

平成 27 年 10 月

ANSER-VALUXをご利用のお客様へ

中兵庫信用金庫

ANSER-VALUXにおけるサーバ証明書の変更について

ANSERセンターより、ANSER-VALUXサービスにおけるサーバ証明書の変更について、下記のとおり連絡を受けておりますのでお知らせいたします。

これに伴い、**マイクロソフト社のサポートが終了している環境(Windows XP以前のOS)を使用されているお客様**の場合は、**平成 28 年 7 月 18 日以降**の取引がご利用いただけなくなります。

上記に該当される場合は、マイクロソフト社がサポートしている環境(Windows Vista以降のOS等)に変更していただくようお願い申し上げます。

記

1. 変更内容

ANSERセンターでは、ANSER-VALUXサービスに利用しているSSLサーバ証明書(※1)のハッシュ関数(※2)をSHA-1からSHA-2に変更します。

※1. SSLサーバ証明書は、「通信の暗号化」と「Webサイトの証明」を行い、インターネット上で安全お取引いただく役割を果たしています。

※2. ハッシュ関数は、サーバ証明書が真正であることを証明するために利用され、主に改ざん検知の目的に利用されています。また、ハッシュ関数はSHA-1、SHA-2、MD-5 など、複数存在します。

2. 変更背景

SHA-1は、セキュリティ研究の進展やコンピュータの計算能力の向上などから安全性が低下しているため、様々な機関からSHA-1の使用停止が勧告されております。

また、マイクロソフト社など大手ベンダーがSHA-2への移行方針を発表していることから、ANSERセンターもSHA-2に変更いたします。

なお、Windows XP SP3については、変更となるSHA-2に対応していますが、Windows XPは、マイクロソフト社のサポートが終了しているため、お早めにサポート環境への変更をお願いします。

3. 変更時期

平成 28 年 7 月 18 日(月)

以上