ドコモ口座問題とは何か、私たちは何をすればよいか

福島県情報化推進アドバイザー
日本大学工学部　情報工学科　情報セキュリティ講座　林　隆史

全国の主に地方銀行の銀行口座から、NTT ドコモの電子決済サービス「ドコモ口座」を使って不正に預金が引き出されるという事件が発生しました。報道によれば、被害の発生した金融機関およびドコモ側の対応はほぼ収束しつつあるようです。

しかしながら、今回の問題はドコモ口座だけで留まるものでなく、他の電子決済サービスや各種電子マネーによる取引においても、容易に発生する可能性があります。

また、NTT ドコモの携帯電話の利用者のみが関係すると思っている人、銀行口座や各種取引口座の暗証番号やパスワードを容易に推測できるものにしている人、複数の取引で共通のパスワードを使っている人はまだまだ多いようです。

そこで、今回の問題について考察し、今後、我々が注意すべきことをまとめてみました。

１．今回の事件の考察

まず、ドコモ口座とは、銀行口座を登録し、入金すれば、「ｄ払い」で買い物や送金ができるサービスです。今回の犯人が他人の銀行の預金者になりすまして、ドコモ口座を開設したとみられています。

➢　なぜ、なりすましができてしまったのか？

ドコモ口座開設時に、本人確認のステップを踏まずに、口座を開設できるシステムが原因の１つと考えられます。悪意を持った第３者(犯人)が、他人名義のドコモ口座を、銀行口座の名義人の確認なしに開設できてしまったのです。

銀行口座にしろ、ドコモ口座にしろ、口座の開設には名義人の本人確認は欠かせません。銀行窓口であれば、銀行口座開設の際、運転免許証や健康保険証等を使って、銀行員による本人確認が行われます。

一方、オンラインでの口座開設では、本人確認の方法として、登録されたスマホにショートメッセージで確認番号を送り入力させる、または、登録したメールアドレスにメールを送り、メール内のリンクをクリックする等の方法がよく使われます。

スマホにショートメッセージを送る方法と、登録したメールアドレスにメールを送る方法は、似ているように見えますが、大きな違いがあります。

スマホは通常所有者（キャリアと契約している人）が特定されます。特定された所有者と、パスワードなどを紐づけて本人確認する方法は、2 要素認証とよばれています。他に 2 要素認証を用いた例として、銀行のキャッシュカードと 4 桁の暗証番号があげられます。

一方、メールアドレスには、そのアドレスの持ち主が明確になっているものとそうでないものがあります。持ち主が明確なメールアドレスとは、メールアドレスを作る際に何等かの方法で本人確認がされているものです。会社のメールアドレス等は、偽造でなければ本人確認がされていると考えられます。

持ち主が明確でないメールアドレスとは、メールアドレス作成時の本人確認が不十分なものです。氏名や電話番号などを登録時に入力していたとしても、その確認が十分ではないものも見受けられます。

本人確認がしっかりとされているメールアドレスであれば、2 要素認証相当の信頼度がありますが、そうでない場合は本人確認が十分とはいえません。

例えば、Amazon はメールアドレスとクレジットカード等を紐づけてユーザ登録をしています。このように持ち主が特定されたクレジットカードと紐づいたメールアドレスは本人確認として使用可能です。

しかしながら、今回のドコモ事件のように、クレジットカード等の本人を特定できる他の情報と結びつけられていないメールアドレスは、本人確認には使えません。

報道によれば、今回の事件では、銀行口座名義人＋銀行口座番号＋ 4 桁の暗証番号と、メールアドレスでドコモ口座の開設ができたと報道されています。「ドコモ口座を開いた人＝犯人」に直接つながる情報がなく、犯人は証拠を（あまり）残さずにドコモ口座を勝手に開設できてしまったと考えられます。

- **犯人はどうやって銀行口座の情報を入手したのか？**

  1．何等かの理由で、犯人が被害者の口座番号を知っていた場合

  暗証番号を入力し、合致した場合に、ドコモ口座を開くことができた可能性があります。不特定多数を狙うことで、偶然合致した人の口座で不正を行った可能性があります。銀行口座の名義人と銀行口座番号の情報は、過去に名義人が行った振込などで知られていたこともありえます。

  2．銀行口座番号と名義人のリストが出回っていた場合

  犯人が 4 桁の暗証番号をランダムに作成し、何度か入力して合致した場合に、ドコモ口座を開くことができたケースと、暗証番号を固定（例えば 1234）して口座名義と口座番号のリストに対し順番に試していき、合致した場合にドコモ口座を開設したケースがあります。

3．同じ暗証番号を複数の口座で使っている人の場合
どこかで暗証番号が漏れてしまい、同一名義の口座でその暗証番号でドコモ口座を開設した可能性が考えられます。

いずれにしても、銀行の口座名義人＋口座番号＋暗証番号で口座を開設されたのが問題だったと考えられます。

4桁の暗証番号は、カードや通帳とセットだから4桁でも機能しているので、カードなどの本人所有物やその他、スマホ等の「本人を確認できるもの」との組み合わせによる本人確認（2要素認証）なしで暗証番号を使ったのはとても危険なことだと考えられます。
犯人がドコモ口座を開設したときに、銀行口座に登録されている名義人のスマホや、銀行に登録してあるメールアドレス、住所、などに連絡があれば、今回の事件は防げたかもしれません。

2．私たちは何をすればよいか

➢ 今回のドコモ口座事件の被害をうける可能性のある人

- ドコモ口座と連携している銀行に、銀行口座を持っている人全員。
  ドコモの携帯を使っているかどうかは関係ありません。今回の事件では、銀行口座の口座番号、暗証番号とメールアドレスでドコモ口座が開設されています。メールアドレスは銀行口座の持ち主とは無関係のものです。
  犯人がドコモ口座開設時に指定した他人の銀行口座から、ドコモ口座にお金が移されてしまったようです。

➢ 自分が被害を受けたかどうかの確認

- ドコモ口座と連携している銀行に銀行口座を持っている場合、口座の取引状況を通帳記入やネットバンキング等で時々確認し、身に覚えのない怪しい取引があったら、すぐに銀行に知らせてください。
  ドコモ口座と連携している銀行は以下で確認できます。
  https://docomokouza.jp/detail/bank_list.html
- NTTドコモでもお問い合わせ窓口を開設しています。
  https://www.nttdocomo.co.jp/info/notice/page/200911_00.html

➢ ドコモ口座の事件は特別なのか

- ドコモ口座と同様に、別の金融機関と連携した口座を簡単に開設できるものがあれば、同様のことは起こりえます。実際に、LINE Pay で同様の不正取引が発生しています。

➢ ではどうすればよいのか

- ドコモ口座の事件であれば、前述のように、ドコモ口座と連携している銀行の利用者がターゲットになりますが、他にも同様の犯罪は起きている可能性はゼロではありません。どの銀行を使っているかに関わらず、自分の持っている銀行口座は折に触れて記帳、またはネットバンキングで怪しい入出金がないか確認し、怪しい入出金があったら銀行等に相談してください。
- 簡単な暗証番号の人はすぐに変更してください。

➢ 出金だけでなく、入金もあぶないのか

- 身に覚えのない入金の場合、
  １）特殊詐欺の口実（誤って入金したからカードを貸してほしい）
  ２）犯人が捜査をかく乱するために、無関係の人を仲間にでっちあげる
  等の可能性もあるので油断はできません。

おわりに

今回のドコモ口座問題は、特別な事件ではありません。今回の問題と同様のものはこれからも起こると考えるべきです。オンラインを使ったシステムは、通常の利用者にとって便利なだけでなく、犯罪者にとっても離れたところから、こっそり犯罪を実行できる可能性を持っています。

本人確認をするための仕組みは二要素認証などを含め、改良が続けられていますが、完璧な方法はなかなか実現できません。過去に、優秀な本人確認システムではあるが、使いづらいため、世界中で利用しようという話がでた後に、下火になったものもあります。

大事なのは、

- 誰かがなんらかの方法で自分のお金を引き出すかもしれない。
- 他人が自分になりすまし、買い物をするかもしれない。

という危機感を持って、

- 折に触れて口座の取引状況を確認する。
- 購入履歴をよく確認する

以上を忘れないことです。

口座連携など便利なものが増えるとそれを悪用した犯罪も増えます。便利さを享受するには、自己責任が伴います。いろいろと確認するのは面倒ですが、大切な自分の資産を守るために、必要なことです。これらを踏まえた上で、便利なシステムを利用するようにしましょう。