

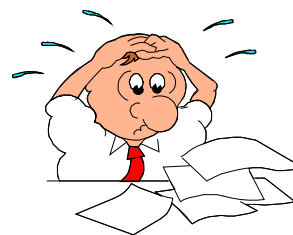
## PCIDSS対応・非保持化の質問・疑問にお答え

### 【パネラー】

NTTデータ先端技術株式会社 セキュリティ事業部  
セキュリティコンサルティング担当  
池谷 陽 (QSA・PA-QSA(P2PE))

株式会社サン・パートナーズ  
常務取締役 シニアコンサルタント  
櫻井 智恵 (ISA・PCIP)

【司会】 JCDSC事務局 森 大吾  
(日本オフィス・システム株式会社)



Copyright 2018 © JCDSC

## 1. カードの取り扱いによっては非保持にならない？

①店舗で、店員がお客様のカードを受け取って、決済端末で決済してお返しするという動作は、**加盟店側が「カードを取り扱う」**行為に当たると思います。非保持と認められますか？

②店舗で、お客様のカードを決済端末に通した際に、**読み取りエラー**になってしまうことがあります。  
やむを得ず臨時の方法として、決済端末に**店員がカード番号を手入力**して、決済を行っています。

これでは「非保持」と言えなくなってしまうのでしょうか。



## 2. お客様からカード番号をお聴きすることがある

非保持化を達成できた通信販売加盟店です。

注文を受けてカード決済が完了したあと、お客様からキャンセルや商品交換のクレームが入ることがあります。

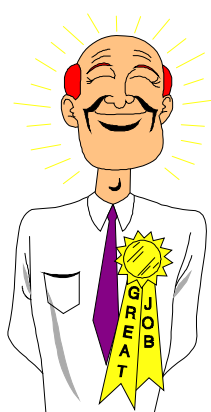
売上データの修正も発生しますので、お客様からカード番号をお聴きして、決済代行会社へ連絡する必要があります。

この行為は、非保持の範囲として認められますか？



## 3. カード情報非保持化達成の認定は？

カード会社から実行計画対応状況の調査が来たので、「非保持化を完了済みです」と回答しました。



当社としては非保持化できたと考えていても、技術的に細かな点でも確かなのか、また後日にカード会社から詳しく尋ねられると、心配があります。

加盟店が非保持化対応済みであることを、PCI DSSのQSA審査のように、第三者機関によって認定する仕組みはありますか？

## 4. 多要素認証にしなければならない判断基準は？

PCI DSSで、CDE(対象となるカード会員データ環境)へのアクセスには、多要素認証が必要とされています。  
たとえば次のケースでは、多要素認証は必要でしょうか。

- ①加盟店向けに、決済状況等を確認できるWEBサイトを提供して、ログインさせる場合
- ②WEBサーバーのOSに対して、コマンドを実行するために、ログインする場合

多要素認証でなくてもよい場合・必須の場合を、**どのような基準で区別**すればよいかを教えてください。

## 5. ポイント機能つきクレジットカードが増えている

近年、ポイントカード機能付きのクレジットカードが増えています。

お客様は現金支払いなのに、POSレジでこの磁気カードを読み取ると、**必要のないクレジットカードの情報も**同時に読み込んでしまいます。

この場合、PCI DSS対応または**P2PE対応のシステム構成**を導入するか、ポイント処理も外付端末で読み取るなど、新たなシステム開発を行う必要があるでしょうか？

また、**クレジットカードの取扱いをしていない商店**が、ポイント併用カードを読み取れば、非保持化対策をしないと**改正割賦販売法に違反**したことになるのでしょうか？

## 6. IVRで加盟店側が代理送信してよいか

MOTOの通販加盟店です。非保持化のために電話自動応答システム(IVR)を導入したのですが、**年配のお客様の場合**いろいろ不都合があり、購入をあきらめてしまいます。

- ・アナログ電話をプッシュトーンに切り替えるアスタリスクボタンの説明が分からない。
- ・スマートホンを使ってはいても、数字キーを表示してキー操作をする方法が分からない。

コールセンターのスタッフが電話でカード番号を聞き取って、**代理でIVRに入力する**方法は、非保持の範囲に認められるでしょうか？



## 7. サービスプロバイダーはPCI DSS必須か

加盟店から委託を受けているサービスプロバイダーは、非保持化対応は認められますか？「実行計画2018」を読んでもよく分かりません。

P19で、**カード会社及びPSPについては、(中略)PCI DSS 準拠は当然の責務である。(中略)なお、カード会社・PSP以外のカード情報を取り扱っている事業者も同様である。**と書かれていますから、**サービスプロバイダーはPCI DSS必須と読めます。**

いっぽうP20では、**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。**と書いてあり、PCI DSS「等」ですから、PCI DSS以外の対策でも認められると読めます。

- ①サービスプロバイダーはPCI DSS必須ですか、または「等」の対策として**加盟店と同様の非保持化の対策や、ISMSの認証**でもよいのでしょうか。
- ②「等」の方策として、多くのものが考えられますが、それでよいかどうかは誰が判断するのでしょうか。

## 8. カード会社の委託先はPCI DSSが必須か

カード会社から、紙媒体に記載されたカード番号の入力をする、業務の委託を受けています。

カード会社はPCI DSS準拠が必須なので、委託先である当社もPCI DSSに準拠するよう、指示がきています。

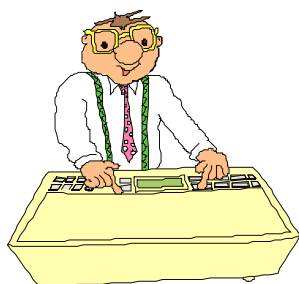
業務委託先もPCI DSS準拠していないと、カード会社はPCI DSSに準拠できないのでしょうか。



## 9. 紙をスキャンしたPDFは非保持でOKのはずだが

「実行計画2018」で、カード番号などが書かれている紙の申込書を、スキャン画像にしたPDFファイルは、非保持の範囲に認めると聞いています。

このPDFを、メール添付で委託元などへ送信してもよいですか。  
パスワード保護を行います。



## 10. 外部のデータセンターがQSA監査に応じてくれない

PCI DSS準拠に取り組んでいるのですが、カード情報の保存サーバーが、契約している外部のデータセンターであったり、クラウド事業者を利用したりしている場合、それらはQSAの審査を受け入れてくれません。

当社がPCI DSSに準拠するにはどうしたらよいですか。

