案

JCAN Certificate Policy

JCAN 証明書ポリシー

GMO グローバルサイン株式会社

Document Change Control

改訂履歴

Version	Release Date	Status + Description	Author	Approver
5.0	XX/XX/2021	Administrative update 事業譲渡に伴う修正	・GMO グローバルサイン ・JIPDEC	・GMO グローバルサイン ・JIPDEC Managing Director JIPDEC 常務理事 (JCAN 担当)
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) applies to JCAN Certificates, and defines policies for the scope of usage. This CP aims to be compliant with JIPDEC Trusted Service (JTS) Registration requirements and WebTrust for CA.

JCAN certificates are issued by JCAN Public CA which has an adequate system for quality and information security management.

JCAN is a service, offered by GlobalSign, to issue digital certificates.

The company profile of GlobalSign is as below:

Commercial Registration Number: 0110-01-040181
Company Registration Number: 1011001040181

The GlobalSign PACOM1 - CA Governance Policy Authority, which is composed of members of the GlobalSign management team and appointed by its Board of Directors, is responsible for maintaining this CP.

本書(CP)は、JCAN 証明書に適用され、用途及び範囲等のポリシーを規定するものである。本 CP は、JIPDEC トラステッド・サービス登録及び WebTrust for CA への準拠を目的としている。

JCAN は、GMO グローバルサイン株式会社（以下「GlobalSign」という） が運用する電子証明書発行サービスである。 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 JCAN 認証局によって発行される。

GlobalSign の会社情報は以下の通り。

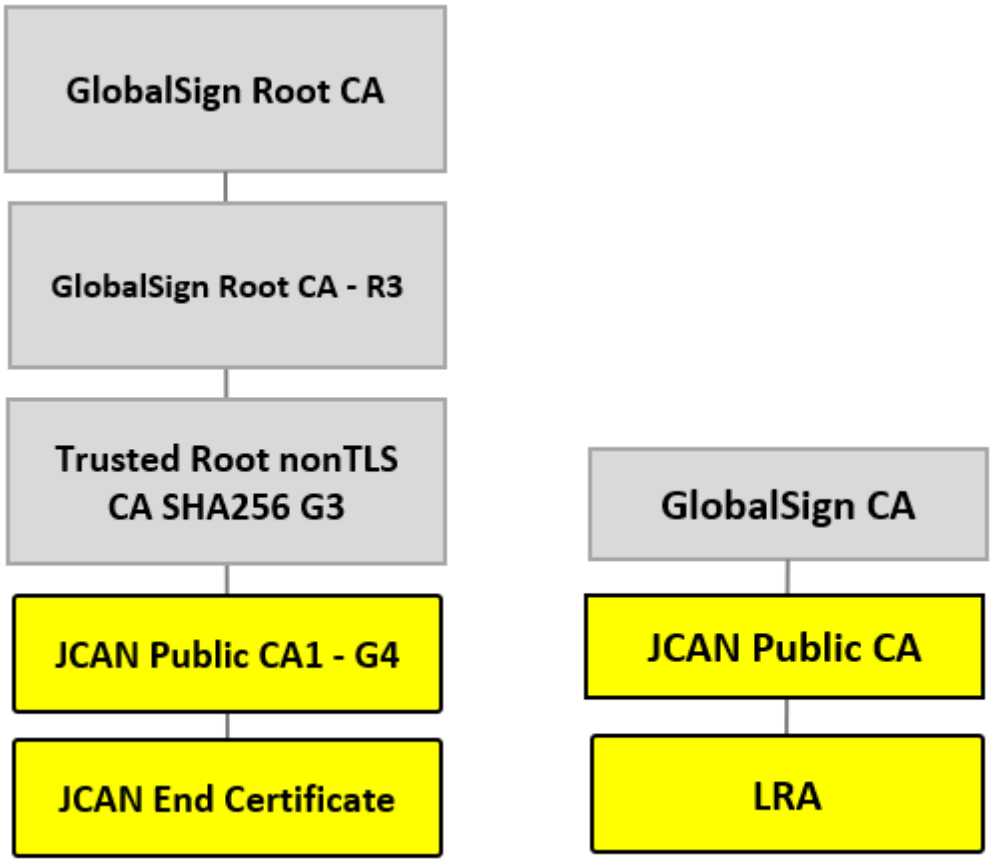
商業登記番号：0110-01-040181
法人番号：1011001040181

GlobalSign の PACOM1 – CA Governance Policy Authority は、GlobalSign の経営チーム、及び GlobalSign の 取締役会で承認されたメンバーで構成されており、本 CP を維持管理する責任を負う。

1.1.1 Diagram of JCAN Certificate　(JCAN 証明書の図)

The JCAN certificate hierarchy and the structure of JCAN certificate management system are shown in the following:

JCAN 証明書の階層を下図左に、JCAN 証明書管理システムの構造を下図右に示す。



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

LRAs are accredited by JIPDEC after their pass of the vetting on JTS Registration requirements (for LRAs), and then are authorized for the operation of the LRA.

JCAN Public CA is one of CAs which are accredited by JIPDEC on their pass of the vetting on JTS Registration　requirements (for CAs).

JCAN 証明書は、LRA の要求に基づき JCAN 認証局から発行される。

LRA は、LRA 業務の第三者評価を一般財団法人日本情報経済社会推進協会（以下、JIPDEC）が実施し、「JIPDEC トラステッド・サービス登録（電子証明書取扱業務）の基準に係る審査」（以下、JTS 登録(LRA)）に合格後、登録され、LRA 運用の権限を得る。

JCAN 認証局は、JIPDEC による JIPDEC トラステッド・サービス登録（認証局）の基準に係る審査に合格した CA である。

1.2 Document Name and Identification (文書名称と識別子)

Document name: Refer to the cover.

Version: Refer to the cover.

OID: 1.3.6.1.4.1.4146.1.40.20.1

1.3 PKI participants (PKI の関係者)

(1) Subscribers (利用者)

Subscribers are the subjects or users of JCAN Certificates.

The obligations of Subscribers are the followings:

- To agree with use/disclose of their personal information by LRA for their operation, audit/accreditation/legal-proceedings and to agree with use/disclose of their personal information recorded on a certificate by Relying Party for their operation and certificate validation ;
- To agree with the LRA (= the representative of the subscribers) to back up the certificates in PKCS#12 format and their PIN codes when in case these PINs have been generated by the LRA;
- To use the certificate only for the permitted usages after agreeing to this CP;
- To use the certificate under secure conditions, protect certificates from unauthorized use, and discontinue the use upon expiration or revocation;
- To notify the LRA promptly of any changes in the certificate information;
- To notify the LRA promptly of the loss or theft of PCs or media in which JCAN Certificates are installed;
- To notify the 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
- To accept a revocation of the certificate by the LRA or the JCAN Public CA.

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。

- JCAN 証明書発行に際し、LRA（業務、監査/登録/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 JCAN 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。
- 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 JCAN 証明書を使用すること
- JCAN 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

JCAN 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、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、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、ウィルスやマルウェア感染等、JCAN 証明書の信頼性が損なわれる可能性がある場合は、LRA に、速やかに知らせること。

LRA または GlobalSign による JCAN 証明書の失効を了解する。

(2)LRA（LRA）

LRA is the LRA which passed the JTS Registration vetting as the representative of Subscribers.

LRA vets the authenticity of the DN and verifies the identity of the Subscriber of JCAN Certificates. Furthermore, the LRA operates the certificate life-cycle management of the certificate under JCAN Certificate Policies.

The obligations of LRAs are the followings:

① General obligations

- To inform the obligation of Subscribers to Subscribers;
- To record the consent by Subscribers;
- To acquire the information disclosed on JCAN Repository to make Subscribers aware of the information necessary for them. Especially in case notified by GlobalSign, the awareness of Subscribers is to be promptly implemented.
- To make those serving for the operation of the LRA to declare not to implement unauthorized issuance and disclosure;

② Obligations related to certificate issuance

- To guarantee the unique identification allotted to OrganizationUnitName2 and CommonName within the Subject;
- To securely distribute the certificates in PKCS#12 format with the corresponding PIN to Subscribers in case this PIN is created by the Accredited LAR themselves;
- To securely manage the backup of the certificates in PKCS#12 format and the corresponding in case this backup is implemented by the Accredited LAR themselves; and
- To save the record of certificate issuance and revocation (c.f. identity verification records, agreements, etc.) after the certificate issuance LRA.

③ Obligations related to certificate revocation

- To revoke the certificates promptly in case the Subjects/users became not related to the applicable organization due to the work termination, organization transfer, or termination of the organization;
- To revoke the certificates promptly when any Subscriber has breached the

obligations under this CP and/or the rules of the LRAs;

- To revoke the certificates promptly when an error or false is recorded there;
- To revoke the certificates promptly when private key becomes compromised such as suffering at the time of disasters or the compromise of the LRA Operator certificates;
- To revoke the certificates promptly when this revocation is decided by the LRA themselves for any reasons other than listed above.

LRA とは、利用者の代表として JTS 登録(LRA)の基準に合格した LRA である。

LRA は、JCAN 証明書ポリシーの下、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を行う。

義務は、以下の通りである。

(a) 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。
- 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、GlobalSign 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。

(b) 証明書発行

- サブジェクトの OrganizationUnitName2、CommonName の唯一性を保証する。
- LRA が PIN を生成した場合、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。
- 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。
- JCAN 証明書の発行後、LRA は、発行の記録（本人確認資料、同意書等）を保管する。

(c) 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、JCAN 証明書を速やかに失効する。
- 利用者が本 CP 及び/又は LRA の規則の義務に違反した場合、JCAN 証明書を速やかに失効する。
- JCAN 証明書に誤り又は虚偽が記載されている場合、JCAN 証明書を速やかに失効する。
- 被災、アクセス認証用証明書の危殆化等で秘密鍵が危殆化した場合、JCAN 証明書を速やかに失効する。
- LRA がその他の理由で失効を決定した場合、JCAN 証明書を速やかに失効する。

(3)Relying Party（検証者）

Relying Parties are the persons who trust any certificates and/or digital signatures of Subscribers.

The obligations of Relying Parties are the followings:

- To verify the validity or revocation of the certificate using current revocation status information as disclosed to the Relying Party; and
- To rely on and trust the JCAN Certificates only under reasonable circumstances.

検証者は、利用者の JCAN 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、JCAN 証明書の有効性、又は失効を確認する。
- 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 認証局）

JCAN Public CA is the CA which issues JCAN Certificates following this JCAN Certificate Policy regarding the purpose of use, scope of use, and procedures.

Subscribers are contacted through the LRA.

The obligations of JCAN Public CA are prescribed on [CPS].

JCAN 認証局は、JCAN 証明書ポリシーに従い 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認証局である。

利用者への連絡は LRA を通じて行う。

義務は、[CPS]に規定する。

(5)JIPDEC Trusted Service Registration（JIPDEC トラステッド・サービス登録）

JIPDEC Trusted Service（JTS）Registration a private accreditation system operated independently by JIPDEC.

The obligations of JIPDEC are the followings:

- To have LRAs receive the vetting on JTS Registration requirements;
- To ensure that the LRAs are registered as LRAs through their pass of JTS Registration requirements.

JIPDEC トラステッド・サービス登録は、JIPDEC が主体的に運用する民間制度である。
JIPDEC の義務は、以下の通りである。

- JIPDEC は LRA に対して JTS 登録(LRA)の審査を実施する。
- LRA の登録は、JTS 登録(LRA)の基準に係る審査への合格を通じて保証される。

1.4 Certificate Usages (証明書の使用方法)

(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 applicable laws and regulations of the country if any.

Certificates issued under this CP may not be used:

- For any application requiring fail safe performance
- For any application or mechanism where issues with the certificate could cause a safety risk (e.g., human, or environmental risk)
- Where prohibited by law

The types of JCAN Certificates which JCAN manages are the followings:

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。

本 CP に準拠して発行された証明書は、以下の目的に使用してはならない。

- フェイルセーフ機能を必要とする用途。
- 安全上の危険(例：人的又は環境に対するリスク)を起こしうる用途又は仕組・構造。
- 法により禁じられている場合。

GlobalSign 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 LRAs. LRAs identify the PERSON by databases which are based on the official documents.
Subject CommonName ("CN") is the real name or a pseudonym (PS[1])

JCAN アドバンストは、LRA から自然人に対し発行される。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 assurance by official documents：

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

[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

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

NOTE) PARTNER is the person who is being contract party, group-company staff, member of any group, constituent of any committee, student, person who are authenticated with reliable document sources, or person who registered his/her credit card, etc.

Subject CN of a JCAN certificate are the followings:

- Name of MEMBER or PARTNER (Real name or PS);
- Name of the applicable person's role;
- Name of an organization such as company, party, department, team, or group;
- 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(メンバー、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(パートナー、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) パートナーは、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。

- メンバー又はパートナー名（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 (ポリシー管理)

1.5.1 Document administrator (文書管理)

The GlobalSign PACOM1 - CA Governance Policy Authority, which is composed of members of the GlobalSign management team and appointed by its Board of Directors, is responsible for maintaining this CP.

GlobalSign の PACOM1 – CA Governance Policy Authority は、GlobalSign の経営チーム、及び GlobalSign の 取締役会で承認されたメンバーで構成されており、本 CP を維持管理

する責任を負う。

1.5.2 Contact Address (連絡先)

(1)LRA

The contact of JCAN Certificate issuance/revocation is the LRA. These contacts are disclosed to Subscribers from the LRA themselves.

NOTE: These contacts are open only during the office hours of each LRA.

利用者からの JCAN 証明書発行/失効に係る連絡先は LRA であり、LRA が利用者に対してその連絡先を公開する。

注）連絡は LRA の営業時間のみ

(2)JCAN Public CA

The contact of JCAN Public CA (GlobalSign) is as follows:

NOTE: The contact is open during the office hours only.

GMO GlobalSign K.K.
Shibuya Fukuras 9-16F
1-2-3, Dogenzaka, Shibuya-ku
Tokyo 150-0043, JAPAN
Tel: +81 3 6370 6500
Fax: +81 3 6370 6505
Email: legal.jp@globalsign.com
URL: www.globalsign.com

- Contact to report the abuse of certificates

Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may report suspected Private Key Compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to:

report-abuse@globalsign.com

GlobalSign may or may not revoke in response to this request. See article 4.8 for detail of actions performed by GlobalSign for making this decision.

JCAN 認証局(GlobalSign)の連絡先は以下の通り。

注）連絡は営業時間のみ

GMO グローバルサイン株式会社
東京都渋谷区道玄坂 1 丁目 2 番 3 号　渋谷フクラス
03-6370-6500（代）／ FAX: 03-6370-6505
Email: legal.jp@globalsign.com
URL: www.globalsign.com

- 電子証明書の問題報告

マルウェア対策団体、利用者、依拠当事者、アプリケーション・ソフトウェア・サプライヤ、及び他の第三 者は、秘密鍵の危殆化の可能性、証明書の不正使用、乗っ取り攻撃、又は他の種類の不正、セキュリティの侵害、証明書の誤発行、不適切な行為、又は証明書に 関連する他の事項は、下記アドレスにメールで報告することとする。

report-abuse@globalsign.com

GlobalSign は、この要求に応じて当該証明書を失効することが可能である。また、調査の結果、失効しない場合もある。この意思決定のために GlobalSign は 4.8 項に記載されている調査を実施する。

1.6 Definitions and acronyms (定義と略語)

1.6.1 Definitions (定義)

Please refer to Article 10.

10 項参照

1.6.2 References (参考)

[CPS]　CPS of JCAN Public CA

JCAN 認証局の CPS

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

2.1 Repositories (リポジトリ)

GlobalSign reserves the rights to publish the information about this CP, [CPS], and JCAN certificates that are published on the repository. GlobalSign publishes the information about CRL on the repository.

These public information shall be available by 24x365.

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

GlobalSign reserves the right to publish the following information on the repository to enable Subscribers and Relying Parties to refer to it online.

GlobalSign notifies the stakeholders as necessary of any change made on the repository.

Archived records shall be disclosed if required for the purposes of providing evidences to any legal disputes or audits.

GlobalSign 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。

GlobalSign 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。

訴訟又は監査対応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) Repository (リポジトリ)

- Public Root CA Certificate and Sub CA certificates
- The latest versions of this CP
- Other information regarding JCAN Public CA

https://jp.globalsign.com/repository/

- パブリックルート CA 証明書とサブ CA 証明書
- 最新の本 CP
- JCAN に関するその他の情報

https://jp.globalsign.com/repository/

2.3 Time or Frequency of Publication (公開の時期及び頻度)

Updates of this CPLRA are published on the repository after the approval by PACOM1.

The status of JTS Registration of LRAs is published on the website of JIPDEC.

CRL is updated periodically and whenever any change happens during the validity period. The information of revocation shall be listed on CRL at least until the certificate expiration.

. Update frequency of the CRL is within 24 hours.

本 CP は、PACOM1 の承認後、GlobalSign のホームページに公開される。LRA の JTS 登録情報は、JIPDEC のホームページに公開される。

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 JCAN 証明書の有効期間満了まで CRL に記載される。CRL の更新頻度は 24 時間以内である。

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

JCAN Public CA publishes its repository.

GlobalSign は当該リポジトリを公開する。

3. Identification and Authentication (本人確認と認証)

3.1 Naming (名称)

In order to identify Subscribers, JCAN Public CA follows the specific naming (c.f. type of names allocated to Subject) and identification of Subscribers such as Distinguished Names defined in X.500, Names defined in RFC 822, and Names defined in X.400.

When applying for the JCAN Certificates, the name of the Subscriber shall be structured as prescribed in this CP.

GlobalSign 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。

3.2 Initial Identity Validation (初回の本人識別情報の検証)

3.2.1 Validation of Organization (組織の確認)

GlobalSign authenticates the LRA entity registered as organization in Subject. Authentication is implemented by whatever method GlobalSign deems reliable, including

- verification of the existence of the Organization concerned, or
- reference to Standard Company Code, JAPAN Corporate Number, official documents issued by the state and local governments, reliable databases which are managed by the state and/or the local public institution (hereinafter called "QGIS"), and third party databases (hereinafter called "QIIS") which JCAN relies on.

GlobalSign は、サブジェクトの organization として登録される 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)、GlobalSign 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、GlobalSign 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, LRAs authenticate subjects as below. LRAs accept all the responsibilities regarding the authentication of the applicable Subject.

JCAN 証明書の発行に際して、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 LRA が負う。

(1) JCAN Advanced

LRAs validate any Subjects by the following one or more reliable documents or their copies/databases (Personnel inventory, etc.):

- a copy of a resident's card;
- Mynumber Card (c.f. national ID card)
- notice of local tax special levy determination;
- employment insurance;
- resident's tax;
- tax exemption;
- insurance premium deduction;
- reliable documents (c.f. Health Insurance Cards, Driver's licenses, or Passports) in validity period; or
- Reliable digital certificates

(a) If an individual's name (real name or pseudonym name) is to be recorded in CommonName field, LRAs validate the name with the documents listed above or their copies/databases.

(b) If an organization's name is to be recorded in OrganizationUnitName2 and/or CommonName field, LRAs validate the organization name by the following one or more reliable documents or their copies/databases.

- Reliable databases; or
- The documents listed above.

(c) If an email address is to be recorded in rfc822Name field, LRAs validate with GlobalSign in accordance with section 3.2.4 whether the email address is registered by the applicable 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 OrganizationUnitName2 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 Email アドレスを記載する場合、Email アドレスが当該組織に登録されていることをセクション 3.2.4 の通り GlobalSign とともに確認を行う。

(2) JCAN Basic

LRAs validate the “subject attributes" by the following one or more documents, their copies, databases, or data (which shows that the organization affiliated with the PARTNER manages the data to be recorded on the certificates: organization name, name, Email address or OBJECT):

①If an individual's name (real name or pseudonym name) is to be recorded in CommonName field

- Employee ID Card, Student ID Card, etc.;
- Document issued from the organization which certifies the Subject’s belonging to the organization
- Reliable databases;
- Valid and non-revoked credit cards; or
- The reliable documents listed in the previous article for JCAN Advanced.

NOTE) It is not necessary to validate pseudonym name.

② If an organization’s name is to be recorded in OrganizationUnitName2 and/or CommonName field

- Reliable databases; or
- The reliable documents listed in the previous article for JCAN Advanced.

③ If an OBJECT name or identifier is to be recorded in OrganizationUnitName2 and/or CommonName field

- The digital document which indicates that the PARTNER’s affiliation organization manages the OBJECT

④ If an Email address is to be recorded to rfc822Name

- The digital document which indicates that the PARTNER’s affiliation organization manages the Email address

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（パートナーの所属組織が証明書記載事項（組織名、名前、Email 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：

① CommonName に名前（実名又は PS 名）を記載する場合

- 社員証、学生証等
- 組織が発行する在籍証明書

- 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

② OrganizationUnitName2 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

③ OrganizationUnitName2 and/or CommonName にオブジェクトの名前、識別子を記載する場合

- パートナー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 Email アドレスを記載する場合

- パートナーの所属組織が当該 Email 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)

As in Article 3.2.2, the information required for Subject's registration are the documents, copies, databases, or data (which indicates that the organization affiliated with the PARTNER manages the data to be recorded on the certificate).

These information and the record of certificate issuance (c.f. identity verification records, agreements, etc.)" are archived in paper or digital form except the case where the information is 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（パートナー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。

当該情報及び発行の記録（本人確認資料、同意書等）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。

3.2.4 Authentication of Email addresses（電子メールアドレスの認証）

If an email address is to be recorded in rfc822Name field, GlobalSign must use one of the following methods to confirm that the Applicant has control of or right to use email addresses:

① Having the Applicant demonstrate control over the requested email address by sending a Random Value to the requested email address and then receiving a confirming response utilizing the Random Value; or

② Having the Applicant demonstrate control over the requested domain part of an email address by sending a Random Value to a Domain Contact via email and then receiving a confirming response utilizing the Random Value.; or

③ Having the Applicant demonstrate control over the requested domain part of an email

address by sending a Random Value to an email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name and obtaining a response utilizing the Random Value.; or

④ Having the Applicant demonstrate control over the requested domain part of an email address by confirming the presence of a Random Value in a DNS CNAME or TXT record on an Authorization Domain Name.

GlobalSign は、rfc822Name に Email アドレスを記載する場合、申請者が電子メールアドレスを管理又は使用する権利を有することを確認するために、以下いずれかの方法を使用する。

① 要求された電子メールアドレス宛に任意の値（認証用 URL）を送信し、その値（認証用 URL）を用いて確認の返信を得ることで、申請者が要求された電子メールアドレスを管理していることを確認する。又は、

② 乱数（パスフレーズ）をメールアドレスのドメイン部の連絡先に電子メールで送信し、確認した相手からその乱数（パスフレーズ）を用いた返答を受信する審査を通し、申請されたメールアドレスのドメイン部が申請者の管理下にあることを確認する。又は、

③ ローカル部分に'admin', 'administrator', 'webmaster', 'hostmaster', 又は'postmaster'を追加し、その直後に@、そのあとに認証されるドメイン名が続く電子メールアドレスに対し、乱数（パスフレーズ）を送信したあと、その乱数（パスフレーズ）を用いた返答を受信する審査を通し、申請されたメールアドレスのドメイン部が申請者の管理下にあることを確認する。又は、

④ 認証されるドメイン名上にある DNS CNAME 又は TXT レコード内に乱数（パスフレーズ）が存在することを確認する審査を通し、申請されたメールアドレスのドメイン部が申請者の管理下にあることを確認する。

3.3 Identification and Authentication for Re-Key Request (鍵更新申請時における識別及び認証)

The identification procedures for the re-key is defined in Article 3.2.2. LRAs can refer to the record of issuance during the identity verification.

鍵更新要求に対する本人確認は 3.2.2 に規定する。本人確認の際、LRA は発行の記録を参照することができる。

3.4 Identification and Authentication for Revocation Request (失効申請における本人確認と権限の認証)

LRAs or GlobalSign authenticate revocation requests by verifying the identity of the requester with specific sources. LRAs may refer to the records of certificate issuance (c.f. identity verification records)

LRA 又は GlobalSign は、失効申請を行う要求者に対して、特定の情報を用いて本人確認を行い、その権限を認証する。LRA は、発行の記録（本人確認資料等）に基づき JCAN 証明書の失効を行うことができる。

4. Certificate Lifecycle Operational Requirements (証明書のライフサイクルに対する運用上の要求事項)

4.1 Certificate Application (証明書申請)

GlobalSign maintains its own blocklists of individuals from whom and entities from which it will not accept Certificate applications. In addition, other external sources such as government denied lists or internationally recognized denied persons lists which are applicable to the jurisdictions in which GlobalSign operates are used to screen out unwanted Applicants.

GlobalSign does not issue Certificates to entities that reside in Countries where the laws of a GlobalSign office location prohibit doing business.

LRAs have the duty to provide the JCAN Public CA with accurate information on certificate requests on behalf of the applicants.

Private keys bundled with the certificate issuance requests shall be brand-new per each time.

GlobalSign は、JCAN 証明書の申請を承認しない個人又はエンティティのリストを独自に作成する。加えて、GlobalSign が サービスを提供する国・地域の管轄政府当局が発行する、又は国際的に認知された取引禁止対象者リストなどの外部情報源に依拠して、JCAN 証明書を発行しない申請者を選別する。

GlobalSign は、その事業所の所在国の法律が取引を禁じる対象者に JCAN 証明書を発行しない。

LRA は、申請者に代わって提出する JCAN 証明書要求において、JCAN 認証局に正確な情報を提出する義務を負う。

JCAN 証明書発行の申請に紐づけられている秘密鍵は、各申請毎に新規で生成されたものでなくてはならない。

4.2 Certificate Application Processing (証明書申請手続き)

LRAs shall verify the Subjects and users through the verification steps prescribed in Article 3.2 at the time of vetting per every certificate issuance request. In case certificates are requested to be issued with the information succeeding that included in the JCAN certificates previously used, the record of verification may be reused.

LRA は、JCAN 証明書の各申請に対する審査時に、3.2 項に基づいてサブジェクトの識別と使用者の確認を行わなければならない。事前に利用していた JCAN 証明書に含まれていた情報と同一の情報が申請対象の JCAN 証明書に含まれる場合、検証記録を再利用可能である。

4.3 Certificate Issuance (証明書の発行)

After the verification of Certificate application, LRAs submit the Certificate issuance request to the JCAN Public CA securely.

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

- If PIN code is included in the request, JCAN Public CA generates Key Pairs securely, issues certificates, creates PKCS#12 file, and enables downloading the file.
  Then LRA downloads the file and lend it to the user;
- If PIN code is not included in the request, after inputting the PIN code, JCAN Public CA generates Key Pairs securely, issues certificates, creates PKCS#12 file, and enables downloading the file.
  The user then downloads the file directly from the download servers. The passwords required at the time of downloading is separately informed from the LRA to the user.

After certificate issuance, LRAs record the user name.

JCAN 証明書申請の検証後、LRA は、JCAN 認証局に JCAN 証明書発行の要求をセキュアに送信する。

JCAN 認証局は、JCAN 証明書発行の要求に問題がなければ、次の手順で JCAN 証明書を発行し配送する。

- JCAN 証明書発行の要求に PIN が含まれている場合、JCAN 認証局は、鍵ペアをセキュアに生成し、JCAN 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、LRA は、JCAN 証明書をダウンロードし使用者に貸与する。
- JCAN 証明書発行の要求に PIN が含まれていない場合、JCAN 認証局は、利用者からの PIN 入力後、鍵ペアをセキュアに生成し、JCAN 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 証明書をダウンロードサーバから直接ダウンロードする。ダウンロード時に必要なダウンロードパスワードは、LRA から使用者に別途連絡する。

LRA は、JCAN 証明書の使用者名を記録する。

4.4 Certificate Acceptance (証明書の受領)

The issued certificate is deemed to be accepted by Subscribers upon either of these conditions:

- If PIN code is included in the request: when the LRA delivered the certificate to users, or when the LRA delivered the certificate to the field where users only can access LRA;
- If PIN is not included in the request: when the Subscriber finishes downloading the certificate.

NOTE) Issued certificates will be deleted from the download servers after a certain period of time has passed.

発行された JCAN 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、LRA が利用者に配付した時、又は利用者のみがアクセスできる領域に配付した時
- 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 JCAN 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 (鍵ペアと証明書の利用)

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 in Article 1.3.

義務は 1.3 項参照

4.5.2 Usage of Keys and Certificates by Relying Parties (検証者による公開鍵、及び証明書の使用)

The obligations are described in Article 1.3.

義務は 1.3 項参照

4.6 Certificate Renewal (証明書の更新)

If JCAN certificates are renewed, upon receipt of the request, LRA shall authenticate Subject and identify users following the procedures in article 3.2. Private keys bundled with the requests shall be brand-new per each time.

JCAN 証明書を更新する際、LRA は申請に対し、3.2 項に基づいてサブジェクトの識別と使用者の確認を行わなければならない。申請に紐づけられている秘密鍵は、申請毎に新規で生成されたものでなくてはならない。

4.7 Certificate Modification (証明書記載情報の修正)

Certificates modification does not apply to JCAN certificates.

JCAN 証明書の変更は、適用しない。

4.8 Certificate Revocation (証明書の失効)

Following the circumstances below, revocation of JCAN certificates and update of CRL shall be completed within 72 hours.

1. LRAs revoke the certificates after implementing the checking procedures in Article 3.4 when LRAs accept the contact from Subscribers by Email concerning following matters:
   - Any Changes of the data recorded on 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.

2. LRAs or JCAN Public CA revoke the JCAN certificates at each of their own discretion if:
   - The Subject became not related to the ORGANIZATION due to the work termination, organization transfer, or termination of the organization.;
   - Any Subscriber has breached the obligations under this CP and the rules defined by LRAs;
   - An error or false is recorded on the certificate;
   - Private Key or CA Private Key becomes compromised;
   - The planned or unplanned timing when LRA's Accreditation gets invalidated.
   - JCAN Public CA terminates its services;
   - GlobalSign decides to revoke any certificates for other reasons.

If LRAs revoked certificates, they inform Subscribers of the revocation. If JCAN Public CA revoked certificates, they inform Subscribers of the revocation.

Once any certificates is revoked, it shall not be reinstated.

The integrity and authenticity of CRL shall be protected.

下記の条件に基づき、72 時間以内に JCAN 証明書を失効し、CRL の更新まで完了させる。

1. 利用者からの次の事項に係る連絡を受付けた場合、LRA は、3.4 項に基づく確認後、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
   - JCAN 証明書の信頼性が損なわれる可能性がある場合

2. 次の場合、LRA 又は JCAN 認証局は、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/又は 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
   - 利用者秘密鍵又は CA 秘密鍵が危殆化した
   - LRA が JTS 登録(LRA)の無効化を予定する時期、又は予期せず無効化した際
   - JCAN 認証局がサービスを終了する
   - GlobalSign がその他の理由で失効を決定した

LRA が失効した場合には、LRA が利用者に失効の通知をする。JCAN 認証局が失効した場合には、LRA 経由で利用者に失効の通知をする。

一旦 JCAN 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。

4.9 Certificate Status Services (証明書のステータス情報サービス)

JCAN Public CA provides Subscribers and Relying Parties with CRL services. JCAN Public CA offers certificate status confirmation services, including Web interfaces, to LRAs.

JCAN 認証局は、利用者及び検証者に対して、CRL を提供する。JCAN 認証局は LRA に対して、ウェブインターフェースを含む、JCAN 証明書ステータス情報サービスを提供する。

4.10 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、JCAN 証明書の失効、有効期間満了、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 article is prescribed in [CPS] of JCAN Public CA.

本項は、JCAN 認証局 の[CPS]で規定する。

5.2 Procedural Controls (手続き管理)

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

本項は、JCAN 認証局 の[CPS]で規定する。

5.3 Personnel Controls (人員コントロール)

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

本項は、JCAN 認証局 の[CPS]で規定する。

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

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

本項は、JCAN 認証局 の[CPS]で規定する。

5.5 Records Archival (アーカイブ対象記録)

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

LRA maintains the archived information through reliable methods.

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)

LRAs retain the information required for Subject's registration (c.f. consent forms and agreements, vetting records, verification records, etc.) for at least 7 years after the Certificate is expired or revoked.

LRAs accessing the Admin portal by API retain the logs of certificate issuance for at least 1 year.

LRA は、サブジェクトの登録に使用される情報(同意書、管理台帳、本人確認資料等)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。

API 接続する LRA は、JCAN 証明書発行に係るログ情報を、少なくとも 1 年間保持する。

5.6 Key Changeover (鍵交換)

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

本項は、JCAN 認証局 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 article is prescribed in [CPS] of JCAN Public CA.

本項は、JCAN 認証局 の[CPS]で規定する。

5.8 CA or RA Termination (認証局又は RA の稼動終了)

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

本項は、JCAN 認証局 の[CPS]で規定する。

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

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

本項は、JCAN 認証局 の[CPS]で規定する。

7. Certificate and CRL Profiles (証明書及び証明書失効リストのプロファイル)

7.1 Certificate Profile (証明書プロファイル)

The profile of JCAN certificate follows the X.509 Version 3 Format.

JCAN certificate's max validity period is 39 months.

JCAN Public CA and LRA ensure that over the lifetime of the CA, a distinguished name which has been used on a certificate 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 フォーマットに基づく。詳細は JCAN 認証局 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 認証局と LRA は、その 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。

7.2 CRL Profile (証明書失効リストのプロファイル)

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

本項は、JCAN 認証局 の[CPS]で規定する。

8. Compliance Audit and Other Assessment (準拠性監査及びその他の評価)

8.1 Frequency and Requirement of Audit (監査の頻度及び状況)

LRAs receive the re-registration to JTS Registration requirements at least once a year in order to have their service ensured of its conformity to the requirements, standards, procedures, and service levels of this CP. For this re-registration, LRAs implement internal audit on themselves.

The re-registration of JCAN Public CA to JTS Registration requirements is prescribed in [CPS].

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、JTS 登録(LRA)を受諾する。この JTS 登録更新のため、LRA は内部監査を実施する。

JCAN 認証局の JTS 登録については、[CPS]に規定する。

8.2 Auditor's Identity and Qualification (監査人の身元及び能力)

Internal audit of LRAs for re-registration to JTS Registration requirements is carried out by auditors with a firm auditing experience.

JTS 登録更新のために LRA が受ける外部監査及び実施する内部監査は、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 internal auditors of LRAs are independent from the business operations in the departments subject to this internal audit.

LRA の内部監査人は、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 Matters Subject to Internal Audit (監査対象項目)

The review on LRAs at the time of re-registration to JTS Registration requirements is based on LRA their conformity to this CP.

The review on JCAN Public at the time of re-registration to JTS Registration requirements is based on their conformity to the [CPS]

LRA の JTS 登録更新は、本 CP への準拠性に基づいて評価される。

JCAN 認証局の JTS 登録更新は、[CPS] の準拠性に基づいて評価される。

9. Other Business and Legal Matters (その他ビジネス及び法的事項)

9.1 Fees (費用)

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

本項は、JCAN 認証局 の[CPS]で規定する。

9.2 Financial Responsibility (財務上の責任)

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

本項は、JCAN 認証局 の[CPS]で規定する。

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

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

本項は、JCAN 認証局 の[CPS]で規定する。

9.4 Privacy of Personal Information (個人情報保護)

The retention of personal information by LRAs shall follow the concerning laws and regulations of the applicable country if any.

The Privacy Policy is published on GlobalSign's web site at https://www.globalsign.com/repository.

Personal information which LRA maintains is regarded as confidential except for explicitly published items such as JCAN certificates and CRL.

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。

プライバシーポリシーは、GlobalSign のウェブサイト https://jp.globalsign.com/repository/上で公開される。

LRA が保持する個人情報は、JCAN 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)

GlobalSign owns and reserves all intellectual property rights associated with publications originating from GlobalSign, including this CP.

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

9.6 Representations and Warranties (表明保証)

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

本項は、JCAN 認証局 の[CPS]で規定する。

9.7 Disclaimers of Warranties (保証の免責事項)

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

本項は、JCAN 認証局 の[CPS]で規定する。

9.8 Limitations of Liability (有限責任)

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

本項は、JCAN 認証局 の[CPS]で規定する。

9.9 Indemnities (補償)

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

本項は、JCAN 認証局 の[CPS]で規定する。

9.10 Term and Termination (期間及び終了)

This CP remains in force until GlobalSign notifies on the repository.

本 CP は、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 (関係者への個別通知及び伝達)

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

本項は、JCAN 認証局 の[CPS]で規定する。

9.12 Amendments (改正事項)

The GlobalSign PACOM1 - CA Governance Policy Authority, which is composed of members of the GlobalSign management team and appointed by its Board of Directors, is responsible for maintaining this CP.

GlobalSign should post appropriate notice on their web sites of any major or significant changes to this CP as well as any appropriate period by when the revised CP is deemed to be accepted.

GlobalSign の PACOM1 – CA Governance Policy Authority は、GlobalSign の経営チーム、及び GlobalSign の 取締役会で承認されたメンバーで構成されており、本 CP を維持管理する責任を負う。

GlobalSign は、本 CP に関する主要な又は重要な変更が為された際には、改定版の CP を承認するまでの、 一定の期間、その変更の件をウェブサイトに掲載するものとする。

9.13 Dispute Resolution Procedures (紛争解決に関する規定)

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

本項は、JCAN 認証局 の[CPS]で規定する。

9.14 Governing Law (準拠法)

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

本項は、JCAN 認証局 の[CPS]で規定する。

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

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

本項は、JCAN 認証局 の[CPS]で規定する。

9.16 Miscellaneous Provisions (一般事項)

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

本項は、JCAN 認証局 の[CPS]で規定する。

9.17 Other Provisions (その他の規定)

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

本項は、JCAN 認証局 の[CPS]で規定する。

10. Definitions and Acronyms (定義と略語)

CA (認証局)

A subject that issues, renews or revokes a certificates and creates the keys of CAs (Certification Authorities).

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 assigned by the person in charge of the LRA. A certificate applicant is a person who applies for a certificate on behalf of the Subject.

証明書申請者は、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 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 (証明書ポリシー)

regulation document regarding types of certificates, application, subject of issuance, usages, etc.

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)

document which explains the procedures and security criteria in operating CAs.

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 of certificates that are revoked before their expiration, recorded by the applicable CA.

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 LRAs to the issuing CA.

If issuing CA is requested for key generation, CSR and a key pair is created by RA and CSR is sent to the Issuing Authority

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。
尚、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。

JCAN Certificate (JCAN 証明書)

JCAN Certificates can be used for authentication, encryption, and digital signature.

Use of JCAN Certificates shall follow the laws and regulations of the applicable country if any.

JCAN 証明書は、認証、暗号化、電子署名で使用できる。
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 認証局)

JCAN Public CA consists of the JTS Registration -Accredited CA, and is being the Sub CA of Public Root CA.

JCAN 認証局は、JIPDEC による JIPDEC トラステッド・サービス登録（認証局）の基準に係る審査に合格した CA であり、パブリックルート CA のサブ CA である。

LRA (ローカル登録局)

LRA (Local Registration Authority) is the representative of users who passed the vetting on JTS Registration requirements as LRA. LRA manages certificate lifecycle through the vetting on the validity of DN to be included in JCAN certificates and identity verification under JCAN CP.

LRA とは、利用者の代表として JIPDEC による JIPDEC トラステッド・サービス登録の基準に係る審査に合格した LRA であり、JCAN 証明書ポリシーの下、JCAN 証明書に記載する DN の真正性の審査と利用者の本人確認を行い、証明書ライフサイクルマネージメント（発行、失効）を行う。

LRA Operator Certificate (アクセス認証用証明書)

LRA Operator Certificate is the certificate issued by GlobalSign to a person who is assigned by the LRA.

This certificate is used to authenticate the access to the certificate management services.

アクセス認証用証明書は、LRA が指名する人に、GlobalSign より発行される LRA 操作責任者用の電子証明書である。
この電子証明書は JCAN 証明書の発行など証明書管理サービスへのアクセスを認証するために用いる。

MEMBER (メンバー)

MEMBER is the ORGANIZATION's internal individual 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。

PERSON (人)

PERSON is a natural person.

自然人。

PARTNER (パートナー)

PARTNER is the ORGANIZATION's external person (who is contract party, group-company staff, member of any group, constituent of any committee, student, who are authenticated with reliable document sources, or who registered his/her credit card, etc.).

パートナーは、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 code

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)

The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

アプリケーションソフトウェアサプライヤーが配布するソフトウェアに搭載されるルート証明書を発行するトップ階層にある認証局で、下位認証局の証明書を発行する。

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又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 any network that verifies LRA requests for a certificate and requests CA for the certificate issuance.

ネットワークにおける登録局で、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 relies on a Subscriber's certificates and/or digital signatures. Relying Party shall refer to the revocation information of the CA in order to verify the validity of JCAN certificates.

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。

Sub CA (サブ CA)

CA which gets its validity authenticated upon the authentication from the 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 of certificate issuance.

The Subjects of JCAN Certificates are prescribed in Article 1.4.

証明書発行対象

JCAN 証明書のサブジェクトは、1.4 項で規定する。

X.400

One of the recommendations of ITU-TS and is the prescribed standard of emails.

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。