PCI DSS ReadyCloud

JCDSC主催 PCI DSSセキュリティフォーラム 2019

対面加盟店向け PCI P2PEソリューションのご紹介「PCI P2PE共同利用サービス（仮称）」

2019/6/11

LINK, INC.

セキュリティプラットフォーム事業部

事業部長　滝村 享嗣

本日のアジェンダ

- 会社概要
- サービス沿革
- 改正割賦販売法及び実行計画について
- 対面加盟店におけるカード情報保護対策
- 「PCI P2PE共同利用サービス（仮称）」とは？

株式会社リンク　会社概要

会社名	株式会社リンク
所在地	［本社］ 東京都港区赤坂7丁目3番37号 カナダ大使館ビル１階 ［支社］ 大阪府大阪市北区梅田2-2-2 ヒルトンプラザウエスト オフィスタワー18階
設　立	1987年11月18日
URL	http://www.link.co.jp/
代表者	岡田　元治
資本金	10,000,000円
売上高	53億4,400万円 （2018年 5月 実績）
従業員数	80 名
業務内容	at+link ［ ホスティングサービス ］ リンクベアメタルクラウド［ アプリプラットフォーム ］ PCI DSS Ready Cloud ［ セキュリティプラットフォーム ］ BIZTEL ［ クラウド型テレフォニーサービス ］ e-select ［ オンラインモール ］ 中洞牧場 ［ 乳製品の製造・販売 ］

サービス沿革

- 2013年5月　PCI DSS Ready Cloudを発表
- 2014年1月
  KVH株式会社(現 Coltテクノロジーサービス) との提携を発表
- 2014年9月 Cloud Token for Payment Cardを発表
- 2016年12月 BIZTELコールセンター PCI DSSを開始
- 2017年6月 PCI DSS Ready Cloud AWSを発表
- 2017年9月 Pay TG ビジネスモデル特許出願
- 2017年10月 非保持化サービス「Pay TG」を発表
- 2018年6月 PCI DSS Ready Cloud ビジネスモデル特許取得

改正割賦販売法及び実行計画について

2018年6月1日施行 改正割賦販売法 概要

改正のポイント	内容
（第35条の1） クレジットカード番号等取扱業者	・1号事業者　イシュア ・2号事業者　アクワイアラ ・3号事業者　加盟店
（第35条の16） クレジットカード情報の適切な管理等	・カード情報の非保持化あるいはPCI DSS準拠 ・委託先の情報管理に係る指導等の義務
（第35条17の15） クレジットカードの不正使用対策の義務	・クレジット決済端末のIC化 ・ネット上のなりすまし対策

加盟店がクレジットカード情報保護／不正利用防止を行わない場合、法律上の罰則はないが、加盟店契約が継続できなくなるリスクが存在

『実行計画』の要請

本実行計画は、【改正割賦販売法で求められるセキュリティ対策の実務上の指針】として位置づけられるものであり、本実行計画 に掲げる措置又はそれと同等以上の措置を講じている場合には、セキュリティ対策に係る法令上の基準を満たしていると認められる。
(『実行計画2019』P5より)

以下はその抜粋

対象	要請の内容と期限
加盟店	・カード情報の非保持化（同等相当含む）またはPCI DSS準拠 （非対面加盟店は2018年3月、対面加盟店は2020年3月までに完了） ・対応済の加盟店は、最新の攻撃手口に対応したセキュリティ対策の改善・強化を不断に実施
カード会社・ PSP（決済代行事業者）	・PCI DSS準拠の維持・運用 ・カード会社は、PCI DSSに準拠していないPSPとの取引を見直し ・加盟店に対して非保持、非保持と同等/相当又はPCI DSS準拠に向けた要請

対面加盟店におけるカード情報保護対策

加盟店におけるカード情報保護対策

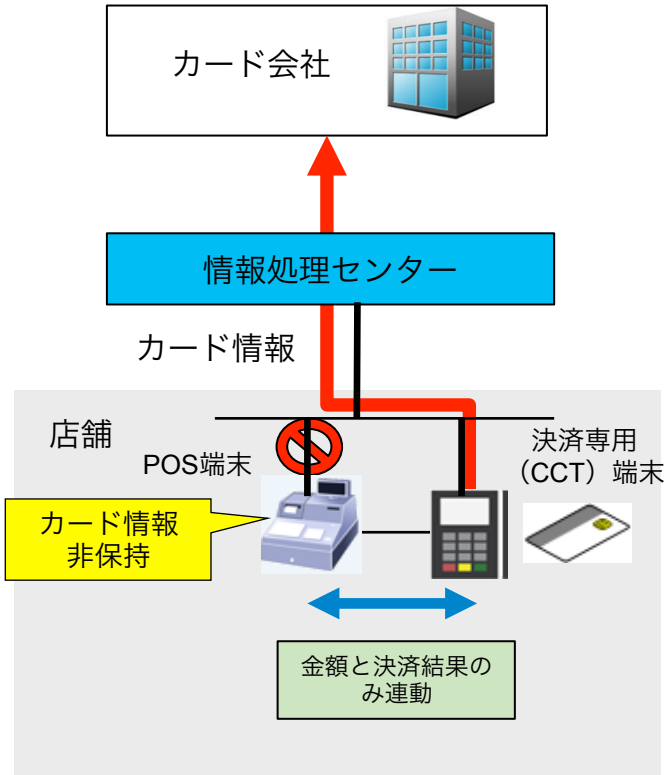
<table>
<tr><th colspan="2" rowspan="2">取引形態</th><th colspan="2">接続形態毎の対応策</th></tr>
<tr><th>外回り・非通過型</th><th>内回り・通過型</th></tr>
<tr><td colspan="2"></td><td>自社で保有する機器・ネットワークにカード情報を保存、処理、通過しない方式</td><td>自社で保有する機器・ネットワークにカード情報を保存・処理・通過する方式</td></tr>
<tr><td rowspan="2">非対面加盟店</td><td>EC加盟店</td><td>非保持化</td><td>PCI DSS準拠</td></tr>
<tr><td>MOTO加盟店</td><td>非保持化 PayTG</td><td>非保持化同等/相当のセキュリティ措置またはPCI DSS準拠</td></tr>
<tr><td colspan="2" rowspan="2">対面加盟店</td><td rowspan="2">非保持化</td><td>非保持化同等/相当のセキュリティ措置またはPCI DSS準拠</td></tr>
<tr><td>PCI P2PE</td><td>ASP／クラウド接続型</td></tr>
</table>

POS加盟店の非保持化

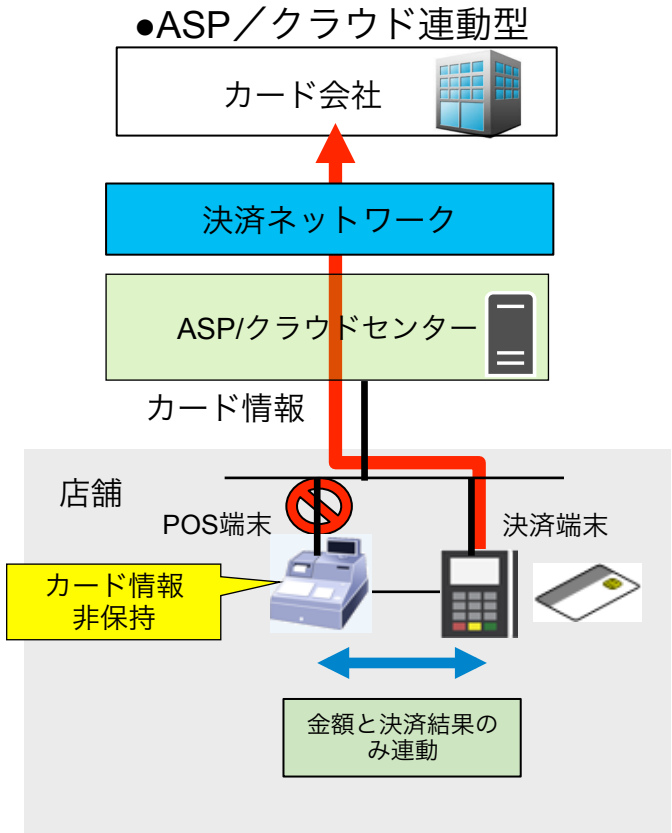
外回り方式

- POS機能と決済機能を分離することで非保持化を実現
- CCTを利用する場合、情報処理センターにそのままカード情報を送信可能
- 『実行計画2016』では外回り方式のみが非保持化方式として記載されていた。

●決済専用端末（CCT）連動型



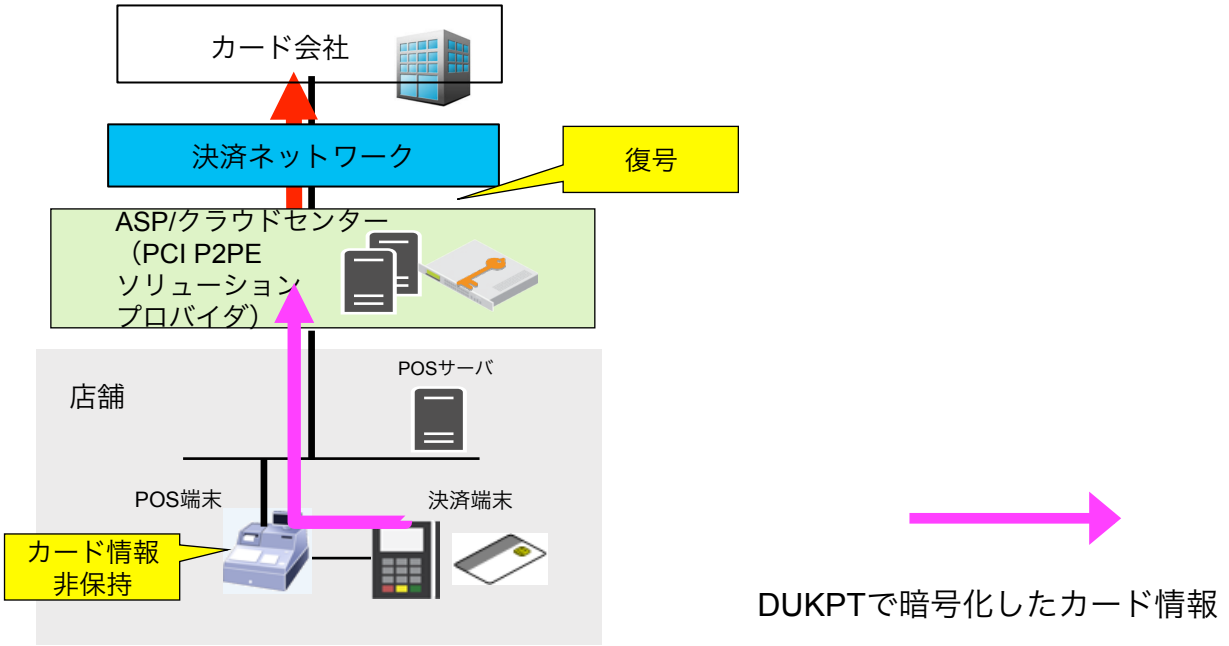
●ASP／クラウド連動型



POS加盟店の非保持化（同等／相当の措置）①

内回り方式（1）PCI Point-to-Point Encryption（PCI P2PE）

- 暗号鍵をトランザクションごとに交換するDUKPTによる暗号化を用いることと、決済端末へのキーインジェクション、復号環境のセキュリティ措置、暗号管理などが、PCI P2PEの要求事項として満たされることから、『実行計画2017』で非保持化同等／相当のセキュリティ措置と整理された。
- 決済端末でカード情報を読み取り後ただちに暗号化し、ASP/クラウドセンター内の復号ポイントまで暗号化したまま送信（加盟店内では復号しない、復号鍵を持たない）



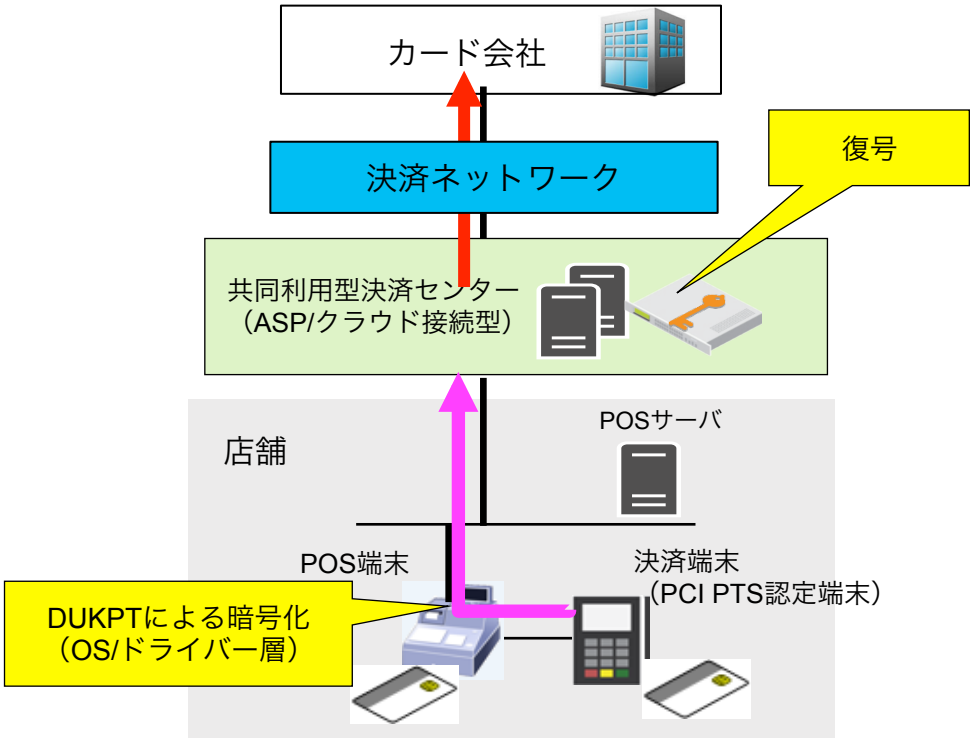
DUKPT：Delivered Unique Key Per Transaction

POS加盟店の非保持化（同等／相当の措置）②

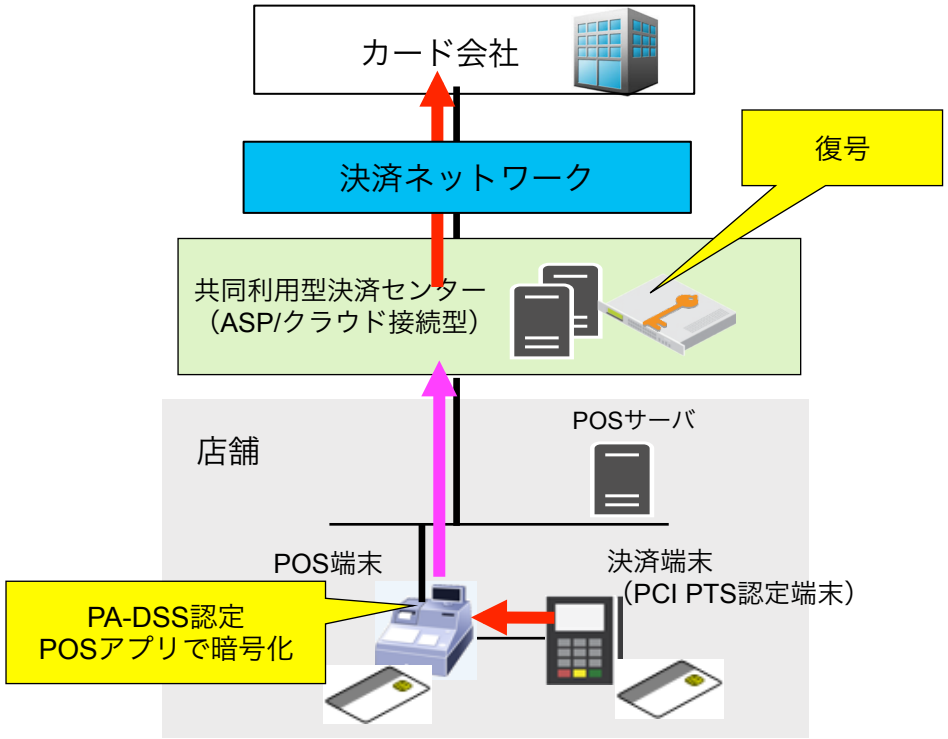
内回り方式（2）ASP/クラウド接続型

- 『対面加盟店における非保持と同等／相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について』が提示され、『実行計画2018』において内回り方式の一つとして整理された。
- 同文書に記載された11項目のセキュリティ技術要件を満たす必要がある。

●パターン①　決済端末（POS端末）でDUKPTにより暗号化



●パターン② PA-DSS認定のPOSアプリで暗号化



DUKPT：Delivered Unique Key Per Transaction
PCI PTS：PCI PIN Transaction Security
PA-DSS：Payment Application Data Security Standard

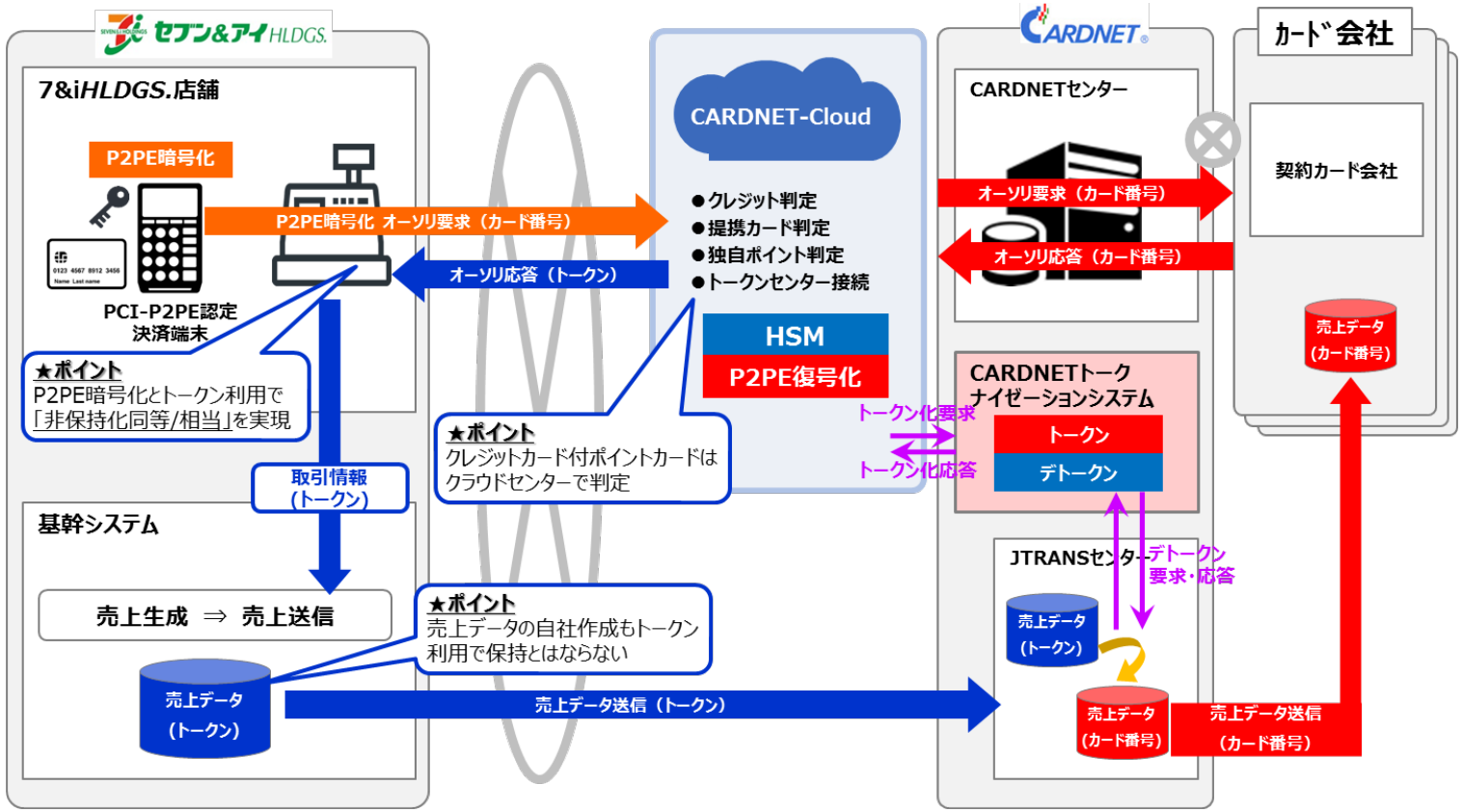
→ 暗号化したカード情報

POS加盟店の非保持化 各方式の比較

	外回り方式	内回り方式	
	CCT連動型	PCI P2PE	ASP／クラウド接続型
優位点	• カード情報がPOSを保存・処理・通過しないので、そのままの形態で非保持となる。	• ハウスポイントや割引プログラムなどが継続して提供できる。 • レシートとカードの伝票が一体化が可能	
課題	• 外付決済端末の導入が必須 • ハウスポイントや割引プログラムなど複雑な処理が困難 • CCTを利用する場合は、レシートとカードの伝票が分離してしまう。	• PCI P2PEソリューションプロバイダが少ない • 選定できる決済端末の種類が少ない • 非ギャザリング処理に課題が残る。	• 加盟店でカード情報は保存できない。 • 非保持と同等／相当と見なすために、11要件のセキュリティ措置を別途満たす必要がある。（技術的な要件を満たすことも容易ではないため、大型の加盟店ではコストが高くなることもある）

PCI P2PEによる内回り方式での非保持化の事例

- セブン＆アイ・ホールディングス
  - 2018年10月からセブンイレブン（全国2万店舗）に導入
  - 2019年4月からグループ店舗（全国1千店舗）に導入し2020年3月までに非保持化を完了



（セブン＆アイ・ホールディングス　報道発表資料より）

プロセッサ／決済代行事業者側の課題

- 顧客であるPOS加盟店向けに非保持化ソリューションを提供する場合の課題

1. 自社の決済サービスをPCI P2PEに対応させたいが、技術、コストの観点でハードルが高い。

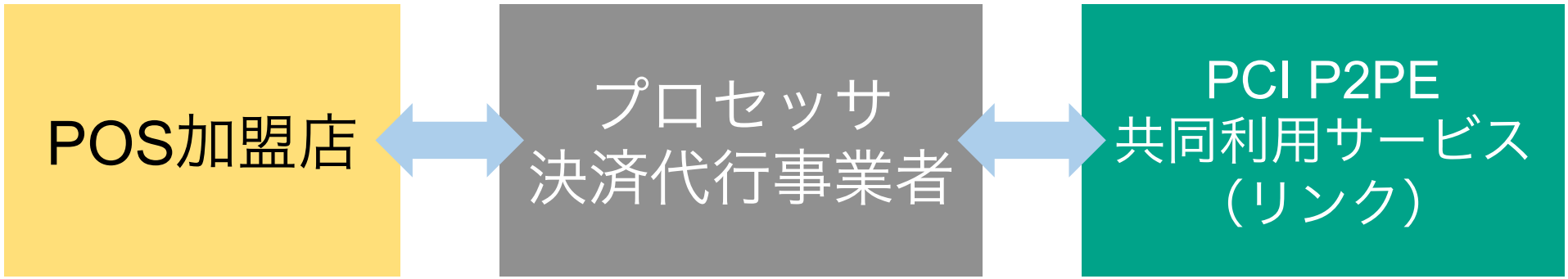
2. PCI P2PEソリューションの認定スケジュールが想定より長くかかるため、顧客が要望する納期に間に合わない。

3. 顧客（加盟店）の多くは非ギャザリングのPOS加盟店であり、PCI P2PEソリューションの提供だけでは非保持化とならない。

「PCI P2PE共同利用サービス（仮称）」とは？

リンクが提供する「PCI P2PE共同利用サービス（仮称）」とは？

- プロセッサ／決済代行事業者はリンクが提供する「PCI P2PE共同利用サービス」と接続することにより、PCI P2PEソリューションをPOS加盟店に提供することが可能
  - リンクのサービス提供先：プロセッサ／決済代行事業者



PCI P2PE共同利用サービス 各社のメリット

プロセッサ／決済代行事業者のメリット

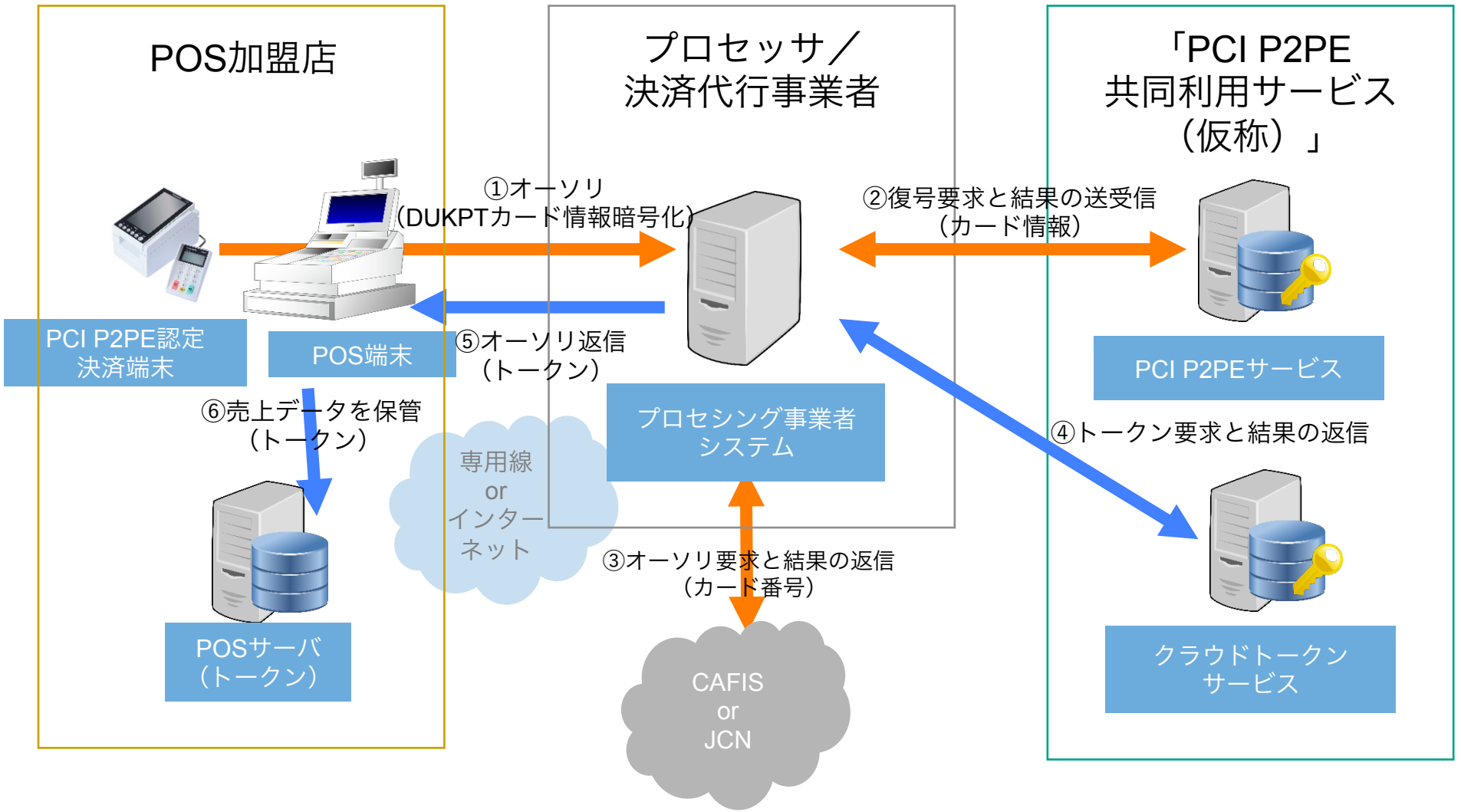
- 自社がPCI P2PE認定を取得することなく、顧客（加盟店）にPCI P2PEの暗号／復号サービスの提供が可能
- 自社の顧客が非ギャザリング処理の加盟店でも本サービスを利用すれば、当該加盟店は非保持化同等／相当のセキュリティ措置が可能（PCI DSSの準拠も不要）

POS加盟店のメリット

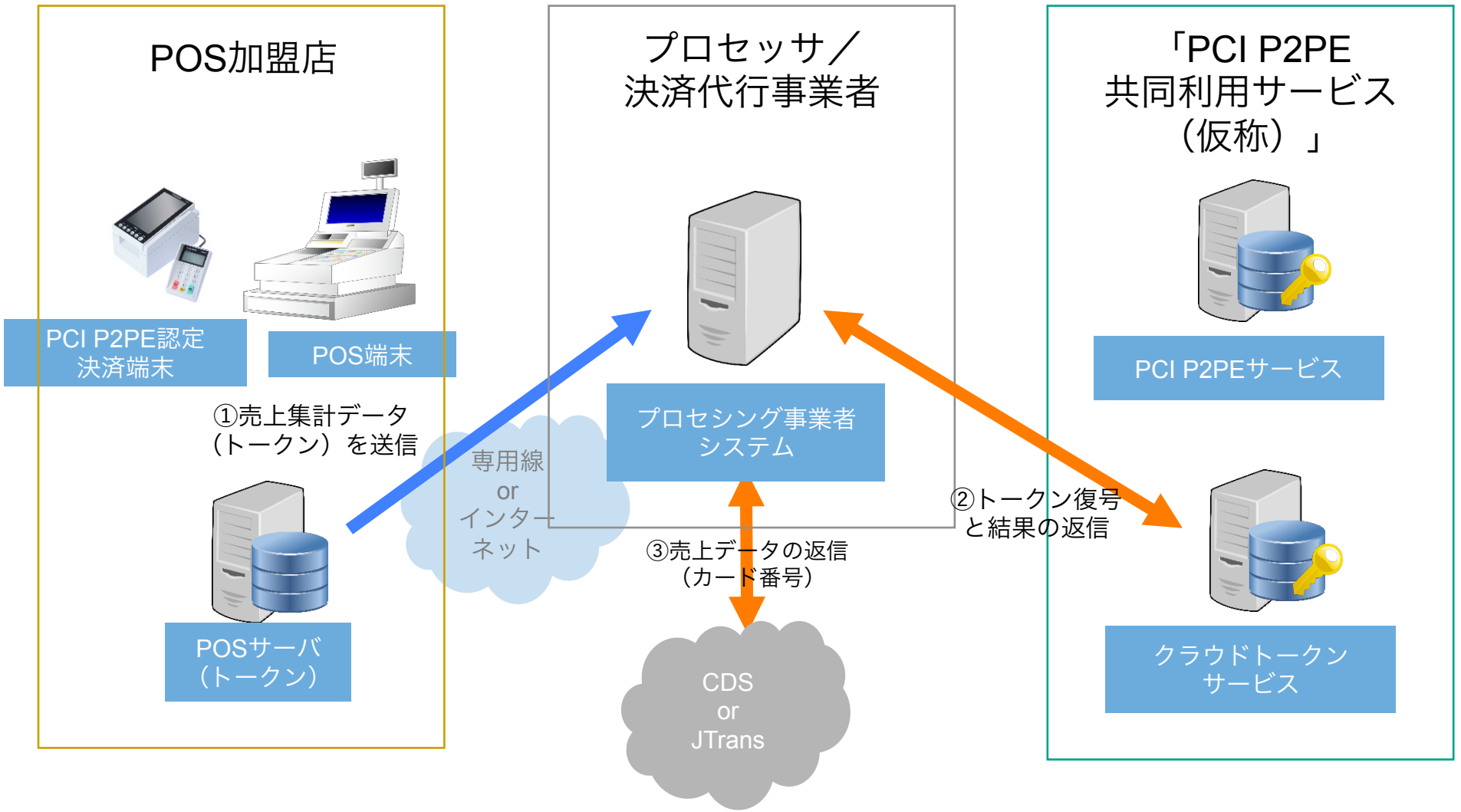
- 現在利用しているプロセッサや決済代行事業者を変更することなくPCI P2PEソリューションの導入が可能
- 希望する決済端末でPCI P2PEに対応することが可能（ただし決済端末はPCI PTS SRED認定が必須）

SRED : Secure Reading and Exchange of Data

PCI P2PE共同利用サービス データフロー（オーソリ）



PCI P2PE共同利用サービス データフロー（売上集計）



まとめ

- プロセッサ／決済代行事業者は、リンクが提供する「PCI P2PE共同利用サービス」（仮称）と接続することで、以下が実現可能です。

  - PCI P2PEの暗号／復号サービスの提供
  - 非ギャザリングを利用している加盟店向けに非保持化同等／相当のセキュリティ措置
  - 本サービスは2019年秋リリース予定

お問い合わせ

株式会社リンク　セキュリティプラットフォーム事業部

TEL　：　03-5785-0555
MAIL　：　spdsales@link.co.jp

PCI DSSに関する旬な情報がご覧いただけます

URL　：　http://www.pcireadycloud.com/

本日はご清聴ありがとうございました。