2026年11月4日

各　位

会　社　名　株式会社きちりホールディングス
（コード番号：3082　東証スタンダード）
本社所在地　大阪府大阪市中央区安土町二丁目３番13号
代 表 者 名　代表取締役社長　平川 昌紀
問 合 せ 先　常務取締役　　葛原 昭
電 話 番 号　06-6262-3456（代表）

当社子会社における個人情報漏えいに関する調査結果および再発防止策のお知らせ（最終報）

当社は、2026年9月9日付「当社子会社における個人情報漏えいに関するお知らせとお詫び」にて、当社子会社である株式会社ApplyNow（以下「ApplyNow社」といいます。）が提供する採用管理プラットフォームに対する第三者の不正アクセスにより、個人データが外部へ漏えいした可能性があることをお知らせいたしました。

このたび、ApplyNow社において外部専門機関による調査が完了し、本件の原因、漏えいした情報の範囲、これまでの対応および再発防止策が確定いたしましたので、別紙のとおりお知らせいたします。

お客様をはじめとする関係者の皆さまには、多大なるご迷惑とご心配をおかけしておりますことを、改めて深くお詫び申し上げます。

当社といたしましては、本件を厳粛に受け止め、ApplyNow社の再発防止策の実施状況を確認するとともに、グループ企業に対してセキュリティの向上と個人情報を含むデータ管理の徹底を引き続き促してまいります。なお、本件につきましては、本お知らせをもちまして最終報といたします。

以　上

（別紙）

2026 年 11 月 4 日
株式会社 ApplyNow

不正アクセスによる個人情報漏えいに関する調査結果および再発防止策のご報告（最終報）

株式会社 ApplyNow（以下「当社」）は、当社が提供する「Interview Cloud」「ApplyNow」「ApplyNow Sign」における第三者による不正アクセスおよび個人情報の漏えいについて、2026 年 9 月 9 日にお知らせし、10 月 9 日に情報を更新してまいりました（当社サービスをご利用いただいているお客様への重要なお知らせとお詫び）。

このたび、外部の専門機関によるフォレンジック調査が完了いたしましたので、その結果と当社による調査を踏まえ、本件の原因、漏えいした情報の範囲、これまでの対応および再発防止策についてご報告いたします。

応募者の皆さま、ご利用企業・団体の皆さま、ならびに関係者の皆さまには、多大なるご迷惑とご心配をおかけしておりますことを、改めて深くお詫び申し上げます。

なお、本お知らせは 2026 年 11 月 4 日時点で確認できている内容に基づいております。

1. 調査により判明した事実

外部専門機関によるフォレンジック調査（2026 年 9 月 18 日開始、10 月 23 日完了）の結果、以下が確認されました。

- 第三者は、当社が社内で利用していたデータ分析ツールについて、提供元が公表していた脆弱性を悪用し、2026 年 8 月 9 日に侵入し、管理者権限を取得していました。
- データ分析ツールに接続されていた当社サービス（「Interview Cloud」「ApplyNow」「ApplyNow Sign」）のデータベースについて、8 月 23 日・26 日に一部が閲覧され、9 月 7 日に一括で取得されました。
- 9 月 7 日、ツールの停止を契機に当社が異常を検知し、同日中に不正なアカウント等の無効化・削除を行い、侵入経路を遮断しました。

2. 漏えいした個人情報

対象サービス	主な項目
「Interview Cloud」	応募者情報：氏名、フリガナ、電話番号、メールアドレス 一部の方は選考に関する情報（応募日、面接日等）、生年月日、性別、職業 企業ユーザー情報：氏名、メールアドレス、パスワード（ハッシュ化して保存）、権限
「ApplyNow」	応募者情報：氏名、フリガナ、電話番号、メールアドレス 一部の方は選考に関する情報（応募日、面接日等）、生年月日、性別、住所、職業、受験番号、学校名 企業ユーザー情報：氏名、メールアドレス、パスワード（ハッシュ化して保存）、権限
「ApplyNow Sign」	契約者情報：氏名、フリガナ、電話番号、メールアドレス

	一部の方は生年月日、性別、住所、個人番号、金融機関名・口座情報、基礎年金番号、在留カード番号、雇用保険被保険者番号、扶養控除に関する情報 企業ユーザー情報：氏名、メールアドレス、パスワード（ハッシュ化して保存）、権限

対象の方	人数
応募者・契約者・企業ユーザー	396,920 人
上記「ApplyNow Sign」で雇用契約を締結された方	30,067 人

※個人番号（マイナンバー）は番号のみが対象です。本人確認書類の画像は対象に含まれません。
※クレジットカード情報は当社では保有しておらず、対象に含まれません。
※面接動画や画像・PDF 等のファイルは、データベースとは別の保管領域に保管しており、漏えい対象に含まれません。

3. 発生原因

調査の結果、本件は当社の管理下にあるツールで発生したものであり、以下の点に原因があると判明いたしました。

1. 提供元が公表していた脆弱性情報を把握しておらず、修正版の適用が遅れたこと
2. 接続元の制限を行っていなかったこと
3. 不正な操作を検知・通知する仕組みはあったが、発見までに時間を要したこと
4. 分析ツールから個人情報を含むデータを参照できる構成となっていたこと。また、データの保管期間を定められておらず、ご利用を終了された企業・団体に係るデータの削除が行われていなかったこと

4. 二次被害の有無

外部専門機関の調査結果を踏まえ、現時点で当社が把握している範囲では、本件を原因とする不正利用などの二次被害は確認されておりません。個人番号を悪用した不正な手続き等のご申告もございません。

当社やご応募先企業を装った不審なメール・電話・SMS には引き続きご注意ください。当社から口座情報やパスワード、個人番号をお尋ねすることはございません。

本件が原因と考えられる被害が生じた場合には、事実関係を確認したうえで、個別に誠実に対応いたします。

5. 当社の対応

- 9 月 9 日：当社ホームページで公表（親会社 株式会社きちりホールディングスもプレスリリースを公表）
- 9 月 10 日：所轄警察署へ相談、プライバシーマーク付与機関へ報告
- 9 月 11 日：個人情報保護委員会へ速報を提出。全管理画面ユーザーのパスワードを強制リセット
- 9 月 14 日～：ご利用企業・団体へ報告
- 9 月 19 日～：対象の方へメール等にて個別に通知。ご本人からのデータ削除の依頼にも順次対応

・10 月 9 日：当社サイトで追加情報を更新（漏えいの事実の確認、対象件数、項目）
・10 月 23 日：外部専門機関による調査が完了
・11 月 4 日：個人情報保護委員会へ確報を提出

6. 再発防止策

【実施済み】
・不正アクセスの侵入経路の遮断
・不正に作成されたアカウント、API キーおよび不正に使用された管理者アカウントの無効化
・データ分析ツールの脆弱性修正版への更新
・データベースの接続情報の更新
・データ分析ツールへのアクセスを、許可した IP アドレスからの接続に限定
・全ユーザーの管理画面パスワードの強制リセット
・脆弱性情報の定期的な確認と、期限を定めた修正の適用
【今後実施予定】
・ご利用を終了された企業・団体に係るデータの削除（実施中）
・不審な操作を検知し担当者へ自動通知する仕組みの導入
・データベースの暗号化対象項目の拡大
・データ分析ツールが参照するデータを、個人情報を含まない形に加工した専用のデータに切り替え
・個人情報・特定個人情報の保管期間の策定と、期間経過後の自動削除の仕組み化
・外部機関による脆弱性診断の定期実施（年 1 回）

7. お問い合わせ先

本件に関するお問い合わせ窓口
電話：0120-401-373
受付時間：平日 10:00〜18:00（土日祝を除く）
受付期間：2026 年 11 月 30 日（月）まで
メール：support_biz@applynow.co.jp
特設ページ：https://biz.applynow.jp/support/
※2026 年 12 月 1 日以降は、メールにて受け付けます。

本件については本公表をもって最終報といたします。今後、新たに公表すべき事実が判明した場合は、速やかにお知らせいたします。

当社は、本件を厳粛に受け止め、個人情報の管理体制の強化に全社を挙げて取り組んでまいります。このたびは多大なるご迷惑とご心配をおかけし、重ねて深くお詫び申し上げます。

以　上