ソ．情報サービス業（ソフトウェア）　ソ社

業務概要	パソコンや関連周辺機器等のハードウェア、ソフトウェア、IT 関連製品等の卸売の販売および関連するサービスの提供		
従業員数	約 500 人	プライバシーマーク取得	あり
保有個人データ件数	約 1,000 万件		

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

・約 1,000 万件を保有している。
・卸ビジネスが中心業務であるため販売店が顧客である。ただし販売店の先のエンドユーザー（ほとんどが企業である）に直接送付することもあり、エンドユーザーの個人情報を取得することもある。結果として保有個人情報件数は非常に多くなっている。
・卸先企業が約 4,000 社、仕入元企業が約 2,000 社程度ある。顧客企業が全国展開していると、支店や支社も非常にたくさんあり、それぞれに担当者がいることも保有個人情報数が非常に多くなっている理由である。
・基本的には一度保有した個人情報は消去していない。
・個人情報の件数については、概算では把握ができる、ということであり、詳細件数まで正確にすぐにわかるわけではない。重複している情報がある可能性もある。
・社員情報・採用情報
・取引先情報、受注情報、発注情報、出荷情報、見積情報、注文書、各種申請書、各種問い合わせ情報
・営業部門：商品・サービスに関する情報の提供、提案、問い合わせ、依頼等の対応、その他
・仕入部門：商品の保守内容確認、品調達などの連絡、問い合わせ、その他
・管理部門：基幹システム登録のため、採用活動、その他

（２）個人情報保護担当部署

・各部署に責任者を設置している。役職としては基本的には部長である。
・個人情報保護委員会が常設されており、事務局は CSR 室内の PMS 事務局が担当している。
・委員会は随時で開催されておりメンバーは固定されている。組織変更実施時などは経営会議に併せて実施し、規程変更時や問題が発生した場合にも開催している。

（３）個人情報保護管理者の有無、位置づけ

・管理部門長である取締役が担当。

（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

・2006 年 10 月にプライバシーマーク（JISQ150001:2006）を取得した。取得の目的は法令遵守、顧客からの信頼確保である。

・取引先の数社が認証取得を契約の条件にしているとことがあるが、ごく稀である。

（５）個人情報保護に向けた取組経緯

・個人情報保護法施行直前に個人情報保護体制を作ろうという計画があった。

・しかし、同時期に会社の合併や合併に伴うシステムの不具合が一時的に生じるなどして順調には進まず、プライバシーマークの取得も想定より遅れた。

（６）個人情報の保有・管理・提供等に関する業界等の特徴

・IT 関連製品を取り扱っているため、個人情報（データ）の取扱いとセキュリティ対応には厳しい業界である。

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）

・漏えい事件後に、事故の教訓を元に、特にセキュリティに関する部分は禁止事項を設けるなど、詳細化した。

・プライバシーポリシーの第三者提供に関して詳細に記載している理由は、仕入元企業からエンドユーザーの個人情報の提供が求められることがあるからである。セキュリティに関するコンサルティング会社のアドバイスを受けての対応である。

（２）個人情報の取得

・個人情報の取得に当たって、取引先担当者等から同意を取得することは、数千社の取引先があるので、業務に著しい支障になり、コストがかかる。このため、プライバシーポリシーに詳細に記載することで対応している。

・外部向けセミナーなどで参加者にアンケートを書いてもらうような場合は、記名をできるだけ求めないようにするなど、個人情報の取得そのものを抑制している。

（３）個人情報の利用

・できるだけ個人情報は取得しない、持ち出さない、利用しないという方針で実施している。

・共同利用も行っていない。

（４）個人情報の管理

①情報の管理体制

・現場では個人情報を極力取り扱わないようにした。
・サーバへのアクセス権もフォルダ単位で設定・管理を行っている。
・USB メモリについては指紋認証などがないものは持ち出しを認めていない。
・携帯電話はパスワードロックが 1 時間ごとに自動的にかかるようになっている。

②従業者への教育方法

・年に一度は必ず全従業員に教育をしている。漏えい事件の発生により、従業員の意識は高まった。
・集合研修の際には、漏えい事件を実際に発生した例として使用している。

③盗難対策

・事務所内は IC カードで認証しなければ入れない。
・高度な個人情報を扱う区画には特に権限が付与された者以外入室できない。

④ノート PC の安全対策

・持ち出しは原則的に禁止しており、持ち出し可能なパソコンには、データが保存できないようにしている。
・個人使用のパソコンの持ち込みも禁止している。持ち込んでも、同社の LAN には接続できない。

⑤外部委託先管理

・外部委託の選定の際には、信頼性の高い企業と取引を選別するために評価シートを使用している。
・外部委託開始時には、委託先を訪問して、相当程度詳細なインタビューを実施した上で、個人情報保護に関する対応体制について確認するようにしている。

⑥日常点検・確認の方策

・各部署は年に 2 回、自己点検を実施している。
・問題があった場合には自分たちで対応・修正することとしている。

⑦初歩的ミスの防止策

・メールは、送信時に必ず送信先のアドレスを確認する画面を表示するように設定して

いる。
・特に外部送信先については、送信ボタンクリック後、“送信対象者リスト”が表示され、個々人にチェックボックスが出る。チェックボックスにチェックを入れなくては送信できないため、必ず確認した上で送信するようになっている。これにより、CC に誤った人を含めてしまうことなどを防止している。

（５）個人情報の消去・破棄

・紙の個人情報についてはシュレッダーにかけ、メディアは全て破砕処理している。
・機密情報は溶解処理を委託している。

（６）個人情報の監査

・年に 1 回の JIS で求められている監査を実施している。

（７）苦情処理・顧客対応

・開示請求も無く、個人情報についての問い合わせなども無い。

（８）事故発生時の対応

※以下は、実際に発生した EC サイトのセキュリティ脆弱性を攻撃されたことに起因する個人情報の漏えい事故（1 万数千件、クレジットカード、電話番号等が漏えい）に関するソ社の対応記録に基づく。

（郵送、メール、電話の順に連絡手段を使い分けて全顧客へ、いち早く連絡することを優先）

・事故発生を認識した当時は、誰が何をしたら良いか全く分かっておらず、“エンドユーザーも含む利害関係者に説明を行うこと”を最優先とすることにした。この判断は社長によるトップダウンの判断であった。
・告知文の作成と連絡対象者のリストの作成後に全ての顧客向けに書簡を送付し、記者会見を実施。翌日には新聞 5 紙に漏えい事件発生についての謝罪広告を掲載した。
・全顧客に書簡で、個人情報の漏えいの可能性を伝える書簡を郵送した。数%は宛先不明で書簡が戻ってきた。特にオンラインで商品をダウンロードして購入した顧客に連絡をつけるのが難しかった。理由はダウンロード購入の場合、商品の発送が伴わないため、登録された住所に不備が多かったことによる。住所不明の顧客には、同じ内容のメールを送付した（メールアドレスは確実に把握していた）。それでもメールが戻ってきた場合は、電話番号がわかるときには電話をした。残り数百名分はどうしても連絡がつかず、ホームページへの掲載などで対応した。
・顧客向けの告知後に、外部委託先企業内にコールセンターを設置した。一次対応は外

部委託先で実施し、対応が難しい質問については、同社に質問が上げられてくるようにして対応した。
・コールセンターには一番多い日は数百件/日のコールがあったようだが、2 ヶ月弱でほとんどコールはなくなった。告知後 1 ヶ月以内のコール数が非常に多く、その後は漸減した。

（顧客からの問い合わせの蓄積により、顧客の知りたいこと、顧客に伝えるべきことを整理し、的確な対応を実現）

・当初はいち早く漏えいの発生を顧客へ伝達することを優先したため、コールセンターでの想定問答などの検討・作成が十分でなかった。このため、当初の問い合わせには十分に回答することができなかった。顧客への対応は公表前にもう少し検討したほうが良かったようにも思うが、逆に顧客からの直接の問い合わせ内容を聞かないと、何を顧客に伝えなくてはいけないのか、ということについてはわからなかったとも考えている。
・なお、漏えいの状況や原因は十分には解明されず、全て結局は「可能性がある」という調査結果で終わってしまったため、追加で有益な情報提供ができなかった。

（ASP サービスを利用している場合でも、バージョンやカスタマイズ状況によっては自社が利用している ASP のみ脆弱性に問題があることがあるので確認が必要）

・サイトの運営は外部企業に委託を行っていた。ASP による EC サイトの運営、コールセンターでの対応も含めて委託を行っていた（外部委託先企業は EC サイト運営、コールセンター運営も独自の事業として実施していた）。
・なお、この外部委託先の ASP を利用していたのは同社以外に 50 社程度あったが、実際に被害にあったのは同社だけであった。同社の EC サイトのための ASP だけがバージョンが古かったことが原因のようであった。「SQL インジェクションには対応済み」というようたい文句に安心していたが、実際には脆弱性があり、SQL インジェクションを許してしまったようであった。

（顧客に生じた損害と同社の EC サイトからの漏えいの因果関係が明確にならない場合には保障は実施せず）

・顧客への金銭的補償やそれに類する対応は行わなかった。同社のサイトからの漏えいと顧客に生じた損害の因果関係が明確に証明された場合には何らかの補償を行おうと考えていたが、実際には因果関係が明確になった例はなかった。
・例えば顧客から「漏洩後にスパムが非常に増えた」というクレームもあった。いつ、どの ID が漏えいした可能性がある、ということまではわかったので、調べたところ、顧客の「スパムが増えた」というタイミングと、実際に ID が漏えいしたタイミングが

ずれていたので（スパムが増えたのが ID の漏えいより前の話であった)、その点を説明して理解していただき、補償などは行わなかった例もあった。

・外部委託先は事故を自社の問題として捉え、全ての問題について同社に歩調をあわせてプレスリリースを行った。同社がプレスリリースをホームページに掲載している間、外部委託先もプレスリリースを取り下げることはなかった。

・広告宣伝費用、顧客向けの書簡発送や対応費用などは同社が負担し、コールセンターの運用は外部委託先が負担した。

（既存取引先には個別に資料を作成し、営業担当が訪問して信頼を維持）

・既存の取引先の顧客からは「他の関連サービスは大丈夫なのか」という問い合わせがあったので、他のシステムやサービスが安全である旨については、個別に説明資料を作成して、問題のあったサービスとは独立しているということについて特に明確に説明した。BtoB ビジネスが中心であったので、営業担当が説明して回ることで、納得してもらえた部分が大きかった。

（外部委託先の独自調査だけでなく、コストはかかっても、専門性の高い企業に漏えいの可能性についてのセカンド・オピニオンを求めることが有効）

・クレジットカード会社からの指摘を受け、最初は外部委託先に事故の可能性について調査を依頼した。この結果、「問題がなさそうである」という報告があったので、EC サイトの閉鎖までは考えなかった。このため、事故発生を認識するのが一層遅れてしまった。

・クレジットカード会社からさらに指摘を受け、同社が推薦する調査会社に委託したところ、10 日程度で調査結果が出て、漏えいの可能性のあることが明らかになった。

・その後、関係者の要望に合わせてさらに複数の調査会社に委託して調査をしてもらったが、調査結果は同じになったので、この調査結果が信頼できるということがわかった。

・最終的には EC サイトで保有していた個人情報は、ハードウェアの物理的な破棄も含め、完全に削除した。顧客から「データ削除ではなく、ハードウェアの破壊を含む完全削除をしてくれ」、という要請があったことが理由である。実際には、漏えい事故発覚の翌年の 12 月に削除を行ったが、本当に物理破壊まで行うべきなのか、このタイミングはいつすべきか、ということについては判断が難しく、未だにそれで良かったのか、ということは気になる。

・ASP サービスであり、個人情報の保有主体は外部委託先であったので、外部委託先と協議した上で物理的削除を実施した。外部委託先は（ハードウェアの）物理的破壊を行い、その証拠写真を提出した。

以　上