山岡レポート：PCI DSS の現場から（2）

クレジットカード加盟店に求められるセキュリティ対策

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、先月号に引き続き、その一端を現場からレポートする。

クレジットカードで守るべきカード情報

クレジットカードで守るべき「カード情報」には以下のものがある。クレジットカード番号（PAN: Primary Account Number）、クレジット会員名、サービスコード、有効期限、セキュリティコード、暗証番号 PIN（PIN:Personal Identification Number）、そして、カード情報を含む全トラックデータである（図 1 参照）。これらのうち、クレジットカード番号はカード会員を識別する番号で、最も重要な情報となる。最大 19 桁までの数字列からなり、チェック・デジットがついている。暗証番号 PIN は、サインの代わりに本人確認に使用される。セキュリティコードは、カード署名欄の右上あるいはカード表面に記録された 3 桁数字で、CVV（Card Verification Value）などと呼ばれている。磁気ストライプデータには含まれていない。そのため、スキミングなどにより磁気データを丸ごとコピーされても、オンライン決済でこのセキュリティコードの入力を求めることにより、不正利用を防ぐことができる。サービスコードは、カードが国外で使えるのかなどが規定されているコードになる。

カード情報を守る実行計画とは

2018 年 6 月 1 日に施行された改正割賦販売法では、クレジットカードを取り扱う加盟店に対して、これらのカード情報を適切に管理することが義務づけられた。

具体的な内容は、「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、実行計画）」に示されている。クレジット取引セキュリティ対策協議会が作成し、年度毎で更新されている。

実行計画には、大きく以下の 3 つの対策が記載されている。

（1）カード情報を盗らせないようにするためのカード情報保護対策。加盟店におけるカード情報の「非保持化」の推進と、カード情報を保持する事業者の PCI DSS 準拠。

（2）偽装カードを使わせないようにするための不正利用対策。「クレジットカードの 100%IC 化」の実現と、「決済端末の 100%IC 対応」の実現。

（3）なりすましをさせないようにするための「非対面取引」における不正利用対策。リスクに応じた多面的・重層的な不正利用対策の導入。

- クレジットカード番号（PAN：Primary Account Number）
- クレジット会員名
- 有効期限
- セキュリティコード（CVV：Card Verification Value）
- 暗証番号PIN（PIN：Personal Identification Number）
- サービスコード
- カード情報を含む全トラックデータ

図 1　クレジットカードの「カード情報」

対面加盟店でのカード情報保護対策

実行計画に示されている（1）カード情報保護対策のうち、店員とカード保有者が対面して決済が行われる

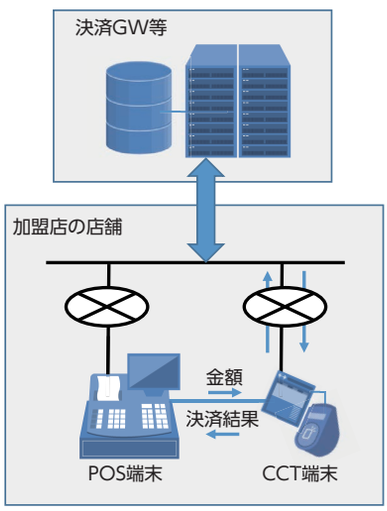

図２　対面加盟店での「外回り方式」

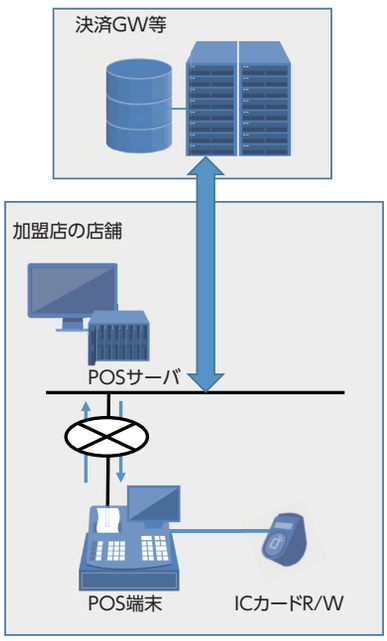

図３　対面加盟店での「内回り方式」

（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-」）

対面加盟店については、「非保持化」または PCI DSS 準拠が求められている。

具体的な方式には、「外回り方式」と「内回り方式」が想定されている。

「外回り方式」は、POS システムを介さないで決済を行っている加盟店に求められる方式である。図 2 に示すように、カード会社から貸与されている、カードを差し込んで暗証番号の入力を求める IC カード対応の CCT 端末を設置し、CCT 端末上で決済することで、自社の POS システムを介さずカード情報を外部の決済 GW 等に伝送することができるため、「非保持化」を実現しているとみなされる。

「内回り方式」は、図 3 に示すように、POS システムを介してカード情報を送付している場合に求められる方式である。前号でも述べた PCI P2PE(Point-to-Point Encryption）と呼ばれる、暗号化することでカード情報を保護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る。また、クレジット取引セキュリティ対策協議会の定めた 11 項目のセキュリティ要件を満たせば、同じく「非保持化と同等 / 相当の措置」を実行したものとみなされる。

なお、「非保持化」とは、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電磁的情報として保存しない、処理しない、通過させないことをいう。そのため、意外かもしれないが、クレジット取引伝票やカード番号を記した FAX、申込書、メモ等の紙媒体、それら紙媒体をスキャンした画像データ、電話での通話データにカード情報が含まれていても、それらがあるだけでは「保持」しているという解釈にはならない。

2020 年に向けた キャッシュレス化の推進

実行計画では、対面加盟店でのカード情報の非保持化、または PCI DSS 準拠をオリンピック・パラリンピック東京大会が開催される前の 2020 年 3 月末までに完了することが求められている。また、(2) 偽装カードを使わせないようにするための不正利用対策である「クレジットカードの 100%IC 化」と、「決済端末の 100%IC 対応」についても、2020 年 3 月末までに完了することが求められている。

政府が「日本再興戦略 2016」において重要な政策課題と位置付けている「キャッシュレス化の推進」が、2020 年のオリンピック・パラリンピック東京大会に向けて進んでいくこととなる。

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