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～

VeriTrans3G-Direct システム対応ガイド

Ver. 1.2 （2016 年 3 月～）

目次

1. はじめに

本ガイドは、SHA-256 証明書に対応した VeriTrans3G-Direct 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。
VeriTrans3G Direct API ドキュメント	VeriTrans3G Direct を導入する際の開発者向けガイドです。 開発の際の参考となるサンプルや、提供ライブラリの説明、電文フォーマットなどについて記載されています。

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/vtdirect
SHA-2 環境の URL	https://api.veritrans.co.jp/vtdirect

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 環境のホスト名への API エンドポイント変更
- ✓ 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）

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 **5.4** 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
Ruby	Ruby **2.0.0** 以上 OpenSSL ver.**1.0.1** 以上[注1]の導入と、サポートする Ruby 環境

【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　ベリトランスでは、OpenSSL ver.1.0.1 以上で動作確認を行っています。
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。

4. API ライブラリをご利用の場合

各言語の設定プログラムに定義されている API エンドポイントのホスト名を下記の通り変更して下さい。

- 最新版 API ライブラリは以下の URL よりダウンロードして下さい。
  https://www.veritrans.co.jp/support/trial/login/3g/

（重要）

設定プログラムの変更を行う際には、必ず現在お使いの API ライブラリおよび設定ファイルを含め、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. Java 版 設定プログラム[ClientConfiguration.groovy]での設定例

- String host = "api.veritrans.co.jp";

4.1.1. Java7 をご利用の場合

Java7 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。
[RequestClient.java]の createClient メソッドを以下のように修正して下さい。

```
private Client createClient(Boolean verifySsl) throws VtDirectNetworkException {
    ClientConfig config = new DefaultClientConfig();
    try {
        SSLContext sc = SSLContext.getInstance("TLSv1.2");
        sc.init(null, null, new SecureRandom());
        config.getProperties().put(HTTPSProperties.PROPERTY_HTTPS_PROPERTIES, new HTTPSProperties(
                (!verifySsl) ?
                        new HostnameVerifier() {
                            @Override
                            public boolean verify(String s, SSLSession sslSession) {return true; }
                        } : null, sc));
    } catch (NoSuchAlgorithmException | KeyManagementException e) {
        throw new VtDirectNetworkException("Cannot override HostnameVerifier.", e);
    }
    config.getProperties().put(ClientConfig.PROPERTY_READ_TIMEOUT, 130000);
    config.getProperties().put(ClientConfig.PROPERTY_CONNECT_TIMEOUT, 30000);
    return Client.create(config);
}
```

4.2. PHP 版 設定プログラム[Setting.php]での設定例

- private $_requestHost = "api.veritrans.co.jp";

4.2.1. 設定変更後、PHP 版 API ライブラリにて通信に失敗する場合

PHP cURL support のバージョンによっては、TLS1.1/1.2 に対応した SSL ライブラリを利用していても通信に失敗するケースがあります。その場合は、API ライブラリの CurlRequest.php に TLS1.2 を強制するオプションを指定し、検証用取引の再実行をお試し下さい。

lib/CurlRequest.php (93～94 行目付近)

- $options[CURLOPT_SSLVERSION] = 6;

4.3. Ruby 版 設定プログラム[Setting.rb]での設定例

- @request_host = 'api.veritrans.co.jp'

5. veritrans.min.js の URL 変更

API エンドポイントが変更となるため、veritrans.min.js の URL も変更となります。マーチャント様システムにて veritrans.min.js の読み込みを定義している箇所を修正してください。

アクセス URL	
既存環境の URL	https://3g.veritrans.co.jp/vtdirect/v2/veritrans.min.js
SHA-2 環境の URL	https://api.veritrans.co.jp/vtdirect/v2/veritrans.min.js

veritrans.min.js をマーチャント様環境にコピーして利用している場合は、SHA-2 環境の URL より最新の JavaScript を取得し、上書きしてください。

6. 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。

6.1. 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。

6.2. 検証用取引の実行

- ✓ マーチャント様サーバからベリトランス SHA-2 環境に取引要求を送信して下さい。
- ✓ 原則として、ご利用のすべての API 呼び出しの確認をお願いいたします。
- ✓ 本番モード（"test_mode": false）での実行を推奨いたしますが、ダミーモード（"test_mode": true）でも実行が可能です。
  - ➢ 本番モードでの取引を行った場合、API によっては実際に与信枠が確保され、売上が成立することになりますので、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 Direct API ドキュメント」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/

6.3. 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。
- ✓ マーチャント様システムの後続処理（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。

6.4. 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

6.5. 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。

7. その他

7.1. 著作権、および問合せ先

［著作権］ 本ドキュメントの著作権はベリトランス株式会社が保有しています。
Copyright (c) 2016 VeriTrans Inc., a Digital Garage company. All rights reserved.

［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

7.2. 改定履歴

2015/11/04 ：Ver1.0 リリース

2015/11/18 ：Ver1.1 リリース

「5.veritrans.min.js の URL 変更」を追加

2016/3/15 ：Ver1.2 リリース

「4.1.1.Java7 をご利用の場合」のソースコードを修正

旧環境の停止時期の前倒し（2016 年 9 月 5 日）の決定に伴い、関連する記載を修正