

(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	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	取扱規程等の見直し等	●
2	講ずべき安全管理措置の内容	●
A	基本方針の策定	●
B	取扱規程等の見直し等	●
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	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等の整備	●
e	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	事務取扱担当者等の教育	●
c	法令・内部規程違反等に対する厳正な対処	●
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	不正アクセス等による被害の防止等	●
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	●

1 安全管理措置の検討手順

行政機関等は、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、特定個人情報等を取り扱う職員（以下「事務取扱担当者」という。）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、特定個人情報等の安全管理に関する基本方針（以下「基本方針」という。）を策定することが重要である。

行政機関等は、個人情報の保護に関する取扱規程等の見直し等を行い、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。

行政機関等は、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。検討に際し、特定個人情報保護評価を実施した事務については、A～Cを省略し、D～Eを実施することもある。

A 個人番号を取り扱う事務の範囲の明確化

行政機関等は、個人番号利用事務等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

行政機関等は、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

行政機関等は、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 取扱規程等の見直し等

行政機関等は、個人情報の保護に関する取扱規程等の見直し等を行わなければならない。→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を記述している。なお、手法の例示は、これに限定する趣旨で記載したものではなく、また、個別ケースによって別途考慮すべき要素があり得るので注意を要する。

行政機関等は、安全管理措置を講ずるに当たり、番号法、個人情報保護法等関係法令、本ガイドライン、個人情報保護法ガイドライン（行政機関等編）、事務対応ガイド及び政府機関等のサイバーセキュリティ対策のための統一基準等に準拠した各府省庁等における情報セキュリティポリシー等を遵守することを前提とする。

なお、地方公共団体においては、これらに加え、地方公共団体における情報セキュリティポリシーに関するガイドライン等を参考に地方公共団体において策定した情報セキュリティポリシー等を遵守することを前提とする。

個人番号と個人情報を紐付ける登録事務（以下「個人番号登録事務」という。）を実施する行政機関等は、デジタル庁が策定した「マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドライン」及び各制度の所管省庁等が策定した個人番号登録事務に係るガイドライン等を遵守することを前提とする。

行政機関等は、特定個人情報保護評価を実施した事務については、その内容を遵守するものとする。また、個人番号利用事務の実施に当たり、接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置等を遵守することを前提とする。

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。

B 取扱規程等の見直し等

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ために、取扱規程等の見直し等を行わなければならない。

特に、特定個人情報等の複製及び送信、特定個人情報等が保存されている電子媒体等の外部への送付及び持ち出し等については、責任者の指示に従い行うことを定めること等が重要である。

《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

＊ 個人番号利用事務の場合、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 住民等からの申請書を受領する方法（本人確認、個人番号の確認等）
- ② 住民等からの申請書をシステムに入力・保存する方法
- ③ 個人番号を含む証明書等の作成・印刷方法
- ④ 個人番号を含む証明書等を住民等に交付する方法
- ⑤ 申請書及び本人確認書類等の保存方法
- ⑥ 保存期間を経過した書類等の廃棄方法

＊ 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。

＊ 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、情報連携を行う際の作業手順等、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。

＊ 取扱規程等は、関係法令、制度所管省庁によるガイドライン、通達等を踏まえ、継続的に見直しを行うことが重要である。

C 組織的安全管理措置

行政機関等は、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。

行政機関等は、組織体制の整備として、次に掲げる事項を含める。

- ・ 総括責任者（行政機関等に各 1 名）の設置及び責任の明確化
- ・ 保護責任者（個人番号利用事務等を実施する課室等に各 1 名）の

設置及び責任の明確化

- ・ 監査責任者の設置及び責任の明確化
- ・ 事務取扱担当者の設置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
- ・ 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
- ・ 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等への報告連絡体制の整備
- ・ 個人番号の漏えい、滅失又は毀損等（以下「漏えい等」という。）事案の発生又は兆候を把握した場合の職員から責任者等への報告連絡体制の整備
- ・ 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

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。

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事が考えられる。
 - ・ 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、[2](#)E 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

＊ 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的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。

→[2](#) F e 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。

- ・ 特定個人情報ファイルの名称
- ・ 行政機関等の名称及び特定個人情報ファイルが利用に供される事務をつかさどる組織の名称
- ・ 特定個人情報ファイルの利用目的
- ・ 特定個人情報ファイルに記録される項目及び本人として特定個人情報ファイルに記録される個人の範囲
- ・ 特定個人情報ファイルに記録される特定個人情報等の収集方法

d 漏えい等事案に対応する体制等の整備

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及び手順等を整備する。

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。

(※) 行政機関等において、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(行政機関等編)」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、体制及び手順等を整備することが考えられる。

- ・ 漏えい等事案が発覚した際の報告・連絡等
- ・ 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

- ＊ 不正アクセス、ウイルス感染の事案に加え、標的型攻撃等の被害を受けた場合の対応について、関係者において定期的に確認又は訓練等を実施することが考えられる。

● 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）監査の方法については、その実効性が担保される限りにおいて、デジタル技術を活用した方法によることも可能である。

D 人的安全管理措置

行政機関等は、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

総括責任者及び保護責任者は、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）。

- ・ 研修の計画をあらかじめ策定し、これに沿ったものとする。
- ・ 研修の内容は、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の確保に関する事項として、情報システムに対する不正な活動その他のサイバーセキュリティに対する脅威及び当該脅威による被害の発生又は拡大を防止するため必要な措置に関するものを含むものとする。
- ・ 特定個人情報ファイルを取り扱う事務に従事する者の全てに対して、おおむね一年ごとに研修を受けさせるものとする。

c 法令・内部規程違反等に対する厳正な対処

法令又は内部規程等に違反した職員に対し、法令又は内部規程等に基づき厳正に対処する。

E 物理的安全管理措置

行政機関等は、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。管理区域において、入退室管理及び管理区域へ持ち込む機器等の制限等の措置を講ずる。

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。

行政機関等は、管理区域のうち、基幹的なサーバ等の機器を設置する室等（以下「情報システム室等」という。）を区分して管理する場合には、情報システム室等について、次の①及び②に掲げる措置を講ずる。

① 入退室管理

- ・ 情報システム室等に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずる。また、情報システム室等に特定個人情報等を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様

の措置を講ずる。

- ・ 必要があると認めるときは、情報システム室等の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置を講ずる。
- ・ 必要があると認めるときは、入室に係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。

② 情報システム室等の管理

- ・ 外部からの不正な侵入に備え、施錠装置、警報装置、監視設備の設置等の措置を講ずる。

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。また、電子媒体及び書類等の庁舎内の移動等において、紛失・盗難等に留意する。

《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、書庫又は必要に応じて耐火金庫等へ保管することが考えられる。
- ＊ 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 電子媒体等の取扱いにおける漏えい等の防止

許可された電子媒体又は機器等以外のものについて使用の制限等の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。

取扱規程等の手続に基づき、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必要が生じた場合には、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、庁舎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、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を行うこと等が考えられる。

d 個人番号の削除、機器及び電子媒体等の廃棄

特定個人情報等が記録された電子媒体及び書類等について、文書管理に関する規程等によって定められている保存期間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－(4)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。
- ＊ 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。

F 技術的安全管理措置

行政機関等は、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利用事務等を行う場合、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。
- アクセス権を有する者に付与する権限を最小化する。
- 情報システムの管理者権限を有するユーザーであっても、情報システムの管理上特定個人情報等の内容を知らなくてもよいのであれば、特定個人情報等へ直接アクセスできないようにアクセス制御をする。
- 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。
- 特定個人情報等を取り扱う情報システムに導入したアクセス制御機能の脆弱性等を検証する。
- 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。

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

情報システムを外部等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等を導入し、適切に運用する。また、個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守する。個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を行う。

《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（又はその他の情報システム）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。
- * 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

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。

特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合、原則として、暗号化又はパスワードにより秘匿する。

《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。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。

- * 暗号化又はパスワードによる秘匿に当たっては、不正に入手した者が容易に復元できないように、暗号鍵及びパスワードの運用管理、パスワードに用いる文字の種類や桁数等の要素を考慮する。

● 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。→[2](#)C b 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。
- * 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 外的環境の把握

行政機関等が、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。