JCAN Public CA CPS

(Certification Practice Statement)

JCAN パブリック CA CPS

(認証業務運用規程)

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)
3.1	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 (CPS) is applied to Issuing CA which issues JCAN Certificates, and prescribes Issuing CA's procedures and operations such as issuance and revocation of certificates.

Issuing CA (Outsource organizations are included) has a system for quality and information security management appropriate.

The policy of JCAN Certificates is prescribed in [CP].

This CPS 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).

JIPDEC outsources the operation of this CA to Global Sign K.K. (Address: Shibuya-ku, Tokyo).

本書(CPS)は、JCAN 証明書を発行するイシュイング CA に適用され、イシュイング CA の証明書の発行及び失効等の手続と運用を規定するものである。

イシュイング CA（委託先を含む）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。

JCAN 証明書のポリシは、[CP]に規定する。

本 CPS は、JCAN によって管理される。

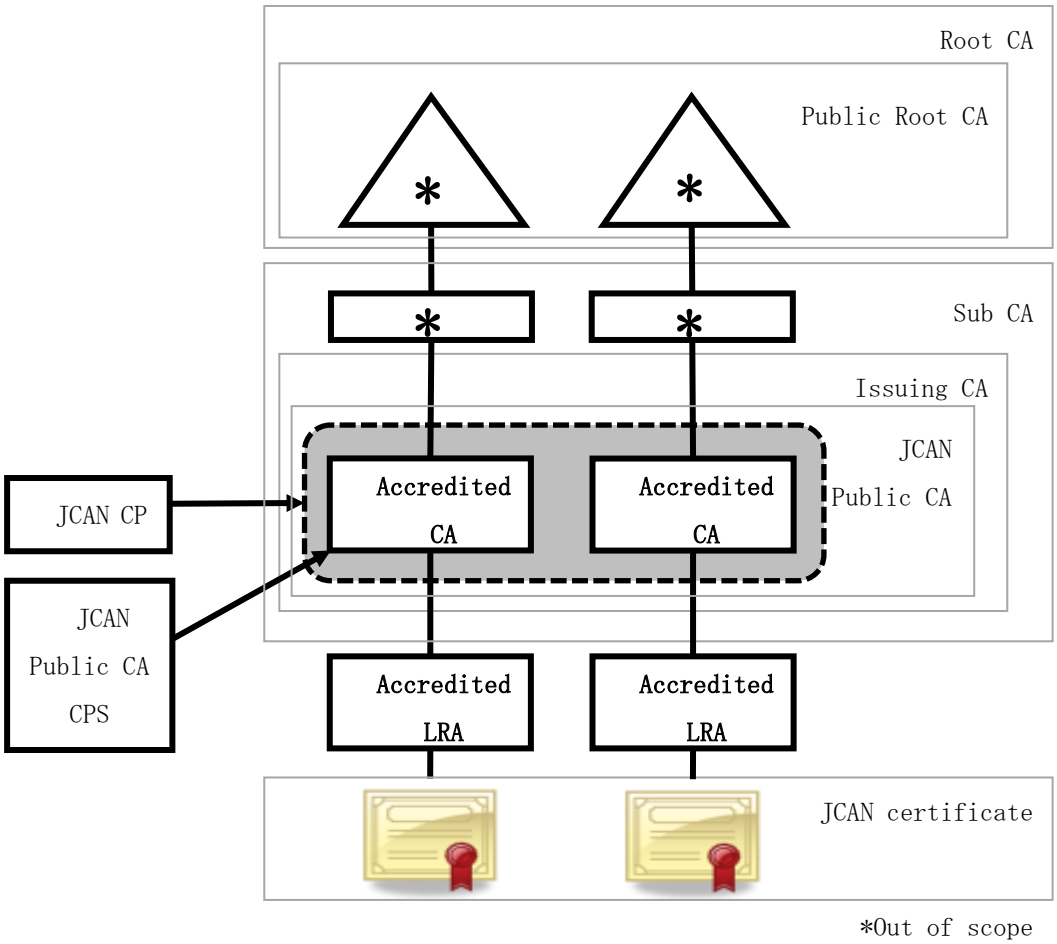
JCAN は、一般財団法人日本情報経済社会推進協会（所在地：東京都港区、商業登記番号：010405009403、法人番号：1010405009403、以下「JIPDEC」という）が運用する民間制度である。

なお、JIPDEC は、GMO グローバルサイン株式会社（所在地：東京都渋谷区）に本 CA の運用を委託する。

1.1.1 PKI Framework (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.

1.3 PKI participants（PKI の関係者）

(1) Subscribers and users（利用者）

This clause is prescribed on [CP] of the certificate which this CA issues.

本項は、この CA が発行する証明書の[CP]に規定する。

(2) Accredited LRA（認定 LRA）

This clause is prescribed on [CP] of the certificate which this CA issues.

本項は、この CA が発行する証明書の[CP]に規定する。

(3) Relying Party（検証者）

This clause is prescribed on [CP] of the certificate which this CA issues.

本項は、この CA が発行する証明書の[CP]に規定する。

(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 LRA

This CA has operated under the Operating Contract which is signed by JIPDEC and Global Sign.

The obligations are the followings:

- JCAN Public CA makes Relying Party follow “30-5270 Relying Party Agreement”.
- After generating the pkcs#12 formatted certificate, JCAN Public CA protects the private key through the use of the PIN. No corresponding PIN is retained but is destroyed.
- JCAN Public CA guarantees the unique identification allotted to the subscribers within the domain of its JCAN Public CA;
- The confidentiality and integrity of registered data is ensured at all times.

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。

本 CA は、JIPDEC と Global Sign が署名した運用契約で運用されている。

義務は以下の通りである。

- JCAN パブリック CA は検証者に「30-5270 検証者規約」を守らせること。
- JCAN パブリック CA は、PKCS#12 形式証明書を生成したあとは、利用証明書の秘密鍵を PKCS#12 と PIN で保護し、対応する PIN は一切保存せず破棄する。
- JCAN パブリック CA は、JCAN パブリック CA の領域内において利用者に割り当てられた識別名の唯一性を保証する。
- 登録データの機密性と完全性は、常時、適切な手段によって保証される。

(5) JCAN（ジェイキャン）

This clause is prescribed on [CP] of the certificate which this CA issues.

本項は、この CA が発行する証明書の[CP]に規定する。

1.4 Certificate Usage（証明書の用途）

(1) JCAN Certificates (JCAN 証明書)

JCAN Certificates are prescribed on [CP] of certificates which this CA issues.

本章は、この CA が発行する証明書の[CP]に規定する。

(2) JCAN Public CA Certificate（JCAN パブリック CA 証明書）

JCAN Public CA Certificate is the followings:

- Sub CA certificate;
- Cross certification certificate.

JCAN パブリック CA 証明書は、次の証明書である。

- サブ CA 証明書
- 相互認証証明書

(3) LRA Operator Certificates (LRA オペレータ証明書)

LRA Operator Certificates are certificates issued to Accredited LRAs.

LRA Operator Certificates are used for access to “Designated CSB Service Site” at the time of JCAN Certificates’ issuance or revocation.

LRA Operator Certificates may be issue a CA except JCAN Public CA.

LRA オペレータ証明書は、認定 LRA に発行される証明書である。

LRA オペレータ証明書は、JCAN 証明書の発行/失効時に「指定 CSB サービスサイト」へのアクセスに用いる。

LRA オペレータ証明書は、JCAN パブリック CA 以外の CA から発行してもよい。

(4) Test Certificate (テスト証明書)

For the purpose of operational checking of JCAN Public CA, JCAN Public CA issues Test Certificate.

Any Certificate with the word TEST in the CommonName (CN=TEST …) is a designated Test Certificate.

The accuracy, authenticity, completeness or fitness of any information contained in these Test Certificate is not warranted.

JCAN パブリック CA の稼働確認を目的に、テスト証明書を発行する。

CommonName に TEST を含む証明書 (CN=TEST…) は、テスト証明書である。

テスト証明書に含まれる情報については、正確性、真正性、完全性、特定目的への適合性は保証されない。

1.5 Policy Administration (ポリシ管理)

1.5.1 Document administrator (文書管理)

PAA manages this CPS. The Authority is comprised of members as mentioned below:

- One(1) entrusted member of JCAN
- Two(2) entrusted member of Global Sign

Any approval or change of the Policy regarding this CPS shall be decided by PAA. Each member of PAA have one vote. In case of locked vote, the vote of the chairperson of PAA counts double.

本 CPS はポリシ管理局により管理され、以下のメンバで構成される。

- JCAN から委任されるメンバ 1 名
- Global Sign から委任されるメンバ 2 名

本 CPS を含むポリシの承認及び変更にはポリシ管理局の議決が必要である。全てのポリシ管理局メンバが 1 票の議決権をもつ。決議が割れた場合は、議長の票を 2 票と数える。

1.5.2 Contact Address (連絡先)

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)

[CP] 30-5300 JCAN Certificate Policy

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

1.7 Repository（リポジトリ）

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

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

JCAN は、本 CPS、[CP]、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 パブリック CA 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。

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

JCAN reserve the rights to publish the followings information in the respective online publicly accessible repositories to the certificate subscribers and relying parties:

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、証明書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。

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 CPS
- 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 CPS
- JCAN に関するその他の情報

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

(2) JCAN Public CA Repository（JCAN パブリック CA リポジトリ）

- Certificate Revocation List (“CRL”)
- Other information regarding certificates which JCAN Public CA issues

- 証明書失効リスト（CRL）
- JCAN パブリック CA が発行する証明書に関するその他の情報

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

Updated this CPS is 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.

本 CPS 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 に記載されている。

1.10 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。

2. Identification and Authentication（識別と認証）

This chapter is prescribed on [CP] of the certificate which this CA issues.

本章は、この CA が発行する証明書の[CP]に規定する。

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

This chapter is prescribed on [CP] of the certificate which this CA issues.

本章は、この CA が発行する証明書の[CP]に規定する。

4. Management, Operational, and Physical Controls (管理的運用的物理的管理策)

4.1 Physical Security Controls（物理的管理）

JCAN Public CA implements high-security controls within the data center. These include restricting personnel and physical access using electronic security mechanisms. Especially in certificate generation and revocation management, continuous monitoring and alarm facilities are provided to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

The Data Center implements measures which protect against waterdamage, earthquakes, fire, and other disasters and implements other structural measures to prevent physical damage to the facility.

The access to the CA implements is restricted to the members who are designated on the Access management list.

Visitors to the Data Center must always be accompanied by the members.

JCAN パブリック CA は、CA の設備の重要性に対応して、人的・物理的なアクセス制御と、電子的なセキュリティメカニズムをもつ高度なセキュリティコントロールを、データセンター内に設置する。特に証明書生成及び失効管理においては、継続的な監視と警報施設がそのリソースにアクセスする無許可のまたは不規則な試みを検出、登録、対応することを可能にするため設けられる。

データセンターは、水害、地震、火災、その他の災害を容易に受けない構造と防災措置を講じる。

CA 設備へのアクセスは、アクセス管理リストに記載されたメンバに制限する。

データセンターへの訪問者は、常に当該メンバに同伴されていなければならない。

4.2 Procedural Controls（手続的管理）

JCAN Public CA follows personnel practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties.

All JCAN Public CA personnel in trusted roles shall be free from Subscribers, Relying Parties, or other third parties by monetary or intervention from an inside and the outside that might prejudice the impartiality of the CA operations.

The trusted role of JCAN public CA is following.

Certification Authority Manager : The responsibility for all the necessary work concerning operation of CA.

The above provision is applied also to the outsource of JCAN public CA.

JCAN Public CA carries out a risk assessment to evaluate risks and determine the necessary security requirements and operational procedures. The risk analysis regularly reviewed and revised if necessary.

JCAN パブリック CA は、要員の信頼性と適性及び技術的な業務遂行について、合理的な保証を提供できる人事を実施する。

信頼される役割を担う JCAN パブリック CA の要員は、CA 運用の公平さを偏らすかもしれない金銭的な或いは内部及び外部からの圧力の影響を受けないものとする。

JCAN パブリック CA の信頼された役割には以下を含む。

・認証局責任者：本 CA の運用に係るすべての必要な作業の責任を負う。

上記規定は JCAN パブリック CA の委託先にも適用する。

JCAN パブリック CA は、リスクを評価し、必要なセキュリティ要求事項と運営手順を決定するためのリスクアセスメントを実施する。リスク分析は常時見直し、必要があれば修正する。

4.3 Personnel Controls（人事的管理）

4.3.1 Qualifications, Experience, Clearance Requirements（資格、経験及び身分の要件）

Employees employed under the employment standards of this CPS or equivalent contractor personnel are the personnel in trusted positions prescribed in Procedural Controls on section 5.2.

信任された役職につく要員は、セクション 5.2 にもとづいて採用され管理される。

4.3.2 Training Requirements（研修要件）

JCAN Public CA publishes training to their personnel assigned to carry out CA functions.

JCAN パブリック CA は、認証業務を実行するための研修を、その要員に実施する。

4.3.3 Retraining Frequency and Requirements（再研修の頻度及び要件）

Personnel are regularly retrained for the purpose of renewing and keeping the procedural knowledge.

手続についての知識の更新と維持を目的に、定期的な再研修をその要員に実施する。

4.3.4 Sanctions for Unauthorized Actions（認められていない行動に対する懲戒）

JCAN Public CA will take disciplinary actions toward personnel who perform

unauthorized actions, use unauthorized authority, or use unauthorized systems.

JCAN パブリック CA は、認められていない行動、認められていない権限の使用、認められていないシステムの使用をした要員に対し、適切でないと判断した時は懲戒を行うことがある。

4.3.5 Documentation Supplied to Personnel（要員に提供する資料）

JCAN Public CA publishes documents to personnel on the first day of training and between other training sessions.

JCAN パブリック CA は、初回の研修とその他の研修の期間、要員に対し資料を提供する。

4.4 Audit Logging Procedures（監査ログの手続）

JCAN Public CA shall implement Audit logging procedures. These include logging of audit events, and audit systems implemented for the purpose of keeping a secure environment.

JCAN Public CA records the following information from startup to shutdown of the CA system.

JCAN パブリック CA は、監査ログの手続を実施する。これには、セキュアな環境を維持する目的で実装されたイベントログと監査ツールのログを含む。

JCAN パブリック CA は、CA システムの起動からシステムシャットダウンまで次の情報を記録する。

4.4.1 Types of Logs to be Audited（監査するログの種類）

JCAN Public CA implements the following logs:

JCAN パブリック CA は、以下の記録を監査する。

(1) System Logs（システムに関するログ）

- Issuance of a certificate;
- Revocation of a certificate;
- Publishing of a CRL;
- Others (such as Logs containing local network components).

- CA 証明書の発行
- CA 証明書の失効
- CRL の公開

- その他（ネットワーク設備を含むログ等）

(2) Records regarding entry/exit and operation of CA private key（**入退室と CA 秘密鍵の操作に関する記録**）

- Record of CA facility visitor entry/exit;
- Records of operation and life-cycle management of CA private key.

- CA を設置する室への入退室記録
- 秘密鍵の操作に関する記録

4.4.2 Audit trail records contain（**監査ツールのログに含まれる項目**）

- The identification of the operation;
- The data and time of the operation;
- The identification of the certificate involved in the operation;
- The identification of the person that performed the operation;
- A reference to the request for the operation.

- 操作の識別
- 操作の日時、時刻
- 操作に含まれる証明書の識別
- 操作を実施した人の識別
- 操作要求に関する参照情報

4.4.3 Frequency of Processing Log（**監査ログを処理する頻度**）

Appointed personnel inspect the log file in regular intervals and detects and reports when there is an abnormal event.

一定の間隔で、指命された要員がログファイルを点検し、異常事象を検知し、報告できるようにする。

4.4.4 Storage and Protection of Records and Backup（**記録の保存と保護、及びバックアップ**）

The log files and auditing trails are recorded. These are appropriately protected using an Access Control Structure. These log files can only be accessed by a person appointed to JCAN Public CA or for the purpose of inspection by the appointed auditor.

The event logs cannot be easily deleted or destroyed within the period of time

that they are required to be held.

Backup containing sensitive data is securely disposed of when no longer required.

JCAN パブリック CA より任命された人、及び指定された監査人による検査のため、ログファイルと監査証跡は保存される。これらは、アクセス制御機構により適切に保護され、バックアップされる。

イベントログは、保持が要求される期間中に容易に削除されたり破壊されることができない。

機密データを含むバックアップは、必要とされない場合は安全に処理される。

4.5 Records Archival（記録のアーカイブ）

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

JCAN Public CA maintains the details of all CA Certificates, auditing data of issuance and revocation of CA Certificates, application information of CA Certificates, CRLs, log files, and other records which support the application of CA Certificates. These records are maintained through reliable methods.

The information maintained by Accredited LRA are prescribed in [CP].

JCAN パブリック CA は、CA 証明書、CA 証明書の発行・失効の監査データ、CRL、CA 証明書申請情報、ログファイル、及び CA 証明書申請の裏付け資料の記録を、信頼性のある方法で保持する

認定 LRA が保持する情報は、 [CP]で規定する。

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

JCAN Public CA retains records of JCAN Certificates, JCAN Public CA Certificate and LRA Operator Certificates (If issued) for at least 7 years after the Certificate is expired or revoked.

Archive containing sensitive data is securely disposed of when no longer required.

JCAN パブリック CA は、JCAN 証明書、JCAN パブリック CA 証明書及び LRA オペレータ証明書（発行した場合）の記録を、有効期限切れ後、又は失効後、少なくとも 7 年間保持する。

機密データを含むアーカイブは、必要とされない場合は安全に処理される。

4.6 Key Changeover（鍵の切り替え）

The Key Pair generation of JCAN Public CA is managed on a HSM and the shared secret system is managed by more than 2 authorized staff according to the procedure described

in section 6.

The procedure of re-generation of JCAN Public CA keys is same as the procedure of the initial generation.

JCAN パブリック CA の鍵ペアの生成は、2 名以上の任命されたスタッフ 2 名以上により、セクション 6 に記載する手順に従って、HSM 上で且つ秘密分散システムで管理される。

JCAN パブリック CA の鍵ペアの再生成手順は、上記の初期の鍵生成と同じである。

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

JCAN Public CA maintains records on reporting, backup/restoration and handling procedures for incidents and compromises in a separate internal document. JCAN Public CA documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

When an algorithm is compromised, JCAN Public CA carries out the following:

- Inform all subscribers and relying parties with whom the CA has agreement or other form of established relations. In addition, this information is made available to other relying parties; and
- Revoke any affected certificate.

JCAN パブリック CA は、インシデント及び危殆化が発生した場合の報告とバックアップ/復元と取り扱い手続を、内部文書として保持する。JCAN パブリック CA は、コンピュータ資源、ソフトウェア、又はデータが破損した場合に使用する復旧手続を文書化する（災害復旧計画)。

アルゴリズムが危殆化した場合、JCAN パブリック CA は以下を実施する：

・すべての利用者、CA と同意書を交わしている検証者、その他関係者に知らせる

・影響を受けた証明書を失効する

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

When terminating CA, a Certification Authority Manager notifies it to subscribers and Relying Parties at least 60 days ago, revokes all issued certificates in principle and disposes CA secret key.

CA を終了する場合は、CA 終了の少なくとも 60 日前に利用者及び検証者に終了方針を通知し、原則として全発行済み証明書を失効し、CA 秘密鍵を破棄する。

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

5.1 Key Pair Generation and Installation（鍵ペアの生成、及びインストール）

5.1.1 CA Key Generation Devices（CA 鍵生成のデバイス）

A Hardware Security Module (”HSM”), which is one of Cryptographic Module is used for securely generating and managing CA private keys.

HSM is checked that it is not tampered with during shipment.

Certificate and revocation status information signing HSM is not tampered with while stored.

CA 秘密鍵のセキュアな生成と管理には、暗号モジュールの一種であるハードウェアセキュリティモジュール（HSM）を用いる。

HSM は、輸送中に改ざんされていないことを確認する。

HSM で署名している証明書と失効の状況情報は、保存されている間に改竄されない。

5.1.2 CA Private Key Generation and Management（CA 秘密鍵の生成と管理）

JCAN Public CA generates the CA private keys by the documented procedures.

The generation of the CA private key requires “Mutual supervision” which needs more than 2 authorized staff members serving in trustworthy positions.

Private keys are managed on a HSM.

JCAN パブリック CA は、文書化された手続に従って CA 秘密鍵を生成する。CA の秘密鍵の生成は、信任された役職 2 名以上の要員による相互牽制を必要とする。

秘密鍵は、HSM で管理される。

5.1.3 CA Private Key Usage（CA 秘密鍵の利用方法）

Private Key of JCAN Public CA is used to sign JCAN Certificates and CRLs in physically secure premises.

JCAN パブリック CA の秘密鍵は、セキュアな施設の中で JCAN 証明書と証明書失効リストの署名に使用される。

5.1.4 CA Private Key Types（CA 秘密鍵のタイプ）

JCAN Public CA private key is 2048 bit in length and uses the RSA algorithm with SHA-2 (256) hashes which are comply to [Algorithm]

JCAN パブリック CA 秘密鍵は、鍵長が 2048bit で RSA SHA-2（256）アルゴリズムを使用する。

5.1.5 CA Key Pair re-generation and re-installation（CA 鍵ペアの再生成と再インストール）

The procedure of CA Key Pair re-generation and re-installation is the same as in section 6.1.2.

CA Key Pair re-generation and re-installation is carried out at suitable time before its expiration.

JCAN Public CA decommissions and destroys keys used in the past and zero-out HSM in a secure manner at the end of the life-cycle and HSM retirement.

All backup or escrowed copies of its private keys are destroyed at the end of the life-cycle.

CA 鍵ペアの再生成と再インストールの手順は、セクション 6.1.2 と同じである。

CA 鍵ペアの再生成と再インストールは、有効期限前の適切な時期に行う。

JCAN パブリック CA はライフサイクルの終了時及び HSM リタイヤ時に、セキュアな方法で過去に使用された全ての鍵を廃棄し、HSM をゼロ設定する。

ライフサイクルの終了時に、すべてのバックアップ及びキーエスクローされた秘密鍵の複写は破棄される。

5.1.6 CA Private Key Storage（CA 秘密鍵の保管）

JCAN Public CA private key is stored in a HSM.

When outside the HSM, the private key is always strongly encrypted and kept by the access-controlled safe which is not carried easily.

JCAN パブリック CA 秘密鍵は HSM に保管する。

HSM の外では、当該 CA 秘密鍵は常に暗号化され、容易に持ち運ぶことができないアクセスコントロールされた金庫に保管される。

5.1.7 CA Public Key Distribution（CA 公開鍵の交付）

JCAN Public CA public key is downloadable from repository.

JCAN パブリック CA の公開鍵は、リポジトリからダウンロードできる。

5.1.8 CA Private Key Destruction（CA 秘密鍵の破壊方法）

JCAN Public CA private keys are destroyed at the end of their life-cycle by at least 2

trusted personnel. The Key destruction process is documented and associated records are archived.

JCAN パブリック CA 秘密鍵は、ライフサイクルの最後に、信任された 2 名以上の要員の立会いの下に破棄される。鍵の破棄の処理は文書化し、関連する記録は保存する。

5.2 Private Key Protection and Cryptographic Module Engineering Controls（秘密鍵の保護、及び暗号モジュール技術の管理）

5.2.1 CA Private Key Protection（CA 秘密鍵の保護）

JCAN Public CA uses a HSM which meets the standards of FIPS140-2 Level 3.

JCAN パブリック CA は、FIPS140-2 レベル 3 相当の認定を取得した HSM を使用する。

5.2.2 Subscriber's Private Key Protection（利用者秘密鍵の保護）

A Private Key of a Subscriber is 2048 bit minimum in length and uses RSA algorithm. For generation, the following method is used:

利用者秘密鍵の生成は、鍵長が最低 2048bit で RSA アルゴリズムを使用し、下記の何れかの方法で行う。

(1) Generation of Private Keys by JCAN Public CA（JCAN パブリック CA による秘密鍵の生成）

When JCAN Public CA generates the private key on behalf of subscribers or LRA, the key pair and CSR is generated according to a secure key generating procedure and by following the key generation policy referenced above. JCAN Public CA enforces to subscribers the use of a PIN code. The PIN protects the generated private key in PKSC#12 format. Once the subscriber or LRA receives the PKSC#12, all instances of this PKSC#12 are destroyed by the CA including the PIN code. None of the generated private keys are archived.

JCAN パブリック CA が利用者又は LRA に代わって秘密鍵の生成を行う場合は、セキュアな鍵生成手順を用いて、上記鍵生成のポリシに準拠して PKI の鍵ペア及び CSR を生成する。JCAN パブリック CA は、申請者に強固な PIN の使用を義務付け、当該 PIN を用いて秘密鍵を含む pkcs#12 形式の暗号化証明書パッケージ（以下「pkcs#12 形式証明書」という）を生成する。当該 PIN 及び生成した秘密鍵はアーカイブせず、全てのインスタンスは pkcs#12 形式証明書の生成後に破棄される。

(2) Generation of Private Keys by Subscriber (利用者による秘密鍵の生成)

Subscriber doesn't generate the private key.

利用者による秘密鍵の生成は行わない。

5.3 The other Aspect of Key Pair Management (鍵ペア管理の他の側面)

(1) Validity period

Validity period of CA Keys and CA Certificate is variable and can be checked the certificates.

Currently the validity period is from "October 19, 2011 10:00:00 UTC" until "November 19, 2022 10:00:00 UTC".

CA 鍵及び CA 証明書の有効期間は、可変であり、当該証明書で確認できる。
現在、有効期間は、UTC で 2011 年 10 月 19 日 10 時から 2022 年 11 月 19 日 10 時までである。

5.4 Activation Data (活性化データ)

JCAN Public CA securely stores activation data associated with its own private key and operations.

JCAN パブリック CA は、自己の秘密鍵と業務に関連する活性化データをセキュアに保管する。

5.5 Computer Security Controls (コンピュータセキュリティの管理)

JCAN Public CA implements computer security controls such as keeping integrity of CA systems and confidential, protecting against obsolescence and deterioration of media, etc.

JCAN パブリック CA は、CA システム及び機密情報の完全性維持、媒体の退化と劣化の保護等のコンピュータセキュリティ管理を実装する。

5.6 Life Cycle Security Controls (ライフサイクルセキュリティの管理)

When development, adoption and change of software, it tests including a security requirement in a test environment after analyzing and designing from the design specification phase and releases to real environment after approval of a responsible person.

ソフトウェアの開発、採用、変更を行う場合は、セキュリティ要求事項を含む文書に基づいて設計仕様の段階から分析し、設計をした上でテスト環境でテストし、責任者の承認の後、実環境

へリリースする。

5.7 Network Security Controls（ネットワークセキュリティの管理）

JCAN Public CA network is protected by a firewall and intrusion detection system.

JCAN パブリック CA のネットワークは、ファイアウォールと不正検知システムにより保護される。

5.8 Time Stamping（タイムスタンプ）

Not applicable.

該当なし。

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

6.1 Certificate Profile（証明書プロファイル）

Certificates profile issued from JCAN Public CA base on the X.509 Version 3 Format and the following table. About Other information, see [CP] and JCAN Repository.

JCAN パブリック CA から発行される証明書プロファイルは、X.509 バージョン 3 フォーマットに基づく。他の情報については、[CP]と JCAN リポジトリを参照。

Field （フィールド）	Value or Value constraint （値、又は値制約）
Serial Number	Unique value within the CA domain
シリアルナンバー	CA が割り当てる一意な番号
Signature Algorithm	Object identifier of the algorithm used to sign the certificate. SHA1 RSA or SHA256 RSA in accordance with RFC3279.
署名アルゴリズム	証明書に署名するために使用されたアルゴリズムのオブジェクト識別子 RFC3279 に従い、SHA1 RSA または SHA256 RSA
Issuer	The name of the CA which issued the digital certificate - written in X.500 identifier (DN) format
発行者	電子証明書を発行した CA の名前、X.500 識別名(DN)で記述
Valid From	Start of the validity period of the certificate
有効期間開始日	証明書の有効期間開始日
Valid To	End of the validity period of the certificate
有効期間終了日	証明書の有効期間終了日
Subject DN	The name of the owner of the digital certificate and other pertinent information
サブジェクト DN	電子証明書の所有者の名前
Subject Public Key	The public key
サブジェクト公開鍵	証明書所有者の公開鍵に関する情報

6.1.1 Authority Key Identifier（AKI）

Authority Key Identifier (“AKI”) can be incorporated in extension of JCAN Certificates and JCAN Public CA Certificates.

The AKI should be composed of the 160-bit SHA-1 hash of the public key of the CA

issuing the Certificate.

JCAN 証明書と JCAN パブリック CA 証明書の拡張に、AKI を挿入してもよい。
AKI は、証明書を発行する CA の公開鍵の 160bit の SHA-1 ハッシュから構成されなければならない。

6.1.2 Authority Information Access (AIA)

Authority Information Access ("AIA") can be incorporated in extension of JCAN Certificates and Sub CA Certificates.

AIA should be incorporated through the URL of the location where a Relying Party can obtain the issuing CA certificate.

JCAN 証明書、及び適当であればサブ CA 証明書に対し、AIA を挿入してもよい。
検証者認定 CA 証明書を取得できる URL と共に挿入しなければならない。

6.1.3 CRL Distribution Points (CRL Distribution Points)

JCAN Certificates and JCAN Public CA Certificates include the cRLDistributionPoints, containing the URL of the location where a Relying Party can obtain a CRL to check the certificate's status, in extension of the Certificates.

JCAN 証明書と JCAN パブリック CA 証明書は、その証明書の拡張に検証者が CA 証明書のステータスを確認するための CRL を取得できる URL である cRLDistributionPoints を含む。

6.1.4 Subject Key Identifier (SKI)

Subject Key Identifier ("SKI") can be incorporated in extension of JCAN Certificates and JCAN Public CA Certificates.

The SKI should be composed of the 160-bit SHA-1hash of the public key of the CA issuing the Certificate.

JCAN 証明書と JCAN パブリック CA 証明書の拡張に、SKI を挿入してもよい。
SKI は、証明書を発行する CA の公開鍵の 160bit の SHA-1 ハッシュから構成されなければならない。

6.1.5 Subject Alternative Name (Subject Alternative Name)

Subject Alternative Name can be incorporated in extension of JCAN Certificates.

The SubjectAlternativeName should be generated in accordance with one of the methods

described in RFC 5280.

JCAN 証明書の拡張に、Subject Alternative Name を挿入してもよい。

SubjectAlternativeName は、RFC 5280 に記述された方法の 1 つに従って生成されなければならない。

6.2 CRL Profile（CRL プロファイル）

CRLs are issued from JCAN Public CA in X.509 CRL Version 2 Format and are incorporated in the “cRLDistributionPoints extension”.

JCAN パブリック CA から発行する CRL は、X.509 バージョン 2 フォーマットにより形成され、“cRLDistributionPoints 拡張”のフィールド域内にリンク先が含まれる。

Field （フィールド）	Value, or Value constraint （値、又は値制約）
Version	V2 in accordance with RFC 5280
バージョン	RFC 5280 に従って、X.509 のバージョン 2
Certificate Issuer	The Entity who has signed and issued the CRL
証明書発行者	CRL に署名し発行したエンティティ
This update	Date of Issuance
今回更新	発行日
Next Update	Date of Issuance＋7days
次回更新	発行日付＋7 日以内
Signature Algorithm	Object identifier of the algorithm to sign the CRL. SHA1 RSA or SHA256 RSA in accordance with RFC 3279.
署名アルゴリズム	CRL に署名するために使用されたアルゴリズムのオブジェクト識別子 RFC3279 に従って、SHA1RSA または SHA256 RSA
Authority Key Identifier	160–bit SHA-1 hash of the public key of the CA issuing the Certificate
AKI	証明書を発行する CA の公開鍵の 160bit の SHA-1 ハッシュ値
CRL Number	A unique sequence number in accordance with RFC5280
CRL 番号	RFC 5280 に従って、ユニークなシーケンス番号
Revoked Certificates	Serial No. of revoked certificate, revocation Date and Time
失効証明書情報	失効した証明書のシリアルナンバー、失効日時

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

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

JCAN Public CA follows the compliance auditing practices and procedures in order to guarantee that the service conforms to this CPS requirements, standards, procedures, and service levels at least once a year.

Audit of Accredited LRA is prescribed in [CP]

JCAN パブリック CA は、年に 1 回以上、本サービスが、本 CPS 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。

認定 LRA の監査は、[CP]による。

7.2 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。

7.3 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。

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

Audit of JCAN Public CA is based on this CPS.

Audit of Accredited LRA is prescribed in [CP]

JCAN パブリック CA の監査は、本 CPS の準拠性を中心に行われる。

認定 LRA の監査は、[CP]による。

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

8.1 The issuance of JCAN certificates is subject to reasonable fees.

JCAN 証明書の発行には、適正な料金が課金される。

8.2 Financial Responsibility（財務的責任）

JCAN Public CA keeps sufficient financial funding for offering these services.

JCAN パブリック CA は、本サービスの提供にあたり、十分な財務基盤を維持する。

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

Business information which JCAN Public CA maintains is regarded as confidential except for public items such as certificates and CRL, [CP], this CPS and other policy documents. These are disclosed intentionally.

JCAN パブリック CA が保持する業務情報は、証明書、CRL、[CP]及び本 CPS 等で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。

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

Personal information which JCAN Public CA maintains is following the concerning law of the country if any.

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

JCAN パブリック CA 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。

JCAN パブリック CA 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。

8.5 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 CPS.

本 CPS 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。

8.6 Representations and Warranties（表明保証）

JCAN Public CA retains trust in authentication operation by following the content prescribed in this CPS, performs vetting prior to issuance of certificates, provides authenticated services including registration of certificates, issuance, revocation and guarantees the integrity of CA private keys.

JCAN パブリック CA は、本 CPS に規定した内容を遵守して証明書申請に関する審査、証明書の登録、発行、失効を含む認証サービスを提供し、CA 秘密鍵の完全性を含む認証業務の信頼性を確保する。

8.7 Disclaimers of Warranties（無保証）

JCAN Public CA does not warrant anything except the guarantees prescribed in this CPS.

JCAN パブリック CA は、本 CPS に規定された保証を除き、一切の保証を行わない。

8.8 Limitations of Liability（責任の制限）

JCAN Public CA is not responsible for damages regarding authenticated services against subscribers, relying parties or other third parties.

- All damages not caused by JCAN Public CA
- Any damages caused by not fulfilling the obligation of subscribers or relying parties
- Any damages originating in the systems of subscribers or relying parties
- Damages caused by Hardware or Software used by JCAN Public CA and other parties which are defective or not maintained.
- Damages resulting in secondary, indirect, loss of profit from use of certificates or digital signatures.
- Damages originating from information published in the certificate and CRLs.
- Damages resulting from improvement in cryptographic algorithm decoding technology beyond current expectations.
- Any responsibilities originating in the termination of JCAN Public CA
- Any damages originating from the suspension of JCAN Public CA which is the result of an extraordinary natural occurrence, other natural disasters, wars, upheavals, terrorism, and other inevitable accidents (Act of God).

JCAN パブリック CA は、認証サービスに関する以下の損害について、利用者、検証者又はそ

の他の第三者に対して、一切の責任を負わないものとする。

- JCAN パブリック CA に起因しない一切の損害
- 利用者又は検証者の義務の履行を怠ったため生じる一切の損害
- 利用者又は検証者のシステムに起因する一切の損害
- JCAN パブリック CA 及びその他当事者のハードウェア、ソフトウェアの瑕疵・不具合による損害
- 証明書又は電子署名に関連して発生する、二次的、間接的、遺失利益の一切の損害
- JCAN パブリック CA の責に帰することの出来ない事由で、証明書及び CRL に公開された情報に起因する損害
- 現時点での予想を超えた、暗号アルゴリズム解読技術の向上に起因する損害
- JCAN パブリック CA の終了に起因する一切の損害
- 天変地異、その他の自然災害、戦争、動乱、テロ、その他の不可抗力に起因する JCAN パブリック CA のサービスの停止に起因する一切の損害

8.9 Indemnities（補償）

JCAN Public CA shall indemnify to Subscribers, Relying Parties, or other third parties for the damages which have not been specified to section 9.8.

In all cases, the amount of money received is set as an upper limit for Liability for damages which JCAN Public CA bears.

Subscribers, Relying Parties, or other third parties shall indemnify for the damages JCAN Public CA suffers originating in failure of unfulfillment of the obligations or responsibilities stated in this CPS. To the extent permitted by law, Subscribers, Relying Parties, or other third parties shall indemnify JCAN Public CA and its partners against any loss, damage, or expense, including reasonable attorney's fees, related to claim, dissent, lawsuit resulting or etc.

Accredited LRA shall indemnify the damages of JCAN Public CA in connection with the requirements specified in "30-5020 LRA accreditation application" To the extent permitted by law, Accredited LRA shall indemnify JCAN Public CA and its partners against any loss, damage, or expense, including reasonable attorney's fees, related to claim, dissent, lawsuit resulting or etc.

JCAN パブリック CA は、9.8 節に規定していない損害について、利用者、検証者又はその他の第三者に対して責任を負うものとする。

いかなる場合においても、JCAN パブリック CA が負担する賠償責任は、受け取った金額を上限とする。

利用者及び検証者は、本 CPS に記載の義務または責任の不履行に起因する JCAN パブリック

CA が被る損害を補償するものとし、法律の許す範囲で、クレーム、異議及び訴訟等に起因するあらゆる損失、損害あるいは出費、またこれらに関する弁護士費用を JCAN パブリック CA 及びそのパートナーに保証するものとする。

認定 LRA は、「30-5020 LRA 認定申請書」に定めた要件に起因して JCAN パブリック CA が被った損害を補償し、法律の許す範囲で、クレーム、異議及び訴訟等に起因するあらゆる損失、損害あるいは出費、またこれらに関する弁護士費用を JCAN パブリック CA 及びそのパートナーに保証するものとする。

8.10 Term and Termination（期間と終了）

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

本 CPS 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。

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

JCAN Public CA accepts notices related to this CPS by means of digitally signed mails. Upon receipt of a valid, digitally signed acknowledgement of receipt from JCAN, the sender of the notice deems its communication effective.

JCAN パブリック CA は、電子署名されたメールで本 CPS に関連する通知を受領する。JCAN から有効に電子署名された受領確認を受信したことを受けてその連絡が有効であったと見なす。

8.12 Amendments（改訂）

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 Qualified Auditors in principle, if there is no opinion within 15 days.

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。

8.13 Dispute Resolution Procedures（紛争解決手続）

Before resorting to any dispute resolution mechanism including adjudication or any type

of Alternative Dispute Resolution, parties agree to notify JCAN Public CA.

訴訟、仲裁を含む法的、またはその他の解決手段を訴えようとする場合、JCAN パブリック CA に対し、事前にその旨を通知するものとする。

8.14 Governing Law（準拠法）

This CPS is governed, construed and interpreted in accordance with the laws of Japan. Tokyo District Court shall have the exclusive jurisdiction over all disputes arising in connection with JCAN Public CA services.

本 CPS の解釈及び、JCAN パブリック CA のサービスに関わる紛争については、日本国の法律が適用され、東京地方裁判所を第一審の専属的合意管轄裁判所とする。

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

JCAN Public CA complies with applicable laws of Japan.

JCAN パブリック CA は、適用可能な日本国の法律を遵守する。

8.16 Miscellaneous Provisions（雑則）

(1) Survival（存続）

The obligations and restrictions contained under legal consequence survive the termination of JCAN Public CA.

法的問題の責任及び制限事項は、JCAN パブリック CA の終了後も存続する。

(2) Severability（分離）

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS should be interpreted in such manner as to represent the original intention of the parties.

本 CPS の賠償責任の制限の節を含むいずれかの条項が無効であるか、あるいは法的強制力がないことが分かった場合にも、本 CPS の他の条項は当事者の本来の意図を損なわない方法で解釈されるものとする。

8.17 Other Provisions（他の条項）

This CPS shall be binding upon the successors, executors, heirs, representatives,

administrators, and assigns, whether express, implied, or apparent, the parties that this CPS applies to.

本 CPS は、明示的か黙示的かにかかわらず、当事者の後継者遺言執行者、相続人、代理人、管財人、および譲受人に対しても拘束力がある。

9. 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。