P. 情報サービス業（ソフトウェア）　P社

事業概要	システム開発等		
従業員数	約 500 人	プライバシーマーク取得	なし
保有個人データ件数	5,000～20,000 件程度		

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

・5,000～20,000 件程度
・従業者の個人情報、入社希望の学生の個人情報を保有している。
・委託元（顧客）から個人情報を預かることは無い。業務形態が顧客企業に常駐してシステム開発を行うことが主であり、顧客企業からは持ち出さないようにしている。

（２）個人情報保護担当部署

・各部署より代表者を選出し、セキュリティ推進委員会が設置している。
・セキュリティ推進委員会の事務局として、ビジネス推進部が担当しており、「個人情報保護」「セキュリティ確保」の担当部局となる。

（３）個人情報保護管理者の有無・位置づけ

・セキュリティ推進委員長（担当取締役）が該当する。

（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 を取得している。
・顧客からは「個人情報保護」ということよりも、「セキュリティ体制の確立」を要求されることからこの認証を取得している。プライバシーマーク取得の予定は無いが、ISO27001 で個人情報保護の分野もある程度カバーできていると考えている。

（５）個人情報保護に向けた取組経緯

・2002 年 4 月　情報セキュリティ分科会を設立（ISMS/BS7799 の調査を開始）
・2003 年 4 月　ISMS/BS7799 認証取得に向けた活動開始
・2003 年 12 月　情報セキュリティマネジメントシステム（ISMS）適合性評価制度」および「BS7799」認証取得
・2006 年 2 月　ISO/IEC27001(情報セキュリティマネジメントシステム)認証取得

（６）個人情報の保有・管理・提供等に関する業界の特徴

・個人情報保護だけでなく、情報セキュリティ確保全般を求めるニーズが高い情報セキュリティ確保に対する要求が年々高まっており、個人情報のみならず機密情報全般に対する会社の取組む姿勢が求められている。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・「個人情報保護方針」「情報セキュリティ保護方針」、「機密情報管理規程」を定め、キューブグループ全体の指針としている。また、各事業所（サイト）や関連会社毎に「情報セキュリティガイドライン」を制定し、キューブグループ全体としての個人情報保護・情報セキュリティ確保に取組んでいる。

（２）個人情報の取得

・特徴的な取組はなし

（３）個人情報の利用（第三者提供を含む）

・特徴的な取組はなし

（４）個人情報の管理

①情報の管理体制

・検疫ネットワークシステムを導入し、Windows Update、ウィルス定義ファイルの更新、不要ソフトの有無状況を把握できる仕組みを構築して監視を行っている。

・個人所有端末の使用を禁止し、すべて会社資産端末若しくは顧客貸与端末を利用することで、セキュリティリスクを軽減している。

②従業者への教育方法

・「個人情報保護」「情報セキュリティ保護」の観点から、日頃より留意すべき事項や緊急時の連絡法等を取りまとめた「コンプライアンス・セキュリティハンドブック」を全社員に配布し、周知徹底している。

・また、このハンドブックにチェック欄を設けており、プロジェクト責任者がプロジェクトメンバーのルールの遵守状況を月次で確認する運用を実施している。

③盗難対策

・暗号化ソフト Secure Doc を全端末に導入し、盗難防止対策を実施。

④ノート PC の安全対策

・暗号化ソフト Secure Doc を全端末に導入及びチェーンロックや個別ロッカーの設置等により、ノート PC の安全対策を実施。

⑤外部委託先管理

・プロジェクトに参画頂く外部委託先従事者においても、「コンプライアンス・セキュリティハンドブック」を配布し、月次でチェックしてもらう事で、セキュリティモラルの向上を図っている。

・また、外部委託先会社に対して、毎年セキュリティ対策状況調査を実施してもらい報告頂いている。

⑥日常点検・確認の方策

・**「コンプライアンス・セキュリティハンドブック」**にチェック欄を設けており、プロジェクト責任者がプロジェクトメンバーのルールの遵守状況を月次で確認する運用を実施している。

⑦初歩的ミスの防止策

・特徴的な取組はなし

（５）個人情報の消去・破棄

・端末においては、個人情報や機密情報等を削除した上で専門の業者に廃棄を依頼している。紙についても、専門の業者を通じて安全に処分廃棄している。

（６）個人情報の監査

・特徴的な取組はなし

（７）苦情処理・顧客対応

・特徴的な取組はなし

（８）事故発生時の対応

・「コンプライアンス・セキュリティハンドブック」にエスカレーションルールが記載されており、事故発生時には速やかにエスカレーションできる体制を整えている。

・事故対応後、必ず「セキュリティ事故報告書」を作成し、再発防止策に取組む仕組みを構築している。

以　上