個人情報を守るために、4つの側面から安全管理措置の徹底を！

個人情報の漏えいを未然に防ぐためには、個人情報保護法20条に定められている安全管理措置を「組織的」、「人的」、「物理的」、「技術的」の4つの側面から検討する必要があります。それぞれの側面で具体的にどんな取り組みを行えばよいか、こちらで一例をご紹介します。

組織的安全管理措置

①組織体制の設備
②規定等の設備と規定等に従った運用
③取扱状況を一覧できる手段の設備
④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

物理的安全管理措置

①個人データを取り扱う区域の管理

個人情報データベース等を取り扱う区域（管理区域）については、入退室管理などを実施。


カードプリンター（入退カード発行）


ネットワークカメラ（入退室管理システムと連携）

②機器及び電子媒体等の盗難等の防止

・個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管。
・個人データを取り扱うパソコンは、セキュリティーワイヤー等で固定。
・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を 机上、社内等に放置しない。


セキュリティワイヤー
施錠キャビネット

③電子媒体等を持ち運ぶ場合の漏えい等の防止

個人データが記録された電子媒体又は書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。

ESET DESlock+
データ暗号化ソフト

④個人データの削除及び電子媒体等の廃棄

個人データの削除個人データが記載された書類は、シュレッダーで廃棄。


シュレッダー

人的安全管理措置

①雇用契約時における従業者との非開示契約、及び委託契約等における委託元と委託先間での非開示契約の締結

②従業者に対する内部規定等の周知・教育・実施

研修テキスト　啓発ポスター

集合研修

講義形式による研修に限らず、個人データの取扱責任者からの講話形式やeラーニング形式など、さまざまな形式が考えられます。研修の頻度は事業者の規模や取り扱う個人データの性質などによって適切に判断していただく必要があります。

定着に向けた日々の啓発活動

個人情報保護などのコンプライアンス意識を向上させるためには、日々の啓発活動が不可欠です。社内研修だけでなく、ポスターの掲示やメルマガの配信、グループMTGの実施など意識定着を図るための啓発活動を継続的に実施することが大切です。

技術的安全管理措置

①アクセス制御

個人データを取り扱うことのできる機器及び機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。


ICカード認証
オフィス向け複合機　レーザービームプリンター

②アクセス者の識別と認証

機器に標準装備されているユーザー制御機能により、情報システムを使用する従業者を識別する。

③外部からの不正アクセス等の防止

・個人データを取り扱う機器等のオペレーティングシステムを最新の状態に維持する。
・個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により最新状態を保つ。

HOME
統合脅威管理


ウイルス対策ソフト

④情報システムの使用に伴う漏えい等の防止

メール等により個人データの含まれるファイルを送信する場合は、ファイルにパスワードを設定する。

ESET DESlock+
データ暗号化ソフト

Canon キヤノンマーケティングジャパン株式会社
〒108-8011 東京都港区港南2-16-6 CANON S TOWER

●お求めは信用のある当社で
NETWORK TOP ASSIST
ネットワークトップアシスト株式会社
〒518-0121 三重県伊賀市上之庄1282-2
TEL：0595-21-7211／FAX：0595-21-7272

2017年4月現在

BUSINESS TREND NEWS

キヤノンマーケティングジャパンがお役に立てること

改正個人情報保護法編

企業の大小によらず すべての事業者が 個人情報保護法の対象へ！

- 2017年5月30日 改正個人情報保護法が施行
- 「個人情報保護委員会」が設立され 事件が発生すると 立ち入り検査や罰金適用のケースも
- 中小規模事業者が 知っておくべきポイントを押さえ 自社が個人情報を適切に 管理しているかチェックしましょう

一人でも従業員がいたり、一件でも個人情報を扱うなら、中小規模事業者でも法の遵守が義務づけられることに！

2005年に個人情報保護法が全面施行されて十数年。スマートフォン、SNSなどの情報技術の発展とともに、中小規模事業者の皆様においても、個人情報を取り扱う業務の内容に変化が生じつつあるのではないでしょうか。また、漏えいによるプライバシー侵害の危険も増大。消費者の間でも不安が高まり、今までは取り扱う個人情報が5,000件以下の中小規模事業者については法の対象外であることに対し、疑問の声が挙がるようになりました。そこで、個人情報の利活用の促進と保護強化という二つの観点から対応を検討。この度、改正法が施行されることになりました。

ここに注目！ 主な改正のポイント

	改正前	改正後
① 対象範囲の拡大	・5,000件以上の個人情報の取り扱いがある事業者のみ	・1件でも個人情報を取り扱っていれば対象となる（すべての事業者が対象）
② 個人情報の定義の明確化	・個人情報＝特定の個人を識別することができる情報 ・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もの（個人情報とひもづく移動履歴や購買履歴）	・「個人識別符号」が新たに対象に ① 生体認証に用いられるデータ（身体の一部の特徴を電子計算機のために変換した符号）：DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋 ② サービス利用や書類において対象者ごとに割り振られる符号：公的な番号旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険証等 ・「要配慮個人情報」が新設　本人の人種、信条、病歴、犯罪の経歴など
③ 監督機関の新設	・業種ごとに所轄省庁やガイドランが異なる	・「個人情報保護委員会」に権限を一元化。立入検査権がある。
④ 第三者提供の制限	・名簿の転売ルートをトレースできなかった ・顧客情報データベースから不正に持ち出しても、個人情報保護法上の刑事罰がなかった	・確認記録作成等を義務化（トレーサビリティを確保。第三者提供についての記録・説明義務） ・「個人情報データベース提供罪」の新設 事業者（提供）：記録の作成・保存義務　提供の年月日、受領者の氏名等の記録・保存 個人情報：第三者提供 事業者（受領）：確認、記録の作成・保存義務　提供者の氏名、取得経緯等を確認　提供の年月日、確認事項等を記録保存

万が一のリスク もしも情報が漏えいしたら・・・

たった一度でも情報漏えいを起こしてしまうと、取引先からの信用低下は免れず、補償金などの支払いも発生するリスクがあります。情報の紛失・盗難や不正アクセスなど、原因となるリスクを的確に把握し、対策に努めて、情報漏えいを防ぎましょう。

会社の信頼低下

罰則あり

○国からの命令に違反した場合
⇒6ヶ月以下の懲役又は30万円以下の罰金

○虚偽の報告等をした場合
⇒30万円以下の罰金

○従業員等が不正な利益を図る目的で個人情報データベース等を提供、又は、盗用した場合
（個人情報データベース等不正提供罪）
⇒1年以下の懲役又は50万円以下の罰金

【身近な事例】

CASE 1 銀行員の家族が芸能人の個人情報をツイート

銀行員の母親が業務上知り得た芸能人たちの個人情報を娘に漏らし、ツイートにより流出。重大な個人情報漏えい事件としてTwitterが炎上し、銀行が謝罪する事態に。

CASE 2 教諭が置き忘れた学級名簿がLINEで流出

教諭が校内に置き忘れた新年度の学級編成用の生徒名簿を生徒が発見。スマートフォンで撮影した上、LINEで複数の同級生に送信したことが保護者からの指摘で発覚。

中小規模事業者が個人情報保護法改正ですべきこと！

準備 個人情報を取り扱う者が複数いる場合、責任者を任命

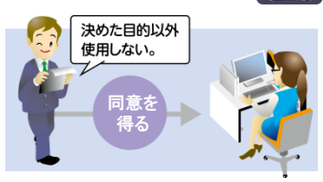
情報漏えい発生時に備えて責任者を任命し、従業員からの報告連絡体制をあらかじめ確認。責任者は年に1回会議を開くなど、取り扱い状況を定期的に点検しましょう。

取得 情報を何に使うか、目的を決めて、本人に伝える

企業が個人情報を利用する際は、あらかじめ利用目的を特定する必要があります。そして、情報取得時に本人に伝えるか、あらかじめホームページや店頭での掲示などで公表してください。

※ただし、例えば名刺交換をした場合など、情報の利用目的が明らかな場合は、逐一相手に伝える必要はありません。

利用提供 決めた目的以外に利用したり、他人に渡す際は本人の同意を得る



取得した個人情報は、あらかじめ公表または同意を得た利用目的の範囲内でしか使えません。したがって、個人情報の取得にあたっては、何に使うかという利用目的をしっかりと考えた上で本人に伝えましょう。もし、すでに取得した個人情報を特定の目的以外のことに利用したり、他人に渡す場合には、あらかじめ本人の同意を得てください。

保管・安全管理措置 安全に管理する

個人情報を取り扱う事業者は、下記のような安全管理措置を施す必要があります。
・個人情報を取り扱う部屋の入退室管理等
・個人情報を取り扱うパソコンをセキュリティーワイヤーで固定
・パソコンのID/パスワード設定、ウイルス対策
・紙の名簿は施錠できるキャビネットで保管など、情報が漏えいしないような措置を検討しましょう。

開示 本人からの請求（開示や訂正など）に応じる

保有している個人情報について、本人から開示や訂正等を請求されたら、企業は対応しなければなりません。また、利用目的を問われた場合もしっかり答えられるようにしておきましょう。

キヤノンマーケティングジャパンの取り組み

キヤノンマーケティングジャパンでは、従業員一人ひとりのコンプライアンス意識向上および浸透を促進するとともに、ワークフローの至るところに漏えい対策のしくみを導入。特別意識しなくても、日頃の業務を通じて知らず知らずのうちに個人情報保護が徹底できています。

物理的安全管理措置

・IDカードによる入退室管理、生体認証、ネットワークカメラの導入
・5Sの徹底によるクリアデスクの実践 など

取り組み例 情報セキュリティ報告書2016
キヤノン 情報セキュリティ 検索

人的安全管理措置

・グループの全社員・従業員を対象とした独自のウェブ教育を毎年実施
・コンプライアンス意識共有のために、「キヤノングループ行動規範」「コンプライアンスカード」を配布
・月次のメールマガジン「Monthly Compliance News」の配信や、半期に1度の「コンプライアンス・ミーティング」でコンプライアンス意識の浸透を推進など

技術的安全管理措置

・電子メールモニタリング「GURDIAN」シリーズの導入
・ウイルスソフト「ESET」の導入
・オフィス向け複合機のICカード認証の導入
・OSやアプリケーションの更新漏れなどを防ぐ「PCセキュリティチェッカー」など

詳しくは 国の行政機関 「個人情報保護法質問ダイヤル（個人情報保護委員会）」 電話番号 03-6457-9849　受付時間 土日祝日および年末年始を除く 9:30～17:30