TAKAMIYA

2023年２月10日

各　　位

会 社 名　株　式　会　社　タ　カ　ミ　ヤ
代表者名　代表取締役会長兼社長 髙 宮 一 雅
（コード番号2445　東証プライム）
問合せ先　取締役兼常務執行役員
経営戦略本部長　　安 田 秀 樹
（TEL. 06-6375-3918）

当社サーバーに対する不正アクセスに関するお知らせ（第２報）

当社は、当社が令和５年（2023年）１月23日に公表した「当社サーバーに対する不正アクセスに関するお知らせ」（以下「既報」といいます。）のとおり、当社並びに当社の子会社である株式会社キャディアン、株式会社トータル都市整備、株式会社青森アトム、株式会社エコ・トライ、株式会社タカミヤの愛菜、八女カイセー株式会社、株式会社イワタ、株式会社ヒラマツ及び株式会社ナカヤ機材（以下、各子会社を総称して「子会社ら」といい、当社と子会社らを総称して「当社グループ」といいます。）のサーバーに対して第三者による不正アクセスを受け、ランサムウェア感染被害を受けたことを確認しました。

当社は、事案発覚以後対策本部を設置のうえ、速やかに、関係機関や外部専門機関との連携のもと、復旧への対応を進めつつ、不正アクセスの原因特定・被害の全容解明・再発防止策の策定に取り組んで参りました。これらの取り組みにつきまして、下記のとおりご報告申し上げます。

本件に関して、お取引先、株主・投資家の皆様をはじめとする関係する方々には、多大なご迷惑とご心配をおかけしておりますことを深くお詫び申し上げます。

記

１．不正アクセスの概要

調査の結果によれば、攻撃者は、当社ベトナム拠点に対して不正アクセスを行ったうえで当社グループの社内サーバーに侵入し、ランサムウェアを実行し、ファイルの暗号化を行ったものと考えられます。既報の後も引き続きベトナム拠点に存在するサーバー等について調査を実施しましたが、外部専門機関から、さらなる調査を実施しても有益な情報が得られない旨の見解が示されており、調査を終了しております。なお、不正アクセスの原因及び再発防止策は後述のとおりです。

２．漏えい等の可能性がある情報

漏えいの可能性がある情報は以下のとおりです。

（１）個人情報について

確認できた事実関係の概要は次の通りです。対象となるお客様には、可能な限り個別にご連絡させていただいております。

＜当社及び当社のお取引先の一般消費者のお客様関連＞
氏名、住所、年齢、電話番号、メールアドレス、性別

＜当社のお取引先関連（お取引先・協力会社の役職員を含む）＞
氏名、住所、所属会社（又は団体）、会社所在地、会社電話番号、所属部署、役職、電話番号、メールアドレス、性別、顔写真、本籍地、血液型、年齢、生年月日、雇入年月日、健康診断結果、健康保険番号（下４桁）又は健康保険証（写し）、年金番号（下４桁）、雇用保険番号（下４桁）、建設業退職金共済手帳番号又は建設業退職金共済手帳（写し）、自動車運転免許証番号

又は自動車運転免許証（写し）、技能取得免許名称又は免許証（写し）、保有資格名称又は資格証（写し）

＜当社の退職者＞
氏名、住所、電話番号、生年月日（ご家族含む）、メールアドレス、マイナンバー（ご家族含む）、その他人事情報等

＜当社の採用選考に応募されたことのある方＞
氏名、住所、電話番号、生年月日、メールアドレス、学歴、職歴（中途採用の場合）

＜当社の株主＞
氏名、住所、保有株式数又は保有されていた株式数

（２）顧客情報等
不正アクセスを受けたファイルサーバ内に、業務関連情報や当社の社内情報に関するファイルが含まれていることが確認されました。

３．発覚の経緯及びこれまでの対応経緯
・令和４年（2022年）12月８日、攻撃が発生しました。
・12月15日、当社の業務システムへのアクセス障害を確認したことから、当社のシステム管理者が調査を行い、社内サーバーに保存されていたファイルが暗号化されるなど、ランサムウェアであるLockBitに感染したことが判明しました。このため、当社は、当社のシステム管理者に、直ちに可能な範囲での被害拡大防止措置を講じさせるとともに、本件の対策本部を設置しました。
・12月16日、当社のシステム管理者の調査により、当社の業務遂行における支障を生じさせない最低限の業務システムの復旧は可能な見込みであることが判明し、直ちに復旧作業を開始するとともに、外部専門家の弁護士及びセキュリティ専門企業に本件の対応に関する支援を依頼しました。
・12月19日、当社において個人情報保護委員会に対する速報を行うとともに、攻撃対象サーバーに関するデジタルフォレンジック調査を実施する外部専門機関の選定作業等を開始しました。
・継続調査により、子会社らにおける本件の影響を確認したため、12月23日、子会社らに関しても個人情報保護委員会に対する速報を行いました。
・令和５年（2023年）１月７日、当社グループに対してランサムウェア攻撃をしたと名乗るものからメールを受信し、また、攻撃者のリークサイトに弊社名が掲載されていることを確認しました。
・１月10日、攻撃者のリークサイトへの掲載を踏まえ、外部専門機関を起用したダークウェブ調査も開始しました。
・１月11日の午前、当社において大阪府警担当課と会議を行い、現状の調査状況を報告し、今後の捜査の進め方につき協議を行いました。
・１月11日、攻撃対象サーバーに関するデジタルフォレンジック調査を実施する外部専門機関からデジタルフォレンジック調査の初期報告を受けました。
・１月18日、デジタルフォレンジック調査の初期報告をもとに社内リリースを公表しました。
・１月19日、大阪府警担当課を訪問し、被害届を提出しました。
・１月23日、東京証券取引所及び当社のホームページにて対外公表を実施いたしました。
・同日、本件に関するお問い合わせ窓口となるコールセンターを設置しました。
・１月26日、デジタルフォレンジック調査を実施する外部専門機関から、更なる調査を実施しても有益な情報が得られない可能性が高い旨の意見を受領し、調査を終了しました。

・２月２日、ダークウェブ調査を実施した外部専門機関から、Lockbitのリークサイト以外には、個人情報を含む当社の情報の流出は確認されなかった旨の初回報告を受けました。
・本日、個人情報保護委員会への確報を行う予定です。

４．調査結果及び再発防止策

（１） 影響範囲

「２．漏えい等の可能性がある情報」に列挙した各情報が暗号化されたこと、また、これらの情報について漏えいのおそれが否定できないことを確認しております。他方で、１月 10 日から開始したダークウェブ調査は現在も継続中であり、現在までにダークウェブ上での情報の流出は確認されていません。また、リークサイトにおいては、マイナンバーを含む個人データの公開はされていない可能性が高いと考えられます。

（２） 不正アクセスの原因

当社ベトナム拠点が不正アクセスを受けたのは、当該拠点に設置されていたセキュリティシステムに脆弱性があったことによるものであると考えられます。また、攻撃者による不審な挙動のログを監視する体制が十分とまではいえず、その後の攻撃を阻止することができなかったと考えております。

（３） 再発防止策

当社は、以下のとおり再発防止と情報セキュリティの強化に取り組んでまいります。

【対応済み】

・被害発覚日である令和４年 (2022 年) 12 月 15 日にインターネット回線を遮断しました。
・同月 16 日、セキュリティシステムに全てのパッチを適用した上、復旧作業を進めました。
・セキュリティソフトのログを確認し、問題がない端末から順次ネットワークへの接続を再開させ、業務を復旧させました。
・被害前から実施している当社グループネットワーク内の異常通信の監視及び自動検知について、継続して実施しています。
・セキュリティシステム、ネットワーク、認証機能を変更・強化しました。
・マルウェア等の感染の早期検知・対応を目的とした最新の EDR 製品を追加的に導入することにより、エンドポイントレベルでの可視化及び情報収集を実施しました。
・データバックアップ方法の見直し及び多重化を実施しました。

【対応予定】

・当社グループネットワーク内の異常通信の監視及び自動検知をさらに強化するため、外部 SOC ベンダーによるネットワークの常時監視を実施するとともに、不正なトランザクションが検出された場合の早期かつ適切な対応を実施することができる体制を構築します。
・管理ログの設定及び保存方法を見直します。
・当社グループの全役職員を対象とする、セキュリティに関する e ラーニング教育を実施します。

５．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。

タカミヤグループお問い合わせ窓口（既報から変更ございません）
電話番号： 0120-885-323
受付時間： ９：00～17：30（平日のみ、土・日・祝日を除く）

今後、お知らせすべき事実が判明した際には、改めて公表致します。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