CA/ブラウザフォーラム

パブリック証明書
発行及びマネジメントの基本要件 ver1.0

発行日：2011 年 11 月 22 日　有効日：2012 年 7 月 1 日

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

パブリック証明書の発行及びマネジメントの基本要件

Version 1.0, as adopted by the CA/Browser Forum on 22 Nov. 2011 with an Effective Date of 1 July 2012.

バージョン 1.0, CA/ブラウザフォーラムは 2011 年 11 月 22 日に採択され、2012 年 7 月 1 日に有効となります。

These Baseline Requirements describe an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are necessary (but not sufficient) for the issuance and management of Publicly-Trusted Certificates; Certificates that are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software. The Requirements are not mandatory for Certification Authorities unless and until they become adopted and enforced by relying–party Application Software Suppliers.

本書では、 公的に信頼された証明書（パブリック証明書）の発行及びマネジメントに必要な(しかし必ずしも完全ではない)技術、プロトコル、身元確認、ライフサイクルマネジメント、監査要件を記載しています；（証明書が公的に信頼されているという事実に則り、対応ルート証明書がアプリケーションソフトウェアに配布されています。）依拠当事アプリケーションソフトウェアベンダにより選定または要請を受けない認証局に本要件は適用されません。

Notice to Readers

読者の方へ

This version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates present criteria established by the CA/Browser Forum for use by Certification Authorities when issuing, maintaining, and revoking publicly-trusted Certificates. The Requirements may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Because one of the primary beneficiaries of these Requirements is the end user, the Forum openly invites anyone to make recommendations and suggestions by email to the CA/Browser Forum at questions@cabforum.org. The Forum members value all input, regardless of source, and will seriously consider all such input.

本書では、CA/ブラウザフォーラムにより制定され、認証局によりパブリック証明書を発行、維持、失効する際に使用される基準を提示しています。本書は、CA/ブラウザフォーラムが承認する手続きに即し、適宜改訂されることがあります。本書の第一の受益者はエンドユーザであるため、ご質問及びご提案については、CA/ブラウザフォーラム (questions@cabforum.org)宛にご連絡ください。お寄せいただいたご提案は、フォーラムメンバーにより検討いたします。

The CA/Browser Forum

CA/ブラウザフォーラム

The CA/Browser Forum is a voluntary organization of Certification Authorities and suppliers of Internet browser and other relying-party software applications. Membership as of September 2011 is as follows:

CA/ブラウザフォーラムは、CA、インターネットブラウザベンダ、及びその他の依拠当事アプリケーションソフトウェアベンダによる、非営利団体です。2011 年 9 月現在の会員は以下の通りです：

Certification Authorities　CA

- A-Trust GmbH
- AC Camerfirma SA
- Buypass AS
- Certum
- Comodo CA Ltd
- Cybertrust
- D-TRUST GmbH
- DanID A/S
- DigiCert, Inc.
- Digidentity BV

- Echoworx Corporation
- Entrust, Inc.
- GeoTrust, Inc.
- Getronics PinkRoccade
- GlobalSign
- GoDaddy.com, Inc.
- IdenTrust, Inc.
- ipsCA, IPS Certification Authority s.l.
- Izenpe S.A.
- Japan Certification Services, Inc.
- Kamu Sertifikasyon Merkezi
- Keynectis
- Logius PKIoverheid
- Network Solutions, LLC
- QuoVadis Ltd.
- RSA Security, Inc.
- SECOM Trust Systems CO., Ltd.
- Skaitmeninio sertifikavimo centras (SSC)
- StartCom Certification Authority
- SwissSign AG
- Symantec Corporation
- T-Systems Enterprise Services GmbH.
- TC TrustCenter GmbH
- Thawte, Inc.
- TÜRKTRUST
- Trustis Limited
- Trustwave
- TWCA
- Verizon
- Wells Fargo Bank, N.A.

Relying-Party Application Software Suppliers　依拠当事アプリケーションベンダ

- Apple
- Google Inc.
- KDE
- Microsoft Corporation
- Opera Software ASA
- Research in Motion Limited
- The Mozilla Foundation

Other groups that have participated in the development of these Requirements include the AICPA/CICA WebTrust for Certification Authorities task force and ETSI ESI. Participation by such groups does not imply their endorsement, recommendation, or approval of the final product.
AICPA/CICA WebTrust for CA 及び ETSI ESI のメンバーも本書の作成プロセスに参加しています。ただし、これらの組織の参加が、当該組織のサービスへの支持、推奨、承認を意味するものではありません。

TABLE OF CONTENTS 目次

1. 範囲

本書では、パブリック証明書の発行のために認証局が満たさなくてはならない要件について記載されています。特に明記がない限り、これらの要件は本書の有効日より後に行われる事象に適用されます。

本書では、パブリック証明書の発行と管理に関連するすべての事項が記述されているわけではありません。CA/ブラウザフォーラムは、オンラインセキュリティに対する既存及び新規の脅威に対応するため本書を適宜更新します。特に、今後の改訂版には、証明書発行に関わる委託機能についての整理を進めた包括的な監査要件が含まれる予定です。

本バージョンでは、インターネットを通じてアクセス可能なサーバの認証を目的とした証明書についての要件を記述しています。コードサイニング、S/MIME、タイムスタンプ、VoIP、IM、ウェブサービス等についての要件は、今後の改訂版にて記述されます。

本書は、社内利用の自社の公開鍵基盤を持ち、ルート証明書がどのアプリケーションソフトウェアベンダからも配布されていないプライベート認証局による証明書の発行及びマネジメントには言及していません。

2. 目的

本書の主目的は、ユーザが証明書の信頼性について不安を抱く事無く、効率的で安全な電子コミュニケーションを可能にすることです。また、本書は、ユーザが証明書に依拠する際に十分な情報を得たうえで判断を下すためのものです。

3. 参照文献

ETSI TS 102 042 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

ISO 21188:2006, Public key infrastructure for financial services -- Practices and policy framework.

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.

RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.

WebTrust, WebTrust Program for Certification Authorities Version 2.0, AICPA/CICA, available at http://www.webtrust.org/homepage-documents/item49945.aspx

X.509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

4. 定義語

関連会社(Affiliate): パートナー、合弁、他の法的組織体の管理上・管理下・これらと同一の管理下にある組織体、または行政機関の直接的管理下で運営しているエージェンシー・部署・下位行政機関・法的組織体。

申請者(Applicant): 証明書の申請（もしくは更新要求）をする個人もしくは法的組織体。証明書が発行された時点で、申請者は加入者と呼ばれる。デバイスに発行された証明書については、デバイスが実際の証明書要求をした場合においても、申請者は証明書に指定されるデバイスを管理又は運用する個人又は法的組織体となります。

申請権限者 (Applicant Representative): 申請者の代理となる権利を有すると表明する者もしくは申請者が雇った個人または申請者に承認されている代行者であり、(i)申請者の代理で申請書要求の署名、提出、又は承認を行う、及び/又は(ii)加入契約書の署名、提出、又は承認を行う、及び/又は、(iii)証明書要求者が認証局の関連会社であった場合に、申請者の代理として、利用契約書を理解し同意する者。

アプリケーションソフトウェアベンダ(Application Software Supplier): インターネットブラウザソフトウェア、もしくは証明書を表示又は利用し、ルート証明書を実装するその他の依拠当事アプリケーションソフトウェアのベンダ。

意見書(Attestation Letter): 会計士、弁護士、政府職員、もしくは委託可能な信頼のおける第三者機関により文書化された、サブジェクト情報が正確であることを保証する文書。

監査報告書(Audit Report): 当該事業のプロセスと統制が、本書に準拠しているかどうかを記述してある、公認監査人からのレポート。

証明書(Certificate): 公開鍵とアイデンティティを結びつけるために電子署名を使う電子文書。

証明書データ(Certificate Data): 申請者やそれ以外のソースから入手した、認証局が保持、管理、もしくはアクセス可能な証明書要求及び関連データ。

証明書管理プロセス(Certificate Management Process): 認証局が証明書データの認証、証明書発行、レポジトリ管理、証明書失効の際に用いる鍵、ソフトウェア、及びハードウェアの使用に関するプロセス、業務、及び手続き。

証明書ポリシー(Certificate Policy): 特定のコミュニティー及び/又は共通したセキュリティ要件による PKI 実装に対する該当証明書の適用性を示す規定集。以下 CP。

証明書に関する問題の報告(Certificate Problem Report): 鍵の危殆化の疑惑、証明書の誤用、もしくは証明書に関するその他の不正、危殆化、誤用、不適切な行為の報告。

証明書失効リスト(Certificate Revocation List): 証明書を発行した認証局が作成している失効された証明書のリスト。証明書失効リストは発行元認証局による電子署名、発行時間及び有効期間が記載されており、定期的に更新される。

認証局(Certification Authority): 証明書の生成、発行、失効、管理の責任を負う組織。ルート認証局と下位認証局の両方に同意で使われる。以下 CA。

認証業務運用規程(Certification Practice Statement): 証明書の生成、発行、管理及び使用の枠組みを規定する文書の一つ。以下 CPS。

クロス証明書(Cross Certificate): 二つのルート CA 間の信頼関係を構築するために使われる証明書。

外部委託先 (Delegated Third Party): 本書に定められた要件を満たす証明書管理プロセスを行うことを CA から承認されている、CA 以外の個人又は法的組織体。

ドメイン利用権限(Domain Authorization): 申請者が特定ドメインネームスペースへの証明書の申請を行うことの正当性を証明するためにドメイン名登録機関が提供された書状やその他の文書。

ドメイン名 (Domain Name): DNS(Domain Name System)内のノードに割り当てられている名称。

ドメインネームスペース(Domain Namespace): DNS の一つのノード内に入りうる全てのドメイン名の総称。

ドメイン名登録者(Domain Name Registrant): ドメイン名の「所有者」とも呼ばれているが、正確には WHOIS やドメイン登録機関により「登録者」として登録されている個人や法的組織体のように、ドメイン名登録機関によりドメイン名をコントロールする権利を持つものとして登録されている個人や法的組織体。

ドメイン名登録機関(Domain Name Registrar): (i) Internet Corporation for Assigned Names and Numbers(ICANN)、(ii)国営ドメイン名維持管理機関、(iii)ネットワークインフォメーションセンター(関連会社、契約者、代理人、法的相続人、権利継承者を含む)との契約のもとにドメイン名を登録する個人や法的組織体。

有効日(Effective Date): 本書は 2012 年 7 月 1 日に有効となる。

エンタープライズ RA (Enterprise RA): 当該組織に証明書発行を承認する CA と関連企業でない組織の従業員もしくは代理人。

有効期限(Expiry Date): 証明書に指定される証明書有効期間の最終日。

FQDN(Fully-Qualified Domain Name): DNS に設定されたすべての上位ノードの名称を含むドメイン名。

行政機関(Government Entity): 政府が運営する法的組織体、政府機関、部署、省庁、支部、政府と同類の役割、もしくは国内の政治的な下位区分(州、都市、郡など)。

内部サーバ名(Internal Server Name): 公開されている DNS では解決ができないサーバ名(未登録のドメイン名を含むこともあれば、含まないこともある)。

発行元 CA(Issuing CA): 特定の証明書に関して証明書を発行した CA。ルート CA 又は下位 CA のいずれかの場合がある。

鍵の危殆化(Key Compromise): 秘密鍵は、情報が権限のない人物に公開されてしまった場合、権限のない人物がアクセスしたと考えられる場合、又は権限のない人物が情報を入手する方法・実用可能な技術が存在する場合に、危殆したと言われる。

鍵の生成スクリプト(Key Generation Script): CA 鍵ペアの生成手続きが収められた計画文書。

鍵ペア(キーペア)(Key Pair): 秘密鍵とそれに対応する公開鍵。

法的組織体(Legal Entity): 該当国の法律制度に則った組織、企業、パートナーシップ、事業体、トラスト、行政機関、及びその他組織体。

オブジェクト ID(OID:Object Identifier): 国際標準化機構の適用規格に従って登録された、オブジェクト又はオブジェクトクラスをユニークに識別するための英数字又は数字の識別子。

OCSP レスポンダ(OCSP Responder): CA の権限で運用される、リポジトリに接続され、証明書のステータス要求を処理するオンラインサーバー。オンライン証明書ステータスプロトコルを参照。

オンライン証明書ステータスプロトコル(Online Certificate Status Protocol): 証明書依拠者のアプリケーションソフトウェアによる特定証明書の有効性確認に用いられるオンライン証明書確認プロトコル。

秘密鍵(Private Key): 鍵ペアの一方の鍵であり、所有者によって秘匿性が保たれ、デジタル署名の作成及び対になる公開鍵で暗号化された電子的な記録及び/又はファイルの復号に使用される。

公開鍵(Public Key): 鍵ペアの一方の鍵であり、対となる秘密鍵の所有者によって広く公開され、依拠当事者によって、対になる秘密鍵で生成したデジタル署名の検証及び/又は対応する秘密鍵でのみ復号できるメッセージの暗号化に使用される。

公開鍵基盤(Public Key Infrastructure): 公開鍵暗号化技術に基づいた、信頼できる証明書及び鍵の生成、発行、管理及び使用を実現するための、ハードウェア、ソフトウェア、人、手順、規則、ポリシー、及び義務により構成される仕組み。

パブリック証明書(Publicly-Trusted Certificate): 対応するルート証明書がトラストアンカーとして広く用いられているアプリケーションソフトウェアで配布されていることから、信頼できると判断することができる証明書。

公認監査人(Qualified Auditor): セクション 17.6(監査資格)の要件を満たす個人又は法的組織体。

登録済みドメイン名(Registered Domain Name): ドメイン名登録機関に登録されているドメイン名。

登録局(RA: Registration Authority): 登録局は証明書のサブジェクトの識別と認証の責任を負う法的組織体だが、CA ではない。従って、証明書への署名又は発行は行わない。登録局は、証明書申請プロセス又は失効プロセス又はその両方を援助することができる。機能や役割を指すために用いられる際の RA は、必ずしも別組織体を意味するものではなく、RA が CA の一部であることも可能。

信頼できる連絡手段(Reliable Method of Communication): 申請者当人以外の情報源により確認された、住所、電話番号、メールアドレスなどの連絡方法。

依拠当事者(Relying Party): 有効な証明書に依拠する任意の個人又は法的組織体。単にアプリケーションソフトウェアベンダが配布するソフトウェアが証明書に関する情報を表示するだけという場合は、アプリケーションソフトウェアベンダは依拠当事者とはみなされません。

リポジトリ(Repository): CP や CPS 等の PKI ガバナンス文書及び CRL や OCSP による証明書ステータス情報を公開するオンラインデータベース。

要件(Requirements): 本書に記載されている要件。

予約 IP アドレス(Reserved IP Address): IANA により既に予約されている IPv4 アドレス又は IPv6 アドレス。
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

ルート CA(Root CA): アプリケーションソフトウェアベンダからルート証明書が配布される最高位の CA。下位 CA 証明書を発行する。

ルート証明書(Root Certificate): 自身を識別するため、及び、下位 CA に発行した証明書の検証のためにルート CA が発行する自己署名証明書。

サブジェクト(Subject): 証明書のサブジェクト(Subject)として特定される、個人、デバイス、システム、設備、又は法的組織体。サブジェクトは、加入者もしくは、加入者の管理・運用のもとにあるデバイスのいずれかとなる。

サブジェクトアイデンティティ情報(Subject Identity Information): 証明書のサブジェクトを識別する情報。サブジェクトアイデンティティ情報は SubjectAlternativeName 拡張領域や Subject common name フィールドに記載されるドメイン名を含まない。

下位 CA(Subordinate CA): 証明書がルート CA 又はその下位 CA によって署名されている CA。

加入者(Subscriber): 証明書が発行され、利用契約書又は利用約款により法的に拘束される個人もしくは法的組織体。

利用契約書(Subscriber Agreement): CA と申請者/加入者の間での契約で、両当事者の権利と義務を規定する契約。

利用約款(Terms of Use): 申請者/加入者が CA の関連会社であった場合に、本書に従って発行された証明書の保管と許可された利用方法に関する条項。

信頼できるシステム(Trustworthy System): 侵入及び誤用の恐れがないと合理的に考えられ、合理的レベルの可用性、信頼性、正確な運用を備え、意図した機能の実行に適していると合理的に考えられ、適用しうるセキュリティポリシーを実装しているコンピュータハードウェア、ソフトウェア及び手順。

未登録ドメイン名(Unregistered Domain Name):登録済みでないドメイン名。

有効証明書(Valid Certificate): RFC 5280 に規定されている検証手続きにパスした証明書。

審査担当者(Validation Specialists): 本書で指定される認証業務を行う人員。

有効期間(Validity Period)： 証明書が発行された日から有効期限日までの期間。

ワイルドカード証明書(Wildcard Certificate): 証明書上サブジェクトの FQDN の左端にアスタリスク(*)がついている証明書。

5. 略語と頭文字

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol

6. 慣例

本書に定義されていない用語は、各 CA の該当契約、ユーザマニュアル、CP 及び CPS において定義されます(SHALL)。

本書で使用する「MUST」、「MUST NOT」、「REQUIRED」、「SHALL」、「SHALL NOT」、「SHOULD」、「SHOULD NOT」、「RECOMMENDED」、「MAY」、「OPTIONAL」は、RFC 2119 の記載に従って解釈するものとします。

7. 証明書の保証と表明

7.1 CA による保証と表明

証明書を発行することにより、CA は、セクション 7.1.1.の証明書受益者に対し、セクション 7.1.2 に記された事項を保証します。

7.1.1 証明書受益者

証明書受益者には以下が含まれますが、これに限定されません。

1. 証明書の利用契約書や利用約款の当事者である加入者
2. 提供するソフトウェアにルート証明書を実装する契約を締結しているアプリケーションソフトウェアベンダ
3. 有効証明書に合理的に依拠している全依拠者

7.1.2 証明書保証

CA は証明書受益者に対し、証明書が有効な間、本書、CP(証明書ポリシー)や CPS (認証業務運用規程)(以下「CP/CPS」という)を遵守することを表明し保証します。

1. 証明書保証には特に以下が含まれますが、これに限定されません。**ドメイン名もしくは IP アドレス使用の権利：**発行時に CA が、(i)証明書のサブジェクトフィールドと SubjectAltName 拡張領域に指定されているドメイン名及び、IP アドレスの使用権もしくは管理権限を申請者が持っていると証明する手続きを実施していること(もしくは、ドメイン名の場合に限り、申請者が当該権利及び管理の所有者からそれらの権利及び管理が委託されていること) (ii) 定められた手続きに従って証明書が発行されていること、そして(iii)CA の CP/CPS にその手続きを正確に記述していること
2. **証明書の承認：**発行時に CA が、(i)証明書発行を承認したサブジェクトを審査し、申請者の代理人がサブジェクトの代理で証明書要求をする権利を有することを証明するための手続きを実施していること (ii)定められた手続きに従って証明書が発行されていること、そして、(iii)CA の CP/CPS にその手続きを正確に記述していること
3. **情報の正確性：** 発行時に CA が、(i)証明書に含まれる全ての情報が正確であることを審査する手続きを実施していること(subject:organizationalUnit Name 属性は除く) (ii) 定められた手続きに従って証明書が発行されていること、そして (iii) CA の CP/CPS にその手続きを正確に記述していること
4. **誤解を招く情報がないこと：**発行時に CA が、(i)証明書の subject:organizationalUnitName 属性に含まれている情報が誤解を招く可能性を低くする手続きを実施していること、(ii) 定められた手続きに従って証明書が発行されていること、そして (iii) CA の CP/CPS にその手続き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：**証明書にサブジェクトアイデンティティ情報が含まれている場合、CA は、(i)セクション 9.2.4 とセクション 11.2 に従い申請者のアイデンティティを審査する手続きを実施していること (ii) 定められた手続きに従って証明書が発行されていること、そして (iii) CA の CP/CPS にその手続きを正確に記述していること
6. **利用契約書：**CA と加入者が関連会社でない場合、加入者と CA は、当該要件を満たす法的効力があり行使可能な利用契約書の当事者となること。もしくは、CA と加入者が関連会社の場合、申請者が利用約款を理解し受け入れていること。
7. **ステータス：**CA は 24 時間 365 日アクセス可能な公開レポジトリを、有効期限内の全証明書のステータス(有効か失効済みか)についての最新の情報とともに管理していること
8. **失効：**本書の要件に定める事由により、CA が証明書を失効すること

7.2 申請者による保証と表明

CA は、利用契約書と利用約款の一部として、CA と証明書受益者のため申請者に対しセクション 10.3.2 に定められたコミットメントと保証を義務付けることとします(SHALL)。

8. コミュニティーと適用性

8.1 コンプライアンス

CA はいかなるときも、(SHALL)

1. 運用している事業と発行する証明書に適用される法律に従い、証明書を発行し PKI を運用するものとします
2. 本書の要件を遵守するものとします
3. セクション 17 に定められる監査要件を遵守するものとします
4. 証明書発行業務を行うために法的な許可が必要な場合は、地域の法律に従って CA として認可を受けるものとします

裁判所もしくは本書に関する裁判権を持つ政府機関が本書の必須要件を違法と判決した場合、本書に必要最低限の変更を加えることを検討し、要件の有効性及び合法性を保ちます。ただし、当該変更点は現地の法律で問題となる運用もしくは証明書の発行業務のみに適用されます。当事者は CA/ブラウザフォーラムに事実、状況、関連する法律を通知するものとします(SHALL)。それにより、CA/ブラウザフォーラムは当該要件の変更を検討します。

8.2 証明書ポリシー

8.2.1 導入

CA は、当該 CA がどのように最新の本書要件を導入しているかを記述した、CP/CPS を策定、導入、施行し、年次で更新するものとします(SHALL)。

8.2.2 公開

CA は、適切かつアクセスが容易で 24 時間 365 日アクセス可能なオンライン手段を通じて、CP/CPS を公開するものとします(SHALL)。CA は選択した監査基準(セクション 17.1 を参照)により要求される範囲で、CA 事業運営方法を公開するものとします(SHALL)。開示資料は RFC 2527 もしくは RFC 3647 で求められる全資料を含み、RFC 2527 もしくは RFC 3647 のいずれかの通りに構成される必要があります(MUST)。

8.3 準拠のコミットメント

CA は、本書の要件を実施し、最新版に遵守することとします(SHALL)。CA は、自社の CP/CPS に直接本書の要件を加えることにより、又は以下のような条項を使用して本書に言及することにより、本書の要件を満たすことが可能です (MAY) 。ただし、その場合は本書の正式なバージョンへのリンクを張らなければなりません(MUST)。

> [CA 名]は、同ウェブサイト(http://www.cabforum.org)に掲載されているパブリック証明書発行と管理に関する基本要件書に遵守しています。本書と当該要件書に不一致が生じた場合には、当該要件書が優先されます。

8.4 信頼モデル

CA が信頼関係を構築、もしくは受諾した場合、CA がサブジェクトとして識別しているクロス証明書を全て公開するものとします(SHALL)。

9. 証明書のコンテンツとプロファイル

9.1 発行者情報

発行元 CA は、本書が採択された後に発行される証明書の issuer フィールドについて、以下のサブセクションに従う形で実装することとします(SHALL)。

9.1.1 発行者コモンネーム・フィールド

証明書フィールド名: issuer:commonName (OID 2.5.4.3)

必須/任意: 任意

コンテンツ: 証明書に記載される場合には、Common Name フィールドには発行元 CA の正確な識別名が入らなければなりません(MUST)。

9.1.2 発行者ドメインコンポーネントフィールド

証明書フィールド名：issuer:domainComponent (OID 0.9.2342.19200300.100.1.25)

必須/任意: 任意

コンテンツ: 証明書に設定される場合には、Domain Component フィールドには発行元 CA の全ての登録ドメイン名について、最も上位の、最もルートに近い、最後に書かれているコンポーネントから順に、全てのコンポーネントが記述されなければなりません。 (MUST)

9.1.3 発行者組織名フィールド

証明書フィールド名: issuer:organizationName (OID 2.5.4.10)

必須/任意: 必須

コンテンツ: このフィールドには、CA を正確に識別するための、当該 CA の名前(あるいは略称)、商標名、あるいはその他の意味のある識別名が設定されなくてはなりません(MUST)。このフィールドには、“Root” や “CA1” のような一般的な称号を含んではなりません(MUST NOT)。

9.1.4 発行者国名フィールド

証明書フィールド名: issuer:countryName (OID 2.5.4.6)

必須/任意: 必須

コンテンツ: このフィールドには発行者の事業所が位置している国を表す、ISO 3166-1 で規定された 2 ケタの国コードが設定されなくてはなりません。 (MUST)

9.2 サブジェクト情報

証明書の発行にあたり、CA は、証明書発行時点においてサブジェクト情報が正確であったことの検証を、CP/CPS に定められた手続きに則って行われたことを表明することとします。

9.2.1 Subject Alternative Name 拡張領域

証明書フィールド名: extensions:subjectAltName

必須/任意: 必須

コンテンツ: この拡張領域には少なくとも 1 つのエントリーが設定されなければなりません(MUST)。それぞれのエントリーは、FQDN(Fully-Qualified Domain Name)が設定された dNSName か、サーバの IP アドレスが設定された iPAddress でなければなりません(MUST)。CA は、申請者がこの FQDN あるいは IP アドレスをコントロールしているか、あるいはドメイン名登録者もしくは IP アドレスの付与者から適切に使用権を与えられていることを確認しなければなりません(MUST)。

ワイルドカードの FQDN(Wildcard FQDNs)は許可されています。

本書 の有効日時点において、CA は、subjectAlternativeName や Subject commonName フィールドに予約 IP アドレス(Reserved IP)や内部サーバ名(Internal Server Name)が設定された証明書を発行する際には、申請者に対して、このような証明書の利用は CA/ブラウザフォーラム によって廃止予定であり、2016 年の 10 月までには排除されることを示さなければなりません(SHALL)。同様に本書の有効日時点において、CA は 2015 年 11 月 1 日より後を有効期限とする、subjectAlternativeName や Subject commonName フィールドに予約 IP アドレスや内部サーバ名が設定された証明書を発行してはなりません(SHALL NOT)。

また、2016 年 10 月 1 日をもって、subjectAlternativeName 又は Subject commonName フィールドに予約 IP アドレスや内部サーバ名が設定された有効期間が満了していない証明書を全て失効しなければなりません(SHALL)。

9.2.2 サブジェクトコモンネームフィールド

証明書フィールド名: subject:commonName (OID 2.5.4.3)

必須/任意: 非推奨(推奨されないが、禁止ではない)

コンテンツ: 設定される場合には、このフィールドには subjectAltName(see Section 9.2.1)拡張領域に含まれる IP アドレスあるいは FQDN のうち 1 つのみが設定されなければなりません(MUST)。

9.2.3 サブジェクトドメインコンポーネントフィールド

証明書フィールド名: subject:domainComponent (OID 0.9.2342.19200300.100.1.25)

必須/任意: 任意

コンテンツ: 証明書に設定される場合には、Domain Component フィールドにはサブジェクトの全ての登録ドメイン名について、最も上位の、最もルートに近い、最後に書かれているコンポーネントから順に、全てのコンポーネントが記述されなければなりません。 (MUST)

9.2.4 組織名フィールド

Organization name: organizationName (OID 2.5.4.10)

Number and street: subject:streetAddress (OID: 2.5.4.9)

City or town: subject:localityName (OID: 2.5.4.7)

State or province (where applicable): subject:stateOrProvinceName (OID: 2.5.4.8)

Country: subject:countryName (OID: 2.5.4.6)

Postal/Zip code: subject:postalCode (OID: 2.5.4.17)

必須/任意: organization name は任意。もし organization name が設定される場合には、localityName, stateOrProvinceName (該当する場合), 及び countryName は必須であり(REQUIRED)、streetAddress 及び postalCode は任意。 もし organization name が設定されない場合には、その証明書には streetAddress, localityName, stateOrProvinceName, postalCode を設定してはいけません。(MUST NOT)。 CA は、Section 9.2.5 で規定されるその他のサブジェクト属性情報(Subject Identity Information)の設定なしに、countryName フィールドを設定することが可能です(MAY)。

コンテンツ: organizationName フィールドが設定される場合、そのフィールドはサブジェクトの名称もしくは屋号が設定され、必須の住所フィールドには Section 11.2 の規定に従って CA によって検証されたサブジェクトの所在地が設定されなければなりません。(MUST)。サブジェクトが個人の場合、個人用の Subject name の属性（例えば givenName (2.5.4.42) や surname (2.5.4.4)）が多くのアプリケーションソフトウェアでサポートされていないため、CA は organizationName をサブジェクト名もしくは屋号を表すために使用することが可能です(MAY)。

これらのフィールドが、例えば一般的なバリエーションや略語のように、CA が軽微だと判断する程度の相違を含んでいる場合には、CA はその相違について文書化しなければならず (SHALL) 、また、組織名の略称については、地域によって了承されている略称を使用しなければなりません(SHALL)。例えば公式には“Company Name Incorporated”である場合、CA は “Company Name, Inc.”を使用することが可能です(MAY)。

organizationName フィールドは、検証された屋号やサブジェクトの商標を含むことが可能です。

9.2.5 サブジェクト国名フィールド

証明書フィールド名: subject:countryName (OID: 2.5.4.6)

必須/任意: 任意

コンテンツ: subject:countryName フィールドが設定される場合、CA は Section 11.2.5 に従って、その国とサブジェクトの結びつきを検証し、ISO 3166-1 で規定される 2 ケタの国コードを使用しなければなりません(SHALL)。

9.2.6 その他のサブジェクト属性

サブジェクト情報の例外：organizationalUnitName (OU)、これは任意フィールドですが、もし subject フィールドの中に設定される場合には、CA によって検証された情報が設定されなければなりません(MUST)。『.』（ドット）、「-」（ハイフン） や 『 』 (スペース)などのメタデータ、又はその他欠落・不完全・不適切な値として表示される値を使用してはなりません(SHALL NOT)。

CA は Sections 9.2.1 及び 9.2.2 に定義されるもの以外で、FQDN を Subject の属性に設定してはなりません (SHALL NOT)。

CA は、Section 11.2 に従ってその情報を検証し、かつその証明書が同じく Section 11.2 に従って検証された subject:organizationName, subject:localityName, 及び subject:countryName を含む場合を除き、OU 属性に名称・屋号・商品名・商標・住所・所在地あるいはその他の個人あるいは法的組織体を表すテキストを含めることを除外可能なプロセスを実装しなければなりません(SHALL)。

9.3 証明書ポリシーID

このセクションでは、ルート CA、下位 CA、サブジェクトそれぞれの証明書についての、証明書ポリシー(CP)の表記について記述します。

9.3.1 予約済み証明書ポリシーID

以下の Certificate Policy identifier は、以下の本書要件に対して準拠していることを CA が表明するために使用されます。

> {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), 証明書が本書要件を満たしているが、Section 11.2 の規定に従って検証されたサブジェクト情報を含まない場合。

証明書が policy identifier として 2.23.140.1.2.1 を表明する場合には、organizationName, streetAddress, localityName, stateOrProvinceName, postalCode in は Subject フィールドに含まれてはなりません。(MUST NOT)。

> {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) subject-identity-validated(2)} (2.23.140.1.2.2), 証明書が本書要件を満たしており、かつ Section 11.2 の規定に従って検証されたサブジェクト情報を含む場合。

証明書が policy identifier として 2.23.140.1.2.2 を表明する場合には、organizationName, localityName, stateOrProvinceName (該当する場合), countryName を Subject フィールドに含まなければなりません (MUST)。

9.3.2 ルート CA 証明書

ルート CA は、certificatePolicies 拡張を含むべきではありません(SHOULD NOT)。

9.3.3 下位 CA 証明書

本書の有効日より後に、発行元 CA と異なる運営母体によって運営される下位 CA に対して発行される証明書は：

1. その下位 CA が順守し本要件への迎合性を示す 1 つ以上の明確な policy identifier を設定しなければなりません(MUST)。(例えば CA/ブラウザフォーラムの予約 Identifier や、その CA によって CP/CPS に規定された identifier)　また、
2. “anyPolicy” identifier (2.5.29.32.0) を含んではなりません(MUST NOT)。

有効日より後に、発行元 CA と同じ運営母体によって運営される下位 CA に対して発行される証明書は：

1. その下位 CA が順守しまた準拠する Requirements を示すために、CA/ブラウザフォーラムの予約 Identifier やその CA によって CP/CPS に規定された identifier を設定することが可能です(MAY)。また、
2. “anyPolicy” identifier (2.5.29.32.0) を、特定の policy identifier の代わりに設定することが可能です(MAY)。

下位 CA は CP/CPS において、全ての証明書は本書に準拠していることを示す policy identifier が設定された状態で発行され、本書 に従って管理されることを表明しなければなりません(SHALL)。

9.3.4 加入者証明書

加入者に対して発行される証明書には、その CA によって定義され、本書 に従いまた準拠することを示す 1 つ又は複数の policy identifier が、certificatePolicies extension として設定されなければなりません(MUST)。本書 に準拠する CA はまた、policy OID をそれらの証明書に設定することが可能です(MAY)。

発行元 CA は CP/CPS、当該発行元 CA が発行する特定のポリシーID を含む証明書が本書要件に準拠して管理されていることを CP/CPS に記載することとします(SHALL)。

9.4 有効期間

有効日より後に発行される証明書は、60 カ月以上の有効期間が設定されてはなりません(MUST)。

下記に挙げる要件を満たすものを除き、2015 年 4 月 1 日より後に発行される証明書は、39 カ月以上の有効期間を設定されてはなりません(MUST)。

2015 年 4 月 1 日より後、CA によって文書化された以下のシステム又はソフトウェアに対して提供される証明書については、CA は 39 カ月以上 60 カ月以下の証明書を発行することが可能です(MAY)：

(a) 本書有効日より前から使用されている

(b) 現在でも申請者及び相当数の依拠当事者によって使われている

(c) 60 カ月以下の有効期間に変更すると、使用できなくなる

(d) 依拠当事者に既知のセキュリティリスクが存在しない

(e) パッチの提供やシステムの入れ替えに相当の費用がかかり困難な場合

9.5 加入者証明書

CA は Appendix A に記述されている要求事項に合致しない公開鍵を含む場合、あるいは秘密鍵が既知の脆弱性を含む場合(例：Debian weak key・参照：http://wiki.debian.org/SSLkeys)には、その証明書リクエストを拒絶することとします(SHALL)。

9.6 証明書シリアル番号

CA は、最低でも 20bit のエントロピーからなる非連続の証明書シリアル番号を生成するすることとします(SHOULD)。

9.7 追加の技術要件

CA は Appendix A に記述される暗号アルゴリズムと鍵に対する要求 及び Appendix B の証明書拡張領域に対する要求、及び Appendix C の User Agent の検証に関する要求、それぞれの技術要件を満たすこととします(SHALL)。

10. 証明書申請

10.1 必要書類

CA は、証明書発行前に申請者から以下の文書を取得するものとします(SHALL)。

1. 証明書要求(電子的手段も可)及び
2. 署名済みの利用契約書又は利用約款 (電子的手段も可)

CA は、本書の要件を満たすために必要だと判断した場合、あらゆる追加文書を取得することとします(SHOULD)。

10.2 証明書要求

10.2.1 概要

証明書発行前にCAは、申請者より本要件に準じた形式の証明書要求をCAが規定し取得するものとします(SHALL)。証明書申請組織情報を記した現在の証明書申請は、適切な申請権限者により署名され、11.3のデータ有効期間・更新要件を満たす場合においてはこの申請者による複数の証明書申請に使用できます(MAY)。証明書要求は、電子的に作成、提出、及び/又は署名されることが可能です(MAY)。

10.2.2 要求と認証

証明書要求には、申請者あるいはその代理人からの証明書発行の要求と、申請者あるいは代理人によるその情報の正確性についての証明が含まれなければなりません(MUST)。

10.2.3 情報要件

証明書要求には、証明書に含まれるべき申請者の事実に基づいた情報と、本書要件と、さらに CA の CP/CPS に準拠するために CA が必要に応じ追加情報を含めることが可能です (MAY)。証明書要求に、申請者に関する必要な情報の全てが含まれていない場合は、CA は申請者から残りの情報を取得する、又は信頼のおける独立した第三者データソースから取得した上で、申請者にその情報について確認するものとします(SHALL)。

申請者情報には、少なくとも一つ以上、証明書の SubjectAltName 拡張領域に記載するべき FQDN、又は IP アドレスが含まれなくてはなりません(MUST)。

10.2.4 加入者秘密鍵

加入者以外の関係者は、加入者秘密鍵を保管しないものとします(SHALL NOT)。

CA もしくは、指定された登録局のいずれかが加入者に代わって秘密鍵を生成した場合、CA は加入者に送信するために、秘密鍵を暗号化するものとします(SHALL)。

CA もしくは、指定された登録局のいずれかが、加入者の秘密鍵が、加入者に関連しない権限のない個人又は組織に伝達されたことを認識した場合には、CA は伝達された秘密鍵に対応する公開鍵を含む証明書の全てを失効するものとします(SHALL)。

10.3 利用契約書及び利用約款

10.3.1 概要

CA は証明書の発行前に、CA と証明書受益者の利益を表明するために、以下のいずれかを取得するものとします(SHALL)：

1. 該当 CA との利用契約書に対する申請者の同意
2. 利用約款に対する申請者の同意。

CA は各利用契約書、又は利用約款が申請者に対して法的に効力を持つと認められるプロセスを構築するものとします(SHALL)。いずれの場合も契約は、証明書要求に準じて発行される証明書に対して適用されなければなりません(MUST)。CA が法的に適用可能であると決定した場合、CA は電子的手段もしくは“クリックスルー”方式の契約方法が利用可能です (MAY)。申請者に CA が発行する各証明書が利用規

約もしくは利用約款によって明確に規定されている限り、証明書要求毎に契約書が使用されることが可能であり (MAY)、また、結果として一つの契約書がこれから発行される複数の証明書要求をカバーすることも可能です(MAY)。

10.3.2 契約要件

利用契約書、又は利用約款には、以下の義務と保証が申請者自身に課せられる(もしくはサブコントラクターまたはホスティングサービスを提供する申請代行者が策定した)条項が記載されなければなりません(MUST)。

1. **情報の正確性：**証明書要求、及びその他証明書の発行に関し、常に正確で完全な情報を CA に提供する義務と保証。
2. **秘密鍵の保護：**すべての合理的な手法により、証明書に含まれる公開鍵に対応する秘密鍵 (及びパスワードやトークンなどの関連するあらゆる活性化データやデバイス)を管理、機密保持し、常に適切に保護する申請者の義務と保証。
3. **証明書の受諾：**加入者が証明書のコンテンツの正確性を確認することの義務と保証。
4. **証明書の利用：**証明書に記載されている subjectAltName によってアクセスできるサーバのみに証明書がインストールされ、全ての関連する法律、及び利用契約書又は利用約款に準拠して証明書を使用する義務と保証。
5. **報告と失効：**以下の場合、証明書及び当該秘密鍵の使用を即座に中止し、直ちに CA に当該証明書の失効を依頼する義務と保証。(a)証明書内のいずれかの情報が不適当、もしくは不正確になった場合。(b)証明書の悪用や加入者の公開鍵に対応する秘密鍵が危殆化した事実や疑惑がある場合。
6. **証明書利用の終了：**鍵の危殆化が理由で証明書が失効された場合、直ちに証明書及びその証明書に含まれる公開鍵に対応した秘密鍵の利用を中止する義務と保証。
7. **即応性：**鍵の危殆化や証明書の不正利用の疑いに関する CA からの指示に対し、提示された期間内に対応する義務。
8. **承認と合意：**申請者が利用契約書又は利用約款に違反した場合や、証明書がフィッシング、不正、マルウェアの配布など、犯罪行為のために使用されていることを CA が発見した場合、CA は証明書を直ちに失効する権限を持つことの承認及び合意。

11. 審査手続き

11.1 ドメイン名登録者による承認

CA は証明書が発行される日付に、申請者が証明書に指定する FQDN と IP アドレスを使用する権利又は管理を所有している、もしくは、FQDN と IP アドレスの含まれる証明書を取得できる権利又は管理を所有する人物によって承認されていることを確認するものとします(SHALL)。

CA がドメイン名登録機関での登録済ドメイン名の使用権利又は管理の確認に依拠する場合、及びトップレベルドメインが 2 文字の国別コード(ccTLD)の場合、CA は ccTLD のルールが適用されるドメイン名レベルで、ドメイン名登録機関に直接確認するものとします(SHALL)。例えば、要求されている FQDN が www.mysite.users.example.co.uk の場合、ドメイン名の申請は uk レジストリのルールにより管理された.co.uk に帰属しているため、CA は、ドメイン名(example.co.uk)のドメイン名登録者に確認するものとします(SHALL)。

もし CA がインターネットメールシステムを利用しドメイン名登録者から申請者の FQDN 利用権限を確認する場合、CA は以下のいずれかの方法で形成されるメールシステムアドレスを使用するものとします(SHALL)。

1. ドメイン名登録機関によって提供されたメールアドレス
2. 当該ドメインの WHOIS に表示されているドメイン名登録者の、“登録者”“技術者”又は“アドミン”情報のメールアドレス
3. ドメイン名の前に以下のローカル部分を追加することによって
    a. ローカル部分 - ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’, 又は ‘postmaster’のうちの一つ、及び
    b. ドメイン名- 登録済みドメイン名または申請された FQDN 情報から抽出したドメイン名情報を用いる。

ドメイン名登録者が非公開・匿名、または代理登録のサービスを使用しており、CA が前述の代替としてドメイン利用権限の確認を依存する場合、ドメイン利用権限の確認は、該当ドメイン名の WHOIS 情報で認識されている非公開・匿名、または代理登録のサービスからされなければなりません(MUST)。書類には、非公開・匿名、または代理登録のサービスのレターヘッドと、ゼネラルマネージャー、または同等の代理人による署名、証明書要求日またはそれより後の日付、及び、証明書に記載される FQDN が含まれなければなりません(MUST)。WHOIS レコードが、非公開・匿名、または代理登録のサービスを登録者と特定した場合、ドメイン利用権限の確認は、申請者が証明書の FQDN を使用する権利を付与する記述を含めなければなりません(MUST)。CA は、信頼のおける、独立した第三者機関のデータソースのコンタクト情報を使って、非公開・匿名、または代理登録のサービスに直接連絡をし、ドメイン利用権限の確認の真正性をドメイン名登録者と確認するものとします(SHALL)。

11.2 サブジェクトアイデンティティ情報の審査

申請者が、サブジェクトアイデンティティ情報の countryName フィールドしか含んでいない証明書を申請した場合、CA は、セクション 11.2.5 の要件を満たす審査プロセスを使用してサブジェクトに関連する国及び CP/CPS に記載されている国を審査するものとします(SHALL)。申請者が、countryName フィールドとその他のサブジェクトアイデンティティ情報を含む証明書を要求する場合、セクション 11.2 の要件を満たし、CA の CP/CPS に記載されているプロセスに基づき、CA は申請者のアイデンティティを審査し、申請者代理人の証明書要求の真正性を審査するものとします(SHALL)。CA は本セクションに依拠し、いかなる資料も改ざんや偽造のチェックをするものとします(SHALL)。

11.2.1 アイデンティティ

サブジェクトアイデンティティ情報に、組織名もしくは組織の住所が含まれる場合、CA は、組織のアイデンティティと住所、また、その住所が申請者の所在地もしくは事業所所在地の住所であることを審査することとします(SHALL)。CA は、少なくとも以下のいずれか一つの提出された文書、または連絡手段を用いて申請者のアイデンティティと住所を審査することとします(SHALL)。

1. 申請者の法人が設立又は運営されている地域を管轄する政府機関
2. セクション 11.6 に準じて CA が評価をする定期的に更新される第三者機関のデータベース
3. CA もしくは、CA の代行者として機能する第三者機関による現地訪問
4. 弁護士や会計士など、情報を委託可能な信頼のおける第三者機関により提供された意見書

CA は、申請者のアイデンティティ及び住所両方の審査のために、上記 1 から 4 の文書もしくは連絡手段を用いることが可能です(MAY)。

あるいは、CA は、公共料金請求書、銀行の明細書、クレジットカードの明細書、政府発行の税務書類、又はセクション 11.6 の要件を満たすその他の本人確認書類を使用することにより、申請者の住所を審査することが可能です(MAY)。(しかし、申請者のアイデンティティの審査には使用できません。)

11.2.2 名称/屋号

サブジェクトアイデンティティ情報に、名称もしくは屋号が含まれる場合、CA は、少なくとも以下のいずれか一つを用いて、申請者が名称もしくは屋号を使用する権利があることを審査することとします(SHALL)。

1. 申請者の法人設立、運営する地域を管轄する政府機関より提供された文書、もしくは政府機関からのメール文書など
2. セクション 11.6 の要件を満たす第三者ソースによる資料やメール文書などの記録
3. 名称もしくは屋号の管理をしている政府関連機関とのメール文書などの連絡の記録
4. セクション 11.6 の要件を満たすことを証明する意見書
5. 公共料金請求書、銀行の取引明細書、クレジットカードの明細書、政府発行の税務書類、またはセクション 11.6 の要件を満たすその他の本人確認書類

11.2.3 証明書要求の真正性

サブジェクトアイデンティティ情報を含む証明書の申請者が組織の場合、CA は申請者の証明書要求の真正性を審査するため、信頼できる連絡手段を用いることとします(SHALL)。

CA はセクション 11.2.1 に記載されている情報で、信頼できる連絡手段を用いた審査をすることが可能です(MAY)。CA は信頼できる連絡手段を使用し、申請者の申請権限者に直接、または申請者の主要オフィス・人事部門・IT 部門、またはその他 CA が適切だと判断する部門など、申請者の組織内の信頼できるソースに証明書要求の真正性を確認することが可能です(MAY)。

更に CA は、申請者が証明書の申請する担当者の指名をすることができるプロセスを作成することとします(SHALL)。申請者が証明書の申請担当者を書面で指名した場合、CA は担当者以外の証明書要求を受け付けないものとします(SHALL)。CA は申請者からその書面を受領後、申請者に証明書要求可能担当者リストを送るものとします(SHALL)。

11.2.4 個人申請者の審査

セクション 11.2 に関連する申請者が個人の場合、CA は申請者の氏名、住所、証明書要求の真正性を確認するものとします(SHALL)。

CA は申請者の名前を、申請者の顔が識別できる少なくとも 1 つの現在有効な政府発行フォト ID(パスポート・運転免許証・ミリタリーID・国の ID、または、同等の資料)の判読できるコピーを使って審査するものとします(SHALL)。CA は当該 ID に改ざんや偽造の痕跡がないかどうかの確認をするものとします(SHALL)。

CA はセクション 11.6 の要件を満たす身元証明書(政府により発行された ID、公共料金請求書、銀行・クレジットカードの明細書等)を利用して申請者の住所を審査するものとします(SHALL)。CA は申請者の氏名を審査するのに使用した政府発行 ID に依拠することが可能です(MAY)。

CA は信頼できる連絡手段を用いて、申請者に証明書要求の有無を確認するものとします(SHALL)。

11.2.5 国の審査

subject:countryName が存在する場合、CA はサブジェクトに関連する国を、以下を利用して審査するものとします(SHALL)。(a) 国ごとに割り当てられた IP アドレスの範囲を以下のどちらかの方法で調査します。(i)ウェブサイトの DNS に記録されている IP アドレス(ii)申請者の IP アドレス (b) 申請者ドメイン名の ccTLD (c)ドメイン名登録機関からの情報(d)セクション 11.2.1 において記載されている方法。CA は申請者の所在地と相違する IP アドレス所在地への割り当てを防ぐために、プロキシーサーバーを検出するプロセス構築をすることが推奨されています(SHOULD)。

11.3 認証に用いる情報の有効期間

セクション 9.4 において加入者証明書の有効期間を定めています。CA は 39 カ月以上古いデータや文書を用いて証明書を発行しないものとします(SHALL NOT)。

11.4 拒否リスト

セクション 15.3.2 と同様、フィッシングやその他不正利用などの可能性があるため、CA は過去に失効された証明書や審査により拒絶された証明書に関し、社内データベースを維持するものとします。CA はこの情報を用い、疑わしい証明書要求を識別するものとします(SHALL)。

11.5 ハイリスク証明書要求

CA はリスクの高い証明書要求を識別し、必要に応じて追加審査を行い、これらの証明書要求が本要件に従って十分審査された上で発行するものとします(SHALL)。

CA は頻繁にフィッシングや不正利用に使用される組織名のリストをチェックすること、また、リストに記載されている組織からの証明書要求に対し自動的にフラグを立て、審査をより慎重に行うことにより、リスクの高い証明書要求を識別することが可能です(MAY)。リストの例として、CA により維持されている内部データベース内の、フィッシングや不正の疑いのため失効させられた証明書や、過去に審査が通らなかった証明書要求が挙げられる。

CA はこれらの情報を利用し、リスクが高いと判断される条件を満たした証明書リクエストに対し、フラグを立てるものとします(SHALL)。CA はリスクが高いというフラグが立てられた証明書要求に対して、文書化されたマニュアルに則って追加審査を行うこととします(SHALL)。

11.6 データソースの正確性

サブジェクトアイデンティティ情報を審査するためにデータソースに依拠する前に、CA はデータソースの正確性、信頼性を評価するものとします(SHALL)。データソースが正確性、信頼性を欠いていると CA の評価で判断された場合、CA はそのデータソースを利用してサブジェクトアイデンティティ情報を審査しないものとします(SHALL)。

12. ルート証明書による証明書発行

ルート CA が証明書を発行する際は、CA により権限を付与された担当者(CA システムオペレータ、システムオフィサー、PKI 管理者など)により、ルート CA が証明書に署名するために慎重に直接コマンドを打つものとします(SHALL)。

以下の場合を除いてルート CA の秘密鍵は証明書の署名に使用してはなりません(MUST)

1. ルート CA であることを示す自己署名された証明書
2. 下位 CA の証明書やクロス証明書
3. インフラ目的の証明書 (管理者の証明書、CA 運用のための内部で使用されるデバイス証明書、OCSP レスポンス検証用証明書など)
4. ルート CA により発行された、テスト目的のみの証明書
5. 以下の場合の加入者証明書
    a. ルート CA が本要件有効日より前に生成された 1024-bit RSA キーを使用する場合。
    b. 申請者のアプリケーションが本要件 有効日より前に導入された場合。

c. 申請者のアプリケーションがすでに申請者により使用されている場合、又は CA が文書化されたプロセスを使用し、証明書の利用が多くの依拠当事者により必要とされていると判断した場合。

d. CA が文書化されたプロセスを使用し、申請者のアプリケーションが既知のセキュリティリスクを依拠当事者に与えないと判断した場合。

e. 申請者のアプリケーションがパッチの適用やシステムの入れ替え多大なコストがかかると CA が文書化した場合。

13. 証明書失効とステータスチェック

13.1 失効

13.1.1 失効リクエスト

CA は加入者が自身の証明書の失効申請を行うプロセスを定めることとします(SHALL)。また、当該プロセスは CA の CP/CPS に記載しなければなりません(MUST)。CA は失効申請及び関連する照会に、24 時間 365 日対応可能な体制を維持することとします(SHALL)。

13.1.2 証明書問題報告

CA は加入者、依拠当事者、アプリケーションソフトウェアプロバイダ、及びその他第三者に対し秘密鍵の危殆化、証明書の悪用、その他の不正、セキュリティ侵害、悪用、不適切な行動や証明書に係る事象について報告するための明確な方法を提示するものとします(SHALL)。CA は連絡手段を容易にアクセス可能なオンラインの手段によって提示するものとします(SHALL)。

13.1.3 調査

CA は証明書に関する問題の報告を受けてから 24 時間以内に調査を実施し、以下の基準をもとに失効又は他の適切な処置をするかどうかの判断をするものとします(SHALL)。

1. 報告された問題の性質
2. 特定の証明書もしくは加入者全体に関連する証明書に関する問題の報告数
3. 問題の報告を行った法的組織体 (例として、Web サイトが違法行為を行っているという捜査当局からの報告は、オーダーした製品が届かなかったという顧客の主張よりも重要と判断されます。)
4. 関連する法律

13.1.4 対応

CA は重要な証明書に関する問題の報告があった場合に社内で対応可能な 24 時間 365 日体制を維持し、必要に応じてこれらの報告を捜査当局に連絡及び/又は報告にあった証明書を失効させるなどの対応をするものとします(SHALL)。

13.1.5 失効の事由

CA は以下の事象が一つ以上発生した場合、24 時間以内に証明書を失効するものとします(SHALL)。

1. 加入者が書面で証明書失効依頼を出した場合。
2. 加入者が CA に当該証明書要求は許可されておらず、遡及的な許可もしないとの連絡をした場合。

3. CA が加入者の証明書の公開鍵に対応する秘密鍵が危殆化された、もしくは証明書が悪用された(セクション 10.2.4 参照)という証拠を入手した場合。
4. 加入者が利用契約書、利用約款における重要な義務のうち、一つ以上の違反を犯していることを CA が認知した場合。
5. CA が FQDN や IP アドレスの使用が法的に認められていないと判断した場合(裁判所や仲裁人がドメイン名登録機関のドメイン名を使用する権利を剥奪した場合、ドメイン名登録局と申請者との間の関連するライセンス契約、サービス契約が終了した場合、又はドメイン名登録局がドメイン名の更新をしなかった場合。)
6. 悪用目的のため、ワイルドカード証明書が誤解を招く可能性の高い下位 FQDN の認証に使用されていると CA が判断した場合。
7. CA が証明書内の情報に重要な変更が加えられていると判断した場合。
8. 証明書が本書、CA の CP/CPS 通りに発行されていないと CA が判断した場合。
9. CA が証明書の情報が正確でない、もしくは誤解を招く恐れがあると判断した場合。
10. CA がいかなる理由であれ認証業務を中止し、他の CA に証明書の失効サポートの依頼を行わなかった場合。
11. CA が本書に従って証明書を発行する権利が失効、廃止、終了し、CA が CRL/OCSP レポジトリの維持管理を続けない場合。
12. CA が証明書発行を行う下位 CA の秘密鍵が危殆化した可能性があると判断した場合。
13. CP/CPS により失効が必要な場合。
14. 証明書の技術面やフォーマットがアプリケーションソフトウェアベンダや依拠当事者に受け入れ難いリスクを与える場合。(CA/ブラウザフォーラムは廃止予定の暗号化/署名アルゴリズムや鍵サイズが受け入れ難いリスクを与えると判断した場合、それらを使用している証明書を定められた期間内に失効させるか差し替える必要があると判断することもあります。)

13.2 証明書のステータスの確認

13.2.1 メカニズム

CA は下位証明書や加入者証明書の失効情報を Appendix B に記載されている要件通り提供するものとします(SHALL)。

加入者証明書がアクセスの多い FQDN の場合、CA は RFC4366 の通り、Stapling を利用して OCSP レスポンスを配布することが可能です(MAY)。その場合、CA は加入者が TLS ハンドシェイク中に証明書の OCSP レスポンスを“ステープル”していることを保証することとします(SHALL)。CA はこの要件を利用契約書又は利用約款、もしくは CA により導入されている技術審査基準に含め、準拠させることとします(SHALL)。

13.2.2 レポジトリ

CA は、その CA が発行した有効期間内の証明書について、アプリケーションソフトウェアが自動的に現在のステータスについての照会を行うことを可能にするオンラインレポジトリを 24 時間 365 日維持するものとします(SHALL)。

加入者証明書のステータスについては以下の通りとします。

1. CA が CRL を発行する場合、CA は最低 7 日に 1 度、CRL の更新、再発行を行うものとします(SHALL)。また、「nextUpdate」フィールドの値は「thisUpdate」のフィールドの値より 10 日以上大きい値になってはなりません(MUST NOT)。
2. CA は OCSP で提供される情報を最低四日に一度は更新するものとします(SHALL)。このサービスからの OCSP レスポンスの有効期間は 10 日以下でなければなりません(MUST)。

下位証明書のステータスについては以下の通りとします。

1. CA は CRL の更新、再発行を最低(i)12 カ月に 1 度、(ii)下位 CA 証明書の失効から 24 時間以内に行うこととします(SHALL)。また、「nextUpdate」フィールドの値は「thisUpdate」フィールドの値より 12 カ月以上大きい値になってはなりません(MUST NOT)。
2. CA は OCSP で提供される情報について、最低(i)12 カ月に一度、(ii)下位証明書の失効から 24 時間以内に更新するものとします(SHALL)。

2013 年 1 月 1 日より、CA は本書要件を満たして発行された証明書に対し、GET Method を使用した OCSP をサポートするものとします(SHALL)。

13.2.3 レスポンスタイム

CA は CRL 及び OCSP を運用、維持し、通常運用時に 10 秒以内のレスポンスタイムを達成するものとします(SHALL)。

13.2.4 データの削除

CRL 及び OCSP の失効データは失効証明書の有効期限まで削除してはなりません(MUST NOT)。

13.2.5 OCSP 署名

OCSP レスポンスは RFC2560 及び/又は RFC5019 に準拠しなければなりません(MUST)。OCSP レスポンスは以下のどちらかにより署名されていなければなりません(MUST)。

1. 失効状況の確認対象となる証明書を発行した CA により署名されている。
2. 失効状況の確認対象となる証明書を発行した CA によって署名された証明書を持つ OCSP レスポンダにより署名されている。

後者の場合、OCSP への署名に使用される証明書は RFC2560 に記載されている通り、type id-pkix-ocsp-nocheck の拡張領域を含まなければなりません(MUST)。

14. 従業員及び第三者に関する事項

14.1 信頼性及び能力

14.1.1 本人確認及び身元審査

証明書マネジメントプロセスに従事する前に、従業員、代行者、CA の契約社員に係らず、CA は担当者の本人確認及び担当者の身元を審査することとします(SHALL)。

14.1.2 トレーニング及び技術レベル

CA は全ての審査担当者に基礎的な PKI の知識、認証、及び審査ポリシーや手順(CA の CP/CPS を含む)、審査プロセスにおける一般的な脅威(フィッシングやその他ソーシャルエンジニアリング手法を含む)、また、本書などについてのトレーニングを行うものとします(SHALL)。

CA はトレーニングの記録を保持し、審査担当者が業務を行うにあたり十分な能力を保持することを確認するものとします(SHALL)。

証明書の発行を行う審査担当者は CA のトレーニング及びパフォーマンスプログラムに沿ったスキルレベルを保持することとします(SHALL)。

CA は各審査担当者が実務を行う前に必要な能力を保持していることを確認し、文書化するものとします(SHALL)。

CA は審査担当者が本書により定められている審査要件に基づき作成・実施するテストに必ず合格することを求めます (SHALL)。

14.2 機能の委託

14.2.1 概要

CA は本書のセクション 11 の要件を全て満たす場合のみ、セクション 11 に記載されている要件の全てもしくは一部を CA 組織以外の第三者に委託することが可能です(MAY)。

CA が外部委託先に機能を委託する前に CA は第三者に対し、契約に以下の要求を含めることとします(SHALL)。

1. 委託された機能を実施する場合はセクション 14.1 における必要条件を満たしていること
2. セクション 15.3.2 に記載されている通り、必要資料を保持すること
3. 本書要件以外の機能委託に係る事項を順守する
4. (a)委託する CA の CP/CPS、又は(b) 本書要件を満たすことが CA によって確認されている、外部委託先の運用規程に準拠していること

CA は外部委託先の証明書を発行する担当者がセクション 14 で定められているトレーニングやスキル要件を満たし、セクション 15 における資料保管やイベントログの必要要件を満たすことを確認することとします(SHALL)。

14.2.2 コンプライアンスの義務

CA は年次で各外部委託先が本書に準拠しているかどうかを確認するものとします(SHALL)。

14.2.3 法的責任の配分

委託された業務については、CA 及び外部委託先は法的責任の分配方法を自分たちで決定し、契約することが可能です(MAY)。しかし、業務委託をしていたとしても、CA は全当事者によって行われる本書に関連する行為について、それが委託されていない場合と同様に全責任を負うこととします(SHALL)。

14.2.4 エンタープライズ RA

CA はエンタープライズ RA の組織内からの証明書要求を審査するために、エンタープライズ RA を指定することが可能です(MAY)。

CA は以下の要件を満たさない限り、エンタープライズ RA により認証されている証明書要求を受け付けないものとします(SHALL NOT)。

1. CA は申請された FQDN がエンタープライズ RA の審査済みのドメインネームスペース内(セクション 7.1.2 参照)のものであることを確認するものとします(SHALL)。

2. 証明書要求が FQDN 以外のサブジェクト名を含む場合、CA はそのサブジェクト名が委託した企業、委託した企業の関連会社、もしくは委託した企業がサブジェクト名の企業の申請権限者であることを確認するものとします(SHALL)。例えば、CA は“ABC.Co”のエンタープライズ RA 内に“XYZ Co.”というサブジェクト名を含む証明書を発行してはなりません。(二つの企業が関連企業である場合(セクション 11.1)、もしくは“ABC Co.”が“XYZ Co.”の申請権限者である場合を除きます。) この要件はサブジェクトの FQDN が ABC Co.のドメインネームスペースの登録されたドメイン名内に含まれる場合も適用されることとします(SHALL) 。

CA は上記制限を契約上の要件としてエンタープライズ RA に課し、準拠されているかを監視するものとします(SHALL)。

15. データ記録

15.1 文書及びイベントログ

CA 及び外部委託先は、証明書依頼や証明書発行にあたり実施された事項(全ての生成された情報、証明書要求において受領した文書、日時、担当者などを含む、証明書要求及び発行を処理するにあたり実施した事項)の詳細な記録をするものとします(SHALL)。また、CA は自社が本書要件を満たすことの証拠として、上記情報を公認監査人が利用できるようにするものとします(SHALL)。

15.2 イベント及び行動

CA は最低でも以下を記録するものとします(SHALL)。

1. 以下のような CA キーライフサイクルマネジメントに関連する事項
    a. 鍵生成、バックアップ、保管、リカバリー、アーカイブ、破棄。
    b. 暗号化デバイスのライフサイクルマネジメント。
2. 以下のような CA 及び証明書ライフサイクルマネジメントに関する事項
    a. 証明書の申請、更新、再発行、及び失効申請。
    b. 本書及び CA の CPS に規定されている全ての審査に係る事項。
    c. 日時、利用された電話番号、電話応対者、及び電話での審査結果。
    d. 証明書要求の受領・拒否判定。
    e. 証明書の発行。
    f. CRL の生成及び OCSP のエントリー。
3. 以下のようなセキュリティに関する事項
    a. PKI システムへのアクセス(成否に係らず)。
    b. PKI 及びセキュリティーシステムが実施したアクション。
    c. セキュリティープロファイルの変更。
    d. システム障害、ハードウェア故障、その他異常など。
    e. ファイアーウォール、ルータの動作。
    f. CA 施設への入退室。

ログは以下を含まなければなりません(MUST)。

1. 記録日時
2. 情報を記録した担当者情報
3. 記録の詳細

15.3 保存

15.3.1 監査記録の保存

CA は本書有効日以降、CA は監査ログを最低 7 年間保存し、監査人による要請があれば提出するものとします(SHALL)。

15.3.2 文書の保存

CA は証明書要求や審査、証明書や失効に係る全ての文書を、当該証明書が失効してから最低 7 年間保存するものとします(SHALL)。

16. データセキュリティ

16.1 目的

CA は以下の目的のために包括的なセキュリティプログラムを開発、実装、維持するものとします(SHALL)。

1. 証明書及び証明書マネジメントプロセスのデータの機密性、完全性、可用性を保持するため。
2. 既知の脅威や危機から証明書データや証明書マネジメントプロセスの機密性、完全性、可用性を保護するため。
3. 許可されていない又は違法なアクセス、使用、公開、変更、及び破壊から証明書データ及び証明書マネジメントプロセスを保護するため。
4. 事故による損失、破壊、もしくは損害から証明書データ及び証明書マネジメントプロセスを保護するため。
5. その他 CA が法律で定められているセキュリティ要件に準拠するため。

16.2 リスクアセスメント

CA のセキュリティプログラムは年次で以下を含むリスクアセスメントを実施しなければなりません(MUST)。

1. 証明書データや証明書マネジメントプロセスへの不正アクセス、公開、不正利用、改ざん、破壊をもたらす可能性のある、内部・外部の脅威の識別。
2. 証明書データ及び証明書マネジメントプロセスに対する上記脅威の発生可能性及び発生した場合の潜在的被害額の評価。
3. ポリシー、手順、情報システム、技術、及びその他脅威に対抗するための手段の評価。

16.3 セキュリティプラン

リスクアセスメントをもとに、CA はセキュリティ手順、対策、及び製品を利用して上記目的を達成し、リスクアセスメントで識別されたリスクを管理及び制御するため、証明書データ及び証明書マネジメン

トプロセスの重要度に応じたセキュリティ計画を設計、導入、及び維持するものとします(SHALL)。セキュリティ計画では、証明書データ及び証明書マネジメントプロセスの重要度に応じ、管理的、組織的、技術的、及び物理的に対策を実装しなければなりません(MUST)。また、セキュリティ計画は使用可能なテクノロジーや導入コストを考慮し(MUST)、セキュリティが侵害された際の被害や保護するデータの性質に応じて適切なレベルのセキュリティを実装するものとします(SHALL)。

16.4 ビジネス継続性

更に、災害、セキュリティ侵害、及び事業の失敗の際に CA はアプリケーションソフトウェアベンダ、加入者、及び依拠当事者に連絡し、合理的に保護するために事業継続計画及び災害復旧計画を文書化するものとします(SHALL)。CA は外部に事業継続計画を公表する必要はありませんが、CA の監査人による要請があった場合には、事業継続計画及びセクション 15.3 におけるセキュリティ計画を提出するものとします(SHALL)。また、CA は年次で事業計画をテスト、評価、及び更新することとします(SHALL)。

事業継続計画は以下を含まなければなりません(MUST)。

1. 事業継続計画を発動する際の条件
2. 緊急手順
3. フォールバック手続き
4. 再開手続き
5. 計画のメンテナンススケジュール
6. 認知及び教育要件
7. 個人の役割
8. 目標復旧時間(RTO)
9. 緊急対策計画の定期的なテスト
10. 重要なビジネスプロセスの障害や不具合が発生した場合の CA 業務の維持や復旧計画
11. 代替オフィスにおける重要な暗号化機器(暗号化デバイスや起動機器など)の設置要件
12. 許容可能なシステム停止時間及び復旧時間の策定
13. 必要な業務情報及びソフトウェアのバックアップ頻度
14. CA のメインサイトからの代替オフィスの距離
15. 災害後から安全な環境を現地もしくはリモートサイトに構築するまでの期間に、可能な範囲の施設の保護方法

16.5 システムセキュリティ

証明書管理プロセスは以下を含まなければなりません(MUST)。

1. 物理セキュリティ及び環境統制
2. コンフィギュレーションマネジメント、Trusted code の完全性維持、マルウェア検知/防止を含むシステムインテグリティ統制
3. ポート制限、IP アドレスフィルタリングを含むネットワークセキュリティ及びファイアーウォールマネジメント
4. ユーザマネジメント、職務分掌、教育、認知、トレーニング
5. 個々の責任を明確にするためのロジカルアクセス制御、アクティビティログ、不使用時のタイムアウト。

CA は証明書を直接発行することが可能な全てのアカウントに対し複数要素認証を適用させることとします(SHALL)。

16.6 秘密鍵の保護

CA は FIPS140 レベル 3、もしくはコモンクライテリアプロテクションプロファイルやセキュリティ水準 EAL 4 以上の要件(秘密鍵やその他の資産を既知の危機から保護するための要件を含む)を満たすと認められているシステム又はデバイスの中で秘密鍵を保護するものとします(SHALL)。また、CA は物理的、論理的に不正証明書発行を防ぐ手段を導入しなければなりません(MUST)。上記に適合しているシステム又は機器以外で秘密鍵を保護する場合は物理セキュリティや暗号化もしくは両方を実装し、秘密鍵の漏えいを防ぐものとします(SHALL)。CA は秘密鍵を最高水準のアルゴリズム及び鍵長で暗号化し、鍵、及び鍵パーツの使用可能期間の終了まで暗号解読攻撃に耐えうるようにするものとします(SHALL)。秘密鍵のバックアップ、保管、復元は、安全な物理的環境において信頼できる人間の複数立会いの元でのみ行うものとします(SHALL)。

17. 監査

17.1 適格監査基準

CA は以下のいずれかの基準での監査を受けるものとします(SHALL)。

1. CA 向け Webtrust 監査 v2.0 以降
2. ETSITS 101 456 v1.2.1 以降への準拠を監査する国際基準
3. ETSITS 102 042 v1.1.1 以降への準拠を監査する国際基準
4. ISO 21188:2006 への準拠を公認監査人により監査する基準
5. 政府運営 CA が CP にて異なる内部の監査基準を使用することを必須とした場合、以下を条件に使用することが可能です。(a)上記基準のどれかを全て満たす監査、もしくは同等の公表されている基準を使用した監査、(b)監査がセクション 17.6 の基準を満たす CA から独立した監査人により実施される場合。

17.2 監査期間

CA が証明書を発行する期間は全て監査の対象となります(SHALL)。監査期間は 1 年を超えてはなりません(MUST NOT)。

17.3 監査報告

CA は監査報告書を公表するものとします(SHALL)。CA は全体の監査意見に影響がない程度の監査指摘事項を公表する必要はありません。政府 CA、商用 CA ともに、監査報告書は監査期間の終了時から 3 カ月以内に公表するべきです(SHOULD)。もし監査報告書の公表が 3 カ月以上遅れ、アプリケーションソフトウェアベンダにより提出を求められた場合、CA は公認監査人により署名された説明文を提出するものとします(SHALL)。

17.4 証明書発行開始前の準備状況の監査(初回審査時)

CA が現在有効なセクション 17.1 に記載されている基準を満たす監査報告書を保持している場合、発行前の準備状況の評価は必要ありません。

CA が現在有効なセクション 17.1 に記載されている基準を満たす監査報告書を保持していない場合、パブリック証明書を発行する前に CA はセクション 17.1 に記載されている監査基準のいずれかで、基準を満たすかどうかについてのその時点における準備状況の評価を行うものとします(SHALL)。準備状況の評価はパブリック証明書の発行を開始する 12 カ月より前に評価しないものとします(SHALL)。また、パブ

リック証明書の発行開始後から 90 日以内に同じ監査基準にて包括的な監査を受けるものとします(SHALL)。

17.5 委託機能の監査

外部委託先がセクション 17 において定められている基準で監査されておらず、エンタープライズ RA でない場合、証明書の発行前に CA はセクション 11.1 において定められているドメインコントロール審査プロセスが委託された第三者により準拠されていることを確かめるために、以下のどちらかの方法を実施することとします(SHALL)。(1) CA の代理として、もしくは外部委託先の代理としての役割で最低 1 人を参加させ、アウトオブバンドメカニズム用いて証明書要求に使用された情報の正当性を確認する。(2)ドメインコントロール審査プロセスそのものを実施する。

CA が上記手続きを実施せず、外部委託先がエンタープライズ RA でない場合、CA はセクション 17.1 において認められている監査基準を満たす監査報告書を入手し、外部委託先の行為が業務委託先の運用規程もしくは CA の CP/CPS に準拠しているかどうかを確認することとします(SHALL)。外部委託先が準拠していないとみなされた場合、CA は外部委託先に引き続き業務委託を委託してはなりません(SHALL NOT)。

外部委託先の監査期間は 1 年間を超えてはなりません(SHALL NOT) (委託する CA の監査と同時期に行われることが望ましいとされています)。しかしながら、CA や外部委託先が行政機関により運用、制御、監視されており、監査結果が数年にわたり問題ないと判断された場合、年次の監査ではコアなコントロールのみを監査し、コアでないコントロールの監査頻度を下げることも可能です。しかし、コアでないコントロールでも最低 3 年に 1 度は監査されなければなりません(MUST)。

17.6 監査資格

CA の監査は公認監査人により実施されなければなりません(SHALL)。公認監査人とは以下の必要要件及び能力を保持する個人、法的組織体、個人の集団、もしくは法的組織体の集団のことを意味します。

1. 被監査先からの独立
2. 適切な監査基準の必要要件を監査することができる能力
3. PKI 技術、情報セキュリティツールや技法、IT 及びセキュリティ監査に習熟した人物を雇用している第三者認証機関。
4. 監査基準に規定されている資格を有する、認定されている、免許を持つ、もしくは必要要件を満たすと評価できること。
5. 法律、政府の法令、職業倫理に準拠している。
6. 国内政府監査機関の場合以外は、最低 100 万 US ドルを保証する賠償責任保険に入っていること

17.7 鍵生成セレモニー

有効日より後に生成された(i)ルート CA 鍵ペアとして使用されるルート CA 鍵ペアもしくは(ii)ルート CA の運営者やルート CA の関連会社によらない下位 CA のために生成された鍵ペアの場合、CA は以下を実施するものとします(SHALL)。

1. 鍵生成スクリプトを用意し、スクリプト通りに実施する。
2. 公認監査人にルート CA 鍵ペアの生成プロセスへの立会いを依頼するか、ルート CA 鍵ペア生成プロセスの全てを録画する。
3. 公認監査人に CA が鍵及び証明書発行プロセスの際に鍵ペアの完全性、機密性を確実にするキーセレモニーを実施したという報告書を提出してもらう。

ルート CA の管理者もしくはルート CA の関連会社において、本要件有効日より後に発行された CA の鍵ペアに関しては以下を実施すべきです(SHOULD)。

1. 鍵作成スクリプトを用意し、スクリプト通りに実施する。
2. 公認監査人にルート CA 鍵ペアの生成プロセスへの立会いを依頼するか、ルート CA 鍵ペア生成プロセスの全てを録画する。

全ての場合において、CA は以下を実施するものとします(SHALL)。

1. CA の CP/CPS に記載されている通り、鍵を物理的に安全な環境で生成する。
2. 複数人による統制や知識分散という原則のもと信用されるべき役職の担当者により CA の鍵を生成する。
3. CA の CP/CPS に記載されている技術要件、ビジネス要件を満たす暗号モジュール内で CA の鍵を生成する。
4. CA 鍵生成の記録を取得する。
5. 有効的な統制を維持し、CP/CPS、及び鍵生成スクリプト(該当する場合)に記載されている手続きに沿って秘密鍵が生成、保護されることの合理的な保証を与えること。

17.8 定期的な内部監査

CA が証明書を発行している期間、CA は本書、CP/CPS に準拠していることをモニターし、内部監査を最低四半期ごとに実施することにより厳格にサービス品質を管理するものとします(SHALL)。内部監査ではランダムに選定した最低 1 証明書、もしくは前回の監査で使用した最後のサンプルより後に発行された証明書数の 3%の多い方をサンプルとして利用することとします(SHALL)。また、セクション 16.3 に記載された要件を満たす年次の監査を受けている外部委託先以外は、審査の専門家を利用して四半期の監査を行うことにより、CA は外部委託先により発行された証明書や審査された情報の品質を厳密に管理するものとします(SHALL)。外部委託先の監査ではランダムに選定した最低 1 証明書もしくは、前回の監査で使用した最後のサンプルより後に発行された証明書数の 3%の多い方をサンプルとして利用します(SHALL)。また、CA は外部委託先が本書や CP/CPS に確実に準拠させるために、各外部委託先の運用方法や手続きを調査することとします(SHALL)。

18. 義務と免責

18.1 加入者と依拠当事者に対する義務

CA が本書及び CP/CPS の要件に準拠する運用方法で証明書を発行・管理している限り、証明書利用者やその他第三者に対し、証明書を利用や信用した結果、被ったいかなる損害についても、CP/CPS に規定された損害賠償を上限とし、それ以上の要求に関してはされうるものとします(MAY)。CA が本書及び CP/CPS に準拠しないで証明書を発行・管理を行っていなかった場合、当該 CA は加入者や依拠当事者に対し、証明書の使用や信用した結果、被ったいかなる損失及び損害についても、その訴因や関連法理論に係らず、CA は CA が適切と考える手段によって、加入者や依拠当事者に対する賠償責任の制限を要求することが可能とします(MAY)。CA が本書や CP/CPS に準拠せずに発行・管理された証明書に関する賠償を限定する場合、当該 CA は、その賠償責任の上限を CP/CPS に記載するものとします(SHALL)。

18.2 アプリケーションソフトウェアベンダの免責

加入者や依拠当事者への賠償責任の限定に係らず、ルート CA とルート証明書配布契約を結んでいるアプリケーションソフトウェアベンダは CA により発行・管理されている証明書の利用もしくは信用により発生した賠償に一切関与しないということを、当該 CA は理解し、認識しなければなりません。そのため、CA が行政機関の場合を除き、CA は訴訟の原因や関連法理論に係らず CA により発行された証明

書に関連する訴訟、被害や損害から各アプリケーションソフトウェアベンダを守り、補償、もしくは免責するものとします(SHALL)。しかしながら、アプリケーションソフトウェアベンダのソフトウェアが以下のような不正な証明書を有効、又は信頼可能と表示したことによって生じたアプリケーションソフトウェアベンダの被害に関して、上記は適用されません。(1)期限切れの証明書、(2)失効している証明書(ただし、失効ステータスが CA によりオンラインで公開されており、アプリケーションソフトウェアが失効ステータスのチェックに失敗した場合、又は失効ステータスを無視した場合のみ)

18.3 ルート CA の義務

ルート CA は、下位 CA の運用方法や正当性、下位 CA が本書に準拠していることや、本書に記載されている法的責任や補償義務について、ルート CA がその証明書の発行を行った下位 CA であった場合に発生すると考えられる全責任を負うものとします(SHALL)。

Appendix A – 暗号アルゴリズムと鍵の要求事項(基準)

証明書は以下のアルゴリズムの種類とサイズの要件を満たさなければなりません(MUST)。

(1) ルート CA 証明書

	有効期間が 2010 年 12 月 31 日より前に開始した場合	有効期間が 2010 年 12 月 31 日より後に開始した場合
ダイジェストアルゴリズム	MD5 (推奨されない)、 SHA-1、 SHA-256、 SHA-384 、もしくは SHA-512	SHA-1*、 SHA-256、 SHA-384 もしくは SHA-512
最低 RSA モジュールサイズ(bits)	2048**	2048
ECC カーブ	NIST P-256、 P-384、もしくは P-521	NIST P-256、 P-384、 もしくは P-521

(2) Subordinate CA Certificates 下位 CA 証明書

	有効期間が 2010 年 12 月 31 日より前に開始し、2013 年 12 月 31 日より前に終了する場合	有効期間が 2010 年 12 月 31 日より後に開始し、2013 年 12 月 31 日より後に終了する場合
ダイジェストアルゴリズム	SHA-1、 SHA-256、 SHA-384、もしくは SHA-512	SHA-1*、 SHA-256、 SHA-384 、もしくは SHA-512
最低 RSA モジュールサイズ(bits)	1024	2048
ECC カーブ	NIST P-256、 P-384、もしくは P-521	NIST P-256、 P-384 もしくは P-521

(3) 加入者証明書

	有効期間が 2013 年 12 月 31 日より前に終了する場合	有効期間が 2013 年 12 月 31 日より後に終了する場合
ダイジェストアルゴリズム	SHA1*、 SHA-256、 SHA-384 もしくは SHA-512	SHA1*、 SHA-256、 SHA-384 もしくは SHA-512
最低 RSA モジュールサ	1024	2048

イズ(bits)		
ECC カーブ	NIST P-256、 P-384、 もしくは P-521	NIST P-256、 P-384、 もしくは P-521

* SHA-1 は、SHA-256 が世界中の相当数の依拠当事者が使用するブラウザによって広範囲にサポートされるまでは使用することが可能です(MAY)。

** 2010 年 12 月 31 日より前に 2048bit 以下の RSA の鍵に対して発行されたルート CA 証明書は、Requirements に則ったサブジェクト証明書に対するトラストアンカーとして提供されることが可能です(MAY)。

Appendix B – 証明書拡張領域(基準)

この appendix では、本書有効日より後に発行される証明書の拡張領域について定義します。

ルート CA 証明書

ルート証明書は、X.509 v3 でなければなりません(MUST)。

A. basicConstraints

cA フィールドは true にセットされなければなりません(MUST)。pathLenConstraint フィールドは設定さるべきではありません(SHOULD NOT)。

B. keyUsage

この拡張領域は critical extension でなければなりません(MUST)。keyCertSign 及び cRLSign に対するビット位置は設定されなければなりません(MUST)。ルート CA の秘密鍵が OCSP のレスポンスに対する署名に使用される場合には、digitalSignature ビットが設定されなければなりません(MUST)。

C. certificatePolicies

この拡張領域は設定されるべきではありません(SHOULD NOT)。

D. extendedKeyUsage

この拡張領域は設定されてはなりません(MUST NOT)。

その他全てのフィールド及び拡張領域の設定については RFC 5280 に準拠しなければなりません(MUST)。

下位 CA 証明書

下位 CA 証明書は X.509 v3 タイプでなければなりません(MUST)。

A. certificatePolicies

この拡張領域は設定されなければならず(MUST)、critical にすべきではありません(SHOULD NOT)。

certificatePolicies:policyIdentifier (MUST)

以下のフィールドは、下位 CA がルート CA コントロール下にない場合には設定してもよい(MAY)。

certificatePolicies:policyQualifiers:policyQualifierId (Optional)

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

- ルート CA の CP/CPS の HTTP URL 、依拠当事者規程、あるいはその他 CA によって提供されるオンラインポリシー情報のポインター

B. cRLDistributionPoints

この拡張領域は設定されなければならず(MUST)、critical に設定されてはなりません(MUST NOT)。この領域は CA の CRL サービスの HTTP URL が設定されなければなりません(MUST)。

C. authorityInformationAccess

この拡張領域は、以下に述べるものの集合として、設定されなければならず(MUST)、critical であってはならず(MUST NOT)、かつ発行元 CA の OCSP レスポンダの HTTP URL (accessMethod = 1.3.6.1.5.5.7.48.1)を含まなければなりません(MUST)。また、発行元 CA 証明書の HTTP URL (accessMethod = 1.3.6.1.5.5.7.48.2)を含むべきです(SHOULD)。詳細は 13.2.1 を参照のこと。

発行元 CA の OCSP レスポンダの HTTP URL を省略し、TLS ハンドシェイク中に、当該証明書に対する OCSP レスポンスを”ステープル”して提供することが可能です(MAY)。 [RFC4366].

D. basicConstraints

この拡張領域は設定され、critical でなければなりません(MUST)。cA フィールドは true に設定されなければなりません(MUST)。pathLenConstraint フィールドは設定されてもよい(MAY)。

E. keyUsage

この拡張領域は critical extension でなければなりません(MUST)。keyCertSign 及び cRLSign に対するビット位置は設定されなければなりません(MUST)。下位 CA の秘密鍵が OCSP のレスポンスに対する署名に使用される場合には、digitalSignature ビットが設定されなければなりません(MUST)。

その他全てのフィールド及び拡張領域の設定については RFC 5280 に準拠しなければなりません(MUST)。

加入者証明書

A. certificatePolicies

この拡張領域は設定されなければならず(MUST)、critical にすべきではありません(SHOULD NOT)。

certificatePolicies:policyIdentifier (Required)

- 発行元 CA それを順守し、また本書に準拠することを主張する、発行元 CA によって定義された CP を示す 1 つの Policy Identifier

以下の拡張領域は表示することが可能です(MAY)。

certificatePolicies:policyQualifiers:policyQualifierId (Recommended)

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

- 下位 CA の CP/CPS の HTTP URL 、依拠当事者規程、あるいはその他 CA によって提供されるオンラインポリシー情報のポインター。

B. cRLDistributionPoints

この拡張領域は設定されてもよく(MAY)、critical に設定されてはなりません(MUST NOT)。この領域は CA の CRL サービスの HTTP URL が設定されなければなりません(MUST)。詳細は 13.2.1 を参照のこと。

C. authorityInformationAccess

この拡張領域は、以下に述べるものの集合として、設定されなければなりません(MUST)。これは critical であってはならず(MUST NOT)、かつ発行元 CA の OCSP レスポンダの HTTP URL (accessMethod = 1.3.6.1.5.5.7.48.1)を含まなければなりません(MUST)。また、発行元 CA 証明書の HTTP URL (accessMethod = 1.3.6.1.5.5.7.48.2)を含むべきです(SHOULD)。

発行元 CA の OCSP レスポンダの HTTP URL を省略し、TLS ハンドシェイク中に、当該証明書に対する OCSP レスポンスを”ステープル”して提供することが可能です(MAY)。 [RFC4366]

D. basicConstraints (optional)

設定される場合、cA フィールドは false でなければなりません(MUST)。

E. keyUsage (optional)

設定される場合は、keyCertSign と cRLSign は設定されてはなりません(MUST NOT)。

F. extKeyUsage (required)

id-kp-serverAuth [RFC5280] もしくは id-kp-clientAuth [RFC5280] 、もしくは両方が設定されていなければなりません(MUST) 。id-kp-emailProtection [RFC5280]は設定されてよいこととします(MAY)。その他の値は設定されるべきではありません(SHOULD NOT)。

その他全てのフィールド及び拡張領域の設定については RFC 5280 に準拠しなければなりません(MUST)。

Appendix C – ユーザ代行者認証 (基準)

CA は、アプリケーションソフトウェアの供給者に対して、各 trusted Root Certificate にチェインされたサブジェクト証明書のテストの目的で、テスト WEB ページを提供することとします(SHALL)。最低でも、CA は(i) 有効, (ii) 失効 (iii) 期限切れそれぞれのサブジェクト証明書に対して個別の WEB ページを用意することとします(SHALL)。