フィッシングに立ち向かう

二要素認証（多要素認証）とその先

「フィッシング」と言う言葉をご存知ですか？金融機関や通販サイトを装って偽の不正なサイトへ誘導し、個人の住所、氏名、銀行口座番号、クレジットカード番号、パスワードなどの個人情報を詐取する行為をフィッシング（詐欺）と言います。ニュースで大きな話題になった「ドコモ口座」の事件も、利用された暗証番号などはフィッシングで詐取された可能性があると言われています。ニュースでは「“二要素認証”を採用していれば防げた」や「“二要素認証”を採用していたサービスからは被害がなかった」ということを耳にしますが、“二要素認証”とはいったいどのようなものなのでしょうか？また二要素認証で本当にフィッシングを防ぐことができるのでしょうか？

フィッシングとは？

フィッシングとは、前述の通り金融機関や通販サイトを装って偽の不正なサイトへ誘導し、個人情報を詐取する行為のことです。具体的には、誰もが1度は利用したことがあるような大手の銀行や通販サイトや有名企業の名前やサービスをかたり、メールや携帯番号宛のSMS（ショートメッセージサービス）が送られてきて、不安を煽ったり興味を引くような内容で言葉巧みに不正なサイト（フィッシングサイト）へ誘導しようとします。
サイトへ誘導されると一見では本物のサイトと区別がつかなくなっており、個人情報を入力させるという手法です。
特にここ最近ではコロナ禍の影響で通販需要が増え、6割以上が大手通販サイトを装っているというデータもあります。

二要素認証（多要素認証）とは？

本人を認証（確認）するための「知識」「所有」「生体」の3つの要素の内、2種類の要素を組み合わせて行う認証方法を二要素認証と呼び、2種類以上の要素を組み合わせる方法をまとめて「多要素認証」と呼びます。
認証の3要素「知識」「所有」「生体」とは、

【知識認証】
本人だけが知りうる情報を使った認証。「ID・パスワード」や「秘密の質問」など。

【所有物認証】
本人が持っている物を使った認証。「ICカード」「トークン」「ワンタイムパスワード」など。

【生体認証】
本人の身体的な特徴を使った認証。「指紋」「顔」「虹彩」「静脈」など。

二要素認証と二段階認証は何が違う？

以前「7pay」で不正ログインされたというニュースがありましたが、ここで注目されたのが「二段階認証」です。
他人が簡単にパスワードを再設定できたため起きた事件であり、二段階認証を導入していれば防げた（または被害を少なくできた）と言われています。
二段階認証は二要素認証とは違い、認証を2段階に分けていれば利用している認証要素は1種類でも構いません。
よくある例で言えば「ID・パスワード」を入力させた後に「秘密の質問」を入力させるといった場合がこれに当たり、認証の方法はどちらも「知識認証」で要素は1種類となります。
上記のような二段階認証では、ブルートフォースアタックという全てのパターンでログインを試すような攻撃に対しては弱く、そもそもフィッシングによってどちらの情報も盗まれる可能性があるため、認証方法としては十分とは言えません。
そこでより確実に本人と確認するために「二要素認証」が利用されるようになってきました。

二要素認証での対策でも不十分？

二要素認証で主に利用されているのが「ID・パスワード」を入力させた後に、本人の携帯電話のSMS宛に1回限りの「ワンタイムパスワード」を送信し、それを入力させることで本人確認するといった方法で、この方法ですと本人の所有している携帯電話でないとパスワードが受け取れないため、フィッシングで「ID・パスワード」が盗まれたとしてもその先には進めず対策として非常に有効とされてきました。
ですが、最近ではこのSMS宛のワンタイムパスワードも入力させるようなフィッシングサイトが増えています。また生体認証でも写真や指紋を入手されて悪用される可能性があったり、生体情報を認識するAIに本人情報を与えてなり替わるようなことも起こりえるので、対策としては不十分と言われています。

これから求められる対策

【ユーザー側】
- PCは当然ですがスマホにもセキュリティ対策ソフトを入れる
- メールやSMSの送信元（From）の確認
  送信元が信頼できる相手か確認する。表面上では偽って表示させている場合もあるので注意が必要。
- メールやSMSに書いてあるアクセスするURLの確認
  URLに不審な点がないか、正規のサイトか確認する。
- アクセスしたサイトのURLの確認
  普段アクセスしているURLと違っていないか確認する。
- ブックマークからアクセスする
  普段利用しているサイトをブックマークしておき、必ずブックマークからアクセスする。
- 自分の利用しているサービスを把握しておく
- 銀行口座やクレジットカードの利用履歴をこまめにチェック

【ネットバンキング、決済や通販サイトなどサービス提供側】
FIDO（ファイド）という認証に関する業界団体によって、専用のソフトウェアやハードウェアなしで指紋や顔認証を行い、かつパスワードを使用しない認証技術（FIDO2）が開発されており、今年に入りAppleもこの団体へ加盟し環境も整いつつあります。この技術を利用することで本人のPCやスマホからのみ認証可能となるため、現在のフィッシング被害を防げるようになると考えられています。

開発室から

ようやく庭の栗の木に実がなりました。公園から拾ってきた栗の実を庭に埋めてから、かれこれ7，8年になります。今まで一粒もできなかったのに、今年はたくさんの実ができました。が、気が付けば栗の木の下には中が空っぽのトゲトゲだけが落ちています。どうやら鳥たちが実を取って行くみたいです。でもまだまだたくさんあるから気にしません。