サポート情報記事

Password Vault のパスワード強度メーター: 各レベルの意味

2026 © Vitextra SIA. 無断転載を禁じます。

免責事項

本免責事項の適用上、次のとおり定義します。

- **会社** (本免責事項では「当社」と表記します) とは、Vitextra SIA (Matīsa iela 61-25, Rīga, LV-1009, Latvia) を指します。
- **本ドキュメント**とは、ナレッジベースの記事を指します。
- **お客様**とは、本ドキュメントにアクセスする個人、または該当する場合は、その個人が本ドキュメントにアクセスまたは使用する際に代理となっている会社その他の法人を指します。
- **本 Web サイト**とは、https://vitextra.com からアクセスできる Vitextra を指します。

免責事項

本ドキュメントに記載されている情報は、一般的な情報提供のみを目的としています。

当社は、本ドキュメントの内容における誤りや脱漏について、一切責任を負いません。

いかなる場合も、契約上の訴訟、過失、その他の不法行為上の訴訟であるかを問わず、本ドキュメントの内容の使用に起因または関連して生じる、特別損害、直接損害、間接損害、結果的損害、付随的損害、またはその他一切の損害について、当社は責任を負いません。当社は、事前の通知なく、いつでも本ドキュメントの内容に追加、削除、または変更を行う権利を留保します。

誤りおよび脱漏に関する免責事項

本ドキュメントに記載されている情報は、関心のある事項に関する一般的な指針を示すことのみを目的としています。そのため、本ドキュメントの内容を最新かつ正確に保つために当社があらゆる予防措置を講じている場合でも、誤りが生じる可能性があります。また、法律、規則、規制は変化するため、本ドキュメントに記載されている情報に遅れ、脱漏、または不正確な点が含まれる場合があります。

当社は、誤りや脱漏、またはこの情報の使用によって得られた結果について、責任を負いません。

フェアユースに関する免責事項

当社は、著作権者から明示的な許可を得ていない著作物を使用する場合があります。当社は、批評、論評、ニュース報道、教育、学術研究、または調査の目的で、そのような資料を提供しています。

当社は、これが、米国著作権法第 107 条に規定されている、当該著作物の「フェアユース」にあたると考えています。

お客様が、フェアユースの範囲を超えて、ご自身の目的で本ドキュメントの著作物を使用することを希望される場合は、著作権者から許可を得る必要があります。

「自己責任での使用」に関する免責事項

本ドキュメントのすべての情報は、完全性、正確性、適時性、またはこの情報の使用によって得られる結果について何ら保証することなく、また、性能、商品性、特定目的への適合性に関する保証を含むがこれらに限定されない、明示または黙示を問わずいかなる種類の保証もなく、「現状のまま」提供されます。

当社は、本ドキュメントに記載されている情報に依拠して行われた判断や措置、または結果的損害、特別損害、もしくはこれらに類する損害について、たとえそのような損害の可能性について知らされていた場合でも、お客様またはその他の者に対して責任を負いません。

お問い合わせ

本免責事項についてご不明な点がある場合は、メール (support@vitextra.com) でお問い合わせください。

目次

メーターが表示される場所 4

5 つのレベル 4

推定の計算方法 5

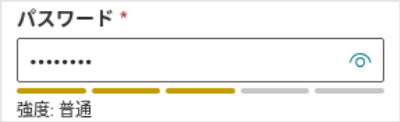
例 6

メーターは保存をブロックしない 7

より強力なパスワードにするためのヒント 7

メーターが表示される場所

Password Vault の**新しいアイテム**ダイアログと**プロパティの編集**ダイアログでは、**パスワード**フィールドが空でなくなるとすぐに、フィールドのすぐ下に強度メーターが表示されます。メーターは 5 つのセグメントからなるバーと**強度**ラベル (例: *強度: 普通*) で構成されます。メーターは文字を入力するたびに更新され、パスワード ジェネレーターが新しいパスワードをフィールドに入力したときにも更新されます。



パスワード フィールドの下の強度メーター

5 つのレベル

メーターは、ビット数で表す概算のエントロピーを使用します。数学的なモデルでは 1 ビット増えると探索空間は 2 倍になりますが、この簡易計算は実際の試行回数や解読に必要な時間を予測するものではありません。推定値は次の 5 つのレベルに対応付けられます。

レベル	塗りつぶされるセグメント	色	推定される強度
非常に弱い	5 個中 1 個	濃い赤	28 ビット未満
弱い	5 個中 2 個	オレンジ	28 ビット以上 40 ビット未満
普通	5 個中 3 個	黄	40 ビット以上 60 ビット未満
強い	5 個中 4 個	薄い緑	60 ビット以上 80 ビット未満
非常に強い	5 個中 5 個	緑	80 ビット以上



5 つの強度レベル

推定の計算方法

計算はブラウザー内で行われ、次の 4 つの要素が考慮されます。

1 **文字プール。** メーターは、パスワードに含まれる文字の種類を確認し、その文字数を合計します。小文字の英字 (a–z) は 26、大文字の英字 (A–Z) は 26、数字は 10、それ以外の文字 (記号、スペース、発音区別符号付きの文字など) は 32 として数えます。したがって、4 種類すべてを含むパスワードのプールは 94 文字となり、1 文字あたり約 6.55 ビットになります。小文字だけのパスワードでは、1 文字あたり約 4.7 ビットです。

2 **実効長。** まず、パスワードの長さを異なる文字の数の 2 倍までに制限します。次に、直前の文字を繰り返す文字 (aa) や昇順・降順の連続を続ける文字 (ab、21) の数を差し引き、結果が負になる場合はゼロとします。そのため、少ない種類の文字で構成された長いパスワードは、強度があまり上がりません。

3 **ビット数。** 推定値は、実効長にプールの 1 文字あたりのビット数を掛けたものです。

4 **よく使われる単語。** パスワードに、よく知られた弱い単語 (password、passw0rd、qwerty、admin、welcome、letmein、123456、abc123、iloveyou、11111) のいずれかが大文字と小文字を問わず含まれている場合、推定値は 20 ビットに制限されます。これは、パスワードの残りの部分がどれだけ長くても、常に**非常に弱い**になります。

例

次の例は、いくつかのパスワードに対してメーターが表示するレベルを示しています。

パスワード	レベル	理由
`Password123!`	非常に弱い	よく使われる単語 *password* を含んでいます。
`qwerty2024!`	非常に弱い	よく使われる単語 *qwerty* を含んでいます。
`abcdefgh`	非常に弱い	1 つの長い連続で、ほぼすべての文字が予測可能です。
`48271935`	非常に弱い	数字のみで、プールが 10 文字と小さいためです。
`contosocrm`	普通	小文字のみです。
`Contoso2026`	普通	3 種類の文字を含みますが、長さが 10 文字しかありません。
`7Vq!x2Lp`	普通	4 種類すべてを含みますが、長さが 8 文字しかありません。
`7Vq!x2Lp#9`	強い	4 種類すべて、10 文字です。
`7Vq!x2Lp#9Dk4`	非常に強い	4 種類すべて、パターンのない 13 文字です。

これらの例のパスワードは使用しないでください。

メーターは保存をブロックしない

メーターはあくまで目安です。**非常に弱い**パスワードのエントリも保存できます。たとえば、サービス側でパスワードが指定されている場合や、既存のパスワードを記録する場合です。Password Vault がパスワードを拒否したり変更したりすることはありません。判断はユーザーに委ねられます。

メモ

推定は、ローカルで行われる簡易的な計算です。上記のよく使われる単語の短いリストを除き、パスワードを辞書や漏えいしたパスワードのリストと照合することはなく、同じパスワードをほかの場所で使用しているかどうかもわかりません。**非常に強い**と評価されたパスワードでも、情報漏えいが発生した別のサイトで使い回していた場合は安全ではありません。

より強力なパスワードにするためのヒント

- **長くしてください。** 長さは最も効果的な要素です。ランダムな文字を 1 文字追加するごとに、最大 6.55 ビット増えます。
- **4 種類の文字をすべて組み合わせてください。** サービスで許可されている場合は、大文字と小文字、数字、記号を組み合わせます。
- **パターンを避けてください。** 繰り返しの文字、キーボードやアルファベットの並び、年、上記のよく使われる単語などです。
- **文字セットが小さい場合の限界に注意してください。** 数字だけのパスワードは、異なる文字が最大でも 10 種類しかないため、**非常に強い**には決して達しません。
- **ジェネレーターに任せましょう。** 4 種類すべてを使用して生成された 16 文字のパスワードは、ほぼ必ず**非常に強い**になります。KB10445. Password Vault のジェネレーターで強力なパスワードを生成する方法を参照してください。

ヒント

保管庫で弱いパスワードを改善したら、サイトやサービス側でもパスワードを変更してください。エントリの編集については、KB10443. Password Vault でエントリを追加、編集、削除する方法で説明しています。