お客様各位

2016 年 4 月 11 日
ジェイサート株式会社

スターフィールド SHA-1 ルート証明書が「無効化」されることはありません

有力他社認証局の一部ルート証明書が、米国時間 2016 年 4 月 19 日（米国時間）（予定）に Windows OS 上で、その「利用目的」から「サーバー認証」を無効化 （信頼停止）される旨の通知が、マイクロソフトによりなされておりますが、これは**同有力認証局の 2 世代旧い公開鍵長 1024bit（ハッシュ関数は SHA-1 ですが）のルート証明書に限ったアナウンス**であり、弊社提携先スターフィールド SSL SHA-1 ルート証明書（公開鍵長 2048bit 以下、SHA-1 ルート）が「信頼停止」となることはありません。

スターフィールドには、“SHA-1 ルート”は、「SHA-1 接続拒否」が予定されている 2016 年 12 月末まで、Windows OS 上において問題なく有効に利用できることを確認済です。

さはさりながら、お客様におかれましては、以下弊社サイト FAQ をご参照頂き、出来るだけ前倒しでの SHA-2 証明書への切替をお奨め致します。
https://www.jcert.co.jp/support/faq_detail01.html#faq01-2

切替方法につきましては、弊社までお問い合わせください。

以上