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 1,900 人	プライバシーマーク取得	あり
保有個人データ件数	従業員の個人情報： 約 37,000 件、顧客預かり情報：約 153,000 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

・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 37,000 人分の個人情報（7 年間の給与データ、DB：約 25,000 人分、書面：約 12,000 人分）である。

・正社員数は約 90 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 153,000 件である。

（２）個人情報保護担当部署

・管理本部

（３）個人情報保護管理者の有無・位置づけ

・管理本部　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 2009.05.16～2011.05.15）

・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。
・短期間で終了するオペレータも多く、要員の入れ替わりが激しいため、要員の採用と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）

・同社は大手通信事業者の一事業部門が独立して設立された会社であり、現在も大手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、特に違和感なく取り入れることができた。
・コンプライアンスは管理本部が担当しており、個人情報保護の他に企業情報、法令順守、社内ルールの策定なども担当している。既に JISQ15001：2006 年版での更新認証を 2 度受けており、2006 年版個人情報保護マネジメントシステムに基いた運用も浸透している。

（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。
・自社コールセンター（東北、東京、関西）では、顧客が正当に取得した個人情報を預かって、顧客から受託したコールセンター業務をおこなっている。
・当社として取得するのは、従業者の個人情報のみである。

（３）個人情報の利用（第三者提供を含む）
・受託業務で利用する個人情報は、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。
・従業者の個人情報は労務管理などの社内利用が主である。ただし、出向先や就業先企業には一部の個人情報を提供することがあるが、すべて本人の同意を得て提供している。

（４）個人情報の管理
①情報の管理体制
・受託業務の運用のために顧客から個人情報を預かる場合、必ずパスワードの設定又は暗号化など何らかのデータ保護措置を施して受け渡しをし、セキュリティエリア内で管理する。
・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 カード管理としたいが、コスト面から採用していない。
・来訪者の入室には、単票式の来客票に記入して頂き、かつゲストカードを着用して頂いている。

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
・可搬可能な外部記録メディアは使用禁止としている。
・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 を携帯し、紛失・盗難にあうリスクを低減する措置として、ノート PC の使用自体を原則禁止としている。現在、一部のノート PC を除き、ほとんどをデスクトップ PC に切り換えている。
・ノート PC のみならず、全ての PC にセキュリティワイヤーの取付けを義務つけている。

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。

（イントラネットで事故事例を紹介、ポップアップ画面の使用で注意を引く）

・全従業者に宛てたイントラネットを通じて個人情報漏洩事件・事故の事例を紹介し、個人情報保護への取組みの重要性について周知・啓蒙を行っている。特に、トップのポップアップ画面に、マスコミに発表された個人情報漏洩事件・事故の概要を掲載し、常に新しいニュースを社員に発信している。朝礼などで発表し、教育のテーマとして活用している。
・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

（FAX は原則使用禁止。使用するときは許可申請による）

・誤送信防止のため、FAX の使用を原則禁止している。まずは、電話や PDF など他の方法で解決できないか検討する。どうしても送信する必要がある場合には、予め送信内容を詳しく記入した申請書を提出し、許可された送信物のみを送信する。その際には、2 名以上で確認しながら送信する。あるいは短縮登録する。短縮登録の場合は登録時に 2 名で確認する。番号は直接、契約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 を使用したときは、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、複数回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。タイトルや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（社外に出ないメール）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、記録メディア（FD・CD・MD・USB メモリーなど）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、管理簿に記載して管理し、データ消去の記録も残し、破棄する際には物理的に裂傷処理している。
・**個人情報の破棄には、**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実施）

・1 年に一度、社内、コールセンター、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ごとに点検を行い確認している。
・現在、テレビ会議を利用した監査を行っている。すべての項目について現地で監査を行うことより、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。目視確認が必至の項目については、現場に出向いた時に確認をしている。
・「個人情報保護マネジメントシステム要求事項　JISQ15001：2006」に準拠した監査ハンドブックを作成し、教育資料としている。

（教育・研修方法の効果測定を監査の際に実施。部署ごとにフィードバック）

・教育内容の浸透度を確認するために、各拠点のオペレータに直接監査を実施している。「オペレータ個人の理解度を確認する」というよりも、教育・研修方法の効果測定が第一の目的である。同じ教育・研修を受けたオペレータは同様の回答をすることが多く、管理者の意識レベルがそのまま影響することがうかがえる。
・監査結果については、当該部署別にフィードバックし、全社的な傾向分析をコンプライアンス委員会で発表している。

（７）苦情処理・顧客対応

・開示の手数料は 1,500 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。

・社内的にも、事故発生部署の責任者、機密管理者や事故関係者を交えて、事故原因を掘り下げ、再発防止について議論をし、その結果を社内に公開して共有している。

（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