特集

地方公共団体組織認証基盤（LGPKI）が発行する証明書について

地方公共団体組織認証基盤（以下「LGPKI」という。）では、地方公共団体職員が安全に電子文書をやりとりするための電子証明書を発行しています。今月号では、電子証明書をご存じでないという方々向けに、LGPKIが発行する電子証明書の概要について、分かりやすく説明します。

1 電子文書のやり取りにおける脅威

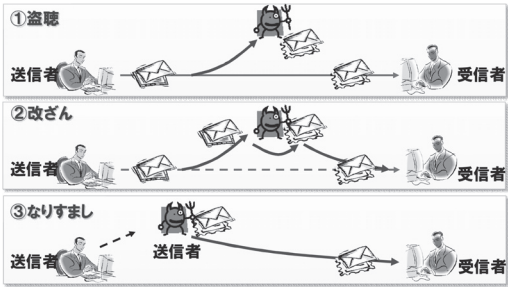
従来の対面による紙文書の手続きとは異なり、通信回線による電子文書のやりとりでは相手方の顔を見ることができません。特にインターネットにおいては、送信者と受信者との間に悪意のある第三者（犯罪者）が介在した場合、文書の内容を盗聴、改ざんされたり、送信者になりすまされたりする危険性があります。

図－１で取り上げた通信回線上の脅威に関する一例として、公共工事における電子入札を考えてみます。電子文書を「入札書」、送信者を「工事事業者」、受信者を「地方公共団体」、悪魔マークを公正な入札を阻害する「犯罪者」と置きかえてみた場合を表－１にまとめます。

2 電子文書を脅威から守るための仕組み

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電子証明書（以下「証明書」という。）です。証明書の基本的な仕組み※1は「電子的な

図－１ 電子文書のやりとりにおける脅威



表－１ 電子入札における脅威

脅威	内容
盗聴 	①　工事事業者は「1,000万円」の入札書を入札締め切り１時間前に地方公共団体へ送信します。 ②　犯罪者は工事事業者の入札金額を読み取ります。この後、犯罪者は締め切り１時間以内にこの金額を他者へ伝え、他者がこの金額よりも安価な金額で札入れします。 ③　地方公共団体は上記②の作為に気づくことなく、他者が落札したとみなします。
改ざん 	①　工事事業者は「1,000万円」の入札書を地方公共団体へ送信します。 ②　犯罪者はこの金額を「１億円」へ書き換えます。 ③　地方公共団体は上記②の作為に気づくことなく、この工事事業者は予定価格を超過したとみなします。
なりすまし 	①　工事事業者は他案件を抱えているため、次の入札参加を見送る予定でいます。 ②　犯罪者がこの工事事業者へなりすまして偽の入札書を地方公共団体へ送信します。 ③　地方公共団体は上記②の作為に気づくことなく、この工事事業者が落札したとみなします。しかし、本物の工事事業者は主任技術者不足から契約できません。この後、このことがきっかけで、この工事事業者は指名停止の処分を受けてしまいます。

錠前※2と鍵※3」によって電子文書の安全性を担保するというものです。例えば、送信者が電子文書を電子的な錠前で施錠（暗号化）して送信し、受信者が送信者の錠前を開ける電子的な鍵で錠前を解錠（復号化）するというものです。また、この電子的な錠前と鍵は、証明書が採用する仕組みの技術的特性上、「電子的な印鑑と印影」に例えることもできます（図－２）。これらのことを踏まえ、前に説明した電子入札における脅威への対応例を表－２にまとめます。いずれの例においても送信者となる工事事業者が証明書を利用することで解決することができます。

3 証明書を発行する認証局

前に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、認証局と呼ばれる組織が発行しています。例えば全国の市区町村に証明書の発行窓口が設けられている公的個人認証サービス（略称：JPKI）認証局では、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押印されていた印鑑に替わる「電子的な印鑑※4」として、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。LGPKIも認証局です。JPKI認証局の証明書発行対象者が日本国民であること

図－２ 電子的な錠前と鍵を使った電子文書の送受信

表－２ 電子入札における脅威への対応例

対応策	内容
盗聴の対応例	① 工事事業者は「1,000万円」の入札書を入札締め切り１時間前に地方公共団体へ送信します。このとき、入札書は証明書を利用して暗号化します。 ② 犯罪者は暗号化された入札金額を限られた時間内に解読することができません。よって、犯罪者はこの金額を他者へ伝えることもできません。 ③ 地方公共団体は正しい入札書をもとに、公正な開札を行うことができます。
改ざんの対応例	① 工事事業者は「1,000万円」の入札書を地方公共団体へ送信します。このとき、入札書を電子的な印鑑で押印します。 ② 犯罪者はこの金額を「１億円」へ書き換えます。 ③ 地方公共団体は開札の際、電子的な印鑑で押印された印影をシステムで自動的に確認します。この時、上記②の作為（入札金額が電子的な砂消しゴムで書き換えられていること）に気づくことができますので、この後に再入札を実施することができます。
なりすましの対応例	① 工事事業者は他案件を抱えているため、次の入札参加を見送る予定でいます。 ② 犯罪者がこの工事事業者へなりすまして偽の入札書を地方公共団体へ送信します。 ③ 地方公共団体は開札の際、電子的な印鑑で押印された印影をシステムで自動的に確認します。この時、上記②の作為（印影が本物の工事事業者印ではないこと）に気づくことができますので、この後に再入札を実施することができます。

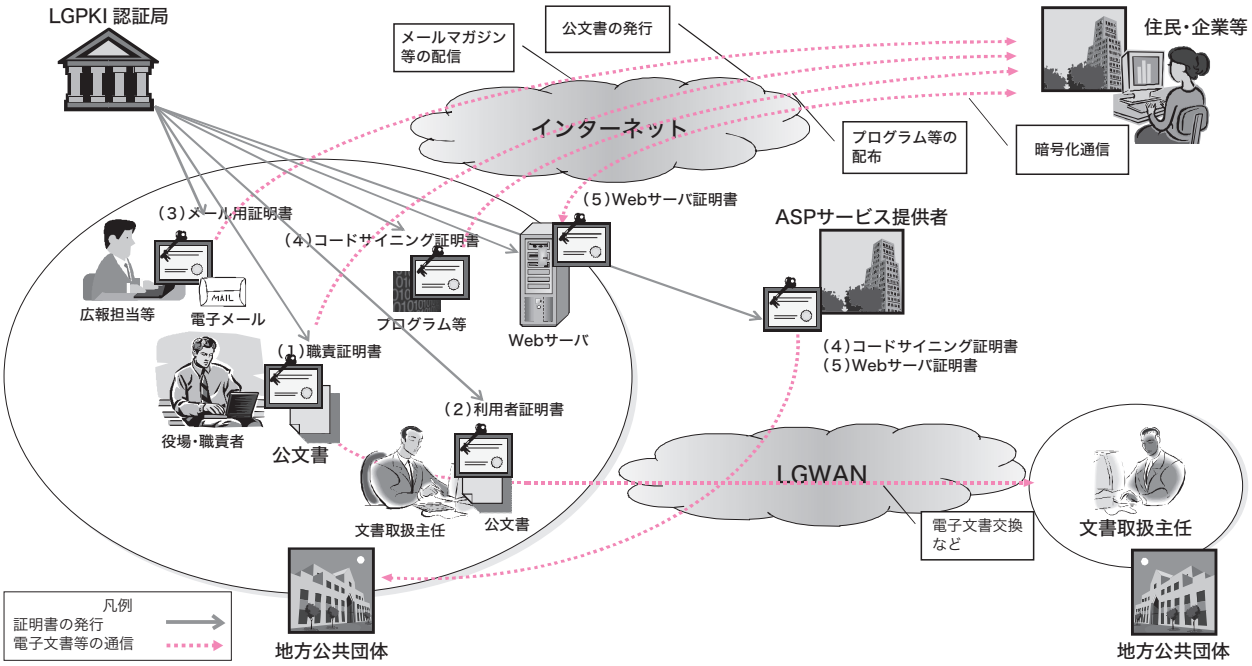
実際に運用されているシステムでは、例示した「電子的な錠前と鍵」、または「電子的な印鑑と印影」の仕組みを複雑に組み合わせる、または基本的な仕組みを応用する形で構成することで、通信回線上の電子文書を悪意ある第三者の犯罪から保護しています。

※１ LGPKIでは、“Public Key Infrastructure”（略称［PKI］）というインターネットをはじめとした通信回線上で電子文書を安全に送受信するための標準的な仕組みを採用しています。この仕組みは、政府認証基盤（GPKI）や公的個人認証サービス（JPKI）等でも採用されています。なお、LGPKIの前の２文字“LG”は、“Local Government”の略称です。
※２ ここでいう電子的な錠前は、PKIの世界では「公開鍵」と呼ばれています。
※３ ここでいう電子的な錠前を開ける鍵は、PKIの世界では「秘密鍵」と呼ばれています。

表－３　主な認証局と対象者

認証局	対象者
GPKI 認証局	総務省が運営する政府認証基盤（通称「GPKI」）と呼ばれる認証局で、電子文書を送信する国の職員の官職等に対し官職証明書を発行しています。
LGPKI 認証局	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」）と呼ばれる認証局で、電子文書を送信する地方公共団体職員の職責等に対し職責証明書を発行しています。
JPKI 認証局	電子署名に係る地方公共団体の認証業務に関する法律（公的個人認証法）に基づき都道府県知事が各市町村の住民基本台帳に登録された住民向けにJPKIから電子証明書を発行しています。
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ともない法務省が運営する認証局で、電子文書を送信する法人代表者に対し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ともな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向けに電子証明書を発行しています。

図－３　LGPKIが発行する証明書の利用イメージ



に対し、LGPKIにおける証明書発行対象者は地方公共団体の役職や業務システムのサーバ等となります。現在では、このような認証局が証明書発行対象者別に複数存在しています（表－３）。

4 LGPKIが発行する証明書と利用例

LGPKIでは、電子文書の送信者となる地方公共団体職員（以下「証明書利用者」という。）が希望される用途に応じて５種類の証明書を発行しています（図－３）。

表－４にまとめたLGPKIが発行する証明書の内、特に多くの方々に利用されているものとして、職責証明書、利用者証明書及びWebサーバ証明書があり、主に次のように利用されています。

職責証明書は、証明書利用者が電子自治体システムとインターネットを利用して、住民、企業等と電

※４　従来の紙による住民向けの各種行政手続きの中には、印鑑証明書が必要となるものが多くあります。この意味において、インターネット行政手続きで利用されるJPKI認証局発行の証明書は、「電子的な印鑑証明書」にも例えられます。

表－４　LGPKIが発行する証明書の種類と内容

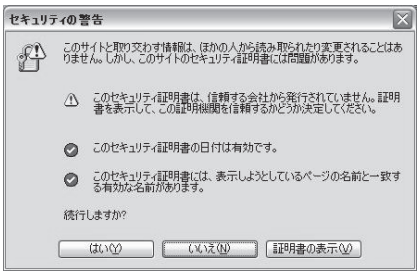
種類	受信者	内容	
（1）職責証明書 	国、他の地方公共団体、住民、企業等	目的	電子文書の改ざんとなりすましを防ぐための証明書です。
		用途	送信者が受信者へ送付する電子文書（公文書等）へ電子的な印鑑を押印することができ、その印鑑は、首長、土木部長、情報政策課長等の「職責」が刻印されたものとなります。
		効果	送付した電子文書の内容が改ざんされていないこと、送信者が確実に証明書利用者であることを、受信者に対し保証することができます。
（2）利用者証明書 	国、他の地方公共団体	目的	文書署名者の真正性確認、電子文書の盗聴、改ざんとなりすましを防ぐための証明書です。
		用途	送信者がLGWAN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るもので、その印鑑は、文書取扱主任等の「名義」が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盗聴、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。
（3）メール用証明書 	住民、企業等	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 	住民、企業等	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布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 	住民、企業等	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	送信者側の（電子自治体システム等が稼働する）Webサーバと受信者側のPCとの間の通信を暗号化する場合に必要となるものです。
		効果	送信者側の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。

子文書のやりとりを行う場合に利用できます。職責証明書は、前の事例に説明した電子入札システムの他にも、電子申請や電子申告システム等、多くの電子自治体システムで利用できます。また、次に説明する利用者証明書とともに、LGWAN電子文書交換システムでも利用できます。いずれの利用事例においても､送付した電子文書が証明書利用者の「職責」で送付されたかどうか、また改ざんされていないかどうかを電子的に確認することができます。

利用者証明書は、証明書利用者がLGWAN電子文書交換システムを利用して、他の地方公共団体職員と電子文書を交換する場合に利用できます。前に説明した職責証明書が電子文書へ「職責」の印鑑を押印するものであることに対し、利用者証明書は文書取扱主任等の「名義」をあらわすもので、送付した電子文書が証明書利用者の「名義」で送付されたかどうか、また改ざんされていないかどうかを電子的に確認することができます。Webサーバ証明書は、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が盗聴されないように、電子文書等の内容を暗号化※5

※5　このような通信は、PKIの世界では「SSL通信」と呼ばれています。通信中は、Webブラウザの URLの冒頭に、“https”の５文字が表示されます。

ところで、インターネットの利用中に次のような警告ダイアログが表示された経験はありませんか？　これは、Web ブラウザが、Web サイトから受信した証明書が社会的に信頼された認証局から発行されたかどうか確認できなかった場合に表示されるものです。この場合、Web ブラウザは暗号化通信を開始するか、止めるかを利用者へ委ねます。ここで「はい」のボタンをクリックして通信を開始することは、相手方がフィッシング等の犯罪者サイトである可能性があるため、一般的には推奨されていません。



しかし、LGPKI アプリケーション認証局が発行する Web サーバ証明書であれば、主要な Web ブラウザ製品については、ブラウザ自体に LGPKI アプリケーション認証局を信頼のおける認証局と認める設定が整っているため、このような警告が出ることはありません※6。住民、企業等は安心して証明書利用者が運営する電子自治体等の Web サイトへアクセスすることができます。

今回説明した内容に興味をお持ちになり、今後、実際の業務で証明書を利用する機会が訪れた場合には、是非とも各地方公共団体に設置されている登録分局※7の担当者へ証明書の発行手続き等についてご相談ください

する場合に利用できます。WebブラウザとWebサイトで暗号化通信を行う際には、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、この証明書がインターネット犯罪者等のものではなく「社会的に信頼された認証局から発行されたものかどうか」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。

LGPKIが発行する証明書の概要を説明しました。LGPKIでは、今後も地方公共団体職員の方々がインターネットやLGWANを利用した電子文書を交換する際の安全性、真正性の確保に取り組んでまいります。次号では、登録分局の業務について詳しく説明します。

※6　LGPKIアプリケーション認証局では“WebTrust for CA”（米国公認会計士協会（AICPA）及びカナダ勅許会計士協会（CICA）が定めた、認証局についての業界最高水準の規準）に基づく検証報告書を取得しています。このことが契機となり、現在ではMicrosoft社のWebブラウザであるInternet ExplorerへLGPKIアプリケーション認証局そのものを証明する証明書（PKIの世界では、これを「自己署名証明書」といいます。）が標準搭載されることになりました。この自己署名証明書が搭載されたWebブラウザであれば、LGPKIが発行したWebサーバ証明書を利用したWebサイトへアクセスしても、セキュリティの警告ダイアログがでることはありません。
なお、現在対応済みのMicorosoft社製品のバージョン等は、次のURLをご参照ください。
http://www.microsoft.com/japan/presspass/detail.aspx?newsid=2821

※7　証明書利用者と同じ地方公共団体の中に整備された証明書発行に係る申請受付、審査と証明書の配付窓口で、証明書利用者とLGPKIとを仲介します。

LGWAN-ASPサービス接続／登録状況（平成21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	173件	■ホスティング	接続	98件
■通信	登録	153件	■ファシリティ	登録	186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