キ．情報サービス業（アウトソーシング等）　キ社

事業概要	情報サービス		
従業者数	約 2,700 人	プライバシーマーク取得	あり
保有個人データ件数	約 4 万件		

１．個人情報に関する概要

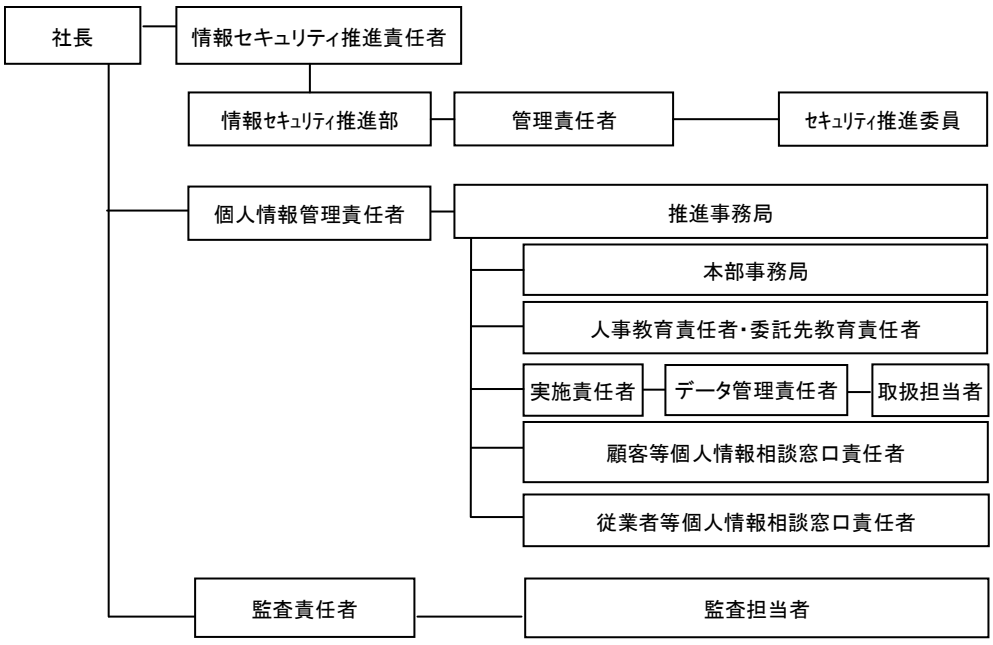
（１）保有する個人情報の件数、個人情報の種類、個人情報の利用目的

・全体で約 4 万件
・アウトソーシング部門：約 9,000 件（社員等の氏名、所属、連絡先、監視カメラ映像、入退管理、指紋・静脈血流など）
・システム部門：約 22,000 件（パッケージソフトのユーザ情報、プロジェクト情報を共有するユーザ情報など）
・営業部門：約 6,000 件（商品 DM などのアンケート結果に伴う情報）
・人事部門：約 3,000 件（従業員の情報）
・顧客から受託している業務に伴う個人情報は上記の対象外。

（２）個人情報保護担当部署

・情報セキュリティ推進部

図表　個人情報保護に係る体制



（３）個人情報保護管理者の有無・位置づけ

・個人情報管理責任者を、アウトソーシング部門の常務取締役が担当。
なお、監査責任者は、システム部門の常務取締役が担当。

（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、運用初年度（1998 年度）に取得。アウトソーシング事業者として、セキュリティ対策が今後ますます重要になるとの認識の下で取得。プライバシーマークは、対外的な信頼性獲得に効果があると認識している。
・ISMS は 2001 年 12 月に認証取得。
・ISMS の国際認証規格 ISO20000 は、2007 年 4 月に認証取得。

（５）個人情報保護に向けた取組経緯

・1998 年のプライバシーマーク取得にあわせて、社内における個人情報の管理体制を構築。
・個人情報保護法が施行される前年の 2004 年に、社内の体制を大幅に刷新。現在の体制に至る。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・アウトソーシングのためのデータセンターを所有しているため、物理的安全管理措置に対して、大きな投資が行われている。

２．個人情報の適切な保護のための取組について

（１）準備（規定・体制づくり）

・個人情報保護に関連する規定類は、情報管理規定、個人情報保護管理規定・細則、他社秘密情報管理規定、各本部ガイドライン、各種規定等から構成される。なお、規定類をコンパクトにまとめた「携行ハンドブック」を作成している（後述）。
・個人情報保護の推進事務局は、情報セキュリティ推進部が中心となって運営。現場でのセキュリティ推進は、セキュリティ推進委員（全社で約 110 名）が担当。

（２）個人情報の取得

・個人情報を取得する際は、個人情報管理責任者に対して、登録許可の申請を行う。申請書には、個人情報の内容や、取得理由、保持期限などを記載する。

（３）個人情報の利用（第三者提供を含む）

・特になし。共同利用も行っていない。

（４）個人情報の管理

①情報の管理システム

（退職者にも Winny 対策を徹底）

・Winny などのファイル共有ソフトは、使用禁止。

・全従業者に対して、過去に持ち帰ったファイル等を削除することを指示し、本人の署名つきの確認書を取っている。

・退職者に対しては、過去 3 年間にさかのぼり、ファイル等を削除したことをチェックすることを依頼する文書を郵送し、やはり本人の署名つきの確認書を返送してもらっている。

［事務局会議］

・情報セキュリティに関する担当者 20 名が集い、四半期毎にテーマを決めて事務局会議を実施。

・事務局で検討した内容については、現場にフィードバックされる。

②従業者への教育方法

・月に 1 度、「セキュリティチェックデー」を設定し、セキュリティ推進委員が、事務局の指定する内容に沿って、チェックを実施。約 1 週間かけて、チェック工程を完了させる。

・ガイドライン等の改正に伴って、規定類等が改正された際は、事務局が全国を行脚して説明する。

・e ラーニングを最低年 1 回全従業員に対して実施。

・新入社員研修、専門職研修等、階層教育を実施する際にもあわせて、個人情報保護に対する教育を実施。

③盗難対策

・2004 年より、顧客の指定があるとき以外は、可搬式メモリの使用は禁止。

・携帯電話は、指紋認証を搭載した専用機を使用。会社で支給している。

④ノート PC の安全対策

・ノート PC は、BIOS、ハードディスク、ログイン全てにパスワードを設定し、ハードディスク内は全領域を暗号化。さらに、セキュリティワイヤーロックの使用を義務付けている。視覚的効果が大きい。

⑤外部委託先管理

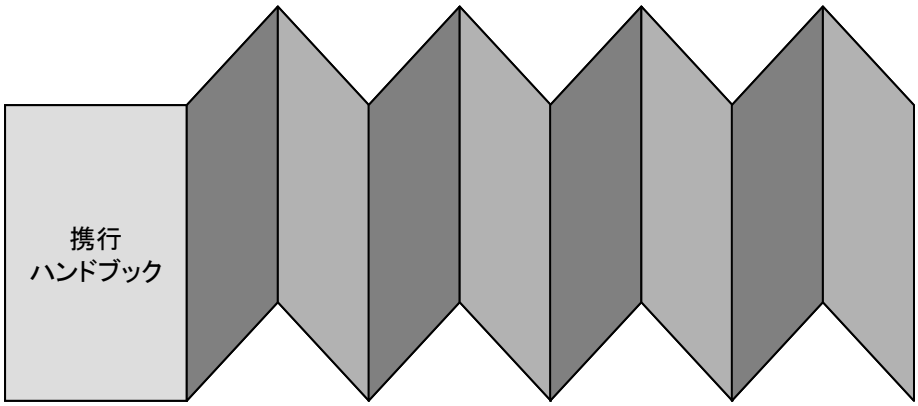
・2004 年に、個人情報を委託している数百に及ぶ事業者に対しては、一斉に監査を実施。
・現在は、年に 1 回、購買部がチェックシートを用いて外部委託先を評価。外部委託先の中からサンプリング抽出して、チェックシートを送付している。
・プライバシーマークなどの取得を奨励し、一所懸命に個人情報保護の取組みを行っている事業者を評価することにしている。

⑥日常点検・確認の方策

（実践的な携行ハンドブックの携行を全従業者に義務付け）

・「携行ハンドブック」を作成し、全従業者に携行を義務付けている。毎月、携行ハンドブックが実際に所持されているか、チェックしている。
・携行ハンドブックには、表面が情報セキュリティ、裏面が個人情報保護に関する内容となっており、全体で 18 ページにわたって、手順及び要点を解説している。
・携行ハンドブックは半年近くの検討を重ねて作成した。見開きで閲覧できるよう、配置を工夫している。
・携行ハンドブックは、定期的に見直し、最新情報を掲載している。

図表　携行ハンドブックのイメージ



［主な記載内容］

・情報セキュリティ推進体制
・セキュリティ対策の項目別の原則、及び実施要領
・他社秘密情報管理体制
・個人情報に関する社内手続
  ✓ 行為別の社内手続、受付窓口、備考
  ✓ 罰則
  ✓ ライフサイクル別の手続（商談発生～受託個人情報受領、利用、管理、外部委託、業務終了後（廃棄・返還）

図表　ハンドブック記載事項のイメージ（各見開きで２ページ分）

実施項目		原則	ﾁｪｯｸ	実施要領
データ保護〈アクセス制限〉	ＰＣの保護	・全PC にBIOSパスワード設定 ・全PCにパスワード付スクリーンセーバ設定 ・ノートパソコンを机上に放置しない		
	サーバ アクセス	秘密情報/個人情報の格納サーバ（イントラ用） ・ＩＤ／パスワード設定 ・アクセスコントロール		
	ファイルの データ保護	暗号化		
	可搬記憶媒体	・USBメモリ、メモリカード等使用禁止 （顧客都合の場合に限り申請により許可） ・ポータブルHDDは使用可 ・使用時はドライブ全体を暗号化		
	PCの持込み /持出し	原則持込み/持出し禁止 （特別な場合のみ条件付きで許可）		
	外出時	**「手放すな　とにかく絶対　手放すな」** **「飲むなら持つな、持つなら飲むな」**		
	情報の保管	電子媒体や紙媒体は鍵付ロッカーに保管する		
協力会社	秘密情報 管理義務	水準を満たす業者の選定		
		適正管理義務		
		外部委託		
ネットセキュリティ	ウィルス対策ソフト	全てのPCにウィルス対策ソフトをインストール		
	PCのﾈｯﾄﾜｰｸ接続	業務作業開始前に十分なセキュリティチェックを行う		
		危険な社外アクセス行為の禁止		

実施項目		原則	ﾁｪｯｸ	実施要領
ネット セキュリティ	社外との接続	他の社外ネットワークに接続しない		
データの受渡し	情報の 受渡し方法	許可申請		
		顧客との取り決め		
		直接手渡す		
		次善策はセキュアなネットワーク経由		
		授受データの暗号化・搬送後の媒体からの削除		
		登録申請		
		機微情報は鍵付きトランクで専用デリバリで運搬		
特別注意事項		私的利用の禁止		
		デモデータ、テストデータ適正管理		
		電子メール送受信の注意点		
		ＦＡＸ送受信時の注意点		
		パスワードの適正管理		
		情報の破棄		
		携帯電話の取り扱い		
		紛失・盗難事故発生時は、直ちに報告		

⑦初歩的ミスの防止策

・全社のクライアントパソコンに、社外に送信する前に誤送信を検出、送信を止めることができる電子メールの誤送信対策製品を導入しメール誤送信対策を強化した。

（５）個人情報の消去・破棄

・書面はシュレッダーを原則とし、容量が多いときには溶解などを用いる。電子媒体は破砕をする。

・個人情報を取得する際に登録した保持期限内に処理を実施する。

・個人情報の登録台帳は、棚卸しを行って、保持期限を過ぎたデータについて、チェックを行っている。

（６）個人情報の監査

・監査責任者による年に１回以上の定期的な監査を実施。

（７）苦情処理・顧客対応

・苦情処理の担当窓口が対応。

・開示請求はこれまでほとんどない。

（８）事故発生時の対応

・連絡体制を整備。

以　上