

# マイナナンバー チェックリスト

## 1. 個人番号を受け取る必要のある事務の洗い出し

- 個人番号受け取りが必要な対象者と事務洗い出しを行いましたか？
  - ・【参照】安全管理措置ガイドライン1. A
  - ・役員・従業員のほか、報酬支払先、株主などの個人番号の受け取りも必要。

## 2. 取り扱う特定個人情報等の洗い出し

- 上記1により洗い出した個人番号を受け取る事務に関して、取り扱う特定個人情報(個人番号を含む個人情報)等を洗い出しましたか？
  - ・【参照】安全管理措置ガイドライン1. B

## 3. 事務取扱担当者の選任

- 個人番号を取り扱う事務取扱担当者を選任しましたか？
  - ・【参照】安全管理措置ガイドライン1. C
    - ✓ 担当部署・責任者の設置も必要となります。

## 4. 本人確認の方法

- 従業員等から個人番号を受け取る際の本人確認の方法について、手続方法を定めましたか？
  - ・【参照】番号法16条

## 5. 個人番号・特定個人情報の記録・保存方法

- 個人番号・特定個人情報の記録・保存方法を定めましたか？
  - ・例：書類、システム上の電子ファイル

## 6. 委託先の選定(個人情報利用事務等に関して外部委託をする場合)

### □ システムベンダー等の委託先を選定しましたか？

- ✓ 特定個人情報ガイドライン第4-2-(1). 1. Bに基づく、委託先の選定基準に合致する必要があります。

## 7. 社内規程の整備

### □ 以下の社内規程を整備しましたか？

- 基本方針の策定
  - ✓ 【参照】安全管理措置ガイドライン(既存の個人情報保護基本方針等への追加でも可)
- 取扱規程等の策定
  - ✓ 【参照】安全管理措置ガイドライン(既存の個人情報保護規程への追加でも可)
- 個人情報の利用目的の特定・通知等
  - ✓ 【参照】個人情報保護法15条、18条(就業規則への追加などの措置が必要です)

## 8. 委託契約書の整備(個人情報利用事務等に関し外部委託をする場合)

### □ 特定個人情報ガイドラインの要件を満たす委託契約書を整備しましたか？

- ✓ 既存の委託契約書が要件を満たす場合、あるいは変更する場合は、それで可。

## 9. 組織的安全管理措置

### □ 組織体制の整備

- ✓ 個人番号や特定個人情報の安全管理を行えるよう組織体制を変更、構築しましたか？

- 中小規模事業者の場合

- 事務取扱担当者が複数いる場合、責任者と事務取扱担当者を区分していますか？

### □ 取扱規程等に基づく運用

- ✓ 取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する体制をとっていますか？

- 中小規模事業者の場合

- 特定個人情報等の取扱状況の分かる記録を保存する体制をとっていますか？

### □ 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方法を用意しましたか？

- 中小規模事業者の場合

- 上記②に同じ。

### □ 情報漏えい等に対応する体制の整備

- ✓ 情報漏えい等の発生又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体制をとっていますか？

- 中小規模事業者の場合

- 情報漏えい等の事案の発生等に備え、従業員から上司や責任者に対する報告・連絡体制等をあらかじめ確認しておくようにしていますか？

### □ 取扱状況の把握及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、安全管理方法の評価、見直し、及び改善に取り組むための体制をとっていますか？

## 10. 人的安全管理措置

### □ 事務取扱担当者の監督

- ✓ 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、事務取扱担当者に対して必要かつ適切な監督を行う体制をとっているか

### □ 事務取扱担当者の教育

- ✓ 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体制をとっているか

## 11. 物理的安全管理措置

### □ 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（以下「管理区域」）、及び特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」）を明確にし、物理的な安全管理を行っているか

### □ 機器及び電子媒体等の盗難等の防止

- ✓ 管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理を行っているか

### □ 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又は書類等を持ち出す場合、容易に個人番号が判明しない対策の実施、追跡可能な移送手段の利用等、安全対策を行っているか。「持出し」とは、特定個人情報等を管理区域又は取扱区域の外へ移動させることで、事業所内での移動等であっても紛失・盗難等に注意する必要があります。

#### ➤ 中小規模事業者の場合

- 特定個人情報等が記録された電子媒体又は書類等を持ち出す場合、パスワードの設定、封筒に封入しカバンに入れて搬送する等、紛失・盗難等を防ぐための安全対策を行っているか

### □ 個人番号の削除、機器及び電子媒体等の廃棄個人番号もしくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する体制をとっていますか？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又は廃棄したことについて、証明書等により確認する体制をとっていますか？

#### ➤ 中小規模事業者の場合

- 特定個人情報等を削除・廃棄したことを、責任ある立場の者が確認する体制をとっていますか？

## 12. 技術的安全管理措置

### □ アクセス制御

- ✓ 情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者、及び当該事務で取り扱う特定個人情報ファイルの範囲の限定のため、適切なアクセス制御を行うようにしているか？

（独立のデータベース構築は必ずしも必要ではありませんが、個人番号を同一筐体内、かつ、同一データベース内で管理する場合、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、アクセス制御等を行う必要があります。）

### □ 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を有する者であることを、識別した結果に基づき認証することとしていますか？

➤ 中小規模事業者の場合

- 特定個人情報等を取り扱う機器を特定し、その機器を取り扱う事務取扱担当者を限定していますか？
- 機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、情報システムを取り扱う事務取扱担当者を限定していますか？

### □ 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、又は不正ソフトウェアから保護する仕組みを導入し、適切に運用していますか？

➤ 中小規模事業者の場合

- 上記②に同じ。

### □ 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対策を行っていますか？