

2023年9月15日

関係者各位

東京都港区新橋 5-1-3
新正堂第一ビル 5階
株式会社 仕事旅行社

不正アクセスに関するご報告（続報）

時下ますますご盛栄のこととお慶び申し上げます。弊社では、関係する皆様に対し、ご通知及び公表をさせて頂きました通り、弊社サーバが不正アクセスを受け、個人情報を含む情報が不正に収奪及び利用されたこと、並びにサービス運営に必要な全ての情報が削除されるといった事案が生じております（以下「本件」といいます。）。

現在におきましても、調査の途中ではございますが、本報告日現在での調査結果及び再発防止に向けた取り組みの概要につきまして、下記の通りご報告申し上げます。

関係者の方々に多大なご迷惑をお掛けしておりますことを、改めて深くお詫び申し上げます。

記

1. 対応の経緯

2023年9月4日	弊社関係者より、弊社に関わる不審なメールが2通届いているとの連絡を受け、弊社サーバへの不正アクセスの疑いが浮上。ホームページを閉鎖し被害状況の把握に着手
2023年9月5日	不正アクセスの原因が弊社サーバ内に設置していた外部メールソフトのセキュリティホールであることが判明。同時に弊社のサーバデータが不正に削除されているのを確認
2023年9月5日	個人情報及び一部の企業情報の流出を確認
2023年9月5日	弁護士、所轄の警察署及び警視庁サイバー犯罪対策課、個人情報保護委員会に報告
2023年9月5日	【重要】弊社に関する虚偽情報にご注意ください 公表
2023年9月6日	【重要】弊社サーバへの不正アクセスのご報告と今後の対応 公表
2023年9月6日	弊社ホームページのトップページのみを限定して復旧
2023年9月8日	弊社関係者に対して、犯人と思われる人物より3通目のメール配信
2023年9月8日	情報の流出及び流出可能性について調査を継続

2023年9月8日	【重要】不正アクセスに関するご報告(続報)公表
2023年9月8日	愛宕警察署及び警視庁サイバー犯罪対策課へ情報を共有
2023年9月11日	セキュリティ専門企業へ原因究明調査を打診
2023年9月11日	問い合わせフォームを復旧。一般からの問い合わせ受付開始
2023年9月13日	セキュリティ会社にホームページセキュリティの脆弱性チェックの検討開始
2023年9月15日	弊社関係者に対して、犯人と思われる人物より4通目のメール配信
2023年9月15日	【重要】不審メールに関するご連絡公表

2. 被害の原因及び状況

外部専門家及び弊社システムエンジニアと共に、不正アクセスを受けたデータサーバの通信ログを調査した結果、本件の概要は以下の通りであることが判明しました。

2023年9月4日深夜、弊社サーバにアップされていた外部メルマガ管理システムがサイバー攻撃を受け、弊社サーバが不正なアクセスを受けました。弊社では2021年頃から当該メルマガ管理システムの使用していませんでしたが、サーバ上で保管していたため攻撃の対象となりました。なお、当該システムは現在弊社サーバ上から完全に削除されています。

なお、特定の弁護士名を名乗る犯人より3回にわたり送信された一斉メールは、その送信範囲からすると、不正アクセス時に不当に取得された個人情報に対して送られたものであると判断しております。

また、弊社サーバの通信ログを解析した結果、弊社が利用していた外部メルマガ管理システムを起点に、不正アクセスをした者によってサーバ内のデータを全て削除されたと判断しております。これにより弊社の主なサービスは現在も運営できない状況に陥っております。
(なお、本報告日現在におきましても復旧対応中となります。)

弊社では、所轄の警察署及び警視庁のサイバー犯罪対策課と連携を進めており、警察からは、既に調査を開始しているとの連絡を受けています。また、個人情報保護委員会に対しても、本件の報告を行っております。

3. 漏えい等したデータの内容

①流出の規模「仕事旅行サーバ」に保管されていた情報となります。2011年2月から2023年9月5日までに入力された情報となります。

②流出した主な情報

- ・氏名(ふりがな)
- ・住所 ・電話番号

・メールアドレス

・生年月日

・職業／業種／性別／職種 ・学歴・職務経歴(求人応募をされた方のみ)

③漏洩した件数 33,670 件(2023 年 9 月 15 日現在)

※9 月 5 日時点で退会済みの顧客データも含まれます。

なお、弊社では、サービス販売等における決済取引は全て外部委託先のシステムを利用しております。このため、弊社は決済情報を一切保有しておらず、本件においてはクレジットカード情報等の流出はございません。

また、弊社の運営するサービスにログインする際に設定いただきましたパスワードに関しましても、ハッシュ化(二重暗号化)を行なっているため、流出はございません。

情報の流出に関連する皆様に向け、新たにお問い合わせ窓口を設置しております。

仕事旅行社情報流出に関するお問い合わせ窓口

URL : https://www.shigoto-ryokou.com/information/contact/

4. 再発防止に向けたセキュリティ強化策

本報告日現在で対策済みの事項及び今後の対策予定に分けてそれぞれご説明いたします。

【対策済】

(1) 被害拡大防止等のため実施した内容

1. 弊社 Web サーバの遮断
2. 対象者に緊急の注意喚起メールの送信
3. サイトでの注意喚起の公表
4. サーバに関連するパスワードの変更
5. 外部専門家との事実関係調査

(2) 行政等との連携及び報告のため実施した内容

1. 管轄の警察署及び警視庁サイバー犯罪対策課への報告
2. 個人情報保護委員会への報告
3. 外部のセキュリティ対策専門家への相談

【対策予定】

1. 外部の専門家による脆弱性チェックの実施

2. 再発防止策の策定
3. 外部専門家及びセキュリティ監督委員会等の提言を踏まえ、再発防止に向けた種々のセキュリティ強化の検討・体制の構築
4. (上記対策を講じた上での)安全性を担保したサービスの復旧

本報告日現在でのご報告とご案内は以上のとおりでございますが、今後におきましても、本件の状況、犯行状況、弊社サービスの復旧状況につきましては、引き続きご案内申し上げます。

この度は、皆様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、重ねてお詫び申し上げます。

以 上