オ．小売業（通販等）　オ社

事業概要	通信販売		
従業者数	約 1,800 人	プライバシーマーク取得	あり
保有個人データ件数	約 1,700 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、個人情報の種類、個人情報の利用目的

・約 1,700 万件（重複あり）

・通信販売事業で保有している個人情報の種類は、氏名、性別、年齢、住所、FAX 番号、メールアドレス、口座番号、クレジットカード番号、購入履歴、不払い情報等である。カード決済のみを行う顧客については、口座番号は保有していない。個人情報の登録は 1 回で、2 回目以降に注文するときには前回登録した情報で決済できるようにしている。

（２）個人情報保護担当部署

・事務局は総合的リスク管理室にある。（2008 年 11 月時点）

・会社リスクマネジメントの一環として、個人情報保護に関する取組もリスク管理部門が担当するようになった。

・各部署に個人情報保護の担当者がいる。各部署の担当者は、役付きの人が多い。

（３）個人情報保護管理者の有無・位置づけ

・リスク管理室長が兼務している。当該役職が責任者になることになっている。（2008 年 11 月時点）

（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

・2005 年にプライバシーマークを取得した。

・2007 年には新 JIS 規格への移行審査を受審、認定付与を受けた。

（５）個人情報保護に向けた取組経緯

・2003 年からプライバシーマーク取得を視野に入れて取組を開始した。

・2003 年以前にも、システム部門など関連部署では、顧客情報を重要視し厳密な管理を行っていた。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・通信販売の場合、大型家具などの産地直送システムがあり、個人情報を委託する場合があるという特徴がある。
・電話対応を行うオペレーターが多い。オペレーターは人材の入れ替わりが激しいことや、事業拡大に伴って大量雇用する場合があることがあり、教育が難しい。

２．個人情報の適切な保護のための取組について

（１）準備（規定・体制づくり）

・個人情報保護規程は法律の施行前からあり、プライバシーマークの取得を目指し始めたことを契機として規程を改訂した。規程の改訂は新規格への対応時、更新審査の前後などに行っており、今年は１年で２回改訂した。

（２）個人情報の取得

・取得した電子メールアドレスに送信したメールマガジンが顧客に届かなかった場合には、WEB 上のネット会員用のマイページに届かなかった旨を通知し、登録更新を促している。
・郵送の DM が届かない場合には、転居している、又は宛て先不明の状態であるということを把握し、DM を送らないようにしている。
・以前は、DM を送った際に電話で着荷確認をしており、その際に登録情報の更新を行うこともあった。
・ガイドブックを年に 2 回作っており、個人情報への取組や方針などを明記して送付している。また、ホームページにも掲載している。
・WEB での注文の場合は、ホームページ上に同意するかを問うチェックボックスを設けている。ホームページ上の注文書を出力、印刷して書き込む場合にもホームページ上に説明を記載し、読んでもらうようにしている。
・電話で注文を受ける場合には、カタログを新規に希望する場合、商品を注文する場合、それぞれにマニュアルを作っており、口頭で個人情報の取得目的に関する説明をしている。
・棚卸は、定期的に年１度行っている。各部署から保有個人情報をすべて挙げてもらい、ライフサイクルごとにリスク管理をしている。どういったリスクが発生するかを網羅する一覧表と対応方法を作成し、提出してもらうようにしている。
・監査の前に部門点検を各部門で行い、規定に沿って確認、棚卸をしてもらう。
・業務代行をするため、他企業の個人情報を預かる場合がある。その場合、受託者として確認をしている。新しい個人情報が発生する場合には、棚卸を行い、確認すること

を義務付けている。

（３）個人情報の利用（第三者提供を含む）

・第三者提供はない。
・しばらく自社の通信販売を利用していない顧客に対し、電話で広告を行うことはある。
・社内では、購入履歴の傾向を分析して例えば広告に反映させるようなマーケティング分析を実施している。

（４）個人情報の管理

①情報の管理システム

・建物はすべてIC機能の付いた社員証で入退室の管理をしている。
・サーバールームは1箇所に集中させており、退室時もICカードが必要である。
・個人情報のデータベースは、保険事業、通販事業、ネット会員、金融事業など、個人情報の種類によって分けている。
・データベースのアクセス権限は仕組みによって異なるが、個人情報のダウンロード権限や閲覧権限を設定している。ただし、クレジットカードの情報はクレジットカード担当しか分からないようにしている。

（データベースのアクセスログの定期点検を実施。時間外や休日のログに注目。）

・データベースのアクセスログを取得し、定期的（少なくとも3ヶ月に1度）に点検している。時間外、休日等のアクセス状況に着目している。
・PCの操作ログも取得している。セキュリティポリシーを設定し、ポリシーに抵触する操作が発生した場合、通知が電子メールで事務局、内部監査担当、システム担当に送付される。公開はしていないが、監視基準が定められており、不正操作と判断された場合、監視責任者より警告が発信される体制になっている。
・外部メモリは原則として禁止しており、許可制にしている。

②従業者への教育方法

・全社で個人情報保護に関するeラーニングを、年に1回実施している。所要時間やテスト問題の理解度はデータとして把握している。オペレーターも全員に教育している。

（実践に近い事例や投げかけ形式の質問を用いた教育を実施）

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

・加えて、実際に取り扱いのある個人情報（および個人情報と思われるような情報）を引き合いに出し、「この情報は個人情報に該当するか」、など投げかけ形式で従業者に考えさせるような電子メールを送付し、教育している。
・啓発のため、漏えい事故の事例を全社全員にメールで配信している。
・管理者に対する研修を実施している。
・業務委託先に対し、委託先教育を実施している。

③盗難対策
・持ち出すノート PC には暗号化ソフトを入れている。

④ノート PC の安全対策
・ノート PC の持ち出しには申請が必要である。そもそも持ち出す必要がある部署が限られており、持ち出す人は把握できる程度の数である。ノート PC は返却の義務があり、返却後の確認を行う。
・ノート PC は鍵のかかる引き出しに入れる、またはワイヤーで固定している。

⑤外部委託先管理
・外部委託先の選定に際しては基準を設けている。基準に沿って選定されているかの確認を申請部門が実施し、事務局と個人情報保護管理者が承認する流れで確認している。セキュリティ対策について質問・把握し、対策が現在進行中か、既に導入済みでなければ委託先として認めない。
・チェック項目はセキュリティの状況や再委託の予定などの内容である。再委託先に対しては自社と同様の取り決めを交わしてもらうことにしている。取引終了時のデータ廃棄の手順も定めている。
・委託中のチェックは半年に 1 度の提出を義務付けている。
・委託先についても、テキストを渡し、ビデオを見せ、アンケートをとるなどの教育を実施している。

⑥日常点検・確認の方策
・フロアの施錠確認は毎日行い、記録している。
・個人情報は施錠管理しており、鍵は原則管理職が持っている。
・監査前には、点検表に沿って各部門で自己点検を行っている。

⑦初歩的ミスの防止策
・送信時のリスクについては、講じるべき対策について一覧表の中で明確にしている。
・以前は FAX を送る人は決められた人としていた。

・書類は重要度によって箱を分け、部門に一箇所、所属長が目の届くところに箱を置き、施錠管理していた。4 段階に分類し、機密順であった。現在は環境保護の観点から、白黒プリント、カラープリント、紙の種類、再利用の可否などによって 4 段階に分別しており、リサイクルや固形燃料化の処理をしている。廃棄業者とも情報保護の契約を結んでいる（所属長の目の届くところでの施錠管理の方法は同じ）。

（５）個人情報の消去・破棄

・個人情報については、データの作成依頼画面において、個人情報の有無と利用期間を申告する仕組みになっている。それに基づいて台帳を作成し、期限が来た時点でデータの現状を聞くようにしている。
・紙媒体のものは委託して廃棄しており、外部に廃棄を依頼する場合は廃棄証明をもらうようにしている。

（６）個人情報の監査

・個人情報保護のための監査を、全部門に対して年に 1 度実施している。規格への適合性の監査（事務局に対する監査）もある。

（７）苦情処理・顧客対応

・問い合わせは全て、お客様相談室で対応している。
・DM を送らないでほしい、などの苦情に対してはご案内をやめるようにしている。情報の物理的な消去はしていない。
・社内のイントラネットで顧客からの苦情を開示し、閲覧可能にしている。
・開示請求はまれにあるが、多くはない。
・本人確認は、名前、住所、顧客番号、電話番号など、複数項目について確認することで行っている。

（８）事故発生時の対応

・対応手順は規程で定めている。緊急事態の定義、対応方法、保護管理者の対応、緊急時の対策委員会の設置、協議内容、監督官庁への連絡などの手順が定められている。

以　上