中小企業 と サイバーセキュリティ

第5回 お手軽サイバー防犯対策④
「パスワードはもう古い？新しいビジネスの鍵で守ろう！」

　前回はフィッシングによる被害を防ぐ「ログインさせようとするメールやSMSは全部偽物」という対策をご紹介しましたが、今回はフィッシングなどで狙われている「パスワード」について考えてみましょう。
　よく「長くて複雑なものを使い、複数サイトで使い回さない」ことが推奨されますが、フィッシングで盗まれてしまえば、どんなに複雑でも無力です。
　前回の「全部偽物」対策で防げることも多いのですが、残念ながら100%防ぐことは保証できません。

　そもそもパスワードは1960年代に生まれた古い技術です。当時は高価なコンピュータを複数人で使うため、「誰がどのデータにアクセスできるか」を管理する目的でした。しかし、今やインターネットは社会経済活動に欠かせない公共空間となり、攻撃者は世界中から巧妙にみなさんの大切な情報を狙ってきます。そのため、パスワードだけに頼るセキュリティは時代にそぐわなくなっています。
　そこでお薦めなのが「パスワードに頼りすぎない」仕組みです。

　まず取り入れやすいのが多要素認証(MFA)です。
　さらに進んだ方法が「パスワードレス認証」です。
　パスワードを使わず、生体認証や端末固有の鍵でログインするもので、「パスキー」が代表例です。
　入力の手間が減り、フィッシングで盗まれる心配もほとんどありません。
　お手軽サイバー防犯対策として、まず今使っているシステムで多要素認証、パスワードレス認証が使えるのなら有効化し、新しいシステム導入時にはパスワードレス対応かどうかを確認しましょう。
　パスワードは半世紀以上前の技術。 DXを推進し新しいビジネスを進めるためには、“新しい鍵”を活用することが必要です。

神奈川県警察サイバーセキュリティ対策本部

※ この記事は川崎市産業振興財団機関紙「産業情報かわさき（2025年11月号）」に掲載されたコラムを再編集したものです。