ベリトランスサービスをご利用のマーチャント各位

Confidential
1.1版

2015-2016 ベリトランス決済サービスセキュリティ強化対応
【付録】PHPをご利用の際の注意点

2016/04/12

ベリトランス株式会社

PHP＋OpenSSLをご利用の際のシステム環境要件

ベリトランスのサービスにPHP＋OpenSSLを利用してSSL接続している場合、ベリトランスの新環境（新URL）に接続するためには、以下の環境要件を満たしていただく必要がございます。

OS・言語環境	環境要件
PHPをご利用の場合	OpenSSL 1.0.1以上をサポートするPHP環境 （TLS1.1以上で通信可能な環境）

ベリトランスの新環境では、SSL3.0/TLS1.0の通信を無効化します。そのため、マーチャント様の環境からは、TLS1.1以上（TLS1.1またはTLS1.2）のプロトコルでの通信が可能でなければなりません。

- OpenSSLの脆弱性は、1.0.1以上のバージョンでも報告されています。マーチャント様のシステムをアップグレードする際には、最新バージョンをお使い頂きますようお願いいたします。

注）
ただし、OpenSSLを利用せずにSSL接続を行うケースや、SSL通信モジュールをMDK内部に包含している一部のベリトランスサービスでは、OpenSSLのバージョン要件は適用されません。
詳細につきましては、次のスライドをご確認ください。

サービス毎のSSL接続方式について

◇ VeriTrans3G関連サービスの場合

サービス名	SSL接続の方式
VeriTrans3G - MDK（モジュール型）-	PHP版MDKをご利用の場合は、PHP＋OpenSSLの形態でSSL接続を行いますので、OpenSSLのバージョン要件を満たす必要があります。 注）MDK-less方式（MDKを利用しない）でVeriTrans3Gとの通信を実装しているマーチャント様におかれましては、実装方法によって対応が異なります。OpenSSLをご利用の場合は、OpenSSLのバージョン要件を満たす必要があります。
VeriTrans3G - 3G-Direct（JavaScript(API)型）-	ベリトランスが提供しているAPIライブラリをご利用の場合は、PHP＋cURL(curl)によるSSL接続を行っていますので、cURLが利用しているSSLのバージョンを確認する必要があります。詳細は3G-Directのシステム対応ガイド（10月中旬以降に公開予定）をご確認ください。 APIライブラリを利用していない場合は、マーチャント様の実装方法によって対応が異なります。OpenSSLをご利用の場合は、OpenSSLのバージョン要件を満たす必要があります。

◇ 上記以外の場合

サービス名	SSL接続の方式
クレジットカード決済 FLEXプラン	MDKをご利用の場合、OSによって対応が異なります。 ダイナミックリンク方式でOpenSSLライブラリを動的にリンクするケースでは、OSにインストールされたOpenSSLのバージョンが、要件を満たす必要があります。 スタティックリンク方式でOpenSSLライブラリを静的にリンクするケースでは、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す。 詳細は、各サービスのシステム対応ガイド（10月中旬以降に公開予定）をご参照ください。
コンビニ・ペイジー決済	
MPIホスティング（3D-Secure）	
電子マネー決済	PHP版MDKをご利用の場合は、PHP＋OpenSSLの形態でSSL接続を行いますので、OpenSSLのバージョン要件を満たす必要があります。

OpenSSLのバージョン確認方法

以下の手順で、ご利用のOpenSSLのバージョンをご確認ください。

1. ご利用のPHP環境でサポートされているOpenSSLのバージョンを確認する

```
$ php -i | grep OpenSSL
OpenSSL support => enabled
OpenSSL Library Version => OpenSSL 1.0.2d 9 Jul 2015
OpenSSL Header Version => OpenSSL 1.0.2d 9 Jul 2015
OpenSSL support => enabled
```

2. システム（OS）にインストールされているOpenSSLのバージョンを確認する

```
$ openssl version
OpenSSL 1.0.2d 9 Jul 2015
```

注）
PHP＋OpenSSLでSSL接続を行っているシステムにおいて、このコマンドの表示がPHPでサポートしているバージョンと異なる場合は、コマンドラインから実行したopensslは、PHPがサポートしているものではありません。（この状況は、複数のOpenSSLバージョンがインストールされている場合に起こります。）

本件に関するお問い合わせ

本件に関するお問い合わせ窓口：

ベリトランス株式会社 SSL-SHA2切替窓口メールアドレス

ssl-sha2@veritrans.jp

※お電話によるお問い合わせは受け付けておりません

- お問い合わせの際は、ご契約中のサービス名（VeriTrans3G, クレジットカード決済FLEXプラン等）とマーチャントIDを合わせてご連絡いただけると幸いです。
- ご契約中のサービスなどがご不明な場合はその旨をご連絡ください。

各種ドキュメントへのリンク：

本書ならびにサービス毎のシステム対応ガイドはこちら

https://www.veritrans.co.jp/support/sha256/

MDKおよび開発ドキュメントはこちら（10月中旬よりダウンロード公開を開始予定）

https://www.veritrans.co.jp/support/trial/login.html

変更履歴

No.	日付	変更内容	変更者
1	2015/10/08	1.0版（初版）公開	ベリトランス技術部
2	2016/04/12	1.1版作成	ベリトランス技術部