

**JPRSサーバー証明書
認証局運用規程
(Certification Practice
Statement)
Version 1.50**

2024年2月22日

株式会社日本レジストリサービス

改版履歴		
版数	日付	内容
1.00	2019.06.17	初版発行
1.10	2020.04.01	Mozilla Root Store Policy(v2.7)への準拠に伴う改訂
1.11	2021.04.01	表紙の日付及び Version を更新
1.12	2022.04.01	表紙の日付及び Version を更新
1.20	2022.09.30	「6.3.2 私有鍵および公開鍵の有効期間」のタイトル変更および現状に合わせて記述を追加・修正
1.30	2023.06.08	Baseline Requirement への準拠に関する記述の修正
1.40	2023.08.28	Baseline Requirement の各要件への準拠を明確にするため記述見直し
1.50	2024.02.22	Baseline Requirement の正式名称に関する記述の修正

目次

1. はじめに.....	11
1.1 概要.....	11
1.2 文書名と識別.....	12
1.3 PKI の関係者.....	12
1.3.1 CA.....	12
1.3.2 RA.....	12
1.3.3 証明書利用者.....	12
1.3.4 検証者.....	12
1.3.5 その他関係者.....	12
1.4 証明書の用途.....	13
1.4.1 適切な証明書の用途.....	13
1.4.2 禁止される証明書の用途.....	13
1.5 ポリシー管理.....	13
1.5.1 文書を管理する組織.....	13
1.5.2 連絡先.....	13
1.5.3 ポリシー適合性を決定する者.....	13
1.5.4 承認手続.....	13
1.6 定義と略語.....	13
2. 公開とリポジトリの責任.....	18
2.1 リポジトリ.....	18
2.2 情報の公開.....	18
2.3 公開の時期または頻度.....	18
2.4 リポジトリへのアクセス管理.....	18
3. 識別と認証.....	19
3.1 名前決定.....	19
3.1.1 名前の種類.....	19
3.1.2 名前が意味を持つことの必要性.....	19
3.1.3 証明書利用者の匿名性または仮名性.....	19
3.1.4 様々な名前形式を解釈するための規則.....	19
3.1.5 名前の一意性.....	19
3.1.6 商標の認識、認証および役割.....	19
3.2 初回の本人性確認.....	19
3.2.1 私有鍵の所持を証明する方法.....	19
3.2.2 組織とドメイン名の認証.....	19

3.2.3	個人の認証	19
3.2.4	検証されない証明書利用者の情報	19
3.2.5	権限の正当性確認	19
3.2.6	相互運用の基準	20
3.3	鍵更新申請時の本人性確認と認証	20
3.3.1	通常の鍵更新時における本人性確認と認証	20
3.3.2	証明書失効後の鍵更新時における本人性確認と認証	20
3.4	失効申請時の本人性確認と認証	20
4.	証明書のライフサイクルに対する運用上の要件	21
4.1	証明書申請	21
4.1.1	証明書申請を提出することができる者	21
4.1.2	申請手続および責任	21
4.2	証明書申請手続	21
4.2.1	本人性確認と認証の実施	21
4.2.2	証明書申請の承認または却下	21
4.2.3	証明書申請の処理時間	21
4.2.4	CAA レコードの確認	21
4.3	証明書の発行	21
4.3.1	証明書発行時の処理手続	21
4.3.2	証明書利用者への証明書発行通知	21
4.4	証明書の受領確認	21
4.4.1	証明書の受領確認手続	21
4.4.2	認証局による証明書の公開	22
4.4.3	他のエンティティに対する認証局の証明書発行通知	22
4.5	鍵ペアおよび証明書の用途	22
4.5.1	証明書利用者の私有鍵および証明書の用途	22
4.5.2	検証者の公開鍵および証明書の用途	22
4.6	鍵更新を伴わない証明書の更新	22
4.6.1	鍵更新を伴わない証明書の更新事由	22
4.6.2	証明書の更新申請を行うことができる者	22
4.6.3	証明書の更新申請の処理手続	22
4.6.4	証明書利用者に対する新しい証明書発行通知	22
4.6.5	更新された証明書の受領確認手続	22
4.6.6	認証局による更新された証明書の公開	22
4.6.7	他のエンティティに対する認証局の証明書発行通知	22
4.7	鍵更新を伴う証明書の更新	23

4.7.1 鍵更新を伴う証明書の更新事由.....	23
4.7.2 新しい証明書の申請を行うことができる者.....	23
4.7.3 鍵更新を伴う証明書の更新申請の処理手続.....	23
4.7.4 証明書利用者に対する新しい証明書の通知.....	23
4.7.5 鍵更新された証明書の受領確認手続.....	23
4.7.6 認証局による鍵更新済みの証明書の公開.....	23
4.7.7 他のエンティティに対する認証局の証明書発行通知.....	23
4.8 証明書の変更.....	23
4.8.1 証明書の変更事由.....	23
4.8.2 証明書の変更申請を行うことができる者.....	23
4.8.3 証明書の変更申請の処理手続.....	23
4.8.4 証明書利用者に対する新しい証明書発行通知.....	23
4.8.5 変更された証明書の受領確認手続.....	23
4.8.6 認証局による変更された証明書の公開.....	24
4.8.7 他のエンティティに対する認証局の証明書発行通知.....	24
4.9 証明書の失効と一時停止.....	24
4.9.1 証明書失効事由.....	24
4.9.2 証明書失効を申請することができる者.....	24
4.9.3 失効申請手続.....	24
4.9.4 失効申請の猶予期間.....	24
4.9.5 認証局が失効申請を処理しなければならない期間.....	24
4.9.6 失効調査の要求.....	24
4.9.7 証明書失効リストの発行頻度.....	24
4.9.8 証明書失効リストの発行最大遅延時間.....	24
4.9.9 オンラインでの失効/ステータス確認の利用可能性.....	24
4.9.10 オンラインでの失効/ステータス確認を行うための要件.....	24
4.9.11 利用可能な失効情報の他の形式.....	24
4.9.12 鍵の危殆化に対する特別要件.....	25
4.9.13 証明書の一時停止事由.....	25
4.9.14 証明書の一時停止を申請することができる者.....	25
4.9.15 証明書の一時停止申請手続.....	25
4.9.16 一時停止を継続することができる期間.....	25
4.10 証明書のステータス確認サービス.....	25
4.10.1 運用上の特徴.....	25
4.10.2 サービスの利用可能性.....	25
4.10.3 オプションな仕様.....	25

4.11 加入（登録）の終了	25
4.12 キーエスクローと鍵回復	25
4.12.1 キーエスクローと鍵回復ポリシーおよび実施	25
4.12.2 セッションキーのカプセル化と鍵回復のポリシーおよび実施	25
5. 設備上、運営上、運用上の管理	26
5.1 物理的セキュリティ管理	27
5.1.1 立地場所および構造	27
5.1.2 物理的アクセス	27
5.1.3 電源および空調	27
5.1.4 水害対策	27
5.1.5 火災対策	27
5.1.6 媒体保管	27
5.1.7 廃棄処理	28
5.1.8 オフサイトバックアップ	28
5.2 手続的管理	28
5.2.1 信頼される役割	28
5.2.2 職務ごとに必要とされる人数	29
5.2.3 個々の役割に対する本人性確認と認証	29
5.2.4 職務分割が必要となる役割	29
5.3 人事的管理	29
5.3.1 資格、経験および身分証明の要件	29
5.3.2 適性調査	29
5.3.3 教育要件	29
5.3.4 再教育の頻度および要件	30
5.3.5 仕事のローテーションの頻度および順序	30
5.3.6 認められていない行動に対する制裁	30
5.3.7 業務委託先の管理	30
5.3.8 要員へ提供される資料	30
5.4 監査ログの手続	30
5.4.1 記録されるイベントの種類	30
5.4.2 監査ログを処理する頻度	31
5.4.3 監査ログを保持する期間	31
5.4.4 監査ログの保護	32
5.4.5 監査ログのバックアップ手続	32
5.4.6 監査ログの収集システム	32
5.4.7 イベントを起こした者への通知	32

5.4.8 脆弱性評価.....	32
5.5 記録の保管	33
5.5.1 アーカイブの種類.....	33
5.5.2 アーカイブ保存期間.....	33
5.5.3 アーカイブの保護.....	33
5.5.4 アーカイブのバックアップ手続.....	33
5.5.5 記録にタイムスタンプを付与する要件.....	33
5.5.6 アーカイブ収集システム	33
5.5.7 アーカイブの検証手続.....	33
5.6 鍵の切り替え.....	34
5.7 危殆化および災害からの復旧.....	34
5.7.1 事故および危殆化時の手続.....	34
5.7.2 ハードウェア、ソフトウェアまたはデータが破損した場合の手続.....	35
5.7.3 私有鍵が危殆化した場合の手続.....	35
5.7.4 災害後の事業継続性.....	35
5.8 認証局または登録局の終了	35
6. 技術的セキュリティ管理.....	36
6.1 鍵ペアの生成およびインストール.....	36
6.1.1 鍵ペアの生成	36
6.1.2 証明書利用者に対する私有鍵の交付.....	37
6.1.3 認証局への公開鍵の交付	37
6.1.4 検証者への CA 公開鍵の交付	37
6.1.5 鍵サイズ	37
6.1.6 公開鍵のパラメータの生成および品質検査.....	37
6.1.7 鍵の用途	37
6.2 私有鍵の保護および暗号モジュール技術の管理	37
6.2.1 暗号モジュールの標準および管理	37
6.2.2 私有鍵の複数人管理.....	38
6.2.3 私有鍵のエスクロー.....	38
6.2.4 私有鍵のバックアップ	38
6.2.5 私有鍵のアーカイブ.....	38
6.2.6 私有鍵の暗号モジュールへのまたは暗号モジュールからの転送.....	38
6.2.7 暗号モジュールへの私有鍵の格納	38
6.2.8 私有鍵の活性化方法.....	38
6.2.9 私有鍵の非活性化方法	38
6.2.10 私有鍵の破棄方法	38

6.2.11 暗号モジュールの評価	38
6.3 鍵ペアのその他の管理方法	38
6.3.1 公開鍵のアーカイブ	38
6.3.2 証明書の有効期間と私有鍵および公開鍵の有効期間.....	39
6.4 活性化データ	39
6.4.1 活性化データの生成および設定.....	39
6.4.2 活性化データの保護.....	39
6.4.3 活性化データの他の考慮点.....	39
6.5 コンピュータのセキュリティ管理.....	39
6.5.1 コンピュータセキュリティに関する技術的要件.....	39
6.5.2 コンピュータセキュリティ評価.....	39
6.6 ライフサイクルの技術的管理.....	40
6.6.1 システム開発管理.....	40
6.6.2 セキュリティ運用管理.....	40
6.6.3 ライフサイクルセキュリティ管理.....	40
6.7 ネットワークセキュリティ管理.....	40
6.8 タイムスタンプ	40
7. 証明書および証明書失効リストのプロファイル.....	41
7.1 証明書のプロファイル.....	41
7.1.1 バージョン番号.....	41
7.1.2 証明書の拡張	41
7.1.3 アルゴリズムオブジェクト識別子	41
7.1.4 名前の形式.....	41
7.1.5 名前制約	41
7.1.6 証明書ポリシーオブジェクト識別子.....	41
7.1.7 ポリシー制約拡張の使用	41
7.1.8 ポリシー修飾子の構文および意味	41
7.1.9 クリティカルな証明書ポリシー拡張に対する解釈の方法	41
7.2 CRL のプロファイル.....	41
7.2.1 バージョン番号.....	41
7.2.2 証明書失効リストおよび証明書失効リストエントリ拡張	41
7.3 OCSP のプロファイル	42
7.3.1 バージョン番号.....	42
7.3.2 OCSP 拡張	42
8. 準拠性監査と他の評価	43
8.1 監査の頻度	43

8.2 監査者の身元／資格	43
8.3 監査者と被監査者の関係	44
8.4 監査で扱われる事項	44
8.5 不備の結果としてとられる処置	44
8.6 監査結果の開示	44
8.7 内部監査	45
9. 他の業務上および法的事項	46
9.1 料金	46
9.2 財務的責任	46
9.3 企業情報の機密性	46
9.3.1 機密情報の範囲	46
9.3.2 機密情報の範囲外の情報	46
9.3.3 機密情報を保護する責任	46
9.4 個人情報保護	47
9.5 知的財産権	47
9.6 表明保証	47
9.6.1 CA 業務の表明保証	47
9.6.2 RA 業務の表明保証	47
9.6.3 証明書利用者の表明保証	47
9.6.4 検証者の表明保証	47
9.6.5 その他関係者の表明保証	47
9.7 無保証	47
9.8 責任の制限	47
9.9 補償	48
9.10 有効期間と終了	48
9.10.1 有効期間	48
9.10.2 終了	48
9.10.3 終了の効果と効果継続	48
9.11 関係者間の個別通知と連絡	48
9.12 改訂	48
9.12.1 改訂手続	48
9.12.2 通知方法および期間	48
9.12.3 オブジェクト識別子を変更されなければならない場合	48
9.13 紛争解決手続	49
9.14 準拠法	49
9.15 適用法の遵守	49

9.16 雑則	49
9.17 その他の条項.....	49

1. はじめに

1.1 概要

JPRS サーバー証明書認証局運用規程 (以下「本 CPS」という) は、JPRS サーバー証明書発行サービスを提供するために株式会社日本レジストリサービス (以下「当社」という) が構築する認証局 (以下「本 CA」という) の運用に関するポリシーを規定した文書である。

本 CA は、CA/Browser Forum が <https://www.cabforum.org/> で公開する「Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates」(以下「Baseline Requirements」という) およびアプリケーションソフトウェアサプライヤーの規準の最新版に準拠する。

表 1.1 規準一覧

本CAが発行する証明書種類	準拠すべき規準
TLSサーバー証明書	<ul style="list-style-type: none">• Baseline Requirements for the Issuance and Management of Publicly - Trusted TLS Server Certificates• Apple Root Certificate Program• Chrome Root Program Policy• Microsoft Trusted Root Program• Mozilla Root Store Policy

本 CA が発行する証明書の種類、用途、運用等に関する各種規則は JPRS サーバー証明書認証局証明書ポリシー (以下「CP」という) として規定される。

なお、本 CPS とご利用条件、CP の内容に矛盾がある場合は、ご利用条件、CP、本 CPS の順に優先して適用される。また、本 CPS の日本語版と[英語版](#)の内容に矛盾がある場合は、[英語版](#)が日本語版に優先して適用される。本サービスに関して当社の定める規定と Baseline Requirements の間に矛盾がある場合、Baseline Requirements が当社の定める規定に優先して適用される。

本 CPS は、IETF が認証局運用のフレームワークとして提唱する RFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。

本 CPS は、認証業務に関する技術面、サービス面の発展や改良にともない、それらを反映

するために必要に応じ改訂されるものとする。

1.2 文書名と識別

本 CPS の正式名称は、「JPRS サーバー証明書認証局運用規程」という。本 CA が本 CPS に基づき割り当てるオブジェクト識別子(以下「OID」という)、および本 CPS が参照する CP の OID は、次のとおりである。

名称	OID
JPRS サーバー証明書認証局運用規程 (CPS)	1.3.6.1.4.1.53827.1.2.4
JPRS サーバー証明書認証局証明書ポリシー (CP)	1.3.6.1.4.1.53827.1.1.4

1.3 PKI の関係者

1.3.1 CA

証明書の発行、失効、失効情報の開示、OCSP (Online Certificate Status Protocol) サーバーによる証明書ステータス情報の提供および保管、CA 私有鍵の生成・保護および証明書利用者の登録等を行う主体のことをいう。

1.3.2 RA

CA の業務のうち、証明書の発行、取消を申請する申請者の実在性確認、本人性確認の審査、証明書発行に必要な情報の登録、CA に対する証明書発行要求等を行う主体のことをいう。RA は、本 CA が担う。

1.3.3 証明書利用者

証明書利用者とは、本 CA より証明書の発行を受け、発行された証明書を利用する個人、法人または組織とする。

1.3.4 検証者

検証者とは、本 CA により発行された証明書の有効性を検証する個人、法人または組織とする。

1.3.5 その他関係者

規定しない。

1.4 証明書の用途

1.4.1 適切な証明書の用途

本項については、CP に規定する。

1.4.2 禁止される証明書の用途

本項については、CP に規定する

1.5 ポリシー管理

1.5.1 文書を管理する組織

本 CPS の維持、管理は、本 CA が行う。

1.5.2 連絡先

本 CPS に関する連絡先は、次のとおりである。

窓口：株式会社日本レジストリサービス お問い合わせ窓口

住所：〒101-0065 東京都千代田区西神田 3-8-1 千代田ファーストビル東館 13F

電子メール：info@jprs.jp

なお、本 CA が発行したサーバー証明書について私有鍵の危殆化や不正利用などが発覚した場合の連絡先は、次のとおりである。

専用窓口：https://jprs.jp/pubcert/f_mail/

1.5.3 ポリシー適合性を決定する者

本 CPS の内容については、本 CA のサーバー証明書発行サービス運営会議において決定される

1.5.4 承認手続

本 CPS は、本 CA のサーバー証明書発行サービス運営会議の承認によって発効する。

1.6 定義と略語

Archive：アーカイブ

法的またはその他の事由により、履歴の保存を目的に取得する情報のことをいう。

Audit Log：監査ログ

認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局シス

テムの動作履歴やアクセス履歴等をいう。

CA (Certification Authority) : 認証局

証明書の発行・更新・失効、失効情報の開示、OCSP (Online Certificate Status Protocol) サーバーによる証明書ステータス情報の提供および保管、CA私有鍵の生成・保護および証明書利用者の登録等を行う主体のことをいう。

CAA (Certificate Authority Authorization)

ドメインを使用する権限において、DNSレコードの中にドメインに対して証明書を発行できる認証局情報を記述し、意図しない認証局からの証明書誤発行を防ぐ機能のことをいう。本機能はRFC 6844で規定されている。

CP (Certificate Policy) : 証明書ポリシー

CAが発行する証明書の種類、発行対象、用途、申込手続、発行基準等、証明書に関する事項を規定する文書のことをいう。

CPS (Certification Practices Statement) : 認証局運用規定

CAを運用する上での諸手続、セキュリティ基準等、CAの運用を規定する文書のことをいう。

CRL (Certificate Revocation List) : 証明書失効リスト

証明書の有効期間中に、証明書記載内容の変更、私有鍵の危殆化等の事由により失効された証明書情報が記載されたリストのことをいう。

CT (Certificate Transparency)

RFC 6962で規定された、発行された証明書の情報を監視・監査するためにログサーバー (CTログサーバー) に証明書の情報を登録し、公開する仕組みのことをいう。

Digital Certificates : 電子証明書

ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CAが電子署名を施すことで、その正当性が保証される。

ECDSA (Elliptic Curve Digital Signature Algorithm)

公開鍵暗号方式として普及している最も標準的な暗号技術のひとつである。

Escrow : エスクロー

第三者に預けること（寄託）をいう。

FIPS140-2

米国NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準のことをいう。最低レベル1から最高レベル4まで定義されている。

HSM（Hardware Security Module）

私有鍵の生成、保管、利用などにおいて、セキュリティを確保する目的で使用する耐タンパー機能を備えた暗号装置のことをいう。

JPRS Partners : 指定事業者

当社が提供するサーバー証明書発行サービスに関して、当社の認定する事業者のことをいう。

Key Pair : 鍵ペア

公開鍵暗号方式において、私有鍵と公開鍵から構成される鍵の対のことをいう。

NTP（Network Time Protocol）

コンピュータの内部時計を、ネットワークを介して正しく調整するプロトコルのことをいう。

OCSP（Online Certificate Status Protocol）

証明書ステータス情報をリアルタイムに提供するプロトコルのことをいう。

OID（Object Identifier） : オブジェクト識別子

ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。

PKI（Public Key Infrastructure） : 公開鍵基盤

電子署名、暗号化、認証といったセキュリティ技術を実現するための、公開鍵暗号方式という暗号技術を用いる基盤のことをいう。

Private Key : 私有鍵

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

保有する鍵のことをいう。「秘密鍵」ともいう。

Public Key : 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をいい、私有鍵に対応し、通信相手の相手方に公開される鍵のことをいう。

RA (登録局) (Registration Authority) : 登録機関

CAの業務のうち、証明書の発行、取消を申請する申請者の実在性確認、本人性確認の審査、証明書発行に必要な情報の登録、CAに対する証明書発行要求等を行う主体のことをいう。

Repository : リポジトリ

CA証明書およびCRL等を格納し公表するデータベースのことをいう。

RFC 3647 (Request For Comments 3647)

インターネットに関する技術の標準を定める団体であるIETF (Internet Engineering Task Force) が発行する文書であり、CP/CPSのフレームワークを規定した文書のことをいう。

RFC 5280 (Request For Comments 5280)

インターネットに関する技術の標準を定める団体であるIETF (Internet Engineering Task Force) が発行する文書であり、公開鍵基盤について規定した文書のことをいう。

RSA

公開鍵暗号方式として普及している最も標準的な暗号技術のひとつである。

SHA-1 (Secure Hash Algorithm 1)

電子署名に使われるハッシュ関数 (要約関数) のひとつである。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいう。ビット長は160ビット。データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

SHA-256 (Secure Hash Algorithm 256)

電子署名に使われるハッシュ関数 (要約関数) のひとつである。ビット長は256ビット。データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

Time Stamp : タイムスタンプ

電子ファイルの作成日時やシステムが処理を実行した日時等を記録したデータのことをいう。

2. 公開とリポジトリの責任

2.1 リポジトリ

本 CA は、リポジトリを 24 時間 365 日利用できるよう維持管理を行う。ただし、利用可能な時間帯においてもシステム保守等により、利用できない場合がある。

2.2 情報の公開

本 CA は、CRL、本 CPS および CP をリポジトリ上に公開し、証明書利用者および検証者がオンラインによって閲覧可能となるようにする。

2.3 公開の時期または頻度

本 CPS は、改訂の都度、リポジトリ上に公開する。

2.4 リポジトリへのアクセス管理

本項については、CP に規定する。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

本項については、CPに規定する。

3.1.2 名前が意味を持つことの必要性

本項については、CPに規定する。

3.1.3 証明書利用者の匿名性または仮名性

本項については、CPに規定する。

3.1.4 様々な名前形式を解釈するための規則

本項については、CPに規定する。

3.1.5 名前の一意性

本項については、CPに規定する。

3.1.6 商標の認識、認証および役割

本項については、CPに規定する。

3.2 初回の本人性確認

3.2.1 私有鍵の所持を証明する方法

本項については、CPに規定する。

3.2.2 組織とドメイン名の認証

本項については、CPに規定する。

3.2.3 個人の認証

本項については、CPに規定する。

3.2.4 検証されない証明書利用者の情報

本項については、CPに規定する。

3.2.5 権限の正当性確認

本項については、CPに規定する。

3.2.6 相互運用の基準

本項については、CP に規定する。

3.3 鍵更新申請時の本人性確認と認証

3.3.1 通常の鍵更新時における本人性確認と認証

本項については、CP に規定する。

3.3.2 証明書失効後の鍵更新時における本人性確認と認証

本項については、CP に規定する。

3.4 失効申請時の本人性確認と認証

本項については、CP に規定する。

4. 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書申請を提出することができる者

本項については、CPに規定する。

4.1.2 申請手続および責任

本項については、CPに規定する。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施

本項については、CPに規定する。

4.2.2 証明書申請の承認または却下

本項については、CPに規定する。

4.2.3 証明書申請の処理時間

本項については、CPに規定する。

4.2.4 CAA レコードの確認

本項については、CPに規定する。

4.3 証明書の発行

4.3.1 証明書発行時の処理手続

本項については、CPに規定する。

4.3.2 証明書利用者への証明書発行通知

本項については、CPに規定する。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

本項については、CPに規定する。

4.4.2 認証局による証明書の公開

本項については、CP に規定する。

4.4.3 他のエンティティに対する認証局の証明書発行通知

本項については、CP に規定する。

4.5 鍵ペアおよび証明書の用途

4.5.1 証明書利用者の私有鍵および証明書の用途

本項については、CP に規定する。

4.5.2 検証者の公開鍵および証明書の用途

本項については、CP に規定する。

4.6 鍵更新を伴わない証明書の更新

4.6.1 鍵更新を伴わない証明書の更新事由

本項については、CP に規定する。

4.6.2 証明書の更新申請を行うことができる者

本項については、CP に規定する。

4.6.3 証明書の更新申請の処理手続

本項については、CP に規定する。

4.6.4 証明書利用者に対する新しい証明書発行通知

本項については、CP に規定する。

4.6.5 更新された証明書の受領確認手続

本項については、CP に規定する。

4.6.6 認証局による更新された証明書の公開

本項については、CP に規定する。

4.6.7 他のエンティティに対する認証局の証明書発行通知

本項については、CP に規定する。

4.7 鍵更新を伴う証明書の更新

4.7.1 鍵更新を伴う証明書の更新事由

本項については、CPに規定する。

4.7.2 新しい証明書の申請を行うことができる者

本項については、CPに規定する。

4.7.3 鍵更新を伴う証明書の更新申請の処理手続

本項については、CPに規定する。

4.7.4 証明書利用者に対する新しい証明書の通知

本項については、CPに規定する。

4.7.5 鍵更新された証明書の受領確認手続

本項については、CPに規定する。

4.7.6 認証局による鍵更新済みの証明書の公開

本項については、CPに規定する。

4.7.7 他のエンティティに対する認証局の証明書発行通知

本項については、CPに規定する。

4.8 証明書の変更

4.8.1 証明書の変更事由

本項については、CPに規定する。

4.8.2 証明書の変更申請を行うことができる者

本項については、CPに規定する。

4.8.3 証明書の変更申請の処理手続

本項については、CPに規定する。

4.8.4 証明書利用者に対する新しい証明書発行通知

本項については、CPに規定する。

4.8.5 変更された証明書の受領確認手続

本項については、CPに規定する。

4.8.6 認証局による変更された証明書の公開

本項については、CP に規定する。

4.8.7 他のエンティティに対する認証局の証明書発行通知

本項については、CP に規定する。

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由

本項については、CP に規定する。

4.9.2 証明書失効を申請することができる者

本項については、CP に規定する。

4.9.3 失効申請手続

本項については、CP に規定する。

4.9.4 失効申請の猶予期間

本項については、CP に規定する。

4.9.5 認証局が失効申請を処理しなければならない期間

本項については、CP に規定する。

4.9.6 失効調査の要求

本項については、CP に規定する。

4.9.7 証明書失効リストの発行頻度

本項については、CP に規定する。

4.9.8 証明書失効リストの発行最大遅延時間

本項については、CP に規定する。

4.9.9 オンラインでの失効/ステータス確認の利用可能性

本項については、CP に規定する。

4.9.10 オンラインでの失効/ステータス確認を行うための要件

本項については、CP に規定する。

4.9.11 利用可能な失効情報の他の形式

本項については、CP に規定する。

4.9.12 鍵の危殆化に対する特別要件

本項については、CP に規定する。

4.9.13 証明書の一時停止事由

本項については、CP に規定する。

4.9.14 証明書の一時停止を申請することができる者

本項については、CP に規定する。

4.9.15 証明書の一時停止申請手続

本項については、CP に規定する。

4.9.16 一時停止を継続することができる期間

本項については、CP に規定する。

4.10 証明書のステータス確認サービス

4.10.1 運用上の特徴

本項については、CP に規定する。

4.10.2 サービスの利用可能性

本項については、CP に規定する。

4.10.3 オプションな仕様

本項については、CP に規定する。

4.11 加入（登録）の終了

本項については、CP に規定する。

4.12 キーエスクローと鍵回復

4.12.1 キーエスクローと鍵回復ポリシーおよび実施

本項については、CP に規定する。

4.12.2 セッションキーのカプセル化と鍵回復のポリシーおよび実施

本項については、CP に規定する。

5. 設備上、運営上、運用上の管理

CA/Browser Forum の「Network and Certificate System Security Requirement」は、参照することにより本書に完全に組み込まれる。

本 CA は、以下の目的で設計された包括的なセキュリティプログラムを開発、実装、維持する。

1. 証明書データおよび証明書管理プロセスの機密性、完全性、および可用性を保護する。
2. 証明書データおよび証明書管理プロセスの機密性、完全性、および可用性にとっての潜在的な脅威または危険から保護する。
3. 証明書データおよび証明書管理プロセスに対する不正または違法なアクセス、使用、開示、改変、または破壊から保護する。
4. 証明書データおよび証明書管理プロセスの不慮の損失、破壊、または損傷から保護する。
5. 法律によって本 CA に適用されるその他のセキュリティ要件すべてに準拠する。

証明書管理プロセスは、以下を含む必要がある。

1. 物理的なセキュリティ制御や環境制御。
2. 構成管理、信頼済みコードの整合性メンテナンス、マルウェア検出/防止を含む、システム整合性制御。
3. ポート制限や IP アドレスフィルタリングを含む、ネットワークセキュリティおよびファイアウォール管理。
4. ユーザー管理、信頼済みロールの分担、教育、意識向上、トレーニング。
5. 個々の責任を明確にするための論理的なアクセス制御、アクティビティロギング、およびアイドル時のタイムアウト。

本 CA のセキュリティプログラムには、以下のような年次リスクアセスメントを含める必要がある。

1. 証明書データまたは証明書管理プロセスに対する不正なアクセス、開示、不正使用、改変、または破壊につながる、予測可能な内外の脅威を特定する。
2. これらの脅威がもたらす可能性があるダメージについて、証明書データや証明書管理プロセスの秘密度を考慮に入れて評価する。
3. このような脅威に対抗するために本 CA が配備したポリシー、手順、情報システム、技術、その他の手配の充実度に関して評価する。

リスクアセスメントに基づき、本 CA は、上述の目的を実現するべく設計されたセキュリ

ティ手順、対策、および製品で構成されるセキュリティ計画を開発、実装、および維持し、リスクアセスメント中に識別されたリスクを、証明書データおよび証明書管理プロセスの重要度に応じて管理するものとする。セキュリティ計画には、証明書データおよび証明書管理プロセスの秘密度に適した管理上、組織的、技術的、および物理的な保護対策を含めなければならない。また、セキュリティ計画では、その時点で利用可能な技術および特定の対策の実装コストを考慮に入れなければならない。セキュリティの侵害から生じる可能性がある損害および保護対象のデータの性質に適した合理的な水準のセキュリティを実装するものとする。

5.1 物理的セキュリティ管理

5.1.1 立地場所および構造

当社は、本 CA のシステムをセキュアなデータセンター内に設置する。データセンターは、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建設されており、かつ建物の構造上も、これら災害防止のための対策を講じている。

5.1.2 物理的アクセス

当社は、本 CA のシステムの重要性に応じて、物理的なアクセス制御および電子的なアクセス制御を組み合わせた適切なセキュリティコントロールを構築する。また、監視カメラ、各種センサーを設置し、認証基盤システムへのアクセスを監視する。

5.1.3 電源および空調

データセンターでは、瞬断および長時間の停電時においても本 CA のシステムの運用を可能とするために、無停電電源装置および自家発電装置による電源対策を施している。また、本 CA のシステムは、空気調和機により最適な温度、湿度を一定に保つことが可能な環境下に設置する。

5.1.4 水害対策

本 CA は、水害対策として、本 CA のシステムを建物の二階以上に設置する。また、防水対策として、本 CA のシステムを設置する室には漏水検知器を設置する。

5.1.5 火災対策

本 CA のシステムを設置する室は、防火壁によって区画された防火区画とし、火災報知機および消火設備を設置する。

5.1.6 媒体保管

本 CA は、アーカイブデータ、バックアップデータを含む認証業務を行ううえで必要な情報を、適切な入退管理が行われた室内の保管庫に保存するとともに、毀損、滅失防止のための

措置を施す。

5.1.7 廃棄処理

本 CA は、機密情報を含む書類および電子媒体の廃棄を、情報の初期化、裁断等により行う。

5.1.8 オフサイトバックアップ

本 CA は、本 CA のシステムの運用のために必要なデータ、機器等を、遠隔地に保管するかまたは調達できる手段を講ずる。

5.2 手続的管理

5.2.1 信頼される役割

本 CA のシステムの運用に関わる役割を以下に示す。

(1) サービス責任者

- ・ CA 全体の統括
- ・ サービス管理者の任命

(2) サービス管理者

- ・ CA 業務責任者、RA 業務責任者の任命

(3) CA 業務責任者

- ・ CA 業務の統括
- ・ CA のシステムの変更、運用手続変更の承認

(4) CA 業務管理者

- ・ CA 業務担当者への作業指示
- ・ CA 私有鍵に関する作業立会い
- ・ CA 業務の全般管理

(5) CA 業務担当者

- ・ CA サーバ、リポジトリサーバ等 CA のシステムの維持管理
- ・ CA 私有鍵の活性化、非活性化等の操作

(6) RA 業務責任者

- ・ RA 業務の統括

(7) RA 業務管理者

- ・ RA 業務担当者への作業指示
- ・ RA 業務の遂行管理

(8) RA 業務担当者

- ・ 証明書申請における情報の検証
- ・ 証明書申請、失効要求、更新要求の承認、拒絶その他の処理

・その他、RA 業務管理者の指示に基づく証明書発行審査の遂行

(9) ログ検査者

・入退室ログ、システムログ等の検査

5.2.2 職務ごとに必要とされる人数

本 CA は、サービス提供に支障をきたさないよう、サービス責任者、サービス管理者、CA 業務責任者、RA 業務責任者を除く本 CPS「5.2.1.信頼される役割」に記載する役割に関し、役割ごとに 1 名以上の要員を配置する。なお、CA 私有鍵の操作等の重要な業務については複数名の要員で行う。

なお、CA 私有鍵の操作等の重要な業務については複数名の要員で行う。CA 私有鍵のバックアップ、保管、回復は、信頼される役割を持つ担当者が、少なくとも物理的に安全な環境で、二重制御を用いながら行うものとする。

5.2.3 個々の役割に対する本人性確認と認証

本 CA は、本 CA のシステムへのアクセスに関し、物理的または論理的な方法によってアクセス権限者の識別と認証、および認可された権限の操作であることを確認する。

5.2.4 職務分割が必要となる役割

本 CPS「5.2.1.信頼される役割」に記載する役割は、原則として異なる要員がその役割を担う。なお、CA 業務管理者および RA 業務管理者については、ログ検査者との兼務を可能とする。

5.3 人事的管理

5.3.1 資格、経験および身分証明の要件

本 CPS「5.2.1.信頼される役割」に記載する役割を担う者は、当社の定めた採用基準に基づき採用された従業員等とする。

本 CA のシステムを直接操作する担当者には、専門のトレーニングを受け、PKI の概要とシステムの操作方法等を理解している者を配置する。

5.3.2 適性調査

本 CA は、本 CPS「5.2.1.信頼される役割」に記載する役割を担う者の信頼性と適性を任命時および定期的に評価する。

5.3.3 教育要件

本 CPS「5.2.1.信頼される役割」に記載する役割を担う者は、役割に就く前に本 CA のシステムの運用に必要な教育を受け、以降、必要に応じ、役割に応じた教育・訓練を受ける。また、業務手順に変更がある場合はその変更に関わる教育・訓練を受ける。

本 CA は、情報検証業務を実行するすべての要員に、基本的な公開鍵インフラストラクチャの知識、認証および検証ポリシーおよび手順（本 CA の CP および CPS を含む）、情報検証プロセスに対する一般的な脅威（フィッシングおよびその他のソーシャル・エンジニアリング手法を含む）、および Baseline Requirements を網羅したスキル研修を提供するものとする。

本 CA は、かかる訓練の記録を維持し、検証スペシャリスト業務を委託された要員が、かかる業務を十分に遂行できるスキルレベルを維持することを保証しなければならない。

本 CA は、検証スペシャリストにそのタスクの実行を許可する前に、各検証スペシャリストがタスクに必要なスキルを有していることを文書化しなければならない。

本 CA は、すべての検証スペシャリストに対し、Baseline Requirements に概説されている情報検証要件について CA が提供する試験に合格することを要求しなければならない。

5.3.4 再教育の頻度および要件

本 CPS 「5.2.1.信頼される役割」に記載する役割を担う者は、必要に応じ再トレーニングを受ける。

信頼される役割のすべての要員は、本 CA のトレーニングおよびパフォーマンスプログラムと一致したスキルレベルを維持するものとする。

5.3.5 仕事のローテーションの頻度および順序

本 CA は、サービス品質の維持、向上および不正防止の観点から、必要に応じて要員のジョブローテーションを行う。

5.3.6 認められていない行動に対する制裁

就業規則に従い、処罰が課せられる。

5.3.7 業務委託先の管理

当社は、本 CA のシステムの運用の一部を外部組織に委託する場合、業務委託先との契約によって、業務委託先のもとで運用業務が適切に行われていることを確認する。

本 CA は、証明書の発行に携わる外部委託先の担当者が本 CPS 「5.3.3 教育要件」ならびに本 CPS 「5.4.1 記録されるイベントの種類」を満たしていることを検証するものとする。

5.3.8 要員へ提供される資料

要員は、関連する業務上必要な文書のみ閲覧をすることができる。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類

本 CA は、監査ログとして以下の記録を収集する。

1. 以下を含む CA 証明書と鍵ライフサイクルイベント
 1. 鍵の生成、バックアップ、保管、回復、アーカイブ化、破棄。
 2. 証明書の要求、更新、鍵の再生成の要求、および失効
 3. 証明書要求の承認と拒否。
 4. 暗号化デバイスライフサイクル管理イベント。
 5. 証明書失効リストと OCSP エントリの生成。
 6. 新しい証明書プロファイルの導入と既存の証明書プロファイルの廃止。
2. 以下を含む利用者向け証明書ライフサイクル管理イベント
 1. 証明書の要求、更新、鍵の再生成要求、および失効化。
 2. Baseline Requirements および CA の証明書運用規定で定められたすべての検証アクション。
 3. 証明書要求の承認と拒否。
 4. 証明書の発行。
 5. 証明書失効リストおよび OCSP エントリの生成。
3. 以下を含むセキュリティイベント
 1. 成功および失敗した PKI システムアクセス試行。
 2. 実行された PKI およびセキュリティシステムアクション。
 3. セキュリティプロファイルの変更。
 4. 証明書システムへのソフトウェアのインストール、更新、および削除。
 5. システムクラッシュ、ハードウェア障害、およびその他の異常。
 6. ファイアウォールおよびルーターアクティビティ。
 7. CA 施設への出入記録。

ログ記録には、以下の要素を含める必要がある。

1. 記録の日時。
2. ジャーナルレコードを作成する人の身元。
3. 記録の詳細。

5.4.2 監査ログを処理する頻度

本 CA は、監査ログを定期的に確認する。

5.4.3 監査ログを保持する期間

本 CA は、本 CA のシステムに関する監査ログを、アーカイブとして最低 10 年保存する。入退室、ネットワークに関するログについては最低 1 年間保存する。ただし、Baseline Requirements に関連する場合、本 CA は、少なくとも 2 年間、以下を保持するものとする。

1. CA 証明書および鍵のライフサイクル管理イベント記録 (本 CP「5.4.1 記録される イ

ベントの種類」に記載) は、以下のいずれかが発生した後に保持する。

1. CA 私有鍵の破壊
2. cA フィールドが true に設定された X.509v3 basicConstraints 拡張を持ち、CA 私有鍵に対応する共通の公開鍵を共有する一連の証明書のうち、最後の CA 証明書の失効または有効期限切れ。
2. 利用者向け証明書の失効または満了後の利用者向け証明書ライフサイクル管理イベントレコード (本 CPS 「5.4.1 記録されるイベントの種類」に記載)。
3. イベント発生後のセキュリティイベントレコード (本 CPS 「5.4.1 記録されるイベントの種類」に記載)

5.4.4 監査ログの保護

本 CA は、認可された者のみが監査ログにアクセスすることができるよう、適切なアクセスコントロールを採用し、許可されていない者が閲覧できないようにする。

5.4.5 監査ログのバックアップ手続

監査ログはオフラインの記録媒体にバックアップとして取得し、それらの媒体を安全な場所に保管する。

5.4.6 監査ログの収集システム

監査ログの収集システムは、本 CA のシステムの機能に含まれている。

5.4.7 イベントを起こした者への通知

本 CA は、監査ログの収集を、事象を発生させた人、システムまたはアプリケーションに対して通知することなく行う。

5.4.8 脆弱性評価

本 CA は、監査ログの検査結果をもとに、運用面およびシステム動作面におけるセキュリティ上の脆弱性を評価するとともに、必要に応じて最新の実装可能なセキュリティテクノロジーの導入等、セキュリティ対策の見直しを行う。

さらに CA のセキュリティプログラムには、以下のような年次リスクアセスメントを含める必要がある。

1. 証明書データまたは証明書管理プロセスに対する不正なアクセス、開示、不正使用、改変、または破壊につながる、予測可能な内外の脅威を特定する。
2. 証明書データおよび証明書管理プロセスの機密性を考慮して、これらの脅威の可能性及び潜在的な損害を評価する。
3. このような脅威に対抗するために CA が導入しているポリシー、手順、情報システム、技術、およびその他の取り決めが十分であるかどうかを評価する。

5.5 記録の保管

5.5.1 アーカイブの種類

本 CA は、本 CPS 「5.4.1.記録されるイベントの種類」の本 CA のシステムに関するログに加えて、次の情報をアーカイブとして保存する。

- ・発行した証明書および CRL
- ・CRL の発行に関する処理履歴
- ・本 CPS
- ・本 CPS に基づき作成された認証局の業務運用を規定する文書
- ・認証業務を他に委託する場合には、委託契約に関する書類
- ・監査の実施結果に関する記録および監査報告書
- ・証明書利用者からの申請書類
- ・OCSP レスポンダーへのアクセスログ (OCSP レスポンダーを使用している CA の場合)

5.5.2 アーカイブ保存期間

本 CA は、アーカイブを最低 10 年間保存する。

ただし、Baseline Requirements に関連する場合、アーカイブされた監査ログ(本 CPS 「5.5.1 アーカイブの種類」で規定)は、記録作成タイムスタンプから少なくとも 2 年間、または本 CPS 「5.4.3 監査ログを保持する期間」に従って保持する必要がある限り、いずれか長い方の期間保持する。

5.5.3 アーカイブの保護

アーカイブは、許可された者以外がアクセスできないよう制限された施設において保管する。

5.5.4 アーカイブのバックアップ手続

証明書発行、取消または CRL の発行等、本 CA のシステムに関する重要なデータに変更がある場合は、適時、アーカイブのバックアップを取得する。

5.5.5 記録にタイムスタンプを付与する要件

本 CA は、NTP (Network Time Protocol) を使用して本 CA のシステムの時刻同期を行い、本 CA のシステム内で記録される重要な情報に対しタイムスタンプを付与する。

5.5.6 アーカイブ収集システム

アーカイブの収集システムは、本 CA のシステムの機能に含まれている。

5.5.7 アーカイブの検証手続

アーカイブは、セキュアな保管庫からアクセス権限者が入手し、定期的に媒体の保管状況の

確認を行う。また必要に応じ、アーカイブの完全性および機密性の維持を目的として、新しい媒体への複製を行う。

5.6 鍵の切り替え

本項については、CP に規定する。

5.7 危殆化および災害からの復旧

5.7.1 事故および危殆化時の手続

CA 私有鍵が危殆化または危殆化のおそれがある場合および災害等により本サービスの中断、停止につながるような状況が発生した場合には、予め定められた計画、手順に従い、安全にサービスを再開させる。

本 CA は、インシデント対応計画および災害復旧計画を準備するものとする。

本 CA は、災害、セキュリティの危殆化、または企業倒産が発生した場合にアプリケーションソフトウェアサプライヤー、証明書利用者、および依頼当事者に通知し、それらを合理的に保護するように設計された、事業継続および災害復旧手順を文書化するものとする。本 CA は事業継続計画を公開する必要はないが、本 CA の監査人が要求した時には事業継続計画とセキュリティ計画を提供できるようにするものとする。本 CA は、年 1 回これらの手順をテスト、レビュー、および更新するものとする。

事業継続計画には以下を含めなければならない。

1. 計画を始動するための条件
2. 緊急対応手順
3. フォールバック手順
4. 再開手順
5. 計画の保守スケジュール
6. 意識向上および教育要件
7. 個人の責任範囲
8. 目標復旧時間(RTO)
9. 緊急対策計画の定期的なテスト
10. 重要な事業プロセスの中断または障害発生後、タイムリーに CA の事業運営を維持または復元するための計画
11. 重要な暗号化資材(つまり、セキュリティ保護された暗号化装置やアクティベーション資材)を代替場所に保管するための要件
12. 容認可能なシステム停止期間および回復時間
13. 必須の事業情報およびソフトウェアのバックアップコピーの作成頻度
14. 復旧施設から CA のメインサイトまでの距離

15. 災害発生から元のサイトまたはリモートサイトで安全な環境を復元するまでの期間に可能な範囲で設備を保護するための手順

5.7.2 ハードウェア、ソフトウェアまたはデータが破損した場合の手続

本 CA は、本 CA のシステムのハードウェア、ソフトウェアまたはデータが破損した場合、バックアップ用として保管しているハードウェア、ソフトウェアまたはデータを使用して、すみやかに本 CA のシステムの復旧作業を行う。

5.7.3 私有鍵が危殆化した場合の手続

本 CA は、本 CA の私有鍵が危殆化したまたは危殆化のおそれがあると判断した場合、および災害等により本 CA のシステムの運用が中断、停止につながるような状況が発生した場合には、予め定められた計画、手順に従い、安全に運用を再開させる。

5.7.4 災害後の事業継続性

本 CA は、不測の事態が発生した場合にすみやかに復旧作業を実施できるよう、予め本 CA のシステムの代替機の確保、復旧に備えたバックアップデータの確保、復旧手続の策定等、可能な限りすみやかに本 CA のシステムを復旧するための対策を行う。

5.8 認証局または登録局の終了

本項については、CP に規定する。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成およびインストール

本項について、本 CPS では、本 CA の鍵管理に関して規定する。証明書利用者を含むその他関係者に関する鍵管理については CP に規定する。

6.1.1 鍵ペアの生成

本 CA の鍵ペアに対しては以下の管理を行う。

1. 鍵生成スクリプトを用意して、スクリプトに従って実施する。
2. 公認監査人に CA 鍵ペア生成プロセスに立ち会わせる、または CA 鍵ペア生成プロセス全体を録画する。

本 CA は以下を実施するものとする。

1. 本 CPS および CP の内容に従って物理的に保護された環境で CA 鍵ペアを生成する。
2. 複数人物による統制および知識分割の原則に基づく信頼された役割の担当者により CA 鍵ペアを生成する。
3. 本 CPS および CP で公開されている適切な技術および事業要件を満たす暗号化モジュール内で CA 鍵ペアを生成する。本 CA の鍵ペアは FIPS140-1 レベル 3 の認定を取得したハードウェアセキュリティモジュール (Hardware Security Module: 以下、「HSM」という) 上で生成する。
4. CA 鍵ペア生成アクティビティをログ記録する。
5. 私有鍵が本 CPS、CP および鍵生成スクリプトに記載されている手順に従って生成および保護されたことを合理的に保証する効果的な統制を維持する。

Baseline Requirements に準拠した利用者向け証明書の鍵ペア生成に関しては、次の条件の1つ以上が満たされた場合、本 CA は証明書要求を拒否する必要がある。

1. 鍵ペアが CP 「6.1.5 鍵サイズ」または CP 「6.1.6 公開鍵のパラメータの生成および品質検査」に記載されている要件を満たしていない。
2. 私有鍵の生成に使用された特定の手法に欠陥があるという明確な証拠がある。
3. 本 CA は、申請者の私有鍵を危殆化させる、実証済みまたは証明された方法を認識している。
4. 本 CA は、CP 「4.9.1 証明書失効事由」の規定などにより、申請者の私有鍵が鍵の危殆化を受けたことを以前に認識していた。
5. 本 CA は、公開鍵 (Debian の弱い鍵など。 <https://wiki.debian.org/SSLkeys> を参照) に基づいて申請者の私有鍵を簡単に計算するための実証済みまたは証明された方法を

認識している。

6.1.2 証明書利用者に対する私有鍵の交付

本項については、CPに規定する。

6.1.3 認証局への公開鍵の交付

本 CA に対する証明書利用者の公開鍵の送付は、証明書の申請時にオンラインによって行うことができる。この時の通信経路は TLS により暗号化を行う。

6.1.4 検証者への CA 公開鍵の交付

本項については、CPに規定する。

6.1.5 鍵サイズ

本項については、CPに規定する。

6.1.6 公開鍵のパラメータの生成および品質検査

本 CA のシステムで使用する HSM は、暗号機能の品質検査機能を有する。公開鍵のパラメータは、品質検査の行われた暗号機能を用いて生成される。

RSA について、本 CA は、公開指数の値が 3 以上の奇数であることを確認する。加えて、公開指数は $2^{16}+1$ および $2^{256}-1$ の範囲内であるべきとする。法の特性として、奇数であること、素数の累乗ではないこと、752 より小さい因数がないこととする。[参照: Section 5.3.3, NIST SP 800-89]

ECDSA について、本 CA は、ECDSA 完全公開鍵検証ルーチンまたは ECDSA 部分公開鍵検証ルーチンを使用して、すべての鍵の有効性を確認する。[参照: NIST SP800-56A: Revision2 の Section 5.6.2.3.2 と 5.6.2.3.3]

6.1.7 鍵の用途

本項については、CPに規定する。

6.2 私有鍵の保護および暗号モジュール技術の管理

本 CA は、不正な証明書発行を防止するための物理的および論理的な保護対策を実装する。前述の検証済みのシステムまたはデバイス外部での CA 私有鍵の保護は、CA 私有鍵の開示を防止する方法で実装された、物理セキュリティ、暗号化、またはその両方の組み合わせから構成する。CA は、暗号化された鍵または鍵の一部の残存期間中、暗号解読攻撃に耐えることができる最先端技術のアルゴリズムおよび鍵長によって、私有鍵を暗号化する。

6.2.1 暗号モジュールの標準および管理

本 CA の私有鍵の生成、保管、署名操作は、FIPS140-2 レベル 3 準拠の HSM を用いて行う。

6.2.2 私有鍵の複数人管理

本 CA の私有鍵の活性化、非活性化、バックアップ等の操作は、安全な環境において複数人の権限者によって行う。

6.2.3 私有鍵のエスクロー

本 CA の私有鍵のエスクローは行わない。

6.2.4 私有鍵のバックアップ

本 CA の私有鍵のバックアップは、複数名の権限者によって行われ、暗号化された状態で、セキュアな室に保管される。

6.2.5 私有鍵のアーカイブ

本 CA 私有鍵のアーカイブは行わない。

6.2.6 私有鍵の暗号モジュールへのまたは暗号モジュールからの転送

本 CA の私有鍵の HSM への転送または HSM からの転送は、セキュアな室において、私有鍵を暗号化した状態で行う。

6.2.7 暗号モジュールへの私有鍵の格納

本 CA の私有鍵は、暗号化された状態で HSM 内に格納する。

6.2.8 私有鍵の活性化方法

本 CA の私有鍵の活性化は、セキュアな室において複数名の権限者によって行う。

6.2.9 私有鍵の非活性化方法

本 CA の私有鍵の非活性化は、セキュアな室において複数名の権限者によって行う。

6.2.10 私有鍵の破棄方法

本 CA の私有鍵の廃棄は、複数名の権限者によって完全に初期化または物理的に破壊することによって行う。バックアップについても同様の手続によって行う。

6.2.11 暗号モジュールの評価

本 CA のシステムで使用する HSM の品質基準については、本 CPS 「6.2.1.暗号モジュールの標準および管理」のとおりである。

6.3 鍵ペアのその他の管理方法

6.3.1 公開鍵のアーカイブ

本 CA の公開鍵のアーカイブは、本 CPS 「5.5.1 アーカイブの種類」に含まれる。

6.3.2 証明書の有効期間と私有鍵および公開鍵の有効期間

本 CA の鍵ペアの有効期間は定めないが、CA 証明書の有効期間は 20 年以下を想定している。

また、本 CA が証明書利用者向けに発行するサーバー証明書の有効期間については、CP に規定する。

OCSP 証明書は、125 日を超える有効期間を設定してはならない。

計算上、1 日は 86,400 秒となる。これを超える時間は、小数点以下の秒数やうるう秒を含めて、追加の 1 日を意味する。

6.4 活性化データ

6.4.1 活性化データの生成および設定

本 CA の私有鍵を操作するために必要な活性化データは、複数名の権限者によって生成され、電子媒体に格納する。

6.4.2 活性化データの保護

本 CA の私有鍵の活性化に必要なデータが格納された電子媒体は、セキュアな室において保管管理を行う。

6.4.3 活性化データの他の考慮点

本 CA の私有鍵の活性化データの生成や設定等の管理は、本 CPS 「5.2.1.信頼される役割」に記載された者が行う。

6.5 コンピュータのセキュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件

本 CA は、本 CA のシステムに導入するハードウェア、ソフトウェアに対して、その品質、安定性、安全性等について十分に検討を行い、導入を決定する。

本 CA は、証明書を直接発行させることができるすべてのアカウントに対して、多要素認証を実施するものとする。

6.5.2 コンピュータセキュリティ評価

本 CA は、本 CA のシステムにおいて使用するすべてのソフトウェア、ハードウェアに対して事前にシステムテストを行い、本 CA のシステムの信頼性の確保に努める。また、本 CA のシステムのセキュリティ上の脆弱性についての情報収集、評価を継続的に行い、脆弱性が

発見された場合には、すみやかに必要な対処を行う。

6.6 ライフサイクルの技術的管理

6.6.1 システム開発管理

本 CA のシステムの構築およびメンテナンスは、安全な環境下で行う。本 CA のシステムの変更を行う場合は、十分に安全性の評価、確認を行う。また、本 CA のシステムに対して、適切なサイクルで最新のセキュリティ技術を導入するためにセキュリティチェックを行い、セキュリティを確保する。

6.6.2 セキュリティ運用管理

本 CA は、情報資産管理、要員管理、権限管理等の運用管理の実施、不正侵入対策、ウイルス対策等のセキュリティ対策ソフトウェアの適時更新等を行い、セキュリティを確保する。

6.6.3 ライフサイクルセキュリティ管理

本 CA は、本 CA のシステムのシステム開発、運用、保守が適切に行われていることを適時評価し、必要に応じ改善を行う。

6.7 ネットワークセキュリティ管理

本 CA は、本 CA のシステムへのネットワークからの不正アクセス対策として、ファイアウォール、IDS 等を設置する。

6.8 タイムスタンプ

タイムスタンプに関する要件は、本 CPS「5.5.5 記録にタイムスタンプを付与する要件」と同様とする。

7. 証明書および証明書失効リストのプロファイル

7.1 証明書のプロファイル

7.1.1 バージョン番号

本項については、CP に規定する。

7.1.2 証明書の拡張

本項については、CP に規定する。

7.1.3 アルゴリズムオブジェクト識別子

本項については、CP に規定する。

7.1.4 名前の形式

本項については、CP に規定する。

7.1.5 名前制約

本項については、CP に規定する。

7.1.6 証明書ポリシーオブジェクト識別子

本項については、CP に規定する。

7.1.7 ポリシー制約拡張の使用

本項については、CP に規定する。

7.1.8 ポリシー修飾子の構文および意味

本項については、CP に規定する。

7.1.9 クリティカルな証明書ポリシー拡張に対する解釈の方法

本項については、CP に規定する。

7.2 CRL のプロファイル

7.2.1 バージョン番号

本項については、CP に規定する。

7.2.2 証明書失効リストおよび証明書失効リストエントリ拡張

本項については、CP に規定する。

7.3 OCSP のプロファイル

7.3.1 バージョン番号

本項については、CP に規定する。

7.3.2 OCSP 拡張

本項については、CP に規定する。

8. 準拠性監査と他の評価

8.1 監査の頻度

本 CA は、電子認証基盤の運用が本 CPS に準拠して行われているかについて、適時、監査を行う。

新しい利用者向け証明書を発行するために使用することができる証明書は、CP「7.1.5 名前制約」に従って技術的に制約され、かつ CP「8.7 自己監査」に従って監査されているか、制約はされていないものの、このセクションの残りすべての要件に従って完全に監査されているかのいずれかである必要がある。証明書は、X.509v3 basicConstraints 拡張領域を含み、cAboolean が true に設定された、ルート CA 証明書または下位 CA 証明書である場合、新規証明書の発行に使用可能と見なされる。

本 CA が利用者向け証明書を発行している期間は、監査期間の連続したシーケンスに分割されるものとする。監査期間は 1 年を超えてはならない。

本 CA が、本 CPS「8.4 監査で扱われる事項」に記載された監査スキームに準拠していることを示す現在有効な監査レポートを有している場合、発行前準備の評価は必要ない。

本 CA が、本 CPS「8.4 監査で扱われる事項」に記載された監査スキームのいずれかに準拠していることを示す現在有効な監査レポートを有していない場合、本 CA は、パブリックな信頼された利用者向け証明書を発行する前に、本 CPS「8.4 監査で扱われる事項」に記載された監査スキームのいずれかに基づき、適用される規準に従って実施される時点での準備状況の評価を完了しなければならない。当該準備状況の評価は、パブリック証明書を発行する 12 か月前までに完了し、最初のパブリック証明書を発行してから 90 日以内に、当該スキームに基づく完全な監査を受けなければならない。

8.2 監査者の身元／資格

本 CA の監査は、公認監査人が行わなければならない。公認監査人とは、以下の資格および技能を総合的に有する自然人、法人、または自然人もしくは法人のグループをいう。

1. 監査の対象から独立している。
2. 適格な監査スキームで指定されている条件に対応する監査を実施できる（本 CPS「8.4 監査で扱われる事項」を参照）。
3. 公開鍵基盤技術、情報セキュリティツールおよび技法、情報技術およびセキュリティ監査、および第三者認証機能の審査に熟達している人材を採用している。
4. (WebTrust 規格に基づいて実施される監査の場合) WebTrust による実施許可を受けている。
5. 法律、政府の規制、または職業倫理に準拠している。

- 国内政府監査機関の場合を除き、少なくとも 100 万米ドルの補償を保険範囲とする業務上の過失および不備に対する責任保険に加入している。

8.3 監査者と被監査者の関係

監査人は、監査に関する事項を除き、被監査部門の業務から独立した立場にあるものとする。監査の実施にあたり、被監査部門は監査に協力するものとする。

8.4 監査で扱われる事項

監査は、本 CA の運用の本 CPS に対する準拠性を中心として行う。

本 CA は、必要に応じて以下のスキームに従って監査を受けるものとする。

- ・ WebTrust for CAs
- ・ WebTrust for CAs SSL Baseline with Network Security

監査が継続的にスキームの要件に従って実施されるようにするため、定期的な監査手順や説明責任手順を組み込む必要がある。

監査は、本 CPS「8.2 監査人の身分と資格」の規定どおり、公認監査人によって実施される必要がある。

外部委託先がエンタープライズ RA でない場合、本 CA は、本 CPS「8.4 監査で扱われる事項」に記載された容認されている監査スキームの基になる監査標準に従って発行された監査レポートを取得するものとする。

この監査レポートは、外部委託先の遂行する監査が外部委託先の運用規定または本 CA の CP/CPS に準拠するかどうかについての意見を提供する。外部委託先が条件に準拠しないという意見である場合、本 CA は、外部委託先による委託職務の履行継続を許可しないものとする。

外部委託先による監査期間は、1年を超えないものとする（この場合、本 CA の監査と整合することが望ましい）。

8.5 不備の結果としてとられる処置

本 CA は、監査報告書で指摘された事項に関し、すみやかに必要な是正措置を行う。

8.6 監査結果の開示

監査結果は、監査人から本 CA に対して報告される。

本 CA は、法律に基づく開示要求があった場合、当社との契約に基づき関係組織からの開示要求があった場合、または本 CA のサーバー証明書発行サービス運営会議が承認した場合を除き、監査結果を外部へ開示することはない。

なお、WebTrust 認証に関する報告書は、WebTrust 認証の規則に従い、特定のサイトにて参照可能となる。

8.7 内部監査

本 CA は、CA の運用が本 CPS、CP および Baseline Requirement に準拠して行われているかについて内部監査を行い、Baseline Requirement で定められた要件に基づき、証明書の無作為のサンプル抽出による定期的な検証を実施する。

本 CA が証明書を発行する期間中、本 CA は、前の自己監査でサンプルが取得された直後から始まる期間に発行された Baseline Requirements に準拠した証明書のうち 2 つ以上、または 3%のいずれか多い方の数の証明書をサンプルとしてランダムに選択し、少なくとも四半期に 1 回の頻度で自己監査を実施して、本 CPS、CP および Baseline Requirements への準拠を監視し、サービス品質を厳密に管理するものとする。本 CPS「8.4 監査で扱われる事項」に規定されている条件を満たす年次監査対象の外部委託先を除き、本 CA は、最後のサンプルが取得された直後から始まる期間に外部委託先によって検証された Baseline Requirements に準拠した証明書のうち 2 つ以上、あるいは 3%のいずれか多い方の数の証明書をサンプルとしてランダムに選択し、本 CA が雇用する検証スペシャリストに四半期に 1 回の監査を継続的に実施させることで、外部委託先によって発行された証明書または検証された情報を含む証明書のサービス品質を厳密に管理するものとする。本 CA は、各外部委託先の運用および手順をレビューして、外部委託先が Baseline Requirements、ならびに本 CPS および CP に準拠していることを保証するものとする。本 CA は、年 1 回の頻度で、各外部委託先が Baseline Requirements に準拠しているかどうかを内部監査するものとする。技術的に制約された CA が Baseline Requirements に準拠した証明書を発行する期間中、本 CA の CP への準拠状況を監視するものとする。本 CA は、少なくとも四半期に 1 回の頻度で、最後のサンプルが取得された直後から始まる期間において CA によって発行された証明書のうち 2 つ以上、あるいは 3%のいずれか多い方の数の証明書をサンプルとしてランダムに選択し、CP に準拠していることを確認する。

9. 他の業務上および法的事項

9.1 料金

本項については、CP に規定する。

9.2 財務的責任

本 CA は、本 CA の運用維持にあたり、十分な財務的基盤を維持するものとする。

9.3 企業情報の機密性

9.3.1 機密情報の範囲

本 CA が保持する個人情報および組織情報は、証明書、CRL、本 CPS および CP の一部として明示的に公表されたものを除き、機密保持対象として扱われる。

本 CA は、法の定めによる場合および証明書利用者による事前の承諾を得た場合を除いてこれらの情報を社外に開示しない。かかる法的手続、司法手続、行政手続あるいは法律で要求されるその他の手続に関連してアドバイスする法律顧問および財務顧問に対し、本 CA は機密保持対象として扱われる情報を開示することができる。また会社の合併、買収あるいは再編成に関連してアドバイスする弁護士、会計士、金融機関およびその他の専門家に対して、本 CA は機密保持対象として扱われる情報を開示することができる。

9.3.2 機密情報の範囲外の情報

証明書および CRL に含まれている情報は機密保持対象外として扱う。その他、次の状況におかれた情報は機密保持対象外とする。

- ・本CAの過失によらず知られた、あるいは知られるようになった情報
- ・本CA以外の出所から、機密保持の制限無しに本CAに知られた、あるいは知られるようになった情報
- ・本CAによって独自に開発された情報
- ・開示に関して証明書利用者によって承認されている情報

9.3.3 機密情報を保護する責任

本 CA は、法の定めによる場合および証明書利用者による事前の承諾を得た場合に機密情報を開示することがある。その際、その情報を知り得た者は、契約あるいは法的な制約によりその情報を第三者に開示させない。

9.4 個人情報の保護

当社の個人情報保護方針については、ホームページにて公表する。

9.5 知的財産権

本 CPS は、「クリエイティブ・コモンズ表示・改変禁止 4.0 国際ライセンス」の下に公開する。



(<https://creativecommons.org/licenses/by-nc/4.0/>)

その他の事項については、CP に規定する。

9.6 表明保証

9.6.1 CA 業務の表明保証

本項については、CP に規定する。

9.6.2 RA 業務の表明保証

本項については、CP に規定する。

9.6.3 証明書利用者の表明保証

本項については、CP に規定する。

9.6.4 検証者の表明保証

本項については、CP に規定する。

9.6.5 その他関係者の表明保証

本項については、CP に規定する。

9.7 無保証

本項については、CP に規定する。

9.8 責任の制限

本項については、CP に規定する。

9.9 補償

本項については、CP に規定する。

9.10 有効期間と終了

9.10.1 有効期間

本 CPS は、本 CA のサーバー証明書発行サービス運営会議の承認により有効となる。本 CPS 「9.10.2 終了」に規定する終了以前に本 CPS が無効となることはない。

9.10.2 終了

本 CPS は、「9.10.3 終了の効果と効果継続」に規定する内容を除き、本 CA の終了と同時に無効となる。

9.10.3 終了の効果と効果継続

証明書利用者と本 CA との間で利用契約等を終了する場合、または本 CA 自体を終了する場合であっても、その性質上存続されるべき条項は終了の事由を問わず証明書利用者、検証者および本 CA に適用されるものとする。

9.11 関係者間の個別通知と連絡

当社は、証明書利用者、検証者に対する必要な通知をホームページ上、電子メールまたは書面等によって行う。

9.12 改訂

9.12.1 改訂手続

本 CPS は、本 CA の判断によって適宜改訂され、本 CA のサーバー証明書発行サービス運営会議の承認によって発効する。

9.12.2 通知方法および期間

本 CPS を変更した場合、変更した本 CPS をすみやかに公表することにより、証明書利用者に対しての告知とする。

9.12.3 オブジェクト識別子の変更されなければならない場合

規定しない。

9.13 紛争解決手続

本項については、CP に規定する。

9.14 準拠法

本項については、CP に規定する。

9.15 適用法の遵守

本項については、CP に規定する。

9.16 雑則

本項については、CP に規定する。

9.17 その他の条項

本項については、CP に規定する。