Ver.1.9

証明書自動発行支援システム
操作手順書(加入者用)

2013/6/20

国立情報学研究所

改版履歴			
版数	日付	内容	担当
V.1.0	2009/5/15	初版	NII
V.1.1	2009/6/3	改行コード「LF」を追加	NII
V.1.2	2009/6/18	加入者 FQDN 文字数を修正 dNSName 文字数・入力値を修正	NII
V.1.3	2009/7/13	ブラウザの設定方法の記述内容変更 誤植の修正	NII
V.1.4	2009/8/6	TSV ファイル形式の「文字」列の変更 「半角英字」→「半角英数字」	NII
V.1.5	2009/9/11	ファイル名変更、文字の統一、誤植の修正	NII
V.1.6	2009/10/13	DN 使用可能文字拡張 登録担当者氏名欄等の半角入力対応 失効申請 TSV への加入者メールアドレス包括対応 誤植の修正	NII
V.1.7	2011/2/28	誤植の修正 ブラウザの設定方法の記載を削除 動作環境に Windows7 を追加。 動作環境から Widows2000SP4、WindowsME、Windows98 SE を削除。 動作環境から Netscape を削除。 動作環境を IE6.0 以降へ変更。 登録担当者証明書取得の記述内容変更(証明書選択画面の表示を記載) サーバ証明書インストールマニュアルに IIS7.0・IIS7.5 を追加 DN のルールの記載変更	NII
V.1.8	2012/03/30	暗号アルゴリズムのセキュリティ対応のため、サーバ証明書および CSR の鍵長 1024 ビット記載削除 サーバ証明書更新申請及び失効申請ファイル形式でシリアル番号に 16 進数を許容したことを記載	NII
V.1.9	2013/6/20	誤植の修正	NII

目次

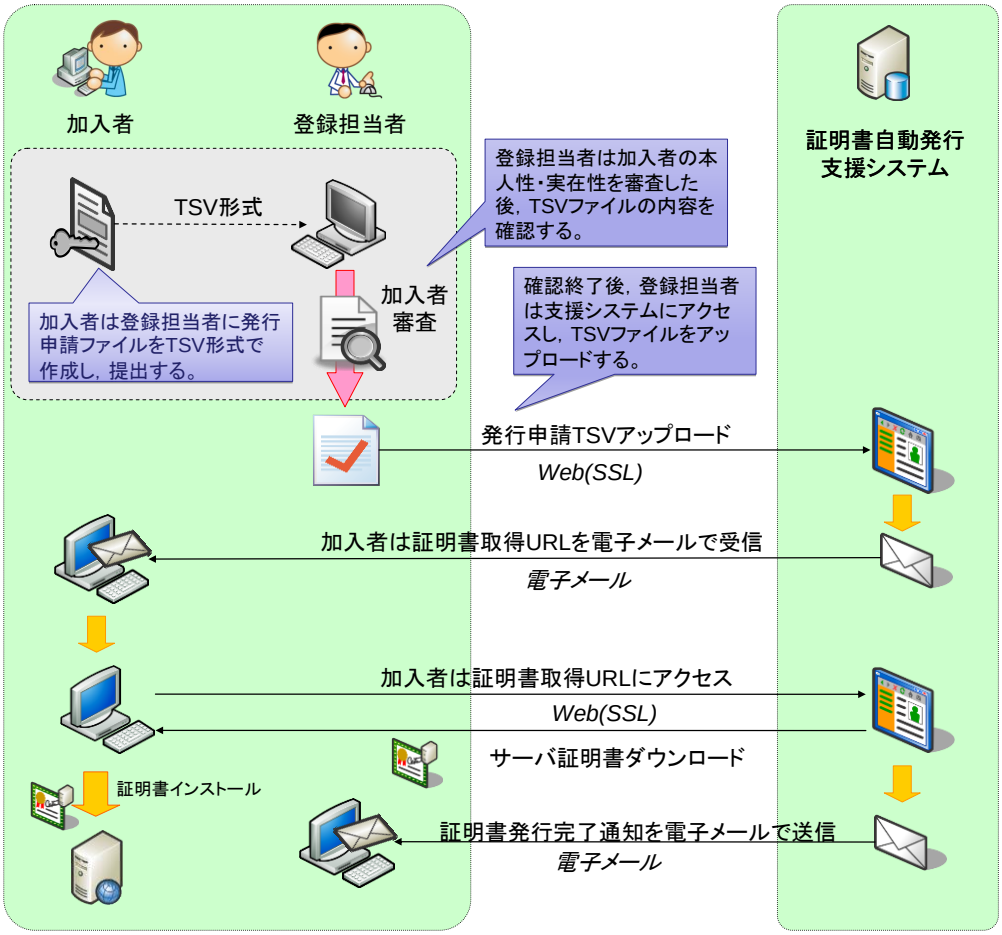
1.はじめに

証明書自動発行支援システム操作手順書（加入者用）（以下、「本手順書」）は、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、「プロジェクト」）に参加する機関に所属する加入者が、サーバ証明書を申請するための手続き、申請方法等を記載します。

1-1.サーバ証明書の取得概要

サーバ証明書の取得までの概要を以下に示します。

サーバ証明書の発行申請



【プロジェクトの関係者】

機関責任者	プロジェクトに参加する、または参加申請を行う機関の代表者。
証明書自動発行支援システム（以下、本システム）	証明書の申請の受付、審査、送付、管理を代行するシステムです。プロジェクトでは、本システムを用いて証明書の申請、審査、配付を実施します。
事務局	国立情報学研究所が実施する、プロジェクト参加手続き、証明書発行手続きの実務を行う組織。
登録担当者	各プロジェクト参加機関の加入者からの申請を取りまとめ、本システムに申請を行う者
加入者	各プロジェクト参加機関に所属し、証明書を申請、使用するサーバの管理者。

【証明書の取得まで】

サーバ証明書の取得まで
【サーバ証明書発行申請】 1. プロジェクトに参加した機関の加入者は、発行申請ファイルを作成し、各機関の登録担当者へ提出します。 2. 登録担当者は加入者の申請内容を審査し、本システムへ発行申請ファイルをアップロードします。 3. アップロードされたデータに問題がなければ、本システムより加入者へ証明書取得 URL を通知します。 4. 加入者は証明書取得 URL にアクセスし証明書の取得を行います。

1-2.本書の範囲

本書では以下の(a、b、c、d)の作業について記述をします。

マニュアル名	内容
操作手順書（加入者用）	a. 加入者が実施する本システムへのサーバ証明書発行申請・取得について（2 章に記載） b. 加入者が実施する本システムへのサーバ証明書更新申請・取得について（3 章に記載） c. 加入者が実施する本システムへのサーバ証明書失効申請について（4 章に記載） d. 本システムへの証明書アップロードフォーマットについて(５章に記載)
サーバ証明書インストールマニュアル※1	e. ＣＳＲと鍵ペアの作成方法について f. サーバ証明書のインストール方法について

※1 以下のマニュアルを総称して「サーバ証明書インストールマニュアル」と呼びます。

- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IBM HTTP Server 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Tomcat(JavaKeytool)編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Apache-SSL 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Apache2.0 系+mod_ssl 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Apache1.3 系+mod_ssl 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS7.0・IIS7.5 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS6.0 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS5.0 編

1-3.動作環境について

本システムで動作を確認している環境は、次表の通りです。

ブラウザ
Microsoft Internet Explorer 6.0 以降
Firefox2.0 以降

OS
Microsoft Windows 7
Microsoft Windows Vista(SP なし～SP2)
Microsoft Windows XP(SP なし～SP3)

なお、各種証明書をダウンロードする際は、以下を前提します。

- **Web ブラウザの設定で JavaScript が有効であること。**

※ JavaScript の設定方法に関しましては「1-4 ブラウザの設定方法」をご確認ください。

1-4.CSR とは

CSR（証明書発行要求：Certificate Signing Request）は証明書を作成するための元となる情報で、その内容には、加入者が管理する SSL/TLS サーバの組織名、Common Name（サーバの FQDN）、公開鍵などの情報が含まれています。NII では、加入者に作成いただいた CSR の内容を元に、証明書を作成します。CSR ファイルは通常 PEM 形式で表示されます。CSR を PEM 形式で表示したフォーマットは以下のようなものとなります。

CSR の例
-----BEGIN CERTIFICATE REQUEST----- MIIBSTCB9AIBADCBjjELMAkGA1UEBhMCSlAxEDAOBgNVBAcTB0FjYWRlbWUxKjAo BgNVBAoTIU5hdGlvbmFsIEluc3RpdHV0ZSBvZiBJbmZvcm1hdGljczEiMCAGA1UE ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ lGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z/ze BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG7ORkIss4ST6PDF+RQw+TRdkzl8TUF -----END CERTIFICATE REQUEST-----

1-5.認証のパス

プロジェクトでは、Web Trust for CA を取得した認証局（以下 RootCA という）の下位CAとして、NII Open DomainCA -G2(以下本CA)を運用し、プロジェクト参加機関に対してサーバ証明書の発行を行います。

プロジェクトで必要となる証明書の種類は以下の通りです。

役割	名称	解説
RootCA 証明書	Security Communication RootCA1 証明書	Web Trust for CA 基準の認定を取得した RootCA。主要なブラウザ、携帯電話に登録されています。
	リポジトリ:https://repository.secomtrust.net/SC-Root1/	
中間 CA 証明書	NII Open DomainCA -G2 証明書	Web Trust for CA 基準の認定を受けた認証局から発行された中間CA証明書。この証明書を持つ認証局から、プロジェクト参加機関への証明書発行を行います。この証明書は SSL 通信を行うサーバに登録する必要があります。
	リポジトリ:https://repo1.secomtrust.net/sppca/nii/odca2/index.html	

1-6.証明書の申請種別

Web サーバ証明書の新規発行が必要な場合は「新規証明書発行」を行ってください。

既にWeb サーバ証明書を本システムから発行していて、Web サーバ証明書の更新、失効された証明書の再発行を行う場合は「更新証明書発行」を行ってください。

Web サーバ証明書の失効を行う場合は「証明書失効」を行ってください。

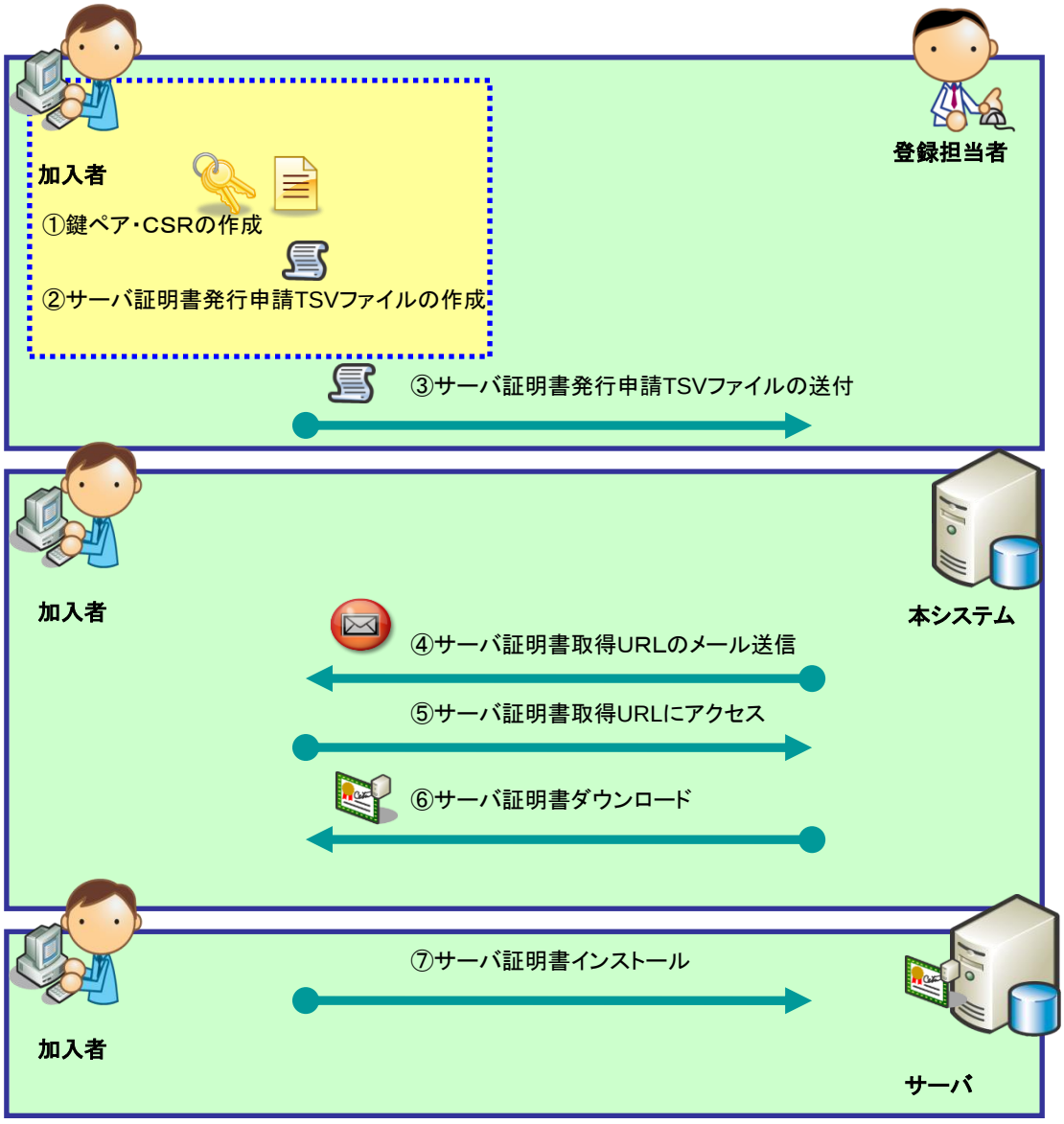
手続きの種別	手続きを行う主な機会
新規証明書発行 (**2.サーバ証明書の新規申請手続き**)	新規にサーバ証明書の発行を必要とする場合。
	サーバ証明書の記載内容（主体者 DN）を変更する場合。
証明書更新発行 (**3.サーバ証明書の更新申請手続き**)	サーバ証明書の(主体者 DN 以外の)記載内容を変更する場合。
	有効期限内の証明書を継続利用したい場合。
	有効期限の切れた証明書を継続利用したい場合。
	失効されたサーバ証明書の再発行を行う場合。
証明書失効 (**4.サーバ証明書の失効申請手続き**)	サーバ証明書が不要になった場合や秘密鍵が危殆化した場合。

2.サーバ証明書の証明書新規申請手続き

2-1.サーバ証明書新規発行手続き概要

本章では加入者のサーバ証明書の取得手続きの流れについて記述を行います。

加入者は以下の手続きにより証明書の新規申請・取得を行います。



加入者用証明書新規発行手続き概要
① 鍵ペアとCSRを作成してください。（**別冊「サーバ証明書インストールマニュアル」～2-3 に記載**）
② サーバ証明書の発行申請を行うためのサーバ証明書発行申請 TSV を作成してください。**(2-3 に記載)**
③ 決められた手続きに従い、登録担当者へサーバ証明書発行申請 TSV を送付してください。**(2-4 に記載)**
④ 登録担当者がサーバ証明書発行申請 TSV を本システムにアップロードすると、本システムより、メールで証明書取得 URL が送信されます。**(2-5 に記載)**
⑤ メールを受信したら、証明書取得 URL にアクセスしてください。**(2-5 に記載)**
⑥ 「Web サーバ証明書ダウンロード画面」が開きますので、証明書をダウンロードしてください。**(2-6 に記載)**
⑦ 当該のサーバへサーバ証明書のインストールを行ってください。（**別冊「サーバ証明書インストールマニュアル」～2-5 に記載**）

2-2.鍵ペア・CSR の作成

別冊「**サーバ証明書インストールマニュアル**」または、ご使用のサーバのマニュアルに従い、鍵ペア・CSRを作成してください。鍵長、DNのルールは以下の通りです。

DN のルール			
項目	指定内容の説明と注意	必須	文字数および注意点
Country(C)	本認証局では必ず「JP」と設定してください。 例） C=JP	○	JP 固定
State or Province Name(ST)	本認証局では使用しないでください。	×	
Locality Name(L)	本認証局では必ず「Academe2」と設定してください。 例)L=Academe2	○	Academe2 固定
Organization Name(O)	プロジェクト参加申請時の機関名英語表記を設定してください。この情報は各所属機関の登録担当者にお問い合わせください。 例)O=National Institute of Informatics	○	半角の英数字 64 文字以内 (記号は「' (),-./:=」と半角スペースのみ使用可能)
Organizational Unit Name(OU)	証明書を使用する部局等の名前を設定してください。 （この値は省略可能です） （この値は複数設定することが可能です。複数指定する方法につきましては、CSR 作成時ご使用のアプリケーションのマニュアルをご確認ください。） 例)OU=Cyber Science Infrastructure Development Department	△	・半角の英数字 64 文字以内 (記号は「' (),-./:=」と半角スペースのみ使用可能) ・複数 OU を指定する場合は、全体で 64 文字以内
Common Name(CN)	証明書をインストールするウェブ・サーバの名前を FQDN で設定してください。例えば SSL/TLS を行うサイトが https://www.nii.ac.jp の場合には、「www.nii.ac.jp」となります。FQDN にはプロジェクト参加申請時に登録いただいた対象ドメイン名を含む FQDN のみ、証明書発行が可能となります。 例)CN=www.nii.ac.jp	○	証明書をインストールする対象サーバの FQDN で 64 文字以内 半角英数字、”.“、“-”のみ使用可能。 また、先頭と末尾に“.”と“-”は使用不可
Email	本認証局では使用しないでください。	×	

鍵長			
RSA 2048bit			

○・・・必須　×・・・入力不可　△・・・省略可

2-3.サーバ証明書発行申請 TSV ファイルの作成

登録担当者へ送付するためのサーバ証明書発行申請 TSV ファイルを作成してください。サーバ証明書発行申請 TSV ファイルのフォーマットは「5.本システムで扱うファイル形式」をご確認ください。

2-4.サーバ証明書発行申請 TSV ファイルの送付

「2-3.サーバ証明書発行申請 TSV ファイルの作成」で作成した TSV ファイルを各機関の決められた手続きに従い、登録担当者に送付してください。

2-5.サーバ証明書取得 URL の通知

サーバ証明書の発行が完了すると、本システムよりサーバ証明書を取得するための証明書取得 URL がメールにて通知されます。メール本文に記載された証明書取得 URL にアクセスし、サーバ証明書の取得を実施してください。

証明書取得 URL の通知

【件名】

Web サーバ証明書発行受付通知

・・・・・

#以下に証明書の取得先が記述されています。

貴機関の登録担当者経由で発行申請をいただきましたサーバ証明書を配付いたします。

本日から 1 ヶ月以内に以下の証明書取得 URL へアクセスし、サーバ証明書の取得を行ってください。

証明書取得 URL：https://scia.nii.ac.jp/～ **←左記 URL にアクセスし証明書の取得を行ってください。**

・・・・・

2-6.サーバ証明書の取得

「2-5.証明書取得 URL の通知」で通知された URL にアクセスしサーバ証明書を取得する方法を記述します。

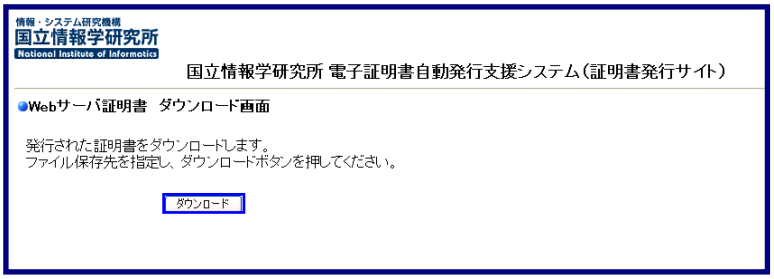
サーバ証明書の取得

1.「2-5.サーバ証明書取得 URL の通知」で通知された URL にアクセスします。

デジタル証明書の選択画面が表示される場合は、キャンセルしてください。

2. ダウンロードボタンをクリックすると、Base64 フォーマットで記載されたサーバ証明書ファイルが取得できます。

server.crt 等わかりやすい名前をつけて保存してください。



2-7.サーバ証明書のインストール

「2-6.サーバ証明書の取得」で取得したサーバ証明書を、対象のサーバにインストールしてください。サーバのインストール方法につきましては、当該のサーバのマニュアルをご確認ください。また、プロジェクトでは、以下のサーバに関して別冊「サーバ証明書インストールマニュアル」を用意しておりますので、あわせてご確認ください。

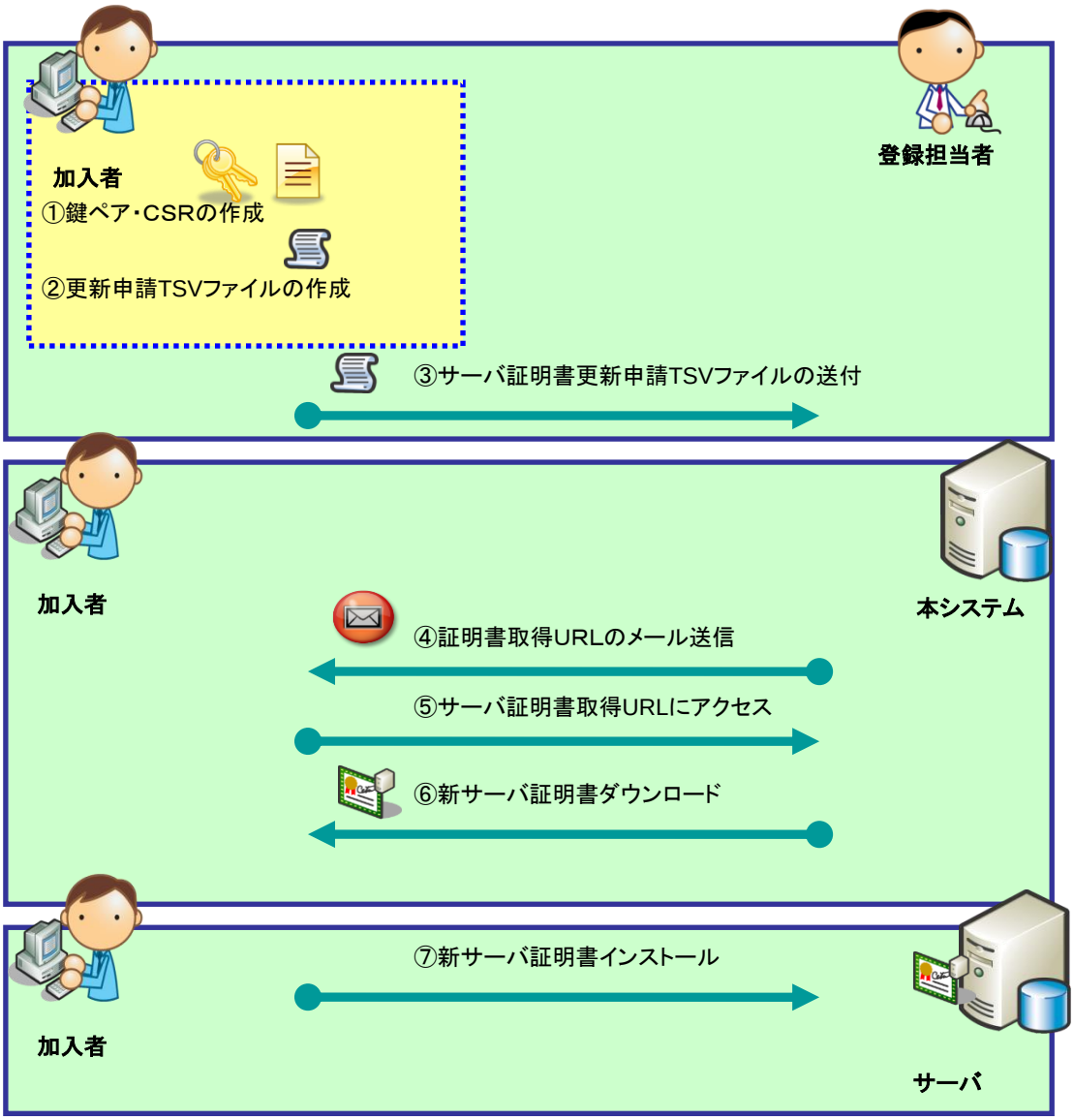
- Apache1.3 系
  - Apache-SSL
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル　Apache-SSL 編
  - Apache1.3+mod_SSL
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル　Apache1.3 系+mod_ssl 編
- Apache2.0 系
  - Apache2.0+mod_SSL
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル　Apache2.0 系+mod_ssl 編
- IIS 系
  - IIS5.0
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル　IIS5.0 編
  - IIS6.0
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル　IIS6.0 編
  - IIS7.0
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル　IIS7.0・IIS7.5 編
  - IIS7.5
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル　IIS7.0・IIS7.5 編
- Tomcat 系
  - Tomcat 4.0 / 5.0 / 6.0
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル Tomcat(JavaKeytool)編
- IBM HTTP Server
  - IBM HTTP Server7.0
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル　IBM HTTP Server 編

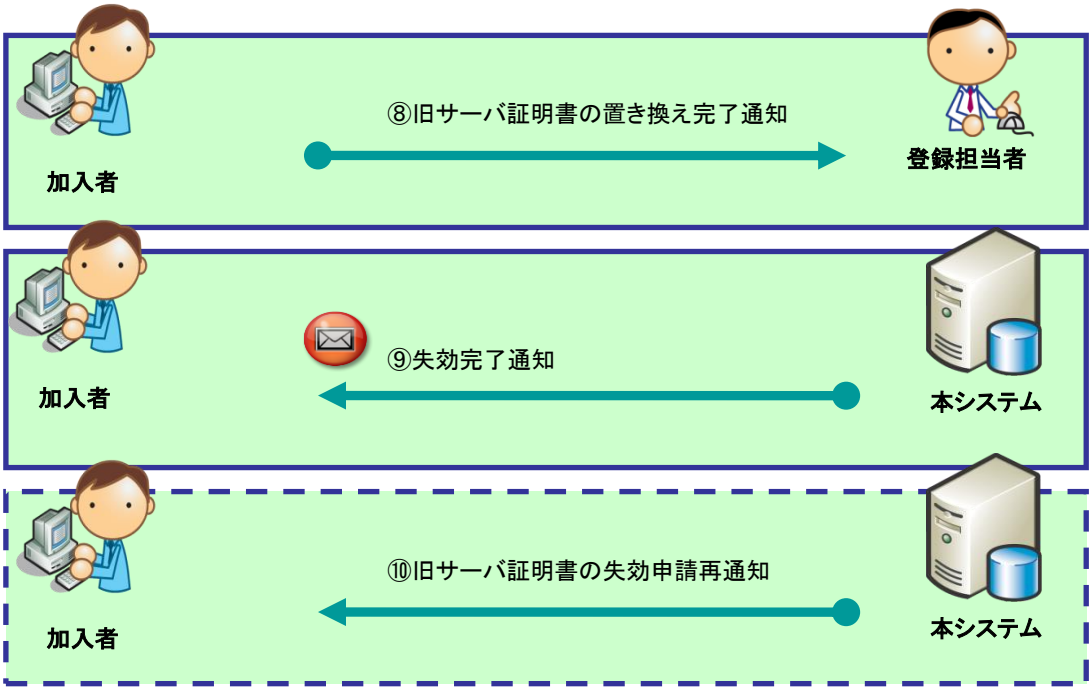
3.サーバ証明書の証明書更新申請手続き

3-1.サーバ証明書更新発行手続き概要

本章では加入者のサーバ証明書の更新取得手続きの流れについて記述を行います。

加入者は以下の手続きによりサーバ証明書の更新申請・取得を行います。




⑧旧サーバ証明書の置き換え完了通知
加入者
登録担当者
⑨失効完了通知
加入者
本システム
⑩旧サーバ証明書の失効申請再通知
加入者
本システム

加入者用サーバ証明書更新発行手続き概要
① 鍵ペアとCSRを作成してください。（**別冊「サーバ証明書インストールマニュアル」～2-3 に記載**）
② サーバ証明書の更新申請を行うためのサーバ証明書更新申請 TSV を作成してください。**(3-3 に記載)**
③ 決められた手続きに従い、登録担当者へサーバ証明書更新申請 TSV を送付してください。**(3-4 に記載)**
④ 登録担当者がサーバ証明書更新申請 TSV を本システムにアップロードすると、本システムより、メールで証明書取得 URL を送信します。**(3-5 に記載)**
⑤ メールを受信したら、証明書取得 URL にアクセスしてください。**(3-5 に記載)**
⑥ 「Web サーバ証明書ダウンロード画面」が開きますので、新サーバ証明書をダウンロードしてください。**(3-6 に記載)**
⑦ 当該のサーバへ新サーバ証明書のインストールを行ってください。（**別冊 「サーバ証明書インストールマニュアル」～2-5、2-6 または 2-7 に記載**）
⑧ 旧サーバ証明書の置き換えが完了しましたら、各機関の決められた手続きに従い、登録担当者へ証明書の置き換え完了通知を行ってください。**(3-8 に記載)**
⑨ 登録担当者が本システムへサーバ証明書の失効申請を行うと、本システムより、失効完了通知が送信されます。**(3-9 に記載)**
【旧サーバ証明書の失効を行わないと・・・】
⑩ ⑥の**サーバ証明書**ダウンロードから 2 週間以上たっても旧サーバ証明書の失効申請が行われない場合、本システムより、失効依頼の再通知をメールで通知させていただきます。本メールを受領した加入者は速やかにサーバ証明書の置き換え完了通知を登録担当者に行ってください。**(3-10 に記載)**

3-2.鍵ペア・CSR の作成

別冊「サーバ証明書インストールマニュアル」または、ご使用のサーバのマニュアルに従い、CSRを作成してください。DN のルールにつきましては、「2-2.鍵ペア・CSR の作成」を参照してください。**更新時は以前の鍵ペアは使用せず、新たに鍵ペアを作成してください。更新時の DN に関しましては以前と同様の DN で申請をお願いします。DNの表記が旧サーバ証明書と異なる場合は、更新を行うことができません。**

3-3.更新申請 TSV ファイルの作成

登録担当者へ送付するためのサーバ証明書更新申請 TSV ファイルを作成してください。更新申請 TSV ファイルのフォーマットは「5.本システムで扱うファイル形式」をご確認ください。

3-4.更新申請 TSV の送付

各機関の決められた手続きに従い、更新申請 TSV ファイル登録担当者に送付してください。

3-5.サーバ証明書取得 URL の通知

サーバ証明書の発行が完了すると、本システムより新サーバ証明書を取得するための証明書取得 URL がメールにて通知されます。メール本文に記載された証明書取得 URL にアクセスし、新サーバ証明書の取得を実施してください。

サーバ証明書取得 URL の通知
【件名】 Web サーバ証明書発行受付通知 ・・・・・ **#以下に証明書の取得先が記述されています。** 貴機関の登録担当者経由で発行申請をいただきましたサーバ証明書を配付いたします。 本日から 1 ヶ月以内に以下の証明書取得 URL へアクセスし、サーバ証明書の取得を行ってください。 **証明書取得 URL：https://scia.nii.ac.jp/～**　**←左記 URL にアクセスし新サーバ証明書の取得を行ってください。** ・・・・・

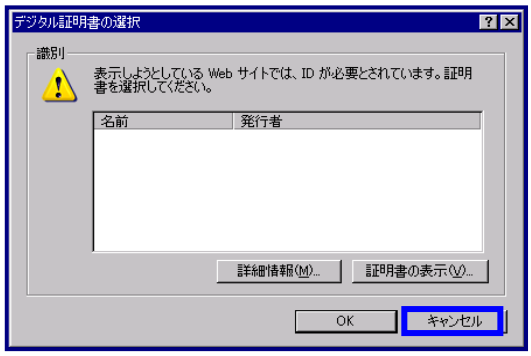
3-6.新サーバ証明書の取得

「3-5.サーバ証明書取得 URL の通知」で通知された URL にアクセスし新サーバ証明書を取得する方法を記述します。

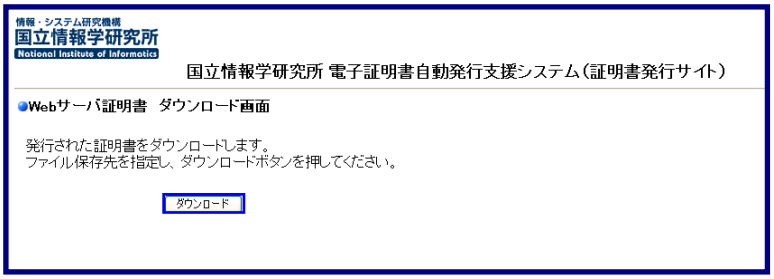
サーバ証明書の取得

1.「3-5.サーバ証明書取得 URL の通知」で通知された URL にアクセスしします。

デジタル証明書の選択画面が表示される場合は、キャンセルしてください。



2. ダウンロードボタンをクリックすると、Base64 フォーマットで記載されたサーバ証明書ファイルが取得できます。server.crt 等わかりやすい名前をつけて保存してください。



3-7.サーバ証明書のインストール

「3-6.サーバ証明書の取得」で取得したサーバ証明書を、対象のサーバにインストールしてください。サーバへのインストール方法につきましては、「2-7.サーバ証明書のインストール」で記載した別冊「サーバ証明書インストールマニュアル」または、当該のサーバのマニュアルをご確認ください。

3-8.新サーバ証明書の置き換え完了通知

更新したサーバ証明書をサーバにインストール後、各機関の決められた手続きに従い、登録担当者へサーバ証明書の置き換えが完了したことを通知してください。完了通知をもって、登録担当者はサーバ証明書の失効申請を本システムに行います。

3-9.旧サーバ証明書の失効通知

旧サーバ証明書の失効が完了すると、本システムよりサーバ証明書失効完了通知がメールで送信されます。失効されたサーバ証明書のシリアル番号に誤りが無いか確認してください。

サーバ証明書失効完了の通知

【件名】

Web サーバ用証明書失効完了通知

・・・・・

#失効された証明書のシリアル番号に誤りが無いか確認してください。

【失効証明書シリアル番号】

xxxxxxxxxx

・・・・・

3-10.旧サーバ証明書の失効申請依頼再通知について

サーバ証明書の置き換え完了後、登録担当者に対して、旧サーバ証明書の失効完了通知が行われなかった場合、または各機関の登録担当者に完了通知を行ったものの、登録担当者が何らかの理由で、旧サーバ証明書の失効を実施しなかった場合、旧サーバ証明書の失効を依頼する再通知が送信されます。本メールを受信した場合は、速やかに登録担当者へサーバ証明書の置き換え完了を通知してください。また、完了通知を行っていたにもかかわらず、本メールを受信した場合は、各機関の登録担当者へ失効の申請状況を確認してください。

失効申請依頼再通知

【件名】

Web サーバ用証明書更新(旧証明書の失効申請)再通知

加入者の方が Web サーバ用更新証明書を取得してから 2 週間が経過いたしました。

旧証明書は不要ですので、速やかに失効申請をお願い申し上げます。

・・・・・

【旧証明書のシリアル番号】

xxxxxxxxxx

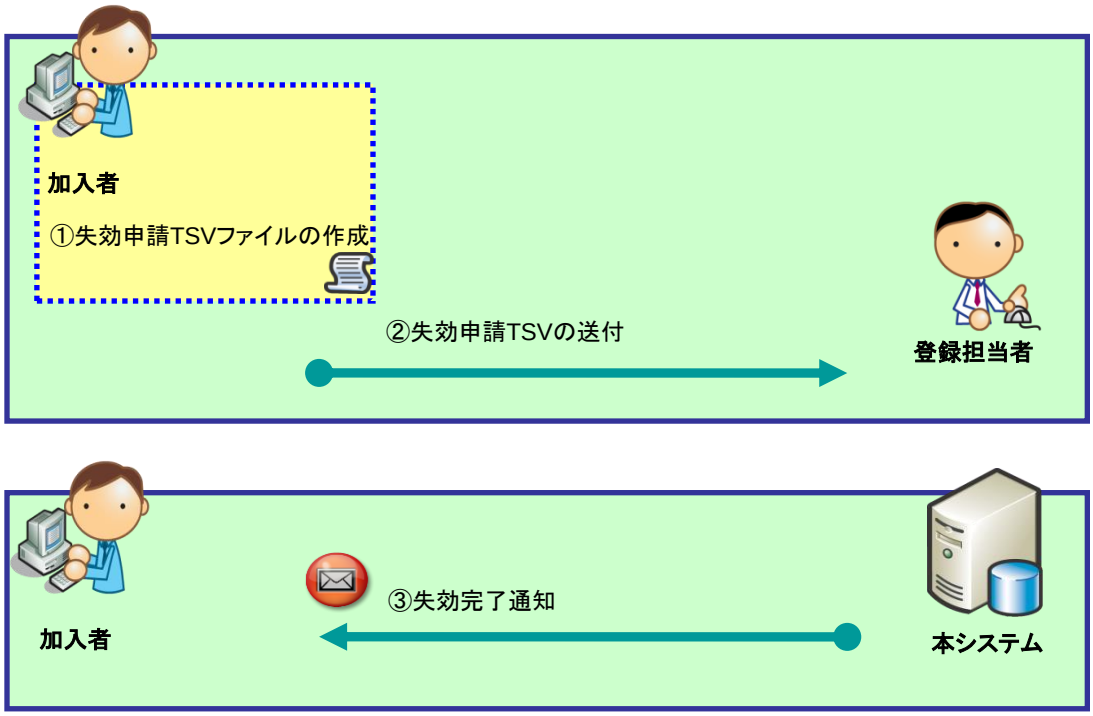
・・・・・

4.サーバ証明書の証明書失効申請手続き

4-1.サーバ証明書失効手続き概要

本章では加入者のサーバ証明書の失効手続きの流れについて記述を行います。

加入者は以下の手続きによりサーバ証明書の失効・取得をおこないます。



加入者用サーバ証明書失効発行手続き概要
① サーバ証明書の失効申請を行うための失効申請 TSV を作成してください。 ② 決められた手続きに従い、登録担当者へ失効申請 TSV を送付してください。 ③ 登録担当者が本システムへサーバ証明書の失効申請を行うと、本システムより、失効完了通知が送信されます。

4-2.失効申請 TSV ファイルの作成

登録担当者へ送付するためのサーバ証明書失効申請 TSV ファイルを作成してください。失効申請 TSV ファイルのフォーマットは「5.本システムで扱うファイル形式」をご確認ください。

4-3.失効申請 TSV ファイルの送付

各機関の決められた手続きに従い、登録担当者へ失効申請 TSV ファイルを送付してください。

4-4.失効完了通知

サーバ証明書の失効が完了すると、本システムより Web サーバ証明書失効完了通知がメールで送信されます。

サーバ証明書失効完了の通知
【件名】 Web サーバ用証明書失効完了通知 ・・・・・ **#失効された証明書のシリアル番号に誤りが無いか確認してください。** 【失効証明書シリアル番号】 xxxxxxxxxx ・・・・・

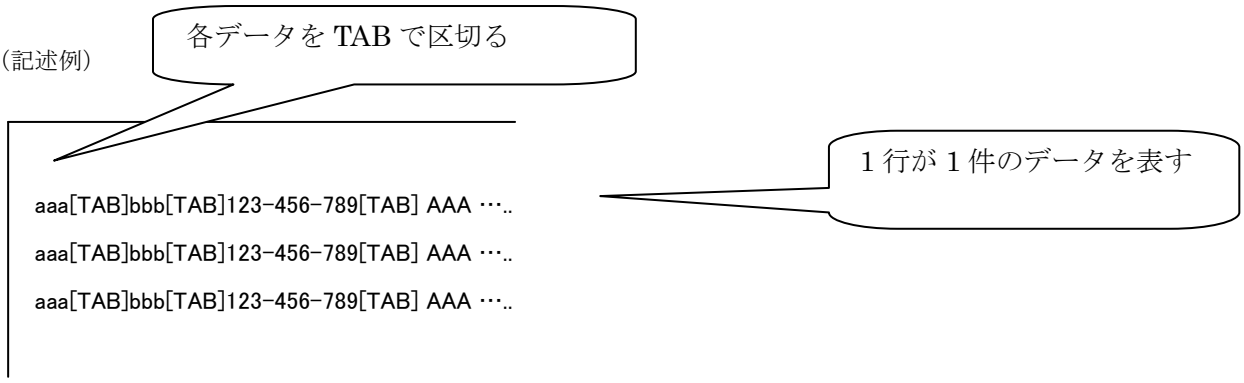
5.本システムで扱うファイル形式

5-1. TSV ファイル形式

本システムで申請を受け付けることができるファイル形式 TSV 形式とします。

ファイル形式	TSV 形式（※:タブ区切りのプレーンテキストファイル）
申請ファイル拡張子	.tsv または .txt
文字コード	Shift-JIS
改行コード	CR+LF または LF

（記述例）



入力が必須でない項目は[TAB]で埋めてください。1 レコードに保有する TAB の数は、全項目入力した際の TAB の数と同数となります。

例)

aaa[TAB]bbb[TAB]123-456-789[TAB] AAA[TAB]　　※bbb のデータを Null とする場合

↓

aaa[TAB][TAB]123-456-789[TAB] AAA[TAB]

5-2.サーバ証明書発行申請 TSV ファイル形式

No	項目名称	文字	サイズ (文字数)	入力値
1	主体者 DN	半角英数字記号	250	CSR 作成時に設定した DN を”CN,OU,O,L,C“の順序で記述してください。 ※CSR に記述された DN と異なる場合はエラーとなります。 例) CN=www.nii.ac.jp, OU=Cyber Science Infrastructure Development Department, O=National Institute of Informatics, L=Academe2, C=JP
2	証明書プロファイル ID	半角数字	1	1(固定値)
3				・・・・・・・・・・No3～No6 まで空白
4				・・・・・・・・・・No3～No6 まで空白
5				・・・・・・・・・・No3～No6 まで空白
6				・・・・・・・・・・No3～No6 まで空白
7	CSR	半角英数字	2048	「**2-2 CSR の作成**」で記述した作成した CSR を記述してください。 -----BEGIN CERTIFICATE REQUEST-----から-----END CERTIFICATE REQUEST-----までを削除し、一行で記述してください。 ※鍵長が 2048bit 以外はエラーとなります。
8	加入者氏名	全角、半角	64	加入者の氏名を記述してください。 例)国立　太郎
9	加入者所属	全角、半角	64	加入者の所属部署を記述してください。 例)学術基盤推進部基盤企画課
10	加入者 mail	半角英数字	78	加入者の Email アドレスを記述してください。 証明書取得 URL の送信先となります。 例)xxxxx@example.com
11	加入者 FQDN	半角英数字記	64	CSR で設定した CN を記述してください。 例)www.nii.ac.jp

		号		
12	加入者ソフトウェア名・バージョン	半角 全角	128	証明書をインストールするソフトウェアの名前・バージョン番号を記述してください。 例)apache2.0
13	dNSName	半角英数字記号	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。加入者 FQDN 値が含まれていない場合、自動付与されます。自動付与されるサーバ FQDN 値含め 250 文字以内としてください。 ホスト名を「dNSName=XXX,dNSName=ZZZ」の形式で記載してください。 ※半角英数字、”.“、“-”のみ使用可能です。また、先頭と末尾に“.”と“-”は使用できません。

5-3.サーバ証明書更新申請 TSV ファイル形式

No	項目名称	文字	サイズ（文字数）	入力値
1	主体者 DN	半角英数字記号	250	CSR 作成時に設定した DN を”CN,OU,O,L,C“の順序で記述してください。 ※CSR に記述された DN と異なる場合はエラーとなります。 例） CN=www.nii.ac.jp, OU=Cyber Science, Infrastructure Development Department, O=National Institute of Informatics, L=Academe2, C=JP
2	証明書プロファイル ID	半角数字	1	1(固定値)
3				・・・・・・・・・・No3 は空白
4	失効対象証明書シリアル番号	半角英数字	32	旧証明書のシリアル番号を 10 進数または 16進数で記述してください。 10 進数の場合 例) 1234567812345678123 16 進数の場合 例) 0x112210E261FEC92B ※16 進数の場合は先頭に[0x]をつけてください。半角英字は大文字小文字どちらも使用できます。
5				・・・・・・・・・・No5～No6 まで空白
6				・・・・・・・・・・No5～No6 まで空白
7	CSR	半角英数字	2048	「**2-2 CSR の作成**」で記述した作成した CSR を記述してください。 -----BEGIN CERTIFICATE REQUEST-----から -----END CERTIFICATE REQUEST-----までを削除し、一行で記述してください。 ※以前使用した鍵ペアの再利用はできません。 ※鍵長が 2048bit 未満はエラーとなります。
8	加入者氏名	全角、	64	加入者の氏名を記述してください。 例)国立　太郎

		半角		
9	加入者所属	全角、半角	64	加入者の所属部署を記述してください。 例)学術基盤推進部基盤企画課
10	加入者 mail	半角英数字	78	加入者の Email アドレスを記述してください。 証明書取得 URL の送信先となります。 例)xxxxx@example.com
11	加入者 FQDN	半角英数字記号	64	CSR で設定した CN を記述してください。 例)www.nii.ac.jp
12	加入者ソフトウェア名・バージョン	半角全角	128	証明書をインストールするソフトウェアの名前・バージョン番号を記述してください。 例)apache2.0
13	dNSName	半角英数字記号	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。加入者 FQDN 値が含まれていない場合、自動付与されます。自動付与されるサーバ FQDN 値含め 250 文字以内としてください。 ホスト名を「dNSName=XXX,dNSName=ZZZ」の形式で記載してください。 ※半角英数字、”.“、“-”のみ使用可能です。また、先頭と末尾に“.”と“-”は使用できません。

5-4.サーバ証明書失効申請 TSV ファイル形式

No	項目名称	文字	サイズ（文字数）	入力値
1	主体者 DN	**半角英数字記号**	250	CSR 作成時に設定した DN を”CN,OU,O,L,C“の順序で記述してください。 ※CSR に記述された DN と異なる場合はエラーとなります。 例） CN=www.nii.ac.jp, OU=Cyber Science Infrastructure Development Department, O=National Institute of Informatics, L=Academe2, C=JP
2				・・・・・・・・・・No2～No3 は空白
3				・・・・・・・・・・No2～No3 は空白
4	失効対象証明書シリアル番号	半角数字	32	旧証明書のシリアル番号を 10 進数または 16 進数で記述してください。 10進数の場合 例）1234567812345678123 16進数の場合 例）0x112210E261FEC92B ※16 進数の場合は先頭に[0x]をつけてください。半角英字は大文字小文字どちらも使用できます。
5	失効理由	半角数字	1	失効理由を以下から選択し、記述してください。 0・・・unspecified（未定義） 1・・・KeyCompromise（鍵の危殆化） 3・・・affiliationChanged（主体 DN の変更） 4・・・superseded（証明書の更新または証明書記載内容の変更） 5・・・cessationOfOperation（証明書の利用終了）
6	失効理由コメント	**全角、半角**	128	失効理由にコメントが必要な場合は、記述してください。
7				・・・・・・・・・・No7～No9 は空白
8				・・・・・・・・・・No7～No9 は空白

9				・・・・・・・・・・No7～No9 は空白
10	加入者 mail	半角英数字	78	加入者が変更になった場合、変更後の Email アドレスを記述してください。 例)xxxxx@example.com
11				・・・・・・・・・・No11～No13 は空白
12				・・・・・・・・・・No11～No13 は空白
13				・・・・・・・・・・No11～No13 は空白