特集

LGPKIにおける暗号アルゴリズムの移行について

地方公共団体組織認証基盤（以下「LGPKI（Local Government Public Key Infrastructure）」という。）では、現在使用している暗号アルゴリズムを平成26年度から順次新たな暗号アルゴリズム（以下「新暗号アルゴリズム」という。）に移行する予定です。

LGPKIについては、「月刊LASDEC」平成22年10月号の総合行政ネットワークNO.96特集「LGPKIとは？」において、その目的、役割、仕組みなどを紹介しましたが、本号では、暗号アルゴリズムの移行に関して、その必要性を理解していただくことを目的として解説し、移行するとは具体的にどのような内容か、LGPKIの利用者が何を行うか、などを併せて説明します。

1 暗号アルゴリズム移行の必要性

（1）安全性の低下

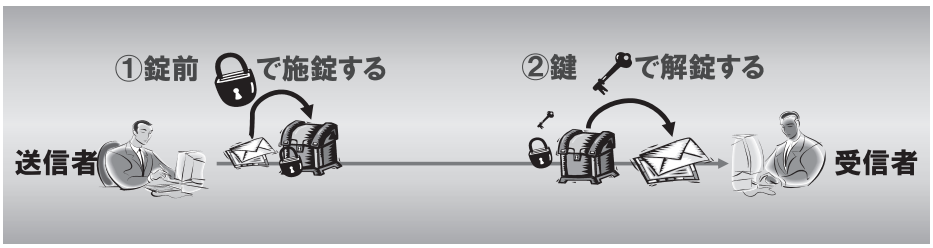
LGPKIでは、公開鍵暗号方式という暗号技術を使って、文書を暗号処理したりデジタル署名を行ったりすることにより、安全・正確に届けることを実現しています。暗号処理を例に仕組みを簡単に説明しますと、文書を金庫のようなものに格納して「電子的な錠前」を使って鍵をかけ（暗号化）、電子的な錠前がかかった金庫は、その錠前に対応する「電子的な鍵」で開けられます（復号・図－１）。この「電子的な錠前」と「電子的な鍵」は、実際の公開鍵暗号方式では、それぞれ数字の羅列であり、「鍵」と呼ばれています。「電子的な錠前」に該当する「鍵」が広く公開されることから、公開鍵暗号方式と呼ばれています（詳細については前述の10月号の記事を参照してください）。

LGPKIの公開鍵暗号方式で使っている暗号アルゴリズムは、公開されている「電子的な錠前」から「電子的な鍵」を解読するのに必要な計算量が膨大であり、世界最高速のコンピュータを使っても現実的ではないほどの時間がかかることから、安全であるとされています。このことは裏を返せば、計算するためのコンピュータの性能が向上するほど、徐々に安全性が脅かされていくことを示しています。コンピュータの性能は日々向上していますので、今と比較して性能が飛躍的に向上すれば安全ではなくなる日を迎えることになります。

また、安全性を確認する目的で、効率的に解読する研究も進められており、コンピュータの性能向上とともに、結果的に脅威に繋がっているとも考えられます。

このように、LGPKIで使っている暗号アルゴリズムは、近い将来、安全性が低下する可能性が高いことが既に予想さ

図－１　証明書を利用した電子文書の送受信



れ、公表※1されています。

アメリカでは、安全性が低下すると予想されているこれらの暗号アルゴリズムを、平成22年に廃止しました。日本の政府機関においては、平成26年までに、現在の暗号アルゴリズムより安全性の高い新暗号アルゴリズムを使い始めることが決まっています※2。

したがって、LGPKIにおいて現在使用している暗号アルゴリズムも、より安全性の高いものへと移行する必要があります。

（2）移行しない場合のリスク

1－(1)で説明しましたように、現在使用している暗号アルゴリズムはいつの日か安全性が低くなるリスクを内在しています。安全性が低くなると、例えば、暗号化し、盗聴を防止した文書のはずなのに誰にでも読める可能性が高くなります。また、このときになって、慌てて新暗号アルゴリズムに移行しようとしても、その準備ができていなければ、対応までの間の安全性が確保できなくなります。準備には相応の時間と費用がかかることから、政府の方針等に足並みを揃え、一体的に移行を進めることが望まれます。

2 暗号アルゴリズム移行における変更点

新暗号アルゴリズムに移行するための変更点は、次のとおりです。

（1）証明書が新しくなる

LGPKIで対象となるのは、職責証明書、利用者証明書、Webサーバ証明書、コードサイニング証明書及びメール用証明書のすべて、そして、ログイン用データ（LGWAN責任者用、登録分局責任者用）です。

（2）鍵格納媒体が変更になる

現行の暗号アルゴリズムに対応した鍵格納媒体製品には、所定の型番のICカード、ICカード読取装置及びUSBトークンがありますが、新暗号アルゴリズムの証明書を発行する場合は、これに対応した新しい鍵格納媒体製品を使うことを想定しています。なお、新しい証明書を発行するまでは、現在の証明書や鍵格納媒体とそれに対応した読取装置等の周辺機器は、そのまま使用できます。

3 暗号アルゴリズムを移行するためにすること

では具体的には何をすればよいのでしょうか。

前項で示したように、証明書、鍵格納媒体と周辺機器が変更になりますので、対応した機器、媒体及びソフトウェアを準備することになります。

（1）LGWAN-ASP

LGWAN-ASPサービス提供事業者（以下「ASPサービス提供者」という。）は、現在提供しているアプリケーションに対し、新暗号アルゴリズムに対応した証明書や暗号化した文書を使えるようにするとともに、現在使用されている暗号アルゴリズムに対応した証明書や暗号化した文書も引き続き使えるようにしておかなければなりません。

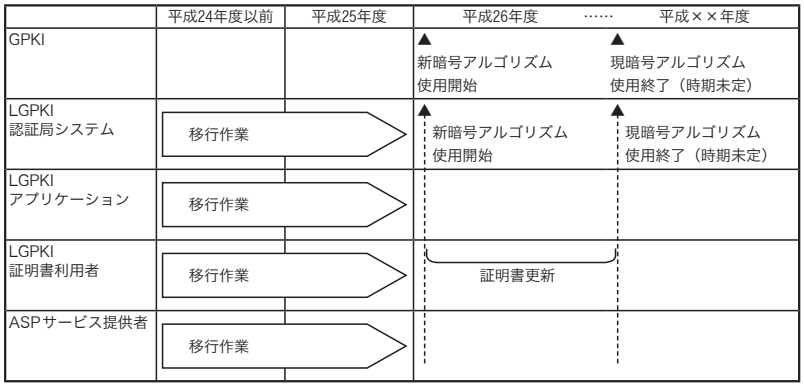
（2）各種証明書

参加団体は、職責証明書や利用者証明書、ログイン用データ等を新暗号アルゴリズムの証明書にする前に、新暗号アルゴリズムに対応した鍵格納媒体製品をあらかじめ準備してください。

現在の暗号アルゴリズムの証明書は、有効期限が切れるまでは使える予定です。しかし、暗号アルゴリズムの安全性が急激に低下した場合には、新暗号アルゴリズムの証明書に切り替える可能性があります。このような事態が発生した場合は、その旨が公表される予定になっていますが、そのような事態の想定か

※1　『SHA-1及びRSA1024の安全性評価について』
http://www.soumu.go.jp/menu_03/shingi_kenkyu/kenkyu/kouteki_kojin/pdf/080916_1_si3.pdf
※2　『政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針』
http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf

図－２　想定スケジュール



らも早めに移行の準備をしておくことが大切です。

（３）アプリケーション

各参加団体が調達して使用している各種アプリケーションは、ASPサービス提供者が提供するアプリケーションと同様に新暗号アルゴリズムに対応した証明書や暗号化した文書を使えるようにするとともに、現在の暗号アルゴリズムに対応した証明書や暗号化文書も引き続き使えるようにしておかなければなりません。

（４）認証局

認証局では、新暗号アルゴリズムの証明書が発行できるようにCAシステムと「証明書発行等申請管理システム（CIRS）」を変更します。また、新暗号アルゴリズムの証明書の有効性を検証するための証明書検証サーバ（CVS）も変更します。これにあわせて、各種アプリケーションを移行する際に必要な動作確認用の環境も提供する予定です。

4 スケジュール

LGPKIは、政府認証基盤（GPKI）との相互認証を行っている関係から、他の認証基盤とも歩調を合わせて暗号アルゴリズム移行を進めていく必要があります。平成26年度から発行する証明書は、すべて新暗号アルゴリズムに対応したものになり、現在の暗号アルゴリズムの証明書は順次切り替えていくことになります。

なお、現在の暗号アルゴリズムの証明書は、前述したとおり、その有効期限が切れるか更新するまではそのまま使えることを予定しております。現時点で想定しているスケジュールを図－２に示します。

5 最後に

新暗号アルゴリズムに対応した鍵格納媒体製品及びそれに対応した読取装置等の周辺機器の仕様、アプリケーションの動作を検証するための環境を提供する時期など、これから決めていくものが多くあります。決定した情報は、総合行政ネットワークポータルサイト等によって随時にお知らせします。参加団体、ASPサービス提供者の方々にもご協力いただきながらLGPKI全体の暗号アルゴリズム移行をスムーズに進めたく、引き続きご協力をよろしくお願いします。

LGWAN-ASPサービス接続／登録状況（平成23年２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　271件	■ホスティング	接続　170件
■通信	登録　160件	■ファシリティ	登録　211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