

[マイナンバー制度 対応チェックリスト]

マイナンバー制度対応のために行うべき事項をまとめました。

企業は、マイナンバーが記載された通知カードが送付される、平成27年10月頃までにはこちらに記載された体制を整備する必要があります。
実施したものにチェックを入れていき、対応の漏れのないようにしましょう！

マイナンバー法が求める対応内容		✓	メモ
1	マイナンバー制度に対応するためにプロジェクトチームの立ち上げをしましたか？		
2	プロジェクトチームメンバーで、個人番号（以下、マイナンバー）の取得・保管・廃棄や、法定調書等の作成における全体スケジュールを策定しましたか？		
3	マイナンバーを受け取る必要のある対象者と事務の洗い出しをしましたか？		
4	上記の事務に関して担当部署・責任者・取扱責任者を選任しましたか？		
5	従業員からマイナンバーを受け入れる際の本人確認の手順を定めましたか？		
6	マイナンバー・特定個人情報の記録・保存方法を定めましたか？		
7	（個人情報利用事務等に関して外部委託をする場合）委託先を選定しましたか？ 注：委託者は、委託先において、番号法に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければなりません。		
8	基本方針の策定（安全管理措置ガイドライン）は済みましたか？		
9	特定個人情報取扱規程等の策定（誰が、いつ、何に、どのように利用するか）は済みましたか？		
10	個人情報の利用目的の特定、従業員への通知をしましたか？		
11	事務取扱担当者が従業員から質問を受けた際のQ & A マニュアルの策定をしましたか？		
12	自社の対策レベルにあった委託先を選定し、適切な契約を結びましたか？		

13	<p>特定個人情報ガイドラインの要件を満たす委託契約書（下記、①～⑩の項目）を整備しましたか？</p> <p>注：既存のものが要件を満たす場合又は要件を満たすように変更される場合は、それで認められます。</p> <p>①秘密保持義務 ②事業所内からの特定個人情報の持出しの禁止 ③特定個人情報の目的外利用の禁止 ④再委託における条件 ⑤漏えい事案等が発生した場合の委託先の責任 ⑥委託契約終了後の特定個人情報の返却又は廃棄 ⑦従業員に対する監督・教育 ⑧契約内容の遵守状況について報告を求める規程 ⑨特定個人情報を取り扱う従業員の明確化 ⑩委託者が委託先に対して実地の調査を行うことができる規程</p>		
14	マイナンバー制度についての教育計画・準備は整えましたか？		
15	従業員の住民票の住所と実際の住所が一致しているか確認をしましたか？		

組織的安全管理措置

①組織体制の整備			
16	<p>安全管理措置を講ずるための組織体制は整備しましたか？</p> <p>[中小規模事業者の場合] 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していますか？</p>		
②取扱規程等に基づく運用			
17	<p>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体制をとっていますか？</p> <p>[中小規模事業者の場合] 特定個人情報等の取扱状況の分かる記録を保存する体制を整備していますか？</p>		
③取扱状況を確認する手段の整備			
18	<p>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決めましたか？</p> <p>[中小規模事業者の場合] 特定個人情報等の取扱状況の分かる記録を保存する体制を整備していますか？</p>		
④情報漏えい等事案に対応する体制の整備			
19	<p>情報漏えい等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しましたか？</p> <p>[中小規模事業者の場合] 情報漏えい等の発生等に備え、従業員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ようになっていますか？</p>		
⑤取扱状況の把握及び安全管理措置の見直し			
20	<p>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ための体制をとっていますか？</p>		

人的安全管理措置

①事務取扱担当者の監督		
21	<p>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体制をとっていますか？</p>	
②事務取扱担当者・従業員の教育・周知		
22	<p>事務取扱担当者に、マイナンバー制度に関する特定個人情報等の要点、禁止事項等の適正な取り扱いについて、社内研修する等の周知を徹底すると共に適切な教育を行う体制をとっていますか？</p>	
物理的安全管理措置		
①特定個人情報等を取り扱う区域の管理		
23	<p>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、対象区域に対して入退室管理、入室制限等物理的な安全管理措置を講じていますか？</p>	
②機器及び電子媒体等の盗難等の防止		
24	<p>「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取っていますか？（施錠キャビネット・書庫・セキュリティワイヤー等）</p>	
③電子媒体等を持ち出す場合の漏えい等の防止		
25	<p>特定個人情報等が記録された電子媒体及び書類等を持ち出す場合、容易にマイナンバーが判明しない措置の実施、追跡可能な移送手段の利用等、安全管理を行っていますか？</p> <p>[中小規模事業者の場合]</p> <p>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際、電子媒体の場合、データ暗号化・パスワード保護実施、紙媒体の場合、施錠ケース・封緘・目隠しシール等で漏えい防止実施等、紛失・盗難・漏えい等を防ぐための安全管理を行っていますか？</p>	
④マイナンバーの削除、機器及び電子媒体等の廃棄		
26	<p>マイナンバーも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体制をとっていますか？</p> <p>また、廃棄方法を決めていますか？</p> <p>注：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体制をとる必要があります。</p> <p>[中小規模事業者の場合]</p> <p>特定個人情報等を削除又は廃棄したことを、責任ある立場の者が確認する体制を整備していますか？</p>	

技術的安全管理措置

① アクセス制御		
27	<p>情報システムを使用してマイナンバー関係事務又はマイナンバー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ようにしていますか？</p>	
② アクセス者の識別と認証		
28	<p>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こと（ユーザーID・パスワード認証・生体認証・ICカード認証等）としていますか？</p> <p>[中小規模事業者の場合]</p> <p>○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していますか？</p> <p>○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していますか？</p>	
③ 外部からの不正アクセス等の防止		
29	<p>外部ネットワークからの不正アクセス又は情報システムにアクセス可能な端末へウィルス対策ソフトの導入をし、適切に運用していますか？</p> <p>[中小規模事業者の場合]</p> <p>○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していますか？</p> <p>○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していますか？</p>	
④ 情報漏えい等の防止		
30	<p>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対策を取っていますか？（通信経路の暗号化・データ暗号化等）</p>	

中小規模事業者とは

事業者のうち従業員の数が100人以下の事業者であって、次に掲げる事業者を除く事業者をいいます。

- ・ マイナンバー利用事務実施者
- ・ 委託に基づいてマイナンバー関係事務又はマイナンバー利用事務を業務として行う事業者
- ・ 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
- ・ 個人情報取扱事業者