○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（行政機関等編）（平成二十六年特定個人情報保護委員会告示第六号）の一部を次のように改正する。

令和八年　　月　　日

個人情報保護委員会委員長　手塚　　悟

特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）（平成二十六年特定個人情報保護委員会告示第六号）の一部を次のように改正する。

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 （行政機関等編） **【目次】** 1　［略］ 2 ［**A～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］	**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 （行政機関等編） **【目次】** 1　［同左］ 2 ［**A～E**　同左］ **F　技術的安全管理措置** ［**a～d**　同左］ ［新設］ **G**　［同左］

1　［略］	1　［同左］
2　講ずべき安全管理措置の内容	**2　講ずべき安全管理措置の内容**
［略］	［同左］
A　［略］	**A**　［同左］
B　取扱規程等の見直し等	**B　取扱規程等の見直し等**
［略］	［同左］
≪手法の例示≫	≪手法の例示≫
＊　［略］	＊　［同左］
＊　［略］	＊　［同左］
＊　特定個人情報等を含む書類等の複製等を作成している場合には、当該複製等を削除・廃棄する手続を明確にしておくことが重要である。	［新設］
＊　［略］	＊　［同左］
＊　［略］	＊　［同左］
C　組織的安全管理措置	**C　組織的安全管理措置**
［略］	［同左］
a　［略］	**a**　［同左］
b　取扱規程等に基づく運用	**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、特定個人情報等の取扱状況等を記録し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する。記録については、改ざん、窃取又は不正な削除の防止のために必要な措置を講ずるとともに、分析等を行う。	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し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する。記録については、改ざん、窃取又は不正な削除の防止のために必要な措置を講ずるとともに、分析等を行う。
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、保護責任者等が確認する。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

＊　情報システムの利用状況等の記録に関する分析等としては、ログイン実績、アクセスログ等を定期に及び必要に応じ随時に分析することが考えられる。また、ログと関連する書面の記録を照合し、確認することが考えられる。

→2Ｆｅ参照

ｃ　取扱状況を確認する手段の整備

≪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］

＊　情報システムの利用状況等の記録に関する分析等としては、ログイン実績、アクセスログ等を定期に及び必要に応じ随時に分析することが考えられる。また、ログと関連する書面の記録を照合し、確認することが考えられる。

→2Ｆｃ参照

ｃ　取扱状況を確認する手段の整備

行政機関等は、次に掲げる項目を含めて記録することで、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。

・　［略］
・　［略］
・　［略］
・　［略］
・　［略］

d　漏えい等事案に対応する体制等の整備

［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、体制及び手順等を整備することが考えられる。

・　［略］
・　［略］
・　［略］
・　委員会等関係機関への報告
・　［略］
・　［略］

＊　［略］

e　取扱状況の把握及び安全管理措置の見直し

監査責任者は、特定個人情報等の管理の状況について、定期に及び必要に応じ随時に監査（注）（外部監査及び他部署等による点検を

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。

行政機関等は、次に掲げる項目を含めて記録する。

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。

・　［同左］
・　［同左］
・　［同左］
・　［同左］
・　［同左］

d　漏えい等事案に対応する体制等の整備

［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、体制及び手順等を整備することが考えられる。

・　［同左］
・　［同左］
・　［同左］
・　委員会への報告
・　［同左］
・　［同左］

＊　［同左］

e　取扱状況の把握及び安全管理措置の見直し

監査責任者は、特定個人情報等の管理の状況について、定期に及び必要に応じ随時に監査（注）（外部監査及び他部署等による点検を

含む。）及び点検を行い、その結果を総括責任者に報告する。

総括責任者は、監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずる。

（注）　［略］

D　人的安全管理措置

［略］

a　［略］

b　事務取扱担当者等の教育

総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等の保護に関する意識の高揚を図るための啓発その他必要な教育研修をおおむね一年ごとに行う。

また、特定個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に対し、特定個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修をおおむね一年ごとに行う。

総括責任者は、保護責任者に対し、課室等における特定個人情報等の適切な管理のために必要な教育研修をおおむね一年ごとに行う。

前記教育研修については、教育研修への参加の機会を付与するとともに、研修未受講者に対して再受講の機会を付与する等の必要な措置を講ずる。

なお、サイバーセキュリティの研修については、番号法に基づき特定個人情報ファイルを取り扱う事務に従事する者に対して、次に掲げるところにより、特定個人情報の適正な取扱いを確保するため

含む。）を行い、その結果を総括責任者に報告する。

総括責任者は、監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずる。

（注）　［同左］

D　人的安全管理措置

［同左］

a　［同左］

b　事務取扱担当者等の教育

総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。

また、特定個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に対し、特定個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。

総括責任者は、保護責任者に対し、課室等における特定個人情報等の適切な管理のために必要な教育研修を行う。

前記教育研修については、教育研修への参加の機会を付与するとともに、研修未受講者に対して再受講の機会を付与する等の必要な措置を講ずる。

なお、サイバーセキュリティの研修については、番号法に基づき特定個人情報ファイルを取り扱う事務に従事する者に対して、次に掲げるところにより、特定個人情報の適正な取扱いを確保するため

に必要なサイバーセキュリティ（「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）第２条に規定するサイバーセキュリティをいう。）の確保に関する事項その他の事項に関する研修を行う（番号法第 29 条の２、番号法施行令第 32 条）。	に必要なサイバーセキュリティ（「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）第２条に規定するサイバーセキュリティをいう。）の確保に関する事項その他の事項に関する研修を行う（番号法第 29 条の２、番号法施行令第 32 条）。
・　［略］	・　［同左］
・　［略］	・　［同左］
・　［略］	・　［同左］
c　［略］	**c**　［同左］
E　物理的安全管理措置	**E　物理的安全管理措置**
［略］	［同左］
［**a**～**c**　略］	［**a**～**c**　同左］
d　個人番号の削除、機器及び電子媒体等の廃棄	**d　個人番号の削除、機器及び電子媒体等の廃棄**
［略］	［同左］
≪手法の例示≫	≪手法の例示≫
＊　［略］	＊　［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、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。	＊　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。
＊　［略］	＊　［同左］
＊　［略］	＊　［同左］
F　技術的安全管理措置	**F　技術的安全管理措置**
［略］	［同左］
a　アクセス制御	**a　アクセス制御**
［略］	［同左］

≪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ＩＰ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ＩＤ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。

［削除］

・　［略］

・　［略］

・　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。

・　［略］

・　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

≪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。

・　特定個人情報ファイルへのアクセス権を付与すべき者を最小化する。

・　［同左］

・　［同左］

［新設］

［新設］

［新設］

・　［同左］

［新設］

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。

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ＩＤ、パスワード、磁気・ＩＣ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ＩＤ・パスワードを利用する場合には、同一のユーザーＩＤ・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ＩＤ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、ＩＰ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。

c　不正アクセス等による被害の防止等

［略］

≪手法の例示≫

＊　［略］

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、生体情報等が考えられる。

［新設］

［新設］

［新設］

c　不正アクセス等による被害の防止等

［同左］

≪手法の例示≫

＊　［同左］

＊　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］

［削除］

＊　情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講ずることが考えられる。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］

＊　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。

＊　定期に及び必要に応じ随時にログ等の分析を行い、不正アクセス等を検知することが考えられる。→2Ｃｂ参照

＊　不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用することが考えられる。

＊　情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講ずることが考えられる。

［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。

＊　定期に及び必要に応じ随時にログ等の分析を行い、不正アクセス等を検知する。→2Ｃｂ参照

＊　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］

＊　不正アクセス等の被害に遭った場合であっても、特定個人情報等を取り扱う情報システムの被害を最小化する仕組み（ネットワークの遮断、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等）を導入し、適切に運用する。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。 **G**　［略］ （別添２）　［略］	**G**　［同左］ （別添２）　［同左］
備考　表中の［　］の記載は注記である。	

附　則

この告示は、令和九年〇月〇日から施行する。