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）

一般社団法人　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 …… 2
(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
(5) 削除情報等に係る取扱規程の整備 …… 2
(6) 加工方法等情報に係る取扱規程の整備 …… 3
３．実施体制の整備 …… 3
３－１．組織的安全管理措置 …… 3
(1)　個人データ管理責任者等の設置 …… 3
(2)　就業規則等における安全管理措置の整備 …… 4
(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)　漏えい等事案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 …… 6
(3)　従業者への安全管理措置の周知徹底、教育及び訓練 …… 6
(4)　従業者による個人データ管理手続の遵守状況の確認 …… 6
３－３．物理的安全管理措置 …… 6
(1)　個人データの取扱区域等の管理 …… 6
(2)　機器及び電子媒体等の盗難等の防止 …… 7
(3)　電子媒体等を持ち運ぶ場合の漏えい等の防止 …… 7
(4)　個人データの削除及び機器、電子媒体等の廃棄 …… 7
３－４．技術的安全管理措置 …… 7
(1)　個人データの利用者の識別及び認証 …… 7

(2)　個人データの管理区分の設定及びアクセス制御 ……7
(3)　個人データへのアクセス権限の管理 ……8
(4)　個人データの漏えい等防止策 ……8
(5)　個人データへのアクセスの記録及び分析 ……8
(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 ……8
(7)　個人データを取り扱う情報システムの監視及び監査 ……8
４．従業者の監督 ……9
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 ……9
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 ……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）情報の取扱い ……１０
５－２．取得・入力段階 ……１０
(1)　組織的安全管理措置 ……１０
(2)　機微（センシティブ）情報の取扱い ……１０
(3)　生体認証情報の取扱い ……１０
(4)　留意点 ……１１
５－３．利用・加工段階 ……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）情報の取扱い ……１１
(4)　生体認証情報の取扱い ……１２
(5)　留意点 ……１２
５－４．保管・保存段階 ……１３
(1)　組織的安全管理措置 ……１３
(2)　技術的安全管理措置 ……１３
(3)　機微（センシティブ）情報の取扱い ……１３
(4)　生体認証情報の取扱い ……１３
(5)　留意点 ……１３
５－５．移送・送信段階 ……１４

(1)　組織的安全管理措置 ……１４
(2)　技術的安全管理措置 ……１４
(3)　機微（センシティブ）情報の取扱い ……１４
(4)　留意点 ……１４
５－６．消去・廃棄段階 ……１５
(1)　組織的安全管理措置 ……１５
(2)　機微（センシティブ）情報の取扱い ……１５
(3)　生体認証情報の取扱い ……１５
(4)　留意点 ……１５
５－７．漏えい等事案への対応の段階 ……１６
(1)　漏えい等事案への対応の段階における取扱規程 ……１６
(2)　自社内外への報告に関する手続 ……１６
６．委託先の監督 ……１６
(1)　個人データ保護に関する委託先選定の基準 ……１６
(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 …１７
(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 ……１７
(4)　安全管理措置の遵守状況の確認等 ……１７
(5)　代理店に対する指導・監督 ……１８
７．仮名加工情報等の安全管理措置 ……１８
７－１．削除情報等の安全管理措置等 ……１８
８．匿名加工情報等の安全管理措置 ……１８
８－１．加工方法等情報の安全管理措置 ……１９
８－２．匿名加工情報の安全管理措置等 ……１９

	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
改正	平成２６年　２月２１日	平成２６年　４月　１日
改正	平成２７年　６月１２日	平成２７年　７月　９日
改正	平成２７年１１月２０日	平成２７年１１月２０日
改正	平成２９年　４月２１日	平成２９年　５月３０日
改正	平成３０年　３月１６日	平成３０年　４月　１日
改正	令和　４年　３月３０日	令和　４年　４月　１日
改正	令和　６年　３月１５日	令和　６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Ⅱ．３－５．安全管理措置、３－６．従業者の監督、３－７．委託先の監督、３－１１．仮名加工情報取扱事業者等の義務、３－１２．匿名加工情報取扱事業者等の義務に基づき、「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（当該生命保険会社等が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。以下同じ）、仮名加工情報及び匿名加工情報等の安全管理に必要かつ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、（公財）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。

個人番号については、本実務指針における「個人データ」に含むものとする。生命保険会社等は「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」及び「金融業務における特定個人情報の適正な取扱いに関するガイドライン」において定める安全管理措置等を遵守するとともに、本実務指針に従うものとする。

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。

①生命保険会社等の名称

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。

①取扱者の役割・責任

②取扱者の限定

③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

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。

①点検及び監査の目的

②点検及び監査の実施部署

③点検責任者及び点検担当者の役割・責任

④監査責任者及び監査担当者の役割・責任

⑤点検及び監査に関する手続

（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。

①委託先の選定基準

②委託契約に盛り込むべき安全管理に関する内容

（５）削除情報等に係る取扱規程の整備

生命保険会社等は、仮名加工情報を作成したときは、削除情報等の取扱いに関する規程類を整備し、当該規程類に従って削除情報等を適切に取り扱うとともに、その取扱いの状況について評価を行い、その結果に基づき改善を図るために必要な措置を講じなけ

ればならない。

（６）加工方法等情報に係る取扱規程の整備

生命保険会社等は、匿名加工情報を作成したときは、加工方法等情報の取扱いに関する規程類を整備し、当該規程類に従って加工方法等情報を適切に取り扱うとともに、その取扱いの状況について評価を行い、その結果に基づき改善を図るために必要な措置を講じなければならない。

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。

なお、生命保険会社等は、「個人データの管理責任者等の設置」として、個人データの取扱いの点検・改善等の監督を行う部署又は合議制の委員会を設置することが望ましい。

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。

①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
②個人データ管理者及び３－４（１）に規定する「本人確認に関する情報」の管理者の任命
③個人データ管理者からの報告徴収及び助言・指導
④個人データの安全管理に関する教育・研修の企画
⑤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。

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個人データを取り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個人データ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

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、従業者の教育、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。

①個人データの取扱いに関する従業者の役割・責任
②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。

①取得項目
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

（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）情報の取扱いについても外部監査を行うこととする。

なお、生命保険会社等は、新たなリスクに対応するための、安全管理措置の評価、見直し及び改善に向けて、個人情報保護対策及び最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者による、社内の対応の確認（必要に応じ、外部の知見を有する者を活用し確認させることを含む）等を実施することが望ましい。

（６）漏えい等事案に対応する体制の整備

生命保険会社等は、漏えい等事案（漏えい等又はそのおそれのある事案をいう。以下同じ。）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。

①対応部署

②漏えい等事案の影響・原因等に関する調査体制

③再発防止策・事後対策の検討体制

④自社内外への報告体制

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。

①各管理段階における個人データの取扱いに関する従業者の役割・責任の明確化

②個人データの管理区分及びアクセス権限の設定

③違反時の懲戒処分を定めた就業規則等の整備

④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。

①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ＰＲ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。

②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

③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、従業者に対する教育、訓練の中で徹底させることをいう。

④従業者に対する教育・訓練の評価及び定期的な見直し

（４）従業者による個人データ管理手続の遵守状況の確認

生命保険会社等は、従業者による個人データ管理手続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．物理的安全管理措置

（１）個人データの取扱区域等の管理

生命保険会社等は、個人データの取扱区域等の管理として、次に掲げる措置を講じなければならない。

①個人データ等を取り扱う重要な情報システムの管理区域への入退室管理等
②管理区域への持ち込み可能機器等の制限等
③のぞき込み防止措置の実施等による権限を有しない者による閲覧等の防止

（２）機器及び電子媒体等の盗難等の防止
生命保険会社等は、機器及び電子媒体等の盗難等の防止として、次に掲げる措置を講じなければならない。
①個人データを取り扱う機器等の施錠等による保管
②個人データを取り扱う情報システムを運用する機器の固定等

（３）電子媒体等を持ち運ぶ場合の漏えい等の防止
生命保険会社等は、電子媒体等を持ち運ぶ場合の漏えい等の防止として、次に掲げる措置を講じなければならない。
①持ち運ぶデータの暗号化、パスワードによる保護等
②書類の封緘、目隠しシールの貼付等

（４）個人データの削除及び機器、電子媒体等の廃棄
生命保険会社等は、個人データの削除及び機器、電子媒体等の廃棄として、次に掲げる措置を講じなければならない。
①容易に復元できない手段によるデータ削除
②個人データが記載された書類等又は記録された機器等の物理的な破壊等

３－４．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。
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

（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。
①従業者の役割・責任に応じた管理区分及びアクセス権限の設定
②事業者内部における権限外者に対するアクセス制御
③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。

①アクセス可能な通信経路の限定
②外部ネットワークからの不正侵入防止機能の整備
③不正アクセスの監視機能の整備
④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。

①従業者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
②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
③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等防止策

生命保険会社等は、個人データの漏えい等防止策として、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。

①蓄積データの漏えい等防止策
②伝送データの漏えい等防止策
③コンピュータウィ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。

①不正アクセスの発生に備えた対応・復旧手続の整備
②コンピュータウィルス等不正プログラムによる被害時の対策
③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や操作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。また、不正が疑われる異常な記録の存否を定期的に確認しなければならない。

（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、個人データへのアクセス状況及び情報システムへの外部からのアクセス状況を３－４（５）及び３－４（６）により監視するとともに、監視システムの動作の定期的な確認等、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。また、セキュリティパッチの適用や情報システム固有の脆弱性の発見・その修正等、ソフトウェアに関する脆弱性対策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。

①取扱者の役割・責任
②取扱者の限定
③対象となる個人データの限定
④照合及び確認手続
⑤規程外作業に関する申請及び承認手続
⑥機器・記録媒体等の管理手続
⑦個人データへのアクセス制御
⑧状況の記録及び分析
⑨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。

①個人データの利用者の識別及び認証
②個人データの管理区分の設定及びアクセス制御
③個人データへのアクセス権限の管理
④個人データの漏えい等防止策

⑤個人データへのアクセス記録及び分析

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

（３）機微（センシティブ）情報の取扱い

各管理段階における機微（センシティブ）情報の取扱いについては、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。

①生保指針Ⅱ３－２に定める場合又は目的のみによる取り扱い

②取扱者の必要最小限の限定

③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Ⅱ３－２⑦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。

④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）①～⑧に規定する事項を定めなければならない。

なお、生命保険会社等は、取得・入力段階における取扱規程について、「個人データへのアクセス制御」として、次に掲げる事項を定めることが望ましい。

①入館（室）者による不正行為の防止のための、業務実施場所及び情報システム等の設置場所の入退館（室）管理の実施

（例）

・入退館（室）の記録の保存

②盗難等の防止のための措置

（例）

・カメラによる撮影や作業への立会い等による記録又はモニタリングの実施

・記録機能を持つ媒体の持込み・持出し禁止又は検査の実施

③不正な操作を防ぐための、個人データを取り扱う端末に付与する機能の、業務上の必要性に基づく限定

（例）

・スマートフォン、パソコン等の記録機能を有する機器の接続の制限及び機器の更新への対応

（２）機微（センシティブ）情報の取扱い

機微（センシティブ）情報の取扱いについては、上記に規定する事項に加えて、５－１（３）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。

①なりすましによる登録の防止策

②本人確認に必要な最小限の生体認証情報のみの取得

③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。

①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）①～⑧に規定する事項を含まなければならない。

なお、生命保険会社等は、利用・加工段階における取扱規程について、「個人データへのアクセス制御」として、５－２（１）①～③に規定する事項を定めることが望ましい。

また、個人データの管理区域外への持出しに関する上乗せ措置として、次に掲げる事項を含まなければならない。

①個人データの管理区域外への持出しに関する取扱者の役割・責任

②個人データの管理区域外への持出しに関する取扱者の必要最小限の限定

③個人データの管理区域外への持出しの対象となる個人データの必要最小限の限定

④個人データの管理区域外への持出し時の照合及び確認手続

⑤個人データの管理区域外への持出しに関する申請及び承認手続

⑥機器・記録媒体等の管理手続

⑦個人データの管理区域外への持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）①～⑥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）情報の取扱い

機微（センシティブ）情報の取扱いについては、上記（１）および（２）に規定する

事項に加えて５－１（３）①～④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。

①偽造された生体認証情報による不正認証の防止措置

②登録された生体認証情報の不正利用の防止措置

③残存する生体認証情報の消去

④認証精度設定等の適切性の確認

⑤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

（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。

①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、３－４（３）②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３－４（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。

②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）⑦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。

③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。

④生命保険会社等は、５－１（１）⑥に規定する「機器・記録媒体等の管理手続」の中に社外持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、社外に持出す場合の取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。

⑤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）④に規定する「個人データの漏えい等防止策」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）①～③及び⑤～⑨に規定する事項を含まなければならない。

なお、生命保険会社等は、保管・保存段階における取扱規程について、「個人データへのアクセス制御」として、５－２（１）①～③に規定する事項を定めることが望ましい。

（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）①～⑥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）情報の取扱い

機微（センシティブ）情報の取扱いについては、上記（１）及び（２）に規定する事項に加えて、５－１（３）②及び④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。

①生命保険会社等は、５－１（１）⑥に規定する「機器・記録媒体等の管理手続」

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、物の持出しを防止するための措置等を講じる。

②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）⑦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）①～⑤及び⑦～⑨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」には宛先の照合及び確認手続が含まれる。

（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）①～⑤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）情報の取扱い

機微（センシティブ）情報の取扱いについては、上記（１）および（２）に規定する事項に加えて、５－１（３）①及び④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。

①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。）

②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）④に規定する「個人データの漏えい等防止策」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）①、②及び④～⑧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）情報の取扱い

機微（センシティブ）情報の取扱いについては、上記（１）に規定する事項に加えて、５－１（３）②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。

①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。

②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．漏えい等事案への対応の段階

（１）漏えい等事案への対応の段階における取扱規程

漏えい等事案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。

①対応部署の役割・責任

②漏えい等事案への対応に関する取扱者の限定

③漏えい等事案への対応の規程外作業に関する申請及び承認手続

④漏えい等事案の影響・原因等に関する調査手続

⑤再発防止策・事後対策の検討に関する手続

⑥自社内外への報告に関する手続

⑦漏えい等事案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

自社内外への報告に関する手続は、次に掲げる事項を含まなければならない。

①個人情報保護委員会又は監督当局への報告

②本人への通知等

③二次被害の防止・類似事案の発生回避等の観点からの漏えい等事案の事実関係及び再発防止策等の速やかな公表

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。

①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

②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

③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。

④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。

①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
②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
③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
④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、３－３の物理的安全管理措置及び３－４の技術的安全管理措置及び金融分野ガイドライン第８条第６項の外的環境の把握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。

①委託者の監督・監査・報告徴収に関する権限
②委託先における漏えい等の防止及び目的外利用の禁止
③再委託に関する条件
④漏えい等事案が発生した場合の委託先の責任

なお、生命保険会社等は、「再委託に関する条件」として、再委託の可否及び再委託を行うに当たっての委託元への文書による事前報告又は承認手続等を、委託契約に盛り込むことが望ましい。

また、生命保険会社等は、委託先において個人データを取り扱う者の氏名・役職又は部署名を、委託契約に盛り込むことが望ましい。

（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、定期的に監査を行う等により、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等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。

７．仮名加工情報等の安全管理措置

７－１．削除情報等の安全管理措置等

生命保険会社等は、仮名加工情報を作成したとき、又は仮名加工情報及び当該仮名加工情報に係る削除情報等を取得したときは、以下のとおり削除情報等の安全管理のための措置を講じなければならない。

①削除情報等を取り扱う者の権限及び責任の明確化

（例）

・削除情報等の安全管理措置を講ずるための組織体制の整備

②削除情報等の取扱いに関する規程類の整備及び当該規定類に従った削除情報等の適切な取扱い並びに、削除情報等の取扱状況の評価及びその結果に基づき改善を図るために必要な措置の実施

（例）

・削除情報等の取扱いに係る規程等の整備とこれに従った運用

・従業者の教育

・削除情報等の取扱状況を確認する手段の整備

・削除情報等の取扱状況の把握、安全管理措置の評価、見直し及び改善

③削除情報等を取り扱う正当な権限を有しない者による削除情報等の取扱いを防止するために必要かつ適切な措置

（例）

・削除情報等情報を取り扱う権限を有しない者による閲覧等の防止

・機器、電子媒体等の盗難等の防止

・電子媒体等を持ち運ぶ場合の漏えいの防止

・削除情報等の削除並びに機器、電子媒体等の廃棄

・削除情報等へのアクセス制御

・削除情報等へのアクセス者の識別と認証

・外部からの不正アクセス等の防止

・情報システムの使用に伴う加工方法等情報の漏えいの防止

８．匿名加工情報等の安全管理措置

８－１．加工方法等情報の安全管理措置

生命保険会社等は、匿名加工情報を作成したときは、加工方法等情報の漏えいを防止するために、次に掲げる必要な措置を講じなければならない。

①加工方法等情報を取り扱う者の権限及び責任の明確化

（例）

・加工方法等情報の安全管理措置を講ずるための組織体制の整備

②加工方法等情報の取扱いに関する規程類の整備及び当該規程類に従った加工方法等情報の適切な取扱い並びに加工方法等情報の取扱状況の評価及びその結果に基づき改善を図るために必要な措置の実施

（例）

・加工方法等情報の取扱いに係る規程等の整備とこれに従った運用

・従業者の教育

・加工方法等情報の取扱状況を確認する手段の整備

・加工方法等情報の取扱状況の把握、安全管理措置の評価、見直し及び改善

③加工方法等情報を取り扱う正当な権限を有しない者による加工方法等情報の取扱いを防止するために必要かつ適切な措置

（例）

・加工方法等情報を取り扱う権限を有しない者による閲覧等の防止

・機器、電子媒体等の盗難等の防止

・電子媒体等を持ち運ぶ場合の漏えいの防止

・加工方法等情報の削除並びに機器、電子媒体等の廃棄

・加工方法等情報へのアクセス制御

・加工方法等情報へのアクセス者の識別と認証

・外部からの不正アクセス等の防止

・情報システムの使用に伴う加工方法等情報の漏えいの防止

８－２．匿名加工情報の安全管理措置等

生命保険会社等は、匿名加工情報を取り扱うに当たっては、匿名加工情報の安全管理措置、苦情処理等の匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

当該安全管理等の措置については、個人情報と同様の取扱いを求めるものではないが、例えば、３．実施体制の整備から６．委託先の監督に定める個人データの安全管理、従業者の監督及び委託先の監督等を参考にすることも考えられる。具体的には、行おうとする事業の性質、当該業務に用いる匿名加工情報の取扱状況、取り扱う匿名加工情報の性質、量等に応じて合理的かつ適切な措置を講ずることが望ましい。

なお、匿名加工情報には識別行為の禁止義務が課されていることから、匿名加工情報

を取り扱うに当たっては、それを取り扱う者が不適正な取扱いをすることがないよう、匿名加工情報に該当することを明確に認識できるようにしておくことが重要である。そのため、作成した匿名加工情報について、匿名加工情報を取り扱う者にとってその情報が匿名加工情報である旨が一見して明らかな状態が望ましい。

以　上