令和 5 年（2023 年）2 月 16 日

当社親会社のサーバーに対する不正アクセスに関するお知らせ

株式会社キャディアン
代表取締役社長　笠原　靖子

当社は、当社の親会社である株式会社タカミヤ（以下「タカミヤ」といいます。）が令和 5 年（2023 年）1 月 23 日及び同年 2 月 10 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」及び「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）のとおり、タカミヤ及び当社を含むタカミヤの子会社（以下タカミヤ及びその子会社を総称して「タカミヤグループ」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。

本件につきましては、事案発覚以後、タカミヤにおいて対策本部を設置のうえ、速やかに、関係機関や外部専門家との連携のもと、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。

このたびは、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. 不正アクセスの詳細

調査の結果によれば、攻撃者は、タカミヤのベトナム拠点に対して不正アクセスを行ったうえでタカミヤ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。ベトナム拠点に存在するサーバー等について事案発覚以後、継続した調査を実施してまいりましたが、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。対象となる方には、可能な限り個別にご連絡させていただいております。

＜当社のお取引先関連＞
氏名、所属会社（又は団体）、所属部署、役職、電話番号、メールアドレス

＜当社の退職者（退職者のご家族を含む）＞
氏名、住所、電話番号、生年月日、メールアドレス、緊急連絡先（氏名・住所・電話番号・関係）、血液型、顔写真、給与振込口座番号、給与・賞与・退職金の額、所得税源泉徴収票（中途採用者は前職分も含む）、健康保険被保険者記号・番号、健康診断結果、人事面談記録、保有株式数、証券口座番号、マイナンバー、本人との関係（退職者のご家族に限る）

(2) 顧客情報等
不正アクセスを受けたファイルサーバー内に、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、タカミヤの業務システムへのアクセス障害を確認したことから、タカミヤ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、タカミヤは、タカミヤ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、タカミヤのシステム管理者の調査により、タカミヤグループ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、タカミヤ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。
・タカミヤは、継続調査により、当社を含むタカミヤの一部の子会社における本件の影響を確認したため、12 月 23 日、当社を含む当該一部の子会社は、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、タカミヤ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タカミヤの名前が掲載されていることを確認しました。
・1 月 10 日、タカミヤは、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、タカミヤ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、タカミヤは、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、タカミヤは、デジタルフォレンジック調査の初期報告をもとにタカミヤへの社内リリースを公表しました。

・1 月 19 日、タカミヤにおいて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、タカミヤは、東京証券取引所及びタカミヤのホームページにて対外公表を実施いたしました。

・同日、タカミヤは、本件に関するお問い合わせ窓口となるタカミヤグループのコールセンターを設置しました。

・1 月 26 日、タカミヤは、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、タカミヤは、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、個人情報を含むタカミヤグループ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。

・2 月 6 日、タカミヤは、当社を除くタカミヤの一部子会社における本件の影響を確認したため、2 月 8 日、当社を除く当該一部の子会社は、個人情報保護委員会に対する速報を行いました。

・2 月 10 日、タカミヤは、東京証券取引所における対外公表（第 2 報）の適時開示及び個人情報保護委員会への確報を行いました。

・2 月 16 日、本件の影響を受けた当社を含むタカミヤの子会社について、各子会社のホームページにて対外公表の実施及び個人情報保護委員会に対する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

タカミヤの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

タカミヤグループは、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タカミヤ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】

・タカミヤ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。
・タカミヤ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