

Page	新文書	旧文書	備考	差分
				(略)
新:1 旧:1	第2.2版	第2.1版		変更
				(略)
新:1 旧:1	令和6年11月16日	令和4年3月8日		変更
				(略)
新:2 旧:2	2.2. LGPKI組織CA	2.2. 第三次LGPKI組織CA		変更
新:2 旧:2	2.3. 第五次LGPKI組織CAR2	2.3. 第四次LGPKI組織CAR2		変更
新:2 旧:2	2.4. 第五次LGPKIアプリケーションCAR2 (LGWAN 内部環境用)	2.4. 第四次LGPKIアプリケーションCAR2 (LGWAN 内部環境用)		変更
新:2 旧:2	2.5.1. 第五次LGPKI公開リポジトリ	2.5.1. 第四次LGPKI公開リポジトリ		変更
新:2	2.5.2. 第五次LGPKI統合リポジトリ	2.5.2. 第四次LGPKI統合リポジトリ		変更

Page	新文書	旧文書	備考	差分
旧:2				
新:2 旧:2	<u>2.6. 第五次 LGPKI 証明書検証サーバ</u>	<u>2.6. 第四次 LGPKI 証明書検証サーバ</u>		変更
新:2 旧:2	<u>2.7. Security Communication RootCA2</u>	<u>2.7. Security Communication RootCA2</u>		変更
旧:2		2.8. Security Communication RootCA3		削除
新:2 旧:2	<u>2.8. セコムパスポート for Web SR3.0 CA</u>	<u>2.9. セコムパスポート for Web SR3.0 CA</u>		変更
新:2 旧:2	<u>2.9. セコムパスポート for PublicID CA</u>	<u>2.10. セコムパスポート for PublicID CA</u>		変更
新:2	2.10. SECOM Document Signing RSA Root CA 2023			追加
				(略)
				(略)
新:4 旧:4	LGPKI は、LGPKI 組織 CA 及び第 五 次 LGPKI 組織 CA R2（以下「組織 CA 等」という。）を中心とした認証基盤である。	LGPKI は、 第三次 LGPKI 組織 CA 及び第 四 次 LGPKI 組織 CA R2（以下「組織 CA 等」という。）を中心とした認証基盤である。		変更

Page	新文書	旧文書	備考	差分
				(略)
新:4 旧:4	● LGPKI 組織 CA	● 第三次 LGPKI 組織 CA		削除
新:4 旧:4	● 第五次 LGPKI 組織 CA R2	● 第四次 LGPKI 組織 CA R2		変更
新:4 旧:4	● 第五次 LGPKI アプリケーション CA R2	● 第四次 LGPKI アプリケーション CA R2		変更
新:4 旧:4	● 第五次 LGPKI 公開リポジトリ	● 第四次 LGPKI 公開リポジトリ		変更
新:4 旧:4	● 第五次 LGPKI 統合リポジトリ	● 第四次 LGPKI 統合リポジトリ		変更
新:4 旧:4	● 第五次 LGPKI 証明書検証サーバ	● 第四次 LGPKI 証明書検証サーバ		変更
				(略)
新:4 旧:4	● SECOM Document Signing RSA Root CA 2023 (外部サービス)	● Security Communication RootCA3 (外部サービス)		変更

Page	新文書	旧文書	備考	差分
				(略)
新:7 旧:6	1.1. LGPKI 組織 CA	1.1. 第三次 LGPKI 組織 CA		削除
新:7 旧:6	LGPKI 組織 CA は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL/ARL）をリポジトリ等に格納する。	第三次 LGPKI 組織 CA は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL/ARL）をリポジトリ等に格納する。		削除
新:7 旧:7	LGPKI 組織 CA には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。	第三次 LGPKI 組織 CA には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。		削除
				(略)
新:7 旧:7	LGPKI 組織 CA は以下の機能を備える。	第三次 LGPKI 組織 CA は以下の機能を備える。		削除
				(略)
新:7 旧:7	<ul style="list-style-type: none"> 自己署名証明書の発行及び第五次 LGPKI 統合リポジトリへの格納 	<ul style="list-style-type: none"> 自己署名証明書の発行及び第四次 LGPKI 統合リポジトリへの格納 		変更
				(略)

Page	新文書	旧文書	備考	差分
新:7 旧:7	1.2. 第 五 次 LGPKI 組織 CAR2	1.2. 第 四 次 LGPKI 組織 CAR2		変更
新:7 旧:7	第 五 次 LGPKI 組織 CAR2 は他認証ドメインに属する CA（以下「他 CA」という。）の公開鍵を含む相互認証証明書の発行、失効、更新を行う。	第 四 次 LGPKI 組織 CAR2 は他認証ドメインに属する CA（以下「他 CA」という。）の公開鍵を含む相互認証証明書の発行、失効、更新を行う。		変更
新:7 旧:7	第 五 次 LGPKI 組織 CAR2 は第 五 次 LGPKI 組織 CAR2 が発行した相互認証証明書を含む相互認証証明書ペアと、失効情報をリポジトリ等の第 五 次 LGPKI 組織 CAR2 エントリに格納する。	第 四 次 LGPKI 組織 CAR2 は第 四 次 LGPKI 組織 CAR2 が発行した相互認証証明書を含む相互認証証明書ペアと、失効情報をリポジトリ等の第 四 次 LGPKI 組織 CAR2 エントリに格納する。		変更
新:7 旧:7	第 五 次 LGPKI 組織 CAR2 は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL/ARL）をリポジトリ等に格納する。	第 四 次 LGPKI 組織 CAR2 は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL/ARL）をリポジトリ等に格納する。		変更
新:7 旧:7	第 五 次 LGPKI 組織 CAR2 には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。また、相互認証証明書に含まれる公開鍵が確実にその CA の公開鍵であり、CA がこの公開鍵に一致する秘密鍵を持っていることを保証する。	第 四 次 LGPKI 組織 CAR2 には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。また、相互認証証明書に含まれる公開鍵が確実にその CA の公開鍵であり、CA がこの公開鍵に一致する秘密鍵を持っていることを保証する。		変更
				(略)

Page	新文書	旧文書	備考	差分
新:7 旧:7	第 五 次 LGPKI 組織 CAR2 は以下の機能を備える。	第 四 次 LGPKI 組織 CAR2 は以下の機能を備える。		変更
				(略)
新:8 旧:8	1.3. 第 五 次 LGPKI アプリケーション CA R2 (LGWAN 内部環境用)	1.3. 第 四 次 LGPKI アプリケーション CAR2 (LGWAN 内部環境用)		変更
				(略)
新:8 旧:8	第 五 次 LGPKI アプリケーション CA は証明書の発行、失効、更新を行う。また各種証明書と失効情報 (CRL) を第 五 次 LGPKI 統合リポジトリに格納する。	第 四 次 LGPKI アプリケーション CA は証明書の発行、失効、更新を行う。また各種証明書と失効情報 (CRL) を第 四 次 LGPKI 統合リポジトリに格納する。		変更
新:8 旧:8	第 五 次 LGPKI アプリケーション CA には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。	第 四 次 LGPKI アプリケーション CA には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。		変更
				(略)
新:8 旧:8	第 五 次 LGPKI アプリケーション CA は以下の機能を備える。	第 四 次 LGPKI アプリケーション CA は以下の機能を備える。		変更
				(略)

Page	新文書	旧文書	備考	差分
新:8 旧:8	<ul style="list-style-type: none"> 自己署名証明書の発行と第五次 LGPKI 統合リポジトリへの格納 	<ul style="list-style-type: none"> 自己署名証明書の発行と第四次 LGPKI 統合リポジトリへの格納 		変更
				(略)
新:8 旧:8	<ul style="list-style-type: none"> 自 CA が発行した証明書に関する失効要求の受け付け、失効情報の発行と第五次 LGPKI 統合リポジトリへの格納 	<ul style="list-style-type: none"> 自 CA が発行した証明書に関する失効要求の受け付け、失効情報の発行と第四次 LGPKI 統合リポジトリへの格納 		変更
				(略)
新:8 旧:8	1.3.1. 第 五 次 LGPKI 公開リポジトリ	1.3.1. 第 四 次 LGPKI 公開リポジトリ		変更
新:8 旧:8	第 五 次 LGPKI 公開リポジトリは、証明書の有効性検証に必要な各種証明書、CRL/ARL を格納する。また、LDAPv3(389/tcp)を備えており、各 PKI コンポーネントからの証明書、CRL/ARL の検索、取り出し、格納が行える。	第 四 次 LGPKI 公開リポジトリは、証明書の有効性検証に必要な各種証明書、CRL/ARL を格納する。また、LDAPv3(389/tcp)を備えており、各 PKI コンポーネントからの証明書、CRL/ARL の検索、取り出し、格納が行える。		変更
				(略)
新:8 旧:8	第 五 次 LGPKI 公開リポジトリは以下の機能を備える。	第 四 次 LGPKI 公開リポジトリは以下の機能を備える。		変更
				(略)

Page	新文書	旧文書	備考	差分
新:8 旧:8	● 第 五 次 LGPKI 組織 CA R2 の自己署名証明書の格納	● 第 四 次 LGPKI 組織 CA R2 の自己署名証明書の格納		変更
				(略)
新:9 旧:9	1.3.2. 第 五 次 LGPKI 統合リポジトリ	1.3.2. 第 四 次 LGPKI 統合リポジトリ		変更
新:9 旧:9	第 五 次 LGPKI 統合リポジトリは、証明書の有効性検証に必要な各種証明書、CRL/ARL を格納する。また、LDAPv3(389/tcp)を備えており、各 PKI コンポーネントからの証明書、CRL/ARL の検索、取り出し、格納が行える。	第 四 次 LGPKI 統合リポジトリは、証明書の有効性検証に必要な各種証明書、CRL/ARL を格納する。また、LDAPv3(389/tcp)を備えており、各 PKI コンポーネントからの証明書、CRL/ARL の検索、取り出し、格納が行える。		変更
				(略)
新:9 旧:9	第 五 次 LGPKI 統合リポジトリは以下の機能を備える。	第 四 次 LGPKI 統合リポジトリは以下の機能を備える。		変更
				(略)
新:9 旧:9	● LGPKI 組織 CA の自己署名証明書の格納	● 第三次 LGPKI 組織 CA の自己署名証明書の格納		削除
新:9	● 第 五 次 LGPKI 組織 CA R2 の自己署名証明書の格納	● 第 四 次 LGPKI 組織 CA R2 の自己署名証明書の格納		変更

Page	新文書	旧文書	備考	差分
旧:9	納			
新:9 旧:9	<ul style="list-style-type: none"> 第五次 LGPKI アプリケーション CAR2 の自己署名証明書の格納 	<ul style="list-style-type: none"> 第四次 LGPKI アプリケーション CAR2 の自己署名証明書の格納 		変更
				(略)
新:9 旧:9	1.4. 第 五 次 LGPKI 証明書検証サーバ	1.4. 第 四 次 LGPKI 証明書検証サーバ		変更
新:9 旧:9	第 五 次 LGPKI 証明書検証サーバは、検証要求者が指定した証明書の妥当性を検証し、その検証要求者に証明書の検証結果を返すサーバである。証明書認証パス構築と各証明書の有効性に関する検証も可能なプロトコルを使用する。	第 四 次 LGPKI 証明書検証サーバは、検証要求者が指定した証明書の妥当性を検証し、その検証要求者に証明書の検証結果を返すサーバである。証明書認証パス構築と各証明書の有効性に関する検証も可能なプロトコルを使用する。		変更
				(略)
新:9 旧:9	第 五 次 LGPKI 証明書検証サーバは相互運用に関する機能として以下を備える。	第 四 次 LGPKI 証明書検証サーバは相互運用に関する機能として以下を備える。		変更
				(略)
新:9 旧:9	<ul style="list-style-type: none"> 第五次 LGPKI 証明書検証サーバ自身の証明書の発行要求、発行された証明書の受け入れ 	<ul style="list-style-type: none"> 第四次 LGPKI 証明書検証サーバ自身の証明書の発行要求、発行された証明書の受け入れ 		変更

Page	新文書	旧文書	備考	差分
				(略)
新:10 旧:10	1.5. SECOM Document Signing RSA Root CA 2023	1.5. Security Communication RootCA3		変更
新:10 旧:10	SECOM Document Signing RSA Root CA 2023 はセコムトラストシステム株式会社が運用するパブリックな Root 認証局である。SECOM Document Signing RSA Root CA 2023 は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL）をセコム公開リポジトリに格納する。SECOM Document Signing RSA Root CA 2023 には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。	Security Communication RootCA3 はセコムトラストシステム株式会社が運用するパブリックな Root 認証局である。Security Communication RootCA3 は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL）をセコム公開リポジトリに格納する。Security Communication RootCA3 には RA が存在する。RA は証明書所有者の身元を保証し、証明書に含まれる公開鍵と一致する秘密鍵を確実に証明書所有者が持っていることを保証する。		変更
				(略)
新:10 旧:10	SECOM Document Signing RSA Root CA 2023 の備える機能については、「Security Communication RootCA 認証運用規定」及び「Security Communication RootCA 下位 CA 証明書ポリシー」を参照のこと。 (https://repository.secomtrust.net/root/docrsa/)	Security Communication RootCA3 の備える機能については、「Security Communication RootCA 認証運用規定」及び「Security Communication RootCA 下位 CA 証明書ポリシー」を参照のこと。 (https://repository.secomtrust.net/SC-Root3/)		変更
				(略)

Page	新文書	旧文書	備考	差分
新:10 旧:10	セコムパスポート for PublicID CA は Security Communication RootCA2 または SECOM Document Signing RSA Root CA 2023 からサイニングを受けたセコムトラストシステムズ株式会社が運用するパブリックなメール用証明書、文書等署名用職責証明書を発行するサービスである、セコムパスポート for PublicID CA は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL）をセコム公開リポジトリに格納する。	セコムパスポート for PublicID CA は Security Communication RootCA2 又は Security Communication RootCA3 からサイニングを受けたセコムトラストシステムズ株式会社が運用するパブリックなメール用証明書、コードサイニング証明書を発行するサービスである、セコムパスポート for PublicID CA は証明書の発行、失効、更新を行う。また各種証明書と失効情報（CRL）をセコム公開リポジトリに格納する。		変更
				(略)
新:10 旧:10	セコムパスポート for PublicID CA の備える機能については、「セコム電子認証基盤認証運用規程」及び「セコムパスポート for Member 2.0 PUB 証明書ポリシー」を参照のこと。	セコムパスポート for PublicID CA の備える機能については、「セコム電子認証基盤認証運用規程」及び「セコムパスポート for Member 2.0 PUB 証明書ポリシー」を参照のこと。 (https://repo1.secomtrust.net/spcpp/pfm20pub/)		削除
新:11	• https://repo1.secomtrust.net/spcpp/pfm20pub/			追加
新:11	• https://repo1.secomtrust.net/root/docrsa/			追加
				(略)
新:11 旧:11	Security Communication RootCA2 : https://repository.secomtrust.net/SC-Root2/	Security Communication RootCA2 : https://repository.secomtrust.net/SC-Root2/		追加

Page	新文書	旧文書	備考	差分
新:11 旧:11	SECOM Document Signing RSA Root CA 2023 : https://repo1.secomtrust.net/root/docrsa/	Security Communication RootCA3 : https://repository.secomtrust.net/SC-Root3/		変更
				(略)
新:11 旧:11	セコムパスポート for PublicID CA : https://repo1.secomtrust.net/spcpp/pfm20pub/	セコムパスポート for PublicID CA : https://repo1.secomtrust.net/spcpp/pfm20pub/		
新:11	https://repo1.secomtrust.net/root/docrsa/			追加
				(略)
新:11 旧:11	SECOM Document Signing RSA Root CA 2023 : https://repo1.secomtrust.net/root/docrsa/	Security Communication RootCA3 : https://repository.secomtrust.net/SC-Root3/		変更
				(略)
新:11 旧:11	セコムパスポート for PublicID CA : https://repo1.secomtrust.net/spcpp/pfm20pub/	セコムパスポート for PublicID CA : https://repo1.secomtrust.net/spcpp/pfm20pub/		
新:11	https://repo1.secomtrust.net/root/docrsa/			追加
				(略)
新:12	● OCSP レスポンダへの問い合わせ機能、第5次	● OCSP レスポンダへの問い合わせ機能、第4次 LGPKI 証明書検証サーバへの問い合わせ機能、もしくは証明		変更

Page	新文書	旧文書	備考	差分
旧:12	LGPKI 証明書検証サーバへの問い合わせ機能、もしくは証明書検証サーバ等と同等の証明書検証機能	書検証サーバ等と同等の証明書検証機能		
				(略)
新:13 旧:13	Security Communication RootCA2 : https://repository.secomtrust.net/SC-Root2/	Security Communication RootCA2 : https://repository.secomtrust.net/SC-Root2/		追加
新:13 旧:13	SECOM Document Signing RSA Root CA 2023 : https://repo1.secomtrust.net/root/docrsa/	Security Communication RootCA3 : https://repository.secomtrust.net/SC-Root3/		変更
				(略)
新:13 旧:13	セコムパスポート for PublicID CA : https://repo1.secomtrust.net/spcpp/pfm20pub/	セコムパスポート for PublicID CA : https://repo1.secomtrust.net/spcpp/pfm20pub/		追加
新:13	https://repo1.secomtrust.net/root/docrsa/			追加
				(略)
新:13 旧:13	表 2-1 に各認証情報と第 五 次 LGPKI 公開リポジトリへの格納・削除・更新の関係を示し、次節以降で格納形式等を記述する。	表 2-1 に各認証情報と第 四 次 LGPKI 公開リポジトリへの格納・削除・更新の関係を示し、次節以降で格納形式等を記述する。		変更
				(略)

Page	新文書				旧文書				備考	差分																																																																																													
新:13 旧:13	表 2-2 認証情報の第5次 LGPKI 公開リポジトリへの格納・削除・更新				表 2-2 認証情報の第4次 LGPKI 公開リポジトリへの格納・削除・更新					変更																																																																																													
新:13 旧:13	<table><tr><th colspan="2" rowspan="2"></th><th rowspan="2">LGPKI 組織 CA の処理</th><th rowspan="2">第5次 LGPKI 組織 CA R2 の処理</th></tr><tr></tr><tr><td rowspan="3">相互認証証明書</td><td>格納</td><td>—</td><td>○</td></tr><tr><td>削除</td><td>—</td><td>○</td></tr><tr><td>更新</td><td>—</td><td>○</td></tr><tr><td rowspan="3">エンドエンティティ 用証明書</td><td>格納</td><td>—</td><td>—</td></tr><tr><td>削除</td><td>—</td><td>—</td></tr><tr><td>更新</td><td>—</td><td>—</td></tr><tr><td rowspan="2">自己署名証明書</td><td>格納</td><td>—</td><td>○</td></tr><tr><td>削除</td><td>—</td><td>○</td></tr><tr><td rowspan="2">リンク証明書</td><td>格納</td><td>—</td><td>○</td></tr><tr><td>削除</td><td>—</td><td>○</td></tr><tr><td rowspan="2">失効情報</td><td>格納</td><td>—</td><td>○</td></tr><tr><td>削除</td><td>—</td><td>○</td></tr></table>						LGPKI 組織 CA の処理	第5次 LGPKI 組織 CA R2 の処理	相互認証証明書	格納	—	○	削除	—	○	更新	—	○	エンドエンティティ 用証明書	格納	—	—	削除	—	—	更新	—	—	自己署名証明書	格納	—	○	削除	—	○	リンク証明書	格納	—	○	削除	—	○	失効情報	格納	—	○	削除	—	○	<table><tr><th colspan="2" rowspan="2"></th><th rowspan="2">第3次 LGPKI 組織 CA の処理</th><th rowspan="2">第4次 LGPKI 組織 CA R2 の処理</th></tr><tr></tr><tr><td rowspan="3">相互認証証明書</td><td>格納</td><td>—</td><td>○</td></tr><tr><td>削除</td><td>—</td><td>○</td></tr><tr><td>更新</td><td>—</td><td>○</td></tr><tr><td rowspan="3">エンドエンティティ 用証明書</td><td>格納</td><td>—</td><td>—</td></tr><tr><td>削除</td><td>—</td><td>—</td></tr><tr><td>更新</td><td>—</td><td>—</td></tr><tr><td rowspan="2">自己署名証明書</td><td>格納</td><td>—</td><td>○</td></tr><tr><td>削除</td><td>—</td><td>○</td></tr><tr><td rowspan="2">リンク証明書</td><td>格納</td><td>—</td><td>○</td></tr><tr><td>削除</td><td>—</td><td>○</td></tr><tr><td rowspan="3">失効情報</td><td>格納</td><td>—</td><td>○</td></tr><tr><td>削除</td><td>—</td><td>○</td></tr><tr><td>更新</td><td>—</td><td>○</td></tr></table>						第3次 LGPKI 組織 CA の処理	第4次 LGPKI 組織 CA R2 の処理	相互認証証明書	格納	—	○	削除	—	○	更新	—	○	エンドエンティティ 用証明書	格納	—	—	削除	—	—	更新	—	—	自己署名証明書	格納	—	○	削除	—	○	リンク証明書	格納	—	○	削除	—	○	失効情報	格納	—	○	削除	—	○	更新	—	○		変更
		LGPKI 組織 CA の処理	第5次 LGPKI 組織 CA R2 の処理																																																																																																				
相互認証証明書	格納	—	○																																																																																																				
	削除	—	○																																																																																																				
	更新	—	○																																																																																																				
エンドエンティティ 用証明書	格納	—	—																																																																																																				
	削除	—	—																																																																																																				
	更新	—	—																																																																																																				
自己署名証明書	格納	—	○																																																																																																				
	削除	—	○																																																																																																				
リンク証明書	格納	—	○																																																																																																				
	削除	—	○																																																																																																				
失効情報	格納	—	○																																																																																																				
	削除	—	○																																																																																																				
		第3次 LGPKI 組織 CA の処理	第4次 LGPKI 組織 CA R2 の処理																																																																																																				
相互認証証明書	格納	—	○																																																																																																				
	削除	—	○																																																																																																				
	更新	—	○																																																																																																				
エンドエンティティ 用証明書	格納	—	—																																																																																																				
	削除	—	—																																																																																																				
	更新	—	—																																																																																																				
自己署名証明書	格納	—	○																																																																																																				
	削除	—	○																																																																																																				
リンク証明書	格納	—	○																																																																																																				
	削除	—	○																																																																																																				
失効情報	格納	—	○																																																																																																				
	削除	—	○																																																																																																				
	更新	—	○																																																																																																				

Page	新文書				旧文書				備考	差分																																																																																																						
		更新	－	○																																																																																																												
										(略)																																																																																																						
新:14 旧:14	表 2－2 に各認証情報と第 五 次 LGPKI 統合リポジトリへの格納・削除・更新の関係を 示し、次節以降で格納形式等を記述する。				表 2－2 に各認証情報と第 四 次 LGPKI 統合リポジトリへの格納・削除・更新の関係を 示し、次節以降で格納形式等を記述する。					変更																																																																																																						
										(略)																																																																																																						
新:14 旧:14	<table><tr><td colspan="2" rowspan="2"></td><td rowspan="2">組織 CA の 処理</td><td rowspan="2">第五次組織 CAR2 の処 理</td><td rowspan="2">第五次アプ リケーショ ン CAR2 の 処理</td></tr><tr></tr><tr><td rowspan="3">相互認証証明 書</td><td>格納</td><td>－</td><td>－</td><td>－</td></tr><tr><td>削除</td><td>－</td><td>－</td><td>－</td></tr><tr><td>更新</td><td>－</td><td>－</td><td>－</td></tr><tr><td rowspan="3">エンドエン ティティ用 証明書</td><td>格納</td><td>－</td><td>－</td><td>－</td></tr><tr><td>削除</td><td>－</td><td>－</td><td>－</td></tr><tr><td>更新</td><td>－</td><td>－</td><td>－</td></tr><tr><td rowspan="2">自己署名証明 書</td><td>格納</td><td>○</td><td>○</td><td>○</td></tr><tr><td>削除</td><td>○</td><td>○</td><td>○</td></tr></table>						組織 CA の 処理	第 五 次組織 CAR2 の処 理	第 五 次アプ リケーショ ン CAR2 の 処理	相互認証証明 書	格納	－	－	－	削除	－	－	－	更新	－	－	－	エンドエン ティティ用 証明書	格納	－	－	－	削除	－	－	－	更新	－	－	－	自己署名証明 書	格納	○	○	○	削除	○	○	○	<table><tr><td colspan="2" rowspan="2"></td><td rowspan="2">第三次組織 CA の処理</td><td rowspan="2">第四次組織 CAR2 の処 理</td><td rowspan="2">第四次アプ リケーショ ン CAR2 の 処理</td></tr><tr></tr><tr><td rowspan="3">相互認証証明 書</td><td>格納</td><td>－</td><td>－</td><td>－</td></tr><tr><td>削除</td><td>－</td><td>－</td><td>－</td></tr><tr><td>更新</td><td>－</td><td>－</td><td>－</td></tr><tr><td rowspan="3">エンドエン ティティ用証 明書</td><td>格納</td><td>－</td><td>－</td><td>－</td></tr><tr><td>削除</td><td>－</td><td>－</td><td>－</td></tr><tr><td>更新</td><td>－</td><td>－</td><td>－</td></tr><tr><td rowspan="2">自己署名証明 書</td><td>格納</td><td>○</td><td>○</td><td>○</td></tr><tr><td>削除</td><td>○</td><td>○</td><td>○</td></tr><tr><td rowspan="2">リンク証明書</td><td>格納</td><td>○</td><td>○</td><td>－</td></tr><tr><td>削除</td><td>○</td><td>○</td><td>－</td></tr><tr><td rowspan="3">失効情報</td><td>格納</td><td>○</td><td>○</td><td>○</td></tr><tr><td>削除</td><td>○</td><td>○</td><td>○</td></tr><tr><td>更新</td><td>○</td><td>○</td><td>○</td></tr></table>						第 三 次組織 CA の処理	第 四 次組織 CAR2 の処 理	第 四 次アプ リケーショ ン CAR2 の 処理	相互認証証明 書	格納	－	－	－	削除	－	－	－	更新	－	－	－	エンドエン ティティ用証 明書	格納	－	－	－	削除	－	－	－	更新	－	－	－	自己署名証明 書	格納	○	○	○	削除	○	○	○	リンク証明書	格納	○	○	－	削除	○	○	－	失効情報	格納	○	○	○	削除	○	○	○	更新	○	○	○		変更
		組織 CA の 処理	第 五 次組織 CAR2 の処 理	第 五 次アプ リケーショ ン CAR2 の 処理																																																																																																												
相互認証証明 書	格納	－	－	－																																																																																																												
	削除	－	－	－																																																																																																												
	更新	－	－	－																																																																																																												
エンドエン ティティ用 証明書	格納	－	－	－																																																																																																												
	削除	－	－	－																																																																																																												
	更新	－	－	－																																																																																																												
自己署名証明 書	格納	○	○	○																																																																																																												
	削除	○	○	○																																																																																																												
		第 三 次組織 CA の処理	第 四 次組織 CAR2 の処 理	第 四 次アプ リケーショ ン CAR2 の 処理																																																																																																												
相互認証証明 書	格納	－	－	－																																																																																																												
	削除	－	－	－																																																																																																												
	更新	－	－	－																																																																																																												
エンドエン ティティ用証 明書	格納	－	－	－																																																																																																												
	削除	－	－	－																																																																																																												
	更新	－	－	－																																																																																																												
自己署名証明 書	格納	○	○	○																																																																																																												
	削除	○	○	○																																																																																																												
リンク証明書	格納	○	○	－																																																																																																												
	削除	○	○	－																																																																																																												
失効情報	格納	○	○	○																																																																																																												
	削除	○	○	○																																																																																																												
	更新	○	○	○																																																																																																												

Page	新文書					旧文書	備考	差分
	リンク証明書	格納	○	○	—			
		削除	○	○	—			
	失効情報	格納	○	○	○			
		削除	○	○	○			
		更新	○	○	○			
								(略)
新:15 旧:15	ア) 第 五 次 LGPKI 組織 CAR2 の CA エントリへの格納					ア) 第 四 次 LGPKI 組織 CAR2 の CA エントリへの格納		変更
新:15 旧:15	第 五 次 LGPKI 組織 CAR2 が他 CA へ発行した、あるいは他 CA から発行された相互認証証明書のリポジトリ等への格納は、次の形式で行う。					第 四 次 LGPKI 組織 CAR2 が他 CA へ発行した、あるいは他 CA から発行された相互認証証明書のリポジトリ等への格納は、次の形式で行う。		変更
								(略)
新:15 旧:15	格納するエントリ	第 五 次 LGPKI 組織 CAR2 の CA のエントリ				格納するエントリ	第 四 次 LGPKI 組織 CAR2 の CA のエントリ	変更
	格納するエントリが持たなければならないオブジェクトクラス	PkiCA (joint-iso-itu-t(2) ds(5) objectClass(6) pkiCA(22))				格納するエントリが持たなければならないオブジェクトクラス	PkiCA (joint-iso-itu-t(2) ds(5) objectClass(6) pkiCA(22))	
						格納する属性名	crossCertificatePair 属性	
						属性値の型	CertificatePair	

Page	新文書			旧文書			備考	差分
	格納する属性名	crossCertificatePair 属性		格納するフィールド	Forward フィールド	他 CA が第4次 LGPKI 組織 CA の公開鍵に署名した相互認証証明書		
	属性値の型	CertificatePair			Reverse フィールド	第4次 LGPKI 組織 CA が他 CA の公開鍵に署名した相互認証証明書		
	格納するフィールド	Forward フィールド	他 CA が第5次 LGPKI 組織 CA の公開鍵に署名した相互認証証明書	複数 CA と相互認証した場合の属性値の扱い	相互認証した CA ごとに別の属性値として格納する			
		Reverse フィールド	第5次 LGPKI 組織 CA が他 CA の公開鍵に署名した相互認証証明書					
	複数 CA と相互認証した場合の属性値の扱い	相互認証した CA ごとに別の属性値として格納する						
								(略)
新:16 旧:16	組織 CA 等及び第5次 LGPKI アプリケーション CAR2 が自らの公開鍵に自らの秘密鍵で署名して発行した自己署名証明書及びリンク証明書のリポジトリ等への格納は、次の形式で行うものとする。なお、LGPKI 組織 CA は、自己署名証明書及びリンク証明書の第5次 LGPKI 公開リポジトリへの格納は行わない。			組織 CA 等及び第4次 LGPKI アプリケーション CAR2 が自らの公開鍵に自らの秘密鍵で署名して発行した自己署名証明書及びリンク証明書のリポジトリ等への格納は、次の形式で行うものとする。なお、第3次 LGPKI 組織 CA は、自己署名証明書及びリンク証明書の第4次 LGPKI 公開リポジトリへの格納は行わない。				変更

Page	新文書	旧文書	備考	差分
				(略)
新:16 旧:16	CA が発行した証明書の証明書失効リストは、各証明書の cRLDistributionPoint 拡張に示されたエントリ、または CA のエントリに格納するものとする。なお、LGPKI 組織 CA は、失効情報の第 五 次 LGPKI 公開リポジトリへの格納は行わない。	CA が発行した証明書の証明書失効リストは、各証明書の cRLDistributionPoint 拡張に示されたエントリ、または CA のエントリに格納するものとする。なお、 第三次 LGPKI 組織 CA は、失効情報の第 四 次 LGPKI 公開リポジトリへの格納は行わない。		変更
				(略)
新:18 旧:18	SECOM Document Signing RSA Root CA 2023 : https://repo1.secomtrust.net/root/docrsa/	Security Communication RootCA3 : https://repository.secomtrust.net/SC-Root3/		変更
				(略)
新:18 旧:18	セコムパスポート for PublicID CA : https://repo1.secomtrust.net/spcpp/pfm20pub/	セコムパスポート for PublicID CA : https://repo1.secomtrust.net/spcpp/pfm20pub/		
新:18	https://repo1.secomtrust.net/root/docrsa/			追加
				(略)
新:18 旧:18	なお、第 五 次 LGPKI 組織 CA R2 の発行する証明書の名義 (Subject) を表 3-1、表 3-2 に、セコムパスポート for Web SR3.0 CA が発行する Web サーバ証明書の名義 (Subject) を表 3-3 に、セコムパスポート	なお、第 四 次 LGPKI 組織 CA R2 の発行する証明書の名義 (Subject) を表 3-1、表 3-2 に、セコムパスポート for Web SR3.0 CA が発行する Web サーバ証明書の名義 (Subject) を表 3-3 に、セコムパスポート for PublicID CA		変更

Page	新文書				旧文書				備考	差分																																														
	for PublicID CA が発行するメール用証明書の名義（Subject）を表 3-4 に、文書等署名用職責証明書の名義（Subject）を表 3-5 に、LGPKI 組織 CA の発行する暗号化通信用等証明書の名義（Subject）を表 3-6 に示す。				が発行するメール用証明書、コードサイニング証明書の証明書の名義（Subject）を、表 3-4 に、第三次 LGPKI 組織 CA の発行する暗号化通信用等証明書の名義（Subject）を表 3-5 に示す。																																																			
										(略)																																														
新:19 旧:19	<table><tr><th>識別属性型</th><th>属性型</th><th>読み替え</th><th>値の設定例</th></tr><tr><td>c</td><td>countryName</td><td>国コードをそのまま指定。</td><td>JP</td></tr><tr><td>st または s</td><td>state or province</td><td>各地方公共団体の属する都道府県域を指定。</td><td>東京都の場合 「Tokyo」「Tokyo-to」</td></tr><tr><td>l</td><td>localityName</td><td>各地方公共団体の組織の所在地（代表）が置かれている市区町村名を指定。</td><td>東京都の場合 「Shinjuku-ku」 「Shinjuku City」</td></tr><tr><td>o</td><td>organizeitionName</td><td>各地方公共団体の団体名</td><td>東京都の場合 「Tokyo」「Tokyo-to」</td></tr><tr><td>cn (*1)</td><td>commonName</td><td>サーバの完全修飾ドメイン名（FQDN）を指定。</td><td>www.pref.xxxxx.lg.jp</td></tr></table>	識別属性型	属性型	読み替え	値の設定例	c	countryName	国コードをそのまま指定。	JP	st または s	state or province	各地方公共団体の属する都道府県域を指定。	東京都の場合 「Tokyo」「Tokyo-to」	l	localityName	各地方公共団体の組織の所在地（代表）が置かれている市区町村名を指定。	東京都の場合 「Shinjuku-ku」 「Shinjuku City」	o	organizeitionName	各地方公共団体の団体名	東京都の場合 「Tokyo」「Tokyo-to」	cn (*1)	commonName	サーバの完全修飾ドメイン名（FQDN）を指定。	www.pref.xxxxx.lg.jp	<table><tr><th>識別属性型</th><th>属性型</th><th>読み替え</th><th>値の設定例</th></tr><tr><td>c</td><td>countryName</td><td>国コードをそのまま指定。</td><td>JP</td></tr><tr><td>st または s</td><td>state or province</td><td>各地方公共団体の属する都道府県域を指定。</td><td>東京都の場合 「Tokyo」「Tokyo-to」</td></tr><tr><td>l</td><td>localityName</td><td>各地方公共団体の組織の所在地（代表）が置かれている市区町村名を指定。</td><td>東京都の場合 「Shinjuku-ku」 「Shinjuku City」</td></tr><tr><td>o</td><td>organizeitionName</td><td>各地方公共団体の団体名</td><td>東京都の場合 「Tokyo」「Tokyo-to」</td></tr><tr><td>ou (*1)</td><td>organizationalUnitName</td><td>部署又はグループ名。省略可能。</td><td>xxxxx Prefecture Soumubu IT Suishinshitsu</td></tr><tr><td>cn (*1)</td><td>commonName</td><td>サーバの完全修飾ドメイン名（FQDN）を指定。</td><td>www.pref.xxxxx.lg.jp</td></tr></table>	識別属性型	属性型	読み替え	値の設定例	c	countryName	国コードをそのまま指定。	JP	st または s	state or province	各地方公共団体の属する都道府県域を指定。	東京都の場合 「Tokyo」「Tokyo-to」	l	localityName	各地方公共団体の組織の所在地（代表）が置かれている市区町村名を指定。	東京都の場合 「Shinjuku-ku」 「Shinjuku City」	o	organizeitionName	各地方公共団体の団体名	東京都の場合 「Tokyo」「Tokyo-to」	ou (*1)	organizationalUnitName	部署又はグループ名。省略可能。	xxxxx Prefecture Soumubu IT Suishinshitsu	cn (*1)	commonName	サーバの完全修飾ドメイン名（FQDN）を指定。	www.pref.xxxxx.lg.jp		削除
識別属性型	属性型	読み替え	値の設定例																																																					
c	countryName	国コードをそのまま指定。	JP																																																					
st または s	state or province	各地方公共団体の属する都道府県域を指定。	東京都の場合 「Tokyo」「Tokyo-to」																																																					
l	localityName	各地方公共団体の組織の所在地（代表）が置かれている市区町村名を指定。	東京都の場合 「Shinjuku-ku」 「Shinjuku City」																																																					
o	organizeitionName	各地方公共団体の団体名	東京都の場合 「Tokyo」「Tokyo-to」																																																					
cn (*1)	commonName	サーバの完全修飾ドメイン名（FQDN）を指定。	www.pref.xxxxx.lg.jp																																																					
識別属性型	属性型	読み替え	値の設定例																																																					
c	countryName	国コードをそのまま指定。	JP																																																					
st または s	state or province	各地方公共団体の属する都道府県域を指定。	東京都の場合 「Tokyo」「Tokyo-to」																																																					
l	localityName	各地方公共団体の組織の所在地（代表）が置かれている市区町村名を指定。	東京都の場合 「Shinjuku-ku」 「Shinjuku City」																																																					
o	organizeitionName	各地方公共団体の団体名	東京都の場合 「Tokyo」「Tokyo-to」																																																					
ou (*1)	organizationalUnitName	部署又はグループ名。省略可能。	xxxxx Prefecture Soumubu IT Suishinshitsu																																																					
cn (*1)	commonName	サーバの完全修飾ドメイン名（FQDN）を指定。	www.pref.xxxxx.lg.jp																																																					
										(略)																																														

Page	新文書				旧文書	備考	差分
新:20	(*1) cn の英語表記は 64 文字以内という制限があり、64 文字を超える名称等については 64 文字以内で収まるような名称に変更する。						追加
							(略)
新:20	表 2-1 メール用証明書						移動
新:20	識別属性型	属性型	属性型説明	値の設定例			追加
	cn	commonName	電子証明書所有者のメールアドレス	xxxxx@pref.xxxx.lg.jp			
	E	E-mail address	電子証明書所有者のメールアドレス	xxxxx@pref.xxxx.lg.jp			
							(略)
新:20	表表 3-5 文書等署名用職責証明書						追加
新:20	識別属性型	属性型	属性型説明	値の設定例			追加
	c	countryName	電子証明書所有者の国名	JP			
	st	state or province	各地方公共団体の属する都道府県域を指定。	都道府県名 (英語)			
	l	localityName	各地方公共団体の組織の所在地 (代表)	市区町村名(英語)			

Page	新文書				旧文書	備考	差分
			が置かれている市区町村名を指定。				
	o	organizeitionName	各地方公共団体の団体名	地方公共団体名（英語）			
	ou (*1)	organizationalUnitName	電子証明書所有者の組織単位名	部門・部署名（英語）			
	cn (*1)	commonName	電子証明書所有者の固有名称	役職名等（英語）			
							（略）
新:20 旧:20							追加
新:20	表表 3-6 暗号化通信用等証明書						追加
新:20	識別属性型	属性型	属性型説明	値の設定例			移動
	c	countryName	電子証明書所有者の国名	JP			
	o	organizeitionName	電子証明書所有者の組織名	Local Governments			
	l	localityName	電子証明書所有者の地域名	都道府県（英語）			
	ou (*1)	organizationalUnitName	電子証明書所有者の組織単位名	地方公共団体名（英語）			
	cn (*1)	commonName	電子証明書所有者の固有名称	情報提供ネットワークシステムが			

Page	新文書				旧文書				備考	差分
				定める機関コード						
旧:20					表表 3-2 メール用証明書					移動
旧:20					識別 属性 型	属性型	属性型説明	値の設定例		削除
					c	countryName	電子証明書所有者の国名	JP		
					o	organizeitionName	電子証明書所有者の組織名	Local Governments		
					l	localityName	電子証明書所有者の地域名	都道府県（英語）		
					ou	organizationalUnitName	電子証明書所有者の組織単位名	地方公共団体名（英語）		
					ou (*1)	organizationalUnitName	電子証明書所有者の組織単位名（*2）	所属部門名（英語）		
					cn (*1)	commonName	電子証明書所有者の固有名 称	役職名等（英語）		
					E	E-mail address	電子証明書所有者のメール アドレス	xxxxx@pref.xxxx.lg.jp		
										（略）
旧:20					(*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。					削除
										（略）
旧:20					表 3--3 コードサイニング証明書					削除

Page	新文書	旧文書				備考	差分																										
旧:20		<table><tr><th>識別属性型</th><th>属性型</th><th>読み替え</th><th>値の設定例</th></tr><tr><td>c</td><td>countryName</td><td>国コードをそのまま指定。</td><td>JP</td></tr><tr><td>st または s</td><td>state or province</td><td>指定しない。省略不可の場合、各地方公共団体の属する都道府県域を指定。</td><td></td></tr><tr><td>l</td><td>localityName</td><td>各地方公共団体の属する都道府県域を指定。</td><td>都道府県（英語）</td></tr><tr><td>o</td><td>organizeitionName</td><td>Local Governments を固定で指定。</td><td>Local Governments</td></tr><tr><td>ou (*1)</td><td>organizationalUnitName</td><td>地方公共団体名を指定。サーバ管理組織名も任意で指定可能。</td><td>xxxxx Prefecture Soumubu IT Suishinshitsu</td></tr><tr><td>cn (*1)</td><td>commonName</td><td>地方公共団体名及びコード管理責任者を表す CodeAdmin を指定 (*2)。組織名、アプリケーション名も任意で指定可能。</td><td>CodeAdmin of xxxxx Prefecture {組織名} {アプリケーション名}</td></tr></table>	識別属性型	属性型	読み替え	値の設定例	c	countryName	国コードをそのまま指定。	JP	st または s	state or province	指定しない。省略不可の場合、各地方公共団体の属する都道府県域を指定。		l	localityName	各地方公共団体の属する都道府県域を指定。	都道府県（英語）	o	organizeitionName	Local Governments を固定で指定。	Local Governments	ou (*1)	organizationalUnitName	地方公共団体名を指定。サーバ管理組織名も任意で指定可能。	xxxxx Prefecture Soumubu IT Suishinshitsu	cn (*1)	commonName	地方公共団体名及びコード管理責任者を表す CodeAdmin を指定 (*2)。組織名、アプリケーション名も任意で指定可能。	CodeAdmin of xxxxx Prefecture {組織名} {アプリケーション名}			削除
識別属性型	属性型	読み替え	値の設定例																														
c	countryName	国コードをそのまま指定。	JP																														
st または s	state or province	指定しない。省略不可の場合、各地方公共団体の属する都道府県域を指定。																															
l	localityName	各地方公共団体の属する都道府県域を指定。	都道府県（英語）																														
o	organizeitionName	Local Governments を固定で指定。	Local Governments																														
ou (*1)	organizationalUnitName	地方公共団体名を指定。サーバ管理組織名も任意で指定可能。	xxxxx Prefecture Soumubu IT Suishinshitsu																														
cn (*1)	commonName	地方公共団体名及びコード管理責任者を表す CodeAdmin を指定 (*2)。組織名、アプリケーション名も任意で指定可能。	CodeAdmin of xxxxx Prefecture {組織名} {アプリケーション名}																														
旧:20		(*1) ou、cn の英語表記は 64 文字以内という制限があり、64 文字を超える名称等については 64 文字以内で収まるような名称に変更する。					削除																										
旧:20		(*2) コード管理責任者の表記は、特段の理由がない限り CodeAdmin 固定とする。					削除																										
							(略)																										
旧:20		表 3-4 暗号化通信用等証明書					削除																										

Page	新文書	旧文書				備考	差分																							
旧:20		<table><tr><th>識別属性型</th><th>属性型</th><th>属性型説明</th><th>値の設定例</th></tr><tr><td>c</td><td>countryName</td><td>電子証明書所有者の国名</td><td>JP</td></tr><tr><td>o</td><td>organizeitionName</td><td>電子証明書所有者の組織名</td><td>Local Governments</td></tr><tr><td>l</td><td>localityName</td><td>電子証明書所有者の地域名</td><td>都道府県（英語）</td></tr><tr><td>ou (*1)</td><td>organizationalUnitName</td><td>電子証明書所有者の組織単位名</td><td>地方公共団体名（英語）</td></tr><tr><td>cn (*1)</td><td>commonName</td><td>電子証明書所有者の固有名称</td><td>情報提供ネットワークシステムが定める機関コード</td></tr></table>	識別属性型	属性型	属性型説明	値の設定例	c	countryName	電子証明書所有者の国名	JP	o	organizeitionName	電子証明書所有者の組織名	Local Governments	l	localityName	電子証明書所有者の地域名	都道府県（英語）	ou (*1)	organizationalUnitName	電子証明書所有者の組織単位名	地方公共団体名（英語）	cn (*1)	commonName	電子証明書所有者の固有名称	情報提供ネットワークシステムが定める機関コード				移動
識別属性型	属性型	属性型説明	値の設定例																											
c	countryName	電子証明書所有者の国名	JP																											
o	organizeitionName	電子証明書所有者の組織名	Local Governments																											
l	localityName	電子証明書所有者の地域名	都道府県（英語）																											
ou (*1)	organizationalUnitName	電子証明書所有者の組織単位名	地方公共団体名（英語）																											
cn (*1)	commonName	電子証明書所有者の固有名称	情報提供ネットワークシステムが定める機関コード																											
旧:20		(*1) ou、cn の英語表記は 64 文字以内という制限があり、64 文字を超える名称等については 64 文字以内で収まるような名称に変更する。					削除																							
							(略)																							
新:20 旧:21	LGPKI では基本的に第 五 次 LGPKI 公開リポジトリを使用し各種証明書や失効情報（CRL/ARL）を公開するものとする。そのため、登録内容に基準が無ければ、認証パスの構築や検証の際に参照できなくなってしまう。	LGPKI では基本的に第 四 次 LGPKI 公開リポジトリを使用し各種証明書や失効情報（CRL/ARL）を公開するものとする。そのため、登録内容に基準が無ければ、認証パスの構築や検証の際に参照できなくなってしまう。					変更																							
							(略)																							
新:21 旧:21	また、 メール用証明書 と 文書等署名用職責証明書 については、少なくとも以下の鍵長での署名検証ができなければならない。	また、 コードサイニング 証明書については、少なくとも以下の鍵長での署名検証ができなければならない。					変更																							

Page	新文書	旧文書	備考	差分
				(略)
新:23 旧:23	<p>LGPKI では、第五次 LGPKI 証明書検証サーバは第五次 LGPKI 組織 CA R2 によって認証される。また、証明書検証サーバを利用するのは、第五次 LGPKI 組織 CA R2 をトラストアンカーとする地方公共団体の職責者もしくはそれに準ずる証明書検証者である。また、検証対象となる証明書は、LGPKI が発行する証明書のほかに、第五次 LGPKI 組織 CA R2 が相互認証している他 CA が発行した証明書である。第五次 LGPKI 証明書検証サーバは、LGPKI が発行した証明書を検証する者に対し、証明書検証という非常に複雑な処理の代行や、さらに、LDAP による第五次 LGPKI 公開リポジトリへのアクセスが困難な者に対し、各種認証情報を提供する等、LGPKI が発行した証明書を検証する側の負担を軽減するものである。</p>	<p>LGPKI では、第四次 LGPKI 証明書検証サーバは第四次 LGPKI 組織 CA R2 によって認証される。また、証明書検証サーバを利用するのは、第四次 LGPKI 組織 CA R2 をトラストアンカーとする地方公共団体の職責者もしくはそれに準ずる証明書検証者である。また、検証対象となる証明書は、LGPKI が発行する証明書のほかに、第四次 LGPKI 組織 CA R2 が相互認証している他 CA が発行した証明書である。第四次 LGPKI 証明書検証サーバは、LGPKI が発行した証明書を検証する者に対し、証明書検証という非常に複雑な処理の代行や、さらに、LDAP による第四次 LGPKI 公開リポジトリへのアクセスが困難な者に対し、各種認証情報を提供する等、LGPKI が発行した証明書を検証する側の負担を軽減するものである。</p>		変更
				(略)
新:23 旧:23	<p>本章では、まず第五次 LGPKI 組織 CA R2 が提供する第五次 LGPKI 証明書検証サーバについて記述し、その後証明書を発行する第五次 LGPKI 組織 CA R2 と、第五次 LGPKI 証明書検証サーバを利用する利用者クライアントが満たすべき仕様について記述する。</p>	<p>本章では、まず第四次 LGPKI 組織 CA R2 が提供する第四次 LGPKI 証明書検証サーバについて記述し、その後証明書を発行する第四次 LGPKI 組織 CA R2 と、第四次 LGPKI 証明書検証サーバを利用する利用者クライアントが満たすべき仕様について記述する。</p>		変更
				(略)

Page	新文書	旧文書	備考	差分
新:23 旧:23	第 五 次 LGPKI 証明書検証サーバの証明書は、第 五 次 LGPKI 組織 CA R2 が発行する。また、証明書検証サーバの証明書の extendedKeyUsage には id-kp-OCSPSigning を設定する。	第 四 次 LGPKI 証明書検証サーバの証明書は、第 四 次 LGPKI 組織 CA R2 が発行する。また、証明書検証サーバの証明書の extendedKeyUsage には id-kp-OCSPSigning を設定する。		変更
				(略)
新:23 旧:23	第 五 次 LGPKI 証明書検証サーバを利用するクライアントが備えているべき点を記述する。	第 四 次 LGPKI 証明書検証サーバを利用するクライアントが備えているべき点を記述する。		変更
				(略)
新:23 旧:23	第 五 次 LGPKI 証明書検証サーバのレスポンスデータに含まれる署名を検証する必要があるため、クライアントは自分の利用する第 五 次 LGPKI 証明書検証サーバの署名を検証するのに必要な下記の情報を設定する必要がある。	第 四 次 LGPKI 証明書検証サーバのレスポンスデータに含まれる署名を検証する必要があるため、クライアントは自分の利用する第 四 次 LGPKI 証明書検証サーバの署名を検証するのに必要な下記の情報を設定する必要がある。		変更
				(略)
新:23 旧:23	第 五 次 LGPKI 証明書検証サーバとの通信プロトコルについては、別添 1 に示す。	第 四 次 LGPKI 証明書検証サーバとの通信プロトコルについては、別添 1 に示す。		変更
				(略)
新:23	第 五 次 LGPKI 証明書検証サーバは、公的個人認証サービスから発行された証明書の検証を行う際、公的	第 四 次 LGPKI 証明書検証サーバは、公的個人認証サービスから発行された証明書の検証を行う際、公的個人認証		変更

Page	新文書	旧文書	備考	差分
旧:23	個人認証サービスの失効情報を参照する。LGPKI では、第 五 次 LGPKI 証明書検証サーバの利用に当たって、公的個人認証サービスから失効情報の参照が許可された地方公共団体からの利用だけに限ることとする。	サービスの失効情報を参照する。LGPKI では、第 四 次 LGPKI 証明書検証サーバの利用に当たって、公的個人認証サービスから失効情報の参照が許可された地方公共団体からの利用だけに限ることとする。		
				(略)
新:25 旧:25	LGPKI では、第 五 次 LGPKI にて、セコムトラストシステムズ株式会社が運用する各認証サービスの OCSP レスポンダを利用する。この OCSP レスポンダについてはセコムトラストシステムズ株式会社が運用する各認証サービスのリポジトリで公開する CP、CPS を参照のこと。	LGPKI では、第 四 次 LGPKI にて、セコムトラストシステムズ株式会社が運用する各認証サービスの OCSP レスポンダを利用する。この OCSP レスポンダについてはセコムトラストシステムズ株式会社が運用する各認証サービスのリポジトリで公開する CP、CPS を参照のこと。		変更
				(略)
旧:25		Security Communication RootCA3 : https://repository.secomtrust.net/SC-Root3/		削除
				(略)
新:25 旧:25	セコムパスポート for PublicID CA : https://repol.secomtrust.net/spcpp/pfm20pub/	セコムパスポート for PublicID CA : https://repol.secomtrust.net/spcpp/pfm20pub/		
新:25	https://repol.secomtrust.net/root/docrsa/			追加

Page	新文書	旧文書	備考	差分
新:25	SECOM Document Signing RSA Root CA 2023 : https://repo1.secomtrust.net/root/docrsa/			追加
				(略)
新:26 旧:26	DIT の第一階層は国、第二階層は LGPKI ("LGPKI"、"LGPKI2") コンテナとする。第三階層は、"LGPKI"以下に LGPKI 組織 CA、第 ^五 次 LGPKI アプリケーション CAR2、"LGPKI2"以下に第 ^五 次 LGPKI 組織 CA R2 とする。	DIT の第一階層は国、第二階層は LGPKI ("LGPKI"、"LGPKI2") コンテナとする。第三階層は、"LGPKI"以下に ^{第三} 次 LGPKI 組織 CA、第 ^四 次 LGPKI アプリケーション CAR2、"LGPKI2"以下に第 ^四 次 LGPKI 組織 CA R2 とする。		変更
新:26 旧:26	なお LGPKI においては、発行する証明書の subject や issuer で使用される DN を記述する文字コードが Printable String の CA と UTF8String の CA がある。LGPKI 組織 CA 及び第 ^五 次 LGPKI 組織 CA R2 の文字コードは UTF8String である。	なお LGPKI においては、発行する証明書の subject や issuer で使用される DN を記述する文字コードが Printable String の CA と UTF8String の CA がある。 ^{第三} 次 LGPKI 組織 CA 及び第 ^四 次 LGPKI 組織 CA R2 の文字コードは UTF8String である。		変更
				(略)
新:31 旧:31	CA 名称 (LGPKI 組織 CA ("Organization CA U8")) あるいは第 ^五 次 LGPKI 組織 CA R2 (" Organization CA R2") を格納する属性として、organizationalUnit オブジェクトクラスの必須属性である ou 属性を用いる。	CA 名称(^{第三} 次 LGPKI 組織 CA ("Organization CA U8")) あるいは第 ^四 次 LGPKI 組織 CA R2 (" Organization CA R2") を格納する属性として、organizationalUnit オブジェクトクラスの必須属性である ou 属性を用いる。		変更
新:31 旧:31	CA 名称 (第 ^五 次 LGPKI アプリケーション CAR2 ("Application CA R2")) を格納する属性として、organizationalRole オブジェクトクラスの必須属性であ	CA 名称 (第 ^四 次 LGPKI アプリケーション CA R2 ("Application CA R2")) を格納する属性として、organizationalRole オブジェクトクラスの必須属性である cn 属性を用いる。		変更

Page	新文書	旧文書	備考	差分
	る cn 属性を用いる。			
				(略)
新:32 旧:32	自己署名証明書及びリンク証明書は、第 五 次 LGPKI 組織 CAR2 が持つ。	自己署名証明書及びリンク証明書は、第 四 次 LGPKI 組織 CAR2 が持つ。		変更
				(略)
新:33 旧:33	第 五 次 LGPKI 組織 CAR2 の CA エントリでは、他 CA との間で取り交わした相互認証証明書が、pkiCA オブジェクトクラスの設定上追加必須属性である crossCertificatePair 属性に格納される。	第 四 次 LGPKI 組織 CAR2 の CA エントリでは、他 CA との間で取り交わした相互認証証明書が、pkiCA オブジェクトクラスの設定上追加必須属性である crossCertificatePair 属性に格納される。		変更
				(略)