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

No. 142

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。）、政府認証基盤（以下「GPKI」という。）、公的個人認証サービス及び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※1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においては、「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※2及びRSA1024※3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。

これを受け、GPKIと相互認証を行っているLGPKIにおいても、平成26年９月に、電子証明書（以下「証明書」という。）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、現在使用している暗号アルゴリズム（SHA-1、RSA1024）（以下「旧暗号」という。）から新たな暗号アルゴリズム（SHA256、RSA2048）（以下「新暗号」という。）に移行します。

今回は、LGPKIにおける暗号アルゴリズムの移行スケジュール並びに移行に伴う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について説明します。

1　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では、平成26年９月13日（土）から15日（月）※4にかけて移行作業を実施します。

移行作業中は、表－１のとおり、地方公共団体情報システム機構（以降、「運営主体」という）が提供するサービスが停止します。これに伴い、LGPKIの証明書を利用するシステム（電子申請、電子入札等）の利用に影響がある場合は、システムの提供者からシステムの利用者に周知をお願いします。

なお、停止期間は都合により変更する場合がありますので、LGWANポータルサイト（http://center.lgwan.jp/info/second5.html）、LGWAN-ASPポータルサイト（https://www-asp.lgwan.jp/）又は地方公共団体組織認証基盤（LGPKI）ホームページ（http://www.lgpki.jp/）でサービス停止に係る最新情報の確認をお願いします。

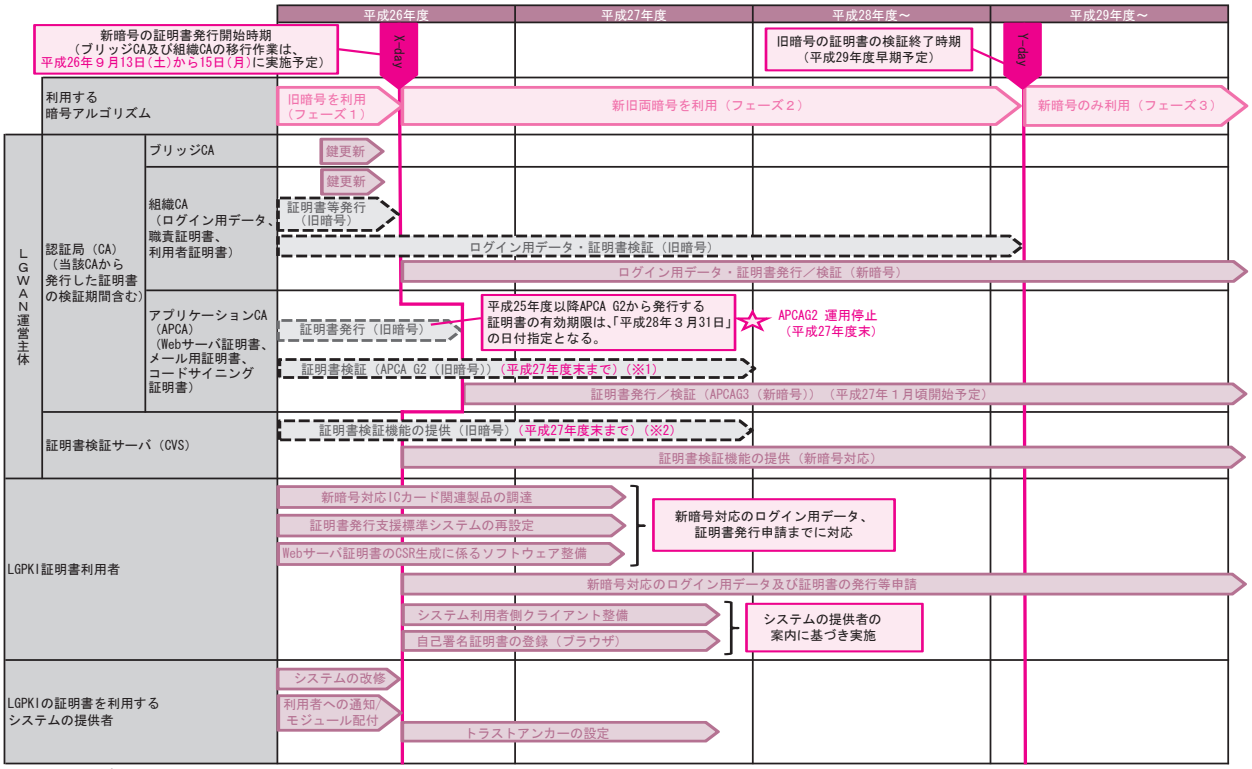
※１　電子政府推奨暗号の監視、電子政府推奨暗号の安全性及び信頼性確保のための調査・検討、暗号モジュールのセキュリティ要件及び試験要件の作成等について、総合的な観点から検討を行う組織（事務局：総務省、経済産業省）

※２　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。

※３　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」の対になる二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。

※４　暗号移行時期に関し変更が生じる場合もあります。その場合は、事務連絡等でお知らせします。

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（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。
（※２）　旧証明書検証サーバは、CVSクライアントとCVSサーバ間のSSL通信で利用するアプリケーション認証局（第二世代）から発行したWebサーバ証明書が有効期限満了となる平成27年度末までの運用となりますので、それまでに新証明書検証サーバへの切替えが必要です。なお、フェーズ２期間中は、新証明書検証サーバにおいて旧暗号の証明書の検証が可能です。

表－１　暗号アルゴリズムの移行作業中に停止する主なサービス一覧

サービス名	停止期間	対象／影響等
証明書発行等申請管理システム（CIRS）	平成26年９月12日（金）18時から平成26年９月16日（火）10時まで ※ただし、旧暗号の証明書の発行／更新申請受付期限は、平成26年９月５日（金）22時（詳細は表－２を参照）	【対象】LGWAN接続団体 （登録分局及び証明書利用者） 【影響】停止期間中は、証明書の発行等申請を行うことができません。
証明書検証サーバ（CVS）	平成26年９月13日（土）から 平成26年９月15日（月）まで （終日）	【対象】運営主体に「地方公共団体組織認証基盤証明書検証サーバ（インターネット向けCVS）利用申請書」を提出しているLGWAN接続団体 【影響】停止期間中は、証明書検証サーバを利用した証明書の検証を行うことができません。

2　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な事項は、次のとおりです。

詳細な情報は、これまでの事務連絡でのご案内のとおりですので、あわせて確認をお願いいたします[※5]。

（１）LGPKIの登録分局、証明書利用者

暗号アルゴリズム移行後、ログイン用データ[※6]及び証明書（以下まとめて「証明書等」という。）は、

※５　これまでにお送りした事務連絡は以下から確認できます（lgwan.jpドメイン名のサイトの閲覧には、LGWAN接続環境が必要です。以下同様。）。
http://center.lgwan.jp/information/second2.html#PKI_Ikou（LGWANポータルサイト）
https://www-asp.lgwan.jp/Ainf/lgpkica.html（LGWAN-ASPポータルサイト）
※６　運営主体への証明書発行等申請において、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

旧暗号対応版の発行は行わず、新暗号対応の証明書等のみ発行します※7（表－２）。そのため、LGPKIの登録分局、証明書利用者は、表－３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※8。

なお、暗号アルゴリズム移行前に発行した旧暗号対応の証明書等については、証明書利用者の移行期間として、暗号アルゴリズム移行後一定期間（最長平成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※9。

また、LGPKIの証明書を利用するシステムを利用する場合に、表－４の作業が必要となる場合があります。具体的な作業は、システムの提供者に確認してください。

（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（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－５のとおり、新暗号に対応させるためのシステム改修等の作業が必要になる場合があります。

なお、システムの提供者向け資料として、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をLGWANポータルサイト、LGWAN-ASPポータルサイト及びLGPKIホームページに掲載していますので、必要に応じて参照してください。

表－２　証明書等の今後の申請受付予定

申請種別	旧暗号対応申請受付期限	新暗号対応申請受付開始
発行及び更新	■ログイン用データ 平成26年９月１日（月）（運営主体必着） ■証明書 平成26年９月５日（金）22時	■ログイン用データ及び証明書 平成26年９月16日（火） 10時から
失効及び廃止	特になし（暗号アルゴリズム移行後も受付）	同上

表－３　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
暗号アルゴリズム移行後、新暗号対応の証明書等発行申請まで	新暗号対応のICカード等関連製品の調達に係る予算確保／調達	新暗号対応の証明書等の発行にあたり、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、製品を調達する※10。
	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	運営主体が提供する「証明書発行支援標準システム※11」の新暗号対応版のプログラムを端末にインストールする。

※７　更新申請の場合も、暗号アルゴリズム移行後は、更新対象の証明書等の新旧暗号を問わず、更新後の証明書等は全て新暗号となります。
※８　申請時に利用するシステムの操作方法を含め、申請方法については、変更ありません。また、旧暗号対応のログイン用データで新暗号対応の証明書の各種申請が可能なため、暗号アルゴリズムの移行時に新暗号対応のログイン用データを発行する必要はありません。
※９　アプリケーション認証局（第二世代）から発行した旧暗号対応の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有効期限は、当該認証局を廃止する平成27年度末までとなります。
※10　新暗号対応ICカード等関連製品の提供会社、型番等は、F-1-1-3総合行政ネットワーク接続仕様書（資料編）別冊（http://center.lgwan.jp/library/second3.html#F-1-1-3）を参照してください。
※11　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/second9.html#K-3-3）

表－4　LGPKIの証明書を利用するシステムを利用する場合の対応事項

対応時期	作業項目	作業概要
暗号アルゴリズム移行時	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（Root）の自己署名証明書をインストールする※12。

表－5　LGPKIの証明書を利用するシステム提供者の対応事項

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※13。改修にあたっては、必要に応じて、運営主体が提供する暗号移行対応試験環境※14を利用して検証を行う。
	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～平成27年度末※15まで	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。

3　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。

また、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。

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。

※12　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。また、新暗号対応のWebサーバ証明書については、階層型アプリケーション認証局の下位CAから発行されるため、自己署名証明書とは別に、ブラウザに下位CA証明書の登録が必要な場合があります（登録方法は運営主体から別途案内）。

※13　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。

※14　暗号移行対応試験環境の利用申請については、「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#PKI_Ikou）を参照してください。

※15　現在運用している旧暗号対応の証明書検証サーバは、当該サーバに搭載しているWebサーバ証明書の有効期限である平成27年度末に運用を終了する予定のため、それまでに対応が必要となります。

LGWAN-ASPサービス登録／接続状況（平成26年７月９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：370件　■ホスティング　接続：221件

■通信　登録：178件　■ファシリティ　登録：298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