グローバルサイン電子証明書サービス利用約款

本利用約款が英語以外の言語に翻訳されている場合でも、本利用約款の英語版を常に原本とし、本利用約款の条項の解釈の唯一の基礎となるものとします。

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 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又は電子証明書を受領する利用者との間で成立します。

「グローバルサイン」とは、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であり、GMO グローバルサイン株式会社（日本）、GlobalSign China Co., Ltd. （中国）、GMO GlobalSign LTD（英国）、GlobalSign NV/SA（ベルギー）、GMO GlobalSign, Inc（米国）、GMO GlobalSign Pte. Ltd （シンガポール）、GMO GlobalSign Inc.（フィリピン）、GMO GlobalSign Certificate Services Pvt. Ltd （インド）, GMO GlobalSign Russia LLC （ロシア）、GMO GlobalSign Solutions in Technology S/A（ブラジル）、GMO GlobalSign FZ LLC (UAE)の何れかとなります。上記にかかわらず、利用者が eIDAS 適格証明書を注文した場合、「グローバルサイン」は GlobalSign NV/SA（ベルギー）を意味するものとします。

貴社が調達当事者であり、利用者の正式な代理人として、証明書の申請又は再販を行っている場合、貴社は、グローバルサイン及び依拠当事者に対し、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証明書を調達する場合、利用者は、ここに、当該調達当事者が証明書のために利用者に代わって行動すること（利用者証明書の申請、受領、運用、更新及び失効を含むがこれに限らない）について許可したことを、表明し保証するものとします。調達当事者が証明書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証明書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、グローバルサインの証明書を購入又は使用することはできません。

サブジェクトと利用者が２つの別個のエンティティであり、サブジェクトが自然人又は法人である場合、利用者は、サブジェクトが自身に適用される本契約の要件を承認することを確認するものとします。

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。ここに定義されていない用語は、業界標準で定義された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、合弁企業又はその他組織の総称であり、これ以外の他の組織又は代理人若しくは部局若しくは行政下部組織又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、又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、申請者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機能。

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。MC Requirements が適用される場合においては、証明書には MC Requirements で規定されたサブジェクト情報及び拡張機能が含まれており、MC Requirements に従って検証及び発行される。

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、グローバルサイン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。本利用約款において、認証局(CA)とは、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を指す。

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、相続人又は権利継承者を含む)。

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(eIDAS):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。

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小区内の下部組織(たとえば州、県、市、郡等)。

業界標準:以下の文書の最新版を指す:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”)
- CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (“EV Guidelines”)
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for Code Signing (“Baseline Requirements for Code Signing”)
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates (“Baseline Requirements for S/MIME”)

- Minimum Security Requirements for Issuance of Mark Certificates（“MC Requirements”）

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers（“ETSI 319 401”）

- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements（“ETSI 319 411-1”）

- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates（“ETSI 319 411-2”）

- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps（“ETSI 319 421”）

- ETSI TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking（“ETSI 119 495”）

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、又は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は、その秘密鍵は危殆化したと見なされる。

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、政府機関又は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。

マーク証明書: MC Requirements に規定されるサブジェクト情報及び拡張機能を含み、MC Requirements に従ってマーク証明書認証局(MVA)によって検証され、発行された証明書。グローバルサインでは認証マーク証明書（メールロゴ認証証明書（VMC））のみを提供している。

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するために用いるものをいう。MC Requirements が適用される場合においては、秘密鍵と公開鍵ペアが生成された後、秘密鍵は使用されず、破棄することができる。当該秘密鍵はデジタル署名の生成やデータの復号には使用されない。

調達当事者:利用者に証明書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する鍵をいい、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、又は対になる秘密鍵を用いてのみ復号が可能な暗号化メッセージを生成するために使用するものをいう。MC Requirements が適用される場合においては、公開鍵はメッセージの暗号化やデジタル署名の検証には使用されない。

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/シール生成デバイス(QSCD):電子署名/シール生成デバイスであって、eIDAS 規則の付属書 II 内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、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。

登録マーク:マーク証明書に含まれるマークの一種で MC Requirements のセクション 3.2.17.1 の要件を満たすもの。

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。サブジェクトがデバイス又はシステムの場合は、利用者の管理下になければならない。

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、利用約款又は利用条件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、又はその削除若しくは検出を困難にしてあるもの、及び、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、及び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。

認証マーク証明書:MC Requirements で規定されたサブジェクト情報及び拡張機能を含み、MC Requirements に従って CA によって検証及び発行された証明書。さらに、この証明書には、登録マークとして検証されたマーク表示が含まれる。

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講じるものとします。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において、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、若しくはその他の理由で当該事実を認識した場合、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又は、PKCS12 形式ファイルなどを利用して、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、利用者はグローバルサインが 3072 ビット未満の鍵ペアに署名しないことを了承すること。

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又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 ステープリ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適切なグロールサインのタイムスタンプ局を使用してタイムスタンプをすることを推奨します。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（「文書署名用証明書（AATL 用証明書)」のタイムスタンプサービス）

当社は、グローバルサインの「文書署名用証明書（AATL 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(該当する場合はサブジェクト)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)に関連する秘密鍵を、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。

コードサイニング証明書に関しては、申請者は、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、コードサイニング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します。

第４条４項（誤用防止）

利用者(該当する場合はサブジェクト)は、秘密鍵を不正使用又は誤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。証明書の受領から 7 日以内に利用者がグローバルサインへ通知しない限り、利用者は証明書を受け入れたものとみなされます。

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、利用約款又は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、詐欺又はマルウェアへの証明若しく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若しくはプログラムを含むソフトウェア又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 署名）

証明書が PDF への署名に使用される場合、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(該当する場合はサブジェクト)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「Code Signing Requirements」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（該当する場合はサブジェクト）は、以下の規定に従うものとします。

- グローバルサインからの通知、又は証明書の失効申請を認識した場合、該当する失効期限及び要件を遵守するため、グローバルサインに協力することに同意する。
- グローバルサインが業界標準、ブラウザのルートプログラムの要件その他の適用可能なポリシー及び標準を順守する義務を負っていることを認識し、状況によっては失効期限が数日又は数時間となる場合もあることを認識する。
- 証明書の適時の再発行に対する責任を認識し、承諾し、事前に備える。

グローバルサインは、利用者が、失効の影響を受けた証明書を再発行するための実施可能な計画を準備及び維持することを推奨します。

失効申請は、証明書の申請に使用されたアカウントを通じて行うか、report-abuse@globalsign.com へ提出するものとします。

第４条７項１（失効理由）

利用者は、CPS 第 4.9.1 項に記載される事由を含め、証明書を失効しうる理由を理解していることを確認するものとします。

また、利用者（該当する場合はサブジェクト）は、以下の何れか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（鍵の解読を除く）を中止し、かつ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。

a. 電子証明書に記載された情報の何れかが不正確である場合、又はそうなった場合。
b. 電子証明書に記載された公開鍵と対になる秘密鍵が誤用、紛失、盗難、危殆化した可能性がある若しくは危殆化した場合、又はアクティブ化データ（PIN コードなど）の危殆化その他の理由によりサブジェクトの秘密鍵の管理ができなくなった場合。
c. コードサイニング証明書について、疑義のあるコードへの署名に使用されたことを示す根拠がある場合。

第４条７項２（ステータス変更の通知）

利用者が所持する別の有効な証明書（以下「発行元証明書」という）に基づいて、証明書が利用者に対して発行された際（以下「新証明書」という）、発行元証明書が停止又は失効された場合、利用者は、発行元証明書のステータスが変更されたことをグローバルサインに通知する義務を負う。この通知を受けて、グローバルサインは、新証明書の停止又は失効が必要であるかどうかを判断するために調査を行う。

第４条８項（証明書の使用終了）

利用者(該当する場合はサブジェクト)は、証明書が有効期間満了若しくは失効し又は発行局が危殆化した場合、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(該当する場合はサブジェクト)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、又はフィッシング攻撃、詐欺若しくは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、又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業界標準、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ルトネーム(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、文書署名用証明書（AATL 用証明書）については、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こと。
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. 証明書管理者が、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。

第４条１５項１（コードサイニング及び EV コードサイニング証明書）

2023 年 4 月 24 日より前に発行された、非 EV のコードサイニング証明書に関して：

コードサイニング証明書について、利用者は以下の何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します。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。

1. 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。
2. 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。
3. 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、コード署名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。

2023 年 4 月 24 日より前に発行された、EV コードサイニング証明書に関して：

利用者の秘密鍵は、FIPS 140-2 Level 2 又は Common Criteria EAL 4+ の要件を満たすか、その基準を超える暗号モジュールで生成、保存及び使用される必要があります。

2023 年 4 月 24 日以降、非 EV 及び EV のコードサイニング証明書に関して、以下が有効となります：

利用者は、少なくとも 140 Level 2 又は Common Criteria EAL 4+ 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でコードサイニング証明書の秘密鍵を生成し保護するために、以下の何れかを使用することを表明するものとします。：

- 利用者は、指定された要件を満たすハードウェア暗号化モジュールを使用する。
- 利用者は、以下の要件を満たすクラウドベースの鍵生成・保護ソリューションを利用する：

  a. 鍵の生成、保存及び秘密鍵の使用は、指定された要件に準拠するクラウドソリューションのハードウェア暗号モジュールのセキュリティ境界内に留まるものとする。

  b. 秘密鍵を管理するレベルの利用においては、秘密鍵を保護するリソースへのアクセス、操作及び設定変更を全て記録するよう設定するものとする。

- 利用者は、「Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates」のセクション 6.2.7.3 の要件を満たす署名サービスを利用する。

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、鍵ペアがこれらの要件を満たす暗号デバイスに生成・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。

第４条１５項２（適格証明書）

適格証明書について、利用者(該当する場合はサブジェクト)は以下のことを認識し、了解するものとします。

- 秘密鍵は、（適格電子署名証明書の場合）サブジェクトによる単独の管理下において、（適格 e シール証明書の場合）サブジェクトによる管理下において、維持（又は個々で利用）されなければならない。
- 秘密鍵は電子署名(適格電子署名証明書の場合)又は e シール(適格 e シール証明書の場合)にのみ使用されること。
- 適格 e シール証明書の保有者がベルギーに設立されている場合、保有者は、当該証明書が使用されるたびに、保有者及び必要に応じて侵害の検出及び立証のために行動する管轄の行政又は司法当局が、当該自然人の身元及び代理権を立証できるような方法で、当該証明書を実際に利用する法人を代表する自然人の名前、法的能力及び代理権を立証できる措置を講じるものとする。

適格署名又は e シール生成デバイス（QSCD）を必要とする適格証明書の場合、

- 電子署名は、QSCD デバイスによってのみ作成されるものとする。
- 秘密鍵はグローバルサインが提供するか、または書面で承認した認定 QSCD デバイス内で生成、保管されなければならない。
- 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講じられねばならない。

第４条１６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拠を提出し 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１６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、又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、電気産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 規格を確認したものとします。

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、電気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。

- 自分の秘密鍵を他者によるアクセスから保護すること。
- 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。

- 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。
- グローバルサインの CPS に規定されている全ての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。
- 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。
- 証明書秘密鍵セキュリティ及び運用ポリシー
- 証明書失効ポリシー
- 利用者の本人確認情報を確認し(個人、役職、デバイス、若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４条１７項（マーク証明書）

マーク証明書の利用者は、さらに以下の本条本項の各条項（以下「マーク証明書条項」という）に同意するものとします。

全てのマーク主張エンティティ（以下「MAE (Mark Asserting Entity)」という）は、マーク証明書が発行される条件として、本マーク証明書条項に同意しなければなりません。消費エンティティ (Consuming Entity)、依拠当事者、その他如何なる者による、全てのマーク証明書（及びそこに記載されるマークの表示、その他のデータ又は情報）の使用、表示又は依拠は、本マーク証明書条項に同意することを条件とします。マーク証明書の OID 1.3.6.1.4.1.53087.1.1 は、参照により本マーク証明書条項を組み込みます。本マーク証明書条項に同意しない者は、マーク証明書、マーク表示又はマーク証明書に含まれるその他のデータ若しくは情報を取得、使用、公表又は依拠することができません。

第４条１７項１（定義）

マーク証明書に関する語句は、MC Requirements の 1.6 に定める意味を有するものとします。

第４条１７項２（複製及び表示の限定的権利）

MAE は、MC Requirements 及び本マーク証明書条項の条件と制限に従って、次の権利を付与します：

第４条１７項２－１

CA に対して、MC Requirements で要求される範囲内でマーク証明書マークを含むマーク証明書を発行し、その証明書を制限された数の Certificate Transparency (CT) ログに記録するための、限定的で非独占的なワールドワイドのライセンスを付与します。

第４条１７項２－２

消費エンティティに対して、内部のロゴ認識システムと連携してマーク証明書マークを使用し、第４条１７項３－１項で許可された範囲内で、マーク証明書マークをホスト、保存、複製、表示、処理及び修正するための、限定的で非独占的なワールドワイドのライセンスを付与します。このマーク証明書マークは、直接的な視覚的関連性を持つ通信、文書又はサービスにのみ使用されるものであり、それらは MAE によってマーク証明書の Subject Alternative Name フィールド内の同一のドメインの内の１つから又はそれを通じて作成されるか、又は提供されるものです。

第４条１７項２－３

証明書の Certificate Transparency (CT) ログオペレーター（発行 CA と異なる場合）には、発行された証明書の永続的な公開記録をサポートし、公衆がマーク証明書の正確性検証を監査できるようにする目的で、マーク証明書のコピーを保持し、かつマーク証明書を複製するための、限定的で非独占的なワールドワイドのライセンスが付与されます。他のいかなる当事者に対しても、使用目的に対しても、ライセンスは付与されません。

第４条１７項３（ライセンスの制限及び条件）

発行され、公開されたマーク証明書を通じて取得したマーク証明書マークを、その製品及びサービスに組み込む、又は組み込む意向のある消費エンティティは、そのライセンスが以下の条件及び制約を受けることに同意するものとします。

第４条１７項３－１（品質管理、同一処理）

消費エンティティは、発行されたマーク証明書から取得したマーク表示を、サイズや縮尺を調整したり、同じ文脈で表示される他のマーク表示のトリミングと一貫性のある方法でトリミングする場合を除き、表示時に歪ませたり、色や背景を変えたり、透明度を変更したり、その他何らかの方法で変更したりしてはなりません。消費エンティティは、発行されたマーク証明書から取得した文字商標を表示する場合、同じ視覚的文脈で表示される全てのマーク証明書から取得した文字商標に対して一貫性をもって適用される中立的な方法で表示しなければなりません。

第４条１７項３－２（パートナーシップ又は関係性の示唆の否定）

消費エンティティと MAE の間で明示的な合意がある場合を除き、マーク証明書マーク又はマーク証明書のその他の内容は、本マーク証明書条項によって形成された単なるライセンサーとライセンシーの関係を超えて、消費エンティティと MAE との関係を合理的に示唆するような方法で使用又は表示することはできません。

第４条１７項３－３（CRL 又は OCSP の確認）

消費エンティティは、CA が保持する証明書失効リストを確認するか、又は OCSP を使用してオンラインで失効状態を確認し、マーク証明書が失効したかどうかを最低 7 日毎に確認しなければなりません。

第４条１７項３－４（合法的な使用）

消費エンティティは、適用法令に従ってのみマーク証明書のマーク表示を使用することができます。

第４条１７項３－５（十分な所有権又はライセンス）

MAE は、マーク証明書を通じて公開されるマーク証明書マークが、MAE が保有しているか、又は本マーク証明書条項において限定されたライセンスを付与するために十分なライセンスを取得した登録商標（及び存在する場合は文字商標）を表していることを保証し、該当する登録商標（又は存在する場合は文字商標）を保有しなくなったか、又はその十分なライセンスを持たなくなった場合には、直ちにマーク証明書を失効させることを保証します。MAE は、マーク証明書の申請内容に起因する消費エンティティ、依拠当事者又は CA に対する知的財産権又はその他の請求に関して防御し、責任を負うものとします。

第４条１７項３－６（表示義務の不存在）

MAE は、ドメイン登録者として MAE が所有又は管理するドメインに関連し MAE が公開するコンテンツに関係するマーク証明書マークにつき、通信又はメッセージが MAE からのものであることが確認され、該当するマーク証明書から適切なマーク証明書マークを取得し安全に表示できる場合であっても、消費エンティティがこれを表示する義務を負わないことを承諾します。それに代わって、消費エンティティは、マーク証明書条項に従ってマーク証明書マークを表示するか、又は表示しないかを選択することができます。

第４条１７項３－７（終了）

マーク証明書が失効し、又は期限が切れた場合、MAE はマーク証明書の公開又は使用を直ちに停止し、第４条１７項２で消費エンティティに付与されたライセンスは終了するものとします。第４条１７項２における消費エンティティへのライセンスは、消費エンティティが本マーク証明書条項の何れかの条項に違反した場合には、自動的に、かつ直ちに終了します。消費エンティティは、該当するライセンスが終了した場合、直ちにマーク証明書マークの使用を中止しなければなりません。

第４条１７項３－８（MC Requirement 及びマーク証明書条項の更新）

MC Requirements 及びマーク証明書条項は、随時更新されることがあります。全ての当事者は、マーク証明書発行時に有効な MC Requirements 及び利用約款のバージョンは、マーク証明書の有効期間満了日又は失効日まで（また、その性質上、有効期間満了日又は失効日を超えて適用される条項については、その条項が適用されなくなるまで）適用されることに同意するものとします。マーク証明書を取得、使用、公開又は信頼する各エンティティは、MC Requirements 及びマーク証明書条項の更新版を随時確認し、十分に理解する責任を負います。

第５条（クレデンシャル）

グローバルサインは、サービス又は証明書へのアクセス及び/又は使用のためのクレデンシャルを提供することがあります。利用者は、自身のクレデンシャルの機密性及びセキュリティを維持する責任を負い、これらのクレデンシャルを使用して発生する全ての活動に対して全責任を負うものとします。

第６条（料金）

証明書がグローバルサイン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７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８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、利用者の使用権は、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権を終了することができます。利用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い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９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 CPS に準拠して証明書を発行及び管理している限り、利用者や依拠当事者、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拠当事者、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 枚につき利用者又は依拠当事者 1 人当たり 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、EV コードサイニング証明書又はマーク証明書に対しては、証明書 1 枚につき利用者又は依拠当事者 1 人当たり 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ポリシーでの規定外で修復できるものに限ります。ワランティーポリシー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の規定に基づくあらゆる取引又はサービスの利用、交付、依拠、ライセンス承諾、履行又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、特殊な損害若しくは結果的損害又は逸失利益若しくは逸失データ、その他の間接的、偶発的若しくは結果的損害に対しても、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、関連処理量又は苦情の多少に関わらず適用されます。

上記は、eIDAS 規則第 13 条に基づく、適格証明書に関するグローバルサインの責任を制限するものではありません。

第１０条（期間及び終了）

本利用約款は次のうちの何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若しくは間接的に、又はマネージド SSL サービス若しくはマネージド 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発送した後、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１１条（契約終了の効果）

本利用約款に基づく契約関係が終了し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５条、第６条、第７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１２条（雑則）

第１２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、構築及び執行に適用される法律、及び（ii） 何れかの事項、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
GMO グローバルサイン株式会社	日本	日本　東京地方裁判所
GlobalSign China Co., Ltd.	中国	中国　上海
GMO GlobalSign Ltd.	イングランド及びウェールズ	英国　ロンドン
GlobalSign NV	ベルギー	ベルギー　ルーベン
GMO GlobalSign, Inc. (US)	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
GMO GlobalSign Pte. Ltd	シンガポール	シンガポール
GMO GlobalSign Inc.	フィリピン	フィリピン　マカティ市
GMO GlobalSign Certificate Services Pvt. Ltd	インドの法令	インド　デリー
GMO GlobalSign Russia LLC	ロシア連邦の法令	ロシア　モスクワ

GMO GlobalSign Solutions in Technology S/A	ブラジル	ブラジル　ベロホリゾンテ
GMO GlobalSign FZ LLC	アラブ首長国連邦	アラブ首長国連邦　ドバイ

eIDAS 適格証明書の、財務的または商業的な問題に関連する紛争は、上記に示される準拠法及び管轄裁判所に従って処理されるものとし、証明書に関する紛争については、上記に示される GlobalSign NV の準拠法及び管轄裁判所となります。

第１２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、管理人及び譲受人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何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１２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、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又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１２条４項（分離条項）

本利用約款の何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、保証の否認又は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１２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、送達の完了が書面又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何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１２条６項（輸出入法令への準拠）

各当事者は、本契約の履行に関連して、適用される全ての制裁法、輸出入法、制限、国家安全保障管理及び規制（以下総称して「輸出入法令」という）を含むがこれらに限定されない、全ての連邦、州及び地域の法律及び規制を遵守するものとします。利用者は、輸出入法令に違反して、証明書又はその他の製品を輸入、輸出、再輸出せず、また輸出又は再輸出を許可しないものとします。

第１２条７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（https://ww

w.globalsign.com/en/repository 日本語版は https://jp.globalsign.com/repository/）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。

利用者が証明書の申請時にグローバルサインに個人情報を提供した後、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、代理店及び下請け業者に情報を公開及び/又は転送する場合があります。これには、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/又は転送、またそれらの国で情報を処理することが含まれます。

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。これはグローバルサインがサービスを提供するために必要なことであり、係る検証にあたり、利用者は本利用約款の締結と同時にこれに同意したこととみなします。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。これはグローバルサインがサービスを提供するために必要なことであり、グローバルサインは利用者の個人情報を、ロシア連邦法 FZ-No.152（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、また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ができることとします。

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。これはグローバルサインがサービスを提供するために必要なことであり、グローバルサインは利用者の個人情報を、共和国法第 10173 号又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、また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ができることとします。

第１２条８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、他方当事者の如何なる商標、ブランド名、ロゴ又は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、ロゴ又は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１３条（カスタマーサポート）

利用者はカスタマーサポートに関し、support@globalsign.com 若しくはリストに記載されている当社の海外拠点又は https://www.globalsign.com/en/company/contact から問い合わせることができます。

第１３条１項（返金ポリシー）

利用者は、発行された電子証明書に完全に満足していない場合、当該証明書を直接グロ

ーバルサインへ注文していた場合に限り、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。

[V 5.6　2025-08-28]