利用管理者用

改版履歴			
版数	日付	内容	担当
V.1.1	2014/12/22	初版	NII
V.1.2	2015/1/14	誤植の修正 サーバ証明書発行／更新時の制限追記 サーバ証明書発行／更新／失効申請ファイル中の制限追記	NII
V.1.3	2015/4/1	サーバ証明書の発行・更新機能の修正 クライアント証明書の発行・更新・失効機能の追加 コード署名用証明書の発行・更新・失効機能の追加	NII
V.1.4	2015/4/9	誤植の修正	NII
V.1.5	2015/12/11	全角文字使用可能文字の範囲を追記 アクセスPIN／証明書ZIPファイル構成説明追加	NII
V.1.6	2016/4/7	誤植の修正 目次の修正	NII
V.1.7	2017/2/28	コード署名用証明書のダウンロード種別P12を削除 クライアント証明書P12一括発行時の注意事項追記	NII
V.1.8	2017/7/27	誤植の修正	NII
V.2.0	2018/2/26	SHA-1に関する記述削除	NII
V.2.1	2018/ 7 / 9	1-3.認証のパスに関する記述の修正 5-3-1. サーバ証明書発行申請TSVファイル形式 5-3-2. サーバ証明書更新申請TSVファイル形式 CSRの鍵長の記載を修正、主体者DNの修正とSTの追加 2-1-1. DNのルールの修正 3-2-3. 誤植の修正 メールテンプレートにおけるLの修正とSTの追加 5-3-3.サーバ証明書失効申請TSVファイル形式 5-4.クライアント証明書申請TSVファイル形式 5-5.コード署名用証明書申請TSVファイル形式 主体者DNの修正とSTの追加 5-4.クライアント証明書申請TSVファイル形式 項目番号１５：アクセスPINの追加 項目番号１２：P12ダウンロードファイル名、その他の記載内容を修正 5-7-1.証明書情報ファイル構成 Lの修正とSTの追加	NII
V.2.2	2018/7/11	証明書プロファイルID:11の追加	NII
V.2.3	2018/8/27	5-3-1. サーバ証明書発行申請TSVファイル形式 5-3-2. サーバ証明書更新申請TSVファイル形式 項目番号７:CSRの記述を修正 5-5-1. コード署名用証明書発行申請TSVファイル形式 5-5-2. コード署名用証明書更新申請TSVファイル形式項目番号７:CSRの記述を修正	NII
V.2.4	2019/4/22	5-3-2. サーバ証明書更新申請TSVファイル形式 5-3-3. サーバ証明書失効申請TSVファイル形式 項目番号4: シリアル番号桁数変更 5-4.クライアント証明書申請TSVファイル形式 証明書プロファイルID:13 証明書プロファイルID:14 証明書プロファイルID:15 証明書プロファイルID:16 の追加 5-4-1. クライアント証明書発行申請TSVファイル形式 5-4-2. クライアント証明書更新申請TSVファイル形式 項目番号15: アクセスPIN指定条件追加	NII
V.2.5	2019/6/10	2.1.1 DNのルール(Locality Name)の修正	NII
V.2.6	2019/6/26	5-3-1. サーバ証明書発行申請TSVファイル形式 5-3-2. サーバ証明書更新申請TSVファイル形式 項目番号13: dNSNameの指定可能個数条件追加	NII
V.2.7	2020/4/27	コード署名用証明書の発行・更新・失効の方式について追記および修正	NII
V.2.8	2020/6/4	コード署名用証明書の中間CA証明書とリポジトリの変更 tsvファイルを利用したコード署名用証明書の発行・失効方式を削除 コード署名用証明書申請tsvファイル形式削除 IIS7.5に関する記載を削除	NII
V.2.9	2020/7/15	DNのルール、TSVファイル形式のSTおよびLの値の説明、リンクの変更	NII
V.2.10	2020/8/25	コード署名証明書、発行申請書、失効申請書フォーマットを修正	NII

V.2.11	2020/12/22	中間CA証明書を修正 サーバー証明書L、STを必須に修正 サーバー証明書OUの利用条件を修正	NII
V.2.12	2021/5/31	コード署名用証明書の中間CA証明書を修正 NII Open DomainCA-G5、G6の削除	NII
V2.13	2022/03/10	証明書プロファイルID:7:S/MIME証明書 の有効期間の変更	NII
V2.14	2022/08/02	2-1-1. 鍵ペア・CSRの作成 OU欄の削除	NII
V.2.15	2023/5/19	コード署名用証明書のCSR作成に関する手順を削除	NII
V.2.16	2023/9/5	S/MIME証明書 BR対応に関する申請TSVファイル形式の修正	NII
V.2.17	2023/9/14	クライアント証明書の有効期限変更	NII
V.2.18	2023/12/14	クライアント証明書および登録担当者用証明書切り替え	NII

目次

1. はじめに

1-1. 本書の範囲

本書では以下の（a、b、c、d、e、f、g、h、i、j、k、l）の作業について記述します。

マニュアル名	内容

証明書自動発行支援システム操作マニュアル（利用管理者用）	a.利用管理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（2-1に記載） b.利用管理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（2-2に記載） c.利用管理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（2-3に記載） d.本システムへの申請アップロードフォーマットについて(5-３に記載) e.利用管理者が実施する本システムへのクライアント証明書発行申請・取得について（3-2に記載） f.利用管理者が実施する本システムへのクライアント証明書更新申請・取得について（3-3に記載） g.利用管理者が実施する本システムへのクライアント証明書失効申請について（3-4に記載） h.本システムへの申請アップロードフォーマットについて(5-4に記載) i.利用管理者が実施する本システムへのコード署名用証明書失効申請について（4-2に記載） j.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(5-5に記載)
サーバ証明書インストールマニュアル※1	k.CSRと鍵ペアの作成方法について l.サーバ証明書のインストール方法について
証明書インストールマニュアル※2	m.Webブラウザへの証明書のインストール方法について n.メーラーへの証明書のインストール方法について
コード署名用証明書利用マニュアル※3	o.CSRと鍵ペアの作成方法について p.コード署名用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 はじめに -サーバ証明書インストールマニュアルについて-
・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(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 IBM HTTPServer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 IIS8.0・IIS8.5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 IIS10.0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 OpenLDAP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 Nginx編

※2 以下のマニュアルを総称して「証明書インストールマニュアル」と呼びます。
・Webブラウザへのインストールマニュアル はじめに -Webブラウザへのインストールマニュアルについて-
・Webブラウザへのインストールマニュアル Internet Explorer・Edge・Chrome・Opera編 (Windows)
・Webブラウザへのインストールマニュアル Safari・Chrome・Opera編 (macOS)
・Webブラウザへのインストールマニュアル Firefox編 (Windows・macOS)
・Webブラウザへのインストールマニュアル Android編
・Webブラウザへのインストールマニュアル iOS編
・メーラーへのSMIME証明書インストールマニュアル はじめに -メーラーへのS/MIME証明書インストールマニュアルについて-
・メーラーへのSMIME証明書インストールマニュアル Microsoft Office Outlook編
・メーラーへのSMIME証明書インストールマニュアル Mozilla Thunderbird編
・メーラーへのSMIME証明書インストールマニュアル Apple Mail編

※3 以下のマニュアルを総称して「コード署名用証明書利用マニュアル」と呼びます。
・コード署名用証明書利用マニュアル はじめに -コード署名用証明書利用マニュアルについて-
・コード署名用証明書利用マニュアル 鍵ペアの生成とCSRの作成～ 証明書の申請から取得まで
・コード署名用証明書利用マニュアル Windows用(.exe,.cab,.dll)形式編
・コード署名用証明書利用マニュアル Windows PowerShell用スクリプト形式編
・コード署名用証明書利用マニュアル JAVA .jar形式編
・コード署名用証明書利用マニュアル Adobe AIR形式編
・コード署名用証明書利用マニュアル VBAマクロ形式編
・コード署名用証明書利用マニュアル Android用 .apk形式編

1-2. 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、利用管理者が管理する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、利用管理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---- MIIBSTCB9AIBADCBjjELMAkGA1UEBhMCSIAxEDAOBgNVBAcTB0FjYWRlbWUxKjAo BgNVBAoTIU5hdGlvbmFsIEluc3RpdHV0ZSBvZiBJbmZvcm1hdGljczEiMCAGA1UE ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ lGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z /ze BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG70RkIss4ST6PDF+RQw+TRdkzI8TUF ----END CERTIFICATE REQUEST----

1-3. 認証のパス

サービスでは、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、
・SECOM Passport for Member PUB CA8(個人認証用証明書、S/MIME用証明書の発行日時が2020年12月25日0時以降の場合)
・NII Open Domain CA - G7 RSA(サーバ証明書の発行日時が2020年12月25日0時以降の場合)
・NII Open Domain CA - G7 ECC(サーバ証明書の発行日時が2020年12月25日0時以降の場合)
・SECOM Passport for CodeSigning CA G2(コード署名証明書の発行日時が2021年5月31日0時以前の場合)および(コード署名証明書の発行日時が2021年5月31日0時以降の場合)
・NII Open Domain S/MIME CA(S/MIME用証明書の発行日時が2020年12月25日0時以前の場合)
・NII Open DomainCA-G4(サーバ証明書の発行日時が2018年3月26日14時以前の場合、個人認証用証明書の発行日時が2020年12月25日0時以前の場合)
より、サービス参加機関に対して証明書の発行を行います。
サービス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
Root CA証明書	Security Communication RootCA2 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、スマートフォンに登録されています。
	リポジトリ：https://repository.secomtrust.net/SC-Root2/	
Root CA証明書	Security Communication RootCA3 証明書	Web Trust for CA基準の認定を取得したRootCA。Microsoft Windowsに登録されています。
	リポジトリ：https://repository.secomtrust.net/SC-Root3/	
Root CA証明書	Security Communication ECC RootCA1 証明書	Web Trust for CA基準の認定を取得したRootCA。Microsoft Windowsに登録されています。
	リポジトリ：https://repository.secomtrust.net/SC-ECC-Root1/	
Root CA証明書	SECOM Passport for Member RSA CA16 【2023年12月14日00:00以後の発行証明書が対象】	既存の中間CA証明書（PUB CA8）の有効期限切れに伴い、プライベートCA移行を目的として発行されたRootCA証明書。この証明書を持つ認証局から、サービス参加機関への証明書発行を行います。 このRootCAから発行される証明書はクライアント認証時に使用します。
	リポジトリ：https://repo1.secomtrust.net/spcpp/pfm20/index.html	
中間CA証明書	SECOM Passport for Member PUB CA8 【2020年12月25日00:00以後の発行証明書が対象】	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、サービス参加機関への証明書発行を行います。 この中間CAから発行される証明書は電子メールへの電子署名時、クライアント認証時に使用します。
	リポジトリ：https://repo1.secomtrust.net/spcpp/pfm20pub/index.html	
中間CA証明書	SECOM Passport for PublicID SMIME RSA CA 2023 【2023年8月30日00:00以後の発行証明書が対象】	S/MIME証明書のBR有効化に伴い、BR要件を満たした中間CA証明書。この証明書を持つ認証局から、サービス参加機関への証明書発行を行います。 この中間CAから発行される証明書は電子メールへの電子署名時に使用します。

	リポジトリ：https://repo1.secomtrust.net/spcpp/pfm20pub/index.html	
中間CA証明書	NII Open Domain CA - G7 RSA 【2020年12月25日00:00以後の発行証明書が対象】	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、サービス参加機関への証明書発行を行います。 この中間CA証明書およびこの中間CAから発行される証明書はSSL/TLS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/odca4/index.html	
中間CA証明書	NII Open Domain CA - G7 ECC 【2020年12月25日00:00以後の発行証明書が対象】	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、サービス参加機関への証明書発行を行います。 この中間CA証明書およびこの中間CAから発行される証明書はSSL/TLS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/odca4/index.html	
中間CA証明書	SECOM Passport for CodeSigning CA G2 【2021年5月31日00:00以前の発行証明書が対象】 【2021年5月31日00:00以後の発行証明書が対象】	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、サービス参加機関への証明書発行を行います。 この中間CAから発行される証明書はプログラムファイルへの電子署名時に使用します。
	リポジトリ：https://repo1.secomtrust.net/spcpp/pfm20pub/index.html	
中間CA証明書	NII Open DomainCA –S/MIME証明書（SHA-2認証局） 【2020年12月25日00:00以前の発行証明書が対象】	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、サービス参加機関への証明書発行を行います。 この中間CAから発行される証明書は電子メールへの電子署名時に使用します。
	リポジトリ：https://repo1.secomtrust.net/sppca/nii/odca3/index.html	
中間CA証明書	NII Open DomainCA –G4証明書（SHA-2認証局） 【2020年12月25日00:00以前の発行証明書が対象】	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、サービス参加機関への証明書発行を行います。 この中間CAから発行される証明書はクライアント認証時に使用します。 また、この中間CA証明書およびこの中間CAから発行される証明書はSSL/TLS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/odca3/index.html	

2. サーバ証明書管理手順

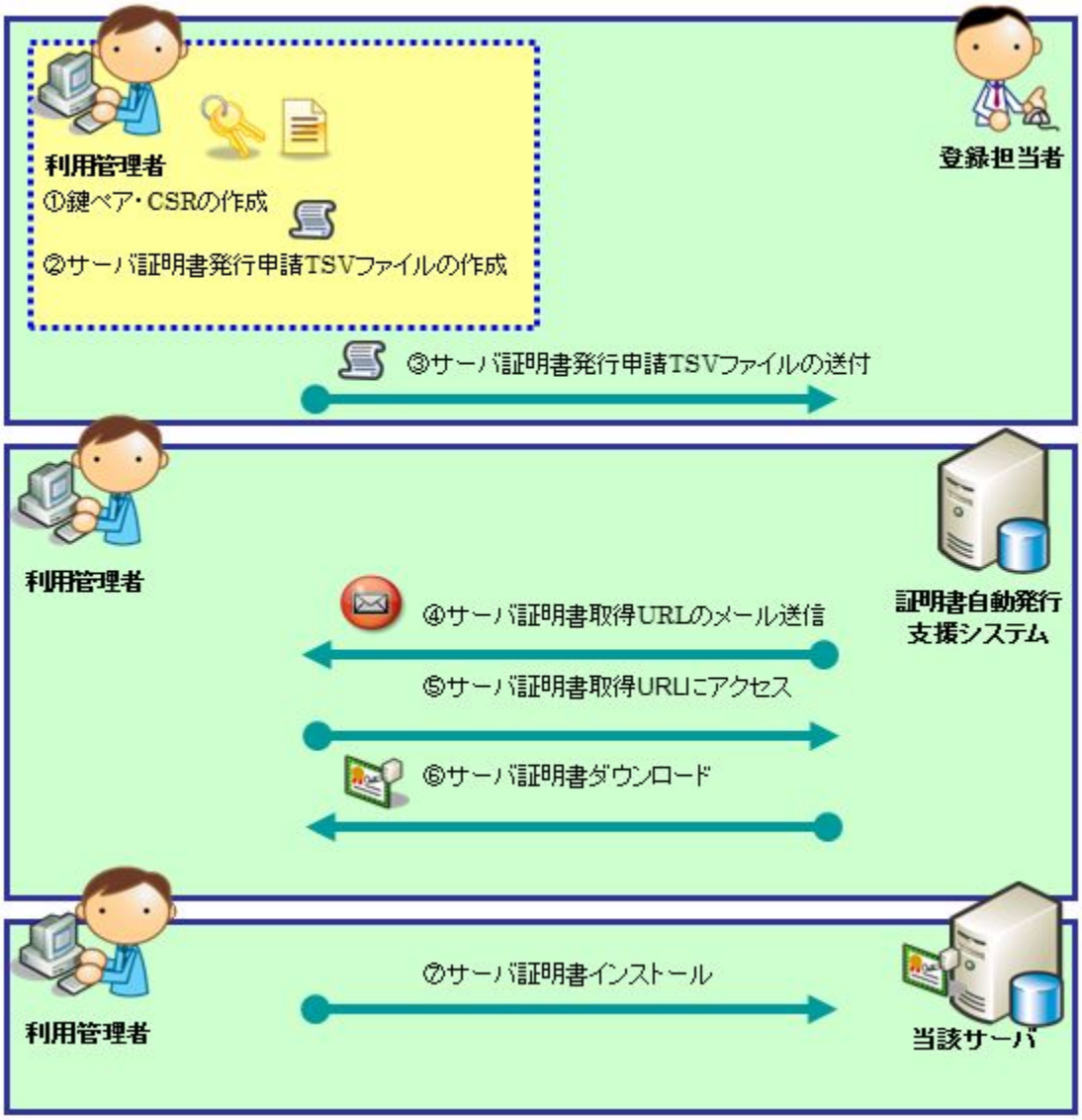
本章では利用管理者のサーバ証明書の各種手続きの流れについて記述します。
サーバ証明書の新規発行が必要な場合は「証明書新規発行」を行ってください。
既にサーバ証明書を本システムから発行していて、サーバ証明書の更新、失効された証明書の再発行を行う場合は「証明書更新発行」を行ってください。
サーバ証明書の失効を行う場合は「証明書失効」を行ってください。

手続きの種別	手続きを行う主な機会
証明書新規発行 (**2-1.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 (**2-2.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 (**2-3.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。

2-1. サーバ証明書新規発行手続き概要

本章では利用管理者のサーバ証明書新規発行手続きの流れについて記述します。
利用管理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。



サーバ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。（**2-1-1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。**（2-1-2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。**（2-1-3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。**（2-1-4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。

⑥「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。**（2-1-5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。（**2-1-6に記載**）

2-1-1. 鍵ペア・CSRの作成

「**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)	「都道府県」（ST）は利用管理者及び利用者が所属する組織の所在地の都道府県名とし、原則としてサービス窓口に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定してください。 例）ST=Tokyo	○	STとして指定できる値は下記リンクを参照してください。機関ごとに固定となります。 UPKI証明書 主体者DNにおける ST および L の値一覧 ※STおよびLが必須。（2020年12月22日以降）
Locality Name(L)	「場所」（L）は利用管理者及び利用者が所属する組織の所在地の市区町村名とし、原則としてサービス窓口に事前に届出したとおりの所在地の市区町村名をローマ字表記で指定してください。 例)L=Chiyoda-ku	○	Lとして指定できる値は下記リンクを参照してください。機関ごとに固定となります。 UPKI証明書 主体者DNにおける ST および L の値一覧 ※STおよびLが必須。（2020年12月22日以降）
Organization Name(O)	サービス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)
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にはサービス利用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 ECDSA 384bit			

○・・・必須　×・・・入力不可　△・・・省略可

主体者DNの順序について

主体者DNの各項目について，CSR中に現れる順序が

C=…… → ST=…… →L=…… → O=…… → (OU=……) → CN=……

もしくはその逆順となるようにCSRを生成してください。
例えば，OとOUが入れ替わっているものは受理されません。

2-1-2. 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。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
サーバ証明書発行申請TSVファイルのフォーマットは「5-3-1. サーバ証明書発行申請TSVファイル形式」をご確認ください。

2-1-3. サーバ証明書発行申請TSVファイルの送付

「2-1-2. 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。

2-1-4. 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サーバ証明書取得URLがメールにて通知されます。メール本文に記載されたサーバ証明書取得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。

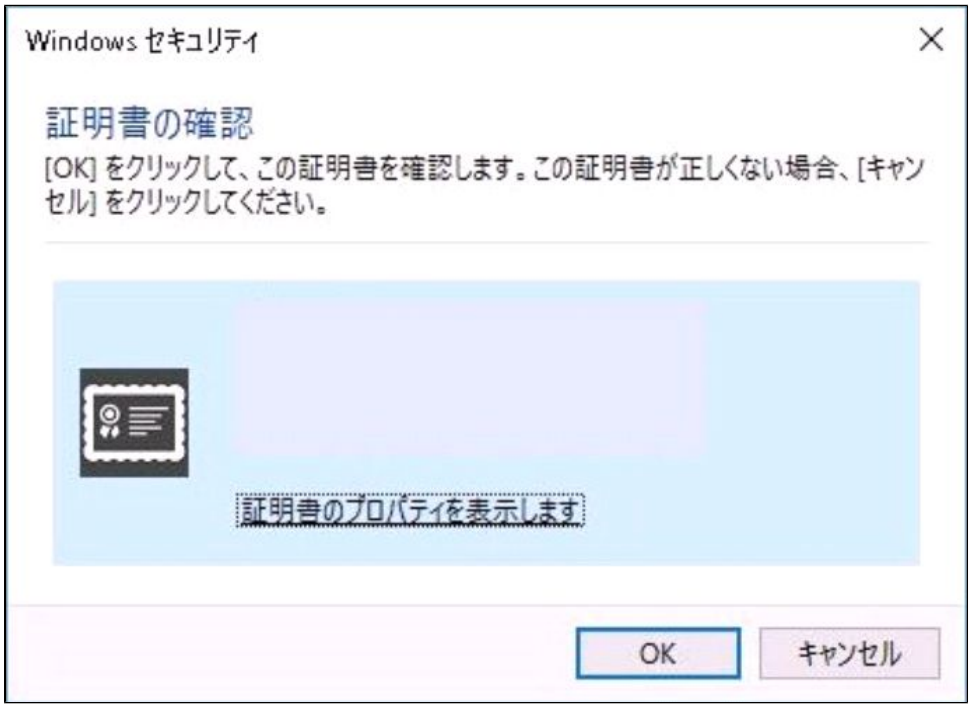
サーバ証明書取得URLの通知
【件名】 サーバ証明書発行受付通知 ・・・・・ **#以下に証明書の取得先が記述されています。** 貴機関の登録担当者経由で発行申請をいただきましたサーバ証明書を配付いたします。 本日から1ヶ月以内に以下の証明書取得URLへアクセスし、サーバ証明書の取得を行ってください。 **証明書取得URL：**https://scia.secomtrust.net/～　　**←左記URLにアクセスし証明書の取得を行ってください。** ・・・・・

2-1-5. サーバ証明書の取得

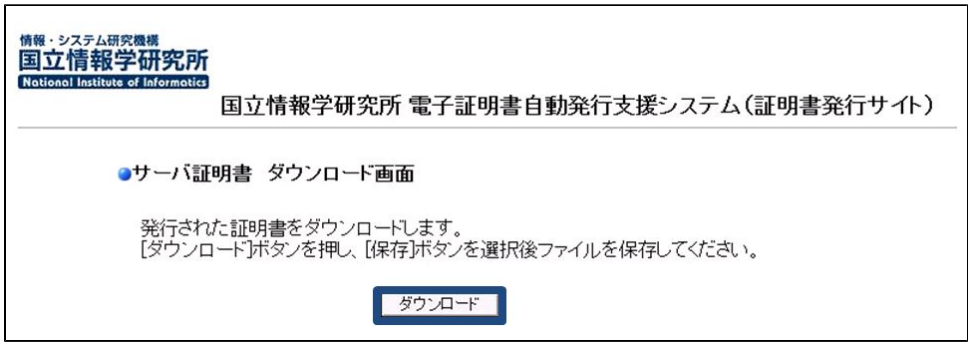
「2-1-4. 証明書取得URLの通知」で通知されたURLにアクセスしサーバ証明書を取得する方法を記述します。

サーバ証明書の取得

1．「2-1-4. 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。



2-1-6. サーバ証明書のインストール

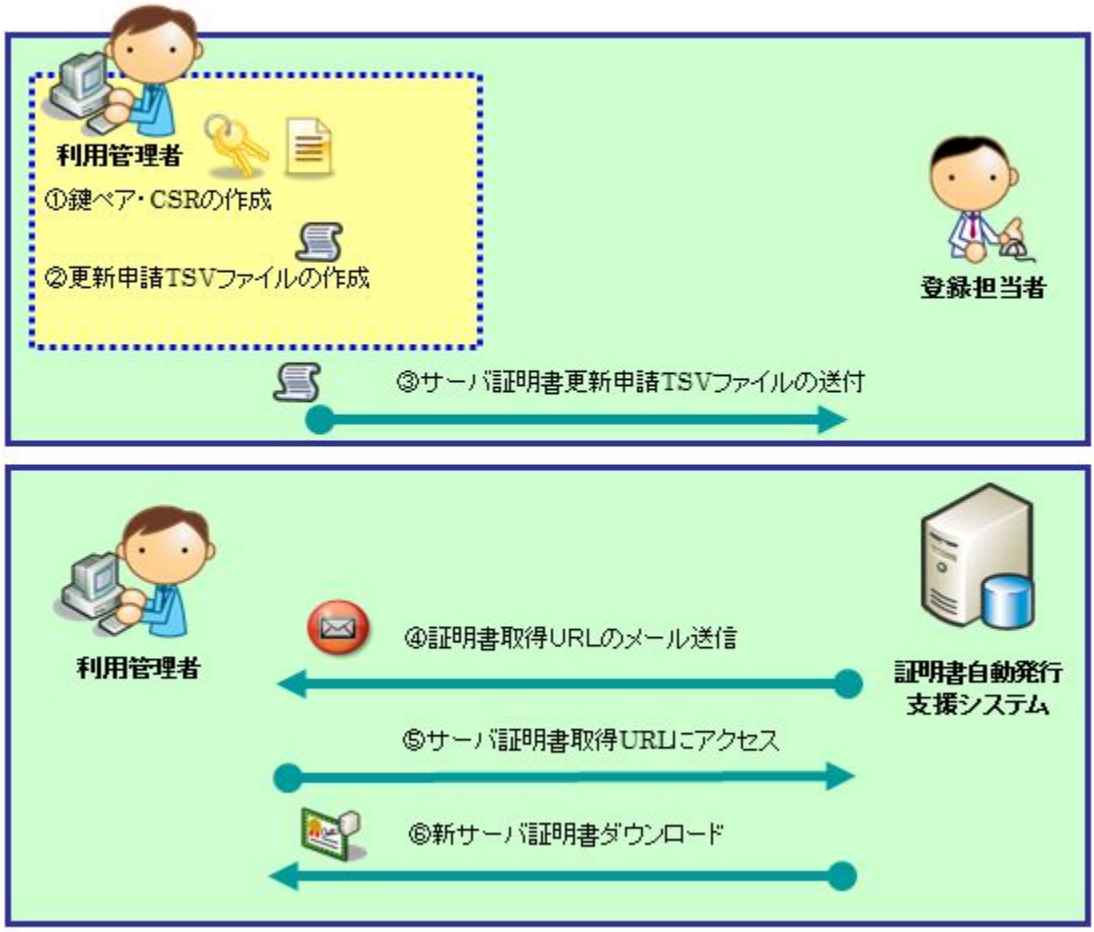
「2-1-5. サーバ証明書の取得」で取得したサーバ証明書を、対象のサーバにインストールしてください。サーバのインストール方法につきましては、当該のサーバのマニュアルをご確認ください。
また、サービスでは、以下のサーバに関して「サーバ証明書インストールマニュアル」を用意しておりますので、あわせてご確認ください。

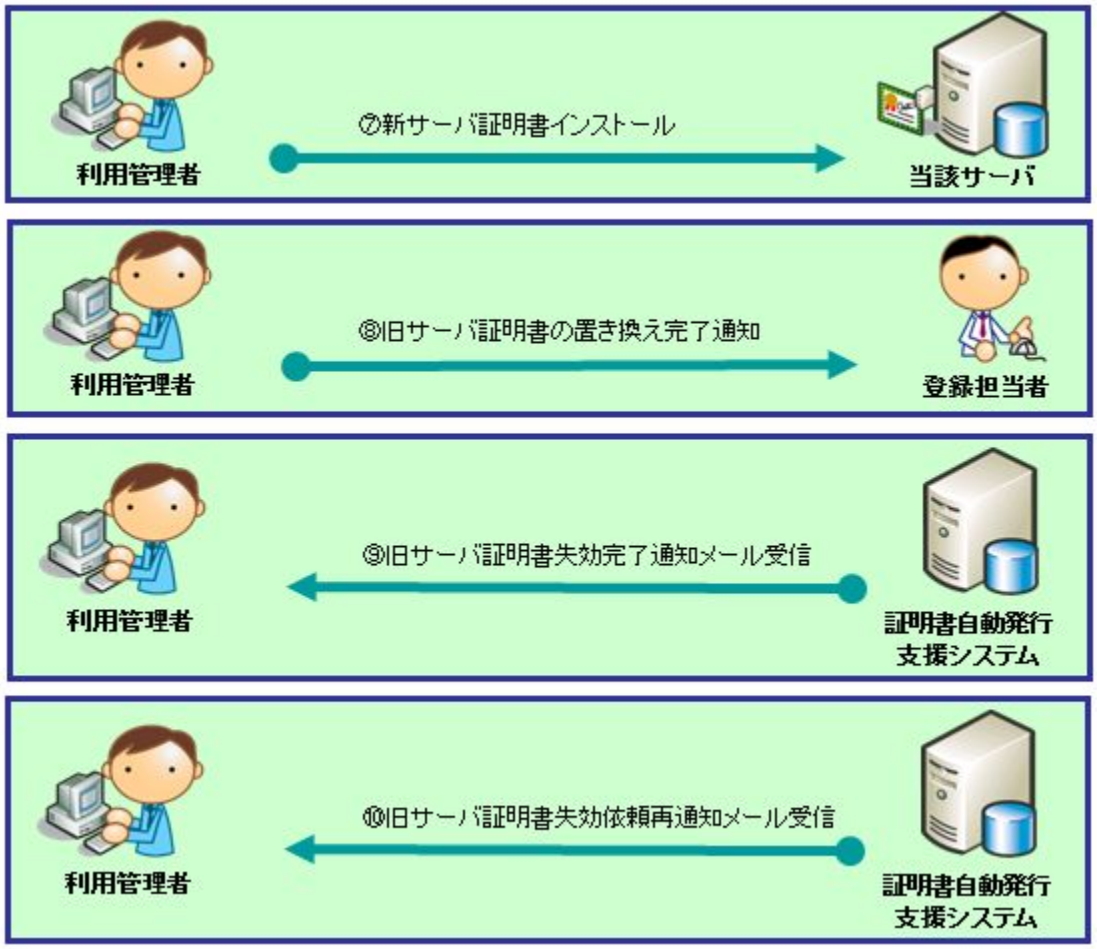
- **Apache系**
  - Apache(mod_SSL)
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル Apache(mod_ssl)編
- **IIS系**
  - IIS8.0
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル IIS8.0・IIS8.5編
  - IIS8.5
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル IIS8.0・IIS8.5編
  - IIS10.0
    ドキュメント名：証明書自動発行支援システムサーバ証明書インストールマニュアル IIS10.0編
- **Tomcat系**
  - Tomcat
    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編
- **IBM HTTP Server**

    - IBM HTTP Server
      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
- **Nginx系**
    - Nginx
      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 Nginx編
- **OpenLDAP系**
    - OpenLDAP
      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 OpenLDAP編

2-2. サーバ証明書更新申請手続き概要

本章では利用管理者のサーバ証明書更新発行手続きの流れについて記述します。
利用管理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。





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。（**2-2-1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。**（2-2-2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。**（2-2-3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。**（2-2-4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。
⑥「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。**（2-2-5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。（**2-2-6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。**(2-2-7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。**(2-2-8に記載)**
【旧サーバ証明書の失効を行わないと・・・】
⑩⑥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利用管理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。**(2-2-9に記載)**

2-2-1. 鍵ペア・CSRの作成

「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、「2-1-1. 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。

2-2-2. 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。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
更新申請TSVファイルのフォーマットは「5-3-2. サーバ証明書更新申請TSVファイル形式」をご確認ください。

2-2-3. 更新申請TSVファイルの送付

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

2-2-4. 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サーバ証明書取得URLがメールにて通知されます。
メール本文に記載されたサーバ証明書取得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。

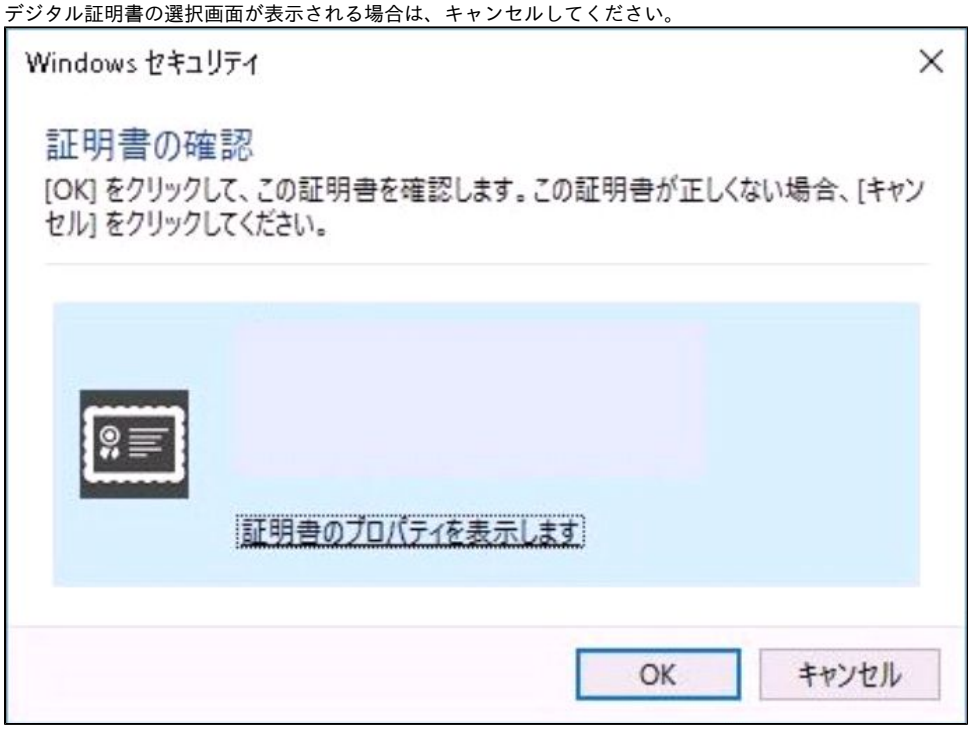
サーバ証明書取得URLの通知
【件名】 サーバ証明書発行受付通知 ・・・・・ **#以下に証明書の取得先が記述されています。** 貴機関の登録担当者経由で発行申請をいただきましたサーバ証明書を配付いたします。 本日から1ヶ月以内に以下の証明書取得URLへアクセスし、サーバ証明書の取得を行ってください。 **証明書取得URL：**https://scia.secomtrust.net/〜　　**←左記URLにアクセスし新サーバ証明書の取得を行ってください。** ・・・・・

2-2-5. 新サーバ証明書の取得

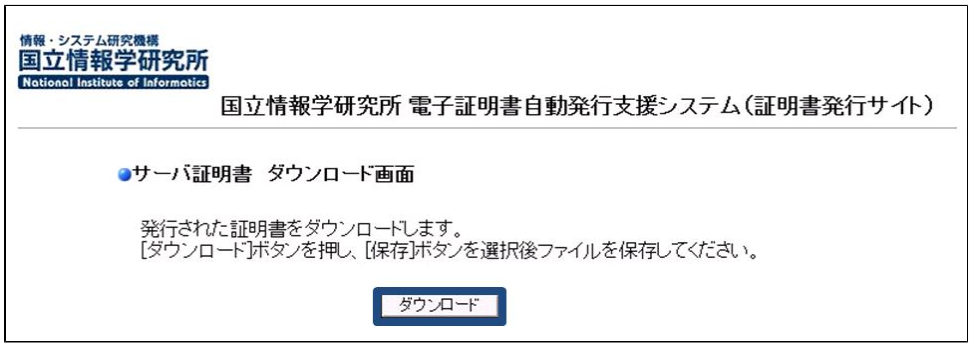
「2-2-4. サーバ証明書取得URLの通知」で通知されたURLにアクセスし新サーバ証明書を取得する方法を記述します。

サーバ証明書の取得

1．「2-2-4.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。



2-2-6. サーバ証明書のインストール

「2-2-5. 新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、「2-1-6. サーバ証明書のインストール」で記載した「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。

2-2-7. 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。

2-2-8. 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】
サーバ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

・・・・・

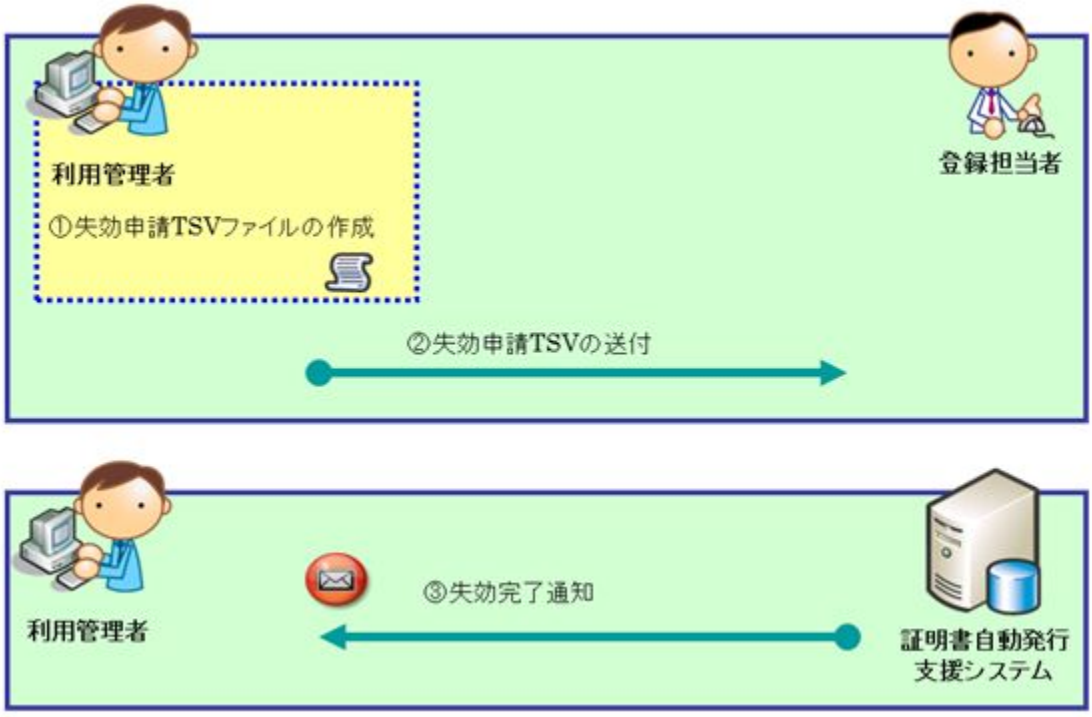
2-2-9. 旧サーバ証明書の失効申請依頼再通知について

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】 サーバ用証明書更新(旧証明書の失効申請)再通知   利用管理者の方が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 ・・・・・

2-3. サーバ証明書失効申請手続き概要

本章では利用管理者のサーバ証明書失効手続きの流れについて記述します。
利用管理者は以下の手続きによりサーバ証明書の失効を行います。



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。 **（2-3-1に記載）**
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。 **（2-3-2に記載）**
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。 **（2-3-3に記載）**

2-3-1. 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。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
失効申請TSVファイルのフォーマットは「5-3-3. サーバ証明書失効申請TSVファイル形式」をご確認ください。

2-3-2. 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。

2-3-3. 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】 サーバ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. クライアント証明書管理手順

本章では利用管理者のクライアント証明書の各種手続きの流れについて記述します。
クライアント証明書の新規発行が必要な場合は「証明書新規発行」を行ってください。
既にクライアント証明書を本システムから発行していて、クライアント証明書の更新、失効された証明書の再発行を行う場合は「証明書更新発行」を行ってください。
クライアント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 (**3-2.クライアント証明書新規発行**)	新規にクライアント証明書の発行を必要とする場合。
	クライアント証明書の記載内容（主体者DN）を変更する場合。
証明書更新発行 (**3-3.クライアント証明書更新発行**)	クライアント証明書の記載内容(主体者DN以外)を変更する場合。
	クライアント証明書を継続利用したい場合。
	失効されたクライアント証明書の再発行を行う場合。
証明書失効 (**3-4.クライアント証明書失効**)	クライアント証明書が不要になった場合や秘密鍵が危殆化した場合。

3-1. 証明書ダウンロード方法ごとの操作手順

証明書新規発行、証明書更新発行の手続きで使用する発行申請TSVファイルを作成するときに以下の証明書ダウンロード方法を選択してください。

証明書ダウンロード種別	手続きを行う主な機会
P12個別	証明書の発行、更新、失効をP12個別ダウンロード方法で申請を行う場合。
P12一括	証明書の発行、更新、失効をP12一括ダウンロード方法で申請を行う場合。
ブラウザ発行	証明書の発行、更新、失効をブラウザ発行のダウンロード方法で申請を行う場合。

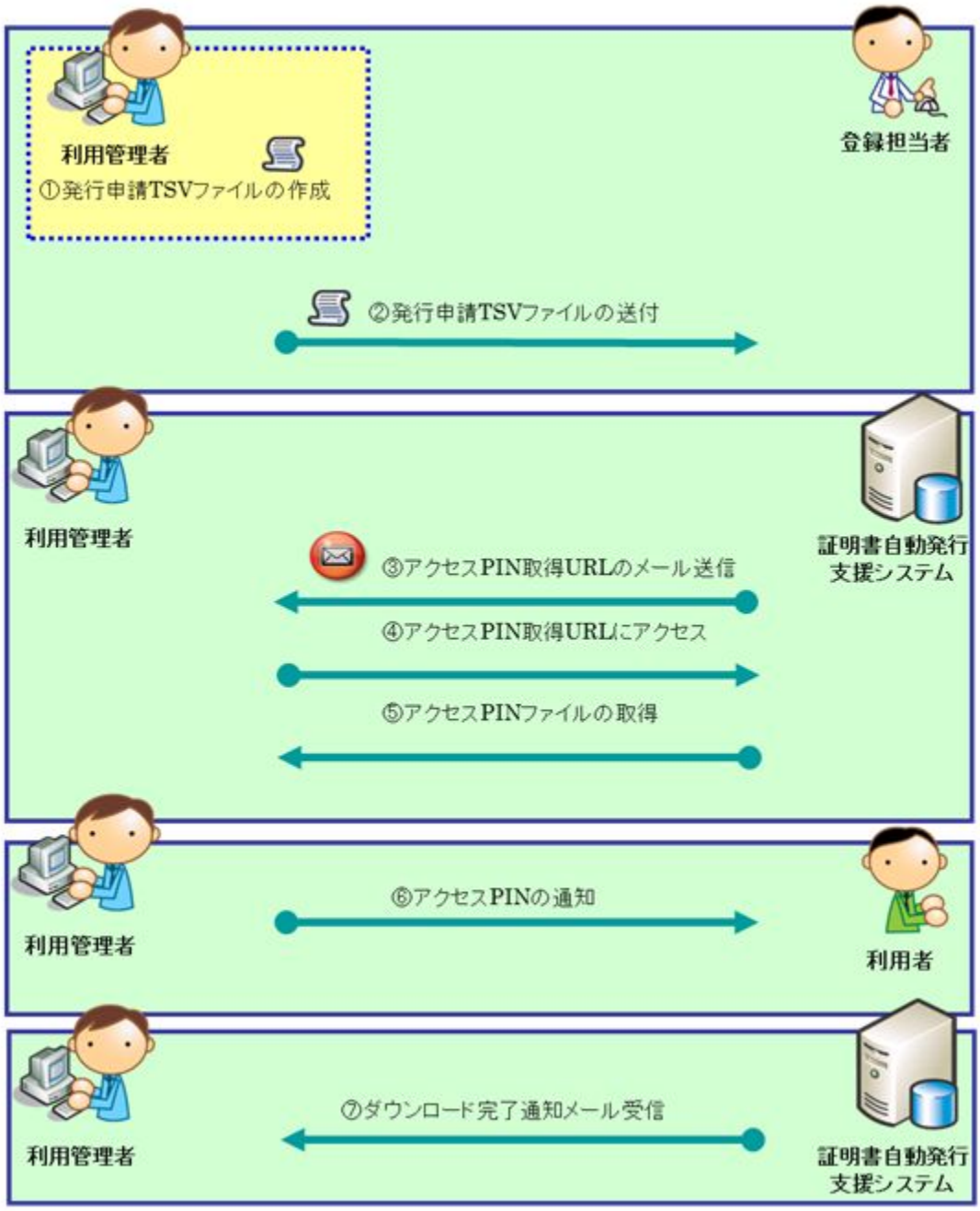
1つの発行申請TSVファイルに複数の証明書ダウンロード種別を選択することはできません。証明書ダウンロード種別ごとに発行申請TSVファイルを分けて作成してください。

3-2. クライアント証明書新規発行手続き概要

本章ではクライアント証明書新規発行手続きの流れについて記述します。
証明書ダウンロード種別ごとに記述します。

3-2-1. クライアント証明書新規発行（P12個別）

証明書の発行をP12個別ダウンロード方法で申請を行う場合について記述します。



クライアント証明書発行（P12個別）手続き概要
①クライアント証明書の発行申請を行うための証明書発行申請TSVを作成してください。**（3-2-1-1に記載）**
②決められた手続きに従い、登録担当者へクライアント証明書発行申請TSVを送付してください。**（3-2-1-2に記載）**
③登録担当者がクライアント証明書発行申請TSVを本システムにアップロードすると、本システムより、メールでアクセスPIN取得URLを送信します。**（3-2-1-3に記載）**
④メールを受信したら、アクセスPIN取得URLにアクセスしてください。
⑤「アクセスPINダウンロード画面」が開きますので、アクセスPINを取得してください。**（3-2-1-4に記載）**
⑥取得したアクセスPINを利用者へ通知してください。（**3-2-1-5に記載**）
⑦利用者がクライアント証明書のダウンロードを行うと、本システムより、ダウンロード完了通知が送信されます。**(3-2-1-6に記載)**

3-2-1-1. 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証明書発行申請TSVファイルを作成してください。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
発行申請TSVファイルのフォーマットは「5-4-1. クライアント証明書発行申請TSVファイル形式」をご確認ください。

3-2-1-2. 発行申請TSVファイルの送付

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

3-2-1-3. アクセスPIN取得URLの通知

クライアント証明書の発行が完了すると、本システムよりアクセスPINを取得するためのアクセスPIN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アクセスPIN取得URLにアクセスし、アクセスPINの取得を実施してください。

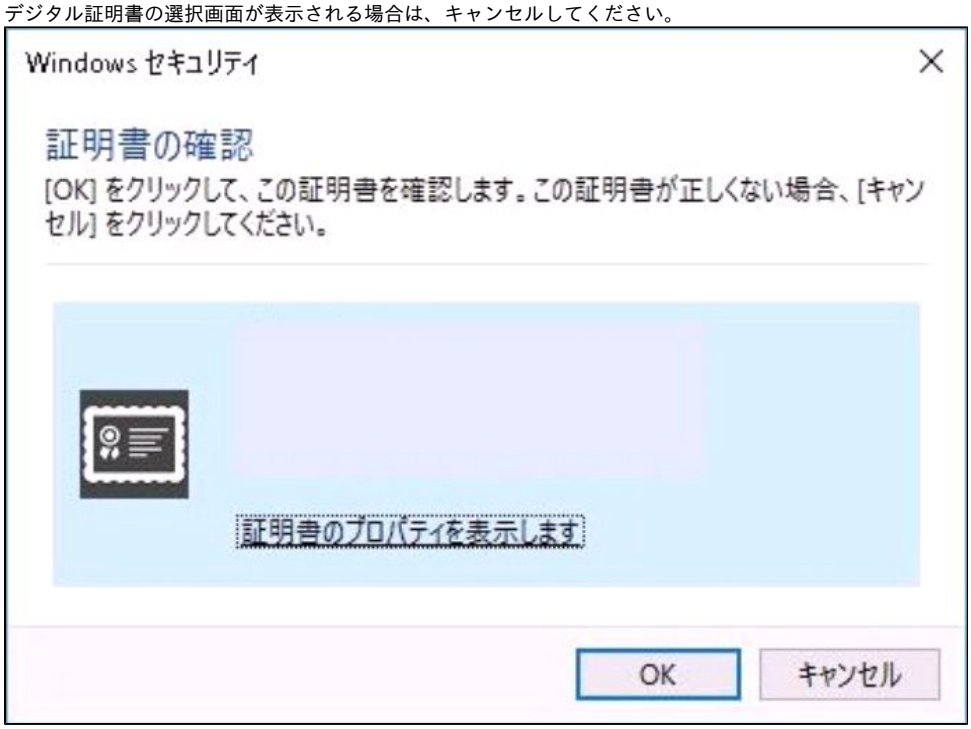
アクセスPIN取得URLの通知
【件名】 アクセスPIN発行通知 ・・・・・ **#以下に証明書の取得先が記述されています。** 貴機関の登録担当者経由で発行申請をいただきました証明書のアクセスPINを配付いたします。 本日から１ヶ月以内に以下のアクセスPIN取得URLへアクセスし、アクセスPINの取得を行ってください。 **アクセスPIN取得URL：**https://scia.secomtrust.net/～　　**←左記URLにアクセスしアクセスPINの取得を行ってください。** ・・・・・

3-2-1-4. アクセスPINの取得

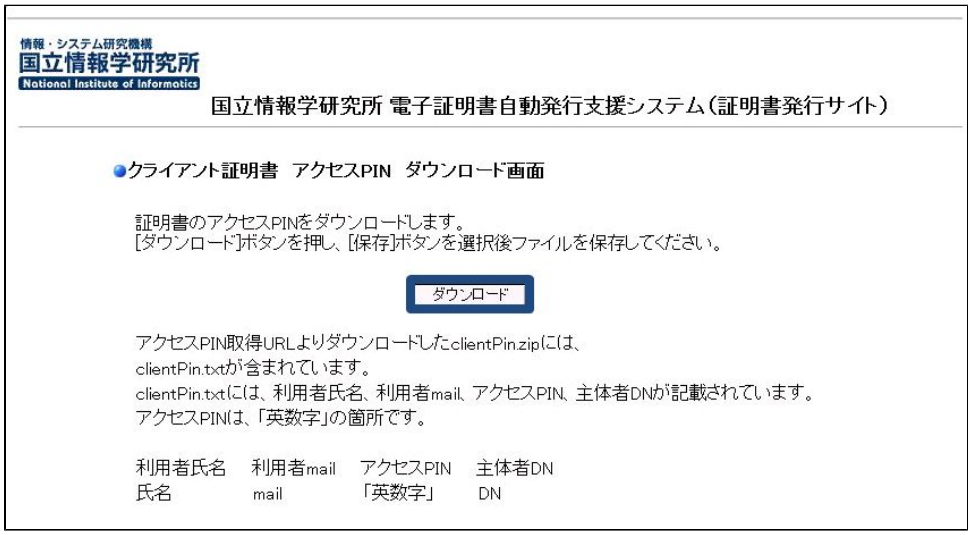
「3-2-1-3. アクセスPIN取得URLの通知」で通知されたURLにアクセスし、アクセスPIN証明書を取得する方法を記述します。

アクセスPINの取得

1. 「3-2-1-3アクセスPIN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、clientPin.zipファイルが取得できますので保存してください。



3. clientPin.zipファイルを解凍し、アクセスPINを利用者へ配付してください。

3-2-1-5. アクセスPINの通知

利用管理者は利用者に対してアクセスPINを通知してください。

3-2-1-6. ダウンロード完了通知メール受信

クライアント証明書利用者がクライアント証明書のダウンロードを行った場合、本システムより、ダウンロードが完了したことを通知するメールが自動送信されます。このメールは、電子署名されています。

クライアント証明書ダウンロード完了通知メール

【件名】
クライアント証明書取得通知

【本文】・・・・・
貴機関利用者の方がクライアント証明書の取得を完了致しましたので、下記の通り連絡をさせていただきます。

【対象証明書DN】

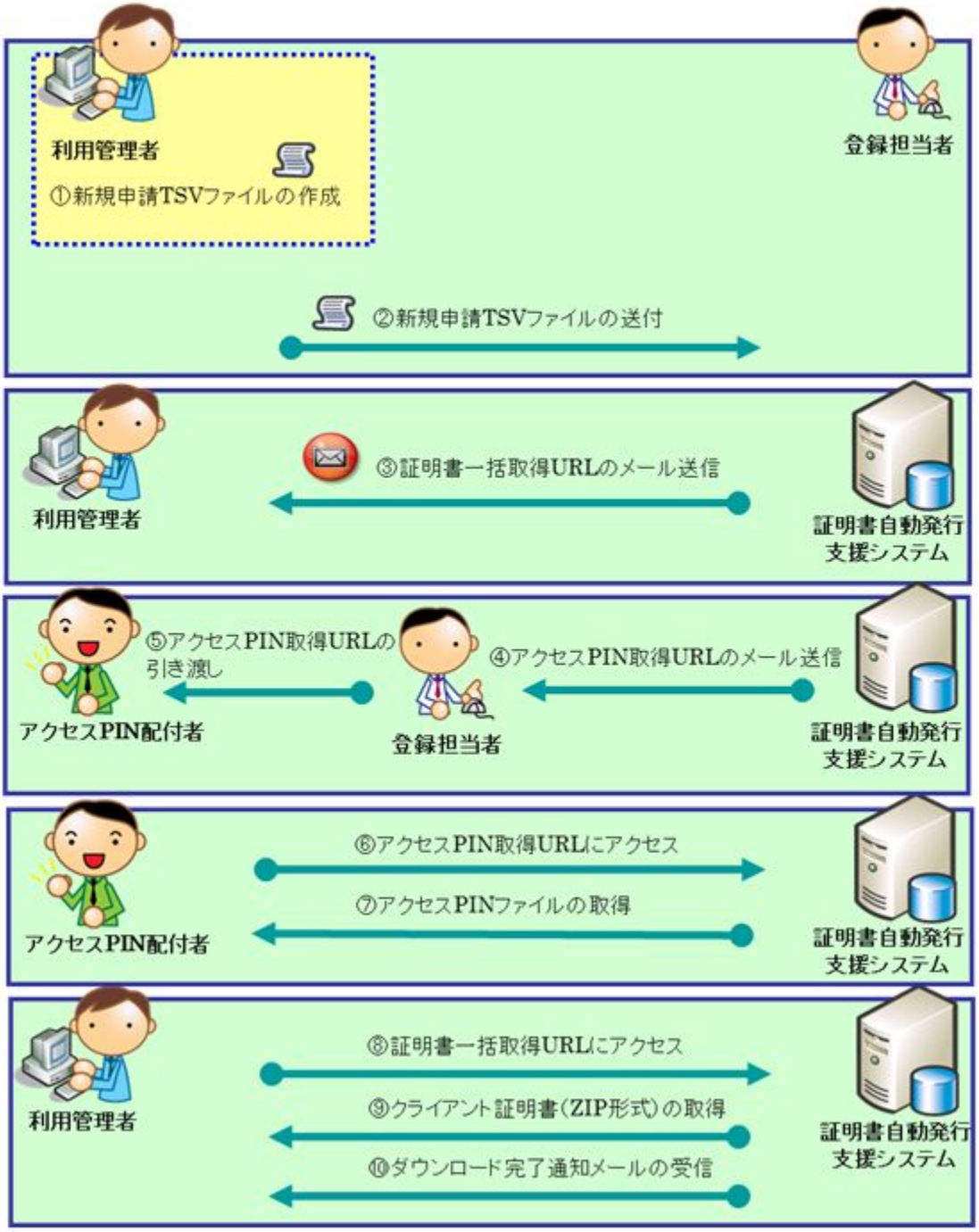
CN=KOKURITSU HANAKO
OU=XXXXXX（学生番号等）
OU=Cyber Science
Infrastructure Development Department,
O=National Institute of Informatics,
L=Chiyoda-ku,
ST=Tokyo
C=JP

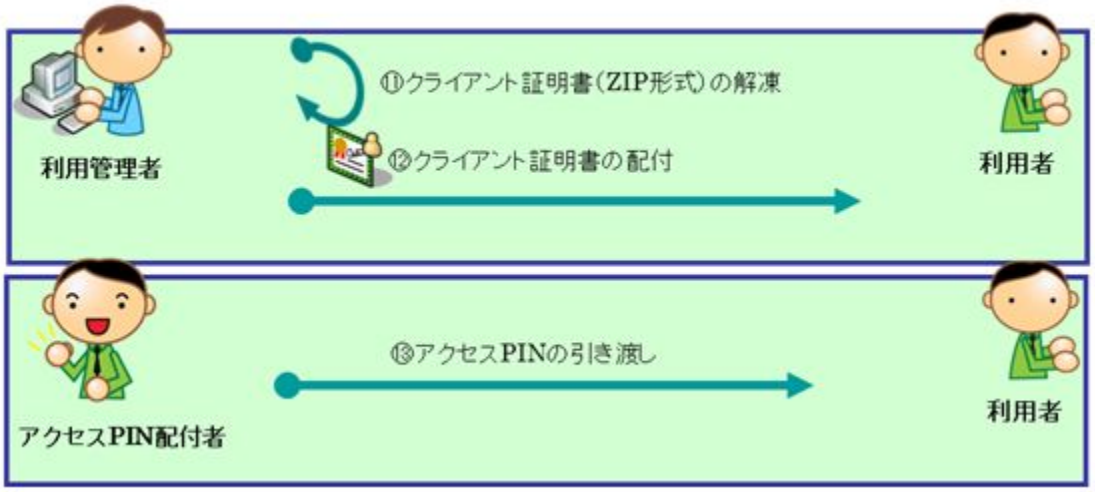
【対象証明書シリアル番号】

・・・・・

3-2-2. クライアント証明書新規発行（P12一括）

証明書の発行をP12一括ダウンロード方法で申請を行う場合について記述します。





クライアント証明書発行（P12一括）手続き概要
①クライアント証明書の発行申請を行うための証明書発行申請TSVを作成してください。**（3-2-2-1に記載）**
②決められた手続きに従い、登録担当者へクライアント証明書発行申請TSVを送付してください。**（3-2-2-2に記載）**
③登録担当者がクライアント証明書発行申請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を送信します。**（3-2-2-3に記載）**
④登録担当者へアクセスPIN取得URLが送信されます。**（3-2-2-4に記載）**
⑤アクセスPIN配付者へアクセスPIN取得URLを引き渡してください。
⑥アクセスPIN取得URLにアクセスします。
⑦「アクセスPINダウンロード画面」が開きますので、.clientAllPin.zipを取得してください。取得したclientAllPin.zipを解凍してください。**（3-2-2-5に記載）**
⑧アクセスPIN配付者がアクセスPINファイルを取得後、証明書取得URLにアクセスしてください。**(3-2-2-6記載)**
⑨「証明書ダウンロード画面」が開きますので、clientAll.zipを取得してください。
⑩利用管理者がクライアント証明書のダウンロードを行うと、本システムより、ダウンロード完了通知が送信されます。**(3-2-2-7に記載)**
⑪取得したclientAll.zipを解凍してください。
⑫利用者へ証明書P12ファイルを配付してください。
⑬アクセスPIN配付者は利用者へアクセスPINを引き渡してください。**(3-2-2-8に記載)**

3-2-2-1. 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証明書発行申請TSVファイルを作成してください。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
発行申請TSVファイルのフォーマットは「5-4-1. クライアント証明書発行申請TSVファイル形式」をご確認ください。

3-2-2-2. 発行申請TSVファイルの送付

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

3-2-2-3. 証明書取得URLの通知

クライアント証明書の発行が完了すると、本システムより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。

クライアント証明書取得URLの通知

【件名】
クライアント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クライアント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、クライアント証明書の取得を行ってください。。
証明書取得URL：https://scia.secomtrust.net/**～**

・・・・・

3-2-2-4. アクセスPIN取得URLの通知

登録担当者へアクセスPIN取得URLがメールにて通知されます。登録担当者はアクセスPIN配付者へアクセスPIN取得URLを引き渡してください。

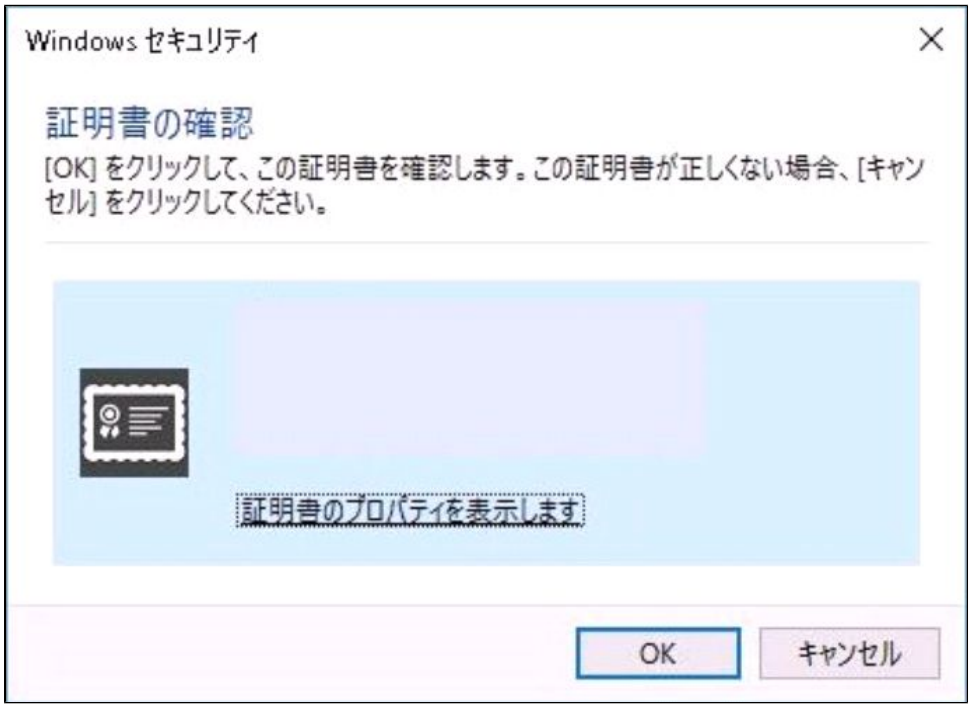
アクセスPIN取得URLの通知
【件名】 アクセスPIN発行通知 ・・・・・ **#以下に証明書の取得先が記述されています。** 貴機関の登録担当者経由で発行申請をいただきました証明書のアクセスPINを配付いたします。 本日から１ヶ月以内に以下のアクセスPIN取得URLへアクセスし、アクセスPINの取得を行ってください。 **アクセス取得URL：**https://scia.secomtrust.net/**～** ・・・・・

3-2-2-5. アクセスPINの取得

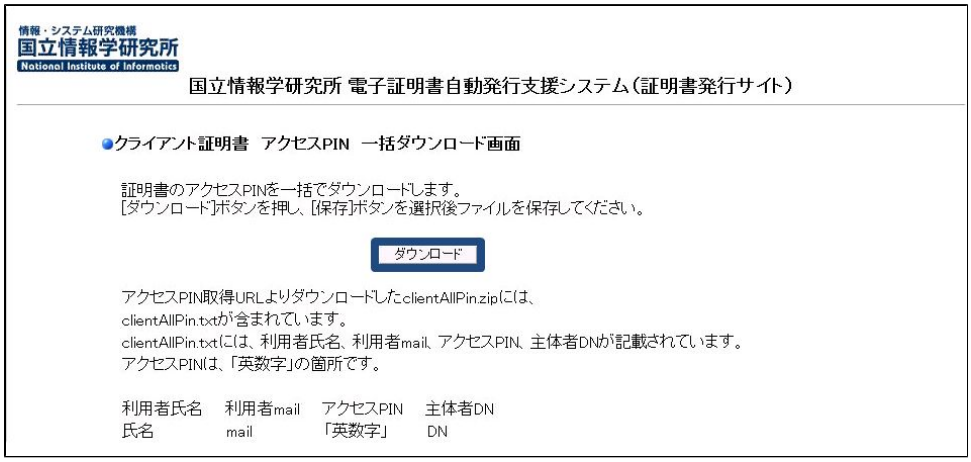
「3-2-2-4. アクセスPIN取得URLの通知」で通知されたURLにアクセスし、アクセスPIN証明書を取得する方法を記述します。

アクセスPINの取得

1．「3-2-2-4. アクセスPIN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、clientAllPin.zipファイルが取得できますので保存してください。



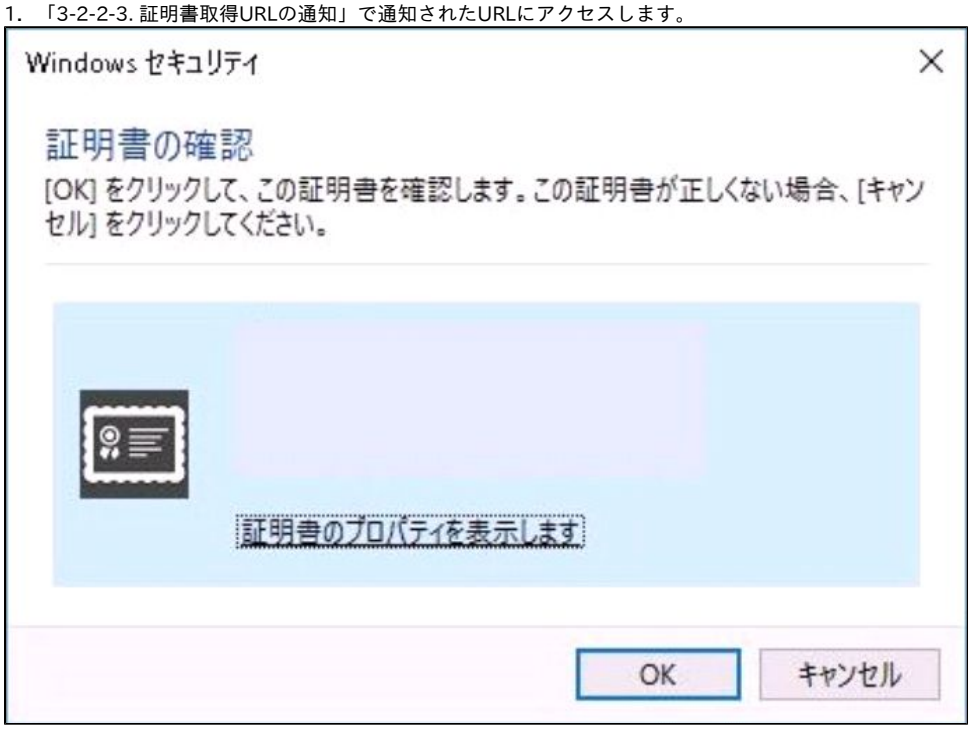
3．clientAllPin.zipファイルを解凍してください。

3-2-2-6. クライアント証明書の取得

「3-2-2-3. 証明書取得URLの通知」で通知されたURLにアクセスし、証明書を取得する方法を記述します。

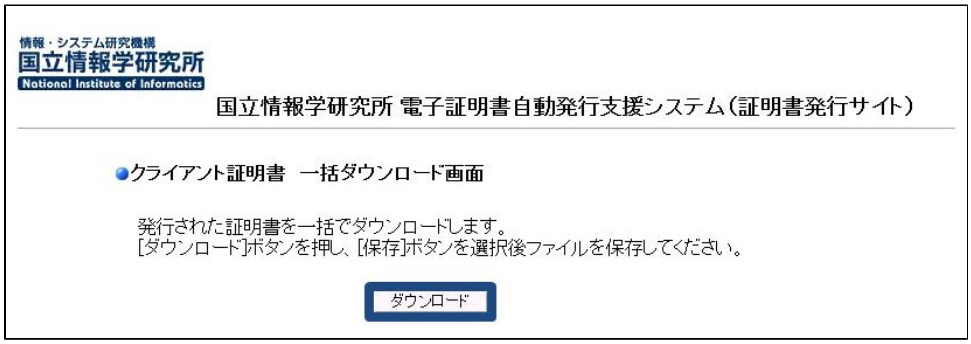
クライアント証明書の取得

1. 「3-2-2-3. 証明書取得URLの通知」で通知されたURLにアクセスします。



※証明書取得URLにアクセスする前に、アクセスPIN配布者がアクセスPINを取得しておく必要があります。 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、clientAll.zipファイルが取得できますので保存してください。



3. clientAll.zipファイルを解凍し、証明書を利用者へ配付してください。

3-2-2-7. ダウンロード完了通知メール受信

利用管理者がクライアント証明書のダウンロードを行った場合、本システムより、ダウンロードが完了したことを通知するメールが自動送信されます。
このメールは、電子署名されています。

証明書ダウンロード完了通知メール

【件名】
クライアント証明書取得通知

【本文】・・・・・
貴機関利用者の方がクライアント証明書の取得を完了致しましたので、下記の通り連絡をさせていただきます。

【対象証明書DN】

CN=KOKURITSU HANAKO
OU=XXXXXX（学生番号等）
OU=Cyber Science
Infrastructure Development Department,
O=National Institute of Informatics,
L=Chiyoda-ku,
ST=Tokyo
C=JP

【対象証明書シリアル番号】

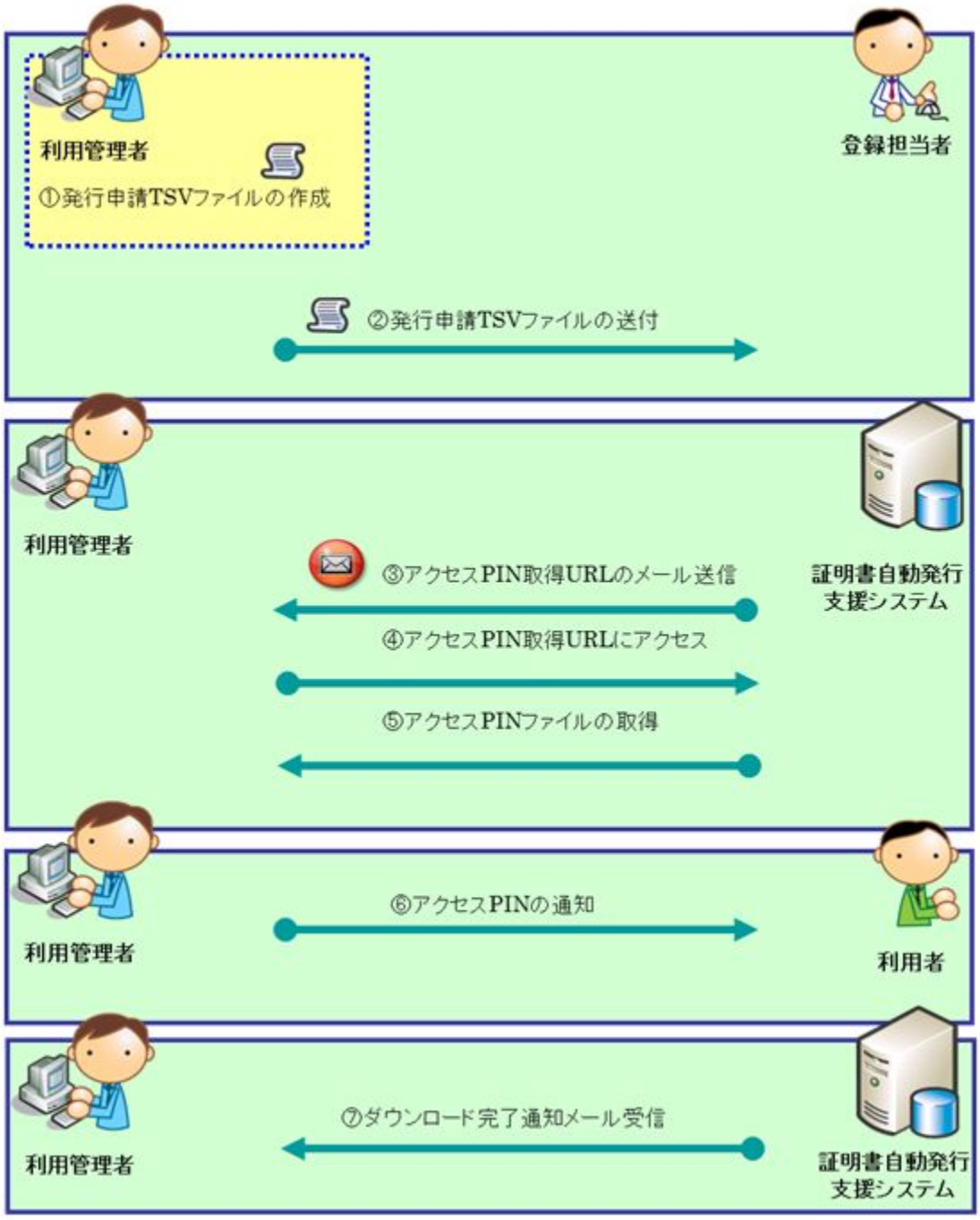
・・・・・

3-2-2-8. アクセスPINの引き渡し

アクセスPIN配付者は利用者へ「3-2-2-5. アクセスPINの取得」で取得したアクセスPINを引き渡してください。

3-2-3. クライアント証明書新規発行（ブラウザ）

証明書の発行をブラウザダウンロード方法で申請を行う場合について記述します。



クライアント証明書発行（ブラウザ）手続き概要

①クライアント証明書の発行申請を行うための証明書発行申請TSVを作成してください。 **（3-2-3-1に記載）**

②決められた手続きに従い、登録担当者へクライアント証明書発行申請TSVを送付してください。 **（3-2-3-2に記載）**

③登録担当者がクライアント証明書発行申請TSVを本システムにアップロードすると、本システムより、メールでアクセスPIN取得URLを送信します。 **（3-2-3-3に記載）**

④メールを受信したら、アクセスPIN取得URLにアクセスしてください。

⑤「アクセスPINダウンロード画面」が開きますので、アクセスPINを取得してください。 **（3-2-3-4に記載）**

⑥取得したアクセスPINを利用者へ通知してください。

⑦利用者がクライアント証明書のダウンロードを行うと、本システムより、ダウンロード完了通知が送信されます。**(3-2-3-5に記載)**

3-2-3-1. 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証明書発行申請TSVファイルを作成してください。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
発行申請TSVファイルのフォーマットは「5-4-1. クライアント証明書発行申請TSVファイル形式」をご確認ください。

3-2-3-2. 発行申請TSVファイルの送付

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

3-2-3-3. アクセスPIN取得URLの通知

クライアント証明書の発行が完了すると、本システムよりアクセスPINを取得するためのアクセスPIN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アクセスPIN取得URLにアクセスし、アクセスPINの取得を実施してください。

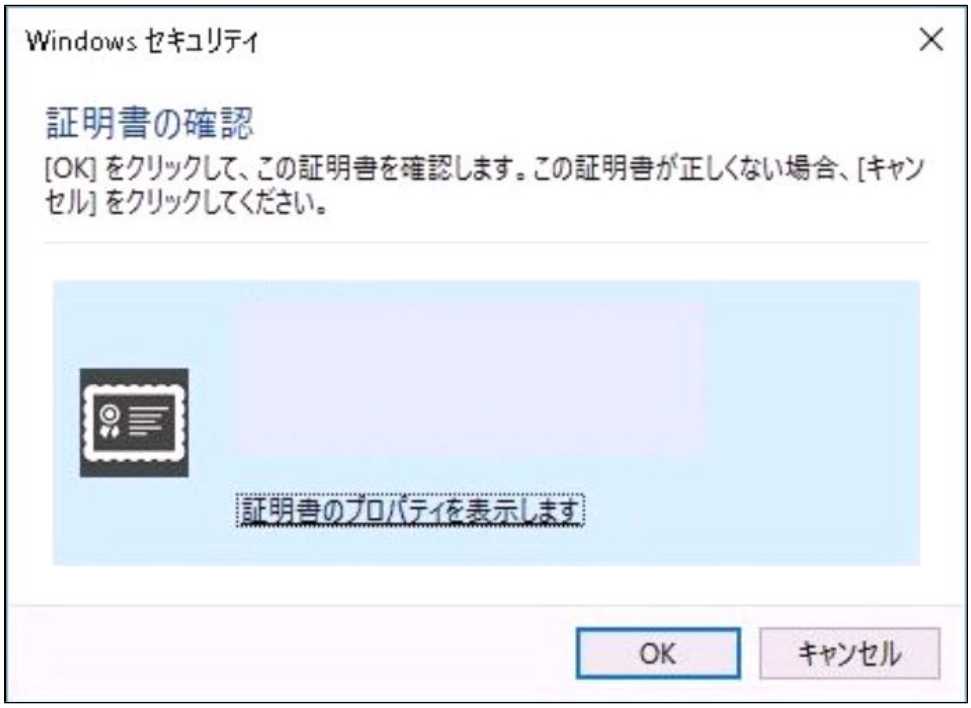
アクセスPIN取得URLの通知
【件名】 アクセスPIN発行通知 ・・・・・ **#以下に証明書の取得先が記述されています。** 貴機関の登録担当者経由で発行申請をいただきました証明書のアクセスPINを配付いたします。 本日から１ヶ月以内に以下のアクセスPIN取得URLへアクセスし、アクセスPINの取得を行ってください。 **アクセスPIN取得URL：**https://scia.secomtrust.net/～　　**←左記URLにアクセスしアクセスPINの取得を行ってください。** ・・・・・

3-2-3-4. アクセスPINの取得

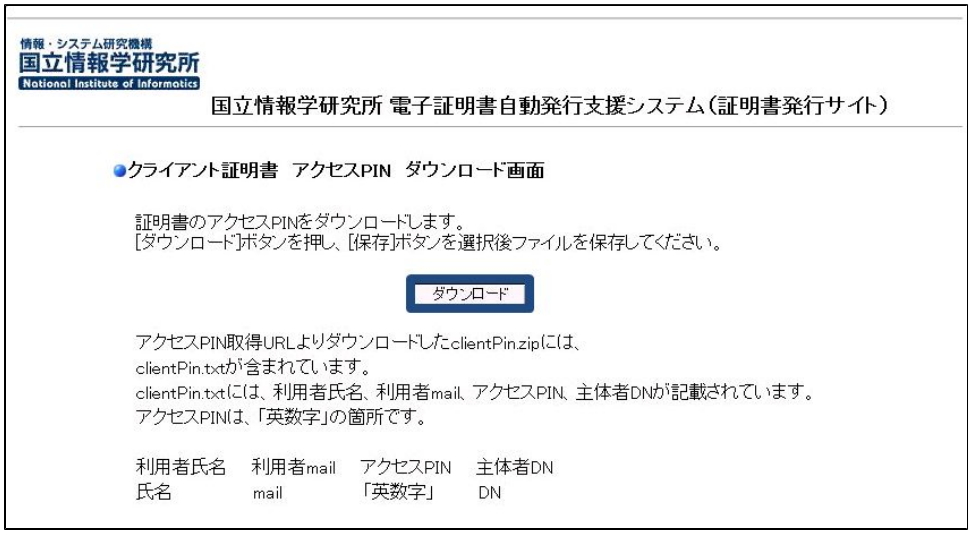
「3-2-3-3. アクセスPIN取得URLの通知」で通知されたURLにアクセスし、アクセスPIN証明書を取得する方法を記述します。

アクセスPINの取得

1. 「3-2-3-3. アクセスPIN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、clientPin.zipファイルが取得できますので保存してください。



3. clientPin.zipファイルを解凍し、アクセスPINを利用者へ配付してください。

3-2-3-5. ダウンロード完了通知メール受信

クライアント証明書新規発行依頼者である利用者がクライアント証明書のダウンロードを行った場合、本システムより、ダウンロードが完了したことを通知するメールが自動送信されます。このメールは、電子署名されています。

クライアント証明書ダウンロード完了通知メール

【件名】
クライアント証明書取得通知

【本文】

・・・・・
貴機関利用者の方がクライアント証明書の取得を完了致しましたので、

下記の通り連絡をさせていただきます。

【対象証明書DN】

CN=KOKURITSU HANAKO
OU=XXXXXX（学生番号等）
OU=Cyber Science
Infrastructure Development Department,
O=National Institute of Informatics,
L=Chiyoda-ku,
ST=Tokyo
C=JP

【対象証明書シリアル番号】

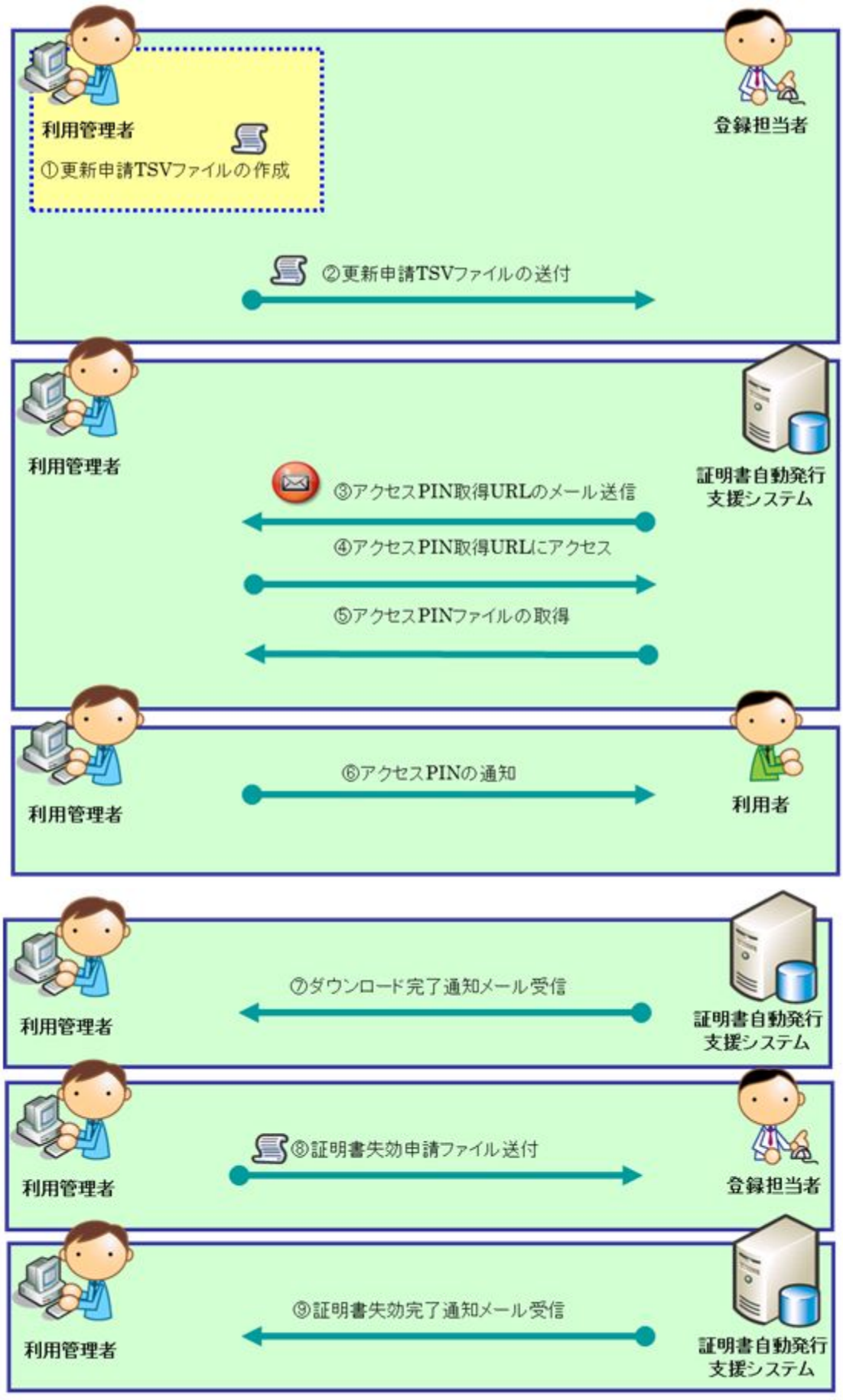
・・・・・

3-3. クライアント証明書更新発行手続き概要

本章ではクライアント証明書更新発行手続きの流れについて記述します。
以下の手続きにより証明書の新規申請・取得を行います。
証明書ダウンロード種別ごとに記述します。

3-3-1. クライアント証明書更新発行（P12個別）

証明書の更新をP12個別ダウンロード方法で申請を行う場合について記述します。


利用管理者
①更新申請TSVファイルの作成
登録担当者
②更新申請TSVファイルの送付
利用管理者
証明書自動発行
支援システム
③アクセスPIN取得URLのメール送信
④アクセスPIN取得URLにアクセス
⑤アクセスPINファイルの取得
利用管理者
⑥アクセスPINの通知
利用者
利用管理者
⑦ダウンロード完了通知メール受信
証明書自動発行
支援システム
利用管理者
⑧証明書失効申請ファイル送付
登録担当者
利用管理者
⑨証明書失効完了通知メール受信
証明書自動発行
支援システム

クライアント証明書更新（P12個別）手続き概要
①クライアント証明書の発行申請を行うための証明書更新申請TSVを作成してください。**（3-3-1-1に記載）**
②決められた手続きに従い、登録担当者へクライアント証明書更新申請TSVを送付してください。**（3-3-1-2に記載）**
③登録担当者がクライアント証明書更新申請TSVを本システムにアップロードすると、本システムより、メールでアクセスPIN取得URLを送信します。**（3-3-1-3に記載）**
④メールを受信したら、アクセスPIN取得URLにアクセスしてください。
⑤「アクセスPINダウンロード画面」が開きますので、アクセスPINを取得してください。**（3-3-1-4に記載）**
⑥取得したアクセスPINを利用者へ通知してください。
⑦利用者がクライアント証明書のダウンロードを行うと、本システムより、ダウンロード完了通知が送信されます。**(3-3-1-5に記載)**
⑧決められた手続きに従い、登録担当者へクライアント証明書失効申請TSVを送付してください。**（3-3-1-6に記載）**
⑨登録担当者が本システムへクライアント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。**（3-3-1-7に記載）**

3-3-1-1. 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証明書更新申請TSVファイルを作成してください。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
更新申請TSVファイルのフォーマットは「5-4-2. クライアント証明書更新申請TSVファイル形式」をご確認ください。

3-3-1-2. 更新申請TSVファイルの送付

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

3-3-1-3. アクセスPIN取得URLの通知

クライアント証明書の更新が完了すると、本システムよりアクセスPINを取得するためのアクセスPIN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アクセスPIN取得URLにアクセスし、アクセスPINの取得を実施してください。

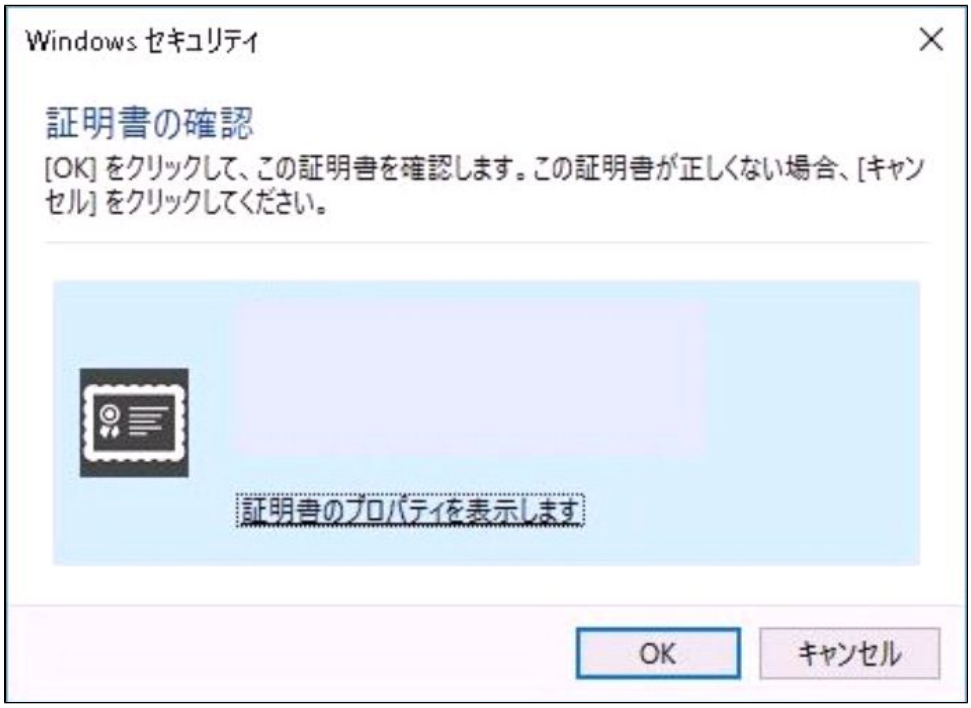
アクセスPIN取得URLの通知
【件名】 アクセスPIN発行通知 ・・・・・ **#以下に証明書の取得先が記述されています。** 貴機関の登録担当者経由で発行申請をいただきました証明書のアクセスPINを配付いたします。 本日から１ヶ月以内に以下のアクセスPIN取得URLへアクセスし、アクセスPINの取得を行ってください。 **アクセスPIN取得URL：**https://scia.secomtrust.net/～　　**←左記URLにアクセスしアクセスPINの取得を行ってください。** ・・・・・

3-3-1-4. アクセスPINの取得

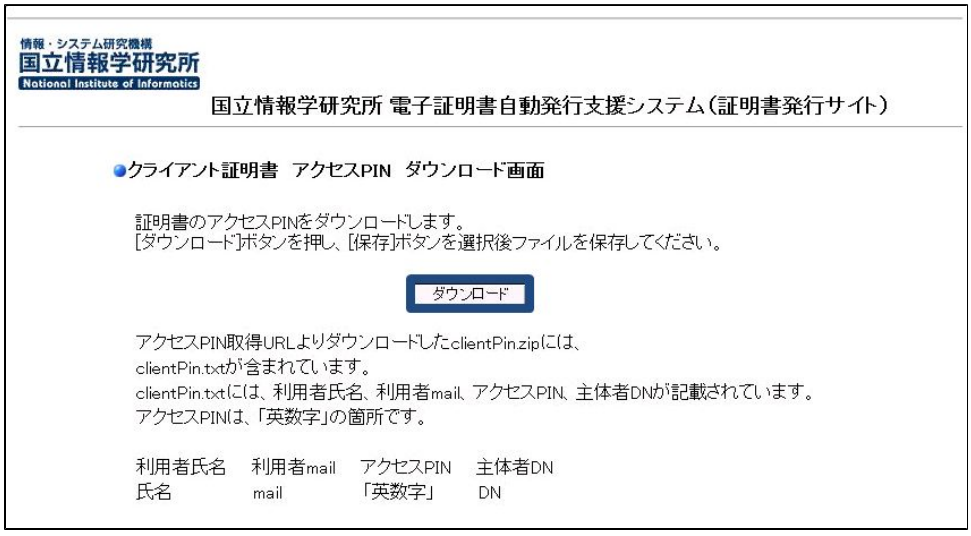
「3-3-1-3. アクセスPIN証明書取得URLの通知」で通知されたURLにアクセスし、アクセスPIN証明書を取得する方法を記述します。

アクセスPINの取得

1. 「3-3-1-3. アクセスPIN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、clientPin.zipファイルが取得できますので保存してください。



3. clientPin.zipファイルを解凍し、アクセスPINを利用者へ配付してください。

3-3-1-5. ダウンロード完了通知メール受信

クライアント証明書の利用者がクライアント証明書のダウンロードを行った場合、本システムより、ダウンロードが完了したことを通知するメールが自動送信されます。このメールは、電子署名されています。

クライアント証明書ダウンロード完了通知メール

【件名】
クライアント証明書取得通知

【本文】

・・・・・
貴機関利用者の方がクライアント証明書の取得を完了致しましたので、

下記の通り連絡をさせていただきます。

【対象証明書DN】

CN=KOKURITSU HANAKO
OU=XXXXXX（学生番号等）
OU=Cyber Science
Infrastructure Development Department,
O=National Institute of Informatics,
L=Chiyoda-ku,
ST=Tokyo
C=JP

【対象証明書シリアル番号】

・・・・・

3-3-1-6. 失効申請TSVファイルの送付

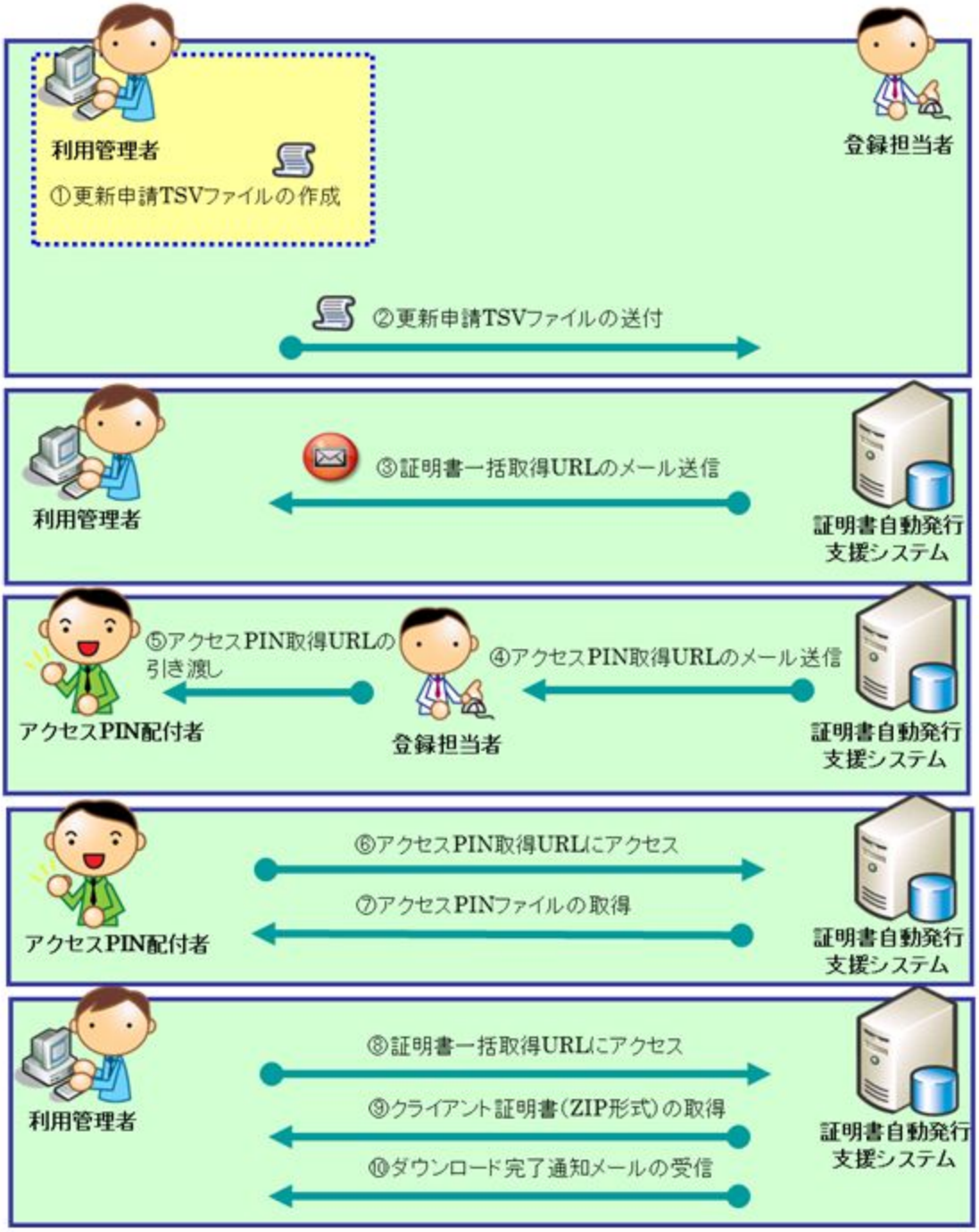
各機関の決められた手続きに従い、登録担当者へ失効申請TSVファイルを送付してください。

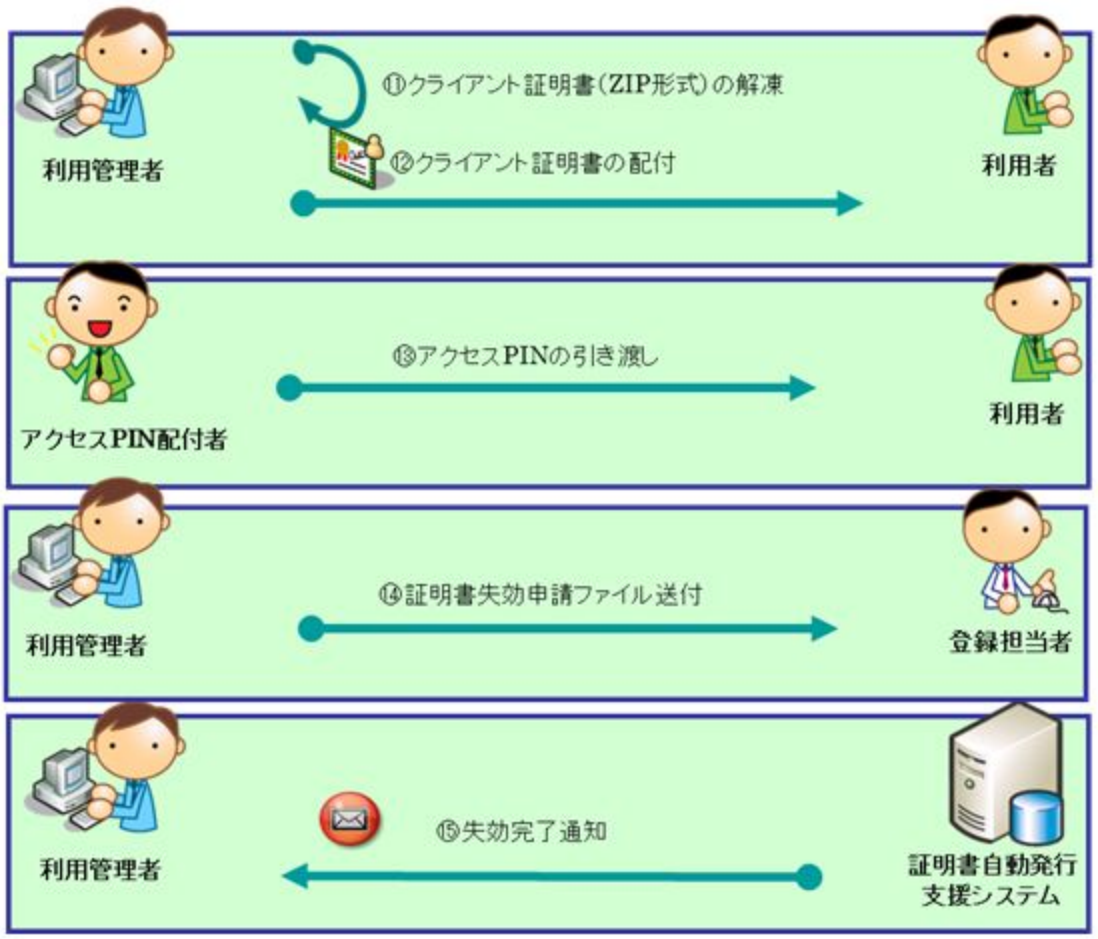
3-3-1-7. 失効完了通知

クライアント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。

3-3-2. クライアント証明書更新発行（P12一括）

証明書の更新をP12一括ダウンロード方法で申請を行う場合について記述します。


利用管理者
①更新申請TSVファイルの作成
登録担当者
②更新申請TSVファイルの送付
利用管理者
③証明書一括取得URLのメール送信
証明書自動発行
支援システム
アクセスPIN配付者
⑤アクセスPIN取得URLの
引き渡し
登録担当者
④アクセスPIN取得URLのメール送信
証明書自動発行
支援システム
アクセスPIN配付者
⑥アクセスPIN取得URLにアクセス
⑦アクセスPINファイルの取得
証明書自動発行
支援システム
利用管理者
⑧証明書一括取得URLにアクセス
⑨クライアント証明書(ZIP形式)の取得
⑩ダウンロード完了通知メールの受信
証明書自動発行
支援システム



クライアント証明書更新（P12一括）手続き概要
①クライアント証明書の更新申請を行うための証明書更新申請TSVを作成してください。**（3-3-2-1に記載）**
②決められた手続きに従い、登録担当者へクライアント証明書更新申請TSVを送付してください。**（3-3-2-2に記載）**
③登録担当者がクライアント証明書更新申請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。**（3-3-2-3に記載）**
④登録担当者へアクセスPIN取得URLが送信されます。**（3-3-2-4に記載）**
⑤アクセスPIN配付者へアクセスPIN取得URLを引き渡してください。
⑥アクセスPIN取得URLにアクセスします。
⑦「アクセスPINダウンロード画面」が開きますので、clientAllPin.zipを取得してください。取得したclientAllPin.zipを解凍してください。**（3-3-2-5に記載）**
⑧アクセスPIN配付者がアクセスPINを取得後、証明書取得URLにアクセスしてください。**（3-3-2-6に記載）**
⑨「証明書ダウンロード画面」が開きますので、clientAllzipを取得してください。
⑩利用管理者がクライアント証明書のダウンロードを行うと、本システムより、ダウンロード完了通知が送信されます。**(3-3-2-7に記載)**
⑪取得した.clientAllzipを解凍してください。
⑫利用者へ証明書P12ファイルを通知してください。
⑬アクセスPIN配付者は利用者へアクセスPINを引き渡してください。**(3-3-2-8に記載)**
⑭決められた手続きに従い、登録担当者へクライアント証明書失効申請TSVを送付してください。**（3-3-2-9に記載）**
⑮登録担当者が本システムへクライアント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**（3-3-2-10に記載）**

3-3-2-1. 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証明書更新申請TSVファイルを作成してください。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
更新申請TSVファイルのフォーマットは「5-4-2. クライアント証明書更新申請TSVファイル形式」をご確認ください。

3-3-2-2. 更新申請TSVファイルの送付

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

3-3-2-3. 証明書取得URLの通知

クライアント証明書の発行が完了すると、本システムより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。

クライアント証明書取得URLの通知
【件名】 クライアント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クライアント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、クライアント証明書の取得を行ってくださ い。。 **証明書取得URL：**https://scia.secomtrust.net/**～** ・・・・・

3-3-2-4. アクセスPIN取得URLの通知

登録担当者へアクセスPIN取得URLがメールにて通知されます。登録担当者はアクセスPIN配付者へアクセスPIN取得URLを引き渡してください。

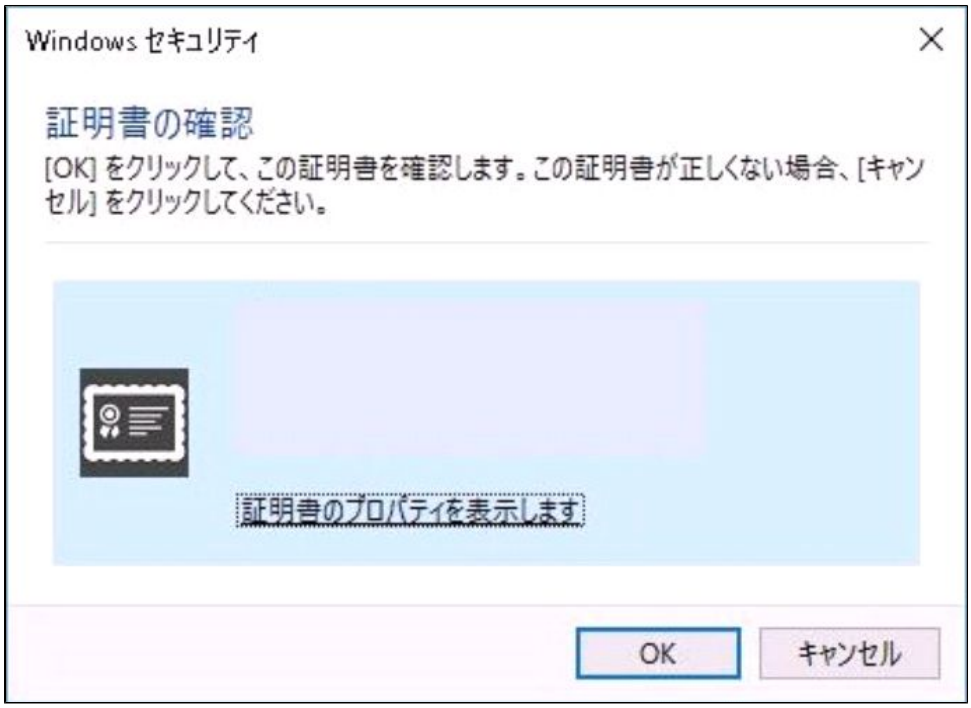
アクセスPIN取得URLの通知
【件名】 アクセスPIN発行通知 ・・・・・ **#以下に証明書の取得先が記述されています。** 貴機関の登録担当者経由で発行申請をいただきました証明書のアクセスPINを配付いたします。 本日から１ヶ月以内に以下のアクセスPIN取得URLへアクセスし、アクセスPINの取得を行ってくださ い。 **アクセスPIN取得URL：**https://scia.secomtrust.net/**～** ・・・・・

3-3-2-5. アクセスPINの取得

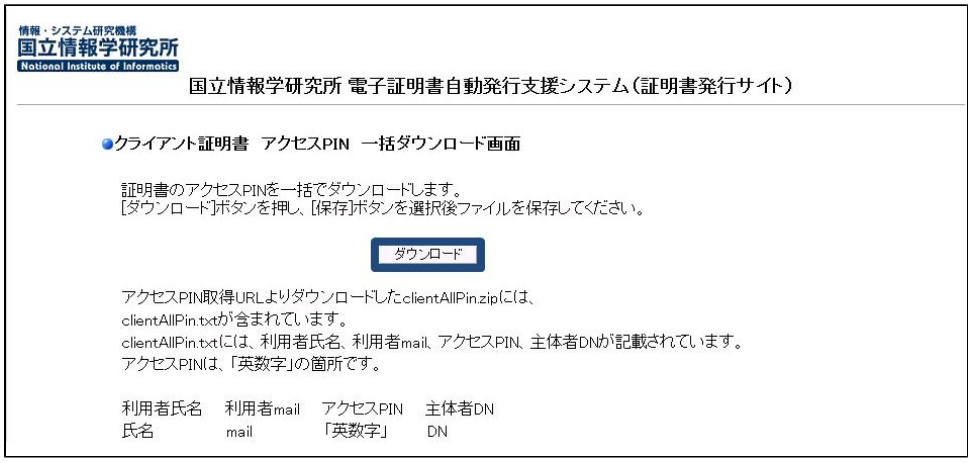
「3-3-2-4. アクセスPIN取得URLの通知」で通知されたURLにアクセスし、アクセスPIN証明書を取得する方法を記述します。

アクセスPINの取得

1. 「3-3-2-4. アクセスPIN取得URLの通知」で通知されたURLにアクセスします。
※証明書取得URLにアクセスする前に、登録管理者にてアクセスPINを取得しておく必要があります。
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、clientAllPin.zipファイルが取得できますので保存してください。



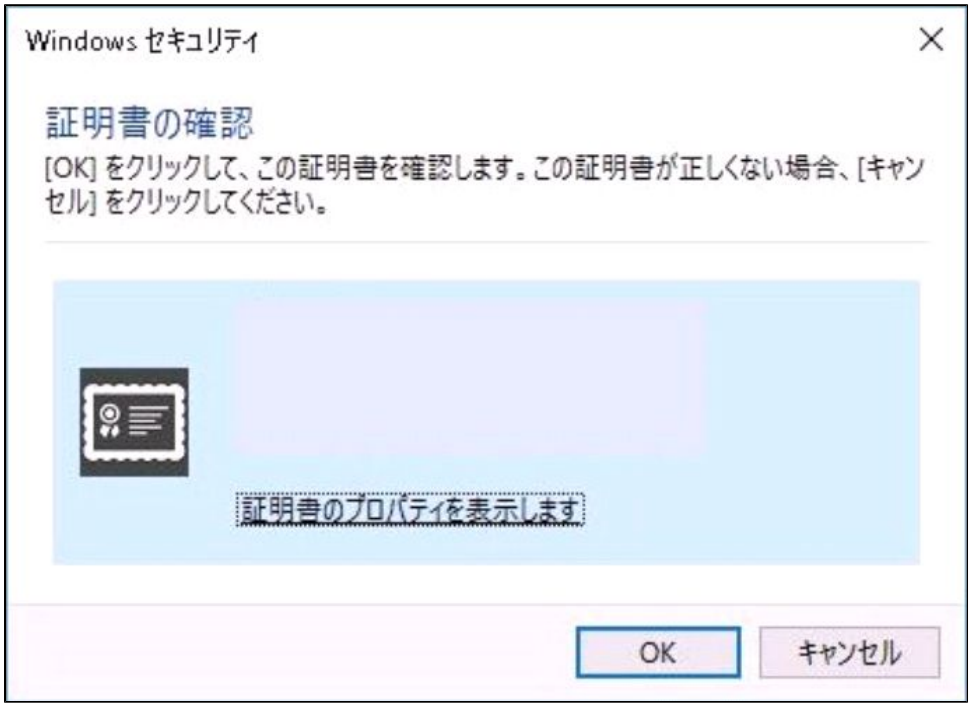
3. clientAllPin.zipファイルを解凍してください。

3-3-2-6. クライアント証明書の取得

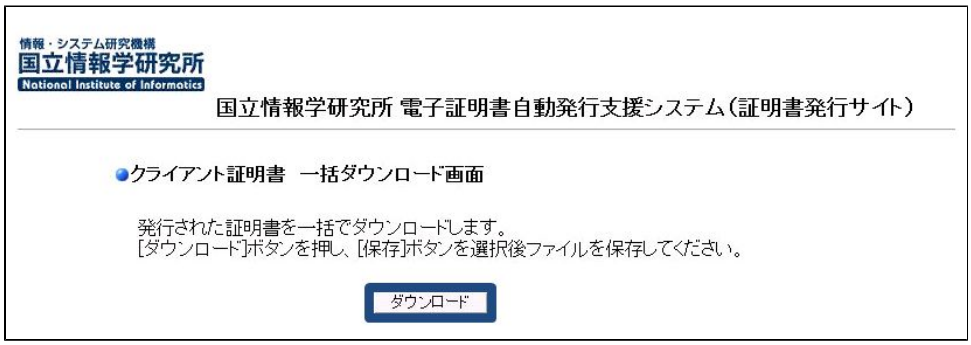
「3-3-2-3. 証明書取得URLの通知」で通知されたURLにアクセスし、証明書を取得する方法を記述します。

クライアント証明書の取得

1. 「3-3-2-3. 証明書取得URLの通知」で通知されたURLにアクセスします。
※証明書取得URLにアクセスする前に、アクセスPIN配布者がアクセスPINを取得しておく必要があります。
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、clientAll.zipファイルが取得できますので保存してください。



3. clientAll.zipファイルを解凍し、証明書を利用者へ配付してください。

3-3-2-7. ダウンロード完了通知メール受信

利用管理者がクライアント証明書のダウンロードを行った場合、本システムより、ダウンロードが完了したことを通知するメールが自動送信されます。
このメールは、電子署名されています。

クライアント証明書ダウンロード完了通知メール

【件名】
クライアント証明書取得通知

【本文】

・・・・・
貴機関利用者の方がクライアント証明書の取得を完了致しましたので、

下記の通り連絡をさせていただきます。

【対象証明書DN】

CN=KOKURITSU HANAKO
OU=XXXXXX（学生番号等）
OU=Cyber Science
Infrastructure Development Department,
O=National Institute of Informatics,
L=Chiyoda-ku
ST=Tokyo
C=JP

【対象証明書シリアル番号】

・・・・・

3-3-2-8. アクセスPINの引き渡し

アクセスPIN配付者は利用者へ「3-3-2-5. アクセスPINの取得」で取得したアクセスPINを引き渡してください。

3-3-2-9. 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。

3-3-2-10. 失効完了通知

クライアント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。

クライアント証明書失効完了の通知

【件名】
クライアント証明書失効完了通知
・・・・・

下記クライアント証明書の失効が完了致しましたの
で、
下記の通り連絡をさせていただきます。

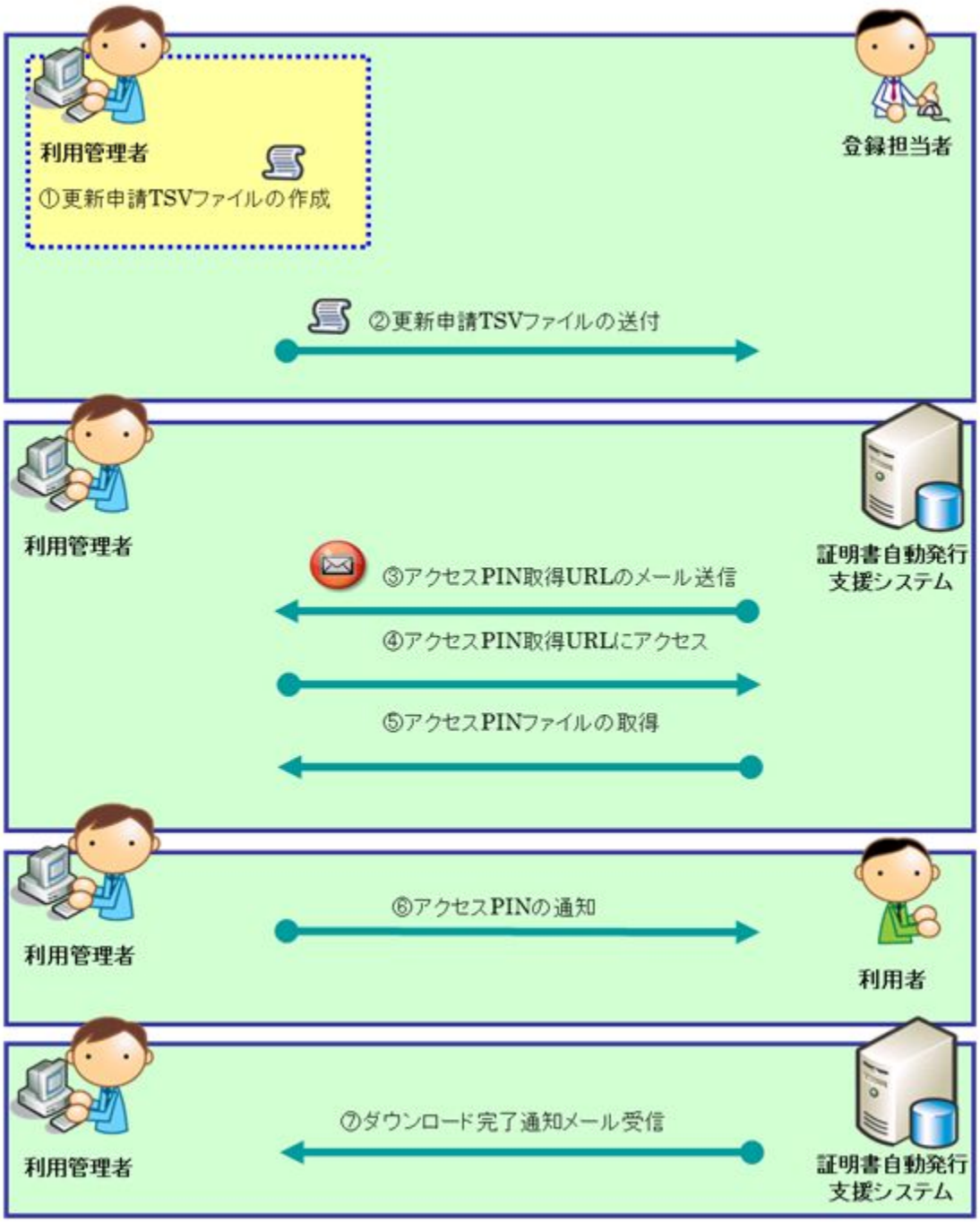
【失効証明書DN】

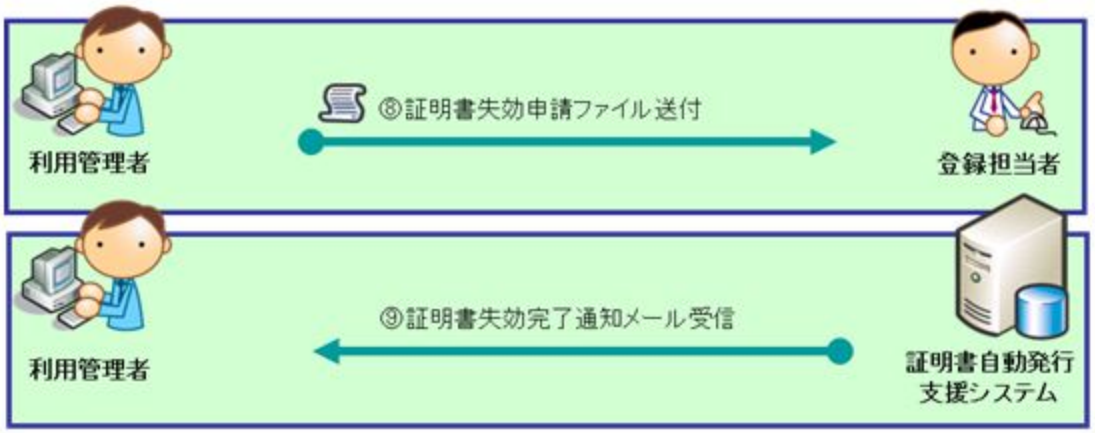
CN=KOKURITSU HANAKO
OU=XXXXXX（学生番号等）
OU=Cyber Science
Infrastructure Development Department,
O=National Institute of Informatics,
L=Chiyoda-ku,
ST=Tokyo
C=JP

・・・・・
【失効証明書シリアル番号】
・・・・・
【失効理由】
・・・・・

3-3-3. クライアント証明書更新発行（ブラウザ）

証明書の発行をブラウザダウンロード方法で申請を行う場合について記述します。





クライアント証明書更新（ブラウザ）手続き概要
①クライアント証明書の更新申請を行うための証明書更新申請TSVを作成してください。 **（3-3-3-1に記載）**
②決められた手続きに従い、登録担当者へクライアント証明書更新申請TSVを送付してください。 **（3-3-3-2に記載）**
③登録担当者がクライアント証明書更新申請TSVを本システムにアップロードすると、本システムより、メールでアクセスPIN取得URLを送信します。 **（3-3-3-3に記載）**
④メールを受信したら、アクセスPIN取得URLにアクセスしてください。
⑤「アクセスPINダウンロード画面」が開きますので、アクセスPINを取得してください。 **（3-3-3-4に記載）**
⑥取得したアクセスPINを利用者へ通知してください。
⑦利用者がクライアント証明書のダウンロードを行うと、本システムより、ダウンロード完了通知が送信されます。**(3-3-3-5に記載)**
⑧決められた手続きに従い、登録担当者へクライアント証明書失効申請TSVを送付してください。 **（3-3-3-6に記載）**
⑨登録担当者が本システムへクライアント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。**(3-3-3-7に記載)**

3-3-3-1. 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証明書更新申請TSVファイルを作成してください。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
更新申請TSVファイルのフォーマットは「5-4-2. クライアント証明書更新申請TSVファイル形式」をご確認ください。

3-3-3-2. 更新申請TSVファイルの送付

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

3-3-3-3. アクセスPIN取得URLの通知

クライアント証明書の更新が完了すると、本システムよりアクセスPINを取得するためのアクセスPIN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アクセスPIN取得URLにアクセスし、アクセスPINの取得を実施してください。

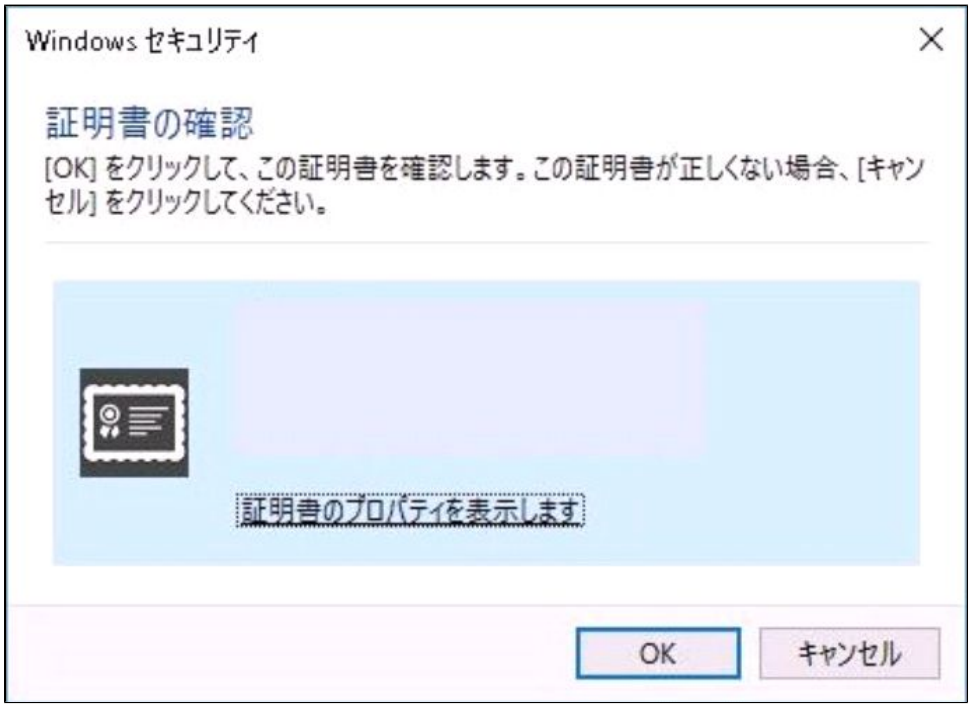
アクセスPIN取得URLの通知
【件名】 アクセスPIN発行通知 ・・・・・ **#以下に証明書の取得先が記述されています。** 貴機関の登録担当者経由で発行申請をいただきました証明書のアクセスPINを配付いたします。 本日から１ヶ月以内に以下のアクセスPIN取得URLへアクセスし、アクセスPINの取得を行ってください。 **アクセスPIN取得URL：**https://scia.secomtrust.net/～　　**←左記URLにアクセスしアクセスPINの取得を行ってください。** ・・・・・

3-3-3-4. アクセスPINの取得

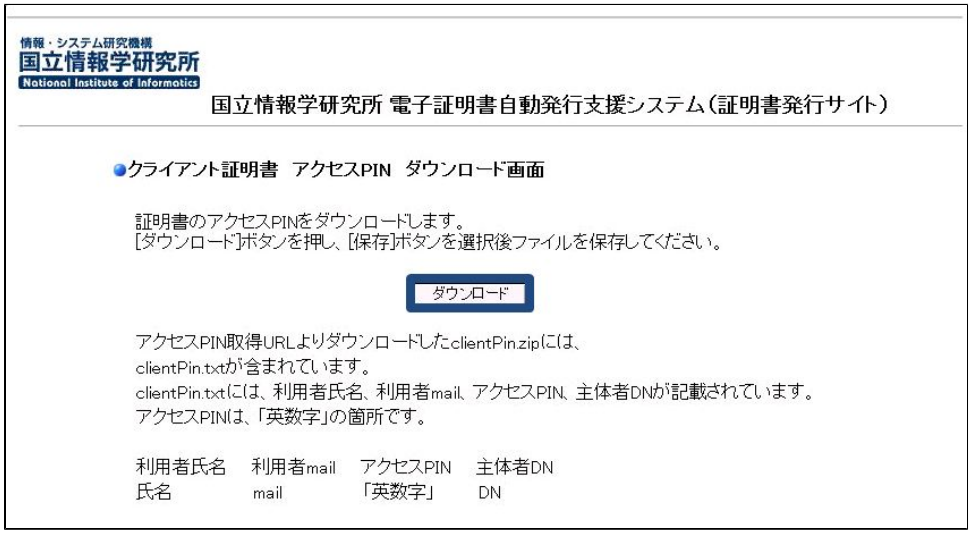
「3-3-3-3. アクセスPIN取得URLの通知」で通知されたURLにアクセスし、アクセスPIN証明書を取得する方法を記述します。

アクセスPINの取得

1．「3-3-3-3. アクセスPIN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、clientPin.zipファイルが取得できますので保存してください。



3．clientPin.zipファイルを解凍し、アクセスPINを利用者へ配付してください。

3-3-3-5. ダウンロード完了通知メール受信

クライアント証明書利用者がクライアント証明書のダウンロードを行った場合、本システムより、ダウンロードが完了したことを通知するメールが自動送信されます。このメールは、電子署名されています。

クライアント証明書ダウンロード完了通知メール

【件名】
クライアント証明書取得通知

【本文】

・・・・・
貴機関利用者の方がクライアント証明書の取得を完了致しましたので、

下記の通り連絡をさせていただきます。

【対象証明書DN】

CN=KOKURITSU HANAKO
OU=XXXXXX（学生番号等）
OU=Cyber Science
Infrastructure Development Department,
O=National Institute of Informatics,
L=Chiyoda-ku,
ST=Tokyo
C=JP

【対象証明書シリアル番号】

・・・・・

3-3-3-6. 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。

3-3-3-7. 失効完了通知

クライアント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。

クライアント証明書失効完了の通知

【件名】
クライアント証明書失効完了通知
・・・・・

下記クライアント証明書の失効が完了致しましたの
で、
下記の通り連絡をさせていただきます。

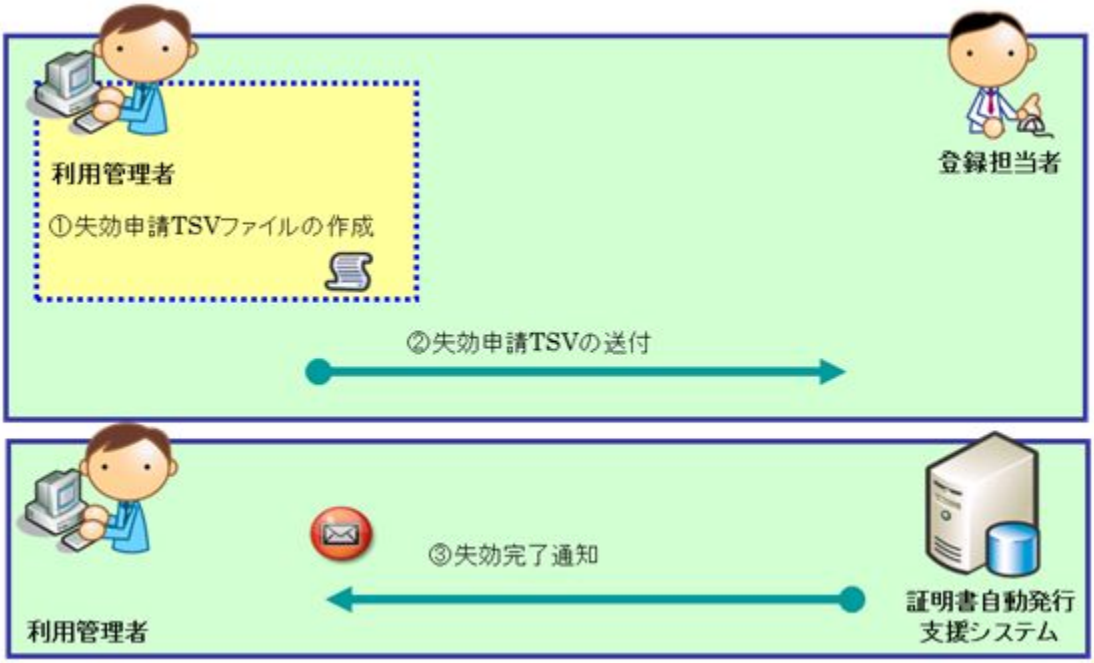
【失効証明書DN】

CN=KOKURITSU HANAKO
OU=XXXXXX（学生番号等）
OU=Cyber Science
Infrastructure Development Department,
O=National Institute of Informatics,
L=Chiyoda-ku,
ST=Tokyo
C=JP

・・・・・
【失効証明書シリアル番号】
・・・・・
【失効理由】
・・・・・

3-4. クライアント証明書の証明書失効申請手続き概要

本章ではクライアント証明書失効手続きの流れについて記述します。
利用管理者は以下の手続きによりクライアント証明書の失効を行います。



クライアント証明書失効発行手続き概要
①クライアント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。 **（3-4-1に記載）**
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。 **（3-4-2に記載）**
③登録担当者が本システムへクライアント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。 **（3-4-3に記載）**

3-4-1. 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クライアント失効証明書失効申請TSVファイルを作成してください。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
失効申請TSVファイルのフォーマットは「5-4-3. クライアント証明書失効申請TSVファイル形式」をご確認ください。

3-4-2. 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。

3-4-3. 失効完了通知

クライアント証明書の失効が完了すると、本システムよりクライアント証明書失効完了通知がメールで送信されます。

クライアント証明書失効完了の通知

【件名】
クライアント証明書失効完了通知
・・・・・

下記クライアント証明書の失効が完了致しましたので、
下記の通り連絡をさせていただきます。

【失効証明書DN】

CN=KOKURITSU HANAKO
OU=XXXXXX（学生番号等）
OU=Cyber Science
Infrastructure Development Department,
O=National Institute of Informatics,
L=Chiyoda-ku,
ST=Tokyo
C=JP

・・・・・
【失効証明書シリアル番号】
・・・・・
【失効理由】
・・・・・

4. コード署名用証明書管理手順

本章では利用管理者のコード署名用証明書の各種手続きの流れについて記述します。
コード署名用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
証明書発行 (**4-1.コード署名用証明書発行**)	コード署名用証明書を発行する場合。
証明書失効 (**4-2.コード署名用証明書失効**)	コード署名用証明書が不要になった場合や秘密鍵が危殆化した場合。

4-1. コード署名用証明書発行

コード署名用証明書の無償提供は2023年5月12日で終了いたしました。
詳しくは、以下のお知らせをご覧ください。

コード署名用証明書の新規・更新発行の受付終了に関するお知らせ

4-2. コード署名用証明書の証明書失効申請手続き

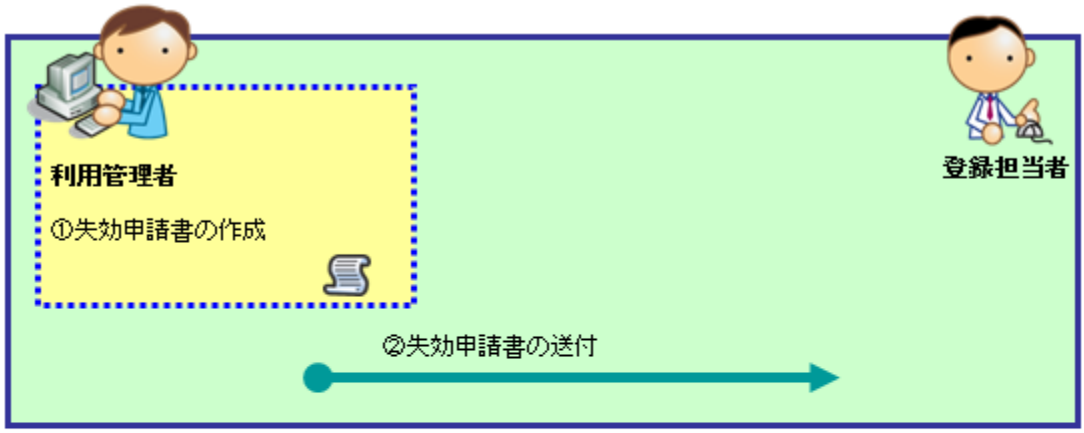
本章では利用管理者のコード署名用証明書失効手続きの流れについて記述します。利用管理者は以下の手続きにより証明書の失効を行います。

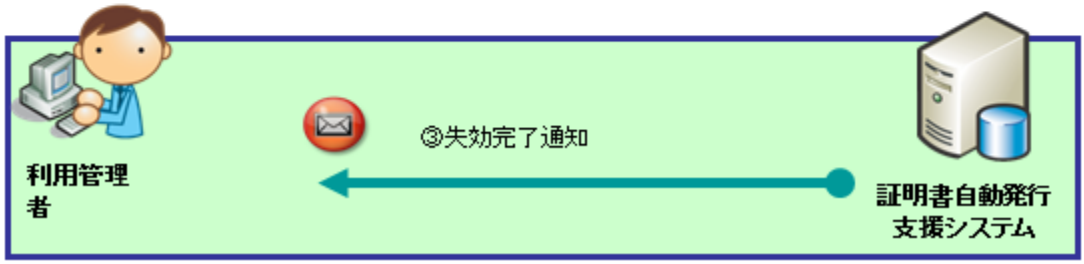
失効申請書（Excel）に利用管理者のメールアドレスが記載されている場合は、利用管理者に失効完了通知メールが送信されます。

・【コード署名証明書】失効申請書（UPKI電子証明書発行サービス）（Excel）

※「住所」は利用機関登録した際の本部所在地をご記入ください。
※「利用機関名」は法人名から記入してください。
（例）申請大学　→　学校法人申請学園　申請大学

・【コード署名証明書】失効申請書（UPKI電子証明書発行サービス）記入例（PDF）





コード署名用証明書失効発行手続き概要
①失効申請書(Excel)を作成します。 **（4-2-1に記載）**
②失効申請書(Excel)を登録担当者に送付します。 **（4-2-2に記載）**
③失効完了通知メール受信。 **（4-2-3に記載）**

4-2-1. 利用管理者による失効申請書(Excel)の作成

利用管理者は、失効申請書(Excel)を作成します。

4-2-2. 失効申請書(Excel)の送付

利用管理者は、作成した失効申請書(Excel)を登録担当者宛にメールで送付します。

4-2-3. 失効完了メール受信

コード署名用証明書の失効を行った場合、失効完了通知メールが送信されます。

5. 本システムで扱うファイル形式

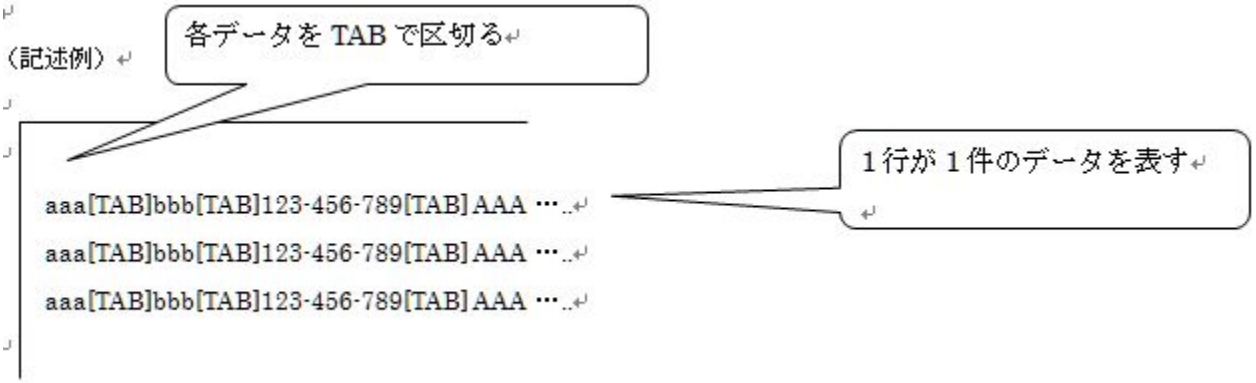
5-1. TSVファイル形式

サーバ証明書発行／更新／失効申請ファイル中の申請件数の制限は、１ファイル99件までです。
クライアント証明書発行／更新／失効申請ファイル中の申請件数の制限は、１ファイル99件までです。
※ダウンロード方法「2:P12一括」発行時の場合のみ、１ファイル1000件までです。

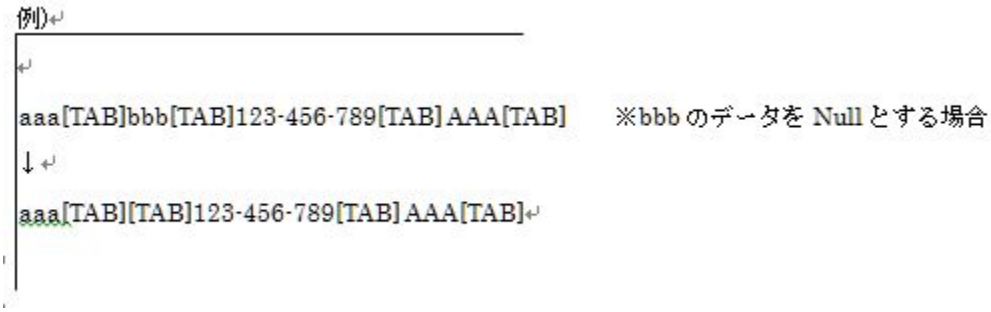
> **TSV作成ツールについて**
>
> 本システムで扱う各TSVファイルを作成するWebアプリケーションを提供しております。
>
> 下記リンクからご利用ください。
>
> TSV作成ツール https://certs.nii.ac.jp/tsv-tool/

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は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



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。



5-2. ファイル制約事項

全角文字が入力可能な項目において，使用可能文字はJIS X0208:1997（JIS第一・第二水準の漢字）＋JIS X0201の範囲です。
第三水準以降のものにつきましては第二水準以下の漢字に置換して作成してください。

5-3. サーバ証明書申請TSVファイル形式

5-3-1. サーバ証明書発行申請TSVファイル形式

項目番号	項目名称	必須	文字	サイズ（文字数）	その他
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,O,L,ST,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 ,O=National Institute of Informatics ,L=Chiyoda-ku ,ST=Tokyo ,C=JP
2	証明書プロファイルID	○	半角数字	2	3:sha256WithRSAEncryption 11:ecdsa-with-SHA384
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	「サーバ証明書インストールマニュアル」に従って作成したCSRを記述してください。 ----BEGIN CERTIFICATE REQUEST----行と ----END CERTIFICATE REQUEST----行を削除し、一行で記述してください。 ※項目番号2の証明書プロファイルIDを"3"(sha256WithRSAEncryption)に指定した場合　鍵長は2048にしてください。　署名アルゴリズムは以下のいずれかを指定してくださ い。　・sha1WithRSAEncryption　・sha256WithRSAEncryption　・sha384WithRSAEncryption　・sha512WithRSAEncryption ・md5WithRSAEncryption ※項目番号2の証明書プロファイルIDを"11"（ecdsa-with-SHA384)に指定した場合 曲線名は"secp384r1" を指定してください。 署名アルゴリズムは以下のいずれかを指定してください。 ・ecdsa-with-SHA256 ・ecdsa-with-SHA384
8	利用管理者氏名	△	全角、半角	64	利用管理者の氏名を記述してください。 例)国立　太郎
9	利用管理者所属	△	全角、半角	64	利用管理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	利用管理者mail	○	半角英数字	78	利用管理者の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	利用管理者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	利用管理者ソフトウェア名・バージョン	○	全角、半角	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。 利用管理者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。 dNSNameは8つまで指定可能です。 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。 ※また末尾に "," を記載しないでください。 ここで指定した値は、証明書の拡張領域 SANs（Subject Alternative Names）に記載されます。

5-3-2. サーバ証明書更新申請TSVファイル形式

項目 番号	項目名称	必須	文字	サイズ（文字数）	その他
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,O,L,ST,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、また更新対象のDNと異なる場合はエラーとなります。 例) CN=www.nii.ac.jp ,O=National Institute of Informatics ,L=Chiyoda-ku ,ST=Tokyo ,C=JP
2	証明書プロファイルID	○	半角数字	1	3:sha256WithRSAEncryption 11:ecdsa-with-SHA384
3					・・・・・・・・・・No3は空白
4	失効対象証明書シリアル番号	○	半角英数字	50	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	「サーバ証明書インストールマニュアル」に従って作成したCSRを記述してください。 ----BEGIN CERTIFICATE REQUEST----行と ----END CERTIFICATE REQUEST----行を削除し、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。 ※項目番号2の証明書プロファイルIDを"3"(sha256WithRSAEncryption)に指定した場合 鍵長は2048にしてください。 署名アルゴリズムは以下のいずれかを指定してください。 ・sha1WithRSAEncryption ・sha256WithRSAEncryption ・sha384WithRSAEncryption ・sha512WithRSAEncryption ・md5WithRSAEncryption ※項目番号2の証明書プロファイルIDを"11"（ecdsa-with-SHA384)に指定した場合 曲線名は"secp384r1" を指定してください。 署名アルゴリズムは以下のいずれかを指定してください。 ・ecdsa-with-SHA256 ・ecdsa-with-SHA384
8	利用管理者氏名	△	全角、半角	64	利用管理者の氏名を記述してください。 例)国立　太郎
9	利用管理者所属	△	全角、半角	64	利用管理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	利用管理者mail	○	半角英数字	78	利用管理者の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	利用管理者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	利用管理者ソフトウェア名・バージョン	○	全角、半角	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。 利用管理者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。 dNSNameは8つまで指定可能です。 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。 ※また末尾に "," を記載しないでください。 ここで指定した値は、証明書の拡張領域 SANs（Subject Alternative Names）に記載されます。

5-3-3. サーバ証明書失効申請TSVファイル形式

項目 番号	項目名称	必須	文字	サイズ（文字数）	その他

1	主体者DN	○	半角英数字記号	250	失効対象のDNを記入してください。 ※異なる場合はエラーとなります。 例) CN=www.nii.ac.jp ,O=National Institute of Informatics ,L=Chiyoda-ku ,ST=Tokyo ,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	50	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	利用管理者mail	△	半角英数字	78	利用管理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

5-4. クライアント証明書申請TSVファイル形式

5-4-1. クライアント証明書発行申請TSVファイル形式

項目番号	項目名称	必須	文字	サイズ（文字数）	その他

1	主体者DN	○	半角英数字記号	250	発行するクライアント証明書のDNを"CN,OU,O,L,ST,C"の順序で記述してください。 学生番号等を記載しているのは、同姓同名を考慮しているためです。 CNに使用できる文字は、半角英数字、空白「 」、アポストロフィ「'」、括弧「()」、カンマ「,」、ハイフン「-」、ピリオド「.」、スラッシュ「/」、コロン「:」、イコール「=」、アットマーク「@」、アンダースコア「_」です。 O、OUおよびLに使用できる文字は、半角英数字、空白「 」、アポストロフィ「'」、括弧「()」、カンマ「,」、ハイフン「-」、ピリオド「.」、スラッシュ「/」、コロン「:」、イコール「=」です。OUは64文字以内で記述してください。 Lは利用管理者及び利用者が所属する組織の所在地の市区町村名とし、原則としてサービス窓口に事前に届出したとおりの所在地の市区町村名をローマ字表記で指定してください。Lは64文字以内で記述してください。 STは利用管理者及び利用者が所属する組織の所在地の都道府県名とし、原則としてサービス窓口に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定してください。 LおよびSTとして指定できる値は「UPKI証明書 主体者DNにおける ST および L の値一覧」を参照してください。機関ごとに固定となります。 LとSTのいずれかは記述してください。 例) CN=KOKURITSU HANAKO ,OU=XXXXXX（学生番号等） ,OU=Cyber Science Infrastructure Development Department ,O=National Institute of Informatics ,L=Chiyoda-ku ,ST=Tokyo ,C=JP ◆S/MIME証明書の注意点 証明書プロファイルIDが7, 15, 16の場合、CNの値が利用者メールの値と一致している必要があります。 発行される証明書はCNの値のみが設定されますが、CN以外の値（O, L, ST, C）も記載が必要です。 UPKIアプリ上ではCN以外も表示されます。 以下の例の場合、発行される証明書の主体者DNは、「CN=xxxxx@example.com」のみです。 例) CN=xxxxx@example.com ,O=National Institute of Informatics ,L=Chiyoda-ku ,ST=Tokyo ,C=JP
2	証明書プロファイルID	○	半角数字	2	5:クライアント証明書（sha256WithRSAEncryption）(2023年9月8日21:00以降は証明書有効期間:48ヶ月。それ以前は証明書有効期間:52ヶ月) 7:S/MIME証明書（sha256WithRSAEncryption）(2022年3月22日以降は証明書有効期間:823日。それ以前は証明書有効期間:52ヶ月) 13:クライアント証明書（sha256WithRSAEncryption）(証明書有効期間:13ヶ月) 14:クライアント証明書（sha256WithRSAEncryption）(証明書有効期間:25ヶ月) 15:S/MIME証明書（sha256WithRSAEncryption）(証明書有効期間:13ヶ月) 16:S/MIME証明書（sha256WithRSAEncryption）(証明書有効期間:25ヶ月)
3	ダウンロード方法	○	半角数字	1	1:P12個別 2:P12一括 3:ブラウザ個別
4					・・・・・・・・・・No4～No7まで空白
5					・・・・・・・・・・No4～No7まで空白
6					・・・・・・・・・・No4～No7まで空白
7					・・・・・・・・・・No4～No7まで空白
8	利用管理者氏名	△	全角、半角	64	利用管理者の氏名を記述してください。 例)国立　太郎
9	利用管理者所属	△	全角、半角	64	利用管理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	利用管理者mail	○	半角英数字	78	利用管理者のEmailアドレスを記述してください。 証明書の発行をP12一括ダウンロード方法で行った場合の証明書取得URLの送信先となります。それ以外に場合はアクセスPIN取得URLの送信先となります。 例)xxxxx@example.com
11	利用者氏名	△	全角、半角	64	利用者の氏名を記述してください。 例)国立　花子
12	P12ダウンロードファイル名	△	半角英数字	64	本項目は証明書ダウンロード時のファイル名です。主体者DN(#1)中のCNと一致する必要はありません。 使用可能文字は、半角英数字、空白「 」、アポストロフィ「'」、括弧「()」、カンマ「,」、ハイフン「-」、ピリオド「.」、イコール「=」です。 未指定の場合、ダウンロード方法「2：P12一括申請」以外だとP12ダウンロードファイル名は、主体者DN(#1)中のCNとなります。 ※証明書プロファイルIDが6,7かつダウンロード方法「2：P12一括申請」以外の場合、必須項目となります。 例）KOKURITSU HANAKO ◆ブラウザ個別発行の注意点 ダウンロード方法が3でP12ダウンロードファイル名に「'」が含まれている場合、現在証明書取得ができません。 P12個別またはP12一括でのご申請お願いいたします。対応は3月上旬を予定しております。
13	利用者所属	△	全角、半角	64	利用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

14	利用者mail	○※	半角英数字	78	利用者のEmailアドレスを記述してください。 例)xxxxx@example.com ※証明書プロファイルIDが5かつダウンロード方法が2の時のみ、任意項目です。
15	アクセスPIN	△	半角英数記号	36	PKCS#12のアクセスPINを記述してください。 ※6桁以上36桁以下が申請可能です ダウンロード方法「2：P12一括申請」の場合のみ、パスワード指定可能です。 未指定の場合、システムで生成したアクセスPINを使用します。 パスワード指定使用可能文字は、 半角英数字、感嘆符「!」、シャープ「#」、ドルマーク「$」、パーセント「%」、アンパサンド「&」、アスタリスク「*」、プラス「+」、カンマ「,」、ハイフン「-」、ピリオド「.」、スラッシュ「/」、コロン「:」、セミコロン「;」、イコール「=」、疑問符「?」、アットマーク「@」、カレット「^」、アンダースコア「_」、バッククォート「`」、パイプ「|」、チルダ「~」、括弧「( ) { } [ ] < >」である。 ※以下の文字は使用できません。 ・半角空白「 」 ・円マーク「\」 ・アポストロフィ「’」 ・ダブルクォーテーション「”」 ◆S/MIME証明書の注意点 証明書プロファイルIDが7, 15, 16の場合、アクセスPINはシステム生成のみで指定不可

5-4-2. クライアント証明書更新申請TSVファイル形式

項目番号	項目名称	必須	文字	サイズ（文字数）	その他
1	主体者DN	○	半角英数字記号	250	発行済の証明書のDNを"CN,OU,O,L,ST,C"の順序で記述してください。 CNに使用できる文字は、半角英数字、空白「 」、アポストロフィ「'」、括弧「()」、カンマ「,」、ハイフン「-」、ピリオド「.」、スラッシュ「/」、コロン「:」、イコール「=」、アットマーク「@」、アンダースコア「_」です。 O、OUおよびLに使用できる文字は、半角英数字、空白「 」、アポストロフィ「'」、括弧「()」、カンマ「,」、ハイフン「-」、ピリオド「.」、スラッシュ「/」、コロン「:」、イコール「=」です。OUは64文字以内で記述してください。 Lは利用管理者及び利用者が所属する組織の所在地の市区町村名とし、原則としてサービス窓口に事前に届出したとおりの所在地の市区町村名をローマ字表記で指定してください。Lは64文字以内で記述してください。 STは利用管理者及び利用者が所属する組織の所在地の都道府県名とし、原則としてサービス窓口に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定してください。 LおよびSTとして指定できる値は「UPKI証明書 主体者DNにおける ST および L の値一覧」を参照してください。機関ごとに固定となります。 LとSTのいずれかは記述してください。 例) CN=KOKURITSU HANAKO ,OU=XXXXXX（学籍番号等） ,OU=Cyber Science Infrastructure Development Department ,O=National Institute of Informatics ,L=Chiyoda-ku ST=Tokyo ,C=JP ◆S/MIME証明書の注意点 証明書プロファイルIDが7, 15, 16の場合、CNの値が利用者メールの値と一致している必要があります。 発行される証明書はCNの値のみが設定されますが、CN以外の値（O, L, ST, C）も記載が必要です。 もし、更新元の証明書にOUが含まれている場合は、OUも記載が必要です。 UPKIアプリ上ではCN以外も表示されます。 以下の例の場合、発行される証明書の主体者DNは、「CN=xxxxx@example.com」のみです。 例) CN=xxxxx@example.com ,O=National Institute of Informatics ,L=Chiyoda-ku ,ST=Tokyo ,C=JP
2	証明書プロファイルID	○	半角数字	2	5:クライアント証明書（sha256WithRSAEncryption）(2023年9月8日21:00以降は証明書有効期間:48ヶ月。それ以前は証明書有効期間:52ヶ月) 7:S/MIME証明書（sha256WithRSAEncryption）(2022年3月22日以降は証明書有効期間:823日。それ以前は証明書有効期間:52ヶ月) 13:クライアント証明書（sha256WithRSAEncryption）(証明書有効期間:13ヶ月) 14:クライアント証明書（sha256WithRSAEncryption）(証明書有効期間:25ヶ月) 15:S/MIME証明書（sha256WithRSAEncryption）(証明書有効期間:13ヶ月) 16:S/MIME証明書（sha256WithRSAEncryption）(証明書有効期間:25ヶ月)
3	ダウンロード方法	○	半角数字	1	1:P12個別 2:P12一括 3:ブラウザ個別

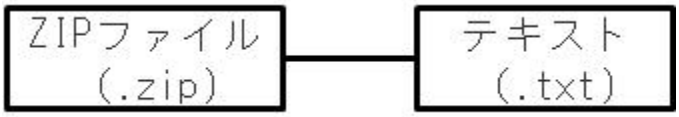
4	更新対象証明書シリアル番号	○	半角英数字	32	旧証明書のシリアル番号を10進数または１６進数で記述してください。 10進数の場合 例) 1234567812345678123 16進数の場合 例) 0x112210E261FEC92B ※16進数の場合は先頭に[0x]をつけてください。半角英字は大文字小文字どちらも使用できます。
5					・・・・・・・・・・No5～No7まで空白
6					・・・・・・・・・・No5～No7まで空白
7					・・・・・・・・・・No5～No7まで空白
8	利用管理者氏名	△	全角、半角	64	利用管理者の氏名を記述してください。 例)国立　太郎
9	利用管理者所属	△	全角、半角	64.	利用管理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	利用管理者mail	○	半角英数字	78	利用管理者のEmailアドレスを記述してください。 証明書の発行をP12一括ダウンロード方法で行った場合の証明書取得URLの送信先となります。それ以外に場合はアクセスPIN取得URLの送信先となります。 例)xxxxx@example.com
11	利用者氏名	△	全角、半角	64	利用者の氏名を記述してください。 例)国立　花子
12	P12ダウンロードファイル名	△	半角英数字	64	本項目は証明書ダウンロード時のファイル名です。主体者DN(#1)中のCNと一致する必要はありません。 使用可能文字は、半角英数字、空白「 」、アポストロフィ「'」、括弧「()」、カンマ「,」、ハイフン「-」、ピリオド「.」、イコール「=」です。 未指定の場合、ダウンロード方法「2：P12一括申請」以外だとP12ダウンロードファイル名は、主体者DN(#1)中のCNとなります。※証明書プロファイルIDが6,7かつダウンロード方法「2：P12一括申請」以外の場合、必須項目となる 例）KOKURITSU HANAKO ◆ブラウザ個別発行の注意点 ダウンロード方法が3でP12ダウンロードファイル名に「'」が含まれている場合、現在証明書取得ができません。 P12個別またはP12一括でのご申請お願いいたします。対応は3月上旬を予定しております。
13	利用者所属	△	全角、半角	64	利用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
14	利用者mail	○※	半角英数字	78	利用者のEmailアドレスを記述してください。 例)xxxxx@example.com ※証明書プロファイルIDが5かつダウンロード方法が2の時のみ、任意項目です。
15	アクセスPIN	△	半角英数記号	36	PKCS#12のアクセスPINを記述してください。 ※6桁以上36桁以下が申請可能です ダウンロード方法「2：P12一括申請」の場合のみ、パスワード指定可能です。 未指定の場合、システムで生成したアクセスPINを使用します。 パスワード指定使用可能文字は、 半角英数字、感嘆符「!」、シャープ「#」、ドルマーク「$」、パーセント「%」、アンパサンド「&」、アスタリスク「*」、プラス「+」、カンマ「,」、ハイフン「-」、ピリオド「.」、スラッシュ「/」、コロン「:」、セミコロン「;」、イコール「=」、疑問符「?」、アットマーク「@」、カレット「^」、アンダースコア「_」、バッククォート「`」、パイプ「|」、チルダ「~」、括弧「( ) { } [ ] < >」である。 ※以下の文字は使用できません。 ・半角空白「 」 ・円マーク「\」 ・アポストロフィ「' 」 ・ダブルクォーテーション「" 」 ◆S/MIME証明書の注意点 証明書プロファイルIDが7, 15, 16の場合、アクセスPINはシステム生成のみで指定不可

5-4-3. クライアント証明書失効申請TSVファイル形式

項目番号	項目名称	必須	文字	サイズ（文字数）	その他
1	主体者DN	○	半角英数字記号	250	証明書発行／更新時に設定したDNを"CN,OU,O,L,ST,C"の順序で記述してください。 CNに使用できる文字は、半角英数字、空白「 」、アポストロフィ「'」、括弧「()」、カンマ「,」、ハイフン「-」、ピリオド「.」、スラッシュ「/」、コロン「:」、イコール「=」、アットマーク「@」、アンダースコア「_」です。 O、OUおよびLに使用できる文字は、半角英数字、空白「 」、アポストロフィ「'」、括弧「()」、カンマ「,」、ハイフン「-」、ピリオド「.」、スラッシュ「/」、コロン「:」、イコール「=」です。OUは64文字以内で記述してください。 Lは利用管理者及び利用者が所属する組織の所在地の市区町村名とし、原則としてサービス窓口に事前に届出したとおりの所在地の市区町村名をローマ字表記で指定してください。Lは64文字以内で記述してください。 STは利用管理者及び利用者が所属する組織の所在地の都道府県名とし、原則としてサービス窓口に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定してください。 LおよびSTとして指定できる値は「UPKI証明書 主体者DNにおける ST および L の値一覧」を参照してください。機関ごとに固定となります。 LとSTのいずれかは記述してください。 例) CN=TEST TAROU ,OU=Cyber Science Infrastructure Development Department ,O=National Institute of Informatics ,L=Chiyoda-ku ,ST=Tokyo ,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	利用管理者mail	△	半角英数字	78	利用管理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
14	利用者mail	△	半角英数字	78	利用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
15	アクセスPIN		半角英数記号	36	

5-5. アクセスPINファイル構成

クライアント証明書（P12個別、P12一括、ブラウザ発行）、コード署名用証明書（P12個別）にて使用するアクセスPINファイルの構成を以下に示す。



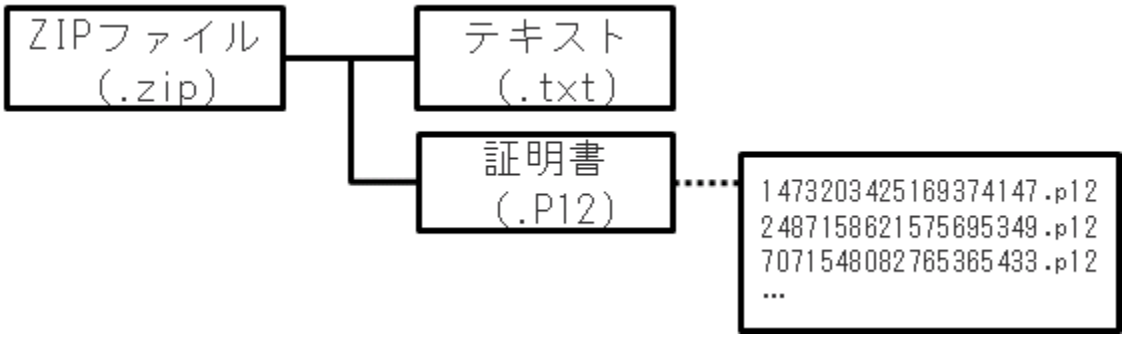
5-5-1. クライアント証明書アクセスPINファイル構成

クライアント証明書（P12個別、P12一括、ブラウザ発行）にて使用するアクセスPINファイルの構成を以下に示す。

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)
ファイル拡張子	.txt
文字コード	Shift-JIS
ファイル名	clientPin　　（P12個別の場合） clientAllPin　（P12一括の場合）

5-6. 証明書ZIPファイル構成

クライアント証明書（P12一括）にてダウンロードされる証明書ZIPファイルは、
証明書及び証明書情報ファイルから構成される。構成を以下に示す。



5-6-1. 証明書情報ファイル構成

証明書ZIPファイルに含まれる証明書情報ファイルの構成を以下に示す。

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)

ファイル拡張子	.txt
文字コード	Shift-JIS
ファイル名	client

(記載例)