

LGPKI
ブリッジ認証局 CP/CPS

第1.9版

平成21年9月29日

総合行政ネットワーク運営協議会

1. イントロダクション	1
1.1 概要	1
1.1.1 証明書の種類	1
1.1.2 関連規程	1
1.2 識別	2
1.3 運営体制及び証明書適用範囲	3
1.3.1 運営体制	3
1.3.2 適用性・適用環境等	5
1.4 CP/CPS に関する連絡先	5
1.4.1 管理組織	5
1.4.2 連絡先	5
2. 一般規定	6
2.1 義務	6
2.1.1 発行局の義務	6
2.1.2 登録局の義務	6
2.1.3 証明書利用者の義務	6
2.1.4 証明書検証者の義務	7
2.1.5 リポジトリの義務	7
2.1.6 VA の義務	7
2.2 責務	7
2.2.1 発行局の責務	7
2.2.2 登録局の責務	7
2.2.3 証明書利用者の責務	8
2.2.4 証明書検証者の責務	8
2.2.5 リポジトリの責務	8
2.2.6 VA の責務	8
2.3 財産権に関する責任	8
2.4 解釈と実行	8
2.4.1 準拠法	8
2.4.2 分離可能性条項、残存規定条項、完全合意条項及び通知条項	8
2.4.3 紛争解決手続き	9
2.5 料金	9
2.6 公表情報に関する規定	9
2.6.1 CA に関する情報の公表	9
2.6.2 公表の頻度	10
2.6.3 アクセスコントロール	10
2.6.4 リポジトリ	10
2.7 準拠性監査	12

2.7.1	準拠性監査の頻度	12
2.7.2	監査人の識別及び資格	12
2.7.3	監査人と被監査者との関係	12
2.7.4	監査項目	12
2.7.5	監査指摘事項への対応	12
2.7.6	監査結果の通知	12
2.8	機密性のポリシー	13
2.8.1	機密情報	13
2.8.2	機密情報対象外の情報	13
2.8.3	失効情報の開示	13
2.8.4	法律執行者への開示	13
2.8.5	民事手続き上の情報開示	13
2.8.6	証明書利用者本人の要求に基づく開示	13
2.8.7	その他の情報開示状況	13
2.9	知的財産権	13
3.	識別及び認証	14
3.1	初期登録	14
3.1.1	名前の型	14
3.1.2	名前の意味	14
3.1.3	多様な名前形式の解釈のルール	14
3.1.4	名前の一意性	14
3.1.5	名前に関する係争の解決手段	14
3.1.6	登録商標の認知、認証及び役割	14
3.1.7	秘密鍵の所有証拠の確認手段	14
3.1.8	組織的な識別	15
3.1.9	個人の識別	15
3.2	通常 of 更新	15
3.3	失効後の鍵更新	15
3.4	失効要求	15
4.	運用要件	16
4.1	証明書申請	16
4.2	証明書発行	16
4.3	証明書受入れ	16
4.4	証明書一時停止と失効	16
4.4.1	失効要件	16
4.4.2	失効申請者	17
4.4.3	失効要求手続き	17
4.4.4	失効猶予期間	17
4.4.5	一時停止要件	18

4.4.6	一時停止申請者.....	18
4.4.7	一時停止要求手続き.....	18
4.4.8	一時停止期間.....	18
4.4.9	CRL/ARL 発行頻度.....	18
4.4.10	CRL/ARL 検証要件.....	18
4.4.11	オンライン有効性検証・状態検証.....	18
4.4.12	オンライン有効性検証・状態検証要件.....	18
4.4.13	失効を公知する他の手法.....	18
4.4.14	失効を公知する他の手法の検証要件.....	18
4.4.15	鍵危殆化による特別な要件.....	18
4.5	セキュリティ監査手続き.....	18
4.5.1	記録事象.....	19
4.5.2	監査ログの監査頻度.....	19
4.5.3	監査ログの保管期間.....	19
4.5.4	監査ログの保護.....	19
4.5.5	監査ログのバックアップ手続き.....	19
4.5.6	監査ログシステム.....	19
4.5.7	記録事象の通知.....	19
4.5.8	脆弱性の検証.....	19
4.6	アーカイブ.....	20
4.6.1	アーカイブデータの種類.....	20
4.6.2	アーカイブデータの保管期間.....	20
4.6.3	アーカイブデータの保護.....	20
4.6.4	アーカイブデータのバックアップ手順.....	20
4.6.5	レコードのタイムスタンプ要件.....	20
4.6.6	アーカイブデータの収集システム.....	20
4.6.7	アーカイブデータの検証手順.....	20
4.7	鍵の更新.....	20
4.8	鍵の危殆化及び災害からの復旧.....	21
4.8.1	ハードウェア、ソフトウェア及びデータ破壊からの復旧手段.....	21
4.8.2	証明書が失効した場合の復旧手段.....	21
4.8.3	秘密鍵が危殆化した場合の復旧手段.....	21
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.....	21
4.9	認証業務の終了.....	21
5.	物理的、手続き的及び要員のセキュリティ制御.....	23
5.1	物理的セキュリティ制御.....	23
5.1.1	建物の立地場所及び構造.....	23
5.1.2	物理的アクセス.....	23
5.1.3	電力及び空調.....	23
5.1.4	水害.....	23

5.1.5	防火及び耐火	23
5.1.6	媒体保管	23
5.1.7	廃棄処理	24
5.1.8	オフサイトバックアップ	24
5.1.9	地震	24
5.2	手続き的セキュリティ制御	24
5.2.1	信頼される役割	24
5.2.2	業務ごとの要員数	26
5.2.3	役割ごとの識別と認証	26
5.3	要員のセキュリティ制御	26
5.3.1	経歴、資格、経験及び信頼性要件	26
5.3.2	経歴検査手順	26
5.3.3	トレーニング要件	26
5.3.4	再トレーニング期間及び要件	26
5.3.5	役割交代の期間及び順序	26
5.3.6	許可されない行動に対する罰則	26
5.3.7	要員に対する契約要件	26
5.3.8	要員へ提供される文書	27
6.	技術的セキュリティ制御	28
6.1	鍵ペア生成とインストール	28
6.1.1	鍵ペア生成	28
6.1.2	秘密鍵の配付	28
6.1.3	CA への公開鍵の登録	28
6.1.4	CA 公開鍵の配布	28
6.1.5	鍵長	28
6.1.6	公開鍵パラメータ	28
6.1.7	公開鍵パラメータの質検証	28
6.1.8	ハードウェア/ソフトウェア鍵生成	29
6.1.9	鍵利用目的	29
6.2	秘密鍵保護	29
6.2.1	暗号モジュール標準	29
6.2.2	秘密鍵の複数人制御	29
6.2.3	秘密鍵の預託	29
6.2.4	秘密鍵バックアップ	29
6.2.5	秘密鍵のアーカイブ	29
6.2.6	暗号モジュールへの秘密鍵の登録	29
6.2.7	秘密鍵活性化の方法	30
6.2.8	秘密鍵非活性化の方法	30
6.2.9	秘密鍵破壊の方法	30
6.3	鍵管理に関する他の局面	30

6.3.1	公開鍵保管	30
6.3.2	公開鍵及び秘密鍵の利用期間	30
6.4	活性化データ	31
6.4.1	活性化データの生成及びインストール	31
6.4.2	活性化データの保護	31
6.4.3	活性化データに関する他の局面	31
6.5	コンピュータセキュリティ制御	31
6.5.1	特定のコンピュータセキュリティ技術要件	31
6.5.2	コンピュータセキュリティ評価	31
6.6	ライフサイクル技術制御	31
6.6.1	システム開発	31
6.6.2	セキュリティ管理	32
6.6.3	セキュリティ評価の基準	32
6.7	ネットワークセキュリティ制御	32
6.8	暗号モジュールのエンジニアリング制御	32
7.	証明書及び CRL プロファイル	33
7.1	証明書プロファイル	33
7.2	CRL プロファイル	33
8.	仕様管理	34
8.1	本 CP/CPS の変更管理	34
8.2	開示及び通知	34
8.3	CP/CPS 承認手続き	34
9.	用語集	35
	附則	38
	附則	38
	附則	38
	附則	38
	附則	38
	附則	38
	附則	39
	附則	39
	附則	39

附則39

LGPKI ブリッジ認証局 CP/CPS

平成18年4月1日 総合行政ネットワーク運営協議会制定
改正平成18年9月1日
改正平成18年11月24日
改正平成19年3月20日
改正平成19年5月24日
改正平成19年10月5日
改正平成20年5月28日
改正平成20年10月22日
改正平成21年3月25日
改正平成21年9月29日

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。

なお、本 CP/CPS の構成は、IETF(Internet Engineering Task Force) PKIX(Public-Key Infrastructure X.509) Working Group による RFC(Request For Comment) 2527 「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。

本 CP/CPS の記述においては、RFC2527 で定める項目のすべてを記載する。ただし、他の規程等を参照する場合には、見出しだけを残し、参照内容を明示することとする。

1.1 概要

1.1.1 証明書の種類

ブリッジ CA は、ブリッジ CA に認証を要求し、ブリッジ CA と相互認証を行う外部認証基盤の認証局（以下「相互認証先 CA」という。）に対し、認証を行い、相互認証証明書を発行すると共に、相互認証先 CA に対し認証を要求し、相互認証証明書を受け取る。

また、ブリッジ CA は、LGPKI 組織認証局と相互認証証明書を取り交わす。

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、インターネット側の証明書検証者向けに整備される VA サーバに証明書（以下「VA 証明書」という。）を発行する。

1.1.2 関連規程

LGPKI 及びブリッジ CA の関連規程を以下に示す。本 CP/CPS は、必要に応じて関連規程を参照する。

- ・総合行政ネットワーク基本要綱

- ・ 地方公共団体組織認証基盤の運営に関する基本綱領

1.2 識別

ブリッジ CA の証明書ポリシーの識別子は、次のとおりとする。

- ・ 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]
- ・ VA 証明書ポリシー:[1.2.392.200110.10.8.5.1.3.1]

1.3 運営体制及び証明書適用範囲

1.3.1 運営体制

組織と体制図を以下に示す。

ブリッジ CA を構成する組織は、図 1-1 に示すとおり意思決定組織及び運営組織である。

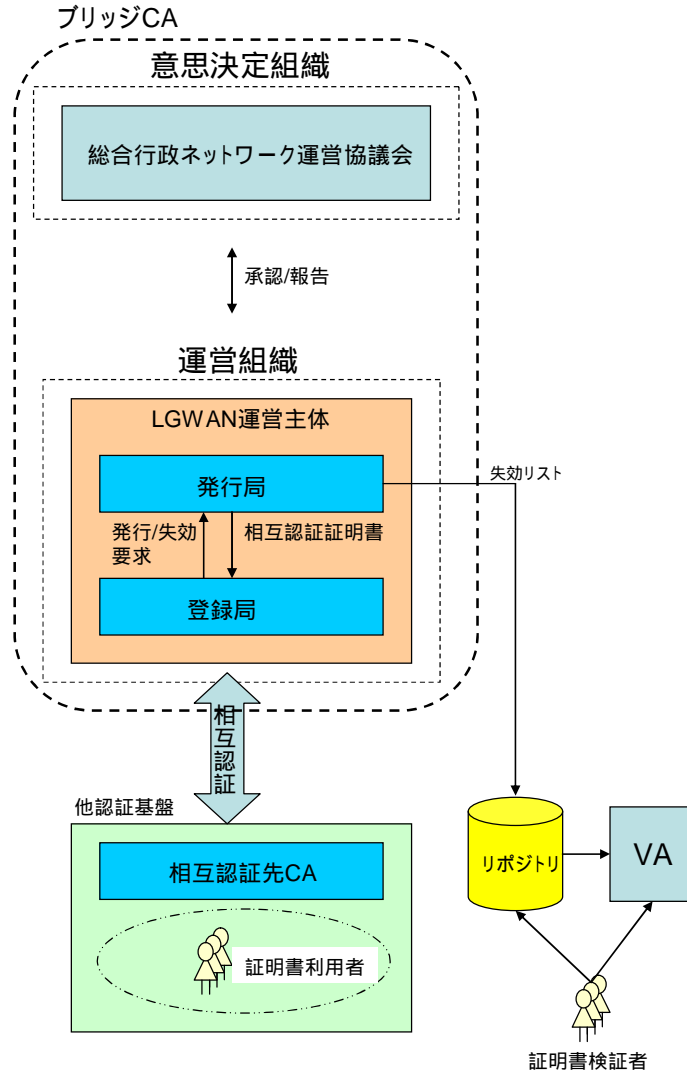


図 1-1 組織と体制

構成組織とその役割を以下に示す。

表 1-1 構成組織と役割

構成組織	役割
総合行政ネットワーク 運営協議会	ブリッジ CA の運営に関する意思決定組織として、次に挙げる事項の決定を行う。 <ul style="list-style-type: none"> ・ブリッジ CA の CP/CPS の制定及び改正 ・相互認証 ・CA 秘密鍵危殆化時の対応 ・災害発生等による緊急時の対応 ・その他ブリッジ CA の運営に関する重要事項
LGMAN 運営主体	ブリッジ CA の運営組織として、主に次の業務を行う。 <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 ・ブリッジ CA の運営 ・CA システムの運用及び維持管理 (登録局) ・相互認証証明書の発行、更新、失効申請の受付及び審査 ・相互認証証明書の発行及び失効の要求 (発行局) ・相互認証証明書、VA 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、リポトリ操作員、VA 操作員及び監査ログ検査者</p>
証明書利用者	相互認証先 CA に属する相互認証証明書の管理者又は VA サーバの管理者であり、本 CP/CPS に従い相互認証証明書又は VA 証明書を利用する。
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。

1.3.2 適用性・適用環境等

相互認証証明書及び VA 証明書（以下「相互認証証明書等」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。

- ・相互認証証明書

地方公共団体間及び外部認証基盤との相互認証を実現するために、LGPKI 組織認証局及び相互認証先 CA（以下「相互認証先 CA 等」という。）と相互認証証明書を取り交わす。

相互認証証明書の適用により、相互認証先 CA 等の証明書利用者に対し、ブリッジ CA を介して証明書検証を可能とする。

相互認証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 5 年とする。

- ・VA 証明書

総合行政ネットワークにおいて運用する VA サーバに適用する。

VA 証明書の適用により、VA サーバを運営する組織の実在性証明並びに証明書検証結果が改ざんされていないことを保証できる。

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 1 年とする。

1.4 CP/CPS に関する連絡先

1.4.1 管理組織

本 CP/CPS の変更及び更新等に関する事務は、LGWAN 運営主体が行い、決定は総合行政ネットワーク運営協議会（以下「LGWAN 運営協議会」という。）が行う。

1.4.2 連絡先

本 CP/CPS に関する照会は、LGWAN 運営主体を窓口とする。窓口の連絡先は、以下の URL に掲示する。

URL <http://www.lgpki.jp/>

2. 一般規定

2.1 義務

2.1.1 発行局の義務

発行局に関する義務を以下に定める。

- ・本 CP/CPS に基づき、自己署名証明書、リンク証明書及び相互認証証明書等を発行する。
- ・証明書の失効処理を行い、有効期間 48 時間の CRL/ARL を通常運用時には 24 時間ごとに発行する。
- ・CA 秘密鍵を安全に管理する。
- ・CA 秘密鍵が危殆化した場合には、速やかに認証局最高責任者及び相互認証先 CA の運営組織に報告し、定められた手順に従い対処を行う。
- ・相互認証先 CA 等からの相互認証証明書の発行要求に含まれる公開鍵が、確実に相互認証先 CA 等の公開鍵であり、かつ、相互認証先 CA 等がこの公開鍵に対する秘密鍵を保有していることを確認する。
- ・発行する証明書プロファイル情報の定義及び保管を行う。
- ・証明書の発行、更新及び失効等に関する監査ログ及びアーカイブデータを必要な期間保管する。
- ・発行申請情報の保管、発行情報の改ざん検出、IA システムにおける機密情報の暗号化及びアクセスコントロールを行う。
- ・システムの稼働監視は常時的確に行い、24 時間 365 日の安定的な運用を目標とする。

2.1.2 登録局の義務

登録局に関する義務を以下に定める。

- ・相互認証先 CA からの相互認証証明書の発行、更新及び失効申請又は VA 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、受付及び審査を行う。
- ・相互認証先 CA に対して、相互認証証明書の発行要求及び失効要求を行う。
- ・相互認証証明書の発行、更新及び失効に係る申請は、正確な情報に基づくものとする。
- ・各申請手続きにおいて入手した相互認証先 CA の情報を安全に保管する。

2.1.3 証明書利用者の義務

証明書利用者は、次の義務を負う。

- ・相互認証証明書等の発行、更新及び失効に係る申請は、正確な情報に基づくものとする。

- ・相互認証証明書等は、本 CP/CPS に従って利用する。
- ・相互認証証明書等及びその秘密鍵を安全に管理する。
- ・秘密鍵が危殆化した場合は、速やかに LGWAN 運営主体に報告する。
- ・相互認証証明書等は、本 CP/CPS 「1.3.2 適用性・適用環境等」に規定する用途以外で使用しない。

2.1.4 証明書検証者の義務

証明書検証者は、次の義務を負う。

- ・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、本 CP/CPS 「1.3.2 適用性・適用環境等」に規定する用途で利用されている証明書のみを検証対象とする。

2.1.5 リポジトリの義務

リポジトリは、次の義務を負う。

- ・本 CP/CPS 「2.6.1 CA に関する情報の公開」に規定する情報の公表を行う。
- ・統合リポジトリに登録された情報の一部を、公開リポジトリに複製する。
- ・原則として、24 時間 365 日の安定的な運用を行う。
- ・登録された情報の保護を行う。

ただし、保守等により一時的に運用を停止する場合がある。

2.1.6 VA の義務

VA は、次の義務を負う。

- ・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。
- ・有効性確認問合わせに対する検証結果に電子署名を行う。
- ・原則として、24 時間 365 日の安定的な運用を行う。

ただし、保守等により一時的に運用を停止する場合がある。

2.2 責務

2.2.1 発行局の責務

発行局は、本 CP/CPS に基づいて自己署名証明書、リンク証明書及び相互認証証明書等の発行、更新、失効、保管及び公表を適切に行う。ブリッジ CA は、発行した証明書の内容について責任を持つ。ブリッジ CA は、これらの情報に電子署名を付与しているが、第三者による改ざん及び攻撃法の発見等による署名アルゴリズムの陳腐化があった場合、その内容は保証しない。

2.2.2 登録局の責務

登録局は、相互認証証明書等の発行、更新及び失効申請の受付と審査に関し責任を持つ。

2.2.3 証明書利用者の責務

相互認証証明書等の証明書利用者は、発行された相互認証証明書等に対する秘密鍵に関し責任を持つ。

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。

2.2.5 リポジトリの責務

リポジトリは、本 CP/CPS 「2.1.5 リポジトリの義務」に規定する運用時間において、正当な情報検索要求に対する応答を返却する。

リポジトリは、公表する CRL/ARL に関して、証明書検証者が検証した時点における、最新の有効性情報が反映された CRL/ARL であることを保証しない。

2.2.6 VA の責務

VA は、本 CP/CPS に規定する運用時間において、正当な証明書有効性検証要求に対する応答を返却する。

VA は、検証結果に関して責任を持つ。

2.3 財産権に関する責任

ブリッジ CA は、本 CP/CPS 「2.1 義務」及び「2.2 責務」に規定する事項の履行において、故意又は重大な過失がある場合を除き、一切の損害賠償責任を負わない。

2.4 解釈と実行

2.4.1 準拠法

本 CP/CPS に基づく認証業務から生ずる紛争については、日本国の法令及び例規を適用する。

2.4.2 分離可能性条項、残存規定条項、完全合意条項及び通知条項

ブリッジ CA の分離可能性条項、残存規定条項、完全合意条項及び通知条項を以下に定める。

(1)分離可能性条項

本 CP/CPS のいずれかの規定が無効又は違法であっても、本 CP/CPS のほかの規定はそれになんら影響を受けることなく有効とする。

(2)残存規定条項

証明書利用者又は証明書検証者が、本 CP/CPS に対する同意を解除し又は取り消した場合であっても、本 CP/CPS 「2.1 義務」、「2.2 責務」、「2.3 財産権に関する責任」、

「2.4 解釈と実行」、「2.5 料金」、「2.8 機密性のポリシー」及び「2.9 知的財産権」に規定する事項はそのまま有効とする。

(3)完全合意条項

本 CP/CPS は、同意時現在におけるブリッジ CA、証明書利用者及び証明書検証者の合意を規定したものであり、同意以前に当事者間でなされた協議内容、合意事項又は一方当事者から他の当事者に提供された資料、申入れその他の通信と本 CP/CPS の内容が相違する場合は、本 CP/CPS が優先するものとする。

(4)通知条項

本 CP/CPS 上必要とされ、又は許容されるブリッジ CA に対する通知、請求、要求、依頼その他の連絡は LGWAN 運営主体を窓口とする。LGWAN 運営主体の連絡先は本 CP/CPS 「1.4.2 連絡先」に規定する。

2.4.3 紛争解決手続き

ブリッジ CA、証明書利用者及び証明書検証者は、本 CP/CPS に関する紛争について、東京地方裁判所を第一審専属管轄裁判所とする裁判によって最終的に解決されることに合意する。ただし、東京簡易裁判所に調停の申立てをすることを妨げない。

2.5 料金

証明書の利用に係る料金は、LGWAN 運営協議会が別に定める。

2.6 公表情報に関する規定

2.6.1 CA に関する情報の公表

ブリッジ CA に関する情報は、統合リポジトリ、公開リポジトリ及び Web サーバ上で公表する。なお、Web サーバには、LGWAN を通じて地方公共団体に提供する Web サーバ（以下「地方公共団体向け Web サーバ」という。）及びインターネットを通じて住民・企業等に提供する公開 Web サーバ（以下「公開 Web サーバ」という。）がある。

(1)リポジトリ上での公表

(統合リポジトリ)

- ・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
- ・相互認証先 CA からの相互認証証明書
- ・政府認証基盤が公開している証明書情報
- ・組織 CA からの相互認証証明書

詳細は、地方公共団体向け Web サーバに公表する技術仕様書に定める。

(公開リポジトリ)

- ・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
- ・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
- ・組織 CA への相互認証証明書

詳細は、公開 Web サーバに公表する技術仕様書に定める。

(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
- ・ CA 秘密鍵危殆化に関する情報
- ・ブリッジ CA CP/CPS
- ・ブリッジ CA CP/CPS の改正履歴
- ・ブリッジ CA の自己署名証明書
- ・ブリッジ CA 自己署名証明書のフィンガープリント
- ・プロファイル設計書
- ・技術仕様書

(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
- ・ CA 秘密鍵危殆化に関する情報
- ・ブリッジ CA CP/CPS
- ・ブリッジ CA CP/CPS の改正履歴
- ・ブリッジ CA の自己署名証明書
- ・ブリッジ CA 自己署名証明書のフィンガープリント
- ・プロファイル設計書
- ・技術仕様書

2.6.2 公表の頻度

公表する情報の更新頻度は、次のとおりとする。

- ・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
- ・プロファイル設計書及び技術仕様書の変更の都度
- ・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相互認証先 CA の名称は、LGWAN 運営協議会による決定の都度

2.6.3 アクセスコントロール

公開リポジトリ及び公開 Web サーバ上で公表する情報は、インターネットを通じて提供する。公表情報を提供するに当たっては、特段のアクセス制御は行わない。統合リポジトリ及び地方公共団体向け Web サーバ上で公表する情報は、LGWAN を通じて地方公共団体のみに提供する。

2.6.4 リポジトリ

統合リポジトリに保有する情報のうち、本 CP/CPS 「2.6.1 CA に関する情報の公表 (1)

「リポジトリ上での公表」に規定する情報を公開リポジトリに複製し、公開リポジトリ上で公表する。

2.7 準拠性監査

本 CP/CPS 及び関連規程に基づき、認証業務が適正に行われていることを確認するために、ブリッジ CA に対して準拠性監査を実施する。

2.7.1 準拠性監査の頻度

準拠性監査は、少なくとも年 1 回定期的を実施する。また、必要に応じて随時に実施する場合がある。

2.7.2 監査人の識別及び資格

ブリッジ CA の準拠性監査は、監査業務及び認証業務について十分な知識と経験を有する者が行う。

2.7.3 監査人と被監査者との関係

ブリッジ CA の監査人は、監査対象となる業務に携わっていない者とする。

2.7.4 監査項目

ブリッジ CA の監査人による監査は、ブリッジ CA が本 CP/CPS 及び関連規程に準拠して、認証業務を適切に行っていること、並びに外部からの不正行為及び内部の不正行為に対する措置が適切に講じられていることを主な対象として実施する。

2.7.5 監査指摘事項への対応

ブリッジ CA は、重要又は緊急を要する監査指摘事項については、速やかに対応する。CA 秘密鍵の危殆化に関する指摘があった場合は緊急事態と位置付け、緊急時対応の手続きをとる。重要又は緊急を要する監査指摘事項があった場合は、改善されるまでの間、LGWAN 運営協議会の決定により運営を停止することがある。LGWAN 運営協議会は、監査指摘事項への対策を実施したことを確認する。

2.7.6 監査結果の通知

ブリッジ CA の監査人は、監査を終了したときは、監査報告書を作成する。監査報告書には、以下に掲げる事項を記載する。

- ・ 監査を実施した年月日
- ・ 監査の概要
- ・ 監査の結果

ブリッジ CA の監査人は、作成した監査報告書を LGWAN 運営主体に提出する。LGWAN 運営主体は、LGWAN 運営協議会に対し監査の結果を報告する。また、LGWAN 運営主体は、LGWAN 運営協議会の指示により、相互認証先 CA に対し、監査の結果を報告する。

なお、監査の証跡及び改善措置を含む監査報告書は、機密事項として扱うものとし、契約等によって特段の定めがある場合を除き非公開とする。監査報告書は、5 年間保管する。

2.8 機密性のポリシー

2.8.1 機密情報

ブリッジ CA は、漏えいすることによって認証業務の信頼性が損なわれる恐れのある情報を機密扱いとする。機密扱いとする情報は、当該情報を含むデータ及びファイルの管理責任者を定め、「電気通信事業法」及び「個人情報の保護に関する法律」等の関連法令に基づき、安全に保管管理する。

2.8.2 機密情報対象外の情報

ブリッジ CA が保有する情報のうち、証明書及び失効情報等公表する情報として明示的に示すものは、機密扱いの対象とはしない。

2.8.3 失効情報の開示

ブリッジ CA は、発行した証明書の失効情報を公開する。失効理由の詳細は開示しない。

2.8.4 法律執行者への開示

法的根拠に基づいて法律執行機関から情報を開示するように正式な要求があった場合には、これを開示する。

2.8.5 民事手続き上の情報開示

ブリッジ CA は、司法手続き、又は行政手続きに基づいて、本 CP/CPS「2.8.1 機密情報」に規定した機密保持対象情報を開示する場合がある。

2.8.6 証明書利用者本人の要求に基づく開示

証明書利用者がブリッジ CA に提示した情報について、当該証明書利用者から開示要求が行われた場合は開示する。

2.8.7 その他の情報開示状況

規定しない。

2.9 知的財産権

ブリッジ CA が相互認証先 CA に対して発行する相互認証証明書の鍵ペア及び主体者名は、証明書利用者に知的財産権が帰属するものとする。

CA 鍵ペア、ブリッジ CA が発行する相互認証証明書等、CRL/ARL、自己署名証明書、リンク証明書及び本 CP/CPS の知的財産権は、ブリッジ CA に帰属するものとする。

3. 識別及び認証

3.1 初期登録

3.1.1 名前の型

相互認証証明書等の発行者名及び主体者名は、X.500 識別名 (DN:Distinguished Name) の形式に従って設定する。

3.1.2 名前の意味

相互認証証明書等において使用する名前は、証明書利用者が定める名称及びブリッジ CA が定める名称とする。

3.1.3 多様な名前形式の解釈のルール

名前の形式を解釈するためのルールは、ブリッジ CA が定める規則等に従う。

3.1.4 名前の一意性

相互認証証明書等の主体者名は、一意に割り当てる。

3.1.5 名前に関する係争の解決手段

名前に関する紛争があった場合は、ブリッジ CA が決定権限を有するものとする。

3.1.6 登録商標の認知、認証及び役割

登録商標に関する制約、取扱い及び紛争について以下に定める。

- ・証明書利用者は、他者の登録商標を侵害するような申請をしてはならない。
- ・ブリッジ CA は、登録商標が証明書利用者に帰属するかに関する検証は行わない。
- ・ブリッジ CA は、登録商標の帰属に関する紛争の仲裁、調停等を行わない。
- ・ブリッジ CA は、登録商標の帰属に関する紛争を理由として、申請を却下することができる。

3.1.7 秘密鍵の所有証拠の確認手段

(1)相互認証証明書

相互認証先 CA 等から提出された証明書発行要求の電子署名の検証を行い、含まれている CA 公開鍵とペアとなる CA 秘密鍵で電子署名されていることを確認する。また、証明書発行要求のフィンガープリントを確認し、CA 公開鍵の所有者を特定する。

(2)VA 証明書

証明書発行要求の電子署名の検証を行い、含まれている公開鍵に対応する秘密鍵で電子署名されていることを確認する。

3.1.8 組織的な識別

ブリッジ CA は、相互認証証明書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。

3.1.9 個人の識別

規定しない。

3.2 通常の更新

相互認証証明書等更新時における識別及び認証は、本 CP/CPS「3.1 初期登録」に規定する手続きに基づいて行う。

3.3 失効後の鍵更新

相互認証証明書等失効後の再発行時における識別及び認証は、本 CP/CPS「3.1 初期登録」に規定する手続きに基づいて行う。

3.4 失効要求

相互認証証明書等の失効時における識別及び認証は、本 CP/CPS「3.1.8 組織的な識別」に規定する手続きに基づいて行う。

4. 運用要件

4.1 証明書申請

(1)相互認証証明書

相互認証証明書の発行申請は、相互認証先 CA と合意した手続きに基づいて行う。

(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。

4.2 証明書発行

(1)相互認証証明書

ブリッジ CA は、相互認証先 CA 等から提出された証明書発行要求に対し、自 CA の電子署名を付して相互認証証明書を発行する。

(2) VA 証明書

ブリッジ CA は、VA 側で生成した公開鍵に、自 CA の電子署名を付して VA 証明書を発行する。

4.3 証明書受入れ

(1)相互認証証明書

ブリッジ CA は、発行した相互認証証明書を所定の手続きに基づき、安全かつ確実な方法で相互認証先 CA 等に配付する。相互認証先 CA 等においても、同様に、発行した相互認証証明書を、所定の手続きに基づきブリッジ CA に配付する。

相互認証証明書の受渡しは、認証局システム責任者が双方の相互認証証明書の配付確認を行うことにより、完了とする。

なお、相互認証先 CA との相互認証証明書の受渡しについては、相互認証先 CA と合意した手続きに基づいて行う。

(2) VA 証明書

ブリッジ CA は、発行した VA 証明書を所定の手続きに基づき、安全かつ確実な方法で配付する。

4.4 証明書一時停止と失効

4.4.1 失効要件

(1)相互認証証明書

- ・ CA 秘密鍵の危殆化
- ・ 相互認証基準違反（対政府認証基盤）
- ・ 相互認証業務の終了
- ・ 相互認証更新

(2) VA 証明書

- ・ CA 秘密鍵の危殆化
- ・ VA 秘密鍵の危殆化
- ・ 証明書記載事項の変更
- ・ 証明書の利用停止
- ・ 鍵格納媒体の不良、破損
- ・ ブリッジ CA の責めに帰すべき事由による証明書の誤発行等、認証局システム責任者が必要と判断した場合

4.4.2 失効申請者

(1)相互認証証明書

- ・ 失効申請を受ける場合
相互認証先 CA 等からブリッジ CA に対する失効申請は、相互認証先 CA 等の責任者が行う。
- ・ 失効申請を行う場合
ブリッジ CA から相互認証先 CA 等に対する失効申請は、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。

(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。

4.4.3 失効要求手続き

(1)相互認証証明書

- ・ 失効申請を受ける場合
本 CP/CPS 「3.1.8 組織的な識別」に規定する手続きを行い、要求された相互認証証明書を失効し、ARL をリポジトリに登録する。
- ・ 失効申請を行う場合
所定の手続きに従い、失効申請を行う。相互認証証明書を失効し、ARL をリポジトリに登録する。

(2) VA 証明書

認証局システム責任者の指示に基づき、VA 証明書を失効し、CRL をリポジトリに登録する。

4.4.4 失効猶予期間

ブリッジ CA は、失効申請手続きの終了後、直ちに失効処理を行う。失効処理完了後の CRL/ARL の発行については、本 CP/CPS 「4.4.9 CRL/ARL 発行頻度」に規定する。

4.4.5 一時停止要件

相互認証証明書等の一時停止は、行わない。

4.4.6 一時停止申請者

規定しない。

4.4.7 一時停止要求手続き

規定しない。

4.4.8 一時停止期間

規定しない。

4.4.9 CRL/ARL 発行頻度

有効期間 48 時間の CRL/ARL を通常運用時には 24 時間ごとに発行する。ただし、CA 秘密鍵の危殆化等が発生した場合には、CRL/ARL を直ちに発行する。

4.4.10 CRL/ARL 検証要件

相互認証証明書の証明書検証者は、リポジ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。

4.4.11 オンライン有効性検証・状態検証

オンラインでの有効性検証は、リポジトリ及び VA によって提供される。

4.4.12 オンライン有効性検証・状態検証要件

オンラインでの有効性検証は、リポジトリに公開されるブリッジ CA の発行する CRL/ARL 並びに VA への問い合わせによって、行なわなければならない。

4.4.13 失効を公知する他の手法

規定しない。

4.4.14 失効を公知する他の手法の検証要件

規定しない。

4.4.15 鍵危殆化による特別な要件

規定しない。

4.5 セキュリティ監査手続き

監査ログ検査者は、ブリッジ CA における発生事象を記録したログ（以下「監査ログ」

という。)を業務実施記録等と照合し、不正操作等異常な事象を確認するセキュリティ監査を行う。

4.5.1 記録事象

ブリッジ CA におけるセキュリティに関する重要な事象を対象に、アクセスログ、操作ログ等の監査ログを記録する。監査ログには、次の情報を含める。

- ・事象の種類
- ・事象が発生した日付及び時刻
- ・各種処理の結果
- ・事象の発生元の識別情報（操作員名、システム名等）

4.5.2 監査ログの監査頻度

監査ログ検査者は、業務実施記録等と監査ログとの照合を原則として週次で行う。ただし、認証局システム責任者が認める場合には、監査ログ検査の時期を変更することができる。

4.5.3 監査ログの保管期間

監査ログは、3年間保管する。

4.5.4 監査ログの保護

監査ログは、改ざん防止対策を施し、かつ、改ざん検出を可能とする。

監査ログのバックアップは、週次で外部記憶媒体に取得し、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管する。

なお、監査ログの閲覧及び削除は、監査ログ検査者が行う。

4.5.5 監査ログのバックアップ手続き

監査ログは、日次でバックアップし、週次で外部記憶媒体に取得する。

4.5.6 監査ログシステム

監査ログの収集機能は、IA システムの一機能とし、セキュリティに関する重要な事象をシステムの起動時から監査ログとして収集する。

4.5.7 記録事象の通知

監査ログの検査は、事象を発生させた者に通知することなく行う。

4.5.8 脆弱性の検証

監査ログを検査することにより、IA システムの運用面及び技術面におけるセキュリティ上の脆弱性を評価する。

4.6 アーカイブ

4.6.1 アーカイブデータの種類

アーカイブデータは、次のものとする。

- ・発行した証明書、証明書要求
- ・CRL/ARL の発行履歴
- ・IA システムの起動、停止履歴
- ・IA システムの操作履歴

4.6.2 アーカイブデータの保管期間

30 年間保管する。

4.6.3 アーカイブデータの保護

アーカイブデータには、アクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。アーカイブデータのバックアップは、月次で外部記憶媒体に取得し、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管する。

4.6.4 アーカイブデータのバックアップ手順

アーカイブデータは、日次でバックアップし、月次で外部記憶媒体に取得する。

4.6.5 レコードのタイムスタンプ要件

アーカイブデータには、レコード単位でタイムスタンプを付与する。

4.6.6 アーカイブデータの収集システム

規定しない。

4.6.7 アーカイブデータの検証手順

アーカイブデータが記録された外部記憶媒体は、少なくとも年 1 回は可読性の確認を行う。

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 鍵ペア更新時には、古い CA 公開鍵及び新しい CA 公開鍵の認証パスを構築するリンク証明書を発行し、リポジトリ上で公表する。

(2)VA 鍵

証明書利用者の鍵ペアは、1 年以内に更新を行う。

4.8 鍵の危殆化及び災害からの復旧

4.8.1 ハードウェア、ソフトウェア及びデータ破壊からの復旧手段

ハードウェア、ソフトウェア及びデータが破壊された場合には、バックアップ用に準備されたハードウェア、ソフトウェア及びデータにより、速やかに復旧作業を行う。なお、復旧に必要なソフトウェア及びデータは、定期的又は必要に応じて取得する。

4.8.2 証明書が失効した場合の復旧手段

発行した証明書の失効処理に当たっては、その失効の取消しは、行わない。相互認証証明書等を失効後、再度、相互認証証明書等を発行する場合には、あらためて発行手続きを行う。

4.8.3 秘密鍵が危殆化した場合の復旧手段

証明書利用者が CA 秘密鍵の危殆化を発見した場合は、速やかに LGWAN 運営主体に報告する。

認証局運営要員が CA 秘密鍵の危殆化を発見した場合は、速やかに認証局システム責任者を經由して認証局最高責任者に報告し、所定の手続きに基づいて認証業務を停止し、次の手続きを行う。

- ・ 相互認証証明書等の失効
- ・ CA 秘密鍵の廃棄及び再生成
- ・ 相互認証証明書等の再発行

また、VA 証明書の秘密鍵が危殆化した場合には、本 CP/CPS 「4.4 証明書一時停止と失効」に規定する手続きに基づき、証明書の失効手続きを行う。

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

災害等によりブリッジ CA の設備が被害を受けた場合には、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。

- ・ 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。
- ・ 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。
- ・ 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。

4.9 認証業務の終了

認証業務の終了は、LGWAN 運営協議会において決定する。LGWAN 運営主体は、決定に基づき、以下の内容を業務終了 90 日前までに証明書利用者及び証明書検証者に告知する。

- ・ 業務終了の事実
- ・ 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

イブデータ等の保管組織及び開示方法
告知後、所定の業務終了手続きを行う。

5. 物理的、手続き的及び要員のセキュリティ制御

5.1 物理的セキュリティ制御

5.1.1 建物の立地場所及び構造

ブリッジ CA の施設は、水害、地震、火災その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火及び不正侵入防止のための対策を講ずる。また、使用する機器等を災害及び不正侵入から防護された安全な場所に設置する。

5.1.2 物理的アクセス

実施される認証業務の重要度に応じ、複数のセキュリティレベルで物理的アクセス管理を行う。ブリッジ CA の施設は、操作権限者が識別できる IC カード及び生体認証装置により認証を行う。

物理的アクセス権限は、本 CP/CPS「5.2 手続き的セキュリティ制御」に規定する各要員の業務に応じて、別に定める認証基盤設備室入退室管理責任者が付与する。ブリッジ CA の施設は、監視員の配置及び監視システムにより 24 時間 365 日監視を行う。

5.1.3 電力及び空調

ブリッジ CA は、機器等の運用のために十分な容量の電源を確保するとともに、瞬断、停電、電圧・周波数の変動に備えた対策を講ずる。商用電源が供給されない事態においては、一定時間内に発電機による電源供給に切り換える。また、空調設備を設置することにより機器類の動作環境及び認証局運営要員の作業環境を適切に維持する。

5.1.4 水害

ブリッジ CA の設備を設置する建物及び室には、漏水検知器を設置し、天井及び床には、防水対策を講ずる。

5.1.5 防火及び耐火

ブリッジ CA の設備を設置する建物は耐火構造及び室は防火区画とし、自動火災報知設備及び消火設備を適切に設置する。

5.1.6 媒体保管

アーカイブデータ及びバックアップデータを含む媒体は、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管するとともに、所定の手続きに基づき適切に搬入出管理を行う。

5.1.7 廃棄処理

機密扱いとする情報を含む書類及び記憶媒体の廃棄については、所定の手続きに基づいて適切に廃棄処理を行う。

5.1.8 オフサイトバックアップ

重要なデータ等の媒体を別地保管するに当たっては、移送経路のセキュリティを確保するとともに、媒体保管の施設は、適切なセキュリティ対策を施した施設とする。

5.1.9 地震

ブリッジ CA の設備を設置する建物は耐震構造とし、機器・什器の転倒及び落下を防止する対策を講ずる。

5.2 手続き的セキュリティ制御

5.2.1 信頼される役割

各要員の業務を次のとおり定める。

(ブリッジ CA)

(1) 認証局最高責任者

認証局最高責任者は、ブリッジ CA の運営に関する責任者であり、次の業務を行う。

- ・ブリッジ CA の運営方針の策定
- ・CA 秘密鍵の危殆化発生時、災害発生時等緊急時における対応の統括
- ・ブリッジ CA の業務手続きに関する内規の改正の承認
- ・認証局運営要員の任命、解任
- ・認証局運営要員の任命、解任に伴う別に定める認証基盤設備室入退室管理責任者に対する入退室権限の追加及び削除依頼
- ・認証局運営要員の教育計画の作成及び実施報告書の管理

(2) 認証局システム責任者

認証局システム責任者は、認証業務及び CA システムの運用に関する責任者であり、次の業務を行う。

- ・認証業務の統括
- ・認証局運営要員への作業指示及び作業結果の確認
- ・その他ブリッジ CA の運用に関する統括
- ・HSM の機能を制御する鍵（以下「管理鍵」という。）及び PIN の保管管理

認証局システム責任者に事故等があった場合、あらかじめ定められた者が職務を代行できるように、認証局システム責任者は、複数人任命する。

(3) 鍵管理者

鍵管理者は、CA 秘密鍵を使用する業務に関する責任者であり、次の業務を行う。

なお、作業は複数の鍵管理者が行う。

- ・CA 秘密鍵のバックアップ媒体の保管管理
- ・CA 秘密鍵生成及び自己署名証明書発行時の HSM に対する操作
- ・CA 秘密鍵の更新時における HSM に対する操作
- ・CA 秘密鍵のバックアップ、バックアップからのリストア時の HSM に対する操作及び CA 秘密鍵のバックアップ媒体のセット

(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。

(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。

(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。

(7) IA 操作員

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。なお、作業は複数の IA 操作員が行う。

- ・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等の発行、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

(8) RA 操作員

RA 操作員は、相互認証証明書等の発行申請及び失効申請業務を行う。なお、作業は複数の RA 操作員が行う。

(9) リポジトリ操作員

リポジトリ操作員は、統合リポジトリ及び公開リポジトリの設定管理に関する業務を行う。

(10) VA 操作員

VA 操作員は、VA システムに対する証明書の設定等に関する業務を行う。

(11) 監査ログ検査者

監査ログ検査者は、IA システムのログに関する次の業務を行う。

- ・監査ログの検査
- ・不要な監査ログの削除

5.2.2 業務ごとの要員数

証明書の発行、更新及び失効等の重要な業務の実施に当たっては、要員の職務権限を分離し、相互牽制を行う。CA 秘密鍵操作を行う鍵管理者は、複数人任命する。

5.2.3 役割ごとの識別と認証

業務の指示は、認証局システム責任者が各要員に対して指示を行う。各要員が CA システム操作を行う際、システムは、要員が正当な権限者であることの識別・認証を行う。

5.3 要員のセキュリティ制御

5.3.1 経歴、資格、経験及び信頼性要件

認証局運営要員は、次のとおりとする。

- ・ LGWAN 運営主体の役職員
- ・ 契約に基づく委託要員
- ・ 労働者派遣事業の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律に基づく派遣労働者

5.3.2 経歴検査手順

LGWAN 運営主体は、所定の手続きに基づき要員の経歴と信頼性を確認する。

5.3.3 トレーニング要件

認証局運営要員は、任命時、業務遂行に必要な教育を受けなければならない。

5.3.4 再トレーニング期間及び要件

認証局運営要員は、業務が変更された場合、新しい業務内容について教育を受けなければならない。

5.3.5 役割交代の期間及び順序

規定しない。

5.3.6 許可されない行動に対する罰則

認証局運営要員は、許可されない行動を行った場合、就業規則又は契約等の定めるところにより罰則を受ける場合がある。

5.3.7 要員に対する契約要件

LGWAN 運営主体は、認証局運営業務の一部を委託する場合は、委託先との間で委託業務に関する機密保持義務を含む適切な契約を締結する。

5.3.8 要員へ提供される文書

LGWAN 運営主体は、認証局運営要員に対し、任命した役割に応じて必要な文書を開示する。

6. 技術的セキュリティ制御

6.1 鍵ペア生成とインストール

6.1.1 鍵ペア生成

(1)CA 鍵

CA 鍵ペアは、複数の鍵管理者が FIPS140-1 レベル 3 相当の HSM を用いて生成する。

(2)VA 鍵

VA の鍵ペアは、複数の鍵管理者が FIPS140-1 レベル 3 相当の HSM を用いて生成する。

6.1.2 秘密鍵の配付

規定しない。

6.1.3 CA への公開鍵の登録

ブリッジ CA は、相互認証証明書の取り交わしにおいて、相互認証先 CA 等の公開鍵を安全かつ確実に受け取る。

VA の公開鍵は、VA からの証明書発行要求に含まれる。

6.1.4 CA 公開鍵の配布

ブリッジ CA の自己署名証明書は、本 CP/CPS「2.6.1CA に関する情報の公開(2)」に規定する LGWAN 参加団体向け Web サーバ及び公開 Web サーバ等により配布される。

配布されたブリッジ CA の自己署名証明書は、自己署名証明書を配布した Web サーバで公開するフィンガープリントによって確認される。CA の自己署名証明書及びフィンガープリントは、SSL 通信を用いて公開する。

6.1.5 鍵長

(1)CA 鍵

RSA2048 ビット長の鍵を使用する。

(2) VA 鍵

RSA1024 ビット長の鍵を使用する。

6.1.6 公開鍵パラメータ

規定しない。

6.1.7 公開鍵パラメータの質検証

規定しない。

6.1.8 ハードウェア/ソフトウェア鍵生成

本 CP/CPS 「6.1.1 鍵ペア生成」に規定する。

6.1.9 鍵利用目的

以下に定める利用目的以外には、鍵を利用しないものとする。

(1)CA 鍵

CA 秘密鍵は、電子署名に用いる。

(2)VA 鍵

VA の秘密鍵は、電子署名に用いる。

6.2 秘密鍵保護

6.2.1 暗号モジュール標準

(1)CA 鍵

CA 秘密鍵は、FIPS140-1 レベル 3 相当の HSM により保護する。

(2)VA 鍵

VA の秘密鍵は、FIPS140-1 レベル 3 相当の HSM により保護する。

6.2.2 秘密鍵の複数人制御

CA 秘密鍵は、複数の鍵管理者の合議により、制御及び管理される。

6.2.3 秘密鍵の預託

秘密鍵の預託は、これを行わない。

6.2.4 秘密鍵バックアップ

CA 秘密鍵のバックアップは、複数の鍵管理者が行う。HSM からバックアップした CA 秘密鍵は、暗号化して複数に分割し、複数の鍵管理者によって安全に保管する。

VA の秘密鍵バックアップは、ブリッジ CA では行わない。

6.2.5 秘密鍵のアーカイブ

秘密鍵のアーカイブは、これを行わない。

6.2.6 暗号モジュールへの秘密鍵の登録

(1)CA 鍵

CA 秘密鍵は、複数の鍵管理者が HSM の中で生成し、格納する。

(2)VA 鍵

VA の秘密鍵は、複数の鍵管理者が HSM の中で生成し、格納する。

6.2.7 秘密鍵活性化の方法

(1)CA 鍵

CA 秘密鍵は、複数の IA 操作員により管理鍵を用いて活性化する。

(2)VA 鍵

VA の秘密鍵は、定められた管理者により、PIN を用いて活性化する。

6.2.8 秘密鍵非活性化の方法

(1)CA 鍵

CA 秘密鍵は、複数の IA 操作員により管理鍵を用いて非活性化する。

(2)VA 鍵

VA の秘密鍵は、定められた管理者により非活性化する。

6.2.9 秘密鍵破壊の方法

(1)CA 鍵

HSM 内の CA 秘密鍵の破棄は、複数の鍵管理者が HSM を初期化することによって行う。また、バックアップ媒体内の CA 秘密鍵の破棄は、複数の鍵管理者がバックアップ媒体を初期化することによって行う。

HSM を室外に持ち出す場合は、複数の鍵管理者が HSM を初期化する。また、破棄する CA 秘密鍵のバックアップ媒体を室外へ持ち出す場合は、複数の鍵管理者が、CA 秘密鍵のバックアップ媒体を初期化する。

(2)VA 鍵

VA の秘密鍵の破棄は、所定の手続きに従い行う。

6.3 鍵管理に関する他の局面

6.3.1 公開鍵保管

公開鍵は、証明書のアーカイブに含まれ、本 CP/CPS「4.6.2 アーカイブデータの保管期間」に規定する期間において保管する。

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。

(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。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。

6.4 活性化データ

6.4.1 活性化データの生成及びインストール

(1)CA 鍵

CA 秘密鍵を格納する HSM の操作は、複数の管理鍵により行う。

(2)VA 鍵

VA の秘密鍵の PIN は、定められた管理者が設定する。

6.4.2 活性化データの保護

(1)CA 鍵

CA 秘密鍵を格納する HSM の活性化に必要な管理鍵は、安全に保管する。

(2)VA 鍵

VA の秘密鍵の活性化に必要な PIN は、安全に保管する。

6.4.3 活性化データに関する他の局面

規定しない。

6.5 コンピュータセキュリティ制御

6.5.1 特定のコンピュータセキュリティ技術要件

CA システムには、アクセス制御機能、操作員の識別と認証機能、監査ログ及びアーカイブデータの収集機能、CA 鍵及びシステムのリカバリ機能等を備える。

6.5.2 コンピュータセキュリティ評価

セキュリティ対策、運用管理の実施状況についての客観的な監査を受ける体制を確立し、コンピュータセキュリティ評価を行う。

6.6 ライフサイクル技術制御

6.6.1 システム開発

CA システムの開発、修正又は変更に当たっては、所定の手続きに基づき、信頼できる組織及び環境下において作業を実施する。開発、修正又は変更したシステムは、CA システムの評価環境において検証を行い、認証局システム責任者の承認を得た上で導入する。また、システム仕様及び検証報告については、文書化し保管する。

6.6.2 セキュリティ管理

CA システムを維持管理するため、OS 及びソフトウェアのセキュリティチェックを定期的に行う。また、この検証結果を文書化し保管する。

6.6.3 セキュリティ評価の基準

規定しない。

6.7 ネットワークセキュリティ制御

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の接続は行わない。

6.8 暗号モジュールのエンジニアリング制御

本 CP/CPS 「6.1.1 鍵ペア生成」及び「6.2.1 暗号モジュール標準」に規定する。

7. 証明書及び CRL プロファイル

7.1 証明書プロファイル

証明書プロファイルは、プロファイル設計書に定める。

7.2 CRL プロファイル

CRL/ARL プロファイルは、プロファイル設計書に定める。

8. 仕様管理

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。

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。

8.3 CP/CPS 承認手続き

8.1 節に含まれる。

9. 用語集

- ・ARL (Authority Revocation List)

有効期限前に失効した CA 証明書のみでの識別リスト。通常、CA によるデジタル署名が付与される。

- ・CA (Certification Authority)

認証局。鍵ペア (秘密鍵と公開鍵) の所有者に対し、公開鍵証明書の発行、開示、失効、もしくは一時失効を行う。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、発行局と登録局を含む。

- ・CA システム

認証局を構成するシステム。LGPKI では、IA システム、HSM、RA システム及びリポジトリを指す。

- ・CP (Certificate Policy)

証明書ポリシー。一般的なセキュリティ要件を伴った特定のコミュニティやアプリケーションに対する証明書の適用方針。

- ・CPS (Certification Practice Statement)

認証局運用規程。CP で規定された方針を認証局の運用に適用するための実施手順、約款及び外部との信頼関係等を詳細に規定した文書。

- ・CRL (Certificate Revocation List)

有効期限前に失効した証明書の識別リスト。通常、CA によるデジタル署名が付与される。

- ・FIPS (Federal Information Processing)

米国連邦情報処理標準。FIPS140-1 は暗号モジュール評価の基準。

- ・HSM (Hardware Security Module)

耐タンパ機能を有した秘密鍵の管理装置で、CA 秘密鍵を格納する。

- ・IA (Issuing Authority)

発行局。CA の業務のうち証明書の発行及び失効を行う。

- ・IA システム

発行局システム。証明書の発行及び失効を行うシステム。

- ・PIN (Personal Identification Number)

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。

- ・PKI (Public Key Infrastructure)

公開鍵基盤。本人認証 (本人確認) をインターネット上でより厳密 (確実) に行うための基盤。

- ・PKCS (Public Key Cryptography Standards)

米国 RSA 研究所が提唱する業界標準で、暗号アルゴリズム等の暗号演算の周辺におけるアプリケーションのポータビリティや、相互接続性を目的とした業界標準群。

PKCS#1: RSA 暗号に関する標準。署名形式等を規定。

PKCS#7:暗号メッセージの形式に関する標準

PKCS#10:証明書要求に関する形式標準

PKCS#12:個人秘密情報に関する標準

・RA (Registration Authority)

登録局。LGPKI では、LGWAN 運営主体に置く登録局及び登録業務の一部を委任する地方公共団体に置く登録分局を指す。

・RA システム

登録局システム。証明書発行及び失効に係る申請処理を可能にするシステム。証明書利用者からの申請データの受付、審査、承認、発行までの一連の処理フローを管理することが可能である。

・RFC (Request For Comments)

IETF が取りまとめている一連の文書群。

・RSA (Rivest-Shamir-Adleman)

現在最も一般的な公開鍵暗号方式。十分に大きな2つの素数を掛け合わせた数の素因数分解が難しいことを暗号技術の基礎としている。

・SHA-1 (Secure Hash Algorithm-1)

任意の長さのデータから160bitのハッシュ値を作り出す一方向性ハッシュアルゴリズム。

・SSL (Secure Sockets Layer)

サーバとクライアント間の通信の暗号化と認証を行い、安全にデータをやりとりするプロトコル。

・VA (Validation Authority)

証明書有効性検証機関。証明書検証者からの証明書有効性確認問い合わせに対し、検証対象証明書の電子署名の検証、有効期限及び失効情報を確認し応答する。

・X.500

ITU-T (国際電気通信連合の電気通信標準化部門) が定めたネットワーク上での分散ディレクトリサービスに関する国際標準。ディレクトリの概念やその階層構造、サービスやオブジェクトの定義等を定めている。

・X.509

ITU-T (International Telecommunications Union: 国際電気通信連合電気通信標準化部門) のリコメンデーションで、ディレクトリ分野の技術から認証に関する技術標準が規格化された。認証局 (CA) の役割、公開鍵証明書、失効リスト、利用する属性等に関して規定。

・アーカイブデータ

証明書、CRL/ARL、操作履歴等をまとめた電子データ。

・アクセスログ

システムがアクセスされた日付、時刻、動作及びアクセス元の識別情報等を記録した電子データ。

・オブジェクト識別子 (OID: Object Identifier)

情報を相互に区別するために、情報の意味とは無関係に割り当てられた識別子。一意に特定するためにツリー構造で管理される。

・鍵格納媒体

公開鍵証明書及び秘密鍵等を格納する媒体。LGPKIでは、証明書利用者の公開鍵証明書及び秘密鍵等を格納するICカード、USBトークン、HSMを指す。

・活性化

秘密鍵を使用可能な状態にすること。

・監査ログ

セキュリティに関する事象の種類、日付、時刻及び操作員の識別情報等を記録した電子データ。

・危殆化

危険な状態に陥ること。LGPKIでは、CA及び証明書利用者の秘密鍵が紛失・盗難等により第三者の手に渡った(もしくはその可能性が高い)と判断された場合や公開鍵から秘密鍵を容易に計算できる可能性が判明した場合を指す。

・公開鍵証明書(証明書)

CAが記載内容を確認の上、CAが電子署名をすることで、その公開鍵の正当性を保証する。

・公開鍵

公開鍵暗号方式において用いられる鍵ペアの一方で、秘密鍵に対応する公開している鍵。

・自己署名証明書

自CAの公開鍵に対して、自CAの秘密鍵で電子署名した証明書。自CAの公開鍵の正当性を保証する。

・失効

証明書の有効期限内に秘密鍵の危殆化、証明書記載事項の変更、証明書の利用中止などの事由で証明書を無効にすること。

・証明書検証者(Relying Party)

証明書を受けとって、それを信頼して行動する者。

・証明書利用者(Subscriber)

秘密鍵保持者で、公開鍵証明書の利用者。個人の場合の他、サーバアプリケーション等の場合もある。LGPKIでは、地方公共団体、ASPサービス提供者及び公的機関に属する証明書保持者を指す。

・デジタル署名(Digital Signature)

署名対象データのハッシュ値に対して、秘密鍵で暗号化したもの。デジタル署名の検証は、デジタル署名を公開鍵で復号した値と元データのハッシュ値とを照合することで可能。デジタル署名は当該秘密鍵保有者のみが生成できることから文字による署名と同等の効果が推定される。

・電子署名(Electronic Signature)

電子文書の作成者を特定し、電子データが改変されていないことを確認するために付与する署名。デジタル署名を含めた電子的な署名行為全般を指す。

・認証パス

ある1つの証明書の有効性検証を行うために必要な証明書の連鎖のこと。

・ハッシュ(Hash)

任意の長さのデータから固定長のデータに圧縮するためのアルゴリズム。ハッシュ値から元のデータの再現は不可能。一方向性のハッシュアルゴリズムは、メッセージは破損、改ざんされ

ていない事を確認するためのチェックサムとして使用され、デジタル署名の中で用いられる。

・秘密鍵

公開鍵暗号方式において用いられる鍵ペアの一方で、公開鍵に対応する本人のみが保有する鍵。

・リポジトリ(Repository)

様々なオブジェクトに関する情報を保持し、その情報の検索、更新手順を提供する。国際標準規定は ITU-T 勧告 X.500 シリーズ ISO/IEC 国際規格 9594 シリーズ(OSI ディレクトリ)。自己署名証明書、リンク証明書及び CRL/ARL を保管して公開する。LGPKI のリポジトリは、統合リポジトリ及び公開リポジトリからなり、統合リポジトリは LGWAN 上に公開し、公開リポジトリはインターネット上に公開する。

・リンク証明書

新しい CA 鍵ペアと古い CA 鍵ペアの関係を保証するための証明書。

附則

この CP/CPS は、平成 18 年 4 月 1 日から施行する。

附則

この改正 CP/CPS は、平成 18 年 9 月 1 日から適用する。

附則

この改正 CP/CPS は、平成 18 年 11 月 24 日から適用する。

附則

この改正 CP/CPS は、平成 19 年 3 月 20 日から適用する。

附則

この改正 CP/CPS は、平成 19 年 5 月 24 日から適用する。

附則

この改正 CP/CPS は、平成 19 年 10 月 5 日から適用する。

附則

この改正 CP/CPS は、平成 20 年 5 月 28 日から適用する。

附則

この改正 CP/CPS は、平成 20 年 10 月 22 日から適用する。

附則

この改正 CP/CPS は、平成 21 年 3 月 25 日から適用する。

附則

この改正 CP/CPS は、平成 21 年 9 月 29 日から適用する。