JCSI ルート認証局

Certification Practice Statement

(認証局運用規程)

Version 2.6

サイバートラスト株式会社

2021 年 6 月 30 日

■JCSI ルート認証局 Certification Practice Statement（認証局運用規程) の著作権と配布条件

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
1.5	2018 年 6 月 1 日	・ 「3.2.2.5 IP アドレスの認証」からその他の確認方法④を削除
1.6	2018 年 9 月 5 日	・ 「JCSI 証明書発行サービス」対応のための追加修正 ・ 連絡窓口住所に関し本社移転を反映 ・ Baseline Requirements 対応のため追加修正
2.0	2018 年 12 月 25 日	・ 「JCSI 証明書発行サービス」対応 ・ パブリックかつ有効な中間認証局証明書プロファイル例反映 ・ Baseline Requirements 対応のため追加修正 ・ リポジトリ URL を cyberstrust.ne.jp から cybertrust.co.jp に変更 ・ 誤記修正
2.1	2019 年 5 月 10 日	・ Baseline Requirements v1.6.5 までの対応のため追加修正 ・ 誤記修正
2.2	2020 年 1 月 31 日	・ Mozilla Root Store Policy v2.7 に対応のための追加修正 ・ Baseline Requirements v1.6.7 までの対応のため追加修正 ・ 誤記修正
2.3	2020 年 5 月 26 日	・ Baseline Requirements v1.6.8 への対応のための以下追加修正 ・ 「3.2.2.4ドメイン名の認証またはコントロールの検証」に.onion を含む証明書を発行しないことを追加 ・ Baseline Requirements v1.6.8 の改訂に伴い、「3.2.2.4.6 合意に基づく Web サイトの変更」の検証方法の利用を廃止し、「3.2.2.4.18 合意に基づく Web サイトの変更」で新たに規定 ・ 「6.3.2 証明書および鍵ペアの有効期間」加入者の証明書の有効期間を修正 ・ 誤記修正
2.4	2021 年 3 月 10 日	・ CAA レコードの RFC のバージョン情報を更新 ・ 「1.1 概要」準拠する規程を明確化 ・ 「3.2.2.4 ドメインの承認または管理権限の審査」内に記述を追加 ・ 「4.9.1.1 加入者証明書の失効理由」の記述を修正 ・ 「5.4.1 記録されるイベントの種類」を明確化のため修正 ・ 「5.4.3 監査ログの保管期間」の記述を修正 ・ 「6.1.1 鍵ペアの生成」に加入者の鍵ペアの生成を修正 ・ 「6.1.5 鍵アルゴリズムと鍵長」に記述を追加 ・ 「7.1.2 証明書拡張領域」」内の記述を修正 ・ 「7.1.3 アルゴリズムオブジェクト識別子」に記述を追記 ・ 「7.1.4 名前の形式」に記述を追記 ・ 「7.2 CRL のプロファイル」に記述を追加 ・ 「7.3 OCSP のプロファイル」に記述を追記 ・ 「9.6.3 加入者の表明保証」の記述を修正 ・ Appendix A に用語の定義を追加 ・ 誤記修正
2.5	2021 年 4 月 30 日	・ 「3.2.2.4 ドメインの承認または管理権限の審査」に審査結果の再利用期間を追加 ・ 「4.9.1.1.2 本認証局による失効事由」に失効事由を追加

		・「4.9.12 鍵の危殆化に関する特別要件」に秘密鍵の危殆化についての報告方法を追加 ・「5.4.3 監査ログの保管期間」の記述を修正 ・「7.1.2 証明書拡張領域」の記述を修正 ・その他、軽微な修正
2.6	2021 年 6 月 30 日	・「3.2.2.4.18 合意に基づく Web サイトの変更 v2」のリダイレクト時に使用可能な HTTP ステータスコードを修正 ・「4.9.12 鍵の危殆化に関する特別要件」の秘密鍵の危殆化についての報告方法を修正 ・「6.1.1 鍵ペアの生成」に加入者の鍵ペアの生成を追記 ・Appendix A に用語の定義を追加 ・その他、軽微な修正

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、「ルート認証局」という）を運営する。

ルート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に信頼されている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ルート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、ルート認証局の鍵ペアおよびルート認証局証明書は、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 年に当該ルート認証局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（当該ルート認証局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、サイバートラストは、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。

ルート認証局は、JCSI 中間認証局（以下、「中間認証局」といい、中間認証局を運営する主体を「中間認証局運営者」という。）の証明書（以下、「中間認証局証明書」という。）を発行する。中間認証局は、加入者に JCSI SSL/TLS 証明書を発行する。ここで、JCSI SSL/TLS 証明書（以下、「加入者の証明書」という。）は、SSL/TLS 通信に際してのサーバ・ネットワーク機器の認証に用いられる SSL/TLS サーバ証明書である。中間認証局は用語の定義にある通り、「JCSI 証明書発行サービス」（以下、「本サービス」という。）により中間認証局運営者に提供されるが、本サービスの特性上、中間認証局運営者は加入者と同一組織となる。

ルート認証局は、中間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 用証明書をルート認証局の認証局責任者の承認の下、発行する。また、中間認証局は加入者の証明書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 用証明書を本サービスにおいて中間認証局の認証局責任者の承認の下、発行する。

ルート認証局および中間認証局（以下、特段の規定がない限り、総称して「認証局」という。）は、以下の規程および法令等に準拠する。

① CA/Browser Forum が定める Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates（以下、「BR」という。）

② CA/Browser Forum が定める Network and Certificate System Security Requirements

③ ルート認証局の証明書が登録されたブラウザの提供元が認証局にも課す要件

- Microsoft Trusted Root Store (Program Requirements)
- Mozilla Root Store Policy
- Apple Root Store Program
- Chromium Root Store Policy

④ 本 CPS

⑤ 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

認証局は、BR に準拠する。本 CPS と BR との間に齟齬がある場合には BR が 優先される。

本 CPS は、開局日以後のルート認証局の運営とそれに係る要件、中間認証局の運営とそれに係る要件、および中間認証局が加入者の証明書を発行するための要件を規定する。要件には、認証局の義務、加入者の義務、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、IETF PKIX ワーキンググループが定める RFC3647「Certificate Policy and Certification Practices Framework」が採用される。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。本 CPS の各規定において、認証局に適用されない事項については、「適用しない」と記載する。

なお、中間認証局は、加入者の証明書毎のポリシー（以下、「CP」という。）を個別に定めず、本 CPS が各 CP を包含するものとする。すなわち、本 CPS が、ルート認証局およびルート認証局配下の全ての認証局に適用される。

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」に定めるルート認証局および中間認証局をいう。認証局は、発行局および登録局から構成される。認証局は本 CPS「5.2.1 信頼される役割」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

ルート認証局の登録局はサイバートラストが運営し、本サービスの申込を受け付け、本 CPS に基づき申込内容の審査を行う。同登録局は審査結果に基づき、ルート認証局の発行局に対し、中間認証局証明書の発行もしくは失効の処理の指示、または申込の棄却をする。サイバートラストは、同登録局を第三者に委託しない。

中間認証局の登録局は加入者と同一の組織が運営し、加入者からの証明書の申込を受け付け、本 CPS に基づき申込内容の審査を行う。同登録局は審査結果に基づき、中間認証局の発行局に対し、加入者の証明書の発行もしくは失効の処理の指示、または申込の棄却をする。サイバートラストは、中間認証局運営者に対し、同登録局の第三者への委託を認めない。

1.3.3 発行局

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

中間認証局の発行局は本サービスにおいてサイバートラストによって提供され、中間認証局の登録局の指示に基づき加入者の証明書の発行または失効を行う。また、本 CPS に基づき、中間認証局の秘密鍵を管理する。

1.3.4 加入者

加入者は、中間認証局へ証明書の申請を行い、本 CPS および加入契約書に基づき加入者の証明書を利用する組織である。

また、加入者の証明書の申請に責任を有する者を申請責任者という。加入者は、申請責任者を加入者組織の内部の者から選任しなければならない。

加入者において、中間認証局に対して証明書に関する申請を行うことができる者は、申請責任者または申請責任者より当該申請についての権限を付与された手続き担当者に限られる。手続き担当者については、加入者組織の内部の者から選任することができる。

1.3.5 信頼当事者

信頼当事者は、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、自らの判断で認証局および加入者の証明書を信頼する組織または個人である。

1.3.6 その他の関係者

適用しない。

1.4 証明書の用途

1.4.1 証明書の種類

1.4.1.1 ルート認証局証明書

本 CPS の Appendix B に示す、ルート認証局の証明書である。

1.4.1.2 中間認証局証明書

本サービスによりルート認証局の下位に発行される中間認証局の証明書である。

ルート認証局の登録局は、中間認証局証明書の発行にあたり、本 CPS に基づき、以下の事項について審査する。

① 加入者の法的または物理的な実在性と申込まれた DN 値が適正であること

② 中間認証局証明書に含まれる名前制約拡張子の中の DNS Name に指定されるドメイン名を本サービス申込組織である加入者が使用する権利があること

③ 申請責任者の在職

④ 加入契約書への同意の有無

⑤ 手続き担当者による申請行為に対する申請責任者による承認

⑥ ハイリスク・ステータス等※

※ ハイリスク・ステータス等として、以下を調査する。

- 過去のフィッシング事例
- フィッシングおよびその他詐欺行為等の疑義により、ルート認証局が過去に棄却した申請の記録または失効した中間認証局証明書の記録（存在する場合）

上記調査により、疑義が生じた場合、ルート認証局は、必要に応じて適切と判断した追加の審査を行う。

1.4.1.3 加入者の証明書

中間認証局は、加入者に対し証明書を発行する。

加入者の証明書は、加入者のサーバまたはネットワーク機器を認証し、また、これらと信頼当事者のクライアント機器間における SSL/TLS 暗号化通信を実現する。中間認証局の登録局は、加入契約書が継続して有効である（本サービスを継続して利用している）場合、加入者の証明書の発行にあたり、本 CPS に基づき、以下の事項について審査する。

① 加入者の法的または物理的な実在性

② 加入者の証明書に含まれる Fully-Qualified Domain Name（以下、「FQDN」という。）を加入者が使用する権利があり、名前制約に抵触しないこと

③ 申請責任者の在職

④ 手続き担当者による申請行為に対する申請責任者による承認

⑤ ハイリスク・ステータス等※

※ハイリスク・ステータス等として、以下を調査する。

- 過去のフィッシング事例
- フィッシングおよびその他詐欺行為等の疑義により、中間認証局が過去に棄却した申請の記録または失効した加入者の証明書の記録

上記調査により、中間認証局へ申請された加入者の証明書の不正使用の嫌疑が生じた場合、中間認証局は、必要に応じて適切と判断した追加の審査を行う。

なお、本サービスにおいては、加入者の証明書に OU は含まれない。

また、ルート認証局の配下に EV 証明書は発行しない。

1.4.1.4 OCSP 証明書

OCSP 証明書は、認証局が発行し使用する OCSP 用証明書であり、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

証明書の用途を次のとおり定める。

1.4.2.1 加入者の証明書

① 証明書を設定する機器（サーバ、ネットワーク機器等）の認証

② SSL または TLS 暗号化通信

1.4.2.2 OCSP サーバ証明書

① 失効情報を提供する OCSP レスポンスの応答への電子署名

1.4.2.3 中間認証局証明書

① 名前制約で指定されたドメインを保有する加入者への加入者証明書の発行

② 加入者証明書の失効情報を提供する OCSP レスポンダ用の OCSP サーバ証明書の発行

1.4.3 禁止される証明書の用途

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 および加入契約書は、CTJ PA により管理される。

1.5.2 連絡窓口

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　東京都港区六本木一丁目 9 番 10 号 アークヒルズ仙石山森タワー 35 階 宛　先　：jcsi-r@cybertrust.ne.jp 受付内容: ・発行のための申請方法および技術に関するお問合せ ・失効のための申請および申請方法に関するお問合せ ・証明書に問題が生じた場合や不正な証明書を発見された場合のお問合せ ・その他苦情の連絡 ・本 CPS 等に関するお問合せ

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 CPS 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

リポジトリはサイバートラストが管理する。サイバートラストは、本 CPS を適宜または少なくとも年に 1 回改訂する。

2.2 公開する情報

次の情報をリポジトリで公開する。

① 以下の情報を https://www.cybertrust.co.jp/jcsi/repository.html 上に公開する。

- 本 CPS

なお、加入契約書については窓口より本サービス申込者へ開示するものとする。

② 以下の情報を、http://rtcrl.managedpki.ne.jp/SecureSignAD/SecureSignRootCA11/SSAD-rca.crt 上に公開する。

- ルート認証局の証明書

③ 以下の情報を、http://rtcrl.managedpki.ne.jp/SecureSignAD/SecureSignRootCA11/cdp.crl 上に公開する。

- ルート認証局が発行する証明書の CRL

2.3 公開の時期と頻度

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 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 ルート認証局の証明書は、少なくともルート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

サイバートラストは、読み取りのみの制限を講じたうえでリポジトリを公開する。

3. 識別および認証

3.1 名前の決定

3.1.1 名称のタイプ

加入者は、証明書の中の X.500 識別名 Distinguished Name（以下、「DN」という。）により識別される。

3.1.2 名称の意味に関する要件

証明書の DN に含まれる名称は、次項の意味を持つ。

DN 項目	意味
コモンネーム（Common Name）	中間認証局の名称、または加入者の証明書を使用するサーバまたはネットワーク機器の完全なホスト名
組織名（Organization）	加入者の組織名称
組織単位名（Organization Unit）	（本サービスでは使用不可）
市区町村名（Locality）	加入者の事業所住所（市区町村名）
都道府県名（State or Province）	加入者の事業所住所（都道府県名）
国名（Country）	加入者の事業所住所（国）

3.1.3 加入者の匿名・仮名について

認証局は匿名または仮名での証明書を許容しない。

3.1.4 様々な名称形式を解釈するためのルール

認証局が発行する証明書の DN の形式を解釈するためのルールは、X.500 に準ずる。

3.1.5 名称の一意性

認証局が発行する証明書は、DN により加入者を一意に識別する。

3.1.6 商標等の認識、認証および役割

認証局は、証明書の発行に際し、著作権、営業秘密、商標権、実用新案権、特許権その他の知的財産権（特許その他の知的財産を受ける権利を含むがこれらに限られない。以下単に「知的財産権」という。）については認証しない。

3.2 初回の本人性確認

3.2.1 秘密鍵の所有を確認する方法

加入者からの申請情報の一部である証明書発行要求（以下、「CSR」という。）には、公開鍵および公開鍵に対応する秘密鍵による電子署名が含まれる。

中間認証局は、CSR に含まれる公開鍵を使用して電子署名を検証することで、加入者の秘密鍵で署名されていることを確認し、また、加入者が秘密鍵を所有していると判断する。

ルート認証局は、本サービスの利用をもって、中間認証局運営者が中間認証局の秘密鍵の管理者になったものとみなす。

3.2.2 組織とドメインの認証

3.2.2.1 身元の確認

認証局は、本 CPS「1.4.1 証明書の種類」に定める事項を審査し確認する。

加入者の確認に際しては、公的書類・データ、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。

ただし、加入者より受理した書類もしくはデータまたは認証局が独自に入手した書類やデータ等で審査済みかつ有効なものがある場合には、当該書類やデータ等の再提出を求めない。

加入者に求める確認手続きの詳細については、加入者への個別の通知により行う。

なお、本サービスでは、加入者以外の第三者が保有するドメイン名に対し加入者が証明書を取得・利用することを認めない。

3.2.2.2 DBA/Tradename

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

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

ルート認証局は中間認証局証明書の発行に先立って、ルート認証局が以下のうち最低一つの方法を使用し、中間認証局証明書の名前制約拡張子内の許可された DNS 名に記載されるそれぞれのドメイン名(FQDN)を審査したことを確認するものとする。

中間認証局は加入者の証明書の発行に先立って、中間認証局が以下のうち最低一つの方法を使用し、加入者の証明書内に記載されるそれぞれの FQDN を審査したことを確認するものとする。ただし、認証局は「.onion」のラベルで終わる FQDN の証明書を発行しない。

加入者のドメイン名の承認、または管理についての審査結果は、初回の審査完了から 398 日未満の期間において再利用を認め、複数の加入者の証明書の発行に有効とする。また、再利用期間を経過した後の申請においては、再度ドメイン名の承認、または管理についての審査を行う。すべてのケースにおいて、審査は、加入者の証明書の発行に先立ち、関連のある要項（BR4.2.1 など）で指定された期間内に開始されなければならない。ただし、ドメイン審査を目的としたとき、本サービスにおいて「加入者」という単語は、加入者の親会社、子会社を含むものとする。

認証局は、すべてのドメイン審査に使用した審査方法について、BR のバージョン情報を含むどの方法であったかの証跡を保持するものとする。

注意：FQDN は subjectAltName 拡張子にある dNS 名を使用して加入者の証明書に記載されるか、ネーム制約拡張子内の許可されたサブツリーにある dNS 名によって中間認証局証明書内に記載される。

なお、認証局は、ドメイン名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込者の検証

認証局は BR 3.2.2.4.1 で規定される手法を使用しない。

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

認証局は、ランダム値を電子メール、FAX、SMS、または郵便により送付し、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、または郵便により、複数の承認ドメイン名について確認を行う場合がある。

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、または郵便でそれぞれ一意とする。

認証局は、再利用したランダム値を含む電子メール、FAX、SMS、または郵便全体を再送する場合がある。但し、通信における内容と受信者が同一の場合に限るものとする。

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。

注意：一度この方法を使用して FQDN の審査が行われると、中間認証局は審査済みの FQDN で終わるすべてのラベルの他の FQDN に対しても加入者の証明書を発行することができる。この手法はワイルドカードドメイン名の申請にも適用できる。

3.2.2.4.3 ドメイン連絡先への電話連絡

認証局は、以下に示す手法を用いた検証を 2019 年 3 月 31 日以後、行わない。なお同手法を用いて検証済みの情報は、後続の発行に対し、該当する証明書データの再利用期間の間は引き続き有効とする。

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、確認の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。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特定されている電話番号に対し電話するものとする。

それぞれの通話は、一つの番号に対して行うが、複数の FQDN の管理権限の確認を行うことができるものとする。ただし、その電話番号は、電話で検証しようとしているすべてのベースドメイン名において、有効な連絡手段として、ドメイン名レジストラによって特定されているものを使用するものとする。

注意：一度この手法により FQDN が検証されたら、認証局は、すべてのラベルが検証された物と同じもので終わる FQDN に対する加入者の証明書の発行も行うことができる。この手法はワイルドカードドメイン名の審査にも適用できる。

3.2.2.4.4 ドメイン連絡先への作り込まれた電子メール

FQDN に対する加入者の管理権限を

① 'admin', 'administrator', 'webmaster', 'hostmaster', または'postmaster'をローカルパートとして、その後に@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、かつ

② ランダム値をメール内に含め、

③ その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。

それぞれのメールは、複数の FQDN について管理権限を確認する場合がある。ただし、電子メールに使用される承認ドメイン名は、確認されるべきそれぞれの FQDN に関わ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ものとする。

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。

注意：一度この方法を使用して FQDN の審査が行われると、中間認証局は審査済みの FQDN で終わるすべてのラベルの他の FQDN に対しても加入者の証明書を発行することができる。この手法はワイルドカードドメイン名の申請にも適用できる。

3.2.2.4.5 ドメイン認可文書

認証局は BR 3.2.2.4.5 で規定される手法を使用しない。

3.2.2.4.6 合意に基づく Web サイトの変更

認証局は、以下に示す方法を用いた審査を 2020 年 6 月 1 日以後行わない。ただし、同日より前に同方法を用いて審査済みの情報は、該当する証明書データの再利用期間内は引き続き有効とする。

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、アクセス可能な承認ドメイン名を確認し、申込者の 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、証明書申込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)申込者が加入者の証明書の発行要求を行った場合には、加入者の証明書に関する有効な情報の再利用が許可された期間（BR 4.2.1）を超えて使用しない。

ただし、名前制約が指定された中間認証局ではリクエストトークンを採用しないこととする。

3.2.2.4.7 DNS の変更

1）承認ドメイン名、または 2）アンダースコア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およ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込者の 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、認証局は申込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)申込者が証明書発行要求を行った場合、証明書に関する（BR 4.2.1 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。

ただし、名前制約が指定された中間認証局ではリクエストトークンを採用しないこととする。

3.2.2.4.8 IP アドレス

ルート認証局は、IP アドレスを含む加入者の証明書を配下に発行することを認めず、中間認証局証明書の名前制約にこれを指定する。

3.2.2.4.9 テスト証明書

認証局は BR 3.2.2.4.9 で規定される手法を使用しない。

3.2.2.4.10 ランダムナンバーを使用した TLS

認証局は BR 3.2.2.4.10 で規定される手法を使用しない。

3.2.2.4.11 その他の方法

認証局は BR 3.2.2.4.11 で規定される手法を使用しない。

3.2.2.4.12 申請者をドメインの連絡先としての検証

認証局は BR 3.2.2.4.12 で規定される手法を使用しない。

3.2.2.4.13 DNS CAA Contact へのメール

認証局は BR 3.2.2.4.13 で規定される手法を使用しない。

3.2.2.4.14 DNS TXT Contact へのメール

認証局は BR 3.2.2.4.14 で規定される手法を使用しない。

3.2.2.4.15 Domain Contact への電話連絡

ドメイン連絡先(Domain Contact) の電話番号に電話して、申請者の FQDN 管理権限を確認し、承認ドメイン名の検証のための確認を取る。検証する各承認ドメイン名に同じ Domain Contact 電話番号がリストされており、それらにより各承認ドメイン名の確認がとれるのであれば、各電話で、複数の承認ドメイン名についての管理権限を確認してよい。ドメイン連絡先以外の誰かに電話がつながった場合には、認証局はドメイン連絡先への転送を求めてもよい。ボイスメールにつながった場合には、認証局は、ランダム値と検証中の承認ドメイン名をメッセージとして残す。認証局は、ランダム値が返された場合に申請を承認する。認証ドメイン確認のためのランダム値は、作成から 30 日以内は有効として使用できる。

注意：一度この方法を使用して FQDN の審査が行われると、中間認証局は審査済みの FQDN で終わるすべてのラベルの他の FQDN に対しても加入者の証明書を発行することができる。この手法はワイルドカードドメイン名の申請にも適用できる。

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

DNS TXT レコード記載の電話連絡先(DNS TXT Record Phone Contact) の電話番号に電話して、申請者の FQDN 管理権限を確認し、承認ドメイン名の検証のための確認を取る。検証する各承認ドメイン名に同じ DNS TXT Record Phone Contact 電話番号がリストされており、それらにより各承認ドメイン名の確認がとれるのであれば、各電話で、複数の承認ドメイン名についての管理権限を確認してよい。この電話番号はドメイン検証の目的で明確に記載されているため、認証局は、故意に電話を転送されたり、また、転送を求めたりしない。ボイスメールにつながった場合には、認証局は、ランダム値と検証中の承認ドメイン名をメッセージとして残す。認証局は、ランダム値が返された場合に申請を承認する。認証ドメイン確認のためのランダム値は、作成から 30 日以内は有効として使用できる。

注意：一度この方法を使用して FQDN の審査が行われると、中間認証局は審査済みの FQDN で終わるすべてのラベルの他の FQDN に対しても加入者の証明書を発行することができる。この手法はワイルドカードドメイン名の申請にも適用できる。

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

認証局は BR 3.2.2.4.17 で規定される手法を使用しない。

3.2.2.4.18 合意に基づく Web サイトの変更 v2

認証局は、リクエストトークンまたはランダム値が、ファイルの内容に含まれていることを確認することにより、加入者の FQDN に対する承認または管理について審査する。

① リクエストトークンまたはランダム値が、ファイルの取得に使用される要求に現れてはならない。

② HTTP リクエストを送信し、成功したステータスコードの受信（HTTP ステータスコード 2xx）を確認しなければならない。

リクエストトークンまたはランダム値が含まれるファイルは、以下について審査する。

① 承認ドメイン名の下に配置されなければならない。

② 「/.well-known/pki-validation」ディレクトリ下に配置されなければならない。

③ 「HTTP」または「HTTPS」スキームにより取得されなければならない。

④ 認可されたポートを介してアクセスされなければならない。

リダイレクトで確認する場合、以下について審査する。

① リダイレクトは、HTTP プロトコル層により開始されなければならない。

リダイレクトは、RFC7231 の 6.4 節に定める HTTP ステータスコード 301、302、または 307、および RFC7538 の 3 章で定める HTTP ステータスコード 308 のいずれかによらなければならない。また、リダイレクト先は RFC7231 の 7.1.2 項に定めるロケーション HTTP 応答ヘッダーの最終値でなければならない。

② 「HTTP」または「HTTPS」スキームで表される リソース URL へのリダイレクトでなければならない。

③ 認可されたポートを介してアクセスされるリソース URL へのリダイレクトでなければならない。

ランダム値が使用される場合、以下について審査する。

① 認証局は、証明書の要求に対し、一意のランダム値を発行するものとする。

② ランダム値は、ランダム値の作成日から 30 日以内の確認応答につき有効なものとする。

ただし、名前制約が指定された中間認証局ではリクエストトークンを採用しないこととする。

注意：一度この方法を使用して FQDN の審査が行われると、中間認証局は審査済みの FQDN で終わるすべてのラベルの他の FQDN に対しても加入者の証明書を発行することができる。この手法はワイルドカードドメイン名の申請にも適用できる。

3.2.2.4.19 合意に基づく Web サイトの変更 - ACME

認証局は BR 3.2.2.4.19 で規定される手法を使用しない。

3.2.2.4.20 ALPN を使用した TLS

認証局は BR 3.2.2.4.20 で規定される手法を使用しない。

3.2.2.5 IP アドレスの認証

ルート認証局は、IP アドレスを含む加入者の証明書を配下に発行することを認めず、中間認証局証明書の名前制約にこれを指定する。

3.2.2.6 ワイルドカードドメインの認証

中間認証局は、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（*）を使用する加入者の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、BR 3.2.2.6 に従うものとする。

中間認証局は、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

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。

① 提供された情報の期間

② 情報源への更新の頻度

③ データ収集のデータ提供者と目的

④ データ可用性の一般的なアクセシビリティ

⑤ データを改ざんまたは変更する際の相対的な難しさ

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。

3.2.2.8 CAA レコード

ルート認証局は、Technically Constrained SubCA である中間認証局の提供を行う本サービスへの申込をもって、加入者が中間認証局を加入者の証明書の発行を許可する認証局として指定したものと認識し、中間認証局証明書の発行において、CAA レコードの確認を行わない。同様に中間認証局は BR 3.2.2.8. CAA Records の記載に従いオプション扱いとなる CAA レコードの確認を行わない。

なお、Technically Constrained SubCA ではない中間認証局においては、RFC8659（DNS Certification Authority Authorization (CAA) Resource Record）ならびに BR3.2.2.8 に従い、CAA レコードを確認する。

同中間認証局は、CAA レコード（issue/issuewild）に、本 CPS「4.2.1 本人性確認と認証業務の実行」で指定した値が含まれる場合、加入者の証明書の発行を許可する認証局として指定されたものと認識する。

3.2.3 個人の身元の認証

認証局は、個人に対して証明書を発行しない。

3.2.4 確認しない加入者情報

適用しない。

3.2.5 権限の確認

認証局は、申請責任者の在職および加入者を代表して申請を行う権限を有することを確認する。また、申請責任者が加入契約書に同意し、手続き担当者による申請行為を承認しているということを、コールバックまたはコールバックに相当する手段により確認する。コールバックに際して用いる電話番号は、第三者より提供を受けたもの、または加入者より提供される書類・データで認証局により信頼性が確保されていると判断された書類・データとする。

3.2.6 相互運用性基準

適用しない。

3.3 鍵更新申請時の本人性確認と認証

3.3.1 鍵定期更新時の本人性確認と認証

本 CPS「3.2 初回の本人性確認」を準用する。

3.3.2 失効を伴う鍵再発行時の本人性確認と認証

本 CPS「3.2 初回の本人性確認」と同様の手続きにより行う。

但し、再発行申請の CSR に含まれる公開鍵、証明書情報および満了日が再発行元の加入者の証明書と一致することを確認した場合、本 CPS「3.2 初回の本人性確認」の確認は行わず、それら一致の確認をもって加入者の証明書を発行する。

3.4 失効申請時の本人性確認と認証

加入者から電子メールにより失効申請を受理した際、申請した者の本人確認、申請する権限を有する者であることおよび失効の事由を確認する。確認方法としては、加入者の証明書の発行申込時に認証局へ通知された情報および認証局と加入者のみが知る情報の提示を受け、照合を行う。

加入者以外の者より証明書に対する失効申請を受けた場合、認証局は失効の事由を調査する。

加入者または加入者以外の者からの失効申請における失効事由が、証明書に関する加入契約書に定める失効対象事由に該当する場合、認証局は当該加入者へ連絡のうえ、失効する。

なお、失効申請のための電子メールアドレスは、本 CPS「1.5.2 連絡窓口」およびサイバートラストの Web サイト上に案内する。

4. 証明書のライフサイクル運用的要件

4.1 証明書申込

4.1.1 証明書の申込が認められる者

認証局に対し申込を行うことができる者は、申請責任者または申請責任者より申請する権限を付与された手続き担当者のみとする。

申請責任者、手続き担当者の選任については、本 CPS「1.3.4 加入者」の規定に定めるところによる。

また、認証局が加入者に対して行う申請の意思確認は、申請責任者または申請責任者より権限を付与された加入者組織内部の担当者が応ずるものとする。

4.1.2 申込方法および責任

申込者は、本 CPS および加入契約書に同意の上、申込を行う。申込に際し、申込者には、真正かつ正確な情報を提供する責任がある。申込方法については、申込を希望する者に個別に通知する。

4.2 証明書申込の処理

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。認証局の登録局が実施する。

中間認証局は、CAA レコード（issue/issuewild）に以下のいずれかの値が含まれる場合、加入者の証明書の発行を許可する認証局として指定されたものと認識する。

cybertrust.ne.jp
jcsinc.co.jp

4.2.2 証明書申込の承認または拒否

本 CPS「3.2 初回の本人性確認」に規定される要件がすべて確認された場合、認証局の登録局は申請を承認し、発行局へ発行を指示する。認証局は、加入者に対し事前に発行の案内をすることはない。

また、本 CPS「3.2 初回の本人性確認」に規定される要件が満たされない場合、認証局は申込を棄却する。この場合、認証局は、申込を行った申請責任者または手続き担当者に対し拒否の理由を通知する。なお、認証局は、申込のために申請責任者または手続き担当者より得た情報およびデータは返却しない。

申請責任者または手続き担当者から申込の取り下げがある場合、認証局は当該申込を棄却する。なお、認証局は、申込のために申請責任者または手続き担当者より得た情報・データは返却しない。

なお、認証局は Internal Name を含む証明書を発行しない。

4.2.3 証明書申請の処理に要する時間

認証局の登録局が本 CPS「4.2 証明書申込の処理」の規定に基づき申請を処理した後、発行局は遅滞なく指示された証明書を発行する。

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

認証局の登録局は、本 CPS「3.2 初回の本人性確認」に基づき申込処理を完了した後、発行局に対し証明書の発行を指示する。同発行局は、指示された証明書を発行した後、登録局にこれを伝え、登録局は加入者に対する通知を行う。

4.3.2 証明書の発行通知

認証局は、証明書の発行後速やかに、証明書が発行された旨と、加入者が証明書を受領するために必要な手続きについて、加入者に通知する。

4.4 証明書の受領

4.4.1 証明書受領手続き

加入者は、本 CPS「4.3.2 証明書の発行通知」の規定に基づき、中間認証局から送信された電子メールに従い、証明書を受領する。中間認証局は、当該通知をもって、加入者が証明書を受領したものとみなす。

4.4.2 認証局による証明書の公開

中間認証局は、基本的に証明書を公開しない。ただし必要に応じて、CT ログサーバ、CCADB 等に証明書を登録・公開する場合がある。

4.4.3 認証局による他の関係者に対する証明書発行の通知

中間認証局は、他の関係者に本 CPS「4.3.2 証明書の発行通知」の規定に基づく証明書の発行通知を行わない。

4.5 鍵ペアと証明書の利用

4.5.1 加入者による秘密鍵と証明書の利用

加入者は、本 CPS「1.4.2 適切な証明書の用途」に定める用途に限り秘密鍵および証明書を利用するものとし、その他の用途での利用は認められない。また、加入者の秘密鍵および証明書は、加入者のみが利用できるものとし、加入者は第三者に対してその利用を許諾してはならない。なお、秘密鍵と証明書の利用に関するその他の加入者の義務は、本 CPS「9.6.3 加入者の表明保証」に定める。

4.5.2 信頼当事者による加入者の公開鍵と証明書の利用

信頼当事者は、加入者が本 CPS「1.4.2 適切な証明書の用途」に定める用途で利用する証明書について、自らの責任で証明書の有効性について確認する。

なお、信頼当事者に対しての加入者の公開鍵と証明書の利用に関するその他の義務は、本 CPS「9.6.4 信頼当事者の表明保証」に定める。

4.6 鍵更新を伴わない証明書の更新

4.6.1 鍵更新を伴わない証明書の更新に関する要件

中間認証局は、加入者の証明書の有効期間の満了に伴い、更新申請を受け付ける。

4.6.2 更新申請が認められる者

本 CPS「4.1.1 証明書の申込が認められる者」を準用する。

4.6.3 更新申請の手続き

本 CPS「4.2 証明書申込の処理」を準用する。

4.6.4 更新された証明書の発行に関する通知

本 CPS「4.3.2 証明書の発行通知」を準用する。

4.6.5 更新された証明書の受領手続き

本 CPS「4.4.1 証明書受領手続き」を準用する。

4.6.6 更新された証明書の公開

本 CPS「4.4.2 認証局による証明書の公開」を準用する。

4.6.7 認証局による他の関係者に対する証明書の発行通知

本 CPS「4.4.3 認証局による他の関係者に対する証明書発行の通知」を準用する。

4.7 鍵更新を伴う証明書の更新

4.7.1 鍵更新を伴う証明書の更新に関する要件

中間認証局は、加入者が利用している証明書の有効期間の満了に伴い、更新申請を受け付ける。

4.7.2 更新申請が認められる者

本 CPS「4.1.1 証明書の申込が認められる者」を準用する。

4.7.3 鍵更新申請の手続き

本 CPS「4.2 証明書申込の処理」を準用する。

4.7.4 鍵更新された証明書の発行に関する通知

本 CPS「4.3.2 証明書の発行通知」を準用する。

4.7.5 鍵更新された証明書の受領手続き

本 CPS「4.4.1 証明書受領手続き」を準用する。

4.7.6 鍵更新された証明書の公開

本 CPS「4.4.2 認証局による証明書の公開」を準用する。

4.7.7 他の関係者に対する鍵更新された証明書の発行通知

本 CPS「4.4.3 認証局による他の関係者に対する証明書発行の通知」を準用する。

4.8 証明書の変更

4.8.1 証明書の変更に関する要件

中間認証局は、既に発行された加入者の証明書の変更の申請を受け付けないものとする。

加入者は、加入者の証明書の情報に変更が生じる場合、中間認証局に対し、遅滞なく当該証明書について失効を申請しなければならない。

4.8.2 証明書変更申請が認められる者

適用しない。

4.8.3 証明書変更の手続き

適用しない。

4.8.4 変更された証明書の発行に関する通知

適用しない。

4.8.5 変更された証明書の受領手続き

適用しない。

4.8.6 変更された証明書の公開

適用しない。

4.8.7 他の関係者に対する変更された証明書の発行通知

適用しない。

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

4.9.1.1.1 加入者の失効理由

加入者は、以下のいずれかの事由が生じた場合、中間認証局に対し該当する加入者の証明書の失効を申請しなければならない。

① 加入者が承認していない発行申請に基づき発行された加入者の証明書を発見した場合

② 加入者の秘密鍵の危殆化、または危殆化の可能性があることを知り得た場合

③ 加入者の秘密鍵または証明書の誤用、不正使用もしくはその可能性があることを知り得た場合

④ 加入者の証明書の内容に変更が生じた場合

⑤ 加入者の証明書に含まれる FQDN を独占的に使用する権利を失った場合

⑥ 加入者の証明書に記載されている情報が不正確であることを発見した場合

⑦ 加入者の証明書の利用にあたり、本 CPS、加入契約書のいずれかにおいて義務違反をした場合

⑧ 加入者の証明書が CA/Browser Forum の要件、本 CPS、加入契約書のいずれかに準拠していないことを知り得た場合

⑨ 加入者の証明書に名前制約に抵触する値が含まれていることを発見した場合

⑩ 加入者の証明書に組織単位名（OU）が含まれていることを発見した場合

⑪ 加入者が契約の解除を希望する場合

4.9.1.1.2 中間認証局による失効事由

中間認証局は、加入者の証明書の失効処理を行う前に、失効を要求する者の身元と権限を認証する。中間認証局は、以下の一つ以上の事象が生じた場合、加入者の証明書を 24 時間以内に失効するものとする。

① 加入者が、加入者の証明書を失効することを文書により中間認証局に要求した場合

② 加入者が、元の証明書要求を承認しておらず、可及的に許可を与えないことを中間認証局に通知した場合

③ 加入者の公開鍵に対応する秘密鍵が危殆化したという証拠を得た場合

④ 公開鍵を基に容易に加入者秘密鍵を算出できるよう発達した手法（例えば、「http://wiki.debian.org/SSLkeys」に記載される Debian weak key）を確認した場合

⑤ 加入者の証明書の FQDN についてのドメイン認証またはコントロールの検証に依拠すべきでないという証拠を得た場合

中間認証局は、以下の一つ以上の事象が生じた場合、24 時間以内に加入者の証明書を失効することがあり、また、5 日以内に加入者の証明書を失効するものとする。

① 加入者の証明書が BR の 6.1.5 章および 6.1.6 章に、もはや準拠していない場合

② 加入者の証明書が誤用されたという証拠を得た場合

③ 加入者が本 CPS、加入契約書のいずれかにおいて重要な義務違反をした場合

④ 加入者の証明書内の FQDN の使用が許可されていないことを示す事実を確認した場合（例：裁判所の調停人がドメイン名登録者によるドメイン名の使用権を取り消した場合、またドメイン名登録者と申請者の関連するライセンスやサービス協定が破棄された場合や、ドメイン名登録者がドメイン名の更新に失敗した場合）

⑤ 加入者の wildcard 証明書が、不正な下位 FQDN を認証するために使用されていることを確認した場合

⑥ 加入者の証明書内に含まれる情報に重大な変更があることを確認した場合

⑦ CA/Browser Forum の要件、本 CPS、加入契約書のいずれかに準拠せずに加入者の証明書を発行した場合

⑧ 加入者の証明書に記載されている情報が不正確であることを判断または確認した場合

⑨ CA/Browser Forum の要件に基づき、中間認証局が加入者の証明書を発行する権利が満了、失効および終了した場合。ただし、中間認証局が CRL/OCSP リポジトリを維持する調整を行った場合を除く

⑩ 本 CPS によって失効が必要とされた場合

⑪ 加入者秘密鍵を危殆化させるよう発達した手法が、実演されたまたは証明されたことを確認した場合

中間認証局が以下のいずれかに該当すると判断した場合、中間認証局は自らの単独裁量でいかなる加入者の証明書についても失効することができる。

① 本 CP「3.4 失効申請時の本人性確認と認証」に定める手続きにおいて、失効事由を確認できた場合

② 本 CPS に基づく加入者または中間認証局の義務が、当事者の合理的な管理の範囲を超える状況（コンピュータまたは通信の障害を含む）により遅延しまたは妨げられており、その結果、本認証局、加入者、または信頼当事者の情報に重大な脅威または危殆化が生じた場合

③ 加入者の証明書の失効処理を行うよう政府機関または規制機関から適法かつ拘束力を有する命令を受けた場合

④ 中間認証局が業務を停止し、他の認証局へ証明書の失効サポートを提供するよう手配をしなかった場合

⑤ 加入者の証明書の技術的コンテンツまたはフォーマットが、アプリケーションソフトウェアベンダー、信頼当事者、その他の者に対して許容できないリスクを呈している場合

⑥ 加入者が、取引禁止当事者または取引禁止対象者のブラックリストに掲載された場合

⑦ 加入者が、サイバートラスト所定の料金を支払わない場合

⑧ 加入契約書に基づきサイバートラストが加入者との契約を解除した場合

⑨ 中間認証局および／またはルート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知り得た場合

4.9.1.2 中間認証局証明書の失効理由

ルート認証局は、以下のいずれかの事由が生じた場合、7 日以内に該当の中間認証局証明書を失効する。

① 中間認証局から書面により失効が要求された場合

② 中間認証局から、本サービス申込は許可されておらず、遡及して許可を与えないことがルート認証局に通知された場合

③ 中間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 BR 6.1.5 または BR 6.1.6 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ルート認証局が知り得た場合

④ 中間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ルート認証局が知り得た場合

⑤ 中間認証局が BR または CPS に違反していることをルート認証局が知り得た場合

⑥ 中間認証局の証明書の内容が事実と異なる、または誤解を招くことをルート認証局が知り得た場合

⑦ ルート認証局、または中間認証局が何らかの理由で運用を中止し、かつ、発行済みの加入者の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 ルート認証局、または中間認証局が 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 ルート認証局が、本 CPS に基づき中間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

⑪ 本サービスが終了される場合

4.9.1.3 その他の証明書の失効理由

4.9.1.1.1 ルート認証局証明書

ルート認証局は、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、ルート認証局の証明書を失効する。ただし②については、別途ルート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 ルート認証局の秘密鍵の危殆化を知り得た場合

② ルート認証局が認証業務を終了する場合

4.9.1.1.2 OCSP 用証明書

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。

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 認証局が認証業務を終了する場合

4.9.2 失効申込が認められる者

失効申請が認められる者は、申請責任者または手続き担当者とする。

4.9.3 失効申込の手続き

失効申込が認められる者は、基本的に電子メールにより失効申込を行う。失効申込内容には、失効事由、連絡先等を含めなければならない。認証局は、失効事由を確認する。

認証局証明書および OCSP 証明書の失効については、当該認証局または上位認証局の認証局責任者が発行局に指示する。

4.9.4 失効申込までの猶予期間

加入者は、本 CPS「4.9.1.1 加入者証明書の失効理由」に該当する事由が生じたときは、速やかに失効申請を行うものとする。

該当する認証局責任者は、本 CPS「4.9.1.2 中間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

認証局は、24 時間 365 日失効申込を受け付ける。

認証局は、証明書の問題に関わる報告（Certificate Problem Report）を受領してから 24 時間以内に同報告に関連する事実および状況を調査し、その発見事項に関する予備的な報告を加入者および報告者の両方に連絡する。認証局は、事実および状況を検討した後、加入者および報告者、またはその他の失効通知者と協力し、証明書を失効するかどうか、および失効する場合の失効日を確定する。同報告または失効に関わる連絡の受領から失効情報公開までの期間は、本 CPS「4.9.1.1 加入者証明書の失効理由」に規定された期間を超えないこととする。認証局は、日付の選択に際し、以下の基準を考慮する。

① 申し立てられた問題の性質（範囲、文脈、重大度、規模、危害のリスク）

② 失効の影響（加入者および依拠当事者への直接的および付随的な影響）

③ 特定の証明書または加入者について受信した、証明書の問題に関わる報告数

④ 苦情を申し立てている事業体

⑤ 関連する法律

4.9.6 信頼当事者による失効の確認方法

信頼当事者は、認証局が発行する CRL または OCSP（Online Certificate Status Protocol）により、証明書の失効を確認する。

4.9.7 CRL 発行周期

中間認証局は、CRL を 24 時間以内の周期で発行する。

ルート認証局は、本 CPS「4.9.1.2 中間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

中間認証局の CRL の有効期間は 168 時間である。

中間認証局は、遅くとも CRL 発行から 1 時間以内に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

認証局の OCSP レスポンダは RFC 6960 および/または RFC5019 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 RFC6960 で定める 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

認証局は、CRL に加え OCSP により失効情報を提供する。

OCSP については、RFC 6960 および/または RFC5019 の記述通り GET method をサポートする。

中間認証局は、最大 168 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。

ルート認証局は、OCSP により、中間認証局に関わる失効情報の提供を行う。ルート認証局は少なくとも1年に1度、および中間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。

認証局は、セキュリティ確認の一環として、”unused” を返すシリアル番号の要求について OCSP レスポンダを監視する。

Pre-certificate [RFC6962]については発行されないため、ルート認証局および中間認証局の OCSP レスポンダは、発行予定となる証明書シリアル番号についての応答を特に提供しない。

なお、ルート認証局の 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

適用しない。

4.9.12 鍵の危殆化に関する特別要件

4.9.12.1 証明書

中間認証局は、加入者の秘密鍵の危殆化もしくは危殆化の可能性を知り得た場合、本 CPS「4.9.3 失効申請の手続」に基づき失効処理を行う。第三者が秘密鍵の危殆化により証明書の失効を要求する場合は、本 CP「1.5.2 連絡窓口」に定める”証明書に問題が生じた場合のお問合せ連絡先”へ通報することとし、同通報、またはその後の本認証局とのやり取りにおいて、以下を含めることとする。

① 鍵の危殆化を証明するための以下のいずれかの情報

- 秘密鍵自体
- 当該危殆化した秘密鍵を用い、本認証局が指定した文字列を Common Name 値として新たに作成した CSR

② 報告者の氏名と連絡可能な電子メールアドレスおよび電話番号

4.9.12.2 OCSP 用証明書

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 失効申込の手続」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

認証局は、証明書の一時停止に関する申請を受け付けない。

4.9.14 一時停止の申込が認められる者

適用しない。

4.9.15 一時停止の申込手続き

適用しない。

4.9.16 一時停止の期間

適用しない。

4.10 証明書のステータス確認サービス

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

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。

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。

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法執行当局または 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。

4.10.3 その他の要件

適用しない。

4.11 加入（登録）の終了

本サービスの利用が終了する事由は、契約書に定める。また、加入者は、証明書が有効期間中であるにもかかわらず、利用の中止を希望する場合、本 CPS「4.9.3 失効申請の手続」に基づき、中間認証局へ加入者の証明書の失効申込を行わなければならない

4.12 鍵の第三者預託および鍵回復

4.12.1 鍵の預託および鍵回復のポリシーならびに手順

適用しない。

4.12.2 セッションキーのカプセル化・復旧のポリシーの手順

適用しない。

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

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「5.1.8 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、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、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 媒体保管場所

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、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。

5.1.7 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。

5.1.8 バックアップサイト

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。

5.1.9 地震対策

本施設は耐震構造の建物であり、また、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。

5.2 手続的管理

5.2.1 信頼される役割

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。

5.2.1.1 認証局責任者

認証局責任者は、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、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、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、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、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、申込を処理し、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

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

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

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

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

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 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

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 s

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

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、記録を行う担当の識別情報、記録の概要を含めるものとする。

① **認証局証明書と鍵のライフサイクルイベントは、以下を含む**

- 鍵生成、バックアップ、保管、復元、アーカイブ、および破棄
- 証明書申請、更新/鍵更新申請、および失効
- 証明書申請の承認と棄却
- 暗号化デバイスのライフサイクル管理イベント
- 証明書の CRL および OCSP エントリの生成

- 新しい証明書プロファイルの導入、および既存の証明書プロファイルの停止

② **加入者証明書のライフサイクル管理イベントは、以下を含む**

- 証明書申請、更新/鍵更新申請、および失効
- 関連要件および認証局の CP/CPS に規定されるすべての審査証跡
- 証明書申請の承認と棄却
- 証明書発行
- CRL および OCSP エントリの生成

③ **セキュリティイベントは、以下を含む**

- PKI システムへのアクセス試行の成功および失敗結果
- 実行された PKI およびセキュリティシステムの動作
- セキュリティプロファイルの変更
- 証明書システムへのソフトウェアのインストール、更新および削除
- システムクラッシュ、ハードウェア障害、およびその他の異常
- ファイアウォールとルータの動作
- 認証局施設への入退室

④ **ログレコードには以下を含める**

- レコードの日時
- レコードの記録を行う担当の識別情報
- レコードの種類

5.4.2 監査ログを処理する頻度

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

本認証局は、下記の監査ログを少なくとも 7 年間保管するものとする。

① BR5.4.1 (1)**項に規定の認証局証明書および鍵のライフサイクル管理イベントの記録（直近に発生した以下の事象の発生後も上記期間まで保管する）**

- 認証局秘密鍵の破棄
- cA field が True に設定された X.509v3 basicConstraints 拡張を持ち、認証局証明書の秘密鍵に対する共通の公開鍵を共有する証明書内の最後の認証局証明書の失効または期限切れ

② BR5.4.1 (2)**項に規定の加入者証明書のライフサイクル管理イベントの記録**

③ BR5.4.1 (3)**項に規定のすべてのセキュリティイベント**

認証局は、監査ログが不要となったとき、本 CPS「5.1.7 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

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

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

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、認証局に関わるシステム（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

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。

① 認証局の証明書
② 加入者の証明書
③ CRL
④ 内部監査報告書
⑤ 外部監査報告書
⑥ 申込書類・データ
⑦ 本 CPS

5.5.2 記録の保管期間

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。

認証局は、記録が不要となったとき、本 CPS「5.1.7 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 記録のタイムスタンプについて

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、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

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

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

中間認証局は、本サービスへの新規の申込により、中間認証局の証明書の有効期限に至る前に中間認証局の鍵ペアを更新することができる。

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

5.7.1.1 中間認証局の危殆化時

サイバートラストは、本サービスにおいて中間認証局の秘密鍵が危殆化した場合、以下を実行すると同時に、危殆化の事実を加入者および信頼当事者へ公開する。

① 危殆化した秘密鍵を用いた認証業務の停止

② すべての加入者の証明書の失効

③ 危殆化の原因調査

④ 是正処置案の策定ならびに CTJ PA による評価・承認

⑤ 是正処置の実行

⑥ 業務再開の妥当性の評価

⑦ 新規の本サービスへの申込受付と新たな鍵ペアの生成、および中間認証局の用意

⑧ 認証業務の再開（加入者および信頼当事者への通知を含む）

⑨ 加入者の証明書の再発行

また、中間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、バックアップ用のハードウェア、ソフトウェアおよびデータ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加入者および信頼当事者に公開する。

5.7.1.2 ルート認証局の危殆化時

サイバートラストは、ルート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、危殆化の事実をルート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 ルート認証局の開局後発行されたすべての中間認証局証明書の失効

③ 対応措置（中間認証局への対応、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、ルート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

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

加入者は、自己の責任により管理する秘密鍵の危殆化もしくは危殆化が疑われる事態が生じた場合、本 CPS「4.9 証明書の失効および一時停止」に規定された手続に基づき、加入者の証明書の失効手続を行わなければならない。

中間認証局は、本 CPS「4.9.3 失効申込の手続き」に基づき、加入者の証明書を失効する。

5.7.4 災害時等の事業継続性

ルート認証局は、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、ルート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。

中間認証局の業務継続についてはルート認証局の業務継続を準用するものとする。

5.8 認証局の業務の終了

ルート認証局は、ルート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。

中間認証局は、本サービスの利用の終了をもって中間認証局の業務の終了となる。

中間認証局が保有する加入者の情報については、廃棄するものとする。

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

6.1.1.1 認証局の鍵ペアの生成

ルート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、ルート認証局の鍵ペアの管理のため FIPS 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。

ルート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、ルート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。

中間認証局および OCSP サーバで使用する鍵ペアは、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。

中間認証局の鍵ペア生成の際には、FIPS 140-2 レベル 4 の規格を満たした秘密鍵暗号モジュール（以下、「HSM」という。）の他、秘密分散の手法が用いられる。OCSP サーバで使用す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。

中間認証局の鍵ペアの生成は、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録画された生成作業を監査人へ提示することで、中間認証局の鍵ペアの生成が所定の鍵生成手順に即し行われることを担保する。

6.1.1.2 登録局の鍵ペアの生成

適用しない。

6.1.1.3 加入者の鍵ペアの生成

中間認証局は、要求された公開鍵が本 CPS「6.1.5 鍵アルゴリズムと鍵長」および「6.1.6 公開鍵パラメータ生成および検査」に記載された要件を満たさない場合、または既知の弱い秘密キーを持っている場合、証明書要求を拒否する。

中間認証局は、加入者証明書の鍵ペアの生成について、以下の一つ、または複数の条件に該当する場合、加入者からの証明書申請を棄却する。

① **BR6.1.5 項または 6.1.6 項で定められる鍵ペアの要件を満たさない場合**

② **秘密鍵生成に利用される特定の手法に欠陥があることを示す明確な証拠を得た場合**

③ **加入者の秘密鍵を危殆化させる実証された、または既知の手法を中間認証局が認識した場合**

④ **本 CPS の「4.9.1.1 加入者証明書の失効理由」の規定などにより、加入者の秘密鍵が危殆化していることを中間認証局が事前に認識した場合**

⑤ **公開鍵を基に加入者秘密鍵を容易に算出することが実証された、または既知の手法（例：Debian weak key https://wiki.debian.org/SSLkeys 参照）を中間認証局が認識した場合**

中間認証局は、加入者証明書の extKeyUsage 拡張に id-kp-serverAuth [RFC5280]または anyExtendedKeyUsage [RFC5280]のいずれかを含む場合、加入者証明書に使用される鍵ペアの生成は行わない。また中間認証局は、上記加入者証明書の発行において加入者の鍵ペアを過去生成したことはなく、従って中間認証局が過去に生成した鍵ペアを使用した証明書要求を受け入れることもない。

6.1.2 加入者秘密鍵の配送

中間認証局は、加入者の秘密鍵を配送しない。加入者の秘密鍵は、加入者自らが生成する。

6.1.3 認証局への加入者公開鍵の配送

加入者は、証明書発行要求データ中に公開鍵を含めたうえで、メールにより中間認証局へ配送する。

6.1.4 信頼当事者への認証局公開鍵の配送

中間認証局は、信頼当事者に対する中間認証局の公開鍵の配送を行わない。

ルート認証局の公開鍵が含まれるルート認証局の証明書は、リポジトリにて公開される。

6.1.5 鍵アルゴリズムと鍵長

6.1.5.1 ルート認証局

ルート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（モジュラスのサイズとしては、8 で割り切れる bit 数とする。）

6.1.5.2 中間認証局

中間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 が発行する中間認証局証明書	SHA2 with RSA	2048 bit（モジュラスのサイズとしては、8 で割り切れる bit 数とする。）

6.1.5.3 加入者証明書

加入者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。

加入者の証明書	署名方式	鍵長
中間認証局が発行する加入者の証明書	SHA2 with RSA	2048 bit（モジュラスのサイズとしては、8 で割り切れる bit 数とする。）

6.1.5.4 OCSP サーバ証明書

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 または中間認証局が発行する OCSP 用証明書	SHA2 with RSA	2048 bit（モジュラスのサイズとしては、8 で割り切れる bit 数とする。）

6.1.6 公開鍵パラメータ生成および検査

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

ルート認証局証明書の鍵用途（Key Usage）は、Certificate Signing 、CRL Signing である。

中間認証局の証明書の鍵用途（Key Usage）は、Digital Signature 、Certificate Signing 、CRL Signing とする。

加入者の証明書の鍵用途（Key Usage）は、Digital Signature、Key Encipherment 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

6.2.1 暗号モジュールの標準および管理

ルート認証局の鍵ペアを管理するための暗号モジュールは、FIPS 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。

中間認証局の鍵ペアを管理するための暗号モジュールは、FIPS 140-2 レベル 4 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(n out of m)

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

認証局は、認証局および OCSP で使用する秘密鍵の預託を行わない。また、加入者の秘密鍵の預託も行わない。

6.2.4 秘密鍵のバックアップ

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

認証局は、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

ルート認証局は、中間認証局に代わり同中間認証局の秘密鍵を生成することはしない。

認証局は、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

ルート認証局および 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。中間認証局の秘密鍵は、FIPS 140-2 レベル 4 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

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

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

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

認証局は、本 CPS「6.2.1 暗号モジュールの標準および管理」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

ルート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
ルート認証局の鍵ペア	2029 年 4 月 8 日

中間認証局の鍵ペアの有効期限は以下のとおりとする。

鍵ペア	有効期限
中間認証局の鍵ペア	2029 年 4 月 8 日までとする

OCSP 証明書の有効間は以下のとおりとする。

証明書	有効期間
OCSP 用証明書	25 ヶ月以内とする

加入者の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
加入者の証明書	397 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

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

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。

6.4.3 活性化データに関するその他について

適用しない。

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

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

認証局は、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 ライフサイクル技術管理

6.6.1 システム開発管理

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

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

認証局は、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

ルート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。

中間認証局のシステムおよび認証局の 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 記録のタイムスタンプについて」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

Appendix B に記載する。

7.1.2 証明書拡張領域

本認証局は、RFC5280 を含む適用可能な業界の基準に準拠した証明書拡張領域を使用する。本認証局は、重要なプライベート拡張を持つ証明書を発行しない。

下位認証局は、アプリケーションソフトウェア供給事業者が認める信頼ビットと PKI 使用例に則した ExtendedKeyUsage 拡張を含めるものとする。証明書には、anyExtendedKeyUsage の値が含めることはできない。対応するルート証明書と秘密鍵を共有するクロス証明書を除き、2019 年 1 月 1 日以降発行されるパブリックに信頼された証明書を発行するための中間認証局証明書においては：EKU 拡張を含む必要があるが、その KeyPurposeId は、anyExtendedKeyUsage を含めないものとし、また、id-kp-serverAuth と id-kp-emailProtection を同時に同じ証明書の KeyPurposeId として含めないものとする。

Technically Constrained Subordinate CA Certificate（技術的制約をかけた中間認証局）は、当該中間認証局が発行することを許可されたすべての鍵使用用途を、EKU 拡張に含むものとする。anyExtendedKeyUsage という KeyPurposeId は、パブリックに信頼された証明書の EKU には含めないものとする。

加入者証明書においては、SubjectAltName 拡張は RFC5280 に準拠して入力する。SubjectAltName 拡張に承認された Subject DN のコモンネームフィールド内の値（ドメイン名または IP アドレス）を入力する。SubjectAltName 拡張は、追加の承認されたドメイン名やグローバル IP アドレスを含む場合がある。国際化ドメイン名の場合には、そのドメイン名を Punycode アルゴリズムで符号化した値を SubjectAltName 拡張内に Punycode A-ラベル値として入力する。

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

本認証局は、BR、Mozilla Root Store Policy および関連要件に準じて、SHA256 with RSA を使用して証明書に署名を行う。

Appendix B に記載する。

なお、ルート認証局は SHA-1 ハッシュアルゴリズムを使用して中間認証局の証明書を発行せず、また中間認証局は SHA-1 ハッシュアルゴリズムを使用して加入者証明書を発行しない。

7.1.4 名前の形式

本認証局は RFC5280 の条項などで定められる、標準属性で構成される識別名を使用する。RFC5280 の 4.1.2.4 項に定めがある通り、IssuerDN フィールドの内容は、証明書チェーンをサポートするため、発行認証局の SubjectDN と同一とする。証明書には発行者名と 3.1.1 項で要件づけられている SubjectDN を含める。

加入者証明書においては、subjectAlternativeName 拡張は少なくとも1つ以上の FQDN を含む必要があり、その FQDN を 3.2.2.4 項に従い確認する。

Appendix B に記載する。

なお、アンダースコア（'_'）は、dNSName に含めてはならないものとする。

証明書の被発行者の属性には、'.'（ピリオド）、'-'（ハイフン）、' '（スペース）文字などのメタデータのみ、および/または、その他、値が存在しない、不完全、または該当しない、という表示のみを含めない。

証明書の被発行者の属性に、他の属性は存在してもよい。その場合、認証局は他の属性の情報を検証する。

7.1.5 名称の制約

中間認証局は、中間認証局証明書中の nameConstraints フィールドに名前制約を含む。

7.1.6 証明書ポリシーオブジェクト識別子

加入者の証明書のポリシーOID については、本 CPS「1.2 文書名と識別」に規定するとおりとする。併せて、CA/Browser Forum が定める {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} — 2.23.140.1.2.2 を含める。

① ルート認証局の Affiliate ではない中間認証局においては、

- BR を遵守した発行ポリシーを1つ以上含め、
- anyPolicy(2 5 29 32 0) を含めてはならない

② ルート認証局の Affiliate となる中間認証局においては、

- 発行ポリシーとして anyPolicy(2 5 29 32 0) を含める

③ ルート認証局のポリシーOID については、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

適用しない。

7.1.8 ポリシー修飾子の構文および意味

Appendix B に定める。

7.1.9 証明書ポリシー拡張についての処理方法

適用しない。

7.2 CRL のプロファイル

2020 年 9 月 30 日以降、失効された加入者証明書において、CRLReason に、「未指定(0)」または「証明書保留(6)」を含めない。過去の要件上の許容により、証明書の失効理由が未指定である場合には、認証局は reasonCode エントリ拡張を含めない。

2020 年 9 月 30 日以降、reasonCode CRL エントリ拡張がある場合には、RFC5280 の 5.3.1 項に記載されている下記の失効理由の中から最も適切な理由を CRLReason として指定する。

① keyCompromise (1) （鍵危殆化）

② cACompromise (2) （CA 危殆化）

③ affiliationChanged (3) （所属変更）

④ superseded (4) （破棄）

⑤ cessationOfOperation (5) （運用停止）

7.2.1 バージョン番号

Appendix B に定める。

7.2.2 CRL、CRL エントリ拡張

Appendix B に定める。

7.3 OCSP のプロファイル

発行局は、RFC6960 に準拠して OCSP サービスを運用する。

2020 年 9 月 30 日以降、パブリックに信頼された SSL/TLS サーバ証明書のクロス証明書を含むルート認証局証明書、および中間認証局証明書に対する OCSP レスポンスにおいて、証明書が失効されている場合、CertStatus の RevokedInfo 内における revocationReason フィールドが存在し有効な値を示さなければならない。

2020 年 9 月 30 日以降、パブリックに信頼された加入者証明書に関しては、表示される CRLReason について、本 CPS7.2 節「CRL のプロファイル」に規定にされた CRL に含めることが許容された値を含む。

7.3.1 バージョン番号

Appendix B に定める。

7.3.2 OCSP 拡張

Appendix B に定める。

8. 準拠性監査およびその他の評価

8.1 監査の頻度および要件

ルート認証局は、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。

Technically Constrained SubCA である中間認証局については、BR 8.1 に従い、BR 8.7 に定められる監査を実施する。

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。なお、資格を有する監査人とは、BR 8.2 に記載されている自然人、法人、または自然人または法人のグループを意味する。

8.3 監査人と被監査者の関係

監査人は、原則として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

ルート認証局の監査の範囲は、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。

中間認証局の監査の範囲は、BR 8.7 に従う。

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

中間認証局が加入者の証明書を発行する期間中、CPS および BR 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の証明書から、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

本サービスに関する料金については、加入者が適切に確認できる手段により通知する。

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

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 申込情報

② 本 CPS「9.4.2 個人情報として扱われる情報」に定める情報

③ 加入者、信頼当事者、その他第三者より受けた問合せ情報

④ 認証局のセキュリティに関する情報報

9.3.2 機密情報の範囲外の情報

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 加入者の証明書、中間認証局証明書およびルート認証局証明書

③ 認証局の過失によらず公知となった情報

④ 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

⑤ 加入者または申込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

9.3.3 機密情報の保護責任

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、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

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

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。

なお、認証局は、信頼当事者の OCSP 要求からのデータ（IP アドレスを含む）を一般データ保護規則（「GDPR」）、規則（EU）2016/679 に従い、個人データとして扱う。サイバートラストは、サーバーログ内のこれらのデータを使用したプロファイルの作成や個人の特定は行いません。サーバーログは運用目的でのみ使用され、通常少なくとも次の監査まで保持されます。その後、サイバートラストの内部ルールに従って削除されます。

9.4.3 個人情報とみなされない情報

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

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

認証局は、申込をもって、当該認証局が本 CPS で予定されている証明書発行・失効業務の履行および認証局の監査の実施のために申込書に記載された個人情報を使用することについて同意を得たものとみなす。

また、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

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

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、本サービスに関わる、以下の情報に関するすべての知的財産権は、サイバートラストに帰属するものとする。

① 本 CPS

② 認証局の公開鍵および秘密鍵

③ 開局日以後、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、加入者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、加入者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。

9.6.1 発行局の表明保証

発行局は、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 登録局からの申込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 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

9.6.2 登録局の表明保証

登録局は、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 本 CPS に基づく審査を行うこと

② 発行局への証明書発行申請および失効申請の正確な処理を行うこと

③ 問合せ受付（本 CPS「1.5.2 連絡窓口」）を行うこと

9.6.3 加入者の表明保証

加入者は、以下の義務を負うことを表明し保証する。

① 加入者の証明書の発行申込時における真正かつ正確な情報提供を行うこと

② 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

③ 加入者の証明書に含まれる情報の正確性が確認できるまで、加入者の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

④ 加入者の証明書に含まれる subjectAltName 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、法令ならびに加入契約書に従い証明書を使用すること

⑤ 証明書に含まれる公開鍵に紐づく加入者の秘密鍵に誤用や危殆化の疑いがある場合、速やかに証明書ならびに関連する秘密鍵の利用を停止し、失効申請を行うこと

⑥ 鍵の危殆化を理由として証明書を失効した場合、証明書に含まれる公開鍵に対応する秘密鍵のすべての使用を迅速に停止すること

⑦ 鍵の危殆化など本 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、指定期間内にサイバートラストの指示に従うこと

⑧ 本 CPS、加入者契約のいずれかに違反した場合、または CA/Browser Forum の要件により失効が必要な場合、本認証局が直ちに証明書を失効することを確認し承諾すること

⑨ 加入者の証明書に組織単位名（OU）を含めないこと

⑩ 加入者の証明書用途の遵守すること（本 CPS「1.4.2 適切な証明書の用途」）

⑪ 公序良俗に反する Web サイトで加入者の証明書を利用しないこと

⑫ 有効期間が満了した加入者の証明書および失効された加入者の証明書を使用しないこと

⑬ 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 証明書が本 CPS「1.4.2 適切な証明書の用途」に定める用途で利用されていることの確認を行うこと

② 証明書の有効期間と記載項目の確認を行うこと

③ 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

④ 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

⑤ 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

適用しない。

9.7 不保証

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。

認証局は、信頼当事者が自らの判断で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 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 加入者または信頼当事者が、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 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加入者、信頼当事者またはその他の第三者に対し、本サービスまたは証明書の申込、その承諾、信頼またはその他の利用を行うこと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、認証局は責任を負わない。

9.9 補償

認証局が発行した証明書を加入者または信頼当事者が受領または利用した時点で、加入者または信頼当事者には、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 証明書の不正使用、改ざん、利用時の不実の表明

② 本 CPS または加入契約書への違反

③ 加入者の秘密鍵保全の怠慢

また、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。

9.10 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、ルート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

サイバートラストから加入者に対し個別の通知を行う場合は、書面による手渡しがなされたとき、受取確認付き書留郵便により配達されたとき、または電子メールを送信したときをもって通知がなされたものとみなす。また、加入者からサイバートラストへのすべての通知は書面によりなされるものとし、当該通知が郵送され、サイバートラストが受領したときをもって到達したものとみなす。

9.12 改訂

9.12.1 改訂手続き

ルート認証局は、CTJ PA の指示に基づき本 CPS の見直しを年 1 回行う。また、適宜、本 CPS の改訂を行うことができる。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

ルート認証局は、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、加入者および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。加入者がその発効後 15 日以内に、加入者の証明書の失効を請求しない場合、加入者は改訂後の本 CPS につき同意したものとみなされる。

9.12.3 オブジェクト識別子の変更

CTJ PA は、本 CPS の改訂が OID の変更を必要とするかを判断する責任を負うものとする。

9.13 紛争解決手続き

本 CPS、サイバートラストが提供する本サービスまたは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

本 CPS に適用される全ての法令を遵守する。

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

サイバートラストは本サービスを第三者に譲渡不可とする。

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

サイバートラストは、いずれかの当事者の行為に関連して被った損害、損失、および費用について補償および弁護士費用の支払を求めることができるものとする。サイバートラストが本 CPS の何れかの規定の執行を怠った場合でも、かかる規程をサイバートラストがその後に執行する権利または本 CPS の他のいずれかの規定を執行する権利をサイバートラストが放棄したものとみなされることはないものとし、サイバートラストが署名した書面により、権利の放棄が有効となる。

9.16.5 不可抗力条項

天災地変、裁判所の命令、労働争議、その他サイバートラスト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、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

9.17 その他の事項

適用しない。

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。
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。
加入契約書	証明書を申請、使用するために加入者が同意する契約書である。本 CPS は、加入契約書の一部となる。
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。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。
中間認証局	Subordinate CA の別名。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。
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・失効の申込受付業務、審査業務、発行・失効・棄却業務、問合対応業務、請求業務、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。
ACME	Automated Certificate Management Environment の略であり、X.509 証明書のドメイン検証、インストール、および管理を自動化するための標準プロトコルである。
ALPN	Application-Layer Protocol Negotiation の略であり TLS の拡張機能である。
Baseline Requirements	Baseline Requirements for the Issuance and Management of Publicly‑Trusted Certificates 。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り、本 CPS ではその現行最新バージョンを指す。
CAA contactemail Property	CAA contactemail プロパティは、パラメータとして電子メールアドレスを取る。パラメータ値全体は、追加のパディングや構造を持たない、RFC 6532 のセクション 3.2 で定義されている有効な電子メールアドレスでなければならない。それ以外は、使用できない。 構文：contactemail <rfc6532emiladdress> 以下は、ドメインの所有者が電子メールアドレスを使用して連絡先プロパティを指定した例となる。 $ORIGIN example.com. CAA 0 contactemail "domainowner@example.com" ドメイン所有者が、認めていない認証局からドメインに関わる証明書が発行されることを望まない場合、contactemail プロパティを critical とすることができる。
CA/Browser Forum	認証局ベンダ、ブラウザベンダ、その他 SSL/TLS 証明書及びコード署名証明書を利用するアプリケーションベンダからなる任意団体である。EV ガイドラインや Baseline Requirements の策定等の活動を行っている。URL は、https://www.cabforum.org 。
Certification Authority Authorization Resource Record（CAA レコード）	ドメイン名に対して、サーバ証明書の発行を行う認証局を明確にし、意図しない証明書の発行を防ぐことを目的とした RFC8659 で定義されている DNS レコードの 1 つである。
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。
DNS TXT Record Email Contact	DNS TXT レコードは、検証されているドメインの "_validation-contactemail"サブドメインに配置されなければならない。この TXT レコードの RDATA 値全体は、RFC 6532 の 3.2 章で定義されているように、追加のパディングや構造を含まない有効な電子メールアドレスでなければならない。それ以外は、使用できない。

DNS TXT Record Phone Contact	DNS TXT レコードは、検証されているドメインの "_validation-contactphone"サブドメインに配置されなければならない。この TXT レコードの RDATA 値全体は、RFC 3966 の 5.1.4 章で定義されている有効なグローバルな番号でなければならない。それ以外は、使用できない。
FIPS 140-2	FIPS 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。
IP Address Contact	1 つ以上の IP アドレスの使用に関する管理権を持つ者として IP アドレス登録局に登録されている人または団体。
IP Address Registration Authority	Internet Assigned Numbers Authority (IANA、インターネット割当番号公社) 、または地域インターネットレジストリ（Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC)え
ITU-T	国際電気通信連合の電気通信標準化部門である。
JCSI SSL/TLS 証明書	JCSI 中間認証局から発行される SSL/TLS 用の証明書をいう。
JCSI 証明書発行サービス	加入者が JCSI SSL/TLS 証明書を取得・利用できるよう、Technically Constrained Subordinate CA である JCSI 中間認証局を用意し、これを提供するサイバートラストのサービスをいう。 サイバートラストは、JCSI 証明書発行サービスを JCSI SSL/TLS 証明書を取得・利用する加入者に対して提供し、Technically Constrained として登録・制約されるドメインを保有する加入者以外の組織に対して提供しない。
JCSI 中間認証局	JCSI ルート認証局下に発行される、Technically Constrained Subordinate CA である中間認証局をいう。
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。
RFC7231	IETF PKIX ワーキンググループが定める HTTP/1.1 メッセージの意味を定義した文書「Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content」である。
RFC7538	IETF PKIX ワーキンググループが定める追加のハイパーテキスト転送プロトコル（HTTP）ステータスコード 308（Permanent Redirect）を定義した文書「The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect)」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。
Technically Constrained Subordinate CA	Baseline Requirements に定義されている Technically Constrained Subordinate CA Certificate（技術的制約をかけた中間認証局証明書）、すなわち当該証明書中に Key Usage 拡張子および Name Constraint（名前制約）拡張子を登録し加入者証明書の発行に制約をかけた中間認証局証明書を使用する中間認証局をいう。
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

ルート認証局証明書（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 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	 2.5.4.6

	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	基本的制約	
cA	ＣＡかどうかを示すフラグ	
	型：Boolean	
	値：True（認証局である）	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 Parameters	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 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
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）

authoritytKeyIdentifier （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	失効リストがルート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	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	 sha256WithRSAEncryption
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
Validity		**値**
Validity notBefore	電子証明書の有効期間 開始日時 型：UTCTime 値：160306064915Z	 ＊有効開始日時 2017 年 3月 6日 06:49:15(GMT)
notAfter	終了日時 型：UTCTime 値：190331145959Z	 ＊有効終了日時 2019年 3月 31日 14:59:59(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 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 OCSP Responder	SecureSign RootCA11 OCSP Responder
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo AlgorithmIdentifier algorithm parameters subjectPublicKey	電子証明書所有者の公開鍵情報 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 (RSA PUBLIC KEY) 型：OID 値：1 2 840 113549 1 1 1 暗号アルゴリズムの引数 型：NULL 値： 公開鍵値 型：BIT STRING 値：公開鍵値	 1.2.840.113549.1.1.1 NULL 2048Bit 長の公開鍵

（拡張領域）

basicConstraints (extnId :== 2 5 29 19，critical :== FALSE)		**値**
BasicConstraints cA	基本的制約 ＣＡかどうかを示すフラグ 型：Boolean 値：FALSE（認証局ではない）	 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
extendedKeyUsage （extnId :== 2 5 29 37，critical :== FALSE)		**値**
extendedKeyUsage 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 （extnId :== 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

JCSI 中間認証局証明書(参考)

（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 （ランダムシリアル番号）
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-256) 型：OID 値：1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型：NULL 値：	 1.2.840.113549.1.1.11 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：yymmddhhmmssZ 終了日時 型：UTCTime 値：yymmddhhmmssZ	 ＊有効開始日時 yymmddhhmmssZ (作成年月日日時) ＊有効終了日時 290408045647Z (2029年 4月8 日 4:56:47 GMT)
Subject		**値**
CountryName type value OrganizationName type	電子証明書所有者の国名 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 電子証明書所有者の組織名 組織名のオブジェクト ID	 2.5.4.6 JP

	型：OID 値：2 5 4 10	2.5.4.10
value	組織名の値 型：PrintableString 値：Cybertrust Japan Co., Ltd.	Cybertrust Japan Co.,Ltd.
CommonName	電子証明書所有者の固有名称	
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：JCSI TLSSign Public CA	JCSI TLSSign Public CA (サンプル値)
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）

certificatePolicies （extnId :== 2 5 29 32，critical :== FALSE）		**値**
PolicyInformation	ポリシーに関する情報	
policyIdentifier	型：OID 値：2.5.29.32.0 (anyPolicy)	2.5.29.32.0
policyQualifiers	ポリシーに関する情報	
policyQualifierID	policyQualifiers の種別 型：OID 値：CPSuri のオブジェクト ID (id-qt-cps)	1.3.6.1.5.5.7.2.1
Qualifier	CPS が公開されている URI 型：OctetString 値：https://www.cybertrust.ne.jp/jcsi/repository.html	https://www.cybertrust.ne.jp/jcsi/repository.html
authorityInfoAccess (extnId :== 1 3 6 1 5 5 7 1 1，critical :== FALSE）		**値**
Authority Information Access	認証局情報アクセス	
Ocsp	オンライン証明書状態プロトコル 型：OID 値：1.3.6.1.5.5.7.48.1 型：OctetString 値：http://rtocsp.managedpki.ne.jp/OcspServer	1.3.6.1.5.5.7.48.1 http://rtocsp.managedpki.ne.jp/OcspServer
Caissuers	認証局アクセス方法 型：OID 値：1.3.6.1.5.5.7.48.2 型：OctetString 値：http://rtcrl.managedpki.ne.jp/SecureSignAD/SecureSignRootCA11/SSAD-rca.crt	1.3.6.1.5.5.7.48.2 http://rtcrl.managedpki.ne.jp/SecureSignAD/SecureSignRootCA11/SSAD-rca.crt
extendedKeyUsage (extnId :== 2 5 29 37，critical :== FALSE）		**値**
extendedKeyUsage	鍵の使用目的(拡張)	
KeyPurposeID	使用目的 ID	
serverAuth	型：OID 値：サーバ認証利用	1.3.6.1.5.5.7.3.1
authorityKeyIdentifier (extnId :== 2 5 29 35，critical :== FALSE）		**値**
AuthorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報	
keyIdentifier	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
cRLDistributionPoints (extnId :== 2 5 29 31，critical :== FALSE）		**値**
cRLDistributionPoints DistributionPoint uniformResourceIdentifie	CRL 配布ポイント CRL 配布ポイント URI 型：OctetString 値： http://rtcrl.managedpki.ne.jp/SecureSignAD /SecureSignRootCA11/cdp.crl	 http://rtcrl.managedpki.ne.jp/SecureSignAD /SecureSignRootCA11/cdp.crl
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 subjectPublicKey の Hash 値	 （subjectPublicKey のハッシュ値）
basicConstraints (extnId :== 2 5 29 19，critical :== TRUE）		**値**
BasicConstraints cA PathLenConstraint	基本的制限 ＣＡかどうかを示すフラグ 型：Boolean 値：True（認証局である） パス長の制約 型：INTEGER 値：0 （下位に認証局を持たない）	 TRUE 0
Name Constraints (extnId :== 2.5.29.30，critical :== TRUE）		**値**
Name Constraints Permitted Names Excluded Name	名前制限 dNS 名称 ディレクトリ名 IP アドレス(IPv4) IP アドレス(IPv6)	 .managedpki.ne.jp O=Cybertrust Japan Co.,Ltd., L=Minato-ku, ST=Tokyo, C=JP 0.0.0.0/0.0.0.0 0:0:0:0:0:0:0:0/0
keyUsage （extnId :== 2 5 29 15，critical :== TRUE）		**値**
KeyUsage	鍵の使用目的 型：BitString 値：10000110 (Digital Signature,keyCertSign,cRLSign)	 10000110 (0x86)

JCSI SSL/TLS 証明書（参考）

（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 （ランダムシリアル番号）
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-256) 型：OID 値：1 2 840 113549 1 1 11 暗号アルゴリズムの引数 型：NULL 値：	 1.2.840.113549.1.1.11 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：Cybertrust Japan Co., Ltd. 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：JCSI TLSSign Public CA	 2.5.4.6 JP 2.5.4.10 Cybertrust Japan Co.,Ltd. 2.5.4.3 JCSI TLSSign Public CA
Validity		**値**
Validity notBefore notAfter 	電子証明書の有効期間 開始日時 型：UTCTime 値：yymmddhhmmssZ 終了日時 型：UTCTime 値：yymmddhhmmssZ	＊有効期間：25ヶ月、編集可 ＊有効開始日時 ＊有効終了日時
Subject		**値**
CountryName Type value StateOrProvinceName type 	電子証明書所有者の国名 国名のオブジェクト ID 型：OID 値：2.5.4.6 国名の値 型：PrintableString 値：《所有者の国名》 電子証明書所有者の都道府県名 都道府県名のオブジェクト ID 型：OID	 2.5.4.6 JP

	値：2.5.4.8	2.5.4.8
value	都道府県名の値	
	型：PrintableString / UTF8String	
	値：《所有者の都道府県名》	Tokyo
LocalityName	電子証明書所有者の市町村名	
type	市町村名のオブジェクト ID	
	型：OID	
	値：2.5.4.7	2.5.4.7
value	市町村名の値	
	型：PrintableString / UTF8String	
	値：《所有者の市町村名》	Minato-ku
OrganizationName	電子証明書所有者の組織名	
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 / UTF8String	
	値：《所有者の会社名称》	Cybertrust Japan Co.,Ltd.
CommonName	電子証明書所有者の固有名称	
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	＊SSL/TLS 通信を行うサーバの FQDN
	値：《所有者の固有名称》	＊但し、ドメイン：.managedpki.ne.jp
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	＊鍵長は申請による
	値：公開鍵値	＊2048bit 以上が必須

（拡張領域）

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：FALSE（認証局ではない）	FALSE
certificatePolicies （extnId :== 2 5 29 32，critical :== FALSE)		**値**
PolicyInformation	ポリシーに関する情報	
policyIdentifier	型：OID	
	値：1.2.392.00200081.1.10.10	1.2.392.00200081.1.10.10
policyQualifiers	ポリシーに関する情報	
policyQualifierID	policyQualifiers の種別	
	型：OID	
	値：CPSuri のオブジェクト ID (id-qt-cps)	1.3.6.1.5.5.7.2.1
Qualifier	CPS が公開されている URI	
	型：URL	
	値： https://www.cybertrust.ne.jp/jcsi /repository.html	https://www.cybertrust.ne.jp/jcsi/repository.html
policyIdentifier	型：OID	
	値：2.23.140.1.2.2	2.23.140.1.2.2
subjectAltName （extnId :== 2.5.29.17，critical :== FALSE)		**値**
dnsName	dnsName	
	型：IA5String	

	値：《所有者の固有名称》	＊SSL/TLS 通信を行うサーバの FQDN ＊但しドメイン： .managedpki.ne.jp
authorityInfoAccess (extnId :== 1 3 6 1 5 5 7 1 1，critical :== FALSE)		**値**
Authority Information Access Ocsp	認証局情報アクセス オンライン証明書状態プロトコル 型：OID 値：1.3.6.1.5.5.7.48.1 型：OctetString 値：http://jcsitlssignpublicca-ocsp.managedpki.ne.jp/OcspServer	 1.3.6.1.5.5.7.48.1 http://jcsitlssignpublicca-ocsp.managedpki.ne.jp/OcspServer
Caissuers	認証局アクセス方法 型：OID 値：1.3.6.1.5.5.7.48.2 型：OctetString 値：http://rtcrl.managedpki.ne.jp/SecureSignAD/JCSITLSSignPublicCA/SSAD-JCSITLS.crt	 1.3.6.1.5.5.7.48.2 http://rtcrl.managedpki.ne.jp/SecureSignAD/JCSITLSSignPublicCA/SSAD-JCSITLS.crt
keyUsage （extnId :== 2 5 29 15，critical :== TRUE）		**値**
KeyUsage	鍵の使用目的 型：BitString 値：1010000 (digitalSignature,keyEncipherment)	 1010000(0xa0)
extendedKeyUsage (extnId :== 2.5.29.37，critical :== FALSE)		**値**
extendedKeyUsage KeyPurposeID serverAuth clientAuth	拡張鍵用途 使用目的 ID 型：OID 値：1.3.6.1.5.5.7.3.1 型：OID 値：1.3.6.1.5.5.7.3.2	 1.3.6.1.5.5.7.3.1（serverAuth） 1.3.6.1.5.5.7.3.2（clientAuth）
authorityKeyIdentifier (extnId :== 2 5 29 35，critical :== FALSE)		**値**
AuthorityKeyIdentifier keyIdentifier	電子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 subjectPublicKey の Hash 値	 *SubCA **公開鍵の** Hash **値**
cRLDistributionPoints (extnId :== 2 5 29 31，critical :== FALSE)		**値**
cRLDistributionPoints DistributionPoint uniformResourceIdentifie	CRL 配布ポイント CRL 配布ポイント URI 型：OctetString 値：http://rtcrl.managedpki.ne.jp/SecureSignAD/JCSITLSSignPublicCA/cdp.crl	 http://rtcrl.managedpki.ne.jp/SecureSignAD/JCSITLSSignPublicCA/cdp.crl
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 subjectPublicKey の Hash 値	 ＊所有者の subjectPublicKey の Hash 値