

平成31年3月

インターネットバンキング等利用者 各位

岐阜商工信用組合  
事務部

### SSL/TLSにおける64ビットブロック暗号(3DES)の無効化対応について

岐阜商工信用組合では、インターネットバンキングサービス「しょうしんインターネットバンキング」、「しょうしんビジネスバンキング」(以下、「IB等」という)、「しょうしんでんさいネット」において、これまでセキュリティ対策としてSSLにおける64ビットブロック暗号【3DES】を採用しておりました。

「3DES」方式は、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等から安全性が低下しているため、今回、同方式を無効化とする対応を行います。

下記の適応時期以降、「3DES」暗号化方式を採用しているOS・ブラウザの利用者は、ご利用いただけなくなる可能性があります。

つきましては、NTTデータが運営するWebページ「[どこでもバンク※](https://www.dokodemobank.ne.jp/index.asp)」にて、動作確認済のOS・ブラウザを確認していただき、動作確認対象外のOS・ブラウザを使用されている利用者は、既にメーカーのサポートも終了していることから、可能な限り速やかに動作確認済のOS・ブラウザへ切替をお願いいたします。

※ [どこでもバンク](https://www.dokodemobank.ne.jp/index.asp) … (URL : <https://www.dokodemobank.ne.jp/index.asp>)

#### 【ご参考】

- ・「3DES」方式とは、64ビットブロック暗号ともいいます。「DES」は、データを64ビット長のブロックに分割し、各ブロックを56ビット長の鍵で暗号化する共通暗号鍵アルゴリズムであり、「3DES」は「DES」を3重に繰り返すことで、暗号強度を高めているものになります。IB等に利用者が接続し使用している暗号化方式の1つが「3DES」方式になります。利用者から各サービスに接続する際に、SSL暗号化通信方式を決定し、決定したSSL暗号化通信の方式を用いて、通信を行います。
- ・「SSL」とは、ブラウザとサーバー間を暗号化する「secure sockets layer」の頭文字をとった略称です。インターネットで広く使われているホームページ上の画面入力情報の送信や、ファイルをサーバーにアップロード、ダウンロードするときのデータに対して、暗号化鍵やデジタル証明書などのセキュリティ技術を組み合わせることで安全性を高めています。利用者は、URLが「https://～」と「s」が入っていることで、利用しているサービスはSSLを導入していると判断できます。

#### 記

#### 1. 無効化の適応時期

当組合では、SSL暗号化通信の方式として、下記のサービスで「3DES」方式を採用しています。「3DES」方式の暗号化方式を採用しているOS・ブラウザについては、適応時期以降に「3DES」方式の無効化を進め、接続利用できなくなります。

サービス	無効化の適応時期
しょうしんビジネスバンキング	2019年4月15日(月) Am6:00~
しょうしんでんさいネット	
しょうしんインターネットバンキング	2019年5月20日(月) Am6:00~

## 2. 「3DES」の暗号化方式を採用しているOS・ブラウザ

アクセス不可となる <sup>おそれ</sup> のOS・ブラウザ
Windows VISTA以前のWindows OS
OS X 10.8以前のmac OS
Android 2.2以前のAndroid OS
iOS 4.x以前のiOS
Firefox 24未満のFirefoxブラウザ

なお、各利用者の動作確認の詳細については、当組合では確認・回答いたしかねます。恐れ入りますが、「どこでもバンク」掲載してある動作確認済のOS・ブラウザを確認していただき、切替が必要な利用者是对応をお願いいたします。

## 3. 注意事項

動作確認対象外のOS・ブラウザを利用されている方においては、「3DES」暗号化方式を使用しているものもあり、サービスを利用できなくなる可能性があります。利用できなくなったご利用者につきましては、動作確認済のOS・ブラウザへ変更いただくことで、再度利用が可能となります。

以 上

### ○ 本件に関するお問合せ先

「しょうしん事務センター」

電話番号 0120-201-228 (通話料無料)

受付時間 平日9:00~17:00

※土、日、祝日、1月1日~3日、5月3日~5日、12月31日はご利用いただけません。