

その取扱いで大丈夫？ あなたの会社の “個人情報”

こんな時
どうしたらいい??

不正アタックで
情報が漏れた

うちから
情報漏れと
苦情がはいった

アンケート
とりたいけど
どうしたらいい

PC落とした

これを読んで！
解決！！

本パンフレットは、事業者の皆さんに、
個人情報保護法を遵守し、
大切な個人情報を適切に活用するために、
最低限知っていただきたいことを
☆まとめたものです。



経済産業省商務情報政策局情報経済課

http://www.meti.go.jp/policy/it_policy/privacy/

1 「個人情報」ってなんだろう？



個人情報保護法では、保護が必要な情報を「個人情報」、「個人データ」、「保有個人データ」の3つの概念に分かれています。

3つの概念ごとに、実施しなくてはならない義務が定められています。個人情報よりも個人データ、個人データよりも保有個人データの方が、守るべき義務が増えていきます。

① 個人情報

- ☞ 生存している個人に関する情報
- ☞ 特定の個人を識別可能な情報
- ☞ 他の情報と容易に照合でき、その結果個人が識別できる情報も含まれる。

② 個人データ

- ☞ ①のうち、特定の個人情報を検索できるように体系的に構成したもの（個人情報データベース等）に含まれる個人情報

③ 保有個人データ

- ☞ ②のうち、6ヶ月を超えて継続利用するもののことで、かつ、開示、訂正、消去等の権限のあるデータ

① 個人情報

- ☞ 利用目的の特定（15条）
- ☞ 利用目的による制限（16条）
- ☞ 適正な取得（17条）
- ☞ 取得に際して利用目的の通知等（18条）
- ☞ 苦情の処理（31条）

② 個人データ

- ☞ データ内容の正確性の確保（19条）
- ☞ 安全管理措置（20条）
- ☞ 従業員の監督（22条）
- ☞ 第三者提供の制限（23条）

③ 保有個人データ

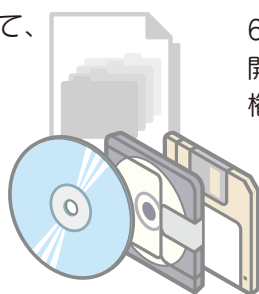
- ☞ 保有個人データに関する事項の公表等（24条）
- ☞ 開示（25条）、訂正等（26条）、利用停止等（27条、理由の説明（28条）、開示手続（29条）、手数料（30条）

① 個人情報



ソフトに入力して、データベースにした場合

② 個人データ



③ 保有個人データ

6ヶ月以上保有。
開示・訂正等の
権限を有する



2 「個人情報取扱事業者」って誰のこと？



個人情報保護法上の義務を負う「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者です。

しかし、現実には、ほとんどの事業者がこの定義に該当すると考えられます。個人事業主、NPO 等の非営利組織であるからと言って、法律上の義務の対象にならないわけではありません。

個人情報保護法の義務を負うのは誰か？

「個人情報取扱事業者」

個人情報データベース等を事業の用に供している者（2 条 3 項）

☞ 情報処理やソフトウェア開発等をしている会社ばかりが対象ではない。

【個人情報データベースに該当する事例】

- メールソフトのアドレス帳、仕事で使う携帯電話の電話帳、ソフトウェア等でリスト化された従業者や顧客台帳
- 五十音順に整理し、インデックスを付してファイルしている、登録カード
- 氏名、住所、企業別に分類されている市販の人名録

☞ 上記を業務に使っている会社は全て「個人情報取扱事業者」となる。

☞ 法人には限定されないで、「個人事業主」であっても、個人情報取扱事業者。

☞ 営利、非営利も問われないので、「NPO など」も個人情報取扱事業者。

【例外 1】：事業者に該当しない

個人情報データベース等に含まれる個人情報によって、識別される特定の個人情報の数の合計が、過去 6 ヶ月以内のいずれの日においても 5,000 を超えない者

【例外 2】：義務規定が適用されない

- ①報道機関が報道活動の用に供する目的
- ②著述を業として行う者が著述の用に供する目的
- ③学術研究期間等が学術研究の用に供する目的
- ④宗教団体が宗教活動の用に供する目的
- ⑤政治団体が政治活動の用に供する目的

3 これだけはやっておこう

(1) 利用目的の特定・適正取得



個人情報を取得するときの最も基本的なルールは、①あらかじめ利用目的をできる限り特定する、②取得する際には利用目的の通知・公表等を行う、③利用目的の範囲内で個人情報を取り扱う、④個人情報は適正な方法で取得する、という4つです。

利用する目的を明確にして、本人にわかるようにした上で、適正に取得してください。

①利用目的の特定

● 利用目的は、予めできる限り特定する（15条1項）

☞ 個々の取扱いが利用目的の達成に必要な範囲内かどうか、本人が実際に判断できる程度に明確に利用目的を定める

☞ 「事業活動に用いるため」、「マーケティング活用を求めるため」のような利用目的では、“特定した”ことにならない

● 利用目的は、「変更前の利用目的と相当の関連性を認められる範囲」内でない限り、事後的に変更することはできない（15条2項）

● 個人情報は、予め特定された利用目的の達成に必要な範囲でのみ、取り扱うことができる（16条1項）

③利用目的の範囲内で扱う

● 変更前の利用目的と相当の関連性を有すると合理的に認められる範囲であれば、変更可能

→変更された利用目的を、
本人に通知・公表することが必要

● 変更前の利用目的と相当の関連性を有すると合理的に認められない範囲

→変更には、事前に本人の同意取得が必要

②利用目的の通知・公表等

● 個人情報を取得した場合は、あらかじめその利用目的を本人に通知し、又は公表しなければならない（18条1項）

間接取得 18条1項

個人情報を取得（直接取得・間接取得ともに）
①インターネット上で本人が自発的に公にしている個人情報を取得する場合

②個人情報の第三者提供を受ける場合

③個人情報の委託を受けて、個人情報を取得する場合

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らない

直接取得 18条2項

直接書面等による取得
書面等による記載、ユーザー入力画面への打ち込み等による取得

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

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

④適正な方法で取得する

● 偏りその他不正な手段によって個人情報を取得することはできない。

☞ 親の同意なく、十分な判断能力を有していない子どもから、家族の収入事情などの個人情報を取得する行為は「不正な取得」に該当します。

☞ 不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにも関わらず、取得する場合も「不正な取得」に該当します。



取り扱う個人情報が「個人データ」に該当する場合には、適切な個人情報の保護と活用を実現するために、「安全管理措置（情報セキュリティ管理策）」を実施することが必須です。

安全管理措置（情報セキュリティ管理策）の実施

安全管理措置には、「組織的」、「人的」、「物理的」、「技術的」の4つの側面があります。それぞれ、具体的には以下のような対応を行うことが考えられます。

【組織的安全管理措置】

①組織体制の整備

（例：個人情報保護管理者の設置、部署や従業員の役割・責任の明確化、監査実施体制の整備など）

②規程等の整備と規程等に沿った運用

（例：情報システムに関する規程等の整備とそれに従った運用、監査証跡の保持など）

③取扱状況を一览できる手段の整備

（例：個人データ取扱台帳の整備など）

④安全管理措置の評価、見直し及び改善

（例：監査計画の立案・実施など）

⑤事故又は違反への対処

（例：事故発生時の対応手順の整備など）

【人的安全管理措置】

①雇用契約時における従業員との非開示契約の締結、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従業員に対する内部規程等の周知・教育・訓練の実施

（例：安全管理措置について定めた規程等についての周知、従業員の役割・責任についての教育・訓練の実施、必要且つ適切な教育・訓練の実施に係る確認）

【技術的安全管理措置】

①アクセスにおける識別と認証

（例：ID/パスワードによる認証、生体認証など）

②アクセス制御

（例：アクセスを付与する者の最小化など）

③アクセス権限の管理

（例：アクセス権の許可権限管理の適切な実施など）

④アクセスの記録

（例：データ操作の成功と失敗の記録など）

⑤不正ソフトウェア対策

（例：ウイルス対策ソフトウェア導入など）

⑥個人データ移送・送信時の対策

（例：データの暗号化等の秘匿化など）

⑦情報システムの動作確認時の対策

（例：情報システム変更時にセキュリティが損なわれないことの検証など）

⑧情報システムの監査

（例：定期的監査の実施、アクセス状況の監視など）

なるほど！
なるほど！





取扱う個人情報が「個人データ」に該当する場合には、適切な個人情報の保護と活用を実現するために、正確で最新の内容に保つことに取り組むほか、実質的に個人データの安全性を確保するために、従業者や委託先の監督をしっかりと行うことが求められます。

個人データの正確性・最新性の担保

- 個人データは、利用目的の達成に必要な範囲内で、
正確性・最新性を担保しなくてはならない。
- ☞ 誤った個人情報を利用することで、不利益を与えないようにするため。
- ☞ 具体的には、「個人データ入力時の照合・確認手続の整備」、「訂正等の手続の整備」、「記録事項の更新」、「保存期間の設定」などを行うことが求められます。

従業者の監督

- 安全に個人データを管理するためには、従業者に対して必要かつ適切な監督が必要です。
- 「従業者」とは、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、監査役、感じ、派遣社員等も含まれます。

委託先の監督

- 個人データの取扱いを委託する場合には、委託先に対し、必要かつ適切な監督が必要です。
- 委託する場合にも、委託する業務内容に対して必要のない個人データを提供しないようにする必要があります。

具体的対策

- 委託先の選定の際の基準の策定と運用
(一定の安全管理措置を講じている事業者への委託、委託先の評価の実施)
- 委託先との間の機密保持契約の締結
- 委託先との契約への、
委託された個人データの取り扱い状況を合理的に把握することを盛り込んだ契約の締結と、委託先の取り扱い状況の確認
- 委託契約に盛り込むことが望ましい内容
 - ・ 委託元及び委託先の責任の明確化
 - ・ 個人データの安全管理措置に関する事項
 - ・ 再委託に関する事項
 - ・ 個人データの取扱状況に関する委託元への報告の内容及び頻度
 - ・ 契約内容が遵守されなかった場合の措置
 - ・ 事件・事故発生時の報告 / 連絡に関する事項

苦情の処理 第31条

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らない

事業者にとって、
苦情への対応って
大切よね



③ これだけはやっておこう (3)「第三者提供」をする時には



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いけません。
同意の取得にあたっては、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範囲の内容を明確に示すことが必要です。

【原則】 第三者提供には、あらかじめ本人から同意を得なくてはならない。

例外的な場合

① 法令に基づく場合

- ☞ 警察や検察等から、刑事訴訟法に基づく捜査関係事項照会があった場合
- ☞ 弁護士会等から、弁護士法に基づく所要の弁護士会照会があった場合

② 人の生命、身体又は財産の保護に必要な場合

- ☞ 大規模災害や事故等の緊急時に、患者の家族等から医療機関に対して、患者に関する情報提供依頼があった場合

③ 公衆衛生・児童の健全育成に特に必要な場合

- ☞ 地域がん登録事業において、地方公共団体から医療機関に関しての、がんの診療情報の提供依頼があった場合

④ 国等に協力する場合

- ☞ 税務署等から事業者に対して、任意の顧客情報の提供依頼があった場合
- ☞ 統計調査に協力する場合

第三者に当たらない場合

① 委託先への提供

② 事業の承継合併等に伴う提供

③ 共同利用

(ただし、共同利用する者の範囲や利用目的等をあらかじめ名隠している場合に限る)

オプトアウトを行っている場合には、本人の同意なく、個人データを第三者に提供することができます。

- 第三者に提供される個人データについて、本人の求めに応じて第三者への提供を停止することとしている場合
 - 以下の項目について、あらかじめ通知し、または本人が容易に知り得る状態に置いているとき
- ① 第三者への提供を利用目的とすること ※注
 - ② 第三者に提供される個人データの項目
 - ③ 第三者への提供の手段又は方法
 - ④ 求めに応じて提供を停止すること

※法第15条の規定により取得時の利用目的に第三者提供の事項が含まれていない場合は、オプトアウトはできない

③ これだけはやっておこう (4)「共同利用」をする時には



「共同利用」については、第三者提供の制限に関する“第三者”に該当しないとみなされます。但し、共同利用する者の範囲や利用目的等をあらかじめ明確にしている場合のみ認められます。

共同利用とは、例えば金融機関相互で延滞や貸し倒れ等の情報を共有する場合や、グループ企業でイベントを開催する場合に、親会社と子会社の間で来場者についての情報を共有するような場合を想定しています。

以下の4つについて、あらかじめ明確に本人に示していることが必須です。

- 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
- ③ 利用する者の取得時の利用目的
- ④ 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融資、責任を有する者の氏名又は名称

「共同利用」か「委託」かは、個人データの取扱形態によって判断されるので、共同利用者の範囲に委託先事業者が含まれる場合にも委託先との関係では監督義務を免れるわけではありません。



個人情報取扱事業者は、本人への周知のため、及び内外に個人情報の取扱方針を広く周知・宣言するために、プライバシーポリシー（個人情報保護指針）を作成することが望ましいです。具体的には、以下のような事項を掲げることが期待されます。

●事業の内容及び規模を考慮した適切な個人情報の取扱いに関すること。

(ア) 取得する個人情報の利用目的
(法第18条関係)

(イ) <個人データの取扱いの委託を行う場合>
(法第22条関係)

- ・個人データの委託を行うこと。
- ・委託する事務の内容

(ウ) <本人の同意なく第三者提供する場合>
(法第23条第2項及び第3項関係)

- ・利用目的に第三者提供が含まれていること。
- ・第三者に提供される個人データの項目
- ・第三者への提供の手段又は方法
- ・本人の求めに応じて第三者への提供を停止すること。

(エ) <共同利用する場合>

(法第23条第4項及び第5項)

- ・特定の者との間で共同利用すること。
- ・共同して利用される個人データの項目
- ・共同利用者の範囲
- ・共同して利用する者の利用目的
- ・共同して利用する者のうち、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

(オ) 以下の保有個人データに関すること。

(法第24条、第25条及び第27条関係)

- ・自己の氏名又は名称
- ・すべての保有個人データの利用目的
- ・「開示等の求め」に応じる手続（定めた場合）
- ・保有個人データの利用目的の通知及び開示に係る手数料の額（定めた場合）
- ・苦情の申出先（認定個人情報保護団体の対象事業者である場合には当該認定個人情報保護団体の名称及び苦情解決の申出先を含む。）

(カ) 開示等の求めに応じる手続に関すること。

(法第29条関係)

- ・申請書の様式（定めた場合）
- ・受け付ける方法（定めた場合）
- ・保有個人データの特定に役立つ情報の提供

(キ) 問い合わせ及び苦情の受付窓口に関すること。

(法第23条第5項、第24条第1項、第29条第1項及び第31条関係)。

●個人情報の保護に関する法律を遵守すること。

●個人情報の安全管理措置に関すること。

●マネジメントシステムの継続的改善に関すること。

もっと詳しい情報をお知りになりたい方は・・・

👉 経済産業分野に関するガイドライン

http://www.meti.go.jp/policy/it_policy/privacy/kojin_gadelane.htm

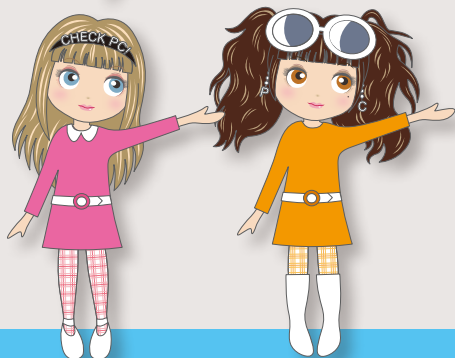
👉 経済産業省の個人情報保護に関連する施策

http://www.meti.go.jp/policy/it_policy/privacy/

👉 消費者庁の個人情報保護に関する施策

<http://www.caa.go.jp/seikatsu/kojin/index.html>

まずは相談 ☆



お問い合わせ先

経済産業省 商務情報政策局 情報経済課
電話：03-3501-0397