご連絡させていただきます。
6	アクセス権限付与連絡	登録担当者 ↓ 事務局	前項の証明書を取得し通知を受けた登録担当者の方は、登録担当者審査のため各自が電話にて事務局までご連絡をいただく必要があります。審査終了後、登録担当者証明書ダウンロードに必要なアクセス権限をご連絡させていただきます。
7	登録担当者用証明書の取得	登録担当者	アクセス権限を受けたら、前項でご連絡した証明書を取扱いにアクセスして前項6のアクセス権を入力して登録担当者用証明書をダウンロードしてください。証明書はアクセスしたブラウザに自動的にインストールされます。

なお、プロジェクトの参加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、プロジェクト参加申請が事務局に到着してから、概ね 10 日前後となりますので、予めご了承ください。

プロジェクトに参加いただきましたら、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プロジェクトにご参加いただいた旨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。

プロジェクトにご参加いただいた後、概ね 1～2 日程度で登録担当者の方は支援システムをご利用いただけるようになります。

4-2. プロジェクト参加申請書（表面）の記入方法

プロジェクト参加にあたりご提出いただく参加申請書は次のとおりです。この参加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、機関責任者（自署）の欄では、必ず機関責任者の方により自署押印が必要となりますので、ご注意ください。（代理の方の記入は認められておりません。）

平成21年5月11日

(表) **UPKIオープンドメイン証明書自動発行検証プロジェクト 参加申請書**

国立情報学研究所
学術情報ネットワーク運営・連携本部長 殿

記入例

所属機関名 **記入例大学**
機関責任者(自署) **機関責任者の自署を願います。** 印

本プロジェクトの参加要領を理解し、次のとおりプロジェクトの参加を申し込みます。

参加申請種別	(2)旧プロジェクトから継続参加			
所属機関	機関名 (日本語表記)	記入例大学		
	機関名 (英語表記)	The University of Example		
	所在地	〒123-4567 東京都千代田区一ツ橋2-1-2		
機関責任者	氏名	菅 太郎	所属	菅 菅 菅センター
	職名	センター長	電話番号	03-1111-3333
	E-Mail	taro@example.ac.jp		
	所属住所	所属機関に同じ		
対象ドメイン	example.ac.jp			
登録担当者1	氏名	研究 花子	所属	菅 菅 菅センター
	ローマ字	Kenkyu Hanako	電話番号	03-1111-7777
	職名	准教授	FAX	03-1111-8888
	E-Mail	hanako@example.ac.jp		
	所属住所	〒 (所属機関所在地と同じ場合は省略可)		
登録担当者2	氏名	李 一郎	所属	菅 菅 菅課
	ローマ字	Jimu Ichiro	電話番号	03-8888-9999
	職名	菅 菅 菅課長	FAX	03-8888-5555
	E-Mail	ichiro@example.ac.jp		
	所属住所	〒 (所属機関所在地と同じ場合は省略可)		
登録担当者3	氏名		所属	
	ローマ字		電話番号	
	職名		FAX	
	E-Mail			

(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)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、プロジェクト参加要領第8条をご参照ください。

2-4) 電話番号：機関責任者と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)対象ドメイン

本プロジェクトに参加する対象のドメイン名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¹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、3)の対象ドメインのものをご記入ください。

3)の対象ドメインと異なる場合は、事前に事務局宛にご相談ください。

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。

4-3. プロジェクト参加申請書（裏面）の記入方法

参加申請書の裏面には、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。

(裏) 機関責任者確認事項	
記入例	記入日 平成21年5月11日 機関名称 記入例大学 機関責任者 皆報 太郎
(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。	
【OK】	SINET加入機関の確認 自機関が、学術情報ネットワーク(SINET)加入機関[1]であることを確認した。
【OK】	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、 <u>ドメイン登録担当者[2]</u> の承諾を得た。
【OK】	登録担当者からの承諾(登録担当者の本人性確認) 確認実施手順調査票で定めた手順をもとに、登録担当者がプロジェクト参加要領を理解し、参加要領第6条に定める事項について承諾していることを確認した。
【OK】	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。
【OK】	確認実施手順調査票の確認 (新規参加機関の場合)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。 (旧プロジェクト参加機関の場合)旧プロジェクトの確認実施手順から変更が無いこと[3]を確認した。
【旧プロジェクト参加機関のみ】	
(B)機関責任者変更	旧プロジェクトの機関責任者の本人性について、どちらか該当する項目を選択してください。後者の場合は、旧プロジェクト機関責任者氏名についてもご記入ください。 (A)旧プロジェクトの機関責任者が、引き続き本プロジェクトの機関責任者を務める。 (B)本申請書に記載されている機関責任者が、本プロジェクトの機関責任者を務めることについて、旧プロジェクト機関責任者の承諾を得ている。
	機関責任者氏名: 皆報 太郎
	旧プロジェクト機関責任者氏名: 基盤 三郎
(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)	
公印を押印できる文書が本学所定の様式に限られるため、別途学長が押印した文書「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申請について(依頼)」(〇〇第XX-NN号)を文書の裏として添付します。どうぞよろしくお願ひ致します。	

プロジェクト参加機関の裏面では、機関責任者がプロジェクト参加にあたり、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。なお、最後の設問については、「旧プロジェクト参加機関のみ」にご回答いただくものとなっています。

1) SINET 加入機関の確認

本プロジェクトでは、SINET に加入していることをプロジェクト参加の要件として、参加要領第 4 条で定めています。貴機関が SINET の加入機関であることについてご確認ください。確認いただき、参加機関であることを確認できた場合には「OK」を選択してください。

なお、SINET 未加入機関の方で、本プロジェクトに参加ご希望の機関の方は、SINET 加入についてご検討くださいますよう、お願いいたします。(参照 URL : <http://www.sinet.ad.jp/>)

2) ドメイン登録担当者への確認 (ドメインの本人性の確認)

本プロジェクトに参加する対象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²⁾」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) 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、登録担当者がプロジェクト参加要領を理解し、参加要領第 6 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。

4) 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) 確認実施手順調査票の確認

新規参加機関の場合には、本プロジェクト参加申請書とともにご提出いただく「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。

旧プロジェクト参加機関の場合には、旧プロジェクトで提出いただいた「確認実施手順調査票」の内容から変更がないことを確認してください。確認いただき変更が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。

なお、本プロジェクト参加にあたり確認実施手順を変更される場合は、確認欄のリストから「NG」を選択した上で「その他」欄に確認実施手順調査票を更新する旨をご記入いただくとともに、変更後の確認実施手順調査票を合わせてご提出ください。

6) 【旧プロジェクト参加機関のみ】

旧プロジェクト参加機関の場合、機関責任者の変更等について、もう少し詳細にお尋ねしています。選択肢のとおり、新プロジェクトの機関責任者を旧プロジェクトの機関責任者が継続する際には、確認欄のリストから「A」を選択してください。また、本申請書に記載されている

²⁾ JPRS が提供する Whois サービスにおける m. [登録担当者] に該当する方になります。

機関責任者が旧プロジェクトの機関責任者から承諾を得たうえで変更することとなっている場合には確認欄のリストから「B」を選択してください。なお、「B」を選択した場合には、設問下にある「旧プロジェクト機関責任者氏名」欄に、旧プロジェクト機関責任者の氏名を記載してください。

※本欄の記載は、新プロジェクト機関責任者に記載いただいても結構です。

7)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。

4-4. 確認実施手順調査票の記入方法

プロジェクトへの新規参加機関および旧プロジェクト参加機関で、確認実施手順が旧プロジェクトで確認した手順と異なる機関は、プロジェクト参加申請書とともに「確認実施手順調査票」をプロジェクト参加時に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プロジェクトに参加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加入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。

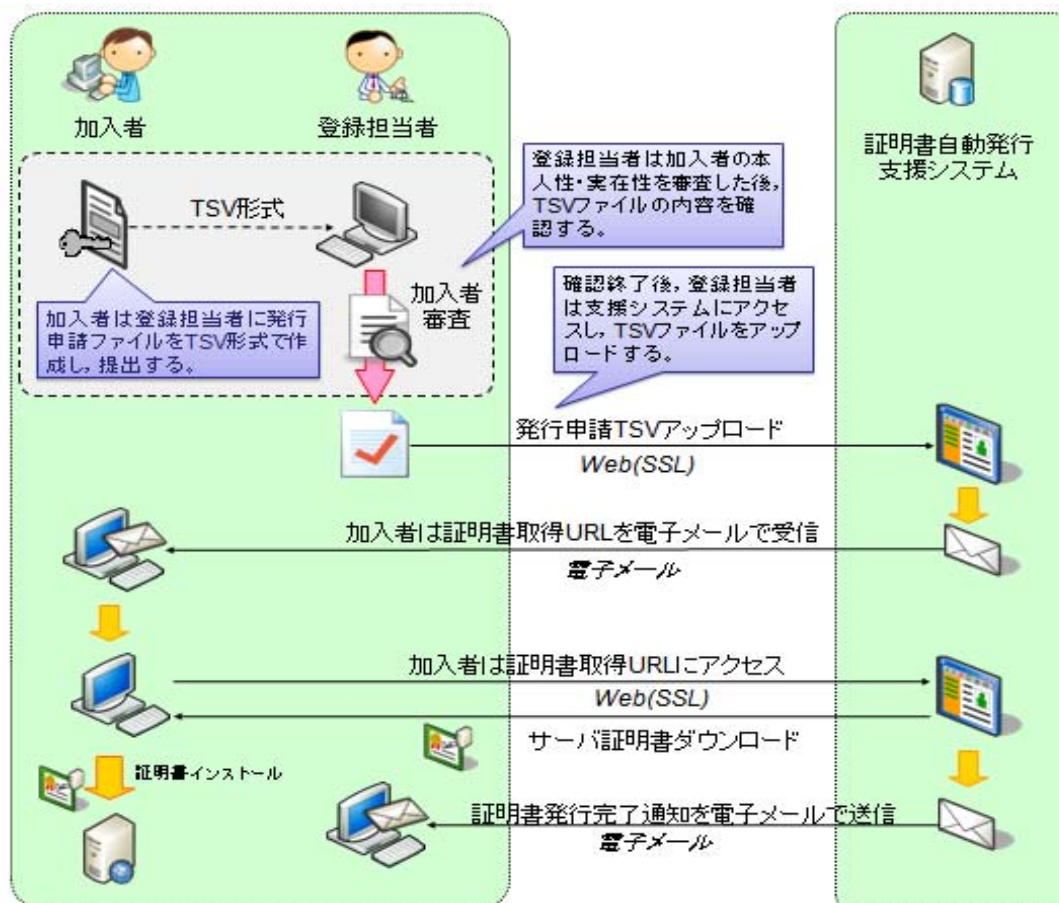
ご提出いただく際には、お手数をお掛けいたしますが、確認実施手順調査票と体制図が表裏1枚となるように印刷のうえ、事務局までお送りくださいますようお願いいたします。

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、事前にプロジェクト参加申請書とともに電子媒体で事務局(cerpj2@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. 発行申請手続（登録担当者，加入者向け）

5-1. 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。



プロジェクト参加の後，サーバ証明書の発行申請を行っていただくわけですが，加入者は「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。）加入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プロジェクト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，直接加入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。

No.	項目	担当	説明
1	サーバ証明書発行申請ファイルの作成及び登録担当者への提出	加入者 ↓ 登録担当者	加入者は、照会仕様に基つて「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ください。加入者から登録担当者への受け渡し方法は欄頭に任意で定めてください。
2	加入者の審査及びファイルの確認	登録担当者	登録担当者は、サーバ証明書の発行を申請する 加入者の本人性・実在性等 について確認したうえ、TSVファイル記載情報について確認を実施してください。
3	TSVファイルのアップロード	登録担当者	登録担当者は、確認済みのTSVファイルを「証明書自動発行支援システム」にアップロードすることで、サーバ証明書発行申請を行います。 TSVファイル形式に問題がなければ、加入者に証明書取得URLをシステムから自動で送信します。なお、TSVファイル形式に問題があった場合は、画面のエラーメッセージに従って、加入者にTSVファイルを再作成いただくよう指示してください。
4	証明書取得URL送信	加入者	証明書自動発行支援システムから直接加入者に対して証明書取得URLが通知されます。
5	証明書ダウンロード	加入者	加入者は、前項の証明書取得URLにアクセスし、証明書をダウンロードしてください。
6	発行完了通知の送信	システム ↓ 登録担当者	加入者から発行申請のあった証明書の発行が完了すると、登録担当者宛てに証明書発行完了通知が電子メールで送信されます。 このメールによって、登録担当者はサーバ証明書の発行が完了したことを把握することが可能となります。

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加入者の本人性・実在性確認等を行います。そして、加入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。

発行申請TSVファイル記載情報の確認ポイント	
• 主体者DN	– OUが含まれる場合、加入者の所属部局名または加入者サーバの所管部局であること
• 加入者氏名	– 加入者FQDNのサーバの管理者氏名であること
• 加入者E-mail	– 加入者のメールアドレスに間違いがないこと – 間違えると証明書取得URLが加入者に正しく通知されず、証明書の発行を受けることができません。
• 加入者FQDN	– プロジェクトで申請した「対象ドメイン」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（加入者向け）

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

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（加入者用）」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。

TSVビューア

- TSVファイル読込

TSV作成ツール **発行申請TSV** ▼

- CSRファイルから
- ~~証明書ファイルから~~
- 新規作成

クイック送信(ファイルを選択すると同時に送信します)

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な事項を入力してください。

通常は「dNSName」は空白のまま構いません。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。

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レコードの一覧です。

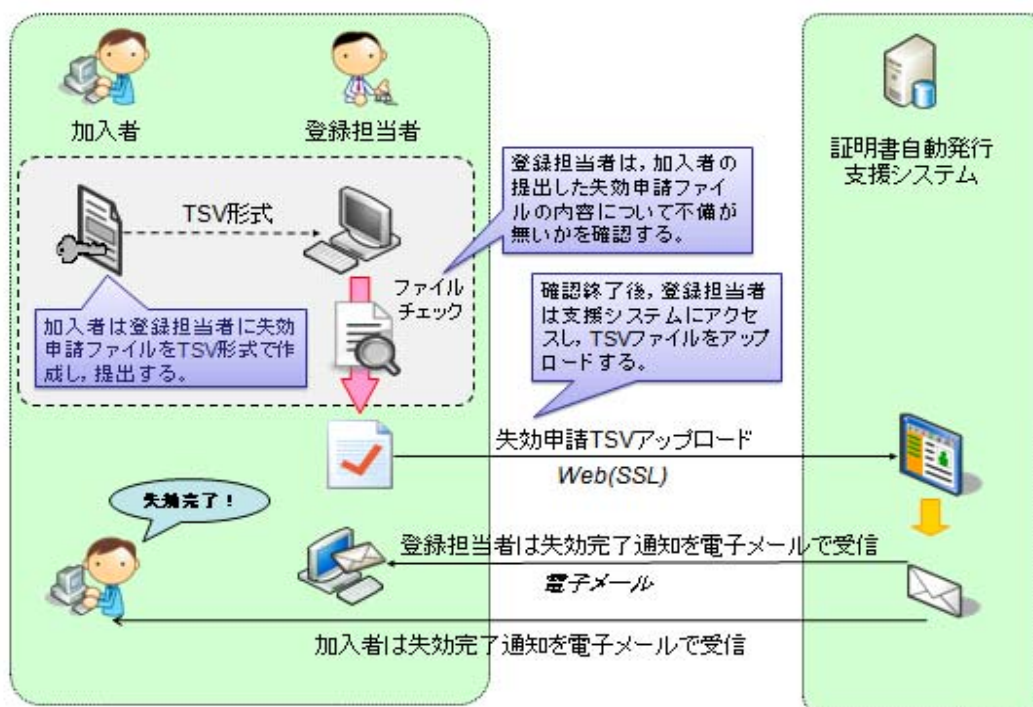
主体者DN	証明書プロファイルID	d3d4d5d6 CSR	加入者氏名	加入者所属	加入者Email	サーバ\FQDN	ソフトウェア名等	dNSName
CN=...	1	###	Apache 2.2.3	

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. 失効申請手続（登録担当者，加入者向け）

6-1. 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。



加入者は，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，登録担当者及び加入者の両方に失効完了通知が電子メールで送信されます。

No.	項目	担当	説明
1	サーバ証明書失効申請ファイルの作成及び登録担当者への提出	加入者 ↓ 登録担当者	加入者は，別途仕様に基づき「サーバ証明書失効申請ファイル」をTSV形式で作成し，登録担当者宛てに提出してください。
2	ファイルの確認	登録担当者	登録担当者は加入者が提出したTSVファイル記載情報を確認してください。
3	TSVファイルのアップロード	登録担当者	登録担当者は，確認済みのTSVファイルを「証明書自動発行支援システム」にアップロードすることで，サーバ証明書の失効申請を行います。 なお，TSVファイル形式に問題があった場合は，画面のエラーメッセージに従って，加入者にTSVファイルを再提出いただくように指示してください。
4	失効完了通知の受信	登録担当者 加入者	証明書自動発行システムから登録担当者と加入者に対して，失効完了通知が電子メールで送信されます。

加入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加入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加入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，加入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、加入者が失効申請 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 (加入者向け)

- 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。

証明書の表示方法によっては16進数表記で表示される場合がありますが10進数でご入力ください。

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

- 加入者mail
 - 加入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加入者メールアドレス(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。

加入者から失効申請 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

– 0(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加入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 (加入者向け)

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 (加入者用)」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 (加入者向け)

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。

The screenshot shows the 'TSVビューア' (TSV Viewer) interface. It contains several sections:

- TSVファイル読込**: A text input field followed by '参照...' and 'TSV送信' buttons.
- TSV作成ツール**: A dropdown menu currently showing '発行申請TSV'. A red circle highlights this dropdown, and a red rectangle highlights the '失効申請TSV' option which is selected.
- CSRファイル**: A text input field followed by '参照...' and 'CSR送信' buttons.
- 証明書ファイル**: A text input field followed by '参照...' and '証明書送信' buttons.
- 新規作成**: A '新規作成' button.

At the bottom, there is a checkbox labeled 'クイック送信(ファイルを選択すると同時に送信します)'.

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	<input type="text" value="CN=..."/>
シリアル番号	<input type="text" value="5150170000100100100 or 16進数:47-0470-40-4100-04"/>
加入者Email	<input type="text"/>
失効理由	<input type="text"/>
失効理由コメント	<input type="text"/>

末尾に新しいレコードを追加:

CSRから

証明書から

クイック送信

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 理由 コメント	d7 d8 d9	加入者Email	d11 d12 d13
CN=...		5150170000100100100	1				

作成したTSVファイルをダウンロードするにはこのボタンをクリックしてください。

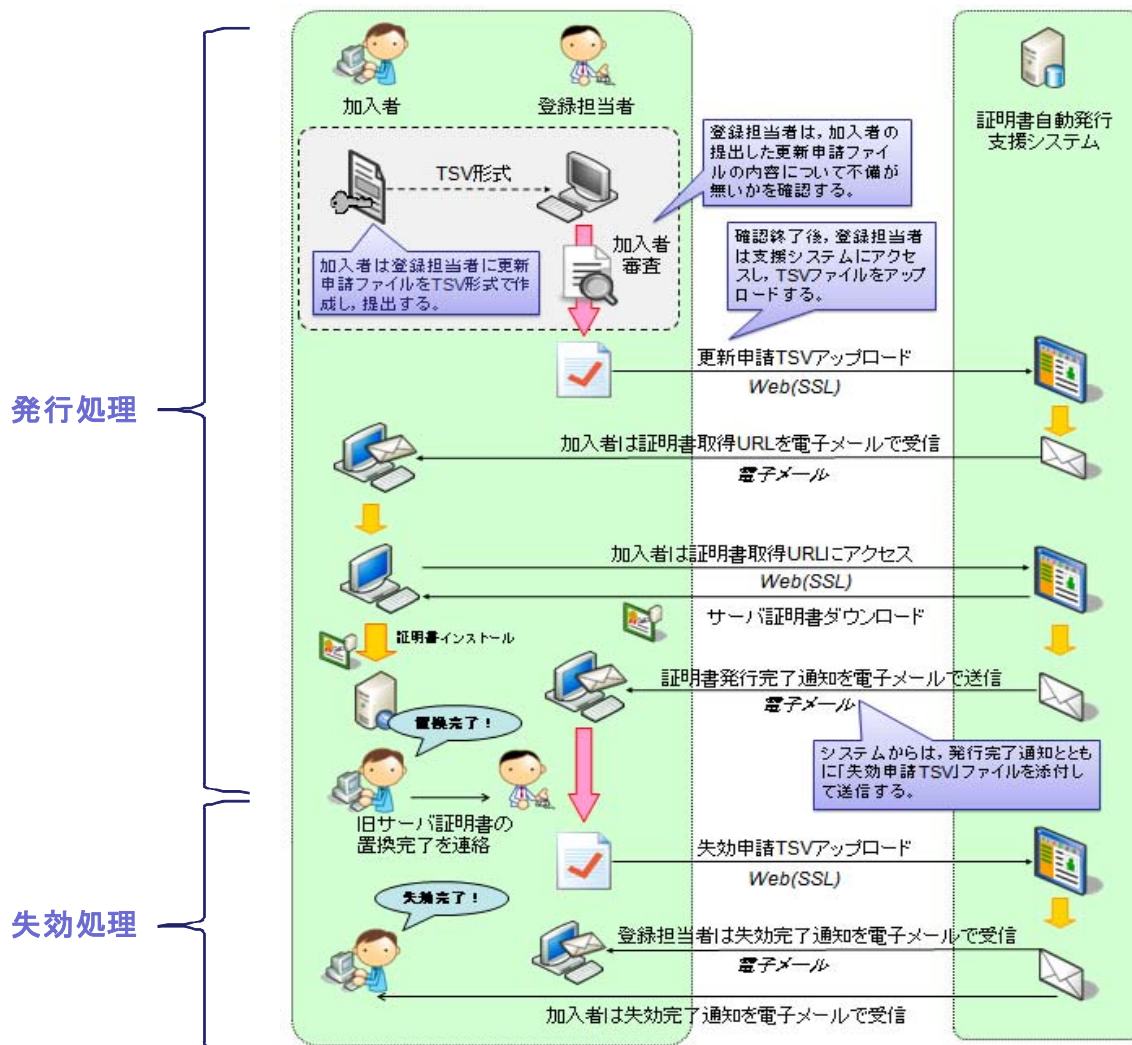
再編集したい場合は一旦ダウンロードしたファイルを再度アップロードしてください。

終了しましたら【終了】ボタンをクリックしてください。

7. 更新申請手続（登録担当者，加入者向け）

7.1. 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と失効申請手続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。



加入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 が加入者宛てに通知され，その URL から更新後の証明書を加入者が直接ダウンロードし加入者サーバにインストールします。

ここで，発行申請手続では，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，加入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と同様に登録担当者及び加入者宛てに失効完了通知をシステムから受信し，本手続は完了することとなります。詳細は次表のとおりです。

更新申請手続きの流れについては、以下のとおりです。

No.	項目	担当	説明
1	サーバ証明書更新申請ファイルの作成及び登録担当者への提出	加入者 ↓ 登録担当者	加入者は、別途仕様に沿ってサーバ証明書更新申請ファイルを作成し、登録担当者へ提出します。この際、加入者のメールアドレスは今後の処理の中で重要なものとなりますので、必ず間違いがないよう正確に入力するようにしてください。
2	加入者の申込及びファイルの確認	登録担当者	登録担当者は、サーバ証明書の更新を申請する加入者の本人性・住所等について確認し、かつ、TSVファイル記載情報について確認を実施してください。
3	TSVファイルのアップロード	登録担当者	登録担当者は、確認済みのTSVファイルを「証明書自動発行支援システム」にアップロードすることで、サーバ証明書更新申請を行います。TSVファイル形式に問題がなければ、加入者に証明書発行URLをシステムから自動で送附します。なお、TSVファイル形式に問題があった場合は、画面のエラーメッセージによって、加入者にTSVファイルを送信いただくよう表示してください。
4	証明書取得URL受領	加入者	証明書自動発行支援システムから申込加入者に対し、証明書取得URLが通知されます。
5	証明書ダウンロード	加入者	加入者は、前項の証明書取得URLにアクセスし、証明書をダウンロードしてください。
6	発行完了通知の受信	システム ↓ 登録担当者	加入者から更新申請の完了と証明書の発行が完了した際、登録担当者宛てに証明書発行完了通知が失効申請TSVファイルと共に送信された際、電子メールで送信されます。
7	領受済完了通知	加入者 ↓ 登録担当者	領受済証明書を入力した加入者は、サーバに導入されているサーバ証明書を更新後の証明書に置き換えさせ、登録担当者宛に領受済完了の通知を行ってください。加入者から登録担当者への通知方法は画面で任意に変更してください。
8	TSVファイルのアップロード	登録担当者	登録担当者は、前項で通知されたTSVファイルが「証明書自動発行支援システム」にアップロードすることで、更新後のサーバ証明書の失効申請を行います。
9	失効完了の通知	登録担当者 及び 加入者	登録担当者及び加入者は、証明書自動発行支援システムから失効申請が完了した際のメールを受信することで、本更新申請が完了したことがわかります。

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(≠ superseded)」が失効理由として設定されます。)
- 加入者氏名・加入者所属
 - 更新前サーバ証明書の加入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
- 加入者E-mail
 - 加入者メールアドレスに間違いがないこと
 - 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。

証明書の表示方法によっては16進数表記で表示される場合がありますが10進数でご入力ください。

加入者から更新申請 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://upki-portal.nii.ac.jp/docs/odcert/document/install>

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。

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

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。

The screenshot shows the 'TSVビューア' (TSV Viewer) interface. It contains several sections:

- TSVファイル読込**: A text input field followed by '参照...' and 'TSV送信' buttons.
- TSV作成ツール**: A dropdown menu with '発行申請TSV' selected. The dropdown list shows '発行申請TSV', '更新申請TSV' (highlighted in blue), and '発効申請TSV'. This section is circled in red.
- CSRファイルから**: A text input field followed by '参照...' and 'CSR送信' buttons. This row is highlighted with a red box.
- 証明書ファイルから**: A text input field followed by '参照...' and '証明書送信' buttons.
- 新規作成**: A '新規作成' button.
- クイック送信**: A checkbox labeled 'クイック送信(ファイルを選択すると同時に送信します)'.

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

更新申請TSV

旧証明書シリアル番号 or 6進数

号

CSR-----BEGIN CERTIFICATE REQUEST-----
 MIID...-----END CERTIFICATE REQUEST-----

主体者DN

サーバFQDN

dNSName

加入者Email

加入者氏名

加入者所属

ソフトウェア名等

末尾に新しいレコードを追加:
 CSRから
 証明書から
 クイック送信

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。

TSVツール α版

1件の更新申請TSVレコードの一覧です。

主体者DN	証明書 プロファイルID	旧証明書シリアル番号	d5d6 CSR	加入者氏名	加入者所属	加入者Email	サーバFQDN	ソフトウェア名等	dNSName
<input type="text"/>	1	0100470000100120007	###	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Apache 2.2.3	<input type="text"/>

作成したTSVファイルをダウンロードするにはこのボタンをクリックしてください。
 再編集したい場合は一旦ダウンロードしたファイルを再度アップロードしてください。

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 イニシアティブサイト上に掲載しております。ご参照ください。

<https://upki-portal.nii.ac.jp/docs/odcert/document>

【規程類】

- 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要領
- 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に関する事務手続き要領
- UPKI オープンドメイン証明書自動発行検証プロジェクト証明書利用に係る申合せ
- 国立情報学研究所オープンドメイン認証局 2 証明書ポリシー (Certificate Policy : CP)
- 国立情報学研究所運用支援認証局証明書ポリシー (Certificate Policy : CP)
- セコム電子認証基盤認証運用規程 (Certificate Practice Statement : CPS)

【申請書類】

- 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申請書、変更申請書、変更届
- UPKI オープンドメイン証明書自動発行検証プロジェクト確認実施手順調査票

【マニュアル等】

- UPKI オープンドメイン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 オープンドメイン証明書自動発行支援システム操作手順書 (加入者用)
- UPKI オープンドメイン証明書インストールマニュアル一式

【FAQ】

- UPKI オープンドメイン証明書自動発行検証プロジェクト FAQ
- <https://upki-portal.nii.ac.jp/docs/odcert/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