

JPRSサーバー証明書
（組織認証型）
認証局証明書ポリシー
（Certificate Policy）
Version 2.20

2019年08月01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	2016.04.26	初版発行
1.10	2017.02.19	・「4.6 証明書の更新」に関する記述の追加 ・「4.8 証明書の変更」に関する記述の追加
1.20	2017.09.06	・ Baseline Requirements に準拠する旨の記述の追加 ・ CAA レコードの処理に関する記述の修正
1.30	2017.10.18	・ 組織単位名（OU）に指定する、または含めることのできな い文字列の追加に伴う修正
1.40	2018.01.17	・ 証明書の有効期間の上限に関する記述の修正
2.00	2018.04.05	・ Certificate Transparency 対応に伴う記述の追加
2.10	2018.08.01	・ OV 証明書の審査方法変更に伴う記述の修正
2.20	2019.08.01	・ 認証局切替に伴う記述の追加、その他表記修正等

目次

1. はじめに.....	9
1.1 概要.....	9
1.2 文書名と識別.....	10
1.3 PKI の関係者.....	10
1.3.1 認証局.....	10
1.3.1.1 IA.....	10
1.3.1.2 RA.....	10
1.3.2 証明書利用者.....	10
1.3.3 検証者.....	10
1.4 証明書の用途.....	11
1.4.1 適切な証明書の用途.....	11
1.4.2 禁止される証明書の用途.....	11
1.5 ポリシー管理.....	11
1.5.1 文書を管理する組織.....	11
1.5.2 連絡先.....	11
1.5.3 ポリシー適合性を決定する者.....	11
1.5.4 承認手続.....	11
1.6 定義と略語.....	11
2. 公開とリポジトリの責任.....	15
2.1 リポジトリ.....	15
2.2 情報の公開.....	15
2.3 公開の時期または頻度.....	15
2.4 リポジトリへのアクセス管理.....	15
3. 識別と認証.....	16
3.1 名前決定.....	16
3.1.1 名前の種類.....	16
3.1.2 名前が意味を持つことの必要性.....	16
3.1.3 証明書利用者の匿名性または仮名性.....	17
3.1.4 様々な名前形式を解釈するための規則.....	17
3.1.5 名前の一意性.....	17
3.1.6 商標の認識、認証および役割.....	17
3.2 初回の本人性確認.....	17
3.2.1 私有鍵の所持を証明する方法.....	17
3.2.2 組織の認証.....	17

3.2.3	個人の認証	17
3.2.4	検証されない証明書利用者の情報	17
3.2.5	権限の正当性確認	17
3.2.6	相互運用の基準	18
3.2.7	ドメイン名の認証	18
3.3	鍵更新申請時の本人性確認と認証	18
3.4	失効申請時の本人性確認と認証	18
4.	証明書のライフサイクルに対する運用上の要件	19
4.1	証明書申請	19
4.1.1	証明書申請を提出することができる者	19
4.1.2	申請手続および責任	19
4.2	証明書申請手続	19
4.2.1	本人性確認と認証の実施	19
4.2.2	証明書申請の承認または却下	19
4.2.3	証明書申請の処理時間	19
4.2.4	CAA レコードの確認	19
4.3	証明書の発行	20
4.3.1	証明書発行時の処理手続	20
4.3.2	証明書利用者への証明書発行通知	20
4.4	証明書の受領確認	20
4.4.1	証明書の受領確認手続	20
4.4.2	認証局による証明書の公開	20
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	20
4.5	鍵ペアおよび証明書の用途	20
4.5.1	証明書利用者の私有鍵および証明書の用途	20
4.5.2	検証者の公開鍵および証明書の用途	20
4.6	鍵更新を伴わない証明書の更新	21
4.6.1	鍵更新を伴わない証明書の更新事由	21
4.6.2	証明書の更新申請を行うことができる者	21
4.6.3	証明書の更新申請の処理手続	21
4.6.4	証明書利用者に対する新しい証明書発行通知	21
4.6.5	更新された証明書の受領確認手続	21
4.6.6	認証局による更新された証明書の公開	21
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	21
4.7	鍵更新を伴う証明書の更新	21
4.7.1	鍵更新を伴う証明書の更新事由	21

4.7.2	新しい証明書の申請を行うことができる者	21
4.7.3	鍵更新を伴う証明書の更新申請の処理手続	22
4.7.4	証明書利用者に対する新しい証明書の通知	22
4.7.5	鍵更新された証明書の受領確認手続	22
4.7.6	認証局による鍵更新済みの証明書の公開	22
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	22
4.8	証明書の変更	22
4.8.1	証明書の変更事由	22
4.8.2	証明書の変更申請を行うことができる者	22
4.8.3	証明書の変更申請の処理手続	22
4.8.4	証明書利用者に対する新しい証明書発行通知	22
4.8.5	変更された証明書の受領確認手続	22
4.8.6	認証局による変更された証明書の公開	22
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	22
4.9	証明書の失効と一時停止	23
4.9.1	証明書失効事由	23
4.9.2	証明書失効を申請することができる者	23
4.9.3	失効申請手続	23
4.9.4	失効申請の猶予期間	23
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	24
4.9.13	証明書の一時停止事由	24
4.9.14	証明書の一時停止を申請することができる者	24
4.9.15	証明書の一時停止申請手続	24
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.....	26
5.2 手続的管理.....	26
5.2.1 信頼すべき役割.....	26
5.2.2 職務ごとに必要とされる人数.....	26
5.2.3 個々の役割に対する本人性確認と認証.....	26
5.2.4 職務分割が必要となる役割.....	26
5.3 人事的管理.....	26
5.3.1 資格、経験および身分証明の要件.....	26
5.3.2 適性調査.....	27
5.3.3 教育要件.....	27
5.3.4 再教育の頻度および要件.....	27
5.3.5 仕事のローテーションの頻度および順序.....	27
5.3.6 認められていない行動に対する制裁.....	27
5.3.7 業務委託先の管理.....	27
5.3.8 要員へ提供される資料.....	27
5.4 監査ログの手続.....	27
5.4.1 記録されるイベントの種類.....	27
5.4.2 監査ログを処理する頻度.....	28
5.4.3 監査ログを保持する期間.....	28
5.4.4 監査ログの保護.....	28
5.4.5 監査ログのバックアップ手続.....	28
5.4.6 監査ログの収集システム.....	28
5.4.7 イベントを起こした者への通知.....	28
5.4.8 脆弱性評価.....	28
5.5 記録の保管.....	28
5.5.1 アーカイブの種類.....	28
5.5.2 アーカイブ保存期間.....	28
5.5.3 アーカイブの保護.....	29
5.5.4 アーカイブのバックアップ手続.....	29
5.5.5 記録にタイムスタンプを付与する要件.....	29
5.5.6 アーカイブ収集システム.....	29
5.5.7 アーカイブの検証手続.....	29

5.6	鍵の切り替え	29
5.7	危殆化および災害からの復旧	29
5.8	認証局または登録局の終了	29
6.	技術的セキュリティ管理	30
6.1	鍵ペアの生成およびインストール	30
6.1.1	鍵ペアの生成	30
6.1.2	証明書利用者に対する私有鍵の交付	30
6.1.3	認証局への公開鍵の交付	30
6.1.4	検証者への CA 公開鍵の交付	30
6.1.5	鍵サイズ	30
6.1.6	公開鍵のパラメータの生成および品質検査	30
6.1.7	鍵の用途	30
6.2	私有鍵の保護および暗号モジュール技術の管理	31
6.3	鍵ペアのその他の管理方法	31
6.4	活性化データ	31
6.5	コンピュータのセキュリティ管理	31
6.6	ライフサイクルの技術的管理	31
6.7	ネットワークセキュリティ管理	31
6.8	タイムスタンプ	31
7.	証明書および証明書失効リストのプロファイル	32
7.1	証明書のプロファイル	32
7.2	CRL のプロファイル	35
7.3	OCSP のプロファイル	36
7.3.1	バージョン番号	38
7.3.2	OCSP 拡張	38
8.	準拠性監査と他の評価	39
8.1	監査の頻度	39
8.2	監査者の身元／資格	39
8.3	監査者と被監査者の関係	39
8.4	監査で扱われる事項	39
8.5	不備の結果としてとられる処置	39
8.6	監査結果の開示	39
9.	他の業務上および法的事項	40
9.1	料金	40
9.2	財務的責任	40
9.3	企業情報の機密性	40

9.3.1 機密情報の範囲.....	40
9.3.2 機密情報の範囲外の情報	40
9.3.3 機密情報を保護する責任	40
9.4 個人情報の保護.....	40
9.5 知的財産権	40
9.6 表明保証.....	41
9.6.1 認証局の表明保証.....	41
9.6.1.1 IA の表明保証.....	41
9.6.1.2 RA の表明保証.....	41
9.6.2 証明書利用者の表明保証	41
9.6.3 検証者の表明保証.....	41
9.6.4 他の関係者の表明保証.....	41
9.7 無保証.....	41
9.8 責任の制限	42
9.9 補償.....	42
9.10 有効期間と終了	42
9.10.1 有効期間	42
9.10.2 終了.....	42
9.10.3 終了の効果と効果継続.....	43
9.11 関係者間の個別通知と連絡.....	43
9.12 改訂	43
9.12.1 改訂手続	43
9.12.2 通知方法および期間.....	43
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	43
9.13 紛争解決手続.....	43
9.14 準拠法.....	43
9.15 適用法の遵守.....	43
9.16 雑則	44
9.17 その他の条項.....	44

1. はじめに

1.1 概要

JPRS サーバー証明書（組織認証型）認証局証明書ポリシー（以下「本 CP」という）は、株式会社日本レジストリサービス（以下「当社」という）が認証局（以下「本 CA」という）として発行する電子証明書の用途、利用目的、適用範囲等、電子証明書に関するポリシーを規定するものである。

本 CA の運用維持に関する諸手続については、セコム認証基盤運用規程（以下「CPS」という）に規定する。

本 CA は、セコムトラストシステムズ株式会社（以下「セコムトラストシステムズ」という）が運営する認証局である Security Communication RootCA2 より、片方向相互認証証明書の発行を受けており、証明書利用者に対する証明書発行を行う。

本 CA が発行する証明書は、サーバー認証および通信経路で情報の暗号化を行うことに利用する。証明書の有効期間は、証明書を有効とする日から起算して 825 日以内とする。また、発行対象は、JPRS サーバー証明書発行サービスご利用条件（以下「ご利用条件」という）により定める。

本 CA から証明書の発行を受ける者は、証明書の発行を受ける前に自己の利用目的とご利用条件、本 CP および CPS とを照らし合わせて評価し、ご利用条件、本 CP および CPS を承諾する必要がある。

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 Certificates」（以下「Baseline Requirements」という）および RFC 5280「Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile」に準拠する。

なお、本 CP の内容がご利用条件、CPS の内容に抵触する場合は、ご利用条件、本 CP、CPS の順に優先して適用されるものとする。

本 CP は、IETF が認証局運用のフレームワークとして提唱する RFC 3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。

本 CP は、本 CA に関する技術面、運用面の発展や改良に伴い、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 CP の正式名称は、「JPRS サーバー証明書（組織認証型）認証局証明書ポリシー」という。

本 CA が本 CP 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 CP が参照する CPS の OID は、次のとおりである。

名称	OID
JPRS サーバー証明書（組織認証型）認証局証明書ポリシー（CP）	1.2.392.200091.110.208.2
セコム電子認証基盤認証運用規程（CPS）	1.2.392.200091.100.401.1

1.3 PKI の関係者

1.3.1 認証局

CA（Certification Authority：認証局）とは、IA（Issuing Authority：発行局）および RA（Registration Authority：登録局）によって構成される。本 CA においては、セコムトラストシステムズが IA としての役割を担い、当社が RA としての役割を担う。

1.3.1.1 IA

IA は、証明書の発行、取消、証明書失効リスト（以下「CRL」という）の開示等を行う。

1.3.1.2 RA

RA は、証明書の発行、取消を申請する申請者の審査および証明書を発行、失効するための登録業務等を行う。

1.3.2 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。

1.3.3 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。

1.4 証明書の用途

1.4.1 適切な証明書の用途

本 CA が発行する証明書は、サーバー認証および通信経路で情報の暗号化を行うことに利用する。

1.4.2 禁止される証明書の用途

本 CA が発行する証明書の用途は「1.4.1 適切な証明書の用途」のとおりであり、証明書をそれ以外の目的に利用することはできないものとする。

1.5 ポリシー管理

1.5.1 文書を管理する組織

本 CP の維持、管理は、本 CA が行う。

1.5.2 連絡先

本 CP 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 CP 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 CP 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

(1) 「あ」～「ん」

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。

エスクロー

第三者に預けること（寄託）をいう。

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。

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。

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。

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。

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。

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。

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。

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。

(2) 「A」～「Z」

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。

IA (Issuing Authority) : 発行局

CA の業務のうち、証明書の発行・更新・失効、CA 私有鍵の生成・保護、リポジトリの維持・管理等を行う主体のことをいう。

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。

OCSP (Online Certificate Status Protocol)

証明書の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。

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。

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。

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。

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 日利用できるように維持管理を行う。ただし、利用可能な時間内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 CP および CPS 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できるようにする。

2.3 公開の時期または頻度

本 CP および CPS は、改訂の都度、リポジトリ上に公開する。

本 CA は、24 時間ごとに新たな CRL を発行し、リポジトリ上に公開する。また、証明書の失効が行われた場合、即時に新たな CRL を発行し、リポジトリ上に公開する。

また、証明書の有効期間を過ぎたものは CRL から削除する。

2.4 リポジトリへのアクセス管理

本 CA は、リポジトリでの公開情報に関して、特段のアクセスコントロールは行わない。証明書利用者および検証者は、本 CA の CRL を、リポジトリを通じて入手することを可能とする。リポジトリへのアクセスは、一般的な Web インターフェースを通じて可能とする。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

本 CA が発行する証明書に記載される証明書利用者の名前は、X.500 シリーズ（ITU-T(国際電気通信連合/電気通信標準化部門)が発行する勧告）の識別名規定に従い設定する。

本 CA が発行する証明書には以下の情報項目を含むものとする。

情報項目	値
Country（国名）	組織の住所または個人の住所（国）
State Or Province（都道府県名）	組織の住所または個人の住所（都道府県名）
Locality（市区町村名）	組織の住所または個人の住所（市区町村名）
Organization（組織名）	証明書利用者の組織名または個人の氏名
Organizational Unit（組織単位名） ※任意項目	証明書利用者の部署名 ※本項目には「記号のみおよびスペースのみで構成される文字列」を指定してはならない。また、本項目には以下の文字列を含めてはならない ・申請組織以外の情報と誤解される恐れのある名称・社名・商号・商標 ・法人格を示す文字列（「Co., Ltd」など） ・特定の自然人を参照させる文字列 ・住所を示す文字列 ・電話番号 ・ドメイン名および IP アドレス ・「空欄」「該当なし」などの意味を示す文字列（「null」、「N/A」など）
Common Name（コモンネーム）	証明書をインストールする予定のサーバーの DNS 内で使われるホスト名

3.1.2 名前が意味を持つことの必要性

本 CA が発行する証明書中に用いられるコモンネームの有用性は、証明書利用者が本 CA が発行する証明書をインストールする予定のサーバーの DNS 内で使われるホスト名とする。

3.1.3 証明書利用者の匿名性または仮名性

本 CA が発行する証明書のコモンネームには、匿名や仮名での登録は行わないものとする。

3.1.4 様々な名前形式を解釈するための規則

様々な名前の形式を解釈する規則は、X.500 シリーズの識別名規定に従う。

3.1.5 名前の一意性

本 CA が発行する証明書に記載される識別名(DN)の属性は、発行対象となるサーバーに対して一意なものとする。

3.1.6 商標の認識、認証および役割

本CAは、証明書申請に記載される名称について知的財産権を有しているかどうかの検証を行わない。証明書利用者は、第三者の登録商標や関連する名称を、本CAに申請してはならない。本CAは、登録商標等を理由に証明書利用者と第三者間で紛争が起こった場合、仲裁や紛争解決は行わない。また、本CAは紛争を理由に証明書利用者からの証明書申請の拒絶や発行された証明書の失効をする権利を有する。

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

証明書利用者が私有鍵を所持していることの証明は、証明書発行要求（以下「CSR」という）の署名の検証を行い、当該CSRが、公開鍵に対応する私有鍵で署名されていることを確認することで行う。

3.2.2 組織の認証

本 CA は、国や地方公共団体が発行する公的書類、国や地方公共団体の Web ページもしくはそのデータベース、または本 CA が信頼する第三者による調査もしくはそのデータベースを用いて組織の実在性確認を行う。

3.2.3 個人の認証

本 CA は、個人を認証するための証明書を発行しない。

3.2.4 検証されない証明書利用者の情報

本CAは、検証されない証明書利用者の情報を規定しない。ただし、組織単位名（OU）に記載される情報の正確性を保証しない。

3.2.5 権限の正当性確認

本CAは、証明書の申込を行う者が、その申請を行うための正当な権限を有していること

を、本CP「3.2.2. 組織の認証」で利用する書類やデータベース等で確認できる連絡先に連絡することによって確認する。

3.2.6 相互運用の基準

本CAは、セコムトラストシステムズが運営する認証局であるSecurity Communication RootCA2より、片方向相互認証証明書を発行されている。

3.2.7 ドメイン名の認証

本CAは、次のいずれかの方法により、証明書利用者にそのドメイン名の利用権があることを確認する。

1. 証明書利用者が証明書のドメイン名の登録者であることを、レジストリもしくはレジストラへ問い合わせることによって、またはWHOISに登録されたメールアドレスにランダム値をメール送信し、確認した相手からそのランダム値を使用した確認応答を受け取ることによって確認する。ランダム値は、その発行のときから10日以内の確認応答につき有効なものとする。
2. 証明書利用者にそのドメイン名の利用権があることを、管理者を表す一般的な電子メールアドレス（「admin@example.jp」、「hostmaster@example.jp」など。example.jp は証明書のドメイン名を表す）へランダム値をメール送信し、確認した相手からそのランダム値を使用した確認応答を受け取ることによって確認する。ランダム値は、その発行のときから10日以内の確認応答につき有効なものとする。
3. 証明書利用者にそのドメイン名の利用権があることを、証明書利用者が、そのドメイン名を含む URIにより識別されるWebページの情報を、本CAが指定したランダム値を記載したものに変更することによって確認する。ランダム値は、その発行のときから10日以内を有効なものとする。
4. その他、Baseline Requirementsに準拠した合理的な方法を用いて、証明書利用者にそのドメイン名の利用権があることを確認する。

3.3 鍵更新申請時の本人性確認と認証

鍵更新時における証明書利用者の本人性確認および認証は、「3.2 初回の本人確認」と同様とする。

3.4 失効申請時の本人性確認と認証

本CAは、証明書発行申請時に証明書利用者からの申請を取り次いだ指定事業者を經由して、証明書利用者からの失効申請を受け付けることによって、証明書失効申請時の本人性確認を行う。

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

証明書の申請を行うことができる者は、日本国内に住所を有する個人、または日本国内に本店・主たる事務所、支店・支所、営業所その他これに準じる常設の場所を有する法人格を有しまたは法人格を有さない組織とする。

4.1.2 申請手続および責任

証明書の申請を行うことができる者は、証明書の申請を行うにあたり、ご利用条件、本CPおよびCPSの内容を承諾した上で申請を行うものとする。また、証明書の申請を行う者は、本CAに対する申請内容が正確な情報であることを保証しなければならない。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施

本CAは、本CP「3.2 初回の本人性確認」に記載の情報をもって、申請情報の審査を行う。

4.2.2 証明書申請の承認または却下

本CAは、審査の結果、承認を行った申請について証明書の発行登録を行う。不備がある申請については、申請を却下し、申請を行った者に対し申請の再提出を依頼する。

4.2.3 証明書申請の処理時間

本CAは、承認を行った申請について、適時証明書の発行登録を行う。

4.2.4 CAA レコードの確認

本CAは、RFC 6844に従い、申請情報の審査時にCAAレコードを確認する。CAAレコードに記載する本CAのドメインは「jprs.jp」とする。

4.3 証明書の発行

4.3.1 証明書発行時の処理手続

本CAは、証明書申請の審査を完了した後、申請された情報に基づき、第三者が運営する本CA所定のCTログサーバーに証明書発行に必要な情報を登録した上で、証明書を発行する。CTログサーバーに登録する情報は、本CP「7.1 証明書のプロファイル」に記載する。

4.3.2 証明書利用者への証明書発行通知

本CAは、指定事業者または証明書利用者に対し電子メールを送付することにより証明書の発行通知を行う。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

証明書利用者が、証明書利用者だけがアクセス可能なホームページから証明書をダウンロードするか、あるいは他の方法によって証明書利用者が送付された証明書をサーバーに導入した時点をもって、証明書が受領されたものとする。

4.4.2 認証局による証明書の公開

本CAは、証明書利用者の証明書の公開は行わない。

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CAは、第三者（ただし指定事業者は除く）に対する証明書の発行通知は行わない。

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

証明書利用者は、本CAが発行する証明書および対応する私有鍵を、サーバー認証および通信経路で情報の暗号化を行うことにのみ利用するものとする。証明書利用者は、本CAが承認をした用途のみに当該証明書および対応する私有鍵を利用するものとし、その他の用途に利用してはならない。

4.5.2 検証者の公開鍵および証明書の用途

検証者は、本CAの証明書を使用することで、本CAが発行した証明書の信頼性を検証することができる。本CAが発行した証明書の信頼性を検証し、信頼する前に、本CPおよび

CPSの内容について理解し、承諾しなければならない。

4.6 鍵更新を伴わない証明書の更新

鍵更新を伴わない証明書の更新とは、公開鍵を変更することなく、証明書利用者に新しい証明書を発行することをいう。本CAは、証明書利用者が証明書を更新する場合、新たな鍵ペアを生成することを推奨する。

4.6.1 鍵更新を伴わない証明書の更新事由

鍵更新を伴わない証明書の更新は、証明書の有効期間が満了する場合に行う。

4.6.2 証明書の更新申請を行うことができる者

「4.1.1 証明書申請を提出することができる者」と同様とする。

4.6.3 証明書の更新申請の処理手続

「4.3.1 証明書発行時の処理手続」と同様とする。

4.6.4 証明書利用者に対する新しい証明書発行通知

「4.3.2 証明書利用者への証明書発行通知」と同様とする。

4.6.5 更新された証明書の受領確認手続

「4.4.1 証明書の受領確認手続」と同様とする。

4.6.6 認証局による更新された証明書の公開

「4.4.2 認証局による証明書の公開」と同様とする。

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

「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」と同様とする。

4.7 鍵更新を伴う証明書の更新

鍵更新を伴う証明書の更新とは、新たな鍵ペアを生成した上で証明書利用者に新しい証明書を発行することをいう。

4.7.1 鍵更新を伴う証明書の更新事由

鍵更新を伴う証明書の更新は、証明書の有効期間が満了する場合に行う。

4.7.2 新しい証明書の申請を行うことができる者

「4.1.1 証明書申請を提出することができる者」と同様とする。

4.7.3 鍵更新を伴う証明書の更新申請の処理手続

「4.3.1 証明書発行時の処理手続」と同様とする。

4.7.4 証明書利用者に対する新しい証明書の通知

「4.3.2 証明書利用者への証明書発行通知」と同様とする。

4.7.5 鍵更新された証明書の受領確認手続

「4.4.1 証明書の受領確認手続」と同様とする。

4.7.6 認証局による鍵更新済みの証明書の公開

「4.4.2 認証局による証明書の公開」と同様とする。

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

「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」と同様とする。

4.8 証明書の変更

4.8.1 証明書の変更事由

証明書の変更は、証明書に登録された情報（証明書のコモンネームを除く）の変更が必要となった場合に行う。

4.8.2 証明書の変更申請を行うことができる者

「4.1.1 証明書申請を提出することができる者」と同様とする。

4.8.3 証明書の変更申請の処理手続

「4.3.1 証明書発行時の処理手続」と同様とする。

4.8.4 証明書利用者に対する新しい証明書発行通知

「4.3.2 証明書利用者への証明書発行通知」と同様とする。

4.8.5 変更された証明書の受領確認手続

「4.4.1 証明書の受領確認手続」と同様とする。

4.8.6 認証局による変更された証明書の公開

「4.4.2 認証局による証明書の公開」と同様とする。

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

「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」と同様とする。

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由

証明書利用者は、次の事由が発生した場合、本CAに対しすみやかに証明書の失効申請を行わなければならない。

- ・ 証明書記載情報に変更があった場合
- ・ 私有鍵の盗難、紛失、漏洩、不正利用等により私有鍵が危殆化したまたは危殆化のおそれがある場合
- ・ 証明書の内容、利用目的が正しくない場合
- ・ 証明書に含まれる情報項目（本CP「3.1.1 名前の種類」で記載）に設定される値に、不適切な文字列が指定され、または含まれていることを発見した場合
- ・ 証明書の利用を中止する場合

また、本CAは、次の事由が発生した場合に、本CAの判断により証明書を失効することができる。

- ・ 証明書利用者のご利用条件、本CP、CPS、関連する契約または法律に基づく義務を履行していない場合
- ・ 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
- ・ 証明書に含まれる情報項目（本CP「3.1.1 名前の種類」で記載）に設定される値に、不適切な文字列が指定され、または含まれていることを合理的な証拠に基づき知り得た場合
- ・ 本CAが失効を必要とすると判断するその他の状況が認められた場合

4.9.2 証明書失効を申請することができる者

証明書の失効の申請を行うことができる者（以下「失効申請者」という）は、本サービスの契約者、または契約組織の担当者とする。なお、本CP「4.9.1 証明書失効事由」に該当すると本CAが判断した場合、本CAが失効申請者となる。

4.9.3 失効申請手続

失効申請者は、本CP「3.4 失効申請時の本人性確認と認証」に定める手続を行うことにより本CAへ届け出るものとする。

本CAは、所定の手続によって受け付けた情報を確認し、証明書の失効処理を行う。

4.9.4 失効申請の猶予期間

失効申請者は、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には、すみやかに失効申請を行わなければならない。

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CAは、有効な失効申請を受け付けてからすみやかに証明書の失効処理を行い、CRLへ当該証明書情報を反映させる。

4.9.6 失効調査の要求

本CAが発行する証明書には、CRLの格納先であるURLを記載する。検証者は、本CAが発行する証明書について信頼し利用する前に、当該証明書の有効性をCRLにより確認しなければならない。なお、CRLには、有効期限の切れた証明書情報は含まれない。

4.9.7 証明書失効リストの発行頻度

CRLは、失効処理の有無に関わらず、24時間ごとに更新を行う。証明書の失効処理が行われた場合は、その時点でCRLの更新を行う。

4.9.8 証明書失効リストの発行最大遅延時間

本CAは、発行したCRLを即時にリポジトリに反映させる。

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

オンラインでの証明書ステータス情報は、OCSPサーバーを通じて提供される。

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

検証者は本CAにより発行された証明書を信頼し利用する前に、証明書の有効性を確認しなければならない。リポジトリに掲載しているCRLにより、証明書の失効登録の有無を確認しない場合には、OCSPサーバーにより提供される証明書ステータス情報の確認を行わなければならない。

4.9.11 利用可能な失効情報の他の形式

規定しない。

4.9.12 鍵の危殆化に対する特別要件

規定しない。

4.9.13 証明書の一時停止事由

規定しない。

4.9.14 証明書の一時停止を申請することができる者

規定しない。

4.9.15 証明書の一時停止申請手続

規定しない。

4.9.16 一時停止を継続することができる期間

規定しない。

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

証明書利用者および検証者はOCSPサーバーを通じて証明書ステータス情報を確認することができる。

4.10.2 サービスの利用可能性

本CAは、24時間365日、証明書ステータス情報を確認できるようOCSPサーバーを管理する。ただし、保守等により一時的にOCSPサーバーを利用できない場合もある。

4.10.3 オプションな仕様

規定しない。

4.11 加入（登録）の終了

証明書利用者が証明書の利用を終了する、または本サービスを解約する場合、証明書の失効申請を行わなければならない。なお、証明書の更新手続きを行わず、該当する証明書の有効期間が満了した場合にも終了となる。

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CAは、証明書利用者の私有鍵のエスクローは行わない。

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

規定しない。

5. 設備上、運営上、運用上の管理

5.1 物理的セキュリティ管理

本項については、CPSに規定する。

5.2 手続的管理

5.2.1 信頼すべき役割

本サービスの運用に関わる役割を以下に示す。

(1) RA 責任者

- ・本サービスの統括
- ・RA 管理者の任命

(2) RA 管理者

- ・RA 担当者への作業指示
- ・RA 業務の遂行管理

(3) RA 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 管理者の指示に基づく証明書発行審査の遂行

5.2.2 職務ごとに必要とされる人数

当社は、サービス提供に支障をきたさないよう、RA 責任者を除く本 CP「5.2.1 信頼すべき役割」に記載する役割に関し、複数名の要員を配置する。

5.2.3 個々の役割に対する本人性確認と認証

当社は、RA システムへのアクセスに関し、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物理的または論理的な方法で確認する。

5.2.4 職務分割が必要となる役割

規定しない。

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 CP「5.2.1 信頼すべき役割」に記載する役割を担う者は、当社の採用基準に基づき採用

された従業員とする。

5.3.2 適性調査

当社は、本 CP「5.2.1 信頼すべき役割」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

当社は、要員が役割に就く前に本サービスの運用に必要な教育を実施し、以降、必要に応じ、役割に応じた教育・訓練を実施する。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・訓練を実施する。

5.3.4 再教育の頻度および要件

当社は、本 CP「5.2.1 信頼すべき役割」に記載する役割を担う者に対して、必要に応じ再トレーニングを行う。

5.3.5 仕事のローテーションの頻度および順序

規定しない。

5.3.6 認められていない行動に対する制裁

当社の就業規則の罰則に関する規定に従う。

5.3.7 業務委託先の管理

当社は、本サービスの運用のすべてあるいは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。

5.3.8 要員へ提供される資料

当社は、要員に対して、関連する業務上必要な文書のみ閲覧を許可する。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類

当社は、次の内容を監査ログとして記録する。

- ・ 証明書の発行、失効の処理履歴
- ・ CRL の発行の処理履歴

監査ログは、以下の項目を含む。

- ・ 日付
- ・ 時刻
- ・ イベントを発生させた主体

- ・ イベントの内容

5.4.2 監査ログを処理する頻度

当社は、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

当社は、本サービスに関する監査ログを、アーカイブとして最低7年間保存する。

5.4.4 監査ログの保護

当社は、許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

当社は、RA システム上のログについては、バックアップを取得する。

5.4.6 監査ログの収集システム

RA システムは、実装された機能により監査ログを自動的に収集する。

5.4.7 イベントを起こした者への通知

当社は、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

当社は、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、必要に応じてセキュリティ対策の見直しを行う。

5.5 記録の保管

5.5.1 アーカイブの種類

本CAは、CPSの「5.5 記録の保管」に加えて、次の情報をアーカイブとして保存する。

- ・ 本CP
- ・ 本CPに基づき作成された認証局の業務運用を規定する文書
- ・ 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情報およびその処理履歴

5.5.2 アーカイブ保存期間

当社は、アーカイブを最低7年間保存する。

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

「5.4.5 監査ログのバックアップ手続」と同様とする。

5.5.5 記録にタイムスタンプを付与する要件

当社は、RA システム内で記録される重要な情報に対し、日付・時刻を記録する。

5.5.6 アーカイブ収集システム

RA システムの機能により自動的に収集する。

5.5.7 アーカイブの検証手続

アーカイブへは、許可された者だけがアクセスすることができる。アーカイブされた情報の復旧の際には、その整合性の検証を行う。

5.6 鍵の切り替え

本CAの私有鍵は、私有鍵に対する証明書の有効期間が証明書利用者に発行した証明書の最大有効期間よりも短くなる前に新たな私有鍵の生成および証明書の発行を行う。新しい私有鍵が生成された後は、新しい私有鍵を使って証明書およびCRLの発行を行う。

5.7 危殆化および災害からの復旧

本項については、CPSに規定する。

5.8 認証局または登録局の終了

本CAは、業務停止する必要がある場合、その旨を事前に「9.11 関係者間の個別通知と連絡」に定められた方法で証明書利用者に通知する。

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

6.1.1 鍵ペアの生成

本CA私有鍵についてはCPS「6.1.1 鍵ペアの生成」に規定する。

6.1.2 証明書利用者に対する私有鍵の交付

証明書利用者の私有鍵は、証明書利用者自身が生成するものとし、本CAは証明書利用者の私有鍵生成および交付は行わない。

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交付は、証明書の申請時にオンラインによって行われる。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

検証者は、本CAのリポジトリにアクセスすることによって、本CAの公開鍵を入手することができる。

6.1.5 鍵サイズ

本CAの鍵ペアは、RSA方式で鍵長2048ビットとする。

証明書利用者の鍵ペアについては、RSA方式で鍵長2048ビットとする。

6.1.6 公開鍵のパラメータの生成および品質検査

本CAの公開鍵のパラメータの生成、およびパラメータの強度の検証は、鍵ペア生成に使用される暗号装置に実装された機能を用いて行われる。証明書利用者の公開鍵のパラメータの生成および品質検査について規定しない。

6.1.7 鍵の用途

本CAおよび本CAが発行する証明書の鍵の用途は以下の通りとする。

表 6.1 鍵の用途

	本CA	本CAが発行する証明書
digitalSignature	—	yes
nonRepudiation	—	—
keyEncipherment	—	yes
dataEncipherment	—	—

keyAgreement	—	—
keyCertSign	yes	—
cRLSign	yes	—
encipherOnly	—	—
decipherOnly	—	—

6.2 私有鍵の保護および暗号モジュール技術の管理

本項については、CPSに規定する。

6.3 鍵ペアのその他の管理方法

本項については、CPSに規定する。

6.4 活性化データ

本項については、CPSに規定する。

6.5 コンピュータのセキュリティ管理

本項については、CPSに規定する。

6.6 ライフサイクルの技術的管理

本項については、CPSに規定する。

6.7 ネットワークセキュリティ管理

本項については、CPSに規定する。

6.8 タイムスタンプ

本項については、CPSに規定する。

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

本CAが発行する証明書のプロファイルは、次表のとおりである。

本CAは2018年4月5日以降、第三者が運営する本CA所定のCTログサーバーに証明書発行に必要な表7.1.2の情報を登録した上で、CTに対応した証明書を発行する。

表7.1.1サーバー証明書プロファイル（発行日が2018年4月4日までの証明書に適用）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	CN=JPRS Organization Validation Authority - G1	-
Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	-
	NotAfter	例) 2009/3/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	State Or Province	組織の住所または個人の住所（都道府県名）（必須）	-
	Locality	組織の住所または個人の住所（市区町村名）（必須）	-
	Organization	証明書利用者の組織名または個人の氏名（必須）	-
	Organizational Unit	証明書利用者の部署名（任意）	-
	Common Name	証明書をインストールする予定のサーバーのDNS内で使われるホスト名（必須）	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		TLS Web Server Authentication	n
Subject Alt Name		dNSName=サーバー名	n

CertificatePolicies	policyIdentifier OID=1.2.392.200091.110.208.2 policyQualifiers policyQualifierId=CPS qualifier=https://jprs.jp/pubcert/info/ repository/	n
CRL Distribution Points	http://repo.pubcert.jprs.jp/sppca/jprs/ovca/fullcrl.crl	n
Authority Information Access	accessMethod <u>ocsp (1 3 6 1 5 5 7 48 1)</u> accessLocation http://ov.ocsp.pubcert.jprs.jp	n
Authority Key Identifier	発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier	主体者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

表 7.1.2 サーバー証明書プロファイル（発行日が 2018 年 4 月 5 日から 2019 年 7 月 31 日までの証明書に適用）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	CN=JPRS Organization Validation Authority - G2	-
Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	-
	NotAfter	例) 2009/3/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	State Or Province	組織の住所または個人の住所（都道府県名）（必須）	-
	Locality	組織の住所または個人の住所（市区町村名）（必須）	-
	Organization	証明書利用者の組織名または個人の氏名	-

		(必須)	
	Organizational Unit	証明書利用者の部署名 (任意)	-
	Common Name	証明書をインストールする予定のサーバーの DNS 内で使われるホスト名 (必須)	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		TLS Web Server Authentication	n
Subject Alt Name		dNSName=サーバー名	n
CertificatePolicies		[1]policyIdentifier OID=1.2.392.200091.110.208.2 policyQualifiers policyQualifierId=CPS qualifier=https://jprs.jp/pubcert/info/repository/ [2]policyIdentifier=2.23.140.1.2.2	n
CRL Distribution Points		http://repo.pubcert.jprs.jp/sppca/jprs/ovca_g2/fullcrl.crl	n
Authority Information Access		accessMethod <u>ocsp (1 3 6 1 5 5 7 48 1)</u> accessLocation http://ov.g2.ocsp.pubcert.jprs.jp	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値 (160 ビット)	n
Subject Key Identifier		主体者公開鍵の SHA-1 ハッシュ値 (160 ビット)	n
Certificate Transparency Timestamp (※) (1.3.6.1.4.1.11129.2.4.2)		SignedCertificateTimestampList の値	n

(※ : Certificate Transparency Timestamp は、証明書発行時に第三者が運営する本 CA 所定の CT ログサーバーへ登録しない。これを除いた証明書プロファイルの情報を CT ログサーバーへ登録する。)

7.2 CRL のプロフィール

本CAが発行するCRLのプロファイルは、次表のとおりである。

表 7.2.1 CRL プロファイル（発行日が 2018 年 4 月 4 日までの証明書に適用）

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	CN=JPRS Organization Validation Authority - G1	-
This Update		例) 2008/3/1 00:00:00 GMT	-
Next Update		例) 2008/3/5 00:00:00 GMT 更新間隔=24H、有効期間=96H とする	-
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2008/3/1 00:00:00 GMT	-
	Reason Code	失効事由（unspecified, etc.）	-
拡張領域		設定内容	critical
CRL Number		CRL 番号	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値 (160 ビット)	n

表 7.2.2 CRL プロファイル（発行日が 2018 年 4 月 5 日から 2019 年 7 月 31 日までの証明書に適用）

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	CN=JPRS Organization Validation Authority - G2	-
This Update		例) 2008/3/1 00:00:00 GMT	-
Next Update		例) 2008/3/5 00:00:00 GMT 更新間隔=24H、有効期間=96H とする	-

Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2008/3/1 00:00:00 GMT	-
	Reason Code	失効事由（unspecified, etc.）	-
拡張領域		設定内容	critical
CRL Number		CRL 番号	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

7.3 OCSP のプロフィール

本CAが発行するOCSPのプロファイルは、次表のとおりである。

表 7.3.1 OCSP プロファイル（発行日が 2018 年 4 月 4 日までの証明書に適用）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	CN=JPRS Organization Validation Authority - G1	-
Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	-
	NotAfter	例) 2008/3/5 00:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	Organization	Japan Registry Services Co., Ltd. （固定値）	-
	Common Name	OCSP サーバー名（必須）	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		null	n
CertificatePolicies		policyIdentifier OID=1.2.392.200091.110.208.2 policyQualifiers policyQualifierId=CPS	n

	qualifier=https://jprs.jp/pubcert/info/repository/	
Authority Key Identifier	発行者公開鍵の SHA-1 ハッシュ値 (160 ビット)	n
Subject Key Identifier	主体者公開鍵の SHA-1 ハッシュ値 (160 ビット)	n

表 7.3.2 OCSP プロファイル（発行日が 2018 年 4 月 5 日から 2019 年 7 月 31 日までの証明書に適用）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	CN=JPRS Organization Validation Authority - G2	-
Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	-
	NotAfter	例) 2008/3/5 00:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	Organization	Japan Registry Services Co., Ltd. （固定値）	-
	Common Name	OCSP サーバー名（必須）	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		null	n
CertificatePolicies		policyIdentifier OID=1.2.392.200091.110.208.2 policyQualifiers policyQualifierId=CPS qualifier=https://jprs.jp/pubcert/info/repository/	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値 (160	n

	ビット)	
Subject Key Identifier	主体者公開鍵の SHA-1 ハッシュ値 (160 ビット)	n

7.3.1 バージョン番号

本CAは、OCSPバージョン1を適用する。

7.3.2 OCSP 拡張

規定しない。

8. 準拠性監査と他の評価

8.1 監査の頻度

本CAは、本CAの運用が本CPに準拠して行われているかについて、年に1回以上の監査を行う。

8.2 監査者の身元／資格

準拠性監査は、十分な監査経験を有する監査人が行う。

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。

8.4 監査で扱われる事項

監査は、本CAの運用の本CPに対する準拠性を中心として行う。

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。

9. 他の業務上および法的事項

9.1 料金

別途、規定する。

9.2 財務的責任

本CAは、電子認証基盤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CPおよびCPSの一部として明示的に公開されたものを除き、機密保持対象として扱う。

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、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

本CA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CPは著作権を含み、当社の権利に属するものとする。

9.6 表明保証

9.6.1 認証局の表明保証

9.6.1.1 IA の表明保証

本CAは、IAの業務を遂行するにあたり次の義務を負う。

- ・ CA私有鍵のセキュアな生成・管理
- ・ RAからの申請に基づいた証明書の正確な発行・失効管理
- ・ IAのシステム稼働の監視・運用
- ・ CRLの発行・公表

9.6.1.2 RA の表明保証

本CAは、RAの業務を遂行するにあたり次の義務を負う。

- ・ 登録端末のセキュアな環境への設置・運用
- ・ 証明書発行・失効申請におけるIAへの正確な情報伝達
- ・ 証明書失効申請におけるIAへの運用時間中の速やかな情報伝達
- ・ リポジトリの維持管理

9.6.2 証明書利用者の表明保証

証明書利用者は、ご利用条件および本CPに定める諸事項を遵守することについて保証するものとする。また、証明書利用者は、ご利用条件および本CPに遵守しない場合、すべての責任を有するものとする。

9.6.3 検証者の表明保証

検証者は、本CPに定める諸事項を遵守することについて保証するものとする。また、検証者は、本CPに遵守しない場合、すべての責任を有するものとする。

9.6.4 他の関係者の表明保証

規定しない。

9.7 無保証

本CAは、本CP「9.6.1 認証局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害または派生的損害に対する責任を負わず、また、いかなる逸失利益、データの紛失またはその他の間接的もしくは派生的損害に対する責任を負わない。

9.8 責任の制限

本CP「9.6.1 認証局の表明保証」の内容に関し、次の場合、本CAは責任を負わないものとする。

- ・本CAに起因しない不法行為、不正使用または過失等により発生する一切の損害
- ・証明書利用者が自己の義務の履行を怠ったために生じた損害
- ・証明書利用者のシステムに起因して発生した一切の損害
- ・本CA、証明書利用者のハードウェア、ソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
- ・本CAの責に帰することのできない事由で証明書およびCRLに公開された情報に起因する損害
- ・本CAの責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- ・証明書の使用に関して発生する取引上の債務等、一切の損害
- ・現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
- ・天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、本CAの業務停止に起因する一切の損害
- ・証明書発行に必要な情報のCTログサーバーへの登録・公開に付随または関連して発生した一切の損害

9.9 補償

本CAが発行する証明書を申請、受領、信頼した時点で、証明書利用者には、本CAおよび関連する組織等に対する損害賠償責任および保護責任が発生するものとする。当該責任の対象となる事象には、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅滞、不履行等の各種責任が含まれる。なお、証明書利用者の損害に関する補償については、ご利用条件で定める。

9.10 有効期間と終了

9.10.1 有効期間

本CP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CP「9.10.2 終了」に規定する終了以前に本CPが無効となることはない。

9.10.2 終了

本CP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

本CAは、証明書利用者および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CP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CPを変更した場合、すみやかに変更した本CPを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を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

証明書の利用に関し、本CAに対して訴訟、仲裁を含む解決手段に訴えようとする場合、本CAに対して事前にその旨を通知するものとする。なお、JPRSサーバー証明書発行サービスに関する全ての紛争の第一審の専属的合意管轄裁判所を東京地方裁判所とする。

9.14 準拠法

本CA、証明書利用者の所在地にかかわらず、本CPの解釈、有効性および証明書の利用にかかわる紛争については、日本国の法律が適用されるものとする。

9.15 適用法の遵守

規定しない。

9.16 雑則

規定しない。

9.17 その他の条項

規定しない。