

## コ. その他サービス業（印刷・広告） コ社

事業概要	プリントサービス、発送、カード製造、ビジネスフォーム用紙製造など		
従業者数	約 1,400 人	プライバシーマーク取得	あり
保有個人データ件数	約 1,000 万件		

### 1. 個人情報に関する概要

#### (1) 保有する個人の情報件数、個人情報の種類、個人情報の利用目的

- ・個人情報の種類別の保有件数は以下の通り。

	個人情報の種類	件数
1	【受託業務の個人情報】 顧客より受託した業務（プリント処理、社員証製作等）を実施するため、顧客より一時預りした個人情報	プリント処理等＝約 950 万件／月 社員証製作等 ＝約 1 万件／月
2	【受託業務外／社外の個人情報】 顧客、仕入先等の窓口担当者や配送先等に関わる個人情報	約 11 万件／月
3	【受託業務外／社内の個人情報】 従業員の個人情報	約 1,650 件（従業者数）

- ・個人情報の利用目的は以下の通りである。

当社は、お客様からの受託業務を遂行するために個人情報をお預りする場合、および当社が個人情報を取得する場合、次の通り利用目的を特定し、その範囲内で利用をいたします。特定した利用目的の範囲を超えて個人情報の利用を行う場合は、ご本人の同意を得てから利用いたします。

#### (1) お客様からの受託業務において個人情報を取り扱う場合の利用目的

##### 1) 情報処理サービス業務

- ①データプリント、封入封緘、シーリング等の処理
- ②発送先別区分け、抜取り、納品・郵便局出し等の処理
- ③データエントリー業務
- ④上記に関する付帯業務

##### 2) カード発行業務

- ①カード製造、エンボス、エンコード等の処理
- ②上記に関する付帯業務

- 3) 印刷加工業務
- ①印刷・加工、発送業務
  - ②上記に関する付帯業務
- (2) 当社が取得する場合の利用目的
- 1) お取引先様情報
    - ①製品・商品の発送および請求・入金処理等の業務のため
    - ②お客様との業務上必要な連絡のため
    - ③電話、メール、FAX、郵便等での製品・商品・サービス等のご案内送付のため
  - 2) ウェブサイト運営、展示会等での取得情報
    - ①当社事業に関するお問合せ・苦情等への回答のため
    - ②アンケート調査等を各種サービスへ反映するため
    - ③電話、メール、FAX、郵便等での製品・商品・サービス等のご案内送付のため
  - 3) 採用関連情報
    - ①採用に関連する各種資料・案内の発送のため
    - ②採用に関連する連絡、および採用選考のため
  - 4) 従業者情報
    - ①当社従業者の給与・税務・保険・福利厚生等、及び従業者管理のため
  - 5) 株主様情報
    - ①株主総会等の開催案内並びに事業活動の報告書等を送付するため
    - ②関係法令に基づく権利の行使・義務の履行のため
  - 6) その他
    - ①当社の場内セキュリティ管理のため
- (3) 上記 (1)、(2) に掲載されていない当社の事業活動における個人情報の利用目的につきましては、問合せ窓口にお問合せください。

**(2) 個人情報保護担当部署**

- ・ CSR 推進グループが本社、全国の事業所全ての個人情報保護について統括している。

**(3) 個人情報保護管理者の有無、位置づけ**

- ・ 個人情報保護管理者をおいている。個人情報管理責任者という名称である。個人情報統括管理責任者により、社内から指名され、個人情報保護マネジメントシステムに関する運用の責任と権限を有する者として位置づけられている。
- ・ 現在は、CSR 推進グループ部長が同責任者に任命されている。

**(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**

- ・ 認証としてはプライバシーマークを取得している。本社ではないものの、データ処理

を主に扱う情報処理センターの全てで ISMS を取得している。

- ・プライバシーマークの取得の理由としては企業の責任という点が一番大きい。また、プライバシー・マネジメント・システム（以下、PMS という）の日本のスタンダードである点もプライバシーマークの取得を選択した理由である。
- ・営業のためという認識は認証取得当初はそれほど強くなかった。印刷業界では最も早く認証を取得した企業である。認証取得後、プライバシーマークが業務を実施する上でも求められるようになり、営業ツールとしても活用できるようになった。
- ・ISO14001 を取得した直後にプライバシーマークを取得した経緯がある。

#### （５）個人情報保護に向けた取組経緯

- ・1999年7月：プライバシーマーク認証取得（※印刷業としての取得は日本初）
- ・2005年4月：個人情報保護法の施行に併せ、関連規程の改訂と教育の実施。
- ・2006年11月～2007年3月：JIS15001/2006年版の規格に準拠するよう、関連規程の改訂と教育の実施。
- ・2007年10月：プライバシーマーク更新審査合格（JIS15001/2006年版での更新認定）

#### （６）個人情報の保有・管理・提供等に関する業界の特徴

- ・委託業務実施用の個人情報を顧客から一時預かりし、大量に保有している点が特徴的である。
- ・また、この個人情報の顧客・会社間の貸与・受渡しは、主に磁気媒体や電送による方法をとっている。その他、個人情報をプリント済みの用紙を貸与されることもあり、様々な媒体で個人情報を管理しなくてはならないことも特徴的である。
- ・どうしても自社だけで捌ききれないので、外部委託が発生することも特徴的である。
- ・委託ということでは、情報処理の作業は子会社に委託している。子会社は本社と同じ敷地内に立地し、PMS の仕組みに組み入れ、本社と違いは無い。
- ・地方の支店・営業所・事業所は市区町村からの受注（税金の納付書など）がある。断裁をして、重ねて、ホッチキスで止めて発送するという仕事があり、それは地元の会社に委託するようなケースもあり、自社内での処理に比べるとリスクが有ると感じているが、遠距離にある情報処理センターに送るのもビジネス上は現実的ではない。これらを勘案し、委託先を一定基準により評価・管理を行った上で委託している。
- ・印刷や発送する書類の中にどのような個人情報が含まれていようが、そのことは直接的に委託費には反映されない。高いセキュリティ管理が求められるような個人情報が含まれている場合でも、価格は同じということも問題である。
- ・顧客から個人情報の含まれるデータベースを受領してから、実際に発送するまで、工程がかなりたくさんあるので、トレーサビリティが一番難しいと考えている。

## 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・体制作り）

- ・個人情報保護の全体会議を年に 4 回開催している。本社や支社、営業所などから代表者(9人程度)が集まり、規程のたたき台を必ず確認した上で表に出すようにしている。
- ・規程の作成に当たっては、事務局だけで作るわけではなく、いろいろな部署に確認してもらったりしている。営業担当部署が自分たちのルールとして策定したものを、製造担当部署がチェックするというも行っている。
- ・合意の上で作ることが実効的であるということや、ルールを作っても周知できないという問題があったので、営業を管轄する部門や製造を管轄する部門に周知をお願いするためにそのような体制をとっている。
- ・規程については特別に定期的な見直しを実施しているわけではない。法改正、制度改正、認証の基準の変更などがあれば機動的に改訂を行っている。同種事業者が事故を起こしたような場合にも改定が行われることがある。同じ規程でも第 8 版になっている部分がある。
- ・また、全体会議で、現場を担当する部署から規程改定の提案が上がってくることもある。必ずしも規程の内容を緩和してほしいという内容だけではない。

### (2) 個人情報の取得

- ・ホームページから問い合わせを行う際には、個人情報に関する同意をすることをクリックした上でしか送信できないような仕組みにしている。

### (個人情報を委託元から受領する際に、適正に取得されたものであることを確認)

- ・個人情報の含まれたデータを、委託元から受領するタイミングで、「取得については法令を遵守し適切であること」、「機微な情報については、その利用等についてご本人の同意を得ていること」を前提に処理させていただきますのでご了承ください。」ということを預かり書に明記して、委託者側での適法な個人情報の取り扱いを前提として個人情報の委託を受けている。

図表 預かり書（イメージ）

データ預かり書(〇〇〇株式会社)	
「取得については法令を遵守し適切であること」、「機微な情報については、その利用等について本人の同意を得ていること」を前提に処理をさせていただきます。	
顧客名:	
受領データベースの名称・内容・媒体・数量:	
担当者:	弊社担当者:
実施する処理:	
受領日:	返却:要(予定 月 日 )/不要

- ・ 個人情報は利用目的で限定した上で委託を受けている。そうしないと印刷・発送などのシステムも組めないで、極力余分な情報はもらわないようにしている。
- ・ 基本的には、預かった個人情報は返却を行っている。

### (3) 個人情報の利用（第三者提供を含む）

- ・ 受託案件で第三者提供を行っていることは無い。
- ・ 従業員情報の第三者提供はあるが、労働組合や保険関係などだけである。
- ・ どちらかという、個人情報を委託元から受領する側である。（委託元が何らかの個人情報の不適切な利用をした結果として）委託元の事情説明に同行するようなケースはありえる。

### (4) 個人情報の管理

#### ①情報の管理システム

- ・ 物理的措置という部分では、従来は本社のセキュリティが弱かったが、外部からの侵入を防ぐように、外壁の改修、センサーを設置した。
- ・ セキュリティ・レベルを5段階（G1～G5）に分けて、作業場単位でレベル分けを行い、入室と退室を厳格に管理している。
- ・ モニタリング面でも厳しくなっており、G3以降はビデオカメラが設置されている。
- ・ G3以降はカメラ付き携帯電話の持ち込みは禁止されているなど、持ち込み可能な情報媒体の制限も行っている。
- ・ 当然ながらPCにアクセスできる者の権限も制限している。
- ・ パソコンを使用したデータベースアクセス、ファイルアクセスなどのモニタリングはログ管理を行っている。誰がいつ個人情報を含むデータをダウンロードしたのかとい

うこともわかるようになってきている。(全社員のパソコンがモニタリングされている)。

## ②従業員への教育方法

- ・2007年に規程を改定した際には、それぞれの本部ごとに教育を実施することを依頼したが、それだけでは無理があるので、CSR推進グループが地元に出向いて説明会を開催した。説明会における内容を確認する手段として、全職員を対象としてeラーニングシステム上でテストを実施した。1人ずつのパソコンが無い製造部の方には紙ベースで試験を実施した。
- ・eラーニングは他の教育にも活用している。全国に事業所が点在しているので、eラーニングのほうが有効に機能している。
- ・パソコンを使える派遣職員・契約職員にもeラーニングで教育を実施している。
- ・年1回の定期教育と随時の教育を実施している。
- ・eラーニングを使うことで、集中的に事務局で管理ができるようになった。
- ・啓蒙教育は年に1度であり、規程などが変わってくればその度実施している。
- ・職制を通じて必ず受講するように促している。部門長と事務局が実施状況を見られるようになってきている。
- ・見た後にテストに合格しないとeラーニング受講が終了したことにならないもの、テストだけeラーニングで実施するものの2種類がある。いずれも点数を一定程度取らないと終わらないということになっている。

## ③盗難対策

- ・持ち出しパソコンの暗号化ソフトを導入している。
- ・個人情報の持ち出しについては許可制を導入した。
- ・それぞれの部門長による許可がないと持ち出せないという形になっている。

## ④ノートPCの安全対策

- ・PCおよび媒体の持ち出しは禁止されている。申請をしないと持ち出し可能にならない。
- ・持ち出し可能PCは必ず暗号化ソフトが組み込まれている。
- ・アクセス制御は行っている。

## ⑤外部委託先管理の方策

- ・委託先を新たに選定する際には、「個人情報委託取引先調査シート」をセルフ・チェックしてもらうようにしている。チェックしてもらった後は、事務局もしくは実際に管理を行う関係事業部が立ち入りチェックに行き、チェック内容を元に委託の承認をするようにしている。
- ・立ち入りチェックで問題が指摘されるような場合には、対応策を実施することを要請

することもある。

- ・「個人情報委託取引先調査シート」には、必ず守っていなければならない項目もあり、ある程度できていれば良い、という項目もある。
- ・チェックに加えて、委託先については必ず個人情報に関する覚書を取り交わさないと作業を開始できないようにしている。

#### (委託先については認証の有無、委託業務の内容などでグループ分けを実施)

- ・プライバシーマーク、ISMS を取得していない事業者については、外部委託先として適切か否かのチェックを年に1度以上行うようにしている。
- ・主管事業部と相談して、(個人情報の適切な保護の観点から問題が多いため) 委託を行わなくなった事業者もいる。監査時に問題点を指摘し、対応を要請したにも関わらず、対応を要請した点についての改善が見られないような企業である。
- ・社内イントラネット上に、委託可能事業者リストを掲示している。
- ・委託先企業については、2段階で分けている。「データを渡してよい(処理を任せてよい)事業者」と「封入・封緘などの事後処理だけを委託できる事業者」である。
- ・また、具体的なミスがあった場合は、臨時で監査に行くようにしている。

#### ⑥日常的点検・確認の方策

- ・全社員、パソコン保有者に対して、パスワードを3ヶ月に一度の変更を依頼している。
- ・5分～10分作業を行わない場合はロック付スクリーンセーバーがかかるように規定している。
- ・これらのチェックは日常的には行わず、内部監査時にチェックする形にしている。
- ・受注するごとに、委託される個人情報のリスト(「個人情報特定表」)を作らせてリスク把握を行っている。含まれるデータ項目、受託件数、保管期限、顧客との再委託などの契約条件などについて一覧管理するようにしている。
- ・上記の個人情報特定表について、会社の中のイントラネットに、部ごとに貼り付けておくような工夫をしてある。
- ・この個人情報特定表については、年に1回棚卸しするようにしている。
- ・棚卸しの際には、1年間に受託した案件と記載されている案件について照合する。その際に、照合で個人情報の登録漏れが生じているかどうかを判断している。これをまとめたものが受託個人情報台帳という形になっている。

#### ⑦初歩的ミスの防止策

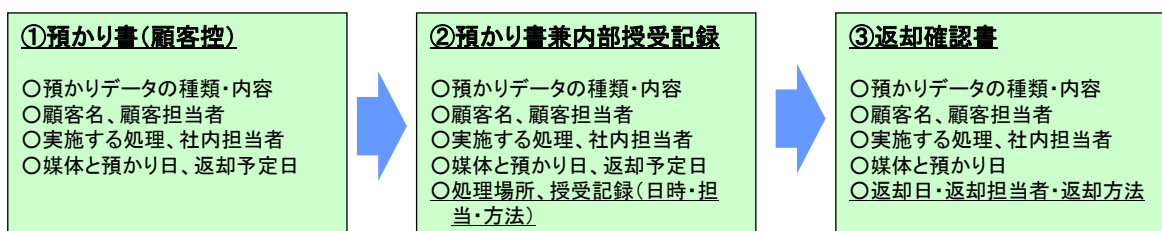
- ・FAXについては送信手順を決めている。短縮ダイヤルの使用などが決められている。
- ・メールで個人情報を送付する場合には暗号化するようにルールが定められている。

## (5) 個人情報の消去・破棄

(個人データは3枚複写式の預かり書で受領・作業・返却まで一貫して管理)

- ・個人データは返却することが基本になっている。受託時に預かった個人情報については「預かり書」を取り交わすが、この預かり書は3枚複写式になっている。受領、記録から返却まで一連で管理できるようになっている。
- ・月に一度、媒体の返却の有無を管理者がチェックするようにしている。
- ・メールや郵送で預かった個人情報については、預かり書とは異なる様式書類でチェックして、月に1度管理責任者がチェックするようにしている。
- ・プリンタなどに個人情報が残ることについては、次の印刷される情報が機械に読み込まれると、自動的に消去されるようになっている。
- ・営業における「預かり書」と、処理場所に渡すときの台帳の照合により、万が一、ミスが発生して営業が預かり書を授受・作成しなかった場合でもチェックはできるようになっている。

図表 3枚の預かり書の主な内容



(※図表中の下線部は、「特にその預かり書だけに記載されている項目」であり、特徴を示す。)

- ・返却しないで良い個人情報は、媒体破棄時は破砕して捨てている。特定の顧客でどうしても消去証明書を求められる場合もあるので、特別処理で証明書を出している。
- ・紙媒体については、環境負荷も配慮し、セキュリティランクをルール化し、セキュリティボックス（鍵がかかるもの）に入れたり、さらに重要度が高い個人情報については、破砕機に直接投入するようにしている。

## (6) 個人情報の監査

- ・内部監査は年1回実施している。2～2.5時間程度かけて実施している。
- ・基本的には内部監査チームで担当している。しかし、営業所が全国30箇所以上あるので、内部監査チームがいけない場合には自己監査で実施してもらっている。営業所によっては必ずしも年に1回の内部監査が実施されないところがある。
- ・本年度は、営業所は全てCSR推進グループと内部監査員で手分けをして実施した。内部監査員はまだ新しい仕組みなので、CSR推進グループが必ず1名は付いていくようにした。



- ・監査は抜き打ちで実施しているわけではない（話を聞きたい人がそのタイミングでないことがあるため）。

#### （内部監査員は地区別の偏りが出ないように内部で育成し、負担の平準化に配慮）

- ・内部監査員の養成が必要になっている。個人情報に関しては昨年より養成を開始した。今年度より営業店勤務職員の一部に、内部監査員になってもらった。
- ・部署、部門や支店・営業店間では、内部監査員がたすきがけで監査を実施するようにしている（A支店の内部監査員がB支店の監査を行い、逆にB支店の内部監査員がA支店の監査を行うような体制）。
- ・内部監査員は社内資格として取得してもらうようにしている。課長・係長クラスの人が担当されている。地区別に何名か出してもらうようにした。これは、あまりに特定の地域に監査員が固まると、そのような地域の監査員が、監査員が全くいない遠く地域にある支店等まで監査に行かなくてはならなくなる状況を懸念したことが理由である。
- ・内部監査の結果については、個人情報に関する全体会議で報告を行い、社長にも報告した。但し、全体的な講評を説明するにとどめており、事業部署ごとにつぶさに状況を比較して報告するわけではない。
- ・監査で出てきた具体的な問題としては、例えば個人情報特定表が十分にできていないということがあった。その他の記録漏れなどが生じていることがある。また、パスワードを定期的に変更していない場合があった。

#### （7）苦情処理・顧客対応

- ・個人情報保護に関する重大な苦情は特に無い。
- ・個人情報の開示請求は特に無い。

#### （8）事故発生時の対応

（事故発生時の混乱や不要な報告を防ぐため、漏えい発生時の報告は2段階に分け、第一報では必要な最低限の情報を挙げてもらうようにしている）

- ・事故などが起きたときに備えて緊急連絡表を設けている。慌てると何を報告してよいかかわからなくなるので、第一報ではどの程度の内容を報告し、第二報以降ではどの程度報告するのか、という点で2つの段階に分けて報告するようにしている。第一報用のフォーマットを作成している。
- ・そのように、「どこまで報告するか」ということを明確にしないと、何度も電話で現場の担当者聞きなおしたりする手間が生じた事例があったからである。不要な情報ばかり報告され、本当に必要な情報の報告が遅れることを懸念していることによる対応である。

- ・漏えいなどの事故が生じた場合に備え、「公表判断基準」を策定している。「管理主体は誰か」「漏えい形態はどうか」「漏えい内容はどうか」「漏えい情報量」「被害の大きさ」の 5 つの視点で判断し、公表するか、公表しないか、ということを明確にしている。公表に際しては経営企画部とも連携している。

以 上