応般 Jr.

「ドコモ口座」はなぜ攻撃されたか？
～開設時本人確認と出金時本人確認の間隙～

板倉陽一郎 | ひかり総合法律事務所

「ドコモ口座」不正利用事件

2020年9月，NTTドコモの「ドコモ口座」を利用した銀行からの不正引き落としが発覚した．「ドコモ口座」の不正利用事件である．広く報道されたため，「ドコモ口座」が不正利用されたということは知られているであろうが，なぜ攻撃されたのか，という点について，十分整理された論稿が少ない．また，「ドコモ口座」にせよ，同時期に問題が発覚した他の決済サービスにせよ，被害の保障が行われ，法的紛争に発展していないため，決済サービスや銀行口座において，どのような本人確認がなされていれば十分であったのかということについて，裁判所の判断は示されておらず，おそらくは今後も示されない．そこで，本稿では，①「ドコモ口座」がなぜ攻撃されたのか，②「ドコモ口座」不正利用事件を踏まえ，QRコード決済サービスに銀行口座が紐付くスキームにおいて，いつ，どのような本人確認が求められるようになったのか，について整理する．なお，筆者らは，本稿と関連した論点について本会の研究会発表を行っているが[1]，本稿の内容の責任は筆者のみにある．

NTTドコモのプレスリリースによれば，「本不正利用は，第三者が銀行口座番号やキャッシュカードの暗証番号等を不正に入手し，ドコモ口座に銀行口座を新規に登録することで発生しておりました」とのことであり，「お客さまにより安心・安全にご利用頂けるよう，本人確認をオンライン本人確認システム（eKYC）で確実に行う対策等，更なる対策強化に努めてまいります」との対応策が掲げられた[2]．「ドコモ口座」は，いわゆるQRコード決裁（d払い）に用いることができる．同口座には銀行からチャージができるため，不正利用された銀行口座の持ち主名義で「ドコモ口座」が作成され，さらに物品の購入を経て現金化されたというわけである．報道では，「不正はドコモが手掛ける電子決済サービスのドコモ口座で起きた．犯人は被害者になりすまし，ドコモ口座を開設．不正に入手した口座情報を使って，ドコモ口座と被害者の銀行口座をひも付け，銀行口座からドコモ口座に資金を移していた．最終的にキャッシュレス決済の『d払い』でたばこや家電製品などを購入し，転売していたとみられる」とされている[3]．被害総額は2,776万円，被害額の約6割はゆうちょ銀行であった．ここでは，「ドコモ口座」の開設における本人確認の甘さが指摘されている．報道によると，「きっかけは2019年9月に始めたドコモ口座の『開放』にある．それまでドコモ口座の開設はドコモの通信回線契約者だけに限っていたが，このタイミングでドコモ回線の非契約者もドコモ口座を開設できる『キャリアフリー』と呼ばれる展開に切り替えた」「しかも，ドコモ回線を契約していない利用者は，電子メールによる認証だけでドコモ口座を開設できた．犯人は厳格な本人確認なしに，銀行口座やd払いと連携するドコモ口座を持てたわけだ」とされている[3]．

つまり，「ドコモ口座」は，本来は，NTTドコモの通信回線契約者のみが開設できたので，通信回線の契約時に厳格な本人確認が行われていた（携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（平成17年

法律第 31 号）による）はずであるが,キャリアフリーになった段階で，単なる Web サービス同様に開設できるようになっており，本人確認がまったく行われなくなってしまった．

他方，銀行口座からの出金も，通常の，オンラインバンキングにおける本人確認に比して，著しく甘かった．報道によると，その説明は以下のとおりである．すなわち，「地銀はドコモ口座と銀行口座の連携に当たって，地銀ネットワークサービス（CNS）の『Web 口振受付サービス』を使う．同サービスは，NTT データが提供する『ネット口座振替受付ゲートウェイ（GW）サービス』の利用が前提となっている．CNS は Web 口振受付サービスの開始当初から，通帳残高の入力といった 2 要素認証を実装していたという．2018 年前後には，自動音声応答（IVR）による認証も追加していた．認証方法は銀行ごとに決める仕組みで，今回被害を受けた地銀はセキュリティー水準が低い認証方法を採用していたとみられる」[3]．「Web 口振受付サービス」は，口座振替の Web 版である．正常に「ドコモ口座」と銀行口座が紐付けられた場合，毎回の出金ごとに本人確認がなされるのは，ユーザにとって煩雑である．このような煩雑さを回避するための仕組みというわけである．他方で，不正な「ドコモ口座」と紐付けられてしまえば，何度でも銀行口座から「ドコモ口座」への出金（チャージ）ができてしまう．それにもかかわらず，銀行側の本人確認は，「被害が判明した銀行の多くは名前と口座番号，暗証番号，生年月日の入力だけでドコモ口座との連携を認めていた．これらでは一要素認証にすぎず，明らかに不十分との指摘が出ている」という状態であった[4]．

それでも，銀行側にキャリアフリーへの切り替えが伝わっていれば，Web 口振受付サービス側で，二要素認証や IVR を用いるきっかけがあったかもしれない．ところが，報道によると，被害を受けた地方銀行からは，「キャリアフリーへの移行時期や細かい中身も聞かされていなかった」とされている[3]．

以上，報道から得られる情報をまとめると，以下のようになる．①「ドコモ口座」は，キャリアフリーとした段階で，本人確認を，電子メールによる認証だけにしてしまった．元は，ドコモの通信回線契約者のみが「ドコモ口座」を開設でき，この場合は通信回線の契約時に厳格な本人確認が行われていた．②「ドコモ口座」に関して Web 口振受付サービスを用いて紐付ける銀行の多くは，本人確認を，名前と口座番号，暗証番号，生年月日の入力だけで済ませていた．これは，オンラインバンキングからの振込と比べても緩やかなものであった．③②（銀行口座との紐付けにおける本人確認）が緩やかでも不正利用が多くなかったのは，①（「ドコモ口座」開設時の本人確認）が厳格だったからであるが，「ドコモ口座」がキャリアフリーになったことは，紐付けられる銀行に伝わっていなかった．これにより，銀行は，Web 口振受付サービスを用いて紐付ける際の本人確認を厳格にするタイミングを失した．

のちに，政府は，この事案をまとめている（図 -1）．ここでは，「事案の主な原因」として，銀行は「銀行が資金移動業者と連携する際に，暗証番号といった記憶要素のみで認証していたこと」，ドコモ口座は「ドコモ口座では，銀行において本人確認済みの顧客であるかどうかを確認する方法により本人確認を実施していたこと」とされているが，言葉足らずであるように思われる．まず，銀行の中に「記憶要素のみで認証」していたものがあることはそのとおりであるが，時系列を考えれば，「ドコモ口座」の開設にかかる本人確認が行われなくなったのに，記憶要素のみでの認証を継続していたこと，が問題である．また，「ドコモ口座」が，「銀行において確認済みの顧客であるかを確認する方法により本人確認を実施していた」というのは半分の事実しか述べられていないように思われる．「ドコモ口座」は，本来は，通信回線の契約時に，それ自身で厳格な本人確認が実施されていたが，キャリアフリーへの切り替えにより，単体での本人確認は行われなくなった．銀行との紐付けは Web 口振受付サービスで行われており，銀行側の本人確認が適切になされていたかをドコモが確認するといっても，結局銀行口座と Web 口振受付サービスの有効性のみ確認されていたとすれば，本人確認は実質的には実施されていなかったということになる．この点も触れるべきであろう．

このように，銀行において問題となったのは出金時の

本人確認であり，「ドコモ口座」において問題となったのは出金時および開設時の本人確認である．「ドコモ口座」側の対策としては，「連携先の銀行において実行的な多要素認証が導入されているか確認する」とされているが，資金移動業者側の開設時の本人確認には触れていない．

ゆうちょ銀行への波及

前述の通り，ゆうちょ銀行は「ドコモ口座」の不正利用について金額ベースで 6 割を占めていた．もっとも，前項で整理したとおり，「ドコモ口座」へのチャージの仕組みは，通信回線契約における厳格な本人確認を前提としていると考えれば，どちらかといえば銀行は被害者のようでもある．しかしながら，ゆうちょ銀行は，「連携する 12 社の決済サービスのうち，6 社で不正出金の被害が生じている」という状態であり，銀行口座開設時の本人確認すら，「免許証のように顔写真の付いた本人確認書類が必須ではない」状態であった（顔写真のない本人確認書類を 2 種類用意する必要はあった）．そのため，決済サービスへのチャージによって出金されるほかに，他人名義のゆうちょ銀行口座が作られ，セキュリティが破られたネット証券会社からの出金先にすらされている始末であった[5]．つまり，「ドコモ口座」の不正利用において，銀行側の本人確認に問題があったのは出金時であると思われたが，ゆうちょ銀行では開設時にも問題があったというわけである．

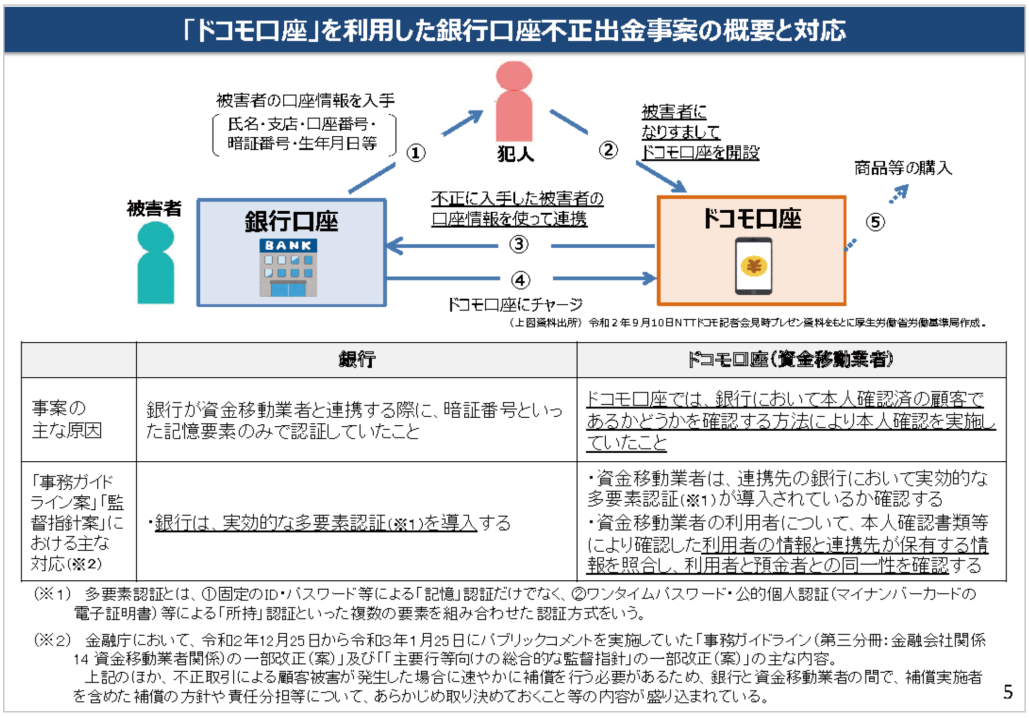
かくして，「ドコモ口座」の不正利用から始まった問題は，ゆうちょ銀行の銀行口座自体の不正利用，多くの決済サービスの不正利用を発覚させることとなったのである．

金融庁による対応

次に，このような問題に対してその後とられた対策について確認してみたい．

(1) 要請文

まず銀行および資金移動業（いわゆる QR コード決裁のスキームの一部である）を所管する金融庁から，「資金移動業者の決済サービスを通じた銀行口座からの不正出金に関する対応について」（2020 年 9 月 15 日付）と



	銀行	ドコモ口座（資金移動業者）
事案の主な原因	銀行が資金移動業者と連携する際に、暗証番号といった記憶要素のみで認証していたこと	ドコモ口座では、銀行において本人確認済の顧客であるかどうかを確認する方法により本人確認を実施していたこと
「事務ガイドライン案」「監督指針案」における主な対応（※2）	・銀行は、実効的な多要素認証（※1）を導入する	・資金移動業者は、連携先の銀行において実効的な多要素認証（※1）が導入されているか確認する ・資金移動業者の利用者について、本人確認書類等により確認した利用者の情報と連携先が保有する情報を照合し、利用者と預金者との同一性を確認する

（※1） 多要素認証とは、①固定のID・パスワード等による「記憶」認証だけでなく、②ワンタイムパスワード・公的個人認証（マイナンバーカードの電子証明書）等による「所持」認証といった複数の要素を組み合わせた認証方式をいう。

（※2） 金融庁において、令和2年12月25日から令和3年1月25日にパブリックコメントを実施していた「事務ガイドライン（第三分冊：金融会社関係14 資金移動業者関係）の一部改正（案）」及び「「主要行等向けの総合的な監督指針」の一部改正（案）」の主な内容。
上記のほか、不正取引による顧客被害が発生した場合に速やかに補償を行う必要があるため、銀行と資金移動業者の間で、補償実施者を含めた補償の方針や責任分担等について、あらかじめ取り決めておくこと等の内容が盛り込まれている。

5

図 -1　政府による「ドコモ口座」不正利用の整理
（厚生労働省第 165 回労働政策審議会労働条件分科会資料 No.3「資金移動業者の口座への賃金支払について」p.5）

して，預金取扱金融機関向けと，資金移動業者向け，それぞれに要請文が発せられた（金融庁監督局長「資金移動業者の決済サービスを通じた不正出金への対応について（要請）」（令和 2 年 9 月 15 日）および金融庁総合政策局長「資金移動業者の決済サービスでの不正出金への対応について（要請）」（令和 2 年 9 月 15 日））．要請文はいずれも，「事案の概要」として，「〇現時点では，＜略＞キャッシュカードの暗証番号のみで認証するケースにおいて，被害の発生が確認されている」とし，資金移動業者等のアカウントと銀行口座を連携して口座振替を行うプロセスに脆弱性がないか確認することが双方で重要であるとされ，脆弱性については，「（注）例えば，上記口座振替契約（チャージ契約）に際して，預金取扱金融機関においてワンタイムパスワード等による多要素認証を実施していない場合など，不正に預金者の口座情報を入手した悪意のある第三者が，預金者の関与なしに資金移動業者等のアカウントへ資金をチャージ可能なケースは脆弱性があると考えられる」とされている．しかしながら，これらの要請は，やはり，出金時の本人確認に問題を集約しており，「ドコモ口座」で問題となった，資金移動業者等の開設時の本人確認に触れていない．

(2) 事務ガイドライン，監督指針等の改正

次に，金融庁は「ドコモ口座」の不正利用等一連の事案を受けて，「事務ガイドライン（第三分冊：金融会社関係）」，「主要行等向けの総合的な監督指針」等の一部改正を行った（2020 年 12 月 25 日～ 2021 年 1 月 25 日パブリックコメント，2021 年 2 月 26 日施行）．ここでは，たとえば，「事務ガイドライン（第三分冊：金融会社関係 14 資金移動業者関係）」において，「II-2-5 口座振替サービス等の他の事業者の提供するサービスとの連携」の項目が新たに設けられ，QR コード決裁サービスにおいて，銀行等への口座振替サービスを用いた出金時の本人確認の厳重化が図られている．また，「主要行等向けの総合的な監督指針」において，「III-3-9 外部の決済サービス事業者等との連携」の項目が新たに設けられ，「当該サービス利用者の預金者との同一性の確認を継続的に把握・評価し，多要素認証等の導入により預金者へのなりすましを阻止する対策」を講ずることを求めている．これも，出金時の本人確認を厳格にするものである．

開設時本人確認の厳格化の必要性

「ドコモ口座」の事案を受けた金融庁の手当は出金時の本人確認に論点が集中しており，「ドコモ口座」およびゆうちょ銀行で起きた，開設時の本人確認の問題については触れられていない．開設時の本人確認を突破されてしまうと，出金時の本人確認は意味をなさないことがある．たとえば，第三者が ID とパスワードを設定し，さらに，端末で完結する生体認証を加えたもので多要素認証とされてしまうと，あとは自由に出し入れできることになってしまう．この点に対策がなされなかった理由としては，すでに犯罪収益移転防止法施行規則の改正で手当がなされていたことによると思われる．しかしながら，この改正は 2020 年 4 月には施行されていたのに，「ドコモ口座」の事案を防ぐことはできなかった．開設時本人確認と出金時本人確認について，資金移動業者等と銀行，相互の継続的なモニタリングが必要であるということになり，しかもその実質が求められているといえよう．

参考文献

1) 板倉陽一郎，間形文彦，藤村明子，亀石久美子：インターネット上の金融関係サービスにおける本人確認義務及び本人みなし条項の民事的考察，情報処理学会研究報告電子化知的財産・社会基盤（EIP）2021-EIP-91(8)，pp.1-6.
2) （株）NTT ドコモ「ドコモ口座を利用した不正利用についてのお問い合わせ窓口設置について」（2020 年 9 月 11 日プレスリリース）．
3) 緊急版　動かないコンピュータ　NTT ドコモ「ドコモ口座」不正の全容　Web 口振に落とし穴，日経コンピュータ，2020 年 10 月 1 日号，p.6.
4) 榊原　康：「安心・安全」の誇りを汚したドコモ不正利用問題で地銀から恨み節，日経コンピュータ，2020 年 10 月 1 日号，p.129.
5) 動かないコンピュータ　ゆうちょ銀行　相次ぐ口座の金銭被害　組織の縦割り体質が真因か，日経コンピュータ，2020 年 10 月 29 日号，p.72.

(2021 年 5 月 1 日受付)

板倉陽一郎（正会員）　itakura@hikari-law.com

2007 年慶大法科大学院修了．2008 年弁護士（ひかり総合法律事務所，2016 年よりパートナー）．2017 年より理研 AIP 客員主管研究員，2018 年より国立情報学研究所客員教授，2020 年より阪大 ELSI センター招へい教授，2021 年より国立がん研究センター客員研究員．本会電子化知的財産・社会基盤研究会（EIP）運営委員．