外発２３０７２０－第５号

令和５年７月２０日

お客様各位

小林労務®

社労夢サーバへの不正アクセスに関する調査結果のご報告とシステム利用開始のお知らせ

拝啓　平素は格別の御愛顧を賜り厚く御礼申し上げます。まずは、皆様には、大変なご迷惑とご心配をおかけしておりますこと、深くお詫び申し上げます。

株式会社エムケイシステム（３９１０東証スタンダード）（以下 MK システムという。）の社労夢データベースのランサムウェア感染被害につきまして下記の通り、MK システムより発表がされている調査報告とシステム利用開始をお知らせいたします。

敬具

記

［概要］

１．発生事象

令和５年６月５日（月）未明、MK システム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、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

【MKシステム側の対応経緯】

令和５年６月５日（月）未明、MKシステム担当者が同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。

事象を認知した後、MKシステム担当者がデータセンターへ入館し状況を確認した結果、社労夢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。

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の実施。

以下、その後の主な対応経緯

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 ～その後、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
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
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
6/8（木）	個人情報保護委員会へ報告
6/9（金）	「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

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）
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
6 月中旬～現在	再発防止策及び対策強化（継続対応中）
6/30（金）0 時	一部サービスの再開
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
7/19（水）	個人情報保護委員会へ確報情報として報告

【小林労務側の対応経緯】

令和５年６月５日（月）9時頃（営業開始時間）より社労夢システムにログインができない事象の確認。社会保険労働保険手続き、ならびに給与賞与計算業務が一時的に行えなくなる。

同日　13時50分　MKシステムより社労夢接続障害のお知らせをメールで受信。６月６日（火）明朝までの復旧を目指すと記載有。

同日　19時45分　MKシステムより社労夢のサーバが外部からの不正アクセスによる接続障害のお知らせをメールで受信。

同日　小林労務内に「MKシステム障害対策本部」を設置。

以下、その後の主な対応経緯

6/5（月）～6/6（火）	MKシステムより社労夢データへの不正アクセスの通知を受信後、当社ファイルサーバの影響の確認（影響を受けていないことを確認）
6/6（火）	本事案をお客様へ報告
6/6（火）	社会保険労働保険手続きにおいて、代替として自社システムのe-asy電子申請.comの利用を開始
6/9（金）	MKシステムから給与計算代替システム「ネットde賃金web版」の提供により、給与計算業務を随時実施
6/13（火）	個人情報保護委員会へ報告
6/15（木）	MKシステムよりオンプレ版社労夢の提供により、利用開始
6/16（金）	お客様へ 「当社利用ソフトのランサムウェア感染被害による個人情報保護委員会への報告のお知らせ」 「個人情報漏えい等における本人（従業員）通知について」 「個人情報保護委員会への報告についてよくあるご質問」を通知
6/26（水）	お客様へ「エムケイシステム中間報告と今後のセキュリティ対策のご案内」を通知
7/4（火）	個人情報保護委員会へ中間報告を提出
7/21（金）	ご本人通知として「当社利用ソフトのランサムウェア感染被害のお知らせ」を当社ホームページに掲載予定
7/24（月）	オンプレ版社労夢のデータをクラウド版社労夢へ移行、クラウド版利用開始予定
7/25（火）	個人情報保護委員会へ確報情報として報告予定

<u>［フォレンジック調査により判明した事実］</u>

MK システムが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行っております。

・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、詳細の公表は行わないと報告を受けております。

［原因］

【MKシステム側の原因】

サービス提供セグメントで稼働していた公開システム（RemoteAPP　サーバ）からリモートデスクトップ（RDP）を介してドメイン a の AD サーバへ不正アクセスされた痕跡を確認。

これらのアクセス痕跡から、攻撃者はドメイン a のアカウント情報を何らかの方法で取得し、公開システム（RDP サーバ）へログインしたものと考えらる。その後、攻撃者はドメイン a の管理者権限 を奪取し、その権限を利用して同ドメインに所属するサーバに対して侵害を行ったものと考えられる。

【小林労務側の原因】

本事案については、MKシステム側の原因になりますが、サービスの一時的な停止が発生しているため、セキュリティ対策とバックアップ体制の強化についても検討しており、今後の体制が決まりましたら改めてご報告いたします。

［情報漏洩の有無について］

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、MKシステムの調査の結果、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、MKシステム情報がダークウェブ等に掲載されていないか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、MKシステムからは情報漏洩の事実が確認されていないことの報告がありました。また、当社内のファイルサーバに対して、本案件による影響はないことを確認しております。

［再発防止策］

【MKシステム側の再発防止策】

本事案については、外部専門機関による調査に基づき、「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。現時点において対策済みの事項及び今後の対策予定以下の通りです。

（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

【小林労務側の再発防止策】
不正アクセスを受けたのは MK システムではあるものの、社会保険労働保険手続きについては代替として自社システムの e-asy 電子申請.com の利用ができましたが、給与賞与計算においては通常のサービスの提供が難しい状況となり、大変なご迷惑とご心配をおかけし、深くお詫び申し上げます。セキュリティ対策とバックアップ体制の強化についても検討しており、今後の体制が決まりましたら改めてご報告いたします。

［クラウド版社労夢システムの利用開始について］
MK システムの再発防止策については MK システムの代表者に直接、対策を講じていることを確認し社内で慎重な議論を重ねました結果、今後の業務効率を鑑みて社労夢クラウド版に７月２４日付でデータを移行し、利用を開始いたします。
なお、社労夢クラウド版の利用開始をもって、「エムケイシステム障害対策本部」は解散とし、業務は「個人情報保護推進委員会」に引継ぎいたします。

以上

【エムケイシステム障害対策本部】
本部長　　上村美由紀
（社会保険労務士法人小林労務　社員　／株式会社小林労務　代表取締役社長）
事務局長　蜂須賀由佳（株式会社小林労務　取締役管理部長）
連絡先：03-3261-4911　　メールアドレス：kob_kanri-01@kobayashiroumu.jp