OricoPayment Plusをご利用の加盟店各位

Confidential
1.2版

2015-2016 OricoPayment Plus 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

2017/08/01

株式会社オリエントコーポレーション

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、OricoPayment Plus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（以下、SHA-2と記載）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、加盟店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加盟店様におかれましては、OricoPayment Plus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。

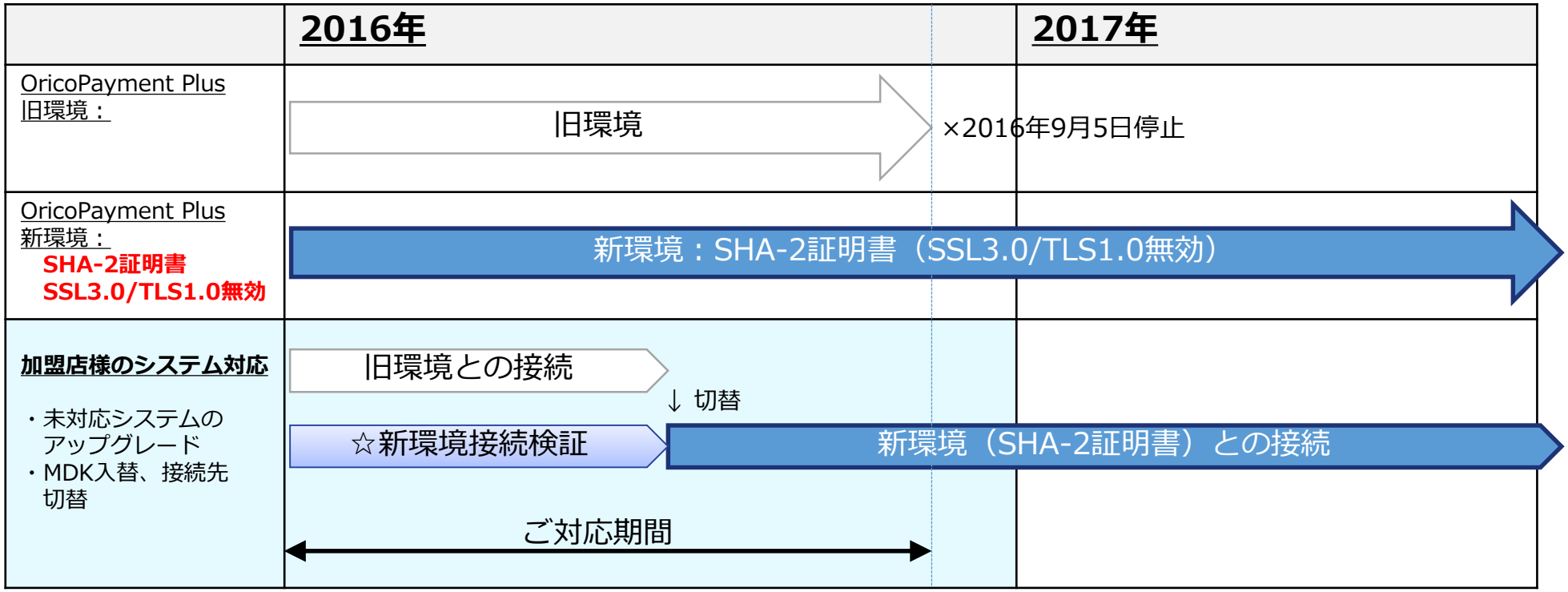
また、OricoPayment Plusでは、**SSLの暗号化方式において脆弱性が多数報告されているSSL3.0およびTLS1.0につきましても、ご利用を停止させていただきます。**

加盟店様には、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

OricoPayment Plus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、加盟店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。



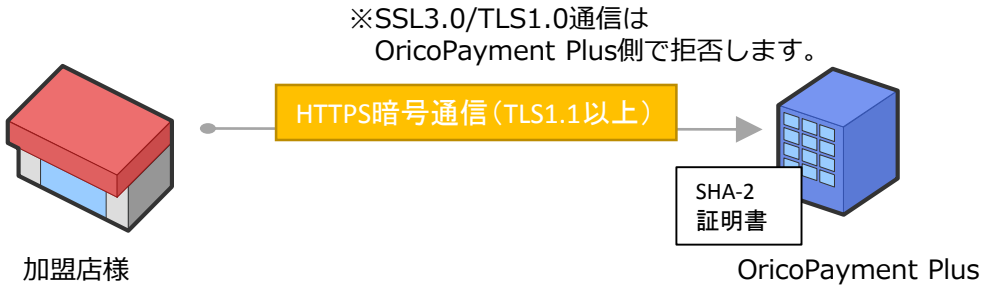
※OricoPayment Plusでは、各方面からのSHA-1脆弱性に関する報告や、暗号化に関する国際専門家チームの勧告を受け、旧環境（SHA-1）の停止時期の前倒しを決定しました。加盟店様には大変ご面倒をおかけいたしますが、2016年9月5日までに接続検証～切替実施をお願い申し上げます。

◇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

- **加盟店様システム⇒OricoPayment Plusの新環境（SHA-2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>OricoPayment Plus側</u>サーバ証明書のSHA-2対応／TLS1.1対応についてのご説明を主としています。<u>加盟店様サーバ側</u>のSHA-2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。加盟店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、 OricoPayment Plus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）
OricoPayment Plus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、加盟店様のシステムで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、OricoPayment Plusからの通信がすべてエラーとなってしまいます。
OricoPayment Plus側の通知システムのTLS1.1対応につきましては、現在スケジュールを検討中ですが、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。）

４-１．加盟店様システムのご対応概要 （その１）

1. 加盟店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 1.0.1i以上をサポートするPHP環境 （TLS1.1以上で通信可能な環境）*1
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 3.5 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
OricoPayment Plusにて動作環境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。

４-２．加盟店様システムのご対応概要 （その２）

2. OricoPayment Plus新環境（SHA-2証明書対応の新URL）への接続先変更

- OricoPayment Plus新環境との接続試験を実施して頂き、加盟店様の本番環境をOricoPayment Plus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。

- OricoPayment Plus Standard MDK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（三者間の決済フロー）、SHA-2証明書に未対応の端末(2008年以前のフューチャーフォンなど)をご利用のエンド・ユーザ(購買者)様は決済を続けることが出来ませんので、加盟店様のWebサイトでのご連絡等をご検討ください。

- OricoPayment Plus新環境への接続切替前に、加盟店様サイトや三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。

４-３．加盟店様システムのご対応概要 （その３）

4. OricoPayment Plus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、加盟店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、OricoPayment Plus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
OricoPayment Plus コンビニ/電子マネー/銀行決済/PayPal/ネット銀聯/Alipay/ショッピングクレジット	通知先URLを加盟店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。
OricoPayment Plus 本人認証/キャリア決済	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。加盟店様の検証環境のURLをご指定いただくことで、OricoPayment Plusからの通知の受信が可能です。

（補足）

OricoPayment Plus側の通知システムのTLS1.1対応は、現在スケジュールを検討中です。この対応を実施する際には、今回システムのアップグレードを実施頂く加盟店様にも、再度のご確認をお願いすることになりますが、できる限り加盟店様のご負担とならないような確認方法をご案内させて頂きますので、その際はご協力を賜りますよう、お願い申し上げます。

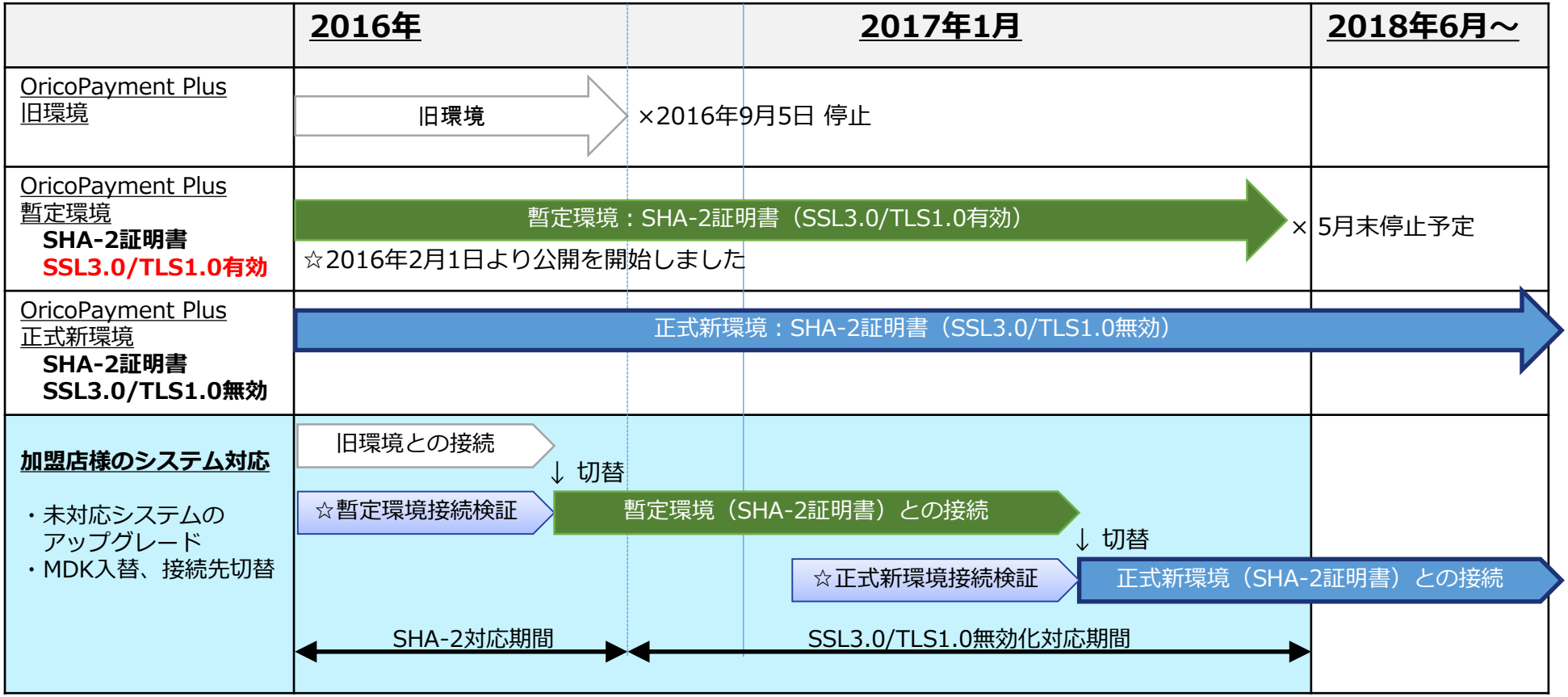
5．サービス毎のご対応内容一覧 (OricoPayment Plus)

サービス名	加盟店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
OricoPayment Plus - Standard MDK （モジュール型）-	最新版MDK（version 3.0.0）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。 OricoPayment Plus新環境（SHA-2環境）との接続試験を行って頂き、加盟店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、OricoPayment Plusからの通知が受信できることをご確認下さい。	公開中
OricoPayment Plus - Simple 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。 OricoPayment Plus新環境（SHA-2環境）との接続試験を行って頂き、加盟店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
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。 2016年5月10日付で弊社カスタマーサポートよりご案内差し上げた「MAP（管理画面）セキュリティ強化及び機能改善のご案内とご対応依頼」をご確認ください。	–

- 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．TLS1.1以上の対応が困難な場合の暫定対応

OricoPayment Plus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加盟店様向けに、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。



※ OricoPayment Plus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．暫定環境のご利用方法

SHA-2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： Standard MDKをご利用の加盟店様 ※.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メインパッケージ 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-2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：

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（OricoPayment Plus Standard MDK または Simple Web）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、サービス毎のシステム対応ガイド、MDK、および開発ドキュメントはこちら

http://www.orico.co.jp/partner/online/paymentplus/support/login/index.html

変更履歴

版	日付	変更内容	変更者
1.0	2016/03/01	1.0版（初版）公開	OricoPayment Plus
1.1	2016/06/01	1.1版公開 「3.システム対応のポイント」の（重要）欄の記載を修正 「5.サービス毎のご対応内容一覧」の管理画面欄の記載を修正	OricoPayment Plus
1.2	2017/08/07	1.2版公開 「４-１．加盟店様システムのご対応概要 （その１）」の「.NET」環境要件を修正	OricoPayment Plus