<table>
<tr><th>Page</th><th>新文書</th><th>旧文書</th><th>備考</th><th>差分</th></tr>
<tr><td></td><td>第 2.5 版</td><td>第 2.4 版</td><td></td><td>変更</td></tr>
<tr><td></td><td>令和 7 年 4 月 17 日</td><td>令和 6 年 11 月 16 日</td><td></td><td>変更</td></tr>
<tr><td></td><td></td><td></td><td></td><td>（略）</td></tr>
<tr><td>新: ii
旧: ii</td><td>
<table>
<tr><th>版数</th><th>年月日</th><th>主な改訂内容</th></tr>
<tr><td>1.0</td><td>平成 23 年 11 月 1 日</td><td>新規作成</td></tr>
<tr><td colspan="3">（略）</td></tr>
<tr><td>2.3</td><td>令和４年３月８日</td><td>コードサイニング証明書 Root 認証局変更に伴う改訂</td></tr>
<tr><td>2.4</td><td>令和６年１１月１６日</td><td>コードサイニング証明書の廃止に伴う改訂
文書等署名用職責証明書の追加に伴う改訂</td></tr>
<tr><td>2.5</td><td>令和７年４月 16 日</td><td>LGPKI アプリケーション認証局 R3 の運用開始に伴う改訂</td></tr>
</table>
</td><td>
<table>
<tr><th>版数</th><th>年月日</th><th>主な改訂内容</th></tr>
<tr><td>1.0</td><td>平成 23 年 11 月 1 日</td><td>新規作成</td></tr>
<tr><td colspan="3">（略）</td></tr>
<tr><td>2.3</td><td>令和４年３月８日</td><td>コードサイニング証明書 Root 認証局変更に伴う改訂</td></tr>
<tr><td>2.4</td><td>令和６年１１月１６日</td><td>コードサイニング証明書の廃止に伴う改訂
文書等署名用職責証明書の追加に伴う改訂</td></tr>
</table>
</td><td></td><td>変更</td></tr>
<tr><td></td><td></td><td></td><td></td><td>（略）</td></tr>
<tr><td>新:51</td><td>5.アプリケーション CA R3 (PS)
アプリケーション CA R3 (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 R3 から発行される証明書プロファイルを示す。</td><td></td><td></td><td>追加</td></tr>
<tr><td></td><td></td><td></td><td></td><td>（略）</td></tr>
<tr><td>新:51</td><td>1.1.1. Web サーバ証明書

(1)証明書基本領域(Basic)
<table>
<tr><th colspan="2">version</th></tr>
<tr><td>version</td><td>電子証明書フォーマットのバージョン番号</td></tr>
</table>
</td><td></td><td></td><td>追加</td></tr>
</table>

Page	新文書		旧文書	備考	差分
		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 R3			

<table>
<tr><th>Page</th><th>新文書</th><th>旧文書</th><th>備考</th><th>差分</th></tr>
<tr><td></td><td></td><td></td><td></td><td>（略）</td></tr>
<tr><td>新:53</td><td>(2)証明書拡張領域（extensions）

<table>
<tr><td colspan="2">authorityKeyIdentifier（クリティカルフラグ = FALSE）</td></tr>
<tr><td>authorityKeyIdentifier
keyIdentifier</td><td>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</td></tr>
<tr><td colspan="2">subjectKeyIdentifier（クリティカルフラグ = FALSE）</td></tr>
<tr><td>subjectKeyIdentifier</td><td>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</td></tr>
<tr><td colspan="2">keyUsage（クリティカルフラグ = TRUE）</td></tr>
<tr><td>keyUsage</td><td>鍵の使用目的
型:BitString
値 : 101000000(digitalSignature 、keyEncipherment)</td></tr>
<tr><td colspan="2">extendedKeyUsage（クリティカルフラグ = FALSE）</td></tr>
<tr><td>KeyPurposeId</td><td>鍵の使用目的(拡張)
型:OID
値:1 3 6 1 5 5 7 3 1(serverAuth)</td></tr>
<tr><td colspan="2">subjectAltName（クリティカルフラグ = FALSE）</td></tr>
<tr><td>dNSName</td><td>サーバの FQDN
型:IA5String
値:サーバの FQDN</td></tr>
<tr><td colspan="2">certificatePolicies（クリティカルフラグ = FALSE）</td></tr>
<tr><td>policyInformation
policyIdentifier

policyQualifiers
policyQualifierID

qualifier</td><td>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 31
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/</td></tr>
</table></td><td></td><td></td><td>追加</td></tr>
</table>

<table>
<tr><th>Page</th><th>新文書</th><th>旧文書</th><th>備考</th><th>差分</th></tr>
<tr><td></td><td>
<table>
<tr><th colspan="2">cRLDistributionPoints（クリティカルフラグ = FALSE）</th></tr>
<tr><td>cRLDistributionPoints</td><td>CRL 配布点に関する情報</td></tr>
<tr><td>distributionPoint</td><td>CRL 配布点</td></tr>
<tr><td>fullName</td><td></td></tr>
<tr><td>uniformResourceI dentifier</td><td>CRL 配布点の URL

型：IA5String
値 ：
http://lgpkir2.lgwan.jp/CRL/AppCAR3Crl.crl</td></tr>
<tr><td>uniformResourceI dentifier</td><td>CRL 配布点の URL

型：IA5String
値：
ldap://ldapr2.lgwan.jp/CN=Application%20CA%20R3,O=LGPKI,C=JP?certificateRevocationList</td></tr>
</table>
</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td>（略）</td></tr>
<tr><td>新:54</td><td>
5.1.2 自己署名証明書

(3)証明書基本領域(Basic)

<table>
<tr><th colspan="2">version</th></tr>
<tr><td>version</td><td>電子証明書フォーマットのバージョン番号
型：INTEGER
値：2</td></tr>
<tr><th colspan="2">serialNumber</th></tr>
<tr><td>certificateSerialNumber</td><td>電子証明書のシリアル番号
型：INTEGER
値：ユニークな整数</td></tr>
<tr><th colspan="2">signature</th></tr>
<tr><td>algorithmIdentifier

algorithm

parameters</td><td>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</td></tr>
</table>
</td><td></td><td></td><td>追加</td></tr>
</table>

Page	新文書	旧文書	備考	差分
	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 R3			
				(略)
新:55 旧:55	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 R3			追加

Page	新文書	旧文書	備考	差分
	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			
				（略）
新:56	**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　R3から発行される失効リスト(CRL)プロファイルを示す。	地		追加
				（略）
新:56	**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			追加

Page	新文書	旧文書	備考	差分
	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 R3 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			
				(略)
新:57	(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			追加
新:58 旧:52	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			移動

Page	新文書	旧文書	備考	差分
	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、Security Communication RootCA 下位 CA 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、文書等署名用職責証明書、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/ https://repo1.secomtrust.net/root/docrsa/ 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。 ## 9. SECOM Document Signing RSA Root CA 2023 セコムトラストシステムズ株式会社が運用する SECOM Document Signing RSA Root CA 2023 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、SECOM Document Signing RSA Root CA 2023 下位 CA 証明書ポリシに示す。 https://repo1.secomtrust.net/root/docrsa/			