安全管理措置①

■ 安全管理措置（12条等）

個人番号及び特定個人情報を取り扱うにあたっては、安全管理措置を講じなければならない

（個人番号利用事務実施者等の責務）
第12条　個人番号利用事務実施者及び個人番号関係事務実施者（以下「個人番号利用事務等実施者」という。）は、個人番号の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない。

■ 中小規模事業者には軽減措置あり

- 中小規模事業者＝事業者のうち従業員の数が100人以下の事業者であって、次の①～④以外の事業者

①	個人番号利用事務実施者	健康保険組合等
②	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	税理士、社会保険労務士等
③	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	生命保険代理業、金融ファンド等
④	個人情報取扱事業者	個人情報の取扱いが5000件を超える事業者

安全管理措置②

■ 安全管理措置の考え方と検討手順

- 前提として、以下を明確にする

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（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) 特定個人情報等を取り扱う事務に従事する従業者（注）
（「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。

- 基本方針の策定

- 取扱規程等の策定（安全管理措置を盛り込む）

安全管理措置③

■ 講ずべき安全管理措置の内容

A) 基本方針の策定（任意）

B) 取扱規程等の策定（義務的）

C) 組織的安全管理措置（義務的）

D) 人的安全管理措置（義務的）

E) 物理的安全管理措置（義務的）

F) 技術的安全管理措置（義務的）

C)～F)をその内容に含む

安全管理措置　～取扱規程等の策定～

B) 取扱規程等の策定

「安全措置の考え方と検討基準」のスライド

- 前記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

誰が個人番号を取り扱うのかを決めておく

例）業務マニュアル、業務フロー図等に、個人番号・特定個人情報の取扱いを加える

中小規模事業者における対応

- ✓ 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。

安全管理措置～組織的安全管理措置①～

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。

	項 目	内容（中小規模事業者以外）	中小規模事業者
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	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、システムログまたは利用実績を記録する	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	
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また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	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

安全管理措置～組織的安全管理措置②～

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。

システムログまたは利用実績の記録そのものは義務的

≪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。

記録する項目は例示

- 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

削除・廃棄が例示されている点に留意

中小規模事業者における対応

✓ 特定個人情報等の取扱状況の分かる記録を保存する

例1）業務日誌等において、例えば、特定個人情報等の入手・廃棄、源泉徴収票の作成日、本人への交付日、税務署への提出日等の、特定個人情報等の取扱い状況を記録する。

例2）取扱規程、事務リスト等に基づくチェックリストを利用して事務を行い、その記入済みのチェックリストを保存する。（Q&A「Q14-2」）

安全管理措置～人的安全管理措置～

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。

	項 目	内容（中小規模事業者以外）	中小規模事業者
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。

安全管理措置～物理的安全管理措置①～

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。

	項 目	内容（中小規模事業者以外）	中小規模事業者
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、「管理区域」及び「取扱区域」を明確にし、物理的な安全管理措置を講ずる	
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また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	
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また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	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	復元できない手段で削除または廃棄する	
		削除または廃棄した記録を保存する。委託する場合には、委託先が確実に削除または廃棄したことを証明書等により確認する	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

安全管理措置～物理的安全管理措置②～

a. 特定個人情報等を取り扱う区域の管理

✓ 以下を明確にし、物理的な安全管理措置を講じる

「管理区域」＝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

「取扱区域」＝特定個人情報等を取り扱う事務を実施する区域

≪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。

座席配置＝例えば、事務取扱担当者以外の者の往来が少ない場所への座席配置や、後ろから覗き見される可能性が低い場所への座席配置等が考えられます（Q&A「Q15-1」）。

安全管理措置～物理的安全管理措置③～

b. 機器及び電子媒体等の盗難等の防止

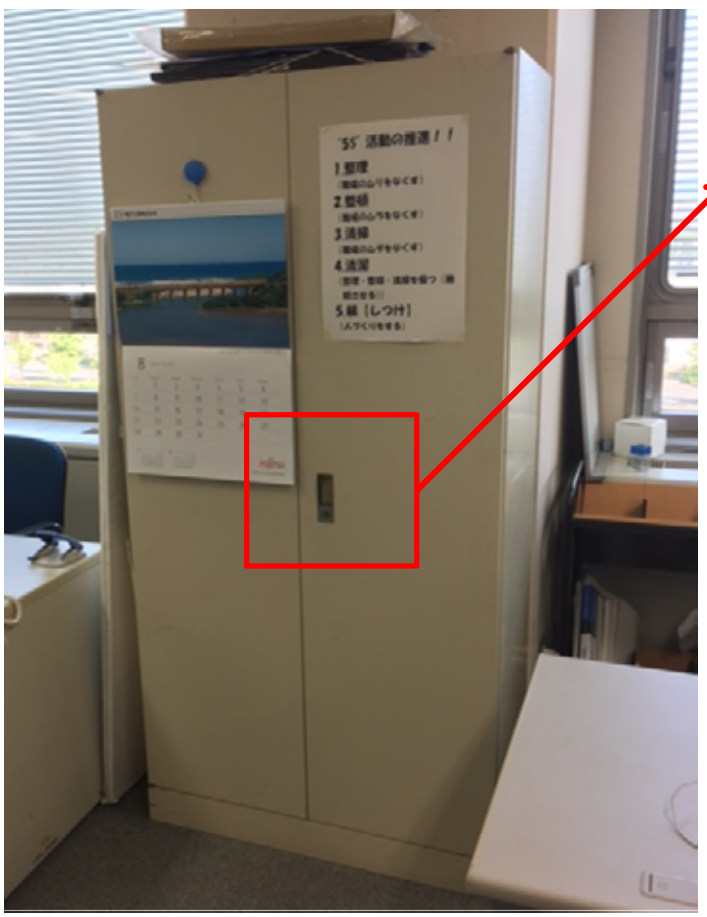
✓ 管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。

≪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。

管理区域（保管場所）と取扱区域（作業場所）



管理区域

取扱区域

安全管理措置～物理的安全管理措置④～

d. 個人番号の削除、機器及び電子媒体等の廃棄

✓ 個人番号利用事務等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。

例）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、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、又は個人番号部分を復元できない程度にマスキングする（Q&A「Q15-3」）。

✓ 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。

削除又は廃棄した記録の保存は義務的

中小規模事業者における対応

✓ 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。

安全管理措置～技術的安全管理措置①～

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。

	項 目	内容（中小規模事業者以外）	中小規模事業者
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また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	• 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	
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また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	
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	