株式会社日本レジストリサービス（JPRS）

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー（Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー（Certificate Policy）（整形版）	備考
# JPRSサーバー証明書 （組織認証型） 認証局証明書ポリシー （Certificate Policy） Version ~~1.10~~1.20 2017年~~02月19日~~09月06日 株式会社日本レジストリサービス	# JPRSサーバー証明書 （組織認証型） 認証局証明書ポリシー （Certificate Policy） Version 1.20 2017年09月06日 株式会社日本レジストリサービス	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（組織認証型）認証局証明書ポリシー （Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（整形版）	備考

改版履歴

版数	日付	内容
1.00	2016.04.26	初版発行
1.10	2017.02.19	・「4.6 証明書の更新」に関する記述の追加 ・「4.8 証明書の変更」に関する記述の追加
1.20	2017.09.06	・Baseline Requirement に準拠する旨の記述の追加 ・CAA レコードの処理に関する記述の修正

改版履歴の追加

目次

（省略）

1. はじめに

1.1 概要

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー（以下「本CP」という）は、株式会社日本レジストリサービス（以下「当社」という）が認証局（以下「本CA」という）として発行する電子証明書の用途、利用目的、適用範囲等、電子証明書に関するポリシーを規定するものである。
本CAの運用維持に関する諸手続については、セコム認証基盤運用規程（以下「CPS」という）に規定する。
本CAは、セコムトラストシステムズ株式会社（以下「セコムトラストシステムズ」という）が運営する認証局であるSecurity Communication RootCA2より、片方向相互認証証明書の発行を受けており、証明書利用者に対する証明書発行を行う。

本CAが発行する証明書は、サーバー認証および通信経路で情報の暗号化を行うことに利用する。証明書の有効期間は、証明書を有効とする日から起算して39ヵ月以内とする。また、発行対象は、JPRSサーバー証明書発行サービスご利用条件（以下「ご利用条件」という）により定める。
本CAから証明書の発行を受ける者は、証明書の発行を受ける前に自己の利用目的とご利用条件、本CPおよびCPSとを照らし合わせて評価し、ご利用条件、本CPおよびCPSを承諾する必要がある。
本CAは、CA/Browser Forumがhttps://www.cabforum.org/で公開する「Baseline Requirements」に準拠する。

BR に準拠している旨の追記
（STS からの要請による追記）

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー（Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー（Certificate Policy）（整形版）	備考

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

本CPは、IETFが認証局運用のフレームワークとして提唱するRFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。
本CPは、本CAに関する技術面、運用面の発展や改良に伴い、それらを反映するために必要に応じ改訂されるものとする。

1.2 文書名と識別

本CPの正式名称は、「JPRSサーバー証明書（組織認証型）認証局証明書ポリシー」という。
本CAが本CPに基づき割り当てられるオブジェクト識別子（以下「OID」という）、ならびに本CPが参照するCPSのOIDは、次のとおりである。

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

1.3 PKI の関係者

1.3.1 認証局

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

1.3.1.1 IA

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

1.3.1.2 RA

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

1.3.2 証明書利用者

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

1.3.3 検証者

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

本CPは、IETFが認証局運用のフレームワークとして提唱するRFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。
本CPは、本CAに関する技術面、運用面の発展や改良に伴い、それらを反映するために必要に応じ改訂されるものとする。

1.2 文書名と識別

本CPの正式名称は、「JPRSサーバー証明書（組織認証型）認証局証明書ポリシー」という。
本CAが本CPに基づき割り当てられるオブジェクト識別子（以下「OID」という）、ならびに本CPが参照するCPSのOIDは、次のとおりである。

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

1.3 PKI の関係者

1.3.1 認証局

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

1.3.1.1 IA

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

1.3.1.2 RA

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

1.3.2 証明書利用者

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

1.3.3 検証者

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（整形版）	備考
検証者とは、本CAが発行する証明書の有効性を検証する個人、法人または組織とする。 **1.4 証明書の用途** **1.4.1 適切な証明書の用途** 本CAが発行する証明書は、サーバー認証および通信経路で情報の暗号化を行うことに利用する。 **1.4.2 禁止される証明書の用途** 本CAが発行する証明書の用途は「1.4.1 適切な証明書の用途」のとおりであり、証明書をそれ以外の目的に利用することはできないものとする。 **1.5 ポリシー管理** **1.5.1 文書を管理する組織** 本CPの維持、管理は、本CAが行う。 **1.5.2 連絡先** 本CPに関する連絡先は、次のとおりである。 窓口：株式会社日本レジストリサービス お問い合わせ窓口 住所：〒101-0065 東京都千代田区西神田3-8-1 千代田ファーストビル東館13F 電子メール：info@jprs.jp **1.5.3 ポリシー適合性を決定する者** 本CPの内容については、本CAのサーバー証明書発行サービス運営会議において決定される。 **1.5.4 承認手続** 本CPは、本CAのサーバー証明書発行サービス運営会議の承認によって発効する。 **1.6 定義と略語** **(1) 「あ」～「ん」** アーカイブ 法的またはその他の事由により、履歴の保存を目的に取得する情報のことをいう。 エスクロー 第三者に預けること（寄託）をいう。 鍵ペア 公開鍵暗号方式において、秘密鍵と公開鍵から構成される鍵の対のことをいう。	検証者とは、本CAが発行する証明書の有効性を検証する個人、法人または組織とする。 **1.4 証明書の用途** **1.4.1 適切な証明書の用途** 本CAが発行する証明書は、サーバー認証および通信経路で情報の暗号化を行うことに利用する。 **1.4.2 禁止される証明書の用途** 本CAが発行する証明書の用途は「1.4.1 適切な証明書の用途」のとおりであり、証明書をそれ以外の目的に利用することはできないものとする。 **1.5 ポリシー管理** **1.5.1 文書を管理する組織** 本CPの維持、管理は、本CAが行う。 **1.5.2 連絡先** 本CPに関する連絡先は、次のとおりである。 窓口：株式会社日本レジストリサービス お問い合わせ窓口 住所：〒101-0065 東京都千代田区西神田3-8-1 千代田ファーストビル東館13F 電子メール：info@jprs.jp **1.5.3 ポリシー適合性を決定する者** 本CPの内容については、本CAのサーバー証明書発行サービス運営会議において決定される。 **1.5.4 承認手続** 本CPは、本CAのサーバー証明書発行サービス運営会議の承認によって発効する。 **1.6 定義と略語** **(1) 「あ」～「ん」** アーカイブ 法的またはその他の事由により、履歴の保存を目的に取得する情報のことをいう。 エスクロー 第三者に預けること（寄託）をいう。 鍵ペア 公開鍵暗号方式において、秘密鍵と公開鍵から構成される鍵の対のことをいう。	

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（整形版）	備考
監査ログ 認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局システムの動作履歴やアクセス履歴等をいう。 公開鍵 公開鍵暗号方式において用いられる鍵ペアの一方をいい、秘密鍵に対応し、通信相手の相手方に公開される鍵のことをいう。 秘密鍵 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。「私有鍵」ともいう。 指定事業者 当社が提供するサーバー証明書発行サービスに関して、当社の認定する事業者のことをいう。 タイムスタンプ 電子ファイルの作成日時やシステムが処理を実行した日時等を記録したデータのことをいう。 電子証明書 ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CA が電子署名を施すことで、その正当性が保証される。 リポジトリ CA 証明書および CRL 等を格納し公表するデータベースのことをいう。	監査ログ 認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局システムの動作履歴やアクセス履歴等をいう。 公開鍵 公開鍵暗号方式において用いられる鍵ペアの一方をいい、秘密鍵に対応し、通信相手の相手方に公開される鍵のことをいう。 秘密鍵 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。「私有鍵」ともいう。 指定事業者 当社が提供するサーバー証明書発行サービスに関して、当社の認定する事業者のことをいう。 タイムスタンプ 電子ファイルの作成日時やシステムが処理を実行した日時等を記録したデータのことをいう。 電子証明書 ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CA が電子署名を施すことで、その正当性が保証される。 リポジトリ CA 証明書および CRL 等を格納し公表するデータベースのことをいう。	
(2) 「A」～「Z」 CA（Certification Authority）：認証局 証明書の発行・更新・失効、CA 秘密鍵の生成・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 RFC6844 で規定されている。 CP（Certificate Policy） CA が発行する証明書の種類、用途、申込手続等、証明書に関する事項を規定する文書のこと	**(2) 「A」～「Z」** CA（Certification Authority）：認証局 証明書の発行・更新・失効、CA 秘密鍵の生成・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 RFC6844 で規定されている。 CP（Certificate Policy） CA が発行する証明書の種類、用途、申込手続等、証明書に関する事項を規定する文書のこと	RFC6844で規定されている旨を追記

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（整形版）	備考
をいう。 CPS（Certification Practices Statement）：認証運用規定 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、秘密鍵の紛失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。 IA（Issuing Authority）：発行局 CA の業務のうち、証明書の発行・更新・失効、CA 秘密鍵の生成・保護、リポジトリの維持・管理等を行う主体のことをいう。 OID（Object Identifier）：オブジェクト識別子 ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。 OCSP（Online Certificate Status Protocol） 証明書のステータス情報をリアルタイムに提供するプロトコルのことをいう。 PKI（Public Key Infrastructure）：公開鍵基盤 電子署名、暗号化、認証といったセキュリティ技術を実現するための、公開鍵暗号方式という暗号技術を用いる基盤のことをいう。 RA（登録局）（Registration Authority）：登録機関 CA の業務のうち、申込情報の審査、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。 RFC3647（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。 RSA 公開鍵暗号方式として普及している最も標準的な暗号技術のひとつである。 SHA-1（Secure Hash Algorithm 1） 電子署名に使われるハッシュ関数（要約関数）のひとつである。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいう。ビット長は 160 ビット。	をいう。 CPS（Certification Practices Statement）：認証運用規定 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、秘密鍵の紛失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。 IA（Issuing Authority）：発行局 CA の業務のうち、証明書の発行・更新・失効、CA 秘密鍵の生成・保護、リポジトリの維持・管理等を行う主体のことをいう。 OID（Object Identifier）：オブジェクト識別子 ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。 OCSP（Online Certificate Status Protocol） 証明書のステータス情報をリアルタイムに提供するプロトコルのことをいう。 PKI（Public Key Infrastructure）：公開鍵基盤 電子署名、暗号化、認証といったセキュリティ技術を実現するための、公開鍵暗号方式という暗号技術を用いる基盤のことをいう。 RA（登録局）（Registration Authority）：登録機関 CA の業務のうち、申込情報の審査、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。 RFC3647（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。 RSA 公開鍵暗号方式として普及している最も標準的な暗号技術のひとつである。 SHA-1（Secure Hash Algorithm 1） 電子署名に使われるハッシュ関数（要約関数）のひとつである。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいう。ビット長は 160 ビット。	

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（整形版）	備考
データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。 SHA-256（Secure Hash Algorithm 256） 電子署名に使われるハッシュ関数（要約関数）のひとつである。ビット長は256ビット。 データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。 ## 2. 公開とリポジトリの責任 ### 2.1 リポジトリ 本CAは、リポジトリを24時間365日利用できるように維持管理を行う。ただし、利用可能な時間内においてもシステム保守等により利用できない場合がある。 ### 2.2 証明情報の公開 本CAは、CRL、本CPおよびCPSをリポジトリ上に公開し、証明書利用者および検証者がオンラインによって閲覧できるようにする。 ### 2.3 公開の時期または頻度 本CPおよびCPSは、改訂の都度、リポジトリ上に公開する。 本CAは、24時間ごとに新たなCRLを発行し、リポジトリ上に公開する。また、証明書の失効が行われた場合、即時に新たなCRLを発行し、リポジトリ上に公開する。 また、証明書の有効期間を過ぎたものはCRLから削除する。 ### 2.4 リポジトリへのアクセス管理 本CAは、リポジトリでの公開情報に関して、特段のアクセスコントロールは行わない。証明書利用者は、本CAのCRLを、リポジトリを通じて入手することを可能とする。リポジトリへのアクセスは、一般的なWebインターフェースを通じて可能とする。 ## 3. 識別と認証 ### 3.1 名前決定 #### 3.1.1 名前の種類	データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。 SHA-256（Secure Hash Algorithm 256） 電子署名に使われるハッシュ関数（要約関数）のひとつである。ビット長は256ビット。 データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。 ## 2. 公開とリポジトリの責任 ### 2.1 リポジトリ 本CAは、リポジトリを24時間365日利用できるように維持管理を行う。ただし、利用可能な時間内においてもシステム保守等により利用できない場合がある。 ### 2.2 証明情報の公開 本CAは、CRL、本CPおよびCPSをリポジトリ上に公開し、証明書利用者および検証者がオンラインによって閲覧できるようにする。 ### 2.3 公開の時期または頻度 本CPおよびCPSは、改訂の都度、リポジトリ上に公開する。 本CAは、24時間ごとに新たなCRLを発行し、リポジトリ上に公開する。また、証明書の失効が行われた場合、即時に新たなCRLを発行し、リポジトリ上に公開する。 また、証明書の有効期間を過ぎたものはCRLから削除する。 ### 2.4 リポジトリへのアクセス管理 本CAは、リポジトリでの公開情報に関して、特段のアクセスコントロールは行わない。証明書利用者は、本CAのCRLを、リポジトリを通じて入手することを可能とする。リポジトリへのアクセスは、一般的なWebインターフェースを通じて可能とする。 ## 3. 識別と認証 ### 3.1 名前決定 #### 3.1.1 名前の種類	

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（整形版）	備考
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シリーズの識別名規定に従い設定する。 **3.1.2 名前が意味を持つことの必要性** 本CAが発行する証明書中に用いられるコモンネームの有用性は、証明書利用者が本CA が発行する証明書をインストールする予定のサーバーのDNS内で使われるホスト名とする。 **3.1.3 証明書利用者の匿名性または仮名性** 本CAが発行する証明書のコモンネームには、匿名や仮名での登録は行わないものとする。 **3.1.4 様々な名前形式を解釈するための規則** 様々な名前の形式を解釈する規則は、X.500シリーズの識別名規定に従う。 **3.1.5 名前の一意性** 本CAが発行する証明書に記載される識別名(DN)の属性は、発行対象となるサーバーに対して一意なものとする。 **3.1.6 認識、認証および商標の役割** 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、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失効をする権利を有する。 **3.2 初回の本人確認** **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有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。 **3.2.2 組織の認証** 本CAは、国や地方公共団体が発行する公的書類、国や地方公共団体のWebページもしくはそのデータベース、または本CAが信頼する第三者による調査もしくはそのデータベースを用いて組織の実在性確認を行う。 **3.2.3 個人の認証** 本CAは、国や地方公共団体が発行する公的書類、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、証明書の申込を行う者が証明書利用者もしくはその代理人であることについて、本人性の確認および申込の意思確認を行う。 **3.2.4 検証されない証明書利用者の情報** 規定しない。	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シリーズの識別名規定に従い設定する。 **3.1.2 名前が意味を持つことの必要性** 本CAが発行する証明書中に用いられるコモンネームの有用性は、証明書利用者が本CA が発行する証明書をインストールする予定のサーバーのDNS内で使われるホスト名とする。 **3.1.3 証明書利用者の匿名性または仮名性** 本CAが発行する証明書のコモンネームには、匿名や仮名での登録は行わないものとする。 **3.1.4 様々な名前形式を解釈するための規則** 様々な名前の形式を解釈する規則は、X.500シリーズの識別名規定に従う。 **3.1.5 名前の一意性** 本CAが発行する証明書に記載される識別名(DN)の属性は、発行対象となるサーバーに対して一意なものとする。 **3.1.6 認識、認証および商標の役割** 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、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失効をする権利を有する。 **3.2 初回の本人確認** **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有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。 **3.2.2 組織の認証** 本CAは、国や地方公共団体が発行する公的書類、国や地方公共団体のWebページもしくはそのデータベース、または本CAが信頼する第三者による調査もしくはそのデータベースを用いて組織の実在性確認を行う。 **3.2.3 個人の認証** 本CAは、国や地方公共団体が発行する公的書類、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、証明書の申込を行う者が証明書利用者もしくはその代理人であることについて、本人性の確認および申込の意思確認を行う。 **3.2.4 検証されない証明書利用者の情報** 規定しない。	

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（整形版）	備考
### 3.2.5 権限の正当性確認 本CAは、証明書の申込を行う者が、その申請を行うための正当な権限を有していることを、本CP「3.2.2. 組織の認証」または「3.2.3 個人の認証」で利用する書類やデータベース等で確認できる連絡先に連絡することによって確認する。 ### 3.2.6 相互運用の基準 本CAは、セコムトラストシステムズが運営する認証局であるSecurity Communication RootCA2より、片方向相互認証証明書を発行されている。 ### 3.2.7 ドメイン名の認証 本CAは、次のいずれかの方法により、証明書利用者にそのドメイン名の利用権があることを確認する。 1. 証明書利用者が証明書のドメイン名の登録者であることを、レジストリもしくはレジストラへの問い合わせ、またはWHOISによって確認する。 2. ドメイン名登録者が証明書利用者と異なる場合は、証明書利用者が本CAに提出する、ドメイン名登録者から利用許諾を得ていることが確認できる書類によって確認する。 ## 3.3 鍵更新申請時の本人性確認と認証 鍵更新時における証明書利用者の本人性確認および認証は、「3.2 初回の本人確認」と同様とする。 ## 3.4 失効申請時の本人性確認と認証 本CAは、証明書発行申請時に証明書利用者からの申請を取り次いだ指定事業者を経由して、証明書利用者からの失効申請を受け付けることによって、証明書失効申請時の本人性確認を行う。 # 4. 証明書のライフサイクルに対する運用上の要件 ## 4.1 証明書申請 ### 4.1.1 証明書申請を提出することができる者 証明書の申請を行うことができる者は、日本国内に住所を有する個人、または日本国内に本店・主たる事務所、支店・支所、営業所その他これに準じる常設の場所を有する法人格を有しまたは法人格を有さない組織とする。 ### 4.1.2 登録手続および責任 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、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。	### 3.2.5 権限の正当性確認 本CAは、証明書の申込を行う者が、その申請を行うための正当な権限を有していることを、本CP「3.2.2. 組織の認証」または「3.2.3 個人の認証」で利用する書類やデータベース等で確認できる連絡先に連絡することによって確認する。 ### 3.2.6 相互運用の基準 本CAは、セコムトラストシステムズが運営する認証局であるSecurity Communication RootCA2より、片方向相互認証証明書を発行されている。 ### 3.2.7 ドメイン名の認証 本CAは、次のいずれかの方法により、証明書利用者にそのドメイン名の利用権があることを確認する。 1. 証明書利用者が証明書のドメイン名の登録者であることを、レジストリもしくはレジストラへの問い合わせ、またはWHOISによって確認する。 2. ドメイン名登録者が証明書利用者と異なる場合は、証明書利用者が本CAに提出する、ドメイン名登録者から利用許諾を得ていることが確認できる書類によって確認する。 ## 3.3 鍵更新申請時の本人性確認と認証 鍵更新時における証明書利用者の本人性確認および認証は、「3.2 初回の本人確認」と同様とする。 ## 3.4 失効申請時の本人性確認と認証 本CAは、証明書発行申請時に証明書利用者からの申請を取り次いだ指定事業者を経由して、証明書利用者からの失効申請を受け付けることによって、証明書失効申請時の本人性確認を行う。 # 4. 証明書のライフサイクルに対する運用上の要件 ## 4.1 証明書申請 ### 4.1.1 証明書申請を提出することができる者 証明書の申請を行うことができる者は、日本国内に住所を有する個人、または日本国内に本店・主たる事務所、支店・支所、営業所その他これに準じる常設の場所を有する法人格を有しまたは法人格を有さない組織とする。 ### 4.1.2 登録手続および責任 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、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。	

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（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 初回の本人確認」に記載の情報をもって、申請情報の審査を行う。~~本CAは、申請情報の審査時にCAAレコードを確認しない。~~ **4.2.2 証明書申請の承認または却下** 本CAは、審査の結果、承認を行った申請について証明書の発行登録を行う。 不備がある申請については、申請を却下し、申請を行った者に対し申請の再提出を依頼する。 **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、RFC6844に従い、申請情報の審査時にCAAレコードを確認する。CAAレコードに記載する本CAのドメインは「jprs.jp」とする。 **4.3 証明書の発行** **4.3.1 証明書発行時の処理手続** 本CAは、証明書申請の審査を完了した後、申請された情報に基づき証明書を発行する。 **4.3.2 証明書利用者への証明書発行通知** 本CAは、指定事業者または証明書利用者に対し電子メールを送付することにより証明書の発行通知を行う。 **4.4 証明書の受領確認** **4.4.1 証明書の受領確認手続** 証明書利用者が、証明書利用者だけがアクセス可能なホームページから証明書をダウンロードするか、あるいは他の方法によって証明書利用者が送付された証明書をサーバーに導入した時点をもって、証明書が受領されたものとする。 **4.4.2 認証局による証明書の公開** 本CAは、証明書利用者の証明書の公開は行わない **4.4.3 他のエンティティに対する認証局の証明書発行通知** 本CAは、第三者（ただし指定事業者は除く）に対する証明書の発行通知は行わない。 **4.5 鍵ペアおよび証明書の用途**	**4.2 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 初回の本人確認」に記載の情報をもって、申請情報の審査を行う。 **4.2.2 証明書申請の承認または却下** 本CAは、審査の結果、承認を行った申請について証明書の発行登録を行う。 不備がある申請については、申請を却下し、申請を行った者に対し申請の再提出を依頼する。 **4.2.3 証明書申請の処理時間** 本CAは、承認を行った申請について、適時証明書の発行登録を行う。 **4.2.4 CAA レコードの確認** 本CAは、RFC6844に従い、申請情報の審査時にCAAレコードを確認する。CAAレコードに記載する本CAのドメインは「jprs.jp」とする。 **4.3 証明書の発行** **4.3.1 証明書発行時の処理手続** 本CAは、証明書申請の審査を完了した後、申請された情報に基づき証明書を発行する。 **4.3.2 証明書利用者への証明書発行通知** 本CAは、指定事業者または証明書利用者に対し電子メールを送付することにより証明書の発行通知を行う。 **4.4 証明書の受領確認** **4.4.1 証明書の受領確認手続** 証明書利用者が、証明書利用者だけがアクセス可能なホームページから証明書をダウンロードするか、あるいは他の方法によって証明書利用者が送付された証明書をサーバーに導入した時点をもって、証明書が受領されたものとする。 **4.4.2 認証局による証明書の公開** 本CAは、証明書利用者の証明書の公開は行わない **4.4.3 他のエンティティに対する認証局の証明書発行通知** 本CAは、第三者（ただし指定事業者は除く）に対する証明書の発行通知は行わない。 **4.5 鍵ペアおよび証明書の用途**	CAA レコードの確認を行う旨を追記

JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（変更履歴付き）	JPRSサーバー証明書（組織認証型）認証局証明書ポリシー （Certificate Policy）（整形版）	備考
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。 【後略】	**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。 【後略】	