二段階認証とは

「認証」というと難しそうですが、実は日常的にみなさんが行っているパソコンやスマートフォン、ATM などを利用するときに行うログイン、ログオン、サインインなどと呼ばれている作業、iPhone のロックを外すときの「Touch ID」や、目で見たり、タッチしたりするだけでサインインできる「Windows Hello」なども「認証」です。

「認証」は、パソコンやスマートフォンなどの端末やサービスなどを「誰が扱うのか」や「その人物が利用する正当な本人か」を識別する役割を持っています。コンピュータが開発されてからこれまで、ほとんどの認証には「ID とパスワード」が用いられてきました。

パスワードには、漏えいによる不正アクセスの被害が起き、そのうえ漏えいしたパスワードを使い回していたことにより被害が広がったことなどの問題が起こっています。また、類推しやすいパスワードを使用したことでパスワードが不正に使われることが起き、その対策としてパスワードを複雑にしたり長くしたり定期的に変更したりと使いにくさが増してきています。

この問題に対処する手段として使われるようになったのが「二段階認証」です。オンラインバンクやクレジットカード決済などに使われています。

「二段階認証」には、1 段階目は「ID・パスワード」で 2 段階目は携帯電話のショートメールへ認証番号を送ってそれを入力させる、持参したカードをカードリーダーに読ませてそのリーダーに PIN コードを入力するなどがあります。

現在「認証」に使われている要素（方法）には次の 3 種類があり、「認証の 3 要素」と呼ばれています。

１．知識：あなたが知っていること
（例：パスワード、暗証番号、秘密の質問、パターンなど）

２．所有：あなたが持っているもの
（例：IC カード、スマートフォン（ＱＣコードアプリ）、携帯電話用 SIM カード（SMS メッセージ用）、キーホルダートークン、USB トークンなど）

３．生体：あなた自身のもの。身体的特徴

（例：指紋、顔、静脈、虹彩など）

この３要素は、それぞれ互いに影響を与えたり、関連があったりすることはないため、認証するときにこれらを組み合わせることにより本人以外が認証を受けることが難しくなります。

今、使われている多くの「二段階認証」では、知識要素であるパスワードと、所有要素である「番号を登録済みの自分の」スマートフォンといった異なる２つの要素を利用しています。このように２つの要素を使用するため「二要素認証」とも呼ばれています。

今後、スマートフォンの普及によりスマートフォンを使用した「二段階認証」は多く使われるようになるでしょう。