人的安全管理措置

人的安全管理措置とは、従業者に対する、業務上秘密と指定された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う。人的安全管理措置には以下の事項が含まれる。

①雇用及び契約時における非開示契約の締結

②従業者に対する教育・訓練の実施

なお、管理者が定めた規程等を守るように監督することについては、法第２１条を参照のこと。

【人的安全管理措置として講じることが望まれる事項】

①雇用及び契約時における非開示契約の締結をする上で望まれる事項

- 従業者の採用時又は委託契約時における非開示契約の締結
  ※雇用契約又は委託契約等における非開示条項は、契約終了後も一定期間有効であるようにすることが望ましい。
- 非開示契約に違反した場合の措置に関する規程の整備
  ※個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲及びアクセス条件について契約書等に明記することが望ましい。なお、個人データを取り扱う従業者以外の者には、情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。

②従業者に対する周知・教育・訓練の実施する上で望まれる事項

- 個人データ及び情報システムの安全管理に関する従業者の役割及び責任を定めた内部規程等についての周知
- 個人データ及び情報システムの安全管理に関する従業者の役割及び責任についての教育・訓練の実施
- 従業者に対する教育・訓練が必要かつ適切に実施されていることの確認

物理的安全管理措置

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う。物理的安全管理措置には以下の事項が含まれる。

①入退館（室）管理の実施

②盗難等に対する対策

③機器・装置等の物理的な保護

【物理的安全管理措置として講じることが望まれる事項】

①入退館（室）管理の実施の上で望まれる事項

- 個人データを取り扱う業務の、入退館（室）管理を実施している物理的に保護された室内での実施
- 個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置

②盗難等に対する対策の上で望まれる事項

- 離席時の個人データを記した書類、媒体、携帯可能なコンピュータ等の机上等への放置の禁止
- 離席時のパスワード付きスクリーンセイバ等の起動
- 個人データを含む媒体の施錠保管
- 氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管
- 個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止

③機器・装置等の物理的な保護の上で望まれる事項

- 個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護

技術的安全管理措置

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へのアクセス制御、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う。技術的安全管理措置には、以下の事項が含まれる。

①個人データへのアクセスにおける識別と認証
②個人データへのアクセス制御
③個人データへのアクセス権限の管理
④個人データのアクセスの記録
⑤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
⑥個人データの移送・通信時の対策
⑦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
⑧個人データを取り扱う情報システムの監視

【技術的安全管理措置として講じることが望まれる事項】

①個人データへのアクセスにおける識別と認証を行う上で望まれる事項

- 個人データに対する正当なアクセスであることを確認するためにアクセス権限を有する従業者本人であることの識別と認証（例えば、IDとパスワードによる認証、生体認証等）の実施

※　IDとパスワードを利用する場合には、パスワードの有効期限の設定、同一

又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗したIDを停止する等の措置を講じることが望ましい。

- 個人データへのアクセス権限を有する各従業者が使用できる端末又はアドレス等の識別と認証（例えば、MACアドレス認証、IPアドレス認証等）の実施

②個人データへのアクセス制御を行う上で望まれる事項

- 個人データへのアクセス権限を付与すべき従業者数の最小化
- 識別に基づいたアクセス制御（パスワード設定をしたファイルが誰でもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある）
- 従業者に付与するアクセス権限の最少化
- 個人データを格納した情報システムへの同時利用者数の制限
- 個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等）
- 個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定）
- 個人データにアクセス可能なアプリケーションの無権限利用の防止（例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる従業者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等）

※　情報システムの特権ユーザーであっても、情報システムの管理上個人データの内容を知らなくてもよいのであれば、個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。

※　特権ユーザーに対するアクセス制御については、トラステッドＯＳやセキュアＯＳ等の利用が考えられる。

- 個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ウェブアプリケーションの脆弱性有無の検証）

③個人データへのアクセス権限の管理を行う上で望まれる事項

- 個人データにアクセスできる者を許可する権限管理の適切な実施（例えば、個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする）
- 個人データを取り扱う情報システムへの必要最小限のアクセス制御の実

施

④個人データへのアクセスの記録を行う上で望まれる事項

- 個人データへのアクセスや操作の成功と失敗の記録（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）
- 採取した記録の漏えい、滅失及びき損からの適切な保護

※ 個人データを取り扱う情報システムの記録が個人情報に該当する場合があることに留意する。

⑤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の実施の上で望まれる事項

- ウイルス対策ソフトウェアの導入
- オペレーティングシステム（ＯＳ）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用
- 不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）

⑥個人データの移送（運搬、郵送、宅配便等）・通信時の対策の上で望まれる事項

- 移送時における紛失・盗難した際の対策（例えば、媒体に保管されている個人データの暗号化）
- 盗聴される可能性のあるネットワーク（例えば、インターネットや無線ＬＡＮ等）で個人データを通信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化

⑦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の上で望まれる事項

- 情報システムの動作確認時のテストデータとして個人データを利用することの禁止
- 情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証

⑧個人データを取り扱う情報システムの監視を行う上で望まれる事項

- 個人データを取り扱う情報システムの使用状況の監視
- 個人データへのアクセス状況（操作内容も含む）の監視

※ 個人データを取り扱う情報システムを監視する内容が個人情報に該当する場合があることに留意する。

3) 従業者の監督（法第２１条）

法第２１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。

個人情報取扱事業者は、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。

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事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、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、派遣社員も含まれる。

【従業者に対して必要かつ適切な監督を行っていない場合】

事例１）　従業者が、個人データの安全管理措置を定める規程等に従って業務を行っていることを、予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）　内部規程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し、それを放置した結果、紛失し、個人データが漏えいした場合

【従業者のモニタリングを実施する上での留意点】

個人データの取り扱いに関する従業者及び委託先の監督、その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリング（以下「モニタリング」という）を実施する場合は、次の点に留意する。

その際、雇用管理に関する個人情報の取扱いに関する重要事項を定めるときは、あらかじめ労働組合等に通知し、必要に応じて、協議を行うことが望ましい。また、その重要事項を定めたときは、労働者等に周知することが望ましい。

なお、本ガイドライン及び厚生労働省告示第　　号「雇用管理に関する個人情報の適正な取扱を確保するために事業者が講ずべき措置に関する指針」第三 九 （一）に規定する雇用管理に関する個人情報の取り扱いに関する重要事項とは、モニタリングに関する事項等をいう。

- モニタリングの目的、即ち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業者に明示すること。
- モニタリングの実施に関する責任者とその権限を定めること。
- モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底すること。
- モニタリングの実施状況については、適正に行われているか監査、又は確認を行うこと。

4)　委託先の監督（法第２２条）

法第２２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。

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、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らない。

「必要かつ適切な監督」には、委託契約において委託者である個人情報取扱事業者が定める安全管理措置の内容を契約に盛り込むとともに、当該契約の内容が遵守されていることを、予め定めた間隔で定期的に確認することも含まれる。

また、委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意を要する。

【受託者に必要かつ適切な監督を行っていない場合】

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後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わず、かつ受託者の個人データの取扱状況の確認を怠り、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

【個人データの取扱いを委託する場合に契約書への記載が望まれる事項】

- 委託者及び受託者の責任の明確化
- 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
  - 委託契約範囲外の加工、利用の禁止
  - 委託契約範囲外の複写、複製の禁止
  - 委託処理期間
  - 委託処理終了後の個人データの返還・消去・廃棄に関する事項
- 再委託に関する事項
  - 再委託を行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
- セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

(4) 第三者への提供（法第２３条関連）

① 法第２３条第１項関連

個人情報取扱事業者は、あらかじめ※1、本人の同意を得※2ないで、個人データを第三者に提供してはならない（１．(4)※電話帳、カーナビゲーションシステム等の取扱いについての場合を除く。）。同意の取得に当たっては、事業の性質及び個人情報の取扱い状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示すこと。

※１「あらかじめ」とは、「個人データの第三者への提供にあたりあらかじめ」をいう。

※２「本人の同意を得（る）」については、１．(10)参照。

【第三者提供とされる事例】（ただし、法第２３条第４項各号の場合を除く。）
事例１）親子兄弟会社、グループ会社の間で個人データを交換する場合
事例２）フランチャイズ組織の本部と加盟店の間で個人データを交換する場合
事例３）同業者間で、特定の個人データを交換する場合
事例４）外国の会社に国内に居住している個人の個人データを提供する場合

【第三者提供とされない事例】（ただし、利用目的による制限がある。）
事例）同一事業者内で他部門へ個人データを提供すること。

ただし、以下の場合は本人の同意なく第三者への提供を行うことができる。

ｉ．法第２３条第１項第１号関連

法第２３条第１項第１号 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。 一　法令に基づく場合

法令に基づいた個人データを提供する場合は、本人の同意なく第三者への提供を行

うことができる。

※ 事例は、２．(1)⑤ｉ．と同様。

【追加事例】

事例）法第４２条第３項に基づき認定個人情報保護団体が対象事業者に資料提出等を求める場合

ii．法第２３条第１項第２号関連

法第２３条第１項第２号 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。 二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

人（法人を含む。）の生命又は財産といった具体的な権利利益が侵害されるおそれがあり、これを保護するために個人データの提供が必要であり、かつ、本人の同意を得ることが困難である場合（他の方法により、当該権利利益の保護が十分可能である場合を除く。）は、本人の同意なく第三者への提供を行うことができる。

※ 事例は、２．(1)⑤ii．と同様。

iii．法第２３条第１項第３号関連

法第２３条第１項第３号 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。 三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって本人の同意を得ることが困難であるとき。

公衆衛生の向上又は心身の発展途上にある児童の健全な育成のために特に必要な場合であり、かつ、本人の同意を得ることが困難である場合（他の方法により、公衆衛生の向上又は児童の健全な育成が十分可能である場合を除く。）は、本人の同意なく第三者への提供を行うことができる。

※ 事例は、２．(1)⑤iii．と同様。

iv．法第２３条第１項第４号関連

法第２３条第１項第４号

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

国の機関等が公的な事務を実施する上で、民間企業等の協力を得る必要がある場合であって、協力する民間企業等が当該国の機関等に個人データを提供することについて、本人の同意を得ることが当該事務の遂行に支障を及ぼすおそれがある場合は、本人の同意なく第三者への提供を行うことができる。

※ 事例は、２．(1)⑤ⅳ．と同様。

② 法第２３条第２項関連

個人情報取扱事業者は、第三者提供におけるオプトアウト[※1]を行っている場合には、本人の同意なく、個人データを第三者に提供することができる。

※１「第三者提供におけるオプトアウト」とは、提供にあたりあらかじめ、以下のｉ．～ⅳ．の情報を、本人に通知する又は本人が容易に知り得る状態に置いておく[※2]とともに、本人の求めに応じて第三者への提供を停止することをいう。

※２「本人が容易に知り得る状態」については、１．(11)参照。

【オプトアウトが認められている事例】

事例１）住宅地図業者（表札を調べて住宅地図を作成し、販売（不特定多数への第三者提供））

事例２）データベース事業者（ダイレクトメール用の名簿等を作成し、販売）

ｉ．法第２３条第２項第１号関連

法第２３条第２項第１号

個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。