「サーバ証明書発行・導入の啓発・評価研究プロジェクト」

subjectAltName 対応証明書申請手続きについて

1.01

2008 年 8 月 26 日

国立情報学研究所

改訂履歴		
版数	日付	内容
V1.00	2008/6/24	初版（配布開始）
V1.01	2008/8/26	誤字修正

-- 目次 --

1. 概要

「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（以下「本プロジェクト」という。）では，平成 20 年 7 月 7 日以降発行する証明書へ複数の subjectAltName を追加できるように変更を行ないました。

subjectAltName 項目にバーチャルホスト名（FQDN）を申請することにより，サーバ証明書 1 枚で，同一環境(OS)上の異なるホスト名(FQDN)を持つ複数のサーバを動作させることができます。subjectAltName を持つサーバ証明書の申請は通常の申請と同様の方法で申請することができます。

【新規サーバ証明書発行フロー】

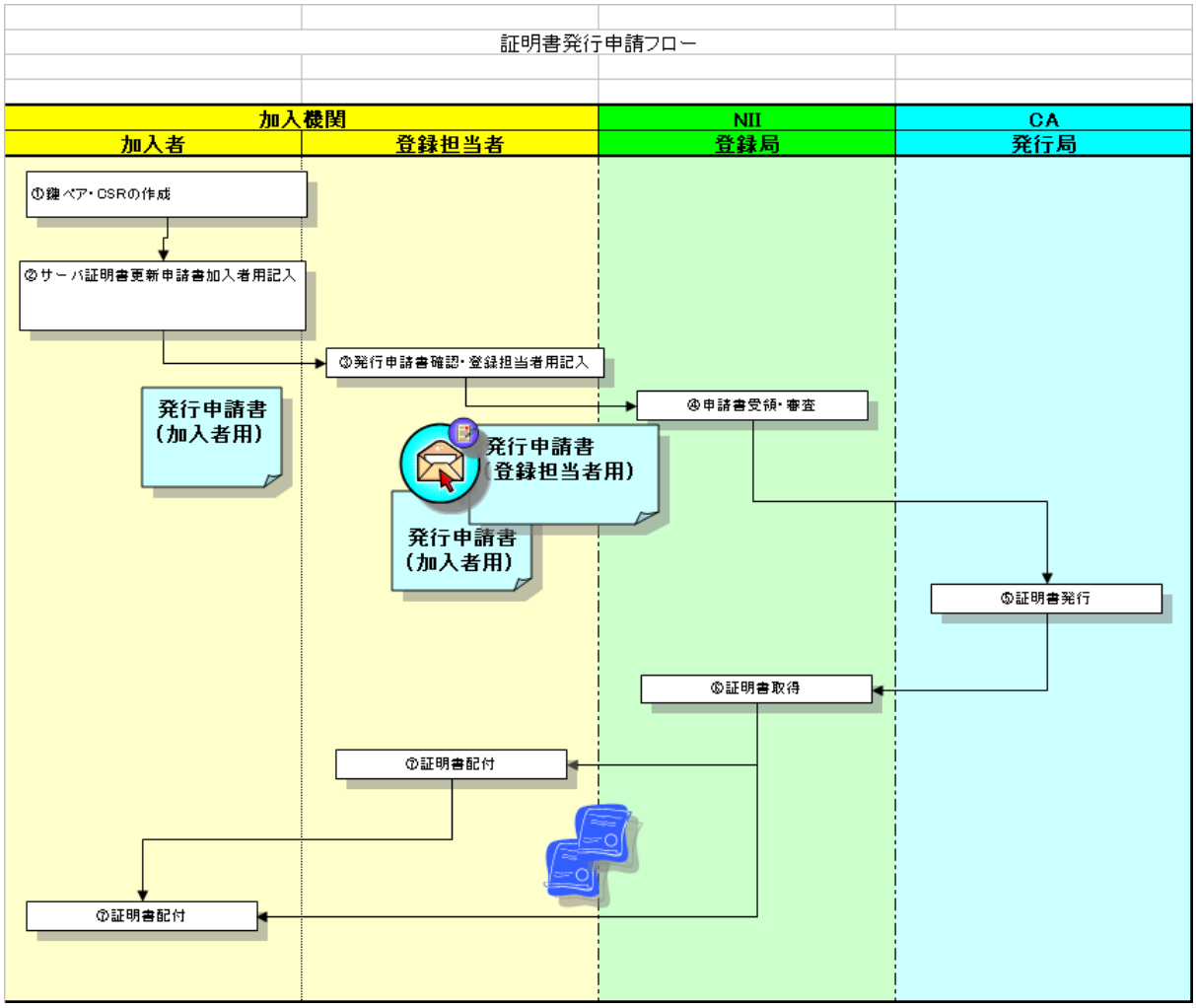

図 1 サーバ証明書申請フロー

サーバ証明書発行申請書：
https://upki-portal.nii.ac.jp/cerpj/cert_request_form/requestform20070525.xls

【更新用サーバ証明書発行フロー】

証明書更新時, subjectAltName を利用することにより, 複数の証明書を 1 枚にまとめる場合は, CN に記述する証明書を更新し, subjectAltName に記述することにより, 不要となる証明書は失効をお願いいたします。証明書の失効方法につきましては,「別紙 3 証明書更新申請書加入者用」をご確認ください。

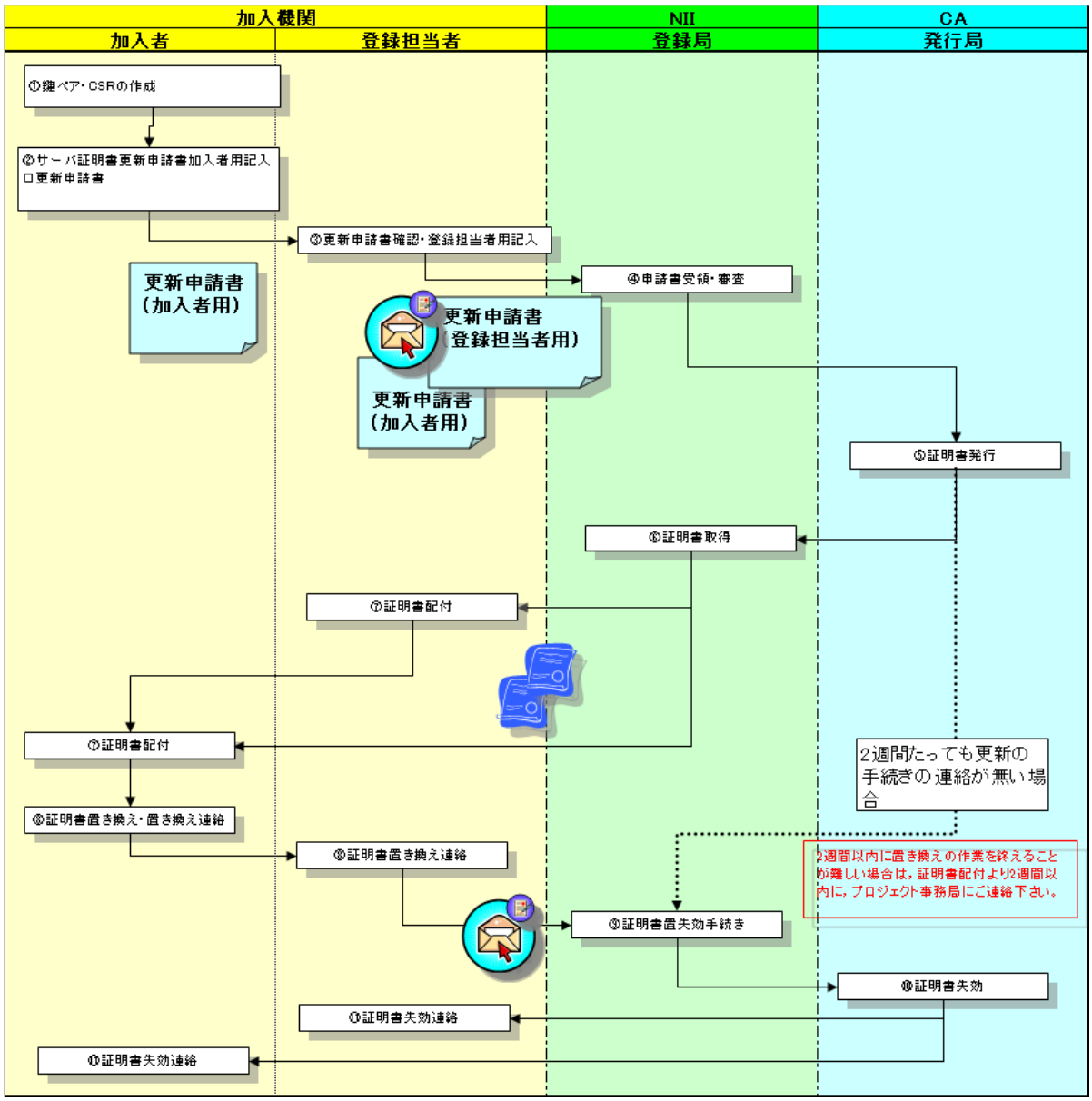

図 2 サーバ証明書更新フロー

サーバ証明書更新申請書：

https://upki-portal.nii.ac.jp/cerpj/renwal_requirment/renewal_request_sheets_all.xls

2. subjectAltName の利用について

1. 同一環境(OS)上で異なるホスト名(FQDN)のサーバ証明書を必要とする場合(Apache の virtualHost 機能など)にご利用ください。

2. 同一計算機上でも VMware や Xen などで，複数の仮想環境(ゲスト OS)が動作している場合には，subjectAltName を使用することはできません。仮想環境(ゲスト OS)ごとの証明書発行申請をお願いします。

3. サーバソフトウェアでバーチャルホスト機能を設定する際は，名前ベースのバーチャルホスト機能をご利用ください。IP ベースのバーチャルホストには対応しておりませんのでご注意ください。名前ベースのバーチャルホスト機能の具体的な設定方法についてはご利用のサーバソフトウェアのマニュアル等をご覧ください。

4. subjectAltName に記載可能なホスト名(FQDN)は，プロジェクト参加申請書に記載いただいたドメイン名に限ります。他のドメインを含めた申請は受理できかねますのでご了承ください。

3. 1 枚の証明書で利用可能な subjectAltName 項目の上限

1 枚の証明書に併記可能な subjectAltName 項目の合計文字数には仕様上の制約があり，ホスト名(FQDN)の合計文字数によっては申請いただいた全てのホスト名を 1 枚の証明書に併記できない場合がございます。

併記するホスト名が 4 件以上(subjectDN に記載するホスト名も含めると 5 件以上)となる場合には，事前に下記問い合わせ先（事務局宛）にご相談ください。

また，併記するホスト名が 3 件以下(subjectDN に記載するホスト名も含めると 4 件以下)であってもドメイン名の文字数によっては 1 枚の証明書に併記できない場合がありますのでご了承ください(別途事務局より調整させていただきます)。

4. CSR の作成について

発行申請書に添付する CSR は、subjectAltName に記載するホスト名を含めず、subjectDN に記載するホスト名のみを含めた従来通りの CSR を生成・添付ください。subjectAltName に記載するホスト名を CSR に記載しても受理可能ですが、証明書には発行申請書にご記入いただいたホスト名が記載されますので、subjectAltName に記載したいホスト名は必ず漏れなく発行申請書の subjectAltName 欄にご記入いただけますようお願いいたします(CSR に記載された subjectAltName は無視されます)。CSR の作成方法の詳細につきましては，サーバ証明書インストールマニュアルをご参照ください。

サーバ証明書インストールマニュアル
https://upki-portal.nii.ac.jp/cerpj/niiodcamanual-v1-0.pdf

5. 注意事項

発行した証明書の subjectAltName 項目に後からホスト名を追記する場合は，証明書の再発行が必要となりますのでご了承ください。

同様に，発行した証明書の subjectAltName 項目に後からホスト名を削除する場合は，証明書の再発行が必要となりますのでご了承下さい。

6. その他

NII オープンドメイン認証局では、発行申請時に加入者サーバの実在性およびドメインの実在性を確認する必要があるため、ワイルドカードを含んだ証明書の発行は行いません。

7. お問い合わせ先

プロジェクト事務局（連絡先）

各種申請やお問い合わせこちらにご連絡ください。

〒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 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

別紙 1 サーバ証明書発行申請書（加入者用）

○ 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			
		氏名			
		E-Mail			
	サーバ情報	FQDN			
		サーバソフト名 及び バージョン			
	C S R	-----BEGIN CERTIFICATE REQUEST-----			
		1 ページ			
		-----END CERTIFICATE REQUEST-----			
	SubjectAlt Name	SubjectAltName 追加申請数		個	
		dNSName=			
		dNSName=			
		dNSName=			
		※ 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、セルをダブルクリックしてから行なってください。			
		※証明書のCNは必ずSubjectAltNameに追加されるため，上記の項目への入力は不要となります。			
		※subjectAltNameが4件以上になる場合には、証明書に記載したいホスト名(FQDN)を全て列記した上で			
		事前に事務局宛にご相談ください。			
確認欄	確認実施日				
	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。			□
		「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 サーバ証明書利用に係る申合せ」「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要領」「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の参加に関する事務手続き要領」の内容を理解し，同意しました。			□

図 2 サーバ証明書発行申請書（加入者用）

所属：加入者の所属部署を部名から記入してください

氏名：加入者の氏名を記入してください

E-Mail：加入者の(ac.jp ドメインでの)連絡先 E-Mail を記入してください。

FQDN：サーバの FQDN（証明書の CN に記述する項目）を記入してください。

サーバソフト名:証明書を更新するサーバのサーバソフト名及び Version を記入してください。

CSR：「4. CSR の作成について」で作成した CSR を貼り付けてください。

subjectAltName：申請数と，必要となる Host 名を記入してください。

※証明書に記述した FQDN は CN に登録されるため，記述の必要はありません。

※申請する Host 名の数が 4 つ以上となる場合は，登録担当者経由で cerpj@nii.ac.jp までお問い合わせ下さい。

確認項目：記述されている内容に確認・同意し，チェック欄にチェックをつけてください。

別紙 2 サーバ証明書発行申請書（登録担当者用）

○ 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	
	機関責任者	氏名	
	登録担当者（又は、補佐）	氏名	
		E-Mail	
		申請ドメイン	

▼ 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		
	申請したCSRについて	申請数		枚
		申請したFQDNを全て記載してください		
	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。	☐

図 3 サーバ証明書発行申請書（登録担当者用）

所属機関：機関責任者の所属機関名を記入してください。

機関責任者氏名：機関責任者の氏名を記入してください

登録担当者氏名：登録担当者の氏名を記入してください。

登録担当者 E-mail：プロジェクト登録時の連絡先 E-Mail を記入してください。

申請ドメイン：プロジェクト登録時に申請したドメインを記入してください。

確認実施日：申請書記入日時を記入してください。

申請数：証明書発行申請数を記入してください。

申請した FQDN：サーバの FQDN（証明書の CN に記述する項目）を記入してください。

CSR：「4. CSR の作成について」で作成した CSR を貼り付けてください。

確認項目：記述されている内容に確認・同意し，チェック欄にチェックをつけてください。

別紙３ 証明書更新申請書（加入者用）

○ 更新用サーバ証明書申請書(加入者記入用)						
申請情報	加入者情報	所属				
		氏名				
		E-Mail				
	サーバ情報	FQDN				
		サーバソフト名 及び バージョン				
	ＣＳＲ	-----BEGIN CERTIFICATE REQUEST-----				
		-----END CERTIFICATE REQUEST-----				
	SubjectAlt Name	SubjectAltName 追加申請数				個
		dNSName=				
		dNSName=				
		dNSName=				
		※ 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セルをダブルクリックしてから行なってください。				
		※証明書のCNは必ずSubjectAltNameに追加される為、上記の項目への入力は不要となります。				
		※subjectAltNameが4件以上にわたる場合には、証明書に記載したいホスト名(FQDN)を全て列記した上で				
		事前に事務局宛にご相談ください。				
		↓subjectAltName項目を利用することにより，不要となる証明書を記述してください。				
失効情報	シリアル番号					
	失効理由	鍵危殆化　内容変更　取り替え　その他　※該当する失効理由以外を削除してください。				
	シリアル番号					
	失効理由	鍵危殆化　内容変更　取り替え　その他　※該当する失効理由以外を削除してください。				
	シリアル番号					
	失効理由	鍵危殆化　内容変更　取り替え　その他　※該当する失効理由以外を削除してください。				
確認欄	確認実施日					
	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。				□
		新規鍵ペアで本CSRを作成しました。(以前の鍵ペアは使用していません)				□
		更新用サーバ証明書を受領してから，2週間以内にプロジェクト事務局に証明書置き換えが終了した旨の連絡を行わなかった場合には，登録局によって本申請書で申請した証明書の失効を行うことに同意します。				□
		「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 サーバ証明書利用に係る申合せ」「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 参加要領」「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の参加に関する事務手続き要領」の内容を理解し，同意しました				□

図 4

図 5 サーバ証明書更新申請書（加入者用）

所属：加入者の所属部署を部名から記入してください

氏名：加入者の氏名を記入してください

E-Mail：加入者の(ac.jp ドメインでの)連絡先 E-Mail を記入してください。
FQDN：サーバの FQDN（証明書の CN に記述する項目）を記入してください。
サーバソフト名:証明書を更新するサーバのサーバソフト名及び Version を記入してください。
CSR：「4. CSR の作成について」で作成した CSR を貼り付けてください。
subjectAltName：申請数と，必要となる Host 名を記入してください。
※証明書に記述した FQDN は CN に登録されるため，記述の必要はありません。
※申請する Host 名の数が 4 つ以上となる場合は, 登録担当者経由で cerpj@nii.ac.jp までお問い合わせ下さい。

シリアル番号：失効する証明書のシリアル番号を記入してください。
失効理由：証明書の失効理由を選択してください。
確認実施日：申請書記入日を記入してください。
確認項目：記述されている内容に確認・同意し，チェック欄にチェックをつけてください。

別紙 4 サーバ証明書更新申請書（登録担当者用）

○ 更新用サーバ証明書申請書(登録担当者記入用)				
登録情報	所属機関	機関名		
	機関責任者	氏名		
	登録担当者（又は、補佐）	氏名		
		E-Mail		
		申請ドメイン		
▼ 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		
	申請したCSRについて	申請数		枚
		申請したFQDNを全て記載してください		
	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。	☐
		5. 証明書の失効について	更新用サーバ証明書を受領してから，2週間以内にプロジェクト事務局に証明書置き換えが終了した旨の連絡を行わなかった場合には，登録局によって本申請書で申請した証明書の失効を行うことに同意します。	☐
		6. 失効申請の本人性確認	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。	☐

図 6 証明書更新申請書(登録担当者用)

所属機関：機関責任者の所属機関名を記入してください。

機関責任者氏名：機関責任者の氏名を記入してください

登録担当者氏名：登録担当者の氏名を記入してください。

登録担当者 E-mail：プロジェクト登録時の連絡先 E-Mail を記入してください。

申請ドメイン：プロジェクト登録時に申請したドメインを記入してください。

確認実施日：申請書記入日時を記入してください。

申請数：証明書発行申請数を記入してください。

申請した FQDN：サーバの FQDN（証明書の CN に記述する項目）を記入してください。

CSR：「4. CSR の作成について」で作成した CSR を貼り付けてください。

確認項目：記述されている内容に確認・同意し，チェック欄にチェックをつけてください。