（３）個人情報の盗難対策

本節では、個人情報が含まれる情報媒体や書類、またそれを保管するための設備・備品等に関して、盗難に遭遇しないために行われている効果的・効率的な取組について取り上げている。特に、個人情報が盗難に遭う原因として挙げられることが多い、“車上荒らし”に対する対応策についても取り上げている。

例えば、必ずしも“盗難対策”には限定しないものの、遠隔ロックが可能な携帯電話を導入したり（③、④）、二重の施錠を実施するなどして個人情報の盗難対策を徹底している事例（⑤）を紹介している他、事業所外にいる際の盗難（特に車上荒らし）対策として、営業用車両に個人情報保管用の専用ボックスを設置したり、盗難に遭いそうになった場合にアラームが鳴るようにしているような事例（⑥）も紹介している。

また、個人情報が含まれる書類やファイルを持ち歩くことそのものが盗難リスクを高めていると考え、コストは一定程度犠牲にしても持ち歩きをできるだけ回避している事例（⑧）も紹介している。

そして、個人情報を取り扱う者をできる限り限定することで、内部職員による持ち出し・盗難のリスクを業務に支障の無い範囲で低減するようにしている事例（⑩、⑪）も紹介している。

本節で紹介している取組事例

4-(3)-①：記憶媒体の情報が記録から一定時間経過後に自動消去
4-(3)-②：営業用車両に個人情報保管ボックスと盗難アラームを設置
4-(3)-③：携帯電話に遠隔ロックを導入
4-(3)-④：携帯電話は遠隔ロックが可能な機種を採用
4-(3)-⑤：個人情報の保管ロッカーの鍵を開けるための鍵を準備して二重の対応を実施
4-(3)-⑥：センシティブ情報を含む書類はジュラルミンケースで持ち運び、アラームを設置
4-(3)-⑦：建物の安全管理を徹底
4-(3)-⑧：持ち歩きリスクを回避するため、ダイレクトメールなどの収集・一括送付を停止
4-(3)-⑨：ICカードによるプリント出力認証、印刷ログ管理、業務内容に応じた複合機の利用制限を実施
4-(3)-⑩：個人データ取扱者を機能別に分離。システム処理による自動化を進め、個人データを持ち出すことのできない仕組みを構築
4-(3)-⑪：個人データ記憶媒体の持出しを防ぐため、担当者数を極少化して社員に限定し、作業エリアを限定し、アクセスログのチェックを頻度高く実施

4-⑶-①【記憶媒体の情報が記録から一定時間経過後に自動消去】

（製造業：約 300,000 人（グローバル））

・A 社では修理等の長期間外回りの業務を担当する社員が個人情報を持ち運ぶ事による紛失・盗難のリスクを回避するために、SD カードの個人情報（修理処理が未完了な顧客のデータ等）は一定時間を経過すると自動消去されるようになっている。

4-⑶-②【営業用車両に個人情報保管ボックスと盗難アラームを設置】

（製造業：約 300,000 人（グローバル））

・A 社では修理等の業務のために使用する社用車には、個人情報保管ボックスを社用車に登載し、盗難アラーム発生装置を設置している。

4-⑶-③【携帯電話に遠隔ロックを導入】（小売業（百貨店・スーパー）：約 10,000 人）

・F 社では外商担当者に対しては、遠隔ロック可能な携帯を導入している。

4-⑶-④【携帯電話は遠隔ロックが可能な機種を採用】

（その他サービス業（ダイレクトメール等）：約 600 人）

・Z 社では携帯電話は遠隔ロックが可能な機種を導入している。登録された電話番号から一定時間内に 3 回電話がかかるとダイヤルロックがかかる仕組みである。また、一段のセキュリティ強化も検討中である。

・見学者の訪問があった場合には、社内には携帯電話を持ち込ませず、ロッカーに預けるようにお願いしている。

4-⑶-⑤【個人情報の保管ロッカーの鍵を開けるための鍵を準備して二重の対応を実施】

（その他サービス業（債権回収支援）：約 30 人）

・γ社では個人情報の保管は部署ごと、業務ごとのロッカーで実施している。個々人に個人情報を保管させるのは望ましくないという考えからである。

・個人情報を保管しているロッカーの鍵は、鍵を保管するロッカーに入れて施錠されている。このことで、二重のチェックとしていると同時に、鍵を管理する専任の者を設定した場合に起こりえる“その者がいないと個人情報が取り扱えない”という状況を回避している。

4-⑶-⑥【センシティブ情報を含む書類はジュラルミンケースで持ち運び、アラームを設置】
（そのサービス業（高齢者等生活支援）：約 60 人）

・δ社ではサービス対象者宅で聞き取り調査した内容は聞き取り調査用紙に記載している。聞き取り調査用紙はジェラルミンケースに入れて持ち運ぶ。ジェラルミンケースは持ち運びをする者から 20m以上離れるとアラームが鳴るようになっている。また、常に 2 人 1 組で行動するようにしている。

4-⑶-⑦【建物の安全管理を徹底】
（そのサービス業（高齢者等生活支援）：約 60 人）

・δ社では単体ビルに移り、監視カメラをすべての部屋の入口に設置した。外部から玄関に人が来ると、コールセンターでアラームが鳴る。
・各従業者の担当業務によってセキュリティレベルが 5 段階あり、部屋によって入室できるレベルに制限がある。
・情報が入っている金庫は施錠管理しており、鍵は常に担当者が保持している。
・コールセンターは 24 時間体制であり、セキュリティ対策も最高レベルであるため、すべての情報はコールセンターのフロアで保管する。
・個人情報を扱うコールセンター内には、オペレータが常時 3～4 人いる。互いの目があるため、個人情報の聞き取り調査用紙を持ち出すことは容易ではない。
・コールセンター内で個人情報を扱うパソコンに USB メモリ、CD-R 等の記録媒体には記録できないようにするソフトをインストールしている。インターネット、社内 LAN にはつながっていないため別のパソコンへ送信することもできない。操作ログをとっており、不審なアクセスについてはチェック可能である。

4-⑶-⑧【持ち歩きリスクを回避するため、ダイレクトメールなどの収集・一括送付を停止】
（製造業：約 3,500 名）

・ア社では、とにかく、外に持ち歩くこと自体が大きなリスクと認識している。
・ダイレクトメールも、大量にまとめて発注するほうがコストを削減できることから、営業担当がいくつかの販売店舗を回ってまとめ、ある程度のロットになってから発送していたが、移送リスクがあるのでこのような対応はやめて、大量発注によるコスト削減を諦め、個別の販売店舗から発送するようにした。

4-⑶-⑨【IC カードによるプリント出力認証、印刷ログ管理、業務内容に応じた複合機の利用制限を実施】（製造業：約 12,000 人）

・シ社では IC カード(社員証)を、社内の入退室管理、PC へのログイン、プリント出力時の認証に適用している。
・この IC カードを活用し、業務内容に応じた複合機の利用機能制限、ログ管理を行って

いる。
・紙文書を PDF 化する際、全従業員の権限に応じた閲覧・印刷のアクセス権を付与して暗号化することで、共有文書の情報漏えい防止を図っている。

4-⑶-⑩【個人データ取扱者を機能別に分離。システム処理による自動化を進め、個人データを持ち出すことのできない仕組みを構築】

（その他サービス業（印刷・広告）：約 10,000 人）

・テ社では個人データを取り扱う業務を、設計・開発、出入力・保管、暗号化・複号、データ編集処理、というように機能別に分解し、機能毎に個人データを取り扱える従業員を限定したうえでルールをつくった。
・分業化と共に、システム処理による自動化を進め、容易に個人データを持ち出すことのできない仕組みを構築した。

4-⑶-⑪【個人データ記憶媒体の持出しを防ぐため、担当者数を極少化して社員に限定し、作業エリアを限定し、アクセスログのチェックを頻度高く実施】

（その他サービス業（印刷・広告）：約 10,000 人）

・テ社では個人データを記憶媒体に書き出すことのできる担当者数を極少化し、同社およびグループ会社社員に限定した。
・個人データ記憶媒体を取り扱うエリアを他のエリアと分離し、同エリア以外での書き出しは一切出来ない環境とした。
・個人データ記憶媒体の数量、書き出しログと納品記録の三つを毎日チェックすることで、不正書き出しがないか確認している。
・個人データを取り扱う職場からの個人データ記憶媒体の不正持ち出しを防止するため、警備員による金属探知器を用いた検査を常時実施している。
・ポケットのない作業着着用による記憶媒体等の持ち出し防止を図っている。
・なお、同社グループではグループ共通の IC カード社員証を採用し、同社員証を利用したセキュリティゲートシステムを各拠点に導入している。またプリンター・コピー複合機の利用時に IC カード社員証による認証を行い、自分が出力指示した文書のみ印刷可能とし、出力紙の放置などによる情報漏えいを防止する仕組みを自社で開発、自社製品の活用を進めている。