

LGPKI プロファイル設計書

第 1 . 4 版

平成 20 年 10 月 22 日

総合行政ネットワーク運営協議会

1.	ブリッジ CA (UTF8).....	1
1.1.	証明書プロファイル.....	1
1.1.1.	相互認証証明書 (ブリッジ CA (UTF8) 組織 CA).....	1
1.1.2.	相互認証証明書 (ブリッジ CA (UTF8) 政府認証基盤ブリッジ CA).....	5
1.1.3.	VA 証明書.....	9
1.1.4.	自己署名証明書.....	11
1.1.5.	リンク証明書.....	14
1.2.	失効リストプロファイル.....	17
1.2.1.	CRL プロファイル.....	17
1.2.2.	ARL プロファイル.....	20
2.	組織 CA.....	22
2.1.	証明書プロファイル.....	22
2.1.1.	職責証明書.....	23
2.1.2.	利用者証明書.....	27
2.2.	失効リストプロファイル.....	31
2.2.1.	CRL プロファイル.....	31
2.2.2.	ARL プロファイル.....	34
3.	アプリケーション CA (PS).....	36
3.1.	証明書プロファイル.....	36
3.1.1.	Web サーバ証明書.....	36
3.1.2.	メール用証明書.....	39
3.1.3.	コードサイニング証明書.....	42
3.1.4.	アプリケーション基盤用サーバ証明書.....	45
3.1.5.	自己署名証明書.....	48
3.1.6.	リンク証明書.....	51
3.2.	失効リストプロファイル.....	54
3.2.1.	CRL プロファイル.....	54
3.2.2.	ARL プロファイル.....	57

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。

1. 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。

1.1. 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。

1.1.1. 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	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 5(Sha-1WithRSAEncryption)
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

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	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	ポリシーに関する情報
policyIdentifier	ポリシーのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 1 1
policyQualifiers	ポリシー修飾子
policyQualifierID	ポリシー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 へのポイント(URL) 型:IA5String 値:http://www.lgpkj.jp
policyIdentifier	ポリシーのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 7 1
policyQualifiers	ポリシー修飾子
policyQualifierID	ポリシー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 へのポイント(URL) 型:IA5String 値:http://www.lgpkj.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

1.1.2. 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	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 5(Sha-1WithRSAEncryption)
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(政府認証基盤) 組織名の値 型: UTF8String 値: Japanese Government
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: 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
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	ポリシーに関する情報
policyIdentifier	ポリシーのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 1 1
policyQualifiers	ポリシー修飾子
policyQualifierID	ポリシー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	ポリシーのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 7 1
policyQualifiers	ポリシー修飾子
policyQualifierID	ポリシー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 = FALSE)	
issuerDomainPolicy	発行者のドメイン・ポリシー OID 型:OID 値:1 2 392 200110 10 8 5 1 1 1

SubjectDomainPolicy	相互認証先 CA のドメイン・ポリシー OID 型:OID 値:0 2 440 100145 8 1 1 1 10
issuerDomainPolicy	発行者のドメイン・ポリシー OID 型:OID 値:1 2 392 200110 10 8 5 1 7 1
SubjectDomainPolicy	相互認証先 CA のドメイン・ポリシー OID 型:OID 値:0 2 440 100145 8 3 1 21 30

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	ポリシー制約に関する情報 証明書ポリシーの明示を要求 型: INTEGER 値: 0 ポリシーマッピングの制限 型: INTEGER 値: 1
cRLDistributionPoints (クリティカルフラグ = FALSE)	
CRLDistributionPoints DistributionPoint FullName directoryName countryName organizationName organizationalUnitName	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: Bridge CA U8

1.1.3. 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	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 5(Sha-1WithRSAEncryption)
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: yymddhmmssZ
notAfter	終了日時 型: UTC Time 値: yymddhmmssZ
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	
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:10000000(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	ポリシーに関する情報
policyIdentifier	ポリシーのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 3 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

1.1.4. 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) sha-1WithRSAEncryption
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 5
parameters	暗号アルゴリズムの引数 型: NULL 値: なし
validity	
validity notBefore	電子証明書の有効期間 開始日時 型: UTC Time 値: yymddhhmmssZ
notAfter	終了日時 型: UTC Time 値: yymddhhmmssZ
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

1.1.5. 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	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) sha-1WithRSAEncryption
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 5
parameters	暗号アルゴリズムの引数 型: NULL 値: なし
validity	
validity notBefore	電子証明書の有効期間 開始日時 型: UTC Time 値: yymddhhmmssZ
notAfter	終了日時 型: UTC Time 値: yymddhhmmssZ
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)
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)
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

1.2. 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。

1.2.1. 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 5 (sha-1WithRSAEncryption)
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 distributionPoint fullName DirectoryName CountryName OrganizationName organizationalUnitName onlyContainsUserCerts	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:Bridge CA U8 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

1.2.2. 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	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 5(sha-1WithRSAEncryption)
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: yymddhhmmssZ
nextUpdate	
nextUpdate	失効リストの次回更新日 型: UTC Time 値: yymddhhmmssZ
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: yymddhhmmssZ
crlEntryExtensions reasonCode (クリティカルフラグ= FALSE)	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

2. 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、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、組織 CA から発行される証明書プロファイルを示す。

2.1.1. 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	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) sha-1WithRSAEncryption
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 5
parameters	暗号アルゴリズムの引数 型: NULL 値: なし
validity	
validity notBefore	電子証明書の有効期間 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
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 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:11000000 (digitalSignature, nonRepudiation)
certificatePolicies (クリティカルフラグ = TRUE)	
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:1 2 392 200110 10 8 5 1 1 1
policyQualifiers policyQualifierID	ポリシー修飾子 ポリシー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.lgpkj.jp
subjectAltName (クリティカルフラグ = FALSE)	
subjectAltName directoryName countryName	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
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できる。

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

2.1.2. 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	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 5(sha-1WithRSAEncryption)
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: yymddhmmssZ
notAfter	終了日時 型: UTC Time 値: yymddhmmssZ
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(*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 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	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:1 2 392 200110 10 8 5 1 7 1
policyQualifiers policyQualifierID	ポリシー修飾子 ポリシー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.lgpkj.jp
subjectAltName (クリティカルフラグ = FALSE)	
subjectAltName directoryName countryName	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
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できる。

issueAltName (クリティカルフラグ = FALSE)	
issueAltName	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

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、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。

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 5 (sha-1WithRSAEncryption)
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: 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

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	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 5(sha-1WithRSAEncryption)
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: Organization CA U8
thisUpdate	
thisUpdate	失効リストの更新日 型: UTC Time 値: yymddhhmmssZ
nextUpdate	
nextUpdate	失効リストの次回更新日 型: UTC Time 値: yymddhhmmssZ
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: yymddhhmmssZ
crlEntryExtensions reasonCode (クリティカルフラグ= FALSE)	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

3. アプリケーション CA (PS)

アプリケーション CA (PS)から発行される相互認証証明書、Web サーバ証明書、メール用証明書、コードサイニング証明書、アプリケーション基盤用サーバ証明書、自己署名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、アプリケーション CA から発行される証明書プロファイルを示す。

3.1.1. 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	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(Sha-1WithRSAEncryption) 型: OID 値: 1 2 840 113549 1 1 5
parameters	暗号アルゴリズムの引数 型: NULL 値: なし
validity	
validity notBefore	電子証明書の有効期間 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
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2

subject	
	申請内容の形式に従う
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: 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 1(serverAuth)
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: 1 2 392 200110 10 8 5 1 3 1
policyQualifiers policyQualifierID	ポリシー修飾子 ポリシー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.lgpkj.jp
cRLDistributionPoints (クリティカルフラグ = FALSE)	
cRLDistributionPoints distributionPoint fullName directoryName countryName	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
organizationName	CRL 配布点の組織名 組織名の値 型: PrintableString 値: LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2
uniformResourceIdentifier	CRL 配布点の URL (インターネット側) 型: IA5String 値: http://www.lgpkj.jp/Information/CRL/AppCACrI.crl
uniformResourceIdentifier	CRL 配布点の URL (LGWAN 側) 型: IA5String 値: http://www-asplgwan.jp/Information/CRL/AppCACrI.crl

3.1.2. メール用証明書

(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(sha-1WithRSAEncryption) 型: OID 値: 1 2 840 113549 1 1 5
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
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2

subject	
	申請内容の形式に従う
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(RSAEncryption) 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: 10000000 (digitalSignature)
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: 1 2 392 200110 10 8 5 1 4 1
policyQualifiers policyQualifierID	ポリシー修飾子 ポリシー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.lgpk.jp
cRLDistributionPoints (クリティカルフラグ = FALSE)	
cRLDistributionPoints distributionPoint fullName directoryName countryName	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
organizationName	CRL 配布点の組織名 組織名の値 型: PrintableString 値: LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2
uniformResourceIdentifier	CRL 配布点の URL (インターネット側) 型: IA5String 値: http://www.lgpk.jp/Information/CRL/AppCACrl.crl
uniformResourceIdentifier	CRL 配布点の URL (LGWAN 側) 型: IA5String 値: http://www-asp.lgwan.jp/Information/CRL/AppCACrl.crl

3.1.3. コードサイニング証明書

(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(Sha-1WithRSAEncryption) 型: OID 値: 1 2 840 113549 1 1 5
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
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2

subject	
	申請内容の形式に従う
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: 10000000(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 3(CodeSigning)
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: 1 2 392 200110 10 8 5 1 5 1
policyQualifiers policyQualifierID	ポリシー修飾子 ポリシー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.lgpk.jp
cRLDistributionPoints (クリティカルフラグ = FALSE)	
cRLDistributionPoints distributionPoint fullName directoryName countryName	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
organizationName	CRL 配布点の組織名 組織名の値 型: PrintableString 値: LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2
uniformResourceIdentifier	CRL 配布点の URL (インターネット側) 型: IA5String 値: http://www.lgpk.jp/Information/CRL/AppCACrI.crl
uniformResourceIdentifier	CRL 配布点の URL (LGWAN 側) 型: IA5String 値: http://www-asp.lgwan.jp/Information/CRL/AppCACrI.crl

3.1.4. アプリケーション基盤用サーバ証明書

(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	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(Sha-1WithRSAEncryption) 型: OID 値: 1 2 840 113549 1 1 5
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: yymddhhmmssZ
notAfter	終了日時 型: UTC Time 値: yymddhhmmssZ
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
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2
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
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:11110000(digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment)
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) 型:OID 値:1 3 6 1 5 5 7 3 2(clientAuth) 型:OID 値:1 3 6 1 5 5 7 3 8(timeStamping)
certificatePolicies (クリティカルフラグ = FALSE)	
policyInformation	ポリシーに関する情報
policyIdentifier	ポリシーのオブジェクト ID 型:OID 値:1 2 392 200110 10 8 5 1 6 1
policyQualifiers	ポリシー修飾子
policyQualifierID	ポリシー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.lgpkj.jp

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: PrintableString 値: LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2
uniformResourceIdentifier	CRL 配布点の URL (インターネット側) 型: IA5String 値: http://www.lgpkj.jp/Information/CRL/AppCACrI.crl
uniformResourceIdentifier	CRL 配布点の URL (LGWAN 側) 型: IA5String 値: http://www-asp.lgwan.jp/Information/CRL/AppCACrI.crl

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 5(Sha-1WithRSAEncryption)
parameters	暗号アルゴリズムの引数 型: NULL 値: なし
validity	
validity notBefore	電子証明書の有効期間 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
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2

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
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2
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)
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:PrintableString 値:LGPKI CRL 配布点の組織単位名 組織単位名の値 型:PrintableString 値:Application CA G2

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 5(Sha-1WithRSAEncryption)
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
organizationalUnitName	電子証明書発行者の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2

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
organizationalUnitName	電子証明書所有者の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2
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)
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:PrintableString 値:LGPKI CRL 配布点の組織単位名 組織単位名の値 型:PrintableString 値:Application CA G2

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、アプリケーション 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	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 5(sha-1WithRSAEncryption)
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
organizationalUnitName	失効リスト発行者の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2
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: yymddhhmmssZ
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 = FALSE)	
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:PrintableString 値:LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型:PrintableString 値:Application CA G2
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	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 5 (sha-1WithRSAEncryption)
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
organizationalUnitName	失効リスト発行者の組織単位名 組織単位名の値 型: PrintableString 値: Application CA G2
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: yymddhhmmssZ
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:PrintableString 値:LGPKI
organizationalUnitName	CRL 配布点の組織単位名 組織単位名の値 型:PrintableString 値:Application CA G2
onlyContainsCACerts	CA 証明書に対する失効のみかを示すフラグ 型:BOOLEAN 値:TRUE