ダイレクト・メールの利用に関する
個人情報保護ガイドライン

平成１６年１２月

ＪＤＭＡ

社団法人　　日本ダイレクト・メール協会

目　次

序　章……1

第一章　総則
第１条　目的……2
第２条　適用範囲……2
第３条　基本原則（ガイドラインの遵守）……2

第二章　定義
第４条　定義……2～6

――――　実行と運用について　――――――――――――――――――――――――――――

第三章　個人情報の収集に関する措置（情報収集・取得）
第５条　利用目的の特定……6～7
第６条　利用目的による制限……7
第７条　適正な取得（取得の原則）……7
第８条　取得に際しての利用目的の通知等（利用目的の通知・公表）……8～9

第四章　個人情報の適正管理措置（情報管理）
第９条　個人データの正確性の確保……9
第１０条　安全管理措置……9
第１１条　従業者の監督……１０
第１２条　委託先の監督……１０～１１

第五章　個人情報の利用と提供に関する措置（情報利用と第三者提供）
第１３条　個人情報の第三者への提供……１１～１３

第六章　個人情報に関する本人の権利（本人からの要求への対応）
第１４条　保有個人データに関する事項の公表等……１３～１４
第１５条　保有個人データの開示……１４
第１６条　保有個人データの訂正等……１４～１５
第１７条　保有個人データの利用停止等……１５
第１８条　理由の説明……１５
第１９条　開示、訂正等、利用停止等の求めに応じる手続き……１５～１６
第２０条　問い合わせ対応……１６

第七章　方針・内部規程・管理体制等
第２１条　個人情報保護方針……１６
第２２条　内部規程・運用ルールの策定……１６～１７
第２３条　個人情報管理責任者……１７

―――― ガイドラインの見直し等について ――――――――――――――――――――

第八章　その他
　第２４条　報告等……**１７**
　第２５条　見直し……**１８**

附　則……**１８**

―――――― 別紙参考 ――――――――――――――――――――――――――

安全管理措置として講じることが望まれる具体的事項……**別１～別９**

序　章

企業各社においては、顧客情報・個人情報は企業情報資産としての重要情報であり、企業戦略の核となっています。一方、その取扱方法と活用は戦略実現を左右し、また、組織の存亡にも関わるものです。

飛躍的に進歩するＩＴ（情報通信・処理技術）、インターネットの普及により個人情報の活用性が高まる中で、その不正・不当な流用・漏えい問題も急増しています。その中には、無意識の行動に起因するものや、内部からの問題発生も少なくありません。

こうした背景のもと、個人情報の有用性に配慮しつつ個人の権利利益を保護することを目的とした「個人情報の保護に関する法律（平成１５年5月３０日法律第５７号）＝以下、「個人情報保護法」という。」が平成１７年（２００５年）４月から完全施行されます。これに伴い、企業各社には益々厳格化される個人情報の保護と取り扱い、そしてその一層の理解と浸透、対応実践の徹底が要求されています。

そこで、社団法人　日本ダイレクト・メール協会（以下、当協会という。）では、個人情報保護法の趣旨を踏まえながら、会員企業各社が取り扱う個人情報の適切・適正な保護のための基礎としての、【ダイレクト・メールの利用に関する個人情報保護ガイドライン】（以下、「本ガイドライン」という。）を策定しました。

本ガイドラインは、経済産業省『個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン』を基に、日本工業規格「個人情報保護に関するコンプライアンス・プログラムの要求事項」（ＪＩＳ　Ｑ　１５００１）を参考として策定したものです。

当協会は、【ダイレクト・メール】利用企業のほか、データベース事業者、広告代理店、発送代行会社など、【ダイレクト・メール】を取り巻く様々な業種企業で構成されていますが、会員各社は本ガイドラインを参考に、独自の業態に即した個人情報に関する保護規程を個別に定め、コンプライアンス・プログラムを実行されることを希求します。

本ガイドラインは、会員以外であっても、【ダイレクト・メール】の計画・実施に携わる企業各社は独自の保護規程を定める等、適切な対応を図るために参考にすることができます。

また、複数の業種の事業を行うことがある場合には、関連するすべての業界ガイドラインを参照し、その趣旨を十分に踏まえながら、適切な個人情報保護対策を講じていくようにしてください。

平成１６年１２月
社団法人　日本ダイレクト・メール協会

第一章　総則

第１条　：　目的

当協会会員企業各社（以下、「会員」という。）においては、事業活動を行う上で不可欠な個人情報を適切に取り扱うことが最大の課題であると認識する。

本ガイドラインは、【ダイレクト・メール】の計画・実施に携わる会員における個人情報保護体制、個人情報の取扱方法、その運用に関する事項を定め、もって円滑な事業活動と企業倫理・法遵守、およびコンプライアンス経営を支援する具体的な指針として定めたものであり、個人情報の有用性に配慮するとともに、個人の権利利益を保護することにより、健全な【ダイレクト・メール】の普及・発展に寄与することを目的とする。

第２条　：　適用範囲

１．本ガイドラインは、【ダイレクト・メール】の計画・実施において個人情報を取り扱う会員に適用される。

２．第１項に該当しない【ダイレクト・メール】の計画・実施において個人情報を取り扱う事業者においても、個人情報を取り扱う際の基準または個人情報保護に関する規程を策定する際の参考として本ガイドラインを用いることができる。その場合は、本ガイドラインの趣旨を充分に踏まえること。

第３条　：　基本原則　（ガイドラインの遵守）

１．本ガイドラインは、個人情報保護法、およびその関係法令に基づいて、最低限度の遵守すべきルールをまとめたものである。

２．会員は、個人情報保護と利用・活用のバランスの上に、個人情報の取り扱いに関する方針を独自に策定し、規程を定め、その周知と徹底、実行することが望まれる。

３．会員がこのガイドラインに違反、またそれによる事件・事故を起こした場合は、理事会の判断を経て、総会の議決を通して「退会」措置に至ることもある。

第二章　定義

第４条　：　定義

本ガイドラインで用いる用語の定義は、次による。

１．「個人情報」とは

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、または個人別につけられた番号、その他の符号、画像もしくは音声によって当該個人を識別できるもの。加えて、当該情報だけでは識別できないが、他の情報と容易に照合することができ、それによって当該個人を識別できるものを含む。

【該当する事例】

①本人の氏名
②特定の個人を識別できる【ダイレクト・メール】の宛名情報
（会社住所宛の【ダイレクト・メール】であっても宛名に個人名を使用したものは個人情報となる）
③電話帳等で公にされている情報（本人の氏名等）
④生年月日、性別、過去の購買履歴などの属性情報について、それらと本人の氏名を組み合わせた情報

【該当しない事例】

①企業の財務情報、団体情報
②特定の個人を識別することができない統計情報
③特定の個人を識別することができない【ダイレクト・メール】の宛名情報
（例えば、会社住所宛の【ダイレクト・メール】で、「総務ご担当者様」や「総務部御中」など、個人名を使用しない宛先としている場合）

２．「個人情報データベース等」とは

個人情報を含む情報の集合物であって、次に掲げるものをいう。

(1)特定の個人情報をコンピュータを用いて検索することができるように体系的に構成したもの

(2)一定の規則に従って整理することにより特定の個人情報を、容易に検索することができるように体系的に構成した情報の集合物であって、コンピュータを用いていない場合であっても、目次、索引その他検索を容易にするためのものを有するもの

【該当する事例】

①顧客管理データベース
②紙に記載された顧客管理台帳
③本体データベース顧客管理台帳から抽出した【ダイレクト・メール】発送用データベースまたは発送リスト
④【ダイレクト・メール】発送のために氏名、住所等で分類整理された顧客登録カード
⑤氏名、住所、企業別に分類整理されている市販の人名録

【該当しない事例】

①アンケート回答やプレゼントキャンペーンの応募はがきで、氏名、住所等で分類整理されていない状態である場合
（ただし、これらは当然、個人情報であり、管理の対象である）

３．「個人情報取扱事業者」とは

個人情報データベース等を事業の用に供している者をいう。なお、個人であっても個人情報取扱事業者に該当し得る。

４．「個人データ」とは

個人情報データベース等を構成する個人情報をいう。

【該当する事例】

①個人情報データベース等から、他の媒体に格納した【ダイレクト・メール】発送作業用の個人情報
②個人情報データベース等から、コンピュータ処理により出力された帳票等

【該当しない事例】

①個人情報データベース等を構成する前の入力帳票に記載されている個人情報

※電話帳、カーナビゲーションシステム等の取り扱いについて

個人情報データベース等が、以下の要件の全てに該当する場合は、その個人情報データベース等を構成する個人情報は、「本ガイドライン第９条（個人データの正確性の確保）～第１３条（個人情報の第三者への提供）」までの規定の適用においては、「個人データ」には該当せず、個人情報取扱事業者の義務（第四章：個人情報の適正管理措置）は課されない。ただし、この場合においても、会員はできる限り、義務遂行に取り組むものとする。

ア）個人情報データベース等の全部または一部が他人の作成によるもの

イ）個人情報データベース等を構成する個人情報として、氏名、住所（居所を含み、地図上またはコンピュータの映像面上において所在場所を示す表示を含む）、または電話番号のみを含んでいる

ウ）個人情報データベース等について、新たに個人情報を加え、識別される特定の個人を増やしたり、他の個人情報を付加したりして、個人情報データベース等そのものを変更するようなことをせずに、その事業の用に供している

５．「保有個人データ」とは

個人情報取扱事業者が、開示、内容の訂正、追加または削除、利用の停止、消去および第三者への提供の停止を行うことのできる権限を有する個人データであって、次に掲げるものを除くものとする。

(1)当該個人データの存否が明らかになることにより、本人または第三者の生命、身体または財産に危害が及ぶおそれがあるもの

(2)当該個人データの存否が明らかになることにより、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もの

(3)６ヶ月以内に消去することとなるもの

６．「本人」とは

個人情報によって識別される、または識別され得る特定の個人をいう。

７．「本人に通知」とは

本人に直接知らしめることをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

【通知の事例】

①【ダイレクト・メール】において、取得後最初に送付する【ダイレクト・メール】の同封物または封筒、パンフレット類において文書の記載によること （【ダイレクト・メール】と独立した通知を【ダイレクト・メール】の事前に行う必要はない）
②面談においては、口頭またはちらし等の文書を渡すこと
③電話においては、口頭または自動応答装置等で知らせること

④隔地者間においては、電子メール、ＦＡＸ等により送信すること、または文書を郵便等で送付すること

８.「公表」とは

広く一般に自己の意思を知らせることをいう。

【公表の事例】

①自社のウェブ画面上への掲載、自社の店舗・事務所内におけるポスター等への掲示、パンフレット等の備え置き・配布等
②通信販売用のパンフレット、カタログ、請求書等への記載によること

９.「本人に対し、その利用目的の明示」とは

本人に対し、その利用目的を明確に示すことをいう。

【利用目的の明示の事例】

①利用目的を明記した契約書その他の書面を相手方である本人に対し手交し、または送付すること。契約約款または利用条件等の書面中に利用目的条項を記載する場合は、例えば裏面約款等に記載されている利用目的条項を表面にも記述する等本人が実際に利用目的を目にできるように留意する必要がある
②インターネット上において本人がアクセスした自社のウェブ画面上、または本人の端末装置上にその利用目的を明記すること

１０.「本人の同意」とは

本人の個人情報が、個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいう。また「本人の同意を得（る）」とは、本人の承諾する旨の意思表示を当該個人情報取扱事業者が認識することをいう。

【本人の同意を得ている事例】

① 同意する旨を本人から口頭または書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）で確認すること
② 本人が署名または記名押印した同意する旨の申込書等文書を受領し確認すること
③本人からの同意する旨の電子メールを受信すること
④本人による同意する旨の確認欄へのチェック
⑤本人による同意する旨のウェブ画面上のボタンのクリック
⑥本人による同意する旨の音声入力、タッチパネルへのタッチ、ボタンやスイッチ等による入力

１１.「本人が容易に知り得る状態」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、簡単に知ることができる状態に置いていることをいう。

【容易に知り得る状態の事例】

①ウェブ画面上への掲載等が継続的に行われていること
②事務所の窓口等への掲示、備え付け等が継続的に行われていること
③広く頒布されている定期刊行物への定期的掲載を行っていること

１２.「本人の知り得る状態」とは

本人が知ろうとすれば、常にその時点での正確な内容を本人が知ることができる状態に置いていることをいう。本人の求めに応じて、遅滞なく回答することでもよい。

【知り得る状態の事例】

① 問い合わせ窓口を設け、問い合わせがあれば口頭または文章で回答できるよう体制を構築、整備しておくこと
②【ダイレクト・メール】においては、送付する【ダイレクト・メール】の同封物または封筒、パンフレット類において文書の記載の方法によること

１３.「提供」とは

個人データを、物理的またはインターネット等をとおして利用可能な状態に置くことをいう。

第三章　個人情報の収集に関する措置（情報収集・取得）

第５条　：　利用目的の特定

１．会員は、個人情報を取り扱うに当たっては、その利用目的をできる限り特定しなければならない。なお、利用目的の特定に当たっては、個々の処理の目的を特定するだけにとどめるのではなく、あくまで最終的にどのような目的で個人情報を利用するかを特定する必要がある。

【利用目的を特定している事例】

①「当社の商品に関する、ご案内・ご紹介のための【ダイレクト・メール】を送付させて頂くために、利用させていただきます。」
②「ご記入頂いた氏名、住所、電話番号は、名簿として販売することがあります。」
③情報処理サービスを行っている事業者の場合は、「給与計算処理サービス、宛名印刷サービス、伝票の印刷・発送サービス等の情報処理サービスを業として行うために、委託された個人情報を取り扱います。」

【利用目的を特定していない事例】

①「当社の提供するサービスの向上のため。」
②「当社のマーケティング活動、事業活動に用いるため。」

２．会員は、利用目的を変更する場合には、変更前の利用目的から本人が想定することが困難でない範囲内で利用目的を変更することができる。

【本人が想定することが困難でない場合の事例】

①「当社の行う○○事業における新商品・サービスに関する情報を電子メールにより送信することがあります。」とした利用目的において、「郵便によりお知らせすることがあります。」旨追加することは、許容される

第６条　：　利用目的による制限

１．会員は、利用目的の達成に必要な範囲を超えて個人情報を利用または提供する場合は、あらかじめ、本人の同意を取得しなければならない。

２．会員は、合併、分社化、営業譲渡等により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得し、承継前における利用目的の達成に必要な範囲を超えて当該個人情報を利用する場合は、あらかじめ、本人の同意を取得しなければならない。

【同意が必要な場合の事例】

①就職のための履歴書情報をもとに、自社の商品の販売促進のために自社取扱商品のカタログと商品購入申込書を送る場合

②合併、分社化、営業譲渡等により事業が承継され個人データが移転される場合、譲渡後に、個人データが譲渡される前の利用目的の達成に必要な範囲を超えて利用される場合

【同意が必要でない場合の事例】

①合併、分社化、営業譲渡等により事業が承継され個人データが移転される場合、譲渡後も、個人データが譲渡される前の利用目的の範囲内で利用する場合

※第６条（利用目的による制限）第１、２項の「本人の同意」については、法施行前に得たものであっても、法に基づく同意があったものとみなされる。

第７条　：　適正な取得　（取得の原則）

会員は、偽りその他不正の手段により個人情報を取得してはならない。なお、不正の競争目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを詐欺等により取得したり、使用・開示した者には、不正競争防止法により刑事罰が科され得る。

【不適正な取得の事例】

①親の同意がなく、十分な判断能力を有していない子供から家族の個人情報を取得する場合

②第三者提供制限違反をするよう強要して個人情報を取得した場合

③他の事業者に指示して不正な手段で個人情報を取得させ、その事業者から個人情報を取得する場合

④不正な手段で個人情報を取得した他の事業者から、事情を知って取得すること

⑤第三者提供における制限（第１３条　個人情報の第三者への提供）に違反した他の事業者から、事情を知って取得すること

第８条　：　取得に際しての利用目的の通知等　（利用目的の通知・公表）

１．会員は、個人情報を取得した場合、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、または公表しなければならない。

【本人に通知または公表が必要な場合の事例】

①インターネット上で本人が自発的に公表している個人情報を取得する場合
②インターネット、官報、職員録等から個人情報を取得する場合
③電話による問い合わせやクレーム等により、本人から自発的に提供される個人情報を取得する場合
④個人情報の第三者提供を受ける場合（データベース事業者等からの購入を含む）
⑤取得時の利用目的と相当な関連性を有すると合理的に認められる範囲内で利用目的を変更した場合

【友達紹介により取得した個人情報を利用する場合の利用目的の通知について】

友達紹介というかたちで紹介された個人に【ダイレクト・メール】を送付する場合は、個人情報の利用目的をウェブ画面上への継続的な掲載等で公表しているか否かにかかわらず、取得方法、利用目的、個人データの利用停止方法を記載した書面を同送する。また、紹介する側にも提供する友達の個人情報の利用目的について通知、または公表しておくことが望ましい。

２．会員は、本人から直接、個人情報を書面、電子メールなどの電子手段などにより取得する場合は、あらかじめ本人に対し、その利用目的を明示しなければならない。

【あらかじめ本人に対し、その利用目的を明示しなければならない場合の事例】

①申込書・契約書に記載された個人情報を本人から直接取得する場合
②アンケートに記載された個人情報を直接本人から取得する場合
③懸賞の応募はがきに記載された個人情報を直接本人から取得する場合

３．会員は、利用目的を変更した場合は、変更された利用目的について本人に通知または公表しなければならない。

４．第８条（取得に際しての利用目的の通知等）第１～３項の規定は、次に掲げる場合については、適用しない。

(1)利用目的を本人に通知し、または公表することにより本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
(2)利用目的を本人に通知し、または公表することにより当該会員の権利または正当な利益を害するおそれがある場合
(3)国の機関若しくは地方公共団体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、利用目的を本人に通知し、または公表す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場合
(4)取得の状況からみて利用目的が明らかであると認められる場合

第四章　個人情報の適正管理措置（情報管理）

取得した個人データは、全て利用目的の範囲内において、紙媒体または電子媒体にて適正な管理がなされなければならない。

第９条　：　個人データの正確性の確保

会員は、利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認の手続きの整備、誤り等を発見した場合の訂正等の手続きの整備、記録事項の更新、保存期間の設定等を行うことにより、個人データを正確かつ最新の内容に保つよう努めなければならない（第４条第４項※電話帳、カーナビゲーションシステム等の取り扱いについての場合を除く。）。

この場合、保有する個人データを一律にまたは常に最新化する必要はなく、それぞれの利用目的に応じて、その必要な範囲内で正確性・最新性を確保すれば足りる。

第１０条　：　安全管理措置

会員は、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の個人データの安全管理のために、以下の組織的、人的、物理的、および技術的安全管理措置を講じなければならない。各々の規程については、別紙「安全管理措置として講じることが望まれる具体的事項」を参考。

(1)組織的安全管理措置として講じなければならない事項
- ①個人データの安全管理措置を講じるための組織体制の整備
- ②個人データの安全管理措置を定める規程等の整備と規程等に従った運用
- ③個人データの取扱状況を一覧できる手段の整備
- ④個人データの安全管理措置の評価、見直しおよび改善
- ⑤事故または違反への対処

(2)人的安全管理措置として講じなければならない事項
- ①雇用契約時および委託契約時における非開示契約の締結
- ②従業者に対する教育・訓練の実施

なお、管理者が定めた規程等を守るように監督することについては、第１１条（従業者の監督）を参照。

(3)物理的安全管理措置として講じなければならない事項
- ①入退館（室）管理の実施
- ②盗難等の防止
- ③機器・装置等の物理的な保護

(4)技術的安全管理措置として講じなければならない事項
- ①個人データへのアクセスにおける識別と認証
- ②個人データへのアクセス制御
- ③個人データへのアクセス権限の管理
- ④個人データのアクセスの記録
- ⑤個人データを取り扱う情報システムについての不正ソフトウェア対策
- ⑥個人データの移送・送信時の対策
- ⑦個人データを取り扱う情報システムの動作確認時の対策
- ⑧個人データを取り扱う情報システムの監視

第１１条　：　従業者の監督

１．会員は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督・教育を行わなければならない。その際、本人の個人データが漏えい、滅失またはき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質および個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。

２．なお、第１０条（安全管理措置）(2)②および第１１条第１項の「従業者」とは、会員の組織内にあって直接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員（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、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。

３．従業者への教育は以下の項目を含むことが望まれる。
(1)個人情報保護の重要性および利点
(2)個人データおよび情報システムの安全管理に関する従業者の役割および責任
(3)個人情報保護に関する内部規程等の違反に対する従業者個人への罰則等
(4)個人データの漏えい、滅失またはき損により予想される本人の損害
(5)個人データの漏えい、滅失またはき損により予想される企業リスク

４．会員は、従業者に対する必要な教育および監督体制の確立を図るとともに、教育・訓練が必要かつ適切に実施されていることを定期的に確認することが望まれる。

【従業者に対して適切な監督を行っていない場合の事例】

①従業者が、個人データの安全管理措置を定める規程に従って業務を行っていることを、あらかじめ定めた間隔で定期的に確認せず、結果、個人データが漏えいした場合
②内部規程等に違反して個人データが入ったノート型パソコンを繰り返し持ち出されていたにもかかわらず、その行為を放置した結果、紛失し、個人データが漏えいした場合

第１２条　：　委託先の監督

１．会員は、個人データの取り扱いの全部または一部を委託する場合、第１０条（安全管理措置）に基づく安全管理措置を遵守させるよう、受託者に対し必要かつ適切な監督をしなければならない。その際、本人の個人データが漏えい、滅失またはき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質および個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。

２．会員は、「必要かつ適切な監督」には、委託契約において、当該個人データの取り扱いに関して、必要かつ適切な安全管理措置として、委託者、受託者双方が同意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認することも含まれる。なお、優越的地位にある者が

委託者の場合、受託者に不当な負担を課すことがあってはならない。

【受託者に必要かつ適切な監督を行っていない事例】

①個人データの安全管理措置の状況を契約締結時およびそれ以後も定期的に把握せず外部の事業者に委託した場合で、受託者が個人データを漏えいした場合
②個人データの取り扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えいした場合
③再委託の条件に関する指示を受託者に行わず、かつ受託者の個人データの取扱状況の確認を怠り、受託者が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合

また、委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取り扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意を要する。

【個人データの取り扱いを委託する場合に契約に盛り込むことが望まれる事項】

(1)委託者および受託者の責任の明確化
(2)個人データの安全管理に関する事項
・個人データの漏えい防止、盗用禁止に関する事項
・委託契約範囲外の加工、利用の禁止
・委託契約範囲外の複写、複製の禁止
・委託契約期間
・委託契約終了後の個人データの返還・消去・廃棄に関する事項
(3)再委託に関する事項
・再委託を行うに当たっての委託者への文書による報告
(4)個人データの取扱状況に関する委託者への報告の内容および頻度
(5)契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）
(6)契約内容が遵守されなかった場合の措置
(7)セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

第五章　個人情報の利用と提供に関する措置（情報利用と第三者提供）

第１３条：個人情報の第三者への提供

１．会員は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。
(1)法令に基づく場合
(2)人の生命、身体また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)公衆衛生の向上また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また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

※「本人の同意」については、法施行前に得たものであっても、法に基づく同意があったものとみなされる。

2．同意の取得に当たっては、事業の性質および個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示すこと。

【第三者提供とされる事例】

（ただし、第１３条（個人情報の第三者への提供）第４項(1)～(3)の場合を除く。）

①親子兄弟会社、グループ会社の間で個人データを交換する場合
②フランチャイズ組織の本部と加盟店の間で個人データを交換する場合
③同業者間で、特定の個人データを交換する場合
④外国の会社に国内に居住している個人の個人データを提供する場合

【第三者提供とされない事例】（ただし、利用目的による制限がある。）

①同一事業者内で他部門へ個人データを提供すること

3．会員は、第三者提供におけるオプトアウト※を行っている場合には、本人の同意なく、個人データを第三者に提供することができる。

※「第三者提供におけるオプトアウト」とは、提供に当たりあらかじめ、以下の(1)～(4)の情報を、本人に通知し、または本人が容易に知り得る状態に置いておくとともに、本人の求めに応じて第三者への提供を停止することをいう。

(1)第三者への提供を利用目的とすること

(2)第三者に提供される個人データの項目

【事例】

①氏名、住所、電話番号
②氏名、商品購入履歴

(3)第三者への提供の手段または方法

【事例】

①書籍として出版
②インターネットに掲載
③プリントアウトして交付等
④【ダイレクト・メール】の宛名を磁気媒体として企業に販売

(4)本人の求めに応じて第三者への提供を停止すること

４．第三者提供に該当しない場合

次に掲げる場合において、当該個人データの提供を受ける者は、第１３条（個人情報の第三者への提供）第１～３項の規定の適用については、第三者に該当しないものとする。

(1) 委託…利用目的の達成に必要な範囲内において個人データの取り扱いの全部または一部を委託する場合

【事例】

①データの打ち込み等、情報処理を委託するために個人データを渡す場合

(2)事業の承継…合併その他の事由による事業の承継に伴って個人データが提供される場合
ただし、事業の承継後も、個人データが譲渡される前の利用目的の範囲内で利用しなければならない

【事例】

①合併、分社化により、新会社に個人データを渡す場合 **②営業譲渡により、譲渡先企業に個人データを渡す場合**

(3)共同利用…個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的および当該個人データの管理について責任を有する者の氏名または名称について、あらかじめ、本人に通知し、または本人が容易に知り得る状態に置いているとき

※第１３条（個人情報の第三者への提供）第３、４項の「本人に通知」については、法施行前に本人に通知していても、法に基づき、本人に通知したものとみなされる。

第六章：個人情報に関する本人の権利　（本人からの要求への対応）

第１４条　：　保有個人データに関する事項の公表等

１．会員は、保有個人データに関し、次の各号に掲げる事項について、本人の知り得る状態に置くこととする。

(1)会員の氏名または名称
(2)すべての保有個人データの利用目的　（ただし、第８条（「取得に際しての利用目的の通知等」）第４項第１～３号までに該当する場合を除く）
(3)保有個人データの利用目的の通知および保有個人データの開示に係る手数料の額（定めた場合に限る）並びに開示等の求め※の手続き
(4)保有個人データの取り扱いに関する苦情の申出先

なお、法施行前から保有している個人情報については、法施行時に個人情報の取

得行為がなく、第８条（取得に際しての利用目的の通知等）の規定は適用されないので、法施行時に第１４条（保有個人データに関する事項の公表等）第１項の措置（上記の措置）を講ずる必要がある。

※「開示等の求め」とは、保有個人データの利用目的の通知、保有個人データの開示、保有個人データの内容の訂正、追加または削除、保有個人データの利用の停止または消去、保有個人データの第三者への提供の停止の求めをいう。

２．会員は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められた時は、原則として本人に対し、遅滞なく、これを通知しなければならない。また、通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

第１５条　：　保有個人データの開示

１．会員は、本人から、当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しない時にその旨を知らせることを含む。以下同じ。）を求められた時は、本人に対し、遅滞なく、当該保有個人データを開示する。ただし開示することにより次の各号のいずれかに該当する場合は、その全部または一部を開示しないことができる。

(1)本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

(2)当該業務の適正な実施に著しい支障を及ぼすおそれがある場合

【事例】

①同一の本人から複雑な対応を要する同一内容について繰り返し開示の求めがあり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ち行かなくなる等、業務上著しい支障を及ぼすおそれがある場合

(3)他の法令に違反することとなる場合

２．第１５条（保有個人データの開示）第１項の規定に基づき求められた保有個人データの全部または一部について開示しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知する。

第１６条　：　保有個人データの訂正等

１．会員は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正、追加または削除（以下「訂正等」という）を求められた場合には、その内容の訂正等に関して、他の法令の規定により特別の手続きが定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。ただし、利用目的から見て訂正等が必要ではない場合や誤りである旨の指摘が正しくない場合には、訂正等を行う必要はない。

２．第１６条（保有個人データの訂正等）第１項の規定に基づき求められた保有個人データの内容の全部若しくは一部について訂正等を行った時、または訂正等を行わない旨の決定をした時は、本人に対し遅滞なく、その旨を通知しなければならない。

【訂正を行う必要がない事例】

①訂正等の対象が事実でなく評価に関する情報である場合

第１７条　：　保有個人データの利用停止等

会員は、本人から当該本人が識別される保有個人データの利用の停止、削除または、消去および第三者への提供の停止（以下「利用停止等」という）を求められた場合、その求めに理由があることが判明した時は、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、違反を是正するための必要な限度を超えている場合や手続違反である旨の指摘が正しくない場合には、利用の停止等を行う必要はない。

第１８条　：　理由の説明

会員は、第１４条（保有個人データに関する事項の公表等）第２項、第１５条（保有個人データの開示）第２項、第１６条（保有個人データの訂正等）第２項または第１７条（保有個人データの利用停止等）の規定により、本人から求められた措置の全部または一部についてその措置をとらない旨を通知する場合またはその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めなければならない。

第１９条　：　開示、訂正等、利用停止等の求めに応じる手続き

１．会員は、開示等の求めを受け付ける方法として、次の各号の事項を定めることができる。また、その求めを受け付ける方法を定めた場合には、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置いておかなければならない。

(1)開示等の求めの受付先
(2)開示等の求めに際して提出すべき書面の様式、その他の開示等の求めの受付方法
(3)開示等の求めをする者が本人またはその代理人であることの確認の方法
(4)保有個人データの利用目的の通知、または保有個人データの開示をする際に徴収する手数料の徴収方法

３．会員は、円滑に開示等の手続きが行えるよう、本人に対し、自己のデータの特定に必要な事項の提示を求めることができる。なお、本人が容易に自己のデータを特定できるよう、自己の保有個人データの特定に資する情報の提供その他本人の利便性を考慮しなければならない。

【開示等の求めを受け付ける方法の事例】

①本人の場合（来所）：運転免許証、健康保険の被保険者証、写真付き住民基本台帳カード、旅券（パスポート）、外国人登録証明書、年金手帳、印鑑証明書と実印
②本人の場合（オンライン）：ＩＤとパスワード
③本人の場合（電話）：一定の登録情報（生年月日等）、コールバック
④本人の場合（郵送）：運転免許証のコピーと住民票の写し
⑤代理人の場合（来所）：本人および代理人ついて、運転免許証、健康保険の被保険者証、パスポート、外国人登録証明書、年金手帳、弁護士の場合は登録番号、代理を示す旨の委任状

４．会員は、開示等の求めに応じる手続きを定めるに当たっては、必要以上に煩雑な書類を求めることや、求めを受け付ける窓口を他の業務を行う拠点とは別にいたずらに不便な場所に限定すること等して、本人に過重な負担を課することのないよう配慮しなければならない。

第２０条　：　問い合わせ対応

会員は、個人情報の取り扱いに関する問い合わせを受け付けて、迅速に処理する体制の整備に努めなければならない。

第七章　方針・内部規程・管理体制等

第２１条　：　個人情報保護方針

１．会員は、以下の事項を含む個人情報保護に関わる全社方針を定め、それを役員・従業者に周知・徹底させるとともに、顧客への通知、および広く一般にも公表することが望ましい。

(1)事業の内容および規模を考慮した適切な個人情報の収集、利用および提供に関すること
(2)個人情報への不正アクセス、個人情報の紛失、破壊、改ざんおよび漏えいなどの予防ならびに是正に関すること
(3)個人情報に関する法令およびその他の規範を遵守すること
(4)コンプライアンス・プログラムの継続的改善に関すること
(5)個人情報保護に関わる方針についての啓蒙・教育活動方針に関すること

２．顧客の信頼を保持し、競争力を維持・向上していくために、所有・管理情報資産に対して、適切な安全対策を実施し、紛失、盗難、不正使用などから保護することを経営者の意思表明・声明として、策定、宣言することが望ましい。

第２２条　：　内部規程・運用ルールの策定

１．会員は、個人情報保護方針を受けて、内部規程・運用ルール※を策定し、周知・徹底させると共に、個人情報に関する法令およびその他の規範を特定し、全役員、従業者が参照できる手順を確立し、維持することが望ましい。

内部規程には、次の事項が含まれる。

(1)事業者の各部門および階層における個人情報を保護するための権限および責任の規定
(2)個人情報の収集、利用、提供および管理の規定
(3)本人からの個人情報に関する開示、訂正および削除の規定
(4)個人情報保護に関する教育の規定
(5)個人情報保護に関する監査の規定
(6)内部規程の違反に関する罰則の規定

２．なお、第２２条（内部規程・運用ルールの策定）第１項の内部規程は、取締役会の決議を経るなど従業者を正当に拘束するに足りる一定の手続きを経て定める必要がある。

※上記の「運用ルール」とは内部規程実施の詳細手順のことをいうものであり、会員はその策定が望ましい。

第２３条　：　個人情報管理責任者

１．会員は、個人情報保護について全社を代表する者として、役員以上での責任者を指名しなければならない。

２．第２３条（個人情報管理責任者）第１項の個人情報管理責任者は、本ガイドラインに定められた事項を理解し、および遵守するとともに、以下のような項目を実施する責任を負うものとする。

(1)内部規程の整備
(2)安全対策の実施
(3)従業者への教育訓練
(4)委託先の適切な監督
(5)事故時の対応
(6)個人情報の適切な収集、利用、提供の実施

第八章　その他

第２４条　：　報告等

１．会員は、個人情報の取り扱いに関し、当協会および総務省、経済産業省等関係機関から報告を求められた場合は直ちに報告しなければならない。

２．会員は、第三者へ個人情報が漏えいした事実、および漏えいしたおそれがある事実を把握した場合は当協会に報告するものとする。

３．個人情報の漏えい等の事案が発生した場合は、二次被害の防止、類似事案の発生回避等の観点および本人が被る権利利益の侵害の大きさを考慮し、可能な限り事実関係等を公表するものとする。

第２５条　：　見直し

個人情報の保護についての考え方は、社会情勢の変化、国民の意識の変化、技術の進歩等に応じて変わり得るものであり、当協会は、本ガイドラインを、法の施行後の状況等、諸環境の変化を踏まえて、見直しを行うものとする。

附　則

１．本ガイドラインは、平成１７年４月１日から施行する。
２．平成１０年制定の、『ダイレクト・メールに関する個人情報保護ガイドライン』は、本ガイドラインの施行の時をもって廃止する。

別　紙

安全管理措置として講じることが望まれる具体的事項

１．組織的安全管理措置

組織的安全管理措置とは、安全管理について従業者（本ガイドライン第１１条（従業者の監督）第２項参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。

【組織的安全管理措置として講じなければならない事項】

①個人データの安全管理措置を講じるための組織体制の整備
②個人データの安全管理措置を定める規程等の整備と規程等に従った運用
③個人データの取扱状況を一覧できる手段の整備
④個人データの安全管理措置の評価、見直しおよび改善
⑤事故または違反への対処

【各項目について講じることが望まれる事項】

①個人データの安全管理措置を講じるための組織体制の整備をする上で望まれる事項

ﾁｪｯｸ	内　　容
	従業者の役割・責任の明確化 ※個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。
	個人情報管理責任者の設置
	個人データの取り扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置および作業担当者の限定
	個人データを取り扱う情報システム運用責任者の設置および担当者（システム管理者を含む。）の限定
	個人データの取り扱いに関わるそれぞれの部署の役割と責任の明確化
	監査責任者の設置
	監査実施体制の整備
	個人データの取り扱いに関する規程等に違反している事実または兆候があることに気づいた場合の、代表者等への報告連絡体制の整備
	個人データの漏えい等の事故が発生した場合、または発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備 ※個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい（法第３１条、本ガイドライン第２０条（問い合わせ対応）を参照）。
	漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備
	漏えい等の事故発生時における主務大臣および認定個人情報保護団体等に対する報告体制の整備

②個人データの安全管理措置を定める規程等の整備と規程等に従った運用をする上で望まれる事項

	個人データの取り扱いに関する規程等の整備とそれらに従った運用
	個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用 ※なお、これらについてのより詳細な記載事項については、下記の【個人データの取り扱いに関する規程等に記載することが望まれる事項】を参照。
	個人データの取り扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用
	個人データの取り扱いを委託する場合における受託者の選定基準、委託契約書のひな型等の整備とそれらに従った運用
	定められた規程等に従って業務手続が適切に行われたことを示す監査証跡※の保持 ※保持しておくことが望ましい監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば、だれがどのような操作を行ったかの記録）、教育受講者一覧表等が考えられる。

③個人データの取扱状況を一覧できる手段の整備をする上で望まれる事項

	個人データについて、取得する項目、通知した利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取り扱いに必要な情報を記した個人データ取扱台帳の整備
	個人データ取扱台帳の内容の定期的な確認による最新状態の維持

④個人データの安全管理措置の評価、見直しおよび改善をする上で望まれる事項

	監査計画の立案と、計画に基づく監査（内部監査または外部監査）の実施
	監査実施結果の取りまとめと、代表者への報告
	監査責任者から受ける監査報告、個人データに対する社会通念の変化および情報技術の進歩に応じた定期的な安全管理措置の見直しおよび改善

⑤事故または違反への対処をする上で望まれる事項

	事実関係、再発防止策等の公表
	その他、以下の項目等の実施 ア）事実調査、イ）影響範囲の特定、ウ）影響を受ける可能性のある本人および主務大臣等への報告、エ）原因の究明、オ）再発防止策の検討・実施

【個人データの取り扱いに関する規程等に記載することが望まれる事項】

以下、①取得・入力、②移送・送信、③利用・加工、④保管・バックアップ、⑤消去・廃棄という、個人データの取り扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項を列記する。

①取得・入力

ア）作業責任者の明確化	
	個人データを取得する際の作業責任者の明確化
	取得した個人データを情報システムに入力する際の作業責任者の明確化（以下、併せて「取得・入力」という。）
イ）手続の明確化と手続に従った実施	
	取得・入力する際の手続の明確化
	定められた手続による取得・入力の実施
	権限を与えられていない者が立ち入れない建物、部屋（以下「建物等」という。）での入力作業の実施
	個人データを入力できる端末の、業務上の必要性に基づく限定
	個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。）
ウ）作業担当者の識別、認証、権限付与	
	個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定
	IDとパスワードによる認証、生体認証等による作業担当者の識別
	作業担当者に付与する権限の限定
	個人データの取得・入力業務を行う作業担当者に付与した権限の記録
エ）作業担当者およびその権限の確認	
	手続の明確化と手続に従った実施および作業担当者の識別、認証、権限付与の実施状況の確認
	アクセスの記録、保管と、権限外作業の有無の確認

②移送・送信

ア）作業責任者の明確化	
	個人データを移送・送信する際の作業責任者の明確化
イ）手続の明確化と手続に従った実施	
	個人データを移送・送信する際の手続の明確化
	定められた手続による移送・送信の実施
	個人データを移送・送信する場合の個人データの暗号化（例えば、公衆回線を利用して個人データを送信する場合）移送時におけるあて先確認と受領確認（例えば、配達記録郵便等の利用）
	ＦＡＸ等におけるあて先番号確認と受領確認
	個人データを記した文書をＦＡＸ等に放置することの禁止
	暗号鍵やパスワードの適切な管理
ウ）作業担当者の識別、認証、権限付与	
	個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定
	IDとパスワードによる認証、生体認証等による作業担当者の識別
	作業担当者に付与する権限の限定（例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない。）
	個人データの移送・送信業務を行う作業担当者に付与した権限の記録
エ）作業担当者およびその権限の確認	
	手続の明確化と手続に従った実施および作業担当者の識別、認証、権限付与の実施状況の確認
	アクセスの記録、保管と、権限外作業の有無の確認

③利用・加工

ア）作業責任者の明確化	
	個人データを利用・加工する際の作業責任者の明確化
イ）手続の明確化と手続に従った実施	
	個人データを利用・加工する際の手続の明確化
	定められた手続による利用・加工の実施
	権限を与えられていない者が立ち入れない建物等での利用・加工の実施
	個人データを利用・加工できる端末の、業務上の必要性に基づく限定
	個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定（例えば、個人データを閲覧だけできる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。）
ウ）作業担当者の識別、認証、権限付与	
	個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定
	IDとパスワードによる認証、生体認証等による作業担当者の識別
	作業担当者に付与する権限の限定（例えば、個人データを閲覧することのみが業務上必要とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない。）
	個人データを利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等）の記録
エ）作業担当者およびその権限の確認	
	手続の明確化と手続に従った実施および作業担当者の識別、認証、権限付与の実施状況の確認
	アクセスの記録、保管と権限外作業の有無の確認

④保管・バックアップ

ア）作業責任者の明確化	
	個人データを保管・バックアップする際の作業責任者の明確化
イ）手続の明確化と手続に従った実施	
	個人データを保管・バックアップする際の手続※の明確化 ※情報システムで個人データを処理している場合は、個人データのみならず、オペレーティングシステム（ＯＳ）やアプリケーションのバックアップも必要となる場合がある。
	定められた手続による保管・バックアップの実施
	個人データを保管・バックアップする場合の個人データの暗号化
	暗号鍵やパスワードの適切な管理
	個人データを記録している媒体を保管する場合の施錠管理
	個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理
	個人データを記録している媒体の遠隔地保管
	個人データのバックアップから迅速にデータが復元できることのテストの実施
	個人データのバックアップに関する各種事象や障害の記録
ウ）作業担当者の識別、認証、権限付与	
	個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定
	IDとパスワードによる認証、生体認証等による作業担当者の識別
	作業担当者に付与する権限の限定（例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない。）
	個人データの保管・バックアップ業務を行う作業担当者に付与した権限（例えば、バックアップの実行、保管庫の鍵の管理等）の記録
エ）作業担当者およびその権限の確認	
	手続の明確化と手続に従った実施および作業担当者の識別、認証、権限付与の実施状況の確認
	アクセスの記録、保管と権限外作業の有無の確認

⑤消去・廃棄

ア）作業責任者の明確化	
	個人データを消去する際の作業責任者の明確化
	個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化
イ）手続の明確化と手続に従った実施	
	消去・廃棄する際の手続の明確化
	定められた手続による消去・廃棄の実施
	権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施
	個人データを消去できる端末の、業務上の必要性に基づく限定
	個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に１回または複数回上書きする。）
	個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する。）
ウ）作業担当者の識別、認証、権限付与	
	個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定
	IDとパスワードによる認証、生体認証等による作業担当者の識別
	作業担当者に付与する権限の限定
	個人データの消去・廃棄を行う作業担当者に付与した権限の記録
エ）作業担当者およびその権限の確認	
	手続の明確化と手続に従った実施および作業担当者の識別、認証、権限付与の実施状況の確認
	アクセスの記録、保管、権限外作業の有無の確認

２．人的安全管理措置

人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

【人的安全管理措置として講じなければならない事項】

①雇用契約時および委託契約時における非開示契約の締結
②従業者に対する教育・訓練の実施

なお、管理者が定めた規程等を守るように監督することについては、法第２１条、本ガイドライン第１１条（従業者の監督）を参照。

【各項目について講じることが望まれる事項】

①雇用契約時および委託契約時における非開示契約の締結をする上で望まれる事項.

	従業者の採用時または委託契約時における非開示契約の締結 ※雇用契約または委託契約等における非開示条項は、契約終了後も一定期間有効であるようにすることが望ましい。
	非開示契約に違反した場合の措置に関する規程の整備 ※個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲およびアクセス条件について契約書等に明記することが望ましい。なお、個人データを取り扱う従業者以外の者には、情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。

②従業者に対する周知・教育・訓練を実施する上で望まれる事項

	個人データおよび情報システムの安全管理に関する従業者の役割および責任を定めた内部規程等についての周知
	個人データおよび情報システムの安全管理に関する従業者の役割および責任についての教育・訓練の実施
	従業者に対する必要かつ適切な教育・訓練が実施されていることの確認

３．物理的安全管理措置

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。

【物理的安全管理措置として講じなければならない事項】

①入退館（室）管理の実施
②盗難等の防止
③機器・装置等の物理的な保護

【各項目について講じることが望まれる事項】

①入退館（室）管理を実施する上で望まれる事項

	個人データを取り扱う業務上の、入退館（室）管理を実施している物理的に保護された室内での実施
	個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置

②盗難等を防止する上で望まれる事項

	離席時の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の机上等への放置の禁止
	離席時のパスワード付きスクリーンセイバ等の起動
	個人データを含む媒体の施錠保管
	氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管
	個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止

③機器・装置等を物理的に保護する上で望まれる事項

	個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護

４．技術的安全管理措置

技術的安全管理措置とは、個人データおよびそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。

【技術的安全管理措置として講じなければならない事項】

①個人データへのアクセスにおける識別と認証
②個人データへのアクセス制御
③個人データへのアクセス権限の管理
④個人データのアクセスの記録
⑤個人データを取り扱う情報システムについての不正ソフトウェア対策
⑥個人データの移送・送信時の対策
⑦個人データを取り扱う情報システムの動作確認時の対策
⑧個人データを取り扱う情報システムの監視

【各項目について講じることが望まれる事項】

①個人データへのアクセスにおける識別と認証を行う上で望まれる事項

	個人データに対する正当なアクセスであることを確認するためにアクセス権限を有する従業者本人であることの識別と認証（例えば、IDとパスワードによる認証、生体認証等）の実施 ※IDとパスワードを利用する場合には、パスワードの有効期限の設定、同一または類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗したIDを停止する等の措置を講じることが望ましい。
	個人データへのアクセス権限を有する各従業者が使用できる端末またはアドレス等の識別と認証（例えば、MACアドレス認証、IPアドレス認証、電子証明書や秘密分散技術を用いた認証等）の実施

②個人データへのアクセス制御を行う上で望まれる事項

	個人データへのアクセス権限を付与すべき従業者数の最小化
	識別に基づいたアクセス制御（パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。） 従業者に付与するアクセス権限の最小化
	個人データを格納した情報システムへの同時利用者数の制限
	個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等）
	個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定）
	個人データにアクセス可能なアプリケーションの無権限利用の防止（例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる従業者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等） ※情報システムの特権ユーザーであっても、情報システムの管理上個人データの内容を知らなくてもよいのであれば、個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。 ※特権ユーザーに対するアクセス制御については、例えば、トラステッドＯＳやセキュアＯＳ、アクセス制御機能を実現する製品等の利用が考えられる。
	個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ウェブアプリケーションのぜい弱性有無の検証）

③個人データへのアクセス権限の管理を行う上で望まれる事項

	個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。）
	個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施

④個人データへのアクセスの記録を行う上で望まれる事項

	個人データへのアクセスや操作の成功と失敗の記録（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）
	採取した記録の漏えい、滅失およびき損からの適切な保護 ※個人データを取り扱う情報システムの記録が個人情報に該当する場合があることに留意する。

⑤個人データを取り扱う情報システムについて不正ソフトウェア対策を実施する上で望まれる事項

	ウイルス対策ソフトウェアの導入
	オペレーティングシステム（ＯＳ）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用
	不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）

⑥個人データの移送（運搬、郵送、宅配便等）・送信時の対策の上で望まれる事項

	移送時における紛失・盗難が生じた際の対策（例えば、媒体に保管されている個人データの暗号化）
	盗聴される可能性のあるネットワーク（例えば、インターネットや無線ＬＡＮ等）で個人データを送信（例えば、本人および従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化

⑦個人データを取り扱う情報システムの動作確認時の対策の上で望まれる事項

	情報システムの動作確認時のテストデータとして個人データを利用することの禁止
	情報システムの変更時に、それらの変更によって情報システムまたは運用環境のセキュリティが損なわれないことの検証

⑧個人データを取り扱う情報システムの監視を行う上で望まれる事項

	個人データを取り扱う情報システムの使用状況の定期的な監視
	個人データへのアクセス状況（操作内容も含む。）の監視 ※ 個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。

ダイレクト・メールの利用に関する
個人情報保護ガイドライン

発　行　日　平成 16 年 12 月 28 日
編集・発行　社団法人　日本ダイレクト・メール協会
〒106-0041 東京都港区麻布台 1-9-14
ランドコム麻布台 4F
TEL(03)3584-3447㈹　FAX(03)3584-3909
ホームページアドレス（URL）http://www.jdma.or.jp
Eメールアドレス　webmaster@jdma.or.jp