

**生命保険業における個人情報保護のため
の安全管理措置等についての実務指針
(生保安全管理実務指針)**

社団法人 生命保険協会

目 次

1．総則	1
2．基本方針・取扱規程等の整備	1
(1) 個人データの安全管理に係る基本方針の整備	1
(2) 個人データの安全管理に係る取扱規程の整備	1
(3) 個人データの取扱状況の点検及び監査に係る規程の整備	2
(4) 外部委託に係る規程の整備	2
3．実施体制の整備	2
3 - 1．組織的安全管理措置	2
(1) 個人データ管理責任者等の設置	2
(2) 就業規則等における安全管理措置の整備	3
(3) 個人データの安全管理に係る取扱規程に従った運用	4
(4) 個人データの取扱状況を確認できる手段の整備	4
(5) 個人データの取扱状況の点検及び監査体制の整備と実施	4
(6) 漏えい事案等に対する体制の整備	5
3 - 2．人的安全管理措置	5
(1) 従業者との個人データの非開示契約等の締結	5
(2) 従業者の役割・責任等の明確化	5
(3) 従業者への安全管理措置の周知徹底、教育及び訓練	5
(4) 従業者による個人データ管理手続きの遵守状況の確認	6
3 - 3．技術的安全管理措置	6
(1) 個人データの利用者の識別及び認証	6
(2) 個人データの管理区分の設定及びアクセス制御	6
(3) 個人データへのアクセス権限の管理	6
(4) 個人データの漏えい・き損等防止策	7
(5) 個人データへのアクセスの記録及び分析	7
(6) 個人データを取り扱う情報システムの稼働状況の記録及び分析	7
(7) 個人データを取り扱う情報システムの監視及び監査	7

4．従業員の監督	7
5．個人データの各管理段階における安全管理に係る取扱規程	7
5 - 1．各管理段階における安全管理に係る取扱規程の総則	8
(1) 組織的安全管理措置	8
(2) 技術的安全管理措置	8
(3) 機微（センシティブ）情報の取り扱い	8
5 - 2．取得・入力段階	9
(1) 組織的安全管理措置	9
(2) 機微（センシティブ）情報の取り扱い	9
(3) 生体認証情報の取り扱い	9
(4) 留意点	9
5 - 3．利用・加工段階	9
(1) 組織的安全管理措置	9
(2) 技術的安全管理措置	9
(3) 機微（センシティブ）情報の取り扱い	10
(4) 生体認証情報の取り扱い	10
(5) 留意点	10
5 - 4．保管・保存段階	11
(1) 組織的安全管理措置	11
(2) 技術的安全管理措置	11
(3) 機微（センシティブ）情報の取り扱い	11
(4) 生体認証情報の取り扱い	11
(5) 留意点	11
5 - 5．移送・送信段階	12
(1) 組織的安全管理措置	12
(2) 技術的安全管理措置	12
(3) 機微（センシティブ）情報の取り扱い	12
(4) 留意点	12
5 - 6．消去・廃棄段階	13
(1) 組織的安全管理措置	13

(2) 機微(センシティブ)情報の取り扱い	13
(3) 生体認証情報の取り扱い	13
(4) 留意点	13
5 - 7 . 漏えい事案等への対応の段階	14
(1) 漏えい事案等への対応の段階における取扱規程	14
(2) 自社内外への報告に関する手続き	14
6 . 委託先の監督	14
(1) 個人データ保護に関する委託先選定の基準	14
(2) 委託先選定の基準に定める事項の委託先における遵守状況の確認	15
(3) 委託契約において盛り込むべき安全管理に関する内容	15
(4) 安全管理措置の遵守状況の確認等	15
(5) 代理店に対する指導・監督	15

決裁年月日

適用年月日

制定 平成17年2月18日

平成17年4月 1日

生命保険業における個人情報保護のための安全管理措置等についての実務指針 (生保安全管理実務指針)

1. 総則

生命保険業における個人情報保護のための取扱指針(以下、「生保指針」という。)における 3 - 5 安全管理措置、3 - 6 従業員の監督、3 - 7 委託先の監督に基づき、「生命保険業における個人情報保護のための取扱指針の安全管理措置等についての実務指針」(以下、「実務指針」という。)を生保指針の別冊として定める。

本実務指針の内容は、生命保険会社等における個人データの安全管理に必要な適切な規程及び実施体制の整備等を定めるものである。生命保険会社等は、本実務指針に記載のある事項については、各社の規程等として整備しなければならないが、各事項に基づく具体的な対応については、各生命保険会社等が自主的に取組むことが求められる。

技術的安全管理措置の策定にあたっては、(財)金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準」を踏まえる必要がある。

なお、(例)に記載の事項については、あくまで具体的な対策の例示であって、当該内容そのものの実施を必須とするものではなく、また各社が自らの判断で他の適切な対策をとることを妨げるものではない。また、別段の定めがない限り、実務指針において用いられる用語は、生保指針で定義された意味を有する。

2. 基本方針・取扱規程等の整備

(1) 個人データの安全管理に係る基本方針の整備

生命保険会社等は、次に掲げる事項を定めた個人データの安全管理に係る基本方針を策定し、当該基本方針を公表するとともに、必要に応じて基本方針の見直しを行わなければならない。

- 生命保険会社等の名称
- 安全管理措置に関する質問及び苦情処理の窓口
- 個人データの安全管理に関する宣言
- 基本方針の継続的改善の宣言
- 関係法令等遵守の宣言

(2) 個人データの安全管理に係る取扱規程の整備

生命保険会社等は、個人データの各管理段階における安全管理に係る取扱規程を整備し、各管理段階ごとに5. 個人データの各管理段階における安全管理に係る取扱規程に規定する事項を定めるとともに、必要に応じて規程の見直しを行わなければならない。

なお、全ての管理段階を同一人が取り扱う小規模事業者等においては、各管理段階ごとに取扱規程を定めることに代えて、全管理段階を通じた安全管理に係る取扱規程において次に掲げる事項を定めることも認められる。

- 取扱者の役割・責任

取扱者の限定

各管理段階において個人データの安全管理上必要とされる手続き

また、生命保険会社等は、「個人データの各管理段階における安全管理に係る取扱規程」において、機微(センシティブ)情報の取り扱いについて規程を整備するとともに、情報通信技術の状況等を踏まえ、必要に応じて、当該規程の見直しを行うこととする。

(3) 個人データの取扱状況の点検及び監査に係る規程の整備

生命保険会社等は、個人データの取扱状況に関する点検及び監査の規程を整備し、次に掲げる事項を定めるとともに、必要に応じて規程の見直しを行わなければならない。

なお、個人データ取扱部署が単一である事業者においては、点検により監査を代替することも認められる。

点検及び監査の目的

点検及び監査の実施部署

点検責任者及び点検担当者の役割・責任

監査責任者及び監査担当者の役割・責任

点検及び監査に関する手続き

(4) 外部委託に係る規程の整備

生命保険会社等は、外部委託に係る取扱規程を整備し、次に掲げる事項を定めるとともに、定期的に規程の見直しを行わなければならない。

委託先の選定基準

委託契約に盛り込むべき安全管理に関する内容

3. 実施体制の整備

3-1. 組織的安全管理措置

(1) 個人データ管理責任者等の設置

生命保険会社等は、個人データの安全管理に係る業務遂行の総責任者である個人データ管理責任者及び個人データを取り扱う各部署における個人データ管理者を設置しなければならない。なお、個人データ取扱部署が単一である事業者においては、個人データ管理責任者が個人データ管理者を兼務することも認められる。個人データ管理責任者は、株式会社組織であれば取締役又は執行役等の業務執行に責任を有する者でなければならない。

生命保険会社等は、個人データ管理責任者に、次に掲げる業務を所管させなければならない。

個人データの安全管理に関する規程及び委託先の選定基準の承認及び周知

個人データ管理者及び3-3(1)に規定する「本人確認に関する情報」の管理者の任命
個人データ管理者からの報告徴収及び助言・指導
個人データの安全管理に関する教育・研修の企画
その他生命保険会社等全体における個人データの安全管理に関すること

生命保険会社等は、個人データ管理者に、次に掲げる業務を所管させなければならない。

個人データの取扱者の指定及び変更等の管理
個人データの利用申請の承認及び記録等の管理
個人データを取り扱う保管媒体の設置場所の指定及び変更等
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
個人データの取扱状況の把握
委託先における個人データの取扱状況等の監督
個人データの安全管理に関する教育・研修の実施
個人データ管理責任者に対する報告
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

上記に加えて、生命保険会社等は、個人情報保護全般の取りまとめを担当する部署及び個人情報を取り扱う部署を明確化することとする。

また、生命保険会社等は、個人情報保護を推進するための体制を整備し、明確化することとする。

(例)

- ・個人情報保護に係る関連部署を定め、個人情報保護推進のためそれぞれの役割を明確化する。(対外窓口、顧客対応の取りまとめ、従業員の教育、システムの安全対策、新契約・保全・支払等における個人情報保護対策等)
- ・社内全体で個人情報保護を推進できるように個人情報保護に係る関連部門長で構成する「個人情報保護推進委員会」等を設置する。

(2) 就業規則等における安全管理措置の整備

生命保険会社等は、就業規則等における安全管理措置の整備として、次に掲げる事項を就業規則等に定めるとともに、従業者との個人データの非開示契約等の締結を行わなければならない。

個人データの取り扱いに関する従業者の役割・責任
違反時の懲戒処分

(3) 個人データの安全管理に係る取扱規程に従った運用

生命保険会社等は、個人データの安全管理に係る取扱規程に従った体制を整備し、当該取扱規程に従った運用を行うとともに、取扱規程に規定する事項の遵守状況の記録及び確認を行わなければならない。

(4) 個人データの取扱状況を確認できる手段の整備

生命保険会社等は、個人データの取扱状況を確認できる手段の整備として、次に掲げる事項を含む台帳等を整備しなければならない。

取得項目

利用目的

保管場所・保管方法・保管期限

管理部署

アクセス制御の状況

(5) 個人データの取扱状況の点検及び監査体制の整備と実施

生命保険会社等は、個人データを取り扱う部署が自ら行う点検体制を整備し、点検を実施するとともに、当該部署以外の者による監査体制を整備し、監査を実施しなければならない。

なお、個人データ取扱部署が単一である事業者においては、点検により監査を代替することも認められる。

生命保険会社等は、個人データを取り扱う部署において点検責任者及び点検担当者を選任するとともに、点検計画を策定することにより点検体制を整備し、定期的及び臨時の点検を実施しなければならない。また、点検の実施後において、規程違反事項等を把握したときは、その改善を行わなければならない。

生命保険会社等は、監査の実施に当たっては、監査対象となる個人データを取り扱う部署以外から監査責任者・監査担当者を選任し、監査主体の独立性を確保するとともに、監査計画を策定することにより監査体制を整備し、定期的(生命保険会社等については原則として年一回以上)及び臨時の監査を実施しなければならない。また、監査の実施後において、規程違反事項等を把握したときは、その改善を行わなければならない。

なお、監査部署が監査業務等により個人データを取り扱う場合には、当該部署における個人データの取り扱いについて、個人データ管理責任者が特に任命する者がその監査を実施しなければならない。

また、生命保険会社等は、機微(センシティブ)情報に該当する生体認証情報(機械による自動認証に用いられる身体的特徴のうち、非公知の情報。以下同じ。)の取り扱いに関し、外部監査を行うとともに、必要に応じて、その他の機微(センシティブ)情報の取り扱いについても外部監査を行うこととする。

(6) 漏えい事案等に対応する体制の整備

生命保険会社等は、漏えい事案等に対応する体制の整備として、次に掲げる体制を整備しなければならない。

対応部署

漏えい事案等の影響・原因等に関する調査体制

再発防止策・事後対策の検討体制

自社内外への報告体制

生命保険会社等は、自社内外への報告体制を整備するとともに、漏えい事案等が発生した場合には、次に掲げる事項を実施しなければならない。

監督当局等への報告

本人への通知等

二次被害の防止・類似事案の発生回避等の観点からの漏えい事案等の事実関係及び再発防止策等の早急な公表

3 - 2 . 人的安全管理措置

(1) 従業者との個人データの非開示契約等の締結

生命保険会社等は、採用時等に従業者と個人データの非開示契約等を締結するとともに、非開示契約等に違反した場合の懲戒処分を定めた就業規則等を整備しなければならない。

(2) 従業者の役割・責任等の明確化

生命保険会社等は、従業者の役割・責任等を明確化として、次に掲げる措置を講じなければならない。

各管理段階における個人データの取り扱いに関する従業者の役割・責任の明確化

個人データの管理区分及びアクセス権限の設定

違反時の懲戒処分を定めた就業規則等の整備

必要に応じた規程等の見直し

(3) 従業者への安全管理措置の周知徹底、教育及び訓練

生命保険会社等は、従業者への安全管理措置の周知徹底、教育及び訓練として、次に掲げる措置を講じなければならない。

従業者に対する採用時の教育及び定期的な教育・訓練

(例)

- ・ 層別研修、業務担当者研修等、教育カリキュラムの中に個人情報保護の内容を盛り込む。
- ・ 社内報への個人情報保護の重要性に関する記事掲載等により社内 P R を促進する。
- ・ 個人情報保護についての強化月間等を設け、研修等を実施する。

個人データ管理責任者及び個人データ管理者に対する教育・訓練
個人データの安全管理に係る就業規則等に違反した場合の懲戒処分の周知
ここにいう「周知」とは、従業員に対する教育、訓練の中で徹底させることをいう。
従業員に対する教育・訓練の評価及び定期的な見直し

(4) 従業員による個人データ管理手続きの遵守状況の確認

生命保険会社等は、従業員による個人データ管理手続きの遵守状況の確認として、個人データの安全管理に係る取扱規程に定めた事項の遵守状況について、3-1(3)に基づく記録及び確認を行うとともに、3-1(5)に基づき点検及び監査を実施しなければならない。

3-3. 技術的安全管理措置

(1) 個人データの利用者の識別及び認証

生命保険会社等は、個人データの利用者の識別及び認証として、次に掲げる措置を講じなければならない。

本人確認機能の整備

本人確認に関する情報の不正使用防止機能の整備

本人確認に関する情報が他人に知られないための対策

(2) 個人データの管理区分の設定及びアクセス制御

生命保険会社等は、個人データの管理区分の設定及びアクセス制御として、次に掲げる措置を講じなければならない。

従業員の役割・責任に応じた管理区分及びアクセス権限の設定

事業者内部における権限外者に対するアクセス制御

外部からの不正アクセスの防止措置

このうち、「外部からの不正アクセスの防止措置」として、次に掲げる措置を講じなければならない。

アクセス可能な通信経路の限定

外部ネットワークからの不正侵入防止機能の整備

不正アクセスの監視機能の整備

ネットワークによるアクセス制御機能の整備

(3) 個人データへのアクセス権限の管理

生命保険会社等は、個人データへのアクセス権限の管理として、次に掲げる措置を講じなければならない。

従業員に対する個人データへのアクセス権限の適切な付与及び見直し

個人データへのアクセス権限を付与する従業員数を必要最小限に限定すること

従業者に付与するアクセス権限を必要最小限に限定すること

(4) 個人データの漏えい・き損等防止策

生命保険会社等は、個人データの漏えい・き損等防止策として、個人データの保護策を講ずることとともに、障害発生時の技術的対応・復旧手続を整備しなければならない。

生命保険会社等は、「個人データの保護策を講ずること」として、次に掲げる措置を講じなければならない。

蓄積データの漏えい防止策

伝送データの漏えい防止策

コンピュータウイルス等不正プログラムへの防御対策

生命保険会社等は、「障害発生時の技術的対応・復旧手続の整備」として、次に掲げる措置を講じなければならない。

不正アクセスの発生に備えた対応・復旧手続の整備

コンピュータウイルス等不正プログラムによる被害時の対策

リカバリ機能の整備

(5) 個人データへのアクセスの記録及び分析

生命保険会社等は、個人データへのアクセスを記録するとともに、当該記録の分析・保存を行わなければならない。

(6) 個人データを取り扱う情報システムの稼動状況の記録及び分析

生命保険会社等は、個人データを取り扱う情報システムの稼動状況を記録するとともに、当該記録の分析・保存を行わなければならない。

(7) 個人データを取り扱う情報システムの監視及び監査

生命保険会社等は、個人データを取り扱う情報システムの利用状況及び個人データへのアクセス状況を3-3(5)及び3-3(6)により監視するとともに、監視状況についての点検及び監査を行わなければならない。

4. 従業者の監督

生命保険会社等は、3-2に規定する措置を講ずることにより、従業者に対し必要かつ適切な監督を行わなければならない。

5. 個人データの各管理段階における安全管理に係る取扱規程

生命保険会社等は、2(2)に基づき、各管理段階ごとの安全管理に係る取扱規程において、次に掲げる事項を定めなければならない。

なお、各管理段階とは、取得・入力段階、利用・加工段階、保管・保存段階、移送・送信段階、消去・廃棄段階をいう。

5 - 1 . 各管理段階における安全管理に係る取扱規程の総則

(1) 組織的安全管理措置

各管理段階における取扱規程において、組織的安全管理措置として次に掲げる事項のうち5 - 2 以降で指定する事項を定めなければならない。

- 取扱者の役割・責任
- 取扱者の限定
- 対象となる個人データの限定
- 照合及び確認手続き
- 規格外作業に関する申請及び承認手続き
- 機器・記録媒体等の管理手続き
- 個人データへのアクセス制御
- 状況の記録及び分析
- 障害発生時の対応・復旧手続

(2) 技術的安全管理措置

利用・加工段階、保管・保存段階、移送・送信段階においては、技術的安全管理措置として次に掲げる事項のうち5 - 2 以降で指定する事項を定めなければならない。

- 個人データの利用者の識別及び認証
- 個人データの管理区分の設定及びアクセス制御
- 個人データへのアクセス権限の管理
- 個人データの漏えい・き損等防止策
- 個人データへのアクセス記録及び分析
- 個人データを取り扱う情報システムの稼動状況の記録及び分析

(3) 機微（センシティブ）情報の取り扱い

各管理段階における機微（センシティブ）情報の取り扱いについては、上記に規定する事項に加えて、次に掲げる事項のうち5 - 2 以降で指定する事項を定めることとする。

- 生保指針 3 - 2 に定める場合又は目的のみによる取り扱い
- 取扱者の必要最小限の限定
- 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
- ここにいう「説明」とは、たとえば生命保険契約の申込に際しては、生保指針 3 - 2 に規定する保険業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲で機微（センシティブ）情報を取得、利用又は第三者提供することについて説明することをいう。
- 必要最小限の者に限定したアクセス権限の設定及びアクセス制御の実施

5 - 2 . 取得・入力段階

(1) 組織的安全管理措置

取得・入力段階における取扱規程において、5 - 1 (1) ~ に規定する事項を定めなければならない。

(2) 機微 (センシティブ) 情報の取り扱い

機微 (センシティブ) 情報の取り扱いについては、上記に規定する事項に加えて、5 - 1 (3) ~ に規定する事項を定めることとする。

(3) 生体認証情報の取り扱い

機微 (センシティブ) 情報に該当する生体認証情報の取り扱いについては、上記 (1) および (2) に規定する事項に加えて、次に掲げる事項を定めなければならない。

なりすましによる登録の防止策

本人確認に必要な最小限の生体認証情報のみの取得

生体認証情報の取得後、基となった生体情報の速やかな消去

(4) 留意点

取得・入力段階における取扱規程を定めるにあたっては、次に掲げる点に留意する必要がある。

生命保険会社等は、個人データの取得・入力にあたっては、業務遂行上必要な範囲で行うこととする。

5 - 3 . 利用・加工段階

(1) 組織的安全管理措置

利用・加工段階における取扱規程に関する組織的安全管理措置は、5 - 1 (1) ~ に規定する事項に加え、個人データの管理区域外への持ち出しに関する上乘せ措置として、次に掲げる事項を含まなければならない。

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

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必要最小限の限定

個人データの管理区域外への持ち出しの対象となる個人データの必要最小限の限定

個人データの管理区域外への持ち出し時の照合及び確認手続き

個人データの管理区域外への持ち出しに関する申請及び承認手続き

機器・記録媒体等の管理手続き

個人データの管理区域外への持ち出し状況の記録及び分析

(2) 技術的安全管理措置

利用・加工段階における取扱規程に関する技術的安全管理措置は、5 - 1 (2) ~

に規定する事項を含まなければならない。

(3) 機微(センシティブ)情報の取り扱い

機微(センシティブ)情報の取り扱いについては、上記(1)および(2)に規定する事項に加えて5-1(3) ~ に規定する事項を定めることとする。

(4) 生体認証情報の取り扱い

機微(センシティブ)情報に該当する生体認証情報の取り扱いは、上記(1)~(3)に規定する事項に加えて、次に掲げる事項を含まなければならない。

偽造された生体認証情報による不正認証の防止措置

登録された生体認証情報の不正利用の防止措置

残存する生体認証情報の消去

認証精度設定等の適切性の確認

生体認証による本人確認の代替措置における厳格な本人確認手続き

(5) 留意点

利用・加工段階における取扱規程を定めるにあたっては、次に掲げる点に留意する必要がある。

生命保険会社等は、個人データの利用・加工にあたっては、業務遂行上必要な範囲で行うこととする。

このうち、技術的安全管理措置として、3-3(3) に規定する「個人データへのアクセス権限を付与する従業者数を必要最小限に限定すること」及び3-3(3) に規定する「従業者に付与するアクセス権限を必要最小限に限定すること」についての措置を講じなければならない。

生命保険会社等は、個人データの利用目的、重要性に応じて5-1(1) に規定する「個人データへのアクセス制御」を行わなければならない。

(例)

・保険契約申込時あるいは支払時等に審査を行うために必要となる医療・健康情報等、特に厳重な管理を要する個人データについては、特定場所の専用システム・端末の利用に限定する等、特段の措置を講じる。

生命保険会社等は、個人データの利用目的、重要性に応じて情報システム等の使用機能を限定することとする。

(例)

・ホストコンピューターに接続し個人保険の大量・詳細な契約内容を閲覧することが可能な業務端末についてはフロッピーディスク等の媒体への出力制限をする等、利用形態に応じた適切な措置を講じる。

生命保険会社等は、5-1(1) に規定する「機器・記録媒体等の管理手続き」の中に社外持ち出し可能な個人データが印字された帳票、個人データが記録された

媒体を明確化するとともに、社外に持ち出す場合の取り扱いを明確化しなければならない。

(例)

- ・個人データを社外に持ち出す場合には、業務遂行上必要不可欠なものに限る。
- ・個人データの社外への持ち出しを、システム履歴の管理等により、適正に管理できる体制を整備する。
- ・個人データを社外に持ち出したときには常時携行等の指導を徹底する。また、盗難防止のため、特に車内への放置は厳禁とし、電車等の網棚を使用しない等の指導を徹底する。

営業活動に利用する携帯端末については、本人認証、登載する個人データの暗号化等、5 - 1 (2) に規定する「個人データの漏えい・き損等防止策」を講じなければならない。

(例)

- ・専用鍵、パスワード等による本人認証を実施する。
- ・一定期間使用されない場合は、自動的にロックされる等の対策を講じる。
- ・登載情報を暗号化し、第三者がハードディスクを取り出し個人データを読み取ることを困難にする。

5 - 4 . 保管・保存段階

(1) 組織的安全管理措置

保管・保存段階における取扱規程に関する組織的安全管理措置は、5 - 1 (1) ~ 及び ~ に規定する事項を含まなければならない。

(2) 技術的安全管理措置

保管・保存段階における取扱規程に関する技術的安全管理措置は、5 - 1 (2) ~ に規定する事項を含まなければならない。

(3) 機微(センシティブ)情報の取り扱い

機微(センシティブ)情報の取り扱いについては、上記(1) 及び(2) に規定する事項に加えて、5 - 1 (3) 及び に規定する事項を定めることとする。

(4) 生体認証情報の取り扱い

機微(センシティブ)情報に該当する生体認証情報の取り扱いは、上記(1) ~ (3) に規定する事項に加えて、保存時における生体認証情報の暗号化を含まなければならないほか、サーバー等における氏名等の個人情報との分別管理を含むこととする。

(5) 留意点

生命保険会社等は、保管・保存段階における取扱規程を定めるにあたっては、次に掲

げる点に留意する必要がある。

生命保険会社等は、5 - 1 (1) に規定する「機器・記録媒体等の管理手続き」の中に、個人データが印字された帳票、個人データが記録された媒体の保管・保存について、重要度を考慮した措置を定めなければならない。

(例)

- ・個人データを集中管理するコンピュータセンター等については、物の持ち出しを防止するための措置等を講じる。

生命保険会社等は、個人データが印字された帳票、個人データが記録された媒体の保管・保存について、重要度を考慮した、5 - 1 (1) に規定する「個人データへのアクセス制御」を行わなければならない。

(例)

- ・個人データを取り扱う建物、室内については、入退館(室)管理や施錠管理を徹底する。
- ・個人データを集中管理するコンピュータセンター等については、ゾーンごとの入退室管理(とりわけコンピュータ機械室、総合監視センターについては一層厳格な入室チェックの実施)を行う。

5 - 5 . 移送・送信段階

(1) 組織的安全管理措置

移送・送信段階における取扱規程に関する組織的安全管理措置は、5 - 1 (1) ~ 及び ~ に規定する事項を含まなければならない。

このうちの「移送・送信時の照合及び確認手続き」には宛先の照合及び確認手続きが含まれる。

(2) 技術的安全管理措置

移送・送信段階における取扱規程に関する技術的安全管理措置は、5 - 1 (2) ~ に規定する事項を含まなければならない。

(3) 機微(センシティブ)情報の取り扱い

機微(センシティブ)情報の取り扱いについては、上記(1)および(2)に規定する事項に加えて、5 - 1 (3) 及び に規定する事項を定めることとする。

(4) 留意点

生命保険会社等は、移送・送信段階における取扱規程を定めるにあたっては、次に掲げる点に留意する必要がある。

生命保険会社等は、個人データの重要度、媒体の性質に応じて移送・送信方法を定めることとする。

(例)

- ・個人データが印字された帳票、個人データが記録された媒体の送付方法については、郵便（配達記録等を含む。）指定運送業者による配送、責任者への直接授受等、個人データの重要度に応じた措置を講じる。
 - ・個人データが印字された帳票をファクシミリ送信する場合は、予め登録した短縮コードを使用する等、誤送信防止のための措置を講じる。
 - ・複数の顧客へメールで送信する場合については宛先に複数のアドレスを設定しないあるいはBCCで送信する等、メールアドレスが第三者の目に触れることを防止する措置を講じる。（但し、複数の顧客へメールで送信する場合であって、メールアドレスで個人を識別できる場合については、BCCで送信しなければならない。）
- 生命保険会社等は、個人データの移送・送信を行う場合には、データの重要性、送付方法に応じた、媒体に対する、5 - 1（2）に規定する「個人データの漏えい・き損等防止策」を講じなければならない。

(例)

- ・個人データをメール等により社外へ送信する場合は個人データの暗号化、データファイルへのパスワード設定等を行う。
- ・個人データが記録された媒体（フロッピーディスク、テープ等）の社外への移送については、個人データの暗号化、個人データファイルへのパスワード設定等の措置を講じる。また、必要に応じて施錠可能なジュラルミンケースの使用を行う。

5 - 6 . 消去・廃棄段階

(1) 組織的安全管理措置

消去・破棄段階における取扱規程において、5 - 1（1）、及び～に規定する事項を定めなければならない。

(2) 機微（センシティブ）情報の取り扱い

機微（センシティブ）情報の取り扱いについては、上記（1）に規定する事項に加えて、5 - 1（3）に規定する事項について定めることとする。

(3) 生体認証情報の取り扱い

機微（センシティブ）情報に該当する生体認証情報の取り扱いについては、上記に規定する事項に加えて、生体認証情報等を本人確認に用いる必要性がなくなった場合には、速やかに保有する生体認証情報を消去することを含まなければならない。

(4) 留意点

生命保険会社等は、消去・廃棄段階における取扱規程を定めるにあたっては、次に掲げる点に留意する必要がある。

生命保険会社等は、個人データが印字された帳票、個人データが記録された媒体の廃

棄について、媒体の性質等を考慮し、裁断、焼却、溶解（以下、「物理的な破壊」という。）消去等の方法によって行うこととする。

（例）

- ・個人データが印字された帳票は、シュレッダーによって裁断する等物理的な破壊を行う。
 - ・個人データが記録された媒体は、物理的な破壊を行うもしくは意味のないデータを媒体に上書きすることによって完全に消去する。
- 生命保険会社等は、個人データが印字された帳票、個人データが記録された媒体の廃棄について、保存期間、利用期間終了後速やかに行うこととする。

5 - 7 . 漏えい事案等への対応の段階

（1）漏えい事案等への対応の段階における取扱規程

漏えい事案等への対応の段階における取扱規程において、次に掲げる事項を定めなければならない。

対応部署の役割・責任

漏えい事案等への対応に関する取扱者の限定

漏えい事案等への対応の規格外作業に関する申請及び承認手続き

漏えい事案等の影響・原因等に関する調査手続き

再発防止策・事後対策の検討に関する手続き

自社内外への報告に関する手続き

漏えい事案等への対応状況の記録及び分析

（2）自社内外への報告に関する手続き

自社内外への報告に関する手続きは、次に掲げる事項を含まなければならない。

監督当局等への報告

本人への通知等

二次被害の防止・類似事案の発生回避等の観点からの漏えい事案等の事実関係及び再発防止策等の早急な公表

6 . 委託先の監督

（1）個人データ保護に関する委託先選定の基準

生命保険会社等は、個人データの取り扱いを委託する場合には、次に掲げる事項を委託先選定の基準として定め、当該基準に従って委任先を選定するとともに、当該基準を定期的に見直さなければならない。

委託先における個人データの安全管理に係る基本方針・取扱規程等の整備

委託先における個人データの安全管理に係る実施体制の整備

実績等に基づく委託先の個人データ安全管理上の信用度

なお、過去に漏えい事案等の発生があった委託先であっても、事後に適切な措置がな

されていれば、それらを一律に排除するものではない。

委託先の経営の健全性

なお、財務状況が悪化している企業を一律に排除するものではない。

委託先選定の基準においては、「委託先における個人データの安全管理に係る基本方針・取扱規程等の整備」として、次に掲げる事項を定めなければならない。

委託先における個人データの安全管理に係る基本方針の整備

委託先における個人データの安全管理に係る取扱規程の整備

委託先における個人データの取扱状況の点検及び監査に係る規程の整備

委託先における外部委託に係る規程の整備

委託先選定の基準においては、「委託先における個人データの安全管理に係る実施体制の整備」として、3 - 1の組織的安全管理措置、3 - 2の人的安全管理措置及び3 - 3の技術的安全管理措置に記載された事項を定めるとともに、委託先から再委託する場合の再委託先の個人データの安全管理に係る実施体制の整備状況に係る基準を定めなければならない。

(2) 委託先選定の基準に定める事項の委託先における遵守状況の確認

生命保険会社等は、6(3)に基づき、委託契約後に委託先選定の基準に定める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、委託先が当該基準を満たすよう監督しなければならない。

(3) 委託契約において盛り込むべき安全管理に関する内容

生命保険会社等は、委託契約において、次に掲げる安全管理に関する事項を盛り込まなければならない。

委託者の監督・監査・報告徴収に関する権限

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

再委託における条件

漏えい事案等が発生した際の委託先の責任

(4) 安全管理措置の遵守状況の確認等

生命保険会社等は、6(3)に基づき、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措置の遵守状況を確認するとともに、当該契約内容が遵守されていない場合には、委託先が当該契約内容を遵守するよう監督しなければならない。また、生命保険会社等は、定期的に委託契約に盛り込む安全管理措置を見直さなければならない。

(5) 代理店に対する指導・監督

生命保険会社等は、保険募集の委託を行っている代理店に対して、個人データの取り

扱いの委託先として、生保指針に加えて本実務指針に準じた取り扱いがなされるよう必要かつ適切な指導・監督を行わなければならない。

以 上