LGWAN
Local Government Wide Area Network
総合行政ネットワーク

No. 135

特集　LGPKIとは？

地方公共団体が住民・企業等との間で実施する電子申請・届出等の手続き、また、地方公共団体相互の電磁的記録文書のやり取りにおける様々な脅威を防止し、安全に通信を行うために、公開鍵基盤（Public Key Infrastructure、以下「PKI」という。）の仕組みを地方公共団体向けに提供するものが地方公共団体組織認証基盤（Local Government PKI、以下「LGPKI」という。）です。

本特集では、LGPKIの目的と概要、LGKPIで発行する電子証明書（以下「証明書」という。）の種類及び利用例について説明します。

1　脅威から文書を守る仕組み ～PKI～

通信相手が見えないインターネット上で文書をやり取りする場合、盗聴、改ざん、なりすまし、事後否認といった脅威があります。これらの脅威から文書を守り、安全に通信を行うために、PKIの仕組みを利用することで、図－1のような対策を取ることができるようになります。

「暗号化」及び「電子署名」は、PKIの構成要素である「公開鍵暗号方式」を利用して行います。公開鍵暗号方式では、表－1に示す「公開鍵」と「秘密鍵」の対となる二つの鍵を使ってデータの暗号化／復号化を行います。また、一方の鍵で暗号化した情報は、対になるもう一方の鍵を使わないと復号化できないという特長があります。

それでは、公開鍵暗号方式を利用して、どのように脅威から文書を守ることができるかを説明します。

（1）暗号化による盗聴対策

①文書の暗号化

盗聴対策では、受信者以外の人は文書を読めないようにする、つまり、受信者だけが暗号化された文

図－1　想定される脅威とその対策

想定される脅威	どのような対策が必要？	具体的な対策
盗聴	通信相手以外は情報が読めないようにする	暗号化
改ざん	情報に変更が加えられたら分かるようにする	電子署名
なりすまし	通信相手が誰か分かるようにする	電子署名
事後否認	文書を送信したあと、その事実を否認できないようにする	電子署名

書を復号化できるようにする必要があります。そのため、送信者は、受信者の公開鍵※1を使って文書を暗号化し、暗号化した文書を受信者に送信します。

②文書の復号化

受信者が受け取った文書を復号化する際に利用するのが、暗号化に利用された公開鍵と対になる受信者の秘密鍵です。秘密鍵は、受信者本人しか保有していないため、仮に第三者が文書を入手したとしても文書を復号化することはできません。そのため、盗聴を防止し、文書の秘匿性が保たれます（図－２）。

なお、秘匿性を確保するため、本人以外の者が秘密鍵を利用することがないように、秘密鍵を格納した媒体は安全に管理することが重要です。

（２）電子署名による改ざん、なりすまし、事後否認を防止する対策

①電子署名の付与

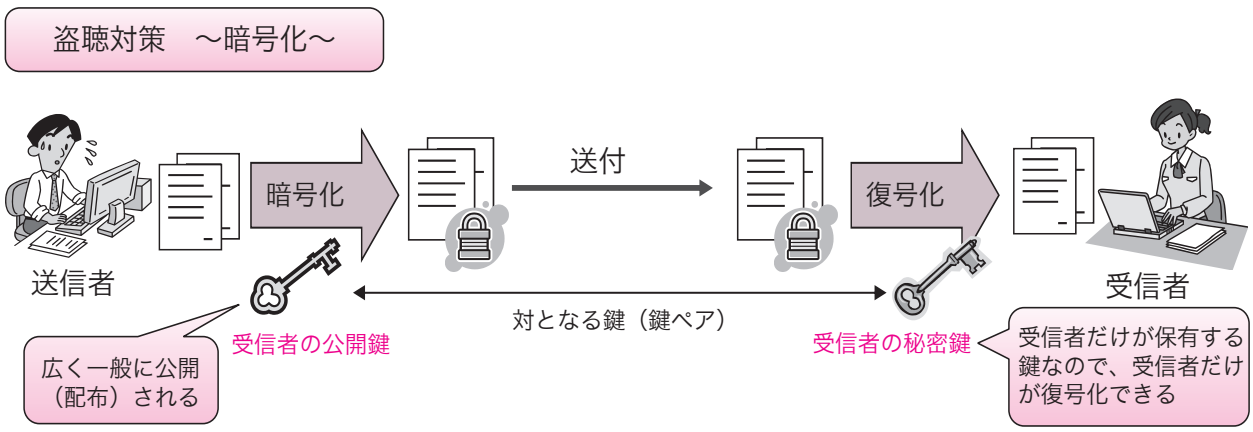
送信者は、作成した文書から、特殊な「データ※2」を生成し、このデータを暗号化して電子署名を作成します。電子署名によって、文書が送信者本人から送信されたものであることを受信者が確認できるようにするため、電子署名の作成には、送信者が保有する秘密鍵を利用します。作成した電子署名は、文書と一緒に送ります。

②改ざん、なりすまし、事後否認の有無の確認

表－１　公開鍵暗号方式で利用する鍵の種類

鍵の種類	用途
公開鍵	広く一般に配布することを前提とした鍵で、電子署名の確認や、ファイルの暗号化において利用する。
秘密鍵	公開鍵に対応する、本人だけが保有する鍵で、電子署名の作成や暗号化されたファイルの復号化の際に利用する。

図－２　暗号化による盗聴対策



※１　受信者の公開鍵は、本人から直接又はリポジトリ（認証局で発行した証明書やその他の関連情報を公開したデータベース）からダウンロードして入手します。

※２　生成したデータは、「メッセージダイジェスト」と呼ばれます。メッセージダイジェストから元の文書を復元することはできません。また、元の文書に変更が加えられると、メッセージダイジェストは元の内容とは異なるため、改ざんの有無を検出することができます。

受信者は、まず送信者の公開鍵を使って電子署名を復号化します。送信者の公開鍵で復号化できれば、暗号化に使用した鍵が送信者の秘密鍵であることになります。秘密鍵は送信者しか持たない鍵なので、送られた文書が送信者本人から送信されたものであることの証しとなります。また、送信者が文書を送った事実を後で否認することを防止します。

次に、受信した文書から送信者と同じ方法で「データ※2」を作成し、電子署名を復号化して得たデータと比較します。同じ結果の場合、このデータの持つ特長から、文書が改ざんされていないことの証明となります（図－３）※3。

（３）証明書と認証局

図－２と図－３において、文書の暗号化と電子署名の復号化の際に通信相手の公開鍵を利用しましたが、公開鍵を利用する前にその所有者を確認する必要があります。このときに証明書が必要になります。

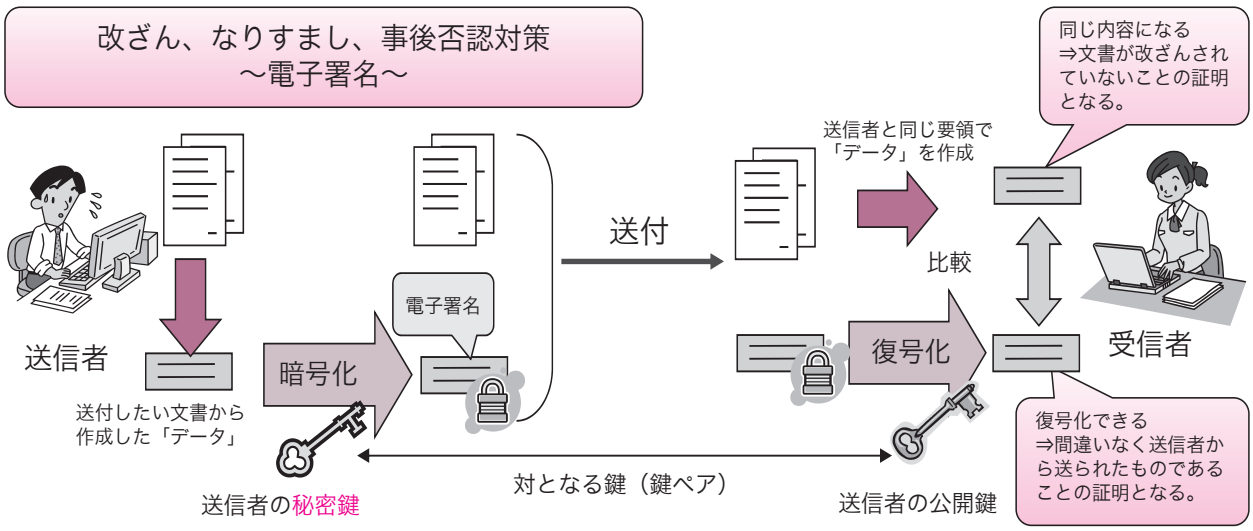
証明書は、公開鍵とその所有者の結びつきを証明するもので、証明書には、公開鍵、その所有者、証明書の有効期限等の情報が含まれます。証明書は、認証局と呼ばれる信頼できる第三者の専門機関が発行し、その内容を保証します。公開鍵の利用者は、証明書の内容を認証局が設置する証明書の有効性を検証するシステムに問い合わせることで、その公開鍵の所有者とその有効性を確認することができます。

2 LGPKIとは

（１）LGPKIの目的と概要

LGPKIの証明書の発行は、地方公共団体の職責者、アプリケーションの利用者、さらには、業務システムのサーバ、プログラムコード及び電子メールを対象としています。LGPKIの認証局は、電子文書等の送受信において、LGPKIの証明書の発行を受けた証明書利用者が、地方公共団体の職員又は地方公共団体が提供する情報システムであることを保証します※4。

図－３　電子署名による改ざん、なりすまし、事後否認対策



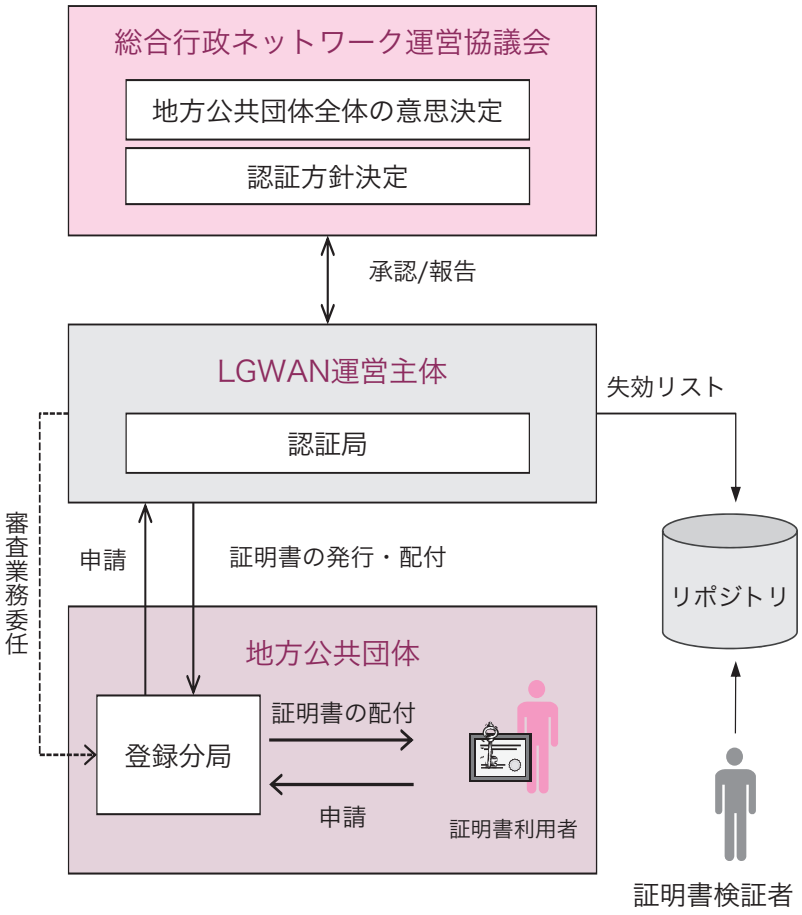
※３　暗号化や電子署名の付与などの一連の処理は、実際にはシステムで自動化されているのが一般的です。
※４　LGWAN-ASPサービス提供者に対しても、地方公共団体に対してASPサービスを提供するWebサーバ及び地方公共団体に配布するプログラムコードに限り証明書を発行しています（ただしLGWAN-ASPですから、LGWAN内に閉じたASPサービスに限ります）。

LGPKIを利用することによって、地方公共団体が住民・企業等との間で実施する申請・届出等の手続き、また、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、事後否認といった脅威を防止し、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。

（2）LGPKIの構成組織

LGPKIの運営における構成組織は図－４のとおりです。LGPKIの運営に関する意思決定は、すべての都道府県及び市区町村の代表で構成される総合行政ネットワーク運営協議会（以下「協議会」という。）が行います。協議会が決定した証明書ポリシー※5（CP：Certificate Policy）及び認証局運用規程※6（CPS：Certification Practice Statement）に従い、LGWAN運営主体である財団法人地方自治情報センターが認証局を運営し、証明書の発行業務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。また、証明書利用者は、所属する地方公共団体（LGWAN接続団体）内に設置された「登録分局※7」を経由して、LGWAN運営主体に証明書の発行等申請を行います。登録分局では、証明書発行等申請における証明書利用者の実在性、同一性の確認を行い、認証局に対し発行等申請をするとともに発行された証明書を申請者に配付するといった役割を担います。

図－４　LGPKIの構成組織



（3）LGPKIの認証局及び発行証明書の種類

LGPKIの認証局は、図－５のとおり、組織認証局、アプリケーション認証局及びブリッジ認証局の三つの認証局で構成されます。組織認証局では、職責証明書及び利用者証明書を、また、アプリケーション認証局では、Webサーバ証明書、メール用証明書及びコードサイニング証明書を発行しています※8。

一方、ブリッジ認証局は、証明書利用者向けの発行は行わず、政府認証基盤（GPKI）や他の認証局

※５　認証局が発行する証明書の用途等について規定した文書
※６　証明書ポリシーで規定された方針を認証局の運用に適用するための実施手順、約款及び外部との信頼関係等を規定した文書
※７　登録分局の業務については、本誌平成25年６月号の特集記事「LGPKIにおける登録分局の業務について」を参照してください。（https://www.lasdec.or.jp/cms/15,4769,67.html）
※８　組織認証局からは、職責証明書、利用者証明書のほかに、LGWAN運営主体が提供する各システムにログインする際に利用する「ログイン用データ」も発行しています。

との相互認証（互いの認証局を信頼しあうための手段）を行います。これにより、地方公共団体では、国の機関や他の地方公共団体から受け取る公文書、住民・企業等からの電子申請書、地方公共団体から住民・企業等に交付された電子文書等に付与される証明書の有効性検証が自動的かつ効率的に実現されます。

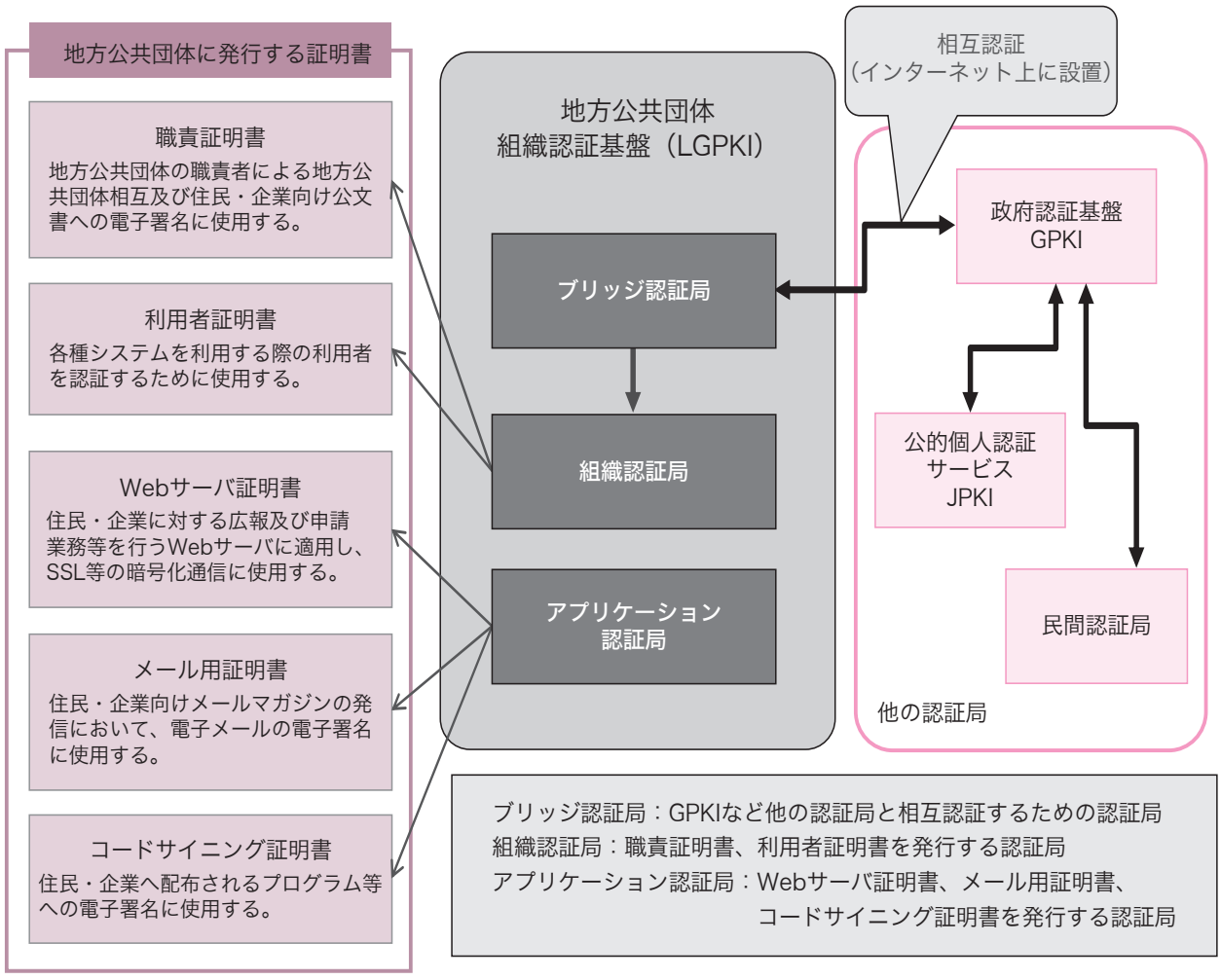
（4）LGPKIが発行する証明書の利用例

LGPKIの証明書は、電子入札、電子申請等の各システムや地方公共団体が設置するWebサイトにおいて利用され、電子行政サービスの提供における文書や申請データの安全な通信を実現します。LGPKIが発行する証明書のうち、職責証明書、利用者証明書及びWebサーバ証明書の利用例を紹介します（表－２）。

3 おわりに

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、地方公共団体相互間の文書のやり取りを安全に行うにあたり、LGPKIは重要な基盤です。多くの方にLGPKIについての理解を深めていただき、LGPKIの一層の利活用を改めてお願いし、本特集を終わります。

図－５ LGPKIを構成する認証局と発行する証明書



表－2　LGPKIの証明書の主な利用例

No.	証明書の種類・用途	システム名称等
1	職責証明書 （電子署名等）	電子入札コアシステム （一般財団法人日本建設情報総合センター（JACIC）） http://www.cals.jacic.or.jp/coreconso/index.html
2		地方税ポータルシステム（eLtax） http://www.eltax.jp/
3		国税電子申告・納税システム（e-Tax） http://www.e-tax.nta.go.jp/
4		特許出願システム（特許庁） http://www.inpit.go.jp/pcinfo/index.html
5		登記・供託オンライン申請システム（法務省） http://www.touki-kyoutaku-net.moj.go.jp/
6		e-Gov電子申請システム（e-Gov：総務省） http://www.e-gov.go.jp/
7	利用者証明書 （利用者認証等）	会計検査院宛電子文書送信ツール（会計検査院） ※本ツールは、都道府県のみ利用します。
8		共通認証サービス※9を利用したLGWAN基本アプリケーション・サービスやLGWAN-ASPサービスにログインするためのLGWANアカウント
9	Webサーバ証明書 （SSL通信）	地方公共団体が運営するWebサイト※10
10		ASPサービス提供者が運営するWebサーバ（電子入札、電子決済及びコンビニ交付等）

※9　共通認証サービスでは、利用者認証を行い、アクセスが許可された利用者に対し、Webアプリケーションのサービスを提供します。

※10　発行の対象となるWeb サーバには、LG.JPドメイン名を付す必要があります（LG.JPドメイン名とは、株式会社日本レジストリサービス（JPRS）が管理するJPドメイン名の一つで、属性型（組織種別型）・地域型JPドメイン名に分類され、インターネット空間において地方公共団体及び地方公務員を収容するためのドメイン名として平成14年に創設されたものです。詳細は、本誌平成25年12月号特集記事「LG.JPドメイン名について」を参照してください）。

LGWANサービス提供設備からLGWAN接続ルータへの移行状況（平成25年12月10日現在）

■LGWAN接続団体　1000/1820団体

■LGWAN-ASP　57（140）/212 ASP

※（　）内は接続団体が自団体の接続ルータを利用してASPサービスを提供する形態を含めた件数です。

LGWAN-ASPサービス登録／接続状況（平成25年12月10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：347件　■ホスティング　接続：212件

■通信　登録：180件　■ファシリティ　登録：279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.lasdec.or.jp/cms/15,0,41.html