

LGPKI組織認証局CP/CPS新旧対照表

第1.9版の改正履歴

平成23年3月30日

No	項番・タイトル	新(第1.9版)	旧(第1.8版)	変更理由
1	1.3.1 運営体制 表1-1 構成組織と役割 (LGWAN運営主体の役割)	<p>組織CAの運営組織として、主に次の業務を行う。</p> <ul style="list-style-type: none"> ・総合行政ネットワーク運営協議会に対する運用状況に関する報告 ・登録分局に対する監査 ・組織CAの運営 ・CAシステムの運用及び維持管理(登録局) ・エンドエンティティ証明書の発行、更新、失効申請の受付及び審査 ※地方公共団体からのエンドエンティティ証明書の発行、更新及び失効申請については、受付・審査業務の一部については登録分局に委任 ・エンドエンティティ証明書の発行及び失効の要求(発行局) ・エンドエンティティ証明書、相互認証証明書の発行及び失効の処理 <p>運営組織として次の認証局運営要員を置く。 認証局最高責任者、認証局システム責任者、鍵管理者、受付担当者、審査担当者、審査承認者、IA操作員、RA操作員、リポジトリ操作員、VA操作員、監査ログ検査者及び登録分局監査担当者</p>	<p>組織CAの運営組織として、主に次の業務を行う。</p> <ul style="list-style-type: none"> ・総合行政ネットワーク運営協議会に対する運用状況に関する報告 ・登録分局に対する監査 ・組織CAの運営 ・CAシステムの運用及び維持管理(登録局) ・エンドエンティティ証明書の発行、更新、失効申請の受付及び審査 ※エンドエンティティ証明書の発行、更新及び失効申請については、受付・審査業務の一部については登録分局に委任 ・エンドエンティティ証明書の発行及び失効の要求(発行局) ・エンドエンティティ証明書、相互認証証明書の発行及び失効の処理 <p>運営組織として次の認証局運営要員を置く。 認証局最高責任者、認証局システム責任者、鍵管理者、受付担当者、審査担当者、審査承認者、IA操作員、RA操作員、リポジトリ操作員、VA操作員、監査ログ検査者及び登録分局監査担当者</p>	<p>地方公共団体からの申請については登録分局に委任しているが、特定公的機関LGWAN-ASPからの申請については、登録局の中のASP等審査部門が実在性、同一性の確認を実施しているため(文書表現上の誤記の訂正を含む)。</p>

LGPKI組織認証局CP/CPS新旧対照表

平成21年9月29日

第1.8版の改正履歴

No	項番・タイトル	新(第1.8版)	旧(第1.7版)	変更理由
1	5.2.1信頼される役割 (7) IA操作員 (冒頭部分)	IA操作員は、CAシステムの設定管理、CA秘密鍵を使用する業務並びに相互認証証明書の発行等に関する次の業務を行う。 <ul style="list-style-type: none"> ・ CA秘密鍵の活性化及び非活性化 ・ CAシステムの起動及び停止 ・ CAシステムの動作に関する設定管理 ・ CAシステムのデータベースのバックアップに関する諸設定管理並びにバックアップ、リストア及びアーカイブの操作 ・ 証明書ポリシーの設定登録及び変更 ・ 自己署名証明書及び相互認証証明書の発行、更新及び失効処理 ・ 要員へのシステム操作用証明書の発行、更新及び失効処理 	IA操作員は、CAシステムの設定管理、CA秘密鍵及びVA秘密鍵を使用する業務並びに相互認証証明書の発行等に関する次の業務を行う。 <ul style="list-style-type: none"> ・ CA秘密鍵及びVA秘密鍵 (HSM) の活性化及び非活性化 ・ CAシステムの起動及び停止 ・ CAシステムの動作に関する設定管理 ・ CAシステムのデータベースのバックアップに関する諸設定管理並びにバックアップ、リストア及びアーカイブの操作 ・ 証明書ポリシーの設定登録及び変更 ・ 自己署名証明書及び相互認証証明書の発行、更新及び失効処理 ・ 要員へのシステム操作用証明書の発行、更新及び失効処理 	誤記の訂正。
2	3.1.8組織的な識別	エンドエンティティ証明書の申請手続きにおいて、登録局、又は登録分局は、定められた手続きにより、証明書利用者の属する組織の実在性及び同一性の確認を行う。	エンドエンティティ証明書の申請手続きにおいて、登録分局は、定められた手続きにより、証明書利用者の属する組織の実在性及び同一性の確認を行う。	誤記の訂正。
3	3.1.9個人の識別	エンドエンティティ証明書の申請手続きにおいて、登録局、又は登録分局は、定められた手続きにより、証明書利用者の実在性及び同一性の確認を行う。	エンドエンティティ証明書の申請手続きにおいて、登録分局は、定められた手続きにより、証明書利用者の実在性及び同一性の確認を行う。	誤記の訂正。

LGPKI組織認証局CP/CPS新旧対照表

平成21年3月25日

第1.7版の改正履歴

No	項番・タイトル	新(第1.7版)	旧(第1.6版)	変更理由
1	1 イントロダクション	本文書(以下「CP/CPS」という。)は、地方公共団体及び特定公的機関LGWAN-ASPの役職・職責を認証するための証明書(以下「エンドエンティティ証明書」という。)を発行するLGPKI組織認証局(以下「組織CA」という。)の認証業務に関する運用規程である。	本文書(以下「CP/CPS」という。)は、地方公共団体の役職・職責を認証するための証明書(以下「エンドエンティティ証明書」という。)を発行するLGPKI組織認証局(以下「組織CA」という。)の認証業務に関する運用規程である。	特定公的機関LGWAN-ASPへのエンドエンティティ証明書発行対応に伴う変更(追加修正)
2	1.3.2 適用性・適用環境等 ・職責証明書	地方公共団体の職責者による地方公共団体相互及び住民・企業等向け公文書への電子署名に使用する。 特定公的機関LGWAN-ASPの職責者による地方公共団体向け文書への電子署名に使用する。 職責証明書の適用により、職責者による文書であること並びに内容が改ざんされていないことを保証できる。 職責証明書の有効期間は、証明書を有効とした	地方公共団体の職責者による地方公共団体相互及び住民・企業等向け公文書への電子署名に使用する。 特定公的機関LGWAN-ASPの職責者による地方公共団体向け文書への電子署名に使用する。 職責証明書の適用により、職責者による公文書であること並びに内容が改ざんされていないことを保証できる。 職責証明書の有効期間は、証明書を有効とした	同上
3	4.8.4 自然災害その他災害後の安全な施設への復旧手段	災害等により組織CAの設備が被害を受けた場合には、 <u>バックアップサイトにおいてバックアップデータを用いて運用を行う。災害時の業務方針を以下に定める。</u> <u>・リポジトリによるCRL/ARLの公開を最優先として、公開停止から48時間以内に公開を再開する。</u> <u>・エンドエンティティ証明書等の失効業務は、業務停止より14日以内に再開する。</u> <u>・エンドエンティティ証明書等の発行業務は、メインサイトの組織CAの設備及びセキュリティが完全に復旧されたことを確認後に再開する。</u>	災害等により組織CAの設備が被害を受けた場合には、 <u>予備機を確保し、バックアップデータを用いて運用を行う。</u>	バックアップサイト運用開始に伴う変更
4	6.7 ネットワークセキュリティ制御	<u>メインサイトにおいては、不正アクセスを防止するため、外部ネットワークからの通過を許可するネットワークサービスは必要最小限とする。登録局と登録分局間は、RAシステムを使用した専用線経由のSSL通信のみとする。また、不正侵入検知等十分なセキュリティ保護対策を行う。メインサイトによる運用が行われている間、バックアップサイトは、外部ネットワークとの接続は行</u>	不正アクセスを防止するため、外部ネットワークからの通過を許可するネットワークサービスは必要最小限とする。登録局と登録分局間は、RAシステムを使用した専用線経由のSSL通信のみとする。また、不正侵入検知等十分なセキュリティ保護対策を行う。	同上

LGPKI組織認証局CP/CPS新旧対照表

平成20年10月22日

第1.6版の改正履歴

No	項番・タイトル	新(第1.6版)	旧(第1.5版)	変更理由
1	1.1.1 証明書の種類	<ul style="list-style-type: none"> ・職責証明書 ・利用者証明書 	<ul style="list-style-type: none"> ・職責証明書 ・利用者証明書 ・文書交換証明書 	文書交換証明書の廃止に伴う変更
2	1.2 識別	<ul style="list-style-type: none"> ・相互認証証明書ポリシー 1:[1.2.392.200110.10.8.5.1.1.1] ・相互認証証明書ポリシー 2:[1.2.392.200110.10.8.5.1.7.1] ・職責証明書ポリシー:[1.2.392.200110.10.8.5.1.1.1] ・利用者証明書ポリシー:[1.2.392.200110.10.8.5.1.7.1] 	<ul style="list-style-type: none"> ・相互認証証明書ポリシー 1:[1.2.392.200110.10.8.5.1.1.1] ・相互認証証明書ポリシー 2:[1.2.392.200110.10.8.5.1.2.1] ・相互認証証明書ポリシー 3:[1.2.392.200110.10.8.5.1.7.1] ・職責証明書ポリシー:[1.2.392.200110.10.8.5.1.1.1] ・文書交換証明書ポリシー:[1.2.392.200110.10.8.5.1.2.1] ・利用者証明書ポリシー:[1.2.392.200110.10.8.5.1.7.1] 	文書交換証明書の廃止に伴う変更
3	1.3.2 適用性・適用環境等 ・文書交換証明書	(削除)	<ul style="list-style-type: none"> ・文書交換証明書 <p>LGWAN電子文書交換システムにおいて、文書取扱主任が電子署名及び暗号化に使用する。文書交換証明書の適用により、発信者本人が作成したメッセージであること並びにメッセージの内容が改ざんされていないことを保証できる。また、暗号化通信により特定の送信相手のみ解読可能とすることができる。文書交換証明書の有効期間は、証明書を有効とした日から起算して3年とする。</p>	文書交換証明書の廃止に伴う変更
4	6.1.9 鍵利用目的 (2)証明書利用者鍵	(削除)	文書交換証明書の証明書利用者秘密鍵は、電子署名及び暗号化に用いる。	文書交換証明書の廃止に伴う変更

第1.6版の改正履歴

No	項番・タイトル	新(第1.6版)	旧(第1.5版)	変更理由
1	1. イントロダクション	本CP/CPSにおいて、地方公共団体とは、地方自治法に定める地方公共団体のうち総合行政ネットワーク(以下「LGWAN」という。)への参加団体をいう。 また、特定公的機関LGWAN-ASPとは、総合行政ネットワークASP基本綱領に定める公的機関であり、LGWANにASPサービス(以下「LGWAN-ASPサービス」という。)を提供する日本国内の組織等を指す。	本CP/CPSにおいて、地方公共団体とは、地方自治法に定める地方公共団体のうち総合行政ネットワーク(以下「LGWAN」という。)への参加団体をいう。	特定公的機関LGWAN-ASPへのエンドエンティティ証明書発行対応に伴う変更。
2	1.3.1 運営体制 図1-1組織と体制			同上
3	1.3.1 運営体制 表1-1構成組織と役割	証明書利用者 地方公共団体、 特定公的機関 LGWAN-ASP に属するエンドエンティティ証明書保持者であり、本CP/CPSに従いエンドエンティティ証明書を利用する。	証明書利用者 地方公共団体に属するエンドエンティティ証明書保持者であり、本CP/CPSに従いエンドエンティティ証明書を利用する。	同上
4	1.3.2 適用性・適用環境等	エンドエンティティ証明書及び相互認証証明書(以下「エンドエンティティ証明書等」という。)は、以下の用途及びアプリケーションでの使用を前提とする。 ただし、特定公的機関LGWAN-ASPが使用する場合は、LGWAN-ASPサービスを提供する手段としてLGWAN電子文書交換システムを使用する用途に限定する。	エンドエンティティ証明書及び相互認証証明書(以下「エンドエンティティ証明書等」という。)は、以下の用途及びアプリケーションでの使用を前提とする。	同上
5	1.3.2 適用性・適用環境等 ・職責証明書	地方公共団体の職責者による地方公共団体相互及び住民・企業等向け公文書への電子署名に使用する。 特定公的機関LGWAN-ASPの職責者による地方公共団体向け文書への電子署名に使用する。	地方公共団体の職責者による地方公共団体相互及び住民・企業等向け公文書への電子署名に使用する。	同上

第1.6版の改正履歴

No	項番・タイトル	新(第1.6版)	旧(第1.5版)	変更理由
6	1.3.2 適用性・適用環境等 ・利用者証明書	各種情報システムを利用する場合の認証等、電子署名並びに暗号化に使用する。利用者証明書の適用により、利用者が各種情報システムを使用する際、証明書に記載された利用者であること、発信者本人が作成したメッセージであること並びにメッセージの内容が改ざんされていないことを保証できる。また、暗号化通信により特定の送信相手のみ解読可能とすることができる。	各種情報システムに対する認証等に使用する。利用者証明書の適用により、利用者が各種情報システムを使用する際、証明書に記載された利用者であることを保証できる。また、LGWAN電子文書交換システムにおいて、文書取扱主任が電子署名および暗号化に使用する。利用者証明書の適用により、発信者本人が作成したメッセージであること並びにメッセージの内容が改ざんされていないことを保証できる。また、暗号化通信により特定の送信相手のみ解読可能とすることができる。	同上
7	2.1.2 登録局及び登録分局の義務 (1)登録局	<ul style="list-style-type: none"> ・特定公的機関LGWAN-ASPの証明書利用者からのエンドエンティティ証明書の発行、更新及び失効申請に際して、LGWAN運営主体の稼働日において、受付、証明書利用者の実在性、同一性及び申請内容の確認を行う。 ・特定公的機関LGWAN-ASPの証明書利用者に対して、エンドエンティティ証明書の発行完了及び失効完了を通知する。 ・各申請手続きにおいて入手した特定公的機関LGWAN-ASPの証明書利用者情報を安全に保管する。 	(なし)	同上
8	4.1 証明書申請 (2)エンドエンティティ証明書	証明書利用者は、定められた手続きによりエンドエンティティ証明書の発行申請書等を登録分局の受付担当者へ提出する。登録分局では、登録分局責任者が登録局へ発行申請を行う。 特定公的機関LGWAN-ASPの証明書利用者は、定められた手続きによりエンドエンティティ証明書の発行申請書等を登録局の受付担当者へ提出する。	証明書利用者は、定められた手続きによりエンドエンティティ証明書の発行申請書等を登録分局の受付担当者へ提出する。登録分局では、登録分局責任者が登録局へ発行申請を行う。	同上
9	4.2 証明書発行 (2)エンドエンティティ証明書	登録分局の受付担当者は、証明書利用者に対して、エンドエンティティ証明書と証明書情報を記載した発行通知を配付する。 登録局の受付担当者は、特定公的機関LGWAN-ASPの証明書利用者に対して、エンドエンティティ証明書と証明書情報を記載した発行通知を配付する。	登録分局の受付担当者は、証明書利用者に対して、エンドエンティティ証明書と証明書情報を記載した発行通知を配付する。	同上

第1.6版の改正履歴

No	項番・タイトル	新(第1.6版)	旧(第1.5版)	変更理由
10	4.3 証明書受入れ (2)エンドエンティティ証明書	組織CAは、発行した証明書及びPIN情報、又は証明書のみを、所定の手続きに基づき安全かつ確実な方法で、登録分局の受付担当者、 特定公的機関LGWAN-ASPの証明書利用者 に配付する。登録分局への受渡しは、登録局の受付担当者が配付確認を行うことにより、完了とする。登録分局の受付担当者は、所定の手続きに基づき安全かつ確実な方法で、証明書利用者に配付する。証明書利用者への配付管理は、登録分局が行い、 特定公的機関LGWAN-ASPの証明書利用者への配付管理は、登録局が行う。	組織CAは、発行した証明書及びPIN情報、又は証明書のみを、所定の手続きに基づき安全かつ確実な方法で、登録分局の受付担当者、特定公的機関LGWAN-ASPの証明書利用者に配付する。登録分局への受渡しは、登録局の受付担当者が配付確認を行うことにより、完了とする。登録分局の受付担当者は、所定の手続きに基づき安全かつ確実な方法で、証明書利用者に配付する。証明書利用者への配付管理は、登録分局が行い、特定公的機関LGWAN-ASPの証明書利用者への配付管理は、登録局が行う。	同上
11	4.4.3 失効要求手続き (2)エンドエンティティ証明書	地方公共団体の 証明書利用者は、定められた手続きによりエンドエンティティ証明書の失効申請書を登録分局の受付担当者へ提出する。 特定公的機関LGWAN-ASPの証明書利用者は、定められた手続きによりエンドエンティティ証明書の失効申請書を登録局の受付担当者へ提出する。 組織CAは、所定の手続きに基づき要求された証明書を失効し、CRLをリポジトリに登録する。認証局システム責任者は、失効完了を確認し、RAシステムにその旨を反映する。 登録分局の受付担当者は、RAシステムで失効完了を確認し、証明書利用者に対して、エンドエンティティ証明書の失効通知を行う。 登録局の受付担当者は、RAシステムで失効完了を確認し、特定公的機関LGWAN-ASPの証明書利用者に対して、エンドエンティティ証明書の失効通知を行う。	証明書利用者は、定められた手続きによりエンドエンティティ証明書の失効申請書を登録分局の受付担当者へ提出する。登録分局では、登録分局責任者が登録局へ失効申請を行う。 組織CAは、所定の手続きに基づき要求された証明書を失効し、CRLをリポジトリに登録する。認証局システム責任者は、失効完了を確認し、RAシステムにその旨を反映する。 登録分局の受付担当者は、RAシステムで失効完了を確認し、証明書利用者に対して、エンドエンティティ証明書の失効通知を行う。	同上

LGPKI組織認証局CP/CPS新旧対照表

平成19年10月5日

第1.5版の改正履歴

No	項番・タイトル	新(第1.5版)	旧(第1.4版)	変更理由
1	1.1.1 証明書の種類	<ul style="list-style-type: none"> ・職責証明書 ・文書交換証明書 ・利用者証明書 	<ul style="list-style-type: none"> ・職責証明書 ・文書交換証明書 	利用者証明書追加のため
2	1.2 識別	<ul style="list-style-type: none"> ・相互認証証明書ポリシー1:[1.2.392.200110.10.8.5.1.1.1] ・相互認証証明書ポリシー2:[1.2.392.200110.10.8.5.1.2.1] ・相互認証証明書ポリシー3:[1.2.392.200110.10.8.5.1.7.1] ・職責証明書ポリシー:[1.2.392.200110.10.8.5.1.1.1] ・文書交換証明書ポリシー:[1.2.392.200110.10.8.5.1.2.1] ・利用者証明書ポリシー:[1.2.392.200110.10.8.5.1.7.1] 	<ul style="list-style-type: none"> ・相互認証証明書ポリシー1:[1.2.392.200110.10.8.5.1.1.1] ・相互認証証明書ポリシー2:[1.2.392.200110.10.8.5.1.2.1] ・職責証明書ポリシー:[1.2.392.200110.10.8.5.1.1.1] ・文書交換証明書ポリシー:[1.2.392.200110.10.8.5.1.2.1] 	利用者証明書追加のため
3	1.3.2 適用性・適用環境等	<ul style="list-style-type: none"> ・利用者証明書 <p>各種情報システムに対する認証等に使用する。利用者証明書の適用により、利用者が各種情報システムを使用する際、証明書に記載された利用者であることを保証できる。</p> <p>また、LGWAN電子文書交換システムにおいて、文書取扱主任が電子署名および暗号化に使用する。利用者証明書の適用により、発信者本人が作成したメッセージであること並びにメッセージの内容が改ざんされていないことを保証できる。また、暗号化通信により特定の送信相手のみ解読可能とすることができる。</p> <p>利用者証明書の有効期間は、証明書を有効とした日から起算して3年とする。</p>	(なし)	利用者証明書追加のため
4	6.1.9 鍵利用目的 (2)証明書利用者鍵	<p>職責証明書の証明書利用者秘密鍵は、電子署名に用いる。</p> <p>文書交換証明書の証明書利用者秘密鍵は、電子署名及び暗号化に用いる。</p> <p>利用者証明書の証明書利用者秘密鍵は、電子署名及び暗号化に用いる。</p>	<p>職責証明書の証明書利用者秘密鍵は、電子署名に用いる。</p> <p>文書交換証明書の証明書利用者秘密鍵は、電子署名及び暗号化に用いる。</p>	利用者証明書追加のため

LGPKI組織認証局CP/CPS新旧対照表

平成19年5月24日

第1.4版の改正履歴

No	項番・タイトル	新(第1.4版)	旧(第1.3版)	変更理由
1	2.6.1 CAに関する情報の公開 (2)Webサーバ上での公表 (公開Webサーバ)	<ul style="list-style-type: none"> ・組織CAと相互認証したCAの名称及び相互認証を取り消したCAの名称 ・CA秘密鍵危殆化に関する情報 ・組織CA CP/CPS ・組織CA CP/CPSの改正履歴 ・プロフィール設計書 ・技術仕様書 	<ul style="list-style-type: none"> ・組織CAと相互認証したCAの名称及び相互認証を取り消したCAの名称 ・CA秘密鍵危殆化に関する情報 ・組織CA CP/CPS ・組織CA CP/CPSの改正履歴 ・プロフィール設計書 ・技術仕様書 ・組織CAが発行及び失効した証明書の一覧(地方公共団体が公文書等に電子署名を行うために利用する証明書のみ) 	政府認証基盤(GPKI)府省認証局CP/CPSガイドラインの改定(平成19年3月30日付)に伴う変更
2	2.6.2 公表の頻度	<ul style="list-style-type: none"> ・本CP/CPS「2.6.1 CAに関する情報の公表」に規定する各証明書及びそのCRL/ARLは、発行及び更新の都度 ・CP/CPS変更の都度 ・エンドエンティティ証明書の申請書類、LGPKI証明書利用者の手引(地方公共団体編)、プロフィール設計書及び技術仕様書の変更の都度 ・組織CAが認証した認証局の名称及び認証を取り消した認証局の名称は、LGWAN運営協議会による決定の都度 	<ul style="list-style-type: none"> ・本CP/CPS「2.6.1 CAに関する情報の公表」に規定する各証明書及びそのCRL/ARLは、発行及び更新の都度 ・CP/CPS変更の都度 ・エンドエンティティ証明書の申請書類、LGPKI証明書利用者の手引(地方公共団体編)、プロフィール設計書及び技術仕様書の変更の都度 ・組織CAが認証した認証局の名称及び認証を取り消した認証局の名称は、LGWAN運営協議会による決定の都度 ・組織CAが発行及び失効した証明書の一覧変更の都度 	政府認証基盤(GPKI)府省認証局CP/CPSガイドラインの改定(平成19年3月30日付)に伴う変更
3	6.1.3 CAへの公開鍵の登録	<ul style="list-style-type: none"> ・その他の場合は、組織CAにおいて証明書利用者の鍵ペアを生成、登録する。 	<ul style="list-style-type: none"> ・その他の場合は、組織CAにおいてが証明書利用者の鍵ペアを生成、登録する。 	誤記の修正

LGPKI組織認証局CP/CPS新旧対照表

平成19年3月20日

第1.3版の改正履歴

No	項番・タイトル	新(第1.3版)	旧(第1.2版)	変更理由
1	4.4.3 失効要求手続き (2)エンドエンティティ証明書	組織CAは、所定の手続きに基づき要求された証明書を失効し、CRLをリポジトリに登録する。	組織CAは、所定の手続きに基づき要求された証明書を失効し、CRLをリポジトリ及びWebサーバに登録する。	誤記の修正
2	4.6.1 アーカイブデータの種類	・IAシステムの起動、停止履歴	・IAシステム及びRAシステムの起動、停止履歴	運用の実態との差異による修正
3	4.9 認証業務の終了	・業務終了後の組織CAのバックアップのバックアップデータ及びアーカイブデータ等の保管組織及び開示方法	・業務終了後のアプリケーションCAのバックアップのバックアップデータ及びアーカイブデータ等の保管組織及び開示方法	誤記の修正

LGPKI組織認証局CP/CPS新旧対照表

平成18年11月24日

第1.2版の改正履歴

No	項番・タイトル	新(第1.2版)	旧(第1.1版)	変更理由
1	4.7 鍵の更新 (1)CA鍵	CA鍵ペアは、5年以内に更新を行う。 ただし、公開鍵と秘密鍵の有効期間内にCAを廃止する場合は、この限りでない。	CA鍵ペアは、5年以内に更新を行う。	CAを廃止する場合の特例措置の追加による変更。
2	6.3.2 公開鍵及び秘密鍵の利用期間 (1)CA鍵	組織CAの公開鍵及び秘密鍵の有効期間は、有効とした日から起算して10年以内とし、5年以内に鍵更新を行う。 ただし、公開鍵と秘密鍵の有効期間内にCAを廃止する場合は、この限りでない。 なお、暗号のセキュリティが脆弱になったと判断した場合には、その時点で鍵長又はアルゴリズムの変更等適切な処置を行った上で鍵更新を行うことがある。	組織CAの公開鍵及び秘密鍵の有効期間は、有効とした日から起算して10年以内とし、5年以内に鍵更新を行う。ただし、暗号のセキュリティが脆弱になったと判断した場合には、その時点で鍵長又はアルゴリズムの変更等適切な処置を行った上で鍵更新を行うことがある。	CAを廃止する場合の特例措置の追加による変更。

LGPKI組織認証局CP/CPS新旧対照表

第1.1版の改正履歴

平成18年9月1日

No	項番・タイトル	新(第1.1版)	旧(第1版)	変更理由
1	1.3.1 運営体制 表1-1の総合行政ネットワーク運営協議会	組織CAのCP/CPSの制定及び改正	組織CAのCP/CPSの制定及び改訂	誤記による修正
2	2.1.4 証明書検証者の義務	エンドエンティティ証明書の証明書検証者は、認証パスの構築と認証パスの検証を行う。	エンドエンティティ証明書の証明書検証者は、証明書の有効性と認証パスの有効性について検証する。	誤記による修正
3	2.1.6 VAの義務	エンドエンティティ証明書の有効性確認問合わせに対し、認証パスの構築と認証パスの検証を行う。	エンドエンティティ証明書等の有効性確認問合わせに対し、組織CAの電子署名検証、有効期限及び失効情報の確認を行う。	誤記による修正
4	2.6.1 CAに関する情報の公表 (1)リポジトリ上での公表	組織CAが発行した自己署名証明書、リンク証明書、相互認証証明書、エンドエンティティ証明書及びCRL/ARL	組織CAが発行した自己署名証明書、リンク証明書、相互認証証明書、エンドエンティティ証明書等及びCRL/ARL	誤記による修正
5	2.6.1 CAに関する情報の公表 (2)Web上での公表	組織CA CP/CPSの改正履歴	組織CA CP/CPSの改訂履歴	誤記による修正
6	8.1本CP/CPSの変更管理	本CP/CPSの制定及び改正は、LGWAN運営協議会が行う。本CP/CPSはLGWAN運営協議会が制定又は改正した日から有効となる。	本CP/CPSの制定及び改訂は、LGWAN運営協議会が行う。本CP/CPSはLGWAN運営協議会が制定又は改訂した日から有効となる。	誤記による修正
7	8.2 開示及び通知	LGWAN運営主体は、本CP/CPSが制定又は改正した場合、速やかにこれを公表し、これをもって、証明書利用者及び証明書検証者への通知とする。	LGWAN運営主体は、本CP/CPSが制定又は改訂した場合、速やかにこれを公表し、これをもって、証明書利用者及び証明書検証者への通知とする。	誤記による修正
8	9. 用語集 PIN	個人識別番号。LGPKIでは、CA秘密鍵活性化に用いるパスワード、証明書利用者に配付するICカードの活性化に用いるパスワード及び証明書利用者が鍵ペアを生成した場合に設定する秘密鍵保護に用いるパスワード等を指す。	個人識別番号。LGPKIでは、CA秘密鍵活性化に用いるパスワード、証明書利用者に配付するICカードの活性化に用いるパスワード、証明書利用者が鍵ペアを生成した場合に設定する秘密鍵保護に用いるパスワード及び秘密鍵が格納されるWebサーバの操作員カードのパスワード等を指す。	誤記による修正