JPRSサーバー証明書認証局証明書ポリシー（Certificate Policy）新旧対照表

変更履歴あり	整形版	備考
凡例： 赤字（下線付き）　：追加 ~~青字（取消線付き）~~：削除		
JPRSサーバー証明書 認証局証明書ポリシー (Certificate Policy) Version 3.74~~3~~	JPRSサーバー証明書 認証局証明書ポリシー (Certificate Policy) Version 3.74	バージョンの更新
2025~~2024~~年3~~11~~月27~~7~~日 株式会社日本レジストリサービス	2025年3月27日 株式会社日本レジストリサービス	改訂日の更新

変更履歴あり	整形版	備考

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	・「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	・「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	ACME 対応版の提供に関する改訂
3.10	2022.03.02	ACME 対応版のご利用条件への参照を追加
3.11	2022.04.01	表紙の日付及び Version を更新
3.20	2022.09.30	・「6.3 鍵ペアのその他の管理方法」の構成変更および本 CA が発行するサーバー証明書の有効期間に関する記述を追加 「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）」に本 CA で取り扱う失効理由コードを明記
3.30	2023.04.24	証明書の有効期限の上限に関する記述の修正
3.40	2023.06.08	・Baseline Requirement への準拠に関する記述の修正 ・OCSP プロファイルの変更に伴う改訂
3.50	2023.08.28	・Baseline Requirement の各要件への準拠を明確にするため記述見直し
3.60	2024.02.22	中間 CA 追加に伴う改訂
3.70	2024.04.11	表 7.1-2、表 7.1-3 のプロファイルの変更
3.71	2024.06.05	「1.6 定義と略語」、「4.2.4 CAA レコードの確認」の修正
3.72	2024.08.26	「4.2.1 本人性確認と認証の実施」の記述を修正
3.73	2024.11.07	「4.3.1 証明書発行時の処理手続」、「4.9.1 証明書失効事

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	・「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	・「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	ACME 対応版の提供に関する改訂
3.10	2022.03.02	ACME 対応版のご利用条件への参照を追加
3.11	2022.04.01	表紙の日付及び Version を更新
3.20	2022.09.30	・「6.3 鍵ペアのその他の管理方法」の構成変更および本 CA が発行するサーバー証明書の有効期間に関する記述を追加 「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）」に本 CA で取り扱う失効理由コードを明記
3.30	2023.04.24	証明書の有効期限の上限に関する記述の修正
3.40	2023.06.08	・Baseline Requirement への準拠に関する記述の修正 ・OCSP プロファイルの変更に伴う改訂
3.50	2023.08.28	・Baseline Requirement の各要件への準拠を明確にするため記述見直し
3.60	2024.02.22	中間 CA 追加に伴う改訂
3.70	2024.04.11	表 7.1-2、表 7.1-3 のプロファイルの変更
3.71	2024.06.05	「1.6 定義と略語」、「4.2.4 CAA レコードの確認」の修正
3.72	2024.08.26	「4.2.1 本人性確認と認証の実施」の記述を修正
3.73	2024.11.07	「4.3.1 証明書発行時の処理手続」、「4.9.1 証明書失効事

変更履歴あり			整形版			備考
		由」、「8.4 監査で扱われる事項」を更新			由」、「8.4 監査で扱われる事項」を更新	
3.74	2025.03.27	「4.2.4 CAA レコードの確認」を更新	3.74	2025.03.27	「4.2.4 CAA レコードの確認」を更新	改訂履歴の追記

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、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、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 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

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、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、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 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

変更履歴あり	整形版	備考

	Issuance and Management of Publicly - Trusted TLS Server Certificates ・ Apple Root Certificate Program ・ Chrome Root Program Policy ・ Microsoft Trusted Root Program ・ Mozilla Root Store Policy

なお、本 CP とご利用条件、CPS の内容に矛盾がある場合は、ご利用条件、本 CP、CPS の順に優先して適用される。また、本 CP 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 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。

整形版	備考

	Issuance and Management of Publicly - Trusted TLS Server Certificates ・ Apple Root Certificate Program ・ Chrome Root Program Policy ・ Microsoft Trusted Root Program ・ Mozilla Root Store Policy

なお、本 CP とご利用条件、CPS の内容に矛盾がある場合は、ご利用条件、本 CP、CPS の順に優先して適用される。また、本 CP 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 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。

変更履歴あり	整形版	備考
### 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「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 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。	### 1.3.3 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「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 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。	

変更履歴あり	整形版	備考
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。 Archive ： アーカイブ 法的またはその他の事由により、履歴の保存を目的に取得する情報のことをいう。 Audit Log ： 監査ログ 認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局システムの動作履歴やアクセス履歴等をいう。 CA（Certification Authority）：認証局 証明書の発行・更新・失効、失効情報の開示、OCSP（Online Certificate Status Protocol）サーバーによる証明書ステータス情報の提供および保管、CA 私有鍵の生成・保護および証明書利用者の登録等を行う主体のことをいう。 CAA (Certificate Authority Authorization) ドメインを使用する権限において、DNS レコードの中にドメインに対して証明書を発行できる認証局情報を記述し、意図しない認証局からの証明書誤発行を防ぐ機能のことをいう。本機能は RFC 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）：認証局運用規定 CA を運用する上での諸手続、セキュリティ基準等、CA の運用を規定する文書のことをいう。 CRL（Certificate Revocation List）：証明書失効リスト 証明書の有効期間中に、証明書記載内容の変更、私有鍵の危殆化等の事由により失効された証明書情報が記載されたリストのことをいう。 CT（Certificate Transparency） RFC 6962 で規定された、発行された証明書の情報を監視・監査するためにログサーバー（CT ログサーバー）に証明書の情報を登録し、公開する仕組みのことをいう。 Digital Certificates ： 電子証明書	**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。 Archive ： アーカイブ 法的またはその他の事由により、履歴の保存を目的に取得する情報のことをいう。 Audit Log ： 監査ログ 認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局システムの動作履歴やアクセス履歴等をいう。 CA（Certification Authority）：認証局 証明書の発行・更新・失効、失効情報の開示、OCSP（Online Certificate Status Protocol）サーバーによる証明書ステータス情報の提供および保管、CA 私有鍵の生成・保護および証明書利用者の登録等を行う主体のことをいう。 CAA (Certificate Authority Authorization) ドメインを使用する権限において、DNS レコードの中にドメインに対して証明書を発行できる認証局情報を記述し、意図しない認証局からの証明書誤発行を防ぐ機能のことをいう。本機能は RFC 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）：認証局運用規定 CA を運用する上での諸手続、セキュリティ基準等、CA の運用を規定する文書のことをいう。 CRL（Certificate Revocation List）：証明書失効リスト 証明書の有効期間中に、証明書記載内容の変更、私有鍵の危殆化等の事由により失効された証明書情報が記載されたリストのことをいう。 CT（Certificate Transparency） RFC 6962 で規定された、発行された証明書の情報を監視・監査するためにログサーバー（CT ログサーバー）に証明書の情報を登録し、公開する仕組みのことをいう。 Digital Certificates ： 電子証明書	

変更履歴あり	整形版	備考
ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CA が電子署名を施すことで、その正当性が保証される。 ECDSA（Elliptic Curve Digital Signature Algorithm） 公開鍵暗号方式として普及している最も標準的な暗号技術のひとつである。 Escrow ： エスクロー 第三者に預けること（寄託）をいう。 FIPS140-2 米国 NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準のことをいう。最低レベル 1 から最高レベル 4 まで定義されている。 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。 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。	ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CA が電子署名を施すことで、その正当性が保証される。 ECDSA（Elliptic Curve Digital Signature Algorithm） 公開鍵暗号方式として普及している最も標準的な暗号技術のひとつである。 Escrow ： エスクロー 第三者に預けること（寄託）をいう。 FIPS140-2 米国 NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準のことをいう。最低レベル 1 から最高レベル 4 まで定義されている。 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。 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。	

変更履歴あり	整形版	備考
OID（Object Identifier）：オブジェクト識別子 ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。 PKI（Public Key Infrastructure）：公開鍵基盤 電子署名、暗号化、認証といったセキュリティ技術を実現するための、公開鍵暗号方式という暗号技術を用いる基盤のことをいう。 Private Key ： 私有鍵 公開鍵暗号方式において用いられる鍵ペアの一方をいい、公開鍵に対応する本人のみが保有する鍵のことをいう。「秘密鍵」ともいう。 Public Key ： 公開鍵 公開鍵暗号方式において用いられる鍵ペアの一方をいい、私有鍵に対応し、通信相手の相手方に公開される鍵のことをいう。 RA（登録局）（Registration Authority）：登録機関 CA の業務のうち、証明書の発行、取消を申請する申請者の実在性確認、本人性確認の審査、証明書発行に必要な情報の登録、CA に対する証明書発行要求等を行う主体のことをいう。 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。 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）	OID（Object Identifier）：オブジェクト識別子 ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。 PKI（Public Key Infrastructure）：公開鍵基盤 電子署名、暗号化、認証といったセキュリティ技術を実現するための、公開鍵暗号方式という暗号技術を用いる基盤のことをいう。 Private Key ： 私有鍵 公開鍵暗号方式において用いられる鍵ペアの一方をいい、公開鍵に対応する本人のみが保有する鍵のことをいう。「秘密鍵」ともいう。 Public Key ： 公開鍵 公開鍵暗号方式において用いられる鍵ペアの一方をいい、私有鍵に対応し、通信相手の相手方に公開される鍵のことをいう。 RA（登録局）（Registration Authority）：登録機関 CA の業務のうち、証明書の発行、取消を申請する申請者の実在性確認、本人性確認の審査、証明書発行に必要な情報の登録、CA に対する証明書発行要求等を行う主体のことをいう。 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。 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）	

変更履歴あり	整形版	備考
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。 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。 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。	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。 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。 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。	
# 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、少なくとも年次で改訂するものとし、改訂の都度、リポジトリ上に公開する。本 CP および 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。	# 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、少なくとも年次で改訂するものとし、改訂の都度、リポジトリ上に公開する。本 CP および 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。	

変更履歴あり	整形版	備考
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。 ### 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。	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。 ### 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。	

変更履歴あり	整形版	備考
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 3.2.2.4.20 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。 本 CA は、すべてのドメイン名の認証に使用した認証方法（関連する Baseline Requirements のバージョン番号を含む）を記録する。 **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	**3.2.2.1 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 3.2.2.4.20 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。 本 CA は、すべてのドメイン名の認証に使用した認証方法（関連する Baseline Requirements のバージョン番号を含む）を記録する。 **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	

変更履歴あり	整形版	備考
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 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. 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 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。	

変更履歴あり	整形版	備考
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 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。 **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	**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 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。 **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	

変更履歴あり	整形版	備考
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 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。 **3.2.2.4.20 TLS Using ALPN** 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	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 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。 **3.2.2.4.20 TLS Using ALPN** 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	

変更履歴あり	整形版	備考
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。 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 ・ドメインのゾーンは ICANN ルートへの DNSSEC 検証チェーンを持っていない 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。	**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。 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 ・ドメインのゾーンは ICANN ルートへの DNSSEC 検証チェーンを持っていない 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。	
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。	**3.2.3 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。	**3.2.4 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「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	**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	

変更履歴あり	整形版	備考
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 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、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。	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 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、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。	

変更履歴あり	整形版	備考
## 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。 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 や 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「6.3.2 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限を制限する。 本 CA は、証明書情報の検証のために、本 CP「3.2 初回の本人確認」に規定したデータとドキュメントを利用することができる。また、本 CP「3.2 初回の本人確認」で特定されるソースからデータ・ドキュメントを取得した場合、または、証明書発行の 825 日前を超えない期間に認証自体が完了している場合に、以前の認証自体を再利用することができる。 ただし、本 CP「3.2.2.4 ドメイン名の認証」に従ったドメイン名の認証のために、利用するデータ、ドキュメントまたは完了した認証は、証明書を発行する 398 日前までに取得されたものである必要がある。 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。 ### 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 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。 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 や 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「6.3.2 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限を制限する。 本 CA は、証明書情報の検証のために、本 CP「3.2 初回の本人確認」に規定したデータとドキュメントを利用することができる。また、本 CP「3.2 初回の本人確認」で特定されるソースからデータ・ドキュメントを取得した場合、または、証明書発行の 825 日前を超えない期間に認証自体が完了している場合に、以前の認証自体を再利用することができる。 ただし、本 CP「3.2.2.4 ドメイン名の認証」に従ったドメイン名の認証のために、利用するデータ、ドキュメントまたは完了した認証は、証明書を発行する 398 日前までに取得されたものである必要がある。 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。 ### 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。	

変更履歴あり	整形版	備考
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~~「jprs.jp」~~のドメイン名値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「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	**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「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	「JPRSサーバー証明書発行サービス ACME対応版」のCAAリソースレコードに指定するドメイン名を「acme.jprs.jp」に変更

変更履歴あり	整形版	備考
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	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。	### 4.4.2 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。	### 4.4.3 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 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。	### 4.5.1 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。	### 4.5.2 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 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。	### 4.6.1 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。	### 4.6.2 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。	### 4.6.3 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。	### 4.6.4 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	### 4.6.5 更新された証明書の受領確認手続	

変更履歴あり	整形版	備考
「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。	「4.4.1 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。	

変更履歴あり	整形版	備考
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 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（CRLReason #4、superseded）	**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 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（CRLReason #4、superseded）	

変更履歴あり	整形版	備考
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、ドメイン名登録者と申請者間の関連するライセンス契約またはサービス契約が終了したこと、またはドメイン名登録者がドメイン名の更新を懈怠したことなど）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または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または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。 ・ 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）	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、ドメイン名登録者と申請者間の関連するライセンス契約またはサービス契約が終了したこと、またはドメイン名登録者がドメイン名の更新を懈怠したことなど）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または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または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。 ・ 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）	

変更履歴あり	整形版	備考
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） 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。 **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「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** 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。 OCSPレスポンスは、RFC 6960やRFC 5019に準拠するものとする。OCSPレスポンスは、以	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。 3. 指定事業者を経由した申請 4. 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。 **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「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** 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。 OCSPレスポンスは、RFC 6960やRFC 5019に準拠するものとする。OCSPレスポンスは、以	

変更履歴あり	整形版	備考
下のいずれかの条件を満たす必要がある。 1. 失効ステータスの確認対象となる証明書を発行したCAによって署名されている。 2. 失効ステータスの確認対象となる証明書を発行したCAによって署名された証明書のOCSP レスポンダによって署名されている。 後者の場合、OCSP署名証明書には、RFC 6960に定義されている、タイプid-pkix-ocsp-nocheckの拡張領域を含める。	下のいずれかの条件を満たす必要がある。 1. 失効ステータスの確認対象となる証明書を発行したCAによって署名されている。 2. 失効ステータスの確認対象となる証明書を発行したCAによって署名された証明書のOCSP レスポンダによって署名されている。 後者の場合、OCSP署名証明書には、RFC 6960に定義されている、タイプid-pkix-ocsp-nocheckの拡張領域を含める。	
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。 RFC 6960やRFC 5019で説明されているように、本CAが運用するOCSPサーバーはHTTP GETメソッドをサポートする。 OCSP応答の有効期間は、thisUpdateとnextUpdate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時間に等しく、86,400秒の差は1日に等しくなる。 利用者向け証明書のステータスの場合 1. OCSP応答の有効期間は8時間以上とする。 2. OCSP応答の有効期間は10日以下とする。 3. 有効期間が16時間未満のOCSP応答の場合、本CAはnextUpdateの前の有効期間半分に先立ち、オンライン証明書ステータスプロトコルを介して提供される情報を更新する。 4. 有効期間が16時間以上のOCSP応答の場合、本CAはnextUpdateの少なくとも8時間前、およびthisUpdateの4日後までに、オンライン証明書ステータスプロトコルを介して提供される情報を更新する。 OCSPレスポンダが「unused」の証明書シリアル番号のステータスのリクエストを受信した場合、OCSPレスポンダは「good」ステータスを応答しない。 本CAは、セキュリティ応答手順の一部として、「unused」のシリアル番号のリクエストについてOCSPレスポンダを監視する。 OCSPレスポンダは、「reserved」証明書のシリアル番号について、Precertificate [RFC 6962]に一致する対応する証明書があるかのように、明確な応答を提供する場合がある。 OCSP要求内の証明書シリアル番号は、次の3つのオプションのいずれかとする。 1.「assigned」：そのCAのSubjectに関連付けられている現在または以前のキーを使用して、そのシリアル番号の証明書が発行CAにより発行されている場合 2.「reserved」：すでにそのシリアル番号を持つ事前証明書［RFC 6962］が次のいずれかによって発行されている場合 a. 発行CA	**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。 RFC 6960やRFC 5019で説明されているように、本CAが運用するOCSPサーバーはHTTP GETメソッドをサポートする。 OCSP応答の有効期間は、thisUpdateとnextUpdate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時間に等しく、86,400秒の差は1日に等しくなる。 利用者向け証明書のステータスの場合 1. OCSP応答の有効期間は8時間以上とする。 2. OCSP応答の有効期間は10日以下とする。 3. 有効期間が16時間未満のOCSP応答の場合、本CAはnextUpdateの前の有効期間半分に先立ち、オンライン証明書ステータスプロトコルを介して提供される情報を更新する。 4. 有効期間が16時間以上のOCSP応答の場合、本CAはnextUpdateの少なくとも8時間前、およびthisUpdateの4日後までに、オンライン証明書ステータスプロトコルを介して提供される情報を更新する。 OCSPレスポンダが「unused」の証明書シリアル番号のステータスのリクエストを受信した場合、OCSPレスポンダは「good」ステータスを応答しない。 本CAは、セキュリティ応答手順の一部として、「unused」のシリアル番号のリクエストについてOCSPレスポンダを監視する。 OCSPレスポンダは、「reserved」証明書のシリアル番号について、Precertificate [RFC 6962]に一致する対応する証明書があるかのように、明確な応答を提供する場合がある。 OCSP要求内の証明書シリアル番号は、次の3つのオプションのいずれかとする。 1.「assigned」：そのCAのSubjectに関連付けられている現在または以前のキーを使用して、そのシリアル番号の証明書が発行CAにより発行されている場合 2.「reserved」：すでにそのシリアル番号を持つ事前証明書［RFC 6962］が次のいずれかによって発行されている場合 a. 発行CA	

変更履歴あり	整形版	備考
b. 発行CAに関連する事前証明書の署名証明書 [Baseline Requirements 7.1.2.4項] 3.「unused」：上記の条件のいずれも満たされない場合 **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。 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**	b. 発行CAに関連する事前証明書の署名証明書 [Baseline Requirements 7.1.2.4項] 3.「unused」：上記の条件のいずれも満たされない場合 **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。 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**	

変更履歴あり	整形版	備考
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。 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。 **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 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。 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。 **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**	

変更履歴あり	整形版	備考
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	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	

変更履歴あり	整形版	備考
・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	・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	

<table>
<tr><th>変更履歴あり</th><th>整形版</th><th>備考</th></tr>
<tr>
<td>
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。
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
<table>
<tr><td></td><td>本CA</td><td>本CAが発行する証明書</td></tr>
<tr><td>digitalSignature</td><td>—</td><td>yes</td></tr>
<tr><td>nonRepudiation</td><td>—</td><td>—</td></tr>
<tr><td>keyEncipherment</td><td>—</td><td>yes
（ただし、ECDSA鍵を利用した証明書を除く）</td></tr>
<tr><td>dataEncipherment</td><td>—</td><td>—</td></tr>
<tr><td>keyAgreement</td><td>—</td><td>—</td></tr>
<tr><td>keyCertSign</td><td>yes</td><td>—</td></tr>
<tr><td>cRLSign</td><td>yes</td><td>—</td></tr>
<tr><td>encipherOnly</td><td>—</td><td>—</td></tr>
</table>
</td>
<td>
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。
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
<table>
<tr><td></td><td>本CA</td><td>本CAが発行する証明書</td></tr>
<tr><td>digitalSignature</td><td>—</td><td>yes</td></tr>
<tr><td>nonRepudiation</td><td>—</td><td>—</td></tr>
<tr><td>keyEncipherment</td><td>—</td><td>yes
（ただし、ECDSA鍵を利用した証明書を除く）</td></tr>
<tr><td>dataEncipherment</td><td>—</td><td>—</td></tr>
<tr><td>keyAgreement</td><td>—</td><td>—</td></tr>
<tr><td>keyCertSign</td><td>yes</td><td>—</td></tr>
<tr><td>cRLSign</td><td>yes</td><td>—</td></tr>
<tr><td>encipherOnly</td><td>—</td><td>—</td></tr>
</table>
</td>
<td></td>
</tr>
</table>

変更履歴あり	整形版	備考

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

6.3.1 公開鍵のアーカイブ

本項については、CPS に規定する。

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 CA 証明書の有効期間および鍵ペアの有効期間については、CPS に規定する。
また、2020 年 9 月 1 日以降に本 CA が発行する利用者向け証明書には、398 日を超える有効期間を設定しない。2020 年 9 月 1 日より前に本 CA が発行した利用者向け証明書は、有効期間が 825 日を超えないものとする。

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

6.4 活性化データ

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

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

6.3.1 公開鍵のアーカイブ

本項については、CPS に規定する。

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 CA 証明書の有効期間および鍵ペアの有効期間については、CPS に規定する。
また、2020 年 9 月 1 日以降に本 CA が発行する利用者向け証明書には、398 日を超える有効期間を設定しない。2020 年 9 月 1 日より前に本 CA が発行した利用者向け証明書は、有効期間が 825 日を超えないものとする。

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

6.4 活性化データ

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

変更履歴あり	整形版	備考

7.1 証明書のプロファイル

本 CA は、本 CP「2.2 証明書情報の公開」、本 CP「6.1.5 鍵サイズ」、本 CP「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 RFC　5280 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 もしくは 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 （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）	-

7.1 証明書のプロファイル

本 CA は、本 CP「2.2 証明書情報の公開」、本 CP「6.1.5 鍵サイズ」、本 CP「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 RFC　5280 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 もしくは 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 （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）	-

変更履歴あり				整形版				備考
	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）	-		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）	-		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	-		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	-	Subject Public Key Info		Subject の公開鍵 RSA 2048 ビット	-	
拡張領域		設定内容	critical	拡張領域		設定内容	critical	
Key Usage		digitalSignature, keyEncipherment	y	Key Usage		digitalSignature, keyEncipherment	y	
Extended Key Usage		TLS Web Server Authentication	n	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	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/	n	Certificate Policies		[1] Certificate Policy 1.3.6.1.4.1.53827.1.1.4 CPS http://jprs.jp/pubcert/info/repository/	n	

変更履歴あり			整形版			備考
	[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			[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		
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	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 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	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	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	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	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 もしくは 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	-

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 もしくは 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	-

変更履歴あり				整形版				備考
	Organization	O=Japan Registry Services Co., Ltd.	-		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	-		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	-	Validity	NotBefore	例）2008/3/1 00:00:00 GMT	-	
	NotAfter	例）2009/3/1 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	-	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）	-		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）	-		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）	-		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	-		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	-	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	拡張領域		設定内容	critical	
Key Usage		digitalSignature, keyEncipherment	y	Key Usage		digitalSignature, keyEncipherment	y	
Extended Key Usage		TLS Web Server Authentication TLS Web Client Authentication	n	Extended Key Usage		TLS Web Server Authentication TLS Web Client Authentication	n	
Subject Alt Name		dNSName=サーバー名（複数の場合あり）	n	Subject Alt Name		dNSName=サーバー名（複数の場合あり）	n	

変更履歴あり			整形版			備考
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	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	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 http://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer	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 http://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer	n	
Authority Key Identifier	Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	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	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	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 もしくは 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	-

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 もしくは 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	-

変更履歴あり				整形版				備考
Signature Algorithm		ecdsa-with-SHA384	-	Signature Algorithm		ecdsa-with-SHA384	-	
Issuer	Country	C=JP	-	Issuer	Country	C=JP	-	
	Organization	O=Japan Registry Services Co., Ltd.	-		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	-		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	-	Validity	NotBefore	例）2008/3/1 00:00:00 GMT	-	
	NotAfter	例）2009/3/1 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	-	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）	-		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）	-		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）	-		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	-		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	-	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	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	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	Extended Key Usage		TLS Web Server Authentication	n	

変更履歴あり			整形版			備考
	TLS Web Client Authentication			TLS Web Client Authentication		
Subject Alt Name	dNSName=サーバー名（複数の場合あり）	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	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	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 （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	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 （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	n	
Authority Key Identifier	Issuer 公開鍵の SHA-1 ハッシュ値（160 ビット）	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	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	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	-

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	-

変更履歴あり				整形版				備考
Serial Number		CA が証明書に割り当てる整数のシリアル番号	-	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	-	Signature Algorithm		sha256 With RSA Encryption	-	
Issuer	Country	C=JP	-	Issuer	Country	C=JP	-	
	Organization	O=SECOM Trust Systems CO.,LTD.	-		Organization	O=SECOM Trust Systems CO.,LTD.	-	
	Common Name	OU=Security Communication RootCA2	-		Common Name	OU=Security Communication RootCA2	-	
Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	-	Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	-	
	NotAfter	例) 2009/3/1 00:00:00 GMT	-		NotAfter	例) 2009/3/1 00:00:00 GMT	-	
Subject	Country	C=JP	-	Subject	Country	C=JP	-	
	Organization	O=Japan Registry Services Co., Ltd.	-		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	-		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		Subject の公開鍵 2048 ビット	-	Subject Public Key Info		Subject の公開鍵 2048 ビット	-	
拡張領域		設定内容	critical	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	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	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	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	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	Basic Constraints		Subject Type=CA Path Length Constraint=0	y	
Extended Key Usage		TLS Web Server Authentication	n	Extended Key Usage		TLS Web Server Authentication	n	
CRL Distribution Points		http://repository.secomtrust.net/SC-Root2/SCRoot2CRL.crl	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-Roo	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-Roo	n	

変更履歴あり			整形版			備考
	t2/SCRoot2ca.cer			t2/SCRoot2ca.cer		

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	-
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	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	-
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	n

変更履歴あり			整形版			備考
		TLS Web Client Authentication			TLS Web Client Authentication	
CRL Distribution Points		http://repo1.secomtrust.net/root/tlsrsa/tlsrsarootca2024.crl	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） 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	Authority Information Access		[1] ocsp（1.3.6.1.5.5.7.48.1） 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	n

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

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

変更履歴あり			整形版			備考
		（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			（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	Basic Constraints		Subject Type=CA Path Length Constraint=0	
Extended Key Usage		TLS Web Server Authentication TLS Web Client Authentication	Extended Key Usage		TLS Web Server Authentication TLS Web Client Authentication	
CRL Distribution Points		http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1CRL.crl	CRL Distribution Points		http://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1CRL.crl	
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	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	

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	-
拡張領域		設定内容	critical

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	-
拡張領域		設定内容	critical

変更履歴あり			整形版			備考
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	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	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	Extended Key Usage		同上	n	
Subject Alt Name		同上	n	Subject Alt Name		同上	n	
Certificate Policies		同上	n	Certificate Policies		同上	n	
CRL Distribution Points		同上	n	CRL Distribution Points		同上	n	
Authority Information Access		同上	n	Authority Information Access		同上	n	
Authority Key Identifier		同上	n	Authority Key Identifier		同上	n	
Subject 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。				※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 もしくは JPRS Organization Validation Authority – G4 の証明書に適用）				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 もしくは JPRS Organization Validation Authority – G4 の証明書に適用）				
基本領域		設定内容	critical	基本領域		設定内容	critical	
Version		Version 3	-	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	-	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	-	Signature Algorithm		sha256 With RSA Encryption	-	
Issuer	Country	C=JP	-	Issuer	Country	C=JP	-	
	Organization	O= Japan Registry Services Co., Ltd.	-		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	-		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	-	Validity	NotBefore	例) 2008/3/1 00:00:00 GMT	-	
	NotAfter	例) 2008/3/5 00:00:00 GMT	-		NotAfter	例) 2008/3/5 00:00:00 GMT	-	
Subject	Country	C=JP（固定値）	-	Subject	Country	C=JP（固定値）	-	
	Organization	Japan Registry Services Co., Ltd.	-		Organization	Japan Registry Services Co., Ltd.	-	

変更履歴あり			
		（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 もしくは 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	-
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	n

整形版			
		（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 もしくは 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	-
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	n

備考

変更履歴あり				整形版				備考
		ビット）				ビット）		
Subject Key Identifier		Subject 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	KeyUsage		digitalSignature	y	
ExtendedKeyUsage		OCSPSigning	n	ExtendedKeyUsage		OCSPSigning	n	
OCSP No Check		null	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 もしくは 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. （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

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 もしくは 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. （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

変更履歴あり	整形版	備考

7.1.1　バージョン番号

本 CA は、バージョン 3 を適用する。

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「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　CP オブジェクト識別子

本 CA が発行する証明書の OID は、本 CP「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。

7.1.1　バージョン番号

本 CA は、バージョン 3 を適用する。

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「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　CP オブジェクト識別子

本 CA が発行する証明書の OID は、本 CP「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。

変更履歴あり	整形版	備考

【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利用

設定しない。

7.1.8 ポリシー修飾子の文法および意味

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

7.1.9 重要証明書ポリシー拡張の処理の意味

設定しない。

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もしくは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

【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利用

設定しない。

7.1.8 ポリシー修飾子の文法および意味

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

7.1.9 重要証明書ポリシー拡張の処理の意味

設定しない。

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もしくは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

変更履歴あり	整形版	備考

※：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もしくは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	-
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もしくは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	-

※：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もしくは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	-
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もしくは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	-

変更履歴あり			
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。

7.2.1 バージョン番号

本 CA は、CRL バージョン 2 を適用する。

7.2.2 CRL 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

整形版			
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。

7.2.1 バージョン番号

本 CA は、CRL バージョン 2 を適用する。

7.2.2 CRL 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

備考

変更履歴あり	整形版	備考

	場合 ・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「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。

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、次の資格・技能を有する監査法人が行う。

- 監査対象から独立している
- WebTrust認証で指定された規準に対応する監査を実施する能力を有する
- PKI技術、情報セキュリティツール・技術、情報技術、セキュリティ監査、第三者を認証する機能を審査することに習熟した個人を雇用している
- WebTrustにより認可されている
- 法律、公的な規制または職業倫理の規範に拘束されている
- 少なくとも 100 万米ドルを補償限度額とする専門職業人賠償責任保険／E&O 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。

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。

	場合 ・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「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。

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、次の資格・技能を有する監査法人が行う。

- 監査対象から独立している
- WebTrust認証で指定された規準に対応する監査を実施する能力を有する
- PKI技術、情報セキュリティツール・技術、情報技術、セキュリティ監査、第三者を認証する機能を審査することに習熟した個人を雇用している
- WebTrustにより認可されている
- 法律、公的な規制または職業倫理の規範に拘束されている
- 少なくとも 100 万米ドルを補償限度額とする専門職業人賠償責任保険／E&O 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。

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。

変更履歴あり	整形版	備考
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 - SSL Baseline ・ WebTrust for CAs - Network Security ### 8.5 不備の結果としてとられる処置 本 CA は、監査報告書で指摘された事項に関し、すみやかに必要な是正措置を行う。 ### 8.6 監査結果の開示 監査結果は、監査人から本 CA に対して報告される。 本 CA は、法律に基づく開示要求があった場合、当社との契約に基づき関係組織からの開示要求があった場合、または本 CA のサーバー証明書発行サービス運営会議が承認した場合を除き、監査結果を外部へ開示することはない。 なお、WebTrust 認証に関する報告書は、WebTrust 認証の規則に従い、特定のサイトにて参照可能となる。 ### 8.7 内部監査 本 CA は、本 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監視し、少なくとも四半期ごとに Baseline Requirements で定められた要件に基づき期間中に本CAが発行した証明書を少なくとも3%の無作為のサンプル抽出による定期的な内部監査を実施することで、サービスの品質を厳密に管理するものとする。 ## 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	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 - SSL Baseline ・ WebTrust for CAs - Network Security ### 8.5 不備の結果としてとられる処置 本 CA は、監査報告書で指摘された事項に関し、すみやかに必要な是正措置を行う。 ### 8.6 監査結果の開示 監査結果は、監査人から本 CA に対して報告される。 本 CA は、法律に基づく開示要求があった場合、当社との契約に基づき関係組織からの開示要求があった場合、または本 CA のサーバー証明書発行サービス運営会議が承認した場合を除き、監査結果を外部へ開示することはない。 なお、WebTrust 認証に関する報告書は、WebTrust 認証の規則に従い、特定のサイトにて参照可能となる。 ### 8.7 内部監査 本 CA は、本 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監視し、少なくとも四半期ごとに Baseline Requirements で定められた要件に基づき期間中に本CAが発行した証明書を少なくとも3%の無作為のサンプル抽出による定期的な内部監査を実施することで、サービスの品質を厳密に管理するものとする。 ## 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	

変更履歴あり	整形版	備考
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 個人情報の保護 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 本CP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 ### 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	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 個人情報の保護 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 本CP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 ### 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	

変更履歴あり	整形版	備考
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。 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**	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。 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**	

変更履歴あり	整形版	備考
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。	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。	

変更履歴あり	整形版	備考
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 の解釈、有効性および証明書の利用にかか	**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 の解釈、有効性および証明書の利用にかか	

変更履歴あり	整形版	備考
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** 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 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 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 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。 **9.17 その他の条項** 適用外とする。	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** 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 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 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 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。 **9.17 その他の条項** 適用外とする。	