LGWAN

Local Government Wide Area Network

総合行政ネットワーク

No. 185

特集　次期LGPKIへの移行について

地方公共団体の行政事務専用に設けた公開鍵基盤（PKI）である地方公共団体組織認証基盤（以下「LGPKI」という。）では、第三次LGPKI（以下「現行LGPKI」という。）として平成24年度から現在まで継続運用しているところですが、平成31年度から新たに次期LGPKI（以下「第四次LGPKI」という。）に完全移行する予定です。

今月号では、第四次LGPKI移行に伴うLGPKI発行の電子証明書移行方針、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）の提供者における現時点（平成30年１月末）で想定される影響及び移行スケジュールについて説明します。

1　第四次LGPKI移行の背景とその概要

第四次LGPKIは、平成28年度に策定した第四次総合行政ネットワーク整備計画書において、外部認証局を活用することとしており、「地方公共団体組織認証基盤の構築及び運用業務」に係る調達の結果、認証局運営事業者をセコムトラストシステムズ(株)とすることに決定しました。

これまで、自前で運用していた現行LGPKIとは異なり、外部認証局のソリューションを活用して運用経費を低減しつつ、かつ、セキュリティは現状の水準を維持することを実現するとともに、利便性の向上を両立するため、第四次LGPKIの構築を開始しました。

それでは、第四次LGPKI移行における主なポイントについて説明します。

2　電子証明書について

（１）証明書の再発行

第四次LGPKIでは、基本的に新たに認証局を構築し、新しい証明書を発行していくことになります※1。そのため、地方公共団体で利用している各証明書について、表－１のとおり対応方針を整理しました。

前述のとおり、証明書は「再発行」することになり、現行LGPKIで発行している職責証明書・利用者証明書、Webサーバ証明書などは、平成31年３月末までの利用となります。そのため、平成30年８月ごろから平成31年３月までおよそ８ヵ月間で証明書の再発行を行う必要が生じます。

あわせて、現在LGWANの運営主体で提供している証明書発行支援標準システムや証明書発行等申請管理システム（CIRS）も第四次LGPKI向けに再構築され、操作性や操作イメージが容易になるよう見直しを行い利便性の向上を図ります。主な変更点については、後述の「３ LGWANの運営主体から提供しているシステムについて」で説明します。

また、再発行の際に必要となるICカードやUSBトークンなど、現行LGPKIで動作保証されている鍵格納媒体は継続利用が可能となる予定で

※１　現在発行済みの暗号化通信用等証明書（以下「暗通証明書」という。）は再発行による現時点での影響を考慮し、平成33年３月末（次期は予定）まで、現行の認証局システム（CA秘密鍵）を継続運用します。現在発行済みの暗通証明書の有効期限が切れる平成33年３月末をめどに、暗通証明書は新しく構築した認証局からの発行に順次移行する予定です。

す※2。

（2）Webサーバ証明書について

Webサーバ証明書について現行LGPKIでは「インターネット向け」と「LGWAN内部向け」に発行していました。第四次LGPKIではインターネット向けのWebサーバ証明書の利便性が大きく向上します。

第四次LGPKIのインターネット向けWebサーバ証明書は、表－１にも示したとおり、セコムトラストシステムズ（株）の既存のサービスを活用し、新たに証明書を発行して運営していきます。また、第四次LGPKIでは、「セコムパスポートfor Web SR3.0」を活用することにより、図－１のとおり、これまで現行LGPKIでは対応不可であった主要なブラウザ（Mozilla Firefox、Google Chrome）を始め、主要OS（Windows、Mac OS）と、国内主要通信キャリアのスマートフォン、フィーチャーフォンなど様々なOS・ブラウザ環境で警告が出ることなく利用することが可能となります※3。

また、「セコムパスポート for Web SR3.0」サービスは、図－２のとおり、一つの証明書に対して複数のウェブサーバ名（FQDN）を登録（マルチドメイン）することが可能です。これにより、一つのウェブサーバ上で複数のウェブサイトを運営する場合でも、一つの証明書ですべてのウェブサイトがTLS/SSL通信を行うことができます。

表－１　LGPKI証明書の対応方針

No	証明書の種類	現行LGPKI証明書の対応方針	次期LGPKI証明書の対応方針
1	職責証明書 利用者証明書	現在利用している証明書は、平成31年３月末までに利用ができなくなります。	新しく構築した認証局から、新たに証明書の発行します。 （平成30年８月ごろから発行開始）
2	暗号化通信用等証明書	再発行によるマイナンバーへの影響を考慮し、発行済み暗号化通信用等証明書はシステムを延命し、発行・失効、失効リストの発行の機能に限定し、平成33年３月末（次期は予定）まで継続します。	現在発行済みの暗号化通信用等証明書の有効期限が切れる平成33年３月末をめどに、新しく構築した認証局から、新たに証明書の発行します。
3	Webサーバ証明書 メール用証明書 コードサイニング証明書 （インターネット側で利用）	現在利用している証明書は、平成31年３月末までに利用ができなくなります。	セコムトラストシステムズの認証局サービスを活用し、新たに証明書の発行します。（平成30年８月ごろから発行開始） [インターネット環境用Webサーバ証明書] ・セコムパスポート for Web SR3.0 ※EV2.0サービスは検討中 [メール署名用証明書／コードサイニング証明書] ・セコムパスポートfor PublicIDサービス
4	Webサーバ証明書 コードサイニング証明書 （LGWAN内部環境用で利用）※ASP含む	現在利用している証明書は、平成31年３月末までに利用ができなくなります。	新しく構築した認証局から、新たに証明書の発行します。 （平成30年８月ごろから発行開始）

※２　三菱社製、ペンティオ社製ともに、新ICチップが搭載されたICカードやUSBトークンが新たに販売されるとの通知があり、平成30年度に新ICチップ搭載の新鍵格納媒体の導入を予定しています。この新ICチップ搭載のICカードやUSBトークンについても第四次LGPKIにて利用可能とします。

※３　セコムパスポートfor Web SR3.0　https://www.secomtrust.net/service/pfw/pfw_service/sr30.html
対応環境　https://www.secomtrust.net/service/pfw/pfw_service/service_hikaku.html

証明書の発行費用については、これまでと同様に地方公共団体向けの発行は無償となります。現在、現行LGPKIを利用せず、セコムトラストシステムズ（株）を含む外部認証局よりWebサーバ証明書を購入されている場合は、第四次LGPKIの活用により、証明書発行費用の個別負担が不要となります。

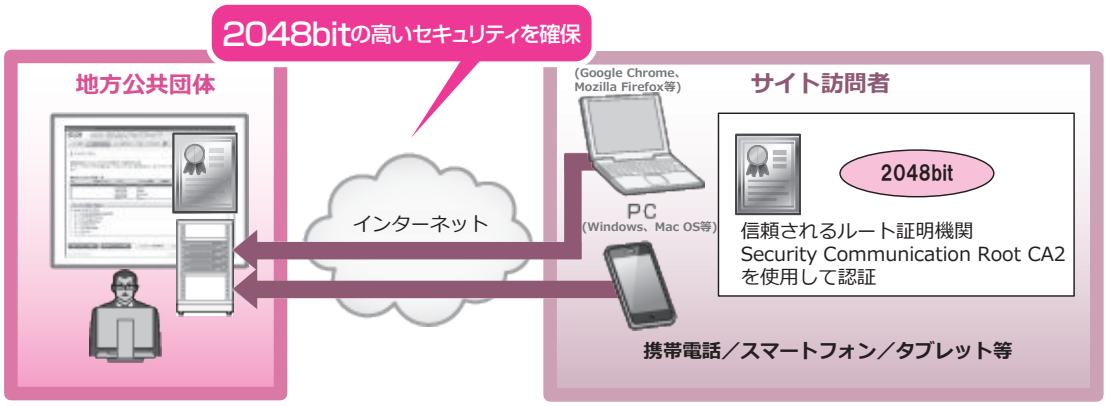
第四次LGPKIのLGWAN内部向けWebサーバ証明書については、これまでと同様にインターネットなどの外部通信が不可となる（パブリックなDNSで名前解決ができない）LGWAN内部環境で、TLS/SSL通信を必要とするウェブサーバに対して、Webサーバ証明書を発行可能とします。地方公共団体を含むLGWAN-ASPサービス提供者などが発行対象者であり、LGWAN内部のみでの利用に限定するため、サーバ認証時（ウェブサイトへのアクセス時）に外部との通信は発生しません。

3 LGWANの運営主体から提供しているシステムについて

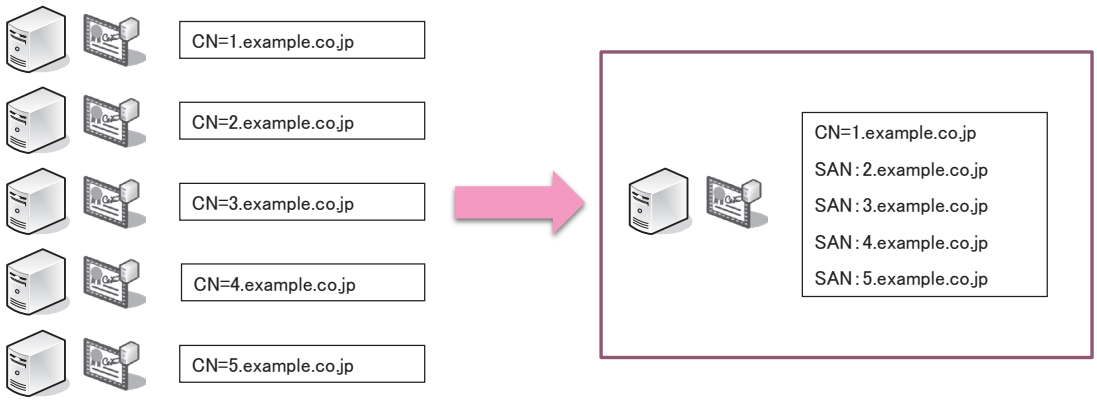
（1）LGPKIの証明書発行に必要なシステム

LGWANの運営主体から提供しているLGPKIの証明書発行に必要なシステムとして、鍵ペアを生成し証明書を格納する「証明書発行支援標準システム（以下「標準システム」という。）」と証明書を電子的

図－1 インターネット側Webサーバ証明書利用イメージ



図－2 複数のウェブサーバ名（FQDN）を登録（マルチドメイン）イメージ



なオンラインで申請することができる「証明書発行申請管理システム（以下「CIRS」という。）」があります。

標準システムとCIRSはともに、表－２のとおり、第四次LGPKI向けにシステム更改を実施します。システム更改の基本的な方針として、基本機能（証明書の申請、ダウンロード等）は現行システムを踏襲しつつ、ユーザーインターフェースを変更するなど利便性を向上した新システムを提供します。

現行LGPKIでは、CIRSにログインするための電子証明書として、「ログイン用データ」が必要でした。第四次LGPKIにおける新システムでも、証明書の発行申請をするために、ログイン用データの電子証明書は必要となりますが、これまでと異なり、ICカードのような媒体は必要がなく、新システムを利用する端末に電子証明書をインストールする仕様に変更となります。

（２）電子証明書の検証に必要なシステム

インターネットにおいて提供されている電子申請・入札システム等の電子行政サービスにおいて、電子証明書の検証を実施するため、現行LGPKIでは、「証明書検証サーバ※4（以下「CVS」という。）」を提供しています。第四次LGPKIにおいても、現行と同様に提供します。

現在、CVSとCVSクライアント間のSSL通信では、アプリケーション認証局（APCA G4）から発行したWebサーバ証明書を利用しています。このWebサーバ証明書は、第四次LGPKIにおいては別途発行するWebサーバ証明書へ切り替えます。

そのため、CVSを利用して電子証明書を検証している場合、CVSを利用するアプリケーションについて、CVSとのSSL通信で利用するトラストアンカー※5は証明書を発行した認証局の自己署名証明書に変更する必要があります。

なお、第四次LGPKI移行におけるCVSのアクセス先に変更はない予定です。

4 第四次LGPKI移行の概略スケジュール

第四次LGPKIは、平成31年４月の完全移行に向けて構築業務がスタートしたところであり、図－３のとおり、平成30年中に新しい認証局、新しいシステムが稼働します。そのため、平成30年８月ごろからは、現行LGPKIと並行運用する期間となり、平成31年３月末で現行LGPKIを廃止する予定です。

今後は、第四次LGPKI移行に伴い、地方公共団

表－２　システム更改方針

No	LGWANの運営主体提供のシステム	システム更改方針
1	新たな標準システム	・基本機能（鍵生成、証明書格納）は現行システムを踏襲 ・ユーザーインターフェースを変更するなど利便性を向上 ・利用する端末にインストール・設定が必要 ・現行動作保証されている鍵格納媒体（「ICカード」「USBトークン」「ICカード読取装置等」）をできる限り、継続利用可能とする
2	新たなCIRS	・基本機能（証明書の申請、ダウンロード等）は現行システムを踏襲 ・ユーザーインターフェースを変更するなど利便性を向上 ・現行のシステムとは接続先が異なる ・ログイン用の電子証明書の取得が必要だが、現行とは異なり、ICカードのような鍵格納媒体は必要がなく、LGWANに接続する利用端末に証明書をインストールする

※４　政府認証基盤（GPKI）と相互認証を行っている認証局が発行した電子証明書の検証ができるシステムサーバ
※５　電子証明書を検証する利用者が信頼している認証局

体における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向けて、移行対応作業が必要となる事項を随時発信してまいります。

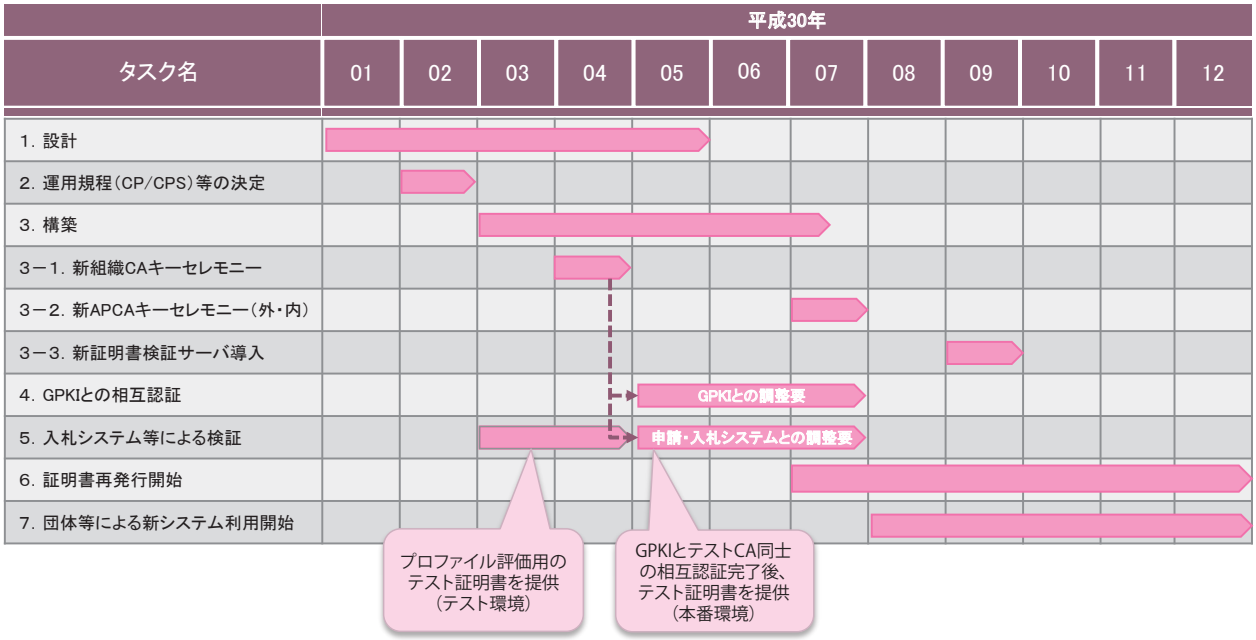
5 おわりに

第四次LGPKIへの移行にあたっては、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等関係各位の協力が不可欠となります。

LGWANの運営主体は、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。

この度の、第四次LGPKIへの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。

図－3 第四次LGPKI移行の概略スケジュール



LGWAN-ASPサービス登録／接続状況（平成30年２月１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：817件	■ホスティング	接続：480件
■通信	登録：184件	■ファシリティ	登録：369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