

## グローバルサイン電子証明書サービス利用約款

グローバルサイン電子証明書サービス利用約款（以下「本利用約款」という）は、GMO グローバルサイン株式会社（以下「グローバルサイン」又は「当社」という）が提供する電子証明書を利用者（以下「利用者」という）がご利用になるための利用条件を定めたものです。電子証明書の利用をご希望の利用者は、サービスの利用に先立ち、本利用約款をお読みください。電子証明書を申し込むことにより、利用者は本利用約款の当事者となり、本利用約款の条項に拘束されるものとします。本利用約款に同意せず、料金の全額返金を希望する場合は、証明書利用可能日から7日以内に解約手続きを行なってください。また本利用約款の解釈につき不明点がある場合は、[legal@globalsign.com](mailto:legal@globalsign.com)に電子メールでお問い合わせください。

本利用約款は、電子証明書の申請日をもって当社と申請者若しくは電子証明書を受領する利用者との間で成立します。

貴社が調達当事者であり、利用者の正式な代理人として、証明書又は関連するホステッド CA サービスの申請又は再販を行っている場合、貴社は、GlobalSign 及び依頼当事者に対し、貴社が本利用者に代わって本契約を締結する権限を取得しており、かつ貴社が本契約を遵守し、また、利用者に本契約を遵守させることを、表明し保証するものとします。

利用者が調達当事者を通じて本サービスを調達又は使用する場合、利用者は、ここに、当該調達当事者が本サービスのために利用者に代わって行動することについて許可したことを、表明し保証するものとします。調達当事者が本サービスを利用者に提供又は再販売することを許可することにより、すなわち利用者は、本契約が利用者自身のサービス利用に関するものであることをここに確認するものとします。利用者が本契約の条項に同意しない場合、利用者は、適用される GlobalSign の本サービスを購入又は使用することはできません。

### 第1条（定義）

以下のポリシー及び関連するガイドラインは、参照により本利用約款に組み込まれます。

- グローバルサイン認証業務運用規程（CPS）
- グローバルサインワランティーポリシー
- グローバルサイン支払ポリシー

上記のグローバルサインの最新版の文書は <https://www.globalsign.com/en/repository/> 及び <https://www.globalsign.com/en/company/corporate-policies> に掲載されています。

（日本語版は <https://jp.globalsign.com/repository/>）

CA/Browser Forum の最新文書は <https://cabforum.org/baseline-requirements-documents/> に掲載されています。

本利用約款中で使われている用語は、以下の意味を有するものとします。

**関連企業**：企業、パートナー企業、合弁企業、或いはその他組織の総称であり、これ以外の他の組織、或いは代理人、部局、行政下部組織、或いは政府組織の直接支配下において運営される組織等を支配下におくか、逆にこれらの支配下におかれているところのもの、或いはこれらとその他の組織との共通支配下におかれているところのもの。

**申請者**：証明書を申請する、又は更新しようとする個人又は組織。証明書が発行されれば、個人又は組織は利用者と呼ばれる。デバイスに対し発行される証明書については、デバイス自体が証明書の申請データを送信している場合であっても、証明書に名称の記載された

デバイスを管理運用するエンティティ（個人又は組織。以後総称して「エンティティ」と呼ぶことがある）がこの証明書の申請者である。

**アプリケーションソフトウェアサプライヤー**：ルート証明書を搭載し証明書を表示・使用するブラウザ又はその他の依拠当事者のアプリケーションソフトウェアの提供者。

**機関情報アクセス**：どのように証明書の発行者の情報やサービスにアクセスするかを示した証明書の拡張領域。

**CA/ブラウザフォーラム**：認証局やウェブブラウザ等のアプリケーションソフトウェア提供企業等を代表する専門家で構成される業界団体。詳細は <https://cabforum.org/> から入手可能。

**証明書**：デジタル署名によってある公開鍵とある本人確認情報との間を紐づける電子文書。

**証明書受益者**：本証明書の利用約款又は利用条件の当事者である利用者、GlobalSign がアプリケーションソフトウェアサプライヤーにより配布されるソフトウェアにルート証明書を含める契約を締結した全てのアプリケーションソフトウェアサプライヤー、及び有効な証明書に合理的に依拠する全ての依拠当事者。

**電子証明書管理者**：電子証明書のライフサイクル管理に責任を負う組織又は個人。これには、利用者自身である場合と、そうでない場合とがある。

**証明書申請**：証明書の発行を要求するために行われる CA/Browser Forum Baseline Requirements for the Issuance of Publicly-Trusted Certificates（以下「Baseline Requirements」）10.2 項に規定される申請行為。

**証明書申請者**：申請権限者から明示的に権限を付与された申請者の代表、又は申請権限者を代理して証明書申請を準備し提出する第三者（ISP（インターネットサービスプロバイダ）やホスティング事業者等。MSSL（SSL マネージドサービス）や ePKI（マネージド PKI Lite）等のマネージド・サービスにおいては、証明書利用者はこのサービスの機能を通じて証明書申請者を事前に承認することができる。

**証明書失効リスト（「CRL」）**：証明書を発行した認証局が作成しデジタル署名した、定期的に更新されタイムスタンプが付与されている、失効した証明書の一覧。

**認証局（「CA」）**：証明書の生成、発行、失効、管理に責任を負う組織。この用語は、ルート認証局、下位認証局のどちらを表す場合にも使用される。グローバルサイン又はグローバルサインによって「サブジェクト」に証明書を発行することが認定されているエンティティのこと。グローバルサインは、本契約に基づく申請者の認証局である。

**電子署名**：メッセージを非対称暗号方式とハッシュ関数を用いてエンコードすること。これによってオリジナルメッセージと署名者の公開鍵を所有する人物が、署名者の公開鍵と対になる秘密鍵が使用されてエンコードが行われたかどうか、及びオリジナルメッセージがエンコード後に書き換えられたかどうかを、正確に判断することができる。電子的に署名されたものというのは、電子署名が付加された電子データを指すものとする。

**ドメイン名**：ドメインネームシステムにおいて単一のノードに与えられた名称。

**ドメイン名の登録者**：「ドメイン名の所有者」とも呼ばれるが、より正確には、WHOIS やレジストラに「登録者」として登録されている個人又は組織といった、ドメイン名の使用について管理権限を有する主体としてレジストラに登録されたその個人又は組織を指す。

**ドメイン名のレジストラ**：以下に列挙する者の援助又は契約に基づきドメイン名の登録業

務を行う個人又は組織をいう。(1)Internet Corporation for Assigned Names and Numbers(ICANN)、(2)各国のドメイン名管理当局(登記所)、又は(3)Network Information Center(その関連会社、契約業者、代理人、相続人、権利継承者を含む)。

**ドメイン名システム(Domain Name System, DNS)**：ドメイン名をIPアドレスに変換するインターネットサービス。

**eIDAS 規則**：欧州議会及び理事会の規則(EU)第910/2014号。2014年7月23日、欧州内市場における電子取引の電子本人確認及びトラストサービスに関する規則。これに伴い、指令1999/93/ECは廃止とされた。

**完全修飾ドメイン名(FQDN)**：ドメインネームシステム内の上位ノードに与えられる名称を含むドメイン名。

**グローバルサイン**：利用者が証明書の購入を申し込んだ以下のグローバルサイン拠点をいう。GMO GlobalSign Limited, GMO GlobalSign, Inc., GMO GlobalSign Pte. Ltd., GMO GlobalSign Certificate Services Pvt. Ltd., GMO GlobalSign Russia LLC., GMO GlobalSign Inc. (Philippines),若しくはGMOグローバルサイン株式会社をいう。

**政府機関**：政府が運営する法的機関、省、支部、その他同様の国又は行政区内の下部組織(たとえば州、県、市、郡等)。

**鍵の危殆化**：秘密鍵に対する権限を持たない人物に秘密鍵が漏えいした場合、権限を持たない人物による秘密鍵へのアクセスがあった場合、権限を持たない人物への秘密鍵の漏えいが技術に可能であった場合に、秘密鍵が危殆化したと称する。

**鍵ペア**：秘密鍵と、その対になる公開鍵。

**法人**：団体、企業、パートナー企業、自営業、信託、政府機関、その他当該国の法制度において法的地位を有する組織体。

**北米エネルギー規格委員会(NAESB)認証局認定要件**：NAESBに認定認証局として認可を受けるために認証局が準拠すべき技術的・管理要件。

**オンライン証明書ステータスプロトコル(OCSP)**：証明書に依拠するソフトウェアが当該証明書の有効性をオンラインで確認するための通信プロトコル。

**秘密鍵**：鍵ペアの一方で、所有者が秘密裏に保管し、デジタル署名の生成や公開鍵を用いて暗号化された電子データやファイルを復号化するのに用いる。

**調達当事者**：利用者にサービスを再販又は提供することをグローバルサインによって承認された法人又は事業者。

**公開鍵**：鍵ペアの一方で、対になる秘密鍵の所有者が公開される鍵をいい、その所有者が生成したデジタル署名を依拠当事者が検証するため、或いは対になる秘密鍵を用いてのみ復号が可能な暗号化データを生成するために使用するものをいう。

**適格証明書**：eIDAS規則で定義された資格要件を満たす証明書。

**適格電子署名生成デバイス(QSCD)**：電子署名生成デバイスであって、eIDAS規則の付属書IIに規定される要件を満たすもの。

**登録局(RA)**：証明書のサブジェクトの本人確認と認証に責任を負う法人であるが、但し認証局ではないため、証明書を発行したり、証明書に署名したりすることはない。登録局は証明書の申請手続き、失効手続きをサポートする。「登録局」という語がその役割や機能

を示す用語として使用される場合、それは必ずしも独立した組織体を意味するわけではなく、認証局の一部組織を表すこともある。

**依拠当事者**：有効な証明書に依拠する個人又は法人。アプリケーションソフトウェアサプライヤーは、単に当該サプライヤーが配布するソフトウェアがある証明書に関する情報を表示するというだけでは、依拠当事者とはみなされない。

**ルート証明書**：ルート認証局が発行し自己署名した証明書。ルート認証局の下位認証局に発行した証明書を検証するために使用される。

**サブジェクト**：証明書にサブジェクトとして記載される個人、デバイス、システム、設備、法人等をいう。サブジェクトは利用者であるか、若しくは、利用者の管理、運営下にあるデバイスの何れかである。

**下位認証局**：その証明書がルート認証局又は別の下位認証局に署名された認証局。

**利用者**：証明書の発行を受ける個人又は法人であり、利用約款或いは利用条件規程等により法的に拘束されるものをいう。

**疑わしいコード**：スパイウェア、マルウェア等を含む悪意のある機能や深刻な脆弱性を持つコードのこと。これには、使用者となる一般ユーザの了承を得ずにインストールされたもの、或いはその削除を困難にしてあるもの、また、そのコード作成者の意図しない方法で悪用されたり、プラットフォームの信頼性を侵害したりする可能性のあるものを含む。

**利用条件**：グローバルサイン認証業務運用規程（CPS）の要求事項に従い発行された証明書に関する安全な利用方法、かつ許可された利用方法に関する規程であり、ここでは、申請者又は利用者が認証局の関連会社である場合をいう。

**ワイルドカード証明書**：サブジェクトとして、完全修飾ドメイン名（FQDN）の一番左の欄がアスタリスク（\*）で示されたものを記載する証明書。

## 第2条（電子証明書の使用の許可）

### 第2条1項（使用権の許可）

グローバルサインは利用者に対し、発行された電子証明書に記載された有効期間（有効期間の開始日から満了日まで）、利用者がその公開鍵及び/又は秘密鍵に関連して使用する電子証明書の使用権を許諾します。

### 第2条2項（権利の制限）

利用者は適正にライセンス許諾を受けた暗号ソフトウェアを用いてのみ、電子証明書を利用するものとします。

## 第3条（グローバルサインが提供するサービス）

本利用約款を承諾の上、適用される料金の支払いの手続きを行った後、グローバルサイン又はグローバルサインが指名する第三者プロバイダーは、電子証明書の発行の時点をもって、利用者にその使用許諾を与えると共に、以下のサービス提供を開始します。

### 第3条1項（CRL、OCSP、及び証明書発行局について）

グローバルサインは、グローバルサイン CA が署名し発行した全ての電子証明書に関する電子情報をまとめ、電子上における一般の利用に供するために合理的な措置を取るものとします。これには以下の措置を含みます。

- 1) CRL 配布ポイントの記載がある電子証明書については、CRL を提供すること。
- 2) OCSP レスポンダの URL の記載がある電子証明書については、OCSP レスポンダを提供すること。
- 3) 機関情報アクセスに記載される認証局を通じて電子証明書を発行すること。但し、機器故障や通信障害など、グローバルサインの合理的な管理責任の範囲を超えた事由に起因するグローバルサインの不履行や遅延が発生した場合に関しては、本利用約款に定める義務違反とはみなされないものとします。

### 第3条2項（電子証明書の失効サービス）

グローバルサインは CPS に明記されている状況、又は利用者が本利用約款に基づく重要な義務に違反しているとの通知を受けた場合、又はその他の理由で証明書を失効させることができるものとします。

### 第3条3項（鍵の生成）

グローバルサインがトークン、PKCS12 形式ファイル或いはスキップ申込サービスなどを利用して、利用者の代理で鍵ペアを生成する場合、以下の方法により信頼性の高いシステムを利用して鍵ペアを生成するものとします。

1. 鍵ペアの生成に適したプラットフォームを利用して鍵ペアを生成し、当該秘密鍵を利用者に送付する場合には暗号化すること。
2. 電子署名に適した鍵長やアルゴリズムを利用すること。
3. コードサイニング証明書及び EV コードサイニング証明書の場合、2048 ビット未満の鍵ペアを署名することはなく、EV コードサイニング証明書の場合、署名アルゴリズムの唯一のオプションとして SHA2 を提供すること。

グローバルサインがパブリックな SSL 証明書の鍵ペアを生成することはありません。

### 第3条4項（SSL サーバ証明書のサイトシールサービス及び OCSP/CRL レスポンス）

当社は、一日に 500,000 回を上限として、申請者のウェブサイト上にグローバルサインサイトシールを表示することを許可します。シールの表示上限回数を超過した場合、当社はシールの表示を制限、或いは中止する権利を有します。

当社は OCSP レスポンダ又は CRL を通じて電子証明書の有効性の検証を可能とするサービスを年中無休(24 時間/各日)で提供します。電子証明書の有効性の検証は一日に 500,000 回を上限とし、この上限回数を超過した場合、当社は OCSP ステージングの実施を利用者に義務付ける権利を有します。

### 第3条5項（コードサイニング証明書のタイムスタンプサービス）

当社は、グローバルサインのコードサイニング証明書を使用してコードへの電子署名を行うにあたり、適正な範囲内でタイムスタンプを無償で付与するサービスを提供します。業界のベストプラクティス（業界標準）として、グローバルサインは利用者に対し、コードに電子署名する際にタイムスタンプをする事を要請します。グローバルサインはコードサイニング証明書の有効期間中にこのタイムスタンプの上限回数を設定しており、利用者の使用回数がこれを超過していると判断した場合、当該利用者へのサービス提供を中止するか、又は追加の利用料金を課金する権利を有します。

### 第3条6項（「PDF 文書署名用証明書 for Adobe CDS」のタイムスタンプサービス）

当社は、グローバルサインの「PDF 文書署名用証明書 for Adobe CDS」を使用して PDF 文書に署名を行うにあたり、タイムスタンプを有償で付与するサービスを提供します。本サービスにおけるタイムスタンプの上限回数は、証明書の申請手続きにおいて決定されます。決定されたタイムスタンプの上限回数を超過した場合、当社はサービスの提供を中止するか、又は追加の利用料金を課金する権利を有します。

### 第3条7項（「AATL 証明書」のタイムスタンプサービス）

当社は、グローバルサインの「AATL 文書署名用証明書」を使用して PDF 文書、及びマイクロソフト社製のアプリケーションソフト、“Office” 関連文書に署名を行うにあたり、タイムスタンプを有償で付与するサービスを提供する場合があります。本サービスにおけるタイムスタンプの上限回数は、証明書の申請手続きにおいて決定されます。決定されたタイムスタンプの上限回数を超過した場合、当社はサービスの提供を中止するか、又は追加の利用料金を課金する権利を有します。

## 第4条（利用者の義務と保証）

利用約款利用者及び申請者は、グローバルサインと証明書受益者に対し、以下を保証します。

### 第4条1項（データの正確性）

利用者は、証明書申請において、またそれ以外にも証明書発行に関してグローバルサインから要求があった場合、証明書申請書の名称、情報 URL、EV コードサイニング証明書における申請情報等に関して、如何なる場合も正確、完全かつ真実の情報をグローバルサイン に提供するものとします。

### 第4条2項（秘密鍵の保護）

申請者は、要求された証明書及び関連するアクティブ化データ又はデバイス（例えば、パスワードやトークン等）に含まれることになる秘密鍵を、いつ如何なる時も、これを単独の管理下におき、機密性を保持し、適切に保護するための、あらゆる合理的な措置を講じなければなりません。

コードサイン証明書に関しては、申請者又は利用者は、要求された証明書に含まれる公開鍵に対応する秘密鍵（及び関連するアクティブ化データ又は デバイス（パスワードやトークン等））を、下記の第 4.15 項に従って、常に単独で管理し、秘密を保持し、適切に保護しなければなりません。利用者は、秘密鍵を保存するデバイスを、コードサインのベストプラクティスの文書に記載されているような安全な方法で生成し、操作することを表明します。利用者は、秘密鍵を転送するために、大文字、小文字、数字、及び記号を含む 16 文字以上でランダムに生成されたパスワードを使用しなければなりません。

### 第4条3項（秘密鍵の再利用）

コードサイニング証明書に関し、申請者又は利用者は、証明書の公開鍵がコードサイニング以外の証明書に使用されているか、又は使用が予定されている場合、申請を行わないものとする。

### 第4条4項（誤用防止）

利用者は、秘密鍵を悪用から保護するために、適切なネットワーク及びセキュリティ対策をとることとします。グローバルサインは、秘密鍵への不正アクセスがある場合、事前通知を

行わずに証明書を失効します。

#### **第4条5項（電子証明書の受領と確認）**

利用者は、申請者又はその代理人が電子証明書に記載された内容が正確であることを確認するまでは、証明書を利用しないものとします。

#### **第4条6項（グローバルサインが発行する電子証明書への利用制限）**

利用者は、証明書に記載されている「subjectAltName」でアクセス可能なサーバにのみ SSL 証明書をインストールするものとし、また、適用される全ての法律、利用約款や利用条件に従った上でのみ証明書を使用することができます。

如何なる状況においても、グローバルサインが発行する証明書をフィッシング攻撃、詐欺、或いはマルウェアへの証明又は署名などの犯罪行為に使用してはなりません。

利用者は、疑わしいコードを含むソフトウェアに意図的に署名したり、受信者に誤解を招いたり、不便を生じたり、不快感を与えたりする効果のあるコンテンツ（インストール前にユーザに適切に開示されていない迷惑な機能やプログラムを含むソフトウェア、或いは商用のアンチウイルススキャンアプリケーションによって迷惑な、又は疑わしいと認識されるソフトウェアなど）を配布するために証明書を使用してはなりません。

利用者は、証明書及び関連する秘密鍵に関して、これらを疑わしいコードに署名するために証明書を使用しないということ、及び適用される全ての法律を遵守し、本利用約款に準拠する上でのみその証明書及び秘密鍵を使用するということを踏まえた上で、承認されたところの、かつ合法的な目的のためにのみ使用することとします。

##### **第4条6項1（PDF 文書署名証明書）**

PDF 文書署名用証明書については、利用者は対象文書に署名することを誰が承認したか、その承認者の情報を記載しなければなりません。

##### **第4条6項2（EV コードサイニング証明書）**

利用者は、EV コードサイニング証明書を利用する際には、以下の追加義務を承諾し、保証するものとします。

- 1) CA/ブラウザフォーラムによる「EV コードサイニング証明書ガイドライン」に定める条件に従ってのみコードに署名すること。
- 2) 適用法令に従ってのみ使用すること。
- 3) 許可された業務においてのみ使用すること。
- 4) 本利用約款に準拠してのみ使用すること。

利用者は、EV コードサイニング証明書が悪意のあるソフトウェアや重大な脆弱性を含むコードを署名するのに用いられたと認識した場合（如何なる方法であれ）、直ちにグローバルサインへ連絡しなければなりません。

##### **第4条6項3（Microsoft 社の規定）**

利用者は、証明書が悪意のあるものであるか、又は秘密鍵が危殆化したかどうか、Microsoft 社が独自に判断する可能性があることを承諾するものとします。加えて、利用者は、Microsoft 社の判断を反映するために、Microsoft 社のサービス及びアプリケーションがカスタマーエクスペリエンス（顧客体験）を改善する可能性があり、これが事前通知なく、かつ証明書の失効状況に関係なく行われうることを承諾するものとします。

#### 第4条7項（報告及び失効）

利用者は、以下の事由に該当すると判断した場合には、速やかに証明書とこれに対応する秘密鍵の利用を中止し、グローバルサインに当該電子証明書の失効を申請するものとします。

- 1) 電子証明書に記載された情報のいずれかが不正確であった場合、或いはそうなった場合。
- 2) 電子証明書に記載された公開鍵と対になる秘密鍵に関して、利用者による不正利用又は危殆化があった場合。
- 3) コードサイニング証明書について、疑わしいコードへの署名へ使用された証拠がある場合。

#### 第4条8項（証明書の使用終了）

利用者は、当該証明書の失効と同時に、証明書の公開鍵に対応する秘密鍵の使用を速やかに中止するものとします。

#### 第4条9項（対応）

利用者は、危殆化又は証明書の誤用に関するグローバルサインからの指示に対しては、48時間以内に対応するものとします。

#### 第4条10項（確認及び了解）

利用者は、グローバルサインのCPSについて評価を完了したものとします。利用者は申請者が本利用約款の利用条件に違反した場合、若しくはフィッシング攻撃、詐欺、マルウェアの頒布等、犯罪行為を可能にするような方法で証明書が使用されたとの事実をグローバルサインが把握した場合、グローバルサインが直ちに当該証明書を失効する権利を有するということを認識し、了解するものとします。

但し、Microsoft サービス及びアプリケーションにおいて使用されるEVコードサイニング証明書に関しては、たとえグローバルサインによって失効されないままでも、Microsoft社によって独自に証明書に悪意がある、若しくは脆弱性があると判断されることがあります。その場合、利用者は証明書の失効状態の如何に拘わらず、Microsoft社の判断により、関連するMicrosoftサービスやアプリケーションが通知なしに変更される可能性があることを了解するものとします。

#### 第4条11項（情報の共有）

コードサイニング証明書について、(a)証明書又は申請者が疑わしいコードの発信元として特定された場合、(b)証明書を要求した権限が検証できない場合、又は(c)証明書が利用者からの要求(たとえば、鍵の危殆化、マルウェアの発見などにより)以外によって取り消された場合、利用者は、グローバルサインがCA/Browserフォーラムを含む他のCA又は業界団体との間で、その申請者、署名されたアプリケーション、証明書、及びその周辺状況に関する情報を共有する権限があることを認識し、了解するものとします。

#### 第4条12項（業界標準への準拠）

利用者は、グローバルサインがCA/BフォーラムのBaseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, the Baseline Requirements 及び/又は the Guidelines For The Issuance And Management of Extended Validation Certificates、ブラウザのルートプログラム要件、又は他の適用可能な要件の変更に準拠するために、必要に応じて利用約款を修正できることを認識し、了解するものとします。



#### 第4条13項（SSL サーバ証明書のドメイン名に対する管理権限）

利用者は、申請する SSL サーバ証明書のサブジェクトオ尔特ネーム（サブジェクト代替名）に記載されるドメイン名、IP アドレスに対し管理権限を有することを表明保証します。利用者が何れかのドメインに関してその管理権限を喪失した場合には、利用者は第4条7項「報告及び失効」の条文に記載されている規定に従い、グローバルサインに当該事実を速やかに通知しなければなりません。

#### 第4条14項（クライアント証明書の電子メールアドレスに対する管理権限）

利用者は、申請するクライアント証明書に記載される電子メールアドレスに対し管理権限を有することを表明保証します。利用者が何れかの電子メールアドレスの管理権限を喪失した場合には、利用者は第4条7項「報告及び失効」の条文に記載されている規定に従い、グローバルサインに当該事実を速やかに通知しなければなりません。

#### 第4条15項（鍵生成及び用途）

利用者又は証明書申請者が鍵ペアの生成を行う際には、そのための信頼性の高い装置を使用しなければなりません。またその際には以下の規定も適用されます。

1. 鍵ペアは、鍵生成の目的に適合するとされるプラットフォームを使用して生成すること。また、「PDF 文書署名用証明書 for Adobe CDS」、「AATL 文書署名用証明書」、及び「EV コードサイニング証明書」では、FIPS 140-2 Level 2 に準拠していること。
2. 電子署名の目的に適合するところの鍵長及びアルゴリズムを使用すること。
3. 利用者はグローバルサインに提出する公開鍵が間違いなく自らの秘密鍵と対になるものであることを保証すること。

鍵生成をハードウェア上で行う場合は、CPS に則って、以下の規定に従うものとします。

- a. 利用者が、アクティブ化データ等を変更する等、その処理工程を保持すること。これによって HSM やトークン内に保管される秘密鍵が、組織内で唯一の証明書管理者（以下「証明書管理者」という）によってのみ、その十分な知識と明確な業務目的の下で適正に使用され得ることをより確かなものとする。
- b. 利用者が、証明書管理者に関して証明書発行のための適正なトレーニングを受けていることを確約すること。
- c. 証書管理者が、要求された認証書に含まれる公開鍵に対応する秘密鍵、及び鍵にアクセスするための関連する認証メカニズム（例えば、トークンや HSM へのパスワード）を常に単独で管理し、秘密を保持し、適切に保護するために必要な全ての合理的な措置を講じること。

コードサイニング証明書について、利用者は以下のいずれかの方法でコードサイニング証明書の秘密鍵を生成し、保護することを表明する。グローバルサインは以下の方法3より、方法1又は2を使用することを推奨します。

- i. TPM(Trusted Platform Module)鍵認証を介し、鍵ペアを生成及び保護し、かつ利用者の秘密鍵保護を文書化できる TPM。
- ii. 少なくとも FIPS 140 Level 2、Common Criteria EAL 4+、又は同等の規格に準拠していると認定されたユニットデザインのフォームファクタを持つハードウェア暗号モジュール。
- iii. SD カード又は USB トークン用のユニットデザインのフォームファクタを持つ、別の種類のハードウェアストレージトークン(FIPS 140 Level 2 又は Common Criteria

EAL 4+ に準拠しているとは限らない)。

利用者はまた、署名セッションが開始されるまで、コードサイニング証明書機能をホストするデバイスからトークンを物理的に分離しておくことを保証するものとします。

EV コードサイニング証明書に関しては、FIPS 140-2 Level 2 の要件を満たすか、それ以上の暗号モジュールで EV コードサイニング証明書の秘密鍵を生成、保存、使用する場合、利用者は次のいずれかの方法を使用しなければなりません。

- FIPS 140-2 Level 2 以上に準拠していると認定されたハードウェアセキュリティモジュール (HSM)。
- ユニットデザインのフォームファクタが USB トークン FIPS 140-2 Level 2 以上である、ハードウェアストレージトークン。

利用者は、証明書の申請期間中及び証明書のライフサイクル中はいつでも、グローバルサインの要求に応じて、証明書(要求)に関連する鍵ペアが FIPS 140-2 レベル 2(又は同等の規格)の要件を満たす暗号デバイスに保管されていることの証明を提示できなければなりません。このような証拠を提供しない場合、証明書が失効される可能性があります。

適格署名又はシール生成用デバイス(QSCD)を必要とする適格証明書の場合、利用者の秘密鍵は認証された QSCD の中で生成、保管されなければなりません。利用者は、グローバルサインによって提供、又は書面で承認された QSCD 内でのみ証明書を使用することに同意し、QSCD の認証ステータスは利用者によって監視され、変更があれば適切な措置が取られねばなりません。鍵は、電子署名(電子署名のための適格な証明書の場合)又は電子シール(電子シールのための適格な証明書の場合)にのみ使用されるものとします。

#### **第 4 条 1 6 項 (NAESB に特有の義務、(※注：北米の利用者にのみ関連))**

NAESB 証明書の利用者は、グローバルサインを通じて果たすべき、WEQ PKI 規格に関連する以下に掲げる義務に対する自らの理解を確認し承諾します。

WEQ PKI 規格に準拠する組織団体は、電力卸売産業に従事する認可事業者であることの証明を提出し NAESB EIR に登録されなければなりません。WEQ PKI 規格に規定されている認証方法を用いたアプリケーションを使用する必要があるものの、電力卸売市場への参加資格を有しない組織団体も(規制当局、大学、コンサルティング企業など)、登録が必須です。

登録された組織団体及びこれが属するコミュニティは、WEQ PKI 規格の定める全てのエンドエンティティとしての義務を履行しなければなりません。

利用者組織は、以下の WEQ PKI 規格を確認し、承認したことをグローバルサインに証明するものとします。

##### **第 4 条 1 6 項 1**

利用者は、次の各項に掲げる目的を達成するために、電気産業界におけるセキュアで非公開の電子的通信の必要性を確認し承諾します。

- 秘匿性：あるエンティティに対し、明確に受信者として意図された相手以外には誰もデータを読み取ることができないことを保証する。
- 認証：あるエンティティに対し、別のエンティティが主張する人物(組織・物)であることを証明する。
- 完全性：あるエンティティに対し、意図的であるかないかを問わず、「其処から此処まで」又は「当時から現在まで」の間にデータが改変されていないことを保証する。

- 否認防止：当事者は、取引を行ったこと、或いは電子メッセージを送信したことを否認することができない。

#### 第4条16項2

利用者は、電気再販業界が公開鍵暗号方式(公開鍵証明書を利用し、個人やコンピュータシステムをエンティティに紐づけること)を利用することについて承諾します。

#### 第4条16項3

利用者は、信頼された PKI を確立するための業界ガイドラインに関して、WEQ PKI 規格をレビューしました。

#### 第4条16項4

利用者は、業界標準に照らしてグローバルサインの CPS について評価を完了したものとします。

利用者は、該当する場合、政府機関発行の事業証明を登録し、NAESB EIR において公開されエンドエンティティが提出する利用者申請や、当該エンドエンティティに発行される電子証明書において使用される、エンティティコードを保護しなければなりません。WEQ-012 の要求事項に準拠するにあたり、電機産業界内において使用する証明書を WEQ-012 への申請以外の目的において発行する際、認定認証局は WEQ PKI 規格の規定へ準拠しなければなりません。但し、NAESB EIR にてエンドエンティティの登録を要求している、WEQ-012.12.1.9、WEQ-012-1.3.3、及び WEQ-012.1.4.3 を除きます。

また、利用者は以下の要件にも準拠しなければなりません。

1. 自分の秘密鍵を他者からのアクセスから保護すること。
2. 該当する場合、NAESB EIR において、グローバルサインを認定認証局として選定したエンティティを確認すること。
3. エンドエンティティが電子的通信を保護するために使用する電子証明書をグローバルサインが発行するため、グローバルサインとの全ての契約を締結すること。
4. グローバルサインの CPS に規定されている全てエンドエンティティの義務に準拠すること、例えば、証明書申請手続き、申請者識別証明/審査、及び証明書管理手続き等に関して。
5. 証明書管理プログラムがあり、プログラムに参加する全ての従業員がトレーニングを受けること、また、当該プログラムへ準拠していることを確認すること。証明書管理プログラムは以下を含むが、それに限定されない。
6. 証明書秘密鍵セキュリティ及び運用ポリシー
7. 証明書失効ポリシー
8. 利用者の本人確認情報を確認し(個人、役職、デバイス、もしくはアプリケーション等)、完全かつ正確な情報を証明書申請の際に提供すること。

#### 第5条 (料金)

証明書が GlobalSign の調達当事者を通じて購入された場合、利用者は利用者と調達当事者との間で合意された支払条件に従って調達当事者に支払うものとします。

利用者は、以下のことを認識し、同意するものとします。(i)利用者が適用される手数料を支払わない場合(例えば、利用者が調達当事者を通じて証明書を調達し、かつ利用者が調達当事者に適用される手数料を支払わない場合)、又は、(ii)調達当事者が、自身に適用される料金を、グローバルサインと調達当事者間の契約に従って支払わない場合、利用者が調達当事者に適用される料金を支払ったかどうかに関わらず、利用者は証明書を使用することがで

きず、グローバルサインは料金が未払いの発行済みの証明書を失効させることができます。

## 第6条（情報公開への同意）

利用者は、電子証明書を申請する際に個人情報を提供することにより、グローバルサインが(i)電子発行される証明書にその情報を組み込み、(ii)その証明書を Certificate Transparency (CT) ログに公開する、という方法でその個人情報を公開することに同意するものとします。

## 第7条（テスト証明書）

グローバルサインは、試験評価、相互運用性テスト、概念実証（「テスト証明書」）を含むがこれらに限定されない、テスト及び評価の目的で証明書の発行を提供又はサポートする場合があります。利用者は、内部の非実稼働環境で、非商用評価の一部としてのみテスト証明書を使用できます。

テスト証明書を使用する権利は、期間が制限され、利用者とグローバルサインの間の追加の契約によってさらに制限される場合があります。その場合、利用者の使用权は、指定された終了日後に終了します。グローバルサインは、独自の裁量により、いつでもテスト証明書の使用权を終了することができます。加入者はその終了に伴いテスト証明書の使用を停止するものとします。

保証の免責事項：利用者は、テスト証明書が「現状のまま」提供され、如何なる保証も行われなことを認識するものとします。適用法令で認められている最大限の範囲で、グローバルサインは、テスト証明書、利用者によるテスト証明書の使用又は使用不能、その使用の結果及び本契約に関連した商品性、特定目的への適合性、又は非侵害性の保証を含むが、これに限定されることなく、あらゆる種類の表明及び保証を明示的又は黙示的に否認します。

責任制限：グローバルサインは、過失を含め、その行為が契約、不法行為、その他の理由の如何を問わず、テスト証明書の使及びテスト証明書の使用又は不備に起因する、直接的、間接的、派生的、又は特別な損害を含むがこれらに限定されない、如何なる申し立て、要求、又は損害についても、利用者に対して責任を負わないものとします。

## 第8条（免責）

法律で認められていない範囲を除き、又は当約款で別途規定されていない限り、商品性と特定目的適合性の保証を含む、如何なる保証に関しても当社は一切の責任を負いません。

グローバルサインが CA/B フォーラムの Baseline Requirement 及び CPS に準拠して証明書を発行及び管理している限り、利用者や依頼当事者、及び如何なる第三者の証明書の利用から生じる損害に対して、当社は一切の責任を負いません。それ以外の場合、グローバルサインの利用者や依頼当事者、及び第三者への証明書利用から生じる賠償責任は証明書1枚につき1000ドル（米国ドル）を超えないものとします。但し、EV SSL 証明書又はEVコードサイン証明書に対しては、証明書1枚につき2000米国ドルを責任限度とします。上記の責任上限はグローバルサインのワランティープリシールでの規定外で修復できるものに限ります。ワランティープリシールのもとで支払われる金額は当社のそれぞれの責任上限に従うものとします。

グローバルサインは、証明書、電子署名又は本約款に規定に基づくあらゆる取引又はサービスの利用、交付、依頼、ライセンス承諾、履行或いは不履行に起因して生じる、如何なる間接的損害、偶発的損害、特殊な損害、結果的損害、又は逸失利益或いは逸失データ、その

他の損害に対しても、当社は一切の責任を負いません。

また、この免責は、電子証明書に関連する、電子署名の数、関連処理量、苦情の多少に関わらず適用されます。

## 第9条（期間及び終了）

本利用約款は次のうちのいずれか早い時点をもって終了します。

- グローバルサインから利用者に直接的又は間接的に、或いはマネージド SSL サービス又はマネージド PKI サービスを通じて発行され、かつ未だ有効期間中の証明書の満了日。
- 本利用約款の定める重要な義務に利用者が違反し、グローバルサインがその是正を求めた通知を送付した後、5日間を経過した後も違反が是正されなかったその時点。

## 第10条（契約解除の効果）

本利用約款に基づく契約関係が解除となった場合はその事由の如何を問わず、当社はその時点で有効なグローバルサインの手続きに従い、利用者の電子証明書を失効することができます。利用者の電子証明書の失効時には、利用者は、第2条に従い利用者に許諾された一切の権限を喪失します。但し、この場合でも、本利用約款の第4条、第6条、第8条及び第11条の各条項は存続し、当該条項の完全な履行のために必要な範囲において、効力を持ち続けるものとします。

## 第11条（雑則）

### 第11条1項（準拠法及び管轄裁判所）

(i) 本約款及び本約款に関連する全ての事項、請求又は紛争（不法行為による請求を含む）の解釈、構築、執行に適用される法律、及び(ii) いずれかの事項、請求又は紛争について専属的な管轄権を有する裁判所は、以下の表に記載の通りです。

請求対象となる法人	準拠法	管轄裁判所
日本	日本	日本 東京地方裁判所
中国	中国	中国 上海
英国	イングランド及びウェールズ	英国 ロンドン
ヨーロッパ	ベルギー	ベルギー ルーベン
北アメリカ、南アメリカ、ラテンアメリカ	米国ニューハンプシャー州	米国 ニューハンプシャー州 州立裁判所及び連邦裁判所
シンガポール	シンガポール	シンガポール
フィリピン	フィリピン	フィリピン マカティ市
シンガポールとフィリピンを除くアジア/パシフィック	日本	日本 東京

地域		
インド	インドの法令	インド デリー
ロシア連邦	ロシア連邦の法令	ロシア モスクワ

### 第 1 1 条 2 項（契約の拘束力）

別途定めのある場合を除き、本利用約款は、本利用約款の当事者の後継者、債権執行者、相続人、代理人、管財人等に対しても拘束力を有し、その利益に帰するための効力を生じるものとします。利用者は、本利用約款及び利用者の電子証明書のいずれも譲渡することはできません。係る譲渡又は委任の試みは無効であり、何らの効力も有しません。また、係る行為は、当社からの解除事由となり得ます。

### 第 1 1 条 3 項（完全なる合意）

本利用約款に参照される全ての文書、如何なる製品又はサービス契約、また契約者がリセラーである場合はリセラー契約、これらを含め本利用約款は両当事者の完全なる合意を構成し、書面、口頭を問わず、本利用約款締結以前にこれに関して両当事者によってなされた全ての口頭或いは文書による合意事項、承諾、交渉事項に優先するものとします。

### 第 1 1 条 4 項（分離条項）

本利用約款のいずれかの条項の規定、又はその適用が、事由の如何を問わず、一部の範囲において無効又は執行不能とされる場合でも、本利用約款の残余の部分は有効に存続し、関連する状況への適用は本利用約款の当事者の意図を合理的に有効とするために最適な解釈を行うことで対応するものとします。本利用約款の当事者は、責任の制限、保証の否認、損害の除外を規定する本利用約款の全ての条項が分離可能であり、他の条項から独立しており、そのように効力を有していることを明確に理解し、同意します。

### 第 1 1 条 5 項（通知）

利用者が本利用約款に関連して当社に通知、請求又は要求することを希望する、又はそれを求められた場合には、これを書面で行うものとします。この通知には、送達の完了が書面或いは電子メールで確認できる配達サービスを使用するか、料金前払いの内容証明郵便又は配達証明付の書留郵便にて <https://www.globalsign.com/en/company/contact> に記載されている海外拠点を含む当社のいずれかの事業所の法務部門宛に行うものとします。尚、この通知は当社に受領された時点をもって有効とみなします。

### 第 1 1 条 6 項（プライバシー：第三者機関データベースの使用）

グローバルサインは、利用者から情報を入手し利用する場合、ホームページに記載されているプライバシーポリシーに従うものとします。グローバルサインは、変更されたプライバシーポリシーをウェブサイトに掲載することで、プライバシーポリシーを随時変更することができるものとします。

利用者は、電子証明書を申請する際に個人情報を提供することにより、グローバルサインがその情報を処理し、電子証明書を認証し発行するにあたり、必要に応じて世界の関連会社、代理店、下請け業者に情報を公開及び転送することに同意したものとします。その際、利用者が居住している国よりデータ保護法が寛容な国への情報の公開及び転送、またそれらの国での情報を処理することへの同意も含まれます。

自然人の検証にあたっては、当社は、申請時に提出された名前、住所、その他の個人情報

を、適切な第三者機関のデータベースで確認する場合があります。利用者は本利用約款の締結と同時にこれに同意したものとみなします。係る検証にあたり、利用者が提出した個人情報は信用照会機関に開示され、当該信用照会機関は当該情報の記録を保管する場合があります。係る検証は本人確認の目的においてのみ行うものであり、信用調査の目的のものではありません。尚、本検証手続きは、利用者の信用格付けに影響しません。

利用者が GMO GlobalSign Russia LLC. に申請を行った場合には、自然人の検証にあたり、グローバルサインは、申請時に提出された名前、住所、その他の個人情報を検証します。本利用約款を締結することにより、利用者はグローバルサインがロシア連邦法 No. 152-FZ (2006年7月27日付) の規定に従い、当該情報を収集、分類、加工、保存、編集、使用、匿名化、ブロック、及び削除を行うこと、及び上級機関や法により規則が整備された場合には、これに従い第三者に当該情報を転送することに同意したことになります。

利用者が GMO GlobalSign Philippines (GSPH) に申請を行った場合には、自然人の検証にあたり、グローバルサインは、申請時に提出された名前、住所、その他の個人情報を検証します。本利用約款を締結することにより、利用者はグローバルサインが共和国法 10173 若しくはフィリピンの個人情報保護法 (2012 年付) の規定に従い、当該情報を収集、分類、加工、保存、編集、使用、匿名化、ブロック、及び削除を行うこと、及び上級機関や法により規則が整備された場合には、これに従い第三者に当該情報を転送することに同意したことになります。

#### **第 1 1 条 7 項 (商号、ロゴ、その他)**

利用者及び当社は、本利用約款による契約行為又はその履行において、他社の如何なる商標、ブランド名、ロゴ、プロダクト名称に関する如何なる権利も取得するものではなく、係る商標、商号、ロゴ、プロダクト名称に関するあらゆる権利を有する権利者から別途書面で許諾を得ている場合を除いては、その事由の如何を問わず一切これらの使用は禁止とします。

#### **第 1 2 条 (カスタマーサポート)**

利用者は、証明書に誤りがあった場合には、グローバルサインの <https://www.globalsign.com/en/company/contact> に記載されている海外拠点を含む当社のいずれかの事務所を通じて、直ちに グローバルサインに通知するものとします。利用者が証明書を受領してから 7 日以内にこれを行わなかった場合、証明書は受領されたものとみなされます。

利用者が発行された電子証明書に完全に満足していない場合、利用者は、証明書の発行から 7 日以内に返金を請求することができます。返金は、グローバルサインが負担する手数料を差し引いた額となります。