

（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 安全管理措置の検討手順	●
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 基本方針の策定	●
E 取扱規程等の策定	●
2 講ずべき安全管理措置の内容	●
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	●
a 組織体制の整備	●
b 取扱規程等に基づく運用	●
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	●
D 人的安全管理措置	●
a 事務取扱担当者の監督	●
b 事務取扱担当者の教育	●
E 物理的安全管理措置	●
a 特定個人情報等を取り扱う区域の管理	●
b 機器及び電子媒体等の盗難等の防止	●
c 電子媒体等の取扱いにおける漏えい等の防止	●
d 個人番号の削除、機器及び電子媒体等の廃棄	●
F 技術的安全管理措置	●
a アクセス制御	●
b アクセス者の識別と認証	●
c 外部からの不正アクセス等の防止	●
d 漏えい等の防止	●
e 不正アクセス等の検知等	●
G 外的環境の把握	●

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（生存する個人のものだけでなく死者のものも含む。）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「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個人情報保護法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
- G 外的環境の把握

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) **1** A 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。→ **2** A 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。→ **2** B 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個人情報保護法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 人以下の事業者をいう。ただし、次に掲げる事業者を除く。

- ・ 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（個人情報保護委員会・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
- ・ その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去 6 月以内のいずれかの日において 5,000 を超える事業者

ここでいう「従業員」とは、「中小企業基本法」（昭和 38 年法律第 154 号）における従業員をいい、「労働基準法」（昭和 22 年法律第 49 号）第 20 条の適用を受ける労働者に相当する者をいう。ただし、同法第 21 条の規定により同法第 20 条の適用が除外されている者は除く。

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 取得段階
 - ② 利用段階
 - ③ 保存段階
 - ④ 提供段階
 - ⑤ 削除・廃棄段階
- * 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
 - 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
- * 特定個人情報等の取扱いにおける人的ミスの発生を防止するため、本人確認及び個人番号の確認の手順、個人番号と個人情報の紐付けの際の複数人による確認（責任者による最終確認を含む。）等の確認の手順等、各管理段階における具体的な手順について、取扱規程等において明確にしておくことが重要である。

【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 **並びに責任部署の設置及び役割の明確化**
 - ・ 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 **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者から責任者、**責任部署**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
 - ・ 特定個人情報等の取扱いにおける人的ミスの発生を防止するための確認体制の整備

【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。

- ・ 特定個人情報ファイルの利用・出力状況の記録
- ・ 書類・媒体等の持ち運びの記録 → 「持ち運び」については、2E c 参照
- ・ 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

＊ 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

【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。

○ 漏えい等事案に対応する体制の整備

漏えい等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。

漏えい等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。（※）

（※）事業者において、漏えい等事案が発生した場合等の対応の詳細については、「（別添2）特定個人情報の漏えい等に関する報告等（事業者編）」を参照のこと。

《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。

- ・ 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通知
- ・ 委員会等関係機関への報告
- ・ 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】

- 漏えい等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。

d 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、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。
- * 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が考えられる。
- * 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】

- 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。
- * 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。
- * 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

特定個人情報ファイルを取り扱う情報システム（サーバ等）を管理する区域（以下「管理区域」という。）を明確にし、物理的な安全管理措置を講ずる。

また、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。）について、事務取扱担当者等以外の者が特定個人情報等を容易に閲覧等できないよう留意する必要がある。

《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。
- ＊ 取扱区域に関しては、間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置等を講ずることが考えられる。

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 電子媒体等の取扱いにおける漏えい等の防止

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運ぶ場合、容易に個人番号が判明しないよう、安全な方策を講ずる。

「持ち運ぶ」とは、特定個人情報等を管理区域又は取扱区域から外へ移動させること又は当該区域の外から当該区域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、特定個人情報等の紛失・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運ぶ方法としては、持ち運ぶデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用、追跡可能な移送手段の利用等が考えられる。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運ぶ方法としては、封緘、目隠しシールの貼付、追跡可能な移送手段の利用等が考えられる。

【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運ぶ場合、パスワードの設定、封筒に封入し鞆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不可能な手段で削除又は廃棄する。

→ガイドライン第4－3－(3)B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、復元不可能な程度に細断可能なシュレッダーの利用、個人番号部分を復元不可能な程度にマスキングすること等の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、**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。
- ＊ 特定個人情報等を取り扱う情報システム又は機器等において、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ことが考えられる。
- ＊ 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ことが考えられる。

【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等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。
 - ・ 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】

- 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。
- * 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ID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】

- 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》

- * 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。
- * 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

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、本人又は従業員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。
- * 情報システム内に保存されている特定個人情報等の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。

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。
- * 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 外的環境の把握

事業者が、外国において特定個人情報等を取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、特定個人情報等の安全の管理のために必要かつ適切な措置を講じなければならない。