JCSI ルート認証局

Certification Practice Statement

(認証局運用規程)

Version 1.4

サイバートラスト株式会社

2018 年 4 月 23 日

改訂履歴

Version	日付	改訂事由
1.0	2014 年 6 月 30 日	・ JCSI ルート認証局開局、第 1.0 版作成
1.1	2017 年 3 月 30 日	・ Baseline Requirements に対応
1.2	2017 年 7 月 20 日	・ Baseline Requirements 対応のため追加修正
1.3	2018 年 2 月 21 日	・ Baseline Requirements v1.5.6 対応のため追加修正
1.4	2018 年 4 月 23 日	・ 誤記修正

目次

1. はじめに

1.1 概要

サイバートラスト株式会社（以下、「サイバートラスト」という。）は、JCSI ルート認証局（以下、「本認証局」という）を運営する。

本認証局は以下の認証局名、シリアル番号、有効期間等で示されるパブリックルート認証局であり、サイバートラストは以下の開局日より本認証局の運営を開始する。

認証局名称	SecureSign RootCA11
認証局開局日	2014 年 6 月 30 日
認証局証明書のシリアル番号	01
認証局証明書の有効期間	2009 年 4 月 8 日～2029 年 4 月 8 日
署名方式	SHA1 with RSA
認証局の鍵長	2048 bit
ハッシュ値(SHA-1)	3BC49F48F8F373A09C1E BDF85BB1C365C7D811B3
ハッシュ値(SHA-256)	BF0FEEFB9E3A581AD5F9E9DB75899857 43D261085C4D314F6F5D7259AA421612

なお、本認証局の鍵ペアおよびルート証明書は、日本認証サービス株式会社（※）（Japan Certification Services, Inc.　以下、「JCSI 社」という。）により 2009 年 4 月 8 日に作成され、JCSI 社が 2014 年に当該ルート証明書を用いたサービス提供を終了した後、サイバートラストが取得したものである。JCSI 社のサービスおよびサービス下に提供された内容等（当該ルート証明書にチェーンする 2014 年 6 月 30 日より以前に発行された証明書と失効情報、および関連する資料・契約・対応等を含むがそれらに限られない。）については、JCSI 社の責によるものであり、サイバートラストは関知せず、その責を負わない。また、本認証局は、JCSI 社の代理人、受託者またはその他代表者ではない。

※：JCSI 社は、2013 年 6 月 30 日をもって清算法人へ移行した。2014 年 5 月時点の本社所在地は〒107-0052 東京都港区赤坂 4 丁目 9 番 17 号 赤坂第一ビル 4 階であった。その後、2015 年 2 月 26 日付けで清算結了し、会社として消滅している。

本認証局は、加入者に証明書を発行する下位の認証局（以下、「下位認証局」といい、それら下位認証局を運営する主体を「下位認証局運営者」という。）の証明書を発行する。以下、特段の規定がない限り、「証明書」という場合、下位認証局の証明書を指すものとする。

また、本認証局は、下位認証局に関わる失効情報を OCSP で提供する際に、その OCSP レスポンスに電子署名を行う OCSP 用証明書を認証局責任者の承認の下、発行する。

本認証局は、JCSI ルート認証局 Certification Practice Statement（認証局運用規程）（以下、「本 CPS」という。）第 1.4 版において、下位認証局の申請に基づく証明書の発行・失効に関わる手続きを行わないものとする。証明書の発行および失効については、本 CPS を改訂の上、それらを実施するものとする。

本認証局は、以下の規程および法令等に準拠する。

① CA/ブラウザフォーラム（以下「CAB フォーラム」という）が現在採用している現行バージョンのガイドライン（Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates（以下「Baseline Requirements」という）

② 本 CPS

③ その他日本国内に設置される本認証局の業務上関連する日本国法

本認証局は、http://www.cabforum.org で公開される Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates の最新のバージョンに準拠する。
本 CPS と Baseline Requirements の間に齟齬がある場合には Baseline Requirements が 優先される。

本 CPS は、開局日以後の本認証局の運営とそれに係る各種要件を規定する。要件には、本認証局の義務、信頼当事者の義務を含む。

また、各種要件を本 CPS に明記する上で、本認証局は、IETF PKIX ワーキンググループが定める RFC3647「Certificate Policy and Certification Practices Framework」を採用する。RFC3647 は、CPS または CP のフレームワークを定めた国際的ガイドラインである。RFC3647 のフレームワークに準じて設けた本 CPS の各規定において、本認証局に適用されない事項については、「規定しない」と記載する。

1.2 文書名と識別

本 CPS の正式名称は、「JCSI ルート認証局 Certification Practice Statement（認証局運用規程）」とする。

本 CPS および関連サービスに割り当てるオブジェクト識別子（OID）は次のとおりとする。

OID	オブジェクト
1.2.392.00200081.1.10.10	Cybertrust Japan JCSI Root Certification Authority Certificate Policy: PolicyIdentifier

1.3 PKI の関係者

本 CPS に記述される PKI の関係者を以下に定める。各関係者は、本 CPS が定める義務を遵守しなければならない。

1.3.1 認証局

本 CPS「1.1 概要」に定める本認証局をいう。本認証局は、発行局および登録局から構成される。本認証局は本 CPS「5.2.1 信頼される役割および人物」に定める認証局責任者が総括し、Cybertrust Japan Policy Authority（以下、「CTJ PA」という。）が本 CPS を承認する。

1.3.2 登録局

登録局はサイバートラストが運営し、下位認証局からの証明書の申請を受け付け、本 CPS に基づき申請内容の審査を行う。登録局は審査結果に基づき、発行局に対し、証明書の発行もしくは失効の処理の指示、または申請の棄却をする。サイバートラストは、登録局を第三者に委託しない。
なお、本 CPS「1.1 概要」に記載のとおり、本 CPS 第 1.4 版においては、本認証局は下位認証局の申請に基づく証明書の発行･失効の手続きを行わない。

1.3.3 発行局

発行局はサイバートラストが運営し、登録局の指示に基づき、証明書の発行または失効を行う。また、本 CPS に基づき、本認証局の秘密鍵を管理する。

1.3.4 下位認証局

本認証局から認証された下位の認証局であり、加入者の証明書の発行および失効等を行う。但し、本 CPS「1.1 概要」に記載のとおり、本 CPS 第 1.4 版においては、本認証局は下位認証局の証明書の発行･失効の手続きを行わない。

1.3.5 加入者

加入者は、本認証局が今後定める規程等に基づき、本認証局の下位認証局へ加入者証明書の申請を行い、下位認証局より発行された加入者証明書を利用する組織である。但し、本 CPS「1.1 概要」に記載のとおり、本 CPS 第 1.4 版においては、本認証局は下位認証局の証明書の発行･失効の手続きを行わない。このため、本 CPS 第 1.4 版においては、下位認証局による加入者の証明書の発行･失効も行われない。

1.3.6 信頼当事者

信頼当事者は、本認証局、下位認証局、および加入者の証明書の有効性について検証を行い、自らの判断でこれらの証明書を信頼する組織または個人である。

1.3.7 その他の関係者

規定しない。

1.4 証明書の用途

1.4.1 証明書の種類

1.4.1.1 本認証局証明書

本 CPS の Appendix B に示す、本認証局の証明書である。

1.4.1.2 証明書（下位認証局証明書）

下位認証局証明書は、加入者証明書を発行する下位認証局運営者の認証局を認証する。但し、本認証局は、本 CPS「1.1 概要」に記載のとおり、本 CPS 第 1.4 版において、下位認証局の申請に基づく証明書の発行を行わない。

1.4.1.3 OCSP 証明書

OCSP 証明書は、本認証局が発行し使用する OCSP 用証明書であり、下位認証局に関わる証明書の失効情報を OCSP により提供する際に、その OCSP レスポンスに対し電子署名を行う証明書である。

1.4.2 適切な証明書の用途

下位認証局の証明書は、本認証局の下位の認証局を認証するもので、認証局証明書として使用されなければならない。

OCSP 証明書は、本認証局が下位認証局の失効情報を提供する OCSP レスポンスに電子署名を行う証明書として使用されなければならない。

1.4.3 禁止される証明書の用途

本認証局は、本 CPS「1.4.2 適切な証明書の用途」に定める用途以外での証明書の使用を禁止する。

1.5 ポリシー管理

1.5.1 文書を管理する組織

本 CPS は、本認証局により管理される。

1.5.2 連絡窓口

本認証局は、本 CPS 等に関する照会の他、関連する問合せ等を以下の連絡先にて受け付ける。

同連絡窓口については、リポジトリにも明記し、24 時間 365 日、それらを受け付ける旨を記載する。

連絡先
サイバートラスト株式会社 JCSI ルート係 住　所　：〒107-6030　東京都港区赤坂 1 丁目 12 番 32 号アーク森ビル 30 階 宛　先　：jcsi-r@cybertrust.ne.jp

1.5.3 CPS の適合性を決定する者

CPS の適合性についてはサイバートラストが決定する。

1.5.4 適合性の承認手続き

サイバートラストの社内規程に定められる評価・承認手続きの中で、サイバートラストの CTJ PA が承認する。

1.6 定義と略語

本 CPS の Appendix A に規定する。

2. 公開とリポジトリの責任

2.1 リポジトリを管理する組織

本認証局のリポジトリは、サイバートラストが管理する。

2.2 公開する情報

本認証局は、次のとおりリポジトリで公開する。

以下の情報を https://www.cybertrust.ne.jp/jcsi/repository.html 上に公開する。

・本 CPS

以下の情報を、http://rtcrl.managedpki.ne.jp/SecureSignAD/SecureSignRootCA11/cdp.crl 上に公開する。

・本認証局が発行する証明書の CRL

以下の情報を、http://rtcrl.managedpki.ne.jp/SecureSignAD/SecureSignRootCA11/SSAD-rca.crt 上に公開する。

・本認証局の証明書

2.3 公開の時期と頻度

本認証局が公開する情報について、公開の時期と頻度は以下のとおりである。ただし、リポジトリのメンテナンス等が生じる場合は、この限りでないものとするが、CRL は 24 時間公開される。

① 本リポジトリは 24 時間 365 日公開を維持する

② 本 CPS については、改訂の都度、公開される

③ CRL は、本 CPS「4.9.7 CRL 発行周期」で規定されたとおり更新を行い、公開される

④ 本認証局の証明書については、少なくとも本認証局の運用期間中は公開される

2.4 リポジトリに対するアクセスコントロール

本認証局は、リポジトリに対する特段のアクセスコントロールは講じない。

3. 識別および認証

本認証局は、本 CPS「1.1 概要」に記載のとおり、本 CPS 第 1.4 版では、下位認証局の申請に基づく証明書の発行・失効を行わず、よって、下位認証局による加入者証明書の発行・失効も行われない。このため、本 CPS 第 1.4 版では、加入者証明書に関わる本章の各項目を規定しない。本章の各項目については、サイバートラストは、証明書の発行・失効を開始する際、改めて規定する。

なお、上記に関わらず、証明書の発行・失効を開始する際には、本 CPS 3.2.2 章に申請者の組織とドメインの確認手続きとして以下を記載する。また、CPS 3.2.3 章、3.2.5 章、3.2.6 章として以下を記載する。

3.2 初回の本人性確認

3.2.2 組織とドメインの認証

3.2.2.1 身元の確認

下位認証局は、加入者の確認に際しては、公的書類・データ、下位認証局により信頼性が確保されていると判断された第三者が提供する書類・データまたは加入者より提供される書類・データを用いるほか、加入者の組織の内部の適切な個人もしくは加入者を構成する組織へ照会を行う。また、必要に応じ加入者への訪問調査を行う。

3.2.2.2 DBA/Tradename

下位認証局は、加入者の証明書に DBA/Tradename を含めることを認めない。

3.2.2.3 Country の確認

下位認証局は、加入者の証明書に含まれる Country を本 CPS「3.2.2.1 身元の確認」で確認する。

3.2.2.4 ドメイン名の認証またはコントロールの検証

下位認証局は、申請者がドメイン名の使用または管理を行う権利について Baseline Requirements により許容される以下の手続きのうち 1 つ以上を用いて認証する。

なお、下位認証局は、ドメインの確認を第三者に委託しない。

3.2.2.4.1 ドメイン連絡先としての申請者の検証

下位認証局は、加入者の FQDN に対する管理を加入者がドメインの連絡先であることをドメイン名レジストラへ直接確認することにより検証する。この手法は以下の場合に使用する。

① 下位認証局が Baseline Requirements 3.2.2.1 章に基づき加入者の身元を証明し、Baseline Requirements 3.2.5 章に記される加入者を代表する権限を証明する場合

② 下位認証局が EV ガイドライン 11.2 に従い申請者の身元を証明し、加入者を代表する権限を EV ガイドライン 11.8 に従い証明する場合

③ 下位認証局がベースドメイン名のドメイン名レジストラ、またはそのアフェリエイトでもある場合

但し、2018 年 8 月 1 日以降、本手法は使用しない。

3.2.2.4.2 ドメイン連絡先への電子メール、FAX、SNS、または郵送

下位認証局は、ランダム値を電子メール、FAX、SMS、または郵送で送付し、確認した相手からそのランダム値を使用した返答を受け取ることで、加入者の FQDN 管理権限を確認する。ランダム値は、ドメイン連絡先として識別されるメールアドレス、SMS 番号または住所へ送付されなければならない。

それぞれの電子メール、FAX、SMS、または郵送では、複数の承認ドメイン名の確認ができる。

下位認証局は、本章で識別された電子メール、FAX、SMS または郵送を、複数の受信者に対して送付することができる。ただし、すべての受信者はドメイン名レジストラによって電子メール、FAX、SMS、または郵送によって検証されたすべての FQDN に対し、ドメイン所有者を表明する者として識別された者とする。

ランダム値は電子メール、FAX、SMS、または郵送でそれぞれ一意でなければならない。

下位認証局は、電子メール、FAX、SMS、郵送書類のその全体を再送することができ、その通信における内容と受信者が同一の場合に限り、ランダム値を再利用する。

ランダム値は、その作成日から 30 日以内の確認応答につき有効なものとする。

3.2.2.4.3 ドメイン連絡先へ電話

下位認証局は、ドメイン所有者の電話番号へ架電し、FQDN の検証のための加入者の要求について承認応答を得ることにより、加入者の FQDN に対する管理権限を確認する。下位認証局は、ドメイン名レジストラによってドメイン連絡先として識別された電話番号を使いドメイン名登録者へ電話す。

それぞれの通話は一つの番号に対して行われるものとし、複数の FQDN の管理権の確認を行うことができる。ただし、その電話番号がドメイン名レジストラによって電話で検証をするすべてのドメイン名に対し有効な通信手段として識別されている場合とする。

3.2.2.4.4 ドメイン連絡先へ構築電子メール

下位認証局は、FQDN に対する加入者の管理権限を(i)'admin', 'administrator', 'webmaster', 'hostmaster', または'postmaster'をローカルパートとして@、承認ドメイン名と続くように作成された一つまたは複数のメールアドレスへ電子メールを送信し(ii)ランダム値をメール内に含め、(iii)ランダム値を使用した返信を受信することにより確認する。

それぞれのメールでは複数の FQDN に対する管理権限の承認が可能である。ただし、電子メール内で使用される承認ドメイン名が確認されたそれぞれの FQDN に対する承認ドメイン名である必要がある。

ランダム値は、それぞれのメールで一意でなければならない。

その内容と受信者が同一である場合に限り、ランダム値の再利用を含めメール全体を再送することができる。

ランダム値は、その作成日から 30 日以内の確認応答につき有効なものとする。

3.2.2.4.5 ドメイン認可文書

下位認証局は、加入者証明書を要求する権限を当該加入者が有することを記載したドメイン認可文書に依拠して、当該加入者が FQDN を管理していることを確認する。

ドメイン認可文書は、ドメイン連絡先から来たことを立証しなれればならない。

下位認証局は、ドメイン認可文書が (i) ドメインの検証要求日以降の日付、または (ii) WHOIS のデータが、以前に提供されたドメイン名スペース用のドメイン許可文書から実質的に変更されていないことを確認する。

但し、2018 年 8 月 1 日以降、本手法は使用しない。

3.2.2.4.6 合意に基づく Web サイトの変更

下位認証局は、認可されたポートを介した HTTP / HTTPS 経由で"/.well‐known/pki‐validation" ディレクトリの下またはドメイン検証の目的で IANA に登録した他のパスのいずれかで、アクセス可能な認証ドメイン名を確認し、申請者の FQDN の管理権限を確認する。

① ファイルのコンテンツの中に構成されたウェブサイトコンテンツの存在。必要とされたウェブサイトコンテンツは、ファイルまたは Web ページの取得に使用されたリクエスト内にあってはいけない。

② リクエストトークンまたはリクエスト値の存在がファイルの内容に含まれるリクエストトークンまたはランダム値として要求に現れてはならない。

ランダム値が使用される場合、下位認証局は、加入者証明書の申請に一意のランダム値を提供し、その値は、(i)30 日間、または(ii)申込者が加入者証明書要求を行った場合には、加入者証明書に関する有効な情報の再利用が許可された期間（Baseline Requirements 4.2.1 章及び EV ガイドライン 11.14.3 章）を超えて使用しない。

3.2.2.4.7 DNS の変更

下位認証局は、1）承認ドメイン名、または 2）アンダーバーのついたラベルを接頭辞とする承認ドメイン名のどちらかに対する、DNS CNAME、TXT、または CAA レコードのいずれかにランダム値及びリクエストトークンの存在を確認することによって申請者の FQDN に対する管理権限を確認する。

ランダム値が使用される場合、下位認証局は加入者証明書の要求に対し一意の値を発行するものとし、そのランダム値は(i)30 日間、または(ii)申請者が加入者証明書要求を行った場合、加入者証明書に関連する（Baseline Requirements 3.3.1 章及び EV ガイドライン 11.14.3 章のような）審査情報の再使用が許可された期間を超えて使用しない。

3.2.2.4.8 IP アドレス

下位認証局は、本 CPS3.2.2.5 に従い、申請者が FQDN の A または AAAA レコードに対する DNS ルックアップから戻される IP アドレスを管理することを確認することで、申請者のドメイン管理権限を承認する。

3.2.2.4.9 テスト証明書

下位認証局では採用しない。

3.2.2.4.10 ランダムナンバーを使用した TLS

下位認証局では採用しない。

3.2.2.5 IP アドレスの認証

下位認証局は、加入者証明書の発行時点で、同加入者証明書に記載されている各 IP アドレスを加入者が管理することを次のいずれかの方法で確認する。

① IP アドレスを含む統一されたリソース識別子によって識別されるオンライン Web ページ上の情報に合意した変更を加えることにより、IP アドレスに対する実用的な制御を実証する

② IANA（Internet Assigned Numbers Authority）または Regional Internet Registry（RIPE、APNIC、ARIN、AfriNIC、LACNIC）からの IP アドレス割り当てに関する資料を入手する

③ 逆 IP アドレス検索の実行し、本 CPS3.2.2.4 の結果として得られるドメイン名の管理を検証する

④ その他の確認方法。この場合、下位認証局は、加入者が IP アドレスの管理を有することを確認した本方法が、少なくとも上記①～③の方法と同レベルの確度を有していることを示す文書証拠を保管するものとする

3.2.2.6 ワイルドカードドメインの認証

下位認証局は、DNS またはタイプ DNS-ID の CN または subjectAltName でワイルドカード文字（*）を使用する加入者証明書を発行する前に、ワイルドカード文字が「レジストリ・コントロール」ラベルまたは「パブリックサフィックス」の左側に第 1 のラベルの位置で発生したかどうかを判断する（例："* .com"、 "* .co.uk"、詳細は RFC 6454 セクション 8.2 を参照）。「レジストリ・コントロール」の判断は、Baseline Requirements 3.2.2.6 章に従うものとする。

下位認証局は、ワイルドカードがレジストリ制御またはパブリックサフィックスのすぐ左側にある場合、ドメインネームスペース全体の正当な管理を証明しない限り、発行を拒否する。

3.2.2.7 データソースの正確度

下位認証局は、データソースを使用する前に信頼できるデータソースとして評価する。データベースの評価は精度、および変更または改ざんに対する耐性など以下の項目について確認する。

- 提供された情報の期間
- 情報源への更新の頻度
- データ収集のデータ提供者と目的
- データ可用性の一般的なアクセシビリティ
- データを改ざんまたは変更する際の相対的な難しさ

下位認証局、その所有者、またはその提携企業によって管理されているデータベースは、本 CPS 3.2 の検証要件を満たす目的で情報を収集することがデータベースの第一の目的である場合、これを信頼できるデータソースとして採用しない。

3.2.3 個人の身元の認証

規定しない。

3.2.5 権限の確認

下位認証局は、Baseline Requirements 3.2.5 章に従い信頼できるコミュニケーション手段を用いて証明書要求を確認する。

3.2.6 相互運用性基準

規定しない。

4. 証明書のライフサイクル運用的要件

本認証局は、本 CPS「1.1 概要」に記載のとおり、本 CPS 第 1.4 版では、下位認証局の申請に基づく証明書の発行・失効の手続きを行わず、よって、下位認証局による加入者証明書の発行・失効も行われない。このため、それら加入者証明書の発行・失効に関わる以下の記載、すなわち、本 CPS「4.1 証明書申請」から「4.8 証明書の変更」、「4.9 証明書の失効および一時停止」の一部、および「4.10 証明書のステータス確認サービス」から「4.12 鍵の第三者預託および鍵回復」の各規程については、サイバートラストは、証明書の発行・失効を開始する際、改めて規定する。

なお、上記に関わらず、証明書の発行・失効を開始する際には、本 CPS 4.1 章、4.2 章、4.3.1 章、4.9 章、4.10 章として以下を記載する。

4.1 証明書申請

4.1.1 証明書の申請が認められる者

申請者または申請者のために加入者証明書の申請を行う資格を有する個人は、下位認証局に対し、加入者証明書の申請を提出することができる。申請者またはその代理人が下位認証局に提供する全てのデータについては、申請者が責任を負う。

4.1.2 申請方法および責任

加入者は、本 CPS および加入契約書に同意の上、加入者証明書の申請を行う。申請に際し、加入者には、真正かつ正確な情報を下位認証局へ提供する責任がある。
加入者証明書の申請方法については、サイバートラストの Web サイトに掲載する。

4.2 証明書申請の処理

4.2.1 本人性確認と認証業務の実行

本 CPS「3.2 初回の本人性確認」と同様の手続きにより行う。下位認証局の登録局が実施する。

4.2.2 証明書申請の承認または拒否

下位認証局は、下位認証局が加入者証明書の申請を認証できない場合、その申請を却下する。また、下位認証局は、加入者証明書の発行がサイバートラストの評判または事業に損害を与えまたはこれらを損なう可能性があると判断した場合に、その申請を却下することがある。

加入者証明書の申請が却下されず、正常に認証された場合、下位認証局は加入者証明書の申請を承認し加入者証明書を発行する。下位認証局は、却下された申請について責任を負わず、その理由を開示する義務を負わない。却下された申請者は再度申請を行うことができる。加入者は、加入者証明書を使用する前に加入者証明書のコンテンツの正確性をチェックする必要がある。

4.3 証明書の発行

4.3.1 認証局における証明書発行処理

下位認証局の登録局は、本 CPS「3.2 初回の本人性確認」に基づき申請処理を完了した後、下位認証局の発行局に対し加入者の証明書の発行を指示する。同発行局は、加入者証明書を発行すると同時に、加入者に対する通知を行う。

4.4 証明書の受領

規定しない。

4.5 鍵ペアと証明書の利用

規定しない。

4.6 鍵更新を伴わない証明書の更新

規定しない。

4.7 鍵更新を伴う証明書の更新

規定しない。

4.8 証明書の変更

規定しない。

4.9 証明書の失効および一時停止

4.9.1 失効に関する要件

4.9.1.1 加入者証明書の失効理由

加入者証明書を発行する下位認証局は、加入者証明書の発行を開始した後、以下のいずれかの事由が生じた場合、24 時間以内に該当の加入者証明書を失効する。

① 下位認証局が、加入者から書面により失効が要求された場合

② 加入者から、元の加入者証明書の申請は許可されておらず、遡及して許可を与えないことが、加入者証明書を発行した下位認証局に通知された場合

③ 加入者の秘密鍵が危殆化または危殆化の可能性があること、または Baseline Requirements 6.1.5 章または 6.1.6 章の要件を満たさなくなったことを合理的な証拠に基づき下位認証局が知り得た場合

④ 加入者証明書が不正に使用されていることを合理的な証拠に基づき下位認証局が知り得た場合

⑤ 加入者が本 CPS または加入契約書に違反していることを下位認証局が知り得た場合

⑥ 加入者が、加入者証明書に含まれる FQDN または IP アドレスを独占的に使用する権利を失ったことを下位認証局が知り得た場合

⑦ 加入者が、ワイルドカード証明書を使用して、間違った下位ドメイン名を認証していることを下位認証局が知り得た場合

⑧ 加入者証明書の内容に変更が生じたことを下位認証局が知り得た場合

⑨ 下位認証局が、CPS に準拠せずに加入者証明書を発行した場合

⑩ 加入者証明書の内容が事実と異なる、または誤解を招く場合

⑪ 加入者証明書を発行する下位認証局が何らかの理由で運用を中止し、かつ、発行済みの加入者証明書について他の認証局も失効に関わる運用を代行しない場合

⑫ 加入者証明書を発行する下位認証局が CRL/OCSP リポジトリを維持しようとせず、各種要件下に加入者証明書を発行する権利が期限切れとなるか、取り消されるか、または解除される場合

⑬ 加入者証明書を発行する下位認証局の秘密鍵が危殆化もしくは危殆化の可能性があることを下位認証局が知り得た場合

⑭ 下位認証局が、CPS に基づき加入者証明書の失効を求められた場合

⑮ 証明書の技術的内容または書式が、アプリケーションソフトウェアサプライヤまたは依拠当事者に容認できないリスクを与える場合

4.9.1.2 下位認証局証明書の失効理由

本認証局は、以下のいずれかの事由が生じた場合、7 日以内に該当の下位認証局証明書を失効する。

① 下位認証局から書面により失効が要求された場合

② 下位認証局から、元の証明書申請は許可されておらず、遡及して許可を与えないことが本認証局に通知された場合

③ 下位認証局の秘密鍵が危殆化または危殆化の可能性があること、または Baseline Requirements 6.1.5 章または 6.1.6 章の要件を満たさなくなったことを合理的な証拠に基づき本認証局が知り得た場合

④ 下位認証局証明書が不正に使用されていることを合理的な証拠に基づき本認証局が知り得た場合

⑤ 下位認証局が Baseline Requirements または CPS に違反していることを本認証局が知り得た場合

⑥ 下位認証局の証明書の内容が事実と異なる、または誤解を招く場合

⑦ 下位認証局または本認証局が何らかの理由で運用を中止し、かつ、発行済みの加入者証明書について他の認証局も失効に関わる運用を代行しない場合

⑧ 下位認証局が CRL/OCSP リポジトリを維持しようとせず、各種要件下に下位認証局または本認証局の権利が期限切れとなるか、取り消されるか、または解除される場合

⑨ 本認証局が、本 CPS に基づき下位認証局証明書の失効を求められた場合

⑩ 証明書の技術的内容または書式が、アプリケーションソフトウェアサプライヤまたは依拠当事者に容認できないリスクを与える場合

4.9.1.3 その他の証明書の失効理由

(1) 本認証局証明書

本認証局は、以下のいずれかの事由が生じた場合、それが判明した時点で、本認証局の証明書を失効する。ただし②については、別途本認証局が業務終了前に事前に通知した日に失効することができる。

① 本認証局の秘密鍵の危殆化を知り得た場合

② 本認証局が認証業務を終了する場合

(2) OCSP 用証明書

本認証局は、以下のいずれかの事由が生じた場合、それが判明した時点で、該当する OCSP 用証明書を失効する。ただし②については、別途本認証局が業務終了前に事前に通知した日に失効することができる。

① OCSP 用証明書に関わる秘密鍵の危殆化を知り得た場合

② 本認証局が認証業務を終了する場合

4.9.2 失効申請が認められる者

正当な資格を有する当事者（加入者の指定する代表者等）は、加入者証明書の失効 処理を下位認証局に要求することができる。第三者は、不正行為、悪用、または危殆化に関連する問題を理由として加入者証明書 の失効処理を下位認証局に要求することができる。証明書失効要求は、失効処理を求めるエンティティと失効処理を求める 理由を特定しなければならない。

4.9.3 失効申請の手続き

加入者は、サイバートラストが提供する Web サイトまたは電子メールにより失効申請を行う。失効申請内容には、加入者証明書を発行する下位認証局の案内に従い、下位認証局と加入者のみが知る情報、失効事由、連絡先等を含めなければならない。同下位認証局は、失効事由を確認する。

本認証局証明書および OCSP 証明書の失効については、認証局責任者が発行局に指示する。

4.9.4 失効申請までの猶予期間

認証局責任者は、本 CPS「4.9.1.2 下位認証局証明書の失効理由」または「4.9.1.3 その他の証明書の失効理由」に該当する事由が生じたときは、速やかに失効指示を行う。

4.9.5 認証局における失効処理にかかる時間

本認証局は、24 時間 365 日失効申請を受け付ける。

本認証局の登録局は、失効申請を受け付け、本 CPS「4.9.3 失効申請の手続き」の規定に基づく手続きを行った後、速やかに発行局に対し対象となる証明書の失効を指示する。発行局は、失効の指示を受けた後、遅滞なく当該証明書を失効する。

4.9.6 信頼当事者による失効の確認方法

信頼当事者は、本認証局が発行する CRL または OCSP により、下位認証局に関わる証明書の失効を確認する。

4.9.7 CRL 発行周期

下位認証局は、CRL を 24 時間以内の周期で発行する。

本認証局は、本 CPS「4.9.1.2 下位認証局証明書の失効理由」または「4.9.1.3 その他の証明書の失効理由」に該当する事由が生じる都度、または少なくとも年1回、CRL を発行する。

4.9.8 CRL 公開までの最大遅延時間

本認証局は、CRL 発行後、遅滞なくポジトリに公開する。

4.9.9 オンラインでの失効情報の確認

本認証局の OCSP レスポンダは RFC 6960 に準拠する。

OCSP レスポンスは、ステータスを確認する証明書を発行した認証局によって署名される OCSP 証明書を使用する OCSP レスポンダによって署名される。

OCSP 証明書は id-pkix-ocsp-nocheck の extension を有する。

4.9.10 オンラインでの証明書ステータスの確認

OCSP については GET method をサポートする。

下位認証局は、CRL に加え OCSP により失効情報を提供する。下位認証局は、240 時間の有効期間を有する OCSP レスポンスを少なくとも 96 時間以内の周期で更新する。

本認証局は、OCSP により、下位認証局に関わる証明書の失効情報の提供を行う。本認証局は少なくとも1年に1度、および下位認証局証明書を失効してから 24 時間以内に OCSP をアップデートする。

OCSP は、認証局が発行していない証明書についてのステータス確認を受けた場合、”good”を返さない。

なお、OCSP リクエスト受付 URL は以下となる。
http://rtocsp.managedpki.ne.jp/OcspServer

4.9.11 その他の利用可能な失効情報の提供手段

規定しない。

4.9.12 鍵の危殆化に関する特別要件

4.9.12.1 本認証局証明書

本認証局は、本認証局の秘密鍵の危殆化を知り得た場合、本 CPS「4.9.3 失効申請の手続」に基づき本認証局証明書の失効処理を行う。

4.9.12.2 OCSP 用証明書

本認証局は、OCSP 用証明書に関わる秘密鍵の危殆化を知り得た場合、本 CPS「4.9.3 失効申請の手続」に基づき当該 OCSP 用証明書の失効処理を行う。

4.9.13 証明書の一時停止に関する要件

規定しない。

4.9.14 一時停止の申請が認められる者

規定しない。

4.9.15 一時停止の申請手続き

規定しない。

4.9.16 一時停止の期間

規定しない。

4.10 証明書のステータス確認サービス

本認証局は、CRL および OCSP 以外で証明書のステータスを確認できるサービスを提供しない。

4.10.1 動作特性

CRL または OCSP レスポンスの失効エントリは、失効した証明書の有効期限まで削除しない。

4.10.2 サービスの可用性

本認証局は、通常の動作条件で 10 秒以下の応答時間を提供するのに十分なリソースをもって、CRL および OCSP 機能を運用および維持するものとする。

本認証局は、アプリケーションソフトウェアが有効期限内の証明書の現行ステータスを確認できるよう、24 時間 365 日、オンラインリポジトリを維持するものとする。

本認証局は、優先順位の高い、証明書に関わる問題の通知に 24 時間 365 日にて対応する能力を維持し、必要に応じてそのような苦情を CTJ PA に送付し、かつ/またはそのような苦情の対象となる証明書を失効する。

4.11 加入（登録）の終了

規定しない。

4.12 鍵の第三者預託および鍵回復

規定しない。

5. 運営、運用、物理的管理

5.1 物理的管理

5.1.1 立地場所および構造

本認証局のシステムは、地震、火災、水害およびその他の災害による影響を容易に受けない施設（以下、「本施設」といい、特段の規定がない限り、「本施設」という場合は、メインサイトおよび本 CPS「5.1.9 バックアップサイト」に定めるバックアップサイトを含むものとする。）内に設置される。また、本施設には、建築構造上、耐震、耐火および水害その他の災害防止ならびに不正侵入防止の措置が講じられる。なお、本施設が設置される建築物の外部および建築物内には、本認証局の所在に関わる情報を表示しない。

5.1.2 物理的アクセス

本施設および本施設内で認証業務が行われる各室は、業務の重要度に応じたセキュリティ・レベルが設けられ、相応する入退室管理が行われる。入退室時の認証には、セキュリティ・レベルに応じ、入退室用カードまたは生体認証その他の実装可能な技術的手段を用いる。また、特に重要な各室への入室および同室内において本認証局のシステムその他重要資産が保管される保管庫の開扉の両方またはいずれか一方は、入室権限を有する複数名が揃わなければ開扉されない措置を講ずる。

本施設および本施設内の認証業務が行われる各室は、監視システムにより、24 時間 365 日の監視が行われる。

5.1.3 電源･空調設備

本施設では、本認証局のシステムおよび関連機器類の運用のために必要かつ十分な容量の電源を確保する。また、瞬断ならびに停電対策として、無停電電源装置および自家発電機を設置する。さらに、認証業務を行う各室には空調設備を設置し、特に重要な室内は 2 重化する。

5.1.4 水害対策

本施設内の認証業務を行う特に重要な各室には漏水検知機を設置し、防水対策を講じる。

5.1.5 火災対策

本施設は、耐火構造の建物である。また、特に重要な各室は防火区画内に設置され、火災報知機および自動ガス式消火設備を備える。

5.1.6 地震対策

本施設は耐震構造の建物であり、また、本認証局のシステム機器および什器には転倒および落下を防止する対策を講じる。

5.1.7 媒体保管場所

本認証局のシステムのバックアップデータが含まれる媒体、本認証局の運用に関わる帳票等については、職務上許可された者のみが入室できる室内に保管する。

5.1.8 廃棄物処理

機密情報を含む書類はシュレッダーにより裁断の上、廃棄する。電子媒体については、物理的破壊、初期化、消磁等の措置によって記録されたデータを完全に抹消の上、廃棄する。

5.1.9 バックアップサイト

本認証局の秘密鍵およびシステムの復旧上重要な資産の原本またはコピーは、メインサイト内のほか、遠隔地のバックアップサイトにも保管する。バックアップサイトの保管庫は、複数名の者により施錠管理され、また、開扉の記録が残される。

5.2 手続的管理

5.2.1 信頼される役割および人物

本認証局は、認証局を運営するために必要な人員（以下「認証局員」という。）およびその役割を以下のとおり定める。
但し、本認証局は、本 CPS「1.1 概要」に記載のとおり、本 CPS 第 1.4 版では、下位認証局、ならびに下位認証局を通じての加入者証明書の発行・失効を行わないことから、登録局に関わる認証局員（以下に定める登録局管理者、登録局オペレータ管理者、および登録局オペレータ）を任命しない。これら登録局に関わる認証局員については、証明書の発行・失効に際して別途任命する。

5.2.1.1 認証局責任者

認証局責任者は、本認証局を総括する。

5.2.1.2 発行局管理者

発行局管理者は、本認証局の発行局業務を管理する。

5.2.1.3 発行局システムアドミニストレータ

発行局システムアドミニストレータは、発行局管理者の管理の下、本認証局のシステムの維持・管理（認証局責任者の指示に基づく OCSP 用証明書の発行等を含む）を行う。

5.2.1.4 発行局オペレータ

発行局オペレータは、発行局管理者および発行局システムアドミニストレータの業務を補佐する。ただし、本認証局のシステムを操作する権限は付与されない。

5.2.1.5 登録局管理者

登録管理者は、本認証局の登録局業務を管理する。

5.2.1.6 登録局オペレータ管理者

登録局オペレータ管理者は、登録局オペレータを管理する。

5.2.1.7 登録局オペレータ

登録局オペレータは、登録局管理者の管理の下、下位認証局からの申請を処理し、発行局に対し証明書の発行または失効を依頼する。

5.2.2 役割ごとに必要とされる人数

本認証局は、発行局システムアドミニストレータおよび登録局オペレータについては、それぞれ 2 名以上配置する。

5.2.3 各役割における本人性確認と認証

本認証局は、各役割に応じ、認証業務を行う各室の入室権限および本認証局のシステムの操作権限を定める。各室の入室時またはシステムの操作時においては、入退室カード、生体認証、電子証明書、ID およびパスワード等の単体または組合せより、本人性および入室・操作権限の確認ならびに認証が行われる。

5.2.4 職務の分離が必要とされる役割

本認証局は、発行局と登録局の業務の兼務を認めない。また、認証局責任者が他の役割を兼務することも認めない。

5.3 人事的管理

5.3.1 経歴、資格、経験等に関する要求事項

認証局員は、サイバートラストが別途定める採用基準に基づき採用され、配置される。

5.3.2 身元調査手続き

認証局員として配置される社員の身元調査は、サイバートラストの社内規程に基づき行われる。

5.3.3 教育および訓練

本認証局は、認証局員として配置されるすべての従業員に対し教育および訓練を実施する。教育および訓練には、本 CPS の教育のほか、認証局員の役割に応じた必要な教育および訓練を含む。

また、教育および訓練の有効性は発行局管理者または登録局管理者が評価し、必要に応じ再教育・訓練を実施する。

5.3.4 再教育・訓練の周期と要件

本認証局は、認証局員に対する再教育および訓練を適宜実施する。少なくとも以下の事態が生じた場合は、教育・訓練を実施する。

① 本 CPS の変更時で、CTJ PA、認証局責任者、発行局管理者または登録局管理者が必要と判断した場合

② 本認証局のシステムの変更をする場合であって、CTJ PA、認証局責任者、発行局管理者または登録局管理者が必要と判断した場合

③ その他、CTJ PA、認証局責任者、発行局管理者、登録局管理者が必要と判断した場合

5.3.5 職務ローテーションの周期と順序

本認証局は、必要に応じ認証局員の配置転換を行う。

5.3.6 許可されていない行動に対する罰則

サイバートラストは、認証局員が本 CPS に反する行動をした場合、速やかに原因ならびに影響範囲等の調査を行った上で、サイバートラストの就業規則に準じ、処罰を課す。

5.3.7 契約社員等に対する契約要件

サイバートラストは、業務委託先の社員、契約社員または派遣社員等（以下、「契約社員等」という。）を認証局員として配置する場合、委託業務の内容、契約社員等に課す守秘義務および罰則等を明確に定めた契約を結ぶとともに、契約社員等に対し、本 CPS およびサイバートラストの社内規程の遵守を要求する。契約社員等が本 CPS およびサイバートラストの社内規程に反する行動をした場合、処罰については、当該契約に基づき行う。

5.3.8 認証局員が参照できる文書

本認証局は、各認証局員に対し、役割に応じた必要な文書のみを参照できる措置を講ずる。

5.4 監査ログの手続き

5.4.1 記録されるイベントの種類

本認証局は、本 CPS の準拠性およびセキュリティの妥当性を評価するため、監査ログとして以下の記録を収集する。なお、記録には日時、記録の主体、イベントの内容を記録する。
但し、登録局に関わる①、②の記録については、別途、下位認証局の申請に基づく証明書の発行・失効の開始後、記録するものとする。

① 登録局による審査の記録
② 登録局および発行局が維持管理するシステム上の記録
③ 本施設の入退室に関する記録
④ 本施設の維持管理に関する記録

5.4.2 監査ログを処理する頻度

本認証局は、本 CPS「5.4.1 記録されるイベントの種類」に規定された監査ログに関し、週次、月次または四半期に一度の頻度で検査する。

5.4.3 監査ログの保管期間

登録局による審査の記録については、当該審査により発行された証明書の有効期間満了日または本認証局の運用終了日のいずれか早い日の後、少なくとも 7 年間は保管する。

他の記録については、少なくとも 7 年間は保管する。

本認証局は、監査ログが不要となったとき、本 CPS「5.1.8 廃棄物処理」の規定に基づき廃棄する。

5.4.4 監査ログの保護

本認証局は、許可された者のみが閲覧可能となるよう、監査ログへのアクセスコントロールを施す。保管庫への物理的なアクセスコントロール、電子媒体であればフォルダ等への論理的なアクセスコントロールを施す。

5.4.5 監査ログのバックアップ手続き

本認証局は、登録局および発行局のシステム上のログについては、バックアップを取得する。紙媒体については、原本のみを保管する。

5.4.6 監査ログの収集システム

登録局および発行局のシステムは、実装された機能により監査ログを自動的に収集する。

5.4.7 当事者への通知

本認証局は、イベントを発生させた当事者に通知することなく、監査ログを収集、検査する。

5.4.8 脆弱性評価

サイバートラストは年 1 回、リスクアセスメントを実施して、本認証局システム（本認証局の OCSP を含む）への無許可のアクセス、開示、悪用、改ざん、または破壊を招く可能性のある合理的に予測可能な内部および外部からの脅威を特定する。またサイバートラストは、かかるリスクを管理するためにサイバートラストが設けている手続き、情報システム、技術、その他の取り決めが十分であるかを定期的に評価する。内部監査人はセキュリティ監査データチェックをレビューする。サイバートラストの監査ログモニタリングツールは、繰り返し失敗したアクション、部外秘情報の要求、システムファイルへのアクセス試行、認証済みでないレスポンス等のイベントについて適切な職員に警告を出す。

5.5 記録の保管

5.5.1 保管対象となる記録

本認証局は、本 CPS「5.4.1 記録されるイベントの種類」で規定された監査ログのほか、以下の情報を保管する。
但し、②、⑥の記録については、別途、下位認証局の申請に基づく証明書の発行･失効の開始後、記録するものとする。

① 本認証局の証明書
② 下位認証局の証明書
③ CRL
④ 内部監査報告書
⑤ 外部監査報告書
⑥ 下位認証局より受理した申請書類･データ
⑦ 本 CPS

5.5.2 記録の保管期間

本認証局は、本 CPS「5.5.1 保管対象となる記録」に規定される記録について、関連する証明書の有効期間満了日または本認証局の運用終了日のいずれか早い日を超えて少なくとも 7 年間保管する。

本認証局は、記録が不要となったとき、本 CPS「5.1.8 廃棄物処理」の規定に基づき廃棄する。

5.5.3 記録の保護

本 CPS「5.4.4 監査ログの保護」と同様の手続きにより行う。

5.5.4 記録のバックアップ手続き

本 CPS「5.4.5 監査ログのバックアップ手続き」と同様の手続きにより行う。

5.5.5 タイムスタンプ

本認証局は、帳票類については起票日もしくは処理した日付を記録する。また、日付のみでは記録としての立証性に欠ける場合は、時刻も記録する。証明書については、発行された日時を記録する。また、本認証局のシステムについては、発行する証明書および監査ログに対して正確な日付･時刻を記録するために必要な措置を講じる。

5.5.6 記録収集システム

証明書については、本認証局のシステムの機能により自動的に収集する。その他の紙媒体については、認証局員が収集する。

5.5.7 記録の取得と検証手続き

本認証局は、記録の取得および閲覧が認められる者として、CTJ PA、認証局員、監査人および認証局責任者が認めた者に限定する。また、記録の可読性に関わる検証は、必要に応じ、実施する。

5.6 認証局の鍵更新

規定しない。

5.7 危殆化および災害からの復旧

5.7.1 危殆化および災害からの復旧手続き

本認証局は、本認証局の秘密鍵の危殆化を知り得た場合、以下を実行すると同時に、危殆化の事実を本認証局の証明書を登録しているブラウザベンダへ連絡し、また、リポジトリに公開する。

① 危殆化した秘密鍵を用いた認証業務の停止

② 本認証局の開局後発行されたすべての下位認証局に関わる証明書の失効

③ 対応措置（下位認証局への対応、危殆化の原因調査、是正措置、サービス再開方法等を含むがそれらに限られない）の検討、決定と実施

また、本認証局が被災した場合には、本 CPS「5.7.4 災害時等の事業継続性」に規定する業務継続計画に基づき、バックアップした鍵情報・データ等により復旧作業を行い、認証業務の再開に努め、再開時には再開の事実をリポジトリに公開する。

5.7.2 システム資源の障害時の手続き

本認証局は、ハードウェア、ソフトウェアまたはデータが破壊された場合には、保守対応やバックアップデータ等を用いてシステムを復旧し、認証業務を継続する。

5.7.3 加入者秘密鍵の危殆化時の手続き

本認証局は、本 CPS「1.1 概要」に記載のとおり、本 CPS 第 1.4 版では、下位認証局の申請に基づく証明書の発行・失効を行わず、従って下位認証局の秘密鍵の危殆化時に関する手続きについて規定しない。当該手続きについては、証明書の発行・失効を開始する際に別途規定する。

5.7.4 災害時等の事業継続性

本認証局は、災害等からの復旧対策ならびに業務継続について、別途、業務継続計画を定める。業務継続計画は、本施設に保管されたデータ等を用い、本認証局の業務の全体または一部（失効処理）の復旧・再開の実施要領が定められる。

被災からの復旧時間については、被災状況の調査に基づき、段階的復旧目標が業務継続計画により定められる。

5.8 認証局の業務の終了

本認証局は、本認証局の業務を終了する場合、サイバートラストの Web サイトにおいて、その旨を事前に公開する。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成および導入

6.1.1 鍵ペアの生成

本認証局で使用する鍵ペアは、本 CPS「1.1 概要」に記載のとおり、JCSI 社により作成され、2014 年に JCSI 社がサービス提供を終了した後、サイバートラストが取得したものである。取得に際し、サイバートラストは、本認証局の鍵ペアの管理のため FIPS PUB 140-2 レベル 3 の規格を満たした秘密鍵暗号モジュール（以下、「HSM」という。）を用意し、JCSI 社が鍵ペアの管理を行っていた同一規格の HSM から、秘密分散の手法を用いて、サイバートラストの HSM への鍵ペアの移送を行っている。

本認証局の鍵ペアの移送は、本 CPS「8.2 監査人の要件」および「8.3 監査人と被監査者の関係」に定める監査人による立会い、あるいは、立会いのない場合は移送の記録および録画された移送鍵確認作業を監査人へ提示することで、本認証局の鍵ペアの移送が所定の手順に即し行われたことを担保する。

OCSP 用証明書に関わる鍵ペアは、認証局責任者の指示を受け、発行局管理者 の管理の下、複数の発行局システムアドミニストレータにより生成される。OCSP 用証明書に関わる鍵ペア生成 の際には、FIPS 140-2 レベル 3 の規格を満たした HSM が用いられる。

6.1.2 加入者秘密鍵の配送

本認証局は、本 CPS「1.1 概要」に記載のとおり、本 CPS 第 1.4 版では、下位認証局の申請に基づく証明書の発行・失効の手続きを行わない。従って、下位認証局による加入者証明書の発行・失効も行われないため、加入者秘密鍵の配送について規定しない。下位認証局および加入者の秘密鍵の配送については、証明書の発行・失効を開始する際に別途規定する。

6.1.3 認証局への加入者公開鍵の配送

本認証局は、本 CPS「1.1 概要」に記載のとおり、本 CPS 第 1.4 版では、下位認証局の申請に基づく証明書の発行・失効の手続きを行わない。従って、下位認証局による加入者証明書の発行・失効も行われないため、認証局への加入者公開鍵の配送について規定しない。認証局への加入者公開鍵の配送については、証明書の発行・失効を開始する際に別途規定する。

6.1.4 信頼当事者への認証局公開鍵の配送

本認証局は、信頼当事者に対する本認証局の公開鍵の配送を行わない。本認証局の公開鍵が含まれる本認証局の証明書は、本認証局のリポジトリにて公開する。

6.1.5 鍵長

本認証局の証明書に関わる鍵の署名方式および鍵長は次のとおりとする。

認証局名称	署名方式	鍵長
SecureSign RootCA11	SHA1 with RSA	2048 bit

OCSP 用証明書に関わる鍵の署名方式および鍵長は次のとおりとする。

OCSP 用証明書	署名方式	鍵長
SecureSign RootCA11 が発行する OCSP 用証明書	SHA2 with RSA	2048 bit

下位認証局の証明書に関わる鍵の署名方式および鍵長は次のとおりとする。

下位認証局証明書	署名方式	鍵長
SecureSign RootCA11 が発行する下位認証局証明書	SHA2 with RSA	2048 bit

加入者証明書に関わる鍵の署名方式および鍵長は次のとおりとする。

加入者証明書	署名方式	鍵長
下位認証局が発行する加入者証明書	SHA2 with RSA	2048 bit

6.1.6 公開鍵パラメータ生成および検査

本認証局は、公開指数の値が 3 以上の奇数であることを確認する。また、公開指数は、2^16+1 と 2^256-1 の間の範囲にあるものを用いる。モジュラスについては、次の特性を持つものとする：奇数であり、素数のべき乗ではなく、752 より小さい約数を持たない。

6.1.7 鍵用途

本認証局証明書の鍵用途（Key Usage）は、Certificate Signing、CRL Signing とする。

OCSP 用証明書の鍵用途（Key Usage）は、Digital Signature とする。

6.2 秘密鍵の保護および暗号モジュール技術の管理

本認証局は、以下に説明する通り、不正な証明書の発行を防ぐための物理的および論理的な保護手段を実装するものとする。

6.2.1 暗号モジュールの標準および管理

本認証局の鍵ペアを管理するための暗号モジュールは、FIPS PUB 140-2 レベル 3 の規格を満たした HSM とする。HSM は、発行局が管理する。

OCSP 用証明書に関わる鍵ペアは、FIPS 140-2 レベル 3 の規格を満たした HSM により管理する。OCSP は発行局が管理する。

6.2.2 秘密鍵の複数人管理

本認証局および OCSP で使用する秘密鍵の管理は、常時複数の発行局システムアドミニストレータが行う。

6.2.3 秘密鍵の預託

本認証局は、本認証局および OCSP で使用する秘密鍵の預託を行わない。

6.2.4 秘密鍵のバックアップ

本認証局の秘密鍵のバックアップは、発行局システムアドミニストレータが行う。HSM からバックアップされた秘密鍵は、暗号化された上で複数に分割され、各々が施錠可能な保管庫に安全に保管される。

OCSP で使用する秘密鍵については、暗号化された状態で、システムのバックアップとして 発行局システムアドミニストレータによりバックアップされ、保管される。

6.2.5 秘密鍵のアーカイブ

本認証局は、本認証局および OCSP で使用する秘密鍵のアーカイブを行わない。

6.2.6 秘密鍵の移送

本認証局は、下位認証局に代わり同下位認証局の秘密鍵を生成することはしない。

本認証局は、本認証局で使用する秘密鍵のコピーを安全な方法でバックアップサイトへ移送する。HSM の故障等により本認証局の秘密鍵の復元が必要となる場合、発行局システムアドミニストレータは、メインサイトまたはバックアップサイトに保管されたバックアップを用いて復元する。

OCSP 用証明書に関わる秘密鍵の復元が必要となる場合、発行局システムアドミニストレータは、メインサイトに保管されたシステムバックアップを用いて復元する。ただし、認証局責任者の承認の下、対応する OCSP 用証明書を失効し、新たに秘密鍵を生成する場合がある。

6.2.7 暗号モジュール内での秘密鍵保存

本認証局および OCSP の秘密鍵は、FIPS 140-2 レベル 3 の規格を満たした HSM 内で保存される。

6.2.8 秘密鍵の活性化

本認証局および OCSP で使用する秘密鍵は、発行局管理者の承認の下、別途規定された手順に基づき、複数の発行局システムアドミニストレータにより活性化される。また、活性化作業は記録される。

6.2.9 秘密鍵の非活性化

本認証局および OCSP で使用する秘密鍵は、発行局管理者の承認の下、別途規定された手順に基づき、複数の発行局システムアドミニストレータにより非活性化される。また、非活性化作業は記録される。

6.2.10 秘密鍵破壊の方法

本認証局および OCSP で使用する秘密鍵は、認証局責任者の指示を受け、発行局管理者の管理の下、別途規定された手順に基づき、複数の発行局システムアドミニストレータにより破壊される。同時に、本 CPS「6.2.4 秘密鍵のバックアップ」に規定されたバックアップされた本認証局の秘密鍵についても、同様の手順に基づき破壊される。また、破壊作業は記録される。

6.2.11 暗号モジュールの評価

本認証局は、本 CPS「0 暗号モジュールの標準と管理」に定める標準を満たした HSM を使用する。

6.3 鍵ペアのその他の管理

6.3.1 公開鍵の保存

公開鍵の保存は、それが含まれる証明書を保存することで行う。

6.3.2 証明書および鍵ペアの有効期間

本認証局の鍵ペアの有効期限は以下のとおりである。

鍵ペア	有効期限
本認証局の鍵ペア	2029 年 4 月 8 日

OCSP 証明書の有効間は以下のとおりである。

証明書	有効期間

OCSP 用証明書	25 ヶ月以内とする

下位認証局による加入者の証明書として以下の証明書の発行を行う場合、当該証明書の有効期間は以下のとおりとする。

証明書	有効期間
OV SSL 証明書	825 日以内とする

6.4 活性化データ

6.4.1 活性化データの作成および設定

本認証局で使用する活性化データは、容易に推測されないよう配慮の上作成され、設定される。

6.4.2 活性化データの保護および管理

本認証局内で使用される活性化データは、本 CPS「5.1.2 物理的アクセス」の規定に基づき入退室管理が施された室内において、施錠可能な保管庫に保管される。

6.5 コンピュータのセキュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件

本認証局のシステムは、セキュリティ対策として以下を実施する。

① 操作者の権限の認証
② 操作者の識別と認証
③ 重要なシステム操作に対する操作ログの取得
④ 適切なパスワード設定
⑤ バックアップ・リカバリ

6.5.2 コンピュータセキュリティの評価

本認証局は、本認証局が導入するハードウェア、ソフトウェアに対して、事前に導入評価を実施する。また、使用するシステムにおけるセキュリティ上の脆弱性に関する情報収集および評価を継続的に行い、評価結果に基づき必要な対応を行う。

6.6 ライフサイクルセキュリティ管理

6.6.1 システム開発管理

本認証局のシステムの構築および変更は、サイバートラスト内部で任命された開発責任者の管理の下、別途定められた規定に基づき行う。開発責任者が必要と判断する場合は、テスト環境において必要かつ十分な検証を行い、セキュリティ上問題がないことを確認する。

6.6.2 セキュリティ運用管理

本認証局のシステムは、十分なセキュリティを確保するために必要な設定が行われる。また、セキュリティ・レベルに則した入退室管理やアクセス権限管理等を実施するとともに、セキュリティ上の脆弱性についての情報収集および評価を継続的に行い、評価結果に基づき必要な対応を行う。

6.6.3 ライフサイクルセキュリティ管理

本認証局は、本認証局のシステムの開発、運用、変更、廃棄の各工程において責任者を定め、作業計画または手順を策定・評価し、必要に応じ試験を行う。また、各作業は記録される。

6.7 ネットワークセキュリティ管理

本認証局のシステムはネットワークに接続せず、オフラインにて運用するものとする。

本認証局の OCSP に関わるシステムとインターネット等の外部システムとは、ファイアウォール等を介し接続され、また、侵入防御システムによる監視が行われる。

6.8 タイムスタンプ

本 CPS「5.5.5 タイムスタンプ」に準じる。

7. 証明書、CRL および OCSP のプロファイル

7.1 証明書のプロファイル

7.1.1 バージョン番号

本認証局の証明書については、Appendix B に記載する。

7.1.2 証明書拡張領域

本認証局の証明書については、Appendix B に記載する。

7.1.3 アルゴリズムオブジェクト識別子

本認証局の証明書については、Appendix B に記載する。

7.1.4 名前の形式

本認証局の証明書については、Appendix B に記載する。

7.1.5 名称の制約

規定しない。

7.1.6 証明書ポリシーオブジェクト識別子

本 CPS「1.2 文書名と識別」に規定するとおりとする。

7.1.7 ポリシー制約拡張の使用

規定しない。

7.1.8 ポリシー修飾子の構文および意味

規定しない。

7.1.9 証明書ポリシー拡張についての処理方法

規定しない。

7.2 CRL のプロファイル

7.2.1 バージョン番号

本認証局の CRL については、Appendix B に定める。

7.2.2 CRL、CRL エントリ拡張

本認証局の CRL については、Appendix B に定める。

7.3 OSCP のプロファイル

7.3.1 バージョン番号

本認証局の OCSP 用証明書については、Appendix B に定める。

7.3.2 OCSP 拡張

本認証局の OCSP 用証明書については、Appendix B に定める。

8. 準拠性監査およびその他の評価

本認証局は、常に以下を満足するものとする。
(i) 事業および証明書に関わる全ての規定に従い証明書を発行し、PKI を運用すること
(ii) それらの要件に従うこと、および
(iii) 下記の監査要件を遵守すること

8.1 監査の頻度および要件

本認証局は、Trust Service Principles and Criteria for Certification Authorities および WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security の検証を年に一度、あるいは本 CPS「8.2 監査人の要件」で定める監査人が必要と判断した時期に往査する。

8.2 監査人の要件

Trust Service Principles and Criteria for Certification Authorities および WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security の検証は、資格を有する外部の監査人が実施する。

8.3 監査人と被監査者の関係

監査人は、原則として本認証局の業務から独立し、中立性を保つ者とする。

8.4 監査の範囲

監査の範囲は、Trust Service Principles and Criteria for Certification Authorities および WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security で定められる範囲とする。

8.5 指摘事項の対応

検証により発見された指摘事項は、CTJ PA、認証局責任者、発行局管理者および登録局管理者へ報告される。監査人、CTJ PA、認証局責任者、発行局管理者または登録局管理者により是正措置が必要と判断された場合、発行局管理者または登録局管理者の管理の下、是正措置を実施する。

8.6 監査結果の開示

Trust Service Principles and Criteria for Certification Authorities および WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security の検証結果は、各ガイドラインの定めに従い、公開される。

8.7 自己監査

下位認証局が加入者証明書を発行する期間中、CPS および Baseline Requirements への準拠を監視し、四半期毎に、以前の自己監査期間以後に発行された加入者証明書から、ランダムに選択された1枚以上または 3%以上のサンプルに対して自己監査を実行することにより、サービス品質を厳しくコントロールするものとする。

9. その他の業務上および法的な事項

9.1 料金

規定しない。

9.2 財務的責任

サイバートラストは、本 CPS に定める内容を遵守のうえ本認証局を運営するために、十分な財務的基盤を維持するものとする。また、賠償責任への対応に備え、適切な保険に加入する。

9.3 企業情報の機密性

9.3.1 機密情報の範囲

本認証局は、以下の情報を機密として取り扱う（以下、「機密情報」という。）。

① 本 CPS「9.4.2 個人情報として扱われる情報」に定める情報
② 第三者（信頼当事者を含む）より受けた問合せ情報
③ 本認証局のセキュリティに関わる情報
④ 加入者からの申請情報、但し本 CPS 第 1.4 版においては発生しない

9.3.2 機密情報の範囲外の情報

本認証局が保有する情報のうち、以下の情報は機密情報の範囲外とする。

① 本 CPS「2.2 公開する情報」において公開するものとして定める情報
② 本認証局の過失によらず公知となった情報
③ 本認証局以外のものから機密保持の制限なしに公知となった情報
④ 当事者から事前に開示または第三者への提供に関する合意を得た情報
⑤ 加入者の証明書、但し本 CPS 第 1.4 版においては発生しない

9.3.3 機密情報の保護責任

本認証局は、機密情報の漏洩を防止する対策を実施する。また、本認証局の運営の用に供する以外には使用しない。ただし、機密情報に関して、裁判上、行政上その他の法的手続きの過程において機密情報の開示要求があった場合、買収、合併等に関連して財務アドバイザー、潜在的買収・合併当事者などサイバートラストとの間で守秘義務契約を締結した者および／または弁護士、公認会計士、税理士等の法により守秘義務を負う者に開示する場合、または当事者から事前の承諾を得た場合、サイバートラストは、当該機密情報を開示要求者に対して開示することができるものとする。この場合、開示を受ける当該開示要求者は当該情報をいかなる方法によっても第三者に開示し、または漏洩させてはならない。

なお、個人情報の保護の取扱いは、本 CPS「9.4 個人情報の保護」に定める。

9.4 個人情報の保護

9.4.1 プライバシー・ポリシー

本認証局が保有する個人情報の取り扱いは、サイバートラストの Web サイト（https://www.cybertrust.co.jp/corporate/privacy-policy.html）で公開するプライバシー・ポリシーに定める。

9.4.2 個人情報として扱われる情報

本認証局は、問合せ等に含まれる特定の個人を識別することができる情報を個人情報として扱う。

9.4.3 個人情報とみなされない情報

本認証局は、本 CPS「9.4.2 個人情報として扱われる情報」に定める情報以外は、個人情報とみなさない。

9.4.4 個人情報の保護責任

本認証局が保有する個人情報の保護責任は、本 CPS「9.4.1 プライバシー・ポリシー」に定めるとおりとする。

9.4.5 個人情報の使用に関する個人への通知および同意

本認証局は、取得した個人情報について、認証業務を実施する目的以外で使用しない。ただし、本 CPS「9.4.6 司法手続または行政手続に基づく公開」に定める場合を除くものとする。

9.4.6 司法手続または行政手続に基づく公開

本認証局で取扱う個人情報に関して、裁判上、行政上その他の法的手続きの過程において情報の開示要求があった場合、サイバートラストは、当該個人情報を開示することができるものとする。

9.4.7 他の情報公開の場合

本認証局は、業務の一部を外部に委託する場合、機密情報を委託先に対して開示することがある。この場合、当該委託に関する契約において、当該委託先に対して機密情報の守秘義務を課す規定を置くものとする。

9.5 知的財産権

特段の合意がなされない限り、以下の情報に関するすべての知的財産権は、サイバートラストまたは本認証局のサービスに関するサイバートラストの仕入先またはライセンサーに帰属するものとする。

① 本 CPS

② 本認証局の公開鍵および秘密鍵

③ 開局日以後、本認証局が発行した証明書と失効情報

9.6 表明保証

以下に発行局、登録局および信頼当事者の表明保証を規定する。なお、本 CPS「9.6 表明保証」で明示的に規定された発行局、登録局および信頼当事者の表明保証を除き、各当事者はいかなる明示的または黙示的な表明保証をも行わないことを相互に確認する。

加入者の表明保証については、別途、下位認証局が加入者の申請に基づく加入者証明書の発行・失効を開始する際に規定する。

9.6.1 発行局の表明保証

サイバートラストは、発行局における業務の遂行にあたり、以下の義務を負うことを表明し保証する。

① 認証局秘密鍵の安全な管理を行うこと

② 登録局からの申請に基づく正確な証明書の発行および失効を行うこと

③ CRL および OCSP によって失効情報を提供すること

④ 本認証局に係るシステムの監視および運用を行うこと

⑤ リポジトリの維持・管理を行うこと

なお、本認証局は本 CPS 第 1.4 版では、下位認証局証明書および下位認証局を通じての加入者証明書の発行・失効の手続きを行わない。

9.6.2 登録局の表明保証

サイバートラストは、登録局における業務の遂行にあたり、以下の義務を負うことを表明し保証する。

① 問合せ受付（本 CPS「1.5.2 連絡窓口」）を行うこと

なお、本認証局は本 CPS 第 1.4 版では、下位認証局証明書および下位認証局を通じての加入者証明書の発行・失効の手続きを行わない。従って、登録局は、下位認証局ならびに加入者の審査、発行局への証明書発行・失効申請処理を行わない。

9.6.3 加入者の表明保証

本 CPS 第 1.4 版では規定しない。

なお、上記に関わらず、証明書の発行・失効を開始する際には、加入者は、以下の義務を負うことを表明し保証する。

① 加入者証明書の発行申請時における真正かつ正確な情報提供を行うこと
② 加入者の証明書用途の遵守すること
③ 公序良俗に反する Web サイトおよび電子メールで加入者証明書を利用しないこと
④ 加入者証明書に含まれる組織単位名（OU）に Baseline Requirements 7.1.4.2.2 章が OU として禁止する値（metadata を含む）を含めた加入者証明書を申請、ならびに利用しないこと
⑤ 加入者証明書に含まれる情報の正確性が確認できるまで、加入者証明書をサーバにインストールし、これを使用しないこと
⑥ 秘密鍵およびパスワードの機密性ならびに完全性を確保するための厳重な管理を行うこと
⑦ 加入者証明書に含まれる FQDN によりアクセス可能なサーバにのみインストールし、かつ、加入契約書に従い、加入者が認める事業においてのみ証明書を使用すること
⑧ 本 CPS「4.9.1.1 加入者証明書の失効理由」に定める事由が生じた場合は、速やかな失効の申請を行うこと
⑨ 秘密鍵の危殆化またはその可能性があると判断したときは速やかに失効申請を行うこと
⑩ 有効期間が満了した加入者証明書および失効された加入者証明書を使用しないこと
⑪ 関連法規制を遵守すること

9.6.4 信頼当事者の表明保証

信頼当事者は、以下の義務を負うことを表明し保証する。

① 本認証局の証明書の有効期間と記載項目の確認を行うこと
② 本認証局の証明書に行われた電子署名の検証と発行者の確認を行うこと
③ CRL または OCSP により、証明書の失効の有無について確認を行うこと
④ 本項に規定された義務の不履行により発生した事態に対し、法的責任を負うこと

9.6.5 他の関係者の表明保証

規定しない。

9.7 不保証

本認証局は、本 CPS「9.6.1 発行局の表明保証」および「9.6.2 登録局の表明保証」に定める保証に関連して発生する直接損害以外の損害については、本 CPS に基づく債務不履行に関していかなる責任も負わない。

本認証局は、信頼当事者が自らの判断で本認証局の証明書を信頼した結果については、いかなる責任も負わない。

9.8 責任の制限

サイバートラストは、本 CPS「9.6.1 発行局の表明保証」および「9.6.2 登録局の表明保証」の内容に関し、以下の場合に一切の責任を負わないものとする。

① 本認証局が本 CPS および法規制を遵守したにも関わらず発生するいかなる損害

② サイバートラストに起因しない、不法行為、不正使用または過失等により発生するいかなる損害

③ 信頼当事者が、本 CPS「9.6 表明保証」の規定に基づきそれぞれが負う義務の履行を怠ったために生じた損害

④ 本認証局が発行した証明書に関わる鍵ペアがサイバートラスト以外の第三者の行為により漏洩または危殆化し生じた損害

⑤ 証明書が加入者、信頼当事者または第三者の著作権、営業秘密またはその他の知的財産権を侵害したことによって生じる損害

⑥ 暗号アルゴリズム解読技術の向上等、技術の進歩に伴う暗号強度の弱体化、その他の暗号アルゴリズムの脆弱性等に起因する損害

サイバートラストが、信頼当事者またはその他の第三者に対し、本認証局の証明書の利用に関連して生ずる一切の損害について負担する賠償額の総額は、いかなる場合においても 10,000,000 円を超えないものとする。

この上限額は、各々の証明書に関してなされた電子署名数、取引数または損害の数に関わらず、証明書1通毎を基準に適用されるものとし、時間的に早い請求から割り当てられるものとする。

また、本 CPS「9.14 準拠法」に定める準拠法により認められる範囲において、本 CPS に対する債務不履行・違反により生じる損害のうち、データ消失、得べかりし利益を含む間接損害、派生的損害、懲罰的損害に対し、本認証局は責任を負わない。

9.9 補償

9.9.1 認証局による補償

本認証局証明書を信頼当事者が受領または利用した時点で、当該信頼当事者には、自らの為した以下に掲げるいずれかの行為に起因して生じた第三者からのサイバートラストに対する請求、訴訟の提起その他の法的措置によってサイバートラストが被った損害を賠償し、かつサイバートラストに損害を生ぜしめないようにする責任が生じるものとする。

① 本認証局証明書の不正使用、改ざん、利用時の不実の表明

② 本 CPS への違反

また、本認証局は、信頼当事者の代理人、受託者またはその他代表者ではない。

9.9.2 加入者による補償

規定しない。

9.9.3 信頼当事者者による補償

規定しない。

9.10 文書の有効期間と終了

9.10.1 文書の有効期間

本 CPS は、CTJ PA が承認することにより有効となる。また、本 CPS「9.10.2 終了」に定める時点の前に本 CPS が無効となることはない。

9.10.2 終了

本 CPS は、本 CPS「9.10.3 終了の影響と存続条項」に定める規定を除き、本認証局が業務を終了した時点で無効となる。

9.10.3 終了の影響と存続条項

本 CPS 9.3、9.4、9.5、9.6、9.7、9.8、9.9、9.10.2、9.10.3、9.13、9.14、9.15、9.16 の規定については本 CPS の終了後も、存続するものとする。

9.11 関係者間の個別通知と連絡

規定しない。

9.12 改訂

9.12.1 改訂手続き

本認証局は、各種要件に対応するため、CTJ PA の指示に基づき、少なくとも年1回の改訂を行い、併せてバージョン番号の更新、及び変更履歴を日付入りで追加する。必要に応じ、認証局員の評価、あるいは弁護士等外部の専門家または有識者の評価を得た後、CTJ PA が改訂の承認を行う。

9.12.2 通知方法と期間

本認証局は、本 CPS の改訂を CTJ PA が承認した後、改訂後および改訂前の CPS を一定期間 Web サイトに公開し、信頼当事者がその変更内容について確認できる措置を講ずる。サイバートラストから当該改訂の撤回の通知が公表されない限り、当該改訂は CTJ PA が定める時点をもって発効するものとする。

9.12.3 オブジェクト識別子の変更

規定しない。

9.13 紛争解決手続き

本 CPS または本認証局が発行する証明書に関連して生じたすべての訴訟については、東京地方裁判所を第一審の専属的合意管轄裁判所とする。また、本 CPS に定めのない事項または本 CPS に疑義が生じた場合は、当事者が誠意をもって協議するものとする。

9.14 準拠法

本 CPS の解釈およびに本 CPS に基づく認証業務にかかわる紛争については、日本国の法律が適用される。

9.15 適用法の遵守

規定しない。

9.16 雑則

9.16.1 完全合意条項

本 CPS における合意事項は、特段の定めをしている場合を除き、本 CPS が改訂または終了されない限り、他のすべての合意事項より優先される。

9.16.2 権利譲渡条項

サイバートラストが本サービスを第三者に譲渡する場合、本 CPS および本 CPS に定める責務およびその他の義務の譲渡を可能とする。

9.16.3 分離条項

本 CPS の一部の条項が、何らかの事由により無効となった場合においても、その他の条項は有効であるものとする。

9.16.4 強制執行条項

規定しない。

9.16.5 不可抗力条項

天災地変、裁判所の命令、労働争議、その他本認証局の責に帰さない事由により、本 CPS 上の義務の履行が一部または全部を遅延した場合には、サイバートラストは当該遅延期間について本 CPS 上の義務の履行を免れ、本認証局証明書を信頼し、もしくは利用した第三者に対し、何らの責任をも負担しない

Appendix A:用語の定義

用語	定義
アーカイブ	本書でのアーカイブとは、使用期限が過ぎたものを所定の期間保管することをいう。
暗号モジュール	秘密鍵の生成、保管、使用等において、セキュリティを確保する目的で使用されるソフトウェア、ハードウェアまたはそれらを組み合わせた装置である。
一時停止	証明書の有効期間中、証明書の有効性を一時的に無効とする措置である。
下位認証局	Subordinate CA。別名、中間認証局。ルート認証局から認証局証明書の発行を受け、End Entity に証明書を発行する認証局を指す。
鍵ペア	公開鍵暗号方式における公開鍵および秘密鍵である。2 つの鍵は、一方の鍵から他方の鍵を導き出せない性質を持つ。
鍵長	鍵の長さをビット数で表したもので、暗号強度を決定する一要素である。
活性化	システムや装置等を使用可能な状態にすることである。活性化には活性化データを必要とし、具体的には PIN やパスフレーズ等が含まれる。
危殆化	秘密鍵および秘密鍵に付帯する情報の機密性または完全性が失われる状態である。
公開鍵	公開鍵暗号方式における鍵ペアの 1 つで、通信相手等の他人に知らせて使用される鍵である。
失効	証明書が有効期間中であっても、証明書を無効とする措置である。
証明書失効リスト	英語では Certificate Revocation List であり、本 CPS では CRL という。CRL は、失効された証明書のリストである。本認証局は、加入者および信頼当事者が証明書の有効性を確認するために、CRL を公開する。
認証業務	証明書のライフサイクル管理を行う上での一連の業務をいう。発行・失効の申請受付業務、審査業務、発行・失効・棄却業務、問合対応業務、請求業務、本認証局のシステムの維持管理業務を含むが、これらに限定されない。
バックアップサイト	災害時等における事業継続性を担保するために、証明書の発行、失効に必要な本認証局の重要な資産をメインサイトとは別に保管する施設である。
秘密鍵	公開鍵暗号方式における鍵ペアの 1 つで、他人には知られないように秘密にしておく鍵である。
ポリシー管理局(CTJ PA)	認証局から独立して、認証局を管理監督し、ポリシーを評価/承認する、サイバートラストが定める組織である。

メインサイト	証明書の発行、失効に必要な本認証局の資産が設置される施設である。
預託	本 CPS での預託とは、秘密鍵または公開鍵を第三者に登録保管することである。
リポジトリ	本 CPS や CRL 等、公開情報を掲載する Web サイトやシステムである。
Baseline Requirements	CA/Browser Forum により策定された、パブリックに信頼される証明書を発行するための要件である。
Distinguished Name	ITU-T が策定した X.500 勧告において定められた識別名である。コモンネーム、組織名、組織単位名、国名等の属性情報で構成される。
FIPS PUB 140-2 レベル 3	FIPS PUB 140（Federal Information Processing Standards Publication 140)は、暗号モジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格であり、最新版の規格は 140-2 である。同規格では、セキュリティ要件によりレベルを 1（最低）～4（最高）に分類している。
IETF PKIX ワーキンググループ	Internet Engineering Task Force（IETF）は、インターネットで利用される技術を標準化する組織であり、同組織の PKIX ワーキンググループが RFC3647 を定めた。
ITU-T	国際電気通信連合の電気通信標準化部門である。
OCSP	Online Certificate Status Protocol の略であり、証明書の失効情報を提供するための通信プロトコルである。
RSA	Rivest、Shamir、Adelman の 3 人が開発した公開鍵暗号方式である。
SHA1/SHA2	電子署名等に使用されるハッシュ関数である。ハッシュ関数は、データを数学的な操作により一定の長さに縮小させるものであり、異なる 2 つの入力値から同じ出力値を算出することを困難とする特性を持つ。また、出力値から入力値を逆算することは不可能である。
SSL/TLS	Netscape Communications が開発したインターネット上で情報を暗号化して送受信するプロトコルである。TLS は SSL 3.0 へ改良を加えたものである。
Trust Service Principles and Criteria for Certification Authorities	米国公認会計士協会およびカナダ勅許会計士協会により制定された、認証局の運営に関する基準である。旧名は WebTrust Program for Certification Authorities。
WEBTRUST FOR CERTIFICATION AUTHORITIES – SSL BASELINE REQUIREMENTS AUDIT CRITERIA	米国公認会計士協会およびカナダ勅許会計士協会により制定された、公的に信頼された証明書の発行および管理のための要件である。
X.500	ITU-T により規格化されたネットワーク上での分散ディレクトリサービスの国際標準である。
X.509	ITU-T により規格化された電子証明書の国際標準である。

Appendix B:証明書等のプロファイル

SecureSign RootCA11

本認証局証明書（有効期間：2009 年 4 月 8 日～2029 年 4 月 8 日）

（標準領域）

Version		**値**
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
Serialnumber		**値**
CertificateSerialNumber	電子証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号 1 (0x01)
Signature		**値**
AlgorithmIdentifier Algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 暗号アルゴリズムのオブジェクト ID(SHA-1) 型：OID 値：1 2 840 113549 1 1 5 暗号アルゴリズムの引数 型：NULL 値：	 1.2.840.113549.1.1.5 NULL
Issuer		**値**
CountryName type value OrganizationName type value CommonName Type value	電子証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP 電子証明書発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10 組織名の値 型：PrintableString 値：Japan Certification Services, Inc. 電子証明書発行者の固有名称 固有名称のオブジェクト ID 型：OID 値：2 5 4 3 固有名称の値 型：PrintableString 値：SecureSign RootCA11	 2.5.4.6 JP 2.5.4.10 Japan Certification Services, Inc. 2.5.4.3 SecureSign RootCA11
Validity		**値**
Validity notBefore notAfter 	電子証明書の有効期間 開始日時 型：UTCTime 値：090408045647Z 終了日時 型：UTCTime 値：290408045647Z	 ＊有効開始日時 2009 年 4月 8日 04:56:47(GMT) ＊有効終了日時 2029年 4月 8日 04:56:47(GMT)
Subject		**値**
CountryName type	電子証明書発行者の国名 国名のオブジェクト ID	

	型：OID	
	値：2 5 4 6	2.5.4.6
value	国名の値	
	型：PrintableString	
	値：JP	JP
OrganizationName	電子証明書発行者の組織名	
type	組織名のオブジェクト ID	
	型：OID	
	値：2 5 4 10	2.5.4.10
value	組織名の値	
	型：PrintableString	
	値：Japan Certification Services, Inc.	Japan Certification Services, Inc.
CommonName	電子証明書発行者の固有名称	
type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
value	固有名称の値	
	型：PrintableString	
	値：SecureSign RootCA11	SecureSign RootCA11
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子証明書所有者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子 （公開鍵暗号とハッシュ関数）	
algorithm	暗号アルゴリズムのオブジェクト ID (RSA PUBLIC KEY)	
	型：OID	
	値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	暗号アルゴリズムの引数	
	型：NULL	NULL
	値：	
subjectPublicKey	公開鍵値	
	型：BIT STRING	
	値：公開鍵値	2048Bit 長の公開鍵

（拡張領域）

subjectKeyIdentifier (extnId :== 2 5 29 14，critical :== FALSE）		**値**
SubjectKeyIdentifier	電子証明書所有者の公開鍵に関する情報	
keyIdentifier	公開鍵の識別子 型：OctetString 値：所有者の subjectPublicKey の Hash 値	5b f8 4d 4f b2 a5 86 d4 3a d2 f1 63 9a a0 be 09 f6 57 b7 de
keyUsage （extnId :== 2 5 29 15，critical :== TRUE）		**値**
KeyUsage	鍵の使用目的 型：BitString 値：000001100 (keyCertSign,cRLSign)	000001100
basicConstraints (extnId :== 2 5 29 19，critical :== TRUE）		**値**
BasicConstraints	基本的制限	
cA	ＣＡかどうかを示すフラグ 型：Boolean 値：True（CA である）	TRUE

CRL

（標準領域）

Version		**値**
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：1	1 (Ver.2)
Signature		**値**
AlgorithmIdentifier Algorithm	CRL への署名に使用された暗号アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 暗号アルゴリズムのオブジェクト ID (SHA-1) 型：OID 値：1 2 840 113549 1 1 5	1.2.840.113549.1.1.5
Parameters	暗号アルゴリズムの引数 型：NULL 値：	NULL
Issuer		**値**
CountryName Type	電子証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6	2.5.4.6
Value	国名の値 型：PrintableString 値：JP	JP
OrganizationName Type	電子証明書発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10	2.5.4.10
Value	組織名の値 型：PrintableString 値：Japan Certification Services, Inc.	Japan Certification Services, Inc.
CommonName Type	電子証明書発行者の固有名称 固有名称のオブジェクト ID 型：OID 値：2 5 4 3	2.5.4.3
Value	固有名称の値 型：PrintableString 値：SecureSign RootCA11	SecureSign RootCA11
ThisUpdate		**値**
ThisUpdate	CRL の発行日時 型：UTCTime 値：yymmddhhmmssZ	＊有効開始日時
NextUpdate		**値**
NextUpdate	次回 CRL の更新予定日時 型：UTCTime 値：yymmddhhmmssZ	* 12 ヶ月以内

（拡張領域）

authorityKeyIdentifier (extnId :== 2 5 29 35, critical :== FALSE)		**値**
AuthorityKeyIdentifier keyIdentifier	CRL 発行者の公開鍵に関する情報 公開鍵の識別子 型：OctetString 値：発行者の subjectPublicKey の Hash 値	5b f8 4d 4f b2 a5 86 d4 3a d2 f1 63 9a a0 be 09 f6 57 b7 de
cRLNumber (extnId :== 2 5 29 20, critical :== FALSE)		**値**
cRLNumber	失効リストのシーケンス番号 型：INTEGER 値：ユニークな整数	＊CRL の番号

issuingDistributionPoint (extnId :== 2 5 29 28, critical :== FALSE)		値
issuingDistributionPoint	失効リスト発行側の配布ポイント 型：OID 値：2.5.29.28	2.5.29.28
onlyContainsUserCerts	失効リストが利用者に関するもののみであることを示すフラグ 型：BOOLEAN 値：FALSE	FALSE
onlyContainsCACerts	失効リストが本認証局に関するもののみであることを示すフラグ 型：BOOLEAN 値：TRUE	TRUE
IndirectCRL	失効リストが間接 CRL であるかを示すフラグ 型：BOOLEAN 値：FALSE	FALSE

（エントリ領域）

RevokedCertificates		値
CertificateSerialNumber	証明書シリアル番号 型：INTEGER 値：ユニークな整数	＊失効した証明書のシリアル番号
revocationDate	失効処理日時 型：UTCTime 値：yymmddhhmmssZ	＊失効処理日時

（エントリ拡張領域）

invalidityDate (extnId :== 2 5 29 24, critical :== FALSE)		値
invalidityDate	無効化日時 型：GeneralizedTime 値：yyyymmddhhmmssZ	＊該当証明書の失効処理日時
cRLReason (extnId :== 2 5 29 21, critical :== FALSE)		値
cRLReason	失効理由コード 型：Enumerated 値：失効理由コード	＊失効 理由コードの値

OCSP 用証明書

（標準領域）

Version		**値**
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
Serialnumber		**値**
CertificateSerialNumber	電子証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号 41 (0x29)
Signature		**値**
AlgorithmIdentifier Algorithm parameters	電子証明書への署名に使用された暗号アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 暗号アルゴリズムのオブジェクト ID (SHA-2) 型：OID 値：1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型：NULL 値：	 sha256WithRSAEncryption NULL
Issuer		**値**
CountryName type value OrganizationName type value CommonName Type value	電子証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP 電子証明書発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10 組織名の値 型：PrintableString 値：Japan Certification Services, Inc. 電子証明書発行者の固有名称 固有名称のオブジェクト ID 型：OID 値：2 5 4 3 固有名称の値 型：PrintableString 値：SecureSign RootCA11	 2.5.4.6 JP 2.5.4.10 Japan Certification Services, Inc. 2.5.4.3 SecureSign RootCA11
Validity		**値**
Validity notBefore notAfter 	電子証明書の有効期間 開始日時 型：UTCTime 値：160306064915Z 終了日時 型：UTCTime 値：190331145959Z	 ＊有効開始日時 2017 年 3月 6日 06:49:15(GMT) ＊有効終了日時 2019年 3月 31日 14:59:59(GMT)
Subject		**値**
CountryName type value OrganizationName type 	電子証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP 電子証明書発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10	 2.5.4.6 JP 2.5.4.10

value	組織名の値 型：PrintableString 値：Japan Certification Services, Inc.	Japan Certification Services, Inc.
CommonName	電子証明書発行者の固有名称	
type	固有名称のオブジェクト ID 型：OID 値：2 5 4 3	2.5.4.3
value	固有名称の値 型：PrintableString 値： SecureSign RootCA11 OCSP Responder	SecureSign RootCA11 OCSP Responder
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子証明書所有者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子 （公開鍵暗号とハッシュ関数）	
algorithm	暗号アルゴリズムのオブジェクト ID (RSA PUBLIC KEY) 型：OID 値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	暗号アルゴリズムの引数 型：NULL 値：	NULL
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値	2048Bit 長の公開鍵

（拡張領域）

basicConstraints (extnId :== 2 5 29 19，critical :== FALSE）		**値**
BasicConstraints cA	基本的制限 ＣＡかどうかを示すフラグ 型：Boolean 値：True（CA である）	FALSE
authorityKeyIdentifier (extnId :== 2 5 29 35，critical :== FALSE）		**値**
authorityKeyIdentifier keyIdentifier	証明書発行者の公開鍵に関する情報 公開鍵の識別子 型：OctetString 値：発行者の PublicKey の Hash 値	5b f8 4d 4f b2 a5 86 d4 3a d2 f1 63 9a a0 be 09 f6 57 b7 de
subjectKeyIdentifier (extnId :== 2 5 29 14，critical :== FALSE）		**値**
SubjectKeyIdentifier keyIdentifier	電子証明書所有者の公開鍵に関する情報 公開鍵の識別子 型：OctetString 値：所有者の PublicKey の Hash 値	B9:49:42:CC:DD:D7:42:9F:7D:A1: 8F:E3:B6:08:F5:C9:BA:26:55:96
keyUsage （extnId :== 2 5 29 15，critical :== FALSE）		**値**
KeyUsage	鍵の使用目的 型：BitString 値：100000000 (digitalSignatur)	100000000
extKeyUsage （entnID :== 2 5 29 31，critical :== FALSE）		**値**
KeyPurposeID OCSPSigning	鍵の使用目的(拡張) 使用目的 ID 型：OID 値：オンラインレスポンダ署名利用	1.3.6.1.5.5.7.3.9
OCSP No Check (entnID :== 1.3.6.1.5.5.7.48.1.5 ，critical :== FALSE）		**値**
OCSP No Check OCSP No Check	署名者証明書の失効確認 失効確認を実施しない	NULL