山岡レポート：PCI DSS の現場から（4）

非対面加盟店での 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、先月号に引き続き、その一端を現場からレポートする。

非対面取引におけるクレジットカードの不正利用対策

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、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、クレジット取引セキュリティ対策協議会が作成した「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」に示されている。

この実行計画では、非対面取引におけるクレジットカードの不正利用対策として、「リスクに応じた多面的・重層的な不正利用対策」の導入を求めている（図 1 参照※）。

※ 2018 年 10 月号の再掲載

店員とカード保有者が対面せずに決済が行われる非対面取引は、主に、EC 加盟店や、電話・はがきで注文を受け付ける MO/TO（Mail-Order/Telephone-Order）加盟店による取引があるが、非対面取引の不正利用被害はほとんどが EC 加盟店において発生している。

実行計画では、EC 取引における不正利用被害を抑えるために、非対面加盟店において、「リスクに応じた多面的・重層的な不正利用対策」を導入することとしている。

実行計画 対策の3本柱

(1)クレジットカード情報保護対策
- ・加盟店によるカード情報の「非保持化」
- ・事業者の「PCI DSS準拠」

(2)クレジットカード偽造防止による不正利用対策
- ・「カードの100%IC化」
- ・「決済端末の100%IC対応」

(3)非対面取引におけるカードの不正利用対策
- ・リスクに応じた多面的・重層的な不正利用対策の導入

図 1　実行計画　対策の 3 本柱

実行計画で示されている多面的・重層的な不正利用対策

具体的な「リスクに応じた多面的・重層的な不正利用対策」には、以下の 4 つの方策が示されている（図 2 参照）。

(1) 本人認証

事前にカード会員がカード会社に登録したパスワード等により利用者本人の取引であることを確認する方策。

国際クレジットカードブランドが推奨している本人認証方式「3D セキュア」の利用がその例となる。しかし、パスワード等が未登録の場合は本人認証処理ができなくなることから、パスワード等の登録をカード会員へ呼びかける活動を強化していくことが必要である。また、加盟店からすると、カード会員がパスワード等を失念した場合は販売機会を失うことになるとの懸念もある。固定的なパスワードではなく、ワンタイムパスワードにより、本人認証を行うことを実施しているカード会社もある。

(2) 券面認証

利用されているカードが真正であることを確認する方策。

「セキュリティコード」の利用がその例となる。カード券面に記載されている「セキュリティコード」を認証することで、真正なカードが利用されていることを確認できる。セキュリティコードは、クレジットカードに100%普及している。また、カード券面に記載されていることから、カード会員が覚えておく必要がないこと、現状のオーソリゼーション電文の仕様で導入できることなどのメリットがある。一方で、カード番号とセキュリティコードが盗まれることにより不正利用されてしまうことは避けられないというリスクがある。

(3) 属性・行動分析

過去の取引情報等に基づいたリスク評価によって不正取引を判定する方策。

購入者のデバイス情報、ＩＰアドレス、過去の取引情報、取引頻度等をもとにリスクを評価し、不正取引を判定する。ただし、不正取引判定の精度を高めるためには、大量の実績データが必要である。小規模加盟店で独自に行うことは容易ではないため、外部サービスの利用が有効である。現在、複数のPSPやシステムベンダーからサービスが提供されている。

(4) 配送先情報

不正配送先の情報を蓄積し、商品等の配送を事前に停止する方策。

不正利用された取引の配送先情報を蓄積し、商品の配送を事前に止めることで取引成立後であっても不正利用被害を防止する。属性・行動分析と同じように、実績データの蓄積には時間がかかることから、外部サービスの利用が有効である。現在、カード会社複数社が共同で運用しているサービスが一部加盟店に提供されている。

不正利用対策における具体的方策

(1)本人認証
- 事前に登録したパスワード等により利用者本人の取引であることを確認する
- 例:「3Dセキュア」

(2)券面認証
- 利用されているカードが真正であることを確認する
- 例:「セキュリティコード」

(3)属性・行動分析
- 過去の取引情報等に基づいたリスク評価によって不正取引を判定する

(4)配送先情報
- 不正配送先の情報を蓄積し、商品等の配送を事前に停止する

図２　多面的・重層的な不正利用対策

非対面加盟店が導入すべき対策

実行計画では、加盟店に対して、上述の４つの方策をベースに、リスクや被害発生状況に応じた以下の指針を示している。

(1) 高リスク加盟店

クレジットカード取引セキュリティ対策協議会の調査で不正利用被害額が大きいとされているオンラインゲーム等のデジタルコンテンツ、家電、電子マネー、チケットの４業種に属する加盟店は、「高リスク加盟店」として、前述の４つの方策のうち１方策以上の対策をする。

(2) 不正顕在化加盟店

不正利用金額が継続的に一定金額を超えた場合、「不正顕在化加盟店」として、４つの方策のうち２方策以上の対策をする。

また、すべての非対面加盟店に対して、カード取引に対する善管注意義務の履行とオーソリゼーション処理の整備を求めている。

新しい技術や仕組みによる不正取引対策

EC取引が拡大している中、クレジットカード決済の利便性を保ったまま、不正取引を防いでいくためには、今後も、新しい技術や仕組みが必要である。

本人認証に使われる「３Ｄセキュア」は、新しい仕様が作成されている。新しい仕様では、スマートフォンでも３Ｄセキュアが利用できる、ワンタイムパスワードが標準仕様として利用できるなどに加え、取引ごとにリスク判定を行うことが可能となり、カード利用者に３Ｄ認証を求める取引が少なくなることが期待されている。

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