４．個人情報の適切な管理の場面

（１）個人情報の管理システム（物理的・技術的措置を中心に）

本節では、特に情報システムを中心とした技術的安全管理措置や、施設や設備、個人情報を含む書類等の事業所内及び事業所外における物理的安全管理措置に着目して事例を取り上げている。

例えば、情報システムに関しては、個人情報にアクセスできる端末そのものを可能な限り少なくしている事例（⑲）や、個人情報専用のネットワークを構築している事例（㉕）などを紹介している。その他、電子メールの送受信について問題がありそうな内容の場合は、自動的に送信停止を行うようなシステムを開発した事例（⑦）も紹介しており、さらに、個人情報を含むファイルを取り扱う作業については逐一管理者にメールで自動的に連絡が行くようなシステムを開発した事例（㉙、㉚）も紹介している。

また、物理的安全管理措置としては、取り扱う機密情報（個人情報を含む）の種類によって執務フロアの区画を分け、それぞれの区画におけるアクセス権限や使用可能機器を細かく規定している事例（⑭、㉖）や、外出の際には個人情報を紛失しにくい作りにした専用カバンの使用を義務付けたり（㉒）、事業所内においては個人情報の機密レベルに応じて色の着いたシールで分類管理を行って施錠管理している事例（⑪）など、日常的に使用する設備・備品等について工夫することで適切な管理を図っている事例なども紹介している。

本節で紹介している取組事例

4-(1)-①：個人情報の重要度にあわせた管理方策の分類
4-(1)-②：扱う個人情報セキュリティ水準に合わせて、機械的管理とソフトな管理を使い分ける
4-(1)-③：個人情報が記載された伝票類は施錠管理、特に顧客名簿は日々の枚数チェック等管理体制強化
4-(1)-④：外商担当者は個人情報をイニシャル等の形式で登録
4-(1)-⑤：物理的・技術的管理を徹底
4-(1)-⑥：生体認証で入退室を管理している
4-(1)-⑦：特定のキーワードを含む電子メールはサーバで送信を自動的に停止する
4-(1)-⑧：“三点セット”による入退室管理
4-(1)-⑨：バーコードによるトレーサビリティ確保
4-(1)-⑩：システム上の安全管理
4-(1)-⑪：情報の機密分類に応じてシールで色分け
4-(1)-⑫：私有パソコンの持ち込み禁止、社内使用パソコンの持ち出し禁止

4-(1)-⑬：センシティブ情報へのアクセスは物理的に厳しく管理
4-(1)-⑭：建物内における“セキュリティ区画”の設置
4-(1)-⑮：ファイル共有ソフト（Winny 等）対策の徹底
4-(1)-⑯：個人情報を集中管理するデータセンターにおいて特に厳重な管理を実施
4-(1)-⑰：ファイル共有ソフトは自己チェックとソフトで二重にチェックを行う
4-(1)-⑱：個人データを保管するサーバにアクセスできる端末は 1 校舎に 1 台のみ設置
4-(1)-⑲：センシティブな個人情報は紙媒体でのみ管理し、大量漏えいを防止している
4-(1)-⑳：データの授受は手渡し又はセキュリティ便を利用
4-(1)-㉑：キャビネットは開閉を記録者名を管理
4-(1)-㉒：専用金庫、専用カバンなどの使用により、物理的管理を徹底
4-(1)-㉓：社外携行時は氏名や住所を 2 つに分けることで、「個人の特定が容易でない形式」で保有
4-(1)-㉔：独自アプリケーションの開発により本社への報告迅速化、営業職員が個人情報を保有し続けるリスクの回避を実現
4-(1)-㉕：個人情報専用のネットワークを構築し、外部との接続を遮断
4-(1)-㉖：個人情報取扱エリアを特定し、業務を集中化
4-(1)-㉗：検針ターミナルから離れるとアラームが鳴り、置き忘れ・盗難を防ぐ
4-(1)-㉘：グループ会社店舗の端末からは外部媒体に書き込みができなくしている
4-(1)-㉙：データベースのアクセスログの定期点検を実施。時間外や休日のログに注目
4-(1)-㉚：個人情報を含むデータに関するアクションは全て個別に管理者に通知
4-(1)-㉛：退職者にも Winny 対策を徹底

4-⑴-①【個人情報の重要度にあわせた管理方策の分類】（製造業：約 334,000 人〔グローバル〕）

・A 社では個人情報を、「内部使用のみ」、「機密（コンフィデンシャル）」、「個人情報厳秘」、の 3 段階に分けて、それぞれについて管理基準を定めている。上記のそれぞれのレベルに合わせ、「保管方法」「アクセス権者」「持ち出し可否」「複製・複写可否」「配布・通信手段」「廃棄要否」「他社への開示に際する秘密保持契約の要否」などを規定している。

・個人情報の棚卸の際には、個人情報データベースを保有する部署に、目的・取得方法・取得者・管理者・件数などの情報を一覧表（インベントリー・リストと呼称）で提供させた。棚卸時に「活用しない」データを削除した。以後も各事業場で棚卸時に不要データを削除する取組みを継続している。

4-⑴-②【扱う個人情報セキュリティ水準に合わせて、機械的管理とソフトな管理を使い分ける】（卸売業：約 110 人）

・E 社では個人情報を取り扱う執務室については管理レベルを分けており、入室可能な者をそもそも相当程度絞り込んでいる。

・最もセキュリティが厳しく、入室可能者が限定されているのが、ガスの使用量やガス漏れ等をオンラインで集中管理しており、大量の個人データが蓄積されているシステムのある部屋であり、ID カードリーダーで入室管理を行っている。

・個人情報を特に扱うような部署については、入室時に必ず「入室理由」、「入室時間」、「面会者」、などについて記帳するようになっている。この記帳が面倒であるので、入室することなく用件を済ませる工夫（その部屋で執務している従業者を入口の内線電話で呼び出す形で話や用件を伝える等）をしている。

4-⑴-③【個人情報が記載された伝票類は施錠管理、特に顧客名簿は日々の枚数チェック等管理体制強化】

（小売業（百貨店・スーパー）：約 10,000 人）

・F 社では顧客名簿や各種伝票においては、保管方法・期間・最終処理方法等について基準を設け、管理を徹底。

・ 特に顧客名簿においては、チェックシートを活用し、日々の獲得枚数、廃棄枚数、ファイルごとの総枚数管理を徹底している。

・ また、顧客情報システムから出力される「顧客リスト」の運用（出力・配布・管理・回収）については、受渡時の枚数や回収予定日の確認、施錠管理などを徹底している。

4-⑴-④【外商担当者は個人情報をイニシャル等の形式で登録】

（小売業（百貨店・スーパー）：約 10,000 人）

・F 社では携帯電話には個人情報を登録しないことをルールとしている。外商担当者は、個人情報をイニシャルで登録するなど、個人情報と識別できない形で登録することになっている。また、ラインの中で誰がどの情報を持っているか登録することになっている。

4-(1)-⑤【物理的・技術的管理を徹底】（小売業（物販）：約 450 人）

・G 社では社用 PC には、規定により許可された以外のアプリケーションのインストールは禁止されており、情報システム部で監視できる体制となっている。

・アプリケーションの起動のログはすべて取っている。

・FD や USB メモリなど、外部メディアへの書き出しは一切できないようになっており、書き込もうとするとブロックがかかる。

・またそれ以外の外付け機器を接続しても同様である。

4-(1)-⑥【生体認証で入退室を管理している】（小売業（通販等）：約 520 人）

・H 社では監視カメラの設置、入館管理時の IC カードによる管理、及び記録メディアや携帯電話の持ち込みの禁止をしている。

・サーバ室など機密度の高い部屋は、入室権限を最小限の人数に抑え、さらに生体認証で入退管理室を実施している。また、コールセンターはセンシティブな情報が多いため、センター長の許可がなければ社長であっても入室できないシステムにしている。

・情報漏えい防止ソフトを導入し、暗号化をしている。

4-(1)-⑦【特定のキーワードを含む電子メールはサーバで送信を自動的に停止する】
（小売業（通販等）：約 520 人）

・H 社では電子メールの利用において、特定のキーワードが含まれるものはサーバで自動的に送信がストップされる仕組みを導入している。添付ファイルがあるものはすぐには送信できず、システムの担当者が中身をチェックして問題がなければ送信するようになっている。

4-(1)-⑧【“三点セット”による入退室管理】（信用業：約 3,700 人）

・I 社ではコールセンターや事務センターといった個人情報を取り扱うことの多い部署において、指紋認証、監視カメラ、個人私物ロッカーの“三点セット”を用いて、入退室管理を行っている。

4-(1)-⑨【バーコードによるトレーサビリティ確保】（信用業：約 3,700 人）

・I 社では個人情報を含む書類等の授受は、自社開発したシステムを活用して、バーコードによる追跡（トラッキング）ができるようにしている。これによってリアルタイムで書類等の所在が確認できる。

4-(1)-⑩【システム上の安全管理】（信用業：約 3,700 人）

・I 社では重要な情報が集中する「システムセンター」で、情報セキュリティの標準規格である「ISO27001（ISMS）」の認証を取得している、また、専管するチームを設置し、技術・設備・運用の各面から安全管理に努めている。

4-(1)-⑪【情報の機密分類に応じてシールで色分け】（信用業：100 人未満）

・K 社では情報を、極秘、機密、その他の３つに分類し、極秘情報は赤色シールを付けて、常時施錠されるキャビネットに保管している。機密情報は黄色シールを付けて、終業時にキャビネットを施錠して管理している。

4-(1)-⑫【私有パソコンの持ち込み禁止、社内使用パソコンの持ち出し禁止】
（情報サービス業：約 6,600 人）

・L 社では個人所有のパソコンをはじめとする私有情報機器の社内持ち込みを禁止している。

・社内使用パソコンは原則として社外持ち出し禁止としている。職種によりノート PC の社外持ち出しが必要な従業者は社内では専用の外部 HDD を用い、この外部 HDD は社外に持ち出しができない運用としている。このため、社外に持ち出したノート PC には機密情報が存在しない。業務上止むを得ず機密情報を持ち出す場合は暗号化を行う運用としている。

4-(1)-⑬【センシティブ情報へのアクセスは物理的に厳しく管理】
（情報サービス業（ソフトウェア）：約 400 人）

・N 社では個人情報保護マネジメントシステムの移行に合わせてリスクマネジメントを強化。情報のリスクランクに応じた安全管理を実施。

・入退室管理では、守衛による IC カードゲートと入館確認、事務所内に入るための IC カードゲートシステム、CPU ルームに入るための入室チェックの厳重な多重チェック体制を構築。

・ログインには登録者のみに付与されたログイン ID が必要である。

・重要な個人情報は、ネットワーク接続禁止で、独立したサーバで管理している。

・クレジットカード情報の取り扱いについては、汎用機で処理、アクセス権を設定し、

厳しい入退室管理とセキュリティ対策を実施。
・ファイル共有ソフト等 P2P ソフト対策のため、『一斉送信監視ソフト』により監視。また、『ライセンス違反検知ソフト』により、P2P ソフト等のインストールを監視。

4-⑴-⑭【建物内における“セキュリティ区画”の設置】

（情報サービス業：約 1,600 人）

・O 社では「情報へのアクセスコントロール」と「取扱いのトレーサビリティ（追跡性）」を目的として、執務エリア（システム開発室）をセキュリティレベル別に 4 段階のセキュリティ区画に分けている。

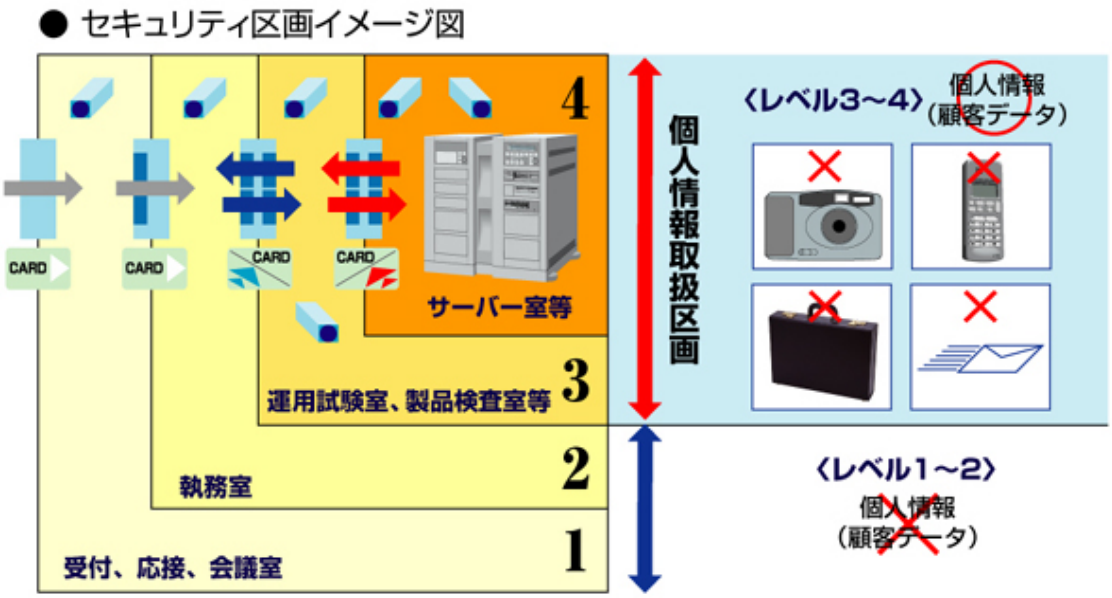
＜セキュリティ区画レベル４，３（個人情報取扱区画）＞

・セキュリティ区画レベル４はサーバ室等で顧客データ（個人情報）が保管されているエリアである。セキュリティ区画レベル３はシステム運用試験や製品検査を行うエリアであり、顧客データ（個人情報）を実際にハンドリングして運用テストなどを実施する。
・セキュリティ区画レベル４，３のエリアにのみ顧客データ（個人情報）の持ち込みが許されている。又は、その２つのエリアにおいては、カメラ、携帯電話の持ち込みが禁止されており、カバンの使用、及び電子メールの発信等も禁止されているなどそれぞれの設備対策が施されている。セキュリティ区画レベル４，３に設置された社内ネットワークがセキュリティ区画レベル２の執務室の社内ネットワークやインターネットと分離されているため電子メールの送受信やインターネット Web の閲覧はできず、顧客データ（個人情報）の漏えいや外部からの不正アクセスを防いでいる。
・セキュリティ区画レベル４，３では入室者が特定されており、入室作業者の作業状況を監視カメラで記録、入退室者の入退室記録が IC 入退室管理装置と監視カメラで行われている。
・顧客から送付された郵送物の中に、システムに関する問合せや確認のために、個人情報が記録された画面のハードコピー等が送付されている場合があるため、開封作業は同区画内で行っている。また、郵送でなく FAX で送付される場合もあるため、同区画内に設置した個人情報受信専用 FAX で受信している。

＜セキュリティ区画レベル２，１＞

・受付・応接・会議室がセキュリティ区画レベル 1、執務室（システム開発室）はセキュリティ区画レベル 2 とされており、顧客データ（個人情報）は存在してはいけないエリアとなっている。

図表　セキュリティ区画の構造



4-(1)-⑮【ファイル共有ソフト（Winny 等）対策の徹底】（情報サービス業：約 1,600 人）

・O 社では、社会問題となっている Winny 等による個人情報漏えい事故が、個人情報や業務情報を会社から自宅に持ち帰り私物のパソコンを使って作業をしていたために重要情報の漏えい事故が発生していることを踏まえ、社員情報、企業機密情報、業務情報などを許可無く持ち出すことを禁止した。もちろん、これらの情報を自宅へ持ち帰って自宅で作業をすることも禁止している。

・社内においても私物のパソコンや私物のＵＳＢ等の外部媒体を持ち込んで作業をすることを禁止している。この方法もファイル共有ソフトによる漏えい防止対策の一環としている。

・社内 LAN に接続されている全国の事業所すべてのパソコンについて、インストールされているプログラムや作成されているファイルを検索するツールが備わっている。このツールによりファイル共有ソフトの存在確認を定期的に行っている。

・毎年、従業者の自宅の私物パソコンについて点検し報告させているが、昨今の漏えい事故件数増加を背景として平成 20 年度から点検を 2 回（半期毎）に増やした。

4-(1)-⑯【個人情報を集中管理するデータセンターにおいて特に厳重な管理を実施】（複合（情報システム／製造）：約 500 人）

・R 社では重要情報はすべて、データセンターを持つ事業所で厳重管理している。他拠点の情報のバックアップも当該事業所で管理しており、施錠管理、入退出管理（カード）、監視カメラ、暗証番号と指紋認証によって厳しい管理がなされている。特に重要度の高い情報が管理されているサーバルームへの入室には指紋認証、パスワード入力、IC

カードの 3 種類の認証が採用されており、入室は一人ずつしかできない。
・パスワードは月に 1 度変更を義務付けている。

4-(1)-⑰【ファイル共有ソフトは自己チェックとソフトで二重にチェックを行う】
（複合（情報システム／製造）：約 500 人）
・R 社では、従業者が各自のパソコンにファイル共有ソフトが入っていないかどうかを自己チェックし、申告した。その後ウイルスチェックソフトでファイル共有ソフトの有無をチェックした。チェックは毎月実施している。

4-(1)-⑱【個人データを保管するサーバにアクセスできる端末は 1 校舎に 1 台のみ設置】
（その他サービス業（教育、学習支援）：約 190 人）
・T 社では個人データを本社のサーバに集約しており、当該サーバにアクセスできる端末は校舎に 1 台のみ設置している。以前は従業者全員が自分の端末内に情報を持っていたが、それを一度すべて消去して上記の仕組みを導入した。
・中央管理しているサーバについては、アクセスログが残り、どの端末からアクセスがあったかがわかるようになっている。

4-(1)-⑲【センシティブな個人情報は紙媒体でのみ管理し、大量漏えいを防止している】
（その他サービス業（エステティックサロン）：非公開）
・W 社では店舗において、利用者の個人情報をすべて紙媒体で管理している。店舗ごとに鍵のかかるロッカーに保管し、ロッカーは帰宅時に施錠している。サロン責任者が施錠の責任者となり、紙情報は、サロン責任者の指示がなければ持ち出せない規則となっている。

4-(1)-⑳【データの授受は手渡し又はセキュリティ便を利用】
（その他サービス業（印刷・広告）：約 11,000 人）
・X 社では外部とのデータの授受において、手渡し又はセキュリティ便を利用している。
・工場間など社内でのデータの授受では、鍵つきジュラルミンケースで運ぶ個人情報専用便を利用している。
・データのやり取りは専用伝票で記録しており、受け取りから返却又は破棄までが管理できるようになっている。

4-(1)-㉑【キャビネットは開閉を記録者名を管理】
（その他サービス業（印刷・広告）：約 110 人）
・Y 社では共有のキャビネットはいつ誰が開けて何を取り出したかを紙で記録するようにしている。スペアキーを持っている者をリスト化している。

4-(1)-㉒【専用金庫、専用カバンなどの使用により、物理的管理を徹底】

（その他サービス業（債権回収支援）：約 30 人）

・γ社では契約社員については個人情報を保管する場合には、指定された特殊な専用金庫を使用することを義務付けた。

・外回り時には専用のカバンを使用することを義務付け、そのカバンは必ずチェーンで自分とつなぐようにしている。とにかくカバンを肌身離さないことを徹底するために実施しており、車の運転中でもチェーンが問題ないように、助手席にカバンを置いた場合の距離やチェーンの具合なども確かめ、金具店に特注して作成してもらったものである。

・専用カバンについては、使いやすく、出し入れの途中で紙やデータが外に落ちにくいもの、ということで既製品を選んで指定している。

4-(1)-㉓【社外携行時は氏名や住所を 2 つに分けることで、「個人の特定が容易でない形式」で保有】（その他サービス業（債権回収支援）：約 30 人）

・γ社では社外に個人情報を携行する必要がある場合は、紙媒体の場合でも、データの場合でも、個人情報は 2 つ（2 枚の紙、2 つのファイル）に「氏と名」「住所の前半と後半」のように分けて管理しており、万が一、片方が紛失しても個人を特定できないようにしている。

・2 つのデータの照合は個人ごとの番号で実施している。

4-(1)-㉔【独自アプリケーションの開発により本社への報告迅速化、営業職員が個人情報を保有し続けるリスクの回避を実現】

（その他サービス業（債権回収支援）：約 30 人）

・γ社では営業の契約社員等が債務者等を訪問した際の対応等について迅速に本社に報告し、また契約社員等がデータの形で個人情報を保有し続けることによるリスクを回避するために、携帯端末を使用して本社のサーバに直接的に情報を送信できるアプリケーションを開発した。

・このアプリケーションを使用すれば、携帯端末で個人情報を呼び出すことができ、その個人に対して行った対応等を携帯端末で書き込み、本社サーバに送信すれば一切の情報が携帯端末には残らないようにできるというものである。

・紙ベースでの個人情報の取扱いはどうしても紛失リスクが大きいため、一定のコストを要してアプリケーションを開発した。

・不正アクセスを防止するため、通信回線は IP-VPN（閉域網）を使用し、暗号化と併用することでセキュリティを確保している。

4-(1)-㉕【個人情報専用のネットワークを構築し、外部との接続を遮断】

（その他サービス業（債権回収支援）：約 30 人）

・γ社では社内での電子データでの個人データの取扱いにおいては、インターネット等外部環境との接続を遮断している。

・専用サーバ、クライアントパソコンは管理ソフトを導入し、物理的なコピーや記録媒体による持ち出しができないように制限をかけている。

4-(1)-㉖【個人情報取扱エリアを特定し、業務を集中化】

（その他サービス業(印刷・広告：11,000 人)）

・X 社では、全国にある個人情報を取り扱う業務を、それぞれの事業所のセキュリティエリアに集中させている。同エリアでは、他のエリアと物理的に切り分け、作業者を特定・極少化し、許可された者以外の入退管理を厳密に行っている。

・作業はセキュリティエリア内のみで行うことにしており、作業中に想定し得るケアレスミスに対し、事故発生につながらないような工程ルールの適正化・標準化・教育・運用（記録・点検・監査）の徹底を行っている。

4-(1)-㉗【検針ターミナルから離れるとアラームが鳴り、置き忘れ・盗難を防ぐ】

（電気・ガス・水道業：約 1,000 名）

・イ社では、検針のハンディターミナルについては ID とパスワードを入力しないと起動できないようになっている。

・機器紛失の危険を回避するために、担当検針員が検針ターミナルから 2、3 メートル以上離れるとアラームが鳴るようになっている。

4-(1)-㉘【グループ会社店舗の端末からは外部媒体に書き込みができなくしている】

（電気・ガス・水道業：約 1,000 名）

・イ社では、サービスショップの端末に関しては、別媒体へ情報が保存できないように設定している。社内の端末に関しても制限を設けている。

・オフィスのセキュリティ管理の強化に取り組んでおり、建物によっては RFID カードによる入退室管理を行っているところもある。

4-(1)-㉙【データベースのアクセスログの定期点検を実施。時間外や休日のログに注目】

（小売業(通販等):約 1,800 名）

・オ社では、データベースのアクセスログを取得し、定期的（少なくとも 3 ヶ月に 1 度）に点検している。時間外、休日等のアクセス状況に着目している。

・PC の操作ログも取得している。セキュリティポリシーを設定し、ポリシーに抵触する

操作が発生した場合、通知が電子メールで事務局、内部監査担当、システム担当に送付される。公開はしていないが、監視基準が定められており、不正操作と判断された場合、監視責任者より警告が発信される体制になっている。

4-(1)-㊿【個人情報を含むデータに関するアクションは全て個別に管理者に通知】

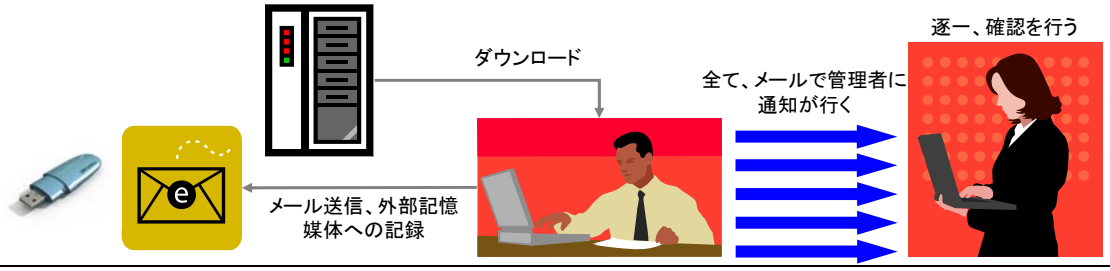
（信用業：約 2,000 名）

・カ社では、個人別に権限が決まっており、業務に関係する情報のみダウンロード権限がある。ダウンロード権限がある人の場合には、ダウンロードの際に毎回上長へ通知され、ダウンロードされた情報と同じものが上長へも送信される。また、いつどのような情報をダウンロードしたかを示すリストが作成され、それを上長がチェックする。

・また、個人情報を電子メールで送信したり、外部記憶装置に移す場合には暗号化をすることが定められており、個人情報を暗号化する際に、どのような個人情報を暗号化したのかということについて上長に電子メールで連絡がいくようになっている。

・電子メールの本文や添付ファイルに個人情報が含まれるかどうかをチェックするシステムをつくり、個人情報が含まれるものを送信すると上長や個人情報管理責任者にメールが送信される。その際、暗号化しているかどうか上長が確認する。

図表　個人情報を含むアクションの管理者への通知（イメージ）



4-(1)-㊿【退職者にも Winny 対策を徹底】

（情報サービス業(アウトソーシング等)：約 2,700 人）

・キ社では、Winny などのファイル共有ソフトは、使用禁止。

・全従業者に対して、過去に持ち帰ったファイル等を削除することを指示し、本人の署名つきの確認書を取っている。

・退職者に対しては、過去 3 年間にさかのぼり、ファイル等を削除したことをチェックすることを依頼する文書を郵送し、やはり本人の署名つきの確認書を返送してもらっている。