ト．その他サービス業（警備）　ト社

業務概要	法人向け警備サービス、個人向け警備サービス、警備輸送、機械警備など警備サービスの提供		
従業員数	約 13,000 人	プライバシーマーク取得	なし
保有個人データ件数	約 250 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 50 万件分の顧客（法人契約、個人契約合計）があり、警備用緊急連絡先名簿として、1 契約先 3～5 名程度の情報と営業関係情報、従業員情報を保有しているので、件数としては約 250 万件ということになる。

・契約先については、法人は連絡担当部署の数名、個人はサービス提供先世帯の情報だけではなく、他に親戚や近隣の人など、緊急時に連絡すべき人の情報の預託を受けているので、1 契約あたり複数名の個人情報を保有している。

・「警備用緊急連絡先名簿」と「営業関係者名簿・名刺等」と従業員情報くらいである。

・契約者の「氏名」と「緊急連絡先電話番号」である。契約者に連絡が付かない場合に連絡する親戚・近隣者についても、氏名と連絡先電話番号を保有している。

・ビデオ等の映像は、個人が特定できないものであるが、個人情報として保管を行っている。

・緊急通報の有無、通報時の電話でのやり取り、通報回数などといった同社との関係で生じる対応などについては、お客様個人に紐づけて一定期間保管するようにしている。

・プライバシーポリシーには以下が利用目的として記載されている。

－サービスの提供、案内、サービス改善・開発の実施、アンケートの実施、プレゼントや懸賞への応募、問い合わせ対応、その他業務遂行に必要な場合

（２）個人情報保護担当部署

・総務部 ISO・内部統制室「情報資産グループ」が担当している。

・同社のグループ会社（直轄会社）は 40 社近くあるが、本社と同じルールが適用されるので、これらの面倒もある程度みている。

（３）個人情報保護管理者の有無、位置づけ

・全社的な「個人情報保護管理責任者」は「情報資産担当役員」が担当している。役職は専務執行役員であり、企画兼総務担当役員が就任している。

・「個人情報保護管理者」は、本社であれば部長が指名した課長クラス、事業所や出先・

支社については副支社長が該当する。これは規程で指定しており、各部や事業所等で自由に決められない。

（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

・JISQ9001:2008（ISO9001）　2002.9.27 をグループ認証としてグループ会社で取得している。目的は、同グループとしての高いサービス水準の維持である。
・また、ISO/IEC27001（ISMS）2004.10.15 も取得しており、情報システムの適切な運用、警備システムの販売を主たる目的として取得した。
・プライバシーマーク取得も検討しているが、部分取得ができないため、取得が容易ではない。
・そこで、プライバーマークはグループ会社で拡大していくことを検討しており、現在はグループで 3 社取得している。ISMS もグループで 5 社取得している。
・これらの認証取得の目的は、セキュリティを守る企業としての外部向けの信用力を高めるということが大きい。
・入札条件として何らかの認証が求められることがあるのでその意味では必要な場合もある。民間企業でも公的機関でも同じである。

（５）個人情報保護に向けた取組経緯

・個人情報保護法の完全施行に対応することを契機として、平成 16 年の 9 月にプロジェクトを立ち上げ、個人情報保護に関する部署を立ち上げたが、会社としては、個人情報保護法ができる前から顧客情報の預託を受けており、顧客情報を重要に扱う体質があった。
・社内組織の編成や個人情報保護方針、個人情報保護規程の整備、安全管理マニュアル等を策定し、グループ会社とも情報共有を行った。
・規程については、平成 21 年末までに、既に 2 回見直しを行っている。
・マニュアルは毎年見直しを行っている。

（６）個人情報の保有・管理・提供等に関する業界等の特徴

・個人情報保護法ができたことで、顧客が個人情報を出したがらないことが多いのが悩みである。特に、個人の顧客で連絡先として自分以外の第三者（親戚、近隣の方など）を説得して頂く必要がある。
・通報・警報を受けるセンターで、「いつ、どのような警報が出たか」、「どのような通報があったか」、といったことを個人情報として追加的に書き込んでいる。
・コールセンターに電話があった場合にはその通話内容も保管している。顧客との聞き間違えによるトラブル防止と、管理者の確認用という目的面が大きい。

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）

・規程を作成・修正する際には、市販のガイドブック、経済産業省・主務官庁のガイドライン等を参考に見るようにしている。

・（金融機関をはじめとして）顧客から、「個人情報保護に関するアンケート」の実施と提出が定期的に求められるが、質問事項に対応できているか、ということを見ながら、新たに求められるようなことが増えた場合には、規程やマニュアルに付加している。

（サービス態様ごとにマニュアルを作成して、社員の対応を現実に沿ったものとする）

・同社でも、警備はサービス態様ごとに「警備輸送部門」、「常駐警備」など、部門が分かれているので、それぞれ個人情報保護についてはどのような視点で注意すべきか、ということを分けてマニュアルを作成している。

・マニュアルは基本編（関連法令等）、機械警備編、警備輸送編、常駐警備編、事例編（他の会社で生じた事故情報などを掲載）などで構成されており、基本編以外はサービス態様によって内容を変えている。

・基本編は ISO 内部統制室情報資産グループで作成している。一方で、サービス態様別のマニュアルは、サービス態様別に、担当部門に依頼して作成してもらい、ISO 内部統制情報資産グループでは「基本編」と「マニュアルのフレーム」の作成、サービス態様別のマニュアルの内容のチェックを行う。

（２）個人情報の取得

・警備用緊急連絡先用の氏名・連絡先については、契約時の必須項目として、同意を得た上で取得している。

・個人情報は管理台帳を作成させており、個人情報保護管理者が必ずチェックするようになっている。個人情報保護管理者の下の部・課長クラスを「取扱管理者」にしており、実務上は取扱管理者が確認して台帳に記載し、個人情報保護管理者の確認印をもらうようにしてチェックが機能するようにしている。廃棄の有無もこの台帳でがわかる。

・年に 1 回、個人情報の棚卸しを実施している。監査部門が年に 1 回、個人情報に特定した監査を実施しており、その際に棚卸しが間違いなくされているかもチェックしている。

（３）個人情報の利用

・緊急連絡等をする以外に利用する事はほとんどない。

（４）個人情報の管理

①情報の管理体制

・執務室内には高セキュリティエリアを設定している。送受信機は必ず高セキュリティエリアに設置するように指導している。また、そのような高セキュリティエリアは執務室の奥に設置するよう指導もしている。特に高セキュリティエリアということで表示してはおらず、レイアウトとして指示を行っている。

・緊急通報等を受け付けるセンターは厳しい入室・退室管理を行っており、同センターで勤務する特定の社員しか入館できないようになっている。

・システム上に存在する個人情報としては、「契約情報」であるが、基幹システムについてはアクセス権限設定を行っており、権限者でなければ利用できないようになっている。ID やパスワードで制限は実施しており、パスワードは定期的な変更が必要な仕組みになっている。

・個別のパソコンについても、誰がいつまで使用しており、どのような作業をしていたのかのログも取得している。パソコン操作のログは全て取得・管理している。

・パソコンからの漏えい防止のためにハードウェアから USB メモリや CD-R などの外部メディアへの情報書き出し制御を行っている。全社で 10,000 台以上のパソコンに特殊な制御アプリケーションが組み込まれている。

・USB メモリは自動的に暗号化する専用 USB を配布しており、それ以外の USB メモリが使えないようになっている。

・携帯電話についてはストラップで体から離さないようにしており、必ずロックを掛けるように指導している。携帯を紛失するケースはたまに生じるが、ダイヤルロック等がかかっているので今のところ個人情報の漏えいにつながった事案はない。

②従業者への教育方法

・年に 2 回、前期（4～9 月）、後期（10～3 月）で個人情報に関する集合研修を各部・事業所単位で行っている。これは全従業者を対象に実施している。

・さらに、一人に対して月 1 回、機会教育を行っている。警備業法では半期ごとに警備員に対して教育を行わなければいけないことになっており、さらに 1 ヶ月に 3 回は現場に行って教育をしなさい、ということになっているので、いずれにしろ月 3 回は教育を受ける機会があることになる。この機会を活用して、3 回のうち 1 回は必ず個人情報に関する教育も含めるようにしている。他の研修機会と合わせて個人情報保護の研修も実施することで、回数は多いが効率的に研修を実施することができている。

・そこで教育される内容としては、マニュアルやイントラネットに掲示された内容を使用して行っている。漏えい事故が新聞記事等で報道されたような場合には、それを題材として教育を行っている。

・研修の受講有無については、個人ごとに「研修記録台帳」を作成しており、受講した

かどうかをチェック・管理しており、これは 1 年に 1 度の監査の際にも必ずチェックを行っている。

③盗難対策

・入室・退室管理は IC カードで管理している。
・来訪者については、社員の同行を義務付けている。
・全ての事業所でそれぞれに入室・退室管理の設定を行っており、自所以外の事業所の者が自分の IC カードで他の事業所に入ることもできない。

④ノート PC の安全対策

・通常使用する PC は、PC セキュリティキット（ワイヤーロープ）で固定している。
・外部持ち出し用パソコンは専門の暗号化ソフトを入れており、仮に紛失しても、起動できない。
・パソコンの持ち出しに際しては台帳への記載が義務付けられている。
・持ち出し用パソコンには個人情報はほとんど入っておらず、個人情報の漏えいを危惧しているというよりも、むしろ機密情報や法人顧客情報の漏えいに配慮しており、対策を行っている面が強い。
・持ち出し用パソコンには、基本は通常の状態ではデータは全く格納されない状態になっており、持ち出す際に、必要に応じて顧客情報（個人情報は原則削除）などを格納するようなルールになっている。

⑤外部委託先管理

・外部委託先は主として、警備業者や防災点検業者などである。
・業務委託先選定基準により業者選択後、個人情報の取り扱いに関する覚書を締結。
・年 1 回の「確認書」による委託先の監督を根拠にした実態調査の実施。
・不備事項については、担当事業所で個別に改善依頼を実施。

⑥日常点検・確認の方策

（職員個々人が自己診断を実施し、取扱責任者が定期的にチェックする目標管理的な運用で自己点検の実効性を確保）

・自己診断書をツールとして準備している。個人情報保護管理者が自分の担当する事業所の状況について定期的（半期に一回程度）にチェックを行い、本社に報告するようにしている。
・個人については、年に 2 回は個人情報保護に関する「自己診断」をさせている。年に 2 回、時期を指定して（GW 前、年末・年始直前など）実施している。
・自己診断後、取扱管理者が見てチェックをすることになっており、その際に、問題が

あれば取扱責任者が指導を行ったり、できていないにも関わらず「できている」としていることなどについては指摘をするように、目標管理制度的に運用することで、単なる書類としての「自己診断」に留まらないようにしている。

⑦初歩的ミスの防止策

・FAX は複数名（2 名以上）、立会いの上で送付するようにしている。
・FAX 送信用紙の表紙に、チェック項目をつけ、チェックをした上でなければ FAX を送らないようにしている。チェック項目に加え、送付者、確認者の名前を書くようなシートになっている。なお、FAX は送信前・送信後に送信先に電話連絡・確認を行うことも義務付けられている。
・社外向け送信メールについては、システム上で、上司に自動的に CC 配信される仕組みになっており、上司は部下が外部に送信したメールをチェックできるようになっている。
・送信先に社外向けアドレスがあると、必ず送信先の確認メッセージが出るメーラーを採用している。

（５）個人情報の消去・破棄

・契約終了時点で個人情報についてはすぐに消去している。
・緊急連絡者の変更などがある場合には、電子データはすぐに削除し、紙媒体は顧客に戻すようにしている（自分たちで処分はしていない）。
・通報を受け付けるセンターで保管されている警備通報に関する情報や、通話記録等については、1 年程度保管することにしている。

（６）個人情報の監査

・個人情報に特化した監査を年に 1 回実施している。
・監査部門は全国で専従 30 名、兼務でまた別途数十名がいる。この体制は平成 17 年度にルールを作った段階で導入した。かなりの人員を監査のために割いている。
・本社で作成したチェック項目の主要な部分について監査で確認するようにしている（必須監査項目は決まっている）。
・日本全国の全ての部署、事業所を毎年回って立ち入りで監査を実施している。
・問題があった場合には、当該部署・事業所に対し、指摘事項に対する「処置回答」を書類で社長宛に提出することを求めている。その後、フォローアップ監査として、実際に対応しているかを監査しているが、これはサンプル監査で実施している。

（監査員は役職定年者など業務に詳しい者が担当。保護法制定後一定期間を経過したことを以って、事前通告無しの監査へと切り替え実施）

・監査員については、年に 2 回、全体会議を開催して教育や情報共有をしている。監査員は役職経験者で役職定年した職員や、その業務に長年従事していた職員が務めることが多いので、業務の内容を理解し、急所がわかっている人が実施している点が特徴である。
・従来は監査の日程についても事前に通告し、監査に備えて「自己チェックリスト」を作成して事前に対応できているか確認してもらうようにしていたが、平成 20 年からは通告なしに監査に入るようになった。これは、個人情報保護法が施行され、ルールも定着しており、通常業務の一環で個人情報保護対策を行えるようになっていて当然である、という考え方から、方針転換したものである。

（７）苦情処理・顧客対応

・顧客からの苦情や情報開示請求はほとんどない。
・専用の電話をセキュリティポリシーに掲載し、同社ホームページに公表している。

（８）事故発生時の対応

・個人情報保護法施行後、平成 17 年度 4 月にパソコン紛失事故を起こした。全対象先に戸別訪問して事故の報告およびお詫びをして回った。
・個人情報に関する事故発生時には事業所の責任者が現場の長として対応に当たることとしており、本社にも担当者が詰めることとなっている。事故やその可能性が生じた場合には、事業所の責任者に連絡し、事業所の責任者は本社に情報を上げ、本社で情報を受けた人は、ISO 内部統制情報資産グループまで連絡し、最終的には本社担当役員および社長まで報告が上がるようになっている。
・事故報告は個人情報保護に関わらず、“巧遅より拙速”、という認識は社員の間で文化として浸透していると考えている。

以　上