2024 年 5 月 31 日

お客様各位

ワークスタイルテック株式会社

個人データの漏えいに関するお詫びと再発防止に関するご報告

2024年3月29日に公表しております「弊社サービスをご利用いただいているお客様への重要なご報告とお詫び」のとおり、弊社サービス「WelcomeHR」にて、弊社のお客様の個人データが漏えいしていたことが判明いたしました（以下「本事案」といいます）。改めまして、お客様及び関係者の皆様には大変ご心配をおかけする事態となりましたことを深くお詫び申し上げます。

今回の事態を厳粛に受け止め、再発防止に向けて個人情報管理体制の強化を図るとともに従業員への教育を徹底し、お客様及び関係者の皆様からの信頼回復に全力で取り組んでまいります。また、本事案で漏えいした個人データについての不正利用その他二次被害の事実は現在までに確認されておりませんが、引き続きお客様の二次被害の防止に向けて各種調査・対応を継続してまいります。

本事案に関するこれまでの調査結果と再発防止に向けた取り組みについて、以下のとおりご報告申し上げます。

1 本事案の概要

弊社のクラウドストレージに対するアクセス権限の誤設定により、2020年1月5日から2024年3月22日までの間（以下「本対象期間」といいます）、特定の条件下(※)において、お客様が弊社サービスを通じてアップロードしたファイルが外部からの閲覧及びダウンロードが可能な状態となっており、実際に2023年12月28日から同年12月29日の間において、第三者からの不正アクセスによりファイルのダウンロードが行われたことが発覚いたしました。

なお、不正アクセスは、弊社と直接契約しているお客様の環境に対して行われたものであり、OEM契約又は再使用権許諾契約に基づくお客様のデータに関しては上記不正アクセスを受けておらず、漏えいもしておりません。

※ファイルは誰でも閲覧可能なオープンな状態にあったわけではなく、意図的に特定の操作を行うことで各ファイルを閲覧し、さらにダウンロード可能な状態にありました。

2 本事案の対応経緯

2024年3月22日：セキュリティ調査の実施過程でクラウドストレージへのアクセス権限の誤設定が発覚しました。なお、当該誤設定については、同日中に直ちに是正いたしました。

2024年3月28日：追加調査の結果、第三者からの不正アクセスにより、クラウドストレージ内のファイルがダウンロードされた痕跡を確認いたしました。

2024年3月29日：弊社ウェブサイトで本事案について公表するとともに、個人情報保護法に従って個人情報保護委員会に対する漏えい等報告（速報）を行い、加えて警察署への相談も行いました。また、同日からご契約先の企業の皆様への通知を実施しております。エンドユーザーのお客様につきましては、お客様ご相談窓口を設置のうえ、公表又は個別のご連絡により漏えい内容について順次通知し、現在もお問い合わせへの対応をさせていただいております。

2024年4月11日：外部専門機関に二次被害に関するダークウェブ調査を依頼しました。当該調査は、現在も継続しております。

2024年4月26日：外部専門機関によるサーバー設定の再点検を実施し、情報漏えいに繋がる可能性がある指摘箇所については同日直ちに是正のうえ安全性を確保しております。情報漏えいリスクのない軽微な指摘箇所については、対応計画を立て、順次是正を行っております。

2024年5月24日：個人情報保護法に従い、個人情報保護委員会に対して漏えい等報告（確報）を行いました。

2024年5月31日：個人情報保護委員会に対して追加の情報提供を行いました。

3 本事案による影響

本事案により漏えいが確認された個人データは、本対象期間中にお客様が弊社サービスを通じてクラウドストレージにアップロードしていた各種身分証明書等のPDFファイル及び画像ファイル（当該ファイル内に含まれる氏名、住所、生年月日、性別、電話番号等）です。当該データに係るエンドユーザーのお客様の数は、以下のとおりです。調査の結果、前回公表時の数値から変更がございます。

なお、漏えいがあったご契約先の企業様及びエンドユーザーのお客様には順次個別にご連絡を差し上げております。

個人データが漏えいした人数（総数）：158,929人

(1) 上記総数のうち 第三者による個人データのダウンロードが確認された人数：150,445人
(2) 上記総数のうち 個人番号情報を含む人数：46,329人
(3) 上記総数のうち クレジットカード又はデビットカード情報を含む人数：8,073人
(4) 上記総数のうち 要配慮個人情報を含む人数：2,707人
(i) 上記(4)のうち 健康診断情報を含む人数：1,937人
(ii) 上記(4)のうち 障がい情報を含む人数：798人

なお、本事案による漏えいは、弊社と直接契約しているお客様が対象であり、OEM契約又は再使用権許諾契約に基づくお客様のデータに関しては、漏えいしておらず、本事案による影響はありません。

4 二次被害について

外部専門機関とともに調査を実施いたしましたが、現在までに、本事案で漏えいした個人データの不正利用の事実は確認されておりません。

5 原因

お客様の個人データを含むファイルの保管先であるクラウドストレージに対するアクセス権限の誤設定により、特定の条件下において、お客様が弊社サービスを通じてアップロードしたファイルが外部からの閲覧及びダウンロードが可能な状態となっておりました。

6 再発防止策

上記2に記載のとおり、クラウドストレージへのアクセス権限の誤設定については、既に2024年3月22日に是正済みです。

これに加え、上記を踏まえ、以下のとおり再発防止策を実施いたします（既に完了したものを含みます）。

(1) システム管理体制の強化
クラウド設定の設計及び変更に関してダブルチェック体制を整備し、不正アクセス等の異常があった際に即時対応できるよう監視体制を強化いたします。
また、万が一、不正アクセスがあった際の被害拡大防止策として、お客様からお預かりしたファイルの保管先分離及びアクセス制限の厳格化を併せて実施いたします。
今後の運用体制やセキュリティ対策につきましては、外部専門機関とも連携し、定期的に見直し・改善を実施してまいります。

(2) 脆弱性診断の強化
本事案の原因となったクラウドストレージへのアクセス権限の誤設定以外にもセキュリティ面におけるその他の不備がないかどうかを点検するため、2024年4月26日、クラウドの設定状況に関する診断を外部専門機関に依頼し、情報漏えいに繋がる可能性がある指摘箇所については同日中に直ちに是正いたしました。情報漏えいリスクのない軽微な指摘箇所については、対応計画を立て、順次是正を行っております。
今後は、現在実施しているアプリケーション及びネットワークに対する定期的な脆弱性診断に加え、上述したクラウド設定状況に関する診断についても定期的に実施してまいります。

(3) 情報セキュリティに関する従業員への再教育
外部専門機関と連携し、個人情報保護や情報セキュリティに関する従業者への再教育を実施いたします。

改めまして、お客様及び関係者の皆様に多大なるご迷惑とご心配をおかけしましたことを深くお詫び申し上げます。
お客様の大事な個人情報を取り扱う会社としてこのたびの事態を厳粛に受け止め、再発防止に全力で取り組むとともに、お客様及び関係者の皆様からの信頼回復に向けて努めてまいります。

本事案に関するお問い合わせ窓口：
ワークスタイルテック株式会社
メールアドレス：support@workstyletech.com