社労連第 637 号
令和５年 11 月 10 日

株式会社エムケイシステム御中

全国社会保険労務士会連合会
（公印省略）

貴社発行の「当社サーバーへの不正アクセスに関する調査結果のご報告（第３報）」に関するご質問について

平素は、当連合会の業務運営にご協力を賜り厚く御礼申し上げます。

さて、標記の件につきまして、社労士業務でのクラウド利用が日常化した中、会員が安心して各システムベンダー様のシステムを活用できる環境の整備が喫緊の課題となっております。

当連合会においては、貴社において発生した情報セキュリティインシデントの実態を把握し、全会員が同様の被害に遭遇しない対策を講ずるべく IT - BCP の重要性を周知していく方針を固めております。

つきましては、今後の社労士業務の円滑な遂行に資するため、別添質問事項について令和５年 11 月 20 日（月）までにご回答いただきますようご協力をお願い申し上げます。

なお、別添質問事項に関しては情報セキュリティに関する法律に精通した専門家の意見を反映したものであることを申し添えます。

担当：事業戦略部　河端祐一
TEL:03-6225-4870
e-mail:kawabatayu@shakaihokenroumushi.jp

質問事項

2023 年 7 月 19 日付貴社代表取締役発信の「当社サーバー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（第 3 報)」（以下「報告書」という。）において、貴社は、「情報セキュリティ面のことを考慮して」判明した事実について公表を控えるとして、ランサムウエアの侵入経路及び侵入原因等を公表しないこととしております。

そのため、今後の同事例の発生する可能性及び再発防止対策の有効性が判断できない状況にあります。

その結果、社労士の顧問先企業に対しても従業員情報の提供を引き続き依頼できるものか憂慮しております。

報告書を拝読するに、再発防止対策によって、同種事案は間違いなく再発しないうえ、さらに強固なものとなったという理解を得るには不十分であり、顧問先企業に対しても、事故の経緯・原因及び改善された安全対策を説明することができません。

つきましては、以下の点について、ご回答をお願いいたします。

1　ランサムウエアの侵入経路及び侵入の理由並びに感染原因を明示されたい。

セキュリティで公開を差し控えるべきか考慮すべきものは、将来の攻撃に対しての対応が問題となるものであり、過去の侵入に関しての事実関係は、十分な防御対策、再発防止対応ができている以上、セキュリティ上の問題はないはずである。

むやみに非公開を続けることは、他社において発生することが危惧される同種事案に対する警戒喚起、未然防止対策立案の必要性からも無益有害であること、さらには、自らの落ち度を覆い隠すもので、いわば、セキュリティの名を借りた自らの落ち度の隠蔽ともなりかねないことを理解されたい。

2　再発防止策の①として「適切なアクセス制御」の実施とあるが、こうした対策がなされていなかったという事実を認めるもの、すなわち「適切なアクセス制御」を欠くことによる侵入が認められたうえでの対応と理解できる。まず、この対策が出てきた理由を説明されたい。

3　同②の「脆弱性管理の徹底」とあるのは、既存システムに脆弱性があったという意味であり、その脆弱性がどのように克服されたのか、脆弱性はなくなったのか、などの確認をすべきであり、その点の説明をされたい。

4　同③の「強固な認証方法の利用」とあるのは、二段階認証、二要素認証などのことを意味しているが、すでにこれらの認証方法は専門事業者間では常識となっており、それらを採用していないのは、重大な過失と言わざるを得ない。この「強固な認証方法の利用」が何を意味しているのか明らかにするとともに、従前の認証方法（4 桁のパスワードでの運用であるなど）がどのようなもので、どのような脆弱性があったの

かを明確にされたい。そのうえで、どのように改善されたのか、明らかにされたい。

5　同④の「定期的なアカウントの棚卸し」とされているが、使われていないアカウントがあり、長期間放置されていたとすれば、アカウントの管理はセキュリティ対策の基本であって、その基本的なセキュリティ対策が実施されていなかったことを意味するものであるが、そうしたアカウントのずさんな放置状態があったのか、明らかにされたい。

6　同⑤「定期的なログレビューの実施」とあるが、事故後のヒアリングにおいて、ログについては常時点検し、３か月ごとに専門家のレビューを受けていると説明されていたが、それ以上何を行うという意味なのか。それとも、そもそもレビュー自体定期的には行われていなかったという意味であるのか、明らかにされたい。

7　再発防止として対策済みの各項目についても、セキュリティ対策の基本であって、初歩的な対策を実施したとの報告であると理解される（EDR などは除く）が如何か。アカウントの見直しを行うなどは前記５に述べた趣旨と同様に明らかにされたい。

以上、御社システムの今後のセキュリティ対策には影響しない事項について質問をさせていただきました。これらの理解ができて初めて、顧問先企業に対しても安心・安全である旨の説明ができるため、事情ご賢察のうえ誠実なご対応をお願いいたします。

万が一にも、誠実な対応をいただけない場合には、安全性の確認が取れないことから、御社がリスクの可能性のある事業者であり、脆弱性の克服が不明なシステムを提供しているものとして評価せざるを得ず、その旨を会員に周知する必要が生じることともなりかねません。

そうしたことがないよう、誠実に、我々に理解できるよう説明されるよう求めます。

2023年７月19日

各　　位

会 社 名　株式会社エムケイシステム
代表者名　代 表 取 締 役 社 長　三宅　登
（コード番号：3910　東証スタンダード）
問合せ先　取締役 管理統括　吉田 昌基
（TEL. 06-7222-3394）

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（第３報）

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。

お客様はじめ関係各位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．サービス再開について

2023年６月30日（金）よりAWS基盤（クラウド環境）での環境を構築し、順次、サービスを再開いたしました。これまでに提供を再開したサービスは以下の通りです。

・これまでに再開したサービス

社労夢 V5.0
社労夢 V3.4
社労夢 CompanyEdition（V5.0のサービス）

ネット de 顧問
MYNABOX
MYNABOX CL
ネット de 事務組合
DirectHR

・7月下旬に再開を予定しているサービス
SR-SaaS
社労夢 CompanyEdition（V3.4のサービス）

６．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及び推奨された以下の①から⑥までの再発防止策を踏まえ、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。

①適切なアクセス制限の実施
②脆弱性管理の徹底
③強固な認証方法の利用
④定期的なアカウントの棚卸し
⑤定期的なログレビューの実施
⑥インシデントに対する体制整備

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
・エンドポイントセキュリティ対策強化
・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
・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

７．第 2 四半期（累計）及び通期連結業績予想について

当社は、2023年６月29日付「業績予想の修正に関するお知らせ」において、第 2 四半期（累計）及び通期連結業績予想につきまして、連結業績予想を一旦取り下げ、未定といたしました。

本事案により影響を受けた対象ユーザー様に対する６月ご利用分について請求を停止することとしましたが、７月ご利用分についてもサービスの提供が順次のリリースとなったことから、一部ユーザー様については日割りでのご請求となる見込みであります。また、インフラ設備の再構築費用、セキュリティ強化のための費用などコストの増加が見込まれます。

しかしながら、今回の不正アクセスによる対象ユーザー様の解約や新規受注の減少の影響を現時点で正確に見積ることが困難であり、かつ、システム復旧やセキュリティ強化のための各種費用が今後も増加する可能性があります。現時点において適正かつ合理的な計画の策定が困難であることから、通期連結業績予想については、策定次第公表させていただきます。

なお、現時点におきましては、１株当たり８円の年間配当予想の修正はございませんが、通期連結業績予想の確定後、修正が必要な場合は、改めて公表いたします。今後も企業価値の向上に努め、株主の皆様へ安定的な利益還元が実現できるように取り組んでまいります

【個人情報に関する個人の方（本人）のお問い合わせ先】

エムケイシステム個人情報お問い合わせ窓口

・電話番号（フリーダイヤル）0120-351-733

・受付時間：７月19日（水）～10月31日（火）9:00～12:00、13:00～17:00（土日祝除く）

※お電話が混み合いつながりにくくなる可能性がございます。お電話がつながらない場合は、誠に申し訳ございませんが、時間をおいておかけ直しいただけますようお願い申し上げます。

※対象事業所を既に退職されているなど諸事情により、対象者ご本人様への直接のお知らせが困難となっている場合がございます。当事案につきまして不安を感じられた方につきましても本問い合せ窓口までお電話いただければ、ご対応させていただきます。

以上