セ．情報サービス業（ソフトウェア） セ社

業務概要	システム開発、ASP やアウトソーシング等サービス提供、アプリケーション及びパッケージ開発・販売、情報処理機器開発・販売		
従業員数	約 5,500 人	プライバシーマーク取得	あり
保有個人データ件数	多数（システム開発に伴い個人情報が預託されるので変動する）		

１．個人情報に関する概要

（１）保有個人情報件数、種類、利用目的

・同社の従業員情報として保有しているもの以外にも、パートナー会社の人員の情報があり、絶えず人が出入りしているので変動する。また、お客様ご本人の情報やお客様から預かるものもカウントしている。システム開発に関してお客様から預かるデータは 1～2 年でお返しする。こういったデータがあるので件数は常に変動している。

・預かる以上、責任がある。なるべく預からないようにしており、必要でないものは預からない。過去にはテストデータを生データで行ったりもしていたことがあるが、現在はダミーデータで行っている。

・同社の従業員情報やパートナー会社の人員情報、従業員採用応募者の情報、お客様ご本人の情報

・「システム開発のために預託される個人情報」と、「同社が Web サイトで実施しているサービスに関する個人情報」もある。また、顧客が Web 経由でサービスを行っており、同社がシステム保守を行う場合には、同社が個人情報を保有している形になることもある。

・Web サイトで実施しているサービスとは ASP（SaaS）のことである。医療機関や金融機関などのシステム運用を行っている。

・運用サービスでは、顧客情報は顧客所有のサーバに格納されているが、保守などのために同社からリモートでアクセスできるので、同社の個人情報として管理が求められるようになっており、同社の個人情報保護規定に即した対応を行っている。

・個人情報の利用目的は以下のように定め、公表している。

同社は、情報サービス業を主とした事業活動に関して、個人情報を次の各号の目的の達成に必要な範囲でのみ取得し、利用するものとします。

①ご本人さま、またはお客様と当社との間で締結した契約の履行

②ご本人さま、またはお客様との商談、打合せのための連絡

③製品のアフターサービスの提供および催物開催、新商品のご案内の送付

④システム開発・運用・保守など、お客様から当社に委託された業務の履行

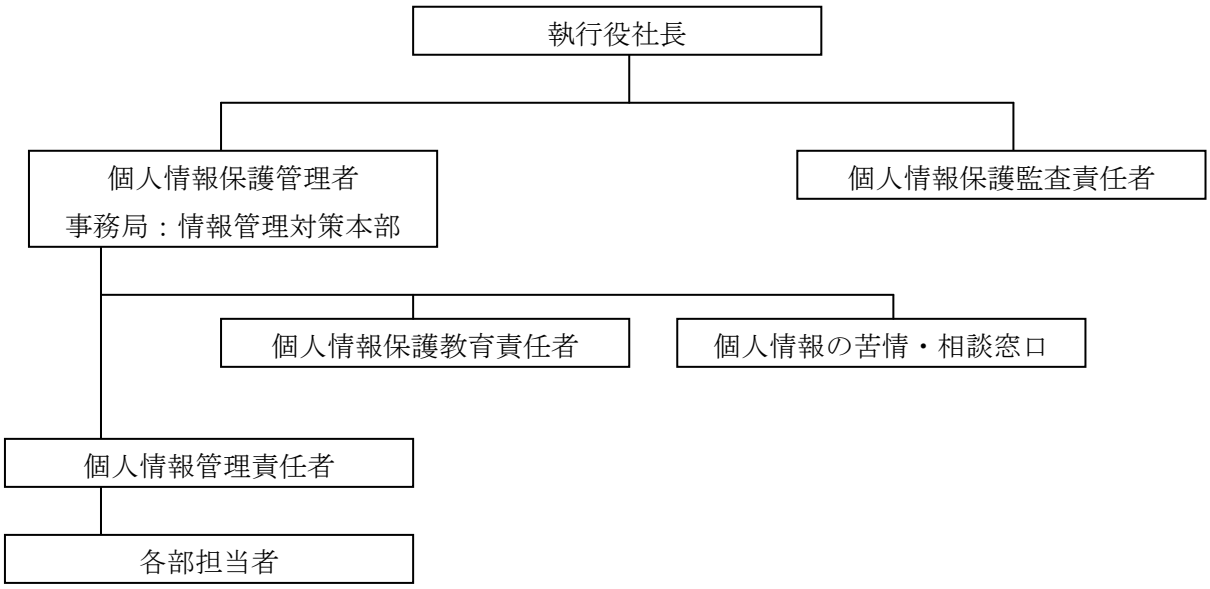
⑤各種会員制サービスの提供

⑥株式に関する事務
⑦各種お問い合わせへの対応
⑧アンケートをもとにした製品やサービスを向上させるための分析
⑨同社が自社のグループ会社と共同して事業活動を遂行する場合における当該グループ会社への個人情報の提供

（２）個人情報保護担当部署

・社長に直結した「情報管理対策本部」を常設組織として設置している。専任で 3 名、兼任が複数名従事し、個人情報含め、機密情報の管理を担当する部署である。機密情報とは「マル秘事項」と捉えられがちだが、お客様情報はすべて機密情報である。
・個人情報保護体制としては、情報管理対策本部の本部長が会社全体の「個人情報保護管理者」となっており、この本部長は常務以上が任命されることになっている。
・ルールをきめるだけではなく、ルールを徹底する・し続けることが重要と考えている。そのためには教育の責任者を置くことが必要であり、情報管理対策本部の部長を「個人情報保護教育責任者」に任命している。
・お客様向けの窓口としては「個人情報の苦情・相談窓口」を設けており、情報管理対策本部の部長がこの任に当っているが、問合せはほとんどない。

図表　個人情報保護体制



（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常務以上の役員が常任として任命される。

・位置付けは CPO（Chief Privacy Officer、統括管理者）であるが、機密情報の管理者でもあり、全社を統括している。PMS（個人情報保護マネジメントシステム）の運用・管理に責任を負っている。

（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 1998 年 11 月に取得した。まだ取得していた会社が一桁台の頃だと思う。

・同社ではセキュリティ製品を扱っており、これに相応しい仕掛けを作り込む必要があった。初めはこの考え方から取得したが、現在は CSR の意味で取組まねばならないものだと考えている。

・プライバシーマークの取得は会社が取組んでいる仕掛けの見直しになるので、よいと思っている。PDCA のフレームワークが参考になる。

（５）個人情報保護に向けた取組経緯

・他の箇所（２(1)等）に記載してあるため割愛。

（６）個人情報の保有・管理・提供等に関する業界等の特徴

・情報サービス業界では、個人情報の取扱いそのものがビジネスであり、顧客から安心と信頼を得るために、早い段階から個人情報保護の重要性を認識・対応してきた。

・プライバシーマーク取得が委託先選定基準にもなっているため、必然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り、結果プライバシーマーク取得企業が増えている。
・IT 化、技術進歩の進行によりビジネス環境・形態が変化し、取扱う個人情報の量が増えてきている。
・厳密に個人情報ではないが、機密情報に触れる人は、普通の企業であれば限定すれば良いが、システム開発・保守・運用では、携わる人は皆、機密情報に触れることになり、パートナー会社も含め、いろいろな人が触れるし、触れる人の入れ替わりが相当早い、ということも特徴的。

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）

・プライバシーマーク制度ができる以前の 1993 年から社内でセキュリティ監査を開始している。
・プライバシーマーク（1998 年取得）の取得を目指したことも、社内の規則と体制整備の契機の一つとなった。
・個人情報保護法ができるということで、常設ではないが、施行の 1 年前に情報管理に関する委員会を社内で設置した。専務取締役が委員長になり、個人情報保護対策を整備していた。事務局も設置し、かなり力を入れていた。この委員会を基礎として、2004 年の 8 月に情報管理対策本部を設置した。
・個人情報保護という形で明確に社内規則を作ったのは 2003 年の委員会である。
・2003 年の規則制定時は、全てが個人情報であるというイメージがあり、整理には非常に配慮した。
・本当に実行できるルールでなければ意味がないが、守らなければならない事が非常に多く、両方を成り立たせるために規則の作りこみは苦労した。社員が見たときにすぐにわかるようにすることにも気を配った。

（規則のレイヤーを 3 段階に分けることで、軽微なルール変更を迅速に実施）

・規則の見直しについては、いろいろな環境変化、事象の発生に合わせて対応している。例えば新 JIS 規程の変更に伴って変更したこともある。それ以前にも、同社グループ全体で、体系整理を行ったこともあった。それは、規則のレイヤーを 3 段階程度に分けようという取組であった。レイヤーを分けることで、簡易な変更にはすぐに対応できるようにした（それまでは会社規則として全てを定めていたので、変更に役員会の決議が必要など、変更が容易ではなかった）。

・今も見直し継続中であるが、方向性としては、ルール相互の間の関係性や整合性を見直そうとしている。現在の規則は文書の規則、システムの規則、個人情報の規則、文書持ち出しの規則などが輻輳してしまっているのが問題だと認識している。

（２）個人情報の取得

・間接取得が非常に多い。お客様から預からなくて済むものは預からないようにしている。顧客によって個人情報保護ルールが異なるので、そのことは契約書の中に明記してもらうようお願いしている。
・さらに、お客様の個人情報保護ルールを教えてもらわないと適切な対応ができないので、必ず教えてもらうようにしている。お客様からルールを教えてもらい、それを代表者だけではなく全員に教育することについては情報管理本部でも徹底して指導している。例えば、「ポータブル音楽プレイヤーの持込の全面禁止」をしている企業があり、同社の社員がそれを知らずに持ち込もうとしてしまい、お客様から叱責を受けたことがあった。
・直接取得については大きな問題は生じていない。用途を示して取得している。また、名簿を買うようなことはしていない。

（３）個人情報の利用

・預託された個人情報については開発やサービス事業以外の目的では利用できないし、していない。
・展示博覧会等で頂戴した名刺などは、マーケティングに活用するなどしている。

（４）個人情報の管理

①情報の管理体制

(技術的対策)

・業務で使用するパソコンは、以前は各職場で購入していたが、会社より一括配布するように変更した。必要なソフトもインストールして配布している。同社の製品でインストールされているソフトを自動検知するソフトも入れてあり、余計なソフトをインストールさせないようにしている。インストールしてはいけないソフトも予め決めている。このような施策は、ライセンスの適正管理にも有効である。
・実際に問題あるソフトのインストールが発見された場合には、情報管理対策本部から「なぜインストールしたのか」ということを直接に問いかけ、即座にアンインストールするように指示している。単にアンインストールの指示を出すより、「なぜ？」という問いかけをすることで、問題意識を高めるようにしている。
・書類からの情報漏えいを防止するために、文書を印刷する際には、プリンタで同社の製品を使用し、静脈認証をした上でないとプリントアウトできないようにしている。

・モバイル用ノートパソコンはシンクライアントに限定し、さらに情報管理対策本部が認定して持出許可シールを発行したパソコンしか持出せないようにしている。

（USB メモリへの書き出しは顧客ニーズに合わせ、限定パソコンで部長決裁の上で実施）

・パソコンから USB メモリへは暗号化した情報しか書き出せないようにしている。ただ、お客様のニーズもあるので、予め決められた一部のパソコンからは平文で書き出せるようにしているが、このパソコンも情報管理対策本部が認定したものに限定し、使用する場合は、部長の許可が必要である。
・在宅勤務を認めているが、自宅で作業をする際には、自宅のパソコンを使用しても、自宅のパソコンの性能・利用環境とは切り離して、シンクライアントパソコンとして使用できるようにするための特殊な USB メモリも配布している。基本的には在宅勤務の場合には、会社で使用するパソコンとは別のパソコンを支給している。
・自宅パソコンを選択した場合、その点検も年に一度実施している。特殊なソフトを活用することで、パソコン内に問題のあるファイルや個人情報がないかをチェックしている。特定ソフトの使用チェックも行っている。この施策はパートナー会社にも実施をお願いしている。
・自宅パソコンについては個人の持ち物ではあるが、対策について強いお願いをしている。チェックを実施した上で、「何も異常は無かった」、「異常はあったが対処した」ということについて、確認書を作成し、押印した上で提出してもらっている。

（物理的対策）

・執務室は IC カードによる開錠が必要であり、入退室ログの管理も行っている。
・情報によってレベル分けし、指認証がなければ入れない部屋もある。
・パソコンや書類の会社からの持出しについては、警備員による抜打ちチェックも行っている。

（個人情報等が含まれる書類の収納スペースを狭くすることで不要な個人情報等を削減）

・ノートパソコン、個人情報や機密情報が含まれている関連書類については、帰宅時・外出時には専用に会社から支給する鞄へ格納して、施錠可能なロッカーに入れるようにしている。このロッカーの幅を非常に狭くしており、一定以上の文書が発生した場合には、電子化や共用のキャビネットを使うように指導したことで、不要な文書の削減（電子化）や保管コストの削減にも寄与した。

②従業者への教育方法

・e ラーニングも実施しているが、直接話し掛けることを重視している。また、同社の社員のみならず、グループ会社やパートナー会社の社員も対象としている。

・ルール変更時にはその都度、職場の個人情報管理責任者（部長クラスなど）には詳細にルールの説明を行っている。
・定期的に、全社員が集合する場があるが、そこでもセキュリティの話はしている。
・運転免許更新時の研修と同じで、実例をできる限り見せることにより、インパクトをもって感じてもらうことに力点を置いている。
・その他、社長以下役員の挨拶などでは、必ずセキュリティ・個人情報の話はするようにしている。特に振り付けをしているわけではなく、自然と話が出てくるようになっている。幹部層にも情報セキュリティの重要性の認識が浸透している。
・教育については、知識を身につけてもらうことよりも、「意識付け」を重視している。
・カードを携帯しており、そこに内部向けの窓口の電話番号が載っている。何かあった時に「2 時間以内に報告（2 時間ルール）」を徹底している。何かをなくしたときは早めに探すのが一番であると考えており、そのためには早い連絡が良い。同社ではこういった意識が徹底しており、かなり小さな出来事でも報告が来るようになっている。

（啓発のためのポスターの定期的変更、従業員からの募集したスローガンを掲載するなどして、継続的に従業員の意識喚起を実施）
・ポスターも定期的に変えており、啓発している。同じポスターをずっと掲示していても皆飽きてしまい、見なくなったり、意識が薄れたりしがちなので、ポスターを頻繁に変えることで注意喚起を行っている。ポスターに記載されるスローガンも社員に対して募集して選定・掲載しており、社員も参加意識を感じられるようになっている。

③盗難対策
・モバイル用ノートパソコンはシンクライアントに限定し、さらに情報管理対策本部が認定して持出許可シールを発行したパソコンしか持出せないようにしている。
・その他は①情報の管理体制：物理的対策と同じ。

④ノート PC の安全対策
・ノートパソコンは、帰宅時には必ず鍵のかかるキャビネットに格納するようにしている。
・ノートパソコンは全てシンクライアントになっている。
・持ち出しても良いパソコンには大きな「持ち出し許可」のシールが貼付されており、周囲の人が見れば、持ち出し可能なのか、違うのかがすぐにわかるようになっている。

⑤外部委託先管理
・外部委託先を管理する際には、二次委託や三次委託は基本的には認めないようにしている。

・パートナーは昔からずっと継続的な関係で実施しているので、できる限り監査などの支援も行っている。
・長い付き合いのパートナー会社が多いので、水準を合わせて貰っている。
・パートナー会社への協力も行っている。教育や監査のお手伝いとしての人の派遣、ツール類の貸出しも行っている。また、パートナー会社の幹部に対するお願いも行っている。
・委託先に対しても、事前に連絡をした上で、個人情報や機密情報の管理体制の確認に行く。

（パートナー会社の経営層向けの意識喚起の機会を設定）

・年に 1 度、パートナー会社の経営層の方に来訪してもらって、弊社の施策や事故事例の話をするような機会を設けている。最近では特に「機密」の概念が変わってきていることについて重点的に説明している（例：かつて、作業記録は機密情報ではなかったが、作業記録に個人名が含まれていると、個人情報、機密情報として扱われるようになってきた)。

⑥日常点検・確認の方策

・毎月１回、「情報漏えい対策の日」を設けており、年に１度、特定の月に「セキュリティ点検の月」を設定して、個人パソコンのチェックなども行っている。
・現場の情報管理責任者が中心になって実施している。

（荷物検査をグループ会社の警備員が社屋出入り口で実施。全ての書類を原則持ち出し禁止とすることで警備員でも判断可能とした）

・荷物検査も抜き打ちで実施している。不定期でしかも抜き打ち実施している。実際のチェックは警備員が実施する。警備員もグループ会社の人間であるので、依頼しやすく、チェックの方法なども指示しやすい。もし、持ち出し禁止の書類などが見つかった場合には、始末書を書くことになる。
・会社の書類は全て機密である、ということにしているので、「この書類は持ち出してよいか、悪いか」、という判断が発生することがない。したがって、（必ずしも機密情報や個人情報に詳しくない）警備員の人であっても判断は求められない。

⑦初歩的ミスの防止策

・メールについては、メーラーを特定のものに制限している。送信時に送信先の確認ができるメーラーのみ利用可能としている。なお、誤送信を防止するために、メール送信後は、一定時間（15 分程度）サーバに蓄積されてから送信されるようになっている。
・メーリングリスト作成・管理は特定の部署でしか認めていない。

・メールは CC だと他の CC の者にもメールアドレスがわかってしまうことがあり、TO と CC を合わせた人数を限定している。
・添付ファイルが付いた社外宛メールは全てサーバで送信を止める。ただし、「上長が CC に含まれていれば送信できる」、ということにしており、フィルタリングシステムが付いている。上司に必ず CC されてしまうことが、抑制力として機能していると考えている。

（外部送信済みファイルでもコピーできないような特殊な処理を実施）

・一度、外部に送信したファイルであっても、勝手に送付先でコピーして欲しくないようなファイルについては、特殊な処理を施して、コピーができないようにしている。具体的には、ファイルを特定のアプリケーションを利用しないと開けないようにしており、そのアプリケーションに「コピーされたファイルは開けないようにする」機能を組み込むことにより、コピーファイルがいろいろなところに無制限に出回ることを防止している。但し、今は PDF 形式のファイル限定でこのような対応ができている。
・自社のパソコンについては、プリントスクリーン（画面をそのまま画像として認識・取り込むパソコンの機能）もできないような技術的処置をしている。

（酒席での漏えい事故発生時には同席者も一部連帯責任を負う）

・酒席にノートパソコン、個人情報を持ち込む事は禁止されている。実際に飲酒が原因で漏えい事故等が発生した場合には、酒席に参加していた者で、実際に漏えいに繋がるような行動をした者、及び管理責任者は連帯責任として処罰される。

（５）個人情報の消去・破棄

・パソコンの廃棄時には特殊なソフトでハードディスクを真白にしている。故障でこれができない場合は、磁気破壊を行っている。
・紙媒体の個人情報・機密情報については、各職場でシュレッダにより裁断することになっている。その他の書類は特殊な箱に廃棄するようになっており、事業所のビルの地下など特殊な部屋で裁断するようにしている。書類のまま外部に委託することはしておらず、外部に持ち出すこと自体がリスクと考えている。

（６）個人情報の監査

・全体監査ということで、内部統制などと一緒に全職場で実施している。
・3 ヶ月に 1 度、情報管理対策本部が独自の監査を実施。サンプリング調査にはなるが、抜き打ちで検査を実施している。
・問題があった場合には改善命令を出している。摘発のための監査ではなく、指導のための監査である。

・お客様先に常駐している部署に対しては、そこに行って監査を行うが、中には監査員が立ち入ることを嫌がるお客様もあり、そういう場合は、管理責任者を同社内に呼んで監査を行う。
・パートナー会社に対しては、調達本部と連携して監査を実施している。国内だけではなく、海外のパートー会社にも実施している。

（７）苦情処理・顧客対応

・苦情が寄せられる事はほとんどない。

（８）事故発生時の対応

・漏えい事件等発生時の連絡先としては、社内に専用の電話窓口を設置しており、問題発生から 2 時間以内に情報管理対策本部に連絡が来るようになっている。些細なことでも必ず連絡が来るようになっている。IC カードホルダーに格納できるコンパクトな携帯ハンドブックに連絡先電話番号が記載されている。24 時間 365 日連絡が付くようになっている。
・鞄などがなくなった場合には、数十人で探すようにしている。早く探すと見つかり、何とかなることが多い。1 人で探すより、大人数で探した方が間違いなく早いので、その人の所属組織だけでなく、複数部署に動員をかけ、仕事を止めてでも対応するようにしている。対応の速さを非常に重要視している。
・最近は意識が高まっているので、飲酒後の帰宅時に失くすということはほとんどない。
・事故のパターンについて、統計をとって分析している。段々と事故の発生の形態も変わってきており、教育にフィードバックしている。

以　上