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 520 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 17 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 17 年）

・ISO27001 を取得(平成 18 年)

・取得理由は、個人情報保護を含む、情報セキュリティの維持・向上と外部認証機関によるセキュリティ環境の検証を受けることにより、客観的な視点で現状を把握できるためである。また効果としては、「PDCA」サイクルによるマネジメントシステムを他の業務効率改善にもカスタマイズして水平展開を行い、成果を導き出せたこと。

（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）

・ポリシー(方針)、スタンダード(規程)、プロシージャー(手順書)を策定し、個人情報保護管理委員会を設置し、専任担当によるお客様窓口開設、また各従業員への保護法教育研修を実施している。(事例を基にした研修・知識確認テストを実施・継続中)

（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）

・カタログや商品等の送付のほか、メーカーによる製品リコール時において、購入者への安全確保のため販売責任として DM にてアウトバウンドを実施する際に利用する。

・顧客情報の内、購入者が分割ショッピングクレジットを希望された場合、提携する信販会社２社へ提供している。提供された顧客情報により信販会社は購入者へクレジット利用確認と与信の可否を実施している。

・従業員情報、採用情報は自社以外での利用はない。

（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

・監視カメラのモニタリング検証などによる監視体制の強化を実践中。
・毎月個人情報資産の棚卸を実施し、月報報告にて照合、監査を実施中

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

（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

・FAX 誤送信が発生したため、短縮登録であっても必ず個人情報に関係する情報のやり取りは、一切 FAX 対応は禁止とした。

（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。
・PC 上の保有データは規定に則り、毎週情報セキュリティ委員により検査を行い、保存不要と判断されたものは原則消去されている。

（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