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」という。）では、電子証明書（以下「証明書」という。）の発行等において現在使用している暗号アルゴリズム（SHA-1※1、RSA1024※2）（以下「旧暗号」という。）を、平成26年度に新たな暗号アルゴリズム（SHA256、RSA2048）（以下「新暗号」という。）に移行する予定です。

今回は、暗号アルゴリズムの移行に伴うLGPKIの登録分局、証明書利用者及びLGPKIの証明書を利用するシステム（電子申請、電子入札システム等）の提供者における対応事項及び移行スケジュールについて説明します。

1　暗号アルゴリズム移行の背景

LGPKI、政府認証基盤（以下「GPKI」という。）、公的個人認証サービス、民間認証局等で利用している暗号アルゴリズムは、政府の暗号技術検討会※3等において安全性の低下が指摘されており、より暗号強度の高い暗号アルゴリズムに移行する必要が生じています。

GPKIでは、「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（平成20年４月22日情報セキュリティ政策会議決定）」に基づき、暗号アルゴリズムを移行することが決定されています。

これに伴い、GPKIと相互認証を行っているLGPKIにおいても、平成26年度早期に暗号アルゴリズムを移行することを総合行政ネットワーク運営協議会において決定※4しており、認証局の運営を行うLGWAN運営主体では、証明書の発行や証明書の有効性を検証するための仕組み等について、新暗号へ移行するための準備を進めています。

2　暗号アルゴリズム全体移行スケジュール

LGPKIの暗号アルゴリズム全体移行スケジュールは図－１のとおりです。

LGPKIの暗号アルゴリズム移行時期は、平成26年９月下旬を予定しています。なお、アプリケーション認証局については、平成26年４月に先行して実施する旨ご案内済みですが、当該認証局の自己署名証明書をInternet Explorerに搭載するための要件が変更になる可能性が出てきたことに鑑み、ブリッジ認証局及び組織認証局と同じ時期の平成26年９月下旬に移行

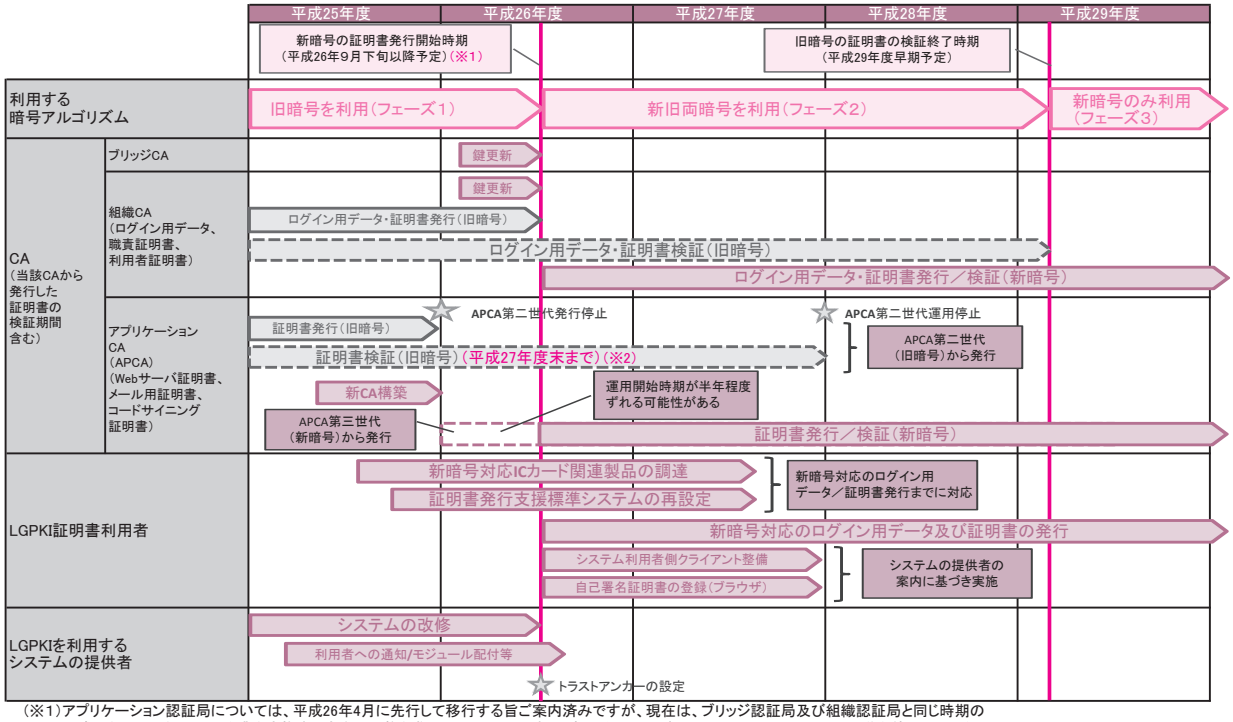
※１　任意の長さのデータから160bitの「ハッシュ値」と呼ばれる値を作成するアルゴリズム。ハッシュ値から元のデータは復元できず、元のデータに変更が加えられると、ハッシュ値は異なる内容になるため、改ざん検知などに用いられる。なお、新暗号のSHA256の場合は、256bitのハッシュ値を作成する。

※２　十分に大きな素数を掛け合わせた数の素因数分解が難しいことを暗号技術の基礎とした公開鍵暗号方式の一つ。一般に公開している「公開鍵」と本人のみ保有する「秘密鍵」の対になる2つの鍵を使ってデータの暗号化／復号化を行う。暗号アルゴリズムの移行においては、その鍵長を1024bitから2048bitに移行し、暗号強度をさらに高める。

※３　電子政府推奨暗号の監視、電子政府推奨暗号の安全性及び信頼性確保のための調査・検討、暗号モジュールのセキュリティ要件及び試験要件の作成等について、総合的な観点から検討を行う組織（事務局：総務省、経済産業省）

※４　平成24年度第１回総合行政ネットワーク運営協議会議案第４号（http://center.lgwan.jp/conference/gm_material120523/gian4.pdf）（LGWAN接続環境が必要です。）

図－1　暗号アルゴリズム全体移行スケジュール



（※1）アプリケーション認証局については、平成26年4月に先行して移行する旨ご案内済みですが、現在は、ブリッジ認証局及び組織認証局と同じ時期の平成26年9月下旬に移行作業を実施する方向で調整を進めているところです。最新の移行スケジュールについては、LGWAN運営主体からの通知文書をご確認ください。
（※2）アプリケーション認証局（第二世代）から発行した証明書の検証期間は、当該認証局を廃止する平成27年度末までとなります。

作業を実施する方向で調整を進めているところです。

3　暗号アルゴリズムの移行に伴う対応

LGPKIにおける暗号アルゴリズムの移行に伴い、LGPKIの登録分局、証明書利用者及びLGPKIの証明書を利用するシステムの提供者において対応が必要となる事項は、次のとおりです。

（1）LGPKIの登録分局、証明書利用者

平成26年９月下旬の暗号アルゴリズム移行後、旧暗号対応のログイン用データ※5及び証明書の発行は停止し、新暗号対応のログイン用データ及び証明書のみ発行します※6。そのため、LGPKIの登録分局、証明書利用者は表－１のとおり、新暗号対応の証明書等の発行に係る対応を行う必要があります。

ただし、暗号アルゴリズム移行前に発行した旧暗号対応のログイン用データ及び証明書については、暗号アルゴリズム移行後も、証明書利用者の移行期間として、一定期間（平成29年度早期までを予定）は、継続して利用することが可能です。

また、LGPKIの証明書を利用するシステムの利用にあたり、表－２の作業が必要な場合があります。具体的な作業内容は、システムの提供者から通知される内容を確認してください。

（2）LGPKIの証明書を利用するシステムの提供者

暗号アルゴリズムの移行に伴い、LGPKIの証明書を利用するシステムにおいて、LGPKIの証明書による暗号化、電子署名の付与及び証明書の検証に影響があります。

そのため、システムの提供者（開発事業者

※５　LGWAN運営主体への証明書発行等申請において、地方公共団体内に設置する登録分局がシステムを利用する際に必要となる操作者識別情報
※６　旧暗号対応の証明書の失効・廃止については、暗号アルゴリズム移行後も引き続き受けつけます。

表－１　新暗号対応の証明書等の発行に係る対応事項

対応時期	作業項目	作業概要
新暗号対応のログイン用データ／証明書発行申請まで（発行申請は平成26年９月下旬以降受付を開始）	新暗号対応のICカード関連機器等の調達に係る予算確保／調達	新暗号対応のログイン用データ／証明書発行にあたり、新暗号対応のICカード、ICカード読取装置、各ドライバソフト等が必要となるため、登録分局／証明書利用者において、予算を確保し、機器等を調達する※7。
	証明書発行等事務において利用するシステムの再インストール	LGWAN運営主体が提供する「証明書発行支援標準システム※8」について、暗号アルゴリズム移行に伴い改修が発生するため、新暗号対応版のプログラムを端末に再インストールする。
暗号アルゴリズム移行後（平成26年９月下旬以降）	新暗号対応のログイン用データ及び証明書発行申請	新暗号対応のログイン用データ及び証明書の発行申請を行う。 （※）LGWAN運営主体への申請方法は原則として変更しない予定です。

表－２　LGPKIの証明書を利用するシステムの利用に係る対応事項

対応時期	作業項目	作業概要
暗号アルゴリズム移行時（平成26年９月下旬予定）	利用者側クライアントの環境整備	システムの提供者から通知される内容に基づき、クライアントモジュールの適用等を行う。また、OS/ブラウザ等が新暗号に対応しているか確認し、必要に応じて環境を整備する。
	Webブラウザへの新アプリケーション認証局の自己署名証明書の登録	LGPKIのWebサーバ証明書を搭載するWebサイトにアクセスする際に、新暗号対応のWebサーバ証明書を検証可能とするため、Webブラウザの「信頼されたルート証明機関」にLGPKIの新暗号対応のアプリケーション認証局の自己署名証明書をインストールする※9。

表－３　LGPKIの証明書を利用するシステムの提供者の対応事項

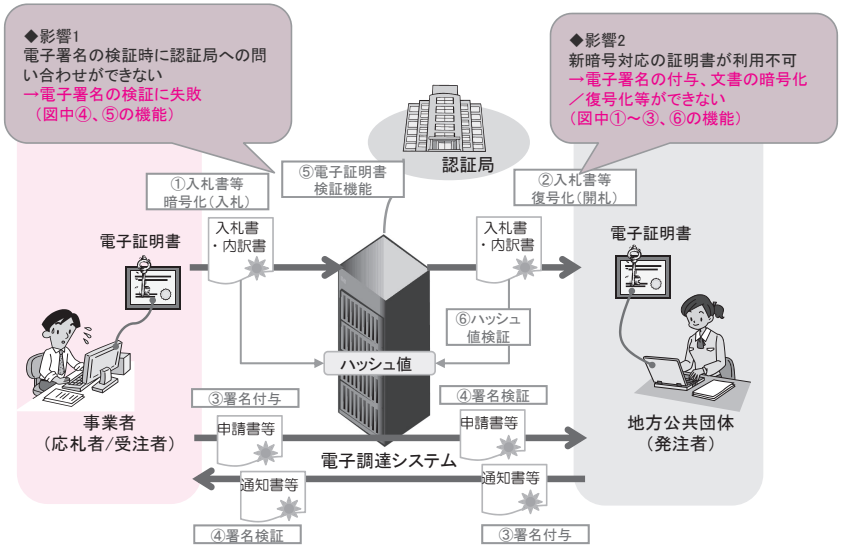
対応時期	作業項目	作業概要
暗号アルゴリズム移行（平成26年９月下旬予定）まで	LGPKIの証明書を利用するシステムの改修の要否の確認及び改修	暗号アルゴリズム移行に伴うシステムへの影響箇所を洗い出し、改修作業を実施する※10。システムの改修にあたっては、必要に応じて、LGWAN運営主体が提供する新暗号検証試験環境※11を利用して事前検証を行う。
	システムの改修に係る利用者への通知	システムの利用者に対し、システムの改修スケジュール、クライアントモジュールの配付等必要な事項を通知する。
暗号アルゴリズム移行時（平成26年９月下旬）	署名検証要求を行うシステムにおけるトラストアンカー等の設定	LGPKIに署名検証要求を行うシステムにおいて、次のとおりトラストアンカー設定等の作業を行う。 ・証明書検証サーバへの署名検証要求で指定するトラストアンカーを新暗号対応のブリッジ認証局の自己署名証明書に変更する。 ・証明書検証サーバとのSSL通信で利用するトラストアンカーを新暗号対応のアプリケーション認証局の自己署名証明書に変更する。 ・証明書検証要求の接続先を新暗号対応の証明書検証サーバに変更する。

(LGWAN-ASPホスティングサービス提供者又はアプリケーション及びコンテンツサービス提供者を含む）及び地方公共団体のシステム管理担当部署）において、表－３のとおり、システムの改修等の作業が必要になる場合があります。なお、改修を行わない場合は、図－２のような影響が想定されます。

なお、LGPKIにおける暗号アルゴリズム移行方針、LGPKI技術仕様書及びプロファイル設計書については、総合行政ネットワークポータルサイト(http://center.lgwan.jp/)、LGWAN-ASPポータル

※７　新暗号対応ICカード関連製品の販売開始時期、型番等の詳細は、別途LGWAN接続団体に通知します。
※８　鍵ペアとログイン用データ／証明書発行要求ファイルの作成及びログイン用データ／証明書の鍵格納媒体への格納を行う際に利用するシステム。システムのプログラムは、LGWANポータルサイトから入手してください。(http://center.lgwan.jp/library/index.html#K-3-3)
※９　Internet Explorerの場合、自己署名証明書は自動的にインストールされるため、通常は利用者の作業は不要ですが、インターネットに接続されていない端末からアクセスする場合やInternet Explorer以外のブラウザを利用する場合には、手動でのインストール作業が必要です。
※10　暗号アルゴリズム移行後、一定期間においては、新旧両暗号の証明書に対応できるよう改修を行う必要があります。
※11　新暗号検証試験環境の利用については、「地方公共団体組織認証基盤（LGPKI）における新暗号検証試験環境の運用開始について（お知らせ）」(http://center.lgwan.jp/information/second2.html）を参照してください。

図－2　改修を行わない場合に想定される影響（電子調達システムの例）



サイト（https://www-asp.lgwan.jp/Ainf/lgpkica.html）及び地方公共団体組織認証基盤（LGPKI）のホームページ（http://www.lgpki.jp/）に掲載していますので、必要に応じて参照してください。

4　おわりに

LGPKIの暗号アルゴリズムの移行にあたっては、LGPKIの登録分局、証明書利用者、LGPKIを利用するシステムの提供者等関係各位の協力が不可欠となります。

LGWAN運営主体は、関係各位が移行対応を実施するにあたって必要な情報をLGWANポータルサイト等で随時提供してまいりますので、ご確認をお願いいたします。

引き続き円滑で効率的な移行にご理解、ご協力をお願いいたします。

LGWANサービス提供設備からLGWAN接続ルータへの移行状況（平成25年9月10日現在）

■LGWAN接続団体　798/1820団体
■LGWAN-ASP　48(113)/201 ASP
※（　）内は接続団体が自団体の接続ルータを利用してASPサービスを提供する形態を含めた件数です。

LGWAN-ASPサービス登録／接続状況（平成25年9月10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：329件　■ホスティング　接続：201件
■通信　登録：179件　■ファシリティ　登録：275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.lasdec.or.jp/cms/15,0,41.html