

D. 卸売業 D社

事業概要	情報関連機器の卸売販売		
従業員数	約 1,480 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

- ・ 総務担当部門（事務局）

(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」は経営管理担当の常務取締役が担当している。

(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。
- ・ 平成 19 年 7 月に認証を更新(1 回目)した。
- ・ 平成 21 年 2 月に更新審査(2 回目)を受審の予定。
- ・ 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員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。

(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。3 万人～4 万

人／月の新規会員登録がある。

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更新審査に向けて、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。
- ・平成18年7月、監査責任者を、別事業を統括している役員に変更し、職務分離した。
- ・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。
- ・全社の業務内容を分類したうえで「リスク管理表 全社版（28種類）」を作成し、想定リスクの洗い出しと、それらのリスクに対する管理方法の見直しを実施した。
- ・さらに「管理方法」について「規程・基準類」に記載の不備があれば、改訂・新規制定を行った。

(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。
- ・顧客との契約は代理店を通じて行う場合もある。代理店経由での顧客との契約登録においても、当社主管部門と事務局にて契約・説明文面を確認し、お客様が誤解を受けることのないように配慮している。
- ・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手紙は、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。(実際に共同利用している関係会社のみ記載)

(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従業員への教育方法

- ・eラーニングにより短時間で全従業員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。

（自己点検ができるモニタリングシートの作成・配布）

- ・モニタリングシート「自己点検付きマニュアル」を作成配付した。
冊子形式で、遵守すべきルールが見開き左、自己点検チェック項目が見開き右に記載されており、ルールの確認とセルフチェックが同時に出来るよう工夫してある。
- ・社内イントラネットで公開し、各自がダウンロードして出力する。B5 版 20 ページの構成である。

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。
- ・会社貸与携帯電話は、遠隔ロック機能付の機種に全て切り替えた。
- ・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（危機管理担当役員）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。平成 20 年 12 月現在までの累計は約 100 件。
- ・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