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

No. 156

特集　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

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、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説明します。

## 1　電子文書を脅威から守るための仕組み

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、送信者と受信者の間に悪意のある第三者が介入し、送信した内容を盗聴・改ざんしたり、送信者になりすまして文書を送信したりすることなどが考えられます。想定される脅威とその対策を整理すると、図－１のとおりになります。

これらの脅威から電子文書を守るために、「RSA公開鍵暗号方式」という仕組みが用いられます（表－１）。

**（１）暗号化による盗聴対策**

送信者は、受信者の公開鍵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。暗号化された文書は、受信者だけが持つ秘密鍵で復号化することができます（図－２）。

**（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**

ア　電子署名の付与

送信者は、送付したい文書から、特殊な「データ※1」

図－１　想定される脅威とその対策

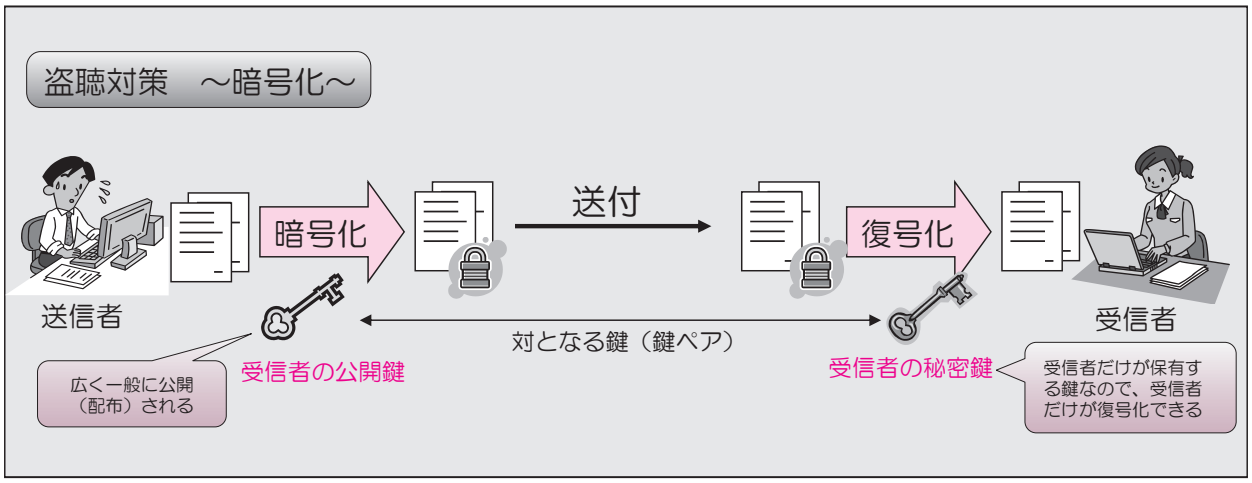
| 想定される脅威 | どのような対策が必要？ | 具体的な対策 |
|---|---|---|
| 盗聴 | 通信相手以外は情報が読めないようにする | 暗号化 |
| 改ざん | 情報に変更が加えられたら分かるようにする | 電子署名 |
| なりすまし | 通信相手がだれか分かるようにする | 電子署名 |
| 事後否認 | 文書を送信したあと、その事実を否認できないようにする | 電子署名 |

※１　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。

**表－1　RSA公開鍵暗号方式について**

| | |
|---|---|
|  <br>ここも確認！ | PKIは、情報セキュリティ技術の中でも、聞きなれない用語が多くなります。ここでは、PKIの説明で頻出の用語を説明します。 |
| RSA公開鍵暗号方式 | 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。 |
| 秘密鍵 | RSA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します。<br>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。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。 |
| 公開鍵 | RSA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します。 |

**図－2　暗号化による盗聴対策**




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。電子署名の作成には、送信者が保有する秘密鍵を利用し、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電子署名によって確認できるようにします。作成した電子署名は、文書と一緒に送ります。

イ　改ざん、なりすまし、事後否認の有無の確認

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が確認できます。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から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」を作成し、電子署名を復号化して得たデータと

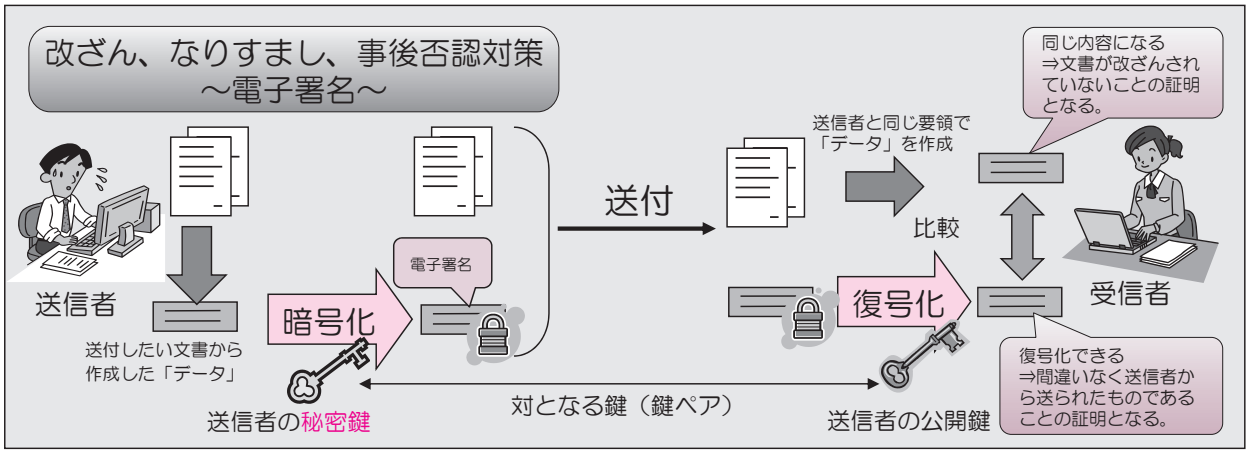
比較※2します。同じ結果の場合、このデータの持つ特長から、文書が改ざんされていないことの証明となります（図－３）。

### （３）証明書と認証局

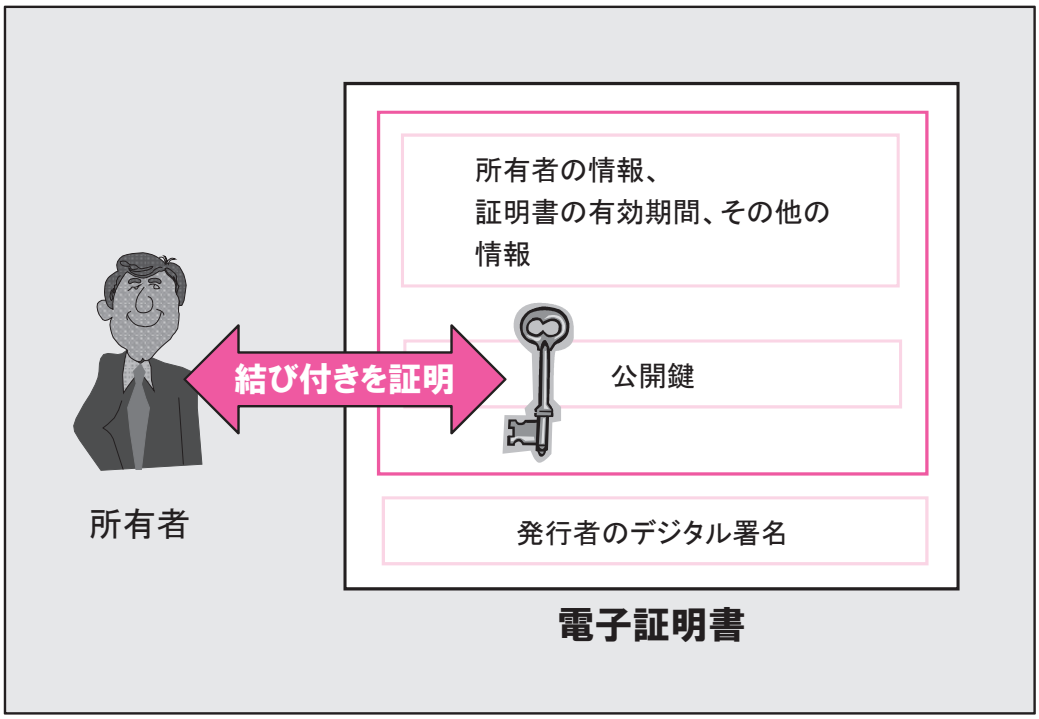
図－２と図－３において、文書の暗号化と電子署名の復号化の際に通信相手の公開鍵を利用しましたが、公開鍵を利用する前にその所有者を確認する必要があります。このときに証明書が必要になります。

証明書は、公開鍵とその所有者の結び付きを証明するもので、証明書には、公開鍵、その所有者、証

**図－３　電子署名による改ざん、なりすまし、事後否認対策**

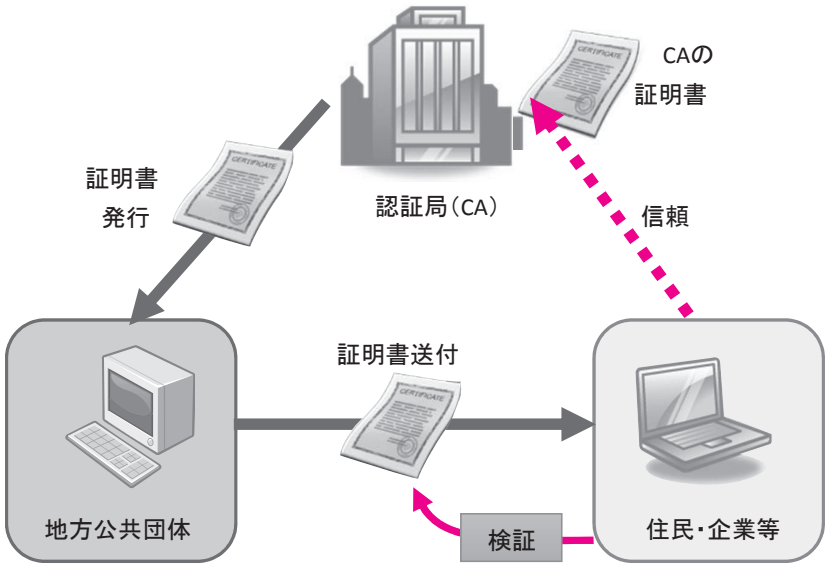



**図－４　証明書が証明する内容**




※２　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。

図－５　証明書の検証




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、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（図－４）。

### （４）証明書の検証

証明書所有者が証明書を使うとき、証明書を受け取る側の人は、証明書を利用する前に、その証明書が信用できることを確認します（図－５）。

証明書の有効性検証は、「認証パスの構築」と「認証パスの検証」の順で行います。

検証したい証明書から出発して信用関係を順にたどり、自分が信用している認証局までの経路を明らかにすることを「認証パスの構築」といいます。また、認証パス上において、信用の基点となる認証局を「信頼点（トラストアンカー）」といいます。

証明書の検証を行うときには、構築した認証パスを使い、信頼点（トラストアンカー）の証明書から順に経路上の証明書の検証を行っていきます。すべての証明書の検証が終わると、証明書の信用性が確認できたことになります。

### （５）認証局の信頼性を確かにする仕組み

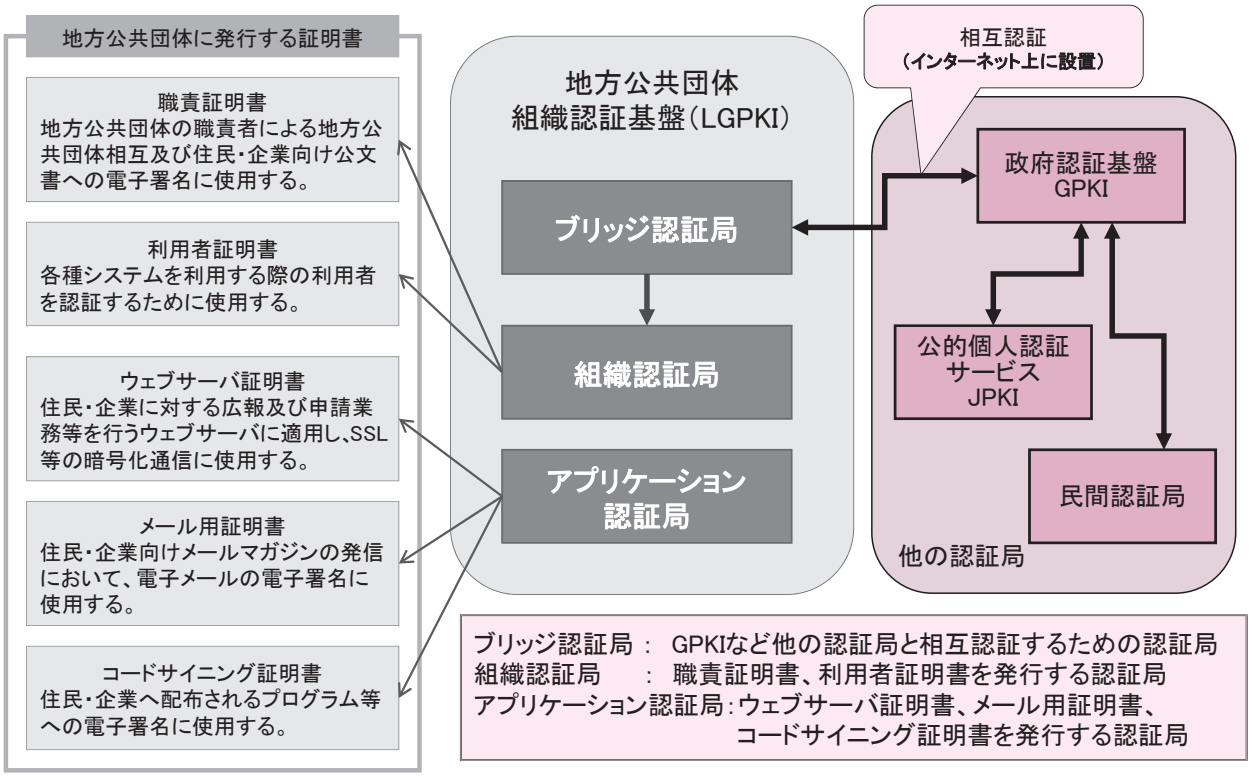
LGPKIは、政府認証基盤（GPKI）と相互認証をしています。相互認証とは、ネットワーク越しに存在する二つの認証局が、お互いの認定結果を信頼しあうことです。GPKIはさらに民間認証局や公的個人認証サービス（JPKI）と相互認証をしています。このように信頼が連鎖していくことにより、地方公共団体が発信する公文書に付与される証明書を受け取った住民・企業等や国の府省では、証明書の有効性を検証することができるようになっています。

また、逆に、地方公共団体では、住民・企業等からの申請書や他の地方公共団体・国（府省）から受け取る公文書などに付与される証明書が有効かどうかを検証することもできます。

## 2　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・届出等の手続き、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、重要な基盤となるのがLGPKIです。LGPKIの証明書は、電子入札、

図－6　LGPKIを構成する認証局と発行できる証明書※3




電子申請等の各システムや地方公共団体が設置するウェブサイトにおいて利用されています（図－6）。

本特集で多くの方にLGPKIに関する理解を深めていただき、LGWAN接続団体における登録分局の整備並びに証明書の利活用の促進につながれば幸いです。

※3　LGPKIで発行できる電子証明書の種類及び利用例については、本誌平成26年1月号・当コーナー（「特集／LGPKIとは？」）で特集しています。

## LGWAN-ASPサービス登録／接続状況（平成27年9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：424件 | ■ホスティング | 接続：262件 |
| ■通信 | 登録：179件 | ■ファシリティ | 登録：329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