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 システム対応ガイド

Ver. 1.5 （2016 年 7 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 6
4.1. Java 版をお使いの場合 6
4.2. PHP 版をお使いの場合 6
4.3. .NET 版をお使いの場合 7
4.4. Ruby 版をお使いの場合 7
4.5. MDK 設定ファイルの変更 8
4.5.1. Ver.2 系(2.x.x)からのバージョンアップの場合 8
4.5.2. Ver.1 系(1.x.x)からのバージョンアップの場合 9
5. 接続検証の手順 11
5.1. マーチャント様環境の準備 11
5.2. 検証用取引の実行 11
5.3. 検証結果の確認 12
5.4. 検証完了のご連絡 12
5.5. 本番運用の開始 12
6. その他 13
6.1. 著作権、および問合せ先 13
6.2. 改定履歴 13

1. はじめに

本ガイドは、SHA-256 証明書に対応した VeriTrans3G 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 開発ガイド	VeriTrans3G 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が記載されています。
VeriTrans3G MDK インストールガイド	VeriTrans3G の MDK を導入する際の開発者向け MDK インストールガイドです。 MDK ファイル構成や設定方法、サンプルプログラム等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:443/
SHA-2 環境の URL	https://api.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	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
.NET (.NET Framework 3.5 対応版 [注2])	Windows Server **2008 R2** 以上、Windows7 以上 .NET Framework **3.5** 以上
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。

注2　.NET Framework 3.5 の環境で.NET 版 MDK をご利用の際には、Windows OS に応じて以下のパッチをインストールしてください。

- Windows Server 2008 R2 SP1 / Windows 7 SP1
  - ✧ Support for TLS v1.2 included in the .NET Framework version 3.5.1
    https://support.microsoft.com/ja-jp/kb/3154518

- Windows Server 2012 / Windows 8
  - Support for TLS v1.2 included in the .NET Framework version 3.5

    https://support.microsoft.com/ja-jp/kb/3154519
- Windows Server 2012 R2 / Windows 8.1
  - Support for TLS v1.2 included in the .NET Framework version 3.5 SP1 on Windows 8.1 and Windows Server 2012 R2

    https://support.microsoft.com/ja-jp/kb/3154520

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/3g/

（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： tgMdk-java-3.x.x.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（tgMdk-x.x.x.jar, tgMdkDto.jar）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（cacerts）を削除して下さい。

④ アーカイブを解凍後、tgMdk/に含まれる新しい jar ファイル（tgMdk-3.x.x.jar, tgMdkDto.jar）をクラスパスに配置して下さい。

⑤ resources/ディレクトリ配下の新しい CA 証明書ストアファイル（cacerts）を、MDK 設定ファイルに記載のパスに配置して下さい。

⑥ lib/に含まれる必要な jar ファイルを、クラスパスに配置して下さい。
- lib/に含まれるファイルは以下のとおりです。
  - commons-codec-1.2.jar
  - json-simple-1.1.1.jar
  - log4j-1.2.17.jar
- 現在お使いの MDK バージョンが ver.2 系（2.x.x）の場合、lib/ディレクトリ配下のファイルが既にマーチャント様サイトのアプリケーションに配置されている場合は、再配置する必要はありません。
- 現在お使いの MDK バージョンが ver.1 系（1.x.x）の場合は、lib/ディレクトリ配下の json-simple-1.1.1.jar をクラスパスに追加して下さい。
- log4j ライブラリは ver1.2.17 を提供していますが、必ずしも更新する必要はありません。
- 既に使用しているライブラリと競合する場合は、MDK の該当ライブラリを除外し、動作をご確認下さい。

⑦ 「4.5 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： tgMdk-php-3.x.x.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古い MDK の tgMdk/Lib/ディレクトリ配下、および tgMdk/3GPSMDK.php 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（cert.pem）を削除して下さい。

④ アーカイブを解凍後、tgMdk/Lib/ディレクトリ配下、および tgMdk/3GPSMDK.php を参照先に配置して下さい。

⑤ resources/ディレクトリ配下の新しい CA 証明書ストアファイル（cert.pem）を、MDK 設定ファイルに記載のパスに配置して下さい。

⑥ 「4.5 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 アーカイブをご利用のシステム環境に応じてダウンロードして下さい。

- ファイル名： tgMdk-net-3.x.x.zip ※.NET Framework 4.5 以上
- ファイル名： tgMdk-net-2.x.x.zip ※.NET Framework 3.5 以上

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。
MDK インストーラーを利用して DLL を配置している場合は、設定ファイルの内容をバックアップした上でプログラムと機能から VeriTrans3G .NET MDK NE をアンインストールして下さい。
Global Assembly Cache(GAC)に MDK の DLL を配置している場合は、GAC から DLL をアンインストールして下さい。

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。

- log4net.dll
- Newtonsoft.Json.dll
- tgMdk.dll
- tgMdkDto.dll

④ 「4.5 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. Ruby 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： tgMdk-ruby-3.x.x.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古い MDK の lib/ディレクトリ配下を削除して下さい。

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（cert.pem）を削除して下さい。

④ アーカイブを解凍後、tgMdk/lib/ディレクトリ配下を参照先に配置して下さい。

⑤ resources/ディレクトリ配下の新しい CA 証明書ストアファイル（cert.pem）を、MDK 設定ファイルに記載のパスに配置して下さい。

⑥ 「4.5 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。

4.5. 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とおりです。

開発言語	MDK 設定ファイル名
Java	3GPSMDK.properties
PHP	3GPSMDK.properties
.NET	3GPSMDK.ini
Ruby	tg_mdk.ini

現在ご利用の MDK バージョンが 1 系(1.x.x)の場合、最新版 MDK では設定ファイルのフォーマットが変更されていますので、ご注意下さい。

4.5.1. Ver.2 系(2.x.x)からのバージョンアップの場合

(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://3g.veritrans.co.jp:443	https://api.veritrans.co.jp:443

- Java 版 MDK 設定ファイル[3GPSMDK.properties]での設定例

  HOST_URL = https://api.veritrans.co.jp:443

(2) (Java 版、Ruby 版のみ)SSL プロトコルの追加

MDK 設定ファイルにて、SSL 通信方式(SSL 通信プロトコル)の設定が必須となります。

<Java 版 追加>
SSL_PROTOCOL = TLSv1.2
<Ruby 版 追加>
SSL_PROTOCOL = TLSv1_2

(3) 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。

4.5.2. Ver.1 系(1.x.x)からのバージョンアップの場合

(1) 接続先 URL の変更

MDK 設定ファイルの接続先 URL が集約され下記の通り変更になります。

<変更前>
https://3g.veritrans.co.jp:443/tercerog/webinterface/GWPostNoSecurityCommandRcv https://3g.veritrans.co.jp:443/tercerog/webinterface/GWTripartiteCommandRcv https://3g.veritrans.co.jp:443/tercerog/webinterface/GWTripartiteSJISCommandRcv
<変更後>
https://api.veritrans.co.jp:443

- Java 版 MDK 設定ファイル[3GPSMDK.properties]での設定例

  HOST_URL = https://api.veritrans.co.jp:443

(2) (Java 版、Ruby 版のみ)SSL プロトコルの追加

MDK 設定ファイルにて、SSL 通信方式(SSL 通信プロトコル)の設定が必須となります。

<Java 版 追加>
SSL_PROTOCOL = TLSv1.2
<Ruby 版 追加>
SSL_PROTOCOL = TLSv1_2

(3) (PHP 版のみ)log4php 設定ファイルの変更

PHP 版において、MDK Ver1.x 系と MDK Ver.2 系以降では、同梱の log4php のバージョンが異なります。

このため、MDK Ver1.x 系を導入済みの環境に最新バージョンの MDK Ver.3 系をインストールする場合には、

log4php の設定ファイルを変更して頂きますようお願いします。

- Log4php のバージョンが v1.x から v2.3 に変更されました。
- Log4php v2.3 では、v1.x との設定ファイルの互換性がありません。
- MDK に同梱の log4php.properties では、次のような変更を行っています。

  (旧) log4php.appender.R1.layout=LoggerPatternLayout

  (新) log4php.appender.R1.layout=Logger**LayoutPattern**

  (旧) log4php.appender.R1.layout.ConversionPattern="%d %5p [%x] - %m%n"

  (新) log4php.appender.R1.layout.ConversionPattern="%d**{Y-m-d H:i:s,u}** %5p [%x] - %m%n"
- 詳細は、http://logging.apache.org/log4php/ をご参照下さい。

(4) （任意） 通信方式（通信プロトコル）の削除

MDK 設定ファイルにおける通信方式（通信プロトコル）の設定は不要となります。

設定を削除しなくても動作に支障はございませんので、ご対応は任意です。

<変更前>
PROTOCOL = POST_NO_SECURITY
<変更後>
（削除）

(5) 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、ご利用の全てのサービスの、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（DUMMY_REQUEST=0）での実行を推奨いたしますが、ダミーモード（DUMMY_REQUEST=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、コマンド（機能）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「VeriTrans3G 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。
  - ➢ 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。
  - ➢ 結果コード(VResultCode)の先頭が M で始まるエラー(MF02/MF03/MF04/MF99 etc.)が発生した場合は、SHA-2 環境との接続に失敗しています。
  - ➢ 接続に失敗した場合は、MDK の出力ログをご確認下さい。
    - ✧ 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

2015/10/20 ：Ver1.0 リリース

2015/10/23 ：Ver1.1 リリース

「4.1 Java 版をお使いの場合」に、CA 証明書ストアファイル（cacerts）の更新手順を追記。

「4.5 MDK 設定ファイルの変更」

Java 版、Ruby 版のみ、SSL 通信プロトコル（SSL_PROTOCOL）の設定を追加する手順を追記。

2015/11/04 ：Ver1.2 リリース

「3 システム環境要件」に、Java、PHP のシステム環境要件の推奨事項を追記。

2016/03/15 ：Ver1.3 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

2016/06/30 ：Ver1.4 リリース

「4.2 PHP 版をお使いの場合」に、3GPSMDK.php の更新手順を追記。

2016/07/11 ：Ver1.5 リリース

「3 システム環境要件」に、.NET Framework 3.5 対応版 MDK をご利用の際のシステム環境要件を追記。

「4.3 .NET 版をお使いの場合」に、.NET Framework 3.5 対応版 MDK のダウンロードに関する記載を追記。