モニタリング事項	当社の対応状況	改善の求め	改善要求に対する対応
【基本方針の策定】 基本方針を策定しているか。基本方針はガイドラインが求める事項を満たしているか。 ＊事業者の名称 ＊関係法令・ガイドライン等の遵守 ＊安全管理措置に関する事項 ＊質問及び苦情処理の窓口 等			
過去１年間、基本方針の改訂を行ったことがあるか。ある場合、どのような点を改訂したか。			
【個人情報取扱規程の策定】 個人情報取扱規程を策定しているか。個人情報取扱規程はガイドラインが求める事項を満たしているか。 ＊取得、利用、保管、廃棄の各段階に安全管理措置を規定しているか。 ＊事務フローは定められているか。			
過去１年間、個人情報取扱規程の改訂を行ったことがあるか。ある場合、どのような点を改訂したか。			
組織的安全管理措置			
【組織体制の整備】 組織体制として以下の事項が定められているか。 ＊事務における責任者の設置及び責任の明確化 ＊事務取扱担当者の明確化及びその役割の明確化 ＊事務取扱担当者が取り扱う個人データの範囲の明確化 ＊事務取扱担当者が個人情報取扱規程に違反している事実又は兆候を把握した場合の責任者への報告連絡体制 ＊情報漏えい等事案の発生又は兆候を把握した場合の従業者から責任者等への報告連絡体制 ＊個人データを複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化			
過去１年間、組織体制の変更を行ったことがあるか。ある場合、どのような点を見直したか。			
【個人情報取扱規程に基づく運用】 個人情報取扱規程に基づく運用状況を確認するため、以下の事項に関して、システムログ又は利用実績を記録しているか。 ＊個人情報データベース等の利用・出力状況の記録 ＊書類・媒体等の持出しの記録 ＊個人情報データベース等の削除・廃棄記録 ＊削除・廃棄を委託した場合、これを証明する記録等 ＊個人情報データベース等を情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録			
過去１年間、個人情報取扱規程の運用状況の確認の記録事項を変更したことはあるか、ある場合どのような点を変更したか。			
【取扱状況を確認する手段の整備】 個人情報データベース等の取扱状況を確認するため、以下の事項を記録する手段を整備しているか。当該個人情報データベース等には、個人情報が記載されていないか。 ＊個人情報データベース等の種類、名称 ＊責任者、取扱部署 ＊利用目的 ＊削除・廃棄状況 ＊アクセス権を有する者			
過去１年間、取扱状況を確認する手段を変更したことはあるか。ある場合、どのような点を変更したか。			
【情報漏えい等事案に対応する体制の整備】 情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するため、以下に掲げる体制が整備されているか。 ⑴ 事業者内部における報告、被害の拡大防止 ⑵ 事実関係の調査、原因の究明 ⑶ 影響範囲の特定 ⑷ 再発防止策の検討・実施 ⑸ 影響を受ける可能性のある本人への連絡等 ⑹ 事実関係、再発防止策等の公表 ⑺ 個人情報保護委員会への報告			
過去１年間において、情報漏えい等の事案があった場合（委託先、再委託先等の情報漏えい等を含む。）、どのように対応したか。			
【取扱状況の把握及び安全管理措置の見直し】 個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善のためにどのような体制を整備しているか。 ・個人データの取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施しているか。 ・外部の主体による監査も実施しているか。			
過去１年間において、監査やモニタリングの体制に変更がある場合、どのような点が変更されたか。			
人的安全管理措置			
【事務取扱担当者の監督】 過去１年間、事務取扱責任者は、個人データが個人情報取扱規程に基づき適正に取り扱われるよう、事務取扱担当者に対してどのような監督を行ってきたか。			

【事務取扱担当者の教育】 ＊事務取扱責任者は、過去１年間、事務取扱担当者その他の役職員に対して、個人データの適正な取扱いに関してどのような研修・教育を行ってきたか。 ＊就業規則等に個人データについての秘密保持に関する事項が盛り込まれているか。			
物理的安全管理措置			
【個人データを取り扱う区域の管理】 個人データの情報漏えい等を防止するために、個人情報データベース等を取り扱う情報システムを管理する区域（「管理区域」）及び個人データを取り扱う事務を実施する区域（「取扱区域」）は設定されているか。 ・「管理区域」に関する物理的安全管理措置として、入退室管理及び管理区域へ持ち込む機器等の制限等がなされているか。 ・「管理区域」の入退室管理方法としては、ICカード、ナンバーキー等による入退室管理システムの設置等はなされているか。 ・「取扱区域」に関する物理的安全管理措置として、壁又は間仕切り等の設置及び座席配置の工夫等がなされているか。			
過去１年間、「管理区域」及び「取扱区域」の管理に関して問題となる事項はなかったか。			
【機器及び電子媒体等の盗難等の防止】 「管理区域」及び「取扱区域」における個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置としてどのような措置を講じているか。 （具体例） ・個人データを取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット・書庫等に保管する。 ・個人情報データベース等を取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定する。			
【電子媒体等を持ち出す場合の漏えい等の防止】 個人データが記録された電子媒体又は書類等を取扱区域又は管理区域から持ち出す場合、容易に個人情報が判明しない措置の実施、追跡可能な移送手段の利用等、安全な方策を講じられているか。 （具体例） ＊個人データが記録された電子媒体を安全に持ち出す方法としては、持出 しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用等が考えられる。ただし、行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う。 ＊ 個人データが記載された書類等を安全に持ち出す方法としては、封緘、 目隠しシールの貼付を行う。			
過去１年間、どのような場合に取扱区域又は管理区域の措置に持ち出したか。			
【個人データの削除、機器及び電子媒体等の廃棄】 個人データの委託業務を行う必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合には、個人データをできるだけ速やかに復元できない手段で削除又は廃棄することになっているか。 （具体例） ＊ 個人データが記載された書類等を廃棄する場合、焼却又は溶解等の復元不可能な手段を採用する。 ＊ 個人データが記録された機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用する。 ＊ 個人情報データベース等中の個人データを削除する場合、容易に復元できない手段を採用する。 ＊ 個人データを取り扱う情報システムにおいては、保存期間経過後における個人データの削除を前提とした情報システムを構築する。			
個人データ若しくは個人情報データベース等を削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存することになっているか。過去１年分の削除又は廃棄した記録は適切に記録されているか。			
個人データの削除・廃棄等の作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認することになっているか。過去１年分の委託先による削除・廃棄の証明書を受領しているか。			
技術的安全管理措置			
【アクセス制御】 情報システムを使用してデータを行う場合、事務取扱担当者及び当該事務で取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行うこととされているか。 （具体例） ＊個人データと紐付けてアクセスできる情報の範囲をアクセス制御により限定する。 ＊個人情報データベース等を取り扱う情報システムを、アクセス制御により限定する。 ＊ユーザーIDに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる者を事務取扱担当者に限定する。			
【アクセス者の識別と認証】 個人データを取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証することができるか。 （具体例） ＊ 事務取扱担当者の識別方法としては、ユーザーID、パスワード、磁気・ICカード等が考えられる。			

【外部からの不正アクセス等の防止】 情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用されているか。 （具体例） ＊ 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。 ＊ 情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。 ＊ 導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。 ＊ 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ＊ ログ等の分析を定期的に行い、不正アクセス等を検知する。			
過去１年間、不正アクセスがあった場合にどのように対応したか。			
【情報漏えい等の防止】 個人データをインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講じているか。 （具体例） ＊ 通信経路における情報漏えい等の防止策としては、通信経路の暗号化等が考えられる。 ＊ 情報システム内に保存されている個人データの情報漏えい等の防止策としては、データの暗号化又はパスワードによる保護等が考えられる。			
委託先管理			
【委託先の選定】 委託先の選定にあたっては、どのような基準に基づいて選定しているか。 （具体例） ＊委託先の設備 ＊技術水準 ＊従業者に対する監督・教育の状況 ＊その他委託先の経営環境等			
過去１年間、上記の基準に基づき、どのような委託先を選定したか。			
【委託契約の内容】 委託契約や覚書には、以下の事項が規程されているか。 ①秘密保持義務 ②事業所内からの特定個人情報の持出しの禁止 ③個人データの目的外利用の禁止、 ④再委託における条件 ⑤漏えい事案等が発生した場合の委託先の責任 ⑥委託契約終了後の個人データの返却又は廃棄 ⑦従業者に対する監督・教育 ⑧契約内容の遵守状況について報告を求める規定 ⑨個人データを取り扱う従業者の明確化 ⑩委託者が委託先に対して実地の調査を行うことができる規定 ⑪漏えい事案等が発生した場合の報告に関する規定			
過去１年間に締結した委託契約や覚書は上記の要件を満たしているか。			
再委託先としてどのような先があるか。			
再委託先に情報の漏えいその他の個人情報保護法違反の事由がある場合、どのように報告を求めることとされているか。			
過去１年間、委託先又は再委託先等で情報の漏えいがあった場合、どのような対応をしたか。			