L. 情報サービス業（ソフトウェア） L 社

事業概要	システム開発、システムインテグレーション事業等		
従業員数	約　6,600 人	プライバシーマーク取得	あり
保有個人データ件数	約 120 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

・顧客の情報が約 120 万件
・従業者情報が約 1 万件

（2）個人情報保護担当部署

・全社マネージメントシステム維持運用のコントロールはコンプライアンス室個人情報管理課。具体的な運用（対策措置実施等）は各担当部署にて実施。

（3）個人情報保護管理者の有無・位置づけ

・個人情報保護統括責任者は取締役

（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と ISMS 及び ISO14001・ISO9001 を取得している。
・プライバシーマークは一部 B2C 形態の事業があることや、社会的な要請、内部統制の必要性等鑑み、平成 16 年初旬に取得を目指すことを決定し、コンプライアンスプログラムの構築を開始、平成 18 年には更新された JISQ15001(2006)に対応して個人情報保護マネジメントシステムとして修正。

（5）個人情報保護に向けた取組経緯

・コンプライアンスプログラム構築に向け、構築を目的にプロジェクトを発足。コンプライアンスプログラム構築後はセキュリティ全般に関する委員会を設置した。その委員会でセキュリティ全般に関する検討を行っている。
・コンプライアンスプログラムの構築に 1 年半を要した。
・情報漏洩事故を機に情報セキュリティ全般を主管する部署を設置。

（6）個人情報の保有・管理・提供等に関する業界の特徴

・属人的な管理を避け、情報システムを活用した管理を行っている。

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）

・運用については、物理的な部分は総務部、従業者教育は人事部、問い合わせ対応はお客様相談室とし、具体的な個別対策ごとに運用実務を担当する部署を定めている。例えば、入退館管理など、物理的な対策措置は総務部が行い、総務部より提供された入退館管理に関する教育コンテンツの材料により、人事部が ｅ ラーニングコンテンツ作成と全従業者への教育を行う。

・全社網羅的な体制を確保するため、各部署における個人情報保護管理者は当該部署の管理職を任命している。

（２）個人情報の取得

・オプトインの取れている個人情報しか保有しない。

（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

・社内就労者に対して与えている情報システムのアクセス権は、正社員とその他就労者（派遣・出向）で明確に分けている。更に正社員でも職位によりアクセス権の階層があり、アクセスできる情報が管理されている。本人のアクセス権を超える社内システムにアクセスする必要がある場合は、当該部署の管理職（兼個人情報保護管理者）の申請によってアクセス権が与えられる。

（私有パソコンの持ち込み禁止、社内使用パソコンの持ち出し禁止）

・個人所有のパソコンをはじめとする私有情報機器の社内持ち込みを禁止している。

・社内使用パソコンは原則として社外持ち出し禁止としている。職種によりノート PC の社外持ち出しが必要な従業者は社内では専用の外部 HDD を用い、この外部 HDD は社外に持ち出しができない運用としている。このため、社外に持ち出したノート PC には機密情報が存在しない。業務上止むを得ず機密情報を持ち出す場合は暗号化を行う運用としている。

②従業員従業者への教育方法

（「CP 免許」を発行することで、個人情報保護を含めたセキュリティ全般に関するモラルアップをはかっている）

・取締役を含めた全従業者就労者に対して CP（コンプライアンスプログラム）免許の取

得を義務付けている。CP 免許は必要な研修を受講し、テストに合格して付与される。また免許には４級から１級まで４クラスあり、社内システムへのアクセス権取得は４級取得が前程条件となる。
・各級を表すシールは社員証に貼付している。また“部”や“部門”単位の各級取得状況を全社の会議などで報告する。この運用はより高い級の取得(＝高いセキュリティ知識・意識)への意識付けに大きく貢献している。

・平成 16 年 9 月ＣＰ免許制度発足以来の全従業者への地道な啓発・教育の成果で、平成 20 年 11 月現在で、正社員の 3 級以上取得比率(ＣＰ免許上位級取得比率)は 78.3%となり、セキュリティに関する基礎的なノウハウ取得の底上げは確実に進展していることが裏付けられている。
・更新試験は毎年行われ、e ラーニングコンテンツを毎年見直しして教育及びテストを実施する。新たなリスクや脅威はこのコンテンツ更新時に取り込まれ、教育される。
・CP 免許は減点制度も運用されている。減点制度はセキュリティ義務違反(例：OS のアップデート不履行)により、持ち点(6 点)がゼロになると免許停止となり、復級するためには、直属上司とともに「免停講習」を受講した上で「復級テスト」に合格する必要がある。
・ＣＰ免許減点対象の月次ウイルスチェックの実施に関しても、当初一年間は毎月 10 名以上の社員が未実施で減点されていたが、ＣＰ免許スタート後 4 年目の平成 19 年 9 月以降一年間は未実施者ゼロとなり、情報セキュリティの運用面でも効果が出ている。
・試験はすべて e ラーニングで受験する運用となっている。多くの問題を用意して、受講者ごとに問題をシャッフルして出題するようにシステム化しており、受験者の不正防止と試験実施の工数を大きくしない運用となっている。
・ＣＰ免許の運用では、従来「個人情報保護」と「情報セキュリティ」に関する運用の啓発・教育に力を入れてきたが、平成 21 年の更新研修及び運用強化月間では、コンプライアンス等他の運用に対象範囲を広げていく計画。

③盗難対策

・USB メモリは使用禁止である。業務上やむを得ず使用が必要な場合は、パスワードがかけられ、情報が暗号化できる機種を個別の申請に基づいて配布している。配布された USB メモリはマネージャーが施錠できる場所に保管、履歴管理を行って、WEB 上に記載する。全社で 300 個程度保有している。
・一部の従業者には業務連絡用に会社からスマートフォン・PHS を貸し出しているが、このスマートフォン・PHS に記録されている電話帳等のデータは、万が一紛失の折、当社からの依頼で消去できるようになっている。

④ノート PC の安全対策

・ノート PC の紛失時のセキュリティは二重三重に対策を講じている。まず物理的対策として USB キーロックがあり、システム起動時にはパワーオンパスワードと Windows

のパスワードの入力を必要としている。更に社外からの社内システムへの接続にはワンタイムパスワードの入力が必要となり、当社従業者以外の者が利用できない仕組みとしている。

⑤外部委託先管理

・特徴的な取組はなし

⑥日常点検・確認の方策

・月に一度、セキュリティに関する対策措置の運用実施、記録管理について全管理職がWEB 画面に報告する運用としている。この運用報告は監査室の監査が行われる折に実態との乖離チェックが入り、二重に牽制が効くように配慮されている。

⑦電子メール誤送付の防止策

・お客様をはじめとした社外への電子メール送付は、「1 to 1 電子メール」を原則としている。

・100 件を超える同報メールはシステム上で従業者個人からは送付できない仕組みとしている。

・電子メールを利用したダイレクトメールやメールマガジンは、すべて専門の担当部署を通じて送付される。また利用される送付先データはオプトインを取得したデータベースから抽出したデータに限定される。

（５）個人情報の消去・破棄

・社内システムから個人情報を含むデータをダウンロードするためには、一定の承認手続を要し、その手続の中に使用期限の入力が定められている。使用期限を過ぎても破棄報告を行わない利用者に対しては、自動的に警告メールが送付され、それでも破棄及びその報告が為されない場合は、以降の当該部署への社内システムによる当該部署への情報提供はストップされる運用となっている。

・ダウンロードしたデータの使用期間は最大 2 ヶ月までである。

・社内システムから個人情報を含むデータを利用する場合、全て各店課の管理職を通じて配布され、使用期限内のデータ破棄が義務付けられているが、平成 20 年 7 月より監査室の各店課への業務監査と合わせて、配布データが残存していないことの確認を実施する運用とした。検査システムでチェックするため、運用徹底に一層の効果が期待される。

（６）個人情報の監査

・確実な運用徹底をはかるために、監査室を主管部署として各現場部署の役職者を選抜、専門教育を施し、ＰＭＳ内部監査員を養成した。平成 20 年 11 月現在 326 名(正社員比率 4.7%)の内部監査員は 100 箇所以上にのぼる拠点の内部監査運用にあたり、実質的

に各所属セクションでのＰＭＳ運用リーダーの役割も担うことになる。
・監査は監査員のスキルによって監査内容に跛行が生じないよう、監査基準や監査ポイントを明確にした監査チェックリストと運用マニュアルを整備し、年一回の内部Ｐマーク監査の前には、内部監査員向けに研修を実施し、継続的なスキルアップと啓発を行っている。
・内部Ｐマーク監査の際には被監査部署にも監査の重点ポイントを事前連絡し、「監査で指摘」することよりも、「監査以前に是正」することの「教育的効果」を狙っている。

（７）苦情処理・顧客対応

・当社に寄せられた苦情は、Ｐマーク取得ためのコンプライアンスプログラム構築と時を同じくしてリリースした、苦情データを登録・分析するためのＶＯＧシステム(Voice of God：神の声)にて管理。苦情の種類・当社瑕疵割合・原因・担当者責任度合い等分析し、苦情内容・対応プロセス等を共有、再発防止に効果を上げている。
・苦情はお客様相談室指導のもと「対応完了」とされるまで追跡・確認を行い。原因分析の上、必要に応じて再発防止策を社内に水平展開する運用としている。
・すべての電子メールに関して送信ログを取っている。よって、外部からの「スパムメール受信についてのクレーム」に関しては、電子メールのヘッダ情報と電子メールの送信ログを比較する事により容易に判断が可能な為、すぐに顧客の苦情に対応できるようになっている（大抵の場合はシステムについて説明すると納得してもらえている)。
・開示請求のマニュアルを作って準備してきた。実際の開示請求はない。開示請求の手数料は実費のみとしている。
・担当は、お客様相談室としている。

（８）事故発生時の対応

（セキュリティ事故が発生した際には、発生日時を問わず（24 時間 365 日対応）担当役員の携帯電話に事故発生の通報電子メールが転送され、迅速・適切な対応を可能としている）

・情報セキュリティ事故発生の場合に誰が何をするか、マニュアルを用意している。
・いち早く正確な事故情報を把握することに重点を置いている。

以　上