



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～

VeriTrans 電子マネー決済

システム対応ガイド

Ver. 1.1 (2016年3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
4.	MDK のバージョンアップ方法.....	5
4.1.	Java 版をお使いの場合.....	5
4.2.	PHP 版をお使いの場合.....	5
4.3.	.NET 版をお使いの場合.....	5
4.4.	MDK 設定ファイルの変更.....	6
4.4.1.	接続先 URL の変更.....	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.....	7
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.....	8
6.1.	著作権、および問合せ先.....	8
6.2.	改定履歴.....	8

1. はじめに

本ガイドは、SHA-256 証明書に対応した VeriTrans 電子マネー決済の新環境(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いたします。

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。
VeriTrans 電子マネー 開発ガイド	VeriTrans 電子マネー決済の MDK 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に変更されています。

- 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://fep.veritrans.co.jp:443/
SHA-2 環境の URL	https:// pay2g .veritrans.co.jp:443/

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。

- ✓ MDK のバージョンアップおよび SHA-2 環境の 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)

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	Java7 以上 (Java8 以上を推奨)
PHP	OpenSSL ver.1.0.1 以上の導入と、サポートする PHP 環境 (TLS1.1 以上で通信可能な環境) 注1
.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 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. MDK のバージョンアップ方法

MDK の開発言語毎に、バージョンアップ方法を記載しておりますので、ご利用言語の対応方法をご確認下さい。

- 最新版 MDK およびインストールガイドは、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/e-money/>

(重要)

バージョンアップを行う際には、必ず現在お使いの MDK 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 版をお使いの場合

- ① 最新バージョンの MDK アーカイブをダウンロードして下さい。
 - ファイル名: vtemmdk-java-110.tar.gz
- ② マーチャント様サイトのアプリケーションのクラスパスにある、古いバージョンの jar ファイル(axis.jar)^{注1} を削除して下さい。
- ③ アーカイブを解凍後、lib/に含まれる新しい jar ファイル(axis.jar)^{注1} をクラスパスに配置して下さい。
- ④ 「4.4 MDK 設定ファイルの変更」をご参照のうえ設定ファイルの変更を行って下さい。

注1 axis.jar はベリトランス SHA-2 環境に接続するため、弊社にて独自に拡張を行っております。MDK 以外のアプリケーションが同一クラスパスの axis.jar を参照している場合は、動作に影響がないことをご確認下さい。万が一、動作に影響がある場合は、MDK 以外のアプリケーションのクラスパスにある axis.jar とは別のクラスパスに新しい axis.jar を配置して下さい。

4.2. PHP 版をお使いの場合

- ① 最新バージョンの MDK アーカイブをダウンロードして下さい。
 - ファイル名: vtemmdk-php-110.tar.gz
- ② マーチャント様サイトのアプリケーションが参照している、MDK ライブラリのパスから古いバージョンの EmClient.php を削除して下さい。
- ③ アーカイブを解凍後、lib/EMLib/に含まれる新しい EmClient.php を MDK ライブラリのパスに配置して下さい。
- ④ lib/EMLib/ディレクトリ配下の CA 証明書ストアファイル(vsign_cli.cer)を、MDK ライブラリのパスに配置して下さい。
- ⑤ 「4.4 MDK 設定ファイルの変更」をご参照のうえ設定ファイルの変更を行って下さい。

4.3. .NET 版をお使いの場合

- ① 最新バージョンの MDK アーカイブをダウンロードして下さい。
 - ファイル名: vtemmdk-net-windows-120.zip
- ② マーチャント様サイトのアプリケーションが参照している古い MDK の DLL を削除して下さい。
- ③ アーカイブを解凍後、DLL を参照先にコピーし、マーチャント様サイトのアプリケーションの参照設定を確認、修正して下さい。

◇ VeriTransEM.dll

◇ log4net.dll

④ 「4.4 MDK 設定ファイルの変更」をご参照のうえ設定ファイルの変更を行って下さい。

4.4. MDK 設定ファイルの変更

各言語の MDK 設定ファイル名は以下の通りです。

開発言語	MDK 設定ファイル名
Java	emgwlib.properties
PHP	emgwlib.properties
.NET	emlib.conf

4.4.1. 接続先 URL の変更

MDK 設定ファイルの接続先 URL が下記の通り変更になります。

<変更前>	<変更後>
https://fep.veritrans.co.jp:443/	https:// pay2g .veritrans.co.jp:443/

MDK 設定ファイルにて、下記の通り設定して下さい。

MDK	設定項目	設定値
Java	GW_HOSTS	https:// pay2g .veritrans.co.jp:443/
PHP	GW_HOSTS	https:// pay2g .veritrans.co.jp:443/
.NET	GW_HOSTS	https:// pay2g .veritrans.co.jp:443/

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いたします。

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いたします。
- ✓ 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いたします。
 - ◇ 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、全てのコマンド(機能)の実行をお願いいたします。
- ✓ 本番モードでの実行を推奨いたしますが、ダミーモード(DUMMY_TYPE=1or2)でも実行が可能です。
- ✓ オーダーID、有効な金額データで検証用取引(entry)を送信し、取引が成功することを確認して下さい。
また、マーチャント様毎に必要なコマンドを実行し、問題なく取引が実行されることを確認して下さい。
取引の送信方法については、各開発言語の開発ガイドを参照して下さい。
- ✓ 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いたします。
 - 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/e-money/>

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。
 - MDK のログに、実際に接続した URL が出力されていますので、ベリトランス SHA-2 環境用の新 URL であ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、MDK のログをご確認下さい。
 - ◇ OS やミドルウェアが出力する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いたします。
 - 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
 - Proxy サーバの利用有無
 - 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

[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

6.2. 改定履歴

2015/11/04 : Ver1.0 リリース

2016/03/15 : Ver1.1 リリース

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