トレンド今知っておきたいITセキュリティスキルワンランクアップ講座（第7回）

ブラウザにパスワードを保存するのはアリなのか？

2019.01.29 Tue

Webサイトへのログインのためにパスワードを入力した時に、「パスワードを保存しますか？」などのメッセージが出ることを経験したことがあると思います。この機能は「オートコンプリート」などとも呼ばれ、一度ブラウザにパスワードを記憶させれば次回からログインする時にキーボードから打ち込まなくても自動的にブラウザが入力してくれるもので、IE/Edge、Chrome、Firefoxなどの各ブラウザでは既定で有効になっています。

Edgeでのパスワード保存の例

この機能は非常に便利ですが、その反面、セキュリティ上の問題があるとする意見もあります。例えば、内閣サイバーセキュリティセンター（NISC）が公開している、「インターネットの安全・安心ハンドブック Ver 4.00」では、「ブラウザの自動入力にパスワードを覚えさせない」(p.31)とされています。

今回は、この「ブラウザにパスワードを保存する」機能について、実際にどのようなリスクがあるのか、本当に使ってはいけないのかについて考えてみたいと思います。なお、環境は基本的にWindowsを想定しています。

ブラウザにパスワードを保存するリスクは？

ブラウザにパスワードを保存することにどのようなリスクがあるのでしょうか？1つ目のリスクは、ブラウザに保存したパスワードにより他人に勝手にサービスを利用されてしまうことです。

まず問題になるのは、ホテルのロビーや図書館などの公共の場所にあるPCでの利用です。このような場所のPCではそもそもログインが必要となるようなサービスを利用すべきではありませんが、やむを得ず利用する場合は、パスワードは絶対に保存せず、利用後は必ずサービスからログアウトするようにしてください。あとから来た人にサービスにログインされてしまう危険性があります。職場で1台のPCを複数人が共通アカウントで使用している場合も同じ問題があるでしょう。

職場で1人1台のPCを使用している場合はどうでしょうか？職場の環境にもよりますが、周囲の目がある中で、勝手に他人のPCを操作してサービスを利用することは、発覚のリスクを考えるとなかなか難しいのではないでしょうか？離席するときはPCを必ず画面ロック（Windowsでは「Windowキー＋L」）するようにすれば、他人に勝手にPCを操作されることを防げますし、スクリーンセーバーでロックが掛かる時間を短く設定しておくのも良いでしょう。

また、最近のサービスでは一度ログインをすれば明示的にログアウトしない限りはログイン状態を維持し、ブラウザのタブを閉じても再度サービスにアクセスすればログインした状態でアクセスできるものも多くなっています。この場合は、ブラウザにパスワードを保存していなくてもブラウザを操作できればサービスを利用されてしまうため、やはり短時間でもPCの前を離れるときは画面ロックをするしかないでしょう。

自宅で、自分や家族しかPCに触れられない場合は、他人に勝手にサービスを利用されるリスクは考えなくて良いでしょう（家族が信用できる限り）。ただし、ノートPCをカフェなどで使用する場合は、ちょっとした離席でもPCを持ち歩くなど盗難に気をつけましょう。

これらを考えると、共有のPCを使うのでない限り、ブラウザにパスワードを保存することにより、他人に勝手にサービスを利用されるリスクはそれほど増える訳ではないように思えます。

2つ目のリスクは、ブラウザに保存されたパスワードを平文で表示させて見られるリスクです。ブラウザの設定画面などから、保存してある平文のパスワードを表示させ、メモするだけなら、短時間で済むため、発覚するリスクは小さいかもしれません。

以前のChromeでは、
設定画面のパスワード管理から「表示」をクリックするだけで平文のパスワードが表示されることから、セキュリティ上の問題があるとして指摘されたこともありました（Google Chromeに保存したパスワードが丸見えに、開発者が問題指摘／IT Media）。

しかし、現在のChromeではOSの資格情報（パスワード又はPINコード）を入力しないと、平文のパスワードを表示できないように改善されています。また、Windows8以降のIE/Edgeでは、「コントロールパネル」の「資格情報マネージャー」で平文のパスワードを表示できますが、この場合もOSの資格情報の入力が必要です。Firefoxでは、既定ではパスワードの入力なしで平文のパスワードを表示できてしまうのですが、マスターパスワードを設定することにより、平文のパスワードを表示する場合にパスワードを要求できます。

よって、職場のPCなどで、離席した間にブラウザに保存されたパスワードを平文で表示させて見られるリスクは、OSの資格情報(Chrome/Edge/IE)またはマスターパスワード（Firefox）に強固なものを設定することで軽減できます。また、PCの前を短時間でも離れる時は、必ず画面ロックをしましょう。

3つ目のリスクは、ブラウザで保存したパスワードを複数のデバイスで同期させる設定にしている場合に、他人にアカウントにログインされパスワードが同期されてしまうことです。

IE/EdgeではMicrosoftアカウント、ChromeではGoogleアカウント、FirefoxではFirefoxアカウントでログインすることにより、ブラウザで保存したパスワードを複数のデバイスのブラウザで同期させることができます。もし、これらのアカウントの認証が突破された場合、パスワードが他人のデバイスに同期されてしまう可能性があります。

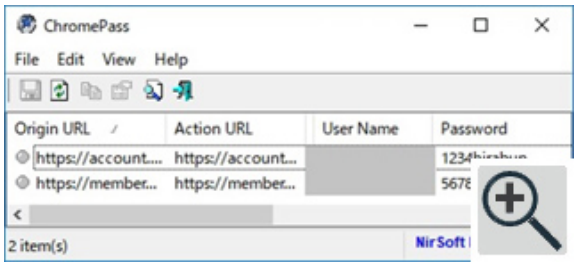
MicrosoftアカウントやGoogleアカウントでは、パスワード以外にもメールやオンラインストレージなど、非常に重要な情報にアクセスが可能です。よって、これらのアカウントは、強固なパスワードや2段階認証を設定し、絶対に破られないようにしておくべきです。

マルウェアに感染して保存してあるパスワードを丸ごと抜き出されるリスク

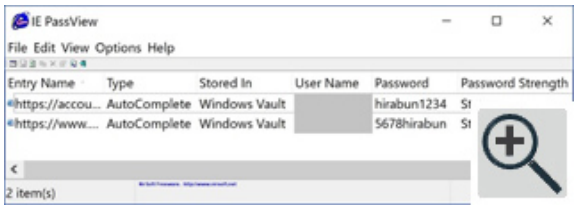
4つめのリスクは、マルウェアなどに感染した場合に、ブラウザに保存してあるパスワードを丸ごと抜き出され、外部に送信されてしまうことです。

ChromeやIE/Edgeに保存したパスワードを平文で表示させるにはOSの資格情報を入力する必要があることは前述しました。しかし、ネット上で公開されているツールを使用すると、資格情報の入力なしに、ブラウザに保存されているすべてのパスワードを平文で抜き出して表示させることができてしまいます。

Chromeに保存された平文パスワードを抜き出して表示



IE/Edgeに保存された平文パスワードを抜き出して表示



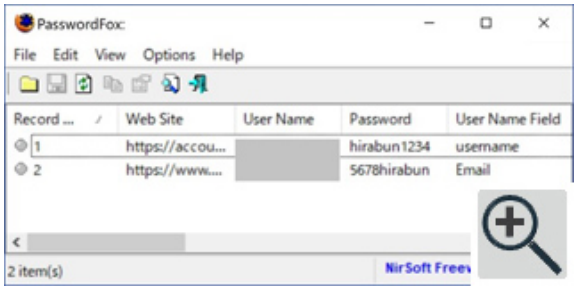
パスワード管理ソフトではインストール時にブラウザに保存されているパスワードをパスワード管理ソフトに自動的にインポートしてくれるものもありますが、これも同様の仕組みを利用してブラウザに保存されているパスワードを抜き出しそれをインポートしています。このようなことができるということは、マルウェアも同じことができるということで、ブラウザに保存されているすべてのサービスの平文パスワードが攻撃者の手に渡ってしまう可能性があります。

ChromeやIE/Edgeで保存したパスワードは、WindowsのDPAPI(Data Protection API)のCryptProtectData関数を用いて暗号化され、ローカルに保存されています。暗号化されたデータは暗号化時と同じ資格情報を持つユーザのみがCryptUnprotectData関数を用いることにより、復号できます。

同じPCの別のユーザがデータを復号することや、暗号化されたデータを外部に送信して外部のPC上でデータを復号することはできません。しかし、ユーザがマルウェアなどに感染した場合に、マルウェアによってCryptUnprotectData関数を用いたツールを実行されれば、暗号化時と同じ資格情報となるので、暗号化されたデータを復号されてしまい、平文のパスワードを外部に送信される可能性があります。

Firefoxでは暗号化の仕組みが異なるのですが、マスターパスワードが設定されていない場合は（既定ではマスターパスワードはなし）、ツールを実行することにより保存されているすべてのパスワードを平文で抜き出せます。

Firefoxに保存された平文パスワードを抜き出して表示



マスターパスワードを設定している場合でも、Firefoxでは暗号鍵の導出に、繰返しなしのSHA-1という弱い方式が使われているので（FirefoxとThunderbirdの「マスターパスワード」は1分で破ることが可能と指摘される／Gigazine）、暗号化されたファイルを外部に送信し、辞書攻撃・総当たり攻撃でパスワードを解析されてしまう可能性があります。

マルウェアは利用者に気づかれない様にバックグラウンドで動作しますので、画面ロックをしていても防げません。これらを

防ぐためにはOSやアプリケーションの更新、ウイルス対策ソフトの導入、メールの添付ファイルや本文に記載されたURLなどを不用意に開かないなど、マルウェアの感染を防ぐ対策が必要です。

ブラウザにパスワードを保存するのはアリなのか？

以上の様なリスクを考えた場合、「ブラウザにパスワードを保存する」機能は本当に使うべきではないのでしょうか？

まず、公共の場所にあるPCや職場で1台のPCを複数人が共通アカウントで使用している場合は、ブラウザにパスワードを保存する機能は、使うべきではありません。ブラウザに保存したパスワードにより、他人に勝手にサービスを利用されてしまいます。

職場で個人専用のPCを使用している場合や、共有PCでユーザ毎に別のアカウントでログインして使用している場合、離席している間に他人に勝手にサービスを利用されたり、ブラウザに保存されたパスワードを平文で表示させて見られたりするリスクは、必ず画面ロックをすることや、OSの資格情報やマスターパスワードに強固なパスワードを設定することで、低減できます。

リスクとして考えなければならないのは、マルウェアに感染してブラウザに保存されたすべてのパスワードを、平文で丸ごと抜き出されることでしょう。マルウェアに感染しないための対策も色々とあるのですが、感染を完全に防ぐのはなかなか難しいことです。

本連載では、パスワード管理ソフトの利用を推奨してきました。信頼できるパスワード管理ソフトであれば、端末がマルウェアに感染しても簡単には平文のパスワードを抜き出されないような強固な暗号化などの対策や、マスターパスワードの入力時には、キーロガーの被害を受け難い「Secure Desktop」と呼ばれるモードを利用するなどの対策が施されています。パスワード管理ソフトであれば絶対に安全ということはないのですが、
ブラウザにパスワードを保存するよりは安全と言えるでしょう。

しかし、パスワード管理ソフトが一般には普及していないことも事実です。パスワード管理ソフトは有償のものも多いですし、使いこなすには一定のITリテラシーが必要です。また、社内環境ではソフトウェアのインストールやクラウドへのアクセスが制限されている場合もあるでしょう。

以前の記事
で紹介した通り、異なるサービスで同じパスワードを再利用（使い回し）したり、既存のパスワードを少しだけ変更して別のサービスに登録したりしている人が半数近くいるという研究結果もありますし、実際に「リスト型攻撃」の被害が多数出ていることも事実です。

パスワードの使い回しには問題があることはわかっているが、そうは言っても利用している数十ものサービスで、サービス毎に異なるパスワードを設定してそれを記憶するのは不可能だと、使い回しを放置している人も多いのではないでしょうか？

また、使い回したパスワードを使用している人も、毎回パスワードを入力するのは面倒なので、「パスワードを保存しますか？」との表示が出たら「はい」をクリックしてブラウザに保存してしまうことも多いのではないでしょうか？その結果、使い回しされたパスワードがブラウザに大量に保存されている状態になっている人が多いのが現実だと思います。

一方、ブラウザに保存されたパスワードを抜き取るマルウェアの存在も確認されていますが、現状、日本国内でそのようなマルウェアへの感染者が大量に出ているという状況ではありません。

よって、

> リスト型攻撃の被害にあう確率 ＞ マルウェアにブラウザに保存したパスワードを抜き取られる確率

であると想定すると、パスワードの使い回しをなかなか止められないが、パスワード管理ソフトを使うのもハードルが高いと感

じている人は、パスワードをブラウザに保存しても良いから（覚える必要はないから）、サービス毎に異なるランダムなパスワードを設定することを優先させた方が良いのかもしれません。

Chromeに実装されたパスワード生成機能

「パスワードをブラウザに保存しても良いから、サービス毎に異なるランダムな安全なパスワードを設定しなさい」と言われても、多くのユーザにとっては、安全なパスワードを考えること自体が難しいことではないでしょうか？安全なパスワードを生成するアプリやWebサービスもありますが、毎回、アプリを起動したりWebサービスにアクセスしたりするもの面倒なことです。

そんな人のために2018年9月に公開されたChrome 69から安全なパスワードを自動生成してくれる機能が追加されました。なお、この機能を利用するにはGoogleアカウントでChromeにログインし、パスワードを同期している必要があります。

Chrome 69以降では、パスワード登録画面や変更画面のパスワード入力フィールドを自動検知し、パスワード入力フィールドをクリックすると、自動生成したランダムなパスワードが表示されます。もし、パスワードが自動で表示されない場合は、パスワード入力フィールドで右クリックし、メニューの[パスワードを生成]をクリックすることで、自動生成したランダムなパスワードが表示されます。

Chrome69以降ではパスワード登録画面や変更画面を
自動検知しランダムなパスワードを表示

「提案されたパスワードを使用」をクリックすると、生成されたランダムなパスワードが自動的に入力され、「登録」ボタンなどをクリックすることによりパスワードがブラウザに保存されます。

パスワードはブラウザに保存される

次回以降、サービスにログインする時には、Chromeに保存されたパスワードが自動入力されるようになります。複数デバイスでChromeを使用している場合は、Googleアカウントでログインすることで保存されたパスワードが各デバイスに同期されます。

パスワードを使い回している人は、この機能を用いて各サービスでパスワードの変更を行うことで、サービス毎に異なる強固なパスワードを設定できます。

なお、前述したように、マルウェアの感染などによりブラウザに保存されたパスワードを丸ごと平文で抜き出されて外部に送信されてしまう可能性もあります。その場合でも、直ちにサービスにログインされて被害にあうことのないよう、特に重要なサービスについては、必ず2段階認証を設定するようにしましょう。