社外秘

個人情報管理マニュアル

平成 17 年 12 月 15 日 制定
平成 20 年 9 月 8 日 改定
(株) ネットグランパス

当マニュアルは、当社役員、正社員、契約社員、パートタイマー、アルバイト、派遣社員も含めた全従業者に適用されます。
当マニュアルは、個人情報保護に関して、特に留意すべきポイントに絞ってお伝えしています。
当マニュアルに関連する規則･基準等は別途、サイトを随時閲覧し、理解を深めてください。
なお、社内規則･基準等は「社外秘」扱いですから、社外に示す場合は許可をとってください。

社長より

当社は、2005年11月8日、個人情報保護JIS規格（JISQ15001）の要求事項に基き、個人情報の取扱いを適切に行っている事業者として、（財)日本情報処理開発協会（JIPDEC）が評価認定している「**プライバシーマーク**」の使用許諾を得ました。今後、以下に留意頂き、個人情報の保護に尽力されるようお願いします。

光回線等、ブロードバンド（高速大容量）通信が浸透し、インターネットのビジネス利用も当り前になった今日、家庭やオフィスに居ながらにして様々な情報やサービスが得られる便利な社会になりました。
しかしその反面、その扱いを誤ると個人情報漏えい・プライバシー侵害を引き起こしてしまうというリスクも増大しています。
事実、マスコミ報道にもあるように、個人情報漏えい事件は依然発生し続けています。大量の流出も目につきます。
・03年6月：ローソンから56万人分、システム委託先から流出
・04年1月：三洋信販から 120 万人分、貸し付け残高情報も
・04年2月：ヤフーBB（現・BBテクノロジー）から460万人分、派遣社員からパスワード流出、対策費は直接分で40億円
・04年3月：ジャパネットたかたから 66 万人分、1ヶ月半営業自粛で 130 億円減収
・04年6月：阪急交通社から 62 万人分、ツアー参加者に金融商品等の電話勧誘
・04年1月：オリエンタルランドから12万人分、入場券購入者の情報が名簿業者に渡り「振り込め詐欺」の被害も
・06年6月：KDDIからネットサービス「DION」の顧客400万人分、内部もしくは委託業者から
・2006年 10 月：日産自動車から顧客情報 538 万人分流出、流出源は特定できず
・2007年3月：大日本印刷から 863 万人分流出、DM 印刷など 43 社からの受託情報を委託先社員が持出し売却
また、最近では Winny や Share といったファイル共有ソフトを介した個人情報漏えい事件が相次ぎ報告されています。
米国でも大きな事件が続いています。
・05年2月：バンク・オブ・アメリカが120万人分、顧客情報を記録した MT を紛失
・05年6月：シティグループから390万人分
・05年6月：マスターカードなどから4000万人分、決済処理委託先会社の情報システムへのウィルス侵入で

個人情報保護制度整備の端緒はすでに1980年の「OECDプライバシー8原則」から始まっています。
OECD8原則の骨子は、個人情報の取得制限、取得目的の明確化、利用制限、安全保護、存在等の公開、確認等への個人参加、等々であり、十分なレベルの個人情報保護を講じていない国への個人データ移転禁止が謳われました。
これらを受けて日本でも様々な制度整備が行われてきました。民間企業に関するものとしては次のようなものがあります。
・1997年：民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン （通産省）
・1998年：プライバシーマーク制度運用開始
・1999年：JIS Q 15001制定
・2005年：個人情報保護法 完全施行
・2006年：JIS Q 15001改定 （個人情報保護法の概念導入）

顧客や消費者の「企業の個人情報保護への取り組み」に対する要求は年々厳しさを増してきております。
当社は、お客様にさまざまなサービスやソリューションを提供しており、顧客からの業務受託、及び関連会社への業務委託における個人情報の管理には万全を期していかなければなりません。

このような取り組みは、先ず皆さんの「個人情報は大切にしなければいけない」という意識を持つことから始めなければなりません。遵法精神の醸成及び意識改革が重要だと考えています。皆さんにおかれましては、個人情報保護の重要性を忘れずに、業務プロセスにおける「基本と正道」の実践はもとより、お客様や社会の信頼に応えるべく、プライバシーマーク認定事業者として相応しい個々の業務遂行を切にお願いします。

平成18年11月　社長

0. はじめに

業務上、個人情報を含む業務を受託する、委託する、等の事象が発生した際に、本マニュアルを参照し適切な取扱いと個人情報の保護に努めてください。

0.1　個人情報の性質及び漏えいの影響

当社は、情報サービス事業を営んでいますので、情報の価値を尊重しなければ当社の事業そのものが成り立ちません。企業の機密情報は、秘密であるが故に情報としての価値があります。これらが他社に漏えいしたり、無断で使用したりすれば重大な問題が生じます。例えば、プログラムなどの著作権のある情報を無断でコピーすると著作権侵害となり、又、営業秘密を無断で使用したり、第三者に開示したりすると使用等の差止めや損害賠償請求の対象となります。その他、秘密保持契約違反の場合は、当該契約解除や損害賠償の問題が生じます。これらは、いずれも権利者や契約相手方との主として企業対企業の関係に限られる問題です。

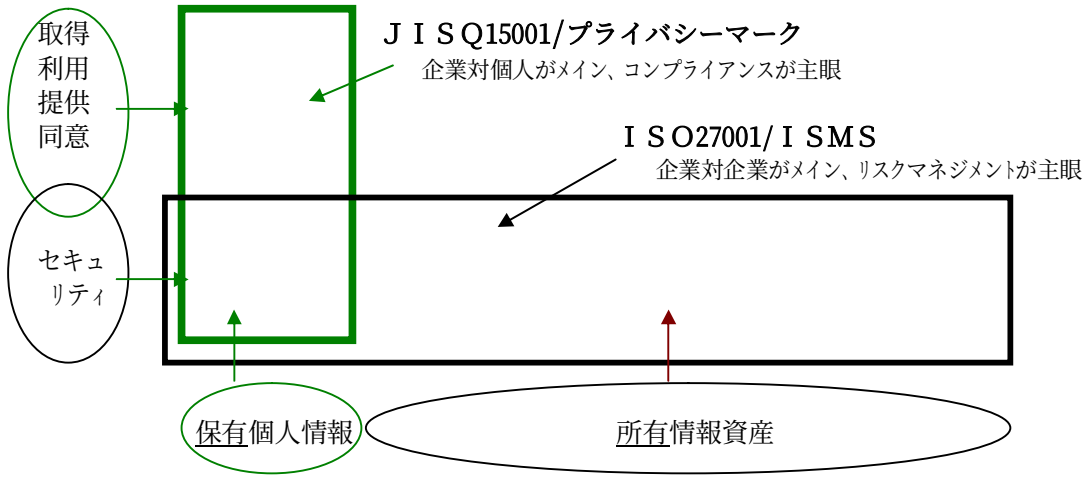
これに対し、個人情報は一般的に企業対個人に関する問題として取扱われるという特性があります。これらが漏えいし、悪用されるとその影響は測り知れません。特に当社が顧客から委託を受けて処理する個人データが万一漏えいすると、顧客との契約に違反し、当該顧客から契約解除や損害賠償請求を受けるだけに止まらず、多数の当該個人からもプライバシー侵害等で責任を追及される恐れがあります。取得禁止情報である人種･民族、門地･本籍地、信教･政治的見解、保健医療等に関係する機微な個人情報が含まれているときは、社会的糾弾に晒される可能性が高く、当社の事業そのものの運営ができなくなります。

このように、個人情報漏えいの影響は、当該個人や契約相手方など一定の範囲内だけでの問題に止まらず、不特定多数の個人や企業の信用失墜等広く社会全体に及ぶことが考えられます。このような事故や事件を引き起こすことがないよう、注意を払いながら個人情報を取扱わなければなりません。

情報サービス業界では、委託先や再委託先から個人情報が漏えいする事件も多く見受けられますので、委託の際には特に注意が必要です。

以上から、個人情報保護のためのプライバシーマークの取得や、セキュリティ対策のためのＩＳＯ27001/ＩＳＭＳ(Information Security Management System) の取得、及びその維持･向上が叫ばれています。当社もプライバシーマークの認証取得を得ておりますので、趣旨ご理解とご協力をお願いします。

参考：ＪＩＳQ15001/プライバシーマーク　と　ＩＳO27001/ＩＳMＳ　の守備範囲



大半の情報は事業者が所有している情報資産であるのに対して、
個人情報は本人からお預かりしている、保有している情報です。

1．適用範囲 （旧JISより適用範囲拡大） （個人情報保護法〔以下「法」という〕 2条3項）

JIS Q 15001：1999（以下「旧JIS」という）では、規格の適用範囲を「個人情報を電子計算機などの自動処理システムで処理している、又は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などによって処理している事業者」としていましたが、JIS Q 15001：2006（以下「JIS」という）では、個人情報を事業の用に供している、あらゆる種類、規模の事業者に適用できる個人情報保護マネジメントシステム（以下「PMS」という）に関する要求事項について規定するとしています。

事業者は、次の事項を行う場合に、JISを用いることができる、とされています。

a)PMSを確立し、実施し、維持し、かつ、改善する。

b)JISとPMSとの適合性について自ら認識し、適合していることを自ら表明する。

c)組織外部又は本人に、JISにたいするPMSの適合性について確認を求める。

d)外部機関によるPMSの認証／登録を求める。

事業とは一定の目的をもって反復継続して遂行される、一般社会通念上事業と認められるものを言います。

従業者の個人情報は事業の用に供している個人情報です。

個人の住所録など個人が自己のために個人情報を取扱っている場合はJISの対象外となります。

運送業、廃棄業、倉庫業、データセンター（ハウジング、ホスティング）等、扱う情報が個人情報に該当するかどうか認識していない（事業の用に供しない）場合もJISの対象外となります。 しかし、当社が これら事業者に個人情報を含む業務を委託する場合は、その旨を明示し、「個人情報保護外注先選定管理規則」に則り、契約をするよう定めています。

当社が事業活動において個人情報を取扱う業務は、下表の通り「**当社業務**」「**受託業務**」の2つに区分できます。

表：当社が個人情報を取扱う場面

業務区分	概　　要
「**当社業務**」	・採用・協力会社従業者受入・顧客の名刺の授受・信用調査会社等からの情報取得等により、直接または間接に**社外の個人情報**を取得する業務。 ・従業者等の氏名、住所、医療・保険情報、口座番号等を取扱う人事、経理等の**社内の個人情報**を取扱う業務。
「**受託業務**」	・取引先企業から、あるいは地方自治体、金融・ガス・電気等個人を対象とした事業を営む顧客から、システム開発や情報処理委託等の業務を受託することにより、住民情報、戸籍情報、預金者情報、利用者情報等**顧客が保有している個人情報**の委託を受けることになる業務など。

この2つの業務毎に適用すべき法令・規則・基準等を考えると、下表の通りとなります。

表：業務に適用する法令・規則等の考え方

	当社の個人情報を取扱う業務形態	
	当社業務	**受託業務**
適用する法令等	・JIS ・個人情報保護法（国）	・JIS ・個人情報保護法（国） ・条例等（地方自治体） ・業界ガイドライン（民間）
適用する規則・基準等	・「**個人情報管理規則**」等 ・その他安全対策関連ルール等	・顧客との契約等で指定された当該顧客が定める規則・基準 ・ただし、顧客より要求された保護の基準に定めのない事項または保護の水準がこの規則に満たない場合は、当該契約に反しない範囲で左記の「**個人情報管理規則**」等を適用。

2. 用語及び定義 （用語を個人情報保護法と統一）（法2条1項～6項、政令1条）

①**個人情報** 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などによって特定の個人を識別できるもの（他の情報と容易に照合することができ、それによって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）。

法の定義では生存者に限られているが、JISでは、当該個人が死亡した場合等、死者の情報も含まれる。病院で昨日亡くなった人の情報は個人情報に含まれる。 ただし（同意の取りようのない）歴史上の人物までは対象としない。

株主総会などで配布される書類等に記載されている役員の経歴、持ち株数など、公表されているような「法人その他の団体の役員に関する情報」を含まない。

②**本人** 個人情報によって識別される特定の個人。

③**事業者** 事業を営む法人その他団体又は個人。

取扱う個人情報の量及び利用方法にかかわらず、個人情報を事業の用に供している全ての事業者が含まれる。

個人情報の取扱い量は問わない。

④**個人情報保護管理者** 代表者によって事業者の内部の者から指名された者であって、PMSの実施及び運用に関する責任及び権限をもつ者。

個人情報の取扱いに関する安全管理面だけではなく、組織全体のマネジメントを含む全体の管理者である。

⑤**個人情報保護監査責任者** 代表者によって事業者の内部の者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、監査の実施及び報告を行う責任及び権限をもつ者。

⑥**本人の同意** 本人が、個人情報の取扱いに関する情報を与えられた上で、自己に関する個人情報の取扱いについて承諾する意思表示。本人が子ども又は事理を弁識する能力を欠く者の場合は、法定代理人等の同意も得なければならない。

本人の署名、同意欄へのチェック、ウェブサイト上での同意ボタンの押下などの明示的口頭による回答などの明示的意思表示が原則。通知後一定期間内に本人の応答が無い場合に同意があったとみなすことは不適切。

子どもとは12歳から15歳までの年齢以下が対象。個人情報の取得時に子ども又は事理を弁識する能力を欠く者であることが明らかな場合若しくは合理的に知り得る状態にある場合、又は取得後に知った場合に、法定代理人等の同意を得ることが求められる。

⑦**個人情報保護マネジメントシステム(PMS)** 事業者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。

旧JISでは「コンプライアンスプログラム（CP）」と称していたが、JIS2006年版では、PDCAのサイクルを重視する他のマネジメントシステム規格と構造の整合性を確保、名称も改められた。

PDCAのサイクルをきちんと回し、個人情報保護水準の維持・向上を行うことも従来以上に求められることになります。

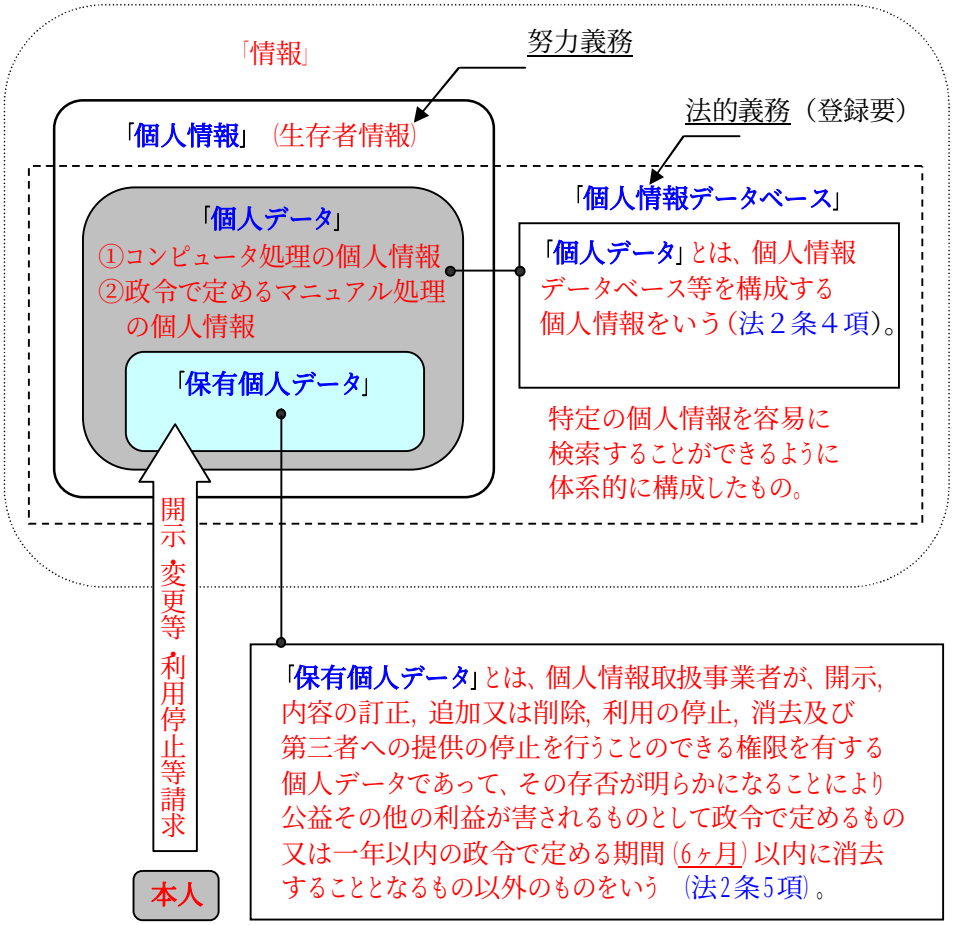
⑧**不適合** JISの要求を満たしていないこと。

不適合だけでは法に違反するとは限りませんが、不適合に対する是正処置及び予防処置は必要です。

【参考】個人情報保護法の定義

「**個人情報**」：生存する個人に関する情報（名前になにかつけば殆ど対象→迷ったら個人情報）
「**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
「**保有個人データ**」：個人情報取扱事業者が（本人に対して）開示・訂正等の権限を有する個人データ
「**個人情報データベース等**」：個人情報を含む情報の集合物（検索が可能なもの）

「個人情報」には努力義務を課し、「個人情報データベース等」に対して法的義務を課している。



法は「個人情報データベース等」に対して法的義務を課しているが、JISはデータベース化していない散在データも対象にしている。
法では6ヶ月以内に消去されるものは対象にしていないが、あまり意味がないため、JISは6ヶ月規定を除いた。また、JISでは個人の数が5000人を超えていない場合も対象としている。
法では個人情報をその形態によって「個人データ」「保有個人データ」「個人情報データベース等」に分類しており、中味によっては色分けしていないが、JISでは個人情報を中味により、リスクに応じて順序付けを行い、それぞれに応じた取扱いを求めている。

3.要求事項

3.1 一般要求事項

JISでは、以下の箇条3で規定する事項のPMSの確立、実施、維持、及び改善を要求しています。

3.2 個人情報保護方針

(法には無い→個人情報の保護に関する基本方針:平成16年4月閣議決定「公表することが望ましい」)

JISでは、「事業者の代表者は、個人情報保護の理念を明確にした上で、個人情報保護方針を取締役会等の決議を経て定めるとともに、これを実行し維持しなければならない」「この方針を文書化し、従業者に周知させるとともに、ウェブサイトや会社パンフレット等、一般の人が入手可能な措置を講じなければならない」 としています。

当社は、個人情報保護方針を別紙のとおり定め、社内に周知徹底するとともに、社外にもWEBで公表しています。

3.3 計画

3.3.1 個人情報の特定

JISでは、「事業者は自らの事業の用に供する全ての個人情報を特定するための手順を確立し、維持しなければならない」としています。

各部署長は、新業務受注・開始の都度、あるいは必要に応じ随時に「個人情報特定手順」により、当該業務が個人情報を含むか否かを特定し、個人情報を含む業務の場合は「プロジェクト個人情報取扱基準」により個人情報保護管理者の承認を得てください。個人情報保護管理者は当該新規業務を都度「個人情報一覧表」に登録し、変更があった旨を毎月の役員会に報告、了承を得るものとします。この台帳には、帳票・ファイル名、媒体形式、取扱件数、取得目的、保有期間、直接間接取得区分、廃棄方法等を定め、PMS適用個人情報を明確にします。個人情報保護管理者は「個人情報一覧表」に記載する全ての個人情報について、PMSの確立並びに有効性の維持のために、個人情報に関するリスク分析を実施し個人情報の漏えい、滅失又は毀損等の発生可能性を認識し、それらに対する合理的な措置を実施します。リスク分析では、事件・事故に起因して想定される損害及び影響を考慮してリスクを評価する。又、個人情報の取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄という情報のライフサイクル各段階におけるリスクを認識します。

①個人情報の洗い出し

偏りや漏れを防ぐため、組織図、個人情報フロー図およびリスク分析表等で、業務を遂行する上発生・利用している個人情報を洗い出す。個人情報フロー図およびリスク分析表は各部署長が作成し、結果を個人情報保護管理者に報告する。

個人情報保護管理者は、個人情報フロー図およびリスク分析表を承認し、当該個人情報を個人情報一覧表へ登録する。

[個人情報洗い出しの手順]

STEP	手順	使用帳票	説明
1	個人情報を含む組織の業務機能を洗い出す 業務で発生、利用している個人情報を書き出す	組織図、 個人情報フロー図およびリスク分析表	発生している情報、利用している情報、他組織とのやりとり、利用するコンピュータシステムなどを可視化するために、業務の流れに合わせてフローチャート化して個人情報フロー図およびリスク分析表に書き出す
2	個人情報を一覧化するために個人情報一覧表を作成する。	個人情報一覧表	個人情報フロー図およびリスク分析表から個人情報を抽出し、個人情報一覧表へ登録する。

②個人情報の属性、管理状態の記入

個人情報保護管理者は、個人情報の属性、管理状態を、個人情報一覧表の該当項目に記入する。

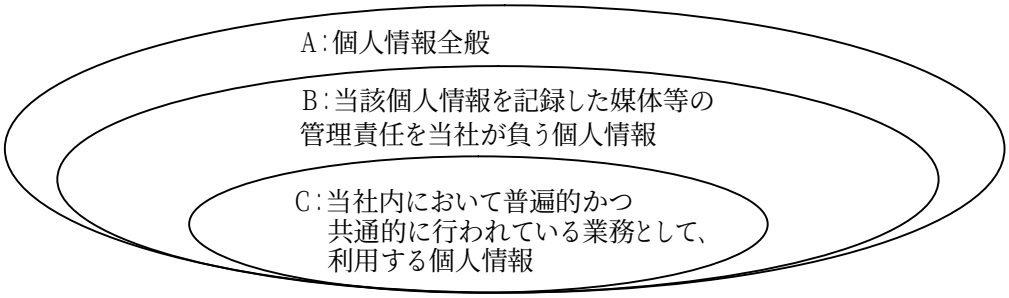
③リスク評価

個人情報保護管理者は、各部署長と調整のうえ、下記手順でリスクの分析･評価を行う。

- 守るべき個人情報を明確にする。
- 個人情報のライフサイクルに応じたリスクを明確にする。
- リスクに対する対応管理策を決定する。
  対応管理策は、有効性、費用のバランスを考慮し、適切なものを採用する。
- 対応管理策実施後に残っている残存リスクを認識する。
  対応管理策を行っても受容可能な水準以下に当該リスクを低減できない場合は、リスクの移転、回避等の対応も検討する。
- 個人情報保護管理者は、個人情報フロー図およびリスク分析表、個人情報一覧表により、リスク評価結果について、社長に報告する。
  また、関連する規則、基準類を整備し、遵守、実行する。

個人情報の区分

当該個人情報A（図内）が 図のBまたはCに該当しない個人の住所録など、個人が自己のために取扱っている情報である場合は、JISの対象外となりますので、これら個人的情報は各個人の責任で、適切に管理をしていただくようお願いします。



次に、 図内のBの、当社が管理する記憶媒体等に記録されている個人情報は、「プロジェクト個人情報取扱基準」等に定め「個人情報一覧表」に登録して、該当部署で管理をお願いします。例えば、以下の業務等が対象になります。

＜登録対象切り分け具体例＞ 《凡例》○：登録対象、×：登録対象外

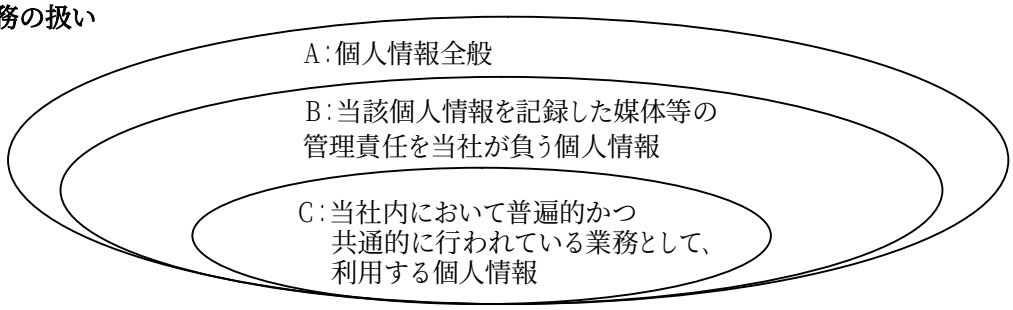
①システム等で、当社にて顧客の実データを借用してテスト実施する。○

②システム等で、個人を特定できないようマスクをした実データを借用し、当社でテストする。×

③マスクされていない実データでのテストを行うがオペレーション及び環境整備のみ実施する。×

④個人情報を含むデータを預かるが、顧客は特に個人情報としての利用や管理を要求していない。×

共通的業務の扱い



さらに、図内のCとして、個人情報のうち当社内の多くの部署において普遍的かつ共通的に実施されている業務（以下「共通的業務」という） において取得、利用する個人情報は、「個人情報一覧表」に登録し、該当各部署で管理します。

共通的業務の扱い　　部分は、登録を要する業務

	分類	該当各部署管理	個人管理
社外情報	1)関係先からの取得	《事例》 ・客先体制表 ・客先電話帖、メールアドレス表 ・障害時緊急連絡表(顧客提出用) ・業務従事者ﾘｽﾄ(顧客提出用) ・業務従事者帰省先一覧(顧客提出用)	《事例》 ・個人管理の名刺 ・個人の手帳・携帯電話等に書かれた連絡先一覧
	2)名刺の授受による取得 3)公開情報等からの取得 4)会員向情報からの取得	《事例》 ・顧客管理ＤＢ ・年賀状ﾘｽﾄ ・ＤＭ送付先ﾘｽﾄ ・帝国データ情報	
	5)その他社外からの取得	《事例》 ・来社受付簿 ・顧客記入のアンケート	
社内情報	6)社内の個人情報	《事例》 ・部署内緊急連絡先 ・部署内帰省先一覧 ・入退室記録表 ・社内情報処理業務 - 利用申請 - 登録 - 履歴管理 - アクセスログ	

3.3.2 法令、国が定める指針その他の規範

JISでは、「事業者は、個人情報の取扱いに関する法令、国が定める指針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」 としています。

JISは全事業者を対象にしており、業界毎の細部については、省庁、自治体毎の法令、指針等の遵守も必要となります。

当社では、個人情報保護法、各地方自治体が制定している個人情報保護条例、その他の法令、行政機関が制定している個人情報保護に関する指針 （ガイドライン）、 各業界が定めたガイドライン 等について、個人情報保護管理者は、定期的（四半期に一度）に関連法規についての省庁のWebサイト又は官報等を参照し、新たに制定あるいは改定された法規及び関連する要求事項を確認し、当社との関連・影響があるものを特定する。関連する法規の新規制定、改訂があった場合は、主な内容と当社事業に関連する条項と主旨について就業者に周知し、対応する。そのうえで、必要に応じ、関連規程等へ反映させる。

これらは「社外文書管理台帳」に登録し、ＷＥＢサイトの従業者向け掲示板で明示します。

3.3.3 リスクなどの認識、分析及び対策

（重要な要求事項であり、かつ審査事項を明確化にするため独立要求項目となった）

JISでは、「事業者は、特定した個人情報について、その取扱いの（ライフサイクル）各局面におけるリスク（個人情報の漏えい又はき損、関連する法令、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」としています。

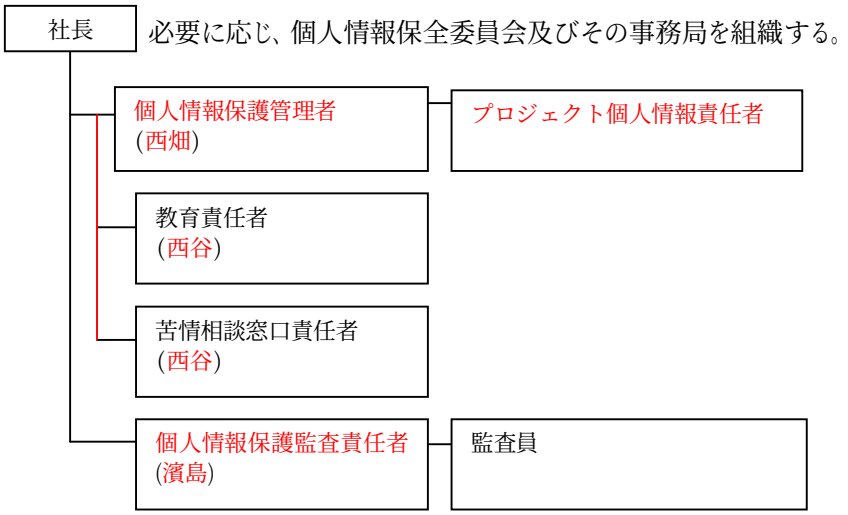
リスクを認識するとは、（ライフサイクル）各局面において適正な保護措置を講じない場合に想定されるリスクを洗い出すことで、リスクを分析するとは洗い出したリスクを定性的な評価などによって評価することです。

必要な対策を講じる手順には利用目的が定められていない個人情報については利用することができない旨の順も含まれてます。特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い(目的外利用)を行わないよう図るため、

個人情報保護管理者は「個人情報一覧表」の内容を新業務受注・開始の都度、あるいは必要に応じ随時に見直し、目的外利用を行っていないか、各部署長に確認を行うものとします。
すべてのリスクをゼロにすることは不可能ですから、現状で取り得る対策を講じた上で、未対応部分は残存リスクとして把握し、管理する必要があります。
リスクは、技術の進展や環境の変化等によって常に変動するものであり、リスクの認識・分析及び対策は、年1回以上、定期的に見直す必要があります。
以上を「個人情報フロー図およびリスク分析表」に記載します。

3.3.4 資源、役割、責任及び権限

JISでは、「事業者の代表者は、PMSを確立し、実施し、維持し、かつ改善するために不可欠な資源を用意しなければならない」としています。また「PMS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、従業者に周知」するよう求めています。従業者とは、当社の組織内で直接間接に当社の指揮監督を受けて当社の業務に従事している者（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のほか、取締役、執行役、理事、監査役、監事、派遣社員等を含みます。特に個人情報保護管理者は「事業者の内部の者から指名し、PMS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、業務を行わせなければならない」とされています。
当社における個人情報の管理体制は以下のように定めています。



各役割と責任等は以下のとおりとなります。

(個人情報保護管理者)
自らこの規則に定められた事項を理解し、及び遵守するとともに、全従業者・関係者に対し、これを理解させ、及び遵守させるため、プロジェクト個人情報責任者を指名し、各プロジェクトの教育計画を立案、実施させ、また安全対策の実施及び周知徹底等の措置を実施する責務を負う。
JISでは「PMSの見直し及び改善の基礎として、社長にPMSの運用状況を報告する」よう求めています。
個人情報保護管理者はPMSの運用状況を、見直しの際等に社長に報告することとしています。

(プロジェクト個人情報責任者)
自プロジェクトで取り扱う個人情報に対し、規則等に定める管理責任を負う。

(教育責任者)
個人情報保護を遵守させるために教育計画を立案し、全従業者・関係者に対する教育を実施する。

(苦情相談窓口責任者)
個人情報保護管理者及びプロジェクト個人情報責任者と協力し、個人情報保護に関して、本人からの苦情及び相談を受け付け、対応する責務を負う。

(**個人情報保護監査責任者**)
規則等に従い、個人情報保護の実施状況及びその運用状況についての監査を定期的に実施する。
実施後速やかに監査報告書を作成の上、社長に報告する。

(**従業者**)
従業者は個人情報保護関連諸規則に精通し、これを遵守しなければなりません。

3.3.5 内部規程

JISでは、事業者は「個人情報を保護するための内部規程を文書化し、維持しなければならない」 また、「事業の内容に応じてPMS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」としています。
当社では以下の諸規程を策定・改訂し、取締役会の決議を経て徹底を図っています。

a) 個人情報を特定する手順に関する規定
「個人情報管理規則」 及び 当マニュアル

b) 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
「個人情報管理規則」 及び当マニュアル

c) 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
「個人情報管理規則」 及び 当マニュアル

d) 事業者の各部門及び階層における個人情報保護のための権限及び責任に関する規定
「個人情報管理規則」 及び 当マニュアル

e) 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
「個人情報保護是正予防処置規則」 及び 当マニュアル

f) 個人情報の取得、利用及び提供に関する規定
「個人情報保護外注先選定管理規則」 「個人情報保護是正予防処置規則」 「個人情報保護見直し規則」
及び 当マニュアル

g) 個人情報の適性管理に関する規定
当マニュアル

h) 本人からの開示等の求めへの対応に関する規定
「プロジェクト個人情報管理規則」「社員個人情報管理規則」 「外注先個人情報管理規則」
及び 当マニュアル

i) 教育に関する規定
「個人情報保護教育規則」 及び 当マニュアル

j) PMS文書の管理に関する規定
「規則等の取扱に関する規則」 及び 当マニュアル

k) 苦情及び相談への対応に関する規定
「個人情報保護是正予防処置規則」 及び 当マニュアル

l) 点検に関する規定
「個人情報保護監査規則」 及び 当マニュアル

m) 是正処置及び予防処置に関する規定
「個人情報保護是正予防処置規則」 及び 当マニュアル

n) 代表者による見直しに関する規定
「個人情報保護見直し規則」 及び 当マニュアル

o) 内部規程の違反に関する罰則の規定
このPMSに違反する行為を行った者に対しては、「就業規則」の定めに従い処分を行います。

3.3.6 計画書

JISでは、「事業者は、PMSを確実に実施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、維持しなければならない」としています。

教育計画書は、個人情報保護研修の年間カリキュラム、個別の研修プログラム（研修名、開催日時、場所、講師、受講対象者及び予定参加者数、研修の概要、使用テキスト、任意参加不可など）及び予算などによって構成され、社長の承認を必要とします。別紙に様式を添付します。

監査計画書は、当年度に実施する監査テーマ、監査対象、目的、範囲、手続、スケジュールなどによって構成され、社長の承認を必要とします。別紙に様式を添付します。

3.3.7 緊急事態への準備 （新設）（審査していた事項を明文化）

JISでは、「事業者は、緊急事態を特定するための手順、また、それらに対応する手順を確立し、実施し、かつ維持しなければならない」また「個人情報が漏えい等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」としています。

また、「個人情報の漏えい等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」としています。

a)当該漏えい等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。
公表によって本人などへの二次被害を招かないように、公表内容、手段及び方法を考慮すること。
受託の場合は、委託契約において何ら取り決めがない場合は、委託者と相談のうえ公表する。

b)二次被害防止、類似案件発生回避などの為、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。

c)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。

緊急事態を特定するための手順及び対応手順の策定に当たっては、次の事項を考慮しています。

－緊急事態及び事故が最も起こりやすい場面
－予想される被害の規模
－被害を最小限に抑えるための一次的な対処方法
－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

漏えい等の緊急事態が発生した場合の対応手順は「個人情報保護是正予防処置規則」に従い、「事件･事故対応票」によって対処してください。

3.4 実施及び運用

3.4.1 運用手順 （新設）（ISO各規格に倣いPDCAサイクルを明確化、ただし、具体的要求事項ではない）

当基準等において、PMSを確実に実施するために、運用の手順を明確にしています。

3.4.2 取得、利用及び提供に関する原則

3.4.2.1 利用目的の特定 （法15条1項）

当社は、当基準等において、個人情報を取得するに当たっては、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うよう定めています。

利用目的は、公序良俗に反しないことが求められています。

「利用目的をできる限り特定し」とは可能な限り具体的に特定することを言います。
利用目的の特定に当たっては次のことに配慮してください。
a)本人から取得する場合、利用目的は、契約などによって明示的に了解されるか、契約類似の信頼関係の中で黙示的に了解されること
b)本人以外の者から取得する場合も、取得する者が利用目的を設定し、取得の相手方との契約などにおいて明示する
c)公開された資料などから取得する場合も、取得する者が公開された目的の範囲内で利用目的を設定する
d)利用目的を特定するに当たっては、取得した情報の利用及び提供によって本人の受ける影響を予測できるように、利用及び提供の範囲を可能な限り具体的に明らかにする

3.4.2.2 適正な取得

当基準等において、適法、かつ、公正な手段によって個人情報を取得するよう定めています。

3.4.2.3 特定の機微な個人情報の取得、利用及び提供の制限

次の各号に掲げる内容の個人情報については、これを取得、利用又は提供（以下「取得等」という）してはなりません。
a)思想、信条及び宗教に関する事項
b)人種、民族、門地、本籍地(所在都道府県情報を除く)、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
c)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
d)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
e)保健医療又は性生活に関する事項
上記 a)～e)に加え、各事業者の実態等によって、一定の範囲を各事業者で定めることができます。
当社は「特定の機微な個人情報」の他に「センシティブな個人情報」を加え下記3区分として、管理を強化しています。

一般的な個人情報：氏名、性別、住所、出生地（県名）、生年月日、家族構成（続柄）、親族関係、電話番号、会社名、職業、地位、社員番号、ID番号、写真（顔など）、声（声紋など）、指紋

センシティブな個人情報：結婚、離婚、学歴、成績、能力、クラブ活動、昇格・降格等、賞罰、容姿、体格、性格、血液型、収入・資産状況、持家・借家の別、各種団体加入状況、趣味、交友関係、各種名簿情報（卒業者名簿、会員名簿等）、口座番号、クレジットカード番号、保険証番号

特定の機微な個人情報：本籍、国籍、犯罪歴、心身障害、傷病名、健康状態、思想、宗教、等.

本項は、法には無い概念です。法では個人情報を中味によって色分けしていません。JISでは個人情報を中味により、リスクに応じて順序付けを行い、それぞれに応じた取扱いを求めています。
ただし、これらの取得等について、明示的な本人の同意がある場合及び 3.4.2.6(利用に関する措置)のただし書き a)～d)（法令、生命の保護等）のいずれかに該当する場合は、取得等を行うことができます。
明示的な本人の同意とは、書面による本人の同意を言います。黙示的な同意は認められません。
特定の機微な個人情報については、これを取得、利用または提供する場合、「個人情報取得等申請書」により個人情報保護管理者の承認を得るようにしてください。

3.4.2.4 書面によって直接取得する場合の措置（同意原則の維持）（法18条,16条）

本人から、書面（電子的方式、磁気的方式など人の知覚よっては認識できない方式で作られる記録を含む）に記載された個人情報を直接に取得する場合には、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、あらかじめ、契約書その他の書面を手渡し又は送付、あるいは本人がアクセスした当社のウェブ画面によって本人に明示し、本人の同意を得なければなりません。
また、新規の種類の個人情報を取得する場合「個人情報取得等申請書」により個人情報保護管理者の承認を得る必要があります。

a)事業者の氏名又は名称
b)個人情報保護管理者（若しくはその代理人）の氏名又は職名、所属及び連絡先
c)利用目的
d)個人情報を第三者に提供することが予定される場合の事項
　－その目的
　－提供する項目
　－提供の手段又は方法
　－当該情報の受領者又は受領者の組織の種類、及び属性（受領企業と提供元企業との関係：関係会社等）
　－個人情報の取扱いに関する契約がある場合はその旨
　個人情報の第三者への提供は、本人が直接関与しないことが多いため、本人に懸念を抱かせないよう、上記事項を具体的に明らかにすることが必要です。
e)個人情報の委託を行うことが予定される場合には、その旨
f)問合わせ窓口
g)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
　本人が個人情報を与えることの任意性とは、申込書への記入が義務的なものなのか、任意（アンケート的なもの）であるかの情報を指し、当該情報を与えなかった場合に本人に生じる結果とは、記入欄に回答しなかった場合に起こり得る結果（例えば、結婚紹介申込書の年収の欄に記入しなければ、年収を考慮した相手を紹介しないことや、中途採用応募時に履歴を記入しなければ選考対象とならないことなど）　を指す。
h)例えばクッキー情報の取得等、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

ただし、人の生命、身体又は財産保護のために緊急に必要がある場合、3.4.2.5（書面以外の直接取得・間接取得）のただし書き a)～d)（生命、当社の利益等に影響）のいずれかに該当する場合及び 3.4.2.6（利用に関する措置）のただし書き a)～d)（法令、生命の保護等）のいずれかに該当する場合は、同意の取得は不要です。

人の生命、身体又は財産保護のために緊急に必要がある場合とは、法18条2項のただし書きを、
3.4.2.5（書面以外の直接取得・間接取得）のただし書きa)～d)は、法18条4項1号～4号を、
3.4.2.6（利用に関する措置）のただし書きa)～d)は、法16条3項1号～4号及び23条1項1号～4号を、
踏まえ規定しています。

3.4.2.5　直接書面取得以外の方法によって取得した場合の措置

（新設）（法概念取込み）（法18条1.4項）

個人情報を 3.4.2.4（直接書面によって取得）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りません。（法18条1項）
直接書面によって取得した場合以外とは間接的に取得した場合　（例えば、委託を受けた、第三者として提供を受けた、公開情報から取得した）、書面によらず取得した場合　（例えば、監視カメラや口頭によって取得した）、等が該当します。
この場合の通知は、事業の性質及び個人情報の取扱状況に応じ、合理的かつ適切な方法によらなければなりません。
サイトの中で利用目的を述べるケースでは、その部分を強調するなりして通知することが望ましいとされています
面談又は電話のように口頭によって個人情報を取得する場合などは、通知も口頭で行ってもよい。
公表は、事業の性質、及び個人情報の取扱状況に応じ、合理的かつ適切な方法によらなければなりません。
例えば、給与計算サービス、伝票の印刷・発送サービス等の場合、「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扱います」等をWEB上で公表するようにしてください。
ただし、次に示すいずれかに該当する場合は、通知又は公表は不要となります。（法18条4項1号～4号）
a)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。 例えば、総会屋情報を取得し、企業相互に情報交換を行う場合、利用目的を通知又は公表

すれば、総会屋の逆恨みによって、第三者たる情報提供者が被害を被るおそれがある場合など。

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

例えば、新商品の開発内容、営業ノウハウ等の企業秘密にかかわるようなものが明らかになる場合など。

c)国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。

例えば、警察から被害者の立ち回りが予想される事業者に限って提供された場合、通知し、又は公表することによって、捜査活動に重大な支障をおよぼすおそれがある場合など。

d)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

例えば、商品やサービス等の販売･提供だけを確実に行うためという利用目的であるような場合（クリーニング店やデリバリーサービスなどで受取人を特定するために個人情報を取得するなど、請求書や見積書等の伝票に記載された担当者名、捺印等）。 ただしその取扱いの委託を受けた場合は該当しない。

3.4.2.6 利用に関する措置

個人情報は、特定した利用目的の達成に必要な範囲内で利用しなければなりません。

必要な範囲を超えて利用する場合はあらかじめ、少なくとも、3.4.2.4（直接書面によって取得）の a)～f)に示す事項又はそれと同等以上の内容の事項を本人に通知し、本人の同意を得なければなりません。

企業内のある部門が取得した個人情報を他の部門が利用する場合、範囲内、範囲外の両方がありえます。範囲外の場合には改めて事前の本人の同意を得ることが必要です。目的外利用に該当するかどうか判断に迷う場合も含め、「目的外利用・提供承認申請書」により社内の承認を得て後、本人に連絡してください。

利用目的を特定した日以降に利用目的を変更した場合、原則本人の同意を得る必要があります。

本人には「個人情報に関するご通知（募集時）」「個人情報の取扱いについて(社員用)」「個人情報の取扱いについて（外注先個人用）」等、すでに取得した同意書に対する変更部分を明示した書面によって通知し、本人の同意を得てください。

ただし、次のいずれかに該当する場合は、同意取得は必要ありません。（法16条3項1号～4号、23条1項1号～4号）

a)法令に基づく場合　　例えば、刑事訴訟法218条の令状による捜査に基づき、個人情報を取扱う場合など。

b)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

例えば、急病その他の事態時に、本人についての、その血液型や家族の連絡先等を医師や看護師に提供する場合。

c)公衆衛生の向上又は児童の健全育成のため特に必要がある場合であっても、本人の同意を得ることが困難であるとき

例えば、不登校生徒について、学校等が連携して対応するために、当該関係機関等の間で情報交換する場合など。

d)国若しくは地方公共団体等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

例えば、事業者が税務署の職員等の任意調査に対し、個人情報を提出する場合など。

3.4.2.7 本人にアクセスする場合の措置 （新設）（同意原則の維持）（法23条4項、16条3項）

取得後でないと連絡先がわからないような個人情報を取得する場合等、事前に本人の同意を得ることが難しい場合は、本人にアクセスする場合に、本人に対して、3.4.2.4（直接書面によって取得）のa)～f)（事業者氏名､利用目的等）に示す事項又はそれと同等以上の内容の事項、及び取得方法を通知し、本人の同意を得なければなりません。

本人にアクセスする場合には「個人情報取得等申請書」により個人情報保護管理者の承認を得てください。

本人にアクセスするとは、本人に対し、郵便、電話、又はメールなどで連絡する又は接触することを言います。

取得方法については、同窓会名簿、及び官報等の取得源の種類並びに、書店から購入等の取得経緯を通知する。

同意については、例えば最初に出すDMに通知文書を同封送付し、同意が得られれば、継続してアクセスできます。

回答が無い場合に黙示の同意があったとみなすことは原則として不適切です。

ただし、次のいずれかに該当する場合は、同意取得は不要です。（法23条4項1号～3号）
この場合も「個人情報取得等申請書」により、個人情報保護管理者の承認を得てください。
a)3.4.2.4（直接書面によって取得）のa)～f)（事業者氏名、利用目的等）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、既に本人の同意を得ているとき
b)個人情報の取扱いを委託された場合でも、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扱うとき
なお、委託を受ける際は、個人情報が適正に取得されたものか委託者に確認するよう努め、明らかに法令違反している場合は委託を受けてはなりません。
c)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3.4.2.4（直接書面によって取得）のa)～f)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扱うとき
d)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3.4.2.4（直接書面によって取得）のa)～f)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
－共同して利用すること
－共同して利用される個人情報の項目
－共同して利用する者の範囲
－共同して利用する者の利用目的
－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
－取得方法
e)3.4.2.5（書面以外の直接取得・間接取得）のただし書きd)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
f)3.4.2.6（利用に関する措置）のただし書きa)～d)（法令、生命の保護等）のいずれかに該当する場合（法16条3項）

3.4.2.8 提供に関する措置 （新設）（法概念取込み）（法23条、16条3項）

個人情報を第三者に提供する場合、あらかじめ本人に対して、取得方法及び3.4.2.4（直接書面によって取得）のa)～d)（事業者氏名、利用目的等）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りません。（法２３条）
なお、旧JISでは、第三者提供を行う場合は、必ず本人同意が必要とされていましたが、 新JISでは下記ただし書きのいずれかに該当する場合は、同意取得は不要とされています。
a)3.4.2.4（直接書面により取得）又は3.4.2.7(本人にアクセスする場合の措置)の規定によって既に3.4.2.4（直接書面によって取得）のa)～d)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
b)大量の個人情報を広く一般に提供するため本人の同意を得ることが困難な場合であって、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、又はそれに代わる同等の措置を講じているとき
－第三者への提供を利用目的とすること
－第三者に提供される個人情報の項目
－第三者への提供の手段又は方法
－本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止すること
－取得方法
c)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、b)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うる状態に置いているとき
d)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

e)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
合併により、両者に利用目的に合致していない新たな部分が生じる場合は同意取得が必要になります。
f)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うる状態に置いているとき
－共同して利用すること
－共同して利用される個人情報の項目
－共同して利用する者の範囲
－共同して利用する者の利用目的
－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
－取得方法
g)3.4.2.6(利用に関する措置)のただし書きa)～d)（法令、生命の保護等）のいずれかに該当する場合（16条3項）

例えば、再提供を含めて本人の同意を得て作成されている名簿は、販売時に改めて同意を得る必要はありません。
大量データベース販売業者も、販売にあたり同意が必要とされていたが、現実困難な場合、本人同意無しに提供することが可能になりました。法ではオプトアウトすることによって直接、提供できるとしていますが、JISでは単にオプトアウトするだけでは駄目でより高いレベルを求めています。例えば、ホームページからクッキーを利用して本人の情報をとる場合も、明示の必要があります。提供を行なう場合は、提供先に「プロジェクト個人情報取扱基準」の写しを交付し、その個人情報がどのように取り扱われるべきか、明確な指示を行なうとともに、提供した年月日、情報名等を記載し受領側の責任者の確認印を受けてください。また、提供先で個人情報が適切に処理されたことを示す証しを残すようにしてください。
個人情報を第三者に提供する場合、「個人情報取得等申請書」により個人情報保護管理者の承認を得てください。
なお、ただし書きb)～g)に該当する事項については、当社は将来に亘って実施の予定はありません。

3.4.3 適正管理

「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」（平成16年10月）を参考。

3.4.3.1 正確性の確保

個人情報は、利用目的の達成に必要な範囲内において、正確、かつ、最新の状態で管理しなければなりません。
正確性を確保するため、誤入力チェック、個人情報を含む内部・外部メモリは別の機器、場所等にバックアップを行うなどの手順を「プロジェクト個人情報取扱基準」に記載してください。
最新性はその利用目的に応じて、必要な範囲内で確保すれば結構です。

3.4.3.2 安全管理措置

個人情報のリスクに応じて、漏えい等の防止その他の安全管理のために必要、かつ、適切な措置を講じてください。
必要、かつ、適切な措置という意味は、経済的に実行可能な最良の技術の適用に配慮することです。
技術面の措置では、①室や保管庫の設置、②特定の者以外がアクセスできないようにすること、③コンピュータにID・パスワード等を設定、④当該個人情報ファイルを暗号化すること　⑤当該個人情報ファイルのバックアップを別の事業所等に保管し管理すること、⑥WEBでの収集はSSL暗号化を施す、等が必要です。

個人情報の組織的安全管理措置・人的安全管理措置については「個人情報管理規則」等で定めています。
個人情報の物理的安全管理措置・技術的安全管理措置については以下のように定めます。

【物理的安全管理措置】
(入退室管理)
・個人情報等の処理は、各事業所内の事務エリア内で行う。パソコン等情報機器は事務エリア内に設置する。
来客等、外来者とは応接エリア内で対応し、事務エリア内には立ち入れないよう図り、他者がパソコン等情報機器を

不正利用又は盗み見できないように留意する。
・各事業所の「面会証」「入退室管理票」は事業所の管理者が毎月内容をチェックし、保管庫に施錠保管する。

(**盗難等の防止**)
・離席時、個人情報関連の書類、マニュアル、媒体、ノートパソコン等は机上に放置せず、保管庫に施錠・保管する。
・デスクトップパソコンは、盗難防止チェーンを取り付けるか、またはHDの暗号化を行う。

(**機器・装置等の物理的な保護**)
・最適化等を毎月1回は実施し、パソコンの性能維持に努める。
・情報機器等の修理を外部業者に委託する場合は、個人情報保護管理者の指示に従う。
・パソコン等情報機器を廃棄する場合、個人情報保護管理者に届出を行い、ツールなどを使用して、HDDの内容を完全に消去する。あるいは指定の外部廃棄業者に委託する。
情報記録媒体は再生不能な状態に破壊して廃棄する。
・その他、盗難、破壊、破損、漏水、火災、停電、地震等への対策等は必要性を見極めつつ順次実施する。

【技術的安全管理措置】

(**アクセス管理**)
・従業者は、業務範囲を超える必要以外の情報へはアクセスしないように心がける。
・従業者は、離席時、パソコンはパスワード付きスクリーンセイバを10分以下で起動するようセットする。
・システム管理者は、新規アカウント・初期設定パスワードを発行し、安全な方法で従業者に通知する。
・従業者は、変更アカウントが必要になった場合、システム管理者に申請する。
・システム管理者は、人事異動・退職等で不要となったアカウントは速やかに削除・停止する。
・システム管理者は、パスワード等が他者へ漏えいの恐れがある場合、直ちにアカウント、パスワードの変更を行う。
・システム管理者は、毎月頭に前月分のアクセスログを取得・点検し、施錠したキャビネット等に保管する。(保管10年)
・システム管理者は、従業者に付与するアクセス権限、同時利用者数、利用時間を最小化する。
・システム管理者は、個人データを格納した情報システムへの不法アクセスからの保護を行う。(ファイアーウォール等)

(**端末、パソコンのパスワードの取扱い**)
・システム管理者は、初期設定のID、パスワードを、社員番号などの推測されやすいものに設定しないよう留意する。
・従業者は、パスワードが発行された後、速やかにログインし、パスワードを変更する。
・システム管理者は、初期設定パスワード発行該当者がログインし、パスワードを変更したことを確認する。
・システム管理者は、ログインの試みの失敗回数を制限するよう手配する。
・異動、退社等の場合は速やかにＩＤを変更・廃棄する。
・従業者は、パスワードを少なくとも3ヶ月に1回以上、下記内容に沿って定期的に変更する。

1	パスワードは数字、英字(大文字、小文字)、記号などを組み合わせて推測されにくいものを使用し、桁数は情報資産及び情報システムの重要度を考慮し、適切に設定しなければならない。(8桁以上とする)
2	一般に使われている単語や本人の氏名番号、電話番号、生年月日などから、他人に推測されやすいパスワードを使用してはならない。
3	設定したパスワードは適切に管理し、他人に漏らしてはならない。

(**情報の漏えい・盗難・紛失等の防止**)
・自分のパソコン・外部メモリに職場の情報はコピーしない。
・職場外に職場のパソコン・外部メモリ、書類、マニュアル類は持ち出さない。
・職場のパソコン・外部メモリ、書類を職場外に持ち出す場合は、身体から離さないよう保持する。
・個人用等の指定外のパソコン等情報機器を職場内に持ち込む場合は、各事業所の管理者の指示に従う。
・不要な情報・書類は即時消去、シュレッダー処理、返却処理を行う。
・パソコン・外部メモリには原則、個人情報(含:メール)は保存しない。
・パソコン等個人情報を含む内部・外部メモリの該当ファイルは暗号化、パスワード付加を行う。
暗号化対策を実施できないモバイル情報機器等は業務用に使用してはならない。

・個人情報を含むモバイル情報機器等を輸送する際は、書留等証跡が残る手段で送付する。
・個人情報を含む書類は郵送せず、持参を原則とする。
・個人情報を含む書類、情報を他部署、他社と収受する場合は収受簿にその旨を記録し、責任者が確認する。
・個人情報を含む書類、モバイル情報機器等を紛失した時は、速やかに個人情報保護管理者へ連絡し、指示を仰ぐ。

(**ウィルス対策**)
・ウィルス対策責任者が定めるアンチウィルスソフトをすべてのパソコン等情報機器に導入しなければならない。
・ウィルス感染を即座に発見、駆除できるよう、アンチウィルスソフトを常時最新の状態に更新するように設定する。
・ウィルス感染していると思われる症状を発見した場合、ウィルス対策責任者へ報告しなければならない。
・ウィルス感染が発見された場合、感染したパソコン等情報機器の属するプロジェクトが利用しているパソコン等情報機器について、社内ネットワークとの接続を中止しなければならない。
・電子メール添付ファイルに対して、必ず利用前にウィルスのスキャンを実施する。
・リスクを考慮し、不要なWebサイトへのアクセスを行ってはならない。
・送信元不明の電子メールに添付された不審な添付ファイルを開いてはならない。
・ファイルを電子メールに添付して送信する場合、ウィルスチェックを必ず実施する。
・社外に持ち出したモバイル情報機器を持ち帰り、再度社内ネットワークに接続する場合、必ず事前に当該モバイル機器のウィルス感染の有無を確認しなければならない。

(**ウィルスに感染した場合**)
・ウィルス感染の対策をすべての作業に優先して行わなければならない。
・発見した場合、速やかにネットワークケーブルを外すと共に、責任者へ連絡する。
・責任者は感染の被害度に応じて、社内ネットワークから切断。
・アンチウィルスソフトの定義ファイルがいつ更新されたかを確認する。
・責任者は、アンチウィルスソフト又はウィルス駆除プログラムを利用し、ウィルスを駆除する。
・ウィルス駆除完了後、再度ファイル全体に対するスキャンを実施しウィルス感染していないことを必ず確認する。
・責任者は、従業者へウィルス感染報告書の提出を指示し、報告を受ける。
・アンチウィルスソフトの未インストール、最新ウィルス定義ファイルの未設定によりウィルス感染した場合、就業規則等に従い処分を受ける場合がある。
・従業者が利用するモバイル情報機器は、インターネット接続等でウィルス感染する可能性が大きいため、対策プログラムの新規リリース時には、これを速やかに適用しなければならない。
・従業者は、モバイル情報機器をＬＡＮ環境から社内ネットワークに接続する場合、所定の事項を必ず実施し、ウィルス感染していないことを必ず確認した後、接続しなければならない。ただし、ウィルス定義ファイルを更新する場合、モバイル環境で更新しなければならない。
・従業者は、顧客常駐先等に当社が貸与するパソコン等情報機器を持ち込む場合、所定の事項を遵守する。
・当社が貸与するパソコン等情報機器のアンチウィルスソフトの運用について、顧客常駐先の規則に従う。

(**セキュリティパッチ等**)
・ＯＳ、アプリケーション等に対するセキュリティ対策用ソフト（セキュリティパッチ）を、常時適用する。
　ウイルス対策をしていても更新をしていないとウィルスに感染する恐れがある。
・自分のパソコンに、Winny、Share 等のファイル交換ソフトは載せない。関係の無いサイトへはアクセスしない。

(**バックアップ等**)
・当該個人情報ファイルのバックアップを毎月１回以上の頻度で実施し、別の事業所等に保管し管理する。

(**電子メールの受信について**)
・心当たりのないメールは開かずに廃棄する。添付ファイルも開かない。
・受信メール閲覧時はプレビューウィンドウを非表示にする。
・受信メールはテキスト形式で表示する。ＨＴＭＬ形式はウィルス感染の恐れあり。
・同報で来たメールに対する回答の宛先は、無用な人に送る事なく、最低限必要な人だけにとどめる。
・用済みのメールはため込まない。（整理・整頓）

(**電子メールの発信について**)
・マル秘情報をメールで送るのは極力避ける。不用意に転送される等で、情報の漏えいに繋がる。
・発信時は、TO（本来の相手。できれば1名に限る。）と、CC（ご参考送付）を使い分ける。
・発信相手が多数になる同報メールでは、メールアドレスを非表示にするため、BCC で送信する。
・添付ファイルはウィルスチェックを行い、チェック済みである旨明示する。
・個人情報等を含むマル秘添付資料は暗号化し、パスワードをかける。
・エクセル、ワード資料についてはパスワードをかける。
・パスワードは別便で通知する。
・会社のメールを個人のＰＣや携帯電話に転送しない。

(**移送について**)
・個人情報を含む媒体、機器を送達する際は、暗号化を行い、書留・小包等証跡が残る手段で送付、または手渡しを原則とする。

(**廃棄について**)
・紙はシュレッダー処理、磁気媒体、PC等は物理的破壊またはデータ消去を確実に実施する。

3.4.3.3 従業者の監督 （新設）（法概念取込み、より明確化）（法２１条）

社長は、従業者に個人情報を取り扱わせるに当たって、安全管理が図られるよう必要、かつ、適切な監督を行うよう求められています。
従業者とは、当社の組織内で直接間接に当社の指揮監督を受けて当社の業務に従事している者（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のほか、取締役、執行役、理事、監事、派遣社員等を含みます。
監査役を他の者が監督することは商法上問題となりますので監督の対象からはずしています。

3.4.3.4 委託先の監督 （法概念取込み、より明確化）

当社が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りません。このため、「個人情報保護外注先選定管理規則」に委託先を選定する基準を定めています。
また、委託先に対して必要、かつ、適切な監督を行っています。（法２２条）
委託先との契約には次の事項を規定しています。
a)委託者及び受託者の責任の明確化
　契約で委託者、受託者の責任分担を定めることはよく行われるが、法的責任は１００％委託元にある。
b)個人情報の安全管理に関する事項
　－個人情報の漏えい防止、盗用禁止に関する事項
　－委託範囲外の加工、利用の禁止
　－委託契約範囲外の複写、複製の禁止
　－委託契約期間
　－委託契約終了後の個人情報の返還・消去・廃棄に関する事項
　派遣者と懲戒処分を含む誓約書をとることは、職安法４４条に反するので注意を要します。
c)再委託に関する事項
　－再委託を行うに当たっての委託者への文書による報告
d)個人情報の取扱状況に関する委託者への報告の内容及び頻度
e)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
f)契約内容が遵守されなかった場合の措置
g)事件・事故が発生した場合の報告・連絡にかんする事項

委託先が倉庫業、データセンター（ハウジング、ホスティング）等の事業者であっても、委託者は委託するものが個人情

報保護であることを認識しているわけですから、委託先選定基準による選定が必要です。
必要、かつ、適切な監督には、契約内容が適切に遂行されていることを毎年1回以上確認することも含まれています。

個人情報の委託を行おうとする場合は、委託先に対し、当該業務は個人情報保護対象業務である旨を明示するとともに、「個人情報の保護に関する覚書」を締結してください。
さらに、委託先に対し、毎年1回以上定期的に、当該案件に係る安全管理等についての「報告書」の提出を求め、個人情報保護責任者は、その内容について確認を行って下さい。
また、2年以内の間隔で「個人情報委託先審査票」により見直しを行い、個人情報保護管理者の承認を得てください。

3.4.4 個人情報に関する本人の権利

3.4.4.1 個人情報に関する権利

(詳細化) (法概念取込み、「開示対象個人情報」の概念を明確化) (法2条5項、政令3条,4条)
電子計算機を用いて、 あるいは他の方法で、 体系的に構成された情報の集合物を構成する個人情報であって、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 (以下「開示等の求め」という) に応じることができる権限を当社が有するもの (以下「開示対象個人情報」という) に関して、本人から開示等を求められた場合は、3.4.4.4 (開示対象個人情報の利用目的の通知) ～3.4.4.7 (開示対象個人情報の利用又は提供の拒否権) の規定によって、遅滞なくこれに応じなければなりません。
本人から何か言われたらそれに従うことを原則とします。
もっとも、受託業務の場合は、受託で預かった個人情報は本人からの「求めのすべて」に応じることは不可能であり、開示対象個人情報とはなりえません。また膨大なアンケート結果等、事業者が整理しきれてない、利用できていない個人情報も開示対象個人情報とはなりえません。
次のいずれかに該当する場合も、開示対象個人情報ではありません。(施行令3条)
a)当該個人情報の在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
例えば、家庭内暴力、児童虐待の被害者の支援団体が加害者及び被害者を本人とする個人情報を有している場合。
b)当該個人情報の在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
例えば、総会屋等による不当要求被害を防止するため、事業者が総会屋等を本人とする個人情報をもっている場合や、不審者、悪質なクレーマー等から不当要求被害を防止するため、当該行為を繰り返す者を本人とする個人情報(ブラックリスト)を保有している場合など。
c)当該個人情報の在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交渉上不利益を被るおそれのあるもの
例えば、防衛に関する兵器・設備・機器・ソフトウェア等の設計、開発担当者名が記録された個人情報を保有している場合や、要人の訪問先やその警備会社が本人の行動予定や記録等を保有している場合など。
d)当該個人情報の在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の安全と秩序維持に支障が及ぶおそれのあるもの
例えば、警察からの捜査関係事項照会や捜査差押令状の対象となった事業者が捜査対象者又は被疑者の個人情報を保有している場合など。

3.4.4.2 開示等の求めに応じる手続き (詳細化) (法概念取込み)

本人から自己の情報について開示等を求められた場合は、「苦情・相談等対応報告書」により、社長に報告した後、「個人情報の開示依頼に関するご回答」を用いて当該個人情報の該当者に対して通知を行う。
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、開示対象個人情報の特定に資する情報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りません。

a)申し出先：苦情相談窓口責任者
b)提出書面の様式その他の開示等の求めの方式
　ｲ.開示依頼の場合「個人情報開示依頼書」
　ﾛ.苦情対応、訂正等依頼の場合「個人情報訂正等依頼書」
　　を、配達記録郵便、または本人限定受取郵便にて送付する。
c)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方法
　本人確認方法は、通常の確認方法（例えば ID、パスワード等）であって、一律に運転免許証又はパスポートの提示を求めるなどすべきではない。
　代理人とは、未成年者又は成年被後見人の法定代理人、本人が委任した代理人を言う
d)3.4.4.4（開示対象個人情報の利用目的の通知）又は 3.4.4.5（開示対象個人情報の開示）の際の手数料の徴収方法
　徴収する手数料は、本人に過重な負担を課するものとならないよう、実費を目処としています。
　特に高額の実費が予想されない場合、上記bの「依頼書」で「手数料として 500 円分の切手をご同封ください」として請求してください。

　対応経過を「苦情･相談等対応報告書」で、都度個人情報保護管理者に報告してください。

3.4.4.3　開示対象個人情報に関する周知など　（詳細化）（法概念取込）（法２４条１項,３７条,政令５条）

当該開示対象個人情報に関し、次の事項を（ウェブ画面等で）本人の知り得る状態に置く必要があります。（法２４条１項）
a)当社の名称
b)個人情報保護管理者の氏名、所属及び連絡先
c)開示対象個人情報の利用目的
d)開示対象個人情報の取扱いに関する苦情の申し出先
e)法３７条１項の認定を受けた者の対象事業者の場合は、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
f)3.4.4.2(開示等の求めに応じる手続き)によって定めた手続き

･上記により、a)～f）をホームページに「開示対象個人情報に関する公表事項」として掲載する。
･本人から問合せがあった場合遅滞なく「開示対象個人情報に関する公表事項」を配布する。
･本人から直接書面によって取得する場合は、下記により a)～c)も通知する。
　　様式 3-b　個人情報に関するご通知（募集時）
　　様式 3-c　個人情報の取扱いについて（社員用）
　　様式 4-b　個人情報の取扱いについて（外注先用）

3.4.4.4　開示対象個人情報の利用目的の通知　（詳細化）（法概念取込み）

本人から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は、苦情相談窓口責任者が個人情報保護管理者の承認を得て、「個人情報の利用目的等に関する通知書」により、遅滞なくこれに応じます。ただし、3.4.2.5（書面以外の直接取得･間接取得）のただし書き a)～c)のいずれかに該当する場合、又は 3.4.4.3(開示対象個人情報に関する周知)の c)によって、開示対象個人情報の利用目的が明らかな場合は利用目的の通知は不要です。そのときは、苦情相談窓口責任者が個人情報保護管理者の承認を得て、「個人情報の利用目的等に関する通知書」により、本人に遅滞なくその旨と理由を説明しなければなりません。（法２４条２項及び３項）

3.4.4.5　開示対象個人情報の開示　（詳細化）（法概念取込み）

本人から開示対象個人情報の開示を求められたときは法令の規定により特別の手続きが定められている場合を除き遅滞なく、苦情相談窓口責任者が個人情報保護管理者の承認を得て、「個人情報開示等依頼書」「個人情報の開示依頼に関するご回答」により、本人に対し当該個人情報を書面等本人の同意した方法で開示しなければなりません。
ただし次の場合には、その全部又は一部を開示する必要はありません。そのときは苦情相談窓口責任者が個人情報保護管理者の承認を得て、「個人情報の開示依頼に関するご回答」により、本人に遅滞なくその旨と理由を通知することとしております。(法25条1項)

a)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
b)当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
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って、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や、同一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、事実上問合せ窓口が占有されることにより他の問合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等。
c)法令違反となる場合

3.4.4.6 開示対象個人情報の訂正、追加又は削除 (詳細化)(法概念取込み)(法26条)

本人から当該個人情報の訂正等を求められた場合、法令の規定により特別の手続きが定められている場合を除き、苦情相談窓口責任者は遅滞なく調査を行い、「個人情報訂正等依頼書」により個人情報保護管理者の承認を得て、、当該個人情報の訂正等を行います。訂正等を行った場合も、行わない場合も、苦情相談窓口責任者が個人情報保護管理者の承認を得て、本人に対し「個人情報の訂正等依頼に関するご通知」により遅滞なく通知します。

3.4.4.7 開示対象個人情報の利用又は提供の拒否権 (詳細化)(法27条,28条)

当社が保有している開示対象個人情報について、本人から自己の情報についての利用又は第三者への提供の停止(以下「利用停止等」という) を求められた場合、苦情相談窓口責任者が個人情報保護管理者の承認を得て、「個人情報訂正等依頼書」によりこれに応じ、措置を講じた後は、個人情報保護管理者の承認を得て、「個人情報訂正等依頼書」により遅滞なくその旨を本人に通知しなければなりません。
停止に著しく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はありません。
ただし、3.4.4.5(開示対象個人情報の開示)のただし書き a)～c)のいずれかに該当する場合は、利用停止等を行う必要はありません。この場合、個人情報保護管理者の承認を得て、「個人情報訂正等依頼書」により本人に遅滞なくその旨と理由を通知しなければなりません。

3.4.5 教育

役員及び従業員に定期的に適切な教育を実施します。教育には、各部門、各階層における以下の事項を含みます。
a)PMSに適合することの重要性及び利点
b)PMSに適合するための役割及び責任
c)PMSに違反した際に予想される結果

個人情報保護教育の内容は、以下のとおりとし、各部署の状況に合わせて実施、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を行います。
結果を報告する際には、単に教育結果を報告するだけでなく、アンケートや小テストを実施することで、従業者の理解度を把握し、必要に応じて教育内容の見直しを図ることや、教育を受けたことを自覚させる仕組みを取り入れるなど、教育の有効性の確認を報告することが必要です。欠席者にも漏れなく教育することが必要であり、全員に実施したことの記録を残すようにしています。

(**全社共通研修**)

年1回、上記 a)～c)の項目について実講座または自習を全員が受けるよう義務づけ、個人情報保護に関する意識の向上と全社共通の規則類の周知を図る。

(**部署研修**)
個人情報を扱うプロジェクトを有する開発･運用部署等についてはプロジェクト個人情報責任者が個人情報を実際に処理する担当者向けに、各部署の基準等の周知徹底のための個別教育を行う。

(**新入社員･異動者向け研修**)
受入後速やかに、前出の研修を行う。

教育は、当社において実際に個人情報を取扱う業務を遂行していく上で、規則等に従い個人情報保護を実践していくために必要かつ重要な事項の一つです。規則等では教育責任者が全員教育や個人情報取扱責任者への教育を策定し実施することにしています。

3.5 PMS文書

3.5.1 文書の範囲 (審査事項の明確化)

以下のPMSの基本となる要素は書面で記述します。
a)個人情報保護方針
b)内部規程
c)計画書
d)JISが要求する記録、及び当社PMSを実施する上で必要と判断される記録

3.5.2 文書管理 (審査事項の明確化)

JISが要求するすべての文書は以下の手順で管理を実施･維持を行います。
文書管理は紙媒体による管理に加え、サイト等、デジタル媒体による管理も行っています。詳しくは「社外文書管理台帳」「社内文書管理台帳」に記載しています。
a)文書の発行及び改訂に関すること
　各文書には発行日、改定日等の日付を明示してください。
b)文書改訂の内容と版数との関連付け
c)必要な文書が必要なときに容易に参照できること

3.5.3 記録の管理 (新設) (審査事項の明確化)

PMS及びJISへの適合を実証するために必要な記録は、以下の手順で作成･維持を行います。
必要な記録とは下記を言います。不必要な記録は「保管しない」、「すぐ廃棄する」 よう徹底をお願いします。
a)個人情報の特定に関する記録
b)法令、国が定める指針及びその他の規範の特定に関する記録
c)個人情報のリスクの認識、分析及び対策に関する記録
d)計画書
e)利用目的の特定に関する記録
f)開示対象個人情報に関する開示等の求めへの対応記録
g)教育実施記録
h)苦情及び相談への対応記録
i)運用の確認の記録

j)監査報告書
k)是正処置及び予防処置の記録
l)代表者による見直しの記録

これら記録は必要なときにすぐに閲覧できるように維持しています。
これらの文書や記録の閲覧部門、閲覧方法、管理担当者、保管場所、保管期間、廃棄方法は、「社外文書管理台帳」及び「社内文書管理台帳」に記載のとおりとします。
廃棄・消去の方法は、紙はシュレッダーで裁断、コンピュータやディスク等は消磁ツール等で完全消去とします。
廃棄・消去を実施した場合は、各責任者は、その実施日、実施方法、実施担当者等の記録を個人情報保護管理者に提出し、個人情報保護管理者の承認を得てください。

3.6 苦情及び相談への対応

個人情報の取扱い及びPMSに関して、本人から苦情及び相談があった場合には、当基準等に従い適切かつ迅速に対応してください。受付時、完了時に「苦情・相談等対応報告書」により、社長に報告してください。

「個人情報保護是正予防処置規則」等で定める緊急時対応、苦情及び相談への対応は以下のとおりですので該当する事態発生時には対応をお願いします。

(対応の対象と報告先)：個人情報保護是正予防処置規則２条～６条を抜粋：

第２条　下記の事象の発生を知った者は影響の程度を自ら判断することなく、その大小に関わらず、「事件・事故対応票」により、下記へ直ちに報告する。

対応の対象		報告先
個人情報の破壊､改ざん､漏洩		社長
本人からの苦情（問合せ、相談）		社長
不適合	JIPDEC 等外部機関による指摘	社長
	その他規則等からの逸脱	個人情報保護管理者
	社内の監査による指摘	個人情報保護管理者
システム障害など		個人情報保護管理者

(個人情報の破壊、改ざんが発生した時の緊急対応手順)

第３条　社長は以下の項目を直ちに関係者に指示し、実施する。
①原因の特定、応急処置を実行する。
②当社内及び影響範囲の全ての組織・人に周知する。（第５条）
本人に影響が及ぶときは、事件・事故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うる状態に置く。
③電子データの場合は、バックアップによる復旧若しくは再作成・入手を行う。
機器の場合は修理、復旧、交換等の手続きを行う。
書類、フィルム等の原本の場合は、可能な範囲で修復を行う。
④二次被害防止及び原因対策を実施する
⑤社内外関連の組織・人に対応結果及び対策を報告、公表、謝罪する。（第５条）

(個人情報の漏洩が発生した時の対応手順)

第４条　社長は以下の項目を直ちに関係者に指示し、実施する。
①原因の特定、応急処置を実行する。
可能な場合、漏洩した個人情報を回収する。
②当社内及び影響範囲の全ての組織・人に周知する。（第５条）
本人に影響が及ぶときは、事件・事故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うる状態に置く
③二次被害防止及び原因対策を実施する

④社内外関連の組織・人に対応結果及び対策を報告、公表、謝罪する。（第５条）

(事件・事故の関係機関への届け出)

第５条　社長は発生した事件・事故が故意の犯罪に基づくと判断される場合、あるいは個人情報に関わる事件・事故である場合は、関係機関に届け出る。（別紙１）

(本人から苦情、問合せ、相談があった場合の対応手順)

第６条　本人から苦情、問合せ、相談があった場合の対応手順は以下のとおりとする。

①本人から個人情報に関する苦情、問合せ、相談を受けた者は、苦情相談窓口責任者に直ちに報告し、その指示に従わなければならない。

②苦情相談窓口責任者は、前項の内容が苦情の場合、第 10 条に定める是正処置を講じる。また都度「苦情･相談等対応報告書」により、社長に報告する。

3.7　点検　（PDCAサイクルの明確化）

3.7.1　運用の確認　（新設）（PDCAサイクルの明確化）

当社のPMSが適切に運用されていることが、各部門、各階層において定期的に確認されるための手順を当基準及び「個人情報保護監査規則」「運用確認手順」等に定めています。

加えて、上記の組織全体として実施する監査とは別に、各部署長は各職場の運用確認を日常的に行います。

毎日、毎月、毎期に確認すべきものには例えば以下のようなものが挙げられます。

毎日：オペレーション、労務、入退室、来客、ウイルスチェック、アクセスログ、等々の見回り確認

毎月：同上、及び機器の適性稼動の確認と検印。部署長が運用状況をチェックし「運用チェック表」に記録、押印

不適合を確認した場合は、「個人情報保護是正･予防処置規則」等に従い、是正処置及び予防処置を行います。

3.7.2　監査

JISへのPMSの適合状況及び運用状況を定期的に監査します。

監査は、PMSの整備状況及び運用状況について行います。

社長は、社内から個人情報保護監査責任者を指名し、監査業務を行わせます。

監査に当たっては、本基準 3.3.3(リスクなどの認識、分析及び対策)によって講ずることとした対策を、監査項目に設定し、実施します。

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、社長に報告します。

監査の計画、及び実施、報告、記録の保持に関して 「個人情報保護監査規則」 に細部を定めています。

3.8　是正処置及び予防処置　（新設）（審査事項の明確化）

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「個人情報保護是正･予防処置規則」に定めています。同規則では次の事項を含んでいます。

a)不適合の内容の確認

b)不適合の根本的な原因の特定、是正処置及び予防処置の立案

c)期限を定め、立案された処置を実施

不適合の内容によっては、長期にわたるものもあり得るので、内容に相応した期限を設定します。

d)実施された是正処置･予防処置の結果の記録

e)実施された是正処置･予防処置の有効性のレビュー

3.9　事業者の代表者による見直し　（詳細化）

監査は社内の現状のルールを前提に、それが守られているかを点検するものであり、それに基づく改善も現状の枠内に止まります。見直しは、それに止まらず、外部環境も考慮した上で、現状そのものを根本的に見直すものです。

社長は、個人情報の適切な保護を維持するために、「個人情報保護見直し規則」に則り、次の事項等について定期的にPMSを見直すこととしています。

a)監査、及びPMSの運用状況に関する報告

b)苦情を含む外部からの意見

c)前回までの見直し結果に対するフォローアップ

d)法令、指針等の改正状況

e)社会情勢の変化、国民の認識の変化、技術の進歩などの諸環境の変化

f)当社の事業領域の変化

g)内外から寄せられた改善のための提案

附則

1．この規則は、平成 17 年 12 月 15 日から施行。

2．平成 18 年 6 月 5 日に改定、施行。

3．平成 18 年 8 月 10 日に改定、施行。

4．平成 18 年 11 月 1 日に改定、施行。

5．平成 20 年 9 月 8 日に改定、施行。

6．この規則を改廃する場合には、つど従業員の意見を聴いて行う。

以 上