「個人情報の保護に関する法律についてのガイドライン」及び
「個人データの漏えい等の事案が発生した場合等の対応について」
に関するＱ＆Ａより（抜粋）

※本書は、「『個人情報の保護に関する法律についてのガイドライン』及び『個人データの漏えい等の事案が発生した場合等の対応について』に関するＱ＆Ａ」から、基本的な項目を抜粋したものです。

※より詳しい内容をお知りになりたい方は、同Ｑ＆Ａをご参照下さい。

目次

１　ガイドライン（通則編）

１-１ 定義

（個人情報）

Ｑ１－３　住所や電話番号だけで個人情報に該当しますか。

Ａ１－３　個別の事例ごとに判断することになりますが、他の情報と容易に照合することにより特定の個人を識別することができる場合、当該情報とあわせて全体として個人情報に該当することがあります。

（個人情報）

Ｑ１－５　新聞やインターネットなどで既に公表されている個人情報は、個人情報保護法で保護されるのですか。

Ａ１－５　公知の情報であっても、その利用目的や他の個人情報との照合など取扱いの態様によっては個人の権利利益の侵害につながるおそれがあることから、個人情報保護法では、既に公表されている情報も他の個人情報と区別せず、保護の対象としています。

（個人情報）

Ｑ１－７　個人情報に該当しない事例としては、どのようなものがありますか。

Ａ１－７　次のような事例が考えられます。

事例１）企業の財務情報等、法人等の団体そのものに関する情報（団体情報）

事例２）統計情報（複数人の情報から共通要素に係る項目を抽出して同じ分類ごとに集計して得られる情報）

（個人情報）

Ｑ１－９　顧客との電話の通話内容は個人情報に該当しますか。また、通話内容を録音している場合、録音している旨を相手方に伝えなければなりませんか。

Ａ１－９　通話内容から特定の個人を識別することが可能な場合には個人情報に該当します。個人情報に該当する場合、個人情報保護法上は、利用目的を通知又は公表する義務はありますが、録音していることについて伝える義務まではありません。

（個人情報）

Ｑ１－17　顧客情報のみでなく、従業員に関する情報も個人情報保護法の規律に従って取り扱う必要がありますか。

Ａ１－17　従業員に関する情報であっても、法第２条第１項の定義に該当する場合には、個人情報に該当するため、同法の規律に従って取り扱う必要があります。

（個人識別符号）

Ｑ１－22　携帯電話番号やクレジットカード番号は個人識別符号に該当しますか。

Ａ１－22　携帯電話番号やクレジットカード番号は、様々な契約形態や運用実態があり、およそいかなる場合においても特定の個人を識別することができるとは限らないこと等から、個人識別符号に位置付けておりません。

　なお、このような番号も、氏名等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場合には、個人情報に該当します。

（個人情報データベース等）

Ｑ１－38　防犯カメラやビデオカメラなどで記録された映像情報は、本人が判別できる映像であれば、個人情報データベース等に該当しますか。

Ａ１－38　本人が判別できる映像情報であれば、個人情報に該当しますが、特定の個人情報を検索することができるように「体系的に構成」されたものでない限り、個人情報データベース等には該当しないと解されます。すなわち、記録した日時について検索することは可能であっても、特定の個人に係る映像情報について検索することができない場合には、個人情報データベース等には該当しないと解されます。

（個人情報取扱事業者）

Ｑ１－46　個人情報を取り扱う件数が少ない事業者も個人情報取扱事業者に該当しますか。

Ａ１－46　個人情報データベース等を事業の用に供している者であれば、当該個人情報データベース等を構成する個人情報によって識別される特定の個人の数の多寡にかかわらず、個人情報取扱事業者に該当します。

　なお、平成 27 年改正の施行（平成 29 年５月 30 日）前においては、5000 人分以下の個人情報しか取り扱っていない者は、個人情報取扱事業者から除外されていましたが、施行後はこれらの者も個人情報取扱事業者に該当することとなりますので、注意が必要です。

（個人情報取扱事業者）

Ｑ１－48　従業者に関する個人情報データベース等しか保有していない場合であっても、個人情報取扱事業者に該当しますか。

Ａ１－48　取り扱っている個人情報が従業者の個人情報のみであっても、個人情報データベース等を事業の用に供している者は、個人情報取扱事業者に該当します。

（個人情報取扱事業者）

Ｑ１－50　NPO 法人や自治会・町内会、同窓会、PTA のような非営利の活動を行っている団体も、個人情報取扱事業者として、個人情報保護法の規制を受けるのですか。

Ａ１－50　個人情報保護法における「事業」とは、一定の目的をもって反復継続して遂行される同種の行為であって、かつ社会通念上事業と認められるものをいい、営利・非営利の別は問いません。したがって、非営利の活動を行っている団体であっても、個人情報データベース等を事業の用に供している場合は、個人情報取扱事業者に該当します。NPO 法人や自治会・町内会、同窓会、PTA のほか、サークルやマンション管理組合なども個人情報取扱事業者に該当し得ます。

（本人の同意）

Ｑ１－56　本人に対して、一定期間内に回答がない場合には同意したものとみなす旨の電子メールを送り、当該期間を経過した場合に、本人の同意を得たこととすることはできますか。

Ａ１－56　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方法によらなければなりません。したがって、一定期間回答がなかったことのみをもって、一律に本人の同意を得たものとすることはできません。

1－2 個人情報の利用目的（法第 15 条～第 16 条、第 18 条第３項関係）

（利用目的の特定）

Ｑ２－１　個人情報取扱事業者は、個人情報の利用目的を「できる限り特定しなければならない」とされていますが、どの程度まで特定する必要がありますか。

Ａ２－１　利用目的を「できる限り」特定するとは、個人情報取扱事業者が、個人情報をどのような目的で利用するかについて明確な認識を持つことができ、本人にとっても、自己の個人情報がどのような事業の用に供され、どのような目的で利用されるのかが、一般的かつ合理的に想定できる程度に特定するという趣旨です。

　このため、特定される利用目的は、具体的で本人にとって分かりやすいものであることが望ましく、例えば、単に「お客様のサービスの向上」等のような抽象的、一般的な内容を利用目的とすることは、できる限り具体的に特定したことにはならないと解されます。

1－3 個人情報の取得（法第 17 条・第 18 条関係）

（適正取得）

Ｑ３－２　名簿業者から個人の名簿を購入することは禁止されていますか。また、不正取得された名簿をそれと知らずに購入した場合は、どうですか。

Ａ３－２　名簿業者から個人の名簿を購入すること自体は禁止されていませんが、その購入に際しては、適正取得（法第 17 条第１項）や第三者提供を受ける際の確認・記録義務（法第 26 条）が適用される点に留意する必要があります。

　具体的には、名簿の購入の際、相手方が個人データを取得した経緯などを確認・記録す

る必要があり、その結果、相手方が不正の手段により個人データを取得したことを知り又は容易に知ることができたにもかかわらず当該個人データを取得する場合、法第 17 条第１項に違反するおそれがあります。

特に、平成 27 年改正の施行（平成 29 年５月 30 日）以降は、一般的に名簿業者はオプトアウト規定による届出が必要となるため（法第 23 条第３項）、個人情報保護委員会のホームページ上で、当該名簿業者が届出をしていることを確認する必要があると解されます。

（適正取得）

Ｑ３－４　個人情報を含む情報がインターネット等により公にされている場合、①当該情報を単に画面上で閲覧する場合、②当該情報を転記の上、検索可能な状態にしている場合、③当該情報が含まれるファイルをダウンロードしてデータベース化する場合は、それぞれ「個人情報を取得」していると解されますか。

Ａ３－４　個人情報を含む情報がインターネット等により公にされている場合、それらの情報を①のように単に閲覧するにすぎない場合には「個人情報を取得」したとは解されません。一方、②や③のようなケースは、「個人情報を取得」したと解し得るものと考えられます。

1-4 個人データの管理（法第 19 条～第 22 条関係）

（データ内容の正確性の確保等）

Ｑ４－２　取得した個人情報は、いつ廃棄しなければなりませんか。

Ａ４－２　個人情報保護法では、個人情報の保存期間や廃棄すべき時期について規定していません。もっとも、個人情報取扱事業者は、その取扱いに係る個人データを利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければなりません（法第 19 条）。

（データ内容の正確性の確保等）

Ｑ４－３　「遅滞なく消去する」とは、具体的にどのような期間で消去することを求めていますか。

Ａ４－３　「遅滞なく」が示す具体的な期間は、個人データの取扱状況等により異なり得ますが、業務の遂行上の必要性や引き続き当該個人データを保管した場合の影響等も勘案し、必要以上に長期にわたることのないようにする必要があると解されます。他方で、事業者のデータ管理のサイクル等、実務上の都合に配慮することは認められます。

（従業者の監督）

Ｑ４－５　町内会やマンション管理組合等において、監督が必要となる「従業者」には、どのような者が該当しますか。

Ａ４－５　町内会やマンション管理組合等の形態や管理の実態にもよりますが、例えば、町内会やマンション管理組合の運営を担う理事等は、個人情報保護法における「従業者」に該当するものと考えられます。

1-5 個人データの第三者への提供（法第 23 条～第 26 条関係）

（第三者提供の制限の原則）

Ｑ５－２　会社の他の部署へ個人データを提供する場合、あらかじめ本人の同意を得る必要はありますか。

Ａ５－２　同一事業者内での個人データの提供は、「第三者提供」には該当しないため、第三者提供に関する本人の同意は必要ありません。ただし、他の部署によって、当初特定した利用目的の達成に必要な範囲を超えて個人情報が利用される場合には、あらかじめ、目的外利用に関する本人の同意を得る必要があります（法第 16 条第１項）。

（第三者提供の制限の原則）

Ｑ５－９　第三者提供の同意を得るに当たり、提供先の氏名又は名称を本人に明示する必要はありますか。

Ａ５－９　提供先を個別に明示することまでが求められるわけではありません。もっとも、想定される提供先の範囲や属性を示すことは望ましいと考えられます。

（第三者提供の制限の原則）

Ｑ５－12　第三者から、当社を退職した従業者に関する在籍確認や勤務状況等について問合せを受けていますが、当該問合せに答えることはできますか。

Ａ５－12　退職した従業者に関する在籍状況や勤務状況等が個人データ（個人情報データベース等を構成する個人情報）になっている場合、問合せに答えることは個人データの第三者提供に該当し、本人の同意がある場合や第三者提供制限の例外事由に該当する場合を除いて、第三者に提供することはできません。

（第三者提供の制限の原則）

Ｑ５－17　刑事訴訟法第 197 条第２項に基づき、警察から顧客に関する情報について照会があった場合、顧客本人の同意を得ずに回答してもよいですか。同法第 507 条に基づき、検察官から裁判の執行に関する照会があった場合はどうですか。

Ａ５－17　警察や検察等の捜査機関からの照会（刑事訴訟法第 197 条第２項）や、検察官及び裁判官等からの裁判の執行に関する照会（同法第 507 条）に対する回答は、「法令に基づく場合」（法第 23 条第１項第１号）に該当するため、これらの照会に応じて個人情報を提供する際に本人の同意を得る必要はありません。要配慮個人情報を提供する際も同様です。

　なお、これらの照会は、いずれも、捜査や裁判の執行に必要な場合に行われるもので、相手方に回答すべき義務を課すものと解されており、また、上記照会により求められた顧

客情報を本人の同意なく回答することが民法上の不法行為を構成することは、通常考えにくいため、これらの照会には、一般に回答をすべきであると考えられます。ただし、本人との間の争いを防止するために、照会に応じ警察等に対し顧客情報を提供する場合には、当該情報提供を求めた捜査官等の役職、氏名を確認するとともに、その求めに応じ提供したことを後日説明できるようにしておくことが必要と考えられます。

（第三者に該当しない場合）

Ｑ５－33　個人情報取扱事業者が、個人データを含む電子データを取り扱う情報システムに関して、クラウドサービス契約のように外部の事業者を活用している場合、個人データを第三者に提供したものとして、「本人の同意」（法第 23 条第１項柱書）を得る必要がありますか。または、「個人データの取扱いの全部又は一部を委託」（法第 23 条第５項第１号）しているものとして、法第 22 条に基づきクラウドサービス事業者を監督する必要がありますか。

Ａ５－33　クラウドサービスには多種多様な形態がありますが、クラウドサービスの利用が、本人の同意が必要な第三者提供（法第 23 条第１項）又は委託（法第 23 条第５項第１号）に該当するかどうかは、保存している電子データに個人データが含まれているかどうかではなく、クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかどうかが判断の基準となります。

当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合には、当該個人情報取扱事業者は個人データを提供したことにはならないため、「本人の同意」を得る必要はありません。

また、上述の場合は、個人データを提供したことにならないため、「個人データの取扱いの全部又は一部を委託することに伴って・・・提供される場合」（法第 23 条第５項第１号）にも該当せず、法第 22 条に基づきクラウドサービス事業者を監督する義務はありません。

当該クラウドサービス提供事業者が当該個人データを取り扱わないこととなっている場合の個人情報取扱事業者の安全管理措置の考え方についてはＱ５－34 参照。

当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合とは、契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等が考えられます。

なお、法第 24 条との関係についてはＱ９－５参照。

１-６ 保有個人データに関する事項の公表等、保有個人データの開示・訂正等・利用停止等（法第 27 条～第 34 条関係）、個人情報の取扱いに関する苦情処理（法第 35 条関係）

（保有個人データの開示）

Ｑ６－８　本人から自分の個人情報の取得元の開示を請求された場合には、どのように対応すればよいですか。

Ａ６－８　個人情報保護法上、本人に個人情報の取得元を明らかにすることを義務付ける規定はありません。

ただし、個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならないとされていますので（法第 35 条第１項）、まずは苦情相談窓口等において相談に対応することが考えられます。

なお、保有個人データ自体に取得元に関する情報が含まれている場合であって、法第 28 条第１項に基づく開示の請求を受けたときは、原則として開示することになります。

（保有個人データの訂正等）

Ｑ６－12　会社の採用面接で不採用にした応募者から、当社に提出された履歴書の返却を求められていますが、個人情報取扱事業者として、返却に応じなければなりませんか。

Ａ６－12　個人情報保護法では、本人からの請求による保有個人データの削除（法第 29 条）、保有個人データの利用の停止又は消去（法第 30 条）に関する規定は定められていますが、履歴書等の受け取った書類を返還する義務は規定されていません。そのため、個人情報保護法上、提出された履歴書を返却する義務はありません。

なお、法第 19 条では、個人データの消去についての努力義務が明記されていますので、個人情報取扱事業者は、個人データを利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければなりません。

1-7 講ずべき安全管理措置の内容

（全般）

Ｑ７－１　ガイドライン（通則編）（８（別添）講ずべき安全管理措置の内容）に示されている項目を全て講じないと違法になりますか。

Ａ７－１　ガイドライン（通則編）では、講じなければならない措置及び当該措置を実践するための手法の例等を示しています。

「講じなければならない措置」として示している内容については、全ての個人情報取扱事業者において講じていただく必要がありますが、これを実践するための具体的な手法については、個人データが漏えい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、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、必ずしもガイドライン（通則編）で示す例示の内容の全てを講じなければならないわけではなく、また、適切な手法は例示の内容のみに限定されるものではありません。

（全般）

Ｑ７－５　「中小規模事業者」も、大企業と同等の安全管理措置を講じなくてはいけませんか。

Ａ７－５　法第 20 条により、個人情報取扱事業者は、取り扱う個人データの安全管理のために必要かつ適切な措置を講じなければなりません。

ただし、安全管理措置を講ずるための具体的な手法については、個人データが漏えい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、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、中小規模事業者において、必ずしも大企業と同等の安全管理措置を講じなければならないわけではありません。ガイドライン（通則編）「８（別添）講ずべき安全管理措置の内容」に記載した「中小規模事業者における手法の例示」等を参考に、具体的な措置の内容を検討してください。

（全般）

Ｑ７－７　標的型メール攻撃や、その他不正アクセス等による個人データの漏えい等の被害を防止するために、安全管理措置に関して、どのような点に注意すればよいですか。

Ａ７－７　ガイドライン（通則編）に記載されている技術的安全管理措置の各項目を遵守することや、それらについて従業者に対して必要な研修・注意喚起を行うことに加え、次のような措置を講ずることが考えられます。

〇不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用すること。

〇巧妙化する攻撃の傾向を把握し、適宜必要な対策を従業者に周知すること。

〇個人データを端末に保存する必要がある場合、パスワードの設定又は暗号化により秘匿すること（なお、データの暗号化又はパスワードによる保護に当たっては、不正に入手した者が容易に解読できないように、暗号鍵及びパスワードの運用管理、パスワードに用いる文字の種類や桁数等の要素を考慮することも有効な取組と解されます）。

また、独立行政法人情報処理推進機構（IPA）等がホームページで公表しているセキュリティ対策等を参考にすることも考えられます。

（組織的安全管理措置）

Ｑ７－９　「個人データの取扱状況を確認する手段の整備」に関して、いわゆる「個人情報取扱台帳」のようなものを作成しなければいけませんか。

Ａ７－９　この項目について、講じていただく必要があるのは、個人データの取扱状況を確認できるように手段を整備することであるため、いわゆる「個人情報取扱台帳」を作成することが義務付けられているわけではありません。

ただし、個人情報取扱事業者において取り扱っている個人データとしてどのようなものがあるかを明確化することは、個人データの取扱状況を把握するに当たって有効な取

組であると考えられます。

（人的安全管理措置）

Ｑ７－13　「従業者の教育」としての研修は、全従業者を一堂に集めて講義形式で行う必要がありますか。

Ａ７－13　個人データの安全管理に関して留意すべき事項は、事業の規模及び性質、取り扱う個人データの性質・量等によって異なり得ますので、研修の形式も個人情報取扱事業者ごとに異なり得るものと考えられます。全従業者を対象とした講義形式による研修も含まれ得ますが、これに限られるものではなく、部署ごとに個人データの取扱いに関する責任者からの講話形式、ｅラーニング形式、標的型メールを疑似体験する形での訓練形式など、様々な形式が考えられます。

（物理的安全管理措置）

Ｑ７－14　「個人データを取り扱う区域の管理」に関して、個人データを取り扱う場所は、全て厳格な入退室管理を実施する必要がありますか。

Ａ７－14　個人データを取り扱う区域の管理として、常に入退室管理の実施が求められるわけではありませんが、個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域（管理区域）については、入退室管理の実施、承認されていない記録媒体やカメラ等の持込の制限等が有効な取組と考えられます。

（物理的安全管理措置）

Ｑ７－15　「座席配置の工夫」「のぞき込みを防止する措置」「個人データを取り扱うことのできる従業者及び本人以外が容易に個人データを閲覧等できないような措置」とは、例えばどのような措置が該当しますか。

Ａ７－15　具体的には、以下のような措置が該当すると考えられます。

〇個人データの取扱いを、個人データを取り扱う権限が付与されていない者の往来が少ない場所で実施すること

〇個人データをパソコンで取り扱う場合、離席時にパスワード付スクリーンセーバーの起動又はコンピュータのロック等で閲覧できないようにすること

〇個人データを記した書類、媒体、携帯可能なコンピュータ等を机上、社内等に放置しないこと

１－８ その他

（勧告、命令、緊急命令）

Ｑ８－１　個人情報取扱事業者等が個人情報保護法に違反した場合、どのような措置が採られるのですか。

Ａ８－１　個人情報取扱事業者等が、個人情報保護法の義務規定に違反し、不適切な個人情報の取扱いを行っている場合には、個人情報保護委員会（※）が、必要に応じて、事業者に対して報告徴収・立入検査を実施し（法第 40 条）、指導・助言を行い（法第 41 条）、ま

た、勧告・命令を行う（法第 42 条）ことができます。個人情報保護委員会の命令に個人情報取扱事業者等が従わなかった場合や、個人情報保護委員会からの報告徴収・立入検査に応じなかった場合、報告徴収に対して虚偽の報告をした場合等には、罰則（30 万円以下の罰金）の対象になります。

なお、個人情報取扱事業者若しくはその従業者又はこれらであった者が、その業務に関して取り扱った個人情報データベース等（その全部又は一部を複製し、又は加工したものを含む。）を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、法第 83 条により刑事罰（１年以下の懲役又は 50 万円以下の罰金）が科される可能性があります。

（※）法第 44 条に基づく権限の委任が行われた場合には、事業所管大臣（各省庁）が報告徴収・立入検査を実施することとなります。

２　ガイドライン（外国にある第三者への提供編）

Ｑ９－５　外国にあるサーバに個人データを含む電子データを保存することは外国にある第三者への提供に該当しますか。

Ａ９－５　当該サーバの運営事業者が、当該サーバに保存された個人データを取り扱わないこととなっている場合には、外国にある第三者への提供（法第 24 条）に該当しません。

当該サーバに保存された個人データを取り扱わないこととなっている場合とは、契約条項によって当該事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等が考えられます（Ｑ５－33 参照）。

３　ガイドライン（第三者提供時の確認・記録義務編）

３－１ 確認・記録義務の適用対象　（略）

３－２ 確認義務、記録義務

Q10－25　記録を作成するに当たって、台帳のようなものを用意する必要はありますか。

A10－25　既存の契約書などで記録事項を充たしている場合は、それらが記録として認められます。したがって、事業者は、別途、台帳のようなものを用意する必要はありませんが、保存義務を履行するために、明確にする必要があります。

Q10－26　個人データを提供先にデータ伝送している場合、伝送日時、伝送先などのログを記録とすることはできますか。

A10－26　ログを記録とすることは認められます。

Q10－27　継続的に又は反復して個人データを授受することを内容とする基本契約書に加えて、当該基本契約書に付帯する資料などをあわせて、施行規則第 12 条第２項・第 16 条第２項に基づく記録とすることはできますか。

A10－27　最初に基本契約書に記録を作成し、継続的に又は反復して個人データを授受する対象期間内に、随時、提供される個人データによって識別される本人の氏名に係る記録を、別途、当該基本契約書に付帯する資料などをもって作成する方法も認められるものと考えられます。

４　ガイドライン（匿名加工情報編）　（略）
５　個人データの漏えい等事案対応告示　（略）
６　その他　（略）