

OricoPayment Plusをご利用の加盟店様各位

**Confidential**  
**1.0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【補足資料】

2017/08/01

株式会社オリエントコーポレーション

# 目次

- 加盟店様へのご依頼事項
- 背景
- SSL（Secure Socket Layer）とは？
- SSLにおけるセキュリティ問題
- 各脆弱性に対する業界の動き
- 各脆弱性の対応におけるハードル
- OricoPayment Plusの対応について
- 加盟店様サイトの脆弱性対応における考慮点
- まとめ
- 本件に関するお問い合わせ

# 加盟店様へのご依頼事項

## **【ご依頼事項】 SSL-SHA2形式、TLS1.1以降への対応**

OricoPayment Plusが提供しているサービスごとにシステム対応ガイドをご用意いたします。  
ご契約中のサービスの資料をご参照の上、ご対応くださいますようお願いいたします。  
ご対応いただきたい内容は以下の3点となります。

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
2. OricoPayment Plus新環境（SHA-2証明書対応の新URL）への接続先変更
3. 未対応端末をご利用のエンド・ユーザ様へのご案内

※後述の「OricoPayment Plusの対応について」および

別紙「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」をご参照ください

注）上記は、OricoPayment Plusにおけるセキュリティ強化（脆弱性対応）へのご対応内容となります。

加盟店様サイトの脆弱性対応を実施される場合には、以下の点にご注意ください。

## **【重要】 加盟店様サイトのSSL3.0/TLS1.0の停止について**

2016年1月現在、コンビニ決済や銀行/ペイジー決済における入金通知やキャリア決済の決済申込完了通知など、OricoPayment Plusより加盟店様のシステムに送信している各種通知の多くが**TLS1.1以上の暗号化強度の通信に対応していません**。

そのため、加盟店様システム（入金通知先として指定しているURL）へのアクセスに対するTLS1.0の通信（インバウンド）が停止されると、加盟店様システムにて入金通知が受信できなくなってしまう。

※ 後述の「加盟店様サイトの脆弱性対応における考慮点」をご参照ください

# 背景

## SSL-SHA1の販売停止

国際SSL発行協会の方針により**2016年末**を最後にSSL証明書が現在のSHA1形式(鍵長1024bit)から、SHA2(SHA256)形式(鍵長2048bit)への移行が強制的に行われます。サーバ証明書大手では販売されなくなるため、SHA1形式のSSL証明書自体が入手できなくなります。OricoPayment Plusで利用しているSSL証明書もSHA2形式の証明書に移行いたします。

## SSL3.0/TLS1.0の重大な脆弱性の発表

SSL3.0/TLS1.0において比較的容易な方法（暗号化方式）で暗号化鍵が解読されてしまうという構造的脆弱性が発表されました。

当脆弱性の危険性を考え、SSL3.0, TLS1.0暗号化方式の利用を停止いたします。

(PCIDSS ver.3.1においても両暗号化方式は非常に危険性が高いとの指摘がされており、またその利用が明示的に禁止となりました)

参考:

シマンテック(旧ベリサイン) ハッシュアルゴリズムのSHA-1からSHA-2への移行に関して

<http://www.symantec.com/ja/jp/page.jsp?id=ssl-sha2-transition>

SSL3.0脆弱性「POODLE」の発表

<https://jvn.jp/vu/JVNVU98283300/>

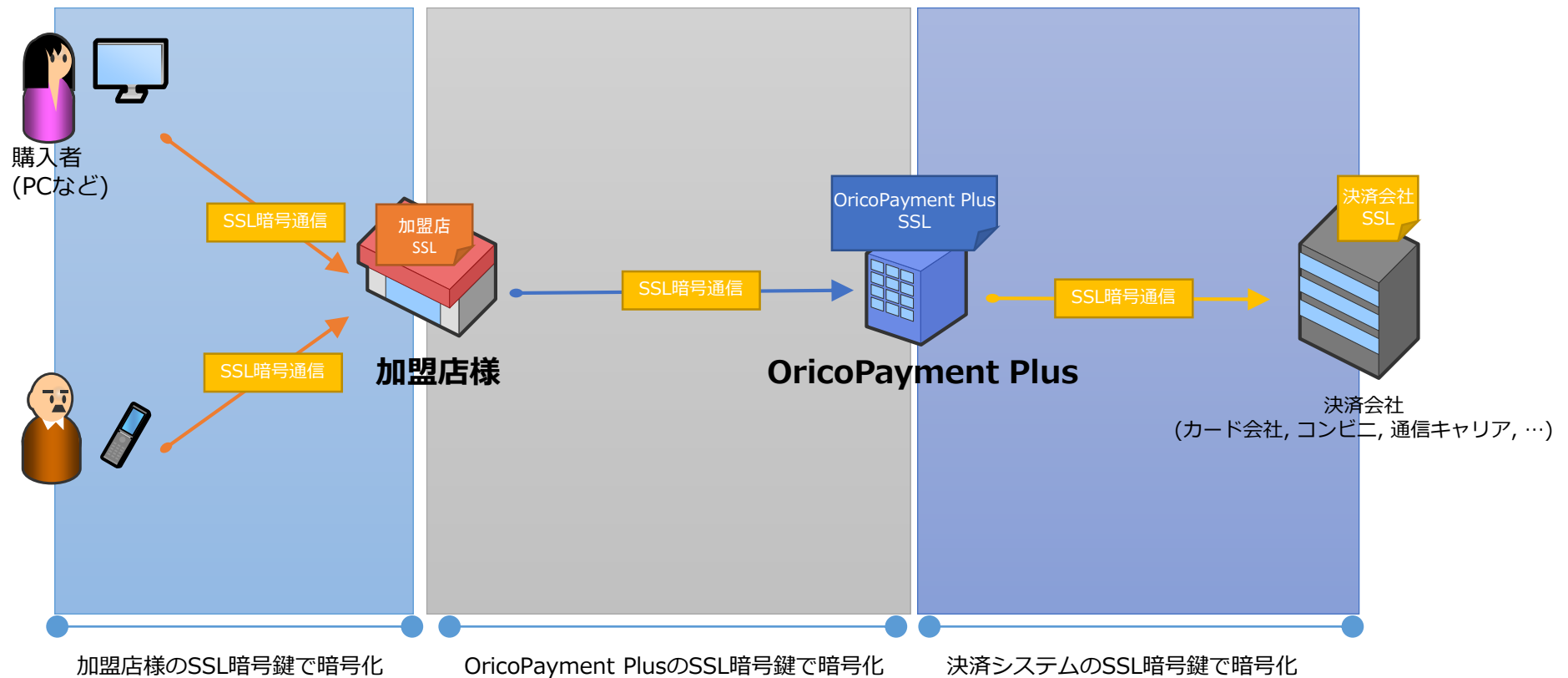
TLS1.0脆弱性「CVE-2014-3566」

<https://jvn.jp/ta/JVNTA98308086/>

# SSL (Secure Socket Layer) とは？

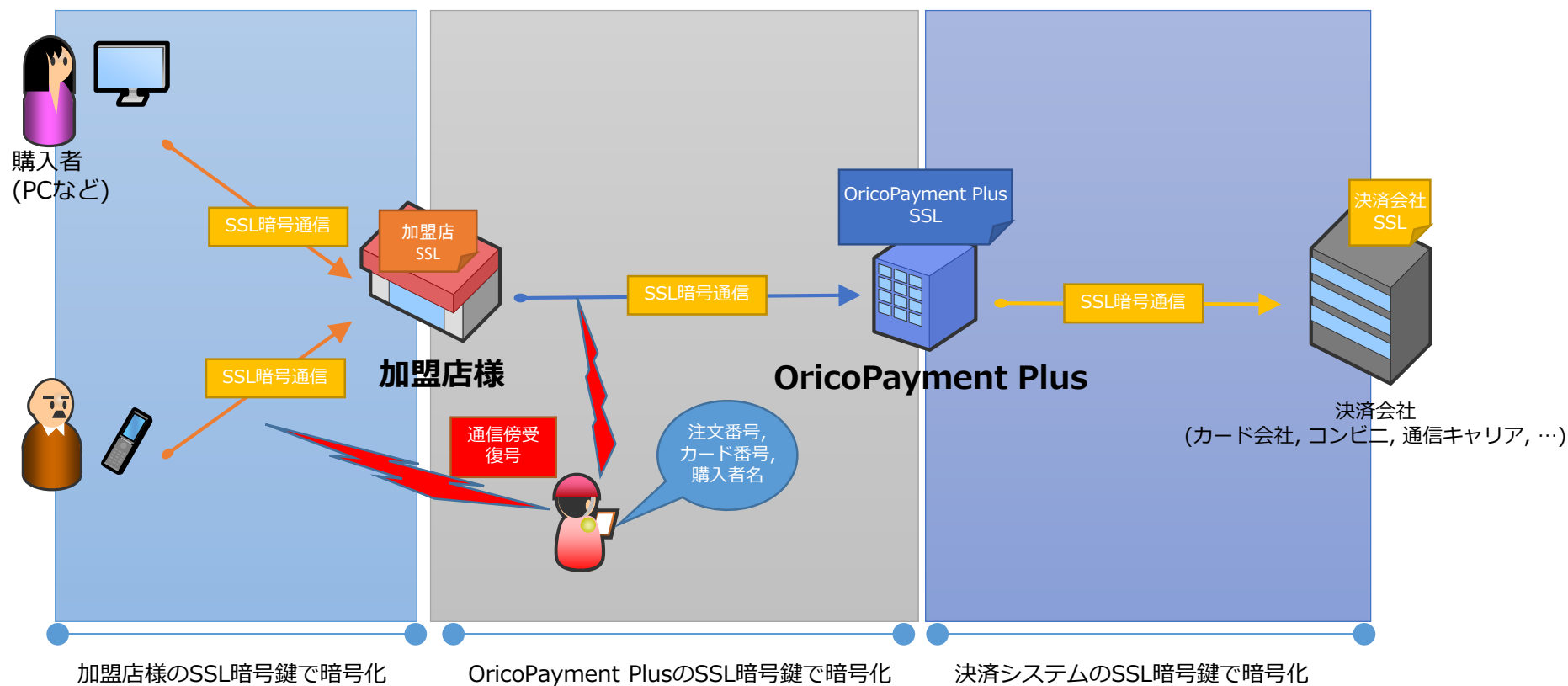
OricoPayment Plusにおいてご利用いただいている決済に関する通信は、全てSSLと呼ばれる仕組みで暗号化が行われております。

その際、ご利用いただく「**SSL暗号化鍵**」は通信する場所によって、どの鍵が使用されるかは異なります。  
(基本的には通信“先”の鍵が使用されます)



# SSLにおけるセキュリティ問題

もし「SSL暗号化鍵」や「暗号方法」にセキュリティ強度の低いもの(暗号化を破られやすいもの)が含まれている場合、通信内容が盗聴され、クレジットカード番号を含む重要なデータが漏えいしてしまう可能性があります。

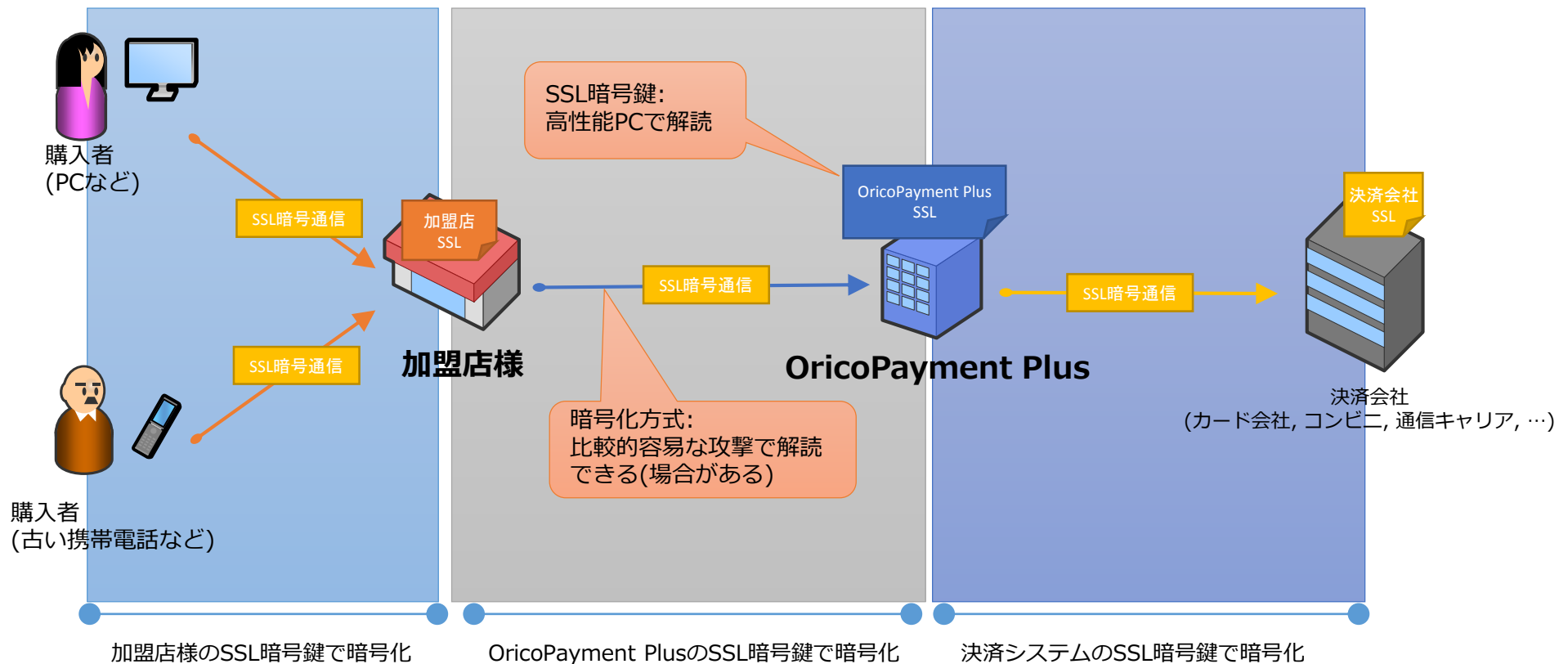


# SSLにおけるセキュリティ問題（2）

近年「**SSL暗号鍵**」と「**暗号化方式**」のそれぞれについて重大な脆弱性の発見、勧告が公表されており、ご利用中の決済通信で、攻撃にさらされる(決済内容が漏えいする)危険性を含んでおります。

「SSL暗号鍵」… 攻撃者のPC性能が向上し、暗号鍵の変更前(多くは1年)に解読される可能性(勧告)

「暗号化方式」… SSL3.0/TLS1.0を使用する場合、比較的容易な攻撃により暗号解読される可能性(脆弱性)



# 各脆弱性に対する業界の動き

「SSL暗号鍵」「暗号化方式」それぞれの課題については既に対応策が発表されております。  
各業界でもその対応策が強く推奨されており、強制適用される流れとなっております。  
(各業界においても脆弱性をついた攻撃が現実のものとなると考えられております)

以下に挙げた対応は、OricoPayment Plusのみならず  
**全世界で対応が求められている内容となっております。**  
加盟店様サイトのシステムにおかれましても、脆弱性へのご対応を推奨いたします(\*\*\*)

課題	対応策	発表組織	適用期限
SSL暗号鍵 (SHA1鍵長)	SSL暗号鍵の長さを攻撃者が短い時間で解読できない長さに変更(SHA256) SSL証明書発行会社は2017年1月1日より、鍵長の短い証明書の販売を禁止(*)	シマンテック等のSSL証明書発行会社	2017年1月1日
	ブラウザベンダー各社は、SHA-1証明書のサポート期限の2016年内の前倒しを検討中	Google Microsoft	2016年内で検討中
暗号化方式 (SSL3.0/TLS1.0)	SSL3.0/TLS1.0の暗号化方式は設計上の脆弱性があるため、一部の例外を除き、より強固なTLS1.1以上の使用を規定(**)	PCI-DSS (PCI SSC)	2016年6月30日 <b>2018年6月30日</b> ※2015年12月18日に適用期限の延長がPCI SSCより発表されました。

- \* 加盟店様でご利用のSSL証明書を2014年以降に更新されている場合、すでに新しい鍵長の証明書(SHA256)をご利用されている可能性があります。
- \*\* OricoPayment Plusでは、強度の高い暗号化方式 (TLS1.1以上) を優先で使用するよう設定しておりますので、加盟店様システムで既にSSL3.0/TLS1.0を無効化されている場合、上記の脆弱性は解消されております。
- \*\*\* 加盟店様システムのインバウンド（内向き）の通信においてTLS1.0が無効化されますとOricoPayment Plusから加盟店様システムへの通信に影響が出る場合がございます。詳細は後述の「加盟店様サイトの脆弱性対応における考慮点」をご確認ください。



# 各脆弱性の対応におけるハードル

暗号化の処理は、システムが稼働するOSやミドルウェアが提供する機能が利用されます(\*)。そのため、強固な暗号化方式に対応していないOSやミドルウェアを利用している場合は、システムのアップグレードが必要です。

- システムがSHA2形式の証明書とTLS1.1以上の暗号方式に未対応であるにもかかわらず、システムのアップグレードを行わなかった場合には、接続先のサーバが各脆弱性対応を実施した瞬間に、全ての通信が行えなくなります。

課題	対応策	影響範囲	影響結果
SSL暗号鍵 (SHA1鍵長)	SSL暗号鍵の長さをSHA2形式に変更する	鍵長が長い鍵を読み込めないシステムが出てくる(例: 古いWindows, 古いフィーチャーフォンなど)	鍵長が変わった瞬間に全てのSSL通信ができなくなる
暗号化方式 (SSL3.0/TLS1.0)	SSL3.0/TLS1.0の暗号化方式を停止し、より強固なTLS1.1以上を使用する	強固な暗号化方式に対応できないシステムが出てくる(例: Java Ver.1.6以前、Windows2003Serverなど) (**)	暗号化方式が変更(SSL3.0/TLS1.0が無効化)された瞬間、全てのSSL通信ができなくなる

\* 間接的（暗黙）に利用されるケースが多いため、加盟店様システムの実装部分だけをみても判別できない構成がほとんどです。

\*\* Ver.1.6以前であってもTLS1.1以上をサポートする有償版Javaにおいては対象外(ご利用可能)となります。

# OricoPayment Plusの対応について

OricoPayment Plusは、この脆弱性への対応のため、セキュリティ問題に対応した新環境の提供を開始いたしました。

2016年9月5日までに、加盟店様のご利用状況にあわせて新環境への切替のご対応をお願いいたします。

注) OricoPayment Plusをご利用の加盟店様で、TLS1.1以上の通信への対応が困難な場合は、SSL3.0/TLS1.0を有効化した暫定環境 (\*)への切替をお願いいたします。

\* 暫定環境は、SHA2形式の証明書を設定していますが、SSL3.0/TLS1.0で接続が可能です。この環境は2018年5月に停止予定です。

## 新本番環境を新設

The diagram illustrates the transition of SSL encryption keys from the franchisee to OricoPayment Plus and then to the payment system. It is divided into three main sections: 1. Franchisee's SSL Key Usage (加盟店様のSSL暗号鍵をご利用), 2. OricoPayment Plus's SSL Key Usage (OricoPayment PlusのSSL暗号鍵をご利用), and 3. Payment System's SSL Key Usage (決済システムのSSL暗号鍵をご利用).

**加盟店様のSSL暗号鍵をご利用**

購入者 (PCなど) and 加盟店様 (Franchisee) are shown. Arrows labeled "SSL暗号通信" (SSL encrypted communication) connect the purchaser to the franchisee and the franchisee to the payment system.

**OricoPayment PlusのSSL暗号鍵をご利用**

OricoPayment Plus is shown with two environments: 旧環境 SSL(SHA1) (Old Environment SSL(SHA1)) and 新環境 SSL(SHA2) (安全版) (New Environment SSL(SHA2) (Secure Edition)). A callout box indicates the transition period: "2015年11月～2016年9月で切替 (加盟店様)" (Transition from November 2015 to September 2016 (Franchisee)). Arrows labeled "SSL暗号通信" connect the franchisee to both environments. The new environment is labeled "SSL3.0/TLS1.0無効" (SSL3.0/TLS1.0 Invalid), while the old environment is labeled "SSL3.0/TLS1.0有効" (SSL3.0/TLS1.0 Valid).

**決済システムのSSL暗号鍵をご利用**

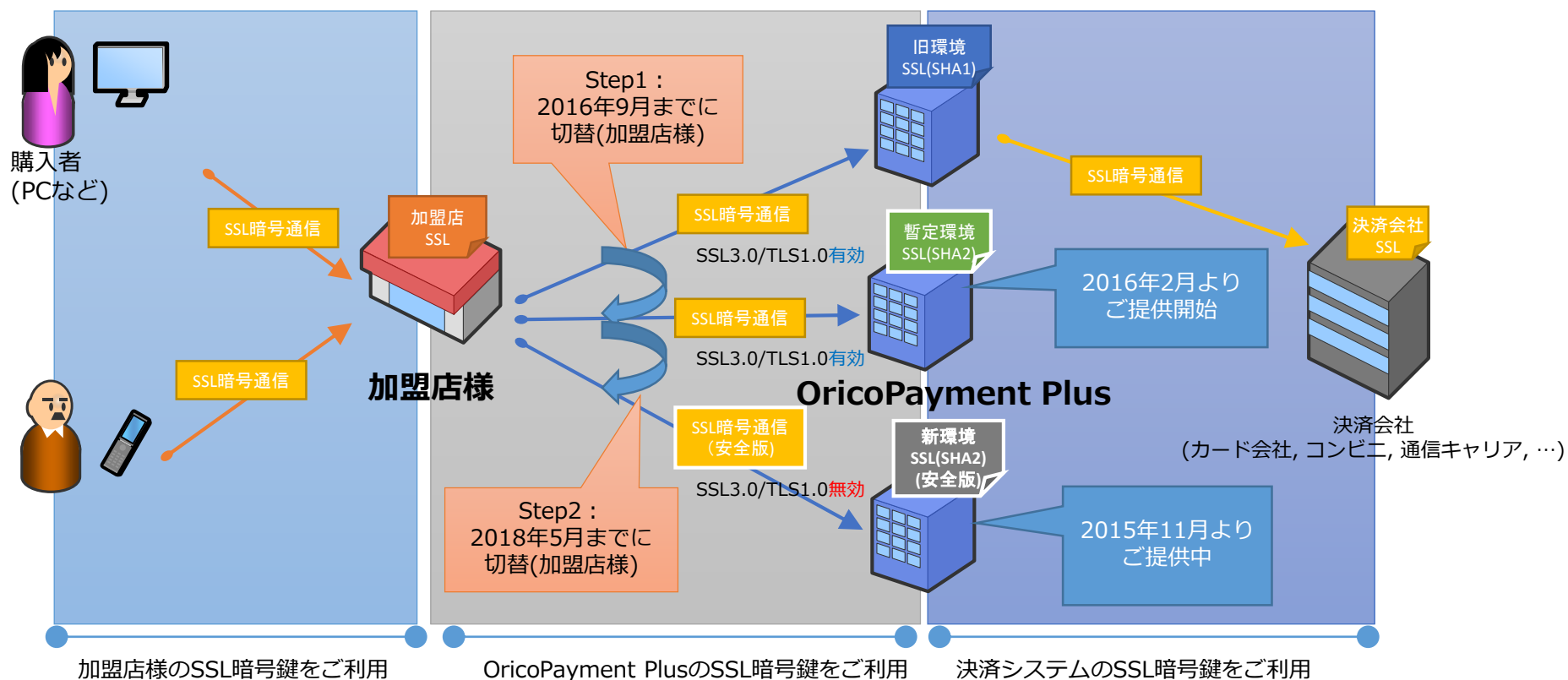
決済会社 SSL (Payment Company SSL) is shown. An arrow labeled "SSL暗号通信" connects OricoPayment Plus to the payment company. A callout box indicates the start date: "2015年11月より順次ご提供開始" (Sequential provision starting from November 2015).

**決済会社 (カード会社、コンビニ、通信キャリア、...)**

# OricoPayment Plusの対応について（3）

## TLS1.1対応が間に合わない加盟店様向けの暫定環境を新設

加盟店様の接続切替を、2段階に分けて実施して頂くことが可能です。



※ 暫定環境は2018年5月に停止予定のため、それまでに新環境に移行して頂きますようお願いいたします。

# OricoPayment Plusの対応について（４） サービス環境一覧

OricoPayment Plusが公開中のサービス環境の仕様一覧を示します。

サービス環境名	SSL証明書形式	暗号化 プロトコル	ご利用期限	その他
旧環境	SHA-1	TLS1.2 TLS1.1 TLS1.0 SSL3.0	～2016年9月5日 旧環境停止まで	ご利用期限までに、新環境への移行をお願いいたします。
暫定環境	SHA-2 (SHA-256)	TLS1.2 TLS1.1 TLS1.0 SSL3.0	2016年2月 ～2018年5月	すべてのバージョンのMDKをご利用可能です。ただし、旧バージョンのMDKをご利用の場合は、 <u>CA証明書ストアファイルの更新が必要です。</u>
新環境	SHA-2 (SHA-256)	TLS1.2 TLS1.1	～無期限	接続するためには、最新版のMDKをご利用いただく必要があります。 最新版のMDKは、以下のサイトよりダウンロードできます。 <a href="http://www.orico.co.jp/partner/online/paymentplus/support/login/index.html">http://www.orico.co.jp/partner/online/paymentplus/support/login/index.html</a>

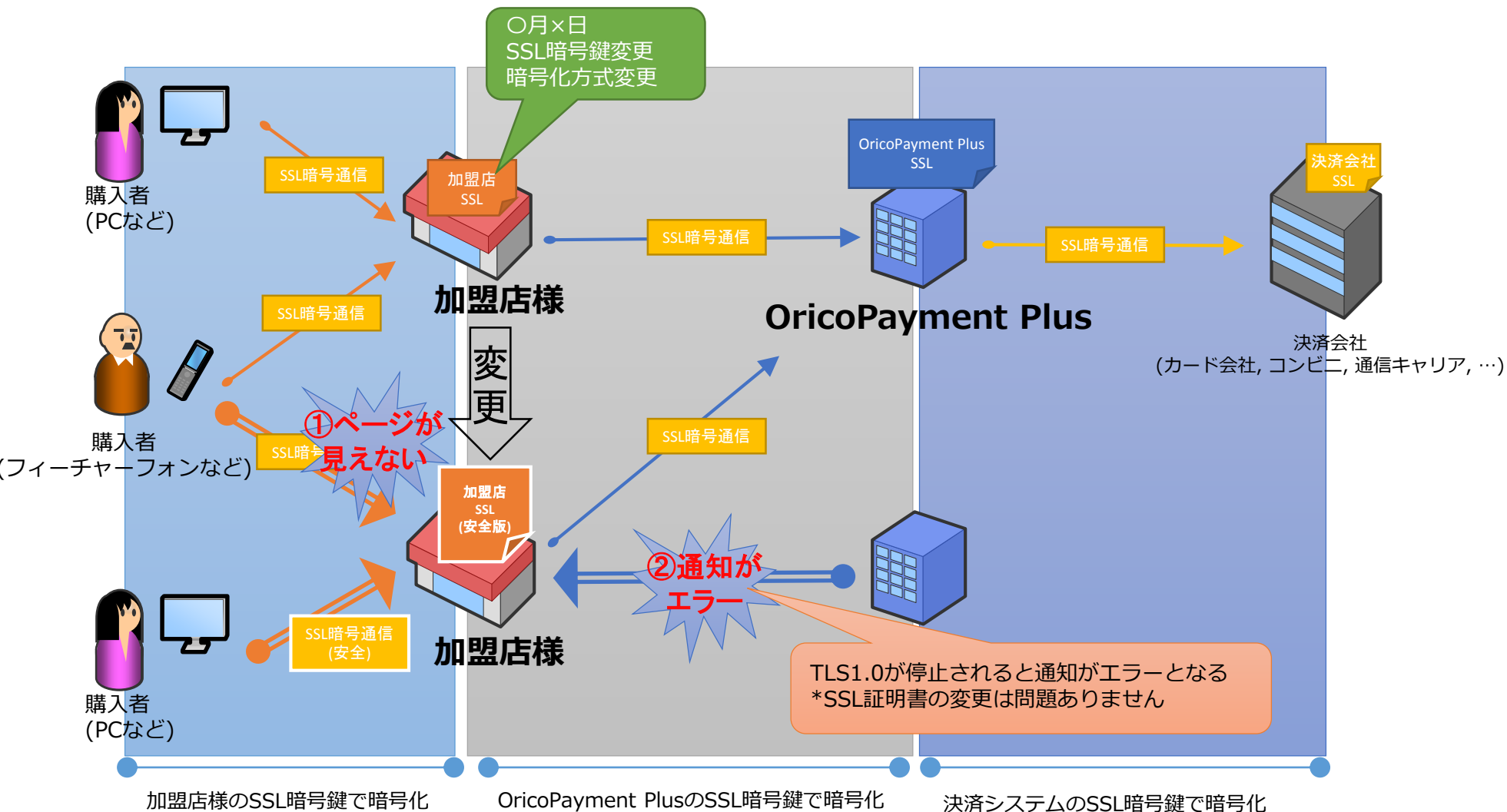
# 加盟店様サイトの脆弱性対応における考慮点

SSLにおける課題(証明書形式, 暗号化方式)は、加盟店様のシステムにおいても発生しておりますが、ご対応の際は、以下を考慮して頂きますようお願いいたします。

課題	対応策	影響結果	コメント
SSL暗号鍵 (SHA1鍵長)	SSL暗号鍵の長さをSHA2形式に変更する	購入者様が未対応の端末 (WindowsXP SP3未満, フューチャーフोनなど)の場合、アクセスできなくなります。(①)	2014年以後にSSLを更新されている場合、既にSHA2になっている可能性があります。 <b>御社Webページなどでご案内いただくことを推奨いたします。</b>
暗号化方式 (SSL3.0/TLS1.0)	SSL3.0/TLS1.0の暗号化方式を停止し、より強固なTLS1.1以上を使用する	OricoPayment Plusから御社向けの通信(PUSH通知など)が届かなくなります。(②)	OricoPayment Plusからの通信におけるTLS1.1以上への対応は、スケジュールが決まり次第、別途ご案内させていただきますので、ご案内をお待ちください。

①, ② については次ページをご参照ください

# 加盟店様サイトの脆弱性対応における考慮点（2）



# まとめ

## 背景として

- SHA1形式のSSL証明書の販売が停止される（SHA2形式に移行しなければならない）
- SSL3.0/TLS1.0の暗号化方式セキュリティ強度が弱い分類に仕分けられた

## OricoPayment Plusの対応

- 決済サービスのSSL証明書をSHA2形式に変更します
- SSL3.0/TLS1.0の暗号化方式を停止します

## 加盟店様へのご依頼事項

- ご契約中のサービスに合わせたご対応をお願いいたします。
- OricoPayment PlusからのPUSH通知(\*)は、当面の間TLS1.0にて送信しますので、加盟店様サーバ側ではTLS1.0の通信を受信できる設定のままでお願いいたします。

\* コンビニ決済の入金通知など、OricoPayment Plusから通知を受信するサービスをご利用の場合。



# 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](mailto: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くと幸いです。
- 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

No.	日付	変更内容	変更者
1	2016/03/01	1.0版作成	OricoPayment Plus