M. 情報サービス業（ソフトウェア）　M 社

業務概要	情報サービス（ソフトウェア）		
従業員数	約 2,000 人	プライバシーマーク取得	あり
保有個人データ件数	約 16,000 件（預託データを含まず）		

１．個人情報に関する概要

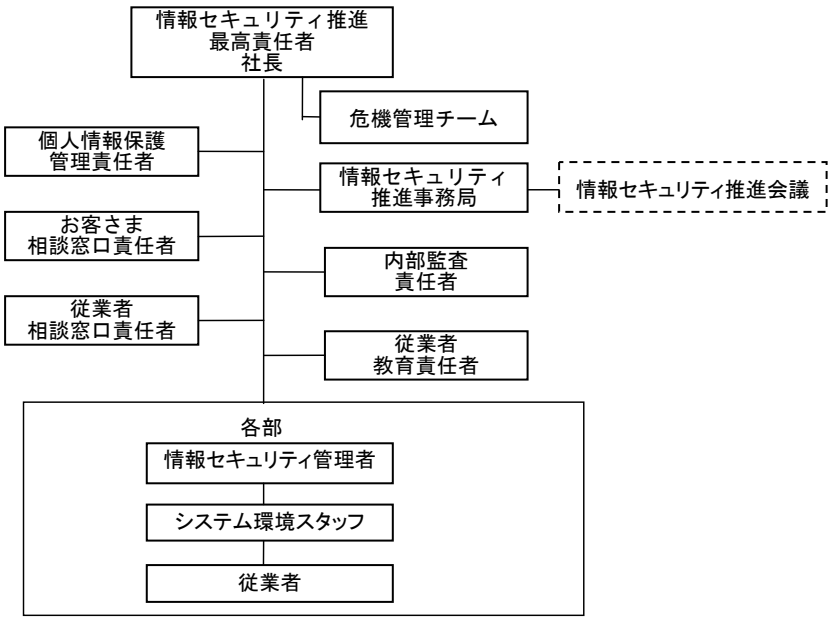
（１）保有する個人情報の件数、種類、利用目的

・独自に収集した顧客情報が約 13,800 件であり、個人向けサービスの運営管理のため、住所、氏名などの他に振込先情報を保有している。
・法人向けサービスの運営管理のため、会社名、部署名、氏名、会社所在地、会社連絡先といった名刺のデータを保有している。
・従業員従業者情報として約 2,200 件程度の情報（出向者を含む）を保有している。
・その他、同社の親会社からの預託情報が約 3,000 万件であり、個人情報は、顧客の住所、氏名、連絡先、利用料金である。同社は親会社から委託を受けて顧客のデータ管理を行っている。

（２）個人情報保護担当部署

・情報セキュリティ推進事務局を総務部が担当している。

図表　個人情報保護も含めた情報セキュリティ全体についての推進体制



（３）個人情報保護管理者の有無・位置づけ

・取締役が個人情報保護管理者となっている。

（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

・プライバシーマークは平成 11 年 2 月取得。

・同社はシステムの開発・運用・利用者サービスなどを通じて非常に多くの個人情報の預託又は収集を行っており、適切に管理することが重要な社会的責務であると考えた。認証を得ることにより、日常業務における個人情報の取扱レベルを客観的に判断できること、こうした認証が業務を受託する要件の一つになりつつあることが理由である。

・早期にプライバシーマークを取得した理由の 1 つは同社が JISA の理事会社であり、プライバシーマークへの理解が早かったことがあげられる。

・ISMS は平成 15 年 3 月取得。

・顧客の信頼を得、それを維持していくためには情報セキュリティの確保が不可欠である。そのためにはシステムとして組織的な管理が必要と考え、ISMS の取得を行った。

（５）個人情報保護に向けた取組経緯

・平成 10 年～11 年にはプライバシーマーク制度の発足に伴う認証取得に向けた取組を行った。

・以前から預託情報に対する保護対策を実施しており、プライバシーマーク認証に向けてそれらの対策を規則として成文化するとともに、それらを自社データの保護対策にも準用するなど必要なルールの追加、見直しを行った。

・平成 14 年～15 年には ISMS の認証取得に向けた取組を行った。

・関連会社との合併による新体制のスタートに併せ、新制度の認証取得に向けた規則見直し、体制整備を実施した。

・平成 16 年～17 年：個人情報保護法施行に合わせた取組を行った。

・経済産業省のガイドライン、JISA のガイドラインに沿った規則・マニュアル等の見直し、例えば、委託先に係る規則の制定や説明会の実施、定期的な社員教育の体制整備等、法の遵守のための取組を実施した。

・平成 17 年 3 月に顧客からの申込依頼書約 50 枚を紛失した（本件の担当部署は現在、別会社となっている）。同社はプライバシーマークを早期取得し更新を続けていたが、この事故のため、再発防止策として、個人情報の総点検、取扱方法の再徹底を行うこととした。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・個人情報は、①親会社からの預託個人情報がほとんどであり約 3,000 万件、②事業のため独自に収集したもの 13,800 件、③その他名刺情報や従業者情報（約 2200 件）と

なっている。①については親会社からの指導のもと保管管理等については厳正な取扱いを行っており、②、③については、独自に規則等を制定し管理している。
受託業務における親会社等からの指示・指導による面と自主的に情報管理を実施する両面を有している。

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）

・平成 11 年にプライバシーマークを取得したときには、特にコンサルティング会社に依頼せず、社外研修等に参加し規程・体制づくりをした。
・ISMS 取得の際は、コンサルティング会社へ依頼した。

（２）個人情報の取得

・親会社である委託元から預託されるデータについては、親会社に設置した端末へ入力されたデータが直接同社のデータセンターへ記録されるシステムとなっている。
・法人顧客情報は展示会等で収集する場合が多い。展示会では、利用目的を明示したアンケート等を用意し、個人情報の利用について同意を確認するようになっている。展示会等で利用する文面は、概ね同様な文面を利用している。

（３）個人情報の利用（第三者提供を含む）

・展示会で収集した情報は商品ごとに管理し、ダイレクトメール発送などの営業活動に利用している。
・個人情報保護法施行以来、グループ会社内でも個人情報の共同利用は行っていない。

（４）個人情報の管理

①情報の管理体制

・預託された個人情報をプリントアウトした用紙は、指定された委託元事務所へ送付している。送付時には重要情報輸送の特別契約をした配送事業者（グループ会社）を利用している。
・会社の情報の自宅への持ち帰りは禁止しているが、やむをえない場合は管理者の承認を得、証跡を残して持ち帰ることが出来る。自宅での作業は貸与された持ち出し用パソコンを利用している。
・携帯電話は会社から貸与し、遠隔操作でデータの消去ができるようになっている。また、携帯電話を持ち出して利用する場合には、必ずパスワードをかけることを指導している。

・自宅のパソコンについては残存業務情報の有無について自己チェックを実施した。自宅のパソコンは家族で共有している人もおり、いつファイル交換ソフトがダウンロードされるかわからないため安全とはいえない。したがって、自宅のパソコンは「業務の使用を禁止する」ルールを定めた。

②従業者への教育方法

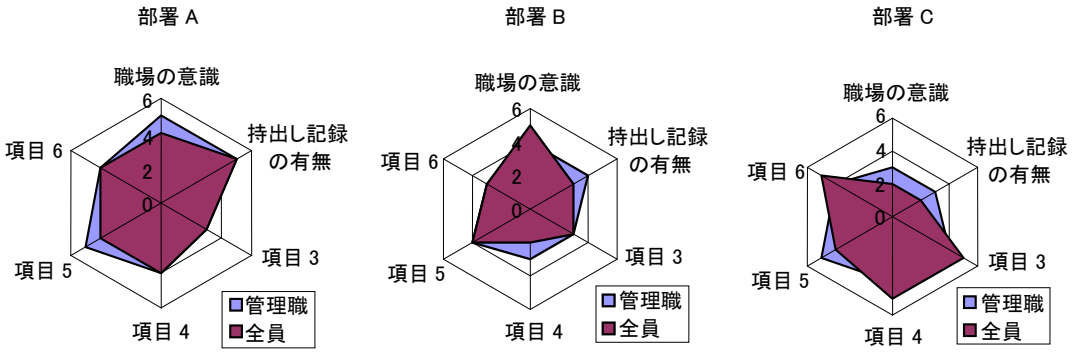
（毎月１７日に総点検を実施、各職場の実態を洗い出し報告）

・平成 17 年 3 月の紛失事故をうけ再発防止策を実施するとともに、平成 17 年 4 月から情報セキュリティ充実のための対策として、毎月 17 日に個人情報等重要情報総点検を実施、以降取組中。

・平成 17 年 3 月～4 月に要しての総点検内容は、個人の意識レベル、情報共有、情報の取扱ルール、情報の廃棄、情報の社外持ち出し、私物記憶媒体の持ち込みなどのルールに対しての職場の実態（管理者がチェック）、と各個人の実態（全員がチェック）を別々に行い、職場ごとに従業者の実態、管理者が見る職場の実態等を整理した。こうした点検を同年 9 月まで繰り返し実施することで意識やルール遵守の向上を目指した。この取組によって、従業者の情報セキュリティに対する意識が高まり、ルールで決まっていない具体的な対応方法について問合せが増えたため、毎月の会議（社長が議長の情報セキュリティ推進会議）で情報セキュリティの管理ルールの細分化や補充を行った。

点検結果は、すべての点検部署の特徴が出るようにレーダチャートで表示し幹部が参加する情報セキュリティ推進会議で発表した。点検後の会議では各部署において得点の低い回答項目等が話題になり、各部署の責任者は改善の検討を進めることとなった。同じ点検を繰り返すと慣れが出てくること、ある程度までは上がるがそれ以上あがらないものも出てくるため半年で終了した。

図表　チェック結果のレーダチャート（イメージ）



（セキュリティ遵守事項を定め、定期的にチェック）

・平成 17 年 3 月以降に決定されたルールを取りまとめ、整理し、これらの遵守状況のチェックを平成 17 年 10 月から半年間の総点検項目とした。チェックは部署内で実施された。

（セキュリティ規則を守っていない従業者を対象に個別事情等をヒアリング）

・平成 18 年 4 月からの総点検の内容は、今まで取り決めたルールを規程化し、このうち 15 項目を質問の形にして 4 月と 6 月の 2 回の総点検で遵守状況について自己チェックした。4 月時点では項目の 1 つ以上を守っていないとした人が延 300 名～400 名おり、職場の長と各人とが面接し、改善を促した。6 月時点の再度の自己チェックでは、延 190 名に減少、190 名を対象に情報セキュリティ推進会議事務局で実態のヒアリングを実施した。ヒアリングを行うことで、事務局と各人の相互理解が増すなどのメリット（誤解が解けるなど）がある。

（年 1 回全社で e ラーニングを実施）

・年 1 回全社で e ラーニングを実施している。テストも同時に実施しており、合格するまで何度でも回答しなければならない。テストは、プライバシーマーク関連の質問 10 問、ISMS 関連の質問 10 問である。
・テストも含んだ受講時間は約 1 時間である。断続的に受講できるシステムとなっている。テスト結果の公表はしていない。
・組織長に対し、受講率を提示し、期日迄の全員の受講を促す方法で実施している。
・受講者は、経営幹部、従業者（派遣社員、パート、アルバイト含む）を対象としている。
・e ラーニング以外は、新入社員研修で 3 時間程度、親会社からの出向者対象に 1 時間程度教育を実施している。

③盗難対策

・私物の USB メモリの利用は禁止し、会社貸与のパスワード付 USB メモリを導入している。
・システム開発作業用の開発 LAN と一般事務作業用の事務 LAN を分離し、開発作業を委託しているパートナーは原則として事務 LAN に接続させないこととした。
・開発 LAN からの、メール発信、インターネット接続は申請により許可された相手先のみとした（ホワイトリスト方式）。
・開発 LAN 事務 LAN ともに、メール発信やデータの外部出力時は暗号化し外部とのデータ入出力の記録を採取するツールを導入した。

④ノート PC の安全対策

・個人所有のノート PC の持ち込みや業務での利用は禁止しており、業務用途では会社からノート PC を貸与している。
・持ち出し用ノート PC は約 300 台保有しており、貸し出しについては各部署で台帳管理している。
・ノート PC は暗号化ソフトを利用しパスワードをかけている。

⑤外部委託先管理

・外部委託先に個人情報を提供することは原則として行っていない。当社の提供するサービスを利用するお客様に対して、契約等の際に得る個人情報等に関しては、原則として郵送頂くなどの配慮をしている。

⑥日常点検・確認の方策

・各部署は、規則で定めた方法で運用管理している。例えば、個人情報や重要情報に関しては、社外へ持ちだす場合は、管理者の承認を得ると共に、持ち出しの証跡を残している。また、こうした実態にあるかどうかを毎月 17 日の総点検日で確認を行っている。

⑦初歩的ミスの防止策

・重要な紙情報の持ち運びについては、組織長の承認と証跡を残すことで緊張感を持つような配慮をしている。また、昼食時の置き忘れには注意するよう呼びかけている。
・必要な箇所では鍵付の専用カバン等を利用している。また、運搬など定期的な情報のやり取りでは、施錠つきのジュラルミンケースを利用するなどの安全措置を実施している。
・電子メールの添付ファイルで個人情報等重要情報を送信するときには、パスワード設定を義務付けている。

（５）個人情報の消去・破棄

・法人顧客の情報は 2～3 年で古いものになるため消去し、ダイレクトメール等には展示会で収集する新しい情報に対してのみ送付している。
・情報の廃棄には注意を払っている。情報によっては廃棄されたことが証明できなければ紛失であり重大事故となる。前述の紛失事故が発生した際、新しい管理策が定着するまでの間、紙ごみすべてを一定期間事務所内に保管し、一業務サイクル経過後廃棄するなどの措置を講じた（情報の出入りをすべて抑えることで安心した業務運行となる）。

（６）個人情報の監査

・委託元である親会社の監査組織からの監査が定期的にある。委託元である親会社からは委託内容について細かい作業内容が指定されている。そのため、監査では、作業途中の経過が指示通り行われているかどうかもチェックされる。立ち入り監査も必要に応じ実施される。

・プライバシーマークと ISMS の内部監査はそれぞれ年 1 回実施している。業務監査の部署が担当している。

（７）苦情処理・顧客対応

・相談窓口は営業総括部長が担当している。現状までで問合せは 2 件程度である。開示請求は 1 件もない。

（８）事故発生時の対応

（個人情報漏えい事故対策訓練を実施）

・平成 18 年 11 月に漏えい事故を想定した訓練を実施。個人情報漏えい事故の発生を想定し、緊急対策本部を設置し、顧客からの問合せ窓口や営業対応、報道対応などを訓練する。訓練は事前に各部署に連絡し、協力を得る。

・事故時の対応については規程で決まっている。事故が発生することは望ましくはないが、いざという時に社内的な混乱を起こさないようにしたい。

（９）その他

・グループ会社の IT 担当者で構成される研究会のメンバーで「情報セキュリティはじめの一歩」という冊子を作成し、グループ会社全員へ配布した。

図表　情報セキュリティに関するハンドブック（抜粋）

以　上