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

Legal-JP

電子署名者 : Legal-JP
日付 : 2021.09.27
12:00:08 +09'00'

Document Change Control

改訂履歴

Version	Release Date	Status + Description	Author	Approver
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.
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。

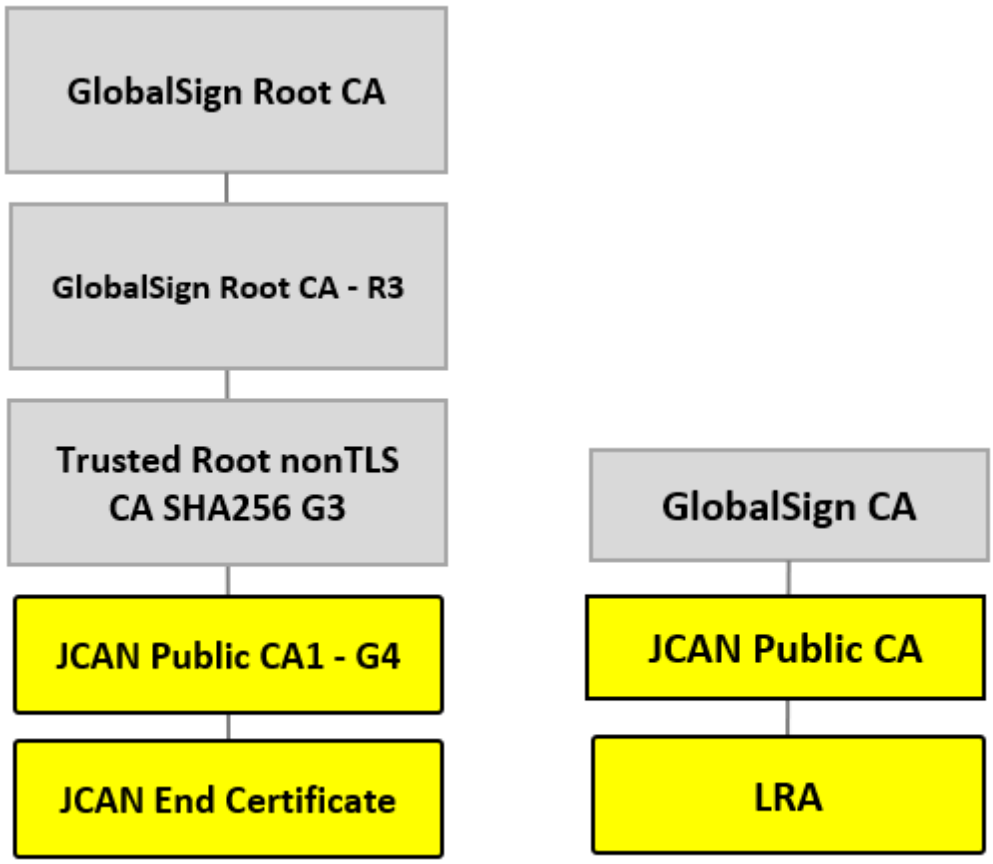
商業登記番号：0110-01-040181
法人番号：1011001040181

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)

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

本項は、JCAN 認証局 が発行する証明書の[CP]に規定する。

1.3 PKI participants (PKI の関係者)

(1) Subscribers and users (利用者)

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

本項は、JCAN 認証局が発行する証明書の[CP]に規定する。

(2) LRA（LRA）

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

本項は、JCAN 認証局が発行する証明書の[CP]に規定する。

(3) Relying Party（検証者）

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

本項は、JCAN 認証局が発行する証明書の[CP]に規定する。

(4) JCAN Public CA（JCAN 認証局）

JCAN Public CA is the CA which issues JCAN Certificates following the JCAN Certificate Policy 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 証明書ポリシーに従い JCAN 証明書を、その利用目的、適用範囲、手続き等に準拠して発行する 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。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あとは、利用証明書の秘密鍵を PKCS#12 と PIN で保護し、対応する PIN は一切保存せず破棄する。
- JCAN 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。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) JCAN（ジェイキャン）

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

本項は、JCAN 認証局が発行する証明書の[CP]に規定する。

1.4 Certificate Usage (証明書の使用方法)

(1) JCAN Certificates (JCAN 証明書)

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

本項は、JCAN 認証局が発行する証明書の[CP]に規定する。

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

report-abuse@globalsign.com

GlobalSign は、この要求に応じて当該証明書を失効することが可能である。また、調査の結果、失効しない場合もある。

1.6 Definitions and acronyms (定義と略語)

1.6.1 Definitions (定義)

Please refer to Article 10.

10 項 参照

1.6.2 References (参考)

[CP] JCAN Certificate Policy

JCAN 認証局の CP

1.7 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。及び 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。

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

GlobalSign reserves the right to publish the following information on the respective online publicly accessible repositories to the certificate subscribers and relying parties: Archived records shall be made available if required for the purposes of providing evidences for legal proceedings 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。
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)

- The latest versions of this CPS
- Other information regarding JCAN

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

- 最新の本 CPS
- JCAN に関するその他の情報

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

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

Updates of this CPS are published after approval by PACOM1.

CRL is updated periodically and whenever any change happens during the validity period.

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。

CRL は、有効期限内で定期的及び変更毎に更新される。

失効情報は、少なくとも証明書の有効期間満了まで CRL に記載されている。

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

GlobalSign keeps its repository available to the public.

GlobalSign は当該リポジトリを公開する。

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

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

本項は、JCAN 認証局 が発行する証明書の[CP]に規定する。

3. 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)

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

本項は、JCAN 認証局 が発行する証明書の[CP]に規定する。

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

4.1. Physical Security Controls (物理的管理)

JCAN Public CA implements high-security controls within the data center. These include

restricting personnel and physical access using electronic security mechanisms. Especially in certificate generation and revocation management, 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。

4.2. 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すかもしれない金銭的な或いは内部及び外部からの圧力の影響を受けないものとする。

JCAN 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。

4.3. Personnel Controls (人事コントロール)

4.3.1. 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 Article 4.2.

信任された役職につく要員は、4.2 項にもとづいて採用され管理される。

4.3.2. Training Requirements (研修要件)

JCAN Public CA 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。

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

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

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

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

JCAN Public CA will take disciplinary actions toward personnel who perform unauthorized 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。

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

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

JCAN 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。

4.4. 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。

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

JCAN Public CA implements the following logs:

JCAN 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

4.4.2. 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

4.4.3. 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。

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

The log files and 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。

4.5. Records Archival (アーカイブ対象記録)

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

JCAN Public CA maintains the details of all CA Certificates, 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.

The information maintained by LRAs are prescribed in [CP]

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 が保持する情報は、 [CP]で規定する

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

JCAN Public CA retains records of JCAN Certificates, JCAN Public CA Certificate, and LRA Operator Certificates (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.

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。

4.6. 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 article 6.

The procedure of re-generating JCAN Public CA keys is as same as the procedures in the previous articles.

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 2 名以上により、 5.1.2 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。

4.7. 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

4.8. 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。

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

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

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

A Hardware Security Module ("HSM"), which is one of Cryptographic Module, is used 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。

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

JCAN Public CA generates the CA private keys 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.

Private keys are managed with HSMs.

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

秘密鍵は、HSM で管理される。

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

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

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

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

JCAN Public CA private 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。

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

The procedure of CA Key Pair re-generation and re-installation is the same as in Article 6.1.2.
CA Key Pair re-generation and re-installation is carried out at any suitable time before the expiration.
JCAN Public CA decommissions and destroys keys used in the past and zero-out HSMs in a secure manner at the end of the key lifecycle and HSM retirement.
All backup or escrowed copies of private keys are destroyed at the end of their key lifecycle.

CA 鍵ペアの再生成と再インストールの手順は、 5.1.2 項 と同じである。
CA 鍵ペアの再生成と再インストールは、有効期限前の適切な時期に行う。
JCAN 認証局 はライフサイクルの終了時及び HSM リタイヤ時に、セキュアな方法で過去に使用された全ての鍵を廃棄し、HSM をゼロ設定する。
ライフサイクルの終了時に、全てのバックアップ及びキーエスクローされた秘密鍵の複写は破棄される。

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

The private key of JCAN Public CA is stored in the devices of FIPS 140-2 level 3 or above.
When outside the HSM, the private key is always encrypted.

JCAN 認証局の秘密鍵は FIPS 140-2 level3 以上のデバイスに保管する。
HSM の外では、当該 CA 秘密鍵は常に暗号化される。

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

The public key of JCAN Public CA can be downloaded from the repository.

JCAN 認証局 の公開鍵は、リポジトリからダウンロードできる。

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

The private key of JCAN Public CA is destroyed at the end of the lifecycle under multi-personnel control at least by two trusted personnel. The Key destruction process is documented and relevant records are archived.

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

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

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

JCAN Public CA uses the HSMs which meet the standards equivalent to FIPS140-2 Level 3.

JCAN 認証局 は、FIPS140-2 レベル 3 相当の認定を取得した HSM を使用する。

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

For private key generation, the following method is used:

利用者秘密鍵の生成は、下記の何れかの方法で行う。

(1) Generation of Private Keys by JCAN Public CA (JCAN認証局 による秘密鍵の生成)

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. JCAN Public CA obliges subscribers the us strong PIN codes. The PIN codes protect the generated private keys formatted in PKSC#12. Once the subscriber or LRA receives the PKSC#12 file, all relevant instances are destroyed by the CA including the PIN code. None of the generated private keys and PIN codes are archived.

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 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。当該 PIN 及び生成した秘密鍵はアーカイブせず、全てのインスタンスは PKCS#12 形式証明書の生成後に破棄される。

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

Subscribers do not generate private keys to request JCAN certificates.

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。

5.3. 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。

5.4. 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。

5.5. 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。

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

6.1. Certificate Profile (証明書プロファイル)

Certificates profile issued from JCAN Public CA is based on the X.509 Version 3 Format and the following format.

JCAN 認証局 から発行される証明書プロファイルは、X.509 バージョン 3 フォーマットに基づく。

Field フィールド	Value or Value constraint (値、又は値制約)
Serial Number	Unique value allocated by CA
シリアルナンバー	CA が割り当てる一意な番号
Signature Algorithm	Object identifier of the algorithm used to sign the certificate. SHA256 RSA.
署名アルゴリズム	証明書に署名するために使用されたアルゴリズムのオブジェクト識別子。SHA256 RSA。
Issuer	The name of the CA which issued the digital certificate - written in X.500 identifier (DN) format
発行者	電子証明書を発行した CA の名前、X.500 識別名(DN)で記述

Valid From	Start date of the validity period of the certificate
有効期間開始日	証明書の有効期間開始日
Valid To	End date of the validity period of the certificate
有効期間終了日	証明書の有効期間終了日
Subject DN	The name of the owner of the digital certificate and other pertinent information
サブジェクト DN	電子証明書の所有者の名前
Subject Public Key	Information regarding the Subscriber's public key
サブジェクト公開鍵	証明書所有者の公開鍵に関する情報

6.1.1. Authority Key Identifier (AKI)

Authority Key Identifier ("AKI") shall be incorporated in the extension of JCAN Certificates and JCAN Public CA Certificates.

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

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

6.1.2. Authority Information Access (AIA)

Authority Information Access ("AIA") shall be incorporated in the extension of JCAN Certificates and Sub CA Certificates. AIA should be inserted with the URL from which Relying Parties can obtain the issuing CA certificate.

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

6.1.3. CRL Distribution Points (CRL Distribution Points)

JCAN Certificates and JCAN Public CA Certificates include cRLDistributionPoints, the URL from which Relying Parties can obtain a CRL to check the certificate's status, in the extension of these Certificates.

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

6.1.4. Subject Key Identifier (SKI)

Subject Key Identifier ("SKI") shall be inserted to the extension of JCAN Certificates and

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

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

6.1.5. Subject Alternative Name (Subject Alternative Name)

Subject Alternative Name can be inserted to the extension of JCAN Certificates.
The SubjectAlternativeName must be generated in accordance with one of the methods described in RFC 5280.

JCAN 証明書の拡張に、Subject Alternative Name を挿入してもよい。
SubjectAlternativeName は、RFC 5280 に記述された方法の 1 つに従って生成されなければならない。

6.2. CRL Profile (証明書失効リスト プロファイル)

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

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

Field (フィールド)	Value, or Value constraint (値、又は値制約)
Version	X509 V2 in accordance with RFC 5280
バージョン	RFC 5280 に従って、X.509 のバージョン 2
Certificate Issuer	The Entity who has signed and issued the CRL
証明書発行者	CRL に署名し発行したエンティティ
This update	Date of Issuance
今回更新	発行日
Next Update	Date of Issuance＋up to 7days
次回更新	発行日付＋7 日以内
Signature Algorithm	Object identifier of the algorithm to sign the CRL. SHA256 RSA is used.
署名アルゴリズム	CRL に署名するために使用されたアルゴリズムのオブジェクト識別子。SHA256 RSA。

Authority Key Identifier	160–bit SHA-1 hash of the issuer CA public key
AKI	証明書を発行する CA の公開鍵の 160bit の SHA-1 ハッシュ
CRL Number	A unique sequence number in accordance with RFC5280
CRL 番号	RFC 5280 に従って、ユニークなシーケンス番号
Revoked Certificates	Serial No. of revoked certificates and their revocation date and time
失効証明書情報	失効した証明書のシリアルナンバー、失効日時

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

7.1. Frequency and Requirement of Audit (監査の頻度或いは条件)

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.

Audit of LRAs is prescribed in [CP]

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 の監査は、[CP]による。

7.2. 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

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

7.3. 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.

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

7.4. Audit processing matters (監査対象項目)

The focal point of the audit of JCAN Public CA is based on this CPS. The audit of LRA is prescribed in [CP]

JCAN 認証局 の監査は、本 CPS の準拠性を中心に行われる。LRA の監査は、[CP]による。

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

8.1. 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。

8.2. 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。

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

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

JCAN 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。

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

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

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。
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。

8.5. 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。

8.6. 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。

8.7. 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。

8.8. 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、遺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

8.9. Indemnities (補償)

JCAN Public CA shall indemnify to Subscribers, Relying Parties, or other third parties for the damages which are not specified in Article 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 partners 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 partners against any loss, damage, or expense, including reasonable attorney's fees, related to claim, dissent, lawsuit resulting, etc.

JCAN 認証局 は、8.8 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 及びそのパートナー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 及びそのパートナーに補償するものとする。

8.10. 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。

8.11. 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: JP-Legal@globalsign.com or by post to GlobalSign in the address provided in Article 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。

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

GlobalSign の PACOM1 – CA Governance Policy Authority は、GlobalSign の経営チーム、及び GlobalSign の 取締役会で承認されたメンバーで構成されており、本 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、GlobalSign が改定版の CPS を承認するまでの、 一定の期間、その変更の件をウェブサイトに掲載するものとする。

8.13. 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。

8.14. 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。

8.15. 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。

8.16. 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。

8.17. 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。

9. Definitions and Acronyms (定義と略語)

CA (認証局)

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

証明書の発行・更新・失効、CA 鍵の生成を行う主体をいう。

Certificate Applicants (証明書申請者)

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

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

Certificate Profile (証明書プロファイル)

The certificate usages specified in x.509 certificate.

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。

CP (証明書ポリシー)

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

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

CPS (認証業務運用規程)

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

CA を運用するうえでの運用手続きやセキュリティ基準を明示した文書をいう。

CRL (証明書失効リスト)

CRL (Certificate Revocation List) is a list of certificates that are revoked before their expiration,

recorded by the applicable CA.

証明書の有効期間内にも拘わらず失効された証明書情報を記録したリストをいう。

CSR (証明書署名要求)

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

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

LRA から CA へ、電子証明書を要求する際に送られる機械可読の申込書式をいう。
尚、CA での鍵ペア生成を要求された場合は、登録局で鍵ペアと CSR を生成し、発行局に CSR を送付する。

JCAN Certificate (JCAN 証明書)

JCAN Certificates can be used for authentication, encryption, and digital signature.
Use of JCAN Certificates shall follow the laws and regulations of the applicable country if any.

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

JCAN Public CA (JCAN 認証局)

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

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

LRA (ローカル登録局)

LRA is the LRA which JIPDEC accredited as Subscribers' representative. LRAs vet the authenticity of the DN and verify the identity of JCAN Certificate Subscribers. Furthermore, the LRA operates the certificate lifecycle management (issuance and revocation) of the certificate under JCAN Certificate Policy.

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 access certificate management services, such as issuance of JCAN

certificates.

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 操作責任者用の証明書である。
この証明書は JCAN 証明書の発行など証明書管理サービスのアクセスに用いる。

MEMBER (メンバー)

MEMBER is the ORGANIZATION's internal individual person.

当該組織の企業内個人。

ORGANIZATION (当該組織)

ORGANIZATION is the organization which operates LRA.

LRA を運用する組織。

PERSON (人)

PERSON is a natural person.

自然人。

PARTNER (パートナー)

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

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

PKCS#12

Encrypted package format of certificate and private key using PIN code

PIN を用いて秘密鍵を含む証明書の暗号化パッケージ

Public Root CA (パブリックルート CA)

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

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

QGIS (行政機関の信頼情報源)

QGIS (Qualified Government Information Source) is a Trustworthy Government Information Source approved by the EV Guidelines, CA/Browser Forum.
It is a database managed by the government and is published online and updated regularly. The

reporting of the data is an obligation under law and a false report will lead to criminal and civil punishment.

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

QIIS（第三者機関の信頼情報源）

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

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

RA（登録局）

RA (Registration Authority) in any network that verifies LRA requests for a certificate and requests CA for the certificate issuance.

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

Relying Party（検証者）

Relying Party is a person that relies on a Subscriber's certificates and/or digital signatures. Relying Party shall refer to the revocation information of the CA in order to verify the validity of JCAN certificates.

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

Repository（リポジトリ）

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

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

Sub CA（サブ CA）

CA which gets its validity authenticated upon the authentication from the upper CAs.

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

Subjects（サブジェクト）

It is the target of certificate issuance.

The Subjects of JCAN Certificates are prescribed in Article 1.4.

証明書発行対象
JCAN 証明書のサブジェクトは、 1.4 項で規定する。

X.400

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

ITU-TS の勧告の一つで電子メールについての標準を定めたもの。

X.500

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

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