

「サーバ証明書の発行・導入における評価・啓発研究プロジェクト」および「UPKI オープンドメイン証明書自動発行検証プロジェクト」の変更点について (登録担当者編)

「サーバ証明書の発行・導入における評価・啓発研究プロジェクト」(以下、旧プロジェクト)の登録担当者の方が、「UPKI オープンドメイン証明書自動発行検証プロジェクト」(以下、新プロジェクト)で引き続き登録担当者を継続されるにあたって、新プロジェクトでの改善点や注意すべき事項について以下に記します

1. 旧プロジェクトからの改善点

新プロジェクトでは、発行・更新・失効申請の効率化を実現するために証明書自動発行支援システム(以下、「支援システム」)を導入しました。これにより、改善された主要な項目について以下に記します。

(ア) 申請様式が Excel 形式から TSV 形式になりました

新プロジェクトでは、Excel 形式の申請書を廃止して、TSV(タブ区切り)形式の申請ファイルを使用することになりました。この申請 TSV ファイルは、加入者自身で作成していただくことを基本としていますが、各機関の状況等に応じて登録担当者の方が代行していただいても構いません。

⇒Web: TSV ツール (Web アプリ版) の使い方

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

(イ) 申請方法が S/MIME 署名メールから Web アップロードになりました

新プロジェクトでは、支援システムにログインするためのクライアント証明書を登録担当者の方に配付します。登録担当者の方は支援システム上で申請 TSV ファイルをアップロードすることになります。

⇒PDF: 証明書自動発行支援システム操作手順書 (登録担当者用)

https://upki-portal.nii.ac.jp/docs/files/odcert_sciaoperation_lra.pdf

(ウ) 加入者が直接証明書をダウンロードできるようになりました

新プロジェクトでは、支援システムにアップロードされた発行・更新申請にもとづきサーバ証明書を発行した後、証明書取得 URL が記載されたメールを事務局から加入者に通知します。加入者は、この証明書取得 URL にアクセスすることで、直接サーバ証明書をダウンロードできるようになりましたので、登録担当者の方はサーバ証明書を配付いただく必要がなくなりました。

(エ) 申請履歴を含む証明書情報をダウンロードできるようになりました

登録担当者の方は、支援システムにログインして、申請履歴や発行済証明書ファイルを含む証明書情報をダウンロードすることが可能になりました。申請状況の確認や、加入者の証明書紛失時などにご活用いただけます。

⇒PDF: 証明書自動発行支援システム操作手順書（登録担当者用）

https://upki-portal.nii.ac.jp/docs/files/odcert_sciaoperation_lra.pdf

2. 新プロジェクトでの新しい証明書の申請方法

旧プロジェクトで証明書発行済の加入者サーバに対して、新プロジェクトから証明書の発行を受ける場合であっても、**新プロジェクトでの新規の発行になりますので「発行申請」を行っていただく**必要があります。

「更新申請」は、新プロジェクトで証明書発行を受けた後に、証明書の再発行や記載事項の変更を行う際の手続きとなります。

なお、新プロジェクトでは「1. 旧プロジェクトからの改善点」(ア)で述べた通り Excel形式の申請書を廃止し、TSV(タブ区切り形式)ファイルによる申請となります。

⇒Web: 利用の手引き→加入者編→「新規証明書発行申請手続き」

<https://upki-portal.nii.ac.jp/docs/odcert/howto/ee#case1>

⇒PDF: 利用の手引き p.18 「5. 発行申請手続(登録担当者、加入者向け)」

https://upki-portal.nii.ac.jp/docs/files/odcert_tebiki.pdf

3. 新プロジェクト証明書へ置き換え後の旧プロジェクト証明書の失効方法

新プロジェクトへの移行期限である平成 21 年 9 月 30 日以降、旧プロジェクト認証局(NII オープンドメイン認証局)では以下の閉局作業を行います。

- ・ 旧プロジェクト認証局が発行した全ての証明書の一括失効
- ・ 上位 SC-Root1 による旧プロジェクト認証局証明書の失効

旧プロジェクトでは通常、新しい証明書への置き換えが完了した際には、旧証明書を失効するために置き換え完了通知を、登録担当者経由でプロジェクト事務局に通知する必要があります。しかしながら、今回の新プロジェクトへの移行にあたっては上記閉局作業において一括失効しますので、新プロジェクトの証明書へ置き換えが完了した際に**旧プロジェクトの証明書について失効申請していただく必要はございません。**

ただし、移行期間終了までの間に鍵ペアの危殆化(紛失・漏洩等)した場合など急ぎ失効する必要がある場合には、上記に関わらず直ちに失効申請を行っていただくようお願いいたします。

⇒Web: 各種手続き→失効手続き

<https://upki-portal.nii.ac.jp/docs/server/5>

4. DN 使用可能文字の変更

新プロジェクトでは、サーバ証明書の DN に使用可能な文字が変更になりました。なお、使用不可能となっている一部の文字については見直しを検討しており、近々に対応する予定です。使用禁止文字は支援システムでもチェックしていますが、登録担当者の方の作業を効率よく進めていただくためには、申請前にこれらの文字が使用されていないことをご確認いただくことをお勧めいたします。

1) サーバ証明書の CN に使用できる文字

FQDN として使用可能な文字だけに制限しました。英数字の他に使用可能な文字はハイフン、ピリオドのみになります。

2) O,OU に使用できる文字

現状では旧プロジェクトと比較して左括弧および右括弧が追加されましたが、アポストロフィ、プラス、カンマ、イコールの4種類の文字が使用できなくなっています。近々に改修を行い互換性確保を図る予定ですが、プラスに限ってはシステム上の制約で改修後も使用することができませんのでご了承ください。

表 1 サーバ証明書の DN 使用可能文字に関する変更点

		英字	数字	空白	ア ポ ス ト ロ フ イ	左 括 弧	右 括 弧	プ ラ ス	カ ン マ	ハ イ フ ン	ピ リ オ ド	ス ラ ッ シ ュ	コ ロ ン	イ コ ー ル	ク エ ス チ ヨ ン
		A-z	0-9		'	()	+	,	-	.	/	:	=	?
旧	O,OU,CN	○	○	○	○	×	×	○	○	○	○	×	○	○	×
新	CN	○	○	×	×	×	×	×	×	○	○	×	×	×	×
	O,OU	○	○	○	×	○	○	×	×	○	○	×	○	×	×
	改修後	○	○	○	○	○	○	×	○	○	○	○	○	○	×

以上