
■■■全てのパートナー様に該当する可能性のある■■■
■■■ 重要なお知らせです ■■■

2020年7月22日

パートナー各位

デジサート・ジャパン合同会社

ドメイン認証SSLサーバ証明書の中間CA証明書変更に関するご案内

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、このたびジオトラスト クイックSSL プレミアム等ドメイン認証製品の中間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。詳細は下記をご参照ください。

弊社では引続きサービス向上に努めて参りますので、今後ともご愛顧賜りますようお願い申し上げます。

記

1 適用日時

2020年7月31日(金) 0:00 より順次

※同変更に伴う弊社の作業を0:00～2:00の間に実施いたします。

同作業に伴うサービスの停止はございませんが、証明書が発行される時間帯により、中間CA証明書が異なりますので何卒ご了承ください。

※時間は前後する場合がありますので何卒ご了承ください。

2 対象製品

・ジオトラスト クイック SSL プレミアム

※マルチドメインパック、ワイルドカードを含みます。

※ジオトラスト 企業認証SSL/TLSサーバ証明書、およびEV SSLサーバ証明書は対象外です。

3 変更内容および注意点

- ・ 中間CA証明書を変更いたします。

【クイックSSLプレミアム RSA SHA-2専用中間CA証明書】

(変更前) GeoTrust RSA CA 2018

(変更後) GeoTrust TLS DV RSA Mixed SHA256 2021 CA-1

- ・ 対象製品のオプションとしてご提供しております「RSA SHA-2 (SHA-2ルート)」タイプのSSLサーバ証明書をご取得の場合は対象外です。
- ・ 上記適用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7月30日 (木) 23時頃までに発行された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7月31日 (金) 0時頃以降に発行された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。証明書を入れ替えていただく必要はございません。

■必ずご確認ください■

- ・ 適用時間は前後する場合がございます。
特に適用日日時前後に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証明書をご選択の上インストールしてください。

方法1. 発行通知メールに含まれるサーバ証明書と中間CA証明書をご利用する。

方法2. サーバ証明書の発行者(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。

- ・ 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.geotrust.co.jp/resources/repository/intermediate.html>

- ・ 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>

4. 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、ドメイン認証製品の中間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。

Stop Certificate Pinning(英文)

<https://www.digicert.com/blog/certificate-pinning-what-is-certificate-pinning/>

5. 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

以上

発行：デジサート・ジャパン合同会社
