【重要なお知らせ】
WEBバンキングの暗号化通信の脆弱性対応について

○ＳＳＬサーバ証明書の「ＳＨＡ－２」への移行について

ＷＥＢバンキングをより安心してご利用いただくため、**平成 28 年 5 月 9 日(月)**より、SSL サーバ証明書を現在の「SHA-1」から「SHA-2」方式に移行いたします。

証明書の移行後、「SHA-2」方式に対応していないご利用環境からは、ＷＥＢバンキングへのアクセスが出来なくなりますのでご注意ください。
なお、「SHA-2」方式に対応していないご利用環境はすでに推奨環境外であり、メーカーサポートも終了しておりますので、セキュリティの面からもバージョンアップを行っていただきますようお願いします。

■「SHA-2」について

「SHA-2」とは、SSL サーバ証明書の正当性を保障する電子署名で使用される方式です。従来の「SHA-1」方式に比べて証明書の偽造が困難となり、安全性が向上します。

■「SHA-2」に対応していないご利用環境

・２００９年前後より以前に発売された一部の携帯電話（※）
（※）携帯電話の機種の詳細につきましては、各携帯電話会社にお問合せください。
・Windows XP SP2 以前、または Internet Explorer6.0 SP2 以下の環境

■ご利用環境が「SHA-2」に対応しているか確認する方法

シマンテック社が提供している「SHA-2 のテストサイト」にアクセスし、正常に確認用ページが表示されれば、ご利用の環境は「SHA-2」に対応しています。

「SHA-2」テストサイト（シマンテック社）
https://ssltest-sha2int.jp.websecurity.symantec.com/

いつも身近なおつきあい
あばしりしんきん

○ＳＳＬ３．０の脆弱性への対応について

インターネット通信で使用する暗号化方式「SSL3.0」に発見された、通信内容の一部が第三者に漏洩する可能性がある脆弱性への対応としまして、**平成 28 年 5 月 9 日（月）**より「SSL3.0」によるアクセスを無効化させていただきます。つきましては、「SSL3.0」ではＷＥＢバンキングへのアクセスができなくなります。

ＷＥＢバンキングでは、「SSL3.0」の次のバージョンである「TLS」方式に対応していますので、今一度ブラウザのセキュリティ設定をご確認のうえ、「TLS1.0」「TLS1.2」の使用を有効としてください。

セキュリティ設定の確認、変更方法については、以下をご確認ください。

■セキュリティ設定の確認、変更手順

以下は、Internet Explorer6.0 以前のブラウザ（注）をご利用の方、またはブラウザの設定で「TLS」を自ら無効化した方が対象となります。

（注）Internet Explorer6.0 以前のブラウザは推奨環境ではありません。

① Internet Explorer の［ツール］→［インターネット　オプション］を選択。

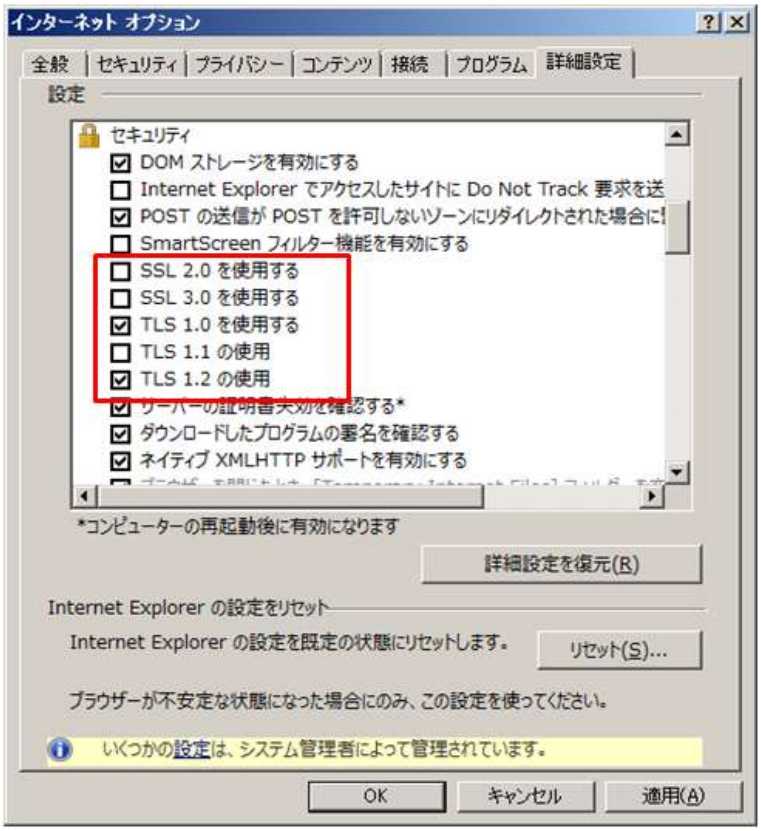
② ［インターネット　オプション］→［詳細設定］タブを選択。

③ ［セキュリティ］の中の、[SSL3.0 を使用する］のチェックをオフにし、[TLS1.0 を使用する］[TLS1.2 を使用]（※）にチェックを入れる。（※ [TLS1.1] にはチェックを入れないでください。）

④ ［ＯＫ］をクリック。

⑤ 全ブラウザを終了し、Internet Explorer を再起動させる。

＜画面例＞



【Safari の場合】

アップル社から「SSL3.0」の脆弱性に対応したセキュリティアップデート「2014-005」が提供されています。ソフトウェアをアップデートしていただきますようお願いします。

［参考］：独立行政法人情報処理推進機構（IPA）のホームページ

「SSL3.0」の脆弱性対策について（CVE-2014-3566）

https://www.ipa.go.jp/security/announce/20141017-ssl.html