JPRSサーバー証明書認証局証明書ポリシー/認証局運用規程 (Certificate Policy/Certification Practice Statement) Version 2.13

2026年9月4日

株式会社日本レジストリサービス

Copyright©2019 Japan Registry Services Co., Ltd.

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 Requirements への準拠に関する記述の修正
1.40	2023.08.28	Baseline Requirements 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 Requirements の正式名称に関する記述の修正
1.51	2024.06.05	「1.6 定義と略語」の修正
1.52	2024.08.26	「5.4 監査ログの手続」の修正
1.53	2024.11.07	「6.1.1 鍵ペアの生成」、「8.4 監査で扱われる事項」を更新
1.54	2025.05.20	「5.4.1 記録されるイベントの種類」、「8.7 内部監査」を更新
2.00	2025.08.22	CPS Version 1.54 と CP Version 3.80 を統合し、本 CP/CPS Version 2.00 として改訂 Baseline Requirements の各要件への準拠を明確にするため記述見直し
2.10	2025.11.28	「1.6 定義と略語」、「3.2.2.4 ドメイン名の認証」、「3.2.2.8 CAA レコード」、「4.2.1 本人性確認と認証の実施」、「5.7.1 事故および危殆化時の手続」、「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」、「6.7 ネットワークセキュリティ管理」、「8.6 監査結果の開示」を更新
2.11	2026.03.31	「1.1 概要」、「1.6 定義と略語」、「3.2.2.4 ドメイン名の認証」、「4.2.2 証明書申請の承認または却下」を更新
2.12	2026.08.04	「1.6 定義と略語」、「3.2.2.4 ドメイン名の認証」、「4.2.1 本人性確認と認証の実施」、「4.9.1 証明書失効事由」「5.4.1 記録されるイベントの種類」、「5.4.3 監査ログを保持する期間」、「6.1.1 鍵ペアの生成」、「7.1.1 バージョン番号」、「7.2.1 バージョン番号」、「8.1 監査の頻度」「8.4 監査で扱われる事項」を更新
2.13	2026.09.04	「7.1 証明書のプロファイル」を更新

Copyright©2019 Japan Registry Services Co., Ltd.

目次

1. はじめに 12
1.1 概要 12
1.2 文書名と識別 13
1.3 PKI の関係者 13
1.3.1 CA 13
1.3.2 RA 14
1.3.3 証明書利用者 14
1.3.4 検証者 14
1.3.5 その他関係者 14
1.4 証明書の用途 14
1.4.1 適切な証明書の用途 14
1.4.2 禁止される証明書の用途 14
1.5 ポリシー管理 14
1.5.1 文書を管理する組織 14
1.5.2 連絡先 14
1.5.3 ポリシー適合性を決定する者 15
1.5.4 承認手続 15
1.6 定義と略語 15
2. 公開とリポジトリの責任 21
2.1 リポジトリ 21
2.2 情報の公開 21
2.3 公開の時期または頻度 21
2.4 リポジトリへのアクセス管理 21
3. 識別と認証 22
3.1 名前決定 22
3.1.1 名前の種類 22
3.1.2 名前が意味を持つことの必要性 22
3.1.3 証明書利用者の匿名性または仮名性 22
3.1.4 様々な名前形式を解釈するための規則 22
3.1.5 名前の一意性 22
3.1.6 商標の認識、認証および役割 22
3.2 初回の本人性確認 22
3.2.1 私有鍵の所持を証明する方法 22
3.2.2 組織とドメイン名の認証 23

Copyright©2019 Japan Registry Services Co., Ltd.

3.2.2.1 組織の認証 23
3.2.2.2 DBA/Tradename（屋号） 23
3.2.2.3 Country の確認 23
3.2.2.4 ドメイン名の認証 23
3.2.2.5 IP アドレスの認証 28
3.2.2.6 ワイルドカードドメイン名の認証 28
3.2.2.7 データ情報源の正確性 28
3.2.2.8 CAA レコード 29
3.2.2.8.1 CAA レコードの DNSSEC 検証 30
3.2.2.9 Multi-Perspective Issuance Corroboration 30
3.2.3 個人の認証 32
3.2.4 検証されない証明書利用者の情報 32
3.2.5 権限の正当性確認 32
3.2.6 相互運用の基準 32
3.3 鍵更新申請時の本人性確認と認証 32
3.3.1 通常の鍵更新時における本人性確認と認証 32
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 32
3.4 失効申請時の本人性確認と認証 33
4. 証明書のライフサイクルに対する運用上の要件 34
4.1 証明書申請 34
4.1.1 証明書申請を提出することができる者 34
4.1.2 申請手続および責任 34
4.2 証明書申請手続 34
4.2.1 本人性確認と認証の実施 34
4.2.2 証明書申請の承認または却下 36
4.2.3 証明書申請の処理時間 36
4.2.4 CAA レコードの確認 36
4.3 証明書の発行 36
4.3.1 証明書発行時の処理手続 36
4.3.1.1 ルート CA の証明書発行の手動承認 36
4.3.1.2 署名前の証明書のリンティング 36
4.3.1.3 発行済み証明書のリンティング 36
4.3.2 証明書利用者への証明書発行通知 36
4.4 証明書の受領確認 37
4.4.1 証明書の受領確認手続 37
4.4.2 認証局による証明書の公開 37

Copyright©2019 Japan Registry Services Co., Ltd.

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 37
4.5 鍵ペアおよび証明書の用途 37
4.5.1 証明書利用者の私有鍵および証明書の用途 37
4.5.2 検証者の公開鍵および証明書の用途 37
4.6 鍵更新を伴わない証明書の更新 37
4.6.1 鍵更新を伴わない証明書の更新事由 38
4.6.2 証明書の更新申請を行うことができる者 38
4.6.3 証明書の更新申請の処理手続 38
4.6.4 証明書利用者に対する新しい証明書発行通知 38
4.6.5 更新された証明書の受領確認手続 38
4.6.6 認証局による更新された証明書の公開 38
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 38
4.7 鍵更新を伴う証明書の更新 38
4.7.1 鍵更新を伴う証明書の更新事由 38
4.7.2 新しい証明書の申請を行うことができる者 38
4.7.3 鍵更新を伴う証明書の更新申請の処理手続 38
4.7.4 証明書利用者に対する新しい証明書の通知 38
4.7.5 鍵更新された証明書の受領確認手続 38
4.7.6 認証局による鍵更新済みの証明書の公開 39
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 39
4.8 証明書の変更 39
4.8.1 証明書の変更事由 39
4.8.2 証明書の変更申請を行うことができる者 39
4.8.3 証明書の変更申請の処理手続 39
4.8.4 証明書利用者に対する新しい証明書発行通知 39
4.8.5 変更された証明書の受領確認手続 39
4.8.6 認証局による変更された証明書の公開 39
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 39
4.9 証明書の失効と一時停止 39
4.9.1 証明書失効事由 39
4.9.2 証明書失効を申請することができる者 41
4.9.3 失効申請手続 41
4.9.4 失効申請の猶予期間 42
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 42
4.9.6 失効調査の要求 42
4.9.7 証明書失効リストの発行頻度 42

Copyright©2019 Japan Registry Services Co., Ltd.

4.9.8 証明書失効リストの発行最大遅延時間 42
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 42
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 43
4.9.11 利用可能な失効情報の他の形式 43
4.9.12 鍵の危殆化に対する特別要件 44
4.9.13 証明書の一時停止事由 44
4.9.14 証明書の一時停止を申請することができる者 44
4.9.15 証明書の一時停止申請手続 44
4.9.16 一時停止を継続することができる期間 44
4.10 証明書のステータス確認サービス 44
4.10.1 運用上の特徴 44
4.10.2 サービスの利用可能性 44
4.10.3 オプショナルな仕様 45
4.11 加入（登録）の終了 45
4.12 キーエスクローと鍵回復 45
4.12.1 キーエスクローと鍵回復ポリシーおよび実施 45
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 45
5. 設備上、運営上、運用上の管理 46
5.1 物理的セキュリティ管理 47
5.1.1 立地場所および構造 47
5.1.2 物理的アクセス 47
5.1.3 電源および空調 47
5.1.4 水害対策 47
5.1.5 火災対策 47
5.1.6 媒体保管 47
5.1.7 廃棄処理 48
5.1.8 オフサイトバックアップ 48
5.2 手続的管理 48
5.2.1 信頼される役割 48
5.2.2 職務ごとに必要とされる人数 49
5.2.3 個々の役割に対する本人性確認と認証 49
5.2.4 職務分割が必要となる役割 49
5.3 人事的管理 49
5.3.1 資格、経験および身分証明の要件 49
5.3.2 適性調査 49
5.3.3 教育要件 49

Copyright©2019 Japan Registry Services Co., Ltd.

5.3.4 再教育の頻度および要件 50
5.3.5 仕事のローテーションの頻度および順序 50
5.3.6 認められていない行動に対する制裁 50
5.3.7 業務委託先の管理 50
5.3.8 要員へ提供される資料 50
5.4 監査ログの手続 50
5.4.1 記録されるイベントの種類 50
5.4.1.1 ルーターおよびファイアウォールのアクティビティのログ 52
5.4.2 監査ログを処理する頻度 52
5.4.3 監査ログを保持する期間 52
5.4.4 監査ログの保護 53
5.4.5 監査ログのバックアップ手続 53
5.4.6 監査ログの収集システム 53
5.4.7 イベントを起こした者への通知 53
5.4.8 脆弱性評価 53
5.5 記録の保管 53
5.5.1 アーカイブの種類 53
5.5.2 アーカイブ保存期間 54
5.5.3 アーカイブの保護 54
5.5.4 アーカイブのバックアップ手続 54
5.5.5 記録にタイムスタンプを付与する要件 54
5.5.6 アーカイブ収集システム 54
5.5.7 アーカイブの検証手続 54
5.6 鍵の切り替え 55
5.7 危殆化および災害からの復旧 55
5.7.1 事故および危殆化時の手続 55
5.7.1.1 インシデント対応および災害復旧計画 55
5.7.1.2 大量失効計画 56
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 56
5.7.3 私有鍵が危殆化した場合の手続 56
5.7.4 災害後の事業継続性 56
5.8 認証局または登録局の終了 56
6. 技術的セキュリティ管理 57
6.1 鍵ペアの生成およびインストール 57
6.1.1 鍵ペアの生成 57
6.1.2 証明書利用者に対する私有鍵の交付 58

Copyright©2019 Japan Registry Services Co., Ltd.

6.1.3 認証局への公開鍵の交付 58
6.1.4 検証者への CA 公開鍵の交付 58
6.1.5 鍵サイズ 58
6.1.6 公開鍵のパラメータの生成および品質検査 59
6.1.7 鍵の用途 59
6.2 私有鍵の保護および暗号モジュール技術の管理 59
6.2.1 暗号モジュールの標準および管理 60
6.2.2 私有鍵の複数人管理 60
6.2.3 私有鍵のエスクロー 60
6.2.4 私有鍵のバックアップ 60
6.2.5 私有鍵のアーカイブ 60
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 60
6.2.7 暗号モジュールへの私有鍵の格納 60
6.2.8 私有鍵の活性化方法 60
6.2.9 私有鍵の非活性化方法 60
6.2.10 私有鍵の破棄方法 60
6.2.11 暗号モジュールの評価 60
6.3 鍵ペアのその他の管理方法 61
6.3.1 公開鍵のアーカイブ 61
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 61
6.4 活性化データ 62
6.4.1 活性化データの生成および設定 62
6.4.2 活性化データの保護 62
6.4.3 活性化データの他の考慮点 62
6.5 コンピュータのセキュリティ管理 62
6.5.1 コンピュータセキュリティに関する技術的要件 62
6.5.2 コンピュータセキュリティ評価 62
6.6 ライフサイクルの技術的管理 62
6.6.1 システム開発管理 62
6.6.2 セキュリティ運用管理 63
6.6.3 ライフサイクルセキュリティ管理 63
6.7 ネットワークセキュリティ管理 63
6.8 タイムスタンプ 63
7. 証明書および証明書失効リストのプロファイル 64
7.1 証明書のプロファイル 64
7.1.1 バージョン番号 79

Copyright©2019 Japan Registry Services Co., Ltd.

7.1.2 証明書の内容と拡張 79
7.1.3 アルゴリズムオブジェクト識別子 79
7.1.4 名前形式 79
7.1.5 名前制約 80
7.1.6 証明書ポリシーオブジェクト識別子 80
7.1.7 ポリシー制約拡張の使用 80
7.1.8 ポリシー修飾子の構文および意味 80
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 80
7.2 CRL のプロファイル 81
7.2.1 バージョン番号 83
7.2.2 CRL と CRL エントリー拡張 83
7.3 OCSP のプロファイル 84
7.3.1 バージョン番号 84
7.3.2 OCSP 拡張 84
8. 準拠性監査と他の評価 85
8.1 監査の頻度 85
8.2 監査者の身元／資格 85
8.3 監査者と被監査者の関係 85
8.4 監査で扱われる事項 86
8.5 不備の結果としてとられる処置 86
8.6 監査結果の開示 86
8.7 内部監査 86
9. 他の業務上および法的事項 88
9.1 料金 88
9.1.1 証明書の発行/更新手数料 88
9.1.2 証明書アクセス料金 88
9.1.3 失効またはステータス情報アクセス料金 88
9.1.4 その他のサービス料金 88
9.1.5 返金ポリシー 88
9.2 財務的責任 88
9.2.1 保険適用範囲 88
9.2.2 その他の資産 88
9.2.3 エンドエンティティに対する保険または保証範囲 88
9.3 企業情報の機密性 88
9.3.1 機密情報の範囲 88
9.3.2 機密情報の範囲外の情報 89

Copyright©2019 Japan Registry Services Co., Ltd.

9.3.3 機密情報を保護する責任 89
9.4 個人情報の保護 89
9.4.1 個人情報保護プラン 89
9.4.2 個人情報として扱われる情報 89
9.4.3 個人情報とみなされない情報 89
9.4.4 個人情報の保護責任 89
9.4.5 個人情報利用に関する通知と同意 90
9.4.6 司法または行政手続に基づく情報開示 90
9.4.7 その他の情報開示要件 90
9.5 知的財産権 90
9.6 表明保証 90
9.6.1 CA 業務の表明保証 90
9.6.2 RA 業務の表明保証 91
9.6.3 証明書利用者の表明保証 91
9.6.4 検証者の表明保証 92
9.6.5 その他関係者の表明保証 92
9.7 無保証 92
9.8 責任の制限 92
9.9 補償 93
9.10 有効期間と終了 93
9.10.1 有効期間 93
9.10.2 終了 93
9.10.3 終了の効果と効果継続 93
9.11 関係者間の個別通知と連絡 93
9.12 改訂 94
9.12.1 改訂手続 94
9.12.2 通知方法および期間 94
9.12.3 オブジェクト識別子が変更されなければならない場合 94
9.13 紛争解決手続 94
9.14 準拠法 94
9.15 適用法の遵守 94
9.16 雑則 94
9.16.1 完全合意条項 94
9.16.2 権利譲渡条項 94
9.16.3 分離条項 94
9.16.4 強制執行条項 95

Copyright©2019 Japan Registry Services Co., Ltd.

9.16.5 不可抗力条項 95
9.17 その他の条項 95

Copyright©2019 Japan Registry Services Co., Ltd.

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/認証局運用規程（以下「本 CP/CPS」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、および当社が構築する本 CA の運用と維持に関する諸手続を規定した文書である。

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、Security Communication ECC RootCA1 または SECOM TLS RSA Root CA 2024 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。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および本 CP/CPS とを照らし合わせて評価し、ご利用条件および本 CP/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 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	準拠するべき規準
TLSサーバー証明書	・ Baseline Requirements for the Issuance and Management of Publicly - Trusted TLS Server Certificates

Copyright©2019 Japan Registry Services Co., Ltd.

	・ Apple Root Certificate Program ・ Chrome Root Program Policy ・ Microsoft Trusted Root Program ・ Mozilla Root Store Policy ・ CCADB Policy

なお、本 CP/CPS とご利用条件の内容に矛盾がある場合は、ご利用条件が本 CP/CPS に優先して適用される。また、本 CP/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 CP/CPS 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/CPS は、本 CA および認証業務に関する技術面、運用面、サービス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/CPS の正式名称は、「JPRS サーバー証明書認証局証明書ポリシー/認証局運用規程」という。
本 CA が本 CP/CPS に基づき割り当て、証明書を発行する際に使用するオブジェクト識別子（以下「OID」という）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	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。

Copyright©2019 Japan Registry Services Co., Ltd.

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。また、本 CA が証明書利用者に対して発行した証明書を、「利用者向け証明書」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本 CP/CPS「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/CPS の維持、管理は、本 CA が行う。

1.5.2 連絡先

本 CP/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

電子メール：info@jprs.jp

Copyright©2019 Japan Registry Services Co., Ltd.

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/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 CP/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

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。

ADN（Authorization Domain Name）：認証ドメイン名
特定の FQDN に対して、証明書発行のための認証を取得するために使用されるドメイン名のことをいう。本 CA は DNS CNAME ルックアップから返された FQDN をドメイン名の認証の目的で FQDN として使用することができる。FQDN にワイルドカード文字が含まれている場合、本 CA は要求された FQDN の左端部分からすべてのワイルドカードラベルを削除する必要がある。本 CA はベースドメイン名に遭遇するまで、左から右へ 0 個以上のラベルを削除し、中間の値のいずれかをドメイン名の認証に使用することができる。

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

Copyright©2019 Japan Registry Services Co., Ltd.

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 8659 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）：認証局運用規程
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。

DNS TXT Record Email Contact
Baseline Requirements の Appendix A.2.1 項で定義される、「_validation-contactemail」ラベルを前置きした FQDN の DNS ゾーンにおける TXT リソースレコードに含まれるメールアドレスのことをいう。

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

Copyright©2019 Japan Registry Services Co., Ltd.

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。

FQDN（Fully-Qualified Domain Name）：完全修飾ドメイン名
インターネットドメイン名システムにおけるすべての上位ノードのラベルを含むドメイン名のことをいう。

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。

Linting：リンティング
事前証明書（RFC 6962）、証明書、CRL、OCSP レスポンスなどの電子署名されたデータの内容、または RFC5280 の 4.1.1.1 項に記述されている tbs 証明書などの今後署名されるデータオブジェクトの内容が、Baseline Requirements に定義されるプロファイルおよび要件に準拠しているか確認するプロセスのことをいう。

Multi-Perspective Issuance Corroboration（MPIC）
証明書発行前に、プライマリー・ネットワーク・パースペクティブによるドメイン名の認証および CAA チェックで行われた確認が、他のネットワーク・パースペクティブによって裏付けされるプロセスのことをいう。

Network Perspective：ネットワーク・パースペクティブ
Multi-Perspective Issuance Corroboration に関連する。ドメイン名利用権の認証方法または CAA チェックに関連するアウトバウンド・インターネット・トラフィックを送信するた

Copyright©2019 Japan Registry Services Co., Ltd.

めのシステム（例えば、クラウド・ホスト・サーバー・インスタンス）またはネットワーク・コンポーネントの集合体（例えば、VPN および対応するインフラストラクチャ）のことをいう。ネットワーク・パースペクティブの場所は、カプセル化されていないアウトバウンド・インターネット・トラフィックが、そのパースペクティブへのインターネット接続を提供するネットワークインフラストラクチャに最初に引き渡される通常のポイントによって決定される。

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。

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。

Primary Network Perspective：プライマリー・ネットワーク・パースペクティブ
CA が、1)申請されたドメインまたは IP アドレスに証明書を発行する CA の権限、および、2)申請されたドメイン名または IP アドレスに対する申請者の権限またはドメイン名の利用権を判断する際に使用するネットワーク・パースペクティブをいう。

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

Copyright©2019 Japan Registry Services Co., Ltd.

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。

Random Value：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。

Subject：主体者
証明書において主体者として識別されている自然人、デバイス、システム、設備、または法人。主体者は、証明書利用者もしくは、証明書利用者の管理および運用下にあるデバイスである。

Copyright©2019 Japan Registry Services Co., Ltd.

Subject Identity Information：主体者識別情報
証明書の主体者を識別する情報。主体者識別情報には、subjectAltName 拡張領域または Subject の commonName フィールドで指定されるドメイン名または IP アドレスは含まれない。

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。

Top-Level Domain：トップレベルドメイン
RFC 8499 (https://tools.ietf.org/html/rfc8499) より：「トップレベルドメインは、"com"や"jp"等のように、ルートの一つ下のレイヤーに位置するゾーンである。」

Wildcard Certificate：ワイルドカード証明書
Subject Alt Name 拡張領域内に少なくともひとつのワイルドカードドメイン名を含む証明書のことをいう。

Wildcard Domain Name：ワイルドカードドメイン名
”*.” (U+002A ASTERISK, U+002E FULL STOP)で始まる文字列の直後に FQDN が続く文字列のことをいう。

Copyright©2019 Japan Registry Services Co., Ltd.

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 および本 CP/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/CPS は、少なくとも 365 日に 1 回改訂するものとし、改訂の都度、リポジトリ上に公開する。本 CP/CPS には、Baseline Requirements の最新バージョンをどのように履行するか詳細に規定するものとする。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。

Copyright©2019 Japan Registry Services Co., Ltd.

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 名前が意味を持つことの必要性

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ァイル」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。

Copyright©2019 Japan Registry Services Co., Ltd.

3.2.2 組織とドメイン名の認証

本 CA は、本項に基づき依拠するすべての書類について、改ざんまたは偽造がないか検査する。

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 Subject Alt Name 拡張領域内に含めるすべての FQDN を認証する。

本項のサブセクション 3.2.2.4.1 項から 3.2.2.4.21 項は、Baseline Requirements におけるセクション番号に対応する。

本 CA では、「RFC 7686 - The ".onion" Special-Use Domain Name」による FQDN が証明書に含まれている場合、証明書を発行しない。

2026 年 3 月 15 日以降：本 CA はプライマリー・ネットワーク・パースペクティブによるドメイン名の認証または管理権限の検証に関連するすべての DNS クエリに対して、IANA DNSSEC Root トラストアンカーまでの DNSSEC 検証を実施する。プライマリー・ネットワーク・パースペクティブによるドメイン名の認証または管理権限の検証に関連するすべての DNS クエリに使用される DNS リゾルバーは、以下を満たさなければならない：

- RFC 4035 Section 5 で定義されるアルゴリズムを使用して DNSSEC 検証を実施すること
- RFC 5155 で定義される NSEC3 をサポートすること
- RFC 4509 および RFC 5702 で定義される SHA-2 をサポートすること
- RFC 6840 Section 4 に列挙されているセキュリティ上の懸念事項を適切に処理するこ

Copyright©2019 Japan Registry Services Co., Ltd.

と
本 CP/CPS の 3.2.2.4.4 項および 3.2.2.4.14 項に記載されているメールによるドメイン名の認証方法において、本 CA はプライマリー・ネットワーク・パースペクティブによるドメイン名の認証または管理権限の検証に関連する認証ドメイン名を取得しようとするすべての DNS CNAME、CAA、TXT クエリに対して、IANA DNSSEC Root トラストアンカーまでの DNSSEC 検証を実施し、また本 CA は DNSSEC 検証を無効化するためにローカルポリシーを使用しない。その他の DNS クエリにおいても、本 CA は IANA DNSSEC Root トラストアンカーまでの DNSSEC 検証を実施するものとし、また本 CA は DNSSEC 検証を無効化するためにローカルポリシーを使用しない。
その他のすべてのドメイン名の認証方法において、本 CA はプライマリー・ネットワーク・パースペクティブによるドメイン名の認証または管理権限の検証に関連するすべての DNS クエリに対して、IANA DNSSEC Root トラストアンカーまでの DNSSEC 検証を実施し、また本 CA はドメイン名の認証または管理権限の検証に関連する DNS クエリに対して DNSSEC 検証を無効化するためにローカルポリシーを使用しない。
IANA DNSSEC Root トラストアンカーまでの DNSSEC 検証は、本 CP/CPS「8.7 内部監査」の要件を満たすために実施される内部監査の対象外とする。

IANA DNSSEC Root トラストアンカーまでの DNSSEC 検証は、本 CP/CPS「5.4.1 記録されるイベントの種類」のログ要件の対象外とする。

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。
2025年7月10日以降に発行する証明書より、この方法を適用外とする。

3.2.2.4.3 Phone Contact with Domain Contact
適用外とする。

3.2.2.4.4 Email to a Constructed Address
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. @の左側にadmin、administrator、webmaster、hostmaster、postmasterのいずれかを用い、これに@と認証ドメイン名を続けて作成した1つ以上のメールアドレ

Copyright©2019 Japan Registry Services Co., Ltd.

ス宛にメールを送信する
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

各メールは、そのメールで使用される認証ドメイン名が、確認される各FQDNの認証ドメイン名である場合に、複数のFQDNの利用権を確認することができる。ランダム値は各メールで一意とする。
メールは、ランダム値の再利用を含め、内容全体および受信者を変更しない限り、全文をそのまま再送信することができる。
ランダム値は生成から25日以内の確認応答につき有効なものとする。

3.2.2.4.5 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。
本 CA は、本 CP/CPS「3.2.2.9 Multi-Perspective Issuance Corroboration」で規定されているとおり、Multi-Perspective Issuance Corroboration を実装する。裏付けとしてカウントされるためには、ネットワーク・パースペクティブは、プライマリー・ネットワーク・パースペクティブと同じランダム値を確認する。

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 Value

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

Copyright©2019 Japan Registry Services Co., Ltd.

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

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、FQDN を認証するために選択された認証ドメイン名の DNS TXT Record Email Contact 宛に送信する。
各メールは､そのメールアドレスが認証される各認証ドメイン名の DNS TXT Record Email Contact である場合、複数の FQDN の利用権を確認することができる。すべての受信者が認証される各認証ドメイン名の DNS TXT Record Email Contact である限り、同じメールを複数の受信者に送信できる。
ランダム値はそれぞれのメールに一意のものとする。メールはランダム値の再利用を含めて全体を再送できるが､全体内容と受信者が変更されないことを条件とする。ランダム値はその生成より 25 日以内のレスポンス確認の使用に有効とする。
2025 年 5 月 29 日以降に発行する証明書より、この方法を適用対象とする。本 CA は、本 CP/CPS「3.2.2.9 Multi-Perspective Issuance Corroboration」で規定されているとおり、Multi-Perspective Issuance Corroboration を実装する。裏付けとしてカウントされるためには、ネットワーク・パースペクティブは、ドメイン名の認証に用いられたプライマリー・ネットワーク・パースペクティブと同じメール連絡先を確認する。

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を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)を確認する。

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

Copyright©2019 Japan Registry Services Co., Ltd.

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、ワイルドカードドメイン名の認証に対してこの方法を適用外とする。

Onionドメイン名を除き、本CAは、本 CP/CPS「3.2.2.9 Multi-Perspective Issuance Corroboration」で規定されているとおり、Multi-Perspective Issuance Corroborationを実装する。裏付けとしてカウントされるためには、ネットワーク・パースペクティブは、プライマリー・ネットワーク・パースペクティブと同じランダム値を確認する。

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)を確認する。
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

Copyright©2019 Japan Registry Services Co., Ltd.

ワイルドカードドメイン名の認証に対してこの方法を適用外とする。
Onionドメイン名を除き、本CAは、本CP/CPS「3.2.2.9 Multi-Perspective Issuance Corroboration」で規定されているとおり、Multi-Perspective Issuance Corroborationを実装する。裏付けとしてカウントされるためには、ネットワーク・パースペクティブは、プライマリー・ネットワーク・パースペクティブと同じランダム値を確認する。

3.2.2.4.20 TLS Using ALPN

適用外とする。

3.2.2.4.21 DNS Labeled with Account ID - ACME

適用外とする。

3.2.2.4.22 DNS TXT Record with Persistent Value

適用外とする。

3.2.2.5 IP アドレスの認証

本 CA は、IP アドレスを認証するための証明書を発行しない。

3.2.2.6 ワイルドカードドメイン名の認証

本 CA は、ワイルドカード証明書を発行する前に、ワイルドカードドメイン名における FQDN 部分が「レジストリ管理」または「パブリックサフィックス」（例: 「* .com」、「* .co.uk」、詳細は RFC 6454 8.2 項を参照）であるかを判断する文書化された手順を確立し履践する。
ワイルドカードドメイン名における FQDN 部分が「レジストリ管理」または「パブリックサフィックス」である場合、本 CA は、ドメイン名空間全体の正当な管理を確認できない限り、発行を拒否する（たとえば、「* .co.uk」または「* .local」を発行してはならないが、Example Co.に対して「* .example.com」を発行することはできる）。
ドメイン名空間全体のうち、何が「レジストリ管理」であり、何が登録可能な国別トップレベルドメイン名空間の部分であるかの判断は、Baseline Requirements の記載に従うものとする。

3.2.2.7 データ情報源の正確性

本 CA は、データ情報源を信頼できるデータ情報源として使用する前に、データ情報源の信頼性、正確性、および改ざんや偽造への耐性を評価する。本 CA は、データ情報源の評価中、下記を考慮する。

1. 情報の提供時期
2. 情報源の更新頻度
3. データ提供者とデータ収集の目的
4. データの利用可能性の公開性
5. データの改ざんまたは偽造の困難性

Copyright©2019 Japan Registry Services Co., Ltd.

3.2.2.8 CAA レコード

発行プロセスの一部として、本 CA は、RFC 8659 で指定されているように、発行される証明書の Subject Alt Name 拡張領域内の各 dNSName について、CAA レコードをチェックし、見つかった処理指示に従う。本 CA は発行する場合、CAA レコードの TTL(有効期限内)または 8 時間のうち、いずれか長い方の範囲内で発行する。

証明書に記載される対象のドメイン名に対する申請者の利用権を認証するために依拠される方法（本 CP/CPS 3.2.2.4 項を参照）の中には、証明書の発行前に追加のリモート・ネットワーク・パースペクティブから CAA レコードを取得して処理する必要があるものがある（本 CP/CPS 3.2.2.9 項 を参照)。プライマリー・ネットワーク・パースペクティブを裏付けるためには、リモート・ネットワーク・パースペクティブの CAA チェック応答は、両方のネットワーク・パースペクティブからの応答がバイト単位で同一であるか否かに関わらず、発行許可として解釈される必要がある。また、本 CA は、このセクションで定義されているとおり、プライマリー・ネットワーク・パースペクティブおよびリモート・ネットワーク・パースペクティブのいずれか、またはその双方において許容可能な CAA レコード検索エラーが発生した場合は、リモート・ネットワーク・パースペクティブにより応答が裏付けられたものと見なすことができる。

CAA レコードを処理する際、本 CA は、RFC 8659 で指定されているとおり、issue、issuewild、および iodef プロパティタグを処理する。 ただし、iodef プロパティタグの内容に対する処理は行わない。他のプロパティタグもサポートする場合は、Baseline Requirements に規定されている必須プロパティタグと衝突を避け、必須プロパティタグより優先することがないようにする。

本 CA は critical フラグを尊重し、このフラグセットを持つ不明なプロパティタグに遭遇した場合は証明書を発行しない。

本 CA は、以下のすべてに該当する場合、レコードルックアップの失敗を発行許可と扱うことができる。
・失敗が CA のインフラストラクチャ外である
・ルックアップが少なくとも 1 回再試行されている
・本 CA が、RFC 4035 Section 4.3 で定義される「Insecure」であることを確認している

本 CA は、処理実務の一環として取られたアクションがあればすべてログで記録するものとする。

Copyright©2019 Japan Registry Services Co., Ltd.

3.2.2.8.1 CAA レコードの DNSSEC 検証

2026 年 3 月 15 日以降：本 CA はプライマリー・ネットワーク・パースペクティブによって実施される CAA レコードのルックアップに関連するすべての DNS クエリに対して、IANA DNSSEC Root トラストアンカーまでの DNSSEC 検証を実施する。プライマリー・ネットワーク・パースペクティブによって CAA レコードのルックアップに関連して使用されるすべての DNS クエリに使用される DNS リゾルバーは、以下を満たす：

- RFC 4035 Section 5 で定義されるアルゴリズムを使用して DNSSEC 検証を実施
- RFC 5155 で定義される NSEC3 をサポート
- RFC 4509 および RFC 5702 で定義される SHA-2 をサポート
- RFC 6840 Section 4 に列挙されているセキュリティ上の懸念事項を適切に処理

2026 年 3 月 15 日以降：本 CA は、CAA レコードのルックアップに関連する DNS クエリに対して、DNSSEC 検証を無効化するためにローカルポリシーを使用しない。

2026 年 3 月 15 日以降：本 CA はプライマリー・ネットワーク・パースペクティブによって観測された DNSSEC 検証エラー（例：SERVFAIL）は、発行の許可として扱わない。

本 CA は Multi-Perspective Issuance Corroboration の一環として、リモート・ネットワーク・パースペクティブによって実施される CAA レコードのルックアップに関連するすべての DNS クエリに対して、IANA DNSSEC Root トラストアンカーまでの DNSSEC 検証を実施してもよい。

IANA DNSSEC Root トラストアンカーまでの DNSSEC 検証は、本 CP/CPS「8.7 内部監査」の要件を満たすために実施される内部監査の対象外とする。

3.2.2.9 Multi-Perspective Issuance Corroboration

2025 年 3 月 15 日以降、本 CA は、Baseline Requirements の 3.2.2.9 項に従い、Multi-Perspective Issuance Corroboration を実施する。
本 CA は、証明書発行前に、複数のリモート・ネットワーク・パースペクティブによって、プライマリー・ネットワーク・パースペクティブが行う次の確認結果の裏付けを行う。

- 本 CP/CPS「3.2.2.4 ドメイン名の認証」に規定されるところにより求められる以下の値の存在。
  1)ランダム値、2)リクエストトークン、3)コンタクトアドレス（連絡先）。
- 本 CP/CPS「3.2.2.8 CAA レコード」に規定される、要求されたドメインに対して発行する CA の権限。

クォーラム要件の表は Multi-Perspective Issuance Corroboration に関するクォーラムの

Copyright©2019 Japan Registry Services Co., Ltd.

要件を説明したものである。本 CA がドメイン名利用権と CAA レコードのチェックの両方において同じネットワーク・パースペクティブのセットを使用していない場合、両方のネットワーク・パースペクティブのセット（すなわち、ドメイン名利用権のセットと CAA レコードのチェックのセット）に対してクォーラム要件を満たす必要がある。ネットワーク・パースペクティブはそれらの間の直線距離が 500km 以上である場合、異なるものとみなされる。ネットワーク・パースペクティブは、プライマリー・ネットワーク・パースペクティブ及びクォーラムで表される他のネットワーク・パースペクティブとは異なる場合、「リモート」とみなされる。

本 CA は、CAA レコードに関して、クォーラム要件への適合を満たすための証拠を最大 398 日間再利用することができる。あるドメイン名に証明書を発行した後、リモート・ネットワーク・パースペクティブは、同じ申請者からの証明書発行申請において、同ドメイン名またはそのサブドメインに対する CAA レコードの取得および処理を最大 398 日間省略することができる。

表 3.2.2.9-1 クォーラム要件の表

使用されるリモート・ネットワーク・パースペクティブの数	許容される失敗数
2〜5	1
6 以上	2

実装タイムライン

- 2025 年 3 月 15 日以降、本 CA は、少なくとも 2 つのリモート・ネットワーク・パースペクティブを使用して Multi-Perspective Issuance Corroboration を実施する。
  本 CA は、プライマリー・ネットワーク・パースペクティブが行った確認の裏付けに失敗したリモート・ネットワーク・パースペクティブの数が、クォーラム要件の表で許容される数より多い場合でも、証明書の発行を続行できるものとする。
- 2025 年 9 月 15 日以降、本 CA は、少なくとも 5 つのリモート・ネットワーク・パースペクティブを使用して、Multi-Perspective Issuance Corroboration を実施する。
  本 CA は、クォーラム要件の表の要件が満たされていること、およびプライマリー・ネットワーク・パースペクティブの裏付けを行うリモート・ネットワーク・パースペクティブが少なくとも 2 つの異なる地域インターネット・レジストリのサービス地域内にあることを確認する必要がある。これら要件が満たされない場合、本 CA は証明書の発行を続行しない。

Copyright©2019 Japan Registry Services Co., Ltd.

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。

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/CPS「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、Security Communication ECC RootCA1 または SECOM TLS RSA Root CA 2024 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

3.3.1 通常の鍵更新時における本人性確認と認証

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、本 CP/CPS「3.2 初回の本人性確認」と同様とする。

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

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、本 CP/CPS「3.2 初回の本人性確認」と同様とする。

Copyright©2019 Japan Registry Services Co., Ltd.

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）

Copyright©2019 Japan Registry Services Co., Ltd.

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事業主、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、ご利用条件および本CP/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/CPS「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。

証明書要求には、証明書に含めるべき申請者に関するすべての事実に関する情報、および本CA が Baseline Requirements、本 CA の CP/CPS に準拠するために申請者から取得する必要がある追加情報を含めてもよい。証明書要求が申請者に関する必要な情報の一部を欠いている場合、本 CA は、残りの情報を申請者から取得するか、または信頼できる独立した第三者のデータ情報源から情報を取得して申請者に確認するものとする。本 CA は、申請者によって証明書に含めることを要求されたすべてのデータを検証するための文書化された手順を確立し履践する。

申請者情報には、証明書の Subject Alt Name 拡張領域に含まれる少なくとも 1 つの FQDN を含める。

本 CP/CPS「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」では、利用者向け証明書の有効期間を制限する。

Copyright©2019 Japan Registry Services Co., Ltd.

本 CA は、本 CP/CPS「3.2 初回の本人性確認」で提供された書類およびデータを証明書情報の認証に使用してもよく、または前回の認証結果（権限の検証を含む）を再利用してもよい。ただし、本 CA が該当するデータまたは書類を本 CP/CPS「3.2 初回の本人性確認」に記載されたソースから入手した場合、または証明書発行前の最大日数以内に自ら認証を完了している場合に限る。この最大日数は以下の表で定義されている。

表 4.2.1-1 主体者識別情報検証データ再利用期間

証明書発行日		最大データ再利用期間
	2026 年 3 月 15 日より前	825 日
2026 年 3 月 15 日以降		398 日

本 CP/CPS「3.2.2.4 ドメイン名の認証」に従うドメイン名に用いるデータ、書類、または完了済みの認証は、証明書発行前の最大日数以内に入手されていなければならない。この最大日数は以下の表で定義されている。

表 4.2.1-2 ドメイン名認証データ再利用期間

証明書発行日		最大データ再利用期間
	2026 年 3 月 15 日より前	398 日
2026 年 3 月 15 日以降	2027 年 3 月 15 日より前	200 日
2027 年 3 月 15 日以降	2029 年 3 月 15 日より前	100 日
2029 年 3 月 15 日以降		10 日

いかなる場合においても、以前の認証で使用されたデータまたはドキュメントのいずれかが、証明書の発行前に、データまたはドキュメントの再利用が許可される最大時間を超えて取得されている場合、以前の認証は再利用しない。

Baseline Requirements に規定される認証方法へ変更した後において、本 CA は、Ballot において特段の規定がない限り、本項に規定する期間については、変更前に収集した認証データもしくは文書または認証そのものを引き続き再利用することができる。

本 CA は、ハイリスク証明書要求が Baseline Requirements に従って適切に検証されること確保するために合理的に必要とされる、証明書の承認前にハイリスク証明書要求に対する追加の検証活動を識別し要求する、文書化された手順を作成、保持および実施するものとする。

外部委託先が本項に基づく本 CA の義務のいずれかを履行する場合、本 CA は外部委託先がハイリスク証明書要求を識別しさらに検証するために用いるプロセスが、本 CA 自身のプ

Copyright©2019 Japan Registry Services Co., Ltd.

ロセスと少なくとも同等の保証レベルを提供していることを確認しなければならない。

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。
本 CA は、「.arpa」で終わるドメイン名を含む証明書を発行しない。

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 8659 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 のドメイン名は「jprs.jp」または「acme.jprs.jp」とする。
FQDN に対して証明書を発行する権限を付与したい証明書利用者は、それぞれの DNS ゾーンの CAA レコードの「issue」または「issuewild」プロパティタグに以下いずれかのドメイン名を含めなければならない。
・「jprs.jp」（ACME プロトコルを介さずに発行する証明書）
・「acme.jprs.jp」（ACME プロトコルを介して発行する証明書）

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/CPS「7.1 証明書のプロファイル」に記載する。

4.3.1.1 ルート CA の証明書発行の手動承認

規定しない。

4.3.1.2 署名前の証明書のリンティング

本 CA は、発行する証明書の一部の項目に関して、Baseline Requirements に技術的に適合しているかどうか証明書の発行前のリンティングにより確認し、要件を満たしていない場合は発行を拒否する。

4.3.1.3 発行済み証明書のリンティング

本 CA は、発行済み証明書をテストするため、リンティングを行うことができる。

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

Copyright©2019 Japan Registry Services Co., Ltd.

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/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

Copyright©2019 Japan Registry Services Co., Ltd.

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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「4.4.1 証明書の受領確認手続」と同様とする。

Copyright©2019 Japan Registry Services Co., Ltd.

4.7.6 認証局による鍵更新済みの証明書の公開

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

本 CP/CPS「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

Copyright©2019 Japan Registry Services Co., Ltd.

・証明書に含まれる情報項目（本CP/CPS「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

本CAは、次のいずれかの事由に該当する場合に、24時間以内に証明書を失効させ、対応する失効理由コードを使用するものとする。

1. 証明書利用者が、失効理由コードを指定することなく、書面にて本CAに証明書の失効を要求した場合（CRLReason "unspecified (0)"、これにより CRL にreasonCode 拡張領域が記載されない）
2. 証明書利用者が、オリジナルの証明書要求が承認されたものでなく、遡及的に承認を付与しないことを本CAに通知した場合（CRLReason #9、privilegeWithdrawn）
3. 本CAが、証明書の公開鍵に対応する証明書利用者の私有鍵が危殆化した証拠を入手した場合（CRLReason #1、keyCompromise）
4. 本CAが、証明書の公開鍵に基づいて証明書利用者の私有鍵を容易に計算できる実証または証明された方法を認識した場合（Baseline Requirements の6.1.1.3項 (5)および本CP/CPS「6.1.1 鍵ペアの生成」で特定されるものを含むが、これらに限定されない）（CRLReason #1、keyCompromise）
5. 本CAが、証明書に記載されるFQDNのドメイン認証または管理の認証について、依拠すべきでないという証拠を入手した場合（CAAレコードのチェックを正しく実行できなかった場合および本CP/CPS「3.2.2.8 CAAレコード」に従って発行が許可されていなかった場合を含む）（CRLReason #4、superseded）

本CAは、次のいずれか事由が発生した場合に、24時間以内に証明書を失効させることがあり、また5日以内に証明書を失効させ、対応する失効理由コードを使用するものとする。

6. 証明書がBaseline Requirementsの6.1.5項および6.1.6項の要件に適合しなくなった場合（CRLReason #4、superseded）
7. 本CAが、証明書が不正に使用されたという証拠を入手した場合（CRLReason #9、privilegeWithdrawn）
8. 本CAが、証明書利用者が利用契約またはご利用条件に基づく1つ以上の重大な義務に違反していることを認識した場合（CRLReason #9、privilegeWithdrawn）；
9. 本CAが、証明書に記載されるFQDNの使用が法的に許容されなくなったこと（たとえば、裁判所または仲裁人がドメイン名登録者のドメイン名を使用する権利を取り消したこと）を示す状況を認識した場合（CRLReason #5、cessationOfOperation）
10. 本CAが、ワイルドカード証明書が、詐欺的に誤信させる下位のFQDNの認証に使用

Copyright©2019 Japan Registry Services Co., Ltd.

されたことを認識した場合（CRLReason #9、privilegeWithdrawn）

11. 本CAが、証明書に含まれる情報に重大な変更があったことを認識した場合（CRLReason #9、privilegeWithdrawn）
12. 本CAが、証明書がBaseline Requirements、本CP/CPSに従って発行されていないことを認識した場合（CRLReason #4、superseded）
13. 本CAが、証明書に記載される情報が不正確であると判断し、または不正確であることを認識した場合（CRLReason #9、privilegeWithdrawn）
14. Baseline Requirementsに基づき証明書を発行する本CAの権利がなくなり、または取り消され、もしくは終了された（ただし、CRL/OCSPリポジトリの管理を継続するための手配を本CAが行った場合を除く）（CRLReason "unspecified (0)" 、これによりCRLにreasonCode拡張領域が記載されない）
15. 本CP/CPSにより、Baseline Requirementsの4.9.9.1項で規定することを要しない理由で失効が要求される場合（CRLReason "unspecified (0)"、これにより、CRLにreasonCode拡張領域が記載されない）
16. 本CAが、証明書利用者の私有鍵が危殆化するような実証または証明された方法を認識し、または私有鍵の生成に使用された特定の方法に欠陥があったことの明確な証拠がある場合（CRLReason #1、keyCompromise）

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。

1. 証明書利用者
2. 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
3. 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/CPS「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）

本CAは、失効申請と証明書問題レポートを24時間365日受け付けて応答する。

Copyright©2019 Japan Registry Services Co., Ltd.

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。
本 CA は、証明書問題レポートを受領してから 24 時間以内に、証明書問題レポートに関する事実と状況を調査し、証明書利用者および証明書問題レポートの報告主体に対して、調査結果についての第一次的な報告書を提供する。
本 CA は、事実および状況を検討した後、証明書利用者、証明書問題レポートまたはその他の失効関連通知の報告主体と協力し、証明書が失効されるべきか否か、また、失効する場合は失効する日付を確定させる。
証明書問題レポートまたは失効関連通知の受領から証明書を失効するまでの期間は、本 CP/CPS「4.9.1 証明書失効事由」に規定する期間を超えないものとする。

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

OCSP応答の有効期間は、thisUpdateフィールドとnextUpdateフィールドの時間差（両端を含む）である。その差を算出する目的で、うるう秒を無視すると、3,600秒の差は1時間に等しいものとし、86,400秒の差は1日に等しくなる。
証明書のシリアルナンバーが「assigned」となるのは、次の場合である

- そのシリアルナンバーを持つ証明書または事前証明書 [RFC 6962] が発行CAによって発行されている。
- そのシリアルナンバーを持つ事前証明書が、発行CAに関連付けられた事前証明書の署名証明書[Baseline Requirements 7.1.2.4項]によって発行されている

証明書のシリアルナンバーは、「assigned」でない場合、「unassigned」となる。

Copyright©2019 Japan Registry Services Co., Ltd.

id-ad ocsp accessMethod を使用した Authority Information Access 拡張を含む証明書および事前証明書のステータスを通信する場合は、以下が適用される。
CAが運用するOCSPレスポンダは、RFC 6960やRFC 5019 で説明されているように、HTTP GETメソッドをサポートする。CAは、RFC 8954 に従って Nonce 拡張 (1.3.6.1.5.5.7.48.1.2) を処理する場合がある。
利用者向け証明書または対応する事前証明書の場合、以下が適用される。

- 2025年1月15日より、証明書または事前証明書が最初に公開された、またはその他の方法で利用可能になってから 15分以内に、信頼できるOCSP応答が利用可能にならなければならない (つまり、応答者は「unknown」ステータスで応答してはならない)。
- 有効期間が16時間未満のOCSP応答の場合、CAは nextUpdate の前の有効期間半分に先立ち更新されたOCSP応答を提供する。
- 有効期間が16時間以上のOCSP応答の場合、CAは nextUpdate の少なくとも8時間前および thisUpdate の4日後までに、更新されたOCSP応答を提供する。

下位CA証明書のステータスの場合、CAは少なくとも12か月ごとおよび証明書の失効後24時間以内に更新されたOCSP 応答を提供する。
OCSPレスポンダが応答する意思がある、または応答する必要があるすべての証明書のステータスを通信するには、以下が適用される。
OCSP応答は、RFC 6960やRFC 5019 に準拠していなければならない。OCSP応答は、次のいずれかでなければならない。

1. 失効ステータスがチェックされている証明書を発行したCAによって署名されている
2. 本CP/CPS「7.1 証明書のプロファイル」 のOCSPレスポンダ証明書プロファイルに準拠しているOCSPレスポンダによって署名されている

利用者向け証明書のOCSP応答の有効期間は 8時間以上10日以下でなければならない。
OCSPレスポンダが「unassigned」の証明書シリアルナンバーのステータスのリクエストを受信した場合、レスポンダは「good」ステータスで応答すべきではない。OCSPレスポンダがBaseline Requirementsの7.1.2.3項または7.1.2.5項に沿って技術的に制約されていないCA向けである場合、レスポンダはそのような要求に対して「good」ステータスで応答してはならない。

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

規定しない。

4.9.11 利用可能な失効情報の他の形式

適用外とする。

Copyright©2019 Japan Registry Services Co., Ltd.

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。

本 CA は、CRL または OCSP サーバーの失効エントリーを、失効した証明書の有効期限日が過ぎるまで削除しない。

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。

Copyright©2019 Japan Registry Services Co., Ltd.

本 CA は、通常の運用状況の下で 10 秒以内のレスポンス時間を提供するために十分なリソースで、CRL および OCSP 機能を運用および維持するものとする。
本 CA は、アプリケーションソフトウェアが、本 CA によって発行されたすべての有効期限内証明書の現在のステータスを自動的にチェックするために使用できるオンラインリポジトリを 24 時間 365 日体制で維持するものとする。
本 CA は、優先度の高い証明書問題レポートを内部で対応し、必要に応じて当該苦情を法執行機関に通報し、または当該苦情の対象となった証明書を失効させる能力を 24 時間 365 日維持するものとする。

4.10.3 オプショナルな仕様

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。

Copyright©2019 Japan Registry Services Co., Ltd.

5. 設備上、運営上、運用上の管理

CA/Browser Forum の「Network and Certificate System Security Requirements」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、

Copyright©2019 Japan Registry Services Co., Ltd.

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ず、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。

Copyright©2019 Japan Registry Services Co., Ltd.

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

Copyright©2019 Japan Registry Services Co., Ltd.

(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 CP/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 CP/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 CP/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 CP/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 CP/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

Copyright©2019 Japan Registry Services Co., Ltd.

の知識、認証および検証ポリシーおよび手順（本 CA の CP/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 CP/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 CP/CPS「5.3.3 教育要件」および に本 CP/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の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

Copyright©2019 Japan Registry Services Co., Ltd.

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. 証明書失効リストの生成。
6. OCSP 応答の署名。
7. 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 および本 CP/CPS で定められたすべての検証アクション。記録には、少なくとも以下を含める。
      1. 検証対象の情報（例：申請された FQDN または組織名）
      2. 使用した認証ドメイン名（該当する場合で、申請された FQDN と異なる場合）
      3. 使用した検証方法（例：Baseline Requirements の該当セクション番号、または ACME 検証方法の登録ラベル）
   3. 証明書要求の承認と拒否。
   4. 証明書の発行。
   5. 証明書失効リストの生成。
   6. OCSP 応答の署名。
   7. 各ネットワーク パースペクティブからの Multi-Perspective Issuance Corroboration の試行では、少なくとも次の情報を記録する。
      1. 使用されたネットワーク・パースペクティブを一意に識別する識別子。
      2. 試行されたドメイン名
      3. 試行の結果（例:「ドメイン名の認証の合格/不合格」、「CAA の許可/禁止」）。
   8. 証明書申請試行されたドメイン名ごとのマルチ・パースペクティブ発行検証のクォーラムの結果。

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. 関連するルーターおよびファイアウォールのアクティビティ。
   7. CA 施設への出入記録。

Copyright©2019 Japan Registry Services Co., Ltd.

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。

5.4.1.1 ルーターおよびファイアウォールのアクティビティのログ

本 CP/CPS「5.4.1　記録されるイベントの種類」3.6 の要件を満たすために必要なルーターおよびファイアウォールのアクティビティのログには、少なくとも次のものを含める必要がある。

1. ルーターおよびファイアウォールへのログイン試行の成功と失敗。
2. 構成の変更、ファームウェアの更新、アクセス制御の変更を含む、ルーターおよびファイアウォール上で実行されたすべての管理アクションのログ。
3. 追加、変更、削除を含む、ファイアウォールルールに対して行われたすべての変更のログ。
4. ハードウェアの障害、ソフトウェアのクラッシュ、システムの再起動を含む、すべてのシステムのイベントとエラーのログ。

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/CPS「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 CP/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 CP/ CPS「5.4.1 記録されるイベントの種類」に記載）

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。

Copyright©2019 Japan Registry Services Co., Ltd.

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 CP/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 CP/CPS

Copyright©2019 Japan Registry Services Co., Ltd.

・本 CP/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おいては、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
・証明書利用者からの申請情報およびその処理履歴
・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 CP/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 CP/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。
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。
・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

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。

Copyright©2019 Japan Registry Services Co., Ltd.

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

5.7.1 事故および危殆化時の手続

5.7.1.1 インシデント対応および災害復旧計画

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、および依拠当事者に通知し、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

Copyright©2019 Japan Registry Services Co., Ltd.

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

5.7.1.2 大量失効計画

本 CA は大量失効事象に備えた包括的かつ実行可能な計画を維持し、大量失効計画の年次テストを実施し、テストや実際の事象から得られた教訓を計画に反映し、継続的に対応力を向上させる。

2025 年 9 月 1 日より、本 CA は、Mozilla Root Store Policy の規定に従い、大量失効イベントに対処するための包括的かつ実行可能な計画を策定し、維持する。

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 CA は、業務停止する必要がある場合、その旨を事前に本 CP/CPS「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

Copyright©2019 Japan Registry Services Co., Ltd.

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、証明書利用者を含むその他関係者に関する鍵管理および本 CA の鍵管理に関して規定する。

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 CP/CPS 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 CP/CPS 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 FIPS140-2 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 CP/CPS 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. 鍵ペアが本 CP/CPS「6.1.5 鍵サイズ」または本 CP/CPS「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方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、本 CP/CPS「4.9.3 失効申請手続」および本 CP/CPS「4.9.12 鍵の危殆化に対する特別要件」の失効要求手続を用いて申請者の私有鍵が危殆化したことを事前に通知されている。
5. 公開鍵が、業界で実証された脆弱な私有鍵に対応している。本 CA は、少なくとも以下

Copyright©2019 Japan Registry Services Co., Ltd.

の予防措置を講じる。

1. Debian weak keys 脆弱性（https://wiki.debian.org/SSLkeys）の場合、本 CA は、リポジトリに記載される鍵の種類（RSA、ECDSA 等）およびサイズごとに https://github.com/cabforum/Debian-weak-keys/で発見されたすべての鍵を拒否する。8192 ビットを超える RSA 鍵サイズを除き、本 CP/CPS「6.1.5 鍵サイズ」の要件を満たすその他の鍵について、本 CA は、Debian weak keys を拒否する。
2. ROCA 脆弱性の場合、本 CA は、https://github.com/crocs-muni/roca で入手可能なツールまたは同等のツールによって識別される鍵を拒否する。
3. Close Primes 脆弱性（https://fermatattack.secvuln.info/）の場合、本 CA は、フェルマーの因数分解法を用いて 100 ラウンド以内に因数分解できる脆弱な鍵を拒否する。

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 は、Baseline Requirements に準拠した利用者向け証明書を発行するにあたって、次のことを確認するものとする。

RSA 鍵ペアの場合

・エンコードされる時点でのモジュラス・サイズは、少なくとも 2048 ビットであること

・モジュラス・サイズ（ビット単位）が 8 で割り切れること

ECDSA 鍵ペアの場合

・キーが NIST P-256、NIST P-384 楕円曲線上の有効な点を表していること

他のアルゴリズムや鍵サイズは許可しない。

Copyright©2019 Japan Registry Services Co., Ltd.

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]

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 （ただし、ECDSA鍵を利用した証明書を除く）
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 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

Copyright©2019 Japan Registry Services Co., Ltd.

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 CP/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。

Copyright©2019 Japan Registry Services Co., Ltd.

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 CP/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。
2026 年 3 月 15 日以前に発行された利用者向け証明書は、有効期間が 397 日を超えるべきではなく、398 日を超えてはならない。

2026 年 3 月 15 日以降かつ 2027 年 3 月 15 日以前に発行された利用者向け証明書は、有効期間が 199 日を超えるべきではなく、200 日を超えてはならない。

2027 年 3 月 15 日以降かつ 2029 年 3 月 15 日以前に発行された利用者向け証明書は、有効期間が 99 日を超えるべきではなく、100 日を超えてはならない。

2029 年 3 月 15 日以降に発行された利用者向け証明書は、有効期間が 46 日を超えるべきではなく、47 日を超えてはならない。

表 6.3.2 利用者向け証明書の最大有効期間の参考

証明書の発行日		最大有効期間
	2026 年 3 月 15 日より前	398 日
2026 年 3 月 15 日以降	2027 年 3 月 15 日より前	200 日
2027 年 3 月 15 日以降	2029 年 3 月 15 日より前	100 日
2029 年 3 月 15 日以降		47 日

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。

Copyright©2019 Japan Registry Services Co., Ltd.

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 CP/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。

Copyright©2019 Japan Registry Services Co., Ltd.

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。

脆弱性管理要件：

- ペネトレーションテストは、少なくとも年 1 回、資格のある第三者によって実施する。
- 脆弱性識別プロセスには、関連するセキュリティアドバイザリの継続的な監視を含める。
- 重大と評価された脆弱性については、発見から 96 時間以内に対応計画を策定する。
- その他のレベルと評価された脆弱性については、本 CA がリスクアセスメントに基づき定めた期間内（通常 60 日を超えない）に修正を完了する。
- 脆弱性は、もはや存在しないように修正された場合、または影響が本 CA のセキュリティ体制に影響しないと確認された場合に、修正済みとみなす。
- すべての対応と結果は文書化し、監査対象とする

6.8 タイムスタンプ

タイムスタンプに関する要件は、本 CP/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。

Copyright©2019 Japan Registry Services Co., Ltd.

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 は、本 CP/CPS「2.2 証明書情報の公開」、本 CP/CPS「6.1.5 鍵サイズ」、本 CP/CPS「6.1.6 公開鍵のパラメータの生成および品質検査」に規定された技術要件を満たすものとする。
本 CA が利用者向け証明書を発行する際、CSPRNG からの 64 ビット以上の出力を含む 1 以上かつ 2^159 未満の連番ではない証明書シリアル番号を生成するものとする。
本 CA が発行する証明書は RFC5280 に準拠している。プロファイルは、次表のとおりである。
表 7.1 - 1 利用者向け証明書プロファイル（Issuer が JPRS Domain Validation Authority – G4 または JPRS Organization Validation Authority – G4 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 証明書利用者の住所（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	-

Copyright©2019 Japan Registry Services Co., Ltd.

		（2）組織認証型 証明書利用者の住所（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 証明書利用者の住所（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 証明書利用者の名称（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） 証明書の Subject Alt Name 拡張領域に含まれる dNSname の値の 1 つを文字単位のコピーとしてエンコードする	-
Subject Public Key Info		Subject の公開鍵 RSA 2048 ビット	-

Copyright©2019 Japan Registry Services Co., Ltd.

拡張領域	設定内容	critical
Key Usage	digitalSignature, keyEncipherment	y
Extended Key Usage	TLS Web Server Authentication	n
Subject Alt Name	dNSName=サーバー名（複数の場合あり）	n
Certificate Policies	[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] ocsp（1.3.6.1.5.5.7.48.1） （1）ドメイン認証型 http://dv.g4.ocsp.pubcert.jprs.jp （2）組織認証型 http://ov.g4.ocsp.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	Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier	Subject 公開鍵の SHA-1 ハッシュ値（160 ビット）	n

Copyright©2019 Japan Registry Services Co., Ltd.

Certificate Transparency Timestamp List （1.3.6.1.4.1.11129.2.4.2）	エンコードされた SignedCertificateTimestampList を含む OCTET STRING とする	n

表 7.1 - 2 利用者向け証明書プロファイル（Issuer が JPRS DV RSA CA 2024 G1 または JPRS OV RSA CA 2024 G1 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 DV RSA CA 2024 G1 （2）組織認証型 CN= JPRS OV RSA CA 2024 G1	-
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 証明書利用者の住所（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 証明書利用者の住所（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 証明書利用者の住所（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	-

Copyright©2019 Japan Registry Services Co., Ltd.

		証明書利用者の名称（必須）	
	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） 証明書の Subject Alt Name 拡張領域に含まれる dNSname の値の 1 つを文字単位のコピーとしてエンコードする	-
Subject Public Key Info		Subject の公開鍵 RSA2048 ビット、RSA3072 ビット、RSA4096 ビットのいずれか	-
拡張領域		設定内容	critical
Key Usage		digitalSignature, keyEncipherment	y
Extended Key Usage		TLS Web Server Authentication	n
Subject Alt Name		dNSName=サーバー名（複数の場合あり）	n
Certificate Policies		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_rsa2024g1/fullcrl.crl （2）組織認証型 http://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/fullcrl.crl	n
Authority Information Access		[1] ocsp（1.3.6.1.5.5.7.48.1） （1）ドメイン認証型 http://dv.rsa2024g1.ocsp.pubcert.jprs.jp （2）組織認証型 http://ov.rsa2024g1.ocsp.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_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer （2）組織認証型	n

Copyright©2019 Japan Registry Services Co., Ltd.

	http://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer	
Authority Key Identifier	Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier	Subject 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Certificate Transparency Timestamp List （1.3.6.1.4.1.11129.2.4.2）	エンコードされた SignedCertificateTimestampList を含む OCTET STRING とする（任意）	n

表 7.1 - 3 利用者向け証明書プロファイル（Issuer が JPRS DV ECC CA 2024 G1 または JPRS OV ECC CA 2024 G1 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		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	（1）ドメイン認証型 CN= JPRS DV ECC CA 2024 G1 （2）組織認証型 CN= JPRS OV ECC CA 2024 G1	-
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 証明書利用者の住所（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 証明書利用者の住所（都道府県名）（必須）	-

Copyright©2019 Japan Registry Services Co., Ltd.

	Locality	（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 証明書利用者の名称（必須）	-
	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） 証明書の Subject Alt Name 拡張領域に含まれる dNSname の値の 1 つを文字単位のコピーとしてエンコードする	-
Subject Public Key Info		Subject の公開鍵 RSA2048 ビット、RSA3072 ビット、RSA4096 ビット、P-256、P-384 のいずれか	-
拡張領域		設定内容	critical
Key Usage		digitalSignature keyEncipherment（ECDSA 鍵を利用した証明書には記載しない）	y
Extended Key Usage		TLS Web Server Authentication	n
Subject Alt Name		dNSName=サーバー名（複数の場合あり）	n
Certificate Policies		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_ecc2024g1/fullcrl.crl （2）組織認証型 http://repo.pubcert.jprs.jp/sppca/jprs/ovca_ecc2024g1/fullcrl.crl	n
Authority Information Access		[1] ocsp（1.3.6.1.5.5.7.48.1） （1）ドメイン認証型 http://dv.ecc2024g1.ocsp.pubcert.jprs.jp	n

Copyright©2019 Japan Registry Services Co., Ltd.

	（2）組織認証型 http://ov.ecc2024g1.ocsp.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_ecc2024g1/JPRSDVCA_ECC2024G1_DER.cer （2）組織認証型 http://repo.pubcert.jprs.jp/sppca/jprs/ovca_ecc2024g1/JPRS_OVCA_ECC2024G1_DER.cer	
Authority Key Identifier	Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier	Subject 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Certificate Transparency Timestamp List（1.3.6.1.4.1.11129.2.4.2）	エンコードされた SignedCertificateTimestampList を含む OCTET STRING とする（任意）	n

表 7.1 - 4 中間証明書プロファイル（Issuer が Security Communication RootCA2 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	-

Copyright©2019 Japan Registry Services Co., Ltd.

		Authority - G4 （2）ドメイン認証型 CN=JPRS Domain Validation Authority - G4	
Subject Public Key Info		Subject の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
Authority Key Identifier		Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		Subject 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Key Usage		Certificate Signing Off-line CRL Signing CRL Signing (06)	y
Certificate Policies		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
Extended Key Usage		TLS Web Server Authentication	n
CRL Distribution Points		http://repository.secomtrust.net/SC-Root2/SCRoot2CRL.crl	n
Authority Information Access		[1] ocsp（1.3.6.1.5.5.7.48.1） http://scrootca2.ocsp.secomtrust.net [2] ca issuers（1.3.6.1.5.5.7.48.2） http://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer	n

表 7.1 - 5 中間証明書プロファイル（Issuer が SECOM TLS RSA Root CA 2024 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	-

Copyright©2019 Japan Registry Services Co., Ltd.

Signature Algorithm		Sha384 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems Co., Ltd.	-
	Common Name	CN=SECOM TLS RSA Root CA 2024	-
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 OV RSA CA 2024 G1 （2）ドメイン認証型 CN= JPRS DV RSA CA 2024 G1	-
Subject Public Key Info		Subject の公開鍵 4096 ビット	-
拡張領域		設定内容	critical
Authority Key Identifier		Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		Subject 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Key Usage		Certificate Signing Off-line CRL Signing CRL Signing (06)	y
Certificate Policies		[1] 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 [2] Certificate Policy 1.2.392.200091.100.901.11	n
Basic Constraints		Subject Type=CA Path Length Constraint=0	y
Extended Key Usage		TLS Web Server Authentication TLS Web Client Authentication	n
CRL Distribution Points		http://repo1.secomtrust.net/root/tlsrsa/tlsrsarootca2024.crl	n
Authority Information Access		[1] ocsp（1.3.6.1.5.5.7.48.1）	n

Copyright©2019 Japan Registry Services Co., Ltd.

	http://tlsrsarootca2024.ocsp.secom-cert.jp [2] ca issuers（1.3.6.1.5.5.7.48.2） http://repo2.secomtrust.net/root/tlsrsa/tlsrsarootca2024.cer	

表 7.1 - 6 中間証明書プロファイル（Issuer が Security Communication ECC RootCA1 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		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Security Communication ECC RootCA1	-
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 OV ECC CA 2024 G1 （2）ドメイン認証型 CN= JPRS DV ECC CA 2024 G1	-
Subject Public Key Info		Subject の公開鍵 384 ビット	-
拡張領域		設定内容	critical
Authority Key Identifier		Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		Subject 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Key Usage		Certificate Signing Off-line CRL Signing CRL Signing (06)	y
Certificate Policies		[1] Certificate Policy	n

Copyright©2019 Japan Registry Services Co., Ltd.

	（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 [2] Certificate Policy 1.2.392.200091.100.902.1	
Basic Constraints	Subject Type=CA Path Length Constraint=0	y
Extended Key Usage	TLS Web Server Authentication TLS Web Client Authentication	n
CRL Distribution Points	http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1CRL.crl	n
Authority Information Access	[1] ocsp（1.3.6.1.5.5.7.48.1） http://sceccrootca1.ocsp.secomtrust.net [2] ca issuers（1.3.6.1.5.5.7.48.2） http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1ca.cer	n

表 7.1 - 7 事前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		利用者向け証明書の同項目とバイト単位で同一	-
Serial Number		同上	-
Signature Algorithm		同上	-
Issuer	Country	同上	-
	Organization	同上	-
	Common Name	同上	-
Validity	NotBefore	同上	-
	NotAfter	同上	-
Subject	Country	同上	-
	State Or Province	同上	-
	Locality	同上	-
	Organization	同上	-
	Common Name	同上	-
Subject Public Key Info		同上	-

Copyright©2019 Japan Registry Services Co., Ltd.

拡張領域	設定内容	critical
Precertificate Poison	extnValue OCTET STRING ● RFC 6962 の 3.1 項で規定されている ASN.1 NULL 値の符号化表現である 0500 バイトを正確に 16 進符号化したものとする。	y
Key Usage	利用者向け証明書の同項目とバイト単位で同一	y
Extended Key Usage	同上	n
Subject Alt Name	同上	n
Certificate Policies	同上	n
CRL Distribution Points	同上	n
Authority Information Access	同上	n
Authority Key Identifier	同上	n
Subject Key Identifier	同上	n

※事前証明書から Precertificate Poison 拡張領域を削除し、利用者向け証明書から Signed Certificate Timestamp 拡張領域を削除した場合、事前証明書と利用者向け証明書の拡張領域の内容は、バイト単位で同一になる。

表 7.1 - 8 OCSP レスポンダ証明書プロファイル（Issuer が JPRS Domain Validation Authority – G4 または JPRS Organization Validation Authority – G4 の証明書に適用）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		CSPRNG から出力される少なくとも 64 ビットを含む、ゼロ(0)より大きく 2^159 より小さい非連続的な数値でなければならない	-
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	-

Copyright©2019 Japan Registry Services Co., Ltd.

		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		Subject の公開鍵 RSA 2048 ビット	-
拡張領域		設定内容	critical
Authority Key Identifier		Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		Subject 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		null	n

表 7.1 – 9 OCSP レスポンダ証明書プロファイル（Issuer が JPRS DV RSA CA 2024 G1 または JPRS OV RSA CA 2024 G1 の証明書に適用）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		CSPRNG から出力される少なくとも 64 ビットを含む、ゼロ(0)より大きく 2^159 より小さい非連続的な数値でなければならない	-
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 DV RSA CA 2024 G1 （2）組織認証型 CN= JPRS OV RSA CA 2024 G1	-
Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	-
	NotAfter	例) 2008/3/5 00:00:00 GMT	-

Copyright©2019 Japan Registry Services Co., Ltd.

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		Subject の公開鍵 RSA2048 ビット、RSA3072 ビット、RSA4096 ビットのいずれか	-
拡張領域		設定内容	critical
Authority Key Identifier		Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		Subject 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		null	n

表 7.1 - 10 OCSP レスポンダ証明書プロファイル（Issuer が JPRS DV ECC CA 2024 G1 または JPRS OV ECC CA 2024 G1 の証明書に適用）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		CSPRNG から出力される少なくとも 64 ビットを含む、ゼロ(0)より大きく 2^159 より小さい非連続的な数値でなければならない	
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	（1）ドメイン認証型 CN= JPRS DV ECC CA 2024 G1 （2）組織認証型 CN= JPRS OV ECC CA 2024 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.	-

Copyright©2019 Japan Registry Services Co., Ltd.

		（固定値）	
	Common Name	OCSP サーバー名（必須）	-
Subject Public Key Info		Subject の公開鍵 256 ビット、384 ビットのいずれか	-
拡張領域		設定内容	critical
Authority Key Identifier		Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		Subject 公開鍵の SHA-1 ハッシュ値（160 ビット）	n
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		null	n

7.1.1 バージョン番号

証明書は X.509 v3 形式とする。

7.1.2 証明書の内容と拡張

本 CA が発行する証明書の内容と拡張は、本 CP/CPS「7.1 証明書のプロファイル」に規定する。

7.1.3 アルゴリズムオブジェクト識別子

本サービスにおいて用いられるアルゴリズム OID は、次のとおりである。

アルゴリズム	オブジェクト識別子
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1.1
sha384 With RSA Encryption	1.2.840.113549.1.1.12
id-ecPublicKey	1.2.840.10045.2.1
ecdsa-with-SHA384	1.2.840.10045.4.3.3

7.1.4 名前形式

本 CA では、RFC5280 で定められる識別名を使用する。
すべての有効な認証パス（RFC 5280 の 6 項で定義されているとおり）について認証パスの利用者向け証明書ごとに、証明書発行者の識別名フィールドのエンコードされた内容は、発行される CA 証明書の Subject 識別名フィールドのエンコードされた形式とバイト単位で同一である必要がある。
本 CA は、証明書を発行することにより、本 CP/CPS に定められた手順に従い、証明書の

Copyright©2019 Japan Registry Services Co., Ltd.

発行日時点で、すべての識別名が正確であることを確認することを表明する。本 CA は、Baseline Requirements の 3.2.2.4 項 に定める場合を除き、識別名にドメイン名を含めてはならない。
識別名には、'.'、'-'、''（スペース）文字などのメタデータや、値が存在しない、不完全、または適用できないことを示すその他の記号のみを含めてはならない。
本 CA では、予約済み IP アドレスまたは内部名を含む Subject Alt Name 拡張領域またはコモンネームを持つ証明書を発行しない。
コモンネームの値が FQDN またはワイルドカードドメイン名の場合、コモンネームの値は、Subject Alt Name 拡張領域の dNSName の値の 1 文字ずつのコピーとしてエンコードする。
具体的には、FQDN のすべてのドメインラベルまたはワイルドカードドメイン名の FQDN 部分のすべての Domain ラベルは LDH ラベルとしてエンコードし、P-ラベルは Unicode に変換しない。

7.1.5 名前制約

本 CA では設定しない。

7.1.6 証明書ポリシーオブジェクト識別子

本 CA が発行する証明書の OID は、本 CP/CPS「1.2 文書名と識別」の OID のとおりである。
次の証明書ポリシー識別子は、証明書または利用者向け証明書が Baseline Requirements に準拠していることを表明するオプションの手段として本 CA が使用するために用意されている。
【ドメイン認証型用】 {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)
【組織認証型用】 {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)

7.1.7 ポリシー制約拡張の使用

設定しない。

7.1.8 ポリシー修飾子の構文および意味

ポリシー修飾子については、本 CP/CPS を公表する Web ページの URI を格納する。

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

設定しない。

Copyright©2019 Japan Registry Services Co., Ltd.

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（IssuerがJPRS Domain Validation Authority – G4またはJPRS Organization Validation Authority – G4の証明書に適用）

基本領域		設定内容	critical
Version		Version 2	-
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	-
This Update		例) 2008/3/1 00:00:00 GMT	-
Next Update		例) 2008/3/5 00:00:00 GMT	-
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2008/3/1 00:00:00 GMT	-
	Reason Code	失効理由コード（※）	-
拡張領域		設定内容	critical
CRL Number		CRL番号	n
Authority Key Identifier		Issuer公開鍵のSHA-1ハッシュ値（160ビット）	n

※：本CAは、CRLのReason Codeの項目に表7.2.2.1に定めるいずれかの失効理由コードを記載する。ただし、失効理由コードが「#0 unspecified」である場合は、Reason Codeの項目自体を記載しない。

表7.2.3 CRLプロファイル（IssuerがJPRS DV RSA CA 2024 G1またはJPRS OV RSA CA 2024 G1の証明書に適用）

基本領域	設定内容	critical
Version	Version 2	-
Signature Algorithm	SHA384 with RSA Encryption	-

Copyright©2019 Japan Registry Services Co., Ltd.

Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	（1）ドメイン認証型 CN= JPRS DV RSA CA 2024 G1 （2）組織認証型 CN= JPRS OV RSA CA 2024 G1	-
This Update		例) 2008/3/1 00:00:00 GMT	-
Next Update		例) 2008/3/5 00:00:00 GMT	-
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2008/3/1 00:00:00 GMT	-
	Reason Code	失効理由コード（※）	-
拡張領域		設定内容	critical
CRL Number		CRL番号	n
Authority Key Identifier		Issuer公開鍵のSHA-1ハッシュ値（160ビット）	n

※：本CAは、CRLのReason Codeの項目に表7.2.2.1に定めるいずれかの失効理由コードを記載する。ただし、失効理由コードが「#0 unspecified」である場合は、Reason Codeの項目自体を記載しない。

表7.2.4 CRLプロファイル（IssuerがJPRS DV ECC CA 2024 G1またはJPRS OV ECC CA 2024 G1の証明書に適用）

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	（1）ドメイン認証型 CN= JPRS DV ECC CA 2024 G1 （2）組織認証型 CN= JPRS OV ECC CA 2024 G1	-
This Update		例) 2008/3/1 00:00:00 GMT	-
Next Update		例) 2008/3/5 00:00:00 GMT	-
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2008/3/1 00:00:00 GMT	-
	Reason Code	失効理由コード（※）	-
拡張領域		設定内容	critical

Copyright©2019 Japan Registry Services Co., Ltd.

CRL Number	CRL番号	n
Authority Key Identifier	Issuer公開鍵のSHA-1ハッシュ値（160ビット）	n

※：本CAは、CRLのReason Codeの項目に表7.2.2.1に定めるいずれかの失効理由コードを記載する。ただし、失効理由コードが「#0 unspecified」である場合は、Reason Codeの項目自体を記載しない。

7.2.1 バージョン番号

証明書失効リストは、X.509 v2 形式とする。

7.2.2 CRL と CRL エントリー拡張

本CAが発行するCRLには、次の拡張領域を使用する。

・reasoncode(OID 2.5.29.21)

失効理由コードが「#0 unspecified」でない限り、2023年7月15日以降に失効する証明書については、CRLのReason Codeの項目に失効理由コードを含めるものとする。

本CAのCRLのReason Codeの項目には、次の表の「#0 unspecified」以外の失効理由を記載するものとする。

表 7.2.2.1 失効理由コード

失効理由コード	この失効理由コードを指定する事由
#0 unspecified	該当なし ・以下に定める失効事由のいずれにも該当しない場合
#1 keyCompromise	鍵の危殆化 ・証明書利用者の私有鍵が危殆化した、またはその可能性がある場合
#3 affiliationChanged	組織情報の変更 ・証明書記載情報のうち組織の名称その他の組織に関する情報に変更が生じた場合
#4 superseded	証明書の取替 ・その他の失効事由に該当しない場合において、既存の証明書を取り替える場合
#5 cessationOfOperation	運用の停止 ・証明書記載情報に含まれるドメイン名の全部または一部について、その管理権限を失った場合

Copyright©2019 Japan Registry Services Co., Ltd.

	・Webサイトの停止に伴い証明書を使用しなくなった場合
#9 privilegeWithdrawn	権限のはく奪 ・証明書利用者がご利用条件に違反した場合

7.3 OCSP のプロファイル

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

本 CP/CPS「7.1 証明書のプロファイル」に記載する。OCSP 応答の singleExtensions には、reasonCode（OID 2.5.29.21）CRL エントリー拡張を含めてはならない。

Copyright©2019 Japan Registry Services Co., Ltd.

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/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。
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、本 CP/CPS「7.1.5 名前制約」に従って技術的に制約され、かつ本 CP/CPS「8.7 内部監査」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、cA boolean 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 CP/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。

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 CP/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。
6. 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。

Copyright©2019 Japan Registry Services Co., Ltd.

8.4 監査で扱われる事項

監査は、本CAの運用の本CP/CPSに対する準拠性を中心として行う。
また、WebTrust認証を受ける際は、次の規準に基づいて行われる。

- WebTrust for CAs
- WebTrust for CAs - TLS Baseline
- WebTrust for CAs - 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 CP/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 CP/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 の本 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

WebTrust 認証に関する監査結果は、監査人から本 CA に対して報告される。
本 CA は、監査期間の終了後 3 か月以内に監査報告書を公開する。
監査報告書の公開が 3 か月を超えて遅延した場合、本 CA は監査人によって署名された説明文書を提供するものとする。

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。

Copyright©2019 Japan Registry Services Co., Ltd.

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 CP/CPS 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。
2025 年 3 月 15 日以降、本 CA は、選択されたサンプルセット内にある証明書の技術的な正確性を検証するためのリンティングプロセスを、対象の証明書について以前に実行されたリンティングとは別に使用する。
本 CP/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 CP/CPS 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。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/CPS に準拠していることを確認する。

Copyright©2019 Japan Registry Services Co., Ltd.

9. 他の業務上および法的事項

9.1 料金

9.1.1 証明書の発行/更新手数料

別途、ご利用条件に規定する。

9.1.2 証明書アクセス料金

規定しない。

9.1.3 失効またはステータス情報アクセス料金

規定しない。

9.1.4 その他のサービス料金

別途、ご利用条件に規定する。

9.1.5 返金ポリシー

別途、ご利用条件に規定する。

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。

9.2.1 保険適用範囲

規定しない。

9.2.2 その他の資産

規定しない。

9.2.3 エンドエンティティに対する保険または保証範囲

規定しない。

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 および本 CP/CPS 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

Copyright©2019 Japan Registry Services Co., Ltd.

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も、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

9.4.1 個人情報保護プラン

当社のプライバシーポリシーについては、ホームページ（https://jprs.jp/privacy.html）にて公表する。

9.4.2 個人情報として扱われる情報

当社のホームページ（https://jprs.jp/privacy.html）にて公表するプライバシーポリシーにて定める。

9.4.3 個人情報とみなされない情報

当社は、当社のホームページ（https://jprs.jp/privacy.html）にて公表するプライバシーポリシーに定める情報以外は、個人情報とみなさない。

9.4.4 個人情報の保護責任

当社のホームページ（https://jprs.jp/privacy.html）にて公表するプライバシーポリシーにて定める。

Copyright©2019 Japan Registry Services Co., Ltd.

9.4.5 個人情報利用に関する通知と同意

当社のホームページ（https://jprs.jp/privacy.html）にて公表するプライバシーポリシーにて定める。

9.4.6 司法または行政手続に基づく情報開示

当社のホームページ（https://jprs.jp/privacy.html）にて公表するプライバシーポリシーにて定める。

9.4.7 その他の情報開示要件

当社のホームページ（https://jprs.jp/privacy.html）にて公表するプライバシーポリシーにて定める。

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

本CP/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-nd/4.0/

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 のシステム稼動の監視・運用
・CRL の発行・公表

Copyright©2019 Japan Registry Services Co., Ltd.

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

本CAは、ご利用条件に規定することで、申請者が本項の誓約と保証を本CAおよび証明書の受益者のために履行することを要求するものとする。

本CAは、証明書の発行前に、本CAおよび証明書の受益者のため、申請者よりご利用条件に対する同意を取得する。

本CAは、ご利用条件が申請者に対して、法的強制力を有することを保証するプロセスを導入する。

ご利用条件には、以下の義務と保証を課す条項を含める。
1. 情報の正確性：証明書申請時、および本CAが証明書の発行に関連して要求する場合、常に正確かつ完全な情報を本CAに提供する義務および保証。

2. 私有鍵の保護：申請者は、要求された証明書に含まれる公開鍵に対応する私有鍵の管理を保証し、機密性を保持し、常に適切に保護するために、あらゆる合理的な手段を講じる義務および保証。

3. 証明書の受領：証明書利用者が証明書の内容を確認し、正確性を検証する義務および保証

4. 証明書の使用：証明書に記載のsubjectAltNameでアクセス可能なサーバーにのみ証明書をインストールし、 適用されるすべての法律に準拠し、ご利用条件にのみ従って証明書を使用する義務および保証。

5. 報告および失効：以下の義務および保証。
a. 証明書に含まれる公開鍵に関連する証明書利用者の私有鍵の不正使用または危殆化の事実または疑いがある場合、速やかに証明書の失効を要求し、証明書および関連する私有鍵の使用を停止すること。

Copyright©2019 Japan Registry Services Co., Ltd.

b. 証明書に記載される情報が間違いもしくは不正確であり、または間違いもしくは不正確になった場合、速やかに証明書の失効を要求し、その使用を停止すること。

6. 証明書の使用停止：鍵の危殆化を理由に証明書が失効した場合、証明書に含まれる公開鍵に対応する私有鍵の使用をすべて速やかに停止する義務および保証。

7. 応答性： 鍵の危殆化または証明書の不正使用に関する本CAの指示に対し、所定の期間内に対応する義務。

8. 承認および受諾： 申請者がご利用条件に違反した場合、あるいは本CP/CPSまたはBaseline Requirementsによって証明書の失効が要求された場合、本CAは直ちに証明書を失効する権利を有することを認め、承諾すること。

9.6.4 検証者の表明保証

検証者は、本 CP/CPS 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/CPS 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/CPS「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/CPS「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

Copyright©2019 Japan Registry Services Co., Ltd.

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

9.10.2 終了

本 CP/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。

Copyright©2019 Japan Registry Services Co., Ltd.

9.12 改訂

9.12.1 改訂手続

本 CP/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 CP/CPS を変更した場合、すみやかに変更した本 CP/CPS 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が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/CPS 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

本 CA は、本 CA 事業および発行する証明書に適用されるすべての法律に従い、証明書を発行しその PKI を運用するものとする。

9.16 雑則

9.16.1 完全合意条項

規定しない。

9.16.2 権利譲渡条項

別途、ご利用条件に規定する。

9.16.3 分離条項

Baseline Requirements と本 CA の運用および証明書の発行を行う地域における法律、規

Copyright©2019 Japan Registry Services Co., Ltd.

制、行政命令（以下「法律」とする）が矛盾する場合、本 CA は、当該地域において要件を合法かつ有効とするために必要な最小限の範囲で、矛盾する要件を修正することができる。これは、該当する法律の対象となる本 CA の運用または証明書の発行に限り適用される。本項に基づく要件の修正を行う場合、本 CA は、直ちに（また、修正された要件に基づいた証明書を発行する前に）、本 CA の CP/CPS の 9.16.3 項に、本項に基づく要件の修正を要求する法律への参照および修正内容について詳細な言及を記載しなければならない。本 CA は、修正された要件に基づいた証明書を発行する前に、CA/Browser Forum が本項に基づく要件の修正の可能性について検討できるようにするため、本 CA の CP/CPS に新たに追加された情報について、questions@cabforum.org 宛にメールを送信するとともに、送信した内容が https://cabforum.org/pipermail/public/ （または CA/Browser Forum が指定するその他の メールアドレスやリンク）で閲覧可能な公開メールアーカイブにインデックスされたことを確認するものとする。

本項に基づき有効となる本 CA の実務に対するいかなる修正も、法律が適用されなくなった場合、または Baseline Requirements が修正され Baseline Requirements と法律を同時に遵守することが可能となった場合は、本項に基づき修正された要件による実務を中止する。

本項に基づく要件の修正、本 CA の CP/CPS の修正、および CA/Browser Forum への通知は、90 日以内に行われる必要がある。

9.16.4 強制執行条項

本 CP/CPS「9.13 紛争解決手続」およびご利用条件に規定する。

9.16.5 不可抗力条項

別途、ご利用条件に規定する。

9.17 その他の条項

適用外とする。

Copyright©2019 Japan Registry Services Co., Ltd.