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」または「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。

第１条（定義）

本利用約款中で使われている用語は、特段の定めがない限り、以下の意味を有するものとします。

1) 「関係会社」とは、一般の企業、パートナー企業、合弁企業、或いはその他法人であり、かつ他の企業、或いは代理人、特定部門、行政関連機関或いは政府直轄機関などを支配するところのもの、或いは逆にこれらに支配される関係にあるものやその影響下にあるもの、以上の全般をいいます。

2) 「申請者」とは、証明書の申請（若しくは更新の申請）をする個人若しくは法人をいいます。証明書が発行された時点で、申請者は利用者と呼ばれます。デバイスに発行された証明書については、デバイスが実際の証明書要求をした場合においても、申請者は証明書に指定されるデバイスを管理または運用する個人または法人となります。

3) 「アプリケーションソフトウェアベンダ」とは、インターネットブラウザソフトウェア、若しくは証明書を表示または利用し、ルート証明書を実装するその他依拠アプリケーションソフトウェアベンダをいいます。

4) 「機関情報アクセス」とは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拡張子をいいます。

5) 「CA/ブラウザフォーラム」とは、認証局やソフトウェア提供企業などを代表する専門家で構成される業界団体です。詳細は https://cabforum.org/ をご覧ください。

6) 「証明書」とは、公開鍵とアイデンティティを結びつけるために電子署名を使う電子文書をいいます。

7) 「証明書受益者」とは、証明書の利用約款に合意した利用者、グローバルサインがルート証明書の組み込み契約を交わした全てのアプリケーションソフトウェアベンダ、及び有効な証明書に依拠する依拠当事者をいいます。

8) 「電子証明書管理者」とは、電子証明書のライフサイクル管理に責任を負う組織または個人をいいます。これは、利用者自身である場合と、そうでない場合があります。

9) 「証明書申請」とは、CA/ブラウザフォーラム・ベースラインリクワイアメント（※注：基本要件）（以下「ベースラインリクワイアメント」という）のパブリック証明書発行及びマネジメントの項目に記載されているところの、証明書発行の申請行為をいいます。

10) 「証明書申請者」とは、利用者の申請権限者から明示的に権限を付与され、これを代理して証明書申請を準備し提出する申請実行者または第三者（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など）をいいます。MSSL（SSL マネージドサービス）やePKI（マネージドPKI Lite）などのマネージド・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ます。

11) 「証明書失効リスト（以下「CRL」という。※注：Certificate Revocation List）」とは、証明書を発行したCAにより生成され、タイムスタンプ及び電子署名される失効済み電子証明書のリストをいいます。CRLは定期的に更新されます。

12) 「認証局（CA）」とは、証明書の生成、発行、失効、及び管理をする組織をいいます。CAは、ルートCA及び下位CA両方を指します。グローバルサインまたはグローバルサインによりサブジェクトに対し証明書発行を許可された組織がCAとなります。以下、申請者のCAはグローバルサインを意味します。

13) 「危殆化」とは、セキュリティポリシーに違反し、機密情報へのコントロールを失うことをいいます。

14) 「電子署名」とは、電子データに付与する、電子的な徴証をいいます。これは秘密鍵を用いて電子データを暗号化し、公開鍵を用いてこの電子データの完全性を検証するものです。

15) 「ドメイン名」とは、DNS(Domain Name System)内のノードに割り当てられている名称をいいます。

16) 「ドメイン名登録者」とは、ドメイン名の所有者であるが、より正確にはWHOISやドメイン名登録機関により「登録者」として登録されている個人や法人であり、それらドメイン名登録機関がそのドメイン名の使用方法について権利を持つところの登録された個人や法人をいいます。

17) 「ドメイン名登録機関」とは、ドメイン名を登録する個人や法人をいい、(i)米国のICANN(Internet Corporation for Assigned Names and Numbers. ※注：世界のドメイン管理本部)、(ii)国営のドメイン名管理機関、または(iii) 民間のネットワーク関連代理機関(その関係会社、契約者、代理人、法的相続人、権利継承者を含む)からの支援、或いは契約のもとにこれを行うものです。

18) 「ドメイン名システム（以下「DNS」という。※注：Domain Name System）」とは、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をいいます。

19) 「FQDN」とは、完全修飾ドメイン名の意味で、DNSに設定されたすべての上位ノードの名称を含むドメイン名をいいます。

20) 「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をいいます。GMO GlobalSign Limited, GMO GlobalSign, Inc., GMO GlobalSign Pte. Ltd., GMO GlobalSign Certificate Services Pvt. Ltd., GMO GlobalSign Russia LLC., 若しくはGMOグローバルサイン株式会社をいいます。

21) 「行政機関」とは、政府が運営する法人、政府機関、部署、省庁、支部、政府と同類の役割、若しくは国内の政治的な下位区分(都道府県など)をいいます。

22) 「鍵ペア」とは、暗号技術上の鍵ペアであり、秘密鍵とこれに対応する公開鍵のセットをいいます。

23) 「法人」とは、該当国の法律制度に則った組織、企業、パートナーシップ、事業体、トラスト、行政機関、及びその他組織体をいいます。

24) 「NAESB（北米エネルギー規格委員会）認定CA」（※注：北米の利用者にのみ関連する項目）とは、NAESBのACA規格で認定されるCAをいい、これには、NAESBの定める技術・管理要件に適合する必要があります。

25) 「OneClickSSL™プラグイン」とは、ドメインが管理下にあることを担保しながらSSLサーバ証明書（本書では「サーバ証明書」を意味する）要求及びそのインストールを簡易に行うためのソフトウェアアプリケーションをいいます。

26) 「オンライン証明書状態プロトコル（以下「OCSP」という。※注：Online Certificate

Status Protocol）」とは、電子証明書の失効情報をリアルタイムで取得するためのインターネット・プロトコルをいいます。

27) 「秘密鍵」とは、鍵ペアの所有者により秘密に保持される鍵をいい、電子署名の作成及びこれと対になる公開鍵により暗号化された電子データの復号に利用されます。

28) 「公開鍵」とは、鍵ペアの所有者により公開される鍵をいい、対になる秘密鍵を用いて生成された電子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います。

29) 「登録局（以下「RA」という。※注：Registration Authority）」とは、証明書のサブジェクトに対する本人確認や認証を行う法人をいい、CA とは異なり、署名や証明書の発行は行いません。また RA は証明書申請プロセスや失効プロセスの補助をすることがあります。「RA」が役割や機能を示す用語として使われる場合、RA は必ずしも独立した組織体を意味するわけではなく、CA の中の一部組織を表すこともあります。

30) 「依拠当事者」とは、有効な証明書に依拠する任意の個人または法人をいいます。アプリケーションソフトウェアベンダは、これが配布するソフトウェアが証明書に関する情報をそのまま表示する機能しかない場合、依拠当事者とはみなされません。

31) 「ルート証明書」とは、ルート CA が、自身を識別するため及び、下位 CA に発行した証明書の検証のために発行するところの自己署名した証明書をいいます。

32) 「サブジェクト」とは、証明書の発行対象であり、証明書のサブジェクト(Subject)として特定される、個人、デバイス、システム、設備、または法人をいいます。サブジェクトは、利用者、若しくは、利用者の管理、運用下にあるデバイスの何れかです。

33) 「下位 CA」とは、その証明書がルート CA またはその他の下位 CA によって署名されている CA をいいます。

34) 「利用者」とは、利用契約書或いは利用約款などに則り、証明書を発行されるところの個人、若しくは法人をいいます。

35) 「疑わしいコード」とは、スパイウェア、マルウェアなどを含む悪意のある機能や深刻な脆弱性を持つコードをいいます。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みます。

36) 「利用条件」とは、ベースラインリクワイアメントに従って発行された証明書の安全な利用方法、許可された利用方法に関する規定であり、ここでは申請者或いは利用者が CA の関係会社である場合をいいます。

37) 「ワイルドカード証明書」とは、証明書上でサブジェクトの FQDN の左端の値がアスタリスク(*)になっている証明書をいいます。

以下の認証業務運用規程（以下「CPS」という）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。また、以下の各規程も引用により本利用約款に組み込まれます。

- グローバルサイン製品向けの CPS： http://www.globalsign.com/repository（注：英語版）（注：日本語版は別途掲載予定）
- ベースラインリクワイアメント：
  https://cabforum.org/documents/#Baseline-Requirements
- グローバルサインワランティーポリシー：https://jp.globalsign.com/repository/
  （英語版については http://www.globalsign.com/repository/ ）
- グローバルサイン返金ポリシー：https://jp.globalsign.com/repository/
  （英語版については http://www.globalsign.com/repository/ ）
- グローバルサイン支払ポリシー：https://jp.globalsign.com/repository/

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本利用約款に基づき、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。利用者は、本利用約款第４条に定める利用者の秘密鍵の管理に関する義務は、本契約の開始日（当該証明書の申込み日）より適用します。なお、2015 年 3 月 30 日をもって、グローバルサインは SSL サーバ証明書の有効期間に関し、新規の発行、更新分、及び再発行の何れにおいても 39 ヶ月を超えるものは発行しないものとします。

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、グローバルサインまた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ともに、以下のサービス提供を開始します。

第３条１項（CRL と OCSP サービスの提供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 が電子署名し発行したすべての電子証明書に関する電子情報をまとめ、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。

- 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。
- 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。
- 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）
１．グローバルサインは、次の各号に掲げるいずれかの事由があるときは、発行した電子証明書を 24 時間以内に失効するものとします。
1) 利用者が電子証明書を発行したグローバルサインに、書面にて証明書の失効を申請し、当社がこれを受領した場合。
2) 利用者が、最初の証明書申請は認可されず、遡って権限を承認しないとグローバルサインに通知した場合。
3) グローバルサインが、利用者の秘密鍵が危殆化した、暗号アルゴリズムや鍵長がベースラインリクワイアメントと適合しない、若しくは電子証明書が不正に利用されたと判断する合理的な根拠となる情報を入手した場合。
4) グローバルサインが、利用者が本利用約款に定める重要な義務に違背したとの通告を受けるか、その他の方法により当該事実を把握した場合。
5) グローバルサインが、利用者の電子証明書の FQDN や IP アドレスの使用がもはや法的に承認されないことの当該事実を把握した場合（裁判所または仲裁人によりドメイン名を

使用するためのドメイン名登録者の権利、またドメイン名登録者と申請者間の関連リストまたはサービス契約を無効とした場合、及びドメイン名登録者がドメイン名を更新できなかった場合)。

6) グローバルサインが、ワイルドカード証明書が不正に誤解を招く下位の FQDN を証明するために使用されていた事実を把握した場合。
7) グローバルサインが、電子証明書に記載された重要な情報に変更があったとの通告を受けるか、その他の方法により当該事実を把握した場合。
8) 電子証明書がベースラインリクワイアメント及びグローバルサインの証明書ポリシーまたは認証業務運用規程に従って発行されていない、とグローバルサインが判断した場合。
9) グローバルサインが電子証明書に記載された情報のいずれかが不正確若しくは誤解を招くものであると判断した場合。
10) グローバルサインが何らかの理由で業務を中止し、その電子証明書の失効業務を他の認証局に委託しなかった場合。
11) グローバルサインのベースラインリクワイアメントに基づいて電子証明書を発行する権限が満了、失効、または終了し、グローバルサインが証明書失効リストや OCSP の維持を続けない場合。
12) グローバルサインが、証明書発行下位認証局に紐づく秘密鍵の危殆化を把握した場合。
13) グローバルサインの証明書ポリシー、認証業務運用規程において失効が必要な場合。
14) 電子証明書のフォーマットの技術的内容がアプリケーションソフトウェアベンダまたは依拠当事者に許容できないリスクがある場合 (例:CA/ブラウザフォーラムが、推奨外の暗号、電子署名のアルゴリズム、または鍵長などに脆弱性があり、一定の時間内に認証局より無効、或いは交換されるべきだと判断する可能性がある)。
15) グローバルサインが、電子証明書が悪意のあるソフトウェア若しくは「マルウェア」の署名に利用された事実を把握した場合。

2. グローバルサインは、次の各号に掲げるいずれかの事由があるときもまた、発行した利用者の電子証明書を 24 時間以内に失効することがあります。

1) 利用者または組織管理者が、証明書のライフサイクルを管理する GS パネルを通して失効を申請した場合。
2) 利用者が OneClickSSL 失効ワークフロープロセス経由で証明書の失効を申請した場合。
3) 利用者が認証された申請により、グローバルサインのサポートチームまたは登録局に失効を申請した場合。
4) グローバルサインが、利用者が取引禁止対象者としてブラックリストに登録された、若しくはグローバルサインの事業を管轄する国・地域の法により取引禁止国と定められた場所で営業しているとの通告を受けるか、その他の方法により当該事実を把握した場合。
5) グローバルサインが自己の裁量により、利用者の証明書の継続利用がグローバルサイン認証局及びグローバルサインのセキュリティーや評判、信用ステータスを危殆化させる可能性があると判断した場合。
6) 当該電子証明書を継続して利用に供することが、グローバルサインの事業または依拠当事者に有害である場合。

3. グローバルサインは、電子証明書の使用方法が有害となるか否かを検討する際に、以下の情報をはじめとする各種情報を確認します。

1) 寄せられる苦情申し立ての内容及び数量
2) 申立人の確認
3) 関連する法令

4)　有害使用の申し立てに対する、利用者からの反応

第３条３項（鍵の生成）
グローバルサインが PKCS12 形式ファイルやスキップ申込サービス、或いはワンクリック SSL 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。

- 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。
- 電子署名に適した鍵長やアルゴリズムを利用すること。
- 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生成することはなく、暗号アルゴリズムのオプションとして SHA2 を提供すること。

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 レスポンダまたは 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タイムスタンプをする事を要請します。但し、グローバルサインは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、また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、または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、また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）
利用者はグローバルサインに対し、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、いかなるときも完全、正確、かつ真実の申請者名、URL、及び申請情報などを提出することを表明し保証します。その情報としては SSL サーバ証明書における申請者名、URL 情報、及び EV コードサイニング証明書における申請者情報などを含まれます。

第４条２項（秘密鍵の保護）
申請者は、申請する電子証明書と対になる秘密鍵や関連する認証情報や装置（パスワード、トークンなど）を、いついかなる時も利用者単独の管理下に置き、その機密性を守り、適切に保護するために必要なすべての合理的措置を取ります。

第４条３項（電子証明書の受領と確認）
利用者は、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ものとします。

第４条４項（グローバルサインの発行する電子証明書の利用）
利用者は、SSL サーバ証明書に関し、その証明書の記載情報であるサブジェクトオルトネーム（サブジェクト代替名）が指定するアクセス可能なサーバに対してのみこれをインストールすることができ、また適用法令に従い、本利用約款或いは使用条件に従う限りにおいて、これを使用することができます。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。如何なる状況においても、当該電子証明書をフィッシング攻撃、詐欺、マルウェアの認証や署名などの犯罪行為に使用してはなりません。

EV コードサイニング証明書については、利用者は疑わしいコードに故意に署名したりしないこと、また以下の事項に従うことを了解し、表明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

第４条５項（通知と失効）
利用者は、以下の事由に該当する場合には、速やかに電子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、利用者に不正利用または危殆化があった場合、またはその疑いがあると判断した場合。

第４条６項（証明書使用の中止）
利用者は、電子証明書が失効された場合、その電子証明書に記載された公開鍵と対になる秘密鍵の利用を速やかに中止するものとします。

第４条７項（対応）
利用者は、証明書の不正利用や危殆化に関して、これに対するグローバルサインの指示に対し、48時間以内に応答するものとします。

第４条８項（承認と受諾）
利用者は、利用者が本利用約款及び利用条件に違反した場合、若しくは当該証明書がフィッシング攻撃、詐欺、マルウェアの頒布などの犯罪行為を可能にするような方法で利用されたとの事実をグローバルサインが把握した場合、当社は当該証明書を直ちに失効する権利があるということを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９項（SSL サーバ証明書ドメインの独占的管理権限）

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、IP アドレスに対し独占的な管理権限を有することをここに表明保証します。利用者が何れかのドメインに関してその独占的管理権限を喪失した場合には、利用者は当社に当該事実を速やかに通知するものとします。

第４条１０項（クライアント証明書の電子メールアドレスに対する独占的管理権限）

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独占的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独占的管理権権限を喪失した場合には、利用者は当社に当該事実を速やかに通知するものとします。

第４条１１項（鍵生成及び使用）

１．利用者また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。

- 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」及び「EV コードサイニング証明書」では、FIPS 140-2 Level 2 に準拠した装置を使用すること。
- 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。
- 利用者はグローバルサイン CA 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。

２．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。

- 利用者が、アクティベーションデータ（活性化データ）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。
- 利用者は証明書管理者が証明書発行の為の適正なトレーニングを受けることを確約すること。
- 証明書管理者は以下を適正に保持する為、あらゆる合理的手段をとって、証明書の唯一の専属的管理担当を維持すること、要求された証明書の公開鍵と対応する秘密鍵を機密に保持し、また常時これを適正に保護すること。これらは例えばトークンや HSM 等のキーにアクセスする際のパスワード管理等にみられる関連認証メカニズムと同様の対応姿勢で行うこと。

第４条１２項（NAESB に特有の義務、（※注：北米の利用者にのみ関連））

NAESB 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。

事業実務に関する基準 WEQ-012 v3.0 に準拠する組織団体は、卸電気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。NAESBが事業実務に関する基準WEQ-012 に定める認証方法を用いて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）、登録が必要です。

登録された組織団体及びこれが属するコミュニティは、事業実務に関する基準に定めるすべ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。

利用者である組織団体は、グローバルサインを通じて果たすべき、WEQ-012 v3.0 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。

エンドエンティティたる組織団体は、証明機関たるエンティティに対し、以下の事業実務に関する基準WEQ-012規格の内容を確認し、これに対する自らの理解を確認し承諾します。

A. 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、明確に意図されたデータの受信者を除き、誰もデータの一片も読み取ることがないことを保証します。
   - 認証：あるエンティティに対し、別のエンティティ自らが誰であるか表明することを保証します。
   - 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」及び「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します。
   - 否認防止：取引の当事者や電子メッセージの送信者は、取引を行い、または電子メッセージを送信した事実を否認することができません。
B. エンドエンティティは公開鍵を記載する電子証明書を使用してある個人またはコンピュータ・システムの公開鍵とエンティティを紐づけ、鍵の交換による共通鍵暗号を行うために、公開鍵による暗号化を用いることが電気産業界に承認された手段であることを確認し承諾します。
C. 利用者は、グローバルサインのCPSを、業界標準に則ったものであることを確認しています。

利用者は、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取得しなければなりません。

利用者は、以下の要求事項にもしたがわなければなりません。

1) 他者にアクセスされないよう、自らの秘密鍵を保護すること。
2) 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 CPSの定める通りすべての契約を締結すること。
4) グローバルサインが定め求める通り、証明書申請手続き、申請者の本人確認手続き、証明書管理手続きなど認証業務に関わる同意事項を順守すること。
5) エンドエンティティにおいて証明書管理制度が導入されており、当該制度に基づき関連する従業員全員がトレーニングを受け、当該制度にしたがった管理が行われるよう体制が整備されているかを確認すること。当該制度には以下を含む（がこれに限るものではない）。
   - 電子証明書秘密鍵のセキュリティポリシー及び取り扱い方針
   - 証明書の失効に関するポリシー
6) 利用者の種別（個人、役割、デバイス、アプリケーションなど）を確認し、各証明書申請に

ついて、完全かつ正確な情報を提出すること。

第５条（情報公開の許可）

利用者は、グローバルサインが利用者の電子証明書のシリアルナンバーを、CRL と OCSP サービスの提供に関連して公開することがあることに同意します。これにはグローバルサイン CA の階層証明による証明書も、またこれ以外の CA 階層による証明書についても同様です。

第６条（免責）

法律で認められていない範囲を除き、また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障を含む、いかなる保証に関しても当社は一切の責任を負いません。

当約款の基準要件と CPS の規定に従いグローバルサインが証明書を発行、管理している限り、利用者や依拠当事者、及びいか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。若しくは、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 1000 ドル（米国ドル）を超えないものとします。但し、EV SSL 証明書または EV コードサイン証明書に対しては、証明書１枚につき 2000 ドル（米国ドル）を保障限度とします。

上記の保障上限はグローバルサインのワランティポリシーでの規定外で修復できるものに限ります。ワランティポリシーのもとで支払われる金額は当社のそれぞれの保障上限に従うものとします。

電子証明書、電子署名に関しては、本約款に規定に基づくあらゆる取引またはサービスの利用、交付、依拠、ライセンス承諾、履行或いは不履行、に起因して生じる、いかなる間接的損害、偶発的損害、特殊な損害、結果的損害、また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応されます。

第７条（期間と解除）

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。

1) グローバルサインから利用者に直接的または間接的に、或いはマネージド SSL サービスまたはマネージド 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。
2) 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、３０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８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５条、第６条、第８条及び第９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９条（雑則）

第９条１項（準拠法）

1) 本利用約款の当事者がGMO GlobalSign Limitedである場合には、本利用約款の準拠法は、イングランド及びウェールズの法令とし、管轄裁判所は英国の裁判所とします。当該法令中にある国際私法の規定は適用しません。
2) 本利用約款の当事者がGMO GlobalSign,Inc.である場合には、本利用約款の準拠法は、米国ニューハンプシャー州の法令とし、管轄裁判所は米国ニューハンプシャー州の裁判所とします。当該法令中にある国際私法の規定は適用しません。
3) 本利用約款の当事者がGMO GlobalSign Pte.Ltd.である場合には、本利用約款の準拠法は、シンガポールの法令とし、管轄裁判所はシンガポールの裁判所とします。当該法令中にある国際私法の規定は適用しません。
4) 本利用約款の当事者がGMO GlobalSign Certificate Services Pvt.Ltd.である場合には、本利用約款の準拠法は、インドの法令とし、管轄裁判所はインドの裁判所とします。当該法令中にある国際私法の規定は適用しません。
5) 本利用約款の当事者がGMO GlobalSign Russia LLC.である場合には、本利用約款の準拠法は、ロシア連邦の法令とし、管轄裁判所はロシア連邦の裁判所とします。当該法令中にある国際私法の規定は適用しません。
6) 本利用約款の当事者がGMOグローバルサイン株式会社である場合には、本利用約款の準拠法は、日本国の法令とし、管轄裁判所は東京地方裁判所とします。当該法令中にある国際私法の規定は適用しません。

第９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、その利益に帰する為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。かかる譲渡また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、かかる行為は、当社からの解除事由となり得ます。

９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、いかなる製品またはサービス契約、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すべ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。本利用約款では、Microsoft社をコードサイニング証明書、EVコードサイニング証明書の第三受益者と定めます。

但し、Microsoft社が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することがあり、その場合Microsoft社は、関連するMicrosoftサービスやアプリケーションの内容を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９条４項（契約の分離）

本利用約款のいずれかの条項の規定、またはその適用が、事由の如何を問わず、一部の範囲において無効また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すべ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９条５項（通知）
利用者が本利用約款に関連して当社に通知、請求または要求することを希望する、また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または配達証明付の書留郵便にて https://jp.globalsign.com/cominfo/international_site.html にリスト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。なお、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９条６項（第三者機関データベースの使用許可）
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こととみなします。かかる検証にあたり、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。かか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。なお、本検証手続きは、利用者の信用格付けに影響しません。

本利用約款の当事者がGMO GlobalSign Russia LLC.である場合には、自然人の検証にあたり、GMO GlobalSign Russia LLC.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。

第９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またはその履行において、他社のいかなる商標、ブランド名、ロゴ、プロダクト名称に関するいかなる権利も取得するものではなく、かかる商標、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１０条（エラーがあった場合の通知）
本利用約款の第４条３項の利用者の確認に関連して、その際に利用者が電子証明書に何らかのエラーを発見した場合、速やかに当社にこれを通知するものとします。但し、電子証明書の利用可能日から７日以内に、利用者からこの通知がなかった場合には、電子証明書は受領されたものとみなされます。
当社は、返金を行う場合には、http://jp.globalsign.com/repository/ に掲載するグローバルサイン返金ポリシー（※注：一部参照資料では「Refund Policy」という名称）に基づきこれを行うものとします。

（以下空白）