新型コロナ禍で広がるネットバンキングやスマホ決済の課題

神戸大学大学院工学研究科教授　**森 井 昌 克**

～要旨～

コロナ禍以前からのスマートフォンの普及に代表されるネットワーク社会の急速な発展は人の活動においても多くの、そして大きなひずみを抱えたまま進行し、コロナ禍によってさらに増幅しようとしている。その問題は国家間のサイバー攻撃から青少年のSNSによるいじめの問題まで、社会の多岐にわたる。本稿では身近なネットバンキングやスマホ決済に視点をおいて、その安全/安心な利用における課題と解決法について論じることとする。パソコンやスマートフォンのアプリにマルウェア（コンピューターウイルス）を感染させ、遠隔操作や自動制御によって、不正送金を可能にするという斬新な手口があるものの、結局のところ、大多数は個人情報漏えいに関わる問題であり、その無意識な漏えいをいかに防ぐか、無条件に安心/安全なネット決済は存在せず、その危険性をいかに排除、被害を最小化できるかを過去の被害や手口を例に論ずる。

1　はじめに

コロナ禍によって、クローズアップされた耳慣れない言葉の一つとしてテレワークが挙げられる。テレワークはリモートワークやモバイルワークともいわれ、本来は所属する会社組織から物理的に離れた場所において仕事を行うことを意味する。しかしコロナ禍での意味合いは、「在宅勤務」であって多数を占める会社や組織に所属する社会人が、自宅から外出することなく勤務することを意味する。コロナ禍は仕事という一つの社会活動だけでなく、学校でのリモート講義をはじめ、できる限り外出を抑え、人と人との接触を避けることを推奨した。一昔前であるならば、コロナ禍は社会活動全般の停止を余儀なくしたであろう。しかし現在においては「高度情報化社会」という言葉が陳腐化したほどにICT（情報通信技術）が発達しただけでなく、スマートフォンの普及によって、人と人とのコミュニケーションだけでなく、人と機械（コンピューターを含むあらゆる人工物）とのコミュニケーションも可能となった。IoT（Internet of Things）という概念はすべてのもの（Things）をインターネットにつなぐことである。この「もの」には人も含まれる。すなわち人と人、人と機械、そして機械と機械が互いにコミュニケーションをとる時代が現在なのである。すでにすべてのものをつなぐという概念を越えて、IoE（Internet of Everything）、つまり物理的な「も

の」を越えて、すべてをインターネットで完結しようという概念も実現しようとしている時代である。その尖兵がAI（人工知能）であり、問題解決をも自動的にネットワーク上で処理しようとしている。コロナ禍はICT社会の基盤の上でこのIoEを不本意にも後押しすることになった。

コロナ禍以前からのスマートフォンの普及に代表されるネットワーク社会の急速な発展は人の活動においても多くの、そして大きなひずみを抱えたまま進行し、コロナ禍によってさらに増幅しようとしている。その問題は国家間のサイバー攻撃から青少年のSNSによるいじめの問題まで、社会の多岐にわたるが、ここでは個人に関わる経済活動、特に身近なネットバンキングやスマホ決済に視点をおいて、その課題と解決法について論じることとする。

2　キャッシュレス決済とスマホ決済

経済産業省の調査によって、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するであろう。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することであろう。

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み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、その他、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。例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できる金額である。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ーとなっている。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。

3　ネット決済における不正送金とその手口

（1）フィッシングとスミッシング

一般に、フィッシング（phishing）とは悪意をもって、インターネットサービス利用者をだまし釣る、すなわち利用者の意思に反して悪意のあるサイトに誘導することである。このフィッシングがネットバンクの不正送金やスマホ決済での不正利用に用いられる最も単純な方法であり、かつ現在でも多くの被害者を生み出す方法である。フィッシング対策協議会という、その対策に特化した組織がつくられるほど社会問題化している。

フィッシングでは本物と区別がつきにくい偽物のウェッブサイトを作り、そのウェッブサイトに誘導し、個人情報を盗み出す手口の総称である。例えば、ネット銀行やカード決済サービス、さらにはフリーマーケットやオークションサイト等のログイン画面とほとんど同じ画面を作り、そこにそれらの正規利用者を誘導し、IDやパスワード、あるいは氏名、住所等の個人情報を入力させ、だまし取る。本物と見分けがつかないようなウェッブサイトを作ることは困難ではなく、だます側にとって、最大の壁（工夫する点）は、いかにして、正規のユーザをその偽物のサイトに誘導するかである。

誘導する方法としては、スパムメール（不特定多数あてのメール）を用いて、「不正アクセスを受けた可能性があります」あるいは「アカウントが一時凍結されます」等、危機感をあおり、平常心を乱させて、注意力を著しく低下させ、偽物のウェッブサイトに誘導する。銀行等のサイトではユーザにメールを送り、そのメールのURLからアクセスさせるようなことは決して行わないと再三注意を促しているものの、もはや平常心をなくした利用者の一部は容易にアクセスしてしまう。詐欺の基本である、相手の平常心を失わせ、考える時間を与えることなく、指示に従わせる手法である。

スマホでは、メールではなく、SMS（ショートメッセージサービス）やツイッター、それにインスタグラムといったSNS（ソーシャルネットワークサービス）の利用がメインとなった。フィッシングもSMSやSNSを利用し、特にSMSを利用した詐欺のメッセージ送信はスミッシング（smishing）と呼ばれている。新たには、スマホのスケジュール管理を行うカレンダー機能を利用した手口も登場している。カレンダー機能には、他人とスケジュールを共有したり、気なるテレビ番組やイベントの通知を自動的に行うような仕組みが備わっている。その機能が不正に利用されたり、自分の不注意で他のサービスと連携してしまうと、特定の日時に、アクセスするURLが興味を引きそうなタイトルとと

もに記入され、アクセスしてしまうのである。

(2) マルウェアと不正送金

ネット銀行の不正送金においてもその主たる手口はフィッシングによる口座番号やパスワード、あるいは乱数表等の搾取であった。現在では二要素認証、例えばワンタイムパスワードという認証方式が一般化し、フィッシングによる直接的な不正送金は大きく減少した。しかしながらさらに巧妙な手口では、やはりフィッシングを足掛かりに、言葉巧みに危機感をあおり、別口座に送金させたり、ワンタイムパスワード自体を不正に利用させ、つまりワンタイムパスワードを表示させると同時に搾取、そしてすばやく利用し、勝手に送金をしてしまう事例も報じられている。

マルウェア（コンピュータウイルス）に感染させて、事実上、パソコンを乗っ取って、不正送金を行う手口も存在する。マルウェアによってパソコンが乗っ取られれば、そのパソコンは自由に操られてしまう。たとえば、乗っ取られたパソコンで、正しいネット銀行のサイトにIDとパスワードを入力したとたんに、マルウェアがそれを検知し、動作して、目にも留まらぬ速さで、不正な送金手続きを行ってしまう。これはMITB（Man in the Browser）攻撃と呼ばれ、ブラウザの中に人（犯罪者）がいるように不正送金の仲介をしてしまうのである。

(3)「ドコモ口座」事件

コロナ禍の2020年9月、スマホ決済だけでなく、キャッシュレス決済全般に関係する象徴的な事件が明らかになった。「ドコモ口座」事件と称される事件である。しかしこれは、キャリアと称される携帯電話事業者であるドコモだけの問題ではなく、キャッシュレス決済に関わる金融業界、ドコモをはじめIT業界全体の問題であった。

ドコモ口座事件とは、スマホ決済を含むキャッシュレス決済に関係しない銀行口座が勝手に他人のドコモ口座に紐付けされてしまい、不正送金されるという事件である。これには、銀行と携帯電話会社であるドコモ、そして決済を仲介する決済システム会社が関係している。一言で問題点を指摘すれば、各社の認証、すなわち利用者の本人確認の脆弱性である。結果的に、メールアドレスがあれば、銀行口座とその名義人氏名、そしてその口座をATMで使うための4桁の暗唱番号を利用してドコモ口座を作れたのである。もちろん、他人の口座で作ることができ、それが不正送金につながった。もしネットワークを熟知したドコモが一切を取り仕切ったとすれば、このような脆弱な認証方式を取らなかったであろう。銀行側も口座番号と名義、それに4桁の暗証番号だけでネットワークを介した取引を行うとは想定していなかったはずである。ほとんどすべての銀行がネットバンク機能を有し、過去になりすまし等の不正送金問題で痛い経験を積み、二段階認証等を進めている。つまり決済システム会社が仲介することによって、相互の確認が取れず、互いに他を過信したことも原因である。

(4) スマホ決済とQRコード

キャッシュレス決済の問題点はすべてスマホ決済に通じると言っても過言ではない。その理由はスマホがICカードに基づく電子マネーのように、決済に特化したシステムではないからである。スマホは人のあらゆる活動を支援する汎用的な携帯情報端末ゆえにさまざまな利用が考えられ、また想定外の使用もあり得る。その中で決済について完全な安全性を保障することは

極めて難しいのである。

例えばスマホ決済で利用されるQRコードであるが、当然のことながら決済用に設計されたシステムではなく、実際にも望みのwebに誘導するためにQRコードにURL、いわゆるwebの識別子を格納している。現在、スマホ決済の主流はQRコードを利用した決済になっている。QRコードの利用はその安全性に基づくものではなく、利便性に基づくものである。スマホのディスプレイで容易に表示することができ、またスマホに限らず、カメラをはじめ安価な光学認識装置で読み取ることができるからである。逆に最大の欠点は人間が認識できないことである。QRコードであると認識できたとしても、どのような情報が格納されているか確認できないのである。これが大きな弱点であり、脆弱性になっている。例えば、決済する人が認識できないゆえに、本来決済に使用するQRコードとは別のQRコードを相手に送り、だますことも可能である。機械が簡単に認識できるゆえに、表示しているQRコードを短時間で知らない間に盗まれ、即座に利用されてしまうこともあり得る。人間が認識できないことで、他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。

4　個人情報の漏えいはなぜ起こる？

ほとんどの人がもはや何がしかの現金決済以外のキャッシュレス方式、特にネット決済を利用していると言ってよいであろう。現金決済でも詐欺が後を絶たないように、歴史が浅く、その利用に慣れないネット決済においては、さまざまな手口の不正利用が報告されている。そのほとんどの手口において、まずは個人情報である口座番号や名義、さらにはパスワード等の機密情報の漏えいが発端となっている。フィッシング等、それらを得ること自体が周到な準備に基づく新たな手口の一端である場合も多いが、すでに漏えいしている個人情報を利用して、標的と定めるのである。

情報は漏えいするものである。その前提で個人においても対策、少なくとも心構えをすべきであろう。個人情報の主体である個人が取るべき対策として、できることはただ一つ、個人情報を出さない、登録しないことである。正確には必要以上に個人情報を他者に漏らさないことである。当然のことと思われがちであるが、これが守られていないのである。懸賞への応募、あるいは特典に釣られてのアンケートの回答等は意識せず、重要な個人情報を漏えいする結果を引き起こす。危機管理意識の欠如は思わぬ情報漏えいを引き起こすのである。例えばSNSで流行している「占い」等のサービスである。占いでは意識することなく、名前や生年月日を入力することもあり、それ以上の個人情報、つまり個人が抱えている問題等を安易に入力することもあり得る。同様に、さまざまな質問に応えて、年齢や性格を当てるサービス（サイト）や、顔写真を登録して、写真から推定される年齢や似ている著名人を紹介するサービス等もあり、極論すれば、それらの無料サービスはすべてデータ収集が目的であり、むやみに行うべきものではない。「いつでも、どこでも、誰とでも」を実現した、携帯情報端末であるスマホの利用は、個人情報を含めて、意識しない間に、秘密にしなければならない情報を自ら送ってしまうことがあるということを自覚し、その予防に十分配慮しなければならない。

5　個人ができる対策と危機管理

まずパソコンやスマホを安全に利用することが第一である。パソコンに関してはマルウェア

の感染を防ぐためにアンチウイルスソフトを導入し、怪しいメールを開かない等の対策を十分に行うことである。スマホに関しては必要のないアプリをインストール（導入）しない、パスワードロックをかけ、自分以外に触れさせない等の管理が必要である。それでもなおマルウェアには感染する可能性は捨てきれない。アンチウイルスソフトは99.99％のマルウェアに有効であっても、残りの0.01％のマルウェアは見逃してしまう。ほんの少しの危機感、つまり注意をすることで不正を防ぐことは多い。日頃の利用と少しでも違和感があれば躊躇なく、パソコンやスマホの扱いに慣れた人に相談すべきである。

個人情報の管理については常に意識し、それでもなお漏れることを想定しなければならないことを述べた。最も個人情報の漏えいやパスワード等の秘密情報の漏えいに至る被害に導く手口がフィッシングである。フィッシングサイト自体を取り締まることは不可能に近い。対策は個人に委ねられるのである。フィッシングサイトにアクセスしないための、その対策の第一はメールやSMSでの危機感をあおるメッセージには反応しないことである。攻撃者はあらゆる文面を駆使して、個人の注目を得ようとする。詐欺の手口は相手の平常心を失わせる、そして判断する時間を与えないことであり、常に平常心を持ち、冷静に対処する、具体的には、一呼吸置くだけで、被害を防げる場合は少なくない。パソコンやスマホの画面上で、警告を次々と表示して、焦らす手口が多い。何も入力しない限り、状態は変わらず、つまり事態を悪化させることはない。事態を悪化させる原因は自分自身のクリックやタップにあることが多く、最終的に危機感をあおり、被害に遭うのである。

概して言えば、便利に使える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え、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、さらにはそのような口座には必要最小限の金額しか預金しないことである。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等である。

ネットバンキング、あるいはネット決済に対して最悪の事態を想定し、その被害を最小に押さ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）と言われるものである。今、求められる対策は被害に遭わないことだけでなく、被害にあ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。

6　むすび　～サイバーセキュリティ～

ネットバンクの不正送金が問題となって久しい。かつてはネットバンクからの案内を装ったスパムメールからフィッシングサイトに誘導し、口座番号とパスワードを入力させ、つまり盗み出し、それを利用して不正送金を行う手口が主流であった。目的を達したフィッシングサイトは入力ミスがあったことを表示し、正規のネットバンクサイトに再誘導すれば怪しまれることなく成功するのである。その後、二要素認証として、ワンタイムパスワードや乱数表を用いるようになり、それに対応して、フィッシングサイトも巧妙となり、乱数表をすべて記入させる工夫やマルウェアを利用したワンタイムパスワード越えも出現している。さらにスマホ決済が主流となるや、併せて独自通貨と言っても過言ではないポイントも多用されると、それらに対する不正流出が出現している。その代表格が7pay や PayPay に対する不正送金や不正利用を目的としたサイバー攻撃であり、昨年には前述のドコモ口座事件に至ったのである。ネット決済に限らず、デジタル化が進む現在、もはや個人においてもサイバーセキュリティの意識なく社会生活を営むことは不可能である。

古代中国の兵法書である孫子の一節、「知彼知己、百戦不殆」は「敵を知り、己を知れば百戦危うからず」と訳され、サイバーセキュリティの分野では最も参照される格言である。己を知ることは、己の弱点をしっかり把握することでもある。さらに史記にある「千慮の一失」とは、十分に注意をしていたにも関わらず失敗を犯してしまうことである。己のリスク（注意力）を冷静に判断し、起こった場合の被害を最小にする運用を心がけるべきであろう。

もりい　まさかつ
1989 年大阪大学大学院工学研究科博士後期課程通信工学専攻修了、工学博士。現在、神戸大学大学院工学研究科教授。情報セキュリティ大学院大学客員教授。国立研究開発法人日本医療研究開発機構プログラムスーパーバイザー。サイバーセキュリティ、情報理論、暗号理論等の研究、教育に従事。加えて、安全・安心に基づくサイバー社会構築に向けての社会活動にも従事。関係各学会等の委員長、内閣府等各種政府系委員会の委員を歴任。サプライチェーンサイバーセキュリティコンソーシアム（SC3）運営委員、同中小企業対策 WG 座長。平成 30 年度情報化促進貢献個人表彰経済産業大臣賞受賞。平成 31 年総務省情報通信功績賞受賞。令和 2 年情報セキュリティ文化賞受賞。電子情報通信学会フェロー。