一般財団法人日本消防設備安全センターの

個人情報保護に関する規程

（1） 個人情報保護に関する基本方針

（2） 個人情報取扱規程

（3） 個人情報管理に関する役割分担表

（4） 個人情報の利用目的に関する事項

（5） 個人データの安全管理措置

取得・入力段階に係る取扱規程

利用・加工段階に係る取扱規程

保管・保存段階に係る取扱規程

移送・送信段階に係る取扱規程

消去・廃棄段階に係る取扱規程

漏えい事案等への対応の段階に係る取扱規程

（6） 個人データの点検・監査に係る取扱規程

（7） 個人データの外部委託に係る取扱規程

（8） 各種参考資料

委託先の選定基準・考え方

2005 年 4 月 1 日制定

一般財団法人日本消防設備安全センターの
個人情報保護に関する基本方針

第１　基本方針

一般財団法人日本消防設備安全センター（以下「当センター」という。）の業務に従事する役員及び職員（非常勤職員及び臨時職員並びに派遣職員・駐在職員を含む。）は、個人情報が重要な資産であること及び個人情報保護が当センターの事業遂行上重要であることを認識し、個人情報保護法等の趣旨と内容を理解して取り組むものとする。

さらに、個人情報保護に関するコンプライアンス・プログラム(基本方針、基本規程、実施手順書等当センターで保有する個人情報を保護するための仕組みをいう。以下同じ。)を遵守し、個人情報を正確、かつ、安全に取り扱うものとする。

第２　コンプライアンス・プログラムの目的

個人情報への不正アクセス並びに個人情報の紛失、破壊、改ざん及び漏えい等を防止するため、個人情報保護に関する方針等を定め、適切に運用するとともに、個人情報保護に関する規程等を整備して、職員等に対する周知・徹底を図ることを目的とする。

第３　当センターの取組み

基本方針を確実に実施するため、以下の活動を積極的に推進する。

(1) 役員及び職員は、個人情報に関する法令及びその他の関連する規範を遵守する。

(2) コンプライアンス・プログラムの実施及び運用に関する責任体制を整備・維持する。

(3) 役員及び職員に対して、個人情報保護に関する教育を定期的に実施する。

(4) 監査責任者を選任し、定期的に個人情報保護の取組状況を監査する。

(5) コンプライアンス・プログラムを継続的に検証する。

第４　個人情報の取扱い

(1) 個人情報の取得、利用または提供

個人情報の取得又は利用は、当センターの正当な事業の範囲内で行うことを明確に定め、個人情報の提供もその目的に限定し適切に取り扱う。

(2) 安全管理の実施

個人情報への不正アクセス並びに個人情報の紛失、破壊、改ざん及び漏えい等が起こらないように規程等を整備し、安全管理を確実に実施する。

(3) 受託業務・委託業務

受託業務及び委託業務処理においては、個人情報を保護するための措置及び委託元・受託元との責任関係を契約書に明記する。

第５　個人データの第３者への提供

個人データの第三者提供については、個人情報の保護に関する法律第 23 条に規定する場合を除き、本人の同意なく第三者に個人データを提供しない。

個 人 情 報 取 扱 規 程

（目的）

第１条　本規程は、一般財団法人日本消防設備安全センター（以下「安全センター」という。）が業務上取扱う個人情報に関して遵守すべき事項及び個人情報保護に係る体制を定め、もって個人情報の適正な取扱いを確保することを目的とする。

（定義）

第２条　本規程における各用語の定義は、「個人情報の保護に関する法律」及び関係各省庁の個人情報保護に関するガイドラインの例によるものとする。

（適用対象者）

第３条　本規程は、すべての従業者（業務に従事する役員及び職員（非常勤職員及び臨時職員並びに派遣職員を含む。））に適用する。

（利用目的）

第４条　安全センターの定める個人情報の利用目的は、個人情報を利用する範囲を本人が合理的に予想できる程度に特定するものとする。

２　安全センターは、利用目的をホームページ又は事務所内の見やすい場所に掲示して公表するとともに、個人情報を書面を通じて取得するときは、当該書面又は添付書面にその旨を明示する。

３　安全センターは、利用目的を変更するときは、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲内で行い、変更後の利用目的を前項の定めるところにより公表、明示する。

（個人情報の取得）

第５条　安全センターは、業務上必要な範囲内で、かつ、適法で公正な手段により個人情報を取得する。

（個人情報の利用）

第６条　安全センターは、利用目的の達成に必要な範囲を超えて個人情報を取り扱わない。

２　安全センターは、前項に定める範囲を超えて個人情報を取り扱うときは、あらかじめ本人の同意を得る。

（データ内容の正確性の確保）

第７条　安全センターは、利用目的の達成に必要な範囲内において個人データを正確かつ最新の内容に保つように努める。

（第三者への提供）

第８条　安全センターは、個人データを第三者に提供するときは、その目的に限定して適切に取り扱うほか、次に掲げる事項を示した上で、本人の同意を得る。

（１）個人データを提供する第三者

（２）提供を受けた第三者における利用目的
（３）第三者に提供される情報の内容

（センシティブ情報の取扱い）
第９条　安全センターは、政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活並びに犯罪歴に関する個人情報（以下「センシティブ情報」という。）の取扱いが安全センターの事業の適切な業務運営を確保するために必要であり、当該業務の遂行に必要な範囲内で取得、利用又は第三者への提供を行うときは、本人の同意を得る。

（安全管理措置）
第１０条　安全センターは、個人データの安全管理のために必要かつ適切な措置を講じる。
２　安全センターが個人データの取扱いの全部又は一部を委託するときは、委託先の選定基準を定め、あらかじめ委託先の情報管理体制を確認し、委託後の業務遂行状況を監視し、事故発生時の責任関係を明確にするなど、委託先に対する必要かつ適切な監督を行う。
３　安全センターは、事業の遂行に際して取り扱う個人情報の漏洩事案等の事故が生じたときは、本人への通知及び委託元への報告を行うとともに、二次被害の防止等の観点から必要に応じ事実関係を公表する。

（開示等請求への対応）
第１１条　安全センターは、委託元の保有個人データに係る保険会社の保有個人データに係る開示等を求められたときは、これを所属関係会社に取り次ぐものとする。
２　安全センターの保有個人データに係る開示等請求に関する手続、その他の事項は別途定める。

（苦情への対応）
第１２条　安全センターは、個人情報の取扱いに関する苦情を受けたときは、迅速かつ適切に対応する。
２　前項の目的を達成するため、苦情の申出先を公表するほか、苦情処理手順を策定するなど必要な体制を整備する。

（基本方針の策定）
第１３条　安全センターは、次の事項を含む基本方針を策定・公表し、実効性あるものとするための体制整備に努める。
（１）個人情報取扱事業者の名称
（２）安全管理措置に関する質問及び苦情処理の窓口
（３）個人データの安全管理に関する宣言
（４）基本方針の継続的改善の宣言
（５）関係法令遵守の宣言
（６）個人情報の利用目的

（情報管理責任者の設置）

第１４条　安全センターは、個人情報保護の取組みを総括する情報管理責任者を設置する。情報管理責任者は常務理事（事務担当）が務める。

２　情報管理責任者は、次の事項を担当する。

（１）個人情報の適正な取扱いを確保するための全社的な施策の立案及びその実施状況の監督

（２）本規定その他の個人情報保護に係る規定の整備及びその遵守状況の監督

（３）情報管理者及び本人確認情報管理者の任命、報告徴求、助言及び指導

（４）従業者に対する教育・研修の企画

（５）個人情報漏えい等事案への対応

（６）その他個人データの安全管理に関する事項のうち事業全体に関するもの

３　次に掲げる事項は、情報管理責任者が決定する。

（１）前条に定めるプライバシーポリシーの制定及び改正

（２）前項第３号に掲げる者の任命

（３）本規定第４条に定める個人情報の利用目的の制定及び改正

（４）個人データの安全管理に係る取扱規定の制定及び改正

（５）個人データの開示等請求への対応に関する規定等の制定及び改正

（６）漏えい事案等が発生した場合における対応（事実関係の調査、原因・責任の究明、委託元（保険会社）との相談、対応方針の決定など）

４　前項第１号、第３号、及び第４号に定める事項の立案者は情報管理責任者が指名する。

（情報管理者、本人確認情報管理者）

第１５条　情報管理責任者は、個人データを取り扱う組織の単位を定め、組織単位毎に情報管理者を指名し、次の事項を所管させる。

（１）個人データの取扱者の指定及び変更等の管理

（２）個人データの利用申請の承認及び記録等の管理

（３）個人データを取扱う保管媒体の設置場所の指定及び変更等

（４）個人データの管理区分及び権限についての設定及び変更の管理

（５）個人データの取扱状況の把握

（６）委託先における個人データの取扱状況等の監督

（７）個人データの安全管理に関する教育・研修の実施

（８）情報管理責任者に対する報告

（９）その他所管部署における個人データの安全管理に関すること

２　本人確認情報管理者は、次に掲げる措置を担当する。

（１）本人確認機能の整備

（２）本人確認に関する情報の不正使用防止機能の整備

（３）本人確認に関する情報が他人に知られないための対策

（個人データ管理台帳）

第１６条　情報管理者は、次の事項を記載した「個人情報管理台帳」を作成し、情報管理責任者に提出する。

（１）取得する個人データの項目
（２）利用目的
（３）保管場所・保管方法・保管期限
（４）管理部署
（５）アクセス制御の状況

（個人データ取扱状況の点検）
第１７条　情報管理者は、「個人データの取扱状況の点検に係る規程」に沿って、個人データ取扱部署が自ら行う取扱状況の点検につき、点検計画を定め、点検責任者及び点検担当者を指名し、それらの者をして点検させる。
２　情報管理者は、点検の結果、取扱規定違反等を把握したときは、その改善を行う。
３　情報管理者は、前項の点検計画及び前項の改善事項につき情報管理責任者に報告する。

（漏えい等事案への対応）
第１８条　個人情報取扱部署は、個人情報の漏えい、滅失又は毀損の可能性がある事案（以下「漏えい等事案」という。）を把握したときは、直ちに情報管理責任者に報告する。
２　情報管理責任者は、前項の報告を受けた事案が個人情報の漏えい、滅失又は毀損につながる可能性があると認められるときは、事実内容の確認、原因の調査、内外への報告、事後対策・再発防止策の検討を行う。

（委託先に対する監督）
第１９条　情報管理責任者は、委託先に対し以下の各号の事項を実施する。
（１）委託先の個人情報保護体制が十分であることを確認した上で委託先を選定する。
（２）委託先との間で、次の事項を含む契約書等を締結する。
① 委託者の監督・監査・報告徴収に関する権限
② 委託先における個人データの漏えい、盗用、改ざん及び目的外利用の禁止
③ 再委託における条件
④ 漏えい事案等が発生した際の委託先の責任

（その他の安全管理措置）
第２０条　安全センターは、取扱う個人データの漏えい、滅失又は毀損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、技術的に適切な措置を講じるものとする。
２　安全管理措置は、「取得・入力」「利用・加工」「保管・保存」「移送・送信」「消去・廃棄」の個人データの管理段階に応じて定めるものとする。ただし、各段階を通じた措置を定めることを妨げない。

（違反行為に対する処置）
第２１条　安全センターは、第３条に定める適用対象者が本規程に違反した場合は、誓約書（同意書・就業規則等）の内容に従い懲戒処分を行うことがある。

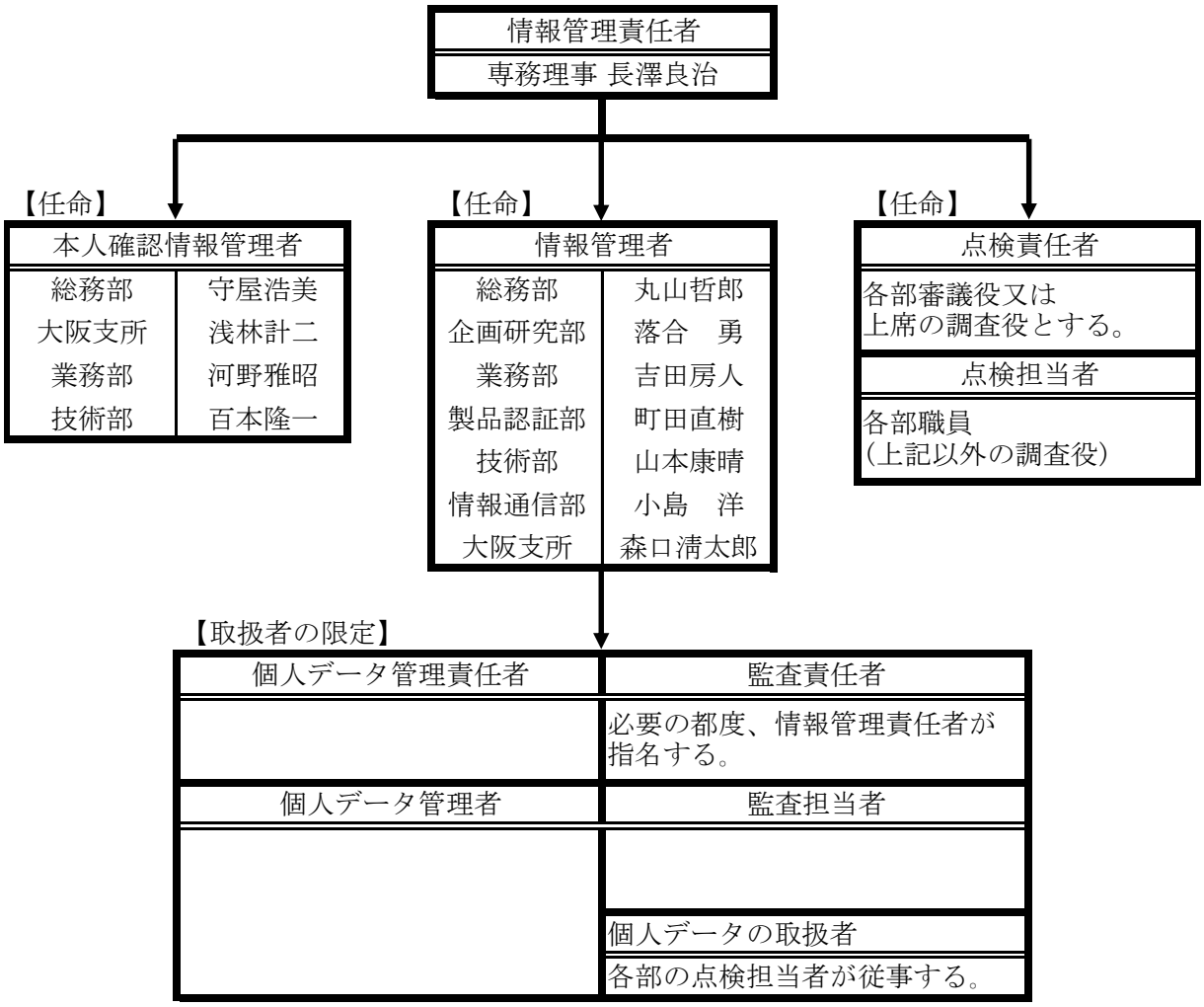
（受託業務の取り扱い）
第２２条　受託業務処理においては、個人情報を保護するための措置及び委託元との責任関係を契約書等（覚書・念書・指示書等を含む。）に記載し、適切に取り扱うものとする。

（本規程の改定）
第２３条　本規程の改廃は情報管理責任者の決定により効力を発する。

附　則
本規程は、2005 年４月１日から実施する。
附　則
本規程は、２０１３年４月１日から実施する。

2013年4月1日現在

個人情報管理役割分担表（組織図）



（注）　ＩＤ、パスワードは、別に定める。

個人情報の利用目的に関する事項

一般財団法人日本消防設備安全センター（以下「安全センター」という。）は、安全センター定款第４条に規定する各種の事業（別紙）を行っており、これらの事業を通じて取得した個人情報を、例えば、講習会受講者管理等のために利用するほか、講師名簿や各種委員名簿を作成して、これを講師・委員等管理に活用いたします。

また、保守協会・防災事業団体役職員名簿や理事長表彰受章者名簿等を整理し、関係者との連携協調のために利用いたします。

さらに、月刊フェスク購読者名簿により刊行物のサービスに関する情報のお知らせに利用します。

保険・共済事業に関して取得した個人情報については、保険・共済加入者の管理のため活用するほか、業務委託先等に情報提供を行うことがあります。

なお、利用目的を変更する場合には、その内容をご本人に対して通知、又は事業所内に掲示する等の方法により公表いたします。

その他、ご不明な点は、下記にお問い合せ下さい。

【お問い合せ窓口】
一般財団法人日本消防設備安全センター
所在地：105-0001
東京都港区虎ノ門 2-9-16　日本消防会館７階
電話　03-3501-7911　FAX 03-3501-7980
総 務 部
（受付時間：月曜日～金曜日　９：００～１７：００　　但し祝祭日を除きます）

定款第４条（事　業）

第４条　この法人は、前条の目的を達成するため、次の事業を行う。
（１）消防防災技術者の養成のための研修及び講習
（２）消防防災用設備機器等の認定、評定、評価、推奨等
（３）消防防災に関連した情報通信システムの調査、設計及び監理
（４）消防防災に係る国際協力
（５）消防防災に関する調査研究、調査研究等への助成及び技術開発の推進
（６）消防法令に関する違反是正の支援
（７）防火防災意識の啓発及び普及
（８）消防防災関係団体等への助言及び情報提供
（９）前各号の事業に附帯する事業及び前条の目的を達成するために必要な事業

個人情報取扱規程第２０条に定める
個人データの取得・入力段階に係る取扱規程

（目的）

第１条　本規程は、一般財団法人日本消防設備安全センター（以下「安全センター」という。）における個人データの安全管理措置のうち、個人データの「取得・入力」段階の取扱いについて定めたものである。

（定義）

第２条　「取得」とは、本人又は第三者から個人データを物理的及び電子的手段により取得することなどをいう（安全センター内の他部門からの取得は含まない）。

２　「入力」とは、取得した個人データをデータベース等に物理的及び電子的に入力することなどをいう。

（取得・入力に関する取扱者の役割・責任及び取扱者の限定）

第３条　個人データ管理責任者は、「個人情報管理役割分担表」により、個人データの取得・入力に関する取扱者の役割・責任を定め、組織内に周知しなければならない。

２　個人データ管理者は、各部署において業務上必要な者に限り個人データの取得・入力が行われるよう取扱者を限定しなければならない。

（センシティブ情報の取得・入力に関する取扱者の限定）

第４条　個人データ管理者は、個人データのうち、政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報（以下、「センシティブ情報」という。）の取得・入力の取扱者を必要最小限に限定しなければならない。

（取得・入力の対象となる個人データの限定）

第５条　個人データ管理者は、取得・入力する個人データを業務上必要な範囲内のものに限定しなければならない。

（取得・入力時の照合及び確認手続き）

第６条　個人データの取扱者は、取得・入力時に個人データの内容を照合及び確認しなければならない。

２　個人データの取扱者は、個人データの取得・入力に際して、「個人データ管理台帳」に記載の範囲内の個人データであることを確認しなければならない。

（取得・入力の規定外作業に関する申請及び承認手続き）

第７条　個人データの取扱者は、本規程に定める以外の方法で個人データを取得・入力する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

（機器・記録媒体等の管理手続き）
第８条　個人データ管理者は、取得・入力した個人データが保存された機器・記録媒体等の設置場所の指定並びに管理区分及び権限の設定をし、必要に応じ変更しなければならない。
２　個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・記録媒体等を適切に保管しなければならない。

（個人データへのアクセス制御）
第９条　個人データ管理者は、取得・入力した個人データへのアクセスを制御するために、取得・入力した個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。
①　個人データの入力に必要なＩＤ及びパスワードの管理を徹底する。
②　個人データが保存された機器・記録媒体等を保管するスペースへの部外者の立ち入りを制限する。
③　受信した郵便物やＦＡＸ等の個人データについて適切な管理を行う。

（取得・入力状況の記録及び分析）
第 10 条　個人データの取扱者は、個人データを取得・入力する場合、「個人データ管理台帳」に必要事項を記載しなければならない。
２　個人データ管理者は、必要に応じ、「個人データ管理台帳」に記載された事項を確認し、個人データの取得・入力が適正に行われているか否かを分析するものとする。

（センシティブ情報の取得の制限）
第 11 条　個人データの取扱者は、センシティブ情報については、次に掲げる場合を除くほか、取得を行わないこととする。
①　法令等に基づく場合
②　人の生命、身体又は財産の保護のために必要がある場合
③　公衆衛生の向上又は児童の健全な育成の推進のため特に必要がある場合
④　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
⑤　源泉徴収事務等の遂行上必要な範囲において、政治・宗教等の団体若しくは労働組合への所属若しくは加盟に関する従業員等のセンシティブ情報を取得する場合
⑥　相続手続による権利義務の移転等の遂行に必要な限りにおいて、センシティブ情報を取得する場合

（センシティブ情報の取得に際して本人同意が必要である場合における本人同意の取得及び本人への説明事項）
第 12 条　個人データの取扱者は、郵送等により取得した個人データが含まれる文書等にセンシティブ情報が含まれている場合は、原則として、本人の指定した方法により、当該情報を速やかに本人に返却若しくは廃棄する。
　ただし、当該文書等に記載された他の情報が業務遂行上必要な場合、取扱者は、直ちに当該センシティブ情報の記載部分を判読不能な状態にして取得するものとする。

個人情報取扱規程第２０条に定める
個人データの利用・加工段階に係る取扱規程

（目的）

第１条　本規程は、一般財団法人日本消防設備安全センター（以下「安全センター」という。）における個人データの安全管理措置のうち、個人データの「利用・加工」段階の取扱いについて定めたものである。

（定義）

第２条　「利用」とは、個人データを利用目的の範囲内で取扱うことなどをいう。

２　「加工」とは、個人データの更新を行うこと、又は個人データを利用し、新たなデータベースを作成することなどをいう。

３　「管理区域外」とは、事務所外（又は事務所から客先等の往復過程以外）をいう。

（利用・加工に関する取扱者の役割・責任及び取扱者の限定）

第３条　個人データ管理責任者は、「個人情報管理役割分担表」により、個人データの利用・加工に関する取扱者の役割・責任を定め、組織内に周知しなければならない。

２　個人データ管理者は、各部署において、業務上必要な者に限り個人データの利用・加工が行われるよう取扱者を限定しなければならない。

（センシティブ情報の利用・加工に関する取扱者の限定）

第４条　個人データ管理者は、個人データのうち、政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報（以下、「センシティブ情報」という。）の利用・加工の取扱者を必要最小限に限定しなければならない。

（利用・加工の対象となる個人データの限定）

第５条　個人データ管理者は、利用・加工する個人データを業務上必要な範囲内のものに限定しなければならない。

（利用・加工時の照合及び確認手続き）

第６条　個人データの取扱者は、利用・加工に際して、「個人データ管理台帳」に記載の範囲内の個人データであることを照合及び確認しなければならない。

（利用・加工の規定外作業に関する申請及び承認手続き）

第７条　個人データの取扱者は、本規程に定める以外の方法で個人データを利用・加工する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

（機器・記録媒体等の管理手続き）

第８条　個人データ管理者は、利用・加工した個人データが保存された機器・記録媒体等の設置場所の指定並びに管理区分及び権限の設定をし、必要に応じ変更しなければならない。

２　個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・記録媒体等を適切に保管しなければならない。

（個人データへのアクセス制御）

第９条　個人データ管理者は、利用・加工する個人データへのアクセスを制御するために、利用・加工する個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。

①　個人データの利用・加工に必要なＩＤ及びパスワードの管理を徹底する。

②　個人データが保存された機器・記録媒体等を保管するスペースへの部外者の立ち入りを制限する。

２　個人データ管理者は、センシティブ情報へのアクセス制御について、当該情報の利用・加工を認められた必要最小限の取扱者に限り利用・加工が行われるよう、ＩＤ及びパスワードの管理を徹底しなければならない。

（利用・加工状況の記録及び分析）

第 10 条　個人データの取扱者は、個人データを利用・加工する場合、「個人情報管理台帳」に必要事項を記載しなければならない。

２　個人データ管理者は、必要に応じ、「個人情報管理台帳」に記載された内容を確認し、個人データの利用・加工が適正に行われているか否かを分析するものとする。

（センシティブ情報の利用・加工の制限）

第 11 条　個人データの取扱者は、センシティブ情報については、次に掲げる場合を除くほか、利用を行わないこととする。

①　法令等に基づく場合

②　人の生命、身体又は財産の保護のために必要がある場合

③　公衆衛生の向上又は児童の健全な育成の推進のため特に必要がある場合

④　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

⑤　源泉徴収事務等の遂行上必要な範囲において、政治・宗教等の団体若しくは労働組合への所属若しくは加盟に関する従業員等のセンシティブ情報を利用する場合

⑥　相続手続による権利義務の移転等の遂行に必要な限りにおいて、機微(センシティブ)情報を利用する場合

（個人データの管理区域外への持ち出しに関する措置）

第 12 条　個人データの管理区域外への持ち出しは、原則として認めない。

２　個人データ管理責任者は、「個人情報管理役割分担表」により、個人データの管理区域外への持ち出しに関する取扱者の役割・責任を定め、組織内に周知しなければならない。

3　個人データの管理者は、個人データの管理区域外への持ち出しに関する取扱者を必要最小限に限定しなければならない。
4　個人データの取扱者は、個人データの管理区域外への持ち出しに該当するか否かを、「個人情報管理台帳」により照合及び確認し、業務上必要最小限のものに限定しなければならない。
5　個人データの取扱者は、個人データを管理区域外に持ち出す場合には、個人データ管理者に申請し、承認を得たうえで行わなければならない。
6　個人データの取扱者は、個人データを管理区域外に持ち出す場合には、別に定める件数等に限るとともに、個人データが保存された機器・媒体等を常時携行するなど適切に管理しなければならない。
7　個人データの取扱者は、個人データを管理区域外に持ち出す場合には、「個人情報管理台帳」に必要事項を記載しなければならない。
　また、個人データ管理者は必要に応じ、「個人情報管理台帳」に記載された事項を確認し、個人データの管理区域外の持ち出しが適正に行われているか否かを分析するものとする。

（個人データの利用者の識別及び認証）
第 13 条　個人データ管理者は、個人データを処理する情報システムについて、個人データを利用・加工する取扱者の識別及び認証機能を、設けなければならない。

（個人データの管理区分の設定及びアクセス制御）
第 14 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの利用・加工段階における管理区分の設定及びアクセス制御機能を設けなければならない。

（個人データへのアクセス権限の管理）
第 15 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの利用・加工段階におけるアクセス権限に関する機能を設けなければならない。
2　個人データ管理者は、第１項のアクセス権限に関する機能の設定に当たっては、センシティブ情報の利用・加工の取扱者が必要最小限の者に限定されるよう設定しなければならない。

（個人データの漏えい・き損等防止策）
第 16 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの利用・加工段階における漏えい・き損等の防止策を講じなければならない。

（個人データへのアクセス記録及び分析）
第 17 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの利用・加工段階におけるアクセス記録を取得し、必要な期間保管するとともに、必要に応じてこれを分析しなければならない。

（個人データを取扱う情報システムの稼動状況の記録及び分析）

第 18 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの利用・加工段階におけるシステムの稼動状況に関し記録を取得し、必要な期間保管するとともに、必要に応じてこれを分析しなければならない。

個人情報取扱規程第２０条に定める
個人データの保管・保存段階に係る取扱規程

（目的）

第１条　本規程は、一般財団法人日本消防設備安全センター（以下「安全センター」という。）における個人データの安全管理措置のうち、個人データの「保管・保存」段階の取扱いについて定めたものである。

（定義）

第２条　「保管」とは、文書等をオフィスフロア内に置き管理することなどをいう。

２　「保存」とは、文書等をオフィスフロア外（書庫）に置き廃棄に至るまで管理すること、及びパソコンや電子媒体等に電子データを格納し消去に至るまで管理することなどをいう。

（保管・保存に関する取扱者の役割・責任及び取扱者の限定）

第３条　個人データ管理責任者は、「個人情報管理役割分担表」により、個人データの保管・保存に関する取扱者の役割・責任を定め、組織内に周知しなければならない。

２　個人データ管理者は、各部署において、業務上必要な者に限り個人データの保管・保存が行われるよう取扱者を限定しなければならない。

（センシティブ情報の取得・入力に関する取扱者の限定）

第４条　個人データ管理者は、個人データのうち、政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報(以下、「センシティブ情報」という。)の保管・保存の取扱者を必要最小限に限定して定めなければならない。

（保管・保存の対象となる個人データの限定）

第５条　個人データ管理者は、保管・保存する個人データを業務上必要な範囲内のものに限定しなければならない。

（保管・保存の規定外作業に関する申請及び承認手続き）

第６条　個人データの取扱者は、本規定に定める以外の方法で個人データを保管・保存する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

（機器・記録媒体等の管理手続き）

第７条　個人データ管理者は、保管・保存した個人データが保存された機器・記録媒体等の設置場所の指定並びに管理区分及び権限の設定をし、必要に応じ変更しなければならない。

２　個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・記録媒体等を適切に保管しなければならない。

（個人データへのアクセス制御）

第８条　情報管理責任者は、保管・保存する個人データへのアクセスを制御するために、保管・保存した個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。

①　個人データの保管・保存に必要なＩＤ及びパスワードの管理を徹底する。

②　個人データが保存された機器・記録媒体等を保管するスペースへの部外者の立ち入りを制限する。

２　個人データ管理者は、センシティブ情報へのアクセス制御について、当該情報の保管・保存を認められた必要最小限の取扱者に限り保管・保存が行われるようＩＤ及びパスワードを付与するとともに、ＩＤ及びパスワードの管理を徹底しなければならない。

（保管・保存状況の記録及び分析）

第９条　個人データの取扱者は、個人データを保管・保存する際に、「個人データ管理台帳」に必要事項を記載しなければならない。

ただし、保険会社所定の事務処理要領に基づき保管・保存する場合はこの限りでない。

２　個人データ管理者は、必要に応じ、「個人情報管理台帳」に記載された内容を確認し、個人データの保管・保存が適正に行われているか否かを分析するものとする。

（保管・保存に関する障害発生時の対応・復旧手続き）

第 10 条　個人データ管理者は、保管・保存した個人データについて、取扱者に対し定期的にバックアップを行うよう徹底するとともに、保管・保存した個人データに障害が発生した際にはバックアップデータにより復旧させなければならない。

２　個人データの取扱者は、作成したバックアップデータを適切に管理しなければならない。

（個人データの利用者の識別及び認証）

第 11 条　個人データ管理者は、個人データを処理する情報システムについて、個人データを保管・保存する取扱者の識別及び認証機能を設けなければならない。

（個人データの管理区分の設定及びアクセス制御）

第 12 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの保管・保存段階における管理区分の設定及びアクセス制御機能を、設けなければならない。

（個人データへのアクセス権限の管理）

第 13 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの保管・保存段階におけるアクセス権限に関する機能を設けなければならない。

２　個人データ管理者は、前項のアクセス権限に関する機能の設定に当たっては、センシティブ情報の保管・保存の取扱者が必要最小限の者に限定されるよう設定しなければならない。

（個人データの漏えい・き損等防止策）

第 14 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの保管・保存段階における漏えい・き損等の防止策を講じなければならない。

（個人データへのアクセス記録及び分析）

第 15 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの保管・保存段階におけるアクセス記録を取得し、必要な期間保管するとともに、必要に応じてこれを分析しなければならない。

（個人データを取扱う情報システムの稼動状況の記録及び分析）

第 16 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの保管・保存段階におけるシステムの稼動状況に関し記録を取得し、必要な期間保管するとともに、必要に応じてこれを分析しなければならない。

個人情報取扱規程第２０条に定める
個人データの移送・送信段階に係る取扱規程

（目的）

第１条　本規程は、一般財団法人日本消防設備安全センター（以下「安全センター」という。）における個人データの安全管理措置のうち、個人データの「移送・送信」段階の取扱いについて定めたものである。

（定義）

第２条　「移送」とは、物理的な手段により個人データを異なる場所や人に移すことなどをいう。

２　「送信」とは、電子的な手段により個人データを異なる場所や人に移すことなどをいう。

（移送・送信に関する取扱者の役割・責任及び取扱者の限定）

第３条　個人データ管理責任者は、「個人データ管理役割分担表」により、個人データの移送・送信に関する取扱者の役割・責任を定め、組織内に周知しなければならない。

２　個人データ管理者は、各部署において業務上必要な者に限り個人データの移送・送信が行われるよう取扱者を限定しなければならない。

（センシティブ情報の移送・送信に関する取扱者の限定）

第４条　個人データ管理者は、個人データのうち、政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報（以下、「センシティブ情報」という。）の移送・送信の取扱者を必要最小限に限定して定めなければならない。

（移送・送信の対象となる個人データの限定）

第５条　個人データ管理者は、移送・送信する個人データを業務上必要な範囲内のものに限定しなければならない。

（移送・送信時の照合及び確認手続き）

第６条　個人データの取扱者は、個人データの移送・送信に際して、以下のとおり照合及び確認を行わなければならない。

①　事前に「個人情報管理台帳」に記載の範囲内であることを確認する。

②　移送・送信先に相違がないか照合する。

③　移送・送信先に到達したことを確認する。

（移送・送信の規定外作業に関する申請及び承認手続き）

第７条　個人データの取扱者は、本規程に定める以外の方法で個人データを移送・送信する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

（個人データへのアクセス制御）

第８条　個人データ管理者は、移送・送信する個人データへのアクセスを制御するために、移送・送信する個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。

①　個人データの移送・送信に必要なＩＤ及びパスワードの管理を徹底する。

②　個人データが保存された機器・記録媒体等を保管するスペースへの部外者の立ち入りを制限する。

２　個人データ管理者は、センシティブ情報へのアクセス制御について、当該情報の移送・送信を認められた必要最小限の取扱者に限り移送・送信が行われるようＩＤ及びパスワードの管理を徹底しなければならない。

（移送・送信状況の記録及び分析）

第９条　個人データの取扱者は、個人データを移送・送信する場合、「個人情報管理台帳」に必要事項を記載しなければならない。

２　個人データ管理者は、必要に応じ、「個人情報管理台帳」に記載された内容を確認し、個人データの移送・送信が適正に行われているか否かを分析するものとする。

（センシティブ情報の移送・送信の制限）

第 10 条　個人データの取扱者は、センシティブ情報については、次に掲げる場合を除くほか、移送・送信を行わないこととする。

①　法令等に基づく場合

②　人の生命、身体又は財産の保護のために必要がある場合

③　公衆衛生の向上又は児童の健全な育成の推進のため特に必要がある場合

④　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

⑤　源泉徴収事務等の遂行上必要な範囲において、政治・宗教等の団体若しくは労働組合への所属若しくは加盟に関する従業員等のセンシティブ情報を利用する場合

⑥　相続手続による権利義務の移転等の遂行に必要な限りにおいて、機微(センシティブ)情報を利用する場合

（移送・送信に関する障害発生時の対応・復旧手続き）

第 11 条　個人データ管理者は、移送・送信した個人データについて、取扱者に対し定期的にバックアップを行うよう徹底するとともに、移送・送信した個人データに障害が発生した際にはバックアップデータにより復旧させなければならない。

２　個人データの取扱者は、作成したバックアップデータを適切に管理しなければならない。

（個人データの利用者の識別及び認証）

第 12 条　個人データ管理者は、個人データを処理する情報システムについて、個人データを移送・送信する取扱者の識別及び認証機能を設けなければならない。

（個人データの管理区分の設定及びアクセス制御）

第 13 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの移送・送信段階における管理区分の設定及びアクセス制御機能を設けなければならない。

（個人データへのアクセス権限の管理）

第 14 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの移送・送信段階におけるアクセス権限に関する機能を設けなければならない。

２　個人データ管理者は、前項のアクセス権限に関する機能の設定に当たっては、センシティブ情報の移送・送信の取扱者が必要最小限の者に限定されるよう設定しなければならない。

（個人データの漏えい・き損等防止策）

第 15 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの移送・送信段階における漏えい・き損等の防止策を講じなければならない。

（個人データへのアクセス記録及び分析）

第 16 条　個人データ管理者は、個人データを処理する情報システムについて、個人データの移送・送信段階におけるアクセス記録を取得し、必要な期間保管するとともに、必要に応じてこれを分析しなければならない。

個人情報取扱規程第２０条に定める
個人データの消去・廃棄段階に係る取扱規程

（目的）

第１条　本規程は、一般財団法人日本消防設備安全センター（以下「安全センター」という。）における個人データの安全管理措置のうち、個人データの「消去・廃棄」段階の取扱いについて定めたものである。

（定義）

第２条　「消去」とは、個人データが保存されている媒体の個人データを電子的な方法その他の方法により削除することなどをいう。

２　「廃棄」とは、個人データが保存されている媒体を物理的に廃棄することなどをいう。

（消去・廃棄に関する取扱者の役割・責任及び取扱者の限定）

第３条　個人データ管理責任者は、「個人情報管理役割分担表」により、個人データの消去・廃棄に関する取扱者の役割・責任を定め、組織内に周知しなければならない。

２　個人データ管理者は、業務上必要な者に限り個人データの消去・廃棄が行われるよう取扱者を限定しなければならない。

（センシティブ情報の消去・廃棄に関する取扱者の限定）

第４条　個人データ管理者は、個人データのうち、政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報（以下、「センシティブ情報」という。）の消去・廃棄の取扱者を必要最小限に限定して定めなければならない。

（消去・廃棄時の照合及び確認手続き）

第５条　個人データの取扱者は、個人データの消去・廃棄に際し、消去・廃棄しようとしている個人データについて、保存期間を照合又は消去・廃棄理由を確認のうえ、消去・廃棄しなければならない。

２　個人データの取扱者は、個人データを消去・廃棄する際には、当該データが保存されている機器・記録媒体等の性質に応じ適正な方法で消去・廃棄しなければならない。

（消去・廃棄の規定外作業に関する申請及び承認手続き）

第６条　個人データの取扱者は、本規程に定める以外の方法で個人データを消去・廃棄する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

（機器・記録媒体等の管理手続き）

第７条　個人データ管理者は、消去・廃棄する個人データが保存された機器・記録媒体等の設置場所の指定並びに管理区分及び権限の設定をし、必要に応じ変更しなければならない。

２　個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・記録媒体等を適切に保管しなければならない。

（個人データへのアクセス制御）

第８条　個人データ管理者は、消去・廃棄する個人データへのアクセスを制御するために、消去・廃棄する個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。

①　個人データの入力に必要なＩＤ及びパスワードの管理を徹底する。

②　個人データが保存された機器・記録媒体等を保管するスペースへの部外者の立ち入りを制限する。

（消去・廃棄状況の記録及び分析）

第９条　個人データの取扱者は、個人データを消去・廃棄する場合、「個人情報管理台帳」に必要事項を記載しなければならない。

２　個人データ管理者は、必要に応じ、「個人情報管理台帳」に記載された事項を確認し、個人データの消去・廃棄が適正に行われているか否かを分析するものとする。

個人情報取扱規程第２０条に定める
個人データの漏えい事案等への対応に係る取扱規程

（目的）

第１条　本規程は、一般財団法人日本消防設備安全センター(以下「安全センター」という。)における個人データの安全管理措置のうち、個人データの漏えい事案等への対応の段階における取り扱いについて定めたものである。

（定義）

第２条　「漏えい事案等」とは、安全センターが取り扱う個人データが外部に流出した事案又は滅失・毀損した事案（そのおそれのある事案を含む。）をいう。

（漏えい事案等への対応に関する対応部署の役割・責任及び取扱者の限定）

第３条　個人データ管理責任者は、「個人情報管理役割分担表」により、漏えい事案等への対応に関する対応部署（以下、「対応部署」という。）の役割・責任を定め、組織内に周知しなければならない。

２　対応部署の個人データ管理者は、各部署において、業務上必要な者に限り漏えい事案等への対応が行われるよう取扱者を限定しなければならない。

（漏えい事案等への対応の規定外作業に関する申請及び承認手続き）

第４条　個人データの取扱者は、本規程に定める以外の方法で漏えい事案等に対応する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

（漏えい事案等の影響等に関する調査手続き）

第５条　漏えい事案等が発生した部署の個人データ管理者は、個人データ管理責任者及び対応部署と連携のうえ、漏えいした個人データの量、質、事故の原因、態様、被害の程度等漏えい事案等の内容及び影響の調査を行うこととする。

（再発防止策・事後対策の検討に関する手続き）

第６条　漏えい事案等が発生した部署の個人データ管理者は対応部署と協議のうえ、再発防止策・事後対策を策定し、個人データ管理責任者へ報告することとする。

（報告に関する手続き）

第７条　漏えい事案等が発生した場合、発見者は、漏えい範囲の拡大防止等必要な措置をとるとともに、直ちにあらかじめ定められた方法により対応部署に報告しなければならない。

２　対応部署は、報告を受けた漏えい事案等について、別に定める報告方法により直ちに取引保険会社に報告しなければならない。

３　対応部署の個人データ管理者は取引保険会社の指示に従い、社外への報告等（監督当局等への報告、本人への通知、二次被害の防止・類似事案の発生回避の観点からの漏えい事案等の事実関係及び再発防止策の公表）の要否及びその方法について決定しなければならない。

（漏えい事案等への対応記録及び分析）

第８条　対応部署の個人データの取扱者は漏えい事案等への対応に関し、その記録をとるとともに、その記録を対応部署の個人データ管理者へ報告しなければならない。

２　対応部署の個人データ管理者は、報告を受けた記録について随時点検のうえ、分析を行い、漏えい事案等への対応が適切に行われていることを確認しなければならない。

個人データの点検・監査に係る取扱規程

（目的）

第１条　本規程は、一般財団法人日本消防設備安全センター（以下「安全センター」という。）における個人データの取扱状況に関する点検及び監査について定めたものである。

（実施部署）

第２条　個人データ管理責任者は、個人データを取り扱う部署において個人データの点検に関する点検責任者及び点検担当者を選任し、当該部署が自ら点検を実施するよう指示しなければならない。

２　個人データ管理責任者は、監査を実施する部署を指定し、その部署から個人データの監査に関する監査責任者及び監査担当者を選任し、監査を実施するよう指示しなければならない。

ただし、監査を実施する部署が個人データを取り扱うときには、個人データ管理責任者は、当該部署以外の部署から当該部署を監査する監査責任者及び監査担当者を選任しなければならない。

（点検）

第３条　個人データ管理責任者は、点検に関する計画を立案し、点検責任者に対し、定期的及び臨時の点検を実施するよう指示しなければならない。

２　点検担当者は、点検責任者の指示に基づいて確実に点検を実施しなければならない。

３　点検担当者は、点検により個人データの取り扱いに関する規定に違反する事項などを発見した場合には、点検責任者に報告しなければならない。

４　点検責任者は、規定に違反する事項について、個人データ管理責任者に報告するとともに個人データ管理責任者の指示を踏まえ、改善のための措置を講じなければならない。

（監査）

第４条　個人データ管理責任者は、監査に関する計画を立案し、監査責任者に対し、定期的及び臨時の監査を実施するよう指示しなければならない。

２　監査担当者は、監査責任者の指示に基づいて確実に点検を実施しなければならない。

３　監査担当者は、監査により個人データの取り扱いに関する規定に違反する事項などを発見した場合には、監査責任者に報告しなければならない。

４　監査責任者は、規定に違反する事項について、個人データ管理責任者に報告するとともに個人データ管理責任者の指示に従い、改善のための措置を講じなければならない。

個人データの外部委託に係る取扱規程

（目的）

第１条　本規程は、一般財団法人日本消防設備安全センター（以下「安全センター」という。）による個人データの取扱いの委託について、個人データを適正に取扱っていると認められる者を選定すること、及び委託先における個人データに対する安全管理措置が図られることを確保するため定めたものである。

（定義）

第２条　「委託」とは、契約の形態や種類を問わず、安全センターが他の者に個人データの取扱いの全部又は一部を行わせることを内容とする契約の一切を含む。

２　「委託先」とは、安全センターが、個人データの取扱いの全部又は一部を第三者に委託する場合の当該第三者のことをいう。

（委託に当たっての所属保険会社への報告）

第３条　個人データ管理責任者は、個人データの委託に当たって、情報管理責任者の承認を得なければならない。

（委託先選定の基準）

第４条　個人データ管理者は、委託先を選定するに当たって、「委託先選定チェックリスト」を別に定め、これに基づき委託先を選定するとともに、「委託先選定チェックリスト」を定期的に見直さなければならない。

２　個人データ管理者は、「委託先選定チェックリスト」の策定及び見直しに当たっては個人データ管理責任者の承認を得なければならない。

３　個人データ管理責任者は、承認した「委託先選定チェックリスト」を組織内に周知しなければならない。

（委託先における選定基準の遵守状況の確認）

第５条　個人データ管理者は、委託契約後に「委託先選定チェックリスト」に定められた事項の委託先における遵守状況を定期的又は随時に確認するとともに、委託先が当該基準を満たしていない場合には、委託先に対して改善を求めなければならない。

（委託契約）

第６条　個人データ管理責任者は、選定した委託先との間で、以下の安全管理事項を盛り込んだ委託契約書を締結しなければならない。

①　当社の委託先に対する監督及び監査報告徴収に関する権限
②　委託先における個人データの漏えい、盗用、改ざん及び目的外利用の禁止
③　再委託における条件
④　漏えい等が発生した際の委託先の責任

２　個人データ管理責任者は、前項各号の内容を盛り込んだ契約書を締結できない場合には委託は行わない。
３　個人データ管理責任者は、定期的に委託契約に盛り込む安全管理に関する事項を見直さなければならない。

（委託先における委託契約上の安全管理措置の遵守状況の確認）
第７条　個人データ管理者は、定期的又は随時に委託先における委託契約上の安全管理の遵守状況を確認するとともに、委託先が遵守していない場合には、委託先に対して改善を求めなければならない。

（8）各種参考資料

委託先の選定基準・考え方

１　一般財団法人日本消防設備安全センターの各情報管理者は、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。

２　各情報管理者は、個人情報の保護について十分な措置を講じている者を委託先として選定するものとする。

３　委託契約等について、主として次の項目を定めることとする。

①　委託先における個人データの取扱いに関すること（目的外使用の禁止）
②　委託先における秘密の保持に関すること
③　委託先における従業員の監督に関すること
④　委託先において漏えいが発生した場合等の委託先の対応及び責任に関すること
⑤　再委託を行う等については、あらかじめ了解を求めると共に、再委託先についても、前記の対応を求めること
⑥　その他個人情報保護のため必要な事項

４　その他

各情報管理者は、委託又は受託する場合には、情報管理責任者の承認を受けるものとする。