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～

口座振替サービス システム対応ガイド

Ver. 1.0 （2016 年 5 月～）

目次

1. はじめに

本ガイドは、SHA-256 証明書に対応した口座振替サービスの新環境（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、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。

なお、引き続きサービスをご利用いただくために、SHA-2 暫定環境（以下、暫定環境）に接続することも可能です。
ただし、暫定環境は 2018 年 5 月に停止を予定していますので、停止日までには必ず 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。

【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。
VeriTrans3GPlus 口座振替サービス 開発ガイド	VeriTrans3GPlus 口座振替サービス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/atp
SHA-2 環境の URL	https://**api**.veritrans.co.jp/atp

ベリトランス 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 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）

TLS1.1 以上に対応していない場合、SSL3.0 および TLS1.0 を有効化した暫定環境を利用することができます。

アクセス URL	
既存環境の URL	https://3g.veritrans.co.jp/atp
暫定環境の URL	https://**3gs**.veritrans.co.jp/atp

ベリトランス暫定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。

- ✓ 暫定環境 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）

ただし、暫定環境は 2018 年 5 月に停止を予定していますので、停止日までには必ず SHA-2 環境（api.veritrans.co.jp）に遷移させるよう、変更して頂く必要があります。

3. Web 口座振替登録をご利用の場合

3.1. TLS1.1 非対応端末（フィーチャーフォン等）への対応

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、SSL3.0 および TLS1.0 の通信を無効化した SHA-2 環境への切り替え対応後は、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 Web 口座振替登録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。

なお、引き続きフィーチャーフォンを利用した口座振替サービスを有効にするために、消費者のブラウザを、暫定環境に遷移させることも可能です。

アクセス URL	
暫定環境の URL	https://**3gs**.veritrans.co.jp/atp

ただし、暫定環境は 2018 年 5 月に停止を予定していますので、停止日までには必ず SHA-2 環境（api.veritrans.co.jp）に遷移させるよう、変更して頂く必要があります。

4. API クライアントをご利用の場合

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。

接続先環境	システム環境要件
既存環境	Java**6** 以上
SHA-2 環境	Java**7** 以上（Java8 以上を推奨）
暫定環境	Java**6** 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。

現在お使いの API クライアントをバージョンアップし、ベリトランス SHA-2 環境もしくは暫定環境に接続するための対応を行ってください。

（重要）

API クライアントのバージョンアップおよび設定ファイルの変更を行う際には、必ず現在お使いの API クライアント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。

① lib/に含まれる jar ファイルのバージョンをご確認下さい。
- atrs-client-x.x.x.jar
  - 2.0.0 以上をご利用下さい。
- atrs-common-x.x.x.jar
  - 1.0.27 以上をご利用ください。

② jar ファイルのバージョンが要件を満たさない場合、別紙「VeriTrans3GPlus 口座振替サービス 開発ガイド」をご参照のうえ、最新バージョンの API クライアントをインストールしてください。

③ 設定ファイルを変更してベリトランス SHA-2 環境もしくは暫定環境に接続するための対応を行ってください。

4.1. API ホスト名の変更

設定ファイル[AtrsHttpsClientConfigure.conf」の API ホスト名を変更してください。

4.1.1. SHA-2 環境にご接続の場合

- API_HOST_NAME=**api**.veritrans.co.jp

4.1.2. 暫定環境にご接続の場合

- API_HOST_NAME=**3gs**.veritrans.co.jp

ただし、暫定環境は 2018 年 5 月に停止を予定していますので、停止日までには必ず SHA-2 環境（api.veritrans.co.jp）に遷移させるよう、変更して頂く必要があります。

4.2. SSL プロトコルの変更

ベリトランス暫定環境に TLS1.0 で接続する場合は、明示的に TLS1 を指定する必要があります。

設定ファイル[AtrsHttpsClientConfigure.conf」の SSL プロトコルを変更してください。

- SSL_PROTOCOL=TLSv1

ベリトランス SHA-2 環境に接続する場合は、SSL プロトコルの設定変更は不要です。

5. 接続検証の手順

ご利用のすべてのサービスについて、ベリトランス SHA-2 環境もしくは暫定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

- ✓ マーチャント様のサイトから検証用の口座振替登録を実行し、ベリトランス SHA-2 環境もしくは暫定環境との通信が正常に行われることをご確認ください。
- ✓ API クライアントをご利用の場合、原則としてすべての API 呼び出しの確認をお願いいたします。
- ✓ 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 を推奨しております。
  - ➢ 本番用マーチャント ID での検証が難しく、かつテスト用のマーチャント ID をお持ちの場合は、テスト用のマーチャント ID をご利用ください。

5.3. 検証結果の確認

- ✓ 取引要求が、ベリトランスの SHA-2 環境もしくは暫定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 環境もしくは暫定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。
- ✓ 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。

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
  - 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

2016/5 ：Ver1.0 リリース