

2024年6月17日

お客様各位

三菱UFJオルタナティブインベストメンツ株式会社

弊社を装ったスパムメールに関するお詫びとお知らせ（続報）

平素は格別のご高配を賜り、厚く御礼申し上げます。

2024年5月21日に、弊社名および弊社社員を装ったスパムメールが複数の方へ送信されました件、メールを受信された皆様には多大なご迷惑をお掛けしましたことを深くお詫び申し上げます。

その後、本件について外部のセキュリティ専門企業の協力のもと弊社内で調査を進めました結果、以下の事象および流出可能性のあるお客様情報が存在することが判明致しました。調査の内容、流出可能性のあるお客様情報の内容および現在の対応状況について以下の通りでございますが、お客様の情報について流出した可能性が生じたことについて、深くお詫び申し上げます。

1. 調査の内容

(1) 2024年5月21日発信の弊社名および弊社社員を装ったスパムメールについて

不審メールの送信元および添付されていたファイルのコンピュータ・ウイルス有無を調査いたしました。その結果、当該メールが当社から発信されたものではないこと、当該添付ファイルにはフィッシングサイトへのURLリンクが存在していることが分かっております。

(2) 発生原因について

弊社内で行いました調査の結果、本件は2024年5月13日に弊社社員が受信した不審メールに起因するものと判明いたしました。当該不審メールの受信履歴から情報流出元となった可能性のあるPCを特定し、外部のセキュリティ専門企業の協力のもとログ解析等を実施した結果、メール等の一部が流出している可能性が判明しました。

2. 流出可能性のあるお客様情報

上記調査の結果、流出可能性のあるお客様情報は以下のとおりです。弊社では情報流出の事実までは確認できておりませんが、お客様の二次被害・類似被害防止の観点から「流出可能性のある」お客様情報をお知らせするものです。お手数をおかけして誠に申し訳ございませんが、お客様の業務（メール連絡等）において所謂「なりすまし」メールがお客様に送信される等の不正行為に利用される可能性があることを念頭にご留意頂きますと幸いです。

- ・ お客様情報（法人名・ご担当者名・メールアドレス）
- ・ お取引に関する一部の情報（私募の取扱いに関する契約書等）
- ・ 業務に関するお客様情報（契約書等）

3. 再発防止について

これまでの調査の過程で判明した事項に基づき、更なるデータ流出を防止するため、2024年5月24日までに以下の不正アクセス遮断措置を実施いたしました。これにより、不審メールを受信した者を含む弊社社員全員について、外部からの不正アクセスを遮断することができたものと判断しております。

- ・外部インターネットから使用アプリケーション（Microsoft365）へのアクセス遮断
- ・弊社社員のPCログインパスワードの変更
- ・社内PC向けリモート操作ツールのパスワード一斉変更
- ・本件メールに添付されていたファイル中のURLへの弊社社員アクセス遮断
- ・不正にデータを窃取するために利用されたアプリケーションの削除及びインストール機能のブロック（Microsoft365）

なお、上記の通り、2024年5月21日発信のメールについては、フィッシングサイトへのURLリンクがございますので、添付ファイルは開封せず、メールごと削除いただきますようお願い致します。

本件に起因する情報の再流出への対応は完了致しましたが、更なるサイバーセキュリティの態勢強化に引き続き取り組んでまいります。ご迷惑・ご心配をお掛けしてしまい誠に申し訳ございませんが、引き続きよろしくお願い申し上げます。

〈本件に関するお問い合わせ先〉
三菱 UFJ オルタナティブインベストメンツ株式会社
TEL: 03-6550-8600
MAIL: system@alt.tr.mufg.jp