CA/ブラウザフォーラム

パブリック証明書の発行
および管理に関する基本要件v.1.1

2011 年 11 月 22 日採択、2012 年 7 月 1 日発効

（2012 年 9 月 14 日改訂）

パブリック証明書の発行および管理に関する基本要件、v. 1.0

バージョン 1.0 は、2012 年 9 月 14 日に改訂し CA/ブラウザフォーラムにより採択

本基本要件では、パブリック証明書の発行および管理に必要な（ただし必ずしも十分ではない）技術、プロトコル、身元確認、ライフサイクル管理、および監査要件について総合的に説明する。パブリック証明書とは、広く利用可能なアプリケーションソフトウェアにルート証明書が配付されているという事実によって信頼されている証明書のことである。本要件は、依拠当事者であるアプリケーションソフトウェアサプライヤによって採択および施行されるまでは、認証局にとって必須ではない。

読者の方へ

本バージョンの基本要件は、CA/ブラウザフォーラムにより制定され、パブリック証明書を発行、保守、および失効する際に認証局が使用する基準を示すものである。要件は、CA/ブラウザフォーラムが承認する手順に従い、適宜改訂される場合がある。本要件の主たる受益者はエンドユーザーであるため、推奨や提案については、CA/ブラウザフォーラム（questions@cabforum.org）にて電子メールで受け付けるものとする。フォーラムメンバーは、提供ソースに関係なくすべての情報を重視し、かかるすべての情報を真剣に検討する。

CA/ブラウザフォーラム

CA/ブラウザフォーラムは、認証局およびインターネットブラウザやその他の依拠当事者であるソフトウェアアプリケーションサプライヤで構成される非営利団体である。2012 年 9 月現在の会員は次のとおりである。

認証局

- Buypass AS
- Certum
- Chunghwa Telecom Co., Ltd.
- Comodo CA Ltd
- D-TRUST GmbH
- DigiCert, Inc.
- Digidentity BV
- E-TUGRA Inc.
- GlobalSign
- GoDaddy.com, Inc.
- Izenpe S.A.
- Japan Certification Services, Inc.
- Kamu Sertifikasyon Merkezi
- Keynectis
- KPN Corporate Market BV
- Logius PKIoverheid
- Network Solutions, LLC
- QuoVadis Ltd.
- SECOM Trust Systems CO., Ltd.
- Skaitmeninio sertifikavimo centras (SSC)
- StartCom Certification Authority
- Swisscom (Switzerland) Ltd
- SwissSign AG
- Symantec Corporation
- TrendMicro
- Trustis Limited
- Trustwave
- TWCA
- Wells Fargo Bank, N.A.

依拠当事者であるアプリケーションソフトウェアサプライヤ

- Apple
- Google Inc.
- Microsoft Corporation
- Opera Software ASA
- The Mozilla Foundation

本要件の作成に参加したその他のグループには、AICPA/CICA WebTrust for Certification Authorities タスクフォースや ETSI ESI が含まれる。ただし、これらのグループの参加が、最終成果物に対する当該グループによる支持、推奨、または承認を示唆するものではない。

目次

1. 適用範囲

『パブリック証明書の発行および管理に関する基本要件』では、パブリック証明書を発行するために認証局が満たさなければならない要件のサブセットについて説明する。別途明示的に規定されている場合を除き、本要件は発効日以降に発生する関連イベントにのみ適用される。

本要件は、パブリック証明書の発行および管理に関連するすべての事項が網羅されているものではない。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および新しい脅威に対応するために、要件を適宜更新する可能性がある。特に、将来のバージョンには、委譲された職務に関する、より正式で包括的な監査要件が含まれることが予定されている。

本バージョンは、インターネット経由で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み対応する。コードサイニング、S/MIME、タイムスタンプ処理、VoIP、IM、Web サービスなどに関する同様の要件については、今後のバージョンにて扱われる可能性がある。

本要件は、社内でのみ使用される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サプライヤからも配布されていない証明書の発行または管理については扱っていない。

2. 目的

本要件の主目的は、効率的で安全な電子通信を実現するとともに、証明書の信頼性に関するユーザーの懸念に対処することである。また、本要件は、ユーザーに情報を提供し、証明書に依拠する際に十分な情報に基づいた決定を下すことができるよう支援する。

3. 参照

ETSI Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – General Requirements and Guidance、
http://www.etsi.org/deliver/etsi_ts/119400_119499/119403/01.01.01_60/ts_119403v010101p.pdf で入手可能。

ETSI TS 102 042 V2.1.1, Electronic Signatures and Infrastructures（ESI）、公開鍵証明書を発行する認証局向けのポリシー要件。

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology、2001 年 5 月 25 日

ISO 21188:2006、金融サービス向けの公開鍵基盤 – 運用およびポリシーフレームワーク

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner、1997 年 3 月

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework、Chokhani 他、1999 年 3 月

RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers 他、1999 年 6 月

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework、Chokhani 他、2003 年 11 月

RFC4366, Request for Comments: 4366, Transport Layer Security（TLS）Extensions, Blake-Wilson 他、2006 年 4 月

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol （OCSP）Profile for High-Volume Environments, A. Deacon 他、2007 年 9 月

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and

Certificate Revocation List （CRL） Profile、Cooper 他、2008 年 5 月

WebTrust for Certification Authorities Version 2.0、
http://www.webtrust.org/homepagedocuments/item27839.aspx で入手可能

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

関連会社(Affiliate): 別の組織体を支配する、別の組織体によって支配される、または別の組織体と共通の支配権の下にある企業、共同経営会社、共同事業、またはその他の組織体、あるいは政府機関の直接的な支配権の下で運営されている機関、部署、下位行政機関、または任意の組織体。

申請者(Applicant): 証明書の申請（または更新要求）をする個人または法的組織体。証明書が発行されると、申請者は加入者と呼ばれるようになる。デバイスに対して発行される証明書については、デバイスが実際の証明書要求を送信する場合であっても、申請者は証明書で指定されているデバイスを管理または運用する組織体である。

申請権限者(Applicant Representative): 申請者である、申請者によって雇用されている、または申請者を代表するための明示的な権限を持ち、（i）申請者に代わって証明書要求に署名して提出する、または承認する、(ii) 申請者を代表して加入者契約に署名して提出する、または (iii) 申請者が CA の関連会社である場合に、申請者に代わって証明書利用規約を認め、同意する認定機関である個人または保証人。

アプリケーションソフトウェアサプライヤ(Application Software Supplier): 証明書を表示または使用し、ルート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であるアプリケーションソフトウェアのサプライヤ。

意見書(Attestation Letter): サブジェクト情報が会計士、弁護士、政府職員、またはかかる情報に対して習慣的に依拠するその他の信頼できる第三者機関によって記述された、サブジェクト情報が正しいものであることを証明する証書。

監査レポート(Audit Report): 当該組織体のプロセスおよび統制が、本要件の必須条項に従っているかどうかについての公認監査人の意見を述べた、公認監査人からのレポート。

証明書(Certificate): デジタル署名を使用して公開鍵と ID を結び付ける電子ドキュメント。

証明書データ(Certificate Data): CA の所有または管理下にある、または CA がアクセスすることができる、証明書要求およびそれに関連するデータ（申請者から取得したかどうかを問わない）。

証明書管理プロセス(Certificate Management Process): 鍵、ソフトウェア、およびハードウェアの使用と関連付けられるプロセス、運用、および手順。これらを使用して、CA は証明書データを検証し、証明書を発行し、リポジトリを保守し、証明書を失効させる。

証明書ポリシー(Certificate Policy): 共通のセキュリティ要件を持つ特定のコミュニティまたは PKI 実装に対する指定された証明書の利用可能性を示す規定集。

証明書問題レポート(Certificate Problem Report): 鍵の危殆化の疑い、証明書の不正使用、または証明書に関連するその他の種類の詐欺、危殆化、不正使用、あるいは不適切な行為の申し立て。

証明書失効リスト(Certificate Revocation List): 証明書を発行した CA によって作成され、デジタル署名された、失効した証明書のリスト。定期的に更新され、タイムスタンプが付けられる。

認証局(Certificate Authority または CA）: 証明書の作成、発行、失効、および管理の責任を担う組織。この用語はルート CA と下位 CA の両方に使われる。

認証局運用規定(Certificate Practice Statement): 証明書の作成、発行、管理、および使用の統

制枠組みを規定したドキュメントの 1 つ。

国(Country): 国連の加盟国、あるいは国連加盟国のうちの少なくとも 2 カ国が主権国家であると認める地理的地域。

クロス証明書(Cross Certificate): 2 つのルート CA 間の信頼関係を確立するために使用される証明書。

権限委譲先の第三者機関(Delegated Third Party): CA ではないが、本ドキュメントに定められた 1 つ以上の CA 要件を実施または履行し、証明書管理プロセスを支援することを CA によって承認されている個人または法人。

ドメイン利用権限ドキュメント(Domain Authorization Document): 特定のドメイン名空間に対する証明書を要求するための申請者の権限を証明する、ドメイン名登録機関、、あるいはドメイン名登録者として WHOIS に記載されている個人または組織体（プライベート、匿名、または代理登録サービスを含む）ドメイン名登録者によって提供されるドキュメント、またはこれらとの通信を記載した CA のドキュメント。

ドメイン名(Domain Name): ドメインネームシステムでノードに割り当てられるラベル。

ドメイン名前空間(Domain Namespace): ドメインネームシステム内の単一ノードに従属することが可能なすべてのドメイン名のセット。

ドメイン名登録者(Domain Name Registrant): ドメイン名の「所有者」を表すこともあるが、正確には、ドメイン名が使用される方法を管理する権利を有するとしてドメイン名登録機関で登録されている個人または組織体のこと。WHOIS またはドメイン名登録機関によって「登録者」として掲載されている個人または法人など。

ドメイン名登録機関(Domain Name Registrar): （i） Internet Corporation for Assigned Names and Numbers （ICANN）、（ii）全国的なドメインネーム機関/レジストリ、または（iii） Network Information Center （その関連会社、契約人、代理人、後継者、譲受人を含む）の指揮の下、または合意によって、ドメイン名を登録する個人または組織体。

発効日(Effective Date): 本要件は 2012 年 7 月 1 日から効力を発する。

エンタープライズ RA (Enterprise RA): CA から証明書の発行を承認され、関連会社でない組織の従業員または代理人。

有効期限日(Expiry Date): 証明書の有効期間の最終日を定義する、証明書内の「有効期間の終了」日付。

FQDN (Fully-Qualified Domain Name): インターネットドメインネームシステム内のすべての上位ノードのラベルを含むドメイン名。

政府機関(Government Entity): 政府が運営する法人、機関、部署、省庁、支部、または同様の構成要素、あるいはかかる国内の下位行政機関（州、市、郡など）

ハイリスク証明書要求(High Risk Certificate Request): CA が維持する内部の条件とデータベースの参照により、さらなる精査が必要であることを CA がフラグ付けする要求。これには、フィッシングおよびその他の詐欺的使用のリスクがさらに高い名前、以前に拒否された証明書要求または失効した証明書に含まれる名前、Miller Smiles フィッシングリストまたは Google Safe Browsing リストに記載されている名前、または CA が自身でリスク軽減のための基準を使用して識別した名前などが含まれる可能性がある。

内部サーバ名(Internal Server Name): パブリック DNS では解決できないサーバ名（未登録ドメイン名を含む場合もある）。

発行 CA (Issuing CA): 特定の証明書に関連して、証明書を発行した CA。これは、ルート CA または下位 CA の可能性がある。

鍵の危殆化(Key Compromise): 秘密鍵は、その値が権限のない人物に開示された、権限のない

人物がアクセスした、または権限のない人物がその値を検出することができる実用的な技法が存在する場合、危殆化したと考えられる。

鍵生成スクリプト(Key Generation Script): CA 鍵ペアの生成手順が記述された計画書。

鍵ペア(Key Pair): 秘密鍵とそれに関連付けられた公開鍵。

法人(Legal Entity): 当該国の法律制度に則った組織、企業、共同経営会社、事業体、トラスト、行政機関、またはその他の組織体。

オブジェクト識別子(Object Identifier): 特定のオブジェクトまたはオブジェクトクラスに該当する国際標準化機構（ISO）の標準に従って登録された一意の英数字または数字の識別子。

OCSP レスポンダ(OCSP Responder): CA の権限の下で運用され、証明書のステータス要求の処理のためにリポジトリに接続されているオンラインサーバ。「Online Certificate Status Protocol」も参照。

Online Certificate Status Protocol: 証明書依拠者であるアプリケーションソフトウェアによる特定の証明書のステータスを判断するために使用されるオンライン証明書確認プロトコル。「OCSP レスポンダ」も参照。

秘密鍵(Private Key): 鍵ペアの一方の鍵。所有者によって秘匿性が保たれ、デジタル署名を作成したり、対応する公開鍵を使用して暗号化された電子記録またはファイルを復号したりするために使用される。

公開鍵(Public Key): 鍵ペアの一方の鍵。対応する秘密鍵の所有者によって広く公開され、所有者の対応する秘密鍵を用いて作成されたデジタル署名を検証したり、メッセージを暗号化して所有者の対応する秘密鍵を用いてのみ復号できるようにしたりするために、依拠当事者によって使用される。

公開鍵基盤(Public Key Infrastructure): 公開鍵暗号方式に基づいて証明書および鍵の信頼できる作成、発行、管理、および使用を促進するために使用される、一連のハードウェア、ソフトウェア、人、手順、ルール、ポリシー、および義務。

パブリック証明書(Publicly-Trusted Certificate): 広く利用可能なアプリケーションソフトウェアにおいて対応するルート証明書が信頼されたルート証明機関として配布されている事実によって信頼されている証明書。

公認監査人(Qualified Auditor): セクション 17.6 （監査役の資格）の要件を満たす個人または法人。

登録ドメイン名(Registered Domain Name): ドメイン名登録機関で登録されているドメイン名。

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

信用できるデータソース(Reliable Data Source): 企業や政府で一般的に信頼性が高いと認識され、申請者の証明書取得以外の目的のために第三者が作成した、サブジェクト アイデンティティ情報の検証に使用する識別のためのドキュメントあるいはデータのソース。

信頼できる連絡手段(Reliable Method of Communication): 申請権限者以外の情報源を使用して確認された、郵便/宅配便の配送先住所、電話番号、電子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は、かかるサプライヤ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は、依拠当事者とは見なされない。

リポジトリ(Repository): 公開された PKI 管理ドキュメント（証明書ポリシーや認証局運用規定など）および証明書ステータス情報を、CRL または OCSP レスポンスの形で含むオンラインデータベース。

要件(Requirements): 本ドキュメント。

予約 IP アドレス(Reserved IP Address): IANA が予約済みとしている IPv4 または 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サプライヤからルート証明書が配布される最高位の認証局。下位 CA 証明書を発行する。

ルート証明書(Root Certificate): 自身を識別し、下位 CA に発効される証明書の検証を容易にするためにルート CA によって発行される自己署名証明書。

サブジェクト(Subject): 証明書において サブジェクト として識別されている個人、デバイス、システム、設備、または法人。サブジェクト は、加入者または加入者の管理および運用下にあるデバイスである。

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には、subjectAltName エクステンション または サブジェクト コモンネーム フィールドで指定されるドメイン名は含まれない。

下位 CA (Subordinate CA): その証明書がルート CA または別の下位 CA によって署名される認証局。

加入者(Subscriber): 証明書の発行先であり、加入者契約または利用規約によって法的に拘束される個人または法人。

加入者契約(Subscriber Agreement): CA と申請者/加入者との間で締結される、両当事者の権利と義務について規定した契約。

利用規約(Terms of Use): 申請者/加入者が CA の関連会社である場合、本要件に従って発行される証明書の保管および利用に関する規約。

信頼できるシステム(Trustworthy System): 侵入や不正使用から合理的に保護されており、合理的なレベルの可用性、信頼性、および正しい運用を提供し、意図される職務の履行に合理的に適しており、かつ適用されるセキュリティポリシーを施行するコンピュータハードウェア、ソフトウェア、および手順。

未登録ドメイン名(Unregistered Domain Name): 登録ドメイン名ではないドメイン名。

有効な証明書(Valid Certificate): RFC 5280 で規定されている検証手順に合格した証明書。

認証スペシャリスト(Validation Specialists): 本要件によって規定されている情報検証職責を果たす人物。

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): 証明書に含まれる サブジェクト の FQDN の左端にアスタリスク（*）を含む証明書。

5. 略語および頭字語

AICPA	American Institute of Certified Public Accountants （米国公認会計士協会）
CA	Certification Authority （認証局）
ccTLD	Country Code Top-Level Domain （国別コードトップレベルドメイン）

CICA	Canadian Institute of Chartered Accountants （カナダ公認会計士協会）
CP	Certificate Policy （証明書ポリシー）
CPS	Certification Practice Statement （認証局運用規定）
CRL	Certificate Revocation List （証明書失効リスト）
DBA	Doing Business As （事業名）
DNS	Domain Name System （ドメインネームシステム）
FIPS	Federal Information Processing Standard （米国政府連邦情報処理標準）
FQDN	Fully Qualified Domain Name （FQDN）
IM	Instant Messaging （インスタントメッセージング）
IANA	Internet Assigned Numbers Authority （インターネット番号割り当て機関）
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization （国際標準化機構）
NIST	（米国政府） National Institute of Standards and Technology （国立標準技術研究所）
OCSP	Online Certificate Status Protocol
OID	Object Identifier （オブジェクト識別子）
PKI	Public Key Infrastructure （公開鍵基盤）
RA	Registration Authority （登録局）
S/MIME	Secure MIME （Multipurpose Internet Mail Extensions）
SSL	Secure Sockets Layer
TLD	Top-Level Domain （トップレベルドメイン）
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol

6. 規約

本要件において定義されていない用語は、CA の該当する契約、ユーザーマニュアル、証明書ポリシー、および認証局運用規定で定義されている意味を持つものとする。

本要件に記載されているキーワード「MUST」、「MUST NOT」、「REQUIRED」、「SHALL」、「SHALL NOT」、「SHOULD」、「SHOULD NOT」、「RECOMMENDED」、「MAY」、および「OPTIONAL」は、RFC 2119 に従って解釈されるものとする。

7. 証明書の保証および表明

7.1 CA によるもの

証明書を発行することによって、CA は 7.1.1 に規定されている証明書の受益者にセクション 7.1.2 に規定されている証明書の保証を行うものとする。

7.1.1 証明書の受益者

証明書の受益者には、以下が含まれるが、これらに限定されない。

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. ルート CA が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。契約は、かかるアプリケーションソフトウェアサプライヤ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のものである。

3. 有効な証明書に合理的に依拠するすべての依拠当事者。

7.1.2 証明書の保証

CA は、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本要件およびその証明書ポリシーや認証局運用規定に従ってきたことを証明書の受益者に表明し、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、CA が、（i）申請者が、証明書の サブジェクト フィールドおよび subjectAltName エクステンション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持つ、またはこれらを管理していること（または、ドメイン名の場合のみ、かかる権利または管理がかかる使用または管理の権利を有する他の人物によって委譲されたこと）を検証するための手順を実装し、（ii）証明書を発行する際にその手順に従い、（iii）CA の証明書ポリシーや認証局運用規定にその手順を正確に記述したこと。

2. **証明書に対する承認**: 発行の時点で、CA が、（i） サブジェクト が証明書の発行を承認し、申請権限者が サブジェクト を代表して証明書を要求する権限を持っていることを確認するための手順を実装し、(ii) 証明書を発行する際にその手順に従い、(iii) CA の証明書ポリシーや認証局運用規定にその手順を正確に記述したこと。

3. **情報の正確性**: 発行の時点で、CA が、（i）証明書に含まれるすべての情報（サブジェクト:organizationalUnitName 属性を除く）の正確性を検証するための手順を実装し、(ii) 証明書を発行する際にその手順に従い、（iii） CA の証明書ポリシーや認証局運用規定にその手順を正確に記述したこと。

4. **誤解を招く情報の不存在**: 発行の時点で、CA が、（i）証明書の サブジェクト:organizationalUnitName 属性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実装し、（ii）証明書を発行する際にその手順に従い、（iii） CA の証明書ポリシーや認証局運用規定にその手順を正確に記述したこと。

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る場合、CA が、(i) セクション 9.2 および 11.2 に従って申請者のアイデンティティを検証するための手順を実装し、（ii）証明書を発行する際にその手順に従い、（iii）CA の証明書ポリシーや認証局運用規定にその手順を正確に記述したこと。

6. **加入者契約**: CA および加入者が関連会社でない場合、加入者および CA は、本要件を満たす法的に有効で施行可能な加入者契約の当事者であること、または CA および加入者が関連会社である場合、申請権限者が利用規約を認め、同意したこと。

7. **ステータス**: CA が、すべての有効期限内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含む 24 時間 365 日対応のパブリックにアクセス可能なリポジトリを保守していること。

8. **失効**: 本要件で規定されている事由が発生した場合、CA が証明書を失効すること。

7.2 申請者によるもの

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、申請者が本要件のセクション 10.3.2 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（SHALL）。

8. コミュニティおよび利用可能性

8.1 準拠

CA は、常に以下に準拠するものとする（SHALL）。

1. 業務を行うすべての管轄地においてその事業および発行する証明書に適用されるすべての法規に従って証明書を発行し、PKI を運用する。
2. 本要件に従う。
3. セクション 17 で規定されている監査要件に従う。
4. 業務を行う各管轄地において CA としての認可を受ける（証明書の発行に対して、該当管轄地の法令によって認可が必要な場合）。

本要件の対象となる活動に対して司法権を有する裁判所または政府機関が、本要件の必須要件の履行を違法と判決した場合、かかる要件は、その要件を有効かつ合法にするために必要な最小限の範囲において是正されると見なされる。これは、その管轄地の法律の対象となる運用または証明書発行にのみ適用される。関与する当事者は、CA/ブラウザフォーラムが本要件を適宜改訂できるよう、事実、状況、および関係する法について CA/ブラウザフォーラムに通知するものとする（SHALL）。

8.2 証明書ポリシー

8.2.1 実装

CA は、CA が本要件の最新バージョンをどのように実装するかを詳細に記述した証明書ポリシーや認証局運用規定を作成、実装、施行し、年に一度更新するものとする（SHALL）。

8.2.2 開示

CA は、証明書ポリシーや認証局運用規定を、24 時間 365 日利用可能な適切で容易にアクセスできるオンライン手段を通して公的に開示するものとする（SHALL）。CA は、CA が選択した監査スキーム（セクション 17.1 を参照）によって必要とされる範囲内で CA の実務を公に開示するものとする（SHALL）。開示には、RFC 2527 または RFC 3647 が要求するすべての資料を含めなければならず（MUST）、RFC 2527 または RFC 3647 に従って構成されなければならない（MUST）。

8.3 準拠のコミットメント

CA は、本要件を施行し、公開されている最新バージョンに準拠することを表明するものとする（SHALL）。CA は、本要件を証明書ポリシーや認証局運用規定に直接組み込む、または以下のような条項（本要件の公式バージョンへのリンクを含めなければならない（MUST））を参照することによって組み込むことにより、本要件を満たしてもよい（MAY）。

> ［CA の名称］は、http://www.cabforum.org に公開されている『パブリック証明書の発行および管理に関する基本要件』の最新バージョンに従うものとする。このドキュメントと要件の間に不一致が生ずる場合は、要件がこのドキュメントよりも優先される。

8.4 信頼モデル

CA は、CA が信頼関係（つまり未解決のクロス証明書）の確立について合意または同意したことを条件として、CA を サブジェクト として識別するすべての相互認証証明書を公開するものとする（SHALL）。

9. 証明書のコンテンツおよびプロファイル

9.1 発行者情報

発行 CA は、本要件の採択後に発行される各証明書の発行者フィールドを以下のサブセクションに従って設定するものとする（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: issuer:commonName （OID 2.5.4.3）

必須/任意: 任意

内容: 証明書に存在する場合、コモンネームフィールドには発行 CA を正確に識別する名前を含めなければならない（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: issuer:domainComponent （OID 0.9.2342.19200300.100.1.25）

必須/任意: 任意

内容: 証明書に存在する場合、ドメインコンポーネントフィールドには、発行 CA の登録ドメイン名のすべてのコンポーネントを、ドメイン名空間のルートに最も近い最後に記述されたコンポーネントから順番に含めなければならない（MUST）。

9.1.3 発行者組織名フィールド

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

必須/任意: 必須

内容: このフィールドには、CA を正確に識別するものであることを条件として、CA の名前（またはその略称）、商標、またはその他の意味のある識別子を含めなければならない（MUST）。このフィールドには、「Root」や「CA1」などの汎用的な指定を含めてはならない（MUST NOT）。

9.1.4 発行者国名フィールド

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

必須/任意: 必須

内容: このフィールドには、発行者の事業拠点がある国の 2 文字の ISO 3166-1 国別コードを含めなければならない（MUST）。

9.2 サブジェクト 情報

証明書を発行することにより、CA は、証明書ポリシーや認証局運用規定で規定された手順に従って、発効日現在で、すべての サブジェクト 情報が正確であることを確認したことを表明する。CA は、以下のセクション 9.2.1 および 9.2.2 に規定される場合を除き、サブジェクト属性にドメイン名を含めないものとする（SHALL NOT）。

9.2.1 Subject Alternative Name エクステンション

証明書フィールド: extensions:subjectAltName

必須/任意: 必須

内容: このエクステンションには、少なくとも 1 つのエントリを含めなければならない（MUST）。各エントリは、FQDN を含む dNSName、サーバの IP アドレスを含む iPAddress のいずれかでなければならない（MUST）。CA は、申請者が FQDN または IP アドレスを管理している、またはドメイン名登録者または IP アドレス譲受人から使用権利を付与されていることを確認しなければならない（MUST）。

ワイルドカード FQDN を使用できる。

本要件の発効日以降、予約 IP アドレスまたは内部サーバ名を含む subjectAlternativeName エクステンションまたは サブジェクト コモンネーム フィールドを備えた証明書を発行する前に、CA は、かかる証明書の使用を CA/ブラウザフォーラムでは推奨していないこと、およびその運用が 2016 年 10 月までに廃止されることを申請者に通知するものとする（SHALL）。また、発効日以降、CA は、予約 IP アドレスまたは内部サーバ名を含む subjectAlternativeName エクステンションまたは サブジェクト コモンネーム フィールドを備えた、有効期限日が 2015 年

11 月 1 日以降の証明書を発行しないものとする（SHALL NOT）。2016 年 10 月 1 日以降、CA は、subjectAlternativeName エクステンションまたは サブジェクト コモンネーム フィールドに予約 IP アドレスまたは内部サーバ名が含まれている、すべての有効期限内の証明書を失効するものとする（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: subject:commonName （OID 2.5.4.3）

必須/任意: 廃止予定（推奨されないが、禁止されてはいない）

内容: 存在する場合、このフィールドには、証明書の subjectAltName エクステンション（セクション 9.2.1 を参照）に含まれている値のいずれかである単一の IP アドレスまたは FQDN を含めなければならない（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: subject:domainComponent （OID 0.9.2342.19200300.100.1.25）

必須/任意: 任意

内容: 存在する場合、このフィールドには、サブジェクト の登録ドメイン名のすべてのコンポーネントを、ドメイン名空間のルートに最も近い最も重要なコンポーネントを最後に記述するという順序で含めなければならない（MUST）。

9.2.4 サブジェクト 識別名フィールド

a. **証明書フィールド**: subject:organizationName （OID 2.5.4.10）

   任意。

   内容: 存在する場合、subject:organizationName フィールドには、セクション 11.2 で検証したサブジェクト名または DBA を含めなければならない（MUST）。一般的なばらつきや略称などの検証した名前とは多少異なる情報については、CA がその違いや略称がその地域で受け入れられている略称であることを文書化している場合には、このフィールドに含めてもよい。たとえば、公認記録が「Company Name Incorporated」の場合、CA は「Company Name, Inc.」または「Company Name」を使用してもよい（MAY）。個人名のサブジェクト属性（givenName （2.5.4.42）、surname （2.5.4.4）など）はアプリケーションソフトウェアによって広範にサポートされていないため、CA は、個人のサブジェクト名または DBA を伝達するために subject:organizationName フィールドを使用してもよい（MAY）。

b. **証明書フィールド**: subject:streetAddress （OID: 2.5.4.9）

   任意（subject:organizationName フィールドが存在する場合）。

   禁止（subject:organizationName フィールドが存在しない場合）。

   内容: 存在する場合は、subject:streetAddress フィールドにはセクション 11.2 で検証したサブジェクトの所在地住所情報を含めなければならない（MUST）。

c. **証明書フィールド**: subject:localityAddress （OID: 2.5.4.7）

   必須（subject:organizationName フィールドが存在し、かつ subject:stateOrProvinceName フィールドが存在しない場合）。

   任意（subject:organizationName フィールドおよび subject:stateOrProvinceName フィールドが存在する場合）。

   禁止（subject:organizationName フィールドが存在しない場合）。

   内容: 存在する場合は、subject:localityName フィールドにはセクション 11.2 で検証したサブジェクトの地域情報を含めなければならない（MUST）。subject:countryName フィールドがセクション 9.2.5 に従って ISO 3166-1 のユーザー割り当ての XX コー

ドを指定する場合、localityName フィールドにはセクション 11.2 で検証したサブジェクトの地域や都道府県の情報を含めてもよい（MAY）。

d. **証明書フィールド**: subject:stateOrProvinceName （OID: 2.5.4.8）

必須（subject:organizationName フィールドが存在し、かつ subject:localityName フィールドが存在しない場合）。

任意（subject:organizationName フィールドおよび subject:localityName フィールドが存在する場合）。

禁止（subject:organizationName フィールドが存在しない場合）。

内容: 存在する場合は、subject:stateOrProvinceName フィールドにはセクション 11.2 で検証したサブジェクトの都道府県情報を含めなければならない（MUST）。subject:countryName フィールドがセクション 9.2.5 に従って ISO 3166-1 のユーザー割り当ての XX コードを指定する場合、subject:stateOrProvinceName フィールドにはセクション 11.2.5 で検証したサブジェクトの国情報のフルネームを含めてもよい（MAY）。

e. **証明書フィールド**: subject:postalCode （OID: 2.5.4.17）

任意（subject:organizationName フィールドが存在する場合）。

禁止（subject:organizationName フィールドが存在しない場合）。

内容: 存在する場合は、subject:postalCode field フィールドにはセクション 11.2 で検証したサブジェクトの郵便番号情報を含めなければならない（MUST）。

9.2.5 サブジェクト 国名フィールド

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

必須（subject:organizationName フィールドが存在する場合）。

任意（subject:organizationName フィールドが存在しない場合）。

内容: subject:organizationName フィールドが存在する場合、subject:countryName にはセクション 11.2 で検証したサブジェクトの場所に関連付けられた 2 文字の ISO 3166-1 国別コードを含めなければならない（MUST）。subject:organizationName フィールドが存在しない場合、subject:countryName フィールドにはセクション 11.2.5 に従って検証したサブジェクトに関連付けられる 2 文字の ISO 3166-1 国別コードを含めてもよい（MAY）。国が公式の ISO 3166-1 国別コードで表せない場合、CA は ISO 3166-1 ユーザー割り当てコードの XX を指定してもよい（MAY）。これは、公式の ISO 3166-1 alpha-2 コードが割り当てられていないことを示す。

9.2.6 サブジェクト 組織ユニットフィールド

証明書フィールド: subject:organizationalUnitName

任意。

CA は、OU 属性に名前、DBA、商号、商標、アドレス、場所、または特定の個人や法人を表すその他のテキストが含まれるのを防止するプロセスを実装するものとする（SHALL）。ただし、CA がセクション 11.2 に従ってこの情報を検証済みであり、証明書にも同じくセクション 11.2 に従って検証済みの subject:organizationName、subject:localityName、および subject:countryName 属性が含まれている場合を除く。

9.2.7 サブジェクトのその他の属性

その他のすべての任意の属性は、サブジェクト フィールド内に存在する場合、CA によって検証済みの情報を含めなければならない（MUST）。任意の属性には、「.」、「-」、「 」（空白）文字などのメタデータや、値が存在しない、不完全である、または適用不可であることを示すものを含めてはならない（MUST NOT）。

9.3 証明書ポリシーの識別

このセクションでは、証明書ポリシーの識別に関して、ルート CA、下位 CA、および加入者の証明書の内容要件について説明する。

9.3.1 予約された証明書ポリシー識別子

以下の証明書ポリシー識別子は、本要件への準拠を表明するためのオプションの手段として CA が使用するために予約されている。

> {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）、証明書が本要件に準拠するが、セクション 11.2 に従って検証された サブジェクト アイデンティティ情報が含まれていない場合。

証明書が 2.23.140.1.2.1 のポリシー識別子を使う場合、organizationName、streetAddress、localityName、stateOrProvinceName、または postalCode を サブジェクト フィールドに含めてはならない（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）、証明書が本要件に準拠し、セクション 11.2 に従って検証された 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。

証明書が 2.23.140.1.2.2 のポリシー識別子を表明する場合、organizationName、localityName、stateOrProvinceName（該当する場合）、および countryName を サブジェクト フィールドに含めなければならない（MUST）。

9.3.2 ルート CA 証明書

ルート CA 証明書には、certificatePolicies エクステンションを含めるべきではない（SHOULD NOT）。

9.3.3 下位 CA 証明書

発行 CA の関連会社ではない下位 CA に、発効日以降に発行された証明書は、以下に準拠するものとする。

1. 下位 CA の本要件への準拠を示す 1 つ以上の明示的なポリシー識別子（つまり、CA/ブラウザフォーラム予約識別子または CA が認証ポリシーや認証局運用規定で定義した識別子）を含めなければならない（MUST）、および
2. 「anyPolicy」識別子（2.5.29.32.0）を含めてはならない（MUST NOT）。

発行 CA の関連会社である下位 CA に、発効日以降に発行された証明書は、以下に準拠するものとする。

1. 本要件への下位 CA の準拠を示すために、CA/ブラウザフォーラムの予約識別子または CA が証明書ポリシーや認証局運用規定で定義した識別子を含めてもよい（MAY）、および
2. 明示的なポリシー識別子の代わりに「anyPolicy」識別子（2.5.29.32.0）を含めてもよい（MAY）。

下位 CA は、証明書ポリシーや認証局運用規定で、本要件への準拠を示すポリシー識別子が含まれているすべての証明書が本要件に従って発行および管理されることを表明するものとする（SHALL）。

9.3.4 加入者証明書

加入者に発行される証明書は、certificatePolicies エクステンションに、発行 CA によって定義された本要件への準拠を示す 1 つ以上のポリシー識別子を含まなければならない（MUST）。

また、本要件に準拠する CA は、かかる証明書で予約されたポリシー OID のいずれかを設定してもよい（MAY）。

発行 CA は、証明書ポリシーまたは認証局運用規定に、指定されたポリシー識別子を含めて発行する証明書が本要件に従って管理されることを文書化するものとする（SHALL）。

9.4 有効期間

発効日以降に発行される証明書には、60 カ月以下の有効期間を設けなければならない（MUST）。

以下に規定される内容を除き、2015 年 4 月 1 日以降に発行される証明書には、39 カ月以下の有効期間を設けなければならない（MUST）。

2015 年 4 月 1 日以降、CA は、有効期間が 39 カ月を超えるが 60 カ月を超えない証明書を引き続き発行してもよい（MAY）。ただし、証明書が以下のようなシステムまたはソフトウェア用であることを CA が文書化することを条件とする。

（a） 発効日よりも前に使用していた。

（b） 申請者または多数の依拠当事者によって現在使用されている。

（c） 有効期間が 60 カ月未満の場合、運用できない。

（d） 依拠当事者に対する既知のセキュリティリスクを含んでいない。および

（e） 多額の経済的支出なしではパッチ適用または交換が難しい。

9.5 加入者公開鍵

CA は、要求された公開鍵が付録 A に規定されている要件を満たさない場合、または既知の脆弱な秘密鍵である（Debian の脆弱鍵など。http://wiki.debian.org/SSLkeys を参照）場合、証明書要求を拒否するものとする（SHALL）。

9.6 証明書シリアルナンバー

CA は、少なくとも 20 ビットのエントロピーを表す、非連続の証明書シリアルナンバーを生成すべきである（SHOULD）。

9.7 その他の技術要件

CA は、「付録 A - 暗号化アルゴリズムおよび鍵要件」、「付録 B - 証明書エクステンション」、および「付録 C – ユーザーエージェント検証」に規定されている技術要件を満たすものとする（SHALL）。

10. 証明書申請

10.1 ドキュメント要件

証明書の発行前に、CA は、申請者から以下のドキュメントを取得するものとする（SHALL）。

1. 証明書要求（電子媒体による取得でもよい）、および
2. 署名された加入者契約または利用規約（電子媒体による取得でもよい）

CA は、本要件を満たすために必要であると CA が判断するその他のドキュメントをすべて取得すべきである（SHOULD）。

10.2 証明書要求

10.2.1 概要

証明書の発行前に、CA は、CA が指定する形式であり、本要件に準拠する証明書要求を申請者から取得するものとする（SHALL）。セクション 11.3 の有効期間および更新要件に従い、同じ

申請者に発行される複数の証明書に 1 つの証明書要求で対応してもよい（MAY）。ただし、各証明書が、申請者を代表する適切な申請権限者によって署名された有効な最新の証明書要求によってサポートされていることを条件とする。証明書要求は、電子的に作成、送信、または署名してもよい（MAY）。

10.2.2 要求および証明

証明書要求には、証明書の発行申請者から、または申請者の代理人からの要求、および申請者から、または申請者の代理人による、要求に含まれるすべての情報が正しいことの証明が含まれていなければならない（MUST）。

10.2.3 情報要件

証明書要求には、証明書に含まれる申請者に関するすべての事実情報、および CA が本要件および 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（MAY）。証明書要求が申請者に関する必要な情報の一部を含んでいない場合、CA は、残りの情報を申請者から取得する、または信頼できる独立した第三者機関のデータソースから情報を取得して申請者に確認するものとする（SHALL）。

申請者情報には、証明書の subjectAltName エクステンションに含まれる FQDN または IP アドレスを少なくとも 1 つ含めなければならない（MUST）が、これに限定されるものではない。

10.2.4 加入者秘密鍵

加入者以外の当事者は、加入者秘密鍵をアーカイブしないものとする（SHALL NOT）。

CA またはその指定された RA は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前に秘密鍵を暗号化するものとする（SHALL）。

CA またはその指定された RA が加入者の秘密鍵が加入者と関連会社でない、権限を持たない個人または組織に伝達されたことを認識した場合、CA は、伝達された秘密鍵に対応する公開鍵を含むすべての証明書を失効するものとする（SHALL）。

10.3 加入者契約および利用規約

10.3.1 概要

証明書の発行前に、CA は、CA および証明書の受益者の明示的な利益のために、以下のいずれかを取得するものとする（SHALL）。

1. CA との加入者契約に対する申請者の合意、または
2. 利用規約に対する申請者の合意

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（SHALL）。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適用しなければならない（MUST）。CA は、電子媒体による契約または「クリックスルー」契約を使用してもよい（MAY）。ただし、CA がかかる契約が法的強制力を持つと断定していることを条件とする。証明書要求ごとに別の契約を使用してもよい（MAY）。または、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のために単一の契約を使用してもよい（MAY）。ただし、CA が申請者に発行する各証明書が明確にその加入者契約または利用規約の対象となっていることを条件とする。

10.3.2 契約要件

加入者契約または利用規約には、申請者自身（または申請者によって本人の代理であると指定された人物または請負あるいはホスティングサービス関係にある代理業者）に以下の義務および保証を課す条項が含まれていなければならない（MUST）。

1. **情報の正確性**: 証明書要求において、および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、CA に常に正確で完全な情報を提供する義務および保証。

2. **秘密鍵の保護**:証明書（およびパスワードやトークンなど、関連付けられたすべてのアクティベーションデータまたはデバイス）に含まれる公開鍵に対応する秘密鍵を、単独で管理し、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ことに関する、申請者の義務および保証。
3. **証明書の受理**: 加入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**: 証明書を証明書に記載されている subjectAltName でアクセス可能なサーバにのみインストールし、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**: （a）証明書の情報が不適当または不正確である、あるいは不適当または不正確になる場合、または（b）証明書に含まれている公開鍵に関連付けられた加入者の秘密鍵の不正使用または危殆化が実際に発生している、あるいは疑われる場合、証明書およびその関連付けられた秘密鍵の使用を直ちに中止し、速やかに CA に証明書の失効を要求する義務およびその保証。
6. **証明書の使用の終了**: 鍵の危殆化を理由とする証明書の失効時に証明書に含まれる公開鍵に対応する秘密鍵のすべての使用を速やかに中止する義務およびその保証。
7. **対応**: 指定された期間内の鍵の危殆化または証明書の不正使用に関する CA からの指示に対応する義務。
8. **確認および同意**: 申請者が加入者契約または利用規約の条項に違反した場合、または CA が証明書がフィッシング攻撃、詐欺、マルウェアの配付などの犯罪行為を可能にするために使用されていることを発見した場合、CA には証明書を直ちに失効する権利があることに対する確認および同意。

11. 認証の実行

11.1 利用権限の確認

11.1.1 ドメイン名登録者による利用権限の確認

証明書に記載された各 FQDN に対して、CA は証明書が発行された日付時点で、申請者がドメイン名登録者である、または FQDN を管理している人物であることを、以下を行うことにより確認するものとする（SHALL）。

1. ドメイン名登録機関に申請者がドメイン名登録者であることを直接確認する。
2. ドメイン名登録機関が提供する住所、電子メールアドレス、電話番号を使用してドメイン名登録者に直接連絡する。
3. WHOIS レコードの「registrant」、「technical」、または「administrative」フィールドに記載されている連絡先情報を使用してドメイン名登録者に直接連絡する。
4. 先頭のローカル部分を「admin」、「administrator」、「webmaster」、「hostmaster」、または「postmaster」とし、次にアットマーク（「@」）、さらにドメイン名（要求される FQDN から 0 個以上のコンポーネントを取り除いて作成）を追加して作成した電子メールアドレスを使用してドメインの管理者に連絡する。
5. ドメイン利用権限ドキュメントに依拠する。
6. FQDN を含む URI により識別されるオンライン Web ページの情報を同意の上で変更することで、申請者が FQDN を実際に管理していることを実演させる。あるいは、
7. その他の確認方法を利用する。ただし、CA はこの確認方法が前述の方法と同程度のレベルで、申請者がドメイン登録者である、または FQDN を管理する人物であることを確認できるという証拠を文書化した形で維持していること。

注記: 適切なドメイン名レベルまたはドメイン名空間を判断するために、登録可能なドメイン名は .com、.net、.org などのような汎用トップレベルドメイン（gTLD）のセカンドレベルドメインである。また FQDN が 2 文字の国別コードのトップレベルドメイン（ccTLD）を含む場合、ccTLD のルールに従って登録が可能なものがすべてドメインレベルとなる。

CA が申請者の FQDN に対する管理を確認するためにドメイン利用権限ドキュメントに依拠する場合、このドメイン利用権限ドキュメントは、WHOIS に記載されたドメイン名登録者（プライベート、匿名、または代理登録サービスを含む）またはドメイン名登録機関と連絡したことを立証しなければならない（MUST）。CA はドメイン利用権限ドキュメントが（i）証明書要求日またはそれ以降の日付に作成された、または（ii）以前に発行された証明書を検証するために CA が使用したことを確認し、さらに前回の証明書発行以降、ドメイン名の WHOIS レコードが修正されていないことを確認しなければならない（MUST）。

11.1.2 IP アドレスの利用権限の確認

証明書に記載された各 IP アドレスに対して、CA は証明書が発行された日付時点で申請者が IP アドレスを管理することを、以下を行うことにより確認するものとする（SHALL）。

1. IP アドレスを含む URI により識別されるオンライン Web ページの情報を同意の上で変更することで、申請者が IP アドレスを実際に管理していることを実演させる。
2. インターネット番号割り当て機関（IANA）、または地域インターネットレジストリ（RIPE、APNIC、ARIN、AfriNIC、LACNIC）からの IP アドレス割り当てのドキュメントを取得する。
3. IP アドレスの逆引きを行い、次にその結果のドメイン名に対する管理をセクション 11.1.1 に基づいて検証する。あるいは、
4. その他の確認方法を利用する。ただし、CA はこの確認方法が前述の方法と同程度のレベルで、申請者が IP アドレスを管理することを確認できるという証拠を文書化した形で維持していること。

11.2 サブジェクトアイデンティティ情報の認証

申請者が countryName フィールドのみで構成されている 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、CA は、セクション 11.2.5 の要件を満たし、CA の証明書ポリシーまたは認証局運用規定に記載されている認証プロセスを使用して、サブジェクト と関連付けられている国を認証するものとする（SHALL）。申請者が countryName フィールドおよびその他の 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、CA は、セクション 11.2 の要件を満たし、CA の証明書ポリシーまたは認証局運用規定に記載されている認証プロセスを使用して、申請者、および申請権限者の証明書要求の真正性を認証するものとする（SHALL）。CA は、本セクションに基づいて依拠されるドキュメントに修正や改ざんがないかどうか調べるものとする（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の名前または住所が含まれる場合、CA は、組織のアイデンティティおよび住所、および住所が申請者が存在する、または事業を行っている住所であることを認証するものとする（SHALL）。CA は、以下の少なくとも 1 つが提供する、または以下の少なくとも 1 つと連絡を取ることによって得られるドキュメントを使用して申請者のアイデンティティと住所を認証するものとする（SHALL）。

1. 申請者が法的に設立、存在、または承認されているの管轄地にある政府機関
2. 定期的に更新され、信用できるデータソースと見なされる第三者機関データベース
3. CA または CA の代理人を務める第三者機関によるサイト訪問、または
4. 意見書

CA は、上記の 1 から 4 に記載されているのと同じドキュメントまたは連絡方法を使用して、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（MAY）。

または、CA は、公共料金請求書、銀行取引明細書、クレジットカード請求書、政府発行の税務書類、または CA が信頼性が高いと判断するその他の識別方法を使用して、申請者の住所を検証してもよい（MAY）（ただし、申請者のアイデンティティの検証には使用できない）。

11.2.2 商号/屋号

サブジェクト アイデンティティ情報に 商号 または屋号が含まれる場合、CA は、以下の少なくとも 1 つを使用して、商号/屋号を使用するための申請者の権利を検証するものとする（SHALL）。

1. 申請者の法的な設立、存在、または認識の管轄地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連絡
2. 信用できるデータソース
3. かかる 商号 または屋号の管理を担当する政府機関との連絡
4. ドキュメントが添付された意見書、または
5. 公共料金請求書、銀行取引明細書、クレジットカード請求書、政府発行の税務書類、または CA が信頼性が高いと判断するその他の識別形式

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、信頼できる連絡手段を使用して、申請権限者の証明書要求の真正性を検証するものとする（SHALL）。

CA は、信頼できる連絡手段を検証するために、セクション 11.2 に記載されているソースを使用してもよい（MAY）。CA が信頼できる連絡手段を使用することを条件として、CA は、申請権限者または申請者の組織（申請者の主なビジネスオフィス、本社オフィス、人事オフィス、IT オフィス、または CA が適切と見なすその他の部門）内の信頼できるソースとの間で直接、証明書要求の真正性を確認してもよい（MAY）。

さらに、CA は、申請者が証明書を要求できる個人を指定するためのプロセスを確立するものとする（SHALL）。申請者が書面にて証明書を要求できる個人を指定する場合、CA は、この指定以外での証明書要求を受け入れないものとする（SHALL NOT）。CA は、申請者の検証済みの書面による要求に応じて、承認された証明書要求者のリストを申請者に提供するものとする（SHALL）。

11.2.4 個人の申請者の検証

本セクション 11.2 に従う申請者が個人の場合、CA は、申請者の氏名、申請者の住所、および証明書要求の真正性を検証するものとする（SHALL）。

CA は、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のフォト ID（パスポート、運転免許証、ミリタリー ID、または同等のドキュメント）の判読可能なコピーを使用して、申請者の氏名を検証するものとする（SHALL）。CA は、コピーに修正や改ざんがないかどうか調べるものとする（SHALL）。

CA は、政府により発行された ID、公共料金請求書、銀行取引明細書、クレジットカード請求書など、 CA が信頼性が高いと判断する識別方法を使用して申請者の住所を検証するものとする（SHALL）。CA は、申請者の氏名を検証するために使用した同じ政府発行の ID に依拠してもよい（MAY）

CA は、信頼できる連絡手段を使用して申請者と証明書要求を検証するものとする（SHALL）。

11.2.5 国の検証

サブジェクト:countryName フィールドが存在する場合、CA は、次のいずれかを使用して サブ

ジェクト と関連付けられた国を検証するものとする（SHALL）。(a)（i） Web サイトの DNS レコードで示されている Web サイトの IP アドレスまたは（ii）申請者の IP アドレスに対する国による IP アドレス範囲割り当て、（b）要求されたドメイン名の ccTLD、（c）ドメイン名登録者によって提供された情報、または（d）セクション 11.2.1 に記載されている方法。 CA は、申請者の実際の拠点以外の国で割り当てられた IP アドレスへの依拠を防ぐために、プロキシ サーバを審査するプロセスを実装すべきである（SHOULD）。

11.3 証明書データの有効期間

セクション 9.4 では、加入者証明書の有効期間を制限している。CA は、証明書の発行前 39 カ月以内にセクション 11 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した場合、証明書情報の検証にそのデータまたはドキュメントを使用してもよい（MAY）。

11.4 拒否リスト

セクション 15.3.2 に従い、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をすべて含む内部データベースを保持するものとする（SHALL）。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（SHALL）。

11.5 ハイリスク要求

CA は、証明書承認の前にハイリスクの証明書要求を識別し、かかる要求が本要件に従って適切に検証されたことを確認するために、追加の検証活動を求める文書化された手順を、開発、保守、実施するものとする（SHALL）。

11.6 データソースの正確性

データソースを信用できるデータソースとして使用する前に、CA はデータソースの信頼性、正確性、および修正や改ざんに対する抵抗力を評価するものとする（SHALL）。CA は評価中に以下を考慮すべきである（SHOULD）。

1. 提供される情報の有効期間
2. 情報源の更新頻度
3. データの提供者とデータ収集の目的
4. 一般の人々がデータにアクセスできる可能性、かつ
5. データの修正や改ざんの相対的な難しさ

CA や所有者、あるいは関連会社が保守するデータベースは、その主要な目的がセクション 11 に基づく検証要件を満たすための情報収集である場合、信用できるデータソースとして使用できない。

12. ルート CA による証明書発行

ルート CA による証明書発行では、ルート CA が証明書への署名操作を実行するために直接コマンドを慎重に発行する、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、システム責任者、または PKI 管理者）が必要となる。

以下の場合を除き、証明書に署名するためにルート CA 秘密鍵を使用してはならない（MUST NOT）。

1. ルート CA 自体を表すための自己署名証明書
2. 下位 CA 用の証明書およびクロス証明書
3. インフラストラクチャ目的の証明書（管理者証明書、内部 CA 運用機器用証明書、OCSP レスポンス検証証明書など）

4. ルート CA によって発行された証明書で製品をテストすることのみを目的として発行される証明書
5. 加入者証明書。ただし、以下を条件とする。
    a. ルート CA が発効日よりも前に作成された 1024-bit RSA 署名鍵を使用する
    b. 申請者のアプリケーションが発効日よりも前に導入されていた
    c. 申請者のアプリケーションが申請者によってアクティブに使用されている、または CA が文書化されたプロセスを使用して、証明書の使用が多数の依拠当事者によって必要であることを立証する。
    d. CA が、文書化されたプロセスに従い、申請者のアプリケーションが依拠当事者に対して既知のセキュリティリスクをもたらさないと判断する。および
    e. CA が、申請者のアプリケーションが多額の経済的支出なしではパッチ適用または交換できないことを文書化する

13. 証明書失効およびステータスチェック

13.1 失効

13.1.1 失効要求

CA は、加入者が自身の証明書の失効を要求するためのプロセスを提供するものとする（SHALL）。そのプロセスは、CA の証明書ポリシーや認証局運用規定に記述しなければならない（MUST）。CA は、失効要求を受け入れ、関連する問い合わせに対応する機能を 24 時間 365 日体制で維持するものとする（SHALL）。

13.1.2 証明書問題レポート

CA は、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、およびその他の第三者機関に、秘密鍵の危殆化の疑い、証明書の不正使用、またはその他の種類の詐欺、危殆化、不正使用、不適切な実施、あるいは証明書に関連するその他の問題を報告するための明確な指示を与えるものとする（SHALL）。CA は、容易にアクセス可能なオンライン手段を通してその指示を公開するものとする（SHALL）。

13.1.3 調査

CA は、証明書問題レポートに関する調査を受領から 24 時間以内に開始し、少なくとも以下の条件に基づいて、失効またはその他の適切なアクションを行うかどうかを決定するものとする（SHALL）。

1. 申し立てられた問題の性質
2. 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
3. 苦情を申し立てている組織体（たとえば、Web サイトが違法な活動に関与しているという捜査当局からの苦情は、注文した商品が届かなかったと申し立てる消費者からの苦情よりも重要視されるべきである）
4. 関連法規

13.1.4 レスポンス

CA は、高優先度の証明書問題レポートに内部で対応し、適宜、かかる苦情を捜査当局に転送したり、かかる苦情の対象である証明書を失効するための機能を 24 時間 365 日体制で維持するものとする（SHALL）。

13.1.5 失効理由

CA は、以下が 1 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する（SHALL）。

1. 加入者が CA による証明書の失効を書面で要求した。
2. 加入者が、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 CA に通知した。
3. CA が、加入者の秘密鍵（証明書の公開鍵に対応）が鍵の危殆化に遭っている、または証明書がそれ以外の方法で不正使用されているという証拠を入手した（セクション 10.2.4 も参照）
4. CA が、加入者が加入者契約または利用規約に基づく 1 つ以上の重要な義務に違反したことを知った
5. CA が、証明書での FQDN または IP アドレスの使用が合法的に許可されたものではなくなっていることを示す状況を知った（たとえば、裁判所または仲裁人がドメイン名登録者のドメイン名使用権利を失効化した、ドメイン名登録者と申請者との間の関連ライセンスまたはサービスが解除された、またはドメイン名登録者がドメイン名を更新しなかった、など）
6. CA が、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知った
7. CA が、証明書に含まれている情報の重大な変更を知った
8. CA が、証明書が本要件または CA の証明書ポリシーや認証局運用規定に従って発行されなかったことを知った
9. CA が、証明書に表示されている情報が不正確または誤解を招く恐れがあると判断した
10. CA が何らかの理由で運用を中止し、別の CA が証明書の失効サポートを提供するように手配していない。
11. 本要件に基づいて証明書を発行するための CA の権利が失効、廃止、終了されている（CA が CRL/OCSP リポジトリの維持を継続するための手配を行っている場合を除く）。
12. CA が、証明書の発行に使用される下位 CA の秘密鍵の危殆化の可能性を知った。
13. CA の証明書ポリシーや認証局運用規定によって失効が必要になった。または
14. 証明書の技術的内容または形式が、アプリケーションソフトウェアまたは依拠当事者に容認できないリスクを与えている（たとえば、CA/ブラウザフォーラムは、廃止予定の暗号化/署名アルゴリズムまたは鍵サイズが容認できないリスクを与えており、かかる証明書が一定の期間内に CA によって失効および差し替えられるべきであると判断する場合がある）。

13.2 証明書ステータスチェック

13.2.1 メカニズム

CA は、付録 B に従って、下位証明書および加入者証明書の失効情報を利用可能にするものとする（SHALL）。

加入者証明書が高トラフィック FQDN 用の場合、CA は、［RFC4366］に従って、OCSP ステイプリングを使って、OCSP レスポンスを配付してもよい（MAY）。この場合、CA は、加入者が TLS ハンドシェーク内に証明書の OCSP レスポンスを「ステイプル」することを保証するものとする（SHALL）。CA は、契約によって、加入者契約または利用規約を通して、あるいは CA によって実装される技術レビュー手段によって、加入者に対してこの要件を施行するものとする（SHALL）。

13.2.2 リポジトリ

CA は、アプリケーションソフトウェアが、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（SHALL）。

加入者証明書のステータスの場合:

1. CA が CRL を公開する場合、CA は、少なくとも 7 日に一度 CRL を更新および再発行するものとし（SHALL）、nextUpdate フィールドの値は thisUpdate フィールドの値から 10 日を超えてはならない（MUST NOT）。
2. CA は、少なくとも 4 日ごとに OCSP 経由で提供される情報を更新するものとする（SHALL）。このサービスからの OCSP レスポンスは、最大で 10 日の有効期間を持たなければならない（MUST）。

下位 CA 証明書のステータスの場合:

1. CA は、少なくとも（i） 12 カ月ごとに一度、および（ii）下位 CA 証明書の失効から 24 時間以内に、CRL を更新および再発行するものとし（SHALL）、nextUpdate フィールドの値は thisUpdate フィールドの値から 12 カ月を超えてはならない（MUST NOT）。
2. CA は、少なくとも（i） 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、OCSP 経由で提供される情報を更新するものとする（SHALL）。

2013 年 1 月 1 日から、CA は、本要件に従って発行された証明書に関して GET メソッドを使用した OCSP 機能をサポートするものとする（SHALL）。

13.2.3 レスポンス時間

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（SHALL）。

13.2.4 エントリの削除

CRL または OCSP レスポンスの失効エントリは、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（MUST NOT）。

13.2.5 OCSP 署名

OCSP レスポンスは、RFC2560 や RFC5019 に従わなければならない（MUST）。OCSP レスポンスは以下のいずれかに準拠しなければならない（MUST）。

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 レスポンダによって署名されている。

後者の場合、OCSP 署名証明書には、RFC2560 に定義されている、タイプ id-pkix-ocsp-nochek のエクステンションが含まれていなければならない（MUST）。

13.2.6 未発行の証明書に対するレスポンス

OCSP レスポンダは、発行されていない証明書のステータス要求を受け取った場合、「Good」のステータスで応答すべきではない（SHOULD NOT）。CA はセキュリティレスポンス手順の一部として、このような要求に対してレスポンダを監視すべきである（SHOULD）。

2013 年 8 月 1 日以降、OCSP レスポンダはこのような証明書に対して「Good」のステータスで応答してはならない（MUST NOT）。

14. 従業員および第三者機関

14.1 信頼性および能力

14.1.1 本人確認および身元審査

CA の従業員、代理人、または契約社員であれ、個人を証明書管理プロセスに関与させる前に、CA は、かかる個人の本人確認および身元審査を行うものとする（SHALL）。

14.1.2 トレーニングおよびスキルレベル

CA は、情報検証職務を履行するすべての担当者に、公開鍵基盤の基本知識、認証ポリシーおよび手順（CA の証明書ポリシーや認証局運用規定を含む）、情報検証プロセスに対する一般的な脅威（フィッシングやその他のソーシャルエンジニアリング戦術を含む）、および本要件について取り上げたスキルトレーニングを提供するものとする（SHALL）。

CA は、かかるトレーニングの記録を維持し、認証スペシャリスト職務を委託されている担当者が、かかる職務を十分に履行できるためのスキルレベルを維持していることを確認するものとする（SHALL）。

証明書発行に従事する認証スペシャリストは、CA のトレーニングおよびパフォーマンスプログラムと一致したスキルレベルを維持するものとする（SHALL）。

CA は、各認証スペシャリストがタスクによって必要とされるスキルを所有していることを、認証スペシャリストにそのタスクの履行を許可する前に、文書化するものとする（SHALL）。

CA は、すべての認証スペシャリストが、本要件に記載されている情報認証要件について CA が実施する試験に合格することを要求するものとする（SHALL）

14.2 職務の委譲

14.2.1 全般

CA は、本要件のセクション 11 の全部または一部の履行を、委譲先の第三者機関に委譲してもよい（MAY）。ただし、プロセス全体としてセクション 11 のすべての要件を満たすことを条件とする。

CA が委譲された職務を履行することを委譲先の第三者機関に承認する前に、CA は、委譲先の第三者機関に対して以下を契約により要求するものとする（SHALL）。

1) 委譲された職務に該当する場合、セクション 14.1 の適格性要件を満たしていること。
2) セクション 15.3.2 に従ってドキュメントを保持すること。
3) 委譲された職務に該当する本要件の他の条項に従うこと。および
4) （a） CA の証明書ポリシー/認証局運用規定、または（b） CA が本要件に準拠するとして検証済みの委譲先の第三者機関の運用規定に従うこと。

CA は、証明書の発行に関与する委譲先の第三者機関の担当者が、セクション 14 のトレーニングおよびスキル要件とセクション 15 のドキュメント保管およびイベントログ記録要件を満たすことを検証するものとする（SHALL）。

委譲先の第三者機関がセクション 11.5（ハイリスク要求）の CA の義務を果たす場合、ハイリスク証明書要求の識別とさらなる検証に委譲先の第三者機関が使用するプロセスが、少なくとも CA 自身のプロセスと同程度のレベルを保証できることを CA は検証するものとする（SHALL）。

14.2.2 準拠義務

CA は、各委譲先の第三者機関による本要件への準拠を、年に一度、内部で監査するものとする（SHALL）。

14.2.3 責任の割り当て

委譲されたタスクに対し、CA および委譲先の第三者機関は、両当事者の判断に従い契約によって責任を両当事者間で分配してもよい（MAY）。ただし、その場合でも、CA は、タスクが委譲されていない場合と同じように、本要件に従い、すべての当事者の履行について完全に責任を

負うものとする（SHALL）。

14.2.4 エンタープライズ RA

CA は、エンタープライズ RA 自身の組織からの証明書要求を検証するエンタープライズ RA を指定してもよい（MAY）。

CA は、以下の要件が満たされない限り、エンタープライズ RA によって承認された証明書要求を受け入れないものとする（SHALL NOT）。

1. CA は、要求された FQDN がエンタープライズ RA が検証済みのドメイン名空間内にあることを確認するものとする（セクション 7.1.2 の第 1 項を参照）。
2. 証明書要求に FQDN 以外のタイプの サブジェクト 名が含まれている場合、CA は、名前が委譲先のエンタープライズの名前または委譲先のエンタープライズの関連会社の名前であること、または委譲先のエンタープライズが指定されている サブジェクトの代理人であることを確認するものとする（SHALL）。たとえば、CA は、エンタープライズ RA 「ABC Co.」の許可を得た サブジェクト 名「XYZ Co.」を含む証明書を、2 つの会社が関連会社である（セクション 11.1 を参照）、または「ABC Co.」が「XYZ Co.」の代理人である場合を除き、発行しないものとする（SHALL）。この要件は、付随の要求された サブジェクト FQDN が ABC Co. の登録ドメイン名のドメイン名空間内にあるかどうかに関係なく適用される。

CA は、これらの制限を契約要件としてエンタープライズ RA に課し、エンタープライズ RA による準拠を監視するものとする（SHALL）。

15. データレコード

15.1 文書化およびイベントログ記録

CA および各委譲先の第三者機関は、証明書要求と関連して生成されるすべての情報および受領されるドキュメントを含め、証明書要求の処理および証明書の発行のために実行するアクションの詳細、日付と時刻、および関与した担当者を記録するものとする（SHALL）。CA は、CA による本要件への準拠の証拠として、これらの記録を公認監査人に対して提供するものとする（SHALL）。

15.2 イベントおよびアクション

CA は、少なくとも以下のイベントを記録するものとする（SHALL）。

1. CA 鍵ライフサイクルマネジメントイベント（以下を含む）：
   a. 鍵の生成、バックアップ、格納、リカバリ、アーカイブ、および破棄
   b. 暗号化デバイスライフサイクル管理イベント
2. CA および加入者証明書ライフサイクルマネジメントイベント（以下を含む）：
   a. 証明書要求、更新、鍵の再生成要求、および失効
   b. 本要件および CA の認証局運用規定に規定されているすべての認証アクティビティ
   c. 認証のための電話連絡の日付、時刻、使用された電話番号、電話対応者、および認証の最終結果
   d. 証明書要求の承諾および却下
   e. 証明書の発行
   f. 証明書失効リストおよび OCSP エントリの生成

3. セキュリティイベント（以下を含む）
    a. 成功および失敗した PKI システムアクセス試行
    b. 実行された PKI およびセキュリティシステムアクション
    c. セキュリティプロファイルの変更
    d. システムクラッシュ、ハードウェア障害、およびその他の異常
    e. ファイアウォールおよびルーターアクティビティ
    f. CA 施設への出入記録

ログエントリには、以下の要素を含めなければならない（MUST）。

1. 記録の日付と時刻
2. 情報を記録した担当者情報
3. 記録の詳細

15.3 保管

15.3.1 監査ログの保管

CA は、発効日以降に生成された監査ログを少なくとも 7 年間保存するものとする（SHALL）。
CA は、要求に応じてこれらの監査ログを公認監査人に対して提出するものとする（SHALL）。

15.3.2 ドキュメントの保管

CA は、証明書要求、その検証、およびそのすべての証明書と失効に関するすべてのドキュメントを、そのドキュメントに基づく証明書が有効でなくなってから少なくとも 7 年間保存するものとする（SHALL）。

16. データセキュリティ

16.1 目的

CA は、以下を目的として設計された包括的なセキュリティプログラムを開発、実装、および保守するものとする（SHALL）。

1. 証明書データおよび証明書管理プロセスの機密性、整合性、および可用性の保護
2. 既知の脅威や危険から証明書データおよび証明書管理プロセスの機密性、整合性、および可用性の保護
3. 証明書データまたは証明書管理プロセスの不正または違法なアクセス、使用、開示、変更、または破壊の防止
4. 証明書データまたは証明書管理プロセスの事故による損失または破壊、あるいは損害の防止
5. 法令によって CA に適用されるその他のすべてのセキュリティ要件への準拠

16.2 リスクアセスメント

CA のセキュリティプログラムには、以下を行う年に一度のリスクアセスメントを含めなければならない（MUST）。

1. 証明書データまたは証明書管理プロセスの不正なアクセス、開示、不正使用、変更、または破壊につながる可能性がある予測可能な内部および外部脅威を識別する
2. 証明書データおよび証明書管理プロセスの秘密度を考慮に入れて、これらの脅威の可能性および考えられる損害を評価する

3. かかる脅威に対抗するために CA が実装しているポリシー、手順、情報システム、技術、およびその他の準備の十分性を評価する

16.3 セキュリティ計画

リスクアセスメントに基づき、CA は、上述の目的を実現し、証明書データおよび証明書管理プロセスの重要度に応じたリスクアセスメント中に識別されたリスクを管理するように設計されたセキュリティ手順、対策、および製品で構成されるセキュリティ計画を開発、実装、および維持するものとする（SHALL）。セキュリティ計画には、証明書データおよび証明書管理プロセスの秘密度に適した管理上、組織的、技術的、および物理的な保護対策を含めなければならない（MUST）。また、セキュリティ計画では、その時点で提出な技術および特定の対策の実装コストを考慮に入れなければならず（MUST）、セキュリティの侵害から生じる可能性がある損害および保護対象のデータの性質に適した合理的なセキュリティレベルを実装するものとする（SHALL）。

16.4 事業継続

さらに、CA は、災害、セキュリティの危殆化、または企業倒産が発生した場合にアプリケーションソフトウェアサプライヤ、加入者、および依拠当事者に通知し、合理的に保護するように設計された、事業継続およびディザスタリカバリ手順を文書化するものとする（SHALL）。CA は、事業継続計画を公開する必要はないが、要求に応じてセクション 15.3 の事業継続計画およびセキュリティ計画を CA の監査人に対して利用可能にするものとする（SHALL）。CA は、これらの手順を年に一度テスト、レビュー、および更新するものとする（SHALL）。

事業継続計画には以下を含めなければならない（MUST）。

1. 計画を始動するための条件
2. 緊急事態発生時の手順
3. フォールバック手順
4. 再開手順
5. 計画の保守スケジュール
6. 意識向上および教育要件
7. 個人の責任範囲
8. 目標復旧時間（Recovery Time Objective）
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中断または障害発生後、タイムリーに CA のビジネスオペレーションを維持または復元するための計画
11. 重要な暗号化マテリアル（つまり、安全な暗号化デバイスおよび起動マテリアル）を代替場所に保管するための要件
12. 容認可能なシステム停止期間および回復時間の構成要素
13. 必須のビジネス情報およびソフトウェアのバックアップコピーが作成される頻度
14. 復旧施設から CA のメインサイトまでの距離
15. 災害発生から元のサイトまたはリモートサイトで安全な環境を復元するまでの期間に、可能な範囲でファシリティを保護するための手順

16.5 システムセキュリティ[1]

[1] CA/ブラウザフォーラムは、本要件の v1.0 の採択後に追加のセキュリティ要件を規定する。

証明書管理プロセスには以下を含めなければならない（MUST）。

1. 物理セキュリティおよび環境管理
2. 構成管理、信頼できるコードの整合性の保守、マルウェア検出/防止を含む、システムの整合性制御
3. ポート制限および 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およびファイアウォール管理
4. ユーザー管理、職務分担、教育、認知、トレーニング
5. 個々人の責任を明確にするための論理的なアクセス制御、アクティビティロギング、およびアイドル時のタイムアウト

CA は、証明書の発行を直接的に引き起こす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施行するものとする（SHALL）。

16.6 秘密鍵保護

CA は、秘密鍵およびその他の資産を既知の脅威から保護するための要件を含め、少なくとも FIPS 140 レベル 3 または該当する Common Criteria のプロテクションプロファイルまたは セキュリティターゲット評価保証レベル４（またはそれ以上）を満たすものとして検証されたシステムまたはデバイスで秘密鍵を保護するものとする（SHALL）。CA は、不正な証明書発行を防止するための物理的および論理的な保護対策を実装するものとする（SHALL）。前述の検証済みのシステムまたはデバイス外部での秘密鍵の保護は、秘密鍵の開示を防止する方法で実装された、物理セキュリティ、暗号化、またはその両方の組み合わせから構成されなければならない（MUST）。CA は、秘密鍵を、暗号化された鍵または鍵の一部の残存期間中、暗号解読攻撃に耐えることができる最先端技術のアルゴリズムおよび鍵長によって秘密鍵を暗号化するものとする（SHALL）。秘密鍵のバックアップ、格納、およびリカバリは、安全な物理的環境において、信頼できる複数の担当者の立ち会いのもとでのみ行なわれるものとする（SHALL）。

17. 監査

17.1 適格な監査スキーム

CA は、以下のスキームのいずれかに従って監査を受けるものとする（SHALL）。

1. WebTrust for Certification Authorities v2.0 以降
2. ETSI TS 101 456 v1.2.1 以降への準拠を監査する政府によるスキーム
3. ETSI TS 102 042 v1.1.1 以降への準拠を監査する政府によるスキーム
4. 公認監査人によって実行される、ISO 21188:2006 への準拠を監査するスキーム。
5. 政府機関 CA が異なる内部監査スキームを使用することを証明書ポリシーによって要求されている場合は、（a）監査が（i）上記のスキームのいずれかのすべての要件を包含している、または（ii）パブリックレビューが可能な同等の条件から構成されている、および（b）監査が、CA から独立していて、セクション 17.6 の要件を満たす公認監査人によって実施されることを条件として、かかるスキームを使用してもよい。

CA は、以下のスキームのいずれかに従って監査を受けるものとする（SHALL）。

1. WebTrust for Certification Authorities v2.0
2. ETSI TS 102 042 への準拠を監査する政府によるスキーム
3. ISO 21188:2006 への準拠を監査するスキーム

4. 政府機関 CA が異なる内部監査スキームを使用することを証明書ポリシーによって要求されている場合は、監査が（a）上記のスキームのいずれかのすべての要件を包含している、または（b）パブリックレビューが可能な同等の条件から構成されていることを条件として、かかるスキームを使用してもよい（MAY）。

いずれのスキームが選択されても、定期的な監視や説明責任の手順を組み込まなければならない（MUST）。これにより、監査がスキームの要件に従って引き続き実行されていることを確認する。

セクション 17.6 に規定されているように、監査は公認監査人が実施しなければならない（MUST）。

17.2 監査期間

CA が証明書を発行する期間は、すべて監査の対象となるものとする（SHALL）。監査期間は、1 年を超えてはならない（MUST NOT）。

17.3 監査レポート

監査レポートは、セクション 9.3.1 に記載された 1 つ以上のポリシー識別子を使用するすべての証明書の発行に対して、使用されたシステムとプロセスを対象とすることを明記するものとする（SHALL）。CA は、監査レポートを公開するものとする（SHALL）。CA は、全体的な監査意見に影響を与えない内容の監査結果については公開する必要がない。政府 CA および民間 CA の両方について、CA は、監査レポートを監査期間の終了後 3 カ月以内に公開すべきである（SHOULD）。3 カ月を越えて遅延し、アプリケーションソフトウェアサプライヤによって要求される場合、CA は、公認監査人によって署名された説明書簡を提供するものとする（SHALL）。

17.4 発行開始前の準備状況の監査

CA がセクション 17.1 に記載されている監査スキームへの準拠を示す現在有効な監査レポートを保持している場合、発行前の評価は不要である。

CA がセクション 17.1 に記載されている監査スキームのいずれかへの準拠を示す現在有効な監査レポートを保持しない場合は、パブリック証明書を発行する前に、CA は、セクション 17.1 に記載された監査スキームのいずれかの該当する基準に従って実施される、特定時点での準備状況の評価を行なうものするものとする（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 カ月間より前に評価しないものとし（SHALL）、最初のパブリック証明書の発行開始後から 90 日以内にかかるスキームの下での完全な監査を行うものとする（SHALL）。

17.5 委譲された職務の監査

委譲先の第三者機関がセクション 17 に従って現在監査されておらず、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 に基づいて要求されるドメイン利用権限確認プロセスが（1）証明書要求または証明書要求をサポートする情報の真正性を確認するために CA または委譲先の第三者機関を代表する少なくとも 1 人の人物が関与するアウトオブバンドメカニズムを使用して、または（2）ドメイン利用権限確認プロセス自体を実行して、委譲先の第三者機関によって適切に実行されていることを保証するものとする（SHALL）。

CA が前述の手順のいずれかを使用せず、委譲先の第三者機関がエンタープライズ RA でない場合、CA は、セクション 17.1 に記載された容認されている監査スキームの基になる監査標準に従って発行された、委譲先の第三者機関の履行が委譲先の第三者機関の運用規定または CA の証明書ポリシーや認証局運用規定に準拠するかどうかについての意見を提供する監査レポートを取得するものとする（SHALL）。意見が委譲先の第三者機関が準拠しないというものである場合、CA は、委譲先の第三者機関による委譲された職務の履行継続を許可しないものとする（SHALL）。

委譲先の第三者機関の監査期間は、1 年を超えないものとする（SHALL NOT）（CA の監査と整合することが望ましい）。ただし、CA または委譲先の第三者機関が行政機関により運用、管理、監督されており、監査結果が数年にわたって問題ないと判断された場合、年次監査では、年に一度の監査が要求されているコアな管理に加え、低い頻度での実施が許可されているコアでない管理の一部の監査を行なうとする（MUST）。ただし、コアでない管理でも最低 3 年に一度は監査しなくてはならない。

17.6 監査役の資格

CA の監査は、公認監査人によって実施されるものとする（SHALL）。公認監査人とは、以下の適格性およびスキルを併せ持つ個人、法人、または個人あるいは法人のグループを意味する。

1. 監査の対象から独立している。
2. 適格な監査スキームで指定されている条件に対応する監査を実施できる。
3. 公開鍵基盤技術、情報セキュリティツールおよび技法、情報技術およびセキュリティ監査、および第三者機関の証明職務の審査に熟達している個人を雇用している。
4. 監査スキームに基づく監査人の適格性要件を満たすとして、認定、認証、ライセンス、またはその他の方法で評価されている。
5. 法律、政府の規制、または職業倫理に準拠している。および
6. 国内政府監査機関の場合を除き、少なくとも 100 万米ドルの補償を保険範囲とする職業上の過失および怠慢責任に関する保険に加入している。

CA の監査は、公認監査人によって実施されるものとする（SHALL）。公認監査人とは、以下の適格性およびスキルを併せ持つ個人、法人、または個人あるいは法人のグループを意味する。

1. 監査の対象から独立している。
2. 適格な監査スキームで指定されている条件に対応する監査を実施できる（セクション 17.1 を参照）。
3. 公開鍵基盤技術、情報セキュリティツールおよび技法、情報技術およびセキュリティ監査、および第三者機関の証明職務の審査に熟達している個人を雇用している。
4. （ETSI 標準のいずれかに従って実施される監査の場合）ETSI TS 119 403 に従って認証されている、または同等の政府スキームによる監査の実施が認証されている、または ISO 27001 監査実施のために ISO 27006 に沿って政府認定機関が認証している。
5. （WebTrust 標準に従って実施される監査の場合）WebTrust が使用を許諾している。
6. 法律、政府の規制、または職業倫理に準拠している。および
7. 国内政府監査機関の場合を除き、少なくとも 100 万米ドルの補償を保険範囲とする職業上の過失および怠慢責任に関する保険に加入している。

17.7 鍵生成セレモニー

発効日以降に作成された、(i) ルート CA 鍵ペアとして使用される、または (ii) ルート CA の運用者またはルート CA の関連会社ではない下位 CA に対して生成された鍵ペアであるルート CA 鍵ペアについて、CA は以下に準拠するものとする（SHALL）。

1. 鍵生成スクリプトを用意して、スクリプトに従って実施する。
2. 公認監査人にルート CA 鍵ペア生成プロセスに立ち会わせる、またはルート CA 鍵ペア生成プロセス全体のビデオを録画する。

3. 公認監査人に、CA が鍵と証明書の生成プロセス中の鍵セレモニーおよび鍵ペアの整合性と機密性を保証するために使用される制御に従ったことについて意見を述べるレポートを発行させる。

ルート CA の運用者またはルート CA の関連会社用として、発効日以降に作成されたその他の CA 鍵ペアの場合、CA は以下に準拠すべきである（SHOULD）。

1. 鍵生成スクリプトを用意して、スクリプト通りに実施する。
2. 公認監査人に、ルート CA 鍵ペア生成プロセスに立ち会わせる、またはルート CA 鍵ペア生成プロセス全体のビデオを録画する。

いずれの場合も、CA は以下に準拠するものとする（SHALL）。

1. CA の証明書ポリシーや認証局運用規定の内容に従って物理的に保護された環境で鍵を生成する。
2. 複数人物による統制および知識分散の原則に基づく信頼される役職の担当者により CA 鍵を生成する。
3. CA の証明書ポリシーや認証局運用規定で公開されている該当する技術およびビジネス要件を満たす暗号化モジュール内で CA 鍵を生成する。
4. CA 鍵生成アクティビティを記録する。および
5. 秘密鍵が証明書ポリシーや認証局運用規定および（該当する場合は）鍵生成スクリプトに記載されている手順に従って生成および保護されたことを合理的に保証する効果的な管理 9 を維持する。

17.8 定期的な品質保証自主監査

CA が証明書を発行する期間中、以前の自己監査で、サンプルが取得された直後の期間に発行された証明書の一つまたは３％のいずれか多い方の数の証明書をランダムに選択し、CA は、少なくとも四半期に一度は内部監査を実施して、証明書ポリシー、認証局運用規定、および本要件への準拠を監視し、サービス品質を厳密に管理するものとする（SHALL）。セクション 16.3 に規定されている条件を満たす年次の監査を受ける委譲先の第三者機関を除き、CA は、最後のサンプルが取得された直後から始まる期間に委譲先の第三者機関によって検証された証明書の一つあるいは 3% のいずれか多いほうの数の証明書をサンプルとしてランダムに選択し、CA が依頼する検証スペシャリストに継続的な四半期に一度の監査を実施させて、委譲先の第三者機関によって発行された証明書または検証された情報を含む証明書のサービス品質を厳密に管理するものとする（SHALL）。CA は、各委譲先の第三者機関の運用および手順をレビューして、委譲先の第三者機関が本要件および関連する証明書ポリシーや認証局運用規定に準拠していることを保証するものとする（SHALL）。

18. 責任および補償

18.1 加入者および依拠当事者に対する責任

CA が本要件およびその証明書ポリシーや認証局運用規定に準拠して証明書を発行および管理している限り、証明書の受益者またはその他の第三者機関が証明書の使用または依拠の結果被った被害については、CA の証明書ポリシーや認証局運用規定に規定されている損害賠償を上限とし、それ以上の損害については、責任を拒否することができる（MAY）。CA が本要件およびその証明書ポリシーや認証局運用規定に準拠して証明書を発行または管理していなかった場合、CA は、CA が望む適切な手段によって、かかる証明書の使用または依拠の結果として被ったすべての申し立て、損失、または損害について、訴因や関連法理論にかかわらず、加入者および依拠当事者への責任の制限を要求することができる（MAY）。CA が本要件またはその証明書ポリシーや認証局運用規定に準拠して発行または管理されていなかった証明書に対する責任を制限することを選択した場合、CA は、CA の証明書ポリシーや認証局運用規定に責任の上限を記

載するものとする（SHALL）。

18.2 アプリケーションソフトウェアサプライヤの補償

加入者および依拠当事者への責任の限定にもかかわらず、ルート CA との間でルート証明書配付契約を締結しているアプリケーションソフトウェアサプライヤが、本要件に基づく、または証明書の発行保守あるいは依拠当事者、その他の者による依拠を理由として存在する可能性がある、CA の義務または潜在的な責任を負わないことを CA は理解し、同意するものとする。したがって、CA が行政機関である場合を除き、CA は、CA によって発行された証明書に関連してかかるアプリケーションソフトウェアサプライヤが被るすべての申し立て、損害、および損失について、訴因または関連法理論にかかわらず、各アプリケーションソフトウェアサプライヤを擁護し、補償し、免責するものとする（SHALL）。ただし、アプリケーションソフトウェアサプライヤのソフトウェアが、以下のような不正な証明書を有効、または信頼可能と表示したことによって直接引き起こされた場合には、CA によって発行された証明書に関連してかかるアプリケーションソフトウェアサプライヤが被った申し立て、損害、または損失に関して、上記は適用されない。（1）有効期限を過ぎた証明書、あるいは（2）失効した証明書（ただし、失効ステータスが現在 CA がオンラインで公開しており、アプリケーションソフトウェアがかかるステータスをチェックしなかったか、失効ステータスの表示を無視した場合に限る）。

18.3 ルート CA の義務

ルート CA は、下位 CA の本要件への準拠、および本要件の下での下位 CA のすべての責任および補償義務について、ルート CA が証明書を発行する下位 CA であるかのごとく、下位 CA の履行および保証について責任を持つものとする（SHALL）。

付録 A - 暗号化アルゴリズムおよび鍵要件（標準的）

証明書は、アルゴリズムの種類および鍵サイズについて以下の要件を満たさなければならない（MUST）。

（1）ルート CA 証明書

	検証期間が 2010 年 12 月 31 日以前に始まる	検証期間が 2010 年 12 月 31 日よりも後に始まる
ダイジェストアルゴリズム	MD5（非推奨） SHA-1、SHA-256、SHA-384、または SHA-512	SHA-1*、SHA-256、SHA-384、または SHA-512
最小 RSA 係数サイズ（ビット）	2048**	2048
ECC 曲線	NIST P-256、P-384、または P-521	NIST P-256、P-384、または P-521

（2）下位 CA 証明書

	検証期間が 2010 年 12 月 31 以前に始まり、2013 年 12 月 31 日以前に終了する	検証期間が 2010 年 12 月 31 日よりも後に始まり、2013 年 12 月 31 日よりも後に終了する
ダイジェストアルゴリズム	SHA-1、SHA-256、SHA-384、または SHA-512	SHA-1*、SHA-256、SHA-384、または SHA-512
最小 RSA 係数サイズ（ビット）	1024	2048
ECC 曲線	NIST P-256、P-384、または P-521	NIST P-256、P-384、または P-521

（3）加入者証明書

	検証期間が 2013 年 12 月 31 日以前に終了する	検証期間が 2013 年 12 月 31 日より後に終了する
ダイジェストアルゴリズム	SHA1*、SHA-256、SHA-384、または SHA-512	SHA1*、SHA-256、SHA-384、または SHA-512
最小 RSA 係数サイズ（ビット）	1024	2048
ECC 曲線	NIST P-256、P-384、または P-521	NIST P-256、P-384、または P-521

* SHA-1 は、SHA-256 が世界中の依拠当事者の大部分によって使用されるブラウザで幅広くサポートされるまで使用してもよい（MAY）。
** 2010 年 12 月 31 日よりも前に、2048 ビット未満の RSA 鍵長で発行されたルート CA 証明書は、本要件に従って発行される加入者証明書のトラストアンカーを引き続き務めてもよい（MAY）。

付録 B - 証明書エクステンション（標準的）

この付録は、発効日以降に生成された証明書の証明書エクステンションの要件を規定する。

ルート CA 証明書

ルート CA 証明書はタイプ X.509 v3 でなければならない（MUST）。

A. basicConstraints

このエクステンションは、重要なエクステンションとして現れなければならない（MUST）。cA フィールドは true に設定しなければならない（MUST）。pathLenConstraint フィールドは存在すべきでない（SHOULD NOT）。

B. keyUsage

このエクステンションは、存在しなければならず（MUST）、重要としてマークされなければならない（MUST）。keyCertSign および cRLSign のビット位置を設定しなければならない（MUST）。ルート CA 秘密鍵が OCSP レスポンスの署名に使用される場合は、digitalSignature ビットを設定しなければならない（MUST）。

C. certificatePolicies

このエクステンションは存在すべきでない（SHOULD NOT）。

D. extendedKeyUsage

このエクステンションは存在してはならない（MUST NOT）。

その他のすべてのフィールドおよびエクステンションは、RFC 5280 に従って設定しなければならない（MUST）。

下位 CA 証明書

下位 CA 証明書はタイプ X.509 v3 でなければならない（MUST）。

A. certificatePolicies

このエクステンションは、存在しなければならず（MUST）、重要としてマークすべきではない（SHOULD NOT）。

certificatePolicies:policyIdentifier （必須）

以下のフィールドは、下位 CA がルート CA を管理する組織体の関連会社ではない場合、存在してもよい（MAY）。

certificatePolicies:policyQualifiers:policyQualifierId （任意）

- id-qt 1 ［RFC 5280］。

certificatePolicies:policyQualifiers:qualifier:cPSuri （任意）

- ルート CA の証明書ポリシー、認証局運用規定、依拠当事者規約、または CA によって提供されるオンラインポリシー情報へのその他のポインタの HTTP URL。

B. cRLDistributionPoints

このエクステンションは、存在しなければならず（MUST）、重要としてマークしてはならない（MUST NOT）。CA の CRL サービスの HTTP URL を含めなければならない（MUST）。

C. authorityInformationAccess

以下に規定するステイプルを除き、このエクステンションは存在しなければならない（MUST）。重要としてマークしてはならず（MUST NOT）、発行 CA の OCSP レスポンダ（accessMethod = 1.3.6.1.5.5.7.48.1）の HTTP URL を含めなければならない（MUST）。発行 CA の証明書（accessMethod = 1.3.6.1.5.5.7.48.2）の HTTP URL も含

むべきである（SHOULD）。詳しくは、セクション 13.2.1 を参照。

発行 CA の OCSP レスポンダの HTTP URL は、加入者が TLS ハンドシェーク［RFC4366］内に証明書の OCSP レスポンスを「ステイプル」することを条件として、省略してもよい（MAY）。

D. basicConstraints

このエクステンションは、存在しなければならず（MUST）、重要としてマークされなければならない(MUST)。cA フィールドは true に設定しなければならない(MUST)。pathLenConstraint フィールドは存在してもよい（MAY）。

E. keyUsage

このエクステンションは、存在しなければならず（MUST）、重要としてマークされなければならない（MUST）。keyCertSign および cRLSign のビット位置を設定しなければならない（MUST）。下位 CA 秘密鍵が OCSP レスポンスの署名に使用される場合は、digitalSignature ビットを設定しなければならない（MUST）。

F. nameConstraints（任意）

存在する場合、このエクステンションは重要（※）としてマークすべきである（SHOULD）。

その他のすべてのフィールドおよびエクステンションは、RFC 5280 に従って設定しなければならない（MUST）。

※重要でない名前制限は RFC 5280 において例外である。世界で多数の依拠当事者が使用するソフトウェアのアプリケーションソフトウェアサプライヤが､かかる名前制限のエクステンションをサポートするまで、これを使用してもよい（MAY）。

加入者証明書

A. certificatePolicies

このエクステンションは、存在しなければならず（MUST）、重要としてマークすべきではない（SHOULD NOT）。certificatePolicies:policyIdentifier （必須）

- 発行 CA によって定義される、発行 CA の本要件への準拠を表明する証明書ポリシーを示すポリシー識別子。

以下のエクステンションは存在してもよい（MAY）。

certificatePolicies:policyQualifiers:policyQualifierId （推奨）

- id-qt 1 ［RFC 5280］。

certificatePolicies:policyQualifiers:qualifier:cPSuri （任意）

- 下位 CA の認証局運用規定、依拠当事者規約、または CA によって提供されるオンライン情報へのその他のポインタの HTTP URL。

B. cRLDistributionPoints

このエクステンションは存在してもよい（MAY）。存在する場合、重要としてマークしてはならず（MUST NOT）、CA の CRL サービスの HTTP URL を含めなければならない（MUST）。詳しくは、セクション 13.2.1 を参照。

C. authorityInformationAccess

以下に規定するステイプルを除き、このエクステンションは存在しなければならない（MUST）。重要としてマークしてはならず（MUST NOT）、発行 CA の OCSP レスポンダ（accessMethod = 1.3.6.1.5.5.7.48.1）の HTTP URL を含めなければならない（MUST）。発行 CA の証明書（accessMethod = 1.3.6.1.5.5.7.48.2）の HTTP URL も含

むべきである（SHOULD）。詳しくは、セクション 13.2.1 を参照。

発行 CA の OCSP レスポンダの HTTP URL は、加入者が TLS ハンドシェーク［RFC4366］内に証明書の OCSP レスポンスを「ステイプル」することを条件として、省略してもよい（MAY）。

D. basicConstraints （任意）

存在する場合、cA フィールドは false に設定しなければならない（MUST）。

E. keyUsage （任意）

存在する場合、keyCertSign および cRLSign のビット位置を設定してはならない（MUST NOT）。

F. extKeyUsage （必須）

値 id-kp-serverAuth ［RFC5280］または id-kp-clientAuth ［RFC5280］あるいは両方の値が存在しなければならない（MUST）。id-kp-emailProtection ［RFC5280］は存在してもよい（MAY）。その他の値は存在すべきでない（SHOULD NOT）。

その他のすべてのフィールドおよびエクステンションは、RFC 5280 に従って設定しなければならない（MUST）。

付録 C - ユーザーエージェント検証（標準的）

CA は、アプリケーションソフトウェアサプライヤが、それぞれのパブリック証明書までチェーンでつながる加入者証明書を使ってソフトウェアをテストするためのテスト Web ページをホストするものとする（SHALL）。最小限、CA は、（i）有効、（ii）失効、および（iii）有効期限切れの加入者証明書を使用する個別の Web ページをホストするものとする（SHALL）。