株式会社日本レジストリサービス（JPRS）

JPRSサーバー証明書（ドメイン認証型）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（ドメイン認証型）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 （ドメイン認証型） 認証局証明書ポリシー （Certificate Policy） Version ~~1.10~~1.20 2017年~~02月19日~~04月26日 株式会社日本レジストリサービス	# JPRSサーバー証明書 （ドメイン認証型） 認証局証明書ポリシー （Certificate Policy） Version 1.20 2017年04月26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（ドメイン認証型）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（ドメイン認証型）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 ・「7.1 証明書のプロファイル」の修正
1.20	2017.04.26	・「3.2.7 ドメイン名の認証」の修正

【中略】

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。

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 ・「7.1 証明書のプロファイル」の修正
1.20	2017.04.26	・「3.2.7 ドメイン名の認証」の修正

【中略】

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。

JPRSサーバー証明書（ドメイン認証型）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（ドメイン認証型）認証局証明書ポリシー （Certificate Policy）（整形版）	備考
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、組織の実在性を確認しない。 **3.2.3 個人の認証** 本CAは、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。 **3.2.5 権限の正当性確認** 本CAは、証明書を発行した時点において、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。 **3.2.6 相互運用の基準** 本CAは、セコムトラストシステムズが運営する認証局であるSecurity Communication RootCA2より、片方向相互認証証明書を発行されている。 **3.2.7 ドメイン名の認証** 本CAは、次のいずれかの方法により、証明書利用者にそのドメイン名の利用権があることを確認する。 1. 証明書利用者が証明書のドメイン名の登録者であることを、レジストリもしくはレジストラへ問い合わせることによって、またはWHOISに登録されたメールアドレスにメールを送信することによって確認する。 2. 証明書利用者にそのドメイン名の利用権があることを、管理者を表す一般的な電子メールアドレス（「admin@example.jp」、「hostmaster@example.jp」など。example.jp は証明書のドメイン名を表す）へメールを送信することによって確認する。 3. 証明書利用者にそのドメイン名の利用権があることを、証明書利用者が、そのドメイン名を含む URIにより識別されるWebページの情報を変更することによって確認する。 ~~3~~4. その他、合理的な手段を講じて、証明書利用者にそのドメイン名の利用権があることを確認する。	**3.2 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、組織の実在性を確認しない。 **3.2.3 個人の認証** 本CAは、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。 **3.2.5 権限の正当性確認** 本CAは、証明書を発行した時点において、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。 **3.2.6 相互運用の基準** 本CAは、セコムトラストシステムズが運営する認証局であるSecurity Communication RootCA2より、片方向相互認証証明書を発行されている。 **3.2.7 ドメイン名の認証** 本CAは、次のいずれかの方法により、証明書利用者にそのドメイン名の利用権があることを確認する。 1. 証明書利用者が証明書のドメイン名の登録者であることを、レジストリもしくはレジストラへ問い合わせることによって、またはWHOISに登録されたメールアドレスにメールを送信することによって確認する。 2. 証明書利用者にそのドメイン名の利用権があることを、管理者を表す一般的な電子メールアドレス（「admin@example.jp」、「hostmaster@example.jp」など。example.jp は証明書のドメイン名を表す）へメールを送信することによって確認する。 3. 証明書利用者にそのドメイン名の利用権があることを、証明書利用者が、そのドメイン名を含む URIにより識別されるWebページの情報を変更することによって確認する。 4. その他、合理的な手段を講じて、証明書利用者にそのドメイン名の利用権があることを確認する。	ファイル認証を追加することに伴う修正

JPRSサーバー証明書（ドメイン認証型）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（ドメイン認証型）認証局証明書ポリシー （Certificate Policy）（整形版）	備考
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。 【後略】	**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。 【後略】	