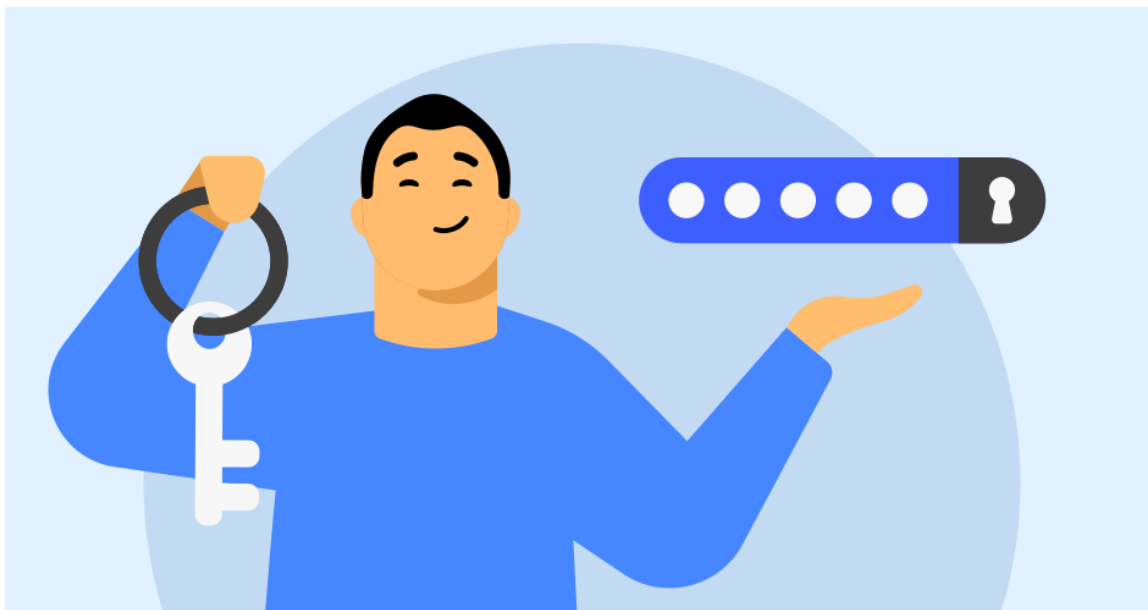


日本で最も使われているパスワード、2025 年は「admin」が 1 位？

NordVPN が日本パスワード利用実態とセキュリティ対策を解説 ～一見安全な「P@ssword」も標的、生活インフラ乗っ取りのリスクも～

個人向けセキュリティサービスを提供する NordVPN（本社：オランダ・アムステルダム、日本代表：小原拓郎）は、1 月 28 日の「データプライバシーデー」に合わせて、傘下のパスワード管理ツール「NordPass」と脅威インテリジェンス「NordStellar」が共同で実施した調査「2025 年日本で最も多く使われているパスワード」の結果を発表しました。調査の結果、日本国内で最も多く使われていたパスワードは、よく知られている単純な数字列「123456」ではなく、ルーターや IoT 機器の初期設定で使用される「admin」であることが判明しました。これは、ユーザーがパスワードを「安易に設定する」段階から、そもそも「変更せずに放置する」段階へとリスクの質が変化していることを示しており、生活インフラの乗っ取りリスクが高まっている実態を浮き彫りにしています。



調査概要

本調査は、NordPass と NordStellar が独立系のサイバーセキュリティ研究者と協力し、2024 年 9 月から 2025 年 9 月にかけて公開されたデータ侵害およびダークウェブ上のリポジトリを統計的に分析したものです。個人の特定につながるデータは一切含まれていません。

- **調査対象**: 公開されたデータ侵害およびダークウェブ上のリポジトリから集計された、世界 44 カ国のパスワードデータおよび関連するメタデータ
- **分析項目**: 国別の最も多く使われるパスワード、パスワードの強度、文化的背景（氏名などの使用傾向）に基づく脆弱性分析など
- **調査期間**: 2024 年 9 月から 2025 年 9 月
- **調査機関**: NordPass、NordStellar

■2025 年日本国内パスワード調査

今回の調査結果において最も顕著な特徴は、1 位となったパスワードが「最弱のパスワード」とされる「123456」ではなく、デバイスの初期パスワードである「admin」であったことです。日本国内におけるパスワードのセキュリティリスクは、単なる「複雑さの不足」から、IoT 機器などの「初期設定を変更せずに利用する」ことへと変化していることが明らかになりました。また、日本特有の人名を含む文字列や、推測されやすい入力パターンも依然として上位を占めており、攻撃者にとって「侵入しやすい環境」が放置されている実態が浮き彫りとなっています。日本国内に限定して分析した今回の調査でも、利便性を優先して推測が容易なパスワードを選択する傾向が依然として続いていることが示されました。

Findings

Japan

Rank ①	Password ①	Count ①
1	admin	42,153
2	123456	38,519
3	password	36,755
4	Freemina123	15,498
5	12345678	10,975
6	yamamoto2580	10,043
7	Chan8899	8,892
8	rosycash	8,828
9	102030Abcd	8,379
10	mokaniku	8,335

1. 首位「admin」が示す IoT セキュリティの死角

今回、日本国内で最も多く検出されたのは「admin」でした。「admin」は、Wi-Fi ルーターやネットワークカメラ、スマート家電などの管理画面において、出荷時の初期パスワードとして広く使用されています。調査の結果、購入後に設定変更が行われていないデバイスが国内に多数存在することが判明しました。こうした状況は、ハッカーにとって家庭内ネットワークへの侵入や、IoT 機器を踏み台にしたサイバー攻撃の実行を可能にするリスクとなります。

2. 「yamamoto」など日本人の名前もランクイン

6 位には「yamamoto2580」がランクインしました。「自分の名前＋数字」の組み合わせは、SNS 等の公開情報と照合されやすく、日本国内のユーザーにとってリスクが高いことが改めて確認されました。ハッカーは、日本人の氏名リストや日本の文化・言語に特化した辞書を用いてパスワードの組み合わせを生成することが可能であり、こうした傾向は不正アクセスのリスクを高める要因となります。

3.「工夫したつもり」のパスワードの脆弱性

12 位の「1qaz2wsx」(キーボードの左端を縦に入力したもの)や、18 位の「P@ssword123456」(a を@に置換したもの)のような、ユーザーが工夫して複雑化したつもりパスワードもランクインしました。ハッカーにとって、このような「物理的パターン」や「典型的な文字置換」はすでに広く知られており、攻撃用の組み合わせとしてデータベース化されています。これらのパスワードは短時間で看破される可能性があります。

(参考:2025 年 日本で最も使われるパスワード Top 20)

1. admin
2. 123456
3. password
4. Freemima123
5. 12345678
6. yamamoto2580
7. Chan8899
8. rosycash
9. 102030Abcd
10. Mocariku
11. tootoo
12. 1qaz2wsx
13. Kanazawa2
14. 123456789
15. mirror2009
16. never4getyou
17. 2020Sank
18. P@ssword123456
19. apple555
20. aabbccdd1234

■ハッカーによるパスワード攻撃の手口

今回の調査において、ハッカーは単に手作業でパスワードを推測しているのではなく、高度な手法を用いて効率的に攻撃を仕掛けている実態が再確認されました。

- **ブルートフォース攻撃(総当たり攻撃):** 自動化されたアルゴリズムを使用し、あらゆる文字の組み合わせを高速で試行する手口です。「admin」や「123456」のような単純なパスワードは、この攻撃に対してほとんど防御効果を持ちません。
- **辞書攻撃とルールベース攻撃:** 「yamamoto」や「P@ssword」のように、人が使いがちな単語や一定の法則(ルール)を登録した辞書を用いて攻撃します。日本の文化に合わせた辞書が使われるため、日本人の名前も瞬時に解析されます。
- **パスワードリスト攻撃:** 過去に流出した ID とパスワードのリストを使い、別のサービスへのログインを試みる手口です。いわゆる「パスワードの使い回し」をしているユーザーを狙い撃ちにするものです。

■NordVPN 最高技術責任者(CTO) マリウス・プリエディスが推奨する、4つのパスワードセキュリティ防御策

① デバイスの「初期設定(デフォルト)」を必ず変更する

今回の調査で「admin」が1位となったことから、初期設定のままのパスワードが多数存在することが明らかになりました。デフォルトのまま使用し続けると、外部からの攻撃リスクが高い状態が続きます。ルーターやIoT機器、管理システムを購入・設置した際は、まず初期設定のパスワードを変更することが重要です。

② 長さや複雑さで「解読コスト」を高める

パスワードは「ハッカーの攻撃を防ぐ壁」にもなります。最低12文字以上の長さにし、大文字、小文字、数字、記号をランダムに組み合わせることで、総当たり攻撃などの手口による解析時間を大幅に引き延ばすことが可能になります。

③ 名前や「ありふれた単語」を排除

自身の名前や「yamamoto」のような一般的な名字、辞書に載っている単語は、ハッカーの組み合わせにも含まれるため、使用を避けましょう。意味を持たないランダムな文字列を設定することで、解析のハードルをさらに高められます。

④ アカウントごとの「使い分け」を徹底

一つのパスワードを複数箇所で使い回すことは、リスクを最大化させる行為です。万が一漏洩した場合の被害を最小限に抑えるため、サービスごとに異なるパスワードを設定してください。信頼性の高いパスワード管理ツールの活用も推奨されます。

■NordVPN 最高技術責任者(CTO) マリウス・プリエディスのコメント

「パスワードはハッカーから、私たちの『デジタル資産』を守る壁のようなものです。氏名、住所、資産など大切な個人情報保存されているアカウントには、より強固な壁を構築する必要があります。しかし今回の調査では、日本でも多くのユーザーが『admin』のまま、もしくは『推測可能な文字列』でその壁を構築していることが明らかになりました。油断しがちなパスワード習慣は国境を問わず共通していることが分かります。『データプライバシーデー』を迎える今だからこそ、パスワードの見直しを行いましょう。パスワードを強化することは、プライバシーを守るだけでなく、デジタルライフ全体を保護する、確実かつ効果的な行動です。」

■NordPass プロダクト責任者 カロリス・アルバチアウスカスのコメント

「一般論として、これまで長年にわたってサイバーセキュリティ教育やデジタル意識向上の取り組みが行われてきましたが、データを見る限り、パスワード管理(パスワード・ハイジーン)の改善はごくわずかにとどまっています。世界は、生体認証に基づく新しいパスワード不要の認証方式『パスキー』へと徐々に移行しつつありますが、広く普及するまでは、強固なパスワードが依然として非常に重要です。特に、データ侵害の約80%は、漏えい・脆弱・使い回しといったパスワードが原因で発生しており、サイバー犯罪者は成功するまで攻撃を繰り返すことになります。」

■NordVPN について

NordVPN は、世界中で何百万人ものユーザーをもつ先進的な VPN サービスプロバイダーです。8,200 台以上のサーバーを世界 127 カ国 165 都市で提供し、専用 IP や Double VPN、Onion Over VPN サーバーなど、多彩な機能を備え、トラッキングなしでオンラインプライバシーを強化します。主要機能の一つである「脅威対策 Pro」は、悪質なウェブサイトやトラッカー、広告のブロックに加え、マルウェアのスキャンが可能です。さらに、最新の製品であるグローバル eSIM サービス「Saily」を展開しています。「Saily」は海外旅行者向けに設計されており、現地で SIM カードを購入する必要がなく、簡単にデータ通信が利用可能です。

【会社概要】

会社名 : NordVPN

本社 : Fred. Roeskestraat 115 1076 EE Amsterdam, Netherlands

日本代表 : 小原拓郎

NordVPN ウェブサイト : <https://nordvpn.com/ja/>

VPN について : <https://nordvpn.com/ja/what-is-a-vpn/>