

## 「ミドルの転職」への不正アクセス発生に関するお詫びとご報告

この度、当社が運営する転職情報サービス「ミドルの転職」において、外部からの不正アクセスが発生したことが判明いたしました。

本件により、サービスをご利用のユーザー様および関係各位の皆様へ、多大なご迷惑とご心配をおかけいたしますことを、ここに深くお詫び申し上げます。

本件に関して、現時点で判明している概要と対応について、下記の通りご報告いたします。

### 1. 経緯

2026年6月2日、「ミドルの転職」のWebサーバーにおいて不正なログインを検知。社内調査の結果、2026年5月26日～6月2日の期間、外部から不正に取得されたと思われるID（メールアドレス）およびパスワードを使った不正ログイン（リスト型アカウントハッキング※）が発生し、一部のユーザー様の会員情報ページにアクセスされた可能性があることが判明しました。そのため、同日、不正ログインを試行していた送信元IPアドレス群からの通信を速やかにブロックするとともに、セキュリティ対策の強化を行いました。また、所轄警察署への通報・相談、および個人情報保護委員会への報告をしております。

※リスト型アカウントハッキング（リスト型攻撃）は、何らかの手段により他者のIDおよびパスワードを入手した第三者が、これらのIDおよびパスワードをリストのように用いて様々なサイトにログインを試みることで、個人情報の閲覧等を行うサイバー攻撃をいいます。

### 2. 不正ログインに関する情報

- ・不正ログインの対象：「ミドルの転職」の会員情報ページ（ログイン総数2,503件）
- ・不正ログインが確認された期間：2026年5月26日～6月2日

※ユーザー様のパスワードはハッシュ化（復元不可能な文字列への変換）を実施した上で管理しており、現時点で当社内からIDやパスワードが流出した事実は確認しておりません。

※「ミドルの転職」への不正ログインによる履歴書をはじめとする情報の改ざんは確認されておりません。同様に、求職者様以外の企業様側の管理画面への不正ログインや情報の改ざんは確認されておりません。

※「ミドルの転職」以外の当社サービスにおいて、同様の不正ログインは確認されておりません。

### 3. ユーザーの皆様への対応について

・不正ログインに該当するユーザー様につきましては、パスワードのリセットを実施いたしました。また、被害拡大防止策として、不正ログインに該当しないユーザー様につきましても、システムにてパスワードのリセットを実施いたしました。パスワードの再設定方法および注意点とあわせて、個別にメールにてお知らせをいたしました。次回「ミドルの転職」をご利用時にパスワードの再設定をお願い申し上げます。

・6月5日、ユーザー様相談窓口を設置いたしました。ご不安な方、ご質問がある方は下記までご連絡いただきますようお願い申し上げます。

**【本件に関するお問い合わせ窓口】**

E-Mail : [info@mid-tenshoku.com](mailto:info@mid-tenshoku.com)

この度は、ご利用ユーザー様および関係各位の皆様へ多大なご迷惑とご心配をおかけいたしますことを、重ねてお詫び申し上げます。本件を厳粛に受け止め、皆様に安心してサービスをご利用いただけるよう、セキュリティ強化に努めてまいります。