（別添）特定個人情報に関する安全管理措置

（事業者編）

【目次】

要点

○　番号法における安全管理措置の考え方

番号法は、個人番号を利用できる事務の範囲、特定個人情報ファイルを作成できる範囲、特定個人情報を収集・保管・提供できる範囲等を制限している。したがって、事業者は、個人番号及び特定個人情報（以下「特定個人情報等」という。）の漏えい、滅失又は毀損（以下「情報漏えい等」という。）の防止等のための安全管理措置の検討に当たり、次に掲げる事項を明確にすることが重要である。

A　個人番号を取り扱う事務の範囲
B　特定個人情報等の範囲
C　特定個人情報等を取り扱う事務に従事する従業者(注)（以下「事務取扱担当者」という。）

（注）「従業者」とは、事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいう。具体的には、従業員のほか、取締役、監査役、理事、監事、派遣社員等を含む。

○　安全管理措置の検討手順

事業者は、特定個人情報等の適正な取扱いに関する安全管理措置について、次のような手順で検討を行う必要がある。→1

A　個人番号を取り扱う事務の範囲の明確化
B　特定個人情報等の範囲の明確化
C　事務取扱担当者の明確化
D　特定個人情報等の安全管理措置に関する基本方針（以下「基本方針」という。）の策定
E　取扱規程等の策定

○　講ずべき安全管理措置の内容

事業者は、安全管理措置の検討に当たり、番号法及び個人情報保護法等関係法令並びに本ガイドライン及び主務大臣のガイドライン等を遵守しなければならない。

本ガイドラインは、次に掲げる項目に沿って記述している。→2

A　基本方針の策定
B　取扱規程等の策定
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

1 安全管理措置の検討手順

事業者は、特定個人情報等の取扱いを検討するに当たって、個人番号を取り扱う事務の範囲及び特定個人情報等の範囲を明確にした上で、事務取扱担当者を明確にしておく必要がある。

これらを踏まえ、特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。

また、取扱規程等を策定し、特定個人情報等を取り扱う体制の整備及び情報システムの改修等を行う必要がある。

事業者は、特定個人情報等の取扱いに関する安全管理措置について、次のような手順で検討を行う必要がある。

A 個人番号を取り扱う事務の範囲の明確化

事業者は、個人番号関係事務又は個人番号利用事務の範囲を明確にしておかなければならない。→ガイドライン第４－１－(1)1A参照

B 特定個人情報等の範囲の明確化

事業者は、Aで明確化した事務において取り扱う特定個人情報等の範囲を明確にしておかなければならない(注)。

(注) 特定個人情報等の範囲を明確にするとは、事務において使用される個人番号及び個人番号と関連付けて管理される個人情報（氏名、生年月日等）の範囲を明確にすることをいう。

C 事務取扱担当者の明確化

事業者は、Aで明確化した事務に従事する事務取扱担当者を明確にしておかなければならない。

D 基本方針の策定

特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。→2A参照

E 取扱規程等の策定

事業者は、A～Cで明確化した事務における特定個人情報等の適正な取扱いを確保するために、取扱規程等を策定しなければならない。→2B参照

2 講ずべき安全管理措置の内容

本セクション2においては、特定個人情報等の保護のために必要な安全管理措置について本文で示し、その具体的な手法の例示及び中小規模事業者における対応方法を記述している。

それぞれの項目の位置付けを次に掲げる。安全管理措置の検討に当たっては、番号法及び個人情報保護法等関係法令並びに本ガイドライン及び主務大臣のガイドライン等を遵守しなければならない。

・　手法の例示：具体的な手法を例示したものである。本例示は、これに限定する趣旨で記載したものではなく、事業者の規模及び特定個人情報等を取り扱う事務の特性等により、適切な手法を採用することが重要である。

・　中小規模事業者(注)における対応方法：中小規模事業者については、事務で取り扱う個人番号の数量が少なく、また、特定個人情報等を取り扱う従業者が限定的であること等から、特例的な対応方法を示すものである。

なお、中小規模事業者が、手法の例示に記載した手法を採用することは、より望ましい対応である。

（注）「中小規模事業者」とは、事業者のうち従業員の数が100人以下の事業者であって、次に掲げる事業者を除く事業者をいう。

- 個人番号利用事務実施者
- 委託に基づいて個人番号関係事務又は個人番号利用事務を業務として行う事業者
- 金融分野（金融庁作成の「金融分野における個人情報保護に関するガイドライン」第1条第1項に定義される金融分野）の事業者
- 個人情報取扱事業者

A 基本方針の策定

特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。

≪手法の例示≫

＊　基本方針に定める項目としては、次に掲げるものが挙げられる。

- 事業者の名称
- 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
- 質問及び苦情処理の窓口　等

B　取扱規程等の策定

1 A～Cで明確化した事務において事務の流れを整理し、特定個人情報等の具体的な取扱いを定める取扱規程等を策定しなければならない。

≪手法の例示≫

＊　取扱規程等は、次に掲げる管理段階ごとに、取扱方法、責任者・事務取扱担当者及びその任務等について定めることが考えられる。具体的に定める事項については、C～Fに記述する安全管理措置を織り込むことが重要である。

① 取得する段階
② 利用を行う段階
③ 保存する段階
④ 提供を行う段階
⑤ 削除・廃棄を行う段階

＊　源泉徴収票等を作成する事務の場合、例えば、次のような事務フローに即して、手続を明確にしておくことが重要である。

① 従業員等から提出された書類等を取りまとめる方法
② 取りまとめた書類等の源泉徴収票等の作成部署への移動方法
③ 情報システムへの個人番号を含むデータ入力方法
④ 源泉徴収票等の作成方法
⑤ 源泉徴収票等の行政機関等への提出方法
⑥ 源泉徴収票等の本人への交付方法
⑦ 源泉徴収票等の控え、従業員等から提出された書類及び情報システムで取り扱うファイル等の保存方法
⑧ 法定保存期間を経過した源泉徴収票等の控え等の廃棄・削除方法　等

【中小規模事業者における対応方法】

○　特定個人情報等の取扱い等を明確化する。
○　事務取扱担当者が変更となった場合、確実な引継ぎを行い、責任ある立場の者が確認する。

C　組織的安全管理措置

事業者は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。

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する。

≪手法の例示≫

＊　組織体制として整備する項目は、次に掲げるものが挙げられる。

・　事務における責任者の設置及び責任の明確化
・　事務取扱担当者の明確化及びその役割の明確化
・　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又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又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
・　特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化

【中小規模事業者における対応方法】

○　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することが望ましい。

b　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。

≪手法の例示≫

＊　記録する項目としては、次に掲げるものが挙げられる。
・　特定個人情報ファイルの利用・出力状況の記録
・　書類・媒体等の持出しの記録
・　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

【中小規模事業者における対応方法】

○　特定個人情報等の取扱状況の分かる記録を保存する。

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する。

なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。

≪手法の例示≫

＊　取扱状況を確認するための記録等としては、次に掲げるものが挙げられる。
・　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

【中小規模事業者における対応方法】

○　特定個人情報等の取扱状況の分かる記録を保存する。

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整備する。

情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。

≪手法の例示≫

＊　情報漏えい等の事案の発生時に、次のような対応を行うことを念頭に、体制を整備することが考えられる。
・　事実関係の調査及び原因の究明
・　影響を受ける可能性のある本人への連絡
・　委員会及び主務大臣等への報告
・　再発防止策の検討及び決定
・　事実関係及び再発防止策等の公表

【中小規模事業者における対応方法】

○　情報漏えい等の事案の発生等に備え、従業者から責任ある立場の者に対する報告連絡体制等をあらかじめ確認しておく。

e　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、安全管理措置の評価、見直し及び改善に取り組む。

≪手法の例示≫

＊　特定個人情報等の取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。
＊　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る。

【中小規模事業者における対応方法】

○　責任ある立場の者が、特定個人情報等の取扱状況について、定期的に点検を行う。

D　人的安全管理措置

事業者は、特定個人情報等の適正な取扱いのために、次に掲げる人的安全管理措置を講じなければならない。

a　事務取扱担当者の監督

事業者は、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。

b　事務取扱担当者の教育

事業者は、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。

≪手法の例示≫

＊　特定個人情報等の取扱いに関する留意事項等について、従業者に定期的な研修等を行う。

＊　特定個人情報等についての秘密保持に関する事項を就業規則等に盛り込むことが考えられる。

E　物理的安全管理措置

事業者は、特定個人情報等の適正な取扱いのために、次に掲げる物理的安全管理措置を講じなければならない。

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（以下「管理区域」という。）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」という。）を明確にし、物理的な安全管理措置を講ずる。

≪手法の例示≫

＊　管理区域に関する物理的安全管理措置としては、入退室管理及び管理区域へ持ち込む機器等の制限等が考えられる。

＊　入退室管理方法としては、ＩＣカード、ナンバーキー等による入退室管理システムの設置等が考えられる。

＊　取扱区域に関する物理的安全管理措置としては、壁又は間仕切り等の設置及び座席配置の工夫等が考えられる。

b　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、物理的な安全管理措置を講ずる。

≪手法の例示≫

＊　特定個人情報等を取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット・書庫等に保管する。

＊　特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定すること等が考えられる。

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、安全な方策を講ずる。

「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をいい、事業所内での移動等であっても、紛失・盗難等に留意する必要がある。

≪手法の例示≫

＊　特定個人情報等が記録された電子媒体を安全に持ち出す方法としては、持出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用等が考えられる。ただし、行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う。

＊　特定個人情報等が記載された書類等を安全に持ち出す方法としては、封緘、目隠しシールの貼付を行うこと等が考えられる。

【中小規模事業者における対応方法】

○　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。

d　個人番号の削除、機器及び電子媒体等の廃棄

個人番号関係事務又は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、個人番号をできるだけ速やかに復元できない手段で削除又は廃棄する。

→ガイドライン第４－３－(3)Ｂ「保管制限と廃棄」参照

個人番号若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。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。

≪手法の例示≫

＊　特定個人情報等が記載された書類等を廃棄する場合、焼却又は溶解等の復元

不可能な手段を採用する。

＊　特定個人情報等が記録された機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用する。

＊　特定個人情報ファイル中の個人番号又は一部の特定個人情報等を削除する場合、容易に復元できない手段を採用する。

＊　特定個人情報等を取り扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提とした情報システムを構築する。

＊　個人番号が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定める。

【中小規模事業者における対応方法】

○　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。

F　技術的安全管理措置

事業者は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。

a　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を限定するために、適切なアクセス制御を行う。

≪手法の例示≫

＊　アクセス制御を行う方法としては、次に掲げるものが挙げられる。

- 個人番号と紐付けてアクセスできる情報の範囲をアクセス制御により限定する。
- 特定個人情報ファイルを取り扱う情報システムを、アクセス制御により限定する。
- ユーザーＩＤに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。

【中小規模事業者における対応方法】

○　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することが望ましい。

○　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することが望ましい。

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。

≪手法の例示≫

＊　事務取扱担当者の識別方法としては、ユーザーＩＤ、パスワード、磁気・ＩＣカード等が考えられる。

【中小規模事業者における対応方法】

○　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することが望ましい。

○　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することが望ましい。

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、適切に運用する。

≪手法の例示≫

＊　情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。

＊　情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。

＊　導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。

＊　機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。

＊　ログ等の分析を定期的に行い、不正アクセス等を検知する。

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ずる。

≪手法の例示≫

＊　通信経路における情報漏えい等の防止策としては、通信経路の暗号化等が考えられる。

＊　情報システム内に保存されている特定個人情報等の情報漏えい等の防止策としては、データの暗号化又はパスワードによる保護等が考えられる。

（巻末資料）

個人番号の取得から廃棄までのプロセスにおける本ガイドラインの適用（大要）

区分	個人情報保護法	本ガイドライン（番号法該当条文）
取得	・利用目的の特定（第 15 条） ・適正な取得（第 17 条） ・利用目的の通知等（第 18 条）	・第４－３－(1)　個人番号の提供の要求（第 14 条）…求める根拠 ・第４－３－(2)　個人番号の提供の求めの制限、特定個人情報の提供制限（第 15 条、第 19 条、第 29 条第 3 項） ・第４－３－(3)　収集・保管制限（第 20 条） ・第４－３－(4)　本人確認（第 16 条）
安全管理措置等	・安全管理措置（第 20 条） ・従業者の監督（第 21 条） ・委託先の監督（第 22 条）	・第４－２－(1)　委託の取扱い（第 10 条、第 11 条） ・第４－２－(2)　安全管理措置（第 12 条、第 33 条、第 34 条） ・（別添）特定個人情報に関する安全管理措置（事業者編）
保管	・正確性の確保（第 19 条） ・保有個人データに関する事項の公表等（第 24 条）	・第４－３－(3)　収集・保管制限（第 20 条）
利用	・利用目的による制限（第 16 条） ※番号法による読替及び適用除外あり ・利用目的の通知等（第 18 条第 3 項）	・第４－１－(1)　個人番号の利用制限（第 9 条、第 29 条第 3 項、第 32 条） ・第４－１－(2)　特定個人情報ファイルの作成の制限（第 28 条）
提供	・第三者提供の制限（第 23 条） ※番号法では適用除外	・第４－３－(2)　個人番号の提供の求めの制限、特定個人情報の提供制限（第 15 条、第 19 条、第 29 条第 3 項）
開示 訂正 利用停止	・開示、訂正等、利用停止等（第 25 条～第 30 条） ※利用停止等（第 27 条）は、番号法による読替あり	・第４－４　第三者提供の停止に関する取扱い（第 29 条第 3 項）
廃棄	・該当条文なし	・第４－３－(3)　収集・保管制限（第 20 条）

注：この表は、各プロセスにおける個人情報保護法の適用条文と本ガイドラインの適用部分のイメージを記載したものです。
よって、各プロセスに正確に適用される条文とは、若干異なりますので、ご留意願います。