

業務監査報告（随時）
～モバイル端末紛失事案について（意見）の要旨～

監査委員会
2019年 5 月 16 日

1 事案の概要

2018年 3 月 30 日、当法人がオルタナティブ投資室 に貸与していたモバイル端末（iPad）が所在不明となる事案が発生。その後、1 年が経過するも当該端末は発見されず、固定資産除却損が 52,800 円発生。なお、当該端末を介した情報漏洩の可能性は低い。

同日、 が自室内本棚上にあるはずの当該端末が見当たらないことを認識。いつ時点でなくなっていたのか明確ではないが、3 月 31 日、4 月 1 日の土日にかけて自室内を探索するも当該端末の発見に至らず、 は、4 月 2 日情報管理部等に報告するとともに警察署に遺失物届を提出し、また、4 月 4 日、経理課に「物品亡失・き損届」を提出。

2 監査委員会の監査に至る経緯

2019年 4 月 1 日、常勤監査委員が事案の概要を示す文書の回覧を受けて認識。監査委員会は、事実関係や問題の所在（情報漏洩リスクの存否・程度や同企画役の過失の存否・程度など）が明確ではないため、当法人における情報管理の重要性に鑑み、業務監査の一環として改めて関係者からヒアリングし、資料を分析するなどの調査を実施。

3 調査結果

（1）当法人でのモバイル端末の貸与手順

自宅での利用、出張時や外部（委託先等）での打合せ等における利用に供するため、管理者からの申請によりモバイル端末を貸与。企画役以上の役職者、特に運用専門職の職員への常時貸与については、申請があれば情報管理部は原則として貸与し、出張時のための一時貸与については、「管理運用法人外におけるモバイル端末利用申請書」を管理者に提出し、同申請書に基づき、情報管理部が貸与する手順。内規「情報システム利用手順書」には、「役員等は、インターネット経由で法人ネットワークシステムへ接続可能なモバイル端末を貸与され、これを利用する場合」は、「モバイル端末及び認証情報を**厳重に管理**すること」、「モバイル端末紛失等の際は、

直ちに情報セキュリティ管理者に連絡するとともに、端末内データの遠隔消去措置を講じるよう通信キャリアに連絡を入れること」などと規定。 2019年4月現在の常時貸与者は、経営委員9名、理事長・理事3名、審議役、部室長及び次長17名、運用担当企画役10名、その他4名。一時貸与者（通常は情報管理部で管理）は7名（最大）。

(2) 当法人の貸与端末に係る情報セキュリティ対策

パスワードを初期設定して貸与し、貸与を受けた職員が任意のパスワードに変更。法人ネットワークシステムにある会議資料やメールにアクセスするには、以下の3段階のパスワード入力が必要

貸与時に手渡される書類には、

「iPad紛失時のフロー」、「iPad紛失時の対応手順」が含まれ、その書類中に、紛失が発覚後、管理者及び通信キャリア（ソフトバンク）に連絡することや、通信キャリア、情報管理部の連絡先電話番号が明記。

紛失等を踏まえた対策として、①紛失の際に所在場所を情報管理部が検出する設定、②紛失の連絡があった時点で、同部が法人ネットワークシステムに接続を許可するための「証明書」を無効化

する設定、③ソフトバンクに依頼をすることでモバイル端末の中身を全消去（リモートワイプ）する設定、などを整備。

(3) 本件端末の保管、紛失状況及びその後の追跡

の供述によれば、「

紛失認識時は使用しておらず、

システムからログオフしスリープ状態で自室内に置いていた。」、「

盗難の可能性が極めて高い。」とのこと。また、

「使用する時以外に、端末の有無を確認することがないため、いつ頃かは特定できないが、3月30日より前の1週間程度の間と推測。

。」

「自室の鍵が壊された形跡はないし、自室の合鍵を持たせている人もいない」とのことであり、これらに照らし、

誰かが

同企画役の自室に侵入し、盗んだ可能性が高い。

紛失報告を受けた情報管理部によれば、追跡の結果、当該端末の最終アクセス日は2月26日であり、また、3月26日時点のバッテリー切れを検知（そのため所在場所も不検出）。同部は、4月2日、証明書無効化をするとともに、ソフトバンクに対しリモートワイプを要求したが、現在に至るも電源がオンされていないため実行されず。

4 監査委員会の意見

(1) 事実関係の評価

本件事案発生の原因は、当該企画役が自室内に置いていた本件端末につき「厳重な管理」を怠った点にある。同企画役の自宅が
、PC管理上危険な状況にあった。

「厳重な管理」をすべきであった。また、紛失を認知したときは「直ちに情報セキュリティ管理者に連絡を入れること」とされているのであるから、少なくとも認知した当日中に連絡すべきであったにもかかわらず、連絡せずに数日間徒過している。

他方、当法人の管理面では、以下の点に留意を要する。①貸与の必要性を個別具体的に十分に吟味していないのではないか。本件事案においては、本件端末を1ヶ月以上一度も利用した形跡がないのであり、そもそも貸与の必要性があったのか疑問。②過去にも、通勤途上での網棚放置、海外出張時の宿泊先での盗難被害があり、貸与端末の管理に関する「セキュリティ研修」や「管理マニュアル」において、「電車では網棚に乗せない」、「飲酒するときは持参しない」、「自室では鍵のある引き出し等に保管する」といった具体的な注意喚起が行われてきたか不明。③窃盗の可能性が高い本件事案の被害者は、形式的には であるが、実質的には当該モバイル端末を所有し、同端末を介して知り得る情報の管理者でもある当法人であり、当法人は、特に情報管理の重要性を踏まえて、盗難被害届を警察に提出し捜査させるべきではなかったか。

(2) 検討すべきと思われる再発防止策

ア 端末貸与の必要性を個別具体的に判断する、あるいは、貸与の条件を内規化する。

イ 貸与端末の管理に係る研修やマニュアルの内容を見直し、具体的で実効性のあるものにする。特に紛失等が発覚した場合は、自身で捜索するより先に情報セキュリティ管理者及び通信キャリア（ソフトバンク）に連絡し、証明書の無効化やリモートワイプを直ちに行ってもらうことを周知徹底する。

ウ 情報漏洩を最小化する技術につき、引き続き常時更新に努める。

エ 本件事案につき、速やかに内部統制委員会に付議し、その原因分析や再発防止策を当法人内で共有し、将来の過誤防止に資する。