

令和5年7月21日

顧問先従業員様各位



## 当社利用ソフトのランサムウェア感染被害のお知らせ

拝啓 平素は格別の御愛顧を賜り厚く御礼申し上げます。

当社では顧問先様からご依頼をいただきました給与計算や社会保険労働保険手続きにおいて、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。）より販売しております「社労夢」というソフトウェアをクラウドにて利用しております。

この度、社労夢のデータセンター上のサーバがランサムウェア感染被害を受けました。現時点でにおいて、MKシステムからは本事案に関わる情報流出は確認されていないと報告を受けております。

つきましては、下記の通り本事案につきましてご通知申し上げます。

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して記載有。

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)	本事案を顧問先様へ報告
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-aspy 電子申請ソフト.com の利用を開始
6/9 (金)	MK システムより給与計算代替システム「ネット de 貸金 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)	顧問先様へ 「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)	顧問先様へ「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を提出
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

#### 【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るが、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。

#### 【漏えい等が発生したおそれがある個人データの項目】

※顧問先様とのご契約内容によって、個人データの項目は異なります。

##### ・社会保険労働保険手続き

氏名 生年月日 性別 住所 入社年月日 退社年月日 基礎年金番号 雇用保険番号 社会保険標準報酬月額 賃金情報（給与・賞与） 扶養者情報（氏名・性別・住所

・基礎年金番号 ・継続給付金支払先口座 ・出産や育休手続きにおける子の氏名、生年月日、性別

##### ・給与賞与年末調整における計算

氏名 生年月日 性別 住所 入社年月日 退社年月日 標準報酬月額 賃金情報（給与・賞与）  
扶養人数 振込先口座情報

#### 【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。

しかしながら、本事案において不審な連絡等がございましたら、以下の窓口までご連絡ください。

#### 【小林労務 個人情報 苦情相談窓口】

連絡先：03-3261-4911 メールアドレス：[kob\\_kanri-01@kobayashiroumu.jp](mailto:kob_kanri-01@kobayashiroumu.jp)

以上