2022 年 9 月 9 日

パートナー各位

デジサート・ジャパン合同会社

TLS 接続における CBC 暗号のサポートの終了について

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、稼働サービスの安全性向上のため、弊社サービスの SSL/TLS 接続における暗号スイートにおいて、Cipher-Block-Chaining 暗号（以下、CBC 暗号）を含む暗号アルゴリズムのサポートを終了いたしますのでご案内申し上げます。 一般的なブラウザを使って弊社サービスにアクセスしている場合は、影響をうけません。
詳細につきましては、以下をご確認いただきますようお願い申し上げます。
なお、現在ご利用の発行済み証明書に影響はございません、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
2022 年 10 月 9 日（土）13:00(日本時間)

2. 対象
弊社サービスにアクセスいただく際の SSL/TLS 通信、以下のサービスを含みます。

CertCentral
CertCentral パートナー
CertCentral Service API

※お客様のサービスでご利用いただいている SSL/TLS サーバ証明書に影響はございません。

3. 変更点弊社サービスにアクセスいただく際の SSL/TLS 接続おける下記の暗号スイートのサポートを終了いたします。通常、最新のブラウザ

(Google Chrome, Safari, Mozilla Firefox, Microsoft Edge 等)を使用している場合は、
ガロア/カウンターモード（GCM）暗号などの強力な暗号をサポートしており、
自動で切り替わるため当変更による影響はございません。 その他のブラウザをご利用の
場合は、適用日前までに最新バージョンに更新いただくよう推奨いたします。

また、DigiCert サービスと相互作用するブラウザ依存のサービス、および CBC 暗号に
依存するアプリケーションをご利用の場合は、当変更に影響する場合がございます。
ウェブサーバー、システム、エージェント、API インテグレーションの場合で、
アプリケーションまたは API 統合がこの変更の影響を受ける場合は、それらの
アプリケーションで GCM 暗号などのより強力な暗号を有効にし、2022 年 10 月 8 日まで
に
API 接続を更新してください。 API 統合やアプリケーションを更新しない場合、
CertCentral、CertCentral Services API と通信するために HTTPS を使用することが
できなくなります。事前に貴社サーバ設定をご確認のうえ、他の強力な暗号スイートを
併用いただきますようお願い申し上げます。

デジサートにて利用を終了する暗号スイート：
TLS_ECDHE_RSA_ WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA

一般的なブラウザを使ってアクセスしているサイトの運用は影響ありません。
発行済み証明書への影響はなく、ご利用中の証明書の取り直しの必要もございません。
継続してご利用いただけますのでご安心ください。

ご参考)
TLS 接続における CBC 暗号サポート終了についてのご案内(デジサート)
https://knowledge.digicert.com/ja/jp/alerts/ALERT2816.html

一般的な TLS 接続における暗号設定に関しては、下記のサイトを
ご参照いただくことを推奨いたします。

TLS 暗号設定ガイドライン（独立行政法人 情報処理推進機構）
https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-3.0.1.pdf

4. 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