

双方向認証に基づくモバイルペイメントの高信頼化

日大生産工（学部） ○堀切 翔太
日大生産工 新井 雅之

1 まえがき

近年、世界的にキャッシュレス化が進んでいる。キャッシュレス決済の一つであるQRコード決済は、スマートフォンだけで決済が可能であり、他の決済手段に比べて店側の端末導入コストが格段に安いなど、様々な利点がある。このため、中国、インドを中心にQRコード決済の普及が進んでいる。しかし、QRコード決済では画像だけを用いて一方認証を行うため、セキュリティ面での信頼性に欠ける。実際に詐欺が報告されており、信頼性の向上が今後の課題といえる[1]。

本研究では、QRコード決済における信頼性の向上を目的として、双方向の認証に基づく手法について提案する。提案システムでは、店と客両方の端末がそれぞれQRコードの表示および撮影（読み取り）を行い、相互に認証する。2台のPCを用いて提案手法を実装し、動作検証を行った。

2 QRコードを用いた決済

QRコードとは、2次元バーコードの一種であり、縦と横の2方向を使って情報を記録する記号体系である。そのため、1方向だけでしか情報を記録できないバーコードと比較して多量の情報を記録できる。また、QRコードは誤り訂正機能を内蔵しているため、汚損に強いという特徴を持つ。記録可能な情報量は、英数字で最大4296字である[2]。QRコードは画像として表示され、携帯端末のカメラで撮影すれば情報を読み取ることができるため、無線通信等のコストを必要としないことが特徴である。

QRコード決済には、大きく分けて以下の2通りの決済手段がある[3]。

(1) ユーザ表示型

(2) 店舗表示型

(1)のユーザ表示型では、まず客が店側にQRコードを表示し、店側がそのQRコードを読み込む。

(2)の店舗表示型では、まず客側がスマー

トフォンで店のQRコードを読み取り、次にスマートフォンで会計金額を入力する。最後に店側がスマートフォンの画面を確認する。

現在、(2)の店舗表示型において、店舗のQRコードが悪意のある他者によって他のQRコードにすり替えられ、客が不正な宛先に送金させられるという詐欺が何件か報告されている[1]。

3 提案手法

本研究では、店側と客側の2台の端末が、互いに専用のQRコードを段階的に表示し、それを読み取っていくことによって相互に認証する手法を提案する。図1に提案する相互認証の流れを示す。

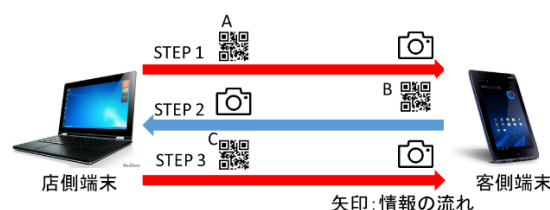


図1. 2台の端末による相互認証の流れ

STEP 1では、店側端末で提示したQRコード(A)を客側端末が読み込む。客側端末内で読み込んだQRコードが正当な値であることを確認した後、STEP 2へ進む。STEP 2では、客側端末がQRコード(B)を提示する。店側端末がQRコード(B)を読み込み、読み込んだQRコードが正当な値であることを確認した後、STEP 3へ進む。STEP 3では、店側端末がQRコード(C)を提示する。客側端末がQRコード(C)を読み込み、読み込んだQRコードが正当な値であることを確認して、相互認証が完了する。

QRコード(A, B, C)は、両端末間でしか認識できない、段階的に暗号化されたデータとして動的に生成されるものとする。

以上のSTEP 1~3を経て初めて決済可能にすることで、QRコードすり替えによる詐欺を防ぐことができると考えられる。

4 実装

4-1. システム実装

提案手法のシステムを2台のPCを用いて評価した。図2にシステムの構成図を示す。店側、客側それぞれのプログラムをWindows 10上でPython 3.7.0によって実装した。また、QRコードを読み込むためにそれぞれWebカメラを搭載した。



図2. システムの構成図

以下に、今回実装した、2台のPCそれぞれのプログラムの機能を示す。

(a) PC 1の機能

店舗端末として動作して、プログラムが実行されると、始めにQRコード(A)を表示する。3秒後、カメラモードに切り替わり、QRコード(B)を認識すると、QRコード(C)と“相互認証完了”を表示する。

(b) PC 2の機能

客側端末として動作して、プログラムが実行されると、カメラが起動する。そこで、QRコード(A)を認識すると、“1回目の認証完了”と表示し、QRコード(B)も表示する。カメラモードに切り替わり、QRコード(C)を認識すると、“相互認証完了”と表示する。

4-2. 動作検証

実行中に自動的にQRコードを読み込めるようにそれぞれのカメラを固定してPCを配置し、動作検証した。図3に動作検証の様子を示す。



図3. 2台のPCを用いた動作検証

それぞれのPCを実行して、動作確認をした結果、相互で認証することに成功した。

次に、システムを10回実行し、通信完了するまでの時間を計測した結果を図4に示す。10回分の平均時間は6.09秒だった。

本研究で提案した手法では、それぞれのSTEPを経た専用のQRコードを読み込まないと認識できない仕様のため、偽のQRコードに対しても安全性が高いといえる。機能面では、それぞれのPCの機能が独立していることから、QRコードを表示している時間を3秒と設定した。そのため、早く読み込めても3秒は待つ必要がある。一方で、ポイントが合わないミスなどで、3秒以内に読み込めなかった場合、画面が切り替わるという問題が発生する。そのため、今後この課題解決に向けて改善を進めている。

5 まとめ

本研究では、2台のPCを用いたQRコード決済において、双方向で認証する手法を提案した。QRコードを用いて、実際の相互認証の暗号通信プロトコルを作成し、2台の端末が店と客として通信可能であることを示した。

今後は、QRコード決済の素早い決済ができるというメリットを活かしたまま機能が実行できるように、さらなる時間の短縮化が課題である。

参考文献

- [1]QRコード決済の落とし穴 HP,
<http://www.afpbb.com/articles/-/3130380>
- [2]コトバンク HP,
<https://kotobank.jp/word/QR%E3%82%B3%E3%83%BC%E3%83%89-2744>
- [3] paypay株式会社 HP,
<https://www.paypay-corp.co.jp/>

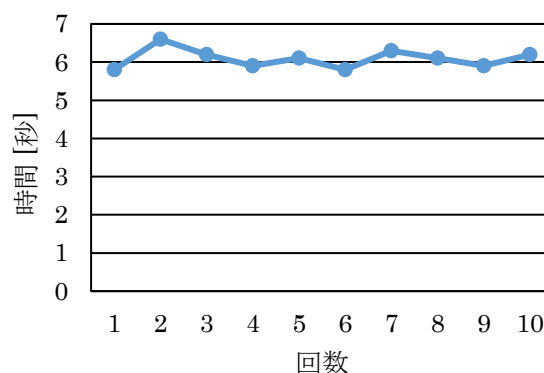


図4. 相互認証が完了するまでの時間