STOP! パスワード使い回し!キャンペーン2018

最終更新: 2018-08-02

[https://www.jpcert.or.jp/common/social_links/images/btn_share_mail_jp.png](mailto:?subject=STOP!%20%E3%83%91%E3%82%B9%E3%83%AF%E3%83%BC%E3%83%89%E4%BD%BF%E3%81%84%E5%9B%9E%E3%81%97!%E3%82%AD%E3%83%A3%E3%83%B3%E3%83%9A%E3%83%BC%E3%83%B32018&body=http%3A%2F%2Fwww.jpcert.or.jp%2Fpr%2F2018%2Fstop-password2018.html)

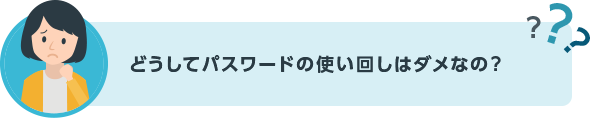
[https://www.jpcert.or.jp/common/social_links/images/btn_share_tweet_jp.png](javascript:;)



STOP! パスワード使い回し! ～知っておきたい、パスワードの危険な落とし穴とその対策～

インターネット上のサービスを利用する際に入力するアカウントIDとパスワードを「認証情報」と言います。この認証情報が漏えいし、悪用されるといった事件が国内外で後を絶ちません。  
同一の認証情報を複数のインターネットサービスで使い回していると、どれか1つのサービスから認証情報が漏えいした際に、他のサービスにも不正にアクセスされ、被害に遭う恐れがあります。  
そうした事態を避けるためには、どのような点に注意すればよいのでしょうか。ここでは、安全なパスワードの設定や、インターネットサービスで提供されているセキュリティ機能の活用など、被害のリスクを減らすための方法と対策をご紹介します。

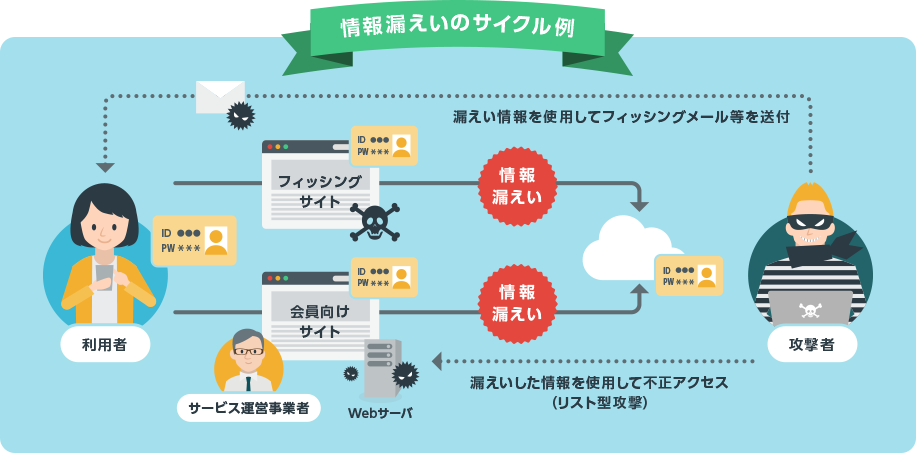
[](https://www.jpcert.or.jp/pr/2018/stop-password2018.html#tips0) [](https://www.jpcert.or.jp/pr/2018/stop-password2018.html#tips1) [](https://www.jpcert.or.jp/pr/2018/stop-password2018.html#tips2) [](https://www.jpcert.or.jp/pr/2018/stop-password2018.html#tips3)

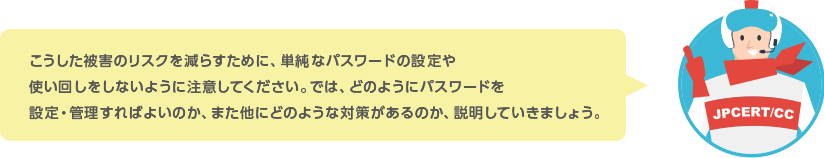


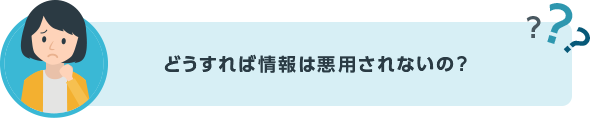
はじめに：情報漏えいのしくみを知ろう

攻撃者がパスワードをどこから盗み出し、どのように悪用するのか、まずは情報漏えいのしくみを知っておきましょう。

|  |  |
| --- | --- |
| pr180002_7.png | pr180002_8.png |
| pr180002_9.png | pr180002_10.png |







TIPS 1：安全なパスワードを設定しよう

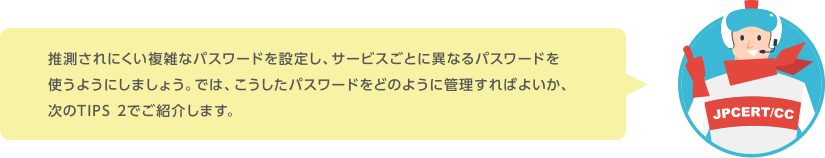
単語や生年月日など、短くて単純なパスワードは、攻撃者に簡単に推測されてしまいます。次のような例を参考にして、安全なパスワードを設定しましょう。

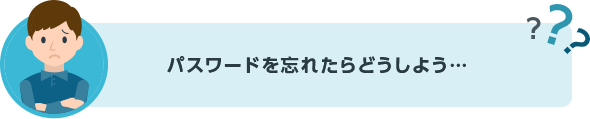
|  |  |
| --- | --- |
| pr180002_14 | **安全なパスワードの条件** |
| **□ パスワードの文字列は、長めにする（12文字以上を推奨） □ インターネットサービスで利用できる様々な文字種（大小英字、数字、記号）を組み合わせると、より強固になる □ 推測されやすい単語、生年月日、数字、キーボードの配列順などの単純な文字の並びやログインIDは避ける □ 他のサービスで使用しているパスワードは使用しない** | |

これまでは、英大文字・小文字、数字に加えて記号を混ぜ込むことが多々推奨されてきました。しかし、「アルファベットを数字や記号に置き換える」等の方法では、憶えやすさが損なわれたり（※後述のコラムを参照）、「p@ssword」（aをアットマーク「@」に置き換え）のような置き換えの場合、辞書攻撃であらかじめ推測されている恐れがあります。したがって、現在では、これまでの方法より数文字でも多くの文字を使うことが望ましいと考えられています。  
  
例えば、8文字で英大小文字＋数字＋記号（94種0.6京通り）をすべて使っても、解読コストの視点から考えると安価なため、容易に解読が可能となりますが、記号を使わない12文字以上であれば英小文字＋数字だけ（36種473京通り）でも解読コストは高くなり**[[1]](https://www.jpcert.or.jp/pr/2018/stop-password2018.html" \l "1)**、一定の強度を保てると推測できます。  
  
特定のアルファベットを記号に置き換えたり、意味のない文字列を覚えるよりも、元々意味のある単語の方が記憶しやすいと考えた場合、  
**［ 英単語 ］＋［ 好きな日本語のローマ字 ］＋［ 英単語 ］＋［ 英単語 ］…**  
のように、単語は辞書からランダムに選んだり、日本語の好きな言葉をローマ字にすることで、記憶しやすく、また文字数の長いパスワードが生成できます。  
利用するサービスによって文字数に上限や英大文字・小文字、数字、記号を必ず加えるなどの制限がある場合は、その制限内で複雑かつ他のサービスで使用していないパスワードを設定しましょう。

**コラム：安全なパスワードって？～米FTCの記事とNISTの文書から考える～**

「どんなパスワードなら大丈夫なのか」という疑問に対して、「攻撃者はどのような手口でパスワードを破るのか」という観点で考えてみたいと思います。  
  
パスワードに関連する攻撃として、単語や人名などをあらかじめ辞書形式にしてログイン試行を行う、辞書攻撃という手法があります。これに使われる辞書データには、一般的な英単語や、推測されやすいパスワード（例:123456、password）が登録されているため、この攻撃への対策として、いくつかの英字を数字や記号に置き換える対策方法が紹介されることがあります（例：p@ssword）。   
  
ところが、攻撃者はこうした対策を見越して、ひとつの単語につき、バリエーションの違う候補（p@ssword,passw@rd,pa$$word）を辞書に登録する恐れがあるため、簡単な置き換えだけでは不十分と言えます。  
このような簡単な置き換えのほか、パスワードの設定・運用の甘さによって、攻撃者に推測されやすくなることを示した実験について、米連邦取引委員会（FTC：FEDERAL TRADE COMMISSION）のLorrie Cranor氏が2016年のブログで紹介しています[**[2]**](https://www.jpcert.or.jp/pr/2018/stop-password2018.html#2)。  
  
ノースカロライナ大学で実施されたこの実験は、1万以上のアカウントパスワードをもとに行われ、3ヶ月ごとに求められる定期変更によって設定されるパスワードの履歴から、次に設定されるパスワードを推測できるかというものでした。その結果、パスワードの定期変更によりパスワードの変更パターンが定型化してしまい、攻撃者に推測されやすいパスワードとなってしまうことが明らかになりました。加えて、何らかの方法で一度漏えいしたパスワードを攻撃者が知った場合、被験者の17％が変更後のパスワードを推測されてしまったと述べられています。  
このように、「パスワードは定期変更で変えているので、使い回しはしていない」と思っていても、わずか数文字程度を入れ変えた数パターンのパスワードは、いずれ攻撃者に推測されてしまう恐れがあると思われます。  
  
ところで、こうした数字や記号の入れ替えによるパターン化は、サービス提供側で文字数の上限（8文字や12文字、16文字など）が設定されていることも要因となっていると考えられます。  
  
米国立標準技術研究所（NIST）は2017年12月に公開した「デジタル認証のガイドライン（DRAFT Special Publication800-63B Digital Identity Guidelines）」[**[3]**](https://www.jpcert.or.jp/pr/2018/stop-password2018.html#3)のドラフトにおいて、サービス提供側へのパスワード提供に関する要件として、ユーザが選択した場合、「少なくとも64文字の長さを選択できるよう許可すべき」と言及しました。  
ユーザの希望に応じて、サービス提供側の文字数上限が広がることで、数字や記号にとらわれず、もっと多くの単語を組み入れることが可能になり、例えば、自分が好きな単語を3、4個組み合わせた、より記憶しやすく長いパスワードを作成することができます。  
  
独立行政法人情報処理推進機構（IPA）が2013年に公開した「情報漏えいを防ぐためのモバイルデバイス等設定マニュアル」[**[1]**](https://www.jpcert.or.jp/pr/2018/stop-password2018.html#1)において「パスワード解読の想定コスト例（表3）」が示されています。これによると、たとえ英小文字、数字のみのパスワードであったとしても、12文字以上の場合、英大文字・小文字、数字、記号を組み合わせた8文字のパスワードよりも計算コストは数百倍かかると推測されています。  
前述のNISTの文書においても付録Aにて「パスワードの長さはパスワードの強度を特徴づける主要な要因である」と触れられています。   
引き続き、パスワードの設定において、文字、数字を組み合わせる方法も有効ですが、限定された文字数内での記号、数字の強制使用が、「数個のパリエーションの使いまわし」という”隠れパスワード使いまわし”を生み出す恐れがあるため、「覚えやすく、使い回しにならない長いパスワード」をユーザが作りやすくなるよう、サービス提供側がNIST文書等を参考にシステムを運用いただく必要があるといえます。



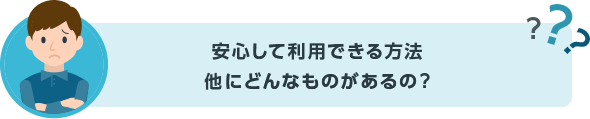


TIPS 2：パスワードを適切に管理しよう

サービスごとに複雑なパスワードをいくつも作成していると、設定した内容を忘れてしまう可能性があります。次のような方法を参考に、適切に管理しましょう。

|  |  |
| --- | --- |
|  |  |
| □ | **紙にメモして、人目に触れない場所で保管する** |
| いちばん簡単な方法が、アカウントIDとパスワードを紙にメモして保管する方法です。ただし、一枚の紙にまとめてメモしてしまうと、万が一盗まれたりすると大変です。アカウントIDとパスワードを別の紙に分けてメモし、別々に保管するようにしましょう。 |
| □ | **パスワード付きの電子ファイルで保管する** |
| パソコンの中で保管したいという場合は、パスワード付きの電子ファイルで保管しましょう。この場合も紙での保管と同様に、アカウントIDとパスワードを別々のファイルに分けて保管するのが安全です。 |
| □ | **パスワード管理ツールを使用する** |
| 「パスワードが覚えられない、そのたびにメモを参照するのは面倒」という方は、信頼性のあるパスワード管理ツールを使用しましょう。多くのパスワード管理ツールでは、各インターネットサービスごとにアカウントIDとパスワードを一度登録しておけば、利用する際にツールから呼び出して自動入力することができます。したがって、利用者はツールを起動するためのパスワードを覚えてさえいればよく、サービスごとに異なる複雑なパスワードをすべて覚えておく必要はありません。  ※クラウドサービスの管理ツールを利用した場合、漏えいリスクは否定できません。クラウドサービスの性質や機能をよく理解してから利用しましょう。 |

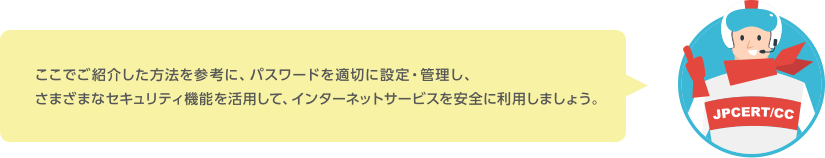




TIPS 3：インターネットサービスのセキュリティ機能を活用しよう

インターネットサービスによっては、安全に利用するために役立つさまざまなセキュリティ機能が提供されています。どのような機能があるのかを事前に確認し、積極的に活用しましょう。

|  |  |
| --- | --- |
| □ **ワンタイムパスワードなどの2段階認証機能を活用する** より強固なセキュリティ対策として、携帯電話やトークンなどを使用したワンタイムパスワードがあります。ワンタイムパスワードによる2段階認証は、アカウントIDとパスワードによる認証に加えて、ログイン時に一定時間だけ有効なパスワードを使用してログインを行う仕組みです。ワンタイムパスワードは毎回変化するため、再利用できず不正なアクセスを防げます。 | pr180002_19 |
| □ **ログイン履歴機能、ログインアラート機能を活用する** ログイン履歴機能のあるサービスの場合、過去にログインされた日時やアクセス元（IPアドレス、国、地域）などを確認することで、心当たりのない不正なアクセスを早期に発見できます。また、通常と異なる時間帯やアクセス元からログインされた場合に、メール等で通知を受けとれるように設定できるサービスもあり、頻繁に利用しないサービスについても異常にいち早く気づくことができます。 **［ 不正なログインに気づいたら ］** 1. すぐにパスワードを変更しましょう 2. インターネットサービスのヘルプデスクに相談しましょう 3. 同じ認証情報を他のサービスで使い回していないかを確認しま  しょう 4. 他のサービスでも不正なログインがないかを確認しましょう | pr180002_20 |
| □**「ID・パスワードを忘れた場合」からパスワードを再設定する** 万が一パスワードを忘れてしまったら、多くのインターネットサービスの場合、ログイン画面には「パスワードを忘れた場合」、「パスワードをお忘れの方」といった案内リンクが用意されており、パスワードの再設定方法を教えてくれます。このような方法を利用することで、簡単にパスワードを再設定し、ログインすることができます。 | pr180002_21 |



**参考情報**

|  |  |
| --- | --- |
|  |  |
| [1] | IPA 独立行政法人情報処理推進機構 |
| 「情報漏えいを防ぐためのモバイルデバイス等設定マニュアル」 <https://www.ipa.go.jp/security/ipg/documents/dev_setting_crypt.html> |
| [2] | FEDERAL TRADE COMMISION(FTC） |
| Time to rethink mandatory password changes <https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes> |
| [3] | National Institute of Standards and Technology（NIST） |
| NIST Special Publication 800-63B <https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.ja.html> |



STOP! パスワード使い回し! キャンペーン 2018 ご賛同企業

複数のインターネットサービスで同じアカウントID、パスワードを使い回すことにより、インターネットサービスへの不正なログイン、いわゆる「パスワードリスト攻撃」による被害が継続的に発生しています。パスワードリスト攻撃による被害の軽減には、サービス提供企業・組織における対策の実施もさることながら、サービス利用者による適切なアカウント管理が重要です。  
サービス利用者へのパスワード使い回しを控えるように広く呼びかけるため、「STOP! パスワード使い回し!」キャンペーンを実施しています。   
  
本キャンペーンにご賛同いただける企業・組織様を募集しています。  
本キャンペーンご賛同企業・組織様には、自社サイトでのキャンペーンバナー、「STOP! パスワード使い回し!」啓発コンテンツの掲載のご協力をお願いいたします。  
  
■ キャンペーン期間  
2018年8月1日（水）～ 2018年8月31日（金）  
  
■ 募集要項  
(1) IDとパスワードを用いて、利用者認証をおこなうサービス提供をしている企業・組織  
(2) 積極的にセキュリティ対策を推進している企業・組織  
(3) 自社サイトにキャンペーンバナーを掲載いただける企業・組織  
(4) 自社サイトに啓発コンテンツを掲載いただける企業・組織  
(5) 反社会的勢力との関係が無い企業・組織   
  
■ お問合せ先  
stop-pass@jpcert.or.jp  
  
■ 関係資料  
STOP!!パスワード使い回し!!～そのパスワードを知っているのは、本当にあなただけですか？～  
<https://www.jpcert.or.jp/pr/2017/pr170002.html>  
  
STOP!! パスワード使い回し!!パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ  
<https://www.jpcert.or.jp/pr/2014/pr140004.html>   
  
STOP!パスワード使い回し！-パスワードリスト攻撃をご存じですか？  
<http://news.mynavi.jp/articles/2015/08/11/stop_pass/>