SECOM TLS サーバー証明書ポリシー

Version 1.03

2024 年 10 月 23 日

セコムトラストシステムズ株式会社

改版履歴		
版数	日付	内容
1.00	2024/04/01	初版発行
1.01	2024/05/17	以下を更新 7.1 証明書のプロファイル
1.02	2024/08/21	以下を更新 1.3.1 CA 1.3.2 RA 1.3.3　証明書利用者 1.3.4 検証者 1.6 定義と略語 2.1 リポジトリー 2.2 証明情報の公開 3.2.2 組織の認証 4.1.2 申請手続および責任 4.2.1 本人性確認と認証の実施 4.9.1 証明書失効事由 4.9.7 証明書失効リストの発行頻度 6.1.1 鍵ペアの生成 7.1 証明書のプロファイル 7.2 CRL のプロファイル 7.2.2 CRL 拡張 以下を削除 4.2.4 CAA レコードの確認
1.03	2024/10/23	表記の修正 以下を更新 1.5.2 連絡先 1.6 定義と略語 2.2 証明情報の公開 3.2.2.4 ドメインの認証 3.2.2.9 マルチ・パースペクティブ発行検証 4.3.1.1 ルート CA の証明書発行の手動承認 4.3.1.2 署名される証明書のリンティング 4.3.1.3 発行済み証明書のリンティング 4.9.11 利用可能な失効情報の他の形式 6.2.1 暗号装置の標準および管理

		6.2.7 私有鍵の暗号モジュールへの格納 7.1.1 バージョン番号 7.1.2 証明書拡張 7.1.8 ポリシー修飾子の文法および意味 7.2.1 バージョン番号

目次

1. はじめに

1.1 概要

本 CP は、セコムトラストシステムズ株式会社（以下「当社」という）が運用する TLS サーバー証明書の利用目的、適用範囲、利用者手続を示し、証明書に関するポリシーを規定するものである。本 CA の運用維持に関する諸手続については、セコム電子認証基盤認証運用規程（以下「CPS」という）に規定する。

「Security Communication RootCA 下位 CA 用証明書ポリシー」に準拠している下位 CA（以下「本 CA」という）から証明書の発行を受ける者は、証明書の発行を受ける前に自己の利用目的と本 CP および CPS とを照らし合わせて評価し、承諾する必要がある。

本 CA は、https://www.cabforum.org/で公開される CA/Browser Forum で定められた規準およびアプリケーションソフトウェアサプライヤーの規準の最新版に準拠する。

表 1.1-1 規準一覧

下位 CA で発行する証明書種類	準拠するべき規準
TLS サーバー証明書	● Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates（以下、Baseline Requirements という） ● Guidelines for the Issuance and Management of Extended Validation Certificates (EV 証明書のみが対象。以下、EV Guidelines という） ● Apple Root Certificate Program ● Chrome Root Program Policy ● Microsoft Trusted Root Program ● Mozilla Root Store Policy

本 CA は、認証業務の一部を Baseline Requirements に準拠した外部の事業者に委託する場合があり（以下「外部委託先」という）、二社間の契約については PB-SSL/TLS 証明書発行サービス約款に定めるものとする。

なお、本 CP の内容が「サービス利用規定または PB-SSL/TLS 証明書発行サービス約款」（以下「サービス利用規定等」という）、CPS の内容に抵触する場合は、サービス利用規定等、本 CP、CPS の順に優先して適用されるものとする。また、当社と契約関係を持つ組織団体等との間で、別途契約書等が存在する場合、サービス利用規定等、本 CP、CPS より契約書等の文書が優先される。本 CP と Baseline Requirements の間に矛盾がある場合、

Baseline Requirements が本 CP に優先して適用される。

本 CP は、本 CA に関する技術面、運用面の発展や改良にともない、それらを反映するために必要に応じ改訂されるものとする。

本 CP は、IETF が認証局運用のフレームワークとして提唱する RFC 3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。

1.2 文書名と識別

本 CP は、表「1.2-1 OID（本 CP)」に示す OID により識別される。

表 1.2-1 OID（本 CP）

CP	OID
SECOM TLS OV CP	1.2.392.200091.100.752.1
SECOM TLS DV CP	1.2.392.200091.100.752.2
SECOM Passport for Web EV 認証局 CP	1.2.392.200091.100.721.1

本 CP に関連する CPS の OID を表「1.2-2 OID（CPS)」に示す。

表 1.2-2 OID（CPS）

CPS	OID
セコム電子認証基盤認証運用規程	1.2.392.200091.100.401.1

1.3 PKI の関係者

1.3.1 CA

CA は、証明書の作成、発行、失効、管理に対して責任を負う組織である。ルート CA と下位 CA の両方に同意で使用される。

1.3.2 RA

証明書の主体者の識別および認証を担当する法人組織。ただし、CA ではないため、証明書の署名や発行は行わない。RA は、証明書申請プロセスまたは失効プロセス、あるいはその両方を支援する。RA が役割や機能を指すために用いられる場合は、必ずしも別の組織体を示唆するものではなく、本 CA の一部である可能性がある。

本 CP「3.2.2.4　ドメインの認証」および本 CP「3.2.2.5 IP アドレスの認証」を除き、

本 CA は本 CP「3.2 初回の本人確認」の要件のすべてまたは一部の遂行を第三者に委託することができる。ただし、プロセス全体として、本 CP「3.2 初回の本人確認」の要件のすべてを満たすことを条件とする。

本 CA は、委託した職務の遂行を許可する前に、契約を通じて下記を委託先に要求する。

1. 委託した職務に該当する場合、CPS「5.3.1 資格、経験および身分証明の要件」の資格要件を満たす。
2. CPS「5.5.2 アーカイブ保存期間」に従い、ドキュメントを保持する。
3. Baseline Requirements 以外にも、委託された職務に適用される条件を遵守する。
4. 以下のいずれかに準拠する。
   a. 本 CA の CP/CPS。
   b. 本 CA が Baseline Requirements に準拠していることを認定した委託先の運用規定。

1.3.3 利用者

利用者とは、証明書の発行先であり、利用契約または利用規約を遵守する自然人または法人をいう。

1.3.4 検証者

検証者とは、有効な証明書に依拠する自然人または法人。アプリケーションソフトウェアサプライヤーによって配布されるソフトウェアが単に証明書に関連する情報を表示するだけの場合、そのサプライヤーは検証者とは見なされない。

1.3.5 他の関係者

他の関係者とは、監査人や当社との間でサービス契約等が存在する企業や組織、そのシステムインテグレーションを行う業者などが含まれる。

1.4 証明書の用途

1.4.1 適切な証明書の用途

本 CA が発行する証明書は、TLS プロトコルを介して Web ベースのデータ通信経路を確立し、実行可能コードの信頼性を検証することを目的としている。

EV 証明書の主な目的は次のとおりである。

1. Web サイトを管理する法人を特定する。
   インターネット ブラウザのユーザーに、ユーザーがアクセスしている Web サイト

が、名前、事業所の住所、EV 証明書で特定される特定の法人によって管理されていることを合理的に保証する。設立または登録の管轄区域および登録番号またはその他の曖昧さを解消する情報。

2. Web サイトとの暗号化通信を有効にする。
   インターネット ブラウザのユーザーと Web サイトの間でインターネットを介した情報の暗号化通信を可能にするために、暗号化キーの交換を容易にする。

EV 証明書の第 2 の目的は、Web サイトの運営または実行可能コードの配布を主張する組織の正当性を確立するのに役立ち、フィッシング、マルウェア、およびその他の形式に関連する問題への対処を支援するために使用できる手段を提供することである。オンラインでのなりすまし詐欺が該当する。 EV 証明書は、ビジネスに関するより信頼性の高い第三者検証の身元情報と住所情報を提供することで、次のことに役立つ。

1. 証明書を使用したフィッシングやその他のオンライン ID 詐欺攻撃をより困難にする。
2. フィッシング攻撃やオンライン ID 詐欺の標的となる可能性のある企業を支援するため、ユーザーに対して自社をより適切に識別できるツールを提供する。
3. 法執行機関によるフィッシングやその他のオンライン ID 詐欺の調査を支援する。これには、必要に応じて、対象者への連絡、調査、または法的措置の実施も含まれる。

1.4.2 禁止される証明書の用途

本 CA が発行する証明書は、サーバー認証や通信経路でデータの暗号化を行うこと以外に証明書を利用してはならない。

本 CA は、本 CP「3.2.2.4　ドメインの認証」に従って検証したドメイン所有者からドメインの利用権を有しているか確認した場合を除いて、証明書発行を許可しない。

EV 証明書は、証明書に指定されている主体者の身元のみに焦点を当てており、主体者の動作には焦点を当てていない。したがって、EV 証明書は、以下のことを保証したり、表明または保証したりすることを目的としてはいない。

1. EV 証明書に名前が記載されている対象者が積極的にビジネスに従事している。
2. EV 証明書に指定されている対象者が適用法を遵守している。
3. EV 証明書に名前が記載されている対象者が、ビジネス取引において信頼できる、誠実である、または評判が良い。
4. EV 証明書に指定されている主体者と取引するのが「安全」である。

1.5 ポリシー管理

1.5.1 文書を管理する組織

本 CP の維持・管理は当社が行う。

1.5.2 連絡先

本 CP に関する問い合わせ先は次のとおりである。

問い合わせ窓口	セコムトラストシステムズ株式会社 CA サポートセンター
住所	〒181-8528　東京都三鷹市下連雀 8-10-16

問い合わせ内容	本 CP に関する問い合わせ 証明書に関する問題報告（Certificate Problem Report）を除く
E-mail	ca-support@secom.co.jp
受付対応時間	9:00～18:00（土日・祝日および年末年始を除く）

利用者、依拠当事者、アプリケーションソフトウェアサプライヤー、その他の第三者は、私有鍵の危殆化の疑い、証明書の誤用、あるいはその他の種類の詐欺、危殆化、誤用、不適切 な行為、または証明書に関連するその他の事項について、以下の連絡先に報告することができる。本 CA では、失効する必要があると判断した場合、証明書を失効する。

問い合わせ内容	証明書に関する問題報告（Certificate Problem Report）
URL	https://www.secomtrust.net/sts/cert/report_entry.html
受付対応時間	24 時間 365 日（24x7）

1.5.3 ポリシー適合性を決定する者

本 CP の内容については、認証サービス改善委員会（以下「本委員会」という）が適合性を決定する。本 CP は、最低でも年次でレビューし、改訂する。

1.5.4 承認手続

本CPは、本CAの本委員会の承認によって発効する。

1.6 定義と略語

五十音順（あ行～わ行）

アーカイブ

法的またはその他の事由により、履歴の保存を目的に取得する情報のことをいう。

アプリケーションソフトウェアサプライヤー(Application Software Supplier)

証明書を表示または使用し、ルート CA 証明書を組み込むインターネットブラウザソフトウェアまたはその他の依拠当事者アプリケーションソフトウェアのサプライヤー。

依拠当事者(Relying Party)

有効な証明書に依拠する個人または法人。アプリケーションソフトウェアサプライヤーによって配布されるソフトウェアが単に証明書に関連する情報を表示するだけの場合、そのサプライヤーは依拠当事者とは見なされない。

エスクロー

第三者に預けること（寄託）をいう。

鍵ペア

公開鍵暗号方式において、私有鍵と公開鍵から構成される鍵の対のことをいう。

監査ログ

認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局システムの動作履歴やアクセス履歴等をいう。

公開鍵

公開鍵暗号方式において用いられる鍵ペアの一方をいい、私有鍵に対応し、通信相手の相手方に公開される鍵のことをいう。

事前証明書

RFC 6962 で定義された、証明書の CT ログに送信できる署名付きデータ構造をいう。事前証明書は、CA が証明書の発行を決定した後、証明書の署名の前に作成される。CA は、証明書の CT ログに送信する目的で、証明書に対応する事前証明書を作成して署名する。CA は、返された署名付き証明書のタイムスタンプを使用して証明書のフィールドを変更し、Baseline Requirements 7.1.2.11.3 で定義され、関連するプロファイルで許可されている署名付き証明書のタイムスタンプリストを追加して、証明書に署名する。

私有鍵

公開鍵暗号方式において用いられる鍵ペアの一方をいい、公開鍵に対応する本人のみが保有する鍵のことをいう。

ショートリブド利用者証明書(Short-lived Subscriber Certificate)

2024 年 3 月 15 日以降かつ 2026 年 3 月 14 日以前に発行される証明書で有効期間が 10 日（864,000 秒）以下の利用者証明書。2026 年 3 月 15 日以降に発行される証明書で有効期間が 7 日（604,800 秒）以下の利用者証明書。

タイムスタンプ

電子ファイルの作成日時やシステムが処理を実行した日時等を記録したデータのことをいう。

電子証明書

ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CA が電子署名を施すことで、その正当性が保証される。

認証ドメイン名：ADN（Authorization Domain Name）

特定の FQDN に対して、証明書発行のための認証を取得するために使用されるドメイン名

認証書（Attestation Letter）

会計士、弁護士、政府関係者、またはその他の信頼できる第三者によって書かれた、主体者情報が正しいことを証明する文書。

リポジトリー

CA 証明書および CRL 等を格納し公表するデータベースのことをいう。

アルファベット順（A～Z）

Baseline Requirements

CA/Browser Forum が証明書の発行･管理に関する基本要件を定めた文書のことをいう。

CA（Certification Authority）：認証局

証明書を発行する認証局であり、証明書の発行・更新・失効、CA 私有鍵の生成・保護および利用者の登録等を行う主体のことをいう。本 CP では発行局（IA:Issuing Authority）も含まれる。

CAA (Certificate Authority Authorization)

ドメインを使用する権限において、DNS レコードの中にドメインに対して証明書を発行できる認証局情報を記述し、意図しない認証局からの証明書誤発行を防ぐ機能をいう。

CA/Browser Forum

認証局とインターネット・ブラウザベンダによって組織され、証明書の要件を定義し、標準化する活動をしている非営利団体組織である。

CP（Certificate Policy）

CA が発行する証明書の種類、用途、申込手続等、証明書に関する事項を規定する文書のことをいう。

CPS（Certification Practices Statement）：認証運用規程

CA を運用する上での諸手続、セキュリティ基準等、CA の運用を規定する文書のことをいう。

CRL（Certificate Revocation List）：証明書失効リスト

証明書の有効期間中に、証明書記載内容の変更、私有鍵の紛失等の事由により失効された証明書情報が記載されたリストのことをいう。

CSPRNG（Cryptographically Secure Pseudo Random Number Generator）：暗号論的擬似乱数生成器

暗号システムで使用されることを目的とした乱数生成器。

CT（Certificate Transparency）

RFC 6962 で規定され、発行された証明書の情報を監視・監査するためにログサーバーに証明書の情報を登録し、公開する仕組みのことをいう。

EV Processes：EV プロセス

EV Guidelines に基づく証明書データの検証、EV 証明書の発行、リポジトリーの保守、および EV 証明書の失効に用いられる鍵、ソフトウェア、プロセス、および手順。

FIPS 140

米国 NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準のこという。

HSM（Hardware Security Module）

私有鍵の生成、保管、利用などにおいて、セキュリティを確保する目的で使用する耐タンパー機能を備えた暗号装置のことをいう。

INAN (Internet Assigned Numbers Authority)

IP アドレスやポート番号など、インターネットに関連する情報をグローバルに管理している団体のことをいう。

Linting：リンティング

事前証明書[RFC 6962]、証明書、CRL、OCSP レスポンスなどの電子署名されたデータまたは RFC 5280 セクション 4.1.1.1 に記述されているような署名されるデータオブジェクトの内容が、Baseline Requirements に定義されるプロファイルおよび Baseline Requirements に準拠しているか確認するプロセス。

Multi-Perspective Issuance Corroboration：マルチ・パースペクティブ発行検証

証明書発行前に、プライマリー・ネットワーク・パースペクティブによるドメイン検証、CAA チェックで行われた決定が、他のネットワーク・パースペクティブによって検証されるプロセス。

Network Perspective：ネットワーク・パースペクティブ

Multi-Perspective Issuance Corroboration に関連する。ドメイン管理検証方法または CAA チェックに関連するアウトバウンド・インターネット・トラフィックを送信するためのシステム（例えば、クラウド・ホスト・サーバー・インスタンス）またはネットワーク・コンポーネントの集合体（例えば、VPN および対応するインフラストラクチャー）。ネットワーク・パースペクティブの場所は、通常、カプセル化されていないアウトバウンドインターネットトラフィックが、そのパースペクティブへのインターネット接続を提供するネットワークインフラに最初に引き渡されるポイントによって決定される。

OID（Object Identifier）：オブジェクト識別子

ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。

OCSP（Online Certificate Status Protocol）

証明書のステータス情報をリアルタイムに提供するプロトコルのことをいう。

PKI（Public Key Infrastructure）：公開鍵基盤

電子署名、暗号化、認証といったセキュリティ技術を実現するための、公開鍵暗号方式

という暗号技術を用いる基盤のことをいう。

Primary Network Perspective：プライマリー・ネットワーク・パースペクティブ

CA が、1)申請されたドメインまたは IP アドレスに証明書を発行する CA の権限、2)申請されたドメインまたは IP アドレスに対する申請者の権限、ドメインの承認または管理権限を判断する際に使用するネットワーク・パースペクティブをいう。

RA（登録局）（Registration Authority）：登録機関

CA の業務のうち、申込情報の審査、証明書発行に必要な情報の登録、CA に対する証明書発行要求、リポジトリーの維持・管理等を行う主体のことをいう。

RFC 3647（Request For Comments 3647）

インターネットに関する技術の標準を定める団体である IETF（The Internet Engineering Task Force）が発行する文書であり、CP/CPS のフレームワークを規定した文書のことをいう。

RSA

公開鍵暗号方式として普及している最も標準的な暗号技術のひとつである。

SHA-1（Secure Hash Algorithm 1）

電子署名に使われるハッシュ関数（要約関数）のひとつである。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいう。ビット長は 160 ビット。データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

SHA-256（Secure Hash Algorithm 256）

電子署名に使われるハッシュ関数（要約関数）のひとつである。ビット長は 256 ビット。データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

WebTrust for CA

CPA Canada によって、認証局の信頼性、および、電子商取引の安全性等に関する内部統制について策定された基準およびその基準に対する認定制度である。

WebTrust for CA - Extended Validation SSL

CPA Canada によって、認証局が EV TLS 証明書を発行するにあたっての審査、証明書

に関する規定について策定された監査基準である。

WebTrust for CA - SSL Baseline with Network Security

CPA Canada によって、認証局が TLS 証明書を発行するにあたっての審査、証明書に関する規定について策定された監査基準である。

WHOIS

RFC 3912 で定義されたプロトコル、RFC 7482 で定義されたレジストリデータアクセスプロトコル、または HTTPS ウェブサイトを介してドメイン名レジストラまたはレジストリ運営者から直接取得された情報。

X.500

ネットワーク上での分散ディレクトリサービスに関する、コンピュータネットワーク標準規格のシリーズのことをいう。

2. 公開とリポジトリーの責任

2.1 リポジトリー

本 CA は､本 CP に基づき下位 CA 証明書と利用者証明書に対する失効情報を提供する。

2.2 証明情報の公開

本 CA は、CP/CPS を、24 時間 365 日利用可能な適切で容易にアクセスできるオンライン手段を通して公開する。本 CA は、本 CA が選択した監査スキーム(本 CP「8.4 監査で扱われる事項」を参照)によって必要とされる範囲内で本 CA の実務を公開する。

CP/CPS は、RFC 3647 に従って構成され、RFC 3647 が要求するすべての事項を含む。

本 CA が遵守する規準については、「1.1 概要」に記載する。

本 CA は、アプリケーションソフトウェアサプライヤーが各パブリックルート証明書までつながる利用者証明書を使用してソフトウェアをテストできるようにテストウェブページをホストする。

本 CA は、以下の利用者証明書を使用したウェブページをそれぞれホストする。

i. 有効。

ii. 失効。

iii. 有効期限切れ。

2.3 公開の時期または頻度

本 CA は、Baseline Requirements の最新バージョンをどのように実施するかを詳細に記述した CP および CPS の策定、導入、施行、年次更新を行うものとする。本 CA は、CP および CPS に変更が加えられていない場合でも、バージョン番号を増やし、変更履歴を追加することにより、Baseline Requirements への準拠を示す。

2.4 リポジトリーへのアクセス管理

本 CA はリポジトリーを読み取り専用の形で公開するものとする。本 CA では、許可された CA 管理者のみがリポジトリーの追加、削除、変更、公開などの操作を実行できる。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

本 CA が発行する証明書は、X.509 規格、RFC 5280 規格および Baseline Requirements の要求事項を満たし、証明書所有者に割り当てられる識別名は X.500 の識別名形式に従い設定する。

本 CA が発行する証明書には下記の情報を含むものとする。

1. 「countryName（国名）」（C）は日本国の 2 文字の ISO 3166-1 国コード略号である JP とする。（OV 証明書と EV 証明書）
2. 「organizationName（組織名）」（O）とは、法人、会社、またはその他の法人からなる組織および個人事業主の名称とする。「stateOrProvinceName（都道府県名）」（ST）および「localityName（市区町村名）」（L）には、組織の地域情報を含める（OV 証明書と EV 証明書）

   EV 証明書は、EV Guidelines Appendix D-1 に従い以下の表記とする。

   A. 日本語のローマ字表記は、修正ヘボン式、ISO 3602 に記載されている訓令式、日本式が使用可能である。

   B. 本 CA は、申請者の正式な法的名称のローマ字変換、言語翻訳（英語名など）、またはその他の公認のローマ 字変換を適格独立系情報源（以下、QIIS という）、Verified Legal Opinion、または Verified Accountant Letter で検証することができる。

   C. 本 CA は、ローマ字、翻訳、またはその他の一般的なローマ字の代用名を検証するために、金融庁の情報を使用することができる。使用した場合、CA は、翻訳された英語が監査済み財務諸表に記録されていることを検証しなければならない。

   D. ローマ字、翻訳、あるいはその他の一般に認められたローマ字の代替名称を検証するために定款に依拠する場合は、法人の代表者印で押印された定款が真正かつ最新であることを証明する文書、 あるいは検証済みの公認会計士または弁護士からの意見書を添付しなければならない。その場合、本 CA は、法人の代表者印の真正性を確認しなければならない。
3. 「commonName（コモンネーム）」（CN）は主要なドメイン名であり、Subject Alternative Name に存在するドメイン名とする。ドメイン名は、すべて Subject Alternative Name に追加される。（DV 証明書、OV 証明書および EV 証明書）
4. Subject Alternative Name 拡張領域の dNSName エントリー値に ASCII 文字列以外の国際文字が含まれる場合、puny-code に変換された文字列が使用され

る。（DV 証明書、OV 証明書および EV 証明書）

3.1.2 名前が意味を持つことの必要性

本 CA が発行する証明書に用いられるコモンネームの有用性は、利用者が 本 CA が発行する証明書をインストールする予定の Web サーバーの DNS 内で使われるホスト名とする。

3.1.3 利用者の匿名性または仮名性

本 CA が発行する証明書は、匿名や仮名での登録は行わない。

3.1.4 様々な名前形式を解釈するための規則

様々な名前の形式を解釈する規則は、X.500 シリーズの識別名規定に従う。

3.1.5 名前の一意性

本 CA では、発行された証明書が、主体者の識別名に含まれる情報により、証明書の所有者を一意に識別できることを保証する。証明書のシリアルナンバーは、CSPRNG で生成した乱数を含むシリアルナンバーとする。本 CA 内で割り当てられたシリアルナンバーは一意である。

3.1.6 認識、認証および商標の役割

本 CA は、証明書申請に記載される名称について、知的財産権を有しているかどうかの検証を行わない。利用者は、第三者の登録商標や関連する名称を、本 CA に申請してはならない。本 CA は、登録商標等を理由に利用者と第三者間で紛争が起こった場合、仲裁や紛争解決は行わない。また、紛争を理由に利用者からの証明書申請の拒絶や発行された証明書失効をする権利を有する。

3.2 初回の本人確認

3.2.1 私有鍵の所持を証明する方法

利用者が私有鍵を所有していることの証明は、次の方法で行う。

証明書発行要求（Certificate Signing Request：以下、「CSR」という）の署名の検証を行い、当該 CSR が、公開鍵に対応する私有鍵で署名されていることを確認する。

3.2.2 組織の認証

申請者が countryName フィールドのみから成る主体者識別情報を含む証明書を申請する場合、本 CA は、本 CP「3.2.2.3 国の検証」ならびに本 CA の CP および CPS に記載さ

れた要件を満たした検証プロセスを使用して、主体者に関連付けられた国を検証する。申請者が countryName フィールドとその他の主体者識別情報を含む証明書を申請する場合、本 CA は、本 CP「3.2.2.1 アイデンティティ」ならびに本 CA の CP および CPS に記載された要件を満たした検証プロセスを使用して、申請者のアイデンティティと、申請権限者の証明書要求の信頼性を検証する。本 CA は、本セクションに基づいて信頼されたドキュメントに改編や偽造がないか検査する。

EV 証明書発行時に使用する検証ソースは、以下 URL にて開示する。
https://www.secomtrust.net/service/pfw/apply/ev/list.html

【EV 証明書】
EV 証明書の場合、申請者の法的存在と身元を確認するため、本 CA は次のことを実行する。

民間組織が主体者の場合

A. 法的存在: 申請者が法的に認められた法人であり、申請者の設立または登録管轄区域内で現存し、登録機関に有効に設立され（例: 法人化され）、法人の設立機関または登録機関の記録に以下が指定されていないことを確認する。 「非活動」、「無効」、「最新ではない」、または同等のラベルであること。

B. 組織名: 申請者の設立または登録管轄区域内の設立または登録機関に記録された申請者の正式な法名が、EV 証明書リクエストの申請者の名前と一致することを確認する。

C. 登録番号: 申請者の設立または登録管轄区域内の設立または登録機関によって申請者に割り当てられた特定の登録番号を取得する。設立機関または登録機関が登録番号を割り当てていない場合、本 CA は申請者の設立日または登録日を取得する。

D. 登録代理人: 申請者の登録代理人または登録事務所の身元および住所を取得する（申請者の設立または登録の管轄区域に該当する場合）。

政府機関が主体者の場合

A. 法的存在: 申請者が法的に認められた政府機関であり、その政府機関が運営される政府部門に存在することを確認する。

B. エンティティ名: 申請者の正式な法人名が EV 証明書リクエストの申請者の名前と一致することを確認する。

C. 登録番号: 本 CA は、申請者の設立、登録、設立の日付、または政府機関を創設した法律上の識別子の取得を試みる。この情報が利用できない状況では、本 CA は対象が政府機関であることを示す適切な言語を入力する。

事業体が主体者の場合

A. 法的存在: 申請者が申請書で提出した名前で事業に従事していることを確認する。

B. 組織名: 申請者の登録管轄区域内の登録機関によって認識されている申請者の正式な法名が、EV 証明書リクエストの申請者の名前と一致することを確認する。

C. 登録番号: 申請者の登録管轄区域内の登録機関によって申請者に割り当てられた、特定の一意の登録番号の取得を試みる。登録機関が登録番号を割り当てない場合、本 CA は申請者の登録日を取得するものとする。

D. 主要な個人: 特定された主要な個人の身元を確認する。

非営利団体が主体者の場合(国際機関)

A. 法的存在: 申請者が法的に認められた国際機関実体であることを確認する。

B. エンティティ名: 申請者の正式な法人名が EV 証明書リクエストの申請者の名前と一致することを確認する。

C. 登録番号: 本 CA は、申請者の設立日、または国際機関を創設した法律上の識別子の取得を試みる。この情報が利用できない状況では、本 CA は主体者が国際組織であることを示す適切な言語を入力する。

申請者の正式な法的名称に加えて、申請者の設立または登録の管轄区域内の該当する設立機関または登録機関に記録されているとおり、EV 証明書で主張されている申請者の身元に、屋号が含まれる場合、申請者がビジネスを行う場合、本 CA は次のことを検証する。

i. 申請者は、その事業所の管轄区域内でそのような届出を行うための適切な政府機関に屋号の使用を登録していること（EV Guidelines に従って確認）

ii. そのような届出は引き続き有効であること。

申請者の物理的な存在とビジネス上の存在を検証するために、本 CA は、申請者が提供した物理的な住所が、申請者、親会社または子会社が事業活動を行っている住所であることを検証する。

A. 設立または登録国の事業所

i. 事業所が申請者の法人設立/登録管轄地と同じ国にあり、かつ事業所が法的 存在を確認するために使用した関連する適格政府情報源（以下、QGIS という）に示されたものと同じでない申請者。

1. 少なくとも 1 つの QGIS(法的実在性を検証するために使用されるもの以外)、QIIS の最新版 に同じ事業所住所が記載されている申請者について、

本 CA は、QGIS、QIIS を参照することで、EV 証明書要求に記載された申請者の住所が、申請者または親会社または子会社の有効な事業所住所であることを確認しなければならず、当該住所が事業所であるという申請者の表明に依拠してもよい。

2. 少なくとも 1 つの QIIS の最新版に同じ事業所住所が記載されていない申請者の場合、本 CA は、信頼できる個人または会社によって実施されなければならない事業所住所の現地訪問の文書を入手して、EV 証明書要求で申請者が提供した住所が申請者または親会社または子会社の事業所住所であることを確認しなければならない。現地視察の文書は以下のものとする。

a. 申請者の事業所が EV 証明書要求に記載された正確な住所にあることを確認する(例：常設の看板、従業員の確認など)、

b. 施設の種類(商業ビル内の事務所、個人住宅、店舗など)と常設の事業所かどうかを確認する

c. 申請者を示す常設の看板（移動できないもの）があるかどうか。

d. 申請者がその場所で継続的な事業活動を行っていることを示す証拠があるかどうか（郵便物の投函、私書箱などではない)。

e. 以下の写真を 1 枚以上添付する。

i. 敷地の外観（申請者の名前を示す看板がある場合はそれを示し、可能であれば住所を示す)。

ii. 内部の受付エリアまたはワークスペース。

ii. すべての申請者について、本 CA は、申請者、親会社または子会社の事業所の住所を示し、そこで業務が行われていることを示す検証済みの公認会計士または弁護士等の専門家から提出される意見書を代わりに信頼してもよい。

iii. 政府機関申請者の場合、本 CA は、申請者の管轄地域の QGIS の記録に含まれる住所に依拠してもよい。

iv. 事業所が申請者の法人設立/登録管轄地と同じ国にあり、QGIS が申請者の事業所住所を含む場合、本 CA は、EV 証明書要求に記載された申請者、親会社または子会社の住所を確認するために、QGIS の住所に依拠してもよい。

B. 設立国または登録国にない事業所: CA は、申請者の事業所の住所とそこで業務が行われていることを示す検証済みの公認会計士または弁護士等の専門家から提出される意見に依存する。

申請者との通信を支援し、申請者が発行を認識し承認していることを確認するために、本 CA は申請者との検証済み通信方法として電話番号､ファックス番号､Email アドレス、または郵便配達先住所を検証する。

申請者との検証済み通信方法を検証するには、CA は次のことを行う。

A. 検証された通信方法が申請者または申請者の親会社、子会社または関連会社のものであることを、次の申請者の親会社、子会社または関連会社の事業所のいずれかと照合することにより検証する。

i. 該当する電話会社によって提供される記録。

ii. QGIS または QIIS。

iii. 検証済みの公認会計士または弁護士等の専門家から提出される意見書。

B. 検証済みの通信方法を使用して、合理的な人が申請者または申請者の親会社、子会社または関連会社に確実に連絡できると結論付けるのに十分な応答を得るために、検証済みの通信方法を使用して確認する。

本 CA は、申請者、関連会社/親会社/子会社の事業体としての実在を検証することで、申請者が事業に携わる能力を持つことを確認しなければならない。本 CA は、政府組織の事業体としての実在を検証するにあたって、EV Guidelines セクション 3.2.2.2 に基づく政府組織の法的実在の検証結果を根拠としてもよい。

申請者の事業遂行能力を検証するため、本 CA は、申請者またはその関連会社/親会社/子会社を、次の方法で検証しなければならない。

1. 申請者、関連会社、親会社、または子会社が、設立機関や登録機関の記録に示されるとおり、少なくとも 3 年間にわたって存在していることを検証する。
2. 申請者、関連会社、親会社、または子会社が最新の QIIS または QTIS に記載されているか検証する。
3. 申請者、関連会社、親会社、または子会社が、認可された金融機関から直接、申請者、関連会社、親会社、または子会社 の預金口座の証明書を受領することにより、認可された金融機関に有効な現行のデモ口座と預金口座を持つことを検証する、
4. 申請者が認可された金融機関に有効な預金口座を持っていることを示す照会書に依拠する。

Onion ドメイン名ではない証明書にリストされている FQDN ごとに、本 CA は、証明書が発行された日の時点で、申請者が、ドメイン名登録者であるか、Baseline Requirements セクション 3.2.2.4 で指定された手順を使用して FQDN を制御できる。

混合文字セットのドメイン名について、 EV 証明書は、ドメインレジストラが定めた規則に従っている場合にのみ、混合文字セットを含むドメイン名を含めることができる。本 CA は、文字セットが混在しているドメイン名を、既知の高リスクドメインと視覚的に比較する。類似性が見つかった場合は、EV 証明書リクエストに高リスクのフラグを立てる。本 CA は、申請者と問題のターゲットが同じ組織であることを合理的な疑いを超えて確実にするために、合理的に適切な追加の認証と検証を実行する。

契約署名者および証明書承認者の両方に関して、本 CA は以下を検証しなければならない。

1. 名前、役職、代理関係

本 CA は適宜、契約署名者と証明書承認者の名前と役職を検証しなければならない。CA はさらに、契約署名者と証明書承認者が、申請権限者であることを検証しなければならない。

2. 契約署名者の署名権限

本 CA は、契約署名者が申請者の代わりに利用契約(およびその他関連する契約上の義務)を締結する権限を申請者によって与えられていることを検証しなければならない。これには、申請者の代わりに 1 名以上の証明書承認者を指定する契約も含まれる。

3. 証明書承認者の EV 権限

本 CA は、証明書承認者自身以外のソースを通じて、証明書承認者が EV 証明書要求の日付時点で以下を実施する権限を申請者から明示的に与えられていることを確認しなければならない。

A. 申請者の代わりに EV 証明書要求を提出する、または該当する場合、証明書要求者に提出させる権限

B. EV 証明書の発行にあたって、本 CA が申請者に要求した情報を提供する、または該当する場合、証明書要求者に提供させる権限

C. 証明書要求者によって提出された EV 証明書要求を承認する権限

本 CA と申請者が今後、複数の EV 証明書要求を提出する予定である場合、本 CA はまず下記を行う。

1. 契約署名者の氏名と役職、ならびに署名者が申請者の従業員または代理人であることを検証する。

2. EV Guidelines セクション 3.2.2.8.3 の手続きのいずれかに基づいて、かかる契約署名者の署名権限を検証する。

その後、本 CA と申請者は、申請者の代わりに契約署名者によって署名された契約書を締結することにより、指定された期間、かかる契約書で指定された 1 名以上の証明書承認者に対し、申請者の代わりに提出され、かかる証明書承認者によって発せられた、または承認されたものとして正式に認証された将来の各 EV 証明書要求に関して、EV 権限を行使することを明示的に許可することができる。

契約書には、当該証明書承認者の要求によって、または承認によって発行されたすべての EV 証明書に対し、EV 権限が取り消されるまで、申請者が利用契約に基づく義務を負う旨を記載する。

i. EV 証明書要求が承認されるときに証明書承認者の認証を行う

ii. 証明書承認者の EV 権限を定期的に再確認する
iii. 申請者が、証明書承認者の EV 権限が取り消されたことを CA に通知する手順を確保する
iv. その他の適切な予防措置が相当程度に必要であることに関して、相互に合意した条項を含める必要がある。

利用契約と、事前認証されていない EV 証明書にはそれぞれ、署名しなければならない。利用契約書には、権限のある契約署名者による署名が必要である。EV 証明書要求には、EV Guidelines のセクション 3.2.2.8.4.に基づいて証明書要求が事前認証されていない限り、ドキュメントを提出する証明書要求者による署名がなければならない。証明書要求者が権限のある証明書承認者でない場合、権限のある証明書承認者が EV 証明書要求を別途承認しなければならない。いずれの場合も、適用される署名は、申請者を各ドキュメントの条件に拘束する、法的に有効かつ強制力がある印または手書きの署名(紙の利用契約書または EV 証明書要求の場合)、もしくは法的に有効かつ強制力がある電子署名(電子版の利用契約または EV 証明書要求の場合)でなければならない。

証明書要求者によって EV 証明書要求が送信される場合、本 CA が要求された EV 証明書を発行する前に、本 CA は、認可された証明書承認者が EV 証明書要求を検討して承認したことを確認する。

証明書承認者による EV 証明書リクエストの承認を検証するために許容される方法は次のとおりである。

1. 申請者向けの検証済みの通信方法を使用して証明書承認者に連絡し、証明書承認者が EV 証明書要求を検討して承認したことを口頭または書面で確認する。
2. 指定されたアクセス制御された安全な Web サイトで 1 つ以上の新しい EV 証明書要求のレビューと承認が可能であることを証明書承認者に通知し、その後、証明書承認者が要求する方法でログインし、Web サイトで証明書承認者から承認を示す。
3. EV 証明書要求の証明書承認者の署名を検証する。

本 CA は、申請者、契約署名者、証明書承認者、申請者の設立/登録管轄地、または事業拠点が、以下に当てはまるかどうかを検証しなければならない。

A. いずれかの政府の拒否リスト、禁止顧客リスト、その他、CA の業務管轄地の国の法律でかかる組織や人物と事業を行うことを禁じるその他のリストに記載されている。
B. 設立/登録管轄地、または事業拠点が、CA の管轄地の法律で事業を行うことが禁じられている国内にある。

申請者、契約署名者、または証明書承認者、あるいは申請者の法人設立/登録管轄地または事業拠点のいずれかが当該リストに登録されている場合、CA は、申請者に EV 証明書を

発行してはならない。

最終照合とデューデリジェンス

1. 本ガイドラインに示した検証のプロセスおよび手順の結果は、個別に、かつグループとして見なされることが意図されている。
   よって、全ての検証プロセスと手順が完了したら、本 CA、情報収集担当者とは別の人物に、EV 証明書申請の根拠として収集された全ての情報やドキュメントの見直しをさせ、さらなる説明が必要な矛盾や詳細がないか確認しなければならない。
2. 本 CA は、さらなる説明が必要な矛盾や詳細を解決するため、必要に応じて、申請者、証明書承認者、証明書要求者、適格な独立系情報源、その他の情報源から、さらなる説明や釈明を得て、文書化しなければならない。
3. 本 CA は、EV 証明書要求の根拠として収集された情報や文書全体が、EV 証明書の発行によって伝えられる情報と本 CA が知り得ている事実情報にずれが生じるようなものである場合、またはデューデリジェンスを実行することによって収集された情報や文書が不正確であることが発見されるようである場合、本 CA は EV 証明書の発行を控えなければならない。満足のいく説明や追加文書が妥当な時間内に提出されない場合、本 CA は EV 証明書要求を却下しなければならず、その旨を申請者に通知するべきとする。
4. 申請の裏付けとして使用された一部またはすべてのドキュメントが、通常 CA が業務で使用している言語と異なる場合、本 CA またはその関連会社は、適切な訓練、経験、判断力をもって組織の識別と認証を行い、EV Guidelines セクション 5.3.2 に記載されたすべての資格要件を満たした本 CA または関連会社の管理下にある従業員を用いて、このセクションの最終照合およびデューデリジェンスの要件を実行させる必要がある。本 CA 管理下の従業員が最終照合およびデューデリジェンスの遂行に必要な言語スキルを有していない場合、本 CA は以下を行うことができる。
   A. ドキュメントの関連する部分の翻訳版を用いる。ただし、翻訳は翻訳者が行う。
   B. 本 CA が RA のサービスを利用している場合、本 CA は RA の言語スキルに依拠して、最終照合とデューデリジェンスを遂行してもよい。ただし、RA は EV Guidelines セクション 3.2.2.13、サブセクション(1)、(2)、(3)に準拠する。前述に関わらず、EV 証明書を発行する前に、本 CA は RA が遂行した作業を見直し、すべての要件が満たされていることを確認しなければならない。
   C. 本 CA が RA のサービスを利用している場合、本 CA は RA に依拠して最終照合とデューデリジェンスを遂行してもよい。ただし、RA はこのセクションに準拠し、EV Guidelines セクション 8.1.1 およびセクション 8.2 の監査要件に従う。

EV Guidelines セクション 1.3.2 の要件に基づいてエンタープライズ EV 証明書を発行する場合、エンタープライズ RA がこのセクションの最終照合およびデューデリジェンス

要件を遂行してもよい。

責務の分割

1. 本 CA は、一人の担当者が単独で EV 証明書の検証と発行を許可できないことを保証するために検証義務を分離に関する厳格な管理手順を実施する。EV Guidelines セクション 3.2.2.13 で概説されている最終的な相互相関およびデューデリジェンスの手順は、一人の担当者が実行しても良い。例えば、一人目の検証スペシャリストがすべての申請者の情報を検証し、二人目の検証スペシャリストが TLS サーバー証明書の発行を承認することができる。
2. 本管理は、監査可能とする。

データのセキュリティ

Baseline Requirements のセクション 5 に加えて、EV 証明書要求の処理および承認に使用されるシステムでは、EV 証明書の作成前に、最低 2 名の信頼できる個人による措置がされなければならない。

本 CP「5.5.2 アーカイブ保存期間」に従い、本 CA は、フィッシングまたはその他の詐欺的使用の疑いあるいは懸念を理由に、以前に失効した証明書および以前に拒否した証明書要求をすべて含む内部データベースを保持するものとする。本 CA は、この情報を使用して、以降の疑わしい証明書要求を識別するものとする。

3.2.2.1 アイデンティティ

主体者識別情報が組織の名前または住所を含む場合、本 CA は、組織のアイデンティティや住所を検証し、その住所が申請者の現存する、または稼働している住所であることを確認するものとする。本 CA は、次のうち 1 か所以上から提供されたドキュメントや、それとのやり取りを通じて得られた情報を使用して、申請者のアイデンティティと住所を検証するものとする。

1. 申請者の法的な設立、存在、または承認の管轄地域にある行政機関。
2. 定期的に更新され、信頼できるデータ情報源と見なされている第三者のデータベース。
3. 本 CA あるいは、本 CA の代理人としての役割を担っている第三者による現場訪問。
4. 認証書。

本 CA は、上記 1 から 4 と同じ文書または情報を使用して、申請者のアイデンティティと住所の両方を検証してもよい。

3.2.2.2 商号/商標名

主体者のアイデンティティ情報に商号または商標名が含まれる場合、本 CA は、以下の

少なくとも 1 つを使用して、商号/商標名を使用するための申請者の権利を検証するものとする

1. 申請者の法的な設立、存在、または承認の管轄地域にある政府機関が提供するドキュメントまたは、このような政府機関とのやり取りで得られた情報。
2. 信頼できるデータ情報源。
3. 当該商号または商標名の管理を担当している政府機関とのやり取りで得られた情報。
4. 文書による裏付けのある意見書。
5. 公共料金請求書、銀行取引明細書、クレジットカード明細書、政府発行の税務書類、その他、本 CA が信頼できると見なした本人確認書類。

3.2.2.3 国の検証

証明書の主体者識別名に countryName フィールドが存在する場合、本 CA は、次のいずれかを使用して主体者と関連付けられた国を検証するものとする。

・ドメイン名登録機関によって提供された情報
・本 CP「3.2.2.1 アイデンティティ」に記載されている方法。

3.2.2.4 ドメインの認証

セコムトラストシステムズは、利用者がドメイン名の利用権を有しているか確認するため、Baseline Requirements に準拠した次の方法を使用してドメインの認証を行う。なお、本項で記載するランダム値は、本 CA が生成する 112 ビット以上の乱数から成るものとする。

本 CA では、WHOIS 問い合わせする場合、DNS サーバーで「<Top Level Domain>.whois-servers.net」により問い合わせ先 WHOIS サーバーの IP アドレスを調べ、まずその WHOIS サーバーに問い合わせを行う。WHOIS 応答はキャッシュせず、問い合わせの都度、参照する。

WHOIS は HTTPS ウェブサイトまたは RFC 3912 で定義されたプロトコルを介してドメイン名レジストラまたはレジストリ運営者から情報を取得する。

本 CA では、「RFC 7686 - The ".onion" Special-Use Domain Name」が証明書に含まれている場合、発行しない。

1. WHOIS レジストリサービスに登録されたドメイン連絡先へ Email、ファックス、SMS、または郵便にてランダム値を送信し、ランダムな値が含まれた確認応答を受け取ることによって、FQDN に対する申請者の権限を立証する。ランダム値は、ドメイン連絡先と認識される Email アドレス、ファックス番号、SMS 番号、または住所宛に送付する。また、Email、ファックス、SMS、または郵便で、複数の認証ドメイン名の管理を確認することもできる。

ランダム値はそれぞれの Email、ファックス、SMS または郵便に一意のものとする。CA はランダム値の再利用を含めて、Email、ファックス、SMS または郵便全体を再送でき、コミュニケーションの全体内容と受信者は変更しない条件とする。

ランダム値はその生成より 30 日間のレスポンス確認の使用に有効とする。

（Baseline Requirements セクション 3.2.2.4.2 ドメイン連絡先への Email、ファックス、SMS または郵便）

2. ローカル部は 'admin'、'administrator'、'webmaster'、'hostmaster'、または 'postmaster' とし、「@」以下は認証ドメイン名として作成した Email アドレスにランダム値を送信して、ランダムな値が含まれた確認応答を受け取ることによって、要求された FQDN の制御を実証する。Email アドレスで使用する「@」以下の認証ドメイン名は、証明書発行対象となる FQDN に含まれるドメイン名とし、また、認証ドメインが同じであれば、Email で複数の FQDN を確認することもできる。

ランダム値はそれぞれの Email で固有のものとする。

Email はランダム値の再利用を含めて全体を再送でき、全体内容と受信者は変更しない条件とする。

ランダム値はその生成より 30 日間のレスポンス確認の使用に有効とする。

（Baseline Requirements セクション 3.2.2.4.4 ドメイン連絡先への Email）

3. 証明書発行対象となる FQDN、または認証ドメイン名（それぞれ先頭にアンダースコア文字で始まるラベルを接頭語に持つものも含まれる）のいずれかの、DNS CNAME、TXT または CAA レコード内のどちらかに、ランダム値か申請トークンがあることを確認することで、FQDN に対する申請者の権限を立証する。

ランダム値の有効期間は、30 日間とし、申請者が証明書要求を提出した場合、証明書に関連する検証済み情報の再利用が認められている期間が経過した後は、ランダム値を使用しないものとする。

本 CA は、本 CP「3.2.2.9 マルチ・パースペクティブ発行検証」で規定されているように、マルチ・パースペクティブ発行検証を実装する。裏付けとしてカウントされるためには、ネットワーク・パースペクティブは、プライマリ・ネットワーク・パースペクティブと同じチャレンジ情報(ランダム値またはリクエストトークン)を確認する。

（Baseline Requirements セクション 3.2.2.4.7 DNS の変更）

4. 認証ドメイン名の DNS CAA レコードの Email 連絡先へ、Email 経由でランダム値を送信し、ランダム値が含まれた確認応答を受け取ることによって、FQDN に対する申請者の権限を立証する。また、Email 連絡先が同じであれば、Email で複数の

FQDN を確認することもできる。関連する CAA リソースレコードは、RFC 8659 のセクション 3 で定義されている検索アルゴリズムを使用して確認する必要がある。

ランダム値はそれぞれの Email に一意のものとする。Email はランダム値の再利用を含めて全体を再送でき、全体内容と受信者は変更しない条件とする。ランダム値はその生成より 30 日間のレスポンス確認の使用に有効とする。

本 CA は、本 CP「3.2.2.9 マルチ・パースペクティブ発行検証」で規定されているように、マルチ・パースペクティブ発行検証を実装する。裏付けとしてカウントされるためには、ネットワーク・パースペクティブは、プライマリ・ネットワーク・パースペクティブと同じ連絡先アドレスを確認する。

（Baseline Requirements セクション 3.2.2.4.13 DNS CAA 連絡先への Email）

5. 認証ドメイン名の DNS TXT レコードの Email 連絡先へ、Email 経由でランダム値を送信し、ランダム値が含まれた確認応答を受け取ることによって、FQDN に対する申請者の権限を立証する。また、Email 連絡先が同じであれば、Email で複数の FQDN を確認することもできる。

ランダム値はそれぞれの Email に一意のものとする。Email はランダム値の再利用を含めて全体を再送でき、全体内容と受信者は変更しない条件とする。ランダム値はその生成より 30 日間のレスポンス確認の使用に有効とする。

本 CA は、本 CP「3.2.2.9 マルチ・パースペクティブ発行検証」で規定されているように、マルチ・パースペクティブ発行検証を実装する。裏付けとしてカウントされるためには、ネットワーク・パースペクティブは、プライマリ・ネットワーク・パースペクティブと同じ連絡先アドレスを確認する。

（Baseline Requirements セクション 3.2.2.4.14 DNS TXT 連絡先への Email）

6. 要求トークンまたはランダム値がファイルの内容に含まれていることを検証することにより、FQDN に対する申請者の制御を確認する。本 CA は承認済みポートを介してアクセスし、「http（または https）:// [証明書発行対象となる FQDN] /.well-known/pki-validation」ディレクトリの配下にランダム値が配置されていること、リクエストから正常な HTTP または HTTPS 応答を受信することを確認する。

本 CA は、承認された方法を使用してその FQDN に対して個別の検証を実行しない限り、検証された FQDN のすべてのラベルで終わる他の FQDN に対して証明書を発行しない。この方法は、ワイルドカードドメイン名の検証には使用しない。

CA がリダイレクトに従う場合、以下が適用される。

1. リダイレクトは、HTTP プロトコルレイヤーで開始する必要がある。2021 年 7 月 1 日以降に実行された検証の場合、リダイレクトは、RFC 7231、セクション 6.4 で定義されている 3xx301、 302、または 307 HTTP ステータスコー

ド応答、または RFC 7538、セクション 3 で定義されている 308 HTTP ステータスコード応答の結果でなければならない。リダイレクトは、RFC 7231、セクション 7.1.2 で定義されているように、Location HTTP 応答ヘッダーの最終値でなければならない。

2. リダイレクトは、「http」または「https」スキームのいずれかを使用したリソース URL へのリダイレクトでなければらない。
3. リダイレクトは、承認済みポートを介してアクセスされるリソース URL へのリダイレクトでなければならない。

ランダム値を使用する場合、次のようになる。

1. CA は、証明書要求に固有のランダム値を提供する必要がある。
2. ランダム値は、確認応答での使用のために、その作成から 30 日以内有効である必要がある。

Onion ドメイン名を除き、本 CA は、本 CP「3.2.2.9 マルチ・パースペクティブ発行検証」で規定されているように、マルチ・パースペクティブ発行検証を実装する。裏付けとしてカウントされるためには、ネットワーク・パースペクティブは、プライマリ・ネットワーク・パースペクティブと同じチャレンジ情報(ランダム値またはリクエストトークン)を確認する。

(Baseline Requirements セクション 3.2.2.4.18 ウェブサイトへの合意に基づく変更 v2)

7. RFC 8555 のセクション 8.3 で定義されている ACME HTTP チャレンジメソッドを使用して FQDN のドメイン制御を検証して、FQDN に対する申請者の制御を確認する。

本 CA はリクエストから正常な HTTP 応答を受信する（2xx HTTP ステータスコードを受信)。

トークン（RFC 8555、セクション 8.3 で定義）は、作成から 30 日を超えて使用しない。

本 CA がリダイレクトに従う場合、以下が適用される。

1. リダイレクトは、HTTP プロトコルレイヤーで開始する。
   2021 年 7 月 1 日以降に実行された検証の場合、リダイレクトは、RFC 7231 のセクション 6.4 で定義されている 301、302、または 307 の HTTP ステータス コード応答、または RFC 7538 のセクション 3 で定義されている 308 HTTP ステータス コードの応答の結果でなければならない。リダイレクトは、RFC 7231、セクション 7.1.2 で定義されているように、LocationHTTP 応答ヘッダーの最終値でなければならない。
2. リダイレクトは、「http」または「https」スキームのいずれかを使用した

リソース URL とする。

3. リダイレクトは、承認済みポートを介してアクセスされるリソース URL とする。

Onion ドメイン名を除き、本 CA は、本 CP「3.2.2.9 マルチ・パースペクティブ発行検証」で規定されているように、マルチ・パースペクティブ発行検証を実装する。裏付けとしてカウントされるためには、ネットワーク・パースペクティブは、プライマリ・ネットワーク・パースペクティブと同じチャレンジ情報(ランダム値またはリクエストトークン)を確認する。

(Baseline Requirements セクション 3.2.2.4.19 ウェブサイトの合意された変更 - ACME)

3.2.2.5 IP アドレスの認証

本 CA は、IP アドレスの認証による証明書発行を行わない。

3.2.2.6 ワイルドカードドメイン認証

ワイルドカード証明書を発行する前に、本 CA は、証明書に含まれるワイルドカードドメイン名の FQDN 部分が「レジストリ管理」ラベルであるか、「パブリックサフィックス」であるかを判断する手続きを文書化する。

ワイルドカードドメインの FQDN 部分が「レジストリ管理下」または「パブリックサフィックス」である場合、本 CA は申請者がドメイン名空間全体を正しく管理していることを検証しない限り、発行を拒否する。

国別コードトップレベルドメインの名前空間において、何が「レジストリ管理下」であり、何が登録可能な部分であるかの判断は、パブリックサフィックスリスト（以下、PSL という）を参照し、定期的にコピーして使用する。PSL を使用する場合、CA は「ICANN DOMAINS」セクションのみを参照し、「PRIVATE DOMAINS」セクションは参照しないものとする。

本 CA では、EV 証明書のワイルドカードは発行しない。

3.2.2.7 データ情報源の正確性

本 CA は、データ情報源を信頼できるデータ情報源として使用する前に、データ情報源の信頼性、正確性、ならびに改変や偽造への耐性を評価する。本 CA は、データ情報源の評価中、下記を考慮する。

1. 提供された情報の古さ。
2. 情報源の更新頻度。
3. データ提供者とデータ収集の目的
4. データ入手の公開性。

5. データの改ざんが比較的困難であること。

EV 証明書を発行するにあたり、QIIS とは、定期的に更新され、一般に利用可能なデータベースで、特定の情報に関して信頼できる情報源として一般に認識されているものである。本 CA が以下の要件をすべて満たしていると判断した場合、そのデータベースは QIIS として適格である。

1. 証明書を扱う業種以外の業種が、正確な場所、連絡先、またはその他の情報を得るためにデータベースに依存していること。
2. データベース提供者は、少なくとも年 1 回のペースでデータを更新している。

本 CA は、文書化されたプロセスを使用して、データベースプロバイダの利用規約の審査を含め、データベースの正確性を確認し、そのデータが容認可能であることを点検する。

本 CA は、QIIS のデータのうち、以下については、使用しない

i. 自己報告されたデータ。

ii. QIIS によって正確なものとして検証されていないデータ。

本 CA またはその所有者、あるいは関連会社が企業支配権を維持しているデータベース、または本 CA が審査プロセスのいずれかの部分を外注している登録機関または請負業者(またはその所有者や関連会社)が所有権または受益権を維持しているデータベースは、QIIS としての資格を持たない。

QGIS とは、定期的に更新される最新の、一般に利用可能な情報源である。データベースは、参照される情報を正確に提供する目的で設計され、政府機関によって維持され、データの報告が法律で要求され、虚偽または誤解を招く報告が刑事罰または民事罰で罰せられることを条件に、かかる情報の信頼できる情報源として一般に認識されている。第三者が政府機関から直接情報を取得する場合のみ、政府機関から情報を取得するために第三者を利用することができる。

3.2.2.8 CAA レコード

発行プロセスの一部として、本CAは、RFC 8659で指定されているように、発行される証明書の Subject Alternative Name拡張内の各dNSNameについて、CAAレコードをチェックし、見つかった処理指示に従う必要がある。本CAは発行する場合、CAAレコードのTTL(有効期限内)または8時間のうち、いずれか長い方の範囲内で上記を行う必要がある。

CAAレコードを処理する際、本CAは、RFC 8659で指定されているとおり、issue、issuewild、およびiodefプロパティタグを処理する必要がある。

ただし、iodefプロパティタグのコンテンツに対する処理は不要である。他のプロパティタグもサポートすることが可能だが、Baseline Requirementsに規定されている必須プ

ロパティタグと衝突したり、必須プロパティタグよりも優先されたりしてはならない。本CAはcriticalフラグを尊重し、このフラグセットを持つ不明なプロパティタグに遭遇した場合は証明書を発行しない。

本CAは、以下の場合、発行許可の際にレコードのルックアップが失敗したと処理し、発行することができる。

·失敗がCAのインフラストラクチャー外である場合

·ルックアップが少なくとも1回再試行されている

·ドメインのゾーンにICANNルートへのDNSSEC検証チェーンを持っていない

本CAは、処理実務の一環として取られたアクションがあればすべてログで記録するものとする。

3.2.2.9 マルチ・パースペクティブ発行検証

マルチ・パースペクティブ発行検証は、証明書発行前に、プライマリー・ネットワーク・パースペクティブが複数のリモートネットワーク・パースペクティブから受けた判断（ドメイン検証の合否、CAA の許可/禁止など）を検証しようとするものである。このプロセスにより、BGP（Border Gateway Protocol）攻撃またはハイジャックに対する防御が向上する。

本CAは、必要とされる 1)ドメインの認証または管理、および 2)CAA記録の確認において、マルチ・パースペクティブ発行検証を行う際、同一または異なるネットワーク・パースペクティブを使用することができる。

依拠するネットワーク・パースペクティブからの一連の応答は、CAが肯定的に評価するために必要な情報を提供するものとする。

- 本CP「3.2.2.4 ドメインの認証」に規定される検証方法によって要求、期待される以下の値の存在。
  1)ランダム値、2)リクエストトークン、3)コンタクトアドレス。
- 本CP「3.2.2.8 CAAレコード」に規定される、要求されたドメインに対して発行するCAの権限。

本CP「3.2.2.4 ドメインの認証」では、マルチ・パースペクティブ発行検証を必要とする検証方法およびプライマリ・ネットワークの観点によって決定された結果をネットワークの観点がどのように検証するかを説明する。

1 つのネットワーク・パースペクティブから取得した結果または情報は、後続のネット

ワーク・パースペクティブを通じて検証を実行するときに再利用またはキャッシュしない（例えば、異なるネットワーク・パースペクティブは、1 つのネットワーク・パースペクティブからのトラフィックを制御している攻撃者が他のネットワーク・パースペクティブによって使用される DNS キャッシュをポイズニングするのを防ぐために、共有 DNS キャッシュに依存することはできない)。ネットワーク・パースペクティブへのインターネット接続を提供するネットワーク・インフラストラクチャーは、ネットワーク・パースペクティブの運用に必要な計算サービスを提供するのと同じ組織によって管理されてもよい。リモートの ネットワーク・パースペクティブと 本 CA との間のすべての通信は、最新のプロトコル（HTTPS 等）に依拠して認証および暗号化されたチャネルを介して行う。

ネットワーク・パースペクティブは、ネットワーク・パースペクティブと同じ場所に配置されていない再帰 DNS リゾルバーを使用できる。ただし、ネットワーク・パースペクティブが使用する DNS リゾルバーは、それに依拠するネットワーク・パースペクティブと同じ地域インターネットレジストリサービス領域内になければならない。さらに、マルチ・パースペクティブ発行検証の試みで使用される DNS リゾルバーのペアは、DNS リゾルバーが存在する 2 つの州、都道府県、国の間の直線距離が少なくとも 500km でなければならない。DNS リゾルバーの場所は、カプセル化されていない送信 DNS クエリが通常、その DNS リゾルバーにインターネット接続を提供するネットワーク・インフラストラクチャーに最初に渡されるポイントによって決まる。

本 CA は、同じ検証方法または別の方法を使用して、マルチ・パースペクティブ発行検証を直ちに再試行できる（例えば「Agreed-Upon Change to Website - ACME」が マルチ・パースペクティブ発行検証の結果に対して確認できなかった場合、本 CA は「Email to DNS TXT Contact」を使用して検証を直ちに再試行できる)。マルチ・パースペクティブ発行検証を再試行する時、本 CA は、以前の検証結果に依拠しない。任意の期間に実行できる検証の最大試行回数に関する規定はない。

「クォーラム要件」の表では、マルチ・パースペクティブ発行検証に関連するクォーラム要件について説明する。本 CA がドメイン認証または管理と CAA レコードチェックの両方について同じネットワーク・パースペクティブのセットに依拠しない場合、クォーラム要件は、両方のネットワーク・パースペクティブのセット（つまり、ドメイン認証または管理セットと CAA レコードチェックセット）について満たす必要がある。ネットワーク・パースペクティブは、存在する 2 つの州、都道府県、国の直線距離が 500 km 以上の場合、別のものとみなされる。ネットワーク・パースペクティブは、プライマリ・ネットワーク・パースペクティブやクォーラム要件で表される他のネットワーク・パースペクティブと異なる場合、「リモート」と見なされる。

本 CA は、CAA レコードのクォーラム要件への適合に関する裏づけとなる証拠を最大 398 日間再利用することができる。あるドメインに証明書を発行した後、リモート・ネットワーク・パースペクティブは、同一申請者からの以後の証明書申請において、同一ドメインまたはそのサブドメインに対する CAA レコードの取得および処理を最大 398 日間省略することができる。

表 3.2.2.9-1 クォーラム要件の表

# 使用されるリモート・ネットワーク・パースペクティブの数	# 許可される非検証の数
2-5	1
6+	2

マルチ・パースペクティブ発行検証を実行するリモート・ネットワーク・パースペクティブ:

必須要件

- ネットワークの強化
  - ネットワーク(インターネット・サービス・プロバイダーやクラウドプロバイダーネットワークなど)が、グローバルインターネットルーティングシステムで BGP ルーティングインシデントを軽減するための対策を実施して、ネットワーク・パースペクティブへのインターネット接続を提供することに依拠する。

推奨要件

- 施設およびサービスプロバイダーの要件
  - ISO/IEC 27001 認定施設または同等のセキュリティ・フレームワークからホストされ、独立した監査、認証または報告を受けていること。
  - System and Organization Controls 2 (SOC 2)、IASE 3000、ENISA 715、FedRAMP Moderate、C5:2020、CSA STAR CCM または独立して監査され、認定または報告された同等のサービス フレームワークのいずれかのレポートに記載されているサービスを利用。
- 脆弱性検出とパッチ管理
  - 侵入検知と防止の制御を実装して、一般的なネットワークとシステムの脅威から保護。

- 脆弱性の特定、レビュー、対応、および修復に対処する脆弱性修正プロセスを文書化し、それに従う。
- 脆弱性スキャンを少なくとも 3 か月ごとに実施。
- 少なくとも年に一度、侵入テストを受ける。
- セキュリティ更新プログラムが利用可能になってから 6 か月以内に推奨されるセキュリティ更新プログラムを適用(ただし、本 CA がセキュリティ更新プログラムを適用することにより、セキュリティ更新プログラムを適用する利点を上回る追加の脆弱性または不安定性をもたらすと文書化している場合を除く。

● システムの強化
- 使用されていないすべてのアカウント、アプリケーション、サービス、プロトコル、およびポートを無効にする。
- すべてのユーザーアカウントに多要素認証を実装。

● ネットワークの強化
- 各ネットワーク境界制御（ファイアウォール、スイッチ、ルーター、ゲートウェイまたはその他のネットワーク制御デバイスまたはシステム）をその操作に必要であると識別されたサービス、プロトコル、ポート、および通信のみをサポートするルールで構成。
- 次のようなネットワーク（インターネット・サービス・プロバイダーなど）に依拠する：

  1) BGP Prefix Origin Validation (RFC 6811)など、Secure Inter-Domain Routing (RFC 6480)に基づくメカニズムを使用する。

  2) RPKI 以外のルートリーク防止メカニズム（RFC 9234 など）を使用する。

  3) BCP 194 に記載されている現在のベストプラクティスを適用する。

  通常の運用条件下では、マルチ・パースペクティブ発行検証を実行するネットワーク・パースペクティブは、RFC 6811 で定義されている RPKI 不正 BGP ルートをフィルタリングするネットワークまたはネットワークセットを経由して、すべてのインターネットトラフィックを転送することが推奨されますが、これは必須ではありません。

上記の考慮事項以外にも、マルチ・パースペクティブ発行検証を実行するコンピューティングシステムは、本 CP「8. 準拠性監査と他の評価」に記載されている監査範囲外と見なされる。

上記の考慮事項のいずれかが委任された第三者によって行われる場合、本 CA は、上記の考慮事項の 1 つ以上が守られていることを保証するために、委任された第三者から合理的な証拠を取得することができる。本 CP「1.3.2 RA」の例外として、委任された第三者は、

上記の考慮事項を満たすために、本 CP「8. 準拠性監査と他の評価」に記載されている監査範囲内である必要はない。

段階的な実装タイムライン

2024 年 9 月 15 日以降、本 CA は、少なくとも 2 つのリモート・ネットワーク・パースペクティブを使用してマルチ・パースペクティブ発行検証を実装するべきである。

2025 年 3 月 15 日以降、本 CA は、少なくとも 2 つのリモート・ネットワーク・パースペクティブを使用してマルチ・パースペクティブ発行検証を実装する。本 CA は、プライマリ・ネットワーク・パースペクティブが行った検証の結果を裏付けないリモート・ネットワーク・パースペクティブの数（非検証の数）が、クォーラム要件の表で許容される数より多い場合でも、証明書の発行を続行できる。

2025 年 9 月 15 日以降、本 CA は少なくとも 2 つのリモート・ネットワーク・パースペクティブを使用してマルチ・パースペクティブ発行検証を実装する。本 CA は、非検証の数がクォーラム要件の表で許可されている数を超えている場合、証明書の発行を続行しない。

2026 年 3 月 15 日以降、本 CA は、少なくとも 3 つのリモート・ネットワーク・パースペクティブを使用して、マルチ・パースペクティブ発行検証を実装する。本 CA は、非検証の数がクォーラム要件の表で許可されている数を超えている場合およびプライマリ・ネットワーク・パースペクティブが行った検証の結果を裏付けるリモート・ネットワーク・パースペクティブが、少なくとも 2 つの異なる地域インターネット・レジストリのサービス地域内に含まれない場合、証明書の発行を続行しない。

2026 年 6 月 15 日以降、本 CA は、少なくとも 4 つのリモート・ネットワーク・パースペクティブを使用して、マルチ・パースペクティブ発行検証を実装する。CA は、非検証の数がクォーラム要件の表で許可されている数を超えている場合、および プライマリ・ネットワーク・パースペクティブが行った検証の結果を裏付けるリモート・ネットワーク・パースペクティブが、少なくとも 2 つの異なる地域インターネット・レジストリのサービス地域内に含まれない場合、証明書の発行を続行しない。

2026 年 12 月 15 日以降、本 CA は少なくとも 5 つのリモート・ネットワーク・パースペクティブを使用して、マルチ・パースペクティブ発行検証を実装する。本 CA は、非検証の数がクォーラム要件の表で許可されている数を超えている場合および プライマリ・ネットワーク・パースペクティブが行った検証の結果を裏付けるリモート・ネットワーク・パースペクティブが、少なくとも 2 つの異なる地域インターネット・レジストリのサービス地域内に含まれない場合、証明書の発行を続行しない。

3.2.3 個人の認証

本 CA は、以下の証明書ポリシー識別子に準拠する個人認証証明書（IV 証明書）を発行しない。

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3)

3.2.4 検証されない利用者の情報

検証されていない利用者の情報は、本 CA から発行される証明書には含まれない。

3.2.5 権限の正当性確認

主体者識別情報を含む証明書の申請者が組織である場合、本 CA は、信頼できる連絡手段を使用して、申請権限者による証明書要求の真正性を検証するものとする。

本 CA は、本 CP「3.2.2.1 アイデンティティ」に掲載された情報源を使用して、信頼できる連絡手段を検証できる。本 CA が信頼できる連絡手段を使用することを条件として、本 CA は、申請権限者、申請者組織内の権限のある情報源(申請者の本社、経営部門、人事部門、情報技術部門、または本 CA が適切と見なすその他の部門)と直接やり取りして、証明書要求の真正性を確認できる。

3.2.6 相互運用の基準

CA は、CA が信頼関係（クロス認証下位 CA 証明書の発行）の確立を取り決めた場合または受諾した場合を条件として、CA を主体者として識別するすべてのクロス認証下位 CA 証明書を開示する。

3.3 鍵更新申請時の本人性確認と認証

3.3.1 通常の鍵更新時における本人性確認と認証

鍵更新時における利用者の本人性確認および認証は、本 CP「3.2 初回の本人確認」と同様とする。

3.3.2 証明書失効後の鍵更新時における本人性確認と認証

失効した証明書の更新は行わない。証明書申請は新規扱いとし、利用者の本人性確認および認証は、本 CP「3.2 初回の本人性確認」と同様とする。

3.4 失効申請時の本人性確認と認証

本 CA は、利用者または申請者から所定の手続きにより失効申請を受け付けた後、利用者の本人性確認と認証を行う。

4. 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書の申請を行うことができる者

証明書の申請を行うことのできる者は、証明書を利用する個人、法人、その他の組織および利用者から委任された代理人（以下「申請者」という）とする。

本 CP「5.5.2 アーカイブ保存期間」に従い、本 CA は、フィッシングまたはその他の詐欺的使用の疑いあるいは懸念を理由に、以前に失効した証明書および以前に拒否した証明書要求をすべて含む内部データベースを保持するものとする。本 CA は、この情報を使用して、以降の疑わしい証明書要求を識別するものとする。

EV 証明書の場合、申請者の法的存在と身元を確認するため、本 CA は次のことを実行する。

民間組織が主体者の場合

A. 法的存在: 申請者が法的に認められた法人であり、申請者の設立または登録管轄区域内で現存し、登録機関に有効に設立され（例: 法人化され）、法人の設立機関または登録機関の記録に以下が指定されていないことを確認する。 「非活動」、「無効」、「最新ではない」、または同等のラベルであること。

B. 組織名: 申請者の設立または登録管轄区域内の設立または登録機関に記録された申請者の正式な法名が、EV 証明書リクエストの申請者の名前と一致することを確認する。

C. 登録番号: 申請者の設立または登録管轄区域内の設立または登録機関によって申請者に割り当てられた特定の登録番号を取得する。設立機関または登録機関が登録番号を割り当てていない場合、本 CA は申請者の設立日または登録日を取得する。

D. 登録代理人: 申請者の登録代理人または登録事務所の身元および住所を取得する（申請者の設立または登録の管轄区域に該当する場合）。

政府機関が主体者の場合

A. 法的存在: 申請者が法的に認められた政府機関であり、その政府機関が運営される政府部門に存在することを確認する。

B. エンティティ名: 申請者の正式な法人名が EV 証明書リクエストの申請者の名前と一致することを確認する。

C. 登録番号: 本 CA は、申請者の設立、登録、設立の日付、または政府機関を創設した法律上の識別子の取得を試みる。この情報が利用できない状況では、本 CA

は対象が政府機関であることを示す適切な言語を入力する。

事業体が主体者の場合

A. 法的存在: 申請者が申請書で提出した名前で事業に従事していることを確認する。

B. 組織名: 申請者の登録管轄区域内の登録機関によって認識されている申請者の正式な法名が、EV 証明書リクエストの申請者の名前と一致することを確認する。

C. 登録番号: 申請者の登録管轄区域内の登録機関によって申請者に割り当てられた、特定の一意の登録番号の取得を試みる。登録機関が登録番号を割り当てない場合、本 CA は申請者の登録日を取得するものとする。

D. 主要な個人: 特定された主要な個人の身元を確認する。

非営利団体が主体者の場合(国際機関)

A. 法的存在: 申請者が法的に認められた国際機関実体であることを確認する。

B. エンティティ名: 申請者の正式な法人名が EV 証明書リクエストの申請者の名前と一致することを確認する。

C. 登録番号: 本 CA は、申請者の設立日、または国際機関を創設した法律上の識別子の取得を試みる。この情報が利用できない状況では、本 CA は主体者が国際組織であることを示す適切な言語を入力する。

具体的には、以下の値を登録する。
利用者が次の場合、本 CA は serialNumber に以下を設定する。

登記されている法人	: 会社法人等番号、または法人番号
中央省庁および国の機関	: 法人番号、または設立日
地方公共団体およびその機関	: 法人番号、または設立日
国公立大学・高校機関	: 法人番号、または設立日

本 CA より法人番号および設立日が確認できなかった場合、serialNumber には以下の文言を記載する。

中央省庁および国の機関	: Government
地方公共団体およびその機関	: Local Government
国公立大学・高校機関	: Public School

利用者が次の場合、本 CA は businessCategory に以下を設定する。

登記されている法人	: Private Organization

中央省庁および国の機関　　：Government Entity
地方公共団体およびその機関　：Government Entity
国公立大学・高校機関　　：Government Entity

4.1.2 申請手続および責任

証明書の発行前に、本 CA は申請者から以下のドキュメントを入手する。

1. 証明書発行申請書。電子版でも可。
2. 契約締結された利用契約または利用規約。電子版でも可。

本 CA は、Baseline Requirements を満たすために必要であると本 CA が判断するその他のドキュメントをすべて取得する。

証明書の発行前に、本 CA は、本 CA が指定した形式で、かつ Baseline Requirements に準拠する証明書発行申請書を申請者から取得する。本 CP「「4.2.1 本人性確認と認証の実施」」の有効期間および更新要件に従い、同じ申請者に発行される複数の証明書に 1 つの証明書発行申請書で対応することがある。ただし、各証明書が、申請者を代表する適切な申請権限者によって署名された有効な最新の証明書発行要求によってサポートされていることを条件とする。証明書発行申請書は、電子的に作成、送信、または署名してもよい。

証明書発行申請書には、申請者または申請者を代理する者による証明書発行の申請、および申請者または申請者を代理する者による証明書に記載されたすべての情報が正確であることの証明が含まれなければならない。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施

本 CA は、証明書申請を受け付けた後、本 CP「3.2 初回の本人確認」に基づく確認を行う。

証明書要求には、証明書に含めるべき申請者に関するすべての事実情報、および本 CA が Baseline Requirements および本 CA の証明書ポリシーや認証局運用規定に準拠するために申請者から取得する必要がある追加情報を含めてもよい。証明書要求が申請者に関する必要な情報の一部を欠いている場合、本 CA は、残りの情報を申請者から取得するか、または信頼できる独立した第三者機関のデータ情報源から情報を取得して申請者に確認するものとする。本 CA は、申請者によって証明書に含めることを要求されたすべてのデータを検証するための文書化された手順を確立し、それに従うものとする。

申請者情報には、証明書の Subject Alternative Name 拡張領域に含まれる少なくとも 1 つの完全修飾ドメイン名を含める。

CPS「6.3.2 私有鍵および公開鍵の有効期間」では、利用者証明書の有効期限を制限する。

本 CA は、本 CP 「3.2 初回の本人確認」で提供されたドキュメントとデータを使用して証明書情報を検証するか、以前の検証自体を再利用する場合がある。

ただし下記を条件とする。

本 CA は、本 CP 「3.2 初回の本人確認」で指定されたソースからデータまたはドキュメントを取得するか、証明書の発行前 825 日以内に検証自体を完了する。

本 CP「3.2.2.4 ドメインの認証」に従ったドメイン名の検証のために、利用されたデータ、ドキュメントまたは完了した検証は、証明書を発行する 398 日前までに取得する必要がある。

もし以前の検証で使用された何らかのデータやドキュメントが、証明書発行に先立ち、データまたはドキュメントの再利用に許された最大期間以上に取得されていたら、以前の認証は再利用しない。

Baseline Requirements または EV Guidelines に規定される検証方法への変更後、本 CA は、Ballot の投票において特に規定がない限り、Baseline Requirements セクション 4.2.1 に記載される期間、変更前に収集した検証データ、文書または検証そのものを引き続き再利用することができる。

本 CA は、申請情報の審査時に CAA レコードを確認する。

FQDN に対して証明書を発行する権限を付与したい利用者は、それぞれの DNS ゾーンの CAA レコードプロパティ「issue」または「issuewild」に「secomtrust.net」の値を含めなければならない。

利用者のそれぞれの DNS ゾーンにすでに CAA エントリーがあり、本 CA から証明書発行が必要な場合、CAA レコードプロパティ「issue」または「issuewild」に「secomtrust.net」の値を含めなければならない。

本 CA は、ハイリスクの証明書要求が Baseline Requirements に従って適切に検証されるようにするために合理的に必要な場合において、証明書の承認前にハイリスク証明書要求に対する追加の検証活動を識別し要求する、文書化された手順を作成、保持、実施するものとする。

本項で定める CA の義務を外部委託先が履行する場合、CA は、ハイリスク証明書要求の識別とさらなる検証のために外部委託先によって用いられたプロセスが、CA 独自のプロセスと同水準の確実性を提供していることを検証する。

EV 証明書の検証済みデータの有効期限は以下のとおりである。

1. EV Guidelines セクション 3.2.2.14.2 に基づいて EV 証明書を再発行した場合や、EV Guidelines セクション 3.2.2.14.1 で別途許可されている場合を除き、EV 証明書の発行の根拠として使用されたすべてのデータの(再検証が必要となるまでの)有効期限は、以下の制限を超えないものとする。
   A. 法的存在とアイデンティティ - 398 日

B. 屋号 - 398 日
C. 事業拠点の住所 - 398 日
D. 信頼できる連絡手段 - 398 日
E. 事業体としての実在 - 398 日
F. ドメイン名 - 398 日
G. 氏名、役職、代理関係、および権限 - 398 日。ただし、本 CA と申請者間の契約で別の期限が指定されている場合は、契約で指定された期限が優先される。例えば契約には、申請者または CA によって失効されるまで、あるいは契約が期限切れまたは停止されるまで続く EV ロールの割り当てを含めることができる。

2. 上記の 398 日という期限は、情報が本 CA によって収集された日を始点とする。
3. 本 CA は、以前に提出された EV 証明書要求、利用契約、または利用規約を再利用できる。これには、EV Guidelines セクション 3.2.2.9 および EV Guidelines セクション 3.2.2.10 で許されている限り、単一の EV 証明書要求を、同じ主体者を含む複数の EV 証明書の根拠とすることも含まれる。
4. 本 CA は、EV Guidelines セクション 3.2.2.14.1 で許可されている場合を除き、前述の期限外に取得された情報に関しては、EV Guidelines で求められている検証プロセスを繰り返す。

EV 証明書の発行には、以下の申請者の役割が必要である。

1.証明書要求者

EV 証明書要求は、権限を有する証明書要求者が提出しなければならない。 証明書要求者は、申請者、申請者に雇用された者、申請者を代理する明示的な権限を持つ代理人、または申請者の代理で EV 証明書要求を完了し提出する第三者(ISP やホスティング会社など)である自然人である。

2. 証明書承認者

EV 証明書要求は、権限を有する証明書承認者によって承認されなければならない。証明書承認者は、申請者、申請者に雇用された者、申請者を代理する明示的な権限を持つ代理人のいずれかで、申請者の代理として利用契約書に署名する権限を持つ自然人である。

i. 証明書要求者として行動し、他の従業員または第三者に証明書要求者として行動する権限を与える。
ii. 他の証明書要求者によって送信された EV 証明書要求を承認する。

3.契約署名者

要求された EV 証明書に適用される利用契約書は、権限を有する契約署名者によって署名されなければならない。契約署名者は、申請者、申請者に雇用された者、

申請者を代理する明示的な権限を持つ代理人のいずれかで、申請者の代理として利用契約書に署名する権限を持つ自然人である。

4.申請代表者

CA と利用者が関連会社である場合、要求された EV 証明書に適用される利用規約は、権限のある申請代表者によって承認され同意されなければならない。申請代表者とは、申請者、申請者に雇用された者、申請者を代理する明示的な権限を持つ代理人のいずれかで、申請者に代わって利用規約を確認し同意する権限を持つ自然人である。

申請者は、1 人の個人に対して、これらの役割のうち 2 つ以上を有することを許可してもよい。申請者は、これらの役割のいずれかを複数の個人に対して許可してもよい。

4.2.2 証明書申請の承認または却下

本 CA は、審査の結果、承認を行った申請について証明書の発行を行い、利用者に審査終了および証明書発行について通知する。

また、すべての項目の審査が正常に完了しない証明書の申請を却下できるものとするのとし、以下理由を含むものは却下とする。

・以前に拒否された、または以前に契約の条項に違反していた申請者または利用者の証明書。

・内部のサーバー名または予約済みの IP アドレスを Subject Alternative Name 拡張領域または「コモンネーム」フィールドに持つ

本 CA は直接または外部委託先を通じ、申請者または利用者に、不備の内容と書類再提出等の通知をするものとする。

4.2.3 証明書申請の処理時間

本 CA は、承認を行った証明書申請について、すみやかに証明書の発行を行う。

4.3 証明書の発行

4.3.1 証明書発行時の処理手続

4.3.1.1 ルート CA の証明書発行の手動承認

ルート CA による下位 CA 証明書発行では、証明書への署名操作を実行するために、本 CA によって承認された個人（CA のシステムオペレーター、システム責任者または PKI 管理者）が意図的に直接コマンドを発行することを必要とする。

4.3.1.2 署名される証明書のリンティング

Baseline Requirements に準拠する証明書プロファイルの実装は複雑であるため、CA による署名前に、CA による署名対象証明書の技術的適合性を検証するためのリンティング処理を実装することがベストプラクティスとみなされる。ただし、RFC 6962 (Certificate Transparency) のセクション 3.2 に記載される方法で、署名される証明書が署名前の証明書と一致していることを検証する技術的管理が CA にあることを条件とする。2024 年 9 月 15 日より、本 CA はこのようなリンティング処理を実装すべきである。2025 年 3 月 15 日より、本 CA は、リンティング処理を実装するものとする。

署名すべき証明書の内容を含む証明書を生成するために使用される方法は、以下のものが含まれるが、これらに限定されない。

1. 公開鍵コンポーネントが、公的に信頼されている CA 証明書とチェーンする証明書によって認証されていない「ダミー」の私有鍵で署名する。
2. 証明書 ASN.1 SEQUENCE の signature フィールドに静的な値を指定。

本 CA は、独自の証明書リンティングツールを実装してもよいが、業界で広く採用されているリンティングツールを使用すべきである
（参照 https://cabforum.org/resources/tools/ ）。

本 CA は、以下のようなオープンソースのリンティングプロジェクトに貢献することができる。

- 新しいリントを作成する、または既存のリントを改善する。
- 不正確な可能性のあるリンティング結果をバグとして報告する。
- 既存のリンティングソフトウェアでカバーされていないチェックをリンティングソフトウェアの保守担当者に通知する。
- 既存のリントのドキュメントを更新する。
- 特定のリントの正常/異常のテスト証明書の生成。

4.3.1.3 発行済み証明書のリンティング

本 CA は、発行済み証明書をテストするため、リンティングプロセスを使用することができる。

4.3.2 利用者への証明書発行通知

利用者に対し、利用者だけがアクセス可能なウェブサイト、Email 送付等で証明書を送付することで発行通知とする。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

利用者が証明書をダウンロードしたことをもって、あるいは他の方法によって利用者が送付された証明書をサーバーに導入した時点をもって、証明書が受領されたものとする。

4.4.2 認証局による証明書の公開

本 CA の CA 証明書は、リポジトリーに公開される。本 CA は、CT（Certificate Transparency）ログに登録することにより、利用者の証明書を公開することができる。

4.4.3 他のエンティティに対する認証局の証明書発行通知

本 CA は、証明書申請時に登録された担当者以外への証明書発行通知は行わない。

4.5 鍵ペアおよび証明書の用途

4.5.1 利用者の私有鍵および証明書の用途

証明書は、本 CP、サービス利用規定等および CPS に従い使用されるものとする。

利用者は、第三者による不正使用または開示から私有鍵を保護し、「9.6.3 利用者の表明保証」に従って意図された目的にのみ私有鍵を使用するものとする。

4.5.2 検証者の公開鍵および証明書の用途

検証者は、本 CP および CPS の内容について理解し、承諾したうえで、本 CA の証明書を使用するものとする。

検証者は本 CA の証明書を使用して、利用者の証明書を検証する事ができる。

4.6 証明書の更新

本 CA は、利用者が証明書を更新する場合、新たな鍵ペアを生成すること推奨する。

4.6.1 証明書更新の状況

鍵更新をともなわない証明書の更新は、証明書の有効期間が満了する場合に行う。

4.6.2 証明書の更新申請を行うことができる者

本 CP「4.1.1.証明書の申請を行うことができる者」と同様とする。

4.6.3 証明書の更新申請の処理手続

本 CP「4.3.1.証明書発行時の処理手続」と同様とする。

4.6.4 利用者に対する新しい証明書発行通知

本 CP「4.3.2.利用者への証明書発行通知」と同様とする。

4.6.5 更新された証明書の受領確認手続

本 CP「4.4.1.証明書の受領確認手続」と同様とする。

4.6.6 認証局による更新された証明書の公開

本 CP「4.4.2.認証局による証明書の公開」と同様とする。

4.6.7 他のエンティティに対する認証局の証明書発行通知

本 CP「4.4.3.他のエンティティに対する認証局の証明書発行通知」と同様とする。

4.7 証明書の鍵更新

4.7.1 鍵更新の状況

鍵更新をともなう証明書の発行は、証明書の有効期間が満了する場合または鍵の危殆化にともない証明書の失効を行った場合等に行われる。

4.7.2 新しい証明書の申請を行うことができる者

本 CP「4.1.1.証明書の申請を行うことができる者」と同様とする。

4.7.3 鍵更新をともなう証明書申請の処理手続

本 CP「4.3.1.証明書発行時の処理手続」と同様とする。

4.7.4 利用者に対する新しい証明書の通知

本 CP「4.3.2.利用者への証明書発行通知」と同様とする。

4.7.5 鍵更新された証明書の受領確認手続

本 CP「4.4.1.証明書の受領確認手続」と同様とする。

4.7.6 認証局による鍵更新済みの証明書の公開

本 CP「4.4.2.認証局による証明書の公開」と同様とする。

4.7.7 他のエンティティに対する認証局の証明書発行通知

本 CP「4.4.3.他のエンティティに対する認証局の証明書発行通知」と同様とする。

4.8 証明書の変更

本 CA は、証明書に登録された情報の変更が必要となった場合、その証明書の失効およ

び新規発行とする。

4.8.1 証明書の変更事由

規定しない。

4.8.2 証明書の変更申請を行うことができる者

本 CP「4.1.1.証明書の申請を行うことができる者」と同様とする。

4.8.3 変更申請の処理手続

本 CP「4.3.1.証明書発行時の処理手続」と同様とする。

4.8.4 利用者に対する新しい証明書発行通知

本 CP「4.3.2.利用者への証明書発行通知」と同様とする。

4.8.5 変更された証明書の受領確認手続

本 CP「4.4.1.証明書の受領確認手続」と同様とする。

4.8.6 認証局による変更された証明書の公開

本 CP「4. 4. 2. 認証局による証明書の公開」と同様とする。

4.8.7 他のエンティティに対する認証局の証明書発行通知

本 CP「4.4.3.他のエンティティに対する認証局の証明書発行通知」と同様とする。

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由

本 CA は、ショートリブド利用者証明書の失効をサポートすることができる。

次の 1 つ以上が発生した場合、ショートリブド利用者証明書を除き、本 CA は 24 時間以内に証明書を失効し、本 CP「7.2.2 CRL 拡張」の CRLReason (失効事由) を使用する。

1. 利用者が、CRLreason を指定せずに、本 CA に証明書失効することを書面で要求する (CRLReason "unspecified (0)"[未定義]の場合、CRL に reasonCode 拡張を含めない)。
2. 利用者が本 CA に対し、元の証明書要求が承認されていなかったこと、および遡及的に承認を許可しないことを通知した場合(CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
3. 本 CA が、利用者証明書内の公開鍵に対応する私有鍵が危殆化された証拠を得た場合

(CRLReason #1, keyCompromise [私有鍵の危殆化])。

4. 本 CA は、証明書に含まれる公開鍵に基づき、利用者の私有鍵を容易に計算できることが実証または証明された方法（Baseline Requirements セクション 6.1.1.3 (5)、CPS「6.1.1　鍵ペアの生成」）で特定されるものを含むが、これらに限定されない (CRLReason #1, keyCompromise [私有鍵の危殆化])。
5. 本 CA が、証明書内におけるドメイン認証の承認、または FQDN や IP アドレスの管理が信用できない証拠を得た場合（CRLReason #4, superseded [証明書の破棄])。

本 CA は、ショートリブド利用者証明書を除き、以下のいずれかが発生した場合、24 時間以内に利用者証明書を失効させるべきであり、5 日以内に証明書を失効し、CRLReason を使用する。

6. 証明書が本 CP「6.1.5 鍵サイズ」および本 CP「6.1.6 公開鍵のパラメーターの生成および品質検査」の要件に準拠しなくなった場合（CRLReason #4, superseded [証明書の破棄])。
7. 本 CA が証明書の不正使用の証拠を得た場合（CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
8. 利用者が利用契約または利用規約に基づく重大な義務の 1 つ以上に違反していることを本 CA が知り得た場合（CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
9. 本 CA が、証明書内における FQDN または IP アドレスの使用が法的にもはや許可されていないことを示す状況を知り得た場合(例えば、ドメイン名を使用するドメイン名登録者の権利が裁判所または調停官によって失効となった。ドメイン名登録者と申請者との間の関連するライセンス契約またはサービス契約が解除された。ドメイン名登録者がドメイン名の更新をしなかったなど）(CRLReason #5, cessationOfOperation [証明書の運用停止])。
10. 詐欺的な紛らわしい下位 FQDN を認証するためにワイルドカード証明書が使用されていたことを本 CA が知り得た場合（CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
11. 本 CA が、証明書に含まれている情報の重大な変更を知り得た場合（CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
12. 証明書が Baseline Requirements または本 CA の CP/CPS に従って発行されなかったことを本 CA が知り得た場合（CRLReason #4, superseded [証明書の破棄])。
13. 証明書に表示されている情報が不正確であると、本 CA が判断または知り得た場合 (CRLReason #9, privilegeWithdrawn [証明書を利用する権利の撤回])。
14. Baseline Requirements に基づいて証明書を発行するための本 CA の権利が期限切

れ、失効、または停止となった場合(本 CA が CRL/OCSP リポジトリーの維持を継続するための手配を済ませている場合を除く) (CRLReason "unspecified (0)" [未定義]の場合、CRL に reasonCode 拡張が提供されない)。

15. 本セクション 4.9.1.1 で指定する必要のない理由により、CA の CP/CPS により失効が必要とされる場合 (CRLReason "unspecified (0)" [未定義]の場合、CRL に reasonCode 拡張が提供されない)。
16. 本 CA が、利用者の私有鍵を危殆化させる実証済みの方法、または私有鍵の生成に使用された特定の方法に欠陥があるという明確な証拠があることを認識した場合 (CRLReason #1, keyCompromise [私有鍵の危殆化])。

4.9.2 証明書の失効申請を行うことができる者

証明書の失効申請を行うことができる者は、利用者または申請者とする。なお、本 CP/CPS「4.9.1 証明書失効事由」に該当すると本 CA が判断した場合、本 CA が申請者となる場合もある。

また、RA、本 CA が失効手続きを開始できる。加えて、利用者、依拠当事者、アプリケーションソフトウェアサプライヤー、およびその他の第三者は、証明書失効に関する妥当な根拠となる証明書問題レポートを本 CA に提出できる。

4.9.3 失効申請手続

利用者または申請者は、本 CA または外部委託先が提供するアプリケーションなどを使用し、定める手続きを行うことにより本 CA へ届け出るものとする。

本 CA は、所定の手続によって受け付けた情報を確認し、証明書の失効処理を行う。

4.9.4 失効申請の猶予期間

利用者または申請者は、私有鍵が危殆化したまたは危殆化のおそれがあると判断した場合には、すみやかに失効申請を行わなければならない。

4.9.5 認証局が失効申請を処理しなければならない期間

本 CA は、有効な失効申請を受け付けてからすみやかに証明書の失効処理を行い、CRL へ当該証明書情報を反映させる。

証明書問題レポートを受領してから 24 時間以内に、本 CA は証明書問題レポートに関する事実と状況の調査を開始するものとし、利用者と証明書問題レポートを提出した事業体両者の見分に基づく予備調査報告書を提出する。

事実と状況のレビュー後、本 CA は利用者そして証明書問題レポートを報告した事業、または他の失効関連告知と協力するものとし、証明書を失効させるか否か、もしそうなら、本 CA が証明書を失効させる日時を決定する。証明書問題レポートまたは失効関連告知の

受領から失効までの期間は、本 CP「4.9.1 証明書失効事由」に記載された時間枠を超えない。

CA に選ばれた日時は次の基準を考慮する。

1. 申し立てられた問題の性質(範囲、状況、厳しさ、規模、被害リスク)
2. 失効の結果(利用者と依拠当事者への直接的そして間接的影響)
3. 特定の証明書または利用者に関して受領した証明書問題レポートの数
4. 苦情を申し立てている組織体

なお、本 CA は、失効日が指定された失効申請を受領した場合は、指定日に失効を行う。

4.9.6 失効確認の要求

本 CA が発行する証明書には、CRL 格納先の URL、および OCSP レスポンダーの URL を記載する。

CRL および OCSP レスポンダーは、一般的な Web インターフェースを用いてアクセスすることができる。なお、CRL には、有効期限の切れた証明書情報は含まれない。

検証者は、利用者の証明書について、有効性を確認しなければならない。証明書の有効性は、リポジトリーに掲載している CRL または OCSP レスポンダーにより確認する。

4.9.7 証明書失効リストの発行頻度

CRL は、アクセス可能な HTTP URL 経由で公開する。

最初の証明書の発行から 24 時間以内に、本 CA は、次のいずれかを生成および公開する。full かつ完全な CRL、または分割 CRL(集約された場合、full かつ完全な CRL と同等になる)。

本 CA が CRL を発行する場合、本 CA は少なくとも 7 日に一度は CRL を更新・再発行し、 nextUpdate フィールドの値は thisUpdate フィールドの値よりも 10 日以上先にしないものとする。

4.9.8 証明書失効リストの発行最大遅延時間

本 CA が発行した CRL は、合理的な時間内にリポジトリーに反映させる。

4.9.9 オンラインでの失効/ステータス確認の適用性

OCSP レスポンスは、RFC 6960 や RFC 5019 に準拠している必要がある。OCSP レスポンスは、以下のいずれかの条件を満たす必要がある。

1. 失効ステータスの確認対象となる証明書を発行した CA によって署名されている。
2. 失効ステータスの確認対象となる証明書を発行した CA によって証明書が署名されている OCSP レスポンダーによって署名されている。

後者の場合、OCSP 署名証明書には、RFC 6960 に定義されている、タイプ id-pkix-ocsp-

nochek の拡張領域が含まれていなければならない。

4.9.10 オンラインでの失効/ステータス確認を行うための要件

検証者は、利用者の証明書について、有効性を確認しなければならない。リポジトリーに掲載している CRL により、証明書の失効登録の有無を確認しない場合には、OCSP レスポンダーにより提供される証明書ステータス情報の確認を行わなければならない。

RFC 6960 および/または RFC 5019 で説明されているように、CA が運用する OCSP レスポンダーは HTTP GET メソッドをサポートする必要がある。

OCSP 応答の有効期間は、thisUpdate と nextUpdate の時間差（両端を含む）である。その差を算出する目的で、うるう秒を無視すると、3,600 秒の差は 1 時間に等しく、86,400 秒の差は 1 日に等しくなる。

利用者証明書のステータスの場合

1. OCSP 応答には、8 時間以上の有効期間が必要である。
2. OCSP 応答には、10 日以下の有効期間が必要である。
3. 有効期間が 16 時間未満の OCSP 応答の場合、CA は nextUpdate の前の有効期間半分に先立ち、オンライン証明書ステータスプロトコルを介して提供される情報を更新する必要がある。
4. 有効期間が 16 時間以上の OCSP 応答の場合、CA は nextUpdate の少なくとも 8 時間前、および thisUpdate の 4 日後までに、オンライン証明書ステータスプロトコルを介して提供される情報を更新する必要がある。

下位 CA 証明書のステータスの場合

CA は、

i. 少なくとも 12 カ月ごと、および

ii. 下位 CA 証明書の失効から 24 時間以内にオンライン証明書ステータスプロトコルを介して提供された情報を更新するものとする。

OCSP レスポンダーが「未使用」の証明書シリアル番号のステータスのリクエストを受信した場合、レスポンダーは「good」ステータスで応答すべきではない。OCSP レスポンダーが本 CP「7.1.5 名前制約」に沿って技術的に制約されていない CA 向けである場合、レスポンダーはそのような要求に対して「good」ステータスで応答してはならない。
本 CA は、セキュリティ応答手順の一部として、「未使用」シリアル番号のリクエストについて OCSP レスポンダーを監視するべきである。

OCSP レスポンダーは、「予約済み」証明書のシリアル番号について、Precertificate [RFC 6962]に一致する対応する証明書があるかのように、明確な応答を提供する場合がある。

OCSP 要求内の証明書シリアル番号は、次の 3 つのオプションのいずれか

1. その CA の主体者に関連付けられている現在または以前のキーを使用して、そのシ

リアル番号の証明書が発行 CA によって発行された場合、「割り当て済み」
2. そのシリアル番号を持つ事前証明書 [RFC 6962]が a または b のいずれか
   a. 発行 CA によって発行された場合、「予約済み」
   b. 発行 CA に関連付けられた事前証明書署名証明書[RFC 6962]
3. 上記の条件のいずれも満たされない場合は「未使用」

4.9.11 利用可能な失効情報の他の形式

本 CA は、RFC 4366 (Transport Layer Security (TLS) Extensions)、RFC 5246 (The Transport Layer Security (TLS) Protocol Version 1.2)、RFC 8446 (The Transport Layer Security (TLS) Protocol Version 1.3)に従い、利用者に OCSP ステープリングの利用を許容する。

4.9.12 鍵の危殆化に対する特別要件

検証者は、次の方法で鍵の危殆化を実証するものとする。

- 私有鍵自体の提出、または私有鍵を含むデータと、データから私有鍵を抽出する方法の提出
- 危殆化されたと認識される識別名などのデータを含み、かつ署名の検証ができる CSR の提出
- 公開鍵によって検証可能な、本 CA が指定したチャレンジ・レスポンスと公開鍵への私有鍵による署名の提出
- 侵害を検証できる脆弱性や、参照したセキュリティ・インシデント・ソースの提供

本 CA は、利用者の私有鍵が危殆化した可能性があることを知りえた場合、利用者に私有鍵が危殆化された可能性があることを通知する。

なお本 CA が、私有鍵が危殆化した、または危殆化のおそれがあると判断した場合、本 CP「4.9.1 証明書失効事由」の対応を行うものとする。

4.9.13 証明書の一時停止事由

本 CA は、証明書の一時停止は行わない。

4.9.14 証明書の一時停止申請を行うことができる者

適用外とする。

4.9.15 証明書の一時停止申請手続

適用外とする。

4.9.16 一時停止を継続することができる期間

適用外とする。

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

利用者は OCSP レスポンダーを通じて証明書ステータス情報を確認することができる。本 CA は、CRL または OCSP レスポンスの失効エントリーは、失効した証明書の有効期限日が過ぎるまで削除してはならない。

4.10.2 サービスの利用可能性

本 CA は、通常の運用状況の下で 10 秒以内のレスポンス時間を提供するために十分なリソースで、CRL および OCSP 機能を運用および維持するものとする。

本 CA は、アプリケーションソフトウェアが、本 CA によって発行されたすべての有効期限内証明書の現在のステータスを自動的にチェックするために使用できるオンラインリポジトリを 24 時間 365 日体制で維持するものとする。

本 CA は、優先度の高い証明書問題の報告を内部で対応し、必要に応じて当該苦情を法執行機関に通報し、または当該苦情の対象となった証明書を失効させる能力を 24 時間 365 日維持しなければならない。

4.10.3 オプショナルな仕様

規定しない。

4.11 利用の終了

利用者は証明書の利用を終了する場合、証明書の失効申請を行わなければならない。なお、証明書の更新申請を行わず、該当する証明書の有効期間が満了した場合にも終了となる。

4.12 キーエスクローと鍵回復

4.12.1 キーエスクローと鍵回復ポリシーおよび実施

本 CA は、利用者の私有鍵のエスクローは行わない。

4.12.2 セッションキーのカプセル化と鍵回復のポリシーおよび実施

適用外とする。

5. 設備上、運営上、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
本項については、CPS に規定する。

5.1.2 物理的アクセス
本項については、CPS に規定する。

5.1.3 電源および空調
本項については、CPS に規定する。

5.1.4 水害対策
本項については、CPS に規定する。

5.1.5 火災対策
本項については、CPS に規定する。

5.1.6 媒体保管
本項については、CPS に規定する。

5.1.7 廃棄処理
本項については、CPS に規定する。

5.1.8 オフサイトバックアップ
本項については、CPS に規定する。

5.2 手続的管理

5.2.1 信頼すべき役割
本項については、CPS に規定する。

5.2.2 職務ごとに必要とされる人数
本項については、CPS に規定する。

5.2.3 個々の役割に対する本人性確認と認証

本項については、CPS に規定する。

5.2.4 職務分割が必要となる役割

本項については、CPS に規定する。

5.3 人事的管理

5.3.1 資格、経験および身分証明の要件

本項については、CPS に規定する。

5.3.2 背景調査

本項については、CPS に規定する。

5.3.3 教育要件

本項については、CPS に規定する。

5.3.4 再教育の頻度および要件

本項については、CPS に規定する。

5.3.5 仕事のローテーションの頻度および順序

本項については、CPS に規定する。

5.3.6 認められていない行動に対する制裁

本項については、CPS に規定する。

5.3.7 独立した契約者の要件

本項については、CPS に規定する。

5.3.8 要員へ提供される資料

本項については、CPS に規定する。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類

本項については、CPS に規定する。

5.4.2 監査ログを処理する頻度

本項については、CPS に規定する。

5.4.3 監査ログを保持する期間

本項については、CPS に規定する。

5.4.4 監査ログの保護

本項については、CPS に規定する。

5.4.5 監査ログのバックアップ手続

本項については、CPS に規定する。

5.4.6 監査ログの収集システム

本項については、CPS に規定する。

5.4.7 イベントを起こした者への通知

本項については、CPS に規定する。

5.4.8 脆弱性評価

本項については、CPS に規定する。

5.5 記録の保管

5.5.1 アーカイブの種類

本項については、CPS に規定する。

5.5.2 アーカイブ保存期間

本項については、CPS に規定する。

5.5.3 アーカイブの保護

本項については、CPS に規定する。

5.5.4 アーカイブのバックアップ手続

本項については、CPS に規定する。

5.5.5 記録にタイムスタンプを付与する要件

本項については、CPS に規定する。

5.5.6 アーカイブ収集システム

本項については、CPS に規定する。

5.5.7 アーカイブの検証手続

本項については、CPS に規定する。

5.6 鍵の切り替え

本 CA の鍵ペア更新または証明書更新は、原則として利用者に発行した証明書の最大有効期間よりも短くなる前に実施する。新しい鍵ペアが生成された後は、新しい鍵ペアを使って証明書および CRL の発行を行う。

5.7 危殆化および災害からの復旧

5.7.1 事故および危殆化時の手続

本項については、CPS に規定する。

5.7.2 ハードウェア、ソフトウェアまたはデータが破損した場合の手続

本項については、CPS に規定する。

5.7.3 私有鍵が危殆化した場合の手続

本項については、CPS に規定する。

5.7.4 災害後の事業継続性

本項については、CPS に規定する。

5.8 認証局または登録局の終了

本 CA を終了する場合、3 か月前に外部委託先を通じて利用者、アプリケーションソフトウェアサプライヤーを含むその他の関係者にその旨を通知する。本 CA によって発行されたすべての証明書は、本 CA の終了以前に失効を行う。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成およびインストール

6.1.1 鍵ペアの生成

本項については、CPS に規定する。

6.1.2 利用者に対する私有鍵の交付

本 CA から私有鍵の交付は行わない。

6.1.3 認証局への公開鍵の交付

本 CA に対する利用者の公開鍵の交付は、オンラインによって行うことができる。この時の通信経路は TLS により暗号化を行う。

6.1.4 検証者への CA 公開鍵の交付

検証者は、本 CA のリポジトリーにアクセスすることによって、本 CA の公開鍵を入手することができる。

6.1.5 鍵サイズ

本項については、CPS に規定する。

6.1.6 公開鍵のパラメーターの生成および品質検査

本項については、CPS に規定する。

6.1.7 鍵の用途

本 CA および本 CA が発行する証明書の鍵の用途は以下のとおりとする。

表 6.1-1 鍵の用途

	本 CA	本 CA が発行する証明書
digital Signature	―	yes
nonRepudiation	―	―
keyEncipherment	―	yes （エンドエンティティ証明書の公開鍵が RSA の場合は任意、ECDSA の場合は禁止）
dataEncipherment	―	―
keyAgreement	―	―

keyCertSign	yes	—
cRLSign	yes	—
encipherOnly	—	—
decipherOnly	—	—

6.2 私有鍵の保護および暗号装置技術の管理

6.2.1 暗号装置の標準および管理

本 CA の私有鍵の生成、保管、署名操作は、CPS「6.2.7 私有鍵の暗号モジュールへの格納」準拠の暗号装置を用いて行う。利用者の私有鍵については規定しない。

6.2.2 私有鍵の複数人管理

本 CA の私有鍵の活性化、非活性化、バックアップ等の操作は、安全な環境において複数人の権限者によって行う。利用者の私有鍵の活性化、非活性化、バックアップ等の操作は、利用者の管理の下で安全に行わなければならない。

6.2.3 私有鍵のエスクロー

本 CA は、本 CA の私有鍵のエスクローは行わない。

本 CA は、利用者の私有鍵のエスクローは行わない。

6.2.4 私有鍵のバックアップ

本 CA の私有鍵のバックアップは、セキュアな室において複数名の権限者によって行われ、暗号化された状態で、セキュアな室に保管される。

利用者の私有鍵のバックアップは、利用者の管理の下で安全に保管しなければならない。

6.2.5 私有鍵のアーカイブ

本 CA では、本 CA の私有鍵のアーカイブは行わない。

利用者の私有鍵については規定しない。

6.2.6 私有鍵の暗号モジュールへのまたは暗号モジュールからの転送

本 CA の私有鍵の暗号装置への転送または暗号装置からの転送は、セキュアな室において、私有鍵を暗号化した状態で行う。利用者の私有鍵については規定しない。

6.2.7 私有鍵の暗号モジュールへの格納

本電子認証基盤の上で運用される CA の私有鍵は、CPS「6.2.7 私有鍵の暗号モジュールへの格納」準拠の暗号装置で保護する。利用者の私有鍵については規定しない。

6.2.8 私有鍵の活性化方法

本 CA の私有鍵の活性化は、セキュアな室において複数名の権限者によって行う。利用者の私有鍵については規定しない。

6.2.9 私有鍵の非活性化方法

本 CA の私有鍵の非活性化は、セキュアな室において複数名の権限者によって行う。

利用者の私有鍵については規定しない。

6.2.10 私有鍵の破棄方法

本 CA の私有鍵の廃棄は、複数名の権限者によって完全に初期化または物理的に破壊することによって行う。バックアップについても同様の手続によって行う。

利用者の私有鍵については規定しない。

6.2.11 暗号装置の評価

本 CA で使用する暗号装置の品質基準については、本 CP「6.2.1.暗号装置の標準および管理」のとおりである。利用者の私有鍵については規定しない。

6.3 鍵ペアのその他の管理方法

6.3.1 公開鍵のアーカイブ

本 CA の公開鍵については CPS「6.2.1 暗号装置の標準および管理」のとおりである。

利用者の私有鍵については規定しない。

6.3.2 私有鍵および公開鍵の有効期間

本項については、CPS に規定する。

6.4 活性化データ

6.4.1 活性化データの生成および設定

本項については、CPS に規定する。

6.4.2 活性化データの保護

本項については、CPS に規定する。

6.4.3 活性化データの他の考慮点

本項については、CPS に規定する。

6.5 コンピュータのセキュリティ管理

6.5.1 システム開発管理

本 CA は、証明書を直接発行させることができるすべてのアカウントに対して、多要素認証を実施するものとする。

6.5.2 セキュリティ運用管理

本項については、CPS に規定する。

6.6 ライフサイクルセキュリティ管理

6.6.1 システム開発管理

本項については、CPS に規定する。

6.6.2 セキュリティ運用管理

本項については、CPS に規定する。

6.6.3 ライフサイクルセキュリティ管理

本項については、CPS に規定する。

6.7 ネットワークセキュリティ管理

本項については、CPS に規定する。

6.8 タイムスタンプ

本項については、CPS に規定する。

7. 証明書および証明書失効リストおよび OCSP のプロファイル

7.1 証明書のプロファイル

本 CA は、本 CP「2.2 証明書情報の公開」、本 CP「6.1.5 鍵サイズ」、本 CP「6.1.6 公開鍵のパラメーターの生成および品質検査」に規定された技術要件を満たすものとする。

本 CA が利用者証明書を発行する際、暗号論的擬似乱数生成器(CSPRNG)からの 64 ビット以上の出力を含む 1 以上かつ 2^{159} 未満の連番ではない証明書シリアル番号を生成するものとする。

本 CA が発行する証明書は RFC 5280 に準拠している。プロファイルは、次表のとおりである。

Baseline Requirements 7.1.2.9 に従い、TLS サーバー証明書の事前証明書の Version, Serial Number, Signature, Issuer, Validity, Subject, SubjectPublicKeyInfo, SignatureAlgorithm は、TLS サーバー証明書とエンコードされた値がバイト単位で同一とする。「Certificate Transparency 用拡張」以外の拡張領域は、順序、Critical、エンコードされた値がバイト単位で同一とする。事前証明書には、事前証明書ポイズン拡張（OID: 1.3.6.1.4.1.11129.2.4.3)を含む。この拡張は、extnValue OCTET STRING を持つ。この extnValue OCTET STRING は、RFC 6962 のセクション 3.1 で規定されている ASN.1 NULL 値の符号化表現である「0500」を正確に 16 進符号化したものとする。

表 7.1-1　TLS サーバー証明書プロファイル

基本領域		設定内容	Critical
version		Version 3	-
serialNumber		CSPRNG からの 64 ビット以上の出力を含む 1 以上かつ 2^{159} 未満の連番ではない値	-
signatureAlgorithm		以下のいずれか。 sha256WithRSAEncryption sha384WithRSAEncryption ecdsa-with-SHA384	-
issuer	countryName	JP	-
	organizationName	本 CA の組織名	-
	commonName	本 CA のコモンネーム	-
validity	notBefore	証明書署名以前の時刻で 48 時間以内の値	-
	notAfter	CPS「6.3.2 私有鍵および公開鍵の有効期間」に規定	-

subject	businessCategory	必須（EV 証明書）	-
	jurisdictionCountryName	必須（EV 証明書） JP	-
	serialNumber	必須（EV 証明書）	-
	countryName	JP（OV 証明書と EV 証明書）	-
	stateOrProvinceName	必須（OV 証明書と EV 証明書）	-
	localityName	必須（OV 証明書と EV 証明書）	-
	organizationName	必須（OV 証明書と EV 証明書）	-
	organizationalUnitName	禁止	-
	commonName	任意 証明書の Subject Alternative Name 拡張機能に含まれる値の 1 つであるエントリーが 1 つだけ含まれていなければならない。値は、Subject Alternative Name 拡張機能からの dNSName エントリー値の文字ごとのコピーとしてエンコードされなければならない。具体的には、完全修飾ドメイン名のすべてのドメインラベルの FQDN 部分を LDH ラベルとしてエンコードする必要があり、P ラベルを Unicode 表現に変換してはならない。予約済み IP アドレスまたは内部名を含んではならない。	-
subjectPublicKeyInfo		以下のいずれか。 RSA2048 ビット、3072 ビット、4096 ビット ECDSA384 ビット（secp384r1）、256 ビット（secp256r1）	-
拡張領域		設定内容	Critical
keyUsage		digitalSignature, (keyEncipherment) * subjectPublicKeyInfo が RSA の場合は、keyEncipherment は任意。ECDSA の場合は、keyEncipherment	Y

	は禁止。	
extKeyUsage	id-kp-serverAuth, id-kp-clientAuth * id-kp-clientAuth は任意。	N
subjectAltName	必須 dNSName を少なくとも 1 つを含む。 dNSName: エントリーには、CA が本 CP「3.2.2.4　ドメインの認証」に従って検証した完全修飾ドメイン名を含む。エントリーに内部名を含めることはできない。エントリーに含まれる完全修飾ドメイン名の FQDN 部分は、U + 002E FULL STOP（ ". "）文字で結合された LDH ラベルで完全に構成されていなければならない。インターネットドメインネームシステムのルートゾーンを表す長さゼロのドメインラベルを含めてはならない。 完全修飾ドメイン名の FQDN 部分は、P-Labels または非予約 LDH Labels であるドメインラベルのみで構成されていなければならない。	N
certificatePolicies	policyIdentifier ● [1]policyIdentifier=CABF Reserved Certificate Policy Identifier（CABF 予約済み証明書ポリシー識別子、最初の値として Reserved Certificate Policy Identifier を記載することを推奨） ● [2]policyIdentifier OID=本 CP の[1.2-1 OID]を設定（DV 証明書と OV 証明書の場合は任意、EV 証明書の場合は必須） policyQualifiers ● policyQualifierID=id-qt-cps	N

	● qualifiier=本 CA のリポジトリー HTTP(S) URL（任意） * policyQualifier は DV 証明書と OV 証明書の場合は非推奨、EV 証明書の場合は必須。	
crlDistributionPoints	本 CA の CRL サービスの HTTP URL * Authority Information Access 拡張に id-ad-ocsp accessMethod が存在する場合は任意。	N
authorityInformationAccess	accessMethod id-ad-ocsp（1.3.6.1.5.5.7.48.1） accessLocation OCSP レスポンダーの HTTP URL id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessLocation 本 CA 証明書の HTTP URL	N
authorityKeyIdentifier	発行者公開鍵の 160 ビット SHA-1 ハッシュ値	N
subjectKeyIdentifier	任意 主体者公開鍵の 160 ビット SHA-1 ハッシュ値	N
Signed Certificate Timestamp List（1.3.6.1.4.1.11129.2.4.2）	任意 SignedCertificateTimestampList の値	N

表 7.1-2　OCSP レスポンダー証明書プロファイル

基本領域		設定内容	Critical
version		Version 3	-
serialNumber		CSPRNG からの 64 ビット以上の出力を含む 1 以上かつ 2^{159} 未満の連番ではない値	-
signatureAlgorithm		以下のいずれか。 sha256WithRSAEncryption sha384WithRSAEncryption ecdsa-with-SHA384	-
issuer	countryName	JP	-
	organizationName	本 CA の組織名	-
	commonName	本 CA のコモンネーム	-
validity	notBefore	証明書署名以前の時刻で 1 日以内の値	-
	notAfter	CPS「6.3.2 私有鍵および公開鍵の有効期間」に規定	-
subject	countryName	JP	-
	organizationName	本 CA の組織名	-
	commonName	OCSP レスポンダー名	-
subjectPublicKeyInfo		以下のいずれか。 RSA2048 ビット、3072 ビット、4096 ビット ECDSA384 ビット（secp384r1）、256 ビット（secp256r1）	-
拡張領域		設定内容	Critical
keyUsage		digitalSignature	Y
extKeyUsage		id-kp-OCSPSigning	N
id-pkix-ocsp-nocheck		NULL	N
certificatePolicies		禁止	N
authorityKeyIdentifier		発行者公開鍵の 160 ビット SHA-1 ハッシュ値	N
subjectKeyIdentifier		主体者公開鍵の 160 ビット SHA-1 ハッシュ値	N

7.1.1 バージョン番号

本 CA は、X.509 v3 を使用する。

7.1.2 証明書拡張

本 CA が発行する証明書は、RFC 5280 に準拠した証明書拡張フィールドを使用する。「7.1 証明書のプロファイル」に記載の証明書プロファイルに証明書拡張を含んでいる。

7.1.3 アルゴリズムオブジェクト識別子

本サービスにおいて用いられるアルゴリズム OID は、次のとおりである。

アルゴリズム	オブジェクト識別子
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3 }

7.1.4 名前形式

本 CA では、RFC 5280 で定められる、識別名を使用する。

すべての有効な認証パス（RFC 5280、セクション 6 で定義されているとおり）について認証パスの利用者証明書ごとに、証明書発行者の識別名フィールドのエンコードされた内容は、発行される CA 証明書の主体者識別名フィールドのエンコードされた形式とバイト単位で同一である必要がある。

本 CA は、証明書を発行することにより、CP/CPS に定められた手順に従い、証明書の発行日時点で、すべての識別名が正確であることを確認することを表明する。本 CA は、Baseline Requirements セクション 3.2.2.4 に定める場合を除き、識別名にドメイン名を含めてはならない。

識別名には、'.'、'-'、''（スペース）文字などのメタデータや、値が存在しない、不完全、または適用できないことを示すその他の記号のみを含めてはならない。

本 CA では、予約済み IP アドレスまたは内部名を含む Subject Alternative Name 拡張領域または「コモンネーム」フィールドを持つ証明書を発行しない。

「コモンネーム」の値が完全修飾ドメイン名またはワイルドカードドメイン名の場合、「コモンネーム」の値は、Subject Alternative Name 拡張領域の dNSName エントリー値の 1 文字ずつのコピーとしてエンコードする。具体的には、完全修飾ドメイン名のすべてのドメインラベルまたはワイルドカードドメイン名の FQDN 部分のすべての Domain Labels は LDH Labels としてエンコードし、P-Labels は Unicode に変換しない。

7.1.5 名前制約

本 CA では設定しない。

7.1.6 CP オブジェクト識別子

本 CA から発行する証明書の OID は、本 CP「1.2 文書名と識別」の OID のとおりである。

次の証明書ポリシー識別子は、証明書または利用者証明書が Baseline Requirements に準拠していることを表明するオプションの手段として本 CA が使用するために用意されている。

CABF Reserved Certificate Policy Identifier（CABF 予約済み証明書ポリシー識別子）

(1) {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)
(2) {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)
(3) {joint - iso - itu - t(2) international - organizations(23) ca - browser - forum(140) certificate - policies(1) ev-guidelines(1)} (2.23.140.1.1)

7.1.7 ポリシー制約拡張の利用

設定しない。

7.1.8 ポリシー修飾子の文法および意味

ポリシー修飾子については、本 CP および CPS を公表する Web ページの URI を格納することができる。

7.1.9 重要な証明書ポリシー拡張の処理の意味

設定しない。

7.2 CRL のプロファイル

本 CA が発行する CRL は RFC 5280 に準拠している。プロファイルは、次表のとおりである。

表 7.2-1　CRL プロファイル

基本領域		設定内容	Critical
version		Version 2	-
signatureAlgorithm		以下のいずれか。 sha256WithRSAEncryption sha384WithRSAEncryption ecdsa-with-SHA384	-
issuer	countryName	JP	-
	organizationName	本 CA の組織名	-
	commonName	本 CA のコモンネーム	-
thisUpdate		CRL の発行日時	-
nextUpdate		次の CRL が発行される日時。 thisUpdate から最大 10 日後。	-
revokedCertificates	serialNumber	失効した証明書に含まれる serialNumber とバイト単位で同一の値	-
	revocationDate	通常、失効が発生した日時	-
	crlEntryExtensions reasonCode	「7.2.2 CRL 拡張」に規定した値	-
拡張領域		設定内容	Critical
CRLNumber		CRL 番号	N
authorityKeyIdentifier		発行者公開鍵の 160 ビット SHA-1 ハッシュ値	N

7.2.1 バージョン番号

本 CA は、RFC 5280 に規定された X.509 v2 CRL を使用する。

7.2.2 CRL 拡張

表 7.2-2-1　CRL 拡張

拡張（Extension）	存在	Critical	説明
authorityKeyIdentifier	必須	N	-

CRLNumber	必須	N	0 以上 2^{159} 未満の INTEGER（数値）を含む。
IssuingDistributionPoint	*	Y	この拡張は、full かつ完全な CRL には推奨されない。 本 CA では、 full かつ完全な CRL を使用している。
Any other extension	非推奨	-	-

表 7.2-2-2　revokedCertificates Component

Component	有無	説明
serialNumber	必須	失効した証明書に含まれる serialNumber とバイト単位で同一。
revocationDate	必須	通常、失効が発生した日時。バックデートが許可される状況については、この表の下を参照。
crlEntryExtensions	*	要件については、「表 7.2-2-3　crlEntryExtensions Component」を参照。

証明書の CRL エントリーに示されている失効日より前に証明書の私有鍵が危殆化したと判断された場合、本 CA は CRL エントリーの失効日を更新するべきである。revocationDate フィールドの日付を遡ることは、RFC 5280 (セクション 5.3.2) で説明されているベストプラクティスの例外である。しかし、Baseline Requirements では、証明書が危殆化したと最初に判断する日付として revocationDate フィールドを処理する TLS 実装をサポートするために revocationDate フィールドの使用を規定する。

表 7.2-2-3　crlEntryExtensions Component

CRL Entry Extension	有無	説明
reasonCode	*	存在する場合（OID 2.5.29.21）、Critical と表示されず、証明書を失効させる最も適切な理由を示す。 ただし、CRL エントリーが技術的に発行できない証明書に関するものであり、かつ、1)CRL エントリーが 2023 年 7 月 15 日より前に失効した本要件の対象である利用者証明書に関するものである場合、または 2)失効の理由（すなわち、reasonCode）が不特定（0）である場合を除く。 要件については、「CRLReasons」の表を参照。
Any other value	非推奨	-

表 7.2-2-4　CRLReasons

RFC 5280 reasonCode	RFC 5280 reasonCode value	説明
unspecified	0	reasonCode の省略により表される。ただし、CRL エントリーが、2023 年 7 月 15 日より前に失効した Baseline Requirements の対象である利用者証明書に対するものである場合を除く。
keyCompromise	1	利用者の私有鍵が危殆化したことが判明している、またはその疑いがあることを示す。
affiliationChanged	3	主体者の名前または証明書内のその他の主体者識別情報が変更されたが、証明書の私有鍵が危殆化されたと疑うに足る根拠がないことを示す。
superseded	4	利用者が新しい証明書を要求したこと、本 CA が証明書に含まれる FQDN または IP アドレスに対するドメインの承認または管理の検証は信頼すべきでないという合理的な証拠を得たこと、あるいは本 CA は、証明書が Baseline Requirements または本 CA の CP/CPS に準拠していない等のコンプライアンス上の理由により証明書を失効したことを示す。
cessationOfOperation	5	証明書の有効期間満了前に、証明書を含むウェブサイトが閉鎖されたこと、あるいは証明書の有効期間満了前に、利用者が証明書に含まれるドメイン名を所有または管理しなくなったことを示す。
certificateHold	6	以下のいずれかの場合、この CRL エントリーを含まない。 1)Baseline Requirements の対象である証明書。 2)Baseline Requirements の対象外の証明書で、いずれかの場合。 A)2020 年 9 月 30 日以降に発行された証明書。 B)2020 年 9 月 30 日以降の日付が notBefore に記載された証明書。

privilegeWithdrawn	9	利用者が証明書申請に際して誤解を招く情報を提供した、利用契約または利用規約に基づく重大な義務を履行しなかった等、鍵の危殆化に至らない利用者側の違反があったことを示す。

利用契約またはその中で参照されるオンラインリソースでは、利用者に上記の失効事由オプションについて通知し、各オプションを選択するタイミングについて説明を提供する必要がある。本 CA が利用者に提供するツールでは、利用者が証明書の失効を要求するときにこれらのオプションを簡単に指定できるようにする必要がある。デフォルト値は失効事由が提供されない設定とする。(デフォルトは CRLReason「unspecified (0)」に対応し、CRL に reasonCode 拡張が提供されない)。

privilegeWithdrawn 事由コードは、失効理由オプションとして利用者には提供しない。この事由コードの使用は利用者ではなく本 CA が決定する。

本 CA が、CRL エントリーに reasonCode 拡張が含まれていない、または reasonCode 拡張に keyCompromise 以外の事由が含まれている証明書において、私有鍵危殆化の検証可能な証拠を取得した場合、本 CA は CRL エントリーを更新して、reasonCode 拡張の CRLReason として keyCompromise を入力するべきである。

本 CA では、以下の reasonCode を使用するものとする。

keyCompromise (1)
affiliationChanged (3)
superseded (4)
cessationOfOperation (5)
privilegeWithdrawn (9)

7.3 OCSP のプロファイル

本 CA は、RFC 5019 および RFC 6960 に準拠する OCSP レスポンダーを提供する。2020 年 9 月 30 日以降より、OCSP 応答がルート CA または下位 CA 証明書（クロス証明書を含む）に対するものであり、その証明書が失効されている場合、CertStatus の RevokedInfo 内の revocationReason フィールドが存在する必要がある。

2020 年 9 月 30 日以降より、CRLReason は、本 CP「7.2.2 CRL 拡張」で指定されているように、CRL に許可された値を含める必要があることを示す。

7.3.1 バージョン番号

本 CA は、OCSP バージョン 1 を適用する。

7.3.2 OCSP 拡張

本 CP「7.1.証明書のプロファイル」に記載する。OCSP 応答の singleExtensions には、reasonCode（OID 2.5.29.21）CRL エントリー拡張を含めてはならない。

8. 準拠性監査と他の評価

CPS に規定する。

8.1 監査の頻度

CPS に規定する。

8.2 監査人の身元／資格

CPS に規定する。

8.3 監査人と被監査部門の関係

CPS に規定する。

8.4 監査で扱われる事項

本 CA は、必要に応じて以下の WebTrust 規準に従って監査を受けるものとする。

・WebTrust for CAs
・WebTrust for CAs SSL Baseline with Network Security
・WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL
・WebTrust Principles and Criteria for Certification Authorities - Network Security

8.5 不備の結果としてとられる処置

CPS に規定する。

8.6 監査結果の開示

CPS に規定する。

8.7 自己監査

CPS に規定する。

9. 他の業務上および法的事項

9.1 料金

9.1.1 証明書の発行または更新にかかる料金

契約書等に別途定める。

9.1.2 証明書のアクセス料金

規定しない。

9.1.3 失効またはステータス情報のアクセス料金

規定しない。

9.1.4 他サービスの料金

規定しない。

9.1.5 返金ポリシー

契約書等に別途定める。

9.2 財務的責任

9.2.1 保険の補償

本 CA の運用維持にあたり、十分な財務的基盤を維持するものとする。

本 CA は、EV Guidelines に基づくそれぞれの履行および義務に関連する以下の保険を保持するものとする。

A. 企業賠償責任保険（発生形式）、保険限度額 200 万米ドル以上。

B. 500 万米ドル以上を補償限度額とし、以下の補償を含む、専門職賠償責任／過失・不作為保険。

i. EV 証明書の発行や維持における行為、誤り、不作為、意図しない契約違反、怠慢に起因する損害賠償請求。

ii.第三者の所有権の侵害（著作権及び商標権侵害を除く）、プライバシー侵害および広告宣伝侵害に起因する損害賠償請求。

この保険は、Best's Insurance Guide の最新版で保険契約者の格付けが A- 以上（あるいは、そのような格付けを受けている会社の各メンバーからなる団体）に加入していなければならない。

本 CA は、過去 12 か月間の監査済み財務諸表に基づく 5 億米ドル以上の流動資産、および 1.0 以上の当座比率（流動資産と流動負債の比率）を有することを条件に、本ガイドラインに基づく当該当事者の履行および義務から発生する負債を自己保証してもよいものとする。

9.2.2 その他の資産

規定しない。

9.2.3 エンドエンティティの保険または保証範囲

規定しない。

9.3 企業情報の機密性

9.3.1 機密情報の範囲

本項については、CPS に規定する。

9.3.2 機密情報の範囲外の情報

本項については、CPS に規定する。

9.3.3 機密情報を保護する責任

本項については、CPS に規定する。

9.4 個人情報の保護

9.4.1 個人情報保護方針

本項については、CPS に規定する。

9.4.2 個人情報として扱われる情報

本項については、CPS に規定する。

9.4.3 個人情報とみなされない情報

本項については、CPS に規定する。

9.4.4 個人情報を保護する責任

本項については、CPS に規定する。

9.4.5 個人情報の使用に関する通知と同意

本項については、CPS に規定する。

9.4.6 司法または行政手続に沿った情報開示

本項については、CPS に規定する。

9.4.7 その他の情報開示条件

本項については、CPS に規定する。

9.5 知的財産権

本 CP は著作権を含み、当社の権利に属するものとする。

本 CP は、原文が適切に参照されることを条件に、複製することができる。「Creative Commons license Attribution-NoDerivatives (CC-BY-ND) 4.0」で公開する。

https://creativecommons.org/licenses/by-nd/4.0/

9.6 表明保証

9.6.1 CA の表明保証

当社は、本 CP および CPS に規定した内容を遵守して利用者に関する審査、証明書の登録、発行、失効を含む認証サービスを提供し、CA 私有鍵の信頼性を含む認証業務の信頼性を確保する。

本 CP および CPS に規定された保証を除き、当社は、明示的あるいは暗示的に、もしくはその他の方法を問わず、一切の保証を行わない。

本 CA は、証明書を発行することによって、下記の証明書受益者に対し、本書に規定されている証明書の保証を行うものとする。

1. 証明書の利用契約または利用規約の当事者である利用者。
2. アプリケーションソフトウェアサプライヤーによって配布されるソフトウェアにルート証明書を含めるため、ルート CA と契約を締結しているすべてのアプリケーションソフトウェアサプライヤー。
3. 有効な証明書に合理的に依拠しているすべての依拠当事者。CA は、証明書の受益者に対し、証明書が有効である間、CA が証明書の発行および管理において Baseline Requirements およびその CP/CPS に従ってきたことを表明し、保証するものとする。

証明書の保証には、具体的に以下が含まれるが、これらに限定されない。

1. ドメイン名または IP アドレスを使用する権利

   発行の時点で、本 CA が、以下を満たすこと。

   i. 証明書の主体者フィールドおよび subjectAltName 拡張領域に指定されているドメイン名および IP アドレスを使用する権利を申請者が保持または管理していること(あるいは、ドメイン名の場合のみ、かかる権利または管理が、それらを使用または管理する権利を有する他の人物によって委託されたこと)を検証するための 手順を導入していること。

   ii. 証明書を発行する際にその手順に従っていること。

   iii. CA の CP/CPS にその手順を正確に記述していること。

2. 証明書に対する承認

   発行の時点で、本 CA が、以下を満たすこと。

   i. 主体者によって証明書の発行が承認され、主体者を代表して証明書を要求する権限を申請権限者が有していることを確認するための手順を導入していること。

   ii. 証明書を発行する際にその手順に従っていること。

   iii. CA の CP/CPS にその手順を正確に記述していること。

3. 情報の正確性

   発行の時点で、本 CA が、以下を満たすこと。

   i. 証明書に含まれるすべての情報の正確性を検証するための手順を導入していること。

   ii. 証明書を発行する際にその手順に従っていること。

   iii. CA の CP/CPS にその手順を正確に記述していること。

4. 申請者のアイデンティティ

   証明書に主体者アイデンティティ情報が含まれる場合、本 CA が、以下を満たすこと。

   i. Baseline Requirements セクション 3.2 およびセクション 7.1.2 に従って申請者のアイデンティティを検証するため手順を導入していること。

   ii. 証明書を発行する際にその手順に従っていること。

   iii. CA の CP/CPS にその手順を正確に記述していること。

5. 利用契約

   本 CA および利用者が関連会社でない場合、利用者および本 CA は、Baseline Requirements を満たす法的に有効で実施可能な利用契約の当事者であること。あるいは、本 CA および利用者が同じ組織体または関連会社である場合、申請権限者が利用規約に同意したこと。

6. ステータス

   本 CA が、有効期限内のすべての証明書のステータス(有効または失効)に関する最

新情報を掲載した、24 時間 365 日アクセス可能なリポジトリーを保守し、公開していること。

7. 失効

Baseline Requirements に示された事由が発生した場合、本 CA が証明書を失効させること。

ルート CA は、自らが証明書を発行する下位 CA であるかのように、下位 CA による責務の履行と保証、下位 CA による Baseline Requirements の遵守、Baseline Requirements に基づく下位 CA のすべての責任および免責義務に対して責任を負う。

9.6.2 RA の表明保証

本 CP「9.6.1 CA の表明保証」と同様とする。

9.6.3 利用者の表明保証

本 CA は、利用契約または利用規約の一部として、CA および証明書の受益者の利益のために、申請者が本項で規定されているコミットメントおよび保証を行うことを要求するものとする。

本 CA は、CA と証明書受益者の明示的な利益のため、証明書の発行前に下記のいずれかを取得するものとする。

1. CA との利用契約に対する申請者の合意。
2. 利用規約に対する申請者の合意。

本 CA は、各利用契約または利用規約が申請者に対して法的強制力を持つことを確実にするためのプロセスを実装するものとする。いずれの場合も、契約書は、証明書要求に従って発行される証明書に準じている必要がある。CA は、電子契約または「クリックスルー」契約を使用してもよい。ただし、このような契約が法的強制力を持つと CA が判断した場合に限る。証明書要求ごとに別々の契約を用いることも、または単一の契約で複数の将来の証明書要求およびその結果発行される証明書を対象とすることもできる。ただし CA が申請者に対して発行する各証明書が、明確にその利用契約または利用規約の対象となっていることを条件とする。

利用契約または利用規約には、以下の義務および保証が申請者自身に課される(または請負やホスティングサービス関係に基づいて、申請者が本人や代理人を代表して策定した)条項が含まれていなければならない。

1. 情報の正確性

証明書要求内において、また証明書の発行に関連して CA から要求された場合において、常に正確で完全な情報を CA に提供する義務および保証。

2. 私有鍵の保護
利用者は、要求された証明書に含まれる公開鍵に対応する私有鍵（および関連する活性化データまたはデバイス（パスワードまたはトークンなど））の管理を保証し、秘密を保持し、常に適切に保護するために、あらゆる合理的な手段を講じる義務および保証を負うものとする。
3. 証明書の受理
利用者が証明書の内容の正確性を確認および検証する義務およびその保証。
4. 証明書の使用
TLS サーバー証明書の場合、証明書に記載されている subjectAltName でアクセス可能なサーバーにのみ証明書をインストールする。
すべての適用法規に準拠し、利用契約または利用規約に従う方法でのみ証明書を使用する義務およびその保証。
5. 報告および失効
以下を実行する義務および保証。
   a. 証明書に含まれる公開鍵に対応する利用者の私有鍵が不正使用または危殆化された事実または疑いがある場合、すみやかに証明書の失効を要求し、証明書と関連する私有鍵の使用を中止する。
   b. 証明書内の情報が正確ではない、または正確でなくなる場合、直ちに証明書の失効を要求し、証明書の使用を中止する。
6. 証明書の使用の終了
鍵の危殆化を理由として証明書が失効された場合、証明書に含まれる公開鍵に対応する私有鍵のすべての使用を直ちに中止する義務および保証。
7. 対応
鍵の危殆化または証明書の不正使用に関して CA から指示があった場合、指定された期間内に対応する義務。
8. 確認および承認
申請者が利用契約の条件または利用規約に違反した場合、または CA の CP、CPS、もしくは Baseline Requirements によって失効が要求された場合、CA が証明書を直ちに失効する権利があることの確認と承認。

9.6.4 検証者の表明保証

本 CA のサービスの検証者は、以下の義務を負う。

- 本 CA が発行する証明書を信頼し、本 CP および CPS に規定されている本 CA が意図する目的のみに証明書を使用すること
- 証明書を信頼しようとするときは、リポジトリー内の CRL または OCSP レスポンダーにより、証明書が失効されていないことを確認すること

- 証明書を信頼しようとするときは、当該証明書の有効期間を確認し、有効期間内であることを確認すること
- 本 CA が発行した証明書を信頼しようとするときは、当該証明書が本 CA の証明書によって署名検証できることを確認すること
- 本 CA の証明書を信頼して利用する際、本 CP および CPS に規定されている検証者として責任を負うことに合意すること

9.6.5 他の関係者の表明保証

規定しない。

9.7 無保証

本 CA は、本 CP「9.6.1 CA の表明保証」および「9.6.2 RA の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害または派生的損害に対する責任を負わず、また、いかなる逸失利益、データの紛失またはその他の間接的もしくは派生的損害に対する責任を負わない。

9.8 責任の制限

本 CP において、次の場合、本 CA は責任を負わないものとします。

- 本 CA 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一切の損害
- 確認された情報の誤りが申請者の詐欺または故意の不正行為の結果である場合、いかなる場合にも生じるすべての責任
- 利用者が自己の義務の履行を怠ったために生じた損害
- 外部委託先および利用者のシステムに起因して発生した一切の損害
- 外部委託先および利用者の環境（ハードウェア、ソフトウェア）の瑕疵、不具合あるいはその他の動作自体によって生じた損害
- 本 CA の責に帰することのできない事由で証明書および CRL、OCSP レスポンダーに公開された情報に起因する損害
- 本 CA の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- 証明書の使用に関して発生する取引上の債務等、一切の損害
- 外部委託先のサービス提供終了など、外部委託先がサービス提供の義務の履行を怠ったために生じた損害
- 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
- 天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、本 CA の業務停止に起因する一切の損害

9.9 補償

本 CA が発行する証明書に関する補償については、別途規定する。

9.10 有効期間と終了

9.10.1 有効期間

本 CP は、本委員会の承認により有効となる。

9.10.2 終了

本 CP は、本 CA を終了した時点で無効となる。

9.10.3 終了の効果と効果継続

利用者が証明書の利用を終了する場合、外部委託先がサービスの提供を終了する場合、または本 CA 自体を終了する場合であっても、その性質上存続されるべき条項は終了の事由を問わず利用者、および本 CA に適用されるものとします。

9.11 関係者間の個別通知と連絡

本 CA は必要な通知を外部委託先に行い、外部委託先は、利用者および検証者に対する必要な通知をホームページ、Email または書面等によって行う。

9.12 改訂

9.12.1 改訂手続

本 CP は、本 CA の判断によって適宜改訂され、本委員会の承認によって発効する。

9.12.2 通知方法および期間

本 CP を変更した場合、変更した本 CP をすみやかに公表することをもって、関係者に対しての告知とする。

9.12.3 オブジェクト識別子が変更されなければならない場合

認証サービス改善委員会で必要であると判断した場合に、OID を変更する。

9.13 紛争解決手続

本 CA が発行する証明書に関わる紛争について、本 CA に対して訴訟、仲裁等を含む法的解決手段に訴えようとする場合は､本CAに対して事前にその旨を通知するものとする。

仲裁および裁判地は東京都区内における紛争処理機関を専属的管轄とする。

9.14 準拠法

本 CP、CPS の解釈、有効性および証明書の利用にかかわる紛争については、日本国の法律を適用する。

9.15 適用法の遵守

本 CA は、国内における各種輸出規制を遵守し、暗号ハードウェアおよびソフトウェアを取扱うものとする。

9.16 雑則

9.16.1 完全合意条項

当社は、利用者または検証者の義務等を本 CP、サービス利用規定等および CPS によって包括的に定め、これ以外の口頭であると書面であるとを問わず、いかなる合意も効力を有しないものとする。

9.16.2 権利譲渡条項

当社が本 CA を第三者に譲渡する場合、本 CP、サービス利用規定等および CPS において記載された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 CP、サービス利用規定等および CPS の一部の条項が無効であったとしても、当該文書に記述された他の条項は有効であるものとする。

Baseline Requirements と本 CA が業務の遂行と証明書の発行を行う地域の法律､規制、行政命令(以下、「法律」という)との間に矛盾が生じる場合、本 CA は、矛盾する要件が地域で有効かつ合法となるために必要な最小限の範囲内で Baseline Requirements の修正を行うことができる。このことは、その法律の対象となる業務または証明書発行にのみ適用される。そのような場合、本 CA はただちに(また修正された要件に基づいて証明書を発行する前に)、本 CA の CPS の本項に、Baseline Requirements への修正を必要としている法律への詳細な参照と、本 CA によって実施された Baseline Requirements への具体的な修正を盛り込むものとする。

本 CA は(修正された要件に基づく証明書を発行する前に) CA/Browser Forum に対し、CPS に新たに追加された情報について、questions@cabforum.org 宛に Email を送信するとともに、それがパブリックメーリングリストに掲載されたこと、および https://cabforum.org/pipermail/public/ (または CA/Browser Forum が指定するその他の

Email アドレスやリンク)で閲覧可能なパブリックメールアーカイブでインデックス化されたことを確認する通知を受信する必要がある。これにより、CA/Browser Forum は Baseline Requirements を改訂するかどうかを適宜検討できる。

法律が適用されなくなった場合、または Baseline Requirements が修正され、Baseline Requirements と法律を同時に遵守することが可能となった場合、本項に基づく本 CA の運用変更を中止する必要がある。前述した運用への適切な変更、本 CA の CPS に対する修正、および CA/Browser Forum への通知は、90 日以内に行われる必要がある。

9.16.4 強制執行条項

本サービスに関する紛争は東京地方裁判所を管轄裁判所とし、当社は、各規定文書の契約条項に起因する紛争、当事者の行為に関する損害、損失および費用について、補償および弁護士費用を当事者に求めることができる。

9.16.5 不可抗力

当社は、天変地異、地震、噴火、火災、津波、水災、落雷、動乱、テロリズム、その他の不可抗力により生じた一切の損害について、その予見可能性の有無を問わず一切責任を負わないものとし、本 CA の提供を不可能にするに至ったときは、当社はその状況の止むまでの間、本 CA を停止することができる。

9.17 その他の条項

規定しない。