

I. 信用業 I社

事業概要	クレジットカード、ファイナンス		
従業員数	約 3,700 人	プライバシーマーク取得	あり
保有個人データ件数	約 2,730 万件		

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

- ・カード有効会員数：約 2,530 万人
- ・ローン有効会員数：約 200 万人
- ・役職員情報：約 3,700 件

(2) 個人情報保護担当部署

- ・情報セキュリティ管理部
- ・個人情報保護に係る業務に従事する従業者は 31 名（専任）

(3) 個人情報保護管理者の有無・位置づけ

- ・個人情報保護総括管理者（情報セキュリティ管理部担当役員が就任する）
- ・個人情報保護監査責任者（内部監査部長が就任する）

(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

- ・ISO27001（ISMS）認証基準（平成 15 年）
- ・プライバシーマークを取得（平成 17 年）
- ・取得理由：①個人情報の安全管理スキルの向上が図れる、②取引先等からの要望、③他社との差別化、④安心の提供と信頼の獲得
- ・効果：①個人情報保護のハイレベルの指針とできる、②外部監査的な検証を受けられる

(5) 個人情報保護に向けた取組経緯

- ・平成 13 年 4 月に個人情報保護全般に係る統括・指導の主管部署として、個人情報部を創設。同年、業界自主ルール等に準拠して「個人情報保護方針」「個人情報保護規程」を制定。
- ・平成 15 年 4 月よりコンプライアンス統括本部傘下に組織変更。
- ・個人情報保護の文書体系と組織体制を整え、PDCA の取組を始め、平成 17 年 4 月にプライバシーマーク認証取得を申請し、同年 9 月 15 日に認証取得。

- ・平成 18 年 10 にコンプライアンス統括本部傘下より、情報資産リスク全般を所管する「情報セキュリティ管理部」として独立。
- ・平成 19 年 1 月に「個人情報保護規程」等の現規程類を JISQ15001：2006 版に準拠し改定。

(6) 個人情報の保有・管理・提供等に関する業界の特徴

- ・与信事業者であり、個人信用情報機関に登録又は提供を受けている「個人信用情報」を取り扱っている。
- ・平成 13 年から“自主ルール”の制定作業を通じて、個人情報保護に取り組んでいる。
- ・自主ルール運営協議会（現 CPIP）の他、日本クレジット産業協会、日本クレジットカード協会等、各業界団体においても独自に個人情報保護に取り組んでいる。

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）

(本社と支店等との分権)

- ・全社的には個人情報保護に関する専任組織が、規程類の整備や教育指導、管理を行っている。各部・支店単位においては各組織長及び次長が、個人情報保護責任者及び個人情報保護代行者となって管理下の組織における個人情報保護に係る業務を管理している。

(2) 個人情報の取得

- ・個人情報は、加盟店が店頭においてカード入会申込を受付する場合と、個人が郵送で申し込んでくる場合がある。
- ・カードの提携先は 1,000 社あり、それぞれの利用目的が少しずつ異なるので、明示する利用目的の文面もそれぞれにあわせて変えている。

(3) 個人情報の利用（第三者提供を含む）

- ・保有個人データの利用目的、共同利用する関連信販会社等を「プラバシーポリシー」と共にホームページ上に公表している。

(4) 個人情報の管理

①情報の管理態勢

(“三点セット”による入退室管理)

- ・コールセンターや事務センターといった個人情報を取り扱うことのできる部署において

は、指紋認証、監視カメラ、個人私物ロッカーの“三点セット”を用いて、入退室管理を行っている。

(バーコードによるトレーサビリティ確保)

- ・ 個人情報を含む書類等の授受は、自社開発したシステムを活用して、バーコードによる追跡（トラッキング）ができるようにして管理している。これによって、リアルタイムで書類等の所在が確認できる。

(システム上の安全管理)

- ・ 重要な情報が集中する「システムセンター」では、情報セキュリティの標準規格である「ISO27001 (ISMS)」の認証を取得している。また、専管するチームを設置し、技術・設備・運用の各面から安全管理に努めている。

②従業員への教育方法

(毎月全部署で勉強会を実施)

- ・ 毎月、全部署において、コンプライアンス定着のための勉強会を開催・実施しているが、個人情報保護に係わる項目を勉強会テーマとして定期的に取り入れ、個人情報保護責任者である組織長が中心となって個人情報保護について周知している。
- ・ テーマ及び資料は個人情報保護担当部が作成して各部署に配布している。勉強会においては、資料を参加者が交代で読み上げたり、理解度テストを実施したりして内容の理解を深めるよう促している。
- ・ 勉強会に要する時間は 30 分～1 時間程度である。

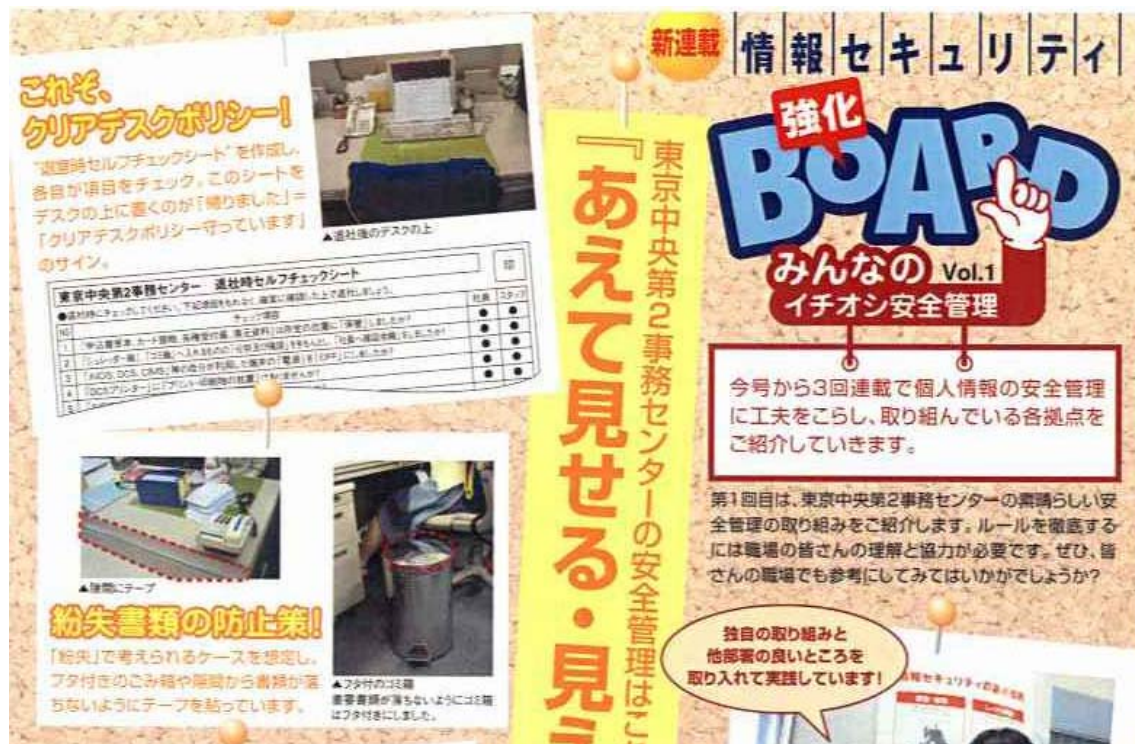
(半年に一度の e ラーニング)

- ・ 個人情報保護の定期点検として、全従業員に対し半年に一度、e ラーニングを用いたテストを実施している。テストは 15 問で、10 分程度で回答できる。また、テスト結果は前述の勉強会のテーマ検討に活用されている。
- ・ テスト問題は、個人情報部が作成している。

(社内報における解説)

- ・ 社内報に紙面を確保し、個人情報保護に関する各拠点の取組みや好事例を紹介している。キャラクターを用いて、簡単にできるセキュリティチェックも実施させている。

図表 社内報のサンプル



③盗難対策

- ・監視カメラ、指紋認証による入退館管理の強化、業務端末の書き出し制限とログ取得、データ授受の電磁媒体から伝送化へ移行など取り組んでいる。

④ノート PC の安全対策

- ・ノート PC は営業プレゼン用のみとして、原則社内への持ち込みを禁止している。

⑤外部委託先管理

(年に1回以上の定期検査の実施)

- ・委託業務ごとに、年に1回以上の定期検査を実施している。
- ・担当部署においてチェックシートを使用したリスク評価を実施し、必要に応じ業務の見直しや委託先への改善指導を実施している。

(個人情報の取り扱いを伴う業務を委託している業者に対する立入検査の実施)

- ・個人情報を取り扱う業務を委託している業者（印刷会社等）に対しては、委託先の作業場所単位での立ち入り検査を実施している。
- ・検査ツールは委託先による自己評価シートと、自己評価シートの回答結果を現地で検証するためのチェックシートの2種類を使用する。

- ・シート内の各設問は点数評価（3点～1点）を行い、1点の項目がある場合は委託できないこととしている。

⑥日常点検・確認の方策

- ・「部店内検査手順書」を半期ごとに配布し、全部署において個人情報責任者が中心となって、毎月、点検を実施し、その結果を報告することとしている。

⑦初歩的ミスの防止策

- ・トラブルデータベースを作成し、誤 FAX 等の事務ミスについて、全社において情報共有している。なお、トラブルの内容は、月例のコンプライアンス委員会に報告・検討・改善指示がされる。

(5) 個人情報の消去・破棄

- ・専門の倉庫業者に保管・廃棄を委託して、独自のシステムを構築している。

(6) 個人情報の監査

- ・個人情報保護監査責任者を定め、その下で内部監査部が、全部署の監査を年1回以上実施している。

(7) 苦情処理・顧客対応

- ・開示手続の規程や、執務の基本姿勢を定めた「コンプライアンス・マニュアル」を策定して対応している。

(8) 事故発生時の対応

- ・トラブル管理規程、危機管理規程、情報漏洩対応基準を定め、経営層にすぐに伝わる態勢を整えている。

以上