

LGPKIブリッジ認証局CP/CPS新旧対照表

第1.9版の改正履歴

平成21年9月29日

No	項番・タイトル	新(第1.9版)	旧(第1.8版)	変更理由
1	1.1.1証明書の種類	ブリッジCAは、総合行政ネットワーク運営主体(以下「LGWAN運営主体」という。)に対し、 <u>インターネット側の証明書検証者向けに整備される</u> VAサーバに証明書(以下「VA証明書」という。)を発行する。	ブリッジCAは、総合行政ネットワーク運営主体(以下「LGWAN運営主体」という。)に対し、 <u>総合行政ネットワークで運用する</u> VAサーバに証明書(以下「VA証明書」という。)を発行する。	LGWAN内部向けVA秘密鍵の管理をCP/CPSの対象外とした。
2	5.2.1信頼される役割 (7)IA操作員	CA秘密鍵 <u>及びVA秘密鍵(HSM)</u> の活性化及び非活性化	CA秘密鍵の活性化及び非活性化	誤記の訂正。
3	3.1.8組織的な識別	ブリッジCAは、相互認証証明書の申請手続きにおいて、定められた手続きにより、相互認証先CAを運営する組織の真偽を確認する。	ブリッジCAは、相互認証証明書の申請手続きにおいて、定められた手続きにより、相互認証先CAを運営する組織の真偽を確認する。 <u>また、VA証明書の申請手続きにおいて、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確認及び同一性の確認を行う。</u>	誤記の訂正。

LGPKIブリッジ認証局CP/CPS新旧対照表

第1.8版の改正履歴

平成21年3月25日

No	項番・タイトル	新(第1.8版)	旧(第1.7版)	変更理由
1	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	<p>災害等によりブリッジ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></p> <ul style="list-style-type: none"> <li>・<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></li> <li>・<u>相互認証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></li> <li>・<u>相互認証証明書等の発行業務は、メインサイトのブリッジ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></li> </ul>	<p>災害等によりブリッジ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></p>	バックアップサイト運用開始に伴う変更
2	6.7 ネットワークセキュリティ制御	<p><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。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</u></p>	<p>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。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。</p>	同上

LGPKIブリッジ認証局CP/CPS新旧対照表

第1.7版の改正履歴

平成20年10月22日

No	項番・タイトル	新(第1.7版)	旧(第1.6版)	変更理由
1	1.2 識別	<ul style="list-style-type: none"> <li>・相互認証証明書ポリシー</li> <li>1:[1.2.392.200110.10.8.5.1.1.1]</li> <li>・相互認証証明書ポリシー</li> <li>2:[1.2.392.200110.10.8.5.1.7.1]</li> <li>・VA証明書ポリシー:[1.2.392.200110.10.8.5.1.3.1]</li> </ul>	<ul style="list-style-type: none"> <li>・<del>相互認証証明書ポリシー</del></li> <li>1:<del>[1.2.392.200110.10.8.5.1.1.1]</del></li> <li>・<del>相互認証証明書ポリシー</del></li> <li>2:<del>[1.2.392.200110.10.8.5.1.2.1]</del></li> <li>・相互認証証明書ポリシー</li> <li>3:[1.2.392.200110.10.8.5.1.7.1]</li> <li>・VA証明書ポリシー:[1.2.392.200110.10.8.5.1.3.1]</li> </ul>	文書交換証明書の廃止に伴う変更

## LGPKIブリッジ認証局CP/CPS新旧対照表

平成20年5月28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. イントロダクション	本文書(以下「CP/CPS」という。)は、LGPKI組織認証局との相互認証及び政府認証基盤等の外部認証基盤との相互認証のために運営される、LGPKIブリッジ認証局(以下「ブリッジ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、LGPKI組織認証局との相互認証及び政府認証基盤、霞が関WAN等の外部認証基盤との相互認証のために運営される、LGPKIブリッジ認証局(以下「ブリッジCA」という。)の認証業務に関する運用規程である。	「霞が関WAN及び政府認証基盤(共通システム)の最適化計画」(平成17年3月31日)の認証局の集約に伴う変更。
2	2.6.1 CAに関する情報の公開 (1)リポジトリ上での公表 (統合リポジトリ)	・政府認証基盤が公開している証明書情報	・霞が関WAN側の証明書情報	「霞が関WAN及び政府認証基盤(共通システム)の最適化計画」(平成17年3月31日)の認証局の集約に伴う変更。
3	2.6.1 CAに関する情報の公開 (1)リポジトリ上での公表 (公開リポジトリ)	・相互認証先CAへの相互認証証明書 ・相互認証先CAからの相互認証証明書	・相互認証先CA(対霞が関WANを除く)への相互認証証明書 ・相互認証先CA(対霞が関WANを除く)からの相互認証証明書	「霞が関WAN及び政府認証基盤(共通システム)の最適化計画」(平成17年3月31日)の認証局の集約に伴う変更。
4	2.6.1 CAに関する情報の公開 (2)Webサーバ上での公表 (地方公共団体向けWebサーバ)	・ブリッジCAと相互認証した相互認証先CAの名称及び相互認証を取り消した相互認証先CAの名称	・ブリッジCAと相互認証した相互認証先CAの名称及び相互認証を取り消したCAの名称	記載の明確化
5	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)	・ブリッジCAと相互認証した相互認証先CAの名称及び相互認証を取り消した相互認証先CAの名称	・ブリッジCAと相互認証した相互認証先CAの名称及び相互認証を取り消したCAの名称	記載の明確化
6	2.6.2 公表の頻度	・ブリッジCAと相互認証した相互認証先CAの名称及び相互認証を取り消した相互認証先CAの名称は、LGWAN運営協議会による決定の都度	・ブリッジCAと相互認証した相互認証先CAの名称及び相互認証を取り消したCAの名称は、LGWAN運営協議会による決定の都度	記載の明確化
7	4.4.1 失効要件 (1)相互認証証明書	(削除)	・相互接続基本要件に不適合となった場合(対霞が関WAN)	「霞が関WAN及び政府認証基盤(共通システム)の最適化計画」(平成17年3月31日)の認証局の集約に伴う変更。

LGPKIブリッジ認証局CP/CPS新旧対照表

第1.5版の改正履歴

平成19年10月5日

No	項番・タイトル	新(第1.5版)	旧(第1.4版)	変更理由
1	1.2 識別	<ul style="list-style-type: none"> <li>・相互認証証明書ポリシー1:[1.2.392.200110.10.8.5.1.1.1]</li> <li>・相互認証証明書ポリシー2:[1.2.392.200110.10.8.5.1.2.1]</li> <li>・相互認証証明書ポリシー3:[1.2.392.200110.10.8.5.1.7.1]</li> <li>・VA証明書ポリシー:[1.2.392.200110.10.8.5.1.3.1]</li> </ul>	<ul style="list-style-type: none"> <li>・相互認証証明書ポリシー1:[1.2.392.200110.10.8.5.1.1.1]</li> <li>・相互認証証明書ポリシー2:[1.2.392.200110.10.8.5.1.2.1]</li> <li>・VA証明書ポリシー:[1.2.392.200110.10.8.5.1.3.1]</li> </ul>	利用者証明書追加のため

LGPKIブリッジ認証局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 (1)リポジトリ上での公表 (統合リポジトリ)	<ul style="list-style-type: none"> <li>・ブリッジCAが発行した自己署名証明書、リンク証明書、相互認証証明書及びCRL/ARL</li> <li>・相互認証先CAからの相互認証証明書</li> <li>・霞が関WAN側の証明書情報</li> <li>・組織CAからの相互認証証明書</li> </ul>	<ul style="list-style-type: none"> <li>・ブリッジCAが発行した自己署名証明書、リンク証明書、相互認証証明書及びCRL/ARL</li> <li>・相互認証先CAからの相互認証証明書</li> <li>・霞が関WAN側の証明書情報</li> </ul>	運用の実態との差異による修正
2	2.6.1 CAに関する情報の公開 (1)リポジトリ上での公表 (公開リポジトリ)	<ul style="list-style-type: none"> <li>・ブリッジCAが発行した自己署名証明書、リンク証明書及びCRL/ARL</li> <li>・相互認証先CA(対霞が関WANを除く)への相互認証証明書</li> <li>・相互認証先CA(対霞が関WANを除く)からの相互認証証明書</li> <li>・組織CAへの相互認証証明書</li> </ul>	<ul style="list-style-type: none"> <li>・ブリッジCAが発行した自己署名証明書、リンク証明書及びCRL/ARL</li> <li>・相互認証先CA(対霞が関WANを除く)への相互認証証明書</li> <li>・相互認証先CA(対霞が関WANを除く)からの相互認証証明書</li> </ul>	運用の実態との差異による修正
3	9. 用語集 ・CA(Certification Authority)	LGPKIでは、ブリッジCA、組織CA及びアプリケーションCAと同義であり、発行局と登録局を	LGPKIでは、ブリッジCA、ブリッジCA及びアプリケーションCAと同義であり、発行局と登録局を	誤記の修正

LGPKIブリッジ認証局CP/CPS新旧対照表

第1.3版の改正履歴

平成19年3月20日

No	項番・タイトル	新(第1.3版)	旧(第1.2版)	変更理由
1	3.1.8 組織的な識別	ブリッジCAは、相互認証証明書の申請手続きにおいて、定められた手続きにより、相互認証先CAを運営する組織の真偽を確認する。 また、VA証明書の申請手続きにおいて、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。	ブリッジCAは、相互認証証明書の申請手続きにおいて、定められた手続きにより、相互認証先CAを運営する組織の真偽を確認する。	記載内容の明確化
2	4.1 証明書申請 (2) VA証明書	VA証明書の発行申請は、認証局システム責任者が行う。	VA証明書の発行申請は、認証局システム責任者の指示に基づき受付担当者が行う。	運用の実態との差異による修正
3	4.4.2 失効申請者 (2) VA証明書	VA証明書の失効申請は、認証局システム責任者が行う。	VA証明書の失効申請は、認証局システム責任者の指示に基づき受付担当者が行う。	運用の実態との差異による修正
4	4.9 認証業務の終了	・業務終了後のブリッジ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
5	5.2.1 信頼される役割 (4)受付担当者	受付担当者は、相互認証証明書の発行、更新及び失効申請の受付、証明書利用者との連絡調整業務及び申請書類等の管理を行う。	受付担当者は、相互認証証明書及びVA証明書の発行、更新及び失効申請の受付、証明書利用者との連絡調整業務及び申請書類等の管理を行う。	運用の実態との差異による修正
6	5.2.1 信頼される役割 (5)審査担当者	審査担当者は、相互認証証明書の発行申請、更新申請及び失効申請の審査業務を行う。	審査担当者は、相互認証証明書及びVA証明書の発行申請、更新申請及び失効申請の審査業務を行う。	運用の実態との差異による修正
7	5.2.1 信頼される役割 (6)審査承認者	審査承認者は、審査担当者からの相互認証証明書の発行申請、更新申請及び失効申請の審査結果に対して承認業務を行う。	審査承認者は、審査担当者からの相互認証証明書及びVA証明書の発行申請、更新申請及び失効申請の審査結果に対して承認業務を行う。	運用の実態との差異による修正

LGPKIブリッジ認証局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	ブリッジ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。	ブリッジ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ブリッジ認証局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	ブリッジCAのCP/CPSの制定及び改正	ブリッジCAのCP/CPSの制定及び承認	誤記による修正
2	1.3.1 運営体制 表1-1の証明書検証者	証明書検証者は、失効リスト(以下「CRL/ARL」という。)により相互認証証明書の有効性を確認する。	証明書検証者は、失効リスト(以下「CRL/ARL」という。)により相互認証証明書等の有効性を確認する。	誤記による修正
3	1.3.2 適用性・適用環境等	VA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1年とする。	VA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。	VA証明書の失効確認を任意とし、かつVA証明書プロファイルの拡張鍵用途にid-pkix-ocsp-nocheckを設定することにより、実運用に合わせるための変更
4	2.1.4 証明書検証者の義務	相互認証証明書等の証明書検証者は、認証パスの構築と認証パスの検証を行う。ただし、VA証明書の失効確認は任意とする。	相互認証証明書等の証明書検証者は、証明書の有効性及び認証パスの有効性について検証する。	VA証明書のプロファイル変更に伴う取扱い変更
5	2.1.6 VAの義務	証明書の有効性確認問合わせに対し、認証パスの構築及び認証パスの検証を行う。	相互認証証明書等の有効性確認問合わせに対し、ブリッジ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
6	2.2.4 証明書検証者の責務	相互認証証明書等の証明書検証者は、本CP/CPSに基づき相互認証証明書又はVA証明書を検証することに関し責任を持つ。ただし、VA証明書の失効確認は任意とする。	相互認証証明書等の証明書検証者は、本CP/CPSに基づき相互認証証明書又はVA証明書を検証することに関し責任を持つ。	VA証明書のプロファイル変更に伴う取扱い変更
7	2.6.1 CAに関する情報の公表	ブリッジCA CP/CPSの改正履歴	ブリッジCA CP/CPSの改訂履歴	誤記による修正
8	4.4.10 CRL/ARL検証要件	相互認証証明書の証明書検証者は、リポトリに公開されるブリッジCAの発行するCRL/ARLによって、相互認証証明書の有効性を確認しなければならない。	相互認証証明書等の証明書検証者は、リポトリに公開されるブリッジCAの発行するCRL/ARLによって、相互認証証明書等の有効性を確認しなければならない。	誤記による修正
9	4.7 鍵更新 (2)VA鍵	証明書利用者の鍵ペアは、1年以内に更新を行う。	証明書利用者の鍵ペアは、3年以内に更新を行う。	VA証明書の失効確認を任意とし、かつVA証明書プロファイルの拡張鍵用途にid-pkix-ocsp-nocheckを設定することにより、実運用に合わせるための変更

LGPKIブリッジ認証局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
10	6.3.2 公開鍵及び秘密鍵の利用期間 (2)VA鍵	VA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1年以内とする。	VA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3年以内とする。	VA証明書の失効確認を任意とし、かつVA証明書プロファイルの拡張鍵用途にid-pkix-ocsp-nocheckを設定することにより、実運用に合わせるための変更
11	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
12	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
13	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