

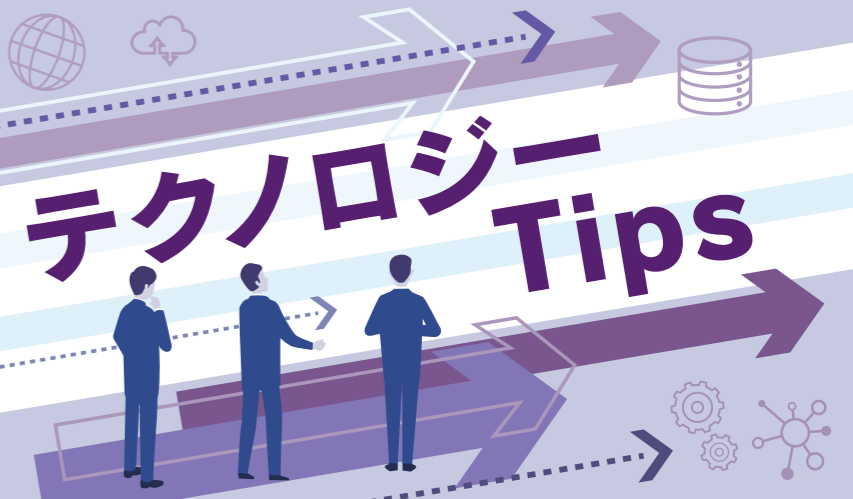
狙われる日本企業—多発する情報漏えいと不正ログイン。事業停止のリスク/パスワード管理は基礎であり基本!!



# そのパスワード、大丈夫ですか?

~数字だけ・短すぎ・使い回しの“本当に怖い”落とし穴~

強いパスワードの作り方、安全な管理、定期見直し、多要素認証(MFA)までを解説します。



パスワードを長くしたり、多要素認証を使ったりすると手間ですよね…  
確かにセキュリティと利便性・手軽さはトレードオフの関係です。  
とは言え!リスクから資産や大切な情報を守ることが優先されます。

## 何が起きているの? 攻撃の手口をやさしく説明



### まずは「総当たり」

これは『0000』『0001』…と、思いつく数字や文字の並びを順番に全部試す方法です。  
パスワードが短かったり単純だったりすると、あっという間に当てられてしまいます。

### 次に「パスワードリスト攻撃」

どこかのサービスで流れ出たIDとパスワードの組み合わせを、別のサービスでも試すやり方です。  
ひとつのパスワードを使い回している、芋づる式に他のサービスまで乗っ取られます。

### 三つ目は「パスワードスプレー」

『Password123!』や『Qwerty!』など、よく使われがちな“ありがちなパスワード”を、たくさんのIDに一斉に投げかけます。ありがちな言葉や並びは、狙われやすいと覚えてください。

### 最後は「フィッシング」

本物そっくりのメールやサイトに誘導して、あなた自身パスワードを入力させるやり方です。多要素認証(MFA)を使っている、偽サイトに6桁コードまで入れてしまうと意味がなくなります。リンク先のアドレスが正しいか、必ず確かめましょう。

まとめると、短い・単純・使い回しのパスワードは、機械にとって

“ごちそう”です。守るコツはとてもシンプルです。

右記の3つを実施・実装するだけで、守りは飛躍的に堅くなります。



長く、いろいろな文字種のパスワードを作成



MFA=多要素認証を使う



パスワードを使いまわさない



## どれだけ危険?

理論的に4桁で数字だけのパスワードを自動化ツールで「総当たり」で「アタリ」を探すまでの所要時間は? 8桁は? 12桁は? 比較してみましょう!

文字数	文字の種類	組み合わせ	計算能力・所要時間	結論
4桁	「数字」のみを使用したパスワード	4桁の数字だけのパスワード(0000~9999)の組み合わせは、全部で10,000通りです。	【前提】現代の一般的なPCや専用のハードウェア(GPUなど)を使った自動化ツールは、1秒間に数万回、数百万回、あるいはそれ以上の試行が可能です。 【計算例】仮にツールが1秒間に10,000回試行できる場合 <b>最悪でも1秒で全て試行でき、高性能なツールなら、事実上「瞬時」。</b>	●4桁の数字パスワードはセキュリティの役割を全く果たしません。
8桁	「数字」「英大文字」「英小文字」を混ぜ合わせたパスワード	使える文字は合計62種類です。組み合わせの総数は「62の8乗」で218,340,105,584,896通り(約218兆通り)になります。	【前提】攻撃者が専用のツール(高性能GPUなど)を使うと、1秒間に数十億~数百億回の試行が可能です。 【計算例】仮に「1秒間に100億回」試行できるツールを使った場合 <b>218兆3401億 ÷ 100億回/秒 = 約21,834秒 21,834秒 ÷ 約6時間。</b>	●非常に高性能なツールを使うと、数時間から半日程度で解読される可能性があります。 ●4桁(瞬時)と比べれば遥かに安全ですが、現代の基準では「脆弱」と判断されます。
12桁	「数字」「大文字」「小文字」「記号」を混ぜ合わせたパスワード	「数字」10種類「英大文字」26種類「英小文字」26種類「記号」32種類と仮定します。合計で94種類の文字を使うこととなります。組み合わせの総数は94の12乗となり、475,920,314,814,213,000,000,000通りとなります。日本語の単位で約4760垓(がい)という天文学的な数字になります。	【前提】攻撃者が手元のマシンで解読する場合です。ここで、8桁の解読で使った「1秒間に100億回」よりも遥かに強力な、専用の巨大クラスター(国家レベルや大規模なハッカー集団)を想定し、「1秒間に1兆回」試行できると仮定します。 <b>約4760億秒 ÷ 約15,000年かかる計算です。</b>	●これは現在推奨される、非常に強力なパスワードです。 ●このレベルのパスワードは、現代の技術で総当たり攻撃を行うことは現実的に不可能。 ●たとえ世界トップクラスの計算能力を持つ攻撃者(1秒間に1兆回試行)が総当たり攻撃を仕掛けたとしても、最悪で1万5千年かかる計算になります。 <b>これが、多くのセキュリティ機関や専門家が「最低12桁以上」「数字・大文字・小文字・記号をすべて使う」ことを強く推奨する理由です。</b>

\*本資料の数値は理論上の概算で、前提条件(オンライン/オフライン、試行制限、ハッシュ方式、計算資源、攻撃手法、文字集合・長さ等)により大きく変動します。

## MFA (多要素認証) とは?

### ●大切な情報を守る「2重ロック」の仕組み

「MFA」と聞くと難しく感じるかもしれませんが、これは「多要素認証(たようそにんしょう)」という、インターネット上のセキュリティを格段に高めるための仕組みです。すごく簡単に言えば、「大事な金庫を開けるための『鍵』を2つ以上にする」という考え方です。

### ●従来の認証(1つの鍵)の問題点

これまでの多くのサービスでは、「IDとパスワード」だけでログインできました。家の鍵(パスワード)1本だけで玄関を開けられる状態です。これだと、もし鍵(パスワード)が盗まれたり、簡単な鍵で(類推されたり)したら、誰でも家に入れてしまいます。

### ●MFA(2つ以上の鍵)で安全に!そこで登場するのがMFA(多要素認証)です。

MFAは、ログイン時に「種類の異なる」複数の証拠を組み合わせ、「本当にあなた本人ですか?」を確認します。MFAが使う「鍵(証拠)」には、大きく分けて3つの種類があります。



知的情報	所持情報	生体情報
例	例	例
●ID・パスワード ●PINコード ●秘密の質問	●携帯電話 ●ワンタイムパスワード ●ICカード	●指紋 ●声 ●網膜

MFAは、これら3種類のうち2種類以上を組み合わせることで認証を行います。例えば、「知識+所持」や「知識+生体」といった具合です。

## なぜ“使い回し”は危険? 今日やめるコツ

### まず結論から!!

同じパスワードを複数のサービスで使うと、1つのサイトで流出しただけで他のサービスまで次々に突破される危険があります。

攻撃者は漏れたIDとパスワードを自動ツールでメール・銀行・会社のクラウドなどへ一気に試す「使い回し攻撃(流出リストの再利用)」を行います。

たとえば通販サイトで情報が漏れると、そのパスワードであなたのメールにログインを試され、乗っ取られると再設定メールを使って銀行や決済サービス、会社のシステムまで奪われる可能性があります。たった1つの流出が、生活と仕事の入り口すべてを開けてしまうのです。

### 今日からできる2つのコツ

#### 1. 大事なアカウントは絶対に使い回さない

最優先で分けるのは次の3種です。

<h4>メール</h4> <p>他サービスの「再発行メール」を受け取る“鍵の束”。ここが破られると芋づるで全滅。</p>	<h4>銀行・決済</h4> <p>金銭被害に直結。2段階認証の有無で被害の大きさが変わります。</p>	<h4>会社の主要サービス</h4> <p>グループウェア、会計、人事、ファイル共有など。社内外の信頼・業務停止リスクに直結。</p>
--	--	---

この3つは最低限、それぞれ別のパスワードにしましょう。理想は、すべてのサービスでパスワードを個別化することです。

#### 2. パスワードマネージャーを使う(保管&自動入力の道具)

全部違う長いパスワードを覚えるなんて無理

そこで登場するのがパスワードマネージャーです!

#### 💡 やることはシンプル

サービスごとに「長く」「複雑な」パスワードを自動生成→自動保存→自動入力。

#### 💡 覚えるのは1つだけ

マネージャーを開くための“マスターパスワード”だけを、長いフレーズで強く複雑に設定します。

#### 💡 安全面

正規のサイト/公式ストアから入手し、ブラウザ拡張やアプリを最新に保つこと。紙やExcelへの書き出しは絶対NG!!です。

### パスワードマネージャーって?

すべてのパスワードを安全な“金庫”に保管し、自動生成・自動保存・自動入力してくれるツール。覚えるのはマスターパスワード1つだけでOK! 手軽で追加アプリ不要なブラウザ内蔵型と、PC・スマホ・拡張で横断利用できる専用アプリ型がある。

**重要なポイント!** 正規ストア以外は使わない+自動更新ON+MFA必須



### それでも? もし「やられたかも」と感じたら: 最初の60分

- 直ちにパスワード変更** | 同じパスワードを使い回していたサービスもすべて変更してください。
- 全端末からのサインアウト** | アカウントの「すべてのセッションを終了」を実行し、ログイン状態を解除します。
- MFA(多要素認証)の再設定** | 認証アプリ・予備端末・物理キーを確認し、回復コードを新しく発行して安全に保管します。
- メール設定の点検** | 転送設定・自動振り分け(フィルタ)・署名等に不審な変更がないか確認します。
- 社内連絡と記録(会社の場合)** | 上長・情報管理担当へ速やかに報告し、対応内容と時刻を記録。必要に応じて同僚にも注意喚起を行います。

### 会社で定められたインシデント対応手順を遵守することが最重要

自分1人で判断せず→即時報告→指示を待つ→担当者・専門家の指示にも続く対応

当社がしっかりご提案、導入サポートいたします!

まずは  
当社にご相談ください!

