N. 情報サービス業（ソフトウェア）　N 社

事業概要	ソリューションサービス、ソフトウエア開発、 クレジットデータ運用処理サービス、健康関連サービス		
従業員数	約 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 200 万件		

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

・保有する個人情報は、決済情報、会員情報、顧客情報及び社員情報等である。

・運用処理サービスと会員サービスの提供及びビジネス情報の案内に利用

（２）個人情報保護担当部署

・品質保証部が活動組織の事務局を担当し、事業部門に部門管理責任者を設置している。

（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は専任の役員である。

（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

①平成 14 年 5 月プライバシーマークを取得した。

・運用処理サービス及びパッケージソフト等を提供するにあたり、個人情報保護の取組を発信する必要性が生じたため、プライバシーマークを取得した。

・平成 14 年の取得は業界では早い方である。取得時点ではクレジットカード会社などの業務委託元からの要請はなかった。

②平成 17 年 ISMS を取得した。

・安全で確実な情報セキュリティ管理システムを構築するため。

（５）個人情報保護に向けた取組経緯

・97 年：通産省「コンピュータウィルス対策基準」「ソフトウェア管理ガイドライン」に基づく社内体制の整備

・01 年：認証取得体制の構築及び「個人情報保護に関する基本規程」等社内規程の制定

・01 年：「個人情報管理委員会」を組織、個人情報保護に関する内部監査を実施

・02 年：「プライバシーマーク」認証取得

・04 年：「プライバシーマーク」第 1 回更新

・05 年：「ISMS／BS7799」認証取得
・06 年：「BS7799」を「ISO27001」に移行
・06 年：「プライバシーマーク」第 2 回更新
・07 年：「JISQ15001：2006」「情報サービス産業　個人情報保護ガイドラインー第 4 版」に基づき、「個人情報保護マネジメントシステム」として整備
・08 年：「プライバシーマーク」第 3 回更新

（６）個人情報の保有・管理・提供等に関する業界の特徴

・ＩＴ化の進行によりビジネス環境・形態が変化し、個人情報の取り扱い量が増えてきている。
・情報システム業界は、個人情報の取扱いそのものがビジネスであり、安心と信頼を付与するために、早い段階から個人情報保護の重要性を認識して対応をしている。
・プライバシーマーク取得が委託先選定基準にもなっており、連鎖的に個人情報保護及び安全管理措置が取られるようになって、プライバシーマーク取得企業が増えてきている。

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）

・個人情報保護活動組織として個人情報管理委員会を設置し活動を推進
・個人情報保護マネジメントシステムの移行にあたり、JISQ15001：2006 及び情報サービス産業個人情報保護ガイドラインに基づいて社内規程を見直す。

（２）個人情報の取得

・運用処理サービスの提供が主業務につき直接本人からの個人情報取得は多くない。
・本人から個人情報を取得する場合は、主に葉書、Web サイトから取得する。

（３）個人情報の利用（第三者提供を含む）

・運用処理サービス及び会員サービスの提供とビジネス情報の案内の送付等に利用
・マーケティング等への利用及び関連会社間の共同利用並びに第三者への提供はしていない。

（４）個人情報の管理

①情報の管理体制

（機微情報へのアクセスは物理的に厳しく管理）

・個人情報保護マネジメントシステムの移行に合わせてリスクマネジメントを強化。情報のリスクランクに応じた安全管理を実施。

・入退室管理では、守衛による IC カードゲートと入館確認、事務所内に入るための IC カードゲートシステム、CPU ルームに入るための入室チェックの厳重な多重チェック体制を構築。

・ログインには登録者のみに付与されたログイン ID が必要である。

・重要な個人情報は、ネットワーク接続禁止で、独立したサーバで管理している。

・クレジットカード情報の取り扱いについては、汎用機で処理、アクセス権を設定し、厳しい入退室管理とセキュリティ対策を実施。

・ファイル共有ソフト等 P2P ソフト対策のため、『一斉送信監視ソフト』により監視。また、『ライセンス違反検知ソフト』により、P2P ソフト等のインストールを監視。

②従業者への教育方法

・教育は、教育担当委員により計画的に実施している。

・制度の変更時には全社一斉に教育を実施する。

・定期的には、新入社員研修、新任管理職を対象にした階層別教育及び全社員を対象に e ラーニングによる研修を実施している。

・定期的にコンプライアンスに関する議論を課単位で行うが、このときにも個人情報保護についても取り上げて認識を高めるようにしている。

・個人情報研修後の確認はこれまでアンケート方式で行っていたが、プライバシーマーク審査時の指摘により、アンケート方式から確認テスト方式に変更した。

・派遣社員、パートについては、受け入れ時に誓約書をとっている。特に個人情報を扱っている部署については、社内手順など教育を徹底している。

・USB メモリの使用制限、パソコン等安全管理については、事故防止の為の安全対策を実施。

③盗難対策

・サーバは、記録媒体の接続不可。

・個人情報の持ち出し、外部記録媒体に入れることの禁止。

・パソコンはアクセス制限とロックによる施錠。

・USB メモリはすべて情報保護タイプに切り替えた。USB メモリの接続は記録され、利用領域の制限を行っている。

④ノート PC の安全対策

（アクセスロックを多重にかけることで対応している）

・ノート PC へのログインには ID とパスワードが必要である。パスワードは英数字 8 文字以上、40 日間隔で更新

・ノート PC には BIOS ロック、HDD ロックが義務付けられている。紛失しても利用することはできない。また、ノート PC には外部との連絡のための電子メールアドレス程度の情報しか入れないようにしている。

⑤外部委託先管理

・委託先の選定基準は、個人情報マネジメントシステムによる管理体制又はプライバシーマークの取得及び情報セキュリティ社内評価基準を満たしていることを条件としている。

・外部の委託先については、基本的に個人情報の再委託することは禁止している。

・定期的に契約時の契約内容の履行状況の確認により監督。

⑥日常点検・確認の方策

・個人情報マネジメントシステムへの移行に伴い「点検チェックリスト」を作成してマネジメントシステムの運用の確認を実施。

⑦初歩的ミスの防止策

・外出時の荷物は手放さないよう、また FAX では重要情報は送らない等折にふれ指示。

・企業倫理活動でのコンプライアンストークで個人情報保護に関する話題を取り上げ、保護意識の向上を図っている。

（５）個人情報の消去・破棄

（紙媒体の情報は外部事業者に委託）

・環境 ISO14001 取得の関係で、紙媒体はシュレッダーによる裁断又は業者による溶解処理をしている。リサイクル処理の場合、担当者立会いのもと、自社の敷地内で行う。

・社内にごみ箱はなく、すべての個人情報が含まれる書類は溶解処分用の BOX にいれるようになっている。

・溶解処分は、業者の溶解処理場で処分している。処理方法及び個々の処理については、契約時及び個々の処理確認書で確認している。

・CD-ROM は、契約した業者により破砕処理して廃棄している。

・HDD は、破砕処理し再利用不能にして廃棄するようになっている。

・データの廃棄については、登録用紙に実施日を記載し、確認している。

（６）個人情報の監査

・同社はプライバシーマーク、ISMS を取得しており、委託元からの監査を受けたことはない。

・独立した監査部門を組織し、1 回／年個人情報保護監査を実施。個人情報保護監査においては、監査のチェックリストに基づいて、エビデンスの確認、手順の遵守状況の監査を実施している。

（７）苦情処理・顧客対応

・苦情、問い合わせの窓口は、委員会事務局が全社対応を及びサービス毎に事業部門で相談窓口を設置している。

（８）事故発生時の対応

・緊急時の対応のための緊急連絡体制を敷いて危機管理マニュアルに従って対処するようにしている。

（９）その他

・マネジメントレビュー、是正処置・予防処置の仕組みの整備等により個人情報保護マネジメントシステムとして整備した。

・同社では、環境保護への取組もグループ会社全体として実施している。

・環境保護はサイトごとの管理であるため、同一ビル内はすべて同じ基準で実施しなければならず、紙媒体等をすべてリサイクル処理・溶解処分とするのはその一環であり、個人情報の関わる媒体の廃棄などは、この環境保護に活動と連携して実施している。

以　上