損害保険会社における個人情報保護に関する安全管理措置等について実務指針

（改訂版）

2022年4月20日

一般社団法人　外国損害保険協会

目次

◆　損害保険会社における個人情報保護に関する安全管理措置等についての実務指針

Ⅰ．損害保険会社に係る個人情報保護指針（以下、「損保指針」）第17条に定める安全管理措置の実施について

１．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

１－１（個人データの安全管理に係る基本方針の整備）
損害保険会社等は、損保指針第17条に基づき、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、当該基本方針をホームページへの掲載等の適切な方法により公表するとともに、必要に応じて当該基本方針の見直しを行わなければならない。
①損害保険会社等の名称
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

＜参考事項＞

・基本方針は、自社の個人情報保護に関する考え方や方針に関する宣言（いわゆるプライバシーポリシー、プライバシーステートメント等。以下「個人情報保護宣言」という。）の一部として、同宣言と併せて公表してもよい。その場合、基本方針として定めるべき内容がすべて含まれていることが必要である。

【具体的な措置の例】
〇ルールの対外的明確化
・損害保険会社は、個人情報保護宣言を策定し、ホームページへの掲載等の適切な方法により公表する。
・個人情報保護宣言には、各社における例えば以下のような項目を規定することとし、その公表により、個人情報を目的外に利用しないことや苦情処理に適切に取り組むこと等を宣言するとともに、損害保険会社等が関係法令等を遵守し、利用目的の通知・公表、開示等の個人情報の取扱いに関する諸手続について、あらかじめ、対外的に分かりやすく説明する。
①当該会社における個人情報保護の考え方
②安全管理措置の概要
③開示の手続き
④苦情対応を含む各問い合わせ窓口　等

１－２（個人データの安全管理に係る取扱規程の整備）
⑴損害保険会社等は、損保指針第17条に定める「個人データの安全管理に係る取扱規程の整備」として、次項に定める、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含む社内規程を整備し、各管理段階ごとに別添１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。

⑵損害保険会社等は、次の各管理段階における安全管理に係る取扱規程を定めるものとする。
①取得・入力段階における取扱規程
②利用・加工段階における取扱規程
③保管・保存段階における取扱規程
④移送・送信段階における取扱規程
⑤消去・廃棄段階における取扱規程
⑥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。）等への対応の段階における取扱規程

＜参考事項＞

・１－２（１）の「各管理段階ごとに定める」という趣旨は、次のとおりである。
全社的には、各管理段階ごとに定める必要がある。
課ベース等で細分化して規程を定める場合には、業務実態に合わせ、複数の管理段階を合わせる、あるいは行っていない管理段階については規程を削除することもできる。
【具体的な措置の例】
〇ルールの明文化
・損害保険会社は、個人情報保護に係るルールを策定した場合には、従業者等に対して周知徹底させる目的から、ルール

の明文化を行い、その徹底を図る。
例：社内規程の策定
例：個人情報漏えいに関する社内通達を作成し、注意喚起を行う
例：業務マニュアルにおいて、個人情報に関連する日常業務における対応方法（開示請求を求められた場合の顧客への説明方法など）を掲載する。

・従業者に対して、就業規則に一般的な秘密保持義務を規定するほか、個人情報に関する秘密保持に関する誓約事項を定めた文書を取り付ける等、重要性を強く認識させる。

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）
損害保険会社等は、損保指針第17条に基づき、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。
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き

＜参考事項＞

・「点検」とは、「個人データを取り扱う部署が自ら取扱規程の遵守状況を確認するもの」、「監査」とは、「当該部署以外のものにより実施されるもの」という区別である。

・１－３①には、例えば次の場合がある。
例：社内規程が整備され、その実施体制が整備されていることを確認する。

１－４（外部委託に係る規程の整備）
損害保険会社等は、損保指針第17条に基づき、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

２．個人データの安全管理措置に係る実施体制の整備

１）実施体制の整備に関する組織的安全管理措置

損害保険会社等は、損保指針第 17 条第６項に基づき、個人データの安全管理措置に係る実施体制の整備における「組織的安全管理措置」として、次に掲げる措置を講じなければならない。

①個人データの管理責任者等の設置
②就業規則等における安全管理措置の整備
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個人データの取扱状況を確認できる手段の整備
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
⑥漏えい等事案に対応する体制の整備

＜参考事項＞

【具体的な情報漏えい防止策の例】
〇責任部署・責任者
・個人情報保護を推進するための社内のルールが適正に機能しているかをチェックし、見直しの要否を見極めるべく、個人情報保護に関する社内推進を行う責任部署・推進委員会（または推進責任者）を定める。
例：情報管理総括責任者（CPO）を設置する。
例：事務、システム、代理店募集等のそれぞれに本社推進責任者を定め、「個人情報保護推進委員会」を設置する。

２－１（個人データ管理責任者等の設置）
損害保険会社等は、「個人データの管理責任者等の設置」として次に掲げる役職者を設置しなければならない。
①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
②個人データを取扱う各部署における個人データ管理者
なお、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。
（注）金融分野における個人情報取扱事業者は、「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。

２－１－１
損害保険会社等は、２－１①に規定する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５－１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その他個人情報取扱事業者全体における個人データの安全管理に関すること

２－１－２
損害保険会社等は、２－１②に規定する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

＜参考事項＞

・２－１－１①には、例えば次の場合がある。
例：個人データの安全管理に関する規程の見直しにあたり、取締役会等の付議前に、個人データ管理責任者の承認を要するものとする。

・２－１－１②の本人確認に関する情報の「管理者」には、例えば次の場合がある。
例：パスワードを付与する人（個人データ管理者と同一人でもよいが、個人データ管理責任者とは別人であること）。

・２－１－２①には、例えば次の場合がある。
例：「○○課（グループ）の総合職」

・２－１－２⑤には、例えば次の場合がある。
例：事務室の施錠や営業時間外入退館（室）者の状況の実態把握

・２－１－２⑦には、例えば次の場合がある。
例：部店内の個人情報管理研修の開催

・２－１－２⑨には、例えば次の場合がある。
例：個人情報保護意識の高揚を図るための日常業務での点検・指導

【具体的な措置の例】
○日常業務における情報管理責任者による指導
・各部署や一定の組織、グループ等において、個人情報の取扱いに関する日常管理を行う情報管理責任者を定め、権限と役割を社内規程の中で明確化するとともに、日常業務の上での点検・指導を行わせ、個人情報保護意識の高揚を図る。
例：事務室の施錠や時間外入退者の状況の実態把握
例：部店内の個人情報管理研修の開催
○教育・研修
・損害保険会社は、従業者や代理店が個人情報に係る取扱ルールを遵守すること、および個人情報の収集・利用・第三者提供等の各段階が適切に行われるよう、教育・研修による個人情報保護に関する注意喚起を行い、意識の徹底と知識の定着を図ることとする。
例：個人情報保護に関するマニュアルやガイドブックの作成
例：対象者（営業社員、代理店、システム担当者等）別の研修会の実施
・情報漏えい事故の未然防止のため、監査やモニタリング等の実施により、個人情報の取扱いに係る管理状況状態を把握の上、必要に応じて改善・指導を行う。
例：社内監査や代理店監査の項目の中に、個人情報の取扱いに関する事項を追加する。
例：個人情報保護の社内ルールの遵守状況に係るモニタリング調査を実施する。

○店舗の防犯対策等
・個人情報を取扱う店舗においては、営業時間外における厳重な入退室管理（施錠、警備員配置等の人的警備、システム警備会社等のシステム的警備等）を徹底し、外部の者が侵入できない措置を講じる。あわせて、店舗責任者は、施錠のための鍵の管理等入退室管理に係るルールを明確化する。
・個人情報を取扱う店舗においては、扉やパーテーション等により接客スペースとの分離を行い、営業時間中に外部の者が執務スペース内に無断で立ち入りできない措置を講じる。
・個人情報が記録された電磁的記録媒体等や個人データが記録された重要書類については、施錠できるキャビネット等へ保管することとし、退社時の施錠確認を徹底する。また、保管場所ごとに鍵の管理者を定めるとともに、鍵の保管ルールを明確化する。

２－２（就業規則等における安全管理措置の整備）
損害保険会社等は、「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

＜参考事項＞

・「非開示契約等」とは、例えば次の場合がある。
例：念書、確認書等、後日、本人の意思が確認できるもの（電子的方式による等、必ずしも書面でなくても可）。

２－３（個人データの安全管理に係る取扱規程に従った運用）
損害保険会社等は、「個人データの安全管理に係る取扱規程に従った運用」として、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。

＜参考事項＞

・「取扱規程に定められた事項の遵守状況の記録」とは、「社内点検の記録」やいわゆる「モニタリング」といった全体の記録ではなく、取扱規程で定めたられた各管理段階での記録を意味している。

２－４（個人データの取扱状況を確認できる手段の整備）
損害保険会社等は、「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

２－５（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）
損害保険会社等は、「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」として、個人データを取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。

２－５－１
損害保険会社等は、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。

２－５－２
損害保険会社等は、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、定期的及び臨時の監査を実施しなければならない。なお、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。
（注）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。

＜参考事項＞

・２－５－１の「定期的及び臨時の点検を実施」とは、例えば次の場合である。
例：通常は「定期的な点検」とし、必要な場合（組織再編時、自社あるいは同業他社等での事故発生時）には「臨時の点検」を行うこと。
・２－５－２の「監査」とは、例えば次の場合である。
例：既存の社内監査部門による監査を活用すること。
例：外部監査を活用すること。

２－６（漏えい等事案に対応する体制の整備）
損害保険会社等は、「漏えい等事案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

＜参考事項＞

【具体的な措置の例】
〇漏えい報告体制の整備

・損害保険会社は、万が一個人情報の漏えい事故またはそのおそれが発生した場合に、迅速かつ適切な対応を講じることができるように、従業者だけでなく、代理店や個人情報を取扱う外部委託業者との間で、発生時の連絡体制や具体的な対処方法を定めておく。
例．委託契約書内に、情報漏えい事故またはそのおそれの発生時には、状況把握の上、速やかに保険会社へ第一報を行う旨の規定を設ける。
・実際に漏えい事故またはそのおそれがあるときは、直接または情報管理責任者を経由して推進責任部署・推進委員会（または推進責任者）へ速やかに（※）報告を行うものとする。
※個人情報保護法に基づき、「速報」、「確報」が必要となるが、委託元（損害保険会社）が委託先から通知を受けた日（知った日）を起算点として、監督当局に対しへの報告は、「速報」は、概ね３～５日以内、「確報」は概ね30日以内（不正目的事案等の場合は60日以内）での報告が必要。

２）実施体制の整備に関する人的安全管理措置

損害保険会社等は、損保指針第17条に基づき、個人データの安全管理措置に係る実施体制の整備における「人的安全管理措置」として、次に掲げる措置を講じなければならない。
①従業者との個人データの非開示契約等の締結
②従業者の役割・責任等の明確化
③従業者への安全管理措置の周知徹底、教育及び訓練
④従業者による個人データ管理手続の遵守状況の確認

＜参考事項＞

・Ⅰ．２．２）②には、例えば次の場合がある。
例：規程の整備による明確化
例：業務マニュアルによる明確化

・Ⅰ．２．２）③には、例えば次の場合がある。
例：社内通達の出状
例：コンプライアンス研修の際に安全管理措置を周知徹底

３－１（従業者との個人データの非開示契約等の締結）
損害保険会社等は、「従業者との個人データの非開示契約等の締結」として、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。

３－２（従業者の役割・責任等の明確化）
損害保険会社等は、「従業者の役割・責任等の明確化」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

＜参考事項＞

・３－２①には、例えば次の場合がある。
例：全社規程において、各管理段階ごとに明確化

・３－２③には、例えば次の場合がある。
例：（就業規則の整備のほか）懲戒処分規程の整備

３－３（従業者への安全管理措置の周知徹底、教育及び訓練）
損害保険会社等は、「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、以下の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
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
④従業者に対する教育・訓練の評価及び定期的な見直し

＜参考事項＞

・３－３①には、例えば次の場合がある。
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。
例：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。
例：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。

・３－３②には、例えば次の場合がある。

例：外部セミナーへの参加、外部講師による研修等

３－４（従業者による個人データ管理手続きの遵守状況の確認）
損害保険会社等は、「従業者による個人データ管理手続きの遵守状況の確認」として、１－２の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、２－３に基づく記録及び確認を行うとともに、２－５に基づき点検及び監査を実施しなければならない。

３）実施体制の整備に関する物理的安全管理措置

損害保険会社等は、損保指針第17条に基づき、個人データの安全管理措置に係る実施体制の整備における「物理的安全管理措置」として、次に掲げる措置を講じなければならない。
①個人データの取扱区域等の管理
②機器及び電子媒体等の盗難等の防止
③電子媒体等を持ち運ぶ場合の漏えい等の防止
④個人データの削除及び機器、電子媒体等の廃棄

４－１（個人データの取扱区域等の管理）
損害保険会社等は、「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

＜参考事項＞

・４－１①「入退室管理の方法」には、例えば次の場合がある。
例：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

・４－１③には、例えば次の場合がある。
例：間仕切り等の設置、座席配置の工夫等
例：個人データの取扱いを、個人データを取り扱う権限が付与されていない者の往来が少ない場所で実施すること
例：個人データをパソコンで取り扱う場合、離席時にパスワード付スクリーンセーバーの起動又はコンピュータのロック等で閲覧できないようにすること
例：個人データを記した書類、媒体、携帯可能なコンピュータ等を机上、社内等に放置しないこと

４－２（機器及び電子媒体等の盗難等の防止）
損害保険会社等は、「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

４－３（電子媒体等を持ち運ぶ場合の漏えい等の防止）
損害保険会社等は、「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持ち運ぶ個人データの暗号化、パスワードによる保護等
②書類等の封緘、目隠しシールの貼付等

４－４（個人データの削除及び機器、電子媒体等の廃棄）
損害保険会社等は、「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

＜参考事項＞

・４－４②の個人データが記載された書類等の廃棄には、例えば次の場合がある。
例：焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。
・また、４－４②の個人データが記録された機器、電子媒体等の廃棄には、例えば次の場合がある。
例：専用のデータ削除ソフトウェアの利用または物理的な破壊等の手段を採用する。

４）実施体制の整備に関する技術的安全管理措置

損害保険会社等は、損保指針第17条に基づき、個人データの安全管理措置に係る実施体制の整備における「技術的安全管理措置」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の記録及び分析
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
⑦個人データを取り扱う情報システムの監視及び監査

＜参考事項＞

・紙ベースの個人データについて、本項で定める「技術的安全管理措置」を施すことまでは求められていない。

【具体的な措置の例】
〇アクセスの制限
・社外インターネットに接続されたシステムでは、外部からの不正アクセスに対応すべく、ファイアーウォールを設置する。
・個人情報が入ったデータファイル等については、個人データの利用目的や重要性に応じて、例えば暗号化やパスワード設定を行って利用制限を設ける等、情報取扱者以外は内容を確認できない措置を講じる。
・パソコン本体につき、データ内容の暗号化やパスワード設定等の措置を講じる。
・個人情報の利用目的や重要性に応じて、例えば部署や役職別にアクセス制限を設ける等の措置を講じる。

〇アクセス記録の監視
・個人情報の不適正な利用を防止する観点から、アクセス記録を検証する。
例：社外メール等による不正使用による個人情報の漏洩防止の観点から、例えば定期的に一定数の社外宛メールをランダムに抽出して内容確認する、等の抜き取り調査を実施する。
例：データベースへの照会履歴を記録できるシステム措置を行い、モニタリング調査を定期的に実施する。

〇ダウンロード制限
・電子的な個人情報データベースからローカル端末へのダウンロードについて、権限や件数の制限を設ける。

５－１（個人データの利用者の識別及び認証）
損害保険会社等は、「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

５－２（個人データの管理区分の設定及びアクセス制御）
損害保険会社等は、「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

５－２－１
損害保険会社等は、「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

＜参考事項＞

・５－２②には、例えば次の場合がある。
例：パスワード設定

５－３（個人データへのアクセス権限の管理）
損害保険会社等は、「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
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
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

５－４（個人データの漏えい等防止策）
損害保険会社等は、「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。

５－４－１
損害保険会社等は、「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コンピュータウイルス等不正プログラムへの防御対策

５－４－２
損害保険会社等は、「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コンピュータウイ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

＜参考事項＞

・５－４－２③は、不正な原因に限らず、システム障害が起こった場合の対応であり、①、②とは区別される。

５－５（個人データへのアクセスの記録及び分析）
損害保険会社等は、「個人データへのアクセスの記録及び分析」として、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。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。

５－６（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）
損害保険会社等は、「個人データを取り扱う情報システムの稼動状況の記録及び分析」として、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。

５）外的環境の把握

損害保険会社等は、損保指針第17条に基づき、個人データの安全管理措置に係る実施体制の整備における「外的環境の把握」として、外国において個人データを取り扱う場合には、外的環境を把握した上で、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なければならない。
「外的環境の把握」とは、外国において個人データを取り扱う場合に、当該外国の個人情報の保護に関する制度等を把握することをいう。

＜参考事項＞

・「外国において個人データを取り扱う場合」とは、次の場合である。

例：損害保険会社等が、外国にある支店・営業所に個人データを取り扱わせる場合
【具体的な措置の例】
〇外国にある支店や営業所に個人データを取り扱わせる場合
・損害保険会社等は、外国において個人データを取り扱うこととなるため、支店等が所在する外国の個人情報の保護に関する制度等を把握した上で、安全管理措置を講じる。
〇外国に支店等を設置していない場合
・外国にある従業者に個人データを取り扱わせる場合、本人が被る権利利益の侵害の大きさを考慮し、その個人データの取扱状況（個人データを取り扱う期間、取り扱う個人データの性質及び量を含む。）等に起因するリスクに応じて、従業者が所在する外国の制度等を把握すべき場合もある。例えば、外国に居住してテレワークをしている従業者に個人データを取り扱う業務を担当させる場合には、当該従業者の所在する外国の制度等も把握して安全管理措置を講じる。他方、外国に出張中の従業者に一時的にのみ個人データを取り扱わせる場合には、必ずしも、安全管理措置を講じるにあたって、外国の制度等を把握する必要まではない。以上は、外国にある支店等や従業者が、日本国内に所在するサーバに保存されている個人データにアクセスして、これを取り扱う場合においても同様。
〇「保有個人データの安全管理のために講じた措置」
・支店等や従業者が所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く。
例：損害保険会社等が、外国にある第三者に個人データの取扱いを委託、再委託する場合

【具体的な措置の例】
〇外国にある第三者に個人データの取扱いを委託する場合
・委託元は、委託先を通じて外国において個人データを取り扱うこととなるため、委託先が所在する外国の個人情報の保護に関する制度等を把握した上で、委託先の監督その他の安全管理措置を講じる。また、委託先が外国にある第三者に個人データの取扱いを再委託する場合、委託元は、委託先及び再委託先を通じて外国において個人データを取り扱うこととなるため、再委託先が所在する外国の制度等も把握した上で、安全管理措置を講じる。以上は、委託先や再委託先が、日本国内に所在するサーバに保存されている個人データにアクセスして、これを取り扱う場合においても同様。
〇「保有個人データの安全管理のために講じた措置」
・委託先・再委託先が所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く。なお、委託元は、個人データの取扱いの委託に伴って委託先に個人データを提供する場合において、委託先が「外国にある第三者」（法第28条第１項）に該当するときは、原則として委託先が所在する外国の名称等を本人に情報提供した上で、本人の同意を取得する（法第28条第１項・第２項）。かかる場合においても、委託元は、上記のとおり、安全管理措置を講じ、また、保有個人データの安全管理のために講じた措置を本人の知り得る状態に置く。

例：外国にある損害保険会社等が、国内にある者に対する物品又は役務の提供に関連して、国内にある者を本人とする個人データを取り扱う場合

例：外国にある第三者の提供するクラウドサービスを利用し、その管理するサーバに個人データを保存する場合（ただし、クラウドサービス提供事業者が個人データを取り扱わないこととなっている場合を除く）
【具体的な措置の例】
〇「保有個人データの安全管理のために講じた措置」
・クラウドサービス提供事業者が所在する外国の名称及び個人データが保存されるサーバが所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く。他方、個人データが保存されるサーバが所在する国を特定できない場合には、サーバが所在する外国の名称に代えて、①サーバが所在する国を特定できない旨及びその理由、及び、②本人に参考となるべき情報を本人の知り得る状態に置く。②本人に参考となるべき情報としては、例えば、サーバが所在する外国の候補が具体的に定まっている場合における当該候補となる外国の名称等。

Ⅱ．損保指針第 17 条に定める「従業者の監督」について

損害保険会社等は、損保指針第17条に基づき、「Ⅰ．２．２）実施体制の整備に関する人的安全管理措置」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。

Ⅲ．損保指針第 17 条第２項に定める「委託先の監督」について

損害保険会社等は、損保指針第17条第２項に基づき、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し、個人データの取扱いを委託するとともに、委託先における当該個人データに対する安全管理措置の実施を確保しなければならない。
なお、再委託を行おうとする場合は、損害保険会社等は委託を行う場合と同様、再委託の相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、委託元に事前報告又は承認手続を求める、直接又は委託先を通じて定期的に監査を実施する等により、再委託先に対して損保指針第17条に基づく委託先の監督を適切に果たすこと、再委託先が個人情報保護法第23条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が、再々委託を行う場合以降も、再委託を行う場合と同様とする。

６－１（個人データ保護に関する委託先選定の基準）
損害保険会社等は、個人データの取扱いを委託する場合には、損保指針第17条第２項に基づき、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託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
④委託先の経営の健全性
なお、委託先の選定に当たっては、必要に応じて個人データを取り扱う場所に赴く又はこれに代わる合理的な方法による確認を行ったうえで、個人データ管理責任者等が適切に評価することが望ましい。

６－１－１
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

６－１－２
委託先選定の規準においては、「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、Ⅰ．２．１）の組織的安全管理措置、同２）の人的安全管理措置、同３）の物理的安全管理措置、同４）の技術的安全管理措置及び「金融分野における個人情報保護に関するガイドライン（以下、「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。

＜参考事項＞

【具体的な措置の例】
<u>〇委託先選定基準</u>
・損害保険会社は、個人情報の取扱いを含めた業務を外部業者へ委託する場合には、財務内容における安全性、業務実績や技術・サービスレベルの質等の観点だけでなく、外部委託先における目的外利用の禁止を含めた顧客情報管理が整備されており、守秘義務を遵守できる体制にあるかを確認した上で、個人情報の取扱いにつき適切と判断できる委託先を選定する。
・委託先が損害保険会社の子会社である場合には、損害保険会社は、原則として親会社の個人情報の取扱規程に準拠した取扱いがなされるよう指導・監督する。

６－２（委託先の遵守状況の定期的又は随時の確認等）
損害保険会社等は、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。

６－３（委託契約において盛り込むべき安全管理に関する内容）
損害保険会社等は、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委託先における個人データの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漏えい等事案等が発生した際の委託先の責任
（注）
・損害保険会社等は、「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。
・損害保険会社等は、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。

＜参考事項＞

・６－３①には、例えば次の場合がある。
例：指導内容の反映方法、報告徴収の頻度

・６－３②には、例えば次の場合がある。
例：守秘義務

・６－３④には、例えば次の場合がある。
例：契約違反、損害発生の場合における連絡体制、解決方法、損害賠償および契約解除
例：損害賠償、被害拡大防止のために必要な措置

・６－３に関する上乗せ措置には、例えば次のものがある。
例：委託業務終了後の個人情報の返却又は消去・廃棄

【具体的な措置の例】
〇適切な委託契約の締結
・損害保険会社は、個人情報の取扱いを含む業務を委託する際の委託契約書に、以下のような具体的な取り決めを規定することとする。
①委託した個人情報に関する委託先の守秘義務を定めること
②委託先が受託業務の遂行に必要な範囲を超えて、個人情報を利用しないこと
③委託先が委託業務終了後、個人情報を損害保険会社に返却するか、委託先自身が確実に消去・廃棄を行うこと
④損害保険会社と委託先の業務範囲、権利義務および責任分担に関する事項を定めること
⑤契約違反・損害発生の場合における連絡体制、解決方法、損害賠償および契約の解除に関する事項を定めること
⑥委託先に対して、事務処理等の適切性に係る検証を行うことを可能とすること

６－４（委託先で遵守されていない場合の監督等）
損害保険会社等は、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、損害保険会社等は、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。
なお、委託契約に定める安全管理措置の遵守状況については、個人データ管理責任者等が、当該安全管理措置等の見直しを検討することを含め、適切に評価することが望ましい。

＜参考事項＞

【具体的な措置の例】
〇監督・監視の実施
・損害保険会社は、外部委託先が行う業務について、例えば１年に１回、委託契約書上の義務の履行状況や安全管理措置の実施状況について報告を求める等、適切な監督・監視を行うものとする。

・損害保険会社は、個人情報を大量に扱うシステム関係の委託先に対して、システム上の監査の実施要領を策定し、例えば１年に１回、安全管理措置に関する監査を行う等、個人情報の取扱いが適切であることの確認を行う。

６－５（損害保険代理店に対する必要かつ適切な監督）
損害保険会社等は、損保指針第19条第１項に基づき、損害保険代理店における個人データの安全管理措置として、以下の事項を含む、代理店に対する必要かつ適切な監督を行わなければならない。
①損害保険代理店選定の基準の策定及び当該基準に従った損害保険代理店の選定
②損害保険代理店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
③損害保険代理店における個人データの安全管理に係る実施体制の整備
④損害保険代理店における個人データの安全管理に係る保護対策の実施
⑤損害保険代理店における店主または従業員の外出時のデータ管理
⑥損害保険代理店に対する個人データの安全管理に係る定期的又は随時の点検・監査の実施

＜参考事項＞

・６－５③には、例えば次の場合がある。
　例：日常の業務指導や教育

・６－５④には、例えば次の場合がある。
　例：代理店オンラインシステムのセキュリティ（アクセス制御等）

【具体的な措置の例】
〇代理店が遵守すべきルール
・損害保険会社は、その個人データを日常的に取扱っていることに鑑み、損害保険会社の従業者に適用される安全管理措置に準じたルールを定めることとする。特に代理店が個人情報の社外・店外持ち出した時の事故が多発している現状を踏まえ、代理店の外出時のデータ管理には最大限の注意を払う必要がある。
・損害保険会社は、代理店が遵守すべきルールを定め、日常の業務指導や教育の中で徹底する。
〇代理店への監督、検証
・損害保険会社は、代理店に対して、個人情報の取扱いに関する各種のルールが遵守されているかの検証を行い、問題がある場合には是正措置を早急に講じることとする。
　例：顧客の保険加入データ等がきちんとファイルされているか、そのファイルは適正な管理がなされているかを確認する。
・損害保険会社は、代理店に対して、定期的に監査・点検を実施し、その項目の中に個人情報の取扱いの状況を含めるものとする。
〇代理店システム措置
・損害保険会社から提供するシステムは、社内システムに準じたセキュリティ（アクセス制御等）を持たせることとする。
・代理店システムを通じて提供される情報は、当該代理店が扱う保険契約に限定することとし、他の情報にはアクセスできない仕組みを講じることとする。
・代理店システムを通じて提供される個人情報を含むデータファイルは、暗号化やパスワード設定等、当該代理店以外には内容が確認できないような措置を講じる。

（別添１）１－２に定める各管理段階における安全管理に係る取扱規程について

損害保険会社等は、１－２に基づき、各管理段階における安全管理に係る取扱規程において、７－１から７－６－１までの事項を定めなければならない。

７－１（取得・入力段階における取扱規程）
損害保険会社等は、取得・入力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取得・入力に関する取扱者の役割・責任
②取得・入力に関する取扱者の限定
③取得・入力の対象となる個人データの限定
④取得・入力時の照合及び確認手続き
⑤取得・入力の規程外作業に関する申請及び承認手続き
⑥機器・記録媒体等の管理手続き
⑦個人データへのアクセス制御
⑧取得・入力状況の記録及び分析
（注）損害保険会社等は、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
（例）記録機能を持つ媒体の持ち込み・持ち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能の更新への対応

＜参考事項＞

・７－１④は、取得時に確認、入力時に照合の手続きを定めるという趣旨である。

・７－１⑥には、例えば次の場合がある。
例：パソコン等の置き場所等の管理ルールを策定

・７－１⑦には、例えば次の場合がある。
例：契約データ入力の際の取扱者の限定
例：個人データを取り扱う室内への部外者の立入制限

・７－１⑧の「記録」とは、漏えい等事案が発生した際に、原因及び漏えいルートの解明等を行い、個人データの漏えい・き損等を防止するために行うものである。（以下の７－２から７－６の「記録」についても同様。）

７－２－１
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、次に掲げる事項を含まなければならない。
①利用・加工に関する取扱者の役割・責任
②利用・加工に関する取扱者の限定
③利用・加工の対象となる個人データの限定
④利用・加工時の照合及び確認手続き
⑤利用・加工の規程外作業に関する申請及び承認手続き
⑥機器・記録媒体等の管理手続き
⑦個人データへのアクセス制御
⑧個人データの管理区域外への持ち出しに関する上乗せ措置
⑨利用・加工状況の記録及び分析
（注）損害保険会社等は、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、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
（例）記録機能を持つ媒体の持ち込み・持ち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能の更新への対応

７－２－１－１
「個人データの管理区域外への持ち出しに関する上乗せ措置」は、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ち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ち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ち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ち出し時の照合及び確認手続き
⑤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
⑥機器・記録媒体等の管理手続き
⑦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

７－２－２
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、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個人データを取扱う情報システムの稼動状況の記録及び分析

＜参考事項＞

・７－２－１－１の「管理区域」とは、次の場合である。
　例：営業範囲を勘案して予め指定した区域（例えば、事務所内、客先及びその間の往復過程）

・７－２－１－１⑥には、例えば次の場合がある。
　例：個人データを持ち出す場合の常時携行

【具体的な措置の例】
○個人情報が記載・記録された書面や情報媒体を社外に持ち出す場合には、その目的・用途に鑑み、業務上必要不可欠なものに限ることとし、持ち出すときは常時携行する等、自らの管理下に置くことを徹底させる。
　例：個人情報が記載・記録された書面や情報媒体の入った鞄を車内に置いて自動車を離れない。
　例：個人情報が記載・記録された書面や情報媒体の入った鞄を電車やバスの網棚の上に置かない。
○情報持ち出し制限に関する社内ルールを策定する。
　例：持ち出した個人情報を携行したまま帰宅する場合には、直属の上司からの承認を得る。
○電子メールやＦＡＸの送信時には、事前に宛先の登録を行い、電子メールには宛先確認の機能を付加するなど、誤送信発生の防止を徹底させる。

７－３（保管・保存段階における取扱規程）
損害保険会社等は、保管・保存段階における取扱規程において、組織的安全管理措置と技術的安全管理措置を定めなければならない。

７－３－１
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として、次に掲げる事項を含まなければならない。
①保管・保存に関する取扱者の役割・責任
②保管・保存に関する取扱者の限定
③保管・保存の対象となる個人データの限定
④保管・保存の規程外作業に関する申請及び承認手続き
⑤機器・記録媒体等の管理手続き
⑥個人データのアクセス制御
⑦保管・保存状況の記録及び分析
⑧保管・保存に関する障害発生時の対応・復旧手続き
（注）損害保険会社等は、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、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
（例）記録機能を持つ媒体の持ち込み・持ち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能の更新への対応

７－３－２
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個人データを取扱う情報システムの稼動状況の記録及び分析

＜参考事項＞

・７－３－１⑤には、例えば次の場合がある。
例：施錠できるキャビネット等へ保管し、退社時の施錠確認を徹底
例：保管場所ごとに鍵の管理者を定め、鍵の保管ルールを明確化

・７－３－１⑥には、例えば次の場合がある。
例：個人情報を取扱う店舗における執務スペースと接客スペースの分離
例：機器・記録媒体等の施錠保管
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、ゾーン毎の入退室管理（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）、物の持ち出しを防止するための措置等を講じる。

７－４（移送・送信段階における取扱規程）
損害保険会社等は、移送・送信段階における取扱規程において、組織的安全管理措置及び技術的安全管理措置を定めなければならない。

７－４－１
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、次に掲げる事項を含まなければならない。
①移送・送信に関する取扱者の役割・責任
②移送・送信に関する取扱者の限定
③移送・送信の対象となる個人データの限定
④移送・送信時の照合及び確認手続き
⑤移送・送信の規程外作業に関する申請及び承認手続き
⑥個人データへのアクセス制御
⑦移送・送信状況の記録及び分析
⑧移送・送信に関する障害発生時の対応・復旧手続き

７－４－２
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、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

＜参考事項＞

・７－４－１④には、例えば次の場合がある。
　例：事前に厳正な番号確認を行ったうえでの、短縮ダイヤルの使用（実際の送り先と短縮ダイヤルの登録内容を確認すること）

７－５（消去・廃棄段階における取扱規程）
損害保険会社等は、消去・廃棄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消去・廃棄に関する取扱者の役割・責任
②消去・廃棄に関する取扱者の限定
③消去・廃棄時の照合及び確認手続き
④消去・廃棄の規程外作業に関する申請及び承認手続き
⑤機器・記録媒体等の管理手続き
⑥個人データへのアクセス制御
⑦消去・廃棄状況の記録及び分析

＜参考事項＞

・７－５③には、例えば次の場合がある。
　例：保存期限にあっているかの照合
　例：消去・廃棄の対象となる書類かどうかの確認

【具体的な措置の例】
○損害保険会社は、業務上必要でなくなった個人情報は、次のような媒体に即した適切な方法にて処分する。
　例：パソコン等個人情報を取扱う機器類の廃棄は、保存データの消去を確実に行った上で、破壊処理（または破壊に準じた処理）を行う。
　例：個人情報が記載された印刷物を破棄する場合は、焼却またはシュレッダー処理を行う。
○損害保険会社は、個人情報の保存期限について、当該個人情報の利用目的に応じた適切な保存期間を設けることとする。
　例：保険契約データについては、満期または解約後一定期間をもってシステム端末からデータをドロップさせる。

７－６（漏えい等事案への対応の段階における取扱規程）
　損害保険会社等は、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き
④漏えい等事案の影響・原因等に関する調査手続き
⑤再発防止策・事後対策の検討に関する手続き
⑥自社内外への報告に関する手続き
⑦漏えい等事案への対応状況の記録及び分析

７－６－１
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。
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早急な公表
(注)損害保険会社等は、個人情報保護法施行規則（平成28年個人情報保護委員会規則第３号）第７条各号に定める事態を知ったときは、個人情報保護法律（平成15年法律第57号）第26条及び個人情報の保護に関する法律についてのガイドライン（通則編）（平成28年個人情報保護委員会告示第６号）３－５－３（個人情報保護委員会への報告）及び３－５－４（本人への通知）に従い、必要な措置を講ずる必要があるため、この点に留意して上記手続を定めること。

＜参考事項＞

・７－６－１①の「個人情報保護委員会又は監督当局への報告」とは、個人情報保護法施行規則第６条の２で法に基づく報告として定める４類型のうち、金融分野ガイドラインおよび金融分野ガイドラインの安全管理措置等についての実務指針の対象外である非顧客情報（金融機関自身の雇用管理情報、株主情報の漏えい等事案）については、個別に個人情報保護委員会への報告が必要となる。その他漏えい等事案の報告に関しては、個人情報保護法施行規則第６条の２で法に基づく報告として定める４類型および保険業法施行規則第53条の８の２、第227条の９の２、金融分野ガイドライン第11条等に基づき個人情報保護委員会又は監督当局へ報告する。

・７－６－１①の「監督当局への報告」の「等」とは、警察への報告を含む趣旨である。

・個人情報の漏えい事故またはそのおそれが発生した場合には、損害保険会社は遅滞なく監督官庁への報告を行うとともに、以下の措置を案件ごとに必要性を判断した上で講じることとする。
①漏えい等により影響を受ける可能性のある本人への通知を行う。
②事業所内部における報告及び被害の拡大防止を行う。
③事実関係の調査及び原因の究明を行う。
④影響範囲の特定を行う。
⑤再発防止策の検討及び実施を行う。
⑥漏えい等による二次被害の防止や、類似事故の発生回避のために必要な場合には、本人その他第三者の権利を侵害することのないよう配慮した上で、事実関係及び再発防止策等の公表を速やかに行う。

・推進責任部署、推進委員会または推進責任者は、情報漏えい等の事故に対する原因調査を踏まえた再発防止策の検討を行い、情報発信を行う等により、社内での徹底を図る。また、必要に応じて社内ルールを見直すこととする。

【具体的な情報漏えいにかかる苦情の事例】
・次のような苦情が寄せられており、損害保険会社は、かかる事例の防止策の検討を行い、情報発信を行う等により、社内での徹底を図る。
　例：停車中に追突され頚椎捻挫の被害にあった被害者の職場に、加害者の損害保険会社の担当者から電話連絡があり、被害者が不在だったため、示談にかかる内容を同僚に伝言した事例。

（別添２）金融分野ガイドライン第５条に定める「機微（センシティブ）情報」（生体認証情報を含む。）の取扱いについて

損害保険会社等は、損保指針第16条に基づき、機微（センシティブ）情報について、同条第１項各号に掲げられた場合を除き、取得、利用又は第三者提供を行わず、同条第２項に基づき、同条第１項各号の事由を逸脱した取得、利用又は第三者提供を行うことのないよう、本実務指針Ⅰ～Ⅲに規定する措置に加えて、８－１、８－１－１、８－１－２、８－１－３、８－１－４、８－１－５及び８－２に規定する措置を実施することとする。また、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）の取扱いについては、別添２に規定する全ての措置を実施しなければならない。

８－１
損害保険会社等は、１－２に規定する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）情報の取扱いについて規程に定めるとともに、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。

８－１－１
損害保険会社等は、７－１に規定する取得・入力段階における取扱規程において、機微（センシティブ）情報の取扱いについては、７－１に規定する事項に加えて、次に掲げる事項を定めることとする。
①損保指針第16条第１項各号に定める場合のみによる取得
②取得・入力を行う取扱者の必要最小限の限定
③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

８－１－１－１
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、取得・入力段階における取扱規程において、７－１－１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

８－１－２
損害保険会社等は、７－２に定める利用・加工段階における取扱規程において、機微（センシティブ）情報の取扱いについては、７－２－１、７－２－１－１及び７－２－２に定める事項に加えて、次に掲げる事項を定めることとする。
①損保指針第16条第１項各号に定める目的のみによる利用・加工
②利用・加工を行う取扱者の必要最小限の限定
③利用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
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

８－１－２－１
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、利用段階における取扱規程において、８－１－２に定める事項に加えて、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等による不正誤証の防止措置
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き

８－１－３
損害保険会社等は、７－３に規定する保管・保存における取扱規程において、機微（センシティブ）情報の取扱いについては、７－３－１及び７－３－２に規定する事項に加えて、次に掲げる事項を定めることとする。
①保管・保存を行う取扱者の必要最小限の限定
②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

８－１－３－１
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、保存段階における取扱規程において、８－１－３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。

８－１－４
損害保険会社等は、７－４に規定する移送・送信における取扱規程において、機微(センシティブ)情報の取扱いについては、７－４－１及び７－４－２に規定する事項に加えて、次に掲げる事項を定めることとする。
①損保指針第16条第１項各号に定める目的のみによる移送・送信
②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

８－１－５
損害保険会社等は、７－５に規定する廃棄・消去における取扱規程において、機微（センシティブ）情報の取扱いについては、７－５に規定する事項に加えて、消去・廃棄を行う取扱者の必要最小限の限定について定めることとする。

８－１－５－１
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、消去段階における取扱規程において、８－１－５に規定する事項に加えて、生体認証情報を本人確認に用いる必要性がなくなった場合は、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。

８－２
損害保険会社等は、２－５－２に定める監査の実施に当たっては、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。

＜参考事項＞

・８－１－１③の「本人への説明事項」の対象は「本人同意の対象となる事項」である。すなわち、そこでの「説明」は、たとえば損保契約の申込に際しては、損保指針第 16 条第 1 項（１）に定める保険事業の適切な業務運営を確保する必要性から、業務遂行上必要な範囲で機微(センシティブ)情報を取得、利用等を行うことについて説明することである。

以上