JCAN Public CA CPS
(Certification Practice Statement)
JCAN 認証局 CPS
(認証業務運用規程)

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
7	01/10/2022	Administrative update 外部要求に合わせた修正	GMOグローバルサイン	GMOグローバルサイン
6.1	15/05/2022	Administrative update JTS審査に合わせた修正	GMOグローバルサイン	GMOグローバルサイン
6.0	01/04/2022	Administrative update 外部要求変更に伴う修正	GMOグローバルサイン	GMOグローバルサイン
5.0	01/10/2021	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
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) applies to JCAN Public CA and prescribes JCAN Public CA's procedures and operations such as issuance and revocation of certificates in accordance with the format of RFC 3647.

JCAN Public CA has systems for the management of adequate quality and information security.

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

This CPS is administered by GlobalSign.

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 CPS.

本書(CPS)は、JCAN 認証局 に適用され、JCAN 認証局からの証明書の発行及び失効等の手続と運用を RFC 3647 の様式に従って規定するものである。 JCAN 認証局は、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 証明書のポリシーは、[CP]に規定する。

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。

GlobalSign の会社情報は以下の通り。

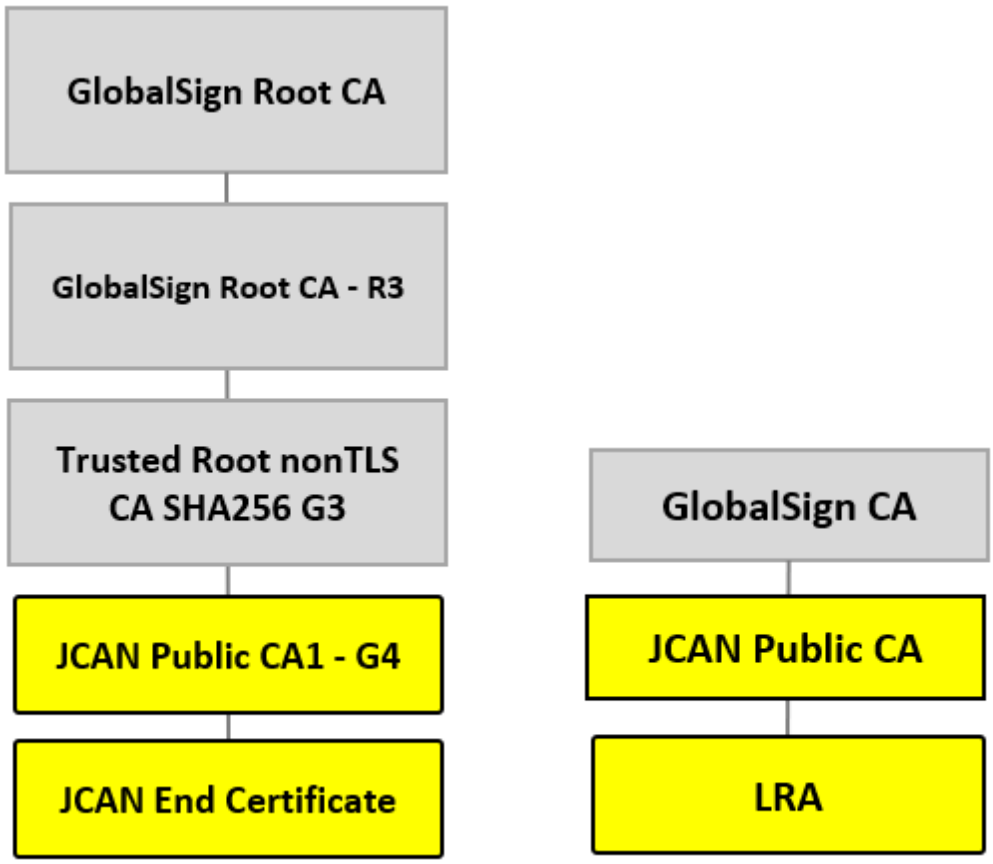
商業登記番号：0110-01-040181
法人番号：1011001040181

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 CPS 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 registered as accredited by JIPDEC after JIPDEC confirms the existence of their organization and their pass of the vetting on JIPDEC Trusted Service (JTS) Registration requirements (for LRAs), and then are authorized for the operation of the LRA.
JCAN Public CA is one of CAs which is accredited by JIPDEC on their pass of the vetting on JTS Registration requirements (for CAs).LRA

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 業務を行う組織の実在性確認と 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）」（以下、「JTS 登録(LRA)」という）の基準に係る審査に合格後、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 to the use/disclosure of their personal information by the LRA (for LRA's operation, LRA's response to audit/accreditation/legal-proceedings, etc) and to agree to the use/disclosure of their personal information recorded on a certificate by Relying Parties (for Relying Parties' operation, certificate validation by Relying Parties, etc) ;
- To agree with the LRA (= the representative of the subscribers) to back up the certificates in PKCS#12 format and their PIN codes in case these PINs have been generated by the LRA;
- To use the certificate only for the permitted usages after agreeing to this CPS;
- 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 CPS 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 comply with the JTS requirements for LRAs
- 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.

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 CPS 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。 LRA の義務は、以下の通りである。

1.全般

- JTS 登録(LRA)の基準 へ準拠する。
- 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。

2.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。

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、JCAN 証明書を速やかに失効する。
- 利用者が本 CPS 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。
検証者の義務は、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 Practice statement regarding the purpose of use, scope of use, and procedures. Subscribers are contacted through the LRA.

The obligations of the JCAN Public CA are the followings:

- After generating the certificates (formatted in pkcs#12), JCAN Public CA protects the private key with PIN codes. These PIN codes are not retained but destroyed by JCAN Public CA.
- JCAN Public CA guarantees the unique identification allotted to the subscribers within the domain of its JCAN Public CA. JCAN Public CA guarantees the unique identification allotted to OrganizationUnitName1 within Subject;
- JCAN Public CA manages the policies of JCAN Public CA;
- The confidentiality and integrity of registered data is ensured by JCAN Public CA through adequate controls at all times.

JCAN 認証局は、JCAN 証明書業務運用規程に従い 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 CA である。
利用者への連絡は LRA を通じて行う。
本 CA は、GlobalSign が運用する。本 CA の義務は以下の通りである。

- JCAN 認証局は、PKCS#12 形式証明書を生成した後は、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 認証局は、 JCAN 認証局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。また、サブジェクトの OrganizationUnitName1 の唯一性を保証する。
- JCAN のポリシーの管理
- 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) JPDEC 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 Usage (証明書の使用方法)

(1) JCAN Certificates (JCAN 証明書)

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

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 (PS1)

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
- 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

(2) LRA Operator Certificates (アクセス認証用証明書)

LRA Operator Certificates are the certificates issued to LRAs.

LRA Operator Certificates are used to access “JCAN certificates issuance service site” at the time of JCAN Certificates’ issuance or revocation.

LRA Operator Certificates may be issued from a CA other than JCAN Public CA.

アクセス認証用証明書は、LRA に発行される証明書である。
アクセス認証用証明書は、JCAN 証明書の発行/失効時に「JCAN 証明書発行サービスサイト」へのアクセスに用いる。
アクセス認証用証明書は、JCAN 認証局以外の CA から発行してもよい。

(3) Test Certificate (テスト証明書)

For the purpose of testing the operational status of JCAN Public CA, JCAN Public CA issues Test Certificates.

Test certificate profile is configured in a way the testing purpose is identifiable. the text “TEST” in the CommonName (CN=TEST …) is a Test Certificate.

The accuracy, authenticity, integrity or adequacy to any specific purposes of the information included in these Test Certificates is not warranted.

JCAN 認証局の稼働確認を目的に、 JCAN 認証局は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 CPS.

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 CPS を維持管理する責任を負う。

1.5.2. Contact Address (連絡先)

The contact details of JCAN Public CA (GlobalSign) is the following:
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, 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 section 4.8 for detail of actions performed by GlobalSign for making this decision.

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、検証者、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。

1.6 Definitions and acronyms (定義と略語)

1.6.1. Definitions (定義)

Baseline Requirements

CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

CA/B Form による、パブリックに信頼される証明書の発行及び管理のための要件

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。

JTS Requirements (JTS 登録の基準)

Requirements for JIPDEC Trusted Service by JIPDEC

JIPDEC による JIPDEC トラステッド・サービス登録制度の基準

LRA (ローカル登録局)

LRA (Local Registration Authority) is the representative of Subscribers which 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 and CPS.

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（LRA）の基準に係る審査に合格した LRA であり、JCAN 証明書ポリシー及び業務運用規程の下、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。

Mozilla Root Store Policy
Root store policy by Mozilla
Mozilla によるルートストアのポリシー

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 に発行依頼を行う。

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 Section 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。

1.6.2. References (参考)

JCAN Certificate Policy

JCAN 認証局の CP

2. Publication and Repository Responsibilities

2.1. Repositories (リポジトリ)

GlobalSign reserves the right to publish the information about this CPS, [CP], and JCAN

certificates that are published on the repository. GlobalSign publishes the information about CRL on the repository.

These public information are made available by 24 x 365.

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

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。
訴訟の際に認証の証拠を提供する目的又は監査対応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 CPS
- Other information regarding JCAN

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 CPS
- 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 CP 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. Update frequency of the CRL is within 24 hours.

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

本 CPS は、PACOM1 – CA Governance Policy Authority 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。CRL の更新頻度は 24 時間以内である
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。

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

GlobalSign maintains its repository publicly available.

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 CPS.

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 CPS 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)

(1) JCAN Advanced

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

- 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

1. 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.
2. 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.

3. 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.

JCAN 証明書の各申請ごとに、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) per each certificate request:

1. If 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 section 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 section 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

JCAN 証明書の各申請ごとに、 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 Section 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.

These verification records shall not be reused.

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。
当審査記録を再利用することはできない。

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@、その後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）を送信した後、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 Section 3.2.2 and 3.2.3

鍵更新要求に対する本人確認は 3.2.2 及び 3.2.3 項に規定する。

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)

All revocation requests are authenticated by LRAs or GlobalSign.

Revocation requests may be granted following a suitable challenge response such as proving possession of unique elements incorporated into the Certificate (e.g., Domain Name or email address) or authentication of specific information from within the account which is authenticated out of band.

LRA 又は GlobalSign は、全ての失効申請について認証する。
利用者からの失効申請は、JCAN 証明書に記載されたドメイン名や電子メールアドレス等が要求者の所有するものであることの確認、ネットワークを経由しない方法で検証済の特定の情報を用いて認証を行うなどの、適切なチャレンジ・レスポンス方式があった場合に認められる。

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 Section 3.2.2 and 3.2.3 at the time of vetting per every certificate issuance request.

LRA は、JCAN 証明書の各申請に対する審査時に、3.2.2 及び 3.2.3 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。

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 Section 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 Section 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 section 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 Re-key (証明書の鍵更新)

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

JCAN 証明書に対し鍵更新する際、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。

4.8. 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。

4.9. Certificate Revocation and Suspension (証明書の失効及び効力の一時停止)

4.9.1 Revocation circumstances (失効の条件)

LRAs or JCAN Public CA revoke(s) JCAN certificates within twenty-four (24) hours under the following circumstances:

- The Subscriber reports the loss or theft of PC or Media in which JCAN Certificates are installed.
- The Subscriber has breached the rules defined by LRAs;
- The Subscriber requests in writing (to the LRA / JCAN Public CA which provided the Certificate) that they wish to revoke the Certificate.
- The subscriber indicates that the original certificate request was not authorized and does not retroactively grant authorization
- LRAs or JCAN Public CA obtain(s) reasonable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise.
- LRAs or JCAN Public CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);

- The evidence is obtained that the validation of domain authorization or mailbox control for any email address in the Certificate should not be relied upon.
- LRAs or JCAN Public CA receives notice or otherwise becomes aware of unexpected termination of a Subscriber's or Subject's agreement or business functions

以下の条件下で、LRA 又は JCAN 認証局は 24 時間以内に JCAN 証明書を失効する：

- JCAN 証明書がインストールされた PC 又は媒体が紛失や盗難に遭ったことを利用者が報告した場合。
- LRA が規定した規則に利用者が違反した場合。
- 利用者が証明書の失効を希望する旨を書面で（証明書を発行した LRA / JCAN 認証局 に）申請した場合。
- 利用者が、元の証明書申請が承認されておらず、遡及的に承認を付与していないことを、LRA 又は JCAN 認証局へ通知した場合。
- (証明書の公開鍵と対になる) 利用者の秘密鍵が危殆化したという合理的な証拠を、LRA 又は JCAN 認証局が取得した場合。
- 証明書の公開鍵に基づいて利用者の秘密鍵を容易に計算できる、実証済み又は証明された方法を、LRA 又は JCAN 認証局が認識した場合。（例えば、Debian の脆弱な鍵など https://wiki.debian.org/SSLkeys を参照）
- 証明書に含まれるメールアドレスへ実施した、ドメイン捜査権又はメールアドレスの捜査権に対する十分性確認の結果へ、依拠すべきでないという証拠を取得した場合。
- 利用者又はサブジェクトとの合意又は業務が予期せず終了したことを、通知又はその他の方法で、 LRA 又は JCAN 認証局が認識した場合。

LRAs or JCAN Public CA revoke(s) JCAN certificates within twenty-four (24) hours and is performed within 5 days if one or more of the following occurs:

- The Certificate no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, as specified in Sections 6.1.5 and 6.1.6.
- LRAs or JCAN Public CA obtain(s) the evidence that the Certificate was misused.
- LRAs or JCAN Public CA receive(s) notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement or Terms of Use.
- LRAs or JCAN Public CA receive(s) notice or otherwise becomes aware of a material change in the information contained in the Certificate. (e.g. The Subject became not related to the ORGANIZATION due to the work termination, organization transfer, or termination of the organization.)
- LRAs or JCAN Public CA are/is made aware that the Certificate was not issued in accordance with Mozilla requirements and/or JCAN CP or CPS.

- LRAs or JCAN Public CA determine(s) that any of the information appearing in the Certificate is not accurate or is misleading.
- The right of LRAs or JCAN Public CA to issue Certificates under the JTS requirements and/or this CPS expires or is revoked or terminated, unless GlobalSign has made arrangements to continue maintaining the CRL/OCSP Repository.
- LRA or JCAN Public CA are/is made aware of a demonstrated or proven method that exposes the Subscriber’s Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.
- Revocation is required by JCAN CP and/or CPS.
- LRAs or JCAN Public CA receive(s) notice or otherwise becomes aware of any circumstance indicating that use of the email address in the Certificate is no longer legally permitted.
- The CA Private Key used in issuing the Certificate is suspected to have been compromised.
- LRAs or JCAN Public CA cease(s) operations for any reason and another LRA/CA has not been arranged to provide revocation support for the Certificate.
- When the reliability of the JCAN Certificates may be damaged.

JCAN 証明書の失効は、LRA 又は JCAN 認証局により 24 時間以内に実施されるべきであり、以下のうち 1 つ以上の状況が発生した場合、5 日以内に実施される：

- 証明書が、6.1.5 項及び 6.1.6 項に規定されているように、Baseline Requirements のアルゴリズムの 種類及び鍵長についての要件をもはや準拠していない場合。
- 証明書が不正使用されたことを示す証拠を、LRA 又は JCAN 認証局が取得した場合。
- 利用者が利用約款に規定された重要な義務に対し違反をした旨、LRA 又は JCAN 認証局が通知を受ける又は 認識した場合。
- 証明書に含まれる情報に重大な変更があった際、 LRA 又は JCAN 認証局がその通知を受けた、またその他の方法で知った場合。（例: 契約終了・退職、異同、組織の閉鎖等によりサブジェクトが当該組織と無関係になった場合。）
- 証明書が Mozilla の要件且つ/或いは JCAN CP 又は CPS に従って発行され たものではないことを、LRA 又は JCAN 認証局が認識した場合。
- 証明書に記載される情報の何れかが正確でないか、誤解を招く恐れがあると、 LRA 又は JCAN 認証局が判断した場合。
- CRL/OCSP リポジトリの維持管理を継続するための調整が行われず、 LRA 又は JCAN 認証局が JTS 登録の基準且つ/又は CPS に従った証明書を発行する権利が満了する、失効する、或いは破棄された場合。
- 利用者の秘密鍵に危殆化をもたらす実証又は証明済みの方法について LRA 又は JCAN 認証局が認識した場合、又は利用者の秘密鍵を生成するのに用いられた方法に欠陥があるという明確な証拠がある場合。
- JCAN CP 及び/又は CPS により失効が要求された場合。

- LRA 又は JCAN 認証局が、証明書に記載された電子メールアドレスの使用が法的に許可されていないことを示す通知を受け取るか、又は、その他の方法で知った場合。
- 証明書を発行する際に使用された CA の秘密鍵が漏洩した疑いがある場合。
- LRA 又は JCAN 認証局が何らかの理由で業務を停止し、他の LRA / CA が証明書の失効を補助するよう調整が行われていない場合。
- JCAN 証明書の信頼性が損なわれる可能性がある場合。

Revocation of JCAN certificates may also be performed by LRAs or JCAN Public CA within a commercially reasonable period of time under the following circumstances:

- The Subscriber or organization administrator requests revocation of the Certificate through GCC account which controls the lifecycle of the Certificate.
- The Subscriber requests revocation through an authenticated request to GlobalSign's report abuse.
- LRA or JCAN Public CA receives notice or otherwise becomes aware that the Subscriber has been added as a denied party or prohibited person to a blocklist, or is operating from a prohibited destination under the laws of the applicable jurisdiction of operation.
- Overdue payment of applicable fees by the Subscriber.
- Under certain licensing arrangements, LRA of JCAN Public CA may revoke Certificates following expiration or termination of the license agreement.
- LRA or JCAN Public CA determines the continued use of the Certificate is otherwise harmful to the business of LRA, GlobalSign, or third parties. When considering whether Certificate usage is harmful to GlobalSign’s or a third party’s business or reputation, LRA or JCAN Public CA will consider, among other things, the nature and number of complaints received, the identity of the complainant(s), relevant legislation in force, and responses to the alleged harmful use by the Subscriber.
- If Microsoft, in its sole discretion, identifies a certificate whose usage or attributes are determined to be contrary to the objectives of the Trusted Root Program, Microsoft will notify GlobalSign and request that it revoke the certificate. GlobalSign will either revoke the certificate or request an exception from Microsoft within 24 hours of receiving Microsoft's notice. Microsoft will review submitted material and inform GlobalSign of its final decision to grant or deny the exception at its sole discretion. In the event that Microsoft does not grant the exception, GlobalSign will revoke the certificate within 24 hours of the exception being denied.
- Death of a Subscriber.
- LRA or JCAN Public CA decides to revoke any certificates for other reasons.

次に掲げる事情があるときは、 LRA 又は JCAN 認証局は商業上合理的な期間内に JCAN 証

明書の失効を実施することとする：

- 利用者又は組織の管理者が、証明書のライフサイクルを管理する GCC アカウントを通じて証明書の失効を申請する場合。
- 利用者が、GlobalSign の report-abuse@globalsign.com へ、認証済みの申請方法によって失効申請した場合。
- 利用者が禁止対象者としてブロックリストに追加されたこと、又は管轄地域の法律に基づき禁止された地域から営業していることについて、LRA 又は JCAN 認証局が通知を受領する又は発見した場合。
- 支払い遅延が利用者よりあった場合。
- 一定のライセンス契約に基づき、LRA 又は JCAN 認証局は、ライセンス契約の満了又は終了後、証明書を取り消 すことができる。
- LRA 又は JCAN 認証局は、JCAN 証明書の継続使用が LRA, GlobalSign, 又は第三者の事業に有害になりうるかの判断を行う。 証明書の利用が LRA, GlobalSign, 又は第三者の事業又は評判に悪影響を及ぼすかどうかを検討する際、LRA 又は JCAN 認証局 はとりわけ、受領した苦情の性質及び件数、苦情申立人の身元、有効な関連法規、及び利用者による有害とされる使用への対応を検討する。
- Microsoft は、専らその裁量で、証明書の用途ないし属性情報が Trusted Root Program の趣旨に反して いると認定した場合、GlobalSign に連絡し、証明書の失効を要求する。GlobalSign は、本証明書を失 効するか、又は Microsoft の要請を受領後 24 時間以内に Microsoft に例外を申請する。Microsoft は、 提出物を確認し、専らその裁量で、例外を許可又は拒否するか、最終決定を GlobalSign に通知する。 Microsoft が例外を認めない場合、GlobalSign は、例外が拒否されてから 24 時間以内に本証明書を失 効させる。
- 利用者の死亡
- LRA 又は JCAN 認証局がその他の理由で失効を決定した場合。

Revocation of JCAN Public CA Certificate is performed by GlobalSign within seven (7) days under the following circumstances:

- GlobalSign obtains reasonable evidence that the JCAN Public CA’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements for algorithm type and key size of the Baseline Requirements as specified in Sections 6.1.5 and 6.1.6
- GlobalSign obtains evidence that the Certificate was misused.
- GlobalSign is made aware that the Certificate was not issued in accordance with or that the JCAN Public CA has not complied with Mozilla requirements and/or applicable CP or CPS.
- GlobalSign determines that any of the information appearing in the Certificate is inaccurate or misleading.

- GlobalSign or JCAN Public CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate
- GlobalSign’s or a Subordinate CA’s right to issue Certificates under JTS requirements and/or this CPS expires or is revoked or terminated, unless the issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository.
- Revocation is required by the Issuing CA’s CP and/or CPS.
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g., the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

次の場合、 GlobalSign は JCAN 認証局の証明書を 7 日以内に失効する。

- 証明書内の公開鍵に対応する JCAN 認証局 の秘密鍵が危殆化した、又は、6.1.5 項及び 6.1.6 項に規定されているように、Baseline Requirements のアルゴリズムの種類及び鍵のサイズの 要件をもはや満たさないという合理的な証拠を、GlobalSign が取得した場合。
- 証明書が不正使用されたことを示す証拠を取得した場合。
- 証明書が Mozilla の要件且つ/或いは JCAN CP 又は CPS に従って発行されていないこと、或いは JCAN 認証局 が Mozilla の要件且つ/或いは JCAN CP 又は CPS を遵守していないことを、GlobalSign が発 見した場合。
- GlobalSign が、証明書に表示される情報の何れかが不正確であるか、誤解を招く恐れがあると判断した場合。
- GlobalSign 又は JCAN 認証局が、何らかの理由で業務を停止し、他の CA が証明書の失効を補助するよう調整が行われていない場合。
- CRL/OCSP リポジトリの維持管理を継続するための調整をすることなく、GlobalSign 又は JCAN 認証局が JTS 登録の基準かつ/または CPS に従った証明書を発行する権利が満了する、失効する、或いは破棄された場合
- JCAN CP 及び/又は CPS により失効が要求される場合。
- 証明書の技術的な内容又は書式が、アプリケーションソフトウェアサプライヤ又は検証者に、 許容できないリスクをもたらす場合。(例えば、推奨されない暗号/署名アルゴリズム又は鍵のサイズが容 認できないリスクをもたらし、そのような証明書が一定の期間内に CA によって取り消され、置き 換えられるべきであると、CA/B Forum が判断する可能性がある場合)

4.9.2 Who Can Request Revocation (失効の申請者)

GlobalSign and JCAN LRAs will accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or

an affiliated organization named in the Certificate.
Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports to notify GlobalSign of a suspected reasonable cause to revoke a Certificate.

GlobalSign 及び LRA は、失効申請が権限を有すると検証できた場合に要求を承認する。失効申請は、利用者 本人又は証明書に記載された組織から提出された場合、権限のある要求として受理される。
利用者、検証者、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、証明書を取り消す合理的な理由が疑われる場合、電子証明書の問題報告を提出し、その旨を GlobalSign に通知することができる。

4.9.3 Procedure for Revocation Request (失効申請の処理手続き)
Due to the nature of revocation requests and the need for efficiency, GlobalSign provides automated mechanisms for requesting and authenticating revocation requests. The primary method is through the GCC account used to issue the Certificate that is requested to be revoked. Alternative out of band methods may be used, such as receipt of a fax/letter/phone call, the origins of which must be authenticated using shared secrets from the GCC account. Alternatively, where GCC accounts are not provided, methods may be used which rely on a demonstration of control of one or more elements of the Subject DN of the Certificate. For S/MIME Certificates, it could include demonstration of control of the email address. GlobalSign and JCAN LRAs will record each request for revocation and authenticate the source, taking appropriate action to revoke the Certificate if the request is authentic and approved.

Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Report via report-abuse@globalsign.com. GlobalSign may or may not revoke in response to this request. See section 4.9.5 for detail of actions performed by GlobalSign for making this decision.

If revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs are published according to this CPS.

失効申請の持つ性質と効率化の観点から、GlobalSign は失効申請を要求し、認証するための自動化されたメカニズムを提供する。主な方法は、GCC アカウントを通じて発行した証明書の失効申請を行う方法がある。次に代替 方法として、ファックス、郵便、電話などを通じて、ネットワークを経由せずに失効を要求することができる。また、GCC アカウントが提供されない利用者については、証明書のサブジェクト識別名に関連する一つ以上の要素に対する管 理権限を実

証する方法で、失効申請権限を検証することもできる。S/MIME 証明書については、電子メールアドレス の管理権限の検証をもって代替とすることが可能である。

GlobalSign 及び RA は、失効申請を記録し、その情報源を認証する。要求が真正であり承認された場合に は、適切な失効手続きを取る。利用者、検証者、アプリケーションソフトウェアサプライヤー、及びその他第三者は、reportabuse@globalsign.com に証明書の問題報告を提出することができる。GlobalSign は、この申請に対応して失効する場合及び、しない場合がある。この意思決定の GlobalSign による判断基準は、4.9.5 項を参照すること。失効された場合、証明書のシリアル番号、失効日、失効時刻が CRL に記載される。理由コードを含むこともある。 CRL は本 CPS に準拠して発行される。

4.9.4 Revocation Request Grace Period (失効申請までの猶予期間)

The revocation request grace period is the time available for a Subscriber to take any necessary actions themselves to request revocation of a suspected Key Compromise, use of a weak key or discovery of inaccurate information within an issued Certificate. A risk analysis shall be completed and recorded for any revocations that cannot be processed by Subscribers, JCAN LRAs, or GlobalSign for any reason. Subscribers have 48 hours to inform GlobalSign or the JCAN LRA of a key compromise.

危殆化の疑いがある場合、脆弱な鍵を使用した場合、発行を受けた証明書に記載された情報に不正確な内容が含まれていた場合などに、利用者が失効を要求する前に必要な対策を取るための時間を指す。利用者、GlobalSign の何れかが、何らかの理由により失効を処理できない場合、リスク分析を行い、記録する。
利用者は 48 時間以内に GlobalSign 又は LRA に鍵の漏洩を通知する。

4.9.5 Time Within Which CA Must Process the Revocation Request (認証局が失効申請を処理すべき期間)

GlobalSign shall begin investigating Certificate Problem Reports within twenty-four (24) hours of receipt of the report.

GlobalSign maintains 24 x 7 ability to respond internally to a high-priority Certificate Problem Report and, where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint. GlobalSign will begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 24 hours of receipt of the report.

GlobalSign decide(s) whether revocation or other action is warranted based on at least the

following criteria:

- The nature of the alleged problem.
- The number of reports received about a particular Certificate or Subscriber.
- The entity making the complaint; and
- Relevant legislations.

エンドエンティティ証明書の失効申請については、GCC アカウントを通じて送信された失効申請、及び GlobalSign が失効手続きを開始したものの何れであっても、受理から 24 時間以内に処理されなければならない。

GlobalSign は、優先順位の高い証明書の問題報告に 24 時間 365 日社内で対応できる体制を整えており、必要に応じて、そのような申し立てを法執行機関に転送し、また、そのような申し立ての対象である証明書を失効する。GlobalSign は、証明書の問題報告を受領してから 24 時間以内に、証明書の危殆化又は不正使用が疑われる場合の捜査手続きを開始する。

GlobalSign は、少なくとも以下の基準に基づいて、失効又はその他の措置が正当化されるかどうかを決定する。

- 申し立ての問題の性質
- 特定の証明書又は利用者に関して受け取った報告の件数
- 申し立てを行っている主体、及び
- 関連規則

4.9.6 Revocation Checking Requirements for Relying Parties (失効情報確認に関する検証者への要求事項)

Prior to relying upon a Certificate, Relying Parties must validate the suitability of the Certificate to the purpose intended and ensure the Certificate is valid, otherwise all warranties become void.

Relying Parties will need to consult the CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI).

GlobalSign will include all applicable URLs within the Certificate to aid Relying Parties in performing the revocation checking process.

証明書に記載された情報を信頼し依拠する前に、検証者は、証明書が適正な目的のために使用されているこ と、証明書が有効であることを確認しなければならず、これを怠った場合には、全ての保証は無効となる。

検証者は依拠しようとする証明書がチェーンされる全ての階層の証明書について、CRL 又は OCSP の情報を 参照すべきであり、またこのチェーンが完全であることを検証すべきである。これには、認証局鍵識別子(以下、「AKI」 という)及びサブジェクト鍵識別子(以下、「SKI」という)の十分性検証を含む。

GlobalSign は、検証者が失効情報の検証を容易に行えるよう URL を証明書に記載する。

4.9.7 CRL Issuance Frequency (CRL の発行頻度)

If GlobalSign decides or is required to terminate a CRL or revoke an Issuing CA, GlobalSign issues and publishes at the corresponding CRL Distribution Point a last CRL with a nextUpdate field value of "99991231235959Z". GlobalSign does not issue a last CRL until all certificates in the scope of the CRL are either expired or revoked. The last CRL is made available until the expiry of the Issuing CA certificate and the integrity of the CRL is preserved during this period.

For the status of Subscriber Certificates: For CAs that publish a CRL, the CRL will be updated and re-issued at least once every seven days, and the value of the nextUpdate field will not be more than ten days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates: If the Subordinate CA contains a CDP, CRLs will be updated and re-issued at least (i) once every 3 months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field will not be more than twelve months beyond the value of the thisUpdate field.

GlobalSign が CRL を終了させるか発行局を失効させることを決定した、又は必要がある場合、GlobalSign は nextUpdate フィールドの値が「99991231235959Z」である最後の CRL を発行し、対応する CRL 配布ポイントで公 表するものとする。GlobalSign は、CRL の範囲内の全ての証明書が期限切れ又は失効するまで、最後の CRL を発 行しない。最後の CRL は CA 証明書の有効期限が切れるまで利用可能となり、この間 CRL の完全性を保つものと する。

利用者証明書のステータスについて： CA が CRL を発行する場合、CRL は少なくとも 7 日毎に更新、再発行され、nextUpdate フィールドの値は、thisUpdate フィールドの値から 10 日を超えてはならない。

下位 CA 証明書のステータスについて： 下位 CA 証明書に CDP(CRL distribution point) が含まれている場合、CRL は、(i) 少なくとも 3 か月に 1 回、(ii) 下位 CA 証明書の失効後 24 時間以内に更新、再発行され、nextUpdate フィールドの値は、thisUpdate フィールドの値より 12 ヵ月を超えては ならない。

4.9.8 Maximum Latency for CRLs (CRL の最大通信待機時間)

CRLs are posted to the repository within a commercially reasonable time after generation.

CRL は生成後、商業的に合理的な期間内にリポジトリに投稿される。

4.9.9 On-Line Revocation/Status Checking Availability (オンラインでの失効情報の確認)

GlobalSign supports OCSP responses in addition to CRLs. Response times are generally no longer than 10 seconds under normal network operating conditions. GlobalSign OCSP responses conform to RFC6960 and/or RFC5019. OCSP responses are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. OCSP signing Certificate contains an extension of type id-pkixocsp-nocheck, as defined by RFC6960.

GlobalSign は、CRL の他、OCSP レスポンダにより失効情報を提供する。通常のネットワーク環境においては、 OCSP による応答までの待機時間は通常 10 秒を超えない。 GlobalSign OCSP 応答は、RFC6960 及び/又は RFC5019 に準拠している。 OCSP 応答は、失効ステータスが確認されている証明書を発行した CA によって署名された証明書を持つ OCSP レ スポンダによって署名される。OCSP 署名証明書は、RFC6960 によって定義されるように、id-pkix-ocsp-nocheck 型 の拡張子を含む。

4.9.10 On-Line Revocation Checking Requirements (オンラインでの失効情報の確認の要件)

For the status of Subscriber Certificates:

1. OCSP responses have a validity interval greater than or equal to eight hours.
2. OCSP responses have a validity interval less than or equal to ten days.
3. For OCSP responses with validity intervals less than sixteen hours, GlobalSign updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
4. For OCSP responses with validity intervals greater than or equal to sixteen hours, GlobalSign updates the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of Subordinate CA Certificates:

・ GlobalSign updates information provided via an OCSP Responder (i) at least every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

OCSP Responders that receive a request for status of a Certificate that has not been issued, shall not respond with a "good" status for such Certificates.

OCSP Responders for CAs which are not Technically Constrained, in line with Section 7.1.5, will not respond with a "good" status for such Certificates.

GlobalSign requires OCSP requests to contain the following data:
・Protocol version
・Service request
・Target Certificate identifier

利用者証明書のステータスについて：
1. OCSP レスポンスの有効期間は、8 時間以上とする。
2. OCSP レスポンスの有効期限は 10 日以下とする。
3. 有効期間が 16 時間未満の OCSP レスポンスについては、GlobalSign は有効期間の半分が経過するより前に、OCSP を介して提供される情報を更新するものとする。
4. 有効期間が 16 時間以上の OCSP レスポンスについては、GlobalSign は OCSP を介して提供される情 報を、少なくとも nextUpdate の 8 時間前から thisUpdate の 4 日後までに更新するものとする。

下位 CA 証明書のステータスについて：
・GlobalSign は、OCSP レスポンダを通じて提供される情報を、少なくとも(i) 12 か月毎、及び(ii) 下位 CA 証明 書を失効した後 24 時間以内に更新する。

発行されていない証明書のステータスのリクエストを受け取った OCSP レスポンダは、そのような証明書に対して「有効」と応答しない。

7.1.5 項に従った技術的な制約をされていない CA の OCSP レスポンダは、このような証明書に対して「有効」と応答 しない。

GlobalSign は、OCSP リクエストに次のデータを含めるよう要求する：
・ プロトコルバージョン
・ サービス要求
・ 対象証明書識別子

4.9.11 Other Forms of Revocation Advertisements Available (その他の方法による失効情報の提供)

No stipulation

規定なし

4.9.12 Special Requirements Related to Key Compromise (認証局の鍵の危殆化に伴う特別な要件)

GlobalSign and JCAN LRAs shall use commercially reasonable methods to inform Subscribers that their Private Key may have been Compromised. This includes cases where new vulnerabilities have been discovered or where the Issuing CA at their own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed, GlobalSign shall revoke Issuing CA Certificates or Subscriber end entity Certificates within 24 hours and publish online CRLs within 30 minutes of creation and ARLs within 12 hours.

Parties may use the following methods to demonstrate key Compromise:

・Submission of a CSR file, created and signed by the private key. The CSR file needs to contain one of the following:

- o A specific string that GlobalSign has provided to the reporter.

OR

- o A string of text that clearly indicates compromise.

・ Providing references to vulnerability and/or security incident sources from which the Compromise is verifiable

・Submission of binaries that contain a Compromised Private Key, including the method to extract the Private Key

GlobalSign 及び LRA は、その秘密鍵が危殆化した恐れがあるときには、合理的な方法をもって利用者にその旨 の通知をする。これには、脆弱性が発見された場合、及び GlobalSign が自己の裁量により鍵の危殆化の疑いがある と判断した場合などが含まれる。鍵の危殆化に疑いの余地がない場合、GlobalSign は発行 CA の証明書、エンドエ ンティティ証明書などを 24 時間以内に失効し、CRL をオンラインで 30 分以内に、及び ARL を 12 時間以内に発行 する。

当事者は、鍵の危殆化を証明するために以下の方法を用いることができる。:

・ 秘密鍵で作成され署名された CSR ファイルの提出。CSR ファイルには以下のいずれかが含まれていること。

- o グローバルサインが報告者に提供した特定の文字列。

または

- o 明らかに侵害を示す文字列。

・ 危殆化を検証するうえでの参照先となる、脆弱性及び/又はセキュリティインシデントに関する情報や解説 資料の提供

・ 秘密鍵を抽出する方法を含む、侵害された秘密鍵を含むバイナリの提出 GlobalSign は他の要求を分析し、新しい提出方法が受け入れられる場合には、それに応じて 本 CPS を更新する。

4.9.13 Circumstances for Suspension (証明書の効力の一時停止を行う条件)

Certificate suspension is not applicable to JCAN.

証明書の効力の一時停止は JCAN 証明書に該当しない。

4.9.14 Who Can Request Suspension (証明書の効力の申請者)

Certificate suspension is not applicable to JCAN.

証明書の効力の一時停止は JCAN 証明書に該当しない。

4.9.15 Procedure for Suspension Request (証明書の効力の一時停止手続き)

Certificate suspension is not applicable to JCAN.

証明書の効力の一時停止は JCAN 証明書に該当しない。

4.9.16 Limits on Suspension Period (証明書の効力の一時停止期限)

Certificate suspension is not applicable to JCAN.

証明書の効力の一時停止は JCAN 証明書に該当しない。

4.10. 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。

4.11. 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、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。

4.12. Key Escrow and Recovery (キーエスクローとリカバリー)

CA Private Keys are never escrowed. GlobalSign does not offer key escrow services to Subscribers.

認証局の秘密鍵は預託（エスクロー）されてはならない。GlobalSign は利用者に対してもキーエスクローサービスを 提供しない。

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)

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, monitoring and alarming systems are equipped to detect, record, and react in a timely manner upon any unauthorized and/or irregular attempts of access.

The Data Center implements preventive measures against water damage, earthquakes, fire, and other disasters as well as other structural measures to prevent physical damage to the facility.

The access to the CA is restricted to the members who are designated on the Access management list. Visitors to the Data Center must always be accompanied by these members.

JCAN 認証局 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又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ーに制限する。データセンターへの訪問者は、常に当該メンバーに同伴されていなければならない。

5.2. Procedural Controls (手続き的管理)

JCAN Public CA follows personnel practices that provide reasonable assurance of the staff's trustworthiness and competence in technical operation.

All JCAN Public CA personnel in trusted roles shall be free from monetary or internal or external pressures that might impact the equity of CA operations.

The trusted role of JCAN public CA is following.

Certification Authority Manager : The responsibility for all the necessary tasks concerning operation of CAs, including any outsourced JCAN public CA.

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

JCAN 認証局 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 認証局 の要員は、CA 運用の公平さを偏らせる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 認証局 の信頼された役割には以下を含む。

・認証局責任者 : 本 CA の運用に係る全ての必要な作業の責任を負う。上記規定は JCAN 認証局 の委託先にも適用する。
JCAN 認証局 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。

5.3. Personnel Controls（人員コントロール)

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

The personnel to be assigned to trusted positions are screened and managed following Section 5.2.

信任された役職につく要員は、5.2 項にもとづいて採用され管理される。

5.3.2. Training Requirements (研修要件)

JCAN Public CA offers training to their personnel assigned to CA operations.

JCAN 認証局は、認証業務を実行するための研修を、その要員に実施する。

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

Personnel are retrained for the purpose of renewing and keeping the knowledge of operational procedures on an annual basis.

手続きについての知識の更新と維持を目的に、年次にて再研修をその要員に実施する。

5.3.4. 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 behaviors, use unauthorized authority, or use unauthorized systems.

JCAN 認証局 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。

5.3.5. 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 認証局 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。

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

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 認証局 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 認証局 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。

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

JCAN Public CA implements the following logs:

JCAN 認証局 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 certificates;
- Revocation of certificates;
- Publishing of 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)

- Records of physical entry/exit to the rooms where CA systems are located;
- Records of operation and lifecycle 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

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

- Identification of the operation;
- Date and time of the operation;
- Identification of the certificates involved in the operation;
- Identification of the persons 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

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

Designated personnel are periodically assigned to inspect the log file for detecting and reporting anomalies.

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。

5.4.4. 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 audit trails are recorded. These are appropriately protected with access controls. These log files can only be accessed by a person assigned to JCAN Public CA or by the appointed auditor.

The event logs cannot be easily deleted or destroyed during the retention period. Backup containing sensitive data is securely disposed of when no longer required.

JCAN 認証局 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や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。

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)

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

LRAs retain the information required for Subject's registration (c.f. consent forms and agreements, vetting records, verification records, etc.) through reliable methods.

JCAN 認証局 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。

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)を信頼性のある方法で保持する。 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)

JCAN Public CA retains records of JCAN Certificates, JCAN Public CA Certificate, and LRA Operator Certificates (where these certificates are issued from JCAN Public CA) for at least 10 years after the Certificate is expired or revoked.
Archive containing sensitive data is securely destroyed when no longer required.

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.

JCAN 認証局 は、JCAN 証明書、JCAN 認証局 証明書及び アクセス認証用証明書（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 10 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破棄される。

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。 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)

The Key Pair generation of JCAN Public CA is managed by more than 2 authorized staff with HSMs and m of n controls according to the procedure described in section 6.
The procedure of re-generating JCAN Public CA keys is as same as the procedures in the previous sections.

JCAN 認証局 の鍵ペアの生成は、2 名以上の任命されたスタッフにより、 6 項 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 認証局 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。

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

JCAN Public CA maintains the records of reporting, backup/restoration, and handling procedures of incidents and compromises in internal documents. JCAN Public CA documents the recovery procedures for the circumstances where computing resources, software, and/or data are corrupted or suspected of being corrupted.
When an algorithm is compromised, JCAN Public CA implements the following:

- Inform all subscribers and relying parties with whom the CA has any agreements, as well as the other stakeholders; and
- Revoke the affected certificates.

JCAN 認証局 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 認証局 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 認証局 は以下を実施する：

- 全ての利用者、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

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

When CA or RA is terminated in a planned way, Subscribers and Relying Parties are notified with a sufficient amount of time from the timing of termination. When CA or RA is terminated unexpectedly, GlobalSign pays effort to minimize the disruption and ensures that Subscribers and Relying Parties are promptly notified. GlobalSign revokes all issued certificates in principle and destruct CA private keys.

CA 又は RA を計画的に終了する場合は、 終了時期から相応の時間的余裕をもって利用者及び検証者に終了方針を通知する。予期せぬ終了にあっては、混乱が最小限となるよう努め、利用者及び検証者が速やかに通知を受けることを保証する。原則として発行済みの証明書を全て失効し、CA 秘密鍵を破棄する。

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

6.1. Key Pair Generation and Installation (鍵ペア生成及びインストール)

6.1.1. Key Pair Generation

(1) CA Key Pairs (CA 鍵のペア)

A Hardware Security Module ("HSM"), which is one of Cryptographic Modules, is used to securely generate and manage CA private keys.

It is confirmed that HSM has not been tampered with during shipment and delivery.

Certificate and revocation status information signed by HSM is not tampered with during retention.

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。

(2) Subscriber Key Pairs (利用者の鍵ペア)

When JCAN Public CA generates the private key on behalf of subscribers or LRAs, the key pair and CSR is generated following secure key generating procedures and the key generation policy described above.

Subscribers do not generate private keys to request JCAN certificates.

JCAN 認証局 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ーに準拠して PKI の鍵ペア及び CSR を生成する。
JCAN 証明書を申請するために、利用者による秘密鍵の生成は行わない。

6.1.2. Private Key Delivery to Subscriber （利用者への秘密鍵の配布）

JCAN Public CA obliges subscribers to use strong PIN codes. These PIN codes protect the generated private keys formatted in PKSC#12.

JCAN 認証局 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。

6.1.3. Public Key Delivery to Certificate Issuer （証明書発行者への公開鍵の配布）

GlobalSign only accepts Public Keys from RAs that have been protected during transit and have had the authenticity and integrity of their origin from the RA suitably verified. RA's shall only accept Public Keys from Subscribers in accordance with Section 3.2 of this CPS.

GlobalSign は、RA から伝送される経路が保護されており、その根源についての真正性と完全性が適切に検証された公開鍵のみを受け入れる。RA は本 CPS の 3.2 項に準拠している場合のみ、利用者からの公開鍵を受け付けるものとする。

6.1.4. CA Public Key Delivery to Relying Parties (認証局から検証者への公開鍵配布)

GlobalSign ensures that its Public Keys are delivered to Relying Parties in such a way as to prevent substitution attacks. Commercial web browsers and platform operators are encouraged to embed Root Certificate Public Keys into their root stores and operating systems. Issuing CA Public Keys are delivered by the Subscriber in the form of a chain of Certificates or via a Repository operated by GlobalSign and referenced within the profile of the issued Certificate through AIA (Authority Information Access) .

GlobalSign は検証者への公開鍵の配布において、鍵のすり替えを防ぐため、相応の方法で請け負うことを保証するも のとする。商業ブラウザ及びプラットフォームオペレーターは、ルートストア及び OS にルート証明書公開鍵を組み込 むことが推奨されている。発行 CA の公開鍵は、証明書の階層又は GlobalSign が運営するレポジトリを介して利用者から配布され、AIA（認証機関アクセス情報）を通じて発行済み証明書のプロファイル内で参照される。

6.1.5. Key Sizes (鍵長)

JCAN Public CA private RSA key length is 2048 bit or longer with the signing algorithm of SHA-2 (256) or above.

JCAN 認証局秘密鍵は、鍵長が 2048bit 以上の RSA 鍵で、SHA-2（256）以上の署名アルゴ

リズムを使用する。

6.1.6. Public Key Parameters Generation and Quality Checking (公開鍵パラメーター生成及び品質検査)

GlobalSign generates Key Pairs in accordance with FIPS 186 and uses reasonable techniques to validate the suitability of Public Keys presented by Subscribers. Known weak keys are tested for and rejected at the point of submission. GlobalSign references the Baseline Requirements Section 6.1.6 on quality checking.

GlobalSign は FIPS 186 の規定に従い鍵を生成し、また利用者から提示される鍵の適合性を適切な技術を用いて検証するものとする。既知の脆弱な鍵は検証され、また提出時に拒否される。GlobalSign は、品質検査に関し Baseline Requirements の 6.1.6 項を参照するものとする。

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field) 鍵の使用目的(X.509 v3 鍵使用フィールドにおいて)

GlobalSign sets key usage of Certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3 (see Section 7.1). The Private Key of JCAN Public CA is used to sign JCAN Certificates and CRLs.

GlobalSign は、申請で提案されるフィールドにしたがい、証明書における鍵の用途を、X.509 v3 鍵使用フ ィールドにより設定するものとする。(7.1 項を参照)JCAN 認証局 の秘密鍵は、JCAN 証明書と証明書失効リストの署名に使用される。

6.2. Private Key Protection and Cryptographic Module Engineering Controls (秘密鍵保護及び暗号モジュール技術管理)

6.2.1. Cryptographic Module Standards and Controls (暗号化モジュールの基準及び管理)

GlobalSign generates the private key of JCAN Public CA with the devices of FIPS 140-2 level 3 or above.

GlobalSign は JCAN 認証局の秘密鍵を FIPS 140-2 level3 以上のデバイスにて生成する。

6.2.2. Private Key (n out of m) Multi-Person Control 秘密鍵(m 中の n) 複数の人員による管理

JCAN Public CA manages the CA private keys following its documented procedures.

The generation of the CA private key requires multi-personnel control by more than two authorized staff serving in trustworthy positions.

JCAN 認証局 は、文書化された手続に従って CA 秘密鍵を管理する。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。

6.2.3. Private Key Escrow (秘密鍵のエスクロー)

GlobalSign does not escrow Private Keys for any reason.

GlobalSign は、如何なる者に対しても秘密鍵を第三者預託するものではない。

6.2.4. Private Key Backup (秘密鍵のバックアップ)

If required for business continuity GlobalSign backs up Root and Subordinate Private Keys under the same multi-person control as the original Private Key.

GlobalSign は災害時事業継続のために必要な場合、ルート及び下位層の秘密鍵を原本の秘密鍵と同様に複数人 員の管理下でバックアップを行なうものとする。

6.2.5. Private Key Archival (秘密鍵のアーカイブ)

GlobalSign does not archive Subscriber Private Keys and ensures that any temporary location where a Private Key may have existed in any memory location during the generation process is purged. Once the subscriber or LRA receives the PKSC#12 file, GlobalSign destroys all the relevant instances none of the generated private keys and PIN codes are archived.

GlobalSign は利用者の秘密鍵のアーカイブを行なわず、秘密鍵の生成過程で鍵が存在していた可能性のある一時 的な記憶場所からも削除されることを保証する。
GlobalSign は、JCAN 証明書の PKCS#12 ファイルの PIN 及び生成した秘密鍵をアーカイブせず、全てのインスタンスを PKCS#12 形式証明書の生成後に破棄する。

6.2.6. Private Key Transfer into or from a Cryptographic Module (暗号モジュール間の秘密鍵移行)

GlobalSign Private Keys are generated, activated, and stored in Hardware Security Modules. When Private Keys are outside of a Hardware Security Module (either for storage or transfer), they are encrypted. Private Keys never exist in plain text outside of a cryptographic module.

GlobalSign の秘密鍵は、ハードウェアセキュリティモジュールにおいて生成、アクティブ化、及び保存されている。秘密鍵がハードウェアセキュリティモジュールの外(保存若しくは移行のため)にある場合は、暗号化されていることが必須となる。秘密鍵は、暗号モジュール外の環境にて、一般テキスト状態で存在しては絶対にならない。

6.2.7. Private Key Storage on Cryptographic Module (暗号モジュールにおける秘密鍵の保存)

GlobalSign stores the private key of JCAN Public CA in the devices of FIPS 140-2 level 3 or above.

GlobalSign は JCAN 認証局の秘密鍵を FIPS 140-2 level3 以上のデバイスに保管する。

6.2.8. Method of Activating Private Key (秘密鍵のアクティブ化方法)

GlobalSign is responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module. Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the form of a Subscriber Agreement.

GlobalSign はハードウェアセキュリティモジュールの製造元が提供する仕様説明書に従い、秘密鍵をアクティブ化する責任を有する。利用者は、利用約款に示される条件に従い、秘密鍵を保護する責任を有する。

6.2.9. Method of Deactivating Private Key (秘密鍵の非アクティブ化方法)

GlobalSign ensures that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorized access. During the time a GlobalSign CA's Hardware Security Module is on-line and operational, it is only used to sign Certificates and CRL/OCSPs from an authenticated RA. When a CA is no longer operational, Private Keys are removed from the Hardware Security Module.

GlobalSign はアクティブ化されたハードウェアセキュリティモジュールを放置せず、また不正アクセスが可 能な状況にしないことを保証するものとする。GlobalSign のハードウェアセキュリティモジュールがオンラ インかつ操作可能な間、証明書及び認証済み RA からの CRL/OCSP の署名にのみ使用される。認証局が運営停止となる際、その秘密鍵はハードウェアセキュリティモジュールから削除される。

6.2.10. Method of Destroying Private Key (秘密鍵の破棄方法)

CA Key Pair re-generation and re-installation is, following the Sections of 6.2, implemented at any suitable time before the expiration of the previous pair.

GlobalSign Private Keys are destroyed under multi-personnel control at least by two trusted personnel when they are no longer needed or when the Certificates to which they correspond have expired or have been revoked. Destroying Private Keys means that GlobalSign destroys all associated CA secret activation data, including backups, in the HSM in such a manner that

no information can be used to deduce any part of the Private Key. The Key destruction process is documented and relevant records are archived.

CA 鍵ペアの再生成と再インストールは、6.2 項の規定に従い、有効期限前の適切な時期に行う。GlobalSign の秘密鍵は、不必要となった時点若しくは対応する証明書が期限切れ又は失効した際に、信任された 2 名以上の要員の立会いの下に破棄される。秘密鍵を破棄するにあたり GlobalSign は秘密鍵の如何なる部分も推定されないよう、バックアップを含め、HSM 内の関連する認証局の秘 密アクティベーションデータ全てを破棄する。鍵の破棄の処理は文書化し、関連する記録は保存する。

6.2.11. Cryptographic Module Rating (暗号モジュール評価)

See Section 6.2.1

6.2.1 項を参照。

6.3. Other Aspects of Key Pair Management (鍵ペア管理におけるその他の側面)

6.3.1. Public Key Archival (公開鍵のアーカイブ)

Issuing CAs must archive Public Keys from Certificates.

GlobalSign は証明書の公開鍵をアーカイブしなければならない。

6.3.2. Certificate Operational Periods and Key Pair Usage Periods (証明書の操作可能期間及び鍵ペアの使用期間)

Certificates shall have a maximum validity period as in the chart below.
The Key Pair usage period can be up to the Certificate Validity Period. Certificates signed by a specific CA must expire before or at the end of that CA Certificate Validity period.
Issuing CAs must comply with the external requirements with respect to the maximum validity period, in some cases thereby reducing the effective available Certificate term. In some cases, the maximum validity period may not be realized by the Subscriber in the event the current or future external requirements impose requirements on Certification Authorities relative to Certificate issuance that were not in place at the time the Certificate was originally issued, particularly in the case of a request for reissuance, e.g., additional requirements are included for identification and authentication for certain Certificate type, or maximum Validity Period is decreased.

パブリックに信頼される GlobalSign の証明書は最長で下記の表に述べる有効期間を持つものとする。
鍵ペアの使用期間は、最大で証明書と同じ有効期間に設定することができる。 特定の CA によって署名された証明書は、その CA 証明書の有効期限またそれ以前に失効しなければならない。
GlobalSign 証明書は、最長有効期間に関し外部要求に準拠しなければならないため、それに 従って証明書の有効期間を短縮する場合がある。利用者の証明書がそれよりも短い有効期間の場合

は、期限 が切れた後に元の有効期間まで再発行が可能となる。 現行又は将来の外部要求が、証明書が最初に発行された時点では実施されていなかった証明書発行に対して認証権限に要件を課す場合、特に再発行の申請がなされた場合においては、利用者が最大の 有効期間を享受できないことがある。 例：ある証明書の種類について識別及び認証に対する追加要件が含まれる場合、又は最大の有効期間が短縮 される場合

Type / 種類	Private key usage / 秘密鍵の利用方法	Max validity period / 最長有効期間
JCAN Public CA Certificate	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	18 years
JCAN Certificates	Digital Signature, Key Encipherment, Data Encipherment (b0)	825 days

6.4. Activation Data (アクティブ化データ)

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

JCAN 認証局 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。

6.5. Computer Security Controls (コンピュータ セキュリティコントロール)

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

JCAN 認証局 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。

6.6. Lifecycle Security Controls (ライフサイクル セキュリティコントロール)

When develop, install, or change software, this software is analyzed from the designing phase and subject to tests on the test environment. The release of this software is implemented after the approval by the responsible personnel.

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。

6.7. Network Security Controls (ネットワークセキュリティコントロール)

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

JCAN 認証局 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。

6.8. Timestamping (タイムスタンプ)

(No stipulation)

(規定なし)

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)

7.1.1. Version numbers (バージョン番号)

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

GlobalSign は、X.509 バージョン 3 に従ってデジタル証明書を発行するものとする。

7.1.2. Certificate Extensions (証明書拡張)

GlobalSign issues Certificates in compliance with RFC 5280 and applicable best practice including compliance to the current Baseline Requirements section 7.1.2.1 through 7.1.2.5. Criticality also follows best practice to prevent unnecessary risks to Relying Parties when applied to name constraints.

Subordinate CA and end entity certificates include an Extended Key Usage extension containing KeyPurposeId(s) describing the intended usage(s) of the certificate. The KeyPurposeId anyExtendedKeyUsage is not included in publicly trusted end entity certificates.

GlobalSign は、RFC5280 及び現在の Baseline Requirements の 7.2.1.1 から 7.2.1.5 項を含む適用可能なベストプラクティスに従い、証明書を発行するものとする。名前の制限(NameConstraints)が設定された場合、検証者 を不要なリスクから守るために、重要度(クリティカリティ)についてはベストプラクティスに従って設定される。サブ認証機関及びエンドエンティティ証明書は、証明書の使用目的を説明する KeyPurposeId(s) を含む Extended Key Usage エクステンションを含む。KeyPurposeId 及び ExtendedKeyUsage は、パブリックに信頼される証明書 には含まれない。

7.1.3. Algorithm Object Identifiers (アルゴリズム識別子)

GlobalSign issues Certificates with algorithms indicated by the following OIDs:

SHA256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}

SHA384WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}

SHA512WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 13}

GlobalSign は、下記の OID に示されるアルゴリズムで証明書を発行するものとする。

SHA256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}

SHA384WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
SHA512WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 13}

7.1.4. Name Forms (名前形式)

GlobalSign issues Certificates with name forms compliant to RFC 5280 and section 7.1.4 of the Baseline Requirements..

GlobalSign は、RFC5280 に従う名前形式及び Baseline Requirements の 7.1.4 項に準拠して証明書を発行する。

7.1.5. Name Constraints (名前制約)

GlobalSign may issue Subordinate CA Certificates with name constraints where necessary and mark as critical where necessary as part of the Trusted Root program. When name constraints are NOT set on a Subordinate CA, such CA must be subject for full audit specified in section 8.0 of this CPS.

GlobalSign name constrains using the following methods:
If the certificate includes the id-kp-serverAuth extended key usage, then the certificate MUST be name constrained with constraints on dNSName, iPAddress and DirectoryName as described in section 7.1.5 of version 1.3 or later of the Baseline Requirements.
If the certificate includes the id-kp-emailProtection extended key usage, it MUST include the name constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2.4 of the Baseline Requirements.
GlobalSign MAY also include name constraints on certificates with the id-kpemailProtection extended key usage with constraints on dNSName, iPAddress and DirectoryName as described in section 7.1.5 of the Baseline Requirements

GlobalSign は必要に応じて名前の制限(NameConstraints)を適用して下位 CA 証明書を発行し、また TrustedRoot プログラムの一部として必要な場合にはそれを重要度として設定する。下位認証局に名前の制限(NameConstraints)が設定されていない場合、その CA は本 CPS の 8.0 項に記載されている全面監査の対象に含まれなければならない。

GlobalSign の名前の制限(NameConstraints)は、次の方法を使用する。
証明書が id-kp-serverAuth extended key usage を含む場合は、Baseline Requirements バージョン 1.3 以降の 7.1.5 項に記載の通り dNSName、iPAddress、及び DirectoryName に制限をかけなければならない。
証明書が id-kp-emailProtection extended key usage を含む場合、Baseline Requirements の 3.2.2.4 項に従い所有権を認証された各名前のうち、最低 1 つは permittedSubtrees に属すと

いう rfc822Name に制限が かかった X.509v3 拡張子の名前の制限(NameConstraints)を含まなければならない。
GlobalSign は Baseline Requirements の 7.1.5 項に従い、id-kp-emailProtection extended key usage の証明書にも dNSName、iPAddress、及び DirectoryName に名前の制限(NameConstraints)をかけることも可能 である。

7.1.6. Certificate Policy Object Identifier (証明書ポリシー識別子)

GlobalSign follows Section 7.1.6 of the Baseline Requirements.

GlobalSign は Baseline Requirements の 7.1.6 項に従う。

7.1.7. Usage of Policy Constraints Extension (ポリシー制約拡張の使用)

No stipulation

（規定なし）

7.1.8. Policy Qualifiers Syntax and Semantics (ポリシー修飾子の構文と意味)

GlobalSign issues Certificates with a policy qualifier and may include suitable text to aid Relying Parties in determining applicability.

GlobalSign は、検証者がそれを受け入れ可能かどうかを判断できるように、ポリシー修飾子と適切なテキストを含めることができる形でデジタル証明書を発行する。

7.1.9. Processing Semantics for the Critical Certificate Policies Extension (クリティカルな証明書ポリシー拡張についての解釈方法)

(No stipulation)

(規定なし)

7.1.10. Serial Numbers (シリアル番号)

Each Issuing CA must issue certificates that include a unique (within the context of the Issuer Subject DN and CA certificate serial number) non-sequential Certificate serial number greater than zero (0) containing at least 64 bits of output from a CSPRNG.

各発行 CA は、CSPRNG からの最低 64 ビットのアウトプットを含む、0 以上の連番でない独自の（発行者サブジェクト識別名及び CA 証明書シリアル番号内のコンテクスト）証明書シリアル番号を含む証明書を発行しなければならない。

7.2. CRL Profile (証明書失効リスト プロファイル)

7.2.1. Version Number(s) (バージョン番号)

GlobalSign issues Version 2 CRLs in compliance with RFC 5280. CRLs have the following fields:

- Issuer The Subject DN of the issuing CA
- Effective date Date and Time
- Next update Date and Time
- Signature Algorithm sha256RSA etc. (Depending upon product)
- Signature Hash Algorithm sha256 etc. (Depending upon product)
- Serial Number(s) List of revoked serial numbers
- Revocation Date Date of Revocation

GlobalSign は RFC5280 に従い、バージョン 2 の CRL を発行するものとする。失効リストは以下のフィールドを含む。

・ 発行者	GlobalSign XXX 等(製品による)
・ 有効開始日	日付及び時間
・NextUpdate	日付及び時間
・ 署名アルゴリズム	sha256RSA 等(製品による)
・ 署名ハッシュアルゴリズム	sha256 等(製品による)
・ シリアル番号	失効された証明書のシリアル番号
・ 失効日	失効日

7.2.2. CRL and CRL Entry Extensions (CRL 及び CRL エントリ拡張子)

CRLs have the following extensions:

- CRL Number Monotonically increasing serial number for each CRL
- Authority Key Identifier AKI of the issuing CA for chaining/validation requirements

Following extensions are supported:

- ReasonCode Identifies the reason for the Certificate revocation.

The extension is present for a CRL entry for a Root CA or Subordinate CA Certificate, including Cross Certificates. Supported values are keyCompromise (1), affiliationChanged (3), superseded (4), cessationOfOperation (5). The extension may be present for a CRL entry for a Subscriber end entity Certificate. Supported values are keyCompromise (1), affiliationChanged (3), superseded (4), certificateHold (6). The value certificateHold (6) is not supported for SSL Certificates. The value keyCompromise (1) is not supported for SSL Certificates revoked via ACME protocols

CRL は、以下の拡張子(エクステンション)を含む

- CRL 番号 連続する番号
- 認証局鍵識別子 チェーン/十分性検証の要件のための発行 CA の発行者鍵識別子 (Authority Key Identifier)

以下の拡張子を含む。

- ReasonCode　　証明書の失効理由についての識別子

当拡張子は、相互認証証明書を含む、ルート CA の証明書又はサブ CA の証明書の CRL エントリに含まれている。当拡張子に含まれる値は、keyCompromise (1), affiliationChanged (3), superseded (4), cessationOfOperation(5)である。
当拡張子は、利用者のエンドエンティティ証明書の CRL エントリに含めることができる。当拡張子に含まれる値は、keyCompromise (1), affiliationChanged (3), superseded (4), certificateHold (6)である。certificateHold (6)については、SSL 証明書には含まれない。

7.3. OCSP Profile （OCSP プロファイル)

GlobalSign operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 6960 and RFC 5019 and highlights this within the AIA extension via an OCSP responder URL.

GlobalSign は、RFC6960 又は 5019 に従いオンライン証明書ステータスプロトコル(OCSP)レスポンダを提供し、OCSP レスポンダ URL を通じて AIA 拡張子内でこれをハイライトする。

7.3.1. Version Number(s) (バージョン番号)

GlobalSign issues Version 1 OCSP responses with following fields:

- Responder ID SHA-1 Hash of responder's Public Key
- Produced Time The time at which this response was signed
- Certificate Status Certificate status referenced (good/revoked/unknown)
- ThisUpdate/NextUpdate Recommended validity interval for the response
- Signature Algorithm SHA256 RSA etc. (depending upon product)
- Signature Signature value generated by the responder
- Certificates The OCSP Responder's Certificate

An OCSP request must contain the following data:

- Protocol version
- Service request

Target Certificate identifier Following fields are supported:

- revocationReason Identifies the reason for the Certificate revocation.

This field is present for OCSP responses for a Root CA or Subordinate CA Certificate, including Cross Certificates, and may be present for a Subscriber end entity Certificate, if the Certificate is revoked. The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

GlobalSign は以下のフィールドを含むバージョン 1 の OCSP レスポンスを発行する。
・ レスポンダ ID レスポンダの公開鍵の SHA-1 ハッシュ
・ 生成時間 OCSP レスポンスが署名された時間
・ 証明書ステータス 問い合わせを受けた証明書のステータス(有効/失効済み/不明)
・ThisUpdate/NextUpdate レスポンスの推奨有効期間
・ 署名アルゴリズム SHA256 RSA 等(商材により異なる)
・ 署名 レスポンダにより生成された署名
・ 証明書 OCSP レスポンダの証明書

OCSP リクエストは下記のデータを含む必要がある：
・ プロトコルのバージョン
・ サービスリクエスト
・ ターゲット証明書の識別子

以下のフィールドを含む:
・revocationReason 証明書の失効理由についての識別子

当フィールドは、相互認証証明書を含む、ルート CA の証明書又はサブ CA の証明書の OCSP レスポンダに含まれ、証明書が失効した際に利用者のエンドエンティティ証明書に含めることができる。CRLReason は CRL に利用が許可されている値を含むことを示し、詳細は 7.2.2 章に記載されている。

7.3.2. OCSP Extensions (OCSP 拡張)

(No stipulation)

(規定なし)

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 (監査の頻度及び条件)

JCAN Public CA annually receives compliance audit to ensure the conformity of this service to the requirements, standards, procedures, and service levels of this CPS.

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 CPS. For this re-registration, LRAs implement internal audit on themselves.

JCAN 認証局 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。

LRA 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、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。

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

Compliance audit is carried out by auditors with a firm auditing experience:

- Independence from the subject of the audit.
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function.
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme.
- Bound by law, government regulation, or professional code of ethics

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

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。:

- 監査対象からの独立性
- 公開鍵基盤技術、情報セキュリティ・ツール及び技術、IT 及びセキュリティ監査、更に第三者を認証する機 能について審査するにあたり、熟練した人員を雇用している
- 資格、認定、認可を有するもの、又は監査スキームに基づいた監査人の能力条件を満たすと評価される者 ・ 法律、公的規定又は職種倫理規定により認定されている者

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 auditors are independent from the other departments. These auditors' involvement with the other departments is limited to audit.

The internal auditors of LRAs are independent from the business operations in the departments subject to this internal audit.

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。

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. Audit processing matters (監査対象項目)

The focal point of JTS Registrationis based on the conformance to JCAN CP and CPS.

JTS の審査は、JCAN CP 及び CPS への準拠性を中心に行われる。

9. Other Business and Legal Matters (他のビジネス及び法的事項)

9.1. Fees (費用)

The issuance of JCAN certificates requires reasonable fees.

JCAN 証明書の発行には、適正な料金が課金される。

9.2. Financial Responsibility (財務上の責任)

JCAN Public CA keeps sufficient financial funding to offer these services.

JCAN 認証局 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。

9.3. 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 認証局 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。

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

The retention of personal information by LRA and/or JCAN Public CA 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 and/or JCAN Public CA maintains is regarded as confidential except for explicitly published items such as certificates and CRL.

LRA 及び/又は JCAN 認証局 による個人情報の保持は、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 及び/又は JCAN 認証局 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)

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

本 CPS 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)

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

JCAN 認証局 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。

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

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

JCAN 認証局 は、本 CPS に規定された保証を除き、一切の保証を行わない。

9.8. Limitations of Liability (有限責任)

JCAN Public CA is not responsible for damages regarding authentication 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 originated from the systems of subscribers or relying parties
- Damages caused by the negligence or failures of Hardware or Software used by JCAN Public CA and other parties
- Damages resulted into secondary or indirect loss of profit from use of certificates or digital signatures.
- Damages originated from information published on the certificate and CRLs but cannot be attributed to the responsibility of JCAN Public CA.
- Damages resulted from improvement in cryptographic algorithm decoding technology beyond current expectations.
- Any responsibilities originated from the termination of JCAN Public CA
- Any damages originated from the suspension of JCAN Public CA which resulted from natural disasters, wars, upheavals, terrorism, and other inevitable accidents.
- Any responsibilities originated from the suspension of JCAN Public CA

JCAN 認証局 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 認証局 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 認証局 及びその他当事者の使用するハードウェア、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、逸失利益の一切の損害
- JCAN 認証局 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 認証局 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

9.9. Indemnities (補償)

JCAN Public CA shall indemnify to Subscribers, Relying Parties, or other third parties for the damages which are not specified in Section 9.8.

In any 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 originated from the failure in fulfilling 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 stakeholders against any loss, damage, or expense, including reasonable attorney's fees related to claim, dissent, lawsuit resulting, etc.

LRA shall indemnify the damages of JCAN Public CA in connection with the requirements specified in Application Form and Terms of Use for LRAs. To the extent permitted by law, LRA shall indemnify JCAN Public CA and its stakeholders against any loss, damage, or expense, including reasonable attorney's fees, related to claim, dissent, lawsuit resulting, etc.

JCAN 認証局 は、9.8 項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。

如何なる場合においても、JCAN 認証局 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 に記載の義務又は責任の不履行に起因する JCAN 認証局 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、損害或いは出費、またこれらに関する弁護士費用を JCAN 認証局 及びその業務上の協力関係者に補償するものとする。

LRA は、 JCAN 証明書及び JIPDEC トラステッド・サービス登録お申込書に定めた要件に関連して JCAN 認証局 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、損害或いは出費、またこれらに関する弁護士費用を JCAN 認証局及びその業務上の協力関係者 に補償するものとする。

9.10. Term and Termination (期間及び終了)

This CPS remains in force until notice is published on the repository.

本 CPS 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 (関係者への個別通達及び伝達)

GlobalSign accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from GlobalSign the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed to the sender. Individuals communications made to GlobalSign must be addressed to: legal.jp@globalsign.com or by post to GlobalSign in the address provided in Section 1.5.2.

GlobalSign は、本 CPS に関してデジタル署名されたメッセージ又は紙媒体を用いた通知を受け入れる。GlobalSign からの有効かつデジタル署名された受領通知があった時点で、通知の送信者はその伝達が有効であったとみなされるものとする。送信者はこの受領通知を 20 営業日以内に必ず受領できるものとする。また書面による場合は、配達証明付きの配送サービスにより発送されるか、もしくは書留郵便、郵便料金前払い、書留郵便受領通知を必須として、 差出人宛てに書面通知するものとする。GlobalSign への個別の連絡は、 legal.jp@globalsign.com 宛、又は本 CPS の 1.5.2 項に指定される GlobalSign のあて先に送付されるものとする。

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 CPS.

GlobalSign notifies JIPDEC of any major or significant changes to this CPS.

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 CPS を維持管理する責任を負う。

GlobalSign は、本 CPS に関する主要な又は重要な変更が為された際には、JIPDEC へ通知する。

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

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution, the party agrees to notify JCAN Public CA.

訴訟、仲裁を含む法的、又はその他の解決手段を訴えようとする場合、当事者は JCAN 認証局に対し、事前にその旨を通知するものとする。

9.14. Governing Law (準拠法)

This CPS is governed, construed, and interpreted in accordance with the laws and regulations 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 認証局 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。

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

JCAN Public CA complies with applicable laws and regulations of Japan.

JCAN 認証局 は、適用可能な日本国の法律を遵守する。

9.16. Miscellaneous Provisions (一般事項)

(1) Survival (存続)

The legal obligations and restrictions survive even after the termination of JCAN Public CA.

法的問題の責任及び制限事項は、JCAN 認証局 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項を含むいずれかの条項が無効であるか、或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。

9.17. Other Provisions (その他の規定)

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、及び譲受人に対しても拘束力がある。