

## パスワードと PIN コード

みなさんは、スマホやパソコンなどの IT 機器や、各種のウェブサービスを使う上で、必ず「パスワード」を使用しています。「パスワード」は、機器やサービスを利用するときに、正式な利用者や持ち主である自分だけが利用でき、他人が利用できないようにするための鍵の役割を果たすものです。パスワードはいわば「家の鍵」や「金庫の鍵」。これを適切に守らなければ、家や車、金庫を勝手に開けられてしまうように、パソコンやスマートフォン、ウェブサービス上にあるみなさんの個人情報やメール、銀行口座が攻撃者に不正にアクセスされ、情報が流出したり、お金を盗まれたりしてしまいます。

「パスワード」と一口に言っていますが、セキュリティ上の性質から大きく 3 つに分けることができます。

1. 銀行のキャッシュカードやクレジットカードの利用時や、パソコンのサインイン、スマートフォンのロック解除時に使用し、通常 4 桁や 6 桁ぐらいの数字だけで構成されることが多いもの（暗証番号や PIN、PIN コード、パスコード。）
2. パソコンやデジタル機器、ウェブサービスなどの利用時に ID とセットで入力し、英大文字小文字+数字+記号混じりで 10 桁以上など、複雑さと一定以上の長さが推奨されるもの（狭い意味でのパスワード、ログインパスワード）
3. パスワードと呼ばれていることもあるけれど、本当はファイルや通信内容を暗号化するための暗号鍵として使われているもの（ZIP ファイルのパスワード、Word や Excel、PowerPoint の保護パスワード、Wi-Fi 機器の暗号化キー、暗号キー、パスワード、セキュリティキー、ネットワークキー）

1. は「PIN コード」が代表です。2. は「ログインパスワード」が代表ですが、ここでは単に「パスワード」とします。3. は「暗号キー」が代表です。

このうち、「PIN コード」と「パスワード」はよく混同して使われますが明確な違いがあります。

「パスワード」は、その内容がそのまま、または暗号化されて（URL の先頭が **https** のウェブページの場合など）ネットワークを通じてサーバーに届き、サーバーに登録保存されている「パスワード」と比較され合致していれば正当な利用者と判断されます。

「PIN コード」は、ネットワークに流されることがありません。パソコンやスマートフォンの場合は、入力したパソコンやスマートフォン内で、その中に保存されている PIN 情報との照合を行ってデスクトップ画面やホーム画面を開いています。ATM でキャッシュカードやクレジットカードを使う場合は、カードに内蔵された IC チップや磁気帯の中にある PIN 情報と入力した番号との照合を、ATM 端末を通じて行って、合致すれば端末・IC カード内のデジタルな認証情報が取り出され、その情報だけがネットワークを通

じてサーバーに伝達され、サーバー上で再度認証が行われます。

Windows10 ではパソコンへのサインインに **Microsoft** アカウントを使用することで **Microsoft** がクラウドで提供する **OneDrive** のようなサービスを利用しやすくしていますが、一方では **Microsoft** アカウントとパスワードでサインインすることはセキュリティの上で推薦できないので **Microsoft** アカウントとヒモつけられた **PIN** コードを使用することを勧めています。

上記の説明のように **PIN** コードはこの **PIN** コードを使用するパソコンに限られており、たとえ **PIN** コードを入力しているところを盗み見られても、他人が他のパソコンからその **PIN** コードを使用して **Microsoft** のサービスへアクセスすることができないからです。

もともと、**OneDrive** のような **Microsoft** が提供するクラウドサービスを利用することがなければ、ローカルサインインにすることで、たとえサインインの時にパスワードを他人に盗み見られても自分の **Microsoft** サービスを使用される心配はありません。