ア．製造業　ア社

事業概要	化粧品製造など		
従業者数	約 3,500 名	プライバシーマーク取得	あり
保有個人データ件数	800 万件		

１．個人情報に関する概要

（１）保有する個人情報の件数、個人情報の種類、個人情報の利用目的

・会員カルテは 800 万人分保有している。但し、名寄せは明確には行っていない。
・それ以外にインターネット会員の個人情報がある。カルテの会員とインターネット会員には一部重複者もいると思われるが名寄せはしていない。
・その他、クレーム・問い合わせによる個人情報がある。これらはクレームや問い合わせの内容について記録しているものなので、氏名・連絡先は必ずしも含まれていない。
・会員カルテには、氏名、住所、電話番号に加え、肌の状況、家族の構成などが含まれている。ライフスタイルに合わせた提案を行うために、職業なども含まれている場合がある。また、購買履歴なども含まれている。（これらの項目についての登録を無理にお伺いすることは無い。）
・直販は行っていないので、銀行等の口座情報・クレジットカード情報などは含まれていない。
・機微な情報としては、アトピー体質、アレルギー体質といったことは情報として含まれている場合がある。販売員のコメントが含まれている。
・会員カルテの情報は、カウンセリングやサービスの提供、新製品やイベントの案内、マーケティングなどの統計分析、会員情報の管理などに活用している。
・ネット会員の情報は、新製品やイベントの案内、ネット会員サービスの提供、サンプル等の送付、マーケティングなどの統計分析、会員情報の管理などに活用している。

（２）個人情報保護担当部署

・総務部の CSR 室が担当している。
・昨年度までは 5 つの委員会が存在していた。個人情報保護、企業倫理、CSR、技術品質などの委員会である。これらは内容が重複する場合もあり、本年度から CSR 委員会に統合し、個人情報保護担当部署も CSR 室ということにした。
・コンプライアンスの問題は「基本的な CSR」という理解であり、義務的にやらなければならない内容を扱っているという認識である。
・総務部で機密情報管理を行っていたこともあり、合わせた方がやりやすかったことも理由の１つである。

（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がいる。総務部長であり、職位は執行役員である。

・個人情報保護の業務を所管する部署の担当トップが個人情報保護管理者になる、ということである。総務部長だけがなるとは限らない。

（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 2003 年 4 月に取得した。

・プライバシーマークは整備する際の雛形が与えられるということであり、監査が入るということで常に実践を継続するということで、社内統制引き締めに有効だと考えられたからである。

・ISMS は業務の一部で取得している。取得時期は 2005 年 3 月である。具体的には、会員カルテのデータをオンラインで管理しており、そのシステム管理について ISMS を取得している。

・ISMS は情報企画部というシステム部門が担当している。公表して社内や外部に伝えるということは行っていない。規格を利用して業務を組み立てることが第一の目的であり、営業等に活用することは現時点では考えていない。

（５）個人情報保護に向けた取組経緯

・2002 年の 11 月に P マーク取得体制を立ち上げた。顧客に対するアピールなどがしていけるということが後からの理由で付いてきた。

・プライバシーマークは 2003 年 4 月に取得した。

・取組みの目的としては、顧客に対しては「個人情報保護に敏感になっている顧客の声に対し、いち早く対応することで、安心感を高める」ことであり、取引先については「IT を活用した新しい顧客サービスの展開に向け、情報流出の不安を払拭し、店舗からの信頼を勝ち取る」ことであり、株主に対しては「倫理上からも、社会規範を守ることは、消費者・取引先のみならず投資家・株主の信頼感を得ることにつながる」、社会に対しては「リスクマネジメントの一環として、法制化に向け先手を打ち、体制を整備する」、社員に対しては、「情報セキュリティに対する社内の意識啓発と管理体制の強化を図る」ことである。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・化粧品業界と言っても、売り方はさまざまである。販売会社の社員や契約社員をカウンセラーとして販売現場に送り込む場合もあるし、テナント入居しているテナントの従業員が販売を担当する場合もある（ドラッグストアや GMS もあり、商店街などの路面化粧品店など）。後者の場合は他の会社の従業員の個人情報の取り扱いについて依頼

の形で口を挟むことになり、容易ではない。
・カルテは直営店ではない店頭においてあるということになる。物理的なカルテ管理は取引先に一任している、という形になっている点も特徴である。
・情報はオンラインとして同社のサーバでも管理しているので、「販売店の情報である」ということには完全にはできない。そこで、共有情報ということで販売店と共有して活用している点も特徴である。
・自前の情報だが他人に預けている情報の管理が困難である。
・より適切な管理を実現するために、店頭情報機器や、個人情報を管理するためのツールについては、一部は販売会社が提供したり貸与したりしている。
・貸与を行っているため、店舗にはある程度、同社の端末が設置されている。専門店はいろいろな規模の専門店があるので、端末がおいていない店舗も存在している。

２．個人情報の適切な保護のための取組について

（１）準備（規定・体制づくり）

・規程は担当部署が作成してトップダウンで遵守してもらっている。
・監査の際に、「この規程は周知徹底がなされていない」ということを監査対象部門から指摘を受けることがある。規程の改定は開始以来、3 訂目となっている。
・事業所ごとに情報管理責任者を配置している。本社関連会社で 130 名、販売会社では 70 名くらいとなっている。200 名ほどの情報管理責任者を配置している。事業所責任者が情報管理責任者である（支店長、部門長などが担当している)。
・販社と製造会社は別会社であるが、全く同じ内容の規程を使用している。

（２）個人情報の取得

・直接取得としては、基本的には個人情報の取得はカルテ会員になってもらうときに発生する。
・無理に会員になっていただく必要はないと考えており、取得の際には記載いただけた個人情報だけを取得するようにしている。
・カルテ会員に申し込みを行う際には、規約が書いてある申込書になっているが、申込書の細かな規約を読むのは大変なので、内容としてわかりやすくまとめて記載した箇所を作っている。規約そのものは顧客に渡すようにしている。(手元に必ず残すようにしている)

(個人情報の取得は規約書使用の場合に限定、販売店のポイントカードなどの取り扱いは行わず、個人情報取得の場合のリスクを限定している)

・店頭では、会員に登録する上での規約書を使用しない個人情報の取得は行わないようにしている。つまり、口頭での取得やメモ書きによる取得、規約書以外の記入用紙を作成しての取得などを禁止している。このことで、個人情報の取得項目が限定され、管理者が預かり知らない個人情報がどこかに蓄積されるということが生じないようになっている。
・また、そうすることで直営販売店舗・販売店の担当者が判断に迷わぬようにしている。
・加えて、会員として取得した内容しか、販売店とは共有しないということにしている。販売店が他の手段で取得した個人情報がある場合でも、共有しないということである。
・直営ではない販売店が独自に発行するポイントカードへの入会手続きなどは、ア社から派遣された販売員は取り扱わないようにしている。管理責任が曖昧になり、リスクが高まるからである。
・会員には購入のたびにポイントが溜まることや、割引が受けられるなどの経済的メリットは特に無い。購買履歴などを管理して適切なサービスを行うことが主な目的であるので、（経済的メリットがあることが特徴である）小売・流通会社のカードとは位置づけを異にしている。

（３）個人情報の利用（第三者提供を含む）

・第三者提供は行っていない。するニーズも無い。
・ダイレクトメールについては「いらない」というチェックをした会員には出さないようにしている。ダイレクトメールは原則として（モニターなど除き）製造本社から送付することは無く、販売店が独自に送付しているようである。
・肌状態をチェックするカウンセリング機器を有償貸与しており、的確なカウンセリングに利用している。機微な情報であり、オンライン情報ではその内容は見れないようになっている。（オンラインでの送信自体を行っていない）。
・製造本社ではカルテ会員の購買履歴等のデータは個々人のデータとしてマーケティングに使用することは行っていない。全体として、“特定の商品の売り上げが上昇している”、“このような属性の顧客が購入している”というような分析を行うだけである。
・せいぜい、新製品のモニタリングの場合に、カルテ会員で特定のブランドを継続して使用しているような顧客にモニターになっていただくための依頼を行うくらいである。

（４）個人情報の管理

①情報の管理システム

・カルテ会員の個人情報管理は情報企画部が担当している。システムのアクセス権限はかなり限られている。そのシステムにアクセスする際には、物理的に後ろからモニタリングを実施する者がいる状態でしか認められていない。
・個人情報は ID で管理されており、ID と氏名を照合しないと個人情報とわからないよ

うな管理方法を採っている。管理者としても、ID と氏名の関連付けを行う者と、データを見る者は完全に分かれており、実際には氏名と情報の照合は社内でも誰もできないような状況になっている。

・ネット会員の個人情報が含まれているオンラインのサーバは管理委託している。セキュリティレベルの最も高い会社に依頼しており、社内でもそのサーバがどこにあるのか、どの会社に管理委託しているのかは知られていない。

・端末の設定時にハードディスクの暗号化が行われており、仕様は本社で決めて提供している。万が一盗難に遭っても、端末の起動や端末へのログインが容易にはできない。

・盗難にあわないようにするために、少なくともセキュリティワイヤーを購入し、販売店に配布している。

②従業者への教育方法

・イントラネットで e ラーニングを提供して、年 2 回実施している。各回とも、20 問程度の設問に全問正解するまで何度でも受験してもらっている。

・販売員などにはパソコンは貸与していないので、支店や営業所に立ち寄りを行った際に、セキュリティについての研修を行っている。正社員も契約社員も同じ内容で研修を実施している。

・得意先に勤務する店舗スタッフについても、店舗スタッフになる際に必ず研修を受けてもらうようにしている。

（地域や担当による教育・研修内容のぶれをできる限り小さくする）

・研修資料を全国一律で作成し、講師役がどのパートについて何をどの程度詳細に教えるべきか、どのくらいの時間をかけて教えるべきか、ということについてまで、指示を行い、誰が研修を実施するのかということで、研修の内容や質、強調する箇所について違いが生じないように配慮している。

③盗難対策

・そもそも個人情報を保有して歩かないようにしている。

・販売店舗が同社と取引を停止する際に、カルテを大量に事業所に移送するときが、一番リスクが高いタイミングである。その際には必ず複数名で移送する、というルールがある。

（持ち歩きリスクを回避するため、ダイレクトメールなどの収集・一括送付を停止）

・とにかく、外に持ち歩くこと自体が大きなリスクと認識している。

・ダイレクトメールも、大量にまとめて発注するほうがコストを削減できることから、営業担当がいくつかの販売店舗を回ってまとめ、ある程度のロットになってから発送

していたが、移送リスクがあるのでこのような対応はやめて、大量発注によるコスト削減を諦め、個別の販売店舗から発送するようにした。

④ノート PC の安全対策

・営業担当者にはモバイル PC を貸与していない。
・モバイル PC にはそもそも個人情報の蓄積を認めていない。
・暗号化は全て施されており、BIOS のパスワードがかけられている。
・各事業所の管理責任者の許可を得てモバイル PC を持ち歩くことはできるが、その都度申請し使用後返却するルールにしている。

⑤外部委託先管理

＜販売店の管理について＞

・販売店は委託先ではないが、個人情報を共有している関係であるので、管理監督や個人情報保護の水準を維持することが重要である。
・店頭で設置する機器は製造本社が機能設定し、販売会社が貸与しており、セキュリティ仕様を自社で決めている。
・そもそも要求される個人情報保護体制をとることができない販売店とは商品の取引契約（カウンセリングを実施し、カウンセリング結果についてもカルテ会員の情報に追記することを認める契約）を締結せず、取引自体を実施しない、ということが最大のポイントではないかと感じている。
・全国7万店のうち､2万店弱しかカルテを取り扱う必要のある商品は取り扱っていない。
・カウンセリングを行うような体制がとれないホームセンターなどにはセルフ販売の化粧品（カウンセリングすること無く購入できる商品）しか置いていない。
・但し、販売店舗については個人情報保護体制のチェックまでは実施していない。化粧品販売に専従の人間が付くかどうか、という点で判断している。日常的に接点があるので、日常業務そのものが個人情報管理体制のチェックになっている。
・販売会社の監査を実施する際に、サンプル調査でいくつかの販売店で個人情報保護の管理体制を確認することを実施している。実際に店舗の写真も撮影して状況を確認することがある。
・紙媒体の管理については販売店に委ねている。

＜委託先管理について＞

・顧客情報についてのサーバ管理は委託している。
・単発的にプレゼント施策や調査委託を行う場合に都度、外部業者に委託することがある。
・委託先の個人情報チェック項目がある。解約締結と委託時のチェックで実施している。

・年に 1 度の書面によるチェックをお願いしている。委託先で記入し、押印の上、提出してもらっている。
・カルテ情報の大量入力などをお願いする際には、実際に担当者が入力現場まで出向いて実際の入力場面を確認した。委託先は 1 社であるが、バラバラの事業所で分散入力をしてもらうことで、委託先内部で個人情報を特定できないような状況で確認した。

⑥日常点検・確認の方策

・啓発としては、システム資産の管理と重複する部分が多いので情報企画部からルールが出ている。啓発は行われている。
・各フロアの施錠確認表などは設置されており、金庫の施錠、電子機器の電源ダウンの確認などは最後にオフィスを退出する者が行っている。

⑦初歩的ミスの防止策

・個人情報の FAX は原則禁止にしている。短縮ダイヤルの事前登録しか認めていない。どうしても FAX 番号を入力して送信する際は、送り手は 2 人以上で送るようにしている。送り先に連絡を入れて待機してもらった状況で送信するようにルール化している。
・メールは一斉送信で情報提供するようなことは少ない。
・ダイレクトメールの内容の誤りのために、混乱が起きたことがあった。個人情報を入れ間違ったわけではないが、異なる店舗名が印刷されたハガキで出してしまったことがあった。これはまとめてダイレクトメールを出そうとしていたことが問題だったので、集約しての外部委託は禁止した（個別店舗でダイレクトメールを出すようにした)。

（５）個人情報の消去・破棄

・個人情報のカルテは販売店で処分している。一定期間以上来店の無い顧客については、廃棄してもらうようにしている。
・各事業所で保有している個人情報カルテの束はあるが、基本的にはシュレッダーで処分している。
・データベースについても保管期限はあるので、期限がくればデータも削除している。(削除データであるという扱いになり、参照ができなくなる)。
・製品回収の際に、顧客の購買履歴を調べて個別に連絡することは無いと考えている。一定期間を過ぎれば顧客の手元に残っているということはあまり無いと考えられる製品特性があるからである。

（６）個人情報の監査

・機密情報と個人情報の監査ということで合わせて年に 1 回実施している。本社だけではなく、関係会社も実施している。全事業所を実地検査して監査している年もあるが、特定のピックアップした部署についてのみ実地監査を行う場合もある。

・書面監査以外は年に応じて柔軟に対応している。特定の監査トピックで問題が生じた年は全事業所の監査を行うが、それほど重大な問題が生じていない年は一部をピックアップして実施しているということである。
・監査は事前通告を行って実施している。

（７）苦情処理・顧客対応

・開示請求は無いわけではないが、少ない。
・カルテ会員としての基本情報についてはオンラインで会員自身が確認できるので、見てくれるように依頼している。
・本人確認は郵送で可能ということにしている。
・電話での問い合わせについては、カルテ会員の氏名、ID、誕生月日および住所だけは確認しているので、これら全てを答えることができることで本人確認としている。

（８）事故発生時の対応

・各部門・事業所の情報管理責任者に事故発生の把握義務を負わせている。把握したら必ず総務部に連絡する義務がある。事故対応手順を決めてある。
・まず個人情報の漏えい事故なのかどうかを確認する。判定基準もある。顧客対応基準も作成している。マスコミ対応基準もある。
・報告事項についてフォーマット化すると、フォーマットに収まるように整理することで時間がかかるので、第一報は電話でも何でも良いからとにかく連絡する、ということにしている。事故であることが明らかになった際にフォーマットがはじめて出てくるようになっている。
・コンプライアンス委員会が招集される。CSR 室と法務室、事故発生部門代表者など関連する人が一同に集められることになっている。実働部隊はプロジェクトチームがその都度組まれるような形である。
・事案の大きさを測る段階では実働部隊で判断している。キーパーソンとして具体的な名前で委員が決まっている。
・3 段階の対応を行っている。全社的対応、部門横断、個別部門で対応、というふうに分けている。
・情報セキュリティの中の一環なので海外部門も報告対象に入れている。

以　上