DIGICERT E-MAIL PKI

CERTIFICATE TERMS OF USE
電子証明書利用規約

PUBLICLY TRUSTED S/MIME CERTIFICATES
公的に信頼される S/MINE 証明書

1. Scope and Purpose
適用範囲及び目的

Short version: *These Terms apply only to DigiCert's publicly trusted S/MIME certificates. They incorporate DigiCert's Certificate Policy and Certification Practice Statement (CP/CPS) and reflect industry standards (like the CA/Browser Forum S/MIME Baseline Requirements and root store policies such as Mozilla's) that apply to publicly trusted S/MIME certificates.*
要約版： *本規約は、デジサートの公的に信頼される S/MIME 証明書にのみ適用します。本規約は、デジサートの Certificate Policy 及び Certification Practices Statement (CP/CPS) の一部を構成し、公的に信頼される S/MIME 証明書に適用される業界規格（CA/Browser Forum S/MIME Baseline Requirements 及び Mozilla などのルートストアポリシー）を反映しています。*

These terms ("**Terms**") apply to publicly trusted S/MIME certificates issued by DigiCert or its affiliates. They do not apply to TLS/SSL (browser-trusted) certificates, private/internal S/MIME, code signing, document signing, or EU qualified certificates. The Terms incorporate the DigiCert Public Trust CP/CPS (the "**CP/CPS**"), available at https://www.digicert.com/legal-repository/, which together with Terms sets forth how S/MIME certificates are issued, managed, and revoked. These Terms reflect the policies and requirements established by the CA/Browser Forum S/MIME Baseline Requirements available at www.cabforum.org/working-groups/smime/documents/ ("Baseline Requirements") and applicable root store policies (e.g., Mozilla, Microsoft, Apple). **As a Certification Authority ("CA"), DigiCert is obligated to abide by these industry standards, including promptly revoking certificates when required, without exception.**
この規約（以下「**本規約**」といいます）は、デジサート又はその関係会社により発行される公的に信頼される S/MIME 証明書に適用します。本規約は、TLS/SSL (browser-trusted) 証明書、プライベート/内部証明書、コードサイニング証明書、ドキュメントサイニング証明書又は EU 適格証明書には適用しません。本規約は、本規約とともに S/MIME 証明書の発行、管理及び失効の方法を定める、https://www.digicert.com/legal-repository/ で閲覧可能な DigiCert Public Trust CP/CPS （以下「**CP/CPS**」といいます）の一部を構成します。本規約は、www.cabforum.org/working-groups/smime/documents/ で閲覧可能な、the CA/Browser Forum S/MIME Baseline Requirements（以下「**Baseline Requirements**」といいます）及び適用されるルートストアポリシー（例えば Mozilla、Microsoft、Apple）により確立されたポリシー並びに要件を反映しています。**認証局（以下「CA」といいます）として、デジサートは、必要なときは速やかに証明書を失効させることを含め、例外なく、同業界規格を遵守する義務を負っています。**

2. Use of S/MIME Certificates
S/MIME 証明書の利用

You may only use DigiCert S/MIME certificates to secure email in connection to signing, encryption, and related client authentication. You may not use them for TLS/SSL web servers, code signing, document signing, or other unrelated purposes.
お客様は、署名、暗号化及びクライアント認証との関連で電子メールを保護するためにのみデジサート S/MIME 証明書を利用することができます。お客様は、TLS/SSL、Web サーバー、コードサイニング、ドキュメントサイニング又はその他の無関係な目的にデジサート S/MIME 証明書を利用することはできません。

Permitted uses:
許諾される利用方法：

- Signing email to authenticate the sender and message integrity
  送信者及びメッセージの整合性を認証するために電子メールに署名すること
- Encrypting email to provide confidentiality
  秘密性を提供するために電子メールを暗号化すること
- Client authentication, if consistent with the certificate's extensions and policies
  クライアント認証（証明書の拡張子及びポリシーと一致する場合）

Prohibited uses:
禁止される利用方法：

- TLS/SSL (web server authentication)
  TLS/SSL（Web サーバ認証）
- Code signing or document signing (unless specifically designated)
  コードサイニング又はドキュメントサイニング（特に指定のない限り）
- Any use outside the intended scope
  意図された範囲外のあらゆる利用

Using a DigiCert S/MIME certificate for a prohibited purpose is grounds for revocation (see **Revocation** section below).
禁止される目的でデジサート S/MIME 証明書を利用することは、失効の根拠となります（**失効**条項を参照）。

3. Requesting a Certificate
証明書の要求

Short version: *When you request an S/MIME certificate, you promise that the info is true and that you're authorized to request it for the email address/domain and (if applicable) organization.*
要約版： *お客様が S/MIME 証明書を要求するとき、お客様は、情報が真実であること並びに電子メールアドレス／ドメイン及び（該当する場合）組織に係る S/MIME 証明書を要求する正当な権限を有していることを保証します。*

When requesting a certificate, you must submit **accurate, complete, and truthful information**. This includes the email address, organization details, and any other data required for issuance.
証明書を要求するとき、お客様は、**正確、完全かつ真実の情報**を提出しなければなりません。例として、電子メールアドレス、組織詳細情報及びその他の発行に必要なデータが挙げれます。

By requesting a certificate, you represent and warrant that: **(a)** you have lawful rights or authority to use and control the domain names (and any organization name or personal names, if applicable) listed in the certificate request, and **(b)** your certificate request and intended use **will not infringe** upon the intellectual property or legal rights of any third party. Misuse of the enrollment process or providing any false, misleading, or unauthorized information is a material breach of these Terms. DigiCert will deny any certificate request that violates these rules, and **any certificate issued on the basis of false or misleading information may be revoked immediately.**
証明書を要求することにより、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、証明書要求書に記載されたドメイン名（及び、該当する場合、組織名又は個人名）を利用し及び管理する正当な権利又は権限を有すること、及び（b）お客様の証明書要求及び意図された用途が、いかなる第三者の知的財産権又は法的権利も侵害するものでないこと。申込手続きの不正利用又は虚偽、誤解を招く若しくは無許諾の情報を提供することは、本規約の重大な違反となります。デジサートは、本規約に違反するいかなる証明書要求も拒否するものとし、**虚偽又は誤解を招く情報に基づき発行されたあらゆる証明書を直ちに失効させることができるものとします**。

4. Verification Before Issuance
発行前検証

Short version: *DigiCert will verify control of the email address (or domain), and for certain certificate types will also verify the individual or organization.*
要約版： *デジサートは、電子メールアドレス（又はドメイン名）のお客様の管理を検証し、特定の種類の証明書については、個人又は組織についても検証するものとします。*

Before issuing any publicly trusted S/MIME certificate, DigiCert will perform the required validation steps in accordance with the CP/CPS and the Baseline Requirements. These include:
公的に信頼される S/MIME 証明書を発行する前に、デジサートは、CP/CPS 及び the Baseline Requirements に従って必要な認証手順を実施するものとします。この手順の例としては、次のものが挙げられます。

- **Mailbox-validated (MV):** DigiCert verifies control of the email address to be included in the certificate. This may involve sending a verification email challenge, requiring a DNS record for the domain, or other approved mailbox control methods. DigiCert also checks DNS CAA records for any “issuemail” property that permits or forbids issuance.
  メールボックス認証（MV）： デジサートは、証明書の中に記載される電子メールアドレスの管理を検証します。この検証の例としては、検証用電子メールチャレンジの送信、ドメインの DNS レコードの要求又はその他の承認されるメールボックス管理検証手法が挙げられます。また、デジサートは、発行を許可し又は禁止する“発行メール”プロパティの DNS CAA レコードを確認します。

- **Organization-validated (OV):** In addition to email control, DigiCert verifies the organization's legal existence, operational status, and authority to use the email domain. This may include checking official registry records, performing address and phone verification, and cross-checking third-party sources.
  組織認証（OV）： 電子メール管理に加え、デジサートは、組織の法的実在、運営状況及び電子メールドメインの利用権限を検証します。この例としては、公的な登記記録の確認、所在地及び電話検証の実施及び第三者の情報との照合が挙げられます。

- **Sponsor-validated (SV):** DigiCert validates the email address and confirms that the organization has sponsored the individual certificate holder. The sponsor organization must be verified and must designate the applicant.
  スポンサー認証（SV）： デジサートは、電子メールアドレスを認証し、組織が個人の証明書保有者のスポンサーとなっていることを確認します。スポンサー組織は検証を受けたうえで、申請者を指名しなければなりません。

- **Individual-validated (IV):** DigiCert verifies the natural person's identity, typically through a government-issued photo ID, notarization, or equivalent method, and verifies control of the email address.
  個人認証（IV）： デジサートは、通常、政府発行の写真付き身分証明書、公証又は同等の方法により自然人の身元を検証し、電子メールアドレスの管理を検証します。

If DigiCert cannot complete validation to its satisfaction, it will not issue the certificate. DigiCert may also decline issuance if there is a risk of fraud or non-compliance with industry standards or its processes.
デジサートがその満足のいくように認証を完了できない場合、デジサートは証明書を発行しないものとします。また、デジサートは、詐欺又は業界規格若しくはその手続きの不遵守のおそれがある場合、発行を拒否できるものとします。

5. Registration Authority ("RA") Representations, Warranties, and Indemnity
登録局（"RA"）の表明、保証及び補償

If your organization acts as an RA, you represent and warrant that:
お客様の組織が 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 CP/CPS, Baseline Requirements and these Terms;
お客様は、CP/CPS 、Baseline Requirements 及び本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 CP/CPS and Baseline Requirements.

お客様は、正確な記録を保持し、CP/CPS 及び Baseline Requirements 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 and its affiliates and their respective directors, officers, agents, employees, successors and assigns 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 CP/CPS, Baseline Requirements and these Terms, (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 としての作為若しく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、デジサート及びその関係会社並びにそのそれぞれの取締役、役員、代理人、従業員、承継人及び譲受人を補償、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) CP/CPS、Baseline Requirements 及び本規約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: *Certificates have limited lifespans. The maximum allowed is 825 days (about 27 months). You must replace them before they expire.*
要約版： *証明書の有効期間は短くなっています。許容される最長期間は 825 日（約 27 か月）です。お客様は、証明書が有効期間満了により終了する前に証明書を入れ替えなければなりません。*

Publicly trusted S/MIME certificates expire after a limited time. As of now, the **maximum validity** permitted under the Baseline Requirements is 825 days. Industry practices may evolve to require short lifecycles in the future. DigiCert may offer subscription terms for convenience, but certificates will still be reissued at industry-mandated intervals.
公的に信頼される S/MIME 証明書は一定期間後に有効期間満了により終了します。現時点では、the Baseline Requirements に基づき許容される**最長有効期間**は 825 日です。業界の慣行は、将来短期の有効期間を要求する方向へ向かっています。デジサートは利便性の高いサブスクリプション条件を提供できますが、それでもやはり証明書は業界によって義務付けられた周期で再発行されるものとします。

It is your responsibility to monitor the expiration date of each certificate and to obtain and install a replacement certificate before it expires. If a certificate expires, any systems relying on it will show errors or fail to connect securely. Expired certificates must not be used. Continuing to use an expired certificate is unsafe and violates these Terms. You should plan to remove or replace certificates promptly upon expiration.
各証明書の有効期間満了日を監視し、証明書が有効期間満了により終了する前に代替証明書を取得しインストールすることは、お客様の責任です。証明書が有効期間満了により終了した場合、証明書に依拠するあらゆるシステムはエラーを表示するか又は安全な方法で接続することはできません。有効期間切れの証明書は利用してはいけません。有効期間切れの証明書を継続して利用することは危険

で、本規約に違反します。お客様は、有効期間満了時の証明書の除去又は入替を予定しておかなければいけません。

DigiCert strongly recommends using automation (such as CertCentral® APIs, Trust Lifecycle Manager, or other automated tools) to handle renewals and replacements.
デジサートは、更新及び入替を処理するため、自動化（例えば、CertCentral® API、Trust Lifecycle Manager 又はその他の自動化ツール）を利用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: *By using or applying for a DigiCert S/MIME certificate, you promise to uphold certain obligations. In summary, you must* ***(a)*** *provide accurate information,* ***(b)*** *protect your private key,* ***(c)*** *review and accept the certificate's contents,* ***(d)*** *use the certificate only as allowed (for the validated email address and in compliance with law and policy),* ***(e)*** *promptly request revocation and cease use if the private key is compromised or if any certificate information becomes inaccurate,* ***(f)*** *stop using the certificate (and its key) upon expiration or revocation (except that you may retain the key solely to decrypt previously received mail where permitted),* ***(g)*** *respond promptly to DigiCert's inquiries about security issues, and* ***(h)*** *acknowledge and agree to DigiCert's right to revoke the certificate when needed. These obligations are derived from industry standards that all subscribers must follow.*
要約版： *デジサート S/MIME 証明書を利用するか又は申し込むことにより、お客様は、ある特定の義務を守ることを約します。要約すれば、お客様は、****(a)*** *正確な情報を提供し、****(b)*** *お客様の秘密鍵を保護し、****(c)*** *証明書の内容を審査、承認し、****(d)*** *認められているとおりのみ証明書を利用し（認証された電子メールアドレスについて、かつ、法律及びポリシーに従って）、****(e)*** *秘密鍵が危殆化した場合又はいずれか証明書情報が不正確となった場合、直ちに失効を要求、利用を中止し、****(f)*** *有効期間の満了又は失効をもって、証明書（及びその鍵）の利用を中止し（以前受信したメールを復号化するためにのみお客様が鍵を維持できることを除き）、****(g)*** *セキュリティ問題に関するデジサートによる照会に対して直ちに応答し、及び****(h)*** *必要に応じ証明書を失効させるデジサートの権利を承認し、これに合意しなければなりません。これらの義務は、すべてのサブスクライバーが従わなければならない業界規格に由来します。*

As the Subscriber (certificate holder), you have important obligations to ensure your S/MIME certificate is used securely and in accordance with these Terms, the CP/CPS, and applicable standards. **You hereby represent and warrant to DigiCert and to the Certificate Beneficiaries that you will do the following:**
サブスクライバー（証明書保有者）として、お客様は、お客様の S/MIME 証明書が安全な方法で、かつ、本規約、CP/CPS 及び適用される規格に従って利用されることを確保する重要な義務を負っています。**お客様は、ここに、デジサート及び証明書受益者に対し、次の各号に掲げる事項を行うことを表明し、これを保証します。**

a. Accuracy of Information. You will provide accurate and complete information at all times in your certificate request and in all communications with DigiCert related to your S/MIME certificates. You will promptly update any information if it changes during validation. If any information you provided becomes outdated or incorrect (for instance, if your legal name,

organization name or address changes, or you cease to control or lawfully use an email address included in the certificate), you will promptly update the information with DigiCert or notify DigiCert of the change.

情報の正確性. お客様は、お客様の証明書要求において並びにお客様の S/MIME 証明書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ものとします。お客様は、認証手続き中にいずれか情報が変更された場合、直ちに情報を更新するものとします。お客様がデジサートに対し提供したいずれか情報が最新でなくなったかまたは不正確になった場合（例えば、お客様の氏名、お客様の組織の名前又は住所が変わるか、またはお客様が証明書に記載された電子メールアドレスの管理又は適法な利用を中止した場合）、お客様は、直ちにデジサートに登録されている情報を更新するか、変更をデジサートに通知するものとします。

b. Protection of Private Key. You will securely generate your certificate's private key using trustworthy systems and strong cryptographic standards (**at least a 2048-bit RSA key or equivalent-strength ECC permitted by the Baseline Requirements**). You must keep the private key confidential and under your sole control at all times, using measures sufficient to prevent loss, disclosure, or unauthorized use (e.g., strong passphrases, secure keystores or tokens, appropriate device and account controls). You are responsible for retaining access to private keys used for **email decryption** so you can read previously received encrypted messages; where permitted by policy and law, maintaining a secure backup/escrow for decryption keys is recommended. (Do not share your private key with third parties except as allowed by the CPS, such as through an approved enterprise key management mechanism.)

秘密鍵の保護. お客様は、信頼できるシステム及び強度の暗号化規格（**少なくとも the Baseline Requirements により許容される 2048-bit RSA 鍵又は等価強度の楕円曲線暗号**）を利用して安全な方法でお客様の秘密鍵を生成するものとします。お客様は、喪失、漏洩又は不正利用を防止するために十分な対策を講じて、秘密鍵を秘密に保持し、常にお客様の単独の管理下に置かなければなりません。お客様は、以前受信した暗号化メッセージを読むことができるようメールの復号化に利用する秘密鍵へのアクセスを維持することについて責任を負います；ポリシー及び法律により許容される場合、復号化鍵のための安全なバックアップ／エスクローを保持することが推奨されます。（例えば承認されたエンタープライズ鍵管理装置など CPS により認められる場合を除き、お客様の秘密鍵を第三者と共有しないでください。）

c. Acceptance of Certificate. After DigiCert issues your certificate, you will review the certificate's details (such as the subject name, rfc822Name email address(es), and any organization info) to ensure all information is correct. You will only use the certificate if you have verified that the data in it is accurate and you accept it. Using the certificate signifies your acceptance of it. If you find any inaccuracies, you must contact DigiCert to revoke or reissue the certificate before using it.

証明書の検収. デジサートがお客様の証明書を発行した後、お客様は、すべての情報が正確であることを確認するため、証明書の細目（例えば、サブジェクト名、rfc822 名、電子メールアドレス、組織情報など）を審査するものとします。お客様が証明書中のデータが正確であることを検証し終わり、お客様が証明書を検収した後にのみ、お客様は証明書を利用するものとします。証明書を利用した場合、お客様は証明書を検収したものとみなされます。お客様が不正確な情報を発見した場合、お客様は、証明書の失効又は再発行について、証明書を使用する前にデジサートへ連絡してください。

d. Use of Certificate. You will install and use the certificate only on your own email clients, devices, and systems (or those you are authorized to operate) that send and/or receive mail for the validated email address(es) listed in the certificate. You agree to use the certificate solely in compliance with these Terms (including the CP/CPS). The certificate must **not** be used for any purpose other than its intended scope (i.e., **email signing and encryption** and related client authentication) and must **not** be used for server TLS/SSL, code signing, document signing (unless explicitly profiled), or any other out-of-scope use.

証明書の利用. お客様は、証明書に記載された認証済み電子メールアドレスにメールを送信及び／又は受信する自己の電子メールクライアント、デバイス及びシステム（又はお客様が運用権限を有するもの）にのみ、証明書をインストールし、利用するものとします。お客様は、本規約（CP/CPS を含む）に従ってのみ証明書を利用することに同意します。証明書はお客様が運用権限を有さないいかなるシステムにも利用してはならず、お客様は証明書の意図された範囲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（上記 Web PKI 証明書の利用条項を参照）。証明書はその意図された範囲以外のいかなる目的（すなわち、**電子メールへの署名及び暗号化**並びに関連クライアント認証）について利用してはならず、サーバーの TLS/SSL、コードサイニング、ドキュメントサイニング（明確にプロフィール化されていない限り）又はその他の範囲外利用についても利用してはなりません。

e. Reporting and Revocation. If you suspect or become aware of any actual or potential compromise of the certificate's private key, or any misuse of the certificate (including phishing, fraud, or other unlawful use), you must **immediately** notify DigiCert and promptly request revocation of the certificate. Similarly, if any information in the certificate is or becomes false, inaccurate, or misleading at any time (for example, an email address is reassigned/retired or organization details change), then you must immediately cease using the certificate and promptly request DigiCert to revoke it.

報告及び失効. お客様が証明書の秘密鍵の現実若しくは潜在的な危殆化又は証明書の不正利用の疑念があるか又は知った場合、お客様は直ちにデジサートに通知し、速やかに証明書の失効を要求しなければなりません。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、そのときは、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。

f. Termination of Use. If a certificate is revoked for any reason, or if it reaches its expiration date, you must promptly remove the certificate from all systems and **cease all use** of the certificate and of that private key for signing or presenting trust to relying parties. Using an **expired or revoked** certificate for any purpose that asserts ongoing trust is strictly prohibited. *For the avoidance of doubt:* retaining the private key **solely to decrypt previously received email** (or for lawful archival/records obligations) is permitted where allowed by policy and law; you must not use the key to continue signing email or to otherwise circumvent revocation or expiry.

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、又は証明書がその有効期間満了日に達する場合、お客様は、速やかにすべてのシステムから証明書を削除し、証明書及び署名又は依拠当事者に信頼を提供するための秘密鍵の**利用をすべて停止**しなければなりません。**有効期間切れの又は失効した**証明書を継続的な信頼を条件とするいかなる目的にも使用することは厳に禁止されます。*疑義を避けるために付言すると*、ポリシー及び法律により認められる場合、**以前受信したメールを復**

号化するためにのみ（又は正当な保存／記録義務のため）秘密鍵を維持することが許容されます；お客様は、電子メールに署名することを継続するため又はその他の方法で失効又は有効期間満了による終了を回避するために鍵を利用してはなりません。

g. Responsiveness. You will respond promptly to inquiries or instructions from DigiCert regarding your certificate or its related key. Timely cooperation may be critical to mitigate security threats or to comply with industry **revocation** requirements. Failure to respond to DigiCert's security inquiries or directions in a timely manner constitutes a breach of these Terms and may result in certificate revocation.

応答. お客様は、お客様の証明書若しくはその関連する鍵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。適時の協力は、セキュリティ上の脅威を軽減し、又は業界失効要件を遵守するためにきわめて重要となることがあります。デジサートのセキュリティ上の照会又は指示に適時に応答しない場合、本規約の違反となり、証明書の失効となることがあります。

h. Acknowledgment of Revocation Rights. You acknowledge and accept that DigiCert, as a Certification Authority, has the right to revoke your certificate at any time, without prior notice if you violate these Terms, or if revocation is required to comply with DigiCert's CP/CPS, applicable law, or industry standards. You agree that you will not object to or impede such revocation, and you waive any right to seek damages or remedies against DigiCert for a revocation conducted in accordance with these Terms. ***Industry standards require CAs to revoke certificates on short notice (for example, within 24 hours for certain critical incidents and within 5 days for other enumerated events). You acknowledge that DigiCert must adhere to these non-negotiable timelines and agree to act accordingly in such events.***

失効権の承認. お客様は、デジサートが、認証局として、お客様が本規約に違反した場合、又はデジサートの CP/CPS、適用法又は業界規格を遵守するために失効が必要な場合、事前通知なくお客様の証明書をいつでも失効させる権利を有することを承認し、これを承諾します。お客様は、当該失効に異議を唱え又は妨げず、本規約に従って実施される失効に対する損害賠償又は救済措置をデジサートに対し求めるあらゆる権利を放棄することに合意します。***認証局は、業界規格に従い直前に証明書を失効させなければならないことがあります（例を挙げると、ある特定の致命的なインシデントについては 24 時間以内、及びその他のイベントについては 5 日以内）。お客様は、デジサートがこの交渉の余地のない期間を遵守しなければならないことを承認し、当該イベントにおいてはそれに応じ行動することに合意します。***

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

Short version: *Some events require a certificate to be revoked before it normally expires. DigiCert must act fast to protect security and comply with industry standards. You are required to help and must not impede revocation.*

要約版： *一部のイベントでは、証明書が有効期間満了により終了する前に、証明書を失効させる必要があります。デジサートは、セキュリティを保護し、業界規格を遵守するために素早く行動しなければなりません。お客様には支援する義務があり、失効を妨げてはなりません。*

In some cases, you must request revocation (for example, if your private key is compromised or you no longer control an e-mail address). In other cases, DigiCert must revoke a certificate even

without your request, often on a short timeline. These revocation obligations are non-negotiable and required by industry standards, including the Baseline Requirements and applicable root store policies (e.g., Mozilla Policy). The following timelines apply.
一部の場合、お客様は、失効を要求しなければなりません（例を挙げると、秘密鍵が危殆化された場合又はお客様が電子メールアドレスを管理しなくなった場合）。その他の場合、デジサートは、お客様の要求がなくとも、多くの場合、短期間で証明書を失効させなければなりません。この失効義務は交渉の余地はなく、the Baseline Requirements 及び適用されるルートストアポリシー（例えば、Mozilla Policy）を含む業界規格により要求されるものです。次に掲げる期間が適用されます。

Revocation within 24 hours (required)
24 時間以内の失効（必須）

DigiCert will revoke certificates within 24 hours if any of the following occur:
デジサートは、下記のいずれか事由が生じた場合 24 時間以内に証明書を失効させるものとします：

a. You request in writing that DigiCert revoke the certificate.
お客様が、デジサートが証明書を失効することを書面で要求した場合。
b. You notify DigiCert that the original certificate request was unauthorized.
お客様が、当初の証明書要求が承認されたものではないことをデジサートに通知した場合。
c. DigiCert obtains evidence that your private key has been compromised.
デジサートが、お客様の秘密鍵が危殆化されている証拠を入手した場合。
d. DigiCert is made aware of a demonstrated or proven method that can easily compute your private key based on the public key in the certificate.
デジサートが、証明書に記載された公開鍵によりお客様の秘密鍵を容易に計算できる実証又は証明された方法を知った場合。
e. DigiCert obtains evidence that the validation of domain authorization or control for any subject identity information in the certificate should not be relied upon.
デジサートが、証明書に記載された主体者識別情報に係るドメイン権限又は管理の認証が依拠すべきではない証拠を入手した場合。

Revocation within 5 days (required)
5 日以内の失効（必須）

DigiCert will revoke certificates within 5 days if any of the following occur:
デジサートは、下記のいずれか事由が生じた場合 5 日以内に証明書を失効させるものとします：

a. The certificate no longer complies with required technical standards (for example, its cryptographic or key size is no longer allowed under the Baseline Requirements or applicable root store policy).
証明書が、要求される技術規格に準拠しなくなった場合（例を挙げると、その暗号方式又は鍵長が the Baseline Requirements 又は適用されるルートストアポリシーにより許容されなくなった場合）。
b. DigiCert obtains evidence that the certificate was misused.
デジサートが、証明書が不正利用された証拠を入手した場合。

c. DigiCert is made aware that you have breached a material obligation of these Terms.
デジサートが、お客様が本規約の重大な義務に違反していることを知った場合。

d. DigiCert obtains evidence that the validation of control for any email address or domain part in the certificate should not be relied upon.
デジサートが、証明書中のいずれかの電子メールアドレス又はドメイン部分に係る管理の認証が依拠すべきではない証拠を入手した場合。

e. DigiCert is made aware of a material change in the information originally contained in the certificate.
デジサートが、証明書に当初記載されていた情報の重大な変更を知った場合。

f. DigiCert is made aware that the certificate was not issued in full compliance with the Baseline Requirements or the CP/CPS.
デジサートが、証明書が Baseline Requirements 又は CP/CPS に完全に準拠することなく発行されたことを知った場合。

g. DigiCert determines that the information appearing in the certificate is inaccurate.
デジサートが、証明書に記載された情報が不正確だと判断する場合。

h. DigiCert's right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OCSP repository.
the Baseline Requirements に基づき証明書を発行するデジサートの権利が有効期間満了により終了するか又は取り消された場合。ただし、デジサートが CRL/OCSP リポジトリを引き続き維持できるよう手続きを行っている場合は、この限りではありません。

i. Revocation is required by DigiCert's CP/CPS for a reason not covered above.
上記に該当しない事由でデジサートの CP/CPS により失効が要求される場合。

j. DigiCert is made aware of a demonstrated or proven method that exposes your private key to compromise or if there is clear evidence that the specific method used to generate the private key was flawed.
デジサートがお客様の秘密鍵を危殆化にさらす実証又は証明された方法を知った場合又は秘密鍵を生成するために利用された特定の方法に欠陥があった明白な証拠がある場合。

If DigiCert determines that revocation is required for any of the above reasons, it will proceed to revoke the certificate as soon as practicable. Certain high-severity threats require short-notice revocation. DigiCert adheres to the industry rule that it SHALL revoke within 24 hours for critical events, and SHALL revoke within 5 days for other enumerated events. In line with its CP/CPS and industry requirements, DigiCert will investigate problem reports promptly and **will not delay revocation** beyond the permitted timeline. If your certificate will be revoked or is revoked, DigiCert will usually send a notice to the contact email on record, with a brief explanation of the reason, as soon as reasonably possible. Once a certificate is revoked, it will be published as revoked in DigiCert's revocation repositories (CRL and/or OCSP), and it must be replaced with a new certificate if service is to continue. You agree that DigiCert has the authority to revoke, and you accept the consequences of such revocation. DigiCert is not liable for any losses or damages you incur due to a revocation that is mandated by these Terms, the CP/CPS, or industry standards.
デジサートが上記事由のいずれかで失効が必要と判断した場合、デジサートは可及的速やかに証明書の失効を進めるものとします。重大度の高い特定の脅威には緊急失効が要求されます。デジサートは、致命的なイベントについては 24 時間以内、その他の列挙されたエベントについては 5 日以内に失効

させなければならない業界規則に従います。自己の CP/CPS 及び業界要件に従って、デジサートは報告された問題を速やかに調査し、許容される期間を超えて**失効を遅滞しない**ものとします。お客様の証明書が失効される場合、通常、デジサートは、合理的に可能な範囲内でできる限り速やかに、理由の概要とともに記録された連絡先電子メールに通知を送るものとします。証明書が失効すると、デジサートの失効リポジトリ（CRL 及び/又は OCSP）で公表されるものとし、サービスの継続が予定される場合、新しい証明書で置き換えなければならないものとします。お客様はデジサートが失効権限を有することに合意し、当該失効の結果を了承します。デジサートは、本規約、CP/CPS 又は業界規格により強制される失効を原因としてお客様が被るいかなる損失又は損害についても責任を負いません。

9. Public Disclosure
公表

DigiCert may maintain its own repositories and status services where certificate information and revocation status are available (e.g., OCSP responders, CRLs, and certificate status websites), as permitted by its CPS and the Baseline Requirements. These are public-facing by design. By using the certificate, you acknowledge that its status (valid/revoked/expired) may be disclosed publicly through such mechanisms.
デジサートは、その CPS 及び the Baseline Requirements の認めるところに従い、証明書情報及び失効状況が参照できる自己のリポジトリ及びステイタスサービス（例えば、OCSP レスポンダー、CRL 及び証明書ステイタス Web サイト）を維持できるものとします。そもそも、これらは公表されるものです。証明書を利用することにより、お客様は、同証明書の状態（有効/失効/有効期間切れ）が当該仕組みを通じて公表される可能性があることを承認します。

10. Unsupported Practices (Use at Your Own Risk)
サポートされていない利用方法（お客様自身のリスクでの利用）

*Short version: Some practices related to certificate usage are **strongly discouraged and not supported** by DigiCert. If you engage in these practices, you do so at your own risk, and DigiCert may not be able to support you or may not accommodate special requests arising from these choices. In particular, avoid hard-coding (pinning) certificates or keys in applications, and avoid trying to use one certificate for multiple incompatible purposes. Such practices can lead to service disruptions or non-compliance.*
***要約版：** デジサートは、証明書の利用に関する一部の利用方法を**強く推奨せず、サポートしておりません**。お客様がこれらの利用方法に関与する場合、お客様はお客様自身のリスクにおいてこれを行うものとし、デジサートはお客様をサポートできない可能性があり、またはこれらの選択から生じる特別依頼に対応できない可能性もあります。特に、証明書又は鍵をアプリケーションにハードコーディング（ピニング）すること、及び 1 つの証明書を複数の一貫性のない目的に利用しようとすることはお止めください。当該利用方法は、サービスの停止又は違反につながる可能性があります。*

Certain practices are **strongly discouraged or unsupported** when using DigiCert certificates. Engaging in these practices is at **your own risk**, and DigiCert's obligations to support or accommodate you may be limited if you do so:
デジサート証明書の利用にあたり、特定の利用方法は**強く推奨されず又はサポートされていません**。

これらの利用方法に関与することは**お客様自身のリスク**であり、その場合、お客様をサポートし又は対応するデジサートの義務は限定的となる可能性があります。

- **Certificate/Key Pinning:** DigiCert does not support **hard-coding or "pinning"** of DigiCert certificates or public keys in applications, firmware, or devices. Pinning means your app or system is configured to trust only a specific certificate. Pinning a certificate can create rigidity. This can lead to outages or security risks (if you can't quickly replace the pinned certificate). If you choose to implement pinning with a DigiCert certificate, you assume full responsibility for any service disruptions that result. **DigiCert will not delay required actions** (including revocation) to accommodate a pinned environment.
  証明書/鍵ピニング： デジサートは、デジサート証明書若しくはアプリケーション、ファームウェア又はデバイスの中の公開鍵の**ハードコーディング又は"ピニング"**をサポートしません。ピニングとは、お客様のアプリケーション又はシステムが特定の 1 つの証明書のみを信頼するように設定することをいいます。ピニングは固定化を生じさることがあります。これは、（お客様がピニングされた証明書を迅速に差し替えることができない場合）サービスの中断又はセキュリティリスクにつながることがあります。お客様がデジサート証明書でピニングを実施することとした場合、お客様は、その結果引き起こされるあらゆるサービスの停止に全責任を負います。**デジサートは**、（失効を含む）ピニングされた環境に対処するために**必要な措置を遅滞しないものとします**。

- **Dual Use / Misuse of Certificates:** Do not rely on a single DigiCert certificate for multiple different usage scenarios that it was not designed for. For example, using one certificate for both S/MIME email encryption *and another purpose like* TLS/SSL (web security) *and* code signing, or client authentication is not supported. Each certificate is intended for a specific use case, as indicated by its type and extensions. Using certificates in unintended ways (even if technically possible) is **not recommended** and may result in security vulnerabilities or non-compliance with guidelines. If you use a certificate in an **unapproved manner**, you do so at your own risk. DigiCert is not responsible for any consequences of such use.
  証明書の重複利用／不正利用： 複数の異なる用途について、それらの用途に合わせて作成されていない単一のデジサート証明書に依拠しないでください。例を挙げると、S/MIME 電子メール暗号化並びに、 TLS/SSL（Web セキュリティ）及びコードサイニング又はクライアント認証などの別の目的の両方について 1 つの証明書を利用することはサポートされていません。各証明書は、その種類及び拡張子により指定される 1 つの特定のユースケースを想定して作成されています。想定されていない方法で証明書を利用することは**推奨されておらず**、セキュリティ上の脆弱性又はガイドラインの違反という結果を招くおそれがあります。お客様が**承認されていない方法**で証明書を利用する場合、お客様はお客様自身のリスクにおいてこれを行います。デジサートは、当該利用のいかなる結果についても責任を負いません。

- **Irretrievable Embedding:** Avoid embedding certificates in a context where they cannot be readily replaced or revoked. For instance, burning a certificate into hardware firmware or widely distributed in a way that cannot be updated is risky. If that certificate expires or must be revoked, those devices may fail and there may be no way to fix it in the field.
  回復不能な組込み： 証明書を容易に差し替え又は失効させることができない環境への証明書

の焼付けはお止めください。例を挙げると、ハードウェアファームウェアへの証明書の焼き付け又はアップデートできない方法での広範囲に及び頒布は危険です。同証明書が期間満了により終了するか又は失効されなければならない場合、これらのデバイスが動作しない可能性及び同問題を解決するこの分野における解決方法が存在しない可能性があります。

You should only use DigiCert certificates in adherence to DigiCert's guidelines, the CP/CPS, and industry best practices. Any use of a certificate that makes it difficult for you or DigiCert to revoke or replace the certificate (such as deeply embedded certificates in hardware, or widespread pinning without backup plans) is done at your own risk. Always have a plan for rapid certificate replacement.
お客様は、デジサートのガイドライン、CP/CPS 及び業界ベストプラクティスに従ってのみデジサート証明書を利用しなければなりません。お客様又はデジサートが証明書を失効させ又は差し替えることを困難にする証明書のあらゆる利用（ハードウェアに深く組み込まれた証明書又はバックアッププランのない広範囲に及ぶピニングなど）について、お客様はお客様自身のリスクにおいてこれを行います。常に迅速な証明書差替え計画を用意ください。

11. Miscellaneous
雑則

Integration with Other Agreements: These Terms, together with the CP/CPS, govern your use of S/MIME certificates 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 CP/CPS, the provisions of the CP/CPS will prevail. In the event of any conflict between these Terms and any other agreements, service contracts, or terms applicable to DigiCert offerings, these Terms will prevail with respect to matters specifically relating to your use of DigiCert S/MIME certificates.
他の契約との統合： 本規約は、CP/CPS とともに、デジサートの提供する S/MIME 証明書のお客様による利用に適用されます。本規約及び CP/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。本規約と CP/CPS との間に齟齬ある場合、CP/CPS の条項が優先します。本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、特にデジサート S/MIME 証明書のお客様による利用に関する事項については、本規約が優先します。

Relying Party Warranty and Third-Party Beneficiaries: Relying Parties and Application Software Vendors (as defined in the CP/CPS, and each, a "**Certificate Beneficiary**") are express third-party beneficiaries of your obligations and representations herein. DigiCert may offer a limited Relying Party Warranty for the benefit of persons who rely on a DigiCert certificate in good faith (for example, email recipients or users who suffer damage due to a certificate being improperly issued). Any such warranty is not a warranty to you as the Subscriber, but rather to third-party relying parties as defined in the CPS or warranty documentation. You are not a third-party beneficiary of any such Relying Party Warranty. Aside from what is expressly stated in these Terms, there are no other third-party beneficiary rights conferred by this Terms of Use.
依拠当事者保証及び第三受益者： 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（CP/CPS

において定義するもので、以下、それぞれ「**証明書受益者**」といいます）は、この規定中のお客様の義務及び表明の明示的な第三受益者です。デジサートは、デジサート証明書に依拠する善意の者（例を挙げると、電子メールの受信者又は不適切に発行された証明書を原因として損害を被った利用者）の利益のための限定的な証明書利用者保証を提供できるものとします。いずれの当該保証もサブスクライバーとしてのお客様に対する保証ではなく、むしろ CPS 又は保証文書において定義する第三者依拠当事者に対するものです。お客様は、いかなる当該依拠当事者保証の第三受益者ではありません。本規約において明示的に定められているものを除き、本規約により付与されるその他の第三受益者権は一切ありません。

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 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 S/MIME 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 S/MIME 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業界規格の変更に対応するため、本規約を随時改定又は変更できます。本規約の改定版は、デジサート Web 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。本規約が改定された後も S/MIME 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。本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）S/MIME 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。本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。本規約は、本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、又は本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 CP/CPS) 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、本規約の一部の条項は、"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。本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 CP/CPS）が優先します。本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、本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: 本規約の正式版は英語で作成されています。本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。