GlobalSign
EDI（流通BMS)用電子証明書サービス
認証業務運用規程

Date: October 1st 2015

Version: 1.2

変更履歴

バージョン	日付	備考
1.0	2008 年 7 月 15 日	初稿
1.1	2009 年 1 月 29 日	流通業界共通認証局証明書ポリシーの改訂を反映
1.2	2015 年 10 月 1 日	SHA256 への移行

変更点

v.1.0 (発行日 : 2008 年 7 月 15 日)

- 初稿

v.1.1 (発行日 : 2009 年 1 月 29 日)

- 証明書の利用用途を証明書タイプによって規定しない改訂
- 本人識別と認証の手続きを追加および/または変更する要件の追記

v.1.2 (発行日 : 2015 年 10 月 1 日)

- 問い合わせ先の住所を変更
- 認証局証明書に SHA256 認証局の証明書情報を追加
- CRL の URL として SHA256 認証局から発行される CRL の情報を追加
- 証明書プロファイルの拡張領域の CRLDP の URL を変更
- アルゴリズムオブジェクト識別子の変更

謝辞

GlobalSign 流通EDI 認証業務運用規程は、以下の標準の一部または全部に従って定義しています。

- RFC 3647：インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク
- RFC 3280：インターネット X.509 PKI：証明書と証明書失効リスト（CRL）のプロファイル
- RFC 3039：インターネット X.509 PKI：適格証明書プロファイル
- RFC 2560：インターネット X.509 PKI：オンライン証明書状態プロトコルーOCSP
- RFC 3279：インターネット X.509 PKI：証明書と CRL プロファイルのためのアルゴリズムと識別子
- ISO 1-7799：情報技術ーセキュリティ技術ー情報セキュリティマネジメントの実践のための規範

1. はじめに

このGlobalSign流通EDI認証局（以下、「GlobalSign CA」）の認証業務運用規定（以下、「CPS」）は、GMOグローバルサイン株式会社（所在地：東京都渋谷区桜丘町20-1　渋谷インフォスタワー。以下、「GlobalSign」）が運用するGlobalSign CAが発行する電子証明書の発行と管理（以下、「GlobalSign証明書サービス」）に関する要件を規定します。
GlobalSign CAは、認定機関より、流通業界共通認証局証明書ポリシー（以下、「CP」）に規定された流通業界共通認証局として適合するとの認定にもとづいて、GlobalSign証明書サービスを提供します。

本CPSは最終であり、GlobalSign、GlobalSign証明書サービスを利用し信頼する利用者および依拠当事者を拘束します。
本CPSは、GlobalSignリポジトリ（https://edi.globalsign.com/repository/）に掲載し、適宜更新します。

本 CPS は広義の証明書ポリシーであり、2003 年 11 月に IETF が作成した RFC3647（インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク）に定められた章・節・項の構成に従って記述しています。証明書ポリシーとは、共通のセキュリティ要件をもつ特定の団体、あるいはアプリケーション類に対して、証明書が適用可能かどうかを示すものとして指定された規範」をいいます。IETF が公開する RFC は、電子署名と証明書管理の分野での標準的な業務の実施の面で、権威ある手引きです。

本 CPS では、章タイトルの多くは RFC 3647 の構成に準じている一方、そこで取り上げられた議題で、必ずしも実装していないものがあります。これらの章は、本 CPS から除外します。追加で記載すべき情報がある場合は、標準的な構成に小項目を書き加えて提示しています。RFC 3647 の書式に合わせることで、GlobalSign CA とその他の CA とをマッピング・相互運用しやすくし、また GlobalSign 証明書に信頼を置く者（以下、「依拠当事者」）が GlobalSign の業務手続を事前に知ることを促進します。
本 CPS では、謝辞の章に採用する標準に関する表明を記載しています。

本 CPS には、GlobalSign 証明書のライフサイクルの期間中における、GlobalSign 証明書サービスの技術的、あるいは手続的な方針と業務について記載します。本 CPS に関する質問、CP への認定機関による適合性判断に関する情報を希望する場合には、以下に問い合わせてください。

GMO グローバルサイン株式会社
150-8512　東京都渋谷区桜丘町 26-1　セルリアンタワー
電話　：03-5728-1551
FAX　：03-5728-1552
電子メール　：edi-info@globalsign.co.jp
URL　：http://edi.globalsign.com/

本 CPS は、利用者が利用約款を承認することで、利用者に対して有効かつ拘束力を持ちます。また、本 CPS は、依拠当事者が GlobalSign ディレクトリに GlobalSign 証明書に関する要求をた

だ送信するだけで拘束力を持ちます。利用者は利用約款により、依拠当事者が同意の有無に関係なく本 CPS の諸条件を承諾することに義務を負わなければなりません。

1.1概要

本CPSの目的は、GlobalSign証明書サービスの業務と手続を説明し、前述の標準仕様への準拠性、公開鍵基盤（以下、「PKI」）業界およびGlobalSign証明書サービスに関連する要件への準拠性を明確にすることにあります。

本CPSで扱う証明書タイプは、以下の通りです。

表 1　証明書タイプ

SSL サーバ証明書 for EDI（法人用）	個人で事業を行っており、かつ法人登記を行っている者を含む法人、法人の従業者、法人が所有するサーバまたはシステムに発行される SSL サーバ証明書。 有効期間は、1 年、2 年、または 3 年。
SSL サーバ証明書 for EDI（個人事業主用）	法人登記を行っていない個人事業主、個人事業主が所有するサーバまたはシステムに発行される SSL サーバ証明書。 有効期間は、1 年、2 年、または 3 年。
クライアント証明書 for EDI（法人用）	個人で事業を行っており、かつ法人登記を行っている者を含む法人に発行されるクライアント証明書。 有効期間は、1 年、2 年、または 3 年。
クライアント証明書 for EDI（法人に属する個人用）	個人で事業を行っており、かつ法人登記を行っている者を含む法人の従業者に発行されるクライアント証明書。 有効期間は、1 年、2 年、または 3 年。
クライアント証明書 for EDI （個人事業主用）	法人登記を行っていない個人事業主に発行されるクライアント証明書。 有効期間は、1 年、2 年、または 3 年。

本CPSは、GlobalSign証明書の使用、管理、信頼など、GlobalSign証明書のライフサイクルに関与するすべてのエンティティの役割と義務と業務を明確に規定します。
本CPSの条項は、GlobalSign CA、GlobalSign登録局（GlobalSign RA）、利用者と依拠当事者など、関与するすべてのエンティティを、その業務のサービスレベルと義務と賠償責任において拘束します。いくつかの条項は、証明書サービスプロバイダやアプリケーションプロバイダ等、他のエンティティにも適用される場合があります。
また、GlobalSign CAは、GlobalSignリポジトリで公開する業務規定に従って、GlobalSign証明書の階層を管理します。

本CPSは、CPの規定に準拠します。CPの目的は、“流通業界において法人や個人事業主がインターネット等のネットワークを利用したGDS、EDI、EPC等に関わる通信を安全に行うために利用する電子証明書を発行するサービスを提供する認証局が最低限守るべき事項を定める”ことであり、従って、GlobalSign証明書サービスに関する広義の運用規定を定めたものといえます。

本CPSに加え、GlobalSignは、以下のようなポリシーを文書で定めます（これらに限定しません）。GlobalSignは、ポリシー文書のうち、GlobalSignが必要と認めたものをGlobalSignリポジトリで公開します。また、内部的なポリシー文書として定めたものについては、一般には公開しませ

ん。

- 事業継続計画
- 情報セキュリティポリシー
- 個人情報保護方針
- 返金ポリシー
- その他

本 CPS が適用される、GlobalSign が運用するルート認証局の名称は以下の通りです。

- GlobalSign EDI CA

これを GlobalSign ルートと呼びます。

GlobalSign 証明書サービスの利用者および依拠当事者は、GlobalSign ルートの一般的な運用に関する説明を読むためだけではなく、GlobalSign 証明書の信頼を確立するために、GlobalSign の CPS を必ず参照しなければなりません。本 CPS での表明にもとづいて GlobalSign ルート階層のチェーン全体の信頼を確立することは、非常に重要です。

電子証明書は、電子取引に参加するエンティティに対し、他の参加者へ身元を証明し、データに電子署名することを可能にします。GlobalSign は、電子証明書によって、利用者とその公開鍵とが関係あることを保証します。
電子証明書を取得する手続には、電子証明書の発行、失効、有効期限などの証明書の管理の側面があると同時に、クライアントの身分証明、名前の識別、認証と登録などを含みます。GlobalSign は、かかる手続を経て電子証明書を発行することで、GlobalSign 証明書のユーザの身分証明について適切な積極的確認と、公開鍵をそのユーザ自身が使っているという積極的関連性を提供します。この場合のエンティティには、状況により必要となるであろうエンドユーザ、他の認証局も含まれます。GlobalSign は、否認防止と認証に使用できる汎用の電子証明書も提供します。かかる証明書は、ワランティポリシーやその証明書が使われるアプリケーションが課す制約に従って、特定のビジネスや契約、商取引レベルでの使用に限定されることがあります。

本CPSは、PKIにおける電子証明書の発行局であるGlobalSignによって保守されています。PKIにもとづいた電子証明書管理環境では、発行局は、すべての利用者証明書が信頼を継承するトラスト階層を管理するエンティティです。

本 CPS は、申請可能期間のあいだ、GlobalSign 証明書の発行をつかさどります。申請可能期間とは、GlobalSign CA が GlobalSign 証明書を発行できる期間のことをいいます。申請可能期間は、GlobalSign 証明書に表示しています。

GlobalSign は、本 CPS に関するご意見を、本書のはじめに記載した宛先で受付けます。

1.2 文書の名前と識別

本書の名称は「GlobalSign 流通EDI 認証業務運用規程」です。

1.3 PKI の関係者

1.3.1 GlobalSign認証局

GlobalSignは、GlobalSign CA を運営します。
GlobalSign CAは、認証局秘密鍵の管理を行い、利用者からのGlobalSign証明書の発行や失効に関わる申請を審査し、GlobalSign証明書を発行します。GlobalSign CAは、GlobalSign証明書の管理について、発行、失効、証明書ステータス情報（証明書失効リスト（CRL））等のサービスの可用性を保証し、また、オンライン登録システムを管理します。

また、依拠当事者が、失効された GlobalSign 証明書に関して情報を取得できるよう、GlobalSign CA はオンラインアクセスの可能な証明書失効リストを用いて情報を公開します。
GlobalSign CAはGlobalSign証明書の発行においてポリシーを作成し、それに従って業務を実施します。
これらは、GlobalSign リポジトリで公開します。

GlobalSign CA には、GlobalSign ルートおよびそれに属するすべての証明書ライフサイクルについて最終的な権限があります。証明書ライフサイクルによって生じる業務の一部は、GlobalSign RA に委託します。

1.3.1.1 GlobalSignが使用する委託業者

GlobalSign は、GlobalSign 証明書の発行、失効、更新、および証明書ステータス情報を含む認証局サービスを供給するために、委託業者を利用して安全な設備を運用します。GlobalSign が使用する委託業者は、機密保持の規定を含むサービス契約にもとづいて GlobalSign 証明書管理の支援サービスを運用します。GlobalSign が使用する委託業者は、GlobalSign が要求するサービスレベルに適合することを保証します。

1.3.2 GlobalSign登録局

GlobalSign RAは、GlobalSign証明書サービスにおいて、GlobalSign CAの機能の一部であり、GlobalSign CA は、GlobalSign RAを通じて加入者たちと連絡を取ります。
GlobalSign RAは、本CPSに従って、利用者から提出した書類等を確認し、GlobalSign証明書の発行や失効に関わる審査を行い、GlobalSign証明書の発行および失効を要求します。GlobalSign RAは、GlobalSign証明書の生成および失効に必要なデータを認証局に提出します。

GlobalSign RAは、

- GlobalSign の利用者の登録業務を担当します。
- GlobalSign 証明書申請登録を受領し、調べ、承認するかあるいは棄却します。
- 発行する証明書タイプによって GlobalSign が指定する利用者の本人識別を実施します。
- 公式の、公証された、あるいは他の承認された文書を使用して利用者申請を調べます。
- 申請を承認する場合には、GlobalSign CA に GlobalSign 証明書を発行するように通知します。
- GlobalSign 証明書について、失効を要求する手続きを実施します。

GlobalSign RA は、GlobalSign の承認と認可にもとづいて活動します。GlobalSign RA は、本 CPS と、GlobalSign RA の業務文書を含め、GlobalSign CA が認可した認証業務手続きに従って活動します。

特定の証明書タイプを発行するために、GlobalSign RA は、サードパーティ認証局が発行した証

明書、あるいは他の第三者データベースおよび情報源を利用する場合があります。信頼できる情報源には、利用者の身分証、運転免許証があります。依拠当事者は、GlobalSign 証明書に適用される CP および本 CPS を参照し、必要な情報を予め確認しなければなりません。
検証後、利用者に GlobalSign 証明書が発行されます。

1.3.3 利用者

GlobalSign証明書サービスの利用者は、GlobalSign証明書を申請し、発行を受け、利用を行う法人、法人の従業者、または個人事業主などです。利用者へのGlobalSign証明書の発行は、GlobalSignと利用者との間のサービス契約関係にもとづいてのみ許可します。

1.3.3.1 サブジェクト（利用者識別情報）

GlobalSign 証明書サービスのサブジェクトは、利用者自身であるか、利用者と関連がある自然人またはサーバやシステムであり、GlobalSign 証明書に記載する公開鍵と対をなす秘密鍵を持ちます。

サブジェクトとして識別される利用者は、

- 法人（日本において法人登記されている組織。個人で事業を行っており、かつ法人登記を行っている者も含む）
- 法人の従業者（役員、社員、契約社員等を含む）
- 個人事業主（法人登記を行っていない事業者のみ）

のいずれかです。
また、GlobalSign 証明書のサブジェクトには、上記の利用者識別情報のほか、

- 法人が所有するサーバまたはシステム
- 個人事業主が所有するサーバまたはシステム

を含めることができます。

すべての利用者に、GlobalSign証明書申請の手続きで説明する信用証明の提出を求めます。

サブジェクトは、GlobalSign RA に登録し、GlobalSign 証明書を申請するために、証明書申請者を指名することができます。

1.3.3.2 証明書申請者

本CPSにおいて、利用者には、サブジェクトによって以下の行為をするように指名された証明書申請者を含みます。

- GlobalSign 証明書を申請します。
- 認証局の利用規約に合意し承諾します。

証明書申請者は、以下のいずれかです。

- 個人の場合、サブジェクト自身です。
- サブジェクトの使用するシステムの管理者です。
- サブジェクトによって雇用された個人です。
- サブジェクトが契約関係にもとづいて行動するサブジェクトの代理人であることを保証する個人です。

1.3.4　依拠当事者
依拠当事者は、利用者証明書に記載した公開鍵に関連して検証することのできる、GlobalSign証明書および電子署名を信頼する自然人あるいは法人です。

依拠当事者は、GlobalSign証明書に依拠して以下の行為を行います。
- 利用者が作成した電子署名を GlobalSign 証明書内の公開鍵を利用して検証します。
- 利用者が提示した GlobalSign 証明書により利用者を認証します。
- 利用者に対して GlobalSign 証明書内の公開鍵を利用して暗号化したデータを送信します。

依拠当事者は、GlobalSign 証明書の妥当性を検証するために、必ず GlobalSign 証明書に記載された情報を信頼する前に、証明書ステータス情報を参照しなければなりません。

依拠当事者は、本 CPS に定める義務を果たさなければなりません。

1.3.5　認定機関
認定機関は、流通業界において法人や個人事業主がインターネット等のネットワークを利用したGDS、EDI、EPC等に関わる通信を安全に行うために利用する証明書を発行するサービスを提供する認証局を認定するエンティティです。CPの管理組織であり、本CPSがCPに適合していることの判断を行います。

1.3.6　他の参加者
規定しません。

1.4 証明書の利用方法
GlobalSign証明書は、下記の明示的に許可された目的にのみ、使用できます。

メッセージ署名：
メッセージ署名は、電子書類、電子メール等の電子署名をサポートする電子取引にのみ使用できます。この用途は、メッセージ署名をサポートするアプリケーションを使用する中で、電子署名を作成することのみを保証されています。

SSLサーバ認証：
SSLサーバ認証は、ウェブサイト、その他のオンラインコンテンツへのアクセスを支援する電子取引にのみ使用できます。SSLサーバ認証は、電子証明書の利用者を認証する目的としたトランザクションの中で、利用します。

SSLクライアント認証：
SSLクライアント認証は、ウェブサイトと、その他ソフトウェアオブジェクト等のオンラインリソースの識別をサポートする電子取引にのみ使用できます。SSLクライアント認証は、電子証明書を介して利用者が安全の確保を望むデバイス認証証明書の目的としたトランザクションの中で、利用します。

暗号化：

すべての証明書タイプは、電子証明書により通信の秘匿性を確実にすることに使用できます。

これ以外の電子証明書の使用は、本CPSではサポートしません。

1.4.1 適切な証明書の利用

GlobalSign 証明書の利用用途は、以下の規定の範囲に制限します。

なお、EPC で使用される証明書については、本 CPS 策定時おいて定められていないために、利用用途を規定しません。

許可されていない使用法は、GlobalSign 証明書の利用者と依拠当事者に与える GlobalSign の保証が無効となる原因となります。

- GDS または EDI 用途のメッセージ署名・暗号化
- GDS または EDI 用途の SSL サーバ認証・暗号化
- GDS または EDI 用途の SSL クライアント認証

1.4.2 禁止される証明書の利用

利用者は如何なる理由によっても、前項に定める証明書の利用用途以外に GlobalSign 証明書を利用してはなりません。
また、エンドエンティティ証明書の使用は、証明書の拡張である keyUsage を使って制限します。この拡張と矛盾した証明書の利用は許可しません。

1.5 ポリシー管理

GlobalSignポリシー管理局が本CPSを管理します。GlobalSignは、GlobalSign証明書のライフサイクル管理での運用条件を本CPSに定め、広く参照可能にします。
信頼性を強化するため、認定要件と法的要件によりよく適合するため、あるいは状況により必要となった場合、GlobalSignは、本CPSを改訂することがあります。

1.5.1 文書を管理する組織

GlobalSignポリシーの最新版は、GlobalSignポリシー管理局が承認します。現在の組織構成において、GlobalSignポリシー管理局は以下メンバーから成ります。

- GlobalSign 経営管理者のメンバー最低 1 人。
- 直接 GlobalSign 業務ポリシーの起草と整備に携わった承認された代理人最低 2 人。

経営管理者は職務上GlobalSignポリシー管理局の議長を務めます。

GlobalSignポリシー管理局のすべてのメンバーが1票を持っています。他のいかなる当事者にも投票権はありません。ロック投票の場合にはGlobalSignポリシー管理局の議長の投票を2票と数えます。

1.5.2 連絡窓口

本CPSに関する連絡窓口は、本CPSの初めの章に記載しています。

1.5.3　CPSのポリシー適合性を決定する者
本CPSのCPへの適合性判断は、認定機関により行われます。かかる適合性判断の責任は、GlobalSignポリシー管理局が負います。

1.5.4　CPS承認手続
GlobalSign ポリシー管理局と認定機関による承認により、本 CPS は GlobalSign リポジトリで公表します。

1.6 定義と略語
用語の定義および略語は、本 CPS の最後に記載します。

2.　公開とリポジトリの責任
2.1 リポジトリ
GlobalSign は、本 CPS と、依拠当事者等が利用者証明書を対象とした証明書ステータス情報を参照できるよう、GlobalSign リポジトリで公布します。

2.2 証明情報の公開
GlobalSign は、GlobalSign リポジトリで以下の情報を公布します。
- CPS
- 利用規約
- 依拠当事者規約
- GlobalSign ルート証明書
- 証明書ステータス情報（CRL として）

2.3 公開の時期、および頻度
GlobalSignは、CPS、利用規約および依拠当事者規約を更新した場合、直ちに公開します。
GlobalSign CAの証明書は発行した都度、直ちに公開します。また、「4.9.7 証明書失効リストの発行頻度」に定める頻度でCRLを発行し、公開します。

GlobalSignは、GlobalSignリポジトリの情報を公開する内部的な手続きを定め、また、内部的なセキュリティポリシーを文書で定めますが、これらは一般には公開しません。しかし、認定機関の行う監査においては、求めに応じて手続きや文書を開示します。

2.4 リポジトリへのアクセス管理
GlobalSign は、GlobalSign リポジトリへのアクセスに制限を行いません。

3.　識別と認証
GlobalSignは、利用者の識別と認証を行う登録局であるGlobalSign RAを運営します。GlobalSign RAは、GlobalSign CAにGlobalSign証明書の発行を要求する前に、利用者の識別と認証を行います。
GlobalSign RAは、登録商標の識別を含め、利用者名の識別業務を執り行う適切な手続を定め、保持しています。また、GlobalSign RAは、GlobalSign証明書の失効を要求するエンティティの認

証業務を行います。

3.1名前決定

3.1.1　名前の種類

GlobalSign証明書のサブジェクト名は、X.500シリーズ勧告におけるDistinguished Nameの形式に従います。

3.1.2　名前が意味を持つことの必要性

EPC用の証明書については標準（「EPCglobal Certficate Profile Ratified Specification 1.0」2006月3月8日　EPCglobal Inc.）に準拠するものとし、本CPSには定めません。

3.1.2.1 GlobalSignルート証明書に記載される名称

GlobalSignルート証明書に記載される名称は以下の通りです。

表　2 GlobalSign EDI CA(2015年9月30日まで証明書を発行)の証明書

No.	項目	仕様
1	ContryName	"jp"
2	OrganizationName	"GlobalSign K.K."
3	CommonName	"GlobalSign EDI CA"
4	OrganizationalUnitName	"CA for manufacturers-distributors-retailers"

表　3 GlobalSign EDI CA – SHA256 – G3 CA (2015年10月1日から証明書を発行)の証明書

No.	項目	仕様
1	ContryName	"jp"
2	OrganizationName	"GMO GlobalSign K.K."
3	CommonName	"GlobalSign EDI CA – SHA256 – G3 "
4	OrganizationalUnitName	"CA for manufacturers-distributors-retailers"

3.1.2.2 利用者証明書に記載される名称

利用者のSSLサーバ証明書に記載される名称は以下の通りです。

表　4 法人のSSLサーバ証明書

No.	項目	設定	仕様
1	ContryName	◎	"JP"
2	OrganizationName	◎	法人の英語名称
3	CommonName	◎	法人の所有するサーバまたはシステムのFQDN名・システム名称

4	OrganizationalUnitName		法人の所有するサーバまたはシステムを管理する部署の英語名称
5	StateOrProvinceName		法人が所在する都道府県名
6	LocalityName		法人が所在する市区町村名

表 5 個人事業主のSSLサーバ証明書

No.	項目	設定	仕様
1	ContryName	◎	"JP"
2	OrganizationName		"Natural Person"
3	OrganizationalUnitName	◎	個人事業主の名称（ヘボン式ローマ字表記）
4	CommonName	◎	個人事業主の所有するサーバまたはシステムのFQDN名又はシステム名称
5	StateOrProvinceName		法人が所在する都道府県名
6	LocalityName		法人が所在する市区町村名

利用者のクライアント証明書に記載される名称は以下の通りです。

表 6 法人または法人の従業者のクライアント証明書

No.	項目	必須	仕様
1	ContryName	◎	"JP"
2	OrganizationName	◎	法人の英語名称
3	OrganizationalUnitName		従業者が所属する部署の英語名称
4	CommonName	◎	法人の英語名称、または従業者の名称（ヘボン式ローマ字表記）
5	StateOrProvinceName		法人が所在する都道府県名
6	LocalityName		法人が所在する市区町村名
7	EmailAddress	◎	法人または従業者の電子メールアドレス

表 7 個人事業主のクライアント証明書

No.	項目	設定	仕様
1	ContryName	◎	"JP"
2	OrganizationName		"Natural Person"
3	CommonName	◎	個人事業主の名称（ヘボン式ローマ字表記）
4	StateOrProvinceName		法人が所在する都道府県名
5	LocalityName		法人が所在する市区町村名
6	EmailAddress	◎	法人または従業者の電子メールアドレス

3.1.3 利用者の匿名性、または仮名性

GlobalSignは、GlobalSign証明書において利用者の匿名を許可しません。

GlobalSignは、条件付きでGlobalSign証明書の仮名の使用を受諾することがあります。GlobalSignは、合理的で正当性のある申請調査に従って、GlobalSign証明書に対して仮名の許可を拒否する権利を保有します。仮名の申請を棄却することの理由は、以下に制限しません。

- 既に使用されている
- 第三者の権利を侵害する
- 中傷である

GlobalSignは、仮名の申請と拒否の文書記録を保存します。

GlobalSignは、正当で合法的な利害を証明できる当事者に対して、仮名のGlobalSign証明書所有者の真の身元を公表する可能性があります。

利用者は、利用者に連絡を取れる物理的な住所、その他の情報を提示します。

GlobalSignは個別の申請に対し、仮名とともに正式な名前をGlobalSign証明書に挿入する権利を保有します。

3.1.4　種々の名前形式を変換するための規則

種々の名前形式を変換するための規則は、本CPS「7. 証明書、CRL、およびOCSPのプロファイル」に従います。

3.1.5　名前の一意性

利用者の名称は、GlobalSignが本CPSのもとで発行するGlobalSign証明書において一意とします。

3.1.6　認識、認証、および商標の役割

商標、商号、トレードマーク等の使用の権利については、所有者にすべての権利が留保されます。GlobalSignは、利用者の名称における利用者のかかる権利の所有について、検証を行いません。

3.2 初回の本人性確認

GlobalSignは、利用者の本人識別と認証をするために、第三者データベースを情報源として利用する場合があります。

GlobalSignの初回の利用者登録の本人識別および認証は、以下のいずれかを含みます。

- 出生国の指定機関が発行した身分証あるいはパスポートのような物理的な本人識別文書にもとづいて、本人識別と認証を行います。
- 提示された他の書類や証明書にもとづいて、本人識別と認証を行います。
- GlobalSign 証明書発行前に、利用者に GlobalSign RA への出頭を要求します。
- サードパーティの代理人との代理関係（例えば外注契約など）についての証拠提出を要求します。

GlobalSignは、利用者の本人識別と認証に十分な証拠が提出されない場合、利用者にGlobalSign

証明書の発行を拒否することがあります。
GlobalSignは、GlobalSign証明書を発行するために、利用者に十分な信用証明物（登録URLとパスワード）を提供するよう努力し、そのような登録プロセスをオンライン化します。GlobalSignの判断で、そのような信用証明を二要素化し、合意された実績のある接続方法を使用する独立経路による通信にするかもしれません。

利用者の本人識別と認証は、GlobalSign RAが作成する手続文書に従って実施されます。

3.2.1 秘密鍵の所持を証明する方法
サブジェクトフィールドで識別される利用者は、サブジェクト自身によってか、指定された代理人を通じて、GlobalSignへ公開鍵情報を含む証明書署名要求（CSR）の提示をすること等で、対応する秘密鍵の所持を証明しなければなりません。

3.2.2 組織の本人性の認証
GlobalSignは、法人の証明書、法人の従業者の証明書、法人が所有するサーバまたはシステムの証明書を発行する際に、以下のいずれかの方法により法人の本人識別と認証を行います。

- 商業登記簿謄本、法人印の印鑑証明書、および法人印による押印がなされた証明書申請書の確認
- 民間調査会社が割り当てる企業コードと公開情報を利用した電話による法人に対する申請の意思の確認

GlobalSign は、これらに準ずる別の方法で法人の本人識別と認証の手続きを行う場合には、GlobalSign ポリシー管理局および認定機関の承認を得て、本 CPS を改訂します。

また、FQDN名を含む証明書についてはwhois等のサードパーティデータベースを検索すること、またはドメインの所有者からドメインの独占的使用を許諾されていることの確認により、かかるFQDNを法人が利用する権利を有していることの確認を行います。

3.2.3 個人の本人性の認証
GlobalSignは、個人事業主の証明書、個人事業主が管理するサーバまたはシステムの証明書を発行する際に、以下の方法により個人事業主個人の本人識別と認証を行います。

- 個人印の印鑑登録証明書、および個人印による押印がなされた証明書申請書の確認

GlobalSign は、これらに準ずる別の方法で個人事業主個人の本人識別と認証の手続きを行う場合には、GlobalSign ポリシー管理局および認定機関の承認を得て、本 CPS を改訂します。

また、FQDN名を含む証明書についてはwhois等のサードパーティデータベースを検索すること、またはドメインの所有者からドメインの独占的使用を許諾されていることの確認により、かかるFQDNを個人事業主が利用する権利を有していることの確認を行います。

3.2.4 確認しない利用者の情報
GlobalSignは、GlobalSign証明書を発行する際に、以下の申請情報について、利用者が真正性を保証することの確認のほかは、本人識別、実在性、所有および使用の権利その他について検証を行いません。

- （法人の場合）部署名
- （法人の従業者の場合）氏名
- （個人事業主の場合）店名・屋号
- メールアドレス

3.2.5 権限の正当性確認
権限の正当性確認は、「3.2.2 組織の本人性の認証」及び「3.2.3 個人の本人性の認証」において定める手続にもとづいて行います。

3.2.6 相互運用の基準
規定しません。

3.3鍵更新申請時の本人性確認と認証
3.3.1 証明書の更新時の本人性確認と認証
GlobalSignは、通常のGlobalSign証明書の更新時には、GlobalSign証明書の初回発行と同様の本人識別と認証を行います。
利用者からの電子署名を確認する等、初回発行と異なる方法により更新に関する申請が利用者から行われていることの確認を行う場合、合せて初回申請と同等の利用者の実在性確認を行うものとします。

3.3.2 証明書の再発行時の本人性確認と認証
GlobalSignは、何らか事由によって利用者のGlobalSign証明書を失効した後に、GlobalSign証明書の再発行を行う場合は、初回発行時と同様の本人識別と認証を行います。

3.3 失効申請時の本人性確認と認証
サブジェクトタイプ（CA、RA、利用者、および他の参加者）に応じた失効要求の認証手続きのために、GlobalSign は、オンライン認証メカニズム（例えば電子証明書認証、PIN など）を使うこと、または GlobalSign に失効要求を送付することを求めます。

利用者より GlobalSign 証明書の失効要求が行われた場合、GlobalSign は以下のような方法により失効要求が、GlobalSign 証明書を所有しているものによって行われていることを確認します。
- 利用者が事前に登録している失効用のパスワードを確認する
- 利用者より GlobalSign 証明書で証明されている公開鍵に対応する秘密鍵による電子署名を受領する
- GlobalSign が管理している利用者の電話番号を利用した、利用者の失効意思の確認
- その他、失効の要求当事者が利用者本人であることを確認する方法

なお失効対象の GlobalSign 証明書の失効要求を発行申請と異なるものが代理申請する場合は、上記の方法による利用者の GlobalSign 証明書所有確認に加えて、利用者が代理申請する者に申請を委任したことを書面等により確認します。

4. 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書申請を提出することができる者

証明書申請者がサブジェクトと異なる場合には、次項の登録手続きに列挙した要件はサブジェクト自身が満たします。そうでなければ、サブジェクトに指示された証明書申請者が要件を満たします。

GlobalSignに証明書サブジェクトとなるべくGlobalSign証明書の利用を申請できる者は以下の通りです。

- 法人の従業者
- 個人事業主

GlobalSign RAは、証明書申請者に代わって、GlobalSign CAに証明書要求において正確な情報を提供する義務があります。GlobalSign CAは、権限を持つ登録局からのGlobalSign証明書発行要請を受けて、その役割を果たします。

4.1.1.1 SSLサーバ証明書の発行ステップ

1. 利用者は、鍵ペアを利用者の装置（例えばコンピュータ、スマートカードデバイスなど）で生成します。利用者の要求により、GlobalSign が代わりに鍵ペアを生成することがあります。これらの場合には、申請者に安全に配信できるよう、申請情報に強固な活性化データ（PIN やパスワード等）を含むことが求められます。
2. 利用者は、SSL リンク（https）を通じて、GlobalSign の指定する URL または API （アプリケーション・プログラミング・インタフェース)を通じて、オンラインで申請情報を提出します。（以下を含みますが、これらに限りません）
   - コモンネーム
   - 公開鍵を含む CSR
   - 法人または個人の情報
   - 電子メールアドレス
   - 請求情報
3. 利用者は、オンラインで利用規約を受諾します。
4. GlobalSign は、オンラインで申請情報を受領します。
5. GlobalSign は、利用者の本人識別と認証を実施します。
6. GlobalSign は、利用者に GlobalSign 証明書を発行し、通知します。 GlobalSign が、証明書とともに GlobalSign が生成した秘密鍵を申請者に供給する場合には、秘密鍵は GlobalSign が生成した活性化データと申請時に申請者によって提供された活性化データの連結から成る活性化データによって保護されます。

更新：できます。
失効：できます。

4.1.1.2 クライアント証明書の発行ステップ

1. 利用者は、鍵ペアを利用者の装置（例えばコンピュータ、スマートカードデバイスなど）で生成します。利用者の要求により、GlobalSign が代わりに鍵ペアを生成することがあります。これらの場合には、申請者に安全に配信できるよう、申請情報に強固

な活性化データ（PIN やパスワード等）を含むことが求められます。

2. 利用者は、SSL リンク（https）を通じて、GlobalSign の指定する URL または API を通じて、オンラインで申請情報を提出します。(以下を含みますが、これらに限りません)
   - コモンネーム
   - 公開鍵を含む CSR または秘密鍵の活性化データ
   - 法人または個人の情報
   - 電子メールアドレス
   - 請求情報
3. 利用者は、オンラインで利用規約を受諾します。
4. GlobalSign は、オンラインで申請情報を受領します。
5. GlobalSign は、利用者の本人識別と認証を実施します。
6. GlobalSign は、利用者に GlobalSign 証明書を発行し、通知します。GlobalSign が、証明書とともに GlobalSign が生成した秘密鍵を申請者に供給する場合には、秘密鍵は GlobalSign が生成した活性化データと申請時に申請者によって提供された活性化データの連結から成る活性化データによって保護されます。

更新：できます。
失効：できます。

4.1.2 登録手続き、および責任

利用者は、以下の登録プロセスを行います。

- 申請フォームに記入します。
- 直接あるいは代理人を通じて、最小で 1024 ビット以上の鍵長の鍵ペアを生成します。（GlobalSign は例外条件下で 1024 ビット未満の鍵を受領することがあります。）
- 生成された、秘密鍵に対応する公開鍵を GlobalSign に提出します。
- 利用規約を受諾します。

利用者は、利用規約によって、GlobalSign証明書サービスの諸条件を受諾しなければなりません。利用規約は、本CPSを参照により組み込みます。

通常は、GlobalSignがそのように明示する場合には、オンライン登録プロセスだけで十分です。その他の場合には、必要に応じて、利用者の正確な身元が合理的に確認できる信用証明を求めます。これには、自署された利用規約や身分証のコピーの提出、GlobalSign RAへの出頭を含みます。

4.2 証明書申請の処理手順

4.2.1 本人性確認と認証機能の実行

GlobalSign RAは、証明書申請があれば利用者の識別を検証する役割を果たします。GlobalSign RAは、手続文書に従って利用者の識別を検証します。

法人および法人内の個人がGlobalSign証明書の発行を希望する場合は、利用者は、「3.2.2 組織の本人性の認証」に定める内容に従ってGlobalSign RAに書類または情報を提出しなければなりません。
また、個人事業主がGlobalSign証明書の発行を希望する場合は、利用者は、「3.2.3 個人の本人

性の認証」に定める内容に従ってGlobalSign RAに書類または情報を提出しなければなりません。

GlobalSign RAは、法人の定款や、組織の法的代表者から法人内の個人の雇用の確認書の提出を要求することがあります。また、GlobalSign RAは、利用者の検証を支援するその他の信用証明を要求することがあります。

4.2.2 証明書申請の承認、または却下

GlobalSign RAは前項に定める手続において、書類の不備、本人識別時における疑義、およびその他の懸念が生じた場合などは、申請を許可しません。承認の場合も、棄却の場合も、必ずしも利用者、または他の当事者に正当性を示す必要はありません。

申請が承認されれば、GlobalSign RAは登録データをGlobalSign CAに伝えます。証明書申請が棄却された場合、GlobalSign RAは申請棄却の理由を注釈として残します。

4.2.3 証明書申請の処理に要する時間

GlobalSignは、申請情報を確認し、GlobalSign証明書を妥当な期間内に発行できるよう努力します。通常、検証には、1～7営業日かかります。

4.3 証明書発行

4.3.1 証明書の発行過程における認証局、および登録局の行為

GlobalSign RA は、証明書申請を承認する場合、GlobalSign CA に証明書発行要求を送ります。GlobalSign CA は、信用証明（特別な登録局管理者証明書）にもとづいて GlobalSign RA を識別します。GlobalSign CA は、申請や、登録局証明書の申請者を棄却する権利を保持します。

登録局からの要求は、GlobalSign CA の仕様に合ったフォーマットで有効な利用者データを含んでいれば承認され、速やかに GlobalSign 証明書が発行されます。

4.3.1.1 証明書生成

GlobalSign証明書の発行および更新に関して、GlobalSignは、すべての当事者に対し、GlobalSign証明書を以下に定める条件に従って安全に発行することを表明します。

- GlobalSign 証明書を発行する手続において、利用者が生成した公開鍵の提出を含め、間違いなく付随する登録と結び付けます。
- 特に利用者が認証局、登録局と通信をする際、データ登録の秘匿性および完全性を常に SSL リンク（https）を通じて保証します。
- 登録者の認証を、提供された適切な信用証明を通じて保証します。
- 広く行われている標準へ適合するため、証明書要求と生成は、堅固試験済みの手順によって行われます。
- GlobalSign は、外部の登録サービスプロバイダが使用する場合、その身元が検証され、認知されている登録サービスプロバイダと登録データをやりとりすることを保証します。
- GlobalSign は、サービスと業務について、第三者の監査を受けます。

4.3.2 利用者に対する証明書発行通知

GlobalSign は、GlobalSign 証明書を発行後ただちに、直接あるいは代理人を通じて、GlobalSign 証明書を利用者に届けます。

4.4 証明書の受領

4.4.1 証明書の受領確認の行為

利用者は、GlobalSign 証明書を受領した場合、GlobalSign 証明書の記載内容を確認し、記載内容に誤りが含まれていないことの確認を行わなければなりません。GlobalSign は、証明書発行後 7 日以内に申し出ない限り、利用者が GlobalSign 証明書を受諾したものとみなします。

GlobalSign 証明書の記載内容に誤りが含まれていた場合を含み、GlobalSign 証明書を受諾することに異議がある場合には、受諾の拒否の理由とともに、明確に GlobalSign に通知しなければなりません。

4.4.2 認証局による証明書の公開

GlobalSign は、発行された GlobalSign 証明書をリポジトリに掲示する権利を保有します。

4.4.3 他のエンティティに対する認証局の証明書発行通知

GlobalSignは、GlobalSign証明書の発行を他のエンティティに通知する権利を保有します。

4.5 鍵ペアと証明書の用途

4.5.1 利用者による秘密鍵、および証明書の使用

利用者はここに、有効期間中のGlobalSign証明書に記載されたいかなるすべての情報の変更も、あるいは、その他の著しくGlobalSign証明書の有効性に影響する事実も、GlobalSignに直接通知すべき、継続的な義務を負うことを通知されます。この義務は利用者自身または代理人を通じて履行することができます。

GlobalSignは、登録局の要請によってのみ、GlobalSign証明書を発行するか、失効します。

4.5.1.1 利用者の義務

利用者の義務は、以下の通りです。

1. 電子証明書の利用と防護に必要な知識を持ち、必要であれば電子証明書を使用するために必要な知識を追求する責任を負うこと
2. GlobalSign リポジトリに公開する本 CPS、利用規約および関連ポリシーのすべての条件に同意すること
3. 本 CPS に従って、GlobalSign 証明書を、準拠法を遵守し、許可された用途にのみ使用すること
4. 利用者の秘密鍵および GlobalSign 証明書を、「1.4.1 適切な証明書の利用」に定める証明書の利用用途に即して利用すること。
5. GlobalSign に、法あるいは他者の権利を侵すなにものも提出しないこと
6. GlobalSign に、正確な情報を提出すること
7. 使用する秘密鍵に対応する公開鍵を GlobalSign に提出すること
8. 信頼性のあるシステムを使用し、鍵ペアを安全に生成すること
9. 秘密鍵を適切に保護する安全な装置や製品を使用すること。

10. 目的に適した鍵長とアルゴリズムを使用して鍵ペアを生成すること
11. GlobalSign 証明書を、合理的な環境下で使用すること。
12. GlobalSign が課すライセンス制限を超えて GlobalSign 証明書を使用しないこと。
13. GlobalSign 証明書の受領後、受諾し利用を開始する前に、GlobalSign 証明書に記載された情報が正しいことを確認し、万一不正確な情報が記載されていた場合、GlobalSign 証明書を使用せず GlobalSign へ通知すること
14. 提出した情報に変更が生じた場合には、GlobalSign へ通知すること
15. GlobalSign 証明書に記載された情報が正しくなくなった場合は、GlobalSign 証明書の利用をやめること
16. GlobalSign 証明書が無効になった場合は、GlobalSign 証明書の使用をやめること
17. GlobalSign 証明書が無効になった場合は、GlobalSign 証明書をインストールした機器やアプリケーションから削除すること
18. GlobalSign 証明書を、不正操作から防護すること
19. 秘密鍵および活性化データを危殆化、紛失、盗難、不正開示、改ざん、その他の不正使用から防護すること
20. 秘密鍵の生成、維持、キーエスクロー、破壊するために利用者が使用するパートナーまたは代理人の行為や不作為に起因するものについて責任を負うこと
21. GlobalSign 証明書の有効期間中に秘密鍵および活性化データの危殆化を疑ったり、または危殆化の事実に気付いたりした場合、直ちに GlobalSign へ通知すること
22. GlobalSign 証明書の保全に重大な影響を及ぼす事象が発生した場合、証明書失効要求を提出すること

利用者は、常に認証局に対して上述の義務を負います。

利用者が異なる名前のサブジェクトの代わりに申請する場合には、特定の義務は証明書申請者に移り、サブジェクトからは軽減されます（代わりに、証明書ライフサイクルに影響する不測の事態が生じた場合、証明書申請者に通知しなければなりません）。かかる場合には、上記の項目のうち、3、4、8、9、10、11、12、13、14、15、16、17、18、19、21、22の義務はサブジェクトに適用され、証明書申請者には適用されません。

4.5.1.2 利用者の依拠当事者に対する義務

本CPSの他の条項に記述された他の利用者の義務を制限することなく、利用者は、そこに含まれる表示合理的に依拠するサードパーティに対するあらゆる不実表示防止する義務を持ちます。

4.5.2 依拠当事者による公開鍵、および証明書の使用

4.5.2.1 依拠当事者の義務

依拠当事者の義務は、以下の通りです。

1. 電子証明書の利用に必要な知識を持ち、必要であれば電子証明書を使用するために必要な知識を追求する責任を負うこと
2. GlobalSign リポジトリに公開する本 CPS、依拠当事者規約および関連ポリシーのすべての条件に同意すること
3. 「1.4.1 適切な証明書の利用」に定める証明書の利用用途に即した場合のみ信頼すること。
4. GlobalSign リポジトリより入手可能な GlobalSign ルート証明書を、信頼できる認証局

証明書として入手すること
5. GlobalSign リポジトリに公開する証明書ステータス情報を使い、GlobalSign 証明書の有効性を、チェーンを含み適切に検証すること
6. GlobalSign 証明書に記載された情報が正しく、最新であると検証できたときに限り、その GlobalSign 証明書を信頼すること
7. GlobalSign 証明書を、合理的な環境下でのみ信頼すること。
8. GlobalSign 証明書を、失効されていない場合のみ信頼すること。
9. GlobalSign 証明書の有効期間中に秘密鍵の危殆化を疑ったり、または危殆化の事実に気付いたりした場合、直ちに GlobalSign へ通知すること
10. 本 CPS または GlobalSign 証明書の中で示された、証明書の用途制限に注意を払うこと
11. GlobalSign 証明書が使用されるアプリケーションに適用される他の規定や条件に沿った安全対策をとること

4.6 証明書の更新

GlobalSignは、鍵の更新を伴わないGlobalSign証明書の更新は実施しません。

4.7 証明書の鍵更新

4.7.1 鍵の更新を伴う証明書の更新の場合

利用者は、失効されていない利用者証明書の有効期限が満了する場合、鍵の更新を伴うGlobalSign証明書の更新要求をオンラインで提出できます。
鍵の更新を伴うGlobalSign証明書更新の要件は、元来サービスに加入するために必要とされたものから変更されることがあります。

4.7.2 新しい公開鍵の証明書の申請を行うことができる者

鍵の更新を伴うGlobalSign証明書の更新を申請できる者は以下の通りです。

- 利用者

4.7.3 証明書の鍵更新申請の処理

GlobalSignは、鍵の更新を伴うGlobalSign証明書の更新時には、GlobalSign証明書の初回発行と同様の利用者に対する認証を行うか、または利用者からの電子署名を確認することで更新に関する申請が利用者から行われていることの確認を行います。

4.7.4 利用者に対する新しい証明書の通知

GlobalSign は、鍵の更新を伴う更新された GlobalSign 証明書が発行されれば、直接あるいは代理人を通じて、発行された GlobalSign 証明書を利用者に届けます。

4.7.5 鍵更新された証明書の受領確認の行為

利用者は発行された鍵更新済みの GlobalSign 証明書を受領した場合、GlobalSign 証明書の記載内容を確認し、記載内容に誤りが含まれていないことの確認を行わなければなりません。登録局が、GlobalSign 証明書の受領を確認した時点で、GlobalSign 証明書は利用者に受諾されたものとみなします。

GlobalSign 証明書の記載内容に誤りが含まれていた場合を含み、GlobalSign 証明書を受諾することに異議がある場合には、受諾の拒否の理由とともに、明確に GlobalSign に通知しなければなりません。

4.7.6 認証局による鍵更新済みの証明書の公開

GlobalSign は、発行された鍵更新済みの GlobalSign 証明書をリポジトリに掲示する権利を保有します。

4.7.7 他のエンティティに対する認証局の証明書発行通知

GlobalSignは、鍵更新済みのGlobalSign証明書の発行を他のエンティティに通知する権利を保有します。

4.8 証明書の変更

GlobalSignはGlobalSign証明書の変更は実施しません。

4.9 証明書の失効と一時停止

4.9.1 証明書失効の場合

GlobalSignは、GlobalSign証明書の失効について明確なガイドラインを発行しする合理的な努力を払い、年中無休で失効要求を受け付け、応答する体制を維持します。

GlobalSignは、GlobalSign証明書の失効要求をする利用者の本人識別を、内部の手続き文書に従って実行します。 この手続の認定機関に規定された要件への適合性は、認定機関による監査対象となります。

GlobalSign証明書は、以下の場合失効されます。

- 利用者が GlobalSign 証明書の利用を取りやめる場合。
- 秘密鍵に危殆化が発生した場合、またはそれを疑うべき事実があることを知った場合。
- GlobalSign 証明書内の情報に変更があった場合。
- その他、GlobalSign が必要と認めた場合。

4.9.2 証明書失効を申請することができる者

GlobalSign証明書の失効を申請できる者は以下の通りです。

- 利用者
- 利用者と同じ法人の従業者
- GlobalSign

要求当事者は、GlobalSign証明書の利用者として、あるいは少なくともGlobalSign証明書の利用者の承認された代理人であることを保証できなければなりません。
登録局は、身元が十分に確認され、他から区別できるまで、さらに要求当事者を厳密に調べることがあります。

4.9.3 失効申請手続き

GlobalSign RAが、GlobalSign証明書の失効を希望する当事者の本人識別と認証を実施します。確実に認可された要求により、この手続に着手することができます。
失効要求は、GlobalSignが指定した方法で提出します。あるいは、直接、本CPSの初めの章に記載したGlobalSignの窓口に宛てて、送付することができます。

利用者の申請に基づくGlobalSign証明書の失効を実施する場合は、GlobalSignは、「3.2　初回の本人性確認」に定める認証方法にもとづき、GlobalSign証明書の失効を申請した者が利用者かまたは利用者と同じ法人に所属するものであることの認証を行います。

GlobalSignの申請に基づくGlobalSign証明書の失効を実施する場合の手続は、内部的な文書で定めます。以下のような理由でGlobalSign RAからの要求があれば、GlobalSign CAはGlobalSign証明書を失効します。

- 紛失、盗用、改ざん、不正開示、あるいはその他の証明書サブジェクトの秘密鍵の危殆化があった場合。
- 証明書サブジェクトか、サブジェクトに任命された利用者が、本 CPS 下の重要な義務に違反した場合。
- 自然災害、コンピュータまたは通信の障害、あるいはその他の合理的な人的コントロールを越えた理由で、本 CPS 下義務の遂行が遅延するか妨害され、結果として、他人の情報が著しく脅かされ、危険にさらされている場合。
- 証明書サブジェクトの情報の変更があった場合。

要求当事者の身元を検証し次第、GlobalSign RAはすぐにGlobalSign CAにGlobalSign証明書の失効を要求します。身元の検証は、利用者がGlobalSignに提出した本人識別データに入っている情報要素を通じて実施できます。GlobalSign RAからの要求があれば、GlobalSign CAはGlobalSign証明書を迅速に失効します。

失効が完了したら、GlobalSignは要求当事者へ通知を送信します。

4.9.4 失効申請の猶予期間
利用者は「4.9.1 証明書失効の場合」に定める失効事由に該当した場合、速やかに GlobalSign が定める失効手続きを行わなければなりません。

4.9.5 認証局が失効申請を処理しなければならない期間
GlobalSignは、失効申請情報を確認し、GlobalSign証明書を妥当な期間内に失効できるよう努力します。通常、検証には、1～7営業日かかります。

4.9.6 依拠当事者の失効確認の要求
依拠当事者は GlobalSign 証明書に依拠する前に GlobalSign の最新の CRL を確認し、かかる証明書が失効されていないことの確認を行わなければなりません。

4.9.7 証明書失効リストの発行頻度
CRLは、3時間ごとに発行します。

4.9.8 証明書失効リストの発行最大遅延時間
規定しません。

4.9.9 オンラインでの失効/ステータス確認の適用性
GlobalSign は、GlobalSign リポジトリで、失効されている GlobalSign 証明書の通知を、CRL を通じて発行します。

4.9.10 オンラインでの失効/ステータス確認を行うための要件
規定しません。

4.9.11 利用可能な失効通知の他の形式
GlobalSign は、失効されている GlobalSign 証明書の通知を、さらにその他適切と思われる手段を通じて発行するかもしれません。

4.9.12 鍵更新の危殆化に対する特別要件
GlobalSign CA の秘密鍵が危殆化した場合は、直ちに関係者にかかる事実を通知します。
利用者の秘密鍵が危殆化した場合は、速やかに GlobalSign に通知しなければならず、また指定された GlobalSign 証明書の失効等に関わる手続きを行わなければなりません。

4.9.13 証明書の一時停止の場合
規定しません。

4.9.14 証明書の一時停止を申請することができる者
規定しません。

4.9.15 証明書の一時停止申請手続き
規定しません。

4.9.16 一時停止を継続することができる期間
規定しません。

4.10 証明書のステータス確認サービス
GlobalSignは、CRLおよび適切なウェブインターフェイスを含む、証明書ステータス情報を提供します。

CRLは、すべての有効期間中の失効されたGlobalSign証明書をリストします。CRLは以下のURLから取得可能です。

- SHA1 証明書(2015年9月30日までに発行された証明書)
  http://crl.globalsign.net/ediRootCA.crl
- SHA256 証明書(2015年10月1日以降に発行された証明書)
  http://crl.globalsign.net/ediRootCAsha2g3.crl

4.11 利用の終了
GlobalSign証明書が失効したり、有効期限を過ぎたりした場合には、それにともない利用を終了します。有効期限よりも前に利用者が何らかの事由によりGlobalSign証明書の利用を終了したい場合は、GlobalSign証明書の失効手続きを行わなければなりません。

4.12 キーエスクローと鍵回復
規定しません。

5. 設備上、運営上、運用上の管理
5.1 物理的管理
5.1.1 立地場所、および構造
GlobalSign CA の秘密鍵の管理・利用が行われる施設（以下、「認証局秘密鍵管理施設」）の所在は、必要な関係者以外には公表しません。また、認証局秘密鍵管理施設はその構造上、洪水・地震等の天災に対する対応が行われます。

5.1.2 物理的アクセス
認証局秘密鍵管理施設は、他用途の証明書管理基幹施設と論理的に分離します。認証局秘密鍵管理施設は、非接触 IC カード・生体認証等を利用した厳格な個人による入退室管理が行われます。また、特に重要な部屋については、セキュリティアラームによって物理的に監視し、正当な権限を有する複数人以上の立会いがなければ入室が不可能となります。
登録局の業務を行う施設（以下、「登録局施設」）は、カードによる電磁的なロックと入退室記録の保持の機能を含めた、適切な入退室管理が行われます。

5.1.3 電源、および空調
認証局秘密鍵管理施設は無停電電源装置およびバックアップ発電用エンジンにより停電に対する対策を講じています。また、認証局秘密鍵管理施設において利用する重要な機器が安定動作するよう、空冷空調機を整備します。

5.1.4 水害対策
認証局秘密鍵管理施設は、洪水による浸水・漏水に備えた整備をします。

5.1.5 火災防止、および火災保護対策
認証局秘密鍵管理施設は、火災の検知システムおよび消化システムを整備します。

5.1.6 媒体保管場所
バックアップ用途を含み、GlobalSign が保管する記録媒体は、施錠可能な保管場所に保管しています。またかかる保管場所については適切な搬入出管理が行われ、水害・火災から保護します。

5.1.7 廃棄処理
GlobalSign が廃棄処理を行う書類・記録媒体については、内部的な手続きを定め、適切に廃棄

処理を行います。

5.1.8 施設外のバックアップ
規定しません。

5.2 手続き的管理
5.2.1 信頼すべき役割
GlobalSign は、各要員から、認証局としての義務と責任および目的を全うする GlobalSign と個人との間に利害の不一致がなく、個人情報を含む秘密保持を宣言する書類を署名付きで取得します。
GlobalSign は、その従業員、管理者、セキュリティオフィサー、監査人、その他 GlobalSign の業務に携わるすべての要員が「信頼すべき役割」を担っているとみなします。

5.2.2 職務ごとに必要とされる人数
GlobalSignは、認証局秘密鍵の管理を行う役割には最低二名の要員を任命し、一人の権限のみでは、認証局秘密鍵の利用が行えないようにするための相互牽制の仕組みを講じます。
また、利用者から提出された書類等の審査については、ダブルチェックを義務づける等により一人の担当者の作業では審査が完了しないための仕組みを講じます。

5.2.3 個々の役割に対する本人性確認と認証
GlobalSign は、信頼すべき役割を担う要員について、業務を任命するよりも前に調査を行い、その信頼性と能力、適正を判定します。

5.2.4 職務分割が必要となる役割
GlobalSign は、認証局秘密鍵の管理等の重要な認証局としての機能には、相互牽制の仕組みを適用します。

5.3 人事的管理
5.3.1 資格、経験および身分の要件
GlobalSignの要員は、業務に必要となる要件に合致する資格と経験および身分を保証するための調査を受けます。調査には以下を含みます。

- 犯罪歴
- 職歴
- 前職の雇用の確認
- 報告された学位の取得の確認
- 本人による虚偽申告の有無
- その他必要とおもわれるもの

5.3.2 経歴の調査手続き
GlobalSignは、特定の業務に採用する予定の要員について、所轄の機関により発行される報告書、第三者による調書、または本人による宣言書等を取得することにより、調査を実施します。

5.3.3 研修要件
GlobalSign は、認証局および登録局業務を実施するための要員の研修を実施します。

5.3.4 再研修の頻度および要件
業務および手続の知識を最新にし、また知識を継続して業務に利用することを保証するために、定期的な再研修を実施します。

5.3.5 職務のローテーションの頻度および要件
規定しません。

5.3.6 認められていない行動に対する制裁
GlobalSign は、権限なくシステムを使用することを含め、認められていない行動に対しては制裁を課します。

5.3.7 独立した契約者の要件
委託契約業者およびその要員は、GlobalSign の要員と同じ秘密保護条件に従います。

5.3.8 要員に提供する資料
GlobalSign CA と GlobalSign RA は、研修および再研修において、要員に適宜資料を提供します。

5.4 監査ログの手続き
5.4.1 記録されるイベントの種類
GlobalSign の監査イベント記録には、以下を含みます（これらに限定しません）。

- 認証局秘密鍵の操作
- 認証局秘密鍵を保管する部屋の入退室
- 認証局の重要なシステムを保管する部屋の入退室
- GlobalSign 証明書の発行
- GlobalSign 証明書の失効
- CRL の発行

5.4.2 監査ログを処理する頻度
GlobalSign は、指名された要員が定期的な間隔で監査イベント記録を精査し、特異なイベントを検知、報告することを保証します。

5.4.3 監査ログを保持する期間
GlobalSign は、監査イベント記録を少なくとも１ヶ月以上の期間、読み取りが容易な場所に保管します。

5.4.4 監査ログの保護
GlobalSign は、正当な権限を有する者のみが監査イベント記録にアクセス可能になるように適切な保護措置を講じます。

5.4.5 監査ログのバックアップ手続き
GlobalSign CA は、監査イベント記録をバックアップし、監査人の要求に応じて提供します。

5.4.6 監査ログの収集システム
規定しません。

5.4.7 イベントを起こしたサブジェクトへの通知
規定しません。

5.4.8 脆弱性評価
規定しません。

5.5 記録のアーカイブ
5.5.1 アーカイブされる記録の種類
GlobalSign は、以下の書類・電子データを保存します。

(1) 証明書の初回発行に関する記録
- 利用者が提出した書類
- GlobalSign の審査記録（審査結果、審査日時、審査担当者、承認者に関する情報等）

(2) 証明書の更新に関する記録
- 利用者が提出した書類
- GlobalSign の審査記録（審査結果、審査日時、審査担当者、承認者に関する情報等）

(3) 証明書の失効に関する記録
- 利用者が提出した書類
- GlobalSign の審査記録（審査結果、審査日時、審査担当者、承認者に関する情報等）

(4) 認証局秘密鍵の操作に関する記録

(5) GlobalSign の組織の維持管理に関する記録
- 認証局の体制図およびこれに準ずる書類
- 認証局に関連する規程類（CPS、利用規約、依拠当事者規約等）

5.5.2 アーカイブ保持期間
GlobalSign は、前項に定める保存すべき書類・電子データを最低限以下の期間の間は保管します。

(1) 証明書の初回発行に関する記録・・・かかる証明書の有効期間が満了してから 3 年間
(2) 証明書の更新に関する記録・・・かかる証明書の有効期間が満了してから 3 年間
(3) 証明書の失効に関する記録・・・かかる証明書の有効期間が満了してから 3 年間
(4) 認証局秘密鍵の操作に関する記録・・・かかる認証局秘密鍵が利用されている限り
(5) GlobalSign CA の組織の維持管理に関する記録・・・改訂後より 10 年間

5.5.3 アーカイブの保護
GlobalSign CA は、保管する書類・電子データが、不正に改ざん、紛失、劣化しないための保護措置を講じます。

5.5.4 アーカイブのバックアップ手続き
GlobalSign CAのアーカイブの内部的なバックアップ手続きを定め、適切に処理を行います。

5.5.5 記録にタイムスタンプを付ける要件
規定しません。

5.5.6 アーカイブ収集システム
規定しません。

5.5.7 アーカイブの情報を入手し検証する手続
規定しません。

5.6 鍵の切り替え
規定しません。

5.7 危殆化、および災害からの復旧
5.7.1 事故、および危殆化の取り扱い手続き
GlobalSignは、対象となるインシデント、危殆化レポートと、対処の手続を内部的な文書で定め、以下のインシデントに対し、迅速な復旧作業を実施するために、関係する要員に必要な教育および訓練を行います。

- 認証局秘密鍵の危殆化
- 認証局内で利用しているシステムの障害

5.7.2 コンピュータの資源、ソフトウェア、またはデータが破損した場合
GlobalSignは、コンピュータの資源、ソフトウェア、またはデータが破損したか、破損した疑いがある場合の復旧手順を内部的な文書で定め、可能な限り速やかにバックアップ機、バックアップデータ等を用いて復旧作業を行い、速やかな業務再開に努めます。
もし、これらの資源またはサービスが、GlobalSignの管理下になく、委託契約等による提供である場合には、GlobalSignは、資源またはサービスの所有者または提供者との契約が、内部的に定めた復旧手順の要件に準拠していることを確認します。

5.7.3 エンティティの秘密鍵が危殆化した場合の手続き
GlobalSignは、エンティティのタイプ別に、秘密鍵が危殆化した場合の対処の手続を内部的な文書で定めます。

5.7.4 災害後の事業継続能力
GlobalSignは、コンピュータの資源、ソフトウェア、またはデータ破損の他、災害時等、障害のタイプ別に、適正な期限内にサービスの完全復旧を保証するための内部的な事業継続計画、災害復旧計画および基準を規定します。

5.8　認証局、または登録局の終了

GlobalSignが、業務を終了する場合は、業務を終了する3ヶ月以上前に利用者に対して通知を行うべく努めます。また、GlobalSignが保管する記録等に関して、継続保管又は廃棄に関する取り決めを行い、必要に応じてかかる処置内容を利用者に通知します。
GlobalSignは、業務を終了するその際には自身が発行した有効な利用者のGlobalSign証明書をすべて失効します。

6.　技術的セキュリティ管理

6.1　鍵ペアの生成、およびインストール

6.1.1　GlobalSign CA鍵ペアの生成

GlobalSign CAの秘密鍵は、手続き文書に従い、信頼できる手順で、FIPS140-1 レベル3以上の暗号モジュール上で生成します。また、GlobalSignは、かかる作業を正当な権限を有する複数の者の立会いの上で実施し、GlobalSign CAの秘密鍵の秘密シェアを配布します。
GlobalSign CAの秘密鍵の生成は、証明書発行の目的に適していると認識されているアルゴリズムを使用し、実施します。GlobalSign CAはRSA 2048bitを使用します。

6.1.2　利用者に対する秘密鍵の配送

利用者の秘密鍵の生成は、利用する証明書タイプおよび申請の方法に応じて、利用者自身が行う場合と、あるいは GlobalSign が行う場合があります。
GlobalSign CA の秘密鍵の生成は、信頼すべき役割を担う二名以上の立会いの上で実施します。
GlobalSign が利用者の秘密鍵を生成する場合は、GlobalSign は、セキュアログインを通じて、またはその他の GlobalSign が適切と認めた方法を通じて、当該秘密鍵を安全な方法により利用者に配送します。また、GlobalSign は、利用者への秘密鍵の配送手続きの完了後は、自身が管理する装置等に記録されている利用者の秘密鍵を、GlobalSign が生成する活性化データと利用者のみが知りえる活性化データを使用して暗号化し、信頼すべき役割を担う複数の者によって相互牽制の仕組みを用いた管理のもと、保管します。

6.1.3　認証局に対する利用者の公開鍵

利用者の公開鍵は、SSL等を利用した安全な方法にてGlobalSignに配送されます。

6.1.4　依拠当事者に対する認証局の公開鍵の交付

GlobalSignは、SSLを利用したGlobalSignリポジトリを通じて、依拠当事者に対してGlobalSignルート証明書を安全に配布します。

6.1.5　鍵サイズ

GlobalSignはそのすべての階層構造中の認証局について、2,048ビット以上の鍵長のRSA暗号鍵アルゴリズムを使用します。
利用者は1,024ビット以上の鍵長のRSA暗号アルゴリズムを使用しなければなりません。

6.1.6　公開鍵のパラメータの生成、および品質検査

規定しません。

6.1.7 鍵用途の目的

6.1.7.1 GlobalSign CA鍵用途の目的

GlobalSignルート証明書のkeyUsageの値には、keyCertSign（ルート認証局の秘密鍵、下位の認証局または利用者証明書への署名用途）、およびcRLSign （証明書ステータス情報署名用途）を設定します。

6.1.7.2 利用者の鍵用途の目的

利用者証明書のkeyUsageの値には、digitalSignature（電子署名用途）、keyEncipherment（鍵暗号化用途）、およびdataEncipherment（データ暗号化用途）を設定します。

6.2 秘密鍵の保護、および暗号モジュール技術の管理

6.2.1 暗号モジュールの標準と管理

6.2.1.1 GlobalSign CA鍵保管の管理

GlobalSign CAの秘密鍵は、手続き文書に従い、信頼できる手順で、FIPS140-1 レベル3以上の暗号モジュール上で管理します。

6.2.1.2 利用者鍵保管の管理

利用者は、自身で秘密鍵を作成した、または GlobalSign より秘密鍵を受領した以降は、自身の秘密鍵を、危殆化、紛失、盗難、不正開示、改ざん、その他の不正使用から防護するよう、適切に保護する安全な装置や製品を使用して保管し、管理しなければなりません。

6.2.2 秘密鍵の複数人管理

GlobalSign CA の秘密鍵は、信頼すべき役割を担う複数の者によって相互牽制の仕組みを用いて管理が行われ、一人の管理者の権限のみでは、GlobalSign CA の秘密鍵の利用が行えないようにしています。

また、GlobalSign が利用者の秘密鍵を作成する場合は、GlobalSign から利用者への秘密鍵の配送手続きが完了するまでの間は、信頼すべき役割を担う複数の者によって相互牽制の仕組みを用いて管理が行われ、一人の管理者の権限のみでは、利用者の秘密鍵の利用が行えないようにしています。GlobalSign から利用者までの配送手段についても、セキュアログインを通じて、またはその他の GlobalSign が適切と認めた方法を通じて配送するなど、秘密鍵の不正詐取が起こらないための対策を講じています。

6.2.3 秘密鍵の預託

規定しません。

6.2.4 秘密鍵のバックアップ

GlobalSign CAの秘密鍵は、バックアップ保存され、信頼すべき役割を担う複数の者によって相互牽制の仕組みを用いて管理が行われ、一人の管理者の権限のみでは、GlobalSign CAの秘密鍵の復元が行えないようにしています。

6.2.5 秘密鍵のアーカイブ

規定しません。

6.2.6 秘密鍵の暗号モジュールへの移動
規定しません。

6.2.7 暗号モジュール内での秘密鍵保存
適切なISOの要件を満たして秘密鍵を保存するために、GlobalSignは安全な暗号デバイスを使用します。

6.2.8 秘密鍵の活性化方法
GlobalSign CA の秘密鍵の活性化は、信頼すべき役割を担う複数の者によって行われます。

6.2.9 秘密鍵の非活性化方法
規定しません。

6.2.10 秘密鍵の破棄方法
GlobalSign CA の秘密鍵は、二度と取り出すことができず、二度と使用されないことを保証するために、そのライフタイムの最後に廃棄処理します。鍵廃棄処理の手順は文書化し、鍵廃棄処理の記録を保管します。
GlobalSign が、利用者の秘密鍵を廃棄する必要がある場合には、二度と取り出すことができず、二度と使用されないことを保証するために、確実に廃棄処理します。
利用者は、利用者の秘密鍵が廃棄される必要がある場合には、二度と取り出すことができず、二度と使用されないことを保証するために、確実に廃棄処理しなければなりません。

6.2.11 暗号モジュールの評価
「6.2.1 暗号モジュールの標準と管理」に定めるとおりとします。

6.3 その他の鍵ペア管理
6.3.1 公開鍵のアーカイブ
GlobalSign は、発行したすべての GlobalSign 証明書を、証明書の有効期間の満了後、3 年間アーカイブします。

6.3.2 証明書の運用上の期間、および鍵ペアの使用期間
GlobalSign のすべての階層構造中の認証局証明書の有効期間および認証局秘密鍵の利用期間は、最大で 20 年とします。
利用者証明書の有効期間および利用者の秘密鍵の利用期間は最大で 3 年 2 ヶ月とします。

6.4 活性化データ
6.4.1 活性化データの生成、および設定
GlobalSign CA の秘密鍵の活性化データは、信頼すべき役割を担う複数の者の関与のもと、生成および設定します。

GlobalSign が利用者の活性化データを作成する場合は、信頼すべき役割を担う複数の者の関与のもと、利用者の秘密鍵の活性化データとして妥当な強度の PIN またはパスワードを生成および設定します。
利用者が自身の活性化データを生成する場合については、本 CPS では規定しません。GlobalSign CA は、利用者が利用者の秘密鍵の活性化データとして妥当な強度の PIN またはパスワードを生成および設定することを推奨します。

6.4.2 活性化データの保護

GlobalSign CA の秘密鍵の活性化データは、信頼すべき役割を担う複数の者によって相互牽制の仕組みを用いて管理します。
GlobalSign が利用者の秘密鍵を作成する場合、利用者への秘密鍵の配送が行われるまでは、秘密鍵の活性化データは信頼すべき役割を担う複数の者によって相互牽制の仕組みを用いて管理されます。また、当該活性化データは、セキュアログインを通じて、またはその他の GlobalSign が適切と認めた方法を通じて、安全な方法にて利用者に配送されます。
利用者は、自身で活性化データを作成した、または GlobalSign より活性化データを受領した以降は、当該活性化データを安全に保管しなければなりません。

6.4.3 活性化データの他の考慮点

規定しません。

6.5 コンピュータのセキュリティ管理

GlobalSignは、ISO/IEC27001並びにJIS Q 27001または同等の規格で求められるコンピュータセキュリティ管理に関する要件に準拠し、情報セキュリティマネジメントシステム(ISMS)を確立します。

6.6 ライフサイクルの技術上の管理

GlobalSignは、ISO/IEC27001並びにJIS Q 27001または同等の規格で求められる開発とセキュリティ制御を含むシステム保守に関する要件に準拠し、情報セキュリティマネジメントシステム(ISMS)を確立します。

6.7 ネットワークセキュリティ管理

GlobalSignは、ISO/IEC27001並びにJIS Q 27001または同等の規格で求められるネットワークセキュリティ確保に関する要件に準拠し、情報セキュリティマネジメントシステム(ISMS)を確立します。

- GlobalSign CA は、GlobalSign RA との接続を、電子証明書を用いて認証します。
- GlobalSign CA は、GlobalSign RA およびその他の関連システムとの接続を、電子証明書を用いて暗号化します。
- GlobalSign のウェブサイトは、SSL を提供し、ウィルスから保護します。
- GlobalSign のネットワークは、侵入検知システムと管理されたファイアウォールで保護します。
- G GlobalSign のネットワーク外からの GlobalSign データベースへのアクセスは禁止しています。

6.8　タイムスタンプ

GlobalSignは、「5.4.1 記録されるイベントの種類」および「5.5.1 アーカイブされる記録の種類」に定める書類・電子データには日時情報（一部日付情報のみ）を付与します。

7.　証明書、CRL、および OCSP のプロファイル

7.1 証明書プロファイル

本節では、GlobalSign CAが発行する証明書プロファイルについて規定します。

7.1.1 バージョン番号

GlobalSign CA は、X.509 V.3 標準で定義されている証明書の拡張を含む証明書を発行します。

7.1.2 証明書の拡張

GlobalSign CA は、国際標準化機構（ISO）が定義するとおりに拡張を使用します。
KeyUsage 拡張は、証明書に記載した公開鍵が使用される技術的な用途を制限します。GlobalSign CA 自身の証明書は、証明書、証明書失効リスト、および他のデータに署名することのみに鍵の機能を制限する KeyUsage 拡張を含みます。

GlobalSign ルート証明書の拡張領域は以下の通りです。

表 8 認証局証明書の拡張領域

No.	フィールド	クリティカル	仕様
1	subjectKeyIdntifier	FALSE	keyIdentifierを必須とします。
2	keyUsage	TRUE	cRLSign、keyCertSignとします。 必須とします。
3	basicConstraints	TRUE	CA=TUREとします。 pathLenConstraint=0とします。

また、GlobalSign CA が発行する利用者証明書の拡張領域は以下の通りです。

表 9 利用者のSSLサーバ証明書の拡張領域

No.	フィールド	クリティカル	仕様
1	authorityKeyIdentifier	FALSE	keyIdentifier=SHA-1 160 bits Hashとして値を設定します。
2	subjectKeyIdntifier	FALSE	keyIdentifierを必須とします。
3	keyUsage	TRUE	digitalSignature、keyEncipherment、dataEnciphermentとします。
4	extendedKeyUsage	-	使用しません。
5	certificatePolicies	FALSE	PolicyIdentifier=1.3.6.1.4.1.4146.1.81 とします。

			PolicyQualifierInfo の policyQualifierID は CPSuri、qualifierは https://jp.globalsign.com/repository/ とします。
6	subjectAltName	FALSE	dnsNamesが設定される場合があります。
7	basicConstraints	-	CA= FALSEとします。
8	cRLDistributionPoints	FALSE	distributionPoint= http://crl.globalsign.net/ediRootCAsha2g3.crlとします。
9	authorityInfoAccess	-	使用しません。

表 10 利用者のクライアント証明書の拡張領域

No.	フィールド	クリティカル	仕様
1	authorityKeyIdentifier	FALSE	keyIdentifier=SHA-1 160 bits Hashとして値を設定します。
2	subjectKeyIdntifier	FALSE	設定します。
3	keyUsage	TRUE	digitalSignature、keyEncipherment、dataEnciphermentとします。
4	extendedKeyUsage	-	使用しません。
5	certificatePolicies	FALSE	PolicyIdentifier=1.3.6.1.4.1.4146.1.80 とします。 PolicyQualifierInfo の policyQualifierID は CPSuri、qualifierは https://jp.globalsign.com/repository/ とします。
6	subjectAltName	FALSE	rfc822Nameが設定される場合があります。
7	basicConstraints	FALSE	CA= FALSEとします。
8	cRLDistributionPoints	FALSE	distributionPoint=http://crl.globalsign.net/ediRootCAsha2g3.crlとします。
9	authorityInfoAccess	-	使用しません。

7.1.3 アルゴリズムオブジェクト識別子

本項では、証明書への署名形式と証明書で証明される公開鍵の形式を規定します。
基本領域の signature フィールドには SHA256 with RSA encryption（1.2.840.113549.1.1.11)が設定されます。

7.1.4 名前の形式

GlobalSign CA および利用者の名称は「3.1.2 名前が意味を持つことの必要性」の内容に従います。

7.1.5 名前制約（nameConstraintsフィールド）
使用しません。

7.1.6 証明書ポリシーのオブジェクト識別子（certificatePoliciesフィールドの一部）
証明書ポリシーのオブジェクト識別子は以下の通りです。

表 11　ポリシー OID

SSL サーバ証明書	1.3.6.1.4.1.4146.1.81
クライアント証明書	1.3.6.1.4.1.4146.1.80

7.1.7 ポリシー制約拡張（policyConstraintsフィールド）
使用しません。

7.1.8 ポリシー修飾子の構文および意味（certificatePoliciesフィールドの一部）
規定しません。

7.1.9 クリティカルな証明書ポリシー拡張に対する処理の意味
GlobalSign CA は、GlobalSign 証明書のなかで、以下のようにクリティカル拡張使っています。

- keyUsage を「6.1.7 鍵用途の目的」の通りに指定しています。
- basicConstraints として、証明書が CA 用か否か、および正の場合 GlobalSign ルート階層の中での何番目かを示しています。

7.2 CRL プロファイル
GlobalSign CA が発行する利用者証明書の CRL は次のフォーマットを満たします。

表 12 CRLプロファイル

No.	領域名	フィールド	クリティカル	仕様
1	CRL基本領域	version		バージョン2を利用
2		signature		sha1withRSAEncryptionまたは sha256withRSAEncryption
3		issuer		CRLを発行する認証局の名称が記載される（証明書を発行した認証局のみ）
4		thisUpdate		CRL発行日時

5		nextUpdate		thisUpdateより10日以内
6		revokedCertificates		
7		userCertificate		失効した証明書のシリアル番号
8		revocationDate		失効した証明書の日時
9		crlEntryExtensions (No.11~No.14)		使用しません。
10		crlExtensions (No.15~20)		
11	CRLエントリ拡張領域	reasonCode	-	使用しません。
12		holdInstructionCode	-	使用しません。
13		invalidityDate	-	使用しません。
14		certificateIssuer	-	使用しません。
15	CRL拡張領域	authorityKeyIdentifier	FALSE	keyIdentifier=SHA-1 160 bits Hashとして値を設定します。
16		issuerAltName	FALSE	使用しません。
17		cRLNumber	FALSE	設定します。
18		deltaCRLIndicator	-	使用しません。
19		issueingDistributionPoint	FALSE	使用しません。
20		freshesCRL	-	-

*No.6 から No.9 までの値は失効された証明書ごとの情報が記載されます。

7.3 OCSP プロファイル

規定しません。

8. 準拠性監査とその他の評価

8.1 監査の頻度あるいは条件

GlobalSign は、取得する認定スキームの要件に現在準拠しており、また今後も準拠性を維持します。GlobalSign が、認定機関に規定された要件に適合しているかどうかは、かかる認定機関により、直接調査されます。

GlobalSign は、CP および本 CPS に準拠して業務を行っていることを確実にするために、必要に

応じて内部監査を行います。利用者の識別および書類の審査を行う業務については少なくとも1年に1度以上の内部監査を行います。また、GlobalSignは、認定機関からの監査を受け入れます。
GlobalSignは、内部監査の手続きを定めますが、一般には公開しません。

8.2 監査人の要件
内部監査は、GlobalSign 自身か、または GlobalSign の代理人が実施します。監査人は、監査に関する知識を有し、かつ認証業務に関する知識を有していなければなりません。

8.2.1 業務委託
GlobalSign は、証明書サービスの運用のために使用した委託業者がある場合、その業務遂行責任を負います。GlobalSignは、証明書ライフサイクルについて最終責任を持ちます。GlobalSignは、本CPSに免責と責任の制限を明記します。

8.3 監査人と被監査人の関係
GlobalSign、または委託業者等、監査を受ける者と同じ組織に所属する者を監査人に任命する場合は、監査対象業務の運用に直接携わっている者を任命しません。

8.4 監査の対象
監査は、以下に対して実施されます（これらに限定しません）。
- CP への適合性
- 本 CPS に定められているサービスレベルへの適合性
- GlobalSign の内部方針、手続き文書
- 発行業務、更新業務、失効業務
- 物理的基盤の管理
- 関連する法律の厳守
- 監査ログ、関連書類の検査
- 上記条件の順守失敗の原因

8.5 監査指摘事項への対応
監査の結果、GlobalSign の業務が本ポリシーに反していることが判明した場合は、GlobalSign はかかる事項の是正をただちに行います。また、かかる是正処置について認定機関に報告を行います。それ以外の監査指摘事項については GlobalSign の判断により必要な是正処置を行います。

8.6 監査結果の開示
GlobalSign は監査結果を外部に公開しません。ただし、認定機関が適合性に関する照会を求められた場合は、監査指摘事項の有無やその対応状況について報告を行います。

9. 他の業務上の問題、および法的問題
9.1 料金
9.1.1 証明書の発行および証明書の更新に関わる手数料
GlobalSignは、利用者証明書の発行および更新について、料金を定め、GlobalSignのウェブサイ

トに掲示します。

9.1.2　証明書の参照に関わる手数料
GlobalSign は、GlobalSign 証明書を依拠当事者等が GlobalSign リポジトリ等より参照することについて、手数料を課しません。

9.1.3　失効情報の参照に関わる手数料
GlobalSign は、GlobalSign 証明書の証明書ステータス情報を依拠当事者等が GlobalSign リポジトリ等より参照することについて、手数料を課しません。

9.1.4　他のサービスに関する利用料金
規定しません。

9.1.5　返金制度
GlobalSign は、返金申請を GlobalSign 指定の方法で受け付けます。GlobalSign は、GlobalSign が提示した返金制度の枠内での返金申請のみを、正当な返金申請とみなし、これを受け付け、承諾し、返金する権利を持ちます。

9.2 財務的責任
9.2.1　保険の範囲
GlobalSign は、現状有姿でサービスを提供し、保険は提供しません。

9.2.2　他の資産
GlobalSign は、本 CPS に定められた責任を十全に果たしうる資産を維持します。

9.2.3　拡張された保証の範囲
規定しません。

9.3 業務情報の機密性
9.3.1　機密として扱う情報の範囲
GlobalSign は、以下を機密情報として取り扱います。

- 利用者を識別できる、GlobalSign 証明書に含まれない個人情報
- 証明書ステータス情報に公開されない、GlobalSign 証明書の失効理由
- 監査ログ
- GlobalSign のサービスに関連する通信
- 秘密鍵

機密情報は、利用者にも依拠当事者にも開示しません。GlobalSign は、以下のいずれかからの開示請求であると認証し、または正当性の判断をした場合にのみ、かかる関係者に対し機密情報を開示します。

- かかる情報を機密に取り扱うべく GlobalSign が義務を負う当事者本人からの開示請求
- 裁判所の命令

GlobalSign は、かかる開示請求に対する手続について、事務手数料を請求することがあります。また、そのような場合には、GlobalSign は、機密情報の開示を請求し、機密情報を受け取る者は、要求した目的でのみかかる情報を使用し、情報を危殆化から保護し、その他の用途での使用や第三者への開示を行わないものとして開示請求を承諾します。

9.3.2 機密として扱わない情報

GlobalSign は、以下を機密情報として取り扱いません。

- 本 CPS
- 利用規約
- 依拠当事者規約
- 自身が発行した GlobalSign 証明書、および GlobalSign 証明書に記載される情報
- CRL、および CRL に記載される情報

GlobalSign は、機密でない情報の開示手続きを適切に管理します。

9.3.3 機密として扱う情報を保護する責任

GlobalSign は、以下の機密情報を含む通信を暗号化します。

- GlobalSign CA と GlobalSign RA の間の通信接続
- GlobalSign 証明書および、証明書ステータス情報を配布する際のセッション

GlobalSign は、認証業務を実施する上で入手した情報を、認証業務を実施する上で必要とする場合を除いて、利用しません。

9.4 個人情報のプライバシー保護

GlobalSign は、GlobalSign リポジトリで参照できるプライバシーポリシーを厳守し、ウェブサイト経由で GlobalSign 証明書を申請する際の個人情報の保護に、プライバシーポリシーを適用します。
このプライバシーポリシーは、平成 16 年 8 月 31 日総務省告示第 695 号「電気通信事業における個人情報保護に関するガイドライン」、および GlobalSign 内部のセキュリティ規定にもとづいています。

9.5 知的財産権

GlobalSign は、ウェブサイト、GlobalSign 証明書、本 CPS を含む、GlobalSign が発行した公布物、および他者に明示的に所有権を譲渡していない自社製品とサービスに関する知的財産権を保持します。

GlobalSign は、GlobalSign 証明書を完全な形で複製し配布するのであれば、非独占的で、ロイヤルティを支払わない形での GlobalSign 証明書の複製と配布を許可します。ただし、誰でもアクセスできるリポジトリやディレクトリで GlobalSign 証明書を複製し配布するには、GlobalSign の明示的な書面による許可を必要とします。GlobalSign は、この制限により、GlobalSign 証明書に記載される個人情報が利用者の承認なく複製されることを防止します。

9.6 表明保証

9.6.1 GlobalSignの表明保証

9.6.1.1 リポジトリとウェブサイトの条件

利用者および依拠当事者を含む、GlobalSign のウェブサイトと GlobalSign リポジトリにアクセスする者は、本 CPS に定められた条件に同意しなければなりません。本 CPS に定められた条件への同意は、GlobalSign 証明書サービスや証明書ステータス情報を利用する、あるいは依拠することで表明します。
GlobalSign リポジトリでは、「2.2 証明情報の公開」に定めるものを公開します。
GlobalSign は、「5.5.2 アーカイブ保持期間」に定める期間、GlobalSign リポジトリで公開したものを保持します。

9.6.1.2 自己責任での信頼

利用者および依拠当事者を含む、GlobalSign のウェブサイトと GlobalSign リポジトリにアクセスする者は、そこで GlobalSign 証明書に記載される情報が信頼できるかを判断するために必要な情報を収集し、自己の責任において情報を信頼すべきです。
GlobalSign は、GlobalSign リポジトリの情報を公開する内部的な手続きに則り、証明書ステータス情報と GlobalSign リポジトリを更新します。
GlobalSign リポジトリとウェブサイトの条件に同意できない場合には、GlobalSign 証明書サービスに依拠し、または利用してはなりません。

9.6.1.3 正確な情報の提供

GlobalSign は、GlobalSign リポジトリにアクセスする者に、正確かつ最新の情報を提供することを保証するよう努めます。しかし、GlobalSign が負うべき責任は、本 CPS に定めたものを越えません。

9.6.1.4 GlobalSign CAの義務

GlobalSign CA は、以下を保証します。

- GlobalSign リポジトリに公開される最新の本 CPS に従うこと
- GlobalSign リポジトリとウェブサイトの適正な運用を含む、公開鍵暗号基盤にもとづく証明書サービスを提供すること
- GlobalSign 自身の鍵生成、秘密鍵の保護の手続きを含む、認証局として信頼に足る仕組みを堅持すること
- GlobalSign CA の秘密鍵が危殆化した場合、即座に公表すること
- GlobalSign 証明書の申請手続を提供し、審査検証手続を実施すること
- 本 CPS に従った GlobalSign 証明書の発行と、本 CPS で表明している義務の遵守
- GlobalSign RA が承認した有効な証明書失効要求の受領にもとづいた、本 CPS に従った GlobalSign 証明書の失効手続きを実施すること
- 本 CPS に従って期限切れの GlobalSign 証明書に対する更新サービスを提供すること
- 本 CPS に従って証明書ステータス情報を提供すること
- GlobalSign リポジトリでの証明書ステータス情報の公開により、依拠当事者へ GlobalSign 証明書の失効を通知すること
- 利用規約に従ったサービスを提供すること

しかしながら、上述の項への違反が直接の原因となる、立証される被害に対し GlobalSign が負うべき補償はないものとします。
GlobalSign CA は、準拠法が許す範囲内で、以下について法的義務を負いません。

- 本 CPS で定めた以外の GlobalSign 証明書の使用に関すること

- 通信データが改ざんされたことに起因すること
- GlobalSign 証明書に関連する通信に使用された、GlobalSign の責任のもとで運用されていない機器の設定の誤り、不適正使用に起因すること
- GlobalSign 証明書にひもづく秘密鍵の危殆化
- GlobalSign 証明書にひもづく秘密鍵を守る PIN コードが紛失、開示、不正使用されたこと、およびそれに起因すること
- 本人識別に使用された情報、公開鍵のデータを含み、利用者から誤情報、不完全情報を提出されたことに起因すること
- 利用者が GlobalSign 証明書に関して誤って申請を提出したことに起因すること
- 自然災害に起因すること
- GlobalSign 証明書を使用したことに起因すること
- 依拠当事者が GlobalSign 証明書を信頼したことに起因すること

GlobalSign は、上述の他に記述すべき義務はないと認識しています。

9.6.1.5 GlobalSign RAの義務

GlobalSign RA は、以下を保証します。

- 信頼性のあるシステムを使用し、GlobalSign RA の業務に使用する鍵ペアを安全に生成すること
- GlobalSign CA に、正確な情報を提出すること
- GlobalSign CA に提出した公開鍵が、正当で真正であること
- GlobalSign CA に要求する GlobalSign 証明書のために、新しい、安全な鍵ペアが生成、使用されていること
- 本 CPS に従って、GlobalSign 証明書の申請を受領すること
- 本 CPS と GlobalSign が内部に定める手続に従って、GlobalSign 証明書の発行要求、更新要求、失効要求を受領し、審査検証を実施し、GlobalSign CA に提出すること
- GlobalSign CA との接続に、電子証明書を用いた認証を使用すること

9.6.2 利用者の表明保証

利用者は、以下の事項を実施又は遵守することを保証しなければなりません。

- 「4.5.1 利用者による秘密鍵、および証明書の使用」に定める義務に同意すること。

GlobalSignは、利用者が上述の項目を認識し、条件に拘束されることを確実にするため、利用規約に明記します。

9.6.3 依拠当事者の表明保証

9.6.3.1 依拠当事者の義務

依拠当事者は、以下の事項を実施又は遵守することを保証しなければなりません。

- 「4.5.2 依拠当事者による公開鍵､および証明書の使用」に定める義務に同意すること。

依拠当事者は、GlobalSign 証明書を信頼することの妥当性を自己の責任において確実としておかなければなりません。

9.6.3.2 依拠当事者の義務の伝達

GlobalSign は、GlobalSign 証明書の信頼性の検証を行えるよう、依拠当事者に証明書ステータス

情報へのアクセスに制限を行いません。また、GlobalSign は、依拠当事者が GlobalSign リポジトリに公開される本 CPS、依拠当事者規約および関連ポリシーのすべての条件に同意しその義務に拘束されるために依拠当事者に GlobalSign との直接の契約締結を条件づけることはさし控えます。

しかしながら、依拠当事者が使用する GlobalSign 証明書および証明書ステータス情報は、CP と本 CPS に導き出される GlobalSign ポリシーに定める条件が暗黙のうちに司るものであり、GlobalSign は、依拠当事者が、GlobalSign 証明書を検証し、その信頼を確立する目的で証明書ステータス情報に問い合わせる都度、本 CPS の義務と条件に拘束されるものであることを、ここに通告します。

9.6.3.3 利用者の依拠当事者に対する義務

利用者は、本 CPS に定める利用者の義務に限らず、GlobalSign 証明書内の情報を妥当に信頼する第三者に対し、その不実表示に関して法的責任を負わなければなりません。

9.6.4 参照により GlobalSign証明書に組み込まれる情報

GlobalSign は、発行するすべての GlobalSign 証明書に、以下の情報を参照により組み込みます。

- 本 CPS の条件条項
- CP
- X.509 標準の必須要素
- X.509 標準の必須ではない、カスタマイズ要素
- 証明書フィールドで、そうあるべきと規定されたその他の情報

参照により組み込まれる情報には、URL や OID 等のポインタを使用します。

9.7 無保証

9.7.1 保証の制限

GlobalSign は、「9.6.1 GlobalSign の表明保証」に定める内容以上の保証は行いません。また、以下についても保証は行いません。

- 本 CPS に定める製品について定義された、GlobalSign 証明書に含まれる審査検証されない情報の正確性
- 本 CPS に定める製品について定義されていない、GlobalSign 証明書に含まれる情報の正確性
- 検証やテストの用途で発行された GlobalSign 証明書に含まれる情報の正確性

また、「9.16.5 不可抗力条項」の規定に従って、免責される保証事項があります。

9.7.2 保証から除外される損害

詐欺行為、意図的な違法行為を除き、いかなる場合も、GlobalSign は以下について責任を負いません。

- 利益の損失
- データの損失
- GlobalSign 証明書または電子署名の使用、配布、ライセンス、および実行／不実行から生じるあらゆる間接的損害、派生的損害、懲罰的損害
- 本 CPS に定める通りに行われた取引およびサービス提供

- 検証やテストの用途で発行されたものを除く GlobalSign 証明書に含まれる、審査検証された情報に信頼した結果負った損害を除く、その他のあらゆる損害
- 利用者の詐欺行為、意図的な違法行為の結果として審査検証された情報が誤っていた場合に生じた賠償責任

9.8 責任の制限

GlobalSign の責任は、CP および本 CPS に定められた要件を果たさなかった場合に限定され、また、補償に際して GlobalSign が支払うべき金額は、いかなる場合にも、利用者が GlobalSign 証明書の利用のために GlobalSign に支払った料金を超えないものとします。
GlobalSign 証明書は、本項に定める金額と同等かそれよりも低い金額の補償に同意できる場合にのみ信頼されるべきことをここに通知します。

9.9 補償

CP および本 CPS に定められた責任を果たさなかったことにより、GlobalSign が関係者に損害を与えた場合は、GlobalSign は「9.8 責任の制限」に定める責任を上限として補償する責任を負います。
ただし、GlobalSign の責に帰さない理由により生じた損害については、GlobalSign は賠償責任を負いません。

また、法の許す範囲で、利用者は、補償、損失、損害、訴訟、弁護士費用、その他の適正な経費等、利用者の以下の行為または不作為の結果生じる損害から GlobalSign を保護し、補償することに同意しなければなりません。

- 利用者の秘密鍵および活性化データの保護義務の不履行
- 信頼性のあるシステムを使用する義務の不履行
- GlobalSign 証明書を、受諾前に適切に検証すること

9.10 有効期間と終了

9.10.1 有効期間

本 CPS は、GlobalSign リポジトリに、最新のものとして掲示されている間、GlobalSign により効力があると通知されていると見なされ、有効とされます。

9.10.2 終了

本 CPS は、GlobalSign リポジトリに、最新でないものとして掲示するか、掲示を削除することにより、GlobalSign により効力がなくなったものと通知されていると見なされ、無効とされます。

9.10.3 終了の効果と効果継続

本 CPS が無効化された場合であっても、「9.3 業務情報の機密性」、「9.4 個人情報のプライバシー保護」および「9.5 知的財産権」に関する規定は効力を継続するものとします。

9.11 関係者間の個別通知と連絡

GlobalSign は、本 CPS に関する通知を、書面、メールフォーム、電子署名された電子メッセー

ジ、その他当社が指定したシステムを使用した通信を通じて受け取ります。
GlobalSign からのかかる通信の受領確認を受け取って初めて、通知の送信者は情報伝達ができたと見なしてよいものとします。
通知の送信者は、GlobalSign からの受領確認を通常 20 営業日以内に受け取ります。万一、GlobalSign からのかかる通信の受領確認が送付されてこない場合には、通知の送信者は、配達記録郵便か受取証明郵便で、書面による通知を本 CPS の初めの章に記載した GlobalSign の窓口に宛てに送付します。また、郵送・通信にかかる費用は通知の送信者が負担しなければなりません。

9.12 改訂

9.12.1 改訂手続き

最新版はすべての既存の、そしてこれからの利用者に対して拘束力をもちます。最新版の CPS が、すべての利用者と以前のバージョンの CPS の下で発行された GlobalSign 証明書を信頼する当事者を含むすべての当事者を拘束します。

変更に影響される利用者は、希望するならば公表から 15 日以内に GlobalSign に意見を提出します。利用者と監督当局だけが変更への異議を提出することができます。利用者ではない依拠当事者には異議を提出する権利はなく、かかる意見提出はなかったものと見なされます。

本CPSの改訂は、新しいバージョン番号を通じて表示されます。新しい版は、小数点1桁の整数によって示されます。マイナーチェンジは、小数点2桁の整数によって示されます。マイナーチェンジには以下を含みます。

- 小さな編集上の修正
- 詳細な連絡先の変更

GlobalSign はウェブサイトで CPS の少なくとも最新の 2 版を公開します。

9.12.2 通知方法、および期間

改訂された本CPSは、GlobalSignリポジトリに掲載された段階で有効化されます。
本 CPS が改訂された事実は、例えば特定権限をもつ監査役等、かかる最新版を受領する法的義務を負う当事者に通知されます。

9.12.3 オブジェクト識別子が変更されなければならない場合

規定しません。

9.13 紛争解決手続

9.13.1 手続き

紛争の当事者は、裁判所が下す判決を含むなんらかの紛争解決制度、またはなんらかのタイプの（例外なくミニ・トライアル、仲裁裁判、拘束力がある専門家のアドバイス、協定のモニタリング、典型的な専門家のアドバイス等を含む）代替的な紛争解決制度に訴える前に、GlobalSign に紛争解決を模索するために通知しなければなりません。

GlobalSign は、紛争の通知を受領したら、20 営業日以内に、GlobalSign の経営管理者に紛争処

理の方針について助言する争議委員会を召集します。争議委員会は弁護士、データ保護の責任者、GlobalSign の業務管理者、セキュリティオフィサー等のメンバーで構成され、その決議で GlobalSign の幹部経営管理者への調停案を提出します。その後、GlobalSign の幹部経営管理者は、提出された調停案を当事者に伝達します。

9.13.2 仲裁

紛争が、通知を受けてから 20 営業日以内に解決しなかった場合は、本 CPS に従い、紛争の仲裁を受けることとします。調停者は 3 人とし、各当事者が 1 人ずつ提案し、両当事者合意の 3 人目を選ぶこととします。紛争の調停は、東京地方裁判所を第一審の専属的合意管轄裁判所とし、調停者が関連する費用を決めることとします。紛争の通知は、本 CPS の初めの章に記載した GlobalSign の窓口に宛てに送付されなければなりません。

9.14 準拠法

本 CPS の準拠法は、日本国の法令とします。

9.15 適用法の遵守

本 CPS の運用にあたり、日本国の法令に抵触する可能性がある場合は、日本国の法令が優先されます。

9.16 雑則

9.16.1 完全合意条項

本CPSは、口頭で変更、追加、削除、または終了させることはできません。

9.16.2 権利譲渡条項

関係者は、本CPSに定める権利義務を、如何なる担保にも供してはなりません。なお、本CPSに反しない限りにおいて、GlobalSignは業務の一部を第三者に委託することがあります。

9.16.3 分離条項

本 CPS の責任の制限の条項を含むいずれかの規定が無効であるか、あるいは法的強制力がないことが分かった場合にも、本 CPS の他の条項は当事者の本来の意図を損なわず有効性は失われないものとします。

9.16.4 強制執行条項

規定しません。

9.16.5 不可抗力条項

地震、洪水、火災、暴風、天変地異、疫病の蔓延、戦争、武力衝突、テロ、ストライキ、ロックアウト、ボイコットにより、本CPSに定める義務の履行が停止、中断または遅延した場合、いずれの当事者も本CPSの不履行とはみなされず、これによる責任を他の当事者に対し負いません。

9.16.6 存続

本 9 章「他の業務上の問題、および法的問題」に記載される責任と制限事項は、本 CPS の終了後も存続します。

9.17　その他の条項

本CPSは、明示的か黙示的かにかかわらず、当事者の後継者遺言執行者、相続人、代理人、管財人、および譲受人に対しても拘束力があります。
本CPSで詳述された権利義務は、本CPSの業務の終了の条項に従って譲渡が行われ、譲渡の時点で譲渡する当事者が他の当事者に対して負ういかなる債務または義務の更改に影響しないことを条件に、合併、議決権株式の譲渡の結果を含む）法の運用、あるいはその他の理由で、当事者から譲渡されることがあります

10. 定義語

CP
経済産業省流通システム標準化事業のウェブサイトから入手可能な流通業界共通認証局証明書ポリシー。

CPS
GlobalSign流通EDI認証局の認証業務運用規定。

証明書失効リスト（CRL）
認証局によって発行・電子署名された失効証明書のリスト。

GlobalSign
GMOグローバルサイン株式会社。

GlobalSign CA
GlobalSign流通EDI認証局。GlobalSign CA秘密鍵の管理を行い、利用者からのGlobalSign証明書の発行や失効に関わる申請を審査し、GlobalSign証明書を発行、失効し、証明書ステータス情報を管理するエンティティ。

GlobalSign RA
GlobalSign流通EDI認証局の機能の一部であり、利用者から提出した書類等を確認し、GlobalSign証明書の発行や失効に関わる審査を行い、GlobalSign証明書の発行および失効を要求するエンティティ。

GlobalSign証明書サービス
GMOグローバルサイン株式会社によるGlobalSign流通EDI認証局から発行される電子証明書の発行と管理にかかわるサービス。

GlobalSignリポジトリ
https://edi.globalsign.com/repository/

公開鍵基盤（PKI）
証明書にもとづく公開鍵暗号システムの実装および業務をサポートするアーキテクチャ、機構、技術、実践、及び手順。

依拠当事者
電子署名された文書を受け取った者で，かかる文書上の電子署名を検証するにあたって証明書を信頼した者。証明書に記載された情報を信頼した証明書の受取人も含む。

証明書署名要求（CSR）
証明書申請の機械可読フォーマット。

危殆化
証明書に付随する秘密鍵が現に不正に開示され，損耗し，管理不能に陥り，または使用されること，またはその疑いが生ずること。

鍵ペア
２つの数学的に関連する鍵で、次のような属性を有するものをいう。(i) 一方の鍵で暗号化されたメッセージは他方の鍵で復号化することができる。(ii) 一方の鍵を知っていても、そこから他方の鍵を導くことは計算上、事実上不可能である。

秘密鍵
鍵ペアの一方で、電子署名を生成するために使用される鍵。この鍵は、秘密裡に保管されなければならない。

公開鍵
鍵ペアの一方で、電子署名を検証するために使用される鍵。公開鍵は、鍵ペアの保有者から電子署名付きのメッセージを受け取ったいずれの者も自由に利用することができる。

略語

API:	Application Program Interface
CA:	Certification Authority
CP:	Certificate Policy
CPS:	Certification Practice Statement
EDI:	Electronic Data Interchange
EPC:	Electronic Product Code
FQDN:	Fully Qualified Domain Name
GDS:	Global Data Synchronization
IETF:	Internet Engineering Task Force
ISO:	International Standards organization
ITU:	International Telecommunications Union
LRA:	Local Registration Authority
OCSP:	Online Certificate Status Protocol
PKI:	Public Key Infrastructure
RA:	Registration Authority
RFC:	Request for Comments