2023年7月19日

お客様各位

株式会社エムケイシステム
代表取締役　三宅　登

当社サーバへの不正アクセスに関する調査結果のご報告

当社は、当社サービスを提供しているデータセンター上のサーバがランサムウェアによる第三者からの不正アクセスを受け、当社が保有するお客様の個人情報が流出したおそれがあること及びデータの暗号化により正常にサービスが提供できない状況になっていたこと（以下、「本事案」といいます。）について、2023年6月6日から2023年6月21日にかけて公表いたしました。

この度、外部専門機関による本事案に関するフォレンジック調査（※）が完了し、報告書を受領しましたので、当該調査結果及び再発防止に向けた取り組みにつきましてご報告申し上げます。

当社システムは現時点でほぼ復旧しており、現時点まで本事案に関わる情報流出は確認されておりません。なお、当社はマイナンバーについては高度な暗号化処理を施しており、今回の流出の恐れがある情報範囲には含まれておりません。

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ましたことを深くお詫び申し上げます。

※フォレンジック調査とは、デジタル機器の記憶装置から証拠となるデータを抽出し、サーバや通信機器などに蓄積されたログ等の証跡情報から発生事象を明らかにする手段や技術のことをいいます。

1．発生事象

2023年6月5日（月）未明、弊社情報ネットワーク内の複数のサーバがサイバー攻撃を受け、サーバ上のデータが暗号化されました。この攻撃により、暗号化されたデータへのアクセスができなくなり、結果としてシステムが停止し、当社サービスの対象である約 3,400 ユーザーの大半に対して正常にサービスを提供できない状況となり、再構築を余儀なくされる事態となりました。

2．本事案の対応経緯

2023年6月5日（月）未明、弊社担当者が弊社のデータセンターで稼働するサーバへアクセスできないことからシステム異常を認知しました。事象を認知した後、弊社担当者がデータセンターへ入館し状況を確認した結果、弊社サービスを使用しているサーバがランサムウェアに感染していることが判明しました。事象確認後、同日9時頃からデータセンターで稼働していた全てのサーバをネットワークから遮断し、マルウェアの感染拡大や被害拡大防止のための対処を行いました。

本事案に関する主な対応経緯は以下の通りです。

日付	対応状況
2023/6/5（月）6:00 頃	システムやサービスにアクセスできない状況を確認、システム異常を検知
2023/6/5（月）7:00 頃	弊社内での調査開始。ランサムウェアによる感染を認知
2023/6/5（月）	ランサムウェア被害対策本部設置
2023/6/5（月）午後	外部の情報セキュリティ専門会社へ対応要請 ～状況ヒアリングや初動対応及び原因調査のためのデータ保全等を実施
2023/6/6（火）	大阪府警（捜査当局）へ本事案について連絡、事情聴取に対応
2023/6/6（火）	「第三者によるランサムウェア感染被害のお知らせ」適時開示
2023/6/8（木）	個人情報保護委員会へ報告
2023/6/9（金）	「第三者によるランサムウェア感染被害への対応状況のお知らせ」適時開示
事案発生直後～現在	システム復旧に向けた再構築（継続対応中）
2023/6/21（水）	「第三者によるランサムウェア感染被害への対応状況のお知らせ（第 2 報）」適時開示
2023/6 月中旬～現在	再発防止策及び対策強化（継続対応中）
2023/6/30（金）0 時	一部サービスの再開：社労夢 V5.0（社労夢シリーズ、ネット de 顧問、ネット de 事務組合）、DirectHR
2023/7/7（金）9 時	一部サービスの再開：社労夢 V3.4（社労夢シリーズ、ネット de 顧問、ネット de 事務組合）、MYNABOX、MYNABOX CL
2023/7/11（火）0 時	一部サービスの再開：一般企業向け社労夢 CompanyEdition V5.0、DirectHR、MYNABOX
2023/7/19（水）	個人情報保護委員会へ確報を提出
2023/7/19（水）	当社サーバへの不正アクセスに関するお知らせと調査結果のご報告（本報告）

3．フォレンジック調査により判明した事実

・外部の第三者による侵入経路の特定

・不正アクセスの影響を受けたサーバ機器の特定

・侵害状況及び流出の恐れがある情報範囲の特定

※今後の情報セキュリティ面のことを考慮し、上記判明した事実の内容については、詳細の公表を控えさせて頂きます。

4．情報漏洩の有無について

調査の結果、本事案がランサムウェアによる侵害であることから、何らかのデータが攻撃者によって窃取された可能性は完全には否定できませんが、情報窃取及びデータの外部転送等に関する痕跡は確認されませんでした。また、現時点において、当社情報がダークウェブ等に掲載されていないか調査を実施してきましたが、当社情報の掲載や公開は確認されませんでした。

以上、調査の結果、情報漏洩の事実が確認されていないことをご報告申し上げます。

なお、 個人情報に関する顧問先及び一般企業の従業員の方からのお問い合わせにつきましては、末尾記載の【個人情報に関する個人の方（本人）のお問い合わせ先】にて対応いたします。

5．再発防止策

本事案については、外部専門機関による調査に基づき、「3．フォレンジック調査により判明した事実」により判明した本事案の発生原因を踏まえ、外部専門機関と連携して今後の情報セキュリティ面の強化及び再発防止のための対策を講じております。本ご報告公表時点において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。

（1）対策済

・各機器の OS 及びソフトウェアの最新化
・ウイルス対策ソフトを最新化した上でのフルスキャンの実施
・アカウントのパスワードポリシーの強化、パスワード再設定
・エンドポイント端末への EDR 導入及び保護、SOC による常時監視
・セキュリティ対策を実装したクラウド環境（AWS）での新規構築
・再構築及び再開サービスに対するペネトレーションテストの実施
・アカウントの棚卸し（不要アカウントの無効化または削除）
・ログの安全な保管及び長期保存の設定実施
・ファイアウォールポリシーの見直し、強化

（2）対策予定

今後、CIS Control Version 8（情報セキュリティガイドライン）の管理策を参考とし、以下の対策を推進します。

・ネットワークセキュリティ対策強化
　→ 拠点やセグメント間での通信制御及び監視
・エンドポイントセキュリティ対策強化
　→ EDR 導入による継続的な保護及び監視
・OS 及びソフトウェアの更新管理の徹底
・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
　→ 外部専門家による外部監査を定期的に実施
・情報セキュリティの運用体制見直し（情報セキュリティ専門家活用）
・情報セキュリティインシデントに対する体制整備（CSIRT 構築運用）
・従業員に対するセキュリティ教育（定期的な啓発活動）
・事業継続計画（IT-BCP）の見直し

6．システム再開や今後の予定

以下のシステムは、7 月中のサービス再開を予定しています。リリース時期は別途ご案内いたします。

・SR-SaaS
・社労夢 CompanyEditionV3.4