SecureSign®

パブリックサービス標準規程

（V1.60）

2012 年 02 月 24 日

日本認証サービス株式会社

SecureSign Certificate Policy and Certification Practice Statement (V1.60)

前バージョンからの主な更改点

1.SecureSign サーバサービスの記述追加(付録 A)－V1.51

2.AccreditedSign パブリックサービスとの整合をとるための記述強化－V1.51

3.証明書有効期間の修正(6 章)－V1.51

4.電子署名用証明書ポリシィの追加－V1.52

5.誤記訂正(A7 章)－V1.53

6.タイムスタンプ用証明書ポリシィの追加－V1.54

7.誤記修正－V1.55

8.タイムスタンプ用証明書についての記述追加－V1.56

9.Web サーバ証明書プロファイルの見直し－V1.57

10.電子署名用証明書の証明書プロファイルの一部変更、個人情報保護に関する記述の変更－V1.58

11.登記簿謄本を登記事項証明書に修正 －V1.59

12.新事務所移転に伴う住所変更 －V1.60

目次

商標

JCSI、SecureSign、AccreditedSign は、日本認証サービス株式会社の登録商標です

1. はじめに

1.1 要約

日本認証サービス株式会社（JCSI）は、SecureSign および AccreditedSign というニ種類の証明書発行サービスを提供している。 SecureSign は、PKI 標準にもとづいた証明書発行システムを組織の中に導入したい顧客のためのものである。AccreditedSign は電子署名法に定められる認定認証業務である。

JCSI は、IETF（Internet Engineering Task Force）の PKIX（Public Key Infrastructure working group）が提唱する「証明書ポリシーと認証実践の枠組み（Certificate Policy and Certification Practices Framework）」に準拠して、SecureSign パブリックサービス標準規程（本文書）を発行する。

SecureSign には、「パブリックサービス」「プライベートサービス」という二種類のサービスがある。プライベートサービスの場合、証明書ポリシーならびに CPS（Certification Practice Statement）は顧客により決定され、顧客が必要とするネットワーク上のドメイン内に開示される。 一方、パブリックサービスでは、JCSI が、証明書ポリシーならびに CPS を決定し、リポジトリにて広く一般に公開する。このことは、JCSI がパブリックサービスの証明書発行者であり、証明書に署名する当事者であるということを意味する（1.3 節参照）。

本文書は、SecureSign パブリックサービスのもとで JCSI が発行する証明書に関して JCSI が定めるポリシーおよびその証明書発行の運営に関して JCSI が適用する実践（CPS）について述べている。

PKIX は、証明書ポリシーと CPS を次のように定義している。証明書ポリシーとは、「命名された規則の集りであり、証明書が、共通のセキュリティ要件のもとで、特定のコミュニティやアプリケーションに対して利用され得る程度を示す。」ということである。したがって、証明書ポリシーは、発行される証明書の種類ごとに定められるものである。一方、CPS は、「認証局が証明書を発行するときに採用する実践に関する声明文である。」と定義されている。したがって、CPS は、利用者が、その CPS に準拠して発行される証明書の品質を評価し、使用の是非を判断するために必要となる文書である。換言すると、証明書ポリシーは、発行者側から提示する証明書の使用に関するメッセージであり、CPS は、利用者が証明書の使用に関して判断するために必要となる発行者からのメッセージである。つまり、証明書ポリシーと CPS は、表裏一体の関係にあり、相補的なものである。

JCSI は、SecureSign パブリックサービスとして発行するすべての証明書に対し、本文書で述べる内容を証明書ポリシーと定める。証明書ごとに異なるポリシーは、必要な個所にてその旨記述する。さらに、本文書は、JCSI が、きわめて高度な安全性と信頼性を確保して証明書発行業務を運営できるようにするために採用するシステムと実践に関する詳細な声明文（CPS）でもある。本文書は、SecureSign パブリックサービスに参加する JCSI、加入者（顧客）を含めたすべてのエンティティ（登場人物、登場オブジェクト）に適用される規則集の役割も担う。

本文書のすべてが、SecureSign パブリックサービスを利用する顧客に関係する。 SecureSign プライベートサービスを利用する顧客には、本文書の一部が関係する。つまり、JCSI が顧客名義の証

明書を代行発行するときに実施するセンタ運用業務について記述した部分が関係する。 しかし、SecureSign プライベートサービスを利用する顧客も、証明書ポリシーや CPS を作成するときに、本文書のその他の部分を参考に供すことができる。

証明書ポリシーや CPS は、SecureSign サービスとして提供すべき要件の進展に応じて更新されて行く。

1.2 名称

本文書の名称を「SecureSign パブリックサービス標準規程」とする。本文書および関連サービスに割り当てられたオブジェクト識別子（OID）を表 1-1 に示す。

表 1-1 JCSI の OID とオブジェクトの対応表

OID	オブジェクト
1.2.392.200075	Japan Certification Services, Inc.
1.2.392.200075.2	SecureSign Public Service
1.2.392.200075.2.1	SecureSign CPS（本文書）
1.2.392.200075.2.2	SecureSign Policy for Web-server certificate
1.2.392.200075.2.3	SecureSign Policy for Public SSL/TLS server certificate
1.2.392.200075.2.4	SecureSign Policy for Public SSL/TLS client certificate
1.2.392.200075.2.5	SecureSign Policy for Public S/MIME certificate
1.2.392.200075.2.6	SecureSign Policy for Public Signing certificate
1.2.392.200075.2.7	SecureSign Policy for Public Time Stamping certificate
1.2.392.200075.2.8	SecureSign Policy for Public Long Term SCA certificate

1.3 コミュニティと適応可能性

1.3.1 エンティティと役割

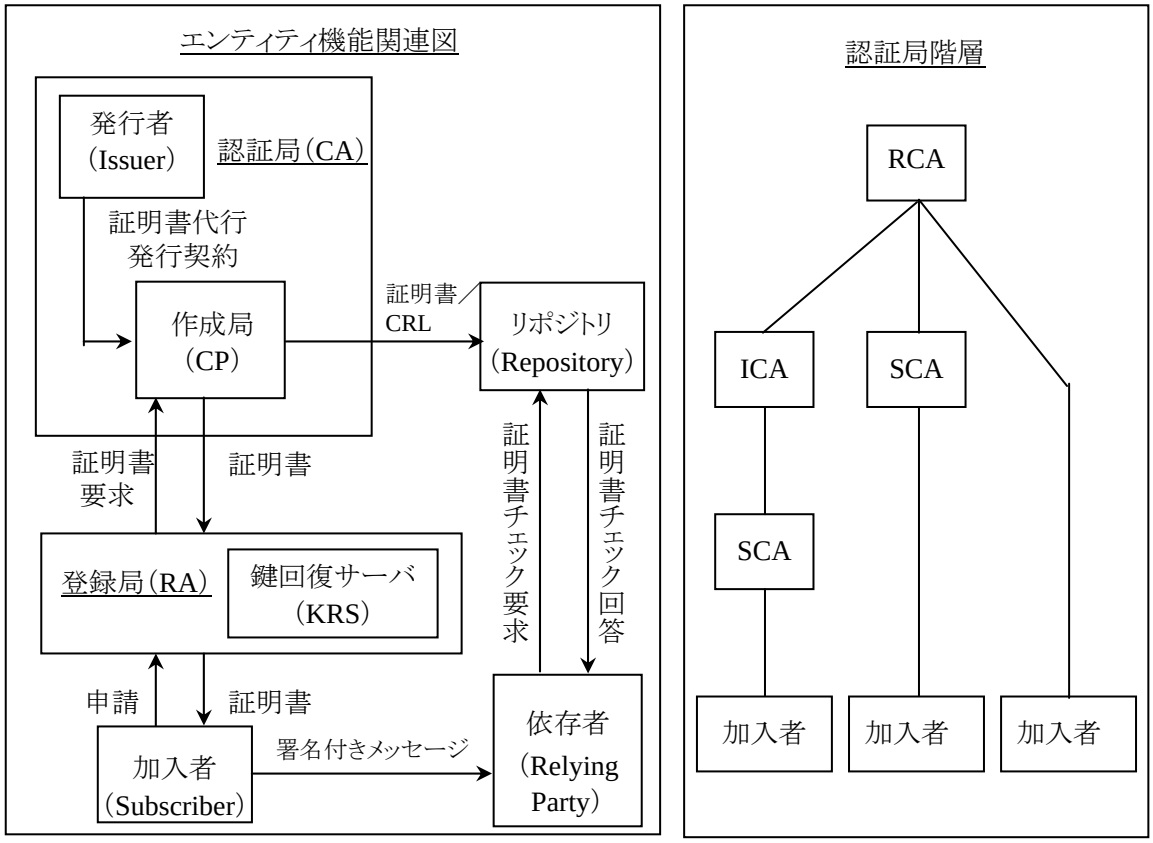
SecureSign には、表 1-2 に示す複数のエンティティが含まれる。 また、エンティティの機能関連と認証局の階層構造を、図 1-1 に示す。

表 1-2 エンティティとその役割

エンティティ	役割
顧客	SecureSign のプライベートないしパブリックサービスの契約を JCSI と交わす組織および組織の責任者 パブリックサービスの場合、証明書の発行者は、JCSI である。顧客は、RA の業務運営を JCSI から委任され、RA の運営に責任を持つ適任者を RAO として選任する。 顧客は、加入者に JCSI と交わしたパブリックサービス契約書に含まれる加入者の義務に関する事項、CPS／証明書ポリシー（本文書）を周知徹底しなければならない。 プライベートサービスの場合、証明書の発行者は、顧客である。顧客は、自組織の中から適任者を RAO として選定しなければならない。
加入者	証明書の中で公開鍵と主体名称を結合される人、組織またはオブジェクト。 加入者は、顧客組織の所属者または会員などの関係者である。パブリックサービスの場合、加入者が遵守すべき事項は、顧客と JCSI が交わす契約書でも規定される。
依存者	加入者の証明書に依存して加入者のディジタル署名を検証する人、組織またはオブジェクト。
エンド エンティティ	加入者と依存者を合わせてエンドエンティティと呼ぶ。
発行者	証明書の発行に伴い、（上位認証局が存在する場合、そのポリシーに抵触することなく、）証明書ポリシーならびに CPS を作成し公開する。発行する証明書の真正性を保証する手段として、その証明書に自己の秘密鍵で署名する組織である。 発行者は、認証局の運営主体である。証明書は、認証局、登録局、RAO、加入者などに発行される。
登録局（RA）	SecureSign では、各モデルに少なくとも一つ RA が存在することを前提にしている。 発行者は、証明書の発行に関連するいくつかの機能を RA に委任する。委任される主な機能は、以下の通りである。 証明書申請受付 本人確認 CA へ証明書要求 証明書（と秘密鍵）の配付 証明書失効決定、CA へ証明書失効要求 * RA: Registration Authority
RAO	RA の管理と運用を実行する人。 * RAO: RA Officers
作成局（CP）	発行者との証明書代行発行契約にもとづき発行者の代わりに発行者の署名付き証明書および CRL（失効した証明書の一覧表）を作成する組織。 CP は、RA から証明書要求を受領後、個々の証明書を発行する。 発行局(IA)は、作成局(CP)に同義である。 * CP: Certificate Processor
リポジトリ	リポジトリは、加入者の証明書、CRL および SecureSign サービスに関連するそ

	の他の情報を保管し、依存者からの問い合わせに回答する。
鍵回復サーバ（KRS）	加入者の秘密鍵の紛失ないし破壊に備えて、KRS はそれを安全に保管し必要なときに回復する。 * KRS: Key Recovery Server
KRO	KRS の管理と運用を実行する人 * KRO: KRS Officers
認証局（CA）	発行者としての機能と作成局としての機能を合わせ持つ組織。 SecureSign では、認証局の機能を上記の二つに大別している。 パブリックサービスでは、JCSI は、認証局、つまり発行者兼作成局として行動する。 一方、プライベートサービスでは、顧客が発行者として行動し、JCSI は作成局として行動する。したがって、プライベートサービスを利用する顧客にとって、本文書のうち、JCSI の作成局としての役割の部分が関係する。 SecureSign では、階層的に複数の認証局を存在させることができる。それらは、ルート認証局、中間認証局、下位認証局である。 * CA: Certificate Authority
ルート認証局（RCA）	RCA は、認証階層経路の頂点に位置し、自己署名し、直下にある認証局（ICA または SCA）の証明書に署名する。 RCA の配下に認証局が存在しない場合、直接、加入者証明書に署名する。 * RCA: Root CA
中間認証局（ICA）	ICA 証明書は、RCA により署名され、ICA は、SCA 証明書に署名する。 ICA の配下に SCA が存在しない場合、直接、加入者証明書に署名する。 * ICA: Intermediate CA
下位認証局（SCA）	SCA 証明書は、直上の認証局（ICA が存在しない場合には RCA）により署名され、SCA は、加入者証明書に署名する。 * SCA: Subordinate CA
CAO	CA の管理と運用を実行する人。 * CAO: CA Officers

図 1-1 エンティティ機能関連と認証局階層



注:一般に、セキュリティドメインとは、同一の発行者により証明書を発行され署名された、発行者が制定した証明書ポリシーを遵守する加入者の集合であると定義され、加入者の証明書や CRL は、そのセキュリティドメイン内に開示される。ただし、SecureSign パブリックサービスでは、SecureSign パブリックサービスルート認証局傘下の加入者およびその加入者の証明書を利用する依存者の集合をセキュリティドメインと定めるので、加入者の証明書および CRL は、一般に公開される。プライベートサービスを利用する顧客は、セキュリティドメインをどのように設定するのか、つまり加入者の証明書や CRL の開示方針(開示ドメイン、方法)について定め、JCSI に指示しなければならない。

さらに、JCSI は、パブリックサービス証明書の発行者として、このドメインを複数の顧客に分割することができる。顧客は、分割されたサブドメインに所属する加入者の名称の一意性を保証しなければならない。JCSI は、分割されたサブドメインをこえて、加入者と依存者が通信することを妨げない。

1.3.2 SecureSignサービスの形態

JCSI は、SecureSign において二種類のサービスを提供する。

パブリックサービス…発行者および作成局が両方とも JCSI により運営される。

プライベートサービス…発行者は顧客により運営され、作成局は JCSI により運営される。

1.3.3 用途

発行する証明書の用途を、「広義の用途」と「狭義の用途」という言葉を用いて表現することにする。広義の用途とは、証明書が、あるコミュニティやアプリケーションに参加する資格を与える判断材料として使用される場合をいい、一定金額未満の取引に対する使用を許諾する場合などの用途である。一方、狭義の用途とは、X.509 証明書の設定フィールドである鍵種別(keyUsage)、拡張鍵種別(extendedKeyUsage)などに設定される内容により、証明書の用途が特定されることをいう。

プライベートサービスでは、広義、狭義のいずれの用途も認証局の運営主体である顧客が定める事項である。

パブリックサービスでは、JCSI は、広義の用途を定めない。したがって、JCSI は、発行する証明書を適用することができるアプリケーションを示さないし、適用を制限するアプリケーションも示さない。ただし、JCSI は、発行する証明書が犯罪行為など法律の定めに違反した行為と関連して使用されることを禁止する。

パブリックサービスとして JCSI は、以下の 6 種類の狭義の用途を持つ証明書を発行する。(7 章参照)

・SecureSign Web-server certificate

・SecureSign SSL/TLS server certificate

・SecureSign SSL/TLS client certificate

・SecureSign S/MIME certificate
・SecureSign Signing certificate
・SecureSign Time Stamping certificate

加入者ならびに依存者は、狭義の目的に違反して証明書を使用してはならない。

注:SecureSign Web-server certificate に関連するサービス標準規定は、付録 A におもに記述される。

1.3.4 相互運用性とルート証明書

JCSI が発行する証明書と CRL は、PKI を必要とする環境において使用される。JCSI は、PKI 標準に準拠した代表的な製品との相互運用性について順次確認している。しかしながら、PKI は、標準化の真っ只中にあるので、相互運用性テストは、今後とも継続して必要になる。相互運用性に関する最新状況については当社の営業部門にご相談いただきたい。

JCSI は、SecureSign パブリックサービス用 RCA/SCA 証明書をリポジトリで公開するので、利用者は、ダウンロードして、それを必要とするソフトウェアに組み込むことができる。なお、 RCA 証明書を組み込んだソフトウェアを第三者に提供する場合には、ダウンロードにあたって、ルート証明書組み込み同意書に同意しなければならない。

1.4 サービス仕様に関する情報提供方法

本 CPS は、リポジトリにて公開される。RAO は、定期的にリポジトリを訪問し、SecureSign の新規サービス内容や仕様変更について把握し承知していなければならない。加入者が、SecureSign のサービス内容について問い合わせたいとき、所属する組織の RAO に質問すべきである。 RAO は、JCSI の顧客向けヘルプデスクに問い合わせることができる。この場合、S/MIME メールによる問い合わせが望まれるが、JCSI の営業時間帯なら電話による問い合わせも受け付ける。

［問い合わせ先］ 日本認証サービス株式会社
住所:〒107-0052 東京都港区赤坂 4-9-17 赤坂第一ビル 4F
部署:システム運用部
電話番号:03-6804-2480
FAX 番号:03-6804-2482
Email アドレス:securesign@jcsinc.co.jp

2. 一般条項

2.1 義務

JCSI は、SecureSign パブリックサービスにおける発行者として、各エンティティの義務を以下の様に定める。プライベートサービスにおいては、顧客は以下を参考にして、各エンティティの義務を定めることができる。ただし、JCSI 受託部分の義務についてはパブリックサービスと同等とする。

2.1.1 CAの義務

CA は、以下に示す原則のもと証明書を発行し運用するものとする。さらに、本文書の他項で述べる条件にもとづくものとする。

(1)作成局(CP)の義務として、発行者の署名鍵(秘密鍵)をセキュアに生成し、管理するものとする。

(2)RA の要求にもとづき加入者証明書の発行を行う。

(3)CRL、および証明書発行に関連するその他の情報をすみやかにリポジトリにて公開する。

(4)RA と協調して証明書ライフサイクル管理を行う。

(5)RA の要求にもとづき加入者証明書を失効させ、CRL を発行する。

2.1.2 RAの義務

本節において、RA は、その管理者(RAO)を含むものとする。なお、RA の操作にかかわる義務について、RAO の義務と記述する場合がある。その場合、RAO 操作の無い自動審査システムにおいても RA 管理者の義務とする。

(1)RA は、証明書申請を適正に検証しなければならない。

(2)RA は、対応する顧客のサブドメイン内からの証明書申請者を特定する仕組みを構築しなければならない。たとえば、申請項目として人名を採用する場合は、同姓同名の人物がドメインの中に複数存在する可能性があるため、そのことへの対処が必要となる。RA は、この仕組みを加入者検証(認証)プロセスとして実装しなければならない。

(3)証明書申請書の項目に組織名、部門名等を含む場合、組織の同一性の認証プロセスを構築／運用するのは RAO の義務である。

(4)RA で加入者の公開鍵と秘密鍵を生成する場合(発行パターン 2、および発行パターン 3)、正当な加入者に証明書と鍵を配付する義務が RA に生じる。

(5)RA は RA サーバをセキュアな環境に設置し、運用する義務がある。

(6)証明書申請書に記入されている加入者と申請者が同一であるかの検証(認証)を行わなければならない。SecureSign では秘密認証キーの使用を義務付ける。

(7)RA は加入者の証明書を失効させる場合、失効の妥当性の確認を行わなければならない。その確認は必要に応じて申請者の身元確認および意思確認を含む。

(8)証明書申請書には証明書に記載されない項目内容を含むことができる。この場合、申請書の

中で証明書に反映されないデータは秘密情報として取り扱う義務がある。

(9)CA と協調して証明書ライフサイクル管理を行う。

2.1.3 KRSの義務

SecureSign では RA のオプション機能として鍵回復機能を実装することができる。その場合、加入者の秘密鍵の紛失ないし破壊に備えて、鍵回復サーバ(KRS)はそれを安全に保管し必要なときに回復する義務が課せられる。

(1)鍵回復の対象となる鍵の選択および指示は KRO(Key Recovery Officer)が行い、鍵回復は KRO と RAO の合議制操作により実行する。

(2)KRS に保管する秘密鍵を含むデータは、証明書の有効期間中、安全にバックアップをとる。

(3)証明書の失効後、および証明書の有効期間終了後、秘密鍵を含むデータは、すみやかに破壊する。

2.1.4 加入者の義務

(1)正確な証明書申請内容の提示

証明書を取得する際、RA に提示する証明書申請内容は、加入者の現状を正確に表したものでなければならない。

(2)証明書利用制限

証明書はその用途範囲、セキュリティドメイン、損害賠償などを記載した本文書(プライベートサービスにおいては顧客 CPS)にもとづいて発行されている。加入者はその範囲外の用途に、証明書を提示してはならない。

(3)依存者の証明書利用についての承知義務

加入者の証明書を使った依存者からの暗号文について、JCSI は、その証明書がどのような取引において使用されるか、また特定の用途、局面に適合しているか、などの審査、確認を行っていないこと、ならびにパブリックサービスの性格上、依存者は何ら限定されていないことについて、加入者は承知しなければならない。

(4)鍵などの管理義務

加入者は、自身の使用するソフトウェアおよびハードウェア等で鍵対(秘密鍵と公開鍵のペア)を生成し、公開鍵を提出し、RA から証明書を受け取る。または、加入者は RA で生成した鍵対(公開鍵は証明書に組み込まれている)を受け取る。いずれの場合も、依存者に確実な情報を伝えるために、加入者には以下の管理義務が課される。

(a)秘密鍵の秘匿管理

生成した、または受け取った秘密鍵が、加入者本人以外によって使用、複写、バックアップされてはならない。そのために、たとえば秘密鍵使用の際に求められる PIN 等の情報を加入者本人以外に知られないように、充分な注意をもって管理しなければならない。使用、複写、バックアップが不正に行われた可能性がある場合は、加入者は失効申請を行わなければな

らない。

(b)鍵対の対応管理

秘密鍵と証明書内公開鍵との対応関係が不正と判断される場合には、加入者は失効申請を行わなければならない。

(5)証明書記載事項の管理

加入者は発行された証明書の記載事項を受領時に確認し、かつその後も使用前に随時、加入者の現状に照らして確認しなければならない。加入者は証明書受領時にその記載事項が加入者の現状に合わなかった場合、または証明書受領後にその記載事項が加入者の現状に合わなくなった場合は、すみやかに失効申請を行わなければならない。

(6)すみやかな失効申請

上記(4)-(a)、(b)、(5)の各事項について、失効申請はすみやかに行わなければならない。

(7)RAO とのコンタクト維持

加入者は上記各事項について、詳細は RAO の判断に従わなければならない。また、失効申請は RAO を経由して行わなければならない。したがって、加入者は RAO とのコンタクトを常時維持する必要がある。

2.1.5 依存者の義務

依存者は、リポジトリにて公開される「依存者同意書」に同意しなければならない。そこに明記されているように、依存者は、取引相手である加入者の証明書の有効性についてチェックしなければならない。

(1)証明書利用制限

証明書はその目的、適用範囲、加入者認証の方法、損害賠償などを記載した本文書(プライベートサービスにおいては、顧客 CPS)にもとづいて運用されており、依存者はこれらを理解し、承認した上で証明書を利用しなければならない。通信相手から提示された証明書は、それ自身に記載されたり引用されている使用目的の範囲内で使用しなければならない。

(2)証明書の有効性確認義務

証明書を利用する際には有効性確認を行わなければならない。 有効性確認内容には以下を含まなければならない。

(a)証明書パス上の全証明書について以下を確認すること。なお、パブリックサービスの場合、JCSI のルート証明書を信頼することが前提となる。

・証明書が改ざんされていないこと
・ 有効期間内であること
・ 失効していないこと
・ 上記(1)の証明書使用目的が正しいこと

(b)加入者証明書の署名を検証すること。

(c)提示された証明書記載項目(特に Subject および Subject Alt Name 項目)が、7 章記載の

規定に合致していること。

(3)SecureSign パブリックルート証明書の組み込み

一部の PKI アプリケーションソフトウェアには SecureSign パブリックルート証明書が組み込まれていないものがある。これらのアプリケーションを使用するには SecureSign パブリックルート証明書を Trusted 証明書として組み込むことができる。組み込みに際しては SecureSign パブリックルート証明書のハッシュ値（SHA-1、MD5）が JCSI の Web サイトにて公開されているので、依存者は組み込むパブリックルート証明書のハッシュ値と比較検証しなければならない。

2.1.6 リポジトリの義務

JCSI は、CRL の作成後、その情報をリポジトリ（表 4-2 参照）に公開するとともに、依存者が、証明書利用の意思決定をするために、常時リポジトリを利用して CRL を検索し、加入者証明書の失効状況を検証できるようにする。

また、JCSIリポジトリは、SecureSign サービスに関するその他の情報を保管し、表 2-1 の公開方法にて公開する。

2.2 責任

SecureSign パブリックサービスを顧客に提供するに際して、JCSI は、認証局(CA)として責任を持ち、顧客は、登録局(RA)とその管理者(RAO)を含んで責任を持つこととする。その責任について以下の様に定める。

2.2.1 JCSIの責任

(1)JCSI は、SecureSign サービスにつき、以下のことを保証する。

- RAO が 3 章に従って加入者の本人確認を実施後証明書発行要求をした場合、RA からの証明書発行要求内容(証明書のサブジェクト識別名等)を正確に反映した証明書を発行すること。
- 発行した鍵ペアを、その鍵ペアを所持すべき加入者だけに確実に渡る手段を提供すること。(発行パターン 2、および発行パターン 3)
- 4 章に従い、パブリックサービスで発行する CRL をシステム保守などの理由による一時停止、緊急やむを得ない場合の停止を除き、作成後、定期的に JCSI リポジトリに登録し、失効対象証明書の有効期間が満了するまで公開し続けること。
- RA からの失効処理要求を受理した場合、失効処理の要求があった加入者の証明書について確実に失効処理を行うこと。
- 5 章、および 6 章に従い、証明書発行システムを運用し、すべての認証局の秘密鍵について、公開鍵から類推・算出されるような場合を除き盗難等による危殆化が無いこと。
- 証明書、CRL の形式、属性が、それぞれの証明書の発行時点における 7 章記載の規定に

合致していること。

(2)顧客が RA アウトソーシングサービスを採用する場合、JCSI は、善良なる管理者の注意をもって当該サービスを運用するものとする。
(3)顧客が鍵回復サービスを採用する場合、JCSI は、善良なる管理者の注意をもって当該サービスを運用するものとする。
(4) (1)～(3)にかかわらず、JCSI は、以下のいずれかの場合には、顧客および加入者に通知することなく、一時的に SecureSign パブリックサービスの全部または一部の提供を中断することができるものとする。
- JCSI が保有する SecureSign パブリックサービス用の設備につき、緊急に保守を行う場合
- 火災、停電等により SecureSign パブリックサービスの提供ができなくなった場合
- 地震、噴火、洪水、津波等の天災により SecureSign パブリックサービスの提供ができなくなった場合
- 戦争、動乱、暴動、騒乱、労働争議等により SecureSign パブリックサービスの提供ができなくなった場合
- その他運用上、技術上、または顧客との契約の履行上、JCSI が SecureSign パブリックサービスの提供の一時的な中断が必要と判断した場合

(5)JCSI が SecureSign サービスに関し顧客、加入者ならびに依存者に対して負う責任は、(1)～(4)に定める範囲に限られるものとする。

2.2.2 顧客の責任

本節において、RA は、その管理者(RAO)を含むものとする。

(1)顧客は、証明書申請内容の審査と検証(認証)、ならびに証明書記載内容正当性の確認プロセスを正しく構築／運用する責任を負う。
(2)顧客は、サービスタイプにより、RA サーバを自ら設置運用する場合、RA サーバのセキュリティ運用について責任を負う。
(3)顧客は、加入者の義務および JCSI の責任範囲について、加入者に周知徹底するものとする。

2.3 財務上の責任

2.3.1 賠償責任

(1)JCSI が 2.2.1 節に定める責任に違反して損害賠償責任を負う場合は、顧客に対しては別途顧客との契約書で定める金額を上限とし、また依存者に対しては依存者同意書で定める金額を上限とする。ただし、JCSI の責に帰すことができない事由から生じた損害、JCSI の予見の有無を問わず特別の事情から生じた損害、逸失利益については、賠償責任を負わないものとする。

(2)顧客が本書に定める義務を履行せず、または 2.2.2 節に定める責任に違反したことにより、JCSI が損害を被った場合、JCSI は顧客に対し、当該損害の賠償を請求することができるものとする。

(3) 2.1.4 節(2)記載の加入者による証明書利用制限において、加入者が範囲外の用途に証明書を提示した結果生じたトラブルについては、加入者が一切の責任を負うものとし、当該トラブルにより JCSI が損害を被った場合は、加入者は JCSI に対し当該損害を賠償するものとする。また、2.1.4 節(5)記載の失効申請において、加入者が失効申請義務を怠ったことにより生じた第三者によるなりすまし、依存者による誤判断等のトラブルについては、加入者が一切の責任を負うものとし、当該トラブルにより JCSI が損害を被った場合は、加入者は JCSI に対し当該損害を賠償するものとする。

(4)2.1.5 節(1)記載の証明書利用制限において、依存者が使用目的の範囲をこえて証明書を使用した結果被った損害については、依存者が一切の責任を負うものとし、JCSI は何ら賠償責任を負わないものとする。また、2.1.5 節(2)記載の依存者による証明書の有効性確認は、一般的には使用するソフトウェアにより自動的に行われるものであるが、最終判断は依存者の責任であり、依存者が有効性を確認できないにもかかわらず取引等した結果被った損害については、JCSI は何ら賠償責任を負わないものとする。

2.3.2 信頼関係

JCSI は、SecureSign パブリックサービスの顧客、加入者、依存者のいずれにに対しても、その財政面での代理人もしくは被信託人ではない。ただし、JCSI は日本電気株式会社、株式会社日立製作所、富士通株式会社と協業関係にある。この 3 社は主要株主として JCSI の経営に参加している。また JCSI は 3 社に業務を委託している。

2.3.3 会計原則

日本国商法にもとづく企業会計原則による。

2.4 解釈および執行

2.4.1 準拠法

本文書は、日本国内法および規制にもとづき解釈されるものとする。

2.4.2 分離、存続、合併、通知

SecureSign パブリックサービスは、細分化されたり、他サービスを統合したり、もしくは他サービスに統合される場合がある。

2.4.3 紛争解決手続き

顧客、加入者、もしくは依存者と JCSI 間に訴訟や法的行為が起こる場合、東京地方裁判所を専

属的合意管轄裁判所とする。本文書および契約書に定められていない事項やこれらの文書の解釈に関し疑義が生じた場合、各当事者は、その課題を解決するために誠意をもって協議するものとする。

2.5 料金

JCSI は SecureSign パブリックサービスの基本価格を JCSI の Web サイトに掲載する。その他の料金は必要に応じて JCSI 営業より提示する。

2.6 公表およびリポジトリ

2.6.1 CA情報の公表

JCSI は、SecureSign パブリックサービスを顧客に提供するに際して、リポジトリを運用する。

注)SecureSign プライベートサービス向けに発行される証明書と CRL は、一般には、公開されない。つまり、それらの情報は、顧客のセキュリティドメイン内に閉じられる。

2.6.2 公表の頻度

(1)本文書の公開は、8 章に規定される。

(2)失効情報については、失効処理が行われてから 24 時間以内に CRL の形式で JCSI リポジトリにて公開が開始される。

(3)CRL 上の失効対象証明書情報は、失効対象証明書の有効期間が満了するまで公開され続ける。

(4)その他の情報については、JCSI の判断により、適宜更新し公開される。

2.6.3 アクセスコントロール

公開される情報は、表 2-1JCSI リポジトリの内容で示している公開方法にて公開される。

注)関与者全員は本文書を入手することができるが、これに修正を加えてはならない。

2.6.4 リポジトリ

(1)JCSI リポジトリは、CRL および SecureSign サービスに関連するその他の情報を保管し、公開する。(表 2-1 参照)

(2)有効期間中の CRL は、リポジトリに保管されており、依存者に対して公開されている。

(3)JCSI リポジトリへのアクセス手段ならびにアドレスは、JCSI の Web サイト (http://www.jcsinc.co.jp)から入手することができる。

(4)顧客は、JCSI のオプションサービスを利用することにより、顧客が管理するリポジトリに、加入者証明書と CRL の複製を作ることができる。

(5)リポジトリは、24 時間運用される。ただし、システムの保守などの理由により、事前に Web サイトで告知し、一時停止することがある。なお、緊急やむを得ない場合は、事前に連絡できないこ

とがある。

表 2-1 JCSI リポジトリの内容

	文書名	対象	公開方法
			http/https
規約	SecureSign パブリックサービス標準規程 (CPS)	関与者全員	○
同意書	依存者同意書	依存者	○
	ルート証明書組み込み同意書	ソフトウェア提供者	○
証明書他	パブリックサービスルート証明書	ソフトウェア提供者、 加入者、依存者	○
	CRL	依存者	○
告知書	SecureSign からのお知らせ	関与者全員	○

2.7 準拠性監査

JCSI は、SecureSign パブリックサービスを運用するに際して、本文書を含むセキュリティ規定に準拠していることを検証するために自己監査を定期的に実施する。

2.7.1 監査の頻度

自己監査は、以下の時点に実施される。

(1)以前の自己監査から 1 年後

(2)セキュリティに関係する重要な更改を実施する都度

2.7.2 監査人の身元保証・資格

JCSI は、準拠性監査に充分なスキルと経験を有したものを監査人として内部的に選定する。

2.7.3 被監査部門と監査人の関係

監査人は、認証局運用部門と独立した組織に所属するものとする。

2.7.4 監査の対象となるトピック

JCSI は、自己監査を実施するために規則と手順を定め、目的、監査組織、スケジュール、監査対象、作業要領、改善状況を明確にする。

2.7.5 監査指摘事項に対する措置

JCSI は、監査の結果、指摘事項があった場合には、可及的すみやかに改善するものとする。

2.7.6 監査結果の報告

JCSI は、自己監査を実施するが、外部への報告は行わない。

2.7.7 顧客監査

顧客が JCSI サービスの実施内容について監査を希望する場合は、有償にてこれに応じるものとする。

2.8 秘密保持

2.8.1 秘密が保たれる情報

JCSI ならびに顧客は、SecureSign サービスに関連して相手方から(i)秘密である旨明示された書面により開示され、または(ii)秘密である旨明確に告げられて口頭により開示され、かつ当該開示後 14 日以内に書面により確認された秘密情報(加入者に関する情報を含む)について、相手方の書面による事前の承諾を得ることなく第三者に開示、漏洩しないとともに、SecureSign サービスを提

供または利用するために必要な範囲をこえて使用しないものとする。

2.8.2 秘密とみなされない情報

2.8.1 節にかかわらず、次の各号に定める情報については、秘密情報とはみなされないものとする。

(1)証明書または CRL に含まれるべき情報、ただし加入者証明書の加入者識別名を除く
(2)本 CPS に含まれる情報
(3)開示の時点で、被開示者が既に保有している情報、または公知の情報
(4)開示後、被開示者の責によらずして公知となった情報
(5)第三者から秘密保持義務を負うことなく適法に入手した情報
(6)被開示者が、開示された情報によらずして独自に開発した情報
(7)開示者が第三者に対し、秘密保持義務を課すことなく開示した情報

2.8.3 証明書の失効情報の公開

加入者証明書が加入者などからの失効要請にもとづいて失効される場合、CRL には理由コード、失効日時が含まれる。したがって、この理由コード、失効日時は秘密情報とはみなされず、全ての依存者に公開されることになる。その他の取消に関する詳細な情報は公開されない。

2.8.4 捜査機関等への開示

JCSI は、捜査機関、裁判所、弁護士会その他法律上権限を有する者から強制力を伴わない任意の照会があった場合で、正当防衛、緊急避難にあたると判断したときは、顧客および加入者に関して知りうる秘密情報につき、当該捜査機関等に開示できるものとする。

2.8.5 民事手続き上の開示

2.8.4 節に含まれる。

2.8.6 証明書名義人の要請にもとづく開示

JCSI または顧客は、発行した証明書の名義人から、名義人自身の権利または利益を侵害されているまたはその恐れがあるとの、文書による申し出があった場合、申し出た者が証明書の名義人またはその委任された代理人であることを確認した上で、申し出た者に対して、その証明書に対応する

- 証明書申請書ならびに添付書類
- 加入者真偽確認に用いられた資料、記録
- 証明書記載内容そのもの

を RAO を介し開示するものとする。

なお、JCSI は 2.8.4, 2.8.5 節に規定する場合を除き、依存者からの加入者情報開示要求には応じ

ない。また発行した証明書についてはその有効期間中に限り、依存者に対して失効の有無の情報のみを CRL により公開する。

2.8.7 その他の情報公開状況

JCSI は、業務の一部を再委託する場合、秘密情報を委託先に開示することがあるが、その漏洩を阻止するため委託契約にて守秘を義務付ける。

2.9 知的財産権

本文書(CPS)ならびに JCSI が顧客に貸与するソフトウェアおよびドキュメント等の著作権は、JCSI に帰属するものとする。なお、顧客が SecureSign プライベートサービスを利用する場合は、証明書ポリシーや顧客 CPS を作成するにあたり、本文書を参考に供することができるものとする、ただし、当該証明書ポリシーや顧客 CPS が本文書の二次的著作物にあたる場合は、JCSI が原著作権者としての権利を保有するものとする。

2.10 個人情報保護

JCSI は当社 WEB サイトに掲載する個人情報保護ポリシーに基づき個人情報を取り扱う。ただし SecureSign サービスの中には証明書に個人情報を記載しないタイプも存在する。また、顧客の委託を受け、個人情報の記載された証明書を発行することがある。

3. 同一性の確認と認証

JCSI は、SecureSign パブリックサービスで発行されるすべての証明書に対する信頼されるルート認証局を運用する。 これは、JCSI が発行した証明書の内容を最終的には保証することを意味する。 このためにJCSIは、証明書申請をJCSIに代わって適正に検証することをRAOに義務付ける。適正な検証には、証明書申請を検証するために利用し得る身元情報の正確なコンテンツと、RAOが開発し適用する証明書申請内容(申請書フォーム内容)と身元情報のコンテンツとの比較検証(認証)プロセスと、証明書申請者がその要求の中にある人と同一人であるかの検証(同一性確認)プロセスの確立が必須である。言い換えるとRAOは

- 身元情報のコンテンツ(同一性確認のためのデータもコンテンツに含まれる)
- 証明書申請書フォーム
- 加入者検証プロセス（同一性の確認と認証）

を正確に設計/構築/維持することが重要な義務であると認識し、この義務を怠ったことによって発生する事故/紛争に関して責任を負うものとする。 以降この章では、同一性の確認と認証にかかわる各種指針、ならびに証明書申請書フォームの内容に同一性の確認と認証に必要な情報を含むことに着目し、証明書申請書フォーム内容設定についての指針を記述する。 なお、証明書一括発行のパターンでは、身元確認済みの加入者に対して証明書を発行送付する。 このパターンでは証明書申請は必要ではないが、正しい加入者に対して証明書を届けるプロセスの確立/維持は、やはりRAOの義務である。 なお、上記 RAOの義務はSecureSignプライベートサービスにおいても発行者により同様に課せられるものとする。

3.1 初期登録(初期申請)

3.1.1 名称のタイプ

SecureSign パブリック/プライベートサービスでは純粋個人には証明書を発行しない。 したがって、申請者(加入者)は、意味のあるドメインに属することとなる。 したがって、証明書申請書フォームに含まれる（当然身元情報にも含まれる）名称には以下のタイプが考えられる。 なお、ドメイン構造、ならびに構成要素タイプの決定に際しては、X.500 ディレクトリ/X.509 証明書のサブジェクト識別名等、関連規則を参考にされたい。

(1)ドメイン名(会社名、団体名、等)
(2)サブドメイン名(組織名、グループ名、等)
(3)加入者名(個人の姓名、アプリケーション名、コンピュータ名、等)
(4)加入者別名（社員番号、MailAdder、URL、等）
(5)秘密認証キー（PKI の外側で RAO と加入者の間で交換、共有される申請者同定のためのデータ）

(注) (1)～(4)は、身元情報のコンテンツとの突き合わせ検証(認証)のための名称タイプ例。 (5)は同一性確認検証のためのデータであり、SecureSign パブリックサービスでは必須である。

3.1.2 名称に意味がある必要

証明書申請書フォームに含まれる名称に意味は必要であるが JCSI はこれに関知しない。 RAO の管理するドメイン内名称ルールに従う。 RAO は、証明書申請者(加入者)に対して、このルールを周知徹底させなければならない。 証明書申請書フォームのフィールドに、名称としてたとえば「組織名」を採用した場合、身元情報のコンテンツにはマッチングキーとしての「組織名」が存在する。 ルールとは、この「組織名」は 部名称なのか 、課名称なのか、正式名称なのか、略称なのか、名称の意味だけではなく細かな設定ルールが必要である。

3.1.3 さまざまな名称の形式を解釈するためのルール

RAO の設定ルールに従う。 たとえば、姓と名の間のスペースは 全角と半角を許すとか、「××株式会社」は「××カ)」と同等なのかどうかなどのルール。

3.1.4 名称のユニークさ

RAO の管理するドメイン内で名称タイプに属する実体を表す名称値はユニークでなければならない。 たとえば、所属部署タイプでは、値としての「第一営業部」はユニークであり「第 1 営業部」とは別物である。 ただし、名称としての人名は、同姓同名の人物がドメインの中に複数存在する可能性があるため、ドメイン名、サブドメイン名などを修飾子として 実体と名称値を結び付けることが必要となる。 あるいは加入者別名、秘密認証キーをマッチングキーとして使用できるかもしれない。具体的には 加入者検証(認証)プロセスとして実装されなければならない。

3.1.5 名称要求の紛争決着の手続き

名称要求の紛争とは、証明書申請書に申請者が記入した名称、認証結果として発行される証明書に記載されるサブジェクト識別名にかかわる何らかの紛争を意味する(商標権侵害、不正競争、不正目的使用等)。

RAO の管理するドメイン内での名称要求の紛争は、ドメイン内で解決することを原則とする。 ドメインをまたがる紛争、もしくは依存者が関係する紛争は、当事者(RAO、依存者)間で解決することを原則とする。 いずれの場合も JCSI は紛争にかかわる当事者とはならない。 ただし RAO が、JCSI の権利を侵害したことにより発生する紛争では JCSI も当事者となる。

3.1.6 商標の認識、認証、および役割

証明書に記載される発行者、加入者の識別名は、他人の商標/商号を含む一切の権利を侵害していないことが保証されていなければならない。 SecureSign サービスでは、申請内容の審査と認証、ならびに証明書記載内容正当性の確認プロセスを正しく構築/運用する RAO にこの保証責任があり、これらの侵害または妨害行為から生じる損害の一切から JCSI は免責されるものとする。

3.1.7 秘密鍵の所有を証明する方法

(1)RA サーバで鍵生成を行うケース(発行パターン 2/3)

RA サーバで公開鍵と秘密鍵を生成する場合、正当な加入者に証明書と鍵を配付する義務が顧客に生じる。この配付する手段、ならびに受け取り確認手段は顧客内に、確かな配付プロセスとして実装されなければならない。 配付事故に関して JCSI は責任を負わない。 なお、証明書と秘密鍵を格納する配付媒体の活性化データとしての秘密認証キーは必須とする(秘密認証キーについては 3.5 節参照)。

(2)クライアント側で鍵生成を行うケース

登録される証明書申請書ならびに公開鍵は、公開鍵に対応する秘密鍵で署名されていることを RA サーバは確認する(EX.PKCS＃10)。

3.1.8 組織の同一性の認証

証明書申請書フォームのフィールドに組織名を含む場合にも、組織の同一性の認証プロセスを構築/運用するのは RAO の義務である。

3.1.9 個人の同一性の認証

SecureSign パブリックサービスでは、証明書申請書に記入されている加入者名と申請者が同一であるかの検証(認証)には、秘密認証キーの使用を義務付ける。 RAO は、事前に加入者に配付した秘密認証キーを、証明書申請書フォームに定義された秘密認証キーフィールドに入力することを加入者に義務付ける。 RAO は、加入者の証明書申請書にある秘密認証キーが、身元情報のコンテンツに保持されている秘密認証キーと一致するか否かを検証するプロセスを実装しなければない(秘密認証キーについては 3.5 節参照)。

3.2 証明書の更新に伴う鍵更新

証明書の期限切れによる証明書更新(作成)は、鍵の更新(生成)を伴う。 これは前述の初期登録と何ら変わるところはなく、証明書の更新手続きにおける同一性の確認と認証に対する指針は前述の初期登録の各節で記述されている指針と同じである。 なお、秘密認証キーの新規生成/配付も必須である。

3.3 失効後の鍵更新

証明書失効後の証明書再発行（作成）は、鍵の更新（生成）を伴う。 これは前述の初期登録と何ら変わるところはなく、 この証明書の再発行手続きにおける、同一性の確認と認証に対する指針は前述の初期登録の各節で記述されている指針と同じである。 なお、秘密認証キーの新規生成/配付も必須である。

(注) 3.2 節、3.3 節に記述している証明書更新や証明書再発行に対する指針は、JCSI は初期登録の各節に記述されている指針と同様と規定する。 ただ、必要に応じて初期登録の際の手続きと

は異なる手続きを規定(プロセスへの実装を含む)することは可能であるが、これは RAO の作業となる。 たとえば、証明書の更新申請は発行済み証明書の期限切れ一ヶ月前から受け付けるとか、再発行申請は発行済み証明書が確かに失効していることを確認できないと受理しないとかの規定の作成と検証プロセスの実装作業。

3.4 失効申請

加入者の証明書の失効要請受付けに始まる受付内容の検証(申請者の身元確認を含む)、失効審査のプロセスは RAO の責任において構築されなければならない。SecureSign サービスでは、RAO に失効オペレーションを提供するのみであり、この失効オペレーションに先立つ失効申請にかかわる標準的な同一性の確認や認証のプロセスは提供しない。 RAO は、証明書申請と異なり失効申請においては申請者が加入者とは限らず、申請者が加入者、発行者、依存者、その他第三者をも想定したプロセスを確立する必要がある。

3.5 秘密認証キー

秘密認証キーは、加入者と RAO 間のみで共有される秘密情報である。 秘密認証キーは、RAO あるいは RA サーバにより生成もしくは選定され、PKI の外側で加入者に安全な方法（第一種郵便、組織内第一種郵便類似メールなど）で配付されなければならない。 また、秘密認証キーは、RAO の管理するドメイン内の加入者に対応してユニークでなければならない。 秘密認証キーは、以下の目的で使用される。 なお、JCSI は SecureSign パブリックサービスにおいては秘密認証キーの使用、運用を RAO に義務付ける。

(1)証明書申請時の加入者の同一性確認検証データ

申請者と、証明書申請書に記入されいる加入者(加入者名)が同一かどうかを検証するための情報として秘密認証キーを使用する。 なりすまし申請、代理申請を排除する目的で使用される(実際の検証方法は 3.1.9 節参照)。

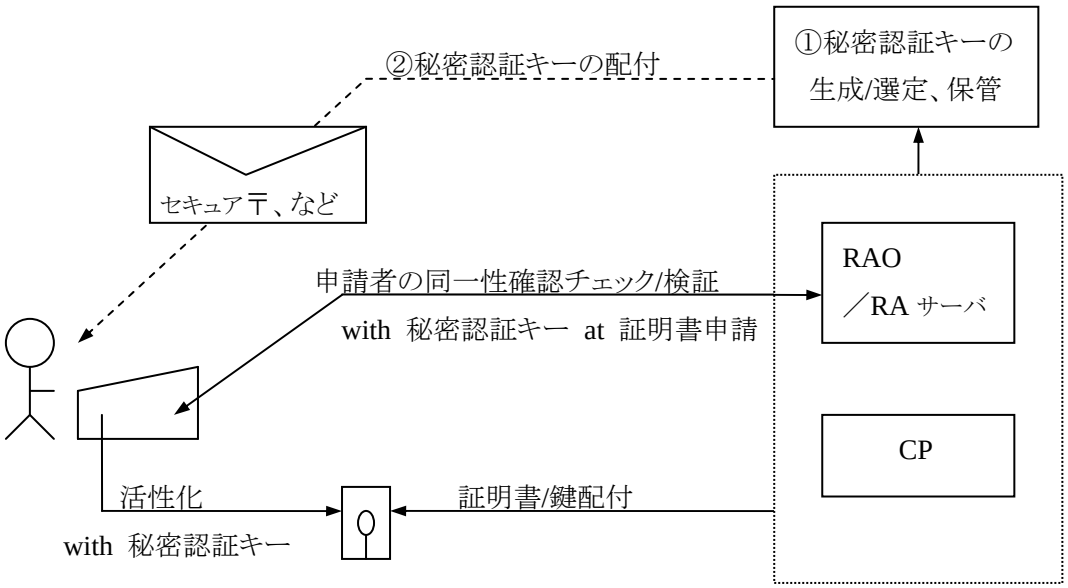
(2)媒体活性化データ

3.1.7(1)項で記述しているように、SecureSign サービスの発行パターン 2 または 3 を採用した場合には、秘密鍵と証明書は FD や IC カードなどの媒体に梱包され加入者に配付される。 この配付媒体には PIN やパスワードなどの活性化データの設定が必須である。 SecureSign サービスでは鍵、証明書を受け取るべき正当な加入者を識別するため情報としてこの活性化データを秘密認証キーとして規定し取り扱う。 なお、 配付媒体と秘密認証キーの同梱配付は、誤配付が起こった場合に第三者による証明書/鍵の誤使用、悪用をまねく可能性があるために、配付媒体と秘密認証キーは別便または別ルートで配付することを原則とする。

秘密認証キー規定 ： 英数字 8 桁以上

なお、秘密認証キーの生成／配付と秘密認証キーの使用例を、図 3-1 に記載する。

図 3-1 秘密認証キーの生成/配付と使用例



3.6 証明書発行申請データの取り扱い

証明書申請データには証明書に記載されない項目内容を含むことができる。この場合、証明書に反映されないデータは 2.8 節に規定する秘密情報として取り扱う。

4. 運用上の要件

4.1 証明書の申請、発行および受領

SecureSign は、証明書発行に関連する業務をアウトソーシングしようとする顧客の種々の要求に対応できるよう幅広いサービス内容から構成されている。サービス内容は、タイプ別にかつパターン別に分類される。 SecureSign には、8 タイプのサービスがある。

タイプ A、タイプ B は、パブリックサービス用である。 タイプ A では、JCSI が発行者であるパブリックサービス認証局が、加入者の証明書を直接発行する。タイプ B では、JCSI が発行者であるパブリックサービス認証局により署名された顧客固有の認証局（SCA）が存在し、その認証局が加入者の証明書を発行する。SecureSign パブリックサービスの一環として JCSI は、パブリックサービス用 RCA 配下の総ての CA で発行する総ての顧客分の加入者証明書の失効情報を、CRL として JCSI リポジトリにて公開する。

タイプ C、タイプ D はプライベートサービス用である。 タイプ C では、単一の顧客固有 RCA が存在し、タイプ D では、顧客固有 RCA ならびにその RCA により署名された顧客固有 SCA が存在する。プライベートサービスでは、リポジトリは、顧客により運用される。つまり、セキュリティドメインは、顧客の内部に存在し、外部に対し閉鎖される。

SecureSign では、顧客が運営する RA が設置されることを必須としている。 RA の設置場所に応じて、サービスタイプ A、B、C、D は、それぞれ二つのサブタイプに分割される。 サブタイプ 1 では、RA システムは JCSI センタに設置され、顧客の施設にいる RAO により運営される。 サブタイプ 2 では、JCSI が提供する RA システムが顧客施設に設置され RAO により運営される。顧客がサブタイプ 1 の配置を選択するなら、JCSI は、鍵回復機能をアウトソーシングサービスとして受託し提供することができる。 顧客がサブタイプ 2 の配置を選択し、鍵回復機能を導入するのなら、同機能は顧客組織内部に顧客自身により設置されることになる。 JCSI は、RA、CA 間のプロトコールを定めているので、サブタイプ 2 を採用する顧客は、CA との接続に際し、そのプロトコールを遵守しなければならない。

以上の説明を サービスタイプ一覧として 表 4-1、表 4-2 にまとめたので参照されたい。

表 4-1 サービスタイプ一覧（その 1：タイプの特徴）

タイプ			発行者と セキュリティドメイン	発行 CA （図 1-1 参照）	RA
パブリックサービス	JCSI SCA	A-1	JCSI が証明書の発行者。 すべての加入者の証明書が、JCSI の信用にもとづき、世界中の任意の依存者から信用される。	RCA, ICA, SCA を JCSI が運営し、その SCA から発行される。	JCSI 設置 （セキュアな環境と運用を短時間で利用開始可能）
		A-2			顧客設置 （顧客基幹システムとの連携による自動審査が容易）
	顧客 SCA	B-1		RCA, ICA を JCSI が運営し、ICA 配下で顧客が運営する SCA から発行される。	JCSI 設置（同上）
		B-2			顧客設置（同上）
プライベートサービス	単一 CA	C-1	顧客が証明書の発行者。JCSI は発行代行。 加入者の証明書は顧客が規定する範囲（RCA 証明書配布範囲）の依存者から信用される。	顧客が運営する単一の RCA から直接発行される。	JCSI 設置（同上）
		C-2			顧客設置（同上）
	階層 CA	D-1		RCA, (ICA,) SCA を顧客が運営し、その SCA から発行される。	JCSI 設置（同上）
		D-2			顧客設置（同上）

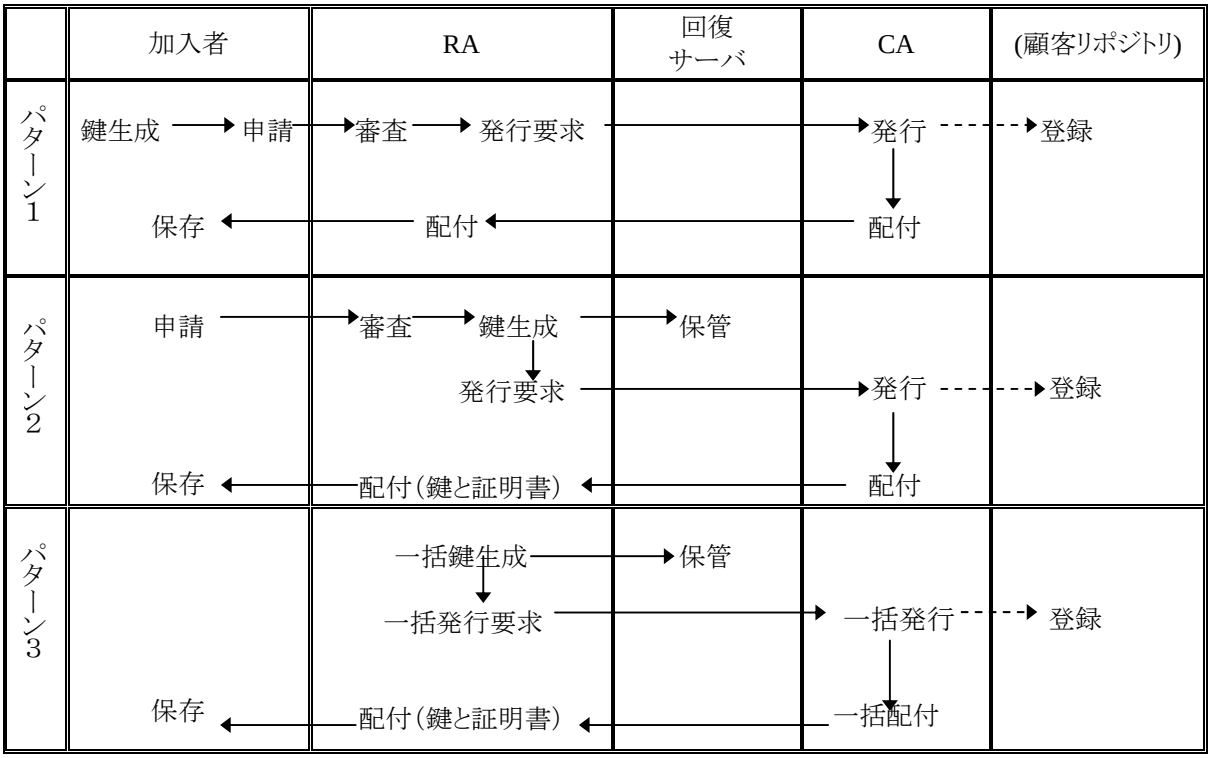
表 4-2 サービスタイプ一覧（その 2：設置先と運営主体の規定）

タイプ			RCA	ICA	SCA	CAO	RA	RAO	リポジトリ	鍵回復
パブリックサービス	JCSI SCA	A-1	JCSI 設置 JCSI 運営	JCSI 設置 JCSI 運営	JCSI 設置 JCSI 運営	JCSI 設置 JCSI 運営	JCSI 設置 顧客運営	顧客設置 顧客運営	JCSI 設置 JCSI 運営	JCSI 受託可
		A-2					顧客設置 顧客運営			顧客運営
	顧客 SCA	B-1			JCSI 設置 顧客運営	JCSI 設置 顧客運営	JCSI 設置 顧客運営			JCSI 受託可
		B-2					顧客設置 顧客運営			顧客運営
プライベートサービス	単一 CA	C-1	JCSI 設置 顧客運営	無	無	JCSI 設置 顧客運営	JCSI 設置 顧客運営	顧客設置 顧客運営	顧客設置 顧客運営	JCSI 受託可
		C-2					顧客設置 顧客運営			顧客運営
	階層 CA	D-1		JCSI 設置 顧客運営	JCSI 設置 顧客運営	JCSI 設置 顧客運営	JCSI 設置 顧客運営			JCSI 受託可
		D-2					顧客設置 顧客運営			顧客運営

SecureSign サービスでは、CRL はリポジトリ上で公開されるものとする。SecureSign パブリックサービスでは JCSI が、(論理的に)単一のリポジトリを運営する。またプライベートサービスでは、リポジトリは顧客内などの適切な場所に顧客により設置され、CA もしくは RA から CRL が掲示される。

SecureSign は、以下に掲げるように 3 パターンの証明書発行方式を提供する(表 4-3)。鍵回復サービスを実施できるのは、RA にて加入者鍵を生成する発行パターン 2、3 に限られる。

表 4-3 発行パターン



発行パターン	加入者鍵生成	発行契機	審査方法		
			自動	事前	マニュアル
1	加入者	加入者または RAO によるトリガー	○	○	○
2	RA		○	○	○
3		一括	--	○	--

審査方法には自動、事前、マニュアルの 3 通りがある。詳細は実装による。

- 自動審査:RA システムと顧客の他のシステムとを連動させ、加入者からの申請の都度、顧客のシステムにアクセスして審査を行う。
- 事前審査:RA システム(RAO 端末を含む)に顧客からの(事前審査済み)登録情報を随時入力しておき、加入者からの申請内容とこの登録情報を突き合わせて審査を行う。一括発行

（発行パターン 3）においては、登録情報にもとづいて一括発行要求が行われる。

・ マニュアル審査：加入者からの申請を 1 件づつ、RAO がその申請内容を確認して審査を行う。

4.2 証明書の一時停止と失効

識別名などの記載事項の変更、その証明書の他の証明書への置き換え、加入者による使用停止、加入者の秘密鍵の危殆化、証明書署名鍵の危殆化などの事象が生じると、該当証明書は失効させられる。 証明書の効力の一時停止に関する処理は、現状では行わない。

失効の手続きは、通常、加入者の要請により開始し、RAO により失効の是非が吟味され、失効処理要求が CA により受理される。証明書失効リスト（CRL）は、定期的に更新、公開される。

4.3 セキュリティ監査手続き

JCSI は、安全な環境を維持して行くための一つの手段としてセンタ運営ログを記録し、監査するシステムを運用する。CA、RA およびリポジトリは、監査証跡を残し、定期的にそれをセキュリティ監査する。監査証跡には以下が含まれる。

・ CP サーバ、RA サーバの操作ログ、稼動ログ。CA 秘密鍵管理、各サーバおよび RAO の権限付与のための証明書発行、始動と停止、個々の加入者証明書の登録、発行、失効、各イベントの総てのログを含む。

・ ファイアウォール、侵入検知システム、その他証明書発行システム設置室内ネットワークおよびサーバの監視ログ。総てのパケット、トランザクションに関する記録を含む。

・ リポジトリの操作ログ、稼動ログ。任意の相手からの、もしくは認証されアクセス制御された相手からの、リポジトリ掲載情報の変更の記録を含む総てのアクセスの記録。

・ 証明書発行システム設置室内をカバーするモーションデテクタ、監視カメラ・ビデオ、入退室ゲートの各機器の、警報発報を含む動作記録。警報発報は以下において異常な記録として扱う。

これらの監査証跡は定期的にセキュリティ監査され、正常と認められた記録は監査記録で置きかえられて抹消される。過誤もしくは故意の、異常と認められる記録は個別に検証され、必要と認められれば対策がとられる。この異常と認められた記録ととられた対策の記録を含むセキュリティ監査記録は、準拠性監査（2.7 節）までの間、次節に規定する方法で保存され、これらにおいて再度検証される。セキュリティ監査は少なくとも毎月行われる。

4.4 アーカイブ

SecureSign パブリックサービスでは、以下の書類およびディジタルデータを保存する。保存にあたっては流出、および改竄の防止措置をとり、書類については原本を保存する。そのために、間仕切り、壁などで区分され、防災、防犯、防火、防水機能を持つ、扉が施錠されて開錠を帳簿記録される、所定の媒体保管庫を使用する。

JCSI は本文書 2.8.4～2.8.7 項で規定された場合に、アーカイブ、保存された情報の、規定された範囲の内容を、規定された相手にのみ提供する。

JCSI は保存期間の過ぎた書類およびディジタルデータを、確実に消去する。書類は細かく裁断するなどの措置を、ディジタルデータは媒体の破壊、もしくは無効情報の上書きにより消去するなどの措置をとる。以下はアーカイブ対象データ。( )内は保存期間である。

- 認証業務の一部を他に委託する場合の委託契約書、および関係する書類の原本。(委託契約終了まで)
- 認証業務に従事する要員、組織、体制、主管、指揮命令系統に関する管理情報、履歴の原本。(最新版は永久、改版後の旧版は次回内部監査(準拠性監査(本文書 2.7 節))まで)
- 内部監査(準拠性監査(本文書 2.7 節))記録および監査報告書の原本。(10 年間)
- CA 秘密鍵管理(鍵生成、保管、活性化／非活性化、バックアップ／復元、破棄)と対応する CA 証明書発行の実施に伴うログデータ。(セキュリティ監査終了まで、セキュリティ監査記録は次回内部監査(準拠性監査(本文書 2.7 節))まで)
- セキュリティ監査(本文書 4.3 節)の記録。(次回内部監査(準拠性監査(本文書 2.7 節))まで)
- 手続き的管理(本文書 5 章)で規定する権限付与、剥奪の記録。(次回内部監査(準拠性監査(本文書 2.7 節))まで)
- 設備保守、システム保守、変更、障害の記録。(次回内部監査(準拠性監査(本文書 2.7 節))まで)
- 発行された総ての証明書、CRL。SecureSign パブリックサービス CA 自身の証明書、CRL、および関係するすべての公開鍵証明書、CRL。(有効期間満了後 10 年間)
- 本文書(SecureSign パブリックサービス標準規程)、詳細手続き文書、関係する個人情報保護などの規定、それらの変更履歴。(最新版は永久、改版後の旧版は改版後 10 年間)

4.5 鍵の交換

SecureSign パブリックサービスの CA 公開鍵の有効期間の残りが加入者証明書の最大有効期間よりも短くなる前に、JCSI はその鍵による新たな加入者証明書の発行を中止し、新たな署名用鍵ペアを本文書 6 章規定の方法で生成する。新たな公開鍵は JCSI の広く信頼された RCA から証明書の発行を受け、この証明書の形式で JCSI の Web サイトから公開する。

なお、JCSI は古い鍵での新しい鍵の証明書発行、新しい鍵での古い鍵の証明書発行は行わない。

4.6 危殆化からの復旧

SecureSign パブリックサービスの CA 秘密鍵が危殆化した場合、JCSI は、その鍵の不正な複写により新たな加入者証明書が出回り、不正に信頼されることを避けるために、その証明書署名鍵を失効させる。具体的には、その鍵にて署名したすべての有効な証明書を、可及的すみやかに失効させ、その CRL に危殆化した鍵で署名し公開する。その後にこの証明書署名鍵を抹消し、JCSI の広

く信頼されたRCAからCRLを更新発行し公開する。またJCSIはサービスを継続するために、可及的すみやかに新たな証明書署名鍵を生成する。加入者は証明書の（更新）発行を申請できる。

JCSI は、危殆化もしくは被災の際の復旧手順について別途定め、計画に従って教育訓練を行う。

4.7 CAの終了

SecureSign パブリックサービス CA は、本文書 2.2 節～2.4 節の規定、および JCSI の事業方針の変更などに起因して終了する。この終了はやむを得ない場合を除き 2 ヶ月前から、終了の 6 ヶ月後まで、JCSI の Web サイト（もしくはこれを引き継ぐサイト）に公表する。CA 終了の際、JCSI は CA 秘密鍵およびそのバックアップ媒体は完全な初期化または物理的に破壊し使用を中止するが、その CA 秘密鍵に対応する CA 証明書の失効処理は行わない。JCSI は新たな証明書の発行（、更新発行を含む）を中止する。その時点で発行済みで有効期間の残っている失効されていない証明書は、CA の終了に伴って一斉に失効処理される。ただし、JCSI はこの一斉失効を追記する最後の CRL 更新および公開を行わず、証明書記載の URL をアクセス不能化することで依存者の証明書検証を失敗させる。なお、CA 終了に伴い、JCSI は 4.4 節の規定に係らず、書類、ディジタルデータを終了時点で完全に抹消するものとする。

5. 物理的、手続き的、人事的セキュリティ管理

5.1 物理的セキュリティ管理

JCSI は、証明書発行システム（CA。タイプ A-1, B-1, C-1, D-1 では RA を含む）が設置され運用される施設のセキュリティを以下のように定める。

(1)JCSI は、証明書発行システムを設置する建物の内部を複数のセキュリティレベルで区画し、レベルごとおよびレベル間の移動に関するセキュリティ規定を設ける。具体的な履行は、センタごとに行われる。

(2)JCSI は、セキュリティレベルのアクセス権限の付与に関する手続きを文書化する。具体的な履行は、センタごとに行う。

(3)証明書発行システムは、耐震・防火・防水・防犯・空調機能を有す安全な施設に設置する。

(4)証明書発行システム（サーバ、鍵暗号化装置、F/W、ルータ）は、JCSI 専用の最高セキュリティレベルに設置する。

(5)施設への入退館は、警備員により管理される。入退館は、事前登録者のみ許可される。各レベルに入室するときは、そのレベルへの入室有資格者の帯同を必要とする。この帯同による入退室は、個別に許可され、完了が報告されるものとする。

(6)最高セキュリティレベルは、ビデオ記録システム、モーションディテクターにより、常時監視され、不正アクセスが検知されると警報が作動するものとする。警報作動の原因はすみやかに確認され、対策が講じられるものとする。

(7)最高セキュリティレベルへ入室するときには、生体認証機能により本人確認が行こなわれ、電子錠付扉が開錠する。入退室には、同時に 2 名の認証を必須とする。

(8)最高セキュリティレベルは、不正侵入を防止する構造により護られている。

(9)監視情報、入退室記録は毎月のセキュリティ監査の対象とし、その監査証跡は、3 年間保管されるものとする。

(10)機密性、安全性を保持するために重要となる機器には、停電に備えて、UPS または自家発電装置から電力が供給されるものとする。

(11)権限を有する者だけが、媒体保管庫・監視室に入室できるものとする。

(12)このセキュリティ管理の考え方に準拠して認証局設備が運営されているか否かを、文書化された手順にもとづき毎月監査する。

5.2 手続き的セキュリティ管理

JCSI は、表に示すように要員区分を設定する。センタ要員は、CA および JCSI に設置される RA ならびに JCSI のリポジトリを操作する。

表 5-1 要員別権限

<table>
<tr><th colspan="2">要員区分</th><th>指名</th><th>入室権限付与</th><th>操作権限付与</th><th>アクセス権限チェック方式</th></tr>
<tr><td colspan="2">PKI 運営管理者</td><td>センタごとに指名され、権限付与される</td><td colspan="2">－</td><td>－</td></tr>
<tr><td colspan="2">セキュリティ管理者</td><td>同上</td><td>あり</td><td>－</td><td>ID カードシステム、
生体認証システム</td></tr>
<tr><td rowspan="3">センタ要員</td><td>PKI 技術要員</td><td>PKI 運営管理者により指名される</td><td rowspan="3">セキュリティ管理者の同意のもとに PKI 運営管理者が付与する</td><td rowspan="3">PKI 運営管理者が付与する</td><td>単独でのアクセス不可
セキュリティシステムへのアクセス権限を有した者の帯同が必要</td></tr>
<tr><td>システム運用者</td><td>セキュリティ管理者により指名され PKI 運営管理者の合意が必要</td><td>ID カードシステム、
生体認証システム</td></tr>
<tr><td>保守要員</td><td>セキュリティ管理者または PKI 運営管理者により指名される</td><td>単独でのアクセス不可
セキュリティシステムへのアクセス権限を有した者の帯同が必要</td></tr>
</table>

証明書発行システムの設置場所のセキュリティを保証するために、センタ要員に入室権限を付与し、当該システム専用室へのアクセスを制限する。各センタの PKI 運営管理者がセキュリティ管理者の同意のもとにセンタ要員に専用室への入室権限を付与できるものとする。セキュリティ管理者は権限付与を表明した文書にもとづいて、ID カードシステム、生体認証システムに当該センタ要員を登録し、また登録を抹消する。

証明書発行システムの運用にかかわるセキュリティを保証するため、装置・機器の操作権限を要員に分散して付与し、可能なアクセスを規定する。各センタの PKI 運営管理者が、証明書発行システムの操作権限を付与できるものとする。PKI 運営管理者は権限付与を表明した文書にもとづいて、アカウント設定（、変更、抹消）、運用証明書の発行（、失効）処理を行う。なお、装置・機器のアカウントのうち特権を付与されるものについては、特に厳重に管理するものとする。

入室権限、操作権限、および遠隔操作権限付与の記録は、PKI 運営管理者により管理され、錠付きの収納キャビネットに、少なくとも 3 年間保管される。

これらの権限付与、および指揮命令系統の詳細は、各センタごとに詳細手順書にて定める。各センタの PKI 運営管理者は、詳細手順において単に運営管理者と呼ぶことがある。業務の一部を委託する場合、JCSI は委託先に本章の規定の遵守を求め、詳細手順書の作成とこれに沿った運用を求める。なお、各センタは、各要員の作業ならびに委託先による作業について、本文書に従って適切なセキュリティを維持すべく監督しなければならない。

5.3 人事的セキュリティ管理

JCSIは、証明書発行システムの運用に携わる要員のセキュリティ管理を、以下の諸要件に適合するよう実施する。

(1)センタの運営に直接携わる要員は、過去 15 年間犯罪を起こしていないということを宣誓する書類に、毎年署名する。

(2)センタ要員に、証明書発行システムの運用に必要な規程、手順などのセキュリティ教育を実施し、これを遵守することの同意をとり、宣誓書に署名させる。この中で特に、鍵の危殆化、または紛失の重大性について熟知させる。

(3)秘密鍵の分割保管（6.2 節)において鍵断片（分割鍵）の保管者は、鍵断片（分割鍵）を受け取る前に管理責任を果たすことに同意し文書に署名をする。

なおセンタ要員の中に、業務に係る技術に関して充分な知識および経験[注 1]を有すると認められた者を適宜配置[注 2]する。

注 1) 認証システムの開発、運用、コンサルテーションの実務の経験が総じて 2 年以上、そして本文書ならびにこれに類する規程の開発経験を有すること。

注 2) その所定人員数はセンタごとに定めるものとする。

6. 技術的なセキュリティ管理

6.1 鍵ペアの生成と組み込み

6.1.1 RCA

(1)鍵ペアの生成

秘密鍵と公開鍵ペアの生成には、ISO 9564-1:1991 および ISO 11568-5 に記載されている乱数処理、または疑似乱数処理を適用し、暗号化装置内に生成する。鍵ペアの生成は、JCSI が指名した 4 人の合議メンバが行う（プライベートサービスでは顧客の指名した 2 人以上の合議メンバ）。

(2)証明書発行者に対する公開鍵の提出

生成した公開鍵は、外部に提出することなく RCA 内で証明書の形式にする。

(3)ユーザに対する JCSI RCA 公開鍵の配布

- デファクトスタンダードアプリケーション(製品、アプリケーションプログラム)に JCSI RCA 公開鍵をプレインストールして配布する。
- JCSI のリポジトリからエンドエンティティにダウンロードしてもらい配布する。ダウンロードする JCSI RCA 公開鍵の正当性は、ハッシュ値(JCSI が公開)からエンドエンティティが確認することを義務付ける。
- 加入者に証明書を発行する際に一緒に配付する。

(4)鍵のサイズ

RSA 公開鍵暗号方式による 2,048 ビットの鍵を使用する（パブリックサービス）
（プライベートサービスでは 1,024 ビットまたは 2,048 ビット）。

(5)ハードウェア鍵の使用

鍵ペアの生成は、暗号化装置（ハードウェア）により生成する。

(6)鍵ペアの組み込み

鍵ペアを生成した装置で使用するため、組み込みは行わない。（必要無い）

(7)使用するハッシュ関数

SHA-1

6.1.2 ICA/SCA

(1)鍵ペアの生成

秘密鍵と公開鍵ペアの生成には、ISO 9564-1:1991 および ISO 11568-5 に記載されている乱数処理、または疑似乱数処理を適用し、暗号化装置内に生成する。鍵ペアの生成は、各 CA の発行者が指名した 2 人の合議メンバが行う。なお、生成された鍵はその暗号化装置内でのみ使用する。

(2)証明書発行者に対する公開鍵の配付

生成した公開鍵は、トークン(FD、IC カード等)に出力し、上位 CA に証明書の発行を要求す

る。

(3)ユーザに対する ICA/SCA 公開鍵の配布

- デファクトスタンダードアプリケーション(製品、アプリケーションプログラム)に SCA 公開鍵をプレインストールして配布する。
- 加入者に証明書を発行する際に一緒に配付する。

(4)鍵のサイズ

RSA 公開鍵暗号方式による 1,024 ビットまたは 2,048 ビットの鍵を使用する。

(5)ハードウェア鍵の使用

鍵ペアの生成は、暗号化装置（ハードウェア）により生成する。

(6)鍵の使用目的

X.509V3 の Extension を使用して、鍵の使用目的を証明書、CRL の署名・検証に限定する。

(7)鍵ペアの組み込み

鍵ペアを生成した装置で使用するため、組み込みは行わない。（必要無い）

(8)使用するハッシュ関数

SHA-1

6.1.3 加入者（発行パターン 1）

(1)鍵ペアの生成

秘密鍵と公開鍵ペアの生成は、ISO 9564-1:1991 および ISO 11568-5 に記載されている乱数処理、または疑似乱数処理で行うこと。生成した鍵ペアは安全に保管する。

(2)証明書発行者に対する公開鍵の提出

生成した公開鍵は、証明書署名要求としてオンラインで、RA 経由 CA に証明書の発行を要求する。

(3)鍵のサイズ

加入者のソフトウェアによって、RSA 公開鍵暗号方式による 512 ビット、768 ビット、1,024 ビットまたは 2,048 ビットの鍵を使用する。

(4)ハードウェア鍵の使用

鍵ペアの生成は、暗号化装置（ハードウェア）により生成することもできる。

(5)鍵の使用目的

鍵の使用目的に合致した X.509V3 の Extension を設定する。 エンドエンティティはこの鍵使用目的の範囲内で証明書を使用するものとする。

(6)鍵ペアの組み込み

鍵ペアを生成した装置で使用するため、組み込みは行わない。（必要無い）

(7)使用するハッシュ関数

SHA-1

6.1.4 加入者（発行パターン 2/3）

(1)鍵ペアの生成

秘密鍵と公開鍵ペアの生成は、ISO 9564-1:1991 および ISO 11568-5 に記載されている乱数処理、または疑似乱数処理で行う。鍵ペアの生成は、RAO 2 人の合議制操作による承認をもとに RA または KRS 上で行う。

(2)証明書発行者に対する公開鍵の提出

生成した公開鍵は、証明書署名要求としてオンラインで、CA に証明書の発行を要求する。

(3)鍵のサイズ

RSA 公開鍵暗号方式による 512 ビット、1,024 ビットまたは 2,048 ビットの鍵を使用する。

(4)ハードウェア鍵の使用

ハードウェア鍵の使用はしない。

(5)鍵の使用目的

鍵の使用目的に合致した X.509V3 の Extension を設定する。 エンドエンティティはこの鍵使用目的の範囲内で証明書を使用するものとする。

(6)鍵ペアの組み込み

鍵ペアは、秘密認証キーをパスフレーズとして用いて加入者が JCSI の指定するダウンロード受領ページにアクセスしダウンロード後目的の PKI アプリケーションに加入者自身が組み込む。なお、

- 鍵ペアは暗号化されていない状態で RA 外には存在してはならない。
- また、鍵ペアは加入者本人の受領確認後すみやかに破棄しなければならない。

(7)使用するハッシュ関数

SHA-1

6.2 秘密鍵の保護

6.2.1 暗号化モジュール標準

CA 秘密鍵は FIPS 140-1 レベル 3 相当の暗号化モジュールによって管理する。
加入者が使用する暗号化モジュールは FIPS 140-1 に準拠していることが望ましい。

6.2.2 秘密鍵(n out of m)の多人数制御

秘密鍵を使用する操作を複数人の合議で行う合議制操作(Dual Control)と、秘密鍵を分割保管する SecretShare(SecretSplit)を採用し、表 6-1 に示す範囲で個々の CA が決定する。
SecretShare 分割数と署名するために必要な Share 数が等しいときは媒体を二重化する。

表 6-1 合議制操作と SecretShare

機関	合議制操作に必要な人数	SecretShare 分割数	署名するために必要な Share 数

RCA(パブリク)	2(サーバ要員)	4	4
RCA(パブリク)以外	2(サーバ要員)	2~5	2~5

(注) 本章で記述する「サーバ要員」とは、5 章で記す「PKI 技術要員」または「システム運用者」を指す。

6.2.3 秘密鍵のエスクロウ

実施しない。

6.2.4 秘密鍵のバックアップ

CA 秘密鍵は Secret Share によってトークンに鍵断片(分割鍵)として保管する。 鍵断片(分割鍵)保管者は各 CA の発行者が指名する。「鍵管理の宣誓書」に署名した上でトークンを扱い、トークンはタンパーエビデント封筒に封印して、鍵断片(分割鍵)保管者の責任において耐火金庫に保管管理する。

なお、秘密鍵のバックアップ操作は、サーバ要員の合議制操作で行われる。

加入者の秘密鍵は加入者の責任で安全にバックアップすること。 加入者(発行パターン 2/3)で鍵回復サービスを利用したものについては KRS で多重暗号化によってバックアップする。

6.2.5 秘密鍵のアーカイブ

CA 秘密鍵はアーカイブしない。

6.2.6 秘密鍵の暗号化モジュールへのエントリー

秘密鍵のエントリーは、サーバ要員の合議制操作で行われる。

CA 秘密鍵は分割トークンから安全に暗号化モジュールに投入する。

トークンは「鍵管理の宣誓書」に署名した鍵断片(分割鍵)保管者がサーバ要員の指示に従い操作する。

6.2.7 秘密鍵を活性化させる方法

CA 秘密鍵の活性化は合議制操作でサーバ要員が行う。活性化された鍵は表 6-2 に示す期間、活性状態におかれる。

表 6-2 CA 秘密鍵の活性期間

機関	活性化期間
CA 証明書を発行する CA	署名時のみ
加入者証明書を発行する CA	常時(ハードウェア保守などを除く)

6.2.8 秘密鍵を非活性化させる方法

CA 秘密鍵の非活性化は合議制操作でサーバ要員が行う。

6.2.9 秘密鍵を破壊する方法

CA 秘密鍵は鍵の有効期間が満了した場合もしくは鍵の使用中止した場合(CA の終了時の処置)、すみやかに破壊する。 秘密鍵の破壊は暗号化装置については完全な初期化を行うものとする。この初期化は、合議制操作でサーバ要員が行う。また、鍵断片(分割鍵)トークンは物理的に破壊する。 作業は第三者組織の立会者のもと、鍵断片(分割鍵)保管者が行う。 立会者および鍵断片(分割鍵)保管者は「鍵破壊の宣誓書」に署名する。

加入者の秘密鍵は鍵の有効期間が満了した場合、すみやかに破壊すること。

6.2.10 秘密鍵のキーリカバリ

加入者（発行パターン 2/3）で、鍵回復サービスを利用したものは合議制操作で回復を行う。

6.3 鍵ペア管理のその他の面

6.3.1 公開鍵のアーカイブ

CA 公開鍵のアーカイブは改竄を防止する措置をとる。 アーカイブ期間については表 6-3 に示す。

表 6-3 CA 公開鍵のアーカイブ期間

機関	アーカイブ種別	アーカイブ期間
RCA	自証明書	証明書有効期間満了から 10 年
	発行証明書	証明書有効期間満了から 10 年
ICA/SCA	自証明書	証明書有効期間満了から 10 年
	発行証明書	証明書有効期間満了から 10 年

6.3.2 公開鍵と秘密鍵の使用期間

公開鍵と秘密鍵の有効期間を表 6-4 に記す。

表 6-4 鍵使用期間

機関	鍵種類	公開鍵使用期間	秘密鍵使用期間
RCA	証明書・CRL 署名鍵	21 年	10 年
ICA/SCA	証明書・CRL 署名鍵	21 年以内	10 年以内
加入者	Web サーバ証明書	1 年 30 日以内	1 年
加入者	長期間証明書	11年以内	11 年以内
加入者	（上記以外）	6 年以内	6 年以内

6.4 活性化データ

CA では PIN とパスワードによって管理する。

6.4.1 活性化データの生成と組み込み

PIN、パスワードは英文字と数字を含む 8 文字以上の長さを使用する。

6.4.2 活性化データの保護

パスワードは、システム上に 1 方向関数による暗号文の形式で保管する。 パスワードの有効期限は 2 日以上 30 日以内とし、定期的にパスワード変更を行う。 PIN はハードウェアモジュールやトークン内に保管され、外部へは取り出せない。

6.5 コンピュータのセキュリティ管理

6.5.1 特定のコンピュータセキュリティの技術的なリクワイアメント

CA が使用するコンピュータシステムは米国国防総省の基準 : Trusted Computer System Evaluation Criteria（オレンジブック）に示される C2 レベルに準拠しているものを使用する。

6.5.2 コンピュータセキュリティの評価

CA のコンピュータシステムセキュリティを評価するためクラッキングテストなどを随時実施する。

6.6 ライフサイクルの技術的な管理

6.6.1 システム開発の管理

CA で採用するシステムは信頼できる組織で開発、テストされたことが証明できるものを使用する。

6.6.2 セキュリティマネジメント管理

CA では定期的なワクチンソフトの適用により、ウイルス感染の予防、検出、回復を行う。

6.7 ネットワークのセキュリティ管理

CA 証明書を発行する CA はネットワークに接続しない。 加入者証明書を発行する CA とインターネットの接続はファイアウォールを介して行う。 ファイアウォールでは不正アクセスを監査証跡として取得する。随時外部機関によるネットワークアタックテストを実施する。

ネットワークベース IDS を使用し不正アクセスを防止する。

6.8 暗号化モジュール工学管理

CA で使用するハードウェア暗号化装置は FIPS140-1 レベル 3 に対応する。

7. パブリックサービスの証明書とCRLのプロファイル

SecureSign の証明書と CRL の形式、属性の仕様は、おもに世界的な技術標準や標準化団体で決められた以下の標準仕様を参考に定義している。

(1)ITU-T Recommendation X.509(1997E)

(2)RFC2459 Internet X.509 PKI Certificate and CRL Profile, January1999

標準仕様は現在も改版作業が続けられており、今後決定されるであろう標準仕様に対して、その対応状況を考慮して準拠して行く方向である。

SecureSign の証明書と CRL のプロファイルの一覧を表 7-1、表 7-2 に示す。

表 7-1 証明書プロファイル

No.	フィールド名(field name)	オブジェクト識別子(OID)	設定 *1			説明
			V1 の CA 証明書	V3 の CA 証明書	V3 の加入者証明書	
証明書基本部(Certificate Basic Fields)						
1	バージョン(version)		V1	V3	V3	
2	シリアル番号(serialNumber)		◎	◎	◎	
3	署名(signature)		◎	◎	◎	
4	発行者(issuer)		◎	◎	◎	
5	有効期間(validity)		◎	◎	◎	
6	所有者(subject)		◎	◎	◎	
7	所有者公開鍵(subjectPublicKeyInfo)		◎	◎	◎	
8	発行者一意 ID(issuerUniqueID)		×	×	×	
9	所有者一意 ID(subjectUniqueID)		×	×	×	
証明書標準拡張部(certificate Standard Extensions)						
10	認証局鍵識別(authorityKeyIdentifier)	2.5.29.35	―	○	◎	
11	所有者鍵識別(subjectKeyIdentifier)	2.5.29.14	―	◎	○	
12	鍵種別(keyUsage)	2.5.29.15	―	◎	◎	公開鍵の使用目的
13	拡張鍵種別(extendedKeyUsages)	2.5.29.37	―	○	○	KeyUsage 以外の使用目的
14	秘密鍵有効期間(privateKeyUsagePeriod)	2.5.29.16	―	×	×	秘密鍵の有効期限
15	証明書ポリシー(certificatePolicies)	2.5.29.32	―	○	○	CA のポリシー
16	ポリシーマッピング(policyMappings)	2.5.29.33	―	○*2	×	他認証ドメインのポリシーとの対応関係
17	所有者別名(subjectAltName)	2.5.29.17	―	○	○	subject の代替名
18	発行者別名(issuerAltName)	2.5.29.18	―	×	×	issuer の代替名
19	基本制約(basicConstraints)	2.5.29.19	―	◎	○	証明書が CA 用かどうか
20	名前制約(nameConstraints)	2.5.29.30	―	○	×	下位証明書の名前空間の制限
21	ポリシー制約(policyConstraints)	2.5.29.36	―	○	×	下位証明書のポリシーの制限
22	CRL 分配点(cRLDistributionPoints)	2.5.29.31	―	○	○	CRL の配布場所
23	所有者ディレクトリ属性(subjectDirectoryAttributes)	2.5.29.9	―	×	×	subject の Directory Attribute の値
証明書プライベートインターネット拡張部(certificate Private Internet Extensions)						
24	認証局情報アクセス(authorityInfoAccess)	1.3.6.1.5.5.7.1.1	―	○	○	発行者の情報へのアクセス方法を指定
証明書 Netscape 拡張部(Netscape Standard Extensions)		2.16.840.1.113730.1				
25	netscape-cert-type	.1	―	○	○	証明書利用目的

◎:必須、 ○:選択、 ×:編集しない、 ―:設定の定義なし。

*1: 設定 証明書種類、バージョンによって分類している。

V1 の CA 証明書: X.509Version1 の CA 証明書の場合

V3 の CA 証明書: X.509Version3 の CA 証明書の場合

V3 の加入者証明書: X.509Version3 の加入者(Subscriber)証明書の場合

*2: 相互認証証明書のみ

表 7-2 CRL プロファイル

No.	フィールド名(field name)	オブジェクト識別子(OID)	設定*1			説明
			V1 の CRL	V2 の CA の CRL	V2 の加入者の CRL	
CRL 基本部(CRL Basic Fields)						
1	バージョン(version)		V1	V2	V2	
2	署名(signature)		◎	◎	◎	
3	発行者(issuer)		◎	◎	◎	
4	今回更新日時(thisUpdate)		◎	◎	◎	今回発行した CRL の発効日時
5	次回更新予定(nextUpdate)		◎	◎	◎	次回の CRL の発行予定
6	失効証明書(revokedCertificates)		◎	◎	◎	
	証明書（userCertificate）		◎	◎	◎	失効した証明書のシリアル番号
	失効日時（revocationDate）		◎	◎	◎	証明書の失効日時
CRL 拡張部(CRL Extensions)						
7	認証局鍵識別(authorityKeyIdentifier)	2.5.29.35	－	◎	◎	
8	発行者別名(issureAltName)	2.5.29.18	－	×	×	issuer の代替名
9	CRL 番号(cRLNumber)	2.5.29.20	－	◎	◎	
10	デルタ CRL 識別(deltaCRLIndicator)	2.5.29.27	－	○	○	デルタ CRL のみに設定
11	発行分配点(issuingDistributionPoint)	2.5.29.28	－	○	○	
CRL エントリー拡張部(CRL Entry Extensions)						
12	理由コード(reasonCode)	2.5.29.21	－	◎	○	失効理由
13	保留詳細コード(holdInstructionCode)	2.5.29.23	－	×	○	失効理由が保留のときの詳細説明コード
14	無効日時(invaliditydate)	2.5.29.24	－	○	○	証明書の無効日時(省略時は今回更新日時)
15	証明書発行者(certificateIssure)	2.5.29.29	－	×	×	

◎:必須、 ○:選択、 ×:編集しない、 －:設定の定義なし。
*1: 設定 CRL 種類、バージョンによって分類している。
V1 の CA の CRL: X.509Version1 の CA の CRL の場合
V2 の CA の CRL: X.509Version3 の CA の CRL の場合
V2 の加入者の CRL: X.509Version3 の加入者(Subscriber)の CRL の場合

7.1 各フィールドの設定者と設定値

証明書/CRL の各フィールドの内容は RA もしくは CA が設定する。設定内容は証明書種類ごとに個別に管理する。

各フィールドの設定者と設定値説明を表 7-3、表 7-4 に示す。

V3 証明書/V2CRL の拡張部では各フィールドにクリティカル指定(criticality)を行うが、個別の説明に記述が無い限りノンクリティカル（認識できないときは無視する）を指定する。

V3 証明書/V2CRL の拡張部の各フィールドの実際のエンコーディングの順序(sequence)は CA が設定する。

設定コードは、現状の利用プロダクトの対応状況からみて ASCII に準ずる 1 バイト系の設定コードで設定を行う。日本語コードの設定は UNICODE、エンコーディングは UTF8String を推奨する。

表 7-3 証明書フィールドの設定者と設定値説明

No.	フィールド名(field name)	設定者			設定値説明
		V1 の CA 証明書	V3 の CA 証明書	V3 の 加入者 証明書	
証明書基本部(Certificate Basic Fields)					
1	バージョン(version)	CA	CA	CA	下位に ICA もしくは SCA を認証する RCA の場合のみ V1 を設定してもよい。その他は V3 を設定する。
2	シリアル番号(serialNumber)	CA	CA	CA	128 ビット以下の正の整数
3	署名(signature)	CA	CA	CA	RSA with SHA-1、または、RSA with MD5
4	発行者(issuer)	CA	CA	CA	7.1.1 参照
5	有効期間(validity)	CA	CA	RA	開始日時と終了日時を秒単位で設定
6	所有者(subject)	CA	CA	RA	7.1.1 参照
7	所有者公開鍵(subjectPublicKeyInfo)	CA	CA	RA	RSA 公開鍵(512～2,048 ビット)
8	発行者一意 ID(issuerUniqueID)	×	×	×	
9	所有者一意 ID(subjectUniqueID)	×	×	×	
証明書標準拡張部(certificate Standard Extensions)					
10	認証局鍵識別(authorityKeyIdentifier)	—	CA	CA	公開鍵の SHA-1 または、issuer の DN とシリアル番号
11	所有者鍵識別(subjectKeyIdentifier)	—	CA	RA	公開鍵の SHA-1
12	鍵種別(keyUsage)	—	CA	CA	7.1.3 参照
13	拡張鍵種別(extendedKeyUsages)	—	CA	CA	7.1.4 参照
14	秘密鍵有効期間(privateKeyUsagePeriod)	—	×	×	
15	証明書ポリシー(certificatePolicies)	—	CA	CA	7.1.5 参照
16	ポリシーマッピング(policyMappings)	—	CA	×	7.1.6 参照
17	所有者別名(subjectAltName)	—	CA	RA	7.1.2 参照
18	発行者別名(issuerAltName)	—	×	×	7.1.2 参照
19	基本制約(basicConstraints)	—	CA	CA	7.1.7 参照
20	名前制約(nameConstraints)	—	CA	×	7.1.8 参照
21	ポリシー制約(policyConstraints)	—	CA	×	7.1.9 参照
22	CRL 分配点(cRLDistributionPoints)	—	CA	CA	7.1.10 参照
23	所有者ディレクトリ属性(subjectDirectoryAttributes)	—	×	×	
証明書プライベートインターネット拡張部(certificate Private Internet Extensions)					
24	認証局情報アクセス(authorityInfoAccess)	—	CA	CA	7.1.11 参照
証明書 Netscape 拡張部(Netscape Standard Extensions)					
25	netscape-cert-type	—	CA	CA	7.1.12 参照

CA: CA が設定、 RA: RA が設定(ただし CA ポリシーで CA が優先設定するポリシーもある)、 ×:編集しない、 ー:設定の定義なし。

表 7-4 CRL フィールドの設定者と設定値説明

No.	フィールド名(field name)	設定		設定値説明
		CA の CRL	加入者 の CRL	
CRL 基本部(CRL Basic Fields)				
1	バージョン(version)	CA	CA	V1 または V2
2	署名(signature)	CA	CA	RSA with SHA-1、または、RSA with MD5
3	発行者(issuer)	CA	CA	7.1.1 参照
4	今回更新日時(thisUpdate)	CA	CA	UTCTime 形式で秒単位で設定
5	次回更新予定(nextUpdate)	CA	CA	UTCTime 形式で秒単位で設定
6	失効証明書(revokedCertificates)	—	—	
	証明書(userCertificate)	CA	RA	証明書のシリアル番号
	失効日時(revocationDate)	CA	CA	UTCTime 形式で秒単位で設定
CRL 拡張部(CRL Extensions)				
7	認証局鍵識別(authorityKeyIdentifier)	CA	CA	公開鍵の SHA-1 または、issuer の DN とシリアル番号
8	発行者別名(issureAltName)	×	×	
9	CRL 番号(cRLNumber)	CA	CA	128 ビット以下の正の整数
10	デルタ CRL 識別(deltaCRLIndicator)	CA	CA	デルタ CRL の場合に設定する

11	発行分配点(issuingDistributionPoint)	CA	CA	間接 CRL(indirect CRL)の場合のみ使用する
CRL エントリー拡張部(CRL Entry Extensions)				
12	理由コード(reasonCode)	CA	RA	
13	保留詳細コード(holdInstructionCode)	×	RA	
14	無効日時(invalidityDate)	CA	CA	
15	証明書発行者(certificateIssure)	×	×	

CA: CA が設定、 RA: RA が設定(ただし CA ポリシーで CA が優先設定するポリシーもある)、 ×:編集しない、 ー:設定の定義なし。

7.1.1 名称の形式(Name forms)

ITU X.500 シリーズ定義の識別名(DistinguishedName)として指定する。実際には PKIX(RFC2459)および LDAP(RFC2256)の RFC で定義された属性の組み合せ(表 7-5)で定義する。各属性のエンコーディングの順序(sequence)は CA が設定する。

表 7-5 証明書プロファイル

No.	属性名(Attribute Name)	オブジェクト識別子(OID)	設定 *1		最大設定数	説明
			CA 名	加入者名		
1	国名(CountryName, c=)	2.5.4.6	◎	◎	1	
2	都道府県(stateOrProvinceName, st=)	2.5.4.8	×	○	1	
3	市町村(localityName, l=)	2.5.4.7	×	○	1	
4	組織名(organizationName, o=)	2.5.4.10	◎	○	1	CA 名のとき→'o=Japan Certification Services, Inc.' または'o=Japan Certification Services' 加入者名のとき→'SecureSignN' (N=1,2,3,…) または加入者(顧客)指定値
5	部門名(organizationalUnitName, ou=)	2.5.4.11	○	○	5	
6	固有名称(CommonName, cn=)	2.5.4.3	◎	◎	1	CA 名または加入者名を設定する。 上位階層からみて唯一値であること。
7	Email(EmailAddress, e=)	1.2.840.113549.1.9.1	×	○	1	PKIX では推奨していないが、加入者用 S/MIME 証明書の場合のみ設定してもよい。

◎:必須、 ○:選択、 ×:編集しない、 ー:設定の定義なし。
*1: 設定: CA の設定該当フィールド→CA 証明書の所有者／発行者フィールドが設定対象
加入者の設定該当フィールド→加入者証明書の所有者フィールドが設定対象

7.1.2 汎用名(GeneralName)

別名で設定する汎用名は X.509 で複数の定義(ASN.1)の選択と定義されており、この設定に関して表 7-6 に示す。証明書の種類によっては必須設定項目になる。

加入者証明書において設定され、設定内容の設定者は RA である。

表 7-6 汎用名(GeneralName)の設定

No.	ASN.1 定義型	設定	設定者	説明
汎用名(GenaralName)				
1	otherName 型	×	-	
2	rfc822Name 型	○	RA	Email アドレス等を設定する。
3	dNSName 型	○	RA	DNS 名等を設定する。
4	x400Address 型	×	-	
5	directoryName 型	○	RA	LDAP 参照等を設定する。
6	ediPartyName 型	×	-	
7	uniformResourceIdentifier 型	○	RA	URL 等を設定する。
8	iPAddress 型	○	RA	IP アドレスを設定する。
9	registerdID 型	×	-	

○:選択、 ×:編集しない。

7.1.3 鍵種別(KeyUsage)

最低一つのビットを ON する。keyCertSign は CA 証明書の場合のみ ON できる。

7.1.4 拡張鍵種別(extendedKeyUsage)

RFC2459 定義または業界標準のオブジェクト識別子(OID)を指定する。鍵種別と矛盾する指定を行わない。クリティカル指定はクリティカルを指定することもある。

7.1.5 証明書ポリシー(certificatePolicies)

表 1-1 で定めるオブジェクト識別子(OID)と証明書の利用規程を定めた文書(注 1 参照)を公開した URL を指定する。

注1）RFC2459 では CPS を推奨しているが、パブリックサービスでは依存者の利便性を考えて CPS より利用者の義務を抜粋した「依存者同意書」を使用する。

7.1.6 ポリシーマッピング(policyMappings)

相互認証証明書のときのみ編集し、相互対応付けを行うオブジェクト識別子ペアを指定する。

7.1.7 基本制約(basicConstraints)

CA 証明書の場合： cA=TRUE、 pathLenConstraint フィールドは省略(無限階層)、または 0(SCA)を設定する。クリティカル指定はクリティカルを指定する。(RFC2459)

加入者証明書の場合： 設定を省略するか、または、cA=FALSE、 pathLenConstraint フィールドは省略する。クリティカル指定はノンクリティカルを指定する。

7.1.8 名前制約(nameConstraints)

SCA の場合（加入者証明書を発行する）、加入者証明書の種類に応じて設定する。設定値は RFC2459 に従う。

7.1.9 ポリシー制約(policyConstraints)

RFC2459 に従う。

7.1.10 CRL分配点(cRLDistributionPoints)

RFC2459 に従う。

7.1.11 認証局情報アクセス(authorityInfoAccess)

RFC2459 に従う。

7.1.12 netscape-cert-type

Netscape 標準に従う。鍵種別、拡張鍵種別と矛盾する設定を行わない。

7.2 証明書/CRLの設定内容の決定までの手続き

証明書の設定内容は以下に示す手順で決定される。

(1) 加入者は RA に対して設定内容を申請する。

(2) RAO は、加入者から要求された申請内容を参考に RA で設定する項目(7.1 節で説明)に対して設定内容を仮決定し CA へ発行を要求する。

(3) CP は、RA サーバから要求された申請内容を参考に全ての項目に対する設定内容を決定する。

CRL の設定内容は以下に示す手順で決定される。

(1) RAO は、失効する証明書を決定し RA で設定する項目(7.1 節で説明)に対して設定内容を仮決定し CA へ発行を要求する。

(2) CP は、RA サーバから要求された失効申請内容を参考に全ての項目に対する設定内容を決定する。また、前回発行 CRL で記載した証明書でその証明書の有効期限が切れていないときは今回の CRL にも記載する。

7.2.1 申請内容の妥当性検査

RAO は、加入者の申請内容が本文書に照らして RA 設定値として妥当かどうかを検査する必要がある。

CP は、発行者(JCSI)と取決めた本文書に照らして RA 設定項目値を検査し、RA の申請値を設定するか、CP で新たに値を設定するか、または申請を拒否する。したがって、7.1 節で RA 設定と定義された項目であっても CP で設定内容を変更することもある。

7.2.2 発行した証明書の設定内容の妥当性検査

RAOもしくは加入者は、発行された証明書の認証内容（設定内容）が本文書の規定に従っているか否かをすみやかに検査し、設定内容が受理できない場合は、すみやかに該当証明書の失効依頼を CA(加入者の場合は RA)に対して行わなければならない。

7.3 各証明書のプロファイル説明

7.3.1 SecureSignパブリックCA証明書

(1)パブリック RCA 証明書

証明書の検証経路のルートとして永続的な信憑性を汎用的に確保することを目的としているため、X.509V1 フォーマットで強暗号(2,048 ビット RSA 鍵)とする。

(2)パブリック ICA 証明書

X.509V3 フォーマットで、拡張部で下位 CA 署名用の属性を設定する。

(3)パブリック SCA 証明書 1(共通利用 CA)

X.509V3 フォーマットで、拡張部で加入者証明書署名用の属性を設定する。 有効期間の長い加入者証明書を発行する SCA(鍵長 2,048 ビット)用の証明書もこの範疇にある。

(4)パブリック SCA 証明書 2(顧客専用 CA)

X.509V3 フォーマットで、拡張部で加入者証明書署名用の属性を設定する。

顧客は証明書の以下のフィールドに顧客情報を JCSI の承認をもとに設定できる。

(a)有効期間

(b)所有者フィールドの o, ou, cn

(c)その他

7.3.2 SecureSignパブリック加入者証明書

(1)パブリック SSL/TLS サーバ証明書

X.509V3 フォーマットで、拡張部で SSL/TLS サーバ証明書用の属性を設定する。

顧客は証明書の以下のフィールドに顧客情報を設定できる。

(a)所有者フィールドの c,st,l,o,ou,cn

(b)RA は、所有者フィールドの cn に所有者が所持するサーバを特定する DNS 名を設定しなければならない。

(2)パブリック SSL/TLS クライアント証明書

X.509V3 フォーマットで、拡張部で SSL/TLS クライアント証明書用の属性を設定する。

顧客は証明書の以下のフィールドに顧客情報を設定できる。

(a)有効期間

(b)所有者フィールドの c,st,l,o,ou(最大 5 個),cn

RA は、RA が設定可能な所有者フィールドの属性に所有者を一意に特定する値を設定しなければならない。

(3)パブリック S/MIME 証明書

X.509V3 フォーマットで、拡張部で S/MIME 証明書用の属性を設定する。

顧客は証明書の以下のフィールドに顧客情報を設定できる。

(a)有効期間

(b)所有者フィールドの c,st,l,o,ou(最大 5 個),cn,e

(c)所有者別名フィールド

RA は、所有者が持つ Email アドレスを所有者フィールドの DN の e（選択）と、rfc822name 型

で所有者別名フィールドに設定しなければならない。

(4)パブリック電子署名用証明書

X.509V3 フォーマットで、拡張部で電子署名用の属性に加え否認防止の属性を設定することができる。

顧客は証明書の以下のフィールドに顧客情報を設定できる。

(a)有効期間

(b)所有者フィールドの c,st,l,o,ou(最大 5 個),cn,

(c)所有者別名フィールド

(5)パブリックタイムスタンプ用証明書

X.509V3 フォーマットで、拡張部で電子署名用の属性と否認防止の属性を設定する。また拡張鍵種別にタイムスタンピング属性を設定する。

顧客は証明書の以下のフィールドに顧客情報を設定できる。

(a)有効期間(6 年と 30 日または 11 年と 30 日)

(b)所有者フィールドの c,st,l,o,ou(最大 5 個),cn

8. 仕様管理

本章は、SecureSign パブリックサービス標準規程(以降、本章では本規程と記述する)の仕様管理について記述するものであり、SecureSign プライベートサービスにおける規程の仕様管理については顧客自身で作成するものとする(顧客は本章を参考にすること、引用することが可能)。
JCSI は、セキュリティを維持するため積極的にセキュリティ技術の最新動向を捕らえて、必要に応じ本規程の仕様変更として反映する。

8.1 仕様変更の手続き、および公表/通知に関するポリシー

JCSI は、顧客(RAO、加入者を含む)や依存者に事前の了解を得ることなく本規程を更改する権利を保有する。本規程更改にあたっては、JCSI 内に設置された仕様管理委員会において更改内容を検討し、その妥当性が確認された後、実施される。 本規程の更改は、更新した本規程を公開するか、または JCSI リポジトリの告知書内に変更告知文書 (本規程の更改部分のみの抜粋版)を公開することで行われる。 この変更告知文書は、本規程の実際の変更と同じ効果をもち、本規程の次版の公開に反映される。 なお、本規程の変更/更改は、変更履歴を表わすバージョン番号と発行日付により識別される。

変更の通知は、JCSI リポジトリに変更告知書または更新後の本規程を公開することにより行うこととする。 仕様変更の発効時期は変更される内容の重要性および緊急性により異なるものとし、JCSI は JCSI のみの裁量により変更の重要性/緊急性について判断を下す権利を保有するものとするが概ね以下の通り。

(1)重要な変更は、通知後、15 日(告知期間)を経て、効力を発する。 顧客(RAO、加入者を含む)や依存者は、JCSI リポジトリを定期的に訪問し、SecureSign サービス仕様の追加や変更について理解しなければならない。 告知期間中に JCSI は、JCSI リポジトリの告知書にその旨掲示することにより、変更を中止することもあり得る。

(2)緊急を要する重要な変更は、通知後、即、効力を発する。ここで、緊急とは、当該変更を直ちに実施しない限り、SecureSign サービスの一部ないし全体が危殆化するような恐れがあるときをいう。

(3)重要でない変更は、通知後直ちに発効する。.

8.2 公表および通知に関するポリシー

8.1 節に含まれる。

8.3 仕様認可の手続き

本規程の更改が行われた場合、加入者の証明書発行時期に拘らず当社リポジトリに掲載されている更改後の規程が適用される。 JCSI が行った個々の仕様変更に対して顧客(RAO、加入者を含む)は、証明書の失効を申請しない限り、変更に同意したとみなされる。 また、依存者はこの変更に同意できない場合は、入手した証明書の使用を中止する。

8.4 本規定の保存

JCSI は、SecureSign パブリックサービスが継続されている間、更改された本規定の各版を保存する。

付録A SecureSignサーバサービス

A1. はじめに

SecureSign サーバサービス（以下本付録内で本サービスと略記する）は、Web サーバの存在を認証する電子証明書を発行するサービスである。JCSI は、顧客のサーバ証明書発行申請に伴い、当該 Web サイトが一意に存在することを確認して、当該 Web サーバに SSL v3 対応 Web サーバ証明書を発行する。そのために SecureSign パブリックルート CA の配下に SCA を設ける。SecureSign の定義に従えば、証明書を発行された Web サーバが加入者であり、当該サーバ証明書を利用する人が依存者である。しかし、本付録では、Web サーバ証明書発行申請を行う顧客自身[注 1)]、または顧客組織内の Web サーバの運営実務に責任を持つ人[注 2)]を加入者と呼ぶ。

本編で述べている SecureSign パブリックサービスでは、JCSI の委任にもとづき顧客が RA を運営する。本サービスでは、JCSI が RA を運営する。JCSI は、本付録において JCSI の本サービスに係る RA の運営について規定する。また、加入者の義務について定める。JCSI の認定にもとづき、本サービスを加入者に仲介する第三者は、本付録で規定する加入者の義務をいかなる変更もすることなく JCSI に代わって加入者に履行させることができなければならない。

注 1)「Web サーバ証明書 申込み書」の中では、お客様と称する。

注 2)「Web サーバ証明書 申込み書」の中では、証明書申請管理者と称する。

A2. 一般条項

A2.1 義務

本サービスでは他の SecureSign パブリックサービスとは異なり、JCSI が発行者ならびに RA の義務を負い、顧客が加入者の義務を負う。以降本節では、この本サービスの特徴を踏まえた義務条項を記述する。

A2.1.1 CAの義務

CA は、以下に示す原則のもと証明書を発行し運用するものとする。本サービスでは、発行者、作成局の運用主体、RA(RAO を含む)運用主体はすべて JCSI である。 したがって、CA の義務は JCSI の義務である。

(1)作成局(CP)の義務として、発行者(JCSI)の署名鍵(秘密鍵)をセキュアに生成し、管理するものとする。

(2)RA の要求にもとづきサーバ証明書の発行を行う。

(3)CRL、および証明書発行に関連するその他の情報をすみやかにリポジトリ上に公開する。

(4)RA と協調して証明書ライフサイクル管理を行う。

(5)RA の要求にもとづきサーバ証明書を失効させ、CRL を発行する。

A2.1.2 RAの義務

本節において、RA は、その管理者(RAO)を含むものとする。なお、RA の操作にかかわる義務について、RAO の義務と記述する場合がある。本サービスでは、RA は JCSI が運用する。 したがって、以下の義務は、JCSI の義務である。

(1)RAO は、証明書申請を適正に検証しなければならない。

(2)RAO は、証明書に記載しようとする加入者固有名称の値の一つである DNS 名の実在性を検証しなければならない。

(3)RAO は、証明書申請に組織名等を含む場合、組織情報の妥当性を検証しなければならない

(4)RA は RA サーバをセキュアな環境に設置し、運用する義務がある。

(5)RAO は、証明書申請者の身元確認を行わなければならない。 また、鍵の生成から証明書の Web サーバへの組み込みを行う証明書申請管理者および証明書申込み者(お客様)の身元確認を行わなければならない。

(6)RAO は加入者の証明書を失効させる場合、失効の妥当性の確認を行わなければならない。その確認は必要に応じて申請者の身元確認および意思確認を含む。

(7)証明書申請書には証明書に記載されない項目内容を含むことができる。この場合、RA には申請書の中で証明書に反映されないデータは、秘密情報として取り扱う義務がある。

(8)CA と協調して証明書ライフサイクル管理を行う。

A2.1.3 KRS義務

本サービスでは KRS サービスを提供しない。

A2.1.4 加入者の義務

本サービスの場合、加入者は顧客に等しい。

(1)正確な証明書申請内容の提示

証明書を取得する際、RA に提示する証明書申請内容は、加入者の現状を正確に表したものでなければならない。

(2)証明書利用制限

証明書はその用途範囲、セキュリティドメイン、損害賠償などを記載した本文書にもとづいて発行されている。加入者はその範囲外の用途に、証明書を提示してはならない(サーバ証明書として以外使用してはいけない)。

(3)依存者の証明書利用についての承知義務

加入者の証明書を使った依存者からの暗号文について、JCSI は、その証明書がどのような取引において使用されるか、また特定の用途、局面に適合しているか、などの審査、確認を行っていない。またパブリックサービスの性格上、依存者は何ら限定されていないことについて加入者は承知しなければならない。

(4)鍵などの管理義務

加入者は、自身の使用するソフトウェアおよびハードウェア等で鍵対（秘密鍵と公開鍵のペア）を生成し、公開鍵を提出し、RA から証明書を受け取る。依存者に確実な情報を伝えるために、加入者には以下の管理義務が課される。

(a)秘密鍵の秘匿管理

生成した秘密鍵が、加入者以外によって使用、複写、バックアップされてはならない。そのために、たとえば Web サーバの権限管理、資格管理なども充分な注意をもって管理しなければならない。使用、複写、バックアップが不正に行われた可能性がある場合は、加入者は失効申請を行わなければならない。

(b)鍵対の対応管理

秘密鍵と証明書内公開鍵との対応関係が不正と判断される場合には、加入者は失効申請を行わなければならない。

(5)証明書記載事項の管理

加入者は発行された証明書の記載事項を受領時に確認し、かつその後も使用前に随時、加入者の現状に照らして確認しなければならない。加入者は証明書受領時にその記載事項が加入者の現状に合わなかった場合、または証明書受領後にその記載事項が加入者の現状に合わなくなった場合は、すみやかに失効申請を行わなければならない。

(6)すみやかな失効申請

上記(4)-(a)、(b)、(5)の各事項について、失効申請はすみやかに行わなければならない。

(7)RAO とのコンタクト維持

加入者は上記各事項について、詳細は RAO の判断に従わなければならない。また、失効申請は RAO を経由して行わなければならない。したがって、加入者は RAO とのコンタクトを常時維持する必要がある。

A2.1.5 依存者の義務

依存者は、リポジトリにて公開される本サービス用「依存者同意書」に同意しなければならない。そこに明記されているように、依存者は、取引相手である加入者の証明書の有効性についてチェックしなければならない。

(1)証明書利用制限

証明書はその目的、適用範囲、加入者認証の方法、損害賠償などを記載した本文書にもとづいて運用されており、依存者はこれらを理解し、承認した上で証明書を利用しなければならない。Web サイトから提示された証明書は、当該サイトと依存者との間での暗号通信と依存者のサーバ認証の目的で使用される。それ以外の目的で証明書が利用されていると判断される場合に依存者はその証明書を使用してはいけない。

(2)証明書の有効性確認義務

証明書を利用する際には有効性確認を行わなければならない。 有効性確認内容には以下を含まなければならない。

(a)証明書パス上の全証明書について以下を確認すること。なお、パブリックサービスの場合、JCSI のルート証明書を信頼することが前提となる。

・証明書が改ざんされていないこと

・有効期間内であること

・失効していないこと注)

・上記(1)の証明書使用目的が正しいこと

(b)サーバ証明書の署名を検証すること

(c)提示された証明書記載項目が、A7 章記載の規定に合致していること。

注)失効情報は、JCSI リポジトリ上の CRL 分配点情報から得ることができる。

(3)SecureSign パブリックルート証明書の組み込み

一部の PKI アプリケーションソフトウェアには SecureSign パブリックルート証明書が組み込まれていないものがある。これらのアプリケーションを使用するには SecureSign パブリックルート証明書を Trusted 証明書として組み込むことができる。組み込みに際しては SecureSign パブリックルート証明書のハッシュ値（SHA-1、MD5）が JCSI の Web サイトにて公開されているので、依存者は組み込むパブリックルート証明書のハッシュ値と比較検証しなければならない。

A2.1.6 リポジトリの義務

本サービスは、本編 2.1.6 項に従う。

A2.2 責任

本サービスを顧客に提供するJCSIは、認証局(CA)、登録局(RA)とその管理者(RAO)を含んで責任を持つこととする。その責任について以下の様に定める。

A2.2.1 JCSIの責任

(1)JCSIは、本サービスにつき、以下のことを保証する。

- JCSI 自らが、A3 章に従って加入者の真偽確認を厳密に実施する。その後加入者からの証明書申請内容(証明書のサブジェクト識別名等)を正確に反映した証明書を発行すること。
- A4 章に従い、パブリックサービスで発行するCRLについて、システム保守などの理由による一時停止、緊急やむを得ない場合の停止を除き、作成後、定期的にJCSIリポジトリに登録し、失効対象証明書の有効期間が満了するまで公開し続けること。
- 失効申請を適正に審査し、失効申請があった加入者の証明書について確実に失効処理を行うこと。
- 本編 5 章、および 6 章に従い、証明書発行システムを運用し、すべての認証局の秘密鍵について、公開鍵から類推・算出されるような場合を除き盗難等による危殆化が無いこと。
- 証明書、CRL の形式、属性が、それぞれの証明書の発行時点における本編 7 章、A7 章記載の規定に合致していること。
- 加入者の審査の対象となった書類を含む各種の文書、書類を、JCSI で定める期間、滅失、改竄などの惧れのない方法で保管すること。

(2) (1)項にかかわらず、JCSIは、以下のいずれかの場合には、加入者(顧客)に通知することなく、一時的に本サービスの全部または一部の提供を中断することができるものとする。

- JCSI が保有する本サービス用の設備につき、緊急に保守を行う場合
- 火災、停電等により本サービスの提供ができなくなった場合
- 地震、噴火、洪水、津波等の天災により本サービスの提供ができなくなった場合
- 戦争、動乱、暴動、騒乱、労働争議等により本サービスの提供ができなくなった場合
- その他、運用上、技術上、または顧客との契約の履行上、JCSI が本サービスの提供の一時的な中断が必要と判断した場合

(3)JCSI が本サービスに関し顧客、加入者ならびに依存者に対して負う責任は、(1)～(2)に定める範囲に限られるものとする。

A2.2.2 顧客の責任

本サービスでは、顧客は加入者に同義である。したがって、顧客は、A2.1.4 項の加入者の義務を果たす責任がある。

A2.3 財務上の責任

本サービスは本編 2.3 節に従う。

A2.4 解釈および執行

本サービスは本編 2.4 節に従う。

A2.5 料金

本サービスは本編 2.5 節に従う。

A2.6 公表およびリポジトリ

失効情報は JCSI リポジトリ上の CRL 分配点情報から得ることができる。

以上の点を除き、本サービスは本編 2.6 節に従う。

A2.7 準拠性監査

本サービスは本編 2.7 節に従う。

A2.8 秘密保持

本サービスは本編 2.8 節に従う。

A2.9 知的財産権

本サービスは本編 2.9 節に従う。

A2.10 個人情報保護

本サービスは本編 2.10 節に従う。

A3. 同一性の確認と認証

本サービスにおける、証明書発行申込み(「Web サーバ証明書 申込み書」)から発行までの手順は A.4.2 節に記載する。この一連の手順の中での、Web サイトの同一性の確認と認証は JCSI（RAO）が行う。ここでの同一性の確認と認証は

- 証明書申請管理者が、当該 Web サイトの管理資格があるかの確認。
- 証明書申込み者(お客様)が証明書申請管理者に認証されていることの確認。
- 申込み書中の証明書に反映記載される項目（証明書申請登録情報）が当該 Web サイ トの実体を表しているかの検証(たとえば、加入者組織の存在、DNS 名の実存と所有者の確認)。
- 申込み書に記載された証明書申請登録情報と、証明書要求(CSR)の情報が一致すること。

等と、JCSI は規定する。なお、確認/認証の方法についは JCSI 内部規定に従う。

(注 1)「Web サーバ証明書 申込み書」は JCSI リポジトリからダウンロードできる。
(注 2) 負荷分散装置や SSL アクセラレータを用いて同一サーバ名（Common Name）で複数の Web サーバを運用する場合、サーバ証明書は Web サーバ台数分必要である。

A3.1 初期登録(初期申請)

A3.1.1 名称のタイプ

「Web サーバ証明書 申込み書」の証明書登録申請情報を参照。

A3.1.2 名称に意味がある必要

当該 Web サイトの実体を正しく表している必要がある。このために「Web サーバ証明書 申込み書」にはその実体を反映し申請する義務が、加入者に生じる。

A3.1.3 さまざまな名称の形式を解釈するためのルール

加入者の設定ルールに従う。

A3.1.4 名称のユニークさ

サーバ証明書に記載される識別名を構成する各項目は加入者の実体を正確に表したものでなければならない。識別名全体で認識される当該サーバはユニークに認識されなければならない。
(注)たとえば同一サーバ名（CommonName）に対して複数のサーバ証明書を取得する場合、サーバ証明書ごとに部門名(OrganizationalUnitName)を変更する。

A3.1.5 名称要求の紛争決着の手続き

名称要求の紛争とは、サーバ証明書に記載される識別名にかかわる何らかの紛争を意味する

（権利/名声侵害、営業妨害、不正競合、不法使用、等）。
加入者のドメイン（サーバ証明書を実装するサーバが属するドメイン）内での名称要求の紛争は、ドメイン内で解決することを原則とする。ドメインをまたがる紛争、もしくは依存者が関係する紛争は、当事者(加入者、依存者)間で解決することを原則とする。いずれの場合も JCSI は紛争にかかわる当事者とはならない。

A3.1.6 商標の認識、認証、および役割

証明書に記載されるサーバの識別名は、第三者の商標を含む一切の知的財産権を侵害しないことが保証されていなければならない。これは証明書記載内容を申請する加入者に保証責任があり、これらの侵害または妨害行為から生ずべき損害の一切から JCSI は免責されるものとする。

A3.1.7 秘密鍵の所有を証明する方法

証明書要求(CSR)は、公開鍵に対応する秘密鍵で署名されていることを前提とする(PKCS＃10 での申請が原則)。

A3.1.8 組織の同一性の認証

加入者の属する組織を確認するために JCSI（RAO）は、加入者に組織の存在証明書(登記事項証明書、等)の提示を求めることがある。

A3.1.9 個人の同一性の認証

A3 節序文で記した同一性の確認のために JCSI（RAO）は A3.1.8 項で記した 組織の存在証明書、ならびに証明書申請管理者の組織所属証明書(社員証、職員証、等)の提示を求めることがある。また、鍵の生成/登録からサーバ証明書の実機への組み込み等の実作業を担う個人(お客様)も証明書申請項目として必須であり、この個人の同一性の認証も証明書申請管理者のそれと同様に JCSI が行う。

A3.2 証明書の更新に伴う鍵更新

初期登録に同じ。

A3.3 失効後の鍵更新

初期登録に同じ。

A3.4 失効要請

JCSI（RAO）は、サーバ証明書の失効要請は証明書申込み者(お客様)または証明書申請管理者からのみ受け付ける。 失効申請者の同一性確認のために A3.1.8 項、A3.1.9 項で記した 証明書類の提示を JCSI は、失効申請者に求めることがある。

A4. 運用上の要件

A4.1 証明書の申請、発行、および受領

本サービスは本編で規定されている 8 タイプのサービス(A-1～D-2)のいずれとも異なる。本サービスのサービスタイプ、リポジトリ設置、発行パターンは以下のように規定される。

表 A4-1 Web-server certificate 発行サービス(設置先と運営主体)

タイプ	RCA	ICA	SCA	CAO	RA	RAO	リポジトリ	鍵回復
SecureSign サーバ サービス	JCSI 設置 JCSI 運営	―	JCSI 設置 JCSI 運営	JCSI 設置 JCSI 運営	JCSI 設置 JCSI 運営	JCSI 設置 JCSI 運営	JCSI 設置 JCSI 運営	×

表 A4-2 リポジトリの設置場所と CRL の開示ならびに検証方法

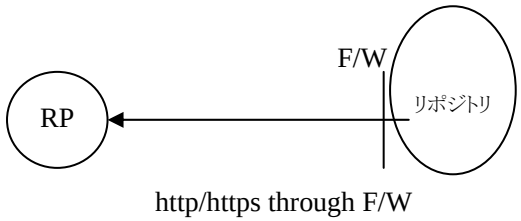
No.	リポジトリ設置場所	形態概要	適用可能サービスタイプ	リポジトリの種類	依存者の検証時参照リポジトリ
4	JCSI		SecureSign サーバ サービスを含む SecureSign パブリック サービス	SecureSign パブリックリポジトリ	http で SecureSign パブリックリポジトリを直接参照

表 A4-3 発行パターン

	加入者	RA	CA	リポジトリ
パターン1	鍵生成 → 申請 (含む失効) 保存 ←	審査 → 発行要求 → ← 配付	発行 ⇢ 配付 ↓	登録 (CRL)

発行パターン	発行契機	加入者用鍵生成	審査方法		
			自動	事前	マニュアル
1	証明書 ： 加入者トリガー CRL ： RAO トリガー	加入者	×	×	○

本サービスでの証明書の発行申請は

(1)加入者は JCSI の Web 上の問い合わせページに仮申込みを行う。

(2)JCSI は、仮申込みの内容を吟味し加入者に対して正式申込み書、ならびに申請に必要な書類の提出指示を行う。

(3)加入者は、Web サーバ申込み書(JCSI の Web からダウンロード)に必要事項を記入し、必要書類とともに JCSI へ郵送する。

(4)JCSI は、Web サーバ申込み書と添付書類を JCSI の規程により審査し、不適合が無ければ契約の成立とする。不都合がある場合は、書類の再提出を加入者に催促する。

(5)加入者による鍵生成～証明書要求(CSR)作成～申請（加入者→RAO）。

(6)JCSI による証明書申請(CSR)のマニュアル審査(RAO 操作)。

(7)JCSI RAO 操作による証明書発行依頼～CA による証明書発行(RAO 受領)。

(8)加入者に対する証明書送付（加入者←RAO）。

の手順で実施される。

A4.2 証明書の一時停止と失効

本サービスにおいても、識別名などの記載事項の変更、証明書の他の証明書への置き換え、加入者による使用停止、加入者の秘密鍵の危殆化、SCA 証明書署名鍵の危殆化などの事象が生じると、該当証明書は失効させられる。 証明書の一時停止処理は、現状実装していない。

失効の手続きは、通常、加入者の JCSI 内 RAO への要請により開始し、JCSI 内 RAO により失効の是非が吟味され、失効処理要求が CA により受理される。証明書失効リスト（CRL）は、定期的に公開される。

A4.3 セキュリティ監査の手続き

本サービスは本編 4.3 節に従う。

A4.4 アーカイブ

本サービスは、本編 4.4 節に従い、さらに以下を追加する。

- 加入者からの証明書発行申請に伴い提出される、申込み書原本、および添付される書類。（証明書の有効期間満了後 10 年間）
- 加入者などからの証明書失効申請に伴い提出される、申請書など、JCSI または顧客が失効判断に用いた書類一式。（証明書の有効期間満了後 10 年間）
- 加入者に公開される案内書、加入者同意書、依存者に公開される依存者同意書、それらの変更履歴。（最新版は永久、改版後の旧版は改版後 10 年間）

A4.5 鍵の交換

本サービスは、本編 4.5 節に従う。

A4.6 危殆化と災害からの回復

本サービスは、本編 4.6 節に従う。

A4.7 CAの終了

本サービスは、本編 4.7 節に従う。

A5. 物理的、手続き的、人事的セキュリティ管理

本サービスは本編 5 章に従い、以下を追加規定する。

A5.1 物理的セキュリティ管理

SecureSign サービスではサーバ（CA、およびタイプ A-1, B-1, C-1, D-1 では RA。以下本章内で同様）は、セキュアな施設の外部（JCSI 本部）から業務運用される。JCSI は、この JCSI 本部からの総ての運用操作に関するセキュリティを以下のように定める。

(1)総てのアクセスはサーバによってクライアント認証される。
(2)クライアント証明書はスマートカード媒体に格納され、PIN で保護される。
(3)各媒体に所有者（RAO）が定められ、文書に記録される。
(4)総てのアクセスは盗聴防止のために充分な強度の暗号通信が適用される。
(5)総ての運用操作に合議制操作が適用される。
(6)総てのアクセスは監査証跡として、サーバ側に記録される。
(7)JCSI 本部の端末設置場所は、鍵付きのドアにより出入りを限定された場所とする。この場所は消防法の規定範囲内で外部からの侵入防止措置を施す。この場所への出入りは任命された要員に限定される。またドアの施錠は閉扉時自動施錠、入退室はその度に帳簿に記録するものとし、PKI 運営管理者が毎月監査するものとする。

A5.2 手続き的セキュリティ管理

JCSI は、表 A5-1 に示すように要員区分を設定する。センタ要員および本部要員は、CA および JCSI に設置される RA ならびに JCSI のリポジトリを操作する。

表 A5-1 要員別権限

<table>
<tr><th colspan="2">要員区分</th><th>指名</th><th>入室権限付与</th><th>操作権限付与</th><th>アクセス権限チェック方式</th></tr>
<tr><td colspan="2">PKI 運営管理者</td><td>JCSI 本部およびセンタごとに指名され、権限付与される</td><td colspan="2">－</td><td>－</td></tr>
<tr><td colspan="2">セキュリティ管理者</td><td>同上</td><td>あり</td><td>－</td><td>ID カードシステム、
生体認証システム</td></tr>
<tr><td rowspan="3">センタ要員</td><td>PKI 技術要員</td><td>PKI 運営管理者により指名される</td><td rowspan="3">セキュリティ管理者の同意のもとに PKI 運営管理者が付与する</td><td rowspan="4">PKI 運営管理者が付与する</td><td>単独でのアクセス不可
セキュリティシステムへのアクセス権限を有した者の帯同が必要</td></tr>
<tr><td>システム運用者</td><td>セキュリティ管理者により指名され PKI 運営管理者の合意が必要</td><td>ID カードシステム、
生体認証システム</td></tr>
<tr><td>保守要員</td><td>セキュリティ管理者または PKI 運営管理者により指名される</td><td>単独でのアクセス不可
セキュリティシステムへのアクセス権限を有した者の帯同が必要</td></tr>
<tr><td>本部要員</td><td>業務運用者</td><td>PKI 運営管理者により指名される</td><td>－</td><td>遠隔アクセス用
クライアント証明書</td></tr>
</table>

証明書発行システムの設置場所のセキュリティを保証するために、センタ要員に入室権限を付与し、当該システム専用室へのアクセスを制限する。各センタの PKI 運営管理者がセキュリティ管理者の同意のもとにセンタ要員に専用室への入室権限を付与できるものとする。セキュリティ管理者は権限付与を表明した文書にもとづいて、ID カードシステム、生体認証システムに当該センタ要員を登録し、また登録を抹消する。

証明書発行システムの運用にかかわるセキュリティを保証するため、装置・機器の操作権限を要員に分散して付与し、可能なアクセスを規定する。各センタの PKI 運営管理者が、証明書発行システムの操作権限を付与できるものとする。PKI 運営管理者は権限付与を表明した文書にもとづいて、アカウント設定（、変更、抹消）、運用証明書の発行（、失効）処理を行う。なお、装置・機器のアカウントのうち特権を付与されるものについては、特に厳重に管理するものとする。

証明書発行システムの JCSI 本部からの遠隔運用にかかわるセキュリティを保証するため、業務運用を JCSI 本部から行う権限を本部要員に付与し、操作のセキュリティを確保する。PKI 運営管理者が、証明書発行システムの遠隔操作権限を付与できるものとする。

入室権限、操作権限、および遠隔操作権限付与の記録は、PKI 運営管理者により管理され、錠付きの収納キャビネットに、少なくとも 3 年間保管される。

これらの権限付与、および指揮命令系統の詳細は、各センタ、JCSI 本部ごとに詳細手順書にて定める。各センタの PKI 運営管理者は、詳細手順において単に運営管理者と呼ぶことがある。業務の一部を委託する場合、JCSI は委託先に本章の規定の遵守を求め、詳細手順書の作成とこれに沿った運用を求める。なお、各センタ、JCSI 本部は、各要員の作業ならびに委託先による作業について、本規程に従って適切なセキュリティを維持すべく監督しなければならない。

A5.3 人事的セキュリティ管理

本サービスは、本編 5.3 節に従う。

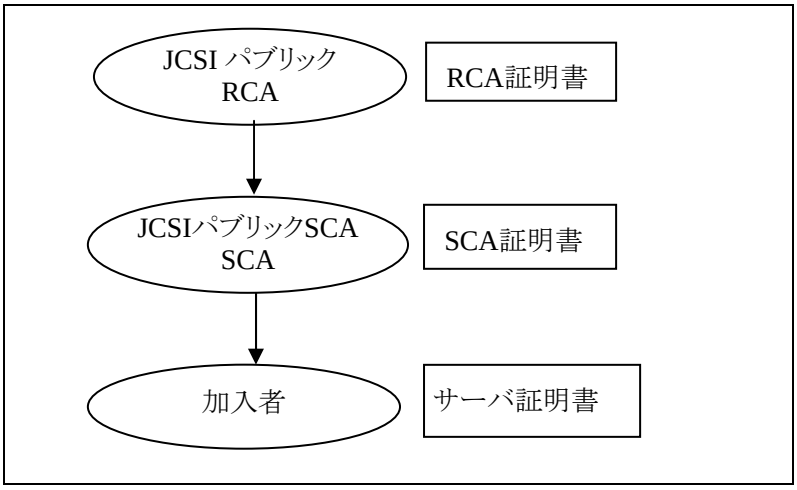
A6. 技術的なセキュリティ管理

本サービスも本編 6 章に従う。 ただし、サーバ証明書は発行パターン 1 で RAO 経由で登録/検証/発行される。

A7.SecureSignサーバサービスの証明書とCRLのプロファイル

A7.1 証明書階層

SecureSign サーバサービスの証明書階層を以下に示す。



A7.2 各証明書のプロファイルとその設定内容

SecureSign 証明書の設定値は RFC2459 に従う。設定内容は加入者もしくは JCSI が設定する。設定内容は証明書種類ごとに個別に管理する。 RCA 証明書と SCA 証明書、ならびに CRL のプロファイルは、本編 7 章の記述に従い、ここではサーバ証明書のプロファイルを、表 A7-1 に記載する。

表 A7-1 サーバ証明書のプロファイルとその設定

No.	フィールド名(field name)	設定者	c/nc	設定値説明
証明書基本部				
1	バージョン(version)	JCSI	―	V3 固定
2	シリアル番号(serialNumber)	JCSI	―	128 ビット以下の正の整数
3	署名(signature)	JCSI	―	RSA with SHA-1
4	発行者(issuer)	JCSI	―	c=JP o=Japan Certification Services,Inc. cn=SecureSign PublicCAn (n=1,2,3,…)
5	有効期間(validity)	JCSI	―	申請時から 1 年間＋30 日
6	所有者(subject)	加入者および JCSI	―	c=JP st=都道府県名(加入者設定、オプション) l=市町村(加入者設定、オプション) o=サーバ管理組織名(加入者設定、必須) ou=サーバ管理部署名(加入者設定、オプション) cn=サーバの DNS 名(加入者設定、必須)
7	所有者公開鍵(subjectPublicKeyInfo)	加入者	―	RSA 公開鍵(1,024～2,048 ビット) *1
証明書標準拡張部				
8	認証局鍵識別(authorityKeyIdentifier)	JCSI	nc	公開鍵の SHA-1 と issuer の DN とシリアル番号
9	所有者鍵識別(subjectKeyIdentifier)	JCSI	nc	公開鍵の SHA-1
10	鍵種別(keyUsage)	JCSI	nc	digitalsignature、keyEncipherment
11	拡張鍵種別(extendedKeyUsages)	JCSI	nc	PKIX-IDKP-ServerAuth、PKIX-IDKP-ClientAuth
12	証明書ポリシー(certificatePolicies)	JCSI	nc	policyOID:1.2.392.200075.2.2 policyURL:https://cp.jcsinc.co.jp/SecureSign/1/ RPA1.html
13	基本制約(basicConstraints)	JCSI	nc	cA:FALSE pathLenConstraint:フィールドは省略
証明書 Netscape 拡張部				
14	netscape-cert-type	JCSI	nc	SSL Client, SSL Server

c/nc はクリティカル指定 c と nc を示す　　－:設定の定義なし
*1 例外的に 512 ビットの鍵長も認める場合あり

A7.2.1 加入者の申請内容(特記事項)

(1)所有者フィールドの Email 項目

加入者は、証明書要求(CSR)にはこの項目を設定してはいけない。

(2)RAO は、所有者フィールドの cn に加入者が所持するサーバを特定する DNS 名が設定されているか検証しなければならない。

A7.2.2 発行した証明書の設定内容の妥当性検査

加入者は、発行された証明書の設定内容が妥当か否かをすみやかに検査し、設定内容が受理できない場合は、すみやかに該当証明書の失効申請を JCSI に対して行わなければならない。

A8. 仕様管理

本サービスは、本編 8 章に従う。