お客さまからの信頼を高めていくための

募集コンプライアンスガイド

保険募集等の情報管理態勢の留意事項について

本ガイドは、保険募集時等における情報管理態勢を整備するうえで、代理店・募集人の皆さまの参考となる対応例等をとりまとめた雛形であり、本ガイドに記載された内容以外の取組みや対応を妨げるものではありません。

2025年3月版（情報管理版）

一般社団法人 日本損害保険協会

はじめに

近年、サイバー攻撃の巧妙化やシステム脆弱性等の管理の難易度の高まりを受けて、保険会社の業務の健全性および適切性の確保の観点から、サイバーセキュリティ強化の重要性が高まっており、保険募集時等の顧客等に関する情報管理もますます重要になっています。

これを受けて、金融庁では、2024年10月に金融機関等のサイバーセキュリティ管理態勢に関して留意すべき点を定めた「金融分野におけるサイバーセキュリティに関するガイドライン」を策定しています。

また、損害保険業界において情報漏えい事案が相次いで発生しており、2025年３月には一部の保険会社に対して、業務改善命令が発出される事態となりました。

これら課題の解決に向け、損害保険業界として情報管理を強化する取組みの一環として、「保険募集時等の情報管理態勢の留意事項」について、基本的な考え方を整理しました。

保険募集時等における情報管理の強化については、損害保険各社だけでなく、代理店・募集人の皆さまとともに取り組んでいく必要があります。本コンテンツに基づき情報管理態勢の整備状況を改めて確認いただき、業界の信頼回復にともに取り組んでいただくようお願いします。

なお、損保協会ではe-ラーニング学習サイト「募集人向けの教育支援サイト（https://www.sonpo-dairiten.jp/education/index.html）」にて情報セキュリティについて解説していますので、お役立てください。

2025年３月作成

一般社団法人 日本損害保険協会

もくじ

1 保険募集時等の情報管理態勢について

参考資料

1 保険募集時等の情報管理態勢について

1-1 保険募集人の健全かつ適切な業務運営

代理店は、健全かつ適切な業務運営に向けて、顧客等に関する情報管理態勢およびシステムリスク管理態勢を整備し、適切に情報管理する必要があります。

（１）顧客等に関する情報管理態勢

顧客等に関する情報は、保険契約取引の基礎をなすものであり、その適切な管理が確保されることが極めて重要となります。

保険募集人が健全かつ適切な業務運営を行うにあたっては、顧客等に関する情報管理態勢を整備する必要があります。なお、保険会社等からの出向者についても、代理店の一員として情報管理を徹底してください。

ａ．保険契約取引にあたって必要となる顧客情報（企業情報・個人情報など）
ｂ．保険契約手続きにあたって必要となる情報（クレジットカード情報など）
ｃ．保険事故に関する情報

また、顧客に関する情報以外にも、所属保険会社に関する情報（各種引受ルールなど）や代理店経営において取り扱う情報（従業員情報）があります。

保険募集時等に取り扱う顧客等に関する情報には、個人情報および企業情報（法人関係情報(注１)を含む）、さらには営業秘密(注２)などの機密情報があります。

基本的には、保険募集人は、保険業法に基づき適切に情報管理を行うことが求められるほか、個人である顧客に関する情報を取り扱う場合には、個人情報の保護に関する法律（以下「個人情報保護法」）に基づく対応が求められます。また、所属保険会社との代理店委託契約に基づき、適切に管理する必要があります。

（注１）インサイダー取引の防止の観点から法人関係情報を取り扱う場合には、金融商品取引法に基づく対応が必要となります。

（注２）経営情報をはじめとする営業秘密を取り扱う場合には、不正競争防止法に基づく対応が必要となります。

<table>
<tr><td colspan="2">保険業法の対象
顧客等に関する情報</td></tr>
<tr><td>個人情報保護法の対象
個人情報</td><td>金融商品取引法の対象
法人関係情報</td></tr>
</table>

ア．保険業法

保険業法では、保険募集に関する業務の健全かつ適切な運営を確保するために、保険募集人に対して、個人顧客情報の安全管理措置をはじめ、次の措置を講じることを求めています（保険業法第２９４条の３、施行規則第２２７条の９～１１）。

ａ．個人顧客情報の安全管理措置
ｂ．個人顧客情報の漏えい等の報告
ｃ．特別の非公開情報の取扱い
ｄ．委託業務の的確な遂行を確保するための措置

イ．保険会社向けの総合的な監督指針（以下「監督指針」）

保険募集人は、顧客等に関する情報管理の適切性を確保する必要性および重要性を認識したうえで、その適切性を確保するための組織体制の確立や社内規程の策定など、内部管理態勢を整備する必要があります（監督指針Ⅱ―４－２－９（２）、Ⅱ―４―５―２（１）①）。

ａ．顧客等に関する情報の取扱いについて、具体的な取扱い基準を定めた上で、研修等により役職に周知徹底を図っているか。
ｂ．顧客等に関する情報の管理が適切に行われているかを検証できる体制となっているか。
①顧客等に関する情報へのアクセス管理の徹底
②内部関係者に顧客等に関する情報の持出の防止に係る対策
③外部からの不正アクセスの防御等情報システム管理の堅牢化の対策

顧客等に関する情報の取扱いを委託する場合には、外部委託先において顧客等に関する情報管理が適切に行われているか確認する必要があります（監督指針Ⅱ―４―５―２（１）④）。

ａ．外部委託先の管理について、責任部署を明確化し、外部委託先における業務の実施状況を定期的または必要に応じてモニタリングしているか。
ｂ．外部委託先において漏えい等が発生した場合に、適切な対応がなされ、速やかに委託元に報告される体制になっていることを確認しているか。
ｃ．外部委託先による顧客等に関する情報へのアクセス権限について、委託業務の内容に応じて必要な範囲内に制限しているか。
ｄ．二段階以上の委託が行われた場合には、外部委託先が再委託先等の事業者に対して十分な監督を行っていることを確認しているか。

また、顧客等に関する情報の漏えい等が発生した場合についても、対応が適切に行われる体制を整備する必要があります（監督指針Ⅱ―４―５―２（１）⑤）。

ａ．情報漏えい等が発生した場合に、適切に責任部署に報告され、二次被害等の発生防止の観点から、対象となった顧客等への説明、当局への報告および必要に応じた公表が迅速か適切に行われる体制が整備されているか。
ｂ．情報漏えい等が発生した原因を分析し、再発防止に向けた対策が講じられているか。さらには、他社における漏えい事故等を踏まえ、類似事例の再発防止のために必要な措置の検討を行っているか。

ウ．関連法令

顧客等に関する情報管理態勢の整備にあたっては、保険業法をはじめ、個人である顧客に関する情報を取り扱う場合には、個人情報保護法を遵守する必要があります。

また、保険募集の業務を遂行するなかで、営業秘密を取り扱う場合には、不正競争防止法を遵守する必要があり、法人関係情報を取り扱う場合には、金融商品取引法を遵守する必要があります。

参考　営業秘密について

不正競争防止法は、「この法律において『営業秘密』とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上または営業上の情報であって、公然と知られていないものをいう。」と規定し、営業秘密を秘密管理性、有用性、非公知性を有する技術上または営業上の情報と定義しています（同法第２条６項）。例えば、代理店においては、契約取扱規程集や引受指針等が該当する可能性があります。

（２）システムリスク管理態勢

システムリスクとは、システムのダウンまたは誤作動等のシステムの不備やシステムが不正に利用されることにより、顧客や保険会社が被るリスクとされ、近年、ネットワーク化の拡大に伴い、重要情報に対する不正なアクセス、漏えい等のリスクが大きくなっていると指摘されています。

そのような環境下においてシステムが安全かつ安定的に稼働することは保険会社に対する信頼性を確保するための大前提であり、システムリスク管理態勢の充実強化は極めて重要であるとされています（監督指針Ⅱ－３―１３－２）。

保険会社の委託先である保険代理店もその一翼を担うことが求められており、保険会社のシステムリスク管理における取組みを十分に理解したうえで、保険募集を行う必要があります。

なお、代理店は、リスクの規模や大きさ等を踏まえ、システムリスク管理における取組みを行う必要があります。

ア．情報セキュリティ管理

監督指針では、保険会社に対して、情報資産を適切に管理するための内部管理態勢の整備を図り、他社における不正・不祥事件も参考に、情報セキュリティ管理態勢のＰＤＣＡ(注)サイクルによって継続的に改善を図ることを求めています（監督指針Ⅱ―３―１３―２―２（４））。

（注）社内規則等の策定（Ｐｌａｎ）、適切な教育・管理・指導（Ｄｏ）、自己点検等の監査（Ｃｈｅｃｋ）、改善に向けた態勢整備（Ａｃｔ）を指します。

ａ．情報資産を適切に管理するために、方針の策定、組織体制の整備、社内規程の策定をしているか。
ｂ．情報の機密性、完全性、可用性を維持するために、情報セキュリティに係る管理者を定め、その役割・責任を明確にした上で、管理しているか。
ｃ．コンピューターシステムの不正使用防止対策、不正アクセス防止対策、コンピューターウイルス等の不正プログラムの侵入防止対策等を実施しているか。

顧客の重要情報については、網羅的に洗い出したうえで重要度判定やリスク評価を実施し、そのリスクに応じた対策を講じる必要があります（監督指針Ⅱ―３―１３―２―２（４）⑤）。

ａ．保険会社が責任を負うべき顧客の重要情報を網羅的に洗い出し、把握、管理しているか。
ｂ．洗い出した顧客の重要情報について、重要度判定やリスク評価を実施しているか。
ｃ．それぞれの重要度やリスクに応じて、情報管理ルールを策定しているか。
・情報の暗号化、マスキングのルール
・情報を利用する際のルール
ｄ．顧客の重要情報について、不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。

不正に利用されることにより顧客に財産的損害が生じる可能性のあるクレジットカードやその他「機密情報」ついては、より厳格な取扱いをする必要があります（監督指針Ⅱ―３―１３―２―２（４）⑦～⑧）。

ａ．機密情報について、暗号化やマスキング等の管理ルールを定めているか。
ｂ．機密情報の保有・廃棄、アクセス制限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いをしているか。

また、情報資産については、管理ルール等に基づいて適切に管理されていることを定期的にモニタリングし、管理態勢を継続的に見直す必要があります。

さらに、セキュリティ意識の向上を図るため、全役職員に対するセキュリティ教育を行う必要があります（監督指針Ⅱ―３―１３―２―２（４）⑨）。

イ．サイバーセキュリティ管理

監督指針では、保険会社に対して、「金融分野におけるサイバーセキュリティに関するガイドライン」を踏まえた必要な態勢を整備することを求めています（監督指針Ⅱ―３―１３―２―２（５））。

例えば、インターネット等の通信手段を利用した非対面取引を行う場合には、取引に見合った適切な認証方法を導入することが考えられます（監督指針Ⅱ―３―１３―２―２（５）②）。

ａ．可変式パスワードや電子証明書などの固定式のＩＤ・パスワードのみに頼らない認証方式
ｂ．取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証
ｃ．ハードウエアトークン等でトランザクション署名を行うトランザクション認証(注)

（注）トランザクション認証とは、顧客が行った取引情報の内容が改ざんされていないことを確認し、実行する方法です。

また、インターネット等の通信手段を利用した非対面取引を行う場合には、業務に応じた不正防止対策を講じることが考えられます（監督指針Ⅱ―３―１３―２―２（５）③）。

ａ．取引時においてウイルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供
ｂ．利用者のパソコンのウイルス感染状況を保険会社側で検知し、警告を発するソフトの導入
ｃ．電子証明書をＩＣカード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用
ｄ．不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備

（３）代理店が被る損失

近年、ＩＴが普及し、個人情報の漏えいや、システム改ざん等により損失を伴う事故が増えています。代理店が被る損失として、次の具体例が挙げられます。

これらのリスクに適切に対応する観点から、代理店は、顧客等に関する情報管理態勢およびシステムリスク管理態勢を整備し、保険募集時等に取り扱う情報を適切に管理することが重要となります。

ア．経済的損失

代理店が、顧客情報や取引先から預かった機密情報等を漏えいした場合、善管注意義務違反や任務懈怠に基づく損害賠償請求といった経済的損失を被るおそれがあります。その他にもサイバー攻撃による不正利用やランサムウェア等による損失のおそれがあります。

イ．顧客の喪失と事業の停止

個人情報の漏えいやシステム改ざん等の事故を起こした代理店は管理責任が問われます。個人情報保護法等に違反する場合は行為者だけでなく事業者にも罰則が科せられるケースがあります。それだけでなく、社会的評価や顧客の信頼が低下します。

また、システム障害等によって事業継続に支障が生じるケースや、最悪の場合には、代理店の存続が危うくなるケースも想定されます。

ウ．代理店として取り組むべきこと

代理店は、情報管理態勢について明確な方針を示すとともに自ら実行していくために、リスク範囲を網羅し、組織的に対策を実施することが重要です。

また、委託先に提供した情報が漏えいした場合、委託元としての管理責任が問われます。そのため、委託先の情報管理も自店と同様に留意する必要があります。

上記を踏まえ、代理店は、日頃から募集人に向けて教育・指導を行い、理解を促していく必要があります。

代理店業務における情報管理の留意点

●代理店業務（各ステップ）における情報管理の留意点は次のとおり。

●顧客等に関する情報について、代理店は必要かつ適切な措置を講じる必要があります
●個人情報の取得にあたり、その利用目的を通知・公表、明示する必要があります。
●個人情報保護に関する基本方針（プライバシーポリシー）をお客さまに見えやすい場所に掲示することが挙げられます。

ステップ①　契約見込み客の発掘・募集人の権限等に関する説明

●見込み客情報についても、適正な取得・利用が必要となります。
●保険契約が満期を迎えるケースにおいて、乗合代理店で見積書を作成する場合は、お客さま情報を現契約保険会社以外の保険会社に提供することがあります。その際、見積もり提案の希望有無（お客さま情報の提供希望有無）について事前に確認し、適切な保険募集につなげる必要があります。

ステップ②　意向把握、商品の選定、商品説明および重要事項説明

●重要事項説明では､｢個人情報の取扱いに関するご案内｣等を用いて説明することが挙げられます。この場合には、その説明を行った証として「個人情報取扱同意欄」に個人情報の取扱いに関する同意の記録を取り付けるなどが必要となります。

ステップ③　契約締結（告知受領・意向確認）

●保険契約申込書等に記載した個人情報について、適切な取得・利用が必要となります。
●受領した告知事項について、機微情報が含まれる場合がありますので、取扱いに留意ください。

ステップ④　保険料の領収・申込書写等の交付

●銀行口座の情報やクレジットカードの情報は、不正利用された場合に経済的な損失に繋がりやすいことを踏まえ、取扱いに留意ください。

ステップ⑤　契約の管理・満期管理・満期案内

●代理店は、取得した情報の適切な削除等が必要となります。

1-2 個人情報の管理

個人情報の管理については、個人情報保護法を遵守することが大前提となります。ここでは、個人情報保護法で規定されている主な事項について解説します。

なお、個人情報保護法では「個人情報」を保護の対象としていますが、保険募集においては、法人情報を含む顧客等に関する情報の保護にも留意する必要があります。

（１）基本ルール

個人情報保護法は、個人情報の適正な取扱いに関して、個人情報を取り扱う事業者が遵守すべき義務等を定めたものです。

参考　個人情報保護の関係法令等

代理店は、個人情報保護法の遵守が必要であるほか、金融庁が策定した「金融分野における個人情報保護に関するガイドライン」「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」や「保険会社向けの総合的な監督指針」「代理店委託契約書」等についても遵守する必要があります。

ア．対象となる個人情報等（用語の定義）

個人情報	①生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む） ②身体の一部の特徴をコンピュータのために変換した文字、番号、記号等の符号、および、サービス利用や個人に発行されるカードその他の書類において割り当てられた文字、番号、記号等の符号（個人識別符号） ・顔認識、声紋、指紋、静静脈認証データ　等 ・公的な番号（運転免許証番号、マイナンバー、旅券番号等（注１））
個人データ（注２）	個人情報を含む情報の集合体であって、特定の個人情報を検索できるように体系的に整理したものを「個人情報データベース等」といい、それを構成する個人情報

（注１）証券番号、電話番号、クレジットカード番号等は個人識別符号に該当しません。

（注２）2024 年 4 月 1 日に施行された「個人情報保護法施行規則」その他ガイドラインの一部改正により、安全管理措置について、個人情報取扱事業者が取得し、または取得しようとしている個人情報であって、当該個人情報取扱事業者が個人データとして取り扱うことを予定しているものも含まれるとされています（通則ガイドライン３－４－２）。具体的には、代理店ホームページの問い合わせページなどが第三者により改ざんされ、窃取された問い合わせページへの入力された個人情報などが該当します。

イ．対象となる事業者

代理店は、個人情報保護法の個人情報取扱事業者に該当するため、個人情報保護法に則った個人情報の取扱いが求められるのみならず、保険業務の適正な運営や契約者保護の観点および所属保険会社から個人情報の取扱いの委託を受けた者として、個人情報保護の関係法令等に則った個人情報の取扱いが求められます。また、所属保険会社の規定等に従って対応する必要がありま

そのうえで、お客さまの意向に沿った情報の取り扱い（お客さま情報の適切な管理）も求められます。

ウ．法令上の罰則等

個人情報保護法に違反して不適切な個人情報の取扱いを行った場合には、個人情報保護委員会が必要に応じて違反行為の中止その他違反を是正するために必要な勧告・命令の措置をとることができます。当該勧告・命令に従わなかった場合には１年以下の懲役、または、100 万円以下の罰金に処されます。（個人情報保護法 178 条）。

☞関連 check☞

個人情報保護法については、個人情報保護委員会のホームページ（https://www.ppc.go.jp/）を参照してください。

（２）解説

ア．対象となる個人情報

（ア）代理店が取り扱う個人情報の種類

代理店が取り扱う個人情報の種類としては、例えば次のようなものがあります。

ａ．お客さま等（注１）の氏名を含む情報

ｂ．生年月日、連絡先（住所・居所・電話番号・電子メールアドレス（注２））、会社における職位または所属に関する情報について、それらと本人の氏名を組み合わせた情報

ｃ．上記ａ、ｂに付随しお客さま等が契約申込書等に記載した保険契約の締結に必要な情報（注３）

（注１）「お客さま等」とは、契約者のほか、被保険者、同居の親族、団体保険等の加入者、契約見込み客、事故の際に当事者となった被害者および加害者、法定相続人、代理人、法人代表者、法人担当者等が含まれます。

（注２）特定の個人を識別できる電子メールアドレスの場合は、それが単独でも個人情報となります。例えば、氏名が分かるようなメールアドレスの場合が挙げられます。

（注３）特定の個人を識別できる情報が記載されていなくても、代理店として個人が特定できる場合には個人情報に該当します。例えば、自動車の登録番号や証券番号単独の情報であっても、代理店端末などにより、特定の個人を識別することができる場合がありますので、個人情報保護法に則った対応が重要です。

（イ）個人情報が含まれる帳票等

個人情報が含まれる帳票や業務利用機器等[注1・2]として、例えば次のようなものがあります。

（注 1）「機器」とは、「端末」に加えて、端末周辺機器やＵＳＢメモリやメモリカードなどの外部記憶媒体、ファイルサーバ（ＮＡＳなど）も含みます。「端末」とは、パソコン、タブレット、スマートフォン、携帯電話等を指します。

（注２）「機器等」とは、機器に加えて、システム、メールサービスまたはその他外部サービス（クラウドストレージ等）を指します。

ａ．契約申込書、保険料領収証（写）
ｂ．事故関係書類一式、事故受付記録簿
ｃ．収支明細書などの事務関係書類
ｄ．個人情報の表示された端末画面のハードコピー等各種アウトプット・データ

イ．個人情報取扱事業者の義務

代理店は個人情報の漏えい等の防止その他の安全管理のために、必要かつ適正な措置を講じなければなりません。

なお、ここでいう安全管理措置上の個人データには、代理店が取得し、また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うことを予定しているものも含みますので、留意ください。

☞関連 check☜

代理店が講ずべき安全管理措置の対象となる個人情報については、上記「１－２（１）ア．対象となる個人情報等（用語の定義）」を参照ください。

代理店が講ずべき安全管理措置	解説・例示等
組織的安全管理措置	
・個人データの管理責任者および 個人データ管理者の設置	個人データ管理責任者とは、個人データの安全管理に関する業務遂行の総責任者です。個人データ管理者とは、個人データを取り扱う各部署における責任者です。 また、代理店の規模に応じ、個人データの取扱いの点検・改善等の監督を行う部署や合議制の委員会を設置してください。
・個人データ取扱者情報の保管	個人データ取扱者の氏名・役職・部署名等について、書面・リストを作成・保管する等の方法により、常に確認できる状態にしてください。
・個人情報保護に関する基本方針の策定 および公表	個人情報保護に関する基本方針（プライバシーポリシー）には次の項目を記載する必要があります。 ・関係法令等の遵守 ・安全管理のために講じた措置（基本方針、規律の整備、組織的・人的・物理的・技術的措置の内容） ・利用目的 ・目的外利用の禁止 ・適切な苦情処理 ・利用目的の通知・公表等の手続き ・開示等の手続き ・質問、苦情窓口 また、お客さまに見えやすい場所（ホームページ、店頭等）に掲示してください。
・個人データの安全管理に係る取扱規程の整備	取扱規程は、定めるだけでなく、備え置いたうえで、遵守してください。 ・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 ・漏えい等事案への対応の段階に係る取扱規程
・個人情報の漏えい（注１）等の対応に関する 体制整備	個人情報の漏えい、滅失、毀損等があった場合，直ちに所属保険会社に報告することも含めたルールを定めて代理店内で周知・徹底してください。
・個人データ管理台帳等の作成・更新	個人データ管理台帳には次の項目を記録する必要があります。 ・取得項目（氏名、住所、電話番号等の項目） ・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
・点検・監査の実施	点検・監査においては、具体的には、個人データ管理台帳等に記載されている内容（例：契約見込み客リスト、満期リスト等）の保管・管理状況の点検や、従業者にチェックリスト等による点検を実施してください。
人的安全管理措置	
・個人データの非開示契約等の締結・ 就業規則等の整備	すべての従業者と個人データの非開示契約を締結してください。非開示契約とは、個人データを許可なく第三者に開示しない旨を約束する契約です。
・個人情報保護に関する定期的な社内教育や 研修の実施	具体的には、次に掲げる措置を講じてください。 ・従業者に対する採用時の教育および定期的な研修 ・個人データ管理責任者および個人データ管理者に対する教育・研修 ・個人データの安全管理に関する就業規則等に違反した場合の懲戒処分の周知 ・従業者に対する教育・研修の評価と定期的な見直し

物理的安全管理措置	
・個人データを取り扱う区域の管理	施錠可能なロッカー等への個人情報の含まれる書類や業務利用機器（注２）の保管や外出時・退出時の施錠は、遵守すべきルールとして整備されている必要があります。
・業務利用機器の盗難防止の実施	
・個人情報の含まれる書類や業務利用機器を持ち運ぶ場合の漏えい等防止の実施	業務上必要最小限の情報に限定し、常時携帯する等のルールを設定する必要があります。
・個人データの削除および業務利用機器等の廃棄	保管期間終了後の個人情報（電子記録媒体を含む）について、シュレッダー処理・溶解処理等の適切な方法で確実に廃棄するルールを定めて社内教育を通じて徹底してください。
技術的安全管理措置	
・個人データへのアクセス制限およびアクセス者の管理	アクセス権限は必要な範囲内に制限してください。 また、台帳等を使って、業務利用機器等（注３）のユーザーＩＤの管理を行ってください。 ・ユーザーＩＤは利用者ごとに個別に設定し、業務分担に応じてアクセス制御を実施してください。ユーザーＩＤを共有する場合は、利用している従業者の特定、退職等により共有している従業者が利用しなくなった場合のパスワード変更を徹底してください。また、定期的に共有パスワードを変更することを徹底してください。 ・従業者の入退社や異動に伴う、ＩＤの追加・削除を適切に行う体制を構築してください。
・外部からの不正アクセスや、漏えい等の防止の情報セキュリティ対策 ☞関連check☞ 「１－３ 情報セキュリティ管理」も参照ください。	従業者と、サイバー攻撃の脅威に対する認識を共有するとともに、次のような対策を講じてください。 ・パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等による本人認証の強化 ・情報資産の保有状況の把握と、インターネットとの接続制御装置へのセキュリティパッチの迅速な適用 ・メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内への周知 ・サーバ等における各種ログの確認 ・通信の監視・分析やアクセスコントロールの再点検 ・データ消失等に備えて、データのバックアップの実施および復旧手順の確認 ・インシデントを認知した際の対処手順の確認、対外応答や社内連絡体制等の準備 ・保険業務に使用するパソコンへのファイル共有ソフトのインストール禁止 ・保険業務に使用するパソコンへのウイルス対策ソフトのインストール徹底と常に最新版への更新など

（注１）漏えいとは個人情報が外部に流出すること、滅失とは個人情報の内容が失われること、毀損とは個人情報の内容が意図しない形で変更されたり、内容を保ちつつも利用不能な状態にされたりすることを指します。

（注２）「機器」とは、「端末」に加えて、端末周辺機器やＵＳＢメモリやメモリカードなどの外部記憶媒体、ファイルサーバ（ＮＡＳなど）も含みます。「端末」とは、パソコン、タブレット、スマートフォン、携帯電話等を指します。

（注３）「機器等」とは、機器に加えて、システム、メールサービスまたはその他外部サービス（クラウドストレージ等）を指します。

（ア）個人情報の利用目的の通知・公表・明示

代理店は、個人情報を取得する場合は個人情報の利用目的をできる限り特定して、所属保険会社の規程等に従ってお客さまへ利用目的を通知・公表・明示する必要があります。

お客さまに対して個人情報の利用目的や保険会社による共同利用など、個人情報の取扱いに関する説明を行わなければなりません。

そして、その説明を行った証として「個人情報取扱同意」欄にお客さまの同意の記録を取り付けるなど、所属保険会社の規定等に従って対応する必要があります。

具体的には次のような方法があります。書面等で個人情報を取得する際は、お客さまへ個人情報の利用目的を明確に示す、「明示」が必要となります。

・通知：チラシ、郵送、ファックスおよび電子メールの送信等
・公表：ホームページへの掲載、代理店事務所内等の見やすい場所への掲示
・明示：会社案内、パンフレット（重要事項説明書）等へ記載し、利用目的が記載されている旨を説明

なお、代理店のホームページに利用目的を掲載する等して公表していることだけをもって「明示」しているとはいえませんので留意してください。

☞関連 check☜

乗合代理店がお客さま情報を取得する際の利用目的の説明については、下記「１－２（３）ア.（ア）乗合代理店～お客さま情報を取得する際の利用目的の説明～」を参照ください。

参考　個人情報の共同利用

代理店は、特定の者で個人情報（保険会社の個人情報は除く）を共同利用する場合（例えば同一の企業グループに属する他の代理店等との間で個人情報を共同して利用する場合）には、利用する者の範囲、責任者等を予め、本人の知り得る状態とすれば、当該提供先は「第三者」に当たらず、本人の同意は不要とされています。

本人の知り得る状態とは、本人が知ろうとすれば時間的にも、その手段においても、容易に知ることができる状態をいいます。具体的には、自店ホームページ等に継続的に掲載することや、自店の窓口等への掲示・備付けなどが考えられます。

なお、代理店が保険会社から取扱いを委託されている個人データに関しては、共同利用を行うことができません。万が一、利用する場合には、所属保険会社に事前に確認してください。

また、代理店以外にも次のような共同利用が挙げられます。

ａ.保険会社の企業グループ内での共同利用

ｂ．業界内の共同利用（注１）

ｃ．国土交通省との共同利用（注２）

（注１）詳細は、各保険会社のホームページおよび損保協会のホームページ（https://www.sonpo.or.jp/about/guideline/kyodoriyou/index.html）、損害保険料率算出機構のホームページ（https://www.giroj.or.jp/about/privacy/utilize_1.html）をご確認ください。

（注２）詳細は、国土交通上のホームページ（https://www.mlit.go.jp/privacy.html）をご確認ください。

（イ）個人情報の適正な取得

代理店が個人情報を取得する場合としては、例えば次のような場合があります。

なお、偽り等の不正な手段で個人情報を取得すること、および、違法または不当な行為を助長し、または誘発するおそれがある方法により個人情報を利用することは禁止されています。

ａ．本人が保険契約申込書等の書面（電磁的記録を含みます）に直接記載した個人情報を取得する場合
ｂ．アンケート等（注１）により見込客情報を取得し、保険商品等を勧める場合
ｃ．取得した個人情報について代理店独自の利用目的を有する場合（注２・３）

（注１）アンケート等とは、例えばアンケート票、保険設計書、保険契約成約前の帳票等が含まれます。
（注２）保険募集にかかる利用目的との混同が生じないように代理店独自の利用目的を通知・公表・明示する必要があります。例えば、同一の書面を用いて、保険会社と代理店それぞれの利用目的を通知・公表・明示する場合は、保険会社と代理店の利用目的をお客さまが混同・誤認しないように明確に区分させること、保険募集において個人情報を取得する場合は、利用目的を「明示」すること等に留意してください。
（注３）☞関連check☞　下記「参考　保険会社の個人情報・代理店の個人情報について」を参照ください。

参考　保険会社の個人情報・代理店の個人情報について

保険募集のために取得した個人情報は、委託元の「保険会社の個人情報」となる一方で、以下の情報は「代理店の個人情報」となります。

ａ．保険募集以外の業務（例えば兼業代理店における他の業務）のために取得した情報
ｂ．本人が特に代理店止まりであることを明示して代理店あてに提供した個人情報

代理店は、保険会社から取扱いを委託されている個人情報については、保険会社が定めるルールに従い取り扱わなければなりません。一方で「代理店の個人情報」については、代理店が自らの責任で、本人に通知・公表・明示した利用目的に従って利用することができます。

（ウ）個人情報の適正な利用

個人情報は利用目的の範囲内でのみ利用してください。万が一、利用目的以外での利用を行う場合には、本人の同意（原則として書面による）をあらためて取得する必要があります。

また、次の情報を取り扱う場合は特に留意する必要があります。

①機微（センシティブ）情報

機微（センシティブ）情報とは、要配慮個人情報（人種・信条・社会的身分・病歴・犯罪の経歴・犯罪被害の事実、その他本人に対する不当な差別、偏見、不利益が生じないように配慮が必要な情報）と、要配慮個人情報に該当しない労働組合への加盟、門地、本籍地、保健医療および性生活に関する情報などを含む個人情報であり、特に慎重な取扱いが求められます。

機微（センシティブ）情報は、原則として取得・利用または第三者提供することができません（注）。例外として、あらかじめ本人の同意を得たうえで、業務遂行上必要な範囲で取得・利用または第三者提供することが認められていますが、取得した情報の取扱いには極めて慎重な姿勢が求められます。

なお、当該個人情報が機微（センシティブ）情報であるか否かにかかわらず、個人情報の第三者提供を行う場合には、個人情報保護法上、本人の同意を取得する必要があります。

また、機微（センシティブ）情報は、オプトアウトの対象外であることに留意してください。

（注）意図せず機微（センシティブ）情報が記載された書類等を受領したような場合は、マスキングを行うなどして、不要な機微（センシティブ）情報を取得しないようにしてください。

②クレジットカード情報の取扱い

クレジットカード情報（カード番号、有効期限等）を含む個人情報は、情報が漏えいした場合、不正使用によるなりすまし購入など二次被害が発生する可能性が高いことから、厳格な管理が求められます。

具体的には、以下のような措置を講じる必要があります。

ａ．クレジットカード情報等について、利用目的その他の事情を勘案した適切な保存期間を設定し、保存場所を限定し、保存期間経過後適切かつ速やかに廃棄

ｂ．業務上必要とする場合を除き、クレジットカード情報等をコンピュータ画面に表示する際には、カード番号を全て表示させない等の適切な措置

ｃ．クレジットカード情報等の取扱いを第三者に委託する場合は、代理店を含む外部委託先において、クレジットカード情報等を保護するためのルールおよびシステムが有効に機能しているかについて、定期的または随時に、点検または立入検査の実施

ｄ．クレジットカード情報等の取扱いを第三者に委託する場合における委託先等の事業者の十分な監督

③マイナンバー（個人番号）の取扱い

「行政手続における特別の個人を識別するための番号の利用等に関する法律」（以下「番号法」）に基づき、2016年１月から、マイナンバー（個人番号）の利用が開始されました。

番号法では、個人情報保護法よりも厳格な情報保護措置が求められており、法令で定められた手続き（社会保障、税、災害対策）以外でマイナンバー（個人番号）を利用することは禁止されています。募集人は、お客さまの同意がある場合であっても、支払調書を作成する目的以外でお客さまのマイナンバー（個人番号）を収集・利用してはいけません。

また、意図せずマイナンバーカードを本人確認書類として提示された場合には、マイナンバーを復元できないようにマスキングを行うなどして、適切に管理してください。

兼業代理店の場合は、保険業務以外でマイナンバー（個人番号）を取り扱う場面も想定されます(注)。この場合は、プライバシーポリシー等の改定など、適切な措置を講じてください。

（注）マイナンバー（個人番号）の取扱いに関する具体的な対応等については、所属保険会社の指示に従ってください。

（エ）個人情報の開示請求

本人から保有個人データについて開示、訂正または利用停止等を求められた場合、原則として、遅滞なく所属保険会社に取り次いだうえで、開示、訂正または利用停止等を行わなければなりません。個人情報保護法に基づく開示等請求に関しては、従来の契約照会や事故処理状況照会の位置づけとは別の受付方法を定め、当該方法によるかどうかは請求者本人に選択していただくものとしています。

また、保険契約者等からの通常の契約照会や事故処理状況の照会は、個人情報保護法上の開示等の請求には当たらず、代理店において照会者の本人確認等を適正に行ったうえで回答することが必要となります。

（注）代理店独自の保有個人データに関しては、代理店自らが個人情報保護法に基づき対応しなければなりません。

（オ）情報漏えい発生時等の対応

代理店において個人情報の漏えい等が生じた場合、またはそのおそれが高い場合、次のような対応を行う必要があります。

ａ．直ちに所属保険会社（注）に報告する。

（注）個人情報が記載・収録された帳票や業務利用機器の盗難または紛失、郵便物の誤送付、電子メールやファックスの誤送信等の事故が生じた場合には所属保険会社に報告する必要があります。

ｂ．代理店が保険会社に報告をする際、以下の事項を報告する。

情報漏えい発生時等の保険会社への報告事項（例）

・事故の内容（盗難・紛失・その他）
・事故発生日時および事故発生場所
・事故当事者
・事故経緯・状況
・漏えいした物件内容（帳票や業務利用機器等の種類）
・漏えいした個人情報の件数
・警察への届出の有無

（カ）個人情報の廃棄・削除

個人データの保存期間については契約終了後一定期間内とする等、保有する個人データの利用目的に応じて保存期間を定め、定めた期間を経過した個人データを消去する必要があります。

（キ）解約・廃業する代理店および退職する役員・使用人における個人情報の取扱い

代理店は、「委託契約書」「守秘義務に関する誓約書」廃業時に保険会社と締結する念書等によって、次の守秘義務を果たす必要があります。

・保険会社から提供を受けた、個人情報が記載・収録された帳票や業務利用機器等を、保険会社の指示により返却または廃棄・消去等しなければなりません。なお、代理店が独自に代理店システムを開発・運用している場合も、代理店委託契約書に定める守秘義務条項に基づき、過去データの削除が必要となります。

・廃業後も個人情報を正当な理由なく他に漏らしてはいけません。

また、代理店は、役員・使用人が退職する場合は、次の措置を講じる必要があります。

ａ．退職する役員または使用人が所持する個人情報が記載・収録された帳票や業務利用機器等を返却または廃棄・消去等させること
ｂ．退職する役員または使用人が付与された個人データへのアクセス権限を遮断するため、ＩＤを削除等すること
ｃ．退職する役員または使用人が退職後も個人情報を正当な理由なく他に漏らすことのないよう、例えば、代理店の就業規則等や退職時の念書の取り交わし等によって、守秘義務を課すといった措置を講じること

ウ．個人情報の第三者提供

（ア）第三者提供の制限

代理店は、委託契約書において守秘義務を負っており、お客さまの情報その他業務上知り得た事項を第三者に提供することは禁止されています。そのため、第三者に個人情報を提供する場合には、所属保険会社の承認を得てください。

また、次の事項を示したうえで、あらかじめ本人の同意（原則として書面による）を取得する必要があります。

ａ．個人情報を提供する第三者の氏名・名称
ｂ．第三者における個人情報の利用目的
ｃ．第三者に提供される情報の内容

ただし、代理店が委託先に個人情報を提供する場合には、第三者提供の例外として本人の同意は不要となりますが、所属保険会社の承認は必要となります。また、委託先の選定等、外部への委託には一定のルールを遵守する必要があります。

参考　個人情報の第三者提供に該当しないケース

個人情報が外部に提供されているが、第三者提供には該当しないケースとして、個人情報保護法上、以下の３つの類型が認められています。

ａ．委託先への提供

代理店が大量の個人情報（データ）のデータ処理やダイレクトメールの作成またはデータの保管、廃棄などについて、外部の専門事業者に委託することが合理的な場合があります。しかし、保険会社の承認なしに、代理店が個人情報の取扱いを外部事業者等に委託することは認められません。

（注）「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」に基づき、代理店が個人情報の取扱いを外部事業者等に委託する場合も、委託契約における安全管理に関する内容として、委託先の個人データ取扱者の氏名・役職又は部署名を委託契約へ盛り込むこと等が考えられます。

ｂ．特定の者との共同利用

代理店が同一の企業グループに属する他の代理店等との間で個人情報を共同して利用するケースなどをいいますが、一定の要件を充足する必要があります。

☞関連check☞

個人情報の共同利用については、上記「１－２（２）イ．参考 個人情報の共同利用」を参照ください。

ｃ．代理店の合併等に伴う提供

代理店の合併や営業譲渡によって他の代理店に保険業務が継承される場合、保険契約者などの個人情報が継承代理店に移管されます（他の代理店への業務の継承は保険会社の承認が必要です）。

個人情報の取扱いについても、従来の取扱い代理店と保険契約者等本人の関係は新たな代理店に引き継がれます。代理店は、合併や営業譲渡にあたり、保険契約者に対してその旨通知します。

（イ）第三者提供時の確認・記録・保存義務

個人情報保護法では、個人データを第三者へ提供する場合は、個人データの提供者と受領者それぞれに所定の記録作成、保存義務が課せられています（受領者においては、取得の経緯等を確認する必要があります）。

一方で、例外適用も設けられており、代理店の実務においては、個人データの第三者提供について、業務委託先との授受や、本人に代わって（本人からの依頼により）提供する場合、生命・身体・財産の保護のために必要である場合等は記録・保存義務の適用除外となります。

したがって、記録・保存義務が課されるのは、本人同意により第三者提供する場合およびオプトアウト（注）を利用して個人データを第三者提供する場合等となります。

また、第三者からの取得についても、受領者にとって個人データに該当しない場合や、単に閲覧する行為などは、確認・記録・保存義務の適用除外となります（個人データに該当しない単体の個人情報の授受も対象外）。

（注）本人の求めに応じて第三者の提供を停止すること、個人情報保護委員会に届け出たうえで公表を行うこと等の要件を満たした個人情報保護法上に定められた手続きのこと。要件を満たせば、本人の同意がなくとも第三者提供が可能ですが、厳しい要件が求められています。

■個人データの第三者提供を行う場合に記録が必要な項目

	提供年月日	第三者の氏名等	本人の氏名等	個人データの項目	本人の同意
本人同意による第三者提供		○	○	○	○
オプトアウトによる第三者提供	○	○	○	○	

■個人データを第三者から取得する場合に確認・記録が必要な項目

	提供を受けた年月日	第三者の氏名等	取得の経緯	本人の氏名等	個人データの項目	保護委員会による公表	本人の同意
本人同意による第三者提供		○	○	○	○		○
オプトアウトによる第三者提供	○	○	○	○	○	○	
私人からの第三者提供		○	○	○	○		

参考　外国にある第三者への個人データの提供

外国にある第三者に個人データを提供するにあたっては、次のいずれかに該当する場合を除き、あらかじめ、外国にある第三者への個人データの提供を認める旨の本人の同意を得なければなりません。

ａ．当該第三者が、我が国と同等の水準にあると認められる個人情報保護制度を有している国・地域として個人情報保護委員会規則で定める国・地域にある場合

ｂ．当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として個人情報保護委員会規則で定める基準に適合する体制を整備している場合

ｃ．法令に基づく場合、人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき等、個人情報保護法第27条第1項各号に該当する場合

なお、個人情報保護法にて、第三者に該当しないとされている、委託先、事業継承、共同利用のケースであっても、上記事項が適用されることに留意が必要です。

エ．個人情報の外部委託

（ア）外部業者に委託する場合の取扱い

ａ．所属保険会社への事前申請

保険業務に係る個人データを代理店の外部（クラウドサービスを含む）に委託[注]する際には、外部委託先を選定のうえ、所属保険会社に対し事前に申請する必要があります。また、外部委託先が再委託を行う場合も同様に、所属保険会社に申請等を行ってください。

なお、個人データの外部委託にあたり、委託内容によっては、外部委託先が募集行為を行ってしまう（無登録・無届募集や保険募集の再委託となる）おそれもありますので、外部委託の可否を所属保険会社に必ず事前に確認してください。

（注）ここでの「委託」とは、契約の形態や種類を問わず、他の者に個人データの取扱いの全部または一部を行わせることを内容とする契約のことをいいます。

ｂ．外部委託先の管理

外部委託を行った場合、外部委託先が、上記ａ．で所属保険会社への事前申請時に定めた選定基準や契約内容[注]を遵守しているか、個人データを適切に取り扱っているか、定期的に確認する必要があります。

（注）委託者（代理店）の監督・監査・報告徴収に関する権限等を盛り込んだ委託契約書を締結してください。

（３）留意点

ア．代理店の属性に応じた留意点

（ア）乗合代理店～お客さま情報を取得する際の利用目的の説明～

乗合代理店においては、取り扱う保険契約が満期を迎える際に、保険料の比較見積もりのために引受保険会社とは異なる他の保険会社にお客さまのご契約内容等を提供し見積書の作成を行う場合（保険会社から提供される代理店システムを利用して代理店が保険料試算をする場合を含む）があります。このお客さま情報の取扱いは代理店から保険会社への「委託」[注]であり、個人情報保護法上の情報漏えいには該当しません。しかしながら、お客さまの意向に反し他社保険契約を見積もることは望ましいとはいえません。

したがって、保険料見積もりに際しては、見積もり提示よりも前にお客さまが代理店に提供したご自身の情報が既契約の引受保険会社以外の保険会社に提供されることを丁寧に説明し、お客さまの理解を得ることが顧客保護の観点で必要となります。

（注）ここでいう「委託」は個人情報保護法上の委託を指します。

ａ．お客さまへの利用目的等の説明

乗合保険会社各社の比較見積もり実施時にお客さまの個人情報を取得するときは、見積もりを実施する前に、お客さまに以下の５点に関する説明を行い、お客さまの理解を得る必要があります。

（注）お客さま情報の提供については、所属保険会社の独占禁止法に関する規定等に従ってください。

① 利用目的：代理店で定める個人情報の利用目的を説明します。
② 保険見積もりのために代理店から保険会社にお客さまの情報を提供すること。
③ 自店は、複数の保険会社の保険募集を受託している代理店であり、お客さまに対して保険契約が満期を迎える際に、自店と取引のある他の保険会社の商品を案内する場合があること。また、この案内のため、見積書・保険設計書等の作成を目的として、他の保険会社に対して、お客さまの情報を提供することがあること。（保険会社名：比較見積もりを行う保険会社の名称）
④ 提供を受けた保険会社でのお客さま情報の取扱い：提供を受けた保険会社は、当該お客さま情報を試算以外の目的では使用しないこと、適切な安全管理措置を講じていること。
⑤ 提供を希望しない場合のお申し出の要請：特定の保険会社へお客さま情報の提供をご希望されない場合には、自店にお申し出を頂きたいこと。ただし、誘導や誹謗中傷にならないよう、お客さまから申し出がある場合の対応であることを十分留意してください。

また、代理店は上記対応をすべての募集人に義務付けるルール整備等を行い、定期的に徹底されているか確認してください。

ｂ．お客さまが情報提供を希望しない場合

お客さまが特定の保険会社への情報提供を希望しない場合には、その内容を記録し、お客さまの意向に反した取扱いとならないように、お客さま情報を管理してください。

参考 見積もり実施に関するお客さま情報管理の方法（例）

代理店での事業実態に応じて、メーカーシステムや個社の顧客管理システムなどを活用したり、Excel等の表計算ソフトで台帳　（以下イメージ）を作成して管理したりすることも考えられます。（契約締結時の意向把握とは違い、乗合保険会社を横断した管理です。）

No.	拠点	担当者名	説明日	お客様氏名	お客さまコード（代理店独自）	既契約保険会社（他代理店情報含む）	既契約保険証券番号（他代理店情報含む）	見積を希望しない保険会社名
1								
2								
3								
4								
5								

（イ）兼業代理店～他業取引による取得した情報の取扱い～

保険募集等により取得した個人情報を保険代理業以外の事業に利用する場合には、所属保険会社の利用目的とは別に、利用目的を定めて明示しなければなりません。

なお、実際の運用にあたっては代理店委託契約書に定める守秘義務や保険契約の維持・管理義務等に留意する必要があります。

・代理店が他の事業において取得した個人情報を保険募集に用いることを利用目的で通知・公表・明示していない場合、その個人情報を保険募集に用いる際には、あらためて本人の同意（原則として書面による。）を取得する必要があります。
・逆に、代理店が保険代理業において取得した個人情報をその他の事業に用いることを利用目的で通知・公表・明示していない場合、その個人情報をその他の事業に用いる際には、あらためて本人の同意（原則として書面による。）を取得する必要があります。
・商品・サービスの内容（例：損害保険、生命保険、投資信託等）については、可能な限り特定し記載することが必要です。

イ．契約の特性に応じた留意点

（ア）団体契約

団体（企業、組合、会員組織等）が保有する構成員の個人データを募集準備のために代理店あるいは保険会社（以下「代理店等」）に提供することや、代理店等が加入データを団体に提供することについては、それぞれの場面ごとに、代理店等と団体との間の委託や第三者提供の関係を整理したうえで対応する必要があります。

ａ．団体契約（任意加入）の場合

団体契約（任意加入）の場合は、以下のとおり整理します。

①団体が保険料を試算するために個人データを代理店等へ提供する場合

この場面では、団体が第三者である代理店等に個人データを提供（以下「第三者提供」）したものと考えます。

本人の同意取得については、団体あるいは構成員の財産の保護のために必要（個人データを提供しなければ、契約締結の判断ができず、契約が成立しない等）との観点から、個人情報保護法第 27 条第１項第２号により、本人の同意を取得する必要はないものと整理します。

したがって、第三者提供時・取得時の確認・記録義務については、団体・代理店等ともに、必ずしも確認・記録は必要ではありません。

②団体が、被保険者ごとの設計書・加入依頼書（プレプリント帳票）等を作成するために、当該団体の構成員（役員、従業員、組合員等）の個人データ（本人、家族の性別、生年月日など）を代理店等へ提供する場合

この場面では、団体から代理店等への「委託」もしくは「第三者提供」(注) による対応となります。この「委託」と「第三者提供」については、個人情報保護法上での整理に違いがあり、団体での対応や義務が異なりますので、メリット・デメリットを検討いただいたうえで、団体の希望により対応方針を決めることとなります。

なお、損保業界では、「委託」により対応するケースが多いと考えられますが、その場合の注意点は、以下のとおりです。

（注）☞関連check☞　上記「１－２（２）ウ．個人情報の第三者提供」を参照ください。

団体が構成員のために行う福利厚生業務の一部を、当該団体が代理店等に委託したものと考えます。代理店等は委託された範囲でしか個人情報を利用できないため、社内で十分に周知する必要があります。

また、団体は代理店等に対し、個人情報保護法第 25 条に定める委託先の監督にかかる措置を講じなければならないことになります。実務上は以下の対応が考えられます。

・代理店等が団体から個人データの取扱いの委託を受けること、提供される個人データは委託元が定め、本人に通知された利用目的の範囲内であること、およびその安全管理を図るための合意事項について、団体と代理店等との間で共有します。
・委託元の団体の監督に従って、委託先である代理店等は個人データの取扱状況について定期的に点検等を行い、委託元である団体の求めに応じてその結果を報告します。

なお、個別の点検を行うことに代えて、契約更改時の打合せの際等において、団体と代理店等との間で合意事項の確認を行うことを団体に提案することも考えられます。

一方で、「第三者提供」により対応する場合は、第三者提供時の確認・記録義務が団体・代理店等ともに課されますので、必要に応じた適切な対応が必要となります。

③契約申込時に、団体が被保険者の加入依頼書等の個人データを代理店等へ提供する場合

この場面では、被保険者が契約者である団体に対し、加入を依頼していると考えられ、本人に代わって提供していると整理できるため、必ずしも同意取得は必要ではなく、また、団体・代理店等ともに、確認・記録義務の対象外です。

ｂ．団体契約（全員加入）の場合

団体契約（全員加入）の場合は、以下のとおり整理します。

団体が保険料を試算するため、構成員の個人データを代理店に提供する場合、団体が契約の申し込みに至り、構成員の個人データを代理店に提供する場合のいずれも、団体から代理店への第三者提供に該当すると整理します。

本人の同意取得については、団体あるいは構成員の財産の保護のために必要（個人データを提供しなければ、契約締結の判断ができず、契約が成立しない、あるいは全員加入の契約が成立しないことによって、団体および構成員に不利益が生じる）との観点から、個人情報保護法第 27 条第１項第２号により、本人の同意を取得する必要はないものと整理します。

なお、準記名式付保等においては契約時のデータ提供はないものの、事故発生時には保険会社による名簿の閲覧等があります。この場合は、個人情報保護法第２７条第１項第２号に該当するとし、仮に同意のない第三者提供がなされても、法的な問題はないと整理します。

（イ）代理店間分担契約

代理店間分担契約を取扱う代理店は、本人に通知・公表・明示した保険会社および代理店の利用目的の範囲内で個人情報を取扱う必要があります。

また、代理店間分担契約を取扱う代理店が本人に通知・公表・明示した利用目的の範囲外で個人情報を利用する場合には、その個人情報を取得する際に当該代理店が自ら本人に対してその利用目的を通知・公表・明示する必要があります。取得する際に利用目的が通知・公表・明示されていない場合には、あらためて本人の同意（原則として書面による。）を取得する必要があります。

なお、保険会社との委託契約上の守秘義務もありますので、保険会社に事前に対応を確認してください。

1-3 情報セキュリティ管理

万が一、お客さまの個人情報等を漏えいさせてしまうと、漏えいした情報が悪意の第三者によって悪用されるおそれがあります。このような事故が発生してしまった場合、代理店はお客さまからの信頼を損なうだけでなく、事故対応にかかる費用の負担や、業務の停滞等といった様々な不利益を被ることになります。

このため、代理店はお客さまの情報等を守るため、情報漏えい事故を未然防止として情報セキュリティ対策が求められます。また、お客さまの情報のほかに、代理店が守るべき情報として、自社重要情報である「経営情報」や「従業員情報」「取引先・委託先情報」等が挙げられます。

☞関連 check☞

個人情報については、上記「１－２（２）ア.（ア）代理店が取り扱う個人情報の種類」を参照ください。

参考　サイバーセキュリティ対策の必要性

近年では、代理店がサイバー攻撃を受け、その結果としてお客さまの個人情報や顧客情報が漏えいする事例も発生しています。これらの情報が漏えいしてしまった場合、被害の拡大を防止するために事業を停止しなければならない状況となることも想定されます。

このため、代理店においてもサイバーセキュリティ対策を講じる必要があります。具体的な対策としては、次のような対応が挙げられますが、サイバー攻撃は日々巧妙化しているため、対策について定期的にＰＤＣＡを行うことが重要です。

特に、実際にサイバー攻撃を受けた場合や個人情報・顧客情報の漏えい等が発生した場合の対応は、コンティンジェンシープランとして定めておく必要があります。

■具体例

・　募集人が使用するパソコンなどの端末にかかる管理規程の整備
・サイバーセキュリティ対策に関する担当部署の設置や各種規程整備
・サイバーセキュリティに関する研修や自己点検の実施
・標的型攻撃メール対策訓練の実施
・コンティンジェンシープランの策定

（１）基本ルール

ア．マルウェア感染の防止

マルウェアとは、悪意のある不正なプログラム全般を指します。情報や金銭を奪うために、マルウェアを用いて様々なサイバー攻撃を仕掛けてくることがあります。マルウェアの感染経路には、自分自身でマルウェアを実行して感染してしまうケースと、脆弱性を悪用されて感染してしまうケースがあります。

【マルウェア感染の具体例】

概要	対策
・標的型攻撃メールの添付ファイル・ＵＲＬリンクや、ダウンロードファイル、ＵＳＢメモリ等から感染	・不要なファイルやＵＲＬリンク、Ｗｅｂサイトは開かない ・ＯＳやソフトウェアを最新にする ・ウイルス対策ソフトを使用する ・推測されにくいパスワードを使用する ・組織に許可されていない行為は行わない
・罠が仕掛けられた不正なＷｅｂサイトの閲覧による感染 ※企業の公式Ｗｅｂサイトが改ざんされて罠が仕掛けられる場合もある	
・同一ネットワーク経由で他のパソコンから感染	

イ．情報漏えい発生時等の対応

万が一、マルウェアに感染してしまった場合の対応として、具体的には次のようなものがあります。被害拡大防止のため、事前に対応手順を作成して手順どおりに対応できるか確認することが望ましいといえます。

・ネットワークから遮断する（無線ＬＡＮをオフ、ＬＡＮケーブル抜栓　等）
・パソコンの電源は切らずに、操作しないようにする
・代理店責任者・所属保険会社に速やかに報告する

参考　ランサムウェアについて

メールの添付ファイルやＵＲＬ、改ざんされたホームページの閲覧によりウイルス感染したり、サーバやネットワーク機器の脆弱性を突かれたりして、サーバ、パソコン内のデータを暗号化して使用不能にします。その解除と引き換えに金銭を要求してくる不正プログラムのことをランサムウェア（「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語）といいます。そのため、個人データの保存にあたっては、外部ネットワークとの通信制御機能を整備し、外部のインターネットと内部ネットワークの境界に設置するネットワーク機器にて、必要な通信のみに制限すること等が考えられます。

（２）解説

代理店は個人情報の漏えい防止やマルウェア感染防止のため、次のような対策を講ずる必要があります。

ア．業務利用機器（パソコン等）のセキュリティ対策

（ア）業務利用機器

代理店の業務で利用する端末・機器等の私的利用、および、個人利用機器等の業務利用は行わないでください（注）。端末・機器等は、ＯＳやソフトウェアを最新の状態にアップデートし、ウイルス対策、外部からの不正アクセス対策を実施してください。

また、パスワード等のセキュリティ設定や、定期的なバックアップを行うことも重要です。特に個人情報にアクセスできる端末・機器等については、強固な認証（パスワード）を設定してください。

特に、個人情報を保存する機器は限定したうえで、個人情報へのアクセス履歴を取得し、必要な期間（できるだけ長めに（１年以上が望ましい））保管してください。

（注）やむを得ず利用する場合は、ルールに則ったパスワード設定やセキュリティ対策を実施すること等、セキュリティルールを確保する旨、誓約書等を用いて代理店内で管理者を明確にし、責任を持って徹底してください。

（イ）無線ＬＡＮ（Ｗｉ－Ｆｉ）

自宅や事務所において、代理店業務で利用する業務に無線ＬＡＮを使用する場合は、暗号化設定（注１）を行い、ＯＳやソフトウェアを最新の状態にアップデートしてください。

提供元が明確でない、または暗号化とパスワードの設定が設定されていない無線ＬＡＮは利用しないでください（注２）。

（注１）暗号化方式は、ＷＰＡ２またはＷＰＡ３を使用し、できるだけランダムで長いパスワードを設定してください。

（注２）具体的にはカフェ、駅、空港等のＷｉ－Ｆｉは原則接続しないでください。

（ウ）ユーザーＩＤ・パスワード

ユーザーＩＤは利用者ごとに個別のＩＤを取得し、ユーザーＩＤ・パスワードの共有は原則行わないでください。個人情報にアクセスできる業務利用機器は所属保険会社の規定等に従い、強固なパスワード設定を行ってください。

また、機器やサービスが対応している場合は、原則として二要素認証機能を利用してください。

イ．業務利用ソフト（アプリ等）のセキュリティ対策

（ア）メールおよびチャットアプリ

メールを送信するときは、個人情報は必要最低限とし、宛先、添付ファイル等をよく確認[注]し、誤送信に留意してください。大量の個人情報をメールで送信するときには、添付ファイルは強固なパスワード設定を行い、パスワードを本文には記載せずメール以外の方法（口頭、書面、ＳＭＳ等）で通知するなどの対策を実施してください。

（注）複数人で複数回の確認を行う体制を整備することが有効です。

＜留意事項＞

乗合代理店の場合、お客さま情報を含むファイルを送付する際は、送付先以外の保険会社の契約情報が含まれていないか 確認（特に、Excelファイルの場合は複数のシート、行や列の非表示等まで確認）し、代理店管理者を宛先等に含めることや、パスワードの設定等、代理店所定の送信ルールに従って対応してください。

また、代理店業務において取り扱うお客さま情報をはじめとする顧客等に関する情報をメールで送受信する場合は、メールシステムにおいて TLS1.2 以上の暗号通信を用いることを必須としてください。

なお、フリーメールおよびフリーチャットは原則利用しないでください。万が一、フリーメールを業務利用する場合には、誓約書等を用いて代理店内で利用する従業者を把握したうえ、パスワード設定等に加え、フリーメールで提供されているセキュリティ対策の設定を行ってください。

サイバー攻撃の一つである標的型攻撃メールの開封を未然に防止するため、不用意に添付ファイルを開いたり、ＵＲＬリンクをクリックしたりしないように、日頃から差出人のアドレス等を確認してください。

参考　標的型攻撃メールの対策

標的型攻撃メールとは、業務上の連絡や重要そうな情報を装った悪意のあるメールを指します。万が一、添付ファイルを開いたり、ＵＲＬリンクをクリックしたりすると、それらに仕込まれていたウイルスにパソコンが感染するおそれがあります。ウイルスはパソコンからお客さま情報等の重要情報を盗み出すほか、社内や他のパソコンにも広がり、多くの情報が盗まれてしまうこともあります。

（イ）Ｗｅｂ会議アプリ

Ｗｅｂ会議アプリを使用して会議や顧客面談等を主催する場合には、会議に参加するためのパスコード（パスワード）を設定のうえ、待機室（ロビー）での参加者確認機能、参加者の事前登録機能などの機能を活用してください。

招待メールを受けて参加する場合には、送信元を十分に確認ください。会議中は、画面共有時に個人情報や重要情報等が映りこまないように留意してください。

（ウ）クラウドサービス

お客さまの個人情報または、お客さまとのやり取りにクラウドサービスを利用するにあたっては、次の点を確認ください。

ａ．不正アクセス等に対して十分なセキュリティを確保できること（具体例：ＩＰアドレス規制や二要素認証、危険な機能の無効化、利用履歴の記録など）
ｂ．クラウド事業者に対し、事故情報の開示や再発防止等の協力を得られること
ｃ．所属保険会社から、保険業務での利用を認められているサービスであること

また、所属保険会社の規定等に従い、外部業者に委託する場合の対応が必要となります。

☞関連 check☜

外部業者に委託する場合の対応については、上記「１－２（２）エ.（ア）外部業者に委託する場合の取扱い」を参照ください。

ウ．代理店ホームページの公開

代理店ホームページを公開する場合には、稼働するサーバにウイルス対策ソフトの導入等の適切なセキュリティ対策を行い、定期的に安全性チェックを実施してください。

ホームページが稼働するサーバ等への具体的なセキュリティ対策は次のようなものがあります。

ａ．ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状況に保つ。
ｂ．インターネット上での盗聴や改ざんを防止するため、お客様に個人情報を入力いただくページ遷移の通信（https）では、TLS1.2以上による暗号化を設定する。
ｃ．ホームページ管理用パソコンに適切なセキュリティ対策を実施する。また、組織外から遠隔操作でホームページの管理・メンテナンスを実施する場合、安全なアクセスを確保する（アクセスするＩＰアドレスを制限する等）。
ｄ．スマートフォン等のモバイルアプリを構築・運用する場合についてもホームページと同様の管理を行う。
ｅ．ホームページからの「情報漏えい」「他システムへの攻撃の踏み台化」「改ざん」等の被害を防ぎ、お客様情報等の適切な管理を行う。その対応策として、具体的には以下等の対策を講じることを推奨する。
・ホームページのサーバを代理店で構築・運用している場合、脆弱性診断（セキュリティ上の欠陥の発見）を「新規構築や変更の都度」「定期的」に実施する。特に個人情報を持つ「ページ」および「モバイルアプリ」については、定期的な脆弱性診断を通常よりも高い頻度で行う。検出された脆弱性の指摘事項について、リスクに応じて適切に対処する。
・外部のサーバでホームページを構築・運用している場合、当該サーバが脆弱性診断を受け、検出された脆弱性の指摘事項についてリスクに応じて適切に改善対応がなされているサービスを利用し、構築したホームページについては上記を実施する。

エ．ＳＮＳの利用

代理店の業務においてＳＮＳは原則利用しないでください。万が一、ＳＮＳを業務利用する場合には所属保険会社に確認のうえ、私用アカウントとは切り離し、電話番号等を使い分けるとともに、不適切な内容の投稿はしないでください。

メッセージの送信等を行う場合は、お客さまの承諾有無を踏まえるとともに、誤送信に留意し、また、用済みとなったメッセージ履歴はこまめに削除してください。アカウントの乗っ取り等のスミッシングによる被害に留意する必要があります。

オ．テレワークをする場合の対応

テレワークを実施する場合は、情報セキュリティに関する社内規則等を定めてください。第三者に情報を漏えいすることがないように、パソコンの画面や声量に留意ください。

また、情報の持ち出しは業務上必要最小限のものに限定して管理し、不要になった際には事務所で破棄してください。テレワーク中に起きた事故についても、直ちに所属保険会社に報告してください。

参考　生成ＡＩサービスの利用に関する注意

近年では、生成ＡＩサービスが普及しており、個人情報保護委員会から「生成ＡＩサービスの利用に関する注意喚起等について」（https://www.ppc.go.jp/files/pdf/230602_kouhou_houdou.pdf）が公表されています。個人情報の漏えいのおそれや、著作権侵害のおそれ、誤った情報の提供に繋がるおそれがあると考えられます。

このため、保険募集および契約管理等において、生成AIサービスを利用する場合は十分留意する必要があります。具体的な取扱いは、所属保険会社に確認ください。

参考資料

代理店および募集人の情報管理態勢の整備にかかる参考資料として各チェックリストや取扱規定等の雛形を掲載していますので、適宜ご確認ください。なお、詳細は所属保険会社にご確認ください。

【１－１】個人情報の取扱いにかかる代理店点検チェックリスト（代理店向け）
【１－２】個人情報の取扱いにかかる代理店点検チェックリスト（従業者向け）
【２】個人情報保護に関する基本方針（プライバシーポリシー）
【３－１】保険代理店業務に係る個人情報取扱規程
【３－２－１】取得・入力段階における取扱規程
【３－２－２】利用・加工段階における取扱規程
【３－２－３】保管・保存段階における取扱規程
【３－２－４】移送・送信段階における取扱規程
【３－２－５】消去・廃棄段階における取扱規程
【３－２－６】漏えい事案等への対応の段階における取扱規程
【３－３】個人データの取扱状況の点検及び監査に係る規程
【３－４】個人データの外部委託に係る規程

参考資料【１－１】

個人情報の取扱いにかかる代理店点検チェックリスト（代理店向け・雛形）

代理店名		点検実施日	年　月　日
代理店登録番号		点検責任者	印

No	チェック項目	回答
1	個人情報保護に関する基本方針（プライバシーポリシー）をホームページへの掲載や店頭等への掲示により公表していますか。	はい・いいえ
2	個人データの安全管理に係る取扱規程を定め、備え置いていますか。	はい・いいえ
3	個人データ管理責任者および個人データ管理者を設置していますか。 また、代理店の規模（注1）に応じ、個人データの取扱いの点検・改善等の監督を行う部署や合議制の委員会を設置していますか。	はい・いいえ
4	個人データ管理台帳等を作成し、更新していますか。	はい・いいえ
5	すべての従業者（注2）と個人データの非開示契約等を締結していますか。	はい・いいえ
6	個人データ取扱者の氏名等を常に確認できる状態にしていますか。	はい・いいえ
7	第三者に個人データを提供したとき、提供先の氏名等の記録を作成し、一定期間保存する体制を整備していますか。 また、第三者から個人データの提供を受けたとき、提供元や個人データの取得経緯等を確認した記録を作成し一定期間保存する体制を整備していますか。	はい・いいえ
8	外国にある第三者に個人データを提供するときは、あらかじめ、外国にある第三者への個人データの提供を認める旨の本人の同意を得る体制を整備していますか。	はい・いいえ
9	機微（センシティブ）情報の取得・利用は業務上必要な範囲に限定し、特に慎重に取り扱うようルールを定めていますか。	はい・いいえ
10	乗合代理店の場合、見積書作成のため、顧客が提供した自身の個人情報を保険会社に提供することについて、あらかじめ丁寧に説明し、顧客の理解を得るようにルールを定めていますか（利用目的は、プライバシーポリシーで公表しているだけでは足りず、顧客に明示する必要がある）。	はい・いいえ
11	従業者（注2）に対して、個人情報保護に関する定期的な社内教育や研修、必要に応じたフォローアップを実施していますか。	はい・いいえ
12	外出時・退社時、個人情報の含まれる書類や業務利用機器（注3） は、施錠可能なロッカー等に保管し、施錠するルールを定めていますか。	はい・いいえ
13	所属保険会社の代理店向け商品説明ハンドブック・引受規定等、「社外秘」等の記載がある秘密管理性が高い情報や、兼業代理店においては代理店業以外の業務に関わる情報等が社外に流出させない体制を構築していますか。	はい・いいえ
14	個人情報の含まれる書類や業務利用機器を保険会社（または代理店自ら）が設定した管理区域外（注4） に持ち出すとき、常時携帯する等のルールについて社内教育を通じて徹底していますか。	はい・いいえ

参考資料【１－１】

15	個人データの取扱いを外部委託しようとするとき、所属保険会社に事前に申請して承認を受けていますか。	はい ・ いいえ
16	個人データの取扱いを外部委託するとき、委託先の適格性を確認し、所定の事項を盛り込んだ委託契約書を締結していますか。	はい ・ いいえ
17	個人データの取扱いを外部委託しているときは、委託先に対して十分な監督を行い、個人データが適切に管理されていることを定期的に確認していますか。	はい ・ いいえ
18	個人データへのアクセス権限を必要な範囲内に制限し、権限が付与された者と実際の利用者を確認する等、アクセス管理を徹底していますか（注 5）。特に、ユーザーID は個人ごとに設定していますか。	はい ・ いいえ
19	個人情報の漏えい、滅失、毀損等があった場合、直ちに所属保険会社に報告していますか。	はい ・ いいえ
	また、個人データの漏えい、滅失、毀損等を防止するため、定期的に点検・監査を実施していますか。	はい ・ いいえ
20	保険業務に使用し、個人情報にアクセスできる業務利用機器等については、所属保険会社の規定等に従い、強固なパスワードの認証を設定するルールを定めていますか。	はい ・ いいえ
	また、機器やサービス等が対応している場合は、原則として二要素認証機能（注6）を利用していますか。	はい ・ いいえ
21	フリーメールの業務利用は原則禁止とすることにしていますか。やむを得ず利用を認める場合、誓約書等を用いて代理店内で利用する従業者を把握したうえで、対策（注7） を講じていますか。	はい ・ いいえ
22	テレワークを実施する場合、情報セキュリティに関する社内規則等を定めていますか（注8） 。	はい ・ いいえ
23	オンラインによる会議や顧客面談等を実施する場合、情報漏えい、サイバー攻撃等のセキュリティリスクに十分注意する必要があることを社内教育を通じて徹底していますか。	はい ・ いいえ
24	個人情報の漏えい、滅失、毀損等が発生した際の報告ルールを定め、社内に周知徹底する体制を整備していますか。	はい ・ いいえ
25	保管期間終了後の個人情報（電子記録媒体を含む）について、シュレッダー処理・溶解処理等の適切な方法で廃棄するルールを定めていますか。	はい ・ いいえ
26	不要なデータを定期的に削除・廃棄することを社内教育を通じて徹底していますか。	はい ・ いいえ
27	個人情報の含まれる業務利用機器を廃棄するときは、データの削除や破棄を確実に行うルールを定め、管理していますか。	はい ・ いいえ
28	下記事項について、誓約書等を用いて従業者に周知徹底していますか。 （ア）業務利用機器等をプライベート目的で利用することを原則禁止する。 （イ）従業者が個人で所有する機器等を代理店業務に利用することは原則禁止する。	はい ・ いいえ
29	持ち出し可能な業務利用機器について、セキュリティ対策上のルールを設定していますか。	はい ・ いいえ
30	無線LAN（Wi-Fi）を利用するときは、提供元が明確で、暗号化とパスワードの設定が行われている無線LANに接続するルールを定めていますか（注9）。	はい ・ いいえ

参考資料【１－１】

31	業務利用機器等には十分なセキュリティ対策（注10） を実施していますか。	はい ・ いいえ
32	（ホームページの構築・運用をしている場合、）ホームページには適切なセキュリティ対策（注11） を実施していますか。	はい ・ いいえ
33	サイバー攻撃への備えとして、サイバーセキュリティ対策の強化を図り、セキュリティ対策（注12） を実施する体制を整備していますか。	はい ・ いいえ

（注1）対応が必要となる規模の１つの目安として、保険業法施行規則第236 条の2（規模が大きい特定保険募集人）に定められる代理店が該当すると考えられます。

（注2）「従業者」とは、個人情報取扱事業者の組織内にあって直接又は間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業者（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、事業者との間の雇用関係にない者（取締役、執行役、理事、監査役、監事、派遣社員等）も含まれます。

（注3）「機器」とは、「端末」に加えて、端末周辺機器や USBメモリやメモリカードなどの外部記憶媒体、ファイルサーバ（NASなど）も含みます。「端末」とは、パソコン、タブレット、スマートフォン、携帯電話等を指します。

（注4）「管理区域外」の範囲については、保険会社の指導や代理店独自のルールによります。

（注5）以下を行う体制を構築し、台帳等を使って、業務で利用する機器等のユーザーIDの管理を行ってください。なお、「機器等」とは、機器に加えて、システム、メールサービスまたはその他外部サービス（クラウドストレージ等）を指します。

- ユーザーID は利用者ごとに個別に設定し、業務分担に応じてアクセス制御を実施してください。ユーザーID を共有する場合は、利用している従業者の特定、退職等により共有している従業者が利用しなくなった場合のパスワード変更を徹底してください。また、定期的に共有パスワードを変更することを徹底してください。
- 従業者の入退社や異動に伴う、ID の追加・削除を適切に行う体制を構築してください。

（注6）不正ログイン対策として、二つの段階を経る認証方式である「二段階認証」や、複数の要素を用いた認証方式である「二要素認証」などが提供されています。「要素」とは、認証に用いる情報の種類を指し、大きく3つに分類できます。①記憶認証…ユーザーが知っていること（パスワードや秘密の質問など）②所持認証…ユーザーが持っているもの（電子証明書、ICカード、パスワード生成器など）③生体認証…ユーザーの身体的特性（指紋、静脈、虹彩、顔、掌紋、筆跡など）。二段階認証かつ二要素認証の主な例としては、ID/パスワードの認証後に、登録済の電子メールアドレスに通知されるワンタイムパスワードを入力する方式があります。ただし、サービスやシステムによっては、異なる呼称をすることがあります。

（注7）強固なパスワードの認証設定、原則として二要素認証の実施、不必要なメールの削除、フリーメールで提供されているセキュリティ対策（アクセス制限等）の設定をいいます。

（注 8）社内規則等には、以下のような事項を含めてください。

- 個人情報、重要情報、業務利用機器を事務所外に持ち出したり、個人所有機器を業務に利用したりするときは、必要な社内手続きを経ること。
- 個人情報、重要情報、業務利用機器を事務所外に持ち出してテレワークに利用するときは、業務上必要最小限のものに限定するとともに、常時管理下に置き、車中等に放置しないものとすること。
- テレワーク中に情報セキュリティに関する事故が発生した場合、直ちに所属保険会社に報告すること。
- テレワークで使用する業務利用機器には覗き見防止フィルターを使用して、情報が第三者に漏えいしないようにすること。また、テレワークをしている近くに第三者がいるときは、その場所から移動するなどの覗き見防止対策を行うこと。さらに、会議中や面談中に必要以上に大声になって個人情報や重要情報が第三者に漏えいすることのないように注意すること。
- テレワークのときに使用した、個人情報や重要情報の記載された書類を廃棄するときは、原則として代理店事務所での裁断破棄とすること。

（注9）暗号化方式は、WPA2またはWPA3を使用し、できるだけランダムで長いパスワードを設定してください（旧来からあるWEPとWPAの方式は、解読される危険性等が判明しており、安全ではありません。）。

参考資料【１－１】

（注 10）以下のようなセキュリティ対策を実施してください。

・業務利用機器は、暗号化、パスワード設定等のアクセス制御できる機器を選定し、アクセス制御を設定する。また、ウイルス対策、外部からの不正アクセス対策を実施する。

・外部サービスを利用してデータ保存をする場合、クラウドサービスは、不正アクセス等に対して十分なセキュリティを確保し、事故情報の開示、再発防止等の協力を得られるサービスを選定する（フリーのクラウドストレージサービスは、これら協力を期待できないため、禁止とする。）。また、「二段階認証または二要素認証」を利用できるサービスを選定し、設定する。

・個人データを保存する機器を限定したうえで、個人データへのアクセス履歴を取得し、必要期間（できるだけ長めに（1年以上が望ましい））保管する。

・業務利用機器の OS、ブラウザのサポート期限を確認し、サポート期限内のバージョンを適用する。

（注11）ウイルス対策ソフトの導入と最新の定義ファイルの保持、個人情報入力ページはTLS1.2以上による暗号化設定、ホームページ管理用パソコンの適切なセキュリティ対策と組織外からの遠隔操作による安全なアクセス確保、モバイルアプリによる構築・運用もホームページの取扱いと同じ、ホームページからの情報漏えい、他システムへの攻撃の踏み台化、改ざん等の被害防止による顧客情報の適切な管理など。

（注 12）以下のようなことが対策として挙げられます。

・パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等による本人認証の強化

・情報資産の保有状況の把握と、インターネットとの接続制御装置へのセキュリティパッチの迅速な適用

・電子メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内への周知

・サーバ等における各種ログの確認

・通信の監視・分析やアクセスコントロールの再点検

・データ消失等に備えて、データのバックアップの実施および復旧手順の確認

・インシデントを認知した際の対処手順の確認、対外応答や社内連絡体制等の準備

・保険業務に使用するパソコンへのファイル共有ソフトのインストール禁止

・保険業務に使用するパソコンへのウイルス対策ソフトのインストール徹底と常に最新版への更新　など

以 上

参考資料【１－２】

個人情報の取扱いにかかる代理店点検チェックリスト（従業者向け・雛形）

代理店名		点検実施日	年　月　日
被点検者名		点検責任者	印

No	チェック項目	回答
1	個人情報を不正に取得したり、本人の同意なく、利用目的の達成に必要な範囲を超えて取り扱ったりしていませんか。	はい ・ いいえ
2	乗合代理店の場合、見積書作成のため、顧客が提供した自身の個人情報を保険会社に提供することについて、あらかじめ丁寧に説明し、顧客の理解を得ていますか（利用目的は、プライバシーポリシーで公表しているだけでは足りず、顧客に明示する必要がある）。	はい ・ いいえ
3	契約締結の際、契約申込書や申込書お客さま控え等に記載されている「個人情報の利用目的」等を契約者に明示していますか。	はい ・ いいえ
4	第三者に個人データを提供したときは、提供先の氏名等の記録を作成し、一定期間保存していますか。 また、第三者から個人データの提供を受けたときは、提供元や個人データの取得経緯等を確認した記録を作成し、一定期間保存していますか。	はい ・ いいえ
5	外国にある第三者に個人データを提供するときは、あらかじめ、外国にある第三者への個人データの提供を認める旨の本人の同意を得ていますか。	はい ・ いいえ・ 提供はない
6	保険業務に使用し個人情報にアクセスできる業務利用機器等（注1）については、所属保険会社の規定等に従い、強固なパスワードの認証を設定していますか。	はい ・ いいえ
	また、機器やサービス等が対応している場合は、原則として二要素認証機能(注2)を利用していますか。	はい ・ いいえ
7	保険業務用のパソコンを使用する際には、他の者とは起動時パスワードまたはログインパスワード等を共有せず、独自のパスワードを設定していますか。	はい ・ いいえ
8	フリーメールを業務に利用していませんか。やむを得ず利用するときは、以下のセキュリティ対策を講じていますか。 （ア）前記5の強固な認証を設定する。（必須） （イ）「原則として二要素認証」（注1）を実施する。（必須） （ウ）不必要なメールを削除する。（必須） （エ）フリーメールで提供されているセキュリティ対策（アクセス制限等）の設定を行う。（強く推奨）	はい ・ いいえ
9	保険業務に使用するパソコンにファイル共有ソフトをインストールしていませんか。	はい ・ いいえ
10	保険業務に使用するパソコンにウィルス対策ソフトをインストールし、常に最新の状態にしていますか。	はい ・ いいえ
11	個人情報の含まれる書類や業務利用機器を管理区域外（注3） に持ち出すとき、管理簿等で持ち出し状況を記録していますか。 また、管理区域内、外にかかわらず持ち出す個人情報は、訪問先の個人情報に限定する等、業務上必要最小限のものに限定していますか。 さらに、車内に放置して車から離れたり、電車等の網棚に載せたりすることなく、常時携行していますか。	はい ・ いいえ

参考資料【１－２】

12	テレワーク（注4）をするときは、取扱者以外が容易に個人情報を閲覧できない措置（注5）を講じていますか？	はい ・ いいえ
13	オンラインにより会議や顧客面談を行う場合、招待メールを受けたときは送信元確認をし、また主催するときは参加者や顧客の本人確認をしていますか。	はい ・ いいえ
14	個人情報を郵送等で送付したり、ファックスや電子メールで送信したりする場合、宛先および送付物に誤りがないかの確認を行っていますか。	はい ・ いいえ
15	顧客情報付きファイルを送付するときは、送付先以外の保険会社の契約情報が含まれていないか確認（特に、Excelファイルの場合は複数のシート、行や列の非表示等まで確認）し、代理店管理者を宛先等に含めることや、パスワードの設定等、代理店所定の送信ルールに従って対応していますか。	はい ・ いいえ
16	外出時・退社時、個人情報の含まれる書類や業務利用機器は、施錠可能なロッカー等に保管し、施錠していますか。	はい ・ いいえ
17	外出時や退社時には事務室の施錠を行っていますか。	はい ・ いいえ
18	機微（センシティブ）情報の取得・利用は、業務上必要な範囲に限定し、特に慎重に取り扱っていますか。	はい ・ いいえ
19	お客さま等外部からの照会等に対応する場合は、照会者等に応じて本人の確認や保険会社に確認したうえで、対応していますか。	はい ・ いいえ
20	保管期間終了後の個人情報（電子記録媒体を含む）について、シュレッダー処理・溶解処理等の適切な方法で廃棄していますか。	はい ・ いいえ
21	個人情報の漏えい、滅失、毀損等が発生した場合、直ちに代理店の責任者に報告していますか。	はい ・ いいえ
22	以下の要領で不要なデータを定期的に削除・廃棄していますか。 （ア）電子メール等データ保存期間の定めのないものについては、代理店内で定めたルールに従いデータを削除・廃棄する。 （イ） データ保存期間（用済廃棄含む）を越えたものは速やかに削除・廃棄する。	はい ・ いいえ
23	個人情報の含まれている業務利用機器の廃棄時のデータ削除を確実に行っていますか。	はい ・ いいえ
24	業務利用機器等のプライベート目的での利用や個人所有機器等の業務利用を行っていませんか。（注6）	はい ・ いいえ
25	無線 LAN（Wi-Fi）を利用するときは、提供元が明確で、暗号化とパスワードの設定が行われている無線LANに接続していますか。	はい ・ いいえ
26	受信した電子メールについて、身に覚えがなかったり、不審に感じたりしたとき、開いたりしていませんか。また、添付ファイルを不用意に開いたり、URLを不用意にクリックしたりしていませんか。	はい ・ いいえ

（注１）「機器」とは、「端末」に加えて、端末周辺機器や USB メモリやメモリカードなどの外部記憶媒体、ファイルサーバ、（NAS など）も含みます。「端末」とは、パソコン、タブレット、スマートフォン、携帯電話等を指します。「機器等」とは、機器に加えて、システム、メールサービスまたはその他外部サービス（クラウドストレージ等）を指します。

（注２）不正ログイン対策として、二つの段階を経る認証方式である「二段階認証」や、複数の要素を用いた認証方式である「二要素認証」などが提供されています。「要素」とは、認証に用いる情報の種類を指し、大きく３つに分類できます。①記憶認証…ユーザーが知っていること（パスワードや秘密の質問など）②所持認証…ユーザーが持っているもの（電子証明書、IC カード、パスワード生成器など）③生体認証…ユーザーの身体的特性（指紋、静脈、虹彩、顔、掌紋、筆跡など）。二段階認証かつ二要素認証の主な例としては、ID/パスワードの認証後に、登録済の電子メールアドレスに通知されるワンタイムパスワードを入力する方式があります。ただし、サービスやシステムによっては、異なる呼称をすることがあります。

参考資料【１－２】

(注３)「管理区域外」の範囲については、保険会社の指導や代理店独自のルールによります。

（注４）「テレワーク」とは、在宅勤務、サテライトオフィス勤務もしくはモバイル勤務といった募集人が情報通信技術を利用して行う事業場外勤務のことを指すものとします。

（注５）以下のような措置をいいます。

- 個人情報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取り扱う。
- パソコンは、パスワード付きのスクリーンセーバーの起動またはコンピューターのロック等で閲覧できないようにする。
- 書類・媒体・携帯可能なパソコン等を机上等に放置しない。

(注６) 次のことを遵守する必要があります。

（ア）業務利用機器等をプライベート目的で利用していない。

（イ）従業員が個人で所有する機器等を代理店業務に利用していない（やむを得ず利用する場合は、ルールに則ったパスワード設定やセキュリティ対策を実施していますか。）。

以 上

参考資料【２】

個人情報保護に関する基本方針【プライバシーポリシー】（雛形）

当社は、個人情報保護の重要性に鑑み、また保険業に対するお客さまの信頼をより向上させるため、個人情報の保護に関する法律（個人情報保護法）、行政手続における特定の個人を識別するための番号の利用等に関する法律（番号法）その他の関係法令、関係官庁からのガイドライン、特定個人情報の適切な取扱いに関するガイドラインなどを遵守して、個人情報を厳正・適切に取り扱うとともに、安全管理について適切な措置を講じます。

当社は、個人情報の取扱いが適正に行われるように、従業者への教育・指導を徹底し、適正な取扱いが行われるよう取り組んでまいります。また、個人情報の取扱いに関する苦情・ご相談に迅速に対応し、当社の個人情報の取扱いおよび安全管理に係る適切な措置については、適宜見直し、改善いたします。

１．個人情報の取得・利用

当社は、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（個人番号および特定個人情報については、下記８．を参照ください。）を取得・利用します。

２．個人情報の利用目的

当社は、保険会社から保険募集業務[注]の委託をうけて、取得した個人情報（個人番号および特定個人情報については、下記８．を参照ください。）を当該業務の遂行に必要な範囲内で利用します。

専業 専属	当社における具体的な個人情報の利用目的は次のとおりであり、それら以外の他の目的に利用することはありません。 当社が取り扱う損害保険、生命保険およびこれらに付帯・関連するサービスの提供
専業 乗合	当社は複数の保険会社と取引があり、取得した個人情報を取引のある保険会社の商品・サービスをご提案するために利用させていただくことがあります。 当社における具体的な個人情報の利用目的は次のとおりであり、それら以外の他の目的に利用することはありません。 当社が取り扱う損害保険、生命保険およびこれらに付帯・関連するサービスの提供
兼業 専属	また、当社は〇〇業を営んでおり、当該業務の遂行に必要な範囲においても、取得した個人情報を利用します。 当社における具体的な個人情報の利用目的は次のとおりであり、それら以外の他の目的に利用することはありません。 ①（　　）（　　）（　　）およびこれらに付帯・関連するサービスの提供 ②当社が取り扱う損害保険、生命保険およびこれらに付帯・関連するサービスの提供

参考資料【２】

兼業 乗合	当社は複数の保険会社と取引があり、取得した個人情報を取引のある保険会社の商品・サービスをご提案するために利用させていただくことがあります。 また、当社は〇〇業を営んでおり、当該業務の遂行に必要な範囲においても、取得した個人情報を利用します。 当社における具体的な個人情報の利用目的は次のとおりであり、それら以外の他の目的に利用することはありません。 ①（　　）（　　）（　　）およびこれらに付帯・関連するサービスの提供 ②当社が取り扱う損害保険、生命保険およびこれらに付帯・関連するサービスの提供

（注）代理店への委託業務の内容に応じ、「保険業務」とすることも可。

上記の利用目的の変更は、相当の関連性を有すると合理的に認められている範囲にて行い、変更する場合には、その内容をご本人に対し、原則として書面（電磁的記録を含む。以下同じ。）などにより通知し、または当社のホームページ（　　）などにより公表します。

当社に対し保険業務の委託を行う保険会社の利用目的は、保険会社のホームページ（下記）に記載してあります。

・〇〇〇〇保険株式会社（　　）
・〇〇〇〇保険株式会社（　　）
・〇〇〇〇保険株式会社（　　）

３．個人データの安全管理措置

当社は、取り扱う個人データ（下記８．の個人番号および特定個人情報を含みます。）の漏えい、滅失または毀損の防止、その他個人データの安全管理のため、安全管理に関する取扱規程などの整備および実施体制の整備など、十分なセキュリティ対策を講じるとともに、利用目的の達成に必要とされる正確性・最新性を確保するための適切な措置を講じ、万が一、問題等が発生した場合は、速やかに適当な是正対策を行います。

当社は、個人データの安全管理措置に関する社内規程を別途定めており、その具体的内容は主として以下のとおりです。安全管理措置に関するご質問については、下記１３．のお問い合わせ窓口までお寄せください。

（１）基本方針の整備

個人データの適正な取扱いの確保のため、「関係法令・ガイドライン等の遵守」、「安全管理措置に関する事項」、「質問および苦情処理の窓口」等について本基本方針を策定し、必要に応じて見直しています。

（２）個人データの安全管理に係る取扱規程の整備

取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者およびその任務等についての規程を整備し、必要に応じて見直しています。

参考資料【２】

（３）組織的安全管理措置

・個人データの管理責任者等の設置

・就業規則等における安全管理措置の整備

・個人データの安全管理に係る取扱規程に従った運用

・個人データの取扱状況を確認できる手段の整備

・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

・漏えい等事案に対応する体制の整備

（４）人的安全管理措置

・従業者との個人データの非開示契約等の締結

・従業者の役割・責任等の明確化

・従業者への安全管理措置の周知徹底、教育及び訓練

・従業者による個人データ管理手続の遵守状況の確認

（５）物理的安全管理措置

・個人データの取扱区域等の管理

・機器及び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等の防止

・個人データの削除及び機器、電子媒体等の廃棄

（６）技術的安全管理措置

・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・毀損等防止策

・個人データへのアクセスの記録及び分析

・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

・個人データを取り扱う情報システムの監視及び監査

（７）委託先の監督

個人データの取扱いを委託する場合には、個人データを適正に取り扱っている者を選定し、委託先における安全管理措置の実施を確保するため、外部委託に係る取扱規程を整備し、定期的に見直しています。

（８）外的環境の把握

・個人データを取り扱う国における個人情報の保護に関する制度を把握した上で安全管理措置を実施しています。

参考資料【２】

（※外国における情報の取扱いがない場合は削除）

４．外国における情報の取扱い

当社は、個人データの取扱いを海外にある外部に委託するにあたって、以下の安全管理措置を講じるとともに、個人情報保護法で求められる、委託先における個人データの安全管理措置に相当する措置（以下、相当措置といいます）を義務付けた委託契約を委託先との間で締結しています。

（１）以下の項目について年に１回、定期的に書面等により確認を行っています。

①移転先の第三者による相当措置の実施状況

②移転先の第三者の所在する外国における相当措置の実施に影響を及ぼすおそれのある制度の有無

（２）相当措置の実施に支障が生じた際には、是正を求め、当該相当措置の継続的な実施の確保が困難となったときは、当該個人データの提供を停止します。

（３）委託契約では、委託契約の範囲内で個人データを取り扱う旨、必要かつ適切な安全管理措置を講じる旨、従業者に対する必要かつ適切な監督を行う旨、再委託が必要な場合の事前承諾、個人データの第三者提供の禁止等を定めています。

（４）海外にある外部への個人データの取扱いの委託に関するご質問については、下記１３．のお問い合わせ窓口までご連絡ください。

５．個人データの第三者への提供および第三者からの取得

（１）当社は、次の場合を除き、あらかじめご本人の同意なく第三者に個人データ（個人番号および特定個人情報については、下記８．を参照ください。）を提供しません。

①法令に基づく場合

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であって、本人の同意を得ることが困難であるとき。

③公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

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であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

⑤当該第三者が学術研究機関等である場合であって、当該第三者が当該個人データを学術研究目的で取り扱う必要があるとき（当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）。

（２）個人データを第三者に提供したとき、あるいは第三者から取得したとき（個人関連情報を個人データとして取得する場合を含みます。）、提供・取得経緯等の確認を行うとともに、提供先・提供者の氏名等、法令で定める事項を記録し、保管します。

参考資料【２】

（※個人関連情報の第三者への提供の取扱いがない場合は削除 ）

６．個人関連情報の第三者への提供

（１）当社は、法令で定める場合を除き、第三者が個人関連情報を個人データとして取得することが想定されるときは、当該第三者において当該個人関連情報のご本人から、当該情報を取得することを認める旨の同意が得られていることを確認することをしないで、当該情報を提供しません。

（２）当社は、法令で定める場合を除き、前項の確認に基づき個人関連情報を第三者に提供した場合には、当該提供に関する事項（いつ、どのような提供先に、どのような個人関連情報を提供したか、どのように第三者がご本人の同意を得たか等）について確認・記録します。

７．センシティブ情報の取扱い

当社は、要配慮個人情報（人種、信条、社会的身分、病歴、前科・前歴、犯罪被害情報などをいいます）ならびに労働組合への加盟、門地および本籍地、保健医療および性生活（これらのうち要配慮個人情報に該当するものを除く）に関する情報（センシティブ情報）については、次の場合を除き、原則として取得、利用または第三者提供を行いません。

（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）保険料収納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、利用又は第三者提供する場合

（６）相続手続を伴う保険金支払事務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、利用又は第三者提供する場合

（７）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センシティブ情報を取得、利用又は第三者提供する場合

８．個人番号および特定個人情報の取扱い

当社は、個人番号および特定個人情報について、法令で限定的に明記された目的以外のために取得・利用しません。また、番号法で限定的に明示された場合を除き、個人番号および特定個人情報を第三者に提供しません。

（※仮名加工情報の取扱いがない場合は削除）

９．仮名加工情報の取扱い

（１）仮名加工情報の作成

当社は、仮名加工情報（法令に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報）を作成する場合には、以下の対応を行います。

・法令で定める基準に従って、適正な加工を施すこと

・法令で定める基準に従って、削除した情報や加工の方法に関する情報の漏えいを防止するために安全管理措置を講じること

参考資料【２】

（２）仮名加工情報の利用目的

当社は、仮名加工情報の利用目的を変更した場合には、変更後の利用目的をできる限り特定し、それが仮名加工情報に係るものであることを明確にしたうえで、公表します。

（※匿名加工情報の取扱いがない場合は削除）

１０．匿名加工情報の取扱い

（１）匿名加工情報の作成

当社は、匿名加工情報（法令に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたもの）を作成する場合には、以下の対応を行います。

・法令で定める基準に従って、適正な加工を施すこと
・法令で定める基準に従って、削除した情報や加工の方法に関する情報の漏えいを防止するために安全管理措置を講じること
・作成した匿名加工情報に含まれる情報の項目を公表すること
・作成の元となった個人情報の本人を識別するための行為をしないこと

（２）匿名加工情報の提供

当社は、匿名加工情報を第三者に提供する場合には、提供しようとする匿名加工情報に含まれる個人に関する情報の項目と提供の方法を公表するとともに、提供先となる第三者に対して、提供する情報が匿名加工情報であることを明示します。

（※Cookie 等の識別子に紐づけされた情報の取扱いがない場合は削除　）

１１．Cookie 等の識別子に紐づけされた情報の取得・利用・提供

Cookie（クッキー）とは、ウェブサイトを閲覧した際に、ウェブサイトから送信されたウェブブラウザに保存されるテキスト形式の情報のことです。また、ウェブビーコンとは、ウェブページや電子メールに小さな画像を埋め込むことによって、お客様がそのページやメールを閲覧した際に情報を送信する仕組みです。本ウェブサイトでは、cookie、ウェブビーコンまたはそれに類する技術（以下「Cookie 等」といいます）を利用して、お客様の情報を保存・利用しています。

当社は、Cookie 等に保存された識別子を統計的に収集・分析することができるサービスとして、Google Inc.が提供する Google Analytics を利用しております。Google Analytics の Cookie による情報収集や情報の取り扱いについて、また、Google が提供するサービスのプライバシーポリシーについては、下記のサイトをご確認ください。

また、お客様は、オプトアウト用のブラウザーアドオンにより、Google Analytics からオプトアウトすることができます。

■Google Analytics

Google が提供するサービスでの Cookie による情報収集や情報の取扱いについて
（https://policies.google.com/technologies/partner-sites?hl=ja）

Google プライバシーポリシー
（https://policies.google.com/privacy?hl=ja）

Google Analytics からのオプトアウト
（https://tools.google.com/dlpage/gaoptout）

参考資料【２】

１２．個人情報保護法に基づく保有個人データの開示、訂正、利用停止など

専　業	個人情報保護法に基づく保有個人データ（上記８．の個人番号および特定個人情報を含みます。）に関する開示（確認・記録の開示を含む）、訂正または利用停止などに関するご請求については、データの保有者である保険会社に対してお取次ぎいたします。
兼　業	個人情報保護法に基づく保有個人データ（上記８．の個人番号および特定個人情報を含みます。）に関する開示（確認・記録の開示を含む）、訂正または利用停止などに関するご請求については、ご請求者がご本人であることを確認させていただいたうえで手続きを行います。保険会社や他社の保有個人データに関しては当該会社に対してお取次ぎいたします。当社の保有個人データに関し、必要な調査を行った結果、ご本人に関する情報が不正確である場合は、その結果に基づいて正確なものに変更させていただきます。 なお、上記開示などのお手続きについては所定の手数料をいただきます。手続きを希望される方は、下記お問い合わせ先までお申し付けください。

１３．お問い合わせ先

ご連絡先は下記のお問い合わせ窓口となります。また保険事故に関する照会については、下記お問い合わせ窓口のほか、保険証券記載の保険会社の事故相談窓口にもお問い合わせいただくことができます。

なお、ご照会者がご本人であることをご確認させていただいたうえで、ご対応させていただきますので、あらかじめご了承願います。

＜代理店名＞
＜住　　所＞
＜代表者氏名＞
＜電話番号＞
＜受付時間＞
＜E-mail＞
＜ホームページ＞

※当社からのＥメール、ダイレクトメール等による新商品・サービスのご案内について、ご希望されない場合は、上記のお問い合わせ先までお申し出ください。

以　上

●●年●月●日制定
■　■　■　■　■　（代　理　店　名）

参考資料【３－１】

20　年　月　日

保険代理店業務に係る個人情報取扱規程（雛形）

代理店名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

第１章　総則

第１条（目的）

本規程は、当代理店における保険代理店業務に係わる個人情報の適法かつ適正な取扱いの確保に関する基本的事項を定めることにより、個人の権利・利益を保護することを目的とする。

第２条（定義）

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」（以下「個人情報保護法」という。）、「行政手続における特定の個人を識別するための番号の利用等に関する法律」（以下「番号法」という）および関係省庁の個人情報保護に関するガイドラインによるものとする。

第３条（適用）

本規程は、当代理店の従業者（保険募集に従事するか否かを問わない。）に適用する。

第４条（個人情報の安全管理に係わる基本方針）

１．当代理店における個人情報の適法かつ適正な取扱いを確保するため、次の事項を含む個人情報の安全管理に係わる基本方針を定める。

（１）当代理店の名称
（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
（６）個人情報の利用目的

２．個人情報の安全管理に係わる基本方針は、当代理店の従業者に周知すると共に、当代理店のホームページへの掲載、事務所への掲示等により公表する。

第２章　管理体制

第５条（個人データ管理責任者）

１．当代理店は、【＿＿＿＿＿＿＿＿】を個人情報の安全管理に係わる業務遂行の総責任者（個人データ管理責任者）とする。

２．個人データ管理責任者は、次に掲げる業務を所管する。

（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「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）その他当代理店における個人データの安全管理に関すること

参考資料【３－１】

＝代理店において個人データ取扱部署が単一の場合＝

３．前項（２）に定める個人データ管理者は、個人データ管理責任者が兼務することができる。

４．第２項（２）に定める本人確認に関する情報の管理者は、個人データ管理者が兼務することができる。

第６条（個人データ管理者）

個人データ管理者は、次に掲げる業務を所管する。

（１）個人データ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

第７条（点検・監査の実施）

１．個人データ管理責任者は、別に定める個人データの取扱状況の点検及び監査に係わる規程に基づき、個人データの取扱いに関する法令及び諸規定の遵守状況に関する点検または監査の実施計画を立案し、個人データ取扱部署毎に点検または監査を定期的に実施させる。

２．点検の実施責任者は当該取扱部署の個人データ管理者とし、点検結果を個人データ管理責任者へ報告する。

３．監査の実施責任者は当該取扱部署以外の個人データ管理者とし、点検結果を個人データ管理責任者へ報告する。

第８条（体制の見直し）

個人データ管理責任者は、前条の点検または監査の結果を踏まえ、必要に応じて個人データの取扱いに関する組織体制の見直しを行わなければならない。

第９条（秘密の保持）

保険会社の保険業務の委託を受けて取得した個人情報または個人データについて、委託契約の継続中および委託契約終了後も、法令又は行政当局により求められる場合を除き、第三者に開示してはならない。また、法令または行政当局により個人データの開示を求められた場合には、保険会社の指示に従わなければならない。

参考資料【３－１】

第 10 条（委託契約終了時における個人情報の返却等）

１．委託契約書■条に基づき、委託契約が契約期間の満了、解除等で終了した場合、保険会社の保険業務の委託を受けて取得した個人情報または個人データの取扱いについて、保険会社の指示に従わなければならない。

２．前項の義務の履行の確認を保険会社が行う場合、および、保険会社の保険業務の委託を受けて取得した個人情報は個人データを新たに指定するほかの代理店に取り扱わせるにあたり、保険会社に協力しなければならない。

第３章　運用

第 11 条（管理原則）

個人情報および個人データは、本規程に従い適切に管理し、その重要度に応じて取得、利用、移送、保管、廃棄する。

第 12 条（利用目的）

１．当代理店は、個人情報の利用目的をできる限り特定する。

２．個人情報は、あらかじめ本人の同意を得ずに、特定された利用目的の達成に必要な範囲を超えて取り扱ってはならない。

３．利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると認められる範囲を超えて行ってはならず、変更された利用目的は遅滞なく本人に通知または公表を行う。

第 13 条（目的外利用の禁止）

保険会社が本人に対して通知、公表、明示している利用目的の範囲内で委託業務に関する個人情報または個人データを取り扱うこととし、委託業務遂行以外の目的で、個人情報または個人データを利用、加工または複製を行うことはできない。

ただし、保険会社が通知、公表、明示している利用目的とは別に、自らが本人に対して利用目的を通知、公表、明示している範囲内で個人情報または個人データを取り扱うことができる。

第 14 条（適正な取得）

１．直接・間接を問わず、偽りその他不正な手段により、個人情報を取得してはならない。

２．直接・間接を問わず、番号法で定められる個人番号および特定個人情報を取得してはならない。

※上記は、代理店で個人番号および特定個人情報を収集・保管しないケースを想定した記載です。保険業務においては、支払調書を作成する目的以外で個人番号等を収集・利用することは想定されませんが、代理店が独自業務を行っている場合や副業代理店の場合等で、顧客の個人番号等を収集・利用する場合は、番号法により認められている目的を超えて取得・利用しないこと、同法で認められている場合を除き、個人番号等を第三者に提供しないこと等について、記載が必要です。

第 15 条（利用目的の通知・公表・明示）

１．当代理店は、個人情報の取得に際し、当代理店の利用目的をあらかじめ公表している場合を除きその利用目的を本人に通知する。

２．当代理店は、本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ本人に対し利用目的を明示する。ただし、人の生命、身体または財産の保護のために緊急に必要がある場合はこの限りでない。

参考資料【３－１】

第 16 条（センシティブ情報）

１．センシティブ情報については、ガイドラインで定められる場合を除き、取得、利用または第三者提供を行わない。

２．センシティブ情報を取得、利用または第三者提供する場合は、あらかじめ本人の同意を取得する。

第 17 条（個人データの正確性の確保）

当代理店は、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ものとする。

第 18 条（個人データ管理台帳）

個人データ管理責任者は、個人データの取扱状況を確認できる手段の整備のため、以下の事項を含む台帳等を整備すると共に、適宜見直しを行うものとする。

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

第 19 条（安全管理措置）

１．当代理店は、取り扱う個人データの漏えい、滅失またはき損の防止その他個人データの安全管理のため、組織的、人的、技術的に必要かつ適切な措置（以下「安全管理措置」という。）を講じるものとする。

２．組織的安全管理措置として、個人データの安全管理に係わる取扱規程を整備する。取扱規程は、「取得・入力」「利用・加工」「保管・保存」「移送・送信」「消去・廃棄」「漏えい事案等への対応」の個人データの各管理段階毎に定めるものとする。

第 20 条（漏えい時の対応）

１．従業者は、個人情報または個人データの漏えい事故またはそのおそれのある事案を発見した場合は、直ちにその旨を個人データ管理者に報告し、その指示を受けなければならない。

２．個人データ管理者は、個人情報または個人データの漏えい事故またはそのおそれのある事案が発生した旨を直ちに個人データ管理責任者に報告しなければならない。

第 21 条（従業者の監督）

１．当代理店は、個人データの安全管理が図られるよう、その従業者に対する必要かつ適切な監督を行う。

２．当代理店は、従業者に対して個人情報の保護及び適正な取扱いに関する誓約書等の提出を求める。

第 22 条（従業者の教育・指導）

１．従業者に対する個人情報の保護及び適正な取扱いに関する教育・指導方針は、個人データ管理責任者が計画、決定する。

２．従業者は、個人データ管理責任者が指定する個人情報の適正な管理に関する研修を受講しなければならない。

参考資料【３－１】

第 23 条（委託先の監督）

１．個人データ管理責任者は、個人データの取扱いの全部または一部を外部に委託する場合は、取扱いを委託した個人データの安全管理が図られるよう、別に定める個人データの外部委託に係わる規程に基づき、委託先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．個人データ管理責任者は、委託先に対し以下の各号の事項を実施しなければならない。

（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こと

（２）委託先との間で、次の事項を含む委託契約書等を締結すること

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

第 24 条（第三者提供の制限）

当代理店は、法令で定められた場合を除き、あらかじめ本人の同意なく個人データの第三者への提供を行わない。

第 25 条（個人データの開示・訂正・利用停止）

１．当代理店は、保険代理店業務に係わる個人データに関し、個人情報保護法に基づく開示・訂正・利用停止等の求めを受けた場合は、保険会社にその旨を連絡するものとする。

２．保険代理店業務に係わる個人データに関し、個人情報保護法に基づかない照会等を受けた場合は、本人確認を適切に行った上で当代理店から回答を行うことができる。

第 26 条（苦情の処理）

１．当代理店における個人情報の取扱いに関する苦情対応の窓口は、個人データ管理者とする。

２．従業者が、個人情報の取扱いに関する苦情を受け付けた場合は、直ちに個人データ管理者に報告し、その指示を受けなければならない。

３．個人データ管理者は、苦情を受け付けた旨を速やかに個人データ管理責任者に報告しなければならない。

第 27 条（罰則／違反時の懲戒）

当代理店は、本規程に違反した従業者に対して就業規則等に基づき懲戒処分を行う。

第 28 条（改廃）

本規程の改廃は、代理店主の決定または取締役会の決議により行うものとする。

＜附則＞

第１条　本規程は　　年　　月　　日より実施する。

以　上

参考資料【３－１】

当代理店における個人データ管理者等

部署名	個人データ管理者

部署名	本人確認に関する情報の管理者（※）

（※）本人確認に関する情報の管理者とは、当代理店における従業者のＩＤ・パスワードの付与・管理を行う者をいう。

参考資料【３－２－１】

個人データの安全管理に係る取扱規程（雛形）

保険代理店業務に係わる個人情報取扱規程第１９条第２項に定める個人データの安全管理に係わる取扱規程を以下のとおり定める。

１．取得・入力段階における取扱規程

第１条（目的）

本規程は、当代理店における個人データの安全管理措置のうち、個人情報の「取得・入力」段階の取扱いについて定めたものである。

第２条（定義）

１.「取得」とは、本人または第三者から個人情報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（当代理店内の他部門からの取得は含まない）。

２.「入力」とは、取得した個人情報をデータベース等の情報システムに物理的及び電子的に入力することなどをいう。

第３条（取得・入力に関する取扱者の役割・責任及び取扱者の限定）

１．個人データ管理責任者は、個人情報の取得・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情報の取得・入力が行われるよう取扱者を限定しなければならない。

第４条（センシティブ情報の取得・入力に関する取扱者の限定）

個人データ管理者は、個人情報のうち、要配慮個人情報（人種、信条、社会的身分、病歴、前科・前歴、犯罪被害情報などをいう）ならびに労働組合への加盟、門地および本籍地、保健医療および性生活（これらのうち要配慮個人情報に該当するものを除く）に関する情報（以下、各取扱規程において「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。

第５条（取得・入力の対象となる個人データの限定）

個人データ管理者は、取得・入力する個人情報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。

第６条（取得・入力時の照合及び確認手続）

１．個人データの取扱者は、個人情報を取得するときには、情報提供者の本人確認及び権限等の確認を行わなければならない。

２．個人データの取扱者は、個人情報を入力するときには、入力データが正確であることを確認しなければならない。

参考資料【３－２－１】

第７条（個人データの提供、取得時の確認・記録）

個人データの取扱者は、法令で定める場合を除き、個人データを第三者に提供した場合には当該提供に関する事項（提供日、提供先名称、提供内容等）について記録し、個人データを第三者から取得する場合には当該取得に関する事項（取得日、取得先名称、取得経緯、取得内容等）について確認・記録を行わなければならない。

第８条（取得・入力の規程外作業に関する申請及び承認手続）

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情報を取得・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。

第９条（機器・記録媒体等の管理手続）

１．個人データ管理者は、取得・入力した個人情報が保存された機器・記録媒体等の設置場所の指定なら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、個人情報が保存された機器・記録媒体等を適切に保管しなければならない。

第 10 条（個人データへのアクセス制御）

個人データ管理者は、取得・入力した個人情報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の制限、入退室の管理、盗難等の防止措置等を行う。

③ 受信した郵便物やＦＡＸ等の個人情報について適切な管理を行う。

第 11 条（取得・入力状況の記録及び分析）

１．個人データの取扱者は、個人情報を取得・入力する場合、情報の種類や形態等に応じて、必要に応じ、かつ適切に取得・入力状況について記録を行わなければならない。

２．個人データ管理者は、個人情報の漏えい等の防止のため、必要に応じ、記録された状況を確認する。

第 12 条（センシティブ情報の取得の制限）

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、取得してはならない。

① 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センシティブ情報を取得する場合

② 相続手続を伴う保険金支払事務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

③ 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体もしくは労働組合への所属も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

④ 前各号のほか、金融庁ガイドライン第６条第１項各号に掲げる場合

参考資料【３－２－１】

第 13 条（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）

１．個人データの取扱者は、前条①に基づきセンシティブ情報を取得する場合には、当該センシティブ情報を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（原則として書面による。）に基づき業務遂行上必要な範囲で取得しなければならない。

２．個人データの取扱者は、前項において本人の同意に基づかない場合には、当該センシティブ情報を取得してはならない。

３．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もしくは廃棄する。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、個人データの取扱者は、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。

参考資料【３－２－２】

２．利用・加工段階における取扱規程

第１条（目的）

本規程は、当代理店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。

第２条（定義）

１.「利用」とは、個人データを利用目的の範囲内で取り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、また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」とは、営業範囲を勘案してあらかじめ指定した区域をいう。

第３条（利用・加工に関する取扱者の役割・責任及び取扱者の限定）

１．個人データ管理責任者は、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。

第４条（センシティブ情報の利用・加工に関する取扱者の限定）

個人データ管理者は、個人データのうち、センシティブ情報の利用・加工の取扱者を必要最小限に限定しなければならない。

第５条（利用・加工の対象となる個人データの限定）

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。

第６条（利用・加工時の照合及び確認手続）

１．個人データの取扱者は、利用する個人データが対象データとして正しいかについて確認しなければならない。

２．個人データの取扱者は、利用する個人データが正しく加工されたかについて元データと照合しなければならない。

第７条（利用・加工の規程外作業に関する申請及び承認手続）

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。

第８条（機器・記録媒体等の管理手続）

１．個人データ管理者は、利用・加工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なら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。

参考資料【３－２－２】

第９条（個人データへのアクセス制御）

１．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制限、入退室の管理、盗難等の防止措置等を行う。

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及びパスワードを付与すると共に、ＩＤ及びパスワードの管理を徹底しなければならない。

第 10 条（利用・加工状況の記録及び分析）

１．個人データの取扱者は、個人データを利用・加工する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に利用・加工状況について記録を行わなければならない。

２．個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認する。

第 11 条（センシティブ情報の利用・加工の制限）

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・加工してはならない。

① 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センシティブ情報を利用・加工する場合

② 相続手続を伴う保険金支払事務等の遂行に必要な限りにおいて、センシティブ情報を利用・加工する場合

③ 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体もしくは労働組合への所属も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・加工する場合

④ 前各号のほか、金融庁ガイドライン第６条第１項各号に掲げる場合

第 12 条（センシティブ情報の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）

１．個人データの取扱者は、前条①に基づきセンシティブ情報を利用する場合には、当該センシティブ情報を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（原則として書面による。）に基づき業務遂行上必要な範囲で利用しなければならない。

２．個人データの取扱者は、前項において本人の同意に基づかない場合には、当該センシティブ情報を利用してはならない。

３．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もしくは廃棄する。

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、個人データの取扱者は、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。

参考資料【３－２－２】

第 13 条（個人データの管理区域外への持ち出しに関する措置）

１．個人データ管理責任者は、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、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。

３．個人データ管理者は、管理区域外に持ち出すことが可能な個人データを業務上必要最小限の範囲に限定しなければならない。

４．個人データ管理者は、個人データの管理区域外への持ち出しに際し、個人データを持ち出す者が第２項で限定された取扱者本人であることを確認しなければならない。

また、個人データ管理者は、持ち出す個人データが第３項により持ち出すことを限定した個人データの範囲内であるか確認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、必要最小限の件数に限ると共に、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、データの種類や形態等に応じて、必要かつ適切に持ち出した個人データの状況について報告及び記録を行わなければならない。

８．個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、報告及び記録された状況を確認する。

第 14 条（個人データの利用者の識別及び認証）

個人データ管理者は、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。

第 15 条（個人データの管理区分の設定及びアクセス制御）

１．個人データ管理者は、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。

２．個人データ管理者は、前項のアクセス制御機能の設定にあたっては、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。

第 16 条（個人データへのアクセス権限の管理）

１．個人データ管理者は、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、前項のアクセス権限に関する機能の設定にあたっては、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。

第 17 条（個人データの漏えい・き損等防止策）

個人データ管理者は、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。

第 18 条（個人データへのアクセス記録及び分析）

個人データ管理者は、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共に、個人データの漏えい等の防止のため、必要に応じてこれを分析しなければならない。

参考資料【３－２－２】

第 19 条（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）

　個人データ管理者は、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　な期間保管すると共に、個人データの漏えい等の防止のため、必要に応じてこれを分析しなければならない。

参考資料【３－２－３】

３．保管・保存段階における取扱規程

第１条（目的）

本規程は、当代理店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。

第２条（定義）

１.「保管」とは、個人データを加工せず、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、個人データを加工せず、オフィスフロア外（書庫等）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（個人データのバックアップを含む。）などをいう。

第３条（保管・保存に関する取扱者の役割・責任及び取扱者の限定）

１．個人データ管理責任者は、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。

第４条（センシティブ情報の保管・保存に関する取扱者の限定）

個人データ管理者は、個人データのうち、センシティブ情報の保管・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。

第５条（保管・保存の対象となる個人データの限定）

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。

第６条（保管・保存の規程外作業に関する申請及び承認手続き）

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、承認を得た上で行わなければならない。

第７条（機器・記録媒体等の管理手続）

１．個人データ管理者は、個人データ管理台帳を踏まえ、個人データが保存された機器・記録媒体等の保管場所等の指定なら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。

第８条（個人データへのアクセス制御）

１．個人データ管理責任者は、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の制限、入退室の管理、盗難等の防止措置等を行う。

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共に、ＩＤ及びパスワードの管理を徹底しなければならない。

第９条（保管・保存状況の記録及び分析）

１．個人データの取扱者は、個人データを保管・保存する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に保管・保存状況について記録を行わなければならない。

２．個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認する。

第 10 条（個人データに関する障害発生時の対応・復旧手続き）

１．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等を行うよう徹底すると共に、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等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等を適切に管理しなければならない。

第 11 条（個人データの利用者の識別及び認証）

個人データ管理者は、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。

第 12 条（個人データの管理区分の設定及びアクセス制御）

１．個人データ管理者は、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。

２．個人データ管理者は、前項のアクセス制御機能の設定にあたっては、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。

第 13 条（個人データへのアクセス権限の管理）

１．個人データ管理者は、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あたっては、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。

第 14 条（個人データの漏えい・き損等防止策）

個人データ管理者は、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。

第 15 条（個人データへのアクセス記録及び分析）

個人データ管理者は、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共に、個人データの漏えい等の防止のため、必要に応じてこれを分析しなければならない。

第 16 条（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）

個人データ管理者は、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共に、個人データの漏えい等の防止のため、必要に応じてこれを分析しなければならない。

参考資料【３－２－４】

４．移送・送信段階における取扱規程

第１条（目的）

本規程は、当代理店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。

第２条（定義）

１.「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。

第３条（移送・送信に関する取扱者の役割・責任及び取扱者の限定）

１．個人データ管理責任者は、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。

第４条（センシティブ情報の移送・送信に関する取扱者の限定）

個人データ管理者は、個人データのうち、センシティブ情報の移送・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。

第５条（移送・送信の対象となる個人データの限定）

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。

第６条（移送・送信時の照合及び確認手続）

個人データの取扱者は、個人データを移送・送信するときには、移送・送信先に相違がないか照合及び確認を行わなければならない。

第７条（移送・送信の規程外作業に関する申請及び承認手続）

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、承認を得た上で行わなければならない。

第８条（個人データへのアクセス制御）

１．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およ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及びパスワードを付与すると共に、ＩＤ及びパスワードの管理を徹底しなければならない。

参考資料【３－２－４】

第９条（移送・送信状況の記録及び分析）

１．個人データの取扱者は、個人データを移送・送信する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に移送・送信状況について記録を行わなければならない。

２．個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認する。

第 10 条（センシティブ情報の移送・送信の制限）

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・送信してはならない。

① 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センシティブ情報を移送・送信する場合

② 相続手続を伴う保険金支払事務等の遂行に必要な限りにおいて、センシティブ情報を移送・送信する場合

③ 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体もしくは労働組合への所属もしくは加盟に関する従業員等のセンシティブ情報を移送・送信する場合

④ 前各号のほか、金融庁ガイドライン第６条第１項各号に掲げる場合

第 11 条（個人データに関する障害発生時の対応・復旧手続）

１．個人データ管理者は、移送・送信する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等を行うよう徹底すると共に、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等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等を適切に管理しなければならない。

第 12 条（個人データの利用者の識別及び認証）

個人データ管理者は、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。

第 13 条（個人データの管理区分の設定及びアクセス制御）

１．個人データ管理者は、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。

２．個人データ管理者は、前項のアクセス制御機能の設定にあたっては、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。

第 14 条（個人データへのアクセス権限の管理）

１．個人データ管理者は、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あたっては、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。

第 15 条（個人データの漏えい・き損等防止策）

個人データ管理者は、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。

第 16 条（個人データへのアクセス記録及び分析）

個人データ管理者は、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、個人データの漏えい等の防止のため、必要に応じてこれを分析しなければならない。

参考資料【３－２－５】

５．消去・廃棄段階における取扱規程

第１条（目的）

本規程は、当代理店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。

第２条（定義）

１.「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。

第３条（消去・廃棄に関する取扱者の役割・責任及び取扱者の限定）

１．個人データ管理責任者は、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。

第４条（センシティブ情報の消去・廃棄に関する取扱者の限定）

個人データ管理者は、個人データのうち、センシティブ情報の消去・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。

第５条（消去・廃棄時の照合及び確認手続）

１．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・廃棄する個人データについて、個人データ管理台帳等により保管期間を照合または消去・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。

第６条（消去・廃棄の規程外作業に関する申請及び承認手続）

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。

第７条（機器・記録媒体等の管理手続）

１．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なら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。

参考資料【３－２－５】

第８条（個人データへのアクセス制御）

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およ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対置入りを制限する。

第９条（消去・廃棄状況の記録及び分析）

１．個人データの取扱者は、個人データを消去・廃棄する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に消去・廃棄状況について記録を行わなければならない。

２．個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認する。

参考資料【３－２－６】

６．漏えい事案等への対応の段階における取扱規程

第１条（目的）

本規程は、当代理店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。

第２条（定義）

「漏えい事案等」とは、個人情報が記載・収録された帳票や電子記録媒体（USB メモリー・CD・DVD 等）の盗難または紛失、郵便物の誤送付、電子メールやファックスの誤送信等の事故により、個人情報の漏えい、滅失またはき損が生じ、または生じるおそれが高い場合をいう。

第３条（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）

１．個人データ管理責任者は、漏えい事案等への対応に関する部署（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。

第４条（漏えい事案等への対応の規程外作業に関する申請及び承認手続き）

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。

第５条（漏えい事案等の影響等に関する調査手続）

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取扱状況の記録内容の分析を行い、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。

第６条（再発防止策・事後対策の検討に関する手続）

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、漏えいした個人データの取扱状況の記録内容の分析を踏まえた再発防止策・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。

第７条（報告に関する手続）

１．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共に、直ちに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、直ちに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保険会社の指示に従い、社外への報告等（警察への届出、本人への通知等、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。

第８条（漏えい事案等への対応記録及び分析）

１．対応部署の個人データの取扱者は、漏えい事案等へ対応する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に漏えい事案への対応状況について記録を行わなければならない。

２．対応部署の個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認する。

以　上

参考資料【３－３】

個人データの取扱状況の点検及び監査に係る規程（雛形）

保険代理店業務に係わる個人情報取扱規程第７条第１項に定める個人データの取扱状況の点検及び監査に係わる規程を以下のとおり定める。

第１条（目的）

本規程は、当代理店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。

第２条（実施部署）

１．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およ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．点検責任者と点検担当者は兼務することができる。

３．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。

第３条（点検）

１．個人データ管理責任者は、個人データの取扱状況の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扱いに関する規程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、規程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共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。

第４条（監査）

１．個人データ管理責任者は、個人データの取扱状況の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監査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扱いに関する規程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、規程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共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。

以　上

参考資料【３－４】

個人データの外部委託に係る規程（雛形）

保険代理店業務に係わる個人情報取扱規程第２３条第１項に定める個人データの外部委託に係わる規程を以下のとおり定める。

第１条（目的）

本規程は、当代理店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。

第２条（定義）

１.「委託」とは、契約の形態や種類を問わず、当代理店が他の者に個人データの取扱いの全部また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、当代理店が、個人データの取扱いの全部また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。

第３条（外部委託にあたっての所属保険会社への申請及び承認）

個人データ管理責任者は、個人データの外部委託にあたって、所属保険会社に書面により申請し、承認を得なければならない。ただし、所属保険会社が別に定める場合はこの限りではない。

第４条（委託先選定の基準）

１．個人データ管理者は、委託先を選定するにあたって、「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あ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。

第５条（委託先における選定基準の遵守状況の確認）

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または随時に確認すると共に、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。

第６条（委託契約）

１．個人データ管理責任者は、選定した委託先との間で、以下の安全管理に関する事項を盛り込んだ委託契約の締結等を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、改竄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、定期的に委託契約等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。

第７条（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）

個人データ管理者は、定期的また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。

（※）オンラインストレージ使用の際には、「委託先選定チェックリスト」ではなく「オンラインストレージ業務に関するチェックリスト」を使用する。

以　上

MEMO