Ⅱ．個人情報保護対策の場面ごとの取組事例

Ⅱ．個人情報保護対策の場面ごとの取組事例

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

本節では、個人情報保護対策そのものを効果的かつ効率的に実施する前提となる、規程づくり、体制づくりの事例を取り上げている。また、特に効果的・効率的と考えられる工夫を事例として示すようにした。

例えば、規程づくりのためのユニークな方法としては、問題となる事例が社内外で起きるたびに「ヒヤリ・ハット集」として紹介しながら、その内容を次年度以降の社内規程に取り込んでいくことで、職員に違和感無く規程を導入するという方法を採用している事例（⑦）を紹介している。また、効率的な取組としては、規程類の作成そのものは自社で行い、最終チェックだけを外部の専門家に委託する方法を取っている事例（⑤）や、規程等があまりに多くなり過ぎ、有名無実化することを懸念して従業者が守るべき規程はごくごく限定している事例（⑨）などを紹介している。

また、体制構築のための取組としては、役職ごとに責任者と代行者を置き、別な役職ではその関係を逆転させることで、相互監視作用を狙った事例（④）や、より円滑に個人情報保護を実現できるように、個人情報保護とは全く関係の無い既存組織に個人情報保護のための役割を担わせているような事例（②）を紹介している。

本節で紹介している取組事例

1-①：継続的に取得する個人情報については組織管理者に責任
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
1-③：本社と支店等との分権
1-④：タスキがけ人事による効率的な管理体制
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
1-⑥：新ルール適用前に試行実施の期間を確保
1-⑦：ヒヤリ・ハット事例集の作成・掲示
1-⑧：個人情報保護推進の中核メンバーを管理職直前の者とすることで教育的効果も狙う
1-⑨：規程を絞って従業者にわかりやすく説明。常時携帯用のカードも作成

1-①【継続的に取得する個人情報については組織管理者に責任】（製造業：約 334,000 人）

・A社では、ドメイン（事業領域）ごとに CSO（チーフ・セキュリティ・オフィサー）とプロフェッショナル（現場の情報セキュリティ推進実務担当）を設置しており、全社－ドメイン－事業場の 3 層管理体制を採っている。

・継続的に取得する個人情報については、組織管理者が常に最新版にしておく責任を負う。

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。

1-③【本社と支店等との分権】（信用業：約 6,300 人）

・I 社では、全社的には個人情報保護に関する専任組織が、規程類の整備や教育指導、管理を行っている。各部・支店単位においては各組織長及び次長が、個人情報保護責任者及び個人情報保護代行者となって管理下の組織における個人情報保護に係る業務を管理している。

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。

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。

1-⑥【新ルール適用前に試行実施の期間を確保】（信用業：100 人未満）

・K 社では、新たに整備又は変更した規程の本格実施前に、１ヶ月半ほどの試行期間を設け、ルールの抜け漏れや、ルール間の不整合を修正した。

・従業者においては当初新ルールに対する不満は大きかったが、習熟度の高まりと共に定着した。

1-⑦【ヒヤリ・ハット事例集の作成・掲示】（情報サービス業：約 1,600 人）

・O 社では、世間で実際に発生した個人情報事故事例や社内でヒヤリやハットした事象について紹介し、“世間の事故を社内で発生させないために、また、ヒヤリやハットを事故に繋げないためにどのような行動を取ることが求められるか”を記載した「ヒヤリ・ハット集」を随時作成・社内通知している。

・事例集の形式ではあるが、単なる注意喚起の通達ではなく実際には行動基準を示しており、既成事実化した上で次年度は社内ルール集に正式に織り込むことで、従業者の抵抗や戸惑いを極小化しながら円滑なルール策定に役立てている。

1-⑧【個人情報保護推進の中核メンバーを管理職直前の者とすることで教育的効果も狙う】（情報サービス業：約 350 人）

・P 社では、社内の最高機関である「セキュリティ推進委員会」のメンバーをプロジェクト・リーダー候補者で構成している。これはプロジェクト・リーダーになると、監査人のような立場でチームの個人情報保護への取組をチェックする必要が生じるからであり、育成の効果も持たせている。

1-⑨【規程を絞って従業者にわかりやすく説明。常時携帯用のカードも作成】（情報システム／製造業：約 500 人）

・R 社では、規程は全部で 38 あるが、分かりやすい 2 つの規程（「利用者向けガイドライン」と「情報資産取扱ガイドライン」）だけを見ればよい、と従業者には通達し、わかりやすく周知している。

・規程の目的、守るべきこと、事故の連絡ルートなどをまとめた「セキュリティカード」を従業者全員に配布し、常に携帯するようにしている。

２．個人情報の取得の場面

本節では、個人情報の取得の際に本人（情報主体）や情報提供者に対して効果的・効率的な同意をどのように取得しているのか、ということについて事例を取り上げている。

特に、個人情報の取得段階で本人（情報主体）への説明を的確に行ったり、内部的に取得・授受の事実を厳密に確認・記録するための方法を採っているような事例と、有効活用の観点から取得に対する同意を効率的に確認している事例を取り上げている。

前者としては、センシティブな個人情報を取得する際には本人のみならず関係者まで同席した上で取得するような事例（⑪）や、事業者内での個人情報授受についても記録をつけるような事例（⑩）も紹介している。

また、後者の事例としては、情報提供者に“利用目的のうち不同意な目的”について、書き出させることで、本当に利用されたくない目的に限って絞り込んで確認する事例（⑥）や、対面で取得を行うために原則全てオプトアウトとし、オプトアウトの方法等をわかりやすく示している事例（⑨）、利用目的が単純明快な場合には個人情報についての同意を記載を以って代えている事例（③）なども紹介している。

本節で紹介している取組事例

2-①：重要度の高い個人情報の取得時のチェック
2-②:自社 WEB サイトで誕生日の方へのプレゼント抽選会という企画で情報の最新性を確保
2-③：取得目的が明確な場合は使用目的はあえて提示せず
2-④：個人情報を紛失リスクと記載内容で 12 段階に分類
2-⑤：様々な個人情報保護水準の百貨店等にテナントとして入居しているため、個人情報取得時の確認事項としては、最大公約数的な文言で対応
2-⑥：情報提供者は利用目的のうち不同意なものを提示できる
2-⑦：WEB サイトで個人情報を取得する場合、本社承認が必要
2-⑧：センシティブ情報については“回答枠”は設定せず、「特別な希望」という欄に記載してもらうことで個人情報の提供の同意を得たものと考える
2-⑨：原則はオプトアウトとし、事後に第三者提供の停止を要求されたら対応する
2-⑩：顧客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
2-⑪：情報の取得時には関係者が立ち会う

2-①【重要度の高い個人情報の取得時のチェック】（製造業：約 334,000 人）

・A 社では、事前に組織責任者が個人情報リスク評価シートを活用して、取得から廃棄までのライフサイクルに従ってリスク評価を行うことを義務付けている。

2-②【自社 WEB サイトで誕生日の方へのプレゼント抽選会という企画で情報の最新性を確保】（卸売業：約 1,400 人）

・D 社では個人情報の更新が難しいことが問題視されていた。結果として、新情報と旧情報が混在しており、どの情報が最新かを判断できない状況であった。

・そのため、自社 WEB サイトで誕生日の方へのプレゼント抽選会という企画を行い、その際に住所・電子メールアドレス等の修正依頼をするようにしている。この方法による情報更新の効果は大きい。

2-③【利用目的が明確な場合はあえて提示せず】

（小売業（百貨店・スーパー）：約 12,000 人）

・F 社では配送伝票や修理伝票は、利用目的が明確なため記載していない。

・電話帳などの公開情報については、本人の理解を得ることが困難なので、これらを利用してダイレクトメールや商品案内送付などの販売促進目的では一切使用しない。

・取引先（店舗）に利用目的の雛形を提示し、指導している。

2-④【個人情報を紛失リスクと記載内容で 12 段階に分類】

（小売業（百貨店・スーパー）：約 12,000 人）

・F 社では販売部における個人情報のリスクレベルを整理している。記載内容（4 項目）と紛失リスク（3 段階）で評価し、漏えいリスクとして 12 種類に分類してそれぞれに対応を定めている。リスク分析のため、保有個人情報に関してマトリックス表を作成し、リスクを判断している。

＜個人情報の分類管理の前提となる整理表（一部抜粋）＞

									売場において	
対象		記載されている顧客情報				控の有無		保管方法	保管期間の目安	保管期間終
		氏名	住所	電話番号	ｸﾚｼﾞｯﾄ情報	売場控	関連部署控		売場（倉庫・バックヤード含む）	最終処理
■顧客名簿等										
	顧客名簿（ショップ名簿等）	○	○	○	×	－	－	施錠保管	利用期間のみ	店にて廃棄業
	顧客名簿（システムⅡ名簿）	○	○	○	×	－	－	〃	〃	顧客政策担当
	顧客名簿（フロッピー）	○	○	○	×	－	－	〃	〃	店にて廃棄業
	顧客名簿（各種サークル等）	○	○	○	×	－	－	〃	有効会員の期間のみ	〃
	アンケート用紙等	○	○	○	×	－	－	〃	集計作業等の利用期間のみ	〃
	ご尊名台帳	○	○	○	×	－	－	〃	利用期間のみ	〃
■POS関連伝票										
	お買上原票（現売・他クレ等）	○	×	×	○	○	○	施錠保管	6ヵ月	店にて廃棄業
	〃 （自社クレ）	○	×	×	○	○	○	〃	〃	〃

2-⑤【様々な個人情報保護水準の百貨店等にテナントとして入居しているため、個人情報取得時の確認事項としては、最大公約数的な文言で対応】

（小売業（物販）：約 1,000 人）

・G 社ではショッピングセンター、駅ビル等への出店がほとんどであるが（9 割以上）、一部独立店舗などもある。

・百貨店とスーパーマーケットで要求される個人情報保護水準が異なることもある。

・百貨店からは個人情報の共同利用などを要求されることもあり、その都度対応しているが、百貨店は系列が異なっていても大体は要求されることは同じである。

・ポイントカード会員加入時には、個人情報の利用方法として「テナントで入っている百貨店と共同利用する場合がある」旨を申込書に記載している。申込書は一種類しか作っておらず、独立店舗でも同様の申込書を使用している。個別に申込書を分けるのは現実的ではなく、最大公約数で最も広く使用する可能性のある場合まで記載しておく対応が望ましいと考えている。

2-⑥【情報提供者は利用目的のうち不同意なものを提示できる】
（その他サービス業（教育・学習支援）：約 60 人）

・T 社では、個人情報取得の際の同意書においては利用目的を複数提示しており、保護者は同意したくない項目を選ぶことができる。例えば「学校の成績の伝達」に同意しない場合は、適切な進路指導ができない旨を保護者に了承してもらっている。同意したくないものを書き写す仕組みにし、同意を得やすくしている。
・同意書の雛形は業務形態によって少しずつ変化させている。

＜同意のお願いと同意書（一部抜粋）＞

●●●社は個人情報を大切にしています

① 個人情報を大切に扱います
② 個人情報を限定された範囲で扱います
③ 個人情報を同意をもって扱います

「個人情報保護管理」について

●●●社では、生徒の授業、進学指導及び生活指導を行う中で、種々の個人情報が集まり、発生します。それらは、生徒の成績管理・進路指導・生活指導等に必要不可欠なものですが、近年における社会情勢の中で個人情報への不正アクセス、個人情報の紛失、破壊、改ざん、漏えいなどの問題を鑑み、これを保護するために、経済産業省告示のガイドライン、社団法人全国学習塾協会の個人情報保護に関するガイドラインに基づき、独自のコンプライアンスプログラムを作成し「個人情報保護管理」を行っています。

個人情報とは

生徒及びその保護者に関する情報で、その氏名・住所・電話番号等、入会申込書・契約書・口座振替依頼書等に記載されている各事項及び、学校における定期試験・各種模擬試験の成績及び順位、通信簿等をいいます。

利用の原則

個人情報の利用は、次の範囲を原則とします。学習塾の正当な事業の範囲内である、業務管理、生徒管理、成績管理、進路指導、生活指導等に利用します。また、生徒募集の宣伝広告等に利用する場合には、自主基準に則り、プライバシーの保護を含めて細心の注意を払います。

個人情報の適正管理

個人情報は正確かつ最新の状態で管理し、リスクに対して安全対策を講ずるものとします。個人情報の収集・利用及び提供に従事するものは、法令の規程・内部規程を遵守し、個人情報の秘密保持に十分な注意を払います。

生徒及び保護者の同意

個人情報の収集・提供・利用等に関して同意の上ご提出をいただきますが、その提出はあくまで任意のものになります。しかしながら、提出いただけない場合には、事務処理を始め、生徒の成績処理、進路指導等に何らかの支障を来す恐れがあります。●●●社において、情報が円滑な授業を行う上で大変貴重な存在であることをご理解頂きますようお願い申し上げます。

個人情報の取り扱いに関する同意内容

■情報収集をするもの
●提出物（保護者及び生徒→学習塾）による情報
1. 入塾・更新契約書（住所、氏名、生年月日等）
2. 口座振替依頼書（銀行名、口座番号、名義人等）
3. 通信簿・通知表及び／又は定期試験成績表等（学業成績等）
4. 入試開示得点

●情報の発生（指導期間に発生する各種情報）
5. 塾内試験・模擬試験実施による成績・順位等
6. 出席状況等
7. 各種納入金の納入状況等
8. 各種検定の受検状況及び合否結果等
9. 受験校・学部・学科名と合否結果等
10. 塾内・外での写真・ビデオ撮影、音声録音等
11. 合格体験談・面接情報シート

■情報の利用
1. **チラシ** 合否結果及び成績の推移等を、実名もしくはイニシャル及び写真で掲載する場合があります。
2. **DM** 合否結果及び成績の推移等を実名もしくはイニシャル及び写真で掲載する場合があります。
3. **HP** 合否結果及び成績の推移等を実名もしくはイニシャル及び写真で掲載する場合があります。
4. **案内書** 合否結果及び成績の推移等を実名もしくはイニシャル及び写真で掲載する場合があります。
5. **生活指導** 通信簿等の内容及び出席状況に応じて、生徒個人の生活指導を行う場合があります。
6. **学習指導** 学校での定期試験或いは塾内試験の成績により、弱点対策補習・個別特訓などの学習指導を行います。
7. **進路指導** 模擬試験結果及び通信簿の評定を参考に志望校選定のため進学指導を実施します。
8. **DM送付** ●●●社からのサービス・商品のご案内をご本人又はご家族にDM等でご紹介する場合があります。

■情報の提供・委託

2-⑦【WEB サイトで個人情報を取得する場合、本社承認が必要】
（その他サービス業（印刷・広告：11,000 人）

・X 社では同社自らが取得する情報としては、WEB サイト関係のものが多い。平成 14 年には WEB サイトで個人情報を取得する場合には、本社承認を義務付けた。サイトのプライバシーポリシーや個人情報の利用目的については、本社申請書類の中に記載するよう義務付けている。利用目的の表現が曖昧であったり偏りがあったりする場合には、修正するよう指導している。

2-⑧【センシティブ情報については“回答枠”は設定せず、「特別な希望」という欄に記載してもらうことで個人情報の提供の同意を得たものと考える】

（その他サービス業（会議等開催運営支援）：約 170 人）

・α社では宗教上の理由に基づく食事等の情報（ベジタリアンであること／特定の食べ物が禁忌となっていることなど）や、障害があるので障害者対応の施設等を準備してもらいたいことなどは、「特別な希望（Special Requirement）」という欄で自発的に記載してもらうことをもって、情報の提供に同意を得ている。

・この欄には「例えばこのようなことをお書きください」という示し方しかしておらず、明確にセンシティブ情報を集める欄としているわけではない。

2-⑨【原則はオプトアウトとし、事後に第三者提供の停止を要求されたら対応する】

（その他サービス業（情報提供サービス）：大企業）

・β社では企業の情報（役員等の情報を含む。）を収集する際には、口頭での取材でもあり、必要に応じて個人情報の取扱いについて企業としての方針を示した簡易なリーフレットを提示し説明、詳細はホームページに誘導するようにし、本人（当該企業の役員等）が利用目的の確認やオプトアウトが容易にできるように配慮している。

・取得した企業の情報については第三者（お客さま）提供を行い、その後、本人から「情報の提供を停止してほしい」、という要求があった場合には、第三者提供を停止する。

2-⑩【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）

・γ社では保有する個人情報は委託元から預るものが主である。

・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。

2-⑪【情報の取得時には関係者が立ち会う】

（その他サービス業（高齢者等生活支援）：約 60 人）

・δ社ではサービス対象者宅に同社の聞き取り調査員が訪問し、本人から直接個人情報を聞き取る。聞き取り時には調査員が定型フォーム（聞き取り調査用紙）に記載していく。

・取得の際の同意書は訪問時に本人から署名をもらう。同意書の説明文は 2 枚用意している。1 枚は本人の署名をもらって会社へ持ち帰り、1 枚は本人宅へ確認用として置いてくる。聞き取り時にはその家族、地域の民生委員などの関係者に立会いを求め、本人の同意及び関係者の同意を確認してもらう。

３．個人情報の利用（第三者提供含む）の場面

本節では、個人情報を適切に利用する方法や利用する上での配慮などに関する事例を取り上げている。特に個人情報の適切且つ有効な活用に着目した事例である。

例えば、同一企業内で同意がある場合であっても、個人情報を取得した部署とは別な事業目的で取得した個人情報については、郵送を行うと不信感を感じられやすいので、全て訪問によってその場で説明を行いながら営業を行うようにする事例（①）や、第三者に個人情報を提供し、第三者がその個人情報を活用して営業活動を実施する場合には、個人情報提供者として同行するといった事例（②）などを紹介している。

本節で紹介している取組事例

3-①：顧客宅の訪問時に営業資料を配布し、郵送等は行わない
3-②：第三者に個人情報を提供した場合は、第三者が最初に営業訪問する際に同行する
3-③：問合せ先への情報公開については情報取得時に顧客と決定する
3-④：個人情報を識別できないようにした後にマーケティング分析に使用
3-⑤：情報の更新はサービス提供の間に聴取する情報で行う

3-①【顧客宅の訪問時に営業資料を配布し、郵送等は行わない】

（電気・ガス・水道業：約 60 人）

・C 社では顧客のデータベースは、ガス事業とリフォーム事業で分けている。ガス事業の方は委託元から情報を得ているが、リフォーム事業は直接取得したものである。ガス事業で顧客を訪問した際にはリフォーム関係の営業資料を配布するが、郵送等による営業活動は行わない。ガス事業の顧客とリフォーム事業での取引があった場合は、ガス事業のデータベースからリフォーム事業のデータベースへデータを打ち込みでコピーしている。

3-②【第三者に個人情報を提供した場合は、第三者が最初に営業訪問する際に同行する】

（その他サービス（冠婚葬祭）：約 200 人）

・U 社では葬儀を執り行った場合、亡くなった方が仏壇や墓石等を有しているかどうか、ということについての情報を仏壇屋や墓石屋等に提供することがある。これも葬儀等の同意済みの規約に基づいて個人情報の第三者提供を行っている。

・ただし、いきなりこれらの業者が営業で自宅を訪問するようなことがあると、“どこから情報を得たのか”、ということについて問題になるケースがあるので、最初の営業訪問時には同社の営業社員も同行することにしている。

3-③【問合せ先への情報公開については情報取得時に顧客と決定する】

（その他サービス業（冠婚葬祭）：約 70 人）

・V 社が執り行う葬儀では、近隣の人や親戚などから葬儀社へ葬儀の日程、死因等について直接問合せがある場合がある。そのため、施主から情報取得をする際、情報公開の有無を決め、同意書に署名をもらっている。情報公開についての同意がない場合には、一切の問合せに応じないようにしている。

3-④【個人情報を識別できないようにした後にマーケティング分析に使用】

（その他サービス業（エステティックサロン）：非公開）

・W 社ではプライバシーポリシー等では「個人情報を識別できない形式でのマーケティング情報収集及び商品の研究開発」のため個人情報を利用するとしている。

3-⑤【情報の更新はサービス提供の間に聴取する情報で行う】

（その他サービス業（高齢者等生活支援）：約 60 人）

・δ社では生活サポートサービスで、顧客と会話をする機会が頻繁にあることから、随時更新をしている。更新の際は、誰がいつ何を更新したかがログとして残るようになっている。

・対象者の情報の更新は、毎年 5 月と 11 月には必ず電話で確認している。

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、そもそも特定の従業者以外が個人情報そのものに対するアクセスや編集を管理するためにシン・クライアント方式を導入している事例（⑤）や、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）、個人情報専用のネットワークを構築している事例（㉖）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（⑧）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程している事例（⑮）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（㉘）、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（⑫）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：社内システムに『シン・クライアント方式』を採用し、個人情報を集中管理
4-(1)-⑥：物理的・技術的管理も徹底
4-(1)-⑦：生体認証で入退室を管理している
4-(1)-⑧：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)-⑨：“三点セット”による入退室管理
4-(1)-⑩：バーコードによるトレーサビリティ確保
4-(1)-⑪：システム上の安全管理
4-(1)-⑫：情報の機密分類に応じてシールで色分け
4-(1)-⑬：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)-⑭：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)-⑮：建物内における“セキュリティ区画”の設置
4-(1)-⑯：ファイル共有ソフト（Winny 等）対策の徹底
4-(1)-⑰：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)-⑱：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)-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
4-(1)-⑳：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)-㉑：データの授受は手渡し又はセキュリティ便を利用
4-(1)-㉒：キャビネットは開閉を記録者名を管理
4-(1)-㉓：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)-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
4-(1)-㉕：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)-㉖：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)-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）

・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」などを規程している。

・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（最大 11,400 万件から 4,700 万件まで削減）した。

・インベントリー・リストは組織管理者が常に最新状況にしておく責任を負う。

・新たに「個人情報厳秘」「機密（コンフィデンシャル）」レベルの個人情報を取得する際には、事前に組織責任者が「個人情報リスク評価シート」を活用して、取得から廃棄までのライフサイクルに沿ってリスク評価を行うことを義務付けている。その際はドメイン（事業領域）CPO に承認を受ける。

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 200 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-(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】

（小売業（百貨店・スーパー）：約 12,000 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、ファイルごとの総枚数管理を徹底している。

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 12,000 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-⑴-⑤【社内システムに『シン・クライアント方式』を採用し、個人情報を集中管理】

（小売業（物販）：約 1,000 人）

・G 社では最も管理が問題となるのがポイントカードの会員情報であり、この個人データの取扱いについて、いかに販売店から漏えいや不適切な対応が起こらないようにするか、ということを重視した。

・販売店のクライアント端末からは、個人情報は閲覧・検索・登録のいずれもできないようになっている。

・従来のシステムでは、ユーザ ID／パスワードによりポイント会員の個人情報を閲覧等することができたが、そのユーザ ID／パスワードが無造作にメモ書きで机の前に貼られていたりして、個人情報を適切に管理できる体制ではなかった。

・「ポイントカードの拾得」や「ポイント照会」、「複数枚あるポイントカードの合算」などでデータベースに照会する必要が生じた場合には、電話で照会するようにしている。

・ポイントカードの合算などはデータベースにアクセスできなくても、ポイント数だけわかればその場でカード・ライターを使って書き換えることはでき、顧客には迷惑は掛けていない。

・エリア統括事務所（営業部事務所）でも個人情報の閲覧・検索・登録はできない。エリア統括事務所（営業部事務所）でもアルバイトなど外部スタッフを多く活用している状況は同じであるので、管理が徹底できないと考えたからである。

・当初、従業者からは「不便になる」などの反発があり、今も完全に反発がなくなったわけではないが、実際に店舗からの個人情報の漏えいなどの報告は上がってきていないことから、リスク回避の意味で有効性も認識してもらえつつあると理解している。

・システム導入費は 2,500～3,000 万円程度である。

・従業者情報もイントラネット上では見られるようになっているが、画面の印刷やデータのダウンロードはできないようになっている。個人情報や機密情報を掲載しているページは個別にいろいろな動作の制限を掛けている。

4-⑴-⑥【物理的・技術的管理も徹底】（小売業（物販）：約 1,000 人）

・G 社ではアプリケーションのインストールは本部のシステムと連動するアプリケーションのみできるようになっている。

・アプリケーションの起動などの起動ログはすべて取っている。

・FD や USB メモリなどによる外部書き込みは一切できないようになっている（書き込もうとするとブロックがかかるようになっている）。これは外付けの書き込み機器を接続しても同様である。

4-⑴-⑦【生体認証で入退室を管理している】

（小売業（通販等）：約 400 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-⑴-⑧【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 400 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-⑴-⑨【“三点セット”による入退室管理】（信用業：約 6,300 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-⑴-⑩【バーコードによるトレーサビリティ確保】（信用業：約 6,300 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)-⑪【システム上の安全管理】（信用業：約 6,300 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「BS7799・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)-⑫【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)-⑬【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 6,400 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)-⑭【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 社では様々な種類の個人情報を管理している。個人情報は種類に応じたレベル分けをすることなく、厳重に管理している。

・個人データに接触するには１次から３次までのチェックをパスする必要がある。守衛の確認（１次）、管理ルームに入るための IC カードゲート（2 次）、CPU ルームに入るためのチェック（3 次）である。CPU ルームの入退室には氏名を記載し、CPU ルームの管理者の確認後に鍵をもらえるようになっている。

・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。

・特に重要な個人データについてはネットワークに接続していないスタンドアロンのサーバで管理している。

・クレジットカード情報については、汎用機を利用している。誰でも容易にアクセスできないシステム構成で、セキュリティ対策は、非常に厳しい。

・ファイル共有ソフト（Winny 等）対策のため、『一斉送信監視ソフト』を導入しており、ファイル共有ソフトを利用すると自動的に検知するようになっている。また、『ライセンス違反検知ソフト』も利用し、ファイル共有ソフトのインストールを検出している。

4-(1)-⑮【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 段階に分けている。

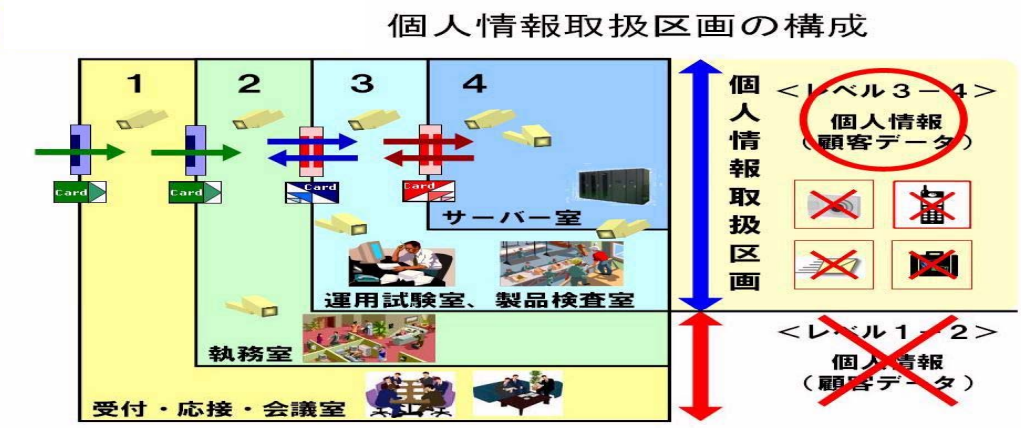
・＜レベル 4＞はサーバ室等で個人情報が保管されているエリアである。＜レベル 3＞はシステム運用試験や製品検査を行うエリアであり、個人情報を実際にハンドリングして運用テストなどを実施する。

・これら 2 つのエリアにのみ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。＜レベル 3、4＞の社内ネットワークが＜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 WEB 閲覧ができなくなっており、個人情報の流失や外部からの不正アクセスを防いでいる。

・同エリア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、入退室者の入退室の記録が 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なかにシステムに関する問合せや確認のために個人情報を含む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、開封作業を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、これらの受信も同区画内に設置した個人情報受信専用 FAX で実施している。

・受付・応接・会議室が＜レベル 1＞、執務室（システム開発室）は＜レベル 2＞とされており、個人情報は存在してはいけないエリアとなっている。

＜セキュリティ区画の構造＞



4-(1)-⑯【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 社では個人情報や業務情報を会社から自宅に持ち帰って、自宅で私物のパソコンを使って作業をしていたため、これらの重要情報の漏えい事故が頻発していた。そこで同社では、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のパソコンについてはすべて、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。

・従業者の自宅にある私物パソコンについてもファイル共有ソフトの有無をチェックをさせた。

4-(1)-⑰【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)-⑱【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)-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 60 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)-⑳【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)-㉑【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)-㉒【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 200 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)-㉓【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)-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。

4-(1)-㉕【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)-㉖【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。

（２）従業者等への教育方法

本節では、個人情報保護の必要性や重要性、社内における規程等について、広く従業者に周知し、意識を高めながら、しっかりと遵守させるために取り組まれている事例について取り上げている。

個人情報保護に対する意識や知識向上のための取組としては、研修の実施などが広く行われているところであるが、ここで取り上げた事例の中では、研修を一歩進めて定期的に個人情報保護に関する知識についての試験を実施し、一定以上の成績を修めなければ社内システムにアクセスできず事実上業務が遂行できなくしている厳しい事例（⑩）も紹介している。

その他、個人情報保護に関する民間資格を全職員に取得推奨するような事例（⑨）や、社内で自前の業務内容に沿った独自の個人情報保護資格を策定して認定しているような事例（⑰）を紹介している。

また、試験や研修のみに依存することなく、管理職による個人情報保護のための面接やヒアリングまで実施しているような事例（㉑）も紹介している他、個々人の業務内容や状況に合わせて個人情報保護についての目標を設定させ、遵守させるという目標管理制度の仕組を導入したような事例（⑳）を紹介している。

さらに、一般的に、わかりやすい形で個人情報保護の重要性と対応方策を喚起させるために、事業所内で独自に「個人情報保護の日」を設定して一斉点検やイベントを行ったり、個人情報保護の原則を定めてキャッチフレーズ化するようなユニークな事例（⑮、⑯）について紹介している。

本節で紹介している取組事例

4-⑵-①：e ラーニングで学習のためのテストと実力テストを合わせて実施
4-⑵-②：年に 6 回テストを開催し、不合格者には補講・再試を実施している
4-⑵-③：毎月全部署で勉強会を実施
4-⑵-④：半年に一度の e ラーニング
4-⑵-⑤：社内報における解説
4-⑵-⑥：毎月コンプライアンスについて勉強会を実施。3 ヶ月に 1 度習熟度をチェック
4-⑵-⑦：従業者全員の「個人情報取扱主任者」の資格取得を目指す
4-⑵-⑧：ビデオとペーパーテストによる教育
4-⑵-⑨：資格取得の推奨
4-⑵-⑩：「CP 免許」を発行することで、個人情報保護を含めたセキュリティ全般に関するモラルアップをはかっている
4-⑵-⑪：毎月１７日に総点検を実施、各職場の実態を洗い出し報告

4-⑵-⑫：セキュリティ遵守事項を定め、定期的にチェック
4-⑵-⑬：セキュリティ規則を守っていない従業者を対象に個別事情等をヒアリング
4-⑵-⑭：年１回全社でｅラーニングを実施
4-⑵-⑮：個人情報保護の日の設定
4-⑵-⑯：個人情報保護３原則の設定
4-⑵-⑰：社内資格認定試験の実施
4-⑵-⑱：事件・事故を具体例で示す
4-⑵-⑲：部単位でのセキュリティ・ミーティングの実施
4-⑵-⑳：目標管理制度的に、従業者個々の立場に合わせたセキュリティ上の目標設定を実施
4-⑵-㉑：毎月１回プロジェクト・リーダーが面接を通じて個人情報保護の認識をチェック
4-⑵-㉒：従業者が持ち回りでセキュリティ監視委員となることで意識向上を図る
4-⑵-㉓：社外業務者には契約更新時に研修を実施
4-⑵-㉔：研修では具体的に発生し得るケースを設定して問題点や対応方法を回答させる
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
4-⑵-㉖：パートを含めたｅラーニングを実施
4-⑵-㉗：情報管理の小冊子を配布し、携行を義務付け
4-⑵-㉘：担当委員を中心に勉強会を開催
4-⑵-㉙：会社の負担でマニュアルや教材を配布、メールマガジンを配信
4-⑵-㉚：検定試験の受験を奨励し、合格者には褒賞を与える

4-⑵-①【e ラーニングで学習のためのテストと実力テストを合わせて実施】

（製造業：約 334,000 人）

・A 社では全従業者を対象に e ラーニング形式のテストをこれまでに 7 回実施している。年に 2 回行っており、これまでは全問正解するまで何度でも受験させていた。直近では、本当の実力を知るために 1 回しか受験できないテストを実施し事業場ごとの成績を出すことで、事業場間の競争心を煽り、教育の実効力を高めた。

4-⑵-②【年に 6 回テストを開催し、不合格者には補講・再試を実施している】

（小売業（通販等）：約 400 人）

・H 社では・コンプライアンステストを年に 6 回行っている。採点評価は A～D に判定され、成績結果を全従業者に公表する。D 評価の不合格者（70 点未満）には、補講・再試験が義務付けられており、全体的な意識と知識の向上を図っている。

・テストで 100 点を年に 3 回以上取った従業者はゴールドスター、B 判定を 4 回以上取った従業者はシルバースターの星印シールを社員証に貼る「マイスター認定制度」がある。

・テスト問題は新入社員、一般社員、所属長などの階層別に作成し、テスト問題の半分は前回の復習にしている。繰り返すことにより学習効果が上がっている。

・テストの前には「コンプライアンスニュース」を掲示し、テストの出題傾向を示し従業者の予習を促す仕組みを導入している。

・来年度は、部署ごとのテストを行うことも考えている。提示のテーマについて議論させ、運用管理についての検証などプレゼンテーション形式にする。

4-⑵-③【毎月全部署で勉強会を実施】（信用業：約 6,300 人）

・I 社では毎月、全部署において、コンプライアンス定着のための勉強会を開催・実施しているが、個人情報保護に係わる項目を勉強会テーマとして定期的に取り入れ、個人情報保護責任者である組織長が中心となって個人情報保護について周知している。

・テーマ及び資料は個人情報保護担当部が作成して各部署に配布している。勉強会においては、資料を参加者が交代で読み上げたり、ロールプレイングを実施したりして内容の理解を深めるよう促している。

・勉強会に要する時間は 30 分～1 時間程度である。

4-⑵-④【半年に一度の e ラーニング】（信用業：約 6,300 人）

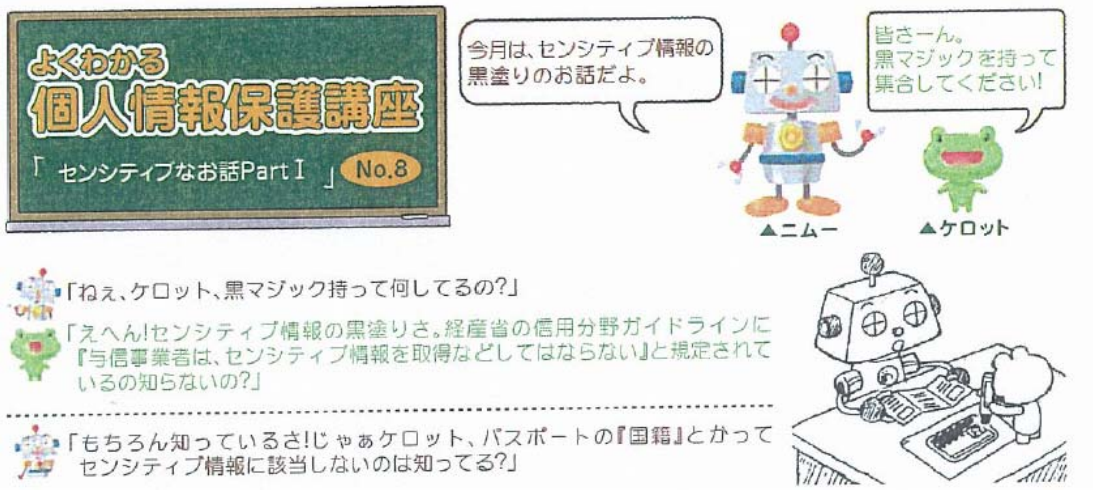
・I 社では個人情報保護の定期点検として、全従業者に対し半年に一度、e ラーニングを用いたテストを実施している。テストは 15 問で、10 分程度で回答できる。また、テスト結果は前述の勉強会のテーマ検討に活用されている。

・テスト問題は、個人情報部が作成している。

4-⑵-⑤【社内報における解説】（信用業：約 6,300 人）

・I 社では社内報に紙面を確保し、個人情報保護について、毎月テーマを決めて解説している。キャラクターや漫画を用いて、難しい内容を、できるだけビジュアル化してわかりやすく伝えている。

＜社内報のサンプル＞



4-⑵-⑥【毎月コンプライアンスについて勉強会を実施。3 ヶ月に 1 度習熟度をチェック】（信用業：約 900 人）

・J 社では毎月コンプライアンスについての勉強会を設けて、同会の中で個人情報保護の教育を行っている。勉強会では自社内で作成したテキストを利用している。テキストは基礎編、実務編にわけ、様々な資料を参考にしながら作成した。

・勉強会では部署ごとにカリキュラムに従いテキストの読み合わせをしている。新人やパートの新規採用があったときには必ず基礎編を教育している。勉強会実施に関しては研修記録をとっている。

・講師は各部署のコンプライアンス担当者が行っている。コンプライアンス担当者の教育については、半年に 1 度本社で半日ほどの集合研修を実施している。

・　勉強会の習熟度を確認するため、3 ヶ月に 1 度イントラネットを使ってコンプライアンスに関するテストを実施している。設問には個人情報保護のみではなく法律やマナ

ーも入っている。
・設問は全 25 問で、15 分程度で回答できるものである。内容はテキストに基づいており、勉強会をきちんと実施しなければ難しい設問もある。対象者は全問正解するまで何度でも解答しなければならない。結果については、対象人数、合格率等が各部ごとにイントラネットに掲示され、全従業者、パートまで閲覧が可能となる。
・初回テストの点数が平均点以下の部署に対しては勉強会のやり直しを求めている。
・点数がよい場合も特に報奨制度はない。報奨制にすると、テスト時に詳しい者が教えるようになり、本当の実力が測れなくなるおそれがあるためである。
・結果表が掲示されることにより、自覚が生まれ、勉強会の実施・充実を図るようになる。

4-⑵-⑦【従業者全員の「個人情報取扱主任者」の資格取得を目指す】
（信用業：約 900 人）
・J 社では従業者全員の日本クレジット産業協会が実施している「個人情報取扱主任者」の資格取得を目指している。
・資格・検定については教育体系の一環として実施している。

4-⑵-⑧【ビデオとペーパーテストによる教育】（信用業：100 人未満）
・K 社では個人信用情報機関及び親会社がそれぞれ作成した２種類の個人情報保護学習用ビデオを従業者に視聴させている。
・また、個人情報保護の理解度確認のため、ペーパーテストを全従業者に受験させている。

4-⑵-⑨【資格取得の推奨】（信用業：100 人未満）
・K 社では日本クレジット産業協会が実施している「個人情報取扱主任者」の資格取得を従業者に推奨し、通信教育費及び受験料を負担している。又合格者へは図書カードを支給している。
・同資格のテキストは大変参考になるので、学習する意義は大きいと考えている。

4-⑵-⑩【「CP 免許」を発行することで、個人情報保護を含めたセキュリティ全般に関するモラルアップをはかっている】（情報サービス業：約 6,400 人）
・Ｌ社では取締役を含めた全従業者に対して CP（コンプライアンスプログラム）免許の取得を義務付けている。CP 免許は必要な研修を受講し、テストに合格して付与される。また免許には４級から１級まで４クラスあり、社内システムへのアクセス権取得は４級取得が前程条件となる。

・各級を表すシールは社員証に貼付している。また“部”や“部門”単位の各級取得状況を全社の会議などで報告する。この運用はより高い級の取得(＝高いセキュリティ知識・意識)への意識付けに大きく貢献している。
・更新試験は毎年行われ、e ラーニングコンテンツを毎年見直しして教育及びテストを実施する。新たなリスクや脅威はこのコンテンツ更新時に取り込まれ、教育される。
・CP 免許は減点制度も運用されている。減点制度はセキュリティ義務違反(例：OS のアップデート不履行)により、持ち点(6 点)がゼロになると免許停止となり、復級するためには、直属上司とともに「免停講習」を受講した上で「復級テスト」に合格する必要がある。
・セキュリティ義務違反の対象範囲は現時点ではシステム的に捕捉できる情報セキュリティに関することが中心となっている。将来的には多岐にわたるコンプライアンス違反に対象を広げていく。
・試験はすべて e ラーニングで受験する運用となっている。多くの問題を用意して、受講者ごとに問題をシャッフルして出題するようにシステム化しており、受験者の不正防止と試験実施の作業量を大きくしない運用となっている。

4-⑵-⑪【毎月１７日に総点検を実施、各職場の実態を洗い出し報告】

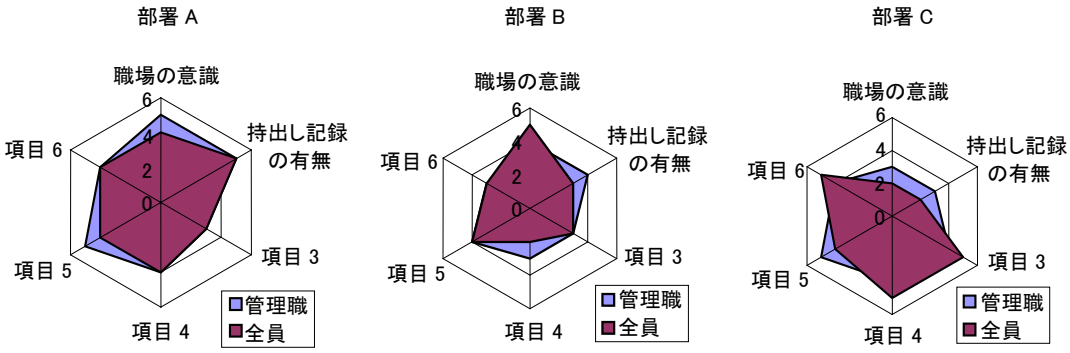
（情報サービス業：約 2,000 人）

・M 社では平成 17 年 3 月の紛失事故をうけ再発防止策を実施するとともに、平成 17 年 4 月から情報セキュリティ充実のための対策として、毎月 17 日に個人情報等重要情報総点検を実施、以降取組中。

・平成 17 年 3 月～4 月に要しての総点検内容は、
個人の意識レベル、情報共有、情報の取扱ルール、情報の廃棄、情報の社外持ち出し、私物記憶媒体の持ち込みなどのルールに対しての職場の実態（管理者がチェック）、と各個人の実態（全員がチェック）を別々に行い、職場ごとに従業者の実態、管理者が見る職場の実態等を整理した。

・こうした点検を同年 9 月まで繰り返し実施することで意識やルール遵守の向上を目指した。この取組によって、従業者の情報セキュリティに対する意識が高まり、ルールで決まっていない具体的な対応方法について問合せが増えたため、毎月の会議（社長が議長の情報セキュリティ推進会議）で情報セキュリティの管理ルールの細分化や補充を行った。
点検結果は、すべての点検部署の特徴が出るようにレーダチャートで表示し幹部が参加する情報セキュリティ推進会議で発表した。点検後の会議では各部署において得点の低い回答項目等が話題になり、各部署の責任者は改善の検討を進めることとなった。同じ点検を繰り返すと慣れが出てくること、ある程度までは上がるがそれ以上あがらないものも出てくるため半年で終了した。

＜チェック結果のレーダチャート（イメージ）＞



4-⑵-⑫【セキュリティ遵守事項を定め、定期的にチェック】

（情報サービス業（ソフトウェア）：約 2,000 人）

・M 社では、平成 17 年 3 月以降に決定されたルールを取りまとめ、整理し、これらの遵守状況のチェックを平成 17 年 10 月から半年間の総点検項目とした。

・総点検は毎月 17 日に実施した。チェックは部署内で実施された。

4-⑵-⑬【セキュリティ規則を守っていない従業者を対象に個別事情等をヒアリング】

（情報サービス業（ソフトウェア）：約 2,000 人）

・M 社における、

平成 18 年 4 月からの総点検の内容は、

今まで取り決めたルールを規程化し、このうち 15 項目を質問の形にして 4 月と 6 月の２回の総点検で遵守状況について自己チェックした。4 月時点では項目の１つ以上を守っていないとした人が延 300 名～400 名おり、職場の長と各人とが面接し、改善を促した。6 月時点の再度の自己チェックでは、延 190 名に減少、190 名を対象に情報セキュリティ推進会議事務局で実態のヒアリングを実施した。ヒアリングを行うことで、事務局と各人の相互理解が増すなどのメリット（誤解が解けるなど）がある。

4-⑵-⑭【年１回全社で e ラーニングを実施】

（情報サービス業（ソフトウェア）：約 2,000 人）

・M 社では年 1 回全社で e ラーニングを実施している。テストも同時に実施しており、合格するまで何度でも回答しなければならない。テストは、プライバシーマーク関連の質問 10 問、ISMS 関連の質問 10 問である。

・テストも含んだ受講時間は約 1 時間である。断続的に受講できるシステムとなっている。テスト結果の公表はしていない。

・組織長に対し、受講率を提示し、期日迄の全員の受講を促す方法で実施している。

・受講者は、経営幹部、従業者（派遣社員、パート、アルバイト含む）を対象としている。

・e ラーニング以外は、新入社員研修で 3 時間程度、親会社からの出向者対象に 1 時間程度教育を実施している。

4-⑵-⑮【個人情報保護の日の設定】（情報サービス業：約 1,600 人）

・O 社では年に１度、『個人情報保護の日』を設定し、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」「改善コンテスト」などを実施している。また、個人情報保護の日には、個人情報保護委員会が主催して「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。さらにこの会議に出席できなかった従業者に対して全国の事業所で地区会議を開催している。

4-⑵-⑯【個人情報保護３原則の設定】（情報サービス業：約 1,600 人）

・O 社では SE が顧客データ（個人情報）を運搬することを禁止している。しかし、顧客企業が SE に個人情報を預ける場合があるため、SE に個人情報を運搬させないための“個人情報保護３原則”を制定して顧客に理解を得ている。“個人情報保護３原則”は「持たない」「預からない」「運ばない」の評語から構成されており、個人情報保護 3 原則をポスターにして執務室や会議室に掲示して啓発している。また、この 3 原則をシールにして各自のパソコンや事務機器などの社内の至る所に貼付し、3 原則を徹底している。

＜「個人情報保護３原則」の社内浸透のために配布されているシール＞

4-⑵-⑰【社内資格認定試験の実施】（情報サービス業：約 1,600 人）

・O 社では社内資格として「個人情報取扱資格認定試験」を実施している。初級・中級・上級の 3 層に分けられている。初級試験と中級試験は毎年実施中であるが、上級試験は平成 18 年 12 月が最初の実施になる予定である。

・初級試験は毎年 8 月に社長はじめ役員、全従業者及び派遣社員のすべてが一ヶ月間の間に合格するまで受験することにしている。

・途中入社の従業者については、毎月 1 日の時点で在籍している従業者が初級試験の合格取得を義務付けられている。

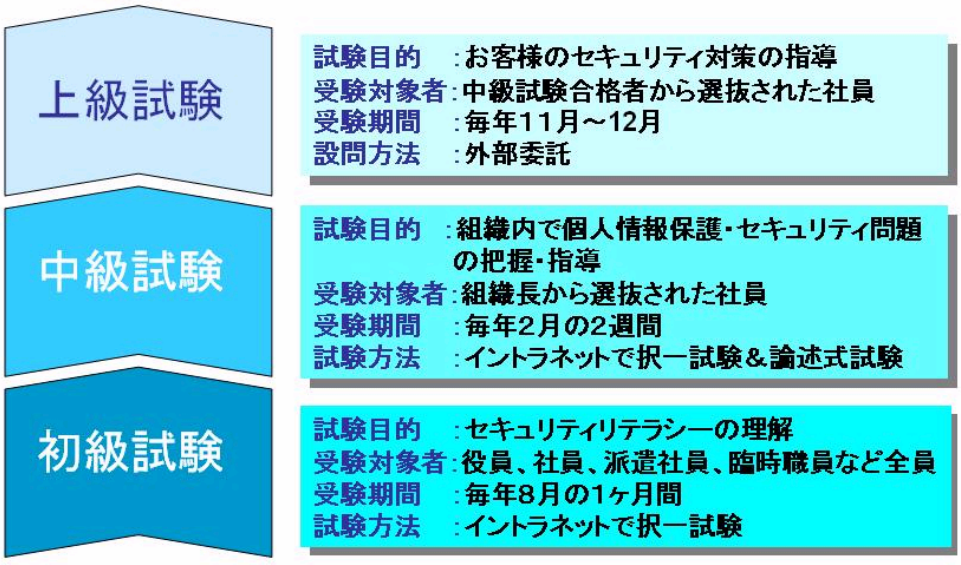
・初級試験の受験方式は e ラーニング方式であり、60 問の問題からランダムに 20 問が出題される形式である。試験問題の内容は従業者が業務や普段の行動に関わるセキュリティリテラシーの問題が中心であり 20 分程度で受験することができる。

・合格すると受験者氏名や認定日が印刷された個人情報取扱資格認定書（プラスティック製のカード）が発行され、社員証と一緒に常時携帯することになる。

・中級試験は、監査人として内部監査が実施できるレベル及び個人情報保護の問題を発見して自ら対策できるレベルであることを認定する試験である。中級試験の問題は、択一式の問題に加え、論述試験も実施する。論述試験の内容は、実際に発生すると想定される具体的な状況と対応についてのケースに対し、セキュリティ上の問題点がどこにあるかということと、その対応として同社のルールに基づいた必要な対策について論述させることにしている。

・中級試験合格者については、社内のナレッジ・データベースに「取得技能」として登録されることになり、人事評価や昇進判断等に利用されるというメリットがある。

＜社内資格認定試験の概要＞



＜社内資格の認定証＞

4-⑵-⑱【事件・事故を具体例で示す】（情報サービス業：約 1,600 人）

・O 社では実際に社内で発生する事件・事故についてどのレベルの事案の場合に報告すべきかの判断が人によって異なることを問題視した。事件・事故が発生した場合には、早期に把握し、さらに事故を拡大させないように早急な対応が求められる。従業者が「事件・事故」と認識すべきケースを具体的に記載したマニュアルを配布して万が一の事件・事故の緊急対応が行えるよう指導している。これにより従業者が勝手に小さな事故と判断して報告を怠ることが無いようにする配慮である。

4-⑵-⑲【部単位でのセキュリティ・ミーティングの実施】（情報サービス業：約 1,600 人）

・O 社では個人情報保護委員会の事務局であるリスク管理室が各部門を訪問して部単位でセキュリティ・ミーティングを１年に１度以上の割合で実施している。

・リスク管理室が各部門を訪問して、従業者がどのような点で悩んでいるか、どのような点に気をつけなくてはならないか、といった事について議論し、自発的に問題を発見して自発的に対策できるよう意識の向上を期待するものである。

・今後は社内個人情報取扱資格試験の中級試験合格者が主催して自発的に開催してくれることを期待している。

4-⑵-⑳【目標管理制度的に、従業者個々の立場に合わせたセキュリティ上の目標設定を実施】

（情報サービス業：約 350 人）

・P 社では経済産業分野ガイドライン等を自己の業務に合わせてわかりやすくカスタマイズしたハンドブックを従業者全員に配布している。

・このハンドブックに基づいて、個々人で顧客のセキュリティ水準や実際に扱っている情報の機密性、案件における役割等を勘案して、セキュリティ上特に自分が気をつけることを幾つか自分で目標として設定している。

4-⑵-㉑【毎月１回プロジェクト・リーダーが面接を通じて個人情報保護の認識をチェック】

（情報サービス業：約 350 人）

・P 社では毎月１回、プロジェクト・リーダーがプロジェクトメンバーを面接し、セキュリティ意識と自分で目標設定したことが守れているかを確認する。問題が無ければプロジェクト・リーダーがチェック欄に押印して、年間の遵守状況も一目でチェックできるようになっている。

・プロジェクト・リーダーは１人あたり 10 数人程度を面接する。

・チェック表は各自が社員証を入れる携帯具に入れられるようにしている。

・このチェック表には問題が発生した際の連絡の方法や連絡先、対応の方法などが記載されており、問題発生時にも誤らずに迅速な対応ができるようになっている。

4-⑵-㉒【従業者が持ち回りでセキュリティ監視委員となることで意識向上を図る】

（情報サービス業：約 350 人）

・P 社では従業者が持ち回りでセキュリティ監視委員となり、オフィスでの書類放置等が無いかを月に２回チェックし、経営会議で報告するようにしている。

・持ち回りで監視委員となることで、自分の問題として捉えられるようになる教育効果を狙う。

4-⑵-㉓【社外業務者には契約更新時に研修を実施】

（情報サービス業（コールセンター）：約 130 人）

・Q 社ではコールセンター業務に従事する契約社員は、短期契約（3 ヶ月ごとの契約更新）の者が多い。契約更新の都度、個人情報保護に関する集合研修を行い、研修後のテストで個人情報への取組の理解度を確認している。

・業務を顧客企業内で行うことから、研修の機会がなかなか確保できないが、契約更新時は全員が研修を受けるチャンスになるため、この時に実施している。

・新聞記事等に掲載されるトピックス的な漏えい事故・事件や個人情報保護に関するポイントについての周知は、業務先の現場で行なっている。

4-⑵-㉔【研修では具体的に発生し得るケースを設定して問題点や対応方法を回答させる】
（その他サービス業（冠婚葬祭）：約 200 人）

・U 社では研修において具体的に問題となったような事例を取り上げてケーススタディを行っている。ケースを示して問題点や管理策、対応策を記載させる形式の問題を出題している。

・「社外において、自社で葬儀を執り行っている故人の死亡原因の話を仲間内でしてしまい、その話が喪主の耳に入ってクレームが来た」といったような極めて具体的に発生しうるケースを示すことで関心と教育効果の向上を目指している。

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。

4-⑵-㉖【パートを含めた e ラーニングを実施】
（その他サービス業（印刷・広告）：約 11,000 人）

・X 社では教材を用意し、e ラーニングを実施している。個人情報の取扱いについて、ファミリー企業及び製造子会社を含めて、個人情報取扱業務に従事するパートに対しても教育している。 e ラーニングはパソコンで回答するが、なんらかの理由でパソコン端末の操作ができない場合は、紙で対応している。

・テキストは全部で 7 章まであり、各章にテストがついている。全問正解しなければ終了しない。設問は各章で約 5 問ずつだが、不正解で再テストになると問題が変わるようになっている。すべて終了するのに 1 時間半～2 時間はかかる。途中保存が可能で 10～20 分ずつ毎日実施するということも可能である。1 回の受講期間は 4 週間である。

・テキストの内容は一般的な情報 4 割、実務編・応用編 6 割である。問題作成はコンプライアンス部が実施している。システムそのものは外部のシステムを利用している。

・e ラーニングは電子メールシステムで案内する。1 回に 2,000 人ほどに案内し、5～6 回にわけて実施している。

・e ラーニングは個人情報保護のみに特化せず、「行動シーン」などテーマを設け、毎年実施する予定である。

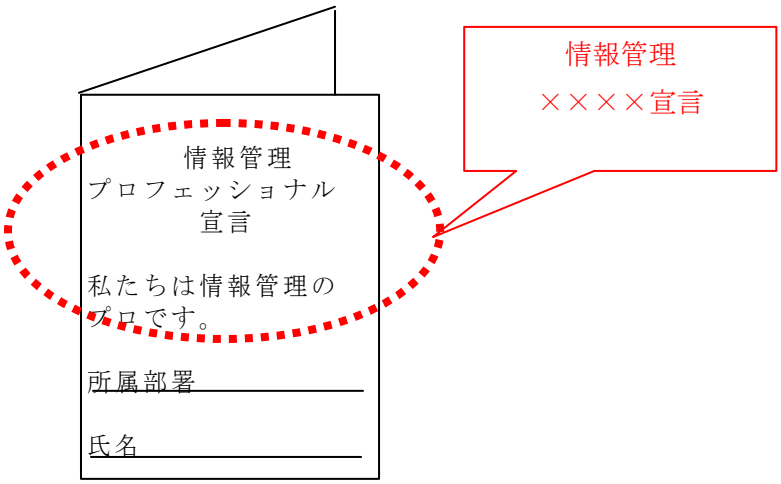
・幹部向け、責任者向けの教育は社内研修の中に組み込んでいる。

・監査員の教育は本社の法務本部の指導のもと実施している。
・e ラーニングに加え、集合教育も適宜実施している。

4-(2)-㉗【情報管理の小冊子を配布し、携行を義務付け】
（その他サービス業（印刷・広告）：約 11,000 人）

・X 社では従業者、パート・アルバイトを対象に小冊子を配布している。規程書は分厚いので従業者が何かあったときに見るため身につけられるものが必要であると考え作成した。本小冊子では自らの部署、氏名を記載し、常に携帯するように指示している。
・小冊子の内容の更新は今後の課題である。

＜小冊子のイメージ＞



4-(2)-㉘【担当委員を中心に勉強会を開催】（その他サービス業（印刷・広告）：約 200 人）

・Y 社では朝礼や部署ごとの勉強会を随時行っている。各部署の保護委員（情報保護担当：中間管理職レベルの職位）とセキュリティ委員（パソコン管理、事業者出入りの鍵の管理を担当）が中心となって勉強会をしている。保護委員は委員会を隔月で開催し、部署に持ち帰って勉強会に活かしている。社内の意識を高める効果がある。
・新入社員研修の初日に基礎教育として個人情報保護に関する教育をしている。アルバイトや派遣社員、パート社員に対しても講義を対面で行っている。
・社内の掲示板に個人情報保護に関する情報を掲示し、全員が閲覧するようにしている。
・集合研修を年に 2 回行っている。講師はシステム管理室が行い、毎回小テストをしている。テスト成績によっては各部署で補習をしている。
・個人情報に関するマニュアルの冊子を作り、全従業者に配布した。別添の問題集もある。

4-⑵-㉙【会社の負担でマニュアルや教材を配布、メールマガジンを配信】

（その他サービス業（ダイレクトメール等）：約 600 人）

・Z 社では従業者に個人情報の保護に関するビデオ（経済産業省のものや民間機関が作成したもの）を見せた。

・従業者全員に個人情報保護の本を購入、配布し、それをテキストとしてテストを行っている。

・セキュリティハンドブックや個人データ取扱ルールを配布した。ルールは関心を集めやすいように、色紙に印刷した。

4-⑵-㉚【検定試験の受験を奨励し、合格者には褒賞を与える】

（その他サービス業（ダイレクトメール等）：約 600 人）

・Z 社では情報セキュリティ検定試験の受験を奨励している。1 回目の受験料、教材費用は会社で負担し、3 級合格で 1 万円、2 級で 2 万円、1 級で 3 万円の報奨金を出している。

・新人や中途採用の従業者を対象に、3 ヶ月に 1 回講習会を開催している。

・『セキュリティ通信』というメールマガジンで、各号ごとにテーマを決めて情報を配信している。現在で 65 号まで出ている。

（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。

本節で紹介している取組事例

4-⑶-①：記憶媒体の情報が記録から 48 時間後に自動消去
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
4-⑶-③：携帯電話に遠隔ロックを導入
4-⑶-④：携帯電話は遠隔ロックが可能な機種を採用
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
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
4-⑶-⑦：建物の安全管理を徹底

4-⑶-①【記憶媒体の情報が記録から 48 時間後に自動消去】

（製造業：約 334,000 人）

・A 社では修理等を担当する外回りの従業者が、訪問先の顧客情報を保有することは仕方が無いことであるが、長期間外回りの従業者が持ち運ぶ事によるリスクを回避するために、SD カードの個人情報（処理が未完了な顧客のデータ）は 48 時間で自動消去されるようになっている（時間設定については週末を考慮して最大 2 日間とした)。

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 334,000 人）

・A 社で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 1,2000 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 30 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 30 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）ノート PC の安全対策

本節では、特に本体そのものが盗難・紛失に遭遇するリスクが高いノート PC について、個人情報保護のためにどのような対策を講じているのか、ということについて取り上げている。

例えば、最も徹底した方法としては、ノート PC そのものの台数を相当程度限定して、ごく一部の従業者にしか認めないような事例（③）を紹介している。

また、万が一盗難・紛失等に遭遇しても、個人情報へのアクセスを許さないために、パスワード等による多重ロックを掛けている事例（①）なども紹介している。

さらに、そもそもノート PC を事業所外で利用することについて、可能な限り限定し、管理を徹底している事例として、データを暗号化済みのノート PC のみに「持ち出し OK」を示すシールを貼ることで誰が見てもチェックができるようにしている事例（②）や、ノート PC 持ち出し時には毎日でも台帳に記入させているような徹底した事例（④）も紹介している。

本節で紹介している取組事例

4-(4)-①：アクセスロックを多重にかけることで対応
4-(4)-②：持ち出し禁止シールを貼って対応
4-(4)-③：ノート PC の配布は特定の従業者に限定
4-(4)-④：ノート PC の外部持ち出し時は台帳に必ず記載。会社では専用ロッカーに保管

4-⑷-①【アクセスロックを多重にかけることで対応】

（情報サービス業（ソフトウェア）：約 400 人）

・N 社ではノート PC へのログインには ID とパスワードが必要である。パスワードは英数字 8 文字以上としており、40 日間隔で更新が必要になっている。

・ノート PC には BIOS ロック、HDD ロックが義務付けられている。また、ノート PC には外部との連絡のための電子メールアドレス程度の情報しか入れないようにしている。

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。

4-⑷-③【ノート PC の配布は特定の従業者に限定】

（その他サービス業（教育、学習支援）：約 1,200 人）

・S 社では地区統括の責任者、エリアマネージャー、教室責任者などの一定レベル以上の者に限定してノート PC を配布し、かつ個人情報保護管理者の許可を得て持ち出している。

4-⑷-④【ノート PC の外部持ち出し時は台帳に必ず記載。会社では専用ロッカーに保管】

（その他サービス業（情報提供サービス業）：大企業）

・β 社ではノート PC を社外に持ち出す際には、持ち出し台帳に必ず記載するようにしており、外勤従業者は、持ち出す度に記帳している。

・ノート PC は外勤従業者のほぼ全員が保有している。

・ノート PC を自宅に持ち帰らない場合には、社内の専用ロッカーに保管するように義務付けている。

（５）外部委託先の監督方法

本節では、業務を実施する上で発生する外部委託について、個人情報保護を徹底させるためにどのような対策を行っているかということについて取り上げている。自らの事業所内における対策や従業者教育等には力を入れていても、事業体の違う外部委託先に対する監督は必ずしも容易ではなく、関与の程度や方法、そもそもの選定のあり方などについて事業者の事例を紹介している。

例えば、そもそも個人情報保護対策を適切に行っている事業者しか外部委託先として選定しないことを明確にして、自社で独自の認定制度やチェック制度を構築している事例（⑩）を紹介している。

また、業務委託中に、適切な管理が継続されているかどうかを確認するために委託元として立ち入り検査を実施しているような事例（⑨）を紹介している。中には検査だけに止まらず、実効性のある改善計画の策定まで求めるような事例（⑤）もある。

一方で、“管理”という姿勢ではなく、パートナーシップと外部委託先事業者における個人情報保護の取組を具体的に支援するような取組（認証取得の支援や従業者教育の支援、合同勉強会の開催など）を行っている事例（①）について紹介している。

なお、一部、業務を受託されている側からみた、委託先の監督に対する協力事例や対応事例（⑧）なども紹介している。

本節で紹介している取組事例

4-⑸-①：委託先を集めて合同勉強会を開催し、委託先との意識を共有
4-⑸-②：委託先から定期的に「報告書」や「証明書」を取得し、さらにモニタリングを実施
4-⑸-③：年に１回以上の立ち入り検査の実施
4-⑸-④：個人情報を大量に委託している業者に対する監査の実施
4-⑸-⑤：業務委託先へはチェックシートを送付。不備項目には改善計画の提出を求め、半年に１回はチェックを実施
4-⑸-⑥：書類発送は監査済みの外部委託先を利用
4-⑸-⑦：外部委託先に出向いて直接指導を実施
4-⑸-⑧：委託元へ個人情報保護のあり方を提案
4-⑸-⑨：取扱情報・事業者規模に応じたチェックリストを作成。立ち入り検査を実施
4-⑸-⑩：協力会社に対して独自の認定制度を導入
4-⑸-⑪：派遣社員からは直接誓約書をとらずコピーで対応

4-⑸-①【委託先を集めて合同勉強会を開催し、委託先との意識を共有】
（小売業（通販等）：約 400 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）に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。

4-⑸-②【委託先から定期的に「報告書」や「証明書」を取得し、さらにモニタリングを実施】（小売業（通販等）：約 400 人）

・H 社では委託先からは「個人情報保護報告書」を毎月提出してもらっている。

・外部委託先に預託された個人情報を破棄した場合、廃棄証明書を必ず提出してもらうようにしている。

・個人情報保護に関する教育やシステムの整備についても報告してもらっている。

・専任担当が適宜、委託先の作業現場までチェックに行っている。

4-⑸-③【年に 1 回以上の立ち入り検査の実施】（信用業：約 6,300 人）

・I 社では委託先に対し、年に 1 回以上、立ち入り検査を実施している。

・質問シートを用意し、回答結果が 5 点満点で平均 3 点以上でないと委託できないこととし、見直しを実施している。

4-⑸-④【個人情報を大量に委託している業者に対する監査の実施】
（信用業：約 6,300 人）

・I 社では大量に個人情報を取り扱う業務を委託している業者（印刷会社等）に対しては、個人情報部が主管している監査に加え、社内の監査部門が別途、業者を訪問してチェックしている。よって、同委託業者に対しては、個人情報部による監査が年 1 回以上、監査部門による監査が年 1 回、業者によっては年 3 回の監査を受ける場合もある。

4-⑸-⑤【業務委託先へはチェックシートを送付。不備項目には改善計画の提出を求め、半年に１回はチェックを実施】（信用業：約 900 人）

・J 社では業務委託先の選定基準として、プライバシーマーク又は ISMS など客観的に評価される認証を取得しているか、認証の取得がない場合には過去にプライバシーマーク、ISMS 認証を剥奪されていないこと、過去に個人情報の漏えい・紛失等の事故を起こしていないこと、委託業者内に適切な情報管理体制が整っていることを条件としている。

・委託の際には個人情報の取扱状況に応じた覚書を委託先と交わす。再委託が発生する場合も、委託先と再委託先との間で同様の覚書を交わさせる。

・委託先に対しては、「委託業務個人情報チェックシート」を委託先に送付し、回答を回収している。回答結果で個人情報保護に不備がある項目については業者から改善計画書（任意フォーマット）を徴収し、少なくとも半年に１回はチェックを実施する。

4-⑸-⑥【書類発送は監査済みの外部委託先を利用】（信用業：約 900 人）

・J 社では利用者への利用明細等の発送を外部委託している。委託先については監査を行っている。

4-⑸-⑦【外部委託先に出向いて直接指導を実施】
（情報サービス業（ソフトウェア）：約 400 人）

・N 社では個人情報の授受に関しては運送事業者との間で特に安全管理を求めた契約を取り交わしている。契約においては、事故の発生に際しての損害賠償についても取り決めている。送付時は情報リスクに応じて「信用ケース」で封印をしている。

・基本的に個人情報の取扱いを委託することは禁止している。委託する場合には、委託先についての基準を決めている。委託先の選定基準としては、管理組織の有無、プライバシーマークの取得、ISMS の取得又はそれに準ずる管理を基準としている。

・この基準は業界ではプライバシーマークや ISMS の取得が増えているので、それほど厳しくはない。

・取得していない企業の中で長年のつきあいのある委託先については、同社から専門家を派遣し、個人情報保護体制の整備のためのアドバイスをすることもある。

4-⑸-⑧【委託元へ個人情報保護のあり方を提案（※）】

（情報サービス業（コールセンター）：約 130 人）

・Q 社では情報管理については、同社から顧客に対して提案する場合もある。時間やコストがよりかかるため顧客から実施しなくてもよいといわれる場合もあるが、同社からは実施した方がいいと提案している。

・逆に、顧客からの厳しすぎる要求に対しては交渉する。社内でも決まりや約束事があるため、それにそぐわない場合には業務を断る場合もある。リスクの高い仕事は請けられないという姿勢を見せる場合もある。

（※）ここでは委託元との関係についての取組を取り上げた。

4-⑸-⑨【取扱情報・事業者規模に応じたチェックリストを作成。立ち入り検査を実施】

（その他サービス業（冠婚葬祭）：約 70 人）

・V 社では委託先として、返礼品を取扱う百貨店、サーバ管理業者、位牌製作事業者等がある。規模は百貨店が最も大きく、位牌製作事業者は個人経営がほとんどである。

・返礼品を取り扱う百貨店へは参列者の送付先リストを渡し、発送からリストの破棄まで委託している。

・委託先を「取扱情報」と「事業規模」に応じてランク分けし、チェックリストを作成した。チェックリストにはランク別の 20～50 項目の必須項目がある。委託先にはすべて立ち入り検査も実施している。

・個人情報保護に関する覚書も交わしている。

4-⑸-⑩【協力会社に対して独自の認定制度を導入】

（その他サービス業（印刷・広告）：約 11,000 人）

・X 社では、委託業務でダイレクトメールの発送を行う際、再委託先を、社内と同程度のセキュリティ確保をしていると認めた認定協力会社に限っている。認定のための検査は半日程度の立ち入り視察で実施している。現在全国で十数社が認定会社となっている。認定先については今後も増やしていきたい。現在は、個人情報管理に厳重を要する特定業務に限ってこのような取扱いにしている。

・委託先の中には、セキュリティ確保のために立ち入り検査に応じられないというケースもある。その場合、同社の作業をしているときに立ち入り検査をさせてもらうよう依頼する。

・委託先には取引基本契約書、個人情報保護についての覚書を交わしている。

4-⑸-⑪【派遣社員からは直接誓約書をとらずコピーで対応】

（その他サービス業（印刷・広告）：約 11,000 人）

・X 社では派遣社員からは直接の誓約書を取ることなく、派遣会社がとった誓約書等のコピーで対応している。

・派遣社員、パート、アルバイトでも個人情報を取り扱う場合は、すべて教育の対象である。テストやアンケートで受講状況をチェックしている。派遣社員からは「受講しました」という書面へのサインもとってはいない。

（６）規程の遵守状況等の日常的点検・確認の方法

本節では、規程などの遵守状況について、日常業務の中で適切に点検・確認を行う上でどのような取組がなされているのか、ということについて取り上げている。定期的に実施され、網羅性の高い監査に加え、日常的に個人情報保護に関する取組の実効性担保のために何がなされているか、ということについて事例を紹介している。

例えば、実際に日常的に担当者や管理職員が個人情報保護に関する規程の遵守状況について業務の現場を巡回等し検査を行うなどの事例を紹介しているが、事業者の規模や考え方などによって、毎日点検を実施している事例（③）や、１ヶ月に１度などの定期的な点検を実施している事例（⑤）も紹介している。

また、パソコン等の個人情報保護対策の進展状況について直感的にわかりやすいシールを貼付することで、職員の誰でもが分かるように対策状況の「見える化」を行っている事例（⑦）や、巡回の際に個人情報保護の面から見て望ましくない行動を取っている職員の席などに“レッドカード”を置いていくというゲーム感覚を取り入れて点検を実施しているようなユニークな事例（⑨）についても紹介している。

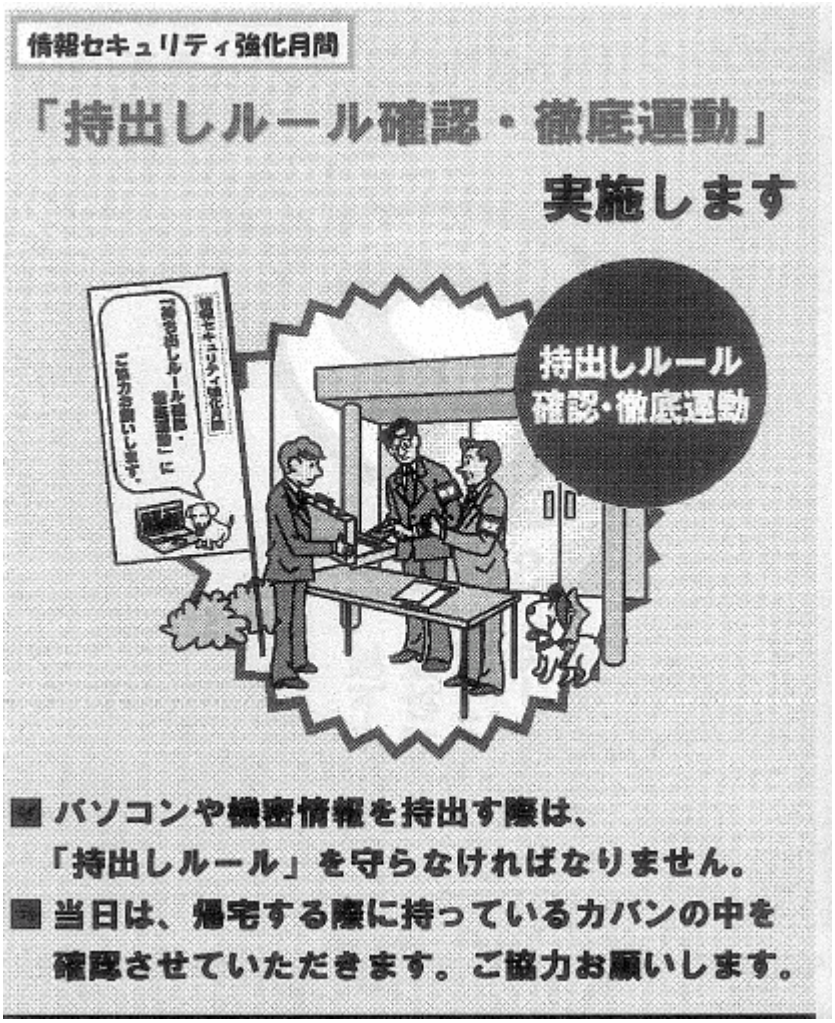
本節で紹介している取組事例

4-⑹-①：全社一斉手荷物検査の実施
4-⑹-②：個人パソコンを定期的に点検し、個人情報が含まれている場合には削除
4-⑹-③：抜き打ちで毎日の放置検査を実行
4-⑹-④：毎月、部署ごとに報告を義務付けている。最終的には査定評価に反映
4-⑹-⑤：月に１日をコンプライアンスデーと定め、項目別に実施を促進
4-⑹-⑥：１日１回以上現物点検・周知徹底
4-⑹-⑦：３つのシールで対策の「見える化」を実現
4-⑹-⑧：毎日朝礼時に「情報管理の誓い」を唱和
4-⑹-⑨：「レッドカード」を導入し、ゲーム感覚の中で従業者のモチベーションを高める

4-⑹-①【全社一斉手荷物検査の実施】（製造業：約 334,000 人）

・A 社では「全社一斉手荷物検査」を実施し、帰宅時に個人情報や重要な情報などを持ち帰ろうとしていないかをカバン等を開けさせてチェックすることで実効力を持たせた。

＜「全社一斉手荷物検査」の実施を呼びかけるポスター＞



4-⑹-②【個人パソコンを定期的に点検し、個人情報が含まれている場合には削除】

（電気・ガス・水道業：約 60 人）

・C 社では従来は見積もりに関する情報も個人で管理していたが、サーバですべて保管するように規程を定め、IT 委員会の活動によって周知を図った。個人のパソコンを定期的にチェックし、サーバに入れていない情報は削除するという取組を始めたところである。サーバの導入は社内の IT 化と情報セキュリティの取組を並行して進めた結果だが、サーバの導入で 100 万円近くの費用がかかっている。

4-⑹-③【抜き打ちで毎日の放置検査を実行】

（小売業（通販等）：約 400 人）

・情報放置整理点検シートがあり、3 時間ごとに FAX や出力物の放置を点検する。このチェックシートで 3 回以上放置があった場合には、指導を受けることになっており、場合によってはプリンタを使用できなくするなどの措置をとる。

4-⑹-④【毎月、部署ごとに報告を義務付けている。最終的には査定評価に反映】

（小売業（通販等）：約 400 人）

・H 社では個人情報管理月報があり、各部署に毎月提出を義務付けている。

・個人情報の保管に関して、「管理者が保管庫の鍵を適切に管理し施錠しているか」、などの項目をチェックする。

・適切な管理がなされていない場合には是正計画書を提出させる。“不適合”の評価を 2 回受けると情報セキュリティ委員会から呼び出しがあり、指導を受ける。

・更に改善が見られない場合には、査定評価に反映することになっている。

4-⑹-⑤【月に 1 日をコンプライアンスデーと定め、項目別に実施を促進】

（信用業：約 900 人）

・J 社ではコンプライアンスについて、各項目別に実施を指示してもなかなか行動に結びつかなかった。そのため、毎月 7 日をコンプライアンスデーと定め行動を促進するようにした。

・実施項目は複数あり、内容によって毎月実施のものと 3 ヶ月、6 ヶ月に一度のものがある。

・年間でいつ何を実施するのかを分かりやすくするため、実施日を記録できる用紙を用意した。各部署の責任者は、実施日を入力し管理している。コンプライアンス統括部もそのデータでどの部署がいつ実施したかをすぐに分かるようになっている。

＜実施日を記録できる用紙イメージ＞

取組確認シート

部門名　　責任者

実施項目	実施日または実施完了日											
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
勉強会の実施	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日
パスワード変更の実施	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日
個人情報一覧表のメンテナンス	－	月 日	－	－	月 日	－	－	月 日	－	－	月 日	－
リスク評価と対策一覧表の見直し	－	月 日	－	－	月 日	－	－	－	－	－	－	－
個人情報破棄の定期点検の実施	－	－	月 日	－	－	－	－	－	月 日	－	－	－
委託先調査の実施	月 日	－	－	－	－	月 日	－	－	－	－	月 日	－
自主監査チェックシート	月 日	－	－	月 日	－	－	月 日	－	－	月 日	－	－
アンケート回答	－	－	－	－	月 日	－	－	－	－	－	月 日	－
	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日	月 日

・前述のコンプライアンスに関する勉強会もコンプライアンスデーに設ける部署が多い。

4-⑹-⑥【1 日 1 回以上現物点検・周知徹底】（信用業：100 人未満）

・K 社では主に朝礼時に、IC カードや鍵等の現物の確認、個人情報の授受記録、出力や作成の管理簿等の確認を行って、個人情報保護の日常的な点検・確認を実施。

4-⑹-⑦【３つのシールで対策の「見える化」を実現】（情報サービス業：約 1,600 人）

・O 社では執務室で扱う各自のパソコンに対して行う重要な対策や点検結果をシールにして、対策が行われていることを一目で分かるようにしている。

・具体的には HD の暗号化や電子メール添付ファイルの暗号化をしている「暗号化対応済シール」、ノート PC などのモバイルを持ち出し許可を受けている「持出し許可済シール」、個人情報を記録していない「個人情報なしシール」の 3 種類である。

・「個人情報なしシール」については、使用期間が半年間（1～6 月／7～12 月）のみに限定されており、管理番号が付けられている。チェックは半年に一度、自分で自分のパソコン内に個人情報があるかないかをチェックするようにしており、パソコンに個人情報がないことを証明するファイル一覧のリストを管理責任者に提出して個人情報が記録されていないことの証明する。証明できた場合「個人情報なしシール」を受領して、各自がそのシールをパソコンに貼っている。「個人情報なしシール」は管理番号で管理されており、個人情報を記録していないことのチェックが終わっているかどうかが分かるようになっている。

・「持ち出し許可済シール」の貼付（持ち出し）は「個人情報なしシール」及び「暗号化対応済シール」が貼られているパソコンで、持ち出し目的が明確な業務においては、最長 3 ヶ月を限度で認められる。

・これらのシールは、誰が見ても一目で必要な対策が終わっているかどうかを確認できるようにするために貼付しており、ノート PC を持ち出した場合にそのシールが貼付されていないと次に事業所への持ち込みが出来なくなってしまう。

＜「見える化」のためのシール（３種）＞

4-⑹-⑧【毎日朝礼時に「情報管理の誓い」を唱和】

（情報サービス業（コールセンター）：約 130 人）

・Q 社では個人情報保護に関して、毎日の作業開始（朝礼）時に「情報管理の誓い」を唱和して注意喚起をしている。作業場の責任者が作業通知の後全員で読み上げている。

・スクリーンセーバーも「情報管理の誓い」が表示されるようにしている。ポスターも掲示している。

・「情報管理の誓い」を唱和することにより、日常業務の中で注意しやすい環境作りができる。毎日全員で唱えているので、説得力がある。

4-⑹-⑨【「レッドカード」を導入し、ゲーム感覚の中で従業者のモチベーションを高める】

（複合（情報システム／製造）：約 500 人）

・R 社では役員や担当がセキュリティ上の危険事項を発見した際に、「レッドカード」を発行している。発行は課単位で集計され、半年毎に優秀な課には報奨金（1 人 3,000 円程度）が支給される。

（７）初歩的ミスの防止策（FAX、メールの誤送信など）

本節では、個人情報保護対策の中でも、特にミスによって個人情報の漏えい等につながる可能性がある、FAX や電子メールの誤送信への対策について取り上げている。

例えば、FAX の誤送信対策としては、短縮ダイヤルを使用することを義務付けし、さらに短縮ダイヤルのメンテナンス要員を任命しているような事業者の事例（①）を紹介している他、FAX の送信時には必ず複数職員で相互に確認しながら送信することを義務付けている事例（⑦）についても紹介している。

また、電子メールの誤送信については、添付ファイルを制限している事例（④）や、自動的に送信される設定を禁止している事例（⑨）、送信後、自動的に 20 分間は送信箱に保管された後で送信されるようにすることで、誤送信に気付いた後にでも対応できるようにしている事例（⑥）なども紹介している。特に、厳格な誤送信対策として、一度付与したメールアドレスを回収し、ごく一部の外部との連絡がどうしても必要な従業者のみにメールアドレスを再交付するといった対策事例（⑩）についても紹介している。

本節で紹介している取組事例

4-(7)-①：FAX 送信は、場合分けして誤送信を回避。短縮ダイヤルメンテナンス責任者を設置
4-(7)-②：番号入力による FAX 送信禁止
4-(7)-③：印刷時に個人情報を白抜きするシステムを自社開発
4-(7)-④：電子メールの添付ファイルの制限
4-(7)-⑤：顧客情報の伝言に、専用連絡帳を使用
4-(7)-⑥：電子メールの誤送信対策
4-(7)-⑦：誤 FAX 防止のため FAX 送信は 2 名以上で確認
4-(7)-⑧：誤封入防止のため複数人でチェック
4-(7)-⑨：電子メールの自動送受信は禁止
4-(7)-⑩：電子メールアドレスは必要な従業者のみに付与
4-(7)-⑪：FAX の誤送信防止のため、広域内線番号サービスを利用
4-(7)-⑫：FAX の送信には 3 名が立ち会うことをルール化

4-⑺-①【FAX 送信は、場合分けして誤送信を回避。短縮ダイヤルメンテナンス責任者を設置】（製造業：約 334,000 人）

・A 社では個人情報が含まれる情報についての FAX 送信は、「責任者の許可」、「受信者に対する送信通知（事前）」、「通信後の受信者に対する受領確認」、「FAX 通信記録の作成」の 4 つの対応を義務付けている。

・さらに、「登録の短縮ダイヤルを使う場合」と「短縮ダイヤル未登録の場合」で対応を変えている。

・「登録の短縮ダイヤルを使う場合」は、メモリ送信は禁止し、ダイレクト送信のみで実施している。短縮ダイヤルの“メンテナンス責任者”を任命し、定期的に登録されている番号が間違っていないか確認している。

・「短縮ダイヤル未登録の場合」は、“テスト送信した上で、受領確認後に、ダイレクト送信でリダイヤル機能を使用して送信する”ことで誤送信を回避している。

4-⑺-②【番号入力による FAX 送信禁止】（信用業：100 人未満）

・K 社では FAX 送信する場合は、予め番号を短縮登録し、その上で送信することとし、番号の手動入力間違いによる誤送信を防いでいる。

・どうしても手動ダイアルしなくてはならない場合は、二人以上で作業をすることとし、かつ、管理簿に記録することとしている。また、個人情報の管理者は毎日、FAX 送信記録を確認し、管理簿と突き合わせしてチェックしている。

4-⑺-③【印刷時に個人情報を白抜きするシステムを自社開発】（信用業：100 人未満）

・K 社では契約内容等のチェックのために、個人情報を印刷する場合に印刷上の事故を防ぐため、印刷時に顧客の名前やセンシティブ情報を“白抜き”する（印字しない）システムを自社開発して運用している。

4-⑺-④【電子メールの添付ファイルの制限】（信用業：100 人未満）

・K 社では電子メールへファイルを添付する場合は、他のシステムを２回経由しないと送付できないようにして、容易に外部へファイルを送信できない仕組みとしている。

・なお、電子メール自体も、全社でアカウントは３つしか保有していない。インターネットも社内 LAN とは切り離している。

4-⑺-⑤【顧客情報の伝言に、専用連絡帳を使用】（信用業：100 人未満）

・K 社では電話等で受けた顧客情報を含む伝言は、専用の連絡帳を各自に配布して管理している。同連絡帳は、終業時に金庫等に保管し、施錠管理している。

・以前は、伝言メモを使用していたが、紛失・盗難の恐れがあるため、禁止した。

4-⑺-⑥【電子メールの誤送信対策】（情報サービス業：約 1,600 人）

・世間では、電子メールの誤送信による個人情報や社内機密情報の漏えい事故がもっとも多いため、O 社の対策としては送信先の再確認を徹底している。主な対策として次の 2 つがある。

・メーラーの設定で、送信ボタンを押してから一旦送信 BOX に蓄積されるようにし、20 分後に実際に送信されるような設定を推奨している。

・これは、“送信ボタンを押して 5 分以内に誤送信に気付くことが多い”、ということから採っている対策である。

・受信した電子メールの自動アドレス登録機能を禁止している。メーラーを自動アドレス登録とすると、アドレス帳に自分で登録した名前とたまたま同じ名前の別人から電子メールを受けた場合、同じ名前で別人のアドレスが自動登録されてしまう。自動登録された人を自分が登録した人と誤認して電子メールを送信するケースがある。この誤送信を防止するために自動登録機能の使用を禁止している。

4-⑺-⑦【誤 FAX 防止のため FAX 送信は 2 名以上で確認】
（情報サービス業（コールセンター）：約 130 人）

・Q 社では FAX の誤送信防止のため、FAX はなるべく使用しないこととしている。電話で済むことは電話で済ます。送信する場合には 2 名以上で確認しながら送信する。又は短縮登録する。短縮登録の場合は登録時に 2 名で確認する。番号は直接、相手先から入手したリストの他、電話帳などの情報源を用いて確認するようにしている。はじめて送付する先に対しては電話をかけテスト送信して確認した後送信している。前回の送信時より期間があいた送信先については、番号が正しいかどうかを確認してから送信している。

・FAX の送信者、確認者の氏名、日付を記載した手書きの管理簿と FAX 機器から出力される通信管理レポートをファイリングしている。顧客内の事業所で業務を行う場合には、顧客の理解を得て設置する。

4-⑺-⑧【誤封入防止のため複数人でチェック】

（情報サービス業（コールセンター）：約 130 人）

・Q 社では封入作業の業務がある。誤封入をふせぐためには、複数人でチェックするようにしている。

・顧客企業によっては打ち出し前に間違いを見つけ出すソフトを利用している。

4-⑺-⑨【電子メールの自動送受信は禁止】（情報サービス業（コールセンター）：約 130 人）

・Q 社では電子メールの誤送信対策として、電子メールの自動送受信を禁止している。各自の電子メールソフトを自動送受信ができない設定にするよう指示し、設定の確認を実施した。

・送信前に一旦送信トレイに入れ、宛先、添付ファイルが合っているかどうかを自分で確認し、送信している。

・添付ファイルについては、読み取りパスワードをつけている。個人情報が含まれる、機能的にパスワードをつけられないファイルは、個人が特定されない表示法（略語等）にする。タイトルの本文に個人情報であることが分かる文言は掲載しない。

・社内電子メールについてはグループウェアのセキュアメールで送信している。

・電子メールの送信についてはセキュリティ規程の監査項目に入れている。

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 60 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。

4-⑺-⑪【FAX の誤送信防止のため、広域内線番号サービスを利用】

（その他サービス業（エステティックサロン）：非公開）

・W 社では紙情報の店舗間の移動には FAX を利用する場合もある。店舗間の通話網は NTT の広域内線番号サービス「メンバーズネット」を利用しており、内線番号で FAX 送信が可能である。社外へ間違って送ることはない。

4-⑺-⑫【FAX の送信には 3 名が立ち会うことをルール化】

（そのサービス業（高齢者等生活支援）：約 30 人）

・δ社ではサービスの対象者の中には聴覚障害者もおり、コミュニケーションの手段として FAX を活用している。

・FAX は必ず 2 人で送信している。一人がダイヤルし、一人が番号確認をしている。FAX 送信簿にはダイヤルと確認の 2 名の氏名を記載し、さらにそれを確認したもう一名の氏名も記載するようになっている。

・電子メールでは個人情報は極力送信しないようにしている。送信する場合には ID 番号のみにするなど個人が特定できないようにする。

５．個人情報の消去・破棄の場面

本節では、個人情報を消去・廃棄する上で導入している機器や、実施している委託、また工夫している取組などを取り上げている。

シュレッダー等の導入による破棄や溶解等について委託などを実施している事業者は少なくなかったものの、例えば個人情報の含まれる書類の焼却等については自分で焼却場に持ち込むといった事例（①）も見られた。

また、そもそも個人情報の消去を忘れやすいことに着目して、特定の個人情報を社内サーバから取得して利用している場合、消去したことを通知しなければ自動的に個人情報消去の警告メールが送付されてくる仕組を導入している事例（③）や、メモ書きにも個人情報が残りやすいことに対する配慮として特製のメモ帳を作成して使用を義務付け、一定期間ごとに回収・焼却処理しているようなユニークな事例（⑤）について紹介している。

本節で紹介している取組事例

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
5-②：消去・破棄は６ヶ月を原則とし、必要がなければそれ以前の消去・破棄も認める
5-③：個人情報の破棄報告を行わないと、社内システムから自動で警告メールが届く
5-④：紙媒体の情報は外部事業者に委託し、自社の敷地内での溶解を義務付け
5-⑤：業務上のメモについても専用のメモ帳を使用し、最終的には廃棄

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 200 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。

5-②【消去・破棄は 6 ヶ月を原則とし、必要がなければそれ以前の消去・破棄も認める】
（小売業（百貨店・スーパー）：約 12,000 人）

・F 社では取得した個人情報を 6 ヶ月で消去することを原則としており、それ以前であっても利用しないのであれば消去するようにしている。

・個人情報が記載されたものは、月に 1 度溶解処理をしている。

・廃棄業者と廃棄のフローに関して覚書を交わしている。

5-③【個人情報の破棄報告を行わないと、社内システムから自動で警告メールが届く】
（情報サービス業：約 6,400 人）

・Ｌ社では社内システムから個人情報を含むデータをダウンロードするためには、一定の承認手続を要し、その手続の中に使用期限の入力が定められている。使用期限を過ぎても破棄報告を行わない利用者に対しては、自動的に警告メールが送付され、それでも破棄及びその報告が為されない場合は、以降の社内システムによる当該部署への情報提供はストップされる運用となっている。

・ダウンロードしたデータの使用期間は最大 2 ヶ月までである。

5-④【紙媒体の情報は外部事業者に委託】
（情報サービス業（ソフトウェア）：約 400 人）

・N 社では環境 ISO14001 取得の関係で、紙はシュレッダーを利用せず、溶解又はリサイクル処理をしている。リサイクル処理の場合、担当者立会いのもと、自社の敷地内で行っている。個人情報等重要書類については、溶解処理をしている。

・社内にごみ箱はなく、すべての個人情報が含まれる書類は溶解処分用の BOX にいれるようになっている。この箱は郵便ポストのような形状であり、入れたら取り出すことはできない。専門業者のみが溶解処分時に箱をあけることができる。

・溶解処分は、業者の溶解処理場で処分している。処理方法及び個々の処理については、契約時及び個々の処理確認書で確認している。

5-⑤【業務上のメモについても専用のメモ帳を使用し、最終的には廃棄】

（その他サービス業（債権回収支援）：約 30 人）

・γ社では業務上、どうしてもメモが発生するが、メモに記載した個人情報の適切な管理まではどうしても対応しきれず、メモから個人情報の漏えいにつながる危険性を強く認識している。

・専用のメモ帳を使用している（メモ帳の外のバインダーにジッパーがついており、ジッパーで完全に閉めることができるもの)。業務上は必ずこのメモ帳を使用するようにしており、メモ帳についても使用後は閉じた状態で本社に送付し、一斉廃棄するようにした。

６．個人情報の点検・監査の場面

本節では、規程等の遵守状況や、管理状況を確認するために定期的に実施される監査に関する取組について取り上げている。

特に個人情報保護のための監査として、ユニークな事例としては、例えば単に監査を実施するだけでなく、社内の異なる部門や部署が相互に監査を実施することで業務についての一定の理解を持ちながら実効性のある監査を実現している事例（⑪）も紹介している。

また、一定以上の職歴のある従業者を中心に監査を実施しているような事例（②）、さらには外部の弁護士や学識経験者等による外部委員会を設置して厳格な監査を実施してもらっているような特徴的な事例（⑤）も紹介している。

本節で紹介している取組事例

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
6-②：監査は一定の役職以上のベテラン職員が担当。問題が見られた場合は短期間で是正計画の策定と再監査を実施することで実効性を高める
6-③：3ヶ月に1度、課単位でコンプライアンスについて自己点検。気づき効果をねらう
6-④：監査は業務監査部門が実施
6-⑤：外部有識者による委員会の設置
6-⑥：リスク管理室による監査
6-⑦：プロジェクト単位で、顧客企業を訪問して常駐しているチームに監査を実施
6-⑧：プロジェクトごとにチェックシートを作成。ヒアリングに基づく実態把握を実施
6-⑨：テレビ会議を利用した監査を検討
6-⑩：トップの指示により、年に4回の監査を実施
6-⑪：監査は異なる部門の監査担当者が複数で実施
6-⑫：監査手法をとった品質指導を実施
6-⑬：用途やチェックの視点に応じて3種類の点検を複層的に実施

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。

6-②【監査は一定の役職以上のベテラン職員が担当。問題が見られた場合は短期間で是正計画の策定と再監査を実施することで実効性を高める】（卸売業：約 200 人）

・E 社では年に１回、内部監査を実施している。15 部署について、2/1～2/14 までの期間を要して実施した。職場の点検だけでも 1 部署 2.5 時間程度掛けて点検を行った。

・監査チームのリーダーは一定の役職以上（部長等）のベテラン社員が担当し、実際に監査員が現場まで立ち入りを行ってチェックをした。

・監査結果については、即日で「適合」、「不適合」、「観察」の評価を下している。「不適合」になった場合には、10 日以内に「是正計画書」を提出し、その計画書を受けて監査員が 18 日以内に「フォローアップ監査」を実施する。また、フォローアップ監査の結果については、23 日以内に「不適合報告書兼是正処置報告書」を提出することになっており、問題点を単なる注意で終わらせないようにしている。

・「観察」は不適合とは言えないが、改善したほうが個人情報保護のためにより望ましいと考えられる場合に出される。

・平成 18 年の監査では、14 件の不適合と 8 件の観察が報告された。

＜E社で使用されている監査のための書式＞

文書コード：P－
[様式－3]

個人情報保護に関する監査規定

確認	作成
監査責任者	内部監査員

頁： 25

内部CP監査チェックリスト

株式会社

監査実施日　　年　　月　　日
被監査部門
監査チームリーダー

○監査基準：JIS Q 15001：1999規格

要求事項	チェック項目	判定	質　問	コメント
4.4.5 個人情報に関する情報主体の権利				
4.4.5.1 個人情報に関する権利	□ 個人情報に関する権利の規定	OK	☑ 情報主体から自己の情報について開示要求があった場合，合理的な期間内に応じるように定めているか。	
		△	☑ 情報主体から自己の情報について開示要求があった場合，情報主体の本人確認を行っているか。	本人の確認方法を定め記載する必要がある また，確認方法と判断結果を記録に残すことも必要。それによっては，要求日より7日以内では難しいこともある
		OK	☑ 開示の結果，誤った情報があり，情報主体から訂正又は削除を求められた場合は，合理的な期間内にこれに応じるように定めているか。	
		△	☑ 情報主体からの要求により，訂正又は削除を行った場合は，可能な範囲内で当該個人情報の受領者に対して通知を行うよう定めているか。	受領者に対する通知についての記載を規定に入れる必要がある
		OK	☑ 情報主体から自己の情報についての開示，訂正又は削除を求められた場合の理由を記録として保存しているか。	

判定欄：適合…OK，重大な不適合…××，軽微な不適合…×，観察…△　　保管期間：3年
（不適合の場合は証拠事実を記入）
配布先：被監査部門の実務責任者，　　保管部門：

文書コード：
[様式－4]

不適合報告書兼是正処置報告書

個人情報保護に関する監査規定

不適合の指摘

被監査部門	場所・職場	報告書番号
管理責任者，推進事務局	本社　3F　会議コーナー	16

監査日・指摘日	適用文書
	P-2040　個人情報保護に関する教育規定

不適合事項　（※ なしの場合は斜線を引く）

CP教育訓練実施報告書，理解の度合いで「ほぼ理解した」と
あるが，このレベルでは不充分である

不適合の理由（証拠）　様式－3
「CP教育訓練実施報告書」に記述の「自覚度の確認」で
受講者への質問とあったが，どんな内容の質問により
判断したか不明である

是正勧告
「ほぼ理解した」レベルの場合，年度がわりに，
初任時教育の再教育を実施することが望ましい

指摘の区分	適用条項該当箇所	監査員	実務責任者	是正計画提出日
・不適合 （重大） （軽微） ・（観察）	P-2040 3. 2) 教育実行			2月27日

配布先：被監査部門の実務責任者　　保管部門：

是正計画書

不適合の原因　実務責任者及び講師は，実施した教育内容について終了直後に自覚度を確認し，記録に記述した。（今後は質問の要点を記載ならびに，理解不十分であった時の対応も記録に残し再教育も実施したい）

是正処置の具体的項目	担当者	スケジュール				
指摘のあった「教育」について再教育を実施する		計画提出 2/25	→	再教育実施3/4まで	→	フォローアップ監査3/6まで

是正責任者	効果確認方法	目標（値）
管理責任者	目視により実施記録を確認する	

予算額　0 円

再発防止

再発防止処置　教育実施責任者及び講師は，自覚度の確認「ほぼ理解した」程度であれば，不充分であるとの判断で理解度がアップするよう資料など揃えて再教育を実施する。

効果確認

確認日	調査対象期間
3月6日	2003年3月6日 ～ 2003年3月6日
経費	確認方法
0 円	目視と受講者の確認

確認結果　教育の実施報告書と受講者に聞き取りをして自覚度の確認ができ以前より理解されていることがわかりました　　添付資料：（有）・無

次回監査での効果確認	確認	作成
	監査責任者	監査チームリーダー
要　・　（不要） （改善中）　（完了）		

保管期間：3年

6-③【3 ヶ月に 1 度、課単位でコンプライアンスについて自己点検。気づき効果をねらう】（信用業：約 900 人）

・J 社では監査部門が実施する監査とは別に、「コンプライアンスチェック」がある。これは、課単位で 3 ヶ月に 1 度コンプライアンス全般について自己点検するものである。約 80 項目を責任者が○△×で評価をする。

・自己監査の結果、できていないとした項目については、いつまでにやるのかを記載する。

・コンプライアンス課はこの自己点検について、本当にできているかどうかについてのチェックは行っていないが監査部門の監査時にチェックしている。評価ではなく気づき効果をねらっている。

・自己点検については、各部署は紙でチェックしている。紙をコンプライアンス課がとりまとめて集計し、結果を各課へフィードバックしている。

6-④【監査は業務監査部門が実施】（信用業：約 900 人）

・J 社では監査は社内の業務監査部が実施する。項目が多いため 1 支店一週間ほどかかる。2 チーム体制で全国を回っている。

6-⑤【外部有識者による委員会の設置】（情報サービス業：約 1,600 人）

・O 社では外部有識者 5 名により構成される「情報セキュリティアドバイザボード」を設置している。大学教授、弁護士、コンサルタントなどが参加している。

・委員会は、2 ヶ月に 1 度開催（昨年度は毎月開催）され、現在のセキュリティ対策の取組状況や対策の問題点などについて報告を行い、対策についてアドバイスをもらう形式で運営している。また、年に 1 回、情報セキュリティアドバイザリボードから提言書が社長宛に提出され、情報セキュリティ対策の評価及び提言を受け次期の対応に活用している。

6-⑥【リスク管理室による監査】（情報サービス業：約 1,600 人）

・O 社では監査室において情報セキュリティ監査を実施しているが、リスク管理室でも定期的にチェックを実施している。

・年度はじめに、リスク管理室は本年度の情報セキュリティチェック基本計画を策定して社長承認を受けセキュリティチェックを行っている。毎年、情報セキュリティに関するチェックポイントを決め、現在のリスクにあって効果的なチェックをするために毎年チェックシートを作成している。

・月に 2～3 部署程度を回り、半年で全国の部署を回れるような頻度で回っている。

6-⑦【プロジェクト単位で、顧客企業を訪問して常駐しているチームに監査を実施】

（情報サービス業：約 350 人）

・P 社では幾つかのプロジェクトを選定し、顧客企業に常駐している場合であっても立ち入り監査を実施している。特に問題があったプロジェクトや、扱う情報のセキュリティレベルが高いプロジェクトが対象となることが多い。

6-⑧【プロジェクトごとにチェックシートを作成。ヒアリングに基づく実態把握を実施】

（情報サービス業：約 350 人）

・P 社ではプロジェクトごとに『顧客の要求する水準を維持できているのか』という視点で監査を行う。まず顧客企業に話を聞きに行き、要求されるセキュリティ水準やポイントとなる管理の方法などを確認した上で監査を実施する。

・監査の際には、事前に、プロジェクトごとの個別チェックシートを作成した上で、実施している。また、現場を見回るだけでなく、プロジェクトメンバーの数人を選んで個別ヒアリングを実施して事情を確認している。

6-⑨【テレビ会議を利用した監査を検討】

（情報サービス業（コールセンター）：約 130 人）

・Q 社では半年に一度、社内、センター、入館許可がとれた顧客先で監査を実施している。定められた記録や教育がなされたかどうかを確認している。

・フォローアップ監査については後日書面で実施している。実際の運用状況については半年後に再度確認している。

・現在、テレビ会議を利用した監査を検討している。すべての項目について現地で監査を行うことにより、事前にテレビ会議で監査項目を開示し、実施に支障のない項目の監査はテレビ会議で終えてしまう方が効率的である。同社では、テレビ会議を積極的に業務に活用しているため、抵抗が小さい。

6-⑩【トップの指示により、年に 4 回の監査を実施】

（複合（情報システム／製造）：約 500 人）

・R 社では専任の監査部門がある。ISMS に詳しい者が監査を行っている。

・この他に内部監査人として社内 33 名、グループ会社 14 名が担当している。内部監査人は、ISO14001 と 9001 の監査ができる人が任命される。

・社長の指示により、監査を年に 2 回から 4 回に増やした。

・個人情報保護の担当者が、今までに 2 回抜き打ちで全事業所を点検している。朝の誰もいない時間帯に訪問し、問題があればレッドカードを発行する。

・自己チェックとして従業者が互いにチェックし合う制度がある。

6-⑪【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。

6-⑫【監査手法をとった品質指導を実施】

（その他サービス業（印刷・広告）：約 11,000 人）

・X 社では監査手法で品質事故防止のための指導をしている。従来は「品質事故」とされていたものが、「個人情報保護法違反」になるケースがあるため、品質を向上させることは個人情報保護の推進のためにも重要であると考えている。

・この監査は、書類が整っているかどうかだけの監査ではない。品質管理の担当者が現場に出向き、1 部署あたり最大 15 人日ほど実際の作業に立会いながら個人情報の管理方法をチェックするものであり、製造実務に係わる監査である。例えば品質保証のルールとその遵守状況、機械停止時の操作、目の動き、ゴミ箱の形、服装、といった細かいことまでチェックし、不適切な点があればその場で指導する。

・協力会社に対しても監査を毎年 1 回行っている。結果によっては認定の取消をする場合もある。

・また、従業者、パート、アルバイトにアンケートで、現在実施している作業の中での不安や工夫している点を聞き、監査項目を抽出した。

6-⑬【用途やチェックの視点に応じて 3 種類の点検を複層的に実施】

（その他サービス業（ダイレクトメール等）：約 600 人）

・Z 社では点検は以下の 3 種類を行っている。

・早朝抜き打ち監査：施錠のチェック、個人情報が記録された書面や媒体が机の上に放置されていないかなどを半年に 1 度程度の頻度で早朝にチェックする。不適合があった場合は改善報告書を提出させ、その 1 ヶ月後にフォローアップとして再び点検を行う。監査で 2 回不備が発見されると、部長が始末書を提出する。上期の点検で問題がない場合は、下期の点検は免除している。

・オフサイトモニタリング：WEB の使用状況のログをチェックしている。休日にわけもなくネットワークを利用していないか、利用禁止のサイトを閲覧していないか、など

を監査する。
・事前通告の点検：データの授受が適切にできているか、データの受け渡し時に顧客の証印をもらっているか、アンケートの枚数確認をしているか、などをチェックする。

７．個人情報に関する苦情処理・開示請求対応の場面

本節では、個人情報に関する本人（情報主体）からの問い合わせや苦情、開示請求に効果的・効率的に対応するための取組について取り上げている。

事業者ヒアリングからは、多数の苦情や開示請求が寄せられているという声は多くなく、実際の対応というよりも、苦情や開示請求が寄せられた際の対応として、どのようなことに備えているかという視点からの事例である。

本節で紹介している取組事例

7-①：開示請求と問い合わせの明確な分類

7-②：受託案件の問合せは委託元へ報告

7-①【開示請求と問い合わせの明確な分類】（製造業：約 334,000 人）

・A 社では会社単位で個人情報に関する問い合わせ担当窓口を開設しており、どこに問い合わせをしても情報保有部署に繋がる仕組みを構築している。

・顧客が個人情報を提供した部署の窓口に問い合わせを受け、本人確認を各部門（個人情報保有部署）で対応する。

・「開示請求」と「問い合わせ」を明確に区分しており、「開示請求」に関しては手数料を取る。

7-②【受託案件の問合せは委託元へ報告】（その他サービス業（印刷・広告）：約 11,000 人）

・X 社では問合せに対しては、受託案件についても受け付けている。本人が、同社で個人情報を処理していると知っていて、問合せをしてきた場合には、事実関係を調査し、委託元へ報告する。委託元に無断で開示することはない。ただし、通常の委託案件で同社の関与が一般消費者にわかることはほとんどない。

８．個人情報に関する事故（漏えい・き損等）発生の場面

本節では、個人情報に関する漏えい、き損等の事故発生時に迅速且つ適切に対応するための方策や、顧客に対して適切に対応を行うための取組などを取り上げている。

例えば、セキュリティ事故発生時には担当役員の携帯電話に 24 時間 365 日必ず電子メールが自動送信されるような仕組を構築している事例（①）などについて紹介している。

本節で紹介している取組事例

8-①：セキュリティ事故が発生した際には、発生日時を問わず（24 時間 365 日対応）担当役員の携帯電話に事故発生の通報電子メールが転送され、迅速・適切な対応を可能としている

8-②：個人情報漏えい事故対策訓練を予定

8-③：ファイル共有ソフトでの情報流出時には個人情報の含まれるファイルの検索を専門家に委託し、“専門家でも特定しづらくなった”ことをもって顧客を説得

8-①【セキュリティ事故が発生した際には、発生日時を問わず（24 時間 365 日対応）担当役員の携帯電話に事故発生の通報電子メールが転送され、迅速・適切な対応を可能としている】（情報サービス業：約 6,400 人）

・Ｌ社では情報セキュリティ事故発生の場合に誰が何をするか、マニュアルを用意している。

・いち早く正確な事故情報を把握することに重点を置いている。

8-②【個人情報漏えい事故対策訓練を予定】（情報サービス業（ソフトウェア）：約 2000 人）

・M 社では平成 18 年 11 月に漏えい事故を想定した訓練を実施予定。個人情報漏えい事故の発生を想定し、緊急対策本部を設置し、顧客からの問合せ窓口や営業対応、報道対応などを訓練する。訓練は事前に各部署に連絡し、協力を得る。

・事故時の対応については規程で決まっている。事故が発生することは望ましくはないが、いざという時に社内的な混乱を起こさないようにしたい。

8-③【ファイル共有ソフトでの情報流出時には個人情報の含まれるファイルの検索を専門家に委託し、“専門家でも特定しづらくなった”ことをもって顧客を説得】
（その他サービス業（教育、学習支援）：約 1,200 人）

・S 社ではファイル共有ソフト（Winny 等）で情報流出事故があった際には該当するすべての方にお詫びの手紙を送った。

・ファイル共有ソフトに関して 1 ヶ月間、監視を専門家に依頼して行った。監視を続けるにつれて、個人情報を含むファイルの検索時間が延びていったので、それを報告した。

・『検索によって個人情報が発見される可能性が完全に無くなった』ということは言えないため、検索時間が相当程度長時間化し、当該ファイルが専門家でさえもネットワーク上で特定することが容易ではなくなったことを示し、リスクが相当程度縮減したことを説明することで、顧客の納得を得ることができた。

・事故発生時の対応、情報伝達手順は定まっている。事故後の対処はマニュアル等の原則に従いつつもケース・バイ・ケースである。

９．その他の場面

本節では、前述の 1～8 の視点では分類されないような事業者の特徴的な取組を取り上げている。

本節で紹介している取組事例

9-①：テナントとは個人情報の利用形態によって 3 種類の覚書を使い分け
9-②：複数のマニュアルのサマリーを集めたマニュアル集を作成
9-③：社内報への写真・個人名の掲載を説明会で説明
9-④：環境への配慮と個人情報

9-①【テナントとは個人情報の利用形態によって 3 種類の覚書を使い分け】

（小売業（百貨店・スーパー）：約 12,000 人）

・F 社では取引先との契約は、①同社のみの所有・利用　②共同利用　③共有　の 3 種類に分類している。「共同利用」は、情報は同社に帰属するが共同で利用するものである。「共有」は情報が同社と取引先に帰属するものであり、取得時に「同社及び○○（取引先）が利用する」などの文言を文書に盛り込む形で顧客の同意を取っている。

・取引先（店舗）の監督は、管理チェックシートによって行っている。取得した顧客名簿を毎日チェックしている。取引先の販売員全員に個人情報保護に関する誓約書を提出させている。

＜テナントに対する顧客情報管理状況の管理チェックシート（一部抜粋）＞

作成日　　年　　月　　日

顧客情報処理　手順確認書

店　　販売部
ブランド
ブランドチーフ

店頭で顧客名簿を取得するブランドにつきましては以下の項目をご記入下さい。

Ⅰ．顧客名簿の取得について（レ点チェックをして下さい）

1）取得する個人情報の項目は何ですか。(該当するものはすべてレ点チェックをして下さい)

□氏名　□住所　□電話番号　□生年月日　□性別
□メールアドレス　□職業　□年収
□その他商品特性上取得している項目がありましたら具体的にご記入下さい。

2）取得の際に、顧客からどのように利用目的の同意を得ていますか。

□口頭でのみ確認　□名簿に利用目的を記載し、口頭で確認
□名簿自体にチェック項目を設け、口頭で確認し記入する
□その他（　　）

3）利用目的の文言は具体的にどのような内容ですか。(口頭のみの場合も含む)

Ⅱ．顧客名簿の管理について（レ点チェックをして下さい）

1）名簿は検索できるよう体系的に管理していますか。(販売員別、日別、あいうえお順等)

□はい　□いいえ

2）名簿を施錠できる場所に保管していますか。

□はい　※鍵の管理責任者をご記入下さい（　　）

9-②【複数のマニュアルのサマリーを集めたマニュアル集を作成】（信用業：約 900 人）

・J 社では規程類の整備を進めた結果、マニュアルが多くなったため、各マニュアルの要点を手軽に参照できるマニュアル集を作った。ポイントは何かということがわかるサマリーを掲載している。

9-③【社内報への写真・個人名の掲載を説明会で説明】

（情報サービス業（ソフトウェア）：約 400 人）

・N 社では社内での個人情報保護の説明会時に、社内報での写真・個人名の掲載について説明している。個人情報保護の重要性とともに社内コミュニケーションの重要性も説明している。

・本説明会時に、同意書を取っている。

9-④【環境への配慮と個人情報】

（情報サービス業（ソフトウェア）：約 400 人）

・N 社では、環境への取組もグループ会社全体として実施している。

・環境はサイトごとの管理であるため、同一ビル内はすべて同じ基準で実施しなければならない。紙の書類をすべてリサイクル処理・溶解処分とするのはその一環である。

・個人情報保護と環境への対応が合致しない場合がある。たとえば、HDD の処分については環境保護では消去ソフトの利用による再利用が推奨されているが、個人情報保護としては破砕となっている。このような場合には、環境の担当者と個人情報の担当者が対応を協議し、適切な取扱方法を定める。