

ファーストサーバ **BIZCERT** 認証局運用規程(**CPS**)



作成日: 2004/06/14

最終改訂日: 2009/12/24

バージョン:2.3

Copyright © 2004-2009 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
2.0	2008.03.03	RFC3647 の章立てへの構成変更および文章表現の修正（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）
2.1	2008.06.10	本 CPS が適用される認証局追加に伴う記述の追加、およびリポジトリ公開 URL の変更
2.2	2009.06.30	本 CPS が適用される認証局の変更に伴う記述の修正、および文章表現の修正
2.3	2009.12.24	CRL の発行頻度に関する記述の変更

目次

1 はじめに	12
1.1 概要	12
1.2 正式名称と識別	12
1.3 PKI の関係者	12
1.3.1 認証局 (CA)	12
1.3.2 登録局 (RA)	13
1.3.3 申請者	13
1.3.4 依拠利用者	13
1.3.5 RSS CA	13
1.4 サーバ証明書の使用	13
1.4.1 発行するサーバ証明書	13
1.4.2 禁止されている用途	13
1.5 ポリシー	14
1.5.1 本 CPS 管理組織と連絡先	14
1.5.2 CP への適合性責任者	14
1.5.3 CPS の認可手続	14
1.6 略語および用語	14
2 公開とリポジトリの責任	15
2.1 リポジトリ	15
2.2 サーバ証明書関連情報の公開	15
2.3 公開の頻度	15
2.4 リポジトリへのアクセス制限	15
3 本人性確認および認証	16
3.1 名前	16
3.1.1 識別名における名前の種類	16
3.1.2 有意な名前である必要性	16
3.1.3 仮名、匿名の使用	17
3.1.4 名称等の解釈に関する指針	17
3.1.5 識別名の一意性	17

3.1.6	商標の認証、識別および役割	17
3.2	初回の本人性確認	17
3.2.1	秘密鍵所有についての検証	17
3.2.2	団体の本人性確認と認証	17
3.2.3	個人の本人性確認と認証	17
3.2.4	検証しない申請情報	18
3.2.5	権限の正当性確認	18
3.2.6	相互運用の条件	18
3.3	鍵更新申請時の本人性確認	18
3.3.1	鍵更新時の本人性確認と認証	18
3.3.2	失効後のサーバ証明書申請時の本人性確認と認証	18
3.4	失効申請の本人性確認と認証	18
4	サーバ証明書のライフサイクルについての運用要件	19
4.1	サーバ証明書申請	19
4.1.1	サーバ証明書申請を行える者	19
4.1.2	登録手続と責任	19
4.2	サーバ証明書申請の処理	19
4.2.1	本人性確認と認証の実施	19
4.2.2	サーバ証明書申請の承認と不承認	19
4.2.3	サーバ証明書申請の処理時間	19
4.3	サーバ証明書発行	19
4.3.1	サーバ証明書発行について認証局が行う行為	19
4.3.2	申請者に対する発行通知	20
4.4	サーバ証明書の受領	20
4.4.1	サーバ証明書の受領確認	20
4.4.2	認証局によるサーバ証明書の公開	20
4.4.3	他の関係者に対する通知	20
4.5	鍵ペアとサーバ証明書の使用	20
4.5.1	申請者の秘密鍵とサーバ証明書の使用	20
4.5.2	依拠利用者の公開鍵とサーバ証明書の使用	20
4.6	鍵の再生成を伴わないサーバ証明書更新	20

4.6.1	サーバ証明書更新が行われる場合	20
4.6.2	サーバ証明書更新申請を行える者	20
4.6.3	サーバ証明書更新申請と手続	21
4.6.4	申請者に対する発行通知	21
4.6.5	サーバ証明書の受領確認	21
4.6.6	認証局によるサーバ証明書の公開	21
4.6.7	他の関係者に対する発行通知	21
4.7	鍵の再生成を伴うサーバ証明書更新	21
4.7.1	サーバ証明書更新が行われる場合	21
4.7.2	サーバ証明書更新申請を行える者	21
4.7.3	サーバ証明書更新申請と手続	21
4.7.4	申請者に対する発行通知	21
4.7.5	サーバ証明書の受領確認	21
4.7.6	認証局によるサーバ証明書の公開	21
4.7.7	他の関係者に対する通知	21
4.8	サーバ証明書の変更	22
4.8.1	サーバ証明書変更が行われる場合	22
4.8.2	サーバ証明書変更申請を行える者	22
4.8.3	サーバ証明書変更申請と手続	22
4.8.4	申請者に対する発行通知	22
4.8.5	サーバ証明書の受領確認	22
4.8.6	認証局によるサーバ証明書の公開	22
4.8.7	他の関係者に対する発行通知	22
4.9	サーバ証明書の一時失効および失効	22
4.9.1	サーバ証明書を失効させる場合	22
4.9.2	失効申請を行える者	22
4.9.3	失効申請の手続	22
4.9.4	失効申請の猶予期間	23
4.9.5	認証局が失効申請処理を行うまでの時間	23
4.9.6	CRL 確認要件	23
4.9.7	CRL の発行頻度	23

4.9.8 CRL が公開されるまでの最長時間	23
4.9.9 オンライン失効状態確認	23
4.9.10 オンライン失効状態確認の要件	23
4.9.11 その他の利用可能な失効状態確認の手段	23
4.9.12 鍵の危殆化についての特別な要件	23
4.9.13 一時失効	23
4.9.14 一時失効申請を行える者	23
4.9.15 一時失効申請の手続	24
4.9.16 一時失効の最長期間	24
4.10 サーバ証明書状態確認サービス	24
4.10.1 サービスの運用上の特徴	24
4.10.2 サービスの利用時間	24
4.10.3 サービスのオプション機能	24
4.11 利用の終了	24
4.12 鍵預託と復旧	24
4.12.1 鍵預託と復旧方針と実施	24
4.12.2 セッション鍵のカプセル化および復旧方針と実施	24
5 物理面、手続面および人事面でのセキュリティ	25
5.1 物理的管理	25
5.1.1 認証局設備の立地と構造	25
5.1.2 物理的アクセス	25
5.1.3 電源および空調	25
5.1.4 水害対策	25
5.1.5 火気対策	25
5.1.6 保存媒体の保護	26
5.1.7 廃棄物処理	26
5.1.8 オフサイトでのバックアップ	26
5.2 手続的管理	26
5.2.1 信頼できる役割	26
5.2.2 作業毎に必要なとされる人員	26
5.2.3 信頼できる役割の本人性確認と認証	27

5.2.4 職務の分離.....	27
5.3 人事的管理.....	27
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.....	28
5.3.5 異動の頻度.....	28
5.3.6 不正行為に対する懲罰.....	28
5.3.7 委託業者.....	28
5.3.8 要員に提供する書類.....	28
5.4 監査ログの手続.....	29
5.4.1 記録の対象となるイベント.....	29
5.4.2 監査ログの処理頻度.....	29
5.4.3 監査ログの保管期間.....	29
5.4.4 監査ログの保護.....	29
5.4.5 監査ログのバックアップ手続.....	30
5.4.6 監査ログシステム.....	30
5.4.7 イベントの原因となった対象への通知.....	30
5.4.8 脆弱性の評価.....	30
5.5 記録の保管.....	30
5.5.1 アーカイブされるデータ.....	30
5.5.2 アーカイブデータ保管期間.....	30
5.5.3 アーカイブデータの保護.....	30
5.5.4 アーカイブデータのバックアップ手続.....	30
5.5.5 アーカイブデータのタイムスタンプ要件.....	31
5.5.6 アーカイブシステム.....	31
5.5.7 アーカイブデータの取得および検証手続.....	31
5.6 鍵ペアの切り替え.....	31
5.7 危殆化および災害時復旧.....	31
5.7.1 認証局秘密鍵危殆化からの復旧手続.....	31
5.7.2 コンピュータ、ソフトウェア、データ、その他資源の破損.....	31

5.7.3	申請者秘密鍵の危殆化	32
5.7.4	災害後の事業継続性	32
5.8	認証局の終了	32
6	技術的セキュリティ管理	33
6.1	鍵ペアの生成とインストール	33
6.1.1	鍵ペアの生成	33
6.1.2	秘密鍵の受渡	33
6.1.3	本認証局への公開鍵の受渡	33
6.1.4	申請者への認証局公開鍵の受渡	33
6.1.5	鍵長と暗号方式	33
6.1.6	公開鍵パラメータの生成と品質検査	33
6.1.7	鍵使用目的	33
6.2	認証局秘密鍵の保護	34
6.2.1	クリプトモジュールの標準	34
6.2.2	秘密鍵複数人管理	34
6.2.3	秘密鍵の預託	34
6.2.4	秘密鍵のバックアップ	34
6.2.5	秘密鍵のアーカイブ	34
6.2.6	秘密鍵のクリプトモジュールへの入出力	34
6.2.7	秘密鍵のクリプトモジュールでの保存	34
6.2.8	秘密鍵の活性化	34
6.2.9	秘密鍵の非活性化	34
6.2.10	秘密鍵の破棄	34
6.2.11	クリプトモジュールの評価	34
6.3	その他の鍵ペア管理について	35
6.3.1	公開鍵の保管	35
6.3.2	鍵ペアの有効期間	35
6.4	秘密鍵の活性化データ	35
6.4.1	活性化データの生成と導入	35
6.4.2	活性化データの保護	35
6.5	コンピュータセキュリティ管理	35

6.5.1	特定のコンピュータのセキュリティに関する技術要件	35
6.5.2	コンピュータセキュリティの評価	35
6.6	ライフサイクルに関する技術上の管理	36
6.6.1	システム開発管理	36
6.6.2	セキュリティ運用管理	36
6.6.3	ライフサイクルセキュリティ	36
6.7	ネットワークセキュリティ管理	36
6.8	タイムスタンプ	36
7	サーバ証明書および失効リストのプロファイル	37
7.1	サーバ証明書のプロファイル	37
7.1.1	バージョン番号	38
7.1.2	サーバ証明書拡張	38
7.1.3	暗号アルゴリズムのオブジェクト識別子	38
7.1.4	名前の形式	39
7.1.5	名前の制約	39
7.1.6	証明書ポリシーのオブジェクト識別子	39
7.1.7	ポリシー制約拡張の使用	39
7.1.8	ポリシー修飾子の構文と意味	39
7.1.9	重要な証明書ポリシー拡張についての処理方法	39
7.2	サーバ証明書失効リストのプロファイル	39
7.2.1	バージョン番号	40
7.2.2	サーバ証明書失効リストエントリ拡張	40
7.3	OCSP のプロファイル	40
7.3.1	バージョン番号	40
7.3.2	OCSP 拡張	40
8	遵守監査	41
8.1	遵守監査の頻度	41
8.2	遵守監査人の要件	41
8.3	遵守監査人と監査対象当事者の関係	41
8.4	遵守監査の対象となる事項	41
8.5	不備の結果としてとられる処置	41

8.6 結果の連絡.....	42
9 他の業務事項と法的事項.....	43
9.1 料金.....	43
9.1.1 サーバ証明書発行料金.....	43
9.1.2 他の料金.....	43
9.1.3 返金.....	43
9.2 財務的責任.....	43
9.3 秘密情報.....	43
9.3.1 秘密情報とみなす範囲.....	43
9.3.2 秘密情報とみなさないもの.....	43
9.3.3 秘密情報の取扱い.....	44
9.4 個人情報の取扱.....	44
9.4.1 プライバシーポリシー.....	44
9.4.2 個人情報の範囲と保護.....	44
9.4.3 個人情報の取扱いの例外.....	44
9.5 知的財産権.....	44
9.6 表明と保証.....	44
9.6.1 本認証局の表明と保証.....	45
9.6.2 申請者の表明と保証.....	45
9.6.3 依拠利用者の表明と保証.....	45
9.7 保証の排除.....	45
9.8 免責.....	45
9.8.1 免責.....	45
9.8.2 賠償額の上限.....	46
9.9 補償.....	46
9.9.1 申請者による補償.....	46
9.9.2 依拠利用者による補償.....	46
9.10 有効期間と終了.....	47
9.10.1 有効期間.....	47
9.10.2 終了.....	47
9.10.3 終了の効果と存続条項.....	47

9.11 関係者間の個別通知と連絡	47
9.12 改定.....	47
9.12.1 改定手続き	47
9.12.2 改定提案の通知方法とコメント期間	48
9.12.3 オブジェクト識別子の変更が必要な場合	48
9.13 紛争解決	48
9.14 準拠法	48
9.15 適用法令への準拠.....	49
9.16 雑則.....	49
9.16.1 完全合意.....	49
9.16.2 譲渡.....	49
9.16.3 分離可能性.....	49
9.16.4 権利放棄.....	49
9.16.5 不可抗力.....	49
別紙 1 略語	50
別紙 2 用語集.....	51

1 はじめに

ファーストサーバ BIZCERT 認証局（以下 本認証局）は、ファーストサーバ 株式会社が運営する、デジタル証明書を発行するための認証局です。

本認証局は、ファーストサーバ 株式会社がサービス提供、運用、管理しているサーバに対して、サーバ証明書を発行します。

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）の発行、管理および本認証局が実施するその他の業務に関する運用と手続きを定めた文書です。本 CPS は、RSA ROOT SIGNING SERVICE 証明書ポリシー(以下 RSS CP)に適合したものです。

http://www.rsasecurity.com/products/keon/repository/practices/Certificate_Policy.pdf

本 CPS は、RFC3647「インターネット X.509 PKI： 証明書ポリシーと認証実施フレームワーク」に準拠しています。

本 CPS は、運用の概要についてのみ定めています。

本 CPS は、次の認証局に適用します。

- ・ Firstserver Corporate Server CA V2

1.2 正式名称と識別

本 CPS の正式名称は「ファーストサーバ BIZCERT 認証局運用規程」です。

本 CPS は RSS CP に適合しています。

本 CPS のオブジェクト識別子は、0.2.440.200188.109.1.1 です。

RSS CP のオブジェクト識別子は、1.2.840.113549.5.6.1 です。

1.3 PKI の関係者

1.3.1 認証局 (CA)

本 CPS に基づき、本認証局は以下の作業を実施します。

- ・ 申請者からの証明書申請に対し認証作業を実施し、認証局秘密鍵を用いてサーバ証明書を発行すること

- 本 CPS 第 4.9 章（サーバ証明書の一時的失効および失効）に基づいたサーバ証明書失効処理
- 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

1.3.2 登録局 (RA)

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

1.3.3 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。

1.3.3.1 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。

1.3.3.1.1 申請責任者

申請責任者とは、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。

1.3.3.2 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。ファーストサーバ株式会社（本認証局を除く部門）がこれに該当します。

1.3.4 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。

1.3.5 RSS CA

RSS CA とは、RSA ROOT SIGNING SERVICE のための認証局であり、RSA Security Inc.により運営されています。

本認証局は RSS CA から認証局証明書の発行を受けます。

1.4 サーバ証明書の用途

1.4.1 発行するサーバ証明書

本認証局は、SSL/TLS サーバ証明書を発行します。

1.4.2 禁止されている用途

本認証局が発行するサーバ証明書は下記の用途での使用を禁止します。

- ファーストサーバ 株式会社がサービス提供、運用、管理をしていないサーバでの利用
- サーバの認証と SSL/TLS セッションの確立以外を目的とした利用

1.5 ポリシー

1.5.1 本 CPS 管理組織と連絡先

本 CPS の管理組織と連絡先は以下の通りです。

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 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

1.5.2 CP への適合性責任者

本 CPS の RSS CP への適合性は、認証局責任者が判断します。また、認証局責任者は RSS CP への適合性の責任を有します。

1.5.3 CPS の認可手続

本 CPS は、RSA ROOT SIGNING SERVICE から認定を受け、認証局責任者が承認を行います。

1.6 略語および用語

別紙 1 および別紙 2 を参照。

2 公開とリポジトリの責任

2.1 リポジトリ

本認証局は、以下の URL においてリポジトリを公開します。

<http://www.fsv.jp/repository/index.html>

2.2 サーバ証明書関連情報の公開

本認証局は、サーバ証明書関連情報として以下の情報を公開します。

- 証明書申請者契約
- 依拠利用者契約
- 本 CPS
- CRL
- RSS CP
- 認証局証明書

2.3 公開の頻度

公開の頻度は、以下のとおりです。

- 本 CPS の改定を行った場合、本 CPS 第 9.12 項（改定）で定める通り公開します。
- 証明書申請契約および依拠利用者契約の改定を行った場合、適宜リポジトリへ公開します。
- CRL は、本 CPS 第 4.9.7 項（CRL の発行頻度）に従い発行を行い、本 CPS 第 4.9.8 項（CRL が公開されるまでの最長時間）で定める通り公開します。

2.4 リポジトリへのアクセス制限

リポジトリにおける公開情報参照に対するアクセスの制限は行いません。

3 本人性確認および認証

3.1 名前

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た証明書署名要求 (CSR) を本認証局へ提出し、本認証局はその内容を検証します。

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)	申請団体の名称を反映した英文。
「組織部署名」 (OU)	申請団体の部署名。 同一組織内の異なる部署を区別するために使用します。 (このフィールドはオプションです。)
「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)	DNS に登録されている完全修飾ドメイン名。

■個人を対象としたサーバ証明書

「組織名」 (O)	申請者個人の名称。
「組織部署名」 (OU)	申請者個人が営む事業の屋号、商号。
「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)	DNS に登録されている完全修飾ドメイン名。

3.1.2 有意な名前である必要性

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。サブジェクト名の相対識別名(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 仮名、匿名の使用

サーバ証明書の利用者は、組織名（O）に仮名および匿名を使用する事ができません。

3.1.4 名称等の解釈に関する指針

本認証局が発行するサーバ証明書において名前等の解釈は、X.501 に従います。

3.1.5 識別名の一意性

識別名(DN)は、全申請者について一意性を備えたものとします。

3.1.6 商標の認証、識別および役割

サーバ証明書の申請において、申請者は他者の知的財産権を侵害する行為を行ってはならず、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。

本認証局は、申請者がサーバ証明書申請に記載する名称の知的財産権を有するかに関する検証を行いません。また、商標、商号、ドメイン名、サービスマークについての紛争は、調停、仲裁、その他の方法で解決するものではありません。本認証局およびファーストサーバ株式会社は申請者に対し一切の責任を負う事なく、上記の紛争を理由としてサーバ証明書申請を拒絶する権利を有します。

3.2 初回の本人性確認

3.2.1 秘密鍵所有についての検証

本認証局は、申請者からサーバ証明書発行申請を受けた際、証明書署名要求（CSR）の電子署名を検証することで、申請者が秘密鍵を所有していることを確認します。

3.2.2 団体の本人性確認と認証

本認証局は、第三者データベースの情報や公的機関が発行または所有する文書およびその他別途規定した方法を用いて団体の実在性について確認を行い、電話や書面など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うものとし、その手続きは手順書に定めた方法に従って行います。

また、サーバ証明書に含まれる完全修飾ドメイン名に含まれるドメイン名について、申請者がその使用权を有していることの確認を行います。

3.2.3 個人の本人性確認と認証

本認証局は、公的機関が発行または所有する身分を証明する文書およびその他別途規定した方法を用いて申請者の実在性について確認を行い、電話や書面などを使用して申請意思確認を行うものとし、その手続きは手順書に定めた方法に従って行います。

また、サーバ証明書に含まれる完全修飾ドメイン名に含まれるドメイン名について、申請者がその使用権を有していることの確認を行います。

3.2.4 検証しない申請情報

以下に記した申請情報についての検証を行いません。

- 団体が発行対象であるときの組織部署名(OU)
- 住所 (L/S)

3.2.5 権限の正当性確認

サーバ証明書の申請は、申請責任者のみが本認証局に対して行う事ができます。申請責任者がサーバ証明書を申請する権限を有する事を、本認証局は提出された書類または電話などの手段で確認を行います。

3.2.6 相互運用の条件

本認証局は相互運用を行いません。

3.3 鍵更新申請時の本人性確認

3.3.1 鍵更新時の本人性確認と認証

鍵更新時の本人性確認と認証は、本 CPS 第 3.2.2 項（団体の本人性確認と認証）ないし第 3.2.3 項（個人の本人性確認と認証）と同じ方法で実施します。

3.3.2 失効後のサーバ証明書申請時の本人性確認と認証

サーバ証明書が失効され新たに証明書申請を行った場合、本認証局は本 CPS 第 3.2.2 項（団体の本人性確認と認証）ないし第 3.2.3 項（個人の本人性確認と認証）と同じ方法で本人性確認と認証を実施します。

3.4 失効申請の本人性確認と認証

申請者がそのサーバ証明書の失効を要請する場合は、申請責任者が失効申請を行うものとします。失効申請は、申請責任者の署名を伴った書面により行うものとします。本認証局は、申請責任者と電話連絡を取るなどして失効申請の検証を行い、申請責任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。

4 サーバ証明書のライフサイクルについての運用要件

4.1 サーバ証明書申請

サーバ証明書の発行申請に関する手順と要件は本 CPS および証明書申請者約款に記載される通りです。サーバ証明書の発行を申請しても、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。

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本 CPS 第 3.2.2 項（団体の本人性確認と認証）ないし第 3.2.3 項（個人の本人性確認と認証）を遵守するものとします。

4.1.1 サーバ証明書申請を行える者

申請者がサーバ証明書の申請を行います。

4.1.2 登録手続と責任

申請者は、登録用 WEB ページ等を経由して PKCS#10 証明書申請及び申請情報を本認証局へ提出するものとします。申請者は、正確な情報を提供する責任を負います。

4.2 サーバ証明書申請の処理

4.2.1 本人性確認と認証の実施

本認証局は、本 CPS 第 3.2.2 項（団体の本人性確認と認証）ないし第 3.2.3 項（個人の本人性確認と認証）の要件を満たした認証手続きを別途定め、申請者の本人性確認および認証を実施します。

4.2.2 サーバ証明書申請の承認と不承認

本認証局は、申請情報を検証の上本 CPS 第 4.2.1 項（本人性確認と認証の実施）に記載の別途定めた認証手続により本人性確認と認証を完了した場合、サーバ証明書申請を承認します。なお、本認証局と RSS に不利益をもたらすと信ずるに足る理由がある場合、サーバ証明書申請を不承認とする場合があります。

4.2.3 サーバ証明書申請の処理時間

本認証局は、本認証局が考える妥当な期間内にサーバ証明書申請の処理を行います。

4.3 サーバ証明書発行

4.3.1 サーバ証明書発行について認証局が行う行為

本認証局は、サーバ証明書申請を承認した場合、サーバ証明書を発行します。

4.3.2 申請者に対する発行通知

本認証局は申請者に対し、サーバ証明書へのアクセス手段を提供すると共に通知を行います。

4.4 サーバ証明書の受領

4.4.1 サーバ証明書の受領確認

サーバ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から本認証局へ異議等の申し出がなかった場合、サーバ証明書が受領されたものとみなします。

4.4.2 認証局によるサーバ証明書の公開

本認証局は、発行したサーバ証明書の公開を行いません。

4.4.3 他の関係者に対する通知

適用しません。

4.5 鍵ペアとサーバ証明書の使用

4.5.1 申請者の秘密鍵とサーバ証明書の使用

申請者は、本 CPS および証明書申請者約款に同意の上、本 CPS 第 1.4.2 項（禁止されている用途）および本 CPS 第 7.1.2 項（証明書拡張）に記載される鍵使用目的（Key Usage）を遵守の上サーバ証明書を使用し、申請者秘密鍵は、それに対応したサーバ証明書の受領前に使用してはいけません。

また、サーバ証明書の有効期間が満了するかサーバ証明書が失効した場合には、申請者秘密鍵の使用を中止しなければなりません。

4.5.2 依拠利用者の公開鍵とサーバ証明書の使用

依拠利用者は、本 CPS および依拠利用者約款に同意の上、本 CPS 第 7.1.2 項（証明書拡張）に記載される鍵使用目的（Key Usage）に合致しない用途で申請者の公開鍵とサーバ証明書を使用してはいけません。

4.6 鍵の再生成を伴わないサーバ証明書更新

本認証局は、鍵の再生成を伴わないサーバ証明書更新を行いません。

4.6.1 サーバ証明書更新が行われる場合

適用しません。

4.6.2 サーバ証明書更新申請を行える者

適用しません。

4.6.3 サーバ証明書更新申請と手続

適用しません。

4.6.4 申請者に対する発行通知

適用しません。

4.6.5 サーバ証明書の受領確認

適用しません。

4.6.6 認証局によるサーバ証明書の公開

適用しません。

4.6.7 他の関係者に対する発行通知

適用しません。

4.7 鍵の再生成を伴うサーバ証明書更新

本認証局におけるサーバ証明書更新は、有効なサーバ証明書と同一のサブジェクト DN を備え、かつ必ず鍵の再生成を伴うものとします。

本 CPS におけるサーバ証明書更新は、特別な記述が無い場合このことを指します。

4.7.1 サーバ証明書更新が行われる場合

サーバ証明書が有効期間を満了する前、または申請者秘密鍵の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、サーバ証明書の更新が行われます。

4.7.2 サーバ証明書更新申請を行える者

本 CPS 第 4.1.1 項（サーバ証明書申請を行える者）と同じとします。

4.7.3 サーバ証明書更新申請と手続

申請者がサーバ証明書の更新申請を行います。申請は第 3.2.2 項（団体の本人性確認と認証）ないし第 3.2.3 項（個人の本人性確認と認証）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。サーバ証明書更新申請の本人性確認と認証は初回申請時と同じ方法で行います。

4.7.4 申請者に対する発行通知

本 CPS 第 4.3.2 項（申請者に対する発行通知）と同じとします。

4.7.5 サーバ証明書の受領確認

本 CPS 第 4.4.1 項（サーバ証明書の受領確認）と同じとします。

4.7.6 認証局によるサーバ証明書の公開

本 CPS 第 4.4.2 項（認証局によるサーバ証明書の公開）と同じとします。

4.7.7 他の関係者に対する通知

本 CPS 第 4.4.3 項（認証局による他の関係者に対する通知）と同じとします。

4.8 サーバ証明書の変更

本認証局は、サーバ証明書の変更を行いません。

4.8.1 サーバ証明書変更が行われる場合

適用しません。

4.8.2 サーバ証明書変更申請を行える者

適用しません。

4.8.3 サーバ証明書変更申請と手続

適用しません。

4.8.4 申請者に対する発行通知

適用しません。

4.8.5 サーバ証明書の受領確認

適用しません。

4.8.6 認証局によるサーバ証明書の公開

適用しません。

4.8.7 他の関係者に対する発行通知

適用しません。

4.9 サーバ証明書の一時失効および失効

4.9.1 サーバ証明書を失効させる場合

本認証局は、以下のいずれかに該当する場合、サーバ証明書を失効させます。

- 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
- 申請者が本 CPS、RSS 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
- サーバ証明書の申請者から失効申請を受け、本 CPS 第 3.4 項（失効申請の本人性確認と認証）の手続きを完了した時
- 本認証局が失効させる必要があると判断した時

4.9.2 失効申請を行える者

申請者がサーバ証明書の失効申請を行います。

4.9.3 失効申請の手続

サーバ証明書の失効申請には、本 CPS 第 4.9.2 項（失効申請を行える者）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。本認証局は、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。

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。

4.9.4 失効申請の猶予期間

サーバ証明書の失効申請は、可能な限り速やかに行わなければなりません。

4.9.5 認証局が失効申請処理を行うまでの時間

本認証局は、受け付けた失効申請の内容に不備がないと確認した場合、7 営業日の内にその申請の処理を行います。

4.9.6 CRL 確認要件

依頼利用者は、サーバ証明書の使用に先立ち、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。

4.9.7 CRL の発行頻度

本認証局は 24 時間毎に 1 回以上 CRL を発行します。

ただし、鍵危殆化等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る場合、サーバ証明書を失効し速やかに CRL を発行します。

4.9.8 CRL が公開されるまでの最長時間

発行された CRL は、最長 24 時間以内にリポジトリで公開されます。

ただし、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、本認証局は速やかに CRL をリポジトリに公開します。

4.9.9 オンライン失効状態確認

本認証局は、オンライン失効状態(OCSP)確認は提供しません。

4.9.10 オンライン失効状態確認の要件

適用しません。

4.9.11 その他の利用可能な失効状態確認の手段

本認証局は、リポジトリにおける CRL 公開以外の失効状態確認に関する手段は提供しません。

4.9.12 鍵の危殆化についての特別な要件

秘密鍵の危殆化または危殆化の恐れがあるサーバ証明書の失効を行った場合、危殆化を識別できる理由コードを使用し CRL に反映します。

4.9.13 一時失効

本認証局は、サーバ証明書の一時失効を行いません。

4.9.14 一時失効申請を行える者

適用しません。

4.9.15 一時失効申請の手続

適用しません。

4.9.16 一時失効の最長期間

適用しません。

4.10 サーバ証明書状態確認サービス

4.10.1 サービスの運用上の特徴

サーバ証明書状態の確認は、リポジトリにて公開された CRL を使用して行うことができます。

4.10.2 サービスの利用時間

サーバ証明書の状態確認サービスは、1年を通して利用できます。ただし、事前通知を実施した上で行うサービス停止や緊急時における事前通知を実施しないサービスの停止を行う場合があります。ここでサービス停止に関する通知手段としてリポジトリにおける停止通知の公開を使用します。

4.10.3 サービスのオプション機能

本サービスのオプション機能はありません。

4.11 利用の終了

申請者は、次の事由によりサーバ証明書の利用を終了することができます。

- サーバ証明書の有効期間の内に失効させた
- サーバ証明書の有効期間が満了し サーバ証明書の更新を行わなかった
- ファーストサーバ株式会社が提供するサービスの利用を終了した

4.12 鍵預託と復旧

本認証局は、秘密鍵の預託と復旧は行いません。

4.12.1 鍵預託と復旧方針と実施

適用しません。

4.12.2 セッション鍵のカプセル化および復旧方針と実施

適用しません。

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

5.1.1 認証局設備の立地と構造

本認証局の設備は、立地および構造として、通常考える事のできる災害に対する耐久性をもつ施設内に置かれます。施設内にセキュリティ区画を階層的に構築し、高レベルのセキュリティ区画に本認証局の設備を置き、不正な侵入や破壊的行為等から設備や機密情報を保護しています。

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、設備内の監視体制等 RSS が定めるセキュリティ要件を満たしています。

5.1.2 物理的アクセス

本認証局の設備は、本認証局の人員の物理的なアクセスについて、職務の内容ごとのアクセス権限を定めたアクセスリストに基づき管理、運用されています。機密情報および重要なシステムのある最重要区画への物理的アクセスは権限を持つ 2 名以上で行う事を義務付けています。

また、セキュリティ区画を分離する事で権限のない者のアクセスを制限しています。

次の機構を用い、本認証局の設備に対する物理的アクセスの管理を行っています。

- モーションセンサによる動体検出
- 生体認証装置を用いた入退室管理
- 監視カメラによる映像記録および異常検出

5.1.3 電源および空調

本認証局の設備は、停電への対策として大型の無停電電源装置および自家発電装置を設置しています。また、認証局設備安定稼働の為に空気の温度や湿度を一定に保つ為の、十分な空調を整えています。

5.1.4 水害対策

本認証局の設備は、洪水による被害が及ばないよう洪水多発地域外にある建築物の地上階に構築しています。漏水対策として漏水センサーを設置し、異常の検出を行っています。

5.1.5 火気対策

本認証局の設備は、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ます。室温センサーの設置や火気の持込を禁止する事により火気被害対策を行っています。

5.1.6 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等に保管し、適切なアクセスコントロールを実施し保護しています。

5.1.7 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物理的に破壊します。

5.1.8 オフサイトでのバックアップ

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 手続的管理

5.2.1 信頼できる役割

本認証局は、適正な業務遂行を維持するため次の責任ある役割を一名以上任命し、それぞれの責任範囲について定めます。

- 認証局責任者
認証局全体の統括および本 CPS の承認
- 認証局管理者
認証局の管理・維持・運営に関わる全ての業務を統括
- 認証業務責任者
認証業務全般に関する統括
- システム運用/管理責任者
本認証局のシステム運用、管理に関する統括
- キーマネージャ
認証局秘密鍵の定常管理およびライフサイクル管理
- セキュリティーマネージャ
本認証局運営に関するセキュリティの検証、維持を統括

その他の信頼できる役割については、別途規定を定め適切に管理を行います。

5.2.2 作業毎に必要なとされる人員

本認証局は、複数人管理を要する重要な業務を定め、いかなる者も単独ではその業務を行えないよう、権限の分離と相互牽制が働く体制のもと適切なセキュリティと実施手順を施します。

本認証局は、申請を受けて行う業務について、一連の作業を全て単独で行い業務を完了することがないように監督できる検証手順を持ちます。

5.2.3 信頼できる役割の本人性確認と認証

本認証局は、信頼できる役割に就く者の本人性確認にファーストサーバ株式会社の定める規定を用います。また、本認証局における重要な作業を実施するにあたり、作業に携わる者の本人性確認を公的な発行物を用い実施します。

信頼できる役割に就くものは、以下の手続きがとられる前に、本人性確認と認証を受けます。

- 認証局設備のアクセスリストへの掲載
- 認証局システムのアクセスリストへの掲載
- 各自の認証局役割実行のための証明書の付与
- 認証局システムのアカウントの付与

証明書とアカウント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
- 認証局ソフトウェア、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

5.2.4 職務の分離

本認証局は兼務ができない職務を定めます。兼務ができない職務には次の職務を含みます。

- 申請者からの証明書発行、更新、失効申請についての手続き
 - 申請内容の検証および審査
 - 申請の承認および却下
 - 承認された申請についての作業の許可
 - 許可された申請についての情報登録
 - 登録された申請についての処理
- リポジトリ内に格納された情報に対する操作
- 認証局証明書について重大な影響を与える作業

5.3 人事的管理

認証局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。

認証局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
- 機密性の高い認証局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
- 各自の認証局任務と抵触す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、認証局運営関連任務を遂行する要員全員に対し、任務を遂行するための十分な資格と経験を備えることを義務付けます。各業務の責任者となる要員はファーストサーバ株式会社の社員と限定します。

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、認証局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

認証局システムの変更に対応するため、本 CPS 第 5.3.3 項（訓練要件）で定める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、認証局責任者および認証局業務検討委員会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

適用しません。

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認証局システムへのアクセスを停止します。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、ファーストサーバ株式会社の社内規定に従い適切な処分を行うものとします。

5.3.7 委託業者

委託業者による本認証局の設備、情報へアクセスは権限のある 2 名以上の認証局要員の監督下で行う事ができます。

5.3.8 要員に提供する書類

本認証局は、全ての認証局要員に対して、RSS 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、依拠利用者契約、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。

5.4 監査ログの手続

5.4.1 記録の対象となるイベント

監査ログは以下の項目を対象として、自動または手動にて記録します。

- 秘密鍵および暗号モジュールのライフサイクルについてのイベント
- 認証局のライフサイクルについてのイベント
- サーバ証明書プロファイルの設定
- 申請者からの申請
- 申請に対する処理
- CRL の発行
- サーバ証明書の発行
- 認証局システムへのアクセス
- 認証局システムの保守についてのイベント
- 認証局設備への物理的アクセス
- 認証局要員の異動

5.4.2 監査ログの処理頻度

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。

5.4.3 監査ログの保管期間

監査ログは認証局設備で少なくとも 1 年間保持し、その保管は安全な方法で行います。

5.4.4 監査ログの保護

以下の要件を確保するため、認証局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

本認証局は、安全かつ確実な手段で監査ログを保管場所に移し保管します。監査ログの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ログは、保管期間満了前の削除または破棄から保護します。

5.4.5 監査ログのバックアップ手続

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。バックアップされた監査ログのセキュリティは、本 CPS 第 5.5 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。

5.4.6 監査ログシステム

監査ログの収集は、手動および自動の両方で行います。認証局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。

監査ログシステムは認証局システムの一部です。

5.4.7 イベントの原因となった対象への通知

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。

5.4.8 脆弱性の評価

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。

5.5 記録の保管

5.5.1 アーカイブされるデータ

本認証局は、以下のデータをアーカイブします。

- 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、CRL
- 本 CPS

5.5.2 アーカイブデータ保管期間

アーカイブデータの最低保管期間は 7 年です。

5.5.3 アーカイブデータの保護

本認証局は、本 CPS 第 5.5.2 項（アーカイブデータ保管期間）に定められた期間中アーカイブデータへアクセスが行えるよう、品質の劣化等を考慮の上記録媒体を選定し、磁気等から保護を行うよう環境的にも配慮します。

アーカイブデータへは権限を与えられた者のみがアクセスすることができます。

アーカイブデータを処理する為に必要な環境は、本認証局が必要とした期間維持します。

5.5.4 アーカイブデータのバックアップ手続

アーカイブデータは、定期的にバックアップ手順に従いバックアップを行います。

5.5.5 アーカイブデータのタイムスタンプ要件

アーカイブデータは、処理を行った日付、時刻が記録されなければなりません。この時記録される情報について暗号技術の使用は定義しないものとします。

5.5.6 アーカイブシステム

データを収集してアーカイブするシステムは、は認証局システムの一部です。

5.5.7 アーカイブデータの取得および検証手続

本認証局のアーカイブデータの取得と検証の詳細を記した手順は、バックアップやリカバリーに関する手順書に記載します。

5.6 鍵ペアの切り替え

本認証局の認証局鍵ペアの有効期間は、RSA KEON ルート署名契約に基づきます。また、本認証局が発行するサーバ証明書の有効期間の満了日が認証局鍵ペアの有効期間の満了日を超えることの無いように認証局鍵ペアの切り替えを行います。

本認証局は新しい鍵ペアを生成後、RSS CA に対し認証局証明書更新申請を行います。本認証局は、認証局証明書の受領後、認証局システムに認証局証明書の導入を行い、新しい認証局証明書をリポジトリで公開します。

古い認証局秘密鍵を用いて発行したすべてのサーバ証明書が有効期間を満了した後、本認証局は、リポジトリにおける古い認証局証明書の公開をやめ、認証局システムより古い認証局鍵ペアを取り除き破棄します。

5.7 危殆化および災害時復旧

5.7.1 認証局秘密鍵危殆化からの復旧手続

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 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 ROOT SIGNING SERVICE が決定した措置の実行

5.7.2 コンピュータ、ソフトウェア、データ、その他資源の破損

本認証局は認証局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。

5.7.3 申請者秘密鍵の危殆化

本認証局が発行したサーバ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サーバ証明書の失効申請を行う必要があります。

5.7.4 災害後の事業継続性

本認証局は、認証局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に遭い、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ます。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、方針を示します。

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

5.8 認証局の終了

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、認証局鍵とアーカイブデータ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。

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クリプトモジュールを用いて鍵ペアの生成を行います。鍵ペア生成の体制、手続については別途規定および手順書を整備して安全に実施されます。

申請者の鍵ペアの生成は、申請者自身が行います。

6.1.2 秘密鍵の受渡

本認証局の秘密鍵は、本認証局内で管理を行います。したがって、秘密鍵を受け渡す事はありません。

申請者の秘密鍵の生成は、申請者自身が行います。したがって、本認証局から申請者に対して申請者の秘密鍵を受け渡す事はありません。

6.1.3 本認証局への公開鍵の受渡

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するものとします。

6.1.4 申請者への認証局公開鍵の受渡

本認証局の公開鍵および関連する RSS CA に向けた証明書チェーンは、本認証局のリポジトリからダウンロードするものとします。

6.1.5 鍵長と暗号方式

本認証局は、2048 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 ビット以上の鍵長を備えた RSA 暗号鍵アルゴリズムを使用するものとします。

6.1.6 公開鍵パラメータの生成と品質検査

適用しません。

6.1.7 鍵使用目的

申請者の鍵の使用方法については、第 7.1 項（サーバ証明書のプロファイル）を参照してください。

認証局秘密鍵は、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 認証局秘密鍵の保護

6.2.1 クリプトモジュールの標準

本認証局は認証局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。

6.2.2 秘密鍵複数人管理

本認証局の認証局秘密鍵は「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 秘密鍵の預託

本認証局の認証局秘密鍵は、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るため、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認証局秘密鍵のバックアップを行います。認証局秘密鍵は HSM 内で暗号化し、論理的に安全であると確認が取れた方法で保護した上で別媒体に保存します。

6.2.5 秘密鍵のアーカイブ

本認証局は、認証局秘密鍵のアーカイブを行いません。

6.2.6 秘密鍵のクリプトモジュールへの入出力

本認証局の認証局秘密鍵は権限を有する複数の担当者により「M of N」管理で HSM に入出力します。バックアップ媒体内において認証局秘密鍵は暗号化されています。

6.2.7 秘密鍵のクリプトモジュールでの保存

本認証局の認証局秘密鍵は、クリプトモジュール内で暗号化されて保存されます。

6.2.8 秘密鍵の活性化

本認証局の認証局秘密鍵の活性化は、権限を有する複数の担当者が定められた環境内で行います。

6.2.9 秘密鍵の非活性化

本認証局の認証局秘密鍵の非活性化は、権限を有する複数の担当者が定められた環境内で行います。

6.2.10 秘密鍵の破棄

本認証局は、認証局秘密鍵を利用しなくなった場合、本認証局は必要に応じてそれらを全て破棄します。認証局秘密鍵のコピーとその断片は、認証局鍵ペアの有効期限満了後に破棄します。本認証局の秘密鍵は、権限を有する複数の担当者による作業で、鍵の復元が不可能である事を合理的に確保できる方法で破棄します。

6.2.11 クリプトモジュールの評価

本認証局の認証局秘密鍵の生成、管理、運用は、全て、FIPS 140-2 レベル 3 の認定を受けた HSM を使用します。

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。認証局データベースのバックアップと保管は、認証局運用の一環として行います。

6.3.2 鍵ペアの有効期間

本認証局の鍵ペアの有効期間は、RSA KEON ルート署名契約に従い 5 年とします。

申請者鍵ペアの有効期間は、サーバ証明書の有効期間とします。

6.4 秘密鍵の活性化データ

6.4.1 活性化データの生成と導入

本認証局の認証局秘密鍵の活性化データは権限を有する複数人の担当者により生成および導入が行われます。本認証局は、その手順を別途定めています。

申請者の秘密鍵の活性化データの生成と導入は申請者自身が行います。

6.4.2 活性化データの保護

本認証局の認証局秘密鍵の活性化データは、権限を有する複数人の担当者により保護されます。本認証局は、その手順を別途定めています。

6.5 コンピュータセキュリティ管理

6.5.1 特定のコンピュータのセキュリティに関する技術要件

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、デジタル証明書管理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。

- 認証局サービスおよび PKI 役割へのアクセス管理
- 要員の本人性確認および本人認証
- 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
- サーバ証明書発行履歴と監査データの保存
- セキュリティ関連イベントの監査

6.5.2 コンピュータセキュリティの評価

本認証局が使用するデジタル証明書管理ソフトウェアは、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。

6.6 ライフサイクルに関する技術上の管理

6.6.1 システム開発管理

本認証局は、認証局業務の実施に使用するシステムの開発、改訂を行う場合、運用上の合理性、要件、実装方法、検証方法について十分に検討し、適切なセキュリティを実現します。

6.6.2 セキュリティ運用管理

本認証局は、認証局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デジタル証明書管理ソフトウェアは、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、認証局を運用する前に認証局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デジタル証明書管理ソフトウェアの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。

6.6.3 ライフサイクルセキュリティ

適用しません。

6.7 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認証局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。認証局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。操作端末を含む本認証局業務についてのシステムは、ファーストサーバ株式会社の定めるセキュリティの標準を満たすものとします。

6.8 タイムスタンプ

本認証局は、各システムが生成する監査ログやサーバ証明書発行、CRL 発行、失効処理についての記録には時刻情報を含みます。また、正確な時刻情報を付与する機構および手続を用意します。

時間情報に関する暗号化については必要としません。

7 サーバ証明書および失効リストのプロファイル

7.1 サーバ証明書のプロファイル

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。

証明書フィールド	内容
バージョン (Version)	3
シリアルナンバー (Serial Number)	本認証局が割当てた一意性を備えた本人性確認番号
署名アルゴリズム (Signature Algorithm)	sha1WithRSAEncryption
発行者 (Issuer)	CN = Firstserver Corporate Server CA V2 OU = Cert Services O = Firstserver, Inc. C = JP
効力 (Validity)	サーバ証明書の開始および終了日時
サブジェクト名 (Subject)	本 CPS 3.1.1 項（識別名における名前の種類）に従う
サブジェクト公開鍵情報 (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

7.1.1 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。

7.1.2 サーバ証明書拡張

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」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 (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、認証局公開鍵の識別子
鍵使用目的 (Key Usage)	鍵暗号化、デジタル署名 (Digital Signature, Key Encipherment)
証明書ポリシー (Certificate Policies)	RSS CP、オブジェクト識別子、および本 CPS の公開先ポイントの識別
CRL 配布ポイント (CRL Distribution Points)	失効情報 (CRL) の公開先ポイント
Netscape 証明書タイプ (Netscape Cert Type)	SSL サーバ (SSL Server)
サブジェクト代替名 (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 (Subject Key Identifier)	特定の公開鍵を含むサーバ証明書の識別子

7.1.3 暗号アルゴリズムのオブジェクト識別子

本認証局が発行するサーバ証明書は、sha1WithRSAEncryption を暗号アルゴリズムとして使用し、署名します。

sha1WithRSAEncryption のオブジェクト識別子は 1.2.840.113549.1.1.5 です。

7.1.4 名前の形式

本認証局が発行するサーバ証明書は、本 CPS 3.1.1 項（識別名における名前の種類）に従い 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。

7.1.5 名前の制約

規定しません。

7.1.6 証明書ポリシーのオブジェクト識別子

本認証局の証明書ポリシーは RSS CA の証明書ポリシーに準じます。RSS CA の証明書ポリシーのオブジェクト識別子は 1.2.840.113549.5.6.1 です。

7.1.7 ポリシー制約拡張の使用

規定しません。

7.1.8 ポリシー修飾子の構文と意味

規定しません。

7.1.9 重要な証明書ポリシー拡張についての処理方法

規定しません。

7.2 サーバ証明書失効リストのプロファイル

本認証局が発行する CRL は以下の基本フィールドを使用します。

フィールド	内容
バージョン (Version)	2
発行者 (Issuer)	CN = Firstserver Corporate Server CA V2 OU = Cert Services O = Firstserver, Inc. C = JP
署名アルゴリズム (Signature Algorithm)	sha1WithRSAEncryption
有効開始日 (Effective Date)	CRL の発行日
次回更新予定	次回 CRL の更新予定日時

(Next Update)	
失効したサーバ証明書 (Revoked Certificates)	失効したサーバ証明書のリスト (シリアルナンバー、失効日)

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」に従って、X.509 バージョン 2 CRL を発行します。

7.2.2 サーバ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
失効理由 (Reason Code)	サーバ証明書の失効を行った理由
失効日 (Invalidity Date)	サーバ証明書の失効を行った日時
認証局鍵識別子 (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、認証局公開鍵の識別子
CRL 番号 (CRL Number)	本認証局が発行した CRL の連番

7.3 OCSP のプロファイル

本認証局は、OCSP を使用しません。

7.3.1 バージョン番号

適用しません。

7.3.2 OCSP 拡張

適用しません。

8 遵守監査

8.1 遵守監査の頻度

遵守監査は、RSA ルート署名契約に基づき、12 ヶ月毎に行います。

8.2 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 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。

8.3 遵守監査人と監査対象当事者の関係

RSA 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 ROOT SIGNING SERVICE が行います。

8.4 遵守監査の対象となる事項

遵守監査の目的は、RSA ROOT SIGNING SERVICE が求める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。

- 認証局事業実務の開示
- 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）
- 認証局環境管理

8.5 不備の結果としてとられる処置

本認証局の設計、運用または維持の実態と、RSA ROOT SIGNING SERVICE が求める要件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ます。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 **RSS CP** を遵守していないと遵守監査人が判断した場合、**RSA 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。

8.6 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、遵守監査合格の確認書として、**RSA 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。

9 他の業務事項と法的事項

9.1 料金

9.1.1 サーバ証明書発行料金

サーバ証明書発行料金は、新規発行と更新発行を問わず、サーバ証明書にかかるサービス約款において定めるものとします。

9.1.2 他の料金

リポジトリへのアクセスに関し、料金を請求しません。

9.1.3 返金

返金については、サーバ証明書にかかるサービス約款において定めるものとします。

9.2 財務的責任

本認証局は、事業の継続に影響する重要な事項および過失等に因る損害に対し、適切な水準の損害賠償保険を付保します。

9.3 秘密情報

本項では、本認証局および申請者間の情報に適用する秘密保持の義務を定めます。

9.3.1 秘密情報とみなす範囲

本認証局は、サーバ証明書申請、認証等の手続きに伴い、申請者が本認証局に対し書面または口頭等方法の如何を問わず開示する、以下に示すものを秘密情報とみなします。

- 以下に示す個人または団体の情報
 - サーバ証明書申請情報
 - サーバ証明書の登録情報、失効情報
 - ログ情報
 - 申請者と本認証局間の通信内容

9.3.2 秘密情報とみなさないもの

本 CPS 第 9.3.1 項（秘密情報の範囲と保護）の定めにかかわらず、以下に示すものは秘密情報とみなしません。

- サーバ証明書または CRL にて公開される情報
- その他適用される法令等により除外される情報

9.3.3 秘密情報の取扱い

本認証局は、秘密情報を第三者へ開示しないものとします。ただし以下に示す場合は、その限りではありません。

- 申請者の事前承諾（証明書にかかるサービス約款等への同意も、当該事前承諾に含まれます）が有る場合
- 本認証局が遵守監査を受けるなど維持運営上必要とする場合
- 法令に基づく開示要請または行政当局もしくは司法当局からの開示要請に従い開示する場合（以下これを「法令等に基づく開示」と呼びます）

9.4 個人情報の取扱

9.4.1 プライバシーポリシー

本認証局は、個人情報の取扱いについて「個人情報保護方針（プライバシーポリシー）」を定め、リポジトリにてリンク先を公開します。本方針は、個人情報の取扱い方針、利用目的、取扱管理者、開示請求の手続などを定めます。

9.4.2 個人情報の範囲と保護

本認証局は、サーバ証明書の申請、発行等の手続に伴い申請者から開示を受けた情報のうち個人に関する情報であって特定の個人を識別出来る情報を個人情報とし、プライバシーポリシー、個人情報の保護に関する法律、および、その他適用される法令または規則等の定めに従い取り扱います。本認証局は、申請者の事前承諾なく個人情報を第三者に開示せず、漏洩等の事故が生じないように管理保管するものとし、また、申請者の事前同意のない利用目的には、一切使用しません。

9.4.3 個人情報の取扱いの例外

個人情報の保護に関する法律、または、その他適用される法令、規則により個人情報の取扱いの例外の定め等がある場合は、前項の定めにかかわらず、当該法令等の定めが優先し適用されます。

9.5 知的財産権

本認証局は、以下の情報等に関する全ての知的財産権を保有します。

- 本認証局の秘密鍵および公開鍵
- 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
- 本認証局が作成、創作等したその他の情報

9.6 表明と保証

9.6.1 本認証局の表明と保証

本認証局は、以下を保証します。

- サーバ証明書の発行、失効等にかかる本認証局の全ての業務が本 CPS の定めを満たしていること
- サーバ証明書の記載情報が申請者から申請された内容に合致していること
- CRL およびリポジトリにおける他の公開情報が本 CPS の定める範囲において、最新で且つ正確な情報であること

9.6.2 申請者の表明と保証

申請者は、サーバ証明書の申請、失効および使用に際し、以下の全てを保証します。

- 本 CPS および本証明書申請者約款の定めに従い、これらを遵守すること
- 申請者が本認証局に提供する情報が完全且つ正確なものであること
- 証明書の記載情報に変更が生じた場合、速やかに本認証局に対し当該変更を書面により通知すること
- 適切な鍵ペアを生成し、その秘密鍵を適切且つ確実にサーバへインストールすること、および、その秘密鍵が本認証局以外の第三者との間の通信に使用されていないこと
- サーバ証明書の秘密鍵が危殆化しないよう適切な保護管理をすること
- サーバ証明書の有効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とき、申請者は、サーバ証明書の使用を直ちに停止し、サーバ証明書および秘密鍵（その複製物の全てを含む）を削除すること

9.6.3 依拠利用者の表明と保証

依拠利用者は、サーバ証明書の利用に際し以下の全てを保証します。

- 本 CPS および依拠利用者契約の定めに従い、これらを遵守すること
- 自らの責任においてサーバ証明書の有効性について必要な検証を行うこと

9.7 保証の排除

本認証局は、証明書申請者約款、本 CPS、または依拠利用者契約において明示的にした保証を除き、サーバ証明書の発行、利用等に関し何らの保証を行いません。但し、適用可能な法令により本項の適用が認められない場合は、この限りではありません。

9.8 免責

9.8.1 免責

本認証局は、証明書申請者約款、本 CPS、または依拠利用者契約において明示的に保証した場合を除き、いかなる場合であっても、本認証局が発行したサーバ証明書に関連し申請者、依拠利用者またはその他の第三者に生じた通常損害および特別損害（付随的、派生的損害を含むがこれに限らない）について何らの責任を負いません。本項は、損害の性質、本認証局が損害を予見した、または、予見し得た場合であっても有効に適用されます。但し、法令により本項の適用が認められない場合は、この限りではありません。

また、本認証局は、以下に列挙するサーバ証明書に関連し生じた損害について申請者、依拠利用者、およびその他の第三者に対し何らの責任を負いません。

- 失効した、または、有効期間が満了したサーバ証明書
- 不正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
- 虚偽の表明、誤解を招く情報の提供、詐称等の不実の表明に基づき発行されたサーバ証明書

9.8.2 賠償額の上限

本認証局が証明書申請者約款、本 CPS、または依拠利用者契約に基づきサーバ証明書に関連し損害賠償責任を負う場合の損害賠償額は、ファーストサーバ株式会社が当該サーバ証明書の発行等にかかるサービス料金として受領した金額を上限とします。

9.9 補償

9.9.1 申請者による補償

申請者は、以下のいずれかに該当する場合、サーバ証明書の発行、使用等に起因し生じた請求、訴訟等の全てに関し本認証局を免責し、当該訴訟等に関連し本認証局に生じる一切の費用（弁護士費用を含む）を補償することに合意します。

- 申請者による本 CPS または証明書申請者約款への違反があった場合
- 申請者による虚偽の表明、誤解を招く表明、詐称等の不実の表明等があった場合
- 申請者が必要な情報、事実等について適切な開示を行わなかった場合
- 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

9.9.2 依拠利用者による補償

依拠利用者は、以下のいずれかに該当する場合、サーバ証明書の発行、使用等に起因し生じた請求、訴訟等の全てに関し本認証局を免責し、当該訴訟等に関連し本認証局に生じる一切の費用（弁護士費用を含む）を補償することに合意します。

- 依拠利用者がサーバ証明書の有効性についての検証を怠った場合
- 依拠利用者によるサーバ証明書の利用が本 CPS または依拠利用者契約のその他の定め違反した場合

9.10 有効期間と終了

9.10.1 有効期間

本 CPS は、本認証局のリポジトリに最新版として掲載されたときに有効となります。本 CPS 第 9.10.2 項（終了）に規定する終了以前に本 CPS が無効になることはありません。

9.10.2 終了

本 CPS は、本 CPS 第 9.10.3 項（終了の効果と存続条項）に規定する内容を除き、新 CPS が効力を発する時点、または本認証局がサービスを終了した時点で無効になります。

9.10.3 終了の効果と存続条項

本認証局がサービスを終了した場合においても申請者のサーバ証明書の残存有効期間中は、本 CPS における以下の条項の効力は申請者のサーバ証明書の残存有効期間中は存続します。

- 第 9.3 項「秘密情報」
- 第 9.4 項「個人情報の保護」
- 第 9.5 項「知的財産権」
- 第 9.7 項「保証の排除」
- 第 9.8 項「免責」
- 第 9.13 項「紛争解決」
- 第 9.14 項「準拠法」

9.11 関係者間の個別通知と連絡

本認証局と申請者の間で個別に連絡が必要な際は、連絡すべき内容の重要度を考慮の上、郵送、電子メール、電話、FAX 等の手段を用います。

9.12 改定

9.12.1 改定手続き

本認証局は、随時本 CPS を改定する権利を留保します。本 CPS の改定は、認証局責任者の責任により行い、改定に対する認可手続きは本 CPS1.5.3（CPS の認可手続き）に従い行われます。

新 CPS の改定内容が発行済みサーバ証明書および CRL を利用するユーザに重大な影響を及ぼすようなポリシーまたは手順の変更があると本認証局が判断したもののについては、改定提案をリポジトリに掲示し、本 CPS9.12.2.1（コメント期間）に従いコメント期間を設定します。期間内に受け付けたコメントは本 CPS9.12.2.2（コメントの取り扱い）に従い取り扱い、コメント期間終了後認可手続きを経て、最新版の CPS としてリポジトリへ掲載します。

新 CPS の改定内容が前述に該当しないと本認証局が判断したもののについては、認可手続きを経て、随時最新版の CPS としてリポジトリへ掲載します。

9.12.2 改定提案の通知方法とコメント期間

本認証局がコメント期間の設置が必要であると判断した改定の場合、改定提案をリポジトリに掲示することにより通知とします。

前述に該当しない改定の場合、特に通知は行わずに改定を行います。

9.12.2.1 コメント期間

新 CPS の改定提案についてのコメント期間は、改定提案をリポジトリへ掲示した日から 15 日間とします。

9.12.2.2 コメントの取り扱い

本認証局はコメント期間中に受け付けたコメントを検討します。検討の結果、改定提案に対する変更が必要であると認めた場合、本認証局は改定提案に対し変更を行います。

9.12.3 オブジェクト識別子の変更に必要な場合

本認証局が新 CPS を発行するにあたってポリシーまたは手順の変更を決定した場合などオブジェクト識別子の変更に必要だと判断した場合、本認証局は新 CPS 用の新たなオブジェクト識別子を割り当てます。

9.13 紛争解決

サーバ証明書に関連し本認証局と申請者、依拠利用者またはその他の第三者との間に生じる紛争については、本 CPS、申請者約款および依拠利用者契約に従い、双方の協議により解決するものとします。但し、当該手段による解決が困難な場合は、大阪地方裁判所または大阪簡易裁判所を第一審の専属的合意管轄裁判所として解決するものとします。

9.14 準拠法

本 CPS は、日本法を準拠法とし、日本法に基づき解釈されるものとします。

9.15 適用法令への準拠

本 CPS は、適用可能な法令を遵守し、本認証局の運営および関係する当事者の権利義務等について定めます。

9.16 雑則

9.16.1 完全合意

適用しません。

9.16.2 譲渡

本 CPS に基づく申請者または依拠利用者の権利義務を譲渡することはできません。

9.16.3 分離可能性

本 CPS の一部条項が適用される法令等により無効と判断された場合であっても、当該条項を除く本 CPS の条項は有効に存続します。

9.16.4 権利放棄

本 CPS に基づく特定の権利を行使しなかった場合であっても、当該不行使をもって当該権利を放棄したものとはみなしません。

9.16.5 不可抗力

天変地異、火災、暴動、ストライキ等の不可抗力により本 CPS、証明書申請者約款、または依拠利用者契約の履行が不能となった場合であっても、本認証局、申請者および依拠利用者は、当該履行不能に関する責任を負わないものとします。

別紙 1 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	
RSS	ROOT SIGNING SERVICE	RSA 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
TLS	Transport Layer Security	トランスポートレイヤーセキュリティ
URI	Uniform Resource Identifier	統一資源識別子
URL	Uniform Resource Locator	統一資源位置指定子

別紙 2 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 ストリング]

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ストリング形式。

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**[TLS]**

Netscape 社が開発した SSL(SSLv3)をベースに IETF が標準化した規格。SSL と共に、Web だけでなくその他の TCP を利用した通信を安全にすることができる。

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。

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ーサーバ間、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。

【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、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