2020 年 9 月 30 日
デジサート・ジャパン合同会社

パートナー各位

中間 CA 証明書の変更(デジサート企業認証(OV)サーバ証明書)に関するご案内

平素は弊社製品の販売支援をいただき、誠にありがとうございます。

弊社では、今後の業界要求事項の変更に対する証明書ライフサイクルの迅速な対応、および軽減化を目的として、SSL/TLS サーバ証明書の中間 CA 証明書をより短期間で定期的に変更してまいります。その一環として、このたびデジサートブランドの企業認証(OV)証明書を対象として 2020 年 10 月 16 日(金)(予定)以降に発行する証明書より中間 CA 証明書を下記のとおり変更いたしますのでご案内申し上げます。

なお、上記適用日以前に発行済みの証明書については、中間証明書の入れ替えなどの対応をいただく必要はございません。

詳細は下記をご参照ください。

弊社では引き続きサービスの向上に努めてまいりますので、今後ともご愛顧を賜りますよう、お願い申し上げます。

記

1. 適用日（予定）
2020 年 10 月 16 日(金)(日本時間)

※　日程が変更となる場合は別途ご案内申し上げます。
※　また同変更に伴う弊社の作業時間が確定次第、追加でご案内申し上げます。

2. 対象製品ならびに対象の階層構造オプション

□対象製品

・デジサート グローバル・サーバ ID

・デジサート セキュア・サーバ ID

※ EV SSL サーバ証明書、ジオトラストブランドの証明書は対象外です。

□対象の階層構造オプション

上述の製品で利用可能な全ての階層構造オプションにおける中間証明書が変更の対象となります。詳細は次のセクションを参照ください。

3. 変更内容および注意点

・対象製品について変更前後の中間 CA 証明書の名称は以下表の通りとなります。

階層構造オプション	変更前	変更後
標準：RSA SHA-2	DigiCert SHA2 Secure Server CA	DigiCert TLS RSA SHA256 2020 CA1 (*1)
オプション：RSA SHA-2 (SHA-2 ルート)	DigiCert Global CA G2	DigiCert Global G2 TLS RSA SHA256 2020 CA1
オプション：ECC (RSA ルート)	DigiCert ECC Secure Server CA	DigiCert TLS Hybrid ECC SHA384 2020 CA1
オプション：ECC (ECC ルート)	DigiCert Global CA G3	DigiCert Global G3 TLS ECC SHA384 2020 CA1

*1：万が一変更前の中間証明書やその公開鍵がピニング(固定登録)されている場合の緊急措置として、適用日以降においても、変更前の中間認証局と同一の鍵を用いた証明書を取得いただくことが可能です。当緊急措置が必要な場合は弊社テクニカルサポートまでお問合せください。

・変更後の中間 CA 証明書は弊社リポジトリの「中間 CA 証明書ダウンロード」ページに公開いたします。
https://www.digicert.co.jp/repository/intermediate.html

4 変更に必要な作業

上記適用日以降に発行された対象製品の証明書をお客様のウェブサーバにインストールい

ただく際には、変更後の新しい中間 CA 証明書を併せてインストールいただく必要があります。

a. 2020 年 10 月 15 日（木)(予定)までに発行された SSL サーバ証明書
変更前の中間 CA 証明書を Web サーバにインストールしてください。

b. 2020 年 10 月 16 日（金)(予定)以降に発行された SSL サーバ証明書
変更後の新しい中間 CA 証明書を Web サーバにインストールしてください。

※ なお、すでに発行済みの証明書には、その有効期間を迎えるまで引き続きご利用いただけます。中間証明書を入れ替えていただく必要はございません。

※ ルート証明書に変更はありません。従って、対応ブラウザ・モバイル端末範囲への影響はございません。

※ クロスルート証明書に変更はありません。ただし弊社リポジトリ「中間 CA 証明書ダウンロード」ページより「クロスルート設定用証明書込み：2 枚 1 組バンドル」をご取得・ご活用いただいている場合、このうち中間証明書の内容が変更となりますので、適用日以降にインストールをいただく場合は新しいバンドルをご取得・ご活用ください。

■必ずご確認ください■
特に適用日前後に SSL/TLS サーバ証明書を取得したお客様におきましては、
以下のいずれかの方法にて適切な中間 CA 証明書をご確認・ご選択の上インストールしてください。

方法 1. CertCentral いただく
方法 2. 発行通知メールから中間 CA 証明書をご利用いただく
方法 3. 発行された SSL/TLS サーバ証明書(End-Entity)の発行者(Issuer)を確認し、弊社リポジトリから中間 CA 証明書を取得する。

・併せて、証明書をインストールした後に SSL サーバ証明書および中間 CA 証明書が
正しく設定されていることをご確認いただくことを推奨いたします。
デジサート SSL Tools
https://ssltools.digicert.com/checker/views/checkInstallation.jsp

5. 背景

業界全体における SSL/TLS サーバ証明書の有効期間短縮をはじめとし、ブラウザコミュニティ、および CA/ブラウザフォーラム等における要求事項の変更により、今後より一層、SSL/TLS サーバ証明書ライフサイクル管理に対し迅速な対応が求められてまいります。また、これらの変更による中間 CA 証明書、および End-Entity 証明書への影響を軽減する目的とし、弊社では中間 CA 証明書のライフサイクルをより短く管理していく方針であり、その一環として、デジサートブランドの企業認証(OV)証明書の中間 CA 証明書をこのたび変更させていただくことといたしました。

弊社では、SSL/TLS サーバ証明書ライフサイクル管理のベストプラクティスとして、証明書のインストール時には、End-Entity 証明書とあわせて中間 CA 証明書も必ず入れ替えていただくようご案内しております。証明書のライフサイクル管理手順において中間 CA 証明書を固定登録すること、またはハードコーディングすることは非推奨とさせていただきます。お客様におきましても、この機会にあらためて中間 CA 証明書のお取り扱いにご留意いただき、運用の変更をご検討いただきますようお願い申し上げます。

より詳細な背景や狙いについては、こちらの弊社ブログ(英文)を併せてご参照ください。
「証明書のピンニングはやめましょう」
https://www.digicert.com/jp/blog/certificate-pinning-what-is-certificate-pinning/

6. 今後の予定について

弊社 SSL/TL S サーバ証明書における今後の中間 CA 証明書の変更の計画については以下の弊社ウェブページをご参照ください。

「【重要】デジサート中間 CA 証明書変更に関するお知らせ」(日本語)
https://knowledge.digicert.com/ja/jp/alerts/ALERT2709.html

(英語)「DigiCert ICA Update」
https://knowledge.digicert.com/alerts/DigiCert-ICA-Update.html

7. 本件に関するお問合せ先

営業窓口
パートナープログラム事務局
電話番号： 03-6893-2743
メールアドレス：SSL-Partner@digicert.com