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 MPI ホスティング

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、VeriTrans MPI ホスティングの新環境（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	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。
2015-2016_VeriTransSslSecurityUpgrade_Overview_1.x.pdf	
【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	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。
2015-2016_VeriTransSslSecurityUpgrade_Appendix_1.x.pdf	
【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】	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。
2015-2016_VeriTransSslSecurityUpgrade_Appendix_PHP_1.x.pdf	
VeriTrans MPI ホスティング 開発ガイド	VeriTrans MPI ホスティングの 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://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	Java**7** 以上（Java8 以上を推奨）
PHP	OpenSSL ver.**1.0.1** 以上[注 1,注 2]
.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　MDK をご利用の場合、OS によって対応が異なります。
「4.2 PHP 版をお使いの場合」の④にて、マーチャント様がご使用になるモジュールのリンク方式をご確認下さい。

- ダイナミックリンク方式の場合、OS にインストールされた OpenSSL のバージョンが上記システム環境要件を満たす必要がございます。
- スタティックリンク方式の場合、ベリトランスが提供する MDK をご利用頂くことで、OS にインストールされた OpenSSL のバージョンに依存せずに通信が可能であるため、OpenSSL の導入は必要ございません。

注2　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 および開発ガイドは、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/mpi/

（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： mpimdk-java-120.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から、古いバージョンの jar ファイル(3DLib.jar)を削除して下さい。

③ アーカイブを解凍後、mdk/に含まれる新しい jar ファイル(3DLib.jar)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。

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： mpimdk-php-121.tar.gz

② マーチャント様サイトのアプリケーションの MDK 設定ファイルに記載のパスにある、古いバージョンのモジュール(xxx_MPICLIENT)を削除して下さい。

③ MDK 設定ファイルに記載のパスにある、古い CA 証明書ストアファイル(vsign_cli.cer)を削除して下さい。

④ アーカイブを解凍後、mdk/lib/3DGW/ディレクトリ配下のマーチャント様の環境に対応するモジュールを MDK 設定ファイルに記載のパスに配置して下さい。

OS	モジュール名	モジュールのリンク方式
Red Hat Enterprise Linux 5(64bit)	RHEL5_MPICLIENT	スタティックリンク
Red Hat Enterprise Linux 5(32bit)	RHEL5_32_MPICLIENT	スタティックリンク
Red Hat Enterprise Linux 6(64bit)	RHEL6_MPICLIENT	ダイナミックリンク注1
Red Hat Enterprise Linux 6(32bit)	RHEL6_32_MPICLIENT	ダイナミックリンク注1
Red Hat Enterprise Linux 7(64bit)	RHEL7_MPICLIENT	ダイナミックリンク注1
CentOS 5(64bit)	CENTOS5_MPICLIENT	スタティックリンク
CentOS 5(32bit)	CENTOS5_32_MPICLIENT	スタティックリンク
CentOS 6(64bit)	CENTOS6_MPICLIENT	ダイナミックリンク注1
CentOS 6(32bit)	CENTOS6_32_MPICLIENT	ダイナミックリンク注1
CentOS 7(64bit)	CENTOS7_MPICLIENT	ダイナミックリンク注1
Amazon Linux AMI release 2015.03(64bit)	AMAZON_LINUX_MPICLIENT	ダイナミックリンク注1

※上記表にマーチャント様の環境に対応するモジュールがない場合は別途ご案内致しますので、SSL-SHA2 切

替窓口（ssl-sha2@veritrans.jp）までお問い合わせください。

注1 ダイナミックリンク方式の場合、OpenSSL の共有ライブラリがライブラリパスに設定されていることをご確認下さい。
OS によっては、弊社提供モジュールの依存ライブラリと、OS のベンダーが提供するライブラリでバージョン番号が異なるため、MDK 実行時にリンクされない場合がございます。
その場合、弊社提供モジュールの依存ライブラリと同名のシンボリックリンクを共有ライブラリパスに作成し、OS のベンダーが提供するライブラリをリンク先とすることで、解決する場合がございます。

- 例えば、共有ライブラリパスに libssl.so.1.0.0, libcrypto.so.1.0.0 が存在せず、代わりに libssl.so.10, libcrypto.so.10 が存在する場合、以下のようにシンボリックリンクを作成して下さい。
  - ✧ libssl.so.1.0.0 -> libssl.so.10
  - ✧ libcrypto.so.1.0.0 -> libcrypto.so.10

⑤ 配置したモジュールに実行権限を付与して下さい。

⑥ mdk/conf/ディレクトリ配下の CA 証明書ストアファイル(vsign_cli.cer)を参照先に配置して下さい。

⑦ 「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： vtmpimdk-net-windows-130.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。

- ✧ VeriTransMpi.dll
- ✧ VeriTransCommon.dll
- ✧ log4net.dll

④ レジストリをご利用の場合は、以下のパスにエントリがありますので、設定を変更して下さい。

- HKEY_LOCAL_MACHINE¥SOFTWARE¥VeriTrans¥MPI.NET¥1¥

<変更前>		<変更後>	
名前	データ	名前	データ
GW_HOSTS	https://fep.veritrans.co.jp:443/	GW_HOSTS	https://pay2g.veritrans.co.jp:443/
TRUSTED_HOSTS	fep.veritrans.co.jp	TRUSTED_HOSTS	pay2g.veritrans.co.jp

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。

4.4. 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	3dlib.properties
PHP	mpilib.conf
.NET	mpilib.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/
	TRUSTED_HOSTS	pay2g.veritrans.co.jp
PHP	GW_HOSTS	https://pay2g.veritrans.co.jp:443/
	TRUSTED_HOSTS	pay2g.veritrans.co.jp
.NET	GW_HOSTS	https://pay2g.veritrans.co.jp:443/
	TRUSTED_HOSTS	pay2g.veritrans.co.jp

4.4.2. (Java 版のみ) SSL プロトコルの追加

MDK 設定ファイルにて、SSL プロトコルの設定が必須となります。

<Java 版 追加>
SSL_PROTOCOL = TLSv1.2

4.4.3. (PHP 版のみ) PLATFORM の設定

MDK 設定ファイルの PLATFORM の項目が正しく設定されているかご確認下さい。

OS	設定値
Red Hat Enterprise Linux 5(64bit)	RHEL5
Red Hat Enterprise Linux 5(32bit)	RHEL5_32
Red Hat Enterprise Linux 6(64bit)	RHEL6
Red Hat Enterprise Linux 6(32bit)	RHEL6_32
Red Hat Enterprise Linux 7(64bit)	RHEL7
CentOS 5(64bit)	CENTOS5
CentOS 5(32bit)	CENTOS5_32
CentOS 6(64bit)	CENTOS6
CentOS 6(32bit)	CENTOS6_32
CentOS 7(64bit)	CENTOS7
Amazon Linux AMI release 2015.03(64bit)	AMAZON_LINUX

- MDK 設定ファイル[mpilib.conf]での設定例(Red Hat Enterprise Linux 7 64bit の場合)

  PLATFORM = RHEL7

4.4.4. MDK の設定の反映

必要に応じてアプリケーションサーバ等を再起動し、MDK の設定を反映して下さい。

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。
- ✓ 以下のテスト用マーチャント ID で実行をお願いいたします。

テスト用マーチャント情報	
マーチャントシークレット	test-bsf
マーチャント認証鍵	83e5f7d3522fedee45df9b177d0e079534c655d1

※MDK 設定ファイルの設定方法は、各開発言語の開発ガイドを参照して下さい。

- ✓ 下記「テスト用カード番号」を用いて、検証用取引(auth/verify)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。

（テスト用クレジットカード番号）

VISA	4111111111111111
Master	5555444455554442
	5555555555554444
JCB	3528000000000007
	3528000000000015
	3528000000000023

- ✓ テスト用マーチャント情報で検証を行う際の注意事項を記載します。

（A）当テスト環境について

- ✓ テスト用マーチャント情報を用いて送信された取引は、決済はされません。

- ✓ 他のマーチャント様との共用環境となります。他のマーチャント様の取引に対して、一切の処理は行わないで下さい。
- ✓ 処理件数の多いバッチ処理等、負荷のかかるテスト取引は行わないで下さい。
  ※詳細なテスト仕様等は、各開発言語の開発ガイドを参照して下さい。

（B）テスト用カード番号について

- ✓ 「テスト用カード番号」は、テスト用マーチャント情報でのみ有効です。本番環境ではこのカード番号を送信できません。

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

［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

2015/11/18 ：Ver1.1 リリース

「4.2. PHP 版をお使いの場合」「4.4.3. (PHP 版のみ) PLATFORM の設定」に新規対応 OS の記載を追加

- Red Hat Enterprise Linux 5(32bit)
- Red Hat Enterprise Linux 6(32bit)
- Cent OS 6(32bit)
- Amazon Linux AMI release 2015.03(64bit)

2016/03/15 ：Ver1.2 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