

**JPRSサーバー証明書
認証局証明書ポリシー
(Certificate Policy)
Version 3.10**

2022年3月2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	2019.09.25	メール認証で選択可能な送付先メールアドレスの追加に伴う記述の追加
1.20	2020.04.01	Mozilla Root Store Policy(v2.7)への準拠に伴う改訂
1.30	2020.07.10	中間証明書プロファイルの変更に伴う改訂
2.00	2020.07.22	認証局切り替えに伴う記述の追加
2.10	2020.08.20	証明書の有効期間の上限に関する記述の修正
2.20	2020.10.06	ドメイン名利用権の審査期間延長に伴う改訂および CRL プロファイルの修正
2.21	2021.04.01	表紙の日付及び Version を更新
2.22	2021.04.28	Mozilla Root Store Policy(v2.7.1)への準拠に伴う改訂
2.23	2021.05.27	<ul style="list-style-type: none">・「3.2.2.4 ドメイン名の認証」の明確化・「7.証明書および証明書失効リストのプロファイル」より、中間 CA(G3)に関する記載を削除
2.30	2021.11.17	<ul style="list-style-type: none">・「3.2.2.4.18 Agreed-Upon Change to Website v2」の仕様変更・Organizational Unit の記載終了
3.00	2021.12.08	<ul style="list-style-type: none">・ACME 対応版の提供に関する改訂
3.10	2022.03.02	<ul style="list-style-type: none">・ACME 対応版のご利用条件への参照を追加

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 CA.....	10
1.3.2 RA.....	10
1.3.3 証明書利用者.....	10
1.3.4 検証者.....	10
1.3.5 その他関係者.....	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.....	16
2.1 リポジトリ.....	16
2.2 情報の公開.....	16
2.3 公開の時期または頻度.....	16
本 CP および CPS は、改訂の都度、リポジトリ上に公開する。.....	16
CRL の発行頻度は、「4.9.7 証明書失効リストの発行頻度」に規定する。.....	16
2.4 リポジトリへのアクセス管理.....	16
3. 識別と認証.....	17
3.1 名前決定.....	17
3.1.1 名前の種類.....	17
3.1.2 意味を持つ名前.....	17
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	組織とドメイン名の認証	18
3.2.2.1	組織の認証	18
3.2.2.2	DBA/Tradename (屋号)	18
3.2.2.3	Country の確認	18
3.2.2.4	ドメイン名の認証	18
3.2.3	個人の認証	21
3.2.4	検証されない証明書利用者の情報	21
3.2.5	権限の正当性確認	22
3.2.6	相互運用の基準	22
3.3	鍵更新申請時の本人性確認と認証	22
3.4	失効申請時の本人性確認と認証	22
4.	証明書のライフサイクルに対する運用上の要件	23
4.1	証明書申請	23
4.1.1	証明書申請を提出することができる者	23
4.1.2	申請手続および責任	23
4.2	証明書申請手続	23
4.2.1	本人性確認と認証の実施	23
4.2.2	証明書申請の承認または却下	23
4.2.3	証明書申請の処理時間	23
4.2.4	CAA レコードの確認	23
4.3	証明書の発行	24
4.3.1	証明書発行時の処理手続	24
4.3.2	証明書利用者への証明書発行通知	24
4.4	証明書の受領確認	24
4.4.1	証明書の受領確認手続	24
4.4.2	認証局による証明書の公開	24
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	24
4.5	鍵ペアおよび証明書の用途	24
4.5.1	証明書利用者の私有鍵および証明書の用途	24
4.5.2	検証者の公開鍵および証明書の用途	25
4.6	鍵更新を伴わない証明書の更新	25
4.6.1	鍵更新を伴わない証明書の更新事由	25
4.6.2	証明書の更新申請を行うことができる者	25
4.6.3	証明書の更新申請の処理手続	25
4.6.4	証明書利用者に対する新しい証明書発行通知	25

4.6.5	更新された証明書の受領確認手続	25
4.6.6	認証局による更新された証明書の公開	25
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	25
4.7	鍵更新を伴う証明書の更新	25
4.7.1	鍵更新を伴う証明書の更新事由	25
4.7.2	新しい証明書の申請を行うことができる者	26
4.7.3	鍵更新を伴う証明書の更新申請の処理手続	26
4.7.4	証明書利用者に対する新しい証明書の通知	26
4.7.5	鍵更新された証明書の受領確認手続	26
4.7.6	認証局による鍵更新済みの証明書の公開	26
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	26
4.8	証明書の変更	26
4.8.1	証明書の変更事由	26
4.8.2	証明書の変更申請を行うことができる者	26
4.8.3	証明書の変更申請の処理手続	26
4.8.4	証明書利用者に対する新しい証明書発行通知	26
4.8.5	変更された証明書の受領確認手続	26
4.8.6	認証局による変更された証明書の公開	26
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	26
4.9	証明書の失効と一時停止	27
4.9.1	証明書失効事由	27
4.9.2	証明書失効を申請することができる者	27
4.9.3	失効申請手続	27
4.9.4	失効申請の猶予期間	28
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	28
4.9.6	失効調査の要求	28
4.9.7	証明書失効リストの発行頻度	28
4.9.8	証明書失効リストの発行最大遅延時間	28
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	28
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	28
4.9.11	利用可能な失効情報の他の形式	28
4.9.12	鍵の危殆化に対する特別要件	28
4.9.13	証明書の一時停止事由	29
4.9.14	証明書の一時停止を申請することができる者	29
4.9.15	証明書の一時停止申請手続	29
4.9.16	一時停止を継続することができる期間	29

4.10	証明書のステータス確認サービス	29
4.10.1	運用上の特徴	29
4.10.2	サービスの利用可能性	29
4.10.3	オプション的な仕様	29
4.11	加入（登録）の終了	29
4.12	キーエスクローと鍵回復	30
4.12.1	キーエスクローと鍵回復ポリシーおよび実施	30
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	30
5.	設備上、運営上、運用上の管理	31
5.1	物理的セキュリティ管理	31
5.2	手続的管理	31
5.3	人事的管理	31
5.4	監査ログの手続	31
5.4.1	記録されるイベントの種類	31
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	31
5.4.5	監査ログのバックアップ手続	31
5.4.6	監査ログの収集システム	31
5.4.7	イベントを起こした者への通知	31
5.4.8	脆弱性評価	32
5.5	記録の保管	32
5.5.1	アーカイブの種類	32
5.5.2	アーカイブ保存期間	32
5.5.3	アーカイブの保護	32
5.5.4	アーカイブのバックアップ手続	32
5.5.5	記録にタイムスタンプを付与する要件	32
5.5.6	アーカイブ収集システム	32
5.5.7	アーカイブの検証手続	32
5.6	鍵の切り替え	32
5.7	危殆化および災害からの復旧	33
5.8	認証局または登録局の終了	33
6.	技術的セキュリティ管理	34
6.1	鍵ペアの生成およびインストール	34
6.1.1	鍵ペアの生成	34
6.1.2	証明書利用者に対する私有鍵の交付	34

6.1.3	認証局への公開鍵の交付	34
6.1.4	検証者への CA 公開鍵の交付	34
6.1.5	鍵サイズ	34
6.1.6	公開鍵のパラメータの生成および品質検査	34
6.1.7	鍵の用途	34
6.2	私有鍵の保護および暗号モジュール技術の管理	35
6.3	鍵ペアのその他の管理方法	35
6.4	活性化データ	35
6.5	コンピュータのセキュリティ管理	35
6.6	ライフサイクルの技術的管理	35
6.7	ネットワークセキュリティ管理	35
6.8	タイムスタンプ	35
7.	証明書および証明書失効リストのプロファイル	36
7.1	証明書のプロファイル	36
7.1.1	サーバー証明書プロファイル	36
7.1.2	中間証明書プロファイル	39
7.2	CRL のプロファイル	40
7.3	OCSP のプロファイル	41
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	43
8.4	監査で扱われる事項	43
8.5	不備の結果としてとられる処置	43
8.6	監査結果の開示	43
8.7	内部監査	43
9.	他の業務上および法的事項	44
9.1	料金	44
9.2	財務的責任	44
9.3	企業情報の機密性	44
9.3.1	機密情報の範囲	44
9.3.2	機密情報の範囲外の情報	44
9.3.3	機密情報を保護する責任	44
9.4	個人情報の保護	44

9.5 知的財産権	44
9.6 表明保証	44
9.6.1 CA 業務の表明保証	44
9.6.2 RA 業務の表明保証	45
9.6.3 証明書利用者の表明保証	45
9.6.4 検証者の表明保証	45
9.6.5 その他関係者の表明保証	45
9.7 無保証.....	45
9.8 責任の制限	45
9.9 補償	46
9.10 有効期間と終了	46
9.10.1 有効期間	46
9.10.2 終了.....	46
9.10.3 終了の効果と効果継続.....	46
9.11 関係者間の個別通知と連絡.....	47
9.12 改訂	47
9.12.1 改訂手続	47
9.12.2 通知方法および期間.....	47
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	47
9.13 紛争解決手続.....	47
9.14 準拠法.....	47
9.15 適用法の遵守.....	47
9.16 雑則	47
9.17 その他の条項.....	48

1. はじめに

1.1 概要

JPRS サーバー証明書認証局証明書ポリシー (以下「本 CP」という) は、JPRS サーバー証明書発行サービス (以下「本サービス」という) 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、JPRS サーバー証明書認証局運用規程 (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 397 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」および「JPRS サーバー証明書発行サービス ACME 対応版ご利用条件」 (以下併せて「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 とご利用条件、CPS の内容に齟齬がある場合は、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 サーバー証明書認証局証明書ポリシー (CP)	1.3.6.1.4.1.53827.1.1.4
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

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 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は、以下の Web フォームより行うものとする。

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。

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。

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。

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。

ランダム値

本 CA が申請者に指定した、少なくとも 112 ビットのエントロピーを示す値。

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」

ACME (Automated Certificate Management Environment)

証明書の発行や審査などに関するプロセスを自動化するためのプロトコルのことをいう。
本プロトコルは RFC 8555 で規定されている。

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。

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。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。

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。

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。CRL の発行頻度は、「4.9.7 証明書失効リストの発行頻度」に規定する。

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。

3.1.2 意味を持つ名前

本 CA が発行する証明書に含まれる情報項目とその意味は、「7.1.1 サーバー証明書プロフィール」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 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 組織とドメイン名の認証

3.2.2.1 組織の認証

(1) ドメイン認証型

本 CA は、組織の実在性を確認しない。

(2) 組織認証型

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。

3.2.2.2 DBA/Tradename (屋号)

本 CA が発行する証明書の情報項目「Organization (組織名)」に DBA/Tradename を記載する場合は、「3.2.2.1 組織の認証 (2) 組織認証型」と同様の確認を行う。

3.2.2.3 Country の確認

本 CA が発行する証明書の情報項目「Country (国)」については、「3.2.2.1 組織の認証」と同様の確認を行う。

3.2.2.4 ドメイン名の認証

本 CA は、証明書を発行する前に、以下に示す少なくとも一つの方法で、発行する証明書の SAN に含めるすべての完全修飾ドメイン名 (FQDN) を検証する。

本項のサブセクション 3.2.2.4.1 項から 3.2.2.4.20 項は、Baseline Requirements におけるセクション番号に対応する。

3.2.2.4.1 Validating the Applicant as a Domain Contact

適用外とする。

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

ランダム値をメール送信し、そのランダム値を利用した確認応答を受け取ることによって、申請者に FQDN の利用権があることを確認する。ランダム値は、WHOIS に表示されているメールアドレス宛に送信する。

本 CA は、ランダム値の送信に、FAX、SMS、郵便を使用しない。

ランダム値は各メールで一意とし、その発行の時から 25 日以内の確認応答につき有効なものとする。

3.2.2.4.3 Phone Contact with Domain Contact

適用外とする。

3.2.2.4.4 Constructed Email to Domain Contact

以下の方法で、申請者に FQDN の利用権があることを確認する。

1. 管理者を表す一般的な電子メールアドレス (※) へメールを送信する
2. メールにはランダム値を含める

3. そのランダム値を利用した確認応答を受け取る

ランダム値は各メールで一意とし、その発行の時から 25 日以内の確認応答につき有効なものとする。

※：管理者を表す一般的な電子メールアドレス

例：admin@example.jp、hostmaster@sub.example.co.jp など

- @の左側は admin、administrator、webmaster、hostmaster、postmaster のいずれかとする。
- @の右側は以下のいずれかとする。
 - ・ FQDN のうちレジストリに登録されているドメイン名部分 (「example.jp」、「example.co.jp」など)
 - ・ FQDN そのもの (先頭ラベルが"*" (ワイルドカード) や"www"の場合は、そのラベルを取り除く。ただし、"www."がレジストリに登録されているドメイン名部分に含まれる場合は取り除かない。)

3.2.2.4.5 Domain Authorization Document

適用外とする。

3.2.2.4.6 Agreed-Upon Change to Website

適用外とする。

3.2.2.4.7 DNS Change

ランダム値がアンダースコアで始まるラベルを前置きした FQDN の DNS ゾーンにおける TXT リソースレコードが含まれていることを検証することで、申請者に FQDN の利用権があることを確認する。

「アンダースコアで始まるラベル」は、"_acme-challenge"とする。

先頭ラベルが"*" (ワイルドカード) の場合は、"*" (ワイルドカード) ラベルそのものを"_acme-challenge"ラベルに置き換える。

ランダム値は各証明書発行申請で一意とし、その発行の時から 25 日以内の確認応答につき有効なものとする。

3.2.2.4.8 IP Address

適用外とする。

3.2.2.4.9 Test Certificate

適用外とする。

3.2.2.4.10 TLS Using a Random Number

適用外とする。

3.2.2.4.11 Any Other Method

適用外とする。

3.2.2.4.12 Validating Applicant as a Domain Contact

申請者がドメイン名の登録者であることを検証することをもって、申請者に FQDN の利用権があることを確認する。ただし、本 CA をレジストリ/レジストラとするドメイン名を含む FQDN である場合に限る。

3.2.2.4.13 Email to DNS CAA Contact

適用外とする。

3.2.2.4.14 Email to DNS TXT Contact

適用外とする。

3.2.2.4.15 Phone Contact with Domain Contact

適用外とする。

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

適用外とする。

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

適用外とする。

3.2.2.4.18 Agreed-Upon Change to Website v2

ランダム値が Web コンテンツのファイルに含まれていること検証することをもって、申請者が FQDN を管理していることを確認する。

1. ランダム値は、ファイルを取得する本 CA によるリクエスト自体に記載しない
2. 本 CA は、ファイルの取得において、成功を意味する HTTP ステータスコード (2xx)を確認しなければならない。

ランダム値を含むファイルは、以下全てを満たす必要がある。

1. FQDN をホスト名とした URI 下に配置されていなければならない
 2. ".well-known/pki-validation"ディレクトリに置かなければならない
 3. http または https のスキームにより取得されなければならない
 4. 80 (http) もしくは、443 (https)のポートでアクセスされなければならない
- 本 CA がリダイレクトに従いファイルを取得する場合は、以下全てを満たす必要がある。
1. HTTP プロトコルレイヤーから開始されるリダイレクトである
 - HTTP ステータスコードは以下のいずれかとする
 - ・ 301, 302, 307 (RFC 7231 に規定)
 - ・ 308 (RFC 7538 に規定)
 - RFC 7231 の 7.1.2 項で定義された、Location ヘッダの"the final value"をリダイレクト先とする
 2. リダイレクトする際は、http または https のスキームを用いる
 3. リダイレクトする際は、80 (http) もしくは、443 (https)のポートにアクセスする

ランダム値は各証明書発行申請で一意とし、その発行の時から 25 日以内の確認応答につき有効なものとする。

2021 年 11 月 18 日以降に発行する証明書について、先頭ラベルが"*" (ワイルドカード) の FQDN に対してこの方法を適用外とする。

3.2.2.4.19 Agreed-Upon Change to Website - ACME

RFC 8555 の 8.3 項で定義された ACME HTTP Challenge メソッドを用いて、申請者が FQDN を管理していることを確認する。以下は、RFC 8555 からの追加要求である。

1. 本 CA は、検証におけるリクエストに対するレスポンスとして、成功を意味する HTTP ステータスコード(2xx)を確認しなければならない。
2. ランダム値は各証明書発行申請で一意とし、その発行の時から 25 日以内の確認応答につき有効なものとする。
3. 本 CA がリダイレクトに従いファイルを取得する場合は、以下全てを満たす必要がある。
 1. HTTP プロトコルレイヤーから開始されるリダイレクトである
 - HTTP ステータスコードは以下のいずれかとする
 - ・ 301, 302, 307 (RFC 7231 に規定)
 - ・ 308 (RFC 7538 に規定)
 - RFC 7231 の 7.1.2 項で定義された、Location ヘッダの"the final value"をリダイレクト先とする
 2. リダイレクトする際は、http または https のスキームを用いる
 3. リダイレクトする際は、80 (http) もしくは、443 (https)のポートにアクセスする

先頭ラベルが"*" (ワイルドカード) の FQDN に対してこの方法を適用外とする。

3.2.2.4.20 TLS Using ALPN

適用外とする。

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

(1) ドメイン認証型

本 CA は、検証されない証明書利用者の情報を規定しない。

(2) 組織認証型

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

(1) ドメイン認証型

本 CA は、証明書を発行する時点において、証明書利用者が証明書に記載されるドメイン名の登録者であるか、あるいはその登録者より排他的な利用権を許諾されていることを確認する。

(2) 組織認証型

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 組織とドメイン名の認証」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。

3.3 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 初回の本人性確認」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、次のいずれかを確認することにより失効申請時の本人性確認を行う。

1. 証明書発行申請時または本サービス利用の申込時に証明書利用者からの申請または申込を取り次いだ指定事業者を経由した失効申請であること
2. 失効申請の署名が、証明書利用者に付与したアカウントに関連付けられた秘密鍵によるものであること (ACME プロトコルを介して発行した証明書に限る)
3. 失効申請の署名が、証明書の秘密鍵によるものであること (ACME プロトコルを介して発行した証明書に限る)

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

(1) ドメイン認証型

証明書の申請を行うことができる者は、証明書に記載されるドメイン名の登録者であるか、あるいはその登録者より排他的な利用権を許諾されている者とする。

(2) 組織認証型

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。ただし、ACME プロトコルを介して証明書が発行された場合は、電子メールによる発行通知は行わない。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

次のいずれかの時点をもって、証明書が受領されたものとする。

1. 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取得を要求し、本 CA が証明書を応答した時
2. 証明書利用者が、ACME プロトコルを介して証明書取得を要求し、本 CA が証明書を応答した時 (ACME プロトコルを介して発行された証明書に限る)
3. 証明書利用者が、上記以外の方法によって入手した証明書をサーバーに導入した時

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（組織認証型のみ）
- ・ 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（組織認証型のみ）
- ・ 本CAが失効を必要とする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、次のいずれかとする。

- ・ 証明書利用者
- ・ 証明書発行申請時または本サービス利用の申込時に証明書利用者からの申請または申込を取り次いだ指定事業者
- ・ 証明書の秘密鍵を有する者（ACME プロトコルを介して発行された証明書に限る）

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

本 CA は、次のいずれかの手続によって受け付けた情報を「3.4 失効申請時の本人性確認と認証」に従って確認し、証明書の失効処理を行う。

1. 指定事業者を経由した申請
2. ACME プロトコルを介した申請 (ACME プロトコルを介して発行された証明書に限る)

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

本 CA は、少なくとも 7 日に一度は CRL を更新し、再発行する。また、発行する CRL の nextUpdate フィールドの値は、thisUpdate フィールドの値から 10 日以内とする。

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

適用外とする。

4.9.12 鍵の危殆化に対する特別要件

本 CA が発行した証明書について私有鍵の危殆化が発覚した場合の連絡は、以下の Web フォームより行うものとする。

https://jprs.jp/pubcert/f_mail/

連絡を行う際には、次のいずれかの情報を提示するものとする。

- ・ 危殆化した私有鍵
- ・ 危殆化した私有鍵によって署名された CSR

(ただし、CNに私有鍵が危殆化したことを示す文字列が記された CSR に限る。

例：CN="This key is compromised")

本 CA は、本 CA が発行した証明書について、提示された私有鍵を利用しているものがないか確認する。

提示された私有鍵を利用する証明書を確認した場合、確認した時点から 24 時間以内に当該証明書を失効する。

4.9.13 証明書の一時停止事由

適用外とする。

4.9.14 証明書の一時停止を申請することができる者

適用外とする。

4.9.15 証明書の一時停止申請手続

適用外とする。

4.9.16 一時停止を継続することができる期間

適用外とする。

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

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。ただし、本 CA は、ACME プロトコルを介して発行された証明書利用者について、上記と異なる取扱いをすることができる。

その他の証明書利用者による本サービスの解約に関する詳細は、ご利用条件で定める。

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

適用外とする。

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

本項については、CPS に規定する。

5.3 人事的管理

本項については、CPS に規定する。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類

本項については、CPS に規定する。

5.4.2 監査ログを処理する頻度

本項については、CPS に規定する。

5.4.3 監査ログを保持する期間

本項については、CPS に規定する。なお、RA システム上の監査ログについては、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

本項については、CPS に規定する。

5.4.5 監査ログのバックアップ手続

本項については、CPS に規定する。

5.4.6 監査ログの収集システム

本項については、CPS に規定する。

5.4.7 イベントを起こした者への通知

本項については、CPS に規定する。

5.4.8 脆弱性評価

本項については、CPS に規定する。

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

本項については、CPS に規定する。なお、次の情報のアーカイブについては、最低 7 年間保存する。

- ・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

5.5.3 アーカイブの保護

本項については、CPS に規定する。

5.5.4 アーカイブのバックアップ手続

本項については、CPS に規定する。

5.5.5 記録にタイムスタンプを付与する要件

本項については、CPS に規定する。

5.5.6 アーカイブ収集システム

本項については、CPS に規定する。

5.5.7 アーカイブの検証手続

本項については、CPS に規定する。

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。このときの通信経路は 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

本項については CPS に規定する。なお、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

7.1.1 サーバー証明書プロファイル

本 CA が発行するサーバー証明書のプロファイルは、次表のとおりである。

本 CA は、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、CT に対応した証明書を発行する。

表 7.1.1.1 (削除)

表 7.1.1.2 サーバー証明書プロファイル(発行日が 2020 年 7 月 29 日以降の証明書に適用)

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		CA が証明書に割り当てる整数のシリアル番号	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) ドメイン認証型 CN=JPRS Domain Validation Authority – G4 (2) 組織認証型 CN=JPRS Organization Validation Authority – G4	-
Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	-
	NotAfter	例) 2009/3/1 00:00:00 GMT	-
Subject	Country	(1) ドメイン認証型 記載しない (2) 組織認証型 組織の住所または個人の住所(国)として、「C=JP」を記載する	-
	State Or Province	(1) ドメイン認証型 記載しない (2) 組織認証型 組織の住所または個人の住所(都道府県)	-

		名) (必須)	
	Locality	(1) ドメイン認証型 記載しない (2) 組織認証型 組織の住所または個人の住所 (市区町村名) (必須)	-
	Organization	(1) ドメイン認証型 記載しない (2) 組織認証型 証明書利用者の組織名または個人の氏名 (必須)	-
	Organizational Unit	(1) ドメイン認証型 記載しない (2) 組織認証型 証明書利用者の部署名 (任意) (ただし、2021年11月18日以降に発行する証明書には記載しない) ・ 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 ・ 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	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 (複数の場合あり)	n
CertificatePolicies	[1] Certificate Policy 1.3.6.1.4.1.53827.1.1.4 CPS http://jprs.jp/pubcert/info/repository/ [2] Certificate Policy (1) ドメイン認証型 2.23.140.1.2.1 (2) 組織認証型 2.23.140.1.2.2	n
CRL Distribution Points	(1) ドメイン認証型 http://repo.pubcert.jprs.jp/sppca/jprs/dvca_g4/fullcrl.crl (2) 組織認証型 http://repo.pubcert.jprs.jp/sppca/jprs/ovca_g4/fullcrl.crl	n
Authority Information Access	[1] ocsip (1.3.6.1.5.5.7.48.1) (1) ドメイン認証型 http://dv.g4.ocsip.pubcert.jprs.jp (2) 組織認証型 http://ov.g4.ocsip.pubcert.jprs.jp [2] ca issuers (1.3.6.1.5.5.7.48.2) (1) ドメイン認証型 http://repo.pubcert.jprs.jp/sppca/jprs/dvca_g4/JPRS_DVCA_G4_DER.cer (2) 組織認証型 http://repo.pubcert.jprs.jp/sppca/jprs/ovca_g4/JPRS_OVCA_G4_DER.cer	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。

7.1.2 中間証明書プロファイル

本 CA が発行する中間証明書のプロファイルは、次表のとおりである。

表 7.1.2.1 (削除)

表 7.1.2.2 (削除)

表 7.1.2.3 中間証明書プロファイル (発行日が 2020 年 7 月 29 日以降の証明書に適用)

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		CA が証明書に割り当てる整数のシリアル番号	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	OU=Security Communication RootCA2	-
Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	-
	NotAfter	例) 2009/3/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) 組織認証型 CN=JPRS Organization Validation Authority - G4 (2) ドメイン認証型 CN=JPRS Domain Validation Authority - G4	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
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
KeyUsage		Certificate Signing Off-line CRL Signing CRL Signing (06)	y

CertificatePolicies	Certificate Policy 1.2.392.200091.100.901.4 CPS http://repository.secomtrust.net/SC-Root2/	N
Basic Constraints	Subject Type=CA Path Length Constraint=0	y
ExtendedKeyUsage	TLS Web Server Authentication	n
CRL Distribution Points	http://repository.secomtrust.net/SC-Root2/SCRoot2CRL.crl	n
Authority Information Access	[1] ocsf (1.3.6.1.5.5.7.48.1) http://scrootca2.ocsf.secomtrust.net [2] ca issuers (1.3.6.1.5.5.7.48.2) http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer	n

7.2 CRLのプロファイル

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 (削除)

表 7.2.2 CRL プロファイル (発行日が 2020 年 7 月 29 日以降の証明書に適用)

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	(1) ドメイン認証型 CN=JPRS Domain Validation Authority - G4 (2) 組織認証型 CN=JPRS Organization Validation Authority - G4	-
This Update		例) 2008/3/1 00:00:00 GMT	-
Next Update		例) 2008/3/5 00:00:00 GMT	-
Revoked Certificate	Serial Number	例) 0123456789	-
	Revocation Date	例) 2008/3/1 00:00:00 GMT	-

s	Reason Code	失効事由 (※)	-
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

※：失効事由が「unspecified」の場合、Reason Code 自体を記載しない。

7.3 OCSP のプロファイル

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 (削除)

表 7.3.2 OCSP プロファイル (発行日が 2020 年 7 月 29 日以降の証明書に適用)

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		CA が割り当てる整数のシリアル番号	-
Signature Algorithm		sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) ドメイン認証型 CN=JPRS Domain Validation Authority - G4 (2) 組織認証型 CN=JPRS Organization Validation Authority - G4	-
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
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

KeyUsage	digitalSignature	y
CertificatePolicies	Certificate Policy 1.3.6.1.4.1.53827.1.1.4 CPS http://jprs.jp/pubcert/info/repository/	n
ExtendedKeyUsage	OCSPSigning	n
OCSP No Check	null	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

当社は、本 CA の運用が本 CP および CPS 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。

また、WebTrust 認証を受ける際に必要な監査は、監査法人が行う。

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 および CPS に対する準拠性を中心として行う。

また、認証局のための WebTrust for CA 規準、WebTrust for BR 規準に基づいて行われる。

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 for CA、WebTrust for BR の検証に関する報告書は、WebTrust for CA、WebTrust for BR 認定の規則に従い、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 CP、CPS および Baseline Requirements に準拠して行われているかについて内部監査を行い、Baseline Requirements 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。

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、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

本項については、CPS に規定する。

9.3.2 機密情報の範囲外の情報

本項については、CPS に規定する。

9.3.3 機密情報を保護する責任

本項については、CPS に規定する。

9.4 個人情報保護

本項については、CPS に規定する。

9.5 知的財産権

特段の合意がなされない限り、以下の情報に関するすべての知的財産権は当社の権利に属するものとする。

- ・本CAが発行した証明書およびサイトシール、証明書の失効情報
- ・本CP、CPSおよび関連文書
- ・本CAの公開鍵および秘密鍵
- ・当社より提供されたソフトウェア

9.6 表明保証

9.6.1 CA 業務の表明保証

本 CA は、CA 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
- ・ CAのシステム稼働の監視・運用
- ・ CRLの発行・公表

9.6.2 RA 業務の表明保証

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CAへの正確な情報伝達
- ・ 証明書失効申請におけるCA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

9.6.3 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。

9.6.4 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。

9.6.5 その他関係者の表明保証

規定しない。

9.7 無保証

本 CA は、本 CP 「9.6.1 CA 業務の表明保証」 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 CA 業務の表明保証」 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

当社は、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

本項については、CPS に規定する。

9.17 その他の条項

適用外とする。