たかがパスワード、されどパスワード

【物語編】

■大学食堂

薫がパソコン画面を見ているところに茉奈がやってくる

茉奈「薫、課題？」

薫「あ、茉奈！ううん、課題はもう全部終わりました～。」

薫が知らないことを察して
茉奈「あ！　・・・授業システムにログインした方がいいよ。」

薫「え、うそぉ。また課題出てるの？」
慌ててパソコンを操作し、タイピングする
薫「あ、ほんとだ。情報科学かぁ。」

茉奈「・・・ん、ちょっと待って。今パスワード短くなかった？」

薫「え？　パスワード・・・？」
PC を確認して
薫「・・・８文字あるけど、これ短いの？」

茉奈「８文字！？　私は 16 文字だよ」

薫「え、面倒くさ！　長すぎでしょ。」

茉奈「え、長いの？」

薫「英数字の他にちゃんと記号も入れてるから、８文字で十分じゃないかなぁ。」

茉奈「あ、私は 16 文字だけど英数字だけだ。これどっちがいいんだろう？」

考え込む二人

【解説編】

■大学食堂

天の声「パスワードに注目するなんて感心ですね。ただ、自分のパスワードの文字数も、他人には言わないようにしましょう。そのような情報も解読のヒントになり得ますよ。
では、文字数の話をする前に、原則を確認しておきましょう。
ログイン ID とパスワードは、ログイン操作をしている人が本人であることをシステム側で確認するためのものです。これを認証と言います。
まず、簡単に推測できる文字列、例えば password や 123456、qwerty（クワーティ）などはパスワードに使ってはいけません。
第三者が不正アクセスを試みる時、パスワード文字列を推測して手で入力する場合もありますし、可能性のありそうな文字列を自動的に次々と試すようなプログラムが使われる場合もあります。
つまり推測されやすい文字列はパスワードとしてはとても弱いのです。ここまでは大丈夫ですね？」

薫と茉奈、うなずく

天の声「それでは、パスワードの長さについてですが、パスワードを破る手段として、「総当たり攻撃」があります。これは、文字のすべての組み合わせを片っ端から試してみる方法です。」

薫「時間かかりそう。」

天の声「こちらも人間が手で入力するのではなく、プログラムによって次々に試していく方法が使われます。その時、パスワードが十分に長ければ、膨大な組み合わせを試すのに時間がかかりすぎるため、コンピューターでもなかなか破ることができません。」

薫「十分に長い・・・ってどのくらいですか？ 」

天の声「はい。それでは、パスワードの長さによっていくつの組み合わせを作れるのか見ていきましょう。通常、アルファベットの小文字 26 個と大文字 26 個、そして数字 10 個を合わせると、合計 62 種類の文字を使えます。ここで使える記号が 26 種類あるとしたら、文字の種類は 88 種類になります。このときパスワードが 5 文字だとすると、何種類のパスワードがつくれますか？」

茉奈「高校の数学で勉強しました。えーっと、１文字目が 88 種類、２文字目も 88 種類・・・。
だから５文字だと 88 の５乗種類作れることになります。」

天の声「そうですね。８８の５乗は計算すると・・・約５３億通りになります。
次に、パスワードを１文字長くして、その代わり文字の種類を減らした場合を考えてみましょう。仮に記号を使わず、アルファベットと数字だけでパスワードを構成した場合には、文字の種類は６２に減ります。パスワードを６文字にすると、６２の６乗なのでこのとおり。約５６８億通りです。
記号を含めても 5 文字のとき 53 億通りでしたから、記号を含めなくても１文字長いほうが、パスワード文字列の種類は多くなります。
薫さんの場合は、記号を含めた８文字。茉奈さんは英数字だけの 16 文字でしたよね。
たとえば記号が 26 種類使えたとして、計算結果はこうなります。
重要なのは桁数です。16 文字のパスワードは、８文字のパスワードの１０の１３乗倍、つまり 10 兆倍くらいの種類がありうる計算になります。
8 文字でも 3600 兆種類なので十分多いように見えますが、最近のハイスペックなパソコンを使うと 1 時間ほどで破られてしまいます。それが 16 文字の場合は、1 兆年かかるということです。」

薫「そんなに違うの？　でも 16 文字のパスワードなんて覚えられないよ。」

茉奈「じゃあブラウザに覚えさせればいいんじゃない？　翔平がやっているらしいよ。」

薫「それどういうこと？」

天の声「Google Chrome や Microsoft Edge、Safari などの Web ブラウザには、パスワードを管理する機能があります。Web サイトにログインする際に一度 ID とパスワードを入力すると、任意でブラウザに記憶させることができ、次回その Web サイトにアクセスした時、自動的にＩＤとパスワードを入力してくれます。」

薫「それって危なくはないんですか。」

天の声「たしかにそのパソコンが盗まれたら、いろいろな Web サイトのパスワードも盗られてしまうリスクがあります。まずは、パソコンを起動する時のパスワードを必ず設定しておきましょう。また、ブラウザに記憶させたパスワードを盗られないように、ブラウザは特にしっかり管理してください。」

茉奈「私は、パスワードは小さなノートに書いて、自宅で管理しています。サイトごとに違うパスワードを設定してるから、とても覚えきれなくて。」

天の声「自宅のノートに書いて保管しておくのも良い方法ですね。万一ノートを紛失した場合に備えて、ID とパスワード文字列のすべてを書くのではなく、自分だけがわかるような書き方をしておくことをお勧めします。
それと、茉奈さんがしているように、サイトごとにパスワードを変えることも大事です。もしどこかのサイトでパスワードが流出したら、流出したパスワードで別のサイトにもログインされて、不正に利用されてしまう可能性があります。」

薫「私もパスワードの使い回しはしないように気をつけています。」

天の声「最近では、ID とパスワードによる認証に加えて、スマートフォンなどに送るショートメッセージを使って本人確認を行う方法も増えています。」

茉奈「それ、「多要素認証」と呼ばれるものですね。「情報科学」の授業で習いました。」

天の声「そうです。よく覚えていますね。」

茉奈「パスワードを管理してくれるアプリもありますが、あれはどうですか。」

天の声「ＩＤとパスワードをネット上のクラウドに保存するアプリと、パソコンやスマホ内に保存するアプリがありますね。たしかに便利ですが、そのアプリ自体に脆弱性がある可能性や、クラウド上のデータが情報漏洩する可能性もあるので注意してください。」

茉奈「そういえば、翔平が、「ウェブサイトのパスワード管理機能を使っているんだけど、そのおかげで偽サイトに騙されなかった」と言っていました。
いつも使ってる通販サイトを名乗った偽サイトから「クレジットカードの有効期限が切れてる」ってメールが来て、偽サイトだって気づかずにログインしようとしたら、パスワードが自動入力されなかったようです。」

天の声「ブラウザのパスワードマネージャは、サイトのＵＲＬが登録されたものと一致したときだけパスワードを自動入力してくれます。つまり、人間が一見しただけでは「偽サイト」だとわからなくても、フィッシングである可能性に気づかせてくれるというメリットもあるというわけです。」

薫「ああ、そういういいこともあるんですね。」

天の声「フィッシングのメールでは、「有効期限切れ」「新サービスの開始」「セキュリティの強化」などを通知し、偽サイトへと誘う手口がよくあります。偽サイトは本物のサイトとそっくりなので、

そこにパスワードやクレジットカードなどの情報を入力すると、悪用されてしまうのです。」

茉奈「サイトの中身まで作り込まれているなんて・・・騙されそうですね。」

天の声「はい、フィッシングの手口は巧妙なので、十分に気をつけてください。
情報処理推進機構という国の機関が、毎年「情報セキュリティ 10 大脅威」を発表しており、フィッシングは、２０１９年から変わらず 10 大脅威に選ばれています。」
フィッシングなどによりパスワードが盗まれ、ログインされてしまった場合、不正アクセスの踏み台とされてしまうケースも少なくありません。そうなった場合、個人情報の詐取に留まらず、これら 10 項目のほとんどのサイバー攻撃の脅威に発展してしまう可能性もあるため、非常に危険です。
内閣サイバーセキュリティセンターのサイトで「インターネット安全・安心ハンドブック」が公開されていますから、サイバー攻撃の手口もぜひ見ておいてくださいね。」

薫と茉奈「わかりました！」