JCAN Certificate Policy

JCAN 証明書ポリシ

JIPDEC

一般財団法人日本情報経済社会推進協会

Date :25/07/2016 Ver 4.0

Document Change Control
改訂履歴

Version	Release Date	Status + Description	Author	Approver
4.0	25/07/2016	Administrative update ETSI 認定中止に伴う修正	ITC/JCAN rep ITC/JCAN 担当	Managing Director 常務理事(JCAN 担当)
3.2	28/03/2014	Administrative update ETSI 認定対応の修正	DUPC/JCAN rep DUPC/JCAN 担当	Managing Director 常務理事(JCAN 担当)
3.1	18/04/2013	Administrative update ETSI 認定対応の修正	DUPC/JCAN rep DUPC/JCAN 担当	Managing Director 常務理事(JCAN 担当)
3.0	02/04/2012	Administrative update ETSI 認定対応の修正	DUPC/JCAN rep DUPC/JCAN 担当	Managing Director 常務理事(JCAN 担当)
2.0	16/10/2011	Administrative update ETSI 認定対応の修正	DUPC/JCAN rep DUPC/JCAN 担当	Managing Director 常務理事(JCAN 担当)
1.0	17/10/2010	Initial Version 初版	DUPC/JCAN rep DUPC/JCAN 担当	Managing Director 常務理事(JCAN 担当)

－Table of Contents－

1. Introduction (はじめに)

1.1 Overview (概要)

This document (CP) is applied to JCAN Certificates, and prescribes policies such as usage and community.

JCAN certificates are issued by CA (Outsource organizations are included) which has a system for quality and information security management appropriate and are comply to "WebTrust for CA".

This CP is administered by JCAN.

JCAN is a private sector system operated by JIPDEC (Address: Minato-ku, Tokyo, JAPAN Commercial Register under Number : 010405009403,JAPAN Corporate Number : 1010405009403).

本書(CP)は、JCAN 証明書に適用され、用途及び範囲等のポリシを規定するものである。

JCAN 証明書は、適切な品質と情報セキュリティ管理のためのシステムを持つ CA（委託先を含む）によって発行され、「WebTrust for CA」に従う証明書である。

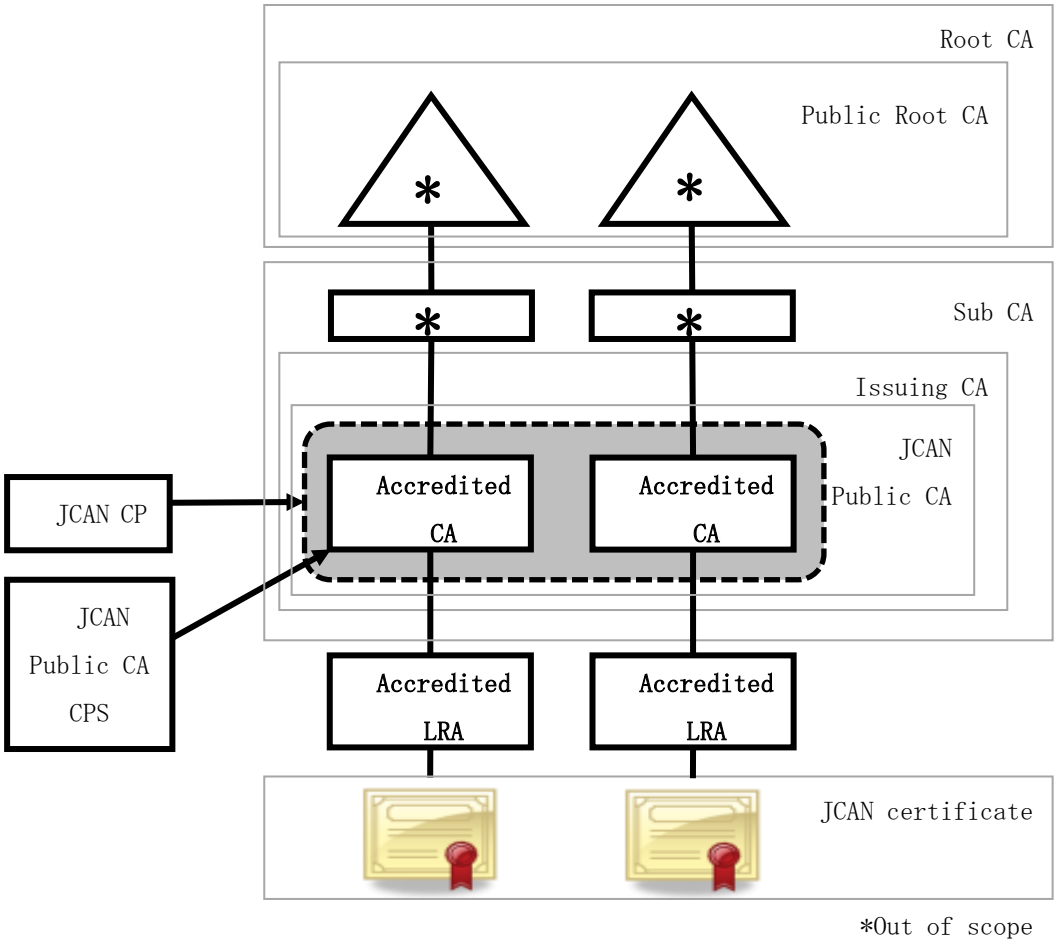
本 CP は、JCAN によって管理される。

JCAN は、一般財団法人日本情報経済社会推進協会（所在地：東京都港区、商業登記番号：010405009403、法人番号：1010405009403、以下「JIPDEC」という）が運用する民間制度である。

1.1.1 JCAN PKI Framework (JCAN PKI の構造)

The framework of JCAN PKI is shown in the following:

JCAN PKI の構造を以下に示す。



JCAN Certificates are issued from JCAN Public CA based on requests of Accredited LRAs.

Accredited LRA is accredited after confirmation of the ORGANIZATION's (which operates LRA) existence by JCAN.

Accredited CA is CA that is accredited by JCAN.

JCAN Public CA is consist of Accredited CAs,and is Sub CA of Public Root CA.

JCAN 証明書は、認定 LRA の要求に基づき JCAN パブリック CA から発行される。
認定 LRA は、LRA 業務を行う組織の実在を JCAN が確認した後、認定される。
認定 CA は、JCAN が認定した CA である。
JCAN パブリック CA は、認定 CA で構成され、パブリックルート CA のサブ CA である。

1.2 Document Name and Identification (文書名と識別)

Document name: Refer to the cover.

Version: Refer to the cover.

OID: 1.2.392.200063.30.5300

1.3 PKI participants (PKI の関係者)

(1) Subscribers (利用者)

Subscribers are subjects or users of JCAN Certificate.

The obligations are the followings:

- Agree with use/disclose of the personal information by LRA (operation, audit/accreditation/legal-proceedings) and agree with use /disclose of the personal information which recorded on a certificate by Relying Party (operation, validation);
- Agree which Accredited LRA (as subscriber's representative) backups PKCS#12 formatted certificates and it's PIN when it generates PIN;
- Use of the certificate shall only be permitted once the Subscriber has agreed to the conditions within this CP;
- Use the certificate under secure conditions, protect certificates from unauthorized use and discontinue use of the certificate upon expiration or revocation;
- Notify the Accredited LRA promptly of any changes of the data recorded in the JCAN Certificates;
- Notify the Accredited LRA promptly of loss or theft of PC or Media in which JCAN Certificates are installed;
- Notify the Accredited LRA promptly when the reliability of the JCAN Certificates may be damaged, such as an unauthorized access by cracking and a virus/Malware infection; and
- Accept a revocation of the certificate by Accredited LRA and JCAN

利用者は、JCAN 証明書の主体又は JCAN 証明書の使用者である。

利用者の義務は以下の通りである。

- 証明書発行に際し、LRA（業務、監査/認定/訴訟対応）による個人情報の利用/開示について及び検証者（業務、検証対応）による証明書に記載された個人情報の利用/開示を行うことに同意する。
- 認定 LRA（利用者の代表）が PIN を生成した場合、PKCS#12 形式証明書及び PIN をバックアップすることに同意する。
- 本 CP の諸条件を承諾し許可された用途にのみ証明書を使用すること

- 証明書を合理的な環境下で使用し、不正な操作から防御すること。また証明書が有効でなくなった場合は、使用をやめること。
- JCAN 証明書の記載事項の変更は、認定 LRA に、速やかに知らせること。
- JCAN 証明書がインストールされた PC 又は媒体の紛失、盗難は、認定 LRA に、速やかに知らせること。
- クラッキングによる不正侵入、ウィルスやマルウエア感染等、証明書の信頼性が損なわれる可能性がある場合は、認定 LRA に、速やかに知らせること。
- 認定 LRA または JCAN による証明書の失効を了解する。

(2)Accredited LRA（認定 LRA）

Accredited LRA is the LRA which JCAN accredited as are subscriber's representative.

Accredited LRA vets the authenticity of the DN and verifies the identity of the subscriber of JCAN Certificates. Furthermore, the Accredited LRA operates the certificate life-cycle management (issue, revoke) of the certificate under JCAN Certificate Policy.

The obligations are the followings:

① General

- Informs "subscribers obligation" to subscriber;
- Record of a subject's consent that the subscriber acts on behalf of the subject. The subject's consent is archived;
- Acquiring information disclosed on JCAN Repository and awereness to subscribers if necessary. Especially, carries out promptly in cases such as receiving a notice from JCAN.
- Makes to vow not performing illegal issuance and disclosure;

② Certificate Issuance

- Guarantees the unique identification allotted to OrganizationUnitName2 and CommonName within subject;
- When Accredited LRA generates PIN, Accredited LRA distributes the PKCS#12 formatted certificates and corresponding PIN to the subscribers securely;
- When Accredited LRA backups PKCS#12 formatted certificates and it's PIN, it manages securely;
- After certificate issuance, Accredited LRA archives the copy of "30-5600 Certificate Life-Cycle Roster".

③ Certificate Revocation

- Revoke the JCAN Certificates promptly when the subject/user is unrelated to the ORGANIZATION due to the reasons such as retirement, withdrawal or disposal;

- Revoke the JCAN Certificates promptly when subscriber has breached obligations under this CP and Accredited LRA's rule;
- Revoke the JCAN Certificates promptly when an error or false is recorded in the JCAN Certificate;
- Revoke the JCAN Certificates promptly when Private Key becomes compromised such as suffering disaster, compromise of LRA Operator Certificate;
- Revoke the JCAN Certificates promptly when Accredited LRA decides to revoke for other reasons.

認定 LRA とは、利用者の代表として JCAN が認定した LRA である。

認定 LRA は、JCAN 証明書ポリシの下、JCAN 証明書に記載する DN の真正性の審査と利用者の本人認証を行い、証明書のライフサイクルマネジメント（発行、失効）を行う。

義務は、以下のとおりである。

① 全般

- 利用者に利用者の義務を通知する。
- 利用者の同意の記録を保管する。
- JCAN リポジトリに公開される情報を取得し、利用者に必要な情報を周知する。特に、JCAN から通知を受けた場合等は速やかに行う。
- LRA 業務に従事する者は、不正な発行及び開示を行わない旨を宣言している。

② 証明書発行

- サブジェクトの OrganizationUnitName2、CommonName の唯一性を保証する。
- 認定 LRA が PIN を生成した場合、認定 LRA は PKCS#12 形式証明書及び対応する PIN をセキュアに利用者に配付する。
- 認定 LRA が PKCS#12 形式証明書及び PIN をバックアップする場合、セキュアに管理する。
- 証明書の発行後、認定 LRA は、「30-5600 管理台帳」のコピーを保管する。

③ 証明書失効

- 退職、脱退、廃棄等によりサブジェクト/使用者が当該組織と無関係になった場合、証明書を速やかに失効すること
- 利用者が本 CP 及び認定 LRA の規則の義務に違反した場合、証明書を速やかに失効すること
- JCAN 証明書に誤り又は虚偽が記載されている場合、証明書を速やかに失効すること
- 被災、LRA オペレータ証明書の危殆化等で秘密鍵が危殆化した場合、証明書を速やかに失効すること
- 認定 LRA がその他の理由で失効を決定した場合、証明書を速やかに失効すること

(3)Relying Party（検証者）

Relying Party is a person that rely on a subscriber's certificate and/or a subscriber's digital signature.

Obligations are the followings:

- Verify the validity or revocation of the certificate using current revocation status information as indicated to the relying party; and
- Rely on and trust the JCAN Certificates only under reasonable circumstances.

検証者は、利用者の証明書を信頼する者、又は利用者の電子署名を信頼する者である。

義務は、以下の通りである。

- 検証者に示された現在の失効状況情報を使って、証明書の有効性、または失効を確認する。
- JCAN 証明書を、合理的な環境下でのみ信頼すること。

(4)JCAN Public CA（JCAN パブリック CA）

JCAN Public CA is the issuing CA which issues JCAN Certificates following JCAN Certificate Policy, in accordance with its purpose of use, range of use, and procedures.

Subscribers are contacted through Accredited LRAThe obligation is prescribed on [CPS].

JCAN パブリック CA は、JCAN 証明書ポリシに従い JCAN 証明書を、その利用目的、適用範囲、手続き等に準拠して発行するイシュイング CA である。

利用者への連絡は認定 LRA を通じて行う。

義務は、[CPS]に規定する。

(5)JCAN（ジェイキャン）

JCAN is a private system operated independently by JIPDEC.

The obligations are the followings:

- Permits or revocates the accreditation of LRA;
- Guarantees the unique identification allotted to OrganizationUnitName1 within subject;
- Manages Policies of JCAN.
- Accredited LRA is ensured through appropriate credentials issued to them.

JCAN は、JIPDEC が主体的に運用する民間制度である。

義務は、以下の通りである。

- LRA の認定の許可/取消

- サブジェクトの OrganizationUnitName1 の唯一性を保証する。
- JCAN のポリシの管理
- 認定 LRA の認証は、その機関に発行される適切な信用証明を通じて保証される。

1.4 Certificate Usage (証明書の用途)

(1) JCAN Certificate (JCAN 証明書)

JCAN Certificates can be used for authentication, encryption and digital signature.
When using a JCAN Certificate, it follows the concerning law of the country if any.
The types of JCAN Certificates which JCAN manages are the following:

JCAN 証明書は、認証、暗号化、署名で使用できる。
JCAN 証明書を使う場合は、もしあればその国の関係する法律に従うこと。
JCAN が取扱う JCAN 証明書のタイプを下記に示す。

(a) JCAN Advanced (JCAN アドバンスト)

JCAN Advanced is issued to a natural person (PERSON) from Accredited LRA.
Accredited LRA identify the PERSON by databases which based on the officially issued documents.
Subject CommonName ("CN") is the real name or a pseudonym (PS[1])

JCAN アドバンストは、認定 LRA から自然人に対し発行される。認定 LRA は、公的な根拠資料に基づくデータベースで自然人を確認する。
サブジェクトの CN は実名又は PS 名である。

(b) JCAN Basic (JCAN ベーシック)

JCAN Basic is issued to the following entities without official documents：

- The ORGANIZATION's internal subjects (MEMBER and/or their role names, organization names, email addresses; OBJECT names or identifiers); or
- The ORGANIZATION's external subjects (PARTNER and/or their role names, organization names, email addresses; OBJECT names or identifiers).

NOTE) PARTNER is the member which is privity of contract, group-company, membership, committee or guest, student, person who authenticated by credible document, person who registed his/her credit card, etc.

[1] PS (Pseudonym) is an alias, or a false or a fictitious name based on a real name
PS 名（シュードニム）とは、実名に裏付けされた擬名、仮名、別名をいう

Subject CN of a JCAN certificate are the followings:

- Name of MEMBER or PARTNER (Real name or PS);
- Name of a role;
- Name of an organization such as company, party, department, team or group;
- E-mail address; orOBJECT names or identifiers such as document names, server names, IDs or Codes.

JCAN(ベーシック)証明書は公式文書のない次の実体に発行される:

- 当該組織の内部サブジェクト(メンバ、それらの役割名、組織名、メールアドレス; オブジェクトの名前,識別子);
- 当該組織の外部サブジェクト(パートナ、それらの役割名、組織名、メールアドレス; オブジェクトの名前、識別子)

注）パートナは、契約関係、グループ会社、会員、委員会の構成員、或いは客員、学生、信頼できる書類で認証した人、クレジットカードを登録した人等

JCAN 証明書に記載するサブジェクト CN は以下である。

- メンバまたはパートナ名（実名又は PS 名）
- 役割名
- 会社、団体、部門、チーム、グループ等の組織名
- メールアドレス
- 文書名、サーバ名、ID、コード等の識別子

1.5 Policy Administration (ポリシ管理)

1.5.1 Document administrator (文書管理)

This CP is managed by PAA which is prescribed on “JCAN Public CA CPS”.

本 CP は「JCAN パブリック CA CPS」に規定されたポリシ管理局が管理する。

1.5.2 Contact Address (連絡先)

(1)Accredited LRA

The contact of JCAN Certificate issuance/revocation is disclosed on the Accredited LRA List in the following JCAN Repository.

NOTE) Only business hours are possible for contact.

http://www.jipdec.or.jp/repository/

JCAN 証明書発行/失効に係る連絡先は、次の JCAN リポジトリの認定 LRA リストに公開されている。
注）連絡は営業時間のみ

http://www.jipdec.or.jp/repository/

(2)JCAN

The contact of JCAN is the followings:
NOTE) Only business hours are possible for contact.

JCAN Secretariat

ROPPONGI FIRST BUILDING
1-9-9, ROPPONGI, MINATO-KU,
TOKYO, JAPAN

E-Mail: jcan-secretariat@jipdec.or.jp
Phone: +81-3-5860-7562

JCAN の連絡先は以下の通り。
注）連絡は営業時間のみ

JCAN 事務局
東京都港区六本木 1-9-9　六本木ファーストビル
E-Mail: jcan-secretariat@jipdec.or.jp
Phone: 03-5860-7562

1.6 Definitions and acronyms (定義語)

1.6.1 Definitions (定義)

See section 10.

セクション 10 参照

1.6.2 References (参考)

[CPS] CPS of JCAN Public CA or Accredited CA.

[OP-LRA] 30-5210 Accredited LRA Operation Policy

[SEMI] SEMI Document 4845A

NOTE) SEMI is stand for “Semiconductor Equipment and Materials International”

2. Publication and Repository Responsibilities (公開とリポジトリの責任)

2.1 Repository (リポジトリ)

JCAN reserves the rights to publish information about this CP, [CPS], and JCAN certificates that it issues in JCAN repository. And JCAN reserves the rights to publish information about CRL that it issues in JCAN repository.

The public information should be deployed so as to provide 24 hours per day, 365 days per year availability.

JCAN は、本 CP、[CPS]、及び、発行する JCAN 証明書に関する情報を JCAN のリポジトリに公開する。及び JCAN は、CRL に関する情報を JCAN のリポジトリに公開する。

公開情報は 24 時間×365 日参照可能とする。

2.2 Publication of Certificate Information (証明書情報の公開)

JCAN reserves the right to publish the followings information in the respective online public accessible repositories to the subscribers and relying parties.

JCAN notified to some of participants if needed, when the repository is changed

Archived records shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings.

JCAN は、次の内容を各リポジトリに公開し、利用者及び検証者がオンラインで参照できるようにする。

JCAN は、リポジトリを変更した場合、必要に応じて関係者に通知する。

訴訟の際に認証の証拠を提供する目的のために必要ならば、保管された記録は開示される。

(1) JCAN Repository (JCAN リポジトリ)

- Public Root CA Certificate and Sub CA certificates
- The 2 latest versions of this CP
- Accredited LRA attribute Information Table which includes contact information.
- Other information regarding JCAN

http://www.jipdec.or.jp/repository/

- パブリックルート CA 証明書とサブ CA 証明書
- 最新 2 世代の本 CP
- 認定 LRA 属性情報テーブル (コンタクト情報含む)
- JCAN に関するその他の情報

http://www.jipdec.or.jp/repository/

2.3 Time and Frequency of Publication (公開の時期と頻度)

Updated this CP and Accredited LRA attribute Information are published after approval by PAA.

CRL is updated periodically and every change within the validity period.

The information of revocation is listed in CRL at least until the certificate expiration.

Accredited LRA revokes the JCAN certificates within 72 hours based on section 4.9 and publishes CRL.

Update frequency of the CRL is within 72 hours.

本 CP 及び認定 LRA 属性情報は、ポリシ管理局の承認後公開される。

CRL は、有効期限内で定期的及び変更毎に更新される。

失効情報は、少なくとも証明書の有効期間満了まで CRL に記載される。

認定 LRA は、4.9 節に基づき、72 時間以内に JCAN 証明書を失効し、CRL を公開する。

CRL の更新頻度は 72 時間以内である。

2.4 Access controls on repositories (リポジトリのアクセス管理)

JCAN keeps its repository available to the public.

JCAN は当該リポジトリを公開する。

3. Identification and Authentication (識別と認証)

3.1 Naming (名前決定)

JCAN follows the subscribers' specific names, including the type of names allocated by a Subject such as Distinguished Names defined in X.500, Names defined in RFC 822, and Names defined in X.400. JCAN follows the regulation of personal identification in order to identify the subscriber. When applying for the JCAN Certificates, the name of the subscriber shall be structured as prescribed in this CP.

Furthermore, the name of the issuer of JCAN Certificates shall be an official name.

JCAN は、利用者を本人識別するために、例えば X.500 の Distinguished Names、RFC 822 の Names、及び X.400 の Names のように、サブジェクトに割り当てられた名前のタイプを含む、特定の命名と本人識別の規則に従う。

JCAN 証明書を申請する場合、利用者の名前は、本 CP で規定された名称でなければならない。

なお、JCAN 証明書の発行者の名前は、正式な名称でなければならない。

3.2 Initial Identity Validation (初回の本人確認)

3.2.1 Validation of Organization (組織の確認)

JCAN authenticates The Organization. Authentication is carried out by whatever method JCAN deems reliable. This includes verification of the existence of The Organization concerned, Standard Company Code, JAPAN Corporate Number, official documents issued by state and local governments, reliable database which the state and/or the local public body manages (hereinafter, QGIS) and Third party databases (hereinafter, QIIS) which JCAN relies on.

JCAN は、サブジェクトの organization として登録される認定 LRA の組織を認証する。当該組織の実在性、標準企業コード、法人番号、国や地方公共団体が発行する公的書類、国や地方公共団体が管理する信頼できるデータベース(以下「QGIS」という)、JCAN が信頼する第三者データベース(以下「QIIS」という)等を用いて、JCAN が、信頼性があると判断した方法によって実施する。

3.2.2 Validation of Subject (サブジェクトの確認)

When JCAN Certificates are issued, Accredited LRA authenticates subjects as below. Accredited LRA accepts all of the responsibilities regarding an Authentication of a Subject.

JCAN 証明書の発行に際して、認定 LRA が下記のサブジェクトの認証を行う。本人認証に関わる全ての責任は認定 LRA が負う。

(1) JCAN Advanced

Accredited LRA validates a subject by the following one or more credible documents or their copies/databases (Personnel Roster, etc.):

- a copy of a resident's card;
- Individual Number Card
- notice of local tax special levy determination;
- employment insurance;
- resident's tax;
- tax exemption;
- insurance premium deduction;
- reliable documents with validity periods, such as Health Insurance Cards, Driver's licenses or Passports; or
- Reliable digital certificate

① When a name (real name or puseudnym name) is recorded into CommonName, Accredited LRA validates the name by avobe one or more credible documents or their copies/databases.

② When a organization name is recorded into OrganoizationUnitName2 and/or CommonName, Accredited LRA validates the organization name by the following one or more credible documents or their copies/databases.

- Reliable databases; or
- The above credible documents.

③ When a E-Mail Address is recorded into rfc822Name, Accredited LRA validates the E-Mail Address by the digital document which indicated that the E-Mail Address has been recorded by the organization.

以下のいずれかの信頼できる書類又はそのコピー/データベース（人事台帳等）でサブジェクトの確認を行う。

- 住民票の写し
- マイナンバーカード(個人番号カード)
- 地方税特別徴収税額決定通知書
- 雇用保険被保険者
- 住民税
- 扶養控除
- 保険料控除情報

- 保険証、運転免許証、パスポート等の有効期間がある公的証明書を根拠資料
- 信頼できるデジタル証明書

① CommonName に名前（実名又は PS 名）を記載する場合、上記信頼できる書類又はそのコピー/データベースで当該名の確認を行う。

② OrganoizationUnitName2 and/or CommonName に組織名を記載する場合、以下のいずれかの信頼できる書類又はそのコピー/データベースで当該組織名の確認を行う。

- 信頼されるデータベース
- 上記信頼できる書類

③ rfc822Name に E-Mail アドレスを記載する場合、E-Mail アドレスが当該組織に登録されていることの確認を行う。

(2) JCAN Basic

Accredited LRA validates the “subjects attributes" by the following one or more documents, their copies, databases or data (which indicated that the PARTNER’s affiliation organization has managed the data which will record in the JCAN Certificates such as organization name, name, E-Mail Address or OBJECT):

①When a name (real name or puseudnym name) is recorded into CommonName

- Employee ID Card, Sudent ID Card,etc;
- Reliable databases;
- Effective and No-Revocated Credit Cards; or
- The credible document shown in JCAN Advanced.

NOTE) It is not necessary to validate puseudnym name.

② When a organization name is recorded into OrganoizationUnitName2 and/or CommonName

- Reliable databases; or
- The credible document shown in JCAN Advanced.

③ When a OBJECT names or identifiers is recorded into OrganoizationUnitName2 and/or CommonName

- The digital document which indicated that the PARTNER’s affiliation organization has managed the object

④ When a E-Mail Address is recorded into rfc822Name

- The digital document which indicated that the PARTNER’s affiliation organization has managed the E-Mail Address

認定 LRA は、次の１つ以上の書類、そのコピー、データベース、データ（パートナの所属組織が証明書記載事項（組織名、名前、E-Mail アドレス、オブジェクト）を管理していることを示したもの）で「サブジェクトの属性」の確認を行う：

①CommonName に名前（実名又は PS 名）を記載する場合

- 社員証、学生証等
- 信頼されるデータベース
- 有効で失効されていないクレジットカード
- JCAN アドバンストに示す信頼できる書類

注）PS 名の確認は不要

②OrganoizationUnitName2 and/or CommonName に組織名を記載する場合

- 信頼されるデータベース
- JCAN アドバンストに示す信頼できる書類

③OrganoizationUnitName2 and/or CommonName にオブジェクトの名前、識別子を記載する場合

- パートナの所属組織が当該オブジェクトを管理していることを示した電子文書

④ rfc822Name に E-Mail アドレスを記載する場合

- パートナの所属組織が当該 E-Mail アドレスを管理していることを示した電子文書

3.2.3 Required Information for Subject's Registration (サブジェクトの登録に必要な情報)

Information required for Subject's registration are the documents, copies databases or data (which indicated that the PARTNER's affiliation organization has managed the data which will record in the JCAN Certificates) shown in 3.2.2.

The Information and "30-5600 Certificate Life-Cycle Roster" are archived as papers or data except the case where the information are archived in other department of the ORGANIZATION.

サブジェクトの登録に使用される情報は、3.2.2 に示した書類、コピー、データベース、データ（パートナの所属組織が証明書記載事項を管理していることを示したもの）である。

当該情報及び「30-5600 管理台帳」は、当該組織の他部門で保管されている場合を除き、紙又はデータとして保管される。

3.3 Identification of Subscribers for Re-Key Requests (鍵の再生成申請時の利用者の本人確認)

Identification of subject for Re-Key Requests is based on "30-5600 Certificate Life-Cycle Roster" except when the certificate is revocated or changed.

When the certificate is revocated or changed, identification of subject for Re-Key Requests is based on 3.2.2.

証明書が失効されたか変更された場合を除き、鍵更新要求の本人確認は、「30-5600 管理台帳」

に基づく。

証明書が失効されたか変更された場合は、鍵更新要求の本人確認は 3.2.2 に規定する。

3.4 Identification and Authentication for Revocation Requests (失効申請時の本人性確認と認証)

For the identification and authentication procedures of revocation requests of the JCAN certificate, Accredited LRA validates the revocation request by comparing it with the recorded information of “30-5600 Certificate Life-Cycle Roster”.

JCAN 証明書の失効要求における本人識別と認証手続として、認定 LRA は、「30-5600 管理台帳」記載情報による照合で失効申請の認証を行う。

4. Certificate Life-Cycle Operational Requirements (証明書ライフサイクルの運用要件)

4.1 Certificate Application (証明書申請)

Accredited LRA has the duty to provide the JCAN Public CA with accurate information on certificate request it lodges on behalf of the applicants.

認定 LRA は、申請者に代わって提出する証明書要求において、JCAN パブリック CA に正確な情報を提出する義務を負う。

4.2 Certificate Application Processing (証明書申請手順)

Upon the request of a certificate, Accredited LRA verifies the subjects and user based on section 3.2, and approves or rejects the application.

認定 LRA は、証明書の申請があった場合、セクション 3.2 に基づいてサブジェクトの識別と使用者の確認を行い、当該申請を承認又は棄却する。

4.3 Certificate Issuance (証明書発行)

After verification of Certificate application, Accredited LRA submits securely the Certificate issuance request to the JCAN Public CA.

If there is no problem in the request, JCAN Public CA issues and distributes JCAN certificates in the following procedure:

- When PIN is included in the request, JCAN Public CA generates Key Pairs securely, issues certificates, make PKCS#12 file and enable to download the file. Then Accredited LRA downloads and lent out the file to user;
- When PIN is not included in the request, JCAN Public CA generates Key Pairs securely, issues certificates, make PKCS#12 file and enable to download the file after input PIN from user.
  Then the user download the file directly.

After certificate issuance, Accredited LRA records user name in "30-5600 Certificate Life-Cycle Roster" and archives the copy.

証明書申請の検証後、認定 LRA は、JCAN パブリック CA に証明書発行の要求をセキュアに送信する。

JCAN パブリック CA は、証明書発行の要求に問題がなければ、次の手順で証明書を発行し配

送する。

- 証明書発行の要求に PIN が含まれている場合、JCAN パブリック CA は、鍵ペアをセキュアに生成し、証明書を発行し、PKCS#12 ファイルをダウンロードさせる。その後、認定 LRA は、JCAN 証明書をダウンロードし使用者に貸与する。
- 証明書発行の要求に PIN が含まれていない場合、JCAN パブリック CA は、利用者からの PIN 入力後、鍵ペアをセキュアに生成し、証明書を発行し、PKCS#12 ファイルにして、ダウンロード可能とする。
  その後、使用者は、JCAN 証明書を直接ダウンロードする。

証明書の発行後、認定 LRA は、使用者名を「30-5600 管理台帳」に記録し、そのコピーを保管する。

4.4 Certificate Acceptance (証明書の受領)

The issued certificate is deemed as accepted by the following:

- When PIN is included in the request, the time of the accredited LRA finishes download the certificates;
- When PIN is not included in the request, the time of the subscriber finishes download the certificate.

NOTE) Issued certificate is erased from download server after a fixed period.

発行された証明書は、次により利用者が受領したとみなす。

- 当該要求に PIN が含まれている場合は、認定 LRA がダウンロードを終えた時
- 当該要求に PIN が含まれていない場合は、利用者がダウンロードを終えた時

注）発行された証明書は、一定期間後、ダウンロードサーバから消去される。

4.5 Key Pair and Certificate Usage (鍵ペアと証明書の用途)

4.5.1 Usage of Private Key and Certificate by Subscriber (利用者による秘密鍵、及び証明書の使用)

The obligations are described section 1.3.

義務はセクション 1.3 参照

4.5.2 Relying Party Public Key and Certificate Usage (検証者による公開鍵、及び証明書の使用)

The obligations are described section 1.3.

義務はセクション 1.3 参照

4.6 Certificate Renewal (証明書の更新)

Accredited LRA can renew certificate based on "30-5600 Certificate Life-Cycle Roster" except when the certificate is revocated or changed certificates renewal shall follow the same process as section 4.1-4.4.

証明書が失効されたか変更された場合を除き、認定 LRA は、「30-5600 管理台帳」に基づき証明書の更新を行うことができる。

証明書が失効されたか変更された場合は、証明書の更新は、セクション 4.1-4.4 と同じ方法による。

4.7 Certificate Re-key (証明書の鍵の再生成)

JCAN Certificates will only be renewed if the private key is also renewed. The renewal of the certificates shall follow the same process as section 4.6.

JCAN 証明書は、鍵更新を伴わない証明書の更新には対応しない。証明書の更新は、セクション 4.6 と同じ方法による。

4.8 Certificate Modification (証明書の変更)

Certificates modification is not applicable.

証明書の変更は、適用しない。

4.9 Certificate Revocation (証明書の失効)

When the contact from subscribers by E-Mail concerning following matters is accepted, Accredited LRA revokes the JCAN certificates promptry after checking based on section 3.4:

- Any Changes of the data recorded in the JCAN Certificates;
- Loss or theft of PC or Media in which JCAN Certificates are installed.
- When the reliability of the JCAN Certificates may be damaged.

Accredited LRA and JCAN Public CA revoke the JCAN certificates by their decision if:

- The subject is unrelated to the ORGANIZATION in the case of retirement, withdrawal, disposal, etc.;
- Subscriber has breached obligations under this CP and Accredited LRA's rule;
- An error or false is recorded in the JCAN Certificate;

- Private Key or CA Private Key becomes compromised;
- The Accreditation of LRA becomes invalid;
- JCAN Public CA terminates service;
- Accredited LRA, JCAN Public CA and JIPDEC decide to revoke for other reasons.

After revocation, Accedited LRA or JCAN Public CA inform by E-Mail to subscribers about the revocation from Accredited LRA.

Once a certificate is revoked, it shall not be reinstated.

The integrity and authenticity of CRL shall be protected.

利用者からの次の事項に係るメールによる連絡を受付けた場合、認定 LRA は、3.4 節に基づく確認後、速やかに JCAN 証明書を失効する。

- JCAN 証明書の記載事項の変更
- JCAN 証明書がインストールされた PC 又は媒体の紛失、盗難
- 証明書の信頼性が損なわれる可能性がある場合

次の場合、認定 LRA 及び JCAN パブリック CA は、自己の判断で JCAN 証明書を失効する。

- 退職、脱退、廃棄等によりサブジェクトが当該組織と無関係になった
- 利用者が本 CP 及び認定 LRA の規則の義務に違反した
- JCAN 証明書に誤り又は虚偽が記載されている
- 秘密鍵又は CA 秘密鍵が危殆化した
- LRA の認定が無効になった
- JCAN パブリック CA がサービスを終了する
- 認定 LRA、JCAN パブリック CA 及び JIPDEC がその他の理由で失効を決定した

失効後、認定 LRA 又は JCAN パブリック CA は、認定 LRA から利用者に失効の通知をメールで行う。

一旦証明書が失効されたら、復旧されない。

CRL の完全性と真正性は保護される。

4.10 Certificate Status Services (証明書のステータス確認サービス)

JCAN Public CA publishes provides CRLs to the Subscribers as well as to the Relying Parties. JCAN Public CA offers certificate status confirmation services including Web interfaces to Accredited LRAs.

JCAN パブリック CA は、利用者及び検証者に対して、CRL を提供する。JCAN パブリック

CA は認定 LRA に対して、ウェブインタフェースを含む、証明書ステータス確認サービスを提供する。

4.11 End of subscription (利用の終了)

Subscription of JCAN certificate ends when a certificate is revoked, expired, or the service is terminated.

JCAN 証明書の利用は、証明書の失効、有効期限切れ、又はサービスが終了したときに終了する。

5. Management, Operational, and Physical Controls (管理的、運用的、物理的管理策)

5.1 Physical Security Controls (物理的管理)

This chapter is prescribed in [OP -LRA] and [CPS] of JCAN Public CA.

本章は、[OP-LRA]及び JCAN パブリック CA の[CPS]で規定する。

5.2 Procedural Controls (手続的管理)

This chapter is prescribed in [OP -LRA] and [CPS] of JCAN Public CA.

本章は、[OP-LRA]及び JCAN パブリック CA の[CPS]で規定する。

5.3 Personnel Controls (人事的管理)

This chapter is prescribed in [OP -LRA] and [CPS] of JCAN Public CA.

本章は、[OP-LRA]及び JCAN パブリック CA の[CPS]で規定する。

5.4 Audit Logging Procedures (監査ログの手続)

This chapter is prescribed in [OP -LRA] and [CPS] of JCAN Public CA.

本章は、[OP-LRA]及び JCAN パブリック CA の[CPS]で規定する。

5.5 Records Archival（記録のアーカイブ）

5.5.1 Types of Records Archived（アーカイブされる記録の種類）

Accredited LRA maintains the archived information through reliable methods.

認定 LRA は、保管情報を、信頼性のある方法で保持する。

5.5.2 Retention Period for Archive（アーカイブ保存期間）

Accredited LRA retains records of information required for Subject's registration for at least 7 years after the Certificate is expired or revoked.

Accredited LRA retains records of logs at least 1 year.

認定 LRA は、サブジェクトの登録に使用される情報を、有効期限切れ後、又は失効後、少なくとも 7 年間保持する。

認定 LRA は、ログ情報を、少なくとも 1 年間保持する。

5.6 Key Changeover（鍵の切り替え）

This chapter is prescribed in [CPS] of JCAN Public CA.

本章は、JCAN パブリック CA の[CPS]で規定する。

5.7 Compromise and Disaster Recovery（危殆化、及び災害からの復旧）

This chapter is prescribed in [CPS] of JCAN Public CA.

本章は、JCAN パブリック CA の[CPS]で規定する。

5.8 Termination of CA or RA（CA 又は登録局の終了）

This chapter is prescribed in [CPS] of JCAN Public CA.

本章は、JCAN パブリック CA の[CPS]で規定する。

6. Technical Security Controls (技術的セキュリティ管理策)

This chapter is prescribed on [CPS] of JCAN Public CA.

本章は、JCAN パブリック CA の[CPS]で規定する。

7. Certificate and CRL Profiles (証明書、及び CRL のプロファイル)

7.1 Certificate Profile (証明書プロファイル)

The profile of JCAN certificate bases on the X.509 Version 3 Format and the following [SEMI]. Other information are prescribed in JCAN Repository and [CPS] of JCAN Public CA.

JCAN certificate's max validity period is 39 months.

JCAN and accredited LRA ensure that over the life time of the CA a distinguished name which has been used in a certificate by it is never re-assigned to another entity.

JCAN 証明書のプロファイルは、X.509 バージョン 3 フォーマット及び次の[SEMI]に基づく。その他の情報は、JCAN リポジトリと JCAN パブリック CA の[CPS]で規定する。

JCAN 証明書は、有効期間は最大 39 ヶ月である。

JCAN と認定 LRA は、CA が存在する間、識別名を別の実体に決して再び割り当てないことを確実にする。

Certificate Fields	Data type (number of characters)	Definition • It shall use alphanumeric characters (capital letters are included), HYPHEN, SPACE, and PERIOD.	Remarks
Basic Certificate Fields : Subject			
CountryName	Printable String (2)	Mandatory: • The two character country code in alpha-2 of ISO3166-1 • All capital letter	Set by JCAN based on LRA accreditation
StateName	Printable String (128)	Mandatory[#1]: • Name of State, Province, etc. • A head character is a capital letter	Set by JCAN based on LRA accreditation
LocalityName	Printable String (128)	Mandatory[#2]: • Name of City, etc. • A head character is a capital letter • A delimiter is a hyphen	Set by JCAN based on LRA accreditation
OrganizationName	Printable String (64)	Mandatory[#3]: • Name of Organization.	Set by JCAN based on LRA accreditation
OrganizationUnitName1	Printable String (64)	Mandatory[#4]: • Unique number, which CSB manages. • This value shall be set up together with OrganizationUnitName2 so that this certificate shall become unique. • In order to distinguish in automatic tracking, it shall attach the Prefix “OU1-”.	Set by JCAN based on LRA accreditation
OrganizationUnitName2	Printable String (64)	Option[#5 #6 #7]: • Local number which organization manages. • In order to distinguish in automatic tracking, it shall attach the Prefix “OU2-”.	Set by Accredited LRA
CommonName	Printable String (64)	Mandatory: • Subject’s name (real name, section name, role or ID). • In order to distinguish in automatic tracking, it shall attach the prefix “BN-” (business name which used as a formal common name in the organization, such as a real name and maiden name), “BO-” (organization/role), or “ID-”	Set by Accredited LRA NOTE) About pseudonym, • it shall attach the prefix “PN- ”.
Standard Certificate Extensions : subjectAltName			
rfc822Name	IA5String (255)	Option: • Subject's e-mail address	Set by Accredited LRA

#1 it may be SPACE, because reservation of a memory space is aim of mandatory.
#2 it may be SPACE, because reservation of a memory space is aim of mandatory
#3 it registered in DUNS, etc.
#4 it can use as a pointer to the open attribute information (the company name, etc. which cannot be written with the alphabet), which could not be recorded on the certificate.
#5 it can use as a pointer to the secret attribute information (section name, etc.), which could not be recorded on the certificate.
#6 it may set up values other than a pointer use.
#7 it may be SPACE, because reservation of a memory space is aim of mandatory.

7.2 CRL Profile (CRL プロファイル)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

8. Compliance Audit and Other Assessment (準拠性監査とその他の評価)

8.1 Frequency and Requirement of Audit (監査の頻度あるいは条件)

Accredited LRA follows the compliance auditing practices and procedures in order to guarantee that the service conforms to this CP requirements, standards, procedures, and service levels at least once a year.

Audit of JCAN Public CA is prescribed in [CPS]

認定 LRA は、年に 1 回以上、本サービスが、本 CP の要件、標準、手続、及びサービスレベルに適合していることを保証するために、準拠性監査を受諾する。

JCAN パブリック CA の監査は、[CPS]による。

8.2 Auditor's Identity and Qualification (監査人の身元・資格)

Compliance audit is carried out by auditors with strong auditing backgrounds.

準拠性監査は、十分な監査経験を有する監査人が行うものとする。

8.3 Relationship between Auditors and Non-auditing sectors (監査人と被監査部門の関係)

The auditor appointed will be independent and will not be affiliated directly or indirectly in any way with the non-auditing sector besides carrying out the audits.

監査人は、監査に関する事項を除き、被監査部門の業務から独立した立場にあるものとする。

8.4 Audit processing matters (監査で扱われる事項)

Audit of Accredited LRA is based on this CP.

Audit of JCAN Public CA is prescribed in [CPS]

認定 LRA の監査は、本 CP の準拠性を中心に行われる。

JCAN パブリック CA の監査は、[CPS]による。

9. Other Business and Legal Matters (他の業務上の問題、及び法的問題)

9.1 Fees (料金)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.2 Financial Responsibility (財務的責任)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.3 Confidentiality of Business Information (業務情報の機密性)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.4 Privacy of Personal Information (個人情報のプライバシー保護)

Personal information which Accredited LRA maintains is following the concerning law of the country if any.

Personal information which Accredited LRA maintains is regarded as confidential except for public items such as certificates and CRL. These are disclosed intentionally.

認定 LRA が保持する個人情報は、もしあればその国の関係する法律に従うこと。

認定 LRA が保持する個人情報は、証明書、CRL として明示的に公表されるものを除き、機密保持対象として取扱われる。

9.5 Intellectual Property Rights (知的財産権)

JIPDEC owns and reserves all intellectual property rights associated with publications originating from JIPDEC. This includes this CP.

本 CP を含み JIPDEC が発行するすべての刊行物の知的財産権について、JIPDEC はその権利を留保する。

9.6 Representations and Warranties (表明保証)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.7 Disclaimers of Warranties (無保証)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.8 Limitations of Liability (責任の制限)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.9 Indemnities (補償)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.10 Term and Termination (期間と終了)

This CP remains in force until notice of the opposite is communicated by JCAN repository.

本 CP は、JCAN リポジトリ上に、効力がなくなったと通知されるまで、効力を持ち続ける。

9.11 Individual notices and communications with participants (関係者間の個別通知と連絡)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.12 Amendments (改訂)

This CP shall be updated on an annual basis.

This document is amended by “a member of JCAN Secretariat (Author)”, reviewed by PAA and finally approved by “Certification Authority Manager (Approver)”.

When it is amended, it is disclosed to the JCAN Repository after notified to the parties such as Subscribers and QuaClified Auditors in principle, if there is no opinion within 15 days.

本 CP は、基本的に毎年更新を行う。

改訂は、JCAN 事務局のメンバー（作成者）が修正し、ポリシ管理局がレビューし、最後に JCAN 事務局の認証局責任者が承認する。

改訂した場合は、原則として利用者及び Qualified Auditor 等関係者に通知し、15 日以内に意見がなければ JCAN リポジトリに公開する。

9.13 Dispute Resolution Procedures (紛争解決手続)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.14 Governing Law (準拠法)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.15 Compliance with Applicable Law (適用法の遵守)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.16 Miscellaneous Provisions (雑則)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

9.17 Other Provisions (他の条項)

This section is prescribed on [CPS] of JCAN Public CA.

本節は、JCAN パブリック CA の[CPS]で規定する。

10. Definitions (定義語)

Accredited CA (認定 CA)

Accredited CA is a CA that is accredited by JCAN.

認定 CA は、JCAN が認定した CA である。

Accredited LRA (認定 LRA)

Accredited LRA is the LRA which JCAN accredited as are subscriber's representative. Accredited LRA vets the authenticity of the DN and verifies the identity of the subscriber of JCAN Certificates. Furthermore, the Accredited LRA operates the certificate life-cycle management (issue, revoke) of the certificate under JCAN Certificate Policy.

認定 LRA とは、利用者の代表として JCAN が認定した LRA であり、JCAN 証明書ポリシの下、JCAN 証明書に記載する DN の真正性の審査と利用者の本人認証を行い、証明書のライフサイクルマネージメント（発行、失効）を行う。

CA（認証局）

A constituent that issues, renews or revokes a certificate and create a CA (Certification Authority) key.

証明書の発行・更新・失効、CA 鍵の生成を行う主体をいう。

Certificate Applicants (証明書申請者)

Certificate applicants are those whom a person in charge of the Accredited LRA designated. A certificate applicant is a person who applies for a certificate on behalf of the subject.

証明書申請者は、認定 LRA の責任者が指名した者。
証明書申請者は、サブジェクトの代わりに証明書を申請する者である。

Certificate Profile (証明書プロファイル)

The certificate usages are specified in x.509 certificate.

汎用的な x.509 証明書に対して、証明書の使用方法等が明記されているものをいう。

CP (証明書ポリシ)

CP (Certificate Policy) which is regulation documents regarding types of certificates, application, subject of issuance, usage CA issues.

CA が発行する証明書の種類、適用範囲、発行対象、用途等、証明書に関する規程文書をいう。

CPS (認証業務運用規程)

CPS (Certification Practice Statement) is documents where are expressed a statement of the practices in CA and management process and security standards.

CA を運用するうえでの運用手続きやセキュリティ基準を明示した文書をいう。

CRL (証明書失効リスト)

CRL (Certificate Revocation List) is a list recorded by the CA of certificates that are revoked before their expiration time.

証明書の有効期間内にも拘わらず失効された証明書情報を記録したリストをいう。

CSR (証明書署名要求)

CSR (Certificate Signing Request) is a machine-readable application form to request a digital certificate. It is sent from Accredited LRA to CA.

If there is a request of the creation of a key pair at CA, CSR and a key pair is created at RA and CSR is sent to Issuing Authority

認定 LRA から CA へ、電子証明書を要求する際に送られる機械可読の申込書式をいう。

なお、CA での鍵ペア生成を要求された場合は、登録局で鍵ペアと CSR を生成し、発行局に CSR を送付する。

EE (エンドエンティティ)

EE (End Entity) is a subject of JCAN Certificates.

EE は、JCAN 証明書のサブジェクトである。

Issuing CA （イシュイング CA)

CA which issues the JCAN Certificates is signed by upper CAs.

上位 CA により署名され、JCAN 証明書を発行する CA である。

JCAN Certificate (JCAN 証明書)

JCAN Certificates can be used for authentication, encryption and digital signature.
When using a JCAN Certificate, it is following the law of the country if any.

JCAN 証明書は、認証、暗号化、署名で使用できる。
JCAN 証明書を使う場合は、もしあればその国の法律に従うこと。

JCAN Public CA (JCAN パブリック CA)

JCAN Public CA is consist of Accredited CAs,and is Sub CA of Public Root CA..

JCAN パブリック CA は、認定 CA で構成され、パブリックルート CA のサブ CA である。

LDAP

LDAP (Lightweight Directory Access Protocol) is the protocol for accessing directory databases which disclose information such as E-Mail addresses.

メールアドレス等を公開するディレクトリデータベースにアクセスするためのプロトコル

LRA (ローカル登録局)

LRA (Local Registration Authority) is an optional part of a public key infrastructure that authenticates a subject and revockes a certificate.

PKI(公開鍵基盤)の一部組織でサブジェクトの認証と証明書の失効を行う。

LRA Operator Certificate (LRA オペレータ証明書)

LRA Operator Certificate is the certificate issued by a designated JCAN Public CA to a person who is assigned by Accredited LRA.
This certificate is used for access of certificate management services, such as issue of JCAN certificates.

LRA オペレータ証明書は、認定 LRA が指名する人に、JCAN パブリック CA より発行される LRA 操作責任者用の証明書である。
この証明書は JCAN 証明書の発行など証明書管理サービスのアクセスに用いる。

MEMBER (メンバ)

MEMBER is the ORGANIZATION's internal person.

当該組織の企業内個人。

ORGANIZATION (当該組織)

ORGANIZATION is the organization which operates LRA.

LRA を運用する組織。

PARSON (人)

PERSON is a natural person.

自然人。

PARTNER (パートナ)

PARTNER is the ORGANIZATION's external person (member which is privity of contract, capital relations, membership, committee or guest, student, person who authenticated by credible document, person who registed his/her credit card, etc.).

パートナは、当該組織の外部の人（契約関係、資本関係、会員、委員会の構成員、或いは客員、学生、信頼できる書類で認証した人、クレジットカードを登録した人等）

PKCS#12

Encrypted package format of certificate and private key using PIN

PIN を用いて秘密鍵を含む証明書の暗号化パッケージ

Public Root CA (パブリックルート CA)

Root CAs which are registered in the trusted CA list by general Browsers.

一般的なブラウザの信頼される認証機関に登録されたルート CA をいう。

QGIS (行政機関の信頼情報源)

QGIS (Qualified Government Information Source) is a Trustworthy Government Information Source approved by the EV Guidelines, CA/Browser Forum.

It is a database managed by the government and is published online and updated regularly. The reporting of the data is an obligation under law and a false report will lead to criminal and civil punishment.

EV ガイドラインで認められている「信頼できる行政機関の情報源」をいう。オンラインで公開され、定期的に更新される、行政機関が運営するデータベースで、データの報告が法律で義務付けられ、虚偽の報告には刑事罰または民事罰が科せられるものをいう。

QIIS (第三者機関の信頼情報源)

QIIS (Qualified Independent Information Source) is a Trustworthy Independent Information Source approved by the EV Guidelines, CA/Browser Forum. It is a database published online and updated regularly, and managed by a private organization.

EV ガイドラインで認められている「信頼できる独立した第三機関の情報源」をいう。オンラインで公開され、定期的に更新される民間機関が運営するデータベースをいう。

RA (登録局)

RA (Registration Authority), in a network, that verifies Accredited LRA requests for a certificate and tells the CA to issue it.

ネットワークにおける登録局で、認定 LRA からの証明書の要求に対し、この身分証明作業を行い、CA に発行依頼を行います。

Relying Party (検証者)

Relying Party is a person that rely on a subscriber's certificate and/or a subscriber's digital signature. Relying Party shall refer to the revocation information of the CA in order to verify the validity of JCAN certificate.

検証者は、利用者の証明書を信頼する者、又は利用者の電子署名を信頼する者である。JCAN 証明書の有効性を検証するために、検証者は必ず CRL を参照しなければならない。

Repository (リポジトリ)

Repository is a database and/or directory listing certificates and other relevant information accessible on-line.

証明書及び他の関連情報を列挙する、オンラインで利用できるデータベース及び/又はディレクトリをいう。

ROBINS (ロビンズ)

ROBINS is a business entity database published online and updated regularly, and managed by JIPDEC

オンラインで公開され定期的に更新される JIPDEC が管理する企業データベース。

Root CA (ルート CA)

Root CA is an Authority which has the authority and responsibility to create and develop the policy of the certificates.

証明書のポリシを起草する権限と責任を負うポリシ管理局である。

Sub CA (サブ CA)

CA which is certified its authenticity by upper CAs.

上位の CA による認証を受けることにより自らの正当性を認証する CA をいう。

Subjects (サブジェクト)

It is the target for certificate issuance.

The Subjects of JCAN Certificates are prescribed in section 1.4.

証明書発行対象

JCAN 証明書のサブジェクトは、セクション 1.4 で規定する。

X.400

One of the recommendations of ITU-TS and is the prescribed standard for digital mail.

ITU-TS の勧告の一つで電子メールについての標準を定めたもの。

X.500

X.509 prescribes the standard format of public key authentication.

ITU-T が定めた、ネットワーク上での分散ディレクトリサービスに関する規格。X.509 は公開鍵認証の標準形式を規定している。