ベリトランスサービスをご利用のマーチャント各位

Confidential
1.2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【補足資料】

2016/3/15

ベリトランス株式会社

目次

マーチャント様へのご依頼事項

【ご依頼事項】SSL-SHA2形式、TLS1.1以降への対応

ベリトランス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．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
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
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「**ベリトランスの対応について**」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、ベリトランスのサービス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。
マーチャント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】マーチャント様サイトのSSL3.0/TLS1.0の停止について

2016年3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、ベリトランスよりマーチャント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おりません**。
そのため、マーチャント様システム（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、マーチャント様システムにて入金通知が受信できなくなってしまいます。
※ 後述の「**マーチャント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

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。
ベリトランスで利用している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

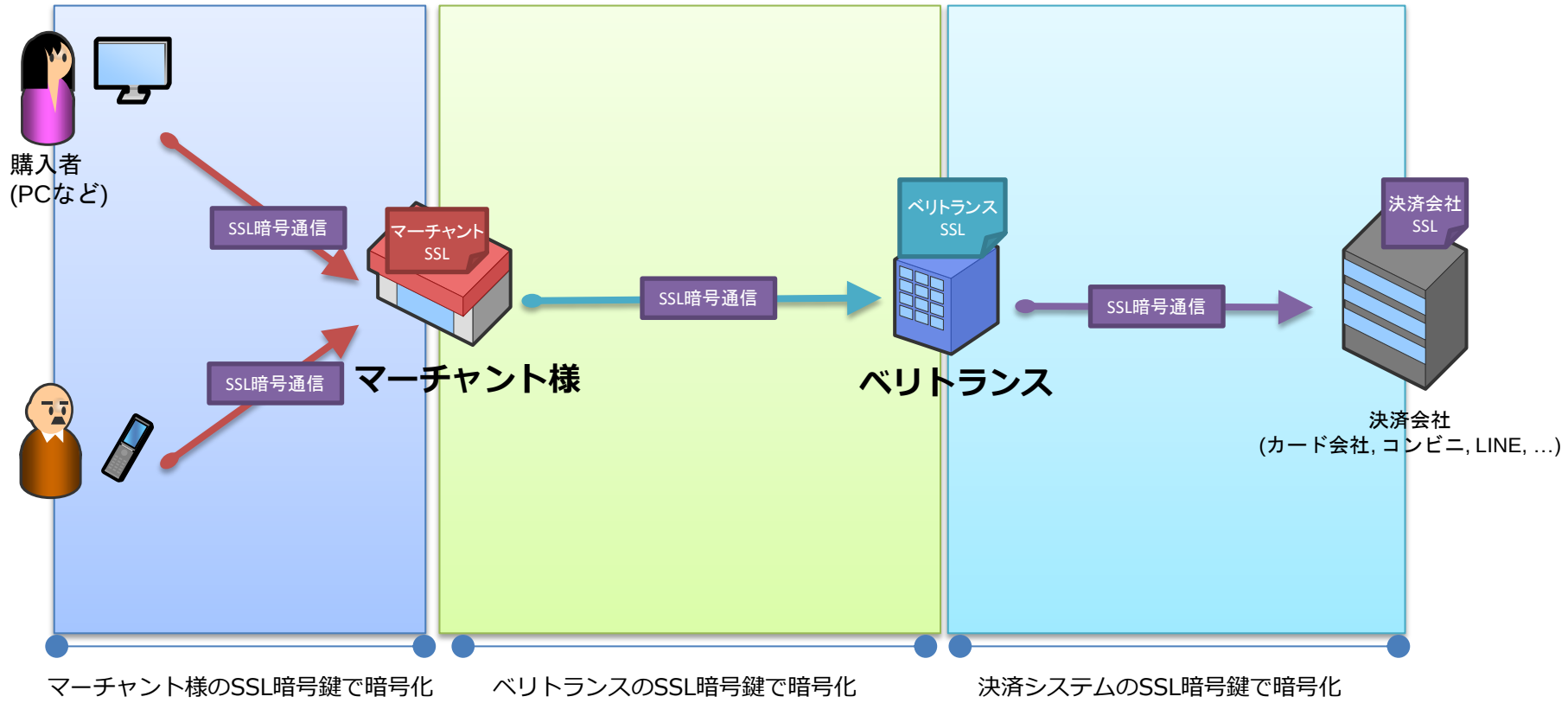
SSL3.0脆弱性「POODLE」の発表
https://jvn.jp/vu/JVNVU98283300/

TLS1.0脆弱性「CVE-2014-3566」
https://jvn.jp/ta/JVNTA98308086/

SSL（Secure Socket Layer）とは？

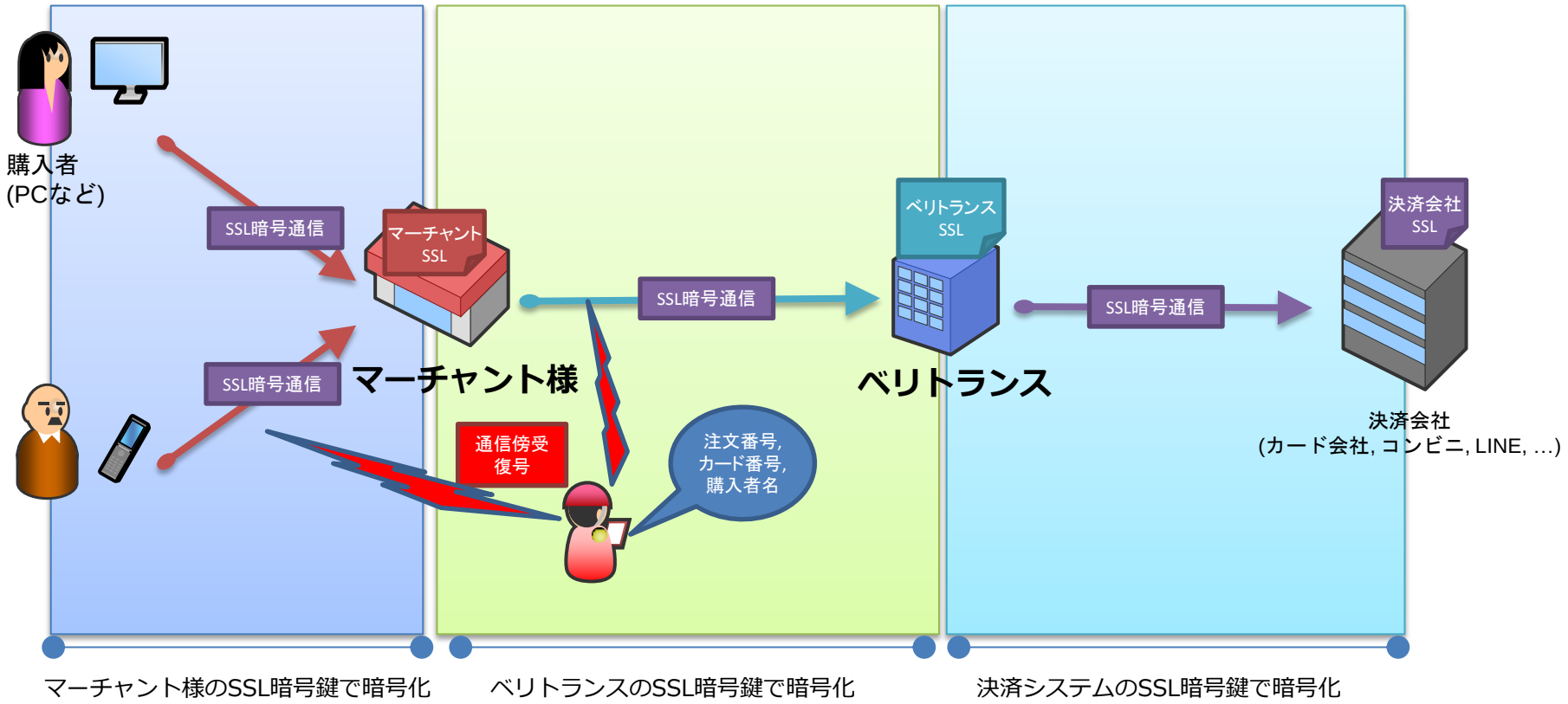
ベリトランス決済サービスにおいてご利用いただいている決済に関する通信は、全て**SSL**と呼ばれる仕組みで**暗号化**が行われております。

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

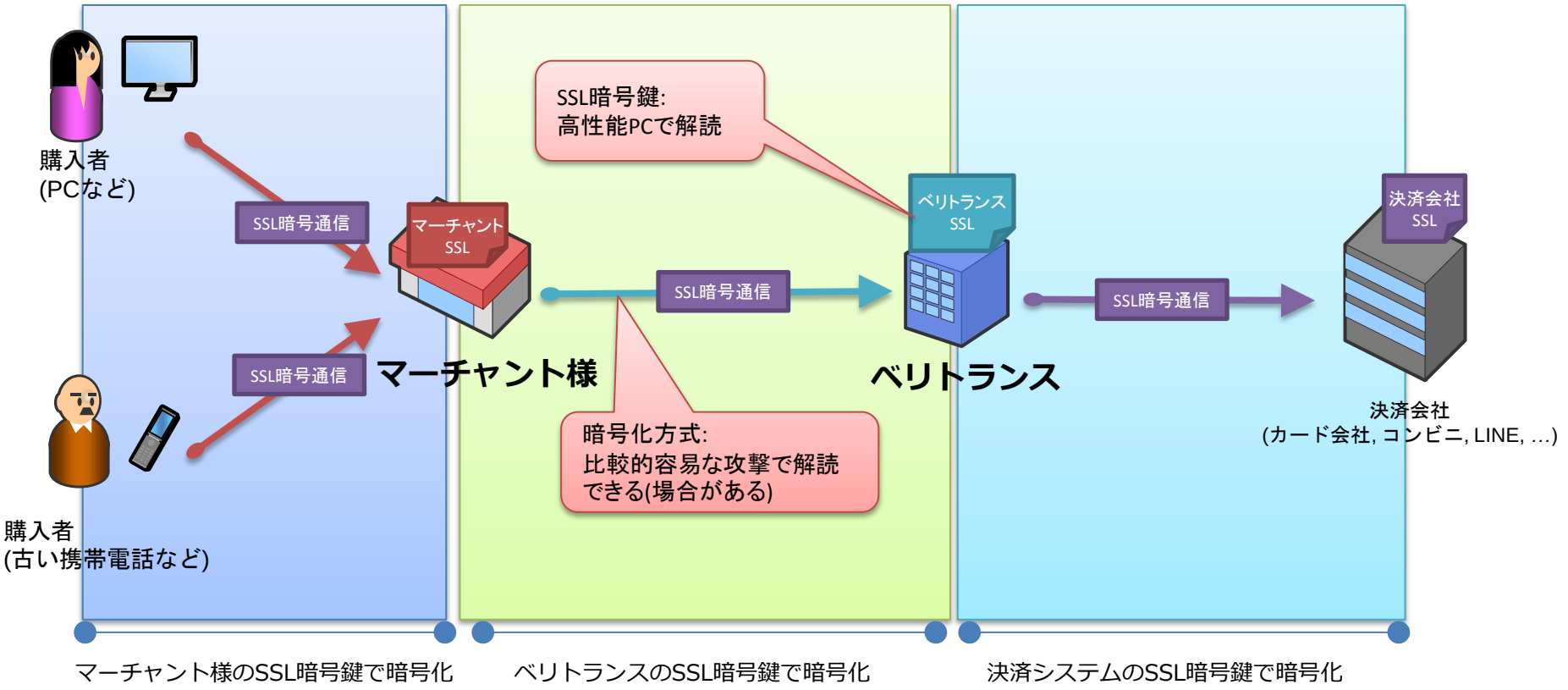
もし「SSL暗号化鍵」や「暗号方法」に**セキュリティ強度の低いもの**(暗号化を破られやすいもの)が含まれている場合、**通信内容が盗聴され、クレジットカード番号を含む重要なデータが漏えいしてしまう**可能性がございます。



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、ベリトランスのみならず
全世界で対応が求められている内容となっております。
マーチャント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 等	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~~ 2018年6月30日 ※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。

* マーチャント様でご利用の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ございます。
**ベリトランスでは、強度の高い暗号化方式 (TLS1.1以上) を優先で使用するように設定しておりますので、マーチャント様システムで既に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。
*** マーチャント様システムのインバウンド（内向き）の通信においてTLS1.0を無効化されますとベリトランスからマーチャント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「マーチャント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、マーチャント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。

ベリトランスの対応について

ベリトランスは、この脆弱性への対応のため、
2015年11月4日 (*)より、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
マーチャント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。

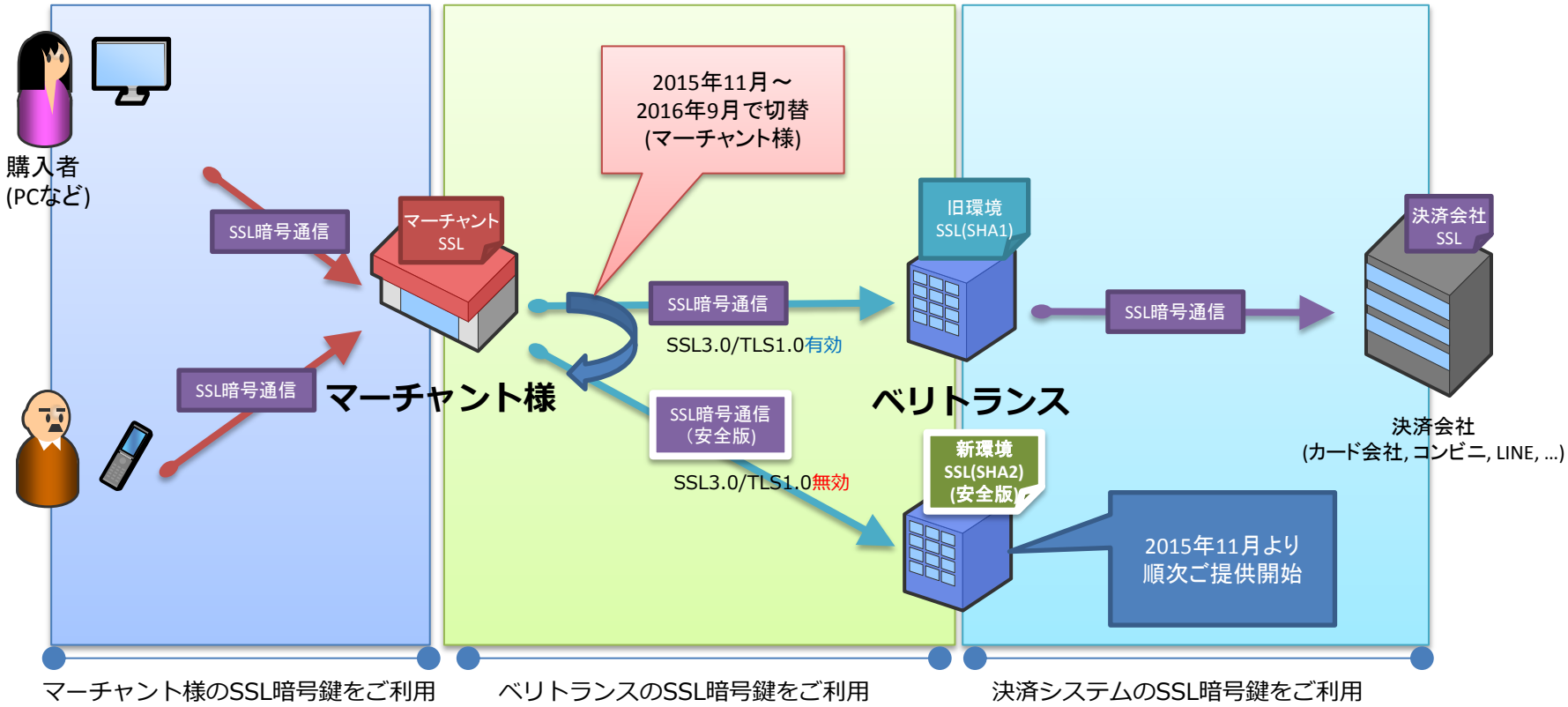
注）VeriTrans3Gをご利用のマーチャント様で、
TLS1.1以上の通信への対応が困難な場合は、SSL3.0/TLS1.0を有効化した暫定環境(**)への切替をお願いいたします。

* ご利用の決済サービスにより提供開始時期が異なります。
** 暫定環境は、VeriTrans3Gのみご利用可能です。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。

ベリトランスの対応について（２）

新本番環境を新設

マーチャント様のご都合のよいタイミングで、新環境に切り替えて頂くことが可能です。

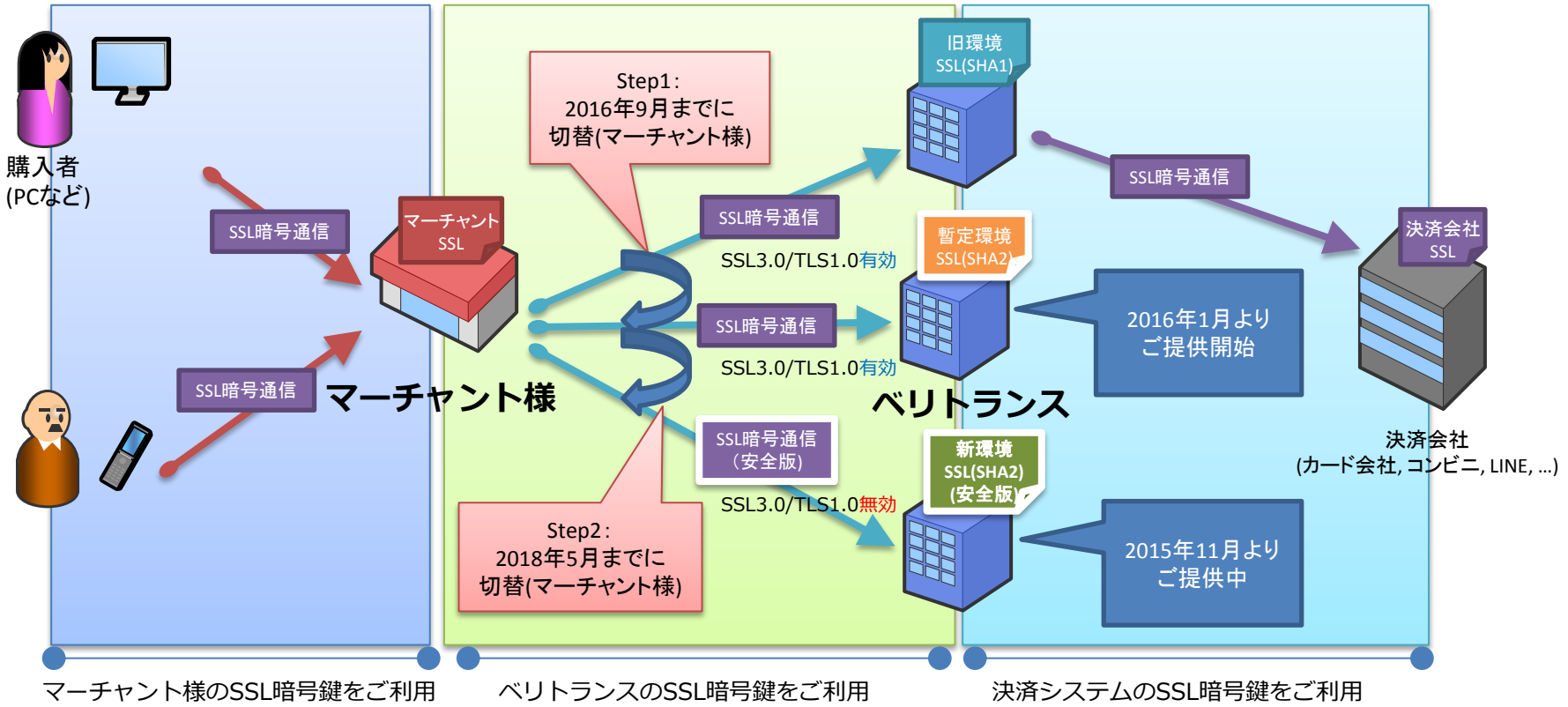


※ 一部サービスについては、システムの都合上、マーチャント様とご相談の上、一斉切替を行わせていただく場合がございます

ベリトランスの対応について（３）※VeriTrans3Gのみ対象

TLS1.1対応が間に合わないマーチャント様向けの暫定環境を新設

マーチャント様の接続切替を、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します。

ベリトランスの対応について（４）サービス環境一覧

ベリトランス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 ※VeriTrans3Gのみ	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、CA証明書ストアファイルの更新が必要です。
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。 https://www.veritrans.co.jp/support/trial/login.html

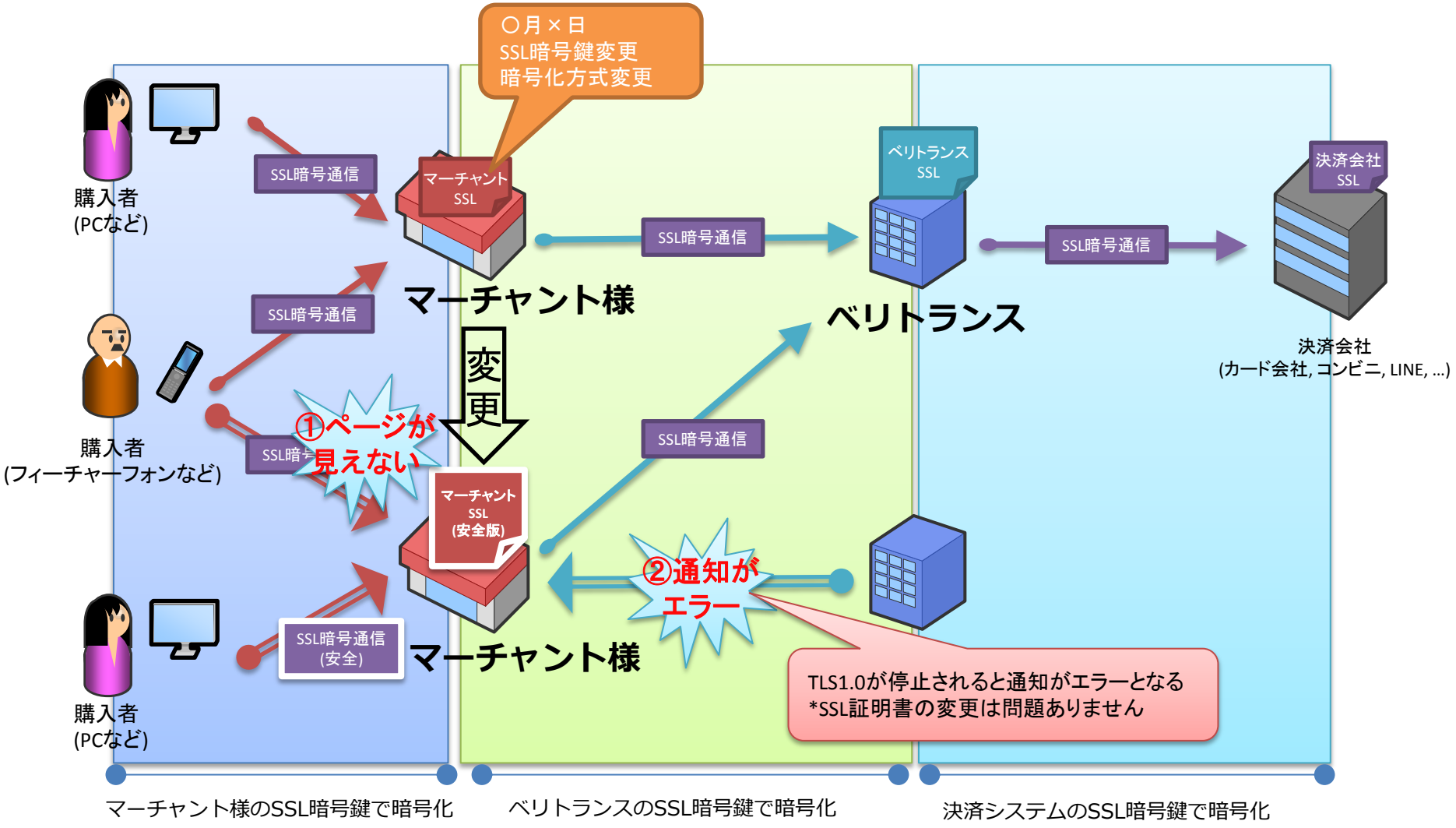
マーチャント様サイトの脆弱性対応における考慮点

SSLにおける課題(証明書形式, 暗号化方式)は、マーチャント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, フューチャーフォンなど)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。 **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。**
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	ベリトランスから御社向けの通信 (PUSH通知など)が届かなくなります。(②)	2016年夏頃にベリトランスより別途、ご案内させていただきますので、ご案内後、ご対応をご検討ください。

①, ② については次ページをご参照ください

マーチャント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

ベリトランスの対応

- 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

マーチャント様へのご依頼事項

- 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。
- ベリトランスからの通知に関する試験の実施(*) をお願いいたします。

* コンビニ決済の入金通知など、ベリトランスから通知を受信するサービスをご利用の場合。
2016年夏頃を予定しております。

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

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

変更履歴

No.	日付	変更内容	変更者
1	2015/09/28	1.0版作成	ベリトランス技術部
2	2016/02/01	1.1版作成 VeriTrans3Gの暫定環境（SHA2証明書、SSL3.0/TLS1.0有効）に関する記載を追加 以下のスライドを追加 「ベリトランスの対応について（3）※VeriTrans3Gのみ対象」 「ベリトランスの対応について（4）サービス環境一覧」	ベリトランス技術部
3	2016/03/15	1.2版作成 旧環境（SHA-1）の停止日決定（2016年9月5日）に伴う記載内容の見直し	ベリトランス技術部