iTrust 電子署名用認証局

Certification Practice Statement

（認証局運用規程）

Version 1.2.1.

サイバートラスト株式会社

2023 年 1 月 19 日

■iTrust 電子署名用認証局 Certification Practice Statement（本 CPS）の著作権と配布条件

Version 1.2.1
改訂日：2023 年 1 月 19 日

改訂履歴

Version	日付	改訂事由
1.0	2018 年 3 月 2 日	・ 初版作成、 iTrust 電子署名用認証局（ルート認証局、中間認証局）開局
1.1	2019 年 1 月 11 日	・ 「1.1 概要」WebTrust for CA の参照 URL の修正 ・ 「1.5.2 連絡窓口」の名称修正 ・ 加入者向け証明書の HSM 対応に伴う修正 「3.2.1 秘密鍵の所有を確認する方法」に HSM の場合を追記 「6.1.2 加入者秘密鍵の配送」に HSM の場合を追記 「6.1.3 認証局への加入者公開鍵の配送」に HSM の場合を追記 「4.4.1 証明書受領確認手続き」に HSM の場合を追記 「9.6.3 加入者の表明保証」に HSM の場合を追記 「6.1.1 鍵ペアの生成」の HSM の記載を修正 ・ 「4.1.2 申請方法および責任」の Web サイトの記載誤字修正 ・ 加入者の対象から「個人事業主」を除外 ・ 「3.1.2 名称の意味に関する要件」の個人向け電子署名用証明書の SerialNumber の定義を修正
1.2	2019 年 8 月 23 日	・ 「4.4.1 証明書受領確認手続き」の記載を修正 ・ その他、表記等の修正
1.2.1	2023 年 1 月 19 日	・ RFC3647 へ適合するため、タイトル、章立てを変更 ・ 「3.1.2 名称の意味に関する要件」の個人向け電子署名用証明書に subjectAltName の定義を追加 ・ 「3.1.3 加入者の匿名・仮名について」を修正 ・ 「3.1.6 商標等の認識、認証および役割」を修正 ・ 「3.2.2.1 身元の確認」に CN と OU の審査方法を追記 ・ 「3.2.2.2 DBA/Tradename」に確認方法を追記 ・ 「3.2.2.4 データソースの正確性」の評価項目を修正 ・ 「3.2.3 個人の身元の認証」に個人向け電子署名証明書の本人確認方法ならびに組織属性の確認方法を追記 ・ 「3.2.4 確認しない加入者情報」を修正 ・ 「3.2.5 申請責任者の確認」に個人向け電子署名用証明書の申請責任者の確認方法を追記 ・ 「3.3 鍵更新申請時の本人性確認と認証」を修正 ・ 「4.4.1 証明書受領手続き」に個人向け電子署名用証明書の受領方法を追記 ・ 「4.6 鍵更新を伴わない証明書の更新」を修正 ・ 「4.9.1.1 加入者による失効事由」の失効事由の修正および追記 ・ 「4.9.1.2 本認証局による失効事由」の失効事由の修正および追記 ・ 「Appendix B:証明書等のプロファイル」の個人向け電子署名用証明書のプロファイルに subjectAltName の定義と組織属性のプロファイルを追記 ・ その他、軽微な文言修正等

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、iTrust サービスにおいて、「iTrust 電子署名用証明書」（以下、特段の規定がない限り、「証明書」または「加入者の証明書」という。）を発行する。

加入者の証明書は、電子文書の署名に用いる証明書であり、それぞれ法人向けならびに個人向けに発行、提供される。

サイバートラストは、Cybertrust iTrust Root Certification Authority（サイバートラスト iTrust ルート認証局、以下、「ルート認証局」という）ならびに、その下位認証局である Cybertrust iTrust Signature Certification Authority（サイバートラスト iTrust 電子署名用認証局、以下、「本認証局」という）を運営し、加入者の証明書は、本認証局より発行される。

認証局名称	Cybertrust iTrust Root Certification Authority
認証局証明書のシリアル番号	09 8e a5 03 20 ee 95 3b b7 b1 a4 88 4d 8c 6f d1 63 1f 8f c2
認証局証明書の有効期間	2018 年 2 月 19 日～2043 年 2 月 19 日
署名方式	SHA2 with RSA
認証局の鍵長	3072 bit
フィンガープリント（SHA1）	d8 84 ef 31 b8 5c db cb 0f 95 a6 f4 cd 03 8f 88 48 13 5d 25

認証局名称	Cybertrust iTrust Signature Certification Authority
認証局証明書のシリアル番号	72 4a bf c5 ea 71 1a 5b 7a 64 52 26 34 3b fd ab 3a d9 07 7f
認証局証明書の有効期間	2018 年 2 月 20 日～2028 年 2 月 20 日
署名方式	SHA2 with RSA
認証局の鍵長	2048 bit
フィンガープリント（SHA1）	e0 54 57 f9 f8 55 ee e0 94 55 29 e5 57 ac ac 89 3d d6 b6 ed
加入者に発行する証明書	電子署名用証明書
ルート認証局	Cybertrust iTrust Root Certification Authority

本認証局ならびにルート認証局は、証明書を発行するために、以下の規程および法令等に準拠する。

- WebTrust Principles and Criteria for Certification Authorities
- iTrust 電子署名用認証局 Certification Practice Statement (認証局運用規程)
- Adobe Approved Trust List Technical Requirements
- 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

本認証局ならびにルート認証局は、https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria で公開される WebTrust Principles and Criteria for Certification Authorities（以下、「WebTrust for CA」という。）の最新のバージョンに準拠する。「Certification Practice Statement（認証局運用規程）」（以下、「本 CPS」という。）と WebTrust for CA の間に齟齬がある場合には、WebTrust for CA が優先される。

本 CPS は、本認証局が証明書を発行するための要件を規定する。要件には、本認証局の義務、加入者の義務、信頼当事者の義務が含まれる。

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 および「Certificate Policy（証明書ポリシー）」（以下、「CP」という。）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、「該当せず」と記載する。

なお、本認証局は、CP を個別に定めず、本 CPS は CP を包含するものとする。

1.2 文書名と識別

本 CPS の正式名称は、「iTrust 電子署名用認証局 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
1.2.392.200081.1.20.1	Cybertrust iTrust Signature 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」に定める本認証局およびルート認証局をいう。各認証局は、発行局および登録局から構成される。

本認証局およびルート認証局は本 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

本認証局の登録局はサイバートラストが運営し、加入者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。同登録局は審査結果に基づき、発行局に対する加入者の証明書の発行もしくは失効の指示、または申請の棄却をする。

1.3.3 発行局

本認証局の発行局はサイバートラストが運営し、本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、本認証局の秘密鍵を管理する。

1.3.4 加入者

加入者は、本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証明書を利用する組織、または個人（自然人）である。

証明書を利用する組織において、申請に責任を有する者を申請責任者という。加入者たる組織は、申請責任者を組織内から選任しなければならない。

証明書を利用する組織において、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申請の権限を付与された手続き担当者に限られる。手続き担当者は、組織内または外部の者から選任することができる。外部の者から選任する場合は、個人であるか組織であるかを問わない。なお、外部の者から選任された手続き担当者については、加入契約書その他の規程において「申請代行者」と定義することがある。

証明書を利用する個人、ならびに個人事業主においては、申請責任者は加入者自身とし、また、証明書の申請を行うことができる者も加入者自身に限定する。

1.3.5 信頼当事者

信頼当事者は、本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、自らの判断で本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

該当せず。

1.4 証明書の用途

1.4.1 適切な証明書の用途

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 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。本認証局証明書は、ルート認証局から発行される。

1.4.1.3 証明書

証明書の用途を次のとおり定める。

(1) 法人向け電子署名用証明書

- 法人向け電子署名用証明書を使用する組織の認証
- 電子文書への電子署名

(2) 個人向け電子署名用証明書

- 個人向け電子署名用証明書を使用する個人の認証
- 電子文書への電子署名

1.4.2 禁止される証明書の用途

本認証局は、本 CPS「1.4.1 適切な証明書の用途」に定める用途以外での利用を禁止する。

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、サイバートラストにより管理される。

1.5.2 連絡窓口

本認証局は、サイバートラストが提供するサービスおよび本 CPS 等に関する照会を以下の連絡先で受け付ける。

連絡先
サイバートラスト株式会社 iTrust サポートデスク 住　所　：〒060-0807　札幌市北区北 7 条西 1 丁目 1-2 SE 札幌ビル 13 階 電　話　：011-708-5283 受付日　：月曜日～金曜日（祝祭日およびサイバートラストの Web サイトに掲載の年末年始、指定日を除く） 受付時間：9:00～18:00 お問合せおよび苦情：以下のとおり

内容	宛先
・発行のための申請方法および技術に関するお問合せ ・本 CPS 等に関するお問合せ	itrust_support@cybertrust.co.jp
・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	itrustca@cybertrust.co.jp

1.5.3 CPS の適合性を決定する者

本 CPS の適合性については CTJ PA 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、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

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、以下のとおりリポジトリを公開する。

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

- 本 CPS
- 加入契約書
- その他、本認証局のサービスに関わる約款等（以下、「関連諸規程」という。）
- ルート認証局の証明書に関わる情報
- 本認証局の証明書に関わる情報

以下の情報を、
http://crl.itrust.ne.jp/CybertrustiTrustRootCA/cdp.crl 上に公開する。

- ルート認証局が発行する下位認証局証明書の証明書失効リスト（以下、「ARL」という。）

以下の情報を、
http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl 上に公開する。

- 本認証局が発行する証明書の証明書失効リスト（以下、「CRL」という。）

以下の情報を、
http://crl.itrust.ne.jp/CybertrustiTrustRootCA/circa.crt 上に公開する。

- ルート認証局の証明書

以下の情報を、
http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.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、ARL および CRL は 24 時間公開される。

- 本リポジトリは 24 時間 365 日公開を維持する。
- 本 CPS、加入契約書、関連諸規程については、改訂の都度、公開される。

- CRL は、本 CPS「4.9.7 CRL 発行周期」で規定された周期で更新を行い、公開される。
- 本認証局およびルート認証局の証明書については、少なくとも有効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

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、および subjectAltName に含まれる名称は、次項の意味を持つ。

(1) 法人向け電子署名用証明書

DN 項目	意味
コモンネーム（Common Name）	加入者の組織名称。ただし、加入者の組織名称に続き、加入者の登録商標（Registered trademark）、部署名、サービス名称等を追記することを禁止しない
組織名（Organization）	加入者の組織名称
組織単位名（Organization Unit） ※（任意項目）	加入者の登録商標（Registered trademark）、部署名、サービス名称等
組織識別子（Organization Identifier）	国税庁の「法人番号公表サイト」において公開されている法人番号（13 桁）を転記し、先頭に「JCN」を付加した組織識別子、なお、法人番号が確認できない組織や個人事業主等の場合は本項目を含めない
国名（Country）	登記住所または実際に事業を行う物理的事業所住所上の国名

加入者の組織名については、QGIS 、QIIS、または本認証局が信頼できると判断した第三者機関のデータソース により確認可能な完全な法的組織名とする。個人事業主の場合の組織名については、個人事業主本人の氏名、もしくは商号登記で確認可能な商号、または開廃業届出書や所得税申告書類の控えにて確認可能な屋号とする。
企業略称、仮名（Assumed Name）等についてはこれを認めない。

組織単位名（Organization Unit）、またはコモンネーム（Common Name）に含める登録商標については、本 CPS 3.2.2.2 DBA/Tradename の規定に従い確認される。

組織単位名（Organization Unit）、またはコモンネーム（Common Name）に含める加入者組織の部署名、サービス名称等については、当該値について、本 CPS 3.2.2.1 身元の確認 に記載の審査・確認を行う。

(2) 個人向け電子署名用証明書

- 個人向け電子署名用証明書（組織属性なし）

DN 項目	意味
固有識別番号（SerialNumber）	「本人確認書類の区分記号」と「本人確認書類の個人識別番号のハッシュ値」を組み合わせた識別番号（但し、「本人確認書類の個人識別番号のハッシュ値」の利用が困難な場合には、本認証局は別途一意となる識別番号を証明書毎に割り振る）

姓（Surname）	加入者の姓
名（Given Name）	加入者の名
コモンネーム（Common Name）	加入者の氏名
国名（Country）	加入者の居住する住所上の国名

subjectAltName 項目	意味
国名（Country）	加入者の居住する住所上の国名（JP 固定）
都道府県名（State）	加入者の居住する住所（都道府県名）
市区町村名（Locality）	加入者の居住する住所（市区町村名、町名、番地）
生年月日（Organization Unit）	加入者の生年月日（西暦）
氏名（Common Name）	加入者の氏名

- 個人向け電子署名用証明書（組織属性あり）

・DN 項目	意味
固有識別番号（SerialNumber）	「本人確認書類の区分記号」と「本人確認書類の個人識別番号のハッシュ値」を組み合わせた識別番号（但し、「本人確認書類の個人識別番号のハッシュ値」の利用が困難な場合には、本認証局は別途一意となる識別番号を証明書毎に割り振る）
姓（Surname）	加入者の姓
名（Given Name）	加入者の名
コモンネーム（Common Name）	加入者の氏名
国名（Country）	加入者の居住する住所上の国名

subjectAltName 項目	意味
組織名（Organization）	加入者が所属する組織の名称
組織識別子（Organization Identifier）	国税庁の「法人番号公表サイト」において公開されている法人番号（13 桁）を転記し、先頭に「JCN」を付加した組織識別子、なお、法人番号を確認できない組織や個人事業主等の場合は本項目を含めない
都道府県名（State）	組織の住所（都道府県名）
市区町村名（Locality）	組織の住所（市区町村名、町名、番地）
組織単位名（Organization Unit） ※（任意項目）	加入者が所属する組織の部署名
肩書（Title） ※（任意項目）	加入者が所属する組織においての役職名

subjectAltName は、JIS 第一水準および JIS 第二水準に含まれない漢字が含まれている場合には、加入者に確認をしたうえで、JIS 第一水準および JIS 第二水準の範囲の漢字に置換する。置換のできない場合、または加入者が置換を希望しない場合には、ひらがなまたはカタカナで記載する。

subjectAltName に含める組織名と組織の所在地については、QGIS 、 QIIS、または本認証局が信頼できると判断した第三者機関のデータソース により確認可能な完全な法的組織名、ならびに所在地とする。
企業略称、仮名（Assumed Name）等についてはこれを認めない。

また、個人向け電子署名用証明書に組織属性を含める場合、部署名、役職名が正しいこと、ならびに加入者が当該組織に在籍する本人であり、当該組織の代表者より組織情報が格納された電子証明書の発行および署名権限の許諾を受けていることを本 CPS 3.2.3 個人の身元の認証 に記載の方法で審査・確認を行う。

3.1.3 加入者の匿名・仮名について

本認証局が発行する証明書については、加入者の匿名・仮名を認めない。

3.1.4 様々な名称形式を解釈するためのルール

本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

本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

法人向け電子署名用証明書については、組織単位名（OU）、またはコモンネーム（CN）の加入者の組織名称に続き、加入者が保有する登録商標（Registered trademark）を追記することを禁止しない。同登録商標については、本 CPS「3.2.2.2 DBA/Tradename」の規定に従い確認される。

3.2 初回の本人性確認

法人向け電子署名用証明書の発行のための組織の認証については「3.2.2 組織の認証」に記載する。
また、個人向け電子署名用証明書の発行のための個人の身元の認証については「3.2.3 個人の身元の認証」に記載する。

3.2.1 秘密鍵の所有を確認する方法

本認証局は、加入者に代わり加入者の秘密鍵を生成することがある。この場合、本 CPS「6.1.2 加入者秘密鍵の配送」に定めるとおり、本認証局は加入者へ秘密鍵を配送し、受領確認をもって加入者の秘密鍵の所有権は、本認証局から加入者に移転したものとし、以後、同秘密鍵の管理について本認証局は関知しない。

また、加入者が秘密鍵暗号モジュール（以下、「HSM」という。）により秘密鍵を生成する場合、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。本認証局は、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。

3.2.2 組織の認証

3.2.2.1 身元の確認

法人向け電子署名用証明書の加入者に関わる情報の確認に際しては、公的書類・データ、本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、加入者の組織の適切な役員・従業員、もしくは加入者を構成する組織へ照会を行う。また、必要に応じ加入者の組織への訪問調査を行う。

ただし、加入者に関わる情報を確認するための書類・データが本認証局によって審査済みであり、かつ、審査を行ってから一定期間（本認証局が予め定める期間）以上を経過していない場合には、本認証局は当該情報を加入者の確認に用いることができるものとする。

加入者に求める確認手続きの詳細については、サイバートラストの Web サイトでの案内または加入者への個別の通知により行う。

本認証局は、上記情報を用い、以下に定める事項を審査し確認する。

- 加入者の法的または物理的な実在性（組織名、組織住所、会社法人番号）
- 申請責任者の在職
- 加入契約書への同意
- 手続き担当者による申請行為に対する申請責任者の承認（手続き担当者による申請の場合）
- 本 CPS「3.1.2 名称の意味に関する要件」の (1) 法人向け電子署名用証明書」に規定される加入者証明書の DN（OU を除く）に含まれる各項目の真正性
- 証明書に含まれる組織単位名（OU）に以下の値が含まれないこと
  - 法人識別番号
  - "株式会社"、"Co. Ltd."等の法人格を示す文字列を含む値
  - 住所（場所を示す値）
  - 申請組織以外の名称、屋号、商標、その他特定の自然人や法人を参照させる値
  - ドット、ハイフン等の記号類およびスペースの単体、または記号類とスペースのみで構成される文字列
  - "NULL" 、"unknown"、"N/A"等の「該当なし」、「不完全」、「空欄」などを示す文字列
- 組織単位名（OU）、またはコモンネーム（CN）の加入者の組織名称に続き、加入者が保有する登録商標（Registered trademark）を追記する場合、本 CPS 3.2.2.2 DBA/Tradename の規定に従い確認する。
- 組織単位名（OU）、またはコモンネーム（CN）の加入者の組織式名称に続き、加入者組織の部署名、サービス名称等を含める場合、以下を確認する
  - 組織単位名（OU）に部署名を含む場合、加入者の組織より当該部署として署名することを許諾、または、その権限委任が行なわれていることを印鑑証明書で証明される当該組織の代表者印が押印された許諾書ないし委任状、およびその印鑑証明書の提出を受けることにより確認する。
  - 組織単位名（OU）に加入者が提供するサービス名称等を含める場合、加入者の組織よりサービス提供者として署名することを許諾、または、その権限委任が行なわれていることを印鑑証明書で証明される当該組織の代表者印が押印された許諾書ないし委任状およびその印鑑証明書の提出を受けることで確認する。
- 以下の調査により当該申請がハイリスクと判断された場合の追加審査
  - 詐欺行為等の疑義や本 CPS・加入契約書等への違反により、本認証局が過去に棄却した申請の記録または失効した証明書の記録

3.2.2.2 DBA/Tradename

法人向け電子署名用証明書の組織単位名（OU）、またはコモンネーム（CN）の加入者の組織名称に続き、加入者が保有する登録商標（Registered trademark）を追記する場合、本認証局は、当該商標等を使用する権利を加入者が有することを以下の少なくとも 1 つを用いて確認する。

- 承認の管轄権にある政府機関によって提供された文書、または政府機関と通信した文書

- 商号の登録管理を担当する政府機関が運営または管理するサイト
- 本認証局が信頼できると判断した第三者機関のデータソース
- 弁護士、司法書士、行政書士のいずれかによる意見書、または、公認会計士、税理士のいずれかによる報告書

3.2.2.3 Country の確認

本 CPS「3.2.2.1 身元の確認」に記載した方法で確認する。

3.2.2.4 データソースの正確性

本認証局は、審査で用いるデータソースの信頼性を評価する。評価では、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。

- 提供された情報の経過期間
- 情報源の更新の頻度
- データ提供者と収集目的
- データの可用性と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

本認証局は、本 CPS3.2 項に規定される確認要件を満たすために情報を収集することをデータベースの主な目的とする本認証局、本認証局の運営者、またはその提携企業により維持されるデータベース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

個人向け電子署名用証明書の加入者に関わる情報の確認として、本認証局は、以下を確認する。

- 加入者の実在性
- 本 CPS「3.1.2 名称の意味に関する要件」の (2) 個人向け電子署名用証明書に規定される、加入者証明書の DN に含まれる加入者の姓、名、氏名、加入者の居住する住所上の国名、および subjectAltName に含まれる加入者の姓、名、氏名、生年月日、加入者の居住する住所上の国名、都道府県名、市町村名、町名、番地の真正性
- 加入契約書への同意

加入者の実在性について、本認証局は、犯罪による収益の移転防止に関する法律施行規則第六条（顧客等の本人特定事項の確認方法）第一項第一号ホ、へまたはワ（以下に記載）のいずれかを用いて本人確認を行うことにより確認する。

ただし、「当該顧客等又はその代表者等」や「当該顧客等」を「加入者」と、また「特定事業者が提供するソフトウェア」を「本認証局が指定するソフトウェア」と、「特定取引等」を「個人向け電子署名用証明書の発行申請」と読み替えることとする。

なお、Adobe Approved Trust List Technical Requirements で許容されるビデオチャットでの本人確認は、犯罪による収益の移転防止に関する法律施行規則第六条（顧客等の本人特定事項の確認方法）第一項第一号ホに含まれる。

また、加入者証明書の DN ならびに subjectAltName に含まれる各項目の確認に際しては、加入者より提供される証明書発行時に有効な写真付き本人確認書類（運転免許証、マイナンバーカード、住民基本台帳カード、在留カード、特別永住者証明書、運転経歴証明書のいずれか1つ）を用いて行う。

- 犯罪による収益の移転防止に関する法律施行規則
  第六条（顧客等の本人特定事項の確認方法）第一項第一号
  - ホ　当該顧客等又はその代表者等から、特定事業者が提供するソフトウェアを使用して、本人確認用画像情報（当該顧客等又はその代表者等に当該ソフトウェアを使用して撮影をさせた当該顧客等の容貌及び写真付き本人確認書類の画像情報であって、当該写真付き本人確認書類に係る画像情報が、当該写真付き本人確認書類に記載されている氏名、住居及び生年月日、当該写真付き本人確認書類に貼り付けられた写真並びに当該写真付き本人確認書類の厚みその他の特徴を確認することができるものをいう。）の送信を受ける方法
  - ヘ　当該顧客等又はその代表者等から、特定事業者が提供するソフトウェアを使用して、本人確認用画像情報（当該顧客等又はその代表者等に当該ソフトウェアを使用して撮影をさせた当該顧客等の容貌の画像情報をいう。）の送信を受けるとともに、当該顧客等又はその代表者等から当該顧客等の写真付き本人確認書類（氏名、住居、生年月日及び写真の情報が記録されている半導体集積回路（半導体集積回路の回路配置に関する法律（昭和六十年法律第四十三号）第二条第一項に規定する半導体集積回路をいう。以下同じ。）が組み込まれたものに限る。）に組み込まれた半導体集積回路に記録された当該情報の送信を受ける方法
  - ワ　当該顧客等から、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成十四年法律第百五十三号。以下この号において「公的個人認証法」という。）第三条第六項の規定に基づき地方公共団体情報システム機構が発行した署名用電子証明書及び当該署名用電子証明書により確認される公的個人認証法第二条第一項に規定する電子署名が行われた特定取引等に関する情報の送信を受ける方法（特定事業者が公的個人認証法第十七条第四項に規定する署名検証者である場合に限る。）
- 以下の調査により当該申請がハイリスクと判断された場合の追加審査

詐欺行為等の疑義や本 CPS・加入契約書等への違反により、本認証局が過去に棄却した申請の記録または失効した証明書の記録

加入者は、本人確認において加入者の写真付き本人確認書類の画像等を本認証局に送信することにより、申請責任者として加入契約書へ同意し、申請を承認していることを表明するものとする。

個人向け電子署名用証明書に組織属性を含める場合、上記個人の身元の認証に加え、本認証局は以下を確認する。

- 組織の法的または物理的な実在性（組織名、組織住所、会社法人番号）
  - 法人向け署名用証明書と同様の書類、データを用いて確認する。
- 部署名、役職名、加入者の在籍、および署名権限

- 登記を行う組織の場合、印鑑証明書で証明される当該組織の代表者印が押印された許諾書ないし委任状、およびその印鑑証明書の提出を受けることにより、部署名や役職名が正しいこと、加入者が当該組織に在籍すること、ならびに当該組織の代表者より組織情報が格納された電子証明書の発行ならびに署名権限についての許諾を受けていることを確認する。なお、加入者が組織の登記簿謄本において代表取締役として、その氏名と住所を確認できる場合は、代表者印が押印された許諾書ないし委任状、およびその印鑑証明書提出は不要とする。
- 登記を行わない行政機関や公法人等の場合、当該組織の代表者印が押印された許諾書ないし委任状の提出をうけ、部署名や役職名が正しいこと、加入者が当該組織に在籍すること、ならびに当該組織の代表者より組織情報が格納された電子証明書の発行ならびに署名権限についての許諾を受けていることを確認する。また、当該組織の代表者印の印影が確認できる、当該組織が官公庁等に提出した書類、もしくは公文書等の資料の提出を受けることにより印鑑証明書の代替とする。
- 個人事業主の場合、個人の身元の認証の審査結果と商号登記、開廃業届出書、または所得税申告書類の控えに記載された氏名、住所の一致の確認により、個人事業主本人が加入者と一致することを確認するものとし、代表者印が押印された許諾書ないし委任状、およびその印鑑証明書提出は不要とする。

- 以下の調査により当該申請がハイリスクと判断された場合の追加審査

詐欺行為等の疑義や本 CPS・加入契約書等への違反により、本認証局が過去に棄却した申請の記録または失効した証明書の記録

なお、本認証局が必要と判断した場合は、追加の本人確認書類の提出を加入者に求めることができるものとし、加入者に関わる確認結果は、本認証局が定める期間において、再利用できるものとする。

3.2.4 確認しない加入者情報

(1) 法人向け電子署名用証明書

本認証局は、証明書の組織単位名（OU）、またはコモンネーム（CN）に含まれる部署名やサービス名称等が他者の権利を侵害しないこと、ならびにその情報の真正性および正確性は保証せず、確認しない。

(2) 個人向け電子署名用証明書

本認証局は、証明書の組織単位名（OU）に含まれる部署名や肩書（Title） に含まれる役職名の真正性および正確性は保証せず、確認しない。

3.2.5 申請責任者の確認

(1) 法人向け電子署名用証明書

本認証局は、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、本認証局は、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・データで本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。

(2) 個人向け電子署名用証明書

本認証局は、申請責任者が加入者自身であることを確認する。また、申請責任者は、「3.2.3 個人の身元の認証」において、写真付き本人確認書類の画像等を本認証局に送信することにより、加入契約書に同意し、申請を承認していることを表明するものとする。

3.2.6 相互運用性基準

該当せず。

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

本認証局は、鍵定期更新の申請を受け付けないものとする。

3.3.2 失効を伴う鍵再発行時の本人性確認と認証

本認証局は、失効を伴う鍵再発行の申請を受け付けないものとする。

3.4 失効申請時の本人性確認と認証

本認証局は、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申請の事由を確認する。確認方法としては、証明書の発行申請時に本認証局へ通知された情報および本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特定の加入者の証明書に対する失効申請を受けた場合、本認証局は失効申請事由を確認する。

いずれの場合も、失効申請事由が証明書に関する失効対象事由に該当する場合、本認証局は当該加入者へ連絡の上、当該証明書を失効する。

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 証明書申請

4.1.1 証明書の申請が認められる者

(1) 法人向け電子署名用証明書

申請を行うことができる者は、申請責任者または手続き担当者に限定する。

(2) 個人向け電子署名用証明書

申請を行うことができる者は、加入者本人に限定する。

4.1.2 申請方法および責任

(1) 法人向け電子署名用証明書

加入者は、本 CPS および加入契約書に同意の上、法人向け電子署名用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本認証局へ提供する責任がある。

証明書の申請方法については、サイバートラストの Web サイトまたは加入者個別に案内する。

(2) 個人向け電子署名用証明書

加入者は、本 CPS および加入契約書に同意の上、個人向け電子署名用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本認証局へ提供する責任がある。

証明書の申請方法については、サイバートラストの Web サイトまたは加入者個別に案内する。

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」に規定する手続きにより行う。

4.2.2 証明書申請の承認または拒否

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、本認証局の登録局は申請を承認し、発行局へ証明書の発行を指示する。本認証局は、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、本認証局は申請を棄却する。なお、本認証局は、申請時に提供された情報・データは返却しない。

申請の取り下げがあった場合も、本認証局は当該申請を棄却する。なお、申請情報・データは返却しない。

4.2.3 証明書申請の処理に要する時間

本認証局の登録局が本 CPS「4.2 証明書申請の処理」の規定に基づき申請を処理した後、発行局は速やかに証明書を発行する。

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

本認証局の登録局が本 CPS「4.2 証明書申請の処理」の規定に基づき申請を処理した後、発行局は速やかに証明書を発行する。併せて、本 CPS「4.3.2 加入者に対する証明書の発行通知」に定める通知を加入者に対し行う。

なお、加入者が証明書の発行を申請した時点から、サイバートラストと加入者との間において、証明書に関する加入契約書が発効するものとする。

4.3.2 加入者に対する証明書の発行通知

本認証局は、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または利用するために必要な手続きについて、加入者が申請時に指定した電子メールアドレスに対し通知する。また、秘密鍵の受領が必要な場合の手続きについても本通知に含めるものとする。

4.4 証明書の受領

4.4.1 証明書受領手続き

(1) 法人向け電子署名用証明書

加入者は、本認証局から送信される発行通知の内容に従い、FIPS140-2 レベル 2 以上の規格を満たした USB トークンに格納された証明書および秘密鍵を受領する。

また、加入者が HSM にて秘密鍵を生成する場合、加入者は本 CPS「4.3.2 加入者に対する証明書の発行通知」に基づき、本認証局から送信された電子メールで指定の URL からダウンロードするか、もしくは本認証局から送信された電子メールで通知されたリクエスト ID を「iTrust リモート署名サービス」の API で指定して、証明書を受領する。

(2) 個人向け電子署名用証明書

加入者は、本認証局から送信される発行通知の内容に従い、FIPS140-2 レベル 2 以上の規格を満たした USB トークンに格納された証明書および秘密鍵を受領する。

4.4.2 認証局による証明書の公開

本認証局は、加入者の証明書を公開しない。

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

本認証局は、本 CPS「4.3.2 加入者に対する証明書の発行通知」に規定する以外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「1.4.1 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「1.4.1 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、加入者の公開鍵と証明書の利用に関する信頼当事者の義務は、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

本認証局は、鍵更新を伴わない証明書の更新を受け付けないものとする。

4.6.2 更新申請が認められる者

該当せず。

4.6.3 更新申請の手続き

該当せず。

4.6.4 更新された証明書の発行に関する通知

該当せず。

4.6.5 更新された証明書の受領手続き

該当せず。

4.6.6 更新された証明書の公開

該当せず。

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

該当せず。

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

本認証局は、鍵更新を伴う証明書の更新を受け付けないものとする。

4.7.2 更新申請が認められる者

該当せず。

4.7.3 更新申請の手続き

該当せず。

4.7.4 鍵更新された証明書の発行に関する通知

該当せず。

4.7.5 鍵更新された証明書の受領手続き

該当せず。

4.7.6 鍵更新された証明書の公開

該当せず。

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

該当せず。

4.8 証明書の変更

4.8.1 証明書の変更に関する要件

本認証局は、既に発行された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、証明書情報に変更が生じた場合、本認証局に対し、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 変更申請が認められる者

該当せず。

4.8.3 変更の手続き

該当せず。

4.8.4 変更された証明書の発行に関する通知

該当せず。

4.8.5 変更された証明書の受領手続き

該当せず。

4.8.6 変更された証明書の公開

該当せず。

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

該当せず。

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 加入者による失効事由

加入者は、以下のいずれかの事由が生じた場合、本認証局に対し該当する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証明書を発見した場合
② 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を知り得た場合
③ 加入者の秘密鍵または証明書の不正使用もしくは不正使用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
⑥ 加入者が本認証局との間の加入契約の解除を希望する場合
⑦ 加入者の証明書の利用にあたり、本 CPS または加入契約書において義務違反をした場合
⑧ 加入者の証明書が本 CPS に準拠していないことを知り得た場合
⑨ 法人向け電子署名用証明書については、証明書に含まれる組織単位名（OU）に本 CPS「3.2.2.1 身元の認証」に記載の OU に含められない値が含まれていることを知り得た場合

4.9.1.2 本認証局による失効事由

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 CPS「4.9.3 失効申請の手続き」を経ることなく、加入者の証明書を失効することができる。ただし⑫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 加入者が加入者の証明書を失効することを文書により本認証局に要求した場合
② 加入者が証明書要求を承認しておらず、遡及して許可を与えないことをサイバートラストに通知した場合
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を合理的な証拠に基づき知り得た場合
④ 加入者の証明書が誤用または不正利用されたという証拠を得た場合
⑤ 加入者の証明書の内容が事実と異なることを合理的な証拠に基づき知り得た場合
⑥ 加入者が本 CPS または加入契約書に違反し、本認証局がその違反の是正を求める通知を発送した後、7 日間を経過した後においても、違反が是正されなかった場合
⑦ 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
⑧ 本認証局が、証明書を発行するために準拠すべき規制や本 CPS に準拠せずに証明書を発行した場合（ただし、この場合、本認証局は無償で正規の証明書申請を受け付ける。）
⑨ 本 CPS により失効が必要とされた場合
⑩ 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）が、実演されたまたは証明されたことを確認した場合
⑪ 本 CPS および CPS に基づく加入者または本認証局の義務が、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、証明書を信頼した当事者の情報に重大な脅威または危殆化が生じた場合
⑫ 加入者の証明書の失効処理を行うよう裁判所または行政機関から適法かつ拘束力を有する命令を受けた場合
⑬ 本認証局が認証業務を終了する場合
⑭ 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、信頼当事者、その他の者に対して許容できないリスクを含んでいる場合
⑮ 加入者が、サイバートラスト所定の証明書の料金を支払わない場合
⑯ 個人向け電子署名用証明書の場合、加入者の死亡を合理的な証拠に基づき知り得た場合
⑰ 法人向け電子署名用証明書については、証明書に含まれる組織単位名（OU）に本 CPS「3.2.2.1 身元の認証」に記載の OU に含められない値が含まれていることを知り得た場合
⑱ 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
⑲ 本認証局および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

4.9.2 失効申請が認められる者

失効申請が認められる者は、申請責任者、手続き担当者または証明書の発行申請時に本認証局から通知され、加入者が正当な代理権を設定した代理人とする。

4.9.3 失効申請の手続き

加入者は、電子メールにより失効申請を行う。失効申請内容には、本認証局の案内に従い、本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。本認証局は、本 CPS「3.4 失効申請時の本人性確認と認証」の定めるところにより、失効事由を確認する。

本認証局は、証明書の失効後、速やかにその旨加入者へ通知する。なお、本 CPS「9.1 料金」に定める無償発行を伴う失効の場合は、無償発行の連絡と併せて失効の通知をすることがある。

4.9.4 失効申請までの猶予期間

加入者は、本 CPS「4.9.1.1 加入者による失効事由」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。

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 により、証明書の失効を確認する。

4.9.7 CRL 発行周期

本認証局は、CRL を 24 時間以内の周期で発行する。

ただし、災害等による復旧対応ならびに業務継続対応が必要になる場合に限り、別途、業務継続計画に基づき、CRL の発行周期が上記周期を超える周期で発行する場合がある。

4.9.8 CRL 発行までの最大遅延時間

本認証局の CRL の有効期間は 168 時間である。

本認証局は、遅くとも発行から 1 時間以内にリポジトリに公開する。

ただし、災害等による復旧対応ならびに業務継続対応が必要になる場合に限り、別途、業務継続計画に基づき、CRL の有効期間が上記時間よりも大きな CRL をあらかじめバックアップサイトに保管し、公開する場合がある。

4.9.9 オンラインでの失効情報の確認

本認証局は、CRL をもって失効情報を提供する。その他オンラインでの失効情報の提供は行わない。

4.9.10 オンラインでの証明書ステータスの確認

該当せず。

4.9.11 その他の利用可能な失効情報の提供手段

該当せず。

4.9.12 鍵の危殆化に関する特別要件

本認証局は、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。

4.9.13 証明書の一時停止に関する要件

本認証局は、証明書の一時停止に関する申請を受け付けない。

4.9.14 一時停止の申請が認められる者

該当せず。

4.9.15 一時停止の申請手続き

該当せず。

4.9.16 一時停止の期間

該当せず。

4.10 証明書のステータス確認サービス

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

4.10.1 運用上の特性

該当せず。

4.10.2 サービスの可用性

該当せず。

4.10.3 その他の要件

該当せず。

4.11 加入（登録）の終了

加入者の証明書の利用が終了する事由は、加入契約書に定める。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、契約の解除を希望する場合、本 CPS「4.9.3 失効申請の手続」に基づき、本認証局へ証明書の失効申請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

該当せず。

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

該当せず。

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「5.1.8 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、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 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、審査業務で使用した書類等については、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

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。

5.1.9 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。

5.2 手続的管理

5.2.1 信頼される役割

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。

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、加入者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 および関連諸規程の教育のほか、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。

- 本 CPS、加入契約書および関連諸規程の変更時で、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
- 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
- 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 および関連諸規程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が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。

- 登録局による審査の記録
- 登録局および発行局が維持管理するシステム上の記録
- ネットワークセキュリティに関する記録
- 本施設の入退室に関する記録
- 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後の少なくとも 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「5.1.7 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

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

本認証局は、外部の専門家による脆弱性に関する評価を受け、当該脆弱性を是正するために必要な対応を行う。また、監査ログの検査により脆弱性が発見された場合についても、同様に必要な対応を行う。

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。

- ルート認証局の証明書
- 本認証局の証明書
- 加入者の証明書
- CRL
- 内部監査報告書
- 外部監査報告書
- 申請時に加入者より受理した書類・データ
- 本 CPS および関連諸規程

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後 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「5.1.7 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

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。本認証局および加入者の証明書については、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、認証局員、監査人および CTJ PA 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

本認証局は、加入者の証明書が有効である間に本認証局の証明書の有効期間が満了することなく、認証局の鍵ペアを更新する。

更新された本認証局の公開鍵が含まれる証明書は、サイバートラストの Web サイトに公開する。

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

本認証局は、本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。

- 危殆化した秘密鍵を用いた認証業務の停止
- すべての証明書の失効
- 危殆化の原因調査
- 是正処置案の策定ならびに CTJ PA による評価・承認
- 是正処置の実行
- 業務再開の妥当性の評価
- 新たな鍵ペアの生成および証明書の発行
- 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）
- 証明書の再発行

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。

5.7.2 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、バックアップ用のハードウェア、ソフトウェアまたはデータを用いて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、証明書の失効手続を行わなければならない。

本認証局は、本 CPS「4.9.3 失効申請の手続」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

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、事前に加入者に通知するほか、サイバートラストの Web サイトにおいても、その旨公開する。

本認証局が保有する加入者の情報については、廃棄もしくは業務移管先へ提供するものとし、この旨は業務終了時にサイバートラストの Web サイト上で告知される。

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

本認証局ならびにルート認証局で使用する鍵ペアは、それぞれ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。

本認証局ならびにルート認証局の鍵ペア生成の際には、それぞれ FIPS 140-2 レベル 4 の規格を満たした HSM の他、秘密分散の手法が用いられる。

本認証局ならびにルート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、本認証局の鍵ペアの生成が所定の手順に即し行われることを担保する。

6.1.2 加入者秘密鍵の配送

本認証局は、加入者に代わり加入者の秘密鍵を生成する場合、秘密鍵の機密性および完全性を確保する措置を講じたうえで、FIPS 140-2 レベル 2 以上の規格を満たした USB トークンを用いて、加入者へ秘密鍵を書留郵便等により、転送不要郵便物等として送付する。以後、本認証局は、当該加入者の秘密鍵を保持しない。

加入者が HSM により秘密鍵を生成する場合、本認証局はこれに関与せず、加入者の秘密鍵を配送しない。

6.1.3 認証局への加入者公開鍵の配送

加入者の公開鍵は、加入者に代わり加入者の秘密鍵を生成する場合、本認証局が生成する。

また、加入者が HSM により自らの秘密鍵を生成する場合には、加入者は、証明書発行要求データの中に公開鍵を含めたうえで、サイバートラストが提供する Web サイトより本認証局へ配送する。

6.1.4 信頼当事者への認証局公開鍵の配送

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、サイバートラストの Web サイトに公開する。

6.1.5 鍵長

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
Cybertrust iTrust Root Certification Authority	SHA2 with RSA	3072 bit

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
Cybertrust iTrust Signature Certification Authority	SHA2 with RSA	2048 bit

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。

証明書	署名方式	鍵長
加入者の証明書	SHA2 with RSA	2048 bit

6.1.6 公開鍵パラメーター生成および検査

該当せず。

6.1.7 鍵用途

本認証局の証明書の鍵用途（Key Usage）は、Certificate Signing 、CRL Signing とする。加入者の証明書の鍵用途（Key Usage）は、Digital Signature、Non Repudiation 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

本認証局ならびに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 4 の規格を満たした HSM とする。HSM 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）

本認証局ならびにルート認証局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

本認証局ならびにルート認証局は、本認証局ならびにルート認証局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

本認証局ならびにルート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。

6.2.5 秘密鍵のアーカイブ

本認証局ならびにルート認証局は、本認証局ならびにルート認証局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

本認証局ならびにルート認証局は、本認証局ならびにルート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。本認証局の 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。

6.2.7 暗号モジュール内での秘密鍵保存

本認証局ならびにルート認証局の秘密鍵は、本認証局の HSM 内で生成され、暗号化された上で保存される。

6.2.8 秘密鍵の活性化

本認証局ならびにルート認証局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

本認証局ならびにルート認証局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

本認証局ならびにルート認証局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

本認証局ならびにルート認証局は、本 CPS「6.2.1 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 証明書の有効期間と鍵ペアの有効期間

本認証局の証明書の最大有効期間は下表のとおりとする。

種別	秘密鍵	証明書
ルート認証局の証明書	指定しない	300 ヶ月以内とする。
本認証局の証明書	指定しない	120 ヶ月以内とする。
法人向け電子署名用証明書	指定しない	39 ヶ月以内とする。
個人向け電子署名用証明書	指定しない	39 ヶ月以内とする。

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

本認証局ならびにルート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

本認証局ならびにルート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。

- 操作者の権限の認証
- 操作者の識別と認証
- 重要なシステム操作に対する操作ログの取得
- 適切なパスワード設定および定期的な変更
- バックアップ・リカバリ

ルート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。

- 操作者の権限の認証
- 操作者の識別と認証
- 重要なシステム操作に対する操作ログの取得
- 外部ネットワークからの遮断（オフラインによる運用）と必要時以外のシステム停止

6.5.2 コンピュータセキュリティの評価

本認証局ならびにルート認証局は、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、重大な脆弱性が発見された場合には、速やかに必要な対応を行う。

6.6 ライフサイクル技術管理

6.6.1 システム開発管理

本認証局ならびにルート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

本認証局ならびにルート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、同システムのウィルス対策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、重大な脆弱性が発見された場合には、速やかに必要な対応を行う。

6.6.3 ライフサイクルセキュリティ管理

本認証局ならびにルート認証局は、本認証局ならびにルート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。

ルート認証局のシステムについては、外部とのネットワーク接続をせず、オフラインでの運用とする。

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 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

本認証局および加入者の証明書については、Appendix B に定める。

7.1.2 証明書拡張領域

本認証局および加入者の証明書については、Appendix B に定める。

7.1.3 アルゴリズムオブジェクト識別子

本認証局および加入者の証明書については、Appendix B に定める。

7.1.4 名前の形式

本認証局および加入者の証明書については、Appendix B に定める。

7.1.5 名称の制約

該当せず。

7.1.6 証明書ポリシーオブジェクト識別子

加入者の証明書については、1.2.392.200081.1.20.1 とする。

7.1.7 ポリシー制約拡張の使用

該当せず。

7.1.8 ポリシー修飾子の構文および意味

本認証局および加入者の証明書については、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

該当せず。

7.2 CRL のプロファイル

7.2.1 バージョン番号

本認証局および加入者の証明書については、Appendix B に定める。

7.2.2 CRL、CRL エントリ拡張

本認証局および加入者の証明書については、Appendix B に定める。

8. 準拠性監査およびその他の評価

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 Adobe Approved Trust List Technical Requirements の検証を年に一度行い、また、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

WebTrust for CA および Adobe Approved Trust List Technical Requirements 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、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

WebTrust for CA および Adobe Approved Trust List Technical Requirements については、これらのプログラムが定める範囲とする。

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

WebTrust for CA および Adobe Approved Trust List Technical Requirements の検証結果は、各規程の定めに従い、公開される。

9. その他の業務上および法的な事項

9.1 料金

本認証局が発行する証明書に関する料金および支払方法については、サイバートラストの Web サイト上、あるいは見積書等、加入者が適切に確認できる手段により通知する。なお、サイバートラストの Web サイト上の記載と、別途サイバートラストが提出した見積書等の記載との間に齟齬がある場合には、見積書等の記載が優先的に適用されるものとする。

また、本認証局は、証明書の発行後 30 日以内に加入者から以下の事由により、新規の証明書の発行を要請された場合、元の証明書を失効のうえ、無償で新規の証明書申請を受け付けるものとする。

- 送付した USB トークンが破損している等、納品物に瑕疵があった場合
- 本認証局が妥当な事由であると認めた場合

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。）。

- 加入者からの申請情報
- 本 CPS「9.4.2 個人情報として扱われる情報」に定める情報
- 加入者、信頼当事者、その他第三者より受けた問合せ情報
- 本認証局のセキュリティに関する情報

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。

- 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
- 加入者の証明書
- 本認証局の過失によらず公知となった情報
- 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
- 加入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

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、または加入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」に規定する。

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、証明書の発行および失効申請、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承認

本認証局は、加入者からの発行または失効申請をもって、本認証局が本 CPS で予定されている証明書発行・失効業務の履行および本認証局の監査の実施のために加入者の個人情報を使用することについて、加入者より同意を得たものとみなす。

また、本認証局は、加入者より得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。

- 本認証局が発行した証明書、証明書の失効情報
- 本 CPS および関連文書
- 本認証局の公開鍵および秘密鍵
- 本認証局から貸与されたソフトウェア、ハードウェア

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 認証局の表明保証

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。

- 認証局秘密鍵の安全な管理を行うこと
- 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
- CRL の発行および公開をもって失効情報を提供すること
- システムの監視および運用を行うこと
- 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

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。

- 本 CPS に基づく加入者の審査を行うこと
- 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
- 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。

- 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
- 証明書用途の遵守（本 CPS「1.4.1 適切な証明書の用途」）
- 公序良俗に反する電子文書で証明書を利用しないこと
- 証明書に含まれる情報の正確性に疑義が生じた場合は、当該疑義を解消するまで、証明書を使用しないこと
- 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
- 加入者が HSM により秘密鍵を生成する場合には、FIPS 140-2 レベル 2 以上の規格を満たした HSM により管理すること
- 法人向け電子署名用証明書については、法人向け電子署名用証明書に含まれる組織が作成した電子文書を署名するために使用し、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
- 個人向け電子署名用証明書については、個人向け電子署名用証明書に含まれる個人が作成した電子文書を署名するために使用し、かつ、加入契約書に従い、加入者個人の使途においてのみ証明書を使用すること
- 本 CPS「4.9.1.1 加入者による失効事由」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

- 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（本 CPS「4.9.12 鍵の危殆化に関する特別要件」）を行うこと
- 有効期間が満了した証明書および失効された証明書を使用しないこと
- 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。

- 証明書が本 CPS「1.4.1 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
- 本認証局が発行した証明書の有効期間と記載項目の確認を行うこと
- 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
- CRL により、証明書の失効の有無について確認を行うこと
- 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

該当せず。

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および加入者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。

- サイバートラストの本認証局が、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
- 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
- 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
- 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し生じた損害
- 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
- 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、証明書の申請、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、加入者がサイバートラストに支払済の金額または 10,000,000 円を超えない金額のいずれか低い額とする。

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、加入契約書および関連諸規程に基づく債務不履行、違反について生じる損害のうち、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

本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、自らのな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。

- 証明書の不正使用、改ざん、利用時の不実の表明
- 本 CPS または加入契約書への違反
- 加入者の秘密鍵保全の怠慢

また、本認証局は、加入者また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、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

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サイバートラスト所定の方法により通知がなされるものとする。なお、書面による通知の場合は、当該通知が郵送され、サイバートラストが受領した場合に到達したものとみなす。

9.12 改訂

9.12.1 改訂手続き

本認証局は、CTJ PA の指示に基づき、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

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、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 が別途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、その電子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

該当せず。

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

該当せず。

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

該当せず。

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、加入者または証明書の全部または一部を信頼し、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。
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。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。
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。
ルート認証局	本認証局の上位の認証局であり、本認証局の証明書を発行する。
DBA/Tradename	組織の法的名称以外の通称、商号、屋号、商標等を指す。
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 140-2 レベル 4	FIPS（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 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。
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。
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。
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。
PDF	情報の配布・交換・蓄積を電子的に行なうために用いられる電子文書で、Portable Document Format の頭文字を取ったものである。文書作成ソフトなどで作成した文書を PDF 形式に変換し利用する。閲覧には PDF リーダーを使用する。
Adobe Approved Trust List Technical Requirements	Adobe Approved Trust List（AATL：アドビ認定の信頼できるルート証明書の一覧）に登録されるために満たすことが要求されている技術要件である。
iTrust リモート署名サービス	サイバートラストが提供する書面の電子化や電子契約で求められる電子文書の長期間に渡る真正性を確保する長期署名に対応したクラウドサービスである。

Appendix B:証明書等のプロファイル

■Cybertrust iTrust Root Certification Authority（署名方式:SHA-2）

認証局証明書（有効期間:2018年2月 19 日～2043年2月 19 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（16 進数） 09 8e a5 03 20 ee 95 3b b7 b1 a4 88 4d 8c 6f d1 63 1f 8f c2
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 OrganizationIdentifer 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識別子 組織識別子のオブジェクト ID 型：OID 値：2.5.4.97 組織識別子の値 型：PrintableString 値：JCN3010401064771 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：Cybertrust iTrust Root Certification Authority	 2.5.4.6 JP 2.5.4.97 JCN3010401064771 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust iTrust Root Certification Authority
Validity		**値**
Validity notBefore	電子証明書の有効期間 開始日時	

	型：UTCTime 値：yymmddhhmmssZ	＊有効開始日時 180219060842Z (2018年2月19 日 15:08:42 JST)
notAfter	終了日時 型：UTCTime 値：yymmddhhmmssZ	＊有効終了日時 430219060842Z (2043 年2 月 19日 15:08:42 JST)
Subject		**値**
CountryName	電子証明書所有者の国名	
type	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
OrganizationIdentifer	電子証明書所有者の組織識別子	
type	組織識別子のオブジェクト ID 型：OID 値：2.5.4.97	2.5.4.97
value	組織識別子の値 型：PrintableString 値：JCN3010401064771	JCN3010401064771
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 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：Cybertrust iTrust Root Certification Authority	Cybertrust iTrust Root Certification Authority
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	3072Bit 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	f1 6a 5a 3b 9b 60 80 69 8f 1a d6 1d 9b 50 36 63 fa f0 45 06
certificatePolicies （extnId :== 2 5 29 32，critical :== FALSE)		**値**
PolicyInformation	ポリシーに関する情報	
policyIdentifier	型：OID 値：1.2.392.200081.1.20.1	1.2.392.200081.1.20.1
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/itrust/repository/index.html	 https://www.cybertrust.ne.jp/itrust/repository/index.html
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：発行者の subjectPublicKey の Hash 値	 f1 6a 5a 3b 9b 60 80 69 8f 1a d6 1d 9b 50 36 63 fa f0 45 06
keyUsage （extnId :== 2 5 29 15，critical :== TRUE）		**値**
KeyUsage	鍵の使用目的 型：BitString 値：00000110 （keyCertSign, cRLSign）	 00000110（0x0006）
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（CA である） パス長の制約 型：INTEGER 値：2	 TRUE 2

■ARL

（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-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	CRL 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	 2.5.4.6 JP
OrganizationIdentifer type value	CRL 発行者の組織識別子 組織識別子のオブジェクト ID 型：OID 値：2.5.4.97 組織識別子の値 型：PrintableString 値：JCN3010401064771	 2.5.4.97 JCN3010401064771
OrganizationIdentifer type value	CRL 発行者の組織識別子 組織識別子のオブジェクト ID 型：OID 値：2.5.4.97 組織識別子の値 型：PrintableString 値：JCN3010401064771	 2.5.4.97 JCN3010401064771
OrganizationName type Value	CRL 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.	 2.5.4.10 Cybertrust Japan Co., Ltd.
CommonName type value	CRL 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 Cybertrust iTrust Root Certification Authority	 2.5.4.3 Cybertrust iTrust Root Certification Authority
ThisUpdate		**値**
ThisUpdate	CRL の発行日時 型：UTCTime 値：yymmddhhmmssZ	 180219062956Z
NextUpdate		**値**
NextUpdate	次回 CRL の更新予定日時 型：UTCTime	 （ThisUpdate＋9131 日後）

	値：yymmddhhmmssZ	430219062956Z

（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	 f1 6a 5a 3b 9b 60 80 69 8f 1a d6 1d 9b 50 36 63 fa f0 45 06
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

（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

■Cybertrust iTrust Signature Certification Authority（署名方式：SHA-2）

認証局証明書（有効期間：2018 年 2 月 20 日～2028 年 2 月 20 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（16 進数） 72 4a bf c5 ea 71 1a 5b 7a 64 52 26 34 3b fd ab 3a d9 07 7f
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-256) 型：OID 値：1 2 840 113549 1 1 11	 1.2.840.113549.1.1.11
parameters	暗号アルゴリズムの引数 型：NULL 値：	 NULL
Issuer		**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 型：PrintableString 値：JP	 2.5.4.6 JP
OrganizationIdentifer type value	電子証明書発行者の組織識別子 組織識別子のオブジェクト ID 型：OID 値：2.5.4.97 組織識別子の値 型：PrintableString 値：JCN3010401064771	 2.5.4.97 JCN3010401064771
OrganizationName type value	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.	 2.5.4.10 Cybertrust Japan Co., Ltd.
CommonName Type value	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：Cybertrust iTrust Root Certification Authority	 2.5.4.3 Cybertrust iTrust Root Certification Authority
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 180220061215Z (2018年 2月 20日 15:12:15 JST) ＊有効終了日時 280220061215Z

		(2028 年2 月20 日 15:12:15 JST)
Subject		**値**
CountryName	電子証明書所有者の国名	
type	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
OrganizationIdentifer	電子証明書所有者の組織識別子	
type	組織識別子のオブジェクト ID	
	型：OID	
	値：2.5.4.97	2.5.4.97
value	組織識別子の値	
	型：PrintableString	
	値：JCN3010401064771	JCN3010401064771
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	
	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 ：Cybertrust iTrust Signature Certification Authority	Cybertrust iTrust Signature Certification Authority
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）

cRLDistributionPoints (extnId :== 2 5 29 31，critical :== FALSE）		**値**
cRLDistributionPoints	CRL 配布ポイント	
DistributionPoint	CRL 配布ポイント	
uniformResourceIdentifie	URI	
	型：OctetString	
	値 ： http://crl.itrust.ne.jp/CybertrustiTrustRootCA/cdp.crl	http://crl.itrust.ne.jp/CybertrustiTrustRootCA/cdp.crl
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	e9 53 9f 51 b0 1e 13 38 ac 7b 6c 28 05 e0 47 52 49 ef ba ce
certificatePolicies （extnId :== 2 5 29 32，critical :== FALSE）		**値**
PolicyInformation	ポリシーに関する情報	
policyIdentifier	型：OID	

	値：1.2.392.200081.1.20.1	1.2.392.200081.1.20.1
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/itrust/repository/index.html	https://www.cybertrust.ne.jp/itrust/repository/index.html
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	f1 6a 5a 3b 9b 60 80 69 8f 1a d6 1d 9b 50 36 63 fa f0 45 06
keyUsage （extnId :== 2 5 29 15，critical :== TRUE）		**値**
KeyUsage	鍵の使用目的 型：BitString 値：00000110 (keyCertSign,cRLSign)	00000110 (0x0006)
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
PathLenConstraint	パス長の制約 型：INTEGER 値：1	1

■法人向け電子署名用証明書

（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（ユニークな整数）
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 OrganizationIdentifer 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識別子 組織識別子のオブジェクト ID 型：OID 値：2.5.4.97 組織識別子の値 型：PrintableString 値：JCN3010401064771 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　：Cybertrust iTrust Signature Certification Authority	 2.5.4.6 JP 2.5.4.97 JCN3010401064771 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust iTrust Signature Certification Authority
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 ＊有効終了日時
Subject		**値**
CountryName 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	2.5.4.6
value	国名の値 型：PrintableString 値：JP	＊所有者の国名
OrganizationIdentifer	電子証明書所有者の組織識別子	
type	組織識別子のオブジェクト ID 型：OID 値：2.5.4.97	2.5.4.97
value	組織識別子の値 型：PrintableString 値：	＊所有者の組織識別子
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》	＊所有者の会社名称
OrganizationUnitName	電子証明書所有者の部署名	＊必要な場合のみ
type	部署名のオブジェクト ID 型：OID 値：2.5.4.11	2.5.4.11
value	部署名の値 型：PrintableString / UTF8String 値：《所有者の登録商標、部署、サービス名称等》	＊所有者の登録商標、部署、サービス名称等
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 / UTF8String 値：《所有者の固有名称、または所有者の固有名称に加え、所有者の登録商標、部署、サービス名称等を含む》	＊所有者の固有名称、または所有者の固有名称に加え、所有者の登録商標、部署、サービス名称等を含む
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

（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（CA でない）	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：1.2.392.200081.1.20.1	1.2.392.200081.1.20.1
policyQualifiers	ポリシーに関する情報	
policyQualifierID	policyQualifiers の種別 型：OID 値：userNotice のオブジェクト ID	1.3.6.1.5.5.7.2.2

Qualifier	(id-qt-unotice) テキストによる声明 型：OctetString 値： https://www.cybertrust.ne.jp/itrust/repository/index.html	https://www.cybertrust.ne.jp/itrust/repository/index.html
authorityInfoAccess (extnId :== 1 3 6 1 5 5 7 1 1，critical :== FALSE）		**値**
Authority Information Access Caissuers	認証局情報アクセス 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://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt	1.3.6.1.5.5.7.48.2 http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt
keyUsage （extnId :== 2 5 29 15，critical :== TRUE）		**値**
KeyUsage	鍵の使用目的 型：BitString 値：11000000 （digitalSignature, nonRepudiation）	11000000（0x00C0）
extendedKeyUsage (extnId :== 2.5.29.37，critical :== FALSE）		**値**
extendedKeyUsage	拡張鍵用途 型：OID 値：1.3.6.1.5.5.7.3.4 型：OID 値：1.3.6.1.5.5.7.3.3	1.3.6.1.5.5.7.3.4（emailProtection） 1.3.6.1.5.5.7.3.3（codeSigning）
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：発行者の subjectPublicKey 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://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl	http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/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

■個人向け電子署名用証明書（組織属性なし）

（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（ユニークな整数）
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 OrganizationIdentifer 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識別子 組織識別子のオブジェクト ID 型：OID 値：2.5.4.97 組織識別子の値 型：PrintableString 値：JCN3010401064771 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　：Cybertrust iTrust Signature Certification Authority	 2.5.4.6 JP 2.5.4.97 JCN3010401064771 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust iTrust Signature Certification Authority
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 ＊有効終了日時
Subject		**値**
CountryName 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	2.5.4.6
value	国名の値	
	型：PrintableString	
	値：《所有者の国名》	＊所有者の国名
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 / UTF8String	
	値：《所有者の氏名》	＊所有者の氏名
GivenName	電子証明書所有者の名	
type	名のオブジェクト ID	
	型：OID	
	値：2.5.4.42	2.5.4.42
value	名の値	
	型：PrintableString / UTF8String	
	値：《所有者の名》	＊所有者の名
Surname	電子証明書所有者の姓	
type	姓のオブジェクト ID	
	型：OID	
	値：2.5.4.4	2.5.4.4
value	姓の値	
	型：PrintableString / UTF8String	
	値：《所有者の姓》	＊所有者の姓
SerialNumber	電子証明書所有者の固有識別番号	
type	固有識別番号のオブジェクト ID	
	型：OID	
	値：2.5.4.5	2.5.4.5
value	固有識別番号の値	
	型：PrintableString	
	値：《所有者の固有識別番号》	＊所有者の固有識別番号
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

（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（CA でない）	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：1.2.392.200081.1.20.1	1.2.392.200081.1.20.1
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/itrust/repository/index.html	https://www.cybertrust.ne.jp/itrust/repository/index.html
authorityInfoAccess (extnId :== 1 3 6 1 5 5 7 1 1，critical :== FALSE）		**値**
Authority Information Access Caissuers	認証局情報アクセス 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://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt	1.3.6.1.5.5.7.48.2 http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt
keyUsage （extnId :== 2 5 29 15，critical :== FALSE）		**値**
KeyUsage	鍵の使用目的 型：BitString 値：11000000 （digitalSignature, nonRepudiation）	11000000（0x00C0）
extendedKeyUsage (extnId :== 2.5.29.37，critical :== FALSE）		**値**
extendedKeyUsage	拡張鍵用途 型：OID 値：1.3.6.1.5.5.7.3.4 型：OID 値：1.3.6.1.5.5.7.3.3	1.3.6.1.5.5.7.3.4（emailProtection） 1.3.6.1.5.5.7.3.3（codeSigning）
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：発行者の subjectPublicKey の Hash 値	
subjectAltName （entnID :== 2 5 29 17，critical :== FALSE）		**値**
subjectAltName directoryName	電子証明書所有者代替名 ディレクトリ名 型：UTF8String （但し、c のみ PrintableString) 値：”c=JP, s=電子証明書所有者住所（都道府県）, l=電子証明書所有者住所（市区町村名）, ou=電子証明書所有者生年月日（西暦）, cn=電子証明書所有者氏名”	c=JP s=”所有者住所（都道府県名）” l=”所有者住所（市区町村名、町名、番地）” ou=”所有者生年月日(西暦)” cn=”所有者氏名”
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://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl	http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/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

■個人向け電子署名用証明書（組織属性あり）

（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（ユニークな整数）
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 OrganizationIdentifer 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識別子 組織識別子のオブジェクト ID 型：OID 値：2.5.4.97 組織識別子の値 型：PrintableString 値：JCN3010401064771 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 ：Cybertrust iTrust Signature Certification Authority	 2.5.4.6 JP 2.5.4.97 JCN3010401064771 2.5.4.10 Cybertrust Japan Co., Ltd. 2.5.4.3 Cybertrust iTrust Signature Certification Authority
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 ＊有効終了日時
Subject		**値**
CountryName	電子証明書所有者の国名	

Type	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：《所有者の国名》	＊所有者の国名
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 / UTF8String 値：《所有者の氏名》	＊所有者の氏名
GivenName	電子証明書所有者の名	
type	名のオブジェクト ID 型：OID 値：2.5.4.42	2.5.4.42
value	名の値 型：PrintableString / UTF8String 値：《所有者の名》	＊所有者の名
Surname	電子証明書所有者の姓	
type	姓のオブジェクト ID 型：OID 値：2.5.4.4	2.5.4.4
value	姓の値 型：PrintableString / UTF8String 値：《所有者の姓》	＊所有者の姓
SerialNumber	電子証明書所有者の固有識別番号	
type	固有識別番号のオブジェクト ID 型：OID 値：2.5.4.5	2.5.4.5
value	固有識別番号の値 型：PrintableString 値：《所有者の固有識別番号》	＊所有者の固有識別番号
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

（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（CA でない）	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：1.2.392.200081.1.20.1	1.2.392.200081.1.20.1
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/itrust/repository/index.html	https://www.cybertrust.ne.jp/itrust/repository/index.html
authorityInfoAccess (extnId :== 1 3 6 1 5 5 7 1 1，critical :== FALSE）		**値**
Authority Information Access Caissuers	認証局情報アクセス 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://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt	1.3.6.1.5.5.7.48.2 http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cisca.crt
keyUsage （extnId :== 2 5 29 15，critical :== FALSE）		**値**
KeyUsage	鍵の使用目的 型：BitString 値：11000000 （digitalSignature, nonRepudiation）	11000000（0x00C0）
extendedKeyUsage (extnId :== 2.5.29.37，critical :== FALSE）		**値**
extendedKeyUsage	拡張鍵用途 型：OID 値：1.3.6.1.5.5.7.3.4 型：OID 値：1.3.6.1.5.5.7.3.3	1.3.6.1.5.5.7.3.4（emailProtection） 1.3.6.1.5.5.7.3.3（codeSigning）
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：発行者の subjectPublicKey の Hash 値	
subjectAltName （entnID :== 2 5 29 17，critical :== FALSE）		**値**
subjectAltName directoryName	電子証明書所有者代替名 ディレクトリ名 型：UTF8String 値：”o=加入者が所属する組織の名称, OID.2.5.4.97=加入者が所属する組織の組織識別子, s=加入者が所属する組織の住所（都道府県名）, l=加入者が所属する組織の住所（市区町村名、町名、番地）, ou=加入者が所属する組織の部署名, t=加入者が所属する組織においての役職名”	o=”加入者が所属する組織の名称” OID.2.5.4.97=”加入者が所属する組織の組織識別子” s=”加入者が所属する組織の住所（都道府県名）” l=”加入者が所属する組織の部署名” ou=加入者が所属する組織の部署名 t=加入者が所属する組織においての役職名
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://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/cdp.crl	http://crl.itrust.ne.jp/CybertrustiTrustSignatureCA/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

■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	CRL 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	 2.5.4.6 JP
OrganizationIdentifer type value	CRL 発行者の組織識別子 組織識別子のオブジェクト ID 型：OID 値：2.5.4.97 組織識別子の値 型：PrintableString 値：JCN3010401064771	 2.5.4.97 JCN3010401064771
OrganizationName type value	CRL 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：UTF8String 値：Cybertrust Japan Co., Ltd.	 2.5.4.10 Cybertrust Japan Co., Ltd.
CommonName type value	CRL 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：UTF8String 値 ：Cybertrust iTrust Signature Certification Authority	 2.5.4.3 Cybertrust iTrust Signature Certification Authority
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	 ＊更新予定日時

（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	e9 53 9f 51 b0 1e 13 38 ac 7b 6c 28 05 e0 47 52 49 ef ba ce
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

(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