

マイナンバー

参考資料

マイナンバーについて定めた法律が、2013年5月24日に成立しました。
2015年10月から個人番号や法人番号が通知され、2016年1月から利用が開始
されます。

本資料では、マイナンバー制度により必要となる企業の対応について解説します。

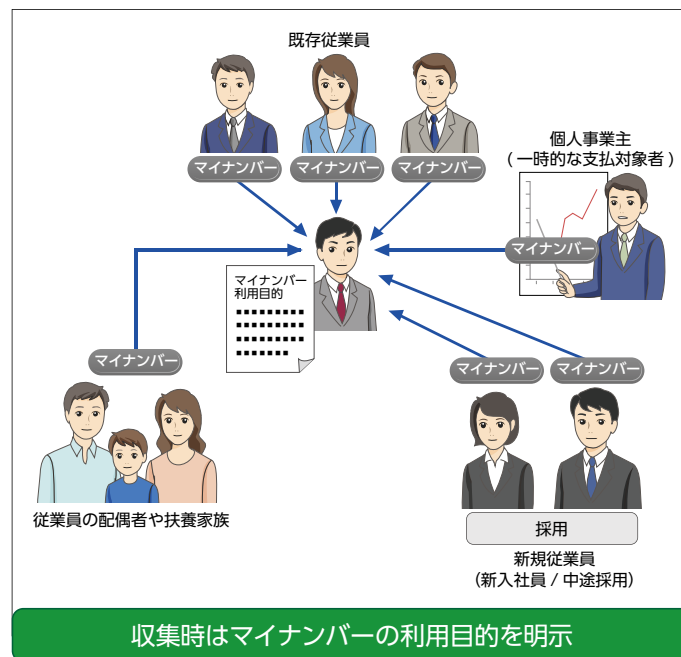
2015年10月
日本商工会議所

-
- 本資料を作成するにあたり、次の文書を参考にしています。
特定個人情報の適正な取り扱いに関するガイドライン(事業者編)平成26年12月11日:特定個人情報保護委員会
 - 本書で題材として使用している個人名、団体名、商品名、ロゴ、連絡先、メールアドレス、場所、出来事などは
全て架空のものです。実在するものとは一切関係ありません。
 - 本書に記載されている内容は2015年10月現在のものです。
 - 本書は法律そのものについての解説資料ではありません。

1 マイナンバーの収集

マイナンバーの利用にあたり、企業では以下の対象者からマイナンバーを収集する必要があります。

- 既存の従業員
- 新規の従業員（新入社員・中途採用社員）
- 従業員の家族（配偶者や扶養家族）
- 健康保険組合の被保険者とその被扶養者、退職した年金受給者
- 個人事業主（弁護士や税理士、講演・執筆者への謝礼金など個人への支払いが発生する場合）



マイナンバーを収集する際は、本人に利用目的を明示する必要があります。源泉徴収や健康保険の手続きなど、マイナンバーを利用する事務利用目的を明示して取得します。

■ 本人確認

マイナンバーの収集には、本人確認が必要です。具体的には以下2点を行います。

● 番号確認

提示されたマイナンバーが提示者本人のものかどうかの確認

● 身元確認

提示者が本人であることの確認

■従業員の扶養家族のマイナンバーを取得する場合の本人確認

扶養家族の本人確認は、各制度の中で扶養家族のマイナンバーの提供が誰に義務づけられているのかによって異なります。

●「税の年末調整」の場合

従業員が、扶養家族のマイナンバーの提供を義務付けられているため、従業員は個人番号関係事務実施者として、その扶養家族の本人確認を行います。

●「国民年金（第3号被保険者）の届出」の場合

従業員の配偶者（第3号被保険者）本人が企業に対して届出を行う必要があるため、企業が当該配偶者の本人確認を行う必要があります。通常は従業員が配偶者に代わって企業に届出をすることが想定されますが、その場合は、従業員が配偶者の代理人としてマイナンバーを提供することになるため、企業は代理人からマイナンバーの提供を受ける場合の本人確認を行う必要があります。

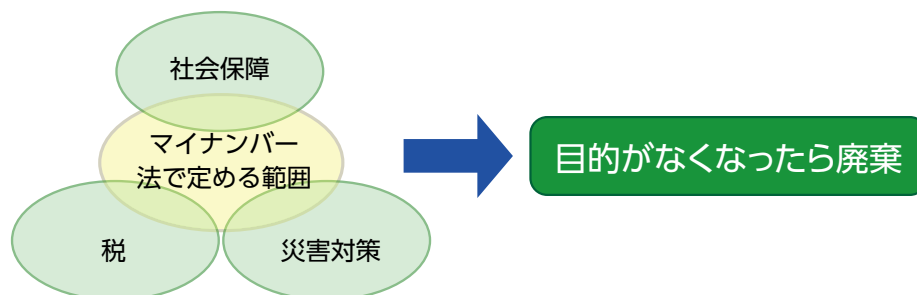
2 マイナンバーの管理・保管

収集したマイナンバーは、適切に管理・保管します。システムで従業員の情報を管理している場合は、マイナンバーを含めシステムで管理できるよう改修する必要があります。

■安全管理措置の概要

マイナンバー法で認められた目的（社会保障、税、災害対策に関する特定の事務等）以外のために、他人（※）の特定個人情報を収集したり保管したりすることは禁止されています。目的がなくなったら廃棄します。

※他人とは「自己と同一の世帯に属さない者」を指すため、子供や配偶者等の本人と同一の世帯の特定個人情報は収集、保管することができます。



企業がマイナンバーを取り扱う際は、その漏えい、滅失、毀損を防止するなど、マイナンバーの適切な管理のために必要な措置を講じる必要があります。

■ 講ずべき安全管理措置の内容

企業は、安全管理措置の検討に当たり、マイナンバー法および個人情報保護法等の関係法令、「特定個人情報の適正な取扱いに関するガイドライン」および各省庁から出されるガイドライン等を遵守しなければなりません。

企業が講ずべき安全管理措置は以下のとおりです。

- | | | |
|------------|-------------|-------------|
| A 基本方針の策定 | B 取扱規定等の策定 | C 組織的安全管理措置 |
| D 人的安全管理措置 | E 物理的安全管理措置 | F 技術的安全管理措置 |

● A 基本方針の策定

特定個人情報等の適正な取り扱いの確保について組織として取り組むために、以下について基本方針として定めます。

- ・事業者名
- ・関係法令・ガイドライン等の遵守
- ・安全管理措置に関する事項
- ・質問および苦情処理窓口

● B 取扱規程等の策定

取扱規程等は、以下の管理段階ごとに、取扱方法、責任者・事務取扱担当者およびその任務等について定めます。

- ・取得する段階
- ・利用を行う段階
- ・保存する段階
- ・提供を行う段階
- ・削除・廃棄を行う段階

● C 組織的安全管理措置

特定個人情報等の適正な取扱いのために、組織的安全管理措置を講じなければなりません。

a. 組織体制の整備

安全管理措置を講ずるための組織体制を整備します。

組織体制として整備する項目には、次のようなものが挙げられます。

- ・事務における責任者の設置および責任の明確化
- ・事務取扱担当者の明確化並びにその役割の明確化
- ・事務取扱担当者が取り扱う特定個人情報等の範囲の明確化
- ・事務取扱担当者が取扱規程等に違反している事実または兆候を把握した場合の責任者への報告連絡体制
- ・情報漏えい等事案の発生または兆候を把握した場合の従業者から責任者等への報告連絡体制
- ・特定個人情報を複数の部署で取り扱う場合の各部署の任務分担および責任の明確化

b. 取扱規定等に基づく運用

取扱規程等に基づく運用状況を確認するため、システムログまたは利用実績を記録します。

記録する項目としては、次のようなものが挙げられます。

- ・特定個人情報ファイルの利用・出力の記録
- ・書類・媒体等の持ち出しの記録
- ・特定個人情報ファイルの削除・廃棄記録
- ・削除・廃棄を委託した場合、これを証明する記録等
- ・特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録

c. 取扱状況を確認する手段の整備

特定個人情報ファイルの取扱状況を確認するための手段を整備します。なお、取扱状況を確認するための記録等には、特定個人情報等は含めません。

取扱状況を確認するための記録等としては、次のようなものが挙げられます。

- ・特定個人情報ファイルの種類、名称
- ・責任者、取扱部署
- ・利用目的
- ・削除・廃棄状況
- ・アクセス権を有する者

d. 情報漏えい等事案に対応する体制の整備

情報漏えい等の事案の発生または兆候を把握した場合に、適切かつ迅速に対応するための対応体制を整備します。情報漏えい等事案の発生時に、以下の対応を行うことを念頭に体制を整備します。

- ・事実関係の調査および原因の究明
- ・影響を受ける可能性のある本人への連絡
- ・委員会および主務大臣等への報告
- ・再発防止策の検討および決定
- ・事実関係および再発防止策等の公表

e. 取扱状況の把握および安全管理措置の見直し

特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直しおよび改善に取り組む必要があります。例として次のようなものが挙げられます。

- ・特定個人情報等の取扱状況について、定期的自ら行う点検または他部署による監査を実施します。
- ・外部の主体による他の監査活動と合わせて、監査を実施することも考えられます。

● D 人的安全管理措置

特定個人情報等の適正な取扱いのために、人的安全管理措置を講じなければなりません。

事務取扱担当者の監督・教育

特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、責任者は事務取扱担当者に対して必要かつ適切な監督を行う必要があります。

また、責任者は事務取扱担当者に特定個人情報等の適正な取扱いを周知徹底するとともに適切な教育を行う必要があります。

● E 物理的安全管理措置

特定個人情報等の適正な取扱いのために、物理的安全管理措置を講じなければなりません。

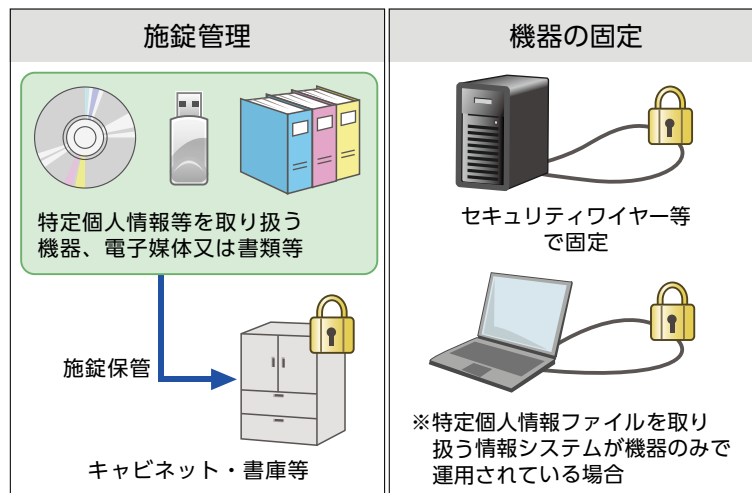
a. 特定個人情報等を取り扱う区域の管理

特定個人情報等の情報漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域および特定個人情報等を取り扱う事務を実施する区域を明確にし、物理的な安全管理措置を講じます。

例えば、機器などの持ち込み制限や、入退室管理を行います。

b. 機器および電子媒体等の盗難等の防止

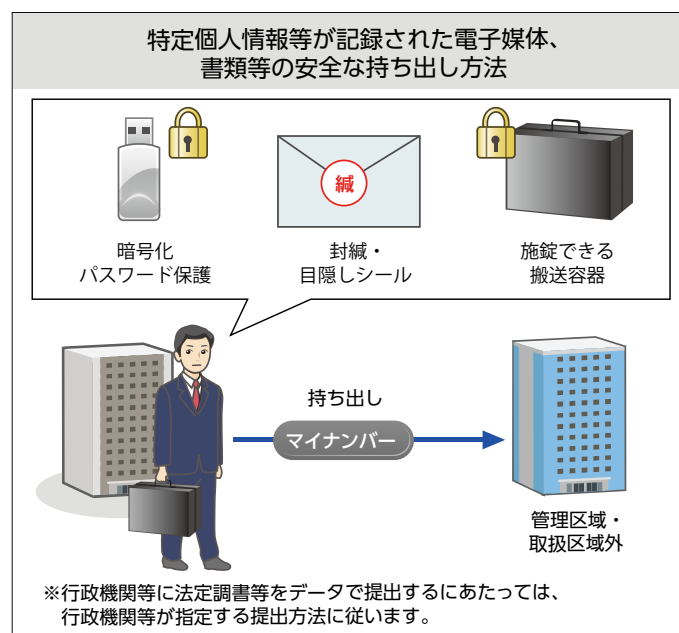
管理区域および取扱区域における特定個人情報等を取り扱う機器、電子媒体および書類等の盗難または紛失等を防止するために、施錠管理、機器の固定などの物理的な安全管理措置を講じます。



c. 電子媒体等を持ち出す場合の漏えい等の防止

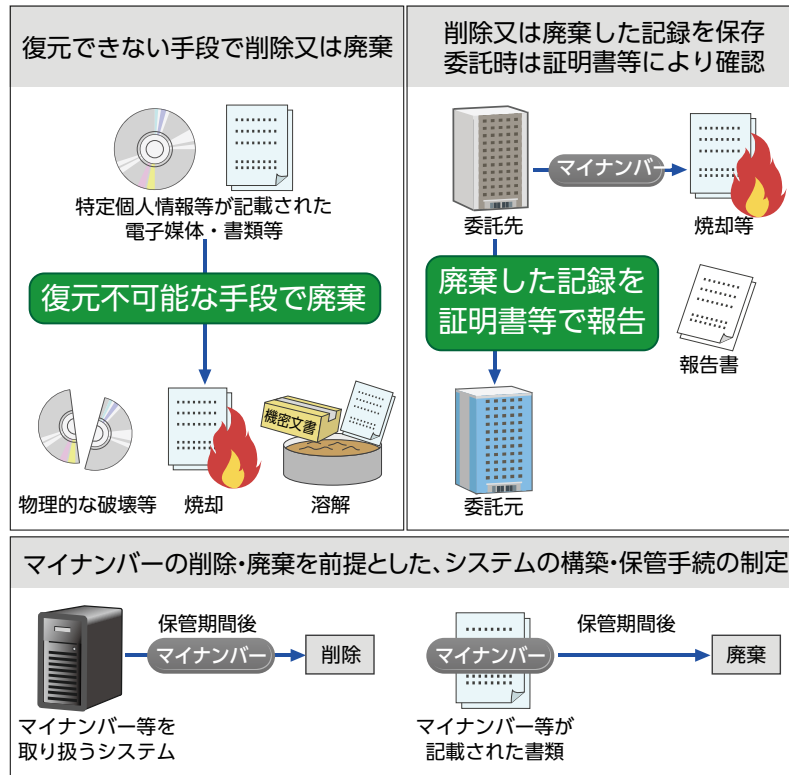
特定個人情報等が記録された電子媒体または書類等を持ち出す場合、容易にマイナンバーが判明しない措置の実施、追跡可能な移送手段の利用等、安全な方策を講じます。

「持ち出し」とは、特定個人情報等を、管理区域または取扱区域の外へ移動させることをいい、事業所内での移動であっても、紛失・盗難等に注意する必要があります。



d. マイナンバーの削除、機器および電子媒体等の廃棄

個人番号利用事務を行う必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合には、マイナンバーをできるだけ速やかに、復元できない手段で削除または廃棄します。マイナンバーもしくは特定個人情報ファイルを削除した場合、または電子媒体等を廃棄した場合には、その記録を保存します。また、これらの作業を委託する場合には、委託先が確実に削除または廃棄したことについて、証明書等により確認します。



● F 技術的安全管理措置

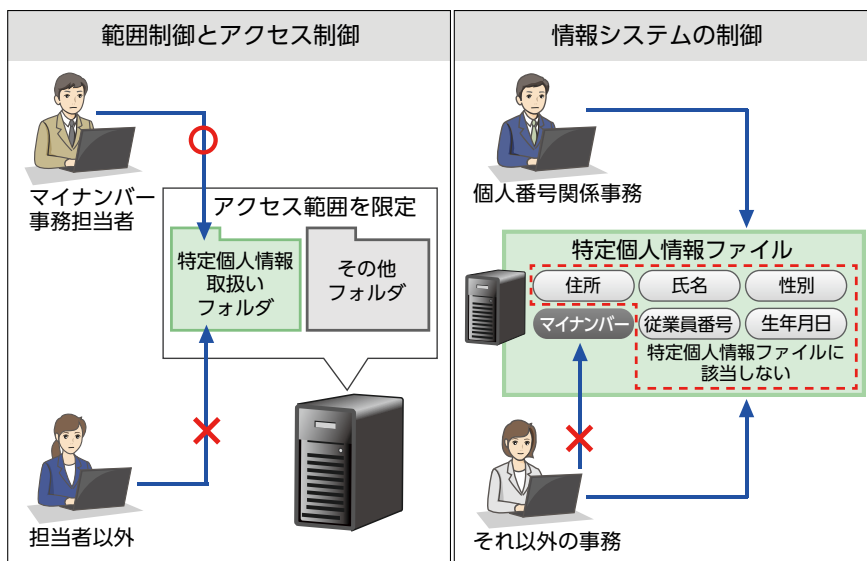
特定個人情報等の適正な取扱いのために、技術的安全管理措置を講じなければなりません。

a. アクセス制御

情報システムを使用して個人番号利用事務を行う場合、事務取扱担当者および当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う必要があります。

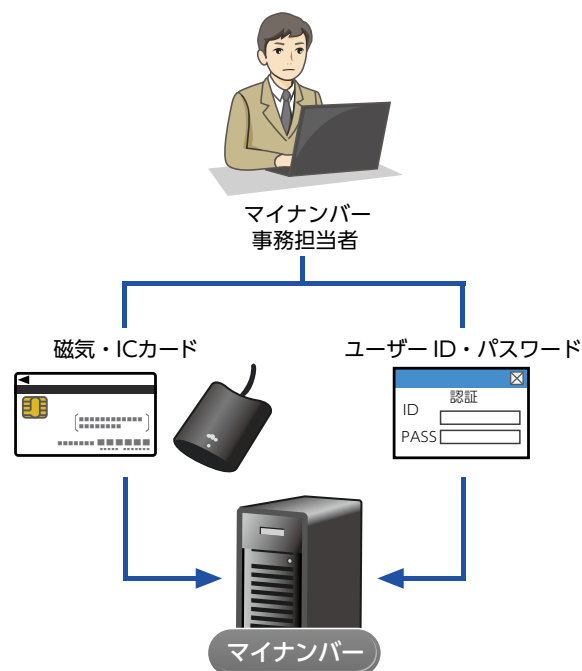
マイナンバーを管理するデータベースは、同一筐体内、かつ、同一データベース内で管理することはできませんが、個人番号関係事務と関係のない事務で利用することのないようにアクセス制限等を行う必要があります。

なお、個人番号関係事務以外の事務において、マイナンバーにアクセスできないよう適切にアクセス制御を行えば、その個人番号関係事務以外の事務においては、当該データベースは特定個人情報ファイルに該当しません。



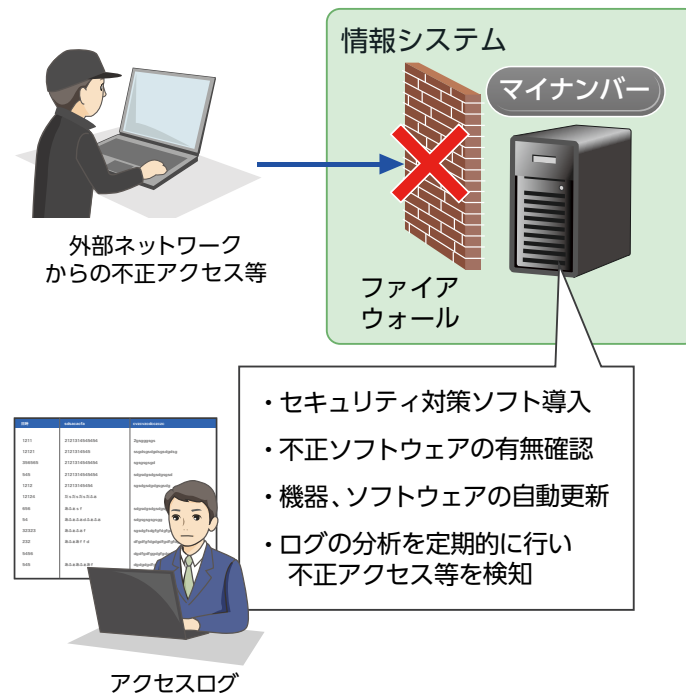
b. アクセス者の識別と認証

特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権がある者であることを識別し、その結果に基づき認証させます。



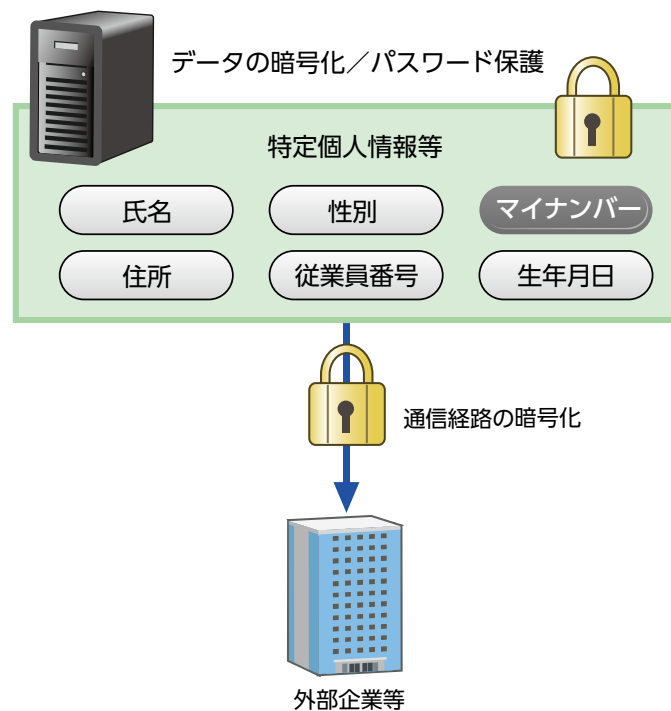
c. 外部からの不正アクセス等の防止

情報システムを外部からの不正アクセスまたは不正ソフトウェアから保護する仕組みを導入し、適切に運用します。



d. 情報漏えい等の防止

特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講じます。



3 各種報告事務にマイナンバーを付与

源泉徴収票・支払調書などにマイナンバーを記載し、行政機関などに提出します。システムで源泉徴収票を出力している場合は、源泉徴収票にマイナンバーが記載できるようにシステムを改修する必要があります。

