O. 情報サービス業（ソフトウェア）　O 社

事業概要	情報処理・通信、システム開発、システムインテグレーション事業等		
従業員数	約 1,600 人	プライバシーマーク取得	あり
保有個人データ件数	（非公表）非常に多く保有		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

（受託の個人情報）

・情報処理サービス事業による顧客から預かった個人情報（以下「顧客データ（個人情報）」と記載）が最も多く、かなりの個人情報を保有している。

・情報処理サービスによる顧客データ（個人情報）の利用は委託契約による情報処理サービスの目的の範囲に限り、システムテスト等における目的外の利用は禁止である。ただし、顧客の委託契約に基づく依頼により、情報システムの開発における運用テスト工程のシステム性能テストなどへの使用に限定して許可している。

（直接取得の個人情報）

・営業活動、フェア、アンケート調査等による直接取得が約 1,000 名分ある。

・利用目的はサービス案内であるがグループ会社等で共同利用するケースがある。

（インハウスの個人情報）

・人事労務管理、健康管理、身分証明、社員研修などの利用による従業者の個人情報としては、社員が約 1,600 名分、協力会社社員が約 1,400 名分を保有している。

・中元・歳暮贈答名簿、採用面接、退職者、株主関係、年賀状名簿の利用による個人情報を多数保有している。

・監視カメラ記録、入退室 IC カード記録、バイオ認証情報、入館申請など、セキュリティ管理により取得した個人情報を一定期間保有している。

（２）個人情報保護担当部署

・総務本部リスク管理室（個人情報保護委員会の事務局を務める）

（３）個人情報保護管理者の有無・位置づけ

・個人情報保護委員会委員長（取締役常務執行役員クラスが就任する）

・個人情報保護委員会の上部組織としてリスク管理統括委員会（委員長は社長）を設置。

図表　リスク管理統括委員会組織図

（４）公的資格認証取得の有無（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取得（平成 11 年 2 月 1 日）。

・個人情報保護の社会的責任として、また情報処理サービス業として預かった顧客データ（個人情報）の保護を目的として取得した。

・その他、ISMS（ISO27001）、QMS（ISO9001）、EMS（ISO14001）等も取得している。

（５）個人情報保護に向けた取組経緯

・顧客データの管理については、旧通商産業省の情報システム安全対策の認定事業所として設備基準、技術基準、運用基準等に対応した安全対策について過去から取組んでいる。

・プライバシーマーク取得後、個人情報の取扱ルールの見直し、内部監査、社員教育等に一層取組む。

・平成 16 年に顧客データ（個人情報）を記載した運用テスト帳票の廃棄事故が発生し、社会的批判を浴びたことからプライバシーマークの取得や ISMS の認証を取得していても事故が起こることを認識し、個人情報保護の対策の基本を見直し、従業者の教育・指導・啓発を強化して再発防止に一層力を入れた。

・日々、情報セキュリティへの脅威が増すように変化しているので、日々の対策を怠ればセキュリティホールが拡大する。「情報セキュリティはゴールがない」ことを肝に銘じ継続的に取組む。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・情報サービス産業においては、個人と直接取引きするケースは少なく、直接取得する個人情報は少ない。

・顧客から大量の個人情報のデータを預かって業務の委託を受け、コンピュータ処理するケースが大半であり、大量の顧客データに適した管理を実施することが最も必要になる。

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）

（ヒヤリ・ハット事例集の作成・掲示）

・世間で発生した個人情報事故事例や社内でヒヤリやハットした事象について紹介し、“世間の事故を社内で発生させないために、また、ヒヤリやハットを事故に繋げないためにどのような行動が求められるか”を記載した「ヒヤリ・ハット集」を随時作成・社内通知している。

・事例集の形式ではあるが、単なる注意喚起の通達ではなく実際には行動基準を示しており、既成事実化した上で次年度に社内ルール集に正式に織り込むことで、従業者の抵抗や戸惑いを極小化しながら円滑なルール策定に役立てている。

（２）個人情報の取得

（個人情報の取得）

・保有している個人情報のうち直接取得した個人情報の割合は極めて少ない。情報処理サービスの上で顧客から大量の個人情報を貸与されている。

・直接取得する個人情報は、フェアの入場の際に入場者名簿に記載した個人情報、又は、その入場時に戴いた名刺の個人情報に限られる。この際、事業者の名称、個人情報管理責任者、利用目的、第三者提供又は共同利用の有無など個人情報を直接取得する条件をフェア入場入口の受付に掲示している。

・アンケート調査で個人情報を取得する場合、上記の取得条件をアンケート説明資料に記載している。

（個人情報の運搬）

・顧客データ（個人情報）の運搬に関しては、インターネット上のオンラインストレージや電子メール添付による顧客データ（個人情報）の転送を禁止している。個人情報を記録した磁気媒体や帳票等は、専用運搬車を用意し、運搬専任の担当者 2 名が同乗して運搬するルールである。

・顧客データ（個人情報）を万が一緊急で運搬しなければならない場合にも、運搬専任の担当者に依頼して専用運搬車で運搬することを原則としているが、専用運搬車が手配できないときは、SE 担当者とその上司の 2 名が顧客を訪問して個人情報を受理・運搬し、その旨を「緊急運搬記録台帳」に記録し顧客に報告することで対応している。

（３）個人情報の利用（第三者提供を含む）

・アンケート調査やフェア等で直接収集した個人情報は、営業活動の利用を目的としており第三者提供は行っていないが、グループ会社と営業活動する際に共同利用するケースはある。

・顧客データ（個人情報）の利用については、情報処理サービス契約、サーバハウジング契約、サーバホスティング契約に基づいた顧客データ（個人情報）の利用目的に限っている。また、情報システム構築に際して、運用テスト工程における運用性能テストに使用する顧客データ（個人情報）の利用も契約による利用目的及び範囲に限っている。

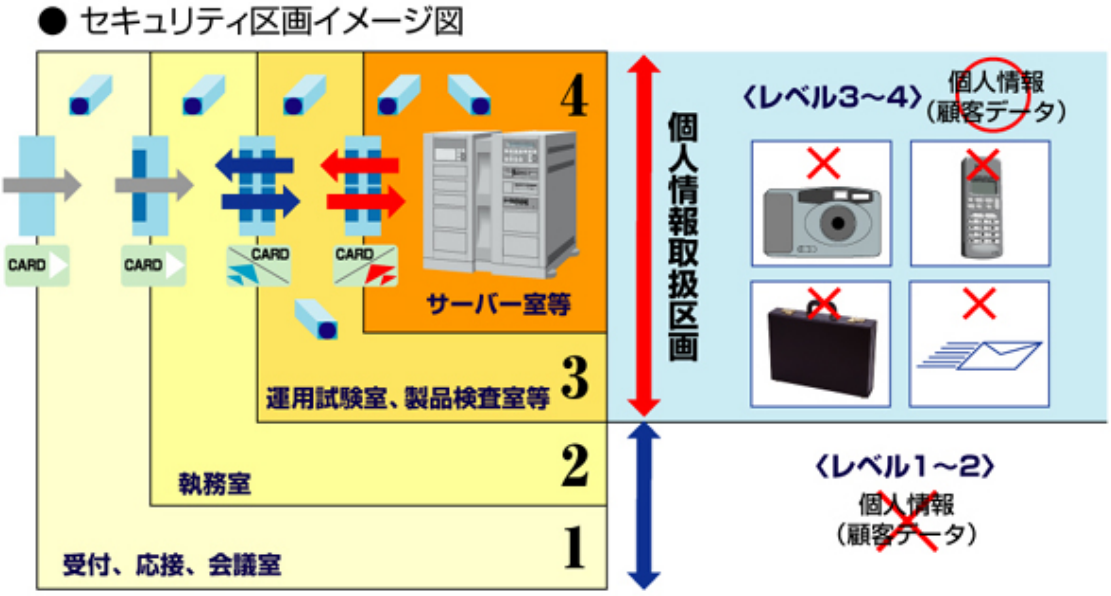
（４）個人情報の管理

①顧客データ（個人情報）の管理

（建物内における“セキュリティ区画”の設置）

・「情報へのアクセスコントロール」と「取扱いのトレーサビリティ（追跡性）」を目的として、執務エリア（システム開発室）をセキュリティレベル別に 4 段階のセキュリティ区画に分けている。

図表　セキュリティ区画の構造



・セキュリティ区画レベル 4，3（個人情報取扱区画）

a.セキュリティ区画レベル 4 はサーバ室等で顧客データ（個人情報）が保管されているエリアである。セキュリティ区画レベル 3 はシステム運用試験や製品検査を行うエリアであり、顧客データ（個人情報）を実際にハンドリングして運用テストなどを実施する。

b.セキュリティ区画レベル 4，3 のエリアにのみ顧客データ（個人情報）の持ち込みが許されている。又は、その 2 つのエリアにおいては、カメラ、携帯電話の持ち込みが禁止されており、カバンの使用、及び電子メールの発信等も禁止されているなどそれぞれの設備対策が施されている。セキュリティ区画レベル 4，3 に設置された社内ネットワークがセキュリティ区画レベル 2 の執務室の社内ネットワークやインターネットと分離されているため電子メールの送受信やインターネット Web の閲覧はできず、顧客データ（個人情報）の漏えいや外部からの不正アクセスを防いでいる。

c. セキュリティ区画レベル 4，3 では入室者が特定されており、入室作業者の作業状況を監視カメラで記録、入退室者の入退室記録が IC 入退室管理装置と監視カメラで行われている。

d.顧客から送付された郵送物の中に、システムに関する問合せや確認のために、個人情報が記録された画面のハードコピー等が送付されている場合があるため、開封作業は同区画内で行っている。また、郵送でなく FAX で送付される場合もあるため、同区画内に設置した個人情報受信専用 FAX で受信している。

・セキュリティ区画レベル 2，1

a.受付・応接・会議室がセキュリティ区画レベル 1、執務室（システム開発室）はセキュリティ区画レベル 2 とされており、顧客データ（個人情報）は存在してはいけないエリアとなっている。

（ファイル共有ソフト（Winny 等）対策の徹底）

・社会問題となっている Winny 等による個人情報漏えい事故は、個人情報や業務情報を会社から自宅に持ち帰り私物のパソコンを使って作業をしていたため、重要情報の漏えい事故が発生している。そこで同社では、社員情報、企業機密情報、業務情報などを許可無く持ち出すことを禁止した。もちろん、これらの情報を自宅へ持ち帰って自宅で作業をすることも禁止している。

・社内においても私物のパソコンや私物の USB 等の外部媒体を持ち込んで作業をすることを禁止している。この方法もファイル共有ソフトによる漏えい防止対策の一環としている。

・社内 LAN に接続されている全国の事業所すべてのパソコンについて、インストールされているプログラムや作成されているファイルを検索するツールが備わっている。このツールによりファイル共有ソフトの存在確認を定期的に行っている。
・毎年、従業者の自宅の私物パソコンについて点検し報告させているが、昨今の漏えい事故件数増加を背景として平成 20 年度から点検を 2 回（半期毎）に増やした。

（リモートアクセスの脆弱性に対して、アクセス権限の対象・期間的に厳格な制限実施）
・リモートアクセスにおけるセキュリティの技術面の脆弱性は以前から認識されており、今まではルール整備は行ったものの、実際にはルールが完全に守られていない可能性があった。
・平成 20、21 年度に、特にリモートアクセスに関する脆弱性対策を対策の 1 つに掲げ、具体的には以下のように、リモートアクセスの仕組みの見直しを行った。
　ア）シンクライアントを大量導入し、データの持ち歩きを一層制限した
　イ）会社貸与のシンクライアント端末等、登録が済んだ機器以外は社内ネットワークに接続できないようにした。
　ウ）リモートアクセスで外部から利用できるシステム・サービスごとに利用者を事細かに分類した
　エ）リモートアクセスの利用者の ID の有効期間は、最長 3 ヶ月とし、利用を継続したい場合には再申請を行うこととした
　オ）通常の個人情報保護教育に加えて、リモートアクセスの利用者に対しては、セキュリティ教育の受講を義務化した

②従業者への教育方法
（毎月の e ラーニングの実施）
・毎月 10 日の個人情報点検の日に合せて従業者に e ラーニングを実施している。ヒヤリ・ハットとして挙がるインシデントをタイムリーに出題することで、予防対策になっている。

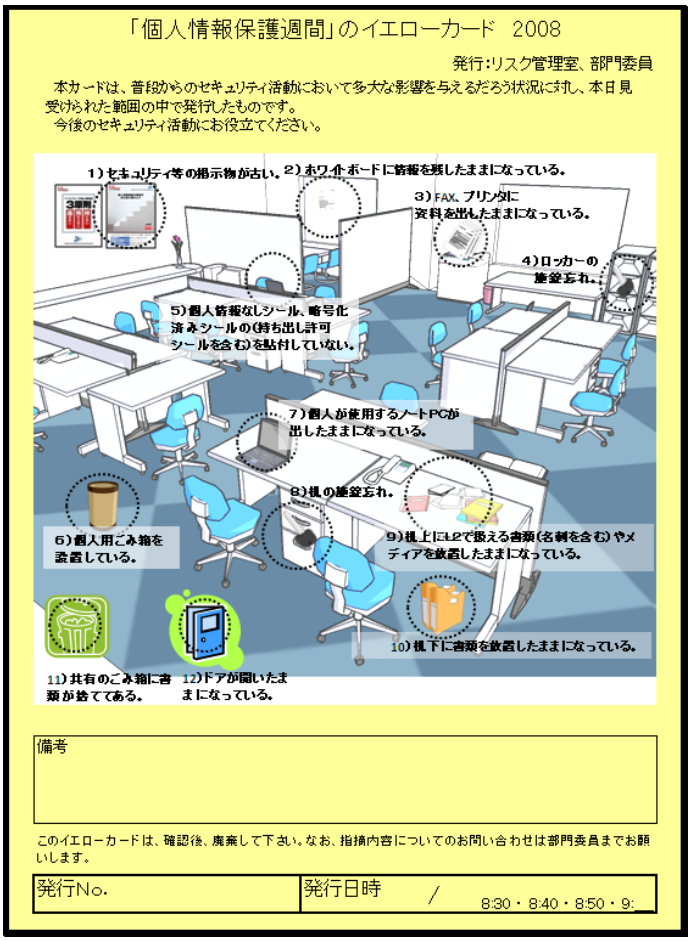
（個人情報保護週間の設定）
・年に 1 度、2 週間の『個人情報保護週間』を設定し、セキュリティ意識を高めている。「手書きによる情報セキュリティ宣言書の提出」「自己点検」「部門間の相互点検」「スローガン募集」「啓発ポスター募集」「個人情報検索ツール募集」「セキュリティ職場点検」などを実施している。
・個人情報保護週間の最終日には、「情報セキュリティ向上会議及びリスク管理統括委員会全体会議」を開催して個人情報保護週間の総括会議を開催している。また、この会議に出席できなかった従業者に対しては、全国の事業所で別途地区会議を開催して必

ず会議の内容が全従業者に行き渡るようにしている。

・地区会議では、「部門間の相互点検」「個人情報保護ミーティング」を行い個人情報保護およびセキュリティ教育・啓発活動を行っている。

・職場点検の方法として、「イエローカード」を作成した。個人情報保護週間に、同カード記載の 10 項目について各事業所で従業者の机回りを確認して問題があれば、カードのチェック内容に赤丸をつけて従業者の席に置く。個人情報の取扱い違反が発見された場合には、レッドカードを発行している。目的は、注意喚起だけでなく、従業者がセキュリティ対策に参加している意識を持ってもらうことにもある。

図表　セキュリティ職場点検（イエローカード）



（個人情報保護 3 原則の設定）

・SE が顧客データ（個人情報）を運搬することを禁止している。しかし、顧客企業が SE に顧客データ（個人情報）を預けるおそれがあるため、SE に顧客データ（個人情報）を運搬させないための“個人情報保護 3 原則”を制定して顧客に理解を得ている。“個人情報保護 3 原則”は「持たない」「預からない」「運ばない」の標語から構成されて

おり、個人情報保護３原則をポスターにして執務室や会議室に掲示して啓発している。また、この 3 原則をシールにして各自のパソコンや事務機器などの社内の至る所に貼付して３原則を徹底している。

図表　「個人情報保護３原則」の社内浸透のために配布されているシール

（社内資格認定試験の実施）

・社内資格として「個人情報取扱資格認定試験」を実施しており、初級・中級・上級の 3 階級に分けられている。

[初級試験]

・初級試験は毎年 8 月の一ヶ月間において、社長はじめ全従業者が合格するまで受験することにしている。
・中途採用の社員や途中入場の協力会社社員については、入社・入場から一ヶ月以内に初級試験の合格を義務付けている。
・初級試験の受験方式は e ラーニング方式としており、60 問の問題からランダムに 20 問が出題される形式である。試験問題の内容は従業者の業務や普段の行動に関わるセキュリティに関する知識及びその活用能力を確認する問題が中心であり 20 分程度で受験することができる。
・合格すると受験者氏名や認定日が印刷された個人情報取扱資格認定証（プラスチック製のカード）が発行され、社員証や館内勤務者証と一緒に常時携帯する。

図表　個人情報取扱資格認定試験　（イントラネットで合格状況を公表）

[中級試験]

・中級試験は、情報セキュリティ監査人として内部監査が実施できるレベル及び個人情報保護の問題点を発見して自ら対策できるレベルの従業者であることを認定する試験である。中級試験の問題は、択一式の問題に加え、論述試験も実施する。論述試験の内容は、実際に発生すると想定される具体的な状況を出題し、セキュリティ上の問題点がどこにあるかということと、その対応として同社のルールに基づいた必要な対策について論述させることにしている。

・中級試験合格者については、社内のナレッジ・データベースに「取得技能」として登録することになり、人事評価等に利用するというメリットがある。

[上級試験]

・上級試験は、情報セキュリティ対策を取引先に提案できるレベル及び個人情報保護に関する法令・基準を理解し、情報セキュリティ監査人の公的資格を取得させる試験である。資格試験は日本セキュリティ監査協会の公認情報セキュリティ監査人（CAIS）資格制度を利用している。

図表　社内資格の認定証

（事件・事故の報告基準を具体例で示す）

・従業者が実際に社内で発生する事件・事故について、どのレベルの事案の場合に、報告すべきかの判断が人によって異なることを問題視した。事件・事故が発生した場合には、早期に把握し、さらに事故を拡大させないように早急な対策が必要である。従業者が「事件・事故」と認識すべきケースを具体的に記載したマニュアルを配布して万が一の事件・事故の緊急対応が行えるよう指導している。これにより従業者が勝手に小さな事故と判断して報告を怠ることが無いように配慮している。

（部単位でのセキュリティ・ミーティングの実施）

・個人情報保護委員会の事務局であるリスク管理室が各部門を訪問して部単位でセキュリティ・ミーティングを１年に１度以上の割合で実施している。

・セキュリティ・ミーティングでは、従業者がどのような点で悩んでいるか、どのような点に気をつけなくてはならないか、といった事について議論し、自発的に問題を発見して対策できるよう、意識の向上を期待するものである。

（個人情報保護法の過剰反応による適正利用の指導）

・個人情報保護法に対する誤解等に起因して、病院が事故で入院した患者の個人情報を公開しなかったり、各種の名簿が作成されなくなったりするなど、「過剰反応」と言われる状況が社会で見られた。同社でも個人情報保護法を過剰に反応して業務遂行に影響しているケースもあるのではないかと調査した。その結果、個人情報の取扱いを間違った認識で行っていることにより業務に過剰に負荷がかかっていることが見受けられた。個人情報の安全管理だけでなく業務の過剰負荷を軽減させるためにも個人情報の適正な利用を指導している。

（事例）

ア）個人情報の提供の誤解

a.協力会社社員が館内勤務手続きをする際、個人情報保護法を理由に館内勤務証・ICカード発行申請に個人情報（氏名、勤務先、写真等）の提供を拒否

b.お客様先に訪問したとき協力会社社員がお客様の入館記録に勤務先の提供を拒否

c.マネージャが社員の個人情報を派遣先に提供する際、個人情報保護法を理由に本人が拒否

イ）個人情報の取得・利用の誤解

a.プロジェクトメンバー表（氏名や役割など）を配布する際、メンバーの同意が必要と誤解

b.管理職が、社員の健康情報はセンシティブ情報であるため、取得していけないと誤解

c.個人情報はできるだけ利用しない方が良いという誤解

・業務遂行に必要な個人情報は取得し利用すべきであり、また、顧客にも顧客の業務遂行に必要な個人情報は提供すべきであることを指導している。

③個人情報の盗難対策

・フェア入場者の入場名簿及びアンケート調査によって取得した個人情報については、利用者制限、アクセス権限、保管ルールなどの管理ルールを定めて、不正利用、不正アクセスによる盗難を防止している。

・顧客データ（個人情報）の盗難防止として、ロボットを内蔵したカードリッジ保管庫（LSM：Library Storage Module ）に格納されたカードリッジに顧客データ（個人情報）を記録しており、この顧客データを情報処理に使用する場合、LSM のロボットがカートリッジをセットする。オペレータは直接カードリッジにふれることができない仕組みにして顧客データ（個人情報）の盗難防止をおこなっている。

④ノート PC の安全対策

・ノート PC は自分の机の引出しに入れ、施錠するように指導している。

・セキュリティワイヤーの使用を禁止している。セキュリティワイヤーによる盗難防止では、ノート PC 本体の盗難を防ぐことはできるが、ノート PC に記録された情報が盗まれる可能性がある。

・複数人が使用できるようなロッカーに格納することも禁止している。本人以外のノート PC の情報を盗用できる状況になるからである。

⑤外部委託先管理

・個人情報の外部委託は、情報処理サービスにおけるパンチ業務の委託がある。また、システム開発の技術者やオペレータ運用要員を派遣先から受け入れる場合がある。さらに、システム開発の一部を請負会社に委託する場合がある。

・派遣社員や社内で勤務する協力会社社員にも社内資格の個人情報取扱資格初級試験（前記（社内資格認定試験の実施）参照）を受験してもらい、合格することを勤務要件としている。

・新規委託先や取引審査、既存取引先においても定期的に取引審査を実施している。個人情報を委託する場合、通常の取引審査に加えて「協力会社調査票」によって審査され、審査合格をもって個人情報の委託を可能としている。

⑥日常点検・確認の方策

（3 つのシールで対策を「見える化」する）

・セキュリティ区画レベル 2 で扱う従業者のパソコンに対して、重要な対策が行われていることを一目で分かるように点検結果のシールを貼付している。

・具体的には HD の暗号化や、電子メール添付ファイルの暗号化を行っている「暗号化対応済シール」、ノート PC などのモバイルの持ち出し許可を受けている「持出し許可済シール」、PC に顧客データ（個人情報）を記録していない「個人情報なしシール」の 3 種類である。「個人情報なしシール」と「暗号化対応済シール」は番号管理されている。

・「個人情報なしシール」については、使用期間が半年間（1～6 月／7～12 月）に限定されている。個人情報なしチェックは半年に一度、従業者のパソコンに顧客データ（個人情報）が入っていないことをチェックし、顧客データ（個人情報）が記録されていないことが証明できた場合に「個人情報なしシール」を貼付する。

・「持ち出し許可済シール」の貼付（持ち出し）は「個人情報なしシール」及び「暗号化対応済シール」が貼られているパソコンで、持ち出し目的が明確な PC に最長 3 ヶ月を限度で認められる。

・これらのシールは、誰が見ても一目で必要な対策が終わっているかどうかを確認できるようにするために貼付しており、貼付がないパソコンは持ち出しが許可されない。また、他事業所へ持ち込む際も同様で、貼付がなければ持ち込めない。

図表　「見える化」のためのシール（３種）

（セキュリティに対する部門間の意識レベルのバラツキを背景に、身の丈にあった目標設定と PDCA サイクルを設計）

・毎年、部門ごとにセキュリティ活動の有効性を評価しているものの、個人情報の誤廃棄事故から数年が経過し、部門間でセキュリティ意識の温度差が拡大してきていることに問題意識を持った。

・この点、再度、セキュリティに対する意識を高めてもらい、認識を新たにしてもらうことを目的として、部門単位でセキュリティ担当者数名を任命し、部門ごとに身の丈に合った目標を設定して PDCA によるスパイラルアップを目的とした会議体を設定した。

⑦初歩的ミスの防止策

（電子メールの誤送信対策）

・社会的に電子メールの誤送信による個人情報の漏えい事故や社内機密情報の漏えい事故が多いため、同社の対策としては送信先の再確認を徹底している。主な対策として次の 2 つがある。

・メーラーの設定で、送信ボタンを押してから一旦送信 BOX に蓄積されるようにし、およそ 20 分後に実際に送信されるような設定を推奨している。

・これは、“送信ボタンを押して 5 分以内に誤送信に気付くことが多い”、ということから採っている対策である。

・受信した電子メールの自動アドレス登録機能を禁止している。メーラーを自動アドレス登録とすると、アドレス帳に自分で登録した名前とたまたま同じ名前の別人から電子メールを受けた場合、同じ名前で別人のアドレスが自動登録されてしまう。自動登録された人を自分が登録した人と誤認して電子メールを送信するケースがある。この誤送信を防止するために自動登録機能の使用を禁止している。

（５）個人情報の消去・破棄

・通常の業務において、顧客データ（個人情報）の破棄は大きく２ケースがある。

・一つ目は、情報処理サービスにおいて、不要になった確認帳票やホストコンピュータによる大量プリント工程におけるセット位置の試しプリント用紙の破棄がある。これらの廃棄用紙に顧客データ（個人情報）が記録されている場合もあるため、ダンボール箱に梱包して、箱ごとシュレッダー装置にかける。廃棄担当者は、個人情報が記載された廃棄用紙を見ることはできない。また、シュレッダーされたゴミについても自動梱包され溶解業者に渡すため、見ることができない。

・二つ目はシステム開発における運用テストの確認のために出力されたテストプリントの破棄である。個人情報取扱区画（セキュリティ区画レベル 3）の部屋でテストプリントされた帳票に顧客データ（個人情報）が記載されている場合がある。テスト帳票の確認後、不要になった帳票を破棄する場合、個人情報取扱区画（セキュリティ区画レベル 3）に設置されたシュレッダーで粉砕する。粉砕されたシュレッダーのゴミはシュレッダー袋に格納され秘密保持契約している廃棄業者に焼却処分を依頼する。SE は、シュレッダー袋管理番号を「顧客データ入出庫・使用・破棄管理台帳」に記録して、顧客データ（個人情報）が消滅した記録をする。これによって、SE が使用した顧客データ（個人情報）をトレースでき、破棄した帳票に記載された顧客データ（個人情報）が消滅したことを証明できる。

（６）個人情報の監査

（外部有識者による委員会の設置）

・個人情報保護に関する第一人者を委員長として、個人情報保護専門の弁護士、生活評論家、情報セキュリティのアドバイザーなど、外部有識者 5 名により構成される「情報セキュリティアドバイザボード」を設置し、同社の個人情報保護の取組について評価と提言をいただいている。

・委員会は、3 ヶ月に 1 度開催され、個人情報保護の取組、セキュリティ対策の取組状況や対策の問題点などについて報告を行い、取組や対策についてアドバイスをもらう形式で運営している。また、年に 1 回、情報セキュリティアドバイザリボードから提言書が社長宛に提出され、個人情報保護や情報セキュリティ対策の評価及び提言を受け次期の対応に活用している。

・監査室は、社長から承認を得た監査基本計画に基づいて、全部門の情報セキュリティ対策、個人情報保護に関する監査を実施している。

・リスク管理室は、情報セキュリティ対策の確認、インターネット Web 等の利用監視、メールの発信監視を定期的にチェックしている。

（７）苦情処理・顧客対応

・営業活動におけるフェアやアンケート調査により個人情報を直接取得しているため個人情報保護法に基づいて開示対応ルールを定めている。
・開示請求に対応するために対応者のマニュアルを制定して開示依頼者に対する対応手順を明確にしている。
・開示対応手数料は 1,500 円に設定している。実際に個人情報の抽出に掛かる手間などを含めると数万円掛かる計算になるが、世間の相場にあわせている。

（８）事故発生時の対応

・個人情報事故が発生した場合、リスク管理統括委員会又は個人情報保護委員会が緊急対策本部の役割となり、現在の部署がそのまま危機管理対応の部署として位置づけになることで、役割が混乱しないようにしている。

本調査で整理した個人情報の管理については、情報処理サービス業における情報システム開発室（執務室）で働く SE 業務の情報セキュリティ対策を中心とした整理であり、コンピュータ室やデータセンターにおけるセキュリティ対策及び社員情報などのインハウス対策の紹介は一部のみの記載としている。

以　上