LGPKI の移行方針について

1　LGPKI の移行方針

LGPKI のブリッジ認証局（以下「BCA」という。）、組織認証局（以下「組織 CA」という。）及びアプリケーション認証局（以下「APCA」という。）並びに証明書検証サーバ（以下「CVS」という。）の新暗号への移行方針は、次のとおりである。

本資料中のフェーズ１～３については、次のとおり定義する。ただし、APCA については、現行の旧暗号対応の APCA の公開鍵及び秘密鍵の有効期間満了となる平成 27 年度末をもって現行の APCA を廃止するため、新旧両暗号利用期間及び新暗号のみの利用期間が組織 CA と異なる。詳細は、1.2.2 の APCA の移行方針を参照すること。

・フェーズ１：現在の旧暗号利用期間

・フェーズ２：新旧両暗号の利用期間（平成 26 年 9 月 16 日[1]～平成 29 年度早期）

・フェーズ３：新暗号のみの利用期間（平成 29 年度早期以降）

なお、現行 LGPKI で使用している署名アルゴリズム(sha1WithRSAEncryption)及び鍵長(1024 ビット）を総称して「旧暗号」という。また、暗号アルゴリズム移行後に使用する署名アルゴリズム（sha256WithRSAEncryption）及び鍵長（2048 ビット）を総称して「新暗号」という。

1.1　BCA 及び組織 CA の使用する暗号アルゴリズム及び移行方針

1.1.1　使用する暗号アルゴリズム

暗号アルゴリズム移行後、BCA 及び組織 CA が発行する電子証明書（以下「証明書」という。）及び失効リストの署名アルゴリズムは、全て「sha256WithRSAEncryption」とする。また、各証明書の鍵長は全て「2048 ビット」とする。

なお、旧暗号による証明書と新暗号による証明書を区別可能とするため、新暗号で発行する職責証明書及び利用者証明書の証明書ポリシには、旧暗号で発行する職責証明書及び利用者証明書の証明書ポリシとは異なるオブジェクト識別子（OID）を採用する。

1.1.2　BCA 及び組織 CA の移行方針

(1) フェーズ 1

BCA 及び組織 CA は、フェーズ１の期間中、新暗号へ移行しない。

また、LGPKI は相互認証を行っている他認証ドメイン（政府認証基盤（GPKI））と同期を取って新暗号へ移行するため、BCA と他認証ドメインに属する CA が発行する相互認証証明書も新暗号へ移行しない。

フェーズ 1 における証明書、CRL 及び相互認証の状態を図 1-1 に、相互認証証明書の証明書ポリシの状態を表 1-1 に示す[2]。なお、利用者証明書用についても職責証明書用と同様で

---

[1] 現時点では、平成 26 年 9 月 13 日～15 日にかけて暗号アルゴリズムの移行作業を実施する予定である。

[2] 政府認証基盤（GPKI）と民間 CA 等との間の相互認証証明書の証明書ポリシ状態については、「政府認証基盤相互運用性仕様書（移行期間編）」を参照。

あるが、記載は省略する。

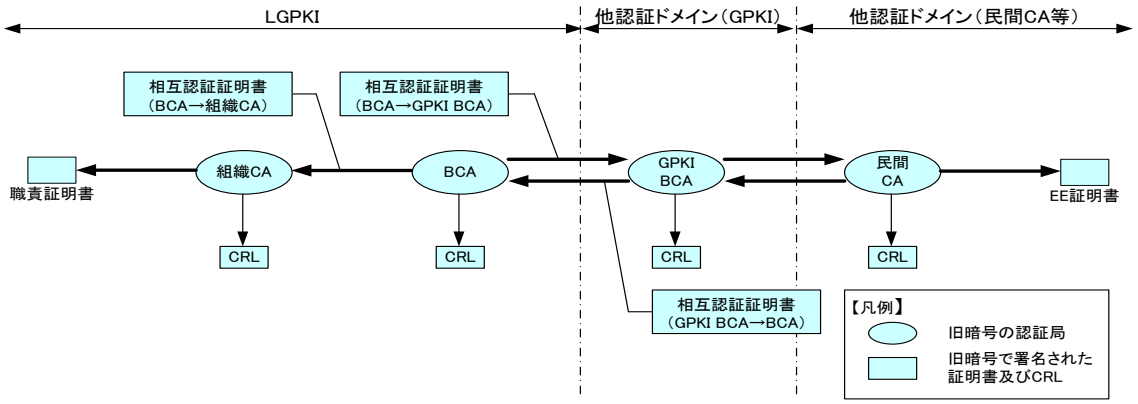

図 1-1 フェーズ 1 における証明書、CRL 及び相互認証の状態

表 1-1 フェーズ 1 における相互認証証明書の証明書ポリシの状態

証明書種別	証明書ポリシ	ポリシマッピング
相互認証証明書 （BCA→組織 CA）	職責証明書用の証明書ポリシ(旧暗号)	なし
相互認証証明書 （BCA→GPKI BCA）	職責証明書用の証明書ポリシ(旧暗号)	職責証明書用の証明書ポリシ(旧暗号) ＝官職証明書用の証明書ポリシ(旧暗号)
相互認証証明書 （GPKI BCA→BCA）	職責証明書用の証明書ポリシ(旧暗号)	官職証明書用の証明書ポリシ(旧暗号) ＝職責証明書用の証明書ポリシ(旧暗号)

(2) フェーズ 2

BCA 及び組織 CA は、フェーズ 2 開始時に鍵更新を行い、新暗号に移行する。新暗号への移行は他認証ドメイン（GPKI）と同期を取って実施する。

BCA は、鍵更新時に新暗号を用いて自己署名証明書及びリンク証明書を発行する。

BCA 及び組織 CA 間は、互いに新暗号による相互認証証明書の発行を行う。なお、旧暗号による相互認証証明書は、特別な事情がない限り、有効期限まで失効しない。[3]

BCA は、新暗号に移行した他認証ドメイン（GPKI）との間で、旧暗号による相互認証証明書の失効及び新暗号による相互認証証明書の発行を行う。

フェーズ 2 における証明書、CRL 及び相互認証の状態を図 1-2 に、相互認証証明書の証明書ポリシの状態は、表 1-2 のとおりである。

[3] 新暗号への移行前に発行された証明書の検証を可能とするため。

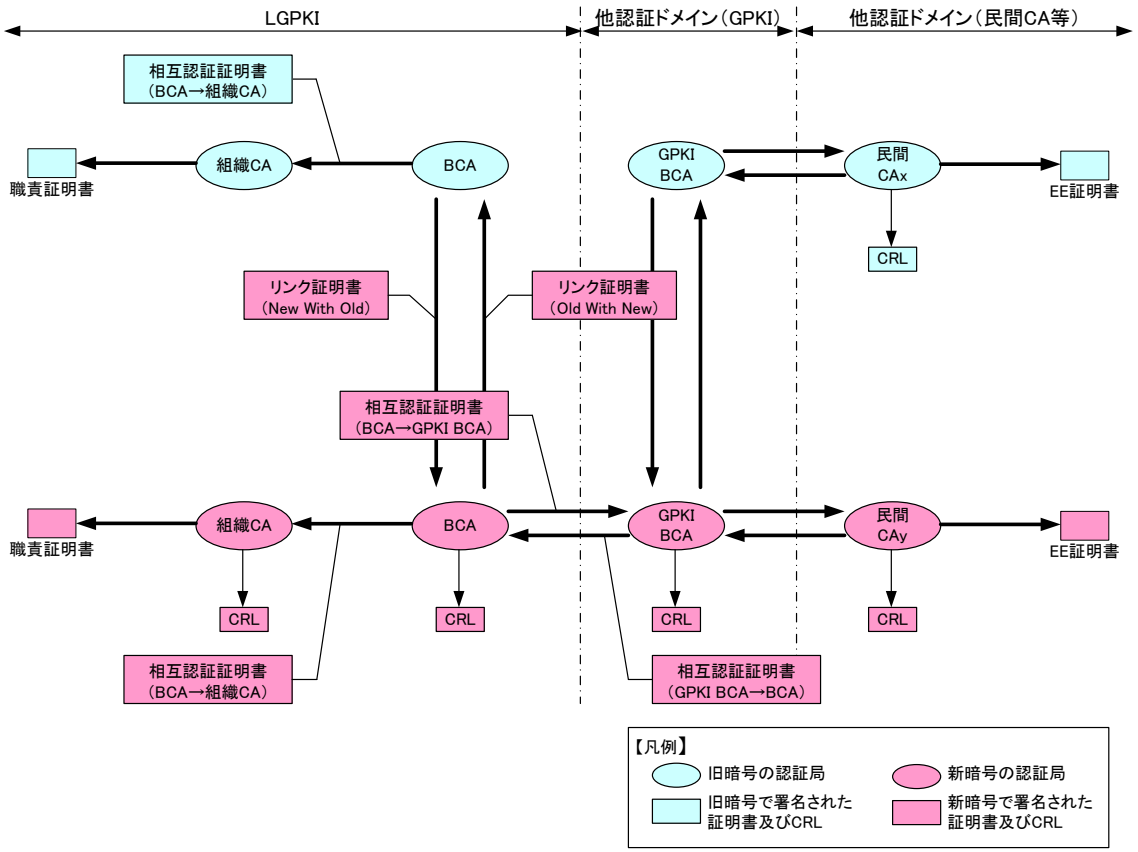

図 1-2 フェーズ 2 における証明書、CRL 及び相互認証の状態

表 1-2 フェーズ 2 における相互認証証明書の証明書ポリシの状態

証明書種別	証明書ポリシ	ポリシマッピング
相互認証証明書 （BCA→組織 CA）	職責証明書用の証明書ポリシ(旧暗号)	なし
相互認証証明書 （BCA→組織 CA）	職責証明書用の証明書ポリシ(新暗号)	なし
相互認証証明書 （BCA→GPKI BCA）	職責証明書用の証明書ポリシ(旧暗号) 職責証明書用の証明書ポリシ(新暗号)	職責証明書用の証明書ポリシ(旧暗号) ＝官職証明書用の証明書ポリシ(旧暗号)
		職責証明書用の証明書ポリシ(新暗号) ＝官職証明書用の証明書ポリシ(新暗号)
相互認証証明書 （GPKI BCA→BCA）	官職証明書用の証明書ポリシ(旧暗号) 官職証明書用の証明書ポリシ(新暗号)	官職証明書用の証明書ポリシ(旧暗号) ＝職責証明書用の証明書ポリシ(旧暗号)
		官職証明書用の証明書ポリシ(新暗号) ＝職責証明書用の証明書ポリシ(新暗号)
		官職証明書用の証明書ポリシ(旧暗号) ＝職責証明書用の証明書ポリシ(新暗号)[4]

[4] GPKI と相互認証しているが、新暗号への移行が完了していない他の CA をトラストアンカとする署名検証者が、組織 CA から発行された新暗号の証明書を検証する場合の対応として設定

(3) フェーズ 3

組織 CA は、フェーズ 3 開始時点で、旧暗号で発行した EE 証明書のうち、有効なものがある場合には、認証局において強制失効する。

BCA 及び組織 CA は、互いに旧暗号による相互認証証明書の失効を行う。

BCA の旧暗号による自己署名証明書及びリンク証明書並びに組織 CA の旧暗号による自己署名証明書の公開を中止する。[5]

BCA は、他認証ドメイン（GPKI）との間の相互認証証明書を更新する。この相互認証証明書には新暗号による証明書ポリシのみを含める。

フェーズ 3 における証明書、CRL 及び相互認証の状態を図 1-3 に、相互認証証明書の証明書ポリシの状態は、表 1-3 のとおりである。

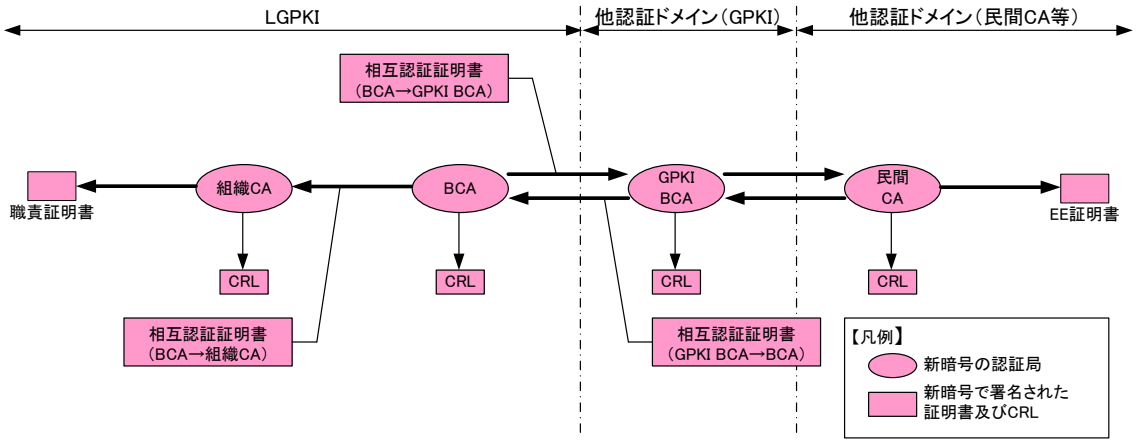

図 1-3 フェーズ 3 における証明書、CRL 及び相互認証の状態

表 1-3 フェーズ 3 における相互認証証明書の証明書ポリシの状態

証明書種別	証明書ポリシ	ポリシマッピング
相互認証証明書 （BCA→組織 CA）	職責証明書用の証明書ポリシ（新暗号）	なし
相互認証証明書 （BCA→GPKI BCA）	職責証明書用の証明書ポリシ（新暗号）	職責証明書用の証明書ポリシ（新暗号） ＝官職証明書用の証明書ポリシ（新暗号）
相互認証証明書 （GPKI BCA→BCA）	官職証明書用の証明書ポリシ（新暗号）	官職証明書用の証明書ポリシ（新暗号） ＝職責証明書用の証明書ポリシ（新暗号）

[5] 旧暗号の自己署名証明書及びリンク証明書は、公表しているリポジトリ等から削除する場合もある。

1.2　APCA の使用する暗号アルゴリズム及び移行方針

APCA は、平成 27 年 1 月以降に移行を行う。

また、APCA の新暗号への移行方式は、階層型 CA による「新局立ち上げ方式」とし、現行の旧暗号対応の APCA（以下「APCA G2」という。）とは別に新暗号対応の認証局（以下「APCA G3」という。）を構築する。

なお、APCA G3 を階層型 CA により構築することに伴い、CA の構成等、現行の APCA G2 から仕様変更が生じる。詳細については、「(参考) APCA G3 の階層化等に伴う APCA G2 からの仕様変更について」を参照すること。

1.2.1　使用する暗号アルゴリズム

暗号アルゴリズム移行後、APCA G3 が発行する証明書及び失効リストの署名アルゴリズムは、全て「sha256WithRSAEncryption」とする。また、各証明書の鍵長は全て「2048 ビット」とする。なお、旧暗号による証明書と新暗号による証明書を区別可能とするため、新暗号で発行する Web 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の証明書ポリシには、旧暗号で発行する各証明書の証明書ポリシとは異なるオブジェクト識別子（OID）を採用する。

1.2.2　APCA の移行方針

(1) 平成 27 年 1 月まで

APCA は、平成 27 年 1 月までは、現行の APCA G2 から旧暗号の証明書を発行する。

また、APCA G2 の公開鍵及び秘密鍵は、平成 25 年 3 月 31 日に鍵生成から 7 年経過したが、APCA G2 の公開鍵及び秘密鍵の有効期限満了となる平成 28 年 3 月 31 日に CA を廃止するため、「LGPKI アプリケーション認証局 CP/CPS　6.3.2 公開鍵及び秘密鍵の利用期間[6]」の規定に基づき、鍵更新は行わない。

なお、APCA が発行する Web 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の有効期間は、通常 3 年としているが、平成 25 年 4 月 1 日以降に発行する証明書については、APCA G2 の廃止時期に合わせて、有効期間を「平成 28 年 3 月 31 日」の日付指定で発行するため、有効期間は 3 年未満となる。

APCA から発行する証明書の有効期間は、図 1-4 のとおりである。

---

[6] アプリケーション CA の公開鍵及び秘密鍵の有効期間は、有効とした日から起算して 10 年以内とし、7 年以内に鍵更新を行う。ただし、公開鍵と秘密鍵の有効期間内に CA を廃止する場合は、この限りでない。（『LGPKI アプリケーション認証局 CP/CPS』　6.3.2 公開鍵及び秘密鍵の利用期間）

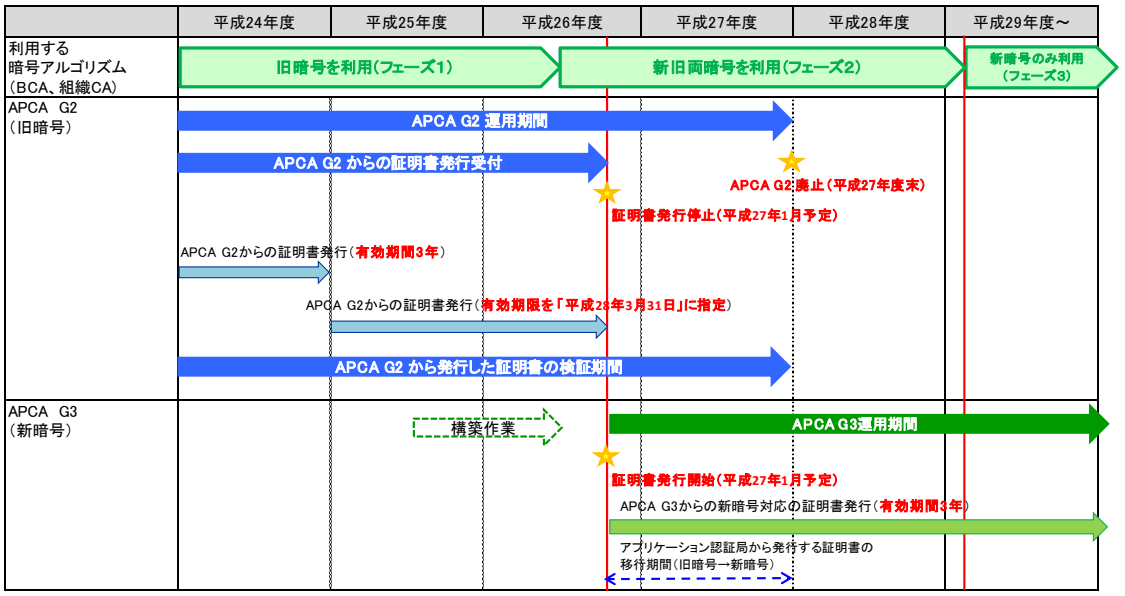

図 1-4　APCA が発行する証明書の有効期間

(2) 平成 27 年 1 月以降～平成 27 年度末まで

APCA は、平成 27 年 1 月以降に予定している暗号アルゴリズムの移行後は、APCA G2 の旧暗号による証明書発行を停止し、APCA G3 から新暗号による証明書発行を開始する。

なお、APCA G2 は、平成 27 年度末まで CRL の発行を継続するため、この期間は、発行済みの旧暗号による証明書も継続して利用可能である。

(3) 平成 28 年度以降

APCA は、平成 28 年度開始時点で、APCA G2 から発行した証明書のうち有効なものがある場合には、認証局において強制失効する。また、APCA G2 を廃止し、自己署名証明書の公開を中止する。[7]

なお、APCA G3 は引き続き新暗号による証明書発行等を行う。

[7] APCA G2 の自己署名証明書は、必要に応じて失効する場合がある。

1.3　CVS の使用する暗号アルゴリズム及び移行方針

1.3.1　使用する暗号アルゴリズム

CVS が使用する暗号アルゴリズムは、表 1-4 のとおりである。

表 1-4 CVS が使用する暗号アルゴリズム

変更項目	旧暗号対応 CVS	新暗号対応 CVS
利用する証明書の署名アルゴリズム及び鍵長（トラストアンカの証明書/検証応答に付与する証明書）	署名アルゴリズム： sha256WithRSAEncryption sha1WithRSAEncryption 鍵長： 1024/2048 ビット	署名アルゴリズム： sha256WithRSAEncryption sha1WithRSAEncryption 鍵長： 1024/2048 ビット
検証可能な証明書の署名アルゴリズム（フェーズ 2）	sha256WithRSAEncryption sha1WithRSAEncryption dsaWithSHA-1	sha256WithRSAEncryption sha1WithRSAEncryption dsaWithSHA-1
検証可能な証明書の署名アルゴリズム（フェーズ 3）	運用停止済み	sha256WithRSAEncryption

1.3.2　移行方針

(1) フェーズ 1

CVS は、フェーズ 1 の期間中、新暗号へ移行しない。

(2) フェーズ 2

CVS は、フェーズ 2 開始時から新旧両暗号の証明書の検証を開始する。また、APCAG3 運用開始に併せて、証明書検証要求のあて先（以下「新 CVS」という。）を追加する。

なお、フェーズ 2 開始前から稼働している CVS（以下「旧 CVS」という。）において、CVS クライアントと CVS サーバ間の SSL 通信に利用している Web サーバ証明書については、APCAG2 を廃止する平成 27 年度末をもって有効期限切れとなるため、旧 CVS については、フェーズ 3 開始前の平成 27 年度末に運用を停止する[8]。

そのため、署名検証者は、旧 CVS の運用を停止する平成 27 年度末までに、次項「1.3.3 署名検証者が証明書を利用する際に必要な対応」表 1-6 項番 3 に示す対応を行うこと。

[8] 旧 CVS 運用停止後も、新 CVS において旧暗号の証明書の検証が可能である。

(3) フェーズ 3 以降

CVS は、フェーズ 3 開始時に、新暗号対応の証明書のみ検証可能とするよう、新 CVS の設定変更を行う[9]。

各フェーズにおける CVS の状態は、図 1-5 のとおりである。また、新旧 CVS の提供期間については、表 1-5 のとおりである。

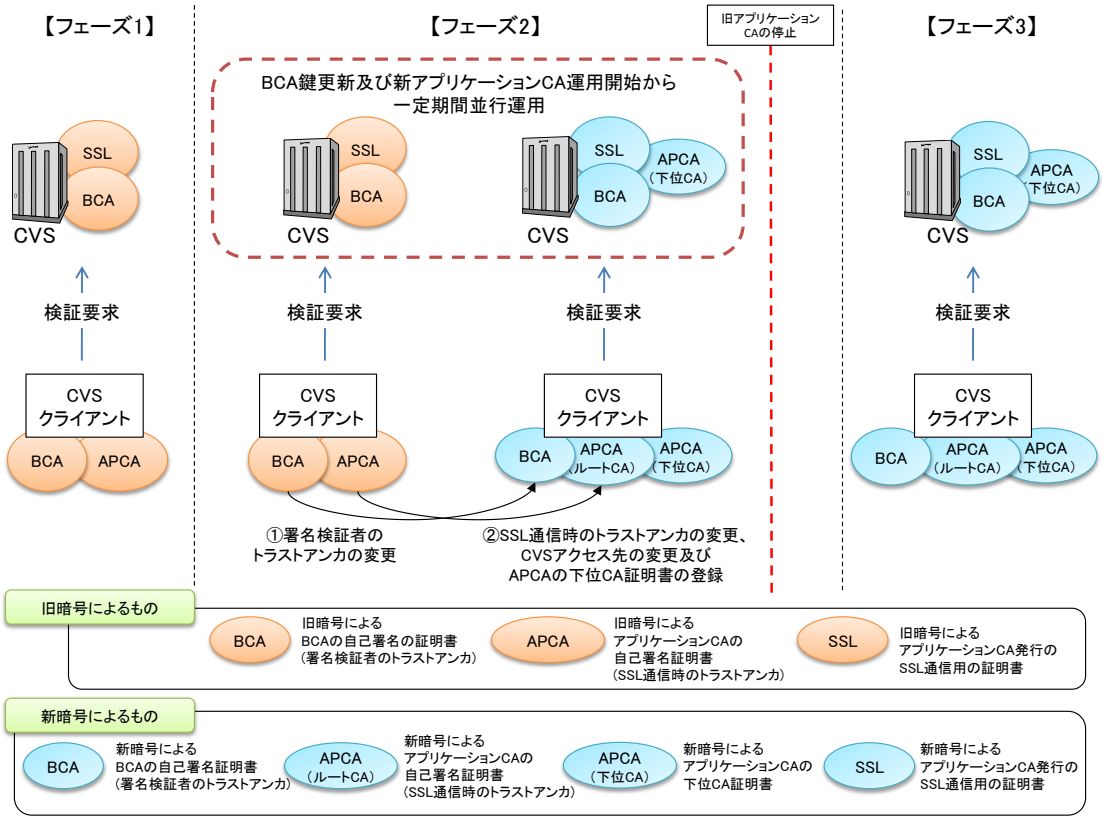

図 1-5　各フェーズにおける CVS の状態

表 1-5 CVS の提供期間

証明書検証サーバ	利用期間	提供時期	利用停止時期
旧CVS	フェーズ1	提供中	APCA G2廃止まで（平成27年度末）
	フェーズ2	平成26年9月中旬～	
新CVS	フェーズ2	平成27年1月以降（APCAG3運用開始後）	平成29年度早期以降
	フェーズ3	平成29年度早期以降	－

[9] 他の CA から発行する証明書については、有効期間が 5 年間のものがあるため、当該証明書の有効期間満了となる平成 31 年度頃までは、他の CA から発行した旧暗号の証明書を検証できるように検証可能期間を延長する場合がある。

1.3.3 署名検証者が CVS を利用する際に必要な対応

署名検証者が CVS を利用する際に必要な対応は、表 1-6 のとおりである。

表 1-6 署名検証者において必要な対応

項番	対応事項	対応時期
1	署名検証者は、利用するアプリケーション[10]を新暗号に対応させる必要がある。	フェーズ 1 （フェーズ 2 開始より前）
2	署名検証者は､利用するアプリケーションを新規に追加される証明書検証結果コードを識別できるように対応する必要がある。	
3	署名検証者は、CVS の並行運用期間中に、CVS を利用するアプリケーションについて以下の対応を行う必要がある。 • CVS への証明書検証要求で指定するトラストアンカ[11]を、鍵更新後の BCA の自己署名証明書に変更する。 • CVS への接続先を、新 CVS に変更する。 • 署名検証者が利用するアプリケーションにおいて、フェーズ 2 の新 CVS の SSL 通信で使用する APCA G3 の下位 CA から発行された Web サーバ証明書の証明書検証を行えるようにする必要がある。(APCA G3 を階層型 CA で構築することに伴う対応) • CVS との SSL 通信で利用するトラストアンカを APCA G3 の自己署名証明書に変更する。また、APCA G3 の下位 CA 証明書を署名検証者のクライアントに登録する[12]。	APCAG3 運用開始～APCA G2 廃止（平成 27 年度末）まで

なお、フェーズ 2 及びフェーズ 3 における相互認証証明書の状態（図 1-2 及び図 1-3）より、フェーズ 2 及びフェーズ 3 においては、表 1-7 及び表 1-8 に示す証明書検証パターンが想定される。

10 利用するアプリケーションが、同一証明書検証要求内で、複数のトラストアンカを指定することは不可とする

11署名検証者は、フェーズ 2 の旧 CVS に対して証明書検証要求を送る場合、リクエストデータに BCA の自己署名証明書以外を設定すると、検証クライアントが対応していない新暗号の署名値で検証結果が返却される。

12 下位 CA 証明書の登録は必要に応じて実施する。巻末の「（参考）APCA G3 の階層化等に伴う APCA G2 からの仕様変更について」を併せて参照すること。

表 1-7 フェーズ 2 において想定される証明書検証パターン

項番	トラストアンカ (TA)	TA の暗号アルゴリズム	EE 証明書発行 CA	EE 証明書の暗号アルゴリズム	有効なポリシ
1	LGPKI BCA	旧暗号	旧暗号 民間 CA	旧暗号	職責証明書用の証明書ポリシ（旧暗号）
2	LGPKI BCA	旧暗号	新暗号 民間 CA	新暗号	職責証明書用の証明書ポリシ（新暗号）
3	LGPKI BCA	新暗号	旧暗号 民間 CA	旧暗号	職責証明書用の証明書ポリシ（旧暗号）
4	LGPKI BCA	新暗号	新暗号 民間 CA	新暗号	職責証明書用の証明書ポリシ（新暗号）

表 1-8 フェーズ 3 において想定される証明書検証パターン

項番	トラストアンカ (TA)	TA の暗号アルゴリズム	EE 証明書発行 CA	EE 証明書の暗号アルゴリズム	有効なポリシ
1	LGPKI BCA	新暗号	新暗号 民間 CA	新暗号	職責証明書用の証明書ポリシ（新暗号）

（参考）APCA G3 の階層化等に伴う APCA G2 からの仕様変更について

APCA G3 を階層型 CA で構築することに伴う現在運用中の APCA G2 からの仕様変更内容は以下のとおりである。

1　APCA G3 の仕様変更

（1）Web サーバ証明書等を発行する認証局

APCAG3 における新暗号移行は、複数の CA を階層型に構成し、トラストアンカーとなるルートの CA と下位に位置する下位 CA からなる「階層型モデル」を採用する。

これに伴い、証明書利用者に発行する Web サーバ証明書などのアプリケーション認証局発行の証明書は、下位 CA から発行される(図1)。

（2）下位 CA 証明書の発行

多段構成の採用により、これまでアプリケーション認証局(ルート CA)から発行されていた自己署名証明書とは別に、下位 CA が信頼できるものであることを証明した「下位 CA 証明書」が発行される(図1)。

（3）失効リストの一本化

ルート CA 及び下位 CA では、失効リストである CRL/ARL は、CRL として発行を一本化し、Web に公開する(図1)。

（4）SubjectAltName（主体者代替名）の設定

ベースライン要件[1]に従い、特定ブラウザにおいて、Web サーバ証明書の証明書拡張領域の「SubjectAltName」の設定が必須要件とされていること、また、SubjectAltName の設定が無い場合、SSL 通信の際に一部のブラウザにおいて警告メッセージが表示される場合があることが判明している。ついては、APCA G3 から発行する Web サーバ証明書については、SubjectAltName を設定することとする。

（5）APCAG3 の証明書の名義（サブジェクト）について

リポジトリのディレクトリ構成について、これまでは、第三階層の識別属性については、組織を意味する「OU」により組織単位として各 CA を配置していた。

APCAG3 については、下位 CA の構築に伴い、ルート、下位の階層を組織単位「OU」として表現するよりは、一般名を意味する「CN」で表現する方が一般的であることから、第三階層の識別属性について、一般名を意味する「CN」に表記を変更する。（図２）

・証明書のサブジェクトの例

ルート CA 証明書：CN=Application CA G3 Root, O=LGPKI, C=JP

下位 CA 証明書　：CN=Application CA G3 Sub1, O=LGPKI, C=JP

[1] 国内外の主要な認証局及び web ブラウザベンダを構成メンバーとする組織（CA/Browser Forum）で策定された要件。電子認証に係る議論及び世界標準ガイドライン策定を行っている。

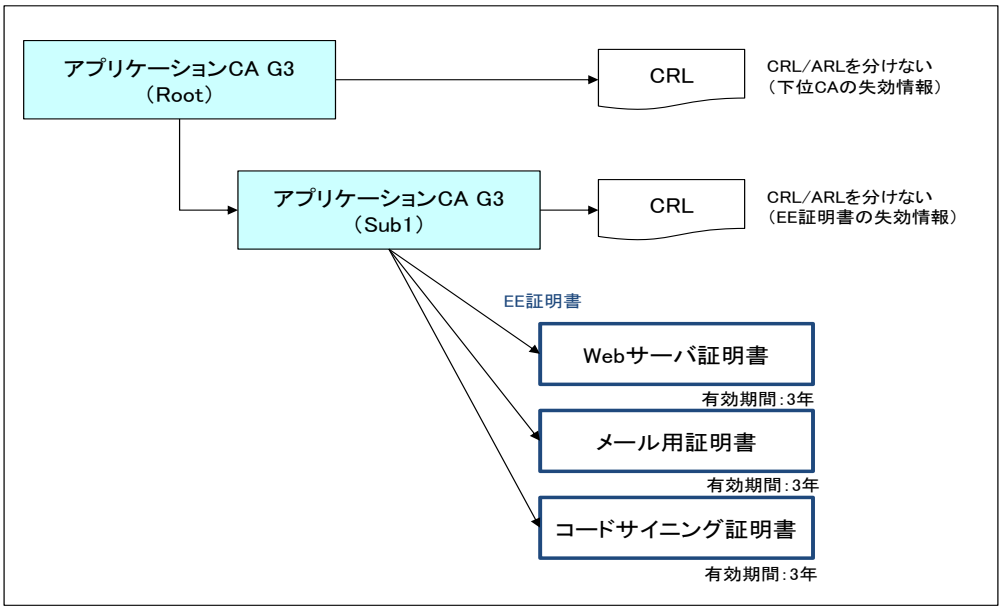

図１　APCA G3 の構成及び証明書等

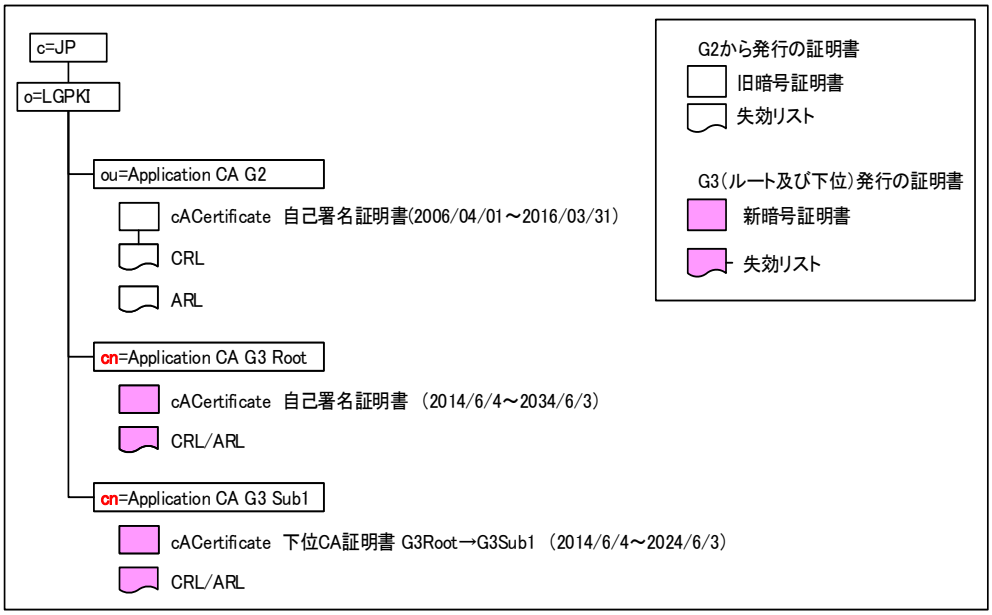

図２　リポジトリのディレクトリ情報ツリー（DIT）構成

２　証明書検証サーバの SSL 通信における変更

証明書検証サーバ（以下「CVS」という。）では、SSL 通信によりクライアントからの証明書検証要求を受け付ける。

APCAG3 の運用開始に併せて、新たに追加される証明書検証要求のあて先(以下「新 CVS」という。）との SSL 通信においては、APCA G3 から発行する Web サーバ証明書を使用するため、１（２）のとおり、Web サーバ証明書の検証において、APCA G3 の最上位の APCA G3（Root）の自己署名証明書に加え、APCA G3（Sub1）の下位 CA 証明書が必要になる。

新 CVS では、図3下段の②のとおり、Web サーバ証明書と併せて下位 CA 証明書を送付し、

CVS とクライアント間の通信において下位 CA 証明書を取得できるような設定を行う[2]。

なお、APCA G3（Root）の自己署名証明書については、従来どおり、クライアントに事前に登録する必要がある[4]。

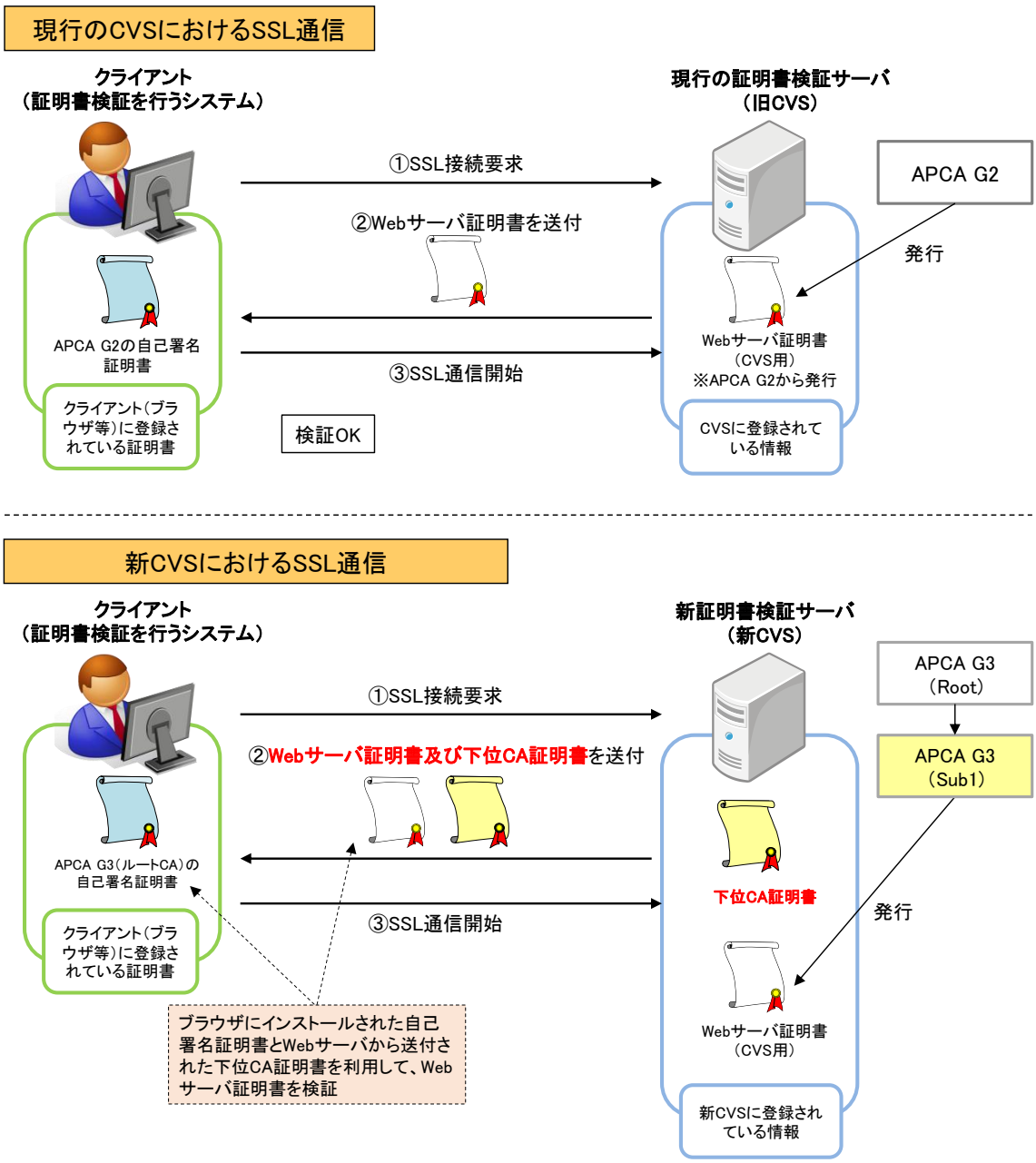

図３　APCA G3 の階層化に伴う CVS の SSL 通信における変更点

[2] クライアントにおいて新 CVS から送付される下位 CA 証明書を取得できない場合には、手動で下位 CA 証明書をクライアントにインストールする必要がある。

[4] Internet Explorer の場合、APCA G3（Root）の自己署名証明書は、自動的に証明書ストアにインストールされる。