SecureSign® AD

サービス標準規程

（V2.5）

2013 年 2 月 1 日

日本認証サービス株式会社

改版履歴

バージョン	日付	改版内容
1.0	2009.1.30	初版
1.0.1	2010.1.25	Mozilla 公開審議結果に基づく修正
2.0	2010.4. 1	クライアント系証明書などの追加
2.1	2010.6.7	TSA サーバ証明書の追加
2.2	2011.4.4	クライアント証明書プロファイル変更
2.3	2011.9.30	3.(2) 事務取扱要領（本部編）V2.1 との整合性
2.4	2012.2.24	1.4 新事務所移転に伴う住所変更
2.5	2013.2.1	4.3、5.1、6.7 IDS 廃止に伴う記述の削除

目次

1. はじめに

1.1 要約

日本認証サービス株式会社(以下「JCSI」と記す)は、SecureSign AD と称する証明書発行サービス(以下「本サービス」と記す)を提供する。本サービスは、当社顧客の「人」「法人」「機器」「ソフトウェア」などに関連付けられた公開鍵暗号方式の鍵ペアに対して、PKI 標準にもとづく公開鍵証明書を JCSI が発行し、その証明書を提示された相手(依存者)に対して鍵ペアの所有者を証明するものである。

JCSI は他に、SecureSign、AccreditedSign などの証明書発行サービスを提供している。本サービスは、当初より定期的に米国カナダ公認会計士協会の監査基準、WebTrust for CA に基づく外部監査を受け、認定を受けて実施するものである。WebTrust for CA は信頼しうる認証局の監査基準として、世界的に広く使われているブラウザ、電子メールソフト、電子文書ソフトなどの多くのベンダに認められている。WebTrust for CA 認定を受けた認証局は、これらのベンダにより、その製品の利用者(すなわち証明書の依存者)に対して、予め「信頼された認証局」として扱われる。

SecureSign AD は、我が国の「電子署名及び認証業務に関する法律」を受けて実施されるものではないので、発行する公開鍵証明書は、e-Tax、インターネット出願などの行政に対する入札・申請・届出等の手続には利用できない。

SecureSign AD は鍵ペアの所有者(証明される加入者)として「人」、「法人」、「機器」、「ソフトウェア」など複数のタイプのエンティティを証明する(予定を含む)。現時点では証明書の利用局面として SSL/TLS サーバ認証、TSA サーバ認証、クライアント認証、S/MIME メール、電子文書署名を想定し、証明書ポリシーを設定する。証明書ポリシーは CPS(Certification Practice Statement)と共に本文書にて規定される。

SecureSign AD は IETF(Internet Engineering Task Force)の PKIX(Public Key Infrastructure working group)が提唱する RFC5280 など各種 RFC に準拠して実施される。

SecureSign AD は JCSI が証明書の発行者となる認証業務である。JCSI は、発行局サーバ運用、特定の証明書ポリシーに係る審査登録業務など、その業務の一部を他社に委託する場合がある。本文書は委託先の遵守すべき事項を含む。

1.2 名称

本文書の名称を「SecureSign AD 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.
1.2.392.200075.4	SecureSign AD Service
1.2.392.200075.4.1	SecureSign AD CPS(本文書)
1.2.392.200075.4.2	SecureSign AD Policy for 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 AD には、表 1-2 に示す複数のエンティティが含まれる。

表 1-2 エンティティとその役割

エンティティ	役割
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(加入者がオブジェクトの場合はその管理者)が、当社から SecureSign AD の証明書を購入する。加入者が遵守すべき事項は、加入者と JCSI が交わす販売契約にも規定される。
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 (認証局) (CA)	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り、本サービスでは JCSI である。発行者は、認証局の運営主体である。なお、公開鍵証明書は、加入者以外に、発行局、登録局の要員、機器などにも発行される。
登録局(RA)	証明書の発行に先立ち、加入者などからの申請受付、その内容の審査、登録などを行う組織。本サービスでは原則 JCSI が実施するが、JCSI との業務委託契約にもとづき委任することがある。登録局の担務は以下の通りである。

	証明書申請受付 本人確認 IA へ証明書要求 証明書(と秘密鍵)の配付 証明書失効決定、IA へ証明書失効要求 * RA: Registration Authority
RAO	① RA を管理し運営する人。 ② 加入者証明書発行要求や失効要求を入力する人。
発行局(IA)	JCSI との業務委託契約にもとづき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。 IA は、RA から証明書要求を受領後、個々の証明書を発行し、RA からの証明書失効要求に基づき個々の証明書を失効させ、定期的に CRL を更新発行する。 * IA: Issuing Authority
IAO	① IA を管理し運営する人。
リポジトリ	リポジトリは、加入者の証明書、CRL および SecureSign AD 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。
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(SCA)の証明書に署名する。RCA からの証明書発行は合議制操作によるものとし、その発行可否は合議により定められる。RCA には RA が存在しない。この自己署名証明書を「ルート証明書」と記すことがある。 * RCA: Root CA
下位認証局（SCA）	SCA 証明書は、直上の認証局(RCA)により署名され、SCA は、加入者証明書に署名する。RA が存在し、加入者の審査登録を行う。 * SCA: Subordinate CA

1.3.2 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。

SecureSign AD 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。またエンドエンティティは高額の取引を SecureSign AD の証明書記載事項に依存して行うべきではない。

SecureSign AD として JCSI は、以下の狭義の用途を持つ証明書を発行する。(7 章参照)

・SecureSign AD Web-server certificate (Web サーバ証明書、TSA サーバ証明書など)

・SecureSign AD client certificate (S/MIME 証明書、クライアント証明書など)

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。

1.3.3 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。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 AD 用 RCA/SCA 証明書をリポジトリで公開する。エンドエンティティは、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。エンドエンティティは、定期的にリポジトリを訪問し、SecureSign AD 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。エンドエンティティが、SecureSign AD のサービス内容について知りたいとき、JCSI のヘルプデスクに問い合わせることができる。この場合、電子メールによる問い合わせが望まれるが、JCSI の営業時間帯(午前 9 時～午後 5 時)には電話による問い合わせも受け付ける。

注)JCSI の定める営業日は、祝祭日、JCSI の特別休日、年末年始休日を除く平日(土曜日・日曜日以外の曜日)である。なお、JCSI の特別休日、年末年始休日については、別途 Web サイト(http://www.jcsinc.co.jp)にて公開する。

［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

電子メールアドレス：securesign@jcsinc.co.jp

2. 一般条項

2.1 義務

SecureSign AD では JCSI が発行者(CA)として IA、RA、リポジトリの、加入者が加入者としての、依存者が依存者としての、それぞれ義務を負う。なお、JCSI はその義務の一部を、第三者に業務委託する形で全うする。

2.1.1 IA の義務

IA 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。IA の義務は JCSI(業務委託先を含む)の義務である。

(1)発行者(JCSI)の署名鍵(秘密鍵)をセキュアに生成し管理する。

(2)RA の要求にもとづき証明書の発行を行う。

(3)RA と協調して証明書ライフサイクル管理を行う。

(4)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。

(5)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。

2.1.2 RA の義務

本節において、RA は、その操作者(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。RA、RAO の義務は JCSI(業務委託先を含む)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。S/MIME 証明書、クライアント証明書の発行にあたり、利用者の鍵対を生成する場合には、権限のある RAO 以外がこれを取り扱えず、入手もできないよう、適切な防御措置を講じなければならない。

(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。S/MIME 証明書、クライアント証明書の発行にあたり、利用者の鍵対を取り扱う場合には、適切な漏洩防止、毀損防止措置を講じつつ、確実に利用者(証明書申込み者(お客様))に届けなければならず、送達確認後は速やかに RA の利用者鍵対を抹消しなければならない。

(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)IA と協調して証明書ライフサイクル管理を行う。

2.1.3 加入者の義務

SecureSign AD サービスの加入者は以下の義務を負う。オブジェクトを証明する場合はその管理者が、以下の義務を負う。

⑴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。

⑵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、証明書を使用してはならない。

⑶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。

⑷鍵などの管理義務(Web サーバ証明書、TSA サーバ証明書)

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。

⑷(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。

⑷(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。

⑸鍵などの管理義務(S/MIME 証明書、クライアント証明書)

鍵対の生成は RA にて行われ、加入者は証明書とともに RA から受け取る。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。

⑸(a)秘密鍵の秘匿管理

受領した秘密鍵が、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。そのために加入者は、たとえば PC 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。

⑸(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。

(6)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。

(7)すみやかな失効申請

上記(4)-(a)、(b)、(5) -(a)、(b)、(6)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。

(8)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。

2.1.4 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によるサーバ認証の目的で使用される。TSA サーバ証明書はタイムスタンプトークン署名に使用される。S/MIME 証明書は利用者の授受する S/MIME メール等に付随して、および利用者が Web サイトにクライアント認証のために提示するためにのみ使用される。クライアント証明書は利用者が電子文書に付す電子署名に付随して、および利用者が Web サイトにクライアント認証のために提示するためにのみ使用される。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、SecureSign AD 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)当該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、7 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 AD 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 AD 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 AD 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 AD ルート証明書のハッシュ値(SHA-1)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。

2.1.5 リポジトリの義務

JCSI は、CRL の作成後、本規程 2.6.2 項で規定される方法で、その情報をリポジトリに公開し、加入者および依存者が、加入者証明書の利用の意思決定をするために、常時、証明書の失効状況を検証できるようにする。

また、リポジトリは、本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 AD サービスを加入者に提供する JCSI は、発行局(IA)、登録局(RA)とその管理者(RAO)を含んで責任を持つ。加入者は JCSI による審査・登録のために、2.1.3 の加入者の義務を果たすことに責任を持つ。その責任の詳細について以下の様に定める。

2.2.1 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。

・3 章に従って加入者の真偽確認を厳密に実施し、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。

・4 章に従い、SecureSign AD 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。

・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。

・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、または加入者との契約の履行上、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。

2.2.2 加入者の責任

加入者は、2.1.3 項の加入者の義務を果たすことに責任を負う。

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、加入者に対しては別途加入者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)加入者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 は加入者に対し、当該損害の賠償を請求することができるものとする。

(3) 2.1.3 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、2.1.3 節(7)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)2.1.4 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、2.1.4 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 AD サービスの加入者、依存者のいずれに対しても、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 AD 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

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 AD 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 AD サービスを加入者に提供するに際して、リポジトリを運用する。

2.6.2 公表の頻度

⑴本文書の公開は、8 章に規定される。

⑵失効情報については、失効処理が行われてから 12 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。

⑶CRL 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。

⑷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 AD 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)加入者は、加入者が管理するサーバに、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。だだし、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 AD 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	SecureSign AD 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	JCSI からのお知らせ	関与者全員	○

2.7 準拠性監査

JCSI は、SecureSign AD サービスを運用するに際して、本文書を含む種々の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、WebTrust for CA 監査基準に基づいた外部監査を、定期的に受ける。

2.7.1 監査の頻度

WebTrust for CA 監査基準に従う。

(1)以前の外部監査から 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、WebTrust for CA 監査を行う資格をもった日本国内の監査法人を選定する。現時点では、新日本有限責任監査法人を選定している。

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、外部監査を受けるために、監査人と共に、その目的、監査組織、スケジュール、監査対象、作業要領を定める。

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

WebTrust for CA 監査の監査報告書を、米国・カナダ監査人協会に提出し、WebTrust for CA 認定を受ける。SecureSign AD サービスが認定されていることは、同協会から公表される。また当社が、SecureSign AD サービスのルート証明書を予め製品に組み込むよう希望する製品のベンダーには、その請求に基づき個別に、監査報告書を開示することがある。

2.8 秘密保持

2.8.1 秘密が保たれる情報

JCSI ならびに加入者は、SecureSign AD 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 AD 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、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 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 が加入者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。

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。

3. 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」または「注文書」)から発行までの手順は 4.1 節に記載する。この一連の手順の中での、Web サイト、S/MIME メールアドレス保有者、または署名者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以下のとおりである。

(1)Web サーバ証明書、TSA サーバ証明書

・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。

・CN=について実存性を DNS 参照により確認し、Whois コマンドにてドメイン名の所有／管理を確認する。異なる場合ドメイン名所有者より証明書申請管理者に発行された「ドメイン名使用 CN=許諾書」を確認する。

（注）TSA サーバ証明書では CN=をドメイン名として検査することは行わない。

・O=、L=、ST= について Whois コマンド情報または「ドメイン名使用許諾書」により組織名と所在地の正確性を確認する。必要情報に欠落がある場合、3.1.8 節のとおり商業登記の記載事項証明書などを求めることがある。

・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の確認。

(2)S/MIME 証明書、クライアント証明書

・注文主の存在とその本人の申込みの意思を、注文書の記名押印により確認。

・注文主の属する組織の存在を、e-mail アドレスのドメイン名部分に関する Whois コマンド情報(S/MIME 証明書の場合のみ)、公開された企業データベース情報、または注文書に記載された注文主の会社情報 URL の検索により確認。

・注文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、注文主の実体を表しているかの検証。

・証明書に記載すべき O=、L=、ST= が、前項で確認された注文主の属する組織のものであることを確認。(一括申込み、代理申請の場合は「証明書発行申請に関する誓約書」の提出を求める。)

・S/MIME 証明書の場合、証明書に記載すべき e-mail アドレスに確認メールを送信し、その本文の案内に従った返信メールがあったことを確認。

(注)S/MIME 証明書、クライアント証明書は企業に属する個人にのみ発行する。S/MIME 証明書ではその e-mail アドレスはその企業のドメインのものでなければならない。JCSI はネットサービスプロバイダ等の e-mail アドレスには S/MIME 証明書を発行しない。

なお、確認/認証の方法については JCSI 内部規定に従う。

(注 1)「申込書」または「注文書」は JCSI Web サイトからダウンロードできる。

3.1 初期登録(初期申請)

3.1.1 名称のタイプ

「申込書」または「注文書」の証明書登録申請情報として規定する。

3.1.2 名称に意味がある必要

当該 Web サイト、S/MIME メールアドレス保有者、または署名者の実体を正しく表している必要がある。このために「申込書」または「注文書」にはその実体を反映し申請する義務が、加入者に生じる。

3.1.3 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。

3.1.4 名称のユニークさ

Web サーバ証明書、TSA サーバ証明書、S/MIME 証明書、クライアント証明書に記載される識別名を構成する各項目(OU=を除く)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、メールアカウント、または署名者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。

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またはメールアドレスが属するドメイン)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。

3.1.6 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またはメールアドレスは、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。

3.1.7 秘密鍵の所有を証明する方法

Web サーバ証明書、TSA サーバ証明書において、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 形式での申請が原則)。S/MIME 証明書、クライアント証明書においては、RA が加入者の秘密鍵を生成し、PKCS#12 形式で加入者に供給する。

3.1.8 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。

3.1.9 個人の同一性の認証

3 節序文で記した同一性の確認のために JCSI(RAO)は 3.1.8 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、Web サーバ証明書、TSA サーバ証明書において鍵の生成/登録から実機への組み込み等の実作業を担う個人、S/MIME 証明書、クライアント証明書において鍵と証明書の受領から実機への組込みまでの実作業を担う個人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。

3.2 証明書の更新に伴う鍵更新

3.1 節、初期登録に同じ。

3.3 失効後の鍵更新

3.1 節、初期登録に同じ。

3.4 失効要請における同一性の認証

JCSI(RAO)は、Web サーバ証明書、TSA サーバ証明書の失効要請は証明書申請管理者から受け付ける。S/MIME 証明書、クライアント証明書の失効要請は注文主から受け付ける。失効申請者の同一性確認のために 3.1.8 項、3.1.9 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。

3.5 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

本サービスでの Web サーバ証明書、TSA サーバ証明書の発行申請は、以下の手順で実施される。

(1)加入者は申込書(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。
(2)JCSI は、申込書と添付書類を 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。
(3)加入者による鍵生成～証明書要求(CSR)作成～申請(加入者→RAO)。
(4)JCSI による証明書申請(CSR)のマニュアル審査(RAO 操作)。
(5)JCSI RAO 操作による証明書発行依頼～IA による証明書発行(RAO 受領)。
(6)加入者に対する証明書送付(加入者←RAO)。

本サービスでの S/MIME 証明書、クライアント証明書の発行申請は、以下の手順で実施される。

(1)加入者は、注文書(JCSI の Web からダウンロード)に必要事項を記入し、証明書記載事項データ、必要書類とともに JCSI へ郵送する。
(2)JCSI は、注文書と添付書類を 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。
(3)JCSI による RA サーバ内での加入者鍵生成～証明書要求(CSR)作成(RAO 操作)。
(4)JCSI による証明書要求(CSR)のマニュアル審査(RAO 操作)。
(5)JCSI RAO 操作による証明書発行依頼～IA による証明書発行。
(6)JCSI RAO 操作による鍵と証明書(PKCS#12 形式ファイル)の受領と加入者送付。
(7)JCSI RAO 操作による PKCS#12 ファイルと PIN の受領と加入者送付。加入者受領後の速やかな破棄。

本サービスの RCA による SCA への証明書発行は以下の手順で実施される。

(1)対象 SCA が条件を満たすことを確認し、証明書発行を決定する。
(2)対象 SCA より安全な方法で CSR を得て、予め定められた合議者が RCA 署名鍵を HSM 内に復元し、RCA を活性化し、SCA の CSR に対して証明書を発行する。
(3)発行した証明書を安全な方法で SCA に届け、SCA の受け入れ動作確認を待つ。
(4)動作確認完了の通知を得て、RCA を非活性化し、HSM 内の RCA 署名鍵を抹消する。
(5)決定どおり SCA に証明書を発行したことを確認する。

4.2 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行わない。

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 IA 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。

本サービスでは、Web サーバ証明書失効申請書、TSA サーバ証明書失効申請書、S/MIME 証明書失効申請書、クライアント証明書失効申請書の郵送もしくは直接持参の方法での失効申請を受け付ける。申請者の真偽確認の手順は以下の通りである。

(1)失効申請者の真偽確認(郵送または持参の場合)

JCSI は、失効申請者の真偽確認を以下の方法で確認ができた場合、申請者の真偽確認を「真」と判断する。確認結果が不可の場合「偽」と判断する。

(a) JCSI が保管している申込書、または注文書に記入されている情報内容

・加入者の情報(申請責任者氏名または注文主氏名、会社・団体名、部門名、役職、印影)と各証明書失効申請書に記入されている申請者情報内容が一致することを確認す

4.3 セキュリティ監査の手続き

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。IA、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。

頻度	監査項目	対象となる監査証跡	成果物
週次	入退室管理システムの正常稼動の確認	入退室管理システムの入退室履歴 監視ﾓﾆﾀ記録(HDDR)	入退室管理システム月例検査報告書 HDDR ﾁｪｯｸｼｰﾄ
月次	入退室管理システムの記録とマニュアル記録の照合	入退室管理システム月例検査報告書 運転指示書、入出庫管理票、非定期作業(兼)トラブル記録	監査実施記録
	入退室要員管理	静脈センサ登録・更新・削除申請書、宣誓書	同上

	監査ログ	ﾌｧｲｱｳｫｰﾙﾛｸﾞ、ＣＡ監査ﾛｸﾞ、各ｻｰﾊﾞのｼｽﾃﾑﾛｸﾞ	同上

・IA 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、、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。ログに記録している総てのパケット、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パッシブセンサー、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。警報発報は異常な記録として扱う。
・本サービスで使用する以下の帳票類(保管期間・保管場所)
  ① 入退室管理システム月例検査報告書(1 年間・JCSI エリア)
  ② HDDR チェックシート(1 年間・JCSI エリア)
  ③ 耐火保管庫入出庫管理票(1 年間・JCSI エリア)
  ④ 非定期作業記録(兼)トラブル対応記録(1 年間・JCSI エリア)
  ⑤ 定期監査実施記録(1 年間・JCSI エリア)
  ⑥ 静脈センサ登録・更新・削除申請書(期限切れ後 3 年間・JCSI エリア)
  ⑦ 天井裏物理鍵貸出申請書(兼)了解書(1 年間・JCSI エリア)
  ⑧ 鍵使用連絡票(1 年間・JCSI エリア)
  ⑨ 運転指示書(写し)(1 年間・JCSI エリア)

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 AD 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る。そのために、間仕切り、壁などで区分され、耐火機能を持ち、媒体に対する電磁的影響を遮断する機能を有する保管庫を使用する。

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準拠性監査(2.7 節)まで)
- 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 RCA/SCA 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準拠性監査(2.7 節)まで)
- セキュリティ監査(4.3 節)の記録。(次回準拠性監査(2.7 節)まで)
- 手続き的管理(5 章)で規定する権限付与、剥奪の記録。(次回準拠性監査(2.7 節)まで)
- 設備保守、システム保守、変更、障害の記録。(次回準拠性監査(2.7 節)まで)
- 発行された総ての証明書、CRL。SecureSign AD サービス RCA/SCA 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 AD 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)
- 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/注文書原本、および添付される書類。(証明書の有効期間満了まで)
- 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 が失効判断に用いた書類一式。(証明書の有効期間満了まで)
- 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)

4.5 鍵の交換

SecureSign AD 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 RCA では自己署名し、SCA

では本サービスの 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 AD サービスの CA 秘密鍵が危殆化注 1 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、RCA では自己署名し、SCA では本サービスの 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 AD サービスは、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 RCA/SCA 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。

(注 1)危殆化の条件・不正侵入、不正操作、パスワードの漏洩、秘密鍵片の紛失

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(IA、RA)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、委託先センタにおいて定められる。

(2)JCSI システムを構成するネットワーク、および接続するネットワークを以下のセグメントに区分し、それぞれのネットワーク上の通信をファイアウォールによって個別に制御する。

セグメント名	接続する機器
インターネット	ルータ、ファイアウォール
DMZ	WebGW/リポジトリ
セキュア	IA/RA サーバ、監視サーバ、 運用管理サーバ、専用操作端末

(3)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、委託先センタにおいて定められる。

(4)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。

(5)証明書発行システム(サーバ、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し、その記録は 5.2 節の表 5-1 で規定されるプロジェクト管理責任者が毎月監査するものとする。

(6)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。最高セキュリティレベルへの出入りは任命され入室権限を付与された要員に限定される。また最高セキュリティレベルの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、5.2 節の表 5-1 で規定されるプロジェクト管理責任者が毎月監査するものとする。

(7)最高セキュリティレベルは、ビデオ記録システム、パッシブセンサーにより、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。

(8)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。

(9)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。

(10)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。

(11)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。

(12)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。

5.2 手続き的セキュリティ管理

JCSI は、表 5-1、表 5-2 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、IA、RA および JCSI に設置される RAO 端末ならびに JCSI のリポジトリを操作する。

表 5-1 センタ要員別権限

<table>
<tr><th>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>プロジェクト管理責任者(業務運用管理責任者)</td><td>センタ業務の主管部門の責任者</td><td colspan="2">－</td><td>－</td></tr>
<tr><td>プロジェクト管理者</td><td>プロジェクト管理責任者により指名される</td><td rowspan="4">プロジェクト管理責任者が付与する</td><td rowspan="4">プロジェクト管理責任者が付与する</td><td>生体認証システム</td></tr>
<tr><td>プロジェクトメンバ</td><td>プロジェクト管理責任者により指名される</td><td>生体認証システム</td></tr>
<tr><td>担当 CSE(システム運用担当者)</td><td>プロジェクト管理責任者の依頼により所属部門にて指名される</td><td>生体認証システム</td></tr>
<tr><td>保守担当</td><td>－</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ものの帯同が必要</td></tr>
</table>

表 5-2 本部要員別権限

役割	任命者	入室権限	操作権限	説明
運営管理者	取締役会	無		入室は権限を有する者の帯同が必要
業務運用管理者	運営管理者	無		入室は権限を有する者の帯同が必要
セキュリティ管理者		有	無	
システム管理者	業務運用管理者	有		
業務運用者	運営管理者	有		証明書発行操作権限を有する

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。センタのプロジェクト管理責任者がプロジェクト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。プロジェクト管理者は権限付与を表明した文書にもとづいて、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。センタのプロジェクト管理責任者が、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。プロジェクト管理責任者またはプロジェクトメンバ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 本部からの遠隔操作(4.1 節、4.2 節)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。プロジェクト管理責任者が、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、プロジェクト管理責任者により管理され、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、センタ、JCSI 本部ごとに詳細手順書にて定める。センタのプロジェクト管理責任者は、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、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。

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が過去２年間、禁錮刑以上の犯罪を起こしていないことを、以下のいずれかにより確認する。

・本人がその旨宣誓する文書に毎年署名する。

・所属する会社が就業規則に定め運用していることを文書により表明する。

(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、要員着任時に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。周知徹底を図るためにセンタ要員へ定期的に教育を実施する。教育実施頻度は概ね１年毎とし、プロジェクト管理責任者に報告する。

(3)秘密鍵のバックアップトークンおよび複数の物理鍵はセンタの管理責任者と JCSI の管理責任者が分けて保管する。管理責任者はバックアップトークンと複数の物理鍵を受け取る前に管理責任を果たすことを十分に認識して保管記録台帳に記載して記録を取り保管する。

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)その所定人員数は委託先センタにて定めるものとする。

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 3 人以上の合議メンバが行う。

(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、外部に提出することなく RCA 内で自己署名証明書の形式にする。

(3)エンドエンティティに対する 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)

(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 SCA

(1)鍵ペアの生成

鍵ペアは、乱数処理または擬似乱数処理を適用し、認証設備室内にて暗号化装置内で生成する。鍵ペアの生成は 3 人の合議メンバが行う。なお、生成された証明書署名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、CSR の形で RCA に手渡し、RCA から発行された証明書を受け取り設定する。

(3)公開鍵と秘密鍵のサイズ

RSA 公開鍵暗号方式による 2,048 ビットの鍵を使用する。

(4)加入者および依存者に対する SCA 公開鍵の配付

RCA から発行された SCA 証明書の形式で、以下のいずれかの方法で配付する。

・JCSI のリポジトリから加入者、依存者にダウンロードしてもらい配付する。ダウンロードした SCA 証明書の正当性は、リポジトリから公開されるフィンガープリント(証明書のハッシュ値)により加入者、依存者が確認することを義務付ける。

・加入者に加入者の鍵ペアを配付する際に一緒に配付する。

(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)で生成する。

(6)鍵用途

X.509 V3 で定められた証明書の標準拡張部(Extension)を使用して、鍵の用途を証明書(加入者証明書、運用証明書、相互認証証明書およびリンク証明書)、CRL の電子署名に限定する。

(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(加入者で生成)

(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 IA 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 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.509 V3 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場合、組み込みは行わなくてよい。

(7)使用するハッシュ関数

SHA-1

6.1.4 加入者(JCSI が生成)

⑴鍵ペアの生成

鍵ペアの生成は、擬似乱数処理で行う。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 上で行われる。

⑵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、IA に加入者証明書の発行を要求する。

⑶公開鍵と秘密鍵のサイズ

RSA 公開鍵暗号方式による 2,048 ビットの鍵を使用する。

⑷ハードウェア鍵の使用

ハードウェア鍵の使用はしない。

⑸鍵の使用目的

鍵の使用目的に合致した X.509 V3 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。

⑹鍵ペアの組み込み

鍵ペアおよび証明書は加入者に PKCS#12 形式ファイルおよびその PIN として別々に送付される。受け取った加入者はこれを目的の PKI アプリケーションに組み込む。なお、鍵ペアは以下の要件を満たすものとする。

・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、RA 側の鍵ペアは加入者本人の受領後速やかに破棄しなければならない。

⑺使用するハッシュ関数

SHA-1

6.2 秘密鍵の保護

6.2.1 暗号化装置標準

CA 秘密鍵は、FIPS PUB 140-2 レベル 3 認定を取得した暗号化装置によって管理する。暗号化装置はパーティションにより分割使用しても良いが、本サービス用パーティションは他認証業務からアクセスできてはならない。

加入者が使用する暗号化モジュールは FIPS PUB 140-2 に準拠していることが望ましい。

6.2.2 秘密鍵の多人数制御

本サービスでは、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)を表 6-1 に示す数で行う。

表 6-1 合議制操作と SecretShare

CA	合議制操作に必要な人数	SecretShare 分割数	秘密鍵を復元するために必要な Share 数
RCA	2-3	3	3
SCA	2-3	3	3

6.2.3 秘密鍵の預託

実施しない。

6.2.4 秘密鍵のバックアップ

秘密鍵は Secret Share を実現する複数の物理鍵の提示、参照によりバックアップトークン(以下トークンと略す)に保管する。

トークンと複数の物理鍵の保管者は発行者から指名され、トークンと複数の物理鍵を扱い(作業記録に記載)、トークンと複数の物理鍵はタンパーエビデント封筒に封印して、その保管者の責任において耐火金庫に保管する。

なお、秘密鍵のバックアップ操作は認証設備室内にて、JCSI 本部要員(システム管理者)およびセンタ要員(システム管理者)による合議制操作で行われる。

6.2.5 秘密鍵のアーカイブ

秘密鍵はアーカイブしない。

6.2.6 秘密鍵の暗号化装置へのエントリー(バックアップリカバリ)

秘密鍵のエントリーは、JCSI 本部要員(システム管理者)およびセンタ要員(システム管理者)による合議制操作で認証設備室内にて行われる。複数の物理鍵の提示、参照により秘密鍵をトークンから復元し、暗号化装置に投入する。トークンと複数の物理鍵は保管者が操作する(作業記録に記載)。

6.2.7 秘密鍵を活性化させる方法

秘密鍵の活性化は複数のセンタ要員(システム管理者)による合議操作で認証設備室内にて行う。活性化された秘密鍵は表 6-2 に示す期間、活性状態に置かれる。

表 6-2 CA 秘密鍵の活性期間

CA	活性化期間
RCA	署名時のみ
SCA	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

秘密鍵の非活性化は複数のセンタ要員(システム管理者)による合議操作で認証設備室内にて行う。なお、RCA については秘密鍵非活性化時に、複数の物理鍵の提示、参照により暗号化装置内の秘密鍵を抹消(完全に消去)するが、複数の物理鍵とトークンは保管する。

6.2.9 秘密鍵を破壊する方法

秘密鍵は RCA 証明書、SCA 証明書の更新に伴い使用されなくなった場合もしくは秘密鍵の使用中止した場合(本サービス終了時の処置)、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使用中パーティションの完全な初期化を伴う削除を行うものとする。この初期化は、JCSI 本部要員(システム管理者)およびセンタ要員(システム管理者)による合議制操作で行う。また、トークンと複数の物理鍵は、秘密鍵の使用を中止する場合(本サービス終了時の処置)には物理的に破壊する。それ以外の場合においてトークンと複数の物理鍵の破棄が必要となった場合には、トークンは初期化するものとする。 作業はセンタ要員(システム管理者)の立会いのもと、トークンと複数の物理鍵の保管者が認証設備室内にて行う(作業記録に記載)。

加入者は自身の秘密鍵は鍵ペアの有効期間が満了した場合、すみやかに破壊(削除)すること。

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
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	20 年	10 年
SCA	証明書・CRL 署名鍵	20 年以内	10 年以内
加入者	Web サーバ証明書	1 ヶ月 1 年 1 ヵ月以内 3 年 1 ヵ月以内 5 年 1 ヵ月以内	-
加入者	TSA サーバ証明書	11 年 1 ヶ月以内	
加入者	S/MIME 証明書	3 年 1 ヵ月以内	-
加入者	クライアント証明書	3 年 1 ヵ月以内	-

6.4 活性化データ

ハードウェア暗号化装置の活性化/非活性化に用いるデータを、活性化データとして扱い、パスワードを使用する。

6.4.1 活性化データの生成と組み込み

パスワードを活性化データとして扱う。パスワードは 6 文字以上の長さを使用する。

6.4.2 活性化データの保護

パスワードは暗号化装置(ハードウェア)内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

IA、RA が使用するコンピュータシステムは、信頼性および安全性に関して実績のあるシステムを使用する。

6.5.2 コンピュータセキュリティの評価

認証設備におけるコンピュータシステムセキュリティを随時評価し、結果に基づいて対策を行なう。

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

IA、RA サーバ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

IA/RA サーバ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

JCSI 本部から業務に使用するプロトコル(https)は、アクセス元を当該ホスト(または代理サーバ)に限定して通信を許可する。

RCA はインターネットに接続しない。 SCA 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。

6.8 暗号化モジュール工学管理

IA で使用するハードウェア暗号化装置は FIPS PUB 140-2 レベル 3 に対応する。

7. 本サービスの証明書と CRL のプロファイル

本章では、本サービスで発行する証明書ならびに CRL のプロファイルを記述する。

7.1 証明書プロファイル

7.1.1 バージョン番号

本サービスでは X.509 V3 の証明書を発行する。

7.1.2 証明書標準拡張部

本サービスでは、発行する証明書の種類によって使用する拡張部は異なる。詳細は、本規程 7.1.9 項に記載される個々の証明書プロファイルを参照されたい。

7.1.3 アルゴリズム OID

本サービスで発行する証明書で使用されるアルゴリズム名とその OID は以下の通りである。

加入者公開鍵(subjectPublicKeyInfo) ： RSA 公開鍵(OID=1 2 840 113549 1 1 1)

署名(signature) ： sha1WithRSAEncryption(OID=1 2 840 113549 1 1 5)

7.1.4 名称形式

本サービスで発行する証明書、CRL に記載される発行者、所有者の名称とその形式詳細は、本規程 7.1.9 項を参照されたい。

7.1.5 名称制約

本サービスでは、名称制約拡張を設定しない。

7.1.6 証明書ポリシーOID

本サービスで使用する証明書ポリシーOID は、本規程 7.1.9 項に記載される個々の証明書プロファイルを参照されたい。

7.1.7 ポリシー制約拡張の使用

本サービスでは、ポリシー制約拡張を設定しない。

7.1.8 ポリシー修飾子

本サービスでは、証明書の種類によりポリシー修飾子の使用法が異なる。詳細は、次項を参照されたい。

7.1.9 証明書プロファイル

以降この項では、本サービスで発行する証明書のプロファイル詳細を記述する。なお、以

降の表で現われる「設定者」と「クリティカリティ」の設定値の意味は以下の通りである。また、後述の CRL の表の記述における意味も同一である。なお、証明書の記載項目は、特に断りのない限り PrintableString でエンコードされる。

設定者　IA： IA で値を設定する
RA: RA で値を設定する
EE: 加入者が CSR 作成時に値を設定する
× ： 値を設定しない

クリティカリティ　T ： TRUE を表す
F ： FALSE を表す
－ ： 設定できない、または設定しない

(1) RCA 証明書プロファイル

名称			設定者	クリティカリティ	設定値
証明書基本部					
	version		IA	－	V3
	serialNumber		IA	－	128bit 以下の正の整数
	signature		IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
	issuer		IA	－	C=JP, O=Japan Certification Services, Inc., CN=SecureSign Root CA11 ※PrintableString でエンコードする
	validity				
		notBefore	IA	－	20 年とする
		notAfter	IA	－	※UTCTime で設定する
	subject		IA	－	C=JP, O=Japan Certification Services, Inc., CN=SecureSign Root CA11 ※PrintableString でエンコードする
	subjectPublicKeyInfo				
		algorithmIdentifier	IA	－	rsaEncryption(OID=1 2 840 113549 1 1 1)
		public key	IA	－	2048bit の値
証明書標準拡張部					
	subjectKeyIdentifier		IA	F	公開鍵の SHA-1 値(ハッシュ値)
	keyUsage		IA	T	keyCertSign、cRLSign を ON とし、他を OFF とする
	basicConstraints		IA	T	

		cA	IA		TRUE
		pathLenConstraint			NULL

(2) SCA 証明書プロファイル

名称				設定者	ｸﾘﾃｨｶﾙﾃｨ	設定値
証明書基本部						
	version			IA	－	V3
	serialNumber			IA	－	128bit 以下の正の整数
	signature			IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
	issuer			IA	－	C=JP, O=Japan Certification Services, Inc., CN=SecureSign Root CA11 ※PrintableString でエンコードする
	validity					
		notBefore		IA	－	20 年とする
		notAfter		IA	－	※UTCTime で設定する
	subject			IA	－	C=JP, O=Japan Certification Services, Inc., CN=SecureSign Public CA11 ※PrintableString でエンコードする
	subjectPublicKeyInfo					
		algorithmIdentifier		IA	－	rsaEncryption(OID=1 2 840 113549 1 1 1)
		public key		IA	－	2048bit の値
証明書標準拡張部						
	subjectKeyIdentifier			IA	F	公開鍵の SHA-1 値(ハッシュ値)
	keyUsage			IA	T	keyCertSign、cRLSign を ON とし、他を OFF とする
	certificatePolicies			IA	F	
		policyIdentifier				
			certPolicyId			1 2 392 200075 4 2
		policyQualifiers				
			policyQualifierId			1 3 6 1 5 5 7 2 1(id-qt-cps)
			qualifier			https://cp.jcsinc.co.jp/SecureSign/AD/RPA.html （同意書の URI)
	basicConstraints			IA	T	
		cA		IA		TRUE

		pathLenConstraint	×		設定しない
	cRLDistributionPoints		IA	F	distributionPoint.fullName.URI に以下を設定する。 http://ssignadcrl01.jcsinc.co.jp/repository/crl/rca.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/rca.crl

(3) Web サーバ証明書プロファイル

名称			設定者	ｸﾘﾃｨｶﾘﾃｨ	設定値
証明書基本部					
	Version		IA	－	V3
	serialNumber		IA	－	128bit 以下の正の整数
	signature		IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
	issuer		IA	－	C=JP, O=Japan Certification Services, Inc., CN=SecureSign Public CA11 ※PrintableString でエンコードする
	validity				
		notBefore	RA	－	1 ヶ月間, 13 ヶ月間, 37 ヶ月間, 61 ヶ月間のいずれかとする ※UTCTime で設定する
		notAfter	RA	－	
	subject		EE	－	C=JP, ST=加入者住所(都道府県) (任意), L=加入者住所(郡、市区町村以下) (任意), O=加入者組織名(任意), OU=加入者所属名(最大 5 つ) (任意), CN=サーバ FQDN, E =メールアドレス(任意), ※　C のみ PrintableString でエンコードし、他を PrintableString または BMPString でエンコードする。
	subjectPublicKeyInfo				
		algorithmIdentifier	IA	－	rsaEncryption(OID=1 2 840 113549 1 1 1)
		public key	EE	－	2048bit で加入者により生成
証明書標準拡張部					
	authorityKeyIdentifier		IA	F	
		keyIdentifier			公開鍵の SHA-1 値(ハッシュ値)
		authorityCertIssuer			設定しない

		authCertSerialNumber			設定しない
	subjectKeyIdentifier		IA	F	公開鍵の SHA-1 値(ハッシュ値)
	keyUsage		IA	F	digitalSignature、keyEncipherment を ON とし、他を OFF とする
	extendKeyUsage		IA	F	PKIX-IDKP-ServerAuth、PKIX-IDKP-ClientAuth を ON とし、他を OFF とする
	certificatePolicies		IA	F	
		policyIdentifier			
		certPolicyId			1 2 392 200075 4 2
		policyQualifiers			
		policyQualifierId			1 3 6 1 5 5 7 2 1(id-qt-cps)
		qualifier			https://cp.jcsinc.co.jp/SecureSign/AD/RPA.html （同意書の URI)
	basicConstraints		IA	F	
		cA			FALSE
		pathLenConstraint			NULL
	cRLDistributionPoints		IA	F	distributionPoint.fullName.URI に以下を設定する。 http://ssignadcrl01.jcsinc.co.jp/repository/crl/sca1.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/sca1.crl

(4) TSA サーバ証明書プロファイル

名称			設定者	ｸﾘﾃｨｶﾙﾃｨ	設定値
証明書基本部					
	Version		IA	－	V3
	serialNumber		IA	－	128bit 以下の正の整数
	Signature		IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
	Issuer		IA	－	C=JP, O=Japan Certification Services, Inc., CN=SecureSign Public CA11 ※PrintableString でエンコードする
	Validity				
		notBefore	RA	－	133 ヶ月とする
		notAfter	RA	－	※UTCTime で設定する

	subject		EE	―	C=JP, ST=加入者住所(都道府県) (任意), L=加入者住所(郡、市区町村以下) (任意), O=加入者組織名(任意), OU=加入者所属名(最大 5 つ) (任意), CN=サーバ FQDN, E =メールアドレス(任意), ※C のみ PrintableString でエンコードし、他を PrintableString または BMPString でエンコードする。
	subjectPublicKeyInfo				
		algorithmIdentifier	IA	―	rsaEncryption(OID=1 2 840 113549 1 1 1)
		public key	EE	―	2048bit で加入者により生成
証明書標準拡張部					
	authorityKeyIdentifier		IA	F	
		keyIdentifier			公開鍵の SHA-1 値（ハッシュ値）
		authorityCertIssuer			設定しない
		authCertSerialNumber			設定しない
	subjectKeyIdentifier		IA	F	公開鍵の SHA-1 値（ハッシュ値）
	keyUsage		IA	F	digitalSignature, nonRepudiation を ON とし、他を OFF とする
	extendKeyUsage		IA	T	PKIX-IDKP-timeStamping を ON とし、他を OFF とする
	certificatePolicies		IA	F	
		policyIdentifier			
			certPolicyId		1 2 392 200075 4 2
		policyQualifiers			
			policyQualifierId		1 3 6 1 5 5 7 2 1(id-qt-cps)
			qualifier		https://cp.jcsinc.co.jp/SecureSign/AD/RPA.html (同意書の URI)
	basicConstraints		IA	F	
		cA			FALSE
		pathLenConstraint			NULL
	cRLDistributionPoints		IA	F	distributionPoint.fullName.URI に以下を設定する。 http://ssignadcrl01.jcsinc.co.jp/repository/crl/sca1.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/sca1.crl

(5) S/MIME 証明書プロファイル

名称			設定者	ｸﾘﾃｨｶﾙﾃｨ	設定値
証明書基本部					
	Version		IA	－	V3
	serialNumber		IA	－	128bit 以下の正の整数
	Signature		IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
	Issuer		IA	－	C=JP, O=Japan Certification Services, Inc., CN=SecureSign Public CA11 ※PrintableString でエンコードする
	Validity				
		notBefore	RA	－	37 ヶ月とする
		notAfter	RA	－	※UTCTime で設定する
	subject		EE	－	C=JP, O=加入者組織名, OU=加入者所属名(任意), CN=加入者氏名, E =メールアドレス, ※C のみ PrintableString でエンコードし、他を PrintableString または BMPString でエンコードする。
	subjectPublicKeyInfo				
		algorithmIdentifier	IA	－	rsaEncryption(OID=1 2 840 113549 1 1 1)
		public key	RA	－	2048bit で RA により生成
証明書標準拡張部					
	authorityKeyIdentifier		IA	F	
		keyIdentifier			公開鍵の SHA-1 値(ハッシュ値)
		authorityCertIssuer			設定しない
		authCertSerialNumber			設定しない
	subjectKeyIdentifier		IA	F	公開鍵の SHA-1 値(ハッシュ値)
	keyUsage		IA	F	digitalSignature、keyEncipherment を ON とし、他を OFF とする
	certificatePolicies		IA	F	
		policyIdentifier			
		certPolicyId			1 2 392 200075 4 2

		policyQualifiers				
			policyQualifierId			1 3 6 1 5 5 7 2 1(id-qt-cps)
			qualifier			https://cp.jcsinc.co.jp/SecureSign/AD/RPA.html （同意書の URI)
	subjectAltName			EE	F	
		rfc822name				メールアドレス
	basicConstraints			IA	F	
		cA				FALSE
		pathLenConstraint				NULL
	cRLDistributionPoints			IA	F	distributionPoint.fullName.URI に以下を設定する。 http://ssignadcrl01.jcsinc.co.jp/repository/crl/sca1.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/sca1.crl

(6)クライアント証明書プロファイル

名称			設定者	ｸﾘﾃｨｶﾙﾃｨ	設定値
証明書基本部					
	Version		IA	－	V3
	serialNumber		IA	－	128bit 以下の正の整数
	Signature		IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
	Issuer		IA	－	C=JP, O=Japan Certification Services, Inc., CN=SecureSign Public CA11 ※PrintableString でエンコードする
	validity				
		notBefore	RA	－	37 ヶ月とする
		notAfter	RA	－	※UTCTime で設定する
	subject		EE	－	C=JP, ST=加入者住所(都道府県), L=加入者住所(郡、市区町村以下), O=加入者組織名, OU=加入者所属名(任意), CN=加入者氏名, ※C のみ PrintableString でエンコードし、他を PrintableString または BMPString でエンコードする。

	subjectPublicKeyInfo				
		algorithmIdentifier	IA	－	rsaEncryption(OID=1 2 840 113549 1 1 1)
		public key	RA	－	2048bit で RA により生成
証明書標準拡張部					
	authorityKeyIdentifier		IA	F	
		keyIdentifier			公開鍵の SHA-1 値(ハッシュ値)
		authorityCertIssuer			設定しない
		authCertSerialNumber			設定しない
	subjectKeyIdentifier		IA	F	公開鍵の SHA-1 値(ハッシュ値)
	keyUsage		IA	F	digitalSignature、nonRepudiation を ON とし、他を OFF とする
	certificatePolicies		IA	F	
		policyIdentifier			
			certPolicyId		1 2 392 200075 4 2
		policyQualifiers			
			policyQualifierId		1 3 6 1 5 5 7 2 1(id-qt-cps)
			qualifier		https://cp.jcsinc.co.jp/SecureSign/AD/RPA.html （同意書の URI)
	subjectAltName		EE	F	
		directoryName			C=JP, O=加入者組織名(日本語名称), OU=加入者所属名(日本語名称) (任意), CN=加入者氏名(日本語名称), ※C のみ PrintableString でエンコードし、他を PrintableString または BMPString でエンコードする。
	basicConstraints		IA	F	
		cA			FALSE
		pathLenConstraint			NULL
	cRLDistributionPoints		IA	F	distributionPoint.fullName.URI に以下を設定する。 http://ssignadcrl01.jcsinc.co.jp/repository/crl/sca1.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/sca1.crl

7.2 CRL プロファイル

7.2.1 バージョン番号

本サービスでは、X.509 V2 の CRL を発行する。

7.2.2 CRL エントリー拡張

本サービスでは、この拡張に設定が可能な項目のうち、理由コード(reasonCode)のみ使用する。

7.2.3 CRL プロファイル

以降この項では、本サービスで発行する CRL のプロファイル詳細を記述する。なお、記載項目は特に断りのない限り PrintableString でエンコードされる。

(1) SCA CRL プロファイル

名称			設定者	ｸﾘﾃｨｶﾙﾃｨ	設定値
証明書基本部					
	version		IA	－	V2
	signature		IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
	issuer		IA	－	C=JP, O=Japan Certification Services, Inc., CN=SecureSign Root CA11※PrintableString でエンコードする
	thisUpdate		IA	－	CRL 発行日時(UTCTime で設定する)
	nextUpdate		IA	－	thisUpdate + 6966 日 999 時間(UTCTime で設定する)
	RevokedCertificates				
		userCertificate	RA	－	シリアル番号
		revocationDate	IA	－	失効日時
	crlEntryExtensions		IA		
		reasonCode	RA		理由コードを設定する
証明書標準拡張部					
	authorityKeyIdentifier		IA	F	
		keyIdentifier			公開鍵の SHA-1 値(ハッシュ値)
		authorityCertIssuer			設定しない
		authCertSerialNumber			設定しない
	cRLNumber		IA	F	128bit 以下の正の整数

(2) EE CRL プロファイル

名称			設定者	ｸﾘﾃｨｶﾙﾃｨ	設定値
証明書基本部					
	version		IA	－	V2
	signature		IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
	issuer		IA	－	C=JP, O=Japan Certification Services, Inc., CN=SecureSign Public CA11※PrintableString でエンコードする
	thisUpdate		IA	－	CRL 発行日時(UTCTime で設定する)
	nextUpdate		IA	－	thisUpdate + 36 時間（UTCTime で設定する）
	RevokedCertificates				
		userCertificate	RA	－	シリアル番号
		revocationDate	IA	－	失効日時
	crlEntryExtensions		IA		
		reasonCode	RA		理由コードを設定する
証明書標準拡張部					
	authorityKeyIdentifier		IA	F	
		keyIdentifier			公開鍵の SHA-1 値(ハッシュ値)
		authorityCertIssuer			設定しない
		authCertSerialNumber			設定しない
	cRLNumber		IA	F	128bit 以下の正の整数

8. 仕様管理

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していく。

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､加入者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 AD 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 AD 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 AD サービスが継続されている間、変更された本規定の各版を保存する。

