企業認証 証明書ポリシー
（Certificate Policy）

Version 1.22

2024 年 4 月 1 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	2018/07/24	初版発行
1.10	2018/10/12	プロファイルの内容変更
1.11	2019/05/24	全体的な文言および体裁の見直し ドメインの認証の IP アドレス削除
1.12	2020/03/30	章立ての見直し、および一部「規定しない」の内容追加
1.13	2020/09/01	証明書有効期間 825 日から 398 日へ変更
1.14	2020/09/29	CRL プロファイルの Reason code を修正
1.15	2020/12/18	CP に割り当てられている OID を追加 Security Communication ECC RootCA1 より発行された CA のプロファイル追加
1.16	2021/05/31	ドメイン認証に関する記述の修正 証明書失効事由の修正 鍵の危殆化に対する特別要件の追記
1.17	2021/06/15	文言および体裁の見直し 証明書失効事由の修正
1.18	2021/11/30	ドメイン認証に関する記述の修正 全体的な文言および体裁の見直し
1.19	2022/06/10	全体的な文言および体裁の見直し
1.20	2023/05/17	「1.2 文書名と識別」を更新 「2.3　公開の時期または頻度」を更新 「4.9.1 証明書失効事由」を更新 「5.5.1　アーカイブの種類」を更新 「5.5.2　アーカイブ保存期間」を更新 「5.5.3　アーカイブの保護」を更新 「5.5.4　アーカイブのバックアップ手続」を更新 「5.5.5　記録にタイムスタンプを付与する要件」を更新 「5.5.6　アーカイブ収集システム」を更新 「5.5.7　アーカイブの検証手続」を更新 「5.7.1　事故および危殆化時の手続」を更新 「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」を更新 「5.7.3　私有鍵が危殆化した場合の手続」を更新 「5.7.4　災害後の事業継続性」を更新

		「7.1 証明書のプロファイル」を更新 「7.2 CRL のプロファイル」を更新 「7.2.2 CRL 拡張」を更新
1.21	2023/08/28	「1.6　定義と略語」を更新 「7.1　証明書のプロファイル」を更新
1.22	2024/04/01	「1.1 概要」を更新 「1.6 定義と略語」を更新 「2.2 証明情報の公開」を更新 「3.2.2.4　ドメインの認証」を更新 「3.2.3 個人の認証」を更新 「3.2.5 権限の正当性確認」を更新 「3.2.6 相互運用の基準」を更新 「4.5.1 証明書利用者の私有鍵および証明書の用途」を更新 「4.9.8 証明書失効リストの発行最大遅延時間」を更新 「6.1.7 鍵の用途」を更新 「7.1 証明書のプロファイル」を更新 「7.1.3 アルゴリズムオブジェクト識別子」を更新 「7.2 CRL のプロファイル」を更新 「8. 準拠性監査と他の評価」を更新 「8.1 監査の頻度」を更新 「8.2 監査人の身元／資格」を更新 「8.3 監査人と被監査部門の関係」を更新 「8.4 監査で扱われる事項」を更新 「8.5 不備の結果としてとられる処置」を更新 「8.6 監査結果の開示」を更新

目次

1. はじめに

1.1 概要

企業認証 証明書ポリシー（以下「本 CP」という）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 SC Organization Validation CA（以下「本 CA」という）が発行する証明書の利用目的、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。

本 CA は、Security Communication RootCA2 または Security Communication ECC RootCA1 より、片方向相互認証証明書の発行を受けている。本 CA が発行する証明書は、サーバー認証や、通信経路で情報の暗号化を行うことに利用する。

本 CA 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） ● 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（以下「当約款」という）に定めるものとする。

なお、本 CP の内容が当約款、CPS の内容に抵触する場合は、当約款、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、当約款、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伴い、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 RFC3647「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 の正式名称は、「企業認証 証明書ポリシー」という。

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
SC Organization Validation CA1 （Security Communication RootCA2 より発行）	1.2.392.200091.110.214.1 2023/05/31 まで利用。
SC Organization Validation CA2 （Security Communication RootCA2 より発行）	1.2.392.200091.110.214.2
SC Organization Validation CA3 （Security Communication RootCA2 より発行）	1.2.392.200091.110.214.3
SC Organization Validation CA4 （Security Communication ECC RootCA1 より発行）	1.2.392.200091.110.214.4

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、証明書の発行、失効、CRL（Certificate Revocation List：証明書失効リスト）の開示、OCSP（Online Certificate Status Protocol）サーバーによる証明書ステータス情報の提供などを行う。電子認証基盤の上で運用される CA の運営主体は当社である。

1.3.2 RA

RA は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等を行う主体のこと

をいう。

証明書申請を受け、内容の審査、証明書の発行、失効を申請する証明書利用者の実在性確認および証明書発行、失効するための登録業務等を行い、また、証明書発行の承認または却下、証明書の失効要求を受けた場合は承認を行う。

外部委託先は本 CP の「3.2.2.4 ドメインの認証」を除く業務を行うことができる。

1.3.3 証明書利用者

証明書利用者とは、本 CA より証明書の発行を受け、発行された証明書を利用する個人、法人、その他の組織とする。

1.3.4 検証者

検証者とは、証明書利用者の身元と公開鍵の有効性を検証する個人、法人その他の組織をいう。また、かかる公開鍵を使って証明書利用者が所有する Web サーバーとの間で暗号化通信を行う目的で、CP、CPS を信頼し利用する個人、法人その他の組織をいう。

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、サーバー認証や通信経路でデータの暗号化を行うことに利用することができる。

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。

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 に関する連絡先は次のとおりである。

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

電子メールアドレス ： ca-support@secom.co.jp

ウェブサイト：https://www.secomtrust.net/

加入者、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、上記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。

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。「私有鍵」ともいう。

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・保護および証明書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。

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。

FIPS140-2

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。最低レベル 1 から最高レベル 4 まで定義されている。

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。

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。

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。

RFC3647（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 - 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

RFC3912 で定義されたプロトコル、RFC7482 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、証明書利用者および検証者が CRL 情報を 24 時間 365 日利用できるようリポジトリーを維持管理する。また、証明書利用者および検証者がオンラインでの証明書ステータス情報を 24 時間 365 日利用できるように OCSP レスポンダーを管理する。ただし、保守等により、一時的にリポジトリーおよび OCSP レスポンダーを利用できない場合もある。

2.2 証明情報の公開

本 CA は、次の内容をリポジトリーに格納し、証明書利用者および検証者がオンラインによって参照できるようにする。

- CRL
- 本 CA 証明書
- 最新の本 CP、CPS
- 本 CA が発行する証明書に関するその他関連情報

また、本 CA は、OCSP レスポンダーにより証明書利用者および検証者がオンラインによって証明書ステータス情報を参照できるようにする。その他公開情報として、ベンダーが検証を行うためにテストサイトを用意している。

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、RFC5280 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. 「国名」（C）は JP とする。
2. 「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の名称とする。
3. 「組織単位名」（OU）は、任意選択の記入欄とする。OU の欄は、組織内のさまざまな部門等（例えば、人事、マーケティング、開発の各部門）を区別するために使用する。ただし、2022 年 9 月 1 日以降に発行される証明書には使用禁止とする。
4. 「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。
5. 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。

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、証明書利用者が 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 証明書利用者の匿名性または仮名性

本 CA が発行する証明書の組織名およびコモンネームには、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。証明書利用者は、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証明書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、紛争を理由に証明書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

証明書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。

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、証明書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し、その生成より 30 日間のレスポンス確認の使用に有効なものとする。

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 RFC3912 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電子メール、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電子メールアドレス、ファックス番号、SMS 番号、または住所宛に送付する。また、電子メール、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。
（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電子メール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。電子メール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、電子メールで複数の FQDN を確認することもできる。
（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。
（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、電子メール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、電子メールで複数の 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。
（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、電子メール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、電子メールで複数の FQDN を確認することもできる。
（Baseline Requirements セクション 3.2.2.4.14 DNS TXT 連絡先への Email）

6. ドメイン連絡先の電話番号へ電話し、認証ドメイン名の使用許可のレスポンスを得ることで、FQDN に対する申請者の権限を立証する。また、複数の認証ドメイン名においてドメイン連絡先の電話番号が同じ場合、各認証ドメイン名を提示して使用許可のレスポンスを得ることで、複数の FQDN に対して権限を立証することもできる。
（Baseline Requirements セクション 3.2.2.4.15 ドメイン連絡先への電話連絡）

7. DNS TXT レコードの電話連絡先の電話番号へ電話し、認証ドメイン名の使用許可のレスポンスを得ることで、FQDN に対する申請者の権限を立証する。また、複数の認証ドメイン名において電話連絡先の電話番号が同じ場合、各認証ドメイン名を提示して使用許可のレスポンスを得ることで、複数の FQDN に対して権限を立証することもできる。
（Baseline Requirements セクション 3.2.2.4.16 DNS TXT 連絡先への電話連絡）

8. DNSCAA レコードの電話連絡先の電話番号へ電話し、認証ドメイン名の使用許可のレスポンスを得ることで、FQDN に対する申請者の権限を立証する。また、複数の認証ドメイン名において電話連絡先の電話番号が同じ場合、各 FQDN を提示して使用許可のレスポンスを得ることで、複数の FQDN に対して権限を立証することもできる。
（Baseline Requirements セクション 3.2.2.4.17 DNS CAA 連絡先への電話連絡）

9. 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。
2021 年 12 月 1 日以降に発行された証明書の場合、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 RFC7538、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。

（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）

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。

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。

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、発行することが出来る。

･失敗がCAのインフラストラクチャ外である場合

･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。

3.2.3 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 検証されない証明書利用者の情報

検証されていない証明書利用者の情報は、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

鍵更新時における証明書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、証明書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、証明書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、証明書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、および証明書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。

4.1.2 申請手続および責任

証明書利用者および申請者は、証明書の発行申請を行うにあたり、本 CP および CPS の内容を承諾した上で申請を行うものとする。また、本 CA に対する申請内容が正確な情報であることを保証しなければならない。

4.2 証明書申請手続

証明書利用者または申請者は、外部委託先が提供する証明書発行サービスをとおして証明書の申請をする。

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。

本 CP「6.3.2 私有鍵および公開鍵の有効期間」では、加入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。

2021 年 10 月 1 日以降は、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、再利用されたデータ、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。

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。

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、証明書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証明書利用者の証明書。

・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、申請者または証明書利用者に、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。

4.2.4 CAA レコードの確認

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証明書利用者は、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。

証明書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

4.3 証明書の発行

4.3.1 証明書発行時の処理手続

証明書申請の審査終了後に証明書発行を行い、証明書利用者だけがアクセス可能なホームページ、メール送付、または郵送にて証明書を証明書利用者に対して送付する。

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(つまり、CA システムオペレーター、システム責任者、または PKI 管理者)に対し、直接コマンドを実行し、慎重に発行する。

本 CA は発行する証明書の一部の項目に関して形式が Baseline Requirements に準拠しているかどうか証明書発行前リンティング機能により確認し、要件を満たしていない場合は発行拒否している。

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。

本 CA では、有効期限、禁止事項またはコードによる制限回避のため、証明書の notBefore の日付をさかのぼることはしない。

4.3.2 証明書利用者への証明書発行通知

証明書利用者に対し、証明書利用者だけがアクセス可能なホームページ、メール送付、または郵送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

証明書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証明書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、証明書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 証明書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。

加入者は、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 証明書利用者の表明保証」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、証明書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、証明書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 証明書利用者に対する新しい証明書発行通知

本 CP「4.3.2.証明書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 証明書利用者に対する新しい証明書の通知

本 CP「4.3.2.証明書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 証明書利用者に対する新しい証明書発行通知

本 CP「4.3.2.証明書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

次の 1 つ以上が発生した場合、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) を使用するものとする。

1. 加入者が、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. 加入者が本 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、加入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 が、証明書の公開鍵 (Debian の弱い鍵など。 https://wiki.debian.org/SSLkeys を参照) に基づいて加入者の私有鍵を簡単に計算できる、実証済みまたは証明された方法を認識した場合 (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、以下のいずれかが発生した場合、24 時間以内に加入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 を使用しなければならない。

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. 加入者が加入者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、証明書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、証明書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、加入者、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

証明書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

証明書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、加入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 は加入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（加入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加入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、証明書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

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、RFC6960 や RFC5019 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、RFC6960 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、証明書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。

加入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 [RFC6962]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[RFC6962]
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、RFC4366、RFC 5246、RFC 8446 に従い、ステープリングを利用して OCSP レスポンスを配布できる。この場合、本 CA は証明書利用者が TLS 処理に証明書の OCSP レスポンスを含めることを確実なものにする。本 CA は、証明書利用者に対してこの要件

を実施する場合、サービス利用規定または証明書利用者との契約書等、あるいは本 CA による技術確認およびサービス責任者の承認を経て対応するものとする。

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、証明書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、証明書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

証明書利用者は 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 加入（登録）の終了

証明書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、証明書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、原則として証明書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証明書利用者、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

認証基盤システムでは、FIPS140-2 レベル 3 準拠の暗号装置で CA の鍵ペアを生成する。鍵ペアの生成作業は、複数名の権限者による操作によって行う。

証明書利用者の鍵ペアは、証明書利用者自身が生成する。

6.1.2 証明書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 に対する証明書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 SSL/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、FIPS140-2 レベル 3 準拠の暗号装置を用いて行う。証明書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。証明書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、証明書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、証明書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。

証明書利用者の私有鍵のバックアップは、証明書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。

証明書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。証明書利用者の私有鍵については規定しない。

6.2.7 暗号装置への私有鍵の格納

本電子認証基盤の上で運用される CA の私有鍵は、暗号化された状態で暗号装置内に格納する。証明書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。
証明書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。
証明書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。
証明書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。証明書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。
証明書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が加入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RFC5280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　サーバー証明書プロファイル
（Security Communication RootCA2より発行されたCA）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		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	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD	-
	Common Name	CN=各認証局のコモンネームを設定	-
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	Country	C=JP（固定値）	-
	State Or Province	必須	-

	Locality	必須	-
	Organization	必須	-
	Organizational Unit	禁止	-
	Common Name	必須 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。	-
Subject Public Key Info		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 は禁止。	y
ExtendedKeyUsage		serverAuth, clientAuth * clientAuth は任意とする	n
Subject Alternative Name		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	n

	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。 2021 年 10 月 1 日より、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。	
CertificatePolicies	[1]policyIdentifier OID=本 CP の[1.2-1 OID]を設定 policyQualifiers policyQualifierId=CPS qualifiier=本 CA のリポジトリー HTTP(S) URL [2]policyIdentifier=2.23.140.1.2.2 * policyQualifier は非推奨	n
CRL Distribution Points	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
Authority Information Access	accessMethod ocsp（1.3.6.1.5.5.7.48.1） accessLocation OCSP レスポンダーの HTTP URL CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation 本 CA 証明書の HTTP URL	n
Authority Key Identifier	発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

Subject Key Identifier	任意 主体者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Certificate Transparency 用拡張 （1.3.6.1.4.1.11129.2.4.2）	任意 SignedCertificateTimestampList の値	n

表 7.1-2　サーバー証明書プロファイル
（Security Communication ECC RootCA1 より発行された CA）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		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	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD	-
	Common Name	CN=各認証局のコモンネームを設定	-
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	Country	C=JP（固定値）	-
	State Or Province	必須	-
	Locality	必須	-
	Organization	必須	-
	Organizational Unit	禁止	-
	Common Name	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。	
Subject Public Key Info		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 は禁止。	y
ExtendedKeyUsage		serverAuth, clientAuth * clientAuth は任意とする	n
Subject Alt Name		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、	n

	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。	
CertificatePolicies	[1]policyIdentifier OID=本 CP の[1.2-1 OID]を設定 policyQualifiers policyQualifierId=CPS qualifiier=本 CA のリポジトリー HTTP(S) URL [2]policyIdentifier=2.23.140.1.2.2 * policyQualifier は非推奨	n
CRL Distribution Points	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
Authority Information Access	accessMethod ocsp（1.3.6.1.5.5.7.48.1） accessLocation OCSP レスポンダーの HTTP URL CA Issuers (1.3.6.1.5.5.7.48.2) accessLocation 本 CA 証明書の HTTP URL	n
Authority Key Identifier	発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier	任意 主体者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Certificate Transparency 用拡張（1.3.6.1.4.1.11129.2.4.2）	任意 SignedCertificateTimestampList の値	n

表 7.1-3　OCSP レスポンダー証明書プロファイル
（Security Communication RootCA2 より発行された CA）

基本領域	設定内容	critical
Version	Version 3	-
Serial Number	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	
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD	-
	Common Name	各認証局のコモンネームを設定	-
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	Country	C=JP（固定値）	-
	Organization	SECOM Trust Systems CO.,LTD.（固定値）	-
	Common Name	OCSP レスポンダー名	-
Subject Public Key Info		以下のいずれか。 RSA2048 ビット、3072 ビット、4096 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		null	n
CertificatePolicies		禁止	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		主体者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

表 7.1-4　OCSP サーバー証明書プロファイル
（Security Communication ECC RootCA1 より発行された CA）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		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	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-

	Organization	O=SECOM Trust Systems CO.,LTD	-
	Common Name	各認証局のコモンネームを設定	-
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	Country	C=JP（固定値）	-
	Organization	SECOM Trust Systems CO.,LTD.（固定値）	-
	Common Name	OCSP レスポンダー名	-
Subject Public Key Info		以下のいずれか。 ECDSA384 ビット（secp384r1）、256 ビット（secp256r1）	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		null	n
CertificatePolicies		禁止	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		主体者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

7.1.1 バージョン番号

本 CA は、バージョン 3 を適用する。

7.1.2 証明書拡張

本 CA が発行する証明書は、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、RFC5280 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加入者証明書ごとに、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、証明書または加入者証明書が 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。
{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)

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 を格納している。

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 RFC5280 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（Security Communication RootCA2 より発行された CA）

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=各認証局のコモンネームを設定	-
This Update		CRL の発行日時	-
Next Update		次の CRL が発行される日時。 thisUpdate から最大 10 日後。	-
Revoked Certificates	Serial Number	失効した証明書に含まれる serialNumber とバイト単位で同一の値	-
	Revocation Date	通常、失効が発生した日時	-
	Reason Code	「7.2.2 CRL 拡張」に規定した値	-
拡張領域		設定内容	critical
CRL Number		CRL 番号	n

Authority Key Identifier	発行者公開鍵の 160 ビット SHA-1 ハッシュ値	n

表 7.2-2　CRL プロファイル
（Security Communication ECC RootCA1 より発行された CA）

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=各認証局のコモンネームを設定	-
This Update		CRL の発行日時	-
Next Update		次の CRL が発行される日時。 thisUpdate から最大 10 日後。	-
Revoked Certificates	Serial Number	失効した証明書に含まれる serialNumber とバイト単位で同一の値	-
	Revocation Date	通常、失効が発生した日時	-
	Reason Code	「7.2.2 CRL 拡張」に規定した値	-
拡張領域		設定内容	critical
CRL Number		CRL 番号	n
Authority Key Identifier		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、CRL バージョ 2 を適用する。

7.2.2 CRL 拡張

本 CA が発行する CRL 拡張フィールドを使用する。

reasonCode (OID 2.5.29.21)

2020 年 9 月 30 日より、次の要件をすべて満たす必要がある。

reasonCode が存在する場合、この拡張を critical としてマークしてはならない。

CRL エントリーがルート CA または下位 CA 証明書（クロス証明書を含む）のためのものである場合、この CRL エントリー拡張が存在しなければならない。

CRL エントリーが CA ではなく、加入者証明書用である場合、この CRL エントリー拡張は存在すべきであるが、以下の要件を満たすことを条件に省略してもよい。

CRLReason は、unspecified (0)であってはならない。失効の理由が特定されていない場合、以前の要件で許可されていれば、CA は reasonCode エントリー拡張を省略しなければならない。CRL エントリーが Baseline Requirements の対象とならない証明書用であり、2020 年 9 月 30 日以降に発行されたか、2020 年 9 月 30 日以降に notBefore（発行日）である場合、CRLReason は certificateHold (6)を使用してはいけない。CRL エントリーが Baseline Requirements の対象となる証明書用である場合、CRLReason は certificateHold (6)を使用してはいけない。

reasonCode CRL エントリー拡張が存在する場合、CRLReason は、その CP/CPS 内の CA によって定義されているように、証明書の失効の最も適切な理由を示さなければならない。

CRLReason が "unspecified (0)"[未定義]ではない限り、2023 年 7 月 15 日以降に失効された加入者証明書に対応する CRL エントリーの reasonCode 拡張に CRLReason を含めなければならない。2023 年 7 月 15 日より前に失効された加入者証明書の失効理由コードエントリーは、追加または変更の必要はない。

次の CRLReasons のいずれかが、加入者証明書の CRL reasonCode 拡張に存在してもよい。

1. keyCompromise (RFC 5280 CRLReason #1) [私有鍵の危殆化]: 加入者の私有鍵が危殆化されている事実がある、またはその疑いがあることを示す。
2. affiliationChanged (RFC 5280 CRLReason #3) [証明書情報の変更]: 証明書内のサブジェクトの名前またはその他のサブジェクト識別情報が変更され、証明書の私有鍵が危殆化されたと疑う理由がないことを示す。
3. superseded (RFC 5280 CRLReason #4) [証明書の破棄]: 次の理由により、証明書が置き換えられることを示す。加入者が新しい証明書を要求した場合、証明書内の FQDN また IP アドレスのドメイン認可または制御の検証が信頼されるべきではないという合理的な証拠が本 CA にある場合、または、証明書が Baseline Requirements または本 CA の CP または CPS に準拠していないなどの準拠上の理由により、本 CA が証明書を失効した場合。
4. cessationOfOperation (RFC 5280 CRLReason #5) [証明書の運用停止]: 証明書の有効期限が切れる前に、証明書を含む Web サイトが閉鎖されたこと、または証明書の有効期限が切れる前に、加入者が証明書のドメイン名を所有または管理していないことを示す。
5. privilegeWithdrawn (RFC 5280 CRLReason #9) [証明書を利用する権利の撤回]: 証明書加入者が証明書要求で誤解を招く情報を提供、加入者契約または利用規約に基づく重大な義務を守らなかったなど、私有鍵危殆化に至らなかった加入者側の違反があったことを示す。

加入者契約、またはそこで参照されているオンラインリソースは、上記の失効理由のオプションについて加入者に通知し、各オプションをいつ選択するかについて説明しなければならない。本 CA が加入者に提供するツールは、加入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しなければならず、デフォルト値は、失効理由が提供されていない状態とする（デフォルトは CRLReason "unspecified (0)"[未定義] に対応し、その結果、CRL で reasonCode 拡張が提供されない)。

privilegeWithdrawn reasonCode [証明書を利用する権利の撤回]の使用は、加入者ではなく本 CA によって決定されるため、この reasonCode の使用は加入者が失効理由オプションとして選択できるようにすべきではない。

本 CA が、CRL エントリーに reasonCode 拡張が含まれていない場合、または keyCompromise 以外の理由を持つ reasonCode 拡張を持つ証明書の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 を入力する必要がある。さらに、証明書の私有鍵が、その証明書の CRL エントリーに示されている失効日の前に危殆化され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必要がある。

備考： revocationDate フィールドのバックデートは、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。ただし、これらの要件では、証明書が最初に危殆化されたと見なされた日付として 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指定している。

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、RFC5019 および 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 - 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

セコムトラストシステムズは、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。

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. 証明書の加入者契約または利用規約の当事者である加入者。
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(主体者識別名の organizationalUnitName 属性を除く)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. 誤解を招く情報の排除

   発行の時点で、本 CA が、以下を満たすこと。

   i. 証明書の主体者識別名の organizationalUnitName に含まれる情報が誤解を与えるものである可能性を減らす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。

5. 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 7.1.4.2.2 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。

6. 加入者契約

   本 CA および加入者が関連会社でない場合、加入者および本 CA は、Baseline Requirements を満たす法的に有効で実施可能な加入者契約の当事者であること。あるいは、本 CA および加入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。

7. 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。

8. 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 証明書利用者の表明保証

本 CA は、加入者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 との加入者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、各加入者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、明確にその加入者契約書または利用規約の対象となっていることを条件とする。

加入者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、加入者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加入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

申請者が加入者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
- 証明書利用者が自己の義務の履行を怠ったために生じた損害
- 外部委託先および証明書利用者のシステムに起因して発生した一切の損害
- 外部委託先および証明書利用者の環境（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

証明書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証明書利用者、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、証明書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、電子メール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、証明書利用者または検証者の義務等を本 CP および当約款、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 および当約款、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 および当約款、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 宛にメール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メールアドレスやリンク)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。