サイバートラスト

Registration Practices Statement
（登録局運用規程）

※注意
サイバートラスト株式会社の“Registration Practices Statement（登録局運用規程）Version 1.01”の記載は、概ね以下の内容です。
以下の内容はあくまでも参考としての翻訳内容であり、効力を有する契約・運用規程は、原文の英語文の契約・運用規程となります。サイバートラスト株式会社は、原文の契約と比した本訳の内容の正確性を保証せず、本訳と原文の契約・運用規程の内容の違い等に基づく一切の責を負いません。
なお、サイバートラスト株式会社は、登録局運用規程の同一 Version に対し、修正した和訳版を日付を更新して提供する場合があります。また、新しい Version の登録局運用規程の原文が公開された場合には、本書の参照・利用を中止してください。予めご了承の上、ご参照ください。

バージョン 1.01
2017年3月24日

サイバートラスト株式会社
107-6030
東京都港区赤坂 1-12-32
アーク森ビル 30 階

目次

1. 初めに

1.1. 概要

本文書は、 DigiCert Inc.の証明書発行サービスへのサイバートラストによる参加に関する原則および運用実務の概要を定めたサイバートラストの登録局運用規程（Registration Practices Statement：RPS）である。本 RPS は、サイバートラストを通じて電子証明サービスを取得する全ての当事者に適用される。

サイバートラストの実務は、パブリック証明書の発行に参加する際、CA/ブラウザフォーラム（以下「CAB フォーラム」という）が現在採用している現行バージョンのガイドライン（Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates（以下「Baseline Requirements」という）および Guidelines for Extended Validation Certificates（以下「EV ガイドライン」という）を含む）に準拠しており、これらは、https://www.cabforum.org から閲覧できる。SSL/TLS サーバー証明書またはコード署名証明書については、本 RPS と Baseline Requirements または EV ガイドラインとの間に齟齬が生じた場合には、EV 証明書については EV ガイドラインが優先し、パブリック SSL 証明書については Baseline Requirements が優先する。

本 RPS は、サイバートラストの証明書発行サービスについて規定する複数の文書のうちの1つに過ぎない。その他の重要な文書には、関連する CP、サイバートラストと顧客との間の契約書、信頼当事者規約、適用あるプライバシーポリシーなどの私的文書および公的文書が含まれる。サイバートラストは、追加的な証明書ポリシーまたは認証局運用規程を提供することがある。これらの補足的なポリシーおよび規程は、それらの適用を受けるユーザーまたは信頼当事者に対して提供される。

本 RPS は、IETF PKIX RFC 3647CP/CPS フレームワークに従って9つのパートで構成され、証明書発行およびタイムスタンプサービスのサイバートラストの部分に関するセキュリティ管理並びに運用実務および手続きについて記述している。RFC 3647 の規定のアウトラインを維持するため、該当しないセクションについては、見出し部分に「該当せず」または「規定なし」との表示が付されている。

1.2. 文書名と識別

本 RPS は、サイバートラストの登録局運用規程（Registration Practices Statement）であり、サイバートラスト Policy Authority から当初 2017 年 2 月 9 日に発行の承認を受けている。

日付	変更	Version
2017 年 2 月 17 日	失効申請の手続きを更新	1.01

1.3. PKI の関係者

1.3.1. 認証局

サイバートラスト は、電子証明書を発行する 認証局 （CA）を運営している DigiCert のための登録局である。CA として、DigiCert は、全ての適切な書類および通信を CTTJ から受領した後、公開鍵オペレーションに関係する機能を果たす。

1.3.2. 登録局および他の委託先第三者

サイバートラスト は、DigiCert PKI に参加する登録局である。DigiCert は、証明書要求および/またはエンドユーザー証明書のための本人確認および認証の実行の権限等、一定の機能の実行を登録局 （RA）としてのサイバートラストに委託した。サイバートラスト RA は、証明書発行、管理、失効またはその他の関連業務におけるサイバートラストの役割に適用される CP に基づき運営される。

1.3.3. 加入者

加入者は、取引およびコミュニケーションをサポートするために証明書発行サービスを使用する。加入者は、常に証明書上で身元が識別された当事者であるとは限らない（例えば、証明書が組織の従業員に発行されている場合など）。証明書の *サブジェクト*は、証明書で指定されたエンティティである。本 RPS 上、*加入者*とは、証明書のサブジェクトおよび証明書発行についてサイバートラスト と契約を交わしたエンティティの両方を意味する。本人確認および証明書発行の前であれば、加入者とは *申請者*を意味する。

1.3.4. 信頼当事者

信頼当事者は、サイバートラストの確認する証明書および/または電子署名を信頼して行為するエンティティを意味する。信頼当事者は、証明書に記述された情報に依拠する前に適切な CRL または OCSP レスポンスを確認しなければならない。CRL 配布点のロケーションについては、証明書に詳細が示されている。

1.3.5. その他の関係者

規定なし

1.4. 証明書の用途

電子証明書（または*証明書*）は、識別された加入者を暗号方式で公開鍵と結び付けるフォーマットされたデータという。電子証明書は、電子取引に携わる組織が、かかる取引の他の当事者に対し、その本人性を証明することを可能にする。電子証明書は、商環境において ID カードに相当するものとして使用される。

1.4.1. 適切な証明書の用途

本 RPS に基づき発行された証明書は、その証明書の鍵用途および拡張鍵用途のフィールドで指定された通り、全ての法的認証、暗号化、アクセス制御、および電子署名の目的で使用することができる。ただし、処理または保護される情報の機密性は証明書ごとに大幅に異なるため、各信頼当事者は、本 RPS に基づき発行された証明書を使用するか否かを決定する前に、アプリケーション環境および関連するリスクを評価しなければならない。

本 RPS は、保証レベルの異なる幾つかの種類のエンドエンティティ証明書/トークンについて扱っている。その各々についての適切な用途の簡単な説明が下表に示されている。下表の記述は、ガイダンスのみを目的とするものであり拘束力を持たない。

証明書	適切な用途
OV SSL 証明書	データ暴露のリスクおよび影響が中程度の場合のオンラインコミュニケーションのセキュリティで保護に使用する（相当の金銭的価値または不正行為のリスクを有する、または、悪意あるアクセスの可能性が相当程度存在する場合における個人情報へのアクセスを含む取引を含む）。
EV SSL 証明書	データ暴露のリスクおよび影響が高い場合のオンラインコミュニケーションのセキュリティで保護に使用する。（金銭的価値または不正行為のリスクの高い取引、個人情報へのアクセスを含み悪意あるアクセスの可能性が高い取引を含む）。
コード署名証明書（EV コード署名を含む）	証明書に名前の記された加入者の身元を確認し、署名されたコードが署名後変更されていないことを証明する。
基礎的レベル 1 クライアント証明書：個人	個人の身元について最低レベルの保証を行う。一般的に、署名された情報についてデータの完全性を保証する目的にのみ使用。このタイプの証明書は、悪意あるアクティビティのリスクが低く、認証された取引が必要とされない場合にのみ使用するべきである。
レベル 1 クライアント証明書：企業	データ暴露のリスクおよび影響が存在するが、かかるリスクが重大なものでない環境で使用する。ユーザーが悪意である可能性は低いものと仮定される。
レベル 2 クライアント証明書	身元の審査された個人に発行される証明書で、名前が仮名である場合にはその旨が示される。データ暴露のリスクおよび影響が存在するが、かかるリスクが重大なものでない環境で使用する。ユーザーが悪意である可能性は低いものと仮定される。
レベル 3 クライアント証明書	データ暴露のリスクおよび影響が中程度の環境で使用する（金銭的価値または不正行為のリスクが相当ある取引、個人情報へのアクセスを含み悪意あるアクセスの可能性が相当ある取引を含む）。
レベル 4 クライアント証明書	データ暴露のリスクおよび影響が高い環境で使用する（金銭的価値または不正行為のリスクの高い取引、個人情報へのアクセスを含み悪意あるアクセスの可能性が高い取引を含む）。
認証のみ	証明書所有者の身元は関連性がなく、安全なサイトへの無許可のアクセスのリスクが低い場合に使用する。

1.4.2. 禁止される証明書の用途

証明書は、サブジェクトについての商取引における信用性、誠実性、および評判、法令順守、取引相手としての安全性を保証するものではない。証明書は、そこに記された情報が証明書発行の時点において合理的に正確なものとして検証されたことを立証するのみである。コード署名証明書は、署名されたコードが安全にインストールできること、または、かかるコードにマルウェア、バグ、または脆弱性が存在しないことを示すものではない。

1.5. ポリシー 管理

1.5.1. 文書を管理する組織

本 RPS およびその文中で言及される文書は CTJ PA により維持管理されており、CTJ PA の連絡先情報は以下の通りである。

住所:
CTJ Policy Authority
サイバートラスト株式会社
日本
107-6030
東京都港区赤坂 1-12-32
アーク森ビル 30 階
+81 3-6234-3800

1.5.2. 連絡窓口

宛先: Policy Authority
CTJ Policy Authority
サイバートラスト株式会社
日本
107-6030
東京都港区赤坂 1-12-32
アーク森ビル 30 階
+81 3-6234-3800

お問い合わせおよび苦情の連絡は以下の通り

・本 RPS に関するお問い合わせ ・証明書の申請方法および技術的なお問い合わせ	digicert_support@cybertrust.ne.jp
・失効要求および失効要求の方法に関するお問い合わせ ・証明書に問題が生じた場合や不正利用など ・その他証明書に関する苦情など	evc-report@cybertrust.ne.jp

1.5.3. RPS のポリシー適合性を決定する者

CTJ PA は、独立した監査人（セクション 8 参照）の監査結果および勧告に基づき、本 RPS の適合性および適用性を判断する。CTJ PA は、準拠性監査の結果を評価しそれに対応する責任も負う。

1.5.4. RPS の承認手続き

CTJ PA は、本 RPS およびその変更を承認する。変更は、CP とかかる変更との整合性を CTJ PA がレビューした上で、RPS 全体の改訂または補遺の公表により行われる。CTJ PA は、本 RPS への変更が CP に準拠しているか、通知または OID 変更を必要とするかを判断する。

1.6. 定義と略語

1.6.1. 定義

「関連組織（Affiliated Organization）」とは、加入者と組織的な関連があり、証明書上にかかる関連性を表示することを承認その他許容する組織を意味する。

「申請者（Applicant）」とは、証明書を申請するエンティティを意味する。

「CAB フォーラム（CAB Forum）」は、セクション 1.1.で定義された意味を持つ。

「証明書(Certificate)」とは、公開鍵とアイデンティティを関連付けるために電子署名を用いる電子文書を意味する。
「証明書承認者 (Certificate Approver)」は、EV ガイドラインで規定された意味を持つ。

「証明書要求者(Certificate Requester)」は、EV ガイドラインで規定された意味を持つ。

「契約署名者（Contract Signer）」は、EV ガイドラインで規定された意味を持つ。

「EV ガイドライン（EV Guidelines）」は、 セクション 1.1.で定義される。

「鍵ペア（Key Pair）」とは、（公開鍵暗号方式における）秘密鍵およびそれに関連する公開鍵のペアを意味する。

「OCSP レスポンダー（OCSP Responder）」とは、サイバートラストの権限の下で運用され、証明書ステータス確認要求を処理するため当社のリポジトリに接続するオンラインソフトウェアアプリケーションを意味する。

「秘密鍵（Private Key）」とは、（公開鍵暗号方式の）一組の鍵ペアのうち、その鍵ペアの所有者が秘密を保持する鍵で、電子署名の生成および/または対応する公開鍵により暗号化された電子記録またはファイルの復号化のために用いられる鍵を意味する。

「公開鍵（Public Key）」とは、（公開鍵暗号方式の）一組の鍵ペアのうち対応する秘密鍵の所有者が公開できる鍵で、所有者が対応する秘密鍵を用いて生成した電子署名を信頼当事者が検証する目的および/又その所有者の対応する秘密鍵によってのみ復号化できるようメッセージを暗号化する目的で使用される。

「信頼当事者（Relying Party）」とは、証明書または タイムスタンプトークンに含まれる情報に依拠するエンティティを意味する。

「信頼当事者規約（ Relying Party Agreement）」とは、証明書の確認、証明書への依拠、若しくは証明書の使用、または、サイバートラストリポジトリへのアクセスもしくはその使用に先立って、信頼当事者が読み同意する必要のある規約を意味する。

「加入者（Subscriber）」とは、証明書のサブジェクトとして識別されたエンティティを意味する。

「加入者契約（Subscriber Agreement）」とは、証明書の発行および使用について定めており、証明書の発行を受ける前に申請者が読み同意する必要のある規約を意味する。

1.6.2. 略語:

AATL	Adobe Approved Trust List（アドビ認定の信頼できるルート証明書の一覧）
CA	Certificate Authority（証明書認証局）または Certification Authority（認証局）
CAB	CA/Browser （CA/ブラウザ）（例えば「CAB Forum （CAB フォーラム）」のように用いる。）
CP	Certificate Policy（証明書ポリシー）
CPS	Certification Practice Statement （認証局運用規程）
CRL	Certificate Revocation List （証明書失効リスト）
CSR	Certificate Signing Request（証明書署名要求）
DBA	Doing Business As （～の通称で営業）、Trading As（～の商号で営業）とも言う。
CTJ PA	サイバートラスト Policy Authority （CTJ Policy Authority）
EV	Extended Validation（拡張認証）
FIPS	（US Government） Federal Information Processing Standard （米国連邦情報処理標準）
FQDN	Fully Qualified Domain Name (完全に指定されたドメイン名)

HSM	Hardware Security Module（ハードウェア・セキュリティ・モジュール）
HTTP	Hypertext Transfer Protocol（ハイパー・テキスト・ランスファー・プロトコル）
IANA	Internet Assigned Numbers Authority（インターネット・アサインド・ナンバーズ・オーソリティ）
ICANN	Internet Corporation for Assigned Names and Numbers（インターネット・コーポレーション・フォー・アサインドネームズ・アンド・ナンバーズ）
IDN	Internationalized Domain Name（国際化ドメイン名）
ISSO	Information System Security Officer（情報システムセキュリティ責任者）
IETF	Internet Engineering Task Force（インターネット・エンジニアリング・タスクフォース）
ITU	International Telecommunication Union（国際電気通信連合）
ITU-T	ITU Telecommunication Standardization Sector（ITU 電気通信標準化部門）
OCSP	Online Certificate Status Protocol（オンライン証明書ステータスプロトコル）
OID	Object Identifier（オブジェクト識別子）
OV	Organization Validated （組織認証）
PIN	Personal Identification Number（個人識別番号、例えば秘密のアクセスコード等）
PKI	Public Key Infrastructure（公開鍵基盤）
PKCS	Public Key Cryptography Standard（RSA セキュリティにより考案され公開された公開鍵暗号標準）
RA	Registration Authority（登録局）
RFC	Request for Comments（IETF による技術仕様公開形式）
SHA	Secure Hashing Algorithm（安全なハッシュアルゴリズム）
SAN	Subject Alternative Name （サブジェクトの別名）
SSL	Secure Sockets Layer（セキュア・ソケット・レイヤー）
TLD	Top-Level Domain （トップレベルドメイン）
TLS	Transport Layer Security（トランスポート・レイヤー・セキュリティー）
URL	Uniform Resource Locator（ユニフォーム・リソース・ロケータ）
UTC	Coordinated Universal Time（協定世界時）
X.509	証明書およびそれらに対応する認証フレームワークについての ITU-T 標準

1.6.3. レファレンス

CA/ブラウザフォーラムのパブリック証明書発行/管理のための証明書ポリシー基本要件（CA Brouser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates（以下「Baseline Requirements」という）
CB/ブラウザフォーラムの EV 証明書発行/管理のためのガイドライン（CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates（以下「EV ガイドライン」という）

2. 公開とリポジトリの責任

2.1. リポジトリ

殆どのサイバートラストサービスについてのリーガルリポジトリは、https://www.digicert.ne.jp/repository/上に公開されている。

CRL および OCSP レスポンスのレポジトリは、ダウンタイム削減のためセクション 5 に記載されたシステムのオンラインリソースを通じて 1 日 24 時間週 7 日利用可能である。

2.2. 認証情報の公開

証明書発行サービスおよびリポジトリには、以下の連絡手段でアクセスできる。

1. ウェブ上：https://www.digicert.ne.jp/（および証明書に記された URI）
2. 電子メール宛先：digicert_support@cybertrust.ne.jp
3. 郵送先住所：サイバートラスト、サイバートラスト株式会社、日本、107-6030、東京都港区赤坂 1-12-32、アーク森ビル 30 階
4. 電話番号：+81 3-6234-3800
5. ファックス番号：1-801-705-5296

2.3. 公開の時期と頻度

本 RPS についての新バージョンまたは変更は、通常、承認から 7 日以内に公開される。

2.4. リポジトリへのアクセスコントロール

リポジトリへの読み取り専用アクセスの制限は行わない。リポジトリへの無許可の書き込みアクセスは、論理的制御および物理的制御により防止される。

3. 識別および認証

3.1. 名前の決定

3.1.1. 名称のタイプ

証明書は、ITU の X.500 標準に準拠した NULL でないサブジェクトの Distinguished Name（DN）を用いて発行される。ただし、critical のフラグのついた alternative name の形式が少なくとも 1 つ含まれる場合、レベル 1 証明書は NULL であるサブジェクトの DN を含むことがある。DN が使用される場合、コモンネームは名前空間の一意性を尊重しなければならず、誤解を招くものであってはならない。ただし、仮名での証明書の使用を妨げるものではない。幾つかの SSL/TLS 証明書（インターネット上での使用のための証明書およびマルチ SAN 証明書を含む）では、一般の利用者が依拠することを目的としない subject alternative name 拡張子が含まれることがある（例えば、「.local」などの標準外のトップレベルドメインが含まれる場合または RFC1918 によりプライベートアドレスに割り当てられた IP アドレス空間のアドレスを含む場合など）。これらのローカル IP アドレスまたは非-FQDN（但し、DNS による名前解決が可能な形式の）サーバー名についてのパブリック SSL 証明書の発行は、廃止される予定である。サイバートラストは、EV ガイドラインの Appendix F に従って、.onion ドメインに対する EV SSL/TLS 証明書の発行を授権することができる。

3.1.2. 名称の意味に関する要件

サイバートラストは、証明書のサブジェクトであるエンティティ（即ち、人、組織、デバイス、またはオブジェクト）および証明書の発行者であるエンティティの両方を識別する識別名を使用する。 サイバートラスト は、組織の構造を正確に反映するディレクトリ情報ツリーのみを許容する。

3.1.3. 加入者の匿名・仮名についての要件

一般にサイバートラストは匿名または仮名での証明書を許容しない。ただし、サイバートラスト は IDN について IDN の Puny コード（ピュニコード）バージョンをサブジェクト名として含めることを授権する場合がある。サイバートラストはまた、その他の仮名でのエンドエンティティ証明書を授権することもある（ただし、かかる発行がポリシーにより禁止されておらず該当する名前空間の一意性要件に適合していることを条件とする）。

3.1.4. 様々な名称形式を解釈するためのルール

証明書上の識別名は、X.500 標準および ASN.1 syntax を用いて解釈される。証明書上の X.500 識別名がどのように Uniform Resource Identifiers（ニフォームリソースアイデンティファイア）および HTTP リファレンスとして解釈されるかの詳細については、RFC2253 および RFC2616 を参照。

3.1.5. 名称の一意性

証明書上の各サブジェクト名についての一意性の確保は以下のように実施される。

SSL サーバー証明書	証明書にドメイン名を含める。ドメイン名の一意性は、ICANN（the Internet Corporation for Assigned Names and Numbers）により管理されている。
クライアント証明書	一意性のある電子メールアドレスまたは一意性のある組織名と一意性のある serial/integer 型データとの組み合わせ/関連付けが必要とされる。
IGTF およびグリッド限定デバイス証明書	デバイス証明書については、FQDN が適切なフィールドに記される。その他の証明書について、サイバートラストは一意性のある ID を証明書に記された名前に付加する場合がある。
コード署名証明書（CDS 証明書を含む）	一意性のある組織名およびアドレス、または一意性のある組織名と一意性のある serial/integer 型データとの組み合わせ/関連付けが必要とされる。

3.1.6. 商標等の認識、認証および役割

加入者は、他のエンティティの知的財産権を侵害するコンテンツを含む証明書の発行を要求することはできない。

OSU サーバー証明書については、Hotspot 2.0 CP のセクション 4.1.7 に従って、サイバートラストはロゴおよびフレンドリーネームについて、特定の商標に関する申請者の使用権を確認するため、米国特許商標庁（U.S.Patent and Trademark Office）または世界知的所有権機関（World Intellectual Property Organization: WIPO）などの該当する標章登録データベースで商標検索を行う。サイバートラストは、かかる検索の結果に基づき、RFC 3709 および Hotspot 2.0 CP のセクション 3.4 に従って、単数または複数のロゴタイプ拡張（サービスプロバイダーに関連するハッシュアルゴリズムおよびハッシュ値を記したもの）を含む OSU サーバー証明書を発行する。申請者の利用可能なフレンドリーネームまたはロゴがない場合、サイバートラストは、Wi-Fi アライアンスが指定するロゴおよびフレンドリーネームを含めることができる。

本 RPS に別段の具体的規程がある場合を除き、サイバートラストは、商標についての申請者の使用権を認証せず、商標紛争の解決も行わない。サイバートラストは、商標紛争の一部となっている証明書については、申請の拒否または失効の要求を行うことができる。

3.2. 初回の本人性確認

サイバートラストは、組織または個人である申請者の本人性を確認するため、全ての法律的な通信または調査の手段を使用することができる。サイバートラストは、当社の単独の裁量において、証明書の発行を拒否することができる。

3.2.1. 秘密鍵の所有を確認する方法

サイバートラストは、署名検証を行うことにより、または電子署名されたとされるまたは秘密鍵で暗号化されたとされるデータを証明書要求に関連する公開鍵を用いて復号化することにより、申請者が公開鍵に対応する秘密鍵を所有または管理していることを立証する。

3.2.2. 組織の認証

SSL サーバー証明書（ドメイン認証）	サイバートラスト又はそのパートナーは、申請者がドメイン名の使用または管理を行う権利について Baseline Requirements により許容される手続き（以下を含む）のうち 1 つ以上を用いて認証する。 1. ドメイン名レジストラから公的に入手可能な記録（例えば、WHOIS またはその他の DNS 記録情報）への依拠 2. 以下の電子メールアドレスとの通信 webmaster@domain.com administrator@dmain.com admin@domain.com hostmaster@domain postmaster@domain （または、そのドメインのレジストラ記録の技術、登録、管理についての連絡窓口のフィールドに記載されたその他のアドレス。） 3. 認知されたディレクトリを用いたドメイン管理の実際のデモンストレーションの要求
	4. ドメイン承認レターの提出（ただし、かかるレターは証明書要求日またはそれ以後の日付で、ドメイン保有者の資格を有する代表者が署名し、承認済みの完全に指定されたドメイン名のリスト、および当該ドメイン名を証明書上で使用する権利を申請者に付与する旨を記したものでなければならない。更に、サイバートラスト は、ドメイン承認レターの真正性を確認するため信頼できる第三者データ情報源を用いてドメイン名保有者に連絡する。）および/または

	5. 申請者によるそのドメイン名の所有、管理および使用権保有について同等のレベルの保証を提供する手続きで、Baseline Requirements に基づき許容される、上記に類するもの サイバートラスト は、(a)国により (i)ウェブサイトについての DNS レコードにより表示されるそのウェブサイトの IP アドレス、または (ii) 申請者の IP アドレスについて割り当てられた IP アドレスレンジ、(b) 要求されるドメイン名の TLD 、または (c) ドメイン名レジストラから提供された情報を用いて、そのドメイン名に含まれる国コードを検証する。
SSL サーバー証明書 （作成認証）	サイバートラストは、申請者が証明書に記載されるドメイン名の使用または管理を行う権利について、前述のドメイン認証手続きを用いて認証する。 サイバートラストはまた、以下の方法で申請者の身元および住所を確認する。 1. 信頼できる第三者/政府機関のデータベースまたはその組織の法律上の設立、存続、および認定を管轄する団体または所轄機関との連絡 2. サイト訪問 3. 会計士、弁護士、政府機関職員その他の信頼できる第三者が署名した認証レター、または 4. 住所の場合に限り：公共料金請求書、銀行取引明細書、クレジットカード取引明細書、税務書類その他の信頼できる本人確認の形式
EV SSL および EV コード署名証明書	EV 証明書の発行に関連する組織の身元に関する情報は、EV ガイドラインに従って認証される。
レベル 1 クライアント証明書	サイバートラストは、 当社が SSL サーバー証明書を発行する前に、ドメインに対する組織の所有権を認証する手続きと同様の認証手続きを用いて電子メールドメインについての組織的管理を認証する。
レベル 2、3、および 4 のクライアント証明書	証明書に組織情報が含まれる場合、サイバートラストは、その個人と証明書に名称の記される組織との関連性を確認するために十分なドキュメンテーションを組織から入手する。

不正行為のリスクが高い可能性のある証明書申請について警告するためのスコアリングシステムが利用される。これらの証明書申請には、「高リスク」のフラグが表示され、証明書発行の前に追加的な精査または検証が行われる（申請者からの追加的文書の入手または申請者との追加的な連絡を含む。）

3.2.3. 個人の認証

証明書に個人の身元が記される場合、サイバートラストは、以下の手続きにより個人の身元を認証する。

証明書	認証手続き
SSL サーバー証明書およびオブジェクト署名証明書（個人に発行されるもの）	1. サイバートラストは、政府機関の発行した写真付 ID（パスポート、運転免許証、軍隊 ID、国家 ID、またはこれらに類する文書）で現在有効なもの少なくとも1点の判読可能な写し（申請者の顔を明らかに表示しているもの）を入手する。サイバートラストは、かかる写しに変更または改ざんの可能性が示されていないかを検査する。 2. サイバートラストは、申請者の名前および住所について、利用

証明書	認証手続き
	可能な第三者データ情報源との整合性を追加的に照合確認することがある。 3. 更に保証が必要とされる場合、申請者は本人確認を行えるもの（最近の公共料金請求書、金融機関の口座明細書、クレジットカード、追加的な ID クレデンシャル、またはこれらに類するもの）を追加的に提出しなければならない。 4. サイバートラストは、申請者が電話、郵便/クーリエ、またはファックスにより連絡可能であることを確認する。 サイバートラストが上記の手続きにより申請者の身元を確認できない場合、申請者は身元宣言書（信頼されるエージェント、公証人、弁護士、会計士、郵便事業者または身元確認を行う権限を有するものとして州または国の政府機関により認定されたその他の団体が証人として署名したもの）を提出しなければならない。
OSU サーバー証明書	サイバートラストは、要求者が組織の従業員、パートナー、メンバー、代理人等としてその組織を代表する正当な資格を有する者であることおよびその組織を代表して行為する権限を有していることを検証する。
EV 証明書 （事業体に発行されるもの）	EV ガイドラインに記載の通り
認証限定証明書	安全なロケーションを管理するエンティティは、証明書所有者がそのロケーションへのアクセスを許可されているとの表明を行わなければならない。
レベル 1 クライアント証明書：個人 （電子メール証明書）	サイバートラストが、証明書に記された電子メールアドレスまたはウェブサイトの申請者による管理を確認する。
レベル 1 クライアント証明書：企業	以下のいずれかの方法による。 1. 登録局または信頼されるエージェントにおいて本人確認を行う担当者のもとに本人が出向き、直接対面で身元を証明できるもの（例えば、運転免許証または出生証明書）を提示する。 2. 消費者信用の申請時に使用される手続きと同様の手続きにより、消費者信用データベースまたは政府機関の記録を用いて以下の事柄を確認する。 a. 一定の電話番号からの通話発信およびその番号での通話受信が行えること b. 既知の物理アドレスに送信されたメールを受け取れること 3. クレデンシャルプロバイダーまたは取引先企業（例えば、金融機関、航空会社、雇用主、または小売事業者など）との継続中の取引関係に由来する情報を通じて以下の事柄を確認する。 a. かかる取引関係上使用されている請求先住所において郵便物を受け取れること b. 以前の取引（例えば、過去の注文番号）において確認された情報の検証 c. 過去の取引で使用された電話番号からの通話発信およびその番号での通話受信が行えること 4. レベル 2、3、または 4 のクライアント証明書について申請者の本人確認に使用されるその他全ての方法
レベル 2 クライアント証明書	RA は、以下の項目について、申請と整合性があることおよび一意性のある個人を特定する目的上、十分であることを確認する。 (a) 以下各号に関連して参照される政府機関発行の写真付 ID 上の名前 (b) 生年月日、および (c) 現住所または個人電話番号

証明書	認証手続き
	1. 登録局または信頼されるエージェント（または身元確認を行う権限を有するものとして州、連邦、または国の機関により認定されたその他の団体）において本人確認を行う担当者のもとに本人が出向き、直接対面で政府機関が発行した現在有効な信頼できる形式の写真付 ID を提示する。 2. 申請者は、政府機関発行の現行かつ有効な写真付 ID を保持していなければならない。本人確認を行う登録局または信頼されるエージェントは、申請者について以下の情報を入手しレビューしなければならない（リモート検証により行うこともできる）：(i) 氏名、生年月日、および現住所または電話番号、(ii)最重要な政府機関発行写真付 ID に割り当てられたシリアル番号、および（iii）追加的に本人確認を行えるもの１点（例えば、別の種類の政府機関発行の ID、従業員証/学生証の ID カード番号、電話番号、金融口座（例えば、当座預金口座、普通預金口座、ローンカードまたはクレジットカード）の番号、または申請者の居住地と一致する住所の公共料金口座（例えば、電気、ガス、水道等）の番号。リモート 検証による本人確認は、データベースを提供するエージェント/機関との記録確認または信用調査機関その他これらに類するデータベースに依拠して行うことができる。
	サイバートラストは、記録のアドレスを確認する形式でクレデンシャルを発行すること、または申請者のアドレスにおける最近のアカウントアクティビティの履歴を検証することによりアドレスを確認することがある。また、電話番号については、チャレンジ/レスポンス SMS テキストメッセージの送信、または（サイバートラストが入手可能な記録で申請者に関連する電話番号を特定した上で）申請者との通話中に申請者の声を録音することにより確認することがある。 3. サイバートラストと申請者との間に現行かつ継続中の関係が存在する場合、以前に交信された共有秘密の交信（例えば、PIN またはパスワードで、NIST SP 800-63 レベル 2 エントロピー要件に適合するかそれ以上のもの）を通じて本人確認を行うことができる。ただし (a)上記 1 または 2 で求められる政府機関発行の写真付 ID を用いた確認と同等の厳格さで当初の本人確認が行われたことおよび(b) 申請者が共有秘密を引き続き保有していることを確認するために十分な関係が継続的に存在していることを条件とする。 4. サイバートラストの レベル 3 または 4 のクライアント証明書について申請者の本人確認に使用されるその他全ての方法
レベル 3 クライアント証明書	本人がサイバートラスト、信頼されるエージェント、または身元確認を行う権限を有するものとして州、連邦、または国の機関により認定されたその他の団体に出向いて直接対面で身元証明を行う。情報は、安全な方法で収集し保管しなければならない。本人確認には、連邦/国の政府機関が発行した有効期限内の写真付 ID（例えば、パスポート）、REAL ID1点、または非連邦政府機関発行の有効な ID2 点（うち一方は写真付が必要とされる。許容される形式の政府機関発行 ID には、運転免許証、州発行の写真付 ID カード、パスポート、国家 ID カード、永住者カード、トラステッドトラベラーカード、部族 ID、軍隊 ID、またはこれらに類する写真付 ID 書類が含まれる。USCIS Form I-9 を参照。

証明書	認証手続き
	本人確認を行う担当者は、クレデンシャル（身元識別情報）を審査し、それらが真正かつ有効期限内であるかを判断し、提供された情報（氏名、生年月日、および 現住所）の正当性を確認するためチェックする。申請者は、以下に定義された身元宣言書に署名し、本人確認を行う担当者が同宣言書に証明の署名を付す。サイバートラストまたは RA は、身元宣言書をレビューしその記録を保管する。 また、サイバートラスト は、直接対面身元確認要件を満たすため、直接対面身元確認の補完的先例（FBCA Supplementary Antecedent, In-Person Definition （FBCA 補完的先例、イン・パーソンの定義）で定義されたプロセス）も用いる。この定義の下では、以下の条件が満たされる場合には、過去の身元確認の先例で十分である。(1)前述の直接対面本人確認の完全性と厳格さに適合し、(2)先例による関係を立証するための裏付けを行う ID 証明アーチファクトが存在すること、および (3)主張された身元と個人を関連付けるメカニズムが設けられていることを条件とする。使用例の 1 つとしては、申請者（例えば従業員）は、雇用主が過去に USCIS Form I-9 を用いて身元確認を行っており、既知の属性又は共有秘密の使用を通じてアサートされた身元と遠隔で関連付けられる場合がある。別の例としては、サイバートラストは複数の過去の身元確認先例データベースに基づき リアルタイムで「5 問プロセス（five-question process）」を構築する第三者の身元確認サービスプロバイダーを用い、申請者は 2 分以内に 5 問のうち少なくとも 4 問に正しく答えることを求められる場合がある。「FBCA Supplementary Antecedent, In-Person Definition（FBCA 補完的面会、イン・パーソンの定義）」を参照。 申請者の身元は、当初の証明書発行に先立ち、かかる発行日の 30 日前より後に確認しなければならない。
レベル 4 クライアント証明書（生体 ID 証明書）	本人がサイバートラスト、信頼されるエージェント、または身元確認を行う権限を有するものとして州、連邦、または国の機関により認定されたその他の団体に出向いて直接対面で身元証明を行う。認定された団体は、収集した情報を安全な方法で直接サイバートラストに転送しなければならない。申請者は、連邦/国の政府機関が発行した有効期限内の写真付 ID（例えば、パスポート）1 点、REAL ID1 点、または非連邦政府機関発行の有効な ID2 点（うち一方は写真付 ID でなければならない）を提出しなければならない。許容される形式の政府機関発行 ID には、運転免許証、州発行の写真付 ID カード、パスポート、国家 ID カード、永住者カード、トラステッドトラベラーカード、部族 ID、軍隊 ID、またはこれらに類する写真付 ID 書類が含まれる。USCIS Form I-9 を参照。また、クレデンシャルを収集する団体は、申請者が申請を否認できないよう保証するために、少なくとも1つの形態の生体データ（例えば、写真または指紋）を入手しなければならない。 サイバートラストのために本人確認を行う者は、クレデンシャルの真正性および有効性を審査する。 申請者は、以下に定義された身元宣言書に署名し、本人確認を行う担当者が同宣言書に証明の署名を付す。サイバートラストは、身元宣言書をレビューし、その記録を保管する。 直接対面の先例の使用は許容されない。申請者の身元は、当初の証明書発行に先立ち、かかる発行日の 30 日前より後に直接対面により確認しなければならない。レベル 4 クライアント証明書は、申請者の住

証明書	認証手続き
	所が確認できる方法で発行される。

身元宣言書は、以下の内容により構成される。

1. 本人確認を行う者の身元
2. 加入者の身元を必要とされる通り検証した旨を本人確認実行者が 28 U.S.C. 1746 に定められたフォーマット（不実記載における罰則および偽証罪の適用に関する事項を確認の上で宣言するフォーマット）で宣言し署名を付したもの（かかる宣言には直筆または（発行されるクレデンシャルのレベルと同等以上の証明書を用いた）電子署名を付すことができる。）、または現地法の下でこれに相当する手続き
3. 申請者の本人確認資料から得られた一意性のある識別番号またはかかる本人確認資料のファクシミリ
4. 本人確認の日付
5. 申請者が、本人確認を行う者の面前で、28 U.S.C. 1746 に定められたフォーマット（不実記載における罰則および偽証罪の適用に関する事項を確認の上で宣言するフォーマット）で身元を宣言し署名したもの（かかる宣言には直筆または（発行されるクレデンシャルのレベルと同等以上の証明書を用いた）電子署名を付すことができる。）、または現地法の下でこれに相当する手続き

直接対面の本人確認が求められるが、申請者が対面登録を単独で行えない場合（例えば、申請者がネットワークデバイス、未成年者、または法的無能力者であるなど）、PKI により既に認証された者または申請者が申請したものと同種の証明書に必要な身元クレデンシャルを有する者が申請者に同行することができる。申請者に同行する者（即ち「スポンサー」）は、要求される証明書のレベルでの登録に十分な情報をスポンサー自身および申請者について提示する。

レベル 3 およびレベル 4 についての面前本人確認の場合、サイバートラストは本人性確認を行う権限を有するものとして州、連邦、または国の機関により認定されたエンティティを頼ることができ、かかるエンティティは RA のために認証を行うことができる。認定されたエンティティは、申請者から収集した情報を安全な方法で直接 RA に転送しなければならない。

3.2.3.1. 役割に基づくクライアント証明書の認証

証明書は、加入者の具体的役割を特定することができる。ただし、かかる役割が、ある組織内の特定の個人（例えば、*最高情報責任者（Chief Information Officer）*は一意性のある個人であるが、*プログラムアナリスト*はこれに該当しない。）を識別するものであることを条件とする。これらの役割ベース証明書は、否認防止が求められる場合に使用される。サイバートラスト は、要求される役割ベース証明書と同等以上の保証レベルの個人加入者証明書を初めに取得した加入者に対してのみ役割ベース証明書を発行する。同一の役割についての証明書が複数の加入者に発行されることができる。ただし、各証明書は固有の鍵ペアを有しなければならない。発行された役割ベース証明書を複数の個人で共有することはできず、かかる証明書の発行を受けた個人は、役割ベース証明書を個人証明書と同様の方法で保護することが要求される。

サイバートラストは、役割ベース証明書を発行する前に、役割ベース証明書を要求する個人（スポンサー）の本人性をセクション 3.2.3 に従い認証する。スポンサーは、該当する役割ベース証明書と同等かより高い保証レベルの DigiCert が発行したクライアント個人証明書を有していなければならない。証明書が、仮名による証明書で FBCA と相互認証され、サブジェクトを組織的役割により識別するものである場合、サイバートラストは、その役割にある個人またはその役割を代表して署名する権限を有する個人について認証を行う。

本 RPS は、役割ベース証明書の発行について、適用ある CP の鍵生成、秘密鍵の保護、および加入者の義務に関する全ての条項を遵守するものとする。

3.2.3.2. グループ クライアント 証明書の認証

いくつかのエンティティが単一の資格で行為している場合で、否認防止が必要でない場合、グループ証明書（複数の加入者により共有される秘密鍵に対応する証明書）が許容される。これらの証明書のスポンサーは、組織内で少なくとも情報システムセキュリティ責任者（Information Systems Security Officer：ISSO）またはそれと

同等以上の役職者でなければならない。

スポンサーは、秘密鍵の管理を保証する責任を負う。スポンサーは、秘密鍵にアクセスできる加入者のリストを維持して継続的に更新し、各加入者がその秘密鍵を制御できる期間を把握していなければならない。グループ証明書は、個人の身元の一覧をサブジェクト名 DN に記載することができる（ただし、サブジェクトはグループであり単独の個人でないことを証明書が特定できるよう、サブジェクト名 DN フィールドに「ダイレクトグループ証明書」等の文字列も含まれることを条件とする）。このような方法で組織に発行されたクライアント証明書は、常にグループクライアント証明書であるとみなされる。

3.2.3.3. 人間のスポンサーをもつデバイスおよびの認証

レベル 1、2、3、または 4 のクライアント証明書は、そのデバイスを所有するエンティティがサブジェクトとして記される場合に発行される。いかなる場合も、人間であるスポンサーがデバイスについて以下の情報を提供しなければならない。

1. 機器の識別情報（シリアル番号等）または サービス名（DNS 名等）
2. 機器の公開鍵
3. 機器認証および属性（それらを証明書に含める場合）
4. 連絡窓口

証明書のスポンサーが変更された場合、新たなスポンサーは、各デバイスが引き続き証明書を受ける資格を有していることを確認するため各デバイスのステータスをレビューする。各スポンサーは、要請に応じてそのデバイスが引き続きそのスポンサーの管理および責任の下にあるとの証拠を提出するよう求められている。スポンサーは、当該機器が使用されなくなった場合、そのスポンサーの管理または責任の下になくなった場合、または証明書を必要としなくなった場合には、サイバートラストに通知するよう契約上義務付けられている。全ての登録は、要求される証明書の種類に応じて認証される。

3.2.4. 確認しない加入者情報

レベル 1 - 個人クライアント証明書は、電子メールにより認証される。コモンネームは加入者の法律上の氏名として認証されない。サイバートラストは、加入者が合法的に所有または管理していないドメイン名または IP アドレスに対しては、SSL 証明書の発行を授権しない。サイバートラストは完全に指定されたドメイン名を構成するものとして加入者が示したホスト名またはサーバー名を信頼することができる。証明書に含まれる他の確認されない情報については、そのように各証明書で指定されている。サイバートラストは、加入者の組織単位（OU）に記載されている情報の真正性と正確性を検証しません。

3.2.5. 権限の確認

証明書要求の権限を以下の通り確認する。

証明書	認証手続き
SSL サーバー証明書	証明書要求は、Baseline Requirements に従い信頼できるコミュニケーション手段を用いて確認される。
OSU サーバー証明書	サイバートラストは、要求者が組織の従業員、パートナー、メンバー、代理人等としてその組織を代表する正当な資格を有する者であることおよびその組織を代表して行為する権限を有していることを検証する。
EV 証明書	証明書要求は、EV ガイドラインに従って確認される。
オブジェクト署名証明書およびAdobe 署名証明書	証明書に組織の名前が記される場合、信頼できるコミュニケーション手段を用いて申請者の組織内の正式な情報源に要求者の連絡先情報を確認する。その後、かかる連絡先情報は、証明書要求の真正性を確認するために使用される。

証明書	認証手続き
レベル 1 クライアント証明書：個人（電子メール証明書）	証明書に記された電子メールアドレスを用いて、証明要求を確認する。
レベル 1 クライアント証明書：企業（電子メール証明書）	証明書要求を、証明書に記されるドメインおよび電子メールアドレスを技術上および運営上管理する者に確認する。
レベル 2、3、および 4 のクライアント証明書 PIV-I 証明書	個人が証明書を取得する資格を有することを、証明書に名称の記される組織がサイバートラストに対して確認する。 かかる組織は、その個人と同組織との関連性が消滅した場合には、証明書の失効を申請するよう求められている。

組織は、サイバートラストに要求を行うことにより証明書要求を行う資格を有する者を限定することができる。資格を有する個人を限定する要求は、サイバートラストにより承認されるまで効力を発揮しない。サイバートラストは、組織が、資格を有する要求者のサイバートラスト側のリストを求める場合、組織による認証済みの要求については、これに応じる。

3.3. 鍵（証明書）更新申請時の本人性確認と認証

3.3.1. 鍵（証明書）定期更新時の本人性確認と認証

加入者は、証明書の期限切れに先立って、その証明書についての鍵更新を要求することができる。鍵更新は、（新しい公開鍵と（オプションで）延長された有効期間以外は）以前と同じ証明書コンテンツで新しい証明書を生成する。証明書の有効期間を延長する際、サイバートラストは申請者について再認証を行うことがあるが、以前に提供されまたは取得した情報に依拠する場合もある。

加入者は、自らの身元の再認証を以下の通り行う。

証明書	通常の鍵更新	再認証の必要頻度
非 EV SSL サーバー証明書	ユーザー名およびパスワード	少なくとも 39ヶ月毎
EV SSL 証明書	ユーザー名およびパスワード	EV ガイドラインに従って
加入者 EV コード署名証明書	ユーザー名およびパスワード	少なくとも 39ヶ月毎
署名権限 EV コード署名証明書	ユーザー名およびパスワード	少なくとも 123ヶ月毎
加入者 EV コード署名証明書	ユーザー名およびパスワード	少なくとも 123ヶ月毎
オブジェクト署名証明書（Adobe 署名証明書を含む）	ユーザー名およびパスワード	少なくとも 6 年毎
レベル 1 クライアント証明書	ユーザー名およびパスワード	少なくとも 9 年毎
レベル 2 クライアント証明書	現行の署名鍵または NIST SP 800-63 レベル 3 に適合するマルチファクター 認証	少なくとも 9 年毎
レベル 3 およびレベル 4 クライアント証明書	現行の署名鍵または NIST SP 800-63 レベル 3 に適合するマルチファクター認証	少なくとも 9 年毎
認証限定証明書	ユーザー名およびパスワードまたは関連する秘密鍵	無し

追加の認証を行わなければ上記の制限を超えた証明書の使用が加入者にとって可能になる場合には、追加認証なしで証明書についての鍵更新を行うことは許容されない。

3.3.2. 証明書失効後の鍵更新における本人性確認と認証

証明書が更新、アップデート、または変更行為以外の何らかの理由で失効処理された場合、加入者は、証明書についての鍵更新を受ける前に当初の登録手続きを再び経なければならない。

3.4. 失効申請時の本人性確認と認証

サイバートラスト は、全ての失効申請について認証を行う。サイバートラストは、関連する秘密鍵が危殆化しているか否かに関わらず、証明書の公開鍵を参照し失効申請を認証することができる。

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

申請者または申請者のために証明書の申請を行う資格を有する個人は、証明書申請を提出することができる。申請者またはその代理人がサイバートラストに提供する全てのデータについては、申請者が責任を負う。

EV 証明書申請は、資格を有する証明書要求者が提出し証明書承認者により承認されなければならない。証明書要求には、契約署名者の（書面または電子形式による）署名を付した加入契約を添付しなければならない。

経済産業省より輸出禁止の行政処分を受けているエンティティに対しては、証明書の発行を行わない。

4.1.2. 申請手続きおよび責任

特に順番はないが、申請手続きには以下のプロセスが含まれる。

1. 証明書申請の提出
2. 鍵ペアの生成
3. 鍵ペアの公開鍵の交付
4. 該当する加入契約への同意
5. 該当する手数料の支払

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

証明書申請を受領後、サイバートラストが申請情報その他の情報をセクション 3.2.に従って確認する。当初の認証過程で、サイバートラスト又はそのパートナーは、CAA レコードの存在について DNS をチェックする。サイバートラストを認証された CA として CAA レコードに記載されていない場合、サイバートラストは、かかる CAA レコードに関わらず申請者が証明書発行を許可していることを確認する。検証の完了後、サイバートラストは全資料の情報を評価し、証明書を発行するか否かを判断する。評価の一環として、疑わしい証明書申請を特定する目的で、以前に失効した証明書および却下した証明書申請の社内データベースと（申請された）証明書の照合が含まれる。

サイバートラスト は、第三者情報源が合理的に信頼できるか否かを判断する上で、かかる情報減の利用可能性、目的、および評判を検討する。サイバートラストは、当社のみが情報源である場合には、そのデータベース、情報源、または身元証明の形式を合理的に信頼できるものとは判断しない。

4.2.2. 証明書申請の承認または却下

サイバートラストは、当社が証明書申請を認証できない場合、その証明書申請を却下する。また、サイバートラストは、証明書の発行がサイバートラスト又は DigiCert の評判または事業に損害を与えまたはこれらを損なう可能性があると判断した場合に、証明書申請を却下することがある。

企業 EV 証明書を除き、EV 証明書発行の承認は、別々のサイバートラスト認証スペシャリスト 2 名が行う必要がある。第 2 の認証スペシャリストは、文書を収集し EV 証明書の当初の承認を行う者と同一の個人であってはならない。 第 2 の認証スペシャリストは、いかなる不一致および更に説明を要する内容などについて、収集された情報および文書をレビューする。第 2 の認証スペシャリストは、証明書の発行を許可する前に追加的な説明および文書を要求することがある。企業である RA は、本 RPS の定める最終的な相互相関関係のチェックと

デューデリジェンスをその企業 RA を代表する単一の個人により行うことができる。十分な説明および/または追加文書を合理的な期間内に受領しない場合、サイバートラストは EV 証明書要求を却下し、申請者にその旨を通知する。

証明書申請が却下されず本 RPS に従って正常に認証された場合、サイバートラストは証明書申請を承認し証明書を発行する。サイバートラストは、却下された証明書申請について責任を負わず、その理由を開示する義務を負わない。却下された申請者は再度申請を行うことができる。加入者は、証明書を使用する前に証明書のコンテンツの正確性をチェックする必要がある。

4.2.3. 証明書申請の処理に要する時間

通常、サイバートラストは合理的な期間内に申請者の情報を認証し電子証明書を発行する。発行の処理時間は、認証を完了するために必要な詳細および文書をいつ申請者が提出するかによって大幅に左右される。通常サイバートラストは、非 EV SSL 証明書については、必要な詳細および文書を申請者から全て受領した後 2 営業日以内に認証プロセスを完了する。ただし、サイバートラストの管理の及ばない事象により発行プロセスに遅れが生じる可能性もある。

4.3. 証明書の発行

4.3.1. CA における証明書発行処理

サイバートラスト は、証明書の発行前に証明書の要求元を確認する。発行の完了後、証明書はデータベースに保存され加入者に交付される。

4.3.2. CA による加入者に対する証明書の発行通知

サイバートラスト は、発行後合理的な時間内に証明書をセキュリティ保護された何らかの方法で交付することができる。一般的に、サイバートラストは、加入者が申請手続の過程で指定した電子メールアドレス宛てに証明書を電子メールで送信する。

4.4. 証明書の受領

4.4.1. 証明書の受領確認手続

加入者は、発行された証明書のコンピュータまたはハードウェア・セキュリティ・モジュールへのインストールにつき全責任を負う。証明書は、証明書の発行から 30 日後または、それ以前の証明書使用時に加入者が証明書を使用した証拠が存在する場合、受領されたものとみなされる。

4.4.2. CA による証明書の公開

エンドエンティティ証明書については、加入者に交付することにより公開される。

4.4.3. CA による他の関係者に対する証明書発行の通知

サイバートラストが証明書発行の通知を受ける。

4.5. 鍵ペアと証明書の利用

4.5.1. 加入者による秘密鍵および証明書の利用

加入者は、自らの秘密鍵を無許可の使用または開示から保護し、関連する証明書の期限が切れた後またはかかる証明書が失効した後は秘密鍵の使用を中止し、証明書を意図された目的に従って使用することを契約上義務付けられている。

4.5.2. 信頼当事者による加入者の公開鍵と証明書の使用

信頼当事者は、X.509、IETF RFC、およびその他の適用される標準に準拠したソフトウェアのみを使用することができる。サイバートラストは、本 RPS に記載された管理方法および要件を第三者ソフトウェアがサポートするとの保証は行わない。

信頼当事者は、自らの裁量で証明書に依拠するべきであり、証明書を信頼する前に状況と損失リスクの全体を考慮しなければならない。状況が追加的保証の必要性を示している場合には、信頼当事者は証明書を使用する前にかかる保証を得なければならない。提供される保証は、信頼当事者による依拠が合理的なものであり、適用ある信頼当事者規約を信頼当事者が順守している場合にのみ有効である。

信頼当事者は、以下の全てに該当する場合にのみ、電子署名または SSL/TLS ハンドシェイクを信頼するべき

である。

1. 電子署名または SSL/TLS セッションが有効な証明書の運用期間中に生成され、有効な証明書を参照することにより検証可能である。
2. 証明書が失効しておらず、信頼当事者は証明書を使用する前に関連する CRL または OCSP レスポンスを参照することにより証明書の失効ステータスを確認済みである。
3. 証明書は、意図された目的のために本 RPS に従って使用されている。

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更新が行われる場合

サイバートラスト は、以下の場合に証明書更新を要請することができる。

1. 関連する公開鍵の有効期間が終了していない。
2. 加入者と属性が整合的である。
3. 関連する秘密鍵が危殆化していない。

サイバートラストは、証明書の有効期限の前に加入者に対して通知する。証明書の更新には、追加料金の支払いが必要となる。

4.6.2. 証明書の更新申請が認められる者

証明書サブジェクトまたは証明書サブジェクトの資格を有する代表者のみが加入者の証明書更新要求を行うことができる。サイバートラストは、署名証明書の鍵更新の場合には、対応する要求が無い場合でも新しい証明書を発行することができる。

4.6.3. 証明書更新申請の処理

更新申請の要件および手続きは、一般的に証明書の当初の発行の際に使用されるものと同様である。サイバートラストは、以前に認証された情報の再使用を単独裁量で選択できる。ただし、セクション 3.3.1.で特定された期間より古い情報については再取得を行う。サイバートラストは、再確認した情報を認証できない場合、証明書の更新を拒否することができる。個人がクライアント証明書を更新する場合で、関連する情報に変更がなければ、サイバートラストは追加的な本人確認を要求としない。幾つかのデバイスプラットフォーム（例えば、Apache など）では、秘密鍵の更新後の使用が許容される。秘密鍵およびドメイン情報に変更がない場合、加入者は以前に発行された証明書または以前に提供した CSR を用いて、SSL 証明書を更新することができる。

4.6.4. 更新された証明書の発行に関する加入者への通知

サイバートラストは、証明書を何らかのセキュリティ保護された方法で交付することができる。通常、電子メール、または加入者にユーザーID/パスワードで保護された（加入者がログインして証明書をダウンロードできる）ロケーションへのハイパーテキストリンクを提供することによって行う。

4.6.5. 更新された証明書の受領確認手続き

更新された証明書は、証明書の更新から 30 日後または、それ以前の証明書使用時に加入者が証明書を使用した証拠が存在する場合、受領されたものとみなされる。

4.6.6. CA による更新された証明書の公開

更新された証明書は、これを加入者に交付することにより公開される。

4.6.7. CA による他の関係者に対する証明書の発行通知

サイバートラストは、更新された証明書発行の通知を受ける。

4.7. 鍵更新を伴う証明書の更新

4.7.1. 証明書の鍵更新を行う場合

証明書の鍵更新は、新しい公開鍵とシリアル番号を持ち、以前と同じサブジェクト情報の新しい証明書を生成することによる。新しい証明書は、有効期限、鍵識別子、CRL および OCSP 配布ポイント、および署名鍵が異なる場合がある。鍵更新を要求する加入者は、セクション 3.3.1.で認められた通り、本人確認および認証を受けなければならない。

4.7.2. 証明書の鍵更新申請が認められる者

サイバートラスト は、証明書サブジェクトまたは PKI スポンサーからの鍵更新要求のみを受理する。サイバート

ラストは、証明書サブジェクトの要求またはサイバートラスト自身の裁量により証明書の鍵更新を開始することができる。

4.7.3. 証明書の鍵更新申請の処理

サイバートラスト は、証明書サブジェクトまたは PKI スポンサーからの鍵更新要求のみを受理する。秘密鍵並びに証明書上の身元およびドメインの情報が変わっていない場合、サイバートラストは以前に発行された証明書または以前に提供された CSR を用いて差し換えの証明書を発行するよう要請することができる。サイバートラストは、再検証および認証がセクション 3.3.1 に基づき必要とされる場合、または情報が不正確になっているとサイバートラストが判断した場合以外は、既存の認証情報を再使用する。

4.7.4. 鍵更新された証明書の発行に関する加入者への通知

サイバートラスト は、証明書の発行から合理的な期間内に加入者に通知する。

4.7.5. 鍵更新された証明書の受領確認手続き

鍵更新された証明書は、証明書の鍵更新から 30 日後、またはそれ以前の証明書使用時加入者が証明書を使用した証拠が存在する場合、受領されたものとみなされる。

4.7.6. 鍵更新された証明書の CA による公開

鍵更新された証明書は、これを加入者に交付することにより公開される。

4.7.7. CA から他のエンティティに対する鍵更新された証明書の発行通知

サイバートラストは、証明書鍵更新の通知を受ける。

4.8. 証明書の変更

4.8.1. 証明書の変更を行う場合

証明書の変更とは、同一のサブジェクトについて古い証明書と認証情報がわずかに異なる（例えば、電子メールアドレスの変更、名前または属性の重要でない部分の変更など）新しい証明書を発行することを意味する。ただし、変更がそれ以外の点で本 RPS に従っていることを条件とする。新しい証明書のサブジェクト公開鍵は前と同じ場合もあれば異なる場合もある。

4.8.2. 証明書変更申請が認められる者

サイバートラスト は、一定の証明書サブジェクトからの要求によりまたは自らの裁量で証明書の変更を行う。サイバートラストは、全ての加入者に対して証明書の変更サービスを提供してはいない。

4.8.3. 証明書変更申請の処理

変更申請を受領後、サイバートラストは変更後の証明書において変更される情報を検証する。サイバートラストは、全ての変更された情報について検証手続を完了した後にのみ変更された証明書の発行を行う。サイバートラストは、変更された証明書にセクション 3.3.1 またはセクション 6.3.2.に記載された該当する制限期間を超える有効期間を与えて発行することはない。

4.8.4. 加入者への変更された証明書発行に関する通知

サイバートラスト は、証明書の発行から合理的な期間内に加入者に通知する。

4.8.5. 変更された証明書の受領確認手続き

変更された証明書は、証明書の変更から 30 日後、またはそれ以前の証明書使用時に加入者が証明書を使用した証拠が存在する場合、受領されたものとみなされる。

4.8.6. CA による変更された証明書の公開

変更された証明書は、これを加入者に交付することにより公開される。

4.8.7. CA から他の関係者に対する変更された証明書の発行通知

サイバートラストは、証明書変更の通知を受ける。

4.9. 証明書の失効および一時停止

4.9.1. 失効処理が行われる場合

証明書の失効処理は、その証明書に記された有効期限を迎える前に、その証明書の運用期間を永久的に終了させる。証明書の失効処理を行う前に、サイバートラストは失効を要求するエンティティの身元と権限を認証する。サイバートラスト は、当社が以下各号のいずれかに該当すると判断した場合、いかなる証明書についても自らの単独裁量で失効処理の要請を行うことができる。

1. 加入者が自らの証明書について失効処理を要求した。
2. 加入者は、当初の証明書要求を許可しておらず、遡及的にも許可していない。
3. 証明書に関連する秘密鍵または証明書の署名に使用された秘密鍵が危殆化しまたは悪用された。
4. 加入者が CP、本 RPS、または該当する加入契約に基づく重要な義務に違反した。
5. CP または本 RPS に基づく加入者またはサイバートラストの義務が、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、その結果他のエンティティの情報に重大な脅威または危殆化が生じた。
6. 証明書の発行を受けた加入者、スポンサー、またはその他のエンティティが、名称、商標、デバイス、IP アドレス、ドメイン名、その他の証明書に関連する属性についての権利を失った。
7. 不正に誤解を招くサブドメイン名を認証するためにワイルドカード証明書が用いられた。
8. 証明書が CP、本 RPS、または適用される業界標準に従って発行されなかった。
9. サイバートラストが、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。
10. DigiCert が業務を停止し、他の認証局が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。
11. サイバートラストが該当する業界標準に基づき証明書を管理する権利が終了した（失効処理サービスの継続と CRL/OCSP リポジトリの維持について取り決めがなされている場合は除く）。
12. 証明書に記されたいずれかの情報が不正確または誤解を招くものであった、または誤解を招いた。
13. 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。
14. 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、または、米国の法律により取引の禁止された先から運営している。
15. Adobe 署名証明書について、Adobe が失効処理を要求している。
16. コード署名証明書が、マルウェア、ユーザーの同意なしにダウンロードされたコード、その他の有害なコンテンツの署名、公開、または配布を行うために使用された。

サブジェクトと証明書上のサブジェクトの公開鍵との関連付けが有効でなくなった場合、または関連する秘密鍵が危殆化した場合には、必ず証明書は失効される。

4.9.2. 証明書失効申請が認められる者

正当な資格を有する当事者（加入者の指定された代表者またはクロス署名したパートナー）は、証明書の失効処理を要求することができる。第三者は、不正行為、悪用、または危殆化に関連する問題を理由として証明書の失効処理を要求することができる。 証明書失効要求は、失効処理を求めるエンティティと失効処理を求める理由を特定しなければならない。

4.9.3. 失効申請の手続き

サイバートラスト は、失効要求を以下のように処理する。

1. サイバートラストは、失効要求を行うエンティティの本人性、問題レポート、および失効処理を求める理由をログに記録する。サイバートラストは、失効処理の当社自体の理由をログに含めることもある。
2. サイバートラストは、既知の管理者に（該当する場合には）帯域外のコミュニケーション（例えば、電話、ファックス等）により失効処理の確認を求めることがある。
3. 要求元が加入者であると認証された場合には、サイバートラストはその証明書の失効処理を要請する。
4. 第三者からの要求については、要求の受領から 24 時間以内にサイバートラストの職員がその要求について調査を開始し、失効処理が適切であるか否かを以下の基準に基づいて判断する。
    a. 疑われる問題の性質
    b. 特定の証明書またはウェブサイトについて受信したレポートの件数
    c. 申立人の身元（例えば、ウェブサイトが違法行為を行っているとの法執行官からの苦情は、注文した商品が届かなかったと主張する消費者の苦情よりも重要度が高い)
    d. 関係法令

5. 失効処理が適切であるとサイバートラストが判断した場合、DigiCert が証明書の失効処理を行い CRL を更新する。

サイバートラストは、優先度の高い失効要求に内部で対応する機能を 1 日 24 時間週 7 日維持している。適切な場合、サイバートラストは、苦情を法執行機関へ転送する。サイバートラストは「1.5.2　連絡窓口」に記載の電子メールおよび/またはサイバートラストの Web サイト上の申請サイトで失効要求を受け付ける。

4.9.4. 失効申請までの猶予期間

加入者は、秘密鍵の滅失または危殆化を発見してから1日以内に失効申請を行わなければならない。

4.9.5. CA における 失効申請処理にかかる期間

証明書については、失効要求の認証後可及的速やかに、通常以下の時間枠内で失効処理を行う。

1. パブリック証明書の証明書失効要求は、受領から 18 時間以内に処理する。
2. CRL 発行の 2 時間以上前に受領した失効要求は、その回の CRL の発行前に処理される。
3. CRL 発行前 2 時間以内に受領した失効要求は、次回の CRL 公開前に処理される。

4.9.6. 信頼当事者による失効確認の要件

信頼当事者は、証明書に記された情報を信頼する前に、証明書パス上で IETF PKIX 標準に従って各証明書の有効性を確認しなければならない（証明書の有効性、「issuer-to-subject name」のチェーン、ポリシーと鍵使用の制限、およびチェーン内の各証明書で特定された CRL または OCSP レスポンダーを通じた失効ステータスについてのチェックを含む）。

4.9.7. CRL 発行周期

CRL は、少なくとも 24 時間ごとに発行する。鍵の危殆化により証明書が失効処理された場合には、実行可能な限り速やかに（ただし、鍵の危殆化の通知を受けてから 18 時間以内）に中間 CRL が発行される。

4.9.8. CRL 発行までの最大遅延時間

エンドエンティティ加入者に発行された証明書についての CRL は、その生成から商取引上合理的な時間内に自動的にオンラインリポジトリに投稿される（通常は、生成から数分以内）。臨時、中間、または緊急の CRL および連邦ブリッジにチェーンする CA についての全ての CRL は、生成から4時間以内に投稿される。定期の CRL は、以前に発行された同様の範囲の CRL の「nextUpdate」フィールドに記載された時期より前に投稿される。

4.9.9. オンラインでの失効/ステータス確認の利用可能性

SSL 証明書についての証明書ステータス情報は OCSP を通じて提供される。他の種類の証明書については、OCSP が利用可能でない可能性がある。該当する CP により OCSP サポートが必要とされる場合、OCSP レスポンスは商取引上合理的な時間内かつ要求の受領後 6 秒以内に提供される。ただし、インターネット上の通信の待ち時間により影響されることがある。

4.9.10. オンラインでの失効確認の要件

信頼当事者は、証明書を信頼する前にその証明書の有効性をセクション 4.9.6 に従って確認しなければならない。

4.9.11. その他の利用可能な失効情報の提供手段

規定なし

4.9.12. 鍵の危殆化に関する特別要件

規定なし

4.9.13. 証明書の一時停止が行われる場合

該当せず

4.9.14. 証明書の一時停止申請が認められる者

該当せず

4.9.15. 証明書一時停止申請手続き
該当せず

4.9.16. 一時停止を継続できる期間の制限
該当せず

4.10. 証明書のステータス確認サービス
4.10.1. 運用上の特徴
証明書のステータス情報は、CRL および OCSP レスポンダーを通じて提供される。失効処理された証明書のシリアル番号は、その証明書の有効期間の終了より後に更に 1 件の CRL が発行されるまで CRL 上に維持される（ただし、失効処理された EV コード署名証明書についてはこの限りでなく、証明書の有効期間の終了後少なくとも 365 日間 CRL 上に保持される）。加入者証明書についての OCSP 情報は、少なくとも 4 日毎に更新される。下位 CA 証明書についての OCSP 情報は、少なくとも 12 か月毎および証明書の失効から 24 時間以内に更新される。

4.10.2. サービスの利用可能性
証明書ステータス確認サービスは 1 日 24 時間週 7 日中断なしに利用可能である。

4.10.3. 運用上の特徴
OCSP レスポンダーは、必ずしも全ての種類の証明書について利用可能ではない。

4.11. 加入（登録）の終了
加入者が加入しているサービスは、証明書の有効期限が切れた場合若しくは証明書が失効処理された場合、または該当する加入契約が更新されずに満了した場合に終了する。

4.12. 鍵の預託とおよび鍵回復
4.12.1. 鍵およびの預託と鍵回復のポリシーおよび手順

サイバートラストは、加入者鍵管理鍵を鍵回復サービスを提供する目的で預託することができる。サイバートラストは預託される秘密鍵を暗号処理し、秘密鍵の生成と交付に使用されたものと同等以上のセキュリティによって保護する。
サイバートラストは、加入者およびその他の許可されたエンティティに対し、第三者預託された秘密鍵の回復（復号化）を行うことを許可する。サイバートラストは、鍵回復の際、第三者預託された加入者の秘密鍵への無許可のアクセスを防止するため複数人管理を行う。サイバートラストは以下の者からの鍵回復要求を受け付ける。

1. 加入者または加入者の組織（加入者が秘密鍵トークンを紛失しまたは破損させた場合）
2. 加入者の組織加入者が利用できないまたは加入者が秘密鍵預託についてサイバートラストと契約を交わした組織の一部でなくなった場合）
3. 資格を有する調査官または監査人（秘密鍵が必要な調査または監査の一部となっている場合）
4. その鍵を用いて暗号化されたコミュニケーションへのアクセスを所轄の法務当局から許可された要求者
5. 法律または政府の規則により許可された要求者、または
6. 秘密鍵預託についてサイバートラストと契約を交わしたエンティティ（鍵回復がミッションクリティカルまたはミッションエッセンシャルである場合）

サイバートラストの鍵預託サービスを利用するエンティティは以下の事柄を行う必要がある。

1. 秘密鍵が第三者に預託されることを加入者に通知する。
2. 第三者預託された鍵を無許可の開示から保護する。
3. 第三者預託された秘密鍵の回復に使用できる全ての認証メカニズムを保護する。
4. 正当に許可された回復要求を行った後または受領した後（該当する通り）、第三者預託された鍵をリリースする。
5. 第三者預託された鍵、かかる鍵に関連する情報、または鍵回復の要求または手続きに関する事実の開示または秘密保持についての法律上の義務を全て順守する。

4.12.2. セッションキーのカプセル化・鍵回復のポリシーおよび手順

規定なし

5. 設備上、運営上、および運用上の管理

5.1. 物理的管理

5.1.1. 立地場所および構造

サイバートラストは、信頼されない人員がサイバートラストのオペレーションにアクセスできないようにするための論理的制御および物理的制御が設けられた安全なデータ・センターを運営する。サイバートラストは、当社のオペレーションへの無許可のアクセスを検出し、抑止し、防止するためのセキュリティポリシーに基づき業務を行っている。

5.1.2. 物理的アクセス

サイバートラスト は、無許可のアクセスから当社のオペレーションを保護し、機器の不正使用のリスクを減らすため物理的制御を実行している。 セキュリティ保護されたサイバートラストの設備は、物理的アクセス制御により保護されており、適切に許可された個人のみがアクセスできる。

建物のセキュリティ保護されたエリアにアクセスするには、アクセスカードまたはパスカードを使用する必要がある。サイバートラストは、全ての取り外し可能な媒体および業務に関連する機密のプレーンテキスト情報を含む書類を、セキュリティ保護されたコンテナに当社のデータ分類ポリシーに従って安全に保管している。

5.1.2.1. データセンター

サイバートラストのデータセンターに対するアクセスには、2 要素認証が必要とされる。
RA オペレーションを行うために使用された活性化データは、頭に記憶するかまたは暗号モジュールと同等のセキュリティで保護された方法で保管しなければならない。

5.1.2.2. サポート/審査室

サイバートラストの職員が本人確認およびその他の RA 機能を実行するサポート/審査室は、アクセスコントロールにより保護されている。アクセスカードの使用は、建物のセキュリティシステムによりログに記録される。

5.1.3. 電源・空調設備

データセンターでは、主電源と二次電源により継続的かつ中断のない電力供給が保証されている。サイバートラストは、要求される容量を監視し、十分な処理能力および保管能力が利用可能であるよう保証するために将来必要な容量を予測する。

5.1.4. 水害対策

規定なし

5.1.5. 火災対策

規定なし

5.1.6. 媒体保管場所

サイバートラストは、事故による破損および権限のない物理的アクセスからメディアを保護している。バックアップファイルは毎日作成される。バックアップメディアは、バックアップファイルはサイバートラストの主要なデータ運用施設とは分離された場所で維持される。

5.1.7. 廃棄物処理

印刷された機密情報の不要な写しは、廃棄する前に全て現場においてシュレッダーで裁断される。

5.1.8. オフサイトバックアップ

サイバートラストは少なくとも 1 件のフルバックアップを維持し、システム障害からの復旧に必要な情報のバックアップコピーを定期的に作成する。

5.1.9. 証明書ステータスホスティング、CMS、および外部の RA システム

規定なし

5.2. 手続き的管理

5.2.1. 信頼される役割

信頼される役割を担当する職員には、RA のシステム管理要員、本人確認、証明書の発行・失効に関わる職員が含まれる。信頼される役割の職員が担う職務および職責は、単独の個人がセキュリティ対策を回避したり PKI のオペレーションの信用性を毀損することが可能にならないように振り分けられている。信頼される役割を担当する職員は、いずれもサイバートラストの運用の公平性を損なう可能性のある利益相反関係を有していてはならない。信頼される役割の職員は、シニアマネジメントにより任命される。信頼される役割に任命された職員については、一覧表が作成され毎年レビューが行われる。

5.2.2. 役割ごとに必要とされる人数

サイバートラストは、信頼される役割を担当する 2 名以上の者が、信頼される役割を要求する行為を行うことを必要とする。

単独の個人は、PIV-I クレデンシャルを発行することはできない。

5.2.3. 各役割における本人性確認と認証

全ての職員は、各々の信頼される役割の職務を果たすため必要なシステムへのアクセスを許可される前に、RA のシステム上で本人確認を行わなければならない。

5.2.4. 職務の分離が必要とされる役割

職務の分離が必要とされる役割には以下のものが含まれる。

1. 認証業務を行う職員（例えば、証明書申請上の情報の認証、証明書申請および失効要求の承認など）
2. バックアップ、記録、および記録保管の職務を担当する職員
3. 監査、レビュー、監督、または照合の職務を担当する職員

この職務分離を達成するために、サイバートラストは信頼される個人を特に指定する。サイバートラストのシステムは、信頼される役割を担当する個人について本人確認および認証を行い、個人が複数の役割を担当することを制限し、個人が複数のIDを持つことを防止する。

5.3. 人事的管理

5.3.1. 資格、経験、およびクリアランス要件

CTJ PA は、サイバートラストの業務についての運営責任および説明責任を負っており、本 RPS および適用ある CP が確実に順守されるようにする。サイバートラストの人事および経営の実施方法は、当社従業員の信用性および能力についておよびかかる従業員による十分な職務の遂行について合理的な保証を提供するものである。

5.3.2. 身元調査手続き

法律により許容される場合、サイバートラストは、信頼できる役職に任命された各従業員の身元を確認し、信頼できる役職で行動することを許可する前に、検証する証明書の種類に該当するガイドラインならびにサイバートラストの社内規程に従い、身元調査手続きを行います。

5.3.3. 訓練要件

サイバートラスト は、サイバートラストの業務に携わる全ての従業員に技能訓練を実施する。訓練は、その従業員の職務に関連し以下の事柄を扱う。

1. 基本的な公開鍵基盤 (PKI) の知識
2. サイバートラストが使用するソフトウェアのバージョン
3. 認証および本人確認のポリシーおよび手続き
4. サイバートラスト のセキュリティ原則およびメカニズム
5. 災害復旧および事業継続の手続き
6. 認証手続きに対する一般的な脅威（フィッシングおよびその他のソーシャルエンジニアリングの手口を含む）
7. 該当する業界および政府のガイドライン

訓練は、その従業員の所属チームの上位メンバーが参加する人材育成プロセスによって実施する。

サイバートラストは、どの従業員が訓練を受けたかおよび修了した訓練のレベルを記録する。認証スタッフは、認証権限を付与される前に、認証業務を十分に遂行するために必要な最低限の技術を有していなければならない。全ての認証スタッフは、認証および証明書発行承認の職務を遂行する前に、EV ガイドラインおよび Baseline Requirements についての内部試験に合格する必要がある。訓練以外の場で能力が示された場合、サイバートラストはそれについて補足資料を作成し維持する。

5.3.4. 再訓練の周期と要件

従業員は、信頼される役割を担当し続けるために、業界に関連するトレーニング・パフォーマンス・プログラムに適合した技術レベルを維持しなければならない。サイバートラストは、当社の業務の変更について、信頼される役割を担当する全ての従業員に周知させる。サイバートラストは、当社の業務に変更が生じた場合、信頼される役割を担当する全ての従業員に対して、実施されているトレーニングプランに従い文書により訓練を行う。

5.3.5. 職務ローテーションの周期と順序

規定なし

5.3.6. 許可されていない行動に対する罰則

サイバートラストの従業員および代理人が、過失または悪意ある意図により本 RPS の順守を怠った場合、（解雇、代理関係の解消、および刑事制裁を含む）行政処分または懲戒処分の対象となる。信頼される役割の担当者が無許可のまたは不適切な行為を行ったとマネジメントが判断した場合、その者はマネジメントによるレビューの結果が出るまで、直ちに信頼される役割から外される。マネジメントは、レビューを行いそのインシデントに関わった従業員と話し合った上で、必要に応じて、その従業員に信頼される役割以外の役割を担当させることまたはその従業員を解雇することができる。

5.3.7. 独立請負業者に関する要件

信頼される役割を担当する独立の請負業者には、かかる役割についてセクション 5.3 に定められた職務および要件並びにセクション 5.3.6 に定められた制裁が適用される。

5.3.8. 職員に提供される文書

信頼される役割を担当する職員には、その職務を遂行するために必要な文書が配布される（本 RPS、EV ガイドライン、およびその他サイバートラストの業務の完全性を維持するために必要な技術上および運用上の文書の写しを含む）。職員には、内部システムおよびセキュリティ文書についての情報、本人確認のポリシーおよび手続き、懲戒手続きに関する冊子、論文および定期刊行物、その他の情報へのアクセスも与えられる。

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

サイバートラストのシステムは、システムへのログオン時に一意性のあるユーザー名およびパスワードによる本人確認および認証を要求する。重要なシステムアクションは、そのアクションを始動したオペレーターの説明責任を立証するためログに記録される。

サイバートラスト は、当社の RA のアプリケーションのエッセンシャルイベント監査機能により、下記のイベントの記録を可能にしている。サイバートラストのアプリケーションがイベントを自動的に記録できない場合、サイバートラストは要件を満たすため手動の手続きを実施する。各イベントについて、サイバートラストは、関連する(i)日時、(ii)イベントの種類、(iii)その成功または失敗、および(iv)そのイベントを発生させまたはそのアクションを始動したユーザーまたはシステムを記録する。 全てのイベントの記録は、サイバートラストの業務運営の証拠として監査人に提供される。

監査対象イベント
セキュリティ監査
監査パラメータ（監査頻度、監査されるイベントの種類等）への全ての変更
監査ログを削除または変更しようとする全ての試行
システム上の認証
役割を担当する試行の成功または失敗

監査対象イベント
最大認証試行回数の値の変更
ユーザーのログイン時に発生した認証試行の最大回数
認証試行の失敗によりロックされたアカウントの管理者によるロック解除
管理者による認証符号の種類の変更（例えば、パスワード認証から生体認証への変更など）
ローカルデータ入力
システムに入力された全てのセキュリティ関連データ
リモートデータ入力
システムが受信した全てのセキュリティ関連メッセージ
データエクスポートおよび出力
機密情報およびセキュリティ関連情報を求める全ての要求（成功したものおよび失敗したもの全て）
証明書の登録
全ての証明書要求（発行、鍵更新、（鍵更新を伴わない）更新、および失効処理に関するものを含む）
認証アクティビティ
証明書の失効処理
全ての証明書失効要求
アカウント管理
役割およびユーザーの追加または削除
ユーザーアカウントまたは役割についてのアクセスコントロール権限の変更
その他
信頼される役割を担当する個人の任命
複数人管理のための職員の指定
PKI アプリケーションへのログオン試行
ハードウェア/ソフトウェアの受領
パスワードの設定または変更の試行
ファイル操作（例えば、生成、名前の変更、移動等）
リポジトリへの資料の投稿
全ての証明書危殆化通知要求
コンポーネントの鍵更新
コンフィギュレーション変更
ハードウェア
ソフトウェア
OS
パッチ
セキュリティプロファイル
異常事態
システムクラッシュおよびハードウェア障害
ソフトウェアエラーの状況
ソフトウェアチェックの完全性障害
不適切なメッセ―および誤った経路で送信されたメッセージの受信
（確認された）ネットワーク攻撃（およびその疑い）
機器障害
停電
無停電電源デバイス（Uninterrupted power supplies：UPS）の故障
明白かつ重大なネットワークサービスまたはネットワークアクセスの障害
本 RPS への違反
OS クロックのリセット

5.4.2. 監査ログを処理する頻度

少なくとも 2 ヶ月に 1 回、サイバートラストの管理者はサイバートラストのシステムが生成したログをレビューし、

システムおよびファイルの完全性チェックを行い、脆弱性を評価する。管理者は、かかるチェックを自動化されたツールを用いて行うことができる。このチェックの過程で、管理者は (1)何者かがログを変更していないかをチェックし、(2) 異常事態または特定の状況（悪意のアクティテビティを含む）が生じていないかスキャンし、(3)レビューの概要を記した文書を作成する。ログ上で発見された異常事態または不正行為については調査が行われる。レビューの概要書には、サイバートラストの業務管理委員会への提言が含まれ、要請に応じてサイバートラストの監査人に提供される。サイバートラストは、レビューの結果として取られたアクションについて文書で記録する。

5.4.3. 監査ログの保管期間

サイバートラストは、監査ログをレビューが完了するまで現場に保持する。

5.4.4. 監査ログの保護

監査ログは、監査ログ保管期間の終了より前に破壊されないよう保護されており、バックアップ場所に移送されるまで現場において安全に保管されている。サイバートラストのオフサイト保管場所は、データが生成された場所とは別の安全かつセキュリティ保護された場所である。監査ログは、要求に応じて監査人に提供される。

5.4.5. 監査ログのバックアップ手続き

サイバートラスト は監査ログのバックアップコピーおよび監査ログの概要を定期的に作成し、監査ログのコピーを月 1 回オフサイトの保管場所に送付する。

5.4.6. 監査ログの収集システム（内部/外部）

自動化された監査プロセスは、システムのスタートアップ時に開始されシステムシャットダウン時に終了する。自動化された監査システムに障害が発生し、システムの完全性またはそのシステムにより保護されている情報の機密性にリスクが生じた場合、CTJ PA に通知され、CTJ PA はその問題が修正されるまで RA のオペレーションを停止することを検討する。

5.4.7. イベントを起こしたサブジェクトへの通知

規定なし

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、いずれかの証明書データまたは証明書発行プロセスについて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。サイバートラストの内部監査人は、連続性の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

サイバートラストは、法律により適用される全ての記録保管ポリシーを順守する。

5.5.1. 保管対象となる記録

サイバートラスト は、以下の情報を（かかる情報がサイバートラストの RA 業務に関連する範囲で）当社のアーカイブに保持する。

1. サイバートラストが受けている認定
2. RPS のバージョン
3. RA 業務に関する契約上の義務およびその他の合意
4. システムおよび機器の構成、変更、および更新
5. 証明書要求の却下または承認
6. セクション 3.2 に定める本人性確認要件を満たすために十分な本人確認データ（認証目的で行われた通話を含む）
7. 証明書またはトークンの受領または受け入れに関連する全ての文書
8. 加入契約
9. 準拠性監査人のレポート
10. サイバートラストの監査パラメータの変更

11. 監査ログの削除または変更の試行
12. 信頼される役割を担当する個人の任命
13. セキュリティ要件違反の結果として取られた是正措置
14. RPS への違反

5.5.2. 記録の保管期間

サイバートラストは、発行に関する又はこれを支援するアーカイブデータを少なくとも 7 年半保管する。

5.5.3. 記録の保護

アーカイブ記録はセキュリティ保護されたオフサイトの保管場所に保管され、無許可の変更、置き換え、または破壊を防止する方法で保持される。アーカイブデータは、CTJ PA が許可した場合または法律により求められた場合以外はリリースされない。サイバートラストは、アーカイブデータが破壊されるまでまたは新しい媒体に移されるまで、かかるデータの処理に必要なソフトウェアアプリケーションを維持する。

サイバートラストが何らかの媒体を別の保管場所またはデバイスに移す必要がある場合、サイバートラストは移送が完了するまで両方の保管場所または保管デバイスを維持する。新しいアーカイブへの全ての移送は、セキュリティ保護された方法で行われる。

5.5.4. 記録のバックアップ手続き

サイバートラストは、セクション 5.5.1 に記載されたデータについて、少なくとも年に 1 回データの種類およびソースごとに別々の圧縮されたアーカイブファイルに分類することにより、アーカイブディスクを作成する。各アーカイブファイルについては、後日完全性認証を行うために別々に保管されるチェックサムを作成する目的でハッシュ値が算出される。 サイバートラストは、アーカイブディスクをセキュリティ保護されたオフサイトの保管場所に所定の保管期間に亘って保管する。RA は、適用される文書保管ポリシーに従ってアーカイブ記録を作成し保管する。

5.5.5. 記録のタイムスタンプ要件

サイバートラスト は、アーカイブ記録が生成される際、その時点における（非暗号化方式の）システムタイムのタイムスタンプを自動的にアーカイブ記録に押す。

5.5.6. 記録の収集システム（内部/外部）

アーカイブ情報は、サイバートラストの内部で収集される。

5.5.7. 記録情報の取得と検証手続き

アーカイブ情報の作成および保管についての詳細はセクション 5.5.4.に記載されている。顧客、当社代理人、またはサイバートラスト PKI に関わるトランザクションについての紛争の当事者から適切な目的の要求を受領した場合、サイバートラスト はアーカイブから情報を読み出すことを選択できる。アーカイブ情報の完全性は、圧縮されたアーカイブファイルのハッシュ値をそのファイルについて（セクション 5.5.4.に記載された通り）当初記録されたチェックサムと比較することにより検証される。サイバートラストは、セキュリティ保護された電子的手段またはクーリエによる関連情報の送付またはかかる情報の（当社の裁量による）提供拒否を選択できる。また、サイバートラストは、かかるデータに関連する全費用の前払いを要求できる。

5.6. 鍵の切り替え

規定なし

5.7. 危殆化および災害からの復旧

5.7.1. 事故および危殆化の取扱手続き

サイバートラストは、システムの危殆化を招く可能性のあるセキュリティインシデント、自然災害、およびこれらに類するイベントへの職員の対応を指導するためにインシデント対応手続きを維持している。サイバートラストは、インシデント対応のためのプランおよび手続きを少なくとも年に1回、レビューし、テストし、更新する。

5.7.2. コンピュータの資源、ソフトウェア、および/またはデータが破損した場合

サイバートラスト は、定期的に（少なくとも週1回）、システムバックアップを取る。サイバートラストは、自らのコンピュータ資源、ソフトウェア、またはデータのオペレーションが危殆化したと知った場合、かかる危殆化が当社ま

たは影響を受ける当事者の業務の完全性またはセキュリティに対して呈する脅威とリスクを評価する。業務の継続は信頼当事者または加入者に対して重大なリスクを呈する可能性があるとサイバートラストが判断した場合、サイバートラストはかかるリスクが軽減されたと認められるまで当該業務を停止する。

5.7.3. エンティティの秘密鍵が危殆化した場合の手続き

規定なし

5.7.4. 災害後の事業継続能力

サイバートラストは、サービスの完全性を維持するため、当社の事業継続管理プラン（Business Continuity Management Plan: BCMP）の一環として、データのバックアップおよび復旧の手続きを実行する。BCMP に定められた目標は、サイバートラストの主要設備に関わる災害により証明書ステータス確認サービスが受ける影響を確実に最小限に留め、サイバートラストが災害後もその他のサービスを維持または可能な限り早急に再開できるよう確実にすることである。サイバートラストは、BCMP および付属手続きを少なくとも年に1回、レビューし、テストし、更新する。

5.8. CA または RA の終了

RA のアクティビティを終了する前に、サイバートラスト は以下の事柄を行う。

1. 終了についての通知および情報を、当社の顧客への電子メール通知の送信によりおよびかかる情報のサイバートラストのウェブサイト上への投稿により提供する。
2. 資格を有する承継エンティティに全ての責任を移管する。

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

全ての鍵は、FIPS の規格を満たす方法またはこれと同等の国際標準を用いて生成しなければならない。

加入者は、自らの鍵を証明書の種類に応じて適切な方法で生成しなければならない。

6.1.2. 加入者秘密鍵の交付

サイバートラストが加入者のための鍵を生成する場合、セキュリティ保護された方法で加入者にその秘密鍵を交付しなければならない。かかる鍵は、電子的に（例えば、セキュリティ保護された電子メールまたはクラウド上のシステムでの保管等）またはハードウェア暗号モジュール/SSCD 上で交付することができる。いかなる場合も、以下の事柄が適用されるものとする。

1. 預託/バックアップサービスが認証され許可されている場合を除き、加入者への秘密鍵の交付後にキージェネレーターがその秘密鍵へのアクセスを保持していてはならない。
2. キージェネレーターは、秘密鍵を交付プロセス中の活性化、危殆化、または変更から保護しなければならない。
3. 加入者は、（通常、加入者が関連する証明書を使用することにより）秘密鍵の受領を確認しなければならない。
4. キージェネレーターは、正しいトークンおよび活性化データが正しい加入者に確実に提供される方法（以下に挙げるものを含む）で秘密鍵を交付しなければならない。
    a. ハードウェアモジュールについては、加入者がその所持を受け入れるまで、キージェネレーターがそのモジュールのロケーションおよびステータスについての説明責任を保持すること
    b. 秘密鍵の電子的交付については、キージェネレーターが秘密鍵と同等以上に強固な暗号アルゴリズと鍵長を用いて鍵マテリアルを暗号化し、セキュリティ保護された別の経路を通じて活性化データを交付すること

鍵の生成について加入者を支援するエンティティは、加入者の鍵ペアを格納したデバイスの加入者による受領確認の記録を維持する。

6.1.3. 証明書発行者への公開鍵の交付

加入者は、鍵ペアを生成し、証明書申請プロセスの一環として CSR により公開鍵をサイバートラストに受け渡す。かかる要求上の加入者の署名は、証明書の発行前に確認される。

6.1.4. 信頼当事者への CA 公開鍵交付

ルート証明書に関する公開鍵は、証明書認証ファイルまたはパスディスカバリーポリシーファイルに記された通り、商業ブラウザおよびオペレーティングシステム・ルートストアにおけるトラストアンカーとしておよび/または他の CA により署名されたルートとして信頼当事者に提供される。

6.1.5. 鍵長

加入者は、少なくとも以下の鍵長の最小値、署名アルゴリズム、およびハッシュアルゴリズムを全てのサーバー証明書について生成し使用しなければならない。

2048-bit RSA 鍵 または
セキュアハッシュアルゴリズム バージョン 2 (SHA-256)またはこれと同等以上の衝突耐性を有するハッシュアルゴリズムを用いた 256-bit ECDSA 鍵）

6.1.6. 公開鍵パラメータの生成および品質検査

規定なし

6.1.7. 鍵用途の目的(X.509 v3 の鍵用途フィールドの通り)

証明書には、証明書の意図される用途を特定し、証明書の機能を技術的に X.509v3 準拠のソフトウェア上に制限する鍵用途拡張フィールドが含まれている。特定の鍵の用途は、X.509 証明書の鍵用途拡張領域により指定されている。

加入者証明書は、その鍵ペアについて意図されるアプリケーションに基づいて鍵用途を表明する。特に、電子署名（認証を含む）に使用される証明書には、「digitalSignature」および/または「nonRepudiation」のビットがセットされている。鍵またはデータの暗号化に用いられる証明書には、「keyEncipherment」 および/または「dataEncipherment」のビットがセットされている。鍵共有に用いられる証明書には、「keyAgreement」のビットがセットされている。

鍵用途のビットおよび拡張鍵用途は、各種類の証明書についての証明書プロファイルにおいて、適用ある証明書プロファイル文書に定める通り、特定されている。

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

証明書サービスの提供において使用される CA および OCSP レスポンダーの全ての鍵ペアのための暗号モジュールは、FIPS140 レベル 3 および（EU においては）情報技術セキュリティ評価のためのコモンクライテリア（International Common Criteria Information Technology Security：CC) の評価保証レベル（Evaluation Assurance Level: EAL）14169 EAL 4+Type 3 （EAL 4 に AVA_VLA.4 および AVA_MSU.3 を追加（Augmented）したもの）の認定を受けている。

加入者および登録局についての暗号モジュールの要件は、下表の通りである。

保証レベル	加入者	登録局
EV コード署名	FIPS 140 レベル 2 （ハードウェア）	FIPS 140 レベル 2 （ハードウェア）
Adobe 署名	FIPS 140 レベル 2 (ハードウェア)	FIPS 140 レベル 3 （ハードウェア）
基礎的	該当せず	FIPS 140 レベル 1 （ハードウェアまたはソフトウェア）
レベル 1 クライアント	適用なし	FIPS 140 レベル 1 （ハードウェアまたはソフトウェア）
レベル 2 クライアント	FIPS 140 レベル 1	FIPS 140 レベル 1

	（ハードウェアまたはソフトウェア）	（ハードウェアまたはソフトウェア）
レベル 3 クライアント	FIPS 140 レベル 1（ソフトウエア） FIPS 140 レベル 2（ハードウエア）	FIPS 140 レベル 2（ハードウェア）
レベル 4 クライアント	FIPS 140 レベル 2（ハードウエア）	FIPS 140 レベル 2（ハードウェア）

EV コード署名証明書の秘密鍵の要件は、サイバートラストまたは DigiCert が(i)クリプトモジュールをプレインストールされた鍵ペアと確認した上で出荷すること、(ii)加入者が要件を満たしているまたはそれ以上であるクリプトモジュールにおいて「PKCS#11 crypto API」を用いて通信すること、または(iii)加入者の IT 監査により FIPS140-2 レベル 2 準拠またはそれに相当する評価を受けることにより、充足される。その他全ての鍵は、ソフトウエアに保管されることができる。

6.2.2. 秘密鍵の (n out of m) による複数人管理
サイバートラストの認証メカニズムは、使用されない時にはセキュリティで保護されており、複数の信頼される職員の行為によってのみアクセス可能である。

6.2.3. 秘密鍵預託
サイバートラストは、署名鍵の第三者預託を行わない。

6.2.4. 秘密鍵バックアップ
規定なし

6.2.5. 秘密鍵のアーカイブ
サイバートラストは、秘密鍵のアーカイブ保管を行わない。

6.2.6. 秘密鍵の暗号モジュールへの転送または暗号モジュールからの転送
全ての鍵は、暗号モジュールにより（暗号モジュール内で）生成しなければならない。秘密鍵は、HSM 移送、オフラインストレージ、およびバックアップの目的でのみ暗号モジュールからバックアップトークンにエクスポートされる。秘密鍵を暗号モジュールから転送する際には必ず暗号化し、プレインテキストフォームで存在することがないようにする。

6.2.7. 暗号モジュール内での秘密鍵保存
ルート証明書に関する秘密鍵は、FIPS140 レベル 3 および EAL4+以上の認定を受けた暗号モジュール内で生成され、かかる暗号モジュール内に保存される。

6.2.8. 秘密鍵活性化の方法
加入者は、自らの秘密鍵の保護について全責任を負う。加入者は、自らの秘密鍵についての無許可のアクセスまたは無許可の使用を防止するために、強固なパスワードまたはこれと同等の認証手段を用いるべきである。加入者は、自らの秘密鍵を活性化する前に、少なくとも、暗号モジュール上での認証を受ける必要がある。

6.2.9. 秘密鍵非活性化の方法
加入者は、使用しない時にはログアウトおよび取り外し手続きにより自らの秘密鍵を非活性化するべきである。

6.2.10. 秘密鍵破壊の方法
規定なし

6.2.11. 暗号モジュールの評価
規定なし

6.3. 鍵ペアのその他の管理
6.3.1. 公開鍵のアーカイブ
規定なし

6.3.2. 証明書の運用の期間および鍵ペアの使用期間

証明書は、最長で以下の有効期間を有する。

証明書の種類	秘密鍵の使用期間	証明書の運用期間
ルート CA	20 年	25 年
下位 CA*	12 年	15 年
CRL および OCSP レスポンダー署名	3 年	31 日†
OV SSL	規定なし	39 ヶ月
EV SSL	規定なし	27 ヶ月
コード署名証明書および文書署名	規定なし‡	123 ヶ月
加入者に発行される EV コード署名証明書	規定なし	39 ヶ月
署名機関に発行される EV コード 署名証明書	123 ヶ月	123 ヶ月
Adobe 署名証明書	39 ヶ月	5 年
エンドエンティティ/クライアント証明書	規定なし	60 ヶ月

コード署名を行う者は、自らの秘密鍵を 3 年間使用することができる。関連する公開鍵のライフタイムは 8 年を超えないものとする。信頼当事者は、これらの鍵により生成された署名について証明書の有効期間終了後でも検証を行うことができる。

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

全てのサイバートラストの職員および加入者は、強固なパスワードを使用し、PIN およびパスワードを保護するよう指示されている。サイバートラストの従業員は、最少文字数以上の辞書にない英数字のパスワードを作成し、定期的にパスワードを変更しなければならない。

6.4.2. 活性化データの保護

全てのサイバートラストの職員は、自らのパスワードを書き留めずに覚え、他の個人と共有しないよう指示されている。サイバートラストは、セキュリティ保護された RA プロセスにアクセスするためのアカウントへのパスワード入力試行が一定回数失敗した場合、そのアカウントをロックする。

6.4.3. 活性化データのその他の考慮点

規定なし

6.5. コンピュータのセキュリティ 管理

6.5.1. コンピュータのセキュリティに関する具体的な技術的要件

サイバートラスト は、当社の RA システムをセキュリティで保護し、当社のシステムと信頼される役割の担当者との間のコミュニケーションを認証し保護する。サイバートラストのサポート/審査ワークステーションは、業界のベストプラクティスに則って強固に構成された信用性のあるシステム上で運用されている。全ての RA システムは、悪意あるコードを検知するためスキャンされ、スパイウェアおよびウィルスから保護されている。

サイバートラストの RA システム（リモートワークステーションを含む）は、以下の通り構成されている。

1. システムまたはアプリケーションへのアクセスを許可する前に、ユーザーの本人確認を行う。
2. ユーザーの権限を管理し、そのユーザーに割り当てられた役割の範囲に制限する。
3. 全てのトランザクションについてのアーカイブ記録を作成し監査する。
4. セキュリティクリティカルなプロセスについては、ドメインの完全性のために境界設定を実行する。
5. 鍵またはシステムの障害からの復旧をサポートする。

6.5.2. コンピュータセキュリティの評価

規定なし

6.6. ライフサイクルの技術的管理

6.6.1. システム開発管理

サイバートラストは、当社の RA システムの取得および開発を制御し監視するメカニズムを設けている。変更要求は、その変更の提出者とは別の少なくとも1名の管理者の承認を必要とする。サイバートラストは、ソフトウェアが RA オペレーションの一部である場合にのみ、ソフトウェアを RA システムにインストールする。

ベンダーは、市場における評判、質の高い製品を提供する能力、および将来おける継続的発展の可能性に基づいて選定される。ベンダー選定および購買決定のプロセスには、マネジメントが参加する。全てのハードウェアおよび ソフトウェアは、そのコンポーネントが直接信頼される従業員（改ざんの余地なくインストールされるよう確実にする者）に引き渡されるよう確実にするため標準条件に基づいて出荷される。

サイバートラストが使用する PKI ソフトウェアコンポーネントの幾つかは、標準ソフトウェア開発メソドロジーを用いて、社内でまたはコンサルタントにより開発される。かかる全てのソフトウェアは、管理された環境で設計および開発され、品質保証レビューを受ける。その他のソフトウェアは商用オフザシェルフ（commercial off-the-shelf: COTS）で購買する。品質保証は、全てのプロセスを通じてテストとドキュメンテーションにより、または前述の通り信頼されるベンダーから購買することにより維持される。

機器およびソフトウェアの更新については、当初の機器またはソフトウェアの購買または開発と同様に行われ、訓練を受けた信頼される職員がインストールおよびテストを行う。サイバートラストのオペレーションに不可欠の全てのハードウェアおよびソフトウェアは、初回使用時およびその後定期的に、悪意あるコードを検知するためスキャンされる。

6.6.2. セキュリティ運用管理

サイバートラスト は、RA システムのセキュリティ関連の構制を制御し監視するメカニズムを設けている。RA システムにソフトウェアをロードする際、サイバートラストはソフトウェアのバージョンが正しいことおよびベンダーから変更なしに供給されたことを確認する。

6.6.3. ライフサイクルセキュリティ管理

規定なし

6.7. ネットワークセキュリティ管理

サイバートラスト は、当社のシステム構成（アップグレードまたは変更を含む）を文書化し管理する。サイバートラストの顧客サポート/審査ワークステーションはファイアウォールで保護されており、社内 IP アドレスのみを使用する。ファイアウォールおよび境界を管理するデバイスは、信用性のある PKI サービス提供のため必要とされるアドレス、ポート、プロトコル、およびコマンドへのアクセスのみを該当するシステムが許可するように構成されている。

サイバートラストのセキュリティポリシーは、全てのポートおよびプロトコルをブロックし、RA 機能を可能にするために必要なポートのみを開く。全ての RA 機器は、最小限のサービスで構成されており、全ての使用されていないネットワークポートおよびサービスは無効化されている。サイバートラストのネットワーク構成は、監査人および（適切な秘密保持契約を交わした）コンサルタントによるオンサイトレビューに供される。

7. 証明書、CRL、および OCSP のプロファイル

証明書は、ITU X.509 バージョン 3 規格の電子証明書である。サイバートラストは、X.509v3 が意図する目的（「ISO/IEC 9594-8 への Amendment 1（1995 年）」に記載の通り）のために、基本的な証明書の構造に一定の証明書拡張領域を追加している。

7.1. 証明書のプロファイル

7.1.1. バージョン番号

全ての証明書は、X.509 バージョン 3 準拠の証明書である。

7.1.2. 証明書拡張領域

規定なし

7.1.3. アルゴリズムのオブジェクト識別子

証明書は、以下のアルゴリズムの1つを用いて署名される。

sha-1WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5]
sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
ecdsa-with-sha384	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures (4) ecdsa-with-SHA2 (3) 3]

7.1.4. 名前の形式

各証明書には、一意性のあるシリアル番号が使用され、その番号は再使用されない。SSL 証明書サブジェクトのオプショナルのサブフィールドは、サイバートラスト が認証した情報を記すかまたは空にしておかなければならない。SSL 証明書に、「.」、「-」、および「‘ ‘」の文字等のメタデータ、またはそのフィールドが該当しないことを示すその他の表示に含めることはできない。

7.1.5. 名称の制約

規定なし

7.1.6. 証明書ポリシーオブジェクト識別子

オブジェクト識別子（OID）は、オブジェクトまたはポリシーを識別する一意性のある番号である。サイバートラスト が使用する OID は、証明書の種類に基づき割り当てられ、適用ある証明書プロファイルにおいて設定される。

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

証明書は、証明書ポリシー拡張領域のポリシー修飾子フィールドに、責任の制限およびその他証明書の使用に関連する規程についての簡潔な記述を含めることができる。

7.1.9. 重要（Critical）とされる証明書ポリシー拡張についての処理方法

規定なし

7.2. CRL のプロファイル

7.2.1. バージョン番号

サイバートラストが授権する証明書は、以下のフィールドを含むバージョン 2 の CRL を使用している。

フィールド	値
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha384 [1 2 840 10045 4 3 3]
Issuer Distinguished Name	DigiCert
thisUpdate	CRL 発行日（UTC フォーマット）
nextUpdate	次回の CRL 発行日（UTC フォーマット）
Revoked Certificates List	失効処理された証明書のリスト（シリアル番号および失効日を含む）
Issuer’s Signature	[署名]

7.2.2. CRL、CRL エントリー拡張

CRL は、以下の拡張領域を有する。

拡張領域	値
CRL Number	絶対に繰り返されず単調に増加する整数型データ（monotonically increasing integer）
Authority Key Identifier	証明書に記載された認証局鍵識別子（Authority Kay Identifier）と同じ
Invalidity Date	UTC フォーマットの日付（オプショナル）
Reason Code	失効理由（オプショナル）

7.3. OCSP のプロファイル

7.3.1. バージョン番号

OCSP レスポンダーは、RFC 2560 のバージョン 1 に準拠している。

7.3.2. OCSP 拡張

規定なし

8. 準拠性監査およびその他の評価

本 RPS に記載された実施方法は、一般に認められた業界標準による要件を満たすまたはそれらを超えることを目的としている。

8.1. 評価の頻度および評価が行われる場合

サイバートラスト は、当社による本 RPS の順守を評価するため独立の外部監査人による年次監査を受けている。

8.2. 評価人の身元および資格

WebTrust に関する監査人は、EV ガイドラインのセクション 14.1.14 に記載された要件を満たさなければならない。具体的には、以下の要件を満たす必要がある。

(1) *資格および経験:* 監査人は監査を主たる業務としている必要がある。個人の監査人または監査グループのメンバーのうち少なくとも1人は、公認情報システム監査人（Certified Information Systems Aucitoror : CISA)、AICPA 認定情報技術者（Certified Information Technology Professional : CPA.CITP）、公認内部監査人（Certified Internal Auditor: CIA）、またはその他の認められた情報セキュリティ監査の資格を有していなければならない。監査人は、該当する認定機関による懲戒処分の適用対象でなければならない。

(2) *専門知識*: 個人の監査人または監査人のグループは、セキュリティ保護された情報システムの監査についての訓練を受け、それについての技能を有し、公開鍵基盤、認証システム、およびインターネットセキュリティの問題に精通している必要がある。

(3) *規則および標準*: 監査人は、米国公認会計士協会（the American Institute of Certified Public Accountants: AICPA）、CPA Canada,、、イングランド・ウェールズ勅許会計士協会（the Institute of Chartered Accountants of England & Wales: ICAEW）、欧州委員会が採用している国際会計基準（the International Accounting Standards: IAS）、情報システムコントロール協会（Information Systems Audit and Control Association: ISACA ）、内部監査人協会（the Institute of Internal Auditor: IIA）、またはその他の資格を有する監査標準設定機関により公布された該当する標準、規則、およびベストプラクティスを順守する必要がある。

(4) *評判*: 当該ファームは、監査業務を有能かつ正確に実施するとの評判を有している必要がある。

(5) *保険*: EV 監査人は、証券総填補限度額（policy limit）が百万 USドル以上の専門業務賠償責任/過失怠慢賠償責任保険（Professional Liability/Errors and Omissions Insurance）への加入を維持している必要がある。

8.3. 評価人と評価されるエンティティの関係
サイバートラストについて WebTrust 監査を行う監査人は、サイバートラストに対して有利または不利な形で著しく不公平な判断を招く可能性があると予測される金銭的利害または事業関係を有しておらず、そのような取引過程にない。

8.4. 評価で扱われる事項
監査は、サイバートラストの業務開示およびサイバートラストによる本ポリシー書類の順守について行われる。

8.5. 指摘事項の対応
法律、本 RPS、またはサイバートラストのサービスに関連するその他の契約上の義務への重大な違反が監査により報告された場合、(1) 監査人はその違反について文書化して、(2)速やかにサイバートラストに通知し、(3) サイバートラストは、かかる違反を是正するための計画を策定する。サイバートラストは、承認を得るため CTJ PA にかかる計画を提出し、またサイバートラストが法律上意を満たす義務を負う第三者にも同計画を提出する。CTJ PA は、違反が招いた重大な問題を是正するために必要な場合、（影響を受けている証明書の失効処理を含む）追加の対策を求めることができる。

8.6. 結果の開示
各監査の結果は、CTJ PA および法律、規則、または合意により監査結果の写しを受領する資格を与えられた全ての第三者エンティティに報告される。

8.7. 内部監査
サイバートラストは、直近の内部監査以後に発行された非 EV SSL 証明書の 3%以上および EV SSL 証明書および EV コード署名証明書の 6%以上に相当する無作為抽出されたサンプルについて、少なくとも四半期ごとに定期的な内部監査を実施する。SSL 証明書およびコード署名証明書についての内部監査は、CA/ブラウザフォーラムが採択したガイドラインに従って実施される。

9. その他の事業上および法律上の事項
9.1. 料金
9.1.1. 証明書の発行料金または更新料金
サイバートラスト は、証明書の発行および更新について料金を請求する。サイバートラストは、該当する顧客との契約に従っていつでも料金を改訂することができる。

9.1.2. 証明書へのアクセス料金
規定なし

9.1.3. 失効処理料金またはステータス情報へのアクセス料金
サイバートラストは、証明書の失効処理または発行済み証明書についての CRL を用いた有効性ステータス確認については料金を請求しない。

9.1.4. その他のサービス料金
規定なし

9.1.5. 返金ポリシー
規定なし

9.2. 財務的責任
9.2.1. 保険による補償
規定なし

9.2.2. その他の資産
規定なし

9.2.3. エンドエンティティに対する保険補償または保証の範囲
規定なし

9.3. 企業情報の機密性
9.3.1. 機密情報の範囲
以下の全ての情報は、機密情報とみなされ、開示されないよう合理的な注意を払って保護される。

1. 事業継続、インシデント対応、緊急事態、および災害復旧についての計画
2. 情報の機密性、完全性、または利用可能性を保護するために使用されるその他のセキュリティ関連の実施方法
3. サイバートラストが個人情報としてセクション 9.4 に従って保持している情報
4. 監査ログおよびアーカイブ記録
5. トランザクション記録、財務監査記録、および外部または内部による監査証跡および監査報告書（本 RPS に規定された管理方法の有効性を確認する監査人レターは除く）

9.3.2. 機密情報の範囲外の情報
機密情報として挙げられていない全ての情報は、全て公開情報とみなされる。公開された証明書および失効についてのデータ は、公開情報とみなされる。

9.3.3. 機密情報の保護責任
サイバートラストの従業員、代理人、および請負業者は、機密情報を保護する責任を負っており、契約上かかる保護を行う義務を負っている。従業員には、機密情報の取り扱いに関する訓練が実施されている。

9.4. 個人情報のプライバシー
9.4.1. プライバシー・プラン
個人情報は、法律により開示が求められた場合または当該個人情報の対象により要求された場合にのみ開示される。

9.4.2. プライバシーとして扱われる情報
サイバートラスト は、証明書または CRL の内容として公表されていない全ての個人情報を、個人情報とみなす。サイバートラストは、個人情報を適切な安全対策を取り合理的な注意を払って保護している

9.4.3. プライバシーとみなされない情報
証明書、CRL、またはそれらの内容は、個人情報に含まれない。

9.4.4. 個人情報の保護責任
サイバートラストの従業員および請負業者は、秘密を厳重に保持して個人情報を取り扱うよう求められている。全ての機密情報は、安全に保管され偶発的に開示されることのないよう保護されている。

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
申請または本人確認の過程で申請者から取得した個人情報は、かかる情報が証明書に含まれない場合、個人情報とみなされる。サイバートラストは、個人情報の対象者から同意を得た場合または適用法令の要件に従う場合にのみ、かかる情報を使用する。全ての加入者は、証明書に含まれる個人データに関しては、グローバルな転送および公開に同意しなければならない。

9.4.6. 司法手続きまたは行政手続きに基づく公開
サイバートラストは、法令により開示が求められているとサイバートラストが判断した場合には、通知を行わずに、個人情報を開示することができる。

9.4.7. 他の情報公開の場合
規定なし

9.5. 知的財産権
サイバートラストおよび/またはそのビジネスパートナーは、サイバートラストのサービスについての知的財産権（証明書、サービス提供に用いられる商標、および本 RPS を含む）を所有している。

9.6. 表明保証

9.6.1. CA の表明保証

規定なし

9.6.2. RA の表明保証

サイバートラストは、以下の通り表明する。

1. サイバートラストによる証明書の発行/管理サービスは、サイバートラストの RPS および DigiCert の CP に準拠している。
2. サイバートラストが提供する情報には、虚偽の情報または誤解を招く情報は含まれていない。
3. サイバートラストが要求する全ての証明書は、適用ある CP の要件を満たしている。

9.6.3. 加入者の表明保証

加入者は、証明書の発行を受け証明書を受領するまで、自らが第三者に対して行った不実表示および加入者の秘密鍵を用いた全ての取引について（かかる使用が許可されたものか否かを問わず）全責任を負う。加入者は、証明書のステータスに影響を与える可能性のある変更が生じた場合、サイバートラストおよび発行 CA に通知しなければならない。加入者は、サイバートラスト、DigiCert、アプリケーションソフトウェアベンダー、および信頼当事者に対し、各証明書について、以下の通り表明する。

1. 自らの秘密鍵を安全に生成し危殆化しないよう保護する。
2. サイバートラストと通信する際に正確かつ完全な情報を提供する。
3. 証明書を使用する前に証明書データの正確性を確認する。
4. 速やかに以下の措置をとる。(i) 証明書に含まれる公開鍵に関連する秘密鍵の悪用または危殆化が実際に発生した場合またはその疑いがある場合には、速やかに証明書の失効を要求し、その証明書及びそれと関連する秘密鍵の使用を中止し、サイバートラストに通知する。また(ii) 証明書上の情報が誤っているもしくは不正確である、またはそのようになった場合には証明書の失効を要求し、その使用を中止する。
5. 組織を代表して証明書を使用する個人が、証明書に関して適切なセキュリティトレーニングを受講済みであるよう確実にする。
6. 許可された適法な目的にのみ証明書を使用し、証明書の使用目的、本 RPS、適用される CP、および関連する加入契約と整合的な方法でのみ証明書を使用する（証明書に記載されたドメインにおいてアクセス可能なサーバー上にのみ SSL 証明書をインストールすることおよびコード署名証明書を悪意あるコードまたはユーザーの同意なしにダウンロードされたコードへの署名のために使用しないことを含む）。
7. 証明書の有効期間終了後は、速やかに証明書および関連する秘密鍵の使用を停止する。
8. サイバートラストは、加入者の組織単位（OU）に記載されている情報の真正性と正確性を検証しません。

9.6.4. 信頼当事者の表明保証

各信頼当事者は、証明書に依拠する前に、以下の通り表明する。

1. 電子証明書と PKI の使用について十分な知識を得た。
2. 証明書の用途について該当する制限を検討し、証明書の使用に関連する適用ある責任の制限に同意している。
3. 適用ある信頼当事者規約および CP を読み、理解し、同意している。
4. 証明書および証明書チェーン内の証明書について関連する CRL または OCSP を用いて検証した。
5. 有効期限が切れたまたは失効処理された証明書を使用しない。
6. 電子署名への依拠に関連するリスクを極小化するために全ての合理的な手段を講じる（以下の事柄について検討した上でのみ証明書を信頼することを含む）。
    a) 当事者の本人確認、情報の秘密性またはプライバシーの保護、および取引の法的強制力に関する適用法および法的要件
    b) 証明書または適用ある CP に記されている証明書の意図された用途
    c) 証明書に記されたデータ
    d) 当該取引または通信の経済的価値
    e) アプリケーション、取引、または通信上における本人確認の誤り、情報の秘密性またはプライバシーの侵害により生じる可能性のある潜在的な損失または損害

f) 信頼当事者と加入者との以前の取引の経過
g) 取引についての信頼当事者の理解（コンピュータベースの取引方法についての経験を含む）
h) 加入者および/またはアプリケーション、通信、または取引についての信頼性または非信頼性に関するその他の証拠

無許可で証明書に依拠した場合には、その当事者の自己責任となる。

9.6.5. 他の関係者の表明保証

規定なし

9.7. 保証の免責

セクション 9.6.1.に明記されている場合を除き、全ての証明書並びに関連するソフトウェアおよびサービスは、「現状有姿」かつ「利用可能な範囲」で提供されるものである。法により許容される最大限の範囲で、サイバートラスト及び DigiCert は、明示的か黙示的かを問わない全ての保証（商品性、特定目的適合性、および非侵害についての全ての保証を含む）を否認する。サイバートラスト及び DigiCert は、いずれかのサービスまたは製品が何らかの期待に応えるとの保証を行わず、適時にまたはエラー無しに証明書にアクセスできるとの保証を行わない。 サイバートラストは、いかなる製品またはサービスの利用可能性についても保証を行わず、いずれの製品またはサービスの提供であれ何時でも変更または停止することができる。いずれかのエンティティによるサイバートラストサービスの使用のみを理由として、（サイバートラストに）受託者義務が生じることはない。

9.8. 責任の制限

本 RPS のいかなる規定も、(i) サイバートラストの過失により引き起こされた死亡若しくは人身傷害、または (ii) サイバートラストによる不正行為に関連する責任を制限しない。前述の範囲を除いて、証明書またはサービスを使用する全てのエンティティ は、かかる使用に関連してサイバートラストまたは DigiCert の責任を問う権利を全て放棄する（ただし、サイバートラストおよび DigiCert が、当該証明書またはサービスの提供において本 RPS を実質的に順守していることを条件とする）。本 RPS または適用ある CP に実質的に従っていない証明書およびサービスについてのサイバートラストおよび DigiCert の責任は、以下の通りとする。

1. **SSL 証明書またはコード署名証明書以外の証明書に関連する損害または損失については、一切責任を負わない。**
2. **SSL 証明書については、取引 1 件当たりの最高責任額を 1,000US ドルとする。**
3. **1 件の証明書またはサービスに関連する全ての請求についての責任限度額は、10,000US ドルとする。**
4. **請求件数または請求元の如何を問わず、全ての請求についての責任限度額の総計は、100 万 US ドルとする。**

サイバートラストおよび DigiCert は、本セクションに基づく責任限度額に関連する支払を、初めに最終的解決に達した各請求間に分配して行う。

全ての責任は、実際または法的に相当な損害に関するものに限られる。DigiCert 及びサイバートラストのいずれも、以下に挙げるものについては、一切責任を負わない。

1. 間接的、結果的、特別、若しくは懲罰的な損害賠償、または利益、収益、データ若しくは機会の喪失（当事者がかかる損害賠償の可能性を認識していた場合も含む）
2. 申請者による不正行為または意図的な違法行為に関連する責任
3. 証明書または適用ある CP に記載された用途、金額、または取引に関する制限の範囲を超えた証明書の使用に関連する責任
4. サイバートラストが供給していない製品（加入者および信頼当事者のハードウェアを含む）についてのセキュリティ、ユーザビリティ、または完全性に関連する責任
5. 加入者の秘密鍵の危殆化に関連する責任

本セクションに基づく制限は、(i)責任の理由または性質（不法行為請求を含む）、(ii)請求件数、(iii)損害の程度および性質、(iv)DigiCert またはサイバートラストによる適用ある CP の規定の不順守があったか否か、または (v)適用ある CP のいずれかの規程が無効であると証明されたか否かにかかわらず、法により許容される最大限の範囲で適用される。

本 RPS に記載された免責規程および責任の制限は、証明書およびサービスを使用する際の基本的条件である。

9.9. 補償

9.9.1. サイバートラストによる補償

規定なし

9.9.2. 加入者による補償

各加入者は、法により許容される最大の範囲で、(i)加入者による重要な事実の虚偽表示または遺漏（かかる虚偽表示または遺漏が故意か否かを問わない）、(ii)加入者による加入契約、適用ある CP、または適用法への違反、(iii) 加入者の過失または意図的な行為に起因する証明書または秘密鍵の危殆化または無許可の使用、または(iv)加入者による証明書または秘密鍵の悪用に関連する損失、損害、または費用（合理的な弁護士費用を含む）につき、サイバートラスト、当社のパートナーおよびクロス署名エンティティ並びにそれらの代表取締役、役員、従業員、代理人、および請負業者に対して補償を行う。

9.9.3. 信頼当事者による補償

各信頼当事者は、法により許容される最大の範囲で、(i)信頼当事者による信頼当事者規約、エンドユーザー ライセンス契約、適用ある CP、または適用法への違反、(ii)証明書への不合理な依拠、または(iii)信頼当事者が証明書の使用前に証明書ステータスのチェックを怠ったことに関連する損失、損害、または費用（合理的な弁護士費用を含む）につき、につき、サイバートラスト、当社のパートナーおよびクロス署名エンティティ並びにそれらの代表取締役、役員、従業員、代理人、および請負業者に対して補償を行う。

9.10. 文書の有効期間と終了

9.10.1. 文書の有効期間

本 RPS およびその変更は、サイバートラストのオンラインリポジトリに投稿された時点で発効し、新しいバージョンにより置き換えられるまで有効であり続ける。

9.10.2. 終了

本 RPS およびその変更は、新しいバージョンにより置き換えられるまで有効であり続ける。

9.10.3. 終了の効果と存続

サイバートラストは、本 RPS 終了の条件とその効果について、サイバートラストのリポジトリを通じて連絡する。かかる連絡は、終了後も存続する規程を定める。少なくとも、機密情報の保護に関連する全ての義務は、本 RPS の終了後も存続する。加入契約は、証明書が失効処理されるまでまたはその期限が切れるまで（本 RPS が終了した場合でも）有効であり続ける。

9.11. 関係者間の個別通知と連絡

サイバートラストは、本 RPS に関連する通知をセクション 2.2.に記載された場所で受け取る。通知は、送付者がサイバートラストから有効な電子署名された受領確認を受け取った時点で発効したものとみなされる。5 日以内に受領確認が届かない場合、送付者はセクション 2.2 に記載された住所宛に、配達確認付のクーリエサービスまたは、郵便料金前払いかつ受領通知付の配達証明郵便または書留郵便を用いて、書面で通知を再送しなければならない。サイバートラストは、加入契約において他の形式の通知を許可する場合もある。

9.12. 改訂

9.12.1. 改訂手続

本 RPS は、年 1 回レビューされる。CTJ PA による事前承諾無しに本 RPS の変更および公開が行われないよう合理的な範囲で確実にするために、管理策が設けられている。

9.12.2. 通知方法と期間

サイバートラストは、通知およびコメント（notice-and-comment）の期間を保証または設定せず、通知およびバージョン番号の変更を行わずに本 RPS を変更することができる。

9.12.3. OID の変更が必要とされる場合

規定なし

9.13. 紛争解決手続き
紛争の当事者は、何らかの紛争解決メカニズム（裁定または全ての種類の代替的紛争解決手段を含む）を用いる前に、サイバートラストに通知しサイバートラストとの間で直接的な紛争解決を試みるよう求められている。

9.14. 準拠法
本 RPS およびサイバートラストの製品およびサービスに関連する全ての法的手続き（不法行為請求を含む）についての（文理的）解釈、（法的効果等の）解釈、および執行は、抵触法の原則に関わらず、日本の法律に準拠する。本 RPS またはサイバートラストサービスに関連する法的手続きについては、日本に所在する裁判所に非専属的な裁判籍が存在し同州が非専属的管轄権を有する。

9.15. 適用法の遵守
本 RPS は、全ての適用法令の適用対象である。

9.16. 雑則
9.16.1. 完全合意
サイバートラストは、当社の製品およびサービスを使用する各当事者に対してその製品またはサービスに関連する条件を規定する契約を交わすよう求めている。契約上に本 RPS と異なる規定が含まれている場合、当該当事者との契約が（その当事者についてのみ）優先する。第三者は、かかる契約に依拠することはできず、かかる契約の法的強制を求める訴訟を提起できない。

9.16.2. 譲渡
本 RPS に基づき業務を行う全てのエンティティは、サイバートラストから書面による事前承諾を得ずには、自らの権利または義務を譲渡できない。当事者との契約に別段の規定がない限り、サイバートラストは譲渡についての通知を行わない。

9.16.3. 可分性
本 RPS の何れかの規定が、管轄権を有する裁判所または法廷により無効または法的強制力無しとされた場合でも、本 RPS の残りの部分は有効性および法的強制力を持ち続ける。責任の制限、保証の免責、または損害の免責について定める本 RPS の各規程は、他のいかなる規程からも分離可能かつ独立したものである。

9.16.4. 強制執行（弁護士費用および権利の放棄）
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。サイバートラストが本 RPS 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 RPS 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。サイバートラストが署名した書面による場合にのみ、権利の放棄が有効となる。

9.16.5. 不可抗力
サイバートラストが本 RPS に基づく義務の履行を遅延させまたは怠った場合でも、かかる遅延または懈怠がサイバートラストの合理的な管理を超えた事象の発生に起因する範囲については、サイバートラストは責任を負わない。インターネットの運用は、サイバートラストの合理的な管理を超えるものである。

9.17. その他の規程
規定なし