資料３

コード決済における無権限取引に関する協議会の対応状況について

一般社団法人キャッシュレス推進協議会

2019年11月12日

PAYMENTS JAPAN

発生したインシデントへの即時対応

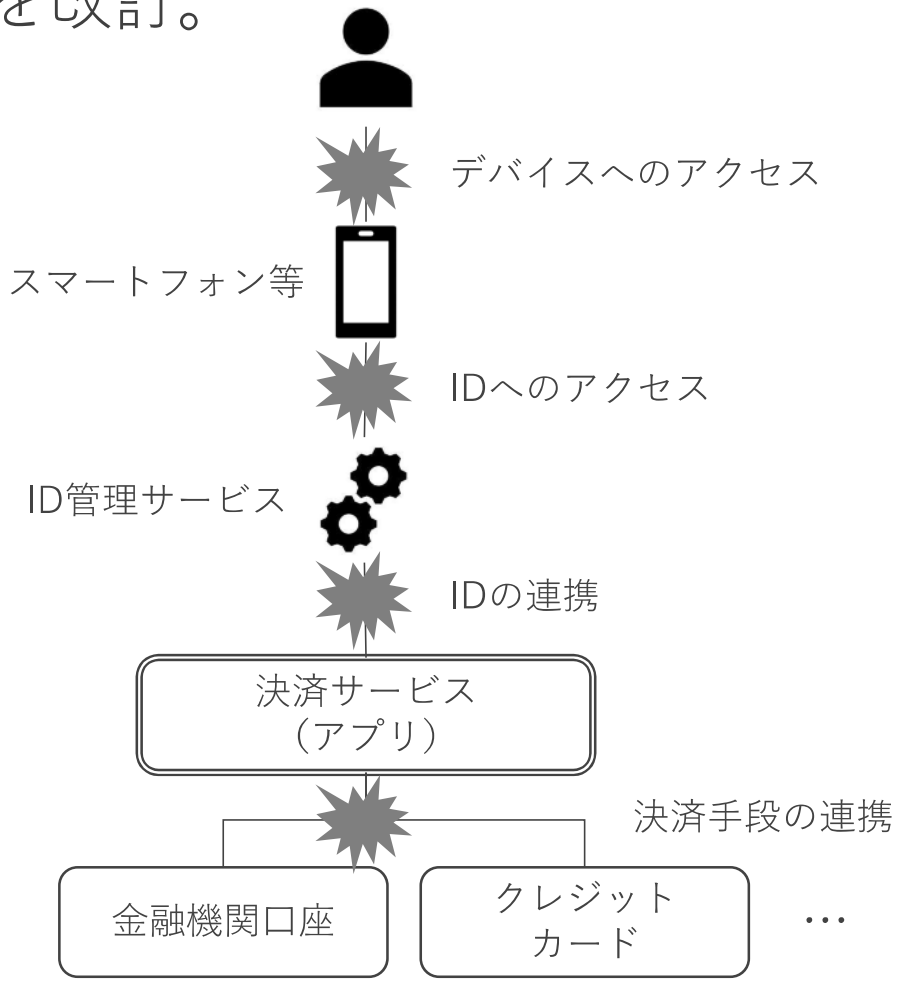
2019年4月に「コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン」の策定、
2019年10月「JPQRガイドライン」を改訂。

不正流出カード番号等の
不正利用防止対策に関するG/L

- 実際にセキュリティコード（CVV）も含めた、クレジットカードの券面情報全てが流出している事象も確認されており、カード券面以外の情報も含めて、いかに本人確認を行うのかを検討し、かつ、あらゆるプロセスでの防止を検討
- ３Dセキュアの導入又はこれと同等/相当のセキュリティ確保が可能である他の不正利用対策（複数の対策を組み合わせることも可）の実施を求めている

JPQR G/L

- 複数システムを連携させたコード決済サービスにおいて不正アクセスにより不正利用される事案が発生したことを受け、JPQRガイドラインを改訂
- 決済事業者に対し、新たに「システム間の情報連携におけるリスク検証の実施」を求める



コード決済事業者における責任分担の強度の違い

責任分担	補償額
• いかなるの場合でも事業者は責任を負わない	• １事案／１アカウントあたり、〇〇円を補償の上限とする
• 所定の本人確認・認証が行われた場合、事業者は責任を負わない	• 損害が発生した月に利用者がチャージした金額を上限とする
• 不正利用の場合、事業者の故意・重過失の場合を除き、事業者は責任を負わない	• 損害が発生した時点においてチャージされている金額を上限とする
• 事業者の故意・重過失の場合を除き、事業者は責任を負わない（不正利用に限定せず）	• 現実に発生した直接かつ通常の損害額を上限とする
• 利用者が適切なID・PWの管理を行っていなかった場合、事業者は責任を負わない	• 利用者に生じた損害のうち、特別な事情から生じた損害について事業者の免責とする
• 警察への届出等の対応を行えば、補償を行う	

各事業者による消費者保護の改善

2019年8月には、「コード決済における不正利用に関する責任分担・補償等についての規定事例集（利用者向け利用規約）」を策定。

事例集策定の目的

不正利用はキャッシュレス決済における利用者の不安のうち、大きなものを占めるものの1つである。不正利用が行われてしまった場合に、どのような補償が受けられるのか、**利用者としてどのような責任を負担する可能性があるか等があらかじめ利用規約等において明示されていることは、利用者の安心感につながる**と思われる。
当協議会は、本事例集において記載されている規定のうち、**特定の規定を推奨等するものではない**し、本事例集に記載される規定以外の規定を否定するものでもない。もっとも、前記のとおり、不正利用における**補償・責任分担等の規定が存在すること自身が利用者の安心感につながる**ものであり、かかる規定自体は利用規約等に明示的に記載してもらいたいと考えている。

2種類の不正（無権限）取引

①不正利用された本人が利用者アカウントの作成（利用者登録）をした後に、当該利用者アカウントが乗っ取り等により本人以外に利用される場合

②第三者により不正に利用者アカウント（不正利用された本人名義とは限らない。）が作成され、当該利用者アカウントにおいて本人のクレジットカードや銀行口座等が登録され、それらを用いて決済されてしまう場合

コード決済事業者が①②の場合にどのように対応していくかを検討し、自社の対応を広く一般に発信していくことも大切

複数のコード決済事業者が規程の改訂、公表を実施


PAYMENTS
JAPAN