2022 年 9 月 16 日

パートナー各位

デジサート・ジャパン合同会社

SSL/TLS サーバ証明書のルート証明書、および中間 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。

このたび弊社では、2023 年 3 月より、パブリック環境で利用いただく SSL/TLS サーバ証明書の中間 CA 証明書を変更し、新たな次世代ルート証明書(以下、第 5 世代 デジサート “G5 ルート”)に署名検証する新証明書階層へ移行を開始する計画であることを通知申し上げます。
ウェブサイトを管理いただくお客様におきましては、適用日以降に発行される証明書には、新しい中間 CA 証明書をご利用いただく予定となりますので、何卒ご理解いただきますようお願い申し上げます。当変更に関する背景、概要、および今後の予定につきましては以下をご確認ください。なお、現在ご利用の発行済み証明書、適用日前に発行される証明書は、その有効期限まで継続してご利用いただけます。

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. 適用予定日
2023 年 3 月 9 日（木）2:00 (日本時間)

※適用時間は前後する場合がございます。日程に変更が生じる場合はご案内いたします。

2. 背景
デジサートが現在利用しているルート証明書は、サーバ証明書やコードサイニング証明書用途など、多目的の利用用途があります。新しい G5 ルート証明書、および中間 CA 証明書は、TLS/SSL のみを発行することに特化した単一目的の証明書となります。 各利用用途専用のルート証明書にすることにより、コードサイニング証明書や S/MIME 証明書など他の証明書に求められる基本要件と区分して管理することができ、業界や CA/ブラウザフォーラムが求めるガイドラインの変更の影響を限定的とすることができます。

3. 対象となるサービス
SSL/TLS サーバ証明書　、 以下の製品を含みます。

・グローバル・サーバ ID EV
・グローバル・サーバ ID
・セキュア・サーバ ID EV
・セキュア・サーバ ID
・スタンダード・サーバ ID EV
・スタンダード・サーバ ID
・ジオトラスト トゥルービジネス ID with EV
・ジオトラスト トゥルービジネス ID
・ジオトラスト クイック SSL プレミアム

※プライベート SSL サーバ証明書は対象外です。

4. 変更内容

4-1. 中間 CA 証明書の変更について

上記適用日以降に、新規、更新、再発行申請により発行される証明書は、新しい中間 CA 証明書から発行されます。適用日以降に発行されたサーバ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。 各製品における新しい中間 CA 証明書の詳細は、今後、後続のメール、および弊社サポートサイトに掲載いたします。

なお、すでに発行済みの証明書、または適用日以前に発行される証明書は、その有効期限をむかえるまで、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。

4-2. ルート証明書の変更について

上記適用日以降に、新規、更新、再発行申請により発行される証明書は、次世代の
G5 ルート証明書に署名検証します。

現在利用されているルート証明書：

・Baltimore CyberTrust Root
・DigiCert Assured ID Root CA
・DigiCert Global Root CA
・DigiCert High Assurance EV Root CA

今後利用するルート証明書：
・DigiCert TLS RSA4096 Root G5
・DigiCert TLS ECC P384 Root G5

ルート証明書は、通常クライアント側に登録されています。Windows、Chrome、360、および Firefox の最新バージョンには、すでに新しい G5 ルートが含まれており一般的なブラウザでアクセスする際には、問題なく通信が可能です。 ただし、G5 ルート証明書が搭載されていないレガシー機器等の端末と TLS 通信を想定している場合は、ルート証明書未対応により通信エラーとなる場合がございます。

ご参考）SSL 証明書とは
https://www.digicert.com/jp/what-is-an-ssl-certificate

5. 今後の予定について
当メールは、今後予定されている中間 CA 証明書、ルート証明書の変更の計画についてご案内しております。今後、当変更における各製品毎の中間 CA 証明書、クロスルート証明書の取得手順等詳細を順次ご案内いたします。

6. よくあるご質問：
Q. 中間 CA 証明書やその公開鍵がピニング(固定登録)しています、および/またはルートストアを管理しています。適用日までに何をすればよいでしょうか？

A. 適用日前までに、お客様の環境を変更、または G5 ルートを配布いただきますようお願いいたします。なお、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いております。

[ブログ] 証明書のピニングはやめましょう
https://www.digicert.com/jp/blog/certificate-pinning-what-is-certificate-pinning

Q. クライアント環境に、G5 ルートが搭載されていない場合はどうすればよいですか？

A.　Windows、Chrome、360、および Firefox の最新バージョンには、すでに新しい G5 ルートが含まれており一般的なブラウザでアクセスする際には、問題なく通信が可能です。ただし、G5 ルート証明書が搭載されていないレガシー機器等の端末と TLS 通信を想定している場合は、ルート証明書未対応により通信エラーとなる場合がございます。

弊社では、各ベンダーにG5 ルート証明書の配布および搭載を依頼するとともに、
従来ルート証明書との接続を可能とするクロスルート証明書の提供の準備をしております。
適用日以降に、レガシー機器端末との接続を継続する場合は、End-Entity 証明書、
中間 CA 証明書とあわせてクロスルート証明書を必ずインストールいただくことで、
従来と同等の接続が可能となります。ブラウザの対応状況、および各製品における
クロスルート証明書の取得手順などの詳細は、今後、後続のメール、および
弊社サポートサイトに掲載いたします。

Q. 適用日までに新 G5 ルートへの対応が間に合わない場合、どうすればよいでしょうか？

A. 弊社ではお客様の期間における緊急措置として、適用日以降においても、変更前の
中間 CA 証明書から発行する従来階層の証明書を取得いただけるよう準備いたします。
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。
ただし、Mozilla は、現在利用しているルート証明書を 2024 年に順次「信頼しない認証局」
としてみなす措置を適用する予定です。信頼されない認証局（ルート証明書）は、
Firefox 等 Mozilla ルートストアを参照するクライアント端末との TLS 接続はエラーとなります。
このため、弊社では、ブラウザベンダの措置適用前までに、新ルート証明書への移行を
強く推奨いたします。また今後、業界全体として、多目的で利用されるルートから、
単一用途のルート証明書への移行が推奨され、今後さらなる業界の規制の対象となる
可能性があることもご留意ください。

Q. クロスルート証明書はどのように取得できますか？
A. クロスルート証明書のご案内、およびご取得方法につきましては、今後追加の
お知らせにてご案内いたします。

ご参考)
【重要】G5 ルート証明書ならびに中間 CA 証明書変更に関するご案内
https://knowledge.digicert.com/ja/jp/alerts/ALERT2817.html

デジサート ルート証明書/中間 CA 証明書

https://www.digicert.com/kb/digicert-root-certificates.htm

7. 本件のお問い合わせ先

デジサート・ジャパン合同会社
テクニカルサポート
Email：server_info_jp@digicert.com
電話：03-4578-1368（自動音声ガイダンス 3）
受付時間：土日祝日および年末年始を除く平日 9:30 - 17:30

以上