2019 年 10 月 25 日

日商三菱日聯銀行股份有限公司

關於本行分行網路銀行通訊加密設備因惡意連線
導致台灣據點部分客戶及第三方交易資訊洩漏一事

謹此通知，日商三菱日聯銀行（取締役頭取執行董事 三毛 兼承，以下稱本行） 提供客戶使用之分行網路銀行（Local Cash Management Service，以下簡稱 LCMS）入口認證系統之通訊加密設備（設置於東京）日前因發生惡意連線入侵，導致台灣據點部分法人客戶之帳戶資訊及客戶往來企業廠商等第三人交易資訊遭洩漏。本行目前查明之內容詳述如下：

因本件造成客戶及相關第三人之紛擾，本行由衷致上歉意。

1. 發生背景

認證系統之通訊加密設備係客戶透過網際網路登入本行 LCMS 時，用於認證客戶身分、加密通訊內容所必要之設備，本行於 2019 年 10 月 4 日得知該設備受外部嘗試惡意連線後即著手進行調查。調查結果確認，因外部惡意連線入侵，部分台灣據點客戶登入 LCMS 操作中之畫面遭瀏覽致使客戶交易資訊洩漏。

2. 遭洩漏之資訊內容

台灣據點 LCMS 使用客戶中 13 家法人客戶之帳戶資訊及匯款等交易明細，以及客戶交易明細中所含客戶之往來企業廠商或員工等第三人資訊；如第三人名稱、設帳銀行及其分行名、帳號、交易金額、公務郵件地址等，共 1,305 件資訊遭洩漏。

截至目前為止，並無因本資訊洩漏所造成二次受害之情事，本件亦未波及台灣據點以外之 LCMS 交易客戶。

3. 發生原因與對策

本件發生原因係 LCMS 認證系統之通訊加密設備中所存在資安上之漏洞遭惡意連線入侵。

本行於確認惡意連線入侵後，已升級該通訊加密裝置，封鎖外部惡意連線並完成該漏洞之修補。今後並將進一步加強系統監視體制等措施，致力於嚴密防範資安事件再次發生。

4. 客戶因應措施

目前本行針對受影響之台灣據點法人客戶逐一進行說明。關於第三人交易資訊亦充分與客戶溝通後進行必要之應對處理。

《客戶諮詢窗口》

本件客戶諮詢窗口如下：

電子郵件諮詢：CMS_shoukai_PF@mufg.jp（日語・英語）

【客戶服務中心】

電話號碼：0120-860-777 （日本國內免付費電話、日語專用）

電話服務時間：（日本時間）上午 9 時至晚間 9 時

以　上

（聯絡窗口）

三菱日聯銀行　広報部（公關部）03-5218-1814