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《概要説明資料》

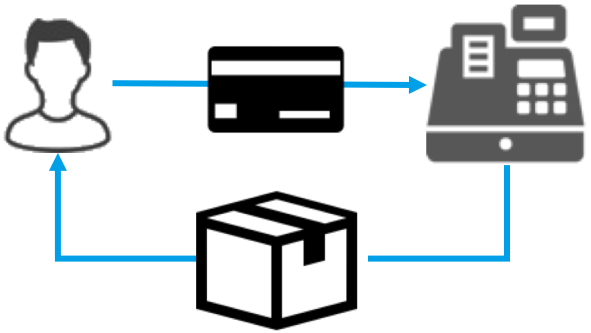
一般社団法人キャッシュレス推進協議会
2019年4月16日

本ガイドライン策定の背景

コード決済において、クレジットカードを活用したサービス提供が増加している。他方、これまでとは異なるクレジットカードの使い方とも見て取れ、新たなセキュリティ対策が求められている。

通常利用のケース

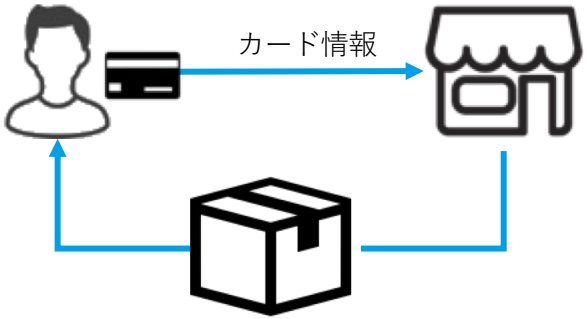
カード券面そのものの存在に加え、PINや署名によって所有者本人であることが確認できる。



物理的なカードの所有そのものが本人であることの理由付けの一つとなりうる

ＥＣ利用のケース

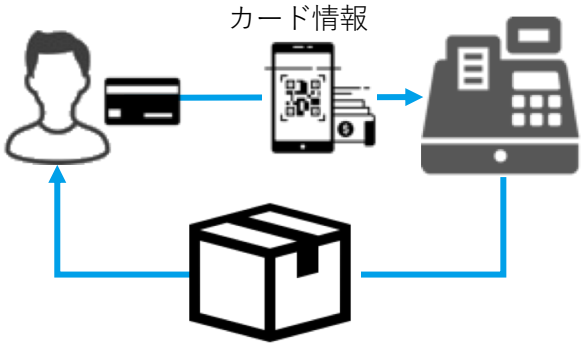
商品の送付先住所により、不正利用者が特定できることから、一定程度の抑止効果がある。



不正取得されたカード情報であったとしても、不正者は利用しにくい環境

コード決済利用のケース

不正取得された情報がスマートフォンに登録され、店頭で利用された場合、本人確認が困難



カード券面もなく、その場で商品を持ち帰れるため、不正者特定も困難

検討の前提

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した。

コード決済までの利用プロセスと起こりうる不正例

端末取得	盗品や悪用目的での購入が起こりうる
SIM取得	盗品や悪用目的での購入が起こりうる
アカウント作成	なりすましや架空人物でのアカウント作成が起こりうる
カード情報登録	不正取得した情報の登録が起こりうる
決済利用	バーコードやQRコード画面の不正取得が起こりうる

今回重点的に検討した場面

検討の体制

ガイドライン策定に向けた検討に際しては、クレジットカード事業者とコード決済等事業者の双方の協力を得ながら実施した。

クレジットカードをスマートフォン等に登録することで決済サービスを提供している複数社（サービス提供予定も含む）

クレジットカード会社複数社

2019年1月18日～2019年3月26日にかけて
全５回の検討会（各２時間程度）を実施

ガイドラインの概要

① アカウント作成	• 利用者からの情報収集を行い、本人であることをしっかりと確認する • コード決済事業者が有する周辺情報の活用	N/A
② カード情報登録	• セキュリティコードの入力回数制限 • リスクに見合った本人認証の方法の選択 • クレジットカート登録時までに収集した情報の活用 • 登録できるクレジットカードの枚数制限	• コード決済事業者と連携し、本人認証及び有効性確認を行う • クレジットカード名義人に対する不正利用防止対策やパスワード登録等の啓発
③ 決済利用	• 金額や利用回数に関する上限設定 • 異常な取引を検知するためのモニタリングの実施及びモニタリング結果の活用	• 取引状況のモニタリングのさらなる精度向上、強化を行う
④ 決済後	• 不正検知の精度向上・強化 • 不正を検知した場合の迅速な対応、関係者との連携	• 不正検知の精度向上・強化 • 不正を検知した場合の迅速な対応、関係者との連携

コード決済サービス①～④全体を通して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


PAYMENTS
JAPAN