個人情報取扱安全管理基準

１　個人情報の取扱いに関する基本方針、規程及び取扱手順の策定

個人情報の適正な取扱いの確保について基本方針を策定していること。

また、以下の内容を記載した個人情報の保護に関する規程及び個人情報の取扱手順等が定められていること。

⑴ 組織的安全管理措置

⑵ 人的安全管理措置

⑶ 物理的安全管理措置

⑷ 技術的安全管理措置

※　上記⑴～⑷の具体的内容については、個人情報保護委員会ホームページ（https://www.ppc.go.jp）に掲載されている「個人情報保護法ガイドライン（通則編）」の「３－４－２」の「安全管理措置（法第23条関係）」及び本会「保有する個人情報　及び特定個人情報の保護に関する規則」、「保有する個人情報及び特定個人情報保護に関する規程」を御確認ください。

２ 個人情報の取扱いに関する総括責任者及び事務取扱責任者の設置

個人情報の取扱いに関する総括責任者及び事務取扱責任者が定められており、基本方針、規程及び個人情報の取扱手順等に明記されていること。

３ 従業者の指定、教育及び監督

⑴ 個人情報の秘密保持に関する事項が就業規則等に明記されていること。

⑵ 個人情報を取り扱う従業者を指定すること。

⑶ 個人情報の取扱い、情報システムの運用・管理・セキュリティ対策及びサイバーセキュリティの研修計画を策定し、従業者に対し毎年1回以上研修等を実施していること。

また、個人情報を取り扱う従業者は、必ず1回以上研修等を受講している者としていること

⑷ 総括責任者及び事務取扱責任者は、従業者に対して必要かつ適切な監督を行うこと。

４ 管理区域の設定及び安全管理措置の実施

⑴ データや紙文書等による個人情報を管理する区域（以下「管理区域」という。）を明確にし、当該管理区域に壁又は間仕切り等を設置すること。

【管理区域の例】

・ サーバ等の重要な情報システムを管理する区域

・ 紙文書等の個人情報を保管する区域　等

⑵ ⑴で設定した管理区域について入室する権限を有する従業者を定めること。

また、入室に当たっては、用件の確認、入退室の記録、部外者についての識別化及び部外者が入室する場合は、管理者の立会い等の措置を講ずること。さらに、入退室の記録を保管していること。

⑶ ⑴で設定した管理区域について入室に係る認証機能を設定し、パスワード等の管理に関する定めの整備及びパスワード等の読取防止等を行うために必要な措置を講ずること。

⑷ 外部からの不正な侵入に備え、施錠装置、警報措置及び監視装置の設置等の措置を講ずること。

⑸ 管理区域では、許可された電子媒体又は機器等以外のものについて使用の制限等の必要な措置を講ずること。

５ セキュリティ強化のための管理策

情報資産の盗難、紛失、持出し、複写・複製、目的外の使用及び第三者への提供を防止するため以下の対策を実施していること。

⑴ 個人情報の取扱いに使用する電子計算機等は、他のコンピュータと接続しない単独による設置又は当該業務に必要な機器のみと接続していること。また、インターネット及び当該業務を実施する施設外に接続するイントラネット等の他のネットワークに接続していないこと。ただし、本会の許可を得た場合はこの限りでない。

⑵ 個人情報の取扱いにおいてサーバを使用している場合は、当該業務を実施する施設内に設置していること。また、サーバへのアクセス権限を有する従業者を定めること。さらに、部外者のアクセスは必要最小限とし、管理者の立会い等の措置を講ずること。ただし、本会の許可を得た場合はこの限りでない。

⑶ 個人情報の取扱いにおいて使用する電子計算機等は、アクセス権等を設定し、使用できる従業者を限定すること。また、アクセスログやログイン実績等から従業者の利用状況を記録し、保管していること。

⑷ 記録機能を有する機器の電子計算機等への接続制限について必要な措置を講ずること 。

⑸ 本会が貸与する文書、電子媒体及び業務にて作成した電子データを取り扱う従業者を定めること。

⑹ 業務にて作成した電子データを保存するときは、暗号化又はパスワードにより秘匿すること。また、保存した電子データにアクセスできる従業者を限定するとともにアクセスログ等から従業者の利用状況を記録し、契約期間終了後、1年以上保管していること。

⑺ 本会が貸与する文書及び電子媒体は、施錠できる耐火金庫及び耐火キャビネット等にて保管すること。また、書類の持ち出し記録等を作成していること。

⑻ 個人情報の取扱いにおいて使用する電子計算機は、従業者が正当なアクセス権を有する者であることをユーザ ID、パスワード、磁気・IC カード又は生体情報等のいずれかにより識別し、認証していること。

⑼ 個人情報の取扱いにおいて使用する電子計算機は、セキュリティ対策ソフトウェア等（ウィルス対策ソフトウェア等）を導入していること。

⑽ 業務にて作成した電子データを削除した場合は、削除した記録を作成していること。また、削除したことについて証明書等により確認できる措置を講ずること。

⑾ 個人情報の取扱いにおいて使用する電子計算機等を廃棄する場合は、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こと。

⑿ 本会の許可なく第三者に委託しないこと。

６ 事件・事故における報告連絡体制

⑴ 従業者が取扱規程等に違反している事実又は兆候を把握した場合の総括責任者及び事務取扱責任者への報告連絡体制を整備していること。

⑵ 情報の漏えい、滅失又は毀損等事案の発生又は兆候を把握した場合の従業者から総括責任者及び事務取扱責任者等への報告連絡体制を整備していること。

⑶ 情報の漏えい、滅失又は毀損等事案が発生した際の本会及び関連団体への報告連絡体制を整備していること。併せて、事実関係の調査、原因の究明及び再発防止策の検討並びに決定等に係る体制及び手順等を整備していること。

７ 情報資産の搬送及び持ち運ぶ際の保護体制

本会が貸与する文書、電子媒体及び左記書類等に基づき作成される電子データを持ち運ぶ場合は、施錠した搬送容器を使用すること。また、暗号化、パスワードによる保護、追跡可能な移送手段等により、破損、紛失、盗難等のないよう十分に配慮していること。

８ 関係法令の遵守

個人情報の保護に係る関係法令を遵守するために、必要な体制を備えていること。

９ 定期監査の実施

個人情報の管理の状況について、定期に、及び必要に応じ、随時に点検、内部監査及び外部監査を実施すること。

10　個人情報取扱状況報告書の提出

本会の求めに応じ、又は当該業務契約に基づき、各月の期間ごとの役務完了の書面提出時において、本会が指定する様式にて個人情報取扱状況報告書を提出すること。

11　情報セキュリティマネジメントシステム（以下「ISMS」という。）又はプライバシーマーク等の規格認証

ISMS（国際標準規格 ISO/IEC27001、日本工業規格 JISQ27001）、プライバシーマーク（日本工業規格 JISQ15001）等の規格認証を受けていること。

（注）委託事務の実態に即して、適宜必要な事項を追加し、又は不要な事項を省略することとする。