個人情報漏洩などの事故をなくすために…

INDEX

平成21年12月　第2版

社団法人
日本グラフィックサービス工業会
the Japan Graphic services industry association JaGra

個人情報とは…

「個人情報」とは、生存する「個人に関する情報」であって、特定の個人を識別することができるものをいいます。「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問いません。

なお、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となります。

また、法人その他の団体は「個人」に該当しないため、法人等の団体そのものに関する情報は含まれません。（ただし、役員、従業員等に関する情報は個人情報です。）

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
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ります）
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）

▸▸経済産業省のガイドライン

特に印刷業界としては、年賀状・暑中見舞いハガキ、名刺、名簿、アルバム、DM用宛名、印刷物やビデオ、Web等のデータ中に含まれる顔写真等、メールアドレスや携帯電話についても個人情報の該当性に対する注意が必要と考えられます。

法令・指針、その他の規範

平成17年４月に全面施行された個人情報の保護に関する法律（以下「個人情報保護法」という）、個人情報保護法施行令及び個人情報の保護に関する基本方針（閣議決定）は、個人情報保護に関する一般的なルールであり、法令遵守の観点から必ず確認しなくてはなりません。因みに、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の合計が、過去６ヶ月以内のいずれかの日においても、5,000を超えていた事業者は、原則として、「個人情報取扱事業者」として法の対象となります。加えて都道府県・市区町村の自治体個人情報保護条例や経済産業省及び厚生労働省のガイドライン、㈱日本グラフィックサービス工業会、㈱東京グラフィックサービス工業会及び㈱日本印刷産業連合会の各業界ガイドラインについても十分承知しておく必要があります。

社団法人　日本グラフィックサービス工業会
http://www.jagra.or.jp/
社団法人　東京グラフィックサービス工業会
http://www.tokyographics.or.jp/
社団法人　日本印刷産業連合会
http://www.jfpi.or.jp/
個人情報保護法（消費者庁）
http://www5.cao.go.jp/seikatsu/
経済産業省ガイドライン
http://www.meti.go.jp/feedback/downloadfiles/i40615hj.pdf
厚生労働省指針
http://www.mhlw.go.jp/topics/2004/07/tp0701-1.html
（財）日本情報処理開発協会
http://www.jipdec.jp/

利用目的の公表

個人情報を取り扱うに当たっては、HP等でその利用の目的をできる限り特定しなければなりません。なお、利用目的の特定の際に、利用する個人情報の項目及び入手先の事業者名等を特定することまで求められるわけではありません。また多くの場合、業種の明示だけでは利用目的をできる限り具体的に特定したことにはなりません。また、単に「事業活動」を「お客様のサービスの向上」等のように抽象的、一般的な内容を利用目的とすることは、具体的に特定したことにはなりません。

なお、あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的において、その旨を特定しなければなりません。

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「ご記入いただいた氏名、住所、電話番号は、名簿として販売することがあります」。
③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ります。

▸▸経済産業省のガイドライン

個人情報の特定

特定については、本人から直接書面で取得した情報（例. 自社の役員・従業員情報、顧客本人から直接受注した名刺・年賀状・各種名簿・発送リスト・メールアドレス・携帯電話番号等、印刷、情報処理に係るもの）及び直接書面以外で印刷・情報処理等で取得した受託物、顧客からの支給品、個人データ、顔写真、フイルム・刷版、DMデータ、印刷見本等を示します。

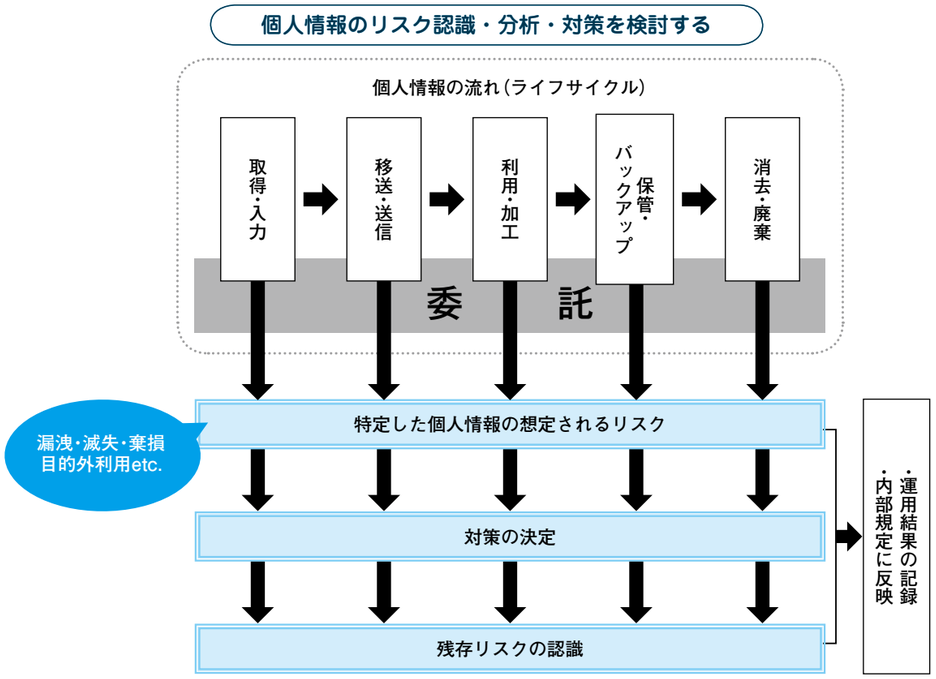
また、個人情報の一覧（台帳）を作ることを勧めます。そこには、カテゴリー毎に利用目的、入手経路、保管場所、保管期間、件数、廃棄方法を記載しておくと一覧性があって管理しやすいでしょう。同時に業務フローを作っておくことも必要です。加えて、開示対象個人情報の可否についても明記しておくと良いでしょう。

個人情報管理台帳（例）

項目	個人情報名	項目			入手経路	件数	利用目的	保管場所	保管形態	保管期間	アクセス権を有するもの	廃棄方法	開示情報の可否
		データ	紙媒体	その他									

リスク分析

リスク分析は、取得、入力・編集、校正、移送・通信、利用（製版・印刷・製本、DM他）、保管（媒体、サーバー、完成製品見本、自社倉庫内在庫）・バックアップ、納品・運搬、消去・廃棄の各局面のライフサイクルに沿って行ないます。そのリスク分析に従い、評価し、対策を講じなければなりません。重要度の高いものから対策を立てますが、経済的理由等で対応できないものについては、「残存リスク」として把握しておくと良いでしょう。



リスク分析とその対策（例）

（個人情報名：　　）

ライフサイクル	取得・入力	移送・送信	利用・加工	保管・バックアップ	消去・廃棄
部門					
想定されるリスク					
選択したリスク対策					
関連規定					
運用結果の記録					
残存リスク					
その他					

※財団法人　日本情報処理開発協会テキストより転載

個人情報の取得と本人の同意

個人情報の取得は適正に行って下さい。

個人情報保護法では、「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、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」とし、「個人情報取扱事業者は、（中略）、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」と規定しています。

「本人の同意」とは、本人の個人情報が、個人情報取扱事業者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をいいます（当該本人であることを確認できていることが前提です）。

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個人情報取扱事業者が認識することをいい、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければなりません。

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

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

▸▸経済産業省のガイドライン

なお、JIS Q15001では機微情報の取得、利用、提供も禁止しています。

＊機微情報とは、①思想、信条、宗教に関する事項②人種、民族、門地、本籍地（所在都道府県情報は除く）、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　③勤労者の団結権、団体交渉その他の団体行動行為に関する事項　④集団示威行為への参加、請願権の行使その他政治的権利の行使に関する事項　⑤保健医療、性生活事項

機微情報を取得する場合は、法令に特別な規定がある場合や司法手続上必要不可欠である場合を除き、本人の明示的同意が必要となります。

直接書面等による取得について

個人情報取扱事業者は、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）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りません。

例えば、個人情報取扱事業者は、書面等による記載や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がこれに該当します。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、この限りではありません。

なお、口頭による個人情報の取得にまで、当該義務を課すものではありませんが、その場合は、あらかじめ利用目的を公表するか、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。

直接書面以外による取得について

印刷業のみならず受注産業にとって注意を払う所です。直接書面以外で取得する顧客から処理を委託されるデータ、印刷物、DM発送等の発注に際して顧客（あるいは元請）から委託を受けるデータを含めた個人情報が、本人の同意を得たものか得ていないものか、委託される際に確認すべき事項であります。

データ内容の正確性の確保

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りません。

印刷業の場合、印刷・データ処理に関してそれを業としているだけに、特に内容の正確性（誤字・誤植等）を保証する必要があります。顧客が「校正」を行なっていても、入力・プリプレス工程での内部チェックは必須の課題です。保存期間、データのバックアップの手順も定めておきます。

緊 急事態について

印刷業では、個人情報が漏洩、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なければなりません。

また、個人情報の漏洩、滅失又はき損が発生した場合に備えましょう。

①当該漏洩、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きます。

②二次被害の防止、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します。

③事実関係、発生原因及び対応策を関係機関（経済産業省、社団法人日本グラフィックサービス工業会、社団法人東京グラフィックサービス工業会等）に直ちに報告します。

DMの誤配送、FAX、メールの誤送信等これらはあってはならないことですが、ウッカリミスであっても事故に変わりはありません。漏洩、滅失、き損の緊急事態への対応は重要な対策です。事故発生にあっては何よりも本人への通知、二次被害の防止が優先します。直接取得でない場合は委託元との連絡、認定個人情報保護団体との連携、社内・外連絡網の作成、そして緊急事態への事前の対処方法の徹底が必要です。

安 全管理措置

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りません。講ずるべき措置は、その内容によって、組織的、人的、物理的及び技術的な安全管理措置に分類することができます。

◆ 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います。

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

▸▸経済産業省のガイドライン

各項目を実践するために講じることが望まれる手法の例示

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」を実践するために講じることが望まれる手法の例示

・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
・個人データを取り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かか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（漏えい、滅失又はき損）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」を実践するために講じることが望まれる手法の例示

・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
・個人データを取り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、次項の【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の例】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委託先の選定基準、委託契約書のひな型、委託先における委託した個人データの取扱状況を確認するためのチェックリスト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れる監査証跡としては、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「個人データの取扱い状況を一覧できる手段の整備」を実践するために講じることが望まれる手法の例示

・個人データについて、取得する項目、明示・公表等を行った利用目的、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」を実践するために講じることが望まれる手法の例示

・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」を実践するために講じることが望まれる手法の例示

・以下の(ア)から(カ)までの手順の整備
ただし、書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合には、以下の対処をする必要はないものと考えられる。

(ア) 事実調査、原因の究明
(イ) 影響範囲の特定
(ウ) 再発防止策の検討・実施
(エ) 影響を受ける可能性のある本人への連絡
(オ) 主務大臣等への報告
(カ) 事実関係、再発防止策等の公表

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例

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の例を列記します。

(1) 取得・入力

①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。）

②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します。）
③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
④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

⑵ 移送・送信
①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
②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等の秘匿化（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、簡易書留郵便その他個人情報が含まれる荷物を輸送する特定のサービスの利用）
・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機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
③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
④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

⑶ 利用・加工
①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
②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。）
③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
④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

⑷ 保管・バックアップ
①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
②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等の秘匿化
・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
③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
④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

⑸ 消去・廃棄
①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
②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。）
③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
④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

◆ 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います。

人的安全管理措置として講じなければならない事項

①雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む）における委託者と受託者間での非開示契約の締結。
②従業者に対する内部規程等の周知・教育・訓練の実施

▸▸ 経済産業省のガイドライン

各項目を実践するために講じることが望まれる手法の例示

①「雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結」を実践するために講じることが望まれる手法の例示

・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。
＊個人情報に関する非開示の義務を、就業規則等の社内規程に規定することも考えられる。なお、社内規程に個人情報に関する非開示の義務を規定する場合には、特に、労働基準法第89条及び第90条などの労働関連法規を遵守する必要がある。
＊個人情報に関する非開示契約の締結の際に、営業秘密を対象とする秘密保持契約をあわせて締結する場合であっても、個人情報保護と営業秘密の保護はその目的・範囲等が異なるため、従業者の「納得感」の向上の観点からは、個人情報保護に関する契約と営業秘密に関する秘密保持契約は峻別する（別書面であるか否かは問わない）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

＊個人データを取り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、個人データを取り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、個人データを取り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「従業者に対する内部規程等の周知・教育・訓練」を実践するために講じることが望まれる手法の例示

・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及び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

◆ 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います。

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

▸▸ 経済産業省のガイドライン

各項目を実践するために講じることが望まれる手法の例示

①「入退館（室）管理」を実践するために講じることが望まれる手法の例示

・個人データを取り扱う業務の、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
・個人データを取り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「盗難等の防止」を実践するために講じることが望まれる手法の例示

・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及び車内等への放置の禁止
・離席時のパスワード付きスクリーンセーバ等の起動によるのぞき見等の防止
・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
・個人データを取り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・装置等の物理的な保護」を実践するために講じることが望まれる手法の例示

・個人データを取り扱う機器・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

◆ 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り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います。

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個人データを取り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個人データを取り扱う情報システムの動作確認時の対策
⑧個人データを取り扱う情報システムの監視

▸▸ 経済産業省のガイドライン

各項目を実践するために講じることが望まれる手法の例示

①「個人データへのアクセスにおける識別と認証」を実践するために講じることが望まれる手法の例示

・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正当なアクセス権限を有する者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」を実践するために講じることが望まれる手法の例示

・個人データへのアクセス権限を付与すべき者の最小化
・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）の実施。
・アクセス権限を有する者に付与する権限の最小化
・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。

・個人データを取り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」を実践するために講じることが望まれる手法の例示
・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）。
・個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施

④「個人データへのアクセスの記録」を実践するために講じることが望まれる手法の例示
・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

＊個人データを取り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「個人データを取り扱う情報システムについて不正ソフトウェア対策」を実践するために講じることが望まれる手法の例示
・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」を実践するために講じることが望まれる手法の例示
・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等の秘匿化）
・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等の秘匿化

⑦「個人データを取り扱う情報システムの動作確認時の対策」を実践するために講じることが望まれる手法の例示
・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「個人データを取り扱う情報システムの監視」を実践するために講じることが望まれる手法の例示
・個人データを取り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

＊個人データを取り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必要があります。

従 業者の監督

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、当該個人情報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りません。

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します。従業者と会社間で個人情報の取扱いに関する各従業者の役割、責任を明確化し、従業者が個人情報保護の役割、責任を認識することが大切です。

なお「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、派遣社員等も含まれます。

委 託先の監督

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りません。その際、本人の個人情報が漏えい、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情報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します。

「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ます。

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します。

個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項

①委託者及び受託者の責任の明確化
②個人データの安全管理に関する事項
・個人データの漏えい防止、盗用禁止に関する事項
・委託契約範囲外の加工、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データの返還・消去・廃棄に関する事項
③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
④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
⑤契約内容が遵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ます）
⑥契約内容が遵守されなかった場合の措置
⑦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

▸▸ 経済産業省のガイドライン

第 三者への提供／共同利用について

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、個人データを第三者に提供してはなりません。

個人データを特定の者との間で共同して利用する場合、以下の①から④までの情報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おくとともに、共同して利用することを明らかにしている場合は、第三者に該当しません。また、既に特定の事業者が取得している個人データを他の事業者と共同して利用する場合は、既に取得している事業者が特定した利用目的の範囲で共同して利用しなければなりません。

共同利用する場合、あらかじめ一定の事項につき取り決めておくことが望ましい。

共同利用の対象となる個人データの提供については、必ずしもすべての共同利用者が双方向で行う必要はなく、一部の共同利用者に対し、一方向で行うこともできます。

個人データの管理について責任を有する者は、利用目的の達成に必要な範囲内において、共同利用者間で利用している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りません。

①共同して利用される個人データの項目

②共同利用者の範囲（本人からみてその範囲が明確であることを要するが、範囲が明確である限りは、必ずしも個別列挙が必要ない場合もある。）

③利用する者の取得時の利用目的（共同して利用する個人データのすべての利用目的）

④開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等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

保 有個人データに関する事項の公表等

個人情報取扱事業者は、保有個人データについて、以下の①から④までの情報を本人の知り得る状態に置かなければなりません。

①個人情報取扱事業者の氏名又は名称

②すべての保有個人データの利用目的

③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）並びに開示等の求めの手続き

④保有個人データの取扱に関する苦情及び問い合わせの申出先（個人情報取扱事業者が認定個人情報保護団体に所属している場合は、その団体の名称及び申出先も含む。）

保有個人データの開示

個人情報取扱事業者は、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りません。（「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。

また、消費者等、本人の権利利益保護の観点から、事業活動の特性、規模及び実態を考慮して、個人情報の取得元又は取得方法（取得源の種類等）を、可能な限り具体的に明記し、本人からの求めに一層対応していくことが望ましい。

なお、他の法令の規定により、別途開示の手続が定められている場合には、当該別途の開示の手続が優先されることとなります。

雇用管理情報の開示の求めに応じる手続については、個人情報取扱事業者は、あらかじめ、労働組合等と必要に応じ協議した上で、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りません。

苦 情の処理

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りません。

また、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りません。

ク レジットカード情報を含む個人情報の取扱いについて

クレジットカード情報（カード番号、有効期限等）を含む個人情報（以下「クレジットカード情報等」という。）は、情報が漏えいした場合、クレジットカード情報等の不正使用によるなりすまし購入などの二次被害が発生する可能性が高いため、クレジットカード会社のほか、クレジットカード決済を利用した販売等を行う事業者及びクレジットカード決済を利用した販売等に係る業務を行う事業者並びにこれら事業者からクレジットカード情報等の取扱いを伴う業務の委託を受けている事業者（以下「クレジット販売関係事業者等」という。）は、クレジットカード情報等の安全管理措置として、特に以下の措置を講じることが望ましい。

①クレジットカード情報等について特に講じることが望ましい安全管理措置の実施

②クレジットカード情報等の保護に関する規定を含む契約の締結

③クレジットカード情報等を直接取得する場合のクレジットカード情報等の提供先名等の通知又は公表

各項目を実践するために講じることが望まれる手法の例示

①クレジットカード情報等について特に講じることが望ましい安全管理措置の実施

・クレジットカード情報等について、利用目的の達成に必要最小限の範囲の保存期間を設定し、保存場所を限定し、保存期間経過後適切かつ速やかに破棄

・クレジット売上伝票に記載されるクレジットカード番号を一部非表示化

・クレジットカード読取端末からのクレジットカード情報等の漏えい防止措置を実施（例えば、クレジットカード読取端末にはスキミング防止のためのセキュリティ機能（漏えい防止措置等）を搭載する等）

・クレジットカード情報等を移送・送信する際に最良の技術的方法を採用

・他のクレジットカード販売関係事業者等に対してクレジットカード情報等が含まれる個人情報データベース等へのアクセスを許容している場合においてアクセス監視等のモニタリングを実施

②クレジットカード情報等の保護に関する規定を含む契約の締結

・クレジットカード情報等を取扱う業務に係る契約の締結の際に、クレジットカード情報等の保護に関する規定を設定（例えば、クレジットカード情報等の保護の観点から情報提供を求める旨の規定や、クレジットカード情報等の取扱いが不適切なことが明らかな場合において当該情報を取扱う業務の是正を求めることや当該業務に係る契約を解除する旨の規定を設定）

③クレジットカード情報等を直接取得する場合のクレジットカード情報等の提供先名等の通知又は公表

・インターネット取引においてクレジットカード情報等を本人から直接取得するなど、クレジットカード情報等を本人から直接取得する場合、法第18条各項の規定に基づき、本人に利用目的を明示又は通知若しくは公表するほか、クレジットカード情報等の取得者名、提供先名、保存期間等を通知又は公表

ま とめ

個人情報保護法が全面施行されて５年間が経過いたしました。この間、国民・消費者の個人情報保護の意識も大きな高まりを見せております。ところが、個人情報に関わる金融機関・クレジット会社・通販会社・官公庁・学校等などにおける流失事故は相次ぎ、直接･間接の被害は決して少ないものではありません。

３年前に大手印刷会社による個人情報の大量流失事故が起こり、重大な事件に至ったことを、私たち印刷事業者は大きな衝撃をもって受けとめました。また私共JaGra会員内での事故もこれまで10件程あがっております。

JaGraでは、個人情報保護を業界活動の重要な柱の一つと位置付け取り組んでまいりました。その一環として平成19年にプライバシーマーク付与指定機関（東京グラフィックスは平成17年）となって、すでに200余社の会員への付与を行ってまいりました。

本マニュアルは、平成21年10月の経済産業省ガイドライン改訂に基づき、第2版として作成いたしました。今回は特に、安全管理面で注意すべき事項を詳細に記載いたしました。CSR（企業の社会的責任）が強く企業に求められる中で、個人情報のみならず顧客の重要な情報を取り扱う私たちグラフィックサービス事業者として、引き続き情報セキュリティに対し社内外に万全の態勢を敷き、顧客、消費者への安心と満足を提供し続けたいと念じております。

私たちが守るべきこと…

1. 個人情報保護法，経済産業省「個人情報保護ガイドライン」をしっかりと遵守します。
2. 全従業者に個人情報を扱う上での教育を必ず実施します。
3. 委託先（協力企業）へ個人情報の処理・加工・発送等を委託する場合は、必ず契約を交わし、充分な監督を行ないます。
4. 直接本人から受注する場合は、同意をとります。
5. 顧客から個人情報を含んだ受注がある場合、顧客との契約のみならず受注する際に本人の同意を得ているか、再委託を行う同意を得ているかを確認します。
6. 利用目的を逸脱する個人情報はお預かりしません。
7. 事業の性質及び個人データの取扱い等に起因するリスクに応じ、必要かつ適切な組織的・人的・物理的・技術的安全管理措置を講じます。
8. 情報漏洩等、緊急事態や苦情が発生した場合は、本人への被害を食い止める手順を定め、また関係官公庁及び社団法人日本グラフィックサービス工業会又は、認定個人情報保護団体である社団法人東京グラフィックサービス工業会へ連絡します。

「個人情報漏洩などの事故をなくすために…」

◇発行人：社団法人　日本グラフィックサービス工業会
〒 103-0001
東京都中央区日本橋小伝馬町 7-16　ニッケイビル 7F
TEL：03-3667-2271　FAX：03-3661-9006
URL：http://www.jagra.or.jp/
◇発行日：平成 21 年 12 月 21 日
◇印　刷：㈱東京文久堂