

2023年6月29日

お客様 各位

みかさ社会保険労務士法人

利用システム障害に伴う個人情報の状況に関して

時下ますますご清栄のこととお慶び申し上げます。

平素より当法人に対しまして、格別のご厚情を賜り厚くお礼申し上げます。

先般、ご報告申し上げました利用システム（株式会社エムケイシステム 社労夢/shalom）における障害発生に伴う個人情報の状況に関し、株式会社エムケイシステムより2023年6月25日付および2023年6月28日付にて、①情報漏洩の事実は確認されていないこと、および②個人情報の不正利用等の事実も確認されていないとの通知がございましたのでご報告申し上げます。

なお、下記に掲載しております株式会社エムケイシステムより2023年6月28日付にて公表されました「セキュリティ調査に関する報告書」において上記の通知事項とともに、本件の発生事象から再発防止策までが記載されております。

しかしながら、株式会社エムケイシステムにおける情報セキュリティに関する重要な情報が部分的に含まれていることから、株式会社エムケイシステムにおいても同報告書は厳秘扱いとしており、利用者である当法人に対しても、関係者以外に一切漏洩することがないように注意喚起が行われております。

大変お手数をおかけしますが、同報告書の詳細につきまして、ご確認を必要とされます際は、当法人までご一報頂きますと幸いです。

当法人よりお客様へ個別に送付申し上げます。

この度は、利用システム（株式会社エムケイシステム 社労夢/shalom）障害により、お客様皆様にご迷惑をお掛けすることとなり、重ねてお詫び申し上げます。

本件に関する新たな情報が入りましたら、随時、お客様各位にご報告申し上げます。

—ご参考 株式会社エムケイシステムからのお知らせ—

2023年6月28日

お客様各位

セキュリティ調査に関する報告書

このたびは、お客様、顧問先様、お取引先様、関係者の皆様に多大なご迷惑をお掛けしておりますことを、深くお詫び申し上げます。

このたび発生しました情報セキュリティインシデント（以下「本事案」という）に関して、調査結果を以下の通りご報告申し上げます。

なお、本事案は情報セキュリティに関するものであり、本報告書においても重要な情報が部分的に含まれていることから弊社内においても厳秘扱いとしています。貴社におかれましても、本書面の取り扱いには充分注意頂き、関係者以外には一切漏洩することがないように、厳密な管理をお願い申し上げます。

1. 発生事象

—省略—

2. 本事案の対応経緯（初期検知と初動対応）

—省略—

3. 保全対象機器

—省略—

4. 状況把握と被害状況

—省略—

5. 侵害状況の概要

—省略—

6. 情報漏洩の有無について

■■■■サーバ及び個人情報を保持する■■■■サーバの調査において、暗号化の実行に利用されたランサムウェアプログラムの存在やデータ暗号化の痕跡は確認されておりますが、■■■■サーバに関するプログラムの実行やサービスに対する接続痕跡、データベース情報の抽出・圧縮や外部転送などの情報搾取を示唆するプログラムの実行の事実や痕跡は確認されていません。

—中略—

また、本事案に関連する情報のダークウェブ等での掲載についても調査を実施していますが、現時点においても該当情報の掲載や公開は確認されていません。

以上のことより、本事案への調査の現時点において、情報漏洩の事実は確認されていないこと、ご報告いたします。

7. 再発防止策

—省略—

以上

—ご参考 株式会社エムケイシステムからのお知らせ—

2023年6月25日

お客様各位

株式会社エムケイシステム
代表取締役社長 三宅 登

サービス再開についてのお知らせ

このたびはお客様、顧問先様、お取引先様、関係者の皆様に多大なご迷惑をお掛けしておりますことを、深くお詫び申し上げます。

6月5日からサービス停止しておりました社労夢のサービス再開について以下の通り、ご案内いたします。

1. 社労夢クラウド版のサービス再開について

—省略—

6月20日の中間報告におきまして、システムの復旧につきまして IDC（従来のデータセンター）と AWS(Amazon Web Services)上の両面で構築作業に着手している旨ご案内いたしました。システムの安定性、安全性を考慮し、外部専門家とも検討の上、AWS 基盤（クラウド環境）でのサービス再開を決定いたしました。

サービス再開にあたり、セキュリティ面の強化を実施しております。下記の「4. セキュリティ対策について」をご確認下さい。

2. サービス再開に際し、お客様へのお願い

—省略—

3. 不正アクセスの調査状況

2023年6月5日（月）早朝にランサムウェアによる第三者からの不正アクセスを確認後、直ちに関連するインターネット回線を切断の上、警察などの関係諸機関への報告とご助言を得るとともに、外部の専門調査会社を交え侵入経路の特定、被害情報の確認、情報流出の有無の確認などの調査を実施しており

ます。6月20日中間報告で既報の通り、専門調査会社による調査はその後進んでおり、6月25日現在、個人情報が外部へ送信された痕跡については発見されておりません。また、本件にかかわる個人情報の不正利用等の事実も確認されておりません。なお、当社がお客様からお預かりしているマイナンバーは、他の社労夢製品とは切り離れた環境で完全に暗号化されております。

4. セキュリティ対策について

今回の事象発生以来、システムの復旧作業と並行して外部の専門調査会社と連携して情報セキュリティ対策の強化策を検討してまいりました。お客様に安心して社労夢クラウド版をご利用いただくための主な強化策は以下の通りであります。情報セキュリティ対策及び監視体制の見直し・更なる強化を実施し、今後同じ事態が発生しないよう再発防止策を取ってまいります。

- ・ネットワークセキュリティ対策の強化（アクセス制限、強固な認証方式 他）
- ・エンドポイントセキュリティ対策の強化（既知脅威情報だけでなく未知の脅威対応 他）
- ・ペネトレーションテスト（脆弱性検査等）の定期的な実施
- ・リスクアセスメント、情報セキュリティ監査の定期的な実施
- ・情報セキュリティの運用体制の見直し（情報セキュリティ専門家の活用）

以上