X. その他サービス業（印刷・広告）　X 社

事業概要	証券・カード、商業印刷、出版印刷、パッケージ、産業資材、エレクトロニクス、Ｅビジネス		
従業員数	約 11,000 人	プライバシーマーク取得	あり
保有個人データ件数	月間取扱規模 7,000 万件以上		

１．個人情報に関する概要

（１）保有個人情報件数、個人情報の種類、個人情報の利用目的

・月間取扱規模約 7,000 万件以上。毎月の取扱規模であるが、一定期間保管される。

・各業務によって扱っている個人情報は異なる。大半の個人情報は住所、氏名といった情報であり、機微情報は極めて少ない。

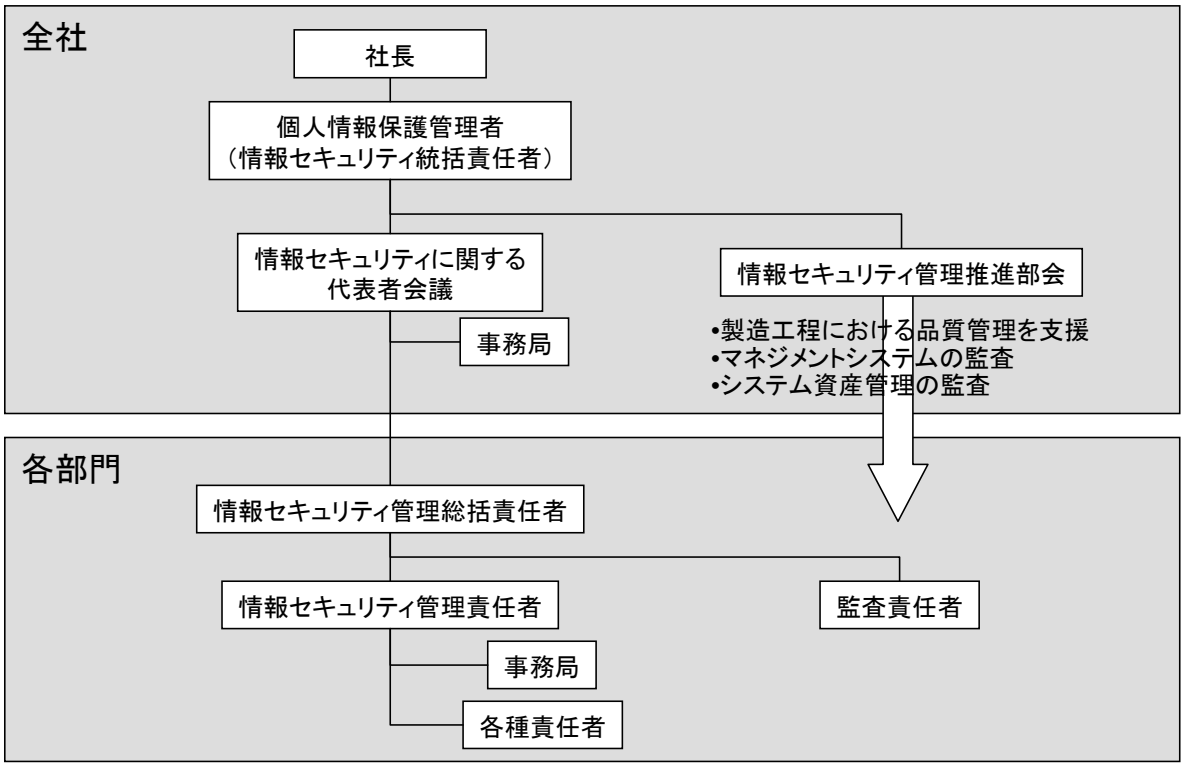
（２）個人情報保護担当部署

・事業領域およびエリアごとに事業部制をとっており、それぞれの事業部ごとに情報セキュリティ管理責任者を定め、事務局等を設けながら、事業部における計画・教育・運用・点検・監査・見直しなどの活動を推進している。

・同社では個人情報が一部署のみの処理で終わることはほとんどない。複数の部門での加工を経ることが大半である。複数の事業部にまたがる例も少なくない。このため、各工程の運用ルールは適正であるか、イレギュラーな事態にも対応できるか、事故を起こさないルールとなっているか、前工程でミスが発生しても次工程で発見し被害発生を食い止める仕組みになっているか、記録は残っているかについて確認する必要がある。また、独立し分散している生産系ネットワークやサーバもあることから、セキュリティ上の脆弱性をチェックし、ウイルス被害等による個人情報滅失事故を防がなければならない。この役割を情報セキュリティ管理推進部会が担っている。

・情報セキュリティ管理推進部会は、本社関連部署による横断的組織として構成されている。

図表　個人情報保護に係る組織図イメージ



（３）個人情報保護管理者の有無・位置づけ

・情報セキュリティ管理統括責任者として取締役が担当している。

・情報セキュリティ管理統括責任者は全社を代表する情報管理の責任者である。各事業（本）部においては、事業（本）部長に代表者としての権限を委譲する。

（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

・平成 12 年 3 月金融証券分野を担当する事業部が同社では初めてプライバシーマークを取得した。個人情報保護の先進事例として、かねてより情報セキュリティに積極的な同社が、JIPDEC の要請も受け、業界内で率先的にプライバシーマークを取得した。以後、全社の各事業部でプライバシーマークの取得を進めた。

・平成 18 年、JIPDEC の要請のもと、全社として統一的なプライバシーマーク取得を行うこととした。平成 19 年 8 月現在、全社統一のプライバシーマーク取得の現地審査済みである。

・同社の子会社についてもグループとしてあるべき姿を示すため、プライバシーマーク取得を勧めている。

・個人情報を取り扱うエリアにおける安全管理レベルを担保するために、ISO/IEC2700 に準拠した ISMS 認証取得を推進している（平成 21 年度時点で 20 エリア）。

（５）個人情報保護に向けた取組経緯

・同社では平成 3 年 5 月に情報リスクマネジメント活動として「秘密情報管理規程」を制定。平成 11 年 2 月に「個人情報保護方針」「個人情報管理規程」制定を行った。
・平成 11 年には金融・証券事業部がプライバシーマークを取得した。
・平成 16 年 10 月に本社の横断的組織として個人情報管理推進部会（現情報セキュリティ管理推進部会）を設置した。プライバシーマーク取得だけでなく、WEB 管理、ホームページ作成等での個人情報管理についても対応を決定した。
・印刷、加工、データ処理におけるケアレスミスが漏えいにつながることから、生産工程でのオペレーションの品質向上を行った。
・品質管理として、生産現場への監査や協力会社の認定も行った。以後、継続して全国の工場や協力会社を回り、品質管理の向上や個人情報保護意識を高める教育につとめている。
・平成 20 年 10 月、21 年 4 月と「ヒヤリハット事例集」を発行し、IT 利用におけるヒューマンエラーによる紛失・盗難事故等の注意喚起を促し、全社教育での周知徹底を図った。
・平成 21 年度から、独立し分散して稼動している生産系のネットワークやサーバにおける脆弱性による情報滅失事故等を防止するため、情報セキュリティ管理推進部会および関連技術部門によるシステム資産監査を実施した。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・印刷業界は顧客から仕事を請け負う業態がほとんどである。顧客あってこその仕事であり、その顧客があらゆる業種にまたがっているため、関係する管轄省庁やそのガイドラインも多岐にわたる。そのため、かなり幅広く多方面に目配りをしておかなければならない。
・そして、個々の個人情報取扱業務は、それぞれに多くの工程を抱えながらも、“一品一様”で、その仕様変更も作業中であるか否かを問わずに発生するという、要求に応えなければならない。
・印刷業界では、多くが規模の小さい中小企業である。そのため、新たな管理者を育成したり、個人情報保護に特別なコストをかけたりするのが難しい場合もある。
・外部協力会社に対する品質管理の指導はもちろんのこと、業界全体に対しても、同社が指針めいたものを提供し、指導的な立場で業界に寄与できればと思っている。ここ 2 年間、印刷業界のガイドラインや Q&A の制作、講演会、説明会など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）

・当初のプライバシーマーク取得にあたっては、JIS 規格のみでは社内に適切に当てはめるノウハウが無かったため、コンサルティングを活用した。

・平成 16 年 10 月に本社の横断的組織である個人情報管理推進部会が開始した。毎週定例で集まって打合せをしている。新制度の社内への説明、ISO との整合性、事故対応、業務の増加による対応等について話をしている。

・事業部との会議は毎月開催されるので、2～3 ヶ月に 1 回は個人情報関連についても会議を持っている。

・情報セキュリティ管理責任者による会議は、以前は個人情報と情報セキュリティについて分けて会議をもっていたが、現在は包含して行っている。

（２）個人情報の取得

（WEB サイトで個人情報を収集する場合本社承認が必要）

・同社自らが取得する情報としては、WEB サイト関係のものが多い。平成 14 年には WEB サイトで個人情報を取得する場合には、本社承認を義務付けた。サイトのプライバシーポリシーや個人情報の利用目的については、本社申請書類の中に記載するよう義務付けている。利用目的の表現が曖昧であったり偏りがあったりする場合には、修正するよう指導している。

（３）個人情報の利用（第三者提供を含む）

・委託元からの預かりデータについは事業部と製造子会社間で処理されているが、両者の関係は委託関係であるので、共同利用はしていない。

・共同利用の課題は従業者情報である。従業者情報は、労務管理、福利厚生、社会保険庁への申請などで利用するとしているが、労務管理の延長線上で、グループ会社との人事交流のために利用される場合もある。異動が関係する事柄であるため、本人の了解を得ることは現状ではしていない。

（４）個人情報の管理

①情報の管理体制

（データの授受は手渡し又はセキュリティ便を利用）

・外部とのデータの授受において、手渡し又はセキュリティ便を利用している。

・工場間など社内でのデータの授受では、鍵つきジュラルミンケースで運ぶ個人情報専用便を利用している。

・データのやり取りは専用伝票で記録しており、受け取りから返却又は破棄までが管理

できるようになっている。

（個人情報取扱エリアを特定し、業務を集中化）

・全国にある個人情報を取り扱う業務を、それぞれの事業所のセキュリティエリアに集中させている。同エリアでは、他のエリアと物理的に切り分け、作業者を特定・極少化し、許可された者以外の入退管理を厳密に行っている。

・作業はセキュリティエリア内のみで行うことにしており、作業中に想定し得るケアレスミスに対し、事故発生につながらないような工程ルールの適正化・標準化・教育・運用（記録・点検・監査）の徹底を行っている。

（平成 19 度からは、個人情報取扱エリアからの悪意の持ち出し防止のための対策を実施）

・セキュリティエリアを、業務内容・個人情報の内容・量などからリスクレベルを設定し、グループ化

・リスクレベルに応じた管理策を ISO/IEC 27001、ISO/IEC 17799 より選択し、ルール化

（ア） グループ 1（高度なセキュリティエリア）

－メール、インターネット、イントラネット等社内ネットワークから分離

－ISO/IEC 27001 の認証取得を前提に情報セキュリティマネジメント（ISMS）を構築

（イ） グループ 2

－ISO/IEC 27001 の 133 項目の管理策の中から悪意による持ち出し防止対策として必要十分な項目を取り上げ、具体的管理策として実施

（ウ） セキュリティエリア共通

－振り分けられたアクセス権限（閲覧・加工・出力）の集中管理システム、ログオン製品、不正操作検知システム、不正な媒体作業を拒絶するシステム、作業ログから不正操作をバックトレースできるシステムの導入

（エ） ファミリー会社に対して当社レベルの個人情報取扱ルールを徹底

－社内規定の対象者にファミリー会社も含み、社内として扱っている。

②従業者への教育方法

（協力会社や外部スタッフに注力した研修を実施）

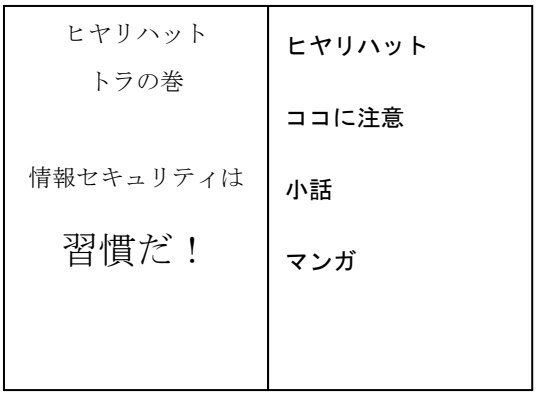
・本体企業よりもファミリー企業もしくは製造子会社、スタッフよりもライン従事者、社員よりもパート・アルバイトにおいて、個人情報を含む情報取扱いのルールの認識が薄まることが無いように、平成 21 年度は、教育方法を対面方式に切り替え、のべ 200 回にのぼる徹底した集合教育を実施し、情報セキュリティ管理の重要性の理解を求めた。

・教育内容としては、「社会の信頼に応えることの重要性の周知」「ヒヤリハットなどヒューマンエラーの注意喚起」「USB メモリの適正利用・PC 利用時のパスワード定期変更など IT サービス利用時のルール徹底」「個人情報を含む高いセキュリティを求められる業務の注意喚起」などを柱とし、約 1 時間の講義とともに、確認テストを実施した。

（日常業務におけるヒューマンエラー防止のための小冊子発行）

・平成 20 年 1～2 月に、手違いによる事故を発生させたことから、日常業務におけるヒューマンエラーを防止するべく、想定される事例を洗い出し、同年 10 月および平成 21 年 4 月の 2 回に分け『ヒヤリハット　トラの巻』を発行した。
・「電子メールという危険」「電話という危険」「FAX という危険」「パソコンを安全に使おう」「身の回りを安全に」「委託先とのコミュニケーション」といったテーマ別に約 40 件の事例をイラスト付きでまとめた。
・前記の集合教育で触れるとともに、職場ごとのミーティングの際に、コンプライアンス推進リーダーを中心として全員で復唱するなどの展開を図っている。

図表　「ヒヤリハット　トラの巻」のイメージ



（内部監査員の育成研修を実施）

・平成 19 年度より、情報セキュリティマネジメントシステムを確実に回していくために、各事業部におけるリーダーを育成するべく、ISMS 審査員補もしくは内部監査員補等の有資格者養成研修を積極的に実施している。平成 21 年度の研修をもって、100 名体制を実現した。

③盗難対策

・印刷会社の体質として情報セキュリティ意識は高く、今までに大きな事故はない。
・扱う情報によっては、カメラ付携帯電話の持ち込み禁止、持ち物チェック、ポケットのないつなぎ服の着用を実施している部署もある。

④ノート PC の安全対策

・モバイル用ノート PC は暗号化している。

⑤外部委託先管理

（協力会社に対して独自の認定制度を導入）

・委託については、宛先に合わせた内容の送信を行うダイレクトメールに関しては、再委託先を、社内と同程度のセキュリティを確保していると認めた認定協力会社に限っている。認定のための検査は半日程度の立ち入り視察で実施している。現在全国で十数社が認定会社となっている。認定先については今後も増やしていきたい。現在は、個人情報管理に厳重を要する特定業務に限ってこのような取扱いにしている。

・委託先の中には、セキュリティ確保のために立ち入り検査に応じられないというケースもある。その場合、同社の作業をしているときに立ち入り検査をさせてもらうよう依頼する。

・委託先には取引基本契約書、個人情報保護についての覚書を交わしている。

（派遣社員からは直接誓約書をとらずコピーで対応）

・派遣社員からは直接の誓約書を取ることなく、派遣会社がとった誓約書等のコピーで対応している。

・派遣社員、パート、アルバイトでも個人情報を取り扱う場合は、すべて教育の対象である。テストやアンケートで受講状況をチェックしている。

⑥日常点検・確認の方策

・各工程の点検・確認方法を独自のノウハウ集にまとめ、その内容を毎日指差呼称することで周知徹底をはかっている。このノウハウ集は、正社員・派遣社員・パート社員を問わず当該作業に従事している担当者全員から作業上のノウハウや注意事項などをブレストで出してもらい、それをリーダーやマネージャーがルールとしてまとめたものである。機械メーカや上からの押し付けルールではない、地に足の着いたルールなので高い効果をあげている。

⑦初歩的ミスの防止策

・初歩的ミスの防止の 1 つとして例えば、誤封入をなくすため、封入は 2 人以上でチェックするようにしている。この場合 1 人目の封入形態と 2 人目の確認後の封入形態を変えることにより、確認漏れを無くす工夫をしている。

（５）個人情報の消去・破棄

・以下の方法を紹介し、復元不能な処理の徹底を励行し、及び記録を残すようにしている。

(a)コマンド処理による消去（主に WS の HD 上のデータ）

(b)証明書発行機能付き専用ソフトによる消去（主にパソコンの HD 上のデータ）

(c)上書き及びフォーマットによる消去（主に電子媒体上のデータ）

(d)物理的破損（主に電子媒体）

（６）個人情報の監査

（監査は異なる部門の監査担当者が複数で実施）

・各事業部内に各種責任者（法令及びその他の規範調査、教育、苦情及び相談窓口、委託契約内容確認、委託業者管理）と監査責任者をそれぞれ任命している。

・日本情報処理開発協会（JIPDEC）によると監査には客観性が求められ自部門の監査ができない。しかし、同社の業務内容は多様であり、監査を受ける部門の業務内容にある程度通じている者が監査に入らなければ、業務内容が分からず適切な監査ができない。そのため、同社では監査を受ける部門に近い部門に所属する監査担当者とそれ以外の部門の監査担当者が複数で監査している。

（監査手法をとった品質指導を実施）

・監査手法で品質事故防止のための指導をしている。従来は「品質事故」とされていたものが、「個人情報保護法違反」になるケースがあるため、品質を向上させることは個人情報保護の推進にかなうもので、重要であると考えている。

・この監査は、書類が整っているかどうかだけの監査ではない。品質管理の担当者が現場に出向き、1 部署あたり最大 15 人日ほど実際の作業に立会いながら個人情報の管理方法をチェックするものであり、製造実務に係わる監査である。例えば品質保証のルールとその遵守状況、機械停止時の操作、目の動き、ゴミ箱の形、服装、といった細かいことまでチェックし、不適切な点があればその場で指導する。

・協力会社に対しても監査を毎年 1 回行っている。結果によっては認定の取消をする場合もある。

・また、従業者、パート、アルバイトにアンケートで、現在実施している作業の中での不安や工夫している点を聞き、監査項目を抽出した。

（情報セキュリティマネジメントシステムを回すための監査等を複層的に実施）

①事業部内の内部監査

②事業部が行うファミリー会社、協力会社への監査

監査ツールを複数タイプ整備し、委託先の規模やプライバシーマークの取得の有無に応じて監査を実施

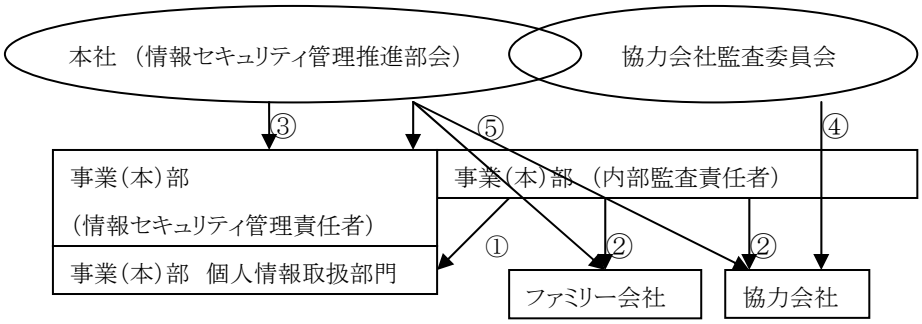
③本社（情報セキュリティ管理推進部会）が事業部に対して行う内部監査

事業部の推進役を担う事務局のみにとどまらず、総務部門・生産管理部門・情報システム部門も含め、事業部全体のマネジメントシステムについての監査を実施するとともに、独立・分散している生産系ネットワークやサーバの管理状況に対して、本社の生産系技術員によるシステム資産監査を実施

④協力会社監査委員会が行う協力会社への監査

⑤本社の品質管理部が総合品質保証の観点で行う、事業部・ファミリー会社・協力会社への監査

図表　監査関連図



（監査の実効性を高めるための従業員への事前アンケートを実施）

・平成 18 年度以降毎年継続的に、監査時の回答と実態とのギャップ、サンプリングによる問題点の見落とし等の問題を解消するため、被監査部門の従業者（派遣社員等を含む）から、日常的な管理運用に関する事前アンケート調査を実施している。

・多岐にわたるアンケート項目により、評価軸に照らして管理レベルを視覚的に捉えられるだけでなく、管理者と一般層に分けることによって、そのギャップを捉えることも可能となった。

・監査員が被監査部門の業務内容に精通していない場合であっても、同アンケートが運用状況を指摘する上で有力な監査ツールとなった。

（７）苦情処理・顧客対応

（受託案件の問合せは委託元へ報告）

・問合せに対しては、受託案件についても受け付けている。本人が、同社で個人情報を

処理していると知っていて、問合せをしてきた場合には、事実関係を調査し、委託元へ報告する。委託元に無断で開示することはない。ただし、通常の委託案件で同社の関与が一般消費者にわかることはほとんどない。

（８）事故発生時の対応

・事故を起こした本人は行動指針に反するものについては処分の対象となる。過去に本人処分があった際には、本人を処分したという情報を全社へ通達した。これによってどのような行動が処分につながるか従業者に分かり注意喚起につながると判断したためである。

・事故については、一通の漏えいでも JIPDEC に報告している。社内でも同様である。事故かどうかは本社で判断するので、どんなことについても申請するよう指導している。

（９）その他

・グループ会社と連携し四半期に一度の推進会議を開催し、各社の取組みの進捗状況をチェックしている。主要なグループ会社とは、さらに毎月 1 度程度の交流会を実施している。過失事故撲滅のための具体的手法や教育・監査手法などについての情報交換、および製造現場管理の相互視察を行っており、大変有効である。

以　上