

令和4(2022)年6月1日

勤怠管理システムサーバに対する攻撃について

株式会社ヴィアックス
代表取締役社長 林 秀和

このたび、弊社においては、勤怠管理システムのサーバに対して第三者の不正アクセスによる攻撃を受けました。攻撃の詳細については下記の通りです。

今後、更なる原因の追及とともに再発の防止に努めて参る所存です。このたびは、皆さまにご迷惑をお掛けすることとなりまして、誠に申し訳ございません。衷心より深くお詫び申し上げます。

記

1. 攻撃発生日および発覚日

発生日 : 令和4(2022)年4月1日 22時10分ごろ

発覚日 : 令和4(2022)年4月2日 8時15分

2. 攻撃対象

勤怠・人事給与システムが稼働中のサーバ

3. 情報毀損が発生し、又は発生したおそれがある個人データの項目

勤怠・人事給与システムに登録されている

氏名、生年月日、性別、住所、電話番号、メールアドレス、従業員番号、所属部署、
扶養者の情報(氏名、生年月日、性別、住所)、世帯主情報(氏名、続柄)、
勤怠システムデータ(ログインパスワード、シフトデータ、出退勤打刻データ、
各種申請履歴<打刻・残業・休暇・勤務変更・直行直帰・休日出勤・出張>)
支払い給与データ(銀行口座情報、給与額、標準報酬月額、税額、社会保険料額)

なお、攻撃対象たるサーバ内のデータは、DBのファイルやツールによりデータのバックアップを取っていたファイルであるため、それ単体で直ちに閲覧できるデータではなく、攻撃者側が当該DBと同様の環境を用意し、当該環境においてデータを展開できない限りは、閲覧等はできないデータです。

また、攻撃対象となったサーバには、弊社のお客様及びお取引先様の個人情報に関するファイルは含まれていなかったことを確認しております。

4. 情報毀損が発生し、または発生したおそれがある個人データの件数

従業員 1,872人分、退職者 2,167人分、扶養者 424人分、世帯主 2,423人分

5. 攻撃の種類

ランサムウェアによるデータの暗号化、身代金の要求

6. 対応状況（時系列）

- ・令和4(2022)年4月1日 22時10分頃攻撃発生
(実施したフォレンジック調査により当該時刻より暗号化されていることを確認した。)
- ・4月2日 8時15分に勤怠システムにアクセスできないとの一報あり。
- ・システム管理者が確認したところ、勤怠・人事給与システムのサーバのユーザデータがすべて何者かに暗号化されている状況が確認された。
- ・4月2日、システム管理者が、データセンタに往訪、当該サーバネットワークを切断し、また他のサーバに現状被害がないことを確認した。
- ・当該サーバの暗号化されたファイルを確認したところ、ランサムウェアの感染が発覚した。
- ・4月5日、関係者による協議の上、攻撃対象サーバはデジタルフォレンジック調査を実施する必要があり、初期化等はできないので、当該システムの代替環境構築を決定した。
- ・4月7日、法律事務所に法務サポートを正式依頼した。
- ・4月14日、社内の他のサーバ・システム及び受託図書館の事務用端末に対し、ウイルス感染・攻撃がないことを確認した。
- ・4月15日、専門機関にフォレンジック調査を正式依頼した。
- ・5月17日、社内における調査・検討の内容も踏まえ、代替環境における勤怠打刻及び申請機能を開始した。
- ・5月25日、専門機関によるフォレンジック調査結果の最終報告を受けた。

7. 現状考えられる原因

データセンタ内 DMZ 上にある勤怠システム WEB サーバのメンテナンスを行う際、当該メンテナンス設定の関係上、外部から WEB サーバに対してリモートデスクトップ接続ができることとなっていたところ、当該接続に必要なパスワードが総当たり攻撃により推測され、当該リモートデスクトップ接続を用いて WEB サーバに不正侵入されたものと推察されます。そのうえで侵入後、ランサムウェアを WEB サーバ上で実行され、アクセスできるサーバのファイルを暗号化されてしまったものと考えられます。

8. 二次被害の有無、再発防止について

今回の攻撃について、勤怠・人事給与システムベンダ、構築会社、データセンタ、ネットワーク機器納入業者、およびセキュリティコンサルティング会社、顧問弁護士事務所とも協力して詳細な調査を行った結果、影響範囲及び被害状況は既に特定しており、二次被害はございません。

また、再発防止策として、サーバに対するセキュリティポリシーの強化、サーバのユーザパスワードの強度向上、データセンタ内のネットワーク環境の設定の変更などの施策を実施済みです。今後も、セキュリティコンサルティング会社や顧問弁護士事務所とも協力しつつ、セキュリティ対策ソフトの導入検討、弊社勤怠システムのセキュリティ対策・監視体制の強化、社内規程の再検討・再整備、社内規程の運用の厳格化をはじめ、再発防止に努めてまいります。

9. 当局に対する報告等

個人情報保護委員会	: 6月1日確報報告済
プライバシーマーク事務局（審査団体JUAS）	: 6月1日確報報告済
情報処理推進機構	: 6月1日報告済
警察への被害相談	: 5月30日相談済

10. 本件に関するお問い合わせ先

本件にかかるお問い合わせにつきまして、専用電話を設置しております。

電話番号： 050-3611-4952（6月1日～6月30日の平日 10:00～18:00）

上記期間以外のお問い合わせについてはこちらとなります。

電話番号： 03-3299-6010（受付時間：平日の10:00～18:00）

またこちらのお問い合わせフォームをご利用いただけます。

お問い合わせフォーム：https://www.viax.co.jp/privacy/privacy_toiawase.html

このたびは、皆さまに多大なるご心配とご迷惑をお掛けすることとなりまして、重ねてお詫び申し上げます。

以 上