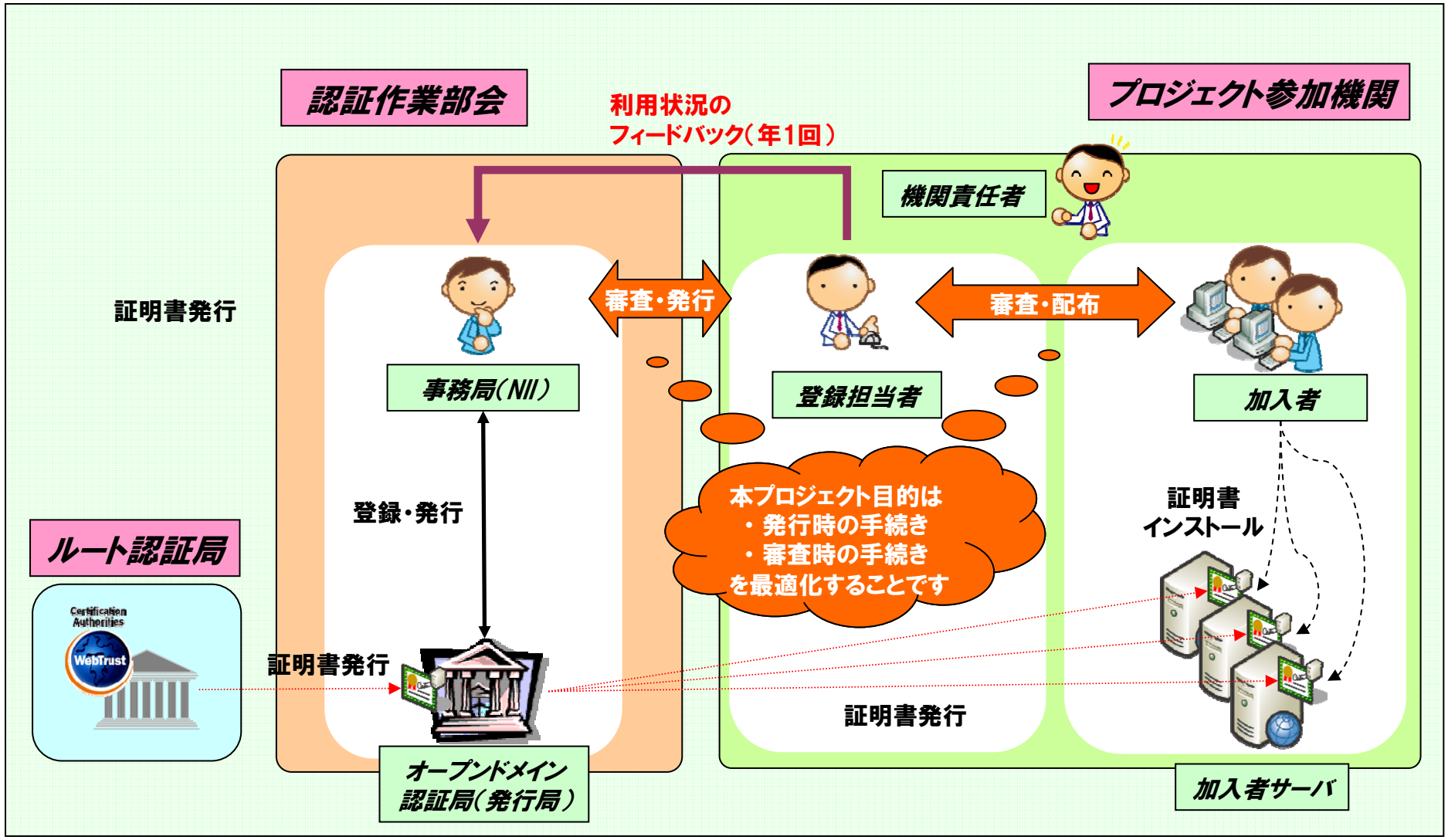
サーバ証明書発行・導入における
啓発・評価プロジェクト
参加方法の説明

国立情報学研究所
学術基盤推進部　基盤企画課
連携システムチーム

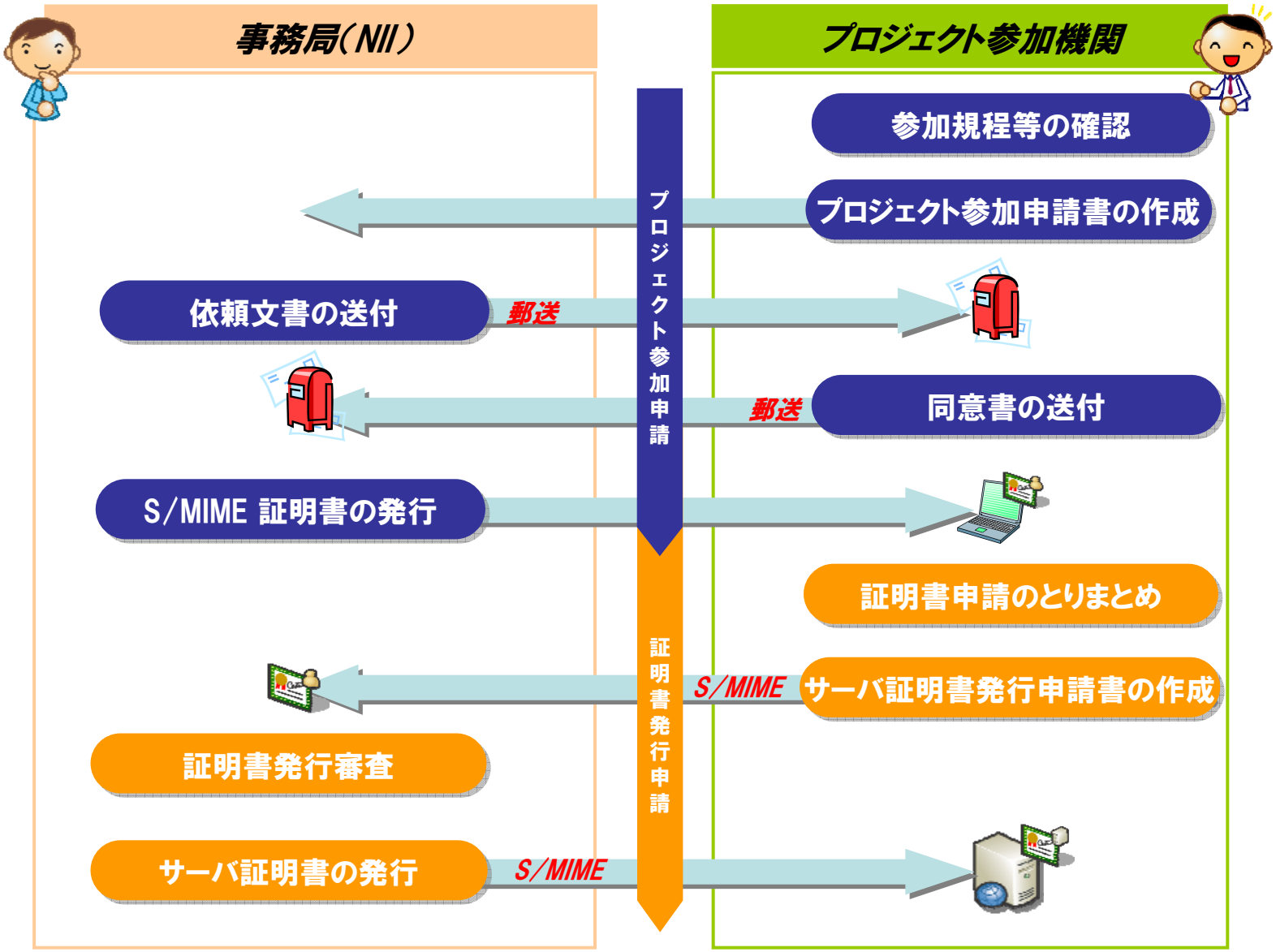
1．サーバ証明書プロジェクト（概念図）



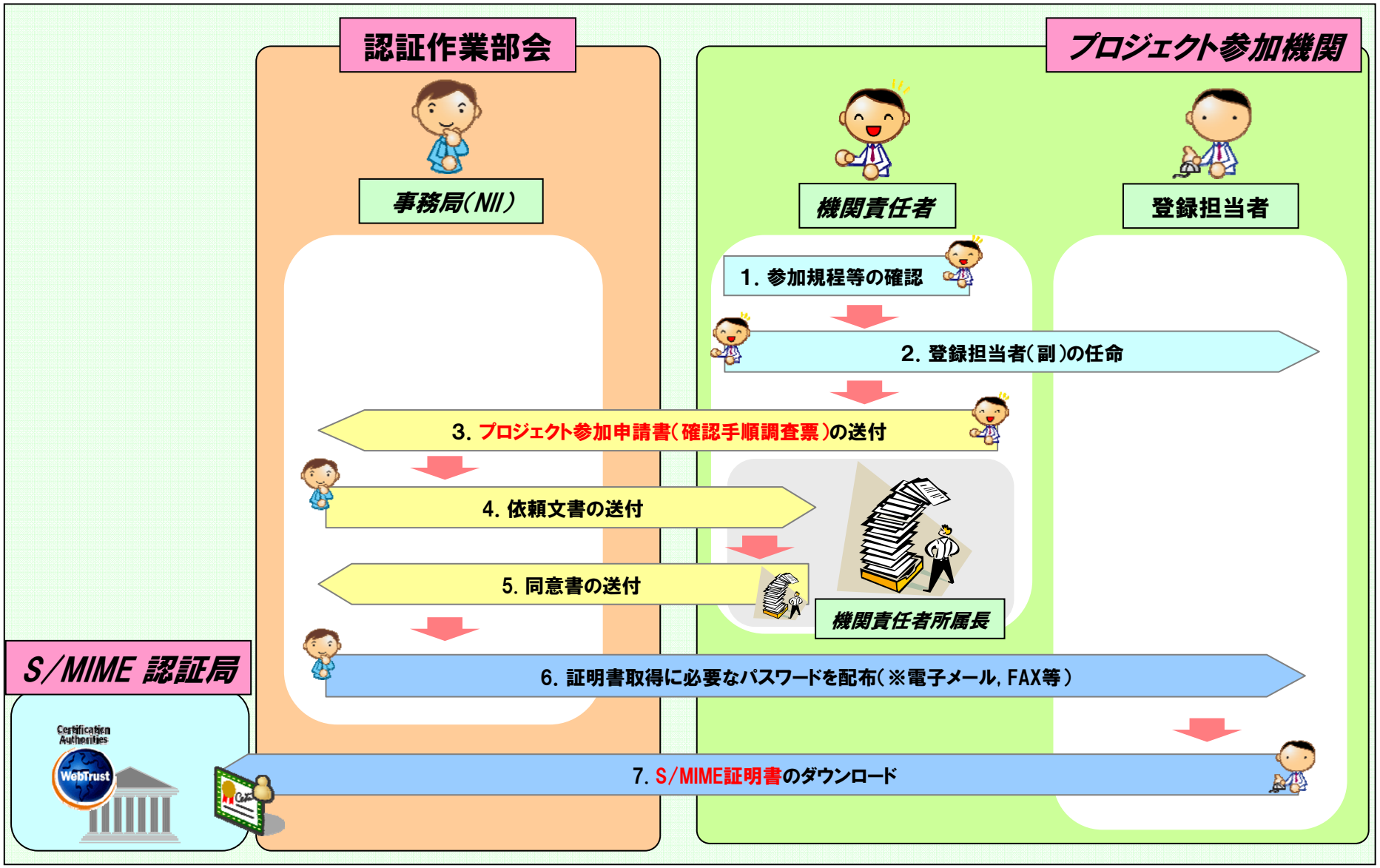
2．プロジェクトで利用する用語と役割

組　織	用語	説　明
NII	オープンドメイン認証局（発行局）	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のPKIアプリケーションに標準でルート認証局が搭載されているため、商用のサーバ証明書と同様に利用することができます。
	事務局	プロジェクト参加申請、証明書発行申請にあたり、審査業務を行なう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。課長職相当または准教授以上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をお願いする方。大学の規模に応じて複数名選出していただくことが可能です。
	加入者	Webサーバを管理し，本プロジェクトのサーバ証明書を利用される方。プロジェクト参加機関内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Webサーバ。
不特定多数	利用者	PKI加入者サーバにアクセスする，不特定多数の方々のことを，この説明では利用者と呼びます。利用者は、ウェブブラウザ等の標準の機能を利用して加入者サーバの証明書を検証いたします。

3. 事務フローの概要


事務局(NII)
プロジェクト参加機関
参加規程等の確認
プロジェクト参加申請書の作成
プロジェクト参加申請
依頼文書の送付
郵送
郵送
同意書の送付
S/MIME 証明書の発行
証明書申請のとりまとめ
証明書発行申請
S/MIME
サーバ証明書発行申請書の作成
証明書発行審査
サーバ証明書の発行
S/MIME

3－1．プロジェクト参加申請フロー
（プロジェクト参加時のみ）



プロジェクト参加申請の説明

（プロジェクト参加時のみ）

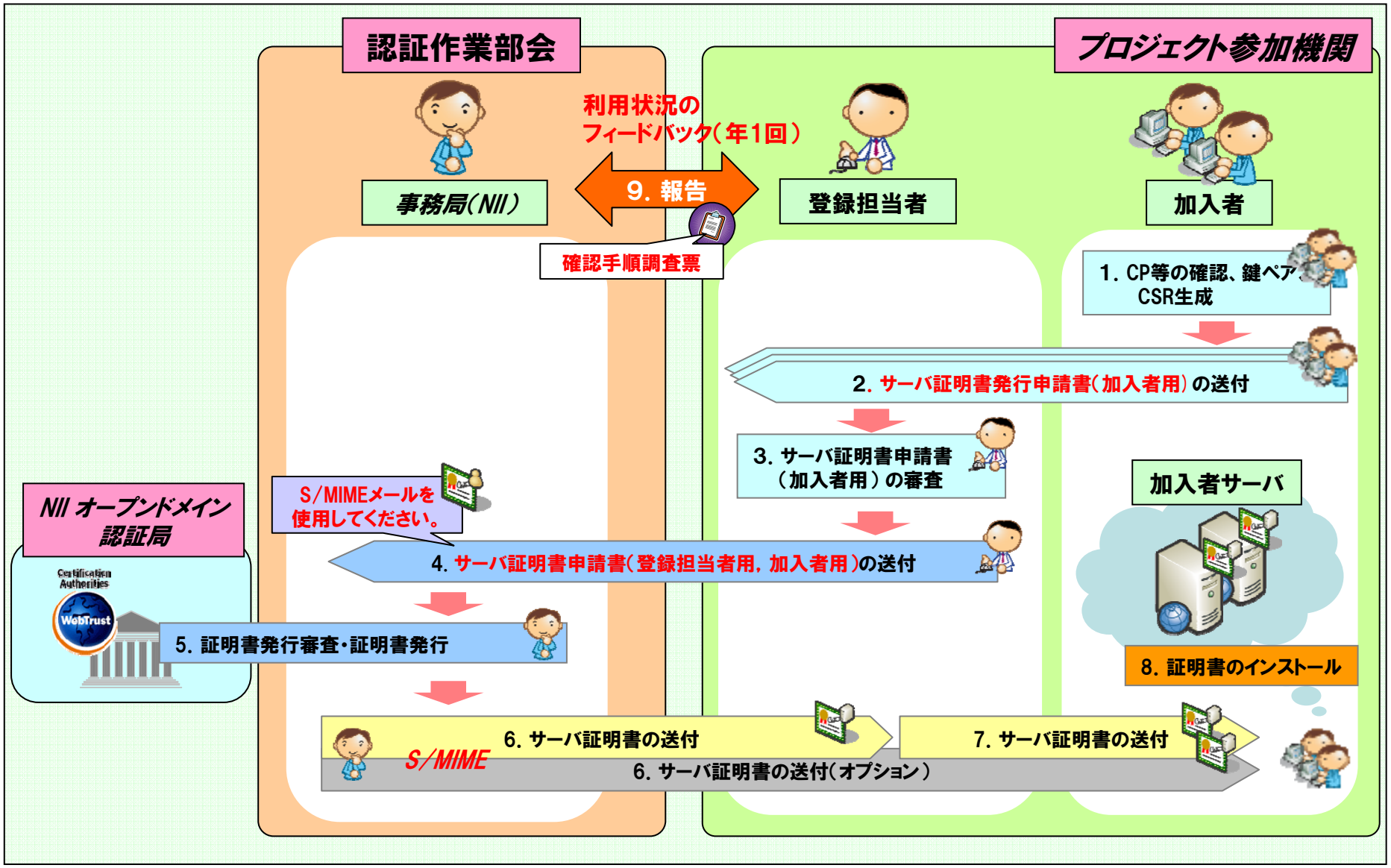
No.	項　目	担　当	説　明
1	参加規程等の確認	機関責任者	次の書類を十分に理解し，承諾してください。 ・本プロジェクト参加要領等 ※1 ・本プロジェクトサーバ証明書利用規定※1 ・本認証局証明書ポリシー (Certificate Policy) ※2 ・本電子認証基盤認証運用規程 (Certification Practice Statement) ※2
2	登録担当者の任命	機関責任者	登録担当者(正、副)の任命を行なってください。
3	プロジェクト参加申請書の送付	機関責任者	プロジェクト参加申請書および確認手順調査票をご記入の上、事務局(NII)宛てに同申請書を郵送してください。なお、プロジェクト申請書には機関責任者の捺印が必要です。 ※記入例は後述
4	委嘱状の送付	事務局(NII)	機関責任者の所属長宛に依頼文書を郵送いたします。
5	同意書の送付	機関責任者(の所属長)	委嘱内容を確認し、事務局(NII)宛てに同意書を郵送してください。
6	証明書に必要なパスワードを配布	事務局(NII)	同意書の確認後、プロジェクト参加申込書に記載されている登録担当者に対し、パスワードを電子メールおよびFAX等で配布いたします。 ※このパスワードは、S/MIME※3証明書の取得時に必要です。
7	S/MIME証明書のダウンロード	登録担当者	事務局(NII)から、送付されたパスワードをもとに、S/MIME証明書を取得してください。また、ご利用のメーラにS/MIME証明書を設定してください。

※1 https://upki-portal.nii.ac.jp

※2 https://repo1.secomtrust.net/sppca/NII/ODCA/index.html

※3 電子メールの暗号化、署名方式の一つ。
本プロジェクトでは、証明書発行申請を行なう際に、電子メールに署名してください。

3－2．サーバ証明書発行申請フロー
（証明書の申請都度）



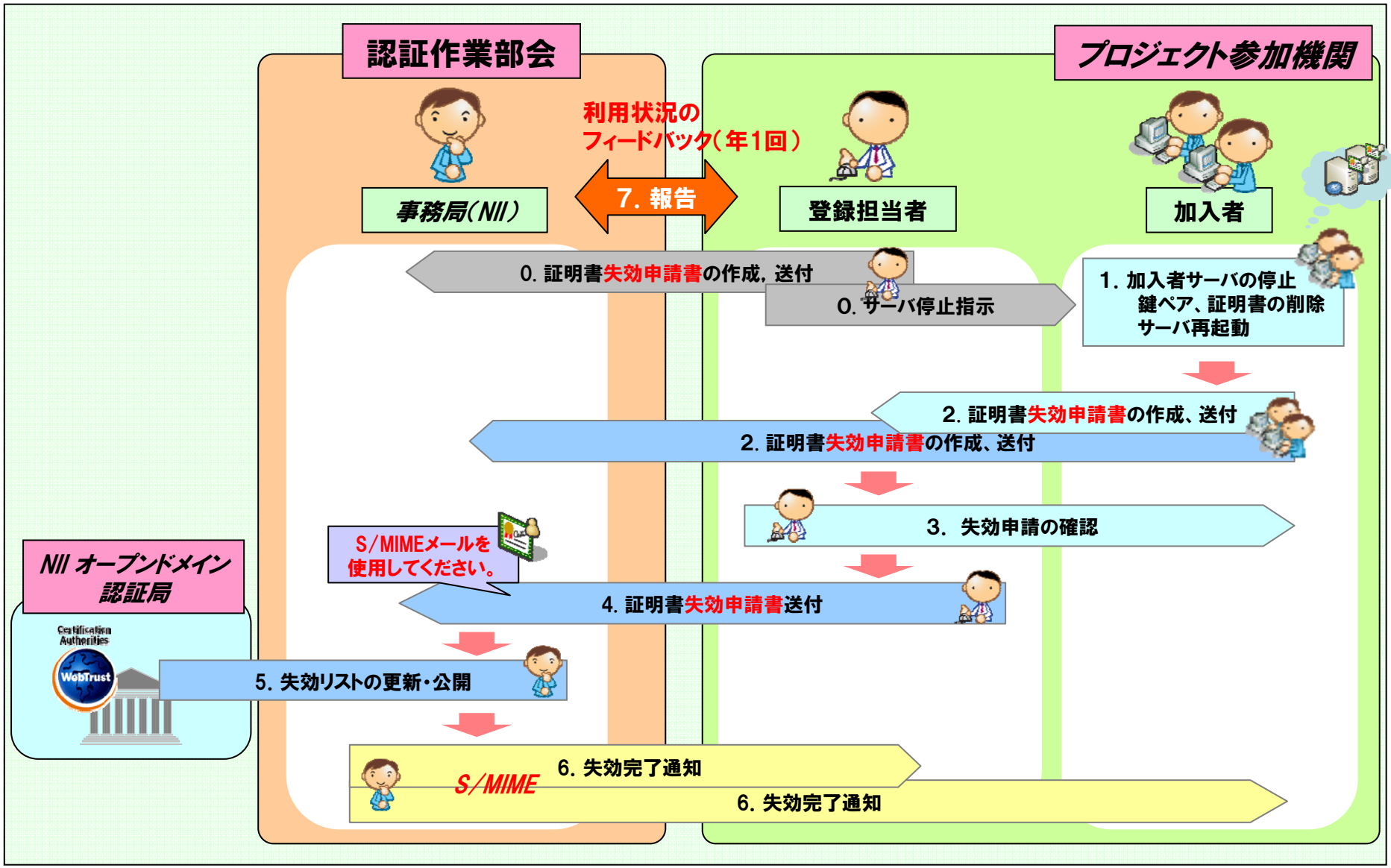
サーバ証明書発行申請の説明

（証明書の申請都度）

No.	項　目	担　当	説　明
1	CP等の確認、 鍵ペア、CSRの生成	加入者	サーバ証明書の発行に必要な情報を生成してください。 ・鍵ペア（秘密鍵は厳重に管理してください。） ・CSR（Certificate Sign Request）
2	サーバ証明書発行申請書 （加入者用）の送付	加入者	サーバ証明書発行申請書（加入者用）をご記入の上、登録担当者に同申請書をご送付ください。※記入例は後述
3	サーバ証明書申請書 （加入者用）の審査	登録担当者	サーバ証明書発行申請書（加入者用）の記載内容をプロジェクト参加申請時に記載した審査内容に基づき審査し、サーバ証明書発行申請書（登録担当者用）をご作成ください。※記入例は後述
4	サーバ証明書申請書 （加入者用、登録担当者用）の送付	登録担当者	サーバ証明書発行申請書（加入者用，登録担当者用）を取りまとめて事務局（NII）にご送付ください。 ※S/MIMEメール（署名）を使用してください。
5	証明書発行審査・証明書発行	事務局（NII）	サーバ証明書発行申請書を審査します。 ※申請内容に問題がある場合は、登録担当者にご連絡いたします。
6	サーバ証明書の送付	事務局（NII）	証明書を登録担当者にお送りいたします。オプションを選択することで、同時に加入者に対し、証明書を配布することも可能です。 ※S/MIMEメール（署名）を使用しています
7	サーバ証明書の送付	登録担当者	6のオプションを選択しない場合、登録担当者から加入者に証明書を配布いたします。
8	証明書のインストール	加入者 サーバ	証明書のインストールを行います。
9	報告（年1回）	登録担当者	証明書の利用状況について、事務局（NII）に報告します。 確認手順調査票を記入し提出します※記入例は後述

4．失効フロー図（証明書失効申請）

（秘密鍵の漏洩，証明書記載情報の変更，運用停止等）



証明書失効申請の説明

（秘密鍵の漏洩，証明書記載情報の変更，運用停止等）

No.	項　目	担当	説　明
0※	証明書失効申請所の作成，送付	登録担当者	サーバ証明書失効申請書をご記入の上、登録担当者およびNII事務局に同申請書をご送付ください。※記入例は後述
	サーバ停止支持	登録担当者	加入者に対し、サーバ証明書の失効を通知し、サーバ証明書に関する削除するように指示してください。
1	加入者サーバの停止、 鍵ペア、証明書の削除、 サーバ再起動	加入者 サーバ	鍵ペアやサーバ証明書等、サーバ証明書に関する情報を削除し、サーバを再起動してください。
2	証明書失効申請書の作成、送付	加入者	サーバ証明書失効申請書をご記入の上、登録担当者およびNII事務局に同申請書をご送付ください。※記入例は後述
3	失効申請の確認	登録担当者	サーバ証明書失効申請書を受領後、加入者に速やかに失効申請に関して規定の確認を行い同申請書にその内容を記載する。事務局（NII）に同申請書を送付する。
4	サーバ証明書の失効申請書送付	登録担当者	サーバ証明書失効申請書を事務局（NII）にご送付ください。 ※S/MIMEメール（署名）を使用してください。
5	失効リストの更新・公開	事務局（NII）	失効申請書に従い証明書を失効します。
6	失効完了通知	事務局（NII）	失効完了したことを登録担当者と加入者に送付いたします。 ※S/MIMEメール（署名）を使用しています

※ 網掛けは、登録担当者が強制的に加入者サーバの証明書の利用を失効させる際に行なう処理です。
この場合、No.2 ～ No.4の手順は必要ありません。

５．CSR作成上の注意

- CSR(証明書発行要求:Certificate signing Request)は証明書を作成するためのもととなる情報で、機関名やウェブサーバのFQDN等が含まれます。詳細は別途公開する証明書インストールマニュアルをご参照ください。

項　目	設　定　内　容
Country Name（C）	「JP」と入力
State or Province Name （ST）	本プロジェクトでは使用しないでください
Locality Name （L）	「Academe」と入力
Organization Name（O）	大学機関名をご記入
Organizational Unit Name（OU）	証明書を使用する部門名又はグループ名を記入(省略可)
Common Name（CN）	サーバ名を記入 ※ウェブサーバのURLがhttps://www.example.ac.jpの場合 [www.example.ac.jp]

6-1．プロジェクト参加申請書の記入例（1/4）

サーバ証明書発行･導入の啓発･評価プロジェクト参加申請書

平成１９年　５月　１５日

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　情報大学

機関責任者　情報　太郎　　印

本プロジェクトの利用規程を理解し，次のとおりプロジェクトの参加を申し込みます。

申請区分	■新規　□変更　□中止			
所属機関	機関名	情報大学		
	機関名(英語表記)	University of Informatics		
	所在地	〒123-4567 東京都千代田区一ツ橋１－２－３		
機関責任者	氏　名	情報　太郎	所属	情報基盤センター基盤企画課
	職　名	基盤企画課長	電話番号	03-1111-2222
	FAX	03-1111-2222	E-Mail	taro@example.ac.jp
	所属住所	〒　所属期間と同じ	（所属機関と同じ場合は省略可）	
対象ドメイン	example.ac.jp			
登録担当者	氏　名 ローマ字	研究 花子 Kenkyu Hanako	所属	情報基盤センター基盤企画課 ネットワーク係
	職　名	係員	電話番号	03-1111-2222
	FAX	03-1111-2222	E-Mail	hanako@example.ac.jp
	所属住所	〒　所属期間と同じ	（所属機関と同じ場合は省略可）	

証明書送付	■登録担当者のみ宛　□登録担当者・加入者の同時送付　（どちらかを選択）

申請書最終確認者

機関責任者

申請書作成者

登録担当者

6-1．プロジェクト参加申請書の記入例（2/4）

機関責任者確認事項

以下の項目を確認の上チェックしてください。(登録担当者は(副)も含めて全員確認してください)

☑ドメインが組織の所有であることを確認しました

☑登録担当者の本人性を確認しました

☑登録担当者の実在性を確認しました

プロジェクト参加申請時に必ずご確認ください。

変更・中止申請の場合の理由

☐機関責任者を変更します。　(変更前:　変更後:　)

☐登録担当者を変更します。　(変更前:　変更後:　)

☐登録担当者(副)を変更します。　(変更前:　変更後:　)

☐登録担当者(副)を追加します。　(　)

☐登録担当者(副)を除名します。　(　)

☐対象ドメインを変更します。　(変更前:　変更後:　)

☐プロジェクト参加の中止（以下に理由を記入してください）

申請内容に変更・プロジェクト参加を中止する場合は、こちらを記入の上、ご連絡ください。

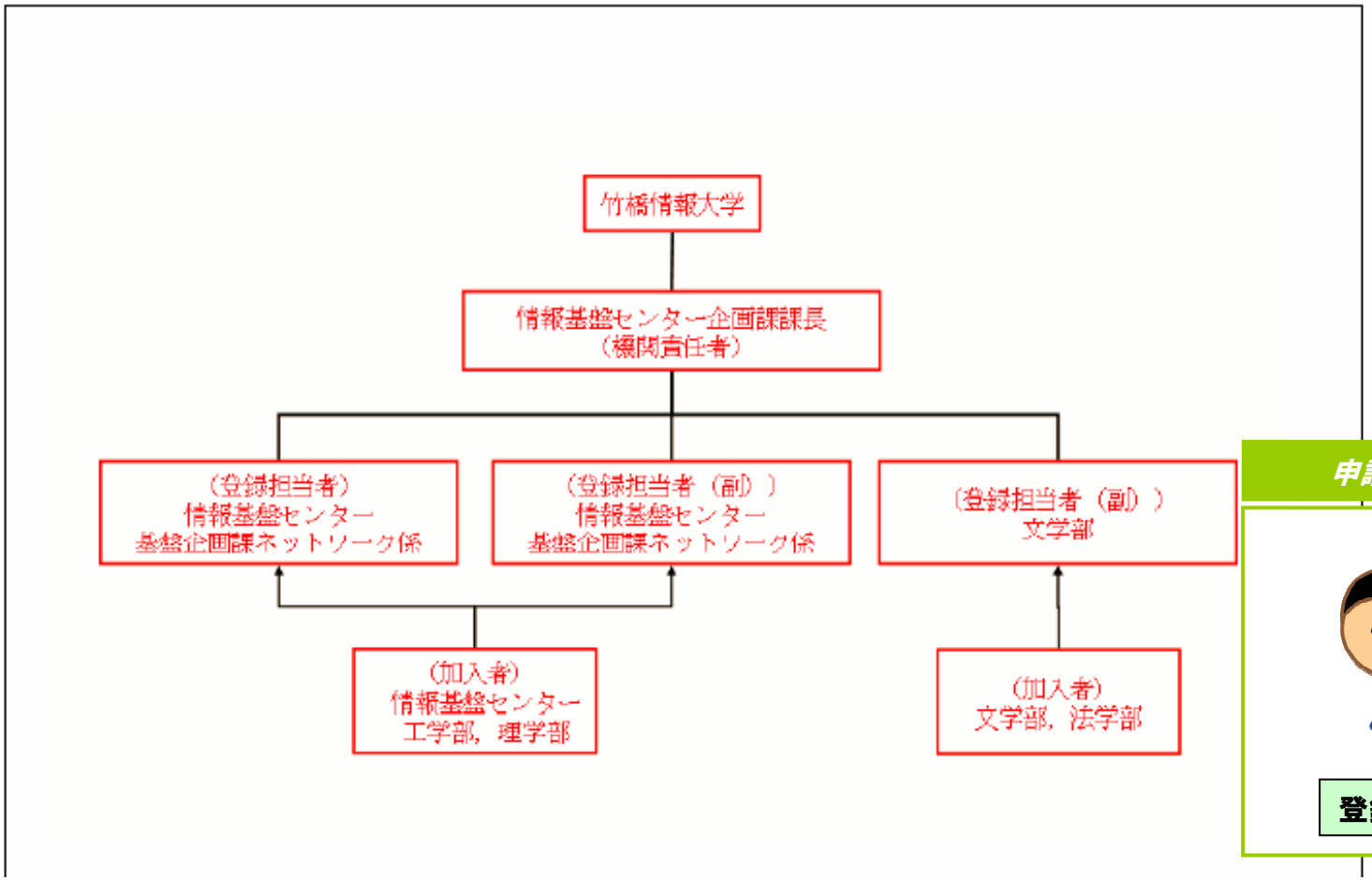
☐その他（以下に理由を記入してください）

申請書作成者

登録担当者

6-1．プロジェクト参加申請書の記入例（3/4）

サーバ証明書の配付について，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。



6-2. プロジェクト参加申請書の記入例（４/４）

（確認実施手順調査票）

- **確認手順調査票には回答例あります。こちらを参考にしてください。**
  回答例が貴機関に運用にそぐわない場合は、実運用に即した方法を記入してください。

1-1 ドメインが組織の保有であることの確認
申請するドメインが組織の所有であることを、「どのような情報」をもとに、「どのような方法で」確認を行い、「どのように承諾を得た」かを教えてください。

○	「Whoisデータベースでxxx.ac.jpのドメイン名管理者」を確認し、「管理者へ直接口頭で問い合わせて」許諾を得ました。
○	本学の広報委員会が「公式のWebページ」で「xxx.ac.jpのドメイン」であることを確認」し、「LAN管理委員会で当該ドメインに対して証明書を発行することの承諾を得ました。
×	xxx.ac.jpのxxxが、組織名と一致していることを確認した。 *名称の確認だけでは、期間のドメインであることを確認したことにはなりません。*

回答例

'回答例'シートの「適切な判断規準」を参考に、貴大学において実施される確認手順についてご回答ください。
確認時には様々な状況が考えられますので、様々なパターンの確認手順を記述いただいて構いません。

1　参加申請書について
機関責任者が参加申請書を記述するにあたって、以下の項目をどのように確認したのかを教えてください。

1-1 ドメインが組織の所有であることの確認
申請するドメインが組織の所有であることを、「どのような情報」をもとに、「どのような方法で」確認を行い、「どのように承諾を得た」かを教えてください。

「Whoisデータベースでxxx.ac.jpのドメイン名管理者」を確認し、「管理者へ直接口頭で問い合わせて」許諾を得ました。

申請書作成者

登録担当者

６-３．サーバ証明書発行申請書（加入者用）

申請書作成者

加入者

○ サーバ証明書発行申請書(加入者記入用)

申請情報	加入者情報	所属	情報基盤センター基盤企画課　ネットワーク係
		氏名	企画 二郎
		E-Mail	jiro@example.ac.jp
	サーバ情報	FQDN	center.example.ac.jp
		サーバソフト名 及び バージョン	apache1.3.37 + mod_SSL2.8.28
	CSR	-----BEGIN CERTIFICATE REQUEST----- MIIBozCCAQwCAQAwYzELMAkGA1UEBhMCSlAxEDAOBgNVBAcTB0FjYWRlbWUxIDAe BgNVBAoTF1RoZSBVbml2ZXJzaXR5IG9mIFRva3lvMSAwHgYDVQQDExd1dC1wb3J0 yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy BAUAA4GBAFnqxwJ0mFLdHe+VE6eUsCL4H3wet05dBMFckAwevBFo+5YZcZS8Afza zEpDShYLKB0jroE44dDCC8X3WdhcM4ETAxWQTHUN49rFGjMMutB/uECJmi+kDvpS vz8yBwC9ybSBX+jFcy6dtkBwZoKtZfSOepEruzzhk+hwdmsru9w -----END CERTIFICATE REQUEST-----

※ コピー(カット)アンドペーストを利用してCSRの貼り付ける場合は、

必ず確認してください

確認欄	確認実施日	2007年5月15日	
	確認項目	▼ 申請するにあたり、次の内容を確認してください。	チェック欄
		作成した鍵ペアのうち秘密鍵が外部へ漏れないよう管理しています。	☑

6-4. サーバ証明書発行申請書(登録担当者用)

申請書作成者

登録担当者

○ サーバ証明書発行申請書(登録担当者記入用)

登録情報	所属機関	機関名	竹橋情報大学
	機関責任者	氏名	情報　太郎
	登録担当者(又は、補佐)	氏名	研究　花子
		E-Mail	hanako@example.ac.jp
		申請ドメイン	example.ac.jp

▼ 加入者が提出した申請情報について、次の内容を確認してください。

確認欄	確認実施日	日付	2007年5月15日
	申請したCSRについて	申請数	2　枚
		申請したFQDNを全て記載してください	center.example.ac.jp, kokusai.examp
	確認項目	▼ 申請情報について次の内容を確認してください	チェック欄
		1. 加入者の本人性	発行申請書(加入者記入用)は、間違いなく加入者本人が申請したことを確認しました。 ☑
		2. 加入者の実在性	加入者が所属機関に所属している人物であることを確認しました。 ☑
		3. ドメインの実在性	加入者サーバのFQDNが、プロジェクトで申請したドメイン名を利用しており、存在するFQDNであること確認しました。 ☑
		4. 加入者サーバの実在性	加入者から申請されたサーバは、所属機関が管理していることを確認しました。 ☑

プロジェクト参加申請書(確認実施手順調査票)の記載事項に従い審査してください

6-4. サーバ証明書失効申請書

○ サーバ証明書失効申請書(加入者記入欄)

申請情報	加入者情報	所属	情報基盤センター基盤企画課 ネットワーク係
		氏名	企画 二郎
		E-Mail	jiro@example.ac.jp
	サーバ情報	FQDN	center.example.ac.jp
		シリアル番号	46 x2 x1 15
	失効理由	▼ 失効理由を選択してください。	チェック欄
		鍵危殆化	☐
		内容変更	☑
		取り替え	☐
		運用停止	☐
		その他	☐

確認欄	確認実施日	2007年5月16日	
	加入者用	▼ 申請するにあたり、次の内容を確認してください。	チェック欄
		加入者サーバを停止し、鍵ペアを削除しました。	☑

↑↑↑↑↑ ここまでの内容を記入し、登録担当者とNII事務局(cerp@nii.ac.jp)までご連絡ください。 ↑↑↑↑↑

登録担当者が強制的に証明を失効する場合は、登録担当者が記入してください

申請書作成者

加入者

○ サーバ証明書失効申請書(登録担当者記入欄)

登録情報	所属機関	機関名	竹橋情報大学
	機関責任者	氏名	情報 太郎
	登録担当者(又は、補佐)	氏名	研究 花子
		E-Mail	hanako@example.ac.jp
		申請ドメイン	example.ac.jp

確認欄	確認実施日	2007年5月16日	
	登録担当者用	▼ 申請するにあたり、次の内容を確認してください。	チェック欄
		失効申請書は、間違いなく加入者本人が申請したことを確認しました。	☑

↑↑↑↑↑本内容を確認し、NII事務局(cerp@nii.ac.jp)までご連絡ください。 ↑↑↑↑↑

申請書作成者

登録担当者

【各種申請やお問い合わせ先】

〒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 基盤企画課 連携システムチーム
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事務局
TEL:03-4212-2218／FAX:03-4212-2230
E-mail:cerpj@nii.ac.jp