

○個人情報保護委員会告示第 号

行政手続における特定の個人を識別するための番号の利用等に関する法律等の一部を改正する法律（令和五年法律第四十八号）の一部の施行に伴い、及び関係法令の規定に基づき、特定個人情報の適正な取扱いに関するガイドライン（事業者編）（平成二十六年特定個人情報保護委員会告示第五号）の一部を次のように改正する。

令和 年 月 日 個人情報保護委員会委員長 手塚 悟

次の表により、改正前欄に掲げる規定の傍線を付した部分をこれに順次対応する改正後欄に掲げる規定の傍線を付した部分のように改め、改正前欄及び改正後欄に対応して掲げるその標記部分に二重傍線を付した規定（以下「対象規定」という。）は、改正前欄に掲げる対象規定を改正後欄に掲げる対象規定として移動し、改正前欄に掲げる対象規定で改正後欄にこれに対応するものを掲げていないものは、これを削り、改正後欄に掲げる対象規定で改正前欄にこれに対応するものを掲げていないものは、これを加える。

改正後	改正前
目次 [略] [第1～第4 略] (別添1) 特定個人情報に関する安全管理措置 (事業者編) 【目次】 要点 1 [略] 2 [A・B 略] C 組織的安全管理措置 [a・b 略] [削除] c 漏えい等事案に対応する体制の整備 d 取扱状況の把握及び安全管理措置の見直し	目次 [同左] [第1～第4 同左] (別添1) 特定個人情報に関する安全管理措置 (事業者編) 【目次】 要点 1 [同左] 2 [A・B 同左] C 組織的安全管理措置 [a・b 同左] c 取扱状況を確認する手段の整備 d 漏えい等事案に対応する体制の整備 e 取扱状況の把握及び安全管理措置の見直し

[D・E 略]

F 技術的安全管理措置

[a～d 略]

e 不正アクセス等の検知等

G [略]

要点

[略]

1 [略]

2 講ずべき安全管理措置の内容

[略]

A [略]

B 取扱規程等の策定

[略]

《手法の例示》

* [略]

* 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 [略]

② [略]

③ [略]

④ [略]

⑤ [略]

⑥ [略]

⑦ 法定保存期間を経過した源泉徴収票等の控え等の廃棄・

[D・E 同左]

F 技術的安全管理措置

[a～d 同左]

[新設]

G [同左]

要点

[同左]

1 [同左]

2 講ずべき安全管理措置の内容

[同左]

A [同左]

B 取扱規程等の策定

[同左]

《手法の例示》

* [同左]

* 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 [同左]

② [同左]

③ [同左]

④ [同左]

⑤ [同左]

⑥ [同左]

⑦ 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

- ⑧ 従業員等から提出された書類等の複製等を作成している
場合に当該複製等の廃棄・削除方法 等

* [略]

【中小規模事業者における対応方法】

[略]

C 組織的安全管理措置

[略]

a 組織体制の整備

[略]

《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並びに責任部署の設置及び役割の明確化
 - ・ [略]
 - ・ [略]
 - ・ 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及び責任部署への報告連絡体制
 - ・ 漏えい等事案の発生又は兆候を把握した場合の従業員から責任者、責任部署等への報告連絡体制
 - ・ [略]
 - ・ [略]

【中小規模事業者における対応方法】

[略]

削除方法 等

[新設]

* [同左]

【中小規模事業者における対応方法】

[同左]

C 組織的安全管理措置

[同左]

a 組織体制の整備

[同左]

《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
 - ・ [同左]
 - ・ [同左]
 - ・ 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
 - ・ 漏えい等事案の発生又は兆候を把握した場合の従業員から責任者等への報告連絡体制
 - ・ [同左]
 - ・ [同左]

【中小規模事業者における対応方法】

[同左]

b 取扱規程等に基づく運用

取扱規程等に基づく運用を行うとともに、特定個人情報等の利用状況等を記録し、特定個人情報等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》

＊ 取扱規程等を明確化し、従業者に周知する。

＊ 取扱規程等に従って特定個人情報等が取り扱われていることを、責任者又は責任部署が確認する。例えば、次に掲げる項目を記録し、取扱規程等と照らし合わせることが考えられる。

- ・ [略]
- ・ [略]
- ・ [略]
- ・ [略]
- ・ [略]

＊ システムログその他の特定個人情報等の取扱いに係る記録等においては、例えば次に掲げるものをあらかじめ明確化しておくことにより、特定個人情報等の取扱状況を把握可能とすることが考えられる。

- ・ 特定個人情報ファイルの種類、名称
- ・ 特定個人情報等を取り扱う部署・当該部署の責任者
- ・ 利用目的
- ・ 削除・廃棄状況
- ・ アクセス権を有する者 等

b 取扱規程等に基づく運用

取扱規程等に基づく運用を行うとともに、その状況を確認するため、特定個人情報等の利用状況等を記録する。

《手法の例示》

[新設]

＊ 記録する項目としては、次に掲げるものが挙げられる。

- ・ [同左]
- ・ [同左]
- ・ [同左]
- ・ [同左]
- ・ [同左]

[新設]

【中小規模事業者における対応方法】

[略]

[削除]

c 漏えい等事案に対応する体制の整備

[略]

《手法の例示》

- * 漏えい等事案の発生時に、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。
 - ・ [略]
 - ・ [略]
 - ・ 委員会等関係機関への報告

【中小規模事業者における対応方法】

[同左]

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 漏えい等事案に対応する体制の整備

[同左]

《手法の例示》

- * 漏えい等事案の発生時に、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。
 - ・ [同左]
 - ・ [同左]
 - ・ 委員会への報告

- ・ [略]
- ・ [略]

【中小規模事業者における対応方法】

[略]

d 取扱状況の把握及び安全管理措置の見直し

[略]

《手法の例示》

* 特定個人情報等の取扱状況について、上記 b による把握に加えて、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ことが考えられる。

* [略]

* 特定個人情報等の取扱状況、情報技術の進歩等を踏まえて、講じた安全管理措置について、定期的に評価及び見直しを行い、必要に応じて改善をすることが考えられる。

【中小規模事業者における対応方法】

[略]

D 人的安全管理措置

[略]

a [略]

b 事務取扱担当者の教育

[略]

《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、従業者に定期的に（少なくとも年 1 回程度）適切な内容の研修等を行うことが考えられる。

- ・ [同左]
- ・ [同左]

【中小規模事業者における対応方法】

[同左]

e 取扱状況の把握及び安全管理措置の見直し

[同左]

《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ことが考えられる。

* [同左]

[新設]

【中小規模事業者における対応方法】

[同左]

D 人的安全管理措置

[同左]

a [同左]

b 事務取扱担当者の教育

[同左]

《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ことが考えられる。

＊ 従業者に対する定期的な研修等の内容、実施方法等を評価、
見直し及び改善することが考えられる。

＊ [略]

E 物理的安全管理措置

[略]

[a ～ c 略]

d 個人番号の削除、機器及び電子媒体等の廃棄

[略]

《手法の例示》

＊ [略]

＊ 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、暗号化消去、物
理的な破壊等により、復元不可能な手段を採用することが考え
られる。

＊ [略]

＊ [略]

＊ [略]

【中小規模事業者における対応方法】

[略]

F 技術的安全管理措置

[略]

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
等の範囲を限定するために、適切なアクセス制御を行う。

[新設]

＊ [同左]

E 物理的安全管理措置

[同左]

[a ～ c 同左]

d 個人番号の削除、機器及び電子媒体等の廃棄

[同左]

《手法の例示》

＊ [同左]

＊ 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ことが考えられる。

＊ [同左]

＊ [同左]

＊ [同左]

【中小規模事業者における対応方法】

[同左]

F 技術的安全管理措置

[同左]

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。
 - ・ 特定個人情報等を取り扱うことのできる情報システムを限定する。
 - ・ 特定個人情報等を取り扱う情報システムへのアクセスを最小化する。例えば、事前に許可した特定の I P アドレスからのみに限定する方法が考えられる。
 - ・ 特定個人情報等を取り扱う情報システムを使用できる事務取扱担当者については、ユーザー I D に付与するアクセス権限を最小化することにより限定する。
 - ・ 特権アカウントを割り当てる従業者、利用する端末、利用する場面等を最小限に限定する。
 - ・ 組織体制に変更が生じた場合（例えば、人事異動、従業者の退職等）等に、アクセス権限の変更を適切に行う。
 - ・ アクセス制御が適切に行われているか確認する。例えば、アクセス権限について定期的に監査する、アクセス権限の棚卸しを行う等の方法が考えられる。
 - ・ 組織内外からのアクセスについて、アクセス要求ごとにアクセス元の場所、アクセス時間、デバイスのセキュリティ状態等の動的コンテキストを評価し、リスクに応じてアクセスの可否を判断する仕組みを導入する。

【中小規模事業者における対応方法】

[略]

b アクセス者の識別と認証

《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。
 - ・ 特定個人情報ファイルを取り扱うことのできる情報システム端末等を限定する。
 - ・ 各情報システムにおいて、アクセスすることのできる特定個人情報ファイルを限定する。
 - ・ ユーザー I D 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。

[新設]

[新設]

[新設]

[新設]

【中小規模事業者における対応方法】

[同左]

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を使用する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 I D、パスワード、磁気・ I C カード、指紋認証・静脈認証・顔認証等が考えられる。

＊ ユーザー I D・パスワードを利用する場合には、同一のユーザー I D・パスワードの使い回しの原則禁止及び類似パスワードの使い回しの制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した I Dの停止等を行う。

＊ 特定個人情報等へのアクセス権限を有する者が使用できる端末又はアドレス等についての識別と認証を実施する。例えば、I P アドレス認証、電子証明書等の方法が考えられる。

＊ 組織外ネットワークからのアクセスや、管理者権限でのアクセス、重要な特定個人情報等へのアクセスにおいては、識別・認証手法を複数組み合わせる多要素認証（フィッシングに耐性のあるものを含む。）を導入する。

＊ 事務取扱担当者以外の者を適切に識別・認証する方法を採用する。例えば、同一及び類似パスワードの使い回しをしないよう周知、最低パスワード文字数の設定、一定回数以上ログインに失敗した I Dの停止、多要素認証（フィッシングに耐性のあるものを含む。）の導入等が考えられる。

【中小規模事業者における対応方法】

[略]

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 I D、パスワード、磁気・ I C カード等が考えられる。

[新設]

[新設]

[新設]

[新設]

【中小規模事業者における対応方法】

[同左]

c 外部からの不正アクセス等の防止

[略]

《手法の例示》

- * 特定個人情報等を取り扱う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ことが考えられる。
- * 特定個人情報等を取り扱う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）を導入して適切に運用（パターンファイルや修正ソフトウェアの更新確認等を行うことを含む。）し、不正ソフトウェアの有無を確認することが考えられる。
- * 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、端末、サーバ、VPN機器等のオペレーティングシステム、ミドルウェア、アプリケーション等に対するセキュリティ対策用修正ソフトウェアの適用により、ソフトウェア等を最新状態とすることが考えられる。

[削除]

※ 事業者において許可していないソフトウェア等の導入を防止する。例えば、ソフトウェアの導入時の確認のほか、定期的な監査などの方法が考えられる。

※ 組織が許可し、セキュリティ基準を満たしたデバイスからのみ特定個人情報等へのアクセスを許可する。

d 漏えい等の防止

[略]

c 外部からの不正アクセス等の防止

[同左]

《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ことが考えられる。
- * 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）を導入し、不正ソフトウェアの有無を確認することが考えられる。
- * 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ことが考えられる。

※ 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ことが考えられる。

[新設]

[新設]

d 漏えい等の防止

[同左]

《手法の例示》

＊ 通信経路における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。例えば、インターネットや無線LAN等による特定個人情報等の送信（例えば、本人又は従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）時に、特定個人情報等の暗号化等の秘匿化（例えば、SSL/TLS、S/MIME等）を行うなどの方法が考えられる。

＊ [略]

e 不正アクセス等の検知等

特定個人情報等を取り扱う情報システムに不正アクセス等が発生した場合に早期に検知等するための措置を平時から講じ、組織内ネットワークにおける被害拡大を防止できるよう適切に運用する。

《手法の例示》

＊ 特定個人情報等を取り扱う情報システムの使用状況、特定個人情報等へのアクセス状況、特定個人情報等を取り扱う情報システムへの外部からのアクセス状況等のログ（例えば、認証ログ、アクセスログ、操作ログ、通信ログ等）等を一定の期間保管する。

＊ 当該ログ等の漏えい、滅失及び毀損並びに改ざん、不正消去等からの適切な保護を行う。

＊ 当該ログ等の定期的な分析により、不正アクセス等の発生又は兆候を早期に検知する。

＊ 不正アクセス等の発生又は兆候を早期に検知等するための仕組み（例えば、IDS/IPS、EDR等）等を導入する。

《手法の例示》

＊ 通信経路における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。

＊ [同左]

[新設]

＊ 不正アクセス等が発生した場合でも特定個人情報等を取り扱う情報システムの被害が広がらないよう、必要な対策を講ずる。例えば、侵害を受けた又はそのおそれがある情報システムの停止・隔離、アカウントの無効化などの方法が考えられる。その他必要な対策については、F 技術的安全管理措置 a から d の手法の例示も参照されたい。 【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情報システムの使用状況、特定個人情報等へのアクセス状況、特定個人情報等を取り扱う情報システムへの外部からのアクセス状況等のログ等を一定の期間保管することが望ましい。 G [略] [（別添 2） 略]	G [同左] [（別添 2） 同左]
備考 表 5 の [] の記載は対応しない。	

監 査

以上を以て、令和九年〇月〇日から施行する。