C-6-4-4

LGPKI
プロファイル設計書

第 2.1 版

令和２年２月１５日

地方公共団体情報システム機構

※文中では、CA 名称の後ろに発行者(Issuer)の識別名(Distinguished Name)に使用している文字コードを付与して記述する。文字コードに PrintableString を使用している場合は(PS)とし、UTF8String を使用している場合は(UTF8)とする。

【改訂履歴】

版数	年月日	主な改訂内容
1.0	平成 23 年 11 月 1 日	新規作成
1.1	平成 25 年 3 月 26 日	記載漏れ追記及び誤記修正
1.2	平成 26 年 4 月 1 日	地方公共団体情報システム機構発足に伴う規程の移管
1.3	平成 26 年 11 月 4 日	アプリケーション CAG3 の階層化に伴う改訂
1.4	平成 27 年 12 月 18 日	暗号化通信用等証明書の追加に伴う改訂
1.5	平成 28 年 10 月 14 日	OCSP レスポンダの追加に伴う改訂
1.6	平成 29 年 2 月 24 日	アプリケーション CAG4 の追加に伴う改訂
1.7	平成 29 年 7 月 3 日	アプリケーション CAG4 の運用本番化に伴う改訂
1.8	平成 30 年 8 月 24 日	第四次 LGPKI アプリケーション CAR2 構築に伴う改訂
1.9	令和元年５月 20 日	第四次 LGPKI 組織 CAR2 構築に伴う改訂 アプリケーション CAG3、アプリケーション CAG4 の運用終了に伴う改訂
2.0	令和元年８月 25 日	相互認証証明書（sha1WithRSAEncryption）**の廃止に伴う改訂**
2.1	令和２年２月 15 日	第四次 LGPKI 証明書検証サーバにおける VA 証明書格納作業に**伴う改訂**

1. はじめに

本プロファイル設計書は、地方公共団体組織認証基盤（LGPKI）の各 CA が発行する各証明書等のプロファイルを示したものである。

2. ブリッジ CA (UTF8)

ブリッジ CA(UTF8)から発行される相互認証証明書、VA 証明書、自己署名証明書、リンク証明書及び失効リスト(CRL/ARL)プロファイルを示す。

2.1. 証明書プロファイル

地方公共団体組織認証基盤において運用される、ブリッジ CA から発行される証明書プロファイルを示す。

2.1.1. 相互認証証明書 (ブリッジ CA (UTF8) → 組織 CA)

(1) 証明書基本領域(Basic)

Version	
Version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
Signature	
algorithmIdentifier algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数) 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
Validity	
validity notBefore notAfter	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
Issuer	
countryName organizationName organizationalUnitName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI 電子証明書発行者の組織単位名

	組織単位名の値 型:UTF8String 値:Bridge CA U8

Subject	
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8
subjectPublicKeyInfo	
subjectPublicKeyInfo algorithmIdentifier algorithm	電子証明書所有者の公開鍵に関する情報 暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数) 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:000001100(keyCertSign、cRLSign)

certificatePolicies （クリティカルフラグ = TRUE）	
policyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型：OID 値：1 2 392 200110 10 8 5 1 1 10
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型：OID 値：1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ（URI） 型：IA5String 値：http://www.lgpki.jp
policyIdentifier	ポリシのオブジェクト ID 型：OID 値：1 2 392 200110 10 8 5 1 7 10
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型：OID 値：1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ（URI） 型：IA5String 値：http://www.lgpki.jp

basicConstraints （クリティカルフラグ = TRUE）	
basicConstraints	基本的制約
cA	CA かどうかを示すフラグ 型：BOOLEAN 値：TRUE
cRLDistributionPoints （クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
directoryName	CRL 配布点のディレクトリ名
countryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
organizationName	CRL 配布点の組織名 組織名の値 型：UTF8String 値：LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Bridge CA U8

2.1.2. 相互認証証明書 (ブリッジ CA (UTF8) → 政府認証基盤ブリッジ CA)

(1) 証明書基本領域(Basic)

Version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
SerialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数) 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
Validity	
validity notBefore notAfter	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
Issuer	
countryName organizationName organizationalUnitName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI 電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8
Subject	
countryName organizationName organizationalUnitName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP 電子証明書所有者の組織名(政府認証基盤) 組織名の値 型:UTF8String 値:Japanese Government 電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:BridgeCA

SubjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）
algorithm	暗号アルゴリズムのオブジェクト ID 型：OID 値：1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型：NULL 値：なし
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier（クリティカルフラグ = FALSE）	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子 SHA-1 160bit 型：OCTET STRING 値：ユニークなバイト列
subjectKeyIdentifier（クリティカルフラグ = FALSE）	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型：OCTET STRING 値：ユニークなバイト列
keyUsage（クリティカルフラグ = TRUE）	
keyUsage	鍵の使用目的 型：BitString 値：000001100(keyCertSign、cRLSign)
certificatePolicies（クリティカルフラグ = TRUE）	
policyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型：OID 値：1 2 392 200110 10 8 5 1 1 10
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型：OID 値：1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ(URI) 型：IA5String 値：http://www.lgpki.jp
policyIdentifier	ポリシのオブジェクト ID 型：OID 値：1 2 392 200110 10 8 5 1 7 10
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型：OID 値：1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ(URI) 型：IA5String 値：http://www.lgpki.jp
policyMappings（クリティカルフラグ = TRUE）	
issuerDomainPolicy	発行者のドメイン・ポリシ OID 型：OID 値：1 2 392 200110 10 8 5 1 1 10
SubjectDomainPolicy	相互認証先 CA のドメイン・ポリシ OID 型：OID 値：0 2 440 100145 8 1 1 1 110

issuerDomainPolicy	発行者のドメイン・ポリシ OID 型：OID 値：1 2 392 200110 10 8 5 1 7 10
SubjectDomainPolicy	相互認証先 CA のドメイン・ポリシ OID 型：OID 値：0 2 440 100145 8 1 1 21 130

basicConstraints （クリティカルフラグ = TRUE）	
BasicConstraints	基本的制約
cA	CA かどうかを示すフラグ 型：BOOLEAN 値：TRUE
policyConstraints （クリティカルフラグ = TRUE）	
policyConstraints	ポリシ制約に関する情報
requireExplicitPolicy	証明書ポリシの明示を要求 型：INTEGER 値：0
inhibitPolicyMapping	ポリシマッピングの制限 型：INTEGER 値：1
cRLDistributionPoints （クリティカルフラグ = FALSE）	
CRLDistributionPoints	CRL 配布点に関する情報
DistributionPoint	CRL 配布点
FullName	
directoryName	CRL 配布点のディレクトリ名
countryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
organizationName	CRL 配布点の組織名 組織名の値 型：UTF8String 値：LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Bridge CA U8

2.1.3. VA 証明書

(1) 証明書基本領域(Basic)

Version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
Signature	
algorithmIdentifier (公開鍵暗号とハッシュ関数) algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
Validity	
validity notBefore notAfter	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
Issuer	
countryName organizationName organizationalUnitName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI 電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8
Subject	
証明書の要求ファイルの内容による	

subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(2) 証明書拡張領域 (extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:100000000(digitalSignature)
extendedKeyUsage (クリティカルフラグ = FALSE)	
KeyPurposeId	鍵の使用目的(拡張) 型:OID 値:1 3 6 1 5 5 7 3 9(OCSPSigning) 型:OID 値:1 3 6 1 5 5 7 48 1 5(id-pkix-ocsp-nocheck)
certificatePolicies (クリティカルフラグ = TRUE)	
PolicyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 3 10
cRLDistributionPoints (クリティカルフラグ = FALSE)	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
directoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型:PrintableString 値:JP
OrganizationName	CRL 配布点の組織名 組織名の値 型:UTF8String 値:LGPKI
OrganizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8

2.1.4. 自己署名証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8

Subject	
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(2) 証明書拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:000001100 (keyCertSign、cRLSign)
basicConstraints (クリティカルフラグ = TRUE)	
basicConstraints cA	基本的制約 CA かどうかを示すフラグ 型:BOOLEAN 値:TRUE

cRLDistributionPoints（クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
countryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
organizationName	CRL 配布点の組織名（地方公共団体組織認証基盤） 組織名の値 型：UTF8String 値：LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Bridge CA U8

2.1.5. リンク証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数) 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity notBefore notAfter	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName organizationName organizationalUnitName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI 電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8

Subject	
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(2) 証明書拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:000001100 (keyCertSign、cRLSign)
certificatePolicies (クリティカルフラグ = FALSE)	
PolicyInformation PolicyIdentifier	ポリシに関する情報 ポリシのオブジェクト ID 型:OID 値:2 5 29 32 0 (AnyPolicy)
basicConstraints (クリティカルフラグ = TRUE)	
basicConstraints cA	基本的制約 CA かどうかを示すフラグ 型:BOOLEAN 値:TRUE

cRLDistributionPoints（クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
countryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
organizationName	CRL 配布点の組織名（地方公共団体組織認証基盤） 組織名の値 型：UTF8String 値：LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Bridge CA U8

2.2. 失効リストプロファイル

地方公共団体組織認証基盤において運用される、ブリッジ CA から発行される失効リスト(CRL/ARL)プロファイルを示す。

2.2.1. CRL プロファイル

(1) 基本領域(Basic)

version	
version	失効リストフォーマットのバージョン番号 型:INTEGER 値:1
signature	
algorithmIdentifier	失効リストへの署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
issuer	
countryName	失効リスト発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	失効リスト発行者の組織名 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	失効リスト発行者の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8
thisUpdate	
thisUpdate	失効リストの更新日 型:UTC Time 値:yymmddhhmmssZ
nextUpdate	
nextUpdate	失効リストの次回更新日 型:UTC Time 値:yymmddhhmmssZ

revokedCertificates	
userCertificate	証明書シリアル番号 型：INTEGER 値：ユニークな整数
revocationDate	失効日 型：UTC Time 値：yymmddhhmmssZ
crlEntryExtensions	失効リストエントリ拡張領域
reasonCode （クリティカルフラグ = FALSE）	理由コード 型：ENUMERATED 値： keyCompromise(1) cACompromise(2) affiliationChanged(3) superseded(4) cessationOfOperation(5)

(2) 標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	失効リスト発行者の公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
cRLNumber(クリティカルフラグ = FALSE)	
cRLNumber	失効リストの番号 型:INTEGER 値:ユニークな整数
issuingDistributionPoint (クリティカルフラグ = TRUE)	
issuingDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型:PrintableString 値:JP
OrganizationName	CRL 配布点の組織名 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8
onlyContainsUserCerts	ユーザ証明書に対する失効のみかを示すフラグ 型:BOOLEAN 値:TRUE

2.2.2. ARL プロファイル

(1) 基本領域(Basic)

version	
version	失効リストフォーマットのバージョン番号 型:INTEGER 値:1
signature	
algorithmIdentifier (公開鍵暗号とハッシュ関数) algorithm parameters	失効リストへの署名に使用された暗号アルゴリズムの識別子 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
issuer	
countryName organizationName organizationalUnitName	失効リスト発行者の国名 国名の値 型:PrintableString 値:JP 失効リスト発行者の組織名 組織名の値 型:UTF8String 値:LGPKI 失効リスト発行者の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8
thisUpdate	
thisUpdate	失効リストの更新日 型:UTC Time 値:yymmddhhmmssZ
nextUpdate	
nextUpdate	失効リストの次回更新日 型:UTC Time 値:yymmddhhmmssZ
revokedCertificates	
userCertificate revocationDate crlEntryExtensions reasonCode (クリティカルフラグ= FALSE)	証明書シリアル番号 型:INTEGER 値:ユニークな整数 失効日 型:UTC Time 値:yymmddhhmmssZ 失効リストエントリ拡張領域 理由コード 型:ENUMERATED 値: keyCompromise(1) cACompromise(2) affiliationChanged(3) superseded(4) cessationOfOperation(5)

(2) 標準拡張領域(extensions)

authorityKeyIdentifier(クリティカルフラグ = FALSE)	
authorityKeyIdentifier	失効リスト発行者の公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
cRLNumber(クリティカルフラグ = FALSE)	
cRLNumber	失効リストの番号 型:INTEGER 値:ユニークな整数
issuingDistributionPoint (クリティカルフラグ = TRUE)	
issuingDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型:PrintableString 値:JP
organizationName	CRL 配布点の組織名 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8
onlyContainsCACerts	CA 証明書に対する失効のみかを示すフラグ 型:BOOLEAN 値:TRUE

3. 組織 CA

組織 CA から発行される相互認証証明書、職責証明書、利用者証明書、暗号化通信用等証明書、自己署名証明書、リンク証明書及び失効リスト(CRL/ARL)プロファイルを示す。

3.1. 証明書プロファイル

地方公共団体組織認証基盤において運用される、組織 CA から発行される証明書プロファイルを示す。

3.1.1. 相互認証証明書 (組織 CA → ブリッジ CA (UTF8))

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数) 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity notBefore notAfter	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName organizationName organizationalUnitName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI 電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8

Subject	
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:Bridge CA U8
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数) RSAEncryption
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:000001100(keyCertSign、cRLSign)

certificatePolicies （クリティカルフラグ = TRUE）	
policyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型：OID 値：1 2 392 200110 10 8 5 1 1 10
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型：OID 値：1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ（URI） 型：IA5String 値：http://www.lgpki.jp
policyIdentifier	ポリシのオブジェクト ID 型：OID 値：1 2 392 200110 10 8 5 1 7 10
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型：OID 値：1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ（URI） 型：IA5String 値：http://www.lgpki.jp
basicConstraints （クリティカルフラグ = TRUE）	
basicConstraints	基本的制約
cA	CA かどうかを示すフラグ 型：BOOLEAN 値：TRUE
cRLDistributionPoints （クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
FullName	
DirectoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
organizationName	CRL 配布点の組織名 組織名の値

organizationalUnitName	型:UTF8String 値:LGPKI CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8

3.1.2. 職責証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8

subject	
countryName	電子証明書所有者の国名 国名の値 型：PrintableString 値：JP
organizationName	電子証明書所有者の組織名 組織名の値 型：UTF8String 値：Local Governments
localityName	電子証明書所有者の地域名 地域名の値 型：UTF8String 値：都道府県名（英語）
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型：UTF8String 値：地方公共団体名（英語）
organizationalUnitName	電子証明書所有者の組織単位名（*1） 組織単位名の値 型：UTF8String 値：所属部門名（英語）
commonName	電子証明書所有者の固有名称 固有名称の値 型：UTF8String 値：役職名等（英語）
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数） RSAEncryption
algorithm	暗号アルゴリズムのオブジェクト ID 型：OID 値：1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型：NULL 値：なし
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値

(*1) 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。

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:110000000 (digitalSignature、nonRepudiation)
certificatePolicies (クリティカルフラグ = TRUE)	
policyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 1 10
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型:OID 値:1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ(URI) 型:IA5String 値:http://www.lgpki.jp
subjectAltName (クリティカルフラグ = FALSE)	
subjectAltName	電子証明書所有者の別名に関する情報
directoryName	所有者別名
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名 組織名の値 型:UTF8String 値:Local Governments の日本語表記
LocalityName	電子証明書所有者の地域名 地域名の値 型:UTF8String 値:都道府県域名(日本語表記)
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:地方公共団体名(日本語表記)
organizationalUnitName	電子証明書所有者の組織単位名(*2) 組織単位名の値 型:UTF8String 値:所属部門名(日本語表記)
commonName	電子証明書所有者の固有名称 固有名称の値 型:UTF8String 値:役職名等(日本語表記)

(*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。

cRLDistributionPoints（クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
OrganizationName	CRL 配布点の組織名 組織名の値 型：UTF8String 値：LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Organization CA U8

3.1.3. 利用者証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier (公開鍵暗号とハッシュ関数) algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity notBefore notAfter	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName organizationName organizationalUnitName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI 電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8

Subject	
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名 組織名の値 型:UTF8String 値:Local Governments
localityName	電子証明書所有者の地域名 地域名の値 型:UTF8String 値:都道府県名(英語)
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:地方公共団体名(英語)
organizationalUnitName	電子証明書所有者の組織単位名(*3) 組織単位名の値 型:UTF8String 値:申請者所属部門名(英語)
commonName	電子証明書所有者の固有名称 固有名称の値 型:UTF8String 値:役職名等(英語)
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(*3) 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。

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:10100000 (digitalSignature、keyEncipherment)
extendedKeyUsage (クリティカルフラグ = FALSE)	
KeyPurposeId	鍵の使用目的(拡張) 型:OID 値:1 3 6 1 5 5 7 3 2(clientAuth)
certificatePolicies (クリティカルフラグ = FALSE)	
policyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 7 10
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型:OID 値:1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ(URI) 型:IA5String 値:http://www.lgpki.jp
subjectAltName (クリティカルフラグ = FALSE)	
subjectAltName	電子証明書所有者の別名に関する情報
directoryName	所有者別名
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名 組織名の値 型:UTF8String 値:Local Governments の日本語表記
LocalityName	電子証明書所有者の地域名 地域名の値 型:UTF8String 値:都道府県域名(日本語表記)
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:地方公共団体名(日本語表記)
organizationalUnitName	電子証明書所有者の組織単位名(*4) 組織単位名の値 型:UTF8String 値:所属部門名(日本語表記)
commonName	電子証明書所有者の固有名称 固有名称の値 型:UTF8String 値:役職名等(日本語表記)

(*4) 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。

issureAltName （クリティカルフラグ = FALSE）	
issureAltName	電子証明書発行者の別名に関する情報
directoryName	発行者別名
countryName	電子証明書発行者の国名 国名の値 型：PrintableString 値：JP
organizationName	電子証明書発行者の組織名（地方公共団体組織認証基盤） 組織名の値 型：UTF8String 値：地方公共団体組織認証基盤
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型：UTF8String 値：組織認証局
cRLDistributionPoints （クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
directoryName	CRL 配布点のディレクトリ名
countryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
organizationName	CRL 配布点の組織名 組織名の値 型：UTF8String 値：LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Organization CA U8

3.1.4. 暗号化通信用等証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8

subject	
countryName	電子証明書所有者の国名 国名の値 型：PrintableString 値：JP
organizationName	電子証明書所有者の組織名 組織名の値 型：UTF8String 値：Local Governments
localityName	電子証明書所有者の地域名 地域名の値 型：UTF8String 値：都道府県名（英語）
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型：UTF8String 値：地方公共団体名（英語）
commonName	電子証明書所有者の固有名称 固有名称の値 型：UTF8String 値：情報提供ネットワークシステムが定める機関コード
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数） RSAEncryption
algorithm	暗号アルゴリズムのオブジェクト ID 型：OID 値：1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型：NULL 値：なし
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:101000000 (digitalSignature、keyEncipherment)
certificatePolicies (クリティカルフラグ = TRUE)	
policyInformation policyIdentifier policyQualifiers policyQualifierID qualifier	ポリシに関する情報 ポリシのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 8 10 ポリシ修飾子 ポリシ修飾子のオブジェクト ID 型:OID 値:1 3 6 1 5 5 7 2 1 CPS へのポインタ(URI) 型:IA5String 値:http://www.lgpki.jp
cRLDistributionPoints (クリティカルフラグ = FALSE)	
cRLDistributionPoints distributionPoint fullName DirectoryName CountryName OrganizationName organizationalUnitName 	CRL 配布点に関する情報 CRL 配布点 CRL 配布点のディレクトリ名 CRL 配布点の国名 国名の値 型:PrintableString 値:JP CRL 配布点の組織名 組織名の値 型:UTF8String 値:LGPKI CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8

3.1.5. 自己署名証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8

subject	
countryName	電子証明書所有者の国名 国名の値 型：PrintableString 値：JP
organizationName	電子証明書所有者の組織名（地方公共団体組織認証基盤） 組織名の値 型：UTF8String 値：LGPKI
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型：UTF8String 値：Organization CA U8
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）
algorithm	暗号アルゴリズムのオブジェクト ID 型：OID 値：1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型：NULL 値：なし
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier（クリティカルフラグ = FALSE）	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier（クリティカルフラグ = FALSE）	
subjectKeyIdentifier	電子証明書所有者(地方公共団体)の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage（クリティカルフラグ = TRUE）	
keyUsage	鍵の使用目的 型:BitString 値:000001100(keyCertSign、cRLSign)
subjectAltName（クリティカルフラグ = FALSE）	
subjectAltName directoryName countryName organizationName organizationalUnitName	電子証明書所有者の別名に関する情報 所有者別名 電子証明書所有者の国名 国名の値 型:PrintableString 値:JP 電子証明書所有者の組織名 組織名の値 型:UTF8String 値:地方公共団体組織認証基盤 電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:組織認証局
basicConstraints（クリティカルフラグ = TRUE）	
basicConstraints cA	基本的制約 CA かどうかを示すフラグ 型:BOOLEAN 値:TRUE
cRLDistributionPoints（クリティカルフラグ = FALSE）	
cRLDistributionPoints distributionPoint fullName directoryName countryName organizationName organizationalUnitName	CRL 配布点に関する情報 CRL 配布点 CRL 配布点のディレクトリ名 CRL 配布点の国名 国名の値 型:PrintableString 値:JP CRL 配布点の組織名 組織名の値 型:UTF8String 値:LGPKI CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8

3.1.6. リンク証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8

subject	
countryName	電子証明書所有者の国名 国名の値 型：PrintableString 値：JP
organizationName	電子証明書所有者の組織名（地方公共団体組織認証基盤） 組織名の値 型：UTF8String 値：LGPKI
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型：UTF8String 値：Organization CA U8
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）
algorithm	暗号アルゴリズムのオブジェクト ID 型：OID 値：1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型：NULL 値：なし
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者(地方公共団体)の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:000001100(keyCertSign、cRLSign)
certificatePolicies (クリティカルフラグ = FALSE)	
PolicyInformation PolicyIdentifier	ポリシーに関する情報 ポリシーのオブジェクト ID 型:OID 値:2 5 29 32 0 (AnyPolicy)
subjectAltName (クリティカルフラグ = FALSE)	
subjectAltName directoryName countryName organizationName organizationalUnitName	電子証明書所有者の別名に関する情報 所有者別名 電子証明書所有者の国名 国名の値 型:PrintableString 値:JP 電子証明書所有者の組織名 組織名の値 型:UTF8String 値:地方公共団体組織認証基盤 電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:組織認証局
basicConstraints (クリティカルフラグ = TRUE)	
basicConstraints cA	基本的制約 CA かどうかを示すフラグ 型:BOOLEAN 値:TRUE
cRLDistributionPoints (クリティカルフラグ = FALSE)	
cRLDistributionPoints distributionPoint fullName directoryName countryName organizationName organizationalUnitName	CRL 配布点に関する情報 CRL 配布点 CRL 配布点のディレクトリ名 CRL 配布点の国名 国名の値 型:PrintableString 値:JP CRL 配布点の組織名 組織名の値 型:UTF8String 値:LGPKI CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8

3.2. 失効リストプロファイル

地方公共団体組織認証基盤において運用される、組織 CA から発行される失効リスト(CRL/ARL)プロファイルを示す。

3.2.1. CRL プロファイル

(1) 基本領域(Basic)

version	
version	失効リストフォーマットのバージョン番号 型:INTEGER 値:1
signature	
algorithmIdentifier algorithm parameters	失効リストへの署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数) 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
issuer	
countryName organizationName organizationalUnitName	失効リスト発行者の国名 国名の値 型:PrintableString 値:JP 失効リスト発行者の組織名 組織名の値 型:UTF8String 値:LGPKI 失効リスト発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8
thisUpdate	
thisUpdate	失効リストの更新日 型:UTC Time 値:yymmddhhmmssZ
nextUpdate	
nextUpdate	失効リストの次回更新日 型:UTC Time 値:yymmddhhmmssZ

revokedCertificates	
userCertificate	証明書シリアル番号 型：INTEGER 値：ユニークな整数
revocationDate	失効日 型：UTC Time 値：yymmddhhmmssZ
crlEntryExtensions	失効リストエントリ拡張領域
reasonCode （クリティカルフラグ = FALSE）	理由コード 型：ENUMERATED 値： keyCompromise(1) cACompromise(2) affiliationChanged(3) superseded(4) cessationOfOperation(5)

(2) 標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	失効リスト発行者の公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
cRLNumber(クリティカルフラグ = FALSE)	
cRLNumber	失効リストの番号 型:INTEGER 値:ユニークな整数
issuingDistributionPoint (クリティカルフラグ = TRUE)	
issuingDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型:PrintableString 値:JP
OrganizationName	CRL 配布点の組織名 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8
onlyContainsUserCerts	ユーザ証明書に対する失効のみかを示すフラグ 型:BOOLEAN 値:TRUE

3.2.2. ARL プロファイル

(1) 基本領域(Basic)

version	
version	失効リストフォーマットのバージョン番号 型:INTEGER 値:1
signature	
algorithmIdentifier (公開鍵暗号とハッシュ関数) algorithm parameters	失効リストへの署名に使用された暗号アルゴリズムの識別子 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
issuer	
countryName organizationName organizationalUnitName	失効リスト発行者の国名 国名の値 型:PrintableString 値:JP 失効リスト発行者の組織名 組織名の値 型:UTF8String 値:LGPKI 失効リスト発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8
thisUpdate	
thisUpdate	失効リストの更新日 型:UTC Time 値:yymmddhhmmssZ
nextUpdate	
nextUpdate	失効リストの次回更新日 型:UTC Time 値:yymmddhhmmssZ
revokedCertificates	
userCertificate revocationDate crlEntryExtensions reasonCode (クリティカルフラグ= FALSE)	証明書シリアル番号 型:INTEGER 値:ユニークな整数 失効日 型:UTC Time 値:yymmddhhmmssZ 失効リストエントリ拡張領域 理由コード 型:ENUMERATED 値: keyCompromise(1) cACompromise(2) affiliationChanged(3) superseded(4) cessationOfOperation(5)

(2) 標準拡張領域(extensions)

authorityKeyIdentifier(クリティカルフラグ = FALSE)	
authorityKeyIdentifier	失効リスト発行者の公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
cRLNumber(クリティカルフラグ = FALSE)	
cRLNumber	失効リストの番号 型:INTEGER 値:ユニークな整数
issuingDistributionPoint (クリティカルフラグ = TRUE)	
issuingDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型:PrintableString 値:JP
organizationName	CRL 配布点の組織名 組織名の値 型:UTF8String 値:LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA U8
onlyContainsCACerts	CA 証明書に対する失効のみかを示すフラグ 型:BOOLEAN 値:TRUE

4. 組織 CA R2

組織 CA R2 から発行される職責証明書、利用者証明書、相互認証証明書、自己署名証明書、リンク証明書及び失効リスト(CRL/ARL)プロファイルを示す。

4.1. 証明書プロファイル

地方公共団体組織認証基盤において運用される、組織 CA R2 から発行される証明書プロファイルを示す。

4.1.1. 職責証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数) 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity notBefore notAfter	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName organizationName organizationalUnitName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI2 電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2

subject	
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名 組織名の値 型:UTF8String 値:Local Governments
localityName	電子証明書所有者の地域名 地域名の値 型:UTF8String 値:都道府県名(英語)
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:地方公共団体名(英語)
organizationalUnitName	電子証明書所有者の組織単位名(*5) 組織単位名の値 型:UTF8String 値:所属部門名(英語)
commonName	電子証明書所有者の固有名称 固有名称の値 型:UTF8String 値:役職名等(英語)
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数) RSAEncryption
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(*5) 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。

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:110000000 (digitalSignature、nonRepudiation)
certificatePolicies (クリティカルフラグ = TRUE)	
policyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 1 21
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型:OID 値:1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ(URI) 型:IA5String 値:https://www.lgpki.go.jp
subjectAltName (クリティカルフラグ = FALSE)	
subjectAltName	電子証明書所有者の別名に関する情報
directoryName	所有者別名
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名 組織名の値 型:UTF8String 値:Local Governments の日本語表記
LocalityName	電子証明書所有者の地域名 地域名の値 型:UTF8String 値:都道府県域名(日本語表記)
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:地方公共団体名(日本語表記)
organizationalUnitName	電子証明書所有者の組織単位名(*6) 組織単位名の値 型:UTF8String 値:所属部門名(日本語表記)
commonName	電子証明書所有者の固有名称 固有名称の値 型:UTF8String 値:役職名等(日本語表記)

(*6) 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。

cRLDistributionPoints（クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
OrganizationName	CRL 配布点の組織名 組織名の値 型：UTF8String 値：LGPKI2
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Organization CA R2
commonName	CRL 配布点の固有名 固有名の値 型：UTF8String 値：CRL<n>(*7)

(*7) エントリ数が一定量増えるたびに、 CRL1,CRL2,CRL3,…,CRL<n>と n の値も増える。

4.1.2. 利用者証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数) 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity notBefore notAfter	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName organizationName organizationalUnitName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI2 電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2

Subject	
countryName	電子証明書所有者の国名 国名の値 型：PrintableString 値：JP
organizationName	電子証明書所有者の組織名 組織名の値 型：UTF8String 値：Local Governments
localityName	電子証明書所有者の地域名 地域名の値 型：UTF8String 値：都道府県名（英語）
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型：UTF8String 値：地方公共団体名（英語）
organizationalUnitName	電子証明書所有者の組織単位名(*8) 組織単位名の値 型：UTF8String 値：申請者所属部門名（英語）
commonName	電子証明書所有者の固有名称 固有名称の値 型：UTF8String 値：役職名等（英語）
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）
algorithm	暗号アルゴリズムのオブジェクト ID 型：OID 値：1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型：NULL 値：なし
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値

(*8) 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。

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:10100000 (digitalSignature、keyEncipherment)
extendedKeyUsage (クリティカルフラグ = FALSE)	
KeyPurposeId	鍵の使用目的(拡張) 型:OID 値:1 3 6 1 5 5 7 3 2(clientAuth)
certificatePolicies (クリティカルフラグ = FALSE)	
policyInformation policyIdentifier policyQualifiers policyQualifierID qualifier	ポリシに関する情報 ポリシのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 7 21 ポリシ修飾子 ポリシ修飾子のオブジェクト ID 型:OID 値:1 3 6 1 5 5 7 2 1 CPS へのポインタ(URI) 型:IA5String 値:https://www.lgpki.go.jp
subjectAltName (クリティカルフラグ = FALSE)	
subjectAltName directoryName countryName organizationName LocalityName organizationalUnitName organizationalUnitName commonName	電子証明書所有者の別名に関する情報 所有者別名 電子証明書所有者の国名 国名の値 型:PrintableString 値:JP 電子証明書所有者の組織名 組織名の値 型:UTF8String 値:Local Governments の日本語表記 電子証明書所有者の地域名 地域名の値 型:UTF8String 値:都道府県域名(日本語表記) 電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:地方公共団体名(日本語表記) 電子証明書所有者の組織単位名(*9) 組織単位名の値 型:UTF8String 値:所属部門名(日本語表記) 電子証明書所有者の固有名称 固有名称の値 型:UTF8String 値:役職名等(日本語表記)

(*9) 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。

issureAltName （クリティカルフラグ = FALSE）	
issureAltName	電子証明書発行者の別名に関する情報
directoryName	発行者別名
countryName	電子証明書発行者の国名 国名の値 型：PrintableString 値：JP
organizationName	電子証明書発行者の組織名（地方公共団体組織認証基盤） 組織名の値 型：UTF8String 値：地方公共団体組織認証基盤2
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型：UTF8String 値：組織認証局　R2
cRLDistributionPoints （クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
directoryName	CRL 配布点のディレクトリ名
countryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
organizationName	CRL 配布点の組織名 組織名の値 型：UTF8String 値：LGPKI2
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Organization CA R2
commonName	CRL 配布点の固有名 固有名の値 型：UTF8String 値：CRL<n>(*10)

(*10) エントリ数が一定量増えるたびに、 CRL1,CRL2,CRL3,…,CRL<n>と n の値も増える。

4.1.3. 相互認証証明書 (組織 CA R2 → 政府認証基盤ブリッジ CA)

(1) 証明書基本領域(Basic)

Version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
SerialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier (公開鍵暗号とハッシュ関数) algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
Validity	
validity notBefore notAfter 	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
Issuer	
countryName organizationName organizationalUnitName 	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI2 電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2
Subject	
countryName organizationName organizationalUnitName 	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP 電子証明書所有者の組織名(政府認証基盤) 組織名の値 型:UTF8String 値:Japanese Government 電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:BridgeCA

SubjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）
algorithm	暗号アルゴリズムのオブジェクト ID 型：OID 値：1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型：NULL 値：なし
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier（クリティカルフラグ = FALSE）	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子 SHA-1 160bit 型：OCTET STRING 値：ユニークなバイト列
subjectKeyIdentifier（クリティカルフラグ = FALSE）	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型：OCTET STRING 値：ユニークなバイト列
keyUsage（クリティカルフラグ = TRUE）	
keyUsage	鍵の使用目的 型：BitString 値：000001100(keyCertSign、cRLSign)
certificatePolicies（クリティカルフラグ = TRUE）	
policyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型：OID 値：1 2 392 200110 10 8 5 1 1 21
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型：OID 値：1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ(URI) 型：IA5String 値：https://www.lgpki.go.jp
policyIdentifier	ポリシのオブジェクト ID 型：OID 値：1 2 392 200110 10 8 5 1 7 21
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型：OID 値：1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ(URI) 型：IA5String 値：https://www.lgpki.go.jp
policyMappings（クリティカルフラグ = TRUE）	
issuerDomainPolicy	発行者のドメイン・ポリシ OID 型：OID 値：1 2 392 200110 10 8 5 1 1 21
SubjectDomainPolicy	相互認証先 CA のドメイン・ポリシ OID 型：OID 値：0 2 440 100145 8 1 1 1 110

issuerDomainPolicy	発行者のドメイン・ポリシ OID 型：OID 値：1 2 392 200110 10 8 5 1 7 21
SubjectDomainPolicy	相互認証先 CA のドメイン・ポリシ OID 型：OID 値：0 2 440 100145 8 1 1 21 130
basicConstraints （クリティカルフラグ = TRUE）	
BasicConstraints cA	基本的制約 CA かどうかを示すフラグ 型：BOOLEAN 値：TRUE
policyConstraints （クリティカルフラグ = TRUE）	
policyConstraints requireExplicitPolicy inhibitPolicyMapping	ポリシ制約に関する情報 証明書ポリシの明示を要求 型：INTEGER 値：0 ポリシマッピングの制限 型：INTEGER 値：1
cRLDistributionPoints （クリティカルフラグ = FALSE）	
CRLDistributionPoints DistributionPoint FullName directoryName countryName organizationName organizationalUnitName commonName 	CRL 配布点に関する情報 CRL 配布点 CRL 配布点のディレクトリ名 CRL 配布点の国名 国名の値 型：PrintableString 値：JP CRL 配布点の組織名 組織名の値 型：UTF8String 値：LGPKI2 CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Organization CA R2 CRL 配布点の固有名 固有名の値 型：UTF8String 値：CRL<n>(*11)

(*11) エントリ数が一定量増えるたびに、 CRL1,CRL2,CRL3,…,CRL<n>と n の値も増える。

4.1.4. 自己署名証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI2
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2

Subject	
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI2
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(2) 証明書拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:000001100 (keyCertSign、cRLSign)
basicConstraints (クリティカルフラグ = TRUE)	
basicConstraints cA	基本的制約 CA かどうかを示すフラグ 型:BOOLEAN 値:TRUE

cRLDistributionPoints （クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
countryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
organizationName	CRL 配布点の組織名（地方公共団体組織認証基盤） 組織名の値 型：UTF8String 値：LGPKI2
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Organization CA R2
commonName	CRL 配布点の固有名 固有名の値 型：UTF8String 値：CRL<n>(*12)

(*12) エントリ数が一定量増えるたびに、 CRL1,CRL2,CRL3,…,CRL<n>と n の値も増える。

4.1.5. VA 証明書 (組織認証局 R2)

(3) 証明書基本領域(Basic)

Version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
Signature	
algorithmIdentifier	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 (sha256WithRSAEncryption)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
Validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
Issuer	
countryName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI2
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2
Subject	
証明書の要求ファイルの内容による	

subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）
algorithm	暗号アルゴリズムのオブジェクト ID 型：OID 値：1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型：NULL 値：なし
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値

(4) 証明書拡張領域 (extensions)

authorityKeyIdentifier（クリティカルフラグ = FALSE）	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子　SHA-1 160bit 型：OCTET STRING 値：ユニークなバイト列
subjectKeyIdentifier（クリティカルフラグ = FALSE）	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型：OCTET STRING 値：ユニークなバイト列
keyUsage（クリティカルフラグ = TRUE）	
keyUsage	鍵の使用目的 型：BitString 値：100000000(digitalSignature)
extendedKeyUsage（クリティカルフラグ = FALSE）	
KeyPurposeId	鍵の使用目的（拡張） 型：OID 値：1 3 6 1 5 5 7 3 9(OCSPSigning)
id-pkix-ocsp-nocheck（クリティカルフラグ = FALSE）	
id-pkix-ocsp-nocheck	CVS 証明書の検証不要を示す 型：OCTET STRING 値：null
certificatePolicies（クリティカルフラグ = TRUE）	
PolicyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型：OID 値：1 2 392 200110 10 8 5 1 9 21
cRLDistributionPoints（クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
directoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
OrganizationName	CRL 配布点の組織名 組織名の値 型：UTF8String 値：LGPKI2
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String

	値：Organization CA R2
commonName	CRL 配布点の固有名 固有名の値 型：UTF8String 値：CRL<n>(*12)

(*12) エントリ数が一定量増えるたびに、 CRL1,CRL2,CRL3,…,CRL<n>と n の値も増える。

4.1.6. リンク証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数) 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity notBefore notAfter	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName organizationName organizationalUnitName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI2 電子証明書発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2

Subject	
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名(地方公共団体組織認証基盤) 組織名の値 型:UTF8String 値:LGPKI2
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2
subjectPublicKeyInfo	
subjectPublicKeyInfo algorithmIdentifier algorithm parameters subjectPublicKey	電子証明書所有者の公開鍵に関する情報 暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数) 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1(RSAEncryption) 暗号アルゴリズムの引数 型:NULL 値:なし 公開鍵値 型:BIT STRING 値:公開鍵値

(3) 証明書拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:000001100 (keyCertSign、cRLSign)
certificatePolicies (クリティカルフラグ = FALSE)	
PolicyInformation PolicyIdentifier	ポリシに関する情報 ポリシのオブジェクト ID 型:OID 値:2 5 29 32 0 (AnyPolicy)
basicConstraints (クリティカルフラグ = TRUE)	
basicConstraints cA	基本的制約 CA かどうかを示すフラグ 型:BOOLEAN 値:TRUE

cRLDistributionPoints （クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
countryName	CRL 配布点の国名 国名の値 型：PrintableString 値：JP
organizationName	CRL 配布点の組織名（地方公共団体組織認証基盤） 組織名の値 型：UTF8String 値：LGPKI2
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型：UTF8String 値：Organization CA R2
commonName	CRL 配布点の固有名 固有名の値 型：UTF8String 値：CRL<n>(*13)

(*13) エントリ数が一定量増えるたびに、 CRL1,CRL2,CRL3,…,CRL<n>と n の値も増える。

4.2. 失効リストプロファイル

地方公共団体組織認証基盤において運用される、組織 CA R2 から発行される失効リスト(CRL/ARL)プロファイルを示す。

4.2.1. 完全 CRL プロファイル

(1) 基本領域(Basic)

version	
version	失効リストフォーマットのバージョン番号 型:INTEGER 値:1
signature	
algorithmIdentifier	失効リストへの署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
issuer	
countryName	失効リスト発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	失効リスト発行者の組織名 組織名の値 型:UTF8String 値:LGPKI2
organizationalUnitName	失効リスト発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2
thisUpdate	
thisUpdate	失効リストの更新日 型:UTC Time 値:yymmddhhmmssZ
nextUpdate	
nextUpdate	失効リストの次回更新日 型:UTC Time 値:yymmddhhmmssZ

revokedCertificates	
userCertificate	証明書シリアル番号 型：INTEGER 値：ユニークな整数
revocationDate	失効日 型：UTC Time 値：yymmddhhmmssZ
crlEntryExtensions	失効リストエントリ拡張領域
reasonCode （クリティカルフラグ = FALSE）	理由コード 型：ENUMERATED 値： keyCompromise(1) cACompromise(2) affiliationChanged(3) superseded(4) cessationOfOperation(5)

(2) 標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	**失効リスト発行者の公開鍵の識別子　SHA-1 160bit** **型:OCTET STRING** **値:ユニークなバイト列**
cRLNumber(クリティカルフラグ = FALSE)	
cRLNumber	**失効リストの番号** **型:INTEGER** **値:ユニークな整数**

4.2.2. 区分 CRL プロファイル

(1) 基本領域(Basic)

version	
version	失効リストフォーマットのバージョン番号 型:INTEGER 値:1
signature	
algorithmIdentifier	失効リストへの署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
issuer	
countryName	失効リスト発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	失効リスト発行者の組織名 組織名の値 型:UTF8String 値:LGPKI2
organizationalUnitName	失効リスト発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2
thisUpdate	
thisUpdate	失効リストの更新日 型:UTC Time 値:yymmddhhmmssZ
nextUpdate	
nextUpdate	失効リストの次回更新日 型:UTC Time 値:yymmddhhmmssZ

revokedCertificates	
userCertificate	証明書シリアル番号 型：INTEGER 値：ユニークな整数
revocationDate	失効日 型：UTC Time 値：yymmddhhmmssZ
crlEntryExtensions	失効リストエントリ拡張領域
reasonCode （クリティカルフラグ = FALSE）	理由コード 型：ENUMERATED 値： keyCompromise(1) cACompromise(2) affiliationChanged(3) superseded(4) cessationOfOperation(5)

(2) 標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	失効リスト発行者の公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
cRLNumber(クリティカルフラグ = FALSE)	
cRLNumber	失効リストの番号 型:INTEGER 値:ユニークな整数
issuingDistributionPoint (クリティカルフラグ = TRUE)	
issuingDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型:PrintableString 値:JP
OrganizationName	CRL 配布点の組織名 組織名の値 型:UTF8String 値:LGPKI2
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2
commonName	CRL 配布点の固有名 固有名名の値 型:UTF8String 値:CRL<n>(*14)
onlyContainsUserCerts	ユーザ証明書に対する失効のみかを示すフラグ 型:BOOLEAN 値:TRUE

(*14) エントリ数が一定量増えるたびに、 CRL1,CRL2,CRL3,…,CRL<n>と n の値も増える。

4.2.3. ARL プロファイル

(1) 基本領域(Basic)

version	
version	失効リストフォーマットのバージョン番号 型:INTEGER 値:1
signature	
algorithmIdentifier (公開鍵暗号とハッシュ関数) algorithm parameters	失効リストへの署名に使用された暗号アルゴリズムの識別子 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
issuer	
countryName organizationName organizationalUnitName	失効リスト発行者の国名 国名の値 型:PrintableString 値:JP 失効リスト発行者の組織名 組織名の値 型:UTF8String 値:LGPKI2 失効リスト発行者の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2
thisUpdate	
thisUpdate	失効リストの更新日 型:UTC Time 値:yymmddhhmmssZ
nextUpdate	
nextUpdate	失効リストの次回更新日 型:UTC Time 値:yymmddhhmmssZ
revokedCertificates	
userCertificate revocationDate crlEntryExtensions reasonCode (クリティカルフラグ= FALSE)	証明書シリアル番号 型:INTEGER 値:ユニークな整数 失効日 型:UTC Time 値:yymmddhhmmssZ 失効リストエントリ拡張領域 理由コード 型:ENUMERATED 値: keyCompromise(1) cACompromise(2) affiliationChanged(3) superseded(4) cessationOfOperation(5)

(2) 標準拡張領域(extensions)

authorityKeyIdentifier(クリティカルフラグ = FALSE)	
authorityKeyIdentifier	失効リスト発行者の公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
cRLNumber(クリティカルフラグ = FALSE)	
cRLNumber	失効リストの番号 型:INTEGER 値:ユニークな整数
issuingDistributionPoint (クリティカルフラグ = TRUE)	
issuingDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
DirectoryName	CRL 配布点のディレクトリ名
CountryName	CRL 配布点の国名 国名の値 型:PrintableString 値:JP
organizationName	CRL 配布点の組織名 組織名の値 型:UTF8String 値:LGPKI2
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型:UTF8String 値:Organization CA R2
commonName	CRL 配布点の固有名 固有名名の値 型:UTF8String 値:CRL<n>(*15)
onlyContainsCACerts	CA 証明書に対する失効のみかを示すフラグ 型:BOOLEAN 値:TRUE

(*15) エントリ数が一定量増えるたびに、 CRL1,CRL2,CRL3,…,CRL<n>と n の値も増える。

5. アプリケーション CA R2 (PS)

アプリケーション CA R2 (PS)から発行される Web サーバ証明書、自己署名証明書及び失効リスト(CRL)プロファイルを示す。

5.1. 証明書プロファイル

地方公共団体組織認証基盤において運用される、アプリケーション CA R2 から発行される証明書プロファイルを示す。

5.1.1. Web サーバ証明書

(1)証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier (公開鍵暗号とハッシュ関数) algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity notBefore notAfter	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName organizationName commonName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP 電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:PrintableString 値:LGPKI 電子証明書発行者の一般名 一般名の値 型:PrintableString 値:Application CA R2

subject	
	申請内容の形式に従う
subjectPublicKeyInfo	
subjectPublicKeyInfo 　algorithmIdentifier 　　algorithm 　　parameters 　subjectPublicKey	電子証明書所有者の公開鍵に関する情報 暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数） 暗号アルゴリズムのオブジェクト ID 　型：OID 　値：1 2 840 113549 1 1 1(RSAEncryption) 暗号アルゴリズムの引数 　型：NULL 　値：なし 公開鍵値 　型：BIT STRING 　値：公開鍵値

(2)証明書拡張領域 (extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:101000000(digitalSignature、keyEncipherment)
extendedKeyUsage (クリティカルフラグ = FALSE)	
KeyPurposeId	鍵の使用目的(拡張) 型:OID 値:1 3 6 1 5 5 7 3 1(serverAuth)
subjectAltName (クリティカルフラグ = FALSE)	
dNSName	サーバの FQDN 型:IA5String 値:サーバの FQDN
certificatePolicies (クリティカルフラグ = FALSE)	
policyInformation policyIdentifier policyQualifiers policyQualifierID qualifier	ポリシに関する情報 ポリシのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 3 21 ポリシ修飾子 ポリシ修飾子のオブジェクト ID 型:OID 値:1 3 6 1 5 5 7 2 1 CPS へのポインタ(URI) 型:IA5String 値:http://lgpkir2.lgwan.jp/
cRLDistributionPoints (クリティカルフラグ = FALSE)	
cRLDistributionPoints distributionPoint fullName uniformResourceIdentifier uniformResourceIdentifier	CRL 配布点に関する情報 CRL 配布点 CRL 配布点の URL 型:IA5String 値:http://lgpkir2.lgwan.jp/CRL/AppCAR2Crl.crl CRL 配布点の URL 型:IA5String 値: ldap://ldapr2.lgwan.jp/CN=Application%20CA%20R2,O=LGPKI,C=JP?certificateRevocationList

5.1.2. 自己署名証明書

(1) 証明書基本領域(Basic)

version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier	電子証明書への署名に使用された暗号アルゴリズムの識別子 (公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 11
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName	電子証明書発行者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名(地方公共団体組織認証基盤) 組織名の値 型:PrintableString 値:LGPKI
commonName	電子証明書発行者の一般名 一般名の値 型:PrintableString 値:Application CA R2

subject	
countryName	電子証明書所有者の国名 国名の値 型:PrintableString 値:JP
organizationName	電子証明書所有者の組織名(地方公共団体組織認証基盤) 組織名の値 型:PrintableString 値:LGPKI
commonName	電子証明書所有者の一般名 一般名の値 型:PrintableString 値:Application CA R2
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数)
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1(RSAEncryption)
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者(地方公共団体)の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:000001100(keyCertSign、cRLSign)
basicConstraints (クリティカルフラグ = TRUE)	
basicConstraints	基本的制約
cA	CA かどうかを示すフラグ 型:BOOLEAN 値:TRUE

5.2. 失効リストプロファイル

地方公共団体組織認証基盤において運用される、アプリケーション CA　R2 から発行される失効リスト(CRL)プロファイルを示す。

5.2.1. CRL プロファイル

(1)基本領域(Basic)

version	
version	**失効リストフォーマットのバージョン番号** **型:INTEGER** **値:1**
signature	
algorithmIdentifier	**失効リストへの署名に使用された暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）**
algorithm	**暗号アルゴリズムのオブジェクト ID** **型:OID** **値:1 2 840 113549 1 1 11**
parameters	**暗号アルゴリズムの引数** **型:NULL** **値:なし**
issuer	
countryName	**失効リスト発行者の国名** **国名の値** **型:PrintableString** **値:JP**
organizationName	**失効リスト発行者の組織名** **組織名の値** **型:PrintableString** **値:LGPKI**
commonName	**失効リスト発行者の一般名** **一般名の値** **型:PrintableString** **値:Application CA R2**
thisUpdate	
thisUpdate	**失効リストの更新日** **型:UTC Time** **値:yymmddhhmmssZ**
nextUpdate	
nextUpdate	**失効リストの次回更新日** **型:UTC Time** **値:yymmddhhmmssZ**

revokedCertificates	
userCertificate	証明書シリアル番号 型:INTEGER 値:ユニークな整数
revocationDate	失効日 型:UTC Time 値:yymmddhhmmssZ
crlEntryExtensions	失効リストエントリ拡張領域
reasonCode (クリティカルフラグ = FALSE)	理由コード 型:ENUMERATED 値: keyCompromise(1) cACompromise(2) affiliationChanged(3) superseded(4) cessationOfOperation(5)

(2)標準拡張領域(extensions)

authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	失効リスト発行者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
cRLNumber(クリティカルフラグ = FALSE)	
cRLNumber	失効リストの番号 型:INTEGER 値:ユニークな整数

6. Security Communication RootCA2

セコムトラストシステムズ株式会社が運用する Security Communication RootCA2 から発行される下位 CA 証明書、OCSP サーバ証明書及び失効リスト(CRL)プロファイルについては、セコムパスポート for Web SR 認証局 証明書ポリシに示す。

https://repository.secomtrust.net/SC-Root2/

7. セコムパスポート for Web SR3.0 サービス

セコムトラストシステムズ株式会社が運用するセコムセコムパスポート for Web SR3.0 サービスから発行される Web サーバ証明書（OV 証明書）OCSP サーバ証明書及び失効リスト(CRL)プロファイルについては、セコムパスポート for Web SR 認証局 証明書ポリシに示す。

https://repo1.secomtrust.net/spcpp/pfw/pfwsr3ca/

セコムパスポート for Web SR3.0 サービスは、Security Communication RootCA2 との階層構造を取る。

8. セコムパスポート for PublicID サービス

セコムトラストシステムズ株式会社が運用するセコムパスポート for PublicID サービスから発行されるメール用証明書、コードサイニング証明書、OCSP サーバ証明書と中間 CA 証明書及び失効リスト(CRL)プロファイルについては、セコムパスポート for Member 2.0 PUB 証明書ポリシに示す。

https://repo1.secomtrust.net/spcpp/pfm20pub/

セコムパスポート for PublicID サービスは、Security Communication RootCA2 との階層構造を取る。