P2PEによって新たな局面を迎えるクレジットカード決済

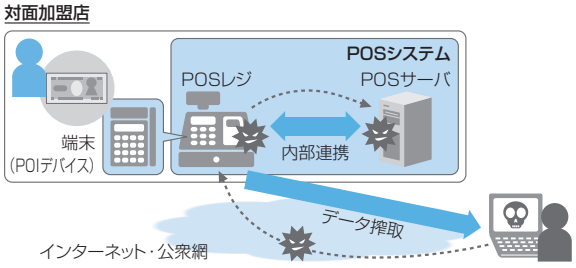
2020年の東京五輪を控え、政府主導のもと、クレジットカード取引の普及とセキュリティ強化に向けた様々な施策が進められている。このような状況の中、特に対面加盟店（店舗）でのクレジットカード決済におけるセキュリティ強化に大きな効果が期待される「P2PE」ソリューションが注目されている。

対面加盟店（店舗）での決済のセキュリティ事情

近年、対面加盟店（店舗）におけるクレジットカード情報の大規模な漏洩事件が発生している。2013年末には、米国の大手流通チェーンTarget社において数千万件にも及ぶクレジットカード情報の大量漏洩事件が発生し、大きな話題となった[1)]。手口としては店舗のPOSシステム[2)]の脆弱性を突いた攻撃によってマルウェアを仕込まれ、クレジットカード情報が不正に大量搾取されたものである。以降、日本でも同様の手口による事件が複数確認されており、もはや対岸の火事ではない。特に対面加盟店ではこれまで業務的な理由によってクレジットカード情報を平文（暗号化されていない状態）で扱うなど、POSシステムの脆弱性を突かれた際の情報漏洩リスクを有しているケースが多かった。

日本国内の制度情勢に目を向けると、2016年2月にクレジット取引セキュリティ対策協議会より発表された『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－2016－』において、クレジットカード情報を取り扱う事業者が順守すべきセキュリティ基準であるPCI DSS[3)]等への対応期限が明確化された[4)]。対面加盟店では、これまで業務上の理由や対策に掛るコスト等が大きなネックとなり、クレジットカード発行会社や決済代行会社に比べ、これらのセキュリティ対応が後手に回っていたが、クレジットカード情報保護のための対策は今や喫緊の課題となっているのである。

図表1　対面加盟店のPOSシステムからの情報漏洩（イメージ）



（出所）NRIセキュアテクノロジーズ

P2PEの概要と「PCI P2PE」基準について

対面加盟店にとってのセキュリティ上の課題をいち早く解決へと導く手段として、「P2PE」が注目されている。P2PEとは、Point-to-Point Encryptionの略で、クレジットカード情報を読み取る端末から決済ネットワークに至るまで、クレジットカード情報を一気通貫で暗号化した状態で処理するソリューションのことである。

一般に、P2PEのソリューションは、暗号化処理を行う端末と復号処理を実施するセンターから構成される[5)]。クレジットカード情報を読み取る端末は対面加盟店内に設置されるが、端末とセンターを含めた提供形態が、P2PEソリューションと見做される。また、P2PEソリューションにおいて、端末として具体的な対象となるのは、POSレジ（店舗のレジ端末）に接続あるいは組み込まれたPOIデバイス[6)]のみであり、この部分がクレジットカード情報を読み取るためのカードリーダーに相当する。このPOIデバイスにはSRED[7)]という機能が内蔵され、これによりクレジットカード情報を読み取った瞬間に暗号化することが可能となる。

P2PEソリューションによって対面加盟店にもたらされる効果としては、大きく以下の2点が挙げられる。

①情報漏洩リスクの縮小（セキュリティ面）：POSレジ

NOTE

1) 2013年に、無線LANの脆弱性を突いた攻撃により外部から店舗のPOSシステムにマルウェアが侵入し、約4000万件に及ぶクレジットカード情報やその他の個人情報がハッキングされた。
2) Point Of Saleの略称。対面加盟店（店舗）におけるPOSレジやPOSサーバー等が含まれ、物品販売の売上実績に関わる集計管理等を行うシステム。
3) Payment Card Industry Data Security Standardの略称。クレジットカードを取り扱う事業者（加盟店、サービスプロバイダー）が、会員データの情報保護を目的に制定し、国際カードブランド5社が共同で設立したPCI SSC（注8参照）により運用・管理されている国際的な情報セキュリティの基準のこと。
4) 対面加盟店におけるクレジットカード情報の非保持化またはPCI DSS準拠の完了期限が、2020年3月末に設定された。
5) このソリューションを提供するITサービス会社は、「P2PEソリューションプロバイダー」と呼ばれる。
6) Point Of Interactionの略称。対面加盟店（店舗）におけるクレジットカード決済端末のこと。クレジットカード情報を読み取るためのカードリーダーに相当する。
7) Secure Reading and Exchange of Dataの略称。POIデバイス内のファームウェアに埋め込まれたデータ暗号化を行うための機能。
8) Payment Card Industry Security Standards Council, LLC.の略称。国際クレジットカードブランド会社5社（VISA、MasterCard、JCB、American Express、Discover）が設立した、クレジットカードのセキュリティ基準の開発、管理、教育、および認知を実施する有限責任会社。
9) NRIセキュアテクノロジーズは、2016年7月、「P2PEソリューション」の評価機関「P2PE QSA」として認定された。

上に、クレジットカード情報を一切残さない。

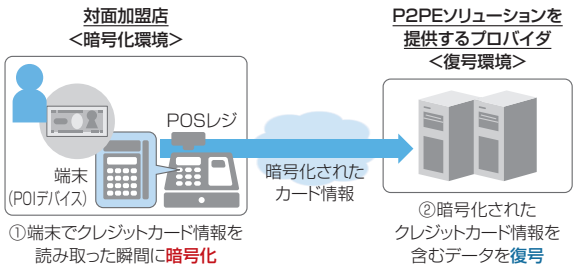
②対面加盟店の運用負荷の低減（運用面）：端末のセキュリティ管理（暗号鍵管理、脆弱性対応）等は、P2PEソリューションプロバイダーが責任を負う。

対面加盟店にとっては、安全かつ効率的にクレジットカード情報を扱えるため、導入のメリットが大きい。

P2PEソリューションについては、PCI SSC[8]がセキュリティ基準として「PCI P2PE」を定めている。本基準の特徴は、システム的な機能要件以上にP2PEソリューションの管理・運用に関する要件が多い点である。中でも最も考慮すべきは「暗号鍵」の管理である。PCI P2PEでは要件の規模がPCI DSSの約3〜4倍となるが、その半数以上が暗号／復号に用いる暗号鍵に関わる要求事項であり、暗号鍵のライフサイクル（生成・導入・利用・廃棄）を通じた管理要件を始め、端末への暗号鍵を埋め込む方法や施設の物理的な要件も詳細に定められている。

また、PCI P2PEとPCI DSSとの関連性では特筆すべきポイントがある。対面加盟店がPCI P2PE認定ソリューションへ完全移行した場合、対面加盟店としてPCI DSS対応を行う際の対象要件が大幅に削減されるのである。対面加盟店がPCI DSSに一から準拠しようとすると、約400項目にも及ぶ要件を満たす必要があるが、PCI P2PE認定ソリューションを導入すれば対面加盟店の満たすべき要件は最少10分の1以下にまで縮小される。これは対面加盟店のPCI DSS対応において大きな効果をもたらすことになる。

図表2　P2PEソリューションのイメージ



（出所）NRIセキュアテクノロジーズ

今後の展望とIoT時代へ向けた期待感

制度情勢に促される面もあって、PCI P2PE認定ソリューションに対するニーズは日々高まっている。日本国内にPCI P2PE認定ソリューションを提供するITサービス会社が未だ存在しない状況の中、各ITサービス会社は、いち早く国内の対面加盟店に対してPCI P2PE認定ソリューションを提供すべく、対応を急いでいる[9]。

一方で、PCI P2PEの本質的要素に目を向けると、情報を暗号化して流通させる仕組みにおいて、暗号鍵の管理方法が文字通り「鍵」となることは論を待たない。IoT時代を迎え、今後、大量のデバイスがネットワークに接続されると、デバイス毎の情報保護や認証用の暗号鍵が埋め込まれるようになる。P2PEソリューションにおける端末もいわば「IoTデバイス」の一種であり、それらの管理方法を網羅的かつ詳細に規定したPCI P2PEは、クレジットカード決済以外の分野においても一つの基準となりえる。今後の社会におけるデバイス管理のための体制を構築し運用規定を定める際には、非常に重要なリファレンスとして活用されることも期待される。

Writer's Profile

須田 直亮 Naoaki Suda
NRIセキュアテクノロジーズ
主任セキュリティコンサルタント
専門は情報セキュリティ全般に関するコンサルティング
focus@nri.co.jp