ベリトランスサービスをご利用のマーチャント各位

Confidential
1.5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

SHA-256証明書対応および、SSL3.0/TLS1.0の廃止に伴う
システム対応のお願い

2016/05/20

ベリトランス株式会社

１．はじめに

多くの企業・団体よりSHA-1証明書の廃止計画が発表されておりますが、ベリトランスが提供するサービスにつきましても、SHA-1証明書を廃止するために、SHA-256証明書に対応した新環境の公開を開始いたしましたので、マーチャント様のシステムにおける接続先切替等のご対応をお願い申し上げます。

なお、**SHA-2（SHA-256）証明書を利用したSSL通信に未対応のシステムをお使いのマーチャント様におかれましては、ベリトランス新環境には接続できません**ので、接続を可能とするためのシステム対応を行って頂く必要がございます。

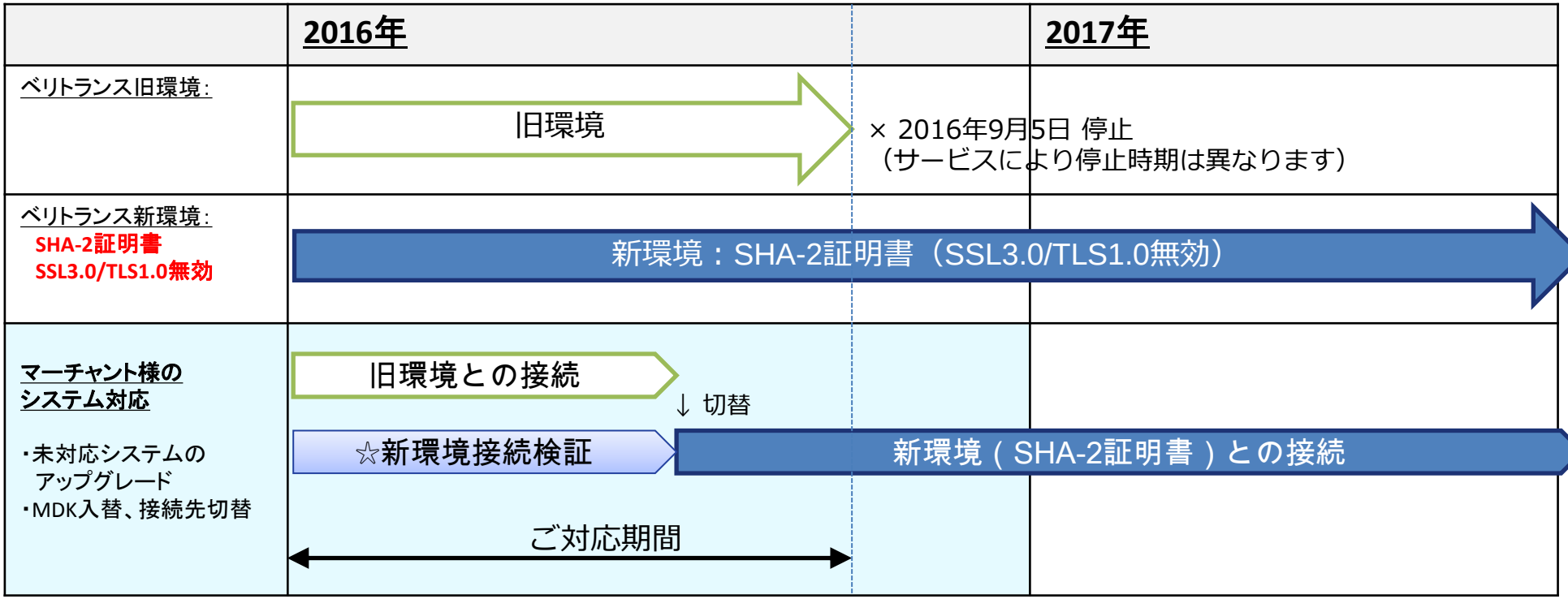
また、ベリトランスでは、**SSLの暗号化方式において脆弱性が多数報告されているSSL3.0およびTLS1.0につきましても、ご利用を停止させていただきます。**

マーチャント様には、大変ご面倒をおかけいたしますが、安全な決済サービスを維持するため、本書の内容をご確認いただき、ご利用のサービス毎に必要となるシステム対応を行って頂きますようお願いいたします。

ご理解、ご協力のほど何卒よろしくお願い申し上げます。

2．システム対応のマイルストーン

ベリトランスでは、SHA-2証明書対応（SSL3.0/TLS1.0無効）の新環境（新URL）を公開していますので、マーチャント様のご都合のよいタイミングで新環境を利用した接続検証と、新環境への本番接続切替を行って頂きますようお願いします。



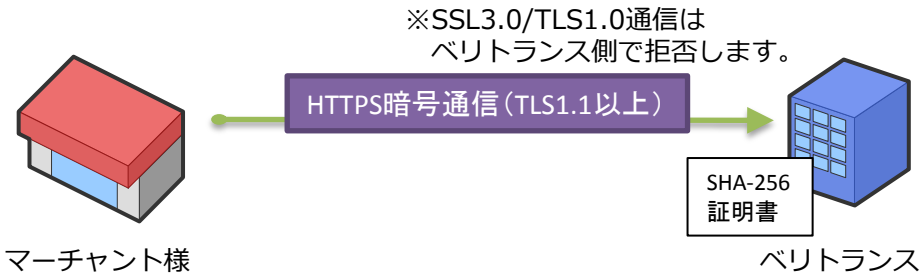
※ベリトランスでは、各方面からのSHA-1脆弱性に関する報告や、暗号化に関する国際専門家チームの勧告を受け、旧環境（SHA-1）の停止時期の前倒しを決定しました。マーチャント様には大変ご面倒をおかけいたしますが、2016年9月5日までに接続検証～切替実施をお願い申し上げます。

◇SHA-1脆弱性を突いた攻撃が早期に現実化される可能性が高まっており、Google社、Microsoft社、Mozilla(Firefox) は、SHA-1証明書のサポート期限前倒しを決定または検討しています。

https://googleonlinesecurity.blogspot.jp/2015/12/an-update-on-sha-1-certificates-in.html
http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-authenticode-code-signing-and-timestamping.aspx
https://blog.mozilla.org/security/2015/10/20/continuing-to-phase-out-sha-1-certificates/

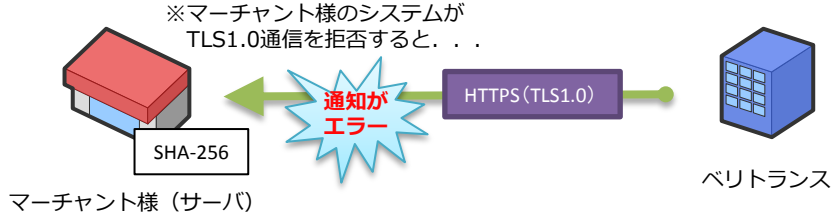
3．システム対応のポイント

- **マーチャント様システム⇒ベリトランスの新環境（SHA-256証明書、SSL3.0/TLS1.0通信無効化）の向きの通信が正常に行えることが必須となります。通信ができない場合はシステムのアップグレードや、MDKのバージョンアップを行って頂く必要があります。**



- **本書は、<u>ベリトランス側</u>サーバ証明書のSHA-256対応／TLS1.1対応についてのご説明を主としています。<u>マーチャント様サーバ側</u>のSHA-256証明書導入に関しましては、本書では詳細を説明しておりません。マーチャント様サーバ側のセキュリティ強化対策を実施される場合は、本書の内容とは別に、ベリトランスからの入金通知等の通信（インバウンド）が受信できるかどうかのご確認を行って頂く必要がございますので、別途ご相談下さい。**

（重要）
ベリトランスからの入金通知や決済結果通知（PUSH通知）は、現在TLS1.0を利用して通信しています。そのため、マーチャント様のシステムでTLS1.0のインバウンド通信を拒否する設定がなされますと、ベリトランスからの通信がすべてエラーとなってしまいます。
この問題への対応といたしましては、2016年夏頃を目途にベリトランス側の通知システムのTLS1.1対応を進めて参りますが、詳細は本書とは別のご案内とさせて頂きます。
（ご案内の際には、弊社の通知システムからの通知を正常に受信できるかどうかのテストにご協力頂くことを検討しております。）



1. マーチャント様システム環境のアップグレード要否のご確認とご対応

- 弊社サービスにAPI接続しているシステムが、TLS1.1以上のプロトコルで接続するための要件を満たしていない場合、システムのアップグレードが必要です。

OS・言語環境	環境要件
PHPをご利用の場合	OpenSSL 1.0.1以上*1をサポートするPHP環境
Javaをご利用の場合	Java7以上（Java8を推奨）
.NETをご利用の場合	Windows Server 2008 R2以上、Windows7以上 .NET Framework 4.5 以上
上記以外でUNIX（LINUX）環境をご利用の場合	OpenSSL 1.0.1 以上*1の導入および OpenSSL 1.0.1 以上を利用可能な言語環境

✓ 一部のサービスについては、環境要件が異なる場合がございますので、詳細はサービス毎のシステム対応ガイドをご確認いただきますようお願いします。

*1 ベリトランスにて動作確認を行ったバージョンです。
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いたします。

2. ベリトランス新環境（SHA-2証明書対応の新URL）への接続先変更

- ベリトランス新環境との接続試験を実施して頂き、マーチャント様の本番環境をベリトランス新環境に接続するように設定を変更して頂く必要があります。

- MDKをご利用のサービスでは、原則としてMDKのバージョンアップが必要となります。詳細はサービス毎のシステム対応ガイドをご確認ください。

3. 未対応端末をご利用のエンド・ユーザ様へのご案内

- 3D-Secureやキャリア決済など、決済フローに消費者ブラウザを介する場合（3者間の決済フロー）、SHA-2証明書に未対応の端末(2008年以前のフィーチャーフォンなど)をご利用のエンド・ユーザ様(購買者)は決済を続けることが出来ませんので、マーチャント様のWebサイトでのご連絡等をご検討ください。

- ベリトランス新環境への接続切替前に、マーチャント様サイトや3者間の決済フローが必要な決済事業者（例：キャリア決済ではdocomo/KDDI/softbank等の通信事業者システム）がSHA-2証明書に変更された場合は、その時点で未対応端末からの決済は行えなくなります。

4. ベリトランスからのPUSH通知電文受信テスト（PUSH通知をご利用の場合）

- システム環境要件を満たすために、マーチャント様システムのアップグレード（サーバリプレース等）を実施される場合は、ベリトランスからのPUSH通知電文を正常に受信できることをご確認いただきますようお願いいたします。

サービス名	テスト方法
3G コンビニ/電子マネー/銀行決済/PayPal/UPOP/Alipay/ ショッピングクレジット 従来サービス コンビニ･ペイジー/電子マネー	通知先URLをマーチャント様の検証環境に向けて設定するために、テスト用のマーチャントIDの貸出をさせて頂きます。 ※ SHA-2切替窓口までお問い合わせください。
3G 本人認証/キャリア決済/楽天ID決済/LINEPay/ リクルートかんたん支払い	ダミー決済時、MDKのリクエストパラメータに通知URLを指定可能です。 マーチャント様の検証環境のURLをご指定いただくことで、ベリトランスからの通知の受信が可能です。
上記以外のサービス	※ 現在、テスト方法を検討中です。 SHA-2切替窓口までお問い合わせください。

（補足）

ベリトランス側の通知システムのTLS1.1対応は別途検討中ですが、これを実施の際にも、弊社の通知システムからの通知を正常に受信できるかどうかのテストにご協力頂く方向で検討しております。
今回システムのアップグレードを実施して頂くマーチャント様にも、再度のご確認をお願いすることになりますが、できるだけマーチャント様のご負担とならないような確認方法をご案内させていただきますので、その際にはご協力を賜りますよう、お願い申し上げます。

5-1．サービス毎のご対応内容一覧（VeriTrans3G/3G+）

サービス名	マーチャント様に実施頂きたい システム対応の概要	システム対応ガイド （ドキュメント）公開状況
VeriTrans3G - MDK（モジュール型）-	最新版MDK（version 3.x.x）へのバージョンアップと、対応システムへのアップグレードをお願いいたします。 ベリトランス新環境（SHA-2環境）との接続試験を行って頂き、マーチャント様本番環境の接続先を、新環境のURLに変更して頂く必要があります。 また、システムのアップグレードを実施される際には、アップグレード後のシステムで、ベリトランスからの通知が受信できることをご確認下さい。	公開中
VeriTrans3G - 3G-Web（Webリンク型）-	対応システムへのアップグレードをお願いいたします。 ベリトランス新環境（SHA-2環境）の公開は2016/4/11（月）を予定しています。公開日以降に接続試験を行っていただき、マーチャント様本番環境の接続先を、新環境のURLに変更して頂く必要があります。	公開中
VeriTrans3G - 3G-Direct（JavaScript(API)型）-	対応システムへのアップグレードをお願いいたします。 ベリトランス新環境（SHA-2環境）との接続試験を行っていただき、マーチャント様本番環境の接続先を、新環境のURLに変更して頂く必要があります。	公開中
IVR決済ソリューション	VeriTrans3G クレジットカード決済との接続部につきましては、弊社にて対応を実施しますので、対応不要です。 決済情報連携APIをご利用のマーチャント様は、検証環境との接続テストの実施をお願いいたします。	公開中
口座振替サービス	対応方針を近日中にご案内差し上げます。	2016年5月公開予定
BPSサービス	BPSサービスとの接続部につきましては、ご対応は不要です。	ー

- ご利用のサービス名がご不明の際は、以下の連絡先までお問い合わせください。
  SSL-SHA2切替窓口　mail: ssl-sha2@veritrans.jp
- システム対応ガイドの公開時には別途ご連絡差し上げます。

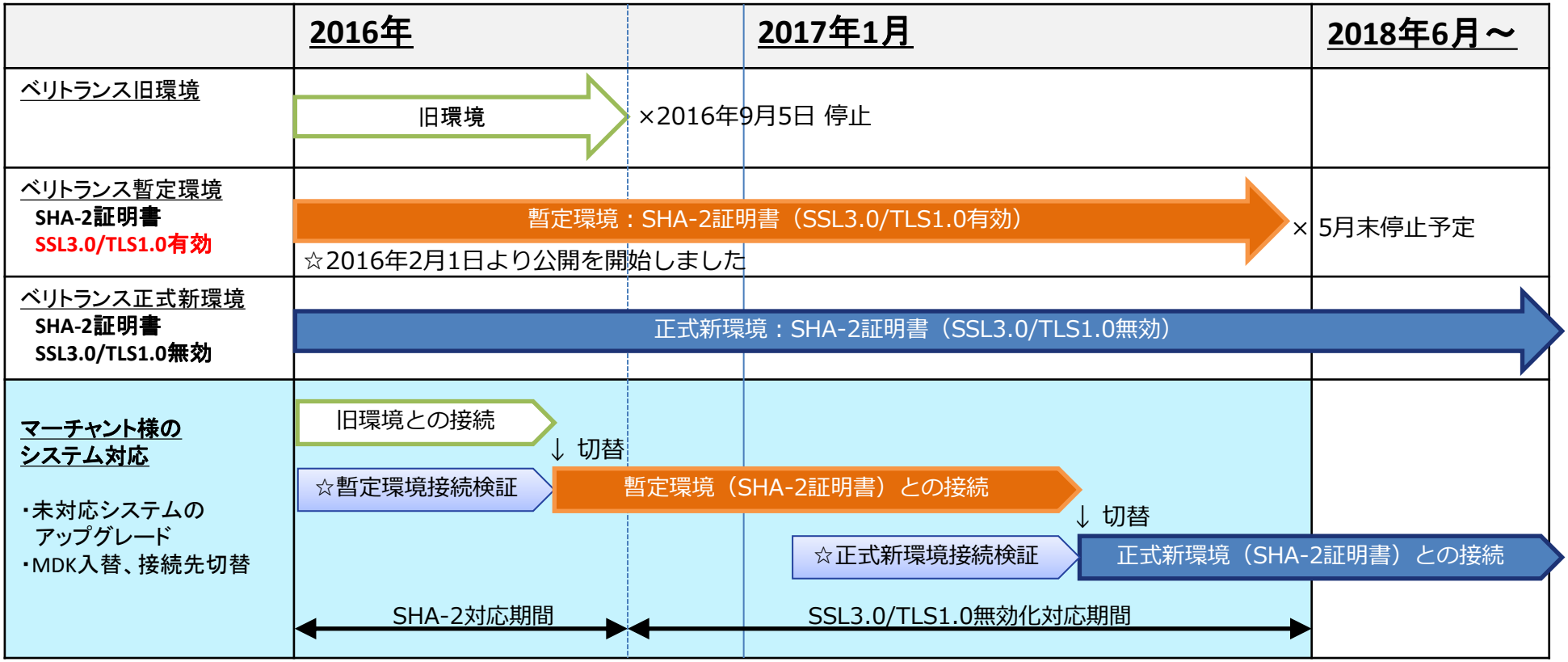
5-2．サービス毎のご対応内容一覧（VeriTrans3G/3G＋以外）

サービス名	マーチャント様に実施頂きたい システム対応の概要	システム対応ガイド （ドキュメント）公開状況
クレジットカード決済 FLEXプラン	PHP版/Java版/.NET版/Perl版のMDKをご利用の場合 現在公開中の最新版MDKへのバージョンアップと、 対応システムへのアップグレードをお願いいたします。 ベリトランス新環境（SHA-2環境）との接続試験を行って頂き マーチャント様本番環境の接続先を、新環境のURLに変更して頂く 必要があります。また、システムのアップグレードを実施される際に は、アップグレード後のシステムで、ベリトランスからの通知を受信できることをご確認下さい。 上記以外の場合： SSL-SHA2切替窓口までご相談下さい。	公開中
コンビニ・ペイジー決済		公開中
電子マネー決済		公開中
MPIホスティング（3D-Secure）		公開中
クレジットカード決済 WEBプラン	現在弊社にて対応方針を検討中です。 対応方針が決まり次第、別途ご案内させて頂きます。	公開中
クレジットカード決済 MEGAプラン	マーチャント様システムのご対応は不要です。 （管理画面のURLのみ変更となります。）	－
各サービスの管理画面 （WEBアプリケーション）	ブラウザでアクセスするURL（ブックマーク等）の変更を行って頂く必要がございます。 別途、2016年4月以降に、弊社のカスタマーサポートよりご案内差し上げます。	－

- ご利用のサービス名がご不明の際は、以下の連絡先までお問い合わせください。
  SSL-SHA2切替窓口　mail: ssl-sha2@veritrans.jp
- システム対応ガイドの公開時には別途ご連絡差し上げます。

6-1．（VeriTrans3G）TLS1.1以上の対応が困難な場合の暫定対応

VeriTrans3G(MDK型および3G-Direct)をご利用で、TLS1.1以上への移行対応がスケジュール面で困難なマーチャント様のために、暫定環境としてSSL3.0/TLS1.0 を有効にしたSHA-2証明書環境をご用意いたしました。この環境は、2018年5月末までの公開を予定していますので、この環境を利用した移行プランをご検討頂きますようお願いします。



※ベリトランスでは、各方面からのSHA-1脆弱性に関する報告や、暗号化に関する国際専門家チームの勧告を受け、旧環境（SHA-1）の停止時期の前倒しを決定しました。暫定環境への移行は2016年9月5日までに行って頂きますようお願いします。

※暫定環境の停止は、現時点では2018年5月末を予定していますが、できるだけ早めに正式新環境への切り替えをお願いいたします。

6-2. （VeriTrans3G）暫定環境のご利用方法

SHA-256証明書に対応した「暫定環境」のご利用方法を以下にご説明します。

1. 接続先URLのホスト名を、暫定環境のホスト名に変更してください。

修正前のホスト名（旧環境）	修正後のホスト名（暫定環境）
3g.veritrans.co.jp	3gs.veritrans.co.jp

2. CA証明書ストアファイルの更新 （対象：MDKをご利用のマーチャント様 ※.NET版を除く）

– MDK設定ファイルに設定されたパスに配置されているCA証明書ストアファイルを、最新のMDK（Version3.x.x）に同梱の新しいファイルに差し替えてください。
ファイル名を下表に示します。

ご使用の開発言語（MDK）	CA証明書ストアファイル名
PHP/Ruby版	cert.pem
Java版	cacerts
.NET版	この対応は不要です。

※その他、MDK設定の詳細につきましては、MDKインストールガイドをご参照ください。
※ご利用のシステムがSHA-256証明書を利用したサーバとの通信に未対応の場合は、暫定環境のご利用はできません。

7．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

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

変更履歴

版	日付	変更内容	変更者
1.0	2015/09/28	1.0版（初版）公開	ベリトランス技術部
1.1	2015/10/05	スライド「４．マーチャント様システムのご対応概要」の以下の修正 ・「PHPをご利用の場合」「上記以外でUNIX（LINUX）環境をご利用の場合」の環境要件に、「TLS1.1以上で通信可能な環境」という記載を追加し、注釈*1を追加。 ・「.NETをご利用の場合」の環境要件の「Windows7」を「Windows7以上」に修正	ベリトランス技術部
1.2	2015/11/04	スライド「４．マーチャント様システムのご対応概要 （その３）」を追加。 スライド「５．サービス毎のご対応内容一覧 」に、ベリトランスからの通知受信テストを行って頂く旨を追記。 スライド「５．サービス毎のご対応内容一覧 」のMDKリリース状況と、システム対応ガイドの公開状況を更新（3G/3G-DirectおよびFLEX/MPI/コンビニ/電子マネー）	ベリトランス技術部
1.3	2016/02/01	スライド「１．はじめに」の記載内容見直し スライド「２．システム対応のマイルストーン」を2016年以降のスケジュールに更新 スライド「６-１．（VeriTrans3G）TLS1.1以上への対応が困難な場合の暫定対応」を追加 スライド「６-２．（VeriTrans3G）暫定環境のご利用方法」を追加	ベリトランス技術部
1.4	2016/03/15	スライド「４-１．マーチャント様システムのご対応概要 （その１）」の記載内容見直し 旧環境の停止時期の前倒し（2016年9月5日）が決定したため、関連する記載を修正	ベリトランス技術部
1.5	2016/05/20	スライド「５．サービス毎のご対応内容一覧 」のIVRに関する記載を修正 スライド「4-3 マーチャント様システムのご対応概要 （その３）」のベリトランス通知システムのTLS1.1対応に関する補足から実施時期（2016年夏頃）の説明を削除	ベリトランス技術部