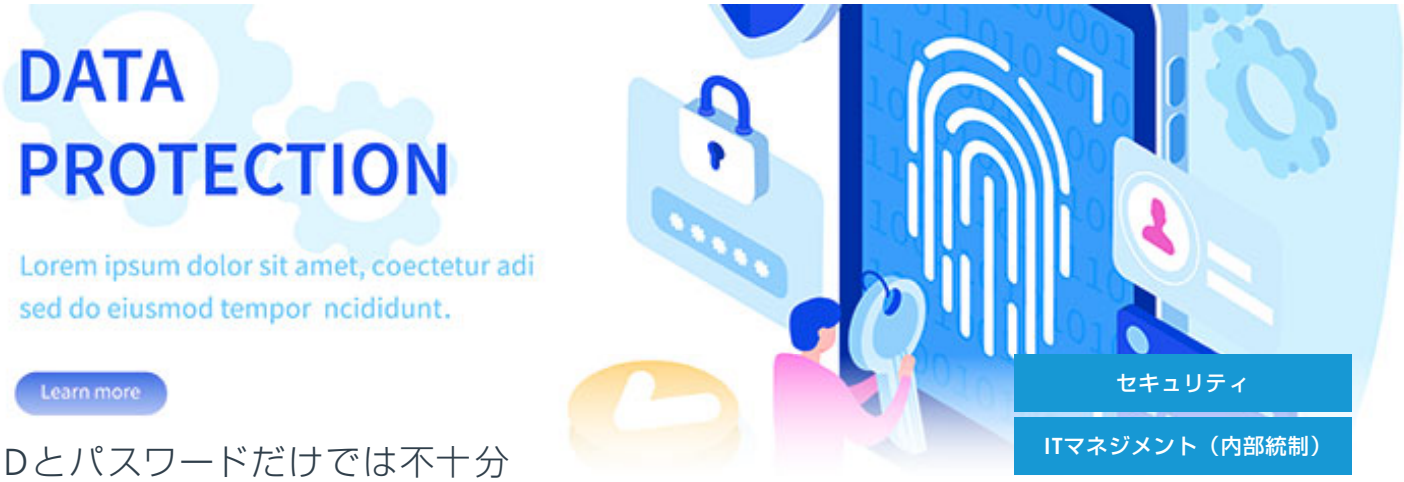

セキュリティ

ITマネジメント（内部統制）

IDとパスワードだけでは不十分

認証のスタンダードは「多要素認証」へ

社内システムやグループウェアへのログイン、PCへのリモートアクセスなど、ビジネスシーンのさまざまな局面において個人認証が使われるようになりました。一方で、情報漏えい事件が頻発し、個人情報が大量に流出している昨今、IDとパスワードのみに頼った認証は、セキュリティの強度という意味では不十分といえます。こうした課題に対応するため、近年普及が進んでいるのが「多要素認証」です。仕組みと効果について解説します。

危険な“IDとパスワードの使い回し”

インターネットを利用している人の数は、世界中で約40億人といわれています。インターネットのサービスを利用する際の認証は、40億人の中の特定の個人であることを証明することが求められます。

現在、個人を証明する手法の中で、最も一般的に使われているものが、IDとパスワードの組み合わせです。また、アカウントのIDは多くの場合メールアドレスが使用されます。例えばECサイトでは、IDとパスワードでログインすることで、過去の購入履歴を確認でき、都度クレジットカード情報や住所などを入力することなく買い物ができます。これは便利な反面、IDとパスワードが外部に漏れてしまうと、第三者が本人になりすまして買い物をされるリスクがあります。もし不正にログインした第三者が、IDとパスワード、連絡先まで変更してしまうと、本人であっても対応が困難になります。

そして近年では、こうしたアカウントの乗っ取りが増えています。多くの人が同じID（メールアドレス）とパスワードの組み合わせを使い回しているからです。そのため、IDとパスワードの組み合わせを1つ入手すれば、高い確率で複数のサービスにログインできるようになります。現在はインターネットユーザーの多くがグループウェアやECサイトを使っていますので、それらすべてが悪用されれば被害は甚大なものになるでしょう。

最近のサイバー攻撃では、アカウントを乗っ取っても行うのは情報収集のみにとどめるケースもあります。メールを盗み見したり、その人になりすましたSNSアカウントを作成したりすることで、フィッシング詐欺などの次なる攻撃を準備するためです。例えば、Facebookで知らない人から友達申請があった場合、承認する人はあまりいないでしょうが、これが知り合いであれば信じてしまうケースも多いでしょう。このように、サイバー攻撃者は収集した情報をもとに、さまざまな攻撃を繰り出すわけです。

異なる種類の認証を組み合わせる「二要素認証」

IDとパスワードのみの認証では、それらを入手すれば誰でも本人になりすますことができるため、今では多くのサービスがセキュリティ対策を追加しています。例えば、メールやSMS（ショートメッセージサービス）のアドレスなどの連絡先を登録するとともに、PCやスマートフォンのエリア情報を活用し、ログインすることの多い場所を記録するようにします。これにより、海外など普段と大きく異なる場所からログインがあった場合、登録された連絡先へ正規のログインかどうかを確認する通知を送ります。ユーザーに心当たりがない場合には、すぐにパスワードを変更するといった対応を行うことで、乗っ取りの被害を防ぐことができます。

ちなみに、IDとパスワードといった「知っていること」をログインに利用することを「知識認証」といいます。IDとパスワードを知っている本人のみがログインできる仕組みですが、逆にその情報が流出してしまえば誰でもログインできてしまいます。そこで、最近ではスマートフォンなど「持っているモノ」をログインに活用する「所有物認証」が使われ始めています。これなら「モノ」自体が盗まれない限り、第三者にログインされる危険はありません。また前述のID×パスワード+スマートフォンのように、異なる種類の認証を組み合わせたものを「多要素認証」といいます。

多要素認証はオンラインバンキングでよく使われています。サービスそのものへのログインはIDとパスワードで行いますが、新たな銀行口座へ振り込みを行う際には、あらかじめ配布されている乱数表を使用したり、スマートフォンなどに4桁から6桁の数字のSMSを送り、その数字を追加入力したりします。乱数表は、例えば9マス×9マスの表にランダムな数字が書かれていて、「C列の5行目の数字から右に4桁」などといった形で入力が求められます。後者は、アクセスのたびに新たに生成され、その一回しか使用されない「ワンタイムパスワード」と呼ばれるものです。

小型化、低価格化が進む生体認証

とはいえ、知識認証や所有物認証だけでは、なりすましの可能性を完全になくすことができません。そこで、これに生体認証を組み合わせるケースも増えています。生体認証とは、本人の身体的な特徴を鍵の代わりに使用する認証方式で、指紋認証や顔認証、静脈認証、虹彩認証などがあります。本人の身体の一部を使用するので、なりすましが非常に困難です。

以前はこうした生体認証用のデバイスは高価で、銀行のATMなどの一部に採用されているだけでした。しかし最近では小型化、低価格化が進み、指紋認証や顔認証などの機能がスマートフォンにも搭載されるようになりました。これにより、スマートフォンそのものを生体認証デバイスとして活用できるようになり、従来のIDとパスワードの認証に、スマートフォンによる生体認証を加えることで多要素認証が可能になったのです。

現在では、多くのセキュリティベンダからさまざまな多要素認証ソリューションが提供されています。例えば、USBで接続する指紋認証機器、PCやスマートフォンのカメラを活用した顔認証や虹彩認証などです。企業でのクラウド利用も増えている昨今、厳正な認証を実現するための多要素認証はますます重要度を高めていくことでしょう。

関連サービス

ID Federation	Office 365・G Suite・Boxなどの1,700以上のSaaSアプリをはじめ、お客さまのオンプレミスアプリやActive Directoryとも連携し、シングルサインオン・アクセスセキュリティ強化を実現する認証サービスです。
テレワーク・スタートパック	設定不要ですぐにセキュアなテレワークを始められる「テレワーク・スタートパック」。テレワークに必要なノートパソコン、モバイル通信、およびセキュリティサービスをパッケージ化。事前の設定も完了した状態でお届けします。
Bizモバイルコネクト	出張先や移動中等のモバイル環境からの接続や、在宅勤務等、様々なリモート環境から、各種クラウドサービスや社内のオンプレ環境（社内のメールやスケジュール）のシステムをセキュアに利用可能な環境を提供します。