サ．製造業　サ社

事業概要	製造業		
従業員数	単体：約 26,000 人 連結：約 182,000 人	プライバシーマーク取得	あり
保有個人データ件数	保有個人情報：約 9,300 万件 顧客から委託を受け管理している個人情報：約 9,600 万件		

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

・保有する個人情報の件数は、保有個人データが約 9,300 万件、顧客から委託を受け管理している個人情報が約 9,600 万件。個人情報は毎年棚卸しており、表記の数値は 2008 年度に棚卸したもの。なお個人情報の件数は本体のみのものであり、子会社の保有する個人情報の件数は含まれない。

・個人情報の種類（主要例）：氏名、住所、電話番号、会社名、会社所在地、所属部署名、役職名、電話番号(勤務先)、FAX 番号(勤務先)、メールアドレス(勤務先)、性別、生年月日、本籍地、医療情報

・個人情報の利用目的（主要例）：製品・サービスに関する情報提供、製品・サービスの販売・提供、セミナー・展示会・イベントのご案内送付、製品・サービス等のサポート対応、お問い合わせ対応、各種会員制サービスの提供、製品開発、アンケート調査実施・分析、契約の履行

・メールアドレスは個人情報として扱っている。特に社員のメールアドレスに関しては、入社時にフルネームの入ったアドレスを配布しているため、そのように扱っている。

・個人情報保護の取組の考えとして、安全管理と礼儀作法の二点を持っている。

（２）個人情報保護担当部署

・プライバシーマーク全社事務局。同事務局は各部門の責任者の集合で構成されている。

・同社はソリューション部門、製造部門、管理部門の大きく三つの部門に分かれており、もともとソリューション部門と製造部門は、各部門内にセキュリティ委員会を持っていたため、同委員会のメンバーが参加することとなった。一方、管理部門は該当委員会を持っていなかったため、最も個人情報を多く保有している人事部が参画することとなった。

・監査役を法務部が担っている。

（３）個人情報保護管理者の有無・位置づけ

・同社の副社長が、「個人情報保護総轄責任者」として同社における個人情報保護マネジメントシステムの実施及び運用に関する権限と責任を有する者に位置づけられている。

（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

・認証種類：プライバシーマーク（2007 年 9 月取得，2009 年 9 月更新）
・取得理由：個人情報保護体制を構築するため
・取得効果：個人情報のみならず情報セキュリティ一般のレベル向上にも寄与
・プライバシーマークの取得は、2000 年に顧客から大量の個人情報を預かっている一部の部門で取得していたことがある。

（５）個人情報保護に向けた取組経緯

・1999 年 4 月：「個人情報管理規程」制定（大手電機メーカーでは初めて）
　- リスクが高い業務につき細則を策定し、監査責任者が個人情報の取扱状況を監査
・2000 年 5 月：ネットワークサービスの部門においてプライバシーマーク認証取得
・2003 年 1 月：「個人情報管理規程」をグループ規定化
・2005 年 2 月：「個人情報管理規程」を改正
　- 監査責任者が行う個人情報の取扱状況の監査結果の報告先を社長に改正
・2006 年 10 月：「個人情報管理規程」を改正
　- プライバシーマーク認証取得のため JIS Q 15001:2006 準拠仕様に規程を改正

（６）個人情報の保有・管理・提供等に関する業界の特徴

・同社の売上の 6 割を占めるテクノロジソリューション（コンサルティングからシステムインテグレーション、運用、保守に至るまでの IT ライフサイクル全般に渡るサービスや、顧客のシステムを支えるサーバを中心とした IT 基盤や先進ネットワークシステムを支えるネットワーク機器を提供する業務）が、主に法人顧客を対象としているので、金融・公共・製造・流通・医療など幅広い分野の法人顧客の窓口担当者情報（名刺レベル）が多く、同社が保有する個人情報の大半を占めている。
・この他には、従業員情報、パソコンや携帯電話を提供している関係で一般消費者の顧客情報、受託業務にて預託される個人情報を保有している。
・同グループ企業では、個人情報保護法や経済産業省ガイドラインに沿った個人情報管理規程がグループ規定化されているので、同社と同一レベルの個人情報保護施策が採られており、また約 50 社がプライバシーマークを取得して個人情報保護の強化に努めている。
・大手電機メーカー9 社のうち 7 社がプライバシーマークを取得している（2009 年 12 月時点）。

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）

・同社では、個人情報を取り扱う業務を業務リスクに応じてレベル分けをしている。

・1999 年に個人情報管理規程を定め、診療情報や信用情報・人事情報などの機微度が特に高い個人情報を扱う業務、データベース化して個人情報を一年以上継続的に利用する・取り扱う業務などのリスクが高い業務で扱う個人情報の管理について、細則を策定するよう運用ルールを定めていた。その後プライバシーマークの取得に向け、法務部の管理職約 10 人がたずさわり、2 ヶ月間で同管理規程を改正した。同改正において苦労したのは、リスクが比較的高くない業務で扱う個人情報をどのように管理するか、という点である。原則「関係者外秘」と同じ扱いにしている。

・個人情報管理規程策定後は、その規程をどのように現場に周知させるか、という点に注力した。

（２）個人情報の取得

・個人情報を取得する場合は、明確な利用目的を提示して、明示的な同意をとりつけている。

（３）個人情報の利用（第三者提供を含む）

・個人情報保護ポリシーで提示しているとおり「取得状況から見て利用目的が明らかな場合」に限定して利用している。例えば、名刺交換後にお礼の連絡などで顧客へアクセスすることは問題ないが、メールマガジンを送信するのは問題がある、という解釈をしている。

・基本的に個人情報の共同利用はしない方針。理由は、責任の所在が曖昧になるため。健康保険組合・企業年金基金・労働組合との間でのみ共同利用を行っている。

（４）個人情報の管理

①情報の管理体制

（個人情報を 3 種類の台帳で管理）

・保有個人情報は、リスクが高い業務で扱う個人情報（台帳 A1）とリスクが高くない業務で扱う個人情報（台帳 A2）に分けて台帳管理している。また、顧客から委託を受けて管理している個人情報（台帳 B）について別途台帳を整備している。台帳の具体的な項目は、次表を参照。

図表　台帳 A2 サンプル（リスクが高くない業務で扱う個人情報）

図表　台帳 B サンプル（顧客から委託を受けて管理している個人情報）

・台帳 A1 に載せる情報は、リスクが高い業務において扱う個人情報である。なお、これらの業務は、更にリスクレベルに応じて、a）信用情報・金融取引情報を継続的に扱うなど特にリスクが高い業務、b)メールマガジン送信のみを行う業務、c)それ以外の業務の三つに分類し、それぞれ管理について定めた細則に従って業務運営をしている。a）特にリスクが高い業務では、アクセスログを記録する等フォレンジック対応にしている。また、データベースは別個に設置しており、情報毎にアクセス制限も設けている。

（リスク分析の義務付けで、不必要な個人情報を大幅に削減）

・個人情報の台帳（A1, A2）に「リスク分析の実施の有無」という項目を追加設置したところ、個人情報の件数が 1 割以上減少した。それまでリスク分析は各事業部の裁量にゆだねているところがあったが、義務付けして台帳でチェックすることができ、必要以上に個人情報を所持することを抑止できるようになった。

・その一例として、ある部門での個人情報集約が挙げられる。当該部門は本来ならばデ

ータベースはひとつでよいにも関わらず、「リスク分析の実施の有無」項目を追加以前は、部の複数の従業員の個人情報を保有していた。しかし同項目を追加したことで、リスク分析実施の負荷を回避するため、各個人が保有していた情報を集約しようという流れになった。

（ツールを導入により台帳管理を効率化、高度化）

・同社は各台帳の管理を各事業部に任せている。このため、問題点を即時に特定し、色付けしてハイライト表示するツールを導入することで、各事業部内で問題把握が出来る仕組みを整えた。

・具体的には、リスクが比較的高くない業務で扱う個人情報を記録する台帳（A2）に信用情報が含まれている場合、リスク分析がおこわなれていない場合、利用者の範囲が適切でない場合、利用目的が適切でない場合に、各項目が、赤や黄色でハイライトされる仕組みとなっている。

・台帳の各項目は自由記入ではなく、プルダウンによる選択式にして管理を効率化している。

・本部の緊急連絡網や一部情報については、全ての部門で必ず保有しているものであり、既に特定ができているものとして台帳記入を割愛してよいとしているものもある。

・名刺の管理は、基本的には個人管理に委ねているが、一部、営業用のキーパーソンの名刺情報は、専用のデータベースで管理している。当該専用のデータベースを管理する業務は、リスクが高い業務として細則策定しているので、その個人情報については台帳（A1）に記載している。

②従業員従業者への教育方法

・毎年社員教育を実施している。基本的には」e ラーニングにより教育している。原案は同社が作成し、それに沿った内容の教育コンテンツの作成を教育専門子会社に依頼している。具体的には、よくある事故事例をリアルに映像により再現し、どうすべきかといった問いかけをしながら進むようなものである。

・新人社員や通年採用者に対しては、情報管理の重要性を認識させる内容の教育を入社時に実施している。中堅社員・幹部社員に対しては、研修コースに情報セキュリティ教育を組み込み、集合形式や e ラーニングにより教育を行っている。

・情報セキュリティ教育は必須であるため、受けないと本人・上司・本部長にメールが送信される仕組みとなっている。全社事務局とは別に教育部門が設置されており、同部門がメールを配信している。

・この教育プログラムのテストは、80 点以上で合格としているにも関わらず、社員全員が 100 点になるまで繰り返し実施されている。

（管理職と非管理職の実習期間を一週間ずらして実施）

・e ラーニングでは管理職が先に受講し、1 週間後に非管理職が受講するようにして、開始時期をずらしている。非管理職の受講時に、先に受講した管理職の回答の一部が表示されることとなっており、自身の回答と比較することができるようになっている。また、非管理職同士でも、相互に回答を公開し、比較することができるようになっている。

（情報管理ハンドブックの配布や、イントラネットでの啓発を行っている）

・社内で情報管理ハンドブックを作成し、全社員にウェブで閲覧可能にしている。
・イントラネット上では、情報管理ハンドブック以外にも、世の中で多発している情報漏えい事件を紹介することで注意喚起を行っている。社外以外にも、社内での失敗事例・優良事例の紹介を行っている。失敗事例については、何が問題であったか現場で考えさせ、情報発信をさせている。優良事例では、常に良い取組を募集しており、何かあった際にはヒアリングをおこない、取り上げている。
・その他には、毎月一度のチェックデーを設け、管理職自らが自部門のセキュリティ対策状況を確認し、従業員に対して注意喚起を行っている。

③盗難対策

・次項「④ノート PC の安全対策」を参照

④ノート PC の安全対策

（ノート PC に遠隔消去システムを導入）

・2009 年 10 月から、社員にハードディスクの内容を遠隔操作で消去できるノート PC を支給している。
・この仕組みは、暗号化したハードディスクを複合するための鍵を記録しているメモリー部分を遠隔操作で消去することができるというもの。
・消去されると、その旨のレポートが管理部門に送信でされる仕組みになっている。同レポートには最終アクセス日が記載されており、不正アクセスがなかったか確認できる。
・この PC は誤作動が最も危惧されるため、2 重 3 重の保護対策を図っている。
・携帯電話に遠隔消去システム・遠隔ロックを導入している。
・携帯電話における個人名の登録は、苗字のみによる登録を促し、漏えい時のリスク低減を図っている。
・携帯電話は現在、会社支給として全部で四機種を扱っている。これらの機種の中には、リモートロックが出来るもの、リモート消去が出来るものなど様々ある。購入時期が古いものは、これらの機能が備わっていないものも多いが、強制的に買い替えを促し

てはいない。
・営業部門の社員は大半が会社支給の携帯電話を保有しているが、管理部門の社員のほとんどは社給携帯を保有していない。
・在宅勤務については、現在準備を進めており、試験運用している。

⑤外部委託先管理

（契約前、契約締結時、契約中、契約後、それぞれの場面に応じて個人情報の安全管理措置を確保）

・技術力や情報セキュリティ一般も含め、外部委託先を格付け評価している。格付けには、プライバシーマークや ISMS の認証を取得しているかどうかも評価項目のひとつである。また、格付けは低いが、この企業を使いたい、という要請が現場からあったときは購買部門が委託先に対して直接改善要求をおこなう。
・契約に一般的な守秘義務条項など詳細な項目を設けている。また、この契約時に、携帯電話・ノート PC を同社同様の基準で管理すること、秘密情報を台帳で管理すること、従業員教育の実施、顧客から同社に破棄証明書の要求があった場合に限られるが、個人情報を廃棄した証明として廃棄証明書を出すことなどを求めている。
・年に一度同社による情報セキュリティ研修会を実施している。研修終了時点でテストをおこなっている。研修会へは、約 6 割の委託先企業が参加している。参加しない企業とは基本的に契約を行わないこととしている。
・契約中は購買部門が定期的に情報セキュリティ対策の状況確認を実施し、確認結果に基づいた是正計画と、実施指導、是正実施内容の確認を行っている。
・事後評価では情報セキュリティ状況確認、情報セキュリティ事故対応などをもとに評価を行っている。重大な事故が発生した場合や、改善が見られない場合には、取引の見直しや新規発注停止なども必要に応じて実施している。

⑥日常点検・確認の方策

（年に一度の台帳の再確認、リスク分析、エンドユーザからの苦情・相談の情報伝達要求、の三点をおこなっている）

・台帳は株主総会や人事異動が行われる前の 6 月に作成している。体制変化後は落ち着くまで時間を要するため、体制変化前に作成している。変化した体制が落ち着いてきたと想定される 11 月頃に、プロジェクトの整理も兼ねて再確認を求めている。
・台帳の再確認にあわせ、リスク分析と対策の再実施を求めている。

⑦初歩的ミスの防止策

（個人情報等に関する事故発生状況をビジュアルに社内 Web で共有）

・部門別の事故の発生状況や概要を社内 Web で共有している。表頭に事故概要、表側に事故を起こした部門を記載した表を作成し、どの部署でどのような事故が何件あったか可視化している。同表では、漏えい事故の悪質性のレベル区分をした上で、その他項目として飲酒かどうか、委託先かどうかも分かるようになっている。

・部門間の事故発生状況の格差や重点項目が明確になり、漏えい事故が減少したものもある。

・このほか、役員が集まる経営会議において、現場の本部長に事故の詳細と解決策を報告させている。

図表　個人情報漏えい案件（サンプル）

職制情報(発生当時)		件数	紛失・盗難		誤送信		目的外利用		ファイル交換ソフト	その他
BG	部門	カッコ内委託先	PC	社給携帯	e-mail	FAX	無断利用	無断提供		
	○○部門	1(1)						②		
	○▲部門	2(1)	③②							△
	■◇部門	1(-)				②			②(②)	
	○●部門	2(2)		①	① ①					
合　　計		18(6)	1	1	1	1	0	1	1	1
			2		2		1		1	1

※　表中の①～③は漏えい事故の悪質性のレベル区分をあらわしている。

・メールの送信時、同社以外のドメインが記載されている送信先について確認用のポップアップが表示されるツールを導入した。全ての宛先を確認しないと送信できない仕組みとなっている。

・このツールによる確認をして送信されたメールかどうかを識別できるシステムを管理部門に設置し、ツールをいれずにメールを送信することは出来ない仕組みにしている。

（５）個人情報の消去・破棄

・保存期間に関する規定はない。自社で収集した保有個人情報については必要なくなった時に、顧客から委託を通じて管理している個人情報については契約が終了した後に破棄するようにしている。

・破棄に関しての規定は、重要文書・機密文書と同じように破棄すればよいとしている。

（６）個人情報の監査

・ソリューション部門については独自に、同部門を監査する部隊を内部に保有している。

（７）苦情処理・顧客対応

・特徴的な取組はなし

（８）事故発生時の対応

（PDCA は現場でまわし、現場から役員に事故詳細と解決策を報告させる）

・事故が発生した際は、再発防止策は現場に JIPDEC フォーマットにしたがって全社事務局に提出させている。それを添削して、現場で再検討し、経営会議に報告させている。

・なお、漏えい事故については、高度な暗号化による秘匿化や割符による情報分散化、遠隔操作による内蔵データの消去といった安全管理対策を講じた場合であっても、現場からの反発（技術的措置を採用しても事故の報告対象になるならば当該措置の開発や採用のインセンティブが失われる）を制して、報告対象としている。

・また、再発防止策の検討においては、報告先機関の欠格性判断の運用ルールが公開されていないので重点的な注意事項が明確にならず、「必要かつ適切な安全管理措置」であるかどうか手探り状態ではあるが、過去の経験を踏まえて立案している。

以　上