

2023年11月2日

株式会社近商ストア

### 当社サーバへの不正アクセスによる情報漏えいの可能性について

当社は、10月31日、当社データセンターに設置の一部サーバにおいて第三者のランサムウェアによる不正アクセスを受けたことを確認しました。保守・メンテナンスを委託している専門会社に調査を依頼し状況を確認した結果、外部漏えいの可能性があるデータに、下記の通り個人情報が含まれていることが判明しました。

現在、影響範囲の確認、原因の究明を進めています。

なお、本件については警察への相談を行うとともに、本日、個人情報保護委員会に報告を行いました。

お客様や関係先の皆様にご心配とご迷惑をおかけしますこと深くお詫び申し上げます。

### 記

#### 1. 判明した経緯とこれまでの対応

10月31日午前7時過ぎに、当社データセンターのサーバの異常停止を検知しました。

当社は保守・メンテナンスを委託している専門会社に依頼し、ただちに全サーバの緊急点検を行いました。その後、本件不正アクセスはランサムウェア攻撃であったことを確認し、速やかに対策本部を設置し、被害拡大防止のため攻撃を受けたサーバへのアクセスを遮断し、原因究明、被害状況の確認等を行っています。

調査の結果、当社が保有するネットスーパー会員様約17,000名、当社従業員および扶養家族約12,000名などの個人情報不正アクセスのあったサーバに保存されていたことが判明しました。現時点ではお客さまから被害の報告は受けておりません。

#### 2. 漏えいの可能性のある情報

- (1) KINSHO・Harvesネットスーパー会員（学園前店、高の原店、白庭台店、あやめ池店、真美ヶ丘店の5店舗）約17,000名のお客さまの以下の情報  
①氏名 ②住所 ③電話番号 ④メールアドレス ⑤生年月日  
クレジットカード情報など決済に関する情報は含まれておりません。
- (2) 会社が保有している、当社従業員および扶養家族約12,000名の個人情報
- (3) お問い合わせ頂いたお客様等の個人情報 約7,000件
- (4) 一部の取引先様に関する約1,400件の取引情報など

※不正アクセスを受けた当該サーバは、近商ストアで保有している独立したサーバです。

他の近鉄グループが保有しているサーバには、影響はございません。

### 3. 今後の対応

#### (1) 対象となるお客さまへの対応

ホームページでお知らせすると共に、ネットスーパー会員様には、現在個別にメールにてご連絡しております。

#### (2) KINSHO・Harvesネットスーパーの営業について

原因究明および被害状況の確認のため、10月31日午後の配送分からの受注を当面の間見合わせております。

なお、各店舗の営業は通常通り行っております。

以上が現時点で判明している情報ではありますが、新たな情報が判明しました際には、その都度公表いたします。当社は、近鉄グループの専門機関や関係機関の協力を受けながら調査を継続し、被害拡大の防止および再発防止に向けて対応してまいります。お客様ならびに関係者の皆様におかれましては、不審なメールや通知が届いた場合は、開封およびリンク先へはアクセスしないようにご注意のほどお願い申し上げます。

### 4. 本件に関するお客さまのお問い合わせ先

株式会社近商ストア 総務部

電話番号：072-338-3800

受付時間：平日（月～金曜日）9：00～18：00

11月6日（月）よりフリーダイヤルを開設いたします。

電話番号：0120-099-698

以上