2119116s 経済学部 2 年　佐野　海徳

2020 年、NTT ドコモの電子決済サービスである「ドコモ口座」を使った預金の不正引き出しが行われる事件があった。2020 年 10 月 16 日時点で被害総額は 2850 万円に上り、大きな被害をもたらした。ではどうしてこんな事件が起こってしまったのか。私はシステム自体に脆弱性があったこと、関係した各金融期間やドコモの企業・金融機関としての姿勢がよくなかったこと、そして顧客自体にも原因があると考えている。

NTT ドコモによれば銀行口座からドコモ口座へと送金するのに必要だった情報は「名前」、「生年月日」、「口座番号」、「キャッシュカードの暗証番号」であるという。犯人はこれらを不正に入手していたというのである。ではどうしてこうした事態が起こったのか。考えられる要因はいくつかあるが、まず考えられるのは他のセキュリティが脆弱なサービスから「名前」と「生年月日」が流出したというものである。サービスの脆弱性を悪用してログイン ID, パスワードを窃取することで他のサービスにログインし、生年月日や名前の情報を手に入れることができてしまうという寸法である。実際、ログイン ID やパスワードを使い回すユーザーは少なくないためにこうした攻撃が成功する。また、サービス自体のセキュリティが甘ければ (情報を暗号化しない、データベースにアクセスする権限の甘さ等)、データベースに保管されている個人情報が盗み出されてしまうということもありえるし、そういった事例も存在する。では暗証番号はどうであるか。これは力任せに当てはめていってもいつかは破ることができる。コンピュータをうまく使えば短期間で漏れなく、人力よりはるかに多くの暗証番号のパターンを列挙することができる。これはパスワードやユーザー ID にも当てはまるし、暗証番号の桁数がわかっていれば暗証番号の入手はそう難しくはない。ちなみに 8 桁の暗証番号くらいであれば 2 秒もあればコンピュータは列挙できてしまう。今回の場合であれば暗証番号は 4 桁の数字であるから、もっと速く列挙してアクセスできることは自明である。また、この事件で被害が確認された全 11 行がドコモ銀行と銀行口座のヒモ付の際に二段階認証を実施していなかった。二段階認証というのは ID・パスワードによる本人確認に加え、ショートメッセージなどを用いて本人確認を行うというものであり、なりすましに対しての有効な対処法と言われている。こうした方法を用いていなかったため、パスワードとログイン ID がわかっていれば誰でもログインでき、利用者にログイン試行が知らされることがなく不正引き出しが行われ、結果として大きな被害を生んだと言える。上記のような脆弱性がシステムに存在すれば、不正アクセスを防ぐことは不可能である。

次に関係した各金融機関・そしてドコモの姿勢が悪かったというのはどういうことかを考える。まず第一に考えられるのはネットバンキングという分野に対しての理解不足である。確かに「バンキング」という意味では普段行っている業務と似通ったところは存在するだろうし、そうした意識があったからネットバンキング事業を始めたという側面はあるだろう。そうやって事業

を拡大していくことで他の金融機関との競争が起こ消費者目線でよりより良いサービスを選ぶことができるようになるので悪いことばかりではないのだが、しかし認識が甘すぎたと言わざるを得ない。前述した二段階認証の不採用は最たる例である。「情報の漏洩」によって何が起こり得るか、そして起こった場合どのような影響があるかを考えられていればそのようなずさんな事業参画・運営はなされなかっただろう。一言で言えばネット社会に適応できていないのに適応者のふりをしてしまったということである。この事件の前には 7pay 事件も起きていた。この事件の教訓が生かされていないのは、自分たちは大丈夫だろうという油断が招いた失態だと言わざるを得ない。これは推測でしかないのだが、もしリスクの計量化という視点があったとして、「インターネットに特有のインシデント」が発生するという可能性が見えていなければリスク計量化もうまく働かないだろう。VaR は過去の事象をもとに推計されるものであり、さらに未来に関して起こる事象として「情報漏洩」が組み込まれていなければ VaR は意味が薄れる指標になってしまうということがしめされた事例だともいえるのではないだろうか。また、この事件が起こったときに私は率直に「IT の専門家はいなかったのか」と感じた。いたとしたらどうしてこんなにセキュリティの甘いサービスをリリースしたのか。人選のミスと見通しの甘さが招いた事態だと感じる。

では利用者側の原因とは何か。これはまず IT への不理解、そして怠惰である。まず、細かいところまで理解するべきであるとは言わないが、どのような方式での本人確認が安全性が比較的高いものかといった知識があれば少しは被害者、被害額の規模は抑えられたのではないのだろうか。利用者側は今や多くのサービスから気に入ったものを選ぶことが大抵の場合可能になっているのだから、サービスごとに自分に降りかかるリスク等の重さを比較して考えることもできるはずである。言い方は悪いかもしれないが、サービスを疑ってかかるのも一つの自衛方法であるだろう。怠惰というのはどういうことか。端的に言えばパスワードや ID の使いまわしである。これは私もよくやってしまうので自戒の面もあるのだが、これによって無駄に自分の情報を漏洩させるリスクを上げていると言える。実際、多くのサービスでパスワードや ID を変えることで覚える量はうんざりするくらい多くなる。しかしこれを嫌がることが自分を危険に晒す可能性を高めるなら、一考の余地がある。自分に合った方法でパスワード等をうまく管理することが肝要である。また、最新のセキュリティなどの情報を追うことで少しでもリスクを下げることができるかもしれない。そうした可能性を捨てて事件で話題になって初めて考えるのでは少し遅いのではないかとも考える。

サービスの運営にあたった企業や、サービス提携した金融機関のセキュリティやリスク管理の考え方が甘かったのは言うまでもない。特に類似の事件が発生した後であったがために非常に情けないことであるとも感じる。しかし、企業にすべて押し付けて利用者が完全な被害者であるというのは、確かに責任の所在の 9 割以上は利用者にないとは思うが、いささか難しい。現

代ではサービスを利用する側にも高いリテラシーが要求されていると考える。
私達もこうした事件を他人事だとして流してしまうのではなく、どうしたら
このような事件に巻き込まれるのを防げるか、現在利用しているサービスは
本当に安全性が高いか、といったことを見直す必要があるだろう。
参考https://www.nttdocomo.co.jp/info/notice/page/200908_02_m.html
https://flets-w.com/user/point-otoku/knowledge/security/security24.
html
https://www.businesslawyers.jp/articles/832
https://xtech.nikkei.com/atcl/nxt/column/18/00138/101900652/?P=
2
https://www.sankeibiz.jp/business/news/200916/bse2009160655002-n1.
html