

LGWAN

Local Government Wide Area Network

総合行政ネットワーク



→特集

LGPKIの証明書の発行手続について

通信相手が見えないネットワーク上で、電子的手段を用いて申請届出等の行政手続や文書交付等を行うにあたり、相手を信頼し、安全な通信を確保する方法として、PKI(Public Key Infrastructure(公開鍵基盤))という情報技術が広く利用されており、地方公共団体の行政事務専用に設けたPKIが地方公共団体組織認証基盤(略称:LGPKI(Local Government Public Key Infrastructure))です。

LGPKIを利用することにより、地方公共団体が住民・企業等との間で実施する申請・届出等の手続、あるいは、地方公共団体相互間の文書のやり取りにおいて、盗聴、改ざん、なりすまし、事後否認の脅威を防止し、送受信された電子文書の真正性(本人が作成した文書に相違ないこと)を担保することができます*1。

LGPKIでは、全地方公共団体の証明書に関する業務を一つのポリシーの元に運営しています。認証 局の運営は、LGWAN全国センターが行い、電子証明書(以下「証明書」という。)の発行や証明書の 有効性を検証するための仕組みを提供しています。

では、電子入札や電子申請のためにLGPKIの証明書を取得したい場合、どこにどのようにして申請を行えばよいのでしょうか。今月号では、地方公共団体の証明書利用者がLGPKIの証明書の発行等申請を行ってから証明書を取得するまでの流れを詳しく説明します。

2

1 LGPKIにおける登録分局の役割

LGPKIの運営にあたり、地方公共団体情報システム機構が意思決定を行い、LGWAN全国センター(以下「運営主体」という。)が証明書の発行等を行う「認証局」を運営しています。これに加えて、地方公共団体内に設置される「登録分局」があり、これらの組織によって、LGPKIの運営体制が構成されています。(図-1)

登録分局は、「地方公共団体組織認証基盤の運営 に関する基本要綱*2」第7条に定める、証明書利用 者からの証明書発行等の申請受付・審査及び認証局 (登録局*3)への発行等申請並びに認証局(発行局*4) が発行した証明書の配付等の業務を運営主体から委 任されています。

LGPKIが発行する証明書の種類

LGPKIでは、職責証明書、利用者証明書、暗号 化通信用等証明書、メール用証明書、Webサーバ 証明書及びコードサイニング証明書の6種類の証明 書を発行しています。

各証明書の用途は、表-1のとおりです。

- **1 LGPKIの目的と概要については、本誌平成27年10月号「電子文書を脅威から守るための仕組みとLGPKIの信頼性を確かにする仕組みについて」を参照してください。
- *2 http://center.lgwan.jp/library/second2.html#C-6-6-1
- ※3 登録分局からの証明書発行等申請の受付及び審査を行い、「発行局」への証明書発行等の要求を行う機関
- ※4 登録局からの発行等の要求に基づき、証明書の発行等を行う機関



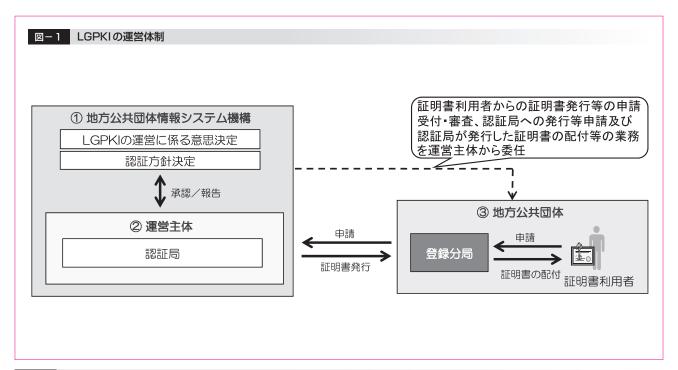


表-1 証明書の種類と用途

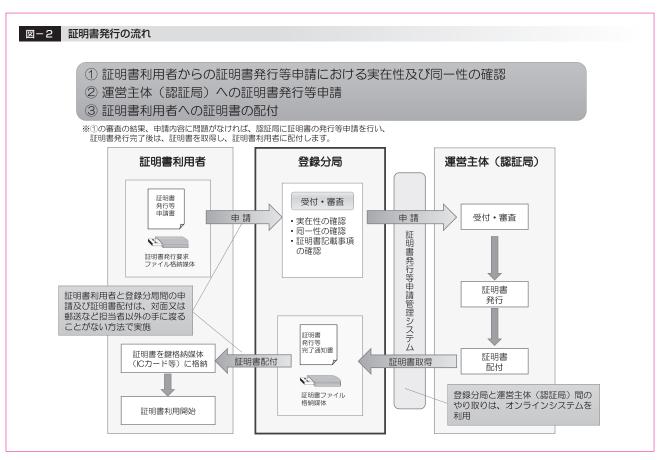
| 証明書 | 用途 |
|-------------|--|
| 職責証明書 | 電子申請システムや電子入札システムで、地方公共団体の職責者による地方公共団体相互及び住民・企業向け公文書への電子署名に使用する。 主な利用例:電子入札、電子申請、電子申告 |
| 利用者証明書 | 各種システムを利用する際の利用者を認証するために利用する。 |
| 暗号化通信用等証明書 | 情報提供ネットワークシステム及びこれに接続する電子計算機並びにその使用者を示す証明書であり、通信データの署名及び暗号化に使用する。 |
| メール用証明書 | 住民・企業向けメールマガジンの発信において、電子メールの電子署名に使用する。 |
| Webサーバ証明書 | 住民・企業に対する広報及び申請業務等を行うウェブサーバに適用し、SSL等の暗号化通信に使用する。 |
| コードサイニング証明書 | 住民・企業へ配布されるプログラム等への電子署名に使用する。 |

3 証明書の発行申請~利用開始ま での流れ

証明書を取得したい場合、証明書利用者は、登録

分局に証明書の発行申請を行います。発行申請を受けつけた登録分局は、申請内容を審査の上、運営主体に発行申請を行います。証明書の発行申請から受領までの流れは、図-2のとおりです。





次に、発行件数が多い職責証明書の発行について、 概要を説明します。

(1) 職責証明書を格納できる媒体等の準備

証明書の発行申請及び利用にあたって、表 - 2のとおり、証明書を格納する鍵格納媒体(ICカード等)と端末で動作させるための環境を整備する必要があります。製品の型番等詳細につ

いては、LGWANポータルサイトの「ICカードを使用する場合の必要なシステム環境」**5及び「認証基盤用ICカード等の動作検証実施状況」**6を参照してください。なお、証明書の鍵格納媒体(ICカード・USBトークン)とICカードを利用する場合のリーダライタ等の調達は、各団体の負担となります。

表-2 鍵格納媒体の種類

| 鍵格納媒体の形状 | 鍵格納媒体以外で調達する必要がある物品 | 製品提供会社 |
|----------|--|-----------|
| ICカード | ICカードドライバ(ソフトウェア・別売) ICカード読取装置 ICカード読取装置ドライバ(ソフトウェア・別売) ICカードフォーマッタ(別売) | 三菱電機株式会社 |
| ICカード | ICカード読取装置 (ドライバソフトウェアとフォーマッタは付属) | ペンティオ株式会社 |
| USBトークン | なし | |

http://center.lgwan.jp/use/third2_3.html

^{% 6} http://center.lgwan.jp/information/second2.html#PKI_Ikou

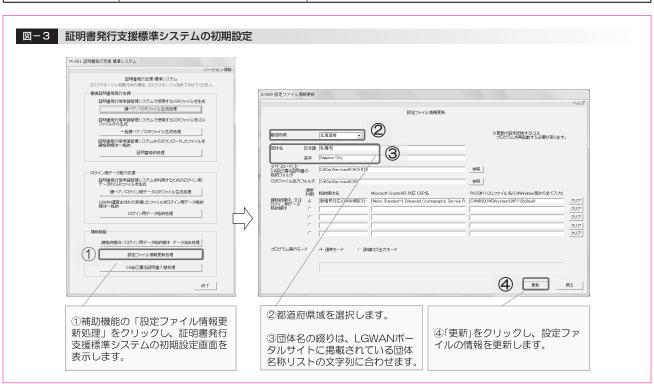


(2) 利用するシステム、費用負担

職責証明書の発行(更新)には、機能の異なる2 種類のシステムを利用します(表-3)。登録分局 からの申請に基づく証明書発行の費用は、都道府県 負担金により賄われており、システムの利用につい ての費用負担は必要ありません。

表-3 利用するシステム

| システム名 | 機能 | 利用方法 |
|---------------------------|---|---|
| 証明書発行支援標準システム*7 (図-3) | | 証明書の利用者がLGWANポータルサイトからダウンロードして、端末にインストールして利用する。 ◆プログラム及び操作マニュアル (http://center.lgwan.jp/library/second9.html#K-3-3) |
| 証明書発行等申請管 理システム (CIRS) | ・登録分局から運営主体への証明 書発行申請及び発行された証明 書をダウンロードする際に利用 するシステム | |



- ※7 証明書発行支援標準システムでは、職責証明書、利用者証明書、メール用証明書及びコードサイニング証明書のCSRファイルを生成できます。
 - 暗号化通信用等証明書とWebサーバ証明書を発行するためのCSRファイルは、サーバ上で生成します。暗号化通信用等証明書とWebサーバ証明書のCSRファイルの生成方法については、自治体中間サーバー・プラットフォームの操作マニュアルまたはウェブサーバの操作マニュアルを確認してください。
- ※8 対になる二つの鍵を使ってデータの暗号化/復号化を行う「公開鍵暗号方式」で使用する、本人のみが保有する「秘密鍵」とそれに対応する「公開鍵」のこと。PKIの仕組みについては、市販の解説書などを参照してください。
- ※9 証明書を発行する際の元となるデータのこと。



(3) 鍵ペアとCSRファイルの作成

最初にICカード(USBトークン)を初期化し、 任意のPIN番号(パスワード)を設定します。ICカードをICカード読取装置にセット(又はUSBトークンを端末に接続)したら、標準システムを起動し、「鍵ペア/CSRファイル生成処理」のメニューで鍵ペアとCSRファイルを作成します(図-4)。

処理が完了すると、鍵ペアがICカード(USBトークン)の中に作成され、CSRファイルは、図 -4-④に設定されたフォルダへ書き込まれます。この CSRファイルを電子媒体(USBメモリ等)へ格納します。



① 図-4の「証明書記載事項」には「名 義」と「組織」を入力する項目があり ます。当該項目に情報を入力する際は、 事前に次の作業が必要です。

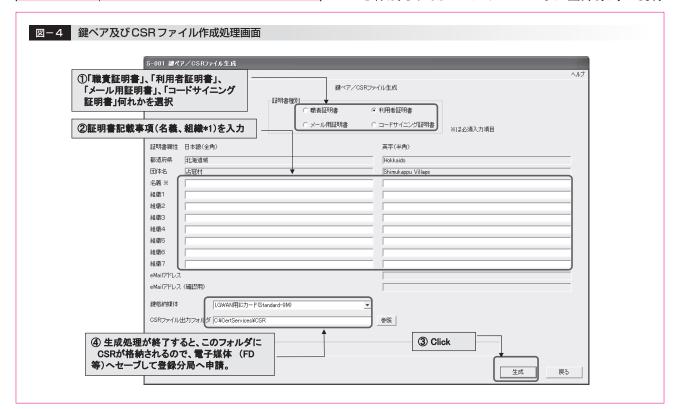
- ◆職責証明書・利用者証明書・メール用 証明書・コードサイニング証明書 「組織」に入力する情報はあらかじめ「組 織管理システム*10」で登録されている 必要があります。
- ◆利用者証明書 「組織」に加え、「名義」に入力する情報を、 あらかじめ「アカウント等管理システム*10」

で登録しておく必要があります。

② 本作業で使用したICカードは、登録分局から証明書を受領するまで大切に保管してください。証明書の格納処理を実施する前にフォーマット等を行った場合、証明書の格納ができなくなり、再度証明書の発行申請を行う必要があります。

(4)証明書発行申請書の作成及び登録分局への証明書発行申請

CSRファイルを作成した後、証明書発行申請書*11 を作成し、CSRファイルとともに登録分局の受付



- ※10 組織管理システム及びアカウント等管理システムはLGWAN運用担当者が利用するシステムのため、登録状況については、 LGWAN運用担当者に確認してください。
- ※11 証明書発行申請書等、登録分局に提出する各種様式については、「LGPKI証明書利用者の手引 様式」を参照してください。 (http://center.lgwan.jp/library/second3.html#F-2-1-5)



担当者に提出します。

(5) 証明書発行申請受付・審査~運営主体への証 明書発行申請

登録分局は、受けつけた証明書発行申請の内容を 処理記録票*12に基づいて審査します。

内容に問題がなければ、「証明書発行等申請管理 システム (CIRS)」を利用して、運営主体に証明書 の発行申請を行います(図-5)。

(6)証明書発行

運営主体は、登録分局からの証明書発行申請の受 付・審査を行い、証明書を発行します。

(7)証明書ダウンロード及び証明書利用者への配付

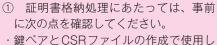
運営主体での証明書発行作業が完了したら、登録 分局は、申請管理システムを利用して、証明書をダ ウンロードします (図-6)。 ダウンロードした証 明書を電子媒体に格納し、証明書発行通知とともに 証明書利用者に配付します。

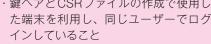
(8) 証明書格納作業

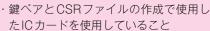
証明書利用者は、登録分局から配付された証明書

をICカード (USBトークン) に格納します。 $\lceil (3) \rceil$ 鍵ペアとCSRファイルの作成 | の作業で使用した 端末とICカード(USBトークン)を準備して、標 準システムのメニューから「証明書格納」を選択し、 格納作業を実施します(図-7)。

格納処理は、1枚のICカードに対し、職責証明 書の格納とCA自己署名証明書(ブリッジCA及び 組織CA) の格納の2回に分けて実施します。





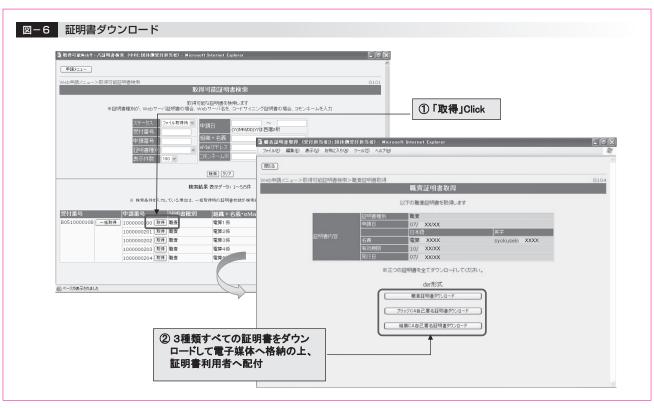


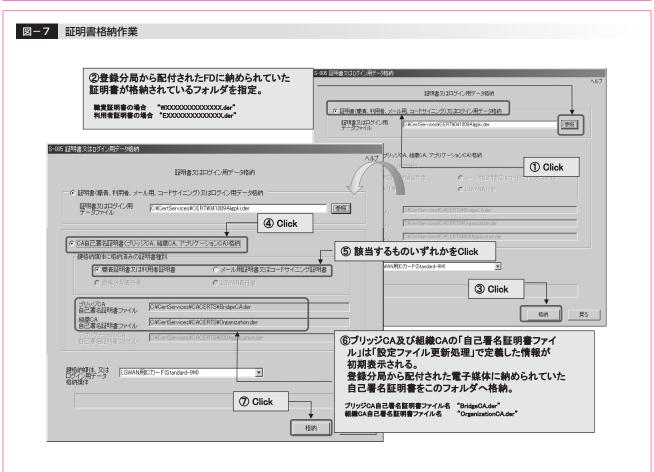
② Windows機能の「証明書のインス トール」を実行すると、証明書をICカー ドに格納することができなくなります。 実行してしまった場合、ICカードを初 期化し、「(3) 鍵ペアとCSRファイル の作成」から作業をやり直す必要があ ります。また、格納できなかった証明 書については、失効申請を行います。



※12 処理記録票等、登録分局が利用する各種様式については、「LGPKI登録分局運営の手引様式」を参照してください。(http:// center.lgwan.jp/library/second3.html#F-2-1-4)









4

おわりに

今月号では、証明書発行申請から受領までの作業 の概要を説明しました。

登録分局の業務の詳細は、「F-2-1-4 LGPKI登録 分局運営の手引*13」において説明していますので、 確認をお願いします。

最後に、平成28年度の登録分局自己点検について、 次のとおりご案内します。

【平成28年度の登録分局自己点検について】

平成28年度の登録分局自己点検については、平成28年6月30日(木)を報告期限として、実 施をお願いしています。未実施の登録分局におかれては、速やかに自己点検を実施してください。 詳細は、http://center.lgwan.jp/information/second2.htmlを確認してください。

なお、例年、期限内に自己点検の実施結果を報告されない団体が多数見受けられますので、期 限までに報告されますようよろしくお願いします。

また、自己点検の実施状況については、LGWANポータルサイトに掲載します。

○登録分局自己点検実施状況(随時更新)

(http://center.lgwan.jp/information/second2.html)

※13 LGPKI 登録分局運営の手引(http://center.lgwan.jp/library/second3.html#F-2-1-4) 登録分局の運営・整備における必要な事項並びに証明書発行等申請における登録分局の手続等について説明した資料

LGWAN-ASPサービス登録/接続状況(平成28年4月1日現在)

LGWAN-ASPサービス提供者の登録/接続状況は次のとおりです。

■アプリケーション及びコンテンツ 登録:546件 ■ホスティング 接続:347件

■通信 登録:182件 ■ファシリティ 登録:342件

登録/接続済のLGWAN-ASPサービス提供者のリストは、下記URLに掲載しています。

https://www.j-lis.go.jp/lgwan/asp/servicelist/cms_15764241.html