digicert

デジサート電子証明書 利用規約

このデジサート電子証明書利用規約（以下「**本電子証明書利用規約**」という）は、公的に信頼された TLS/SSL「証明書」、「クライアント証明書」（第 9 条に定義する）、「適格証明書」（第 10 条に定義する）又はその他米国ユタ州法人 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**」という）により、「デジサート」により提供される「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**」という）若しくは発行済み証明書で特定される団体又は個人（以下「**お客様**」という）に発行された各電子証明書（以下「**証明書**」(Certificate) という）に適用します。「ポータル」を利用又は使用するための「お客様」自身のアカウントについては、「本電子証明書利用規約」において「**ポータルアカウント**」といいます。

その一部を構成するものとして「本電子証明書利用規約」を援用する契約書（当該契約書については、これらの条件と併せ、以下、総称して「**適用契約**」という）を承諾するか又は署名することにより、承諾者又は署名者（以下「**署名者**」(Signer) という）は、以下を表明し、保証するものとします：（i）「署名者」は「お客様」の正当な権限を有する代理人として行動しており、「お客様」を代理して「署名者」が「適用契約」を承諾していること、及び「適用契約」に署名し、「お客様」を「適用契約」に拘束する権限を明示的に付与されていること；（ii）（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」のすべての利用に責任を有することを証明するために、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；（iii）「お客様」を代理して「証明書」要求を承認する権限を「お客様」によって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名を利用する「お客様」の独占的な権利を確証し又は確証すること。

「お客様」と「デジサート」は、以下のとおり合意します：

1. アカウントユーザ

「お客様」は、「ポータルアカウント」に管理者として掲載されている各個人に、「証明書要求者」(Certificate Requester)、「証明書承認者」(Certificate Approver)、そして「契約署名者」(Contract Signer)（「EV ガイドライン」に定義する）として行動し、「証明書」と「鍵ペア」の管理に関して「デジサート」と連絡を取り合う権限を付与します。「**EV ガイドライン**」とは、CA/Browser Forum （以下「**CAB フォーラム**」という） が発行し、www.cabforum.org で公表される EV ガイドライン (Extended Validation Guidelines) を意味します。「お客様」は、「デジサート」に通知することにより、この権限を取り消すことができます。「お客様」は、「証明書」を申請し承認できる個人を定期的に見直し、再確認する責任があります。「お客様」が「ポータルアカウント」のユーザの削除を希望する場合、「ポータルアカウント」のパスワードとその他の認証メカニズムの変更など、そのユーザによる「ポータル」へのアクセスを防ぐための手段を講じるものとします。「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、「お客様」は直ちに「デジサート」に通知するものとします。「お客様」は、以下を確約するものとします：（i）「お客様」は「デジサート」のサービスに関連するデータを「デジサート」が精査し、まとめ、収集し、そして「証明書」の更新とアップグレードを自動化する権限を付与します；（ii）「お客様」は、「お客様」が所有するか支配するドメイン名、IP アドレス又は資産の精査を自動化するためにのみサービスを利用するものとします；（iii）「お客様」は、「デジサート」により説明し販売されている目的で、「お客様」の意図したものについてのみ、https://www.digicert.com/legal-repository にあるデジサート利用規約 (DigiCert Acceptable Use Policy) に従ってサービスを利用するものとします。

2. 要求

「お客様」が「証明書」を要求できるのは、「お客様」、「お客様」の関連会社、又は「証明書」を入手し管理することを「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その他の者について登録されたドメイン名に限定されます。「デジサート」は、その独自の裁量で「お客様」が単一の「証明書」に記載できるドメイン名の数を制限することができます。

3. 認証

「お客様」から「証明書」の要求を受領すると、「デジサート」はその要求を審査し、デジザート認証局運用規程並びに「証明書」発行に関連する適用法令を含む業界基準、ガイドライン及び要求事項（以下「**業界基準**」(Industry Standards) という）に従って、関連情報の認証を試みます。当該要求の認証は、「デジサート」の単独の裁量によるもので、「デジサート」は理由の有無を問わず、「証明書」の発行を拒否することができます。「証明書」発行要求を拒否した場合、デジザートは「お客様」に通知しますが、その理由を提示する義務はありません。「**認証局運用規程**」又は「**CPS**」とは、公開鍵インフラ（以下「**PKI**」という）を運営するために、「デジサート」が遵守する規約と業務を文書化したものを意味し、適用されるタイムスタンプ方針及び表明 (Time-Stamp Policies and Statements) を含みます。「デジサート」の「CPS」は、https://www.digicert.com/legal-repository で入手

することができます。「QTSP」（「QTSP」としての資格において行為するかどうかにかかわらず）又は関係会社から発行されたサービス用「CPS」は、https://www.quovadisglobal.com/repository で入手することができます。

4. 証明書のライフサイクル

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」の要件事項、及び「証明書」の意図された用途によります。「デジサート」は、以下の要件事項を遵守するために、必要に応じて未発行の「証明書」の「証明書」ライフサイクルを変更することができます：（i）「適用契約」；（ii）「業界基準」；（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**」(Application Software Vendor) とは、「デジサート」が加盟しているか、加盟する配布されたルートストア（root store）に関連して、「証明書」を表示するか使用する団体を意味します。「お客様」は、「証明書」の終了日後、又は「デジサート」が「適用契約」で許可されたとおり「証明書」を失効させた後は、「証明書」そしてそれに関連する「秘密鍵」（以下に定義する）の使用を停止することに同意します。

5. 発行

「証明書」の認証が「デジサート」の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、合理的な方法によって「お客様」に交付します。一般的に、「デジサート」は、「ポータル」からの電子ダウンロード、又は「お客様」が「ポータル」経由で行った API コールへの応答という形で、「証明書」を電子メール経由で「お客様」が指定したアドレスに納品します。公的に信頼された「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、「証明書」の発行に使用する「ルート証明書」や「中間証明書」を、「お客様」への通知なくいつでも変更することができます。「お客様」は、「証明書」の申請と利用にあたり、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「業界基準」に従うものとします。「お客様」は、米国財務省外国資産管理局 (United States Treasury Department's Office of Foreign Assets Control)、米国商務省 (United States Commerce Department)、欧州委員会 (European Commission)、英国財務省金融制裁実施庁 (United Kingdom HM Treasury's Office of Financial Sanctions Implementation) 又は「デジサート」に管轄権を有するその他の関連政府機関によって制限されている国又は地域では「証明書」は利用できないことを確認します。

6. 証明書ライセンス

納品後直ちに有効となり、そして「証明書」が終了するか又は失効するまで継続的に、「お客様」は「証明書」の対象被認証者の利益のために、発行された各「証明書」と対応する「鍵ペア」を、全ての適用法令、規制、「業界基準」及び「本電子証明書利用規約」の条件に従って、「CPS」に記載された目的のために利用することができます。「**鍵ペア**」(Key Set) とは、（i）「公開鍵」はメッセージの暗号化を行い、そしてそれを複合化できるのは「秘密鍵」のみであり、そして（ii）「公開鍵」がわかっていても、「秘密鍵」を読み取ることは計算的に不可能とすることを特徴とする、2 つ又はそれ以上の数学的に関連する鍵を意味し、「秘密鍵」又は「公開鍵」に伴う鍵の共有と呼ばれます。「お客様」は、「証明書」や「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」の申請や使用、又はエンドユーザやシステムに頒布するために必要な認可やライセンス（米国輸出規制法令で要求されるライセンスを含む）を取得し、維持する責任を負うものとします。SSL「証明書」は、一度に一以上の物理サーバー又は端末上で使用することができます。但し「デジサート」は、追加サーバー又は端末上での「証明書」の使用について料金を請求することがでるものとします。

7. 鍵ペア

「**秘密鍵**」(Private Key) とは、「お客様」が機密にしている鍵で、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やファイルを復号化するために使われる鍵を意味します。「**公開鍵**」(Public Key) とは、「お客様」が一般に公表している鍵で、「お客様」の「証明書」に記載され、「お客様」が使用している「秘密鍵」に対応するものを意味します。「お客様」は（i）信頼できるシステムを用いて「鍵ペア」を作成し、（ii）少なくとも RSA 2048 ビット鍵と同等の「鍵ペア」を使用し、及び（iii）すべての「秘密鍵」を機密に保持する必要があります。「秘密鍵」を保護しなかった場合、「お客様」は全責任を負うものとします。「お客様」は、Adobe 署名「証明書」(Adobe Signing Certificates) と EV コードサイニング「証明書」(EV Code Signing Certificates) 用の「鍵ペア」については、FIPS 140-2 Level 2 のデバイスで作成し、保存することを表明し、保証します。その他の種類の「証明書」については、安全なソフトウェアかハードウェア・システム上に保存することができます。「お客様」は、「適用契約」に従って「デジサート」により生成された「鍵ペア」を、その地域の適用法令、規則及び規制に従って取得、使用又は受領する責任があるものとします。適用法令、規則、及び規制

には、「お客様」が対象の「鍵ペア」を取得、使用、又はその他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、それらに限定されるものではありません。「お客様」が特定の「デジサート」のサービスに関して「秘密鍵」（その複製を含む）をインポート又はエクスポートすることを許可されている場合、「デジサート」は「お客様」に対し、適用される「ポータル」又はサービスで作成されていないか、若しくは「秘密鍵」（その複製を含む）が適用される「ポータル」又はサービスからエクスポートされた後を含め，当該「ポータル」又はサービス外で使用されている「お客様」の「秘密鍵」（その複製を含む）の使用又は保管について責任を負わないものとします。

8. 証明書の透明性

「証明書」がそのライフサイクルを通して適切に機能するように、「デジサート」は一般に公開されている証明書透明性データベースに「証明書」を記録することができます。ログサーバの情報は、一般に公開されています。いったん提出された情報は、ログサーバから削除することはできません。

9. クライアント証明書

「**クライアント証明書**」(Client Certificate) とは、コードサイニング署名 (codeSigning)、タイムスタンプ (timestamping)、又はサーバ認証 (serverAuthentication) 以外のすべての拡張鍵用途 (extendedKeyUsage) を含む「証明書」を意味します。「クライアント証明書」には多種多様な使用用途があり、そしてそれは「クライアント証明書」のプロファイルで定義されています。「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、電子署名や電子メールの暗号化、及び暗号認証などがあります。「お客様」が「クライアント証明書」を要請する場合は、「お客様」は：（i）「CPS」の規定に従い、適切な社内文書を使って、申請者の身元と所属を確認し、そして（ii）「クライアント証明書」中の提供された情報、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実、完全、そして正確であることを確認しなければなりません。

10. 適格証明書

「**適格証明書**」(Qualified Certificates) とは、(i) 適用される欧州連合 (EU) 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、かつ (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」を意味します。

「**適格トラストサービスプロバイダー**」(Qualified Trust Service Provider) 又は「**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」の関係会社を意味します。「デジサート」の「QTSP」は、以下のとおりです：

QTSP 事業者	トラストリスト (Trusted List)	監督機関の管轄区域
QuoVadis Trustlink B.V.	オランダ・トラストリスト	オランダ王国
DigiCert Europe Belgium B.V.	ベルギー・トラストリスト	ベルギー王国
QuoVadis Trustlink Schweiz AG	スイス・トラストリスト	スイス連邦

「適格証明書」について、「お客様」は (i)「業界基準」により適格電子署名生成装置 (Qualified Signature Creation Device) (QSCD) の使用が要求される場合、「適格証明書」を保存する QSCD を使用して生成された電子証明書についてのみ「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にある自己の「秘密鍵」のみを維持し使用し、及び (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にある自己の「秘密鍵」のみを維持し使用するものとします。

11. 管理

通常「デジサート」は、「ポータル」を通じて「お客様」により提出された指示に従い、「証明書」を発行、管理、更新し、及び失効させますが、これは当該指示の正確性に対する「デジサート」の信頼を基礎とします。「お客様」は、「デジサート」との通信にあたっては正確で完全な情報を提供するものとし、そして「ポータル」におけるアカウントの情報に何らかの変更があった場合は、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」から質問があった場合、当該質問の通知を受領してから 5「営業日」以内に返答するものとします。「お客様」は、「証明書」を使用する前に「証明書」データが正確であるか照合し、そして確認するものとします。「証明書」は、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」を使用した証拠が存在する場合はその使用時に、承認されたものと見なされます。「デジサート」は、有効期限切れが迫った「証明書」に関する通知を送信することができま

すが、それを行う義務はなく、有効期限が切れる前に「証明書」を確実に更新する責任は、全面的に「お客様」にあるものとします。「**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意味します。

12. 登録局

公的に信頼された 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」の条件に従い、登録局 (Registration Authority) として指名されます（また「お客様」は、本書をもって、当該指名を承諾します）。「お客様」が登録局のいずれか機能を遂行する限りにおいて、「お客様」は、適用される「CPS」に従って当該機能を遂行するものとし、「お客様」が登録局として行動する場合、「デジサート」は、「お客様」の行為を信頼することができます。「お客様」は、「お客様」が厳格に登録局の義務を果たさなかったことにより生ずる、第三者によるあらゆる主張、訴訟、訴訟手続き又は判決から「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弁護し、免責し及び補償するものとします。「お客様」は、登録局として運営する場合、「本電子証明書利用規約」に基づき「証明書」を取得するサブスクライバー (Subscriber) 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は、「証明書」を取得する前にサブスクライバー契約書を承諾しなければなりません。

13. 鍵ペアのセキュリティと使用

「お客様」は、「証明書」と関連づけられている「鍵ペア」を安全に生成、保護し、そして「秘密鍵」の危殆化、紛失、不正使用を防ぐ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、ベストプラクティスを満たすよう、「CAB フォーラム」で定めるネットセキュリティ要件及びその他の関連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、その従業員、代理人や委託業者が「お客様」による（法律で許可される範囲の）身元調査と、「PKI」及びその他の情報セキュリティ分野の研修を受けているか、又は経験を有している場合にのみ、該当する従業員、代理人や委託業者にのみ、「秘密鍵」へのアクセス又は使用を許可するものとします。以下の場合、「お客様」は「デジサート」に通知をし、「証明書」とそれに紐づけられた「秘密鍵」の失効を要請し、当該「証明書」とそれに紐づけられた「秘密鍵」の使用を停止し、そして当該「証明書」がインストールされたすべてのデバイスから「証明書」を削除するものとします：（i）「証明書」のいずれかの情報が間違っているか正確でない又は正確でなくなる場合；又は（ii）「証明書」に含まれる「公開鍵」に紐づけられた「秘密鍵」の悪用又は危殆化が起こったか又は起こったことが疑われる場合。コードサイニング「証明書」に関しては、以下の状況であると「お客様」が判断した場合、速やかに「証明書」とそれに紐づく「証明書」の「秘密鍵」の使用を停止し、「証明書」の失効を要請するものとします：（a）「証明書」のいずれかの情報が間違っているか不正確である場合；（b）「証明書」に含まれる「公開鍵」に紐づけられた「秘密鍵」が悪用又は危殆化された場合；あるいは（c）「サスペクトコード」に署名するために「証明書」が使用された証拠がある場合。「**サスペクトコード**」(Suspect Code) とは、有害又は悪意のある機能、又は深刻な脆弱性を含むコード（スパイウェアやマルウェア、ユーザの承認なくインストールされ、及び／又は削除できないその他のコード、ならびにそれが実行されるプラットフォームの信頼性を失わせるような設計者の意図していない方法で利用可能なコードなどを含む）を意味します。お客様」は、異なる「証明書」の種類に同一の「秘密鍵」使用しないものとします。例えば、「お客様」は、コードサイニングに使用する「秘密鍵」を非コードサイニング「証明書」を要求するために使用しないものとします。「デジサート」が、ある特定の種類の「証明書」又はアクション（例えば、コードサイニング）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「証明書」又は「クライアント証明書」）を要求するために利用されていることを発見した場合、「デジサート」は、当該「秘密鍵」、若しくは「お客様」の関連する「ポータルアカウント」にあるか又はその他「デジサート」により発行された関連する「鍵ペア」に関連付けられた全ての「証明書」を失効しなければならないものとします。「お客様」は、「鍵ペア」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 時間以内に応答しなければならないものとします。「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「鍵ペア」の使用を停止するものとします：（I）「証明書」が失効された時；及び（II）許可されている「鍵ペア」の使用期間が切れた時。「お客様」は「証明書」の失効後は使用を停止しなければならないものとします。

14. 証明書の欠陥

「証明書」の不備（以下「**不備**」という）に対する「お客様」の唯一の救済策は、「お客様」から該当「不備」の通知を受け取った後、当該「不備」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」に要請することのみになります。以下の場合は、「デジサート」は「不備」を是正する義務はありません：（i）「お客様」による「証明書」の悪用や損壊、又は改造があった場合；（ii）「お客様」が「デジサート」に速やかに「不備」の報告をしなかった場合；又は（iii）「お客様」が「適用契約」のいずれかの条件に違反した場合。

15. 依拠当事者保証

「お客様」は、「依拠当事者保証」が依拠当事者の利益のためだけのものであることを確認します。「**依拠当事者保証**」(Relying Party Warranty) 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 (Relying Party Agreement) と限定保証 (Limited Warranty) の条件を満たす、依拠当事者に提供される保証を意味します。「QTSP」又は「デジサート」の関係会社から発行された「証明書」に対する「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します。「お客様」には、「依拠当事者保証」の条件を強制する権利、又は「依拠当事者保証」に基づく請求を行う権利を含め、「依拠当事者保証」に基づく一切の権利はありません。「**依拠当事者**」(Relying Party) とは、「依拠当事者保証」に規定される意味を持つものです。「アプリケーション・ソフトウェアベンダー」は、それが提供するソフトウェアが「証明書」に関する情報を表示するだけであったり、あるいは「証明書」や電子署名の使用を斡旋するだけであったりする場合は、「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. 表明

申請される各「証明書」について、「お客様」は以下を表明し保証します：

a. 「お客様」は（i）「証明書」で指定されているすべてのドメイン名、及び（ii）「証明書」で指定されているすべてのコモンネーム又は団体名を使用する権利を有しているか、又は正当な所有者であること；
b. 「お客様」は、権限を与えられた、合法的な目的にのみ「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；「証明書」と「秘密鍵」をすべての適用法令に準じ、「証明書」の目的、「CPS」、適用される証明書ポリシー、及び「適用契約」に従ってのみ使用すること。
c. 「お客様」は「CPS」を読み、理解し、そしてそれに同意すること。
d. 「CPS」又はパブリック証明書の発行及び管理に関する基本要件 (Baseline Requirements) の違反があった場合、「お客様」は速やかに書面で「デジサート」に通知し、及び
e. 「証明書」に含まれる団体と登録されたドメイン名の所有者が、各「証明書」申請を認知し、承認すること。

17. 制限

「お客様」は、TLS/SSL「証明書」を、発行された「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でのみ利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. いずれかの TLS/SSL「証明書」又は「秘密鍵」を修正、再許諾、又は派生物の作成をすること（意図された目的で「証明書」を使用するために必要な場合を除く）；
b. 他人のコンピュータの操作に損害を与えるようなファイルやソフトウェアをアップロード又は頒布すること；
c. 「CPS」で許可されている以外に、TLS/SSL「証明書」に関する表明を行うか、又は「証明書」を使用すること；
d. 「お客様」と団体との関係について偽証又は虚偽表示すること；
e. 「証明書」又は関連するソフトウェアやサービス（「ポータル」など）を、「お客様」や「デジサート」に対する民事又は刑事訴訟を招くような方法で使用すること；
f. 「証明書」又は関連するいずれかのソフトウェアを第三者の秘密を漏洩したり、未承認の大量通信（スパム）を送受信したりするために使用すること；
g. 「サスペクトコード」に署名する目的でコードサイニング「証明書」を利用すること；
h. 「証明書」の「公開鍵」が非コードサイニング「証明書」に使用されているか使用される場合に、コードサイニング「証明書」を申請すること；
i. 「デジサート」のウェブサイトの適切な機能、又は「デジサート」のウェブサイトを介して行われる取引を妨害すること；
j. 他の「証明書」を発行するために「証明書」を利用しようとすること；
k. 「デジサート」のシステム又はソフトウェアの技術実装を監視、妨害又はリバースエンジニアリングしたり、

又はその他「デジサート」のシステム又はソフトウェアのセキュリティを故意に危殆化すること；

l. 第三者の知的財産権を侵害する「証明書」情報を「デジサート」に提出すること；又は

m. 「デジサート」又は第三者の「秘密鍵」に実質的に類似した「秘密鍵」を故意に作成すること。

18. 証明書の失効

「デジサート」は「CPS」に記載される理由により、通知なく「証明書」を失効させることができますが、それには次のいずれかに該当すると「デジサート」が合理的に考える場合も含まれます：

a. 「お客様」が「証明書」の失効を申請したか、「証明書」の発行を許可しなかった場合；

b. 「お客様」が「適用契約」、又は「CPS」上の義務に違反した場合；

c. 「お客様」との契約の条項で、「証明書」の発行や使用、管理、又は失効に関連する表明又は義務を含むいずれかが解除されるか無効とされた場合；

d. 「お客様」が政府の取引禁止対象とされている個人又は団体リストに追加されるか、又は米国の法律で輸出禁止対象とされている仕向地から事業を行なっている場合；

e. 不正確又は誤解を招くような情報が「証明書」に含まれている場合；

f. 「証明書」が、意図された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；

g. 「証明書」に関連付けられた「秘密鍵」が開示又は危殆化された場合；

h. 「証明書」が（i）悪用された場合；（ii）法律や「CPS」又は「業界基準」に反して使用されるか発行された場合；又は（iii）フィッシング攻撃、詐欺、マルウェアの配信、その他の違法若しくは詐欺行為目的、又はデジサート利用規約 (DigiCert Acceptable Use Policy) に概説されるその他の違反行為などの違法若しくは詐欺行為目的で直接的又は間接的に使用された場合；又は

i. 「業界基準」又は「デジサート」の「CPS」により、「証明書」の失効が必要とされる場合、又は「デジサート」や第三者の権利、機密情報、事業、又は評判を保護するために失効が必要な場合。

19. 情報の共有

以下の場合、「デジサート」は、「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」、そして周辺環境に関する情報を、他の認証局や「CAB フォーラム」を含む業界団体と共有する権限を有していることを、「お客様」は承認し、そして受諾するものとします：（i）「証明書」又は「お客様」が「サスペクトコード」のソースであると同定された場合；（ii）「証明書」を申請するための権限が認証できない場合；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（たとえば「秘密鍵」の危殆化、マルウェアの発見などの結果）。

20. 業界基準

両当事者は、「証明書」に適用されるすべての「業界基準」と法律を遵守するものとします。適用法令や「業界基準」が変更され、その変更が「証明書」又は「適用契約」により提供されるサービスに影響する場合、「デジサート」は、その変更を遵守するために必要な限度で、サービスを変更若しくは「適用契約」を改正、又は終了させることができます。

21. 設備

「お客様」は、自らの費用で以下について責任を有するものとします：（i）「証明書」と関連する「デジサート」のソフトウェア又はサービスを利用するのに必要な、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、そして通信ネットワーク（それが必要な場合）；及び（ii）「お客様」の業務ならびに「お客様」のウェブサイトの保守、運営、開発そしてコンテンツ。

22. 証明書の受益者

「依拠当事者」と「アプリケーションソフトウェアベンダー」は、「証明書」の使用と発行に関する「お客様」の義務と表明の明示的な第三受益者です。「依拠当事者」と「アプリケーションソフトウェアベンダー」は、い

かなる「デジサート」のソフトウェアに関しても、その明示的な第三受益者ではありません。

23. プライベート証明書のための中間証明書

本第 23 条は、「お客様」が専用の「プライベートルート証明書」及び／又は申込書に記載の「プライベート証明書」又は公的に信頼された「証明書」を発行するための「中間証明書」を購入される場合についてのみ適用されます。

a. 作成 「適用契約」に従って該当する支払、ならびに以下 b 項に記述する「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」が必要とする情報の受領後 60 日以内に、「デジサート」は、(i) 公的に信頼されていない「証明書」又は (ii)「申込書」に記載された公的に信頼された「証明書」を「ポータル」から発行するための「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**」(Private Certificate) とは、いかなるトラストストア (trust store) にも埋め込まれていない「証明書」を意味します。「**ルート証明書**」(Root Certificate) とは、安全なオフライン状態で保管され、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」(self-signed Certificate) を意味します。「**中間証明書**」(Intermediate Certificate) 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」を発行するのに使用される「証明書」を意味します。

b. 内容 「デジサート」と「お客様」は誠意をもって協力し、「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ものとします。「お客様」は、「ルート証明書」及び／又は「中間証明書」の作成にかかる契約締結後 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「デジサート」に提供するものとします。「お客様」が当該期間内に要求される情報をすべて提供しない場合、「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」の作成の対価として支払われた料金を返還しません。「中間証明書」が作成された後は、「お客様」は当該「中間証明書」の内容を変更することはできませんが、「中間証明書」の同一複製は、必要に応じて何枚でも作成することができます。「中間証明書」には、10 年に設定された有効期間があり、それが経過すると、更新されることなく有効期限が切れます。「お客様」は、「中間証明書」から発行されるすべての「証明書」は、「中間証明書」の有効期間満了の少なくとも 2 年前までに有効期限が切れるようにすることに関し責任を負うものとします。「デジサート」は、「中間証明書」から発行されたなお有効な「証明書」を、「中間証明書」の終了から 2 年以内に失効させる権利を有します。「お客様」は、「中間証明書」を運用するのに必要な限度において。「お客様」のあらゆる商標又は「中間証明書」に含まれる「お客様」を特定する文字列を使用する権利を「デジサート」に許諾します。

c. 所有権 「デジサート」は「中間証明書」の唯一の所有者ですが、「本電子証明書利用規約」において別段の定めある場合を除き、「適用契約」に基づき発行された「中間証明書」を、「ポータル」を介して「お客様」から提供される指示に従ってのみ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、「お客様」のエンドユーザそして顧客に配布することができます。

d. 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」の安全な「PKI」システムにホストします。いかなる理由であっても、「お客様」は「中間証明書」の「秘密鍵」を「デジサート」の「PKI」システムから削除したり、又は第三者によって削除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、ホストします。「デジサート」は、「適用契約」終了後も、「適用契約」に基づき発行されたすべての「証明書」の期限が切れるか失効するまで、CRL/OCSP サービスの提供を継続するものとします。公的に信頼された「証明書」を発行する「中間証明書」については、「中間証明書」は公的に信頼された「証明書」を発行し、「デジサート」の「PKI」でホストされ「デジサート」の職員により管理されるものであるため、「中間証明書」は「デジサート」の WebTrust 監査の対象となります。「業界基準」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」の監査を別途要求するように変更された場合、その時は「デジサート」と「お客様」は要求される監査を受けられるよう誠意を持って協力するものとします。

e. 失効 「デジサート」は以下の場合に「中間証明書」を失効する権利を有するものとします：（i）「お客様」が特定の「業界基準」違反を摘示し「デジサート」に書面で失効を申請した場合；（ii）「中間証明書」が危殆化されたと「デジサート」が信じるに足る根拠がある場合；（iii）「お客様」が「適用契約」の重大な違反を犯した場合で、その違反に関する通知を受領してから 30 日内に是正をしなかったとき；（iv）「お客様」が、「中間証明書」を使用する権利が切れた後も「中間証明書」の使用を継続する場合；又は（v）失効が「業界基準」により要求されると「デジサート」が合理的に判断する場合。

f. 制限 「お客様」は以下を行わないものとします：（i）「中間証明書」から追加の「中間証明書」を作成、又は作成と試みること；（ii）「中間証明書」をいずれかの第三者に販売、配布、貸出、貸与、使用許諾、譲渡、又はその他の方法で移転すること；（iii）「デジサート」が提供した「中間証明書」を、その有効期限切れ、

失効又は「適用契約」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」を変更、修正、又は改定すること；又は（v）「お客様」が「中間証明書」の「秘密鍵」が危殆化されたと信じるに足る理由があるにも関わらず、その「中間証明書」を使用すること。

24. エンドユーザライセンス契約（EULA）と第三者の条件

a. 装置又はデバイスへのインストール用ソフトウェア（以下「**許諾ソフトウェア**」という）としての「お客様」による「デジサート」サービス（又はそのコンポーネント）の利用は、「許諾ソフトウェア」に付属するライセンス契約に準拠するものとします。ただし、「許諾ソフトウェア」にライセンス契約が付属しない場合は、当該「許諾ソフトウェア」の使用は、http://www.digicert.com/eula にあるソフトウェア・エンドユーザー・ライセンス契約（「以下 **EULA**」という）に準拠するものとします。

b. 「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 (legal entity identifier)（以下「**LEI**」という）が含まれる場合、https://rapidlei.com/documents/global-lei-system-terms/ から入手可能な RapidLEI サービス利用規約 (RapidLEI Terms of Service) が、「お客様」の LEI と、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使用に適用されることを認識し、同意するものとします。

c. 「お客様」による「デジサート」の耐量子暗号ツールキット (post-quantum cryptographic toolkit)（以下「**PQC ツールキット**」という）の使用は、次の条件に従うものとします：（i）「お客様」に対して許諾される「PQC ツールキット」に関するライセンスは非独占的で、解除可能なライセンスであり、当該ライセンスは「PQC ツールキット」又は関連検査と設定活動により生成された署名と「公開鍵」を含む「デジサート」の「証明書」についてのみ使用します；（ii）「お客様」は、「PQC ツールキット」又はそれに関連する知的財産に係る知的財産権又はその他の専有権を一切取得するものではありません；（iii）「お客様」は、「PQC ツールキット」に対して、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、又は破壊を行いません；（iv）「お客様」は、「デジサート」の関連サービス終了時に「PQC ツールキット」の使用を中止します；（v）ISARA 社は、いかなる損害についても「お客様」に対して責任を負いません；（vi）「お客様」は、「PQC ツールキット」が使用又は輸入された国又は地域、若しくは「PQC ツールキット」が輸出又は再輸出された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とします；（vii）「デジサート」は ISARA 社に代わって明示黙示の如何を問わず「PQC ツールキット」に関連する保証を一切行いません；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著作権、商標又は特許表示を変更しないものとします。

d. 「お客様」が「デジサート」から Thales, Gemalto 又は SafeNet 製品又はサービスを購入する場合、当該製品又はサービスの「お客様」による使用は、https://cpl.thalesgroup.com/legal で入手可能な Thales エンドユーザーライセンス契約書 (Thales End User License Agreement) に従うものとし、「デジサート」を介した Thales のクラウドベースサービスの購入は、https://www6.thalesgroup.com/service-specific-terms で入手可能な条件に従うものとします。

25. 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セキュリティの技術的実装を監視、妨害、リバースエンジニアリングしたり、又はその他の方法で危殆化しないものとし、また指定された製造業者がある場合、同様の義務を課すものとします。

26. Microsoft 社要求追加義務

a. 「お客様」が Microsoft 社自動登録コンポーネント (Microsoft Auto Enrollment component) を使用する場合は、以下の Microsoft 社の要求補足義務が適用されます：

b. 保証の否認．Microsoft 社とその関連会社は、「適用契約」に基づいて提供されるサーバソフトウェア（以下「**サーバソフトウェア**」）に関して明示、黙示又は法令上の如何を問わず一切の保証を行わず、その実行又は実行不能について一切の責任を負いません。Microsoft 社の「サーバソフトウェア」は、現状有姿の無保証条件で提供されます。Microsoft 社とその関連会社は、本書をもって、「サーバソフトウェア」に関して明示、黙示又は法令上の如何を問わずその他一切の保証、義務、条件（商品適格性、特定目的適合性、信頼性、可用性についての黙示の保証と条件を含むが、これに限定されない）を否認するものとします。また、Microsoft 社とその関連会社は、「サーバソフトウェア」に関して、権原、平穏享有、記述に対する適合性、非侵害性に対する一切の保証及び条件を否認するものとします。

c. 特定の損害の除外．適用法令によって許容される最大限の範囲で、いかなる場合においても、Microsoft 社は、「サーバソフトウェア」の使用又は使用不能、あるいは「サーバソフトウェア」を通じたサポートやその他のサービス、情報、ソフトウェア、関連コンテンツの提供又は不提供、あるいはこれらのサービス記述書の条件に起因若しくは関連する、特別損害、付随的損害、懲罰的損害、間接損害、結果的損害、その他一切の損害（利益の損失、機密情報やその他の情報の喪失、事業の中断、人身傷害、プライバシーの喪失、誠実義

務の不履行、注意義務の不履行、過失、その他の金銭的損失、その他一切の損失による損害を含むが、これに限定されない）に対して、それが Microsoft 社の過失、不法行為（過失を含む）、厳格責任違反、契約違反、保証違反によるものであったとしても、また、かかる損害が発生する可能性を Microsoft 社が事前に通知されていた場合であっても、一切の責任を負わないものとします。

d. サーバソフトウェア要件. 「お客様」は、「サーバソフトウェア」の付属文書に明示されているとおり、「適用契約」に基づいて提供される「サーバソフトウェア」を（適用される注文書において別段定めのない限り）一部に限り使用できるものとし、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（又はその後継）との相互運用や通信のみを目的として使用できます。「お客様」は、いかなる状況であっても、「パーソナルコンピュータ」上で「サーバソフトウェア」を使用することはできません。上記において「**パーソナルコンピュータ**」とは、一度に一人のユーザが使用することを主な目的として構成され、ディスプレイやキーボードを備えたコンピュータを意味します。

e. 第三受益者. 「適用契約」の矛盾する条項にもかかわらず、「お客様」は、本書をもって、Microsoft 社は、「サーバソフトウェア」に含まれる知的財産権のライセンサーとして、本第 25 条の条件の第三受益者として意図されており、Microsoft 社の知的財産や本条の条件に関連する Microsoft 社のその他の権益に影響を与える条件を行使する権利を持つことに同意するものとします。

f. クラス 2 サーバ. 「お客様」がクラス 2 サーバを選択した場合、「お客様」は（a）最大処理能力が 32 ビット、RAM 4GB のプロセッサ 4 基以下で構成され、かつ（b）「サーバソフトウェア」が動作しているサーバを再起動することなくメモリの追加、交換、取り外しができる能力（以下「**ホットスワップ機能**」という）を持たないサーバ上で、「サーバソフトウェア」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」や「クラスタ機能」をサポートするソフトウェアと一緒に、「サーバソフトウェア」を使用することはできません。ここで言う「**クラスタ機能**」とは、複数のサーバをグループ化し、グループ内のサーバノード間でアプリケーションのフェイルオーバーを行うことで、アプリケーション実行のための単一の高可用性プラットフォームとして機能させることを意味します。

g. 監査権. 「デジサート」は、「お客様」が本条のすべての条項を遵守していることを確認するため、「お客様」の監査を実施し、通常の営業時間中に「お客様」の敷地内で「お客様」の施設と手続きを調査する場合があります。「適用契約」の条項と矛盾する場合でも（機密保持規定を含むが、これに限定されない）、「お客様」がそういった監査を受けることを拒否し、また「お客様」がサービス記述書の条件を遵守していないと「デジサート」が信じるに足る正当な理由がある場合、「お客様」は「デジサート」が以下を行うことができることに同意するものとします。（i）「お客様」の身元を、「依拠当事者」と「アプリケーションソフトウェアベンダー」に開示すること、及び（ii）不遵守に対する「デジサート」の根拠を開示すること。

h. 多重化デバイス. 「サーバソフトウェア」により提供されるサービスに直接アクセスし、又は使用するユーザ数を減らすハードウェア又はソフトウェアを使用した場合でも、「サーバソフトウェア」により提供されるサービスにアクセス又は使用していると見なされるユーザー数を減ずるものではありません。「サーバソフトウェア」にアクセスするユーザ又は使用するユーザの数は、直接又は「多重化デバイス」を介するかの如何を問わず、（a）「サーバソフトウェア」、又は（b）その他のソフトウェアあるいはシステムで、当該ソフトウェアあるいはシステムに対する認証又は承認が「サーバソフトウェア」により行われるもの（以下「**その他の認証対象システム**」という）によって提供されるサービスにアクセス又は使用するユーザ数と等しいものとします。ここでいう「**多重化デバイス**」とは、「サーバソフトウェア」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対するアクセスを直接的又は間接的に可能とする、あるいは複数のユーザが少ない接続数でアクセスできるようにするためのハードウェア又はソフトウェアを意味します。

i. Windows CAL 要件. 「お客様」は、直接であるか「多重化デバイス」を介するかの如何を問わず、「サーバソフトウェア」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アクセスする各ユーザ又はそれらを使用する各ユーザに、個別の 「Windows CAL」 を取得して割り当てる必要があります。「**Windows CAL**」とは、（a）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 Server**」という）用の、Windows デバイスのクライアントアクセスライセンス (Windows Device Client Access License) （以下「**CAL**」という）又は Windows ユーザ CAL (Windows User CAL)、若しくは（b）「Windows Server」にアクセスして使用する権利を個々のユーザや電子デバイスに与える Microsoft コア CAL (Microsoft Core CAL) を意味します。この（a）と（b）のいずれの場合でも、「CAL」 は、ユーザーが 1 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で使用するために取得し、かつ、ユーザ単位又はデバイス単位で利用されます。

27. Adobe 社要求追加義務

「お客様」が Adobe 署名「証明書」の発行を受けた場合、以下の条件に同意するものとします：

a. 「お客様」は 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 で現在入手可能な Adobe Systems Inc. AATL 証明書方針第 2.0 版 (Adobe Systems Inc. AATL Certificate Policy 2.0) を遵守するものとします。当該方針は後述の条件を含みますがそれに限定されません： (1) FIPS 140-2 レベル 2 のデバイスを使用するためにのみ Adobe 署名「証明書」の「鍵ペア」を生成し保存すること；及び (2) 新しいアカウントの登録されたとき、又はサブスクライバーのための新しい AATL 証明書登録が開始されたときに、「お客様」が「デジサート」に正確かつ真実の情報を提供すること。なお正確かつ真実の情報の提供に際しては以下が要求されます：(A) アカウント管理者が、「デジサート」との対面会議又は同等の保証を提供する手順（安全なビデオ通信など）に基づいて強力な身元確認を実行すること；(B) アカウント管理者が、「デジサート」が管理者に証拠資料や録音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いて強力な身元確認を実行し、監査を裏付けるための記録を構内に保存すること；及び (C) 管理者又はサブスクライバーの如何を問わず、身元確認手続きには、サブスクライバー自身を表示するサブスクライバー記録と、サブスクライバーと一致する写真を表示する有効な政府発行の身分証明書（運転免許証、パスポート、国民識別番号証明書など）の記録を含めること；及び

b. 適用される「CPS」の条件。

28. コードサイニング証明書に対する追加制限. 「お客様」は、コードサイニング「証明書」を次のいずれにも使用しないものとします：（i）「お客様」の組織以外の団体のために、又はその代理としてコードサイニング「証明書」を使用すること；（ii）「お客様」が提出された「証明書」申請書に記載されている「お客様」のドメイン名及び／又は団体名以外のものに関連して「秘密鍵」又は「公開鍵」の実行に使用すること；（iii）「サスペクトコード」を頒布するために使用すること；又は（iv）「証明書」の「公開鍵」に対応する「秘密鍵」へのアクセスの管理を、「お客様」が権限を付与した従業員以外の者に移転するか又は許可するような方法で使用すること（なお、当該移転は「秘密鍵」を保護するために安全な方法で行われるものとします）。

29. 非公開 TLS/SSL 証明書に対する追加制限. プライベート「ルート証明書」に紐づけられた TLS/SSL「証明書」は、イントラネットドメイン名でのみ使用し、インターネットから一般にアクセスできる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」が確実に本条に遵守すべく、一般公開されているインターネットサーバ及び／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、本条を遵守していないプライベート TLS/SSL「証明書」の利用を発見した場合、直ちに「お客様」に不遵守を通知します。「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」をイントラネットのドメイン名に移行させるか、又は（ii）「お客様」のサーバからプライベート TLS/SSL「証明書」を削除し失効させなければならないものとします。「お客様」が不遵守の「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ます。

[以下余白]