LGWAN

Local Government Wide Area Network

総合行政ネットワーク

No. 147

特集　LGPKIにおける暗号アルゴリズムの移行について（その2）

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。）の発行や証明書の有効性を検証するための仕組みについて、一部を除き、使用する暗号アルゴリズムを、旧暗号（SHA-1※1、RSA1024※2）から新たな暗号アルゴリズム（SHA256、RSA2048）（以下「新暗号」という。）に移行しました。

今回は、LGPKIにおける暗号アルゴリズムの移行に伴う変更点と暗号アルゴリズムの移行に関連した、よくある質問と回答をご紹介します。

1　暗号アルゴリズムの移行に伴う変更点

LGPKIにおける暗号アルゴリズムの移行に伴い、旧暗号のログイン用データ及び証明書の発行（更新）申請の受付を終了し、新暗号による発行（更新）申請のみの受け付けとなります※3。新暗号移行後もログイン用データ及び証明書の申請方法に変更はありませんが、申請にあたっては、新暗号対応の認証基盤用ICカード等関連製品及び証明書発行支援標準システム※4が必要となります。

また、証明書検証サーバ（以下「CVS」という。）については、新旧両暗号の証明書の検証が可能となりました。

さらに、ウェブサーバ証明書等を発行するアプリケーション認証局の暗号アルゴリズムの移行及びCVSのあて先追加に伴い、次のとおり変更が生じます。

（1）階層型モデルによるアプリケーション認証局の構築に伴う変更

アプリケーション認証局の暗号アルゴリズムの移行においては、新暗号に対応したアプリケーション認証局（第三世代）（以下「APCA G3」という。）を新たに構築します。

また、APCA G3は、階層型モデルで構築され、従来の単独型モデルの旧暗号のアプリケーション認証局（第二世代）と比較し、次の点が変更になります（図－1）。

①アプリケーション証明書を発行する認証局

アプリケーション証明書（ウェブサーバ証明書、

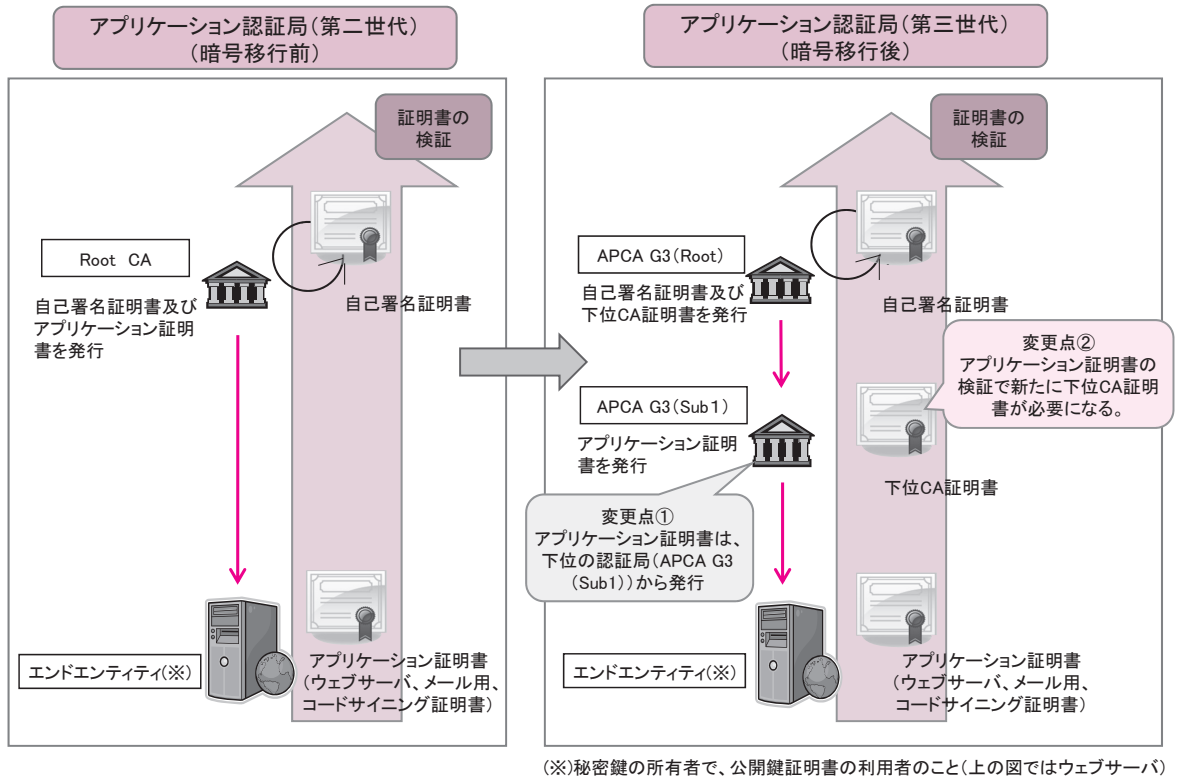
※1　任意の長さのデータから160bitの「ハッシュ値」と呼ばれる値を作成するアルゴリズム。ハッシュ値から元のデータは復元できず、元のデータに変更が加えられると、ハッシュ値は異なる内容になるため、改ざん検知などに用いられる。なお、新暗号のSHA256の場合は、256bitのハッシュ値を作成する。

※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。

※3　旧暗号のログイン用データ及び証明書の失効（廃止）申請は、暗号アルゴリズムの移行後も引き続き受け付ける。

※4　鍵ペアの生成、ログイン用データ／証明書発行要求ファイル（CSR）の作成及び発行済みのログイン用データ／証明書をICカード等に格納する際に使用するシステム。LGWANポータルサイトからダウンロードし、端末にインストールして利用する（http://center.lgwan.jp/library/second9.html#K-3-3）。

図－1　アプリケーション認証局の暗号アルゴリズムの移行に伴う変更点



（※）秘密鍵の所有者で、公開鍵証明書の利用者のこと（上の図ではウェブサーバ）

メール用証明書及びコードサイニング証明書）は、階層型認証局のうち、下位の認証局（APCA G3（Sub1））から発行されます。

②アプリケーション証明書の検証で必要な証明書

①の変更に伴い、アプリケーション証明書の検証において、最上位の認証局（APCA G3（Root））の自己署名証明書に加えて、「下位CA証明書※5」が必要になります。

例えば、証明書の発行対象がウェブサーバの場合、ウェブサーバの管理者は、ウェブサーバ証明書とあわせて下位CA証明書をあらかじめウェブサーバにインストールしておく必要があります。これにより、クライアントからウェブサーバへのSSL接続要求時に、ウェブサーバからクライアントにウェブサーバ証明書及び下位CA証明書が送付されるようになります。

クライアントは、ウェブサーバから送付された証明書と自己署名証明書を使用して、ウェブサーバ証明書の検証を行います（図－２）。自己署名証明書は、クライアントのブラウザにあらかじめインストールされているため※6、本仕様変更に伴うクライアント側の作業は、基本的に不要です。

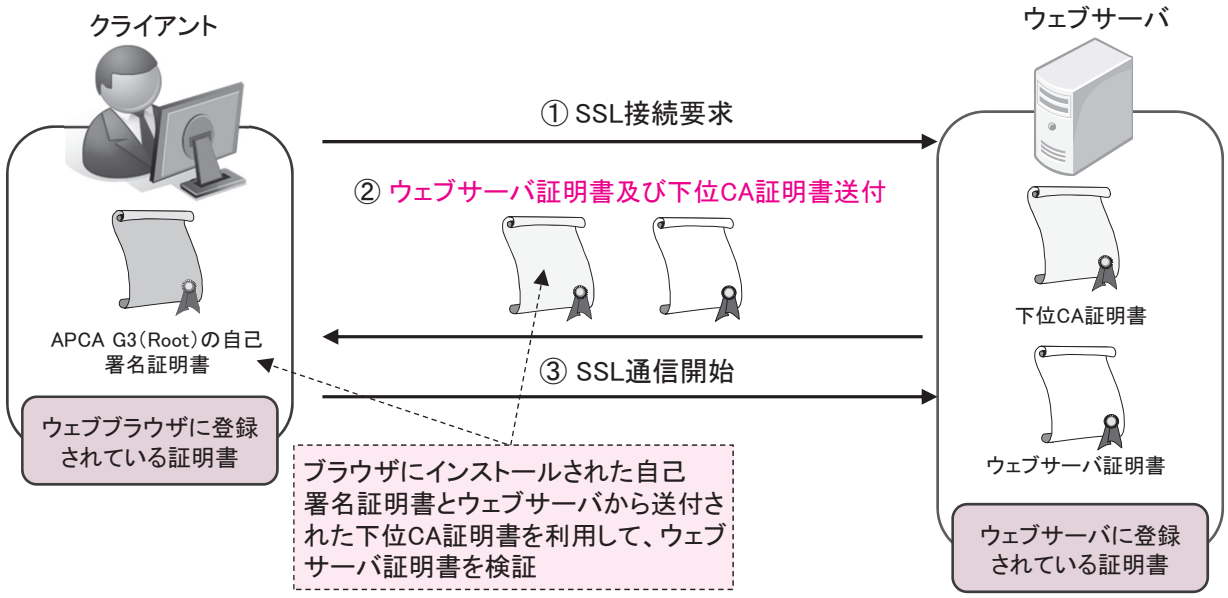
（２）CVSのあて先追加

CVSについては、アプリケーション認証局の暗号アルゴリズムの移行にあわせて、証明書検証要求のあて先（新CVS）を新たに追加します。新CVSにおいては、新CVSとCVSクライアント間のSSL通信で利用するウェブサーバ証明書がAPCA G3から発行された新暗号対応の証明書になります。

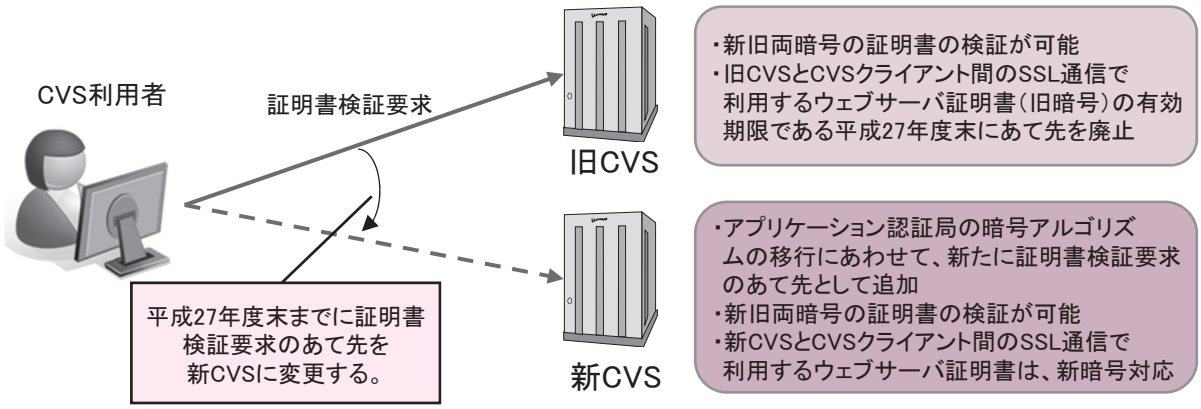
なお、移行前から稼働している旧CVSの証明書検証要求のあて先については、旧CVSとCVSクラ

※５　APCA G3（Root）が発行する、下位CAが信頼できるものであることを証明した証明書のこと。
※６　自己署名証明書がブラウザにあらかじめインストールされているのは、現時点ではInternet Explorerのみとなる。Internet Explorer以外のブラウザを利用する場合は、事前に自己署名証明書をブラウザにインストールしておく必要がある。

図－２　ウェブサーバ証明書の検証



図－３　CVSのあて先追加



イアント間のSSL通信で利用している旧暗号のウェブサーバ証明書が有効期限切れとなる平成27年度末に廃止するため、CVS利用者は、平成27年度末までに証明書検証要求のあて先を新CVSに変更する必要があります（図－３）。

2　暗号アルゴリズムの移行に関連したよくある質問と回答

暗号アルゴリズムの移行にあたり、これまで多くの質問が寄せられました。その中から、よくある質問と回答をご紹介します。

また、暗号アルゴリズムの移行に伴い、対応が必要な事項については、これまでにLGWAN接続団体に送付した通知[※7]及び本誌平成26年８月号LGWAN特集記事「LGPKIにおける暗号アルゴリズムの移行について[※8]」でもご説明していますので、あわせて参考にしてください。

※７　http://center.lgwan.jp/information/second2.html#PKI_Ikou
※８　https://www.j-lis.go.jp/data/open/cnt/3/260/1/LGWAN-H2608.pdf

Q.１：ログイン用データ、職責証明書及び利用者証明書の有効期間は５年になったのでしょうか？

A.１：組織認証局から発行するログイン用データ、職責証明書及び利用者証明書は、暗号アルゴリズム移行後は、有効期間「５年」で発行します。

なお、アプリケーション認証局から発行するウェブサーバ証明書、メール用証明書及びコードサイニング証明書については、暗号アルゴリズム移行後も有効期間は「３年」で発行します。

Q.２：暗号アルゴリズム移行前に発行したログイン用データ、職責証明書及び利用者証明書は、暗号アルゴリズム移行後も引き続き利用することができるでしょうか？

A.２：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、各証明書については、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できます。

なお、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ウェブサーバ証明書、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、最長で当該認証局を廃止する平成27年度末までとなります。

Q.３：暗号アルゴリズムの移行後、ログイン用データ及び証明書の申請にあたり、新暗号対応の認証基盤用ICカード等関連製品が必要となりますが、所有している製品が新暗号に対応しているか、どのように確認すればよろしいでしょうか？

A.３：LGWAN用バージョン確認ツール（※）をPCにインストールし、利用中（又は利用予定）のPCの環境を確認してください（一部本ツールのサポート対象外の製品があります。）。

なお、ICカード読取装置及び各種ドライバソフトウェアであれば、ICカード読取装置又はインストール媒体（CD-R）に記載の型番、版名で確認することもできます。

（※）http://center.lgwan.jp/information/doc/LGWANVERCHK.lzh

Q.４：新暗号対応の認証基盤用ICカード等関連製品はどこから調達すればよろしいでしょうか？　地元事業者（代理店）から購入できますか？

A.４：認証基盤用ICカード等関連製品については、「F-1-1-3総合行政ネットワーク接続仕様書（資料編）別冊 認証基盤用IC カード読取装置及びICカード等鍵格納媒体仕様（※１）」において製品の指定はしていますが、購入先は限定していませんので、代理店を通じての購入も可能です。本資料には代理店の情報は掲載していませんので、製品の提供事業者に個別に問い合わせてください。

なお、現在販売中の製品は、すべて新暗号に対応しています。

また、各製品の動作条件（OS、ブラウザの組み合わせ）等については、「ICカードを使用する場合の必要なシステム環境（※２）」を参照してください。

（※１）http://center.lgwan.jp/library/second3.html#F-1-1-3
（※２）http://center.lgwan.jp/use/doc/CSR_kankyou20140820.pdf

Q.５：新暗号対応のドライバソフトウェアは、旧暗号対応のログイン用データや各種証明書でも利用できますか。

A.５：新暗号対応製品については、旧暗号にも対応していますので、利用することができます。

3　おわりに

平成26年９月に実施したLGPKIにおける暗号アルゴリズムの移行においては、関係者各位のご協力の下、円滑に作業を進めることができました。今後も、LGWAN接続団体の登録分局、ASP提供者及び関連機関と連携し、証明書発行業務、証明書検証サービス及び政府認証基盤（GPKI）との相互認証業務など、認証局運営業務の安全かつ安定的な運用に努めてまいりますので、引き続き、認証局の運営業務にご理解、ご協力をお願いいたします。

LGWAN-ASPサービス登録／接続状況（平成26年12月５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：388件	■ホスティング	接続：237件
■通信	登録：180件	■ファシリティ	登録：308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