

増え続ける ID や パスワード！ 管理はいったい どうしたらいいの？

PASSWORD

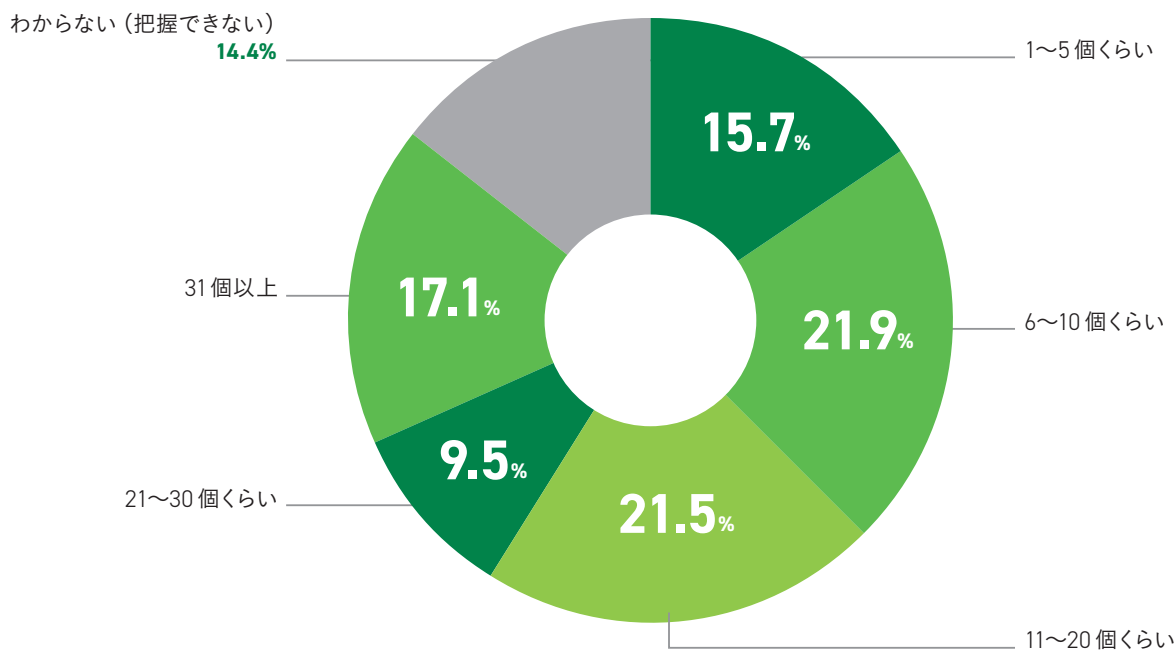
マンション・ラボ

パソコンやスマートフォンなどで利用するサービスの大半は、ID とパスワードで利用者を識別しています。利用するサービスが増えるに従い、パスワードの管理は膨大になってきます。パスワードは「使いまわしてはいけない」「定期的に変更する」などといわれることもあります。実際にはどのように管理するのがよいのでしょうか。ほかの人がどのようにしているのか、などのユーザーアンケートの結果を踏まえて、パスワード管理の課題と対策をご紹介します。

パスワードに対する意識をチェック！

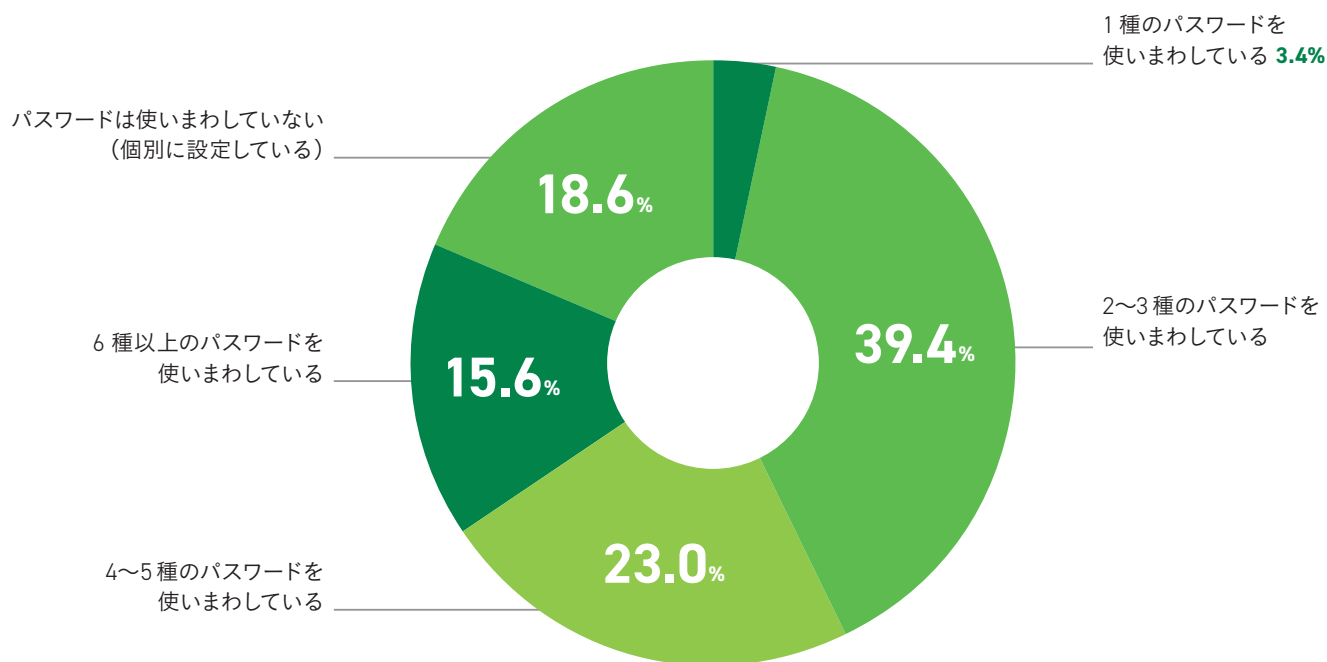
今回、インターネット利用時のパスワードに関する調査をマンション・ラボのアンケート会員の方にうかがいました。まずはユーザーのパスワードに関する現状をチェックして、自分の環境と照らし合わせてみましょう。

Q あなたは今インターネット上で、ID とパスワード設定が必要なサービスをどのくらい利用していますか？



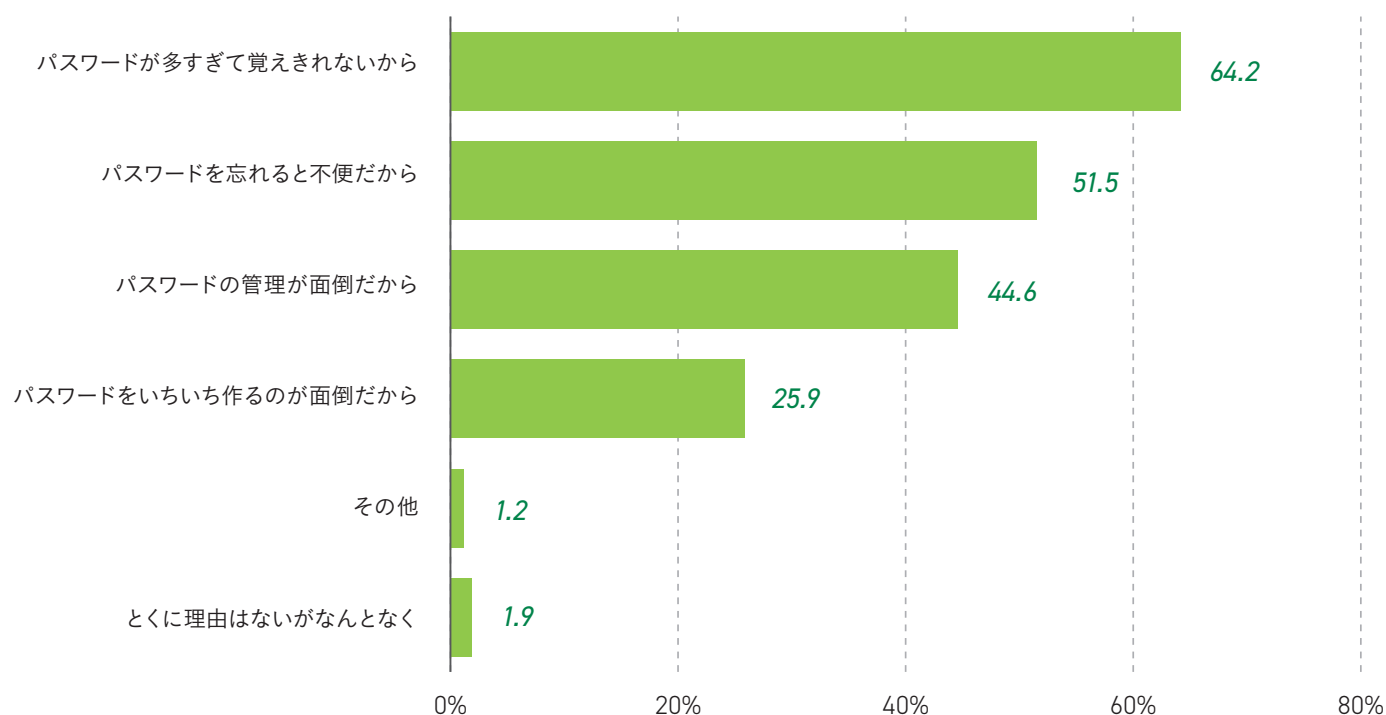
この結果を見ると「6～10 個くらい」(21.9%)と「11～20 個くらい」(21.5%)がほぼ同数で上位 40% あまりを占めています。その一方で「31 個以上」(17.1%)という方もかなりいます。さらに「わからない (把握できない)」(14.4%)という方も、多くは「たくさんありすぎてわからない」であると予想されます。そう考えると約 30% 以上の方が、30 を超えるサービスを利用しています。さすがに 30 を超えると手軽に管理できるとはいえない数ですから、サービスが増えすぎて管理が難しくなっているという現状がわかります。

Q あなたは今インターネット上の各種サービスでパスワードを使いまわしていますか？



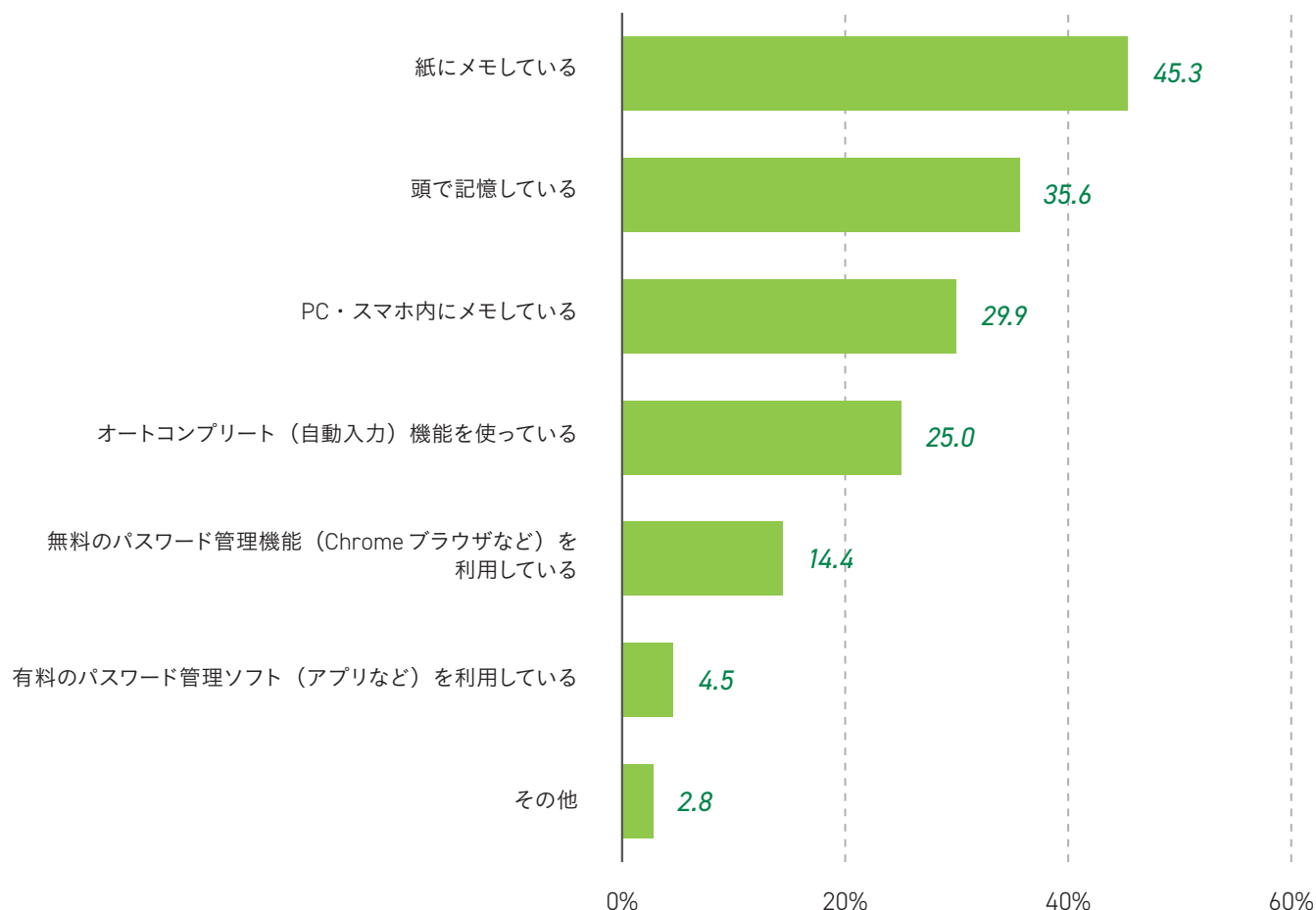
パスワードの使い回しについてのアンケートでは、「2～3種」と答えた方がもっとも多く（39.4%）、続いて「4～5種」（23%）と続きます。この2つの回答で約60%超を占めています。人が手軽に管理できるパスワードの種類は、4～5種までということがわかります。その一方で「6種以上」（15.6%）、「使いまわしていない」（18.6%）というセキュリティ意識の高い方が約36%と相当数いることも注目できます。

Q 危険と思いつつ、パスワードを使いまわしている理由を教えてください。（複数選択可）



パスワードを使いまわしている理由でもっとも多かったのは「パスワードが多すぎて覚えきれないから」で、つぎに「パスワードを忘れると不便だから」、「パスワードの管理が面倒だから」と続きます。いずれもパスワードが増えてくことによる「管理の大変さ」が理由になっているものです。

Q 各種サービスのパスワードはそれぞれどのように管理していますか？（複数選択可）



実際にパスワードをどのように管理しているのかを尋ねた質問では、いちばん多かった回答が「紙にメモしている」（45.3%）でした。アナログな手段ですが確実な管理方法ではあります。つぎが「頭で記憶している」（35.6%）です。記録からパスワードが漏れることがないので安全ではありますが、忘れてしまうリスクが難点でしょう。

以下には「PC・スマホ内にメモしている」（29.9%）、「オートコンプリート（自動入力）機能を使っている」があります。こちらは PC やスマホにデータとして残す方法ですが、それらは利便性は高いものの、機器が壊れたときにどうするか、という問題も考えておく必要があります。

パスワードが漏れるとどんな危険がある？

そもそもパスワードが漏れるとどのような危険があるのでしょうか。それは、漏れたパスワードでどのサービスを使っていたかによって変わってきます。代表的な危険は、以下のようなものです。

- 名前や住所などの個人情報が流出してしまう
- ネットバンキングやクレジットカードなどでの金銭的損害
- SNS や Web サイトなどの乗っ取りや悪用



個人情報の流出

SNS や会員制のサービスなどで、ID とパスワードが漏れて第三者にアクセスされてしまうと、入力していた住所や名前などの個人情報を知られてしまいます。そのような個人を特定できるような情報が、ネット上にばらまかれてしまう危険性があります。

金銭的損害

銀行やクレジットカードのサイトなどで使用する ID やパスワードが漏れて悪用されると、損害は大きくなります。銀行の残高をどこかに振り込みされてしまったり、クレジットカードで買物をされてしまったりという危険があります。もっとも注意すべきパスワードでしょう。

乗っ取りや悪用

SNS や Web サイトのログインパスワードなどが漏れると、本人になりすまして悪用されることがあります。勝手に Web サイトを改変したり、迷惑メールや詐欺メールなどの配信元にされてしまったりということがあります。場合によっては犯罪の踏み台にされてしまう可能性もあります。

ただ、現実には財布などをなくしたときには、自分で気が付いて、カードを止めるなどの対応ができます。しかしネットのパスワード漏洩は、漏洩自体を気付かないことが多いため、被害が起きるまで気が付かないことがあります。そのためパスワード管理については、十分に気をつける必要があります。

利便性と安全性のバランスが取れたパスワード管理方法は？

パスワードの使いまわしを減らして、うまく管理するにはどうしたらいいでしょうか。パスワードの管理方法は、上のアンケートで示したようにいくつかの方法があり、大きく分けると 3 つあります。

- 紙にメモして管理する
- ファイルにして PC やスマホで管理
- パスワード管理ツールを使用



それぞれにメリットもデメリットもあります。また安全性を高めすぎると利便性に欠け、利便性を重視しすぎると安全性が低下することもあります。このあたりのバランスをうまくとるために、複数の方法を使い分けるのがよいでしょう。

紙にメモして管理する

アナログな方法ですが、ネット回線から漏洩することがないので、ネット上での安全性は高いといえます。ただしすべてのサイトの ID やパスワードを記載するのがたいへんで、パスワード変更時に書き換えたりするのも面倒です。また記載したメモ帳などを紛失してしまったり、メモを他人に見られて漏洩するというリスクはあります。

メリット インターネットから漏洩することがない

デメリット 記載や管理が面倒、紛失の恐れ、人に見られる心配

このデメリットを減少させる方法を考えてみましょう。

● 記載や管理が面倒

すべてのサービスに活用するのではなく、重要なサービスなどのネットと切り離して保存したいパスワードに限るなどの工夫をするといでしょう。

●紛失の恐れ

まず紛失しやすい紙切れなどに書くのではなく、メモ帳やノートに記録します。記録した紙を PC や机に貼っておくというのは絶対にだめです。会社の引き出しの中などに入れて帰宅するのも危険です。保管場所はひとめにつきやすく、誰でも簡単にアクセスできるような場所を避けるなどの注意をはらいましょう。

さらに紛失してもリカバリできるようにコピーをとっておくことは必要です。おすすめはノートやメモ帳に記載しているページを、スマホなどで撮影して画像でとっておくことです。もし書き換えなどを行ったときも、すぐに撮影できるので、コピーも最新データを常にキープできます。アナログとデジタルの兼用です。ただし撮影したスマホなどを見られると危険なので、スマホのパスワードロックもしっかりかけておきます。

●人に見られるリスク

パスワードはそのまま記載しないで、自分だけがわかるように暗号化しておきます。たとえばパスワードを「母の名前と結婚記念日」という構成にしておき、メモ帳には「母・結婚」とだけ書いておけばほかの人が見ても推測しにくいでしょう。大文字と小文字の組み合わせがある場合には、たとえば「母大小小小大・結婚」というような書き方をすれば、「母の名前の最初と最後を大文字」にするといったメモになります。

また、自分で設定したパスワードでなく、ランダムな英数字の組み合わせの場合もあります。このときはパスワードそのものにダミーの英数字を足して記載するという方法もあります。これは最初と最後に「0」を付け足して記録しています。自分でパターンを決めておけば、入力時に付け足した「0」を取り除いて入力すればいいので、自分にはわかります。

どちらのパターンでも「◎◎銀行、ID：Tsunagu、Pass:12345678」など、誰が見てもわかるような記録方法だけは絶対にしないようにしましょう。ID とパスワードは同じページに書かないで別にする、パスワードをパスワードとわからないように書くなどの工夫はしましょう。

例

本当のパスワード
AxB_2gje5xZ

↓

記載パスワード
0AxB_2gje5xZ0

ファイルにして PC やスマホに保存

メモ帳や Word、Excel などのツールを使って、入力し、管理する方法です。デジタルデータなので、検索や並べ替えなどもできて、データの更新も容易にできます。使いやすさの点ではとても優れています。一方ファイルなのでデータが流出する危険性がありますし、パソコンを使われた場合には、全文検索でパスワードファイルを容易に見つけられてしまう危険性もあります。

メリット 入力や管理、更新がしやすく使いやすい

デメリット データ流出の可能性、全文検索で探される

デメリットの危険性を軽減する方法を考えてみましょう。

●データ流出の可能性

Word や Excel で管理する場合は、もしファイルが流出してしまったとしても、すぐに開かないように暗号化しておきます。メモ帳などで記録するときは、面倒でも ZIP などに暗号付きで圧縮します。暗号付きの ZIP は Windows の標準機能ではできないので、「Lhaplus」(<http://hoehoe.com>) などのフリーソフトを活用しましょう。

またファイルを保存する際には、ファイル名に気をつけ、決して「パスワード」「Password」などの単語を使わないようにします。もしパソコンごと盗まれた場合などは、まずこうした単語でファイル検索されてしまうからです。保存先もデスクトップやマイドキュメントなどのわかりやすい場所も避けましょう。保存したファイルは PC 内だけでなく、必ず別の場所にバックアップを取っておきます。USB メモリや CD などのメディアや、OneDrive や Google ドライブなどのインターネット上の保存先を活用します。



Excel での暗号化は、「ファイル」→「情報」から行います

●全文検索で探されてしまう

パソコンごと盗まれたり、不在時にパソコンを使われたりしたときには、全文検索によってパスワードを知られてしまうことがあります。全文検索とは、パソコン内にある複数のデータから、特定の文字列を検索することです。これを行うと Excel などのファイルに記載してある文字からも検索できてしまうのです。たとえば「パスワード」「password」などの文字で検索すれば、その文字列が含まれているファイルが羅列されてしまうのです。

基本的には暗号化したファイルからは検索できないようになっていますが、検索でひっかからないような工夫しておくほうが安心です。紙に記録するときと同様に、自分だけがわかる暗号化や、ダミーの文字を付加するなどの対策も同時に行くとさらに安全性が高まるでしょう。

パスワード管理ツールを使用

複数のパスワードを管理することを目的として作られたツールで、パスワードをすべてひとまとめにしてクラウド上で管理します。ユーザーは管理ツールに接続するためのマスターパスワードさえ覚えておけば、Web サイトやサービスごとに設定した ID とパスワードを自動的に入力されます。パスワード設定時にも解読されにくい複雑なパスワードを自動生成するなど、利便性が高く、セキュリティ機能も高いのが特徴です。

デメリットは多くの場合は有料で、ランニングコストがかかることです。製品によっては、使用できる OS に制限があるもの（たとえば iOS と Android のみなど）がありますので、選択するときに注意しましょう。またすべての Web サイトで自動的に入力できるとは限らず、手動で入力しなくてはならないケースもあります。

メリット 利便性が高く、セキュリティ機能も高い

デメリット 費用がかかる、製品が多く選択が難しい

パスワード管理ツールに関しては、デメリットは価格と製品選択程度です。安全にはお金を払うということであれば、安全性と利便性を兼ね備えることができます。

●代表的なパスワード管理ツール



1Password

<https://1password.com/jp/>

古くからある管理ツールでユーザーも多く、ほとんどの OS に対応しています。機能も高度でセキュリティ性能も高いことで人気です。



パスワードマネージャー

https://www.trendmicro.com/ja_jp/

ウイルス対策ソフトで有名なトレンドマイクロによる管理ソフト。セキュリティ対策会社だけにダークウェブ（違法サイト）への個人情報流出もモニタリングし、流出をチェックします。

＼ ショップからのご案内 ／

パスワードマネージャー

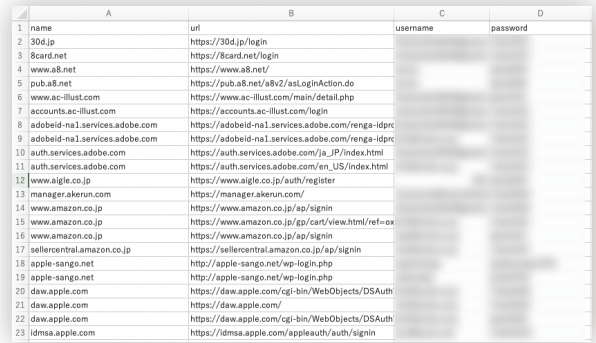
<https://www.tnshop.jp/category/S03/NM1B1PM1151224.html>

●OSで標準のパスワード管理ツール

ChromeやMicrosoft Edge、Safariなどのブラウザを利用していると、「パスワードを保存しますか」というメッセージがあらわれて、パスワードを保存することができます。この機能を使って、パスワードの管理をしている人も少なくありません。

この機能自体は便利な機能ですが、ブラウザを使ったままで席を離れて、パソコンを使われてしまうとパスワードが自動で入力されてしまいます。ブラウザを使い終わったときには必ずログアウトしなくてはなりません。

たとえばログインしたままにしておくと、ChromeのGoogleパスワードマネージャーでは、保存しているパスワード一覧を簡単に出力できます。保存されているすべてのパスワードがCSV形式で書き出されてしまいます。この機能はあまり重要ではない（被害が起きにくい）サイトに使うなどの工夫をしたほうがよいでしょう。



	A	B	C	D
	name	url	username	password
1	30d.jp	https://30d.jp/login		
2	30d.net	https://30d.net/login		
3	www.a8.net	https://www.a8.net/		
4	pub.a8.net	https://pub.a8.net/a8v2/asLoginAction.do		
5	www.ac-illust.com	https://www.ac-illust.com/main/detail.php		
6	accounts.ac-illust.com	https://accounts.ac-illust.com/login		
7	adobeid-na1.services.adobe.com	https://adobeid-na1.services.adobe.com/renga-idpnc		
8	adobeid-na1.services.adobe.com	https://adobeid-na1.services.adobe.com/renga-idpnc		
9	auth.services.adobe.com	https://auth.services.adobe.com/ja_JP/index.html		
10	auth.services.adobe.com	https://auth.services.adobe.com/en_US/index.html		
11	www.aigle.co.jp	https://www.aigle.co.jp/auth/register		
12	manager.akerun.com	https://manager.akerun.com/		
13	www.amazon.co.jp	https://www.amazon.co.jp/ap/signin		
14	www.amazon.co.jp	https://www.amazon.co.jp/gp/cart/view.html/ref=ox		
15	www.amazon.co.jp	https://www.amazon.co.jp/ap/signin		
16	sellercentral.amazon.co.jp	https://sellercentral.amazon.co.jp/ap/signin		
17	apple-sango.net	http://apple-sango.net/wp-login.php		
18	daw.apple.com	https://daw.apple.com/cgi-bin/WebObjects/DSAuth		
19	daw.apple.com	https://daw.apple.com/		
20	daw.apple.com	https://daw.apple.com/cgi-bin/WebObjects/DSAuth		
21	idmsa.apple.com	https://idmsa.apple.com/appleauth/auth/signin		

Googleのパスワードマネージャーで出力したIDとパスワード一覧

COLUMN

パスワードを上手につくるコツ

破られにくいパスワードは、基本的には「いろいろな種類の文字で、なるべく多い文字数」にすることです。

海外のデータ研究サイトによる、パスワード解析ソフトを使って、パスワードが破られる所要時間では、「小文字だけの8文字のパスワードは5秒」だそうです。同じ8文字でも「大文字と小文字、数字と記号を含めれば8時間」かかり、文字数を13文字にすれば「小文字だけでも1年」かかるそうです。もし16文字にするなら「大文字と小文字、数字で20億年」と膨大な時間になります。

上述したように結婚記念日などをパスワードに混ぜるなら、「12月11日」の「1211」よりも「2010年12月11日」の「20101211」を使うほうが効果的です。これに大文字と小文字の混在した8文字を追加すれば、かなり堅牢なパスワードになります。

英文字も英単語として意味のある言葉は避けるほうが無難です。辞書にのっている言葉を当てはめる解析ツールもあり、日本語をそのまま当てはめたほうが、解析されにくいそうです。「potato」よりも「jagaimo」のほうが解析されにくく、大文字と小文字を混ぜて「JaGaim0」とするなどの工夫をしましょう。

●まとめ

IDやパスワードが必要なサイトやサービスが増えてきている現状から、パスワードを使いまわしている人が多いことがわかりました。しかし同じパスワードを使いまわすのは、危険性があるので避けたいところです。

パスワード管理の方法は以下の3つがありました。

- 紙にメモして管理する
- ファイルにしてPCやスマホで管理
- パスワード管理ツールを使用

それぞれにメリット・デメリットがあり、どれが絶対いいとはいえません。たとえば、重要度の低いものはデジタルデータで管理し、金融機関などの重要なものは、ネットからは漏洩しない紙と記憶を使うなどの使い分けをするのがいいでしょう。

これからますますネットの環境が発展していくなか、パスワード管理はいつそう大切で重要になっていきます。この記事を参考に、ぜひパスワードについてもう一度見直してみてください。