特集
Special Feature

［2 次元コードが経済の動きを加速させる］

2 次元コード決済とその安全性
—2 次元コードの潜在的脆弱性—

応 般 Jr.

森井昌克　神戸大学大学院工学研究科

キャッシュレス決済，スマホ決済，そして 2 次元コード決済

2020 年の個人消費におけるキャッシュレス決済の比率が 29.7%になることが経済産業省の調査によって発表されている．金額的には 8 割以上が従来からのクレジットカード決済であるものの，電子マネー，スマホ決済，デビットカード等も着実に増加している．コロナ禍が続く 2021 年，2022 年も外出しての飲食や交通宿泊等における消費は例年以上の増加は見込めないものの，キャッシュレス決済の比率は「巣ごもり」事情もあって確実に増加している．紙幣や貨幣の受け渡しによる間接的な接触の忌避も少なからず影響しているのである．

2014 年の「日本再興戦略」改訂においても，当時の 2020 年東京オリンピック開催計画を契機にキャッシュレス決済の利便性，効率性による普及を図ることが明記されたが，単にインバウンドにおける国際化を求めたわけではなく，いわゆる決済のデータ化を期待したのである．決済のデータ化によって，決済利用者である消費者は，紙幣や貨幣を物理的に入手し，それを持ち歩き，また保管をはじめ管理することなく，手軽に買い物ができると同時に，その履歴に基づく管理も容易となり，盗難や紛失といったリスクを大幅に軽減することができる．もう一方の決済利用者である店舗側でも同様にデータとしての会計管理が容易となる．さらに最も政府がキャッシュレス化を推進する理由は，紙幣や貨幣を運用するコストの低減と見ることも可能である．紙幣や貨幣を製造する費用だけでなく，それを運搬保管する費用，安全に管理する費用，そのほか，諸々の費用は年間数兆円に及ぶという試算も表されている．たとえば銀行での窓口業務での人件費，あるいは ATM と呼ばれる現金自動支払機の製造，運用だけでなく，ATM に紙幣を挿入するためにそれを運搬する警備会社等の費用といった関連する事業を考えれば十分想定される金額である．そして決済のデータ化は消費行動というビッグデータの解析をも期待できるのである．

当初，キャッシュレス決済，特にコンビニエンスストアや商店での少額決済の本命は IC カードを媒体とした電子マネーであった．元々，紙幣や貨幣自体に価値があるわけではなく，政府等の権威機関がその価値を紙幣や貨幣を媒体に保証しているだけであり，その役目を電子データに置き換えることによって取り扱いを容易にしたのである．しかしながら IC カードおよび，それを読み取る IC カードリーダが必要となり普及にとって小さくない障害であった．そこで注目されたのが，この数年で目覚ましい普及を遂げたスマートフォン（以降，スマホと称する）を利用した決済方法，いわゆるスマホ決済である．スマホは当初，携帯電話の進化系として登場したが，基本的には PDA（Personal Digital Assistant）と呼ばれた携帯情報端末であり，人のすべての活動を支援する機械である．それゆえにカメラだけでなく，GPS（全世界位置測位システム），そして加速度センサや光センサ，温度センサ等，各種センサが搭載された高機能コンピュータとなっている．

特集
Special Feature

スマホ決済では IC カードと同様，IC カードの機能を組み込み，スマホを IC カードリーダにかざすことで電子マネーを利用できる方式もあるが，特に最近注目されている方式は，スマホのカメラで店舗側の 2 次元コード，特に QR コードと呼ばれる情報識別子を読み込み，その情報を基に，スマホの通信機能，特にインターネット接続を利用する方式，あるいは逆にスマホのディスプレイに，自身の決済情報を QR コードとして表示し，店側のカメラに読み込ませ，やはりインターネット接続によって決済を完結する方式である．

2 次元コード決済の脆弱性

2022 年の 1 月になって，米連邦捜査局（FBI）は 2 次元コードである QR コードを利用した不正送金について注意を促している．その手口は駐車場のパーキングメータにおいて，不正な QR コードを張り付け，その QR コードをスマートフォンに読み込ませ，偽の決済サイトに誘導し，クレジットカード等の情報を入力させる方法である．2 次元コードが決済に使われ始めた 10 年以上前から繰り返し行われている最も古典的で基本的な不正利用方法である．フィッシング（phishing）と呼ばれるインターネットを利用した詐欺の代表格であり，フィッシング対策協議会が組織されるほど，その手法は年々，巧妙になり，その注意喚起が政府を上げて再三再四行われるものの，被害は増加の一途をたどっている．フィッシング詐欺は何らかの方法で不正なサイト，特に正常なサイトに似せた偽のサイトに導き，ID やパスワード，その他認証にかかわる情報や個人情報を搾取する方法である．一般には，検索システムや SNS（ソーシャルネットワークサービス），あるいはメール等を使って偽の URL やその URL を掲載したタグやバナーを送り，そこにアクセスを導き，情報を搾取する方法である．いかにして興味を引くか，あるいは平常心をなくさせるほどの混乱状態に陥れるかがその手法の脅威につながる．還付金詐欺や大金を得られるという当選詐欺，それに親族が危機に陥り，示談を装うという振り込み詐欺と同様である．

■図 -1　2 次元コードの不正張替え

2 次元コードの利用はフィッシング詐欺にとって格好の材料なのである．その理由は 2 次元コードの本質にある．2 次元コードは機械（スマホ）が容易に読み込めること，つまり認識できることが最大の特質であり，それゆえに人間には認識できなくなっている．つまり，利用する人が認識できないゆえに，本来使用する 2 次元コードとは別の偽の 2 次元コードとの識別が付かず，騙すことが可能になる．人間が認識できないことで，ほかにも漏れることがないであろうと錯覚し，過度な安心感をもたらす可能性もある．2 次元コード自体が大きな弱点，脆弱性を有していると言っても過言ではない．実際，2009 年には，先のフィッシング対策協議会から 2 次元コードを利用したフィッシング詐欺について注意喚起が行われている．2 次元コードをすり替える手口に対してである（図 -1）．

この 2 次元コードを利用する決済方式には，決済方式自体のプロトコル，あるいは認証アルゴリズムと相まって安全性を損なう場合も十分あり得るのである．

2 次元決済は，その 2 次元コードの読み込む対象によって大きく 2 つに分けられる．サービスを受ける側，すなわち顧客が自分のスマートフォンに表示した 2 次元コードをサービス側に読み込ませる CPM（Consumer Presented Mode）方式と，逆にサービス側が表示した 2 次元コードを顧客のスマートフォンで読み取る MPM（Merchant Presented Mode）方式である（図 -2）．双方ともに一長一短

であるが，当初，MPM 方式が主流であった中国では，店舗に貼られたサービス側の口座番号に相当する認識情報が書き換えられ，具体的には正しい 2 次元コードの上に，他者の認識情報を入れた 2 次元コードに張り替えて，不正送金を行う被害が多発していた．2 次元コードを読み取ることによって，相手の認識情報が正しいか否かを確かめることができれば，容易に被害を防ぐことができるのであるが，利便性を優先するあまり，確認することなく送金を終了することが原因であった．サービス側も 2 次元コードが正しいか否かを常に検査することによって，防ぐことが可能であるものの，視認することでは区別がつかず，不正の発見を遅らす結果となっていた．

また CPM 方式においても無条件に安全かと言えば，必ずしも肯定できない．サービス側の端末にマルウェアを仕掛け，中間者攻撃と言われる，データを通信路上で改ざんし，他者に成り済ますことも考えられる（もちろん，QR 決済を運用する側はその対策を十分とっていると考えられる）．同様に顧客側のシステム，通常はスマートフォンのアプリにマルウェアを仕掛け，中間者攻撃により，表示する QR コード，および関連情報を瞬時に他者に送ることも考えられ，必ずしも不可能とは言えない．また図 -3 に示すようにスマホに表示された 2 次元コードを搾取して使用する方法も考えられる．

「CPM (Consumer Presented Mode)」方式
QRコードを表示させ，店員さんに読み込んでもらう方法

「MPM (Merchant Presented Mode)」方式
レジにあるQRコードを読み込み，支払い金額を入力し，店員さんに確認してもらう方法

■図 -2　CPM 方式と MPM 方式

2 次元コードの本質的脆弱性

2 次元コード決済における MPM 方式の場合，不正な情報を格納した 2 次元コードを読ませることによって，不正送金を行うことが可能となることは先に述べた．しかしながら，大概の場合，即座に不正な 2 次元コードと判明し，その不正な 2 次元コードを棄却するなどの対策を取られてしまう．2018 年 6 月，筆者ら神戸大学の研究グループは 2 次元コードの構造上の弱点を利用して，不正な情報を格納する方法を提案した．この方法は従来のように単に 2 次元コードに不正な情報を格納するのではなく，任意の条件のもとに，

■図 -3
MPM 方式下での不正利用例

特集
Special Feature

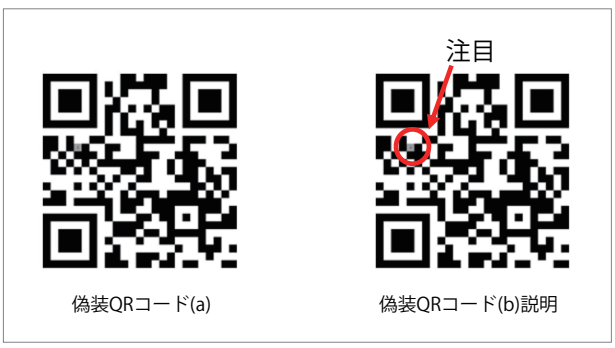
不正なサイトに誘導する方式である．

簡単に言えば，まったく同一の 2 次元コードであるにもかかわらず，A という URL に飛ぶときもあれば，B という URL に飛ぶときもあるという，いわば二重の仮面をかぶった 2 次元コードを開発した．具体的には 2 次元コードである QR コードに対して開発を行っているが，原理的にはほぼすべての 2 次元コードに適用可能である．この QR コードを「偽装 QR コード（Fake QR code）」と呼ぶ．これを悪用すれば，通常は正常なサイトに誘導するが，数十回，あるいは数百回，数千回に 1 回は，悪性サイト，たとえばその正常なサイトを模したフィッシングサイトに誘導し，不正をはたらくことが可能になる．2 次元コード決済の場合，正常な決済に紛れて，不正な決済が行われることになり発見を困難，あるいは遅らせることが可能となる．この偽装 QR コードを使えば，最初に配布された偽装 QR コードを注意深く調べた，つまり不正なサイトに誘導するか否かを逐次調べたとしても，ほとんど気付かれることはない．数十回，数百回，あるいは何千回も利用した結果，正常なサイトに誘導され，安心し，その後，気が付かないうちに不正サイトに誘導される，すなわち不正な決済が行われることとなる．多数の人に利用させることができればさらに効果が期待できる．不正決済が確認されても，2 次元コード自体で再現性は乏しく，発見を困難にするのである．なお，不正なサイトに遷移する確率は任意に制御することができる．

たとえば，図 -4 の偽装 QR コード（a）は通常，試験的に作られた研究室の Web http://srv.prof-morii.net/~lab/ に誘導する．しかしながら数回に一度は，その偽のページとして作られた http://srv.prof-morii.net/~lob/ に誘導される．遷移することの確認が容易なように数回に一度，偽装ページに遷移するように設計されているが，上述のように発見を困難にするためには，数百回，数千回に一度の遷移確率に設計することが勧められる．

一般に偽装 QR コードは視認によって発見することは困難とはいえ，図 -4 での偽装 QR コード（a）を注意深く観測すると，その相違点が分かる．偽装 QR コード（b）説明での，QR コードのモジュール（セル）における注目点である．しかしながら 1 つのモジュールでの形や配色は本質ではなく，視認でもほとんど困難となるように設計することも可能である．図 -5 では，一般の QR コードとほとんど見分けがつかないものの，Google の検索サイトにおいて，SITA2018（2018 年情報理論とその応用シンポジウム）の検索と SCIS2019（2029 年暗号と情報セキュリティシンポジウム）の検索のいずれかがほぼ等確率で表示される．

構成方法の詳細は筆者らの学術論文 [1] に譲るが，簡単に言えば，QR コードを含む 2 次元コード自体の技術の要である，誤り訂正技術を利用している．誤り訂正技術は誤認したモジュールを発見し，それを正常なモジュールに修正する技術である．この誤りを訂正する方式を逆手に取って，わざと限界以上の誤りを訂正させることによって，混乱させ，間違った訂正を行うように仕向けている．誤り訂正方式のアルゴリズムを解析することによって，この誤りを自由に制御し，任



■図 -4　偽装 QR コードの例 1

■図 -5　偽装 QR コードの例 2

特集
Special Feature

意の情報に誤るように設計しているのである．いわば，人工知能（AI）における Adversarial Examples（敵対的サンプル）と同様，2 次元コードの特性を利用して誤認識を引き起こさせている．

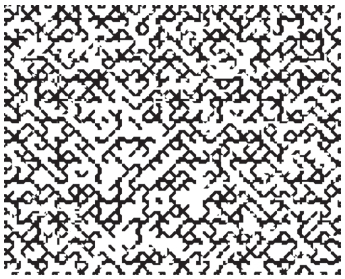
改めてこの偽装 QR コードを作成できる深刻さ，その無視できない脅威を与える．すでに利用されている（公開されている）QR コードについて，その QR コードと同一の QR コードで，他の URL に誘導することは，改ざんされた QR コードリーダ（QR コード認識装置）を配布しない限り不可能である．あるいは，QR コード自体の視認困難性から，そのすり替え，もしくは新たな 2 次元コードを配布する場合である．たとえば，新規のサービスを行うために，それを紹介した新規サイトに誘導する 2 次元コードの作成を希望する場合，その 2 次元コードを作成することができるシステム開発会社に依頼するか，もしくはフリーの 2 次元コード作成プログラム，あるいは 2 次元コード作成サイトを利用して作成する．このとき，依頼したシステム開発会社や 2 次元コード作成サイト等に悪意があった場合，さらに不正アクセス等を受けて，2 次元コード作成プログラムが改ざんされている場合，上述の偽装 QR コードが作成される可能性がある．その偽装 QR コードを配布した場合，当初は問題なく正常なサイトに誘導され，時間が経ってから，悪意のある別なサイトに誘導され多大な被害を受ける．悪意のあるサイトに誘導されるのは数百回，数千回に一度の割合であることから，再現性が乏しく，すなわち発見が難しく，対策が遅れることとなる．特にその悪意のある別なサイトが，識別が難しいフィッシングサイト（正常なサイトに似せて作られ，詐欺をはたらくサイト）であれば，さらに発見を困難にし，被害を広げることになる．決済システムにおいて同様な危険性が完全に排除されている保証はないのである．

一般に 2 次元コード自体の認識，つまり 2 次元コードの存在確認は容易と考えられている．それゆえに 2 次元コードに向けてカメラをかざし，すなわち撮影することによって 2 次元コードの利用を行っている．現在では 2 次元コードの決済での利用を含めて，スマホのカメラをかざしただけで，2 次元コードを自動で認識し，その認識結果に基づいて，認証を含め，自動で動作することも行われている．もし，2 次元コードの正当性，および情報の視認だけでなく，2 次元コード自体の存在の視認が困難となればいかなることになるであろうか．2 次元コードと視認できず，たとえば風景（背景）と混同し，カメラが 2 次元コードを誤認し，不正動作が行われる可能性がある．スマホのカメラが決済システムと誤認識し，決済を不正に進めてしまうことも否定できないのである．

筆者らの研究グループは 2 次元コードの存在自体の視認も困難とする，いわゆる見えない 2 次元コード（Hidden QR code）の開発も進めている．現在，研究の途上であるが，たとえば図 -6 は QR コードとして認識することが可能である．

2 次元コード決済の安全性確保のために

繰り返すことになるが，2 次元コードの本質的な脆弱性は視認できないことである．すなわち 2 次元コードが与えられたとしても，その 2 次元コードの正当性，および格納されている情報を認識することは非常に困難である．したがって 2 次元コードリーダの信頼性とその解析結果，すなわちデコード（復号）された情報の確認が重要となる．まず第 1 には 2 次元コードを認識し，その情報を読み出すデコーダの正当性である．第 2 に，2 次元コード自体の正当性である．2 次元コー



■図 -6
見えない QR コード

ドの発行元の正当性確認が問題となるが，たとえばデジタル署名等を用いて，その発行を制御することが考えられる．そして第 3 に 2 次元コードに格納された情報の視認である．特に 2 次元コードに，アクセスすべき URL が格納されている場合，その URL をアクセスする前に視認する必要がある．

概して言えば，便利に使える 2 次元コードを利用したスマホ決済をはじめ，ネット決済サービスに完全な安全性を求めることは困難なのである．利用者に便利ということは，少なからず悪用する側にとっても便利な面が出てくる．決済サービス会社は，そのサービスを広めるために利便性を追求することが常であり，逆に安全性がどうしても損なわれることになる．このある意味，トレードオフになる関係で，いかに最良な点を探すかが現実的な解決案となる．その解決案もすべての利用者にとっても安全となるかというとそうではない．利用者の不注意が不正利用につながることは十分あり得，これを排除する技術は困難を極める．

少なからず安全性に疑問が残る各種ネット決済サービスであるが，どのように扱えば利用者は安全なのであろうか．答えは利用しないことである．正確に言えば，必要性がなければ利用しないことなのである．身もふたもない解決策であるものの，やはりその利便性から使うことを望む人も少なくない．その場合，利用する人がそれぞれの考えでリスク（危機）管理をすべきである．たとえば，決済サービスで利用できる上限額を定める，銀行口座から決済サービスに送金できる金額を限定する，あるいはそのような口座には必要な金額しか預金しない，さらには決済用には少額を決済する銀行口座を限定し，主な高額な資産はネット決済と紐付けができない銀行口座に預けるなどである．

2 次元コードを利用したネット決済に対して最悪の事態を想定し，その被害を最小に抑える対策をとる必要がある．それがリスクコントロール（危機管理）である．今，求められる対策は被害に遭わないことだけでなく，被害に遭った際にその被害を最小限に止めることなのである．さらに被害に遭わないための最大の対策は，必要のないことは行わないことである．

筆者らの神戸大学での研究グループでは，AI（人工知能）の脆弱性に対する研究を行っている．偽装 QR コードの提案もその一環であり，QR コードを読み込んで，その情報に従って自動的に処理するという行為は AI と同等であると考えることもできる．QR コードに格納された情報の自動修復機能（誤り訂正）を逆手にとって，不正な情報に基づき，悪意のある処理（不正なサイトへの誘導等，不正な情報処理）を容易に実現できることは，AI に処理を委ねることの危険性の一端を示したことになろう．

2 次元コードの使用が一般社会に溶け込み，さらに生活のいたるところで見られるという親和性から，その安全性が担保されている錯覚に陥っている感がある．2 次元コードは単に光学的にデータ（情報）を送受するだけでなく，2 次元コード自体が自動認識，誤り訂正等，いわば高度な情報処理を伴うシステムであり，それ自体の脆弱性も安全性の観点から十分検討する必要がある．今後，さらに広まることになるであろう 2 次元コード決済もその利便性のみならず，改めて安全性を十分確保しなければならない．

参考文献

1）瀧田　愼，大熊浩也，森井昌克：2 つの情報を出力する QR コードの構成―悪性サイトに誘導する QR コードの存在とその脅威―，電子情報通信学会論文 D，Vol.J103-D，No.4，pp.291-300（Apr. 2020）．

（2022 年 3 月 7 日受付）

■森井昌克　mmorii@kobe-u.ac.jp

1989 年阪大大学院工学研究科博士後期課程通信工学専攻修了，工博．同年，京都工繊大助手．愛媛大助教授，徳島大教授を経て，現在神戸大学大学院工学研究科教授．情報理論，情報セキュリティが専門．電子情報通信学会フェロー．