タ．情報サービス業（アウトソーシング等）　タ社

事業概要	モバイルサイトの構築、 モバイルサイトを活用したコンテンツ・広告配信		
従業員数	約 30 人	プライバシーマーク取得	あり
保有個人データ件数	約 300 万件(2008 年 10 月 28 日時点) 約 450 万件(2009 年 11 月時点)		

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

・顧客企業からの委託を通じて管理している情報は約 300 万件。同社で保有する情報の多くは本人から直接取得した情報ではない。
・個人情報の種類は、携帯メールアドレス・性別、居住都道府県などが挙げられる。
・個人情報の定義において、「携帯メールアドレス」は個人情報とみなされない場合があるが、同社では個人情報として管理・運用を行っている。
・個人情報は、メルマガの配信・景品発送・問合せ対応などを目的としている。
・従業者情報が 32 件、うちアルバイト 2 名分の個人情報を保持している。

（２）個人情報保護担当部署

・情報システム部から 1 名と、代表取締役社長、取締役 CTO を加えた 5 名で構成されたプライバシーマーク事務局が個人情報を担当している。情報セキュリティは代表取締役社長が担当しており、同事務局は月に一度定例会議をおこなっている。全員がその他業務と兼任しており、各人は個人情報保護業務について月に 1～2 日程度費やしている。

（３）個人情報保護管理者の有無・位置づけ

・管理担当役員が兼任している。

（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を 2006 年 8 月に取得した。
・個人情報を取り扱っているため、プライバシーマークの取得が取引上の前提となっている。

（５）個人情報保護に向けた取組経緯

・2006 年 8 月：　プライバシーマーク取得

・2008 年 10 月：　個人情報漏えい事件発生（後述）
・2008 年 11 月～現在：
　　社内タスクフォースとして「セキュリティ委員会」を設置し、セキュリティ対策（個人情報保護対策）を大幅に強化。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・モバイル広告業界においては、一般的に機微な情報の取得は行わない。基本的にバンドルネームを利用した覆面ユーザーが主体であるため、個人情報とみなされるのは「携帯メールアドレス」程度である。
・しかしながら、振り込め詐欺に誘引する悪質出会い系サイト等の業者に携帯メールアドレスの情報が流れると、同業者から大量の迷惑メールが送信され、実際に詐欺に至らなくとも多大な迷惑をユーザーにかけることとなる。
・一方、これら迷惑メールや、振り込め詐欺を取り締まる法規制が十分でなく、悪質業者の横暴に対処できていない。

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）

・役員と管理職全員のメンバーの計 7 名で構成されるセキュリティ委員会を設置。臨時メンバーとして、各プロジェクト担当者を必要時に臨時参加させている。同委員会では、個人情報のみでなくセキュリティ全般を議題として扱っている。
・2 月から 11 月までに 10 回近く実施した。委員会を設置した当初は月に 2 回おこない、まとまった資金が必要な議案を除いた、考えうる議案の多くは解決できた。現在は、月に 1 回実施している。

（セキュリティ委員会のメンバーに、セキュリティ改善点を 10 個以上見つけてくることを宿題化）

・各自がセキュリティ委員会において、10 個以上セキュリティ改善点を考えてくることを宿題にし、委員会を実施した。
・メンバーに改善案まで考えさせると躊躇してしまうと考え、宿題をセキュリティ改善点の洗い出しにとどめた。
・セキュリティ改善点への対応は、委員会メンバーから主担当と、期限を決めて実施し、2 週間後に進捗の報告を実施している。進捗はエクセルシートで管理している。

（２）個人情報の取得

・顧客企業からの委託を通じて個人情報を預かっている。個人情報の取得は全て顧客企業が主体となって実施している。

（３）個人情報の利用（第三者提供を含む）

・特徴的な取組みはなし。

（４）個人情報の管理

①情報の管理体制

（問合せデータベースは、独自 ID で個人を特定し、個人情報を不可視に）

・問い合わせデータベース検索において、同社が独自に発行する個人 ID を表記する仕組みとし、個人情報を一覧表示できなくしている。なお、以前は携帯メールアドレス一覧を表示していた。

・問い合わせ管理システムを導入し、細かな管理権限の制御を行えるようにし、必要最低限の内容のみ、共有できるようにした。

②従業員従業者への教育方法

・社員のセキュリティ意識の向上とセキュリティ改善点洗い出しのためにヒヤリハットを社員全員に 10 個ずつ挙げさせ、集約・共有している。これにより、自ずと新たなセキュリティ改善点が見えてくるという効果がある。

・3 ヶ月に 1 度の社員向け講習をおこなっている。

③盗難対策

・セキュリティカードを導入し、オフィス入退出に氏名と時間が記録されるように管理を行っている。

・キャビネットの施錠管理者を決めた上で、開閉時に台帳への記入を義務付けた。

・データベースに触る際は、氏名と「今から○○のデータベース触ります」、と宣言させることなどを徹底させている。

・CD や DVD の読み書き、USB ストレージの読み書きを、一部の社員を除いて原則として禁止している。

④ノート PC の安全対策

・事前申請を除いて、ノート PC の持ち出しは原則禁止。加えて、カードキーロック設定を施している。

⑤外部委託先管理

・個人情報を取り扱う外部委託先に関しては、十分なセキュリティ対策がなされているか調査を行なって「委託先調査報告書」を記載し、委託すべきかどうかを判定している。

（５）個人情報の消去・破棄

・顧客データベースと問い合わせデータベースの二種類を保有しており、それぞれで保存期間が異なる。
・顧客データベースの保存期限は顧客との契約次第ではあるが、基本的には契約終了後 1 ヶ月以内に削除をおこなっている。しかし、一部の個人情報についてはアフターフォローのために、契約終了後から 2～3 ヶ月後に消去している。
・問い合わせ対応データベースの個人情報は、最大で約一年間保存している。

（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

・次項「（８）事故発生時の対応」を参照。

（８）事故発生時の対応

※以下は、実際に発生した内部者の犯行による個人情報の漏えい事故（最大で約 182,000 件、携帯メールアドレス、ニックネーム、生年月日等）に関するタ社の対応記録に基づく。

（原因究明に迅速に着手し、顧客・警察・監督官庁へ連絡）

・出会い系サイトからスパムが送信されているという苦情が、同じ日に多くの顧客から寄せられ、携帯メールアドレスの漏えいの可能性に気づき、警察へ通報、当日夜から調査を開始した。
・最初に、どこのサーバ上のどこの企業の顧客の情報が流出したか調査した。その結果、原因までは分からなかったものの、管理画面に不正アクセスと思われるログが発見された企業があり、同社が事故を起こした可能性が高いことが判明した。
・翌日、同社は顧客と警察に漏えい事故発生の可能性を連絡。主務官庁等へは先ず顧客が連絡し、その後同社から連絡した。
・二日後、アクセスログ結果より、警察の要請に基づき、インターネットプロバイダーに協力してもらい、アクセス元を調査したところ、繁華街のインターネット喫茶から同社のサーバにアクセスされていることが判明し、事故であることを特定した。
・その後、同社ホームページで漏えい事故が発生したことを公表。顧客企業のユーザー

には、顧客企業がそれぞれ連絡した。同社は、顧客企業よりも先に公表できないことから、公表のタイミングを調整する必要があった。

（事故後１ヶ月間、役員が交代でコールセンターを深夜まで運営）

・事件公表から約一ヶ月間、同社内に事故対応のコールセンターを設置し、電話とメールで応対した。
・受付日時は、土日関係なく、朝 10 時～26 時（深夜 2 時）まで。
・体制は、基本的にすべて役員が交代で対応した。社員にはほとんど対応させなかった。
・対応を始めて一ヶ月が経過してからは、コールセンターに委託したが、二次的にエスカレーションさせて同社にも繋がる体制を整えていた。
・顧客企業と調整し、事故に関するユーザーからの連絡はすべて同社で受け付けるようにした。これにより、被害にあったユーザーが、たらいまわしされることなく、均質の応対をうけることができるようにするためである。
・スパムを完全に停止させるためには、メールアドレスを変更していただくしか方法はなかったため、ひたすらお詫びを申し上げた。
・クレームの受付は、メールが 1,000 件、電話が 300 件で、メールが圧倒的に多かった。

以上