digicert

DIGICERT X9 PKI

CERTIFICATE TERMS OF USE
電子証明書利用規約

1. Scope and Purpose
適用範囲及び目的

Short version: *These Terms apply only to DigiCert's X9 PKI certificates. They incorporate the X9 CP, the DigiCert CPS, and reflect industry standards tailored for the high-assurance needs of the financial industry and similarly regulated environments. (They do* ***not*** *cover DigiCert's Web PKI certificates or any other non-X9 certificate services.)*
要約版： *この規約は、デジサートの X9 PKI 証明書にのみ適用します。この規約は、X9 CP、DigiCert CPS の一部を構成し、金融業界及び同様に規制される環境の高保証要求に適合した業界規格を反映しています。（この規約は、デジサートの Web PKI 証明書又はその他のいかなる非 X9 証明書サービスを対象とするものでは****ありません****。）*

These Terms apply to X9 PKI certificates issued by DigiCert or its affiliates under the governance of the Accredited Standards Committee X9, Inc. ("X9 ASC"). They do not apply to certificates outside the X9 PKI, such as DigiCert's publicly trusted Web PKI certificates or other certificate types and services not governed by X9. These Terms incorporate the DigiCert X9 Financial PKI Certificate Policy and applicable policy documentation ("X9 CP") and DigiCert Certification Practices Statement for Private PKI (the "DigiCert CPS"), which together with these Terms set forth how X9 certificates are issued, managed, and revoked. The X9 CP is available upon request at https://x9.org/x9-financial-pki-qa/, as updated from time to time, with a copy for reference purposes only available at https://www.digicert.com/legal-repository/, as updated from time to time (the "DigiCert Legal Repository"). The DigiCert CPS is available at the DigiCert Legal Repository. These Terms reflect the policies and requirements established for the X9 PKI, which are intended to address the requirements of financial industry or other high-assurance PKI. (They differ from the CA/Browser Forum Baseline Requirements and other guidelines that apply to publicly trusted TLS certificates.)
この規約は、the Accredited Standards Committee X9, Inc. ("X9 ASC") の規定に基づきデジサート又はその関係会社により発行される X9 PKI 証明書に適用します。この規約は、デジサートの公的に信頼される Web PKI 証明書その他の X9 ASC により管理されない他の種類の証明書及びサービスなどの X9 PKI 以外の証明書には適用しません。この規約は、この規約とともに X9 証明書の発行、管理及び失効の方法を定める、DigiCert X9 Financial PKI Certificate Policy 及び適用されるポリシー文書 ("X9 CP") 並びに DigiCert Certification Practices Statement for Private PKI ("DigiCert CPS") の一部を構成します。随時改定される X9 CP は、要求により https://x9.org/x9-financial-pki-qa/ で入手できますが、参照のみを目的とするその写しが https://www.digicert.com/legal-repository/ ("DigiCert Legal Repository") で閲覧できます。随時改定される DigiCert CPS は、DigiCert Legal Repository で閲覧できます。この規約は、金融業界及び高保証 PKI の要求に対処することを目的とする、X9 PKI について確立されたポリシー及び要件を反映しています。（この規約は、CA/Browser Forum Baseline Requirements 及びその他の公的に信頼される TLS 証明書に適用される指針とは異なります。）

2. Use of X9 Certificates
X9 証明書の利用

Short version: *You may use an X9 PKI certificate only for authorized use cases defined in the X9 CP and only within your authorized systems or domains. These use cases include, but are not necessarily limited to, those relevant to the financial sector.*
要約版： *お客様は、X9 CP において定められる認定ユースケースについてのみ、かつお客様の認定システム及び領域内においてのみ、X9 PKI を利用することができます。これらのユースケースには金融部門に関連するものが含まれますが、必ずしもこれに限定されるものではありません。*

X9 certificates must only be used for the specific use cases authorized under the X9 CP and reflected in the certificate itself. Examples include:
X9 証明書は、X9 CP に基づき認定され、かつ証明書自体に反映された特定のユースケースについてのみ利用しなければなりません。例としては、次のものが挙げられます：

- mTLS and client authentication
  mTLS 及びクライアント認証
- Closed-network device authentication
  クローズドネットワークディバイス認証
- Secure API communication
  セキュアな API 通信
- Digitally signed messages in the financial domain
  金融領域におけるデジタル署名されたメッセージ

X9 certificates are not intended for public TLS/SSL web PKI, public S/MIME e-mail, or other general purposes outside the X9 trust framework.
X9 証明書は、公的に信頼された TLS/SSL web PKI、パブリック S/MIME 電子メール又はその他の X9 トラストフレームワーク以外の汎用的な目的を対象とするものではありません。

Certificates must only be installed on systems or services under your administrative control and used in accordance with the intended key usage and extended key usage extensions.
証明書は、お客様の管理下にあるシステム又はサービスにインストールされ、意図された鍵用途 (Key Usage) 及び拡張鍵用途 (Extended Key Usage) 拡張機能にしたがって利用しなければなりません。

While the certificate's technical fields may support broader uses, only authorized PKI purposes are permitted. Use outside these constraints may result in revocation and is not supported. While X9 certificates are issued for defined purposes based on certificate type and profile as set forth in the X9 CP, DigiCert may, in consultation with the X9 Policy Authority, approve expanded or adjacent use cases that maintain consistent key usages (e.g., client authentication). Such approvals must remain within the technical and security bounds of the X9 CP and may be subject to supplemental agreement, verification, or policy review.
証明書の技術分野は広範な利用に対応していますが、認定された PKI 目的のみが認められます。これらの制限された目的以外の利用をすると、失効となることがあります。これらの制限された目的以外の利用には対応していません。X9 証明書は、X9 CP において定められた証明書の種類及びプロフィールに基づき、定められた目的について発行されますが、デジサートは、X9 ポリシー承認局と協議の

うえ、一貫性のある鍵用途を保持する拡張又は近似のユースケース（例えば、クライアント認証）を承諾することがあります。当該承諾は、X9 CP の技術上及びセキュリティ上の範囲内でなければならず、補足契約、認証又はポリシーの見直しが条件となることがあります。

3. Requesting a Certificate
証明書の要求

Short version: *When you request an X9 certificate, you must provide truthful, accurate information and have authority to request a certificate for the entity, domain, and/or device identified.*
要約版： *お客様が X9 証明書を要求するとき、お客様は、真実で、正確な情報を提供し、指定された団体、ドメイン及び/又はディバイスに係る証明書を要求する権限を有していなければなりません。*

When requesting a DigiCert X9 PKI certificate, you must submit complete, accurate, and truthful information. You must be properly authorized to request a certificate for the organization, individual, device, and/or any domain name(s) or other identifiers included in your request. Do not submit certificate requests for domains or resources that you do not own or control, and do not include any information (such as organization names, trademarks, or other identifiers) that you are not authorized to use.
X9 PKI 証明書を要求するとき、お客様は、完全、正確かつ真実の情報を提出しなければなりません。お客様は、組織、個人、ディバイス及び/又はあらゆるドメイン名その他のお客様の要求に含まれる識別子に係る証明書を要求する正当な権限を有していなければなりません。お客様が所有又は管理していないドメイン又はリソースの証明書要求は行わないでください。また、お客様が利用する権限を有さないいかなる情報（例えば、組織名、商標又はその他の識別子）も含めないでください。

By submitting a certificate request, you represent and warrant that: (a) you have the lawful rights and authority to use and control all names, identifiers, and information (including any domain names, IP addresses, organization details, etc.) that you include in the certificate request; and (b) your request and the issuance of the certificate will not infringe upon or misappropriate the intellectual property rights or other legal rights of any third party. Any misuse of the enrollment process, any material misrepresentation of facts, or any provision of false or unauthorized information will result in denial of your request and may result in revocation of any certificate that might have been issued in reliance on such information.
証明書要求を提出することにより、お客様は、次の各号に掲げる事項を表明し、これを保証します：（a）お客様は、お客様が証明書要求に含めるすべての名称、識別子及び情報（あらゆるドメイン名、IP アドレス、組織の細目などを含む）を使用し、管理する正当な権利及び権限を有していること；及び（b）お客様の要求及び証明書の発行が知的財産権その他の第三者の法的権利を侵害し又は盗用するものではないこと。申込手続きの悪用、事実の重大な不実表示又は虚偽若しくは無許諾の情報提供を行うと、お客様の要求は拒否されます。また、当該情報に依拠して発行されたかもしれない証明書が失効されることがあります。

4. Verification Before Issuance
発行前検証

Short version: *Either DigiCert or your institution (if acting as an RA) will perform identity checks before certificate issuance.*

要約版：デジサート又はお客様の機関（RA を務める場合）は、証明書発行前の本人確認を実施します。

X9 certificates may only be issued after successful identity and authorization verification, consistent with the X9 CP and applicable CPS. In some cases, your institution will act as a Registration Authority (RA), conducting verification internally in accordance with X9 standards. In other cases, DigiCert may perform these steps directly.
X9 証明書は、X9 CP 及び適用される CPS に従って、成功裏の本人及び権限検証後にのみ発行されます。場合によっては、お客様の機関が X9 規格に従って内部で検証を行う登録局 (RA) を務めます。その他の場合には、デジサートが直接これらの手続きを実施することができます。

The specific procedures depend on the certificate type and intended use, and may include:
具体的な手続きは証明書の種類及び意図された用途によって決まりますが、手続きとしては、次のものが挙げられます：

- Organization or domain validation
  組織又はドメイン認証
- Device or software identity checks
  ディバイス又はソフトウェア同一性確認
- Role-based authorization verification
  ロールベースの権限検証
- Cross-checks with government or industry data sources
  政府又は業界データソースとの照合

All certificates are subject to DigiCert's final approval, even if your institution acts as the RA. DigiCert may decline to issue a certificate if it believes the request does not meet the X9 CP requirements or if it identifies a security or compliance concern.
お客様の機関が RA を務める場合といえども、証明書はすべてデジサートの最終承認に服します。デジサートは、要求が X9 CP の要件を満たしていないと判断した場合、またはセキュリティ上又はコンプライアンス上の懸念点を確認した場合、証明書の発行を拒否できます。

5. Registration Authority Representations, Warranties, and Indemnity
登録局の表明、保証及び補償

If your organization acts as a RA, you represent and warrant that:
お客様の機関が RA を務める場合、お客様は、次の各号に掲げる事項を表明し、これを保証します：

(a) You will perform all identity validation and certificate request functions in full compliance with the X9 CP, the applicable CPS, and these Terms;
お客様は、X9 CP、適用される CPS 及びこの規約に完全に準拠した本人検証及び証明書要求機能をすべて実施するものとします；

(b) You have trained personnel, implemented appropriate background checks, and maintain secure infrastructure to fulfill your RA duties; and

お客様は、要員を教育し、適切なバックグラウンドチェックを実施しており、お客様の RA としての義務を履行するためのセキュアな基盤を保持しています；及び

(c) You will maintain accurate records and support audit rights as required under the X9 CP.
お客様は、正確な記録を保持し X9 CP に基づき要求される監査権に対応するものとします。

You agree to indemnify, defend, and hold harmless DigiCert Inc., its affiliates, and X9 ASC (and its Policy Authority) from any claims, damages, losses, liabilities, or costs (including reasonable attorneys' fees) arising out of or related to your acts or omissions as an RA, including without limitation: (i) failure to perform identity verification in accordance with the X9 CP, (ii) issuance or misrepresentation of certificate information, or (iii) unauthorized use or disclosure of private keys or applicant data.
お客様は、お客様の RA としての作為又は不作為に起因する又は関連するあらゆる申立て、損害賠償額、損失、債務又は費用（合理的な弁護士費用を含みます）について、DigiCert, Inc.、その関係会社及び X9 ASC（及びそのポリシー承認局）を補償、防禦し及び免責することに合意します。お客様の RA としての作為又は不作為には次の各号に掲げる事由を含みますが、これに限定するものではありません：(i) X9 CP に従った本人検証の不実施、(ii) 証明書情報の発行又は不実表示、又は (iii) 秘密鍵若しくは申込者データの不正利用又は不正開示。

6. How Long Certificates Last
証明書の有効期間

Short version: *X9 certificates can be issued for longer periods than Web PKI certificates, but they still expire, and can never outlive the root certificate key that issued them. OCSP keys have a three-year maximum. Use automation to stay ahead of expirations.*
要約版： *X9 証明書は Web PKI 証明書より長期間の発行が可能ですが、やはり X9 証明書も有効期間満了により終了し、X9 証明書を発行したルート証明書の鍵よりも長く存続することはできません。OCSP 鍵の最長有効期間は 3 年です。X9 証明書の有効期間は自動管理するようにしてください。*

X9 certificates are issued for periods defined by your requirements, subject to the X9 CP and DigiCert CPS. However, all certificates expire and must be replaced before their expiration date to remain valid. In all cases, no certificate may have a validity period that exceeds the lifetime of the issuing CA's private key. Additionally, the maximum private key usage period for OCSP responders is limited under the X9 CP. DigiCert will enforce this and other lifecycle constraints as defined in the applicable certificate profiles and policies.
X9 証明書は、X9 CP 及び DigiCert CPS に従って、お客様の要求により定められた期間発行されます。ただし、すべての証明書は有効期間満了により終了するため、証明書を有効に維持するため満了日前に新しい証明書と入れ替えなければなりません。いかなる場合においても、いかなる証明書も、証明書を発行する CA の秘密鍵の存続期間を超える有効期間を有することはできません。さらに、OCSP レスポンダの秘密鍵の最長利用期間は、X9 CP によって制限されています。デジサートは当該秘密鍵の最長利用期間並びにその他の適用される証明書プロフィール及びポリシーにおいて定められた存続期間制限事項を確実に遵守します。

To avoid service interruption, you are responsible for tracking expiration and ensuring timely renewal or reissuance of all certificates in your environment. DigiCert strongly recommends

implementing automated certificate lifecycle management using solutions like DigiCert® Trust Lifecycle Manager or other compatible tooling.
サービスの中断を回避するため、お客様は、お客様の環境にあるすべての証明書の有効期間満了による終了の把握及び適時の更新又は再発行について責任を負います。デジサートは、DigiCert® Trust Lifecycle Manager 又はその他の適合するツールを利用して自動化された証明書ライフサイクル管理を実施することを強く推奨します。

7. Your Responsibilities as a Subscriber
サブスクライバーとしてのお客様の責任

Short version: *You must safeguard your private key, use the certificate only as permitted (within its intended scope and systems), cease using it if any information becomes incorrect or it's compromised, and cooperate with DigiCert on any certificate-related inquiries. These obligations are required by X9 certificate policy and are crucial for security.*
要約版：*お客様は、お客様の秘密鍵を保護し、認められた限度で（その予定された範囲及びシステム内で）のみ証明書を利用し、いずれか情報が正確でなくなった場合又は危殆化された場合には証明書の利用を停止し、証明書関連の照会についてデジサートと協力しなければなりません。これらの義務は、X9 証明書ポリシーにより要求されており、セキュリティ上極めて重要です。*

As the Subscriber (as defined in the X9 CP), you have important obligations to ensure that the certificate is used securely and only in accordance with these Terms and the X9 CP. **By applying for or obtaining an X9 certificate, you agree, represent, and warrant to DigiCert that you have the authority to accept and bind your organization (if applicable) to these Terms (including the incorporated X9 CP), and that you will do all of the following:**
サブスクライバー（X9 CP において定義される）として、お客様は、安全な方法で、かつこの規約及び X9 CP に従ってのみ証明書が利用されることを確保する重要な義務を負っています。**X9 証明書を申し込み又は X9 証明書を取得することにより、お客様は、デジサートに対し、お客様がお客様の組織（該当する場合）をこの規約（その一部を構成する X9 CP を含む）に拘束する権限を有していること、及び次の各号に掲げる事項を行うことに合意し、表明し、これを保証します：**

(a) **Accuracy of Information:** Provide accurate and complete information at all times in your certificate request and in all communications with DigiCert related to the certificate's issuance and maintenance. If any information you provided becomes outdated or changes during the validation process or the certificate's validity period, you will promptly inform DigiCert or update the information as required.
情報の正確性： お客様の証明書要求において並びに証明書の発行及び維持管理に関連するデジサートとのすべての連絡において、常に正確で完全な情報を提供すること。お客様が提供したいずれか情報が、検証手続き中若しくは証明書の有効期間中に最新でなくなったか又は変更された場合、お客様は、速やかにデジサートに連絡するか又は情報を更新するものとします。

(b) **Protection of Private Key:** Securely generate your certificate's private key using trustworthy systems and strong cryptographic standards (for example, at least a 2048-bit RSA key or an equivalent strength elliptic curve key, unless stronger requirements are defined by the X9 CP/CPS). You will take all reasonable measures to keep the private key

confidential and under your sole control. This includes using appropriate hardware or software security modules, protecting any passwords or tokens associated with the key, and preventing any unauthorized access to the private key. Do not share or disclose the private key to any unauthorized person.

秘密鍵の保護： 信頼できるシステム及び強度の暗号化規格（例として、X9 CP/CPS により、より強度な要件が定められていない限り、少なくとも 2048-bit RSA 鍵又は等価強度の楕円曲線鍵）を利用して安全な方法でお客様の秘密鍵を生成すること。お客様は、秘密鍵を秘密に保持し、お客様の単独の管理下に置くため、すべての合理的な手段を講じるものとします。これには、適切なハードウェア又はソフトウェアセキュリティモジュールを利用すること、鍵と関係付けられたあらゆるパスワード又はトークンを保護すること、及び秘密鍵に対するあらゆる不正アクセスを防止することを含みます。秘密鍵を関係者以外の者と共有又は開示しないでください。

(c) **Acceptance of Certificate:** Upon issuance of the certificate by DigiCert, promptly review the certificate's details (such as the subject name, organization information, domain names or other identifiers, and any other included data) to ensure everything is correct. If you discover any inaccuracies or issues, notify DigiCert immediately. You will only install or use the certificate after confirming that all details in it are accurate and that you accept the certificate.

証明書の検収： デジサートによる証明書の発行後速やかに、すべてが正しいことを確保するため、証明書の細目（例えば、サブジェクト名 (subject name)、組織名 (organization name)、ドメイン名 (domain name) 又は他の識別子及びその他の記載データなど）を審査すること。お客様が不正確な情報又は問題点を発見した場合、直ちにデジサートへ連絡してください。お客様は、証明書の細目のすべてが正確であること、及びお客様が証明書を検収したことを確認したあとにのみ証明書をインストールし又は利用するものとします。

(d) **Use of Certificate:** Install and use the certificate only on the server(s), device(s), software, or environment that is intended and authorized, as identified by the certificate's content. This means, for example, that a server TLS certificate should be installed only on the server(s) accessible by the domain name(s) or host identifiers listed in that certificate, an email certificate should be used only for the email address or user specified, and a code signing certificate should be used only to sign code on behalf of the organization or entity named. You agree to use the certificate only in compliance with all applicable laws and regulations, and solely in accordance with these Terms (including the incorporated X9 CP/CPS). The certificate may not be used on any system or by any entity other than those for which it was issued, and you must not use the certificate for any purpose other than securing the communications or transactions for which the certificate was intended.

証明書の利用： 証明書の内容により特定される方法で、承認された対象サーバー、ディバイス、ソフトウェア又は環境においてのみ証明書をインストールし、利用すること。これは、例えば、サーバーTLS 証明書は証明書に記載されるドメイン名又はホスト識別子によりアクセス可能なサーバー上にのみインストールすべきこと、電子メール証明書は特定された電子メールアドレス又はユーザーについてのみ利用すべきこと、及びコードサイニング証明書は指名された組織又は団体を代理してコードに署名するためにのみ利用すべきことを意味しま

す。お客様は、適用法令に従ってのみ、かつこの規約（その一部を構成する X9 CP/CPS を含む）に従ってのみ証明書を利用することに合意します。証明書はその発行対象であるシステム又は団体以外のシステム上で又は団体により利用できないものとし、お客様は、証明書の対象である通信又は取引を保護する以外のいかなる目的についても証明書を利用してはなりません。

(e) **Reporting and Revocation:** If you suspect that the certificate's private key has been compromised or exposed in any way, or if you become aware of any misuse of the certificate, you will immediately notify DigiCert and promptly request that the certificate be revoked. Similarly, if any information in the certificate is or becomes false, inaccurate, or misleading at any time (for example, if you no longer own or control a domain name included in the certificate, if your organization's name or address changes, or if any other detail in the certificate is no longer valid), you must immediately cease using the certificate and promptly request that DigiCert revoke the certificate. You should not wait for DigiCert or any other authority to detect such issues—initiation of revocation in these cases is your responsibility.
報告及び失効： お客様が証明書の秘密鍵が何らかの方法で危殆化又は流失したとの疑念を持つ場合、又はお客様が証明書の不正利用を知った場合、お客様は、直ちにデジサートに連絡し、速やかに証明書の失効を要請するものとします。同様に、いつでも証明書中のいずれか情報が正しくないか又は正しくなくなった場合、不正確か又は不正確になった場合、又は誤解を招くか又は誤解を招くようになった場合（例えば、お客様が証明書に記載されているドメイン名をもう保有又は管理していない場合、お客様の組織の名称又は所在地が変更された場合、又は他のあらゆる証明書の細目がもう有効ではない場合）、お客様は、直ちに証明書の利用を停止し、速やかに証明書の失効をデジサートに要請するものとします。お客様は、デジサート又は他の機関がこれらの問題を探知するのを待っていてはいけませんーこれらの場合において失効手続きを開始するのは、お客様の責任です。

(f) **Termination of Use:** If a certificate is revoked for any reason, or when a certificate reaches its expiration date, you must promptly remove the certificate from all devices and systems on which it was installed and cease all use of the certificate and its associated private key. Using an expired or a revoked certificate (for any purpose) is strictly prohibited. Additionally, after a certificate has been revoked or has expired, you agree not to use the corresponding private key to issue new signatures or in any way that relies on the trust of the revoked/expired certificate. Once a certificate is no longer valid (either due to revocation or expiration), both the certificate and its key should be considered retired from service.
利用の停止： 証明書が理由の如何にかかわらず失効される場合、又は証明書がその満了日に達する場合、お客様は、速やかに証明書がインストールされたすべてのディバイス及びシステムから証明書を削除し、証明書及びその関係付けられた秘密鍵の利用をすべて停止しなければなりません。有効期間満了により終了した又は失効された証明書を（いかなる目的にも）使用することは厳に禁止されます。さらに、証明書が失効されたか又は有効期間満了により終了してしまったあとは、お客様は、新しい署名を発行するため又は失効された/有効期間満了により終了した証明書の信用に依拠するいかなる方法でも、対応する秘密鍵を利用し

ないことに合意します。証明書が（失効又は有効期間満了による終了のいずれかにより）もはや有効でなくなった時点で、証明書及びその鍵はいずれも役目を終えたとみなされなければなりません。

(g) **Responsiveness:** You will respond promptly to any inquiries or instructions from DigiCert regarding the certificate or its use. For example, if DigiCert contacts you to investigate a potential compromise, misuse, or any complaint regarding your certificate, you agree to reply and cooperate within the timeframe specified by DigiCert. Timely cooperation may be necessary to address security incidents or compliance issues and is a condition of your continued certificate use.
応答： お客様は、証明書又はその使途に関するデジサートからの照会又は指示に速やかに応答するものとします。例えば、デジサートがお客様の証明書に関する潜在的な危殆化、不正利用又はあらゆる訴えを調査するためにお客様に連絡する場合、お客様は、デジサートが明示する時間枠内に応答し、協力することに合意します。適時の協力が、セキュリティインシデント又はコンプライアンス上の問題に対処するために必要となることがあり、お客様の継続的な証明書の利用の条件です。

(h) **Acknowledgment of Revocation Rights:** You acknowledge and agree that DigiCert, as an X9-authorized Certification Authority, has the right to revoke your certificate in accordance with the X9 CP. In particular, your certificate may be revoked in the event of a private key compromise, material changes in the information contained in the certificate, or any other circumstance that renders the certificate unreliable or non-compliance with the X9 CP. DigiCert is authorized to perform such a revocation with immediate effect and without prior notice when necessary to protect the security of the PKI or to comply with applicable requirements. In the event of a revocation, DigiCert will provide you with a notice of the revocation and a brief explanation of the reason as soon as practicable thereafter, consistent with the X9 CP's procedures.
失効権の承認： お客様は、デジサートが、X9 認定認証局として、X9 CP に従ってお客様の証明書を失効させる権利を有することを承認し、これに合意します。とりわけ、秘密鍵の危殆化、証明書に記載された情報の重大な変更又はその他の証明書が信用を欠くこととなるか又は X9 CP に準拠しなくなる状況の場合には、お客様の証明書が失効されることがあります。デジサートは、PKI のセキュリティを保護し又は適用される要件を遵守する必要があるときは、事前通知なしに直ちに当該失効を実施する権限を有します。失効の場合には、デジサートは、X9 CP の手続きに従って、失効後、現実的に可能な範囲でなるべく速やかに、失効通知及び理由の概要をお客様に提供します。

8. Revocation (When and Why)
失効（時期及び理由）

Short version: *X9 certificates can be revoked by DigiCert upon Subscriber request or if a certificate poses a security risk. The revocation process follows the X9 CP and may differ from DigiCert's public Web PKI practices (e.g., timing and criteria for revocation).*
要約版： *X9 証明書は、サブスクライバーの要請により又は証明書がセキュリティ上のリスクを生じ*

る場合、デジサートにより失効され得るものとします。失効手続きは X9 CP に従い、デジサートの public Web PKI の運用方法（例えば、失効のタイミング及び基準）とは異なることがあります。

Under the X9 CP, DigiCert may revoke an X9 certificate for a variety of reasons, including:
X9 CP に基づき、デジサートは、次の各号に掲げるものを含む様々な理由で X9 証明書を失効させることができます：

(a) **Private Key Compromise or Suspected Compromise:** If the certificate's private key is known or believed to be compromised, DigiCert will revoke the certificate to protect the integrity of the PKI.
秘密鍵の危殆化又は疑われる危殆化： 証明書の秘密鍵が危殆化されていることが分かっているか又はそう思われる場合、デジサートは、PKI の完全性を保護するため証明書を失効させます。

(b) **Material Changes or Inaccurate Information:** If any information in the certificate becomes materially false or misleading. For example, if the Subscriber's organization name or control has changed such that the certified details are no longer detailed, the certificate will be revoked.
重大な変更又は不正確な情報： 証明書中のいずれか情報が重大な点において不正又は誤解を招くものとなった場合。例えば、サブスクライバーの組織名称又は支配が、証明書の細目がもう記述されていない程に変更されてしまった場合、証明書は失効されます。

(c) **Misuse or Policy Violation:** If a certificate is misused (used outside of the permitted X9 use cases or contrary to these Terms and the X9 CP) or if the Subscriber breaches their obligations, DigiCert may revoke the certificate. Any circumstance that renders the certificate non-compliant with the X9 CP or otherwise unreliable will result in revocation.
不正利用又はポリシー違反： 証明書が不正利用（認められた X9 ユースケース以外で又はこの規約及び X9 CP に反して利用）された場合、又はサブスクライバーがその義務に違反した場合、デジサートは、証明書を失効させることができます。証明書が X9 CP に準拠しなくなるか又はその他の原因で証明書が信用を欠くこととなる状況になると、失効されます。

(d) **Upon Subscriber's or Authorized Request:** DigiCert will revoke an X9 certificate upon request by the Subscriber (or an authorized organizational representative or RA) after verifying the authenticity of the request.
サブスクライバーの要請又は正当な権限ある要請による失効： デジサートは、サブスクライバー（又は正当な権限を有する組織の代表者若しくは RA）の要請により、要請の真正性を検証した後に X9 証明書を失効させます。

(e) **Security or Compliance Requirement:** DigiCert may revoke a certificate if required to comply with law, regulation, or at the direction of the X9 Policy Authority, or if continuing to trust the certificate could adversely affect the security of the X9 PKI environment.
セキュリティ又はコンプライアンス要件： 法令を遵守するために要求される場合、又は X9 ポリシー承認局の指示がある場合、又は継続して証明書を信頼することで X9 PKI 環境のセキ

ュリティに悪影響を及ぼすおそれがある場合、デジサートは 、証明書を失効させることができます。

In addition to revocation, DigiCert reserves the right to suspend certificates (i.e., temporary certificates), subject to and according to the requirements of the X9 CP, while investigating an issue. The suspended certificate may later be fully revoked or reinstated as appropriate.
失効に加え、デジサートは、問題を調査する間、X9 CP の要件に従って証明書を一時停止（すなわち、仮証明書）する権利を留保します。停止された証明書は、その後、完全失効又は復活の中いずれか適切な方法で対応されることがあります。

9. Miscellaneous.
雑則

Integration with Other Agreements: These Terms, together with the DigiCert X9 PKI CP and the DigiCert CPS, govern your use of X9 certificate services provided by DigiCert. They are incorporated into, and supplement, the DigiCert Master Services Agreement (available at https://www.digicert.com/master-services-agreement-jp) or other applicable service agreement between you and DigiCert. In the event of any conflict between these Terms and the X9 CP, the provisions of the CP will prevail. In the event of any conflict between these Terms and any other agreements, service contracts, or terms applicable to DigiCert offerings that you may have, these Terms will prevail with respect to matters specifically relating to your use of X9 certificates.
他の契約との統合： この規約は、DigiCert X9 PKI CP 及び DigiCert CPS とともに、デジサートの提供する X9 証明書サービスのお客様による利用に適用されます。この規約、DigiCert X9 PKI CP 及び DigiCert CPS は、デジサートマスターサービス契約書（https://www.digicert.com/master-services-agreement-jp で閲覧可能）又はお客様とデジサートとの間に適用される他のサービス契約書の一部を構成し、補足するものです。この規約と X9 CP との間に齟齬ある場合、当該 CP の条項が優先します。この規約とお客様が有することのあるデジサート提供サービスに適用される他の契約、サービス契約書又は条件との間に齟齬ある場合、特に X9 証明書のお客様による利用に関する事項については、この規約が優先します。

No Third-Party Beneficiaries: There are no third-party beneficiaries to these Terms.
第三者受益者の不存在： この規約について受益権を有する第三者は存在しません。

Modifications to Terms: DigiCert may update or modify these Terms from time to time to adapt to changes in services, technology, legal or regulatory requirements, or changes in the X9 PKI policies or industry standards. Updated versions of these Terms will be published on the DigiCert website (and/or through any in-product click-through, repository or communication channel) and will be indicated by an updated “Last Updated” date. DigiCert may also inform subscribers of significant changes through means such as email notifications or account alerts. By continuing to use X9 certificates or related services after these Terms have been updated, you signify your acceptance of the revised Terms. If you do not agree to the changes in the Terms, you should discontinue using the X9 certificates and related services (subject to any transitional provisions or grace periods that DigiCert may announce). It is your responsibility to review these Terms periodically for any updates. These Terms will remain in effect until all certificates issued under them have expired or been revoked and are no longer in use, or until

the Terms are replaced by a newer version.
規約の変更： デジサートは、サービス、技術若しくは法令上の要件の変更又は X9 PKI ポリシー若しくは業界規格の変更に対応するため、この規約を随時改定又は変更できます。この規約の改定版は、デジサートウエブサイト（及び/又は製品内のクリックスルー、リポジトリ又はコミュニケーションチャネルを通じて）で公表し、更新された”最終更新“日で表示します。デジサートは、また、電子メールによる通知又はアカウントアラート機能などの手段を通じて重大な変更をサブスクライバーに通知することがあります。この規約が改定された後も X9 証明書又は関連サービスを継続して利用する場合、お客様は、改定された規約に合意したものとみなされます。この規約の変更に同意しない場合、お客様は、（デジサートが発表する経過措置又は猶予期間を条件に）X9 証明書及び関連サービスの利用を中止しなければなりません。この規約の改定を定期的に確認することは、お客様の責任です。この規約は、この規約に基づき発行された証明書がすべて有効期間満了により終了するか又は失効され、もはや利用されなくなるまで、又はこの規約が新版により置き換えれるまで有効に存続します。

Plain Language Disclaimer: For convenience, some sections of these Terms include “Short version” summaries or simplified explanations to help illustrate the meaning of the section. These plain-language summaries are provided only to aid understanding and are not legally operative provisions. In case of any ambiguity or conflict between a summary and the full text of the Terms, the full, detailed text (and the incorporated X9 CP) will govern. The use of plain language in these Terms is intended to make them easier to understand, but it does not diminish the legal enforceability of the provisions. The binding obligations of both you and DigiCert are as stated in the full text of the Terms.
平易な文言に係る否認： 条項の趣意説明の一助とするため、便宜上、この規約のいくつかの条項は、要約版の要旨又は概説を含んでいます。これら平易な文言による概要は、理解に資するためにのみ提供するもので、法的拘束力を有する本文条項ではありません。この規約の概要と正式な本文との間に曖昧さ又は齟齬ある場合、詳細で正式な本文（及びその一部を構成する X9 CP）が優先します。この規約における平易な文言の使用は、理解をより容易にすることを目的とするもので、本文条項の法的強制執行可能性を損なうものではありません。お客様及びデジサート双方の拘束力ある義務は、この規約の正式な本文において定めます。

Controlling Language: The definitive version of these Terms is written in English. If these Terms are translated into another language and there is a conflict between the English version and the translated version, the English language version controls.
優先言語: この規約の正式版は英語で作成されています。この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。