印刷・グラフィックサービスのための

個人情報保護の要点ガイド

公益社団法人
東京グラフィックサービス工業会
the Tokyo Graphic services industry association

個人情報保護の必要性

■個人情報とは

印刷業の場合、扱う個人情報の種類としては、名簿、名刺・年賀状、Web 関連をはじめ多くの受注印刷物、各種データ、顧客リスト、DM 発送代行、さらに自社の社員情報があります。「個人情報」とは、特定の個人が識別できるものが個人情報となります。氏名、年齢、男女、所属組織・部署・肩書き、住所、電話、メールアドレス、写真、ビデオ、録音も対象となります。個人情報保護法では過去 6 ケ月間に 5,001 人以上保有する事業者（個人情報取扱事業者）が法の対象となります。また東京都条例では、5,000 人以下の保有事業者も対象としていることから、都内の印刷業者の場合は、全ての会社が対象者であるということになります。

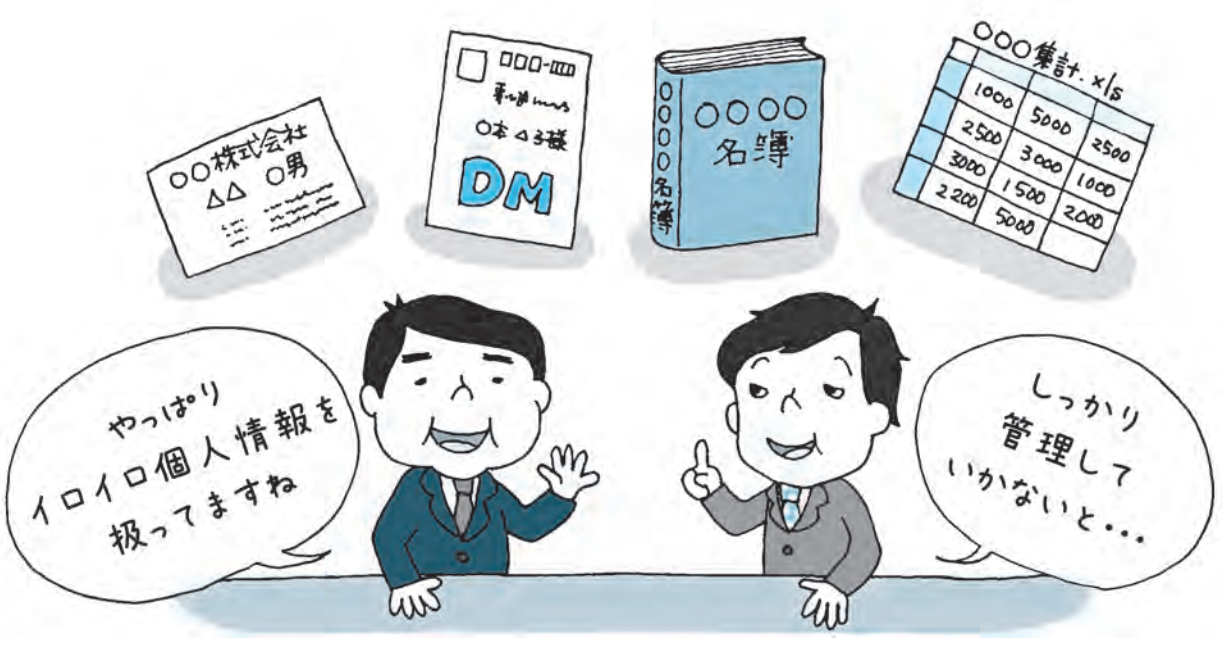
法律の施行を受けて、事業者がしなければならない点を挙げてみますと――

① 利用目的の特定と制限
② 適正な取得
③ 利用目的の通知
④ データ内容の正確性の確保
⑤ 安全管理措置
　(1) 組織的安全管理措置
　(2) 人的安全管理措置
　(3) 物理的安全管理措置
　(4) 技術的安全管理措置
⑥ 従業者の監督
⑦ 委託先の監督
⑧ 第三者提供の制限
⑨ 保有データの公表・開示・訂正・利用停止
⑩ 苦情の処理

以上が、法律で課せられた事業者としての義務となります。

本法の違反には罰則が科せられることになります。但し、違反行為に対する罰則ではなく、主務大臣が是正の勧告を行い、それに従わない時に罰せられるとしています。

日常業務における顧客からの依頼による名簿等のあらゆる印刷物、各種データの集計、DM 発送をはじめそれらを各社で取扱ルールを定め、安全を確保しなくてはなりません。印刷業では直接個人顧客から受注する場合は店舗、通販業を営んでいる業者となります。殆どの印刷物は本人からの直接でない取得です。しかし情報の処理・加工を業として営む限り、お預りする様々な個人情報・機密情報の保護を徹底することは当然の責任となっております。直接取得はもとより通常の印刷受注に個人情報としての“認識”を持ち、細心の注意を払って扱うべきでしょう。



個人情報とは

プライバシーマーク使用許諾のメリット

■個人情報の取扱い

個人情報の取扱いについては個人情報保護法に沿ってすすめれば問題ないはずですが、東京都をはじめ地方自治体の条例そして経済産業省のガイドラインさらに東京グラフィックス、JaGra、日印産連でも個人情報保護方針・ガイドラインを制定していますので、各社の指針に参考にすべきです。さらに、プライバシーマークの使用許諾を受けることで社内外へのアピールとなります。プライバシーマークは、JIS Q15001 の要求事項を遵守していることを外部の審査機関が審査して、JIS の要求事項を満たしていることを認証しています。現在 1 万 3,000 余社、印刷関連では 1,200 余社がプライバシーマークを付与されております。プライバシーマークのメリットは、何よりも消費者 = 顧客の信用・信頼が得られ、社内業務のルールの徹底と従業員の意識の向上、責任体制の明確化、お客様との個人情報の取扱いの明確化、さらに PDCA（6 頁参照）を回すことにより業務の効率化が図られることにあります。

プライバシーマークとは

認定個人情報保護団体について

個人情報保護法で定められている「認定個人情報保護団体」は民間団体で各省大臣が認定し、会員企業と消費者とのトラブルに対して事業者と一緒に、解決を図ることを趣旨としています。

対象事業者の利点としては、認定保護団体が第三者機関として関与することで迅速・円滑な苦情の解決が期待できます。認定保護団体から適切な情報が提供されることによって、適切な個人情報保護の取組みが維持できます。

消費者の「本人」の利点としては、認定保護団体が第三者機関として関与することで迅速・円滑な苦情の解決が期待でき、安心して個人情報の開示ができる環境整備が期待できる、というものです。なお、（公社）東京グラフィックサービス工業会は、印刷業界唯一の認定団体として、経済産業大臣認可を得ております。なお、JaGra 会員で東京以外の方でプライバシーマークを付与されている企業は、（一財）日本情報経済社会推進協会（JIPDEC）を認定個人情報保護団体として指定してください。

個人情報の特定とリスク分析

■保護する内容と特定

個人情報を保護するためにどのように行えばよいのか？

法律対応とも共通しますが、プライバシーマークの認定を受けるためには、自社で扱う『個人情報』を特定すること（洗い出し）から始めます。印刷業者としては、直接個人から取得するものとしては、

① 個人名刺・年賀状等
② 自費出版、写真集類
③ 自社の社員（家族）、アルバイトや採用希望者の履歴書、健康診断等

があります。

しかし、殆どが直接でない取得による顧客が取得した個人情報で①顧客リスト・データ、DM リスト、②各種の印刷関連物です。

企業はそれらのデータで、個人情報の含まれたデータ（氏名、住所、顔写真、メールアドレス等）を洗い出すルールを決めます。それらを、種類別、顧客別等の区分で「個人情報管理台帳」に記載します。

なお、機微な情報の取得は原則禁止しており取得する場合は本人の同意を必要とします。機微情報とは

(1) 思想、信条及び宗教に関する事項
(2) 人種、民族、門地、本籍地（所在都道府県に関する情報を除く。）
(3) 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
(4) 保健医療及び性生活

に関する事項です。

■局面毎のリスク

次に、保有する個人情報を局面毎にリスクを分析します。局面とは、①取得、②移送、③データ送信、④利用、⑤加工、⑥保管、⑦委託、⑧廃棄、⑨返却、⑩発送…があります。

その局面に照らしてリスクを想定し、情報が漏洩、滅失、毀損する可能性をリスクととらえ、リスクを分析し対応策を決め、規程化し、それでも対応できないリスクは「残存リスク」として管理します。（表２を参照）

表１　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									
	名刺（企業）	○	○		直接でない	1,000件	印刷	サーバー、キャビネ	データ、見本	永久	営業、プリプレス	なし	否
	名刺（個人）	○	○		直接本人	300件	印刷	サーバー、キャビネ	データ、見本	永久	営業、プリプレス	なし	可
	年賀状	○			直接本人	50件	印刷	サーバー	データ	２年	営業、プリプレス	ヤレは郵便局	可
	社員名簿	○	○		直接でない	1,000件	印刷	サーバー、キャビネ	データ、見本	３年	営業、プリプレス	シュレッダー	否
	社員証	○			直接でない	300件	製品	サーバー	データ	３年	営業、プリプレス	外注先にて	否
	DM 宛名	○			直接でない	500件	発送データ	なし	なし	なし	営業、プリプレス	納品時消去	否

表２　リスクの洗い出し

局面	ケース	リスク	対　　策（規定）	残存リスク
取得	手渡し	原稿紛失	授受記録（○○規程第○条） 営業カバンにしまう（○○規程第○条）	ひったくり
	宅配便	受領後の放置	管理ゾーンでの保管（○○規程第○条）	伝票類の紛失
	FAX	放置	受信後、担当者に渡す（○○規程第○条）	
	ウェブでの取得（ある場合）	漏えい	暗号化（SSL）する（○○規程第○条）	
移送	社用車で 顧客→自社	車上荒らし	不要な立ち寄り禁止（○○規程第○条） やむを得ない立ち寄りの際は、カバンに入れて携行する。車内放置禁止（○○規程第○条）	鍵のかけ忘れ
	委託先への移送	原稿（媒体）紛失	授受記録（○○規程第○条）	盗難
	メール	漏えい	ファイルの暗号化、または PW 設定を依頼する（○○規程第○条）	データウィルスチェック PW の不備
	委託先からの移送	原稿、成果物紛失	授受記録（○○規程第○条） 原稿またはデータ、中間生成物の処理の報告を受ける（○○規程第○条）	PW 間違い
	校正のやりとり	原稿紛失 誤送信	不要な立ち寄り禁止（○○規程第○条） やむを得ない立ち寄りの際は、カバンに入れて携行する。車内放置禁止（○○規程第○条） 添付データのチェック（○○規程第○条） 授受記録（○○規程第○条）	校正紙の保管 盗みの恐れ 添付データのチェック 誤送信
	社用車で納品	車上荒らし 成果物の紛失	不要な立ち寄りの禁止（○○規程第○条） やむを得ない立ち寄りの際は、カバンに入れて携行する。車内放置禁止（○○規程第○条） 授受記録（○○規程第○条）	トラックの荷くずれ
データの送信	FAX の誤送信 メールの添付データの取扱い 社内の無線 LAN の使用 ネットを通じた校正の暗号化		個別番号打ち込みの禁止（○○規程第○条） 宛先確認（○○規程第○条） 添付データの暗号化対策（○○規程第○条） 無線 LAN の SSL、暗号化対策（○○規程第○条） SSL、SQL インジェクション対策（○○規程第○条）	CC と BCC の間違い
利用	各種印刷	不正アクセス （直接関係ない者の アクセス、アクセス権限 がない者のアクセス）	PC やサーバへのアクセス制限をする（○○規程第○条） アクセスログをチェックする（○○規程第○条）	PC 共有の不可 OS、アプリケーションの メーカーサポート切れ
加工	各種印刷	入力間違い 加工間違い	入力者の制限（○○規程第○条） 内校をする（○○規程第○条） 最終校正、刷版の二重チェックをする（○○規程第○条）	不正持ち出し 保管庫の施錠
保管	データ、外部媒体、 成果物	盗難 不正持ち出し	施錠保管・数量チェック（○○規程第○条） 金庫管理（○○規程第○条）	鍵のかけ忘れ 保管庫の施錠
	データ保管	不正アクセス （直接関係ない者の アクセス、アクセス権限 がない者のアクセス）	PC やサーバへのアクセス制限をする（○○規程第○条） アクセスログをチェックする（○○規程第○条） データバックアップ（○○規程第○条） ノート PC、外付ハードディスクの盗難防止（○○規程第○条）	保管場所、ファイル 間違い
	外部媒体、 成果物保管	保管されていた個人情 報がなくなっているこ とに気づかない	個別管理（○○規程第○条）	保管権限超過後の 処理
	成果物保管	見本として、発注者の 同意を得ずに、他の発 注者に見せる	目的外利用の禁止（○○規程第○条） 予備数チェック（○○規程第○条）	保管場所の安全確認 震災対策
委託	委託先からの漏えいなどの事故		評価し、合格した委託先のみに発注する（○○規程第○条） 契約を締結する（○○規程第○条） 個人情報の取扱状況の報告を受ける（○○規程第○条）	ヤレの処分 データの消去・成果 物の廃棄 運送中の事故
廃棄・消去	廃棄物からの 漏えい	紙	シュレッダー処理（○○規程第○条）	
		外部媒体	物理的破壊（○○規程第○条）	媒体再利用
		HDD	物理的破壊（○○規程第○条）	リース物件の返却
		ヤレ紙、廃版	契約回収業者で廃棄（○○規程第○条）	誤廃棄 廃棄場所間違い
返却	社用車で納品	車上荒らし データ・製品の紛失	不要な立ち寄り禁止（○○規程第○条） やむを得ない立ち寄りの際は、カバンに入れて携行する。車内放置禁止（○○規程第○条） 授受記録（○○規程第○条）	鍵のかけ忘れ 返却先の確認 荷崩れ
発送	宅配便	DM の誤封入・紛失	授受記録（○○規程第○条） 出荷前二重チェック（通数、宛先）（○○規程第○条）	誤発送
	郵送	DM の紛失 宛先間違い	DM の紛失、宛先確認（○○規程第○条）	受領の確認
その他	携帯電話、スマホ	紛失	携帯電話の利用ルール（ナンバーロック、紛失時対応）（○○規程第○条）	終業後の取扱い

PDCA+ スパイラルアップ

■PDCA サイクル

個人情報保護マネジメントシステムにおいて、よりよいシステムを構築していく上で P（Plan―プラン）・D（Do―ドゥ）・C（Check―チェック）・A（Act ―アクト）を回していきますが、その上で「継続的改善 ＝ スパイラルアップ」という目標があります。（図 1 参照）

日常業務で個人情報保護の 1 点にだけ集中していると、代表者の見直し時に、スパイラルアップにまで目が向けられることが少ないようです。改善には具体的な課題・問題点があればトップダウン方式で行えますが、PMS が順調に推移している場合でも、現状に満足せず、意識的に現場の営業、制作部門からボトムアップの提案を受けるようにされてはどうでしょうか。業務改善の一環として現状を少しでも改善していければそれが継続的改善となります。

では、どのようにスパイラルアップをすればいいでしょうか。

まず、毎年の『見直し』時に現場からの提案を奨励されることをお勧めします。次にリスク分析において費用面等で早急に手を打てない幾つかの課題を「残存リスク」として挙げていると思います。それらを、いつまでも残存リスクのまま管理していいものでしょうか？一定期間経った時点で残存リスクを“塩漬け”にせず、残存を顕在リスクとして具体的な対策を立てるべきです。それは、業務フローの見直しであったり自主点検項目の見直しでも有効です。残存リスクを顕在化させることがスパイラルアップにつながります。

あるいは、他の部門メンバーの人材の登用といった組織体制の見直しを図ることもお奨めします。

また新規の受注が発生した際や、社内システムを変更した時には、リスク再分析をなさいますが、日々の業務において顧客・委託協力会社からの助言、他社での事故事例の研究、同業者間での経験交流を通じてヒントを得ることも大切です。是非、PMS を機能的に回し、自社のシステムが業務の効率化と個人情報保護が経営に役に立つように工夫して下さい。

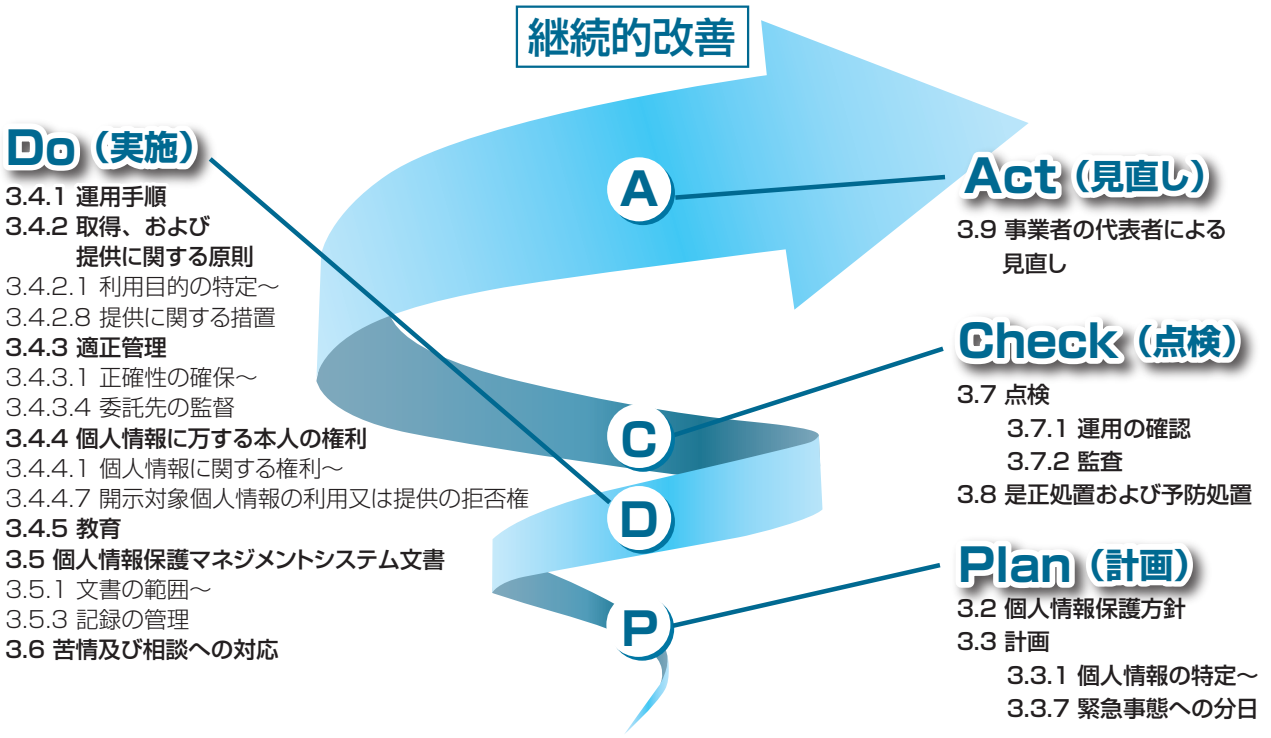


図 1　JIS Q 15001-2006 における PDCA サイクル

※（一財）日本情報経済社会推進協会の資料を参考に作成

個人情報漏洩等の事故とその防止

■個人情報の漏洩

個人情報の漏洩等事故は後を絶ちませんが、プライバシーマークを付与されている事業所からの事故報告も、毎日４～５件にのぼります。

（一財）日本情報経済社会推進協会（JIPDEC）に寄せられた平成 24 年度の事故報告件数は、1,434 件でその原因は、紛失が 26% で１位、以降「封入ミス」「メール誤送信」「宛名間違い」と続いています。なお、紛失の内容は書類は 51%、次いで携帯・スマホ、ノート PC、USB メモリとなっており、この傾向はここ５年程同じ順位です。漏洩の内、誤送信は、封入ミス 17.6%、メール 17.5%、宛名間違い 13.0%、FAX 7.4% の順。盗難は置引き、車上荒らし被害であります。

情報漏洩を防止するためには、まずどのような経路で漏洩にいたるのでしょうか。上記の事故報告にもみられますが、

(1) オフラインでは、紙、PC、メディア（媒体）等で社外へ持ち出され紛失、盗難、故意によるもの

(2) ネットワークを経由するものでメール、外部からの不正アクセス、ウイルス感染等で転送されるもの

(3) 廃棄機器（ゴミ）からでは廃棄サーバ、PC 上で消されず残されたデータ、ヤレ紙等があります。

これらのリスクと安全対策ですが、規程類の不備、ネットワーク上の不正侵入防止（ファイアーウォール）、不正アクセスの検知、セキュリティーホール（セキュイリティパッチの運用）、ウイルス感染（媒体等のウイルスチェック）、外部への送信（メールフィルタリング、Web フィルタリング）、なりすまし（ユーザ認証）、社内 LAN 接続、情報への不正アクセス（アクセス制御）、物理的な不正侵入、廃棄の徹底（データ消去、物理的破壊）…があげられます。

一方で、内部における人的不正行為への対策としては、

①業務内容や責任範囲に即したアクセス権の見直し、アクセス範囲及び権限者を最小限にする。

②不正行為抑制のため、入退室記録、システムへのアクセスログ等の取得と記録の確認

③内部での報告体制の明確化

が挙げられています。

keyword

不正アクセス

Web サイトへの不正アクセスについて、JIPDEC では、従来、コンピュータの OS やアプリケーション等に存在する脆弱性（セキュリティーホール等）を利用して、コンピュータのアクセス制御機能を迂回してコンピュータ内に侵入する行為が多く、最近では、複数のインターネットサイトにおいて【なりすまし】による不正アクセス（不正ログイン）が発生。別の Web サイトから流失した ID やパスワードの情報が転用された可能性が高いといわれています。そこで ID、パスワードの使い回しは避けた方が安全だとしております。

BYOD

BYOD（Bring Your Own Device）とは社員が私有のスマホ、タブレット端末、携帯電話を業務で使用することで、社内のシステムにアクセスし、業務を行う際に利用されています。業務効率の向上のメリットはある一方、セキュリティ面で問題であり、持ち歩いての利用が前提となるため、盗難・紛失による情報漏洩やウイルスもリスクとして考慮すべきです。

印刷・グラフィックサービスに関する

個人情報保護 Q&A

Q 法令遵守について

個人情報保護において、「法令遵守」というキーワードがあります。
どのような法令を特定すればよろしいんでしょうか?

A

個人情報保護において必要な法令、ガイドライン等を以下（表 3） に列記します。ご参照なさり、特定して下さい。

1. 個人情報の保護に関する法律（略称：個人情報保護法平成 15 年 5 月）、2.「個人情報保護に関する法律についての経済産業分野に関するガイドライン」（経済産業省、平成 16 年 10 月策定）、3.「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」（厚生労働省、平成 16 年 7 月策定）4.「雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項について」（厚生労働省労働基準局、平成 16 年 10 月策定）次に、印刷業界として（社）日本印刷産業連合会、（社）日本グラフィックサービス工業会、（公社）東京グラフィックサービス工業会の各ガイドライン。他に自治体の条例として東京都及び所在する市区町村の条例があります。また特定電子メール法、特定商取引法の対象となる事業所はこれらも特定する必要があります。

Q 取材・データ確認

これまで顧客の社内報と OB 名簿の印刷を受注していました。顧客から、これから取材・編集の仕事を受けることとなり、名簿についてはデータ収集、確認から行うようになります。そこでこれまでの印刷受注とは違うので、どのような点に配慮していけばいいでしょうか？

A

まず社内報の発行ですが、貴社がどの段階で取材と編集に関与するのかによって注意すべき点が違ってきます。これまで、社内報は顧客の社内で制作されていたものでしょう。貴社の作業は制作の協力であります。誌面には、役員・従業員の氏名・所属、顔写真、プロフィール等が個人情報として掲載されると思います。ここは、あくまでも「直接でない取得」

表3　個人情報保護に関する法令及び規範一覧

●法　　令
個人情報の保護に関する法律（平成 15 年 5 月 30 日）
●行政ガイドライン
個人情報の保護に関する法律についての経済産業分野に関するガイドライン（経済産業省、平成 16 年 10 月 22 日告示、平成 21 年 10 月 9 日見直し）
雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針（厚生労働省、平成 16 年 7 月策定）
雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項について（厚生労働省労働基準局長、平成 16 年 10 月策定、平成 24 年 6 月 11 日通達）
●業界ガイドライン
公益社団法人東京グラフィックサービス工業会ガイドライン
社団法人日本グラフィックサービス工業会ガイドライン
一般社団法人日本印刷産業連合会ガイドライン
●地方自治体条例・関連法規
都道府県及び市区町村、地方自治体で該当する個人情報保護条例
特定電子メール法、特定商取引法（電子メールの利用や電子商取引をされている企業）
不正アクセス行為の禁止等に関する法律（平成 11 年）
不正競争防止法（平成 23 年 12 月改正）
営業秘密管理に対する指針（経済産業省、平成 25 年 8 月改正）

です。確認すべき点は、貴社が取材する対象者に企業から委託されている旨を伝え、個人情報の利用は社内報の作成のみに使用するという利用目的を伝えること。そして、印刷に至るまでの顔写真等の個人データの利用・保管・廃棄については顧客と確認しておけばよろしいでしょう。

次に、OB 会の名簿ですが、住所等の確認アンケート等で退職者本人への連絡は顧客からの依頼を受けて代行していることを本人へ通知し、個人情報の利用は OB 会名簿の作成のみに使用するという利用目的を伝えることです。そして前述の社内報と同様に、印刷、発送に至るまでの個人データの利用・保管・廃棄については、顧客と確認しておけばよいでしょう。

但し、名簿は OB のみならず在職社員にも配布されるんでしたら、その旨も事前に知らせ、本人が同意しない情報、例えばメールアドレス等は、名簿に記載するかしないかを確認しておく必要があります。

いずれにせよ、これまでの印刷受注から企画やデータ収集段階から請け負うことになりますから、貴社の制作スタッフで新しいリスクを分析され、仕事の着手前に顧客との取り決めを充分に行ってください。

さらに、貴社として直接でない取得にあたりますからホームページ等に、個人情報の利用目的を公表されておくとよいでしょう。

Q 「防犯カメラ」の取り扱い

最近、街の至る所に防犯カメラが設置され、事件での犯人逮捕に利用されています。当社でも繁華街から程近い立地のため、社外に監視カメラを設置しておりますが、機器の入れ替えがあり、これを契機に工場内にも安全と従業者のモニタリング用に設置することにしました。何か問題はありますか？

A

貴社はプライバシーマークの付与事業者ですから、すでに「監視カメラ作動中」というステッカーを貼っていますし、個人情報の取得と特定されてい

Column

ハインリッヒの法則をご存知ですか?

「ハインリッヒの法則」というものをご存知でしょうか。この法則は、アメリカのハーバード・ウィリアム・ハインリッヒ氏が労働災害の発生確率の分析を行ったなかでの経験則の 1 つで、1 つの重大事故の背景には、29 の軽微な事故があり、その背景には 300 の異常（ヒヤリ・ハット）が存在するというもの。さらに幾千件もの不安定状態が存在しているというもので「1：29：300 の法則」とも呼ばれています。この法則から導き出せる教訓として、重大な事故というものは、軽微な事故を防いでいれば発生しないものであり、軽微な事故はヒヤリとするような事故を防いでいれば発生しないものであるということ。この法則は色々なものに適用することができます。300 件のヒヤリ・ハットを分析、原因を探り対策をとることは、その背景にある不安全行動、不安定状態を取り除くことで重大な事故を未然に防げるという考えです。

プライバシーマーク制度では、漏洩等で 1 件の事故が起きても報告してもらっています。「何故 1 件の間違いまで事故報告を要求するのか?」というご指摘もありますが、というのも、たとえ 1 件であってもその背景を考え、事故処理をキチンと行い、再発防止策を立てれば以降の事故がなくなると考えているからです。

この「ハインリッヒの法則」等をご理解願えれば、広く作業ミス防止につながると確信します。

ますので問題はありません。ただ、今回従業者のモニタリング目的で工場内に設置されるとなると、「監視カメラ作動中」と貼りだすだけではいけません。

従業者のモニタリングを実施する場合は、厚生労働省告示で『雇用管理に関する個人情報の取扱い指針』では、予め労働組合等に通知し、必要に応じ協議することが望ましいとし、労働者に周知することが望ましいと定めています。利用目的を通知または公表する必要があります。

1．モニタリングの目的、すなわち取得する個人情報の利用目的を予め特定し、社内規程に定めるとともに、従業者に明示すること。
2. モニタリングの実施に関する責任者とその権限を定めること。
3. モニタリングを実施する場合には、予めモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底すること。
4. モニタリングの実施状況については、適正に行われているか監査又は確認を行うこと。

としています。ここで云う「モニタリング」とは、監視カメラ、従業員のメールチェック等を指します。

Q 「選挙」関連データ

先般、国会と地方自治体の選挙があり当社でも候補者のポスターをはじめハガキ、ビラの印刷、後援会名簿やハガキ宛名印字を候補者から依頼を受けました。選対事務長さんと印刷に関する契約書は結びましたが、プライバシーマークの付与事業者として本人同意の件で「政治団体」は個人情報保護法の適用外だということで、本人同意はないまま仕事を終えました。社内では何か釈然としない思いが残っておりますが…

A

貴社はプライバシーマークの付与事業者ですから、個人情報の取扱いで取得に際しては、本人同意を得ているか、個人情報保護法等に沿って適切に取得していることを委託者に確認しなければなりません。確かに「政治団体」は、個人情報保護法の適用外であります。他にも報道機関、著述業、大学等研究機関、宗教団体は、法律に定める個人情報取扱事業者の義務を負わない、とされております。

ただし、「該当しない」からといっても貴社にも秘密保持義務は生じており、貴社のマネジメントシステムに従った取扱いはしなければなりません。選挙案件は、法の適用外であっても今回のデータ等の保管・廃棄の取扱いは、通常の個人情報物件と同様に扱ってください。

Q 本人の同意の確認の必要性

当社は仲間仕事や代理店さんから名刺や会員証といった仕事を下請けで受注しています。個人情報保護では「本人の同意」ということを求められていますが、当社では他にもオンデマンドでハガキや小物を処理しています。本人同意が必要となると、どの時点で確認すればいいんでしょうか？

A

個人情報に関する受注では「事業者は適法かつ公正な手段によって個人情報を取得しなければならい」と JIS で定められています（個人情報保護法第18条）。下請の場合は、直接でない取得となります。まず、貴社のホームページに個人情報の利用目的を明記され、その中に名刺、はがき、会員証印刷といった営業品目を掲載し、委託された個人情報を取り扱う旨を記載してください。原則は下請であっても、委託元（発注者）に本人の同意が取られているのかを確認する必要があります。ただ、仕事を頂戴する立場で、あまり強く確認できないかもしれません。それでも顧客には「本人確認を取ってください」とお願いしてください。あるいは、当初の契約段階で「委託される印刷物の個人情報は本人確認を得られたものを発注する」といった約束がなされれば結構です。それも無理であるならば、受注毎に委託元（顧客）との伝票に確認欄を設け、貴社でサインなりチェックをなさってください（プライバシーマーク付与事業所にはこの点を要求しております）。トラブルが発生した場合の担保となります。

ところで、貴社は受注している名刺や会員証のデータの保管・廃棄のルールを定め、安全措置は施されていますか？リピート受注目的で保管しているならば顧客と充分、確認を取っておいてください。

また、最近は印刷通販、Web 入稿の形で受注されるケースも増えております。当会会員企業でも通販事業や Web を介した営業展開をされております。そうした企業へは、Web ではどのようなお仕事が飛び込んでくるかわからないので、特にプライバシーマーク付与事業所には、受注段階で、「本人同意のあるものを受注する」旨、明記し、本人同意を得ていないものは受注しないようにお願いしております。

column

スマートフォン情報セキュリティ３か条
～利用者が最低限取るべき情報セキュリティ対策～

スマートフォンの利活用が急速に進む中で、総務省と経済産業省では、「スマートフォン・クラウドセキュリティ研究会」を立ち上げ、平成24年６月29 日に最終報告書をまとめました。研究会で下記の注意事項 3 項目が提案されました。皆様も参考に各社で準拠されるようお奨めいたします。

スマートフォンは、アプリケーションを活用することで、様々な機能を自由に追加できる便利な携帯電話です。しかし自由さの反面、その中には危険なアプリケーションが混じっている場合もあります。利用者自身で情報セキュリティ対策を取ることが必要です。

紛失・盗難対策や他人による不正利用防止対策など、従来の携帯電話と同様の対策が必要です。さらにスマートフォンにおいては、次の 3 つの対策が大切です。

1．OS（基本ソフト）を更新

スマートフォンは、OS の更新（アップデート）が必要です。古い OS を使っていると、ウイルス感染の危険性が高くなります。更新の通知が来たら、インストールしましょう。

2．ウイルス対策ソフトの利用を確認

ウイルスの混入したアプリケーションが発見されています。スマートフォンでは、携帯電話会社などによってモデルに応じたウイルス対策ソフトが提供されています。ウイルス対策ソフトの利用については、携帯電話会社などに確認しましょう。

3．アプリケーションの入手に注意

アプリケーションの事前審査を十分に行っていないアプリケーション提供サイト（アプリケーションの入手元）では、ウイルスの混入したアプリケーションが発見される例があります。アプリ提供事業者や携帯電話会社などが安全性の審査を行っているアプリケーション提供サイトを利用するようにしましょう。インストールの際にはアプリケーションの機能や利用条件に注意しましょう。

スマートフォンを利用する場合の注意点

公衆 WiFi などの携帯電話会社のネットワークを介さないアプリケーションの利用の際には、セキュリティ上の危険性に注意が必要です。

これまでの携帯電話端末と異なり、スマートフォンは、パソコンの場合と同様、ウイルスに感染するおそれがあるなど情報セキュリティ上の危険が高くなっています。

前述の OS（基本ソフト）の更新や、スマートフォン用のセキュリティ対策ソフトの利用をすることや、信頼できるアプリケーション・マーケットからアプリケーションを購入することが有効です。

アプリケーションによっては、スマートフォンに保存された個人に関する情報（電話帳、位置情報など）が、アプリケーション提供者によってアクセス、あるいは保存・管理されることもあります。ダウンロード時は利用許諾画面や利用規約等において、収集される利用者情報の範囲や利用目的などをよく確認し、内容を理解した上で、同意し、利用するよう努めましょう。また、普段からパスワードロックを掛けておくなど端末の紛失や盗難にもご注意ください。

画面がフリーズする（固まってしまう）、バッテリーがすぐに無くなってしまうなどの現象も多く見られます。多くのアプリが同時に起動されているなどが原因の場合が多いので、ご注意ください。

スマホにも注意

ひやり…!? 実際にあった事故事例集

事故事例①

●請求書を別のお客様のものに誤封入してしまった!

原　　因

個人客に対しての請求書ですが、従来から納品とは別に請求書を出しております。単純ミスで中身と宛名シールを貼り間違えてしまいました。ところが、お一人は前回の代金が未収でしたので「再請求書」も同封しており、間違えた方にはその再請求書も同封されており、2重のミスとなりました。

対　　策

単純ミスで片づけてはならなりません。当社が問題視したのは前回未収分の再請求書を同封したことで、別のお客様にも分かってしまったこと。内容と宛名シールを間違えたことへの再発防止は、窓あき封筒を使用することで、チェックが不要となる。そして再請求書の発行ルールを決めること。さらに前回のご注文の集金をキチンと行うこと。ついつい個人客の場合、後払いを慣例にしてきたことも改善するように努めることを決めました。

事故事例②

●年賀状印刷での入れ違いを起こしてしまった!

原　　因

昨年末の年賀状印刷受注で、誤封入をしてしまいました。4 面付けでオンデマンド印刷をしております。たまたま同じ絵柄で端数の注文枚数でしたので、ヤレというか白紙を減らそうと 2 件分を面付けして印刷しましたが、結果、梱包時に複数枚の入れ違いとなり、後日両者から別のものが入っていたとのクレームでした。

対　　策

すぐに両者へ刷直しをして送付、誤送のハガキは廃棄をお願いしました。

当社では、オンデマンドで端数の印刷の場合、こうした心配もあるので「白紙」となってもいいからと口頭で注意はしていたんですが、結果として混入し、さらにそのチェックも絵柄と枚数のみだったため、今回の誤封入が発生しました。

再発防止策として、改めて端数の処理ルールを徹底させ（白紙が出ても良い）、納品チェックに枚数と同時に担当者 2 名で顧客の名前の確認も行うこととを徹底させました。

事故事例③

●送付リストのエクセルデータのズレで DM 誤送信

企業案内の DM 発送 28,000 通の印刷・発送を請け負い、封入封緘・発送を委託先で行っています。DM 送付企業より宛名の担当者名が違っているとの問い合わせ電話が 50 件あり、判明した。送付先リストの企業名と担当者名がずれて印字し発送してしまいました。（28,000 件の内 7,000 件は担当者名記載なし）⇒誤記載件数 21,000 件

原　　因

預かった企業データの内、600 件のリストの削除を依頼され、指示のあったデータをエクセル上のフィルター操作にてフラッグを立て、各行一括削除をしたところ、何らかのバグが発生し、本来削除されるべき 7 名の担当者名が残り、符号すべき企業名と担当者名が順次ずれた状態で印字し発送しました。

定めたルールでは、エクセルデータからアクセスに取り込む手順を遵守せず、専任のデータ処理担当がいるにも関わらず営業担当者が個人的に処理しました。さらにダブルチェックを怠るという 3 重のミスが重なりました。

対　　策

●**委託先**：委託先でのダブルチェック実施フローの徹底、作業フローの徹底（業務担当の明確化）、アクセスでの作業の徹底、飛び番でのデータチェックの実施。

●**当社**：変更データを当社およびクライアントを含む 3 者チェック実施フローの徹底、飛び番でのデータチェックの実施、教育の再実施、委託先への現地調査

●**クライアント**：変更データを当社およびクライアントを含む 3 者チェック実施フローの徹底

★禁止事項：データ作成時のエクセルフィルタの使用禁止

事故事例④

●メールを誤送信してしまった!①

原　　因

顧客へのメール送信の際にアドレス帳で同姓の人がおり、氏名の最終確認を怠り、別人に送信してしまいました。

対　　策

顧客へのメール送信はメルアドの誤入力を避けるため、アドレス帳に登録して利用するルールだったのですが､同姓の人の氏名確認をせず送信しました。そこで、対応策としてアドレス帳には氏名だけでなく所属等を付記し、識別することとしました。

事故事例⑤

●FAX を誤送信してしまった!

原　　因

FAX の送信でグループで一括送信できるようにしております。ところが、名刺の校正で特定のお客様は番号を記憶させており、一々番号入力しないように注意しております。ところが、オペレータが慌てたのでしょうか、個別のお客様と一緒に一括送信ボタンを押してしまい、多数のお客様に対して名刺の校正を送信してしまいました。

対　　策

個人情報を含む FAX 送信には、注意を怠らないことはもとよりですが、単に送信ミスしたオペレータを責めるのではなく、改善策として、FAX の送信ボタンで２つ押してしまうことのないようにボタンの位置間隔をあけることにしました。そして、事務機業者へ FAX 送信の確認方法なり誤送信防止の提案を受けることとし、近々 FAX を入れ替えることにしました。

事故事例⑥

●携帯電話を紛失してしまった!

原　　因

終業後、飲食した際、会社から貸与された携帯電話ごとカバンを紛失、警察に届けたが発見されず、その携帯電話 PHS へ電話してみたが誰も出ませんでした。携帯電話のアドレス帳にはパスワードを掛けていませんでした。

対　　策

紛失と同時に電話会社へ連絡し、通話不能にしてもらいました。携帯電話の利用明細では紛失後、使用された形跡はありません。アドレス帳には500件、その内の数件に不審電話の有無を確認したが相手からは「不審電話はない」との回答。

会社の対応策としては､①終業後の飲酒への注意。②アドレス帳にはパスワードを掛ける。③従業者にパスワードを掛けたことの確認をさせる。④電話会社へ連絡し紛失携帯電話の内部データ消去の機能を利用する。こうした取り扱いルールの徹底を全従業者に教育しました。

事故事例⑦

●メールを誤送信してしまった!②

原　　因

メール送信時に CC と BCC の操作を誤り、70 名余に一斉送信してしまいました。⇒漏洩件数としては 70 名分の氏名とメールアドレス。

対　　策

メールアドレスも個人情報であることから、一斉送信時は特に注意を払わなくてなりません。メールは一旦送信してしまうと取り返しが効きません。当人は 70 余名へ連絡し、メールの削除をお願いしました。CC と BCC は注意を払いたいものです。

メール送信に注意

安全管理措置はどのように対処にすべきか？

■安全管理措置

個人情報保護で最も重要なポイントは、安全管理措置になります。個人情報が漏洩した際に、本人が被る権利の侵害の大きさに即して適切な措置を取ることで、各社で実行可能な範囲で最良の技術を適用することです。

JIS の要求事項では

(1) 組織的安全管理措置
(2) 人的安全管理措置
(3) 物理的安全管理措置
(4) 技術的安全管理措置

の 4 項目があります。これは経済産業省のガイドラインにも詳しく示されております。参照なさって下さい。(JaGra のパンフレット〔H21.12 発行〕にも掲載。)

15 頁にチェックポイントを記載してありますが、社内でリスク分析を行い、対策を立てなくてはならない項目です。自主点検、内部監査時にもチェックしておくとプライバシーマークの外部審査時にも確認される必須の項目となりましょう。

「安全管理措置」を概観すれば、

組織的安全管理措置では、自社に組織を作り、規程を定め、個人情報の一覧表と局面毎のリスク分析をし、PDCA を回し、事故への対処を準備することです。

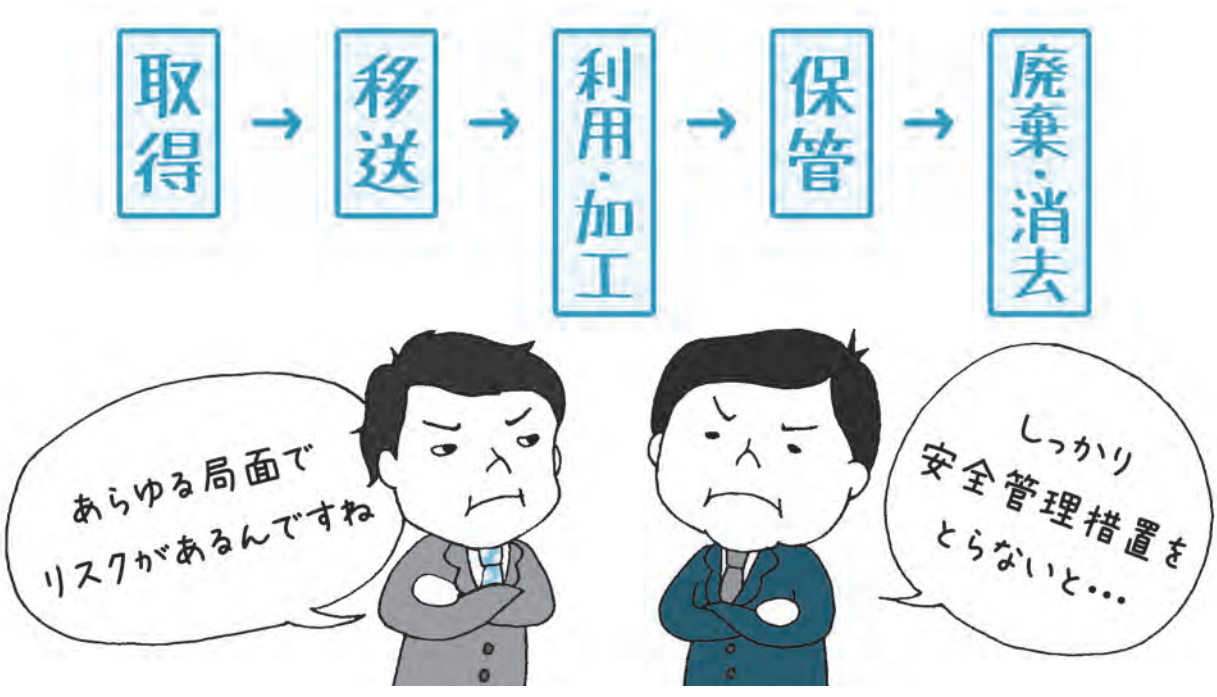
人的安全管理措置は、従業者と雇用契約時に個人情報の非開示契約を締結し、従業者に対する教育・訓練を定期的に実施します。

物理的安全管理措置は、建物等への入退館管理、盗難等の防止、機器・装置等を物理的に保護、個人情報の保管・廃棄・消去を行います。

技術的安全管理措置は、個人情報へのアクセスにおける識別と認証、アクセス制御、アクセス権限を管理、システムの不正ソフトウエア対策を立て、移送・送信時の保護、情報システムの監視を行うことです。

例えば、最初入室・最終退室の施錠確認の記録と確認、情報システムへのアクセスログの取得とチェックといったことですが、取得・移送・消去・廃棄・入退・盗難・アクセス・不正ソフトウエアの対策等々となります。

これはあくまでもリスク分析の結果を反映して、規程化し手順を定めて欲しい措置です。



安全管理措置とは

安全管理のCheck Point! ①

個人情報取得時の対策

- □ 個人情報の誤入力や改ざん等を防止するために、入力作業の入力担当者を限定し、入力作業の手続を明確にし、二重入力や別人による二重チェックを実施し、入力場所や入力端末を限定していますか？
- □ 盗聴される可能性のあるネットワーク（インターネットや無線 LAN 等）で個人情報を送受信するとき、個人情報の暗号化やパスワードロック等の秘匿化を実施していますか？

個人情報移送時、データ送信の対策

- □ 個人情報を記録した媒体（紙、電磁媒体）を社外（顧客、委託先等）や社内の遠隔地事業所から手渡し、郵便、宅配便等で受取るとき、責任所在の明確化や受取り後の紛失等を防止するため、受領記録をとり、保管していますか？
- □ 個人情報を記録した媒体を郵便、宅配便、社用車等で送付するとき、誤送付を防止するため、宛先記載ミス、誤封入がどのような手段や方法で防止されているか確認していますか？
- □ 個人情報が記録された電磁媒体の運搬時（自宅に持ち帰る場合を含む）に紛失や盗難が発生したとき暗号化やパスワードロック等の秘匿化を実施していますか？
- □ 個人情報を電子メールや FAX で送信するとき、誤送信を防止するため、宛先や送信内容を確認するルールを守っていますか？
- □ 電子メールを社外の複数宛先に同時に送信する時、その宛先に BCC を使用する等、必要のない個人情報を送信先が知り得ない対策をとっていますか？
- □ 個人情報を Web サイトや FTP で送信する場合は暗号化を実施していますか？
- □ 個人情報を電子メールで送信する場合は、添付ファイルにパスワードまたは暗号化を実施していますか？

建物の入退時の注意、盗難対策

- □ 建物、室、サーバ室、個人情報の取扱い場所への入退の制限機構があり、入退を制限し、また、入退の記録を保管し、定期的にチェックしていますか？
- □ 最終退出時に施錠、防火等の確認を実施した記録を保管し、定期的にチェックしていますか？
- □ 個人情報を取扱う PC の操作において離席時は、ログオフやパスワード付きスクリーンセーバを何分で起動させていますか？
- □ 業務で使用する携帯電話については、取扱いルールを定め、ルールを遵守していますか？ **《紛失防止策、ナンバーロックを実施するほか、リモートロックが出来るようになっている。》**
- □ 携帯可能な PC や外付けハードディスクに個人情報を保管している場合、チェーンロック又はキャビネット等に施錠保管していますか？

アクセス・不正ソフト対策

- □ 個人情報の定期的なバックアップをとっていますか？
- □ 個人情報を保管している情報システムやネットワークへのアクセスログを取得し、保管し、定期的なチェックをしていますか？
- □ 個人情報を取扱う情報システムにはウィルス対策ソフトウェアを導入し、常に最新のパターンファイルを適用していますか？
- □ Web サーバにて個人情報を取得して利用する場合、SQL インジェクション攻撃やクロスサイトスクリプティング等のウェブベースプログラミングの脆弱性への対策を講じていますか？
- □ 個人情報を取扱う情報システムの OS、アプリケーション等にセキュリティパッチを適用していますか？

➡ 続きは次のページにあります

☞以上の安全管理チェックポイントを日常の確認・自主点検時に利用してください。

安全管理のCheck Point! ②

- □ 個人情報にアクセスできる端末にファイル交換ソフトウエア（Winny、Share 等）をインストールしていませんか？
- □ 識別情報（ID, パスワード等）の発行・更新・廃棄をルール通りに行っていますか？
  《人事異動、退職時にアカウントの発行・廃棄の実施》

消去・廃棄

- □ 保管期間が経過した個人情報を確実に消去・廃棄・返却していますか？
  《個人情報を消去・廃棄・返却した記録を取り、その記録を一定期間保管している。》
  《委託先が消去・廃棄することになっている場合、必要に応じて廃棄証明等を取得している。》
- □ 保管期限が定められた個人情報が誤廃棄されないために対策を実施していますか？
- □ PC やハードディスクの廃棄は再利用できない処置をしていますか？
  《外部に廃棄処理を委託する場合は「廃棄証明」を取得している》
- □ PC やコピー機をリース業者やレンタル業者へ返却する時、データを完全に消去していますか？

利用・加工

- □ 個人情報を利用・加工する作業者を限定し、手順を明確にし、Web サイトや FTP で送信する場合は暗号化を実施していますか？
- □ システムの利用者を必要最低限に限定し、利用者に付与するアクセス権限を限定していますか？

あとがき

個人情報保護が印刷業界で問題になってから 10 年近くが経とうとしております。

しかし、相変わらず漏洩、紛失の事故はあとを絶たず、大きな社会問題でもあります。印刷業界としても個人情報保護法の遵守、各種ガイドラインの周知さらにプライバシーマーク制度の普及が進んでおります。ここでは、印刷企業が注意すべき安全管理をはじめとしたチェックポイント、Q&A、実際の事故事例も紹介しております。是非、個人情報保護の活動にご活用ください。

—JaGra、東京グラフィックス個人情報保護委員会—

◇発行人：公益社団法人　東京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：03-3667-3771　FAX：03-3249-0377
URL：http://www.tokyographics.or.jp/
◇発行日：平成 25 年 11 月 19 日

2013.11.19　600 BK