特集1 LGPKIが発行する証明書の利用例

地方公共団体組織認証基盤（以下「LGPKI」という。）では、地方公共団体が安全に電子データを送受信するために、電子証明書（以下「証明書」という。）を発行しています。先月号では証明書の発行方法についてご説明しました。今月号では、LGPKIが発行する証明書の利用例と現在登録分局で実施している登録分局自己点検についてご紹介します。

1 証明書を利用してどのようなことを行うか

通信相手が見えないネットワーク上で電子データを送受信する場合において、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、第三者によって送信した内容が盗聴・改ざんされたり、送信者になりすまして文書が送信されたり、あるいは、送信者が送信したことを否認したりする可能性があります。

そのため、安全に通信を行うための対策の一つの方法として証明書を利用します。まずは証明書の基本的な働きをご説明します。

（1）盗聴対策

対となる二つの鍵（秘密鍵と公開鍵）をペアとした「公開鍵暗号方式※1」を利用することにより、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。

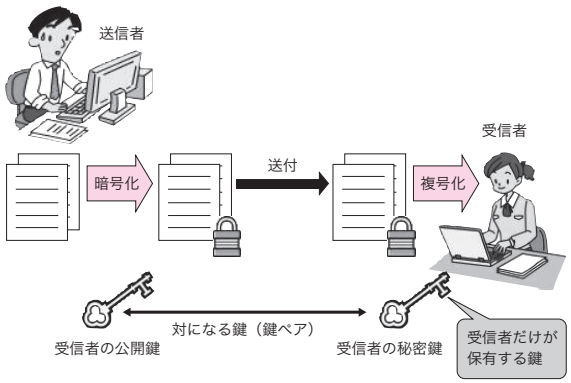
①受信者の公開鍵を使って暗号化

送信者は、あらかじめ受信者本人から又はリポジトリ※2から入手した※3受信者の公開鍵を使って文書を暗号化し、送信します。

②自分の秘密鍵を使って復号化

受信者は、暗号化された文書を受け取り、自分の秘密鍵を使って復号化します（図－1）。

図－1 盗聴対策

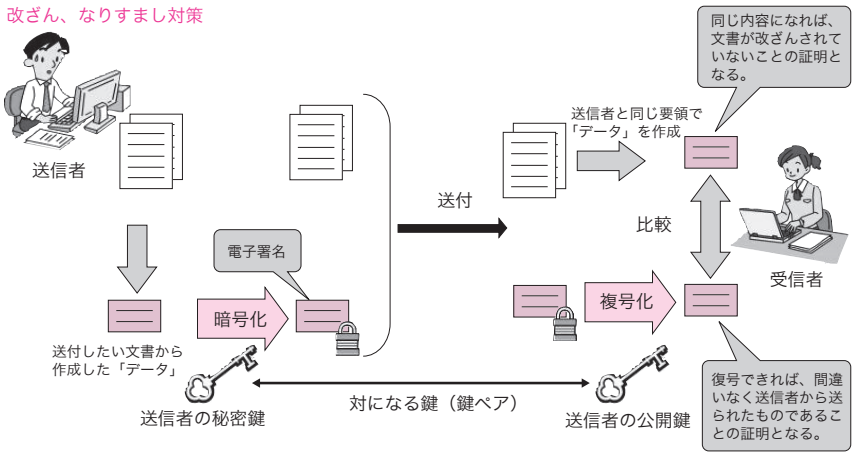


ここも確認！

秘密鍵は受信者本人しか保有していないため、文書の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できたとしても文書を復号化できないため、文書の秘匿性が保証されます。そのためには、秘密鍵を本人以外が利用できないように、秘密鍵が格納された媒体を安全に管理することが重要です。

※1　一般に公開している「公開鍵」と本人のみが保有する「秘密鍵」の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ないという特徴があります。公開鍵は、文書の暗号化、電子署名の復号化に利用し、秘密鍵は、文書の復号化、電子署名の付与に利用します。
※2　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。
※3　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。

図－２　改ざん・なりすまし対策



（２）改ざん・なりすまし対策

電子署名によって、文書の作成者は誰か、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。

①電子署名の付与

送信者は、送付しようとする文書から生成した特定の「データ」を、自分の「秘密鍵」を使って暗号化（電子署名）し、送付すべき文書及び自分の証明書付き公開鍵と一緒に送ります。

②改ざん・なりすましの有無の確認

受信者は、まず、送信者の「公開鍵※４」を使って暗号化された「データ」を復号化し、間違いなく送信者から文書が送信されたことを確認します。次に、送付された文書から送信者と同じ要領で「データ」を作成して、同じ結果が得られれば、文書の内容が改ざんされていないと確認できます（図－２）。

ここも確認！

もとの文書から作成した「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もとの文書は復元できず、また、もと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。

2　LGPKIが発行する証明書の利用例

では、実際に証明書がどのように利用されているのか、LGPKIが発行する職責証明書とWebサーバ証明書を例にご説明します。

職責証明書は、地方公共団体が電子入札や電子交付等の電子行政サービスを提供する際に、インターネットを経由して住民・企業等と文書の送受信を行う場合に、電子的な公印としての役割を担います。証明書の利用により、送信した文書の内容が改ざんされていないこと、あるいは、送信者が間違いなく地方公共団体の職責者であることを住民・企業等に保証します。

職責証明書は、主に次に挙げるようなシステムで利用されています。

・地方公共団体／企業の相互間で利用される電子入札システム
・地方公共団体／住民・企業の相互間で利用される電子申請・交付システム
・政府省庁／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、登記・供託オンライン申請システム等)

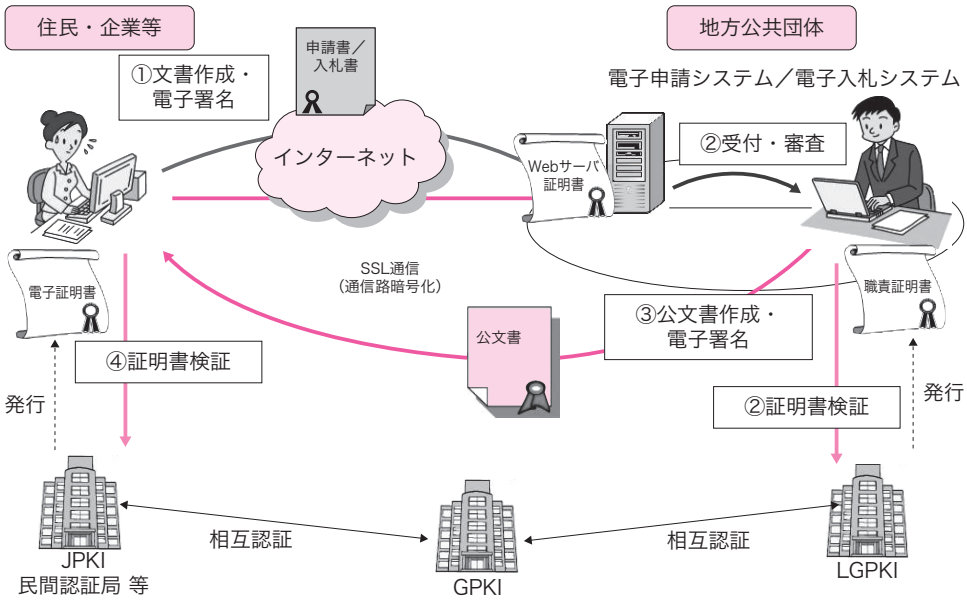
また、Webサーバ証明書は、住民・企業等が地方公共団体の提供する電子行政サービス等を利用する際に、電子行政サービス提供者側のWebサーバと住民・企業等側のPC間の通信を暗号化する場合に利用します。

当該証明書の利用により、Webサーバと住民・企業等のPCとの間の通信が盗聴されていないこと、通信先のWebサーバが間違いなく実在する電子行政サービス提供者側のものであることを住民・

※４　このとき受信者は、送付された証明書が有効であることを確認する必要があります。証明書が有効であることの確認は、システムで自動的に行うように構築し、受信者自らの操作で検証作業を行うことがないのが一般的です。

企業等に保証することができます。

図－３は電子申請システム／入札システムにおいて職責証明書及びWebサーバ証明書を利用するケースを例示したものです。



図－３　電子申請／電子入札システムにおけるLGPKI証明書の利用例

①住民・企業等は、公的個人認証サービス（以下「JPKI」という。）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、地方公共団体あての申請書等に電子署名を付与し、文書を送付します。

文書を安全に送付するには、通信する相手先のWebサーバが信頼できる相手かどうかを確認する必要があり、この時にWebサーバ証明書が利用されます。Webブラウザ（住民・企業等のPC）からWebサーバ（電子入札等のシステムのサイト）にアクセスすると、WebサーバはWebサーバ証明書をWebブラウザに送ります。Webブラウザは、この証明書が住民・企業等が信頼する第三者機関（認証局）から発行されたものかを判断するために、WWWブラウザの「信頼されたルート証明機関」に当該証明書を発行した認証局の自己署名証明書※5が含まれるかを確認します。LGPKIが発行するWebサーバ証明書の場合、特定のブラウザ（現在は、マイクロソフト社のインターネットエクスプローラ（IE）のみ対応）であれば、Webサーバ証明書を搭載されたサイトにアクセスすると、WWWブラウザに自動的に自己署名証明書がインストールされるため、住民･企業等は特に意識することなく、証明書が問題ないことを確認でき、こうして暗号化通信が開始されます。

②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が有効であることの検証を行い、その証明書が有効であることを確認します。

③地方公共団体は、証明書が有効であることを確認した後、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。

④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。

上記②、④において行う証明書の有効性の検証は、システムで自動的に行うようにシステムを構築し、受信者自らの操作で検証作業を行うことがないのが一般的です。証明書の検証に当たっては、認証局が提供している失効した証明書リストから、証明書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。

これらの検証は、LGPKIとJPKI等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。

※５　証明書を発行する認証局自身の公開鍵が含まれた認証局自らを証明する証明書。

なお、地方公共団体に対しては、電子行政サービスにおいて証明書検証を実施するシステム向けに住民・企業等から送付された証明書が有効であるかどうかを検証する「証明書検証サーバ」（以下「CVS」という。）を公開しています。地方公共団体は、CVSに問い合わせることで受信した文書に付与された証明書の有効性を確認できます。CVSでは、GPKIと相互認証しているJPKIや民間認証局等が発行する証明書の検証が可能です。

特集2　登録分局自己点検について

1　目的と概要

LGWANに接続する各地方公共団体においては、LGWAN運営主体から委任された証明書利用者からの証明書発行等の申請の受付及び審査等の業務の一部を行うため、登録分局を設置しています。

登録分局自己点検（以下「自己点検」という。）は、登録分局が「地方公共団体組織認証基盤の運営に関する基本綱領」（以下「LGPKI基本綱領」という。）※6第９条第１項の定めるところにより、LGWAN運営主体から委任された業務を適正かつ円滑に行っていることを年に１回定期的に点検し、LGWAN運営主体に対して報告を行うものです。

自己点検の対象団体及び対象期間等は、次のとおりです。

・対象団体：前年度末までに登録分局整備を完了しているすべての団体
・対象期間：前年度の４月１日から３月31日まで（年度途中に登録分局を整備した団体はその日から３月31日まで）
・報告期限：毎年６月末まで

2　実施方法

自己点検は、登録分局責任者が、登録分局自己点検システムを利用し、所定の点検を実施の上、点検結果を送信することでLGWAN運営主体に報告を行います（図－４）。自己点検実施後は、画面を印刷し、登録分局で点検結果を保管します。※7なお、自己点検結果の内容については、後日、LGWAN運営主体から照会がなされる場合があります。

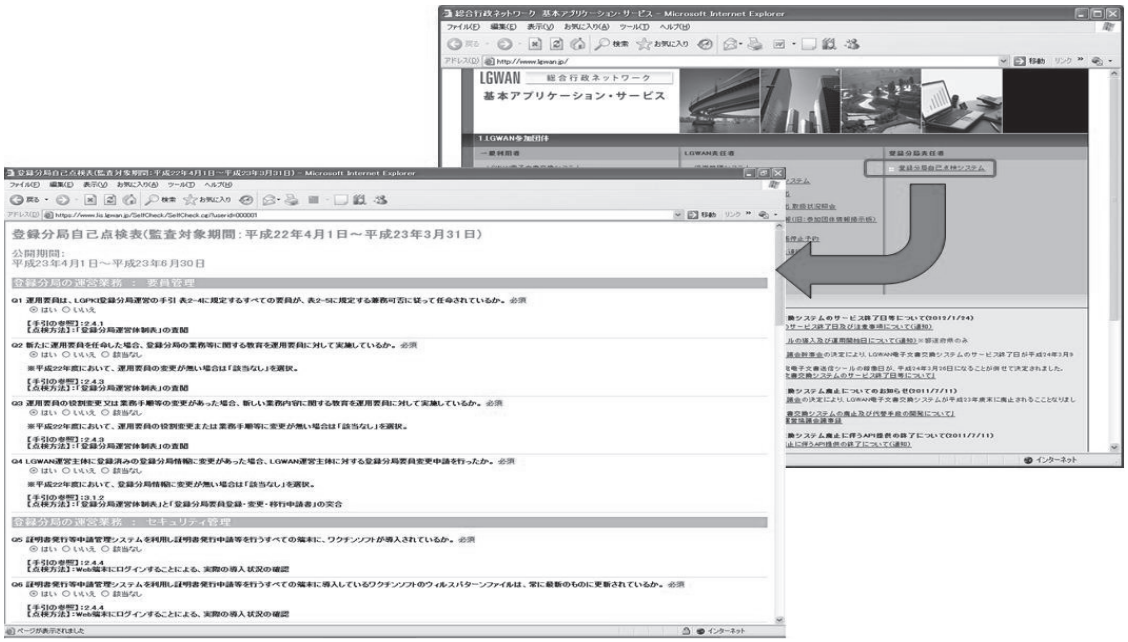
当該システムを利用するためには、登録分局責任者のログイン用データ※8が必要となります。自己点検の実施に当たっては、お手持ちのログイン用データの有効期限を確認し、有効期限切れ又は有効期限が直近となっている場合は、ログイン用データの発行・更新申請を行ってください※9。

登録分局の事情によりログイン用データを用意していない場合は、「登録分局自己点検表※10」を利用して報告することも可能です。この場合、自己点検表の全項目について回答し、表紙には必要事項を記入し、登録分局責任者の押印を行い、FAX又はメール（自己点検表の電子的写しを添付）により、LGWAN運営主体に報告します。

なお、自己点検表の原紙については各登録分局で保管します。

※６　http://center.lgwan.jp/library/second2.html#C-6-6-1
※７　システムの操作方法については、LGPKI登録分局運営の手引の「付録D　登録分局自己点検システムの操作方法」を参照ください。
※８　LGWAN運営主体が提供する各種システムにログインするための操作員識別情報
※９　ログイン用データの発行・更新申請については、平成22年９月６日付センター発1109号「ログイン用データ、職責証明書及び利用者証明書更新手続きの実施について（お願い）」（http://center.lgwan.jp/information/doc/LGPKIoshirase20100906.pdf）を参照ください。
※10　http://center.lgwan.jp/library/doc/F/F-2-1-4_pkitebiki_selfcheck.pdf

図－4　登録分局自己点検システム（イメージ）



3　依頼事項

（1）自己点検報告期限の厳守について

例年において、期限内に自己点検を終了しない登録分局がありますので、期限内の報告についてご協力をお願いします。

（2）LGWAN運営主体が実施する監査への対応

LGPKI基本綱領第９条第１、２項に基づき、証左書類等の提出やヒアリング、現地監査を実施する場合があります。

また、監査の結果によっては、全団体又は個別に改善措置を求めることがありますので、その場合は速やかな対応をお願いします。

4　監査結果について

監査の結果は、例年秋季に開催する当該年度第２回総合行政ネットワーク運営協議会において報告しております。

２回にわたりLGPKIについて特集しました。地方公共団体が住民・企業等との間で実施する申請・届出・交付等の手続、あるいは、地方公共団体・政府省庁相互間の文書通信等において、相互に信頼し、安全に通信を行うに当たり、LGPKIは最も有効かつ重要な基盤といえます。

LGPKIについて、一層のご理解と利活用の促進をお願いするものです。

LGWAN-ASPサービス登録／接続状況（平成24年５月11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：295件	■ホスティング	接続：180件
■通信	登録：167件	■ファシリティ	登録：222件

登録／接続済のLGWAN-ASPサービス提供者のリストは、下記URLに掲載しております。

http://www.lasdec.or.jp/cms/15,0,41.html