特集　LGPKI特集

地方公共団体が住民・企業等との間で実施する電子的な申請・届出等の手続、地方公共団体相互間の文書のやり取りにおける様々な脅威を防止し、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）を担保するための仕組みが地方公共団体組織認証基盤（以下「LGPKI（Local Government Public Key Infrastructure）」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。）の種類及び用途等についてご説明します。

1 電子文書を脅威から守るための仕組み

（1）電子文書等のやり取りにおける脅威

インターネットにおける電子文書のやり取りにおいて、送信者と受信者の間に悪意のある第三者が介入した場合、送信した内容を盗聴･改ざんされたり、送信者になりすまして文書を送信されたりすることなどが考えられます。（図－1）

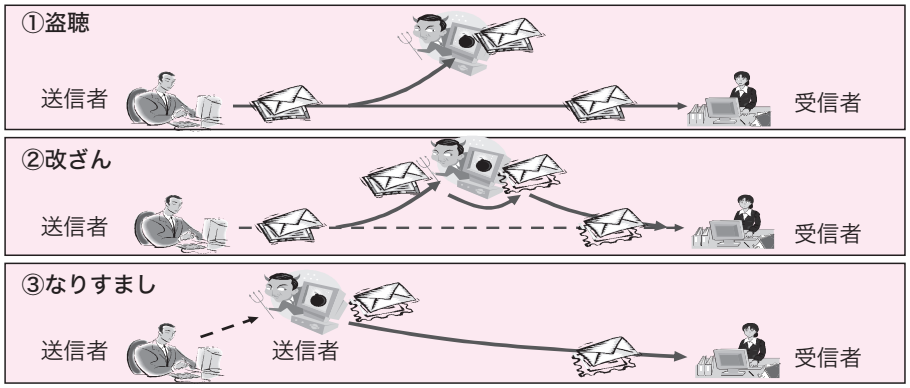
これらの脅威から電子文書を守るために、公開鍵基盤※1（以下「PKI（Public Key Infrastructure）」という。）という仕組みが用いられます。

（2）暗号化による盗聴の防止

PKIの主な構成要素である証明書に用いられている「公開鍵暗号方式※2」によって、文書を暗号化し、文書の秘匿性を保証することができます。

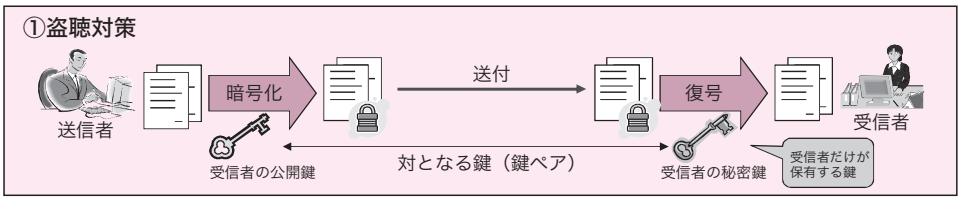
送信者は、あらかじめ受信者本人から入手又はリポジトリ※3からダウンロードした※4受信者の「公開鍵※5」を使って、文書を暗号化し、文書を送信しま

図－1　電子文書等のやり取りにおける脅威

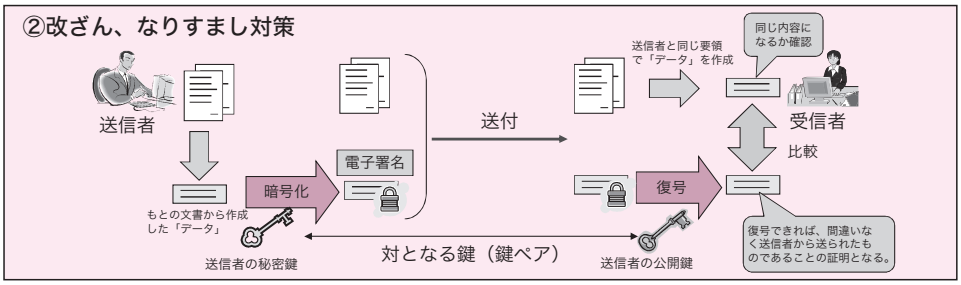


※1　公開鍵暗号方式、証明書、認証局などにより、インターネット上での文書のやり取りにおける脅威から情報資産を守るための仕組み全体を指します。
※2　対になる二つの鍵を使ってデータの暗号化／復号化を行う暗号方式。一方の鍵で暗号化した情報はペアのもう一方の鍵を使わないと復号化できません。
※3　認証局で発行した証明書やその他の関連情報を公開したデータベース。
※4　実際には、公開鍵の入手及び証明書の検証は、システムで自動的に行うのが一般的です。具体例は、「3（2）LGPKIが発行した証明書の利用例」で説明します。
※5　公開鍵暗号方式において用いられる鍵ペアの一方で、秘密鍵に対応する公開している鍵。文書の暗号化、また、電子署名の復号化に使用する鍵。

図－２　盗聴対策



図－３　改ざん、なりすまし対策



す。受信者は、文書を受け取ったら、「公開鍵」と対になっている「秘密鍵※6」を使って暗号化された文書を復号化します。（図－２）

この「秘密鍵」は、文書を受け取った本人しか保有していないため、復号化は、受信者しか行うことができません。したがって、第三者が文書を入手することができたとしても、文書の内容を確認することができないため、文書の秘匿性が保証されます。

（３）電子署名による改ざん、なりすましの防止

電子署名によって、文書の作成者が誰であるか、文書の内容が改ざんされていないかを確認することができます。

送信者は、もとの文書から作成した「データ※7」を送信者の「秘密鍵」で暗号化したもの（電子署名）を、もとの文書、送信者の証明書と一緒に送ります。

受信者は、文書を受け取ったら、まず、送信者の「公開鍵」によって暗号化された「データ」を復号化し、送信者が間違いないことを確認します。次に、もとの文書から送信者と同じ要領で「データ」作成して、内容が改ざんされていないかを確認することができます。（図－３）

（４）証明書はなぜ必要か

文書の暗号化や電子署名の復号化に必要な「公開鍵」は、公開することが前提となっていますが、「公開鍵」を公開しただけでは、その鍵が誰のものか確認する手段がありません。この問題を解決するのが証明書です。

証明書は、「公開鍵」とその所有者情報を結び付けるもので、信頼できる第三者機関（認証局）がその結びつきを証明します。これにより、公開されている「公開鍵」が誰のものであるかを確認することができます（図－４）。

2 LGPKIの目的と概要

LGPKIは、前の章でご説明した、インターネット上で安全に通信をやり取りするための技術的な仕組みであるPKIを地方公共団体に提供することを目的として整備されました。

すなわち、LGPKI証明書の発行は、地方公共団体の職責又は業務システムのサーバ等を対象としており、その利用者は、地方公共団体の職員及び地方

※６　公開鍵暗号方式において用いられる鍵ペアの一方で、公開鍵に対応する本人のみが保有する鍵。文書の復号化、また、電子データに電子署名を付与する際に使用する鍵。

※７　変換後のデータは、「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は復元できず、また、元の文書に変更が加えられると、作成されるメッセージダイジェストは異なる内容になるため、改ざんを検出することができます。

公共団体等が行う情報システムであることをLGPKI認証局が保証します。

LGPKIは、総合行政ネットワーク（以下「LGWAN」という。）に参加している地方公共団体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LGPKIの運営に関する意思決定を行い、協議会が決定した証明書ポリシー※8（CP：Certificate Policy）及び認証局運用規程※9（CPS：Certification Practice Statement）に従って総合行政ネットワーク運営主体である当センターが運営しております。

また、証明書利用者は、所属する地方公共団体（LGWAN参加団体）に設置された「登録分局」を経由してLGWAN運営主体に証明書の発行を申請します。登録分局は、認証局の業務の一部を委任を受け、証明書利用者からの発行申請の受け付け、証明書利用者の実在性・同一性の確認、LGWAN運営主体へ証明書発行申請など、認証局の運営において重要な役割を担っています。

3 LGPKIが発行する証明書及び利用例について

（1）LGPKIで発行する証明書

LGPKIでは、地方公共団体が希望する目的や用途に応じて、５種類の証明書を発行しています（表－１）。

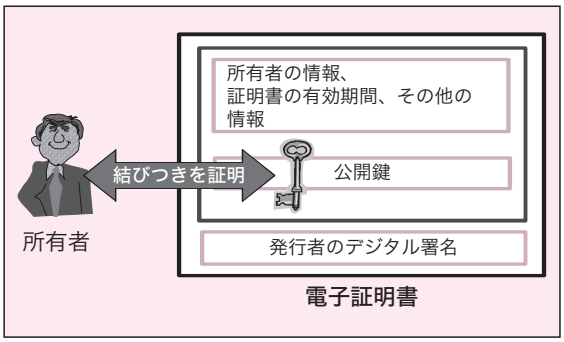
表－１の証明書のうち、職責証明書及びWebサーバ証明書については、主に次のように利用されています。

（2）LGPKIが発行した証明書の利用例

ア　職責証明書

地方公共団体では、住民・企業に対するサービスの向上、行政事務の効率化などを目的として、電子申請／電子入札といった、電子行政サービスを提供しています。

図－４　証明書が証明する内容



住民・企業からの申請や、行政機関からの通知等が、確かにその名義人によって送付されたものか、文書の内容が改ざんされていないかを確認できなければなりません。

職責証明書は、地方公共団体が、住民・企業等と電子文書をやり取りする場合に、改ざんを防止する電子署名の役割を果たします。図－５は電子申請システム／入札システムにおいてLGPKIが発行した証明書を利用するケースを例示したものです。

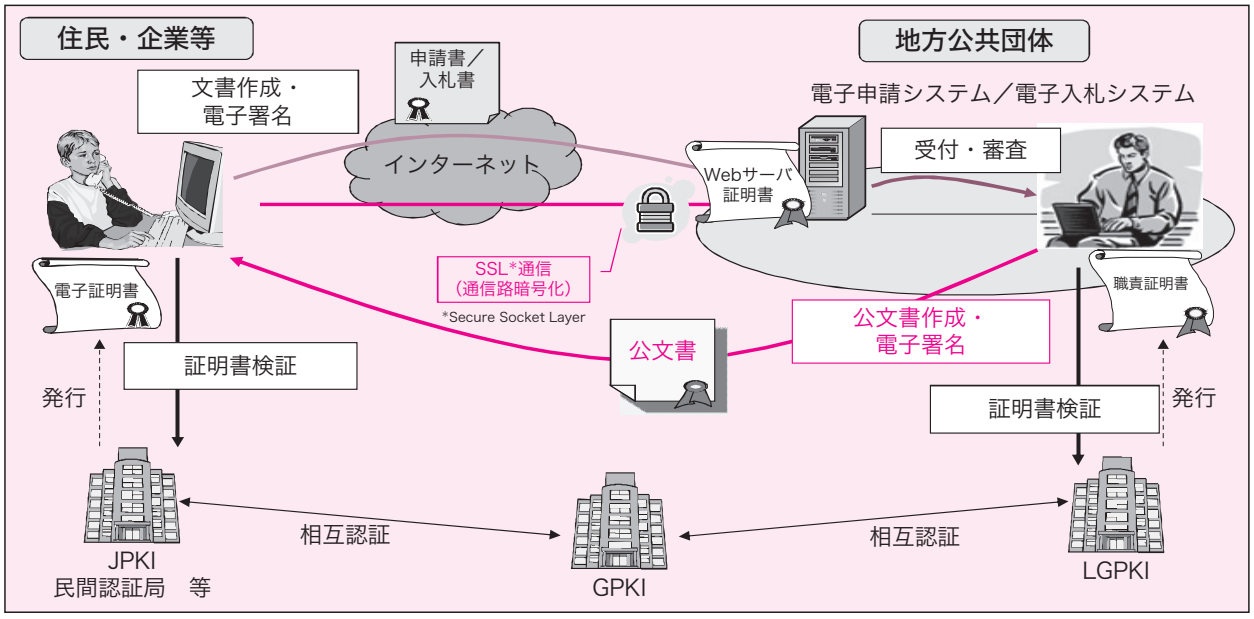
住民・企業等は、JPKIあるいは民間認証局から発行を受けた自らの証明書を用いて、地方公共団体向けの申請書/入札書等に電子署名を付与し、手続を行います。地方公共団体は、申請書等に付与された電子署名や証明書の検証を行い、その証明書が有効であることを確認します。その後、通知を作成の上、職責証明書を用いて文書に電子署名を付与し、公文書として住民・企業等に通知します。住民・企業等は、公文書に付与された電子署名や証明書が有効であることを確認します。これらの検証は、LGPKIと他の認証局間でお互いの認証局を信頼すること（相互認証）により実現されています。また、証明書の検証に当たっては、認証局が提供している、当該認証局が失効した証明書のリストから、証明書

※８　認証局が発行する証明書の用途等について規定する文書。
※９　認証局が行う証明書ライフサイクル管理（発行、更新、失効等）等、運営・運用業務の安全性や信頼性について規定する文書。

表－１　LGPKIが発行する証明書の種類と内容

種類	内容	
（1）職責証明書	目的	電子文書の改ざんとなりすましを防ぐための証明書です。
	用途	送信者が受信者へ送付する電子文書（公文書等）へ電子的な印鑑を押印することができ、その印鑑は、首長、土木部長等の「職責」が電子的に刻印されたものとなります。
	効果	送付した電子文書の内容が改ざんされていないこと、送信者が確実に証明書利用者であることを、受信者に対し保証します。
（2）利用者証明書	目的	各種情報システムを利用する場合の認証、文書署名者の真正性確認、電子文書の盗聴、改ざんとなりすましを防ぐための証明書です。
	用途	各種情報システムにログインする場合の利用者認証として利用することができます。また、送信者がLGWAN電子文書交換システムを利用して、受信者へ電子文書（公文書等）を送付する場合に必要となります。LGWANが提供する共通認証サービスにより、一つの証明書で、複数の情報システムのログインが可能になります。ただし、この証明書に限りLGWAN内部の利用に限定されます。
	効果	送付した電子文書の内容が盗聴、改ざんされていないこと、送信者・ログイン者が確実に証明書利用者であることを、受信者・システム管理者に対し保証することができます。
（3）メール用証明書	目的	電子メールの改ざんとなりすましを防ぐための証明書です。
	用途	送信者が電子メールを利用して受信者向けにメールマガジン等を送付する場合に利用することができます。
	効果	送付した電子メールの内容が改ざんされていないこと、送信者が確実に証明書利用者であることを、受信者に対し保証することができます。
（4）コードサイニング証明書	目的	プログラム等ソフトウェアの改ざんとなりすましを防ぐための証明書です。
	用途	送信者が受信者向けにプログラム等ソフトウェアを配付する場合に利用することができます。
	効果	送付したプログラム等ソフトウェアの内容が改ざんされていないこと、送信者が確実に証明書利用者であることを、受信者に対し保証することができます。
（5）Webサーバ証明書	目的	電子文書の盗聴となりすましを防ぐための証明書です。
	用途	情報システムのサービス側のWebサーバと受信者側のPCとの間の通信の暗号化及びサービスの真正性を確保する場合に必要となるものです。
	効果	サービス側のWebサーバと受信者側のPCとの間の通信が盗聴されていないこと、Webサーバが確実に証明書利用者側のものであることを、受信者側に対し保証することができます。

図－５　電子申請／電子入札システムにおけるLGPKI証明書の利用例



の最新の状態を確認します。証明書を検証する側は、このリストを確認することで、添付された証明書が有効かどうかを知ることができます。

また、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（eTax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

イ　Webサーバ証明書

Webサーバ証明書は、例えば、地方公共団体が運用する情報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、通信先のWebサーバが住民・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「利用者自身が信頼する第三者機関（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。

なお、発行の対象となるWebサーバには、LG.JPドメイン名[※10]を付し、証明書の所定の命名箇所に記載される必要があります。

4　おわりに

地方公共方公共団体が住民・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当たり、重要な基盤となるのがLGPKIです。

本特集で多くの方にLGPKIについての理解を深めていただき、LGPKIの整備並びに利活用の促進につながればと考えます。

※10　（株）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ます。また、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。

LGWAN-ASPサービス接続／登録状況（平成23年９月８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　281件	■ホスティング	接続　172件
■通信	登録　163件	■ファシリティ	登録　217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.or.jp/cms/15,0,41.html