Ⅴ．事業者ごとの個人情報保護対策取組事例

Ⅴ．事業者ごとの個人情報保護対策取組事例

A. 製造業　A 社

事業概要	電化製品等の生産、販売		
従業員数	約 334,000 人	プライバシーマーク取得	あり
保有個人データ件数	約 4,700 万件		

１．個人情報に関する概要

（１）保有個人情報件数、個人情報の種類、個人情報の利用目的

・約 4,700 万件

（２）個人情報保護担当部署

・情報セキュリティ本部（平成 16 年設立）

（３）個人情報保護管理者の有無・位置づけ

・CPO を置いている。CPO は副社長である。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・グループで 14 社がプライバシーマーク取得済み、23 社が今年度取得予定。

（５）個人情報保護に向けた取組経緯

・平成 13 年 11 月：個人情報保護基本規程を制定
・平成 16 度　　：情報セキュリティ本部を設置
・平成 16 年 6 月：　グループ全体の個人情報保有状況や管理状況などの実態を調査、使用していない個人情報を削除
・平成 16 年 10 月：個人情報管理ガイドラインの制定と個人情報登録制度の開始
・平成 17 年 4 月：法律で求められている公表事項のホームページへの掲載と個人情報お問合せ窓口の設置
・平成 17 年度：全社一括プライバシーマーク取得に取組
・平成 18 年度：個人情報保護グローバル・ルールの制定に向けて取組中

・同一の個人情報を複数媒体で保有していて個々の媒体の管理がおざなりになりがちであったこと、個人情報の消去も個々の営業職員に委ねており対応がまちまちだったことが漏えい、紛失につながると考え、管理の一元化により紛失・漏えいの可能性を極小化し、万が一紛失や盗難に遭遇した場合も自動的に個人情報が消去されることでその後の悪用を防止することにした。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・特になし

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・情報セキュリティ本部を平成 16 年に設置し、組織体制で個人情報管理を行っている。情報セキュリティの推進委員会がある。

（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）

・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。

・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。

・入手窓口によって個人情報の取扱ガイドライン・ルールを策定している。（WEB、モニター、営業活動、CS、人事の 5 つ）

・長期保有製品の個人情報については、各ドメインでなく本社で管理することを検討している。

（２）個人情報の取得

（重要度の高い個人情報の取得時のチェック）

・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。

・個人情報の取得時は本人の同意を得ている。グループ間での 利用の場合、同意取得時の文言は「グループで利用する」とし、各社名は明記していない。

（３）個人情報の利用（第三者提供を含む）

・特徴的な取組はなし

（４）個人情報の管理

①情報の管理体制

（個人情報の重要度にあわせた管理方策の分類）

・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（事業領域）ドメイン CPO に承認を受ける。

・個人情報保護のため、営業職員がベルトに直接つけることができる専用のケースを作成し、物理的な紛失対策も実施している。

・どうしても必要な紙媒体の「作業指示書」は姓のみを表示すること、年・名前・住所・電話番号は非表示として万が一盗難に遭遇した場合に備えている。

②従業者への教育方法

（イントラネットのログイン画面のトップに個人情報保護ルールを掲載）

・イントラネット利用時の初期画面（ログイン画面）に毎日個人情報保護の情報を掲示し、必ず職員が一日に一度は個人情報に留意するようにした。他にも、社内にポスターを貼ったり、パソコン盗難啓発ステッカーを配布したりして職員の啓発を行っている。

（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）

・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。

・自社独自で業務内容に沿ったセキュリティガイドブックを作成・配布している。

③盗難対策

（記憶媒体の情報が記録から 48 時間後に自動消去）

・修理等を担当する外回りの職員が、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、長期間外回りの職員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）。

（車上荒らし対策の実施）

・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ノート PC の安全対策

・特徴的な取組はなし

⑤外部委託先管理

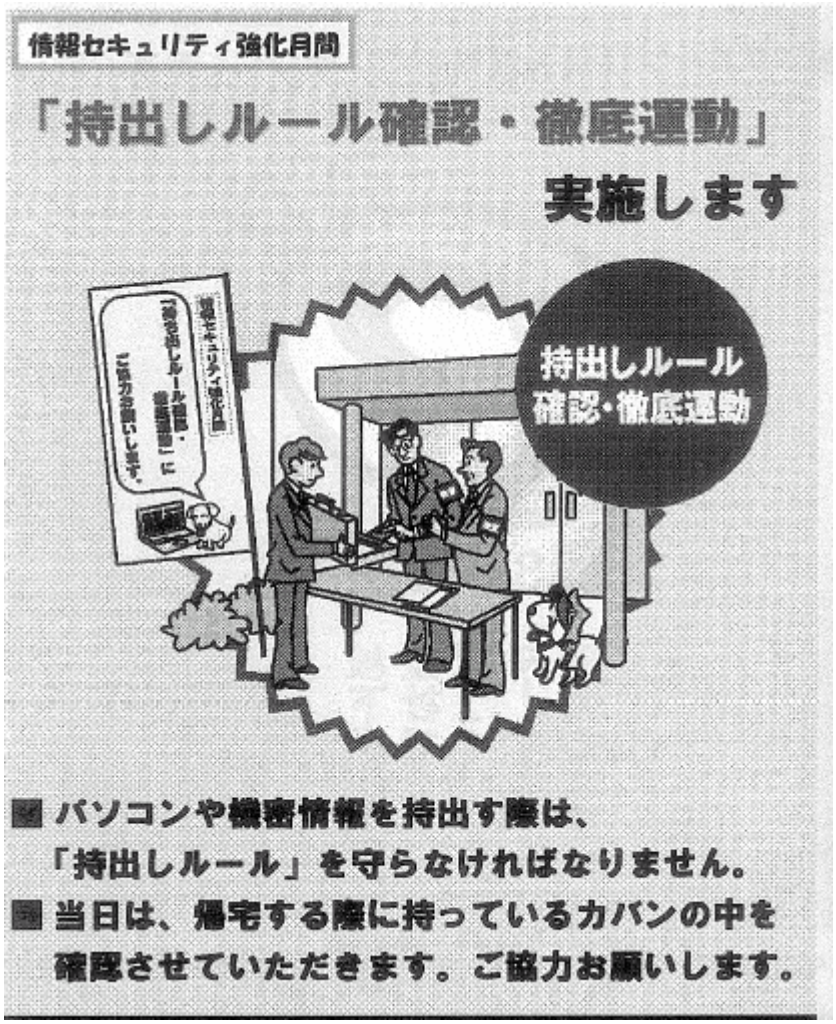
・委託先はチェックシートを用いて管理している。
・まず「外部委託先選定チェックシート」で委託するのに適切な個人情報管理が可能かを確認（14 項目）する。加えて、委託先での管理状況を、「委託先管理チェックシート」によって行っており、契約の内容や委託先の個人情報遵守状況などを二重にチェックするようになっている。
・再委託は基本的に禁止だが、やむを得ず再委託、再々委託がある場合は、本体と同じルールを適用させ、一次委託先の責任で監視させるようにしている。

⑥日常点検・確認の方策

（全社一斉手荷物検査の実施）

・「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。

図表　「全社一斉手荷物検査」の実施を呼びかけるポスター



⑦初歩的ミスの防止策

（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の設置も行う。）

・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。

（５）個人情報の消去・破棄

・保管期限を過ぎた個人情報のうち、「個人情報厳秘」に該当する個人情報はメディアを物理的に破砕するよう定めている。
・インベントリー・リスト（個人情報保管台帳）を年に 2 回作成しており、そこでデータの削除を確認する。
・修理や保証に際して個人情報を取得した場合、取得から一年を経過した分は製品の情報だけを残し、個人情報は削除する。

（６）個人情報の監査

・通常の社内監査に加え、職場・事業所ごとに実施する「自主監査」も年に 2 回実施している。

（７）苦情処理・顧客対応

（開示請求と問い合わせの明確な分類）

・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）でして対応する。

（８）事故発生時の対応

・特徴的な取組はなし

以　上

B. 電気・ガス・水道業　B 社

事業概要	電力の生産・販売		
従業員数	約 38,000 人	プライバシーマーク取得	なし
保有個人データ件数	約 3,000 万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・約 3,000 万件。

・顧客の氏名、住所、電話番号、電気料金などの情報を保有している。

（２）個人情報保護担当部署

・店所や部門に個人情報管理責任者（部門長、店所長）を定め、その下に個人情報の担当（兼任）を置いている。

・個人情報保護の全社事務局はシステム部門の 2 名が兼任で行っている。

・コンプライアンスやリスク管理は法務部門が担当しており、連携を図っている。

（３）個人情報保護管理者の有無・位置づけ

・CPO は設置していないが、前述の個人情報管理責任者の上に、個人情報保護総括管理者と個人情報保護管理者を定めている。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・認証は特にない。

（５）個人情報保護に向けた取組経緯

・平成 2 年に電気事業連合会が定めた「電子計算機処理に係る個人情報保護のためのガイドライン」に沿って取り組んできた。この時点で「電子計算機処理」が中心であったこともあり、システム部門が担当となった。

・平成 10 年の告示及びガイドラインの改定を契機に、社内で「電子計算機処理に係る個人情報保護のための実践遵守規程・マニュアル」を制定した。

・個人情報保護法の成立を受け、「従業者の啓発」、「ルールの強化」、「対応体制の整備」の 3 点を柱として準備を進めた。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・電気供給に関連した顧客データを大量に保有しており、顧客データの対象は電気供給

地域内の居住者が中心である。
・検針や電気料金徴収のため、顧客データを定期的に社外へ持ち出すことが必要である。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・個人データの取扱台帳を作り、管理・メンテナンスしている。
・社内規程は、保護法の全面施行に合わせ、法律・経済産業省のガイドライン・電気事業連合会のガイドラインを網羅してマニュアルを作成した。個人情報の保護に関する全社規程、個人情報の保護に関する全社マニュアル、個人情報の保護に関する各部門のマニュアル、という体系になっている。

（２）個人情報の取得

・特徴的な取組はなし

（３）個人情報の利用（第三者提供を含む）

・大手電力会社とグループ会社間での情報の共同利用はしていない。子会社からも、情報の融通の依頼は来ない。

（４）個人情報の管理

①情報の管理体制

・電話受付を行うカスタマーセンターの従業員従業者は個人情報にアクセスしやすい環境にあるが、例えば、あるカスタマーセンターでは、入館時に全員が透明のバッグに手荷物を入れ、情報の持ち込み・持ち出しができないようにしている。
・物理的安全管理措置としては、入館の警備員配置、機器の物理的な施錠やワイヤーロック、技術的安全管理措置としては、暗号化などを行っている。
・個人情報を社外に持ち出す際は、上長の了解や管理台帳への記入などが必要になる。
・検針員は、ハンディ端末を持っている。検針日毎に数百件程度のデータをダウンロードして入れ替えている。ハンディ端末にはパスワードがかかっており、メモリは特殊なビスで格納されている。

②従業員従業者への教育方法

・周知徹底のため、責任者に対して集合研修を行った。全従業員従業者に対する周知は年に１度程度のｅラーニングによって行っている。また、逐次、社内イントラネットに個人情報情報保護に関する情報を掲載したり、資料を配布したりしている。関係会

社についても、e ラーニング教材を配布し、受講してもらっている。
・検針員、集金員とは「個人事業主」というかたちで委託契約を結んでおり、月に 1 度程度の内勤日を利用するなどして研修を行っている。

③盗難対策
・パソコンのワイヤーロックや暗号化システムを導入している。

④ノート PC の安全対策
・ノート PC の管理方法をマニュアルにしている。

⑤外部委託先管理
・委託先の選定基準を整備し、それに見合う委託先を選定するようにしている。発注の際は個人情報の保護に関する契約を交わしている。

⑥日常点検・確認の方策
・特徴的な取組はなし

⑦初歩的ミスの防止策
・送信・送付ミスの回避については、宛名ミスが多いため、封筒と中身について複数人が確認するようにしたり、メールマガジンなど同報の電子メールの送信先には BCC（ブラインドカーボンコピー）のみ設定可能なメニューも用意したりといった取組をしている。

（５）個人情報の消去・破棄
・保有期間を決め、不要になったものを削除している。
・廃棄は裁断・溶解などで処理している。

（６）個人情報の監査
・監査部門の活動の一環として、個人情報保護についても行ってもらっている。
・システム部門独自のモニタリング、店所や部門での監査も行っている。

（７）苦情処理・顧客対応
・苦情があった場合の受付、開示手順を定めてマニュアルに記載している。どのような開示があったのかの調査も実施している。
・料金等の問い合わせの際、本人確認はカスタマーセンターで、数項目の質問によって行う。書面により回答するような機密性の高い情報開示を求められた場合は、運転免

許証などの提示を求めるようにしている。

・開示の手数料は、10 枚以上の請求の場合のみ 1 枚 60 円としている。10 枚未満の場合は無料である。これまでに手数料が発生したケースはない。開示請求は居住証明を得る目的のものが中心だが、数は少ない。

（８）事故発生時の対応

・情報漏えいの際の対応をマニュアルで定めている。事故発生部署が事実確認を行い、本店の事務局（システム部門）が集約し、最終的な判断を担当役員が行う。

・対応は、顧客への謝罪と社外広報、官庁への報告を行う。

・事故事例を踏まえ、再発防止策を検討している。

以　上

C. 電気・ガス・水道業　C 社

事業概要	大手ガス供給業者からのガス事業受託全般、リフォーム業		
従業員数	約 60 人	プライバシーマーク取得	あり
保有個人データ件数	約 7 万件		

１．個人情報に関する概要

（１）保有個人情報件数、個人情報の種類、個人情報の利用目的

・約 7 万件

（２）個人情報保護担当部署

・担当は店長である。

（３）個人情報保護管理者の有無・位置づけ

・個人情報保護管理者は設置している。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマークを取得済みである。

・認証取得のきっかけとなったのは、IT 化に関する他社の勉強会に参加し、触発されたことである。取得には 1 年半程度の時間が要した。

（５）個人情報保護に向けた取組経緯

・大手ガス会社を経由して委託修理を行う場合と、自社に直接顧客から連絡がある場合があり、その 2 つの経路で取得した個人情報の扱いが煩雑であった。そのため、認証の取得を通して整理しようということになった。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・都市ガス会社など規模が大きい企業は、データが多く、個人情報保護の取組をすることが困難である。特にガスの場合は、古いシステムを使っているため、現在の標準的なシステムに変えてセキュリティ対策を強化することが難しい。

・顧客の使用機器の情報を基に修理や点検を行うが、情報を持っていなくても、情報を持っていても苦情を受けることがある。個人情報の扱いが難しい業界である。

・作業のために紙媒体で情報を社外に持ち出すことが多い。これは、顧客に署名を求めることが多いためである。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・個人情報保護の取組を開始することになった際、従業者全員を収集して説明会を行った。これによって意識が高まり、取組を促進できた。

・プライバシーポリシーは、コンサルタントによる支援と他社の例を見て作成した。

（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）

・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。

（２）個人情報の取得

・電話による取得が多いため、通常はホームページの掲載事項を参照してもらうようにしている。リフォーム事業においては顧客から個人情報を直接的に収集するため、利用目的を記載した書類を渡している。

・ガス事業においては、委託元のガス会社から個人情報を受け取る場合と、自社に顧客から直接連絡がある場合がある。どちらの場合も顧客は自社のことを、委託元のガス会社と認識している。

（３）個人情報の利用（第三者提供を含む）

（顧客宅を訪問時に営業資料を配布し、郵送等は行わない）

・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。

（４）個人情報の管理

①情報の管理体制

・社内に個人情報を置くことを規程で禁止している。作業員は車外に出るときは必ず個人情報を持ち出し、置き去りにしない。

・建物の構造が物理的に厳重でないため、受付を設け、訪問者は氏名と所属を記入した上で来訪者カードを首からかけるようにした。最大委託元の幹部であっても、記入してもらうようにしているが、それについてはむしろ評価されている。常時窓を開け、外の様子が見えるようにしている。取組後に改装を行った支店は受付で来訪者を管理できるつくりにしている。

②従業者への教育方法

・新入社員に対しては、個人情報保護研修を義務付けている。

③盗難対策

・車の中に情報を置かないようにしている。

・営業所には警備システムを入れている。

・机の上に情報を置かないようにしている。

・入退出の管理をしている。

・携帯電話は、遠隔でデータが消去できるものを利用している。

④ノート PC の安全対策

・ノート PC は、拠点を動く必要がある社長のために 1 台と、もう 1 台の計 2 台しか保有していない。 1 台は、委託元のガス会社からの依頼で行っている特定の業務に利用しており、その日の作業に必要な情報のみを格納している。ノート PC の利用を禁止していることに関して、特に従業者からの不満はない。

・データを持ち運びできるメモリ媒体の使用は、管理職以上の許可があるもの以外は、禁止している。

⑤外部委託先管理

・委託先の職人の方には、住所、氏名、設計などの情報を渡すが、情報の重要性を説明し、漏えいがないよう指導している。情報はコピーで渡し、利用後は廃棄するように伝えている。

・委託先に対しては、個人情報に関する教育のための総会を年に 1 度行っている。

⑥日常点検・確認の方策

（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する）

・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。

・作業員は、1 日 12～13 件の紙の情報を持ち出す。外回り開始時に、誰がどの情報を持ち出したかを把握し、帰社後に持ち帰ったデータと照合する。

⑦初歩的ミスの防止策

・特徴的な取組はなし

（５）個人情報の消去・破棄

・シュレッダーの導入は個人情報の話題が社会的になる以前から行っていた。機械も高度で丈夫なものを利用している。

・個人情報を格納するディスク、書類は、法律上の保存期間終了後に溶解処理している。

・個人で管理する個人情報は半年以内に破棄するという規程がある。

（６）個人情報の監査

・領収書は毎朝チェックしている。

・IT 委員会が個人のパソコンをチェックしている。

・車輌委員会がダッシュボードなどのチェックを毎週行っている。

（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）

・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。

（７）苦情処理・顧客対応

・開示請求は特にない。

・顧客からの電話でのガス料金問い合わせは、自宅からの電話で番号がディスプレイによって確認できる場合のみ回答することにした。外からの電話での問い合わせには回答しないことにした。

・警察や弁護士などからの問い合わせは、委託元に委ねるようにしている。

（８）事故発生時の対応

・事故が発生しても従業者個人に対するペナルティはない。原因を追究し、全社で教訓を共有するようにしている。ペナルティを与えると隠すようになってしまうと考える。

（９）その他

・委託元のシステムが古いため、アクセスログをシステムで取ることができないのでノートで手書き管理している。漏えいがなかったことを示すための自衛的な方策である。

以　上

D. 卸売業　D 社

事業概要	電化製品の卸売販売		
従業員数	約 1,400 人	プライバシーマーク取得	あり
保有個人データ件数	約 1,200 万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・1,200 万件程度

（２）個人情報保護担当部署

・監査担当部門

（３）個人情報保護管理者の有無・位置づけ

・「個人情報保護管理者」はビジネスサポート部門の責任者が担当している。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマークを取得（平成 17 年 3 月）している。
・プライバシーマークが取引の際に必須条件になることはないが、一部調査票の回答を免除されることがある。

（５）個人情報保護に向けた取組経緯

・社会的な要請を受けて代表取締役社長が個人情報保護に関する取組を開始した。
・全社キックオフミーティングを開き、プライバシーマークの年内取得を宣言した。認証の取得という明確な目標を設定することで､取組をしやすくすることが狙いだった。
・取得のためにコンサルタントに依頼し、社内の関係部署から従業者を集めてプロジェクトチームを作った。
・保有個人情報の洗い出し、個人情報管理台帳の作成、リスク一覧の作成を経て、プライバシーマークの申請を行った。
・現在は更新審査に向けて全社的に取組を強化しているところである。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・代理店、法人、個人など多種多様の個人情報を取得している。
・ホームページからの会員登録制度があり、個人情報が多数集まっている。年賀状専用ソフト入手のため、12 月に 12 万件（年間の 1／3 程度）の会員登録がある。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・個人情報の保護のための委員会を発足し、規程づくりと周知に努めた。
・お客様担当窓口や教育担当の設置のため、企画担当の長にプロジェクトに参加してもらった。現在は関係会社のプライバシーマーク取得に向けて、同社が支援をしている。月に１回程度の打ち合わせの機会を設けている。
・監査責任者と事務局は同一部署内に存在するが、監査責任者は事務局の活動には関与しないような体制にしている。
・通常の職制の業務組織体制で行い、社長からトップダウンで動かしている。個人情報保護法の管理者は、事務局の支援のもと、全責任と職権を有している。

（２）個人情報の取得

（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）

・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。
・従来は製品に同封する「愛用者カード」によって個人情報を取得していた。これは現在では、自社サイトでの WEB 登録に切り替わっている。
・個人情報は、製品の保守契約時、修理対応した際の記録履歴として取得することが最も多い。保証書の保守申込書に「情報提供を希望しますか」と問う項目を追加して対応している。
・代理店販売が主流なので、顧客との契約は代理店を通じて行う。代理店が顧客とどのような契約を結んでいるかは、ケース・バイ・ケースである。代理店への個人情報の取得に関する指導は行っていない。
・業界のフェアでは、「フェアの主催者」と、取得した個人情報の所有権について、その都度取り決めをしている。
・個人情報を取得する際の書類は、雛形があり、事務局が申請書をチェックしている。（申請書チェックについては）必要に応じて即日でチェックできるようにしている。ほとんどキャンペーンやアンケートのために使用する。

（３）個人情報の利用（第三者提供を含む）

・共同利用をする場合は、共同利用先をホームページ上に明記している。現在はすべて

の関係会社を明記しているが、今後は本当に共同利用をするところだけに絞る予定である。

（４）個人情報の管理

①情報の管理体制

・それぞれの情報データベースごとにアクセス権限が設定されており、担当者のみが閲覧できる。たとえば自社 WEB サイト内の個人情報は WEB 事業部門の担当者のみ閲覧することができる。顧客問い合わせ窓口では自社 WEB サイトだけが閲覧できるようになっている。
・私用パソコンの業務持ち込みは禁止、社内のパソコンにソフトをインストールすることは禁止、業務の社外持ち出しは禁止、自宅のパソコンと会社のパソコンの電子メールやりとりは禁止、などの規程がある。
・社外とのやりとりにはファイヤーウォールがある。サーバからハードディスクにダウンロードした際、ログが残るようになっており、それをチェックしている。
・製品を複数購入した場合などのデータの一元化は行っていない。名寄せは技術的にも経済的にも難しい。

②従業者への教育方法

・ｅラーニングにより短期間で全従業者への教育実施及び受講終了確認ができる仕組みとしている。

③盗難対策

・USB メモリは暗号機能付のものを 配付し、それ以外のものは使用禁止にしている。
・個人情報管理台帳に記入し、上長の許可を得れば USB で情報を持ち出すことができるが、それは同社の他拠点で利用できるということで、自宅への持ち出しは禁止である。

④ノート PC の安全対策

・「HDD パスワード」「HDD 暗号化ソフトパスワード」「ネットワークログオンパスワード」の３つのパスワード設定を必須とし、セキュリティを強化した。

⑤外部委託先管理

・業務委託先 110 社すべてと、ファイル共有ソフト（Winny 等）に関して書面を交わした。

⑥日常点検・確認の方策

・「省エネ」管理も含めて「退出時チェックシート」を運用し、各種電源 OFF、最終退出時間を記録している。

⑦初歩的ミスの防止策

・ 携帯電話に関して「クリップ等で身体から離さない」「オートロックモード」「電話帳の個人名の略称化（イニシャル）登録」を必須としている。

・FAX 機に関して「0 発信」「0 発信不要」の貼り紙をして、FAX 番号を手入力で発信の際、誤送信のないようにしている。

（５）個人情報の消去・破棄

・取得後の年数によってデータベースを分けている。

（紙媒体データの廃棄促進）

・紙媒体での情報は電子データへ入力し、紙は随時廃棄している。

（６）個人情報の監査

・監査責任者（監査部門の部長）を置き、個人情報保護責任者をチェックする。監査責任者は事務局の業務に一切関わらないようにしている。

（７）苦情処理・顧客対応

・開示請求に関するルールを定めている。修正依頼や削除依頼はあるが、全面開示請求は 1 件も来ていない。2 年間に、専用の窓口への問い合わせが 50 件あった。

・請求内容として多いのは、「ご愛用者カード」の情報の削除依頼であるが、情報を削除してほしいデータベースを指定して依頼される。

（８）事故発生時の対応

・具体的な紛失／盗難事故を想定し、各々の対応レベルとその判断基準、発生後の対応手順を明確に規程した。

以　上

E. 卸売業　E 社

事業概要	ガスの卸売、ガス関連機器の卸売等 （ガスの販売小売店からの委託を受け、ガスの消費者の自動検針、配送、ガス代金の口座振替回収代行、設備工事も実施している。）		
従業員数	約 200 人	**プライバシーマーク取得**	あり
保有個人データ件数	約 18 万 8 千件（**※取扱う個人情報件数**）		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・10 万件程度保有している。うち、データ化して集中監視システムを行っているのは 6.5 万件程度である。集中監視センターが社内にあり、24 時間、ガス漏れ等を監視している。

・卸売業ではあるが、小売店よりガスの委託配送、売上代金の口座振替による回収代行、ガス漏れ等の監視なども同社が請け負っている。

・個人情報の種類としては、氏名、年齢、住所、連絡先（本人自宅、本人携帯電話）等の基本的な情報に加え、配送のための地図、配送先の個別の状況（例：耳が遠いので電話でなく FAX で連絡を行う等の情報）、過去のガス漏れ警報の発生状況なども保有している。

・法人でガス契約を行っているような場合は、ガス漏れの場合などに備え、法人の担当者や経営幹部の連絡先など、複数人の個人情報を保有している。

・ガスの配送、機器の修理、ガス使用状況の確認（検針）、緊急時（ガス漏れ等）の対応などに利用している。

（２）個人情報保護担当部署

・管理部が担当になる。

・「個人情報保護委員会及び推進事務局」が常設になっている。専任の担当者はいない。

・個人情報保護委員会は通常は 3 ヶ月に 1 回程度開催されるが、伝達事項や問題が発生したときなどは随時開催される。

（３）個人情報保護管理者の有無・位置づけ

・「個人情報管理責任者」としては常務取締役が担当している。

・代表取締役社長は「個人情報管理総括者」としての位置づけになっている。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマークを取得している。（平成 10 年）

・同社の情報システム部門の前身である情報システムの会社が認定を受けた。情報システムの会社が同社に合併された後、更新の必要性が生じたので全社で取得した。

・情報システム部以外の部門でも個人情報保護に対する意識水準を高め、内部管理を徹底する目的で取得した。

・ISO14001 も取得している。

（５）個人情報保護に向けた取組経緯

・昭和 60 年頃に、ガス業界では先駆け的に、ガス利用世帯におけるガス漏れ、ガス切れ情報などについてオンラインで集中把握･管理ができるようなシステムを導入した。

・このシステムでは非常に大量の個人情報を取り扱うため、情報セキュリティの重要性ということで管理等を厳しく行うことにした。

・平成 10 年にグループ会社（現：情報システム事業部）がプライバシーマークを取得し、同社の合併に伴い、平成 15 年に同社全体でもプライバシーマークを取得した。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・町のガス販売店は必ずしも好況ではなく、原油高によるガス価高騰や後継者不足に悩んでおり、なかなか個人情報保護に目が向かないような状況でもある。

・特にここ最近は一時期の個人情報保護に関する熱心な姿勢が落ち着いてきた感がある。

・ガスボンベの配送等で訪問することがあり、その際に明確な形で情報にならないような家族や世帯等に関する個人情報を取得する可能性があり、その際は業務受託先の販売店に伝達する。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・現在の職位・役職に関係なく、「個人情報保護に関する権限」を与えるため辞令を出して特別な業務執行等を認めている。職位的には下になる「監査員」が個人情報管理責任者である常務取締役などに改善命令等を行うことができるようにしている。

（２）個人情報の取得

・ガス利用の契約時にＬＰガス販売店が書面で取得したデータを預かって委託処理に利用している。

・その他、ＬＰガスボンベの配送等で訪問した際に、個別の消費者や家庭の事情などについても取得することがあり、その際は業務受託先の販売店に伝達する。

（３）個人情報の利用（第三者提供を含む）

・ガス使用量メーターの検針は、オンラインで把握できるようなシステムを導入している。
・このシステムを活用して、独居老人等の安否確認を行うサービスに活用することも可能であり、検討している。
・ガス販売店を対象として個人情報セミナーを開催したことがあるが、その席でも個人情報はルールを守れば有効に活用可能であると説明している。
・その他、配送に行ったときに教えてもらった情報（機器が壊れている、買い換えたい等の情報）については、ガス販売店、ガス機器販売店などにも提供し、販売店は営業活動に利用している。
・配送担当の従業者については、配送伝票の専用フォルダを使用することを義務付けている。専用フォルダは作業着のポケットに差して携帯することができるようになっており、常時身体から話さないようにするための措置である。

（４）個人情報の管理

①情報の管理体制

（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）

・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。

②従業者への教育方法

・年に１回、「リフレッシュ教育」と称して全員が研修を受講している。
・運用基準の見直しなどがあったタイミングで部門の実務責任者もしくは実務責任者から委任を受けた者が所属する従業者を集めて「特定教育」を実施している。その他、「内部監査員教育」も実施している。

・受講した研修の理解度については、「受講者への質問」「受講者のサイン・押印」、「受講者へのアンケート、ペーパーテスト」により確認し、理解の程度をランク別に評価している。
・罰則規程は就業規則に準じる形で作成している。

③盗難対策

・セキュリティの高い情報を扱う部屋は ID カードをリーダーに読み込ませなければ入室できないようになっている。
・警備会社に外注しており、入室・退室等のログを取得するようにしている。

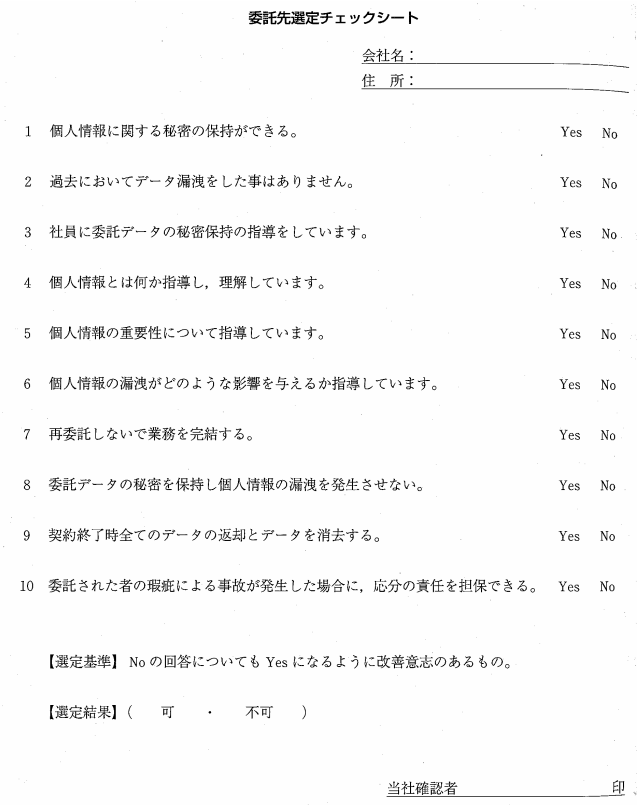
④ノート PC の安全対策

・ノート PC には個人情報は絶対に格納しないようにしている。
・そのため、従来のノート PC を約 100 台、すべてデスクトップ PC に入れ替えた。

⑤外部委託先管理

・工事を実施している部門があり、工事の下請けを委託する場合がある。
・「選定のためのチェックリスト」と「監督のためのチェックリスト」の 2 種類がある。前者は契約締結時に使用し、後者は継続的に委託を実施している事業者について、年に 1 度程度実施している。
・チェックを行うのは、『外部委託を行う部門の実務責任者（部長等）もしくは実務責任者から委任を受けた者』とされている。
・委託契約の締結の際に、契約書に個人情報保護に関する文言が含まれていない場合には、別途覚書を締結している。

図表　委託先チェックシート（選定のためのチェックリスト）



委託先選定チェックシート

会社名：
住　所：

1	個人情報に関する秘密の保持ができる。	Yes	No
2	過去においてデータ漏洩をした事はありません。	Yes	No
3	社員に委託データの秘密保持の指導をしています。	Yes	No
4	個人情報とは何か指導し，理解しています。	Yes	No
5	個人情報の重要性について指導しています。	Yes	No
6	個人情報の漏洩がどのような影響を与えるか指導しています。	Yes	No
7	再委託しないで業務を完結する。	Yes	No
8	委託データの秘密を保持し個人情報の漏洩を発生させない。	Yes	No
9	契約終了時全てのデータの返却とデータを消去する。	Yes	No
10	委託された者の瑕疵による事故が発生した場合に，応分の責任を担保できる。	Yes	No

【選定基準】 No の回答についても Yes になるように改善意志のあるもの。

【選定結果】（　可　・　不可　）

当社確認者　　印

⑥日常点検・確認の方策

・何らかの取組を行う際には、必ず「安全性確保の方策」と「正確性確保の方策」について記載させた上で申請書を提出させている。

⑦初歩的ミスの防止策

・集中監視センターにおいては、FAX の誤送信を防止するために、短縮登録番号と販売店コードを同じものを使用した。

・また、誤送信した場合には、どこであっても必ず送信先に送信した FAX を訪問して取りにいくことを義務付けた。

（５）個人情報の消去・破棄

（外注は行わずに、公的な焼却場等に自社で持ち込み、投げ込みも自社で行う）

・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。

（６）個人情報の監査

（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。）

・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。

図表　監査チェック表

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：

図表　不適合報告書兼是正処置報告書

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

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	蓮見	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）		

配布先：被監査部門の実務責任者　　保管部門：　　保管期間：3年

（７）苦情処理・顧客対応

・相談窓口はホームページに掲載している。担当部門、実務責任者、窓口担当者まで 5 つの部署について掲載し、代表電話に加えて個々人の電子メールアドレスまで掲載している。

・開示手数料については原則無料としており、郵送で対応する場合のみ実費をもらっている。

・本人確認は来社の場合は証明書等の提示を求め、電話の場合はコールバック、又は郵送による対応で本人確認を行っている。

（８）事故発生時の対応

・業界団体が作成、発行した個人情報保護に関するガイドラインを基に対応規程を作成している。

以　上

F. 小売業（百貨店・スーパー）　F 社

事業概要	百貨店事業等		
従業員数	約　12,000 人	プライバシーマーク取得	なし
保有個人データ件数	約 790[1]万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・約 790 万件

（２）個人情報保護担当部署

・個人情報保護委員会事務局（総務部、営業企画部、事業統括室で構成）

（３）個人情報保護管理者の有無・位置づけ

・個人情報保護管理者は百貨店事業本部長

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・個人情報保護に関する認証は取得していない。

（５）個人情報保護に向けた取組経緯

・顧客情報の取得・利用・管理について、基本方針を定めた「プライバシーポリシー」を策定し、この方針に従って適切に管理・利用するよう徹底を図っている。プライバシーポリシーには以下の項目が含まれる。

－取得する際は、利用目的を明らかにし、お客様の同意を得る。

－利用する際は、同意を頂いた利用目的の範囲内で行う。

－個人情報保護推進責任者を選任し、顧客情報の適切な管理に努める。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・百貨店協会が作成したガイドラインに従い、各社が対策を実施している。

・顧客本人から明示の同意を得ることを原則としている。

・公開情報を利用した販売促進活動は一切行わない。

・取引先の顧客情報も百貨店の管理下に置く。

・紙ベースの情報を大量に保有しており、それらが一元的に管理されていない。

---

[1] 紙媒体のうち、配送伝票や修理伝票など販売時点での伝票を含まない数。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・経済産業省ならびに日本百貨店協会のガイドラインに準拠し、「個人情報保護ガイドライン」や各種マニュアルを作成した。個人情報保護の基本原則「顧客本人の同意」に基づき、個人情報の取得・利用・管理の社内ルールを策定した。取引先の監督の項目を設けることにより、取引先に起因する個人情報漏えい事故の未然防止を図っている。

・顧客名簿・伝票等の管理基準を策定した。管理責任者、記載内容、管理方法・期間、最終処理方法等について明確にし、管理を徹底している。

・個人情報保護小委員会の事務局が社内規程を策定し、各店事務局に通達する。**規程は**各店の職制ラインにて徹底を図っている。

（２）個人情報の取得

（利用目的が明確な場合は利用目的はあえて提示せず）

・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。

（個人情報を紛失リスクと記載内容で分類）

・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以下のように分類し、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。

図表　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	保管期間終了後の最終処理方法
		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）	
■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	店にて廃棄業者へ委託
	顧客名簿（システムⅡ名簿）	○	○	○	×	－	－	〃	〃	顧客政策担当に返却
	顧客名簿（フロッピー）	○	○	○	×	－	－	〃	〃	店にて廃棄業者へ委託
	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	店にて廃棄業者へ委託
	〃　（自社クレ）	○	×	×	○	○	○	〃	〃	〃

（３）個人情報の利用（第三者提供を含む）

・特徴的な取組はなし

（４）個人情報の管理

①情報の管理体制

（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）

・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。

（外商担当者は個人情報をイニシャル等の形式で登録）

・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。

・配送伝票付の配送品の移動に施錠台車を使用する取組を 2 店舗で導入している。

・販売付帯業務上、店外に出る各種伝票類については、個人情報が不要な場合は添付項目から削除している。例えば修理に出す際修理先は管理番号以外の情報は不要なため、氏名や住所を提供しない。

・リスクが十分低下した個人情報に関してはリスクの分類表から削除するようにしている。事案が発生した場合は、その都度必要項目を追加している。

②従業者への教育方法

・導入教育は本社にて全店実施、その後の定期教育は各店にて実施している。

③盗難対策

（携帯電話に遠隔ロックを導入）

・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ノート PC の安全対策

・ワイヤーでの固定化、IC カードによる個人認証、データ暗号化等実施している。

⑤外部委託先管理

・すべての委託先と個人情報の取扱いに関する覚書を締結し、管理責任の明確化を図る。

⑥日常点検・確認の方策

・各種チェックシートにより運用上のチェックを強化している。(例 : 顧客名簿等においては、チェックシートに基づき日々枚数管理を徹底、等)。

⑦初歩的ミスの防止策

・特徴的な取組はなし

（５）個人情報の消去・破棄

(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・破棄を認める)

・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。

（６）個人情報の監査

・特徴的な取組はなし

（７）苦情処理・顧客対応

・開示請求はホームページで申入れ方法を公表し、実際の対応は各店お問い合わせ窓口にて実施、一律 500 円を手数料として設定している。
・開示請求はこれまでに 2 件（本社対応分）あった。開示請求の際の本人確認は、店頭受付でなく電話・ホームページでの受付の場合は、身分証明書のコピーを郵送する形で行っている。

（８）事故発生時の対応

・まず顧客対応を優先する。その後、管理体制の見直しとして、覚書・手順書・運用ルール等と照らし合わせ、問題があれば指導し、再発防止を図る。その後、他の店舗に対して指導を行う。
・伝票の紛失が主な事案である。1 件でも紛失があった場合、危機管理委員会へ届け出ることになっている。
・紛失の際はあらゆる可能性を探し、見つからない場合は危機管理委員会で「見つからない」と判断し、顧客対応及び百貨店協会、経済産業省への報告を行う。再発防止策について、事案発生店と協議し、適宜全店通知を行う。

（９）その他

(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る)

・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

される。「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。

図表　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（　　）

以　上

G. 小売業（物販）　G 社

事業概要	CD、DVD、楽器等を中心とした音楽映像関連商品と書籍の販売		
従業員数	約 1,000 人	プライバシーマーク取得	なし
保有個人データ件数	約 72 万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・720,000 件（ポイントカード会員数累計）を保有。ただし、有効会員数は 332,000 件（ポイントカードの期限が切れていない会員の数）
・名寄せはしていないため、複数回加入したような会員については重複があり得る。
・上記の件数は、店舗で取得する得意顧客名簿等の紙媒体の個人情報件数は含まない。
・個人情報の種類としては、氏名、住所、性別、生年月日、電話番号、電子メールアドレスに加え、ダイレクトメール送付の可否に関する情報が含まれる。
・特にマーケティング目的での利用はまだ行っていない。

（２）個人情報保護担当部署

・営業管理部が担当である。
・情報システム部がデータ管理を担当している。他、安全管理委員会は設置されているが、営業管理部が兼務している。

（３）個人情報保護管理者の有無・位置づけ

・安全管理委員会の長が最高責任者（役員がなることが多い）である。
・CPO という呼称は対内的・対外的に用いていない。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・認証は取得しておらず、今後も取得予定は無い。

（５）個人情報保護に向けた取組経緯

・平成 17 年 4 月 1 日の個人情報保護法施行に向け、社内チームで規程及びマニュアルを作成した。
・社内業務で個人情報に関わる部分について、個人情報保護法の遵守のために問題点の抽出と解決策を検討した。店舗責任者の会議及び本社内会議等で、マニュアルその他の概要の説明により規程事項を周知徹底した。
・シン・クライアント方式のシステムは 3 年前から導入を検討してきた。個人情報保護

のためにシン・クライアント方式を導入するということではなく、LAN ですべての地方店舗（約 250 箇所）が結ばれたことを受け、『IT 資産の一元管理』をいかに実現するかという視点から取組は行われた。
・シン・クライアント方式のシステム導入は 1.5 年程度で実現できた。

（６）個人情報の保有・管理・提供等に関する業界の特徴
・チェーン展開をしており、事業所が地方分散の形態をとっているので、全事業所の管理レベルをキープすることは難しい。
・同社では全国で約 250 店の直営店を展開しており、各店で 4～50 名程度の従業者と、アルバイトを雇用している。短期で辞めていくアルバイトも少なくないため、徹底が難しい。
・データ化している情報は本社で中央一括管理体制を敷くことが可能であるが、個別の店舗で取り扱う紙ベースの個人情報の取扱いを徹底し、本社の管理下に置くことが特に難しい。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）
・特徴的な取組はなし

（２）個人情報の取得
（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している）
・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。

（３）個人情報の利用（第三者提供を含む）

・会員番号をキーとして、どの人がどのような種類の商品を購入したかということは判断できるが、まだ個人情報と個人購入履歴を連携させたマーケティング・分析は実験的にしか実施していない。

（４）個人情報の管理

①情報の管理体制

（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）

・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。

（物理的・技術的管理も徹底）

・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インストール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。

②従業者への教育方法

・アルバイトを常時 1,600 人程度雇用しており、毎月 150 人程度の入替えがある。マニュアルはあるが、このようなアルバイトに理解させようとすることが現実的ではない。

③盗難対策

・特徴的な取組はなし

④ノート PC の安全対策

・ノート PC 自体が数台しか存在しておらず、個人情報をデータで登録することは禁止している。

⑤外部委託先管理

・特徴的な取組はなし

⑥日常点検・確認の方策

・特徴的な取組はなし

⑦初歩的ミスの防止策

・特徴的な取組はなし

（５）個人情報の消去・破棄

・ポイントカードの発行対象者情報については、カードが失効した後も消去しておらず、継続的に保有している。現時点では消去は検討していない。これは失効後も顧客が店舗で購入し、ポイントカードを使用することもあるし、再発行を求められることもあるからである。

・改めて入会書を記載してもらうよりも迅速に対応できる場合があり、顧客満足の意味もある。

・各販売店で行われる商品予約、注文、修理などの名簿は紙ベースで各販売店で保管しているが、これらは随時対応が済むたびに廃棄している。

（６）個人情報の監査

・マニュアルの遵守状況チェックを半年に１回実施しているが、実際には必ずしも十分に手が回りきっていない部分もある。

・通常の社内監査の一環に「個人情報保護体制の確立・遵守」も含まれているが、年間50 店舗程度の抽出監査であり、毎年全店舗を監査するまでには至っていない。

（７）苦情処理・顧客対応

・ポイントカードに関する個人情報の開示請求は無い。

・開示の場合は郵送開示を原則としており、実費を請求することとしているが、まだ事例はない。

・問い合わせの受付は「お客様相談窓口」で対応している（個人情報専用の窓口ではない）

（８）事故発生時の対応

・特徴的な取組はなし

以　上

H. 小売業（通販等）　H 社

事業概要	家電製品、電子文具、スポーツ用品、宝飾品、健康食品、健康器具、寝具、生活雑貨などを取り扱う通信販売業		
従業員数	約 400 人	プライバシーマーク取得	なし
保有個人データ件数	数百万件程度		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・保有個人情報は数百万件である。

・情報の種類は、顧客情報、従業者情報、採用情報で、すべて直接収集である。

（２）個人情報保護担当部署

・担当部署はコンプライアンス部で、常務執行役員以下、セキュリティ担当は 6 名（専任）である。

・個人情報管理委員会があり、各部署より最低 1 名、合計 13 名の個人情報に携わる部署の管理者により構成される。

・また組織横断的な情報セキュリティ委員会があり、情報セキュリティ全般に関する議論を行っている。

（３）個人情報保護管理者の有無・位置づけ

・個人情報保護管理責任者は常務執行役員である。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・ISMS を取得している。（平成 18 年）

・情報システムの専門家にコンサルティングを依頼し、コンプライアンスを担当する専任部署を作って対応し、ISMS の認証に 1 年半を要して準備、取得した。

（５）個人情報保護に向けた取組経緯

・企業のリスク管理に対する見直し・強化を図り、積極的な経営資源の投資を行い、物理的・技術的・管理的対策を実装し、特に従業者への教育を重視、注力した。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・通販事業は配送については委託しなければならない。通常期であれば信頼できる事業者に委託すれば大きな問題は無いが、年末年始などの繁忙期となると委託先が小規模

の配送事業者などに再委託、再々委託し、個人情報の管理が希薄になる場合も想定される。
・このような場合に、個人情報に関する事件事故に結びつく可能性もあり得る。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・特徴的な取組はなし

（２）個人情報の取得

・直接収集のみである。
・利用目的は、カタログ、チラシ、ホームページなどに個人情報基本方針を詳細に提示し、「いつでも知り得る状態」にしている。
・個人情報の更新等はカタログ送付時に返信ハガキを添付、又は顧客が電話、FAX、WEBなどで開示・訂正・利用停止・削除の依頼を専用窓口にした場合にいつでも対応できるような仕組みにしている。

（３）個人情報の利用（第三者提供を含む）

・特徴的な取組はなし

（４）個人情報の管理

①情報の管理態勢

（生体認証で入退室を管理している）

・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。
・個人のパソコン持ち込みは禁止している。

（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）

・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。
・個人所有ノート PC の利用を禁止している。
・セキュリティパッチや脆弱性の診断を外部機関に委託して行っている。年に 2 回のテストをしている。
・機密性・完全性・可用性などの指標から脅威、脆弱性を図り個人情報の有するリスクを数値化し、フロー図を描いて「見える化」したい策を実施・管理している。

②従業者への教育方法

（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）

・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、A 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。
・職場環境の安心・安全を確保するために、不正行為や誤解を招く行為を取れない環境作りが会社としての責任と捉えている。
・入社時より定期的に個人情報保護についての教育研修を行っている。また、取引先の駐在員や、派遣・契約社員及びパート従業者にも同様に教育を行っている。

③盗難対策

・特徴的な取組はなし

④ノート PC の安全対策

・ノート PC は使用を禁止している。どうしても必要な場合は貸出申請制にしている。

⑤外部委託先管理

・基本契約書締結時には、必ず NDA(秘密保持契約書)を結んでいる。

（外部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する）

・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。

（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行う）

・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。

・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。

⑥日常点検・確認の方策

（抜き打ちの放置検査を実行）

・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。

（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される）

・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。

⑦初歩的ミスの防止策

・特徴的な取組はなし

（５）個人情報の消去・破棄

・すべてシュレッダー処理している。

・懸賞応募ハガキなど大量なものは、外部委託し専任担当の立会いのもと、大型機でシュレッダー後、焼却処分し廃棄処分証明書を提出してもらっている。

（６）個人情報の監査

・システム上のセキュリティに対しては外部から侵入を試みるテストを行い、セキュリティの確保を確認している。

・内部監査は 3 ヶ月ごとに実施し、是正請求とそのフォローアップ監査を実施している。

（７）苦情処理・顧客対応

・開示に際しては、本人確認のため身分証明書類と開示請求依頼申請書を記入してもらい、成りすまし対策を実施している。

・問い合わせ窓口はフリーダイヤルで、専任の担当者 4 名の他、個人情報保護担当者として 14 名が問い合わせに対応している。

（８）事故発生時の対応

・事故、事件発生時の手順書がある。情報漏えいや改ざん以外にも、災害による停電時に情報を移す手順も定めており、誰がサーバを止めるかなど、業務フローに従って実際に訓練をしている。

・事故が起きた場合の判断者は誰か、どういう対応をするか、追加対策が必要かなど「事件事故対応手順書」を定めている。

・社内・外での事件、事故後には事件事故報告書を作成し、原因究明と是正・予防対策を速やかに実施する。

以　上

Ⅰ. 信用業　Ｉ社

事業概要	クレジットカード、ファイナンス		
従業員数	約 6,300 人	プライバシーマーク取得	あり
保有個人データ件数	約 2,600 万件		

１．個人情報に関する概要

（１）保有個人情報件数、個人情報の種類、個人情報の利用目的

カード有効会員数：約 2,000 万人

・ローン有効会員数：約 70 万人

・役職員情報：約 6,300 件

（２）個人情報保護担当部署

・情報セキュリティ管理部

・個人情報保護に係る業務に従事する従業者は 10 名（専任）

（３）個人情報保護管理者の有無・位置づけ

・個人情報保護総括責任者（コンプライアンス統括本部長が就任する）

・個人情報保護監査責任者（内部監査部長が就任する）

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・BS7799・ISMS 認証基準（平成 15 年）

・プライバシーマークを取得（平成 17 年）

・取得理由：①個人情報の安全管理スキルの向上が図れる、②取引先等からの要望、③他社との差別化、④安心の提供と信頼の獲得

・効果：①個人情報保護のハイレベルの指針とできる、②外部監査的な検証を受けられる

（５）個人情報保護に向けた取組経緯

・平成 13 年 4 月に個人情報保護全般に係る統括・指導の主管部署として、個人情報部を創設。同年、業界自主ルール等に準拠して「個人情報保護方針」「個人情報保護規程」を制定。

・平成 15 年 4 月よりコンプライアンス統括本部傘下に組織変更。

・個人情報保護の文書体系と組織体制を整え、PDCA の取組を始め、平成 17 年 4 月にプライバシーマーク認証取得を申請し、同年 9 月 15 日に認証取得。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・与信事業者であり、個人信用情報機関に登録又は提供を受けている「個人信用情報」を取り扱っている。
・平成 13 年から“自主ルール”の制定作業を通じて、個人情報保護に取り組んでいる。
・自主ルール運営協議会（現 CPIP）の他、日本クレジット産業協会、日本クレジットカード協会等、各業界団体においても独自に個人情報保護に取り組んでいる。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

（本社と支店等との分権）

・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。

（２）個人情報の取得

・個人情報は、加盟店が店頭においてカード入会申込を受付する場合と、個人が郵送で申し込んでくる場合がある。
・カードの提携先は 1,600 社あり、それぞれの利用目的が少しずつ異なるので、明示する利用目的の文面もそれぞれにあわせて変えている。

（３）個人情報の利用（第三者提供を含む）

・保有個人データの利用目的、共同利用する関連信販会社等を「プラバシーポリシー」と共にホームページ上に公表している。

（４）個人情報の管理

①情報の管理態勢

（“三点セット”による入退室管理）

・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は、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。

（バーコードによるトレーサビリティ確保）

・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管理している。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。

（システム上の安全管理）

・重要な情報が集中する「システムセンター」では、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。

②従業者への教育方法

（毎月全部署で勉強会を実施）

・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。

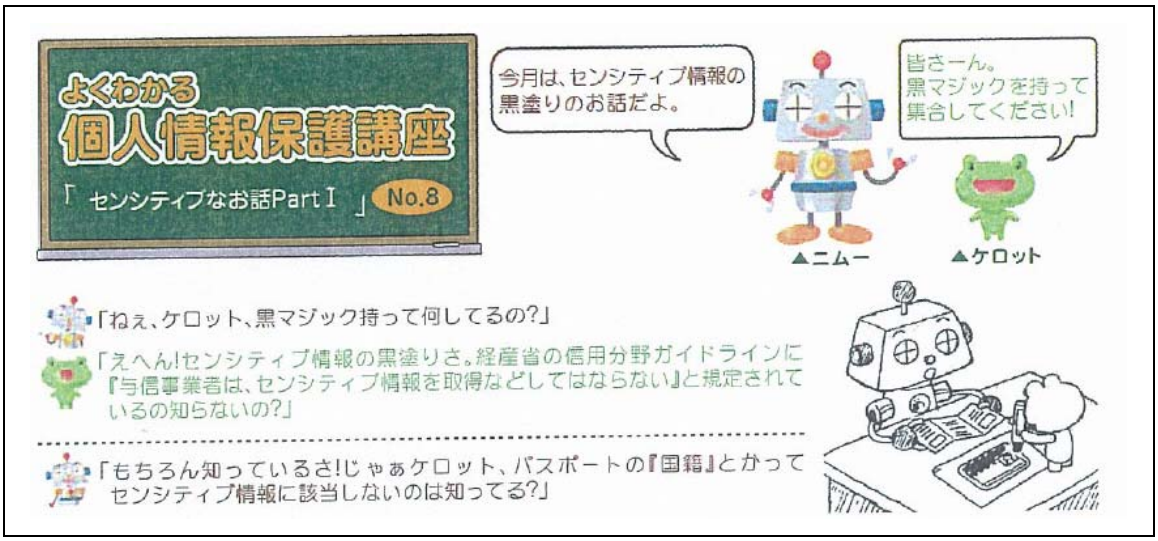
（半年に一度の e ラーニング）

・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。

（社内報における解説）

・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。

図表　社内報のサンプル



③盗難対策

・監視カメラ、指紋認証による入退館管理の強化、業務端末の書き出し制限とログ取得、データ授受の電磁媒体から伝送化へ移行など取り組んでいる。

④ノート PC の安全対策

・ノート PC は営業プレゼン用のみとして、原則社内への持ち込みを禁止している。

⑤外部委託先管理

（年に 1 回以上の立ち入り検査の実施）

・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。

・問題点としては、個人情報保護を理由に、委託先がログや資料へのチェックを拒否するため、せっかく立ち入っても直接的な検査ができないことが多い。

（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）

・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。

⑥日常点検・確認の方策

・「部店内検査手順書」を半期ごとに配布し、全部署において個人情報責任者が中心とな

って、毎月、点検を実施し結果を報告することとしている。

⑦初歩的ミスの防止策

・トラブルデータベースを作成し、誤 FAX 等の事務ミスについて、全社において情報共有している。なお、トラブルの内容は、月例の個人情報安全管理委員会に報告・検討・改善指示がされる。

（５）個人情報の消去・破棄

・特徴的な取組はなし

（６）個人情報の監査

・個人情報保護監査責任者を定め、その下で内部監査部が、全部署の監査を年１回以上実施している。

（７）苦情処理・顧客対応

・開示手続の規程や、執務の基本姿勢を定めた「コンプライアンス・マニュアル」を策定して対応している。

（８）事故発生時の対応

・トラブル管理規程、危機管理規程を定め、経営層にすぐに伝わる態勢を整えている。

以　上

J．信用業　J 社

事業概要	リース、信用販売、カード、ファイナンス		
従業員数	約 900 人	プライバシーマーク取得	なし
保有個人データ件数	約 760 万件		

１．個人情報に関する概要

（１）保有個人情報件数、個人情報の種類、個人情報の利用目的

・約 760 万件

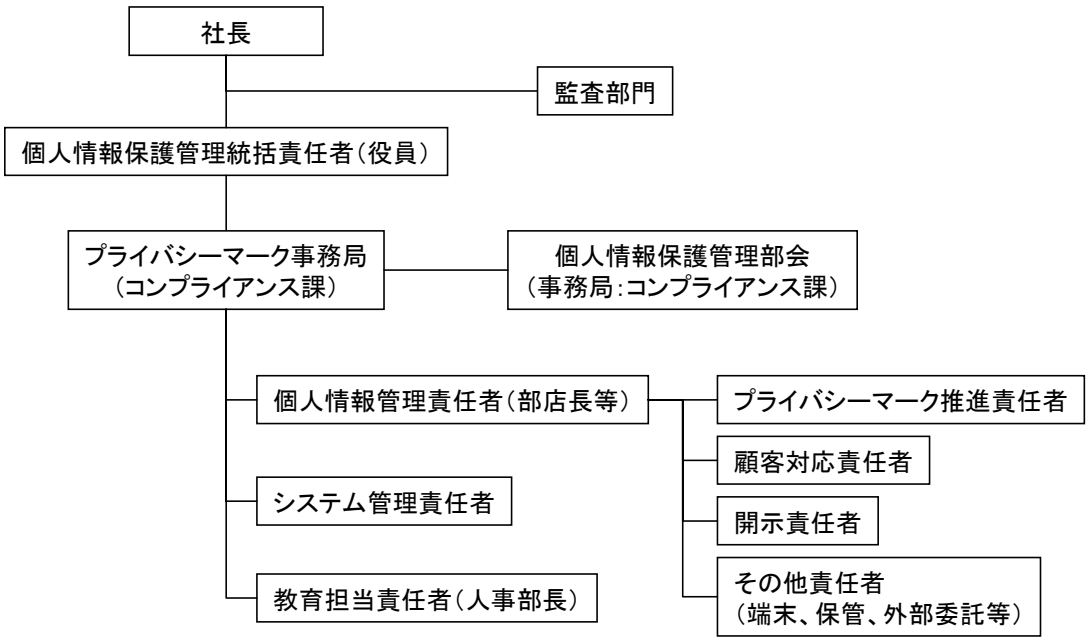
内訳は顧客基本レコードとして 658 万件（内容：与信判断情報、売上情報、債権管理情報、会員情報）リース会社のシステムとして 93 万件（内容：与信判断情報、売上情報、請求情報、回収情報）

・他にもカード会員情報や受注残情報、未回収・貸倒償却データ等でシステム別に個人情報は保有している。システム別にみると全データは 1,839 万件となる。

（２）個人情報保護担当部署

・コンプライアンス統括部コンプライアンス課が担当している。同課は、プライバシーマーク事務局、及び個人情報管理部会の事務局を担当している。

図表　個人情報保護に係る組織図



（３）個人情報保護管理者の有無・位置づけ

・個人情報管理統括責任者は専務取締役である。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・なし

（５）個人情報保護に向けた取組経緯

・平成 16 年 4 月　コンプライアンス部発足

①コンプライアンス体制強化のための組織として発足

②併せて、個人情報保護法の施行を控え、個人情報の安全管理とプライバシーマーク取得推進に向けた専門部門としても発足する。

・平成 16 年 6 月　プライバシーマーク取得推進を、常務会で決裁を得る。以降 1 年間、「個人情報マネジメントシステム」の構築に注力。

・平成 18 年 5 月に更新された、JISQ15001：2006 年版に準拠した「個人情報マネジメントシステム」に基づき、時期を見てプライバシーマーク認証取得の申請を行う予定。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・平成 15 年 5 月 30 日に公布された個人情報保護法の趣旨に基づき業界共通の「個人情報の収集・利用・提供に関する同意条項」を定め、顧客の同意を得る取組を開始した。同社においては、平成 15 年 8 月以降、同条項に基づいて取り組んでいる。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・本社 コンプライアンス統括部 コンプライアンス課が担当している。コンプライアンス課は 4 名。コンプライアンス統括部では、コンプライアンス全般を担当している。個人情報保護のほかに情報セキュリティ、CSR、法令順守等を管轄している。

・CPO は専務取締役。店部長・所長が個人情報管理責任者（約 50 名）である。実務は課長・次長クラスが担っている。部、支店でプライバシーマーク推進責任者、お客様対応責任者、開示責任者、各担当責任者（端末操作機／送付／保管／破棄／外部委託）がいる。担当者は部・支店・営業所の規模によって複数名の場合と 1 人の場合がある。

・規程・体制作りに外部コンサルタントを利用した。

・個人情報保護法の施行にあわせて、従来明文化されていなかった作業をマニュアル化、文書化した。これは、プライバシーマーク取得という具体的な目標があったことによる。

（２）個人情報の取得

・加盟店（販売店）が商品販売時に個人情報を取得している。
・申込書・契約書においては、同社の加盟する信用情報機関である CIC への個人情報の提供についての同意を前提として申込を受け付けている。
・本人確認を必要とする個人情報の開示請求の際は、免許証のコピーを取得するが、本籍地はすぐに黒塗りするように社内にて対応をしている。機微情報は取得していない。

（３）個人情報の利用（第三者提供を含む）

・同社のグループ会社の従業者に対しては同社のサービス（オートローン、住宅ローン等）の案内をしている。
・同社の親会社は個人情報の共同利用先に同社を入れている。
・利用者への販促活動は加盟店が実施しているため、同社が直接顧客にアプローチすることは少ない。

（４）個人情報の管理

①情報の管理体制

・ファイル共有ソフト対策としては、社外からダウンロードしたファイルは利用できないようにしている。
・自宅のパソコンについては、ファイル共有ソフトをしないよう、通達で注意喚起を行った。

②従業者への教育方法

（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）

・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。

（従業者全員の「個人情報取扱主任者」の資格取得を目指す）
・従業者全員の「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。

③盗難対策
・特徴的な取組はなし

④ノート PC の安全対策
・持ち出し専用パソコンを設けている。持ち出し専用パソコンは個人情報の登録・保存は一切行わないこととしている。

⑤外部委託先管理
（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）
・業務委託先の選定基準としては、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委託先から改善計画書（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。

（書類発送は監査済みの外部委託先を利用）

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

・利用情報の発送は普通郵便で親展と記載している。郵便局とのやりとりでは数を照合している。

⑥日常点検・確認の方策

（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）

・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。

図表　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

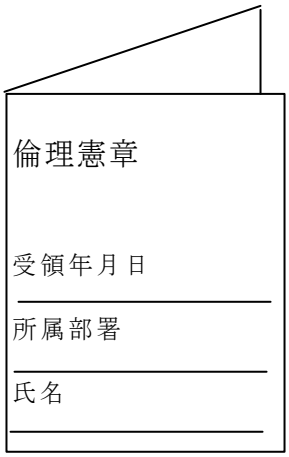
・前述のコンプライアンスに関する勉強会もコンプライアンスデーに設ける部署が多い。

（個人情報保護方針をカードにして、従業者に携行を義務付け）

・個人情報保護方針（6 項目）はカードに印刷し、従業者は署名し常に携行するように決まっている。ポスターにして壁にも貼ってある。

・行動基準もカード化し署名し常に携行するように決まっている。

図表　カードのイメージ



⑦初歩的ミスの防止策

（電子メール、FAX の誤送信防止には 2 人確認をマニュアル化）

・電子メール、FAX の誤送信防止については、2 人確認をマニュアル化している。

・加盟店からの FAX については、審査が通った場合には自動的に返信 FAX が行くようになっている。

（５）個人情報の消去・廃棄

・個人情報の消去・破棄については「個人情報廃棄担当責任者」を全社の部門・センター、営業部・支店・事務所ごとに定める。個人情報廃棄担当責任者は不要になった個人情報の廃棄処分が適正におこなわれているかどうか年 2 回点検し、個人情報管理責任者へ報告する。

・不要になった個人情報は原則として日々シュレッダー等で処分している。

・パソコンを廃棄処分する場合にはフォーマットだけではなく、専用のデータ抹消ソフトを使用して処理している。

（６）個人情報の監査

（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）

・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。

・自己点検の結果、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監査について、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。

（監査は業務監査部門が実施）
・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。

（７）苦情処理・顧客対応
・個人情報開示要求についてはマニュアルを作成し対応している。
・苦情処理、顧客対応は、お客様相談センター、各支店で受け付け。対応部門へ文書又はナレッジシステムにより通告し改善や解決の見届けを行っている。

（８）事故発生時の対応
・事故発生時には電話又は電子メールでコンプライアンス統括部に第一報を入れる。報告対象かどうか判断に迷うケースはコンプライアンス課に相談するよう決めている。
・個人情報漏えい保険には加入している。

（９）その他
（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）
・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。

・ガイドラインについては、金融庁、経済産業省それぞれのものを比較して、違いをチェックしている。

以　上

K. 信用業　K 社

事業概要	割賦販売あっせん		
従業員数	100 人未満	プライバシーマーク取得	なし
保有個人データ件数	約 10 万件		

１．個人情報に関する概要

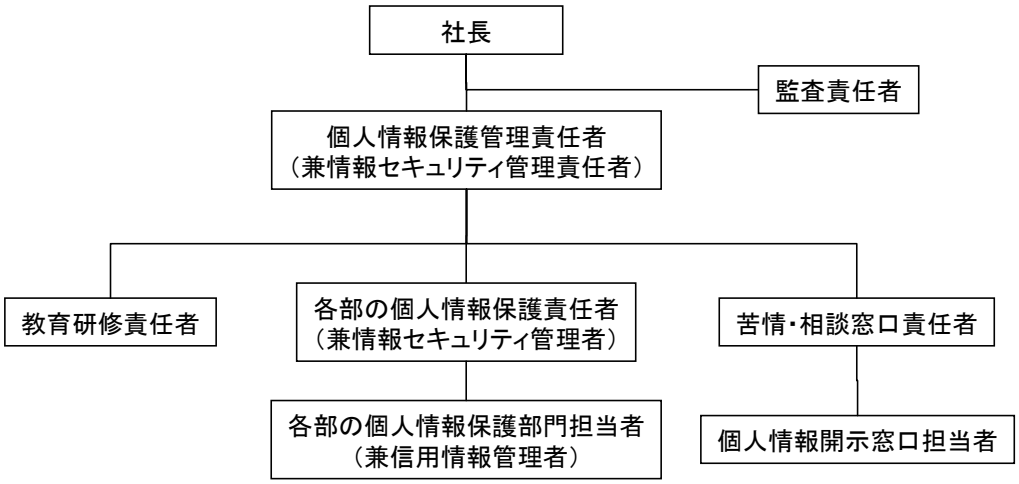
（１）保有個人情報件数、個人情報の種類、個人情報の利用目的

・残高のある契約数：約 10 万人件分
・従業員数分
・電子媒体によるデータベース：約 20 ファイル
・紙媒体、電子媒体の情報資産：約 700 ファイル（種類）

（２）個人情報保護担当部署

・専任部署は無く、業務管理部門が担当している。
・個人情報は、情報セキュリティと一緒に管理されている。

図表　個人情報保護に係る組織図



（３）個人情報保護管理者の有無・位置づけ

・個人情報保護管理責任者を任命し､個人情報保護全般に関する責任権限を与えている。
・業務管理部門の次長が、同管理者の役割を担う。なお、同次長が情報セキュリティ管理責任者も兼務している。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・認証取得はしていない。ただし、プライバシーマークは、今後認証を受ける予定である。業界全体として、プライバシーマークやISMSを取得することが一般的となっているため、今後、認証の取得を目指す予定。

（５）個人情報保護に向けた取組経緯

・平成 13 年 3 月　クレジット産業における個人情報保護・利用に関する自主ルール運営協議会の発足を機に取組を強化。

・個人情報保護法施行前に、個人情報の安全管理の策定（個人情報保護の管理体制、方針策定、規程の見直しなど）、従業者から誓約書の取得、個人情報保護の安全管理体制の点検、ガイドラインの社内説明会実施、プライバシーポリシーの公表、掲示、外部委託先の契約内容の確認及び見直し、第三者機関による個人情報保護適合診断（システム診断）の受診、個人情報の開示、変更等に関する要領及び帳票の整備を実施。

・平成 17 年　全従業者を対象とした個人情報保護学習の実施、第三者機関による情報セキュリティ（個人情報）適合診断の受診を実施。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・クレジット業界として、個人情報の保護及び利用に関する「自主ルール」を定めている。

・顧客から収集した個人データを、個人信用情報機関（CIC）に提供すると共に、与信判断・与信管理の目的で個人信用情報を照会している。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

（タスキがけ人事による効率的な管理体制）

・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。

（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）

・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。

（新ルール適用前に試行実施の期間を確保）

・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。

（２）個人情報の取得

・特徴的な取組はなし

（３）個人情報の利用（第三者提供を含む）

・特徴的な取組はなし

（４）個人情報の管理

①情報の管理態勢

（情報の機密分類に応じてシールで色分け）

・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。

②従業者への教育方法

（ビデオとペーパーテストによる教育）

・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。

（資格取得の推奨）

・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。

③盗難対策

・携帯電話、カメラ等の社内への持ち込みを禁止し、ロッカーへ預け入れることを義務

付けしている。

④ノート PC の安全対策

・特徴的な取組はなし

⑤外部委託先管理

・特徴的な取組はなし

⑥日常点検・確認の方策

（１日１回以上現物点検・周知徹底）

・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。

⑦初歩的ミスの防止策

（番号入力による FAX 送信禁止）

・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。

（印刷時に個人情報を白抜きするシステムを自社開発）

・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。

（電子メールの添付ファイルの制限）

・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。

（顧客情報の伝言に、専用連絡帳を使用）

・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。

（５）個人情報の消去・破棄

・情報の廃棄は、管理者の事前承認が必要とし、管理簿への記録が義務づけられている。

・機密書類を破棄するための専用の箱を用意し、廃棄専門業者によって溶解処理している。

（６）個人情報の監査

・内部監査委員３名によって、半期ごとに監査を実施し、経営会議へ報告している。

（７）苦情処理・顧客対応

・顧客からの相談・クレームは、「お客様相談室」で一元的に管理している。

・開示請求は本人限定としているが、家族の方には理解してもらえない場合があり、クレームを受ける場合がある。

（８）事故発生時の対応

・事故の定義と報告基準、報告体制と報告ルート、行政・監督官庁への報告に関する規程を定めている。

以　上

L. 情報サービス業（ソフトウェア） L 社

事業概要	システム開発、システムインテグレーション事業等		
従業員数	約 6,400 人	プライバシーマーク取得	あり
保有個人データ件数	約 120 万件		

1. 個人情報に関する概要

（1）保有する個人情報の件数、種類、利用目的
- 顧客の情報が約 120 万件
- 従業者情報が約 1 万件

（2）個人情報保護担当部署
- 全社マネージメントシステム維持運用のコントロールはコンプライアンス室個人情報管理課。具体的な運用（対策措置実施等）は各担当部署にて実施。

（3）個人情報保護管理者の有無・位置づけ
- 個人情報保護統括責任者は取締役

（4）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果
- プライバシーマークと ISMS 及び ISO14001・ISO9001 を取得している。
- プライバシーマークは一部 B2C 形態の事業があることや、社会的な要請、内部統制の必要性等鑑み、平成 16 年初旬に取得を目指すことを決定し、コンプライアンスプログラムの構築を開始した。

（5）個人情報保護に向けた取組経緯
- コンプライアンスプログラム構築に向け、構築を目的にプロジェクトを発足。コンプライアンスプログラム構築後はセキュリティ全般に関する委員会を設置した。その委員会でセキュリティ全般に関する検討を行っている。
- コンプライアンスプログラムの構築に 1 年半を要した。

（6）個人情報の保有・管理・提供等に関する業界の特徴
- 属人的な管理を避け、情報システムを活用した管理を行っている。

2. 個人情報の適切な保護のための取組について

（1）準備（規程・体制づくり）
- 運用については、物理的な部分は総務部、従業者教育は人事部、問い合わせ対応はお客様相談室とし、具体的な個別対策ごとに運用実務を担当する部署を定めている。例

えば、入退館管理など、物理的な対策措置は総務部が行い、総務部より提供された入退館管理に関する教育コンテンツの材料により、人事部が e ラーニングコンテンツ作成と全従業者への教育を行う。
・全社網羅的な体制を確保するため、各部署における個人情報保護管理者は当該部署の管理職を任命している。

（２）個人情報の取得
・オプトインの取れている個人情報しか保有しない。

（３）個人情報の利用（第三者提供を含む）
・特徴的な取組はなし

（４）個人情報の管理
①情報の管理体制
・社内就労者に対して与えている情報システムのアクセス権は、正社員とその他就労者（派遣・出向）で明確に分けている。更に正社員でも職位によりアクセス権の階層があり、アクセスできる情報が管理されている。本人のアクセス権を超える社内システムにアクセスする必要がある場合は、当該部署の管理職（兼個人情報保護管理者）の申請によってアクセス権が与えられる。

（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）
・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。

②従業者への教育方法
（「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）
・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工数を大きくしない運用となっている。

③盗難対策
・USB メモリは使用禁止である。業務上やむを得ず使用が必要な場合は、パスワードがかけられ、情報が暗号化できる機種を個別の申請に基づいて配布している。配布された USB メモリはマネージャーが施錠できる場所に保管、履歴管理を行って、WEB 上に記載する。全社で 300 個程度保有している。
・一部の従業者には業務連絡用に会社から PHS を貸し出しているが、この PHS に記録されている電話帳等のデータは、万が一紛失の折、本社側から遠隔操作で消去できるようになっている。

④ノート PC の安全対策
・ノート PC の紛失時のセキュリティは二重三重に対策を講じている。まず物理的対策として USB キーロックがあり、システム起動時にはパワーオンパスワードと Windows のパスワードの入力を必要としている。更に社外からの社内システムへの接続にはワンタイムパスワードの入力が必要となり、当社従業者以外の者が利用できない仕組みとしている。

⑤外部委託先管理
・特徴的な取組はなし

⑥日常点検・確認の方策
・月に一度、セキュリティに関する対策措置の運用実施、記録管理について全管理職が WEB 画面に報告する運用としている。この運用報告は監査室の監査が行われる折に実態との乖離チェックが入り、二重に牽制が効くように配慮されている。

⑦電子メール誤送付の防止策
・お客様をはじめとした社外への電子メール送付は、「1 to 1 電子メール」を原則としている。
・100 件を超える同報メールはシステム上で従業者個人からは送付できない仕組みとしている。

・電子メールを利用したダイレクトメールやメールマガジンは、すべて専門の担当部署を通じて送付される。また利用される送付先データはオプトインを取得したデータベースから抽出したデータに限定される。

（５）個人情報の消去・破棄

・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。

（６）個人情報の監査

・全社の運用として、監査室を主体に“社内の監査員”を育成し現在、約 270 名を配置している。
・監査は年２回、それぞれ設定した期間内に行い、監査の視点・重点を事前通知することで、そのポイントに対する取組を促進する効果も狙っている（“抜き打ち”で現状を把握するよりも、「監査があるのでチェックされるポイントをしっかり取り組もう」とする姿勢を重視したいという考えに基づく）。

（７）苦情処理・顧客対応

・すべての電子メールに関して送信ログを取っている。よって、外部からの「スパムメール受信についてのクレーム」に関しては、電子メールのヘッダ情報と電子メールの送信ログを比較する事により容易に判断が可能な為、すぐに顧客の苦情に対応できるようになっている（システムについて説明すると納得してもらえている）。
・開示請求のマニュアルを作って準備してきた。実際の開示請求はない。開示請求の手数料は実費のみとしている。
・担当は、お客様相談室としている。

（８）事故発生時の対応

（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。

以　上

M. 情報サービス業（ソフトウェア） M 社

業務概要	情報サービス（ソフトウェア）		
従業員数	約 2,000 人	プライバシーマーク取得	あり
保有個人データ件数	約 16,000 件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・独自に収集した顧客情報が約 13,800 件であり、個人向けサービスの運営管理のため、住所、氏名などの他に振込先情報を保有している。

・法人向けサービスの運営管理のため、会社名、部署名、氏名、会社所在地、会社連絡先といった名刺のデータを保有している。

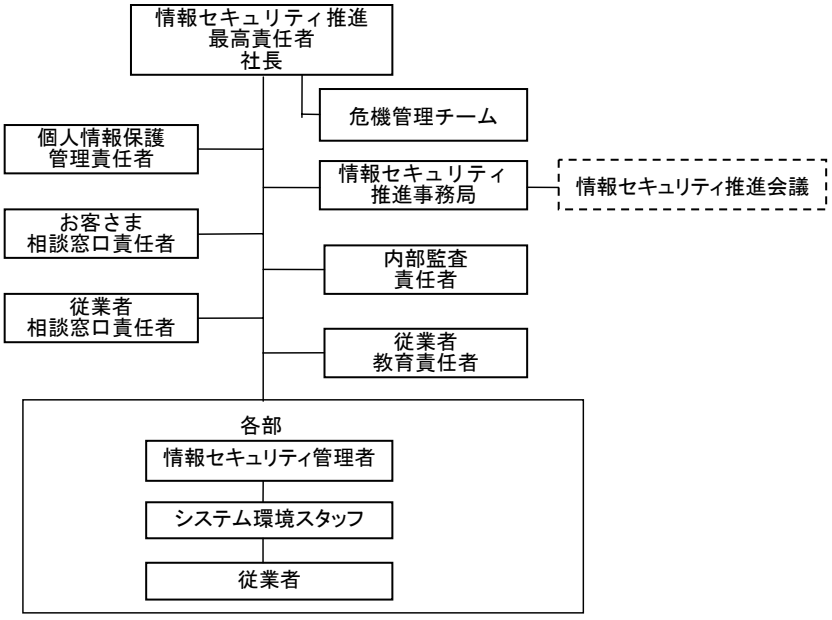
・従業員従業者情報として約 2,200 件程度の情報（出向者を含む）を保有している。

・その他、同社の親会社からの預託情報が約 3,000 万件であり、個人情報は、顧客の住所、氏名、連絡先、利用料金である。同社は親会社から委託を受けて顧客のデータ管理を行っている。

（２）個人情報保護担当部署

・情報セキュリティ推進事務局を品質管理部が担当している。

図表　個人情報保護も含めた情報セキュリティ全体についての推進体制



（３）個人情報保護管理者の有無・位置づけ

・取締役が個人情報保護管理者となっている。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマークは平成 11 年 2 月取得。

・同社はシステムの開発・運用・利用者サービスなどを通じて非常に多くの個人情報の預託又は収集を行っており、適切に管理することが重要な社会的責務であると考えた。認証を得ることにより、日常業務における個人情報の取扱レベルを客観的に判断できること、こうした認証が業務を受託する要件の一つになりつつあることが理由である。

・早期にプライバシーマークを取得した理由の 1 つは同社が JISA の理事会社であり、プライバシーマークへの理解が早かったことがあげられる。

・ISMS は平成 15 年 3 月取得。

・顧客の信頼を得、それを維持していくためには情報セキュリティの確保が不可欠である。そのためにはシステムとして組織的な管理が必要と考え、ISMS の取得を行った。

（５）個人情報保護に向けた取組経緯

・平成 10 年～11 年にはプライバシーマーク制度の発足に伴う認証取得に向けた取組を行った。

・以前から預託情報に対する保護対策を実施しており、プライバシーマーク認証に向けてそれらの対策を規則として成文化するとともに、それらを自社データの保護対策にも準用するなど必要なルールの追加、見直しを行った。

・平成 14 年～15 年には ISMS の認証取得に向けた取組を行った。

・関連会社との合併による新体制のスタートに併せ、新制度の認証取得に向けた規則見直し、体制整備を実施した。

・平成 16 年～17 年：個人情報保護法施行に合わせた取組を行った。

・経済産業省のガイドライン、JISA のガイドラインに沿った規則・マニュアル等の見直し、例えば、委託先に係る規則の制定や説明会の実施、定期的な社員教育の体制整備等、法の遵守のための取組を実施した。

・平成 17 年 3 月に顧客からの申込依頼書約 50 枚を紛失した（本件の担当部署は現在は別会社となっている）。同社はプライバシーマークを早期取得し更新を続けていたが、この事故のため、再発防止策として、個人情報の総点検、取扱方法の再徹底を行うこととした。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・個人情報は、①親会社からの預託個人情報がほとんどであり約 3,000 万件、②事業のため独自に収集したもの 13,800 件、③その他名刺情報や従業者情報（約 2200 件）と

なっている。①については親会社からの指導のもと保管管理等については厳正な取扱いを行っており、②、③については、独自に規則等を制定し管理している。
受託業務における親会社等からの指示・指導による面と自ら自主的に情報管理を実施する両面を有している。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・平成 11 年にプライバシーマークを取得したときには、特にコンサルティング会社に依頼せず、社外研修等に参加し規程・体制づくりをした。
・ISMS 取得の際は、コンサルティング会社へ依頼した。

（２）個人情報の取得

・親会社である委託元から預託されるデータについては、親会社に設置した端末へ入力されたデータが直接同社のデータセンターへ記録されるシステムとなっている。
・法人顧客情報は展示会等で収集する場合が多い。展示会では、利用目的を明示したアンケート等を用意し、個人情報の利用について同意を確認するようになっている。展示会等で利用する文面は、概ね同様な文面を利用している。

（３）個人情報の利用（第三者提供を含む）

・展示会で収集した情報は商品ごとに管理し、ダイレクトメール発送などの営業活動に利用している。
・個人情報保護法施行以来、グループ会社内でも個人情報の共同利用は行っていない。

（４）個人情報の管理

①情報の管理体制

・預託された個人情報をプリントアウトした用紙は、指定された委託元事務所へ送付している。送付時には重要情報輸送の特別契約をした配送事業者（グループ会社）を利用している。
・会社の情報の自宅への持ち帰りは禁止しているが、やむをえない場合は管理者の承認を得、証跡を残して持ち帰ることが出来る。自宅での作業は貸与された持ち出し用パソコンを利用している。
・携帯電話は会社から貸与し、遠隔操作でデータの消去ができるようになっている。また、携帯電話を持ち出して利用する場合には、必ずパスワードをかけることを指導している。

・自宅のパソコンについては残存業務情報の有無について自己チェックを実施した。自宅のパソコンは家族で共有している人もおり、いつファイル交換ソフトがダウンロードされるかわからないため安全とはいえない。したがって、自宅のパソコンでは「業務の使用を禁止する」ルールを定めた。

②従業者への教育方法

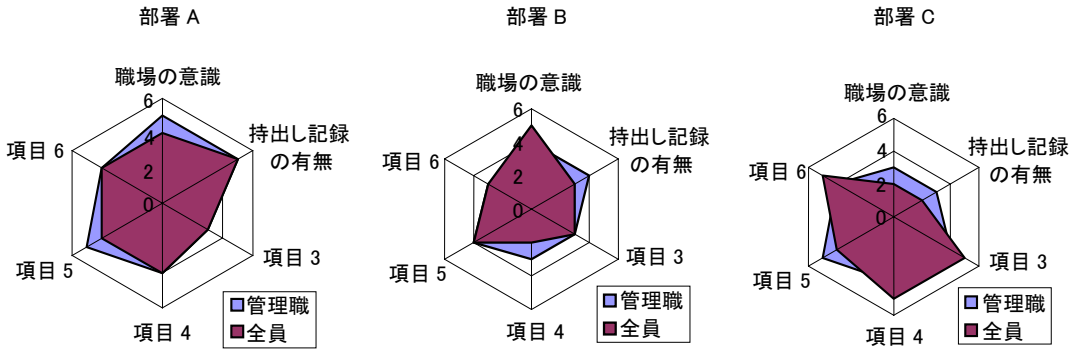
（毎月１７日に総点検を実施、各職場の実態を洗い出し報告）

・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。

図表　チェック結果のレーダチャート（イメージ）



（セキュリティ遵守事項を定め、定期的にチェック）

・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。チェックは部署内で実施された。

（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）

・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。

（年１回全社で e ラーニングを実施）

・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。

③盗難対策

・私物の USB メモリの利用は禁止し、会社貸与のパスワード付 USB メモリを導入している。
・CD やフロッピーディスクについては納品時に利用するので、利用のログが記録できるツールを導入予定である。
・ノート PC、情報記録媒体など携帯可能な機器に対しては、ワイヤーロック、施錠保管している。

④ノート PC の安全対策

・個人所有のノート PC の持ち込みや業務での利用は禁止しており、業務用途では会社

からノート PC を貸与している。
・持ち出し用ノート PC は約 300 台保有しており、貸し出しについては各部署で台帳管理している。
・ノート PC は暗号化ソフトを利用しパスワードをかけている。

⑤外部委託先管理

・外部委託先に個人情報を提供することは原則として行っていない。当社の提供するサービスを利用するお客様に対して、契約等の際に得る個人情報等に関しては、原則として郵送頂くなどの配慮をしている。

⑥日常点検・確認の方策

・各部署は、規則で定めた方法で運用管理している。例えば、個人情報や重要情報に関しては、社外へ持ちだす場合は、管理者の承認を得ると共に、持ち出しの証跡を残している。また、こうした実態にあるかどうかを毎月 17 日の総点検日で確認を行っている。

⑦初歩的ミスの防止策

・重要な紙情報の持ち運びについては、組織長の承認と証跡を残すことで緊張感を持つような配慮をしている。また、昼食時の置き忘れには注意するよう呼びかけている。
・必要な箇所では鍵付の専用カバン等を利用している。また、運搬など定期的な情報のやり取りでは、施錠つきのジュラルミンケースを利用するなどの安全措置を実施している。
・電子メールで個人情報等重要情報を送信する添付ファイルには、パスワード設定を義務付けている。

（５）個人情報の消去・破棄

・法人顧客の情報は 2～3 年で古いものになるため消去し、ダイレクトメール等には展示会で収集する新しい情報に対してのみ送付している。
・情報の廃棄には注意を払っている。情報によっては廃棄されたことが証明できなければ紛失であり重大事故となる。前述の紛失事故が発生した際、新しい管理策が定着するまでの間、紙ごみすべてを一定期間事務所内に保管し、一業務サイクル経過後廃棄するなどの措置を講じた（情報の出入りをすべて抑えることで安心した業務運行となる）。

（６）個人情報の監査

・委託元である親会社の監査組織からの監査が定期的にある。委託元である親会社から

は委託内容について細かい作業内容が指定されている。そのため、監査では、作業途中の経過が指示通り行われているかどうかもチェックされる。立ち入り監査も必要に応じ実施される。

・プライバシーマークと ISMS の内部監査はそれぞれ年 1 回実施している。業務監査の部署が担当している。

（７）苦情処理・顧客対応

・相談窓口は営業総括部長が担当している。現状までで問合せは 2 件程度である。開示請求は 1 件もない。

（８）事故発生時の対応

（個人情報漏えい事故対策訓練を実施）

・平成 18 年 11 月に漏えい事故を想定した訓練を実施。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。

（９）その他

・グループ会社の IT 担当者で構成される研究会のメンバーで「情報セキュリティはじめの一歩」という冊子を作成し、グループ会社全員へ配布した。

図表　情報セキュリティに関するハンドブック（抜粋）

以　上

N. 情報サービス業（ソフトウェア）N 社

事業概要	ソリューションサービス、ソフトウエア開発、 クレジットデータ運用処理サービス、健康関連サービス		
従業員数	約 400 人	プライバシーマーク取得	あり
保有個人データ件数	約 200 万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・全体で約 232 万件の個人情報を保有している。内訳は以下の通り。
　－カード情報：132 万件
　－会員情報　：100 万件
　－顧客情報　：　2 千件
　－社員情報　：　3 千件

（２）個人情報保護担当部署

・事務局は企画室経営企画部が担当している。
・管理部門は各事業部門という位置づけである。

（３）個人情報保護管理者の有無・位置づけ

・個人情報保護管理者は企画室長である。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマークは取得済（平成 14 年 5 月）である。
・運用処理サービス及び一般消費者向けのパッケージソフトを販売するにあたり、会員情報の収集などで個人情報保護の取組を発信する必要性が生じたため、プライバシーマークを取得した。
・平成 14 年の取得は業界では早い方である。取得時点ではクレジットカード会社などの業務委託元からの要請はなかった。
・ISMS も取得済（平成 17 年 3 月）である。
・取得理由は事業展開とより確実な情報セキュリティ管理システムの構築である。

（５）個人情報保護に向けた取組経緯

・97 年：通産省「コンピュータウィルス対策基準」「ソフトウェア管理ガイドライン」に基づく社内規程の制定

・01 年：認証取得体制の整備及び「個人情報保護に関する基本規程」の制定
・01 年：「個人情報管理委員会」を組織、個人情報保護に関する内部監査を実施
・02 年：「プライバシーマーク」認証取得
・04 年：「プライバシーマーク」第 1 回更新
・05 年：「ISMS/BS7799」認証取得
・06 年：「BS7799」を「ISO27001」に移行
・06 年：「プライバシーマーク」第 2 回更新

（6）個人情報の保有・管理・提供等に関する業界の特徴

・情報サービス業界の成熟化とネットワーク化及び IT 化によりビジネス環境とビジネス形態が変化し、必然的に個人情報を取り扱うようになってきた。このようなビジネス背景の中で、個人情報を保有し、管理し、サービスを提供している。
・社会的に個人情報保護の重要性が認識されだした背景には、情報のデジタルデータ化がある。デジタルデータの業務は情報システム事業そのものである。個人情報保護は当初から情報システムサービスにおける個人情報の保護を狙いとしたものであり、情報システム業界は早い段階で個人情報保護の重要性を認識し、対応をしている。
・プライバシーマーク取得企業も多い。またプライバシーマーク取得の要件では委託先にも安全管理を求めるので、業界内で連鎖的に安全管理措置がとられるようになっている。

2．個人情報の適切な保護のための取組について

（1）準備（規程・体制づくり）

・個人情報保護方針については、自社で作成した。
・関連会社が先にプライバシーマークを取得していたため、取組を参考にした。
・個人情報の運営事務局は 3 名で、他業務との兼任で行っている。
・プライバシーマーク取得に際しては、同社より先に取得している同業他社へ見学に行った。

（2）個人情報の取得

・運用処理サービスを委託されることが主であり、個人から直接個人情報を収集することはあまりない。

（3）個人情報の利用（第三者提供を含む）

・直接的な一般消費者向けビジネスはほとんど行っていないため、マーケティングのた

めの利用はしていない。
・委託元からの預託情報が大半であるため、関連会社間での共同利用はない。

（４）個人情報の管理

①情報の管理体制

（機微情報へのアクセスは物理的に厳しく管理）

・同社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。

②従業者への教育方法

・教育は、個人情報管理委員会の教育担当委員が年初に方針を決め、人事総務部が実施している。
・制度の変更時には全社一斉に教育を実施する。
・全社一斉教育とは別に、新入社員の研修時、階層別教育時に教育を実施している。
・定期的にコンプライアンスに関する議論を課単位で行うが、このときにも個人情報保護についても取り上げて認識を高めるようにしている。
・現在セキュリティについて e ラーニングを実施しており、個人情報保護についても検討中である。個人情報については今まではアンケート形式で行っていたが、プライバシーマークの 3 回目の更新時に確認テストをするように指摘された。セキュリティの e ラーニングは自社内で作っているので、個人情報についても自社内で作る予定である。
・派遣社員、パートについては、社内で作業をしているため、受け入れ時に誓約書をとっている。特に個人情報を扱っている部署については、教育を徹底している。

・個人情報保護事務局の従業者の 1 人がプライバシーコンサルタント資格の取得をした。社内で運用推進をし、経験を蓄積することが目的である。他の従業者のプライバシーコンサルタント資格取得も検討中である。
・USB メモリの使用制限などパソコン等安全管理に関する施策については、従業者から厳しいとの声も聞かれるが、従業者のミスを事故にしないための方策であると説明している。

③盗難対策

・サーバは記録媒体を使用できないようにしている。
・個人情報を外部記録媒体に入れることは禁止している。
・パソコンはアクセス制限をかけている。
・USB メモリはすべて情報保護タイプに切り替えた。USB メモリの接続は記録され、利用領域の制限を行っている。

④ノート PC の安全対策

（アクセスロックを多重にかけることで対応している）

・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。紛失しても利用することはできない。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。

⑤外部委託先管理

（外部委託先に出向いて直接指導を行っている）

・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。
・外部の委託先については、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。
・取得していない企業の中で長年の取引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。

⑥日常点検・確認の方策

・入退室時に記録をとっているので、それが日常の確認作業となっている。

⑦初歩的ミスの防止策

・外出時の荷物は１つにするようアドバイスしている。

・FAX では重要情報は送らないよう指示している。仮に送る際には、相手と一度通話してから送るようにしている。FAX の利用そのものが減っているため、事故の可能性も低い。

（５）個人情報の消去・破棄

（紙媒体の情報は外部事業者に委託）

・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。

・CD-ROM についても同一の業者が破砕している。

・コンピュータ内のデータについては、HDD を破砕するようになっている。

・データの消去については、登録用紙に実施日を記載し、確認している。

（６）個人情報の監査

・同社はプライバシーマーク、ISMS を取得しているため、業務委託元からは監査を受けていない。

・社内の監査制度があり、１年に１度個人情報保護監査がある。個人情報保護監査においては、帳票やエビデンスがきちんと蓄積されているのか、運用ができているのか、決められたことが守られているのかを監査している。

・個人情報の監査とは別に、情報セキュリティや環境についての監査がある。

（７）苦情処理・顧客対応

・問い合わせの窓口を設けて対応しているが、現在まで特に苦情はない。一般消費者が問い合わせをする先として同社を認識していないことも理由の一つと考えられる。

（８）事故発生時の対応

・事故の発生時には部門の責任者へ報告され、個人情報保護の事務局、個人情報管理委

員長（企画室長）に報告され、さらに社長に報告される。その後、事故への対応が判断される。また、事務局より JISA への報告を行う。

・事故については、ノート PC の紛失事故が過去にあった。ノート PC については HDD ロック、BIOS ロックがかかっているため、拾っても使うことはできない対策がとってあった。再発防止について検討し、全部門の代表へ通達した。

・事故については、本人への罰則という場合もある。就業規則に沿った処罰となる。

（９）その他

（社内報への写真・個人名の掲載を説明会で説明）

・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。

（環境への配慮と個人情報）

・同社では、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。

以　上

O. 情報サービス業（ソフトウェア）　O 社

事業概要	情報処理・通信、システム開発、システムインテグレーション事業等		
従業員数	約 1,600 人	プライバシーマーク取得	あり
保有個人データ件数	（非公表）非常に多く保有		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・従業者の個人情報としては、従業者が約 1,600 名分、協力会社従業者分として約 1,400 名分を保有している。

・情報処理サービス事業による顧客から預った個人情報（以下「顧客データ（個人情報）」と記載）が最も多く、かなりの個人情報を保有している。

・他、営業活動、フェア、アンケート調査等による直接取得が約 1,000 名分ある。

・情報処理サービスによる顧客データ（個人情報）の利用は契約による情報処理サービスの目的の範囲に限り、システムテスト等における目的外の利用は禁止である。ただし、顧客の契約に基づく依頼により情報システムの開発過程における運用テスト工程におけるシステム性能テストなどによる使用に限定されている。

（２）個人情報保護担当部署

・管理本部リスク管理室（個人情報保護委員会の事務局を務める）

（３）個人情報保護管理者の有無・位置づけ

・個人情報保護委員会委員長（常務取締役クラスが就任する）

・個人情報保護委員会の上部組織としてリスク管理統括委員会（委員長は社長）を設置。

（４）公的資格認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマークを取得（平成 11 年 2 月 1 日）。

・個人情報保護の社会的責任として、また情報処理サービス業として預った顧客データ（個人情報）の保護を目的として取得した。

・その他、ISMS、ISO9000、ISO14000 等も取得している。

（５）個人情報保護に向けた取組経緯

・顧客データの管理については、旧通商産業省の情報システム安全対策の認定事業所として認定され設備基準、技術基準、運用基準等に対応した安全対策について過去から

取組んでいる。
・プライバシーマーク取得後、顧客データ（個人情報）の取扱ルールの見直し、内部監査、社員教育等に一層取組む。
・平成 16 年に顧客データ（個人情報）を記載した運用テスト帳票の廃棄事故が発生し、社会的批判を浴びたことからプライバシーマークの取得や ISMS の認証を取得していても事故が起こることを認識し、個人情報保護の対策の基本を見直し、従業者の教育・指導・啓発を強化して再発防止に一層力を入れるようになった。

（６）個人情報の保有・管理・提供等に関する業界の特徴
・情報サービス産業においては、個人と直接取引きするケースは少なく、直接取得する個人情報は少ない。
・しかし、委託先から膨大な数の個人情報を預って業務の委託を受け、コンピュータ処理するケースが大半であり、大量の顧客データに適した管理を実施することが最も必要になる。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）
（ヒヤリ・ハット事例集の作成・掲示）
・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。

（２）個人情報の取得
・保有している個人情報のうち直接取得した個人情報の割合は極めて少ない。情報処理サービスの上で顧客から大量の個人情報を貸与される。
・直接取得する個人情報は、フェアの入場の際に入場者名簿に記載した個人情報、又は、その入場時に渡された名刺の個人情報に限られる。この場合、個人情報の取得において、事業者の名称、個人情報管理責任者、利用目的、第三者提供又は共同利用の有無など個人情報を直接取得する条件をフェア入場入口の受付に掲示している。
・アンケート調査で個人情報を取得する場合、上記の取得条件をアンケート説明資料に

記載している。

・顧客データ（個人情報）の運搬に関しては、インターネット上のオンラインストレージや電子メール添付による顧客データ（個人情報）の転送を禁止している。個人情報を記録した磁気媒体や紙でも、専用運搬車を用意し、運搬専任の担当者がおり、その者が顧客から顧客データ（個人情報）を預かって 2 名が同乗して運搬するルールである。

・顧客データ（個人情報）を万が一緊急で個人情報を運搬しなければならない場合にも、専任運搬者に依頼して専用運搬車で運搬することを原則としているが、専用運搬車が手配できないとき、SE 担当者とその上司の 2 名が顧客を訪問して個人情報を受理・運搬し、その旨を無事に運搬できたことを「緊急運搬台帳」に記録し顧客に報告することで対応している。

（３）個人情報の利用（第三者提供を含む）

・アンケート調査やフェア等で直接収集した個人情報は、営業活動の利用を目的としており第三者提供は行っていないが、グループ会社と営業活動する際に共同利用するケースはある。

・顧客データ（個人情報）の利用については、情報処理サービス契約、サーバハウジング契約、サーバホスティング契約に基づいた顧客データ（個人情報）の利用目的に限っている。また、情報システム構築に際して、運用テスト工程における運用性能テストに使用する顧客データ（個人情報）の利用も契約による利用目的及び範囲に限っている。

（４）個人情報の管理

①顧客データ（個人情報）の管理

（建物内における“セキュリティ区画”の設置）

・「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＞はサーバ室等で顧客データ（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、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。

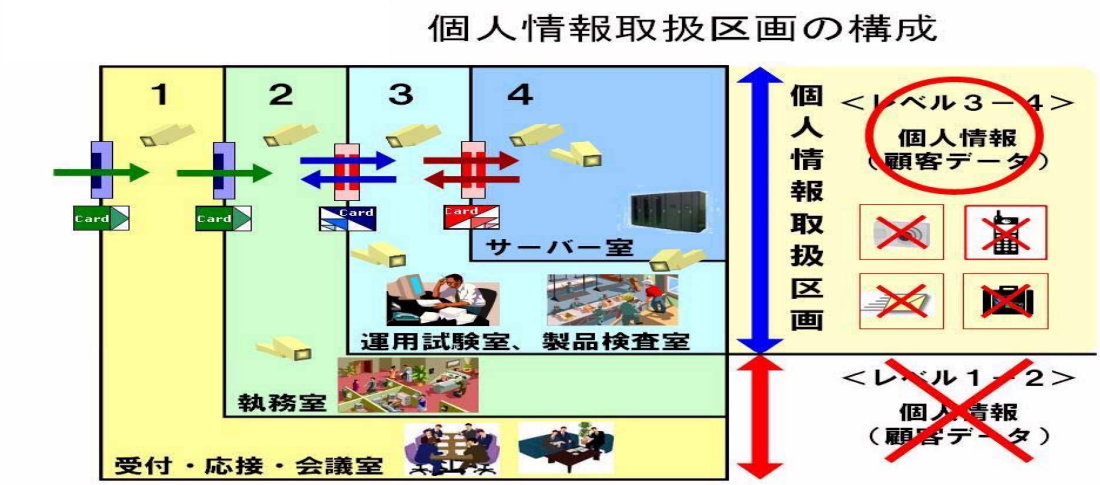
・これら 2 つのエリアにのみ顧客データ（個人情報）の持ち込みが許されている。又は、その 2 つのエリアにおいては、カメラ、携帯電話の持ち込みが禁止されており、カバンの使用、及び電子メールの発信等も禁止されているなどそれぞれの設備対策が施されている。＜レベル 3、4＞の社内ネットワークが＜レベル 2 ＞の執務室の社内ネットワークやインターネットと分離されているため電子メールの送受信や WEB 閲覧がで

きなくなっており、顧客データ（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、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



（ファイル共有ソフト（Winny 等）対策の徹底）

・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。

②従業者への教育方法

（個人情報保護の日の設定）

・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。

（個人情報保護３原則の設定）

・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 に顧客データ（個人情報）を預ける場合があるため、SE に顧客データ（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」の標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て３原則を徹底している。

図表　「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

（社内資格認定試験の実施）

・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を認めた従業者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。

図表　社内資格認定試験の概要

図表　社内資格の認定証

（事件・事故を具体例で示す）

・従業者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策が求められる。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。

（部単位でのセキュリティ・ミーティングの実施）

・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。

③個人情報の盗難対策

・フェア入場者の入場名簿及びアンケート調査によって取得した個人情報については、利用者制限、アクセス権限、保管ルールなどの管理ルールを定めて不正利用、不正アクセスによる不正コピーによる盗難を防止している。
・顧客データ（個人情報）の盗難防止として、ロボットを内臓したカードリッジ保管庫（LSM：Library Storage Module ）に格納されたカードリッジに顧客データ（個人

情報）を記録しており、この顧客データを情報処理に使用する場合、LSM のロボットがカートリッジをセットする。オペレータは直接カードリッジにふれることができない仕組みにして顧客データ（個人情報）の盗難防止をおこなっている。

④ノート PC の安全対策

・ノート PC は自分の机の引出しに入れ、施錠するように指導している。
・セキュリティワイヤーの使用を禁止している。セキュリティワイヤーによる盗難防止では、ノート PC 本体の盗難を防ぐことはできるが、ノート PC に記録された情報が盗まれる可能性がある。
・複数人が使用できるようなロッカーに格納することも禁じている。最終格納者となる本人が本人以外のノート PC の情報を盗難できる状況になるからである。

⑤外部委託先管理

・個人情報の外部委託は、情報処理サービスにおけるパンチ業務の委託がある。システム開発の技術者やオペレータ運用要員を派遣先から派遣社員を受け入れる場合がある。また、システム開発の一部を請負会社に委託する場合がある。
・派遣社員や社内で勤務する請負会社の従業者にも社内資格の個人情報取扱資格初級試験（前記（社内資格認定試験の実施）参照）を受験してもらい、合格することを要件としている。
・新規委託先や取引審査、既存取引先においても定期的に取引審査を実施している。個人情報を預託する場合、通常の取引審査に加えて「個人情報預託先審査書」によって審査され、審査合格をもって個人情報のパンチ委託を可能としている。

⑥日常点検・確認の方策

（３つのシールで対策を「見える化」する）

・＜レベル２＞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」、顧客データ（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顧客データ（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、パソコンに顧客データ（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顧客データ（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、顧客データ（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他の事業所への持ち込みが出来なくなってしまう。

図表　「見える化」のためのシール（３種）

⑦初歩的ミスの防止策

（電子メールの誤送信対策）

・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、同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、およそ 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。

（５）個人情報の消去・破棄

・通常の業務において、顧客データ（個人情報）の破棄は大きく２ケースがある。

・一つ目は、ホストコンピュータによる大量プリント工程におけるセット位置の試しプリント、用紙のジャムリによる仕損じなどの用紙の破棄がある。これらの廃棄用紙に顧客データ（個人情報）が記録されている場合もある。この廃棄用紙をダンボール箱に梱包する。廃棄担当者は、そのダンボール箱のままシュレッダーに入れて廃棄用紙を箱ごとシュレッダーにかける。廃棄担当者は、個人情報が記載された廃棄用紙を見ることはできない。また、シュレッダーされたゴミは自動梱包され溶解業者に渡される。

・二つ目はシステム開発における運用テストの確認のために出力されたテストプリントの破棄である。テストプリントされた帳票に顧客データ（個人情報）が記載されている場合がある。テスト帳票の確認後、この帳票を破棄する場合、<レベル３>に設置されたシュレッダーで粉砕する。粉砕されたシュレッダーのゴミはシュレッダー袋に格納され秘密保持契約している廃棄業者に焼却処分を依頼する。SE は、確認するために出力した帳票の使用とシュレッダー破棄したときのシュレッダー袋に表示されたシュレッダー袋管理番号を「顧客データ使用記録台帳」に記録する。また、シュレッダー袋を破棄業者に渡したことを「シュレッダー出庫記録台帳」に記録する。これによって、SE が使用した顧客データ（個人情報）を破棄したことをトレースでき、顧客データ（個人情報）が消滅したことを証明できる。

（６）個人情報の監査

（外部有識者による委員会の設置）

・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。

（リスク管理室による監査）

・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た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チェックできるような頻度で回っている。

（７）苦情処理・顧客対応

・営業活動におけるフェアやアンケート調査により個人情報を直接取得しているため個人情報保護法に基づいて開示対応ルールを定めている。
・開示請求に対応するために対応者のマニュアルを制定して開示依頼者に対する対応手順を明確にしている。
・開示対応手数料は 1,500 円に設定している。実際に個人情報の抽出に掛かる手間などを含めると数万円掛かる計算になるが、世間の相場にあわせている。

（８）事故発生時の対応

・事故発生時の対応は個人情報保護に限定せず、BCP（ビジネス・コンティンジェンシー・プラン）の一環として体制を決めている。事故発生時に最も重要になるのは役割分担であり、どの部署の誰が何を担当するかということが事前に明確になっていることが必要である。
・個人情報事故が発生した場合、リスク管理統括委員会又は個人情報保護委員会が緊急対策本部の役割となり、現在の部署がそのまま危機管理対応の部署として位置づけになることで、役割が混乱しないようにしている。

本調査で整理した個人情報の管理については、情報処理サービス業における情報システム開発室（執務室）で働く SE 業務の情報セキュリティ対策を中心とした整理であり、コンピュータ室やデータセンターにおけるセキュリティ対策及び社員情報などのインハウス対策の紹介は一部のみの記載としている。

以　上

Ｐ．情報サービス業（ソフトウェア）　Ｐ社

事業概要	システム開発等		
従業員数	約 350 人	プライバシーマーク取得	なし
保有個人データ件数	5,000～10,000 件程度		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・5,000～10,000 件程度
・従業者の個人情報、入社希望の学生の個人情報、契約のあるパートナー会社の職員の個人情報を保有している。
・委託元（顧客）から個人情報を預ることは無い。業務形態が顧客企業に常駐してシステム開発を行うことが主であり、顧客企業からは持ち出さないようにしている。
・従業者やパートナー企業の職員等の個人情報は通常の社内管理に利用している。

（２）個人情報保護担当部署

・セキュリティ推進委員会が経営会議の直下に置かれている。常設の会議である。
・同委員会の事務局はビジネス推進部の一部の職員が担っている。
・同委員会は社内の全部門から、プロジェクト・リーダー候補者程度のクラスの者が参加する。十数名程度で構成されている。

（３）個人情報保護管理者の有無・位置づけ

・セキュリティ推進委員長が該当する。管理部担当の専務である。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・ISO27001 を取得している。
・顧客からは「個人情報保護」ということよりも、「セキュリティ体制の確立」を要求されることからこの認証を取得している。プライバシーマーク取得の予定は無いが、ISO27001 で個人情報保護の分野もある程度カバーできていると考えている。

（５）個人情報保護に向けた取組経緯

・平成 14 年に個人情報保護法が施行されたことを受け、全従業者とパートナー企業向けにセミナーを開催した。同セミナーでは開催後に○×方式の試験を実施し、理解度が不足している者については補習を実施した。
・このセミナーを皮切りに、従来のセキュリティガイドを改訂し、経済産業省のガイド

ラインを社内的に分かりやすくカスタマイズするなどした。

（６）個人情報の保有・管理・提供等に関する業界の特徴

（顧客企業の要求する個人情報保護水準に合わせることが必要）

・顧客企業内に常駐することも多く、顧客企業の策定している個人情報保護水準に合わせた対応を取ることが求められる。

・顧客企業の水準が自社の水準より高い場合にはその水準に合わせ、顧客企業の水準が自社の水準より低い場合には自社の水準に合わせるようにしている。場合によっては自社の個人情報保護水準で仕事をさせてほしいということで顧客に個人情報保護のあり方について提案することもある。

・顧客によって個人情報保護水準が異なることから、個人情報保護水準の低い顧客の事業所に常駐していた職員が、急に個人情報保護水準が厳しい顧客の事業所に移った場合にギャップが大きすぎて戸惑うこともあるので、いかに一定水準の個人情報保護水準を意識させておくかということが重要になる。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

（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）

・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。

（２）個人情報の取得

・特徴的な取組はなし

（３）個人情報の利用（第三者提供を含む）

・特徴的な取組はなし

（４）個人情報の管理

①情報の管理体制

・定期的に禁止ソフトの使用状況を調べるパッチのツールを自社開発し、システム開発現場で使用しているパソコンや自宅のパソコンで定期的にチェックしている。

・現在は、本人にやってもらい、自己申告となっているが、近々監視ツールを導入し、本社機構で状況を把握できる体制とする。
・常駐している場合には顧客から端末も貸与され、自社パソコンの使用は認められないことも多い。これらは顧客が独自に不要ソフトのチェックなどは実施しており、持ち出しや外部接続も禁止されているので、自社独自の対策は行わない。ただし定期的にプロジェクト監査を行い、従業者のルール遵守の確認を行っている。

②従業者への教育方法

（目標管理制度的に、職員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）

・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。

（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）

・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。

（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）

・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。

③盗難対策

・特徴的な取組はなし

④ノート PC の安全対策

・内容の暗号化、チェーンロックの使用をしている。

⑤外部委託先管理

（委託先の管理水準を高めるために、安価に認証取得の支援を行う）

・自社が取得している認証について、委託先が取得する意思がある場合には、安価な金額で認証取得を支援している。

・委託、再委託を行う事業者についても一定の資格を取得している事業者に委託することが顧客から求められつつある。

・従来の取引関係を解消して、新たに認証を取得している事業者に委託するのは業務遂行上、問題があるので、従来から委託関係がある事業者の認証取得を“支援”し、取得させることで、委託関係を継続するようにした。

・特に自社が認証取得のために採用した仕組みや規程に拘泥することなく、それぞれの委託先企業の実情に合わせたシンプルな仕組みや規程にすることを心がけている。支援や助言は行うが、最終的な判断はすべて委託先企業が行うよう誘導している。

・年１回の委託先教育を実施している。

⑥日常点検・確認の方策

・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。

⑦初歩的ミスの防止策

・特徴的な取組はなし

（５）個人情報の消去・破棄

・シュレッダーの使用は禁止している。シュレッダーでは万が一の場合に書類を再生されてしまう可能性があるからである。セキュリティ情報等を廃棄する専門の事業者に委託している。

（６）個人情報の監査

（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）

・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

（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行う）

・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。

（７）苦情処理・顧客対応

・特徴的な取組はなし

（８）事故発生時の対応

・連絡網と役割についてセキュリティ管理基準書に明記し、研修時に繰り返し意識付けを行っている。

以　上

Q. 情報サービス業（コールセンター）　Q 社

事業概要	コールセンター		
従業員数	約 130 人(正社員数)	プライバシーマーク取得	あり
保有個人データ件数	従業者の個人情報： 約 35,000 件 顧客預かり情報：推定約 50,000 件 （1 企業につき、7,000 件～30,000 件） ※顧客預かり情報は都度変更される為、正確な件数は把握出来ない。		

１．個人情報に関する概要

（１）保有個人情報件数、個人情報の種類、個人情報の利用目的

・同社が取扱う個人情報は、従業者の個人情報と、受託しているコールセンター事業を運営する中で取扱う顧客企業の顧客の個人情報の 2 種類である。

・保有個人情報件数は、保管している給与台帳の従業員数と同じで、約 35,000 人分の個人情報（7 年間の給与データ、DB : 約 20,000 人分、書面 : 約 15,000 人分）である。

・正社員数は 130 名である。オペレータは契約社員である。正社員も研修時にオペレータ業務を行うことがある。基本的に正社員はコールセンターではオペレータの管理業務を行う。

・顧客企業の顧客の個人情報（顧客企業の保有個人データ）は、主に大手通信事業者の顧客情報であり膨大な量である。ただし、同社は個人情報の預かりはしていないため、トータルの件数は把握していない。

・顧客から個人情報を預かる件数は約 50,000 件である。

（２）個人情報保護担当部署

・経営管理部経営管理室

（３）個人情報保護管理者の有無・位置づけ

・経営管理部・経営管理室 ジェネラルマネージャーが個人情報保護の責任者である。情報セキュリティの責任者も兼務している。個人情報保護の実施と運用に責任を負っている。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・取得認証：プライバシーマーク（有効期間平成 17.05.16～平成 19.05.15）

・理由：個人情報保護への取組を体系化するとともに、従業者の個人情報保護意識・取

組の一層の向上を図るためである。

・効果：従業者の個人情報保護への取組意識が更に向上し、コールセンター業務を行う事業者としての営業活動における他社との差別化が可能となる。

・当社が全社を上げて（コールセンターの現場だけでなく、事務部門も一体となって）個人情報保護に取組む体制を整備するために「最適の仕組み」と考え、プライバシーマーク認証を取得し、従業者の監督、安全管理措置、社員研修に取組んでいる。

（５）個人情報保護に向けた取組経緯

・テレマーケティング業務を行っていく上でも、通信事業に従事する企業としても、個人情報保護に向けた取組は必須である。プライバシーマーク認定を取得することによって対外的にもその「証」になると理解している。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・テレマーケティング業界は、取扱う個人情報の保護・守秘義務は、企業存続のため当然のことと考えている。

・短期間で終了する業務のオペレータも多く、要員の入れ替わりが激しいため、教育の徹底が課題である。

・テレマーケティング業界はプライバシーマーク取得が進んでいる。顧客企業（官公庁、民間ともに）からは個人情報保護を強く求められている。そのためプライバシーマーク取得は最低条件である。取得していなければ競争できない。

・個人情報の保有状況は各テレマーケティング企業の業務内容によって異なる。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・同社の成り立ちは通信事業者の一部門であり、現在も通信事業者のコールセンター業務を受注している。このため、従来から通信の秘密についての取組は行っていた。この通信の秘密の保持の取組を個人情報保護へと広げ、規程・体制作りを行っている。

・通信の秘密の保持と個人情報保護については、守るべき項目が増えただけで、特に問題はなかった。

・コンプライアンス担当は２名。個人情報保護の他に企業情報、法令順守、社内ルール等も担当している。現在 JISQ15001：2006 年版の対応を行っている。業務の 5～6 割は個人情報保護に割いている。

（２）個人情報の取得

・業務の大半を占める通信事業者のコールセンター業務では、個人情報は預からない。オペレータが顧客である通信事業者の社内に出向き、設備・機器は顧客の通信事業者提供のものを利用し、業務を実施している。取扱う個人情報はすべて通信事業社内で閲覧している。

（３）個人情報の利用（第三者提供を含む）

・顧客のデータであるため、顧客が定めた利用目的以外の利用はしない。

（４）個人情報の管理

①情報の管理体制

・個人情報を外部へ持ち出すことはほとんどない。顧客から預かる事例はほとんどなく、預かりが発生した場合には専用線で受け渡しする。

・自社における入室はテンキーで管理している。キーは定期的に変更している。オペレーションサテライトでは、一部 IC カード管理を導入している部署もある。全社的に IC カード管理とするとコストがかかるので採用していないが、今後は検討したい。

・来訪者の入室にはゲストカードが必要である。来訪者は管理簿に記載する。

②従業者への教育方法

・オペレータへの教育は、顧客との契約に沿った教育と、同社独自の教育がある。顧客企業が直接オペレータに教育する場合もある。

・業務の教育は同社内で約１ヶ月間実施する。このときにセキュリティや個人情報保護についても教育している。セキュリティや個人情報保護については、社内研修の初期に実施すると、現場に出る頃にはすっかり忘れてしまうケースがあるので、最近では現場に出る直前にも再度教育をするようにしている。

（社外業務者には契約更新時に研修を実施）

・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、業務先の現場で行っている。

・退職者については、情報を外部に漏えいしないという誓約書をとっている。

③盗難対策

・USB メモリは持ち出し禁止にしている。

・一部の委託元からは、つなぎのようなポケットのない服装の着用やロッカーに私物を入れる、透明なビニールの袋を利用するといった要求があり、対応している。

④ノート PC の安全対策

・ノート PC は持ち出し禁止にしている。どうしても必要な場合は、目的を記載した申請書を提出させる。業務が終了したら返却させる。

⑤外部委託先管理

（委託元へ個人情報保護のあり方を提案）

・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。

⑥日常点検・確認の方策

（毎日朝礼時に「情報管理の誓い」を唱和）

・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。

・従業者全員に宛てたイントラネットを通じて個人情報漏えい事件・事故の事例を紹介し、個人情報保護への取組の重要性について周知・啓蒙を行っている。

・自主点検表を作り、現場の機密管理者が日常的に状況をチェックしており、オペレータの入れ替わりがあってもセキュリティを保てるように注意している。

⑦初歩的ミスの防止策

（誤 FAX 防止のため FAX 送信は 2 名以上で確認）

・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、相手先等から入

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。

（誤封入防止のため複数人でチェック）

・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。

（電子メールの自動送受信は禁止）

・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。

（５）個人情報の消去・破棄

・個人情報が記載された書面は、業務終了時に即時シュレッダー処理を実施する。

・原則、メディア（FD・CD・MD など）類の使用は禁止しているが、業務上止むを得ず使用した場合には、データ消去の記録を残し、破棄する際には物理的に裂傷処理している。

・産業廃棄物業者を指定し、機密保持契約を締結している。

（６）個人情報の監査

（テレビ会議を利用した監査を検討）

・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。

（７）苦情処理・顧客対応

・開示の手数料は 1500 円としている。
・カード会社から本人確認の問合せがあった場合、本人が在籍証明をとるように指示している。

（８）事故発生時の対応

・各部署にて契約先の企業担当者を含む緊急連絡体制図を作成しており、有事に備えている。

（９）その他

・個人情報管理については、同社は現場からトップまで一丸となって取組んでいる。常に社内外の情報を共有し、高い意識を維持するよう努力している。
現場で行われる教育のみならず、時には本社から経営陣が出張し、直々に機密管理研修を実施することもある。毎日顔を合わせる上司だけでなく、普段は遠い本社に在籍している企業のトップからも同じ指導を受ければ、オペレータの納得感が増すからである。
機密管理教育は、一度実施すれば良いというものではなく、形式や担当者を変え、定期的に継続することが重要である。

以　上

R. 複合（情報システム／製造）R 社

事業概要	情報システム業、化学品の製造販売等		
従業員数	約 500 人	プライバシーマーク取得	あり
保有個人データ件数	顧客名簿約 40 万件、預かりデータ約 53 万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・顧客名簿に 40 万件の個人情報が含まれている。

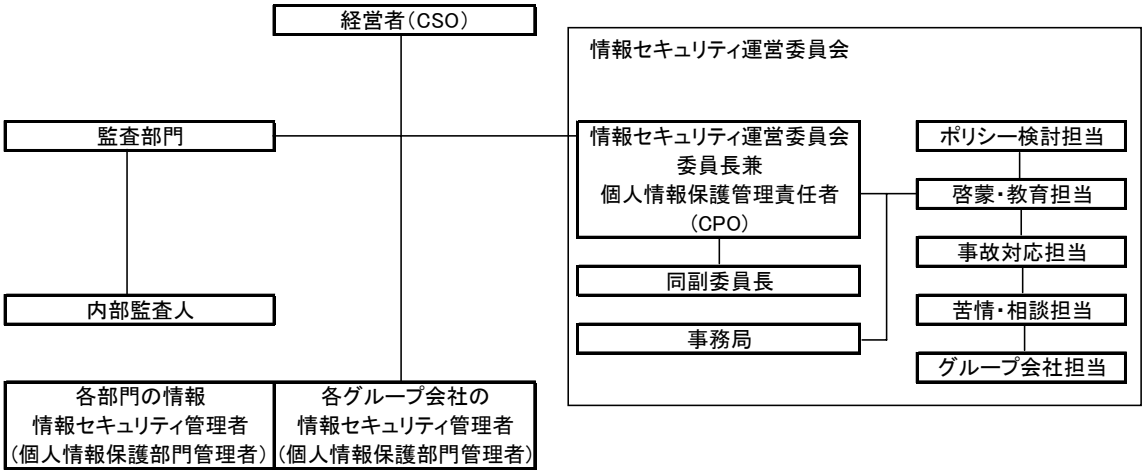
・顧客名簿の個人情報は、会社名、個人名だけでなく、趣味、接待情報、誕生日、家族の誕生日等、営業上知り得た情報についても含まれている。

・テストデータが 1,000 件、顧客から預かったデータは約 53 万件である。

（２）個人情報保護担当部署

・推進室が情報セキュリティ運営委員会の事務局となっている。

図表　個人情報保護組織図



（３）個人情報保護管理者の有無・位置づけ

・CPO は専務取締役である。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマーク、ISO9001、ISO14001、ISMS、BS7799-2 の認証を取得している。

・情報システムインテグレーション及び情報システムアウトソーシング等の事業を通じ、多くの顧客の個人情報を預かっており、社会的責任が極めて高い。特に情報システムアウトソーシング業務の推進にあたっては、顧客からプライバシーマークの取得を求められるケースが増加した。
・そこで個人情報保護への取組を一層強化し、顧客からの要求に応えるため平成 15 年 5 月よりプライバシーマークの取得に取組んだ。

（５）個人情報保護に向けた取組経緯

・平成 15 年の 7 月に「個人情報保護方針」を制定し、ホームページやパンフレットを用いて社内外に公開した。8 月には JIS 規格に基づき構築した「個人情報保護に関するコンプライアンス・プログラム」の運用を開始した。
・その後、平成 16 年 2 月 24 日にプライバシーマークの認定を受け、平成 17 年 1 月には個人情報保護を含む情報セキュリティ活動の適用範囲をグループ 13 社まで拡大した。
・平成 16 年 8 月に発生した「USB メモリ紛失事故」後、情報資産保護策（HDD パスワード、暗号化、媒体管理の徹底）を追加した。
・個人情報保護法が正式施行された平成 17 年 4 月に、利用目的や取扱方針を追加した「個人情報保護方針」をホームページに公開し、2 年間で規程やガイドラインを延べ 29 文書改版した。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・特になし

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・当初は情報システム部門のみの課題であるという認識があり、全社的な協力を得にくかった。経営者が全社体制を一気に作り上げる必要性を感じ、コンサルタントに依頼し、体制づくりをした。
・規程・体制づくりには人件費等含めて約 1 億 2,000 万円要した。この中にはコンサルティング費用も含まれており、コンサルティングに要した費用は約 6,000 万円であった。
・自社 12 部門とグループ会社 14 社の情報セキュリティ管理者が個人情報保護部門管理者として個人情報の管理を実施している。情報セキュリティ運営委員会の事務局の推進室はマネジメントシステムの担当部署であり、2 名で対応している。同社は事業部

単位で運営されているが、推進室は部門横断的な組織である。
・月に一度情報セキュリティ運営委員会が開催され、各部門の責任者が参加する。
・情報セキュリティ運営委員会は、ポリシー検討担当、啓蒙・教育担当、事故対応担当、苦情・相談担当、グループ会社担当が委員となっている。それぞれが業務として教育人事、法務の担当者であり、自分の仕事に近い役割を割り当てられているため、本業の延長として取組むことができる。
・毎月実施する会議では、制度変更、事故等の報告や対策などが話し合われている。仮にこの会議内容を外部に依頼するとしたら約 4,000 万円かかるという試算になった。毎月 2～3 時間の会議を実施することによりこのコストを削減できている。

（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）
・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
・独自の個人情報で最も多いものは顧客名簿で約 40 万件である。
・これは営業等で取得する名刺データから作成しているもので、全事業部で利用が可能である。顧客名簿では、会社名、個人名だけでなく、趣味、接待情報、誕生日、家族の誕生日等、営業上知り得た情報についてもデータ化している。

（３）個人情報の利用（第三者提供を含む）
・顧客名簿についてはグループ内で共同利用をし、有効活用を目指している。営業の引き合い段階で過去の営業履歴などを見ることができる。

（従業者は名刺交換の有無により、顧客情報を閲覧できる範囲が異なる）
・従業者によって、顧客名簿の閲覧可能な内容を分けている。従業者が顧客名簿を閲覧する場合、対象と名刺交換をしたことがない場合には会社名、氏名といった名刺情報程度しか見ることができないが、名刺交換をした人の情報についてはより深い情報を見ることができるようになる。
・役員や上級幹部はすべての情報を見ることができる。特定の従業者しか知り得ない情報はデータベースで保管しているが、取得した本人しか見ることができないようになっている。
・データは 1 年に 1 度スクリーニングしており、機微情報と判断されるものについては

消去するよう指示している。消去の必要の有無については監査や運営委員会で判断している。

（４）個人情報の管理

①情報の管理体制

（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）

・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。

・入退館時には扉が大きな音をたてて開閉するため、人の出入りが警備室等でわかるようになっている。

（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）

・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。

・ファイル共有ソフトについては、社内掲示板でも呼びかけている。

②従業者への教育方法

・1 年に 1 度集合研修を行っている。顔を合わせた場で説明することにより、制度や個人情報保護の重要性について理解が得られる。

・集合研修以外に新規採用時と階層別研修時にも教育をしている。

・単なる事故事例の紹介だけではなく、社内での事故につながる状況などについて具体的に紹介し理解を深めてもらう。

③盗難対策

・記録媒体は暗号化しないと持ち出せない仕組みになっている。

④ノート PC の安全対策

（持ち出し禁止シールを貼って対応）

・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外部委託先管理

・個人情報の取扱いは社内で実施することが決められている。社外で委託先が取り扱うことはない。

⑥日常点検・確認の方策

（「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）

・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、半年ごと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

・月に一度の情報セキュリティ運営委員会で初歩的ミスの防止について討議している。
・個人情報の漏えいは初歩的ミスが原因であることが多い。事務局が事故を報告し、その原因や対応について具体的に考える。例えば輸送時に事故が起こったケースでは、本来発送すべき人と実際に発送した人が異なっていた。発送者は指定の運送事業者があることを知らず、異なった事業者に依頼して事故につながってしまった。このようなケースを取り上げ、対策について検討していく。
・初歩的ミスの防止として様々なルール作りをしている。“電子メールの CC 配信を上司立会いで実施する”というルールも導入を検討したが、事前の従業者アンケートで業務に支障がでると反対が多かったため見送った。

（５）個人情報の消去・破棄

・紙の情報については少量の場合はシュレッダー、大量の場合は溶解処分としている。
・サーバやパソコン上の情報については消去ソフトを利用している。パソコンを破棄する場合には HDD は破砕している。
・顧客情報については消去していない。いつ利用のチャンスがめぐってくるかわからないからである。例えば、顧客の一人が顧客情報に記載されている会社を退職しても、転職先で顧客となる可能性がないわけではない。その際には履歴を使用して、より良い営業につなげることを企図している。

（６）個人情報の監査

（トップの指示により、年に 4 回の監査を実施）

・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。

（７）苦情処理・顧客対応

・従来から顧客窓口は総務部サービス本部が担当しているため、個人情報に関する窓口もサービス本部が担当している。

・開示請求については手順を定めている。手数料は取らないことにしている。基本的に開示請求の対象者となる個人は顧客であり顧客からは手数料を受け取りにくいからである。

・問合せについては電話での対応はしないというルールになっている。そのため電子メールのみ連絡先として掲載している。顧客は電子メールを利用できるので、電子メールのみでも特に問題はない。

（８）事故発生時の対応

・事故発生時には責任者へ報告され、対応が検討される。

・　何かあったらすぐに社長へ報告することになっている。

以　上

S. その他サービス業（教育、学習支援）　S 社

事業概要	学習塾の運営等		
従業員数	約 1,200 人	プライバシーマーク取得	あり
保有個人データ件数	約 180 万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・学習塾に通う生徒（65.000 人）とその保護者の個人情報が 20 万件程度である。
・ダイレクトメールのデータベースが 160 万件程度である。
・従業者情報が 8,000 件程度である。
・英語講座等の顧客情報が 2,000 件程度である。
・生徒情報は、氏名、生年月日、住所、電話番号、所属学校、学年、志望校、成績、得意科目、保護者の氏名、保護者の口座番号などである。
・生徒情報は指導のため、ダイレクトメール情報は営業活動のために利用している。

（２）個人情報保護担当部署

・担当部署は塾長室である。
・現在は組織改変の最中であり、平成 18 年 10 月からは経営管理室に主管を移した。

（３）個人情報保護管理者の有無・位置づけ

・現在の個人情報保護に関する統括責任者は教育事業本部の本部長である。
・平成 18 年 10 月以降は現在の経営管理室の室長が責任者になった。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマークを取得している。（平成 17 年 1 月）
・コンプライアンスプログラムに則り、個人情報保護のレベルアップを図るため。

（５）個人情報保護に向けた取組経緯

・個人情報保護に関する取組をしっかり行っていることを客観的に示すために認証取得を目指した。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・「成績」を個人情報として保有している、ということが特徴的である。
・正社員ではない教師が個人情報を扱う場合もあるため、取扱方法の徹底、意識向上が

不可欠である。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・ＪＩＳＱ１５０００１に準じた規程を段階的に導入

（２）個人情報の取得

・生徒情報は、生徒が入塾する際に取得する。利用目的は入塾申込書に提示する紙に書いてある。

・情報の取得元は保護者である。保護者の直筆で、捺印ももらうようになっている。

（３）個人情報の利用（第三者提供を含む）

・生徒情報は指導のため、ダイレクトメールデータベースは営業活動のために利用する。

・生徒情報は、合格者の分布を数値的に把握するなど氏名や属性が識別できない形で分析に利用している。

（４）個人情報の管理

①情報の管理体制

・個人情報データは、認証取得以前は“教室ごと”で分散して管理していたが、今は一元的に管理している。

・システムは様々なものを使っているため、個人情報が別々のサーバに保管されていて、一括で大量に漏えいが発生するリスクは低くなっている。これは導入時期の違いの影響もあり、将来的には安全性の強化に配慮しつつ統合する方向で検討している。

・情報システムへのアクセスは、アクセスの権限を決め、ID とパスワードで管理している。

・手書きの資料報告書のような紙媒体の情報については、ファイル保管ルールを定めて管理している。廃棄の際は、規程に従い処理している。

②従業者への教育方法

・時間教師（学生）は採用後に１ヶ月間、集合研修を行う。生徒への対応の仕方などの指導に加えて、個人情報の取扱い等コンプライアンスに関することについても教育している。研修後はテストを行い、結果によっては再度研修を行う。

・配属後、月に１回、教室内での研修を受けるようにしている。

・遵守事項や注意点などを「塾内報」に盛り込み、部署ごとに確認している。

・コンプライアンス研修を年に 3 回行っている。契約や個人情報以外も含め、知っておくべき知識や運用事例を紹介している。
・安全対策試験を行っている。責任者が対象で、合格ラインを超えていない場合には再研修を行っている。分野別の内容になっており、特定分野において得点が低い従業者に対しては面接指導を年に 1 回行っている。安全対策試験終了後は、各人に成績表を返している。

③盗難対策

・パソコンの鎖による固定、保管場所の施錠の徹底など規程に定められたとおり運用している。

④ノート PC の安全対策

（ノート PC の配布は特定の従業者に限定）

・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。

⑤外部委託先管理

・模擬試験を開催する企業に対して、住所、氏名といった個人情報を受け渡すことがある。委託先とは秘密保持契約を結んでいる。委託先の管理体制について監査を行っている。
・口座振替のため、金融機関に口座情報や氏名といった情報を受け渡すことがある。

⑥日常点検・確認の方策

・出席簿の保管、成績表の取扱いの注意は各現場で行っている。

⑦初歩的ミスの防止策

・FAX は送信者がその場で番号を打ち込むことを避け、予め登録された番号を選択し、送信するシステムにしている。これに対応するため、FAX の機種の入れ替えをした。このシステムによって情報の更新が容易である。
・電子メールはグループウェアを使用している。

（５）個人情報の消去・破棄

・紙の情報は年に 1 度溶解破棄している。
・年度によって使う情報が限られているため、特定の情報は年度ごとに廃棄している。
・全事務所にシュレッダーを入れており、重要な情報はシュレッダー処理している。

・模擬試験を他社へ依頼する場合、情報は委託先で破棄してもらう。

（６）個人情報の監査

・プライバシーマークの導入に従って、年に１度監査を行っている。

（７）苦情処理・顧客対応

・これまで個人情報の開示請求はない。手数料は 500 円程度と定めた。
・20 年来、氏名公表のための承諾書を頂くことで合格者の氏名公表を行ってきたが、非公表を求める意見が増えた事情もあり、現在は公表を止めている。
・苦情はダイレクトメールの送付の停止依頼や、教室内で生徒が他生徒の成績を見てしまった、というものはあったが、個人情報の漏えい等に関する苦情はない。

（８）事故発生時の対応

（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）

・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。

以　上

T. その他サービス業（教育・学習支援）T 社

事業概要	幼児教室、学習塾の経営		
従業員数	約 60 人	プライバシーマーク取得	あり
保有個人データ件数	約 76,000 件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・総数は 76,000 件で、そのうち生徒及び卒業生の情報が 19,000 件、保護者の情報が 31,000 件である。

・氏名、住所、電話番号、保護者氏名、学校の成績、模擬テストの結果、保護者の最終学歴、自宅の最寄り駅から自宅までの地図、口座番号といった情報がある。

（２）個人情報保護担当部署

・担当部署は総務部である。

（３）個人情報保護管理者の有無・位置づけ

・CPO は総務部の課長である。

・統括は社長（個人情報保護管理責任者）である。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマークを平成 15 年に取得し、平成 17 年に更新を受けた。

・認証は、保護者など外部からの信頼を得るために取得した。

・幼児教室や保育園など年齢層の低い子供を持つご家庭は、個人情報保護法施行以降、特に敏感になってきている傾向があるため、プライバシーマークの取得によって安心感を提供できている。

・近隣の大手塾はすべてがプライバシーマークを取得しており、また、学習塾協会内で認証される独自認証の「トリプル A」という評価を得ている。プライバシーマークを持っていることによって、組織立っていて信頼のおける塾であることを示すことができている。

（５）個人情報保護に向けた取組経緯

・本格的な取組は平成 14 年頃から始めている。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・小学生以下の子供の情報は価値が高いので狙われやすいという認識が学習塾協会にあり、指導も詳細な指摘が行われる。

・顧客と事業者が一対一の関係であるため、（電話窓口等における問い合わせなどの際には）事故発生のリスクは少ない（お互いに顔見知りであり、すぐに本人かどうかの区別がつくため）。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・特徴的な取組はなし

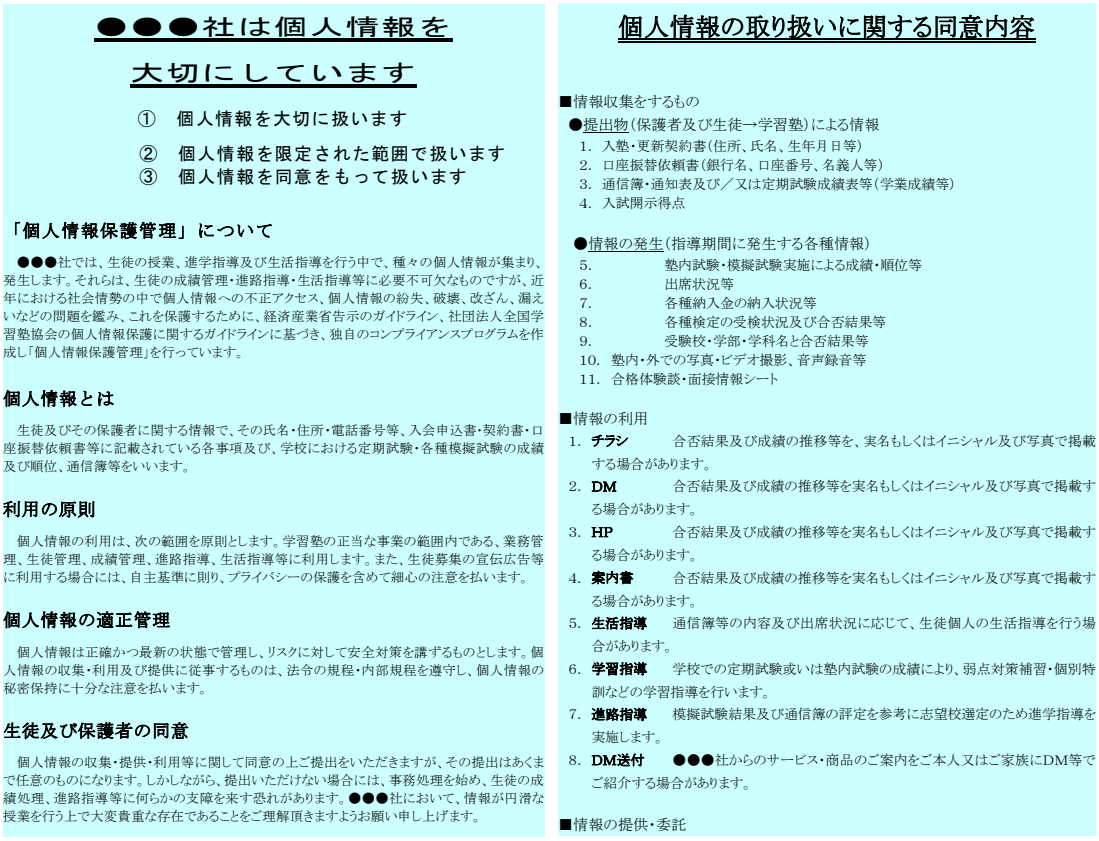
（２）個人情報の取得

（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）

・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。

図表　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

・生徒の会員番号は生年月日を元にしているため、生年月日情報の提供を断られた場合には入会を断らざるを得ない。
・入会した生徒以外に、問い合わせや体験講座の受講者の情報を得る。ダイレクトメール送付の可否の同意を得るようにしている。

（３）個人情報の利用（第三者提供を含む）

・適切な指導のために利用している。
・一度塾を卒業した生徒が、再度受験期を迎えるような場合にはダイレクトメールを出すようにしている。ダイレクトメールを断られた場合や返送があった場合には、ダイレクトメール宛先リストから削除するようにしている。
・卒業生で大学生になった人には、アルバイト募集（時間教員として）の広告を出す。

（４）個人情報の管理

①　情報の管理体制

（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）

・個人データは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。
・パソコンにはワードとエクセル以外のアプリケーションはインストールしないルールになっている。個人パソコンの持ち込みは禁止し、壁紙やスクリーンセーバーのダウンロードも禁止している。
・講師が持ち帰りを許可されているものは、教材と指導カリキュラム（スケジュール）であり、生徒の学年と名前のみの情報に制限している。名簿は見えるところにはおいておらず鍵のかかる書庫に入っているので、それだけをコピーして持ち帰ることがしにくい管理体制にしている。
・以前は書棚に分類シールを貼っていたが、いまはそれをやめている。個人情報を含む媒体は鍵がかかるところにしまっており、鍵は教室長など 2 人が持っている（どちらかが不在でも困らないようにするため)。

②従業者への教育方法
・教育は、教室の担当者が責任を持って行っている。
・講師をする学生の教育は、採用試験時に行い、禁止事項を説明している。あとは誓約書を書いてもらっている。

③盗難対策
・特徴的な取組はなし

④ノート PC の安全対策
・ノート PC の保有は 20 台のみで、管理職しか持たない。
・ノート PC は鍵のかかるところに収納し、持ち帰りは禁止である。
・USB のキーロックで管理している。

⑤外部委託先管理
・模擬テストを行う際は委託をするので、委託先と委託契約を結んでいる。
・漢字検定や英語検定は、生徒と検定の事務局が直接やりとりをしており、塾は場所を提供しているのみなので情報の委託ではないとされている。

⑥日常点検・確認の方策
（総務部の従業者が校舎を訪問する都度チェック、注意）
・総務部の従業者は校舎に行く機会が頻繁にあるので、訪問する度に気付いたことを注

意するようにしている。

⑦初歩的ミスの防止策

（電子メールアドレスは必要な従業者のみに付与）

・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。

（５）個人情報の消去・破棄

・クロスシュレッダーを導入している。
・電子データはサーバから削除している。

（６）個人情報の監査

・特徴的な取組はなし

（７）苦情処理・顧客対応

・開示請求は受けたことがない。
・苦情対応窓口としてホームページ上に電子メールやフリーダイヤルの電話、FAX、を公開している。
・保護者から教室への苦情の場合は、普段のコミュニケーションから電話の相手が保護者本人かどうかは判断できるため、特別な本人確認は行わないことが多い。
・成績照会の依頼がある場合は、出力して自宅に郵送する。郵送することで、本人（及びその保護者）以外は受領できないようにしている。

（８）事故発生時の対応

・個人情報保険に入っている。
・事故が発生した場合には、迅速に電話で謝罪、又は状況によっては自宅訪問して謝罪をするようにしている。

以　上

U．その他サービス業（冠婚葬祭）U社

事業概要	冠婚葬祭等企画・運営、冠婚葬祭互助会運営事業		
従業員数	約 200 人	プライバシーマーク取得	あり
保有個人データ件数	約 15 万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・約 15 万件（15 万人分）
・互助会組織会員、葬儀・婚礼等の利用者（喪主等の主催者の個人情報）
・会葬者・参加者等の個人情報は取得していない(取得した場合もすべて主催者が保有)。
・氏名、住所、年齢、生年月日、家族の名前に加え、口座番号（互助会の会費引落としのため)、宗教・宗派などを機微情報として保有。
・冠婚葬祭の儀礼時の使用に加えて、互助会会員に対しては「会報」を送付している。会報の内容としては営業的な内容が含まれることもある。
・互助会会員についても「会報」の送付可否について了解を得た上で送付している（オプトイン形式)。互助会に加入していることを家族に知られたくない、という会員もいるために、会報の送付も慎重に行う必要がある。

（２）個人情報保護担当部署

・総務部と情報システム課が担当している。
・総務部と情報システム課の個人情報保護の実務担当者（２名）はプライバシーコンサルタント資格を取得している。

（３）個人情報保護管理者の有無・位置づけ

・専務取締役が個人情報保護管理者になっている。
・CPO という対外呼称は使用していない。

（４）認証取得の有無（時期)、認証の種類、その認証を取得した理由・効果

・プライバシーマークを取得（平成 18 年 5 月）
・取得の目的は顧客の信用を得るために取得した。
・プライバシーマーク取得に取組むことを互助会会員等に周知したところ、「いまさら」という声すら上がった。営業活動で特に他社との差別化にはなっていないと感じている。
・社内的なデータ管理体制の整備に加え、机上放置の禁止や施錠可能なロッカー等の導

入により、従業者意識の高まりと職場の機能性や清潔感の高まりなどの効果がある。

（５）個人情報保護に向けた取組経緯

・個人情報保護法の成立・施行に合わせ、顧客の信頼を得るために個人情報保護体制を確立することが重要であるという社長の指令が出た。
・総務部と情報システム課の担当職員が平成 16 年にプライバシーコンサルタント資格を取得した。その過程でプライバシーマークの取得が必要だと感じるようになった。
・プライバシーマーク取得のために、高崎市・太田市・前橋市に点在する 12 の事業所の長を集めた会議などを数回実施して調整を行い、プライバシーマークを取得した。

（６）個人情報の保有・管理・提供等に関する業界の特徴

〇特に葬儀の場合、故人が亡くなってから式を執り行うまでの期間が極めて短いという特徴があり、関連する事業者も多い

・亡くなった直後に葬儀契約を結んで葬儀を執り行うが、契約に個人情報の取扱いが記載されていても、じっくり説明するような余裕は双方になく、また説明しても判断できるような精神状態でないこともある。
・委託を行う事業者としては生花、供物、写真業者などがあり、それぞれに故人の名前や住所、連絡先等は教えなくてはならない。特に、司会業の方は、式において話をしなくてはならないので、自分たちよりも多くの個人情報を持つ可能性があるので、絶対に漏らさないように(派遣元の)法人に加え個人でも確約書を書いてもらっている。

〇関連する者からの問い合わせが頻繁にあり、対応が必要になる

・結婚式であっても、「両親に内緒なので絶対にばれないようにしてほしい」という依頼があったり、葬儀でも「死因が特殊で会葬者にわからないようにしてほしい」、という依頼があったりすることもある。
・これらの個人情報は紙やデータの形式で残るものではないので、厳密には個人情報保護の対象にならないかもしれないが、式の打ち合わせや、式の運営を行うスタッフ等の間では共有しておく必要がある事項なので、絶対に漏れないようにすることが必要で、特に従業者の意識を高く維持することが必要となる。
・また、葬儀や婚礼の際に、近親者や友人等から問い合わせがあることがある。故人の名前や式場、開催日時などは教えることにしているものの、すべてについてコールバックで対応するようにしている。
・家族にも教えることができない情報を保有していることもあり、連絡等は慎重に行う必要がある。

〇会員制度（互助会）を維持・運営しているので、長期的な対応が求められる

・会員制度は定期的に会費を支払い、実際に冠婚葬祭を執り行う場合にその会費の積み立てを使用するものであり、継続的な個人情報の保有が求められる。
・故人の家族から“会員であったかどうか”の問い合わせや、“自分の会費はどの程度貯まっているか”、といった問い合わせもある。これらの問い合わせについて本人の場合は本人確認をする必要があり、また家族等の場合も本当に家族かどうかの確認が必要であり、配慮が必要である。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・社長が顧客の信用を得るために個人情報保護体制の整備が必要であるという号令を明確に掛けた。
・総務部と情報システムの担当職員２名がプライバシーコンサルタントの資格を取得し、この２名が中核となって個人情報保護体制を構築した。

（２）個人情報の取得

・葬儀等の規約の中に個人情報の取得や、委託先事業者等への提供についても記載してある。

（３）個人情報の利用（第三者提供を含む）

・「互助会の会報」の送付について同意を求めた上で、同意がある人に対しては会報を送付しているが、内容として一部営業情報も含んでいる。

（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）

・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。

（４）個人情報の管理

①情報の管理体制

・システムはもともとオフコンを利用しており、クライアント・サーバ型にしていなかった。したがって、クライアント端末では情報のダウンロードや蓄積ができないよう

になっていたことから、個人情報の管理の観点からその体制を維持し、中央サーバの管理をしっかりしている。
・ログインやホームページの閲覧、アプリケーションの起動等のログはすべて中央サーバで管理している。
・社内のすべての記憶メディアに番号を振り、情報システム課で番号管理を行っている。
・鍵のチェックを行い、紛失している場合は鍵をすべて取り替えた。施錠可能なキャビネットも新たに購入した。

②従業者への教育方法
・年に１回の個人情報研修を実施している。

（研修では極めて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）
・研修においては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ケーススタディを問題を出題している。
・具体的には「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。

（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）
・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。

③盗難対策
・特徴的な取組はなし

④ノート PC の安全対策
・そもそも幹部職員以外はノート PC は持っていない。

⑤外部委託先管理
・重要な個人情報を保有する委託先（司会業等）には確約書の提出と、取得した個人情報については当日の返却を要求している。ただし、頭に残る個人情報についてはどうしようもないため、注意を促すに留まっている。

⑥日常点検・確認の方策

・月に1度、プライバシーコンサルタント資格を有する2名の職員が、12事業所を回ってチェックを行う日を作っている。抜き打ちではなく、訪問する日は明示している。
・個人情報のチェックのために訪問する日以外にも、事務所は頻繁に訪問している。チェックの日だけしっかりしているような事業所・従業者はこの際にチェックできることもあり、皆、特にチェックの日だけでなくしっかりと意識付けされるようになっている。

⑦初歩的ミスの防止策

・特徴的な取組はなし

（5）個人情報の消去・破棄

・個人情報の消去はシュレッダーで実施している。
・葬儀等に関連する個人情報は紙媒体で5年間保管している。これは、年季法要が行われるからであり、顧客から前回の費用や内容について問い合わせがある場合も少なくないからである。
・これらの個人情報は倉庫で管理している。
・データ化されてサーバに格納されている個人情報は半永久的に保存されている。具体的な葬儀の内容などについては入力されていないが、故人の名称や施主、費用総額などは入力されている。年季法要や統計的に分析に利用したい事情もあるので、消去等は行っていない。すでに20年近くの個人情報が蓄積されている。
・FD等の記録メディアは情報システム課が一括で破砕している。

（6）個人情報の監査

・月に1回のプライバシーコンサルタント資格保有者の事業所見回りを実施している。
・通常の年1回の社内監査の一環で個人情報保護体制のチェックも行っている。

（7）苦情処理・顧客対応

・業界特性として顧客からの問い合わせが非常に多く、また本人以外からの問い合わせが多い。
・原則的にはすべてコールバックにより本人確認を行うようにしている。

（8）事故発生時の対応

・特徴的な取組はなし　　以　上

Ⅴ. その他サービス業（冠婚葬祭） Ｖ社

業務概要	冠婚葬祭等企画・運営等		
従業員数	約 70 人	プライバシーマーク取得	なし
保有個人データ件数	約 3,000 件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・葬儀社事業の利用者及び会員リスト約 3,000 件である。

・個人情報の種類は、氏名、住所の他に、死因、葬儀費用、参列者情報等がある。

（２）個人情報保護担当部署

・総務部と顧問の 3 名が担当している。

（３）個人情報保護管理者の有無・位置づけ

・専務取締役が個人情報保護管理者となっている。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマーク取得を申請中である（平成 18 年 8 月末現在）。

・個人情報の重要性を全社員が認識し、お客様満足の向上に貢献する意識改革のためである。

（５）個人情報保護に向けた取組経緯

・個人情報保護法が施行され、社会的に個人情報の保護が認識されるようになった。このため、同社では、他社との差別化を図るため、プライバシーマーク取得を決定し、現在体制の整備を行い、認証におけるシステム構築と維持改善を推進している。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・葬儀社事業は免許制ではないため、新規参入がしやすく、また撤退も起こりやすい。そのため個人情報保護の重要性についての認識が低い事業者が多く存在する。数名で事業をしている零細事業者も多い。葬儀関係の個人情報もデータで管理している事業者は少なく、紙で管理しているところが多い。

・葬儀社の中には、仏壇、墓石、返礼品等の取扱事業者へ葬儀で入手した個人情報を販売する業者がいた。中には悪質な事業者もおり、葬儀について知識のない遺族へ押し売りを行う事業者もあった。

・個人情報保護法の施行に伴い、このような悪質な事業者は減っている。上場会社も増えてきており、個人情報保護を実施する事業者とそうでない事業者に二分されている。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・現在、プライバシーマーク認証取得のため、規程・体制づくりを行っている。
・プライバシーマーク認証取得のため、管理責任者を中心としてアドバイザの指導に基づきシステム構築を推進した。

（２）個人情報の取得

・葬儀が発生した際、施主（葬儀の運営責任者）から参列者情報や葬儀関連の情報を取得する。
・電子メール等による個人情報の収集については、本人の同意による情報の送受信を順守するシステムに改善した。
・生前、葬儀社を決定しないまま病院で死亡すると、家族が病院に対し葬儀社の紹介を要望する場合がある。このような場合には、病院から同社が故人の氏名と病室番号の連絡をうけ、病院へ出向き家族に面会し同意の上詳細情報を取得することになる。

（３）個人情報の利用（第三者提供を含む）

・社内組織として仏壇や生花の販売部署があり、顧客の要望があれば紹介する場合がある。外部への提供は一切していない。

（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）

・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。

（４）個人情報の管理

①情報の管理体制

・施主からの情報はすべて特定の記入用紙に記載する。記入用紙の移動には鍵つきカバンを利用している。移動時に保有している用紙は 1～2 枚である。
・記入用紙の情報は入力され、本社のサーバに保管される。サーバは鍵つきの部屋を用意し、入退室記録をつけている。サーバへのログインのパスワードは毎月変更してい

る。

②従業者への教育方法

・従業者の個人情報への認識を最重要課題として意識改革の教育を実践した。
・個人情報保護は今までの業務内容とは全く異なる取組であるため、まず、従業者の意識改革から行わなければならない。例えば、今までは問合せに対しては常に回答するのが親切な対応であったが、個人情報保護上は、回答の可・不可は顧客に応じて異なる。
・全社教育と理解度テストを 3 回実施している。欠席者に対しても教育とテストが実施できるようフォローしている。テストは個人情報保護についての理解を得るための方策である。テストの結果について合格・不合格といったことをすると、従業者が個人情報保護は難しい、面倒だという意識になるため、特に結果については現状では評価していない。

③盗難対策

・特徴的な取組はなし

④ノート PC の安全対策

・ノート PC は利用していない。

⑤外部委託先管理

（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）

・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。
・外部委託先を「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。
・委託先を厳格に管理することも重要だが、個人経営の事業者に極端に厳格な管理を求めると業務の滞りや受託の拒否が発生するおそれがある。外部委託先が対応できる範囲も把握し、個人情報保護を依頼している。

⑥日常点検・確認の方策

・事前確認と事後確認の順守を業務ルールとしている。

⑦初歩的ミスの防止策

・FAX を送信した後は必ず電話で受取確認をするようにしている。
・事前確認と事後確認の順守を業務ルールとしている。
・社内及び社外への個人情報の送受信については、すべて信号化したシステムに改善した。

（５）個人情報の消去・破棄

・利用しなくなってから 3～5 年で消去することにしている。保管期間は情報内容によって異なる。
・サーバに保管されている情報の約 3 分の 1 は消去しない。施主が葬儀運営に係る事柄について何も知らない場合、同社に保管している施主の家族に関する過去の葬儀情報（菩提寺、家紋など）が必要となる場合があるためである。

（６）個人情報の監査

・特徴的な取組はなし
・セキュリティシステムを重視し、内部監査にて各部門に対応するチェックリストを活用して、資格認定された監査員による全部門の監査体制を確立した。

（７）苦情処理・顧客対応

・開示については、本人に来社してもらい、本人確認ができたときのみ開示するとしている。郵送での開示はしない。今まで開示請求はない。
・葬儀においては近隣の情報を欲しがる人も多い。例えば知人の葬儀費用を知り、同程度又はそれより上のランクを求めてくるケースがある。
・顧客の葬儀費用は教えることはできないが、顧客サービスは充実させたい。そのため、費用の情報を求める人に対しては、「○○さんの費用はいくらでしたよ」と伝えることは決してないが、漫然と費用リストを見せるのではなく、特定の費用をお勧めすることで対応している。

（８）事故発生時の対応

・個人情報保護方針において、事故発生における企業対処を明示し、お客様への信頼性と、個人情報の重要性を認識する姿勢を明確にした。

以　上

W．その他サービス業（エステティックサロン）　W 社

事業概要	エステティックサロン運営		
従業員数	非公開	プライバシーマーク取得	なし
保有個人データ件数	非公開		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・個人情報の保有件数については非公開である。

・個人情報としては、氏名、住所、電話番号のほかに、エステティックサービスに必要な情報も取得している。

（２）個人情報保護担当部署

・個人情報保護担当部署(兼務)が設置されている。

（３）個人情報保護管理者の有無・位置づけ

・取締役が個人情報保護管理者として位置づけられている。

（４）認証取得の有無（時期)、認証の種類、その認証を取得した理由・効果

・認証は取得していない。

（５）個人情報保護に向けた取組経緯

・平成 15 年 8 月に「情報セキュリティ規程」を策定し、施行した。

・平成 16 年 8 月に個人情報保護に関する社内プロジェクトを発足し洗い出しを実施した。

・平成 17 年 3 月にサロン責任者及び本社全従業者に研修を実施した。

・平成 17 年 4 月より「個人情報保護管理規程」を施行。委託先に対する契約更新時に秘密保持契約の締結を推進している。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・特になし

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・プライバシーポリシー等は、ガイドライン、法律、書籍等を参考にコンサルタントの意見も聞いて作成した。

・個人情報保護の社内担当は３名（管理者を含む）である。個人情報保護の専任ではなく、他の仕事との兼務で行っている。

・規程についても定期的に見直す方向性で検討している。

（２）個人情報の取得

・利用者は店舗に訪問し個人情報を会員となる為に登録する。

・利用者は広告媒体を見て来店希望の電話をかけてくる。この際、個人情報を取得する。詳細な個人情報は来店時に取得し、紙媒体に記載する。

（３）個人情報の利用（第三者提供を含む）

（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）

・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。分析には主に郵便番号を利用し、電話番号の市外局番は、携帯電話の登録が多いため利用していない。

（４）個人情報の管理

①情報の管理体制

（機微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）

・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。

・本社においては、社外との回線を一箇所に絞っている。ファイヤーウォールや外向けの電子メールサーバは本社にあり、出入口を１つにすることで情報の流出入を管理している。

・本社ではデスクトップ PC をメインで使っている。デスクトップ PC には書き込みのできる CD ドライブは付けていない。

・ログインには ID、パスワードが必要である。部署ごとの共有サーバについても ID、パスワードが必要である。

・本社内はオンラインでつながっている。本社と各営業拠点は VPN（閉域網）でつながっている。

・個人情報のデータが保存されているのは、汎用機であるため、個人のパソコンへのデータのダウンロードはできない。
・ファイル共有ソフト（Winny 等）の使用は禁止している。資産管理ソフトをすべてのパソコンに入れており、起動チェックを行っている。
・電子メールの利用についてはアクセスログをとっている。容量制限をしており、大量にデータが外部に流出しないようにしている。

②従業者への教育方法

・社内への周知徹底については、平成 17 年 3 月の法律施行にあわせて、本社から出向いて、サロン責任者（各店舗の責任者）教育と確認を行った。また本社の全従業者も対象に教育と確認を行った。
・サロン責任者には、「マニュアル」を配布し店舗において教育するよう徹底している。
・機微情報を扱っているので、情報の重要性は法施行前から教育している。また毎月の会合でも随時教育をしている。

③盗難対策

・店舗において機微情報は紙媒体でのみ管理されている。データ化はされない。紙媒体のため、隠れて大量に持ち出すことはできない。
・本社にあるデスクトップ PC の本体にセキュリティワイヤーをつけ、動かないようにしている。

④ノート PC の安全対策

・外回りの営業職はいないので、ノート PC は必要最低限にしている。ノート PC には USB セキュリティキーを利用している。ログイン時に USB キーを接続し、ID、パスワードを入力してはじめて立ち上がるようになっている。HDD の暗号化はしていない。

⑤外部委託先管理

・外部への提供はしない。
・書類の保管は、プライバシーマーク取得の外部業者を利用している。
・外部から個人情報を入手し、ダイレクトメール等を出すということはない。
・個人情報は、関連会社（共同利用会社）に必要な部分のみデータを提供する場合がある。
・関連会社においても本社と同一の管理基準を適用している。
・共同利用について利用者からの問合せや指摘は特にない。

⑥日常点検・確認の方策

・一般的な取組をしている。

⑦初歩的ミスの防止策

（FAX の誤送信防止のため、広域内線番号サービスを利用）

・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。

（５）個人情報の消去・破棄

・プライバシーポリシー等の「開示・訂正・利用停止」の中で、「最終のご利用から相当期間を経過したお客様の情報に関しましては対応できない場合があります」としていて終了分を定期的に消去している。この記載に関する問い合わせは来ていない。

・CD-ROM 等のディスクはセキュリティの観点から、破砕処理している。

（６）個人情報の監査

・外部のセキュリティ専門会社に依頼することについて検討中である。

（７）苦情処理・顧客対応

・問合せに対しては本社に「お客様相談室」を設け対応している。

・開示請求については、本人限定受取書留の費用を設定している。

・開示請求は当初想定していたよりも少なかった。

（８）事故発生時の対応

・漏えい、き損事故発生時への取組としては、保険加入と、連絡体制の整備がある。

・各部署には事故発生時のマニュアルを配布している。

・事故が発生した場合には、担当所属長又は部署の個人情報担当者へ連絡がなされ、委員会が招集される。代表取締役が対応委員長となっている。

以　上

X. その他サービス業（印刷・広告）X 社

事業概要	証券・カード、商業印刷、出版印刷、パッケージ、産業資材、エレクトロニクス、Ｅビジネス		
従業員数	約 11,000 人	プライバシーマーク取得	あり
保有個人データ件数	月間取扱規模 約 6,450 万件		

１．個人情報に関する概要

（１）保有個人情報件数、個人情報の種類、個人情報の利用目的

・月間取扱規模約 6,450 万件。毎月の取扱規模であるが、一定期間保管される。

・各業務によって扱っている個人情報は異なる。大半の個人情報は住所、氏名といった情報であり、機微情報は極めて少ない。

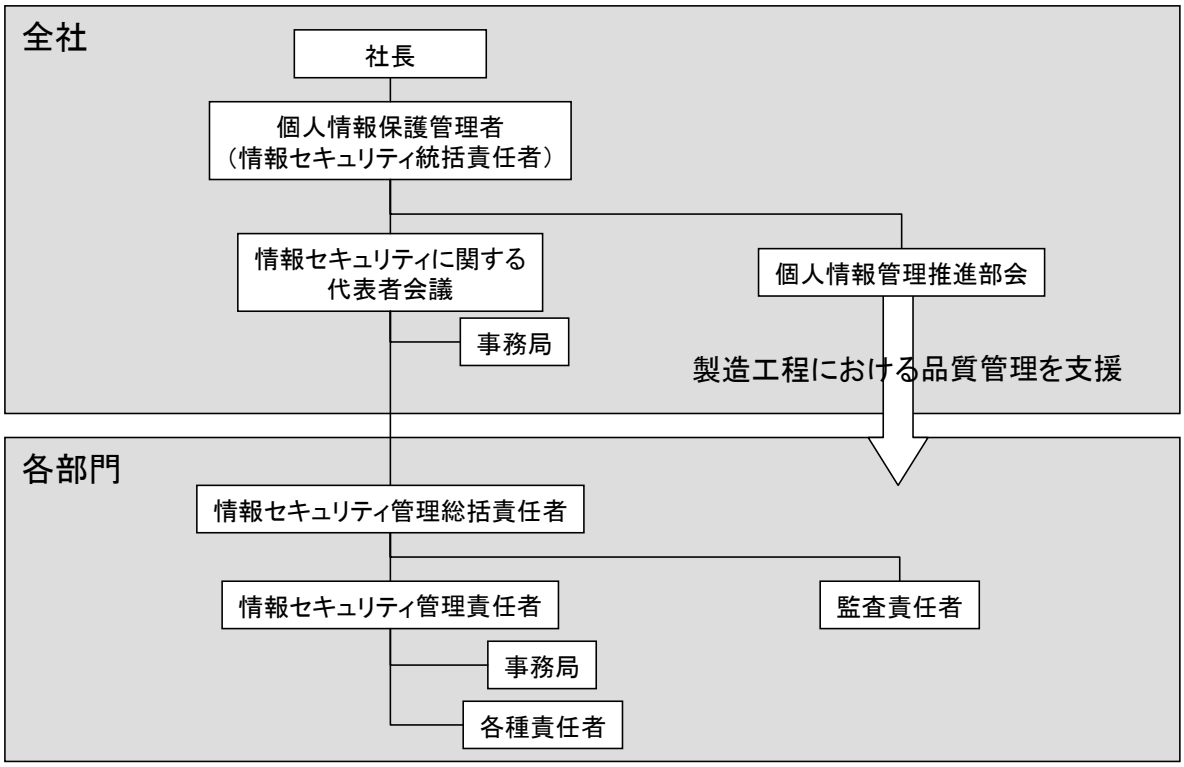
（２）個人情報保護担当部署

・情報セキュリティ管理統括責任者を責任者と決め、各事業所によって構成される委員会を組織し規程作りを行っている。

・同社では個人情報が一部署のみの処理で終わることはほとんどない。複数の事業部での加工を経ることが大半である。このため、各工程の運用ルールは適正であるか、イレギュラーな事態にも対応できるか、事故を起こさないルールとなっているのか、前工程でミスが発生しても次工程で発見し被害発生を食い止める仕組みになっているか、記録は残っているのかについて確認する必要がある。この役割を個人情報管理推進部会が担っている。

・個人情報管理推進部会は、本社関連部署による横断的組織として構成されている。

図表　個人情報保護に係る組織図イメージ



（３）個人情報保護管理者の有無・位置づけ

・情報セキュリティ管理統括責任者として取締役が担当している。

・情報セキュリティ管理統括責任者は全社を代表する情報管理の責任者である。各事業（本）部においては、事業（本）部長に代表者としての権限を委譲する。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・平成 12 年 3 月金融証券分野を担当する事業部が同社では初めてプライバシーマークを取得した。個人情報保護の先進事例として、かねてより情報セキュリティに積極的な同社が、JIPDEC の要請も受け、業界内で率先的にプライバシーマークを取得した。以後、全社の各事業部でプライバシーマークの取得を進めた。

・平成 18 年、JIPDEC の要請のもと、全社として統一的なプライバシーマーク取得を行うこととした。平成 19 年には全社統一のプライバシーマーク取得を行う予定である。

・同社の子会社についてもグループとしてあるべき姿を示すため、プライバシーマーク取得を勧めている。

（５）個人情報保護に向けた取組経緯

・同社では平成 3 年 5 月に情報リスクマネジメント活動として「秘密情報管理規程」を

制定。平成 11 年 2 月に「個人情報保護方針」「個人情報管理規程」制定を行った。
・平成 11 年には金融・証券事業部がプライバシーマークを取得した。
・平成 16 年 10 月に本社の横断的組織として個人情報管理推進部会を設置した。プライバシーマーク取得だけでなく、WEB 管理、ホームページ作成等での個人情報管理についても対応を決定した。
・印刷、加工、データ処理におけるケアレスミスが漏えいにつながることから、生産工程でのオペレーションの品質向上を行った。
・品質管理として、生産現場への監査や協力会社の認定も行った。１年要して全国の工場や協力会社を回り、品質管理の向上や個人情報保護意識を高める教育につとめた。今後も継続していく。
・個人情報の漏えいは、例えば協力会社の製造している封筒の仕様が不充分といったことから発生する。従来は封筒が個人情報の事故につながるという意識は低かったが、請求書を入れたとたんに封筒もまた個人情報そのものとなる。この意識をもって、生産現場での品質管理の向上を図った。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・印刷業界は顧客から仕事を請け負う業態がほとんどである。顧客あってこその仕事であり、その顧客があらゆる業種にまたがっているため、関係する管轄省庁やそのガイドラインも多岐にわたる。そのため、かなり幅広く多方面に目配りをしておかなければならない。
・そして、個々の個人情報取扱業務は、それぞれに多くの工程を抱えながらも、“一品一様”で、その仕様変更も作業中であるか否かを問わずに発生するという、要求に応えなければならない。
・印刷業界では、多くが規模の小さい中小企業である。そのため、新たな管理者を育成したり、個人情報保護に特別なコストをかけたりするのが難しい場合もある。
・外部協力会社に対する品質管理の指導はもちろんのこと、業界全体に対しても、我々が指針めいたものを提供し、指導的な立場で業界に寄与できればと思っている。ここ２年間、印刷業界のガイドラインや Q&A の制作、講演会、説明会などを積極的に行っている。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・当初のプライバシーマーク取得にあたっては、JIS 規格のみでは社内に適切に当てはめるノウハウが無かったため、コンサルティングを活用した。

・平成 16 年 10 月に本社の横断的組織である個人情報管理推進部会が開始した。毎週定例で集まって打合せをしている。新制度の社内への説明、ISO との整合性、事故対応、業務の増加による対応等について話をしている。
・事業部との会議は毎月開催されるので、2～3 ヶ月に 1 回は個人情報関連についても会議を持っている。
・情報セキュリティ管理責任者による会議は、以前は個人情報と情報セキュリティについて分けて会議をもっていたが、現在は包含して行っている。

（２）個人情報の取得

（WEB サイトで個人情報を収集する場合本社承認が必要）

・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。

（３）個人情報の利用（第三者提供を含む）

・委託元からの預かりデータについは事業部と製造子会社間で処理されているが、両者の関係は委託関係であるので、共同利用はしていない。
・共同利用の課題は従業者情報である。従業者情報は、労務管理、福利厚生、社会保険庁への申請などで利用するとしているが、労務管理の延長線上で、グループ会社との人事交流のために利用される場合もある。異動が関係する事柄であるため、本人の了解を得ることは現状ではしていない。

（４）個人情報の管理

①情報の管理体制

（データの授受は手渡し又はセキュリティ便を利用）

・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。

②従業者への教育方法

（パートを含めた e ラーニングを実施）

・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

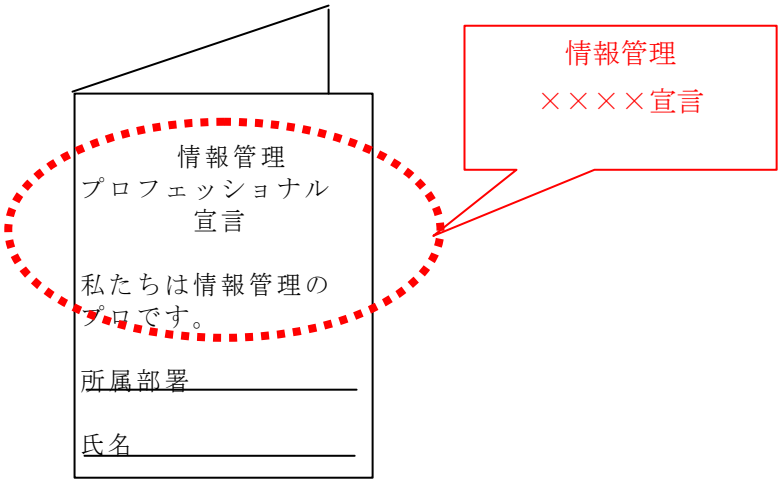
一企業及び製造子会社を含めて、個人情報取扱業務に従事するパートに対しても教育している。ｅラーニングはパソコンで回答するが、なんらかの理由でパソコン端末の操作ができない場合は、紙で対応している。

・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。すべて修了するのに 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。

（情報管理の小冊子を配布し、携行を義務付け）

・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。

図表　小冊子のイメージ



・個人情報についての社内へのお知らせ・通達については、全社一斉の場合と管理者のみへの場合がある。情報の内容によってお知らせ・通達の範囲を判断している。事故発生情報については基本的には管理者のみへ知らせている。顧客との関連事項については注意喚起のために全社通達もある。

③盗難対策

・印刷会社の体質として情報セキュリティ意識は高く、今までに大きな事故はない。
・扱う情報によっては、カメラ付携帯電話の持ち込み禁止、持ち物チェック、ポケットのないつなぎ服の着用を実施している部署もある。

④ノート PC の安全対策

・モバイル用ノート PC は暗号化している。

⑤外部委託先管理

（協力会社に対して独自の認定制度を導入）

・委託については、宛先に合わせた内容の送信を行うダイレクトメールに関しては、再委託先を、社内と同程度のセキュリティを確保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。

（派遣社員からは直接誓約書をとらずコピーで対応）

・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日常点検・確認の方策

・各工程の点検・確認方法を独自のノウハウ集にまとめ、その内容を毎日指差呼称することで周知徹底をはかっている。このノウハウ集は、正社員・派遣社員・パート社員を問わず当該作業に従事している担当者全員から作業上のノウハウや注意事項などをブレストで出してもらい、それをリーダーやマネージャーがルールとしてまとめたものである。機械メーカや上からの押し付けルールではない、地に足の着いたルールなので高い効果をあげている。

⑦初歩的ミスの防止策

・初歩的ミスの防止の１つとして例えば、誤封入をなくすため、封入は２人以上でチェックするようにしている。この場合１人目の封入形態と２人目の確認後の封入形態を変えることにより、確認漏れを無くす工夫をしている。

（５）個人情報の消去・破棄

・以下の方法を紹介し、復元不能な処理の徹底を励行し、及び記録を残すようにしている。

(a)コマンド処理による消去（主に WS の HD 上のデータ）

(b)証明書発行機能付き専用ソフトによる消去（主にパソコンの HD 上のデータ）

(c)上書き及びフォーマットによる消去（主に電子媒体上のデータ）

(d)物理的破損（主に電子媒体）

（６）個人情報の監査

（監査は異なる部門の監査担当者が複数で実施）

・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。

（監査手法をとった品質指導を実施）

・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にかなうもので、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。

（７）苦情処理・顧客対応

（受託案件の問合せは委託元へ報告）

・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）事故発生時の対応

・事故を起こした本人は行動指針に反するものについては処分の対象となる。過去に本人処分があった際には、本人を処分したという情報を全社へ通達した。これによってどのような行動が処分につながるか従業者に分かり注意喚起につながると判断したためである。

・事故については、一通の漏えいでも JIPDEC に報告している。社内でも同様である。事故かどうかは本社で判断するので、どんなことについても申請するよう指導している。

（９）その他

・グループ会社と連携し毎月１度のグループ研究会を実施している。過失事故撲滅のための具体的手法や教育・監査手法などについての情報交換を行っており、大変有効である。

以　上

Ｙ．その他サービス業（印刷・広告）　Ｙ社

事業概要	パンフレット、カタログ等印刷、デザイン、製本等		
従業員数	約 200 人	プライバシーマーク取得	あり
保有個人データ件数	なし		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・保有している個人情報は従業者情報程度しかなく、個人情報は預託されている。
・生命保険番号やレセプト、資格関係などの機微情報を扱うこともある。

（２）個人情報保護担当部署

・システム管理室が担当している。

（３）個人情報保護管理者の有無・位置づけ

・個人情報保護管理者は常務取締役である。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマークを平成 17 年に取得した。取得は、長い付き合いのある大きな取引先にプライバシーマークの取得が必要であると要請されたことがきっかけである。その後、社内でヒアリングを行い、社会的な要請を感じて取得に踏み切った。
・プライバシーマークの取得に当たっては、コンサルタントに委託した。

（５）個人情報保護に向けた取組経緯

・プライバシーマークの取得をきっかけに、取組を行った。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・情報の保管管理を依頼されることがある。既存のデータに新たにデータを追加して印刷することが多く、保管データが上積みされていく。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・特徴的な取組はなし

（２）個人情報の取得

・委託を受ける際は、授受記録（受注件名・内容・取得日・担当者名を記載）をとっている。

（３）個人情報の利用（第三者提供を含む）

・個人情報は直接収集でないため、利用することはない。

（４）個人情報の管理

①情報の管理態勢

（キャビネットは開閉を名簿管理）

・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。
・どの建物も警備会社と契約している。入退出の際、最初に入った人と最後に出た人は記録を採る。
・本社（人とデータ量が最も多い）では、カードキーを持っていない人は受付を通らないと中に入れないようになっている。
・社内のパソコンにはウイルス対策ソフトが入っており、サーバにも導入してある。
・パソコンには、ID やパスワードを設定している。
・フロッピーなどの媒体に関しては、ウイルス対策ソフトを作動させてからファイルを開くよう指導している。
・個人情報を、従業者個人のパソコンに保存することは禁止している。ノート PC を用いて社外で作業することはない。
・電子メールへのファイル等の添付は禁止している。

②従業者への教育方法

（担当委員を中心に勉強会を開催）

・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。

③盗難対策
・特徴的な取組はなし

④ノート PC の安全対策
・ノート PC は使っていない。

⑤外部委託先管理
（外部委託先は管理表で管理）
・業務が大量の場合は発送を委託することがある。委託先はプライバシーマークを取っている業者を優先している。
・委託先には、事前通知の上、実地見学を行っている。

⑥日常点検・確認の方策
・グループウェア上の掲示板に情報を載せている。

⑦初歩的ミスの防止策
・個人情報は FAX や電子メールでの送信禁止を前提としている。

（５）個人情報の消去・破棄
・情報は、委託元との契約に応じて情報が不要になった時に廃棄する。廃棄証明をつけることを要求される場合は、そのようにする。
・紙の情報を溶解するため処分業者と契約しており、処分状況を顧客に報告することもある。紙媒体の情報は一般のゴミでは出さず、定期的に回収に来る処分業者に委託している。
・電子データは消去の記録をつけている。媒体に残っているものは消去ツールで中身を消してから粉砕処理を委託して行っている。フロッピーの再利用は禁止している。
・生産部としては、不要になった時点（生産後）から１ヶ月以内に処分する、というルールにしている。

（６）個人情報の監査

・監査は年 2 回行っている。保護委員が自分の部署以外を担当し、個人情報メインの監査を行っている。

（７）苦情処理・顧客対応

・お客様相談窓口を設置しており、各担当者レベルでは回答はしないようにしている。

・これまで個人情報に関する問い合わせや苦情はない。

（８）事故発生時の対応

・漏えい事故は実際には起こっていないが、事故の際には被害の拡大を防止する措置をとり、事故の規模によっては対策本部を臨時で設置して事故の状況把握と復旧対策を検討する。

・機密情報の契約を顧客と結んでいる。個々の対策、損害賠償は契約によって規程されているので、それに沿って行う。個人情報の漏えいに関しては、実施には大元の方が責任をとって、それからの派生的な損害賠償という形になると考えられる。

以　上

Z. その他サービス業（ダイレクトメール等）Z 社

事業概要	ダイレクトメールの印刷や送付等		
従業員数	約 600 人 （パート、契約社員を含む）	プライバシーマーク取得	あり
保有個人データ件数	約 5,500 万件（預託情報のみ）		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・個人情報は預託されるものが主であり、直接取得するのは従業者情報のみである。
・預託される個人情報は 5,500 万件程度である。氏名、住所、電話番号、購入履歴、申込書送付履歴などがその内容である。
・従業者情報は 180 件だが、パート社員を含めると 400 件以上である。

（２）個人情報保護担当部署

・情報セキュリティ戦略室が個人情報保護を専任で担当している。平成 16 年に新設した。同室には室長と他 3 名が所属している。

（３）個人情報保護管理者の有無・位置づけ

・個人情報保護管理者は取締役である。
・情報セキュリティ戦略室は管理者から諮問を受けているが、組織的には社長の直轄になっており、個人情報保護管理者とは上下関係にはなっていない。これは牽制効果を発揮するためである。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・個人情報保護に関してはプライバシーマークを取得している（平成 13 年）。
・認証取得の理由は、セキュリティが社会的に求められていることと、セキュリティの強化によって他社との差別化を図ればビジネスチャンスになると考えたことである。

（５）個人情報保護に向けた取組経緯

・プライバシーマークの取得時には、コンサルタントに相談した。その後、現在取得を準備している ISMS についても同様にコンサルタントを採用している。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・個人情報の漏えいによって顧客の信頼を失うことは、企業からの受託業務を行う業界

にとって死活問題である。実際に業界内でも漏えい事故によって損害が発生した事例があった。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・プロジェクトチームを立ち上げ、メンバーには特別手当を付与してまで取り組んだ。
・トップのコミットメントがあったことが大きかった。プロジェクトメンバーは、課長、課長代理が実質的なメンバーであった。

（２）個人情報の取得

・個人情報の預託を受ける際には、授受簿を使って管理している。

（３）個人情報の利用（第三者提供を含む）

・特徴的な取組はなし

（４）個人情報の管理

①情報の管理態勢

・電子メールにファイルを添付する場合、データセンターを通してチェックがかかるようにしている。至急の場合は暗号化している。
・社内で利用するパソコンは、外付けの媒体が利用できないようにしている。
・社員証のリボンの色を階によって変えている。

②従業者への教育方法

（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）

・従業者には、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。

（検定試験の受験を奨励しており、合格者には褒賞を与えている）

・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盗難対策

（携帯電話は遠隔ロックが可能な機種を採用している）

・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ノートPCの安全対策

・ノートPCは利用していない。

⑤外部委託先管理

・外部委託先の選定に関しては、明確な基準を持っている。・外部委託先を年に少なくとも1度は回ってチェックしている。

⑥日常点検・確認の方策

・特徴的な取組はなし

⑦初歩的ミスの防止策

・特徴的な取組はなし

（５）個人情報の消去・破棄

・データの消去は消去ソフトで行っている。
・紙媒体の情報の破棄は、処分業者によって溶解処理している。顧客の要請があれば、処分業者に依頼して廃棄証明書を出している。
・破棄のタイミングは、委託元との契約によって決まる。
・個人情報保護法の施行前は、破棄に関する契約を結んでいない場合も多く、法律の施行に合わせて､取り決めのないまま保有している情報を顧客の了承を得てすべて整理、破棄した。

（６）個人情報の監査

（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している）

・監査は以下の 3 種類を行っている。

・早朝抜き打ち点検：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。点検で 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。休日に届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。

・半期に一度、社長出席の下、監査報告会をしている。

・注意すべき項目の一覧を表示した紙を机に貼るなどして、各自がチェックするようにしている。

（７）苦情処理・顧客対応

・法律の施行に合わせて開示請求の様式を整えたり、手数料の設定をしたりしたが、これまで開示請求は一件もない。

・手数料は 1,000 円と常識的な範囲で決めた。

（８）事故発生時の対応

・緊急連絡網など体制は、プライバシーマークの基準通りに整えている。

以　上

α．その他サービス業（会議等開催運営支援）α社

事業概要	国際会議・国内会議・イベント企画運営、通訳・翻訳、人材サービス等		
従業員数	約 170 人	プライバシーマーク取得	あり
保有個人データ件数	約 4 万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・会議等開催・運営支援サービスに関連する個人情報は約 2 万件
・その他サービスが 19,000 件余りで合計約 4 万件
・氏名、所属、部署、職位、住所、電話番号、FAX 番号、電子メールアドレスなどが標準の場合に WEB から登録してもらう情報である。
・必要がある場合には、個別に年齢（年齢制限のあるコンベンションへの参加登録時、年齢制限のある論文賞への応募等)、パスポート情報（ビザ取得の必要がある場合等）なども収集する。
・機微情報は少ないが、“宗教上の理由で肉が食べられない”などの情報については、「Special Requirement」という欄を設け、自発的に記載してもらっている。
・コンベンション参加者の利用登録、論文投稿受付などを行い、コンベンション参加者に対して、参加者リストを配布する。

（２）個人情報保護担当部署

・コーポレートスタッフ部門の経営企画グループにプライバシーマーク事務局を設置しており、担当部署としている。

（３）個人情報保護管理者の有無・位置づけ

・常務取締役が社内の個人情報保護管理者である。CP 管理責任者でもある。

（４）認証取得の有無（時期)、認証の種類、その認証を取得した理由・効果

・平成 15 年 7 月にプライバシーマークを取得した。
・同社が実施する事業の「コンベンション」「通訳・翻訳」「人材サービス」のいずれもがヒューマン・インターフェースに立脚するものであり、個人情報を取り扱うことの重要性を強く認識していたことから取得した。
・コンプライアンス・プログラムの継続的な運用により、従業者の個人情報に関する認識が高まったことが効果である。

（５）個人情報保護に向けた取組経緯

・平成 14 年 4 月：個人情報保護への取組を開始
・平成 14 年 9 月：個人情報保護方針の策定、ホームページに掲出・公表
・平成 15 年 7 月：プライバシーマーク認証取得
・平成 17 年 7 月：プライバシーマーク認証更新

（６）個人情報の保有・管理・提供等に関する業界の特徴

・コンベンションは「オープン型（ほとんど誰でも参加可能な場合）」と「クローズ型（学会等、参加者がかなり限定されている場合）」がある。
・原則的には、参加者が限定されているクローズ型は基本的な個人情報を収集しないと連絡や案内ができないし、参加者名簿も相互交流が目的の会合で配布するので配布自体が必要とされている。個人情報の取得の場面ではほとんど抵抗がない。
・サプライヤーの立場からすると、自らの宣伝や交流の拡大になるので、ある種の個人情報は積極的に開示することを求められることが期待されている部分もある。
・「オープン型」についてはそもそも個人情報を収集しないことも少なくない。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・平成 15 年 4 月から、JISQ15001 に基づく規程・体制づくりを行っている。

（２）個人情報の取得

・取得そのものには、ほとんど本人は抵抗を感じずに提供してくれている。
・いろいろな国・地域から参加者がいるので、WEB 上で参加登録をしてもらっている。基本的な情報（氏名・所属・住所・連絡先等）については、同一の学会の別な会合や、関連する学会等で使用するケースがあるので、「他に参加を希望される学会等で個人情報が使用されることがあります」ということを明示した上で同意を得ている。

（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）

・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、明確に機微情報を集める欄としているわけではない。
・登録してある自分の個人情報については電子メールアドレスとパスワードで管理できるようにしている。
・クレジットカードの番号や振込先の番号は、FAX 等で直接送付されて保管することもあるものの、通常は決済会社を使用しており、自社でコンベンションに参加する方の決済に関連する個人情報は取得・保有しないようにしている。

（３）個人情報の利用（第三者提供を含む）

・第三者提供は参加者リスト等を作成する印刷業者や、旅行・宿泊業者に提供を行うことがあるが、その旨はホームページに明示して示したうえで個人情報を提供してもらっている。
・その他、要人が来賓で参加するようなコンベンションの場合は事前に警備当局に参加者リストを渡すことがある旨もホームページで明示している。

（４）個人情報の管理

①情報の管理体制

・参加者リストごとに特定のパスワードをかけ、当該リストを使用する職員のみにそのパスワードが知らされるようになっている。
・参加者リストに誰がアクセスしたかということについては、ログを取っているので合わせて把握することが可能になっている。

②従業者への教育方法

・オリジナルに実際に発生するようなケースや最新の法令等の問題を WEB テストの形式で実施している。
・そもそも通訳や翻訳業務も実施しており、重要な会議（役員会、国際取引の場など）で機密情報を知ってしまうことも多い立場であった人間が多く、個人情報についても企業機密情報の一部であるとして高い認識の下で取り扱ってもらっている。

③盗難対策

・入退室管理、施錠管理、アクセス制限、ログ監視、パソコン起動パスワード等による暗号化など、種々の対策を講じている。

④ノート PC の安全対策

・業務の性質上、ノート PC もコンベンション会場に持参せざるを得ない。
・BIOS によるログイン管理、格納されているファイルにすべてパスワードを掛ける

ことで安全性を担保している。

⑤外部委託先管理

・外部委託先（印刷会社、旅行・宿泊業者等）とは個別に個人情報保護契約を締結している。

・警備・清掃会社など、何かの機会に会場で個人情報を眼にしたりする機会があるような事業者とも個人情報保護契約書を交わしている。

⑥日常点検・確認の方策

・特徴的な取組はなし

⑦初歩的ミスの防止策

・特徴的な取組はなし

（５）個人情報の消去・破棄

・学会等やコンベンションは連続して場所や主催者を変えて継続していくものであるので、利用目的の終了、学会の会計報告もしくは次の学会の着手まで（数ヶ月～半年前後）の間は保管することにしている。

・20 年に一度、国際会議が日本で開催されるようなケースもあり、日本の学界から前回の参加者リストなどはないかという問い合わせがあることがあるが、対応が不可能なケースもある。

（６）個人情報の監査

・地方営業所についても個人情報の監査等について配慮している。地方の営業所では、通常の社内監査とは別に個人情報の監査を 1～2 年に１回実施している。その際には約一週間前に監査に行くことを連絡している。

・別に、法務の観点から個人情報保護法以外の話で全国を行脚する機会があるので、その際にも個人情報に関しても確認することがある。

（７）苦情処理・顧客対応

・自分の情報が学会やコンベンションを通じて漏れたのではないか、という苦情はほとんどない。

（８）事故発生時の対応

・プライバシーマーク事務局への連絡など、事故発生時に備えて規程に盛り込んでいる。

以　上

β．その他サービス業（情報提供サービス）β社

事業概要	情報提供サービス業		
従業員数	大企業	プライバシーマーク取得	なし
保有個人データ件数	多数		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・個人情報は大きく「企業情報内の代表者・役員等に関する情報（以下、企業内情報）」、「お客さま情報」、「従業者に関する情報（人事情報）」に分かれる。
・「企業内情報」は企業情報自体を多数保有するが、1 社で役員など複数保有している場合もある。（役員情報については氏名のみ）
・「お客さま情報」も多数保有するが、これも 1 社で複数の担当者名などを保有している場合もある。
・「従業者に関する個人情報（人事情報）」は従業員数分プラス採用・退職者情報を保有している。
・個人情報の種類としては、企業内情報のうち、代表者の個人情報として、「氏名、役職、性別、生年月日、出身都道府県、現住所、電話番号」などが含まれる。
・利用方法としては、企業内情報については収集した上で第三者（お客さま）向けに提供する。
・お客さま情報については、本人確認、料金請求、問い合せ対応、各種案内送付、及びその他サービス提供を行うために利用する。

（２）個人情報保護担当部署

・個人情報に関する受付窓口としては、業務部門（お客さま窓口部門）が一元対応している。難しい問題が発生するような場合については企画部門などに相談する。
・社内管理、規程整備、教育等全体の取りまとめという点では、企画部門が中心に対応してきている。

（３）個人情報保護管理者の有無・位置づけ

・管理本部長が情報セキュリティ統括責任者として個人情報保護管理者（CPO）に位置づけられており、現在総務部長がこの職位にあたっている。個人情報保護も情報セキュリティの一環として位置づけられている。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・認証は現在、取得していない。
・以前 BS7799 と ISMS を取得し、2 年後に更新時期を迎えたが更新しなかった。社内の体制を整備するのに一定の役割を果たしたこと、更新費用に見合った効果が期待できないことなどがその理由である。

（５）個人情報保護に向けた取組経緯

・平成 16 年の 4 月頃から、各部署の担当者が集まって、プロジェクトチームとして推進した。
・半年～約 1 年掛けて実施した。担当者は通常業務との兼務で実施していた。
・社内で保有している個人情報の洗い出しから始まり、調査取材時の対応・データの削除要請への対応、ホームページへの掲載文言検討、社内体制の整備（教育・啓蒙を含む）を検討のうえ実施した。
・法施行後は、主として個別の対応や不備部分の強化、監査の実施等を継続してきている。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・データベース事業者は、直接・間接に取得したデータを蓄積し、お客さまに提供している（弊社では代表者・役員等）。情報の取得に際してはオプトアウトの形をとっているところが多く、本人から第三者提供停止の要請があった場合には、提供データからはずすようにしている。
・弊社ではなるべく情報収集を行う現場に負担が掛からないように、取材の場で個人情報について詳細な説明は行わず、説明を求められた場合には、リーフレットを手渡し説明、詳細はホームページへ誘導するというスタンスで対応している。
・個人情報の説明で納得を得るために時間がかかるなどにより、結局情報全体の網羅性が損なわれることはなるべく避けたい。
・情報を提供することが事業の中核であるので、提供する情報について、必要な人が必要な手段で見られるようにすることが重要と考える。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・各部署から兼業で集まった職員がプロジェクトチームを作り、規程や体制作りを行った。

（２）個人情報の取得

（原則はオプトアウトとし、事後~~的~~に第三者提供の停止を要求されたら対応する）

・企業の情報を収集する際には、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、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。

・ただし、オプトアウト方式にすると、個人情報と関係のない企業情報などについても「提供を停止して欲しい」という要請が出てくることもある。

（３）個人情報の利用（第三者提供を含む）

・本人からの要請により個人情報の第三者提供を停止した場合には、その個人情報について削除するわけではなく、提供用データベースからはずし、提供の停止を行う形にしている。

・個人情報の部分的な提供停止要請については、停止要請を受けた種類以外の個人情報は、収集・更新・提供を続けている。

・代表者の住所や生年月日については提供停止もやむを得ないと考えるが、氏名について提供を止めて欲しいという要請がある場合、「企業情報の一部として重要な情報である旨」説明し、納得いただけない時には当該企業情報の提供そのものを止めるようにしている。

（４）個人情報の管理

①情報の管理体制

・サーバに対するアクセスログを取得している。アクセスログについては、現状分析などは行っておらず、問題が生じたらアクセスログを調べる、という体制である。

・外勤職員用パソコンのローカルディスクへの書き込みは禁止している。また、ドライブは原則としてつけないようにしている（FD 除く）。

②従業者への教育方法

・個人情報保護規程を策定し、法解釈や具体的な対応方法ということでは Q&A を作成して対応した。

・「取扱事業者としての義務」「必ずやること」「絶対やってはいけないこと」を平成 17 年 4 月に実施した全体研修で説明した。地方の営業所においては、支店長やキーマンに参加してもらうことで、後日それぞれに教育してもらうこととした。

・何か対応すべきことがあるごとに、社内のイントラネットで達示している。

・中途採用や新卒職員については、入社時にセキュリティに関する研修を実施している。
・従業者には全員、セキュリティ全般の内容を含む誓約書を提出させている。

③盗難対策

・特定のフロアについては立ち入り制限を実施している。
・身分証明書がないと入館できないようにしている。

④ノート PC の安全対策

（ノート PC の外部持ち出し時は台帳に必ず記載する。会社では専用ロッカーに保管する）

・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 は外勤従業者は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外部委託先管理

・個人情報についての取扱合意書を取り交わしている。
・チェックシートを作成し（25 項目程度をチェック項目として設定）、委託先のセルフ・チェックにより点検を行っている。
・外部委託しているのはデータパンチなどが主である。
・今後、チェックシートの確認状況を元に、委託する個人情報の内容の類型化とそれに基づく委託業者への対応を検討していく。

⑥日常点検・確認の方策

・特徴的な取組はなし

⑦初歩的ミスの防止策

・FAX については短縮番号の登録を義務付け、送信時に見直すように指導している。
・外部電子メールは極力しないように指導している。

（５）個人情報の消去・破棄

・データの破棄について、紙はシュレッダーと外部委託業者による溶解を兼用し処理している。
・パソコンについては、ハードディスクの完全消去を行った後で返却・廃棄している。
・企業内情報については、調査のたびに最新の情報に更新されて行くので、過去の情報は基本的に上書きされる。

（６）個人情報の監査

・情報セキュリティ監査を昨年実施した。総務部門が中心となり、各部署の部長やセキュリティ担当者に対するヒアリング及び職場の実際の確認を行い、監査結果をフィードバックした。

・この監査を１年に１度程度は実施したいと考えている。

（７）苦情処理・顧客対応

・業務部門（お客さま窓口）が担当している。

・開示請求に対してはホームページ内に詳細案内を掲載､開示手数料を徴収しているが、法施行後、約 15 件しか開示請求はきていない。

・原則､開示請求の際の本人確認はパスポートや運転免許証のコピー等で実施しており、郵送で開示しているので、郵送だけで手続が済むようにしている。

（８）事故発生時の対応

・「漏えい対応手順書」を策定しており、CPO がトップとなり、連絡・公表・報告などを含めた流れを作成している。

・漏えいした個人情報の本人に対しては、通知・謝罪を以って対応することを想定している。

以　上

γ．その他サービス業（債権回収支援）γ社

業種	信用会社等の債権回収の支援（債務者の居所調査や、債務者から信用会社への電話の取次ぎ等		
従業員数	約 30 人 （他､契約社員約 50 名）	プライバシーマーク取得	あり
保有個人データ件数	3,000～10,000 件程度		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・月間での常時保有件数は 3,000～10,000 件
・自主取得は従業者個人情報のみ。委託元からの間接取得であり、業務期間中のみ保有する。業務終了後すべて返却もしくは破棄する。
・クライアントから個人情報を預託される期間は最長１ヶ月程度である。業務が終了し必要がなくなれば即座に返却する。
・氏名、住所が基本情報である。本人の居所・住所に関する調査が基本業務であるので、これらの情報だけで十分である（原則が訪問であるので電話番号は不要)。
・付加的情報として「性別」や「年齢」､「転居先」や「職場」､「電話の有無」などが顧客から預託されることがある。
・多くはないが、顧客訪問時の注意事項が預託されることもある（例：同居の父親にまず話をしてほしい、等)。
・委託に基づき、滞納者本人の住所地を訪問し、居住確認を行う。
・委託先からの要求に基づき、実態調査を行うこともある。

（２）個人情報保護担当部署

・プライバシー管理委員会（委員長と委員 4 名で構成）が担当している。常設の委員会であり、月一回の定例会議と問題が発生しそうな場合などに随時開催している。
・委員は全員兼任である。各部署から選抜した委員で構成され、組織横断的な体制となっている。

（３）個人情報保護管理者の有無・位置づけ

・代表取締役社長が CP 管理責任者と位置づけられている。

（４）認証取得の有無（時期)、認証の種類、その認証を取得した理由・効果

・プライバシーマーク取得（平成 17 年 3 月)。

・顧客が信用販売の会社であるので、個人情報保護の取組が厳格に行われており、委託を継続してもらう上でも個人情報保護の取組・体制構築は必須であった。
・認証による厳格な個人情報取扱いのための社内体制を構築することも目的であった。
・営業面での効果は特に感じていないが、個人情報を適切に管理していることが必須で求められている。

（５）個人情報保護に向けた取組経緯

・顧客が信用情報を取り扱う企業であるので従来から適切な管理は求められていた。特に顧客から求められるようになったのは 4、5 年前であるが、ここ 2、3 年は特に自社でも踏み込んで取組を行う必要性を感じ、プライバシーマークの取得をはじめ、厳格な体制構築に取組んでいる。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・委託元（クレジット産業）からの個人情報保護に関する要求水準が非常に高まっている。委託元から調査・報告が求められたり、立入監査が行われたりすることもあるが、調査・監査項目の数が増加し、詳細になっている。
・業務の特徴としては、債務者の居所等を訪問することが業務の中心になるので、紙媒体もしくは電子データで個人情報を社外に持ち出すことが必要不可欠な業務である。
・特に、地方展開は契約社員（約 50 名程度）という形で地方居住の者が実施するため、契約職員にいかに個人情報保護の重要性や適切な方策を理解させるかということについて工夫が必要である。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・個人情報保護の責任組織である「プライバシー管理委員会」は部署横断的に委員を選出している。内部監査は独立した組織として、監査の時などは自分の所属部署以外の委員が監査を実施するようにし、厳格な監査ができるようにしている。

（２）個人情報の取得

（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）

・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。
・授受リストは業務終了後も 6 ヶ月程度保管することにしている。
・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（第三者提供を含む）

・特徴的な取組はなし

（４）個人情報の管理

①情報の管理体制

（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）

・契約社員は、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。

（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）

・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。

（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）

・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。

（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）
・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従業者への教育方法
・個人情報保護一般規程と内部規程を定めているが、わかりにくく、営業の契約社員は特に理解が難しいため、「手順書」を作成し、現実の業務で起こりえる行動に落とし込んでマニュアル化している。
・「個人情報を扱う量」や「職位」に応じた研修を実施している。特に地方の営業を担当する契約社員については、地域ブロックごとに集合研修を 4、5 月と 2 回、2 ヶ月連続で開催して、いかに個人情報保護が重要で、会社として力を入れる必要があるかを示した。
・正社員全員を対象に、6 月に集合研修及びテストを実施した。
・この内容については、地方契約社員には「通信教育」の形でテキスト等を配布して実施した。後日、試験を実施して一定水準に満たない者は追加的な補習を行わせた。
・講師はプライバシー管理委員と品質管理グループで指名して内部で手作りで実施した。
・個人情報保護方針については、ID カードと同サイズにしており、ID カードの裏面に貼り付けて常時確認できるようにしている。

③盗難対策
（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）
・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。
・契約社員は自宅で個人情報を保管するので、自宅に指定する型の専用金庫を設置・使用することを義務付けている。

④ノート PC の安全対策
・専用アプリケーションを組み込んだ携帯電話を使用しており、外回り営業の際にはノート PC を使用しなくても済むようにしている。

⑤外部委託先管理
・特徴的な取組はなし

⑥日常点検・確認の方策
・月に 1 度程度、本社において抜き打ち監査を実施している。問題があった場合にはペナルティということで是正するように指導がなされ、その職員の名前が壁などに掲示されるなどの対応がなされる。

⑦初歩的ミスの防止策
・FAX 及び電子メールの使用は原則的に禁止している。
・これらの手段の替わりに、専用に開発したアプリケーションを搭載した携帯電話端末を使用して連絡を取っている。
・どうしても FAX を使用する必要がある場合には、必ず 2 人で送信するものとし、送信時間も 9 時～21 時と限定しており、短縮番号で送信するように義務付けている。
・FAX の結果送信レポートについても必ず送信者と確認者がサインするようにしている。
・具体的取扱手順はマニュアル・フローチャートを作成し教育するが、社内の見えるところにマニュアル等を貼り見えるようにしている。
・社外で業務を行う場合は、個人情報取扱いの注意点・徹底事項を各自点検する。注意点・徹底事項を記載した自己チェックシートを本社が毎回用意している。
・ミスを起こした場合は、該当する部門で是正を行う。原因を考え、同じミスが起こらないよう部門全体で是正するとともに効果を確認する。

（５）個人情報の消去・破棄
・委託業務が終了した後は、委託元に個人情報はすべて速やかに返却している。
・返却が不要な場合は、自社で廃棄している。
・保管期間を 6 ヶ月と定めているが、業務終了後はできる限り早く返却・廃棄している。
・データでの個人情報を取り扱うサーバは、使用年数経過後廃棄時には、記憶装置の破

壊や物理的な処理を加えた上で廃棄し、再利用や譲渡を一切禁止している。
・郵便物の外袋も個人情報が記載されている場合もあるので、授受記録を残し、シュレッダーで廃棄するようにしている。

（業務上のメモについても専用のメモ帳を使用し、最終的には廃棄している）
・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。
・どんな形でも個人情報が増えることを防止しようという考えに基づく対応である。

（６）個人情報の監査
・年に１回の独立した内部監査チームによる内部監査と、プライバシー管理委員会の内部監査がある。
・本社については、不定期の抜き打ち監査も実施している。問題のある行動があればその職員にペナルティということで業務の是正や名前の社内張り出し等を行う。
・地方の営業を担当する契約職員は、自宅を事務所として活動しているので自宅まで監査することはできない。ただし監査日時を設定して、業務中ずっと随行して個人情報を適切に扱っているかどうかを確認している。

（７）苦情処理・顧客対応
・営業本部が常設の対応窓口となっていると同時に、クレーム責任者は別に設置している。
・個人情報は委託元から預託されたものであるので、苦情や問い合わせは委託元との協議により対応する。
・本人からの開示の求めについては、自社では受け付ず、委託元へ開示等の求め、問い合わせをしてもらう。
・今のところ個人情報に関する問い合わせや苦情は寄せられていない。開示の場合の手数料も設定していない。

（８）事故発生時の対応
・CP 管理責任者が対応を指揮する。発生時の体制は常設対応窓口を定めている。
・営業社員が調査を実施する（債務者を訪問する）のは在宅可能性が高い土日、祝日が

多いので、業務が行われる時間帯（8 時 30 分～20 時 30 分）に対応するため、7 時 30 分～22 時は必ず本社に最低 1 名以上の人員が待機し、問題が生じた場合は直ちに対応できる体制をとっている。

・事故発生時において CP 管理責任者は、緊急対応窓口の設置・プライバシー管理委員会を緊急開催し、原因究明・二次被害の防止・予防や継続的な改善活動を実施する。

以　上

δ．そのサービス業（高齢者等生活支援）δ社

業務概要	高齢者・障害者を対象とした緊急通報・生活サポートシステム		
従業員数	約 60 人	プライバシーマーク取得	あり
保有個人データ件数	約 8,000 件		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・全体で約 8,000 件程度を保有している。

・緊急通報・生活サポートシステムを提供する上で必要な個人情報（氏名、住所、電話番号、生年月日、続柄、郵便番号、住所、保険証番号、生活状況、血液型、体重、アレルギー、既往症、かかりつけ病院、診療科、主治医、障害、障害等級、緊急連絡先、緊急連絡先住所、緊急連絡先電話番号など）を幅広く保有している。

・緊急通報・生活サポートシステムは短縮ダイヤルのみついている電話機を利用者宅に設置し、電話機のボタンを押すことであらかじめ入力されている受報センターに電話をかける。受報センターではナンバーディスプレイを使用してどこから電話がかかってきたかを把握し、その番号と関連付けられた個人情報をデータベースから検索し、オペレータの画面に表示する。利用者からの要望に応じて、救急車の手配、お米や灯油の配達手配、隣人、ご家族への連絡等を行う。このようなサービスを利用者に提供するために個人情報を利用している。

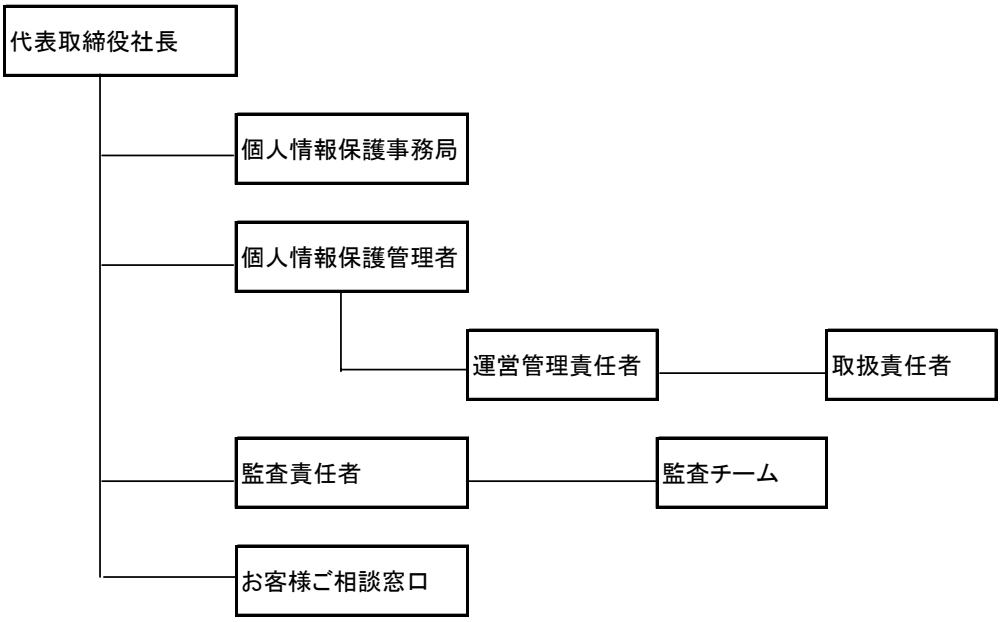
・従業者情報としては、従業者の情報管理をする上で必要な個人情報（氏名、住所、電話番号、生年月日、郵便番号、住所、連帯保証人名、連帯保証人住所、連帯保証人電話番号、人事、給与、保険、年金など）も保有している。

・従業者の情報管理をする上で、入社時の履歴書や職務経歴書に記載されている情報、入社してから必要な情報を管理している。これらの個人情報は業務の円滑な遂行と各個人の業務軽減に利用されている。

（２）個人情報保護担当部署

・システム事業部システム課が担当している。

図表　個人情報保護に関する組織図



（３）個人情報保護管理者の有無・位置づけ

・個人情報保護管理者はシステム事業部システム課主任である。

・代表取締役社長が個人情報保護の宣言ならびに統括管理を実施している。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・プライバシーマーク認証（平成 17 年 6 月 13 日取得）を取得している。

・取得理由は個人情報の重要性を認識した上で、現在の当社の個人情報保護レベルを公正に評価してもらうこと、認証を取得することにより、利用者及び他事業者が個人情報保護のレベルを評価しやすくするためである。

・プライバシーマークを表示することにより、個人情報保護に努めている企業とアピールしやすい。プライバシーマーク認証が第三者機関で行われていることから、利用者に対してより安心してマークの使用ができる。

・同社のサービスは機微情報を所有しており、依頼元の自治体から個人情報の厳重な管理を強く求められる。プライバシーマーク取得により信用が増す。

・最近では、緊急通報対象者の家族から個人情報保護体制について質問を受けることが増えた。プライバシーマーク取得を伝えると安心してもらえる。

（５）個人情報保護に向けた取組経緯

・平成 16 年 4 月　社長宣言による取組を開始した。
・平成 17 年 6 月　プライバシーマーク認証を取得した。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・現在、緊急通報の業界ではプライバシーマークを取得しているのは同社を含めて 2 社である。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・個人情報管理者を中心に 3 名で規程を作成した。体制・規程づくりに際しては一般書籍を参考にし、毎月 2 回程度会議を実施した。
・プライバシーマーク取得準備のため、プライバシーマークを既に取得した経験者にコンサルティング料を支払い、アドバイスを受けた。

（２）個人情報の取得

（情報の取得時には関係者が立ち会う）

・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・利用について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。
・サービスの依頼は個人からの委託の場合と自治体からの委託の場合がある。自治体が依頼主の場合、自治体から同社への業務委託となる。行政からはサービス対象者の氏名と住所、電話番号のみ同社へ連絡される。詳細な個人情報については、聞き取り時に取得する。
・聞き取り内容は必要項目のみ自治体と消防へデータで提出している。データは暗号化し、CD 又はフロッピーディスクに記録して対面で渡している。自治体へは毎月利用状況の報告をしており、その際に渡しているため対面での手渡しの負担はない。

（３）個人情報の利用（第三者提供を含む）

・個人情報については生活サポートと緊急通報のために利用している。
・サービスの一環として訪問聞き取り時に本人と予め確認しておいた第三者（タクシー

会社、隣人等）に対しては必要に応じて連絡している。また、本人からタクシー会社等の紹介の依頼があっても紹介は行わないことにしている。
・生活サポートサービスをしているため、様々なサービス事業者から提携の提案はあるが応じていない。

（情報の更新はサービス提供の間に聴取する情報で行う）
・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。変更点も前述と同様の方法で自治体に報告している。
・救急車を呼ぶような緊急事態が発生した場合は、内容や処理、その後の状況などについて報告を自治体に行っている。

（４）個人情報の管理

①情報の管理体制
・個人情報を取り扱うコールセンターは入口のドアを黄色に塗り、重要ゾーンに入ることを警告し、意識を喚起している。
・コールセンターの外にロッカーを設け、私物は持ち込まないようにしている。コールセンター内で利用する書類等はすべて専用の引出しで管理するようになっている。
・サーバ室に入ることができるのは、システム担当等 3 名のみである。
・個人情報を保管しているサーバは社内 LAN につなげていない。
・本社外にあるバックアップセンターは賃貸ビル内に設置されているが、同センターで管理しているデータはすべて暗号化されており、本社のシステム担当者でなければ暗号を解くことはできない。

②従業者への教育方法
・オペレータ・調査専門員については採用時に 3 ヶ月の教育を実施している。教育を終了すると修了証を発行する。これがなければ業務に就くことができない。
・従業者に対しては年に 2 回集合研修をしている。個人情報保護法、ガイドライン、会社規則、個人情報の処理の流れについて常に一通り教育している。

③盗難対策

（機微情報の紙はジュラルミンケースで持ち運び、アラームを設置している）
・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。

（建物の安全管理を徹底）

・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

・個人情報は入れていない。

⑤外部委託先管理

（外部委託先に対して教育を実施）

・本社外にあるバックアップセンターは警備会社が警備している。この警備会社とは個人情報保護についての覚書を交わしている。

・外部委託先である警備会社に出向き、教育を行った。

⑥日常点検・確認の方策

・特徴的な取組はなし

⑦初歩的ミスの防止策

（FAX の送信には 3 名が立ち会うことをルール化）

・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。
・自治体によって報告の電子メール送信希望がある。送付するファイルは暗号化している。暗号化、添付ファイル、電子メールアドレスは送信前に必ず確認する。

（５）個人情報の消去・破棄

・個人情報はサービス利用終了後問合せに備えて 3 年間は保管している。3 年経過後、紙媒体はシュレッダーで破棄している。シュレッダーの横に抹消記録簿を置き、記録している。
・サーバ内のデータも紙と同様利用終了後 3 年経過した後抹消している。バックアップテープの書き換え作業が一巡する 1 週間程度で完全に抹消される。

（６）個人情報の監査

・年 2 回監査をしている。社内で監査チームを組織し、自分の部署以外の部署の監査を実施する。

（７）苦情処理・顧客対応

・電話でのサービス利用者に関する問合せについては電話を受けてすぐには回答しない。必ず同社からコールバックするようにしている。
・本サービスの適切な運用には、利用者を支援する周辺の人の理解と協力が不可欠である。同社へ問合せをし、その場ですぐにサービス利用者の状況を教えてもらえないことに対し不満を述べる顧客もいるが、支援者の理解を得るための説明は常に行っている。必要に応じて訪問して説明する場合もある。最近は個人情報保護についての認識が深まったせいか、苦情は減った。
・例えば、理解を得るため同社が民生委員大会に出向き、個人情報保護の説明を行うとともに､電話では即答できず必ずコールバックが必要である旨を説明することもある。
・開示請求は今のところない。

（８）事故発生時の対応

・事故発見時に上長に報告され、社長へ報告される。
・社長は休暇中でも連絡がとれるようにしている。
・サービスが 24 時間 365 日提供されているため、事故発生時にはいつでも会社として対応できる体制がとれる。社内の緊急連絡網も用意されている。

以　上