C-6-4-5

LGPKI
技術仕様書

第１.９版

2021 年４月

地方公共団体情報システム機構

1　はじめに

本仕様書は、LGPKI を構成する各 CA 及び LGPKI を利用するアプリケーションに関する技術仕様を定めるものである。本書の対象は、次の技術要件とする。

- LGPKI を構成する各コンポーネントが満たすべき技術要件
- LGPKI を利用するアプリケーションが満たすべき技術要件

1.1. 概要

LGPKI は、第三次 LGPKI 組織 CA 及び第四次 LGPKI 組織 CA R2（以下「組織 CA 等」という。）を中心とした認証基盤である。また、第三次 LGPKI ブリッジ CA は、内部及び外部 CA との相互接続を効率的に実施し、柔軟な拡張性を有している。

本仕様書では、LGPKI を利用するために必要となる機能と仕様を定める。ただし、外部サービスを利用する機能については、外部サービスの規程を参照するものとする。

1.2. 各章の位置付け

（2 章）LGPKI コンポーネント仕様

2 章では、LGPKI を構成する PKI コンポーネントの概要と基本的な仕様について記述する。対象とするコンポーネントの種類は以下のとおりとする。

- 第三次 LGPKI 組織 CA
- 第三次 LGPKI ブリッジ CA
- 第四次 LGPKI 組織 CA R2
- 第四次 LGPKI アプリケーション CA R2
- 第四次 LGPKI 公開リポジトリ
- 第四次 LGPKI 統合リポジトリ
- 第四次 LGPKI 証明書検証サーバ
- Security Communication RootCA2（外部サービス）
- セコムパスポート for Web SR3.0 CA（外部サービス）
- セコムパスポート for PublicID CA（外部サービス）
- セコム公開リポジトリ（外部サービス）
- セコム OCSP レスポンダ（外部サービス）
- エンドエンティティ

（3 章）アプリケーション仕様

3 章では、LGPKI を利用するアプリケーションが満たすべき機能を記述する。

また、この仕様書で記述するアプリケーションは、LGPKI を利用しデータに署名するソフトウェア（署名者）と署名されたデータを検証するソフトウェア（署名検証者）に位置付ける。

（4 章）証明書検証サーバの利用

４章では、LGPKI の提供する証明書検証サーバを利用する際に満たすべき仕様について定める。

（６章）ディレクトリプロファイル

６章では、リポジトリ等のプロファイルについて定める。

1.3. 前提

政府認証基盤相互運用性仕様書
（http://www.gpki.go.jp/session/）及び以下の標準等を考慮し、技術仕様を規定する。

- IETF：Internet X.509 Public Key Certificate Infrastructure and CRL Profile
- ITU-T：ITU-T RECOMMENDATION X.509 | ISO/IEC 9594-8

1.4. 見直し

本仕様書は情報通信技術の動向等を踏まえ必要に応じて見直すものとする。

2　LGPKI コンポーネント仕様

2.1. 概要

本章では、LGPKI を構成する各 PKI コンポーネントの概要と基本的な仕様について記述する。

なお、LGPKI を構成する PKI コンポーネントの概念図を以下に示す。

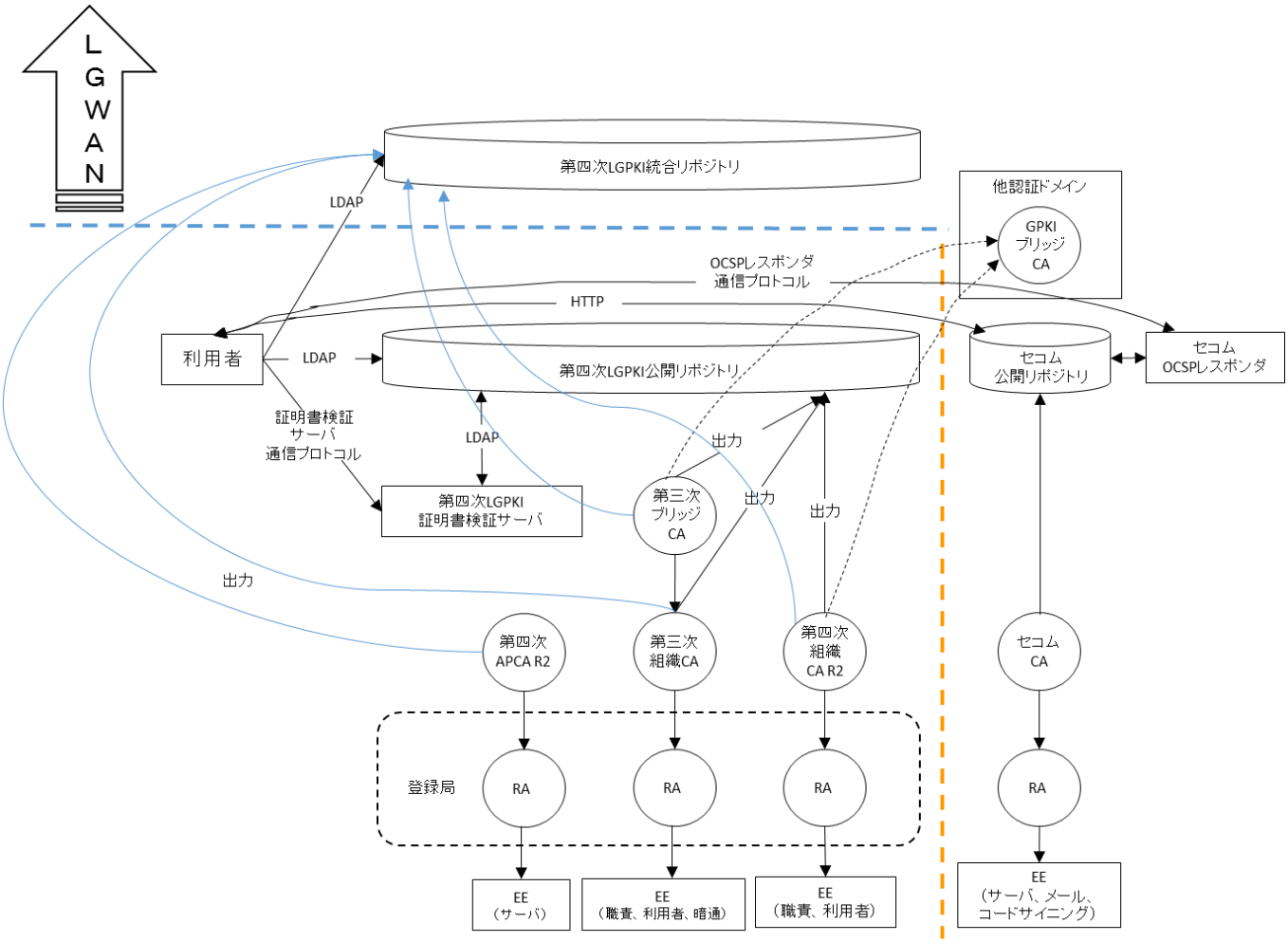

図　2－1　LGPKI 概念図

LGPKI は、組織 CA 等（組織 CA 等発行局及び登録局（以下「RA」という。））、第三次 LGPKI ブリッジ CA、第四次 LGPKI アプリケーション CAR2、第四次 LGPKI 公開リポジトリ及び第四次 LGPKI 統合リポジトリ（以下、総称して「リポジトリ等」という。）、第四次 LGPKI 証明書検証サーバ、セコムトラストシステムズ株式会社の運用する認証サービス、セコム公開リポジトリ、セコム OCSP レスポンダから構成される。

2.2. 第三次 LGPKI 組織 CA

第三次 LGPKI 組織 CA は証明書の発行、失効、更新を行う。また各種証明書と失効情報

（CRL/ARL）をリポジトリ等に格納する。

第三次 LGPKI 組織 CA には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。

第三次 LGPKI 組織 CA は以下の機能を備える。

- 自己署名証明書の発行及び第四次 LGPKI 統合リポジトリへの格納
- 証明書の発行、更新
- 第三次 LGPKI ブリッジ CA への相互認証証明書発行要求の作成、発行・更新された証明書の受け入れ
- 第三次 LGPKI ブリッジ CA への相互認証証明書失効要求の作成
- エンドエンティティ（コンピュータシステムを含む）からの証明書発行要求の受け付け、証明書の発行、失効、更新
- 相互認証証明書のリポジトリ等への格納
- 自 CA が発行した証明書に関する失効要求の受け付け、失効情報の発行とリポジトリ等への格納
- 自 CA の各操作員の明確な権限分離が可能な証明書の発行･更新･失効
- 自 CA の鍵更新

2.3. 第三次 LGPKI ブリッジ CA

第三次 LGPKI ブリッジ CA は二つの役割を担っている。一つは、LGPKI を構成する各 CA を束ねる役割であり、もう一方は、LGPKI が他認証ドメインと相互認証を行う際の橋渡しを行うという役割である。

第三次 LGPKI ブリッジ CA は各 CA と相互認証を行う。具体的には、お互いに相手の CA の公開鍵の証明書として相互認証証明書の発行と交換を行う。

第三次 LGPKI ブリッジ CA は他認証ドメインに属する CA（以下「他 CA」という。）の公開鍵を含む相互認証証明書の発行、失効、更新を行う。

第三次 LGPKI ブリッジ CA は第三次 LGPKI ブリッジ CA が発行した相互認証証明書を含む相互認証証明書ペアと、失効情報をリポジトリ等の第三次 LGPKI ブリッジ CA エントリに格納する。ただし、第三次 LGPKI 組織 CA との間で発行された相互認証証明書は、第三次 LGPKI ブリッジ CA エントリに格納しない。

第三次 LGPKI ブリッジ CA の RA は各 CA の身元を保証し、相互認証証明書に含まれる公開鍵が確実にその CA の公開鍵であり、CA がこの公開鍵に一致する秘密鍵を持っていることを保証する。

第三次 LGPKI ブリッジ CA は以下の機能を備える。

- 自己署名証明書の発行とリポジトリ等への格納
- 他 CA からの相互認証証明書発行要求の受け付けと検証、証明書の発行、更新

- 他 CA への相互認証証明書発行要求の作成、発行・更新された証明書の受け入れ
- 相互認証証明書ペアのリポジトリ等への格納
- 他 CA への相互認証証明書失効要求の作成
- 第三次 LGPKI ブリッジ CA が発行した証明書に関する失効要求の受け付け、失効情報の発行とリポジトリ等への格納
- 第三次 LGPKI ブリッジ CA の各操作員の明確な権限分離が可能な証明書の発行･更新･失効
- 第三次 LGPKI ブリッジ CA の鍵更新

なお、鍵更新、リンク証明書の仕様については、政府認証基盤相互運用性仕様書に定められた仕様に準拠するものとする。

2.4. 第四次 LGPKI 組織 CA R2

第四次 LGPKI 組織 CAR2 は他認証ドメインに属する CA（以下「他 CA」という。）の公開鍵を含む相互認証証明書の発行、失効、更新を行う。

第四次 LGPKI 組織 CAR2 は第四次 LGPKI 組織 CAR2 が発行した相互認証証明書を含む相互認証証明書ペアと、失効情報をリポジトリ等の第四次 LGPKI 組織 CAR2 エントリに格納する。

第四次 LGPKI 組織 CAR2 は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL/ARL）をリポジトリ等に格納する。

第四次 LGPKI 組織 CAR2 には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。また、相互認証証明書に含まれる公開鍵が確実にその CA の公開鍵であり、CA がこの公開鍵に一致する秘密鍵を持っていることを保証する。

第四次 LGPKI 組織 CAR2 は以下の機能を備える。

- 自己署名証明書の発行とリポジトリ等への格納
- 証明書の発行、更新
- 他 CA からの相互認証証明書発行要求の受け付けと検証、証明書の発行、更新
- 他 CA への相互認証証明書発行要求の作成、発行・更新された証明書の受け入れ
- 相互認証証明書ペアのリポジトリ等への格納
- 他 CA への相互認証証明書失効要求の作成
- エンドエンティティ（コンピュータシステムを含む）からの証明書発行要求の受け付け、証明書の発行、失効、更新
- 自 CA が発行した証明書に関する失効要求の受け付け、失効情報の発行とリポジトリ等への格納
- 自 CA の各操作員の明確な権限分離が可能な証明書の発行･更新･失効
- 自 CA の鍵更新

なお、鍵更新、リンク証明書の仕様については、政府認証基盤相互運用性仕様書に定められた仕様に準拠するものとする。

2.5. 第四次 LGPKI アプリケーション CA R2（LGWAN 内部環境用）

第四次 LGPKI アプリケーション CA は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL）を第四次 LGPKI 統合リポジトリに格納する。

第四次 LGPKI アプリケーション CA には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。

第四次 LGPKI アプリケーション CA は以下の機能を備える。

- 自己署名証明書の発行と第四次 LGPKI 統合リポジトリへの格納
- 証明書の発行、更新
- エンドエンティティ（コンピュータシステムを含む）からの証明書発行要求の受け付け、証明書の発行、失効、更新
- 自 CA が発行した証明書に関する失効要求の受け付け、失効情報の発行と第四次 LGPKI 統合リポジトリへの格納
- 自 CA の各操作員の明確な権限分離が可能な証明書の発行･更新･失効
- 自 CA の鍵更新

2.6. リポジトリ等

2.6.1. 第四次 LGPKI 公開リポジトリ

第四次 LGPKI 公開リポジトリは、証明書の有効性検証に必要な各種証明書、CRL/ARL を格納する。また、LDAPv3(389/tcp)を備えており、各 PKI コンポーネントからの証明書、CRL/ARL の検索、取り出し、格納が行える。

第四次 LGPKI 公開リポジトリは以下の機能を備える。

- 第三次 LGPKI ブリッジ CA の自己署名証明書の格納
- 第四次 LGPKI 組織 CA R2 の自己署名証明書の格納
- 相互認証証明書及び相互認証証明書ペアの格納
- CRL/ARL の格納
- 証明書、CRL/ARL の検索
- 他リポジトリとの連携（リフェラル）

他のリポジトリとの連携に関しては、LDAPv3 リフェラルを使うことを前提とする。

2.6.2. 第四次 LGPKI 統合リポジトリ

第四次 LGPKI 統合リポジトリは、証明書の有効性検証に必要な各種証明書、CRL/ARL を格納する。また、LDAPv3(389/tcp)を備えており、各 PKI コンポーネントからの証明書、CRL/ARL の検索、取り出し、格納が行える。

第四次 LGPKI 統合リポジトリは以下の機能を備える。

- 第三次 LGPKI ブリッジ CA の自己署名証明書の格納
- 第三次 LGPKI 組織 CA の自己署名証明書の格納
- 第四次 LGPKI 組織 CA R2 の自己署名証明書の格納
- 第四次 LGPKI アプリケーション CA R2 の自己署名証明書の格納
- 相互認証証明書及び相互認証証明書ペアの格納
- CRL/ARL の格納
- 証明書、CRL/ARL の検索

2.7. 第四次 LGPKI 証明書検証サーバ

第四次 LGPKI 証明書検証サーバは、検証要求者が指定した証明書の妥当性を検証し、その検証要求者に証明書の検証結果を返すサーバである。証明書認証パス構築と各証明書の有効性に関する検証も可能なプロトコルを使用する。

第四次 LGPKI 証明書検証サーバは相互運用に関する機能として以下を備える。

- 第四次 LGPKI 証明書検証サーバ自身の証明書の発行要求、発行された証明書の受け入れ
- 検証要求者からの証明書検証要求受け付け
- 認証パス構築
- 認証パス検証（指定されたポリシーによるチェック等）
- 検証要求者への証明書検証結果の送信

2.8. Security Communication RootCA2

Security Communication RootCA2 はセコムトラストシステム株式会社が運用するパブリックな Root 認証局である。Security Communication RootCA2 は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL）をセコム公開リポジトリに格納する。Security Communication RootCA2 には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。

Security Communication RootCA2 の備える機能については、「Security Communication RootCA 認証運用規定」及び「Security Communication RootCA 下位 CA 証明書ポリシ」を参照のこと。
（https://repository.secomtrust.net/SC-Root2/）

2.9. セコムパスポート for Web SR3.0 CA

セコムパスポート for Web SR3.0 CA は Security Communication RootCA2 からサイニングを受けたセコムトラストシステム株式会社が運用するパブリックな Web サーバ証明書（OV 証明書）を発行する CA である。セコムパスポート for Web SR3.0 CA は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL）をセコム公開リポジトリに格納する。

セコムパスポート for Web SR3.0 CA には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。

セコムパスポート for Web SR3.0 CA の備える機能については、「セコム電子認証基盤認証運用規程」及び「セコムパスポート for Web SR 認証局 証明書ポリシ」を参照のこと。（https://repo1.secomtrust.net/spcpp/pfw/pfwsr3ca/）

2.10. セコムパスポート for PublicID CA

セコムパスポート for PublicID CA は Security Communication RootCA2 からサイニングを受けたセコムトラストシステムズ株式会社が運用するパブリックなメール用証明書、コードサイニング証明書を発行するサービスである、セコムパスポート for PublicID CA は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL）をセコム公開リポジトリに格納する。

セコムパスポート for PublicID CA には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。

セコムパスポート for PublicID CA の備える機能については、「セコム電子認証基盤認証運用規程」及び「セコムパスポート for Member 2.0 PUB 証明書ポリシ」を参照のこと。（https://repo1.secomtrust.net/spcpp/pfm20pub/）

2.11. セコム公開リポジトリ

セコム公開リポジトリは、セコムトラストシステズが運用するセコムの認証局が発行する証明書の有効性検証に必要な各種証明書、CRL/ARL を格納する。

セコム公開リポジトリが備える機能については、セコムトラストシステムズ株式会社が運用する各認証サービスのリポジトリで公開する CP、CPS を参照のこと。

Security Communication RootCA2：https://repository.secomtrust.net/SC-Root2/
セコムパスポート for Web SR3.0 CA：https://repo1.secomtrust.net/spcpp/pfw/pfwsr3ca/
セコムパスポート for PublicID CA：https://repo1.secomtrust.net/spcpp/pfm20pub/

2.12. セコム OCSP レスポンダ

セコム OCSP レスポンダは、検証要求者が指定した証明書の有効性を検証し、その検証要求

者に証明書の有効性の検証結果を返すサーバである。OCSP レスポンダのプロトコルは RFC2560 及び RFC5019 で規定されている。

セコム OCSP レスポンダが備える機能については、セコムトラストシステムズ株式会社が運用する各認証サービスのリポジトリで公開する CP、CPS を参照のこと。

Security Communication RootCA2：https://repository.secomtrust.net/SC-Root2/
セコムパスポート for Web SR3.0 CA：https://repo1.secomtrust.net/spcpp/pfw/pfwsr3ca/
セコムパスポート for PublicID CA：https://repo1.secomtrust.net/spcpp/pfm20pub/

2.13. エンドエンティティ

エンドエンティティは、データに署名し送信する署名者と、認証パスを構築し署名を検証する署名検証者に大別できる。署名者は CA から証明書を発行され、その証明書に含む公開鍵と一致する秘密鍵でデータに署名することができる。

共通の機能として以下を備える。

- エンドエンティティ自身の証明書発行要求、発行された証明書の受け入れ
- エンドエンティティ自身の証明書の更新要求、発行された証明書の受け入れ

署名者のエンドエンティティは以下の機能を備えている。

- データに署名
- リポジトリ等及びセコム公開リポジトリから証明書の取得
- 認証パスの構築（オプション）

署名検証者のエンドエンティティは以下の機能を備えている。

- 署名の検証
- リポジトリ等及びセコム公開リポジトリから証明書、CRL/ARL の取得
- LDAPv3 リフェラルによる他のリポジトリへの連携
  エンドエンティティは、LDAPv3 をサポートすること。
- OCSP レスポンダへの問い合わせ機能、第四次 LGPKI 証明書検証サーバへの問い合わせ機能、もしくは証明書検証サーバ等と同等の証明書検証機能

2.14. LGPKI における認証情報

LGPKI では、相互認証証明書や自己署名証明書及び失効情報を用いる。以降では、これら認証情報について記述する。

なお、セコムトラストシステムズ株式会社が運用する各認証サービスの認証局についてはセコムトラストシステムズ株式会社が運用する各認証サービスのリポジトリで公開する CP、CPS を参照のこと。

Security Communication RootCA2：https://repository.secomtrust.net/SC-Root2/
セコムパスポート for Web SR3.0 CA：https://repo1.secomtrust.net/spcpp/pfw/pfwsr3ca/
セコムパスポート for PublicID CA：https://repo1.secomtrust.net/spcpp/pfm20pub/

2.14.1. 認証情報の公開

LGPKI の各 CA が発行する各種証明書と証明書の有効性を検証する情報である失効情報(CRL/ ARL)の公開に関して記載する。ここでは、主に各種証明書と CRL/ARL のリポジトリ等への格納・削除・更新について記述する。

証明書や CRL などの ASN.1 の構造をもつバイナリデータは、AttributeDescription での「Binary」オプションを指定し、バイナリ符号化して格納する。

表 2－1 に各認証情報と第四次 LGPKI 公開リポジトリへの格納･削除･更新の関係を示し、次節以降で格納形式等を記述する。

表 2－1 認証情報の第四次 LGPKI 公開リポジトリへの格納・削除・更新

		第三次 LGPKI ブリッジ CA の処理	第三次 LGPKI 組織 CA の処理	第四次 LGPKI 組織 CA R2 の処理
相互認証証明書	格納	○	○	○
	削除	○	○	○
	更新	○	○	○
エンドエンティティ用証明書	格納	－	－	－
	削除	－	－	－
	更新	－	－	－
自己署名証明書	格納	○	－	○
	削除	○	－	○
リンク証明書	格納	○	－	○
	削除	○	－	○
失効情報	格納	○	○	○
	削除	○	○	○

	更新	○	○	○

○：処理対象、－：処理対象外

・エンドエンティティ用証明書は、リポジトリ等への情報格納を行わない。

格納についての詳細な形式は RFC4523 の記述にしたがうものとする。

以下の証明書は、リポジトリ内の格納対象のエントリに複数格納される可能性がある。このため削除や更新時には、対象となる証明書以外に影響を与えないようにしなければならない。

- 各 CA エントリの cACertificate 属性に格納される、自己署名証明書及びリンク証明書もしくは相互認証証明書
- ブリッジ CA エントリの crossCertificatePair 属性に格納される、相互認証証明書ペア

表２－２に各認証情報と第四次 LGPKI 統合リポジトリへの格納・削除・更新の関係を示し、次節以降で格納形式等を記述する。

表 ２－２認証情報の統合リポジトリ等への格納・削除・更新（○：処理対象、－：処理対象外）

		第三次ブリッジ CA の処理	第三次組織 CA の処理	第四次組織 CAR2 の処理	第四次アプリケーション CAR2 の処理
相互認証証明書	格納	○	○	－	－
	削除	○	○	－	－
	更新	○	○	－	－
エンドエンティティ用証明書	格納	－	－	－	－
	削除	－	－	－	－
	更新	－	－	－	－
自己署名証明書	格納	○	○	○	○
	削除	○	○	○	○
リンク証明書	格納	○	○	○	－
	削除	○	○	○	－
失効情報	格納	○	○	○	○
	削除	○	○	○	○
	更新	○	○	○	○

格納についての詳細な形式は RFC4523 の記述にしたがうものとする。

以下の証明書は、リポジトリ内の格納対象のエントリに複数格納される可能性がある。このため削除や更新時には、対象となる証明書以外に影響を与えないようにしなければならない。

- 各 CA エントリの cACertificate 属性に格納される、自己署名証明書及びリンク証明書も

しくは相互認証証明書

- BCA エントリの crossCertificatePair 属性に格納される、相互認証証明書ペア

2.14.2.相互認証証明書の格納･削除

(1)相互認証証明書の格納

ア）第三次 LGPKI ブリッジ CA の CA エントリへの格納

第三次 LGPKI ブリッジ CA が他 CA へ発行した、あるいは他 CA から発行された相互認証証明書のリポジトリ等への格納は、次の形式で行う。

格納するエントリ	第三次 LGPKI ブリッジ CA の CA のエントリ	
格納するエントリが持たなければならないオブジェクトクラス	PkiCA (joint-iso-itu-t(2) ds(5) objectClass(6) pkiCA(22))	
格納する属性名	crossCertificatePair 属性	
属性値の型	CertificatePair	
格納するフィールド[1]	Forward フィールド	他 CA が第三次 LGPKI ブリッジ CA の公開鍵に署名した相互認証証明書
	Reverse フィールド	第三次 LGPKI ブリッジ CA が他 CA の公開鍵に署名した相互認証証明書
複数 CA と相互認証した場合の属性値の扱い	相互認証した CA ごとに別の属性値として格納する	

相互認証証明書の格納は、相互認証証明書ペアを構成する 2 つの証明書が両方揃った時点で行っても、リポジトリ等へ格納できる状態になった方から随時格納してもよい。

また、第三次 LGPKI ブリッジ CA が第三次 LGPKI 組織 CA へ発行した相互認証証明書のリポジトリ等への格納は、次の形式で行う。

格納するエントリ	第三次 LGPKI ブリッジ CA の CA のエントリ
格納するエントリが持たなければならないオブジェクトクラス	PkiCA (joint-iso-itu-t(2) ds(5) objectClass(6) pkiCA(22))
格納する属性名	crossCertificatePair 属性

[1] International standard 9594-8 ITU-T RECOMMENDATION X.509 (03/2000)では、これまで forward / reverse と表記されていたフィールドを issuedToThisCA / issuedByThisCA と表記している。しかし、本書では政府認証基盤相互運用性仕様書との整合性を考慮し forward / reverse と表記する。

属性値の型	CertificatePair	
格納するフィールド	Reverse フィールド	第三次 LGPKI ブリッジ CA が第三次 LGPKI 組織 CA の公開鍵に署名した相互認証証明書
複数 CA と相互認証した場合の属性値の扱い	相互認証した CA ごとに別の属性値として格納する	

イ）第三次 LGPKI 組織 CA の CA エントリへの格納

第三次 LGPKI ブリッジ CA が発行した第三次 LGPKI 組織 CA に対する相互認証証明書に関しては、第三次 LGPKI 組織 CA のエントリに格納する。第三次 LGPKI ブリッジ CA のエントリには格納しない。リポジトリ等への格納は、次の形式で行うものとする。

格納するエントリ	第三次 LGPKI 組織 CA の CA のエントリ	
格納するエントリが持たなければならないオブジェクトクラス	PkiCA (joint-iso-itu-t(2) ds(5) objectClass(6) pkiCA(22))	
格納する属性	cACertificate 属性	
属性値の型	Certificate	
格納するフィールド	Reverse フィールド	第三次 LGPKI 組織 CA が第三次 LGPKI ブリッジ CA の公開鍵に署名した相互認証証明書
複数 CA と相互認証した場合の属性値の扱い	相互認証した CA ごとに別の属性値として格納する	

ウ）第四次 LGPKI 組織 CAR2 の CA エントリへの格納

第四次 LGPKI 組織 CAR2 が他 CA へ発行した、あるいは他 CA から発行された相互認証証明書のリポジトリ等への格納は、次の形式で行う。

格納するエントリ	第四次 LGPKI 組織 CAR2 の CA のエントリ	
格納するエントリが持たなければならないオブジェクトクラス	PkiCA (joint-iso-itu-t(2) ds(5) objectClass(6) pkiCA(22))	
格納する属性名	crossCertificatePair 属性	
属性値の型	CertificatePair	
格納するフィールド[2]	Forward フィールド	他 CA が第四次 LGPKI 組織 CA の公開鍵に署名した相互認証証明書

[2] International standard 9594-8 ITU-T RECOMMENDATION X.509 (03/2000)では、これまで forward / reverse と表記されていたフィールドを issuedToThisCA / issuedByThisCA と表記してい

	Reverse フィールド	第四次 LGPKI 組織 CA が他 CA の公開鍵に署名した相互認証証明書
複数 CA と相互認証した場合の属性値の扱い	相互認証した CA ごとに別の属性値として格納する	

相互認証証明書の格納は、相互認証証明書ペアを構成する 2 つの証明書が両方揃った時点で行っても、リポジトリ等へ格納できる状態になった方から随時格納してもよい。

(2)**相互認証証明書の削除**

相互認証証明書の削除は、次のような場合に実施する。

- 自 CA が発行した相互認証証明書を失効した場合
- 相互認証する相手の CA が自 CA に対して発行した相互認証証明書を失効したことが、発行した相手の CA から通知された場合
- リポジトリ等内に存在する相互認証証明書が失効、もしくは、停止されたことを知った場合

2.14.3. 自己署名証明書及びリンク証明書の格納・削除

第三次 LGPKI ブリッジ CA、組織 CA 等の自己署名証明書は 10 年間有効である。そのうち、前半の 5 年間のみ相互認証証明書の発行に使用する。

(1)**自己署名証明書、リンク証明書の格納**

第三次 LGPKI ブリッジ CA、組織 CA 等及び第四次 LGPKI アプリケーション CAR2 が自らの公開鍵に自らの秘密鍵で署名して発行した自己署名証明書及びリンク証明書のリポジトリ等への格納は、次の形式で行うものとする。なお、第三次 LGPKI 組織 CA は、自己署名証明書及びリンク証明書の第四次 LGPKI 公開リポジトリへの格納は行わない。

格納するエントリ	CA のエントリ
格納するエントリが持たなければならないオブジェクトクラス	PkiCA (joint-iso-itu-t(2) ds(5) objectClass(6) pkiCA(22))
格納する属性	cACertificate 属性
属性値の型	Certificate

る。しかし、本書では政府認証基盤相互運用性仕様書との整合性を考慮し forward / reverse と表記する。

複数の自己署名証明書及びリンク証明書を持つ場合の属性値の扱い	発行された自己署名証明書及びリンク証明書ごとに別の属性値として格納する

(2)**自己署名証明書及びリンク証明書の削除**

CA は､CA エントリ内の cACertificate 属性中の証明書の削除を､次のような場合に実施する。

- 証明書内容変更、鍵長変更等で証明書を失効した場合
- 証明書の有効期限が切れた場合

2.14.4.失効情報の格納と更新

(1)**失効情報の格納**

CA が発行した証明書の証明書失効リストは、各証明書の cRLDistributionPoint 拡張に示されたエントリ、または CA のエントリに格納するものとする。

・ARL

格納するエントリ	各証明書内の cRLDistributionPoints で指定されたエントリまたは CA のエントリ
格納するエントリが持たなければならないオブジェクトクラス	・cRLDistributionPoints で指定されたエントリの場合、 CRLDistributionPoint (joint-iso-itu-t(2) ds(5) objectClass(6) cRLDistiributionPoint(19)) ・CA のエントリの場合、 pkiCA (joint-iso-itu-t(2) ds(5) objectClass(6) pkiCA(22))
格納する属性	AuthorityRevocationList 属性（ARL）
属性値の型	CertificateList

・CRL

格納するエントリ	各証明書内の cRLDistributionPoints で指定されたエントリまたは CA のエントリ
格納するエントリが持たなければならないオブジェクトクラス	・cRLDistributionPoints で指定されたエントリの場合、 CRLDistributionPoint (joint-iso-itu-t(2) ds(5) objectClass(6) cRLDistiributionPoint(19)) ・CA のエントリの場合、 pkiCA (joint-iso-itu-t(2) ds(5) objectClass(6) pkiCA(22))
格納する属性	CertificateRevocationList 属性（CRL）
属性値の型	CertificateList

(2)**失効情報の更新**

失効情報は、nextUpdate までに更新しなければならない。この時、実際の更新を nextUpdate より前に行い、新旧の失効情報がオーバーラップする期間を設けておく運用を行う。これにより、障害や事故等により次回の更新が遅れた場合に、失効情報がまったく公開されない期間が出現しないようにできる可能性が大きくなる。

3　アプリケーション仕様

3.1. 概要

本章では、LGPKI を利用するアプリケーションが満たすべき機能を記述する。前提として、以下の要件を満たすことが必要となる。

- アプリケーション間で関連する証明書と失効情報には互換性がなければならない
- 署名アルゴリズムは互換性がなければならない
- 相対する 2 者間で認証パスの構築と検証ができなければならない
- 証明書や失効情報を共有する方法には互換性がなければならない
- 相対する 2 者間で利用する署名フォーマットは互換性がなければならない
- ベンダー固有の依存性は避けなれければならない

また LGPKI は、拡張性やアプリケーションの汎用性を確保する観点から、他の認証ドメインとの技術的な統一性を重視している。具体的には、公的な認証基盤である GPKI との技術的な統一を重視している。そのため、原則として、GPKI の技術仕様である、政府認証基盤相互運用性仕様書に定められた事項に準拠しなければならない。

なお、セコムトラストシステムズ株式会社が運用する各認証サービスの認証局についてはセコムトラストシステムズ株式会社が運用する各認証サービスのリポジトリで公開する CP、CPS を参照のこと。

Security Communication RootCA2：https://repository.secomtrust.net/SC-Root2/
セコムパスポート for Web SR3.0 CA：https://repo1.secomtrust.net/spcpp/pfw/pfwsr3ca/
セコムパスポート for PublicID CA：https://repo1.secomtrust.net/spcpp/pfm20pub/

以降では、LGPKI に固有な仕様について記述する。

3.2. 証明書と失効情報（CRL/ARL）のプロファイル

LGPKI で定義するプロファイルの詳細に関しては「地方公共団体組織認証基盤・プロファイル設計書」に示す。

なお、組織 CA 等の発行する証明書の名義（Subject）を表３－１、表３－２に、セコムパスポート for Web SR3.0 CA が発行する Web サーバ証明書の名義（Subject）を表３－３に、セコムパスポート for PublicID CA が発行するメール用証明書、コードサイニング証明書の証明書の名義（Subject）を表３－４表 ３－３、表３－５に、第三次 LGPKI 組織 CA の発行する暗号化通信用等証明書の名義（Subject）を表３－６に示す。

表 ３－１職責証明書

識別属性型	属性型	属性型説明	値の設定例

c	countryName	電子証明書所有者の国名	JP
o	organizeitionName	電子証明書所有者の組織名	Local Governments
l	localityName	電子証明書所有者の地域名	都道府県（英語）
ou	organizationalUnitName	電子証明書所有者の組織単位名	地方公共団体名（英語）
ou (*1)	organizationalUnitName	電子証明書所有者の組織単位名（*2）	所属部門名（英語）
cn (*1)	commonName	電子証明書所有者の固有名称	役職名等（英語）

(*1) ou、cn の英語表記は 64 文字以内という制限があり、64 文字を超える名称等については 64 文字以内で収まるような名称に変更する。

(*2) 局、室、課名は、organizationalUnitName を用いて表現する。本 organizationalUnitName は、0 ～ 7 個の間で任意に用いることが出来る。

表 3 － 2 利用者証明書

識別属性型	属性型	属性型説明	値の設定例
c	countryName	電子証明書所有者の国名	JP
o	organizeitionName	電子証明書所有者の組織名	Local Governments
l	localityName	電子証明書所有者の地域名	都道府県（英語）
ou	organizationalUnitName	電子証明書所有者の組織単位名	地方公共団体名（英語）
ou (*1)	organizationalUnitName	電子証明書所有者の組織単位名（*2）	所属部門名（英語）
cn (*1)	commonName	電子証明書所有者の固有名称	役職名等（英語）

(*1) ou、cn の英語表記は 64 文字以内という制限があり、64 文字を超える名称等については 64 文字以内で収まるような名称に変更する。

(*2) 局、室、課名は、organizationalUnitName を用いて表現する。本 organizationalUnitName は、0 ～ 7 個の間で任意に用いることが出来る。

証明書発行要求（以下「CSR」という。）ファイルに設定できるサブジェクトが定型化されているなどの Web サーバ及び署名ツール側の技術的理由により、指定する識別名と同様の識別名構造での CSR ファイル作成が不可能な場合は、CSR ファイル作成側で指定する識別名の読み替えを行う。

表 3 － 3 Web サーバ証明書

識別属性型	属性型	読み替え	値の設定例
c	countryName	国コードをそのまま指定。	JP
st または s	state or province	各地方公共団体の属する都道府県域を指定。	東京都の場合 「Tokyo」「Tokyo-to」
l	localityName	各地方公共団体の組織の所在地（代表）が置かれている市区町村名を指定。	東京都の場合 「Shinjuku-ku」 「Shinjuku City」
o	organizeitionName	各地方公共団体の団体名	東京都の場合 「Tokyo」「Tokyo-to」
ou (*1)	organizationalUnitName	部署又はグループ名。省略可能。	xxxxx Prefecture Soumubu IT Suishinshitsu
cn (*1)	commonName	サーバの完全修飾ドメイン名（FQDN）を指定。	www.pref.xxxxx.lg.jp

(*1) ou、cn の英語表記は 64 文字以内という制限があり、64 文字を超える名称等については 64 文字以内で収まるような名称に変更する。

表 3 － 4 メール用証明書

識別属性型	属性型	属性型説明	値の設定例
c	countryName	電子証明書所有者の国名	JP
o	organizeitionName	電子証明書所有者の組織名	Local Governments
l	localityName	電子証明書所有者の地域名	都道府県（英語）
ou	organizationalUnitName	電子証明書所有者の組織単位名	地方公共団体名（英語）
ou (*1)	organizationalUnitName	電子証明書所有者の組織単位名（*2）	所属部門名（英語）
cn (*1)	commonName	電子証明書所有者の固有名称	役職名等（英語）
E	E-mail address	電子証明書所有者のメールアドレス	xxxxx@pref.xxxx.lg.jp

(*1) ou、cn の英語表記は 64 文字以内という制限があり、64 文字を超える名称等については 64 文字以内で収まるような名称に変更する。

(*2) 局、室、課名は、organizationalUnitName を用いて表現する。本 organizationalUnitName は、0 ～ 7 個の間で任意に用いることが出来る。

表 3 － 3 コードサイニング証明書

識別属性型	属性型	読み替え	値の設定例
c	countryName	国コードをそのまま指定。	JP
st または s	state or province	指定しない。省略不可の場合、各地方公共団体の属する都道府県域を指定。	
l	localityName	各地方公共団体の属する都道府県域を指定。	都道府県（英語）
o	organizeitionName	Local Governments を固定で指定。	Local Governments
ou (*1)	organizationalUnitName	地方公共団体名を指定。サーバ管理組織名も任意で指定可能。	xxxxx Prefecture Soumubu IT Suishinshitsu
cn (*1)	commonName	地方公共団体名及びコード管理責任者を表す CodeAdmin を指定(*2)。組織名、アプリケーション名も任意で指定可能。	CodeAdmin of xxxxx Prefecture {組織名} {アプリケーション名}

(*1) ou、cn の英語表記は 64 文字以内という制限があり、64 文字を超える名称等については 64 文字以内で収まるような名称に変更する。

(*2) コード管理責任者の表記は、特段の理由がない限り CodeAdmin 固定とする。

表 3 － 4 暗号化通信用等証明書

識別属性型	属性型	属性型説明	値の設定例
c	countryName	電子証明書所有者の国名	JP
o	organizeitionName	電子証明書所有者の組織名	Local Governments
l	localityName	電子証明書所有者の地域名	都道府県（英語）
ou (*1)	organizationalUnitName	電子証明書所有者の組織単位名	地方公共団体名（英語）
cn (*1)	commonName	電子証明書所有者の固有名称	情報提供ネットワークシステムが定める機関コード

(*1) ou、cn の英語表記は 64 文字以内という制限があり、64 文字を超える名称等については 64 文字以内で収まるような名称に変更する。

3.3. 証明書と失効情報（CRL/ARL）の公開方法

LGPKIでは基本的に第四次LGPKI公開リポジトリを使用し各種証明書や失効情報（CRL/ARL）を公開するものとする。そのため、登録内容に基準が無ければ、認証パスの構築や検証の際に

参照できなくなってしまう。

本仕様書ではリポジトリ内のスキーマや DIT を示すディレクトリプロファイルを「6 ディレクトリプロファイル」に規定する。

3.4. 推奨署名アルゴリズム

LGPKI では以下に示す点に従って、推奨署名アルゴリズムを定める。

- 署名者があるアルゴリズムで署名したデータを、署名検証者が検証する際にはそのアルゴリズムを解釈できなければならない。
- 現状利用できるアルゴリズムが将来アルゴリズム危殆化により利用できなくなることも考慮しなければならない。
- 認証パス中に複数の署名アルゴリズムがある場合、認証パス中にある全てのアルゴリズムを解釈できなければならない。

3.4.1. アルゴリズム

エンドエンティティは署名検証する際、署名者が使用した署名アルゴリズムをサポートしていなければならない。

原則として署名アルゴリズムは以下を用いる。

- Sha256WithRSAEncryption（1.2.840.113549.1.1.11）
- sha1WithRSAEncryption（1.2.840.113549.1.1.5）

なお、sha1WithRSAEncryption は過去の互換性のためにサポートする。

3.4.2. 鍵長

署名検証者は、署名者が使用する鍵長の署名を検証できなければならない。また認証パスに含まれる全ての証明書の署名をその鍵長で検証できなければならない。そのため、少なくとも以下の鍵長での署名検証ができなければならない。

- RSA、2048 ビットまで

3.4.3. 認証パスの構築・検証方法

認証パスの構築・検証に関しては、政府認証基盤相互運用性仕様書に記載の技術要件に準拠することが必須である。

3.5. LGPKI における名前と DIT の規定

3.5.1. 識別名、相対識別名

LGPKI における名前としては、generalName の directoryName を用いる。issuer 及び subject もまた directoryName である。directoryName は識別名、すなわち一個以上の相対識別名のシーケンスである。

ここでは識別名及びその構成要素である相対識別名の使用可能文字、証明書へのエンコード方式について規定する。以後本書では、特に断らない限り「識別名」と記している場合、相対識別名も含むものとする。

これらは原則として RFC5280 の規定にしたがうものとするが、以下では LGPKI における特記事項について記述する。

3.5.2. エンコードタイプ

subject や issuer で使用される DN を記述する文字コードについては、原則として UTF8 String を用いる。ただし、アプリケーション CA 等から発行される証明書については、当面 Printable String で発行する。

3.5.3. issuerAltName 及び subjectAltName

issuerAltName 及び subjectAltName の directoryName については、日本語表記を格納することもできるものとする。その場合、エンコードタイプは UTF8String としなければならない。

4　証明書検証サーバの利用

4.1. 概要

LGPKIでは、第四次LGPKI証明書検証サーバは第三次LGPKIブリッジCA又は第四次LGPKI組織CA R2によって認証される。また、証明書検証サーバを利用するのは、第三次LGPKIブリッジCA又は第四次LGPKI組織CA R2をトラストアンカーとする地方公共団体の職責者もしくはそれに準ずる証明書検証者である。また、検証対象となる証明書は、LGPKIが発行する証明書のほかに、第三次LGPKIブリッジCA及び第四次LGPKI組織CA R2が相互認証している他CAが発行した証明書である。第四次LGPKI証明書検証サーバは、LGPKIが発行した証明書を検証する者に対し、証明書検証という非常に複雑な処理の代行や、さらに、LDAPによる第四次LGPKI公開リポジトリへのアクセスが困難な者に対し、各種認証情報を提供する等、LGPKIが発行した証明書を検証する側の負担を軽減するものである。

本章では、まず第三次LGPKIブリッジCA又は第四次LGPKI組織CA R2が提供する第四次LGPKI証明書検証サーバについて記述し、その後証明書を発行する第三次LGPKIブリッジCA及び第四次LGPKI組織CA R2と、第四次LGPKI証明書検証サーバを利用する利用者クライアントが満たすべき仕様について記述する。

4.2. 証明書検証サーバ用証明書（VA 証明書）

第四次LGPKI証明書検証サーバの証明書は、第三次LGPKIブリッジCA又は第四次LGPKI組織CA R2が発行する。また、証明書検証サーバの証明書のextendedKeyUsageにはid-kp-OCSPSigningを設定する。

4.3. クライアント要件

第四次LGPKI証明書検証サーバを利用するクライアントが備えているべき点を記述する。

4.3.1. クライアント側の前準備

第四次LGPKI証明書検証サーバのレスポンスデータに含まれる署名を検証する必要があるため、クライアントは自分の利用する第四次LGPKI証明書検証サーバの署名を検証するのに必要な下記の情報を設定する必要がある。

- トラストアンカーの証明書

4.4. 証明書検証サーバ通信プロトコル

第四次LGPKI証明書検証サーバとの通信プロトコルについては、別添1に示す。

4.5. 証明書検証サーバのアクセス制御

第四次 LGPKI 証明書検証サーバは、公的個人認証サービスから発行された証明書の検証を行う際、公的個人認証サービスの失効情報を参照する。LGPKI では、第四次 LGPKI 証明書検証サーバの利用に当たって、公的個人認証サービスから失効情報の参照が許可された地方公共団体からの利用だけに限ることとする。

５　OCSP レスポンダの利用

LGPKI では、第四次 LGPKI にて、セコムトラストシステムズ株式会社が運用する各認証サービスの OCSP レスポンダを利用する。この OCSP レスポンダについてはセコムトラストシステムズ株式会社が運用する各認証サービスのリポジトリで公開する CP、CPS を参照のこと。

Security Communication RootCA2：https://repository.secomtrust.net/SC-Root2/
セコムパスポート for Web SR3.0 CA：https://repo1.secomtrust.net/spcpp/pfw/pfwsr3ca/
セコムパスポート for PublicID CA：https://repo1.secomtrust.net/spcpp/pfm20pub/

6　ディレクトリプロファイル

6.1. LGPKI における DIT 構造

全てのエンティティは、全体として矛盾のない一つのディレクトリ情報ツリー（DIT）を構成する。

DIT の第一階層は国、第二階層は LGPKI（"LGPKI"、”LGPKI2”）コンテナとする。第三階層は、"LGPKI"以下に第三次 LGPKI ブリッジ CA と第三次 LGPKI 組織 CA、第四次 LGPKI アプリケーション CAR2、"LGPKI2"以下に第四次 LGPKI 組織 CA R2 とする。

なお LGPKI においては、発行する証明書の subject や issuer で使用される DN を記述する文字コードが Printable String の CA と UTF8String の CA がある。第三次 LGPKI ブリッジ CA、第三次 LGPKI 組織 CA 及び第四次 LGPKI 組織 CA R2 の文字コードは UTF8String である。

図　6 － 1 に LGPKI における DIT 構造を示す。

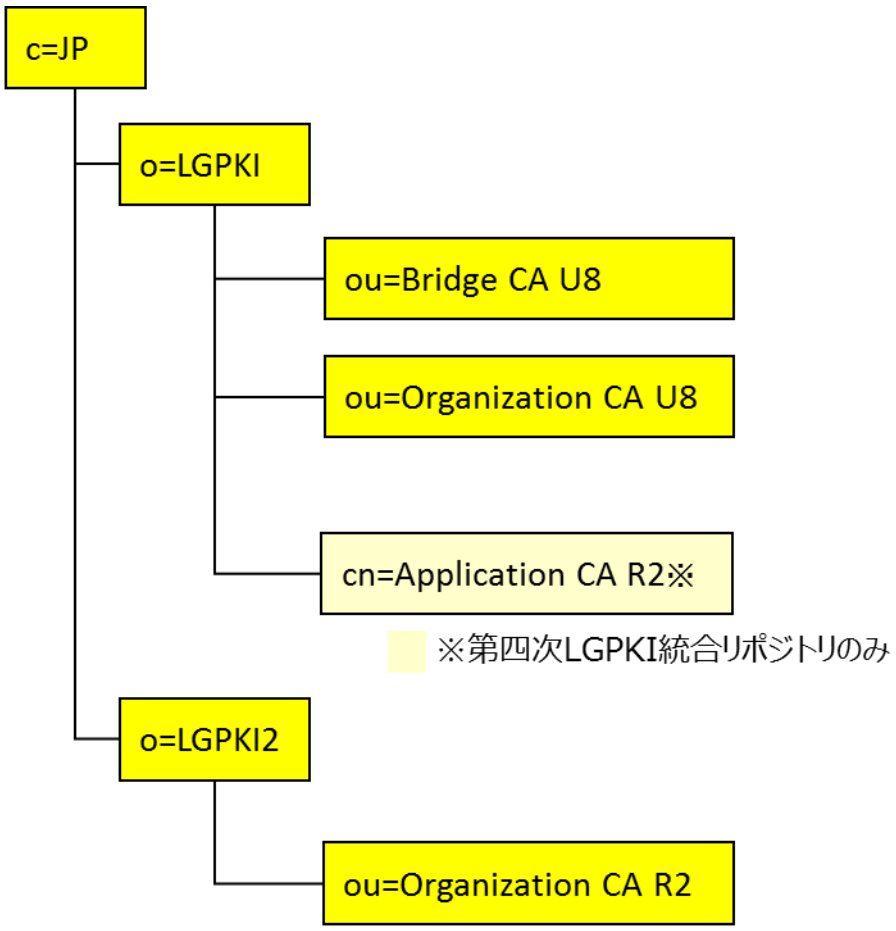

図　6 － 1 LGPKI における DIT 構造

6.2. DIT の名前形式

DIT 構造の各階層において、識別名に用いる属性を表 ６－１のように定める。

表 ６－１階層ごとの識別属性型と属性値

階層	識別属性型	属性値として取り得る値
第一階層	c	"JP"
第二階層	o	"Local Goverments"、"LGPKI"、"LGPKI2"、"地方公共団体"
第三階層	ou	"Bridge CA U8"、”Organization CA U8”、”Organization CA R2”
	cn	“Application CA R2”
	l	都道府県域名
第四階層	ou	地方公共団体名
第五階層以下	ou	地方公共団体内各組織・部門
リーフ	cn	名義（役職名義）

6.3. リポジトリ等に格納される情報

リポジトリ等に格納されるエントリ及び属性について示す。

6.3.1. LGPKI コンテナ

LGPKI コンテナを表すエントリを構成するオブジェクトクラスとして、RFC4519 に定められている organization オブジェクトクラスを用いる。

organization オブジェクトクラスの定義及び organization オブジェクトクラスの上位オブジェクトクラスとして参照される top オブジェクトクラスの定義は、各々表 ６－２、表 ６－３のとおりである。

表 ６－２　organization オブジェクトクラスの定義

【オブジェクトクラス名】	organization
【オブジェクト識別子】	joint-iso-itu-t(2) ds(5) objectClass(6) organization(4)
【種別】	構造型
【上位オブジェクトクラス】	top
【必須属性】	o
【任意属性】	userPassword searchGuide seeAlso businessCategory

	x121Address registeredAddress destinationIndicator preferedDeliveryMethod telexNumber telexTerminalIdentifier telephoneNumber internationaliSDNNumber facsimileTelephoneNumber street postOfficeBox postalCode postalAddress physicalDeliveryOfficeName st l description

表 6－3　top オブジェクトクラスの定義

【オブジェクトクラス名】	top
【オブジェクト識別子】	joint-iso-itu-t(2) ds(5) objectClass(6) top(0)
【種別】	抽象型
【上位オブジェクトクラス】	なし
【必須属性】	objectClass
【任意属性】	なし

(1) LGPKI コンテナ

LGPKI のコンテナを表す名前("LGPKI"、”LGPKI2”)を格納する属性として organization オブジェクトクラスの必須属性である o 属性を用いる。

o 属性の定義及び o 属性の上位属性として参照される name 属性の定義は、各々表 6－4、表 6－5 のとおりである。

表 6－4　o 属性の定義

【属性名】	o
【オブジェクト識別子】	joint-iso-itu-t(2) ds(5) attributeType(4) organizationName(10)
【上位属性】	name

【照合規則】	name 属性を継承
【属性構文】	name 属性を継承

表 6－5　name 属性の定義

【属性名】		name
【オブジェクト識別子】		joint-iso-itu-t(2) ds(5) attributeType(4) name(41)
【上位属性】		なし
【照合規則】	＜完全一致＞	caseIgnoreMatch
	＜部分一致＞	caseIgnoreSubstringMatch
	＜順序性＞	なし
【属性構文】		DirectoryString

6.3.2. CA エントリ

第三次 LGPKI ブリッジ CA 及び組織 CA 等を表すエントリを構成するオブジェクトクラスとして、RFC4519 に定められている organizationalUnit オブジェクトクラスを用い、これに補助クラスとして、RFC4523 に定められている pkiCA オブジェクトクラスを付加する。

organziationalUnit オブジェクトクラスの定義及び organizaionlUnit オブジェクトクラスの上位オブジェクトクラスとして参照される top オブジェクトクラスの定義は、各々表 6－6、表 6－3 のとおりである。

表 6－6　organizationalUnit の定義

【オブジェクトクラス名】	organizationalUnit
【オブジェクト識別子】	joint-iso-itu-t(2) ds(5) objectClass(6) organizationalUnit(5)
【種別】	構造型
【上位オブジェクトクラス】	top
【必須属性】	objectClass ou
【任意属性】	userPassword searchGuide seeAlso

	businessCategory x121Address registeredAddress destinationIndicator preferedDeliveryMethod telexNumber telexTerminalIdentifier telephoneNumber internationaliSDNNumber facsimileTelephoneNumber street postOfficeBox postalCode postalAddress physicalDeliveryOfficeName st l description

organizationalRole オブジェクトクラスの定義及び organizationalRole オブジェクトクラスの上位オブジェクトクラスとして参照される top オブジェクトクラスの定義は、各々表 ６－７、表 ６－３のとおりである。

表 ６－７ organizationalRole の定義

【オブジェクトクラス名】	organizationalRole
【オブジェクト識別子】	joint-iso-itu-t(2) ds(5) objectClass(6) organizationalRole(8)
【種別】	構造型
【上位オブジェクトクラス】	top
【必須属性】	objectClass cn
【任意属性】	x121Address registeredAddress destinationIndicator preferredDeliveryMethod telexNumber teletexTerminalIdentifier telephoneNumber internationaliSDNNumber facsimileTelephoneNumber seeAlso roleOccupant preferredDeliveryMethod street postOfficeBox postalCode postalAddress

	physicalDeliveryOfficeName ou st l description

pkiCA オブジェクトクラスの定義は表 ６－８のとおりである。

表 ６－８　pkiCA の定義

【オブジェクトクラス名】	pkiCA
【オブジェクト識別子】	joint-iso-itu-t(2) ds(5) objectClass(6) pkiCA(22)
【種別】	補助型
【上位オブジェクトクラス】	top
【必須属性】	objectClass
【任意属性】	cACertificate certificateRevocationList authorityRevocationList crossCertificatePair

(1) CA 名称

CA 名称（第三次 LGPKI ブリッジ CA（"Bridge CA U8"）、第三次 LGPKI 組織 CA（"Organization CA U8"））あるいは第四次 LGPKI 組織 CA R2（" Organization CA R2”）を格納する属性として、organizationalUnit オブジェクトクラスの必須属性である ou 属性を用いる。

CA 名称（第四次 LGPKI アプリケーション CA R2（"Application CA R2"））を格納する属性として、organizationalRole オブジェクトクラスの必須属性である cn 属性を用いる。

ou 属性の定義、及び ou 属性の上位属性として参照される name 属性の定義は、各々表 ６－９、表 ６－５のとおりである。

表 ６－９　ou 属性の定義

【属性名】	ou
【オブジェクト識別子】	joint-iso-itu-t(2) ds(5) attributeType(4) organizationalUnitName(11)
【上位属性】	name
【照合規則】	name 属性を継承
【属性構文】	name 属性を継承

cn 属性の定義及び cn 属性の上位属性として参照される name 属性の定義は、各々表 ６－１０、表 ６－５のとおりである。

表 ６－１０　cn 属性の定義

【属性名】	cn
【オブジェクト識別子】	joint-iso-itu-t(2) ds(5) attributeType(4) commonName (3)
【上位属性】	name
【照合規則】	name 属性を継承
【属性構文】	name 属性を継承

(2) 自己署名証明書及びリンク証明書

自己署名証明書及びリンク証明書を格納する属性として、pkiCA オブジェクトクラスの設定上追加必須属性である cACertificate 属性を用いる。

自己署名証明書及びリンク証明書は､第三次 LGPKI ブリッジ CA、第四次 LGPKI 組織 CAR2 が持つ。

この属性は"cACertificate;binary"と指定することによって属性値の受け渡しを行う。

cACertificate 属性の定義は表６－１１のとおりである。

表 ６－１１　cACertificate 属性の定義

【属性名】		cACertificate
【オブジェクト識別子】		joint-iso-itu-t(2) ds(5) attributeType(4) cACertificate(37)
【上位属性】		なし
【照合規則】	＜完全一致＞	certificateExactMatch
	＜部分一致＞	なし
	＜順序性＞	なし
【属性構文】		Certificate

(3)相互認証証明書

相互認証証明書は､次の二つの属性に格納される。

ア）crossCertificatePair 属性

第三次 LGPKI ブリッジ CA と第四次 LGPKI 組織 CAR2 の CA エントリでは、他 CA との間で取り交わした相互認証証明書が、pkiCA オブジェクトクラスの設定上追加必須属性である crossCertificatePair 属性に格納される。

この属性は"crossCertificatePair;binary"と指定することによって属性値の受け渡しを行う。

crossCertificatePair 属性の定義は表６－１２のとおりである。

表 ６－１２　crossCertificatePair 属性の定義

【属性名】		crossCertificatePair
【オブジェクト識別子】		joint-iso-itu-t(2) ds(5) attributeType(4) crossCertificatePair(40)
【上位属性】		なし
【照合規則】	＜完全一致＞	certificatePairExactMatch
	＜部分一致＞	なし
	＜順序性＞	なし
【属性構文】		CertificatePair

イ）cACertificate 属性

第三次 LGPKI 組織 CA の CA エントリでは、第三次 LGPKI ブリッジ CA から発行された相互認証証明書が、pkiCA オブジェクトクラスの cACertificate 属性に格納される。

この属性は"cACertificate;binary"と指定することによって属性値の受け渡しを行う。

cACertificate 属性の定義は表６－１３のとおりである。

表 ６－１３　cACertificate 属性の定義

【属性名】	cACertificate
【オブジェクト識別子】	joint-iso-itu-t(2) ds(5) attributeType(4) cACertificate(37)
【上位属性】	なし

【照合規則】	＜完全一致＞	certificateExactMatch
	＜部分一致＞	なし
	＜順序性＞	なし
【属性構文】		Certificate

(4) CRL

CRL を格納する属性として、pkiCA オブジェクトクラスの設定上追加必須属性である certificateRevocationList 属性を用いる。

この属性は"certificateRevocationList;binary"と指定することによって属性値の受け渡しを行う。

certificateRevocationList 属性の定義は表６－１４のとおりである。

表 ６－１４１１　certificateRevocationList 属性の定義

【属性名】		certificateRevocationList
【オブジェクト識別子】		joint-iso-itu-t(2) ds(5) attributeType(4) certificateRevocationList(39)
【上位属性】		なし
【照合規則】	＜完全一致＞	certificateListExactMatch
	＜部分一致＞	なし
	＜順序性＞	なし
【属性構文】		CertificateList

(5) ARL

CA に関する CRL を格納する属性として、pkiCA オブジェクトクラスの設定上追加必須属性である authorityRevocationList 属性を用いる。

この属性は"authorityRevocationList;binary"と指定することによって属性値の受け渡しを行う。

authorityRevocationList 属性の定義は表 ６－１２１５のとおりである。

表 ６－１２５　authorityRevocationList 属性の定義

【属性名】	authorityRevocationList
【オブジェクト識別子】	joint-iso-itu-t(2) ds(5) attributeType(4) authorityRevocationList(38)

【上位属性】		なし
【照合規則】	＜完全一致＞	certificateListExactMatch
	＜部分一致＞	なし
	＜順序性＞	なし
【属性構文】		CertificateList

6.4. リポジトリ等のインタフェース仕様

リポジトリ等及びセコム公開リポジトリに対して、民間側が利用する行政サービスアプリケーションからは、証明書・署名の検証のための認証情報の検索が行われる。リポジトリ等及びセコム公開リポジトリに対する一切の更新系の操作は許可されない。

民間側が利用する行政サービスアプリケーションは、LDAPv3 をサポートするものとする。

BindRequest

認証なしによる Bind のみを許可する。この場合、BindRequest パラメータは以下のとおりである。

version	2 あるいは 3
name	"" (長さ 0 の文字列)
authenticaton.simple	"" (長さ 0 の文字列)

Bind Response

RFC4511 4.2.2 の規定のとおりとする。

Unbind Request/Response

RFC4511 4.3 の規定のとおりとする。

Search Request

以下の事項以外については、RFC4511 4.5.1 の規定のとおりとする。

derefAliases パラメータは neverDerefAliases のみとする。

typesOnly パラメータは FALSE としなくてはならない。

filter 項目について、approxMatch 及び extensibleMatch はサポートしない。

SearchResEntry/ResDone/ResRef

RFC4511 4.5.2 及び 4.5.3 の規定のとおりとする。

SearchResponse

RFC1777 4.3 の規定のとおりとする。

6.5. リポジトリ等のアクセス制御

6.5.1. 認証ポリシー

- 原則として認証しない。匿名によるアクセスを許可する。
  この時、後述するアクセス制御ポリシーに従い、一部を除く全ての情報の参照が可能となるが、あらゆる情報の更新はできない。
- リポジトリ等及びセコム公開リポジトリが管理・格納する情報を更新する操作員に対しては、最低限パスワードによる認証を行う。この時、後述するアクセス制御ポリシーに従い、許可された範囲の情報に対する参照・更新・削除が可能となる。

6.5.2. アクセス制御ポリシー

以下の方針によるアクセス制御を実施する。

- リポジトリ等及びセコム公開リポジトリにアクセス可能な全てのクライアントに対して、全ての情報に対する参照権限を与える。ただし、一部公開すべきでない属性については、参照権限を与えない。さらに、各操作員を表すエントリに対しては、自分以外からの参照権限を与えない。
- 資格と権限のある操作員に対して、リポジトリ等及びセコム公開リポジトリが管理・格納する全ての情報について、参照・更新権限を与える。さらに、エントリの追加・削除・識別名変更権限を与える。