ツ．情報サービス業（ポータル）　ツ社

事業概要	ポータルサイトを通じたインターネット広告事業、イーコマース事業。会員サービス事業		
従業員数	約 3,600 人	プライバシーマーク取得	なし
保有個人データ件数	多数		

１．個人情報保護に関する概要

（１）保有する個人情報の件数、種類、利用目的

・個人情報の種類：サービスによって異なるが、住所、氏名、電話、クレジット番号、引き落とし銀行口座などがある。
・PC メールアドレスは個人情報ではないと認識している。IP アドレスについても、個人情報は結び付けていないため、個人情報と認識していない。また、メールアドレス作成時に入力した情報はとくにデータベース化していない。
・ブラウザクッキーは ID と結びついていない。

（２）個人情報保護担当部署

・個人情報の管理は、技術的観点からは情報セキュリティ部が、社内教育および事故対応は法務部コンプライアンス部が行っている。
・個人情報に関わる事項はセキュリティ委員会で議論をおこなう。セキュリティ委員会は、各部門の管理職より上の役職の現場セキュリティ担当者から構成されており、ルール制定と審査をおこなっている。
・個人情報はサービス単位で部署がデータを保有している。
・同社はサービス単位で約款を持っている。全ての約款は、法務部によるレビューを受ける。
・決済サービスに関するビジネスは、個人向けサービスに限り、料金サービス部が一括して料金の請求をしている。

（３）個人情報保護管理者の有無・位置づけ

・チーフプライバシーオフィサー（CPO）を設置している。現在 CPO は、チーフコンプライアンスオフィサー（CCO）が兼務している。
・チーフセキュリティオフィサー（CSO）は別の役員が担当している。CSO は技術者よりの責任者である。

（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

・全社レベルで ISMS を取得している。取得に関しては、PDCA をまわすことが出来ているかがポイントであり、作業的な負担・時間はかるものの、取得はそれほど困難ではなかった。

・現状ではプライバシーマークを取得する意向はない。プライバシーマークとは考え方が異なる。同社ほどの規模の企業において、細かい事故を含めると、漏えいを皆無にするのは不可能に近い。プライバシーマークの取得時に、過去に漏えいがなかったかと聞かれても、無かったとはいえない。

（５）個人情報保護に向けた取組経緯

・電子掲示板サービスを開始した 1997 年から個人情報保護の取組を開始した。

・オークションサービス・電子決済サービスを始めた 2001 年から個人情報保護の取組を強化した。個人情報保護法は特に契機とはならなかった。

・電子決済サービスを開始以前は純粋な広告モデルのサービスしかおこなっておらず、また、マス広告であったため、氏名・住所などの個人情報は保有せず、年代・性別程度の情報のみしか保有していなかった。しかし、決済サービスは債務者の情報・氏名・住所が必要となり、保護体制の強化が必要となった。

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）

・参考となるポータル事業者の日本版の規定はなかったため、米国のポータル事業者の規約を参考にした。

（２）個人情報の取得

（不要な情報は収集しない、できる限り機微度を下げて情報を取得）

・取得を検討している個人情報は、本当にその情報量のレベルが必要か、ひとつひとつ審議をおこなう。例えば、「生年月日」の取得を検討している際は、「年齢」で代替することはできないか、など、出来る限り情報量のレベルを落とし、漏えいした場合のリスクを低減するよう努力している。

・担当者が説明できない場合は、再検討するよう、セキュリティ委員会から指導される。

・この仕組みには、定型の回答フォーマットはなく、個人情報取得の申請書を書く担当者が前例を参考にしながら検討する。前例はセキュリティ情報とともに、イントラネット上に掲載されている。

（情報のセキュリティレベルを三段階に区分。セキュリティレベルにあわせてシステム開発にかかる要求事項も多くなる。）

・管理する情報を、個人情報を含んでいないもの、個人情報を含んでいるもの、決済情報を含んでいるもの、の三段階に分け、それぞれデータセンターにおける区画を分けて保存するようにしている。

・管理する情報のセキュリティレベルが高ければ高いほど、開発するシステムへの要求事項も多くなり、サービス開始まで時間がかかる。そのため、現場の企画担当者は自ずと取得する情報に個人情報を含まないようにする等、セキュリティレベルを下げて申請してくる仕組みになっている。

（３）個人情報の利用（第三者提供を含む）

・グループでの共同利用はおこなっていない。責任の所在が不明確になるのが理由である。

・ポータルサイトを通じて提供するオンラインショッピングサービスにおいて、消費者が購買時に提供する必要のある個人情報は、店子と同社の双方が直接取得することにしている。消費者に対して、個人情報が店子と同社の双方へ情報提供されることを盛り込んだ約款を提示して同意を受けている。

・第三者提供クッキーなど、自社で取得した以外の情報は使用していない。

・年代・性別、IP アドレスレベルは個人情報ではないと認識しており、ターゲティング広告を実施する際に活用している。

（４）個人情報の管理

①情報の管理体制

（社員が使用している PC を専門チームにより常時監視）

・教育以外に、社員が使っている PC を監視下に置き、どの URL を見ているか、ネット上にどういう情報を流しているかを把握している。

・法務コンプライアンス部に監視チームがあり、3～4 人で監視している。情報が漏えいした形跡があれば、社員は上長、派遣社員は派遣会社、委託先は、業務委託先にヒアリングをおこなう。

（退職予定者は、特に厳しく監視・管理）

・退職が予定されている社員に対しては、情報の持ち出しが起きないように厳しく監視している。

・退職日の手続きに工夫をしており、出社最終日は人事部への手続きのみをおこない、自席に戻ることができない仕組みとなっている。また、できるだけ早く本人の社員アカウントを停止するようにしている。

・社員が退職する際は、秘密保持に関する誓約書を取っている。誓約書は入社時・新たな役職に就く際も取っている。同誓約書の有効期限は特に設けていない。
・自宅作業は原則禁止としている。ただし、技術者は VPN を活用して社内ネットワークに接続して作業することが認められている。外部から社内 LAN へアクセスする場合は、アクセス可能な領域は限られている。また、VPN 接続する際のワンタイムパスワードは所定の申請をおこない、CSO から許可が出ない限り発行されない。

（データセンター内をセキュリティレベルに応じて区分し、区分ごとに色分けしたベストを職員に着用させている。）
・顧客情報は特定のデータセンターに保管されており、同センターには警備員が配置され、金属探知機が設置されている。
・セキュリティレベルに応じて施設内の保管場所を区分している。職員は入場時に保管場所の区分ごとに指定された色のベストの着用が義務付けられており、区分を誤って入場している者がいないかを容易に判別できるようにしている。
・施設内には電話も印刷機も設置していない。顧客情報を一覧で表示できるようなツールや表は作成していない。
・2002 年から内部告発制度を設けている。内部だけでは対処の難しい部分もあるため、外部の法律事務所を活用している。これまで何件か報告はあったが、ノイズ程度のものしかなかった。
・内部告発制度は、制度の性質上、フィードバックの効果・結果を広めることができず、結果として利用実態が分かりにくい、という難点がある。今後は、ノイズ程度でも構わないので、報告障壁をさげるべく努力していく方針である。

②従業員従業者への教育方法
・試験付きの e ラーニングを全社員対象に四半期に一度ずつ、年四回おこなっている。試験結果は非公開にし、管理職へのフィードバックはしていない。
・個人情報に関しては年に一度 e ラーニング後に、全社員対象にして個人情報保護に関する誓約書を締結している。誓約書の文面は毎年大きな変化を加えてはいないが、全文熟読を指導している。書類は人事部に提出させており、契約の有効期限は特に設けてはいない。
・誓約書は文面を変え、派遣社員・業務委託先企業とも締結している。

③盗難対策

・特徴的な取組はなし。

④ノート PC の安全対策

・営業部門の職員は会社が貸与するノート PC を使用している。貸与するノート PC は半年に一度検疫を行っている。

⑤外部委託先管理

・「（４）②従業員従業者への教育方法」を参照。
・「（６）個人情報の監査」を参照。
・外部委託先には、選定基準を設けている。基準として ISMS やプライバシーマークの取得を必須の要件とはしていない。
・契約時に、個人情報保護に関する覚書を取り付けている。

⑥日常点検・確認の方策

・特徴的な取組はなし。

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

・保存期限はサービス毎に異なる。後日、問い合わせがある場合もあるため、サービス終了にあわせて削除することはしない。
・税務関係書類は、法定年限にあわせて保存している。
・顧客との契約にもよるが、紙面での保存は基本的にはおこなっていない。

（６）個人情報の監査

・監視システムは、半分は自社開発のものを、半分は他社の汎用製品を使用している。
・内部監査は、業務監査室がおこなっている。監査においては、規定の遵守項目が設置されている。
・委託先の監査は、委託した業務内容に精通していないと監査できないため、同社の現場社員が立ち入り監査をおこない、コンプライアンス部門が監査をすることはない。

（７）苦情処理・顧客対応

・顧客対応は基本的にメールで行っている。個人情報漏えい防止のため、顧客情報を見ることができる人の近くに電話は置いていない。

（８）事故発生時の対応

・事故はリンク切れなど小規模のものも含めて報告させている。事故の規模に関わらず、報告は全て管理職にメール送信される。

・事故報告のなかに個人情報漏えいがあった際は、事故把握・応急処置・事故対策を現場でおこない、法務部と広報部に伝達される仕組みとなっている。

・事故報告システムは業務監査室が管理しており、事故のレビューをおこなっているが、実際に事故のクライテリア付けなどをおこなうのは法務部である。

・監督官庁である経済産業省と総務省の両方に対して報告する。

以上