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 カード Web プラン

システム対応ガイド

Ver. 1.1 （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 カード Web プランの新環境（以下、SHA-2 環境）に接続するためのシステム対応の手順および注意点について説明するものです。

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。
VeriTrans カード Web プラン開発ガイド	VeriTrans カード Web プランの 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://merchant.cybercash.co.jp/ https://sfw.cybercash.co.jp/ https://bs.veritrans.co.jp/
SHA-2 環境の URL	https://pay2g.veritrans.co.jp/

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 で設定している接続先情報を、SHA-2 環境の URL へ変更

（重要）

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、

SHA-2 環境へ切り替え対応後は、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。）

3. システム対応概要

MDK のバージョンおよび開発言語毎に、接続先変更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。

（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。

3.1. MDK の接続先設定変更

各バージョン・各言語の MDK 設定ファイル名と設定項目は以下の通りです。

「2. SHA-2 環境の変更点とシステム対応概要」をご参照のうえ、接続先の変更を行って下さい。

設定の際は、ドメイン以下のパス情報は変更を加えないようお願いいたします。

例） https://sfw.cybercash.co.jp/bsw/invoice → https://pay2g.veritrans.co.jp/bsw/invoice

Version	言語(※1)	設定ファイル名	設定項目
1.x	Perl	testdrv.cgi(※2)	invoice-uri
			payto-uri
	ASP	testdrv.asp(※2)	invoice-uri
			payto-uri
2.x	Perl/ASP	ccbsw.conf	INVOICE_URI
			PAYTO_URI
3.x	PHP	web.conf	INVOICE_URI
	Java	bswmdk.properties	invoice-url

※1 表に記載がないものにつきましては、ベリトランスまでお問い合わせ下さい。

※2 “testdrv.cgi”, “testdrv.asp”は MDK 付属のサンプルコードです。マーチャント様の環境に合わせて適宜読み替えて下さい。

3.2. HTML テンプレートの取得元 IP アドレス

SHA-2 環境へ切り替え対応後も、マーチャント様がご提供されている HTML テンプレートは、同じ IP アドレスから取得されます。マーチャント様環境にて HTML テンプレート取得元に対し、IP アドレスによりアクセス制御を行っている場合、切り替え対応後にアクセス制御設定の変更を行う必要はございません。

HTML テンプレート取得元情報	
SHA-2 環境 IP アドレス	210.239.44.144

4. 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。

4.1. 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。

4.2. 検証用取引の実行

- ➢ マーチャント様サーバ(ブラウザ)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	WP3753301099993
マーチャント認証鍵	edc88f911a6df91adcd663021179826f

※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(authonly)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」に記載されているカード番号以外のカード番号はご利用いただけません。実在するカード番号を利用した場合は、エラー（failure-bad-money）が返戻されます。
- ✓ 「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。

4.3. 検証結果の確認

- ベリトランス SHA-2 環境の接続先 URL が設定されていることをご確認下さい。
  - カード情報入力画面に遷移した際に、ブラウザのアドレスバーに表示されている URL が、ベリトランス SHA-2 環境のものであることをご確認下さい。
  - カード情報入力画面で表示される HTML フォームの送信先(action 属性)が、ベリトランス SHA-2 環境のものであることをご確認下さい。
- マーチャント様サイトの決済完了画面まで、正常に遷移することをご確認下さい。
  - 決済が失敗した場合は、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。
- マーチャント様が HTML テンプレートをご利用の場合、マーチャント様がご提供されている HTML テンプレートが、ベリトランスからインターネット経由で正常に取得されることをご確認下さい。
- マーチャント様システムの後続処理（決済完了後の処理）に支障がないことをご確認下さい。
- （本人認証機能ご利用のマーチャント様のみ）本人認証機能がご利用できることをご確認ください。
  - ※本人認証機能は本番用マーチャント ID・本番用カード番号でのみご利用いただけます。そのため、検証の際には、本番用マーチャント ID・本番用カード番号での検証をお願いいたします。

4.4. 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
  - HTML テンプレートの利用有無
  - 検証完了日時
  - 本番切替予定日

4.5. 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。

5. その他

5.1. 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

5.2. 改定履歴

2016/2/24 ：Ver1.0 リリース

2016/3/15 ：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