Local Government Wide Area Network
総合行政ネットワーク
No. 96

特集

LGPKIとは？

地方公共団体組織認証基盤（以下「LGPKI」という。）は、地方公共団体職員が通信回線上で電子文書の送受信を安全に行うための技術基盤です。今月号では、LGPKI登録分局担当者又はLGPKIに関心のある方を対象に、LGPKIの目的、役割及び仕組み等について説明します。また、本文最後には、LGPKIから発行された証明書の有効期限に関して、大事なお知らせがございます。

1 LGPKIの概要

LGPKI（Local Government Public Key Infrastructure）は、大切な情報資産について、盗聴や改ざん、なりすましなどの脅威から守るための技術である「PKI（Public Key Infrastructure）」の仕組みを地方公共団体に提供することを目的に整備されたものです。このLGPKIを構成する主な要素としては、「電子証明書」（以下「証明書」という。）及び証明書を発行する「認証局」があります。今回は、この二つの要素を中心に説明します。

1－1　証明書の概要

従来の対面による紙文書の手続きとは異なり、通信回線による電子文書の送受信では相手方の顔を見ることができません。特にインターネット上においては、第三者による文書の「盗聴」や「なりすまし」、第三者又は受信者による「改ざん」などの危険があります。電子文書をこれらのような脅威から守るために必要となるものが、認証局が発行する証明書です。

（1）盗聴の防止

証明書の基本的な仕組みの一つとして、証明書に含まれている「電子的な錠前（による施錠）」とその錠前に対応する「電子的な鍵（による解錠）」によって、電子文書の秘匿性を保証するというものがあります。（図－1－1）

例えば、送信者が電子文書を金庫のようなものに格納し、それを錠前で施錠して通信回線上において送信し、受信者が受けとった金庫に施錠された錠前を開ける電子的な鍵で解錠すれば、電子文書が安全に送信者から受信者に送られることになり、電子文書を盗聴から守ることができます。

（2）改ざん、なりすましの防止

もう一つの仕組みに、証明書に含まれている「電子的な印影（の照合）」とその印影に対応する「電子的な印鑑」によって、電子文書の真正性を保証するというものがあります。（図－1－2）

図－1－1　証明書を利用した電子文書の送受信（盗聴の防止）

図－1－2　証明書を利用した電子文書の送受信(改ざん､なりすましの防止)

表－１　公開鍵、秘密鍵及び証明書で実現できること

項目	説明	暗号化時 （秘匿性の保証）	電子署名時 （真正性の保証）
公開鍵	通常、認証局が発行する電子証明書に含まれる。 不特定多数に公開。 対応する秘密鍵が一つ存在する。	暗号化する時に使用する鍵。「電子的な錠前」に相当するもの。 送信者は「受信者の公開鍵」を使用して電子文書等を暗号化する。	電子署名の検証時に使用する鍵。「電子的な印影（の照合）」に相当するもの。 受信者は「送信者の公開鍵」を使用して印影を照合する。
秘密鍵	公開鍵に対応する本人のみが有する鍵。対応する公開鍵が一つ存在する。 本人が厳重に管理し、他の者は使用できない。	暗号文を復号する時に使用する鍵。「電子的な鍵」に相当するもの。 受信者は暗号化された電子文書等を「受信者自身の秘密鍵」を使用して復号する。	署名時に使用する鍵。「電子的な印鑑（の押印）」に相当するもの。 送信者は「送信者自身の秘密鍵」で電子文書へ押印する。
証明書	公開鍵と、その公開鍵の所有者の情報が記載されたもの。 公開鍵自体のほか、その公開鍵が誰の秘密鍵に対応したものであるかを証明する。 不特定多数に公開。	送信者は受信者の証明書に記載されている公開鍵を用いて暗号化する。	受信者は送信者の証明書に記載されている公開鍵を用いて送信者を確認する。
ポイント		※秘密鍵は本人しか有していない情報であるため、本人以外は暗号文を復号できない。（暗号化は誰でも可）	※秘密鍵は本人しか有していない情報であるため、本人以外は署名できない。（検証は誰でも可）

秘密鍵は本人が厳重に管理する（＝本人のみ利用できる）鍵です。LGPKIが発行する証明書に係る秘密鍵は、格納された鍵が読み出せない鍵格納媒体（ICカード等）に格納されるため、秘密鍵が漏れる心配はありません。、ただし、悪意ある第三者が鍵格納媒体及び鍵格納媒体に設定されたパスワード一覧等を持ち出して、これを使用することによる「なりすまし」を防ぐために、証明書利用者は鍵格納媒体及びパスワードの取扱いは厳重に管理する必要があります。

例えば、送信者が作成した電子文書に電子的な印鑑を押印し、通信回線上において送信し、受信者が電子文書にある電子的な印鑑の印影が正しいかどうか照会できれば、電子文書の送信者が特定でき、なりすましが防止できます。また、改ざんの防止も、「電子的な印影（の照合）」とその印影に対応する「電子的な印鑑」を使って実現することができます。

（３）証明書が証明するものとは

PKIの世界では、「電子的な錠前」と「電子的な印影（の照合）」を「公開鍵」、「電子的な鍵」と「電子的な印鑑」を「秘密鍵」と呼び、ある「公開鍵」には対応する「秘密鍵」が一つ存在する、という特徴があります。

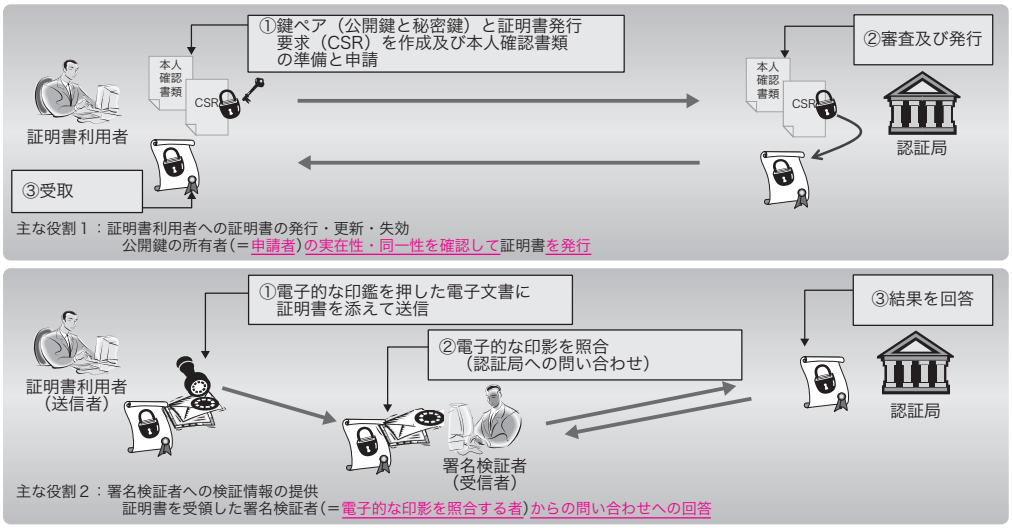
証明書には、この「公開鍵」とその「秘密鍵」のうち、「公開鍵」とその所有者の情報が記載されています。公開鍵、秘密鍵及び証明書について表－１にまとめます。

１－２　認証局の概要

１－１で説明したような通信回線上の脅威から電子文書を守るために必要となる証明書は、認証局が

LGPKIでは、申請者とLGWAN運営主体との仲介役となる登録分局が、申請者からの証明書発行申請を受け付け、申請者の実在性・同一性の確認の後、LGWAN運営主体へ証明書発行申請を行い、発行された証明書を申請者へ配付します（登録分局とLGWAN運営主体とのやりとりは「証明書発行等申請管理システム」を利用します）。なお、登録分局は、LGWAN参加団体単位に設置することが規定されております。

図－２　認証局の主な役割



表－２　主な認証局

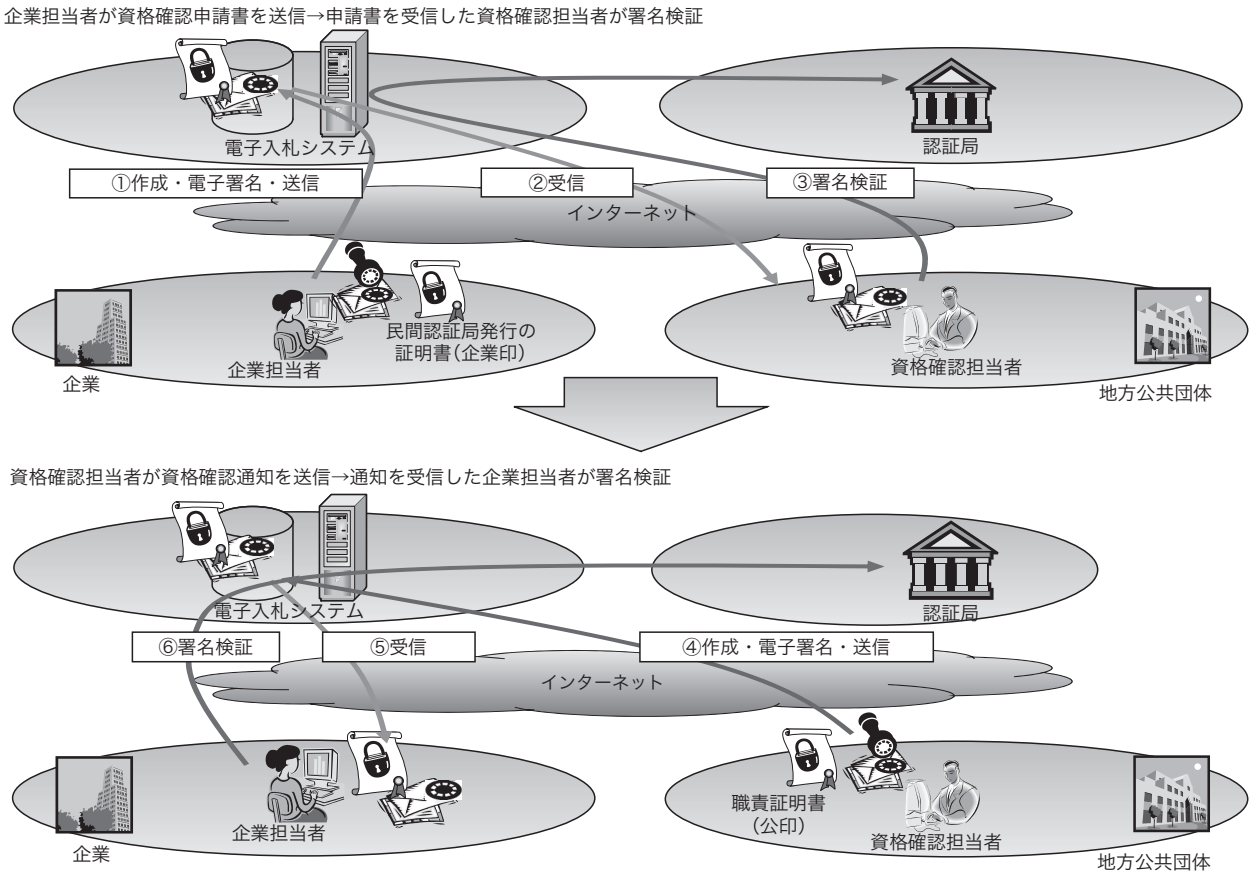
項目	説明
官職認証局（GPKI）	総務省が運営する政府認証基盤（通称「GPKI」）にある認証局で、電子文書を送信する国の職員の官職等に対して官職証明書を発行しています。
組織認証局（LGPKI）	総合行政ネットワーク運営協議会が運営する地方公共団体組織認証基盤（通称「LGPKI」）にある認証局で、電子文書を送信する地方公共団体職員の職責者に対して職責証明書を発行しています。
公的個人認証局（JPKI）	電子署名に係る地方公共団体の認証業務に関する法律（通称：公的個人認証法）に基づき都道府県が運営する（通称「JPKI」）認証局です。電子証明書は住民登録をしている市区町村の都道府県知事より発行されます（発行の手続きは市区町村で行います。鍵格納媒体である住民基本台帳カードの交付が事前に必要です。）。
商業登記認証局	商業登記に基づく電子認証制度の制定に伴い法務省が運営する認証局で、電子文書を送信する法人に対して電子証明書を発行しています。
民間認証局	電子署名法の制定に伴い民間企業が運営する認証局で、個人、法人等を問わず電子文書を送信するインターネット利用者に対して電子証明書を発行しています。

発行します。認証局は、証明書の発行を希望する申請者から申請書類を受け取り、その内容を審査（申請者の実在性・同一性を確認）の上、証明書を発行します。

また、認証局は、過去に発行した証明書が有効であるかどうかの情報を提供しています。例えば「電子的な印鑑」で送信者が電子文書等へ押印した「電子的な印影」を受信者が照合する際、受信者はその印鑑が現在も有効かどうかを認証局へ問い合わせ、認証局がその有効性（証明書が偽造されたものではないか、失効されたものではないか）を回答します。つまり、「証明書の発行」を行うだけではなく、「証明書の有効性」に係る情報を提供することも認証局の重要な役割です（図－２）。

現在ではこのような認証局が、証明書発行対象者別に整備されています（表－２）。例えば、公的個人認証（JPKI）の認証局では、全国の市区町村に証明書の発行窓口が設けられており、日本国民（該当市区町村に居住する住民）向けに証明書を発行しています。ここで発行される証明書は、従来の対面と紙文書による行政手続きにおいて利用されていた印鑑証明書に替わる「電子的な印鑑」と

図－３　電子入札システムにおける利用例



※上図の④（電子署名）で職責証明書が利用されています。

して、住民向けインターネット行政手続きに利用することができます。

2　LGPKIが発行する証明書の利用例

LGPKIでは、５種類の証明書（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及びWebサーバ証明書）を発行していますが、その中でも職責証明書、利用者証明書及びWebサーバ証明書の発行実績が多く、これらの証明書が様々な用途に利用されています。

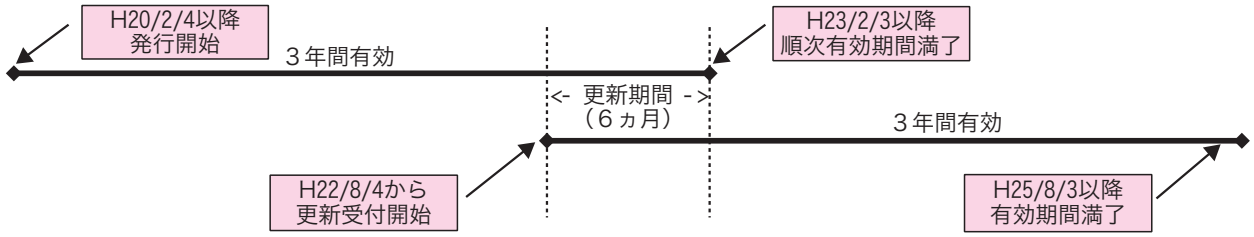
２－１　職責証明書の利用例

職責証明書は、地方公共団体職員が電子政府／電子自治体システムと通信回線（インターネット又はLGWAN）を利用して、住民、企業等と電子文書の送受信を行う場合に利用できるもので、「電子的な公印」の役割を果たします。図－３は、地方公共団体の電子入札システムにおいて、企業の入札担当者及び地方公共団体の資格確認担当者が相互に電子署名を利用するケースを例示したものです。

職責証明書は、地方公共団体／企業間で利用される電子入札システムの他、主に次に挙げる電子政府／電子自治体システムで利用されています。
・地方公共団体／住民間で利用される電子申請システム
・政府／地方公共団体間で利用される電子申請／申告システム（e-Tax等）
・政府／地方公共団体間又は地方公共団体／地方公共団体間で利用されるLGWAN電子文書交換システム

LGPKI発行のWebサーバ証明書が「社会的に信頼された認証局から発行されたものかであるか」をWebブラウザに自動的に確認させるためには、Webサーバ証明書を発行したLGPKIアプリケーション認証局の「自己署名証明書」を事前にWebブラウザにインストールしておく必要があります。ただし、インターネット環境でInternet Explorerを利用する場合は、この事前操作は不要です。認証局の信頼性について、アプリケーション認証局が「WebTrust for CA」という国際的な検証基準を取得しているため、ブラウザ提供者において事前にインストールされているからです。これにより、運用セキュリティも高く確保されています。

図－４　証明書の有効期限と証明書の更新



２－２　Webサーバ証明書の利用例

Webサーバ証明書は、例えば地方公共団体が運用する電子自治体システム等が稼働するWebサーバ（Webサイト）と住民、企業等のPC（Webブラウザ）とのインターネット通信を行う際に、通信しようとしているWebサーバが住民や企業等が確かに意図したWebサーバなのかを確認した上で、Webサーバとの間の通信が盗聴されないよう通信内容を暗号化する場合に利用できます。このような通信を行う際は、WebサイトからWebブラウザへWebサーバ証明書が自動的にダウンロードされます。この時Webブラウザは、この証明書が「社会的に信頼された認証局から発行されたものか」を自動的に確認し、問題がないと確認できればそのまま暗号化通信が開始されます。

3 LGPKIからのお願い

LGPKIが発行する証明書の有効期限は３年です。平成20年２月に、地方公共団体組織認証基盤の運営体制を抜本的に見直し、新たに設置したLGPKI組織認証局へ移行されてから現時点（平成22年10月現在）で２年８ヵ月が経過していますので、開設当初に発行された職責証明書及び利用者証明書は、４ヵ月後の平成23年２月以降に、順次、有効期限を迎えます（図－４）。

職責証明書及び利用者証明書を継続使用する証明書利用者は、有効期限満了の６ヵ月前から更新申請

LGWAN責任者、登録分局責任者の「ログイン用カード」又は「ログイン用データ」も組織認証局から発行されていますので、平成23年２月３日以降にログイン用カード又はログイン用データの有効期限が満了します。LGWAN運営主体ではログイン用カード又はログイン用データの有効期限満了６ヵ月前から更新申請を受け付けていますので、有効期限を確認の上、LGWAN運用担当者、登録分局受付担当者におかれましても更新申請の手続きが必要となります。

更新申請を行う際は、次の点に御注意ください。

①更新申請を行ってから新しい証明書が届くまでの間は証明書の利用ができません。有効期限満了６ヵ月前以降、証明書の利用がない時期を選んで更新申請を行ってください。
②更新申請時期によっては新しい証明書が届くまでに１週間以上の時間を要することが想定されます。有効期限満了直前ということにならないよう、相当の余裕を持ったスケジュールをもって更新申請を行ってください。

を行うことができます。現在の証明書利用者は、証明書の有効期限を確認していただき、「証明書発行支援標準システム」を利用してCSR（証明書発行要求：証明書利用者が証明書発行申請を行う際に認証局へ提出する電子データ）を作成の上、必要事項を記入した「証明書更新申請書」を添えて登録分局へ提出する必要があります。この更新手続きを行うことで、更新された日からさらに３年間が有効期間となります。

また、LGPKI組織認証局移行当初には多くの証明書が発行されています。当時に証明書の発行を受けた証明書利用者が、有効期限満了直前（平成23年１月～２月ごろ）に一斉に更新手続きに入りますと、登録分局、LGWAN運営主体双方において更新作業が集中することになりますので、新しい証明書が届くまでに１週間を超えるような事態が予想されます。できるだけ余裕をもって更新作業に着手され、平準化にご協力をお願いします。

LGWAN-ASPサービス接続／登録状況（平成22年９月９日現在）

LGWAN-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	191件	■ホスティング	接続	109件
■通信	登録	159件	■ファシリティ	登録	206件

接続／登録済のLGWAN-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.nippon-net.ne.jp/cms/15,0,41.html