チ．情報サービス業（E コマース） チ社

業務概要	e コマースサイトの運営（サイト構築、通信販売実施等）		
従業員数	約 60 人	プライバシーマーク取得	なし
保有個人データ件数	約 437,000 件		

１．個人情報保護に関する概要

（１）保有個人情報件数、種類、利用目的

・3 つの e コマースサイトを運営しており、会員数の合計が 43 万 7 千件である。

・漏えい事故（同社のサーバが外部からの侵入を受け、数十万件の個人情報が流出の可能性）が発生した際には保有個人情報件数は約 65 万件であった。会員登録していただいて個人情報を持つという仕組みにしている。会員登録せず非会員でも買い物は可能。発送用データとして保管していた。しかし、漏えい事故後、できるだけ個人情報は保有しないようにしよう、という方針の下、発送用データは 1 ヶ月程度だけ保有した後には破棄するようにしたので、保有個人情報数が減少した。

・漏えい事故発生時には、顧客からも個人情報の削除依頼があったので数百件の保有個人情報を削除した（正確に計数したものではなく、あくまで大体の感覚である）。

・ユーザ ID、パスワード、氏名、e メールアドレスまでが登録時の必須項目である。住所などは実際に購入した場合にはじめて入力することになる。

・「家族構成コード」は任意登録項目である。予めプルダウンで類型が用意されている。

・漏えい事故前後で利用目的の記載方法に特に変更は行っていない。利用目的の提示方法や内容が事故に繋がったとは考えていないからである。

・TRUSTe 取得の際に審査があり、そのタイミングで指摘をもらって修正した。今は、年に一度 TRUSTe のチェックを受けているが、利用目的の提示については、最近は特に問題点を指摘されないようになっている。

（２）個人情報保護担当部署

・部署によって扱う個人情報は様々である。例えば経営戦略室は株主の情報を保有しており、e コマースについてはオペレーションサービス部という接客部署で顧客情報を扱っている。その他、バイヤー部署もあり、そこでは取引先企業の情報の一部として個人情報を保有している。

・個人情報を保有する部署は、その部署長が責任を持っているということにしている。

・管理本部システム部長が社内の情報資産の全ての管理責任を負っている。但しこれは個人情報に限定しているわけではない。CISO（Chief Information and Security Officer）という役割を担っている。なお、システム部長であるということから、この

役割を担っている（役職に基づいて役割が付されている）。
・セキュリティ委員会が設置されているが、この委員会には決定権は無く、決定権があるのは取締役会である。会社および各事業部がセキュリティに関する方向性について助言・指導を行うのがセキュリティ委員会の役割と位置付けられている。
・セキュリティ委員会はシステム開発部長、代表取締役社長、システム部長、経営戦略室長と、社外のアドバイザーなどが中心メンバーであり、適時、適切な人材を入れて運営している。
・セキュリティ委員会は月に 1 回、定例で開催している。但し、決めなくてはならないことがある場合には、必ずしも定例を実施するタイミングでなくとも随時開催している。

（３）個人情報保護管理者の有無、位置づけ

・各営業本部部長である。事業実施者の長であることから、営業本部長がその任にあたっている。
・個人情報部門責任者は各部門長ということになっている。
・個人情報保護管理者、個人情報部門責任者については、その管轄下に置かれる社員スタッフの教育などが重要な部分を占めると考えているため、組織的に営業本部ごとに動くという形をとっている。現在の規模であるから可能という部分はあるので、今後、企業が大きくなっていくに従って、見直しの可能性もある。
・「監査責任者」は管理本部長が実施している。

（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

・2004 年 5 月に TRUSTe を導入した。顧客への信頼の証として導入した。当時は社長が主導して導入した。社内を大きく動かしたわけではなく、一部の関係者が関与して取り組んだという進め方で導入した。
・漏えい事故発生当時は、顧客の利便性を損ねないよう自社でクレジットカード情報の保有を前提に、セキュリティを強化することを考え、クレジットカード業界のセキュリティ対策基準である PCI-DSS をまず取得しようということを検討した。しかし、多額のコストに加え、取得までの準備期間が半年程度要することが判明した。また同タイミングで、クレジットカード決済会社より、クレジットカード情報を持たずとも顧客の利便性を損なわないサービスの情報を受け、即時利用を決定した。これによりそもそもクレジットカードを保有しない方針に切り替え、クレジットカード情報を持つことを前提とした PCI-DSS の取得は取りやめた。
・クレジットカード情報は持たずとも個人情報等、情報資産は継続して有することになるため PCI-DSS を参考に、社内で E コマース事業を行う視点から独自のデータセキュリティ基準を策定、現在対応にあたっているところである。

・漏えい事故発生後に、プライバシーマークと、ISMS の取得の検討を行ったが、まずはステップとして、PCI-DSS を参考にした E コマース事業者向けの独自のデータセキュリティ基準の準拠を先行することとした。プライバシーマークと、ISMS はその後の検討課題としている。情報管理に関して PDCA サイクル等を勘案して社内体制の構築や運営を行うために独自の基準を策定した。今は、この独自基準に沿って社内業務の落としこみ、セキュリティ対策を行おうとしているところである。
・プライバシーマークなどに対する対外的効果の有無はまだ考えておらず、独自基準の策定・普及以降、もう一度考えるということになると考えている。
・e コマース事業者のセキュリティへの取り組みはまだ業界として意識が高い訳ではないと考えている、当社で独自に策定したデータセキュリティ基準を他の事業者にも使っていただくなどして、啓蒙できないかと考えている。
・アジア、太平洋のトラストマーク付与事業者が集まって各国のトラストマーク認識を地域から国際的なものへ高めるための国際提携機関がある（ATA：Asia Pacific Trustmark Alliance）.日本では株式会社 TradeSafe（http://www.tradesafe.co.jp/）が参加している。TradeSafe は EC ショップの会社概要やサービス内容を審査・認定する、日本で唯一の第三者認証機関。漏えい事故発生時にお客様の失った信頼を回復するために、第三者の認証を受けるために同サービスを導入した。TradeSafe は売買契約の事故発生時にお客様へ補償を行うようにしているのが特徴。

（５）個人情報保護に向けた取組経緯

・事故発生前には、個人情報に対する取組は、e コマースの事業者の中では相当にやっている方だというつもりであったし、結果的には侵入に対する適切な措置が足りなかったということだと認識している。
・事故発生前の取り組み事例としては、クレジットカードの下 4 桁をデータベースに保存せず、お客様へは下 4 桁を都度入力していただく工夫等を行っていたが、結果的にはクレジットカード保有そのものをやめようという判断を行った。事故発生時にお客様に最も直接的な被害を与えることになりうる情報であるため。
・事故以降、信頼回復に努めなくてはならないといけないと考えている。セキュリティへの投資は行いつつ、できるだけ顧客への利便性を下げるような負担は掛けないようにするような取組を意識している。

（６）個人情報の保有・管理・提供等に関する業界等の特徴

・e コマース事業を実施している以上、顧客に面倒な負担は掛けられないと考えている。毎回顧客に個人情報を入力してもらうのであれば、それがセキュリティ的には最も良いのだろうが、e コマースという世界においては、それは期待できない（顧客の利便性を著しく損ねることにつながり、選ばれる e コマースサイトにならない）。

・商品の発送、決済等、インターネットにおける通信販売という業態のため、顧客の個人情報を預かる必要がある。返品等の対応のため、販売終了後も一定程度保有する必要があるのも一般的特徴と考えられる。

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）

・セキュリティ委員会でルールは定めている。素案はシステム部で策定している。
・今でこそ、自社独自の基準が策定されており、それに対する対応策を細かく実施できているが、平行してリスクアセスメントを実施した場合に、どこが弱点か、ということをセキュリティ委員会で考えながら対応を進めている。
・対応については、顧客の声によって突発的な対応を行うこともあるし、社内で検査を実施していて見つかったことについて対応することもあるし、一般的に（そのような手法や対策が）普及している、という理由で取り入れるものもある。
・新しいルールなどはイントラネットにまず掲載する。なお、都度、スタッフがやらなくてはならなくてはならないことは、部門長が指示している。
・グループウェアは非常に利用しているが、口頭での対応も同時に非常に重要であると考えている。「口頭で言ったことも書かなくてはいけないし、書いたことも口頭で言わなくてはいけない」ということは口を酸っぱくして依頼している。
・ルールを作った理由をしっかり伝えることに重点を置いている。

（２）個人情報の取得

・個人情報の取得方法は特に漏えい事故後に変えた、ということはない。
・その他に、顧客のパスワードの文字数の制限（最小文字数）を増やすなどの対応を行った。
・顧客側でのパスワード変更について、漏えい事故発生後、最初にログインする際に、ログインパスワードの変更をお願いした。

（３）個人情報の利用

・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

・入室・退室管理は IC カードで行っている。
・個人情報を扱う接客部署は担当の 10 名の方しか入れないことになっている。どうして

も入らないとならない場合は、接客部署の人が同席しないと入れないことになっている。
・サーバ室については、監視カメラを設置している。施錠もしているが、二重の監視措置と考えている。
・資産管理ツールを入れて、操作ログを全て取得している。これは全社員にその旨伝えており、不適切な行為の抑制効果もあるのではと考える。但し、有事のときのためのものなので、クリッピングまでは実施していない。
・個人情報のアクセス制限については、接客部署以外は顧客情報を見られないようにするなど、部署ごとにアクセス権限設定を管理している。現場からは個人情報が扱えないと不便であるという話はあるが、これは内部統制対応として、致し方ないことであるとして対応した。

②従業者への教育方法
・会社全体での集合研修などは実施していない。各部単位での研修はある。
・接客部署については個別に集合研修を行い、漏えい事故の経緯などについて話をし、顧客がどのような質問や苦情を連絡してくるか、その場合の対応をすべきか、ということについて伝えている。
・接客にあたる者は 10 名程度であり、7 名は正規職員、3 名は契約社員・派遣社員である。
・会社全体では漏えいに対しての意識は上がったが、新人や中途職員に対する教育は課題であると認識して進めている。

③盗難対策
・サーバ室には施錠をしており、監視カメラをつけている。

④ノート PC の安全対策
・社外に持ち出すパソコンは社内ネットワークに接続させないルールにしている。ルールブックに定めている。
・社外に持ち出すに当たっては、情報資産は持ち出さないということ、持ち出す場合には承認を得るようにしている（実際には社内ネットワークに接続せずに業務が遂行できる人もいる。むしろ社外取引先用ネットワークでインターネットだけできるようにしている）。
・資産管理ツールなどで、余計なソフトが入っていないかをチェックするようにしている。ウィニーだけでなく、スカイプ等のメッセンジャーソフトも禁止になっている。Web メッセンジャーについては、ブラウザで利用するのであれば許可するということで不便さを補っている。

⑤外部委託先管理

・システムであればネットワーク保守の会社、セキュリティコンサルタント、配送会社が委託先ということになる。
・NDA（秘密保持契約）は必須で交わしている。データをやり取りする際の規定がある。配送会社から NDA を交わすことが嫌われ、それが理由で契約を拒否される、というような話は聞かない。データとして個人情報を渡している。但し、同じ配送会社であっても支店によって対応が違うということがあるようである。
・ルールとしては、委託先の選定基準のようなものは作成している。

⑥日常点検・確認の方策

・そこまで積極的な活動は実施していない。
・80 人程度の企業規模なので、各部署の責任者がチェックできているのが現状である。

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

・注文・出荷に利用したデータで、発送１ヶ月経過したデータについては個人情報を特定の文字列に置き換えたり、削除したりする。会員登録いただいたデータはパスワードをスクランブル化したりして通常ではわからないようにしている。
・クレジットカード情報及び決済業務は、カード決済会社に委託し、自社でデータとしては持たないようにしている。

（６）個人情報の監査

・半年に 1 度ずつ監査を実施している。内部統制のために年に 1 回の監査実施が求められているので、その監査の一部として実施している。
・内部監査は今後実施していきたいと考えている。

（７）苦情処理・顧客対応

・運営サイトの顧客向け接客部門があり、個人情報問題を含む全ての顧客対応の窓口となっている。
・また、日々の CS 向上のため、横断的なプロジェクトである「お客様の声活用委員会」を設置している。

（８）事故発生時の対応

※以下は、実際に発生したシステムの脆弱性に起因する外部からの不正アクセスによる個人情報の漏えい事故（約数十万件のクレジットカード情報等が漏えい）に関するソ社の対応に記録に基づく。

（顧客対応として、「迅速なお知らせ」よりも「適切な状況把握」と「対応策の実施」を優先することで、混乱と二次被害の発生を防止）

・顧客の個人情報が取得されていた可能性があることがクレジット会社からの調査依頼により発覚した。結局、数十万人分の情報が漏えいした疑いがある（うち、クレジットカード情報を含む情報は数万人分）。
・翌日より、まず「対策本部」を設置し、次いで「封じ込め（拡大防止）」を開始し、その後「分析・追跡」に 2 週間程度を要した。その後、対策改善を行い、顧客からの問い合わせ窓口も設置した上で「公表」を行った。
・いち早くお客様に漏えい事故の発生をお伝えすることとのトレードオフで、正確な被害状況把握のために公表まで精査期間を設けたことが、自社でリスクを感じながら採用した方策である。
・社内体制としては、役員と経営戦略室が「方針指導」、「公表」の対応を行い、システム部が「封じ込め」、「分析・追跡」、「対策改善」を担当し、オペレーション部が「窓口設置」を、更に残りの全スタッフも「顧客対応」に協力した。
・結局、公表までタイムラグが 1 ヶ月程度発生したのだが、それは顧客向けコールセンターの設置や原因・現状等を明確にし、公表時にお客様にきちんと説明責任をはたせるようするために時間が必要であったことが理由である。
・お客様からはなぜ早く公表しなかったのかというご意見をかなり頂戴したが、体制が整わないまま公表していれば、お客様に正しい情報を伝えられずかえってご迷惑をおかけしただろうと思われる。
・外部アクセスができる状況になっていることが最大の問題であったので、Web システム上のカード情報をバックアップして消去し、最終的にはサイトでのカード決済を一切停止した。
・調査の間も、クレジットカードの利用だけは止めていた。その点は顧客にはまだ公表できる状態ではなかったので「システムメンテナンスのためにクレジットカードは利用できません」ということで回答していた。
・社内でも漏えいが発生したという情報について対応に当たるスタッフはごく限定し、社内の動揺を誘わないようにしていた。

（外部リソースの有効活用により、迅速で適切な対応を実現）

・問題発覚後、セキュリティ調査会社にすぐに連絡し、対策を相談した。
・社内だけでは対応しきれないと判断し、日常的にサイトの構築などで付き合いのある

システム会社の社員２名に同社に来てもらい、対応体制を整えた。
・システム上の脆弱性の修正のために、リモートで支援を行う協力会社の 12 名と、同社のシステム担当の 4 名が 3 日間、ほぼ 24 時間体制で対応を行い、脆弱性の修正にこぎつけた。
・コールセンター会社に、対応のための体制構築を依頼し、120 名程度の対応チームを設置してもらった。コールセンターに対しても、お叱りや苦情だけでなく、多くの応援もあったようであり、コールセンターからも珍しいケースだと言われた。
・コールセンターは 2 ヶ月程度利用した。120 名体制でスタートしたが、苦情や問い合わせが減少するに従って、オペレータの数は減少させるようにした。
・コールセンター会社も積極的に事態収拾に関与してくれた。同社と一体的に対応のための体制や方法を検討した。その際の「個人情報漏えい時の緊急対応体制構築支援」のようなものは、コールセンター会社の標準営業資料として活用されているようである。
・初日のコール数が 1,400 件、メールが 700 件であった。最終的な顧客からのクレーム数については、対応したコールが 6,400 件、メールが 6,000 件であった。
・同社では業態からしてメインはコールセンターに電話対応をしてもらっていたが、加えて単純な回答が可能なメールへの対応も依頼していた。
・コールセンターで対応しきれない電話は当然ながら同社に転送されたが、漏えい事故発生直後の 1～2 週間は毎日 100 件程度の電話が転送される状況であり、結局毎日社員の 10～15 名で電話対応に当たらなくては対応できなくなった。なお、メール対応を行う部隊は別に設置し、10 数名程度で対応した。
・なお、この問い合わせ対応は午前 9 時～午後 5 時に開設していた。
・機械類・ネットワークの新たな導入などに際してはサイトそのものの運営を停止しないといけないので、スケジューリングなども苦労した。
・ブランドカード会社からの指示については、迅速にその指示に従って対応したことが先方の信頼を失うことなく対応することができ、問題が大きくならずに済んだポイントではないかと考えている。

（過大な報道による風評被害・混乱を防止するため、敢えて大手新聞社に事故情報を詳細に説明して正確な情報を報道してもらう）

・IR や PR も掲載したが、その内容がそのまま顧客や社会に伝わるかは非常に不安であった。そこで、特定の大手新聞社に対して同社から情報を提示し、先に取材してもらって、できるだけ間違いがないように報道してもらえるような工夫を行った。
・当然に新聞社の原稿であるので、掲載前に記事を確認させてもらうことはできなかったのだが、一部は少し過大に書かれた部分もあったものの、間違いが少なく報道してもらうことができた。特定新聞社にリークしたことで、その会社が一番詳細に漏えい

事故の情報について報道することができ、結果として他の新聞紙よりも耳目を集め、IR や PR の趣旨を損ねることなく、正確な情報を伝えることができたと感じている。

（事故後、顧客の声を聞くためのアンケートや掲示板等の設置で信頼回復に尽力）

・事故以降、新たに顧客の声を聞くためにアンケートを設置した。専用のブログ的に Web 上で情報を双方向でやりとりできる仕組みを設置した。顧客の声を取り入れながら、個人情報問題やその他 CS についての対応を考えていくようにしたのも 1 つの工夫である。事故当時はお叱りもあったが、励ましの言葉も多数あった。E コマースはお客様によって支えられる事業であることを痛感した。

アンケートに寄せられた指摘については、必ずしも 1 つ 1 つに回答しているわけではないが、ある程度溜まった段階で、回答レポートのような形でまとめて資料をブログ形式で掲載している。

以　上