2015-2016 ベリトランス決済サービスセキュリティ強化対応

～SHA-256 証明書対応および、SSL3.0/TLS1.0 の廃止対応～

3G-Web システム対応ガイド

Ver. 1.1 （2016 年 4 月～）

目次

1. はじめに 3
2. SHA-2 環境の変更点とシステム対応概要 4
3. システム環境要件 4
3.1. TLS1.1 非対応端末（フィーチャーフォン等）への対応 4
4. SHA-2 環境への接続手順 5
4.1. 接続 URL の変更（設定ファイルの変更） 5
4.2. 通信処理プログラムの変更 6
4.2.1. Java 7 をご利用の場合 6
4.2.2. .NET をご利用の場合 6
4.2.3. PHP をご利用の場合 6
5. 接続検証の手順 7
5.1. マーチャント様環境の準備 7
5.2. 検証用取引の実行 7
5.3. 検証結果の確認 8
5.4. 検証完了のご連絡 8
5.5. 本番運用の開始 8
6. その他 9
6.1. 著作権、および問合せ先 9
6.2. 改定履歴 9

1. はじめに

本ガイドは、SHA-256 証明書に対応した 3G-Web の新環境（以下、SHA-2 環境）に接続するためのシステム環境要件およびシステム対応の手順を説明するものです。

本ガイドに記載の内容に従い、旧環境（SHA-1 環境）の停止（2016 年 9 月 5 日 AM10:00）までに、ベリトランスの SHA-2 環境を利用した接続検証を実施し、マーチャント様の本番環境を、ベリトランス SHA-2 環境への接続に切り替えて頂きますようお願いします。

接続切り替えを行って頂けない場合には、旧環境の停止以降、すべてのサービスのご利用ができなくなりますので、余裕を持ったスケジュールでのご対応をお願い申し上げます。

【関連ドキュメント】

タイトル/ファイル名	概要
【重要】2015-2016 ベリトランス決済サービスセキュリティ強化対応_概要説明資料 2015-2016_VeriTransSslSecurityUpgrade_Overview_1.x.pdf	ベリトランスが実施するセキュリティ強化対応（SHA-256 証明書対応および、SSL3.0/TLS1.0 の廃止）に関する概要説明資料です。
【付録】2015-2016 ベリトランス決済サービスセキュリティ強化対応_補足資料 2015-2016_VeriTransSslSecurityUpgrade_Appendix_1.x.pdf	ベリトランスが実施するセキュリティ強化対応の補足説明資料です。
【付録】2015-2016_ベリトランス決済サービスセキュリティ強化対応 【PHP をご利用の際の注意点】 2015-2016_VeriTransSslSecurityUpgrade_Appendix_PHP_1.x.pdf	ベリトランスが実施するセキュリティ強化対応において、開発言語 PHP をご利用の際にご注意頂きたい内容を説明した資料です。
3G-Web 開発ガイド 3G-Web サンプルプログラム インストールガイド	3G-Web を導入する際の開発者向けガイドです。 店舗様の EC サイトより 3G-Web へ接続し、利用する方法が記載されています。

2. SHA-2 環境の変更点とシステム対応概要

ベリトランス SHA-2 環境では、既存環境から以下の点が変更されています。

- SHA-256 証明書への変更
- 脆弱な暗号方式である SSL3.0 および TLS1.0 の通信の無効化
- サービスに接続するための URL の変更

アクセス URL	
既存環境の URL	https://3g.veritrans.co.jp/web1
SHA-2 環境（SSL3.0/TLS1.0 無効）の URL	https://pay.veritrans.co.jp/web1

SHA-2 環境に接続するためには、マーチャント様システムにて以下の対応が必要となります。

- ✓ SHA-2 環境 URL への接続先変更
- ✓ システムのアップグレード（システム環境要件を満たさない場合）
- ✓ 通信処理プログラムの変更（※Java7 または.NET をご利用の場合）

3. システム環境要件

ベリトランス SHA-2 環境に接続するためには、TLS1.1 以上で通信可能な環境が必要です。

開発言語	システム環境要件
Java	Java**7** 以上（Java8 以上を推奨）
PHP	PHP **5.3** 以上（PHP 5.6 以上を推奨） OpenSSL ver.**1.0.1** 以上[注1]の導入と、サポートする PHP 環境
.NET	Windows Server **2008 R2** 以上、Windows7 以上 .NET Framework **4.5** 以上

【重要】上記の要件を満たさない場合には、マーチャント様システムのアップグレードが必要となります。

注 1　TLS1.1 以上の通信をサポートする OpenSSL のバージョンは 1.0.1 以降となりますが、OpenSSL はいくつかの重大な脆弱性が発表されておりますので、最新バージョンをお使い頂きますようお願い申し上げます。

3.1. TLS1.1 非対応端末（フィーチャーフォン等）への対応

消費者様のブラウザが SHA-2 および TLS1.1 以上に対応していない場合、SSL3.0 および TLS1.0 の通信を無効化した SHA-2 環境への切り替え対応後は、消費者様のブラウザからベリトランスへ接続ができなくなります。
特にフィーチャーフォンをご利用の場合、非対応端末での購入手続きは一切行うことができなくなるため、予めマーチャント様から消費者様へアナウンスを行って頂くようお願いいたします。

※フィーチャーフォンの SHA-2/TLS1.1 対応状況については、各携帯会社へお問い合わせ下さい。

なお、引き続きフィーチャーフォンを利用した決済を有効にするために、消費者のブラウザを、SSL3.0 および TLS1.0 を有効化した SHA-2 暫定環境に遷移させることも可能です。

アクセス URL	
暫定環境（SSL3.0/TLS1.0 有効）の URL	https://3gs.veritrans.co.jp/web1

ただし、暫定環境は 2018 年 5 月に停止を予定していますので、停止日までには必ず SHA-2 環境（pay.veritrans.co.jp）に遷移させるよう、変更して頂く必要があります。

4. SHA-2 環境への接続手順

各プログラミング言語用のサンプルプログラムをベースにマーチャントサイトのアプリケーションを実装している場合は、次に示す手順で、SHA-2 環境に接続するための対応を行ってください。

（重要）

システムの設定変更を行う際には、必ずシステムのバックアップを行って頂きますようお願いいたします。

4.1. 接続 URL の変更（設定ファイルの変更）

3G-Web サービスに接続するための URL を、SHA-2 環境用の URL に変更してください。
下表に、各プログラミング言語用のサンプルプログラムが参照する設定ファイルの変更箇所をご説明します。

言語	接続 URL の変更箇所
Java	設定ファイル：VTWEBMDK.properties
	VTWEB_REGIST_URL = https://pay.veritrans.co.jp/web1/commodityRegist.action ---① VTWEB_SETTLEMENT_URL = https://pay.veritrans.co.jp/web1/deviceCheck.action ---②
PHP	設定ファイル：define.php
	define('VTW_HTTP_POST_URI','https://pay.veritrans.co.jp/web1/commodityRegist.action'); ---① define('PAYMENT_URL','https://pay.veritrans.co.jp/web1/deviceCheck.action'); ---②
.NET	設定ファイル：MerchantConf.xml
	<!--暗号鍵取得 URL--> <vtWebRegistUrl>https://pay.veritrans.co.jp/web1/commodityRegist.action</vtWebRegistUrl> ---① <!--決済 URL--> <vtWebSettlementUrl>https://pay.veritrans.co.jp/web1/deviceCheck.action</vtWebSettlementUrl> ---②

※ 表中の①は、マーチャント様アプリケーションから 3G-Web サーバに接続する URL です。
表中の②は、消費者のブラウザを 3G-Web サーバに遷移させる URL です。
SHA-2 暫定環境をご利用の際は、これらの URL のホスト名を 3gs.veritrans.co.jp に変更してください。

4.2. 通信処理プログラムの変更

✓ マーチャント様の WEB アプリケーションから、SHA-2 暫定環境に TLS1.0 で接続する場合は、以下のプログラム修正は不要です。ただし、SSL3.0 での接続はセキュリティの観点からご利用を控えて頂きますようお願いいたします。

4.2.1. Java 7 をご利用の場合

Java 7 をご利用の場合は、SSLContext のインスタンスを取得する際、明示的に TLS1.2 を指定する必要があります。
以下に、サンプルプログラム［jp.co.veritrans.vtweb.sample.server.action.ConfirmAction.java］の send メソッドの修正箇所をご説明します。

```
～省略～

MerchantConf info = MerchantConf.getInfo();
//以下のコードを追加してください。ここから {
SSLContext sc = SSLContext.getInstance("TLSv1.2");
sc.init(null, null, new java.security.SecureRandom());
HttpsURLConnection.setDefaultSSLSocketFactory(sc.getSocketFactory());
// } ここまで
URL accessURL = new URL(info.getVtWebRegistUrl());

～省略～

注 1. 上記コードを追加するには、以下のクラスの import が必要となります。
import java.security.KeyManagementException;
import javax.net.ssl.SSLContext;


注 2. 上記コードの追加により throw される例外のハンドリングを適切に実装してください。
```

※Java8 をご利用の場合は、上記のコードを追加する必要はありません。

4.2.2. .NET をご利用の場合

サンプルプログラム［APP_Code/PostData.cs］では、HTTPS 通信のために HttpWebRequest クラスを利用していますが、このクラスの既定の状態では SSL3.0 および TLS1.0 が有効となっています。
TLS1.1 および 1.2 を有効にするために、System.Net.ServicePointManager クラスの SecurityProtocol プロパティを設定してください。

```
ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls11 | SecurityProtocolType.Tls12;
```

参考： http://blogs.technet.com/b/jpieblog/archive/2015/04/07/3647694.aspx

4.2.3. PHP をご利用の場合

サンプルプログラムをベースとしたソースコードの場合、変更の必要はありません。

5. 接続検証の手順

ご利用の全てのサービスについて、ベリトランス SHA-2 環境との接続検証を行って頂きますようお願いします。
検証を行って頂く際は、本番サーバと同等スペックのマーチャント様環境から疎通確認を行って頂いたうえで、最終確認として本番環境からの接続検証を行って頂くことを推奨いたします。

5.1. マーチャント様環境の準備

- ✓ 検証を行う環境として、マーチャント様の本番サーバと同等の検証用サーバ環境（OS, ミドルウェア, プログラミング言語環境等のバージョンが同一のサーバ）をご用意頂きますようお願いします。
- ✓ 最終確認として、本番サーバでの検証を行って頂きますようお願いします。
  - ✧ 検証用サーバでは発生しなかった問題が、本番サーバで発生する可能性もありますので、本番サーバでも疎通確認を実施頂いたうえで、本番運用を行って頂きますようお願いいたします。

5.2. 検証用取引の実行

- ✓ マーチャント様のサイトから検証用の取引を実行し、ベリトランス SHA-2 環境との通信が正常に行われることをご確認ください。
- ✓ 原則として、3G-Web サーバと通信を行う全ての機能について、ご確認をお願いいたします。
- ✓ 本番モード（DUMMY_PAYMENT_FLAG=0）での実行を推奨いたしますが、ダミーモード（DUMMY_PAYMENT_FLAG=1）でも実行が可能です。
  - ➢ 本番モードでの取引を行った場合、クレジットカード決済等の決済方法では、実際に与信や売上が成立しますので、必ず取消を行って頂きますようお願いします。
  - ➢ ダミーモードでは、ご利用のサービスにより指定できるパラメータが決まっている場合があります。例えば、カード決済で指定できるカード番号は以下のとおりです。

（テスト用クレジットカード番号）

VISA	4111111111111111
MasterCard	5555555555554444
	5105105105105100
	5500000000000004
JCB	3528000000000007
	3528000000000015
	3528000000000023
	3530111333300000
AMEX	378282246310005
	371449635398431
	377752749896404
	341111111111111
Diners	36666666666660
その他	6950695069506958

※ダミーモードのご利用方法詳細につきましては、別紙「VeriTrans 3G 導入テストガイド」をご参照下さい。

- ✓ 検証に利用するマーチャント ID は、現在ご利用の本番用マーチャント ID をご利用頂きますようお願いします。
  - ➢ 本番用マーチャント ID のご利用が難しい場合は、全マーチャント様で共用のマーチャント ID をご利用頂くことも可能です。共用のマーチャント ID では、全ての取引がダミーモードとなりますのでご留意下さい。
    - ✧ 共用のマーチャント ID は、ベリトランスのサポートサイトより取得可能です。
      https://www.veritrans.co.jp/support/trial/login/3g/

5.3. 検証結果の確認

- ✓ 取引要求が、ベリトランスの SHA-2 環境に向けて送信されていることをご確認下さい。
- ✓ 取引要求に対し、ベリトランス SHA-2 環境からの応答が正常に受信できることをご確認下さい。
  - ➢ 接続に失敗した場合は、例外の内容をご確認下さい。
    - ✧ OS やミドルウェアのログも合わせてご確認下さい。例えば、PHP の場合は WEB サーバ（apache のログ等）に何らかのエラーが出力されている場合がございます。
- ✓ ベリトランスからの結果通知電文が正常に受信できることをご確認下さい。
- ✓ マーチャント様システムの後続の処理（ベリトランスからの応答を受信後の処理）に支障がないことをご確認下さい。

5.4. 検証完了のご連絡

- ✓ 検証完了後、以下の内容を SSL-SHA2 切替窓口（ssl-sha2@veritrans.jp）までご連絡頂きますようお願いします。
  - 本番マーチャント ID／検証時マーチャント ID
  - ご利用のベリトランスサービス
  - ご利用のプログラミング言語・バージョン
  - 検証に利用したサーバ OS・バージョン
  - 接続元グローバル IP アドレス
  - 検証完了日時
  - 本番切替予定日

5.5. 本番運用の開始

- ✓ マーチャント様本番環境の接続先を、ベリトランス SHA-2 環境に向けて切り替えて頂くタイミングは、接続検証の完了後、旧環境（SHA-1 環境）の停止日までに、マーチャント様の任意のタイミングで行って頂きますようお願いいたします。
  - ✧ 接続先の変更時には、問題が発生した場合の切り戻しや復旧の手順などを十分にご検討下さい。

6. その他

6.1. 著作権、および問合せ先

［お問い合わせ先］　ベリトランス株式会社 SSL-SHA2 切替窓口　電子メール：ssl-sha2@veritrans.jp

6.2. 改定履歴

2016/03/15 ：Ver1.0 リリース

2016/04/11 ：Ver1.1 リリース

- 「3.1. TLS1.1 非対応端末（フィーチャーフォン等）への対応」を追加し、SSL3.0/TLS1.0 を有効化した暫定環境の説明を追加。
- 「4.1. 接続 URL の変更（設定ファイルの変更）」の URL の説明を追記