DIGITAL CERTIFICATES BY DIGICERT – TERMS OF USE
デジサート電子証明書利用規約

These Digital Certificates Terms of Use ("**Certificate Terms of Use**") apply to each digital certificate ("**Certificate**"), regardless of Certificate type, whether publicly-trusted TLS/SSL Certificates, Client Certificates (as defined in Section 9), Qualified Certificates (as defined in Section 10), or otherwise, issued by DigiCert, Inc., a Utah corporation or any of its affiliates, including its Qualified Trust Service Providers (collectively, "**DigiCert**") to an entity or person ("**Customer**"), as identified in the DigiCert services management portal and/or related API made available to Customer ("**Portal**") or issued Certificate. The Certificate Terms of Use apply regardless of when Customer requested the Certificate or when the Certificate is issued. The account to access and use the Portal on Customer's behalf is referred to herein as the "**Portal Account**."
この電子証明書利用規約（以下「**本証明書利用規約**」といいます）は、公的に信頼される TLS/SSL「証明書」、「クライアント証明書」（第 9 条に定義します）、「適格証明書」（第 10 条に定義します）その他「デジサート」が発行する前記以外の種類の「証明書」であるかにかかわらず、米国ユタ州法人 DigiCert, Inc.又は「適格トラストサービスプロバイダ」を含む自己の関係会社（以下、総称して「**デジサート**」といいます）が、団体又は個人（以下「**お客様**」といいます）で、「デジサート」が「お客様」に対し提供する「デジサート」サービス管理ポータル及び/又は関連 API（以下「**ポータル**」といいます）若しくは発行された「証明書」で特定される者に対して発行する各電子証明書（以下「**証明書**」といいます）に適用します。「本証明書利用規約」は、「お客様」が「証明書」を申請した時期又は「証明書」が発行された時期にかかわらず適用されます。「本証明書利用規約」において、「お客様」を代理して「ポータル」にアクセスし、使用するためのアカウントを「**ポータルアカウント**」といいます。

By accepting or signing an agreement that incorporates these Certificate Terms of Use by reference (such agreement, together with these terms, collectively, the "**Agreement**"), the accepter or signer (the "**Signer**") represents and warrants that he/she (i) is acting as an authorized representative of the Customer on whose behalf the Signer is accepting this Agreement, and is expressly authorized to sign the Agreement and bind Customer to the Agreement, (ii) has the authority to obtain the digital equivalent of a company stamp, seal, or officer's signature to establish (x) the authenticity of Customer's website, and (y) that Customer is responsible for all uses of the Certificate, (iii) is expressly authorized by Customer to approve Certificate requests on Customer's behalf, and (iv) has or will confirm Customer's exclusive right to use the domain(s) to be included in any issued Certificates.
承諾者又は署名者（以下「**署名者**」といいます）は、「本証明書利用規約」をその一部として援用する契約書（当該契約書については、これら条件とともに、以下総称して「**援用契約**」といいます）を承諾又は署名することで、以下を表明し、これを保証します：「署名者」は、(i) 正当な権限を有する「お客様」の代理人として「お客様」に代わり援用契約」を承諾するものであること、及び「援用契約」に署名し「お客様」を「援用契約」で拘束する権限を明示的に付与されていること；(ii) 以下を証明するため、会社の印章、印鑑又は役員の署名に相当するものの電子版を取得する権限を有すること：(x)「お客様」のウェブサイトの真正性、及び (y)「お客様」が「証明書」の利用すべてについて責任を負うこと；(iii)「お客様」を代理して「証明書」申請を承認する権限を「お客様」から明示的に付与されていること；及び (iv) 発行される「証明書」に記載されるドメインを利用する「お客様」の独占的な権利を有するか又は確証すること。

With respect to any Certificates issued by DigiCert to Customer hereunder, the parties acknowledge and agree that the Certificate Terms of Use together with the Agreement constitutes the subscriber agreement, as required under the applicable industry standards, guidelines and requirements related to the issuance of Certificates (including the EV Guidelines, as defined in Section 1).
「本証明書利用規約」に基づき「デジサート」が「お客様」に対し発行する「証明書」について、両当事者は、「本証明書利用規約」を「援用契約」とあわせ、「証明書」の発行に関して適用される業界規格、ガイドライン及び要件（以下に定義する「EV ガイドライン」を含みます）に基づき要求されるサブスクライバー契約書とみなすことを承認し、これに合意します。

Customer and DigiCert hereby agree as follows:
「お客様」及び「デジサート」は、本書をもって、以下のとおり合意します：

1. **Account Users.**
   アカウント利用者.

Customer authorizes each individual listed as an administrator in the Portal Account to act as a Certificate Requester, Certificate Approver, and Contract Signer (as defined in the EV Guidelines) and to communicate with DigiCert regarding the management of Certificates and key sets. "**EV Guidelines**" means the Extended Validation Guidelines published by the CA/Browser Forum ("**CAB Forum**") and made publicly available at www.cabforum.org. Customer may revoke this authority by sending notice to DigiCert. Customer is responsible for periodically reviewing and reconfirming which individuals have

authority to request and approve Certificates. If Customer wishes to remove a Portal Account user, Customer will take the steps necessary to prevent such user's access to the Portal, including changing its password and other authentication mechanisms for its Portal Account. Customer must notify DigiCert immediately if any unauthorized use of the Portal or Portal Account is detected. Customer affirms that: (i) Customer authorizes DigiCert to scan, gather, and collect data pertinent to DigiCert's services and to automate Certificate renewal and upgrade; (ii) Customer will use the services to scan and automate only the domains, IP addresses, or assets that Customer owns or controls; (iii) Customer will use the services only for its intended purpose as described and marketed by DigiCert and in accordance with the DigiCert Acceptable Use Policy located at https://www.digicert.com/legal-repository.

「お客様」は、「ポータルアカウント」に管理者として記載される各個人に対し、「証明書申請者」、「証明書承認者」及び「契約署名者」（「EV ガイドライン」に定義します）として行動し、「証明書」及び「鍵セット」の管理について「デジサート」と連絡する権限を付与します。「**EV ガイドライン**」とは、CA/Browser Forum （以下「**CAB フォーラム**」といいます） が発行し、www.cabforum.org で一般に閲覧可能な Extended Validation Guidelines をいいます。「お客様」は、「デジサート」に通知することで、当該権限を撤回できるものとします。「お客様」は、いずれの者が「証明書」を申請し承認する権限を有するか定期的に見直し、再確認する責任を負うものとします。「お客様」は、「ポータルアカウント」利用者の削除を希望する場合、当該利用者の「ポータルアカウント」パスワードその他の認証方法の変更を含む、当該利用者による「ポータル」へのアクセスを防止する措置を講じるものとします。「お客様」は、「ポータル」又は「ポータルアカウント」の不正利用が発覚した場合、直ちに「デジサート」に通知しなければいけません。「お客様」は、以下を確約します：(i)「お客様」は、「デジサート」に対し、「デジサート」のサービスに関連するデータをスキャン、蓄積及び収集し、並びに「証明書」の更新及びアップグレードを自動化する権限を付与すること；(ii)「お客様」は、「お客様」が保有又は管理するドメイン、IP アドレス又は資産のスキャンを自動化するためにのみサービスを利用すること；及び (iii)「お客様」は、「デジサート」が定め販売する「お客様」の使用目的についてのみ、https://www.digicert.com/legal-repository/ にあるデジサート利用規約に従ってサービスを利用すること。

2. Requests.
申請.

Customer may request Certificates only for domain names registered to Customer, an affiliate of Customer, or other entity that expressly authorizes DigiCert to allow Customer to obtain and manage Certificates for the domain name. DigiCert may limit the number of domain names that Customer may include in a single Certificate in DigiCert's sole discretion.

「お客様」は、「お客様」、「お客様」の関係会社その他該当ドメイン名について「証明書」を取得し管理することを「お客様」に許可する権限を「デジサート」に明示的に付与した者に登録されたドメイン名についてのみ、「証明書」を申請できるものとします。「デジサート」は、その単独の裁量で、「お客様」が単一の「証明書」に含めることができるドメイン名の数を制限できるものとします。

3. Verification.
認証.

After receiving a request for a Certificate from Customer, DigiCert will review the request and attempt to verify the relevant information in accordance with the DigiCert Certification Practices Statement and applicable industry standards, guidelines and requirements, including laws and regulations related to the issuance of Certificates ("**Industry Standards**"). Verification of such requests is subject to DigiCert's sole discretion, and DigiCert may refuse to issue a Certificate for any reason or no reason. DigiCert will notify Customer if a Certificate request is refused but DigiCert is not required to provide a reason for the refusal. **"Certificate Practices Statement"** or **"CPS"** means the applicable written statements of the policies and practices used by DigiCert to operate its public key infrastructure ("**PKI**"), including applicable Time-Stamp Policies and Statements. DigiCert's CPSs are available at https://www.digicert.com/legal-repository. CPSs for services issued from a QTSP (as defined in Section 10) (whether acting in its capacity as a QTSP or otherwise) or an affiliate entity are available at https://www.quovadisglobal.com/repository.

「デジサート」は、「お客様」から「証明書」の申請を受領すると当該申請を審査し、デジザート「認証局運用規程」並びに「証明書」の発行に関する適用法令を含む業界規格、ガイドライン及び要件（以下「**業界規格**」といいます）に従って関連情報の認証を試みます。当該申請の認証は「デジサート」の単独の裁量によるものとし、「デジサート」は、いかなる理由の有無を問わず、「証明書」の発行を拒否できるものとします。「証明書」発行申請が却下された場合、デジザートは「お客様」に通知しますが、その理由を説明する義務を負わないのとします。「**認証局運用規程**」又は「**CPS**」とは、公開鍵インフラ（以下「**PKI**」といいます）を運営するために「デジサート」が採用する方針及び運用に関する該当声明書をいい、適用されるタイムスタンプ方針及び声明を含みます。「デジサート」の「CPS」は、https://www.digicert.com/legal-repository で閲覧可能です。「QTSP」（第 10 条に定義します）（「QTSP」としての自己の資格において行為するか又はその他であるかにかかわらず）又は関係会社から発行されるサービス用の「CPS」は、https://www.quovadisglobal.com/repository で閲覧可能です。

4. Certificate Life Cycle.
証明書ライフサイクル.

The lifecycle of an issued Certificate depends on the selection made by Customer when ordering the Certificate, the requirements in the CPS, and the intended use of the Certificate. DigiCert may modify Certificate lifecycles for unissued Certificates as necessary to comply with requirements of: (i) the Agreement; (ii) Industry Standards; (iii) DigiCert's auditors; or (iv) an Application Software Vendor. "**Application Software Vendor**" means an entity that displays or uses Certificates in connection with a distributed root store in which DigiCert participates or will participate. Customer agrees to cease using a Certificate and its related Private Key (defined below) after the Certificate's expiration date or after DigiCert revokes a Certificate as permitted in the Agreement.
発行された「証明書」のライフサイクルは、「証明書」申請時の「お客様」の選択、「CPS」の要件及び「証明書」の意図する用途によります。「デジサート」は、以下の要件に準拠するため必要に応じ、未発行「証明書」のライフサイクルを変更できるものとします：(i)「援用契約」；(ii)「業界規格」；(iii)「デジサート」の監査人；又は (iv)「アプリケーションソフトウェアベンダー」。「**アプリケーションソフトウェアベンダー**」とは、「デジサート」が参加し又は参加する分散ルートストアに関連して「証明書」を表示又は使用する者をいいます。「証明書」の終了日後、又は「援用契約」に従って「デジサート」が「証明書」を失効させた後、「お客様」は、「証明書」及び関連「秘密鍵」（以下に定義します）の使用を停止することに同意します。

5. Issuance.
発行.

If verification of a Certificate is completed to DigiCert's satisfaction, DigiCert will issue and deliver the requested Certificate to Customer using any reasonable means of delivery. Typically, DigiCert will deliver Certificates via email to an address specified by Customer as an electronic download in the Portal or in response to an API call made by Customer via the Portal. Publicly-trusted Certificates are issued from a root or intermediate Certificate selected by DigiCert. DigiCert may change which root or intermediate certificate is used to issue Certificates at any time and without notice to Customer. Customer will abide by all applicable laws, regulations and Industry Standards when ordering and using Certificates, including United States export control and economic sanctions laws and regulations. Customer acknowledges that the Certificates are not available in countries or regions restricted by the United States Treasury Department's Office of Foreign Assets Control, the United States Commerce Department, the European Commission, the United Kingdom HM Treasury's Office of Financial Sanctions Implementation, or other applicable governmental agencies having jurisdiction over DigiCert.
「証明書」の認証が「デジサート」が満足する程度に完了した場合、「デジサート」は、申請された「証明書」を発行し、合理的な方法で「お客様」に引き渡すものとします。一般的に、「デジサート」は、「お客様」が指定したアドレスに送信する電子メールを通じて（「ポータル」での電子的ダウンロードとして）、又は「お客様」が「ポータル」を通じた行った API コールに応じ「証明書」を引渡すものとします。公的に信頼される「証明書」は、「デジサート」が選択する「ルート証明書」又は「中間証明書」から発行されます。「デジサート」は、いつでも、「お客様」へ通知することなく、「証明書」を発行するために使用する「ルート証明書」又は「中間証明書」を変更できるものとします。「お客様」は、「証明書」申請及び利用にあたり、米国輸出管理及び経済制裁法令を含むすべての適用法令、規制及び「業界規格」を遵守するものとします。「お客様」は、米国財務省外国資産管理局、米国商務省）、欧州委員会、英国財務省金融制裁実施庁その他の「デジサート」に管轄権を有する関係政府機関によって規制される国又は地域では「証明書」は利用できないことを承認します。

6. Certificate License.
証明書ライセンス.

Effective immediately upon initiating a request for a Certificate and continuing until the Certificate expires or is revoked, Customer may only use, for the benefit of the Certificate's subject, each issued Certificate and related services (whether performed before or after issuance of the Certificate) and corresponding Key Set for the purposes described in the CPS, in accordance with all applicable laws, regulations, Industry Standards, and with the terms herein. Any Certificates trusted by Application Software Vendors are subject to all applicable Industry Standards requirements, including those found in applicable Application Software Vendor root store policies and the CPS, regardless of how the Certificates are used. Any use that is not allowed by applicable Industry Standards or the CPS is not permitted. DigiCert strongly discourages certificate or key pinning, using Certificates trusted for the web with non-web PKI, or any other use of Certificates that would make it difficult for Customer to meet the revocation timelines or other requirements of the CPS, and any such use will not be considered a sufficient reason to delay revocation. "**Key Set**" means a set of two or more mathematically related keys, referred to as Private Keys or key shares along with a Public Key, wherein (i) the Public Key can encrypt a message which only the Private Key(s) can decrypt, and (ii) even knowing the Public Key, it is computationally infeasible to discover the Private Key(s). Customer will promptly inform DigiCert if it becomes aware of any misuse of a Certificate, Private Key, or

the Portal. Customer is responsible for obtaining and maintaining any authorization or license necessary to order, use, and distribute a Certificate to end users and systems, including any license required under United States' export laws. SSL Certificates may be used on one or more physical server or device at a time; however, DigiCert may charge a fee for use of Certificates on additional servers or devices.
「証明書」申請の開始により直ちに有効とし、「証明書」が終了するか又は失効されるまで継続して、「お客様」は、すべての適用法令、規制、「業界規格」、及び「本証明書利用規約」の条件に従って、「証明書」の被認証者の利益のために、「CPS」に記載された目的についてのみ、各発行済み「証明書」及び関連サービス（その実施が「証明書」の発行の前後であるかは問いません）並びに対応する「鍵セット」を使用できるものとします。「アプリケーションソフトウェアベンダー」が信頼するすべての「証明書」は、その使用態様にかかわらず、適用される「アプリケーションソフトウェアベンダー」ルートストア方針及び「CPS」の要件を含む、適用されるすべての「業界規格」要件に従います。適用される「業界規格」又は「CPS」で認められない、いかなる使用も許可されません。「デジサート」は、Web 用の信頼される「証明書」の非 Web PKI との使用その他「お客様」が失効期間その他の「CPS」の要件を満たすことを困難にするような「証明書」を使用する証明書又は鍵ピンニングに反対し、いかなる当該使用も、失効を延期するに足りる相当な理由とはみなさないものとします。「**鍵セット**」とは、(i)「秘密鍵」でのみ復号化できる通信の「公開鍵」による暗号化を可能とし、及び (ii)「公開鍵」がわかっていても「秘密鍵」の解読が計算時間の点で実行不可能な、「公開鍵」と一対の「秘密鍵」又は共通鍵と呼ばれる、数学的に関連する二つ以上の鍵一式をいいます。「お客様」は、「証明書」若しくは「秘密鍵」又は「ポータル」の不正使用を発見した場合、直ちに「デジサート」に通知するものとします。「お客様」は、「証明書」の申請、使用、及びエンドユーザー及びシステムに配布するために必要な許認可又はライセンス（米国輸出規制法令で要求されるライセンスを含みます）を取得、保持する責任を負うものとします。SSL「証明書」は、一度に一つ以上の物理サーバー又はデバイス上で使用できるものとします。但し、「デジサート」は、追加サーバー又はデバイス上での「証明書」の使用について料金を請求できるものとします。

7. Key Sets.
鍵セット.

A "**Private Key**" means the key that is kept secret by Customer that is used to create digital signatures and/or decrypt electronic records or files that were encrypted with the corresponding Public Key. A "**Public Key**" means Customer's publicly-disclosed key that is contained in Customer's Certificate and corresponds to the secret Private Key that Customer uses. Customer must (i) generate Key Sets using trustworthy systems, (ii) use Key Sets that are at least the equivalent of RSA 2048 bit keys, and (iii) keep all Private Keys confidential. Customer is solely responsible for any failure to protect its Private Keys. Customer represents that it will only generate and store Key Sets for Adobe Signing Certificates and EV Code Signing Certificates on a FIPS 140-2 Level 2 device. All other Certificate types may be stored on secure software or hardware systems. Customer is responsible for ensuring that Customer's acquisition, use, or acceptance of Key Sets generated by DigiCert in accordance with the Agreement complies with applicable local laws, rules and regulations – including but not limited to export and import laws, rules, and regulations – in the jurisdiction in which Customer acquires, uses, accepts or otherwise receives such Key Sets. If Customer is permitted to import or export Private Keys (including copies) in connection with its use of specific DigiCert services, DigiCert will not be liable to Customer for Customer's use or storage of Private Keys (including copies) that are not created in the applicable Portal or service or that are used outside such Portal or service, including after they are exported from the applicable Portal or service.
「**秘密鍵**」とは、「お客様」が秘匿する鍵で、電子署名の作成及び/又は対応する「公開鍵」で暗号化された電子記録又はファイルを復号化するために使用される鍵をいいます。「**公開鍵**」とは、「お客様」が一般に公開する鍵で、「お客様」の「証明書」に含まれ、「お客様」が使用する「秘密鍵」に対応するものをいいます。「お客様」は、(i) 信頼性の高いシステムを使用して「鍵セット」を生成し、(ii) 少なくとも RSA 2048 ビット鍵と同等の「鍵セット」を使用し、及び (iii) すべての「秘密鍵」を秘匿しなければいけません。「お客様」は、「秘密鍵」を保護しなかったことについて全責任を負うものとします。「お客様」は、Adobe サイニング証明書及び EV コードサイニング「証明書」用の「鍵セット」を FIPS 140-2 Level 2 のデバイス上でのみ生成、保管することを表明します。他のすべての種類の「証明書」は、セキュアなソフトウェア又はハードウェアシステム上で保管できるものとします。「お客様」は、「デジサート」が「援用契約」に従って生成した「鍵セット」を取得、使用又は受領するにあたり、適用される現地の法令、規則及び規制を確実に遵守するよう責任を負います。当該適用法令、規則及び規制には、「お客様」が当該「鍵セット」を取得、使用その他方法により受領する裁判管轄内の輸出入規制法、規則及び規制が含まれますが、これらに限定するものではありません。「お客様」が特定の「デジサート」サービスの利用に関連する「秘密鍵」（その複製を含みます）を輸入又は輸出する許可を得ている場合であっても、「デジサート」は、「お客様」に対し、「秘密鍵」（その複製を含みます）が該当「ポータル」又はサービスから輸出された後のことを含め，当該「ポータル」又はサービス内で生成されていないか、又は当該「ポータル」又はサービス外で使用されている「秘密鍵」（その複製を含みます）の「お客様」による使用又は保管について責任を負わないものとします。

8. Publication of Certificate Information.
証明書情報の公表.

Notwithstanding anything in these Certificate Terms of Use or any other agreement between Customer and DigiCert to the contrary, Customer consents to: (i) DigiCert's public disclosure of information (such as Customer's domain name, jurisdiction of incorporation, or contact information), embedded in an issued Certificate; and (ii) Customer's Certificates and information embedded therein being logged by or on behalf of DigiCert in publicly-accessible Certificate transparency databases for purposes of detecting and preventing phishing attacks and other forms of fraud, and Customer agrees that such information when logged may not be removed from a log server. Such publication of Certification information will be in accordance with the applicable CPS.
「本証明書利用規約」又はその他の「お客様」と「デジサート」との間の契約の別段の定めにかかわらず、「お客様」は、(i) 発行された「証明書」に埋め込まれた情報（「お客様」のドメイン名、会社設立地又は連絡先情報等）を「デジサート」が公表すること；及び (ii)「お客様」の「証明書」及び当該「証明書」に埋め込まれた情報を、フィッシング攻撃及びその他の形態の詐欺の検知及び防止することを目的に、「デジサート」自ら又は第三者をして一般に公表される「証明書」透明性データベースに記録することに同意し、また「お客様」は、当該情報は、記録された場合、ログサーバーから削除できないことに合意します。「証明書」情報の当該公表は、適用される「CPS」に従うものとします。

9. Client Certificates.
クライアント証明書.

"**Client Certificate**" means a Certificate that contains any extendedKeyUsage other than codeSigning, timestamping or serverAuthentication. The Client Certificate uses are varied and are defined by the Client Certificate profile. Some of the possible uses defined in a Client Certificate profile may include, digital signature, email encryption, and cryptographic authentication. If Customer wishes to request Client Certificates, Customer must (i) confirm the identity and affiliation of the requester using appropriate internal documentation as prescribed the CPS, and (ii) confirm that the information provided and representations related to or incorporated in any Client Certificate are true, complete, and accurate in all material respects.
「**クライアント証明書**」とは、コードサイニング、タイムスタンプ又はサーバー認証以外のすべての拡張鍵用途を含む「証明書」をいいます。「クライアント証明書」の用途は多種多様で、「クライアント証明書」のプロファイルで定義されます。「クライアント証明書」のプロファイルで定義される利用法としては、電子署名、電子メールの暗号化及び暗号認証があります。「お客様」は、「クライアント証明書」の申請を希望する場合、 (i)「CPS」の定めに従って、適切な社内文書を利用して申請者の身元及び所属を確認し、(ii)「クライアント証明書」で提供される情報及び「クライアント証明書」に関連するか又はその一部を構成する表明がすべての重要な点において真正、完全及び正確であることを確認しなければいけません。

10. Qualified Certificates.
適格証明書.

"**Qualified Certificate**" means a Certificate (i) that is issued by a Qualified Trust Service Provider pursuant to the requirements of applicable EU or Swiss certification and electronic signature laws, and (ii) that carries the highest assurance level of "qualified" pursuant to such requirements.
「**適格証明書**」とは、(i) 適用される欧州連合又はスイス連邦の証明書及び電子署名法の要件に従って「適格トラストサービスプロバイダー」によって発行され、(ii) 当該要件に従った最高水準の"適格保証" を有する「証明書」をいいます。

"**Qualified Trust Service Provider**" or "**QTSP**" means an affiliate entity of DigiCert that is certified by governmental authorities to issue Qualified Certificates. DigiCert's QTSP's are as follows:
「**適格トラストサービスプロバイダー**」あるいは「**QTSP**」とは、政府機関により「適格証明書」を発行することを認証された「デジサート」の関係会社をいいます。「デジサート」の「QTSP」は、以下のとおりです：

QTSP Entity **QTSP 会社**	**Trusted List** **トラストリスト**	**Jurisdiction of Supervisory Body** **監督機関の管轄区域**
QuoVadis Trustlink B.V.	Netherlands Trusted List オランダ・トラストリスト	Netherlands オランダ王国
DigiCert Europe Belgium B.V.	Belgium Trusted List ベルギー・トラストリスト	Belgium ベルギー王国
QuoVadis Trustlink Schweiz AG	Swiss Trusted List スイス・トラストリスト	Switzerland スイス連邦

"**QTSP Services**" means services issued by DigiCert's QTSP (as defined above) (whether acting in its capacity as QTSP or otherwise) or its affiliates.
「**QTSP サービス**」とは、「デジサート」の「QTSP」（上記に定義します）（「QTSP」としての自己の資格において行為するか又はその他であるかにかかわらず）又は「デジサート」の関係会社の「QTSP」が発行するサービスをいいます。

If Customer purchases QTSP Services, then the applicable CPS for certain such QTSP Services is located at https://www.quovadisglobal.com/repository/. With respect to Qualified Certificates, Customer will (i) where use of a Qualified Signature Creation Device (QSCD) is required by Industry Standards, only use its Qualified Certificates for electronic signatures generated using the QSCD storing the Qualified Certificates, (ii) if Customer is a natural person, maintain and use their Private Keys only under their sole control; and (iii) if Customer is a legal entity or organization, maintain and use its Private Keys only under its control and direction.
「お客様」が「QTSP サービス」を購入する場合、そのときは、特定の当該「QTSP サービス」について適用される「CPS」は https://www.quovadisglobal.com/repository/ に掲載されています。「適格証明書」について、「お客様」は、(i)「業界規格」により適格電子署名生成装置 (QSCD) の使用が要求される場合、「適格証明書」を保管する QSCD を使用して生成された電子署名についてのみ「適格証明書」を使用し、(ii)「お客様」が自然人の場合、自己の単独の管理下のみに置かれた自己の「秘密鍵」を保全、使用し、(iii)「お客様」が法人又は組織の場合、自己の単独の管理及び監督下のみに置かれた自己の「秘密鍵」を保全、使用するものとします。

11. Management.
管理.

DigiCert will generally issue, manage, renew, and revoke a Certificate in accordance with any instructions submitted by Customer through the Portal and may rely on such instructions as accurate. Customer will provide accurate and complete information when communicating with DigiCert and will notify DigiCert within 5 Business Days if any information relating to its account on the Portal changes. Customer will respond to any inquiries from DigiCert regarding the validity of information provided by Customer within 5 Business Days after Customer receives notice of the inquiry. Customer will review and verify the Certificate data prior to using the Certificate for accuracy. Certificates are considered accepted by Customer thirty (30) days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Customer used the Certificate. Although DigiCert may send a reminder about expiring Certificates, DigiCert is under no obligation to do so and Customer is solely responsible for ensuring Certificates are renewed prior to expiration. "**Business Day**" means Monday through Friday, excluding U.S. Federal Holidays, which are set forth in 5 U.S.C. § 6103.
「デジサート」は、通常、「ポータル」を通じて「お客様」から提示された指示に従い、「証明書」を発行、管理、更新及び失効させるものとしますが、これは当該指示が正確であるという信頼を基礎とします。「お客様」は、「デジサート」との連絡に際し正確で完全な情報を提供するものとし、「ポータル」上のアカウントに関する情報に変更がある場合、5「営業日」以内に「デジサート」に通知するものとします。「お客様」は、「お客様」が提供した情報の有効性について「デジサート」から問合せがある場合、当該問合せの通知を受領してから 5「営業日」以内に応答するものとします。「お客様」は、「証明書」を使用する前に、その正確性について「証明書」のデータを照合、確認するものとします。「証明書」は、その発行から 30 日後、又はそれ以前であっても「お客様」が「証明書」を使用した証拠がある場合はその使用時に承認されたものと見なします。「デジサート」は期間終了が迫った「証明書」について通知することがありますが、通知すべき義務を何ら負うものではなく、「お客様」は、期限終了前に「証明書」を確実に更新することについて全責任を負うものとします。「**営業日**」とは、米国連邦規則集第 5 巻パート 6103 で規定されている米国の連邦祝日を除く月曜日から金曜日をいいます。

12. Registration Authority.
登録局.

Except for publicly-trusted TLS/SSL Certificates and Qualified Certificates, Customer is appointed as a Registration Authority (and Customer hereby accepts such appointment) pursuant to the terms of the applicable CPS. In connection with publicly-trusted TLS/SSL Certificates, Customer is appointed as an Enterprise RA (and Customer hereby accepts such appointment) pursuant to the terms of the applicable CPS. To the extent that Customer performs any functions of a Registration Authority or Enterprise RA, it will do so in compliance with the applicable CPS, and DigiCert may rely on Customer's actions when acting as a Registration Authority or Enterprise RA. To the extent any third-party claim, suit, proceeding or judgment arises from Customer's failure to strictly comply with the obligations of a Registration Authority or Enterprise RA, Customer must defend, hold harmless, and indemnify DigiCert and its directors, officers, agents, employees, successors and assigns from such claim. If operating as a Registration Authority or Enterprise RA, Customer will cause its subscribers receiving Certificates hereunder to abide by the terms of the DigiCert subscriber agreement, found at https://www.digicert.com/subscriber-agreement-jp. Subscribers of Customer must accept the subscriber agreement

before receiving Certificates. "**Enterprise RA**" has the meaning given to it in the current version of the CAB Forum Baseline Requirements, available at https://cabforum.org/baseline-requirements-documents/, as updated from time to time.
公的に信頼される TLS/SSL「証明書」及び「適格証明書」の場合を除き、「お客様」は、適用される「CPS」の条件に従って「登録局」に指名されます（「お客様」は、本書をもって当該指名を承諾します）。公的に信頼される TLS/SSL「証明書」に関し、「お客様」は、適用される「CPS」の条件に従って「エンタープライズ 登録局」に指名されます（「お客様」は、本書をもって当該指名を承諾します）。「お客様」が「登録局」又は「エンタープライズ 登録局」の役割を果たす限度において、「お客様」は、適用される「CPS」に従って当該役割を果たすものとし、「デジサート」は、「登録局」又は「エンタープライズ 登録局」として行う「お客様」の行為に依拠できるものとします。第三者の請求、訴訟、訴訟手続き又は判決が、「お客様」が「登録局」又は「エンタープライズ 登録局」の義務を厳に遵守しなかったことに起因する限度において、「お客様」は、「デジサート」並びにその取締役、役員、代理人、従業員、継承人及び譲受人を当該請求から防御、補償し、損害を被らないようにしなければいけません。「お客様」は、「登録局」又は「エンタープライズ 登録局」として行動する場合、「本証明書利用規約」に基づく「証明書」を受け取るサブスクライバー（登録者）に、https://www.digicert.com/subscriber-agreement-jp にあるデジサート・サブスクライバー契約書の条件を遵守させるものとします。「お客様」のサブスクライバー（登録者）は、「証明書」を受け取る前にサブスクライバー契約書を承諾しなければいけません。「**エンタープライズ登録局**」とは、https://cabforum.org/baseline-requirements-documents/で閲覧可能な"CAB フォーラム基本要件"の最新版においてこれに付与された意義を有します。

13. Security and Use of Key Sets.
セキュリティ及び鍵セットの使用.

Customer will securely generate and protect the Key Sets associated with a Certificate and take all steps necessary to prevent the compromise, loss, or unauthorized use of a Private Key associated with a Certificate. Customer will use passwords that meet the requirements specified by the CAB forum network security requirements and other relevant requirements to meet best practices. Customer will only allow Customer's employees, agents, and contractors to access or use Private Keys if the employee, agent, or contractor has undergone a background check by Customer (to the extent allowed by law) and has training or experience in PKI and other information security fields. Customer will notify DigiCert, request revocation of a Certificate and its associated Private Key, cease using such Certificate and its associated Private Key, and remove the Certificate from all devices where it is installed if: (i) any information in the Certificate is or becomes incorrect or inaccurate, or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate. For code signing Certificates, Customer will promptly cease using a Certificate and its associated Private Key and promptly request revocation of the Certificate if Customer believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect Code. "**Suspect Code**" means code that contains harmful or malicious functionality of any kind or that contains serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes. Customer will not use the same Private Key for different Certificate types. For example, Customer will not use a Private Key that is used for code signing to request a non-code signing Certificate. If DigiCert detects that a Private Key that has been used for a certain Certificate type or action (e.g., code signing) is being used to request a different Certificate type (e.g., TLS/SSL or Client Certificate), then DigiCert will be required to revoke all Certificates associated with such Private Key or related Key Set that are in Customer's related Portal Account or that have otherwise been issued by DigiCert. Customer will respond to DigiCert's instructions concerning Key Set compromise or Certificate misuse within 24 hours. Customer will promptly cease using the Key Set corresponding to a Certificate upon the earlier of (I) revocation of the Certificate, and (II) the date when the allowed usage period for the Key Set expires. After revocation, Customer must cease using the Certificate.
「お客様」は、「証明書」と関連付けられた「鍵セット」を安全に生成、保護し、「証明書」と関連付けられた「秘密鍵」の危殆化、紛失又は不正使用を防止するために必要なすべての手段を講じるものとします。「お客様」は、"CAB フォーラムネットワークセキュリティ要件"及びベストプラクティスを満たすための他の関連する要件を満たすパスワードを使用するものとします。「お客様」は、自己の従業員、代理人及び請負業者が「お客様」による身元調査（法律で許容される範囲で）を受け、かつ、「PKI」及び他の情報セキュリティ分野の研修を既に受けているか又は経験を有している場合に、該当従業員、代理人又は請負業者にのみ「秘密鍵」へのアクセス又は使用を許可するものとします。以下のいずれかの場合、「お客様」は、「デジサート」に通知し、「証明書」及び関連付けられた「秘密鍵」の失効を申請し、当該「証明書」及び関連付けられた「秘密鍵」の使用を停止し、当該「証明書」がインストールされたすべてのデバイスからその「証明書」を削除するものとします：(i)「証明書」中のいずれか情報が不正確であるか又は不正確になった場合；又は (ii)「証明書」に含まれる「公開鍵」に関連付けられた「秘密鍵」の悪用又は危殆化が疑われる場合。コードサイニング「証明書」について、「お客様」は、以下の状況にあると考える場合、速やかに「証明書」及び関連付けられた「秘密鍵」の使用を停止し、「証明書」の失効を申請するものとします：(a)「証明書」中のいずれか情報が不正確であるか又は不正確になった場合；(b)「証明書」に含まれる「公開鍵」に関連付けられた「秘密鍵」が悪用又

は危殆化された場合；又は (c)「サスペクトコード」に署名するために「証明書」が使用された形跡がある場合。「**サスペクトコード**」とは、有害若しくは悪意のあるあらゆる種類の機能又は深刻な脆弱性を包含するコードをいい、スパイウェア、マルウェアその他の使用者の同意なくインストールされ及び/又は削除不能なコード、並びに設計者の意図していない方法で不正利用可能なコードで、それが実行されるプラットフォームの信頼性を損なうものを含みます。「お客様」は、異なる種類の「証明書」について、同一の「秘密鍵」を使用しないものとします。例えば、「お客様」は、非コードサイニング「証明書」を申請するために、コード署名に使用される「秘密鍵」を使用しないものとします。「デジサート」は、特定の種類又は機能の「証明書」（例えば、コードサイニング）について既に使用されている「秘密鍵」が、異なる種類の「証明書」（例えば、TLS/SSL 又は「クライアント証明書」）を申請するために使用されていることを発見した場合、「お客様」の関連「ポータルアカウント」にある「秘密鍵」若しくは関連する「鍵セット」と関連付けられた「証明書」、又は「デジサート」が既に発行したその他の「証明書」をすべて失効させなければなりません。「お客様」は、「鍵セット」の危殆化や「証明書」の悪用に関する「デジサート」の指示に 24 時間以内に応答するものとします。「お客様」は、以下のいずれか早く到来する時に、「証明書」に対応する「鍵セット」の使用を速やかに停止するものとします：(I)「証明書」の失効；及び (II)「鍵セット」の許可された使用期間が終了した日。「お客様」は、失効後、該当「証明書」の使用を停止しなければいけません。

If Customer stores a Private Key that has been generated for a code signing Certificate in an HSM (as defined in the applicable CPS), then Customer agrees with respect to each such Private Key that (w) Customer stores its Private Key securely in an HSM that prevents removal of the Private Key, (x) the HSM is either in sole control of Customer or utilized through an audited cloud (e.g., Azure or AWS), (y) Customer has no cause to believe such Private Key has been or ever will be used outside of the HSM, and (z) the Private Key is protected in a crypto module that meets or exceeds FIPS 140-2 level 2 (or equivalent) or Common Criteria EAL4+.
「お客様」がコードサイニング「証明書」に対して生成された「秘密鍵」を「HSM」（適用される「CPS」に定義します）に保管する場合、そのときは、「お客様」は、各当該「秘密鍵」について、次の各号に掲げる事項に合意します：(w)「お客様」は、自己の「秘密鍵」を「秘密鍵」の持ち出しを防止する「HSM」にセキュアに保管すること；(x)「HSM」は、「お客様」単独の管理下にあるか、又は第三者による監査を受けたクラウドサービス（例えば、Azure 又は AWS）を通じて利用されること；(y) 当該「秘密鍵」は「HSM」外で利用されており、今後も「HSM」外で利用されるだろうとの考えを正当化する理由はないこと；及び (z)「秘密鍵」を FIPS 140-2 レベル 2（又は同等の規格）又は Common Criteria EAL4+を満たす又は超過する暗号化モジュールで保護すること。

14. Defective Certificates.
欠陥ある証明書.

Customer's sole remedy for a defect in a Certificate ("**Defect**") is to require DigiCert to use commercially reasonable efforts to cure the defect after receiving notice of such Defect from Customer. DigiCert is not obligated to correct a Defect if (i) Customer misused, damaged, or modified the Certificate, (ii) Customer did not promptly report the Defect to DigiCert, or (iii) Customer has breached any provision of the Agreement.
「証明書」の欠陥（以下「**欠陥**」といいます）に対する「お客様」の唯一の救済手段は、「お客様」から「欠陥」の通知を受領した後、当該「欠陥」を是正すべく商業的に合理的な努力をするよう「デジサート」に要求することです。「デジサート」は、以下のいずれの場合も、「欠陥」を是正する義務を負いません：(i)「お客様」が「証明書」を悪用、損壊又は改変した場合；(ii)「お客様」が、「デジサート」に対し、速やかに「欠陥」を報告しなかった場合；又は (iii)「お客様」が「援用契約」のいずれか規定に違反した場合。

15. Relying Party Warranty.
依拠当事者保証.

Customer acknowledges that the Relying Party Warranty is only for the benefit of Relying Parties. "**Relying Party Warranty**" means a warranty offered to a Relying Party that meets the conditions found in the Relying Party Agreement and Limited Warranty posted on DigiCert's website at https://www.digicert.com/legal-repository. The Relying Party Warranty for Certificates issued from a QTSP or a DigiCert affiliate is posted at https://www.quovadisglobal.com/repository. Customer does not have rights under the Relying Party Warranty, including any right to enforce the terms of the Relying Party Warranty or make a claim under the Relying Party Warranty. "**Relying Party**" has the meaning set forth in the Relying Party Warranty. An Application Software Vendor is not a Relying Party when the software distributed by the Application Software Vendor merely displays information regarding a Certificate or facilitates the use of the Certificate or digital signature.
「お客様」は、「依拠当事者保証」が依拠当事者の利益にのみ帰するものであることを承認します。「**依拠当事者保証**」とは、「デジサート」のウェブサイト https://www.digicert.com/legal-repository に掲載される依拠当事者契約及び限定保証 (Relying Party Agreement and Limited Warranty) の条件を満たす、依拠当事者に提供される保証をいいます。「QTSP」又は「デジサート」

の関係会社から発行される「証明書」の「依拠当事者保証」は、https://www.quovadisglobal.com/repository にあるウエブサイトに掲載されます。「お客様」は、「依拠当事者保証」の条件を強制し又は「依拠当事者保証」に基づく請求を行う権利を含む、「依拠当事者保証」に基づくなんらの権利も有しません。「**依拠当事者**」とは、「依拠当事者保証」において定める意義を有します。「アプリケーションソフトウェアベンダー」が頒布するソフトウェアが単に「証明書」に関する情報を表示するか、又は「証明書」若しくは電子署名の使用を円滑にするものである場合、「アプリケーションソフトウェアベンダー」は「依拠当事者」とはなりません。

16. Representations.
表明事項.

For each requested Certificate, Customer represents and warrants that:
申請された各「証明書」について、「お客様」は、以下を表明し、これを保証します：

a. Customer has the right to use or is the lawful owner of (i) any domain name(s) specified in the Certificate, and (ii) any common name or organization name specified in the Certificate;
「お客様」は、(i)「証明書」で指定されるドメイン名、及び (ii)「証明書」で指定されるコモンネーム又は団体名を使用する権限を有するか又は正当な所有者であること；

b. Customer will use the Certificate only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and will use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Certificate purpose, the CPS, any applicable certificate policy, and the Agreement;
「お客様」は、許可された合法的な目的についてのみ「証明書」を使用すること。これには、「サスペクトコード」を署名する為に「証明書」を使用しないこと、及びすべての適用法令を遵守し、「証明書」の目的、「CPS」、適用される証明書方針及び「援用契約」に従ってのみ「証明書」及び「秘密鍵」を使用することを含みます；

c. Customer has read, understands, and agrees to the CPS;
「お客様」は、「CPS」を読み理解したうえで、これに同意すること；

d. Customer will immediately report in writing to DigiCert any non-compliance with the CPS or Baseline Requirements; and
「お客様」は、「デジサート」に対し、「CPS」又はベースライン要件 (Baseline Requirements) の不遵守を書面をもって直ちに通知すること；及び

e. the organization included in the Certificate and the registered domain name holder is aware of and approves of each Certificate request.
「証明書」に含まれる組織で、登録ドメイン名の所有者である者が、各「証明書」の申請を認識し、承認していること。

17. Restrictions.
制限事項.

Customer will only use a TLS/SSL Certificate on the servers accessible at the domain names listed in the issued Certificate. Additionally, Customer will not:
「お客様」は、発行される「証明書」に記載されるドメイン名でアクセス可能なサーバー上でのみ、TLS/SSL「証明書」を使用するものとします。さらに「お客様」は、以下を行わないものとします：

a. modify, sublicense, or create a derivative work of any TLS/SSL Certificate (except as required to use the Certificate for its intended purpose) or Private Key;
TLS/SSL「証明書」（その本来の目的で「証明書」を使用する必要がある場合を除く）若しくは「秘密鍵」を修正、再許又はその派生物を作成すること；

b. upload or distribute any files or software that may damage the operation of another's computer;
他人のコンピュータの運用に被害を与えるようなファイル若しくはソフトウェアをアップロードし又は頒布すること；

c. make representations about or use a TLS/SSL Certificate except as allowed in the CPS;
「CPS」で許可される場合を除き、TLS/SSL「証明書」について表明を行い又は使用すること；

d. impersonate or misrepresent Customer's affiliation with any entity;
「お客様」といずれか団体との関係について偽証又は虚偽表示をすること；

e. use a Certificate or any related software or service (such as the Portal) in a manner that could reasonably result in a civil or criminal action being taken against Customer or DigiCert;
「証明書」又は関連ソフトウェア若しくはサービス（「ポータル」など）を、合理的に見て「お客様」若しくは「デジサート」に対する民事又は刑事訴訟をもたらすような方法で使用すること；

f. use a Certificate or any related software to breach the confidence of a third party or to send or receive unsolicited bulk correspondence;
「証明書」又は関連ソフトウェアを、第三者の秘密を侵害し若しくは未承認の大量通信を送信又は受信するために使用すること；

g. use code signing Certificates to sign Suspect Code;
「サスペクトコード」に署名するために、コードサイニング「証明書」を使用すること；

h. apply for a code signing Certificate if the Public Key in the Certificate is or will be used with a non-code signing Certificate;
「証明書」中の「公開鍵」が非コードサイニング「証明書」とともに使用されているか又は使用される場合に、コードサイニング「証明書」を申請すること；

i. interfere with the proper functioning of the DigiCert website or with any transactions conducted through the DigiCert website;
「デジサート」ウェブサイトの正常な機能又は「デジサート」ウェブサイトを通じて行われる取引を妨害すること；

j. attempt to use a Certificate to issue other Certificates;
他の「証明書」を発行するために「証明書」の使用を試みること；

k. monitor, interfere with or reverse engineer the technical implementation of the DigiCert systems or software or otherwise knowingly compromise the security of the DigiCert systems or software;
「デジサート」システム又はソフトウェアの技術的実装を監視、妨害若しくはリバースエンジニアリングし、又はその他の方法で「デジサート」システム又はソフトウェアのセキュリティを悪意で危殆化すること；

l. submit Certificate information to DigiCert that infringes the intellectual property rights of any third party;
「デジサート」に対し第三者の知的財産権を侵害する「証明書」情報を提出すること；

m. intentionally create a Private Key that is substantially similar to a DigiCert or third-party Private Key; or
「デジサート」又は第三者の「秘密鍵」と実質的に類似した「秘密鍵」を故意に作成すること；又は

n. Unless expressly authorized by DigiCert, in writing, Customer will not use any end-entity Certificate to sign any Certificate.
「デジサート」が書面をもって明示的に許可しない限り、「お客様」は、「証明書」に署名するためにエンドエンティティ「証明書」を使用しないものとします。

18. Certificate Revocation.
証明書の失効.

DigiCert may revoke a Certificate without notice for the reasons stated in the CPS, including if DigiCert reasonably believes that:
「デジサート」は、「CPS」に記載された理由で「証明書」を通知なく失効させることができますが、「デジサート」が、以下に該当すると合理的に考える場合を含みます：

a. Customer requested revocation of the Certificate or did not authorize the issuance of the Certificate;
「お客様」が「証明書」の失効を申請したか又は「証明書」の発行を許可していなかった場合；

b. Customer is using the Services, to post or make accessible any material that infringes DigiCert's or any third party's rights;
「お客様」が、「デジサート」又は第三者の権利を侵害する素材を掲載し又はアクセス可能な状態に置くためにサービスを利用している場合；

c. Customer has breached the Agreement or an obligation it has under the CPS;
「お客様」が「援用契約」又は「CPS」に基づく義務に違反した場合；

d. any provision of an agreement with Customer containing a representation or obligation related to the issuance, use, management, or revocation of the Certificate terminates or is held invalid;
「証明書」の発行、使用、管理又は失効に関する表明又は義務を含む「お客様」との契約の規定が解約又は無効と判断された場合；

e. Customer is added to a government prohibited person or entity list or is operating from a prohibited destination under the laws of the United States;
「お客様」が政府の取引禁止対象個人又は団体リストに追加されるか、又は米国の法令で輸出禁止対象とされる仕向地から事業活動を行なっている場合；

f. the Certificate contains inaccurate or misleading information;
「証明書」が不正確又は不実情報を含む場合；

g. the Certificate was used without authorization, outside of its intended purpose or used to sign Suspect Code;
「証明書」がその本来の目的以外に許可なく使用された場合、又は「サスペクトコード」に署名するために使用された場合；

h. the Private Key associated with the Certificate was disclosed or compromised;
「証明書」と関連付けられた「秘密鍵」が開示又は危殆化された場合；

i. the Certificate was (i) misused, (ii) used or issued contrary to law, the CPS, or Industry Standards, or (iii) used, directly or indirectly, for illegal or fraudulent purposes, such as phishing attacks, fraud, or the distribution of malware, other illegal or fraudulent purposes, or any other violations as outlined in the DigiCert Acceptable Use Policy; or
「証明書」が、(i) 悪用された場合；(ii) 法令、「CPS」若しくは「業界規格」に反して使用又は発行された場合；又は (iii) フィッシング攻撃、詐欺若しくはマルウェアの頒布、他の違法若しくは詐欺目的その他デジサート利用規約で概説されている違反行為などの違法又は詐欺目的で直接又は間接に使用された場合；又は

j. Industry Standards or DigiCert's CPS require Certificate revocation, or revocation is necessary to protect the rights, confidential information, operations, or reputation of DigiCert or a third party.
「業界規格」又は「デジサート」の「CPS」により「証明書」の失効が要求される場合、又は「デジサート」又は第三者の権利、秘密情報、事業活動若しくは名声を保護するために失効が必要な場合。

19. Sharing of Information.
情報の共有.

Customer acknowledges and accepts that if (i) the Certificate or Customer is identified as a source of Suspect Code, (ii) the authority to request the Certificate cannot be verified, or (iii) the Certificate is revoked for reasons other than Customer request (e.g. as a result of private key compromise, discovery of malware, etc.), DigiCert is authorized to share information about Customer, any application or object signed with the Certificate, the Certificate, and the surrounding circumstances with other certification authorities or industry groups, including the CAB Forum.
「お客様」は、以下のいずれかの場合、「デジサート」が、「お客様」、「証明書」で署名されたアプリケーション又はオブジェクト、「証明書」及び周辺環境に関する情報を他の認証局又は「CAB フォーラム」を含む業界団体と共有できることを承認し、これを承諾します：(i)「証明書」又は「お客様」が、「サスペクトコード」の発信源であると同定された場合；(ii)「証明書」を申請する権限が確認できない場合；又は (iii)「お客様」の申請以外の理由で「証明書」が失効された場合（例えば、「秘密鍵」の危殆化、マルウェアの発見などの結果として）。

20. Industry Standards.
業界規格.

Both parties will comply with all Industry Standards and laws that apply to the Certificates; if such an applicable law or Industry Standard changes and that change affects the Certificates or other services provided under the Agreement, then DigiCert may alter the services or amend or terminate the Agreement to the extent necessary to comply with the change.
両当事者は、「証明書」に適用されるすべての「業界規格」及び法令を遵守するものとします。なお、当該適用法令又は「業界規

格」が変更され、当該変更が「援用契約」により提供される「証明書」その他サービスに影響を及ぼす場合、「デジサート」は、当該変更に準拠するために必要な限度で、サービスを改変し、又は「援用契約」を変更又は解約できるものとします。

21. Equipment.
設備.

Customer is responsible, at Customer's expense, for (i) all computers, telecommunication equipment, software, access to the Internet, and communications networks (if any) required to use the Certificates and related DigiCert software or services; and (ii) Customer's conduct and its website maintenance, operation, development, and content.
「お客様」は、「お客様」の費用で、以下について責任を負うものとします：(i)「証明書」及び関連「デジサート」ソフトウェア又はサービスを利用するために必要な、すべてのコンピュータ、通信機器、ソフトウェア、インターネット接続及び通信ネットワーク（もしあれば）；及び (ii)「お客様」の管理並びにそのウェブサイトの保守、運営、開発及びコンテンツ。

22. Certificate Beneficiaries.
証明書の受益者.

Relying Parties and Application Software Vendors are express third-party beneficiaries of Customer's obligations and representations related to the use or issuance of a Certificate. The Relying Parties and Application Software Vendors are not express third party beneficiaries with respect to any DigiCert software.
「依拠当事者」及び「アプリケーションソフトウェアベンダー」は、「証明書」の使用又は発行に関する「お客様」の義務及び表明の明示的な第三受益者となります。「依拠当事者」及び「アプリケーションソフトウェアベンダー」は、「デジサート」ソフトウェアについて明示的な第三受益者となるものではありません。

23. Intermediate Certificates.
中間証明書.

This Section 23 only applies if Customer purchases a dedicated Root Certificate and/or Intermediate Certificate for the issuance of Private Certificates or publicly-trusted Certificates as specified in an Order Form.
本第 23 条は、「お客様」が、申込書に記載される「プライベート証明書」又は公的に信頼される「証明書」を発行するための専用「ルート証明書」及び/又は「中間証明書」を購入される場合にのみ適用されます。

a. Creation. Within 60 days after receiving applicable payment pursuant to the Agreement and the information required by DigiCert to create the Root Certificate and/or Intermediate Certificate as described in subsection (b) below, DigiCert will create a Root Certificate and/or an Intermediate Certificate for issuing (i) non-publicly trusted Certificates through the Portal or (ii) publicly-trusted Certificates as specified in an Order Form. A "**Private Certificate**" means a Certificate that is not embedded in any trust store. A "**Root Certificate**" means a self-signed Certificate that is stored in a secure off-line state and used to issue other Certificates. "**Intermediate Certificate**" means a Certificate that is signed by a Private Key corresponding to a Root Certificate and that is used to issue Certificates for use by Customer.
作成. 「デジサート」は、「援用契約」に従った該当支払及び「ルート証明書」及び/又は「中間証明書」を作成するために「デジサート」が必要とする下記(b)項に定める情報の受領後 60 日以内に、(i)「ポータル」による公的に信頼されない「証明書」又は (ii)「申込書」に記載する公的に信頼される「証明書」を発行するための「ルート証明書」及び/又は「中間証明書」を作成するものとします。「**プライベート証明書**」とは、いずれのトラストストアにも組み込まれていない「証明書」をいいます。「**ルート証明書**」とは、セキュアなオフライン状態で保管された、他の「証明書」を発行するために使用される自己署名「証明書」をいいます。「**中間証明書**」とは、「ルート証明書」に対応する「秘密鍵」で署名され、「お客様」が使用する「証明書」の発行に使用される「証明書」をいいます。

b. Contents. DigiCert and Customer will work together in good-faith to determine the appropriate contents of the Root Certificate and/or Intermediate Certificate. Customer must provide DigiCert with all information required by DigiCert for the creation of the Root Certificate and/or Intermediate Certificate within twelve (12) months of concluding an agreement for the creation of that Root Certificate and/or Intermediate Certificate. If Customer fails to provide all required information within that time frame, Customer will forfeit the right to request the Root Certificate and/or Intermediate Certificate and DigiCert will retain any fees paid for the creation of the Root Certificate and/or Intermediate Certificate. After an Intermediate Certificate is created, Customer may not modify the contents of such Intermediate Certificate but may create as many identical copies of the Intermediate Certificate as needed. Intermediate Certificates have a set ten-year lifecycle, after which they expire without renewal. Customer is responsible for ensuring that all Certificates issued from an Intermediate Certificate expire at least two years prior to the expiration of the Intermediate Certificate. DigiCert has the right to revoke any Certificates issued from the Intermediate Certificates that are still valid within two years of the

expiration of the Intermediate Certificate.
内容. 「デジサート」及び「お客様」は、「ルート証明書」及び/又は「中間証明書」の適切な内容を決定するため誠意をもって協力するものとします。「お客様」は、「デジサート」に対し、当該「ルート証明書」及び/又は「中間証明書」作成に係る契約締結後 12 ヶ月以内に、当該「ルート証明書」及び/又は「中間証明書」を作成するために「デジサート」が必要とする情報をすべて提供しなければいけません。「お客様」が要求されるすべての情報を当該期間内に提供しない場合、「お客様」は、「ルート証明書」及び/又は「中間証明書」を請求する権利を失うものとし、「デジサート」は、「ルート証明書」及び/又は「中間証明書」作成に対して支払われた料金を収得するものとします。「お客様」は、「中間証明書」が作成された後、当該「中間証明書」の内容を変更することはできませんが、当該「中間証明書」と同一の複製を必要なだけ何枚でも作成できるものとします。「中間証明書」には 10 年の寿命が設定されており、当該期間後は更新なく終了します。「お客様」は、「中間証明書」から発行される「証明書」がすべて、当該「中間証明書」終了の少なくとも 2 年前までに確実に終了するよう責任を負います。「デジサート」は、「中間証明書」から発行され、当該「中間証明書」の終了から 2 年間なお有効な「証明書」を「失効させる権利を有します。

c. Ownership. DigiCert retains sole ownership of the Intermediate Certificate but, except as otherwise provided herein, will use the Intermediate Certificate issued in connection with this Agreement solely in accordance with the instructions provided by Customer through the Portal. Customer may generate copies of the Intermediate Certificate and distribute copies of the Intermediate Certificate to its own end users and customers.
所有権. 「デジサート」は「中間証明書」の単独の所有権を留保しますが、「本証明書利用規約」において別段の定めのない限り、「ポータル」を通じて「お客様」から提供される指示に従ってのみ「援用契約」に関連して発行される「中間証明書」を使用するものとします。「お客様」は、「中間証明書」の複製を生成し、「中間証明書」の複製を自己のエンドユーザー及び顧客に配布できるものとします。

d. Hosting. DigiCert will host the Intermediate Certificate's Private Key in DigiCert's secure PKI systems. Customer may not remove or have a third party remove the Intermediate Certificate's Private Key from DigiCert's PKI systems for any reason. DigiCert will provide and host CRL/OCSP services for Customer. DigiCert will continue to provide the CRL/OCSP services after the Agreement's termination until all Certificates issued thereunder expire or are revoked. For an Intermediate Certificate that issues publicly-trusted Certificates, because the Intermediate Certificate issues publicly-trusted Certificates, is hosted in DigiCert's PKI, and is managed by DigiCert's personnel, the Intermediate Certificate will be covered by DigiCert's WebTrust audit. If Industry Standards or the policies of an Application Software Vendor change in a manner that requires a separate audit of the Intermediate Certificate, then DigiCert and Customer will work together in good faith to obtain the required audit.
ホスティング. 「デジサート」は、「中間証明書」の「秘密鍵」を「デジサート」のセキュアな「PKI」システムにホスティングするものとします。「お客様」は、いかなる理由によっても、自ら又は第三者をして「中間証明書」の「秘密鍵」を「デジサート」の「PKI」システムから移動させることはできません。「デジサート」は、「お客様」のために CRL/OCSP サービスを提供し、ホスティングするものとします。「デジサート」は、「援用契約」の終了後も、「援用契約」に基づき発行される「証明書」がすべて終了するか又は失効されるまで CRL/OCSP サービスを継続して提供するものとします。公的に信頼される「証明書」を発行する「中間証明書」については、公的に信頼される「証明書」を発行し、「デジサート」の「PKI」にホスティングされ、「デジサート」の従業員により管理されるものであるため、当該「中間証明書」は「デジサート」の WebTrust 監査の対象となるものとします。「業界規格」又は「アプリケーションソフトウェアベンダー」の方針が「中間証明書」の監査が別途要求されるよう変更された場合、「デジサート」及び「お客様」は、要求される監査を受けるため誠意をもって協力するものとします。

e. Revocation. DigiCert will have the right to revoke the Intermediate Certificate if: (i) Customer requests revocation in writing to DigiCert, citing a specific violation of industry standards; (ii) DigiCert has reasonable grounds to believe the Intermediate Certificate has been compromised; (iii) Customer materially breaches the Agreement and fails to remedy the breach within 30 days after receiving notice of the breach; (iv) Customer continues to use the Intermediate Certificate after Customer's right to use the Intermediate Certificate terminates, or (v) DigiCert reasonably believes the revocation is required by Industry Standards.
失効. 「デジサート」は、以下のいずれかの場合、「中間証明書」を失効させる権利を有するものとします：(i)「お客様」が、「デジサート」に対し、特定の「業界規格」違反を摘示し書面をもって失効を申請した場合；(ii)「デジサート」が「中間証明書」が既に危殆化されたと信じるに足る合理的な根拠がある場合；(iii)「お客様」が「援用契約」の重大な違反を犯した場合で、当該違反に関する通知を受領してから 30 日内に当該違反を是正しなかったとき；(iv)「中間証明書」を使用する「お客様」の権利が終了した後も、「お客様」が「中間証明書」の使用を継続する場合；又は (v)「業界規格」により失効が必要とされると「デジサート」が合理的に考える場合。

f. Restrictions. Customer will not: (i) create or attempt to create additional intermediate certificates from the Intermediate Certificate; (ii) sell, distribute, rent, lease, license, assign, or otherwise transfer the Intermediate

Certificate to any third party; (iii) use an Intermediate Certificate provided by DigiCert after its expiration, its revocation, or the termination of this Agreement; (iv) alter, modify or revise an Intermediate Certificate provided by DigiCert; or (v) use the Intermediate Certificate if Customer has reason to believe that the Intermediate Certificate's Private Key was compromised.
制限事項. 「お客様」は、以下のいずれも行わないものとします：(i)「中間証明書」から別の「中間証明書」を作成し、又は作成を試みること；(ii)「中間証明書」を販売、配布、貸出、貸与、使用許諾、譲渡その他方法で第三者に移転すること；(iii)「デジサート」が提供した「中間証明書」を、その終了、失効又は「援用契約」の終了後も使用すること；(iv)「デジサート」が提供した「中間証明書」を改変、変更又は修正すること；又は (v)「中間証明書」の「秘密鍵」が危殆化されたと「お客様」が信じるに足る理由がある場合に、当該「中間証明書」を使用すること。

24. Mark License & Third-Party Terms.
マーク使用許諾及び第三者条件.

a. DigiCert may make certain of its trademarks and logos (each, a "Mark") available for display by Customer to allow Customer to indicate that a particular Certificate issued hereunder has been issued by DigiCert for a particular Customer property. Effective upon issuance of the applicable Certificate, and only for so long as such Certificate remains valid, and Customer is in full compliance with all applicable terms related thereto, DigiCert grants to Customer a limited, revocable license during the validity period of the applicable Certificate to display the applicable Mark (in the form provided by DigiCert to Customer) to accurately and not misleadingly indicate the applicable Certificate on Customer's products, domain names or services. Customer agrees to not modify Marks in any manner (including to not remove or modify any trademark notices that DigiCert may apply to such Marks) or use or display Marks for any inappropriate purpose or in any way that could misrepresent the parties' relationship or diminish or damage DigiCert's reputation or the goodwill associated with any Mark or other DigiCert trademarks or service marks, including using a Mark or Certificate with a website that could be considered associated with crime, fraud, deception, defamation, libel, obscenity, misappropriation or infringement or that is otherwise reasonably objectionable to DigiCert. All goodwill arising in connection with the use of Marks will inure to the benefit of DigiCert and if Customer obtains any right, title or interest in or to any Mark as a result of the use of such Mark, then Customer hereby irrevocably assigns to DigiCert all such right, title and interest therein and thereto.
「デジサート」は、「本証明書利用規約」に基づき発行された特定の「証明書」が「お客様」の特定の財産について「デジサート」により発行されたことを示すことを可能にするため、「デジサート」の特定の商標及びロゴ（以下、それぞれ「**マーク**」といいます）を「お客様」が表示できるようにします。該当「証明書」の発行により有効とし、当該「証明書」が有効である期間中に限り、かつ、「お客様」が当該「証明書」に関するすべての適用される条件を完全に遵守している限り、「デジサート」は、「お客様」に対し、該当「証明書」の有効期間中、「お客様」の製品、ドメイン名又はサービスについて該当「証明書」を正確かつ誤認を生じない方法で表示するために、該当「マーク」を（「デジサート」が「お客様」に提供する形態で）表示する制限付きの、撤回可能な使用権を許諾します。「お客様」は、いかなる方法によっても「マーク」を改変しないこと（「デジサート」が当該「マーク」に付すことのある商標表示を除去又は改変しないことを含みます）、又は不相当な目的について又は両当事者の関係を不実表示し、又はあらゆる「マーク」又はその他の「デジサート」の商標若しくはサービスマークに伴う「デジサート」の評判若しくはのれんを損ない又は毀損するおそれのあるいかなる方法によっても、「マーク」を使用し又は表示しないことに合意します。これには、犯罪、詐欺、騙し、名誉毀損（文書又は口頭によるかを問わない）、猥褻、不正流用若しくは侵害と関連するとみなされるおそれのあるウエブサイト又はその他合理的に見て「デジサート」にとって有害とされるウエブサイトとの「マーク」又は「証明書」の使用を含みます。「マーク」の使用に伴い生じるのれんの利益はすべて「デジサート」に帰属するものとし、「お客様」がいずれか「マーク」の使用の結果として当該「マーク」に係る権利、権原又は権益を取得した場合、そのときは、「お客様」は、本書をもって、「デジサート」に対し、当該「マーク」に係る当該権利、権原及び権益をすべて取消不能で譲渡します。

b. Customer acknowledges and agrees that if Customer's Certificate includes a legal entity identifier ("**LEI**") provided by Ubisecure Oy, then the Ubisecure Oy – RapidLEI Terms of Service available at https://rapidlei.com/documents/global-lei-system-terms/ will apply to Customer's LEI and use of the RapidLEI Legal Entity Identifier Management System or successor service.
「お客様」は、「お客様」の「証明書」に Ubisecure 社により提供される取引主体識別子（以下「**LEI**」といいます）が含まれる場合、「お客様」の「LEI」及び RapidLEI 取引主体識別子管理システム又はその後継サービスの利用については https://rapidlei.com/documents/global-lei-system-terms/ で閲覧可能な Ubisecure 社－RapidLEI サービス規約が適用されることを承認し、これに同意します。

c. Customer acknowledges and agrees that Customer's use of DigiCert's post-quantum cryptographic (PQC) toolkit (the "**PQC Toolkit**") will be governed by the following terms, in addition to the terms of any other applicable license agreement: (i) the license granted to Customer in relation to the PQC Toolkit is a non-exclusive, terminable license to be used only in connection with a DigiCert certificate that includes a signature and public key generated by or with the PQC Toolkit or related testing and configuration activities; (ii) Customer acquires no intellectual property or other proprietary rights in the PQC Toolkit or intellectual property related to it; (iii) Customer will not reverse engineer, translate, disassemble, decompile, decrypt or deconstruct the PQC Toolkit; (iv) Customer will cease use of the PQC Toolkit upon termination of the related services from DigiCert; (v) ISARA Corporation will not be liable to Customer for any damages whatsoever; (vi) Customer will import, export and re-use the PQC Toolkit only in accordance with applicable laws of the countries or territories in which the PQC Toolkit is used or imported or from which it is exported or re-exported; (vii) DigiCert makes no warranties, express or implied, related to the PQC Toolkit on behalf of ISARA Corporation; and (viii) Customer will not alter any copyright, trademark or patent notice included in or with the PQC Toolkit or any related materials.
「お客様」は、「デジサート」の耐量子暗号ツールキット（以下「**PQC ツールキット**」といいます）の「お客様」による利用については、適用されるライセンス契約の条件に加え、以下の条件が適用されることを承認し、これに同意します：(i) 「PQC ツールキット」について「お客様」に許諾されるライセンスは、「PQC ツールキット」又は関連テスト及び設定行為により生成される署名並びに「公開鍵」を含む「デジサート」証明書についてのみ使用される非独占的で、解除可能なライセンスであること；(ii)「お客様」は、「PQC ツールキット」又はその関連知的財産に係る知的財産権その他専有権を何ら取得するものではないこと；(iii)「お客様」は、「PQC ツールキット」をリバースエンジニアリング、翻訳、逆アセンブル、逆コンパイル、復号化又は分解しないものとします；(iv)「お客様」は、「デジサート」から提供される関連サービスが終了した場合、直ちに「PQC ツールキット」の使用を停止するものとします；(v) ISARA 社は、「お客様」に対して、いかなる損害についても責任を負わないものとします；(vi)「お客様」は、「PQC ツールキット」が使用若しくは輸入される仕向国又は地域、又は「PQC ツールキット」が輸出若しくは再輸出される仕出国又は地域の適用法令に従ってのみ、「PQC ツールキット」を輸入、輸出及び再使用するものとします；(vii)「デジサート」は、「PQC ツールキット」について、ISARA 社を代理して、明示黙示の如何を問わず何らの保証を行うものではないこと；及び (viii)「お客様」は、「PQC ツールキット」又は関連資料に含まれるか若しくは同梱される著作権、商標又は特許表示を改変しないものとします。

25. Flow-Down Requirements. Customer must not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any DigiCert system or software, and must impose the same restriction on its appointed manufacturers, if any.
フローダウン要件．「お客様」は、「デジサート」のシステム又はソフトウェアの技術的実装を監視、妨害、リバースエンジニアリングし、又はその他の方法で「デジサート」システム又はソフトウェアのセキュリティを悪意で危殆化してはならず、指名した製造業者がある場合、当該製造業者に同一の義務を課さなければいけません。

26. Microsoft-Required Supplemental Obligations.
Microsoft 要求補足義務.

a. If Customer uses the Microsoft Auto Enrollment component, then the following MICROSOFT REQUIRED SUPPLEMENTAL OBLIGATIONS will apply:
「お客様」が Microsoft Auto Enrollment コンポーネントを使用する場合、以下の MICROSOFT 社の要求補足義務が適用されるものとします：

b. Disclaimer of Warranties. MICROSOFT AND ITS AFFILIATES MAKE NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY AS TO THE SERVER SOFTWARE PROVIDED HEREUNDER ("**SERVER SOFTWARE**"), AND HAVE NO RESPONSIBILITY FOR ITS PERFORMANCE OR FAILURE TO PERFORM. AS TO MICROSOFT, THE SERVER SOFTWARE IS PROVIDED AS IS AND WITH ALL FAULTS, AND MICROSOFT AND ITS AFFILIATES HEREBY DISCLAIM ALL OTHER WARRANTIES, DUTIES AND CONDITIONS, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY (IF ANY) IMPLIED WARRANTIES, CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF RELIABILITY OR AVAILABILITY, ALL WITH REGARD TO THE SERVER SOFTWARE. ALSO, MICROSOFT AND ITS AFFILIATES MAKE NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SERVER SOFTWARE.
保証の否認．Microsoft 社及びその関係会社は、Microsoft 社又はその関係会社が提供するサーバーソフトウェア（以下「**サーバーソフトウェア**」）について、明示、黙示又は制定法上のものであるかを問わず、何らの保証を行わず

、「サーバーソフトウェア」の動作又は不動作について何らの責任を負いません。Microsoft 社について、「サーバーソフトウェア」はすべての欠陥を含んだ現状有姿で提供されるものであり、Microsoft 社及びその関係会社は、本書をもって、「サーバーソフトウェア」について、明示、黙示又は制定法上のものであるかを問わず、すべての他の保証、義務及び条件を否認します。これには、商品適格性、特定目的適合性、信頼性又は可用性の黙示の保証及び条件が含まれますが、これらに限定するものではありません。また、Microsoft 社及びその関係会社は、「サーバーソフトウェア」について、権原、平穏享有、説明との一致又は非侵害の保証又は条件を一切提供しません。

c. Exclusion of Certain Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL MICROSOFT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SERVER SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SERVER SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SERVER SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY OF THESE SERVICE DESCRIPTION TERMS AND CONDITIONS, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF MICROSOFT, AND EVEN IF MICROSOFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
特定損害の除外．適用法令で許容される最大限度において、いかなる場合も、Microsoft 社は、「サーバーソフトウェア」の使用又は使用不能、サポートその他サービス、情報、ソフトウェア及び関連コンテンツの「サーバーソフトウェア」を通じた提供若しくは不提供に起因又は関連し、又はその他何であろうと「サーバーソフトウェア」の使用に起因し、又はその他何であろうと「サービス記述書」の条件のいずれかに基づき又は関連して生じる、特別損害、付随的損害、懲罰的損害、間接損害又は結果的損害（逸失利益又は秘密情報その他情報消失に対する損害、事業中断に対する損害、人身傷害に対する損害、プライバシー喪失に対する損害、誠実義務又は合理的な注意義務を含む義務の不履行に対する損害、過失責任に対する損害、及びその他のあらゆる金銭的損失又はその他のあらゆる損失に対する損害が含まれますが、これらに限定するものではありません）について、Microsoft 社の懈怠、不法行為（過失を含みます）、厳格責任、契約違反又は保証違反の場合であっても、また Microsoft 社が当該損害の可能性について予告されていた場合であっても、一切責任を負わないものとします。

d. Server Software Requirements. Customer may use only one (1) copy (unless otherwise specified in the applicable Order) of the Server Software provided hereunder as specified in the documentation accompanying this software, and only to interoperate or communicate with native Microsoft Windows 2000 Professional, Windows XP Home or Professional, or Vista client operating systems (or any successors thereto). Customer may not use the Server Software on a Personal Computer under any circumstances. For purposes of the foregoing, a "**Personal Computer**" means any computer configured so that its primary purpose is for use by one person at a time and that uses a video display and keyboard.
サーバーソフトウェア要件．「お客様」は、「サーバーソフトウェア」付属の文書に定めるところにより、Microsoft 社又はその関係会社が提供する「サーバーソフトウェア」を一部に限り（該当注文書において別段の定めのない限り）、ネイティブ Microsoft Windows 2000 Professional、Windows XP Home/Professional 又は Vista クライアントオペレーティングシステム（又はそれらの後継システム）と相互運用し又は通信することのみを目的として使用することができます。「お客様」は、いかなる状況においても、「パーソナルコンピュータ」上で「サーバーソフトウェア」を使用することはできません。前記において、「**パーソナルコンピュータ**」とは、その主たる目的が一度に一人の人が使用するためのもので、かつ、ディスプレイ及びキーボードを使用するよう設定されたコンピュータをいいます。

e. Third Party Beneficiary. Notwithstanding any inconsistent terms of the Agreement, Customer hereby agrees that Microsoft Corporation, as a licensor of intellectual property included in the Server Software, is intended to be a third party beneficiary of the terms and conditions of this Section 26 with rights to enforce any terms herein that affect any included Microsoft intellectual property or other Microsoft interest related to the terms hereof.
第三受益者．「援用契約」の齟齬する条件にかかわらず、「お客様」は、本書をもって、Microsoft 社は、「サーバーソフトウェア」に含まれる知的財産のライセンサーとして、本第 26 条の諸条件の第三受益者として意図されてお

り、含まれる当該 Microsoft 社の知的財産又は本条の条件に関連するその他の Microsoft 社の権益に影響を及ぼす本条の条件を強制する権利を有することに同意します。

f. Server Class 2. If Customer has elected the Server Class 2, Customer may use the Server Software on a server that (a) contains not more than four (4) processors, where each such processor has a maximum of thirty-two (32) bits and four (4) gigabytes of RAM, and (b) is not capable of having memory added, changed or removed without the requirement that the server on which it is running be rebooted ("**Hot Swapping Capabilities**"). Customer may not use the Server Software in conjunction with any software that supports Hot Swapping Capabilities or Clustering Capabilities, where "**Clustering Capabilities**" means the ability to allow a group of servers to function as a single high-availability platform for running applications using application failover between Server nodes in the group.
サーバークラス 2. 「お客様」がサーバークラス 2 を選択した場合、「お客様」は、 (a) 最大処理能力 32 ビット及び 4 ギガバイトの RAM を有するプロセッサー最大 4 基で構成され、かつ、(b) メモリの装着、交換又は抜去を行う際には、必ず「サーバーソフトウェア」が稼働しているサーバーを再起動する必要がある（以下「**ホットスワップ機能**」といいます）サーバー上で「サーバーソフトウェア」を使用できるものとします。「お客様」は、「ホットスワップ機能」又は「クラスタ機能」をサポートするソフトウェアと組合わせて「サーバーソフトウェア」を使用できないものとします。前記において、「**クラスタ機能**」とは、複数のサーバーをグループ化し、当該グループ内のサーバーノード間でアプリケーションフェイルオーバーを実装することにより、アプリケーションを実行するための単一の高可用性プラットフォームとして機能することを可能とする能力をいいます。

g. Audit Rights. DigiCert may audit Customer and inspect Customer's facilities and procedures during regular business hours at Customer premises upon not less than fourteen (14) days' notice to verify Customer's compliance with all terms and conditions hereof. Notwithstanding any inconsistent terms of the Agreement (including without limitation any confidentiality provisions), should Customer refuse to undergo such audit and DigiCert has reason to believe Customer may not be in compliance with the Service Description terms and conditions, Customer agrees that DigiCert may disclose (i) Customer's identity to Relying Parties and Application Software Vendors and (ii) the basis for DigiCert's belief of noncompliance.
監査権. 「デジサート」は、「お客様」が「本証明書利用規約」の条件を遵守していることを確認するために、少なくとも 14 日の事前通知をもって、通常の営業時間中に「お客様」の施設で「お客様」及び「お客様」の設備並びに手続きを調査できるものとします。「援用契約」の齟齬する条件（秘密保持条項が含まれますが、これらに限定するものではありません）にかかわらず、万一「お客様」が当該監査を受けることを拒絶した場合で、「デジサート」が「お客様」が「サービス記述書」の条件を遵守していないと信じるに足る理由があるときは、「お客様」は、「デジサート」が、「依拠当事者」及び「アプリケーションソフトウェアベンダー」に対し、(i) 「依拠当事者」及び「アプリケーションソフトウェアベンダー」に対し「お客様」の身元及び (ii) 不遵守に関する「デジサート」の見解を開示できることに同意します。

h. Multiplexing Devices. Hardware or software that reduces the number of users directly accessing or using services provided by the Server Software does not reduce the number of users deemed to be accessing or using services provided by the Server Software. The number of users accessing or using the Server Software is equal to the number of users who access or use, either directly or through a Multiplexing Device, services provided by (a) the Server Software or (b) any other software or system where the authentication or authorization for such software or system is provided by the Server Software (an "**Other Authenticated System**"). As used here, a "**Multiplexing Device**" means any hardware or software that provides or obtains access, directly or indirectly, to services provided by the Server Software or any Other Authenticated System to or on behalf of multiple other users through a reduced number of connections.
多重化装置. 「サーバーソフトウェア」により提供されるサービスに直接アクセス又は利用する利用者の数を低減ずるハードウェア又はソフトウェアは、「サーバーソフトウェア」により提供されるサービスにアクセス又は利用すると見なされる利用者の数を低減することはありません。「サーバーソフトウェア」にアクセス又は利用する利用者の数は、 (a)「サーバーソフトウェア」又は (b) その他のソフトウェア又はシステムで、当該その他のソフトウェア又はシステムの認証又は承認が「サーバーソフトウェア」で行われるもの（以下「**その他の認証対象システム**」といいます）により提供されるサービスに、直接又は「多重化装置」を介して、アクセス又は使用する利用者の数と等しくなります。ここで使用する用語「**多重化装置**」とは、「サーバーソフトウェア」又は「その他の認証対象システム」により提供されるサービスへのアクセスを、複数の他の利用者に対し又は複数の他の利用者を代理して、低減接続数により直接的又は間接的に提供又は取得するハードウェア又はソフトウェアをいいます。

i. Windows CAL Requirement. Customer must acquire and dedicate a separate Windows CAL for each user that is accessing or using, either directly or through or from a Multiplexing Device, services provided by the Server Software or any Other Authenticated System. A "**Windows CAL**" means (a) a Windows Device Client Access License ("**CAL**"), or a Windows User CAL, in either case for a Microsoft Windows Server 2003 (Standard Edition, Enterprise Edition, or Datacenter Edition) server operating system product (or any successors thereto) ("**Windows Server**"); or (b) a Microsoft Core CAL that provides an individual person or electronic device with rights to access and use Windows Server, in either of (a) or (b) above that Customer has acquired for use with one or more such Microsoft Windows Server operating system products or electronic device and that is used on a per user or per device basis.
Windows CAL 要件. 「お客様」は、「サーバーソフトウェア」又は「その他の認証対象システム」によって提供されるサービスに、直接若しくは「多重化デバイス」を介し又は「多重化デバイス」からアクセス又は使用する各利用者について各別に「Windows CAL」 を取得し、割り当てなければいけません。「**Windows CAL**」とは、(a) Windows クライアントアクセスライセンス（以下「**CAL**」といいます）、又は Windows ユーザ「CAL」で、いずれの場合も、Microsoft Windows Server 2003（Standard Edition、Enterprise Edition 又は Datacenter Edition）サーバーオペレーティングシステム製品又はその後継製品（以下「**Windows サーバー**」といいます）用のもの、又は (b)「Windows サーバー」にアクセスし、利用する権利を個人又は電子デバイスに与える Microsoft コア「CAL」で、上記 (a) 又は (b) のいずれの場合も、一つ以上の Microsoft Windows サーバーオペレーティングシステム製品又は電子デバイスと使用するために「お客様」が既に取得しており、利用者単位又はデバイス単位で使用されるものをいいます。

27. Adobe-Required Supplemental Obligations.
Adobe 要求補足義務.

If Customer is issued Adobe Signing Certificates, Customer agrees to:
「お客様」は、Adobe サイニング証明書の発行を受ける場合、以下に同意します：

a. Adhere to the Adobe Systems Inc. AATL Certificate Policy 2.0 currently available at https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf which includes, but is not limited to: (1) only generating and storing Key Sets for Adobe Signing Certificates on a FIPS 140-2 Level 2 device; and (2) upon enrollment of a new account, or at any time a new AATL Certificate enrollment is initiated for a subscriber, providing accurate and true information to DigiCert which requires (A) an account administrator to carry out strong identity proofing based on a face to face meeting with DigiCert or on a procedure that provides an equivalent assurance (e.g. by means of a secure video communication), (B) an account administrator to carry out strong identity proofing based on a face to face meeting with its subscribers (i.e. end-users), and store the recording locally to support audits, until DigiCert provides an online mechanism for administrator to upload attestations and recordings; and (C) the identity proofing process, regardless of an administrator or a subscriber, must include recording of the subscriber showing themselves and a valid government ID (e.g. driving license, passport, national ID card, etc.) displaying a matching photo of the subscriber; and
https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf で現在閲覧可能な Adobe Systems 社 AATL 証明書方針第 2.0 版を遵守すること。なお、これには以下の条件が含まれますが、これらに限定するものではありません：(1) Adobe サイニング証明書の「鍵セット」を FIPS 140-2 レベル 2 のデバイス上でのみ生成し、保管すること；及び (2) 新規アカウントの登録時、又はサブスクライバーのための AATL 証明書の新規登録が開始されたときはいつでも、正確かつ真実の情報を「デジサート」に提供すること。なお、これには、(A) アカウント管理者は、「デジサート」との対面会議又は同等の確証を提供する手段（つまり、セキュアなビデオ通信）に基づく確実な身元確認を実行し、(B) アカウント管理者は、「デジサート」が管理者に証拠資料や録画をアップロードするためのオンライン機能を提供するまで、サブスクライバー（つまり、エンドユーザー）との対面会議に基づく確実な身元確認を実行し、監査を裏付けるための録画を構内に保管し、及び (C) 身元確認手続きに、管理者又はサブスクライバーにかかわらず、サブスクライバー自身を表示するサブスクライバーの録画、及び本人と一致するサブスクライバーの写真を表示する政府発行の有効な身分証明書（つまり、運転免許証、パスポート、国民識別番号証明書等）を含めなければいけません；及び

b. the terms of the applicable CPS.
適用される「CPS」の条件。

28. Additional Restrictions for Code Signing Certificates. Customer must not use a code signing Certificate: (i) for or on behalf of any organization other than Customer's organization; (ii) to perform Private Key or Public Key operations in

connection with any domain and/or organization name other than the one Customer submitted on the Certificate application; (iii) to distribute Suspect Code; or (iv) in a manner that transfers control or permits access for the Private Key corresponding to the Public Key of the Certificate to anyone other than an employee that Customer has authorized (any such transfer to be in a secure manner so as to protect the Private Key).

For all OV code signing Certificates issued on or after June 1, 2023, including any renewed or reissued Certificates, all Private Keys must be stored on hardware certified as FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent. For all OV code signing Certificates issued before June 1, 2023, including any renewed or reissued Certificates, all Private Keys must be stored on hardware tokens.

コードサイニング証明書の追加制限事項. 「お客様」は：(i)「お客様」の組織以外の団体のため又は当該団体を代理して；(ii)「お客様」が「証明書」申請書で提出したドメイン及び/又は組織名以外のものに関連し「秘密鍵」又は「公開鍵」操作を実行するために；(iii)「サスペクトコード」を頒布するために；又は (iv)「証明書」の「公開鍵」に対応する「秘密鍵」の管理を「お客様」が権限を付与した従業員以外の者に移転又はアクセスを許可するような方法で（当該移転は「秘密鍵」を保護するセキュアな方法によります）、コードサイニング「証明書」を使用してはいけません。

2023 年 6 月 1 日以降に発行、更新又は再発行される「証明書」を含む、すべての OV コードサイニング「証明書」については、「秘密鍵」をすべて FIPS 140 Level 2、Common Criteria EAL 4+ 又は同等の規格認定を受けたハードウェア上に保管しなければいけません。2023 年 6 月 1 日前に発行、更新又は再発行された「証明書」を含む、すべての OV コードサイニング「証明書」については、「秘密鍵」をすべてハードウェアトークン上に保管しなければいけません。

29. **Additional Restrictions for non-public TLS/SSL Certificates**. TLS/SSL Certificates that are chained to a Private Root Certificate must be used only with intranet domains and may not be assigned to devices that are publicly accessible from the Internet. DigiCert reserves the right to monitor publicly-facing Internet servers and/or devices to ensure that private TLS/SSL Certificates comply with this clause. If DigiCert discovers any use of private TLS/SSL Certificate(s) not in compliance with this clause, then DigiCert will immediately notify Customer of non-compliance. Customer must, within twenty (24) hours, either (i) immediately move the private TLS/SSL Certificate to an intranet domain; or (ii) remove and revoke the private TLS/SSL Certificate from Customer's servers. If the Customer does not revoke or remove the non-compliant Certificate, then DigiCert may revoke the Certificate.

    非公開 TLS/SSL 証明書の追加制限事項. 「プライベートルート証明書」に関連付けられた TLS/SSL「証明書」はイントラネットドメインのみと使用しなければならず、インターネットから一般にアクセス可能なデバイスに割り当てることはできないものとします。「デジサート」は、プライベート TLS/SSL「証明書」が確実に本条に準拠するよう、一般に公開されるインターネットサーバー及び/又はデバイスを監視する権利を留保します。「デジサート」は、本条に準拠していないプライベート TLS/SSL「証明書」の使用を発見した場合、直ちに「お客様」に非準拠を通知するものとします。「お客様」は、24 時間以内に、(i) 直ちにプライベート TLS/SSL「証明書」をイントラネットドメインに移動させるか、又は (ii)「お客様」のサーバーからプライベート TLS/SSL「証明書」を削除、失効させるか、いずれか一を行わなければいけません。「お客様」が非準拠の「証明書」を失効又は削除しない場合、「デジサート」は「証明書」を失効させることができるものとします。

30. **Electronic Communication/Notification Tools**. When using email or other electronic communication or notification tools ("**Notification Tools**") provided by DigiCert to send a communication or notice ("**Communication**") you agree that (1) the content of any such Communication will be strictly limited to communication or notice about DigiCert products or services; (2) you will follow applicable law (including applicable electronic communications law and data privacy/data protection law) in the jurisdictions of recipients of the Communication; (3) you are solely responsible for the contents of any Communication you send using the Notification Tools; and (4) you will indemnify, defend and hold harmless DigiCert against third-party claims, government regulatory action or fines, and all liabilities, damages and costs, including reasonable attorney fees arising from your use of the Notification Tools or the contents of any Communication you send using the Notification Tools.

    電子コミュニケーション/通知ツール. 連絡又は通知（以下「**コミュニケーション**」といいます）を送信するために「デジサート」が提供する電子メールその他電子コミュニケーション又は通知ツール（以下「**通知ツール**」といいます）を使用する場合、「お客様」は、以下のすべてに合意します：(1) 当該「コミニケション」の内容を、「デジサート」製品又はサービスに関する連絡又は通知に厳に限定すること；(2)「コミュニケーション」の受信者の法域の適用法令（適用される電気通信法、個人情報保護法を含みます）に従うこと；(3)「通知ツール」を使用して送信する「コミュニケーション」の内容について全責任を負うこと；(4)「お客様」による「通知ツール」の利用又は「お客様」が「通知ツール」を使用して送信する「コミュニケーション」の内容に起因する、第三者請求、政府機関による規制措置又は過料、並びに

賠償責任、損害賠償及び合理的な弁護士費用を含む費用すべてについて、「デジサート」を補償、防御し、損害を被らないようにすること。

31. Survival and Termination. The Certificate Terms of Use survive the termination of the Agreement until all Certificates issued expire or are revoked.
存続条項及び解約. 「本証明書利用規約」は、「援用契約」の解約後も、発行済「証明書」がすべて満了又は失効されるまで存続します。

32. Language. The definitive version of this Certificate Terms of Use is written in English. If this Certificate Terms of Use is translated into another language and there is a conflict between the English version and the translated version, the English language version controls.
言語. 「本証明書利用規約」の正式版は英語で作成されています。「本証明書利用規約」が他言語に翻訳されている場合で、英語版と翻訳版との間に齟齬あるときは、英語版が優先します。