エ．小売業（百貨店・スーパー）　エ社

事業概要	百貨店		
従業者数	約 10,000 人	プライバシーマーク取得	あり
保有個人データ件数	約 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、個人情報の種類、個人情報の利用目的

・3,000 万件

・グループのカード会員の情報（データ分析目的のため保持）430 万、販売業務（顧客名簿、カルテ、配送伝票、修理加工伝票等）950 万、ギフト 100 万、クレジットカードの請求データ 1,530 万件、友の会業務（配布通知、入会申込書）累積 184 万件、ネット業務 9 万件、人事情報 220 万件（派遣社員などを含む）

・個人情報の種類は多様で、約 200 種類ある。

（２）個人情報保護担当部署

・総務部内部統制･法務担当

（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専務取締役

（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を取得している。

・プライバシーマークの取得により、漏えい等のリスク軽減、社会的信用の向上、他の百貨店や取引先からプライバシーマークの取得を評価されるなどの効果があった。また、個人情報を保有することのリスクに関する認識を内部的に高めることができた。

（５）個人情報保護に向けた取組経緯

・漏えい事件をきっかけに、会社としてプライバシーマーク取得を目指すと同時に、個人情報の保護体制を一層強化し漏洩等のリスクを軽減することと、第三者の審査を通じ自社の個人情報保護水準を確認する意味があった。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・百貨店業界は個人情報を伴うカード決済の多さや、各種伝票等の種類が多いため、その保管や管理、廃棄等にかかる管理コストが大きい。

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）

・コンプライアンス委員会は委員長を社長とし取締役などで構成され、教育や内部監査等の年度の計画や、内部監査や従業員の教育の実施などを承認する役割を持つ。個人情報保護専門の委員会というわけではない。

・規定は JISQ15001 要求事項に則り内部統制･法務担当で独自に作成した。理解を促すため、規定の説明会を実施した。

・各部門は自部門に存在する全ての個人情報を確認するため「個人情報一覧表」を作成し、整理している。

・確認した全ての個人情報を「個人情報管理表」に記載し、各部門には年１度管理表の提出を義務付けている。情報の数、媒体、保管方法、廃棄方法などを記録している。それぞれの個人情報の重要度と脆弱性をランク付けし、リスクの大きさを把握している。

・日々の点検はチェック表を使っている。毎朝、売場の人が顧客名簿など個人情報があるかどうかをチェックし、定期的に上長が確認する。

・取引先とは覚書を交わしている。覚書の種類は A、A´、B、C と 4 つあり、A と A´については顧客名簿などの所有権が百貨店側にある。A の場合は店舗が退店するときには個人情報を百貨店に置いていくかたちになり、百貨店から顧客名簿等持出す可能性がある場合には A´の契約をする。B は共同利用で、この形態は主に海外のラグジュアリーブランドや化粧品メーカー等が多く、全体の１割強を占める。C は完全に取引先（店舗側）に所有権があり、百貨店との情報共有はない。

（２）個人情報の取得

・本人から直接書面で個人情報を取得する場合は「お客様の個人情報の取扱いについてのお知らせ」の店頭掲示及び利用目的等が書かれた文書を示し本人に口頭で説明する。

（３）個人情報の利用（第三者提供を含む）

・お客様から頂いた個人情報の第三者提供はない。

（４）個人情報の管理

①情報の管理システム

・指紋認証、静脈認証、暗証番号、監視カメラ、ID パスワードなどを導入している。導入の際には、専門家の意見を聞いた。

・個人情報が入っている PC を廃棄する場合には物理的破壊による復元不可能な措置を講じている。

・システムリスクに関しては「システムリスク分析　総括表」を作成している。具体的項目は、システム名、運用部署、システム機能/概要、利用部門、リスクの種類、機能停止時の代替措置及び代替措置等で耐えられる時間、想定されるリスク（影響範囲等）、リスク発生頻度、リスクへの対応（対応済み、今後対応）等からなっている。

②従業者への教育方法

・法律施行後は役員から派遣社員まですべてに対して教育を実施した。現在は年に 1 度の確認テスト（10 問）を実施し、解答例を提示している。テストは自社で作成し、実践で考えられる場面を想定した構成になっている。テスト結果を受けて、問題の誤答率を集計し、教育や監査項目等に反映している。
・従業者に対して、毎年、プライバシーポリシーや年度の行動目標、個人情報に関する問合せ先等を記載したポケットサイズの小冊子を配布している。

③盗難対策

・全てのパソコンに盗難対策としてワイヤーで固定している。ワイヤーを解除するためには専門部署の承認を得て、外した記録をとる仕組みになっている。
・入退館に荷物検査があり、意識付けや防犯に役立っている。

④ノート PC の安全対策

・社員の PC の持ち出し、持ち込みは禁止である。テナントは正規の手続を経た上で PC の持ち出し、持ち込みが可能となる。
・誰がいつどういう作業をしたかというログをシステム上でとっている。

⑤外部委託先管理

・印刷会社、配送会社、データ入力、などが委託先である。
・業務委託先選定基準に基づいて委託先の評価を行っている。委託先の評価は 2005 年度から 2007 年度までの 3 年間で全ての業務委託先を訪問したが、一回りしたため昨年度からは「個人情報調査表」を送付し自己評価をしていただいている。新しく契約する委託先には原則として契約前に実際に訪問し、現場を見て話を聞いている。大規模グループを評価するような場合や IT 分野の業務委託をする場合には専門の外部コンサルが同行することもある。プライバシーマークを取得していることを条件にはしていないが、多くの委託先が取得している。

⑥日常点検・確認の方策

（管理体制チェックシートの定期実施でミスの削減を実現）

・事故の発生の原因が郵送時の誤送付、封入ミス、伝票の持ち運び中の紛失などである

場合が多かったため、チェックシートを事務局が作成し各部門の部長代理クラスに毎月チェックしてもらうようにしている。

・長期間にわたり実施したことにより、個人情報の紛失や漏洩が大幅に減少した。

図表　個人情報管理体制緊急チェックシート

2008部・Div別 個人情報保護管理体制 月別チェックシート

（提出日）
部
検査責任者

チェック内容

必須項目	1	個人情報が無くなれば判る状態か	各職場、ショップ等の個人情報が無くなればすぐ判るよう整理整頓とナンバリング、区分け等出来ていること。
	2	個人情報の受渡し確認と記録はあるか	個人情報の受渡しの際、確認し記録をしているか。（必ずしも授受簿作成が目的ではない）
選択項目	1	個人情報のＦＡＸは厳禁	個人情報のFAX送信は厳禁です。　※顧客の強い要望や業務上必要な場合は、上司の確認を得、相互確認の上送信する。
	2	送付時の相互確認	個人情報を郵送等する際、第三者が宛名等のチェックを行い、封筒の裏に担当者と第三者が押印したうえで郵送する。
	3	移送時のクリアケース使用	個人情報を記載した伝票を館内で移送する際、必ずクリアケースに入れて持ち運ぶ。また、原則、他業務と兼務しない。
	4	並行作業時のバインダー使用	売場のカウンター等で、並行して作業する場合、伝票等が紛失しないようにバインダーに挟んで作業する
	5	個人情報を区別する赤いクリアホルダー使用	個人情報が個人情報以外の書類と区別するため赤いクリアホルダーを使用する(赤いクリアホルダーは10枚単位で用度にて物品購入のこと)
検査責任者必須		個人情報保護活動報告書記入	毎月「個人情報活動報告書」に実施記録を必ず記入すること。

チェック実施月	3月						4月						5月						6月						7月						8月					
	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
チェック内容 ＼ 課・Div・担当名	無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録					無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録					無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録					無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録					無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録					無くなれば直ぐ判る状態か	個人情報はあるかの受渡し確認と記録				
①																																				
②																																				
③																																				
④																																				
⑤																																				
⑥																																				
⑦																																				
⑧																																				
※　検査責任者必須項目																																				

チェック基準
○　全てルール通り行われており、全く問題ない
×　期間中にルール違反があった
△　ルールを知らない者がいたが、指導でルールを守らせた
ー　該当する業務が無い

＊毎月のチェック結果を、翌月初(5日迄)に法務担当までメールで送付して下さい。

⑦初歩的ミスの防止策

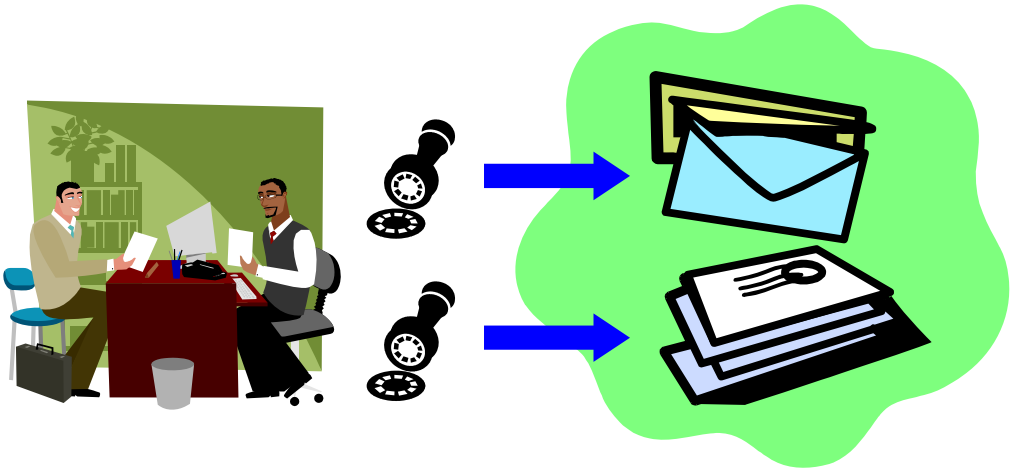
・情報セキュリティ対策として、組織内の機密情報や個人情報、誹謗中傷などの不適切な表現が含まれるメーセージを電子メールで送信した場合、配信がとめられ、内部統制･法務担当に連絡がいく。内部統制･法務担当者がその内容を確認してから配信をするようにしている。

・伝票等の紛失を防ぐため､クリアファイルに入れて持ち運ぶように定めている。

（封入時に 2 名が確認・押印することでミスを軽減）

・郵送物の封入のダブルチェックをしている。封入前に 2 人で確認し、封入時にも 2 回以上確認するようにしている。封入の袋にあらかじめ印鑑を押す場所を 2 つ印刷しており、必ず 2 名が押印するようにしている。

図表　封入のダブルチェック（イメージ）



（５）個人情報の消去・破棄

・廃棄の期間を定めている。
・伝票等まとめて廃棄する場合には、移送を業者へ委託し、廃棄現場まで社員が同行して廃棄の事実を見届けている。
・各売場でもシュレッダーを利用している所が多い。
・廃棄忘れ時は監査の際に指摘する。

（６）個人情報の監査

・個人情報保護マネジメントシステムの運用がどのようになされているかを目的とした内部監査が全部門を対象に実施されており、監査終了後「PMS 運用状況監査報告書」を社長に報告し承認を得ている。監査の際、日時やチェック項目は事前に通知している。改善事項があった場合には、「PMS 監査改善要求書／回答書」を記入・提出することになっている。
・内部監査員の多くはベテラン社員で構成され、個人情報に関する研修を受けて監査を実施している。
・チェック項目は毎年発生した事故や苦情、方針等に応じて変えている。

（７）苦情処理・顧客対応

・2005 年以降現在まで 44 件の個人情報に関する苦情・問い合わせがあった。
・開示請求もあるが、内容は購入金額の証明を目的としたものが多く、保有する情報を知りたいといった要望や、情報をどこで入手したかなどの質問はあまりない。本人確認は自動車免許証等、本人であることの確認を確実に行っている。

（８）事故発生時の対応

・不正・故意であった場合には指導や賞罰の対象となる。

・内容によっては、顧客を直接訪問して説明・謝罪する場合もあり、個人情報保護に関する苦情についてもそれ以外の苦情と同様に担当部門が対応している。関係官公庁や業界団体への説明や、HP にお詫び文を掲載するという対応を行う。

・大きな事故の場合には対策本部を設置し、問答集を作るなどの対応をとる場合もある。

・事故の情報共有は部長会や社内インフォーメーション等で行い、再発防止に役立てる。特に事故が起こった場合はまず内部統制･法務担当へ迅速に報告することにしている。

・他企業等で起こった個人情報の事故で、当社にも参考になりそうな事例は全社又は、関係部門に向けて内部統制･法務担当がメールや社内インフォーメーションで通知文を発信している。

・事故が発生した場合はトップまで報告している。現場では、事故に対するプレッシャーが高く、従業者の意識付けになっている。

以　上