社会 #事件 #iPhone 2023/03/28 14:00

カネも思い出もすべてを奪われる…米国で被害が急増中の「Apple ID泥棒」の卑劣すぎる手口

鉄壁のセキュリティの「最大の弱点」を悪用している

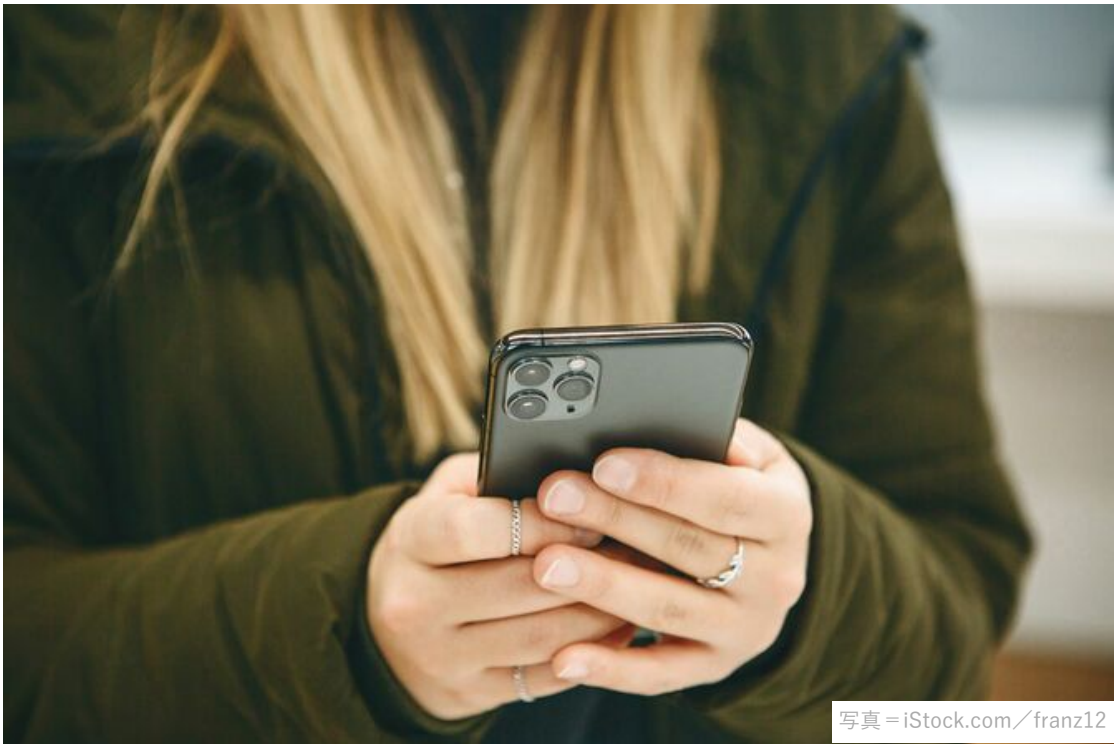
PRESIDENT Online

青葉 やまと
フリーライター・翻訳者

1 2 3 4 5 6 7 次ページ

「6桁のパスコード」を盗まれただけで…

いまアメリカで、スマホ経由で資産やデジタル上の情報などを根こそぎ奪われる事件が多発している。被害者の多くはiPhone利用者だ。Appleは製品同士の連携に優れ、ユーザーのプライバシーを重視する姿勢でも知られている。だが、被害を防げるとは限らない。



写真＝iStock.com／franz12

※写真はイメージです

全ての画像を見る（5枚）

被害者たちは、外出先でiPhoneを盗まれ、わずか数分後にはアカウントから閉め出される。次いで自宅のMacはログインができなくなり、24時間以内に数百万円という預金

が口座から消える――。そんな事例をウォール・ストリート・ジャーナル紙が報じている。

被害のきっかけは、iPhoneの4桁または6桁の簡易的なパスコードを盗み見られたことだ。これによって、より強力なパスワードを設定したはずのApple IDのセキュリティが同時に無力化されてしまった。

同紙が今年2月に「脆弱性」として報じ、さまざまなテックメディアで取り上げられ大きな反響を呼んでいる。Appleは現時点で対策措置を発表していない。

被害はiPhoneからほかのApple製品に広がる…

これはiPhoneの6桁のパスコードさえわかれば、Apple IDのアカウントを丸ごと乗っ取れる状態であることを意味する。

Apple IDとは、多くのApple製品において本人証明に用いられる共通のアカウントであり、その権限は絶大だ。これまでに撮り溜めた写真や各サイトのパスワード、そして場合によってはMacの全データのバックアップなど、デジタル上の記録の大部分を一元管理するクラウドサービス「iCloud」への侵入を許してしまう。

Androidを利用している方は、Googleアカウントが誰かに乗っ取られることを想像していただければ、ほぼそれに近い。

一度乗っ取られると、盗難対策を兼ねているはずの「iPhoneを探す」機能や、リモートによるセキュリティ制御も無効化されてしまい、被害者は対応手段を失う。

犯人はプライベートな写真を盗み見ることや、パスワード・機密情報管理アプリの「キーチェーン」に保存してある社会保障番号（日本のマイナンバーに近い）をのぞき見ることも可能となり、アプリストアでの購入や金融アプリ経由での送金もやりたい放題だ。

写真＝iStock.com／DKart

※写真はイメージです

以前から危険性を指摘する声も上がっていたが、ウォール・ストリート・ジャーナル紙が詳細を報じたことで、多発する被害の実態が明らかになった。同紙は、「世界中で10億台以上使われているiPhoneのソフトウェア設計に内在する、シンプルな脆弱性」が悪用されていると述べ、設計上の欠陥が影響しているとの見方を示している。

iPhoneを奪われた31歳女性の「乗っ取り被害」

同紙は、被害事例が「全米の警察署に山積み」になるほど多発していると述べ、具体例としてマンハッタンのバーで被害に遭ったという31歳女性の話を報じている。

記事によると事件は、昨年11月、週末の早朝に発生した。被害に遭ったレイハン・アヤスさんは、バーで隣の席にいた男性と打ち解け、愉快な会話を楽しんだようだ。

だが、店を去る瞬間になって男性の態度が急変。アヤスさんのiPhoneをひったくり、そのまま持ち去った。初めからiPhoneを奪い取る目的で接近したとみられる、と同紙は報じている。

ITのスタートアップ企業で働く彼女の反応は、素早かった。iPhoneが盗まれた際のほぼ理想的な対応を取っている。同紙の取材に対し、奪われてからの行動をこのように振り返った。

「すぐに友人の携帯を借り、『iPhoneを探す』にログインしました」

この機能はAppleが提供しているもので、Apple IDを登録したユーザーであれば誰でも、持っているiPhoneやMacなどの現在位置を確認したり、リモートからロックし不正利用を防止したりすることが可能だ。いや、正しくは、“可能なはずだった”。

「（ログインは）できませんでした」と、アヤスさんは厳しい表情を浮かべる。
「（iPhoneが）奪われてから3分のうちに、自信を持って覚えていると断言できる私のApple IDのパスワードが、変更されていたのです」

IDを奪われ、130万円を銀行口座から引き出された

犯人は周到な計画のもと、iPhoneをひったくった直後、アヤスさんのApple IDを乗っ取っていたのだ。これはつまり、アヤスさんがiPhoneの正規の持ち主であることの証明が、敵の手に渡ったことを意味する。後述するが、iPhoneのパスコードさえ知られてしまえば、盗まれたiPhoneで容易にIDの乗っ取りを許してしまう。

こうなると、盗難対策の要である「iPhoneを探す」は、もはや使うことができない。Appleのシステムから見れば、アヤスさんはもうiPhoneの持ち主でも何でもない、赤の他人だからだ。自宅のMacBookにもログインできず、所有するApple製品から完全に閉め出された。

ただでさえスマホを失い、なすすべなくただ肩を落とすアヤスさんを、さらなる悲劇が襲った。24時間と経たないうちに、銀行口座から多額が引き出されていることに気づいたのだという。

被害額を訊（たず）ねるウォール・ストリート・ジャーナル紙のリポーターに、アヤスさんは表情を一段とこわばらせる。「1万ドル（約130万円）ほどです」。

同紙によると、このような被害は多発しているのだという。ほかにも3万5000ドル（約465万円）を失ったという被害者からの報告が同紙に寄せられているほか、ニューヨークだけで「幾多の被害者」が存在すると同紙は報じている。

#事件 #iPhone

摘発されたiPhone窃盗団、被害総額は3680万円に上る

これとは別に、米CBS系列のミネソタ局は、12人が関与する「高度に組織化された」犯罪により、男性がiPhoneを盗まれ1万5000ドル（約200万円）が口座から流出したと報じている。

同州のスター・トリビューン紙によると、この窃盗団はすでに告発された。記事は、「40人以上の被害者からアプリを通じて盗み出された金額は合計27万7000ドル（約3680万円）に上る」と述べ、大規模な犯罪であったと報じている。

ミネソタの窃盗団が告発されたことは朗報だが、残念ながら被害がこれで収まることはなさそうだ。同様の被害はデンバーやボストンなど全米各地ほか、イギリスのロンドンでも報告されている。各地の犯罪集団が暗躍していると考えられる。

すべては「6桁のパスコード」を盗み見られたことから始まった

携帯を盗まれただけで、なぜあらゆる資産とデータを失った揚げ句、自宅にあるMacまで使えなくなってしまうのだろうか？　iPhoneはパスコードでロックされており、金融機関にはまた別の暗証番号を使用しているはずだ。Macのログインパスワードも、Apple IDのパスワードも、それぞれ異なる。

ウォール・ストリート・ジャーナル紙は、その手口を次のように解説している。まずiPhoneのパスコードの奪取は、原始的な手段で行われる。多くの被害者に共通しているのは、バーで新しい人間と親しくなり、その後iPhoneを奪われるというパターンだ。

犯人たちはバーで会話を広げるなかで被害者を油断させ、相手がパスコードを使って携帯を開く瞬間を待つ。一度でも面前でパスコードを入力すれば、たとえどれだけ素早く入力を終えたとしても、その瞬間に被害者のApple IDは相手の手に落ちたも同然だ。

ミネソタ州ミネアポリス警察のロバート・イリチコ氏は同紙に対し、「容疑者の一人が被害者の肩越しに、入力するパスコードを録画していることが考えられます」と警鐘を鳴らしている。

Apple関連のニュースを報じるアップル・インサイダーは、Instagramなどソーシャルメディアを見せて、などと誘い込み、目の前でiPhoneのロックを解除させ、パスコードを盗み見る手口も存在すると指摘している。

iPhoneが抱えている「シンプルな脆弱性」

しかし、こうして奪われるのは、iPhoneで使われる簡易的な6桁のパスコードだ。より高度で複雑な、英数字や記号混じりのパスワードを設定しているApple IDまで犯人グループの手に落ちてしまうのは、なぜだろうか？

ウォール・ストリート・ジャーナル紙のジョアンナ・スターン記者は、類似の事件を複数取材したうえで被害の共通項を見いだし、そのからくりを次のように説明している。

iPhoneとそのパスコードを奪取した犯人は、即座にパスコードでiPhoneのロックを解除する。続いて「設定」アプリを開くと、ここから被害者のApple IDのパスワードを変更することができる。

ここからが重要なポイントだ。通常のシステムでは、パスワードを変更する場合、本人確認として現在のパスワードをまず入力するように求められる。非常に基本的かつ重要なセキュリティのしくみだ。

ところが、iPhoneからApple IDのパスワードを変更する場合、本来求められるべきApple IDのパスワードではなく、iPhoneのパスコードの入力画面が出現する。つまり、いくら複雑で強固なパスワードでApple IDの守りを固めていても、iPhoneの簡易的なパスコードが漏れると、Apple IDのパスワードは好き放題に上書きされてしまうのだ。

これが同紙の指摘する、「世界中で10億台以上使われているiPhoneのソフトウェア設計に内在する、シンプルな脆弱性」だ。

※写真はイメージです

米メディアが報じた「Apple ID泥棒」の手口

犯人はさらに、被害者を完全にApple IDから閉め出すべく、数分のうちに一連の操作を行う。まずはリモートで位置情報を追跡できる「探す」をオフにし、現在地をくらませる。

続いて「信頼できるデバイス」に登録されたMacやiPadなどを、リモート操作でサインアウトする。被害者は通常、まだ手元に残っているこれらのデバイスからApple IDのパスワードのリセットをリクエストし、パスワードを取り戻すことが可能だ。だが、サインアウトさせられてしまうと、この手だては絶たれる。

この際に犯人は、Macの内容をリモートで消去することも可能だ。消去機能は、本来は紛失時にMacのデータを守る最後の砦（とりで）だ。強力な機能だけに、Apple IDが悪意ある相手の手に渡った際には問題となる。Apple IDを失ったユーザーはiCloud上のバックアップにもアクセスできないため、すべてのデータをごっそりと失うことになる。

所有者の回復手段をあらかじめ奪う周到さ

さらに犯人たちは、Apple IDの「信頼できる電話番号」を書き換えることで、被害者がSIMを再発行したとしても2段階認証を実施できない状態にし、本人であることの証明手段を無効化する。

このとき、登録済みのiPhoneに警告のための通知が送られるが、覚えているだろうか――通知が送られる先のiPhoneは、すでに犯人の手に落ちている。

手の込んだことに、続いて犯人たちは、「復旧キー」と呼ばれる文字列まで発行する。これは本来、Apple IDを忘れた際にパスワード代わりに入力できる予備の手段だ。

だが、発行することで副作用が生じ、家族や友人のiPhone経由でパスワードをリセットできない次ページ制限がかかる。そして、この副作用こそ犯人のねらいだ。被害者が友人を頼ってパスワードをリセットすることは、この段階で不可能となる。

次ページ

本人になりすました犯人を止める術はない

こうしてApple IDの所有者になりすました犯人は、もはやデジタルの世界で好き放題に振る舞うことができる。

パスワード管理アプリの「キーチェーン」も操作可能となるため、ここに一元管理されている金融アプリ用のパスワードや社会保障番号なども一斉に漏れることになる。

iPhoneのログイン用に、顔認証のFace IDや指紋認証のTouch IDを利用している場合、パスコードが漏れても安全に思えるかもしれない。

だが双方とも、認証に数回失敗した時点で、自動的にパスコードの入力画面に切り替わる。犯人は顔認証にわざと失敗し、その後でパスコードを入力すれば良いだけだ。つまるところパスワードを把握されてしまうと、これらの生体認証も無力化されるに等しい。

「Appleのサポートはまったく役に立たなかった」

口座から1万ドルを奪われたあと、せめてApple IDへのアクセスを戻してもらおうとAppleのサポートに一縷（いちる）の望みを託したアヤスさんだったが、結果は期待外れだったようだ。米インサイダーの取材に対し、「まったく役に立たなかった」と憤る。

警察に被害届を提出したが、それをもってしてもどうやら、アカウントの復旧を取り計らってもらうことはできなかったようだ。電話口の担当者は、「iPhoneを探す」などの基本的な操作を試したかどうかを何度も確認してくるだけだったという。

「当然（紛失から）3分で試しましたよ、もちろんです。冗談でしょう、人生のすべてがボロボロなのに、まだ試したかと聞いてくるなんて」

押し問答の末、担当者はアヤスさんに、iCloudのデータを取り戻す手段はないと告げた。

悪夢は続く。アメリカですでに導入されているクレジットカードのApple　Cardについて、アヤスさんの名義で発行申請が行われていることが発覚した。皮肉にもサポートとの通話のまさにその最中、申請が承認されたとのメールがアヤスさんのもとに届いたという。

Androidも脆弱性を抱えている

不幸中の幸いというべきか、アヤスさんの場合は米法の規定に基づき、金銭的な被害については銀行の補償を受けることができたという。しかし、重要なデータは依然戻らない。「Appleの善良な顧客」を自認していた彼女の心に、傷を残す結果となった。

こうした犯罪の被害者として、iPhoneユーザーが集中的にねらわれているようだ。ミネアポリス警察のイリチコ氏は、ウォール・ストリート・ジャーナル紙に対し、「私が捜査に臨んだ件では、盗まれた携帯の99％がiPhoneでした」と語る。用済みとなった携帯を処分する際、高値で売りやすいためだとイリチコ氏はみている。

ただし、テックメディアのギアライスは、AndroidとGoogleアカウントも基本的に同様の脆弱性を抱えていると指摘する。AndroidのPIN（パスコード）を盗み見られ、次いで携帯を奪われると、Googleアカウント全体が大規模な脅威にさらされるおそれがある。

※写真はイメージです

安全性と利便性との板挟み

こうした状況への技術的な対策が望まれるが、Appleとしても対応を取りづらいところではある。同社として取り得る対策は、Apple IDの変更の際にパスコードではなく、Apple IDのパスワードを求めるという改善だろう。しかし、それも数秒程度の時間稼ぎに終わるおそれがある。

多くのユーザーはApple IDのパスワードを「キーチェーン」に保存していると考えられ、そのキーチェーンはiPhoneのパスコードがあれば解錠できてしまうからだ。

現状でユーザーが取れる最も重要な自衛策は、パスコードの入力に慎重になるという1点に尽きる。流出すれば、預金だけでなくデジタルデータの大部分が失われるおそれもあり、銀行の暗証番号などよりも格段に被害が大きい。人前でパスコードを入力する際は、カードの暗証番号を入力するときのように、確実に画面を手で覆うなどの対策を取りたい。

公共の場ではパスコードの入力を避け、顔認証や指紋認証のみを使うことも有効だ。また、「設定」アプリから英数字混じりの複雑なパスワードに変更することも可能だが、肩越しに録画されてしまえばあまり意味がない。複雑なパスワードを使うこと自体はセキュリティ上望ましいが、依然として入力時には周囲に気をつける必要があるだろう。

加えるならば、銀行アプリや送金アプリなどの重要なパスワードは、キーチェーンに保存しないという方針も検討に値する。利便性との板挟みであり、すべての人が実行できる策ではないこともまた確かではあるが。

スマホを盗まれたらどうしたらいいのか

万一、iPhoneとパスコードが同時に失われると、打てる手だては非常に限られる。

用心深いユーザーならば日頃から、信頼できる家族や友人を「アカウントの復旧用連絡先」に指定しているかもしれない。この場合、家族や友人のiPhoneを使ってコードを受け取ることで、Apple IDのアカウントを復旧することは可能だ。だが、前述のように犯人が復旧キーを生成した瞬間、この手だては無効となる。

復旧用連絡先を設定していなかった場合も、自分でMacやiPad、PCなどからウェブ版のiCloudにログインし、当該のiPhoneを「紛失モード」にすることは可能だ。iPhoneは遠隔でロックされる。しかし、この状態でもiPhoneは、すでに漏洩（ろうえい）している6桁のパスコードを受け付けてしまう。実質的に遠隔ロックとは言えない状態だ。

最も安全な手だては、即座にiCloudにログインし、紛失したiPhoneをApple IDのアカウントから削除することだ。問題のiPhoneがApple IDの「信頼できるデバイス」から除外されるため、それ以上の被害を食い止められる可能性がある。

しかしAppleは、「AppleCare＋盗難・紛失プラン」に加入している場合、補償が承認されるまではこの操作を実施しないよう呼びかけている。承認が下りる頃には、犯人はすでにApple IDのパスコードを変更しており、被害はさらに広がっていることだろう。

パスワードを人前で入力してはいけない

企業側としてもセキュリティには何重もの配慮をしているが、iPhoneとパスコードを同時に失うという状況においては、決定的な保護策を打ち出せていないのが現状だ。

デジタルで情報を一元管理する危険性はずいぶんと前から指摘されているが、それでもまだ、数百万円を失う被害が絶えない。まずは6桁のパスコードを人前で入力しないことを鉄則とし、少しでも安心できるデジタルライフを送りたい。