2023 年 4 月 26 日

株式会社ギンポーパック
代表取締役　田岡　誠也

不正アクセス及びこれに伴うシステム障害について（第 2 報）

（不正アクセスによる個人情報等流出の可能性に関するお詫びとご報告）

この度、当社は、2023 年 3 月 24 日付けで当社ウェブサイト上に公表いたしました「不正アクセス及びこれに伴うシステム障害に関するお知らせ」（以下「既報」といいます。）に記載のとおり、当社のサーバーに対して第三者による不正アクセスを受け、ランサムウェアを使用した攻撃により、当社が保有している個人情報等が漏えいした可能性があることを確認いたしました。これを受け、当社は、対策チームを設置の上、専門業者及び弁護士等外部の専門家の助言を受け、原因特定、被害状況の調査、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、下記のとおりご報告申し上げます。

本件に関して、皆様に多大なるご心配とご迷惑をお掛けしておりますことを深くお詫び申し上げます。

【お問い合わせ先】

本件に関するお問い合わせやご不明な点などがございましたら、当社総務人事部（藍原・宮崎）までお願いいたします。

電話番号：03-3254-1031

（祝祭日を除く月～金曜日 8：45～12：00・13：00～17：45）

以上

記

1. 概要

- 調査の結果によれば、攻撃者は、何らかの方法で当社の VPN（リモートアクセスに使用する機能です。）に侵入し、これを通じて当社社内サーバーに侵入して、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。当社社内サーバーについて調査を実施し、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との意見を受領したため、調査を終了いたしました。

2. 漏えい等の可能性がある情報

(1) 個人情報

当社で連絡先等を把握している方につきましては、個別に通知をお送りしておりますので、各通知書をご参照ください。

当社において、ファイルの暗号化により連絡先等を確認できない方に関する個人情報について、漏えいの可能性がある項目は、以下のとおりです。

漏えい等の可能性がある方	**漏えい等の可能性がある情報**
当社採用選考に応募された方	履歴書等の求人応募関係書類記載事項

(2) 業務関連情報等

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. 発覚の経緯及び現在までの対応状況

- 2023 年 3 月 3 日夜から 4 日早朝にかけて、当社業務システムにおいて障害を検知し、確認を行ったところ、社内サーバーに保存されていたファイルが暗号化されており、ランサムウェアによる被害に遭ったことが判明しました。当社は、直ちに、インターネット接続を遮断し、PC の使用を停止するなど、可能な範囲での被害拡大防止措置を講じるとともに、調査を開始しました。
- 3 月 4 日、外部の専門業者に依頼し、技術的な調査を開始いたしました。
- 3 月 5 日、調査により、当社の生産機能には問題がなく、製品の製造・供給は継続可能であることを確認しました。
- 3 月 6 日、復旧作業を開始し、紙ベースにて、お取引先様からの生産依頼受注、生産、発送依頼及び発送までの工程を滞りなく行えるように体制を整えました。以降、復旧作業を継続しております。
- 3 月 8 日、個人情報保護委員会に対する速報を行いました。
- 3 月 10 日、同種の問題を専門とする外部の弁護士に相談し、助言を得るとともに、今後の対応について連携を開始いたしました。
- 3 月 16 日、警察に被害を申告し、これ以降、継続的に連携を行っています。

- 3 月 24 日、既報を公表し、お問い合わせ窓口を設置いたしました。
- 3 月 31 日及び 4 月 10 日、外部専門機関から、技術的な調査の結果を受領しました。
- 本日、個人情報保護委員会に対する確報を行う予定です。

4. 調査結果等

(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、現在までにインターネット上での情報の流出は確認されていません。

現在、専門の外部機関に依頼し、ダークウェブ上での情報漏えいの有無について調査を行っております。

調査の結果、ご報告すべき事実が判明した場合には改めてお知らせいたします。

(2) 不正アクセスの原因

調査の結果から、当社が利用している VPN が攻撃者からの不正アクセスを受け、社内サーバーに侵入されたことが原因であると考えられます。また、攻撃者による不審な挙動を監視するソフトウェア等の最新化が十分とまでは言えず、侵入後の被害拡大を阻止することができなかったと考えております。

5. 再発防止策

本件の原因を踏まえ、以下の再発防止策を決定し、順次実施しております。

(1) 実施済みの対策

- 侵入防止のため、ファイアウォール及びルータ（VPN 機能を含む。）のセキュリティを強化すること。
- 侵入防止のため、社内の PC 及びサーバーについて、マルウェア対策ソフト等の更新及び定期スキャンを徹底すること。

(2) 今後実施する対策

ア 物理的・技術的対策

- 被害拡大防止のため、侵入したマルウェアを早期に検知・隔離可能なソリューション・サービスを導入すること。
- 被害拡大防止のため、データの重要度に応じたアクセス制御等及びログ保存を徹底すること。
- お取引先様への影響を最小限に留めるため、バックアップの取得方法を見直すこと。

イ 組織的・人的対策

- 不正アクセス・システム障害等の際の対応プロセスを再整備・周知徹底すること。
- 従業員に対する情報セキュリティ教育を再実施し、今後も定期的に実施すること。また、定期的に対応訓練を実施すること。

以上