



LGWAN

Local Government Wide Area Network

総合行政ネットワーク



➤ 特集 LGPKI（前編）～証明書の発行手続～

地方公共団体組織認証基盤（以下「LGPKI」という。）^{※1}は、LGPKIにおける電子証明書の発行及び失効（以下「発行等業務」という。）並びに発行申請及び失効申請の内容の審査及び登録（以下「登録等業務」という。）を行うため、地方公共団体が共同して設けた公開鍵基盤（PKI：Public Key Infrastructure）としての認証局です。

LGPKIでは、地方公共団体が総合行政ネットワーク（以下「LGWAN」という。）又はインターネットを使用して住民又は企業等に対し電子行政サービスを提供する際に、地方公共団体の組織の真正性を認証するための機能、地方公共団体が使用するWebサーバ等の真正性を認証するための機能並びに地方公共団体間及び地方公共団体とLGPKI以外の認証基盤を用いる外部の機関との間の相互認証を行うための機能を設けております。

また、これらの機能に必要な電子証明書は、地方公共団体が自らこれを利用するほか、LGWAN運営協議会がLGWANの機能の提供を受けることができることとされた承認団体及びLGWAN-ASPサービス提供者が利用することができます。

LGWAN運営主体は、LGWAN運営協議会の定めるところにより、LGPKIの運営主体として、電子証明書の発行、登録業務並びに必要な規程の整備等を行います。また、地方公共団体には、当該団体における証明書の利用者からの発行申請及び運営主体から発行された証明書の利用者への配付等を行うため、登録分局を設けています。

今月号と来月号の2回にわたり、LGPKIが発行する証明書について、その種類、発行手順、証明書の利用等について説明します。今月号では、まず、証明書の発行申請方法についてご説明します。来月号では、LGPKIが発行する証明書の利用例並びに現在登録分局で対応いただいている登録分局自己点検についてご説明します。

1 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、メール用証明書、Webサーバ証明書及びコードサインング証明書の5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。

2 証明書の発行申請から利用開始までの流れ

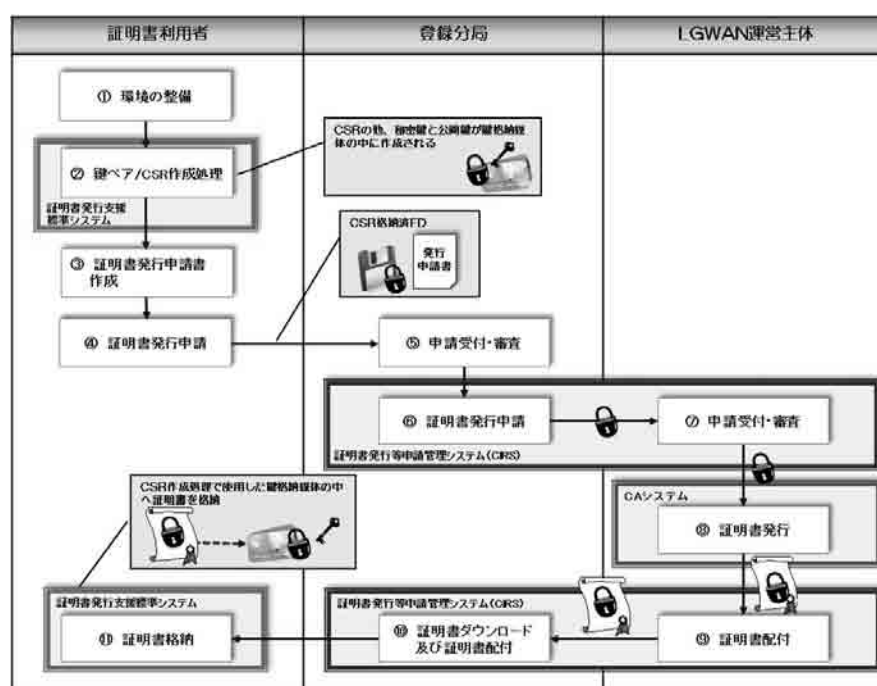
証明書を取得したい場合は、LGWAN接続団体（各地方公共団体）に設置されている登録分局（LGWAN運営主体への申請窓口）に対し証明書の発行申請を行います。発行申請を受け付けた登録分局は、申請内容を審査の上、LGWAN運営主体に発行申請を行います。証明書の発行申請から受領までの流れは図-1のとおりです。

※1 LGPKIの目的と概要については、本誌平成23年10月号「LGPKI特集」を御参照ください。

表-1 証明書の種類と用途

証明書	用途
職責証明書	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。
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。
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Webサーバに適用し、SSL等の暗号化通信に使用する。
コードサイン証明書	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。

図-1 証明書の申請から受領までの流れ



次に各作業の概要を説明します。

(1) 環境の整備

証明書の発行申請並びに利用に当たっては、表-2のとおり証明書を格納する鍵格納媒体（ICカード等）を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^{※2}。

また、図1-②の鍵ペア^{※3}と証明書発行要求^{※4}（以下「CSR」（Certificate Signing Request：署名リクエスト）という。）の作成等を行うための専用ソフトウェア「証明書発行支援標準システム^{※5}（以

- ※2 製品の型番等詳細については、「ICカードを使用する場合に必要なシステム環境」(http://center.lgwan.jp/use/doc/CSR_kankyoku20111018.pdf)を参照してください。なお、一部の証明書では、鍵格納媒体としてUSBトークンも利用できますが、ICカードを利用する場合が多いことから、本特集ではICカードの利用を前提としています。
- ※3 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。
- ※4 証明書を発行する際の元となるデータのこと。
- ※5 証明書発行支援標準システム及び操作手順書はLGWANポータルサイトからダウンロードできます。(<http://center.lgwan.jp/library/index.html#K-3-3>)
 なお、Webサーバ証明書の場合、CSRはWebサーバ機器で作成します。

表-2 必要なハードウェア及びソフトウェア

製品名	説明
LGWAN用ICカード	ICカード媒体
LGWAN用ICカードドライバソフトウェア	ICカード媒体を端末で動作させるためのソフトウェア
LGWAN用ICカードフォーマッタ	ICカード媒体を初期化させるためのソフトウェア
LGWAN用ICカード読取装置	ICカード媒体を端末へ読み書きさせる装置
LGWAN用ICカード読取装置ドライバソフトウェア	ICカード読取装置を端末で動作させるためのソフトウェア

図-2 鍵ペア及びCSR作成処理画面



ここも確認！

- ①図2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・コードサイン証明書
「組織」に入力する情報はあらかじめ「組織管理システム」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」に入力する情報はあらかじめ「アカウント等管理システム」で登録されている必要があります。これらのシステムは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。
- 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。

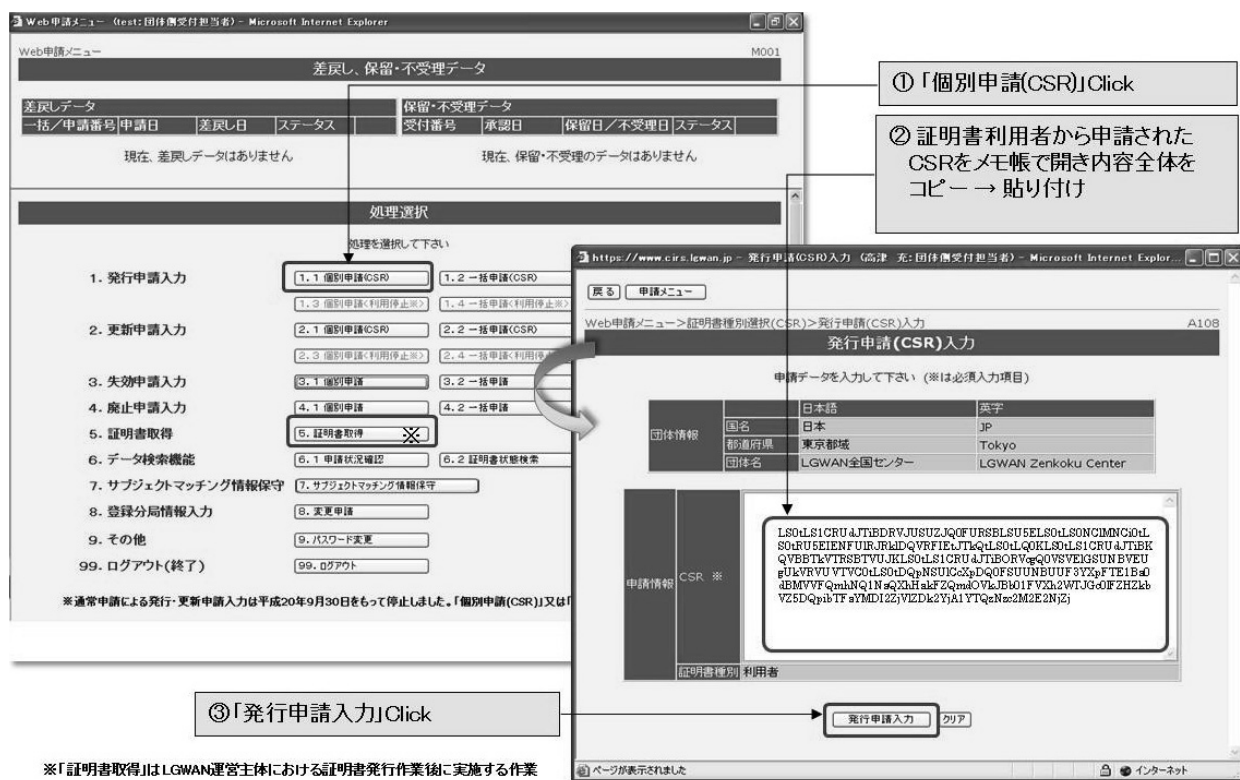
下「標準システム」という。)を利用予定の端末にインストールし、「設定ファイル情報更新処理」を実行して標準システムを利用するために必要な初期設定を行う必要があります。

(2) 鍵ペアとCSRの作成

鍵ペアとCSRの作成に当たり、まずICカードフォーマッタでICカードを初期化し、任意のPIN番号(パスワード)を設定してください。次にICカードをICカード読取装置にセットして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を作成します(図-2)。

処理が完了すると、鍵ペアがICカードに作成され、CSRは図2-④に設定されたフォルダに書き込

図-3 LGWAN運営主体への証明書発行申請



まれます。このCSRを電子媒体（フロッピーディスク等）へ格納します。

(3) 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を作成した後、証明書発行申請書^{※6}を作成し、CSRとともに登録分局の受付担当者に提出します。

(4) 証明書発行申請受付・審査からLGWAN運営主体への証明書発行申請

登録分局は、受け付けた証明書発行申請書の内容を処理記録票^{※7}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^{※8}」（以下「申請管理システム」という。）を利用して、LGWAN運営主体に証明書の発行申請を行います（図-3）。

(5) 証明書発行

LGWAN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。

(6) 証明書ダウンロード及び証明書利用者への配付

登録分局は申請管理システムの「申請状況確認」で申請した証明書のステータスが「ファイル取得待」であることを確認した後、証明書をダウンロードします（図-4）。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。

(7) 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カードに格納します。「(2) 鍵ペアとCSRの

※6 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>）

※7 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>）

※8 証明書発行等申請管理システム（CIRS）<https://www.cirs.lgwan.jp>

図-4 証明書ダウンロード

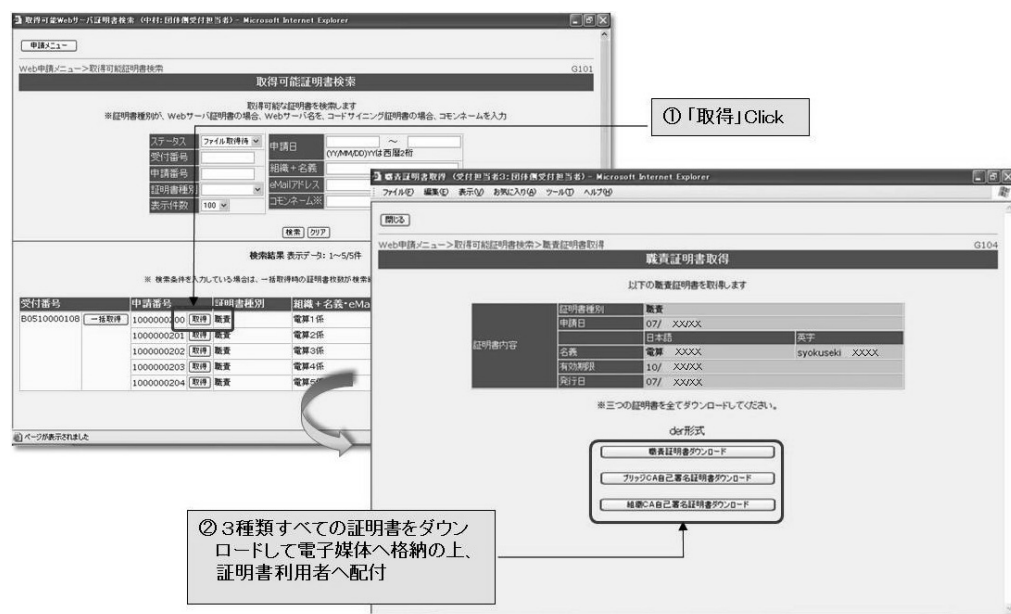
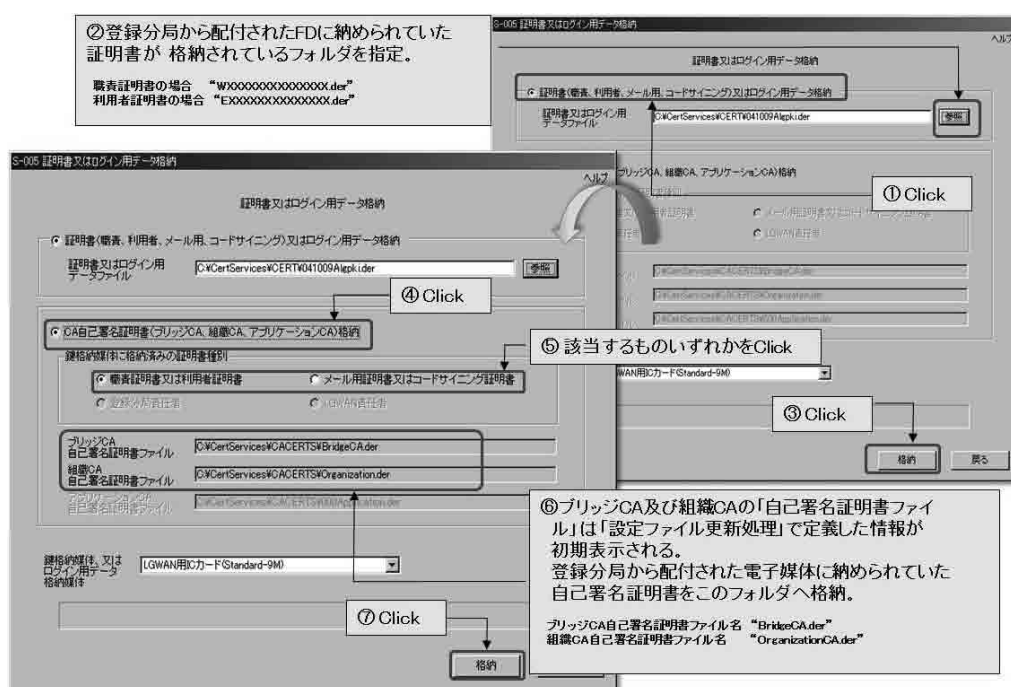


図-5 証明書格納作業



作成」の作業で使用した端末とICカードを準備して、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-5）。

格納処理は、1枚のICカードに対し、証明書（職責等）の格納とCA自己署名証明書（ブリッジCA等）

の格納の2回に分けて実施します。

以上が証明書発行申請から受領までの作業の概要です。詳細については、次のドキュメント（表-3）を参照してください。



ここも確認！

①証明書格納処理に当たっては、事前に次の点を確認してください。

- ・鍵ペアとCSRの作成で使用した端末を利用し、同じユーザでログインしていること
- ・鍵ペアとCSRの作成で使用したICカードを使用していること

②証明書をICカードに格納することができなくなるので、Windows機能の「証明書のインストール」は絶対に実行しないでください。実行してしまった場合は、ICカードを初期化し、図1-②「鍵ペア/CSR作成処理」から作業をやり直す必要があります。なお、格納できなくなった証明書については、失効申請を行う必要があります。

4 証明書の有効期限について

証明書の有効期限は3年です。証明書を継続使用する証明書利用者は、証明書更新申請を行ってください。更新申請手続は発行の場合と基本的に同じで、新しい鍵ペアとCSRを作成の上、「証明書更新申請書」を添えて登録分局へ提出します。

更新申請は、有効期限満了の6ヵ月前から可能で

す。LGPKIが発行する証明書は、LGMANだけでなく、電子入札システム、電子申請等多くの地方公共団体の電子行政サービスで利用されていますので、証明書の有効期限を失念することがないように、十分余裕をもった更新申請の手続きとなるよう留意される必要があります^{※9}。

表-3 証明書発行等申請関連のドキュメント

登録分局向けの資料	
◆LGPKI登録分局運営の手引	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 (http://center.lgwan.jp/library/second3.html#F-2-1-4)
◆証明書発行等申請管理システム操作手順書	登録分局がLGMAN運営主体への証明書発行等申請、発行後の証明書をダウンロードする際に使用するシステムの操作手順書 (http://center.lgwan.jp/library/second9.html#K-3-1)
証明書利用者向けの資料	
◆LGPKI証明書利用者の手引	証明書利用者が行う証明書発行等申請並びに発行された証明書の入手に関する手続等について説明した資料 (http://center.lgwan.jp/library/second3.html#F-2-1-5)
◆証明書発行支援標準システム操作手順書	証明書利用者が鍵ペア/CSRの作成並びに登録分局から受領した証明書を鍵格納媒体に格納する際に使用するシステムの操作手順書 (http://center.lgwan.jp/library/index.html#K-3-3)

3 証明書の利用に係る費用負担について

LGPKIにおける証明書の利用に係る地方公共団体の料金は、無償です。

ただし、証明書の発行等申請に必要なハードウェア及びソフトウェアについては地方公共団体の負担で準備します。

今回は、証明書の発行申請方法についてご説明しました。

新年度を迎え、組織改編等で新しい組織の証明書の発行が必要となる場合には、ぜひ本特集を参考にいただければと考えます。

次回は、LGPKIで発行した証明書の利用例並びに現在登録分局で対応いただいている登録分局自己点検についてご説明します。

※9 証明書の更新申請については、平成22年9月6日付センター発1109号の通知 (<http://center.lgwan.jp/information/doc/LGPKIoshirase20100906.pdf>) を参照ください。

LGMAN-ASPサービス接続／登録状況 (平成24年4月13日現在)

LGMAN-ASPサービス提供者の接続／登録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: 293件	■ホスティング	接続: 180件
■通信	登録: 167件	■ファシリティ	登録: 223件

接続／登録済のLGMAN-ASPサービス提供者のリストは、下記URLに掲載しております。

<http://www.lasdec.or.jp/cms/15,0,41.html>