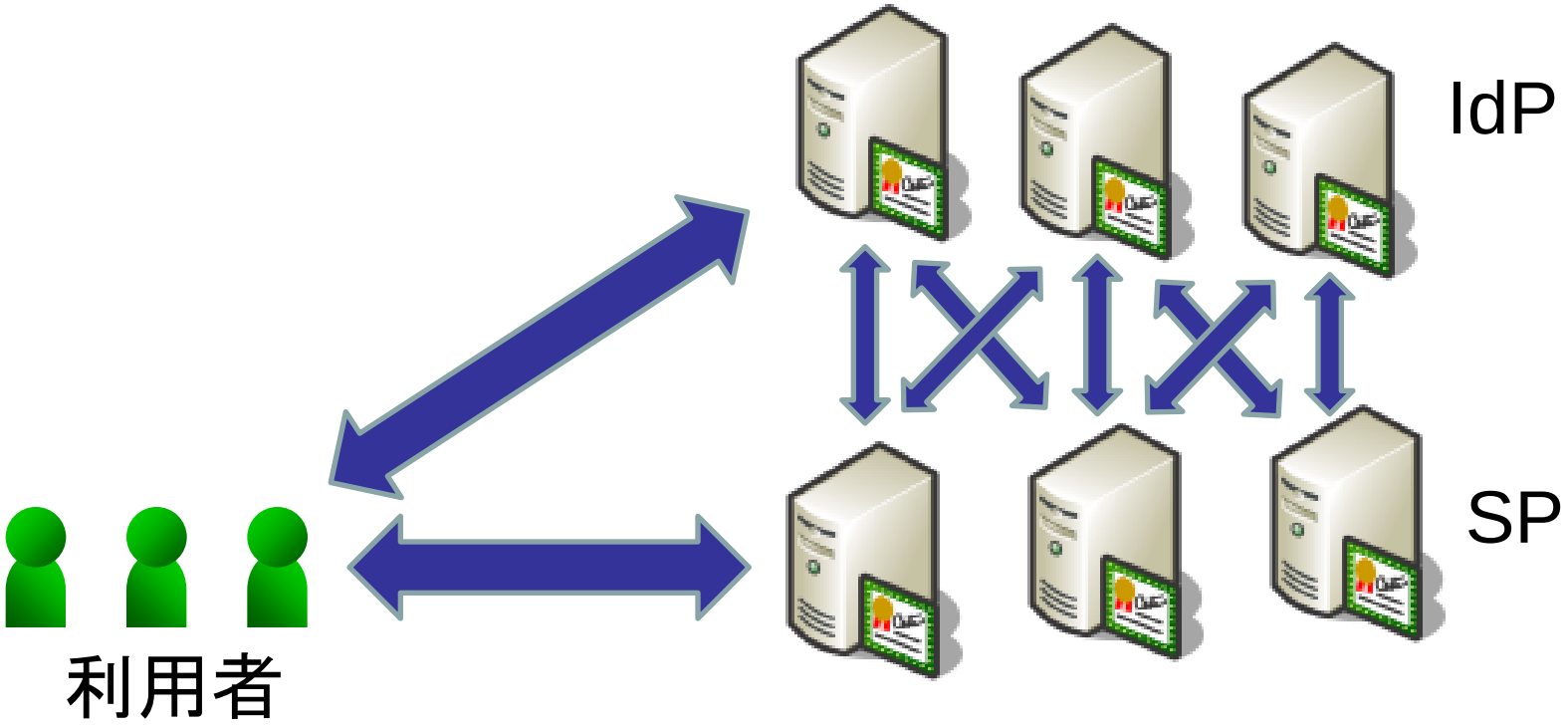
オープンドメイン証明書
自動発行検証プロジェクトについて

国立情報学研究所

はじめに:
学術認証フェデレーションとの関係

- IdP/SP等サーバの認証に証明書を用いる
  - 電子証明書(PKI)はWebセキュリティの根幹



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概要

- 目的

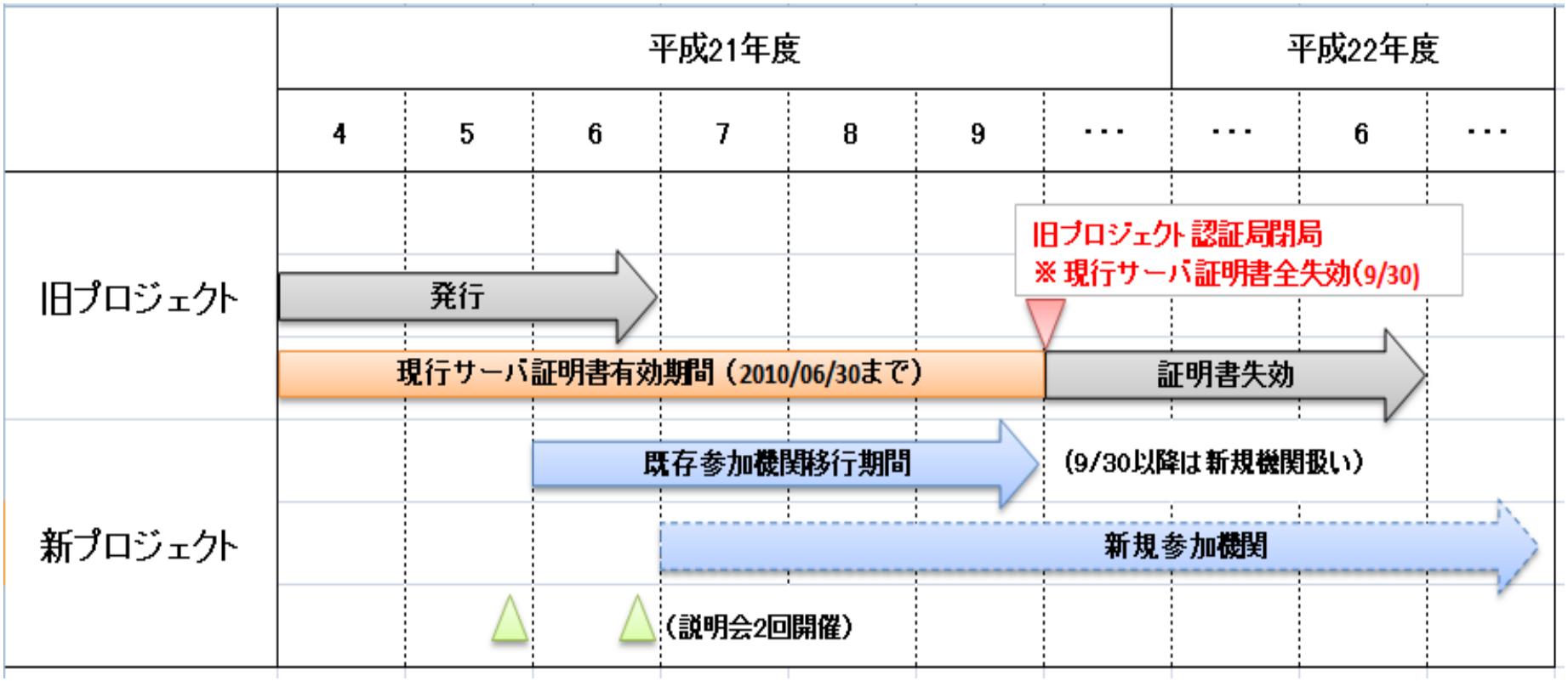
  サーバ証明書発行・導入における啓発・評価研究プロジェクト（旧プロジェクト）で得た知見をもとに，NIIが開発した電子証明書自動発行支援システムを用いて，学術機関へのサーバ証明書発行プロセスの最適化および自動化について検証を行う。

- 実施期間

  平成21年4月1日 ～ 平成24年3月31日

- 実施内容
  - プロジェクトに協力いただく機関(参加機関)を募集します。
  - 参加機関に対してサーバ証明書を発行し，協同して検証評価を実施します。（年度末に評価項目について調査を実施）

プロジェクト実施スケジュール

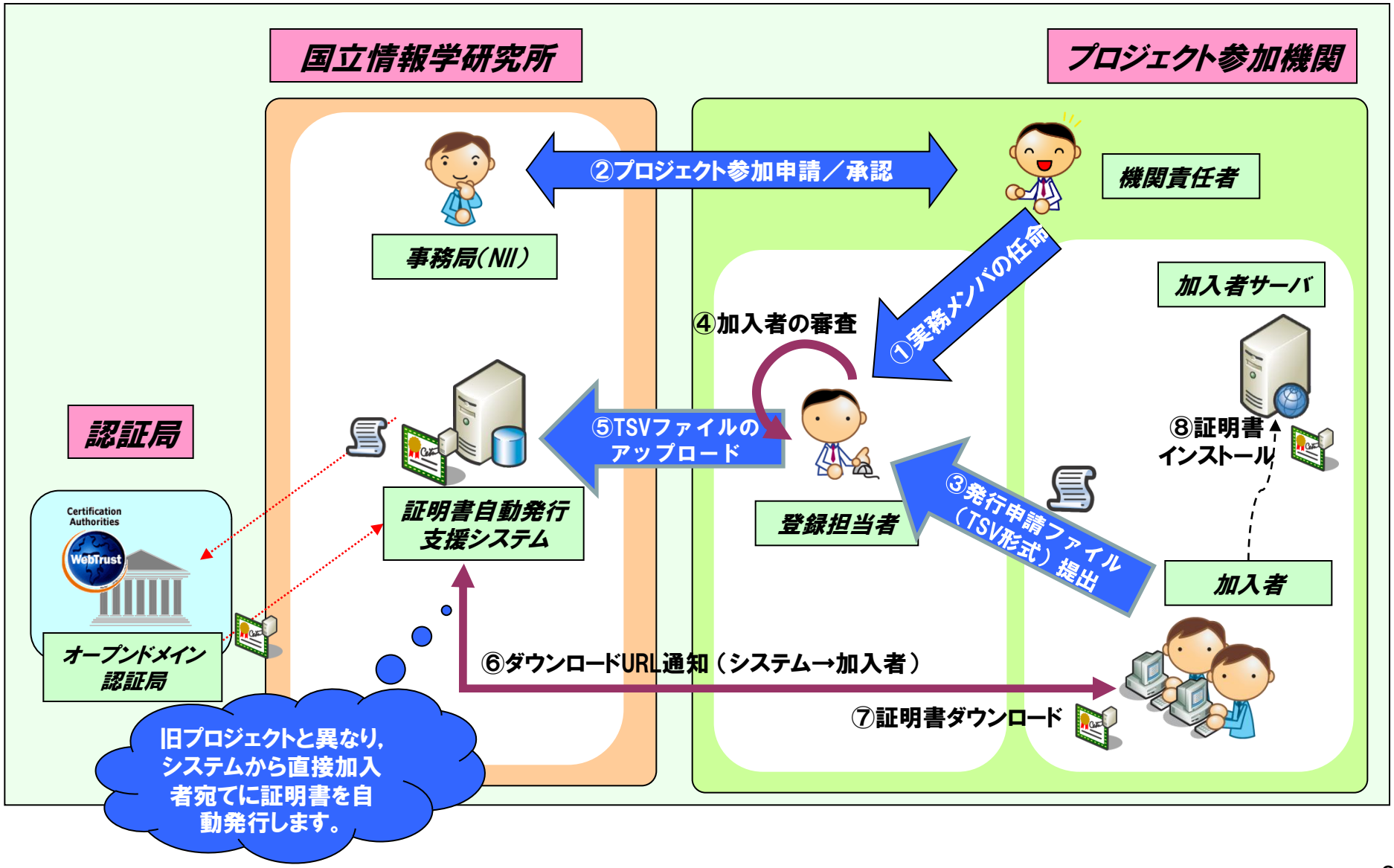


新・旧プロジェクトにおける変更点

変更点	旧プロジェクト	新プロジェクト
対象ドメイン	1機関1ドメイン	1機関複数ドメインに対応(NEW!)
登録担当者認証	S/MIME証明書 （メール送信者の認証）	クライアント証明書 （支援システムへのログイン）
証明書発行申請	発行申請書をExcelファイルで記載のうえ，電子メールで事務局まで送信	加入者が作成したTSVファイルを登録担当者が「支援システム」にアップロード
証明書発行	事務局から電子メールで登録担当者へ送付後，登録担当者から加入者へ個別配付	加入者が直接「支援システム」からダウンロード
プロジェクト参加申請	機関責任者の実在性確認として「機関責任者」の依頼文を送信	事務局が機関責任者の本人性を確認
証明書有効期間	平成21年10月末に全失効 (有効期間は平成22年6月30日まで)	発行日から25ヶ月(※1)
証明書チェーン	+ STN-Root1 + SC-Root1 + NII Open Domain CA + <サーバ証明書>	+ SC-Root1 + NII Open Domain CA + <サーバ証明書>

※1: 将来鍵長に応じて有効期間を見直す可能性あり

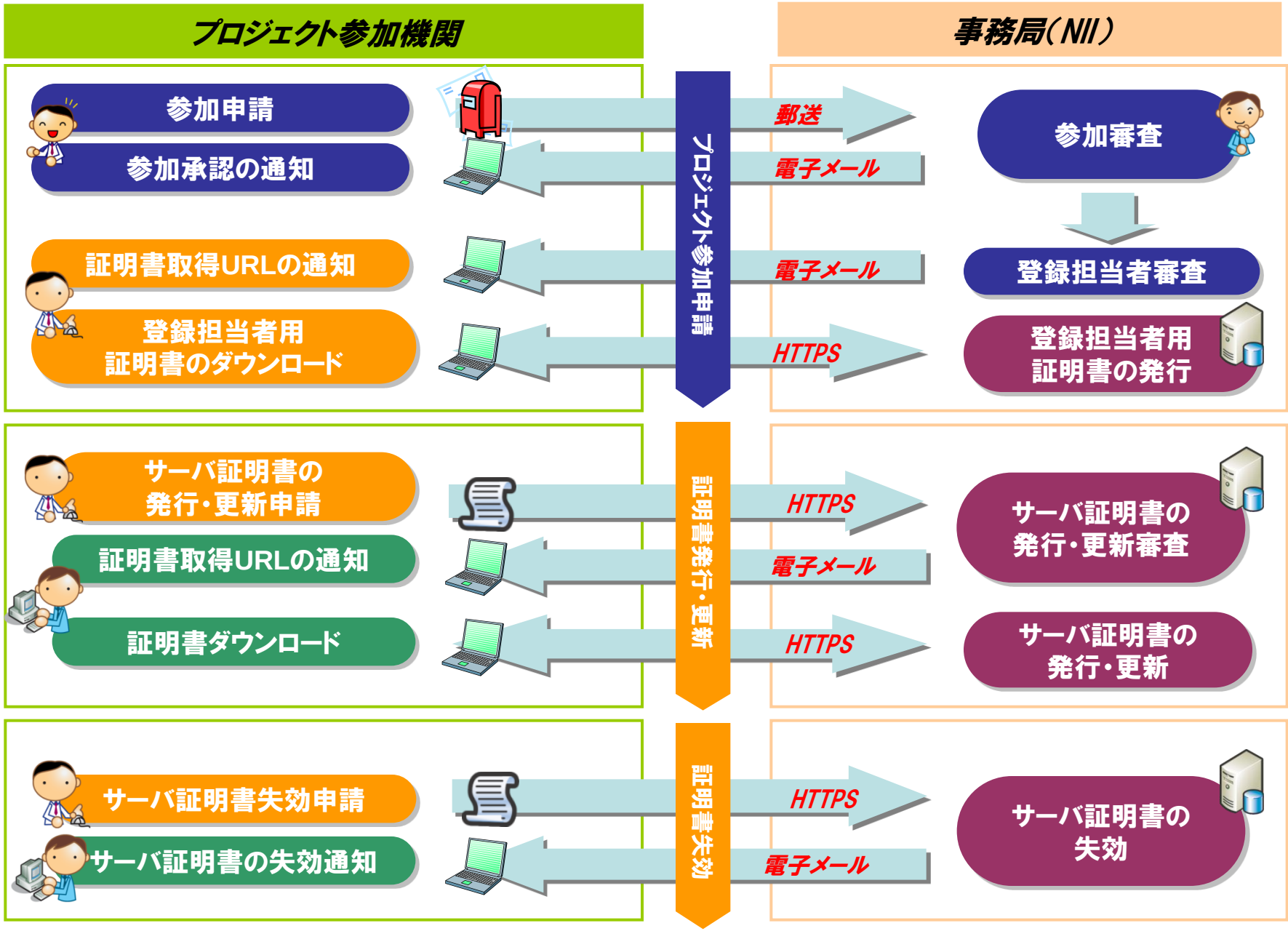
プロジェクト概念図


国立情報学研究所
プロジェクト参加機関
②プロジェクト参加申請／承認
機関責任者
事務局(NII)
①実務メンバの任命
加入者サーバ
④加入者の審査
⑤TSVファイルの
アップロード
⑧証明書
インストール
認証局
証明書自動発行
支援システム
登録担当者
③発行申請ファイル
（TSV形式）提出
加入者
Certification
Authorities
WebTrust
オープンドメイン
認証局
⑥ダウンロードURL通知（システム→加入者）
⑦証明書ダウンロード
旧プロジェクトと異なり，
システムから直接加入
者宛てに証明書を自
動発行します。

プロジェクトで使用する用語と役割

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利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NIIの事務窓口です。
各大学	機関責任者 	本プロジェクト参加にあたり，各機関で選出いただく代表者の方。課長職または准教授相当以上の常勤教職員の方にお願いいたします。
	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および加入者の審査業務の一部をお願いする方です。大学の規模等に応じて複数名選出していただくことも，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，サーバ証明書を実際に利用される方。プロジェクト参加機関内の常勤の教職員の方であれば，どなたでも加入者となれます。
	加入者サーバ	加入者の方が管理するサーバ。

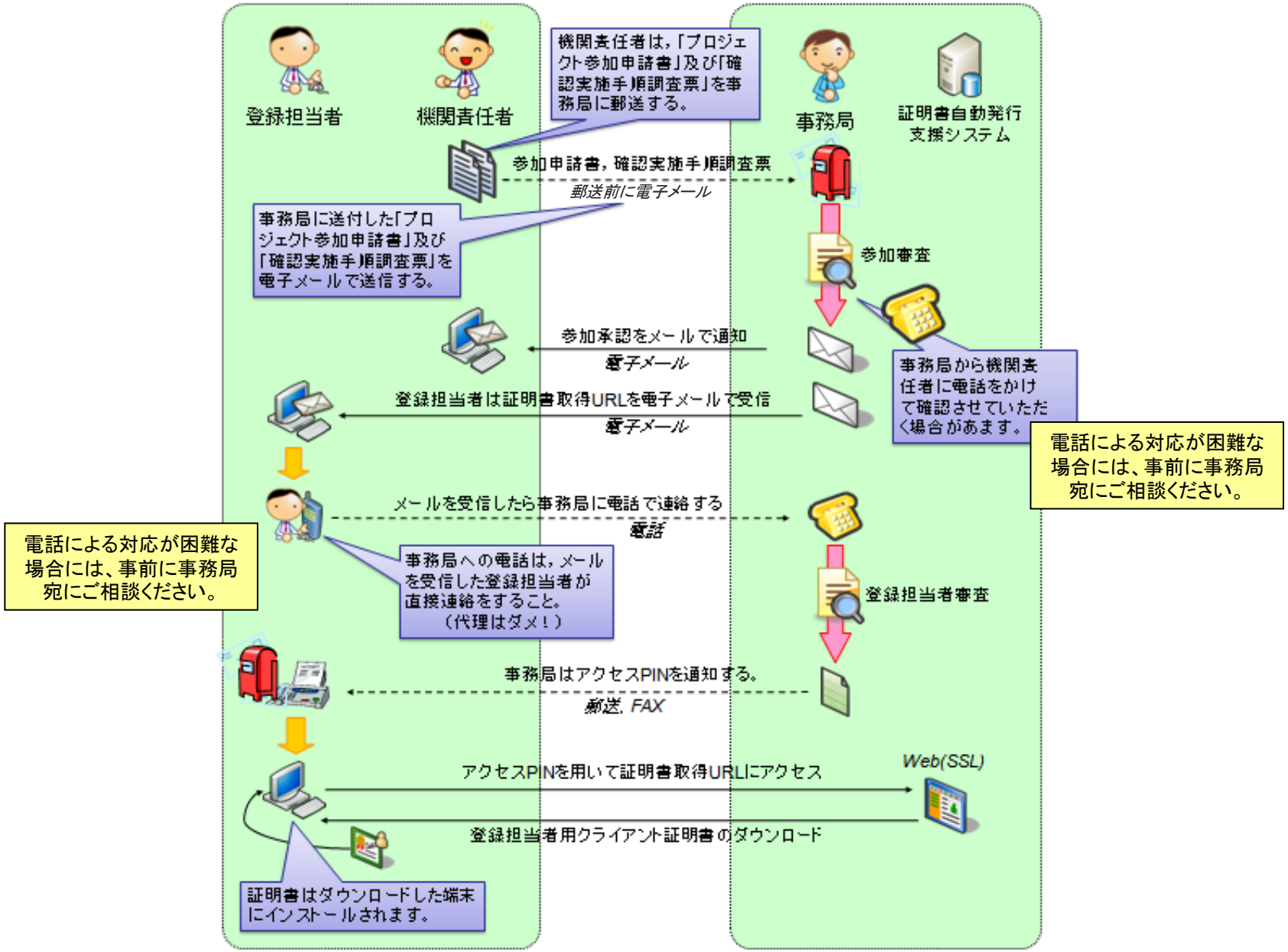
事務フロー全体の概要


プロジェクト参加機関
事務局（NII）
参加申請
参加承認の通知
証明書取得URLの通知
登録担当者用
証明書のダウンロード
郵送
電子メール
電子メール
HTTPS
プロジェクト参加申請
参加審査
登録担当者審査
登録担当者用
証明書の発行
サーバ証明書の
発行・更新申請
証明書取得URLの通知
証明書ダウンロード
HTTPS
電子メール
HTTPS
証明書発行・更新
サーバ証明書の
発行・更新審査
サーバ証明書の
発行・更新
サーバ証明書失効申請
サーバ証明書の失効通知
HTTPS
電子メール
証明書失効
サーバ証明書の
失効

プロジェクトの主な申請手続き

手続き	概要・処理の流れ
プロジェクト参加申請	・機関の所有するドメイン毎にプロジェクトへの参加申請が必要です
	機関責任者→事務局（郵送: 参加申請書・確認実施手順調査票）
サーバ証明書発行申請	・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 ・発行済証明書の主体者DNの変更が必要な場合
	加入者→登録担当者→支援システム（Web: 発行申請用TSVファイル）
サーバ証明書更新申請	・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合 ・サーバ証明書の記載事項（DN以外）について変更が必要な場合
	加入者→登録担当者→支援システム（Web: 更新申請用TSVファイル）
サーバ証明書失効申請	・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 ・発行済証明書の主体者DNの変更を行った後（旧証明書に対して）
	（加入者→）登録担当者→支援システム（Web: 失効申請用TSVファイル）

プロジェクト参加申請の流れ（概要図）



プロジェクト参加申請の流れ

No.	項　目	担　当	説　明
1	参加規程等の確認	機関責任者 登録担当者	次の書類を十分に理解し，承諾してください。 ・プロジェクト参加要領および事務手続き要領 ・サーバ証明書利用に係る申合せ ・オープンドメイン認証局2 証明書ポリシ（Certificate Policy） ・運用支援認証局 証明書ポリシ（Certificate Policy） ・セコム電子認証基盤 認証運用規程（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・実在性を確認のうえ，任命を行なってください。
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確認手順調査票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。※記入例は後述
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様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の結果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得URLについてご連絡させていただきます。
6	アクセスPIN取得連絡	登録担当者 ↓ 事務局	前項5の証明書取得URL通知を受信した登録担当者の方々は，登録担当者審査のため各自お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PIN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PINを受領されましたら，前項5でご連絡した証明書取得URLにアクセスして前項6のアクセスPIN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。

登録担当者の本人性・実在性確認
「利用の手引き」を参考に確認をお願いします。
また，実際に確認いただいた手順について確認実施手順調査票に記入してください。

プロジェクト参加申請書（表面）の記入例 （1/2)

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

記入例

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

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	情報　太郎		所　属	情報基盤センター
	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	情報基盤センター
	ローマ字	Kenkyu	Hanako		
	職　名	准教授		電話番号	03-1111-7777
	E-Mail	hanako@example.ac.jp		FAX	03-1111-8888
	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	事務	一朗	所　属	基盤企画課
	ローマ字	Jimu	Ichiro		
	職　名	基盤企画課長		電話番号	03-8888-9999
	E-Mail	ichiro@example.ac.jp		FAX	03-8888-5555
	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				
	職　名			電話番号	
	E-Mail			FAX	

手書き自署のうえ，押印をお願いします。

書類確認者

機関責任者

機関責任者は，本人性・実在性を確認・審査したうえで，登録担当者を任命してください。

4名以上の登録担当者を任命する必要がある場合は，事前に事務局までご相談ください。

プロジェクト参加申請書（裏面）の記入例　（2/2)

（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　情報　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，ドメイン登録担当者[2]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：	情報　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)」(○○○第XX-NN号)を文書の写として添付します。どうぞよろしくお願い致します。

必ず確認のうえ選択肢を選んでください。なお，選択肢はリストから選択可能です。（全機関必須）

旧プロジェクトの参加機関のみいずれかを選択してください。

書類確認者

機関責任者

機関責任者の承継や事務局への連絡事項等についてご記入ください。

確認実施手順調査票の記入　(1/2)

確認実施手順調査票は，記入例を参考にしながら，貴学の実状に合わせて記入するようにしてください。

1-2　登録担当者の本人性確認

登録担当者の本人性確認を行うにあたって、「どのような情報」をもとに、「どのような方法で」確認を行い了承を得たのかを教えてください。

○	「登録担当者は既に面識があるので」「直接対面で問い合わせて」了承を得ました。
○	「登録担当者の教職員証を提示してもらい」「直接対面で」確認しました。 *面識がない登録担当者の場合、顔写真付きの教職員証を使用してください。*
○	「学内のLAN管理委員会において委員長が担当者を指名」し、「本人から直接」了承を得ました。
○	「最新の学内名簿で登録担当者の内線やメールアドレス」を確認し、「本人へ電話またはメールで問い合わせて」了承を得ました。
×	「登録担当者にメールまたは文書で任命通知を行い」「一定期間以内の異議申し立てがないことを以て」了承されたものとみなしました。 *登録担当者が必ずしもメールまたは文書を理解して合意したことが確認できません。*

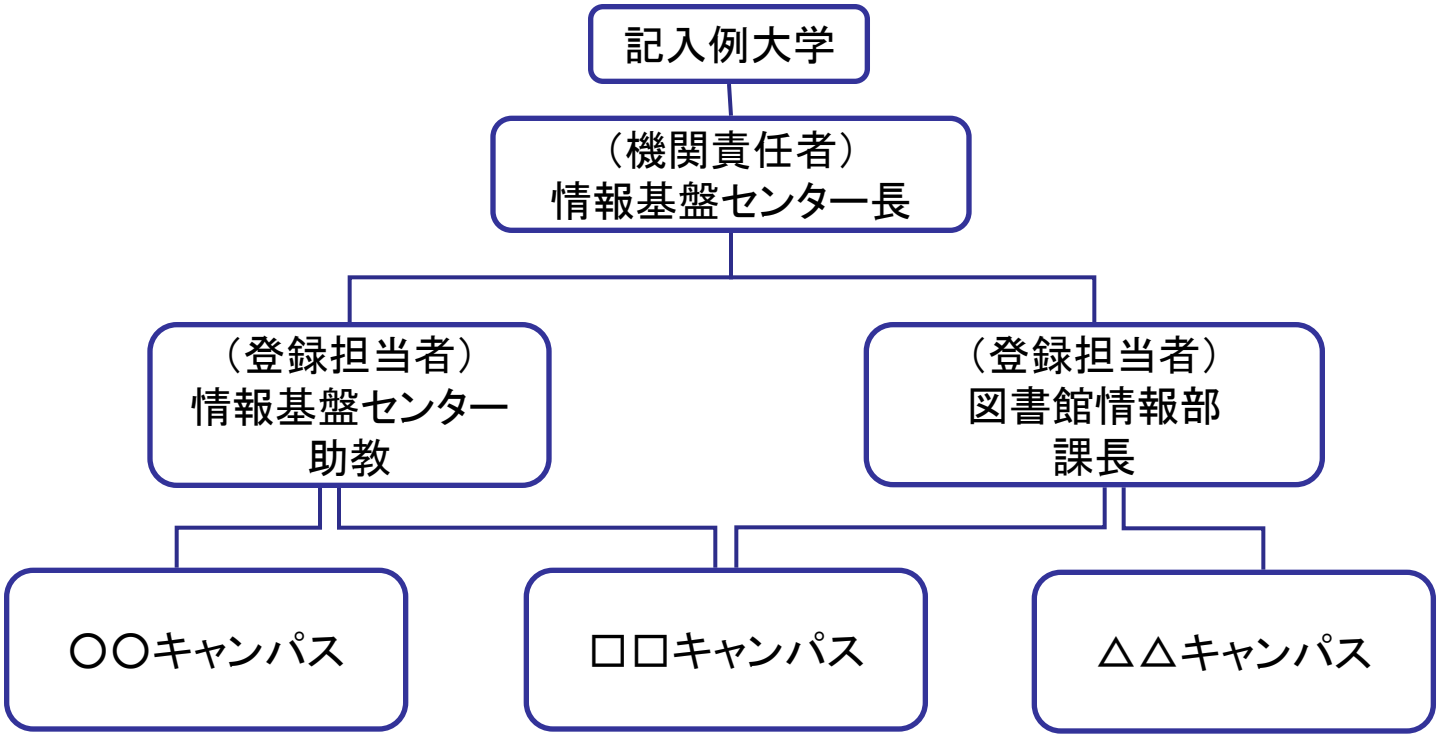
書類確認者

機関責任者

1-2	登録担当者の本人性確認
	登録担当者の本人性確認を行うにあたって，「どのような情報」をもとに，「どのような方法で」確認を行ったかを教えてください。
	「登録担当者は既に面識がある」ので「直接対面で問合わを行いながら」確認を実施した。また，身分証明書を提示していただいた。

確認実施手順調査票の記入　(2/2)

機関責任者と登録担当者の担当や体制を図示してください。

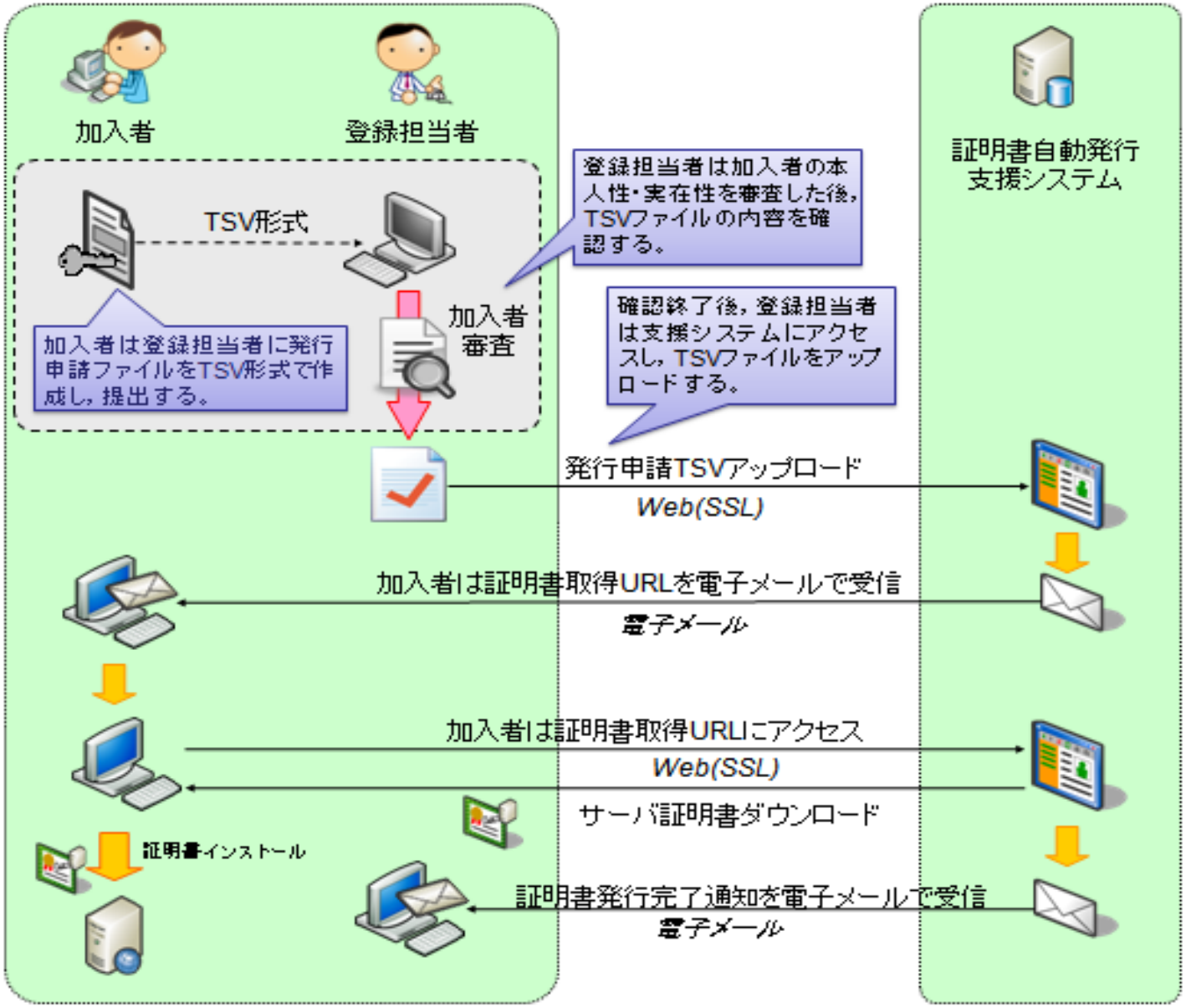


書類確認者

機関責任者

各登録担当者が所管の部局等をお持ちでしたら，併せまして体制図中にご記入ください。

サーバ証明書発行申請から証明書取得までの流れ



サーバ証明書発行申請から証明書取得までの流れ

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，別途仕様に基づき「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機関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無ければ，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受信	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認識することが可能となります。

加入者の本人性・実在性等の確認

登録担当者の方は，確認実施手順調査票の「加入者の本人性確認」および「加入者の実在性確認」などに記入いただいた確認実施手順にもとづいて確認を行ってください。

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名であること
- 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

※TSVファイルをEXCELで確認する際は，データ先頭に数字の”0”が存在する場合，“0”が消えてしまうことがありますのでご注意ください。
確認や修正には，テキストエディタをご利用ください。

サーバ証明書発行申請TSVファイル

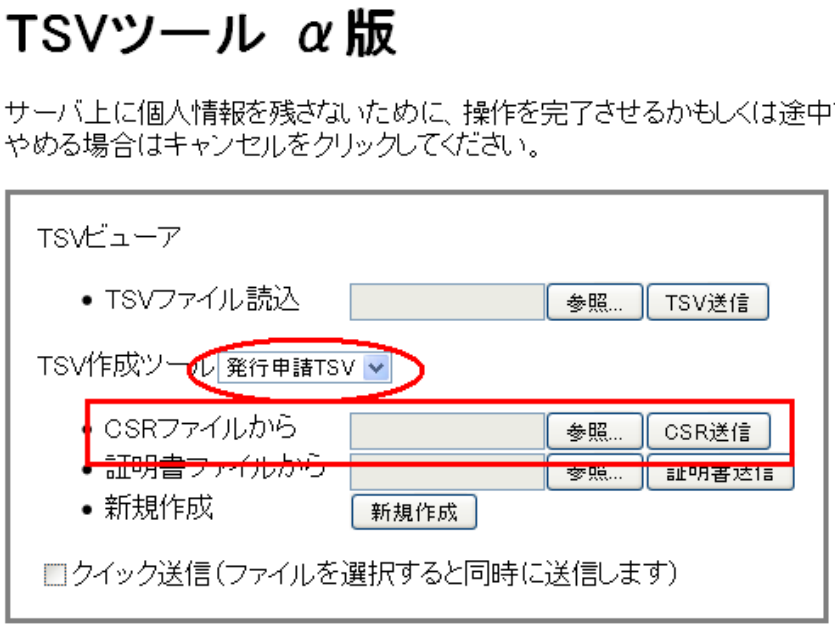
No.	項目名称	入力	入力文字	最大SIZE（文字数）	説　　明
1	主体者DN	必須	半角	250	・DNの順序はCN，OU（任意・複数可），O，L，Cとすること。 ・CN=<加入者FQDN>であること。 ・OUはいずれもprintable stringであること。 ・O=<機関名（英語表記）>，L=Academe2，C=JPとすること。 ・DNにstateOrProvince及びE-Mail属性を含まないこと。
2	証明書プロファイルID	必須	半角	1	・1（固定値）を記入してください。
3～6	予約済	ー	ー	ー	・何も入力しないでください。
7	CSR （証明書発行要求）	必須	半角	2048	・DNは#1の主体者DNと合致していること。 ・鍵長が1024bit以上であること。
8	加入者氏名	必須	全角・半角	64	・加入者の氏名を記入してください。
9	加入者所属	必須	全角・半角	64	・加入者の所属を記入してください。
10	加入者E-Mail	必須	半角	78	・特殊文字は使用できません。（ハイフン"-"，アンダースコア"_"，アットマーク"@"，ドット"."は利用できます。） ・証明書取得URLの通知に用いますので、入力ミスがないようご注意ください。
11	加入者FQDN	必須	半角	64	・証明書の発行を申請するサーバのFQDNを記入してください。その際，プロジェクト参加申請書に記載してある対象ドメインと一致していることを確認してください。
12	加入者ソフトウェア名 およびバージョン	必須	半角・全角	128	利用されているサーバソフトウェア名及びバージョンを記入してください。
13	dNSName	任意	半角	250	同一証明書に複数ホスト名を記載する場合に利用します。 利用詳細は別途事務局までお尋ねください。

※詳細は「支援システム操作手順書（加入者用）」をご確認ください。

発行申請TSVファイル作成支援ツールの使い方(1)

1)TSV作成支援ツールへアクセス
　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

2)CSRの送信
　各自で作成したCSRをツールに画面上から送信します。
　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うえで「CSRファイルから」の行の「参照」をクリックして，各自で既に作成済みのCSRを選択し「CSR送信」をクリックしてください。

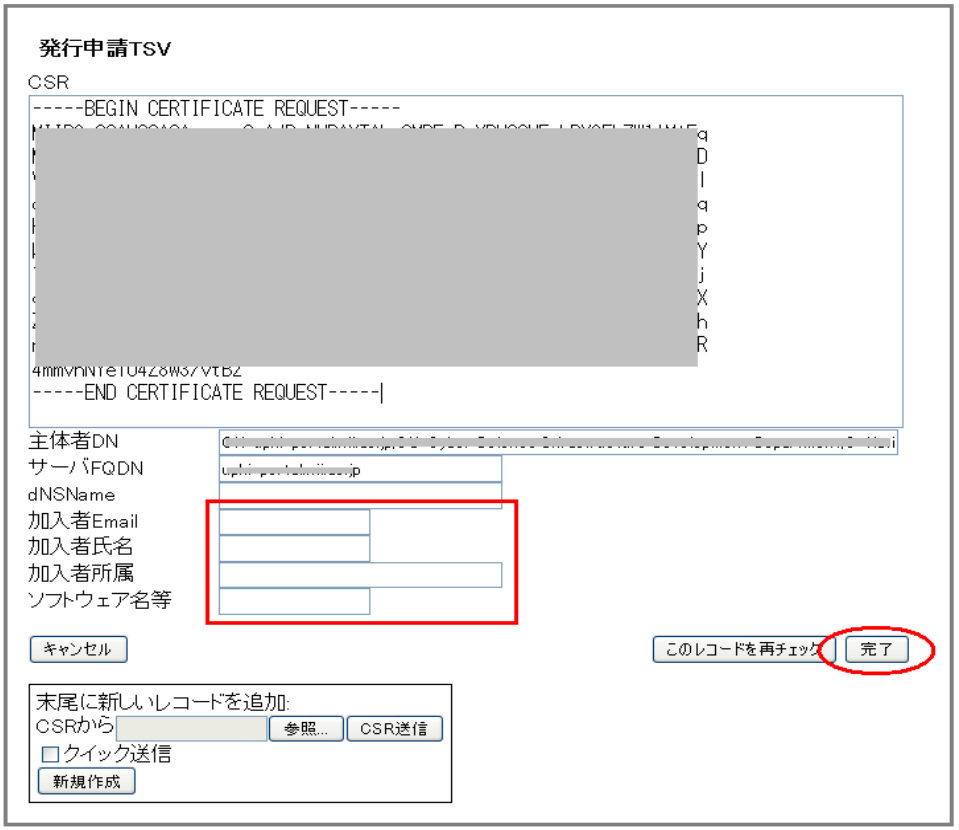


発行申請TSVファイル作成支援ツールの使い方(2)

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ます。

TSVツール α版

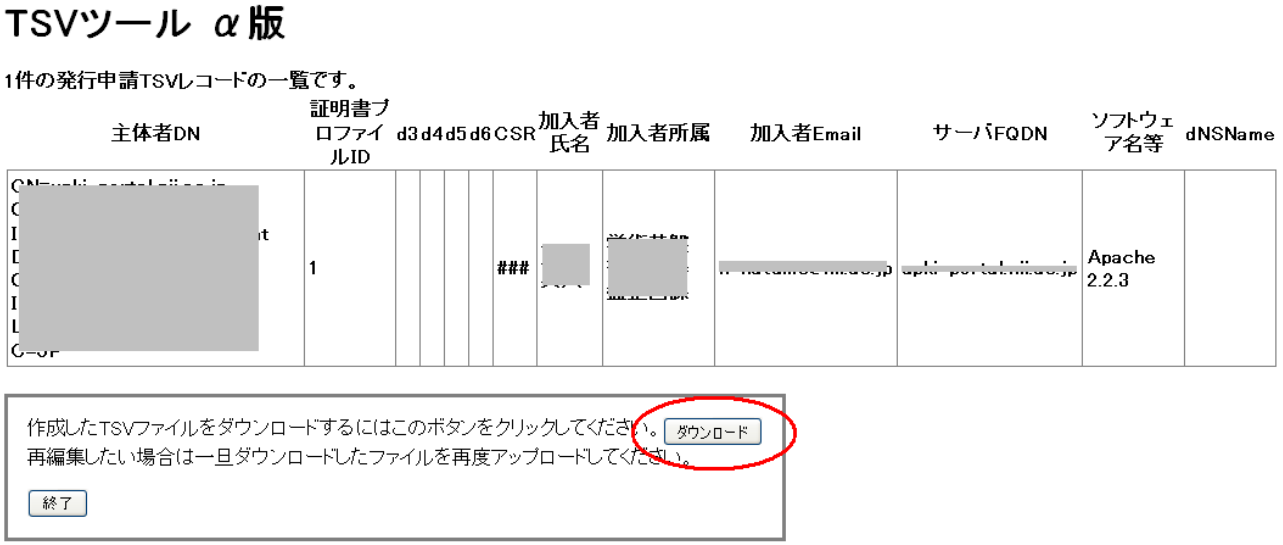


発行申請TSVファイル作成支援ツールの使い方(3)

4)発行申請TSVファイルの出力

次図のとおり，前操作3「サーバ証明書作成データの入力」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。

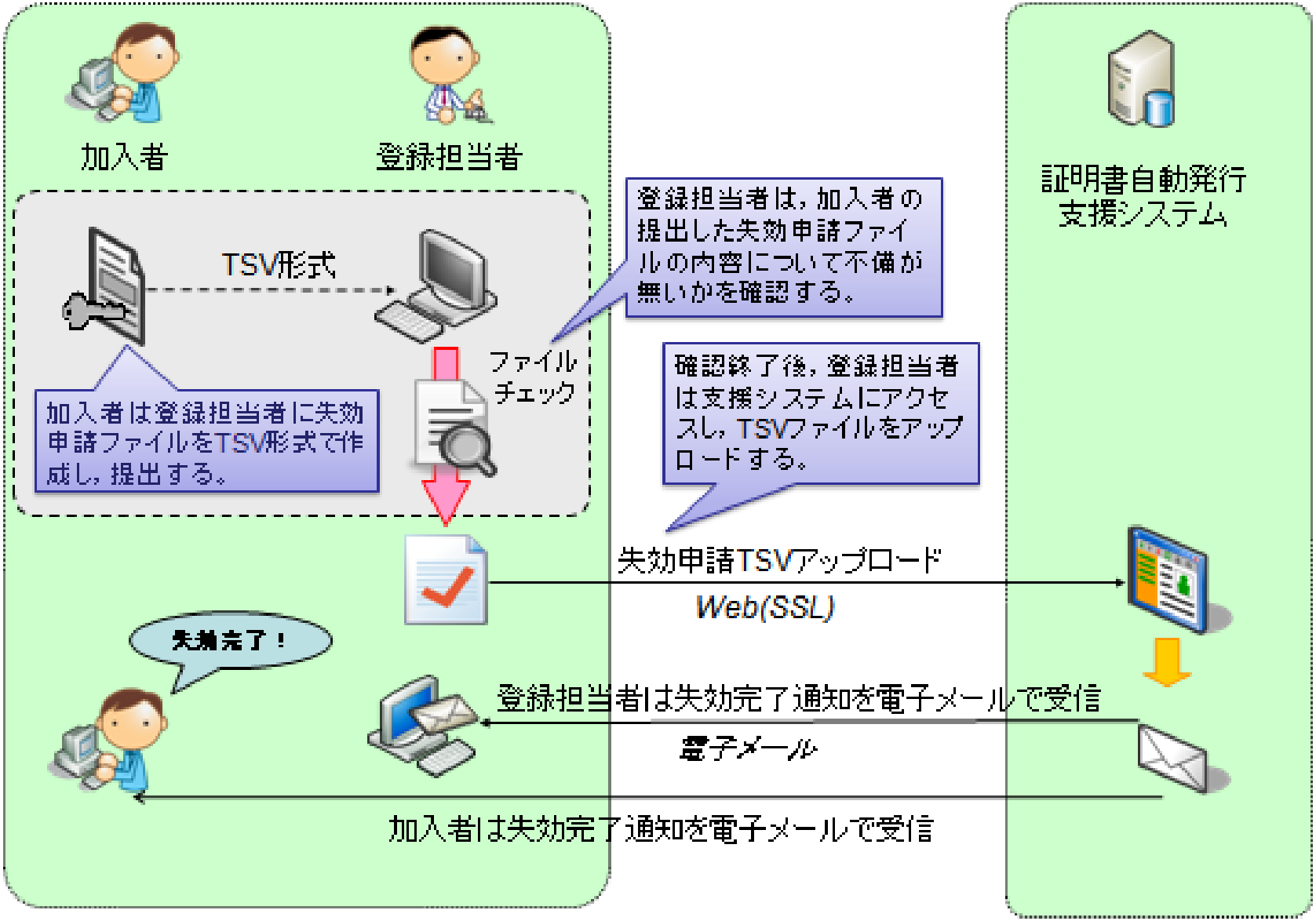
サーバ証明書発行申請TSVファイルがダウンロードできます。



※本ツールの利用方法の詳細は，以下のUPKIイニシアティブWebページをご覧ください。

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

サーバ証明書失効申請から失効完了までの流れ



サーバ証明書失効申請から失効完了までの流れ

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	証明書自動発行支援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，登録担当者が代理して，失効申請を行うことができることとします。
なお，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，本失効申請完了の通知は発信されます。

※加入者のメールアドレスを変更する必要がある場合には，別途，登録担当者を経由して事務局までご相談ください。

失効申請TSVファイル記載情報の注意点 (加入者向け)

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。

- 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

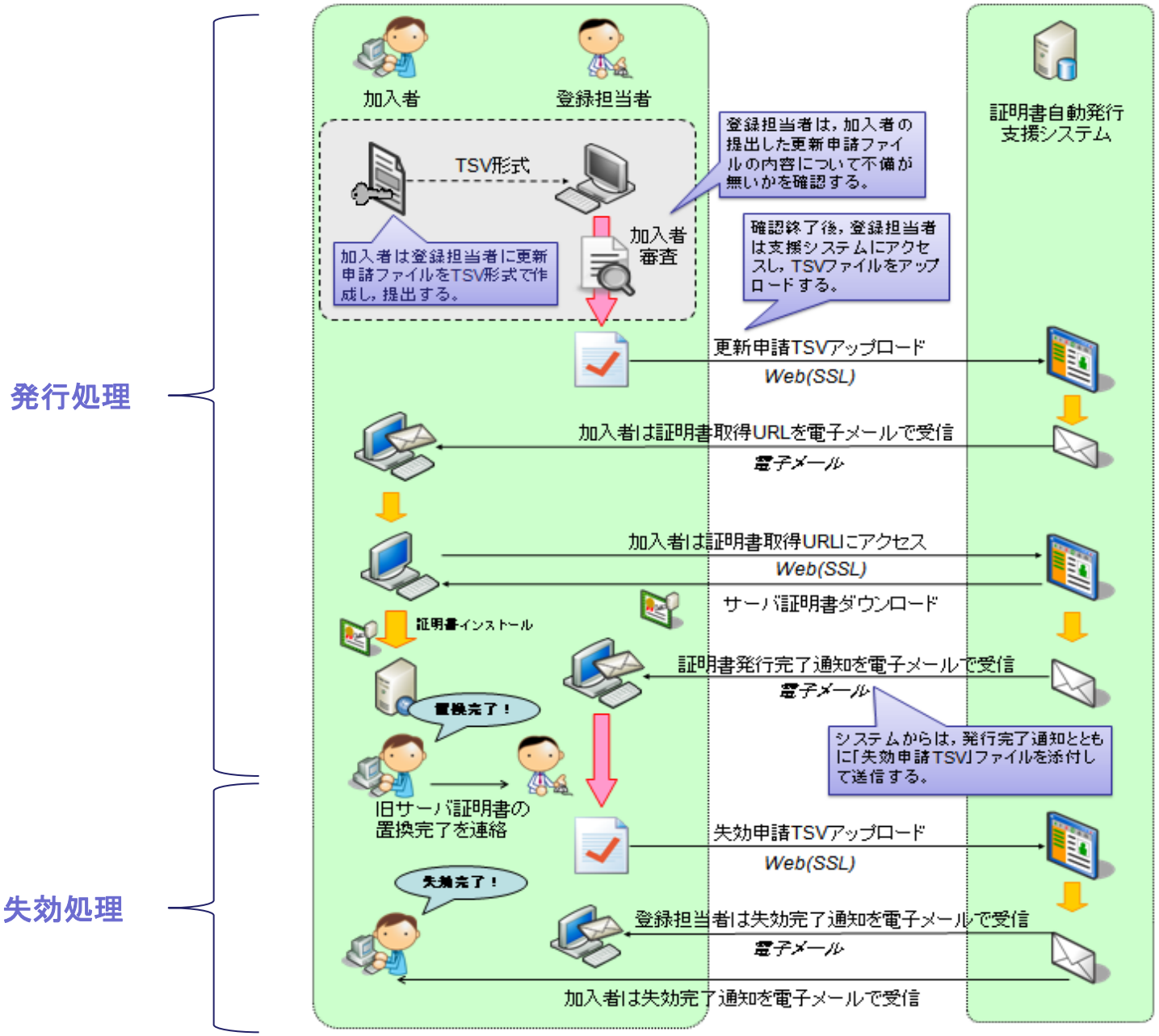
- 加入者mail
  - 加入者メールアドレスが発行申請時と異なる場合は必ず入力してください
  - 記入がない場合、失効完了通知は発行申請時の加入者メールアドレス(および登録担当者)に対して行われます。

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

サーバ証明書更新申請から更新完了までの流れ



サーバ証明書更新申請から更新完了までの流れ

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，別途仕様に基づき「サーバ証明書更新申請ファイル」をTSV形式で作成し，登録担当者に提出します。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，必ず間違いが無いように確認を実施するようにしてください。
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，サーバ証明書の更新を申請する加入者の本人性・実在性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，サーバ証明書更新申請を行います。 TSVファイル形式に問題が無ければ，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ファイルを再提出いただくよう指示してください。
4	証明書取得URL受信	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	発行完了通知の受信	システム ↓ 登録担当者	加入者から更新申請のあった証明書の発行が終了した後，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」を添付した形で電子メールで送信されます。
7	置き換え完了通知	加入者 ↓ 登録担当者	新しい証明書を入手した加入者は、サーバに導入されているサーバ証明書を更新後の新証明書に置き換えた後、登録担当者に置き換え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機関で任意に定めてください。
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6で添付されてきた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，更新前の旧サーバ証明書の失効申請を行います。
9	失効完了の連絡	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終了した旨のメールを受信します.本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.

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。）
- 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。

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

プロジェクト参加時の注意点

- 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
- 参加単位
  - 機関毎に参加申し込みをお願いします

    （同一機関で異なるドメインを用いる場合には，別途事務局までご相談ください。）
- 参加条件
  - 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。
  - 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）
  - 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

サーバ証明書の発行条件

- 対象サーバ
  - 所属する機関が所有または管理するサーバ
  - サーバ認証を必要とするサーバ

  ※下記のようなケースは対象外
    - 特定少数の検証者のみを対象としたサーバ
    - 検証者へのルートCA証明書の配布が容易に実現できる場合

- 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
  - 鍵長は2048bitを推奨、最低1024bit以上。

動作確認済みサーバアプリケーション

次のアプリケーションで動作確認を行っています。

- 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）

推奨するWebブラウザ

次の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





対応する携帯電話

- 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

参考資料

- 申請書類
  - プロジェクト参加申請書、変更申請書、変更届
  - 確認実施手順調査票

- 解説資料・マニュアル
  - 利用の手引き
  - 支援システム操作手順書(登録担当者用)
  - 支援システム操作手順書(加入者用)
  - サーバ証明書インストールマニュアル

- 規程類
  - プロジェクト参加要領
  - プロジェクト参加に関する事務手続き要領
  - 証明書利用に係る申合せ
  - オープンドメイン認証局2証明書ポリシ
  - 運用支援認証局証明書ポリシ
  - セコム電子認証基盤認証運用規程

- TSVファイル作成支援ツール
  https://tsvtool.nii.ac.jp/cgi-bin/tsvtool.cgi
  （利用方法：https://upki-portal.nii.ac.jp/docs/odcert/software/tsvtool）

本プロジェクトに関するお問い合わせ等

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

メールアドレス：cerpj2@nii.ac.jp

プロジェクトホームページ
https://upki-portal.nii.ac.jp/docs/odcert