LGWAN

Local Government Wide Area Network

総合行政ネットワーク

No. 122

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。）においては、現在利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年度の早期に、新たな暗号アルゴリズム（SHA256[3]、RSA2048。以下「新暗号」という。）に移行する予定です。

今回は、LGPKIにおける暗号アルゴリズムの移行の背景、移行方針及びスケジュールについて、また、LGPKIの電子証明書（以下「証明書」という。）を利用したシステムの提供者及び利用者における対応事項等についてご説明します。

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及び各民間認証局等で利用している暗号アルゴリズムについては、政府の暗号技術検討会等[4]において安全性の低下が指摘され、証明書を利用するシステムについては、現在使用している証明書の暗号アルゴリズムを、より強度の高いものへ移行する必要があります。

また、GPKIが「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の移行を決定したことから、GPKIと相互認証を行っているLGPKIについても、暗号アルゴリズムの移行が求められたところです。

これらを背景として、LGWAN運営協議会においては、平成26年度早期に暗号アルゴリズムを移行することを決定したところです[5]。

2　移行スケジュール及び移行方針

（１）移行スケジュール

LGPKIにおける暗号アルゴリズムの移行が完了し、本運用が開始される時期を平成26年度早期と想定した場合の移行スケジュールは、図－１のとおりです。

ただし、暗号アルゴリズムの移行時期については、GPKI及び他の認証局と歩調を合わせて実施する必要があるため、今後変更になる場合があります[6]。

なお、移行スケジュールでは、現在の旧暗号利用期間を「フェーズ１」、平成26年度早期～平成29年度早期の新旧両暗号の利用期間を「フェーズ２」、平成29年度早期以降の新暗号のみの利用期間を

[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を復元できず、また、元のデータに変更が加えられると、作成されるハッシュ値は異なる内容になるなどの特徴があり、改ざん検知などに利用

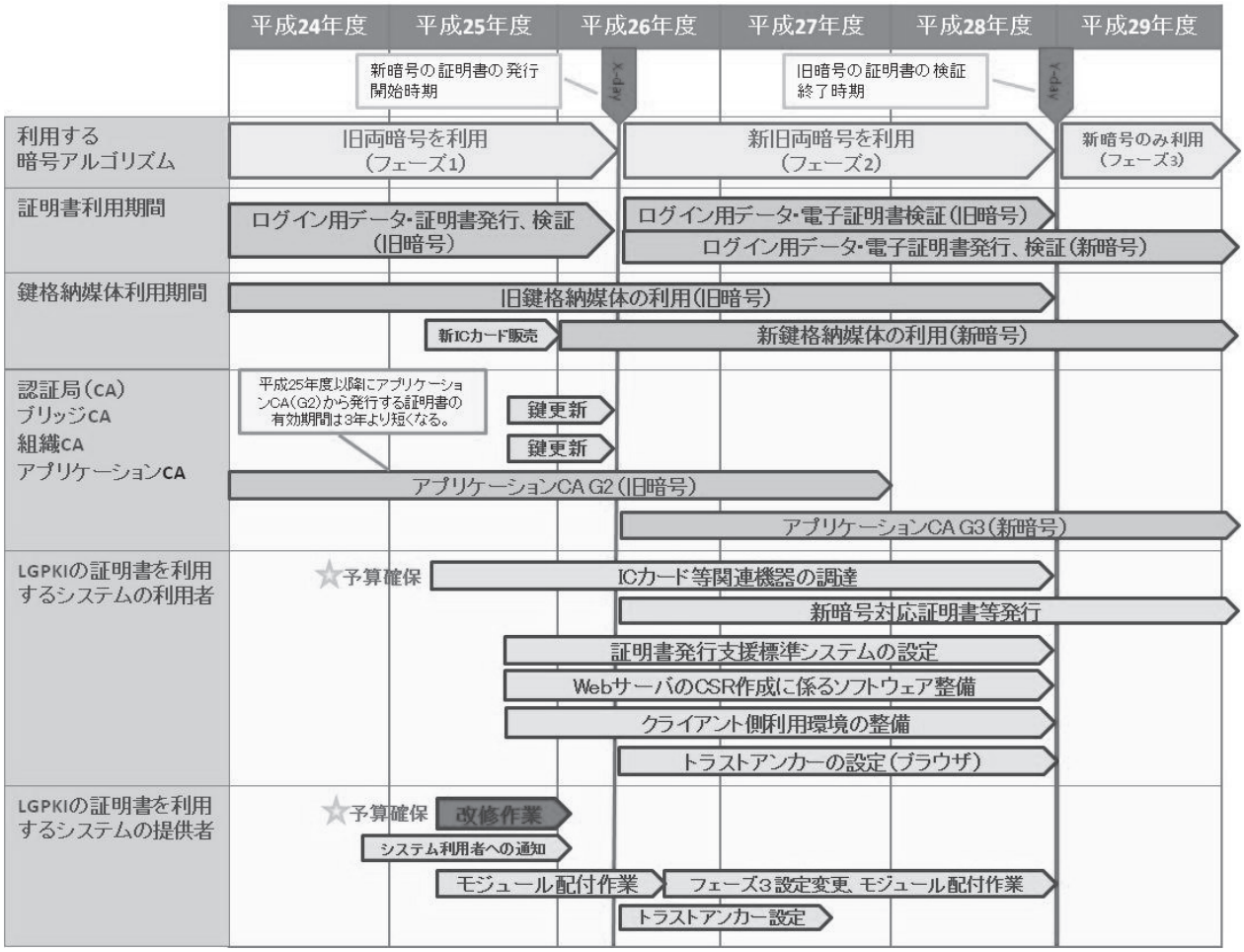
[2] 十分に大きな素数を掛け合わせた数の素因数分解が難しいことを暗号技術の基礎とした公開鍵暗号方式の一つ。公開鍵暗号方式では、一般に公開している「公開鍵」と本人のみが保有する「秘密鍵」の対になる二つの鍵を使ってデータの暗号化／復号化を行う。今回の暗号アルゴリズムの移行において、その鍵長を1024bitから2048bitに移行することで、暗号強度をさらに高める

[3] 任意の長さのデータから256bitのハッシュ値と呼ばれる値を作成するアルゴリズム

[4] 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・検討及び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）

[5] 平成24年度第1回LGWAN運営協議会議案第4号において決定
(http://center.lgwan.jp/conference/doc/gm_material_120523/gian4.pdf)

図－1　暗号アルゴリズム全体移行スケジュール



「フェーズ３」としています。

（２）移行方針

LGPKIにおける暗号アルゴリズムの移行方針は、表－１のとおりです。

3　暗号アルゴリズムの移行に伴い対応が必要となる事項

暗号アルゴリズムの移行は、主に証明書を利用した暗号化、電子署名の付与及び証明書検証機能に影響があり、LGPKIの証明書を利用するシステムの提供者と当該システムの利用者において、次に示す作業が必要となります[7]。

（１）システムの利用者において必要な事項

暗号アルゴリズムの移行に伴う、システム利用者の作業は、表－２のとおりです。

ア　平成24年度中に実施する作業

（ア）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

フェーズ２以降、ログイン用データ及び証明書は新暗号で発行されるため、発行等申請には、新暗号

[6] 政府の情報セキュリティ対策推進会議第８回会合（平成24年10月26日開催）において、政府機関の暗号アルゴリズム（SHA-1及びRSA1024）に係る移行指針が改定され、新暗号方式の電子証明書の発行開始時期及び旧暗号の電子証明書の検証（有効性の確認）終了時期が見直された（http://www.nisc.go.jp/press/pdf/ciso_8_press.pdf）。これを受け、GPKIにおける移行スケジュールが見直された場合には、LGPKIにおいても移行スケジュールを見直す可能性がある。LGPKIの最新の暗号アルゴリズム全体移行スケジュールについては、LGWANポータルサイト（http://center.lgwan.jp/information/second2.html）を参照

表－1　LGPKIにおける暗号アルゴリズムの移行方針

各認証局の新暗号移行方法
各認証局の暗号アルゴリズムの移行については、次のとおりとする。 ・ブリッジCA[8]及び組織CA[9]については、鍵更新（認証局のCA秘密鍵を変更する処理方式）を実施する。 ・アプリケーションCA[10]については、第３代目の認証局として新たに設置する。
新旧暗号の証明書の利用について
平成26年度の暗号アルゴリズムの移行後、一定期間（平成29年度早期までを想定）は、利用者側の対応に必要な期間を考慮し、新旧双方の暗号アルゴリズムで発行した証明書を利用可能とする。ただし、旧暗号の証明書発行は停止となるため、有効性検証サービスのみ継続する。平成29年度早期（時期未定）以降は、新暗号の証明書のみ利用可能とする。
フェーズ２，３の期間中の証明書ポリシー及び証明書検証サーバ[11]の状態
「LGPKIの移行方針」（http://www.lgpki.jp/）に基づく。
フェーズ２，３の期間中の技術仕様及びプロファイル設計
「政府認証基盤相互運用性仕様書（移行期間編/移行完了編）（平成22年３月30日改定）（※）」に対応した、次のドキュメント[12]に基づき実施する 。 ・C-6-4-4　LGPKIプロファイル設計書（移行期間編/移行完了　編　http://center.lgwan.jp/library/second2.html#C-6-4-4） ・C-6-4-5　LGPKI技術仕様書（移行期間編/移行完了編　http://center.lgwan.jp/library/second2.html#C-6-4-5） ・C-6-4-6　LGWAN-PKI技術仕様書（移行期間編/移行完了編　http://center.lgwan.jp/library/second2.html#C-6-4-6） （※）http://www.gpki.go.jp/session/CompatibilitySpecifications_phase2.pdf http://www.gpki.go.jp/session/CompatibilitySpecifications_phase3.pdf

表－2　システム利用者における作業

項番	作業項目	対応完了時期
1	平成25年度に行う新暗号対応のICカード関連機器等の調達に係る予算確保	平成24年度中
2	利用者側クライアント（住民・団体職員）の環境整備	フェーズ２開始まで
3	新暗号対応のICカード関連機器の調達事務	
4	LGWAN運営主体から提供しているシステムの改修に伴う再インストール	
5	新暗号対応のログイン用データ及び証明書発行申請	フェーズ２以降
6	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	

対応のICカード等関連機器が必要となり、証明書利用者（以下「利用者」という。）において当該機器の調達に係る予算を確保する必要があります。

新暗号対応のICカード等関連機器の提供価格は、LGWAN運営主体からLGWAN接続団体に別途通知しておりますので[13]、それを参考にしてください。

[7] 対応しない場合、平成26年度以降、地方公共団体のシステムで利用する電子証明書の検証ができず電子申請及び電子調達システム等、システムが動作しなくなる恐れがある

[8] LGPKI 組織認証局との相互認証及び政府認証基盤等の外部認証基盤との相互認証のために運営される認証局

[9] 地方公共団体及び総合行政ネットワーク基本要綱第７条第2 項の規定によりLGWAN の機能の提供を受けることができることとされた団体の役職・職責を認証するための証明書を発行する認証局

[10] 地方公共団体、総合行政ネットワーク基本要綱第7条第2項の規定によりLGWANの機能の提供を受けることができることとされた団体及びLGWAN-ASPサービス提供者に対し、Webサーバ等の証明書を発行する認証局

[11] 電子申請システム等の電子行政サービスにおいて、住民・企業が電子署名等に用いた証明書について、地方公共団体がその有効性を検証するためのサーバ

[12] LGWANポータルサイトに掲載（LGWAN接続環境が必要です。）

[13] LGWAN接続団体に送付した資料はLGWANポータルサイト（http://center.lgwan.jp/information/second2.html）に掲載

イ　フェーズ２開始までに実施する作業

（ア）利用者側クライアント（住民・団体職員）の環境整備

利用者側クライアントにおいて、OS/ブラウザ、JRE等が新暗号に対応しているかを確認し、未対応の場合は、フェーズ２開始までに利用者側で対応する必要があります。

また、LGPKIの証明書を利用するシステムの提供者から暗号アルゴリズムの移行に対応したクライアントモジュール等が配付された場合には、利用者において適用作業を実施してください。

（イ）新暗号対応のICカード関連機器の調達事務

利用者は、新暗号対応の証明書等発行申請までに新暗号対応のICカード等関連機器を調達してください。

新暗号対応のICカード等の販売開始時期、型番等については、LGWAN運営主体から別途平成25年度上期中に案内する予定です。

（ウ）LGWAN運営主体側から提供しているシステムの改修に伴う再インストール

LGWAN運営主体が提供する証明書発行支援標準システム[14]については、CSR[15]の鍵ペアを2048bitで作成するために必要な改修が行われます。

そのため、新暗号の証明書等の発行に当たっては、利用者において、新暗号に対応したシステムの再インストールが必要となります。

詳細については、システムの準備が整い次第、LGWAN運営主体から別途平成25年度上期中に案内する予定です。

ウ　フェーズ２開始以降に実施する作業

（ア）新暗号対応のログイン用データ及び証明書発行申請

表－３　暗号アルゴリズムの移行に伴う証明書発行等申請における変更点

証明書の種類	フェーズ１まで	フェーズ２以降
Webサーバ証明書[17]	・鍵ペア生成ソフトウェアにおいて1024bitの鍵長でCSRを作成	・鍵ペア生成ソフトウェアにおいて2048bitの鍵長でCSRを作成
ログイン用データ及びWebサーバ証明書以外の証明書	・現行の証明書発行支援標準システムで1024bitの鍵長でCSRを作成	・新暗号対応の証明書発行支援標準システムで2048bitの鍵長でCSRを作成

フェーズ２以降、新暗号対応のログイン用データ及び証明書を発行します。

暗号アルゴリズムの移行に伴う証明書発行等申請における変更点は、表－３のとおりです。なお、登録分局[16]からLGWAN運営主体への申請に利用している証明書発行等申請管理システムについては、原則として現行の操作方法を変更しない予定です。

（イ）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

フェーズ２以降、新暗号対応の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利用者は、新暗号対応のブラウザの利用並びに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Webブラウザの「信頼できるルート証明機関」に登録することで検証が可能になります。

各Webシステムの利用者のブラウザがInternet Explorerである場合、通常、自己署名証明書はブラウザのルート証明機関に自動で登録されます。インターネットにアクセスできない端末やInternet Explorer以外のブラウザを使用している場合は、手動で自己署名証明書をブラウザのルート証明機関に登録してください。

[14] 鍵ペアと証明書発行要求の作成等を行うための専用ソフトウェア
[15] 証明書発行要求。証明書を発行する際の元となるデータのこと
[16] LGWAN運営主体からの委任により、登録局で行う利用者からの証明書の発行、更新、失効申請の受付及び審査業務の一部を行う運営体制のこと
[17] Webサーバ証明書を発行する場合には、CSRを生成するソフトウェアがSHA256、RSA2048で作成可能かを事前に確認する必要がある

（2）システムの提供者側の作業

LGPKIの証明書を利用するシステムの提供者の作業は表－４に示すとおりです。

ア　平成24年度中に実施する作業

暗号アルゴリズムの移行に伴い、フェーズ２開始までにLGPKIの証明書を利用するシステムについては、必要に応じて改修が生じます。

そのため、平成24年度中に、①LGPKIの証明書を利用した電子署名付与並びに検証に関する機能の装備状況の洗い出し、②改修・機器更新等の必要性の確認、③これらの実施に係る予算の確保が必要となります。

参考として、電子調達システムにおける影響（参考１）と各証明書を利用しているシステムにおける確認事項（参考２）を次に示します。

表－４　システム提供者側における作業

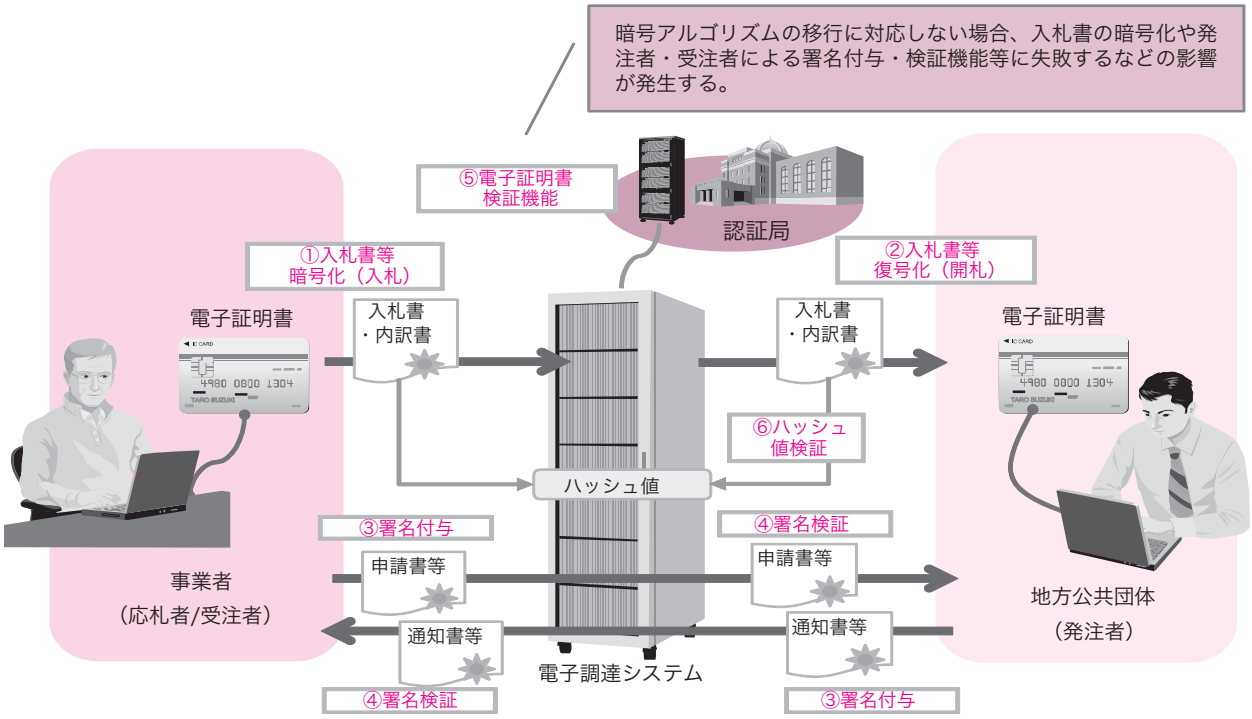
項番	作業項目	対応完了時期
1	LGPKIの証明書を利用しているシステムの改修の必要性の確認及び予算の確保	平成24年度中
2	改修作業・機器増設等の実施並びに利用者への通知	フェーズ２開始まで
3	署名検証要求を行うシステムにおけるトラストアンカー設定作業	フェーズ２以降

イ　フェーズ２開始までに実施する作業

システムの改修等が必要な場合は、フェーズ２開始までにシステム提供者側での作業を完了する必要があります。システムの改修に当たっては、必要に応じてLGWAN運営主体側で用意する新暗号検証環境（平成25年１月運用開始予定）の利用が可能です[18]。

また、システム利用者に対して、暗号アルゴリズムの移行に対応したクライアントモジュールの配付、利用環境の整備の依頼並びに当該システムに係

参考１　電子調達システムにおける影響



[18] 新暗号検証環境は、本番運用環境を最小限の構成で構築した模擬環境である。LGPKIの証明書を利用したシステムの提供者において、システム改修に伴う疎通試験、ICカードRWのドライバソフトウェアのバージョンアップに伴う評価等の動作検証において利用する

参考2　各証明書を利用しているシステムにおる確認事項

証明書の種類	確認事項
職責・利用者証明書	職責証明書及び利用者証明書を使用してシステムへのログインや署名・検証を行っているかを確認。行っている場合は、システム改修が必要か否かを確認
Webサーバ証明書	フェーズ２以降、Webサーバ証明書を発行する際には、CSRをSHA256、RSA2048で作成する必要があるため、鍵ペア生成ソフトウェアにおいて、鍵長として2048bit、署名アルゴリズムとしてSHA256の設定が可能かを確認
メール用・コードサイニング証明書	メール用証明書の場合は、電子署名付与・検証を行っているブラウザやメールクライアント（Outlookなど）、コードサイニング証明書の場合は、電子署名付与・検証を行っているブラウザや署名ツール（Microsoft Authenticodeなど）が、新暗号に対応しているかを確認

る移行スケジュール等について通知する必要があります。

ウ　フェーズ２開始以降に実施する作業

LGPKIに対して証明書の検証要求を行うシステムにおいて、トラストアンカー[19]設定作業を行ってください。主に次の設定が必要となります。

・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
・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
・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

4　おわりに

LGPKIの暗号アルゴリズムの移行に当たっては、LGPKIの証明書を利用するシステムの提供者、利用者並びに運営主体等関係者の協力が不可欠となります。運営主体としましても、今後、LGWANポータルサイト等[20]で暗号アルゴリズムの移行に関連した情報をタイムリーに提供し、また、円滑で効率的な移行作業の実現を目指して参りますので、引き続き関係各位のご協力をお願いいたします。

19　証明書検証における認証パス構築の際の信用の基点のこと
20　http://center.lgwan.jp

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24年11月12日現在）

■LGWAN接続団体　524/1813団体
■LGWAN-ASP　30/190 ASP

LGWAN-ASPサービス接続／登録状況（平成24年11月12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：313件　■ホスティング　接続：190件
■通信　登録：169件　■ファシリティ　登録：237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