

# ファーストサーバ BIZCERT 認証局運用規程(CPS)



作成日: 2004/02/04

最終改訂日: 2005/06/24

バージョン:1.3

Copyright © 2005 by Firstserver, Inc.

本書類のいかなる部分の複製または配布も、その形式もしくは手段を問わず、またデータベースもしくは検索システムに保存してあるかを問わず、ファーストサーバ株式会社の事前書面許可がない限り行えません。

本書に掲載されている他の商標は各所有者の財産です。

**改訂履歴**

| バージョン | 日付         | 変更内容                         |
|-------|------------|------------------------------|
| 1.0   | 2004.06.14 |                              |
| 1.1   | 2004.09.01 | 発行済証明書およびCRLの利用者に影響の少ない軽微な変更 |
| 1.2   | 2005.04.14 | 発行済証明書およびCRLの利用者に影響の少ない軽微な変更 |
| 1.3   | 2005.06.24 | 発行済証明書およびCRLの利用者に影響の少ない軽微な変更 |
|       |            |                              |
|       |            |                              |
|       |            |                              |
|       |            |                              |
|       |            |                              |
|       |            |                              |
|       |            |                              |
|       |            |                              |
|       |            |                              |
|       |            |                              |
|       |            |                              |
|       |            |                              |
|       |            |                              |

# 目次

|       |                      |    |
|-------|----------------------|----|
| 1     | はじめに                 | 5  |
| 1.1   | 概要                   | 5  |
| 1.2   | 正式名称                 | 5  |
| 1.3   | 運営体制と適用範囲            | 5  |
| 1.3.1 | 認証局(CA)              | 5  |
| 1.3.2 | 登録局 (RAs)            | 6  |
| 1.3.3 | リポジトリ                | 6  |
| 1.3.4 | 申請者                  | 6  |
| 1.3.5 | 依拠利用者                | 6  |
| 1.3.6 | 適用性                  | 6  |
| 1.4   | 連絡先                  | 6  |
| 2     | 一般条項                 | 8  |
| 2.1   | 義務                   | 8  |
| 2.1.1 | CAの義務                | 8  |
| 2.1.2 | 申請者の義務               | 9  |
| 2.1.3 | 依拠利用者の義務             | 10 |
| 2.1.4 | リポジトリ提供義務            | 10 |
| 2.2   | 責任                   | 10 |
| 2.2.1 | 要件                   | 10 |
| 2.2.2 | 保証および義務の排除           | 10 |
| 2.2.3 | 責任限定                 | 11 |
| 2.2.4 | 賠償額の上限               | 11 |
| 2.2.5 | その他の条件               | 11 |
| 2.3   | 財務上の責任               | 11 |
| 2.3.1 | 信認関係                 | 11 |
| 2.3.2 | 申請者、依拠利用者による補償       | 11 |
| 2.4   | 解釈および強制執行            | 12 |
| 2.4.1 | 準拠法                  | 12 |
| 2.4.2 | 可分性、存続条項、合併、通知       | 12 |
| 2.4.3 | 紛争解決手続               | 12 |
| 2.5   | 料金                   | 12 |
| 2.6   | 開示およびリポジトリ           | 12 |
| 2.7   | 遵守監査                 | 12 |
| 2.7.1 | 遵守監査の頻度              | 12 |
| 2.7.2 | 遵守監査人の要件             | 13 |
| 2.7.3 | 遵守監査人の監査対象当事者との関係    | 13 |
| 2.7.4 | 遵守監査の対象となる事項         | 13 |
| 2.7.5 | 不備の結果として取られる処置       | 13 |
| 2.7.6 | 結果の連絡                | 13 |
| 2.8   | 情報の機密性               | 14 |
| 2.8.1 | 機密とはみなさない種類の情報       | 14 |
| 2.8.2 | 機密とみなす種類の情報          | 14 |
| 2.8.3 | サーバ証明書失効             | 14 |
| 2.8.4 | 法執行官への開示             | 14 |
| 2.8.5 | 民事訴訟の情報開示手続の一環としての開示 | 14 |

|       |                             |    |
|-------|-----------------------------|----|
| 2.8.6 | 所有者の要請による開示 .....           | 15 |
| 2.9   | 知的財産権 .....                 | 15 |
| 3     | 本人性確認および本人認証 .....          | 16 |
| 3.1   | 初回登録 .....                  | 16 |
| 3.1.1 | 識別名における名前の種類 .....          | 16 |
| 3.1.2 | 名前が意味を持つことの必要性 .....        | 16 |
| 3.1.3 | 識別名の一意性 .....               | 16 |
| 3.1.4 | 名前関連紛争解決手続 .....            | 17 |
| 3.1.5 | 商標の認識、本人認証および役割 .....       | 17 |
| 3.1.6 | 団体の本人性認証 .....              | 17 |
| 3.1.7 | 個人の本人性認証 .....              | 17 |
| 3.1.8 | デバイスおよびアプリケーションの本人性認証 ..... | 17 |
| 3.2   | 鍵更新の為の本人認証手続 .....          | 17 |
| 3.3   | 失効後の鍵更新用の本人認証 .....         | 18 |
| 3.4   | 失効申請の本人認証 .....             | 18 |
| 3.5   | サーバ証明書更新のための認証 .....        | 18 |
| 4     | 運用上の要件 .....                | 19 |
| 4.1   | サーバ証明書申請 .....              | 19 |
| 4.1.1 | サーバ証明書の申請 .....             | 19 |
| 4.1.2 | 相互認証証明書の申請 .....            | 19 |
| 4.2   | サーバ証明書発行 .....              | 19 |
| 4.3   | サーバ証明書の受領 .....             | 19 |
| 4.4   | サーバ証明書の一時失効および失効 .....      | 19 |
| 4.4.1 | 失効時の状況 .....                | 19 |
| 4.4.2 | 失効申請を行える者 .....             | 19 |
| 4.4.3 | 失効申請の手続 .....               | 20 |
| 4.4.4 | 失効申請猶予期間 .....              | 20 |
| 4.4.5 | 一時失効 .....                  | 20 |
| 4.4.6 | CRL 発行頻度 .....              | 20 |
| 4.4.7 | CRL 確認要件 .....              | 20 |
| 4.4.8 | オンライン失効状態確認 .....           | 20 |
| 4.5   | システム・セキュリティ監査手続 .....       | 20 |
| 4.5.1 | 記録の対象となるイベント .....          | 21 |
| 4.5.2 | データ処理の頻度 .....              | 22 |
| 4.5.3 | セキュリティ監査データの保管期間 .....      | 22 |
| 4.5.4 | セキュリティ監査データの保護 .....        | 22 |
| 4.5.5 | セキュリティ監査データバックアップ手順 .....   | 23 |
| 4.5.6 | セキュリティ監査情報収集システム .....      | 23 |
| 4.5.7 | イベントの原因となった対象への通知 .....     | 23 |
| 4.5.8 | 脆弱性評価 .....                 | 23 |
| 4.6   | 記録の保管 .....                 | 23 |
| 4.6.1 | 記録されるイベントの種類 .....          | 23 |
| 4.6.2 | アーカイブ保持期間 .....             | 23 |
| 4.6.3 | アーカイブの保護 .....              | 23 |
| 4.6.4 | アーカイブのバックアップ手続 .....        | 24 |
| 4.6.5 | アーカイブ情報の取得および検証手続 .....     | 24 |
| 4.7   | 鍵の切り替え .....                | 24 |

|       |                                 |    |
|-------|---------------------------------|----|
| 4.7.1 | CA 鍵の切り替え .....                 | 24 |
| 4.7.2 | サーバ証明書鍵の切り替え.....               | 24 |
| 4.8   | 危殆化および災害時復旧 .....               | 24 |
| 4.8.1 | コンピュータ、資源、ソフトウェア、データの破壊.....    | 24 |
| 4.8.2 | CA 秘密鍵の危殆化 .....                | 24 |
| 4.8.3 | 申請者秘密鍵の危殆化.....                 | 25 |
| 4.8.4 | 災害時における事業継続性.....               | 25 |
| 4.9   | CA の終了 .....                    | 25 |
| 5     | 物理面、手続面および人事面でのセキュリティ .....     | 26 |
| 5.1   | 物理的管理 .....                     | 26 |
| 5.1.1 | サイトの立地、構造および物理的アクセス .....       | 26 |
| 5.2   | 手続的な管理.....                     | 27 |
| 5.2.1 | 信用される役割.....                    | 27 |
| 5.2.2 | 職務毎に必要とされる人数.....               | 27 |
| 5.2.3 | 各役割の本人性確認と本人認証 .....            | 27 |
| 5.3   | 人事的セキュリティ管理 .....               | 28 |
| 5.3.1 | 経歴、資格、経験および身分証明の要件.....         | 28 |
| 5.3.2 | 経歴確認手続 .....                    | 28 |
| 5.3.3 | 訓練要件.....                       | 28 |
| 5.3.4 | 再訓練の頻度と要件 .....                 | 29 |
| 5.3.5 | 異動の頻度 .....                     | 29 |
| 5.3.6 | 不正行為に対する懲罰.....                 | 29 |
| 5.3.7 | 委託業者.....                       | 29 |
| 5.3.8 | 要員に提供する書類 .....                 | 29 |
| 6     | 技術的セキュリティ管理.....                | 30 |
| 6.1   | 鍵ペアの生成とインストール .....             | 30 |
| 6.1.1 | 鍵ペアの生成 .....                    | 30 |
| 6.1.2 | 鍵長と暗号方式.....                    | 30 |
| 6.1.3 | ハードウェアまたはソフトウェア鍵の生成 .....       | 30 |
| 6.1.4 | 本認証局への公開鍵の送付.....               | 30 |
| 6.1.5 | 申請者への CA 公開鍵の送付 .....           | 30 |
| 6.1.6 | 鍵使用目的.....                      | 30 |
| 6.2   | 秘密鍵の保護.....                     | 31 |
| 6.2.1 | クリプト・モジュールの標準 .....             | 31 |
| 6.2.2 | 秘密鍵複数人管理 .....                  | 31 |
| 6.2.3 | 秘密鍵預託.....                      | 31 |
| 6.2.4 | 秘密鍵のバックアップ.....                 | 31 |
| 6.2.5 | 秘密鍵アーカイブ .....                  | 31 |
| 6.2.6 | 秘密鍵の破棄 .....                    | 31 |
| 6.3   | その他の鍵ペア管理について .....             | 31 |
| 6.3.1 | 公開鍵の保管 .....                    | 31 |
| 6.3.2 | 鍵の使用期間 .....                    | 31 |
| 6.4   | コンピュータセキュリティ管理.....             | 32 |
| 6.4.1 | 特定のコンピュータのセキュリティに関する技術的要件 ..... | 32 |
| 6.5   | ライフサイクルの技術上の管理.....             | 32 |
| 6.5.1 | システム開発管理 .....                  | 32 |
| 6.5.2 | セキュリティ運用管理.....                 | 32 |
| 6.6   | ネットワークセキュリティ管理.....             | 32 |

|       |                                |    |
|-------|--------------------------------|----|
| 6.7   | 暗号モジュール技術の管理.....              | 33 |
| 7     | 証明書および証明書失効リストのプロファイル .....    | 34 |
| 7.1   | 証明書プロファイル.....                 | 34 |
| 7.1.1 | バージョン番号.....                   | 34 |
| 7.1.2 | アルゴリズムオブジェクト ID .....          | 34 |
| 7.1.3 | 証明書拡張.....                     | 34 |
| 7.2   | 証明書失効リストのプロファイル.....           | 35 |
| 7.2.1 | バージョン番号.....                   | 35 |
| 7.2.2 | 証明書失効リスト及び証明書失効リストエントリ拡張 ..... | 36 |
| 8     | 仕様管理 .....                     | 37 |
| 8.1   | 仕様変更手続.....                    | 37 |
| 8.2   | ポリシー変更手続 .....                 | 37 |
| 8.2.1 | コメント期間.....                    | 38 |
| 8.3   | 開示および通知手続.....                 | 38 |
| 8.4   | 変更の適性および受諾 .....               | 38 |
| 8.5   | CPS 認可手続 .....                 | 38 |
|       | 略語.....                        | 39 |
|       | 用語集.....                       | 40 |

# 1 はじめに

## 1.1 概要

ファーストサーバ BIZCERT 認証局運用規程(以下 本 CPS)は、インターネットサーバ用デジタル証明書(以下、サーバ証明書)および鍵の署名と発行におけるファーストサーバ BIZCERT 認証局(以下 本認証局)の運用と手続を定めるものです。本 CPS は、RSA KEON ROOT SIGNING SERVICE 証明書ポリシー(以下 KRSS CP)に適合したものです。

[http://www.rsasecurity.com/products/keon/repository/practices/Certificate\\_Policy.pdf](http://www.rsasecurity.com/products/keon/repository/practices/Certificate_Policy.pdf)

本 CPS は、インターネット X.509 公開鍵基盤証明書ポリシーおよび認証局運用規程フレームワーク(別名 RFC 3647)に適合しています。本文書は 8 つの章で構成されています。第 1 章は本 CPS の概要を述べたものです。第 2 章は義務、責任、法務、監査、機密について取扱います。第 3 章は、本人性確認および本人認証を対象とします。第 4 章は運用上の要件を取扱い、これにはサーバ証明書の申請、失効、留保、監査、保管および危殆化が含まれます。第 5 章は物理的および手続的なセキュリティを取扱います。第 6 章は暗号鍵の要件について定めています。第 7 章は証明書、証明書失効リスト(CRL)の要件を定義しています。第 8 章は本 CPS の変更に関する手続を掲載しています。

KRSS CP は、サーバ証明書認証局を対象とした法律上、事業上、技術上の要件を記述したものです。本 CPS は、サーバ証明書の発行に際し、これらの要件を遵守する方法について記述するものです。本認証局の運用は大阪府大阪市で行われています。本認証局は、ファーストサーバ株式会社が提供するインターネット・レンタルサーバサービスにて運用しているインターネットサーバに対して、サーバ証明書を発行します。

本 CPS は、運用の概要についてのみ定めています。運用手順の詳細については、別途書類に記述します。

## 1.2 正式名称

本 CPS は KRSS CP に適合しています。

本 CPS のオブジェクト識別子(以下 OID)は、**0.2.440.200188.109.1.1** です。

KRSS CP の OID は 1.2.840.113549.5.6.1 です。

## 1.3 運営体制と適用範囲

本認証局は、RSA セキュリティ株式会社との RSA KEON ROOT SIGNING SERVICE 契約に基づき、ファーストサーバ株式会社が提供するインターネット・レンタルサーバサービスで提供しているインターネットサーバに対して、サーバ証明書に署名の上、発行します。

### 1.3.1 認証局(CA)

KRSS CP の規定に基づき、申請者および秘密鍵を結びつけるサーバ証明書に対し、本認証局は署名を行います。本認証局は以下の作業を実施します。

- 申請者と結びつけたサーバ証明書に対し、CA 署名鍵を用いて署名の上発行すること

- 公開リポジトリにおける CRL 掲載によるサーバ証明書状態の公表
- 本 CPS および KRSS CP の遵守

### 1.3.2 登録局 (RAs)

本認証局に関連した別途の登録局(RA)はありません。証明書発行申請および失効申請の本人性確認や本人認証は、本認証局が行います。

### 1.3.3 リポジトリ

本認証局は CRL リポジトリを備え、依拠利用者による CRL 情報閲覧のために公開します。

### 1.3.4 申請者

本 CPS における申請者とは、特記のない限り、下記二項のいずれか、もしくは両方を指すものとします。どちらに該当するかは、下記二者間の契約等により規定するものとします。

#### 1.3.4.1 申請者

本 CPS の目的上、申請者とは、サーバ証明書の発行を受ける予定、もしくは発行を受けた団体・個人をいいます。

サーバ証明書取得のための申請者資格の有無は、本認証局の判断によるものとします。

なお、団体によるサーバ証明書取得申請の場合、団体を代表して、取得申請の責任者となる正式な権限のある者を申請責任者といいます。権限を有する者とは、申請団体に属する管理職（課長職相当以上）または役員を指します。個人によるサーバ証明書取得申請の場合、その個人本人を申請責任者といいます。

#### 1.3.4.2 申請代行者

申請代行者とは、申請者との特定の契約関係により本 CPS における申請者の義務の一部の遂行を受託し、これを行う者をいいます。尚、ファーストサーバ株式会社（本認証局を除く部門）がこれに該当する場合があります。

### 1.3.5 依拠利用者

依拠利用者とは、本認証局が発行したサーバ証明書またはサーバ証明書関連情報に依拠する組織または個人の全てをいいます。

### 1.3.6 適用性

本 CPS は本認証局が発行した全てのサーバ証明書に適用されます。本 CPS に記述された運用は、申請者のサーバ証明書の発行、使用、失効および依拠利用者に対し適用されます。

#### 1.3.6.1 承認および禁止事項

本認証局は、ファーストサーバ株式会社が提供するインターネット・レンタルサーバサービスを使用している団体・個人に対してのみサーバ証明書を発行します。

## 1.4 連絡先

本 CPS に関する連絡窓口は以下の通りです。

|           |                                     |
|-----------|-------------------------------------|
| 氏名        | ファーストサーバ株式会社 BIZCERT 認証局            |
| 郵便番号      | 541-0052                            |
| 住所        | 大阪府大阪市中央区安土町 1-8-15<br>野村不動産大阪ビル 3F |
| 電話番号      | 06-6261-3332                        |
| ファックス番号   | 06-6261-0051                        |
| 電子メールアドレス | cps@fsv.jp                          |

## 2 一般条項

### 2.1 義務

#### 2.1.1 CA の義務

本認証局は、本 CPS、KRSS CP、該当法（第 2.4.1 章）に従い、サーバ証明書を発行・管理します。本認証局は以下を実施します。

- 本 CPS の発行と管理
- 本 CPS 第 3.1.6 項および第 3.1.7 項に従って申請者の本人性確認および本人認証を行ったサーバ証明書の発行
- 本 CPS 第 4.4 項に従って適切な署名がなされた失効申請を受領し、検証が完了したサーバ証明書の失効
- 本認証局の機密性と完全性を保護するための安全な環境と適切な運用の提供
- KRSS CP の規則を遵守するための仕組みと手続の設定
- 遵守監査を通じた KRSS CP 遵守状況の立証
- ファーストサーバの WEB サイト上での本 CPS の公開

公開鍵基盤にかかる業務を行う本認証局の要員は、其々が行う業務に関する担当者責任を明確化しています。「担当者責任の明確化」とは、特定担当者の行った業務に関し当該担当者が処理すべき業務であったことが特定、説明、且つ、証明できる書面等が本 CPS 第 5.2.3 項に沿って作成保管されることをいいます。

##### 2.1.1.1 サーバ証明書の発行と失効の通知

本認証局は、本 CPS 第 4.2 項および第 4.4 項に従って、申請者または依頼利用者に対してサーバ証明書および CRL 情報を提供します。申請代行者（サーバ管理者）が管理するインターネットサーバの識別名（DN）をもつサーバ証明書を発行した場合、本認証局は当該代行者に対し通知を行います。また申請代行者は、申請者に対しその通知を受けたことを連絡する義務を負いません。

申請者からの失効申請を受けてサーバ証明書を失効した場合、本認証局から失効申請書の指定連絡窓口へ電子メールで通知します。

証明書発行通知および失効通知の送付から 7 営業日を経過しても申請者および申請代行者から本認証局へ異議等の申し出が無かった場合、証明書発行通知および失効連絡が受領されたものとみなし、それぞれの内容に関して確認したものとみなします。

##### 2.1.1.2 表明の正確さ

本認証局がサーバ証明書を公開する場合、本認証局は申請者に対してサーバ証明書を発行した事実、およびサーバ証明書に記載された情報が KRSS CP および本 CPS 第 3 章および第 4 章に従って検証されている旨を証明します。サーバ証明書の申請を受領し、発行したことにより、表明の正確さを立証したことの通知となります。

### 2.1.1.3 サーバ証明書の申請と発行の間の期間

サーバ証明書申請受領時と、サーバ証明書署名時の間の期間については、何の定めもありません。

### 2.1.1.4 サーバ証明書の失効と更新

サーバ証明書の失効と更新の手続は、KRSS CP の該当条項および本 CPS 第 4.4 項に沿って行います。

本認証局は、本 CPS の第 4.4.4 項および第 4.4.6 項が定める期限内に、CRL によりサーバ証明書の失効を公開します。CRL の公開場所は、サーバ証明書に記載しています。

### 2.1.1.5 秘密鍵の保護

本 CPS 第 4 章および第 6 章に従い、本認証局の秘密鍵はハードウェア・セキュリティ・モジュール(以下、HSM)のスマートカードによる「M of N」管理により、権限を有する複数の担当で保護します。

### 2.1.1.6 CA の秘密鍵使用に対する制限

本認証局は、サーバ証明書および CRL の署名に限定して CA 秘密鍵を使用します。

## 2.1.2 申請者の義務

申請者は、本認証局が申請者のサーバ証明書に署名の上、発行するに先立ち、証明書申請者約款および本 CPS の内容を理解し、その条件に同意の上で証明書の申請等をするものとします。申請者及び申請代行者は以下を表明するものとします。

- 本 CPS に規定の申請者の責任と義務を含む全ての使用条件（証明書申請者約款）を受諾し、合意していること
- ハードウェアまたはソフトウェアを使用して適切な鍵ペアを生成すること、また、その秘密鍵を適切かつ確実にインターネットサーバへインストールすること
- 使用する秘密鍵が本認証局以外の組織または個人との通信で使用されていないこと
- 本 CPS 第 3.1.6 項および第 3.1.7 項に従い、サーバ証明書申請時には、本認証局へ完全かつ正確な情報を提供すること
- 秘密鍵を危殆化から保護するため、パスワード保護（利用可能な場合）、HSM / 暗号アクセラレータ、その他の合理的な保護手段を用いるなどして、最善の努力を払うこと
- 申請者のサーバ証明書の掲載情報に何らかの変更があった場合、または申請者のサーバ証明書の内容が誤解を招いたり不正確となるような事情変更があった場合、実務上合理的に可能な限り速やかに本認証局に対して通知すること
- 申請者のサーバ証明書の期間満了時もしくは失効時、またはサーバ証明書の秘密鍵が危殆化した場合やその疑いが発生した場合、申請者はサーバ証明書の使用を直ちに停止し、かつ当該サーバ証明書および関連する秘密鍵をインストールしていたデバイスやソフトウェアから取り除くこと
- サーバ証明書が失効もしくは（サーバ証明書更新完了後に）期間満了となった場合、当該サーバ証明書に関連する秘密鍵およびそのコピーの全てを確実に破棄すること
- 本認証局から証明書発行通知を受諾した際、速やかに申請者のサーバへ証明書をインストールすること

- 本認証局から証明書発行通知を受託したこと、および申請者のサーバへ証明書をインストールしたことを、申請者に通知すること
- KRSS CP、本 CPS および証明書申請者約款を遵守すること

### 2.1.3 依拠利用者の義務

依拠利用者の権利と義務については本 CPS およびこれに関連する依拠利用者契約にて規定します。依拠利用者は以下のことを守るものとします。

- X.509 に明記されたサーバ証明書パス検証手続に従い、重要な拡張項目を考慮の上、CRL の使用を含めて、本認証局が発行したサーバ証明書を検証すること
- 本認証局の発行するサーバ証明書を信頼し使用するにあたり、当該サーバ証明書が期間満了も失効もしていないこと、本認証局が権限を失効していないこと、かつ、信頼できるルート認証局（RSA Keon Root Signing CA）との適切な信頼関係が確立されていることについて検証すること
- 本 CPS および関連する依拠利用者契約（ともにリポジトリ <http://ca.fsv.jp/repository/>に公開）の全ての条項と条件を通読しかつこれらに合意すること

### 2.1.4 リポジトリ提供義務

本認証局はリポジトリを提供し、以下を実施します。

- 本 CPS の条件に従い、本認証局が発行したサーバ証明書の失効情報を利用可能な状態で提供すること
- 本 CPS を申請者および依拠利用者に公開すること

## 2.2 責任

### 2.2.1 要件

本認証局は、サーバ証明書発行サービスおよびリポジトリ・サービスの運営、サーバ証明書の失効および CRL の発行を本 CPS に従って行います。

本人認証および確認手続は本 CPS 第 3 章に従って実行します。

### 2.2.2 保証および義務の排除

本認証局は、サーバ証明書の発行と管理に関連する契約（証明書申請者約款やその他の契約など）に定めがある場合を除き、何らの責任も負いません。

本認証局は、本認証局が発行したサーバ証明書から生ずるか、サーバ証明書に何らかの関連をもつ本認証局の責に帰さない付随的損害、派生的損害、特別損害、間接損害または懲罰的損害、事業利益の損失、または、データの損失、損傷もしくは破壊に対し、たとえ本認証局がこれら損害等の可能性についてあらかじめ知らされていた場合であっても、いかなる場合も何人に対しても何らの責任を負わないものとします。本条は、その訴えが債務不履行、不法行為（過失を含む）、保証違反またはその他に拠るものであるかどうかを問わず適用します。

関連契約に規定がある場合を除き、KRSS CP の条項は、何人に対しても、他人に代わり行動したり、拘束したり、義務や責任を創出もしくは引き受けたり、または何らかの表明を行う権限を与えるものではありません。KRSS CP に従ったサーバ証明書の発行をもって、本認証局が、申請者、一般顧客または依拠利用者の代理人、パートナー、ジョイントベンチャー先、受託者、信

託者等の代理人的な立場に置かれるものではありません。本認証局と申請者との関係は、適用される契約によって定義します。

### 2.2.3 責任限定

本認証局が発行したサーバ証明書のうち、以下に列挙するようなサーバ証明書の誤使用、依拠により発生する損害、または、これらに関連する損害について、本認証局は、いかなる場合も、申請者、依拠利用者、その他何人に対しても責任を負いません。

- 失効または期間満了となったサーバ証明書
- 不正な目的に使用されたサーバ証明書
- 改竄されたサーバ証明書
- 危殆化したサーバ証明書
- 不実表明、誤解を招く作為もしくは不作為を含むサーバ証明書

### 2.2.4 賠償額の上限

本件サービスの利用に関し、本認証局が本 CPS に規定された責任を果たさなかった事により申請者に対し賠償又は補償の責任を負う場合の賠償または補償の額は、いかなる場合であっても、申請者から受領した本件サービス料の額を越えないものとします。

### 2.2.5 その他の条件

本 CPS 第 2.2.2 項および第 2.2.3 項の責任の排除および限定に関し、本認証局が締結した契約上、異なる定めがある場合は、当該契約条件に従います。責任の排除および限定は、KRSS CP および顧客が署名した契約に沿ったものとします。

## 2.3 財務上の責任

本認証局は、CA 秘密鍵の危殆化等事業継続に影響する重要な事項に対し、適切な水準の保険を付保します。

### 2.3.1 信認関係

本認証局は、申請者の信託人、代理人、受託者、またはその他申請者を代表する者のいずれでもなく、本認証局と申請者との関係は代理人と本人の関係ではありません。本認証局は、明示暗示にかかわらず、また、外見上の表示の有無にかかわらず、前述と異なる趣旨の表明は行いません。申請者は、契約、合意その他を根拠として、本認証局に対し、何らの義務を課する権限を持つものではありません。

### 2.3.2 申請者、依拠利用者による補償

申請者、依拠利用者は、KRSS CPまたは本CPS、証明書申請者約款、依拠利用者契約に別途の定めがない限り、サーバ証明書の使用もしくは発行および以下に列挙するような場合に生じた請求、訴訟、要求から本認証局を防禦し、当該請求等にかかる一切の費用について補償することに合意します。

- 申請者による事実の虚偽表明または誤解を招く表明があった場合
- 申請者の怠慢によるか、または詐欺やごまかしを目的として、要件事実を開示しなかった場合

- 申請者が自己の秘密鍵、パスワードもしくは PIN（該当する場合）の保護を怠った場合、または秘密鍵の危殆化、開示、紛失、修正もしくは不正使用を防ぐ為に必要な措置を講じることを怠った場合
- 申請者が自己の秘密鍵の危殆化、開示、紛失、修正もしくは不正使用について認知したか、推定できたにもかかわらず、当該事態につき本認証局に対して速やかに通知することを怠った場合

## 2.4 解釈および強制執行

### 2.4.1 準拠法

本認証局の運営及びサーバ証明書に関連し生じる紛争の解決においては、日本国の法令を準拠法とします。

#### 2.4.1.1 法律取締上の入室許可および情報提供

法律に基づく要請を受けた場合、本認証局は法執行官に対し、あらゆる施設への入室許可および全ての情報提供を行うものとします。

### 2.4.2 可分性、存続条項、合併、通知

本認証局は、関連契約において可分性、存続条項、合併または通知に関する適切な条項を定めるものとします。

### 2.4.3 紛争解決手続

本認証局とそれ以外の組織または個人との間に生じる、鍵および証明書管理に関連する紛争は、双方の協議によりこれを解決するものとします。

協議により解決できない紛争は、大阪地方裁判所に提起されるものとします。

## 2.5 料金

料金請求は適切な権限と方針に従って行います。申請者に対して請求する料金は、サーバ証明書申請受付時点以前に公開するものとします。

## 2.6 開示およびリポジトリ

本認証局は以下を実施します。

- リポジトリを通した CRL の公開
- リポジトリを通した本 CPS の公開

## 2.7 遵守監査

遵守監査により、本認証局が KRSS CP および本 CPS の規定する通り運営されていることの第三者証明を得ます。本認証局は自己費用負担で KRSS CP の遵守を示すため遵守監査を実行します。

### 2.7.1 遵守監査の頻度

遵守監査は、CA 証明書（PKCS #7 証明書）署名処理の実行から 6 ヶ月以内に行い、それ以降は RSA KEON ROOT SIGNING SERVICE 利用契約の一環として、12 ヶ月毎に行います。

## 2.7.2 遵守監査人の要件

遵守監査人は、遵守監査分野における能力をもち、RSA KEON ROOT SIGNING SERVICE が全てのサーバ証明書の発行と管理に対して課す要件と本認証局がそのサーバ証明書の発行と管理に対して課す諸要件とを熟知している必要があります。遵守監査人は当該遵守監査業務を主たる任務として行っていることを必要とします。

遵守監査人は本認証局からは独立しており、かつ、社会的に認知された監査会社に所属する監査人であることの証明を有している者とします。

## 2.7.3 遵守監査人の監査対象当事者との関係

RSA KEON ROOT SIGNING SERVICE と本認証局の双方に対して、偏見のない中立的な評価と認証が行えるよう、遵守監査人は監査対象の組織からは独立した民間会社であるか、または当該組織とは組織上十分に分離している者とします。遵守監査人がこの要件を満たしているかの判定は RSA KEON ROOT SIGNING SERVICE が行います。

## 2.7.4 遵守監査の対象となる事項

年次遵守監査の目的は、KRSS CP および本 CPS の要件に従う組織が当該要件を満たしていることの検証にあります。遵守監査は以下を含む全ての要件をその対象とします。

- CA 事業実務の開示
- サービスの完全性（鍵とサーバ証明書のライフサイクルの管理を含む）
- CA 環境管理

## 2.7.5 不備の結果として取られる処置

本認証局の設計、運用または維持の実態と、本 CPS ならびに KRSS CP の規定が異なると遵守監査人が判定した場合、その遵守の不備の程度に応じて以下の処置を取ります。

- 当該不備が軽微な場合、遵守監査人は遵守監査報告書の一部として当該不備について注記します。
- 当該不備が監査不合格とするべき重大なものであった場合は、遵守監査人は速やかに本認証局の責任者と面談するものとします。責任者は当該不備の是正方法を決定するものとし、かつ当該是正手段が遵守監査の承認に値するものかどうかについて遵守監査人と協議するものとし、是正手段の明確な実行日程を伴う対策案と当該不備、是正手段および最終結果の詳細を記した最終報告書が必要となります。遵守監査人の最終的な判断は拘束力を持つものとし、もし当該不備が依然として深刻なものであると遵守監査人が判定した場合、遵守監査は不合格となります。
- 本認証局が KRSS CP を遵守していないと遵守監査人が判断した場合、RSA KEON ROOT SIGNING SERVICE は、当該遵守不履行状態の深刻度に応じて、自己の裁量により本認証局の証明書を失効させることがあります。

## 2.7.6 結果の連絡

遵守監査人は遵守監査報告書を作成します。遵守監査報告書は、年次遵守監査合格の確認書として、RSA KEON ROOT SIGNING SERVICE に対して提示します。是正措置を含む監査報告書は全て本認証局の専有財産とし、機密情報として保護します。

## 2.8 情報の機密性

本項では、本認証局および申請者間の情報に適用される機密保持義務を設定します。本認証局は、保有する機密情報を保護します。

### 2.8.1 機密とはみなさない種類の情報

サーバ証明書およびCRL、ならびにこれらに掲載され公開ディレクトリに収納されている申請者情報は、機密情報とみなしません。また、以下のいずれかに該当する情報についても機密情報とはみなしません。

- 受領側当事者が開示側当事者の機密情報を不正に参照または利用することなく、受領側当事者が独自に作成したことを証明できる情報
- 受領側当事者が開示側当事者以外の情報源から制約を負うことなく合法的に受領した情報
- 受領側当事者の不正行為や不作為によることなく、現在公知である情報または将来において公知となる情報
- 開示の時点で制約を負うことなく受領側当事者が知っていたことを受領側当事者が書類により証明できる情報
- 開示制約を負った情報ではないことを開示側当事者が書面で合意した情報

### 2.8.2 機密とみなす種類の情報

本認証局が保有する全ての組織情報（登録および失効情報、記録イベント、申請者と本認証局間の通信記録など）および個人情報機密とみなし、法律に基づく要請を受けた場合を除き、申請者の事前同意がない限り開示しません。

監査情報およびレビュー情報は機密とみなし、監査を目的とする場合または法律に基づく要請を受けた場合を除き、理由の如何を問わずいかなる者に対しても開示しません。

本認証局は、サーバ証明書の申請者の秘密鍵を入手する手段を持ちません。申請者本人のみが各々の秘密鍵を保有すべきであり、その秘密鍵は機密として保護しなければなりません。申請者の行ういかなる開示も申請者自身のリスクにおいて行うものとします。

### 2.8.3 サーバ証明書失効

本認証局は、本 CPS の手続に従ってサーバ証明書失効に関する情報の取得、保有および公開を行います。本情報の提供は CRL の公開により行います。

### 2.8.4 法執行官への開示

本認証局は、法令、裁判所命令、もしくは他の行政権限に基づく要請がない限り、いかなる法執行官または取締機関に対しても機密情報を開示しません。情報を開示する場合も、プライバシー関連法および社内ポリシーに従って行います。

### 2.8.5 民事訴訟の情報開示手続の一環としての開示

本認証局は、民事訴訟手続の情報開示要件に応じて機密情報を第三者に対して開示します。但し、当該開示は、必要な範囲に限定して行います。機密情報の開示要請は、署名の上、本認証局に送付されるものとします。

### **2.8.6 所有者の要請による開示**

本認証局 が保有する機密情報は、申請者の事前書面同意があれば第三者に対して開示することができます。情報を開示する場合も、プライバシー関連法および社内ポリシーに基づき開示するものとします。

## **2.9 知的財産権**

秘密鍵は、サーバ証明書にて特定される公開鍵の正当な保有者に属する専有財産とします。

本認証局は、発行したサーバ証明書および失効情報に含まれるか、関連しているあらゆる知的財産権を保有します。

## 3 本人性確認および本人認証

### 3.1 初回登録

#### 3.1.1 識別名における名前の種類

申請者は、PKIX Part1 標準に従い、一意性を備えた X.501 識別名(DN)をサーバ証明書のサブジェクト欄に備えるものとします。申請者は PKIX Part1 標準に従い、SubjectAlternateName 拡張欄を使って代替名も利用できます。DN の形式は X.501 印刷可能ストリング、IA5 ストリングまたは UTF8 名とし、かつ空白のままとすることはできないものとします。

サーバ証明書のサブジェクト名は、X.501 識別名(DN)形式に従います。本認証局は単独命名方式を使用します。サーバ証明書には以下の情報を含むものとします。

##### 団体を対象としたサーバ証明書

- 「組織名」(O)：申請団体の法的名称を反映した英文。
- 「組織部署名」(OU)：このフィールドはオプションです。OU フィールドは、同一組織内の異なる部署を区別するために使用するものです。(例：人事部、マーケティング部および開発部間の区別)通常はサーバ証明書では利用しません。
- 「住所」(L/S/C)：申請団体もしくは申請団体部署(OU)が所在する都道府県名および市区町村名。日本国内の住所でなければなりません。
- 「コモンネーム」(CN)：サーバ証明書をインストールするファーストサーバ株式会社が提供するインターネットサーバで使用されているか、World Wide Web の DNS に登録されている完全修飾ドメイン名です。申請者は完全修飾ドメイン名の一部を構成するドメイン名の使用権を証明する必要があります。

##### 個人を対象としたサーバ証明書

- 「組織名」(O)：申請者個人の法的名称。
- 「組織部署名」(OU)：申請者個人が営む事業の屋号・商号など。
- 「住所」(L/S/C)：申請者個人が所在する都道府県名および市区町村名。日本国内の住所でなければなりません。
- 「コモンネーム」(CN)：サーバ証明書をインストールするファーストサーバ株式会社が提供するインターネットサーバで使用されているか、World Wide Web の DNS に登録されている完全修飾ドメイン名です。申請者は完全修飾ドメイン名の一部を構成するドメイン名の使用権を証明する必要があります。

#### 3.1.2 名前が意味を持つことの必要性

各サーバ証明書のサブジェクト名のフィールドの内容は、当該申請者の認証済の名称と関連性を持っています。相対識別名(RDN)は、団体によるサーバ証明書取得申請の場合は当該組織の法的名称を反映し、個人によるサーバ証明書取得申請の場合は申請者自身の法的名称を反映します。

#### 3.1.3 識別名の一意性

DNは、全申請者について一意性を備えたものとします。

### 3.1.4 名前関連紛争解決手続

本認証局は、発行するサーバ証明書全ての名前に関し全ての意思決定を行う権利を留保します。申請者は、特定の名前を利用できる自己の権利を証明する必要があります。

### 3.1.5 商標の認識、本人認証および役割

商標の使用は、登録商標の保有者にその留保権が与えられます。

### 3.1.6 団体の本人性認証

団体によるサーバ証明書申請は、正式な権限のある者（申請責任者）により行います。申請を行う場合、申請団体情報、申請責任者情報、事務連絡担当者情報、技術担当者情報を提供する必要があります。本認証局は、申請の正当性を確保するため、第三者データベースの情報を用いて、本人面談や電話面談など帯域外の方法を使用して申請責任者の在籍確認および申請意思確認を行います。

第三者データベースにて審査に必要な情報が確認できない場合、以下の情報が必要になる場合があります。

- ・ 正規の窓口担当者の証明と検証手段
- ・ 会社設立の証明
- ・ 正当な資格を有することの証明（六士<sup>1</sup>の事務所に対する証明書の場合）

<sup>1</sup> 六士・・・ 弁護士、公認会計士、税理士、弁理士、司法書士、行政書士

本認証局は、発行済サーバ証明書の有効期間にわたり、審査に使用した情報の写し1部を保管します。

### 3.1.7 個人の本人性認証

個人によるサーバ証明書申請は、その個人本人のみ行えます。申請を行う場合、申請者情報、事務連絡担当者情報、技術担当者情報を提供する必要があります。本認証局は、申請の正当性を確保するため、申請者の実在性確認および申請意思確認を帯域外の方法を使用して行います。

また、審査に必要な他の情報の提出を別途求める場合があります。

本認証局は、発行済サーバ証明書の有効期間にわたり、審査に使用した情報の写し1部を保管します。

### 3.1.8 デバイスおよびアプリケーションの本人性認証

本認証局は、デバイスまたはアプリケーションに対して証明書を発行しません。

## 3.2 鍵更新の為の本人認証手続き

鍵更新の申請は正式な権限のある者により行います。鍵更新に関する全ての申請の認証は本認証局が行い、それに伴い発生した対応については申請者が証明します。鍵更新申請の認証は初回登録時と同じ方法で行います。なお、正式な権限のある者とは、団体によるサーバ証明書取得申請

の場合、申請団体に属する管理職（課長職相当以上）または役員を指し、個人によるサーバ証明書取得申請の場合、その個人本人を指します。

### 3.3 失効後の鍵更新用の本人認証

サーバ証明書に含まれる情報に変更があるか、秘密鍵の危殆化またはその疑いある場合、本認証局は初回登録時と同じ方法で鍵更新の本人認証を行うものとします。本認証局は、サーバ証明書に含まれる情報の変更について、当該サーバ証明書発行前にその検証を行います。

本 CPS または証明書申請者約款の遵守を怠った結果、申請者のサーバ証明書が失効した場合、本認証局はサーバ証明書再発行に先立ち、当該非遵守の理由が本認証局にとって納得のいく形で説明されていることを検証します。

失効したサーバ証明書（CRL に掲載されたサーバ証明書）は鍵更新を受けることができません。本認証局は申請者の名前、日付、時刻および取られた措置等の全ての申請記録を保管します。

### 3.4 失効申請の本人認証

申請者がそのサーバ証明書の失効を要請する場合は、正式な権限がある者が失効申請を行うものとします。失効申請は、権限者の署名を伴った書面により行うものとし、署名を備えた電子的書類とすることもできます。本認証局は、権限者と電話連絡を取るなどして失効申請の検証を行い、権限者の本人性確認と申請の信憑性を確認するものとします。申請、申請確認および取られた措置の詳細を記した記録は本認証局にて保管します。なお、正式な権限のある者とは、団体によるサーバ証明書取得申請の場合、申請団体に属する管理職（課長職相当以上）または役員を指し、個人によるサーバ証明書取得申請の場合、その個人本人を指します。

### 3.5 サーバ証明書更新のための認証

本認証局は、鍵更新を伴わないサーバ証明書更新は行いません。

## 4 運用上の要件

### 4.1 サーバ証明書申請

サーバ証明書申請に関する手順と要件は本 CPS に記載される通りです。サーバ証明書を申請しても、本認証局はサーバ証明書発行の義務を負うものではありません。

申請者は、登録用 WEB ページを経由して PKCS#10 証明書申請を提出するものとします。

全てのサーバ証明書申請は、本人性確認および本人認証に関する第 3.1.6 項および第 3.1.7 項を遵守するものとします。

#### 4.1.1 サーバ証明書の申請

申請者がサーバ証明書の申請を行うものとします。申請は第 3.1.6 項ないし第 3.1.8 項の要件に従い、さらに証明書申請者約款の要件を満たすものとします。

#### 4.1.2 相互認証証明書の申請

本認証局は、外部 CA に対し相互証明を行いません。

### 4.2 サーバ証明書発行

本認証局によるサーバ証明書の発行は、本認証局がサーバ証明書の申請を完全に且つ最終的に承認したことを意味します。

### 4.3 サーバ証明書の受領

証明書発行通知の送付から 7 営業日を経過しても申請者および申請代行者から本認証局へ異議等の申し出が無かった場合、サーバ証明書が受領されたものとみなします。なお、申請代行者はサーバ証明書の受領後、申請者へ速やかに当該事実を通知するものとします。

### 4.4 サーバ証明書の一時失効および失効

#### 4.4.1 失効時の状況

サーバ証明書は以下のいずれかに該当する場合、失効します。

- サーバ証明書の内容に変更があったか、その疑いがある時
- 秘密鍵において危殆化の疑いがあるか、現実に危殆化があったことが確認された時
- 秘密鍵収納媒体において危殆化の疑いがあるか、現実に危殆化があったことが確認された時
- 申請者が本 CPS、KRSS CP、その他の契約または適用可能な法規の遵守を怠った時
- 契約終了時
- 本認証局が失効させる必要があると判断した時

#### 4.4.2 失効申請を行える者

本認証局は正式な権限のある者からのみ本認証局外からのサーバ証明書の失効申請を受け付けます。なお、正式な権限のある者とは、団体へ発行されたサーバ証明書失効申請の場合、申請団体に属する管理職（課長職相当以上）または役員を指し、個人へ発行されたサーバ証明書失効申請の場合、その個人本人を指します。

#### 4.4.3 失効申請の手続

サーバ証明書の失効申請には、第 4.4.2 項の要件を満たした者による本認証局への書面申請が必要となります。サーバ証明書の失効を行う前に、その申請内容を検証します。

本認証局は失効申請にかかる全ての記録を保管するものとし、これには申請者の氏名、連絡手段、失効理由、日付と時刻が含まれます。

サーバ証明書が失効された場合、当該失効は CRL で公開されます。

#### 4.4.4 失効申請猶予期間

失効申請の結果取られる措置は、失効申請受領後 7 営業日以内に開始します。

#### 4.4.5 一時失効

本認証局はサーバ証明書の一時失効の措置は行いません。

#### 4.4.6 CRL 発行頻度

本認証局は最新 CRL を 24 時間毎に発行します。サーバ証明書が失効した場合、本認証局は最新 CRL を第 4.4.4 項の要件の通り発行します。本認証局は、最新 CRL に依拠利用者がアクセスできるように、WEB サーバで CRL を公開します。

##### 4.4.6.1 緊急時の CRL 発行

鍵危殆化などの緊急事態で直ちにサーバ証明書を失効させる必要があり、尚且つ失効した事実を早急に CRL にて公開する必要があると本認証局が判断した場合、本認証局は CRL 発行を手作業で行います。

#### 4.4.7 CRL 確認要件

サーバ証明書の使用に先立ち、依拠利用者は、現行の CRL に照らして、サーバ証明書の有効状態を確認しなければなりません。依拠利用者は、CRL の信憑性および完全性の検証も行う必要があります。依拠利用者の他の義務については本 CPS の第 2.1.4 項を参照してください。

#### 4.4.8 オンライン失効状態確認

本認証局は、サーバ証明書のオンライン失効状態（OCSP）確認は提供しません。

### 4.5 システム・セキュリティ監査手続

本認証局におけるセキュリティに関連するあらゆるイベントに関し、監査ログが生成されます。可能な場合は、セキュリティログの収集は自動的に行います。それ以外の場合は、台帳、紙方式または他の物理的な仕組みを用います。電子のおよび非電子的な全てのセキュリティ監査ログは少なくとも月に 1 回の頻度で保管され、遵守監査の目的または法的根拠に基づく開示要請があった場合に提供します。本条で定義された監査対象となるイベントのセキュリティ監査ログは、本 CPS 第 4.6.2 項「アーカイブ保持期間」に従って保管します。

## 4.5.1 記録の対象となるイベント

アクセス、各種変更、鍵およびサーバ証明書の生成、更新を含む全セキュリティ関連イベント、および、監査目的に必要なイベントの全てを記録します。イベントの種類は二つに分類されます。

- 建物、部屋および保管庫へのアクセス等の物理的なイベント
- オペレーティング・システムおよびCAサーバ運用等の論理的イベント

物理的なイベントは電子的な記録または台帳に記録します。ビデオ監視はセキュリティ要員が物理的に配備されていない場所などに使用します。

論理的イベントは、OSレベルおよびアプリケーションレベルで、自動的に監査ログに記録します。

### 4.5.1.1 物理的なイベント

物理的なイベントの場合、以下の記録を行うものとします。

- イベントの日付と時刻
- 団体/個人の特定
- 実施内容（例、コンソールアクセスを経由したログオン/ログアウトなど）
- イベントに関連する情報を提供する他の要件（不具合の場合、ディスク・ドライブの交換に関するコメントのこともある）

物理的なイベントとは以下のとおりです。

- 入退室
- 機器持出し・返却
- CAシステムアクセス

### 4.5.1.2 論理的イベント

論理的イベントは、オペレーティング・システムとCAシステムに分けられます。いずれのイベントも、以下の情報を監査記録の書式で記録します。

- イベントの種類（アプリケーション，システム・セキュリティ等）
- イベント発生の日時
- イベントの成功または失敗
- イベントの原因となったCAの構成要素、運用者の特定
- イベントに関する詳細（エラー情報やログイン・メッセージ・タイプ情報など）

監査情報は保管するものとし、可能であれば、監査ログは情報の完全性を維持するため署名します。本認証局における重大なセキュリティイベントは、自動的に日時を明記し、監査イベントとしてCA監査ファイルに記録します。

#### 4.5.1.2.1 オペレーティング・システム

ログイン作業は全てシステムログに記録します。管理者レベルのログは全てオペレーティング・システムのロギング機能またはアクセス管理アプリケーションにより適切に記録します。

#### 4.5.1.2.2 CA システム

本認証局は以下のイベントの実行記録を含む監査ログを生成します。

##### CA システム・イベント・ログ

- 鍵生成
- CRL の発行
- サーバ証明書の発行
- サーバ証明書の失効
- 新認証局の設立
- 認証局証明書のインポート
- 新管理者の設定
- 新審査者の設定
- 認証局証明書の更新

#### 4.5.1.3 情報の収集 / 整理

以下の各項目についての本認証局に関連する情報は自動または手動で回収、整理および報告します。

- システム構成の変更と保守
- 人事異動
- 逸脱および危殆化の報告
- ネットワーク・プロバイダおよびソフトウェア・サプライヤー等の認証局業務に関連する外部業者との連絡
- 鍵、活性化データ、または申請者情報を含む媒体の破棄

#### 4.5.2 データ処理の頻度

監査ログは月一回の頻度で検査します。重要なイベントは監査ログ要約で説明されます。ログの検査においては、まずログが外部から改竄を受けていないことの検証を行い、次に全ログエントリーの簡単な検査を行い、ログ中に注意を喚起するものや異常があれば、より綿密な調査を行います。検査の結果施した措置は書面化します。

#### 4.5.3 セキュリティ監査データの保管期間

監査ログは認証局事業所（サイト）で少なくとも 1 年間保持し、その保管は安全な方法で行います。

#### 4.5.4 セキュリティ監査データの保護

以下の要件を確保するため、CA システム構成と処置はあわせて実施します。

- 許可された者のみにログへの読取アクセスを与えること
- 許可された者のみが監査ログの保管または削除を行えること
- 監査ログが改変されていないこと

監査ログ保管を行う者は改変権を持ちません。また保管された監査データは、監査ログ保持期間満了前の削除または破棄から保護します。監査ログは、本認証局の主施設内の安全で確実な保存場所に移します。

#### 4.5.5 セキュリティ監査データバックアップ手順

監査ログのバックアップは、本認証局の運用手順書に従って行います。バックアップ監査データのセキュリティは、本 CPS 第 4.6 項「記録の保管」で取り扱います。また、監査ログの写し 1 部を定期的にオフサイトバックアップ施設に送付します。

#### 4.5.6 セキュリティ監査情報収集システム

監査ログの収集は、手動および自動の両方で行います。CA システムが保管および使用されている建物、部屋および保管室へのアクセスは監視します。

監査ログ収集システムは CA システムの一部です。監査ログ収集システムは CA システムの起動時に発動し、その停止は CA システムの停止したときに限定されます。監査ログシステムが停止している場合、CA システムの運用は行いません。

#### 4.5.7 イベントの原因となった対象への通知

本 CPS は、イベントの原因となった個人、組織、デバイスまたはアプリケーションに対して当該イベントが監査の対象となった旨の通知を行いません。

#### 4.5.8 脆弱性評価

監査ログに異常があった場合、本認証局はこれを受けて脆弱性評価を行います。

## 4.6 記録の保管

### 4.6.1 記録されるイベントの種類

本認証局のアーカイブ記録は、認証局の適切な運用、または、発行済サーバ証明書（失効済、期間満了を含みます）の効力を立証するために必要十分なものとしています。少なくとも以下のデータをアーカイブに記録します。

- 本認証局の証明書
- 本認証局の監査ログ
- 本認証局が発行したサーバ証明書
- 本認証局が発行した CRL、本 CPS

### 4.6.2 アーカイブ保持期間

アーカイブデータの最低保持期間は 7 年です。特定の顧客情報の処分は処分基準に従って行います。CA の運用および継続性に関連する監査情報およびその他の情報を保存します。

元の記録媒体に所定の期間データ保持ができない場合、アーカイブサイトにおいて、アーカイブデータを定期的に新たな媒体に移転する仕組みを定めます。アーカイブデータを処理するために必要なアプリケーションも、本認証局が必要と決定した期間維持します。

### 4.6.3 アーカイブの保護

無許可者によるアーカイブへの書込、修正または削除は認めません。アーカイブの内容は、本認証局がその開示を決定した場合、または、法律が義務づける場合を除き、開示を行いません。個

別取引の記録の開示は、取引に関与した申請者または法定代理人の要請があった場合に限り行います。

#### 4.6.4 アーカイブのバックアップ手続

監査データは、バックアップ手順に従ってバックアップの上、定期的にオフサイトバックアップ施設に送付します。サーバ証明書、CRL、鍵は、CA ホストシステムバックアップの一環としてバックアップします。バックアップ・カートリッジは主サイトおよびバックアップサイト双方で、耐火容器にて保存します。

#### 4.6.5 アーカイブ情報の取得および検証手続

本認証局のアーカイブ情報の取得と検証の詳細を記した手順は、「ファーストサーババックアップ/リカバリー手順」に記載します。

## 4.7 鍵の切り替え

### 4.7.1 CA 鍵の切り替え

本認証局の鍵の切り替えは、RSA KEON ROOT SIGNING SERVICE 契約に基づいて行います。期間満了等を理由に、CA 鍵の切り替えが新たに必要となった場合、本認証局は新しい鍵ペアを生成し、署名のため証明書を RSA KEON ROOT SIGNING SERVICE に提出します。古い CA 鍵ペアは本認証局から取り除き破棄します。本認証局は鍵切り替え期間を置き、この期間中に、以前使っていた CA 秘密鍵と公開証明書を段階的に廃止します。CA 秘密鍵は、秘密鍵の有効期間を上回る有効期間を備えたサーバ証明書の署名には使用しません。

### 4.7.2 サーバ証明書鍵の切り替え

申請者は、サーバ証明書が期間満了となるか危殆化が起きた場合には、新しく生成した鍵ペアを用いて、本認証局に対してサーバ証明書の発行を申請します。期間満了となるか、危殆化が起きた鍵ペアは、申請者がインターネットサーバから取り除き破棄するものとします。

本 CPS または証明書申請者約款の遵守を怠った結果としてサーバ証明書が失効とされた場合、本認証局はサーバ証明書再発行に先立ち、当該未遵守の理由が本認証局にとって納得のいく形で説明されていることを検証します。

## 4.8 危殆化および災害時復旧

### 4.8.1 コンピュータ、資源、ソフトウェア、データの破壊

本認証局は CA を構成するコンピュータおよびサービスを提供する為に必要な資源、ソフトウェア、データ等の破壊に備えるためにバックアップやリカバリーに関する手順書を定めています。

### 4.8.2 CA 秘密鍵の危殆化

本認証局の証明書に対応する秘密鍵が危殆化した場合、以下の措置を実施します。

- RSA KEON ROOT SIGNING SERVICE に対する、実務上可能な限り速やかな通知
- 全申請者に対する、実務上可能な限り速やかな通知
- ファーストサーバ CA 災害時復旧プランに基づく、実務上可能な限り速やかなサービスの復旧

- RSA KEON ROOT SIGNING SERVICE が決定した措置の実行

### 4.8.3 申請者秘密鍵の危殆化

本認証局が発行した証明書に対応する申請者の秘密鍵が危殆化した場合、申請者は本認証局に対して速やかに証明書の失効申請を行う必要があります。

### 4.8.4 災害時における事業継続性

本認証局は、CA 秘密鍵の危殆化および不慮の災害や事故等により重大な被害を被り、通常の業務を遂行する事が困難となるような状況に備え、迅速に必要な業務の再開を行えるよう復旧に関する規定を別途定める。また、重要度が高い下記業務に関しての業務継続性について、方針を示す。

- 証明書失効業務  
業務停止から 14 日以内に復旧
- 証明書発行業務  
業務停止から 60 日以内に復旧

## 4.9 CA の終了

本認証局がその業務を停止した場合、本認証局は申請者に対して速やかに通知を行い、CA 鍵とアーカイブ情報の継続的な保管を手配します。本認証局が発行したサーバ証明書は全て失効します。

# 5 物理面、手続面および人事面でのセキュリティ

## 5.1 物理的管理

主サイトおよびオフサイトにおける本認証局の運用開始に先立ち、以下の物理的セキュリティ管理を施しています。

### 5.1.1 サイトの立地、構造および物理的アクセス

本認証局のサイトの立地および構造は、設備の耐震構造等建物の災害に対する耐久性、物理的障壁による保護、権限のない人物による不正進入の防止、サイト内の監視体制等 KRSS が定めるセキュリティ要件を満たしています。

また、本認証局のサイトへの物理的アクセスは以下の要件を満たしています。

- 「赤外線モーションセンサーによる状態監視」「バイオメトリクス認証と ID/Password の 2 種類の要素認証による入退室制御」「監視カメラ（暗視対応）によるサイト内の状態監視および録画」にて管理されている
- 認証局責任者により本認証局のサイトに入室する事をあらかじめ認められた認証局員のリスト（以下、アクセスリスト）に掲載された要員による、複数人での入退室のみアクセスを許可する
- アクセスリストに掲載されていない者が入室する際は、アクセスリストに掲載された要員複数人が同伴し適切に監視する
- 機密性の高い平文情報を含む持出し可能な媒体および書面は鍵がかかるファイルキャビネットや鍵がかかる金庫等、物理的に安全な場所に保管する
- 証明書発行システムは、アクセスリストに掲載された要員にのみ配布される個人用証明書での認証を必須とする事により、管理されている

#### 5.1.1.1 電気および空調

本認証局のサイトは、地震・落雷等による停電への対策として大容量バックアップ電池(大型 CVCF 無停電電源装置)および CVCF 自家発電装置を設置しています。また、CA 設備安定稼働の為に空気の温度や湿度および空気の流れを一定に保つ為の、十分な空調を整えています。

#### 5.1.1.2 水対策

本認証局のサイトは、洪水による被害が及ばないよう洪水多発地域外のビル地上階に設置し、また漏水対策として漏水センサーを設置することにより、水害対策を行っています。

#### 5.1.1.3 火気対策

本認証局のサイトは、火災による設備や書類等の焼失を防ぐ為の消火設備を配置し、室温センサーを設置する事により火気被害対策を行っています。

#### 5.1.1.4 保存媒体の保護

本認証局の業務に関わる保存媒体は、鍵がかかるファイルキャビネットおよび耐火金庫に保管し、適切なアクセスコントロールを実施しています。

#### 5.1.1.5 廃棄物処理

本認証局の業務に関わる媒体の廃棄は適切に行います。機密書類や重要度の高い書類は処分に先立ち細断します。磁気媒体は処分に先立ち脱磁または細断します。

#### 5.1.1.6 オフサイトバックアップ施設

本認証局は、合理的なセキュリティレベルのオフサイトバックアップ施設を有します。

## 5.2 手続的な管理

### 5.2.1 信用される役割

#### 5.2.1.1 CA の信頼される役割

一人の者が察知されることなく悪意をもって CA 秘密鍵または CA システムを使用することを防ぐため、本認証局は重要な CA 機能については職務分割を義務付けます。各担当者によるシステムへのアクセスは、個々に割り当てられた責任を遂行する為に必要な処理をする場合に限定します。

以下に例示した特定の作業については職務分割および二名管理を施します。

- 新しい CA 鍵ペアの生成
- CA 秘密鍵および関連証明書の交換
- サーバ証明書プロファイルの変更

全ての担当者は、各自の作業について個々に説明責任を負います。これは物理的管理、システム的管理、およびポリシー管理を組み合わせることで実現します。

- 施設へのアクセスの制限 - 入退室時監視
- 管理者のシステムへのログインおよびログアウトの監査ログによる記録
- 管理者の CA へのログインおよびログアウトの監査ログによる記録
- サーバ証明書作成、失効等の監査ログによる記録（第 4.5.1 項参照のこと）
- 複数人管理を強制する技術的管理、ポリシー、手続き上の管理

### 5.2.2 職務毎に必要なとされる人数

本認証局は、明記された二名管理作業をいかなる者も単独では行えないよう、適切なセキュリティと手順を施します。

単独で作業をしている者が、CA 役割に関連する他の全ての業務を行うことがないよう、本認証局は、CA 担当者が行う全ての作業を監督できる検証手順を持つものとします。

### 5.2.3 各役割の本人性確認と本人認証

各役割の管理者について、本人性を確認し本人認証する為のセキュリティ手続を施します。

全ての CA 要員は、以下の手続が取られる前に、本人性確認と本人認証を受けます。

- CA サイトのアクセスリストへの掲載
- CA システムへの物理的アクセスのアクセスリストへの掲載
- 各自の CA 役割実行のための証明書の付与
- CA システム上でのアカウントの付与

証明書とアカウント（CA 署名証明書を除く）は以下の要件を満たします。

- 個人に直接帰属すること
- 他人と共有しないこと
- CA ソフトウェア、オペレーティング・システム、手続管理を通じて行う役割に対して権限を与えられた行為に制限すること

## 5.3 人事的セキュリティ管理

CA 運営関連任務を遂行する要員全員に対して、人事的セキュリティ管理を行います。

CA 運営関連任務を遂行する要員に対し、本認証局が課す義務は以下のとおりです。

- 担当任務への任命は書面で行われること
- 担当任務に課された諸条件の契約上または法令上の拘束を受けること
- 遂行業務に関する包括的な訓練を修了していること
- 機密性の高い CA セキュリティ関連情報または申請者情報を開示しない拘束を受けること
- 各自の CA 任務と抵触する原因となる可能性のある業務の割当を受けないこと

### 5.3.1 経歴、資格、経験および身分証明の要件

本認証局は、CA 運営関連任務を遂行する要員全員に対し、PKI の十分な資格と経験を備えることを義務付けます。すべての要員は組織の要員セキュリティ要件を満たすものとし、さらに CA 管理者は以下の要件を満たす必要があります。

- PKI の知識と訓練を備えていること
- セキュリティ訓練を受けていること
- 製品に特化した訓練を受けていること

### 5.3.2 経歴確認手続

経歴確認は、ファーストサーバ株式会社の標準社内ポリシーおよび手続に従って行います。

### 5.3.3 訓練要件

本認証局は、CA 運営関連任務を遂行する要員全員に対し、各自の役割と職責を対象とした十分な訓練を受けることを義務付けます。

### 5.3.4 再訓練の頻度と要件

CA システムの変更に対応するため、第 5.3.3 項の要件は常に最新状態にします。再訓練は必要に応じて行い、経営陣はこれらの要件を毎年一回見直します。

### 5.3.5 異動の頻度

人事異動があった場合、すべてのパスワードを変更するとともに、業務担当者用証明書の失効と再発行、ユーザーID の削除と再作成を行います。パスワードやアカウントの共有は行いません。

### 5.3.6 不正行為に対する懲罰

本認証局運営関連任務の担当者が不正行為を犯した場合、またはその疑いがある場合、直ちに当該担当者の CA システムへのアクセスを停止します。

本認証局は、申請者が本 CPS、証明書申請者約款またはその他適用可能な法規に定めた義務の履行を怠った場合、サーバ証明書を失効できるものとします。本認証局は、状況により鍵または証明書の危殆化につながるおそれがあるとの疑いを抱いた場合は、いつでも証明書の失効を行えるものとします。安全、事業、運営、データまたは顧客を危機に晒すような不正行為を犯す認証局要員があれば、本認証局はその裁量により、当該行為の結果の深刻度に応じて、停職、退去、または譴責の処分を行うことができるものとします。

### 5.3.7 委託業者

本認証局は、委託業者による CA 施設の入退室が第 5.1.1 項に従って行われるよう義務付けます。

### 5.3.8 要員に提供する書類

本認証局は、全ての CA 要員に対して、KRSS CP、本 CPS、その他各自の職位に関連する特定の手順、書類、約款を提供します。この中には、各種規定、運用手順書、証明書申請者約款、依頼利用者契約、災害時復旧プラン、および担当者がその任務を遂行するにあたって必要な他の書類を含みます。

## 6 技術的セキュリティ管理

### 6.1 鍵ペアの生成とインストール

#### 6.1.1 鍵ペアの生成

本認証局は、FIPS PUB 140-2 レベル 3 の評点が与えられた HSM を用いて鍵ペアの生成を行います。

#### 6.1.2 鍵長と暗号方式

本認証局は、1024 ビットの鍵長を備えた RSA 暗号鍵アルゴリズムを使用します。

インターネットサーバ上で生成される申請者鍵は、1024 ビットの鍵長を備えた RSA 暗号鍵アルゴリズムを使用するものとします。

#### 6.1.3 ハードウェアまたはソフトウェア鍵の生成

##### 6.1.3.1 申請者鍵の生成

申請者は、ソフトウェアまたはハードウェアによる鍵生成により、署名鍵ペアを生成します。ソフトウェアによる鍵ペア生成を行う場合、鍵ペア生成は、インターネットサーバ鍵生成ツール/アプリケーション（例：マイクロソフト証明書ウィザード、Apache ツール等）を使用するものとします。ハードウェアによる鍵生成を行う場合は（例：暗号アクセラレータ等）、アクセラレータは FIPS PUB 140-1 レベル 2 以上の評点を得たものとします。インターネットサーバ SSL 鍵ペアの生成は、可能な限り、サーバ証明書の対象となるインターネットサーバ上で行うものとします。

また、本認証局は申請者から受領した PKCS#10 証明書申請の電子署名を検証する事により、申請者が秘密鍵を所有している事を確認します。

#### 6.1.4 本認証局への公開鍵の送付

サーバ証明書に含むべき公開鍵は、本認証局が用意した申請用の登録サーバに安全な方法で送付します。（例：PKCS 10 ファイルの貼り付け）

#### 6.1.5 申請者への CA 公開鍵の送付

本認証局の公開鍵および関連する RSA Keon Root Signing CA に向けたルート証明チェーンは、サーバ証明書発行プロセスの過程で本認証局 WEB ページからダウンロードするものとします。RSA KEON ROOT SIGNING SERVICE は、ブラウザや Web サーバソフトウェアに標準装備されている ValiCert Class 3 ポリシー検証局により署名されています

#### 6.1.6 鍵使用目的

鍵の使用方法については、第 7.1.1.1 項（基本）および第 7.1.3 項（拡張）を参照してください。

CA 秘密鍵は、サーバ証明書と CRL の署名のみを目的として使用します。

## 6.2 秘密鍵の保護

### 6.2.1 クリプト・モジュールの標準

本認証局は CA の秘密鍵を保護するために、FIPS PUB140-2 レベル 3 で認証された HSM を使用します。申請者は、関連する秘密鍵の保存をソフトウェア（例：マイクロソフト・レジストリ）の中でも、インターネットサーバ SSL 暗号アクセラレータの中でも、いずれでも行えます。SSL アクセラレータを使用する場合は、FIPS PUB 140-1 レベル 2 以上の評点を獲得しているものとします。

### 6.2.2 秘密鍵複数人管理

本認証局の秘密鍵は「M of N」管理が可能な HSM により、権限を有する複数の担当者により管理します。

### 6.2.3 秘密鍵預託

署名秘密鍵については、第三者への預託を行いません。

### 6.2.4 秘密鍵のバックアップ

本認証局は、災害時復旧作業をサポートすべく、本認証局のサイトにおいて権限を有する複数の担当者により CA 秘密鍵のバックアップを暗号化した上で別媒体に保存し、鍵のかかる金庫に保管します。

### 6.2.5 秘密鍵アーカイブ

本認証局の秘密鍵のアーカイブは行いません。

### 6.2.6 秘密鍵の破棄

CA 秘密鍵が利用されなくなった場合、本認証局はそれらを全て破棄します。秘密鍵のコピーとその断片は、鍵ペアの有効期間満了時に破棄します。破棄された CA 秘密鍵に対応する公開鍵は、証明書の有効期間満了後には再配布を行いません。

申請者の秘密鍵に対するサーバ証明書が失効した場合、有効期間が満了したか DN 情報が変更したために使用されなくなった場合、もしくは危殆化した場合、全ての申請者は当該秘密鍵の全てのコピーを確実に破棄する義務を負います。これらの要件は、証明書申請者約款に記載します。

## 6.3 その他の鍵ペア管理について

### 6.3.1 公開鍵の保管

本認証局は、発行済みの全てのサーバ証明書の写しを保管するものとします。CA データベースのバックアップと保管は、CA 運用の一環として行います。

### 6.3.2 鍵の使用期間

本認証局の鍵の有効期間は、RSA セキュリティ社との RSA Keon ルート署名契約に定めたとおり 5 年とします。

本認証局は、1年の有効期間を伴ったサーバ証明書を発行します。申請者鍵使用期間は、証明書の残りの有効期間以下とします。

## 6.4 コンピュータセキュリティ管理

### 6.4.1 特定のコンピュータのセキュリティに関する技術的要件

本 CPS 第 5.1 項に記述する通り、本認証局が運用を行うコンピュータには、物理的な安全を確保します。本認証局は、オペレーティング・システム、CA アプリケーション・ソフトウェアが提供する以下の技術的な安全管理を備えます。

- CA サービスおよび PKI 役割へのアクセス管理（第 5.2.1 項参照）
- 要員の本人性確認および本人認証（第 5.2.3 項参照）
- 通信セッションおよびデータベースのセキュリティ確保のための暗号化、および、外部とのやりとりにおける相互認証および SSL 暗号化
- CA 履歴と監査データの保存（第 4.5 項および第 4.6 項参照）
- セキュリティ関連イベントの監査（第 4.5 項参照）
- PKI 役割および関連本人性確認のための高信頼パス、および、すべての管理者の X.509 証明書使用

## 6.5 ライフサイクルの技術上の管理

### 6.5.1 システム開発管理

RSA Keon 認証局製品は、X.509 公開鍵証明書等の公開鍵証明書の発行、失効および管理を行うコンポーネントの要件を定義する証明書発行・管理コンポーネント（CIMC）ファミリー保護プロファイルに従います。CIMC は Common Criteria/ISO IS15408 基準に準拠しています。  
(<http://csrc.nist.gov/cc/ccv20/ccv2list.htm>)。

### 6.5.2 セキュリティ運用管理

本認証局は、CA システムの導入と保守において適切な構成管理手続きを適用します。本認証局を構成する CA ソフトウェアは、起動時、システム上のソフトウェアが以下の項目を満たすことを検証するための仕組みを提供します。

- 正規の開発元から出荷されたソフトウェアであること
- 導入の前に変更されていないこと
- 使用予定のバージョンであること

導入時、および、必要に応じて、CA を運用する前に CA システムの完全性を検証します。

セキュリティポリシーと Keon CA セキュリティの設定は、年次セキュリティ監査の一環として少なくとも年 1 回検査します。検査結果は書面化します。鍵長を増やす必要があるか、必要な水準のシステム・セキュリティを維持するために運用手順を修正する必要があるかの判断を行うため、リスクおよび脅威度の評価を行います。

## 6.6 ネットワークセキュリティ管理

本認証局サーバの保護は、適切なネットワークセキュリティ管理により行います。ネットワークセキュリティ管理上、許可された者のみが CA サーバにアクセスできます。監査機能の実行と確認は頻繁に行うものとします。CA 環境への遠隔アクセスは、本人認証を伴う SSL セッションにより保護します。上記以外の遠隔アクセスは認めません。不要なサービスは全てその機能を停止します。構成は、ネットワーク上での Unix / NT ホストに設定されたファーストサーバ株式会社の標準を満たすものとします。

## 6.7 暗号モジュール技術の管理

鍵の生成、鍵の保存およびサーバ証明書の署名作業は、全て、FIPS PUB 140-2 レベル 3 の評点を得たハードウェア暗号モジュールの中で実行します。

# 7 証明書および証明書失効リストのプロファイル

## 7.1 証明書プロファイル

### 7.1.1 バージョン番号

本認証局は、本項の規定に従って X.509 バージョン 3 のサーバ証明書を発行します。

#### 7.1.1.1 基本証明書形式

基本証明書形式は、X.509 基準に適合しています。サポート対象となる基本証明書フィールドは以下の通りです。必要に応じて、追加拡張を行います。

| 証明書フィールド                                 | 内容   |
|--|--|
| バージョン<br>(Version)                       | 3  |
| シリアルナンバー<br>(Serial Number)              | 発行 CA が割当てた本証明書用の一意性を備えた本人性確認番号                  |
| 署名アルゴリズム<br>(Signature Algorithm)        | sha1WithRSAEncryption                            |
| 発行者<br>(Issuer)                          | 発行 CA の完全修飾ドメイン名(X.500)                          |
| 効力<br>(Validity)                         | サーバ証明書の開始および終了日時                                 |
| サブジェクト名<br>(Subject)                     | 本 CPS 第 3.1.1 項に従った対象インターネットサーバの完全修飾ドメイン名(X.500) |
| サブジェクト公開鍵情報<br>(Subject Public Key Info) | サブジェクトの公開鍵値、ならびに本公開鍵使用時に用いるアルゴリズムの識別子            |

### 7.1.2 アルゴリズムオブジェクト ID

署名および検証のために、本認証局は以下のアルゴリズムを使用します。

- PKCS#1 に従った RSA 1024
- FIPS PUB 180-1 および ANSI X9.30 part2. に従った SHA-1

### 7.1.3 証明書拡張

本認証局は、RFC 3280「インターネット X.509 公開鍵基盤証明書および CRL プロファイル」(2002 年 4 月付)に従ってバージョン 3 拡張を使用します。

本認証局は、以下のサーバ証明書拡張をサポートします。

| フィールド                                     | 内容                                      |
|---|---|
| 認証局鍵識別子<br>( Authority Key Identifier )   | 発行済サーバ証明書の署名に用いた秘密鍵に対応する、CA の公開鍵を識別する方法 |
| 鍵使用目的<br>( Key Usage )                    | 鍵暗号化、デジタル署名                             |
| 証明書ポリシー<br>( Certificate Policies )       | KRSS CP、OID、および本 CPS の公開先ポイントの識別        |
| CRL 配布ポイント<br>( CRL Distribution Points ) | 失効情報 ( CRL ) の公開先ポイント                   |
| Netscape 証明書タイプ<br>( Netscape Cert Type ) | SSL サーバ                                 |
| サブジェクト代替名<br>( Subject Alternative Name ) | URI 表示を行っているインターネットサーバ名                 |
| サブジェクト鍵識別子<br>( Subject Key Identifier )  | 特定の公開鍵を含むサーバ証明書を識別する方法                  |

## 7.2 証明書失効リストのプロファイル

### 7.2.1 バージョン番号

本認証局は、RFC 3280「インターネット X.509 公開鍵基盤証明書および CRL プロファイル」(2002 年 4 月付)に従って、X.509 バージョン 2 CRL を発行します。

## 7.2.2 証明書失効リスト及び証明書失効リストエントリ拡張

### 7.2.2.1 証明書失効リスト

本認証局は以下の CRL バージョン 2 をサポート、使用します。

| フィールド                             | 内容                         |
|-----------------------------------|----------------------------|
| バージョン<br>(Version)                | 2                          |
| 発行者<br>(Issuer)                   | 発行 CA の完全修飾ドメイン名(X.500)    |
| 署名アルゴリズム<br>(Signature Algorithm) | sha1WithRSAEncryption      |
| 有効開始日                             | CRL の発行日                   |
| 次回更新予定                            | 次回 CRL の更新予定日時             |
| 失効した証明書                           | 失効した証明書のリスト (シリアルナンバー・失効日) |

### 7.2.2.2 証明書失効リストエントリ拡張

本認証局は、以下のサーバ証明書失効リストエントリ拡張をサポート、使用します。

| フィールド   | 内容                                 |
|---------|------------------------------------|
| 認証局鍵識別子 | CRL の署名に用いた秘密鍵に対応する、CA の公開鍵を識別する方法 |
| CRL 番号  | 本認証局が発行した CRL の連番                  |

## 8 仕様管理

### 8.1 仕様変更手続

本認証局は、本 CPS 変更のレビューおよび承認の責任者を定めます。変更提案に対するコメントは書面にまとめ署名した上で本認証局に宛てて届けられるものとします。変更提案に関する決定は本認証局の独自の裁量により行います。

本 CPS の管理は本認証局が行います。本 CPS の窓口の詳細は以下の通りです。

|           |                                     |
|-----------|-------------------------------------|
| 氏名        | ファーストサーバ株式会社 BIZCERT 認証局            |
| 郵便番号      | 541-0052                            |
| 住所        | 大阪府大阪市中央区安土町 1-8-15<br>野村不動産大阪ビル 3F |
| 電話番号      | 06-6261-3332                        |
| ファックス番号   | 06-6261-0051                        |
| 電子メールアドレス | cps@fsv.jp                          |

### 8.2 ポリシー変更手続

本認証局は、随時本 CPS を変更できる権利を留保します。変更は将来においてのみ有効となり、過去に遡っての改訂は行いません。本認証局は、変更を新バージョンの CPS に盛り込み、リポジトリ・WEB サイト(<http://ca.fsv.jp/repository/>)にて公開します。新 CPS には新たなバージョン番号を付します。

本 CPS への変更のうち、発行済サーバ証明書および CRL のユーザには全く影響を及ぼさないか、または及ぶとしても極めて軽微なものに留まるものと本認証局が判断したものについては、WEB サイト上で新たな新 CPS が公開された時点で直ちに効力を発し、変更は全ての発行済サーバ証明書および CRL に適用します。

本 CPS への変更のうち、発行済サーバ証明書および CRL のユーザに重大な影響を及ぼす可能性があるものと本認証局が判断したものについては、一定のコメント期間中、WEB サイト(<http://ca.fsv.jp/repository/>)に掲示します。

本認証局は以下の行為を行います。

- 当該提案を本 CPS の新ドラフト版に盛り込むこと
- 変更提案で定める通り、当該ドラフトをファーストサーバ WEB サイト(<http://ca.fsv.jp/repository/>)に一定期間中掲示すること

新 CPS が発効する日時は、冒頭ページに表示します。本 CPS の最新の有効な写しは、従前のバージョン全てに優先するものとし、変更発効日後の発行済サーバ証明書の使用または依拠について、申請者、依拠利用者を拘束します。

### 8.2.1 コメント期間

発行済サーバ証明書、CRL に重大な影響を及ぼすと本認証局が判断する本 CPS への変更については、コメント期間を設定します。コメント期間は別途指定がない限り、30 日とします。

変更提案に対する書面に署名を付したコメントは、本認証局管理者または指定された他の CA 管理局に宛てて届けられるものとします。変更提案に関する決定は、本認証局の独自の判断によるものとします。

## 8.3 開示および通知手続

本書の電子コピーは、リポジトリから入手するか、第 1.4 項に記載される窓口に電子メールで申請して入手します。本 CPS の対外的な発表の場合は、非開示契約 (NDA) の署名を要します。

## 8.4 変更の適性および受諾

本認証局が新たな CPS の発行を正当化するためにポリシーまたは手順の変更を決定した場合、本認証局は新 CPS 用の新たな OID を割り当てます。

本 CPS の変更は全て、WEB サイト上のリポジトリで最終的な開示が行われた時から 30 日後に発効します。開示後 30 日以降に、本認証局が発行したサーバ証明書を使用または依拠した場合、サーバ証明書の発行日の如何に関わらず、変更された条件を受諾したものとみなします。

## 8.5 CPS 認可手続

本認証局の管理機構は、サーバ証明書発行に用いる本 CPS を認可する責任があります。

当該認可は RSA Keon Root Signing 契約に従って行います。本認証局は、本 CPS の修正、追加または削除の審査のためにその変更提案を RSA KEON ROOT SIGNING SERVICE に提出し、当該修正、追加または削除が容認できるものか、また、当該修正等が RSA KEON ROOT SIGNING SERVICE の運営やセキュリティを危険に晒すものでないことを判断します。

# 略語

| 略称    | 正式名称                                    | 日本語訳                |
|-------|---|---------------------|
| CA    | Certification Authority                 | 認証局                 |
| CP    | Certificate Policy                      | 証明書ポリシー             |
| CPS   | Certification Practice Statement        | 認証局運用規程             |
| CRL   | Certificate Revocation List             | 証明書失効リスト            |
| DN    | Distinguished Name                      | 識別名                 |
| DSA   | Digital Signature Algorithm             | デジタル署名アルゴリズム        |
| FIPS  | Federal Information Processing Standard | 連邦情報処理標準            |
| HSM   | Hardware Security Module                | ハードウェア・セキュリティ・モジュール |
| IETF  | Internet Engineering Task Force         | インターネット技術特別調査委員会    |
| ITU   | International Telecommunications Union  | 国際電気通信連合            |
| LDAP  | Lightweight Directory Access Protocol   | 軽量ディレクトリアクセスプロトコル   |
| OCSP  | On-line Certificate Status Protocol     | オンライン証明書状態プロトコル     |
| PIN   | Personal Identification Number          | 個人識別番号              |
| PKCS  | Public-Key Cryptography Standards       | 公開鍵暗号化標準            |
| PKIX  | Public Key Infrastructure X.509         | 公開鍵基盤 X.509         |
| RA    | Registration Authority                  | 登録局                 |
| RFC   | Request For Comment                     |                     |
| RKRSS | RSA KEON ROOT SIGNING SERVICE           | RSA KEON ルート署名サービス  |
| RSA   | Rivest-Shamir-Adleman                   |                     |
| SHA 1 | Secure Hash Algorithm                   | セキュアハッシュアルゴリズム      |
| SSL   | Secure Sockets Layer                    | セキュアソケットレイヤー        |
| URI   | Uniform Resource Identifier             | 統一資源識別子             |
| URL   | Uniform Resource Locator                | 統一資源位置指定子           |

# 用語集

A

B

C

D

E

F

## [FIPS 140-2]

IT 製品は「取扱注意だが機密扱いなし」の使用条件を満たすべきである、というアメリカ連邦政府の要件を記載した標準。

当該標準の公表は National Institute of Standards and Technology (NIST)が行ったもので、カナダ政府の Communication Security Establishment (CSE)もこれを既に採用しており、American National Standards Institute (ANSI)を通じて金融界も採用する予定である。標準には異なるレベル（1 から 4 まで）があり、レベル毎に異なるセキュリティが設定されている。高レベルでは、書面化要件も異なったものとなる。

## [FIPS 180-1]

メッセージまたはデータファイルの濃縮した表現を算出する、セキュアハッシュアルゴリズム「SHA-1」に関する規格。

G

H

I

## [IA5 スtring]

X.509 証明書において、コモンネーム（CN）等の名前を表すためのString形式。

J

K

L

M

## [M of N]

鍵暗号化処理の一つ。秘密鍵は N 個の単位に分割され、トークン等のハードウェアデバイスに保存される。M は 1 以上 N 以下である。つまり  $1 \leq M \leq N$  となる。M は、秘密鍵再構成時に必要となる単位である。

N

O

**P****[PKCS #1]**

RSA アルゴリズムに準拠した公開鍵暗号化実装のため規格。

**[PKCS #7 PEM エンコード証明書]**

デジタル署名やデジタル封筒など、暗号を伴う可能性があるデータ用の汎用構文を記述した規格。

**[PKCS #10]**

公開鍵、名前、場合によっては属性一式の証明を申請するための汎用構文を記述した規格。

**Q****R****[RFC]**

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 が正式に発行する文書。

**[RSA]**

Ronald L. Rivest, Adi Shamir, および Leonard M. Adleman.が開発した、高い安全性を備えた暗号化方式。RSA は二部構成の鍵を使用する。所有者は秘密鍵を保管し、公開鍵は公開される。受領者の公開鍵を使用して暗号化したデータは、受領者の秘密鍵がない限り復号化できない。その逆も同様である。

**S****[SSL サーバ証明書]**

SSL セッション（安全なチャネル）経由で接続を確立する際に WEB サーバまたはアプリケーション・サーバの本人認証の検証を行うための証明書。

**T****U****[URI]**

Universal Resource Indicator - インターネット上のアドレス。

**[UTF8]**

X.509 証明書においてコモンネーム（CN）などの名前を表すストリング形式。

**V****W**

**X****[X.500]**

当初は X.400 電子メールのためのサポートのために必要となったが、他のアプリケーションでも一般に使用されているディレクトリ・サービス仕様。

**[X501 印刷可能ストリング]**

X.509 証明書においてコモンネーム(CN) などの名前を示すストリング形式。

**[X.509]**

デジタル証明書の基本形式を記述した ISO 標準。

**[X.509 v3 証明書拡張]**

RSA Keon CA は、PKIX、S/MIME、および SSL 証明書のための拡張を含む、X.509 v3 証明書拡張をサポートする。これらの拡張は、RFC 3280「インターネット X.509 公開鍵基盤証明書および CRL プロファイル」(2002 年 4 月付)に記載される X.509 のバージョン 3 標準に適合し、証明書サブジェクトに対する追加の制約と機能を明記するものである。

**Y****Z****あ****[アクセス管理]**

使用またはエントリーの許可または拒否。

**[セキュア・ソケット・レイヤー (SSL)]**

ネットワーク上でのメッセージ送受信のセキュリティ管理を目的として、Netscape 社が開発したプロトコル・レイヤー。セキュリティの実現は暗号による。「ソケット」という用語は、ネットワーク上のクライアント・サーバ間、または同一コンピュータ内のプログラム・レイヤー間で、データをやりとりする際に使用するソケット方式に由来している。

**[セキュア・ハッシュアルゴリズム (SHA-1)]**

U.S. National Institute of Standards & Technology (NIST)が開発したアルゴリズム。SHA-1 は、メッセージまたはデータの暗号ハッシュ(または「指紋」)を作成するために使用する。

**[オブジェクト識別子]**

標準的なオブジェクトやクラスを引用するための ISO 登録標準に基づき登録された一意性を備えた英数字の識別子。PKI 内で使用する証明書ポリシーおよび暗号アルゴリズムは、証明書拡張の OID により一意性を備えた形で識別される。

**か****【鍵】**

暗号化、復号、電子署名、デジタル署名検証に用いる一意性を備えた電子ビット列。ほとんどの場合、二つの鍵ペアが存在し、一つは暗号化・復号用であり、もう一つは署名および電子署名検証用である。

**【完全性】**

オブジェクトまたは情報の一貫性を確保すること。

**【機密性】**

開示されれば組織に害を及ぼす可能性がある、特定可能な関連価値を備えた情報。

**【脅威】**

その機密性、完全性、利用性および合法的使用の観点から見た対資産危険。

**【許可】**

使用許諾の付与。

**【軽量ディレクトリ・アクセス・プロトコル (LDAP)】**

ネットワーク上でディレクトリ・サーバにアクセスするための標準インターネット・プロトコル。Keon CA Secure Directory は LDAP ディレクトリである。

**【検証】**

証明書の有効性を確認する処理。検証は OCSP または CRL を用いてオンラインでも実施可能。

**【公開】**

情報を対象としたセキュリティ分類の一つで、たとえ公開されたとしても個人的な損害や財務的な損失にならないもの。

**【公開鍵】**

デジタル署名用の検証鍵、および特定の申請者向けに情報を暗号化するための暗号化鍵。

**【公開鍵基盤】**

証明書および鍵の管理を目的として使用されるポリシー、手続、技術、監査および管理方法一式。

## さ

### **[識別名 (DN)]**

証明書の識別名 (DN) は、C - 国、O - 組織、OU - 部署、DC - ドメイン・コンポーネント、L - 市区町村名、s - 都道府県名、CN - コモンネーム等の証明書内の属性を組み合わせて作られる。混乱を避けるため、信頼できる CA を含む PKI 内のユーザは一意性を伴う DN を持つべきである。

### **[失効]**

通常の期間満了を待つことなく、証明書を無効とすること。証明書の失効は、認証局が行う。失効状態は、通常、証明書失効リスト(CRL)で開示する。

### **[承認]**

証明書申請の検査と申請において提供された情報の検証を行い、証明書の発行可否を決定する処理。大規模な PKI の場合、CA の代わりに RA が承認を行う場合がある。

### **[承認者]**

証明書申請者が提供した情報の検証を行う者。

### **[証明書]**

関連情報を伴う公開鍵またはユーザーで、発行する認証局の秘密鍵を用いてデジタル署名を行ったもの。証明書形式は ITU-T 勧告 X.509 に従う。

### **[証明書失効リスト (CRL)]**

特定の CA が失効させた証明書のリスト。証明書の状態確認に用いる。

### **[証明書プロファイル]**

関連する拡張フィールド用の規則、制約、デフォルト値を伴った拡張一式。

### **[証明書ポリシー (CP)]**

共通のセキュリティ要件を備えた特定のコミュニティ、アプリケーション類への証明書適用を示す規則一式。デジタル証明書向けの使用上の条件と制限について記述する。

### **[申請者]**

CA により発行された証明書、鍵を使用する人、デバイス、アプリケーション。申請者は証明書のサブジェクトに該当する。申請者は依拠利用者であることもある。申請者は、各自の秘密鍵を適切に確保する義務を CA に対して負う。

### **[脆弱性]**

保護手段における弱点、または保護手段の欠如。

#### **[相互認証]**

複数 CA 間における信頼の確立に関する処理。通常は、CA 証明書の交換と署名、保証レベルの検証が関係する。

#### **[組織]**

公開鍵基盤内の自立した要素。

た

#### **[ディレクトリ]**

LDAP に準拠した、証明書と CRL を保管・公開するためのデータベース。

#### **[デジタル署名]**

鍵を使用した暗号システムによるメッセージ変形の結果で、最初にメッセージを受けた者が、その変形は署名者の鍵に対応する鍵が行ったものであり、メッセージの改竄がないとの判断を行えるもの。

#### **[登録局 (RA)]**

CA の代行として登録サービスを行う組織。RA は、証明書申請の検査のために特定の CA と提携して業務を遂行し、検査後の発行は CA が行う。

#### **[登録サーバ]**

証明書申請、発行済証明書の検索、CA 証明書のダウンロードのために一般ユーザ（クライアント）が使用できるサーバ認証サイト。

な

#### **[認証局 (CA)]**

X.509 証明書および CRL を扱う不特定多数のユーザが信頼する機関。

#### **[認証局運用規程 (CPS)]**

証明書の発行および管理を対象とした組織のセキュリティ運用と手続。

は

#### **[ハードウェア・セキュリティ・モジュール (HSM)]**

暗号化機能の実行と暗号鍵の保存を安全な方法で行うために使用するハードウェア。HSM は FIPS のレベル 1 から 4 の評点を得ており、このうち 4 が最も安全なレベルである。

#### **[否認防止]**

取引またはサービスまたは活動発生の否認に対する保護。

#### **[秘密鍵]**

エンドエンティティの秘密署名用鍵または秘密解読用鍵。

#### **[ポリシー]**

実行計画。熟慮の上採用され、かつ将来の意思決定を導くかそれに影響を及ぼす行動過程または行動手段。

#### **[本人性確認証明書]**

人、コンピュータまたは WEB サーバ等の実在する要素と公開鍵の値を結びつける証明書。サーバ証明書、CA 証明書そしてほとんどのエンドエンティティ証明書はいずれも本人性確認証明書の一例である。

#### **[本人認証]**

検証行為。本人特定の場合は、本人性の保証。

ま  
や  
ら

#### **[依拠利用者]**

デジタル署名の本人認証または証明書対象への通信の暗号化のために CA が署名した証明書を使用する人または組織。依拠利用者は通常は PKI の申請者だが、絶対条件ではない。依拠利用者は証明書検証と適切な証明書の使用について、CA に対する義務を負う。

#### **[リポジトリ]**

PKI のユーザーがアクセスできるよう、証明書、CRL、情報を保管する場所。

わ