

個人情報の保護に関する法律についての ガイドライン

第1章 ガイドラインの目的・適用

(目的・規範・見直し)

- 第1条 このガイドラインは、個人情報の保護に関する法律を規範とし、JISQ15001:2006、個人情報保護にかかる経済産業省・厚生労働省・文部科学省及び関係省庁のそれぞれのガイドライン、関係諸法に準拠するものとする。株式会社早稲田アカデミー(以下「会社」という。)において個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定めるものであり、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、定期的(年一回以上)かつ継続的に見直しを実施し改善することを目的とする。
- 2 このガイドラインは、公益通報者保護法(以下、「公益通報」という。)及び株早稲田アカデミーに通う子どもの安全確保ガイドライン(以下「安全確保」という。)のうち個人情報保護に係る関連事項に関しても定めるものとする。
- 3 個人情報保護マネジメントシステムに関して、JIS規格との適合性を自ら確認し、適合していることを自ら表明すると共に、外部組織又は本人に確認を求め、かつ、外部機関による認証又は登録を求めるものとする。

(適用)

- 第2条 このガイドラインは、会社に常駐する、役員及び正社員、契約社員、アルバイト職員、派遣職員、インターンシップによるインターン等全ての従業員に適用するものとする。

(個人情報保護方針)

- 第3条 会社は、個人情報の保護に関する運用・管理体制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「個人情報保護方針=プライバシーポリシー」という)を定め、全従業員へ書面で配布すると共に入塾案内書又はウェブ画面等への掲載等により公表するものとする。
- 2 プライバシーポリシーは、事業所名、代表者氏名、制定年月日と共に、次に掲げる各事項について可能な限り定め、開示するものとする。
- 個人情報の保護に関する運用・管理体制の推進に関する基本的な方針及び以下の各号に関する事項
- イ 個人情報保護法を遵守すること
 - ロ JISQ15001:2006を遵守すること
 - ハ 個人情報保護に関する法令・指針その他の規範を遵守すること
 - ニ 教育・研修に関すること
- 会社が講ずべき個人情報の保護のための措置に関する事項
- イ 個人情報保護管理体制の措置
 - ロ 取得方法
 - ハ 利用目的
 - ニ 目的外利用を行わないこと及びそのための措置
 - ホ 個人情報の漏えい、滅失又はき損の防止及び是正に関すること

- へ 委託・提供・第三者提供、及び共同利用に関する事項
- ト 開示等の手続き、手数料等の明示
 - 個人情報取扱いに関する苦情の円滑な処理に関する事項
- イ 相談窓口或いは相談方法に関する具体的説明
- ロ 相談受付時間、担当者氏名等
 - その他個人情報の保護に関する運用・管理体制の推進に関する重要事項
 - マネジメントシステム及びプライバシーポリシーの定期的かつ継続的改善について
- 公益通報及び安全確保に係る個人情報の保護管理に係る事項

第2章 定義

(用語の定義)

第4条 このガイドラインにおいて、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ものとする。

個人情報：会社においては、事業の用に供する児童、生徒（以下「生徒」という。）及びその保護者と従業員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、学習成績、成績順位、各種試験及び検定の可否又は個人別に付された番号、記号その他の符号、画像若しくは音声により当該生徒個人若しくは生徒保護者を識別できるもの（当該情報のみ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、それにより識別できるものを含む。）をとす。加えて在籍者に限らず、過去において在籍した或いは在籍しようとした者、現時点で在籍しようとした者、或いは一時的に在籍した或いは在籍しようとした者等全ての特定される個人に関する情報とする。また、人事労務管理及び福利厚生目的以外の、従業員のために利用した、従業員の氏名、所属、学歴、画像若しくは音声により当該従業員を特定できる情報とする。JISQ15001：2006では、生存者以外の情報を含む。

個人情報保護管理者(CPO=チーフ・プライバシー・オフィサー)：会社の代表者若しくは、会社の内部において代表者より指名されたものであって、個人情報の適切な取扱いの確保又はマネジメントシステムの実施及び運用及び営業秘密統括管理者に関する責任と権限を有するものをいう。

本人：個人情報によって識別される特定の個人をいう。情報主体でもある。なお、本人が未成年者（児童・生徒等）又は成年被後見人である場合にはその法定代理人・保護者等も「本人」に含まれるものとする。

生徒及び保護者/従業員の同意：情報主体（本人）である生徒又は保護者、従業員（以下、生徒、保護者、従業員等の全ての情報主体を「本人」という）が、取得、利用又は提供に関する情報を与えられた上で、本人に関する情報の取扱いを承諾する意思表示を行うことをいう。

委託・受託：会社が、模擬試験等の採点・集計・統計、又は広告物の印刷処理等のために、電算機処理等に係る個人情報を、一時的に会社以外の第三者に託すことを委託、委託されることを受託という。

提供・第三者提供：会社が、フランチャイズ契約を結んでいる場合、本部と契約教室の間で各試験成績・合否状況等の個人情報をオプトアウトの上で交換或いは共有する事を提供といい、それ以外の第三者に提供する場合には、第三者提供という。

オプトアウト：提供にあたりあらかじめ、本人に通知する又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利用又は第三者への提供を停止すること等をいう。

個人情報保護監査責任者：会社の代表者によって会社の内部から指名された者であって、公平、かつ、客観的な立場にあり、個人情報保護に関する監査の実施及び報告を行う権限をもつ者。

マネジメントシステム（PMS or C/P）：会社が自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、点検及び見直しを含むマネジメントシステム。

不適合：マネジメントシステムがJISQ15001：2006の要求を満たしていないこと。

第3章 ガイドラインの適用範囲

（対象となる個人情報）

- 第5条 このガイドラインは、会社の内部において、事業の用に供している個人情報を対象とし、自動処理システムによる処理を行うことを目的として書面等により処理されている個人情報についてもこれを適用するものとする。
- 2 会社が人事管理、福利厚生等のため保有する従業員の個人情報は雇用管理情報とする。雇用管理情報に関しては機微な情報を含むことから、「厚生労働省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7月1日厚生労働省告示第259号）を参考にすることができる。
 - 3 公益通報に係る個人情報、安全確保に係る生徒・保護者の個人情報及び教職員監督に係る個人情報は特段の配慮を持ってこのガイドラインを準用するものとする。

（ガイドラインの拡張・見直し）

- 第6条 このガイドラインは、個人情報の適切な保護の目的の範囲内において会社の経営形態、授業形式、生徒募集方法等の実態に応じた項目を追加し、又は修正することができる。
- 2 このガイドラインの前項にかかる見直しを、定期的（年一回以上）かつ継続的に実施するものとする。

第4章 個人情報保護に係る計画・体制

（個人情報の特定）

- 第7条 会社は、自らの事業の用に供するすべての個人情報を特定するための手順を確立し、かつ、維持しなければならないものとする。

個人情報の特定は、個人情報保護管理者が個人情報調査一覧（営業秘密区分に関わる事項含む）を作成することによって特定する。

新規に書式を作成する場合は、使用開始前に一覧に掲載する。

情報の得失時・書式等の変更時等には可及的速やかに実施し、それ以外の場合でも定期的かつ継続的に実施し管理するものとする。

監査責任者は、調査一覧と運用されている書式の整合性の確認及び点検を監査業務として定期的実施する。

- 2 調査一覧は、入塾案内書又はウェブ画面等への掲載等により公表するものとする。

(法令、指針その他の規範)

第8条 会社は、事業に関連する個人情報保護関連の法令、国が定める指針及びその他の規範の制定・改廃状況に注意し、必要に応じて速やかに個人情報保護マネジメントシステムに反映させなければならないものとする。

参照法令・規範等は、第1条第1項・第2項に定めるもの及び会社が属する都道府県・市区町村の関係条例・指針等とする。

制定・改廃の確認は、個人情報保護管理者が行い、改訂等の必要がある場合は代表者に報告する。

第1条第1項・第2項に定める参照法令・規範等は、管理者が所持し管理すると共に、本部事務局に備え置き必要に応じて参照可能な状態で保管する。

参照すべき法令・規範を特定した記録を作成し、保管場所、参照方法、更新履歴等を記録する。

(リスクの認識・分析及び対策)

第9条 会社は、第7条で特定した個人情報について、目的外利用を行わないため、必要な対策を講じる手順を確立し、かつ、維持しなければならないものとする。

2 会社は、第7条で特定した個人情報について、その取扱いの各局面におけるリスク(個人情報の漏えい、滅失又はき損、個人情報保護法との対応、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれ)を認識し、分析し、必要な対策を講じる手順を確立し、かつ、維持しなければならないものとする。

3 前項に規定した各局面とは、以下の各号とする。また、リスクは技術の進展や環境の変化により常に変動するものなので、リスクは常に検証し、定期的に見直すものとする。

個人情報の取得

個人情報の保管

個人情報の利用

個人情報の委託

個人情報の廃棄・返却

4 リスクの認識、分析及び対策の実施・更新に関しては、記録を保存するものとする。

(代表者による個人情報保護管理者の指名)

第10条 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者を会社の内部から指名し、個人情報の保護に関する法律、このガイドラインの遵守、マネジメントシステムの実施及び運用及び営業秘密統括管理者に関する責任及び権限を他の責任に関わりなく与え、業務を行わせるものとする。

代表者本人が管理者である場合も、ガイドラインの内容を理解し実践することによって、個人情報保護管理者及び営業秘密統括管理者としての業務を行うものとする。

2 会社の代表者は、個人情報保護マネジメントシステムを効果的に実施するために個人情報保護管理者・個人情報監査責任者等の役割、責任及び権限を定め、文書化し、かつ、従業員に周知しなければならないものとする。

3 個人情報保護管理者は、個人情報保護マネジメントシステムの見直し及び改善の基礎として、会社の代表者に個人情報保護マネジメントシステムの運用状況を報告しなければならないものとする。

4 個人情報保護管理者は、公益通報制度、安全確保に関するガイドラインの管理・運営及び教職員の監督に関しても、統括するものとする。

(代表者による個人情報保護監査責任者の指名)

第11条 会社の代表者は、このガイドラインの内容を理解し、公平、かつ、客観的な立場にあり、マネジメントシステムの監査を実施し報告を行う権限を他の責任にかかわりなくもつ者を、会社の内部から個人情報保護監査責任者として指名し業務を行わせなければならないものとする。

2 個人情報保護管理者と個人情報保護監査責任者は、同一人物とならないように指名しなければならないものとする。

3 商法及び会社法上の監査役・会計監査人が、個人情報保護監査体制の一部を占めないように指名しなければならないものとする。

(代表者、管理者の責務)

第12条 会社における代表者及び個人情報保護管理者(CPO)は、このガイドラインに定められた事項を理解し、及び遵守するとともに、全従業員にこれを理解させ及び遵守させるための教育訓練、内部規定の整備、安全対策の実施並びにマネジメントシステムの策定、周知徹底、点検及び定期的見直し等の措置を実施する責任を負うものとする。また、代表者は必要不可欠な資源を用意すると共に、適切な監督を行わなければならないものとする。

2 会社における代表者及び個人情報保護管理者(CPO)は、このガイドライン及びマネジメントシステムを入塾案内書又はウェブ画面等への掲載等により公表するものとする。

3 従業員に対する教育(研修)においては、以下の各号に定める事項を周知徹底すると共に、自覚させるものとする。

マネジメントシステムに適合することの重要性及び利点

マネジメントシステムに適合するための役割及び責任

マネジメントシステムに違反した際に予想される結果

4 会社における代表者及び個人情報保護管理者(CPO)は、前項に係る理解度を、報告書を提出させるなどの方法で、確認しなければならないものとする。

(内部規程)

第13条 会社は、次の事項を含む内部規程を文書化し、かつ、維持しなければならないものとする。また、具体的な手順書レベルの規定とするか、別に実施細則を定めなければならないものとする。

個人情報を特定する手順に関する規定

法令、国が定める指針その他の規範の特定、参照及び維持に関する規定

個人情報に関するリスクの認識、分析及び対策の手順に関する規定

事業者の各部門及び教場における個人情報を保護するための権限及び責任に関する規定

緊急事態(個人情報が漏えい、滅失又はき損をした場合)への準備及び対応に関する規定

個人情報の取得、利用及び提供に関する規定

個人情報の適正管理に関する規定

本人からの開示等の求めへの対応に関する規定

教育に関する規定

個人情報保護マネジメントシステム文書の管理に関する規定

苦情及び相談への対応に関する規定

点検に関する規定

是正処置及び予防処置に関する規定

代表者による見直しに関する規定

内部規程に違反した場合に関する罰則の規定
公益通報者保護法に係る周知事項及び手順等の規定

㈱早稲田アカデミーに通う子どもの安全確保ガイドライン及び実施マニュアル

- 2 会社は、事業の内容に応じて、個人情報保護マネジメントシステムが確実に適用されるように取締役会の決議などを経て内部規程を改定しなければならない。
- 3 会社の代表者は、第1項に定められた全ての内部規程に関し、従業員に周知徹底すると共に、従業員が参照できるようにしなければならないものとする。

(計画書)

- 第14条 会社は、個人情報保護マネジメントシステムを確実に実施するために必要な以下の各号に係る計画を立案し、文書化し、かつ、維持しなければならないものとする。
- 教育・研修
 - 監査

(緊急事態への準備)

- 第15条 会社は、緊急事態を特定するための手順、また、それらにどのように対応するかの手順を「緊急事態への対応マニュアル」として確立し、実施し、かつ、維持しなければならないものとする。

マニュアルを定めるにあたっては、以下の各号に考慮するものとする。

緊急事態及び事故が最も起こりやすい場所

予想される被害の規模

被害を最小限に抑えるための一時的な対処方法

社内の緊急連絡網及び社外への報告手順の確立

再発防止処置を実施する手順

緊急時対応についての教育訓練

- 2 事業者は、個人情報漏えい、滅失又はき損をした場合に想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し、その影響を最小限とするための手順を確立し、かつ、維持しなければならないものとする。
- 3 また、個人情報の漏えい、滅失又はき損が発生した場合に備え、次の事項を含む対応手順を確立し、かつ、維持しなければならないものとする。
 - 当該漏えい、滅失又はき損が発生した個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態に置くこと。
 - 二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を、遅滞なく公表すること。
 - 事実関係、発生原因及び対応策を関係機関に直ちに報告すること。
- 4 前各項に係る実施策及び対応策等は、全て記録するものとする。
- 5 第1項における対応マニュアルは、個人情報に係る緊急事態と、安全確保又は公益通報に係る緊急事態とを場合分けし、かつ、それぞれの特性を配慮して対応策・手順を規定するものとする。

第5章 個人情報の取得・利用及び提供に関する原則

(利用目的の特定)

- 第16条 会社は、個人情報を取得するにあたっては、その利用目的をできる限り特定し、その目的の達成に必要な限度において行わなければならないものとする。

(取得の目的、取得範囲の制限)

第17条 個人情報の取得は、取得する会社の正当な事業の範囲内で、従業員募集、生徒募集、業務管理、生徒管理、成績管理、進路指導等の前条で規定した利用目的の達成に必要な限度においてこれを行うものとする。

(適正な取得)

第18条 個人情報の取得は、適法かつ公正な手段によって行うものとする。

(特定の機微な情報の取得、利用及び提供の制限)

第19条 次に掲げる種類の内容を含む個人情報については、これを取得し、利用し又は提供してはならない。ただし、当該情報の取得、利用又は提供について、明示的な本人の同意、法令に特段の規定がある場合及び司法手続き上必要不可欠である場合については、この限りでないものとする。

思想・信条又は宗教に関する事項

人種及び民族、犯罪歴その他社会的差別の原因となる事項

門地及び本籍地(所在都道府県に関する情報を除く)

勤労者の団結権・団体交渉その他の団体行動の行為に関する事項

集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項

保健医療(本人の病歴)又は性生活に関する事項

- 2 会社の代表者は、機微な個人情報を取得する場合には、内部承認の手順に関して定めると共に、その記録を作成し、保管・管理しなければならないものとする。
- 3 機微な個人情報の取得に於いて、第1項の例外を適用する場合の手順及び記録に関しては、前項を準用するものとする。

(本人から直接書面によって取得する場合の措置)

第20条 会社は、本人から、書面(電子的方式、磁気的方式など人の知覚によっては認識できない方式で作られる記録を含む。以下、同じ。)に記載された個人情報を直接に取得する場合には、本人に対して、少なくとも次に掲げる事項又はそれと同等以上の内容の事項を入塾案内書、申込書、契約約款、労働契約書類等の中に記載し、当該個人情報の収集、利用又は委託・提供に関する同意を得るものとする。

会社の名称及び代表者氏名

会社内部の個人情報に関する個人情報保護管理者又はその代理人の氏名又は職名、及び所属並びに連絡先

個人情報の利用目的

外部団体などの模擬試験を実施し答案、成績の送付、若しくは広告物の印刷処理等、個人情報の委託を行うことが予定される場合には、その目的、当該情報の受託者又は受託者の組織の種類、属性及び個人情報の取扱いに関する契約の有無
会社がFC本部等へ、個人情報を提供することが予定される場合には、前号を準用する

本人が、会社に契約書、通信簿等、校内模擬試験成績表、定期試験成績一覧、志望校、入試結果、画像、映像等の個人情報を与えることの、任意性及び当該情報を提供しなかった場合に本人に生じる結果

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方法

本人が容易に認識できない方法によって個人情報を取得する場合には、その旨

- 2 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、第21条各号のいずれかに該当する場合、及び第22条各号のいずれかに該当する場合は、この限りではないものとする。

- 3 会社の代表者は、個人情報の取得をする場合で、前項を適用する場合には、内部承認の手順に関して定めると共に、その記録を作成し、保管・管理しなければならないものとする。

(前条以外の方法によって取得した場合の措置)

第21条 会社は、個人情報を第20条以外の方法によって取得した場合は、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。ただし、次に示すいずれかに該当する場合は、この限りではないものとする。

利用目的を本人に通知し、又は公表することによって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

利用目的を本人に通知し、又は公表することによって会社の権利又は正当な利益を害するおそれがある場合

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って当該事務の遂行に支障を及ぼすおそれがあるとき

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

(利用に関する措置)

第22条 会社は、特定した利用目的の達成に必要な範囲内で個人情報を利用しなければならないものとする。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を利用する場合は、あらかじめ、少なくとも、第20条第1項各号に示す事項又はそれと同等以上の内容事項を書面によって本人に通知し、本人の同意を得なければならないものとする。ただし、次に示すいずれかに該当する場合は、この限りではない。

法令に基づく場合

人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき

公衆衛生の向上又は児童・生徒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

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って当該事務の遂行に支障を及ぼすおそれがあるとき

(本人にアクセスする場合の措置)

第23条 会社は、個人情報を利用して本人にアクセスする場合には、本人に対して、第20条第1項各号に示す事項又それと同等以上の内容事項、および取得方法を通知し、本人の同意を得なければならないものとする。

ただし、次に示すいずれかに該当する場合は、この限りではない。

個人情報の取得時に、既に第20条第1項各号に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ているとき。

個人情報の取扱いの全部又は一部を委託された場合であって、当該個人情報を、その利用目的の達成に必要な範囲内で取り扱うとき。

合併その他の事由による事業の承継に伴って個人情報が提供され、個人情報を提供する事業者が、既に第20条第1項各号に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ている場合であって、承継前の利用目的の範囲内で当該個人情報を取り扱うとき。

個人情報が特定の者との間で共同して利用され、共同利用者が、既に第20条第1項各号に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ている場合であって、次に示す事項又はそれと同等以上の内容の事項を、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。

- イ 共同して利用すること
- ロ 共同して利用される個人情報の項目
- ハ 共同して利用する者の範囲
- ニ 共同して利用する者の利用目的
- ホ 共同して利用する個人情報の管理について責任を有する者の氏名又は名称
- ヘ 取得方法

第 21 条第 4 号に該当するため、利用目的などを本人に明示、通知又は公表することなく取得した個人情報を利用して、本人にアクセスするとき。

第 22 条各号のいずれかに該当する場合。

- 2 会社の代表者は、本人にアクセスする場合の内部承認の手順に関して定めると共に、その記録を作成し、保管・管理しなければならないものとする。

(提供に関する措置)

第24条 会社は、個人情報を第三者に提供する場合には、あらかじめ本人に対して、取得方法及び第 20 条第 1 項第 1、2、3、5 号の事項又はそれと同等以上の内容の事項を通知し、本人の同意を得なければならない。ただし、次に示すいずれかに該当する場合は、この限りではないものとする。

第 20 条又は第 23 条の規定によって、既に第 20 条第 1 項第 1、2、3、5 号の事項又はそれと同等以上の内容の事項を本人に明示又は通知し、本人の同意を得ているとき。

法人その他の団体に関する情報に含まれる当該法人その他の団体の役員及び株主に関する情報であって、かつ、法令に基づき又は本人若しくは当該法人その他の団体自らによって公開又は公表された情報を提供する場合であって、前号で示す事項又はそれと同等以上の内容の事項を、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。

特定した利用目的の達成に必要な範囲内において、個人情報の取扱いの全部又は一部を委託するとき。

合併その他の事由による事業の承継に伴って個人情報を提供する場合であって、承継前の利用目的の範囲内で当該個人情報を取り扱うとき。

個人情報を特定の者との間で共同して利用する場合であって、次に示す事項又はそれと同等以上のないよう事項を、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。

- イ 共同して利用すること
- ロ 共同して利用される個人情報の項目
- ハ 共同して利用する者の範囲
- ニ 共同して利用する者の利用目的
- ホ 共同して利用する個人情報の管理について有する者の氏名又は名称
- ヘ 取得方法

第 22 条各号のいずれかに該当する場合

- 2 会社の代表者は、第三者に提供する場合の内部承認の手順に関して定めると共に、その記録を作成し、保管・管理しなければならないものとする。

第 6 章 個人情報の適正管理義務

(正確性の確保)

第25条 会社は、利用目的の達成に必要な範囲内において、個人情報を、正確、かつ、最新

の状態管理しなければならないものとする。

- 2 会社は、個人情報の保存期間を定めると共に、定期的にバックアップを取らなければならないものとする。

(安全管理措置)

第26条 会社は、その取り扱う個人情報のリスクに応じて、漏えい、滅失又はき損の防止その他の個人情報の安全管理のために以下の各号に従い組織的、人的、物理的及び技術的、面的において必要、かつ、適切な措置を講じなければならないものとする。

- 組織的安全管理措置
- 人的安全管理措置
- 物理的安全管理措置
- 技術的安全管理措置

- 2 安全性の確保に関して、別に定める営業秘密管理規程を準用するものとする。

(従業員の監督)

第27条 会社は、その従業員に個人情報を取り扱わせるに当たっては、当該個人情報の安全管理が図れるよう、当該従業員に対し必要、かつ、適切な監督を行わなければならないものとする。

- 2 会社は、従業員から営業秘密の守秘義務に関する誓約書を取得しなければならないものとする。
- 3 会社は、ビデオ及びオンライン等により従業員のモニタリングを実施する場合には、労働組合等に通知し協議を行い、以下の各号に関して規定した実施に関する細則を別に定めるものとする。

- モニタリングにより取得する個人情報の利用目的
- モニタリング実施責任者とその権限
- モニタリングに関する社内規程と、事前の周知徹底
- モニタリングの実施状況に関する確認及び監査

- 4 安全確保に関する従業員の監督に関しては、前項各号を準用するものとする。

(委託先の監督)

第28条 会社は、個人情報の取扱いの全部又は一部を委託する場合は、十分な個人情報の保護水準を満たしている者を選定しなければならないものとする。

- 2 会社は、委託を受ける者を選定する基準を確立していなければならないものとする。
- 3 会社は、個人情報の取扱い全部又は一部を委託する場合は、委託する個人情報の安全管理が図れるよう、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ものとする。
- 4 会社は、次に示す事項を契約によって規定し、十分な個人情報の保護水準を担保しなければならないものとする。

- 委託者及び受託者の責任の明確化
- 個人情報の安全管理に関する事項
- 再委託に関する事項
- 個人情報の取扱い状況に関する委託者への報告の内容及び頻度
- 契約内容が遵守されていることを委託者が確認できる事項
- 契約内容が遵守されなかった場合の措置
- 事件・事故が発生した場合の報告・連絡に関する事項

- 5 会社は、当該契約書などの書面を少なくとも個人情報の保有期間にわたって保存しなければならないものとする。
- 6 会社が委託を受ける場合、委託を受けた個人情報が適正に取得されたものであるかどうか、委託元に確認するよう努めるものとする。

第7章 個人情報に関する権利

(個人情報に関する権利)

第29条 会社は、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情報の集合物又は一定の規則に従って、整理、分類し、目次、索引、符合などを付すことにより特定の個人情報を容易に検索できるように体系的に構成した情報の集合物を構成する個人情報であって、会社が、本人から求められる開示、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の求めのすべてに応じることができる権限を有するもの(以下、第7章において「開示対象個人情報」という。)に関して、本人から利用目的の通知、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、(以下、「開示等」という。)を求められた場合は、第32条～第35条の規定によって、遅滞なくこれに応じなければならないものとする。ただし、次のいずれかに該当する場合は、開示対象個人情報ではないものとする。

当該個人情報の存否が明らかになることによって、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のあるもの

当該個人情報の存否が明らかになることによって、違法又は不当な行為を助長し、又は誘発するおそれのあるもの

当該個人情報の存否が明らかになることによって、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれのあるもの

当該個人情報の存否が明らかになることによって、犯罪の予防、鎮圧又は捜査その他の公共安全と秩序維持に支障を及ぶおそれのあるもの

(開示等の求めに応じる手続き)

第30条 会社は、開示等の求めに応じる手続きとして次の事項を定めなければならないものとする。

開示等の求めの申し出先

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方式

開示等の求めをする者が、本人又は代理人であることの確認の方法

第32条又は第33条による場合の手数料(定めた場合に限る。)の徴収方法

- 2 会社は、本人からの開示等の求めに応じる手続き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ものとする。
- 3 会社は、第32条又は第33条によって本人からの求めに応じる場合に、手数料を徴収するときは、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額を定めなければならないものとする。

(開示対象個人情報に関する事項の周知)

第31条 会社は、取得した個人情報が開示対象個人情報に該当する場合は、当該開示対象個人情報に関し、次の事項を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ものとする。

事業者の氏名又は名称

個人情報保護管理者(又はその代理人)の氏名又は職名、所属及び連絡先

すべての開示対象個人情報の利用目的

但し、第21条第1号から第3号までに該当する場合を除く。

開示対象個人情報の取扱いに関する苦情の申し出先

会社が個人情報の保護に関する法律(平成15年法律第57号)第37条第1項の認定を受けた者(以下、「認定個人情報保護団体」という。)の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申し出先

第30条によって定めた手続

(開示対象個人情報の利用目的の通知)

第32条 会社は、本人から、当該本人が識別される開示対象個人情報について、利用目的の通知を求められた場合には、遅滞なくこれに応じなければならないものとする。ただし、第21条第1号から第3号のいずれかに該当する場合、又は第31条第3号によって当該本人が識別される開示対象個人情報の利用目的から明らかな場合は利用目的の通知を必要としないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明しなければならないものとする。

(開示対象個人情報の開示)

第33条 会社は、本人から、当該本人が識別される開示対象個人情報の開示(当該本人が識別される開示対象個人情報が存在しないときにその旨を知らせることを含む。)を求められたときは、法令の規定によって特別な手続きが定められている場合を除き、本人に対し、遅滞なく、当該開示対象個人情報を書面(開示の求めを行った者が同意した方法があるときは、当該方法によって開示しなければならない。ただし、開示することによって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する必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明しなければならないものとする。

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
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
法令に違反することとなる場合

(開示対象個人情報の修正、追加又は削除)

第34条 会社は、本人から、当該本人が識別される開示対象個人情報の内容が事実でないという理由によって当該開示対象個人情報の修正、追加又は削除(以下、この項において「訂正等」という。)を求められた場合は、法令の規定によって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、その結果に基づいて、当該開示対象個人情報の訂正等を行わなければならないものとする。また、会社は、訂正等を行ったときは、その旨及びその内容を、本人に対し、遅滞なく通知し、訂正等を行わない旨の決定をしたときは、その旨及びその理由を、本人に対し、遅滞なく通知しなければならないものとする。

(開示対象個人情報の利用又は提供の拒否権)

第35条 会社は、本人から当該本人が識別される開示対象個人情報の利用の停止、消去又は第三者への提供の停止(以下、この章において「利用停止等」という。)を求められた場合は、これに応じなければならないものとする。また、措置を講じた後は、遅滞なくその旨を本人に通知しなければならない。ただし、第33条各号のいずれかに該当する場合は、利用停止等を行う必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明しなければならないものとする。

(教育・研修)

第36条 会社は、従業員に、定期的に適切な教育を行わなければならないものとする。

2 会社は、従業員に、関連する各部門及び階層における次の事項を理解させる手順を確立し、かつ、維持しなければならないものとする。

個人情報保護マネジメントシステムに適合することの重要性及び利点

個人情報保護マネジメントシステムに適合するための役割及び責任

個人情報保護マネジメントシステムに違反した際に予想される結果

3 会社は、教育の計画及び実施、結果の報告及びそのレビュー、計画の見直し並びにこれらに伴う記録の保持に関する責任及び権限を定める手順を確立し、実施し、かつ、維持しなければならないものとする。

第 8 章 個人情報保護マネジメントシステム文書

(文書の範囲)

第37条 会社は、次の個人情報保護マネジメントシステムの基本となる要素を書面で記述しなければならないものとする。

個人情報保護方針

内部規程

計画書

J I S Q 1 5 0 0 1 : 2 0 0 6 が要求する記録及び会社が個人情報保護マネジメントシステムを実施する上で必要と判断した記録。

(文書管理)

第38条 会社は J I S Q 1 5 0 0 1 : 2 0 0 6 が要求するすべての文書(記録を除く。)を管理する手順を確立し、実施し、かつ、維持しなければならないものとする。

文書管理の手順には、次の事項が含まなければならないものとする。

文書の発行及び改訂に関すること

文書の改訂の内容と版数との関連付けを明確にすること

必要な文書が必要なときに容易に参照できること

(記録の管理)

第39条 会社は、個人情報保護マネジメントシステム及び J I S Q 1 5 0 0 1 : 2 0 0 6 の要求事項への適合を実証するために必要な記録を作成し、かつ、維持しなければならないものとする。

2 会社は、記録の管理についての手順を確立し、実施し、かつ、維持しなければならないものとする。

(苦情及び相談への対応)

第40条 会社は、個人情報の取扱い及び個人情報保護マネジメントシステムに関して、本人からの苦情及び相談を受け付けて、適切、かつ、迅速な対応を行う手順を確立し、かつ、維持しなければならないものとする。

2 会社は、上記の目的を達成するために必要な体制を整備して行わなければならないものとする。

(点検・運用の確認)

第41条 会社は、個人情報保護マネジメントシステムが適切に運用されていることが会社の各部門及び階層において定期的に確認されるための手順を確立し、実施し、かつ、維持しなければならないものとする。

(監査)

第42条 会社は、個人情報保護マネジメントシステムの J I S Q 1 5 0 0 1 : 2 0 0 6 への適合状況及び個人情報保護マネジメントシステムの運用状況を定期的に監査しなければならないものとする。

2 個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、会社の代表者に報告しなければならない。監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保しなければならないものとする。

3 会社は、監査の計画及び実施、結果の報告並びにこれに伴う記録の保持に関する責任及び権限を定める手順を確立し、実施し、かつ、維持しなければならないものとする。

(是正処置及び予防処置)

第43条 会社は、不適合に対する是正処置及び予防処置を確実に実施するための責任及び権限を定める手順を確立し、実施し、かつ、維持しなければならないものとする。

その手順には、次の事項を含めなければならないものとする。

不適合の内容を確認する。

不適合の原因を特定し、是正処置及び予防処置を立案する。

期限を定め、立案された処置を実施する。

実施された是正処置及び予防処置の結果を記録する。

実施された是正処置及び予防処置の有効性をレビューする。

2 公益通報又は安全確保に係る是正措置において、個人情報に関係する場合は、前項を準用するものとする。

(代表者による見直し)

第44条 会社の代表者は、個人情報の適切な保護を維持するために、定期的に個人情報保護マネジメントシステムを見直さなければならないものとする。

2 会社の代表者による見直しにおいては、次の事項を考慮しなければならないものとする。

監査及び個人情報保護マネジメントシステムの運用状況に関する報告

苦情を含む外部からの意見

前回までの見直しの結果に対するフォローアップ

個人情報の取扱いに関する法令、国の定める指針その他の規範の改正状況

社会情勢の変化、一般の認識の変化、技術の進歩などの諸環境の変化

事業者の事業領域の変化

改善のための提案

第9章 個人情報の取扱同意書

(適合性の確認)

第45条 会社は、次に示す内容に関して本人に確認を求めするために個人情報の取扱同意内容書を交付し、同意書を受領し保管しなければならないものとする。

個人情報保護マネジメントシステムとJIS規格の適合性

個人情報の保護に関するガイドラインの合法性

前2号に規定される個人情報の取得・利用・提供・開示に関する内容及び本人の個人情報保護に関する権利の内容と権利行使の方法

2 契約約款等の他の書面との混在又は、文字が小さい等の場合、同意を得るための明示とはならないものとする。

3 同意内容書及び同意書は、手段ごとに必要とするものとする。

4 公益通報に係る、通報書式は取扱同意の下に提出されるものとする。

第10章 その他

(通信網を利用して電磁的記録を送受信する場合)

第46条 通信網を利用して電磁的記録を送受信する場合において、送受信の相手先に関する個人情報を通信網により取得、又は会社が所有・管理する個人情報を通信網で利用・提供・委託するときは、このガイドラインの各条を準用すると共に、外部からの不正

なアクセス等に対し十分かつ最新の電磁的記録の保護管理体制を構築しなければならないものとする。

- 2 送受信の相手先たる本人に対しては、このガイドライン第 20 条、第 23 条、第 24 条、第 31 条、第 32 条、第 34 条及び第 35 条等に定める本人への書面による通知に代えて、電磁的記録の送信の方法による通知を行うことができる。その場合において、送受信時に漏洩・改ざん等のトラブルが発生しないように、前項に準じて保護対策を講じなければならないものとする。
- 3 本人は、このガイドライン第 34 条に定める開示・訂正・削除等の権利の行使において、会社に対し電磁的記録の送信の方法による通知を行うことができるものとする。

(ホームページの管理運営と個人情報保護)

第47条 会社が、ホームページを管理運営する場合、安全管理措置の実施に当たっては、通産省告示「コンピュータウィルス対策基準」・「コンピュータ不正アクセス対策基準」、日本工業規格 JISX 5 0 7 0「セキュリティ技術 - 情報技術セキュリティの評価基準」、及び JISX 5 0 8 0「情報セキュリティマネジメントの実践のための規範」を参考にするものとする。

(付則)

第48条 このガイドラインは、平成 17 年 10 月 20 日から施行する。
改 定 平成 19 年 4 月 20 日