個人情報保護管理の手引き

【令和７年５月改訂】

はじめに

個人情報の漏えいや不正利用等の事件が相次ぎ、社会問題化していることを背景に、個人情報保護法制が整備され、このうち国立大学法人が対象となる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が平成17年4月から施行されました。これに伴い、国立大学法人筑波大学（以下「法人」という。）における個人情報の取扱いのルールを規定した国立大学法人筑波大学個人情報保護管理規則（以下「個人情報保護管理規則」という。）が制定され、同じく4月から施行されました。

さらに、令和4年4月の個人情報保護関連法令の改正により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が廃止され、個人情報の保護に関する法律に一本化されました。これに伴い、個人情報保護管理規則の全部改正が行われました。

この手引きでは、個人情報保護管理規則に基づき、職員等として知っておくべき個人情報保護管理のルールを説明していますので、法人の業務を行う上で、ご活用ください。

なお、今後、個人情報保護管理のルールに則って実際に運用していく際に、改善すべき点やご意見などありましたら、巻末の問合せ先にお寄せください。

内容

１　個人情報保護管理規則で使用されることばの定義【2条】・・・・・・・・・・　－2－
２　個人情報保護管理規則の適用の範囲【3条】・・・・・・・・・・・・・・・・　－4－
３　個人情報の保護管理体制【4条～7条】・・・・・・・・・・・・・・・・・・　－5－
４　個人情報の保護に関する職員等の責務【10条】・・・・・・・・・・・・・・　－6－
５　個人情報を取り扱う場合の注意点【11条～15条】・・・・・・・・・・・・・　－7－
６　個人情報の第三者提供制限【16条、18条】・・・・・・・・・・・・・・・・　－10－
７　個人情報の取扱い方法【21条～24条】・・・・・・・・・・・・・・・・・・　－12－
８　情報システムにおける安全確保等【26条～33条】・・・・・・・・・・・・・　－13－
９　情報処理室等の安全管理【34条】・・・・・・・・・・・・・・・・・・・・　－15－
１０　個人情報を取り扱う業務委託の留意点【35条】・・・・・・・・・・・・・　－16－
１１　漏えい等を知った場合の通報体制【36条、37条】・・・・・・・・・・・・　－17－
１２　監査及び点検【38条、39条】・・・・・・・・・・・・・・・・・・・・・　－19－
１３　個人情報ファイル簿の報告【42条、43条】・・・・・・・・・・・・・・・　－19－
１４　個人番号（マイナンバー）及び特定個人情報の取扱い・・・・・・・・・・　－20－
１５　苦情相談及び保有個人情報の開示等の請求【41条、44条】・・・・・・・・　－21－
１６　個人情報保護についての問合せ先・・・・・・・・・・・・・・・・・・・　－21－
個人情報保護管理規則・・・・・・・・・・・・・・・・・・・・・・・・・・・別添

1　個人情報保護管理規則で使用されることばの定義【2条】

① 職員等とは

法人の役員（学長、理事及び監事をいいます。）及び職員（大学教員、附属学校教員、事務職員、技術職員等をいい、非常勤職員を含みます。）並びに派遣労働者をいいます。

② 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。）又は個人識別符号（マイナンバー、運転免許証番号、虹彩、歩行の態様等）が含まれるものをいいます。

③ 個人データとは

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、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又は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をいいます。電子媒体、紙媒体の別を問いません。）を構成する個人情報をいいます。

なお、個人情報保護管理規則附則第２項の規定により、個人情報保護管理規則における「個人データ」は、一部の規定を除き、当分の間、「法人が保有する個人情報」とします。したがって、この手引においては、個人情報保護管理規則において「法人が保有する個人情報」と読み替える定めについては、「個人データ」でなく「法人が保有する個人情報」と表記します。

④ 要配慮個人情報とは

本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとされる個人情報をいいます。

⑤ 保有個人情報とは

職員等が職務上作成し、又は取得した個人情報であって、職員等が組織的に利用するものとして、法人が保有しているもの（ただし、法人文書に記録されているものに限られます。）をいいます。なお、保有個人情報は、本人からの開示等の請求の対象となります。

※法人文書とは、職員等が職務上作成し、又は取得した文書、図画及び電磁的記録であって、組織的に用いるものとして法人が保有しているものをいいます。

⑥ 個人情報ファイルとは

保有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います。

ア　特定の保有個人情報を電子計算機を用いて検索できるよう体系的に構成したもの

イ　氏名、生年月日その他の記述等により特定の保有個人情報を容易に検索できるように体系的に構成したもの（五十音順に並べてあるカルテなど）

なお、個人情報ファイルのうち、1,000 人以上の個人が記録されたものなどの条件を満たしたものは、そのあらましを記載した個人情報ファイル簿を作成し、ウェブサイト等で公開しなければなりません（個人情報ファイル簿については、第４２条を参照してください。）。

⑦ 本人とは

個人情報によって識別される特定の個人をいいます。

Q 「個人に関する情報」とは、具体的にどのようなものですか？

A 本人の氏名など、それだけで特定の個人を識別できる情報だけでなく、性別、生年月日、住所、本籍、学籍番号、職員番号、学業成績、入学試験成績、メールアドレス、学歴、職業などを含みます。

Q 住所だけでも個人情報になるのですか？

A 住所だけでは、特定の個人を識別できないので個人情報には当たりません。ただし、他の情報と照合することで特定の個人を容易に識別できる場合は、その情報と併せて全体として個人情報となることがあります。

Q ウェブサイトに対するアクセスについて、日付、時刻、ＩＰアドレス、ドメイン名をログとして取得しています。このログは個人情報に該当しますか？

A 学外からのアクセス者については、ドメイン名とＩＰアドレスから個人を特定するには、プロバイダ等の事業者への特別な照会が必要となることから、基本的には個人情報には該当しません。ただし、学内からのアクセス者については、そのログとアカウント情報を照合することで個人を特定できるので、個人情報となります。また、欧州（ＥＵ加盟国及びアイスランド共和国、ノルウェー王国、リヒテンシュタイン公国並びに英国（グレートブリテン及び北アイルランド連合王国））からのアクセスの場合、ＧＤＰＲ（General Data Protection Regulation：一般データ保護規則）又はその相当法令が適用され，個人情報として扱う必要があります。したがって、アクセス元によって別のログとして記録するのでない限り、ログも個人情報として扱う方が無難でしょう。

Q 上記のほか、どのようなものが個人情報に該当しますか？

A 評価情報、公刊物等によって公にされている情報、映像や音声による情報なども特定の個人を識別できる情報であれば個人情報に該当します。これらには、防犯カメラに記録された本人が判別できる映像情報、本人の発言などを録音した音声情報、tsukuba-tarou@un.tsukuba.ac.jp のように文字列だけで特定の個人を識別できるメールアドレス、雇用管理情報（職員の職務評価に係る情報を含む。）、教職員一覧に掲載された情報などがあります。

Q 研究目的で個人情報を取得しましたが、漏えいが恐いので、すぐに廃棄してもよいでしょうか？

A それが法人文書に記録された保有個人情報であれば、法人文書管理規程に定められた保存年限があるため、直ちに廃棄することはできません。保存年限の間、漏えい等のリスクを伴うので、極力、個人情報は取得しないよう心がけてください。なお、法人文書に該当しない場合は、保存年限は定められておりませんので、直ちに廃棄して差し支えありません。

２　個人情報保護管理規則の適用の範囲【3 条】

法人の全ての職員等に適用され、法人から個人情報の取扱いの委託を受けた者が受託した業務を行う場合について準用されます。

Q　学生をアルバイト雇用していますが、個人情報保護管理規則が適用されるのですか？

A　職員等には、大学教員、附属学校教員、事務職員、技術職員等のほか、非常勤職員（ＴＡ、短期雇用者等を含みます。）や派遣労働者も含まれます。学生をアルバイトとして雇用している場合は、当該学生も同規則の適用対象となります。

Q　指導している学生が卒業研究でアンケート調査を行い、個人情報を取得した場合にも個人情報保護管理規則が適用されるのですか？

A　指導教員は当然適用の対象となりますが、学生も「法人から個人情報の取扱いの委託を受けた者」として同規則が適用されます。

Q　雇用関係のない派遣研究者を研究指導していますが、その研究過程で個人情報を取得した場合はどうなりますか？

A　個人情報を指導教員の影響下で取得した場合は、指導教員が個人情報保護管理規則の対象となります。

3　個人情報の保護管理体制【4 条～7 条】

法人の個人情報を適切に保護管理するため、下記の体制を整備しています。

管理者	主な役割
個人情報総括保護管理者：総務を担当する副学長	法人が保有する個人情報の管理に関する業務を総括 ・個人情報の保護に関する意識の高揚を図るための啓発や教育研修の実施【9 条】 ・事案の内容等に応じて、学長、文科省等へ速やかに報告、公表等【36 条, 37 条】
個人情報システム管理者：情報を担当する副学長	法人が保有する個人情報に係る情報システムを適切に管理 ・情報システムの管理、運用及びセキュリティ対策に関する教育研修の実施【9 条】 ・個人情報保護管理者に対し保有する個人情報の安全確保措置を講じさせること【26 条】
個人情報保護管理者：系長、計算科学研究センター長、生存ダイナミクス研究センター長及び個人情報総括保護管理者が指名する者（系長、域長、研究群長、専攻長、研究群の学位プログラムリーダー、センター長等） 附属学校長 附属病院長 課長、室長、エリア支援室長、社会人大学院等支援室長、海外教育拠点支援室長、技術室長等	各組織における法人が保有する個人情報の適切な管理を確保 ・課等の職員に対する教育研修への参加の機会を付与【9 条】 ・法人が保有する個人情報の秘匿性等その内容に応じたアクセスや複製等の制限、暗号化、端末の限定、端末の盗難防止・記録機能を有する機器・媒体の接続制限等の措置【21 条, 22 条, 29 条, 30 条, 31 条, 33 条】 ・個人情報の漏えい（発生のおそれを含む。）等に係る事案の報告及び再発防止措置【36 条】
個人情報保護担当者：個人情報を管理する大学教員、附属学校教員、個人情報保護管理者が指名する者	個人情報保護管理者を補佐し、各組織における個人情報の管理に関する業務を処理
監査責任者：学長が指名する監事	法人が保有する個人情報の管理の状況について監査

Q　大学教員が保有し管理する個人情報については、系長の指名する者が個人情報保護管理者となっていますが、どのような趣旨ですか？

A　系によって規模や運営の方法などが異なるため、各系の事情を考慮して、系長に指名していただくものです。情報システムに精通した者や系長本人、域長などが想定されます。なお、人数の制限は設けておりません。

Q　私が所属する組織の個人情報保護管理者は、誰ですか？

A　教職員専用サイトに一覧を掲載していますので、ご確認ください。
（https://ksp.sec.tsukuba.ac.jp/wp/?page_id=4687）

Q　個人情報保護管理者は、どのようなことをすればよいのですか？

A　具体的な業務については、「個人情報保護管理者の職務内容及び責務について」を教職員専用サイトに掲載していますので、ご確認ください。
（https://ksp.sec.tsukuba.ac.jp/wp/?page_id=4687）

4　個人情報の保護に関する職員等の責務【10 条】

①　職員等は、関連法令、個人情報保護管理規則等の規定及び個人情報保護管理者等の指示に従い、個人情報を取り扱わなければなりません。また、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方法により、個人情報を利用してはなりません。

②　職員等は、その業務に関して知り得た個人情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはなりません。職員等ではなくなった後も同様です。

Q　業務に関して知り得た個人情報の内容をみだりに他人に知らせるとは、どういうことですか？

A　「みだりに他人に知らせる」とは、正当な理由がなく個人情報の内容を他人に知らせることです。また、「知り得た個人情報」は、当該情報に秘匿性があるかないかを問いません。

Q　違反した場合はどうなるのですか？

A　職員の場合は、法令遵守義務違反で懲戒処分されることや法の罰則が適用されることが考えられます。

5　個人情報を取り扱う場合の注意点【11 条～15 条】

①　個人情報を取り扱うことができるのは、業務の遂行に必要な場合に限ります。また、取得の際は利用の目的を特定しなければならない上、あらかじめ、本人に対し、その利用目的を通知又は公表しなければなりません。あらかじめ本人に通知又は公表した利用目的に含まれていない目的のために個人情報を利用してはならず、新たに利用目的を追加する場合は当該利用目的の変更について通知又は公表しなければならないため、個人情報を最終的にどのような目的で利用するのか、個人情報を提供することはあるのかなどについて、十分検討を行ってください。なお、第三者に個人情報を提供する予定があるときは、利用目的にその旨を含める必要があります。

※利用目的の通知又は公表の必要がない場合については、個人情報保護管理規則第１２条を参照してください。

②　偽りその他不正の手段により個人情報を取得してはなりません。

③　保有する個人情報は正確性を確保する必要がありますので、利用目的の達成に必要な範囲内で、保有する個人情報が現在の事実と合致するように努めてください。

④　要配慮個人情報は、あらかじめ本人の同意を得ないで取得してはなりません。

※本人の同意を得る必要がない場合については、個人情報保護管理規則第１３条第２項を参照してください。

Q　利用目的の「公表」とは、具体的に何をするのですか？

A　「公表」とは、広く一般に自己の意思を知らせること（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。）をいい、具体的には、ホームページ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、本人となる者（例えば学生等）が訪れることが想定される場所におけるポスター等の掲示やパンフレットの配布等を想定しています。

Q　アンケートの質問項目で個人情報を取得する予定ですが、どのように利用目的を明示すればよいのですか？

A　アンケートの記入要領などに、どのような目的で利用するのかをできる限り詳しく書いてください。

Q　別の部局で保有している個人情報を内部で提供してもらい、新しいイベントの案内を送付するために使いたいが、問題ないですか？

A　取得の際に本人に明示する利用目的の中に、イベント一般の案内の送付が含まれていれば問題ありません。イベント案内が含まれていないか、対象とするイベントが限定されていて「新しいイベント」が対象であれば、利用目的の変更が必要です。
また、変更後の利用目的が変更前の利用目的からみて、社会通念上、本人が通常予期し得る限度と客観的に認められる範囲内で変更する場合は、変更された利用目的を本人に通知又は公表することが必要です。

上記の範囲を超えて変更する場合は、改めて本人の同意を得なければなりません。ただし、本人の身体等の保護のために必要があり、かつ本人の同意を得ることが困難である場合等、個人情報保護管理規則第１２条各号に掲げる場合は、あらかじめ本人の同意を得ることなく、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱うことができます。

Q　個人情報を第三者に提供する予定があるのですが、取得時点の利用目的に「提供」を含めた方がよいのでしょうか。また、提供先の名称なども明示する必要があるのでしょうか？

A　個人情報を第三者に提供する予定がある場合、取得の際に本人に明示する利用目的の中に「提供」することを明確に示しておく必要があります。
なお、外国にある第三者への提供の場合を除き、提供先の名称までは明示する必要はありませんが、想定される提供先の範囲や属性を示すことが望ましいとされています。

Q　構内に防犯カメラを設置したいのですが、利用目的の明示は必要ですか？

A　撮影する映像は個人識別性があり個人情報に当たりますので、利用目的を特定した上でそれを通知又は公表する必要があります。防犯カメラの設置に当たっては、その目的の達成に必要な範囲内で利用し、隠し撮りにならないよう構内の設置場所に「防犯カメラ作動中」などの表示することが必要と考えられますが、この場合、「防犯カメラ」と言えば、それによって取得した個人情報の利用目的は明らかですので、「防犯のため」等具体的な利用目的を付す必要はありません。

Q　隠しマイクを使って、会議や会話などを録音してもよいですか？

A　個人の声は、会話の内容等から特定の個人を識別することが可能な場合（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可能な場合を含む。）は個人情報に該当しますので、個別の事例ごとの判断が必要です。録音した音声から特徴情報を抽出し、これを装置やソフトウェアにより本人を認証することができるデータに変換した場合には、当該データは個人識別符号に該当するため、それ単体で個人情報に該当します。
個人情報に該当する場合は、個人情報保護法上、当該情報を取得する上で利用目的を通知又は公表する義務を負いますが、録音していることについて伝える義務までは負いません。つまり、録音することについては伝えなくてよいものの、会議や会話で得ることとなる個人情報については、その利用目的を通知する必要があります。

Q　入退室管理や学内への入場者管理のため、来訪者に備付けの名簿に氏名などを記入してもらっていますが、何か問題はありますか？

A　本人以外の者が、名簿に記載されている氏名から既に来訪した人物の個人情報を知ることができるので、先に記入した人物の個人情報が見えないように、別の紙で既に記載されている部分を隠す等の対応が必要です。できる限り備付けの名簿形式ではなく、単票

形式で個人毎に氏名を記入してもらうなどの方法をとることがより適切です。

6　個人情報の第三者提供制限【16 条、18 条】

① 個人情報保護管理規則第１６条各号に掲げる場合を除き、あらかじめ本人の同意を得ないで、保有する個人情報を第三者に提供してはなりません。したがって、個人情報を第三者に提供するときは、本人の同意を得ることが必要です。

② 第三者に提供するに当たっては、第三者提供に係る記録を作成し、及びこれを保存することが必要です。保存期間は、別に定めのある場合を除き３年間となっています。第三者提供に当たって契約を締結する場合は、契約書等によって記録とすることができます。

【記録項目】

・提供した年月日
・法に規定する本人の同意（上記①）を得ている旨
・提供先の第三者の氏名又は名称
・提供する個人情報によって識別される本人の氏名等
・提供する個人情報の項目

なお、外国にある第三者に個人データを提供する場合にあっては、別の定めが適用となりますので、個人情報保護管理規則第１７条その他関係法令を参照してください。

Q 「本人の同意を得る」とは、具体的にどのようなことを指しますか？

A 同意する旨の口頭による本人からの意思表示、同意する旨の本人からの書面（電磁的記録を含む。）の受領、同意する旨の本人からのメールの受信、同意する旨の確認欄（又はウェブサイト上のボタン）へのチェック等を本人から得ることをいいます。なお、「拒否する意思表示がなければ同意したものとみなす」といった、いわゆるオプトアウトの取扱いは、個人情報保護法が定める手続を経たものでなければ、ここでいう「同意を得る」には該当しません。

Q 本人の同意を得ることなしに保有する個人情報を第三者に提供してはいけないということですが、その規定が除外される個人情報保護管理規則第１６条第１号に規定する「法令に基づく場合」とは、具体的にどのような場合ですか？

A 例えば、捜査令状や刑事訴訟法第１９７条第２項に基づく捜査関係事項照会書により職員又は学生などの連絡先の照会があった場合や、弁護士法第２３条の２に基づく弁護士会照会制度により調査・照会があった場合が該当します。

Q どのような場合に保有する個人情報を本人以外の者に提供できるのですか？

A 本人の同意があるとき又は個人情報保護管理規則第１６条各号に規定する場合に該当するときです。同条各号に規定されている場合とは、例えば人の生命等を保護するために必要があるとき、個人情報の提供が学術研究の成果の公表等のためやむを得ないとき、共同研究等のために必要があるときなどです。なお、第三者への「提供」には該当しないものではありますが、法人の内部における利用の場合であっても、あらかじめ利

用目的に含めるか、本人の同意を得るか、又は後述する仮名加工情報として取り扱うかのいずれかでなければ個人情報を利用できませんので、ご注意ください（令和４年４月１日施行の法改正による）。

Q　外部から特定の職員の内線番号や研究室、メールアドレスなどの問合せがありましたが、教職員一覧で調べて回答してもよいですか？

A　教職員一覧に掲載された個人情報は学内での連絡に利用するという目的で取得された個人情報になりますので、外部に提供することは、当該職員本人の同意がないとできません。したがって、回答する場合は、個別に当該職員本人の同意を得てから回答してください。

【個別に同意を得る場合の対応方法例】

(1)　「お問合せの件につきましては、本人の了承が必要となります。本人に確認を取りますので、しばらくお待ちください。」と、電話を保留状態として、本人に確認する。

(2)　「○○○様から○○○のため連絡を取りたいので、あなたの内線番号（又は研究室、メールアドレスなど）について問合せが入っておりますが、お伝えしても差し支えないでしょうか？」と確認し、同意が得られたら回答する。

《本人が拒否した場合》「本人に確認しましたところ、同意が得られませんでしたので、回答できません。どうぞご理解いただきますようお願いします。」

《本人が不在で確認できない場合》「本人が不在で確認ができませんでした。」

Q　○○○○さんという職員の在籍確認の問合せがあった場合は、回答してよいですか？

A　在籍情報は個人情報であり、法令等に定めのある場合を除き、本人の同意が必要です。

7　個人情報の取扱い方法【21 条～24 条】

① 個人情報保護管理者は、個人情報の秘匿性等その内容に応じて、当該個人情報にアクセスする権限を有する職員等の範囲とその権限の内容を、当該職員等が業務を行う上で必要最小限の範囲に限定します。当然、アクセスする権限を有しない職員等は個人情報にアクセスしてはいけませんし、アクセスする権限を有する場合であっても、業務上の目的以外の目的で個人情報にアクセスしてはいけません。

② 職員等は、業務上の目的で個人情報を取り扱う場合であっても、個人情報の複製及び送信並びに個人情報が記録されている媒体の外部への送付及び持出し等に際しては、個人情報保護管理者の許可が必要です（ただし、当該個人情報の秘匿性等その内容に応じ、これらを行うことができる場合については限定されます。）。

③ 職員等は、個人情報保護管理者の指示に従い、個人情報が記録されている媒体を定められた場所に保管し、必要な場合は、保管庫等への保管、施錠等を行ってください。

④ 個人情報が不要となった場合は、個人情報保護管理者の指示に従い、復元又は判読が不可能な方法により消去又は廃棄を行ってください。

※ 復元又は判読が不可能な方法の例

紙媒体の場合：溶解処理、シュレッダーを用いた裁断処理

パソコン等の情報機器を記録媒体としていた場合：データ消去ソフトの使用、記憶装置の物理的な破壊

なお、個人情報保護管理者は、管理する個人情報の消去や廃棄について、特殊な媒体の場合や量が多いなどの理由で消去や廃棄が困難な場合には、組織の長や関係部署（大学教員等にあってはエリア支援室等）と連携して措置を講じてください。

Q パソコンが不要になったので、一つひとつのデータを「ゴミ箱」で削除したうえで廃棄してもよいですか？

A ハードディスク等の記録媒体に記録されているデータは、システム上のゴミ箱等の機能でデータを削除しても完全に消去することはできません。専用のデータ消去ソフトを使用するか、当該記録媒体を物理的に破壊した後に廃棄してください。

Q 古い職員録、研究者総覧、学生名簿等を今後も保有して使用してもよいですか？

A 業務上必要であれば構いませんが、個人情報保護管理規則及び法人文書管理規程に従って適切に管理してください。

Q 附属学校の教員ですが、自宅に通知表を持ち帰って、生徒の成績をつけたいのですが？

A まずは、ＵＴＯＳ（筑波大学オンラインストレージ）を利用したり、職場の執務室等で作業を行ったりする等で対応できないかを検討し、極力持出しは行わないようにします。それでもやむを得ない場合の個人情報の持出しには、個人情報保護管理者の許可が必要です。

8　情報システムにおける安全確保等【26 条～33 条】

① システム管理者は、個人情報の漏えい等の防止その他個人情報の適切な管理のため、個人情報保護管理者に(1)パスワード等を使用してのアクセス制御、(2)個人情報へのアクセス状況の記録、(3)外部からの不正アクセス防止、(4) コンピュータウィルスの感染防止等に必要な措置等を講じさせることとしています。これらの措置は、各個人情報保護管理者と各組織の長等及び個人情報システム管理者が連携して講ずることになります。なお、予算や技術的な制約のため直ちに措置ができない場合には、差し当り＝個人情報の処理を行うパソコンはネットワークに接続せずスタンドアローンで使用するなどの対策を講じてください。

② 職員等は、パソコンをネットワークに接続している場合には、不正アクセス等によってデータを書き換えられたり、改ざんされる場合がありますので、定期的に入力原票と入力内容との照合等を行ってください。

③ 個人情報保護管理者は、個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置を講じ、職員等は、その処理する個人情報について、秘匿性等その内容に応じて、適切に暗号化を行ってください。

④ 個人情報保護管理者は、盗難又は紛失の防止等のため、処理を行うパソコンの限定やパソコンの固定、執務室の施錠等の必要な措置を講じてください。

⑤ 職員等は、個人情報保護管理者が必要と認める場合を除き、パソコンの外部への持出しと外部からの持込みを避けてください。

⑥ 職員等は､パソコンの使用に当たって､個人情報が第三者に閲覧されることがないよう、使用状況に応じて、情報システムのログオフを行ったり、パスワードを設定したスクリーンセーバーを施したりする等の必要な措置を講じてください。

⑦ 個人情報保護管理者は、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器・媒体について、処理を行うパソコンへの接続の制限等の必要な措置を講じてください。

Q　研究室のパソコンにＴＷＩＮＳ（教育情報システム）からダウンロードした学生の成績が入っていますが、どうすればよいのですか？

A　業務上必要な場合を除き、ダウンロードした成績データは消去してください。なお、学生の指導などに使用する場合は、保有する個人情報となりますので、個人情報保護管理規則に従って管理してください。

Q　個人情報の入っているデータをＵＳＢメモリ等で自宅に持ち帰り、自宅のパソコンで作業をしたいのですが、よいでしょうか？

A　個人情報の持出しには個人情報保護管理者の許可が必要となります。また、小型の記録媒体は紛失しやすく、個人情報の漏えい等の事案が後を絶ちませんので、許可を得て個人情報を持ち出す場合であっても極力使用を避けてください。
なお、職員等にあっては、ＵＴＯＳを使用すれば、個人情報を持ち出すことなく、当該情報に安全かつ確実にアクセスし、閲覧や編集ができます。

Q　個人情報が入ったパソコンが研究室から行方不明になってしまいました。誰かに報告が必要ですか？

A　直ちに個人情報保護管理者に報告してください。個人情報保護管理者は、状況を確認後、教職員専用サイトに掲載している「個人情報の紛失・漏えいはすぐに報告！」に従い、コンプライアンス・ハラスメント対策室に第一報を報告してください。

Q　Office365 のアプリや職場の同僚の個人情報が入ったスマートフォンをなくしてしまいました。誰かに報告が必要ですか？

A　スマートフォンのリモートロックを設定するとともに、回線を切断することをおすすめします。その後、直ちに個人情報保護管理者に報告してください。個人情報保護管理者は、状況を確認後、教職員専用サイトに掲載している「個人情報の紛失・漏えいはすぐに報告！」に従い、コンプライアンス・ハラスメント対策室に第一報を報告してください。

紛失後の Office365 へのログイン状況等を確認することとなります。

Q　大学教員ですが、毎日メールが大量に届き外出先でも容易に確認できるようにするため、tsukuba.ac.jp のメールアドレスに届くメールを自分のプライベートなメールアドレスに自動転送する設定をしています。何か気を付けることはありますか？

A　法人においては、法人のメールアドレスから私的なメールアドレスに転送設定を行う際の転送先の設定ミスにより、個人情報が第三者に漏えいした事案が発生したことがありますので、転送は十分に気を付けて行ってください。なお、当該漏えい事案を受けて、令和７年度から、本学のメールアドレス（@u.tsukuba.ac.jp 及び@un.tsukuba.ac.jp）において転送設定を有効にした場合、緊急事態を想定して、届け出された転送先の私的メールアドレスのリストを個人情報総括保護管理者が一元的に管理する体制となりましたので、ご承知おきください。

Q　私が担当する業務において、担当教員に個人情報を送付する必要があるのですが、気を付けることはありますか？

A　法人においては、いわゆるＰＰＡＰメール（パスワード付き添付ファイルの略。パスワード設定をしたファイルをメール添付で送信し、その後別メールにてファイルのパスワードを送付する方法のこと。）を使用することは禁止されています。メール添付による送付はリスクが高いため、原則としてＵＴＯＳ等のセキュリティが確保されたシステムを使用してください。

9　情報処理室等の安全管理【34 条】

基幹的なサーバ等の機器を設置する情報処理室等の管理を行う個人情報保護管理者にあっては、次の措置を講じてください。

① 情報処理室等に立ち入る権限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員等の立会い等の措置（媒体保管施設も同様）

② 情報処理室等の出入口を特定することによる入退の管理の容易化、所在表示の制限等の措置

③ 情報処理室等及び保管施設の入退の管理について、立入りに係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等

④ 外部からの不正な侵入に備え、情報処理室等に施錠装置、警報装置、監視設備の設置等

⑤ 災害等に備えるため、情報処理室等に、耐震、防火、防煙、防水等、サーバ等の機器の予備電源の確保、配線の損傷防止等

Q　所在表示の制限等の措置とはどのようなものですか？

A　個人情報のデータ処理を行う情報処理室等については、所在表示をしないこと又は室番号のみの表示にすることです。

Q　ＩＣカードやパスワード設定による入退室管理を行うことにしていますが、導入までに時間がかかるのですが導入までの期間の対応はどのようにするのが適切ですか？

A　さしあたっては、情報処理室等を施錠の上、鍵の貸出し簿によって管理してください。

１０　個人情報を取り扱う業務委託の留意点【35 条】

個人情報保護管理者は、個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、次の措置を講じてください。

① 委託契約書に次に掲げる事項を明記するとともに、委託先における責任者等の管理体制、個人情報の管理状況についての検査に関する事項等の必要な事項について書面で確認してください。

○「個人情報に関する秘密保持、目的外利用の禁止等の義務」「再委託の制限又は条件に関する事項」「個人情報の複製等の制限に関する事項」「個人情報の漏えい等の事案の発生時における対応に関する事項」「委託終了時における個人情報の消去及び媒体の返却に関する事項」「違反した場合における契約解除、損害賠償責任の措置その他必要な事項」

② 個人情報が記録されている媒体又は情報システム等の廃棄を外部に委託する場合には、①に定めるもののほか、当該記録媒体等に記録された情報が復元又は判読できない方法を用いることを定めて契約してください。

③ 業務を派遣労働者によって行わせる場合は、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記してください。

④ 派遣労働者に個人情報の取扱いに係る業務を行わせる場合は、当該派遣労働者に関係法令、個人情報保護管理規則等を遵守させるとともに、指導及び監督を行ってください。

また、漏えい等による被害発生のリスクを低減する観点から、必要に応じ匿名化措置を講ずるとともに、委託する業務に係る個人情報の秘匿性等その内容やその規模等に応じて、委託先における管理体制及び実施体制並びに個人情報の管理状況について、少なくとも年１回以上、原則として実地検査により確認してください。ただし、個人識別の容易性、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質・程度などを勘案の上、報告書又は関係書類の提出をもって実地検査に代えることができます。

Q　再委託の制限はどうして必要なのですか？

A　適正な業者に委託したにもかかわらず、その業者からさらに再委託するような場合は、責任の所在が不明確となり、漏えいの危険性が高まるからです。
なお、再委託先が委託先の子会社である場合も含みます。

１１　漏えい等を知った場合の通報体制【36 条、37 条】

１．基本方針

・紛失・漏えい等が発生した場合は、発見者は、その規模・内容・期間等にかかわらず、個人情報保護管理者に報告します。

・報告を受けた個人情報保護管理者は、コンプライアンス・ハラスメント対策室に第一報を上げます。

・コンプライアンス・ハラスメント対策室は、紛失・漏えい等の状況に応じ、個人情報総括保護管理者に第一報を上げることとします。ただし、電子媒体の紛失も含め情報セキュリティに関する事案については、コンプライアンス・ハラスメント対策室から筑波大学 ISIRT に移送の上、当該部署において個人情報総括保護管理者への報告等の対応を行います。

２．第一報報告の方法

報告については、以下のとおりとします。

・報告時期：発覚後直ちに（紛失・漏えい等した個人情報の内容等に応じて、以下のとおり区分します。）

(A)可及的速やかに（遅くとも２営業日以内）

●個人情報保護委員会への報告が必要なもの

・要配慮個人情報が含まれる事態

・財産的被害が生じるおそれがある事態

・不正の目的をもって行われた漏えい等が発生した事態

・１，０００人を超える漏えい等が発生した事態

●１０人を超える漏えい等が発生した事態

●漏えいしたことが明らかであるもの

●その他重大な影響が想定されるもの（紛失した事案の様態等から調査、懲戒処分等を検討する必要があるものと個人情報保護管理者が判断するもの等）

(B)５営業日以内

(A)以外

・報告者　：個人情報保護管理者

・報告先　：コンプライアンス・ハラスメント対策室

・報告内容：別紙「個人情報の紛失・漏えい等事案に係る第一報」のとおり

（ＵＴＯＳ受取フォルダにて提出後、電話連絡を行ってください。ただし、部局等において様式の提出が困難な場合は、電話等で報告する場合はコンプライアンス・ハラスメント対策室において電話で必要事項を聴取し、記入します。）

※注意　：記入後の「個人情報の紛失・漏えい等事案に係る第一報」は、記入後は【機密性３】として取り扱い、メール（パスワード付きメールを含む。）での提出は行わないようにしてください。

３．再発防止

個人情報保護管理者は、個人情報総括保護管理者の指示に従い、事案の発生した原因を分析し、再発防止のために必要な措置を講じてください。

４．公表等

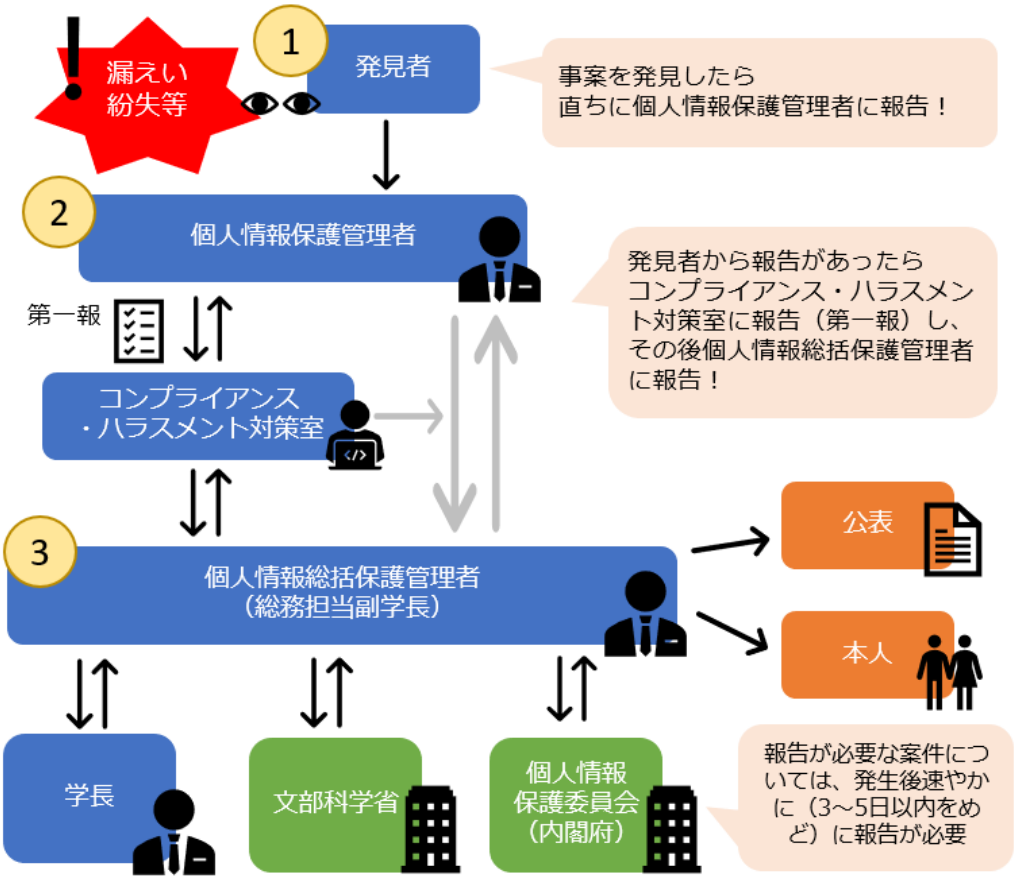
個人情報総括保護管理者は、発生した事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る個人情報の本人への対応等の措置を講ずるものとします。

また、公表を行う事案については、当該事案の内容等、経緯、被害状況等について、速やかに個人情報保護委員会に情報提供を行うものとします。

Q　ウィルス対策ソフトを更新し、ＯＳやアプリケーションのアップデートも行っていたにもかかわらず、ワームウィルスに感染し、個人情報データが勝手に学外に発信されてしまったと思われますが、どのようにしたらよいのですか？

A　直ちに個人情報保護管理者等に報告してください。個人情報保護管理者等は、上記のとおり必要な措置を速やかに講ずるとともに、上記に従い、コンプライアンス・ハラスメント対策室に対し、第一報を報告してください。

通報体制図



１２　監査及び点検【38 条、39 条】

監査責任者による定期又は随時の監査が実施されますので、個人情報保護管理者は、自ら管理責任を有する個人情報の記録媒体、処理経路、保管方法等について、定期に又は随時に点検を行ってください。

１３　個人情報ファイル簿の報告【42 条、43 条】

① 職員等は、個人情報ファイルに該当するものを保有することとなった場合には、作成例及び作成要領を参考に個人情報ファイル簿を作成し、コンプライアンス・ハラスメント対策室法規担当（大学教員の場合はエリア支援室、社会人大学院等支援室又は海外教育拠点支援室、附属学校教員の場合は東京キャンパス事務部）宛てに提出してください。
（様式、作成例及び作成要領：https://ksp.sec.tsukuba.ac.jp/wp/?page_id=4687）

② 報告のあった個人情報ファイル簿は、窓口において一般の閲覧に供するとともに、インターネットにより公開されます。

Q なぜ個人情報ファイル簿を作成しウェブサイトで公開するのですか？

A 法人が保有する個人情報ファイル簿を公開することにより、本人が自己に関する個人情報の利用の実態をより的確に認識することができるようになるばかりでなく、法人における透明性の確保や利用目的ごとの保有個人情報の適正な管理に資するためです。なお、公表は、個人情報保護法第７５条第１項において義務として定められています。

Q 保有個人情報を紙媒体でファイルとして管理はしてあるが、ランダムに綴じてあるようなものも、個人情報ファイルに該当するのですか？

A 紙媒体のものは、番号順、五十音順、年月日順などで整理・分類し、特定の保有個人情報が容易に検索できるように体系的に構成されていれば個人情報ファイルに該当しますが、ランダムに綴じてあって容易に検索できない場合は該当しません。

Q 年度ごとに作成している個人情報ファイルに含まれる本人の数が単年度では 1,000 人を超えませんが、保存年限分の５年分のファイルを合わせると 1,000 人以上になります。この場合、個人情報ファイル簿を作成する必要がありますか？

A その保有個人情報ファイルの使用目的が年度を通じて連続しているものである場合は作成する要件に該当しますが、年度ごとに使用するものであれば、該当しないと考えられます。

Q 個人情報ファイルとして報告しなければならないものの例外として、１年以内に消去するものという条件がありますが、その起算点は年度毎ですか、それとも個人情報の取得時点ですか？

Ａ　個人情報ファイルに記録されている個人情報を取得した時点からです。

Ｑ　個人情報ファイル簿として公開していない保有個人情報に対しても、法に基づく保有個人情報の開示請求の可能性はありますか？

Ａ　開示請求は、個人情報ファイル簿への記載の有無にかかわらず、保有個人情報全てに対し行われる可能性があります。

Ｑ　市販の名簿や論文などで一般に入手可能又は公開されているものの中には、氏名、所属等の個人情報が含まれているものがあります。これらの個人情報を抽出して集めたものは、個人情報ファイルに該当しますか。また、それを第三者に見せる時には、本人の同意が必要になりますか？

Ａ　一般に入手可能又は公開されている個人情報が記載されている書籍類は、不特定多数の者に販売することを目的として発行されるものに該当するため法人文書には当たりません。しかし、それらの書籍類から発明者別、作者別などの個人情報を集めて整理したものは、個人情報ファイルに該当します。ただし、学術研究目的であれば第三者に提供することができ、個人情報ファイル簿の報告も必要ありません。

１４　個人番号（マイナンバー）及び特定個人情報の取扱い

①　平成 25 年に制定された行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」といいます。）に基づき、法人では、平成 27 年 10 月に「国立大学法人筑波大学個人情報及び特定個人情報の安全管理に関する基本方針」及び「国立大学法人筑波大学における個人番号及び特定個人情報の取扱いに関する規則」を制定し、個人番号及び特定個人情報の取扱いが安全かつ適切に行われる体制を整備しました。

②　同規則では、特定個人情報を利用する事務の範囲を列記し、特定個人情報に係るシステム等の使用を総務部人事課及び財務部財務管理課に制限するとともに、利用目的の範囲内でしか利用は不可とする旨等が明記されています。なお、同規則に定めのある事項以外は、番号法その他ガイドライン等の取扱いを遵守することとしています。

１５　苦情相談及び保有個人情報の開示等の請求【41 条、44 条】

① 個人情報の取扱いに係る苦情相談の受付並びに保有個人情報の開示、訂正及び利用停止の受付等を行う窓口が以下のとおり設置されておりますので、苦情相談や開示等の請求があった場合は、まずは窓口にご相談ください。

・コンプライアンス・ハラスメント対策室情報公開窓口（電話 029-853-2036）
・病院総務部総務課情報公開窓口（電話 029-853-3519）
・東京キャンパス事務部学校支援課情報公開窓口（電話 03-3942-6805）

② 上記の窓口において苦情を受け付けたときは、関係する個人情報保護管理者は、当該苦情に関する個人情報の取扱いの状況等を迅速に調査して、その適切かつ迅速な処理に努めるとともに、必要に応じ、個人情報総括保護管理者と協議してください。

③ 本人から保有個人情報の開示、訂正又は利用停止の請求があった場合は、窓口等からの要請に対して、関係する個人情報保護管理者、個人情報保護担当者及び当該保有個人情報を取り扱う職員等は、その適切かつ迅速な処理に努めなければなりません。

１６　個人情報保護についての問合せ先

① 個人情報保護管理規則及び個人情報保護管理の手引きについて
コンプライアンス・ハラスメント対策室（法規）　029-853-2033

② 保有個人情報の開示等の請求及び苦情相談について
コンプライアンス・ハラスメント対策室（情報公開）　029-853-2036

③ 情報システムについて
学術情報部情報基盤課　　029-853-2071

個人情報保護法等に関するＱ＆Ａ

Ｑ　法には、罰則が規定されているということを聞きましたが、どのようなものですか？

Ａ　職員等又は職員等であった者が、正当な理由がないのに、個人の秘密に属する事項が記録された個人情報ファイル（その全部又は一部を複製し、又は加工したものを含む。）を提供したときは、２年以下の懲役又は１００万円以下の罰金が科せられます（法第１７６条）。

Ｑ　具体的にどのような場合に罰則が科せられるのですか？

Ａ　職員録を名簿業者に売り渡す場合などです。

Ｑ　個人情報関係で「ＧＤＰＲに対応しなければならない」といったことを聞きました。ＧＤＰＲとは何ですか？

Ａ　ＧＤＰＲ適用国（欧州経済領域（European Economic Area）の構成国（ＥＵ加盟国、アイスランド共和国、リヒテンシュタイン公国、ノルウェー王国）及び英国（グレートブリテン及び北アイルランド連合王国）をいいます。）に関係する個人データを取り扱う際に遵守しなければならない定めです。
法人におけるＧＤＰＲ（General Data Protection Regulation：一般データ保護規則）に対応するための定め等を、教職員専用サイト上に「ＧＤＰＲに基づくプライバシーポリシー」として掲載しておりますのでご確認ください。
URL：https://ksp.sec.tsukuba.ac.jp/wp/?page_id=172940

個人情報保護管理の手引き

【初版】
平成 17 年 4 月 1 日
編集　国立大学法人筑波大学総務・企画部
監修　図書館情報メディア研究科助教授　新保史生

【改訂版】
平成 28 年 10 月 1 日
平成 31 年 4 月 1 日
令和 2 年 4 月 1 日
令和 3 年 6 月 1 日
令和 4 年 6 月 1 日
令和 5 年 4 月 1 日
令和 6 年 6 月 1 日
令和 7 年 5 月 1 日
編集　国立大学法人筑波大学コンプライアンス・ハラスメント対策室
監修（令和 7 年 5 月～）　生命環境系講師　伊藤希