2019 年 10 月 25 日

株式会社三菱 UFJ 銀行

ローカルキャッシュマネジメントサービスの通信暗号化装置への不正アクセスによる台湾拠点の一部お客さま情報および第三者情報の漏えいについて

株式会社三菱 UFJ 銀行（取締役頭取執行役員 三毛（みけ） 兼承（かねつぐ）、以下 当行）は、当行がお客さまにご提供するローカルキャッシュマネジメントサービス（Local Cash Management Service、以下 LCMS）の認証システムの通信暗号化装置（東京設置）に対する外部からの不正アクセスが発生し、その結果、台湾拠点の一部法人のお客さまの口座情報や、お客さまのお取引先に関する第三者情報等が漏えいしましたことをお知らせいたします。

現時点で判明している詳細については、以下をご参照ください。

お客さまならびに関係者の皆さまには多大なるご迷惑、ご心配をおかけしておりますことを、心よりお詫び申し上げます。

1. 発生事象

認証システムの通信暗号化装置（以下 本装置）は、お客さまがインターネット経由で当行の LCMS に接続する際にお客さまを認証し、通信を暗号化するための装置です。当行は 2019 年 10 月 4 日に、本装置に外部からの不正アクセスがあったことを認識し、調査を進めてまいりました。その結果、今回の不正アクセスにより、台湾拠点で LCMS をご利用頂いておりますお客さまの画面が閲覧され、お客さま情報が漏えいしたことが判明いたしました。

2. 漏えいした情報の内容

LCMS をご利用頂いている台湾拠点の法人のお客さま 13 社の口座情報とお振込み先等のお取引明細に加え、お客さまのお取引明細に含まれているお取引先や従業員さま等の第三者に関する情報が計 1,305 件漏えいしました。これらの情報には、取引先名、取引銀行、支店名、口座番号、取引金額、メールアドレス等が一部含まれております。

現時点では、今回の情報漏えいに基づく二次被害は発生しておりません。また、台湾拠点以外で LCMS のお取引をされているお客さまへの影響はございません。

3. 発生原因と対応策

本件は、本装置の情報セキュリティ上の欠陥（脆弱性）を突いた不正アクセスが行われたことが原因です。

当行は、不正アクセスを認識した後、本装置をバージョンアップすることにより脆弱性を解消し、外部からの不正アクセスを遮断いたしました。また、監視体制を一層強化するなど、再発防止に努めております。

4.　お客さまへのご対応について

今回ご迷惑をおかけしております台湾拠点の法人のお客さまは全て特定しており、既に当行より個別にご説明をさせて頂いております。また、第三者に関する情報についても、台湾拠点のお客さまのご意向を踏まえながら適切な対応を進めてまいります。

《お客さまからのお問い合わせ窓口》

本件に関するお客さまのお問い合わせ窓口は、以下のとおりです。

【お問い合わせ専用メールアドレス】CMS_shoukai_PF@mufg.jp（日本語・英語）

【コールセンター】

電話番号：0120-860-777　（フリーダイヤル、日本語のみ）

電話受付時間：（日本時間）午前 9 時から午後 9 時まで

以　上