【国土交通省ガイドライン】

国土交通省ガイドライン第９条は、次のように定めている。

（安全管理措置）

第９条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損（以下「漏えい等」という。）の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的安全管理措置を講じなければならない。その際、本人の個人データが漏えい等した場合に本人が被る権利利益の侵害の大きさを考慮し、必要かつ適切な措置を講じるものとする。

２　個人情報取扱事業者は、組織的安全管理のために次に掲げる事項について措置を講ずるよう努めるものとする。

一　個人情報保護管理者の設置

二　個人データの安全管理措置を講じるための組織体制の整備

三　個人データの安全管理措置を定める規程等の整備と規程等に従った運用

四　個人データ取扱台帳の整備

五　個人データの安全管理措置の評価、見直し及び改善

六　事故又は違反への対処について手続きの策定

３　個人情報取扱事業者は、人的安全管理のために次に掲げる事項について措置を講ずるよう努めるものとする。

一　従業者の雇用及び委託契約時における非開示契約の締結

二　従業者に対する教育、啓発の実施

４　個人情報取扱事業者は、物理的安全管理のために次に掲げる事項について措置を講ずるよう努めるものとする。

一　入退館（室）管理の実施

二　盗難等に対する対策

三　機器、装置等の物理的な保護

５　個人情報取扱事業者は、技術的安全管理のために次の掲げる事項について措置を講ずるよう努めるものとする。

一　個人データへのアクセスにおける識別と認証

二　個人データへのアクセス制御

三　個人データへのアクセス権限の管理

四　個人データのアクセスの記録

五　個人データを取り扱う情報システムに対する不正ソフトウェア対策

六　個人データの移送・通信時の対策

七　個人データを取り扱う情報システムの動作確認時の対策

八　個人データを取り扱う情報システムの監視

目次へ戻る

■個人データの安全管理措置に関する必要事項

《解　説》

【組織的安全管理措置】

１・組織的安全管理措置とは、安全管理について従業者の責任と権限を定め、安全管理に関する規程等を整備運用するとともに、実施状況を確認することをいいます。個人データの安全管理措置を講じるための組織体制の整備をする上で必要な事項は、例えば次のとおりです。

①　従業者の役割・作業責任の明確化。
②　個人情報保護管理者の設置。
③　個人データを取り扱う情報システム運用責任者の設置及び担当者のアクセスの限定。
④　監査責任者の設置と実施体制。
⑤　苦情窓口の設置及び主務大臣、認定個人情報保護団体への報告体制。
⑥　個人データの取扱に関する規程（文書規程等）の設置と、それに従った運用。

【人的安全管理措置】

２・人的安全管理措置とは、従業者に対する、業務上の個人データの非開示契約の締結や教育・訓練等を行うことをいいます、個人データの取扱に関する必要な事項は、例えば次のとおりです。

①　雇用契約時及び委託契約時における非開示契約の締結。
・就業規則及び職務分掌規程等、内部規程に具体的に定める。
②　従業者に対する教育・訓練の実施。
・個人データ取扱の、「取得、入力」・「移送、送信」・「利用、加工」・「保管、バックアップ」・「消去、廃棄」及び作業担当者の「識別、認証、権限付与」等を、個人情報のライフサイクルの段階に応じて、教育、訓練を実施する。

【物理的安全管理措置】

３・物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいいます。例えば、以下のような措置が考えられます。

①　入退館（室）管理の実施。
・個人データを取り扱う情報システム等の、入退館（室）の管理をしている部屋の設置。
②　盗難等の防止。
・離席時の個人データを記した書類の机上等への放置の禁止。
・離席時のパソコン等のパスワード付きスクリーンセーバの起動。
・個人データを含む媒体の施錠保管。

目次へ戻る

③　機械・装置の物理的な保護

・個人データを取り扱う機器装置等を、盗難、破損、漏水、火災、地震等の脅威から物理的に保護します。

【技術的安全管理措置】

４・技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいいます。例えば、以下のような措置が考えられます。

①　個人ユーザーの ID 及びパスワードの認証を管理。

②　アクセス権限を管理し、いつ、誰が、どのようなデータにアクセスしたかを記録します。

③　不正ソフトウェア対策として、コンピュータウィルスや不正にアクセスからの被害を防ぐ安全措置を取ります。（例：サーバーセキュリティー、ウイルスソフト対策等）

④　通信に対する対策として、インターネットやリモートアクセスを利用する場合は、外部からの不正アクセスをされないようサーバー等のセキュリティー対策が必要となります。また、電子メールの送受信にあたり、データの暗号化対策を講じるというのも一案です。

【不動産業に係わる Q&A】

Q１・オフィスセキュリティーの対策としてはどのようなことが考えられますか？

Ｑ１　入退館管理等、オフィスセキュリティーは、次の①～⑤のような区分に応じて適切に行なう必要があるでしょう。

①　企業の敷地の外側。

②　社外のものでも許可されれば立ち入ることが出来る場合。

③　応接スペース等、社内の許可を取り使用できる場所。

④　事務スペース等、社員だけが入れる場所。

⑤　セキュリティースペース、コンピュータサーバや機密書類が保管されている場所。

オフィスセキュリティーの対策としては、例えば、磁気錠及び生体認証などの装置による管理という安全性が比較的高い対策から、通常の鍵での管理という対策まで様々です。また、⑤のように機密性の高い個人情報を管理している場所では、入退館管理のログ（入退館管理台帳）を残すことも、安全管理措置の大切な抑止力にもなります。

目次へ戻る

Q２・オフィス内で発生し得る事件、事故とは？

Ａ２　オフィス内で発生し得る個人情報流出等の事件、事故としては、次のようなものが考えられます。

①外部からの不正侵入とそれに伴う窃盗。

②内部社員による不正な情報の持ち出し。

③清掃業者・設備点検業者など外部業者による不正な情報の持ち出し。

④パスワードなどの情報が見られる状態にある時の流出。

⑤書類や記憶媒体（ＦＤ、ＣＤ、テープなど）の過失による紛失。

以上のような事件、事故を防ぐには、まずオフィス内の施錠管理が大切です。例えば、共有している書類は共有書棚で施錠管理し、また、休憩や離席の際には、机の上などに置きっ放しにしないで、鍵つきの引き出し等にしまうなど、基本的な対策が必要です。

Q３・個人情報の安全管理措置は、どの程度講じればよいでしょうか？

Ａ３　安全管理措置は、事業者の規模等によって違ってくると思われます。個人情報保護法では、ここまでという基準は規定にありませんが、安全管理措置は「必要かつ適切な処置」を講じなければならないのであり、過度の費用をかけないで行なえる対策は、二、三人の個人事業者でも必ず行なう必要があります。

Q４・自社の情報管理システムに不正アクセスされ、保有個人データが漏えいしました。この場合の管理責任は問われるのでしょうか？

Ａ４　一般的には不正アクセスをされた被害者に該当する場合であっても、安全管理措置を怠っていた場合には、個人情報保護法上の安全管理措置義務違反（法第２０条）や、従業員に対する監督義務違反（法第２１条）に該当し、罰則を受けることがあります。また、保有個人データの本人との関係では、民事上の損害賠償責任が発生することも考えられます。

目次へ戻る

Q５・コンピュータウィルスの添付されたメールで顧客のメールアドレスが漏えいした場合の扱いはどうなりますか？

Ａ５　ウィルス駆除ソフトなど、ウィルスチェックを怠っている過失が認められる場合には、個人情報保護法上の安全管理措置義務違反や、従業員に対する監督義務違反に該当し、罰則を受けることがあります。また、Ｑ４と同様に民事上の損害賠償が発生することもあります。

Q６・不要になった個人データの破棄はどのような方法を選択すればよいでしょうか？

Ａ６　自社で個人データを破棄するに当っては、シュレッダー（クロス式）で裁断処理を行うなど、個人データが流出しないような方法を選択することが望まれます。また、大量の個人データの場合は、外部業者に委託することも考えられます。ただし、委託先の安全管理措置についても監督責任を伴いますので、個人データの破棄に際しての委託先の選定には注意が必要です。

Q７・メールアドレスや、会社のサーバーにアクセスできる携帯電話を紛失してしまいました。携帯電話の情報流出も安全管理義務違反になるのでしょうか？

Ａ７　携帯電話のメールアドレス等も特定の個人を識別できる場合は、個人情報に該当します。また、携帯電話を使って、インターネット経由で自社のサーバーにもアクセスできる場合は、ＩＤ、パスワードなどが解明されれば、会社内のコンピュータに入り込むことも出来、個人データ流出等の二次被害が発生する可能性があります。ノートパソコンの紛失と同様に携帯電話の取扱いの安全管理には注意が必要です。

Q８・当社は、社内において無線ＬＡＮを使ってネットワークを構築しています。この場合のセキュリティーで第三者に傍受されない方法を教えてください。

Ａ８　無線ＬＡＮのセキュリティーを確保するためには、最低限でも以下のことを実施してください。

①無線ＬＡＮを使って通信を行なうコンピュータのＭＡＣアドレス（ネットワークカードに割り当てられる独自の番号）やＩＤ番号を無線ＬＡＮに制御するシステムに登録し、登録していないコンピュータがアクセスできないよう制御をする方法です。

②無線ＬＡＮの通信を暗号化してください。この機能は、市販で購入する無線ＬＡＮシステムに装備してありますので、購入の際には取扱書を確認してください。

目次へ戻る

［7］ 法第２１条（従業者の監督）

（従業者の監督）
第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

《解　説》従業者の監督

個人情報取扱事業者は、法第２０条に基づく安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければなりません。

なお、「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて業務に従事している者をいい雇用関係にある従業員（社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれます。

※法第 20 条に基づく安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない旨を、内部規程に定めると共に、退職する従業者からも機密保持誓約書を取り交わすなどして、個人データの安全管理を強化するのも一案です。

【従業者に対して必要かつ適切な監督を行なっていない場合】

（事例１）従業者が、個人データの安全管理措置を定める規定等に従って業務を行なっていることを、あらかじめ定めた間隔で定期的に確認せず、結果、個人データが漏えいした場合。

（事例２）内部規定等に違反して個人データが入ったノート型パソコンを繰り返し持ち出されていたにもかかわらず、その行為を放置した結果、紛失し、個人データが漏えいした場合。

目次へ戻る

《参　考》

◆個人情報保護法に関連する、従業者に関する規程

規程名	説　　明
就業規則 業務規程	従業者の安全管理義務に関する、基本的な行為や違反があった場合の対応を規程する。
文書管理規程 セキュリティー管理規程	個人情報を含む機密文書・情報の取扱いを規程する。 その他採用時又は、退職時における「機密保持誓約書」を締結。
教育研修マニュアル	従業者の教育に関する研修の実施。

※規程名及び内容は、企業、組織によって異なります。

◆一般的な措置

◇　職場に従業者と管理者が同席している状態で、管理者が監視できる体制
◇　個人情報取扱台帳等で記録からの確認できる体制
◇　オフィス内の監視カメラの設置
◇　内部監査の実施
◇　従業者の個人情報安全管理に関する教育及び定期的な研修の実施

Point !

個人情報を**取り扱うのは「人」**です。この取り扱う者の個人情報保護に対する意識が、安全管理措置を講じる上の**費用にも影響**してきます。特に不動産業においては、物件情報も含め個人情報を絶えず持ち歩き、利用をする業といえます。**従業者に対して安全管理教育を実施し、「個人情報保護についての意識」を啓発することが最も大切なPointです。**

《文例５　機密保持に関する誓約書》（従業者用）

目次へ戻る

［8］ 法第２２条（委託先の監督）

（委託先の監督）
第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

《解　説》委託先の監督

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、法第２０条に基づく安全管理措置を遵守させるよう、受託者に対し必要かつ適切な監督をしなければなりません。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱い状況等に起因するリスクに応じ、必要かつ適切な措置を講じなければなりません。

「必要かつ適切な監督」には、委託契約において、当該個人データの取扱に関して、必要かつ適切な安全管理措置として、委託者、受託者双方が合意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認することも含まれます。

【受託者に必要かつ適切な監督を行なっていない事例】

（事例１）個人データの安全管理措置の状況を契約締結時及びそれ以外も定期的に把握せず外部の事業者に委託した場合で、受託者が個人データを漏えいした場合。

（事例２）個人データの取扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えいした場合。

（事例３）再委託の条件に関する指示を受託者に行なわず、かつ受託者の個人データの取扱い状況の確認を怠り、受託者が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合。

※法第 20 条に基づく安全管理措置を遵守させるよう、受託者に対し必要かつ適切な監督をしなければなりません。必要かつ適切な監督を行なうためには、受託者の義務や責任を明確にした業務委託先基本契約・機密保持契約等を書面で締結しておく必要があるといえるでしょう。

《文例６　機密保持契約書》（委託先用）

目次へ戻る

【個人データの取扱を委託する場合に契約に盛り込むことが望まれる事項】

１．委託者の選定基準

委託者の選定にあたっては、委託先の個人情報保護における安全管理対策等の水準が、当該事業者と同等もしくはそれ以上であることを確認します。

２・業務委託契約書の締結（委託契約の安全管理に必要な事項）

①委託者及び受託者の責任の明確化。

②個人データの安全管理に関する事項。

・個人データの漏えい防止、盗用禁止に関する事項。

・委託契約書範囲外の加工、利用の禁止。

・委託契約書範囲外の複写、複製の禁止。

・委託契約期間。

・委託契約終了後の個人データの返還・消去・廃棄に関する事項。

③再委託に関する事項。

・再委託を行なうにあたっての委託者への文書による報告。

・個人データの取扱状況に関する委託者への報告の内容及び頻度。

・契約内容が遵守されていることの確認。

・契約内容が遵守されなかった場合の措置。

・漏えい事件・事故が発生した場合の報告・連絡に関する事項。

【不動産業に係わるQ&A】

Q１・個人データの取り扱いを第三者に委託しましたが、委託先（受託者）で漏えいしてしまいました。委託者及び受託者にかかる責任は？

Ａ１　本人との関係では、個人データの安全管理措置の責任を負うのは、あくまでも委託者であり、受託者は委託者の履行補助者の立場です。したがって、個人データの取扱いについての本人に対する責任は、委託者たる個人情報取扱事業者が負います。また、委託先が再委託する場合においても、個人データの取扱についての本人に対する責任は、委託元の個人情報取扱事業者が負うことになります。漏えい事件が発生した際に個人情報取扱事業者が適切な監督を怠っていたと認定された場合は、監督義務違反（法第２２条）により、主務大臣より改善勧告、命令等を受け、罰則を受けることもあります。また、委託元の個人情報取扱事業者は、本人に対し、民事上の損害賠償を負う場合もあると考えられます。

目次へ戻る

Q２・既存の委託業者と業務委託契約を締結しています。この場合新たな個人データの委託に関する契約が必要でしょうか？

Ａ２　個人情報取扱事業者は、委託先の安全管理に関する監督をする義務があります。既存の契約では、委託を受ける業者の安全管理に関する約定として不十分であるのであれば、そのような約定を盛り込んだ委託契約を改めて締結することが必要になってきます。

Q３・委託先事業者とはどのようなところがあるでしょうか？

Ａ３　ＤＭ及び会報誌等の封入及び発送業務や、販売現場などへの人材派遣、ホームページ運用を委託する場合、また、個人情報（物件情報も含む）の入力を依頼する場合などの委託先が考えられます。

Q４・個人データである個人情報が漏えい等した時はどのように対応すればよいですか？

Ａ４　国土交通省ガイドライン第２１条は、個人データの漏えい等が発生した場合の対応について次のように定めています。

（漏えい等が発生した場合の対応）

第２１条　個人情報取扱事業者は、個人データの漏えい等が発生した場合は、事実関係を本人に速やかに通知するものとする。

２　個人情報取扱事業者は、個人データの漏えい等が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表するものとする。

３　個人情報取扱事業者は、個人データの漏えい等が発生した場合は事実関係を国土交通省に直ちに報告するものとする。

※ここでいう「直ちに」は最も時間的即時性が強く、「速やかに」は「直ちに」より急迫の程度が低い趣旨である。「遅滞なく」は正当な又は合理的な理由により遅滞は許されるものと解されています。

※個人情報取扱事業者が、事実関係について“本人への通知”、“国土交通省へ報告”及び“公表”する際には、個人情報保護取扱事業者がどのような漏えい防止のための措置を講じていたかも含め報告等を行なうことが必要です。

目次へ戻る