ビルメンテナンス業における
個人情報保護に関するガイドライン

平成 17 年 5 月

社団法人 全国ビルメンテナンス協会

はじめに

企業各社においては、個人情報・顧客情報は企業における重要な情報資産であり、企業戦略の核となっています。一方、飛躍的に進歩する IT（情報通信技術）、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おり、個人情報漏えいや住民基本台帳データの悪用など、個人情報に関わる事件がニュースで取り上げられる機会が増えています。このような事件は、個人の権利利益を害するだけでなく、企業にとっても個人情報保護法の法律違反の責任を問われたり、社会的信用の失墜、取引機会の喪失、顧客離れ、損害賠償が発生するなど多大な影響を受けます。したがって個人情報の取扱いと活用は戦略実現を左右するとともに、組織の存亡にも関わるものともなります。

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」又は単に「法」という。）が平成 17 年 4 月から全面施行されました。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、社団法人全国ビルメンテナンス協会（以下「全国協会」という。）では、個人情報保護法の趣旨を踏まえながら、47 都道府県ビルメンテナンス協会の所属会員企業（以下「ビルメンテナンス会社」という。）が取扱う個人情報の適切・適正な保護のための基礎として『ビルメンテナンス業における個人情報保護に関するガイドライン』（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』及び、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 Q15001：1999）を基にして策定したものです。個人情報保護法に基づいた順守事項を含んでいますので、従わない場合には主務大臣の指導・勧告・命令がなされ、勧告措置及び命令に反したとき、又は報告命令による報告をせず虚偽報告をしたときには、罰則の適用を問われる場合があります。

ビルメンテナンス会社は本ガイドラインを参考に、各社の業務内容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お願い申し上げます。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を講じていただきたくお願いいたします。また、本ガイドラインは、ビルメンテナンス会社以外であっても、ビルメンテナンス業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。

なお、本ガイドラインは今後の運用を経て改訂を行い、平成 18 年 1 月に改訂版ガイドラインを公表することを予定しています。

平成 17 年 5 月

社団法人 全国ビルメンテナンス協会

会 長　狩 野 伸 彌

※ プライバシーマーク制度について

プライバシーマーク制度は、財団法人日本情報処理開発協会が 1998 年に創設し、JIS Q 15001 に適合したマネジメントシステムを構築している企業に認証マークの使用を許可する第三者認証の制度です。個人情報保護の取り組みに対する第三者機関による認定を取得することで個人情報の取扱いに関する社内体制やセキュリティ対策を整備できるほか、個人情報保護やセキュリティに対する積極的な姿勢を対外的にアピールすることができます。認定に当っては個人情報保護法に対応しているレベルよりも高いレベルを要求されています。平成 17 年 5 月現在、1,400 社以上が認定を受けています。

（参考）　コンプライアンス（法令等順守）のための社内体制構築

個人情報保護法を順守するために、また、プライバシーの権利を侵害したとして責任を負うことにならないためにも、企業各社は、コンプライアンスのための社内体制を構築する必要があります。そうすることによって、企業として顧客から信頼を勝ち取り、競争力を維持、強化することもできます。その際、場当たり的なその場しのぎの対応を実施するだけでは不十分となるおそれがありますので、経営陣を巻き込んだマネジメントシステムを構築することが有益です。

マネジメントシステムとは、計画（Plan）を立案し、それを実施（Do）して、計画どおり実施されているか監査し（Check）、監査の結果や経営環境の変化などを踏まえて不足する点が明らかになれば改善（Act）していく、という一連の流れを繰り返すことによって、コンプライアンスのレベルを継続的に向上させていく（スパイラルアップ）仕組みであり、頭文字を取って「PDCA サイクル」とも呼ばれています。

わが日本では個人情報保護のためのマネジメントシステムの規格として JIS Q15001 が 1999 年に定められており、これに基づく第三者評価制度として「プライバシーマーク制度」があります。

まず、どのようなポリシーで個人情報を取扱うのかということを簡潔に整理した「個人情報保護方針」を取締役会などで定め、自社のウェブサイトなどを利用して対外的に公表します。この方針を実現するために、この法律の内容などに照らし、基本的な方向性を明確化する目的で基本規程を定め、さらに詳細化した種々の社内規程、さらに詳細な運用手順書やフォームなどを策定することになります。

個人情報保護を図るための社内組織作りも重要です。経営陣が指名、任命した統括的な個人情報保護管理者を中心に社内体制作りを行い、実施していくことになります。社内の各関係部署から担当者を集めて対応のための社内委員会を設置することも有用です。

個人情報保護策の立案に際しては、社内でどのような個人情報が取扱われているのかについて洗い出し、この法律との関係でどのような措置が必要なのかという点を明確化する必要があります。

個人情報に関わる従業者全員に理解してもらうために、教育研修を社内規程で定め、これを実施していくことが不可欠となります。それは、安全管理措置に関する従業者に対する監督責任（法第 21 条）を果たすことにもつながります。

さらに、監査責任者を選任し、監査の実施体制、監査計画、監査結果の報告などを社内規程として定め、監査計画に基づき実施した監査結果に基づき、継続的改善に努めるべきことになります。

以上のとおり、コンプライアンスの対応には極めて多くの工数、作業を要することを考えると、できる限り早期に対応に着手することが望まれます。

ビルメンテナンス業における個人情報保護に関するガイドライン

目　次

はじめに

ビルメンテナンス業における個人情報保護に関するガイドライン　･････････････　7
　第一章　総則　･･　9
　第二章　指針　･･　12
　　第一節　個人情報の取扱いに関する事項　･･････････････････････････････　12
　　第二節　個人データの取扱いに関する事項　････････････････････････････　14
　　第三節　保有個人データの取扱いに関する事項　････････････････････････　18
　　第四節　苦情の処理に関する事項　････････････････････････････････････　20
　　第五節　コンプライアンス・プログラムに関する事項　･･････････････････　20
　　第六節　その他の事項　･･　22
　第三章　事例　･･　23
　第四章　安全管理措置として講じることが望まれる具体的事項　･････････････　31

ビルメンテナンス業界を取り巻く個人情報問題についてのＱ＆Ａ　･････････････　43

資料編　･･　59
　個人情報の保護に関する法律　･･　61
　雇用管理に関する個人情報の適正な取扱いを確保するために
　事業者が講ずべき措置に関する指針　･･････････････････････････････････　68
　雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての
　留意事項について　･･　69

　参考法令・ガイドライン一覧　･･　71

＜注＞　ガイドライン本文中、（事例○○）とあるのは、第三章「事例」の各番号に対応している。

ビルメンテナンス業における
個人情報保護に関するガイドライン

ビルメンテナンス業における個人情報保護に関するガイドライン

第一章　総　則

（目的）

第一条　このガイドラインは、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）及びその他関係法令に基づき、ビルメンテナンス業における個人情報の適切な取扱いに関する具体的な指針として定めるものであり、これにより個人情報の適切な保護とビルメンテナンス業の健全な発展に資することを目的とするものである。

（適用範囲）

第二条　このガイドラインは、社団法人全国ビルメンテナンス協会（以下「全国協会」という。）が 47 都道府県ビルメンテナンス協会の所属会員企業（以下「ビルメンテナンス会社」という。）におけるビルメンテナンス業に関する個人情報の取扱いに適用する。

ただし、雇用管理に関する情報に関しては、平成 16 年 7 月 1 日厚生労働省告示第 259 号「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」によるものとする。

なお、以下のガイドライン等も参考とする。

一　マンション管理業務に関しては、「マンション管理業における個人情報保護ガイドライン」（社団法人高層住宅管理業協会・平成 17 年 2 月発行）

二　警備業務に関しては、「警備業における個人情報の保護に関するガイドライン」（社団法人全国警備業協会・平成 17 年 1 月発行）

三　派遣業務に関しては、「労働者派遣事業関係業務取扱要領」（厚生労働省発行）、「機密情報保護に関するガイドライン」（社団法人日本人材派遣協会・平成 16 年 10 月発行、※本ガイドラインは現在、日本人材派遣協会会員のみ配布）

（定義）

第三条　このガイドラインにおいて使用する用語の定義は、当該各号に定めるところによる。

一　「個人情報」　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、又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。（法第 2 条第 1 項関連）（事例 1、2）

二　「個人情報データベース等」　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。（法第 2 条第 2 項関連）（事例 3、4）

イ）　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

ロ）　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

三　「個人情報取扱事業者」　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、ここでいう「事業の用に供している」の「事業」とは、一定の目的を持って反復継続して遂行される同種の行為であって、かつ一般社会通念上事業と認められるものをいい、営利事業のみを対象とするものではない。個人であっても個人情報取扱事業者に該当し得る。（法第 2 条第 3 項関連）

四　「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をいう。（法第 2 条第 4 項関連）（事例 5、6）

五　「保有個人データ」　ビルメンテナンス会社が、開示、内容の訂正、追加又は削除、利用の停止、消去及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。（法第 2 条第 5 項関連）

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

ロ）　当該個人データの存否が明らかになることにより、違法又は不当な行為を助長し、又は誘発するおそれがあるもの

ハ）　当該個人データの存否が明らかになることにより、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

ニ）　6 ヶ月以内に消去することとなるもの

六　「本人」　個人情報によって識別される、又は識別され得る特定の個人をいう。（法第 2 条第 6 項関連）

七　「本人に通知」　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。（事例 7）

八　「公表」　広く一般に自己の意思を知らせることをいい、国民一般その他不特定多数の人々が知ることができるように発表することをいう。（事例 8）

九　「本人に対し、その利用目的を明示」　本人に対し、その利用目的を明確に示すことをいう。（事例 9）

十　「本人の同意」　本人の個人情報が、ビルメンテナンス会社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（黙示の承諾を含む。）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ビルメンテナンス会社が認識することをいう。（事例 10）

十一　「本人が容易に知り得る状態」　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。（事例 11）

十二　「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。）」　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。（事例 12）

十三　「提供」　個人データを利用可能な状態に置くことをいい、個人データが、物理的に提

供されていない場合であっても、ネットワーク等を利用することにより、個人データを利用できる状態にあれば（利用する権限が与えられていれば)、「提供」に当たる。

十四　「個人情報保護コンプライアンス・プログラム（CP）(以下、単に「コンプライアンス・プログラム」という。)」　事業者が、自ら保有する個人情報を保護するための方針、組織、計画、実施、監査及び見直しを含むマネジメントシステム。

十五　「個人情報管理責任者」　事業者の内部において代表者によって指名された者であって、コンプライアンス・プログラムの実施及び運用に関する責任と権限をもつ者。

十六　「監査責任者」　事業者の代表者によって指名された者であって、公平、かつ、客観的な立場にあり、監査の実施及び報告を行う権限をもつ者。

十七　「従業者」　事業者の役員、及び従業員、派遣契約に基づき派遣されてきている労働者、業務請負契約等に基づき事業者内に常駐する労働者、事業者が雇用するアルバイト、パート等をいう。

第二章　指　針

第一節　個人情報の取扱いに関する事項

（利用目的の特定）

第四条　ビルメンテナンス会社は、個人情報を取扱うに当たっては、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、利用目的を単に抽象的、一般的に特定するのではなく、ビルメンテナンス会社において最終的にどのような目的で個人情報を利用するかを可能な限り具体的に特定する必要がある（法第 15 条第 1 項関連）（事例 13、14）

2　（利用目的の変更）　ビルメンテナンス会社は、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を超えて行ってはならない。（法第 15 条第 2 項関連）（事例 15）

3　（個人情報の特定）　ビルメンテナンス会社は、自ら保有するすべての個人情報を特定するための手順を確立し、維持することが望ましい。ビルメンテナンス会社は、特定した個人情報に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなど）を認識することが望ましい。

（利用目的による制限）

第五条　ビルメンテナンス会社は、利用目的の達成に必要な範囲を超えて、個人情報を取扱う場合は、あらかじめ本人の同意を得なければならない。（法第 16 条関連）（事例 16）

2　ビルメンテナンス会社は、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た場合には、あらかじめ本人の同意を得ないで、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取扱ってはならない。（事例 17）

3　（利用及び提供の原則）　個人情報の利用及び提供は、本人が同意を与えた利用目的の範囲内で行うこととすること。

なお、次に示すいずれかに該当する場合は、本人の同意を必要としない。

一　法令の規定による場合

二　本人又は公衆の生命、健康、財産などの重大な利益を保護するために必要な場合

4　（収集目的の範囲外の利用及び提供の場合の措置）　本人が同意を与えた利用目的の範囲外で個人情報の利用及び提供を行う場合は、少なくとも、第七条第 5 項（本人から直接収集する場合の措置）の第一号～第四号及び第六号に示す事項を書面又はこれに代わる方法によって本人に通知し、事前の本人の同意の下に行うこととすること。

（適正取得）

第六条　ビルメンテナンス会社は、偽り等の不正の手段により個人情報を取得してはならない。

なお、不正の競争の目的で、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（平成 5

年法律第 47 号）第 14 条により刑事罰（3 年以下の懲役又は 300 万円以下の罰金）が科され得る。（法第 17 条関連）（事例 18）

（利用目的の通知又は公表）

第七条　ビルメンテナンス会社は、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、又は公表しなければならない。（法第 18 条第 1 項関連）（事例 19）

2　（直接書面等による取得）　ビルメンテナンス会社は、書面等による記載、ユーザー入力画面への打ち込み等により、直接本人から個人情報を取得する場合には、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。（法第 18 条第 2 項関連）（事例 20）

3　（利用目的の変更）　ビルメンテナンス会社は、社会通念上、本人が想定することが困難でないと認められる範囲内で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、本人に通知するか、又は公表しなければならない。（法第 18 条第 3 項関連）

4　（適用除外）　前 3 項の規定は、次に掲げる場合については、適用しない。（法第 18 条第 4 項関連）

一　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　利用目的を本人に通知し、又は公表することにより当該ビルメンテナンス会社の権利又は正当な利益を害するおそれがある場合

三　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、又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

四　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

5　（本人から直接収集する場合の措置）　本人から直接に個人情報を取得する場合には、本人に対して、少なくとも、次に示す事項又はそれと同等以上の内容の事項を書面若しくはこれに代わる方法によって通知し、本人の同意の下に行うこととすること。

一　ビルメンテナンス会社の内部の個人情報に関する管理者又はその代理人の氏名若しくは職名、及び所属並びに連絡先

二　利用目的

三　個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又は受領者の組織の種類、属性及び個人情報の取扱いに関する契約の有無

四　個人情報の取扱いの委託を行うことが予定される場合には、その旨

五　本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果

六　個人情報の開示を求める権利、及び開示の結果、当該情報が誤っている場合に訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的な方法

6　（本人以外から間接的に収集する場合の措置）　本人以外から間接的に個人情報を取得する場合には、本人に対して、少なくとも、前項の第一号～第四号及び第六号に示す事項を書面又

はこれに代わる方法によって通知し、本人の同意を得ることが望ましい。ただし、次に示すいずれかに該当する場合は、この限りでない。

一　本人からの個人情報の取得時にあらかじめ自己への情報の提供を予定している旨、前項の第三号に従い本人の同意を得ている提供者から取得を行う場合

二　情報処理を委託するなどのために個人情報の取扱いを委託される場合

三　本人の保護に値する利益が侵害されるおそれのない取得を行う場合

第二節　個人データの取扱いに関する事項

（データ内容の正確性の確保）

第八条　ビルメンテナンス会社は、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・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、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。この場合、保有する個人データを一律に又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。（法第 19 条関連）

（安全管理措置）

第九条　ビルメンテナンス会社は、その取扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない。その際、本人の個人データが漏えい、滅失又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、事業の性質及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。

なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じなければならない。（法第 20 条関連）（事例 21）（具体的事項に関しては第四章「安全管理措置として講じることが望まれる具体的事項」参照のこと）

2　ビルメンテナンス会社は、組織的安全管理のために次の各号の事項について措置を講じるものとする。

一　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

二　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

三　個人データの取扱状況を一覧できる手段の整備

四　個人データの安全管理措置の評価、見直し及び改善

五　事故又は違反への対処

3　ビルメンテナンス会社は、人的安全管理のために次の各号の事項について措置を講じるものとする。

一　雇用契約時及び委託契約時における非開示契約の締結

二　従業者に対する教育・訓練の実施

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、第十条（従業者の監督）を

参照。

4　ビルメンテナンス会社は、物理的安全管理のために次の各号の事項について措置を講じるものとする。

一　入退館（室）管理の実施

二　盗難等の防止

三　機器・装置等の物理的な保護

5　ビルメンテナンス会社は、技術的安全管理のために次の各号の事項について措置を講じるものとする。

一　個人データへのアクセスにおける識別と認証

二　個人データへのアクセス制御

三　個人データへのアクセス権限の管理

四　個人データのアクセスの記録

五　個人データを取扱う情報システムについての不正ソフトウェア対策

六　個人データの移送・送信時の対策

七　個人データを取扱う情報システムの動作確認時の対策

八　個人データを取扱う情報システムの監視

（従業者の監督）

第十条　ビルメンテナンス会社は、その従業者に個人データを取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、滅失又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、事業の性質及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。（法第 21 条関連）（事例 22）

2　（教育）　ビルメンテナンス会社は、従業者に適切な教育を行わなければならない。

3　ビルメンテナンス会社は、関連する各部門及び階層においてその従業者に次の事項を自覚させる手順を確立し維持することが望ましい。

一　コンプライアンス・プログラムに適合することの重要性及び利点。

イ）　個人情報保護の重要性及び利点

二　コンプライアンス・プログラムに適合するための役割及び責任。

イ）　個人データ及び情報システムの安全管理に関する従業者の役割及び責任

ロ）　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

三　コンプライアンス・プログラムに違反した際に予想される結果。

イ）　個人データの漏えい、滅失又はき損により予想される本人の損害

ロ）　個人データの漏えい、滅失又はき損により予想される企業リスク

（委託先の監督）

第十一条　ビルメンテナンス会社は、個人データの取扱いの全部又は一部を委託する場合、第九

条に基づく安全管理措置を順守させるよう、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、滅失又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、事業の性質及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。

「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扱に関して、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。

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。（法第 22 条関連）（事例 23）

2　ビルメンテナンス会社は、十分な個人情報の保護水準を満たしている者を委託先として選定する基準を確立することが望ましい。

3　ビルメンテナンス会社は、前項の規定を順守するために次の各号の事項を契約時に明確にし、その保護水準を担保することが望ましい。

一　個人情報に関する秘密保持

二　委託者及び受託者の責任の範囲

三　個人データの安全管理に関する事項

イ）　個人データの漏えい防止、盗用禁止に関する事項

ロ）　委託契約範囲外の加工、利用の禁止

ハ）　委託契約範囲外の複写、複製の禁止

ニ）　委託契約期間

ホ）　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

四　再委託に関する事項

イ）　再委託を行うに当たっての委託者への文書による報告

五　個人データの取扱状況に関する委託者への報告の内容及び頻度

六　契約内容が順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。）

七　契約内容が順守されなかった場合の措置

八　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

4　ビルメンテナンス会社は、前項に従って定めた契約書などの書面又はこれに代わる記録を、個人情報の保有期間にわたって保存することが望ましい。

（個人情報の第三者への提供）

第十二条　ビルメンテナンス会社は、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。（法第 23 条関連）（事例 24、25）

一　法令に基づく場合
二　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
三　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
四　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

2　同意の取得に当たっては、事業の性質及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。

3　（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、第十二条（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。
一　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扱いの全部又は一部を委託する場合（事例 28）
二　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 29）
三　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及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又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。（事例 30、31）

4　ビルメンテナンス会社は、前項第三号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

第三節　保有個人データの取扱いに関する事項

（保有個人データに関する事項の本人への周知）

第十三条　ビルメンテナンス会社は、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。（法第 24 条関連）
一　当該ビルメンテナンス会社の氏名又は名称
二　すべての保有個人データの利用目的
三　保有個人データの利用目的の通知及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、追加又は削除、保有個人データの利用の停止又は消去、保有個人データの第三者への提供の停止の求め（以下「開示等の求め」という。）の手続き
四　保有個人データの取扱いに関する苦情の申出先

2　（保有個人データの利用目的の通知）　ビルメンテナンス会社は、本人から、自己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ときは、遅滞なく、本人に通知しなければならない。ただし、次の各号のいずれかに該当する場合は、この限りでない。

一　前項の規定により当該本人が識別される保有個人データの利用目的が明らかな場合

二　第七条第４項第一号から第三号までに該当する場合

3　ビルメンテナンス会社は、前項の規定に基づき求められた保有個人データの利用目的を通知しない旨を決定したときは、本人に対し、遅滞なく、その旨を通知しなければならない。

（保有個人データの開示）

第十四条　ビルメンテナンス会社は、本人から、自己が識別される保有個人データの開示（存在しないときにはその旨を知らせることを含む。）を求められたときは、本人に対し、書面の交付による方法（開示の求めを行った者が同意した方法があるときはその方法）により、遅滞なく、当該保有個人データを開示しなければならない。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、その全部又は一部を開示しないことができる。（法第 25 条関連）

一　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合（事例 32

二　ビルメンテナンス会社の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 33）

三　他の法令に違反することとなる場合（事例 34）

2　ビルメンテナンス会社は、前項の規定に基づき求められた保有個人データの全部又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、その旨を通知しなければならない。

（保有個人データの訂正等）

第十五条　ビルメンテナンス会社は、当該本人が識別される保有個人データの内容に誤りがあり、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、追加又は削除（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。（法第 26 条関連）（事例 35）

2　ビルメンテナンス会社は、前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、又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。

（保有個人データの利用停止等）

第十六条　ビルメンテナンス会社は、本人から、同意のない目的外利用、不正な取得、又は同意のない第三者提供、の理由により保有個人データの利用の停止、消去又は第三者への提供の停

止（以下「利用停止等」という。）が求められた場合、その求めに理由が有ることが判明した時は、違反を是正するために必要な限度で、遅滞なく、当該措置を行わなければならない。ただし、当該措置を実施するために多額の費用を要する場合その他の当該措置を実施することが困難な場合であって、本人の権利利益を保護するために必要なこれに代わるべき措置をとるときや手続違反である旨の指摘が正しくない場合には、利用停止等を行う必要はない。（法第 27 条関連）

2　ビルメンテナンス会社は、前項の規定に基づき求められた保有個人データの利用停止等を行った場合、又は利用停止等を行わない旨を決定した場合には、遅滞なく、その旨を本人に通知しなければならない。

（理由の説明）

第十七条　ビルメンテナンス会社は、第十三条（保有個人データに関する事項の本人への周知）第 3 項、第十四条（保有個人データの開示）第 2 項、第十五条（保有個人データの訂正等）第 2 項又は第十六条（保有個人データの利用停止等）第 2 項の規定により、本人から求められた措置の全部又は一部についてその措置をとらない旨を通知する場合又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。（法第 28 条関連）

（開示、訂正等、利用停止等の求めに応じる手続き）

第十八条　ビルメンテナンス会社は、開示、訂正等、利用停止等（以下「開示等」という。）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。（法第 29 条関連）

一　開示等の求めの受付先

二　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

三　開示等の求めをする者が本人又はその代理人であることの確認の方法

四　保有個人データの利用目的の通知、又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

2　ビルメンテナンス会社は、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。（事例 36）

3　ビルメンテナンス会社は、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。

（手数料）

第十九条　ビルメンテナンス会社は、保有個人データの利用目的の通知、又は保有個人データの開示を求められたときは、当該措置の実施に関し、手数料を徴収することができる。（法第 30 条関連）

2　ビルメンテナンス会社は、前項の規定により手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない。

3　ビルメンテナンス会社は、前項の規定により手数料の額を定めた場合には、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。

第四節　苦情の処理に関する事項

（苦情の処理）

第二十条　ビルメンテナンス会社は、個人情報の取扱いに関する苦情及び相談の適切かつ迅速な処理に努めなければならない。（法第 31 条関連）

2　ビルメンテナンス会社は、苦情の適切かつ迅速な処理を行うに当たり、苦情処理窓口の設置や苦情処理の手順を定める等必要な体制の整備に努めなければならない。もっとも、無理な要求にまで応じなければならないものではない。

なお、必要な体制の整備に当たっては、日本工業規格 JIS Z9920「苦情対応マネジメントシステムの指針」を参考にすることができる。

第五節　コンプライアンス・プログラムに関する事項

（個人情報保護方針）

第二十一条　ビルメンテナンス会社の代表者は、次の各号を含む個人情報保護方針を定めるとともにこれを実行し維持することが望ましい。ビルメンテナンス会社の代表者は、この方針を文書化し、従業者に周知させるとともに一般の人が入手可能な措置を講じることが望ましい。

一　事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること

二　個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの予防並びに是正に関すること

三　個人情報に関する法令及びその他の規範を順守すること

四　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

（法令及びその他の規範）

第二十二条　ビルメンテナンス会社は、個人情報に関する法令及びその他の規範を特定し、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）

第二十三条　ビルメンテナンス会社は、個人情報を保護するための内部規程を策定し、維持することが望ましい。

２　内部規程は、次の事項を含むことが望ましい。

一　ビルメンテナンス会社の各部門及び階層における個人情報を保護するための権限及び責任の規定

二　個人情報の取得、利用、提供及び管理の規定

三　本人からの個人情報に関する開示、訂正及び削除の規定

四　個人情報保護に関する教育の規定

五　個人情報保護に関する監査の規定

六　内部規程の違反に関する罰則の規定

３　ビルメンテナンス会社は、事業の内容に応じて、コンプライアンス・プログラムが確実に適用されるように内部規程を改定しなければならない。

（計画書）

第二十四条　ビルメンテナンス会社は、内部規程を順守するために必要な教育、監査などの計画を立案し、文書化し、かつ、維持することが望ましい。

（体制及び責任）

第二十五条　コンプライアンス・プログラムを効果的に実施するために役割、責任及び権限を定め、文書化し、かつ、個人情報に関連のある業務にかかわる従業者に周知することが望ましい。

２　ビルメンテナンス会社の代表者は、コンプライアンス・プログラムの実施及び管理に不可欠な人的、組織的、物理的な対応を用意することが望ましい。

３　ビルメンテナンス会社の代表者は、このガイドラインの内容を理解し実践する能力のある管理者をビルメンテナンス会社の内部から指名し、コンプライアンス・プログラムの実施及び運用に関する責任及び権限を他の責任にかかわりなく与え、業務を行わせることが望ましい。

（特定の機微な個人情報の取得）

第二十六条　次の各号に示す内容を含む個人情報の取得、利用又は提供は行わないことが望ましい。ただし、これらの取得、利用又は提供について、明示的な本人の同意、法令に特別の規定がある場合、及び司法手続上必要不可欠である場合は、この限りでない。

一　思想、信条及び宗教に関する事項

二　人種、民族、門地、本籍地（所在都道府県に関する情報を除く）、身体・精神障害、犯罪歴、その他社会的差別の原因となる事項

三　勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項

四　集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項

五　保健医療及び性生活

（コンプライアンス・プログラム文書）

第二十七条　ビルメンテナンス会社は、書面又はこれに代わる方法で、コンプライアンス・プロ

グラムの基本となる要素を記述することが望ましい。

（文書管理）

第二十八条　ビルメンテナンス会社は、このガイドラインが要求するすべての文書を管理することが望ましい。

（監査）

第二十九条　ビルメンテナンス会社は、コンプライアンス・プログラムがこのガイドラインの要求事項と合致していること、及びその運用状況を定期的に監査することが望ましい。

2　監査責任者は、監査を指揮し、監査報告書を作成し、ビルメンテナンス会社の代表者に報告することが望ましい。

3　ビルメンテナンス会社は、監査報告書を管理し、保管することが望ましい。

（ビルメンテナンス会社の代表者による見直し）

第三十条　ビルメンテナンス会社の代表者は、監査報告書及びその他の経営環境などに照らして、適切な個人情報の保護を維持するために定期的にコンプライアンス・プログラムを見直すことが望ましい。

第六節　その他の事項

（報告等）

第三十一条　ビルメンテナンス会社は、個人データの漏えい等が発生した場合は、事実関係を本人に速やかに通知しなくてはならない。

2　ビルメンテナンス会社は、個人データの漏えい等が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表しなくてはならない。

3　ビルメンテナンス会社は、個人データの漏えい等が発生した場合は、その事業内容に応じて、当該事業を所管する省庁に事実関係を報告しなくてはならない。

第三章　事　例

1　個人情報に該当する事例

1．本人の氏名
2．生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位又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
3．防犯カメラに記録された情報等本人が判別できる映像情報
4．特定の個人を識別できるメールアドレス情報（birumen_taro@j-bma.or.jp 等のようにメールアドレスだけの情報の場合であっても、日本の団体である社団法人全国ビルメンテナンス協会に所属するビルメンタロウのメールアドレスであることがわかるような場合等）
5．特定個人を識別できる情報が記述されていなくても、周知の情報を補って認識することにより特定の個人を識別できる情報
6．雇用管理情報（会社が従業員を評価した情報を含む。）
7．個人情報を取得後に当該情報に付加された個人に関する情報（取得時に生存する特定の個人を識別することができなかったとしても、取得後、新たな情報が付加され、又は照合された結果、生存する特定の個人を識別できた場合は、その時点で個人情報となる。）
8．官報、電話帳、職員録等で公にされている情報（本人の氏名等）

2　個人情報に該当しない事例

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）
2．記号や数字等の文字列のみで特定個人の情報であるか否かの区別がつかないメールアドレス情報（例えば、abc012345@ispisp.jp。ただし、他の情報と容易に照合することによって特定の個人を識別できる場合は、個人情報となる。）
3．特定の個人を識別することができない統計情報

3　個人情報データベースに該当する事例

1．電子メールソフトに保管されているメールアドレス帳（メールアドレスと氏名を組み合わせた情報を入力している場合）
2．ユーザーID とユーザーが利用した取引についてのログ情報が保管されている電子ファイル（ユーザーID を個人情報と関連付けて管理している場合）
3．従業員が、名刺の情報を業務用パソコン（所有者を問わない。）の表計算ソフト等を用いて入力・整理し、他の従業員等によっても検索できる状態にしている場合
4．例えば登録カードを、氏名の五十音順など一定の法則に従って整理し、インデックスを付して誰でも容易に検索できるようにファイルしている場合

5．氏名、住所、企業別に分類整理されている市販の人名録

4　個人情報データベースに該当しない事例

1．従業員が、自己の名刺入れについて他人が自由に検索できる状況に置いていても、他人には容易に検索できない独自の分類方法により名刺を分類した状態である場合
2．アンケートの戻りはがきで、氏名、住所等で分類整理されていない状態である場合

5　個人データに該当する事例

1．個人情報データベース等から他の媒体に格納したバックアップ用の個人情報
2．コンピュータ処理による個人情報データベース等から出力された帳票等に印字された個人情報

6　個人データに該当しない事例

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

7　本人への通知の事例

1．面談においては、口頭又はちらし等の文書を渡すこと。
2．電話においては、口頭又は自動応答装置等で知らせること。
3．隔地者間においては、電子メール、ファックス等により送信すること、又は文書を郵便等で送付すること。
4．電話勧誘販売において、勧誘の電話において口頭の方法によること。
5．電子商取引において、取引の確認を行うための自動応答の電子メールに記載して送信すること。

8　公表の事例

1．自社のウェブ画面中のトップページから 1 回程度の操作で到達できる場所への掲載、自社の店舗・事務所内におけるポスター等の掲示、パンフレット等の備置き・配布等
2．店舗販売においては、店舗の見やすい場所への掲示によること。
3．通信販売においては、通信販売用のパンフレット等への記載によること。

9　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手渡し、又は送付すること（契約約款又は利用条件等の書面（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。）中に利用目的条項を記載する場合は、例えば、裏面約款に利用目的が記載されていることを伝える、又は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留意する必要がある。）

2．ネットワーク上においては、本人がアクセスした自社のウェブ画面上、又は本人の端末装置上にその利用目的を明記すること（ネットワーク上において個人情報を取得する場合は、本人が送信ボタン等をクリックする前等にその利用目的（利用目的の内容が示された画面に 1 回程度の操作でページ遷移するよう設定したリンクやボタンを含む。）が本人の目にとまるようその配置に留意する必要がある。

10　本人の同意を得ている場合の事例

1．同意する旨を本人から口頭又は書面（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．本人が署名又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の事例

1．ウェブ画面中のトップページから 1 回程度の操作で到達できる場所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。
4．電子商取引において、商品を紹介するウェブ画面にリンク先を継続的に掲示すること。

12　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、口頭又は文章で回答できるよう体制を構築しておくこと。
2．店舗販売において、店舗にパンフレットを備え置くこと。
3．電子商取引において、問い合わせ先のメールアドレスを明記すること。

13　具体的に利用目的を特定している事例

1．「○○事業における商品の発送、関連するアフターサービス、新商品・サービスに関する情報

のお知らせのために利用いたします。」
2．例えば、情報処理サービスを行っている事業者の場合であれば、「給与計算処理サービス、あて名印刷サービス、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。」のようにすれば利用目的を特定したことになる

14　具体的に利用目的を特定していない事例

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

15　本人が想定することが困難でないと認められる範囲内に該当する事例

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る」旨追加することは、許容される。

16　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

17　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

18　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に違反した他の事業者から、事情を知って取得すること

19　本人に通知又は公表が必要な事例

1．インターネット上で本人が自発的に公に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のように本人により自発的に提供される個人情報を取得する場合（本人確認や問い合わせに対する回答の目的でのみ個人情報を取得した場合を除く。）
4．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

20　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

21　必要かつ適切な安全管理措置を講じているとはいえない場合の事例

1．公開されることを前提としていない個人データが事業者のウェブ画面上で不特定多数に公開されている状態を個人情報取扱事業者が放置している場合
2．組織変更が行われ、個人データにアクセスする必要がなくなった従事者が個人データにアクセスできる状態を個人情報取扱事業者が放置していた場合で、その従事者が個人データを漏えいした場合
3．本人が継続的にサービスを受けるために登録していた個人データが、システム障害により破損したが、採取したつもりのバックアップも破損しており、個人データを復旧できずに滅失又はき損し、本人がサービスの提供を受けられなくなった場合
4．個人データに対してアクセス制御が実施されておらず、アクセスを許可されていない従業者がそこから個人データを入手して漏えいした場合
5．個人データをバックアップした媒体が、持ち出しを許可されていない者により持ち出し可能な状態になっており、その媒体が持ち出されてしまった場合

22　従業者に対して必要かつ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等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

23　受託者に必要かつ適切な監督を行っていない場合の事例

1．個人データの安全管理措置の状況を契約締結時及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

24　第三者提供とされる事例

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

25　第三者提供とされない事例

1．同一事業者内で他部門へ個人データを提供すること。（ただし、利用目的による制限がある。）
2．法第 42 条第 2 項に基づき認定個人情報保護団体が対象事業者に資料提出等を求め、対象事業者がそれに応じて資料提出をする場合

26　第三者に提供される個人データの項目の事例

1．氏名、住所、電話番号
2．氏名、商品購入履歴

27　第三者への提供の手段又は方法の事例

1．書籍として出版
2．インターネットに掲載

28　委託の事例

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
2．百貨店が注文を受けた商品の配送のために、宅配業者に個人データを渡す場合

29　事業の承継のために第三者提供とされない事例

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

30　共同利用を行うことがある事例

1．グループ企業で総合的なサービスを提供するために利用目的の範囲内で情報を共同利用する場合
2．親子兄弟会社の間で利用目的の範囲内で個人データを共同利用する場合
3．外国の会社と利用目的の範囲内で個人データを共同利用する場合

31　共同して利用される個人データの項目の事例

1．氏名、住所、電話番号
2．氏名、商品購入履歴

32　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合の事例

1．医療機関等において、病名等を開示することにより本人の心身状況を悪化させるおそれがある場合

33　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の事例

1．試験実施機関において、採点情報のすべてを開示することにより、試験制度の維持に著しい支障を及ぼすおそれがある場合
2．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

34　他の法令に違反することとなるために開示を行わない場合の事例

1．金融機関が「組織的な犯罪の処罰及び犯罪収益の規制等に関する法律」第 54 条第 1 項に基づいて、主務大臣に取引の届出を行っていたときに、当該届出を行ったことが記録されている保有個人データを開示することが同条第 2 項の規定に違反する場合

35　訂正を行う必要がない場合の事例

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

36　開示等の求めを受け付ける方法の事例

開示等の求めをする者が本人又はその代理人（(ア)未成年者又は成年被後見人の法定代理人、(イ)開示等の求めをすることにつき本人が委任した代理人）であることの確認の方法の事例

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（送付（郵送、FAX 等））：運転免許証のコピーと住民票の写し

5．本人の場合（送付（郵送、FAX 等））：運転免許証や健康保険の被保険者証等の公的証明書のコピーの送付を顧客等から受け、当該公的証明書のコピーに記載された顧客等の住所にあてて文書を書留郵便により送付

6．代理人の場合（来所）：本人及び代理人ついて、運転免許証、健康保険の被保険者証、旅券（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

第四章　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（本ガイドライン第十条（従業者の監督）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、見直し及び改善
(5) 事故又は違反への対処

【各項目について講じることが望まれる事項】

	チェック
(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	
・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。	□
・個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（CPO））の設置	□
・個人データの取扱い（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及び作業担当者の限定	□
・個人データを取扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定	□
・個人データの取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	□
・個人データの取扱いに関する規程等に違反している事実、又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、又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、本ガイドライン第二十条（苦情処理）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及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、見直し及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（内部監査又は外部監査）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及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及び改善	□
(5) 事故又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 ①事実調査 ②影響範囲の特定 ③影響を受ける可能性のある本人及び主務大臣等への報告 ④原因の究明 ⑤再発防止策の検討・実施	□

【個人データの取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	
イ）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。）	□
ロ）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。）	□
ハ）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	□
ニ）作業担当者及びその権限の確認	
・手続の明確化と手続に従った実施及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	
イ）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	□
ロ）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	□
ハ）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	□
ニ）作業担当者及びその権限の確認	
・手続の明確化と手続に従った実施及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	
イ）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	□
ロ）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。）	□
ハ）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	□
ニ）作業担当者及びその権限の確認	
・手続の明確化と手続に従った実施及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	
イ）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	□
ロ）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	□
ハ）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	□
ニ）作業担当者及びその権限の確認	
・手続の明確化と手続に従った実施及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	
イ）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	□
ロ）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 回又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。）	□
ハ）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	□
ニ）作業担当者及びその権限の確認	
・手続の明確化と手続に従った実施及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) 雇用契約時及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、本ガイドライン第十条（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】　　ﾁｪｯｸ

(1) 雇用契約時及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	
・従業者の採用時又は委託契約時における非開示契約の締結 ※　雇用契約又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及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	
・個人データ及び情報システムの安全管理に関する従業者の役割並びに責任を定めた内部規程等についての周知	□
・個人データ及び情報システムの安全管理に関する従業者の役割並びに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】

	チェック
(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、個人データ及びそれを取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】

	チェック
(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、同一又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又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。）	□
(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、滅失及びき損からの適切な保護 ※　個人データを取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、本人及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又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。	□

ビルメンテナンス業界を取り巻く
個人情報問題についてのＱ＆Ａ

ビルメンテナンス業を取り巻く個人情報問題についてのＱ＆Ａ

１.「個人情報」（ガイドライン第三条第一号）

Q1　地図に住所を表示するシステムについて、住所データが含まれています。個人情報に該当しますか？

A1　単に、地図上の地点を示すのみならば、通常は特定の個人を識別できないので、個人情報とはいえないものと考えます。

Q2　個人情報に該当する事例１で「本人の氏名」とありますが、同姓同名の人もあり、ほかの情報がなく氏名だけのデータでも個人情報といえるのでしょうか？

A2　同姓同名の可能性もありますが、氏名があれば、社会通念上、特定の個人を識別できるものと解されます。

Q3　個人情報に該当する事例５の「周知の情報を補って認識することにより特定の個人を識別できる情報」とは何ですか？

A3　例えば、「現在の厚生労働大臣」とだけあって、氏名がない情報でも、周知の情報を補えば、特定の個人が識別できるので個人情報に該当します。

Q4　個人事業主の財務情報等は個人情報ですか？

A4　例えば、「山田太郎商店」などであれば、個人が特定されるので個人情報となりえます。結果的に個人経営であった場合のように、企業情報であって個人情報ではないと解される場合もあり得ます。

Q5　企業の代表者の情報等の公開情報を個人情報として保護する実益は何もないのではないでしょうか？

A5　個人情報の保護は、プライバシー保護の観点とは異なります。個人情報は、他のデータとのマッチング等によって価値が生じ得ることなどから、公開情報であっても保護すべき実益はあるものと考えられています。

Q6　外国に居住する外国人の個人情報についても、個人情報保護法上の保護の対象になりますか？

A6　本法は国内法でありますから国内の個人情報取扱事業者に適用され、国内事業者が取扱う外国人の個人情報についても対象となり得ます。

Q7　取引先の企業の担当者の名前を管理していますが、これも個人情報ですか？

A7　個人情報です。

Q8　住所だけで個人情報となりますか？

A8　住所だけでは、基本的には個人情報となりません。ただし、その他の情報と容易に照合でき、それによって特定の個人を識別することができれば、その情報と併せて全体として個人情報となることはあるため、ケースバイケースでの判断が必要です。

Q9　求人応募者の情報の取り扱い方は？

A9　求人応募者の情報も個人情報になります。個人情報保護法に要求されている管理体制で取り扱ってください。

Q10　警備用の防犯カメラに録画された画像は個人情報になりますか？

A10　画像や映像も、本人が識別できる場合には個人情報になります。

Q11　個人情報とプライバシー情報と違うのですか？

A11　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等により特定の個人を識別することができるもので、客観的に定義されています。

一方、プライバシー情報とは、私生活の事実であり、他人には公開したくない、かつ公然となっていない情報のことで、主観的な要素が含まれています。例えば、氏名、住所からなる情報は個人情報ですが、プライバシー情報に該当しない場合もあります。

２.「個人情報データベース等」（ガイドライン第三条第二号）

Q1　冊子になっている市販の職員録は、「個人情報データベース等」に該当しますか？

A1　一定の規則で整理・分類されていて、目次、索引などがあり、容易に検索可能なので、「個人情報データベース等」に該当します。

Q2　メールソフトや名刺について、従業員本人しか使用できない状態であれば、企業の個人情報データベース等には該当しない、ということでよいでしょうか？

A2　従業員の個人的な使用に用いているのであれば、企業にとっての個人情報データベース等には含まれませんが、従業員が企業活動の用に供するために使用しているもので企業が管理し得るものであれば、企業の個人情報データベース等に該当することになり得ます。

Q3　個人情報データベースに該当する事例１に、「電子メールソフトに保管されているメールアドレス帳」とありますが、他人には容易に検索できない独自の分類方法によりメールアドレスを分類した状態である場合は、個人情報データベース等に該当しないと考えてよいでしょうか？

A3　「メールアドレス帳」に氏名を付してアドレスを保存した場合は、それが従業員の個人使用で第三者が利用できない場合は別として、事業用のアドレス帳で、その検索機能を使えば、第三者でも特定の個人情報の検索が容易に行える場合には、「他人には容易に検索できない独自の分類方法」にはなりません。

３.「個人情報取扱事業者」（ガイドライン第三条第三号）

Q1　社員のデータベースしか持っていない場合は、個人情報取扱事業者とならないということでよいでしょうか？

A1　社員の情報も個人情報ですので、社員が 5,000 人以上の場合は、個人情報取扱事業者となり得ます。

Q2　個人情報取扱事業者に該当した場合には何か届出等の手続が必要なのですか？

A2　届出や認可などの手続は何もありません。

Q3　個人情報取扱事業者に該当しない場合は、何の責任もありませんか？

A3　個人情報取扱事業者に該当しない場合は、法に基づく行政処分が科せられることはありませんが、漏えい事故等で被害が発生したときには、被害者から民事上の損害賠償責任を追求される可能性はあります。

Q4　個人情報取扱事業者となる基準である個人データ 5,000 件のカウントの解釈の仕方を教えてください。

A4　その事業の用に供する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です。同一個人分の重複分を除き、6 ヶ月以内のいずれの日にも 5,000 を超えないか否かで判断します。個人情報取扱事業者に該当しなくても漏えい事故などで被害者が出た場合、民事上の損害賠償責任は発生し得ることになります。

４.「個人データ」（ガイドライン第三条第四号）

Q1　人名録のデータは個人データに該当しますか。

A1　一般に、人名録の情報は個人データに該当します。ただし、その件数は個人情報取扱事業者の該当条件の 5,000 件には含まれません。

５.「保有個人データ」（ガイドライン第三条第五号）

Q1　6 ヶ月以内に消去することとなるものは該当しないとありますが、その起算点はいつですか？

A1　当該個人データが個人情報データベース等を構成するに至った日の翌日から起算します。

６.「公表」（ガイドライン第三条第八号）

Q1　店頭販売が中心の場合でも、ウェブ画面に公表しておけば足りますか？

A1　基本的には足りますが、本人の目につきにくくするという目的で、恣意的に、店舗の見やすい場所への掲示を回避してウェブ画面上でのみ公表しておくというような場合には、「公表」が合理的かつ適切な方法によっていない、とされるおそれがあります。

７．個人情報の利用目的関係（ガイドライン第四条）

Q1　「利用」とは何でしょうか？

A1　特に定義はありませんが、個人情報を保管しているだけでも「利用」に当たります。

Q2　当初の利用目的が変更となったためその旨を通知する際、利用目的の範囲に含まれない商品告知等をついでに同封することは問題ないでしょうか？

A2　利用目的の範囲に含まれない商品告知等をすることはできません。利用目的の達成に必要な範囲を超える利用は、事前に本人の同意が必要となります。

Q3　よくいうプライバシーポリシーにて、自社の個人情報に対する取扱い方を明記すれば、個々の取得手段に対して、利用目的を明確にする必要はないのですか？

A3　プライバシーポリシーは、個人情報取扱いについての基本方針を明示したのです。個人情報の取得はいろいろの目的で行われる可能性があります。個々の取得ごとに利用目的をできるだけ特定する必要があります。

８．個人情報の取得関係（ガイドライン第六条）

Q1　サービスを利用した本人から友人を紹介してもらい、その友人の個人情報を取得する、「友人紹介キャンペーン」による取得は個人情報の取得の手段として適正ですか？

A1　事業者が偽ったり、騙したりするなどして、個人情報を不正に取得するのでなければ、法に違反しているということにはなりません。

ただし、その友人にとっては自分が関知しないところで個人情報の提供等が行われることとなるので、例えば、紹介してもらうに当たって事前に被紹介者の同意を得てもらう、被紹介者に対してダイレクトメールの送付等を行う場合には紹介者を明示する（紹介者からもその旨同意を得る。）といった慎重な対応が求められるものと考えます。

９．利用目的の通知又は公表（ガイドライン第七条）

Q1　自社の社員に対して、資格を調査するにあたって、利用目的などの明示をする必要はありますか。また必要がある場合、どのように明示すればよいでしょうか？

A1　社員ごとの取得資格としての調査でなく匿名の統計データとしてまとめる目的の場合は個人情報の取得に当たりませんので明示の必要はありません。

社員ごとの取得資格の調査であれば利用目的の明示が必要です。この場合は、社内規則、調査のための通達文書、調査表そのもの等に利用目的を記載し、社員に対して明確に示す配慮が必要となります。

Q2　仕事上で名刺を交換する際に、利用目的などの明示をする必要がありますか？

A2　ガイドライン第七条４項（適用除外）四号（利用目的自明）に該当します。名刺の交換は一般の慣行として今後の連絡のためという利用目的が自明であると認められますので明示の必要はありません。

ただし、ダイレクトメール等の目的に名刺を用いることは自明の利用目的に該当しない場合があるので注意を要します。

10．個人データの管理　(1)データ内容の正確性の確保（ガイドライン第八条）

Q1　個人データ内容の正確性の確保が義務づけられていますが、「正確かつ最新の内容」の程度は、本人の同一性を損なわない程度と理解してよいですか？

A1　個人データの利用目的が達成できる程度に、正確かつ最新の内容に確保（更新等）することが必要です。

10．個人データの管理　(2)安全管理措置（ガイドライン第九条）

Q1　会員（お客様）に対して、本人の情報の変更内容を葉書でお知らせすることは問題がありますか？

A1　葉書に記載されている個人情報は、個別的なものでデータベースを構成する「個人データ」自体ではなく、プライバシーの問題です。

　配達時に本人が直接受け取らないような場合には、家族など第三者がその内容を知り得ることもあります。お知らせする情報の内容によっては、他人に知られたくない情報が記載されていることもあり得ますので、プライバシー事項については、葉書の文面を見ることができないようにするなどの配慮が必要です。

Q2　ガイドラインに記載されている、「個人情報保護管理者（チーフ・プライバシー・オフィサー）」については、各事業所ではなく、各企業ごとに設置するという解釈でしょうか？

A2　各事業所ごとに責任者を設置してもよいですが、それらを統括する個人情報保護管理者（チーフ・プライバシー・オフィサー）は各企業ごとに設置するということを想定した記述です。

Q3　「個人情報保護管理者（チーフ・プライバシー・オフィサー）」の選任にあたっては、特段の資格等は不要という整理でしょうか？（無論、専門的知識を持っている者が選任されるほうが、より望ましいとは思いますが）

A3　個人情報保護管理者の選任にあたっては特段の資格等が必要というわけではありません。

Q4　入館時に備え付けの名簿に住所氏名を記入してもらっています。次の入館者が見える状態ですが、問題はありますか？

A4　入館名簿は、それだけではデータベースを構成する個人データにはなりませんので、本法の対象ではありません。

　ただし、プライバシーに配慮して、当面は、そのような扱いを希望しない来館者に対しては、別の用紙に記入してもらうなどの対応も考えるべきでしょう。

Q5　防犯カメラの記録映像を閲覧する場合、事件又は事故関係者、警察官に立ち会いを求めるべきでしょうか？

A5　防犯カメラの記録映像を閲覧する場合は当然ながら、自社の職責を有した人のみに限定すべきです。事故関係者、警察官に立ち会いについては、本来は第三者提供に当たりますが、通常は公開捜査等除外事項に当たると思われますので、立ち会いを求めたほうがよいでしょう。

Q6　警備用の防犯カメラに録画されたビデオの保存・廃棄の仕方はどのように行えばよろしいでしょうか？

A6　他の個人情報の取扱いと同様です。廃棄については、ガイドライン第四章「安全管理措置として講じることが望まれる具体的事項」に記述されている【個人データの取扱いに関する規程等に記載することが望まれる事項】の「⑤消去・廃棄」を参照してください。

Q7　個人情報の廃棄（PC・FD 等・紙資料）を求められました。どのようにすればよいですか？

A7　ガイドライン第四章「安全管理措置として講じることが望まれる具体的事項」に記述されている【個人データの取扱いに関する規程等に記載することが望まれる事項】の「⑤消去・廃棄」を参照してください。

Q8　委託元（テナント含む）の緊急連絡先の取扱方法（掲示・保管）を教えてください。

A8　個人情報としての適切な取扱いが要求されます。関係者のみがアクセスできるところに掲示又は保管することが望ましいです。

Q9　仕事上で交換した名刺の保管・廃棄について実施すべき事項を教えてください。

A9　保管・廃棄についてはガイドライン第九条（安全管理措置）に記述している個人情報としての安全管理措置の実施が必要です。保管については盗難等の防止措置、廃棄についてはシュレッダーによる裁断等適切な管理が求められます。

Q10　警備を受託しているビルの入退出管理の際に個人情報保護法上行わなくてはならないことはどのようなものですか？

A10　契約で取り決められた事項を順守することは当然ですが、建物等への入退館記録等はガイドライン第九条（安全管理措置）従った管理が求められます。

Q11　個人所有の携帯電話を業務で使用し、業務上の個人データも記憶しています。紛失した場合、個人データ漏えいとして扱うことになるのでしょうか？

A11　たとえ個人所有の機器といえ、業務のためのデータを保有・利用している場合で、企業が承認している場合は、事業者としての安全管理措置が求められます。機器の紛失は、個人データの漏えいの可能性があるものとして対応する必要があります。

10．個人データの管理　(3)従業者の監督（ガイドライン第十条）

Q1　現場従業員に対する監視（モニタリング）の仕方はありますか？

A1　監視した結果は個人情報になります。雇用管理に関する個人情報の取扱いに関する重要事項を定めるときは、就業規則等でその旨明白にしておくことも大事です。

　また、あらかじめ労働組合等（かかる労組がないときは過半数代表者）に通知し、必要に応じて協議を行うことが望ましいと考えます。その重要事項を定めたときは労働者等に周知することが望ましいと考えます。

Q2　従業員（派遣社員・パート・アルバイト含む）との間に、誓約書などは、取り交わした方がよいですか？

A2　従業員（派遣社員・パート・アルバイト含む）との間には、誓約書又は守秘義務契約などを締結した方がよいです。

Q3　従業員に対してどのように教育を行えばよろしいでしょうか？

A3　ガイドライン第十条を参照してください。全従業員への定期的な教育、受講欠席者へのフォロー教育、新入社員への教育があります。方法としては会議室での講習、試験、また朝礼時の訓話があります。最近はウェブを使用したｅ-learning も普及しています。教育記録を残していくことが重要です。

Q4　顧客に対して、どう自社の教育実施体制を報告したらよいですか？

A4　教育計画（教材、スケジュール、対象）と、教育記録の報告を行うことです。ただし、第三者に提供する教育記録の報告には、従業員には同意が必要です。

Q5　現場従業員への教育内容として、どのような教育内容にするとよいですか？

A5　現場で知り得た個人情報は他人に漏えいしないこと、資料類にはみだりに触れたりしないことなど、身近な事例を積み上げて教育するとよいでしょう。

　また、個人情報漏えい事件が社会的に注目を浴びていることを新聞記事などを紹介して知らしめることも有益と考えます。

10．個人データの管理　(4)委託先の監督（ガイドライン第十一条）

Q1　業務を委託する際に、委託先との関係でどのような点に注意しなければなりませんか？

A1　法は、委託者に対して委託先監督責任を課していますが、個人情報の取扱いについてなんら取り決めをしないまま、漏えいがあった際の責任を一方的に受託者に押しつける、ということでは、委託先監督責任の観点からは不十分です。

　個人情報をどのように取り扱うのかについて、事前に、具体的内容について、十分協議して、委託者と受託者の責任分担を明確にしておく必要があります。

Q2　個人情報保護及び機密情報保護を含めた業務委託契約書のモデル、又は個人情報保護及び機密情報保護に関する機密保持契約書又は覚書等はありますか？

A2　次回のガイドラインの改訂にあわせて、サンプルとして揃えていきたいと考えています。また、ガイドライン第十一条（委託先の監督）を参照してください。

Q3　再委託する場合、発注側から求められた個人情報保護を担保する為に、同様のレベルを求めた契約や、管理を行わなければならないでしょうか？

A3　再委託先に対する個人情報保護の管理責任は自社にあります。したがって、再委託先とは同レベルの契約、管理は必要になります。ガイドライン第十一条を参照してください。

Q4　再委託先への従業員の守秘義務をどう徹底し、管理監督したらよいでしょうか？

A4　まず契約締結が必要でしょう。再委託先企業を通して従業員への教育を行うことを契約で定め、定期的に確認を行うことが必要です。

Q5　業務委託の際、順守しなければならない点は何ですか？

A5　ガイドライン第十一条を参照してください。

11．第三者への提供（ガイドライン第十二条）

Q1　個人情報を取得するときに、同時に第三者提供についての本人の同意をとっておくことは可能ですか？

A1　そのような扱いも可能です。

Q2　販売した商品について、葉書で登録を受け付けていますが、同梱したソフトウェアの提供会社への登録についてもその葉書の情報をもって代行することは可能でしょうか？

A2　ソフトウェアの提供会社に第三者提供する旨を、利用目的として登録葉書等に明示し、かつ、第三者提供についての同意等の手続をとっておけば可能です。

　なお、ソフトウェア会社の委託を受けて登録を代行する場合（第三者提供に該当しない場合）は、ソフトウェアの提供会社における個人情報の利用目的を登録葉書等へ明示することが必要となり、第三者提供についての同意等の手続は不要となります。

Q3　その際、第三者提供先である関連ソフトウェア会社における利用目的（新商品の案内等）についても明示しなければならないのでしょうか？

A3　第三者提供先における利用目的について明示しなければならない法律上の義務はありません。顧客サービスの観点から検討することになります。

Q4　社員の所属部署と内線番号の表を作成して、社内で閲覧できるようにすることは第三者提供ですか？

A4　事業者内での閲覧（提供）は第三者提供ではありません。

Q5　自己破産している当社社員に関する情報を、弁護士が職務上聞きたいと言ってきた場合に、弁護士に社員の情報を提供してもよいですか？

A5　ガイドライン第十二条（法第 23 条第 1 項第 1 号）の法令に基づく場合となり得ます。ただし、プライバシー等の観点から、民法その他の法令や判例を踏まえた対応が必要となります（警察からの任意聴取の場合も同様）。

Q6　警察からのテナントに関する問合せがありました。捜査等への協力依頼に対してどのように対応すればよろしいでしょうか？　本人の同意を得る必要はありますか？

A6　法令に基づいて行われる捜査に協力する場合には、当該個人情報を提供するに当たって本人の同意は必要ありません。

Q7　弁護士からテナントに関する個人データの提供を求められた場合、どのように対応すればよろしいでしょうか？

A7　法令に基づいて個人情報の提供を求められた場合には、当該個人情報を提供するに当たって本人の同意は必要ありません。ただ、弁護士の活動は多岐にわたっていますので提供要求の背景／理由を十分に聞きだす必要があるでしょう。

Q8　テナントが転居した後、水道局等（公益事業体）から「滞納料金を請求したいので転居先、連絡先を教えて欲しい」と言われた場合、どのように対応すればよろしいでしょうか？

A8　ガイドライン第十二条第一項第四号に規定されているとおり「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」は本人の同意なく第三者提供ができます。

Q9　当社の提携会社や協力会社から、当社社員にお中元を贈りたいとの理由で、当社社員の連絡先を教えてほしいといわれた場合に、提携会社や協力会社に社員の連絡先を提供してもよいですか？

Q9　提携会社や協力会社に社員の個人情報を提供することは第三者提供に該当するため、事前に社員本人から同意を得ておくなどの措置が必要となります。

Q10　保険会社から、保険サービス提供のため、当社社員の氏名や住所を教えてほしいと言われましたが、提供しても問題ありませんか？

A10　提供すること自体は禁止していませんが、第三者提供となるので、事前に本人同意を得ておくなどの措置が必要となります。

Q11　社員の住所録を作成し、社内閲覧することは第三者提供に当たりますか？

A11　第三者提供ではありません。ただし、社員が第三者に不当に提供しないように管理上の注意を書き添える等の注意が必要です。

12．苦情処理（ガイドライン第二十条）

Q1　お客様から受けた相談・苦情等には、どのような措置をすればよいでしょうか？

A1　苦情相談窓口を設置し、相談対応ルールを定めて対処してください。

13．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格

Q1　プライバシーマークを取得すれば、個人情報保護法を遵守したことになりますか？

A1　プライバシーマークは JIS 規格（JIS Q 15001「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」）に準拠して付与していますが、この JIS と個人情報保護法の比較をすると、JIS が個人情報保護法を上回っているといえます。

Q2　JIS Q 15001 が個人情報保護法を上回っていない部分は、例えば何ですか？

A2　JIS Q 15001 の適用範囲は、コンピュータ処理された個人情報データベースを利用する事業者ですが、個人情報保護法は、コンピュータ処理されたもの以外の紙で処理した個人情報データベースを利用する事業者も対象としている点や、JIS には、委託先における個人情報の利用目的の本人への通知又は公表義務がない点などがあります。ただし、JIS には、個人情報に関する法令及びその他の規範を特定し、参照できる手順を確立し、維持しなければならないとの規定がありますので（4.3.2 法令及びその他の規範）、結果的に個人情報保護法の順守を求められているといえます。

Q3　個人情報保護法を順守するためにはプライバシーマークがもっとも有効な手段ですか？

A3　何をしたらよいかわからない事業者や、他の企業との差別化を図りたい事業者にとっては、有効といえます。

Q4　プライバシーマーク制度及び ISMS 制度の違いを教えてください。

A4　ISMS とは、情報セキュリティマネジメントシステムのことです。ISMS 制度とは、企業が持つ情報資産に対し情報セキュリティ管理策が適切に実施されていることに対して認証されるものです。情報資産には人事情報、顧客情報などの個人情報だけでなく、経営機密、設計情報、得意先情報、企業ノウハウ等があります。認定単位は事業部単位からできます。日本での主管はプライバシーマークと同じ JIPDEC です。両制度で違うのは、

1. 認定の単位：プライバシーマークは全事業者単位、ISMS は事業部単位でも可
2. 対象情報：プライバシーマークは個人情報、ISMS は全情報資産

が主なところです。

その他、複合的な事案

Q1　会員名簿を会員に配布する際にはどのような点に注意が必要ですか？

A1　第 1 に、個人情報を取得するときに、明示する利用目的の中に配布する旨が含まれていることが必要です。その際には、どのような範囲にどのような頻度で配布するのかなど、会員が理解しておくべき内容がわかりやすく示されていることが望ましいといえます。

　第 2 に、第三者提供についての本人の同意等の措置が必要です。少なくとも、会員が掲載を希望しない項目については掲載しないこととするなどの措置が必要になります。その他、個人データの安全管理措置等、個人情報保護法の一般的な義務が課せられます。

Q2　申込書に記載してもらう個人情報については、取得の状況からみて自明といえるので、例えばメールアドレス等を記載してもらう場合でも、利用目的の明示は不要と考えていますが、いかがでしょうか？

A2　申込書に記載してもらう個人情報の利用目的は、取得の状況からみて自明である、と簡単に決めてしまうのは早計です。新たなサービスの案内等、申込内容の確認以外の目的で、メールアドレス情報を利用することは、取得の状況からみて自明の範囲内とはいいきれない場合もあります。提携先へ提供することや、名簿を作成して配布することなど、申込受付作業終了後も利用するこ

とがあるのであれば、その旨を個人情報の利用目的として、申込書等に明示（第三者提供をする場合には本人の同意も必要）しておく必要があります。それがなければ、原則として他に利用することはできません。

Q3　メーカーがプレゼントキャンペーンを行うため、代理店に依頼して広告してもらい、代理店を応募先とした場合、代理店からメーカーに対してその応募情報を提供することは問題ありませんか。また、そのメーカーがその応募情報を使って、ダイレクトメールを送ってもよいですか？

A3　前段については、メーカーからの代理店に対する個人情報収集（取得）の委託と考えられ、委託関係の場合は双方の関係は第三者ではないので、委託者であるメーカーが代理店から提供を受けるにあたっては、第三者提供の場合のように本人からの同意取得等は不要です。なお、この場合、本人から書面で個人情報を取得することとなるため、原則としてキャンペーン広告に個人情報の利用目的を記載（明示）しなければなりません。

　後段については、プレゼントキャンペーン広告に、ダイレクトメールを送る旨の記載（利用目的の明示）があれば問題ありませんが、そうでない場合は、メーカーにおける目的外利用となるので、ダイレクトメールを送るのなら、事前に応募者本人から同意を得る必要があります。

Q4　宅配業者を使って、個人データが記録されているディスクを届けてもらおうと思っていますが、注意すべき点はありますか？

A4　郵便の場合も基本的には同様ですが、宅配業者は物流の効率化を目的としたサービスを行う事業者であることを認識する必要があります。つまり、宅配業者は、通常は配達物の中の情報が個人情報に該当するかどうかを認識することなく個人情報を取り扱っているので、事業の用に供しているとは認められず、義務規定が適用されないものと解されます。したがって、宅配業者を利用する場合にはそのような認識のもと利用するか、又は、個人情報の内容によっては、宅配にあたって特約を定めることができるような業者を選ぶことが必要な場合もありえます。

Q5　自社内の運用ルール及び社内規程の構築方法のヒントは何ですか？

A5　自社内の運用ルール：ガイドライン第四章「安全管理措置として講じることが望まれる具体的事項」に記述されている【各項目について講じることが望まれる事項】を参照してください。社内規定：ガイドライン第四章「安全管理措置として講じることが望まれる具体的事項」に記述されている【個人データの取扱いに関する規定等に記載することが望まれる事項】を参照してください。

Q6　顧客より、現場に配置される従業員の名簿を求められますが、この取扱いについて教えてください。守秘義務契約などを別途取る必要がありますか？　従業員に対しても説明義務がありますか？

A6　守秘義務契約を委託元、委託先双方で締結する必要があります。また、従業員に対しては説明し、第三者提供をする旨の同意が必要です。

Q7　委託元より担当者の（氏名・住所・電話番号）緊急連絡先の提示を求められた場合の対応方法を教えてください。

A7　守秘義務契約を委託元、委託先双方で締結する必要があります。また、従業員に対しては事前にその旨明示しておくことや第三者提供をする旨の同意が必要です。

Q8　清掃作業時・警備巡回時に注意するべき点はありますか？（オフィス内等）

A8　資料などを覗き込んだり、じっと見てみたりしないでください。いらぬ嫌疑の元になります。現場での心構えを教育してください。

Q9　現場従事者が、業務中、口頭（うわさ話など）にて見聞きした情報は個人情報となりますか？また、こういった情報に対する注意点はありますか？

A9　口頭にて見聞きした情報でも、特定の個人を識別できるのであれば個人情報となります。みだりに他人に情報漏えいをしないよう指導していく必要があります。

Q10　ゴミ箱に個人情報を含む書類が捨てられていました。処理方法を教えてください。

A10　通常ゴミとみなして処理することを前もって契約しておくことです。現場従業者がこのような場面に遭遇した場合、上司を通して状況の報告をさせるなど会社として状況を把握していき、今後の契約に盛り込んでいくことを勧めます。

Q11　廃棄物・ゴミの排出管理はどのように行えばよろしいでしょうか？

A11　個人情報の有無に係わらず、決められたルールに従って排出管理をすればよいでしょう。個人情報として認識しないで取扱う廃棄物・ゴミには個人情報保護法でいう安全管理措置は求められていません。

Q12　損害賠償を算定する際の判定基準（リスク内容）はありますか？　また、慰謝料発生時の責任分担はどう明確にしたらよいでしょうか？

A12　1 人につき 15,000 円の賠償の判決（弁護士費用分 5,000 円を除くと 10,000 円）があります。自主的に詫び料として 1 人 500 円を支払った例もあります。個々のケースで異なることが考えられます。

　また、NPO 日本ネットワークセキュリティ協会（JNSA）が「2003 年度セキュリティインシデントに関する調査報告書」に被害の想定賠償額計算式を提案しています。それによると、基礎情報価値、機微情報度、本人特定容易度、社会的責任度、事後対策評価、の 5 項目の評価結果の乗算で算出式を提案しています。

　責任分担は業務委託契約に盛り込むことが望まれます。ガイドライン第十一条も参照してください。

Q13　ビルメンテナンス業が係わった事件事例はありますか？

A13　個人情報の漏えい事件は圧倒的に自社社員又は元社員によるものや盗難によるものが多いです。報道された中には明確にビルメンテナンス業が係わった事件はありません。派遣社員による悪質な個人情報漏えい事件、委託業者の可能性があるという事件は報道されています。

資 料 編

個人情報の保護に関する法律 ····· 61

雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針 ····· 68

雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項について ····· 69

参考法令・ガイドライン一覧 ····· 71

個人情報の保護に関する法律

□個人情報の保護に関する法律
（平成十五年法律第五十七号）

目次

第一章　総則（第一条－第三条）
第二章　国及び地方公共団体の責務等（第四条－第六条）
第三章　個人情報の保護に関する施策等
第一節　個人情報の保護に関する基本方針（第七条）
第二節　国の施策（第八条－第十条）
第三節　地方公共団体の施策（第十一条－第十三条）
第四節　国及び地方公共団体の協力（第十四条）
第四章　個人情報取扱事業者の義務等
第一節　個人情報取扱事業者の義務（第十五条－第三十六条）
第二節　民間団体による個人情報の保護の推進（第三十七条－第四十九条）
第五章　雑則（第五十条－第五十五条）
第六章　罰則（第五十六条－第五十九条）
附則

第一章　総則

（目的）

第一条　この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、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する。

（定義）

第二条　この法律において「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。）をいう。

2　この法律において「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。

一　特定の個人情報を電子計算機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

二　前号に掲げるもののほか、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ものとして政令で定めるもの

3　この法律において「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。ただし、次に掲げる者を除く。

一　国の機関

二　地方公共団体

三　独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成十五年法律第五十九号）第二条第一項に規定する独立行政法人等をいう。以下同じ。）

四　地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。以下同じ。）

五　その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者

4　この法律において「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。

5　この法律において「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、追加又は削除、利用の停止、消去及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、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。

6　この法律において個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。

（基本理念）

第三条　個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない。

第二章　国及び地方公共団体の責務等

（国の責務）

第四条　国は、この法律の趣旨にのっとり、個人情報の適正な取扱いを確保するために必要な施策を総合的に策定し、及びこれを実施する責務を有する。

（地方公共団体の責務）

第五条　地方公共団体は、この法律の趣旨にのっとり、その地方公共団体の区域の特性に応じて、個人情報の適正な取扱いを確保するために必要な施策を策定し、及びこれを実施する責務を有する。

（法制上の措置等）

第六条　政府は、国の行政機関について、その保有する個人情報の性質、当該個人情報を保有する目的等を勘案し、その保有する個人情報の適正な取扱いが確保されるよう法制上の措置その他必要な措置を講ずるものとする。

2　政府は、独立行政法人等について、その性格及び業務内容に応じ、その保有する個人情報の適正な取扱いが確保されるよう法制上の措置その他必要な措置を講ずるものとする。

3　政府は、前二項に定めるもののほか、個人情報の性質及び利用方法にかんがみ、個人の権利利益の一層の保護を図るため特にその適正な取扱いの厳格な実施を確保する必要がある個人情報について、保護のための格別の措置が講じられるよう必要な法制上の措置その他の措置を講ずるものとする。

第三章　個人情報の保護に関する施策等

第一節　個人情報の保護に関する基本方針

第七条　政府は、個人情報の保護に関する施策の総合的かつ一体的な推進を図るため、個人情報の保護に関する基本方針（以下「基本方針」という。）を定めなければならない。

2　基本方針は、次に掲げる事項について定めるものとする。

一　個人情報の保護に関する施策の推進に関する基本的な方向

二　国が講ずべき個人情報の保護のための措置に関する事項

三　地方公共団体が講ずべき個人情報の保護のための措置に関する基本的な事項

四　独立行政法人等が講ずべき個人情報の保護のための措置に関する基本的な事項

五　地方独立行政法人が講ずべき個人情報の保護のための措置に関する基本的な事項

六　個人情報取扱事業者及び第四十条第一項に規定する認定個人情報保護団体が講ずべき個人情報の保護のための措置に関する基本的な事項

七　個人情報の取扱いに関する苦情の円滑な処理に関する事項

八　その他個人情報の保護に関する施策の推進に関する重要事項

3　内閣総理大臣は、国民生活審議会の意見を聴いて、基本方針の案を作成し、閣議の決定を求めなければならない。

4　内閣総理大臣は、前項の規定による閣議の決定があったときは、遅滞なく、基本方針を公表しなければならない。

5　前二項の規定は、基本方針の変更について準用する。

第二節　国の施策

（地方公共団体等への支援）

第八条　国は、地方公共団体が策定し、又は実施する個人情報の保護に関する施策及び国民又は事業者等が個人情報の適正な取扱いの確保に関して行う活動を支援するため、情報の提供、事業者等が講ずべき措置の適切かつ有効な実施を図るための指針の策定その他の必要な措置を講ずるものとする。

（苦情処理のための措置）

第九条　国は、個人情報の取扱いに関し事業者と本人との間に生じた苦情の適切かつ迅速な処理を図るために必要な措置を講ずるものとする。

（個人情報の適正な取扱いを確保するための措置）

第十条　国は、地方公共団体との適切な役割分担を通じ、次章に規定する個人情報取扱事業者による個人情報の適正な取扱いを確保するために必要な措置を講ずるものとする。

第三節　地方公共団体の施策

（地方公共団体等が保有する個人情報の保護）

第十一条　地方公共団体は、その保有する個人情報の性質、当該個人情報を保有する目的等を勘案し、その保有する個人情報の適正な取扱いが確保されるよう必要な措置を講ずることに努めなければならない。

2　地方公共団体は、その設立に係る地方独立行政法人について、その性格及び業務内容に応じ、その保有する個人情報の適正な取扱いが確保されるよう必要な措置を講ずることに努めなければならない。

（区域内の事業者等への支援）

第十二条　地方公共団体は、個人情報の適正な取扱いを確保するため、その区域内の事業者及び住民に対する支援に必要な措置を講ずるよう努めなければならない。

（苦情の処理のあっせん等）

第十三条　地方公共団体は、個人情報の取扱いに関し事業者と本人との間に生じた苦情が適切かつ迅速に処理されるようにするため、苦情の処理のあっせんその他必要な措置を講ずるよう努めなければならない。

第四節　国及び地方公共団体の協力

第十四条　国及び地方公共団体は、個人情報の保護に関する施策を講ずるにつき、相協力するものとする。

第四章　個人情報取扱事業者の義務等

第一節　個人情報取扱事業者の義務

（利用目的の特定）

第十五条　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。

2　個人情報取扱事業者は、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合理的に認められる範囲を超えて行ってはならない。

（利用目的による制限）

第十六条　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

2　個人情報取扱事業者は、合併その他の事由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た場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

3　前二項の規定は、次に掲げる場合については、適用しない。

一　法令に基づく場合

二　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。

三　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。

四　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。

（適正な取得）

第十七条　個人情報取扱事業者は、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。

（取得に際しての利用目的の通知等）

第十八条　個人情報取扱事業者は、個人情報を取得した場合は、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、又は公表しなければならない。

2　個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（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。以下この項において同じ。）

に記載された当該本人の個人情報を取得する場合その他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、その利用目的を明示しなければならない。ただし、人の生命、身体又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。

3　個人情報取扱事業者は、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、本人に通知し、又は公表しなければならない。

4　前三項の規定は、次に掲げる場合については、適用しない。

一　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合

三　国の機関又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、又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とき。

四　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

（データ内容の正確性の確保）

第十九条　個人情報取扱事業者は、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よう努めなければならない。

（安全管理措置）

第二十条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

（従業者の監督）

第二十一条　個人情報取扱事業者は、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を行わなければならない。

（委託先の監督）

第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

（第三者提供の制限）

第二十三条　個人情報取扱事業者は、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。

一　法令に基づく場合

二　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。

三　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。

四　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。

2　個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人データの項目

三　第三者への提供の手段又は方法

四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

3　個人情報取扱事業者は、前項第二号又は第三号に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

4　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、前三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。

一　個人情報取扱事業者が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扱いの全部又は一部を委託する場合

二　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

三　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及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又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

5　個人情報取扱事業者は、前項第三号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

（保有個人データに関する事項の公表等）

第二十四条　個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、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。）に置かなければならない。

一　当該個人情報取扱事業者の氏名又は名称

二　すべての保有個人データの利用目的（第十八条第四項第一号から第三号までに該当する場合を除く）。

三　次項、次条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求めに応じる手続（第三十条第二項の規定により手数料の額を定めたときは、その手数料の額を含む）。

四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

2　個人情報取扱事業者は、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ときは、本人に対し、遅滞なく、これを通知しなければならない。ただし、次の

各号のいずれかに該当する場合は、この限りでない。

一　前項の規定により当該本人が識別される保有個人データの利用目的が明らかな場合

二　第十八条第四項第一号から第三号までに該当する場合

3　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの利用目的を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。

（開示）

第二十五条　個人情報取扱事業者は、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ときにその旨を知らせることを含む。以下同じ。）を求められたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。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、その全部又は一部を開示しないことができる。

一　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　当該個人情報取扱事業者の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

三　他の法令に違反することとなる場合

2　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの全部又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、その旨を通知しなければならない。

3　他の法令の規定により、本人に対し第一項本文に規定する方法に相当する方法により当該本人が識別される保有個人データの全部又は一部を開示することとされている場合には、当該全部又は一部の保有個人データについては、同項の規定は、適用しない。

（訂正等）

第二十六条　個人情報取扱事業者は、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、追加又は削除（以下この条において「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。

2　個人情報取扱事業者は、前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とき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正等を行ったときは、その内容を含む。）を通知しなければならない。

（利用停止等）

第二十七条　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第十六条の規定に違反して取り扱われているという理由又は第十七条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去（以下この条において「利用停止等」という。）を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、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、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

2　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第二十三条第一項の規定に違反して第三者に提供されているという理由によって、当該保有個人データの第三者への提供の停止を求められた場合であって、その求めに理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

3　個人情報取扱事業者は、第一項の規定に基づき求められた保有個人データの全部若しくは一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき、又は前項の規定に基づき求められた保有個人データの全部若しくは一部について第三者への提供を停止したとき若しくは第三者への提供を停止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。

（理由の説明）

第二十八条　個人情報取扱事業者は、第二十四条第三項、第二十五条第二項、第二十六条第二項又は前条第三項の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又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。

（開示等の求めに応じる手続）

第二十九条　個人情報取扱事業者は、第二十四条第二項、第二十五条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求め（以下この条において「開示等の求め」という。）に関し、政令で定めるところにより、その求めを受け付ける方法を定めることができる。この場合において、本人は、当該方法に従って、開示等の求めを行わなければならない。

2　個人情報取扱事業者は、本人に対し、開示等の求めに関し、その対象となる保有個人データを特定するに足りる事項の提示を求めることができる。この場合において、個人情報取扱事業者は、本人が容易かつ的確に開示等の求めをすることができるよう、当該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を考慮した適切な措置をとらなければならない。

3　開示等の求めは、政令で定めるところにより、代理人によってすることができる。

4　個人情報取扱事業者は、前三項の規定に基づき開示等の求めに応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮しなければならない。

（手数料）

第三十条　個人情報取扱事業者は、第二十四条第二項の規定による利用目的の通知又は第二十五条第一項の規定による開示を求められたときは、当該措置の実施に関し、手数料を徴収する

ことができる。

2　個人情報取扱事業者は、前項の規定により手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない。

（個人情報取扱事業者による苦情の処理）

第三十一条　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。

2　個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない。

（報告の徴収）

第三十二条　主務大臣は、この節の規定の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱いに関し報告をさせることができる。

（助言）

第三十三条　主務大臣は、この節の規定の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱いに関し必要な助言をすることができる。

（勧告及び命令）

第三十四条　主務大臣は、個人情報取扱事業者が第十六条から第十八条まで、第二十条から第二十七条まで又は第三十条第二項の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。

2　主務大臣は、前項の規定による勧告を受けた個人情報取扱事業者が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者に対し、その勧告に係る措置をとるべきことを命ずることができる。

3　主務大臣は、前二項の規定にかかわらず、個人情報取扱事業者が第十六条、第十七条、第二十条から第二十二条まで又は第二十三条第一項の規定に違反した場合において個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべきことを命ずることができる。

（主務大臣の権限の行使の制限）

第三十五条　主務大臣は、前三条の規定により個人情報取扱事業者に対し報告の徴収、助言、勧告又は命令を行うに当たっては、表現の自由、学問の自由、信教の自由及び政治活動の自由を妨げてはならない。

2　前項の規定の趣旨に照らし、主務大臣は、個人情報取扱事業者が第五十条第一項各号に掲げる者（それぞれ当該各号に定める目的で個人情報を取り扱う場合に限る。）に対して個人情報を提供する行為については、その権限を行使しないものとする。

（主務大臣）

第三十六条　この節の規定における主務大臣は、次のとおりとする。ただし、内閣総理大臣は、この節の規定の円滑な実施のため必要があると認める場合は、個人情報取扱事業者が行う個人情報の取扱いのうち特定のものについて、特定の大臣又は国家公安委員会（以下「大臣等」という。）を主務大臣に指定することができる。

一　個人情報取扱事業者が行う個人情報の取扱いのうち雇用管理に関するものについては、厚生労働大臣（船員の雇用管理に関するものについては、国土交通大臣）及び当該個人情報取扱事業者が行う事業を所管する大臣等

二　個人情報取扱事業者が行う個人情報の取扱いのうち前号に掲げるもの以外のものについては、当該個人情報取扱事業者が行う事業を所管する大臣等

2　内閣総理大臣は、前項ただし書の規定により主務大臣を指定したときは、その旨を公示しなければならない。

3　各主務大臣は、この節の規定の施行に当たっては、相互に緊密に連絡し、及び協力しなければならない。

第二節　民間団体による個人情報の保護の推進

（認定）

第三十七条　個人情報取扱事業者の個人情報の適正な取扱いの確保を目的として次に掲げる業務を行おうとする法人（法人でない団体で代表者又は管理人の定めのあるものを含む。次条第三号ロにおいて同じ。）は、主務大臣の認定を受けることができる。

一　業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）の個人情報の取扱いに関する第四十二条の規定による苦情の処理

二　個人情報の適正な取扱いの確保に寄与する事項についての対象事業者に対する情報の提供

三　前二号に掲げるもののほか、対象事業者の個人情報の適正な取扱いの確保に関し必要な業務

2　前項の認定を受けようとする者は、政令で定めるところにより、主務大臣に申請しなければならない。

3　主務大臣は、第一項の認定をしたときは、その旨を公示しなければならない。

（欠格条項）

第三十八条　次の各号のいずれかに該当する者は、前条第一項の認定を受けることができない。

一　この法律の規定により刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者

二　第四十八条第一項の規定により認定を取り消され、その取消しの日から二年を経過しない者

三　その業務を行う役員（法人でない団体で代表者又は管理人の定めのあるものの代表者又は管理人を含む。以下この条において同じ。）のうちに、次のいずれかに該当する者があるもの

イ　禁錮以上の刑に処せられ、又はこの法律の規定により刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者

ロ　第四十八条第一項の規定により認定を取り消された法人において、その取消しの日前三十日以内にその役員であった者でその取消しの日から二年を経過しない者

（認定の基準）

第三十九条　主務大臣は、第三十七条第一項の認定の申請が次の各号のいずれにも適合していると認めるときでなければ、その

認定をしてはならない。

一　第三十七条第一項各号に掲げる業務を適正かつ確実に行うに必要な業務の実施の方法が定められているものであること。

二　第三十七条第一項各号に掲げる業務を適正かつ確実に行うに足りる知識及び能力並びに経理的基礎を有するものであること。

三　第三十七条第一項各号に掲げる業務以外の業務を行っている場合には、その業務を行うことによって同項各号に掲げる業務が不公正になるおそれがないものであること。

（廃止の届出）

第四十条　第三十七条第一項の認定を受けた者（以下「認定個人情報保護団体」という。）は、その認定に係る業務（以下「認定業務」という。）を廃止しようとするときは、政令で定めるところにより、あらかじめ、その旨を主務大臣に届け出なければならない。

2　主務大臣は、前項の規定による届出があったときは、その旨を公示しなければならない。

（対象事業者）

第四十一条　認定個人情報保護団体は、当該認定個人情報保護団体の構成員である個人情報取扱事業者又は認定業務の対象となることについて同意を得た個人情報取扱事業者を対象事業者としなければならない。

2　認定個人情報保護団体は、対象事業者の氏名又は名称を公表しなければならない。

（苦情の処理）

第四十二条　認定個人情報保護団体は、本人等から対象事業者の個人情報の取扱いに関する苦情について解決の申出があったときは、その相談に応じ、申出人に必要な助言をし、その苦情に係る事情を調査するとともに、当該対象事業者に対し、その苦情の内容を通知してその迅速な解決を求めなければならない。

2　認定個人情報保護団体は、前項の申出に係る苦情の解決について必要があると認めるときは、当該対象事業者に対し、文書若しくは口頭による説明を求め、又は資料の提出を求めることができる。

3　対象事業者は、認定個人情報保護団体から前項の規定による求めがあったときは、正当な理由がないのに、これを拒んではならない。

（個人情報保護指針）

第四十三条　認定個人情報保護団体は、対象事業者の個人情報の適正な取扱いの確保のために、利用目的の特定、安全管理のための措置、本人の求めに応じる手続その他の事項に関し、この法律の規定の趣旨に沿った指針（以下「個人情報保護指針」という。）を作成し、公表するよう努めなければならない。

2　認定個人情報保護団体は、前項の規定により個人情報保護指針を公表したときは、対象事業者に対し、当該個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとるよう努めなければならない。

（目的外利用の禁止)

第四十四条　認定個人情報保護団体は、認定業務の実施に際して知り得た情報を認定業務の用に供する目的以外に利用してはならない。

（名称の使用制限）

第四十五条　認定個人情報保護団体でない者は、認定個人情報保護団体という名称又はこれに紛らわしい名称を用いてはならない。

（報告の徴収）

第四十六条　主務大臣は、この節の規定の施行に必要な限度において、認定個人情報保護団体に対し、認定業務に関し報告をさせることができる。

（命令）

第四十七条　主務大臣は、この節の規定の施行に必要な限度において、認定個人情報保護団体に対し、認定業務の実施の方法の改善、個人情報保護指針の変更その他の必要な措置をとるべき旨を命ずることができる。

（認定の取消し）

第四十八条　主務大臣は、認定個人情報保護団体が次の各号のいずれかに該当するときは、その認定を取り消すことができる。

一　第三十八条第一号又は第三号に該当するに至ったとき。

二　第三十九条各号のいずれかに適合しなくなったとき。

三　第四十四条の規定に違反したとき。

四　前条の命令に従わないとき。

五　不正の手段により第三十七条第一項の認定を受けたとき。

2　主務大臣は、前項の規定により認定を取り消したときは、その旨を公示しなければならない。

（主務大臣）

第四十九条　この節の規定における主務大臣は、次のとおりとする。ただし、内閣総理大臣は、この節の規定の円滑な実施のため必要があると認める場合は、第三十七条第一項の認定を受けようとする者のうち特定のものについて、特定の大臣等を主務大臣に指定することができる。

一　設立について許可又は認可を受けている認定個人情報保護団体（第三十七条第一項の認定を受けようとする者を含む。次号において同じ。）については、その設立の許可又は認可をした大臣等

二　前号に掲げるもの以外の認定個人情報保護団体については、当該認定個人情報保護団体の対象事業者が行う事業を所管する大臣等

2　内閣総理大臣は、前項ただし書の規定により主務大臣を指定したときは、その旨を公示しなければならない。

第五章　雑則

（適用除外）

第五十条　個人情報取扱事業者のうち次の各号に掲げる者については、その個人情報を取り扱う目的の全部又は一部がそれぞれ当該各号に規定する目的であるときは、前章の規定は、適用しない。

一　放送機関、新聞社、通信社その他の報道機関（報道を業として行う個人を含む。）報道の用に供する目的

二　著述を業として行う者著述の用に供する目的

三　大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者学術研究の用に供する目的

四　宗教団体宗教活動（これに付随する活動を含む）の用に供する目的。

五　政治団体政治活動（これに付随する活動を含む）の用に供する目的。

2　前項第一号に規定する「報道」とは、不特定かつ多数の者に対して客観的事実を事実として知らせること（これに基づいて意見又は見解を述べることを含む。）をいう。

3　第一項各号に掲げる個人情報取扱事業者は、個人データの安全管理のために必要かつ適切な措置、個人情報の取扱いに関する苦情の処理その他の個人情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

（地方公共団体が処理する事務）

第五十一条　この法律に規定する主務大臣の権限に属する事務は、政令で定めるところにより、地方公共団体の長その他の執行機関が行うこととすることができる。

（権限又は事務の委任）

第五十二条　この法律により主務大臣の権限又は事務に属する事項は、政令で定めるところにより、その所属の職員に委任することができる。

（施行の状況の公表）

第五十三条　内閣総理大臣は、関係する行政機関（法律の規定に基づき内閣に置かれる機関（内閣府を除く。）及び内閣の所轄の下に置かれる機関、内閣府、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項及び第二項に規定する機関並びに国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関をいう。次条において同じ。）の長に対し、この法律の施行の状況について報告を求めることができる。

2　内閣総理大臣は、毎年度、前項の報告を取りまとめ、その概要を公表するものとする。

（連絡及び協力）

第五十四条　内閣総理大臣及びこの法律の施行に関係する行政機関の長は、相互に緊密に連絡し、及び協力しなければならない。

（政令への委任）

第五十五条　この法律に定めるもののほか、この法律の実施のため必要な事項は、政令で定める。

第六章　罰則

第五十六条　第三十四条第二項又は第三項の規定による命令に違反した者は、六月以下の懲役又は三十万円以下の罰金に処する。

第五十七条　第三十二条又は第四十六条の規定による報告をせず、又は虚偽の報告をした者は、三十万円以下の罰金に処する。

第五十八条　法人（法人でない団体で代表者又は管理人の定めのあるものを含む。以下この項において同じ。）の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、前二条の違反行為をしたときは、行為者を罰するほか、その法人又は人に対しても、各本条の罰金刑を科する。

2　法人でない団体について前項の規定の適用がある場合には、その代表者又は管理人が、その訴訟行為につき法人でない団体を代表するほか、法人を被告人又は被疑者とする場合の刑事訴訟に関する法律の規定を準用する。

第五十九条　次の各号のいずれかに該当する者は、十万円以下の過料に処する。

一　第四十条第一項の規定による届出をせず、又は虚偽の届出をした者

二　第四十五条の規定に違反した者

附　則

（施行期日）

第一条　この法律は、公布の日から施行する。ただし、第四章から第六章まで及び附則第二条から第六条までの規定は、公布の日から起算して二年を超えない範囲内において政令で定める日から施行する。

（本人の同意に関する経過措置）

第二条　この法律の施行前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第十五条第一項の規定により特定される利用目的以外の目的で個人情報を取り扱うことを認める旨の同意に相当するものであるときは、第十六条第一項又は第二項の同意があったものとみなす。

第三条　この法律の施行前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第二十三条第一項の規定による個人データの第三者への提供を認める旨の同意に相当するものであるときは、同項の同意があったものとみなす。

（通知に関する経過措置）

第四条　第二十三条第二項の規定により本人に通知し、又は本人が容易に知り得る状態に置かなければならない事項に相当する事項について、この法律の施行前に、本人に通知されているときは、当該通知は、同項の規定により行われたものとみなす。

第五条　第二十三条第四項第三号の規定により本人に通知し、又は本人が容易に知り得る状態に置かなければならない事項に相当する事項について、この法律の施行前に、本人に通知されているときは、当該通知は、同号の規定により行われたものとみなす。

（名称の使用制限に関する経過措置）

第六条　この法律の施行の際現に認定個人情報保護団体という名称又はこれに紛らわしい名称を用いている者については、第四十五条の規定は、同条の規定の施行後六月間は、適用しない。

附則（平成十五年法律第百十九号）抄

（施行期日）

第一条　この法律は、地方独立行政法人法（平成十五年法律第百十八号）の施行の日から施行する。ただし、次の各号に掲げる規定は、当該各号に定める日から施行する。

一　第六条の規定個人情報の保護に関する法律の施行の日又はこの法律の施行の日のいずれか遅い日

（その他の経過措置の政令への委任）

第六条　この附則に規定するもののほか、この法律の施行に伴い必要な経過措置は、政令で定める。

雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針

○厚生労働省告示第二百五十九号

個人情報の保護に関する法律（平成十五年法律第五十七号）第八条の規定に基づき、雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針を次のように定め、平成十七年四月一日から適用する。

平成十六年七月一日

厚生労働大臣　坂口　力

雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針

第一　趣旨

この指針は、個人情報の保護に関する法律（以下「法」という。）に定める事項に関し、雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置について、その適切かつ有効な実施を図るために必要な事項を定めたものである。

なお、雇用管理に関する個人情報については、本指針によるほか、当該個人情報取扱事業者が行う事業を所管する大臣等が策定した指針その他の必要な措置に留意するものとする。

第二　用語の定義

法第二条に定めるもののほか、この指針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　事業者法第二条第三項に規定する個人情報取扱事業者のうち雇用管理に関する個人情報を取り扱う者をいう（第四に規定する場合を除く。）。

二　労働者等前号に規定する事業者に使用されている労働者、前号に規定する事業者に使用される労働者になろうとする者及びなろうとした者並びに過去において事業者に使用されていた者をいう。

第三　事業者が講ずべき措置の適切かつ有効な実施を図るための指針となるべき事項

一　法第十五条に規定する利用目的の特定に関する事項

事業者は利用目的の特定に当たっては、単に抽象的、一般的に特定するのではなく、労働者等本人が、取得された当該本人の個人情報が利用された結果が合理的に想定できる程度に、具体的、個別的に特定すること。

二　法第十六条及び法第二十三条第一項に規定する本人の同意に関する事項

事業者が労働者等本人の同意を得るに当たっては、当該本人に当該個人情報の利用目的を通知し、又は公表した上で、当該本人が口頭、書面等により当該個人情報の取扱いについて承諾する意思表示を行うことが望ましいこと。

三　法第二十条に規定する安全管理措置及び法第二十一条に規定する従業者の監督に関する事項

事業者は、雇用管理に関する個人データの安全管理のために次に掲げる措置を講ずるように努めるものとすること。

㈠　雇用管理に関する個人データを取り扱う従業者及びその権限を明確にした上で、その業務を行わせること。

㈡　雇用管理に関する個人データは、その取扱いについての権限を与えられた者のみが業務の遂行上必要な限りにおいて取り扱うこと。

㈢　雇用管理に関する個人データを取り扱う者は、業務上知り得た個人データの内容をみだりに第三者に知らせ、又は不当な目的に使用してはならないこと。その業務に係る職を退いた後も同様とすること。

㈣　雇用管理に関する個人データの取扱いの管理に関する事項を行わせるため、当該事項を行うために必要な知識及び経験を有していると認められる者のうちから個人データ管理責任者を選任すること。

㈤　雇用管理に関する個人データ管理責任者及び個人データを取り扱う従業者に対し、その責務の重要性を認識させ、具体的な個人データの保護措置に習熟させるため、必要な教育及び研修を行うこと。

四　法第二十二条に規定する委託先の監督に関する事項

事業者は、雇用管理に関する個人データの取扱いの委託に当たって、次に掲げる事項に留意するものとすること。

㈠　個人情報の保護について十分な措置を講じている者を委託先として選定するための基準を設けること。

㈡　委託先が委託を受けた個人データの保護のために講ずべき措置の内容が委託契約において明確化されていること。具体的な措置としては、以下の事項が考えられること。

①　委託先において、その従業者に対し当該個人データの取扱いを通じて知り得た個人情報を漏らし、又は盗用してはならないこととされていること。

②　当該個人データの取扱いの再委託を行うに当たっては、委託元へその旨文書をもって報告すること。

③　委託契約期間等を明記すること。

④　利用目的達成後の個人データの返却又は委託先における破棄若しくは削除が適切かつ確実になされること。

⑤　委託先における個人データの加工（委託契約の範囲内のものを除く。）、改ざん等を禁止し、又は制限すること

⑥　委託先における個人データの複写又は複製（安全管理上必要なバックアップを目的とするもの等委託契約範囲内のものを除く。）を禁止すること。

⑦　委託先において個人データの漏えい等の事故が発生した場合における委託元への報告義務を課すこと。

⑧　委託先において個人データの漏えい等の事故が発生した場合における委託先の責任が明確化されていること。

五　法第二十三条に規定する第三者提供に関する事項

事業者は、雇用管理に関する個人データの第三者への提供（法第二十三条第一項第一号から第四号までに該当する場合を除く。）に当たって、次に掲げる事項に留意するものとすること。

㈠　提供先において、その従業者に対し当該個人データの取扱いを通じて知り得た個人情報を漏らし、又は盗用してはならないこととされていること。

㈡　当該個人データの再提供を行うに当たっては、あらかじめ文書をもって事業者の了承を得ること。但し、当該再提供が、法第二十三条第一項第一号から第四号までに該当する場合を除く。

㈢　提供先における保管期間等を明確化すること。

㈣　利用目的達成後の個人データの返却又は提供先における破棄若しくは削除が適切かつ確実になされること。

㈤　提供先における個人データの複写及び複製（安全管理上必要なバックアップを目的とするものを除く。）を禁止すること。

六　法第二十五条第一項に規定する保有個人データの開示に関する事項

事業者は、あらかじめ、労働組合等と必要に応じ協議した上で、労働者等本人から開示を求められた保有個人データについて、その全部又は一部を開示することによりその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に該当するとして非開示とすることが想定される保有個人データの開示に関する事項を定め、労働者等に周知させるための措置を講ずるよう努めなければならないこと。

七　法第二十九条第二項に規定する本人の利便を考慮した適切な措置に関する事項

事業者は、労働者等からの雇用管理に関する個人データの開示等の求めができるだけ円滑に行われるよう、閲覧の場所及び時間等について十分配慮すること。

八　法第三十一条に規定する苦情の処理に関する事項

事業者は、雇用管理に関する個人情報の取扱いに関する苦情の適切かつ迅速な処理を行うため苦情及び相談を受け付けるための窓口の明確化等必要な体制の整備に努めること。

九　その他事業主等が雇用管理に関する個人情報の適切な取扱いを確保するための措置を行うに当たって配慮すべき事項

㈠　事業者は、六に定める保有個人データの開示に関する事項その他雇用管理に関する個人情報の取扱いに関する重要事項を定めるときは、あらかじめ労働組合等に通知し、必要に応じて、協議を行うことが望ましいものであること。

㈡　事業者は、九の㈠の重要事項を定めたときは、労働者等に周知することが望ましいものであること。

第四　個人情報取扱事業者以外の事業者による雇用管理に関する個人情報の取扱い

法第二条第三項に規定する個人情報取扱事業者以外の事業者であって、雇用管理に関する個人情報を取り扱う者は、第三に準じて、その適正な取扱いの確保に努めること。

雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項

雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項

第１　趣旨

この留意事項は、雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針（平成１６年厚生労働省告示第２５９号。以下「指針」という。）に定める雇用管理に関する個人情報のうち健康情報の取扱いについて、指針に定める措置の実施等に加えて事業者が留意すべき事項を定めるものである。

第２　用語の定義

個人情報の保護に関する法律（平成１５年法律第５７号。以下「法」という。）第２条及び指針第２に定めるもののほか、この留意事項において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

１　健康情報

指針に定める雇用管理に関する個人情報のうち、健康診断の結果、病歴、その他の健康に関するものをいう。なお、健康情報に該当するものの例として、次に掲げるものが挙げられる。

(1) 産業医が労働者の健康管理等を通じて得た情報

(2) 労働安全衛生法（昭和４７年法律第５７号。以下「安衛法」という。）第６５条の２第１項の規定に基づき、事業者が作業環境測定の結果の評価に基づいて、労働者の健康を保持するため必要があると認めたときに実施した健康診断の結果

(3) 安衛法第６６条第１項から第４項までの規定に基づき事業者が実施した健康診断の結果並びに安衛法第６６条第５項及び第６６条の２の規定に基づき労働者から提出された健康診断の結果

(4) 安衛法第６６条の４及び第６６条の５第１項の規定に基づき事業者が医師等から聴取した意見及び事業者が講じた健康診断実施後の措置の内容

(5) 安衛法第６６条の７の規定に基づき、事業者が実施した保健指導の内容

(6) 安衛法第６９条第１項の規定に基づく健康保持増進措置（ＴＨＰ：トータル・ヘルスプロモーション・プラン）を通じて事業者が取得した健康測定の結果、健康指導の内容等

(7) 労働者災害補償保険法（昭和２２年法律第５０号）第２７条の規定に基づき、労働者から提出された二次健康診断の結果

(8) 健康保険組合等が実施した健康診断等の事業を通じて事業者が取得した情報

(9) 受診記録、診断名等の療養の給付に関する情報

(10)事業者が医療機関から取得した診断書等の診療に関する情報
(11)労働者から欠勤の際に提出された疾病に関する情報
(12) (1)から(11)までに掲げるもののほか、任意に労働者等から提供された本人の病歴、健康診断の結果、その他の健康に関する情報

2　産業保健業務従事者

産業医、保健師等、衛生管理者その他の労働者の健康管理に関する業務に従事する者をいう。

第３　健康情報の取扱いについて事業者が留意すべき事項

1　法第１６条及び法第２３条第１項に規定する本人の同意に関する事項（指針第３の２関係）

(1) 事業者が、労働者から提出された診断書の内容以外の情報について医療機関から健康情報を収集する必要がある場合、事業者から求められた情報を医療機関が提供することは、法第２３条の第三者提供に該当するため、医療機関は労働者から同意を得る必要がある。この場合においても、事業者は、あらかじめこれらの情報を取得する目的を労働者に明らかにして承諾を得るとともに、必要に応じ、これらの情報は労働者本人から提出を受けることが望ましい。

(2) また、事業者が、健康保険組合等に対して労働者の健康情報の提供を求める場合、事業者と健康保険組合等とは、異なる主体であることから、法第２３条の第三者提供に該当するため、健康保険組合等は労働者（被保険者）の同意を得る必要がある。この場合においても、事業者は、あらかじめこれらの情報を取得する目的を労働者に明らかにして承諾を得るとともに、必要に応じ、これらの情報は労働者本人から提出を受けることが望ましい。

ただし、事業者が健康保険組合等と共同で健康診断を実施する場合等において、法第２３条第４項第３号の要件を満たしている場合は、当該共同利用者は第三者に該当しないため、当該労働者の同意を得る必要はない。

2　法第２０条に規定する安全管理措置及び法第２１条に規定する従業者の監督に関する事項（指針第３の３（１）及び（２）関係）

(1) 健康診断の結果のうち診断名、検査値等のいわゆる生データの取扱いについては、その利用に当たって医学的知識に基づく加工・判断等を要することがあることから、産業医や保健師等の看護職員に行わせることが望ましい。

(2) 産業保健業務従事者以外の者に健康情報を取り扱わせる時は、これらの者が取り扱う健康情報が利用目的の達成に必要な範囲に限定されるよう、必要に応じて健康情報を適切に加工した上で提供する等の措置を講ずること。

3　法第３１条に規定する苦情の処理に関する事項（指針第３の８関係）

指針第３の８に定める苦情及び相談を受け付けるための窓口については、健康情報に係る苦情及び相談に適切に対応するため、必要に応じて産業保健業務従事者と連携を図ることができる体制を整備しておくことが望ましい。

4　その他事業者が雇用管理に関する個人情報の適切な取扱いを確保するための措置を行うに当たって配慮すべき事項

(1) 事業者は、健康診断等を医療機関に委託することが多いことから、健康情報についても外部とやり取りをする機会が多いことや、事業場内においても健康情報を産業保健業務従事者以外の者に取り扱わせる場合があること等にかんがみ、あらかじめ、雇用管理指針第３の６に掲げるもののほか、以下に掲げる事項について事業場内の規程等として定め、これを労働者に周知するとともに、関係者に当該規程に従って取り扱わせることが望ましい。
(a) 健康情報の利用目的に関すること
(b) 健康情報に係る安全管理体制に関すること
(c) 健康情報を取り扱う者及びその権限並びに取り扱う健康情報の範囲に関すること
(d) 健康情報の開示、訂正、追加又は削除の方法（廃棄に関するものを含む。）に関すること
(e) 健康情報の取扱いに関する苦情の処理に関すること

(2) 事業者は、(1) の規程等を定めるときは、衛生委員会等において審議を行った上で、雇用管理指針第３の９(1) に定めるところにより労働組合等に通知し、必要に応じて協議を行うことが望ましい。

(3) 事業者は、安衛法第６６条第１項及び第２項等の規定に基づき行われた健康診断を受けた労働者等に対し、遅延なく、その結果を通知すること。

(4) ＨＩＶ感染症やＢ型肝炎等の職場において感染したり、蔓延したりする可能性が低い感染症に関する情報や、色覚検査等の遺伝情報については、職業上の特別な必要性がある場合を除き、事業者は、労働者等から取得すべきでない。

(5) 労働者の健康情報は、医療機関において「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」に基づき取り扱われ、また、健康保険組合において「健康保険組合等における個人情報の適切な取扱いのためのガイドライン」に基づき取り扱われることから、事業者は、特に安全管理措置等について、両ガイドラインの内容についても留意することが期待されている。

第４　個人情報取扱事業者以外の事業者による健康情報の取扱い

個人情報取扱事業者以外の事業者であって健康情報を取り扱う者は、健康情報が特に適正な取扱いの厳格な実施を確保すべきものであることに十分留意し、第３に準じてその適正な取扱いの確保に努めること。

参考法令・ガイドライン一覧

更新日：平成 17 年 5 月 25 日

＜凡 例＞

法令・ガイドライン名		
発行者	最新版	URL または資料管理部門

・・

個人情報の保護に関する法律		
法律	平成 15 年 5 月 30 日	http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi
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		
経済産業省	平成 16 年 10 月 22 日	http://www.meti.go.jp/policy/it_policy/privacy/041012_hontai.pdf
経済産業分野のうち信用分野における個人情報保護ガイドライン		
経済産業省	平成 16 年 12 月 17 日	http://www.meti.go.jp/policy/it_policy/privacy/041012_hontai.pdf
雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針		
厚生労働省	平成 16 年 7 月 1 日	http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/koyou.pdf
雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項		
厚生労働省	平成 16 年 10 月 29	http://wwwhourei.mhlw.go.jp/%7Ehourei/doc/tsuchi/161112-b.pdf
医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン		
厚生労働省	平成 16 年 12 月 24 日	http://www.mhlw.go.jp/houdou/2004/12/dl/h1227-6a.pdf
福祉関係事業者における個人情報の適正な取扱いのためのガイドライン		
厚生労働省	平成 16 年 11 月 30 日	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161130fukusi.pdf
認定個人情報保護団体の認定等に関する指針		
厚生労働省		http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170330nintei.pdf
職業紹介事業者、労働者の募集を行う者、募集受託者、労働者供給事業者等が均等待遇、労働条件等の明示、求職者等の個人情報の取扱い、職業紹介事業者の責務、募集内容の的確な表示等に関して適切に対処するための指針		
厚生労働省	平成 16 年 11 月 4 日	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161118syoukai.pdf
派遣元事業主が講ずべき措置に関する指針		
厚生労働省	平成 16 年 11 月 4 日	http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161118haken.pdf
労働者派遣事業関係業務取扱要領		
厚生労働省		http://www.mhlw.go.jp/general/seido/anteikyoku/jukyu/haken/youryou/
国土交通省所管分野に係る個人情報保護に関するガイドライン		
国土交通省	平成 17 年 4 月 13 日	http://www.mlit.go.jp/pubcom/04/pubcomt37/01.pdf
医療機関における個人情報の保護		
日本医師会	平成 17 年 2 月 1 日	http://www.hokkaido.med.or.jp/new/juyo/kojinjo2.pdf
警備業における個人情報の保護に関するガイドライン		
(社)全国警備業協会	平成 17 年 1 月	(社)全国警備業協会にて販売（価格：300 円）
機密情報保護に関するガイドライン		
日本人材派遣協会	平成 16 年 10 月	日本人材派遣協会会員のみ配布
マンション管理業における個人情報保護ガイドライン		
(社)高層住宅管理業協会	平成 17 年 2 月	(社)高層住宅管理業協会にて販売（価格：2,000 円）

ビルメンテナンス業における個人情報保護に関するガイドライン
平成 17 年 5 月 31 日　第 1 版　発行

社団法人 全国ビルメンテナンス協会
〒116-0013　東京都荒川区西日暮里 5-12-5
ビルメンテナンス会館
TEL 03(3805)7560　　FAX 03(3805)7561
URL　http://www.j-bma.or.jp/


jBMA