Ⅲ．中小企業における効果的な取組

Ⅲ．中小企業における効果的な取組

ここでは、Ⅱ章で紹介した事業者の効果的・効率的な取組のうち、特に中小規模の事業者でも比較的取組みやすい事例を取り上げている。

個人情報保護に関連する対策としては、情報システムの構築や備品・機器等（暗号化ソフト、専用端末、個人情報保護対応のノートPC、携帯電話等）の購入など、コストをある程度かければ対応の質を高めることができる場合も多い。

しかし、個人情報保護対策そのものは事業者としての責務であり、信用力向上や顧客に対する安心感の醸成には大きく寄与するものの、対策を行うこと自体が必ずしも事業者の売上や利益の維持・増加に直接的につながるものではない。したがって、事業者としては個人情報保護対策のためにコストを無制限で投入することはできないし、特に資金力、人員数等で必ずしも余裕のある事業者ばかりでない中規模企業、小規模企業にとっては、少ないコストで既存の設備・人員等を利用して対策を実施することが有益である。

このような考え方から、本章では特にコストをあまりかけずに実施している対策について、個人情報のライフサイクルに沿って取り上げ、再整理を行っている。

なお、本節で記載している事例の番号は、「Ⅱ．個人情報保護対策の場面ごとの取組事例」において整理されている番号であり、“効果的な事例”でとりあげた事例以外でも事業者の取組事例を知りたい場合には、第Ⅱ章の関連する節の事例も参照することができる。

（1）個人情報保護対策の準備（規程づくり・体制づくりの場面）

ア）新たな組織の構築や人員配置を行うことなく対応した事例

1-②【既存の委員会に個人情報保護の役割を付託することで違和感無く体制を構築】（電気・ガス・水道業：約 60 人）

・C 社では、既存で常設の IT 委員会の活動内容に個人情報保護に関する活動を付加し、個人情報に関するデータのサーバへの移管や、個人パソコンの定期的なチェックを行っている。IT 委員会は各部の情報機器、ネットワークなど IT に詳しい人によって構成されている。

・車輌委員会が車内に情報を置き去りにしていないかをチェックする。この委員会は、もともとは交通事故防止のための委員会だが、個人情報保護の視点を取り入れて活動を展開している。

・もともとあった組織に役割分担をして取組を進めることで、従業者にとって抵抗感が少なかったと考えている。

イ）1 つの役職を 2 人で担当することで少人数でも相互牽制機能を発揮した事例

1-④【タスキがけ人事による効率的な管理体制】（信用業：100 人未満）

・K 社では、各役職に責任者と代行者を設置することとし、1 人で複数の業務の責任者を兼任することの無いよう、タスキがけ人事としている。例えば、個人情報管理において、A 氏が責任者で、B 氏が代行者である場合、情報セキュリティ管理では、B 氏が責任者で、A 氏を代行者としている。タスキがけ人事をすることで、少ない人数で複数の業務をこなしつつ、牽制できる態勢としている。

ウ）外部の力を少ないコストで最大限に活用した事例

1-⑤【規程類は社内で整備し、外部の専門業者のチェックを受ける】（信用業：100 人未満）

・K 社では、経費抑制のため、種々の規程類は自主ルールやガイドライン等を参照しながら社内で作成した後、外部の専門業者による個人情報保護に関する診断を受けている。

エ）外部の力を活用しつつもコストは最小限の活用にとどめ、時間を節約しながら規程を作成した事例

1-⑨【勉強会と規程作成を同時進行で実施。優先テーマから先に担当者を決めて規程作成】（その他サービス業(教育・学習支援)：約 180 人）

・ケ社では、単なる勉強会で終わってしまっては、参加者だけが理解して終わってしまうので意義が薄く、その後仕切りなおして規程等を作り始めると対応に時間がかかってしまうと考えた。そこで、毎回勉強会のテーマを決めて開催し、その中で勉強した

ことについてすぐに規程や関連資料を作成するようにした。そのことで勉強に身が入ったし、時間を効率的に使用できた。
・必ずしも専任の担当者がいなかったこと、個人情報保護にはさまざまな分野やテーマが存在していたことから、テーマや対策内容別に重要・緊急マップを策定して、重要度と緊急度で色分けを行い、特に緊急性と重要性が高い対策について、それぞれに担当を決めて規程作成や準備などを行った。誰がいつまでに策定するのか、ということを明確にすることが効率化と確実な規程類の整備につながった。

オ）委員会のメンバーにセキュリティ改善点 10 個を考えてくることを宿題として課す事で、様々な視点からの問題点を効率的に抽出した事例

1-⑮【セキュリティ委員会のメンバーに、セキュリティ改善点を 10 個以上見つけてくることを宿題化】
（情報サービス業（アウトソーシング等）：約 30 人）
・タ社では各自がセキュリティ委員会において、10 個以上セキュリティ改善点を考えてくることを宿題にし、委員会を実施した。
・メンバーに改善案まで考えさせると躊躇してしまうと考え、宿題をセキュリティ改善点の洗い出しにとどめた。
・セキュリティ改善点への対応は、委員会メンバーから主担当と、期限を決めて実施し、2 週間後に進捗の報告を実施している。進捗はエクセルシートで管理している。

（2）個人情報の取得の場面

ア）社内では安価な手書きの「授受リスト」により個人情報の所在を明確化した事例

2-⑧【委託元との授受リストに加え、社内でも授受リストに記録し、所在の明確化を実施】
（その他サービス業（債権回収支援）：約 30 人）
・ヶ社では保有する個人情報は委託元から預かるものが主である。
・委託元から個人情報を受領する際には授受リストを作成しており、授受に際して両者の氏名記入・捺印を行う。
・郵送で個人情報を授受する場合にも、配達記録郵便を利用しており、個人情報に加えて授受リストを作成して送付する（授受リストの送付を FAX で代用する場合もある）。
・委託元企業によって、毎日授受する場合もあれば、1 週間単位で授受する場合もある。
・すべての郵便物について授受記録をつけている。
・個人情報の場合は、顧客から授受したタイミングで授受リストを作成するのとは別に、社内の個別の担当者に渡す場合にも授受リストを作成して確認している。

（3）個人情報の利用（第三者提供含む）の場面

―

（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）

ア）セキュリティ区画への入室手続きを面倒にすることで職員の出入りを最小化した事例

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】（卸売業：約 170 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。

イ）携帯電話への個人情報の記録については特定が容易でない形式で実施した事例

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】
（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。

ウ）個人情報にアクセスできる端末そのものの数を削減した事例

4-(1)-⑲【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。

エ）ファイルをわずかに編集するだけで個人情報の特定が容易でない状態にした事例

4-(1)-㉔【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。

②従業者等への教育方法

ア）期間の設定、イエローカードなどのキャンペーン的な取組みで注意喚起する事例

4-⑵-⑯【個人情報保護週間の設定】（情報サービス業：約 1,600 人）

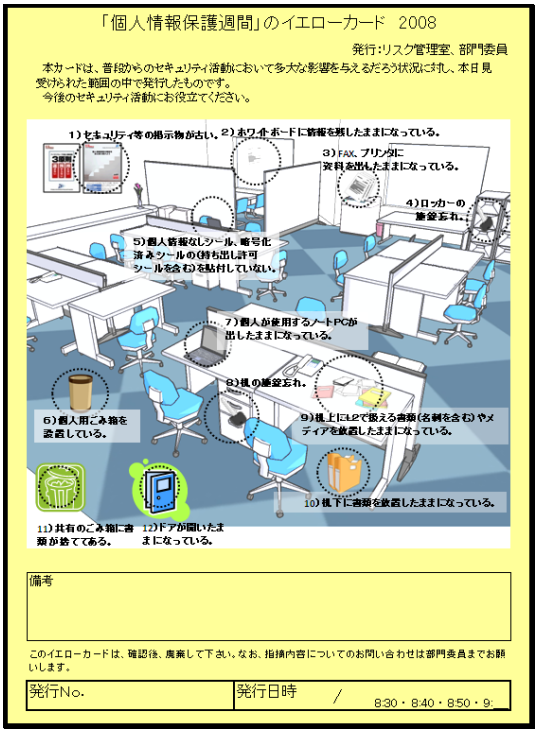
・O 社では年に 1 度、2 週間の『個人情報保護週間』を設定し、セキュリティ意識を高めている。「手書きによる情報セキュリティ宣言書の提出」「自己点検」「部門間の相互点検」「スローガン募集」「啓発ポスター募集」「個人情報検索ツール募集」「セキュリティ職場点検」などを実施している。

・個人情報保護週間の最終日には、「情報セキュリティ向上会議及びリスク管理統括委員会全体会議」を開催して個人情報保護週間の総括会議を開催している。また、この会議に出席できなかった従業者に対しては、全国の事業所で別途地区会議を開催して必ず会議の内容が全従業者に行き渡るようにしている。

・地区会議では、「部門間の相互点検」「個人情報保護ミーティング」を行い個人情報保護およびセキュリティ教育・啓発活動を行っている。

・職場点検の方法として、「イエローカード」を作成した。個人情報保護週間に、同カード記載の 10 項目について各事業所で従業者の机回りを確認して問題があれば、カードのチェック内容に赤丸をつけて従業者の席に置く。個人情報の取扱い違反が発見された場合には、レッドカードを発行している。目的は、注意喚起だけでなく、従業者がセキュリティ対策に参加している意識を持ってもらうことにもある。

図表　セキュリティ職場点検（イエローカード）



イ）アナウンスメントだけで職員の意識の引き締めを実現した事例

4-⑵-㉕【管理を極めて厳格に行っていることを明確にアナウンスすることで緊張感を醸成】（その他サービス業（冠婚葬祭）：約 200 人）

・U 社ではログの管理（どのファイルをコピーしたのか、どのホームページを閲覧したのかということ等）を行っていること、日常的に事務所を回りながらチェックを行っていることについては広く従業者に公表している。従業者はいつも見られている、チェックされている、という認識を持っているようであり、「常に見ている」という姿勢を広く公表することで効果的な従業者教育になっている。

ウ）実際に発生した・発生し得る具体的な事例を用いた教育で効果を高める事例

4-⑵-㊲【実践に近い事例や投げかけ形式の質問を用いた教育を実施】
（小売業(通販等):約 1,800 人）

・オ社では、個人情報に関するテキストを配布している。グループ内でも企業によって事例が異なるので、実践に近いケーススタディを行い、現場で議論してもらう。例えば「クリーニング店が製品をだめにしてしまい、クリーニング店から自社に顧客の購入履歴の問い合わせがあった場合どうすればよいですか」など、実践的な事例を用いて教育をしている。

・加えて、実際に取り扱いのある個人情報（および個人情報と思われるような情報）を引き合いに出し、「この情報は個人情報に該当するか」、など投げかけ形式で従業者に考えさせるような電子メールを送付し、教育している。

・啓発のため、漏えい事故の事例を全社全員にメールで配信している。

エ）現場の実務担当者がそれぞれの現場のテスト問題を作成することで、テスト問題作成のための人員を割くことを回避して効率的に実施し、現場で実際の業務内容に沿った問題を作成している事例

4-⑵-㊳【テスト問題作成は各部署の実務に合わせて現場対象者が作成】
（その他サービス業(教育・学習支援)：約 180 人）

・ケ社では、テストの問題としては、部署ごとに保有している個人情報の性格が異なるので、部署ごとに作成した問題も実施している。

・部署ごとに作問者を任命し、作問者が新入社員向けのテストを作成する行為そのものも作問者に対する教育とした。

・個人情報保護対策を行う事務局から依頼すると、依存体質ができてしまうので、各部署に設問を作成させ、当事者意識を持ってもらうことを目的とした。残存リスクの洗い出しについても各部署で議論させ、この議論に個人情報保護対策を行う事務局から 1 名ずつ入り、必要に応じて指導をしながら作らせている。

・合計 100 問作成した。50 問を部署別編とし、50 問を全体編とした。実際のテストはそのうちから合計 50 問出題（部署別偏 25 問、全体偏 25 問の構成）し、44 点以上取らないと不合格とした。不合格の場合は何度も合格するまでテストを受験させた。

オ）“ファイルにパスワードをかける”などについて実技試験を実施し、知識だけに留まらない実践的な教育を実現している事例（少人数企業の方が実施しやすい）

4-(2)-㉞【CBTに加え、パスワードが実際にかけられるか、などの実技試験も実施】
（その他サービス業(教育・学習支援)：約 180 人）

・ケ社では、CBT（Computer Based Test）だけではなく、実技テストも実施した。具体的には、例えばネットワーク上のファイルにパスワードをかけるということを実際に実施してもらい、できているかどうかを確認した。頭でわかっていても、リテラシとして実施できない場合などがあることに配慮して実施したものである。

カ）管理職の実習結果を非管理職が後から参照することで、その意識を把握している事例

4-(2)-㉟【管理職と非管理職の実習期間を一週間ずらして実施】（製造業：約 26,000 人）

・サ社では e ラーニングでは管理職が先に受講し、1 週間後に非管理職が受講するようにして、開始時期をずらしている。非管理職の受講時に、先に受講した管理職の回答の一部が表示されることとなっており、自身の回答と比較することができるようになっている。また、非管理職同士でも、相互に回答を公開し、比較することができるようになっている。

キ）従業員からのスローガン募集、啓発ポスターの頻繁な取替えにより、継続的に意識喚起を実施している事例

4-(2)-㊱【啓発のためのポスターの定期的変更、従業員からの募集したスローガンを掲載するなどして、継続的に従業員の意識喚起を実施】
（情報サービス業(ソフトウェア)：約 5,500 人）

・セ社ではポスターも定期的に変えており、啓発している。同じポスターをずっと掲示していても皆飽きてしまい、見なくなったり、意識が薄れたりしがちなので、ポスターを頻繁に変えることで注意喚起を行っている。ポスターに記載されるスローガンも社員に対して募集して選定・掲載しており、社員も参加意識を感じられるようになっている。

③個人情報の盗難対策

ア）鍵を二重にすることで担当者を置かずにチェックを実現している事例

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ノートPCの安全対策

ア）誰にでも分かるシールの貼付で全員が監視できる状況を実現した事例

4-⑷-②【持ち出し禁止シールを貼って対応】

（複合（情報システム／製造）：約 500 人）

・R 社ではハードを暗号化しているパソコンには「持ち出し OK」シールを、そうでないものには「持ち出し禁止」シールを貼付し、注意を喚起している。

・800 台あるノート PC のうち 300 台が持ち出し可能である。これらは HDD の暗号化、BIOS ロック、OS、システムで 4 つの ID、パスワードが必要となっている。4 つの ID、パスワードは月に 1 度変更を求めている。パスワードを紙などに記載することは禁止されている。

⑤外部委託先の管理方法

ア）外部委託先も含めた合同勉強会の開催等で底上げを図っている事例

4-⑸-①【委託先を集めての合同勉強会開催により委託先との意識を共有し、さらに定期的監査及び是正後のフォローアップ監査を実施】

（小売業（通販等）：約 520 人）

・H 社では年 3~4 回、委託先を中心として、毎回約 40 社から 70～80 人程が参加する「個人情報保護対策合同会議」を行っている。参加者の多くは個人情報保護責任者であり、各社の取組についての意見交換やヒューマンエラーに関する事故事例の検証を行い、安全対策議論を共有している。

・委託先グループごと（業種ごと）ディスカッションを行い実情に沿った議論になるようにしている。また議事録を参加企業へ必ずフィードバックしていることで、危機意識を高める効果がある。

・外部委託先の情報取扱い管理の検証のため、現地へ赴き「外部監査」を年１～２回実施し、実態を把握し不備や是正を指摘・指導し、是正後のフォローアップ監査も行っている。

イ）点検の際に関係者に同道してもらい、外部の目でのチェックを実現しながら、自社の取組みについてもわかりやすく伝えている事例

4-⑸-⑫【内部点検の際に委託先職員に同道してもらい、自社のチェックの厳しさを伝える】

（その他サービス業(教育・学習支援)：約 180 人）

・ケ社では、内部点検の際に、委託先企業の職員を同道している。自分たちがどれほどキッチリしているかということを見せることで、要求される水準を示すことができ、暗に個人情報保護に関する努力を促すことができていると考えている。

⑥規程の遵守状況等の日常的点検・確認の方法

ア）点検シートの作成と定期的なチェックといった負担の少ない方法で、書類等の紛失ミスを少なくしている事例

4-⑹-⑭【管理体制チェックシートの定期実施でミスの削減を実現】

（小売業(百貨店・スーパー)：約 10,000 人）

・エ社では、事故の発生の原因が郵送時の誤送付、封入ミス、伝票の持ち運び中の紛失などである場合が多かったため、チェックシートを事務局が作成し各部門の部長代理クラスに毎月チェックしてもらうようにしている。

・長期間にわたり実施したことにより、個人情報の紛失や漏えいが大幅に減少した。

図表　個人情報管理体制緊急チェックシート

2008部・Div別 個人情報保護管理体制 月別チェックシート

（提出日）
部
検査責任者

チェック内容

必須項目	1	個人情報が無くなれば判る状態か	各職場、ショップ等の個人情報が無くなればすぐ判るよう整理整頓とナンバリング、区分け等出来ていること。
	2	個人情報の受渡し確認と記録はあるか	個人情報の受渡しの際、確認し記録をしているか。(必ずしも授受簿作成が目的ではない)
選択項目	1	個人情報のＦＡＸは厳禁	個人情報のFAX送信は厳禁です。　※顧客の強い要望や業務上必要な場合は、上司の確認を得、相互確認の上送信する。
	2	送付時の相互確認	個人情報を郵送等する際、第三者が宛名等のチェックを行い、封筒の裏に担当者と第三者が押印したうえで郵送する。
	3	移送時のクリアケース使用	個人情報を記載した伝票を館内で移送する際、必ずクリアケースに入れて持ち運ぶ。また、原則、他業務と兼務しない。
	4	並行作業時のバインダー使用	売場のカウンター等で、並行して作業する場合、伝票等が紛失しないようにバインダーに挟んで作業する
	5	個人情報を区別する赤いクリアホルダー使用	個人情報が個人情報以外の書類と区別するため赤いクリアホルダーを使用する(赤いクリアホルダーは10枚単位で用度にて物品購入のこと)
検査責任者必須		個人情報保護活動報告書記入	毎月「個人情報活動報告書」に実施記録を必ず記入すること。

チェック実施月	3月						4月						5月					
	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
課・Div・担当名 ＼ チェック内容	無くなれば直ぐ判る状態か	個人情報の受渡し確認と記録はあるか					無くなれば直ぐ判る状態か	個人情報の受渡し確認と記録はあるか					無くなれば直ぐ判る状態か	個人情報の受渡し確認と記録はあるか				
①																		
②																		
③																		
④																		
⑤																		
⑥																		
⑦																		
⑧																		
※　検査責任者必須項目																		

チェック実施月	6月						7月						8月					
	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
課・Div・担当名 ＼ チェック内容	無くなれば直ぐ判る状態か	個人情報の受渡し確認と記録はあるか					無くなれば直ぐ判る状態か	個人情報の受渡し確認と記録はあるか					無くなれば直ぐ判る状態か	個人情報の受渡し確認と記録はあるか				
①																		
②																		
③																		
④																		
⑤																		
⑥																		
⑦																		
⑧																		
※　検査責任者必須項目																		

チェック基準
○　全てルール通り行われており、全く問題ない
×　期間中にルール違反があった
△　ルールを知らない者がいたが、指導でルールを守らせた
ー　該当する業務が無い

＊毎月のチェック結果を、翌月初(5日迄)に法務担当までメールで送付して下さい。

イ）外部への書類持ち出しを全て禁止した上で、警備会社に社屋の出入り口での持ち物検査を委託し、効率的に検査を実施している事例

4-⑹-⑱【荷物検査をグループ会社の警備員が社屋出入り口で実施。全ての書類を原則持ち出し禁止とすることで警備員でも判断可能とした】
（情報サービス業(ソフトウェア)：約 5,500 人）

- セ社では荷物検査も抜き打ちで実施している。不定期でしかも抜き打ち実施している。実際のチェックは警備員が実施する。警備員もグループ会社の人間であるので、依頼しやすく、チェックの方法なども指示しやすい。もし、持ち出し禁止の書類などが見つかった場合には、始末書を書くことになる。
- 会社の書類は全て機密である、ということにしているので、「この書類は持ち出してよいか、悪いか」、という判断が発生することがない。したがって、（必ずしも機密情報や個人情報に詳しくない）警備員の人であっても判断は求められない。

ウ）自己点検を基礎としながら、取扱責任者が定期的に自己点検結果をチェックすることで、実効性を担保している事例

4-⑹-⑲【職員個々人が自己診断を実施し、取扱責任者が定期的にチェックする目標管理的な運用で自己点検の実効性を確保】（サービス業（警備）：約 13,000 人）

- ト社では自己診断書をツールとして準備している。個人情報保護管理者が自分の担当

する事業所の状況について定期的（半期に一回程度）にチェックを行い、本社に報告するようにしている。
・個人については、年に 2 回は個人情報保護に関する「自己診断」をさせている。年に 2 回、時期を指定して（GW 前、年末・年始直前など）実施している。
・自己診断後、取扱管理者が見てチェックをすることになっており、その際に、問題があれば取扱責任者が指導を行ったり、できていないにも関わらず「できている」としていることなどについては指摘をするように、目標管理制度的に運用することで、単なる書類としての「自己診断」に留まらないようにしている。

⑦初歩的ミスの防止策

ア）そもそもメールアドレスのアカウントを減らすことで問題の原因を削減した事例

4-⑺-⑩【電子メールアドレスは必要な従業者のみに付与】
（その他サービス業（教育、学習支援）：約 190 人）
・T 社では従業者と常勤職員に対して電子メールアドレスを 1 人ずつ付与するのをやめ、必要な従業者（総務、教室長など）にのみ電子メールアドレスを付与している。
・内部でのやりとりは、市販の社内グループウェアの社内電子メールを使用し、外部への誤送信は起こりえない状況にしている。
・どうしても電子メールアドレスが必要な者に対しては、事情を聞いた上で判断し付与している。
・FAX は短縮ダイヤルを導入している。

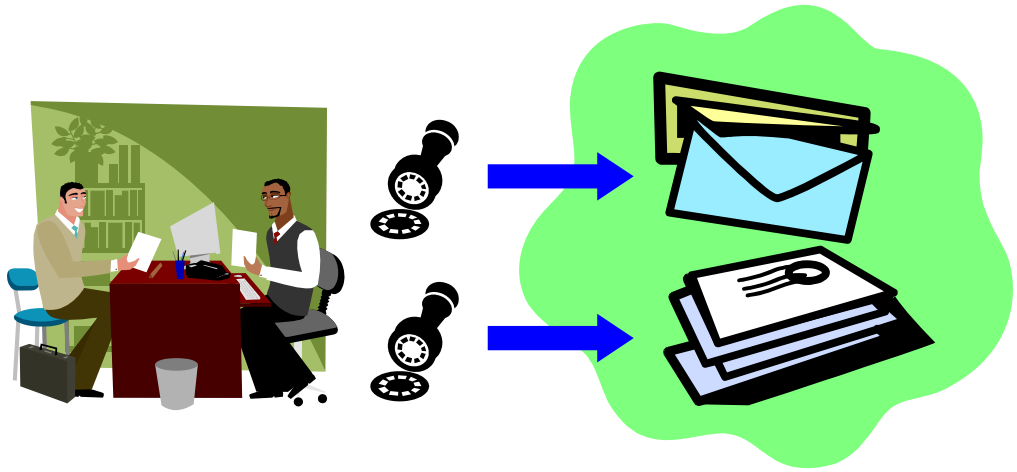
イ）2 名が目視で確認し、責任を持たせるために押印することでミスを軽減している事例

4-(7)-⑬【封入時に 2 名が確認・押印することでミスを軽減】

（小売業(百貨店・スーパー)：約 10,000 人）

・エ社では、郵送物の封入のダブルチェックをしている。封入前に 2 人で確認し、封入時にも 2 回以上確認するようにしている。封入の袋にあらかじめ印鑑を押す場所を 2 つ印刷しており、必ず 2 名が押印するようにしている。

図表　封入のダブルチェック（イメージ）



ウ）酒席同席者にも、一部連帯責任を負わせることで、酒席における個人情報の漏えい等の防止に実効力を持たせている事例

4-(7)-⑱【酒席での漏えい事故発生時には同席者も一部連帯責任を負う】

（情報サービス業(ソフトウェア)：約 5,500 人）

・セ社では酒席にノートパソコン、個人情報を持ち込む事は禁止されている。実際に飲酒が原因で漏えい事故等が発生した場合には、酒席に参加していた者で、実際に漏えいに繋がるような行動をした者、及び管理責任者は連帯責任として処罰される。

（5）個人情報の消去・破棄の場面

ア）コスト、信用の双方から考えて消去・破棄を全て自前で実施している事例

5-①【外注は行わずに、公的な焼却場等に自社で持ち込み、投げ込みも自社で実施】
（卸売業：約 170 人）

・E 社ではシュレッダーをすると紙が相当かさばるし、溶解を委託しても、溶解業者がどこまで信用できるかという問題が残る。

・そこで、同社では、一定の期間は個人情報を含む紙等は施錠できる場所に格納しておき、定期的に集めて自社で公的な処分場等まで持ち込んで処分している。実際に焼却炉等に投げ込むところまで自社の従業者が行っている。

イ）3 枚複写式の預かり書で、受領～返却までを一貫で管理し、アナログなやり方ながら消去や返却を確実に実現している事例

5-⑧【個人データは 3 枚複写式の預り書で受領・作業・返却まで一貫して管理】
（その他サービス業(印刷・広告)：約 1,400 人）

・コ社では、個人データは返却することが基本になっている。受託時に預かった個人情報については「預かり書」を取り交わすが、この預かり書は 3 枚複写式になっている。受領、記録から返却まで一連で管理できるようになっている。

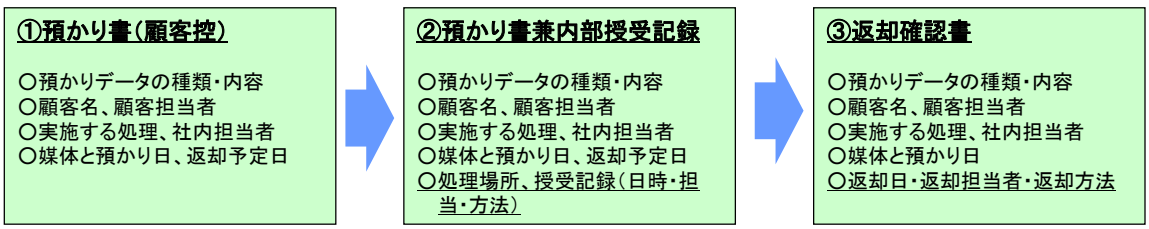
・月に一度、媒体の返却の有無を管理者がチェックするようにしている。

・メールや郵送で預かった個人情報については、預かり書とは異なる様式書類でチェックして、月に 1 度管理責任者がチェックするようにしている。

・プリンタなどに個人情報が残ることについては、次の印刷される情報が機械に読み込まれると、自動的に消去されるようになっている。

・営業における「預かり書」と、処理場所に渡すときの台帳の照合により、万が一、ミスが発生して営業が預かり書を授受・作成しなかった場合でもチェックはできるようになっている。

図表　3 枚の預かり書の主な内容



（※図表中の下線部は、「特にその預かり書だけに記載されている項目」であり、特徴を示す。）

（6）個人情報の監査の場面

ア）従来業務に付随する形で監査を実施することで新たな業務負荷を抑える事例

6-①【社長が従来から行っていた社内点検に個人情報保護の観点を付加】

（電気・ガス・水道業：約 60 人）

・C 社では月に１度、社長が社内を点検している。もともとは社内清掃のチェックの目的で行っていた見回りを、個人情報保護の視点を取り入れて行っている。

・この点検は抜き打ちではなく、事前に通達をしている。それによって従業者の取組を促進すると考えている。

イ）異なる部門の監査担当者が監査を実施することで質を維持しつつ新たな外注コストの発生を抑える事例

6-⑨【監査は異なる部門の監査担当者が複数で実施】

（その他サービス業（印刷・広告）：約 11,000 人）

・X 社では各事業部内に各種責任者（法令及びその他の規範調査、教育、苦情及び相談窓口、委託契約内容確認、委託業者管理）と監査責任者をそれぞれ任命している。

・日本情報処理開発協会（JIPDEC）によると、監査には客観性が求められ自部門の監査ができない。しかし、同社の業務内容は多様であり、監査を受ける部門の業務内容にある程度通じている者が監査に入らなければ、業務内容が分からず適切な監査ができない。そのため、同社では監査を受ける部門に近い部門に所属する監査担当者とそれ以外の部門の監査担当者が複数で監査している。

ウ）監査時に教育・研修効果を測定して、より効果的・効率的な研修の見直しにつなげている事例

6-⑫【教育・研修方法の効果測定を監査の際に実施。部署ごとにフィードバック】

（情報サービス業(コールセンター等)：約 1,900 人）

・Q 社では、教育内容の浸透度を確認するために、各拠点のオペレータに直接監査を実施している。「オペレータ個人の理解度を確認する」というよりも、教育・研修方法の効果測定が第一の目的である。同じ教育・研修を受けたオペレータは同様の回答をすることが多く、管理者の意識レベルがそのまま影響することがうかがえる。

・監査結果については、当該部署別にフィードバックし、全社的な傾向分析結果をコンプライアンス委員会で発表している。

（7）個人情報に関する苦情処理・開示請求対応の場面

ア）緊急時にはFAX＋コールバックという方法で柔軟に本人確認を実施し、本人確認の負担を軽減している事例

7-③【本人確認方法は郵送を原則として、緊急時には FAX＋コールバックで柔軟に実施】
（その他サービス業(教育・学習支援)：約 180 人）

・ケ社では、電話での問い合わせの場合でも、問い合わせした者の個人情報をそのまま教えることは無い。原則は郵送で本人証明書類の写しを送ってもらうが、急ぎの場合には、FAX などで本人確認書類を送ってもらうことでも良いとしている。いずれかの方法で本人確認資料に基づいて本人確認した上でコールバックしている。
・なお、問い合わせした者が急いでいる場合に、通常と異なった対応を行うことについては、受験者本人が同意をした場合のみ実施している。
・本人確認として免許証等のコピーを送ってもらう場合は、機微な情報である本籍地の情報は（黒塗りなどで）見えないようにして送ってもらっている。
・本人が了解した場合は、郵送以外でも返事をしていることがある。

（8）個人情報に関する事故（漏えい・き損等）発生の場面

ア）委託元と連携した事故対応体制を構築することで、単独で作るよりも多くの情報を得、また効果的な体制を構築できている事例

8-⑤【委託元と連携した対応体制の整備】
（情報サービス業(アウトソーシング等)：約 1,400 人）

・ク社では、事故発生時の報告体制について、委託元と連携した対応体制を整備している。
・委託元とは、委託元が主催する「合同リスク検討会」に毎月出席し、事故や問い合わせに対する状況を報告し、今後の対応などについて検討している。

イ）不要な報告などを削除することで、短い時間で必要な情報だけを効率的に収集することができる体制を構築している事例

8-⑥【事故発生時の混乱や不要な報告を防ぐため、漏えい発生時の報告は 2 段階に分け、第一報では必要な最低限の情報を挙げてもらうようにしている】
（その他サービス業(印刷・広告)：約 1,400 人）

・コ社では、事故などが起きたときには緊急連絡表を設けている。慌てると何を報告してよいかがわからなくなるので、第一報ではどの程度の内容を報告し、第二報以降ではどの程度報告するのか、という点で 2 つの段階に分けて報告するようにしている。第一報用のフォーマットを作成している。
・そのように、「どこまで報告するか」ということを明確にしていないと、何度も電話で

現場の担当者に聞きなおしたりする手間が生じた事例があったからである。不要な情報ばかり報告され、本当に必要な情報の報告が遅れることを懸念していることによる対応である。

・漏えいなどの事故が生じた場合に備え、「公表判断基準」を策定している。「管理主体は誰か」「漏えい形態はどうか」「漏えい内容はどうか」「漏えい情報量」「被害の大きさ」の 5 つの視点で判断し、公表するか、公表しないか、ということを明確にしている。公表に際しては経営企画部とも連携している。

ウ）様々な連絡手段を用いて、顧客へいち早く事故情報についてのお知らせを行った事例

8-⑨【郵送、メール、電話の順に連絡手段を使い分けて全顧客へ、いち早く連絡することを優先】（情報サービス業(ソフトウェア)：約 500 人）

・ソ社では事故発生を認識した当時は、誰が何をしたら良いか全く分かっておらず、“エンドユーザーも含む利害関係者に説明を行うこと”を最優先とすることにした。この判断は社長によるトップダウンの判断であった。

・告知文の作成と連絡対象者のリストの作成後に全ての顧客向けに書簡を送付し、記者会見を実施。翌日には新聞 5 紙に漏えい事件発生についての謝罪広告を掲載した。

・全顧客に書簡で、個人情報の漏洩の可能性を伝える書簡を郵送した。数%は宛先不明で書簡が戻ってきた。特にオンラインで商品をダウンロードして購入した顧客に連絡をつけるのが難しかった。理由はダウンロード購入の場合、商品の発送が伴わないため、登録された住所に不備が多かったことによる。住所不明の顧客には、同じ内容のメールを送付した（メールアドレスは確実に把握していた)。それでもメールが戻ってきた場合は、電話番号がわかるときには電話をした。残り数百名分はどうしても連絡がつかず、ホームページへの掲載などで対応した。

エ）顧客からの問い合わせを多数受けることで、顧客に適切に対応することができるようになった事例

8-⑩【顧客からの問い合わせの蓄積により、顧客の知りたいこと、顧客に伝えるべきことを整理し、的確な対応を実現】（情報サービス業(ソフトウェア)：約 500 人）

・ソ社では当初はいち早く漏えいの発生を顧客へ伝達することを優先したため、コールセンターでの想定問答などの検討・作成が十分でなかった。このため、当初の問い合わせには十分に回答することができなかった。顧客への対応は公表前にもう少し検討したほうが良かったようにも思うが、逆に顧客からの直接の問い合わせ内容を聞かないと、何を顧客に伝えなくてはいけないのか、ということについてはわからなかったとも考えている。

・なお、漏えいの状況や原因は十分には解明されず、全て結局は「可能性がある」という調査結果で終わってしまったため、追加で有益な情報提供はできなかった。

オ）監督官庁、警察等に迅速に連絡をいれ、対応に早急に着手した事例

8-⑮【原因究明に迅速に着手し、顧客・警察・監督官庁へ連絡】
（情報サービス業（アウトソーシング等）：約 30 人）

・タ社では出会い系サイトからスパムが送信されているという苦情が、同じ日に多くの顧客から寄せられ、携帯メールアドレスの漏えいの可能性に気づき、警察へ通報、当日夜から調査を開始した。
・最初に、どこのサーバ上のどこの企業の顧客の情報が流出したか調査した。その結果、原因までは分からなかったものの、管理画面に不正アクセスと思われるログが発見された企業があり、同社が事故を起こした可能性が高いことが判明した。
・翌日、同社は顧客と警察に漏えい事故発生の可能性を連絡。主務官庁等へは先ず顧客が連絡し、その後同社から連絡した。
・二日後、アクセスログ結果より、警察の要請に基づき、インターネットプロバイダーに協力してもらい、アクセス元を調査したところ、繁華街のインターネット喫茶から同社のサーバにアクセスされていることが判明し、事故であることを特定した。
・その後、同社ホームページで漏えい事故が発生したことを公表。顧客企業のユーザーには、顧客企業がそれぞれ連絡した。同社は、顧客企業よりも先に公表できないことから、公表のタイミングを調整する必要があった。

カ）事故後一定期間、役員が直接に電話対応を深夜まで行うことで、顧客への適切な対応を実現した事例

8-⑯【事故後 1 ヶ月間、役員が交代でコールセンターを深夜まで運営】
（情報サービス業（アウトソーシング等）：約 30 人）

・タ社では事件公表から約一ヶ月間、同社内に事故対応のコールセンターを設置し、電話とメールで応対した。
・受付日時は、土日関係なく、朝 10 時～26 時（深夜 2 時）まで。
・体制は、基本的にすべて役員が交代で対応した。社員にはほとんど対応させなかった。
・対応を始めて一ヶ月が経過してからは、コールセンターに委託したが、二次的にエスカレーションさせて同社にも繋がる体制を整えていた。
・顧客企業と調整し、事故に関するユーザーからの連絡はすべて同社で受け付けるようにした。これにより、被害にあったユーザーが、たらいまわしされることなく、均質の応対をうけることができるようにするためである。
・スパムを完全に停止させるためには、メールアドレスを変更していただくしか方法はなかったため、ひたすらお詫びを申し上げた。
・クレームの受付は、メールが 1,000 件、電話が 300 件で、メールが圧倒的に多かった。

キ）日常的に付き合いのある事業者など、外部リソースを適切に活用することで、適切且つできる限り早い対応を可能にした事例

8-⑯【事故後 1 ヶ月間、役員が交代でコールセンターを深夜まで運営】
（情報サービス業（アウトソーシング等）：約 30 人）

・タ社では事件公表から約一ヶ月間、同社内に事故対応のコールセンターを設置し、電話とメールで応対した。
・受付日時は、土日関係なく、朝 10 時～26 時（深夜 2 時）まで。
・体制は、基本的にすべて役員が交代で対応した。社員にはほとんど対応させなかった。
・対応を始めて一ヶ月が経過してからは、コールセンターに委託したが、二次的にエスカレーションさせて同社にも繋がる体制を整えていた。
・顧客企業と調整し、事故に関するユーザーからの連絡はすべて同社で受け付けるようにした。これにより、被害にあったユーザーが、たらいまわしされることなく、均質の応対をうけることができるようにするためである。
・スパムを完全に停止させるためには、メールアドレスを変更していただくしか方法はなかったため、ひたすらお詫びを申し上げた。
・クレームの受付は、メールが 1,000 件、電話が 300 件で、メールが圧倒的に多かった。

ク）風評被害を回避するために、敢えて事故の情報を大手新聞社に詳細に説明し、できる限り事実を適切に報道してもらうように努めた事例

8-⑲【過大な報道による風評被害・混乱を防止するため、敢えて大手新聞社に事故情報を詳細に説明して正確な情報を報道してもらう】
（情報サービス業(E コマース)：約 60 人）

・チ社では IR や PR も掲載したが、その内容がそのまま顧客や社会に伝わるかは非常に不安であった。そこで、特定の大手新聞社に対して同社から情報を提示し、先に取材してもらって、できるだけ間違いがないように報道してもらえるような工夫を行った。
・当然に新聞社の原稿であるので、掲載前に記事を確認させてもらうことはできなかったのだが、一部は少し過大に書かれた部分もあったものの、間違いが少なく報道してもらうことができた。特定新聞社にリークしたことで、その会社が一番詳細に漏えい事故の情報について報道することができ、結果として他の新聞紙よりも耳目を集め、IR や PR の趣旨を損ねることなく正確な情報を伝えることができたと感じている。

（9）その他の場面

―