山岡レポート：PCI DSS の現場から（5）

対面加盟店での クレジットカード不正利用対策

NTT データ先端技術株式会社
取締役執行役員 CISO
セキュリティ事業部長　**山岡 正輝**
博士（工学）

2020 年オリンピック・パラリンピック東京大会にむけて、日本政府はキャッシュレス化の推進を重要な政策課題と位置付けている。2016 年 12 月には、改正割賦販売法が成立し、クレジットカード会社だけではなく加盟店にもカード情報の保護が義務化された。国内のクレジットカード業界で、いま、何が起こっているのか、その一端を現場からレポートする。

POS 端末でのクレジットカード情報の取り扱い

前回までのレポートでふれたように、店員とクレジットカード保有者が対面して決済が行われる対面加盟店で、POS システムを介してカード情報を取り扱う内回り方式（図 1 参照）を採用している場合、PCI P2PE（Point-to-Point Encryption）と呼ばれるカード情報を暗号化する技術を備えたソリューションを導入することで、「非保持化と同等／相当のセキュリティ措置」を実行したものとみなされ、クレジットカードセキュリティに関する加盟店の負担が軽減される。

P2PE では、加盟店に設置されているカードからデータを読み取る装置（POI（Point of Interaction）デバイス）で読み取ったカード情報を直ちに暗号化し、決済 GW 等の安全な復号環境へ送達するまでカード情報を復号化しない。暗号でデータを保護する方式が P2PE の技術的なポイントとなる。

POI デバイスには、POI デバイス内のファームウェアに埋め込まれたデータを暗号化するための SRED（Secure Reading and Exchange of Data）機能が内蔵されており、クレジットカード情報を読み取った時点で直ちに暗号化することが可能となっている。

また、暗号化されたカード情報は、内回り方式で加盟店の店舗内 POS 端末や POS サーバを通過する際にも暗号化されており、加盟店の従業員でさえもカード情報を復号して読み取ることはできない仕組みになっている。

POS 端末に感染するマルウェア対策

これまでに、海外のみならず国内においても、POS 端末に感染するマルウェアが確認されている。

アンチウイルスソフトの利用など対策は進んでいるが、POI デバイスから読み取られたカード情報が POS 端末内を平文の状態で通過あるいは処理されると、メモリスクレイピングと呼ばれる POS 端末内のメモリ上から情報を盗み取る攻撃に対して脆弱となってしまう。

前述したように、P2PE では、POS 端末はカードリーダー等の POI デバイスで暗号化されたデータを扱う仕組みとなっているため、これらの脆弱性が低減される。そのため、P2PE は、POS 端末に感染するマルウェアに対する有効な対策といわれている。

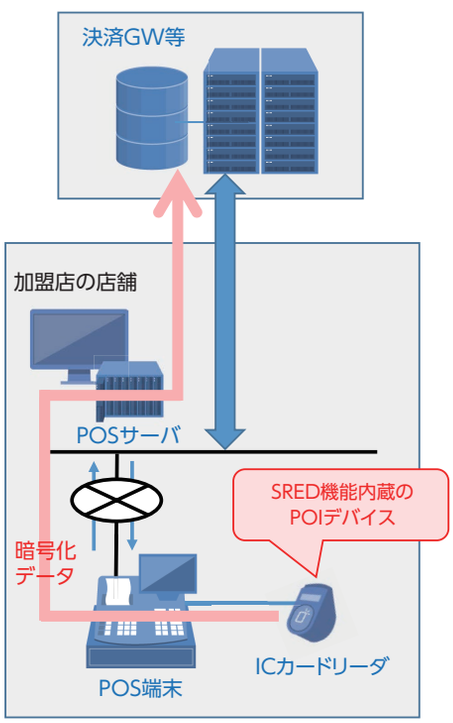

図 1 ：対面加盟店での「内回り方式」
（参考：「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画 -2018-」）

PCI P2PE セキュリティ基準

VISA 等の国際ブランド 5 社が設立した PCI SSC 協議会（Payment Card Industry Security Standards Council）は、P2PE に関するセキュリティ基準（Point-to-Point Encryption Requirements and Testing Procedures）を定めている。

基準は、表 1 に示す 6 個のドメインから構成されており、例えば、ドメイン 1 の「暗号化デバイスとアプリケーション管理」では、PCI 認定の SRED 対応 POI デバイスを使用することが、要件の一つとして定められている。また、そのテスト手順についても定められている。

PCI P2PE で利用されている基本的な技術は、エンドエンドで情報を暗号化して送信する仕組みであり、暗号鍵の管理方法が一番のポイントとなる。そのため、P2PE に関するセキュリティ基準は、運用管理に関する要件が多いのが特徴となっている。特に、暗号鍵の管理に関する検証要件が多く、POI デバイスへの暗号鍵の埋め込みや暗号鍵をリモートで POI デバイスに配信する際に適用される要件なども定められている。

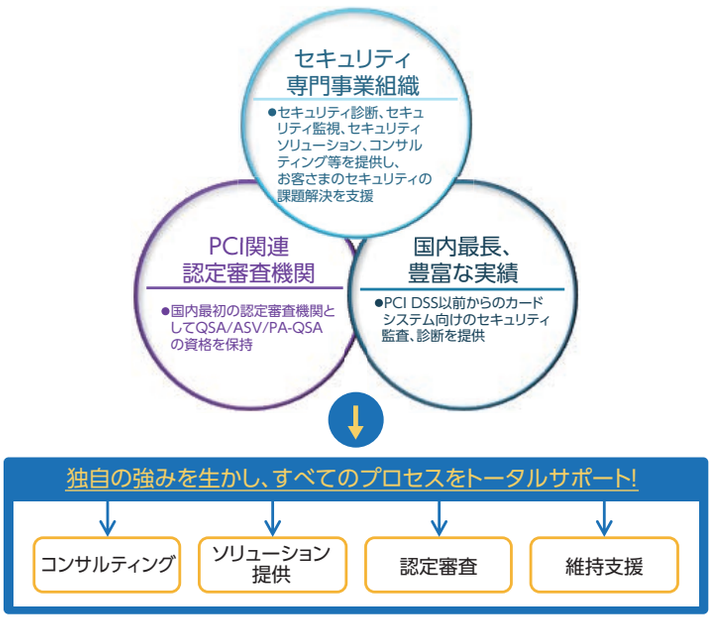

図 2　NTT データ先端技術の PCI DSS 事業の強み

PCI DSS における NTT データ先端技術の強み

P2PE ソリューションプロバイダー等に対するインタビューやドキュメント調査、システム設定調査等の審査を正式に行うことができる機関を、PCI SSC 協議会が認定する制度がある。

表 1 に示した 6 つのドメインのうち、特にドメイン 2「アプリケーションのセキュリティ」の評価を行うには「PA-QSA（P2PE）」の資格が必要となる。NTT データ先端技術は、2017 年 3 月、この資格を有する国内初の審査機関となった。さらに、NTT データ先端技術は、P2PE アプリケーションを開発するベンダーに対する審査を行う「QSA（P2PE）」の資格も有しており、審査機関としても登録されている。

NTT データ先端技術は、セキュリティコンサルティングや診断、監視、インシデントレスポンス、ソリューション提供等を行う「セキュリティ専門事業組織」をもっている。また、PCI DSS に関しては、「認定審査機関」という顔をもっており、実績も豊富である。PCI DSS のフレームワーク検討段階から監査に関する事業をスタートさせ、「コンサルティング、ソリューション提供、認定審査、維持支援」まで、PCI　DSS に関するすべてのプロセスをサポートする体制を整え、多くのお客様にご満足いただいている（図 2 参照）。

<PCI DSS のことなら下記へ>
sec-info@intellilink.co.jp

表 1　PCI Point-to-Point Encryption のためのソリューション要件

	ドメイン	概要	検証要件数
1	暗号化デバイスとアプリケーション管理	PCI認定POIデバイスと内蔵ソフトウェアの安全な管理	5
2	アプリケーションのセキュリティ	平文アカウントデータにアクセスを行うPCI承認POI端末専用ペイメントアプリケーションのセキュアな開発	3
3	P2PEソリューション管理	サードパーティとの関係、インシデント対応、P2PE取扱説明書(PIM)など、ソリューションプロバイダによるP2PEソリューションの全体的な管理	3
4	加盟店管理ソリューション	加盟店の暗号化、復号環境間の役割と機能を分離	3
5	復号環境	暗号化されたアカウントデータを受信し復号する環境のセキュアな管理	5
6	P2PE暗号鍵の運用とデバイスの管理	アカウントデータ暗号化POI端末と復号HSMに鍵管理運用手順を確立し実施	9