

カード情報非保持化とBPO事業者向け クラウドサービス

2018/6/22

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
- PCI DSS準拠/非保持化サービスラインナップ
- 改正割賦販売法及び実行計画2018について
- PCI DSS Ready Cloudのご紹介
- カード情報非保持化サービス Pay TGのご紹介



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	48億7,700万円 (2017年5月実績)
従業員数	73名 (2017年5月末現在)
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]



ながほら牧場



サービス沿革

- 2013年5月 PCI DSS Ready Cloudを発表
- 2013年10月 ビジネスモデル特許を出願
- 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10月 非保持化サービス「Pay TG」を発表



カード情報非保持化/PCI DSS準拠を促進させる サービスラインナップ-1

- BPO事業者、中規模システムを保有するお客さま向け
「PCI DSS Ready Cloud プライベートクラウドモデル」
 - ・ カード会社、決済代行事業者、中堅から大規模のEC事業者

- フィンテック事業者、ECカートを保有するお客さま向け
「PCI DSS Ready Cloud AWSモデル」
 - ・ AWSを利用されているフィンテック事業者、ECカート事業者

- 受注処理を行うコールセンターを保有するお客さま向け
「BIZTELコールセンター PCI DSS」
 - ・ 通販事業者/カード会社のコールセンター及びそれらの外部委託先コールセンター事業者



カード情報非保持化/PCI DSS準拠を促進させる サービスラインナップ-2

- 電話・はがき等で受注処理を行う通販加盟店さま向け
カード情報非保持化サービス「Pay TG」
 - ・ 電話/はがき/FAX等で受注処理を行う通販事業者向け

- 大規模システムを保有するお客さま向け
「Cloud Token for Payment Card」
 - ・ POS加盟店、カード会社、大規模な決済代行事業者



改正割賦販売法及び実行計画2018について



6月1日施行 改正割賦販売法 概要

クレジットカードを取り扱う加盟店において、カード情報の適切な管理や不正使用対策を講じることが義務づけられることになりました。改正割賦販売法の施行は2018年6月1日とされております。

改正のポイント	内容
(35条の16) クレジットカード情報の適切な管理等	<ul style="list-style-type: none"> ■ カード情報を盗らせない <ul style="list-style-type: none"> ・ カード情報の非保持化またはPCI DSS準拠の義務 ・ 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	<ul style="list-style-type: none"> ■ 偽造カードを使わせない (※対面取引) <ul style="list-style-type: none"> ・ 決済端末の「100%IC対応」の実現

■ 行政指導や罰則について

行政指導（報告徴収・立入検査）の可能性有り。罰則（懲役・罰金・過料）はなし。（第49条）
 ※ただし、故意にクレジットカード番号等の情報を漏えいした場合は、会社役員や個人に対して罰則有り【3年以下の懲役または50万円以下の罰金】



3月1日に発表された実行計画2018とは

「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」

・以下はその抜粋

各主体	役割
加盟店	<ul style="list-style-type: none"> ・カード情報の非保持化（同等相当含む）またはPCI DSS準拠（対面加盟店は最終的には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 ・EC加盟店の委託先事業者における対策
カード会社・PSP	<ul style="list-style-type: none"> ・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

【実行計画2018 P20~22】 カード情報の適切な保護を推進するためには、カード情報を取り扱う事業者全てが自主的な取組を進めることが重要である。なお、各主体がカード情報を取り扱う業務を外部委託する場合は、委託者自身が委託先のセキュリティ状況を確認し、責任を持ってPCI DSS準拠等の必要な対策を求めていくこととする。また、複数の委託者からカード情報を取り扱う業務を受託する又はショッピングカート機能等のシステムを提供する事業者は、自社システムにおけるカード情報の保持状況について確認の上、PCI DSS準拠等の必要な対策を行うことが求められる。



BPO事業者等中規模システムを保有するお客さま向け

PCI DSS準拠を低コスト/短期間に実現させる

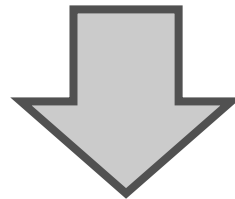
「PCI DSS Ready Cloud」

プライベートクラウドモデル

PCI DSS Ready Cloudのコンセプト①

□ PCI DSSに準拠したクラウドサービス


→ 世界中に多数存在 例) Amazon Web Services/Microsoft Azureなど



□ クラウドサービスを利用する顧客のPCI DSS準拠をイネーブリング（促進）するクラウドサービス

→ 世界初のサービス：  **PCI DSS ReadyCloud**

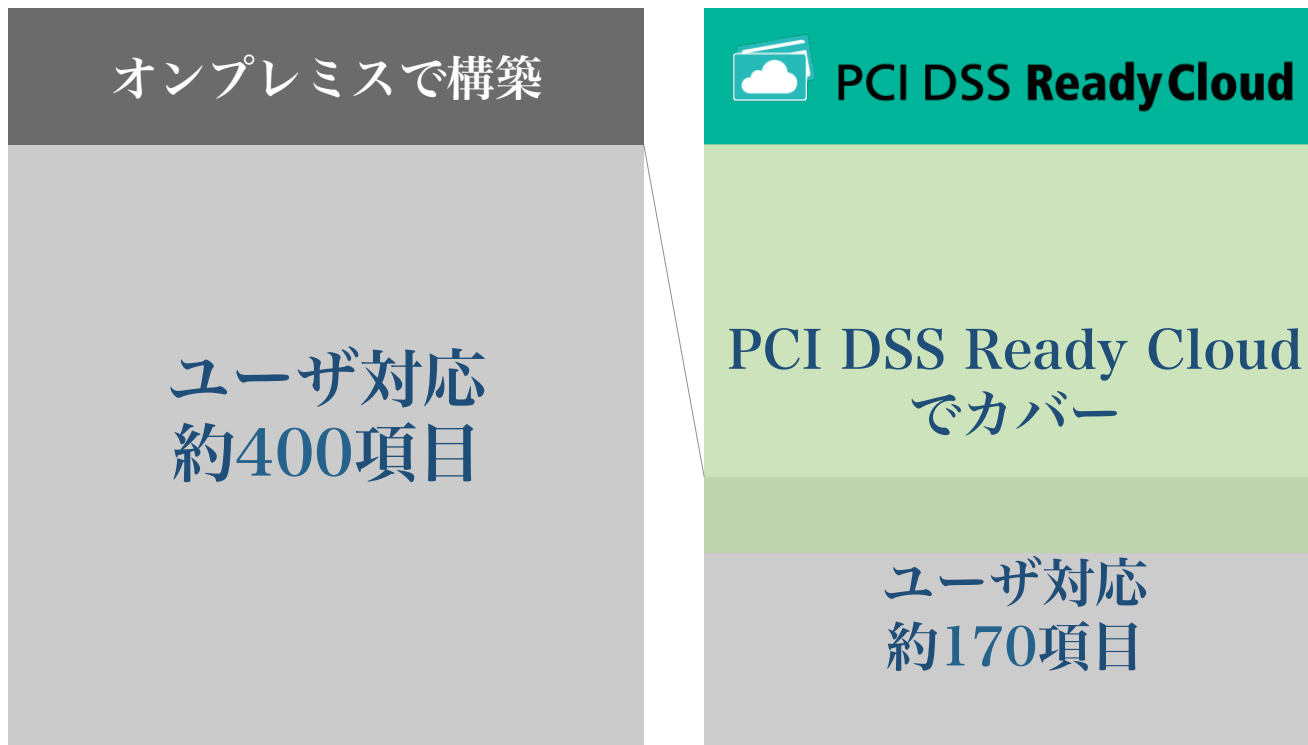
PCI DSS Ready Cloudのコンセプト②

	自身のクラウドサービスの インフラがPCI DSSに準拠	クラウドサービスを利用する 顧客のPCI DSSの準拠を促進
Amazon Web Servicesなど 他社クラウドサービス	○	×
 PCI DSS ReadyCloud	○	○



特長（対応項目比較）

約400項目のPCI DSS要件に対し
オンプレミスと比較して、大幅に対処項目を圧縮





PCI DSS準拠を促進させる仕組み ①

- PCI DSS要件に適合したサービスや仕様を標準で提供
 - ▶ PCI DSSに必要となるセキュリティコンポーネントの標準実装。
個別投資（カスタムアプリケーションは除く）は必要ない。
 - ▶ 環境構築を行う際のツール選定のプロセスが不要
 - ▶ PCI DSSのギャップ分析が不要（カスタムアプリケーションは除く）
 - ▶ OSや各種設定のテンプレート化による、設計プロセスの削減
 - ▶ 手間のかかる関連ベンダコントロールをPCI DSS Ready Cloudに一本化

PCI DSS準拠を促進させる仕組み②

□ PCI DSS準拠を促進させるサポートサイト（ナレッジの提供）





PCI DSS準拠を促進させる仕組み ③

□ PCI DSS準拠のためのコンサルティングを軽減するドキュメント類

The image displays three document covers arranged in a row, each representing a document that reduces consulting for PCI DSS compliance. The first document is the 'PCI DSS Ready Cloud 顧客用 PCI DSS Ver3.1 ガイダンス' (Customer PCI DSS Ver3.1 Guide) dated 2015/12/08. The second is the 'PCI DSS Ready Cloud サービス仕様書' (Service Specification) for '○○○○様' (Mr. OOOO), version Ver4.1, dated 2015/11/11. The third is the 'Payment Card Industry (PCI) Data Security Standard Attestation of Compliance for Onsite Assessments – Service Providers' (Version 3.1, April 2015).

ガイダンスシート

サービス仕様書

準拠証明書



特長（コスト比較）

オンプレミスと比較して圧倒的な低コスト
（サーバ11台の構成で比較）

オンプレミスで構築

初期5,200万円

- インフラ費用他
 - ・ GAP分析等
 - ・ サーバ/ネットワーク
 - ・ ソフトウェア
 - ・ システム設計/構築

- データセンター費用
 - ・ 回線/ラック
 - ・ 監視/運用設定

月次290万円

- インフラ費用
 - ・ ソフトウェア保守
 - ・ ハードウェア保守
 - ・ 運用人件費

- データセンター費用
 - ・ 回線/ラック
 - ・ 24時間 監視/運用



PCI DSS ReadyCloud

初期260万円

月次130万円

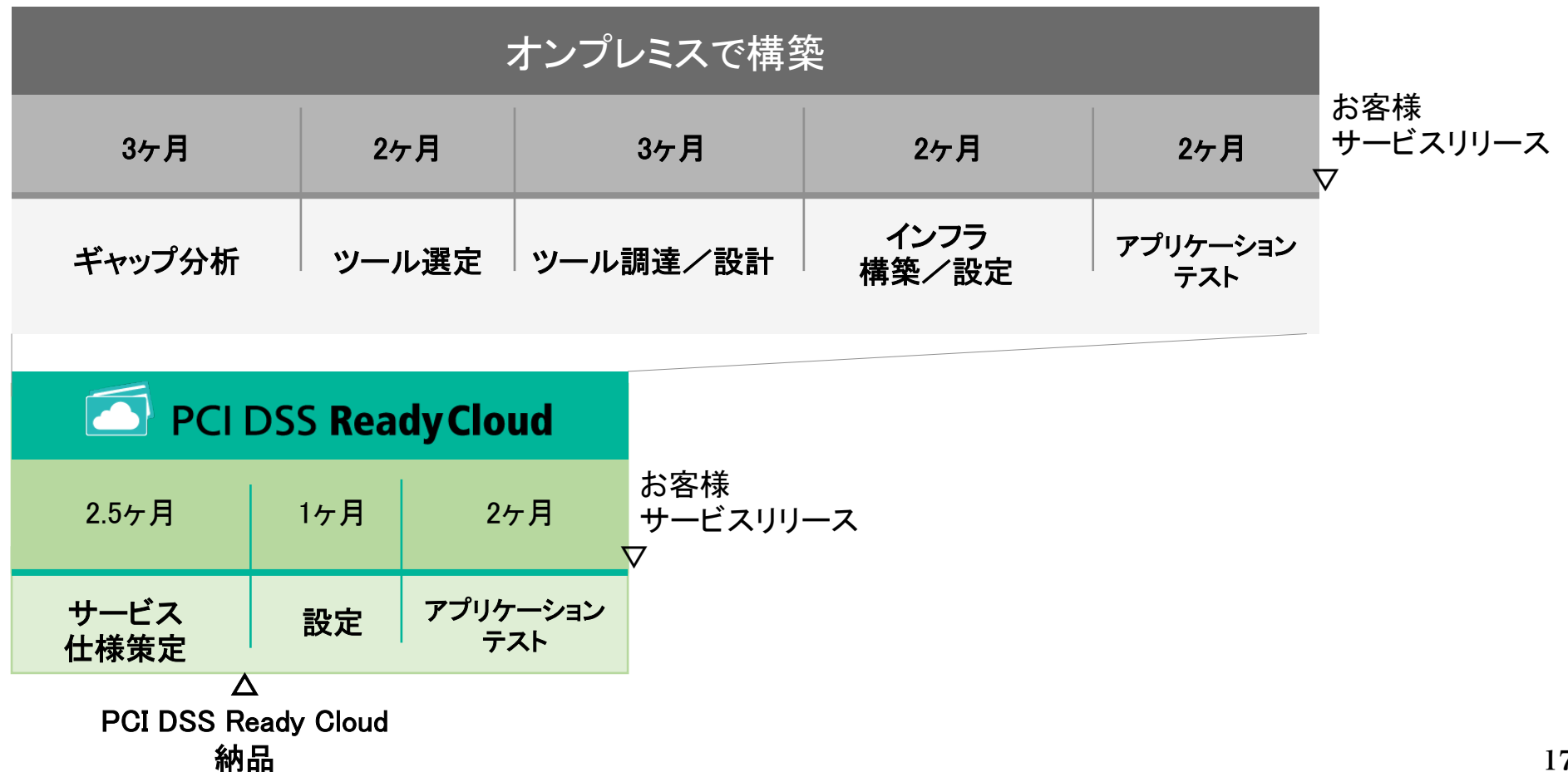
- ※左記同等機能をサービス料金内に含む。
- ※サービス料金以外にお客さま人件費含む

※オンプレミスで構築する場合との比較資料が必要な場合はお問い合わせください。



特長（スケジュール比較）

オンプレミスと比較して圧倒的な短納期





多数のBPO事業者選ばれています

□ BPO事業者サービス概要

- PCI DSS準拠/非保持化のコストを抑制したい、ノウハウに精通した人材が不足するなど課題を持つ企業に向けたBPOサービスを提供
- 電話での決済、カード加盟店の売上集計、データ入力・電子化といった機密性の高い情報を取扱う業務

□ BPO事業者に導入された主なサービス

- PCI DSS Ready Cloud プライベートクラウドモデル
- BIZTEL コールセンターPCI DSS

□ 解決した課題

- ビジネスプランにあったシステム投資
- 「PCI DSS準拠済」BPOサービス開始までのスケジュールを短縮



電話/はがき/FAXオーダーの加盟店向け カード情報非保持化サービス Pay TGのご紹介



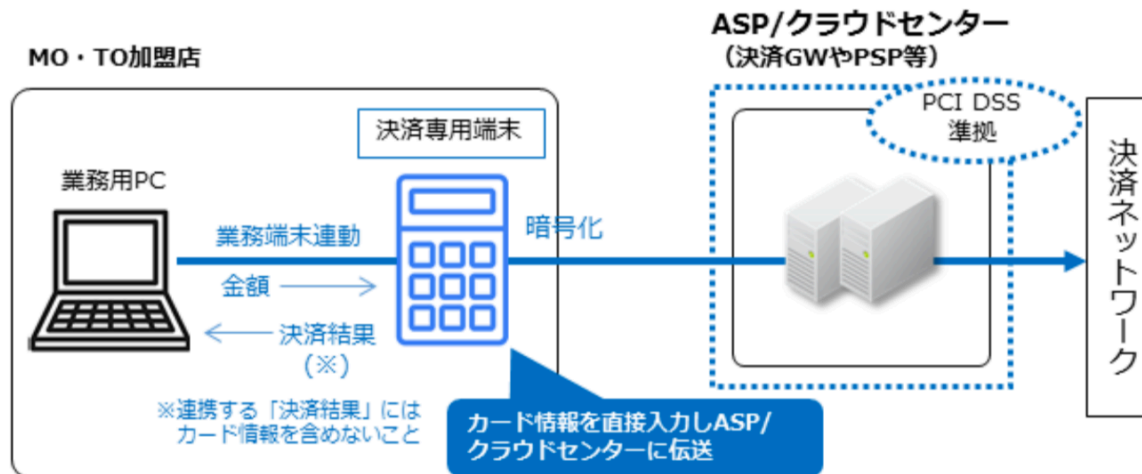
MOTO加盟店 認定非保持化ソリューションとは

【実行計画2018 P13~14】 ② メールオーダー・テレフォンオーダー等の非対面加盟店における非保持化について
 メールオーダー・テレフォンオーダー等の EC 加盟店以外の非対面加盟店(以下「MO・TO 加盟店」という)においては、顧客から電話・FAX・はがき等でカード情報を入力し、MO・TO 加盟店の機器においてカード情報を入力し決済を行うため、カード情報を電磁的情報で自社内に「通過」させない外回り方式を導入することにより、カード情報の非保持を実現することが可能となる。

■外回り方式

カード情報を紙媒体のまま保存する場合や要件を満たした決済専用端末やタブレット端末を活用した外回り方式⁸（自社で保有する機器・ネットワークにおいて、カード情報を「保存」、「処理」、「通過」しない）にて決済を行う場合には、非保持となる。

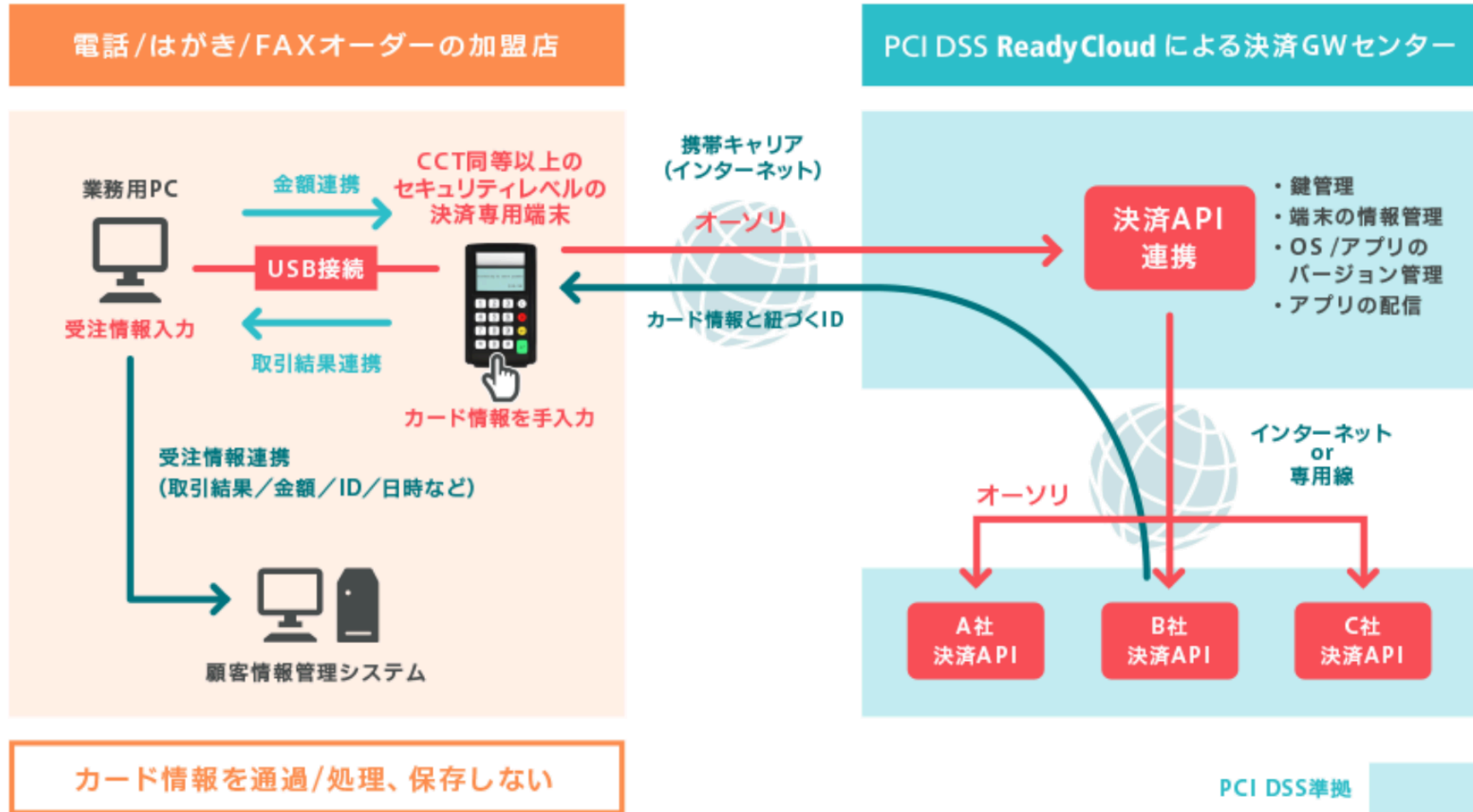
【外回り方式（決済専用端末を利用した方式）】



※ASP は Application Service Provider の略



電話/はがき/FAXで受注処理を行う加盟店向け カード情報非保持化サービス「Pay TG」概要





カード情報非保持化サービス「Pay TG」の特長①

カード情報の非保持化を実現

PCI PTSの認定済のCCT同等以上のセキュリティレベルの決済専用端末を当社から貸与します。外回り決済を実現し、加盟店内の業務端末では正規のカード情報を電磁的に通過/処理/保存されません。



カード情報非保持化サービス「Pay TG」の特長②

既存の決済代行事業者を利用可能

本サービスを利用するにあたり、現在利用されている決済代行事業者を変更する必要はございません。そのまま継続利用することが可能です。



カード情報非保持化サービス「Pay TG」の特長③

ECと同様の決済フローを実現

決済結果や金額、カード番号と紐付くIDを受注システムと関係する仕組みを提供することにより、ECと同様の決済フローを実現しています。



カード情報非保持化サービス「Pay TG」の特長④

業務用PCと金額連携する仕組み

決済結果や金額、カード番号と紐付くIDを受注システムと連携する仕組みを提供することにより、金額の二度打ち等、オペレーション上の手間を発生させない設計を実現しています。



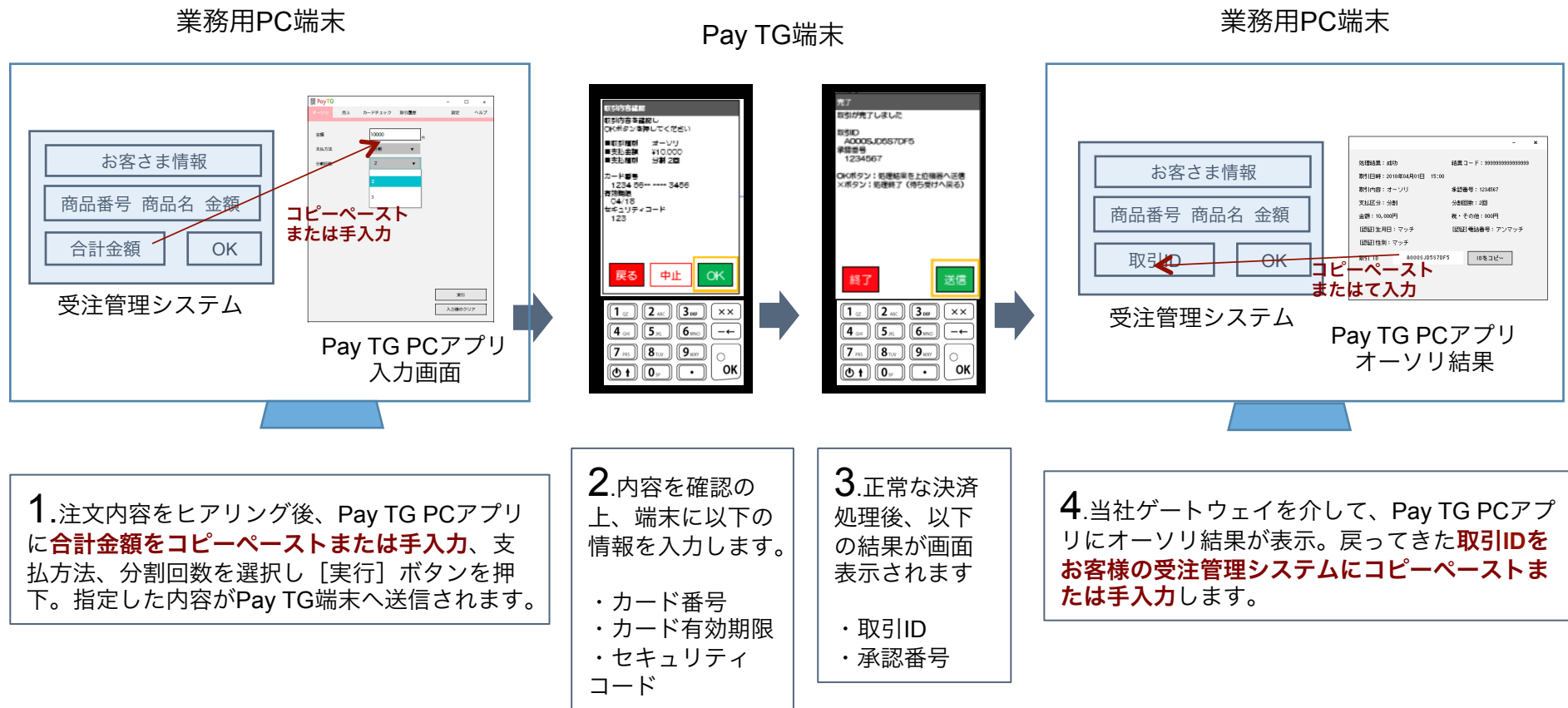
「Pay TG」実装機能概要

- オーソリ
- オーソリ売上
- カード有効性チェック
- カード情報お預かりサービス

※各決済代行事業者が提供するサービスに準じます。



Pay TG PCアプリ利用をし、オーソリ処理から取引IDを受注管理システムに登録する場合の想定イメージ図



※取引結果はPay TG PCアプリの機能でCSVデータとして一括ダウンロードする事も可能です。
 ※上記仕様は開発中の為、変更になる可能性があります。



Pay TG API利用をし、オーソリ処理から取引結果を受注管理システムと連携する場合の想定イメージ図



1.実行ボタンで以下のデータを決済ゲートウェイに送信します。

【送信内容】

- ・トランザクションID
- ・処理カテゴリ
- ・取引ID
- ・取引日付
- ・合計金額
- ・支払区分
- ・支払回数

2.内容を確認の上、端末に以下の情報を入力します。

- ・カード番号
- ・カード有効期限
- ・セキュリティコード

3.正常な決済処理後、以下の結果が画面表示されます

- ・取引ID
- ・承認番号

4.受注管理システムに結果を受け渡します。

【受信内容】

- ・処理結果コード
- ・詳細結果コード
- ・エラーメッセージ
- ・取引ID
- ・応答承認番号
- ・決済GWエラーコード
- ・決済GWエラーメッセージ
- ・端末から電文を受信した時刻
- ・端末へ電文を送信した時刻

※API仕様書はNDA締結後ご提供します。



Pay TG PCアプリケーション仕様

- 対応OS : Windows OS 7、8.1、10
(Windows7および8の場合はUSBドライバーのインストールが必要)
- ディスク容量 : 最大300M 以上
- CPU : 1GHz 以上
- メモリ : 1GB 以上の空き
- USBポート : USB1.1以上

※Pay TG端末は受注処理用PCと1対1でペアリング認証します。

※仮想環境では動作保証いたしません



Pay TG 端末仕様

VEGA3000 Touch		据置型 LTE モジュール搭載モデル
プロセッサ		32 ビット ハイパフォーマンス セキュア マイクロプロセッサ @ 400MHz
メモリ		128MB
ディスプレイ		3.5 インチバックライト搭載 カラー-TFT タッチ液晶 320×480 ピクセル
プリンタ		ロール紙幅/直径：57mm/50mm 印刷速度：100mm/秒
タッチスクリーン		搭載
カードリーダー部	磁気ストライプ	ISO 7810,7811 & 7813 3トラック片面リーダー / Bi-Directional
	接触カード	ISO 7816 ID-1 1.8 V/3V/5V T=0,T=1
	SAM Card	2
	非接触カード (オプション)	ISO14443 TypeA,B, ISO 18092 NFC and Mifare & SONY FeliCa Working Frequency 13.56MHz
	Dual SIM	YES
通信インターフェース		UMTS, GPRS, CDMA, Wi-Fi,(Bluetooth)Ethernet
接続インターフェース		Ethernet,Dial-up Modem,RS232C*2,USB*2
インジケータ	Speaker	搭載
	Audio Buzzer	搭載
キーパッド		Standard Keys 15

AC/DC		DC 9V/4A
サイズ		190mm(長さ)×78mm(幅)×78mm(高さ)
重量		350g
使用環境	温度：動作時	0℃ to 50℃
	温度：保管時	-20℃ to 70℃
	湿度：動作時	5% to 90% (結露なし)
	湿度：保管時	5% to 95% (結露なし)
認定	セキュリティ と 決済ブランド 認定	PCI PTS, EMV L1 L2,TQM,PBOC L1 L2, Visa payWave, MasterCard PayPass, AMEX ExpressPay,JCB J/Speedy, FeliCa,Interac Flash, UnionPay UICS, Discover D-PAS
	安全性・ 電磁両立性	CE,FCC,BSMI,RoHS
ソフトウェア		SDK,KMS,TMS,GDB,CTOS library,ISO 8583 library, Crypto library
暗号化鍵		TRNG,DES,T'DES,AES,RSA,MK/SK,DUKPT,T'DES DUKPT



Pay TG 接続先決済代行事業者について



※掲載されていない決済代行事業者は個別にお問い合わせください。

Pay TG導入事例

- 大手旅行代理店 受注センター
導入台数：80台
複数拠点利用の場合でのコスト抑制を評価

- スキンケア商品 受注センター
導入台数：10台
コンプライアンス（6/1改正割賦販売法への対応）

- 定期購読（新聞、雑誌）サービスセンター
導入台数：10台
運用方法を変更する必要がない点を評価

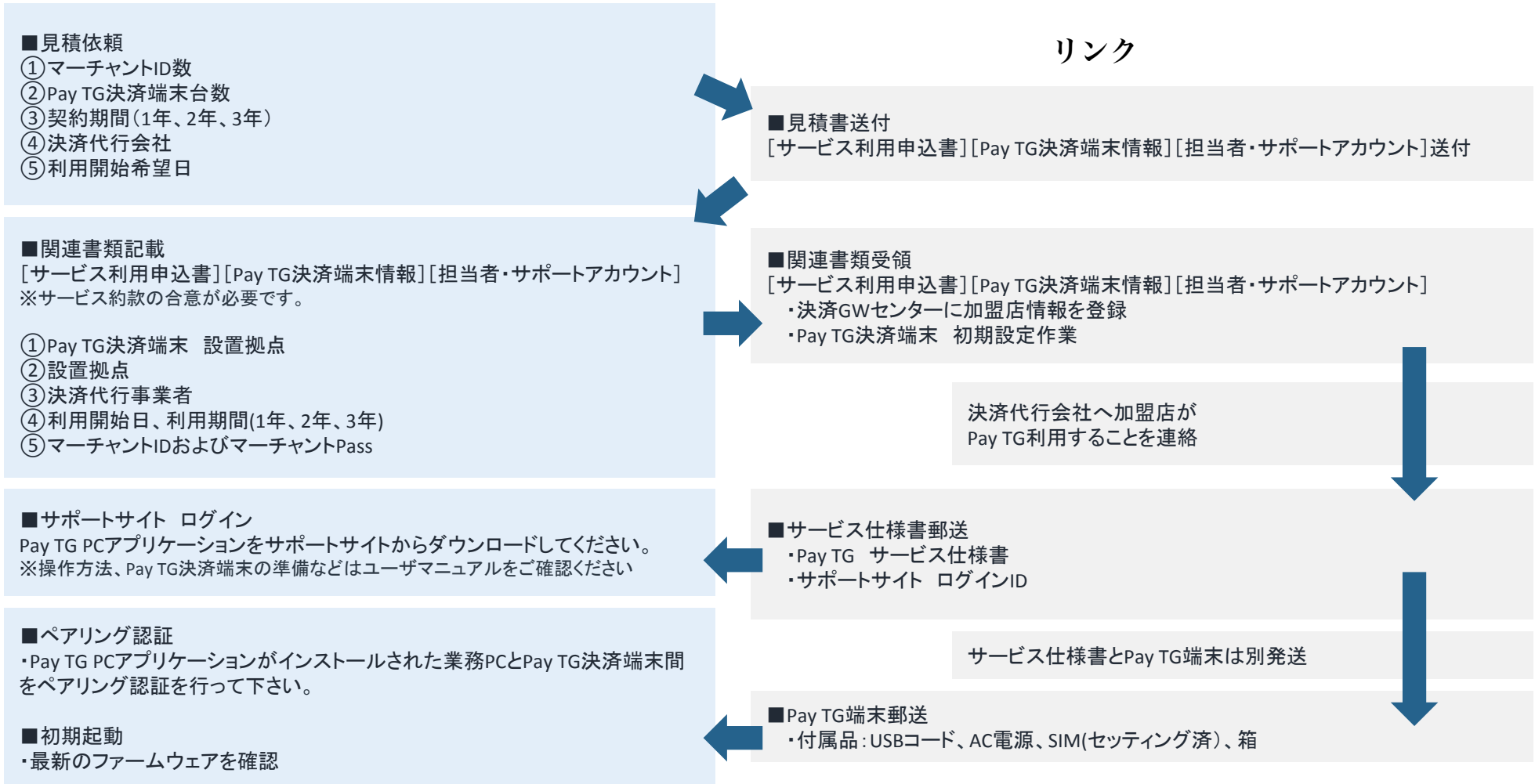
- ISP事業者 コールセンター
導入台数：70台
タブレットと比較・検討して運用面で優れていると判断したため



申込から利用開始までの手順

お客様

リンク



お客様の顧客情報管理システムとPay TGをAPI接続する場合は、別途お客様のカスタマイズが必要です。



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 : 03-6406-4639

FAX : 03-5785-2277

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/>