テ．その他サービス業（印刷・広告）　テ社

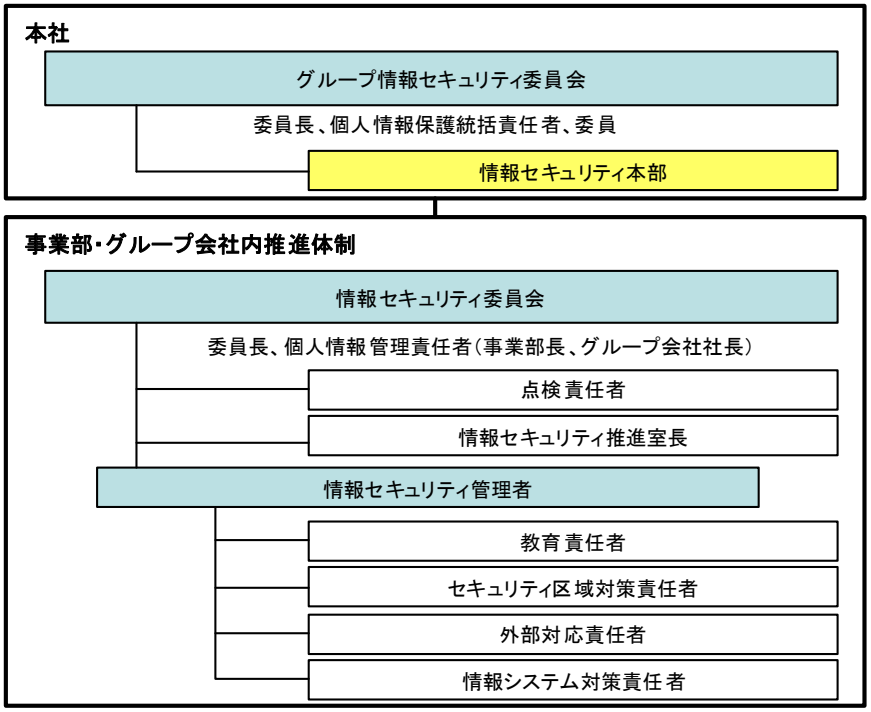
事業概要	印刷業		
従業員数	単体：約 10,000 人 連結：約 40,000 人	プライバシーマーク取得	あり
保有個人データ件数	保有個人情報：約 40 万件 顧客から受託し取り扱う個人情報：約 1 億 1,000 万件/月		

１．個人情報保護に関する概要

（１）保有する個人情報の件数、種類、利用目的

・毎月約 1 億 1,000 万件の個人情報を取扱っており、このほとんどが顧客から受託し取り扱う個人情報で、保有個人データではない。保有個人データは、雇用管理情報のほか顧客担当者情報等の約 40 万件である。
・主な受託業務は請求書・DM等の発行、カード発行、キャンペーン、リサーチ、Web サイト運営、電子出版、などが挙げられる。
・受託業務内容に応じ、業務に必要最小限の個人情報（氏名、住所等）を取扱う。
・自社の Web 運営においては、広報サイト等の各 HP 上で企業や消費者からの意見をいただいている。

（２）個人情報保護担当部署



・全社の統括組織として本社に、役員で構成された「グループ情報セキュリティ委員会」を設置し、さらに同委員会の下に専任で構成された「情報セキュリティ本部」を置き、ルール策定、事業部・グループ会社への検査・指導を実施している。
・さらに、事業主体となる事業部・グループ会社それぞれに「情報セキュリティ委員会」を置き、委員長、個人情報管理責任者（事業部は事業部長、グループ会社は社長と各組織の長が担当)、情報セキュリティ推進室長のもとに、教育、セキュリティ区域、コンピュータ対策など課題ごとの責任者や点検責任者を任命している。

（３）個人情報保護管理者の有無・位置づけ

・個人情報保護統括責任者として、グループ情報セキュリティ委員会委員長である取締役が兼務する。
・体制図は前頁を参照。

（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

・2000 年～個人情報を取扱う主要 5 事業部が順次プライバシーマーク認証取得。
・2005 年：社内で個人情報の 8 割を取り扱う、パーソナルメールなどのデータ処理から印刷・発送を担当する事業部が ISMS 認証取得。
・2008 年：法人としてプライバシーマーク認証取得。
・その他、個人情報を取扱う製造子会社等グループ会社 17 社がプライバシーマーク認証取得、2 事業部、グループ会社 4 社で ISO/IEC27001 を取得。
・個人情報を適正に管理するためには、対策を実施するだけでなく、絶え間ない点検、見直しという PDCA サイクルを回すことが重要であると考え、JISQ15001:2006「個人情報保護マネジメントシステムー要求事項」に準拠したマネジメントシステムを構築し、プライバシーマーク認証を取得した。
・プライバシーマーク認証取得は、一部の顧客からは発注条件に指定されている。

（５）個人情報保護に向けた取組経緯

・さまざまな企業や団体から個人情報を預かり、生活者に向けて発信する各種サービスや製品を提供するビジネスを通じて、個人情報の重要性を認識しており、情報を適切に保護していくことは当然の責務であると考えている。
・1999 年に、「個人情報保護に関するコンプライアンス・プログラムの要求事項（JISQ15001)」制定を受け、企業の自主的な取組として個人情報保護規程を制定し、個人情報保護体制を整備した。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・印刷業界は受託により取得する個人情報の取扱いが多い。

・委託元である顧客の属する業界ガイドラインに従って受託業務を遂行しなければならないため、他の業界ガイドラインや動向に留意する必要がある。
・業界団体である（社）日本印刷産業連合会は、2007 年に JISQ15001:2006 に準拠した「印刷産業における個人情報保護ガイドライン」を制定し、プライバシーマーク制度の指定機関となり、印刷事業者の認証審査業務を開始した。同社は同連合会に役員・委員を派遣するなど、同ガイドラインの制定及び印刷事業者への普及活動を積極的に行っている。

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・体制づくり）

・一般的な体制をとっていると考えており、特に他社の事例は参考としていない。

（２）個人情報の取得

・受託する業務の中で、顧客が所有する個人情報の取得が多い。
・個人情報を取扱う業務を受託した場合は、受注登録システムにおいて、業務開始前に個人情報取扱い識別を行った上で、業務を開始する。
・個人情報の内容や複数部門が係わる場合の個人情報の流れについて記載する様式を用いて、関係部門で情報共有している。
・顧客との個人データ授受は、出来る限り記憶媒体は使わず、ネットワーク経由で行うことを推進している。大手の顧客の場合、専用線を使用していることが多い。通信回線は、VPN が一般に普及してからは、VPN か専用線か、どちらか顧客に選択していただいている。
・個人データ授受におけるネットワーク経由の比率は増加している。

（必要のない個人データを除外するように、口頭又は書面で顧客へ依頼）

・受託する業務内容に対し必要のない個人データを提供しないよう、顧客にお願いしている。口頭で伝わらない場合は書面で要望を伝える場合もある。
・必要のない個人データを除外する作業は顧客への負担となる場合もあるが、各省庁からの指導やガイドラインへの反映もあり、お願いしている。

（IC カードを用いた電子証明書による認証を顧客と自社の双方で実施）

・ネットワーク経由で、IC カードを用いた電子証明書による認証を顧客と自社の双方で利用し、個人データを授受するシステムを構築している。顧客と同社の担当者はそれぞれ電子証明書が格納された IC カードを使って利用者認証を行い、デスクトップセキ

ュリティソフトを導入した個人データ取り扱い用パソコンから、個人データを伝達する。授受サーバ上では自動暗号化している。認証局は自社で運用している。

（記憶媒体での個人データ授受は、暗号化ソフト内蔵 CD-R を自社開発して活用）

・顧客の都合によっては、記憶媒体での個人データ授受を行わなければならない場合がある。その場合のセキュリティ対策として、暗号化ソフト内蔵 CD-R を開発した。PC へのインストールが不要で、CD から暗号化ソフトを起動して書き込むことができる。書き込む際にはパスワードを顧客が自ら設定する。この CD-R は再利用不可の仕様とした。

・この CD-R は、要望があった顧客に販売・提供している。

・記憶媒体の授受は、同社専用のセキュリティ便を用いて実施している。

（紙での個人情報授受は、専用のセキュリティ便を活用）

・紙の授受は減ってきているが、キャンペーンの申し込み葉書をデータ入力する業務においては、紙で授受されることになる。郵便局との授受は、同社専用のセキュリティ便を用いて実施している。

（３）個人情報の利用（第三者提供を含む）

・特徴的な取組はなし。

（４）個人情報の管理

①情報の管理体制

・個人情報保護については、1999 年に制定・2006 年に改訂した「個人情報保護規程」を整備しているほか、具体的な基準についてはグループ内で共通ルールを制定している。

・2007 年には、電算処理室における個人情報の取り扱い、従業員・採用応募者などの個人情報の取り扱い、ノートパソコンや携帯電話の取扱に関するグループ共通ルールを定めた。

・情報セキュリティについては 2002 年に各種関連規程を見直し、新たな体系として、2002 年に情報セキュリティ基本方針を制定、2002 年に情報セキュリティ基本規程を制定・2005 年に改訂し、文書管理・コンピュータ利用・外部立入り禁止区域などの基準を定めている。

（複数のサーバに情報を分散し、保管することで、よりセキュアな環境で管理）

・データを分割し、暗号化した上で、複数のサーバ上に分散して保管するアプリケーションを自社開発し、使用している。

・例えば、あるファイルを A,B,C に分割し、三台のサーバにそれぞれ、「A と B」、「A と

C」、「B と C」を保存する。すると一台のサーバから情報を復元することを防ぐことができるほか、 一台が毀損した場合でも、残り二台が健全であればファイルを復元することが可能となる。

②従業員従業者への教育方法

（営業・企画担当者、工場従業者、海外従業者等の対象別にハンドブック等を作成・配布）

・情報セキュリティ全般、個人情報保護全般（日・英）、個人情報保護（営業・企画担当者向け、リスク分析担当者向け）、コンピュータウィルス対策（日・英）の種類がある。簡易的な教材として、情報セキュリティリテラシーに関する一枚紙を配布している。

・外国語版は、海外主要拠点の従業者用に作成している。各国で法律は異なるため、OECD プライバシー8 原則に準拠し記述しており、日本語のハンドブックとは内容が異なる。

（全社員（ネットワーク環境下にない社員を含）を対象に e ラーニングによる試験を実施して教育効果を検証）

・全社員を対象に e ラーニングによる学習及び試験を年に一度実施し、教育の効果を検証している。

・試験は、40 問ずつあり、ランダムで 10 問出題される。10 問連続正解できて合格となる。各コンテンツにつき、一回ずつ試験を受ける必要がある。

・ネットワークが整っていない環境下の社員へは、PDF に自動採点プログラムを組み込んだファイルを共通パソコンに入れて実施している。

③盗難対策

・個人データを取り扱う電算処理室では、生体認証を導入した入退出管理による入室権限者以外の侵入防止を図っている。

（個人データ取扱者を機能別に分離。システム処理による自動化を進め、個人データを持ち出すことのできない仕組みを構築）

・個人データを取り扱う業務を、設計・開発、出入力・保管、暗号化・複号、データ編集処理、というように機能別に分解し、機能毎に個人データを取り扱える従業員を限定したうえでルールをつくった。

・分業化と共に、システム処理による自動化を進め、容易に個人データを持ち出すことのできない仕組みを構築した。

（個人データ記憶媒体の持出しを防ぐため、担当者数を極少化して社員に限定し、作業エリアを限定し、アクセスログのチェックを頻度高く実施）

・個人データを記憶媒体に書き出すことのできる担当者数を極少化し、同社およびグル

ープ会社社員に限定した。
・個人データ記憶媒体を取り扱うエリアを他のエリアと分離し、同エリア以外での書き出しは一切出来ない環境とした。
・個人データ記憶媒体の数量、書き出しログと納品記録の三つを毎日チェックすることで、不正書き出しがないか確認している。
・個人データを取り扱う職場からの個人データ記憶媒体の不正持ち出しを防止するため、警備員による金属探知器を用いた検査を常時実施している。
・ポケットのない作業着着用による記憶媒体等の持ち出し防止を図っている。
・なお、同社グループではグループ共通の IC カード社員証を採用し、同社員証を利用したセキュリティゲートシステムを各拠点に導入している。またプリンター・コピー複合機の利用時に IC カード社員証による認証を行い、自分が出力指示した文書のみ印刷可能とし、出力紙の放置などによる情報漏えいを防止する仕組みを自社で開発、自社製品の活用を進めている。

④ノート PC の安全対策
・パソコン画面上の情報漏えい対策としてパソコン画面に装着する「のぞき見防止フィルター」を導入している。
・ノートパソコンは、社外持ち出し・構内持ち出し・持ち出し禁止を区別し、それぞれ別の色のシールを貼って容易に識別できるようにしている。
・持ち出し禁止ノートパソコンは、ワイヤーロックを行っている。
・社外持ち出し可能なノートパソコンは、必要最小限の情報持ち出しに留めた上で、念には念を入れて、ハードディスク全体暗号化をしている。

⑤外部委託先管理
・個人情報に関する業務を委託する際は、委託先チェックシートを用いて、評点化している。
・継続して委託する場合には、あわせて年に一度、委託先チェックシートによる再評点を実施している。
・個人情報の取扱いをグループ外に委託する際には、原則として本社情報セキュリティ本部が委託内容の審査を行う。

⑥日常点検・確認の方策
・同項「（4）個人情報の管理③盗難対策」を参照。

⑦初歩的ミスの防止策
・個人データ記憶媒体の受け取りは専門のセキュリティ便が行う。営業担当者が顧客先

に受け取りに行くことは禁止している。
・機密書類の社内間移送においては、主要拠点間で専門の施錠授受袋を導入している。

（５）個人情報の消去・破棄

・受託して管理している個人情報は全て消去又は返却する。
・保有期間は各部門によって異なる。金融機関を扱う事業部は、顧客の指示に基づいて返却していることもあれば、事業部内で 3 週間～1 ヶ月と決めている場合もある。
・顧客から要望があれば、部門長の名前で消去証明を提出する。
・廃棄の記録をとるように義務付けている。

（６）個人情報の監査

・監査法人とシステム会社など複数の企業に委託して監査を実施した。1 社ではなく複数機関から監査を受け、そのアドバイスを元に改善対策を行った。
・上述の監査とは別に、各事業部に対して個別監査が入る。例えば、クレジットカードの発行を受託している事業部は顧客各社による監査が入る場合がある。

（７）苦情処理・顧客対応

・次項「（８）事故発生時の対応」を参照。

（８）事故発生時の対応

※以下は、実際に発生した委託先内部者の犯行による漏えい事故（数百万件、氏名、勤務先、クレジットカード番号、保険証番号、保険料等）に関するテ社の対応記録に基づく。

（公表と再発防止策の徹底）

・事故判明後、個人情報保護に関する危機管理計画に従い、迅速に対策本部を立ち上げた。組織が一体となって対応を進めることが必要である。
・事実関係および再発防止策を速やかに発表できるようにすることが重要であり、そのためには、事故による影響範囲の特定、2 次被害の防止、徹底した原因究明と事故発生をリアルタイムに検知し漏えいさせない対策が必要である。具体的な再発防止策としては、カメラ監視や従業員教育の強化等の一般的対策の他に、個人データ記憶媒体を取り扱う担当者数を極少化して社員に限定、個人データ記憶媒体を取り扱うことのできるエリアを隔離し入退出時の警備員による金属探知検査、複数の企業による外部監査等を行っている。
・再発防止策をたてると共に、個人情報を取り扱う担当者全員への運用と教育を徹底し、維持継続している。

（コールセンターを立ち上げ、問合せ・苦情に対応）

・コールセンターは、情報統制上の観点から、コールセンター業務を行っているグループ会社に設置し、ピーク時は限定した社員による増員で対応した。

・事件発生から二ヵ月ほどでコールセンターへの問合せはほぼ無くなっている。

３．特徴的な取組について（※個人情報保護の体制を維持する上での評価や社内ルールの遵守の徹底のための方策など）

（「グループ行動規範」による企業倫理の定着・浸透）

・すべての社員が社会倫理に基づいた誠実な行動をとるために、グループ全体で遵守すべき基本的な事項を定めた「グループ行動規範」全 10 項のひとつに、個人情報保護を含めた情報セキュリティの確保を掲げている。

（印刷業界における個人情報ガイドライン・手引きの策定に参画）

・印刷業界団体の社団法人 日本印刷産業連合会による「印刷産業のための個人情報保護の手引き」・「個人情報保護 Q&A」・「印刷産業における個人情報保護ガイドライン」策定に参画している。これらは随時改訂されている。

以上