

【マイナンバー制度導入チェックリスト】（詳細チェックリスト）

番号法・特定個人情報ガイドラインが求める対応	当社における対応措置
<p>1. プロジェクトチームの立ち上げ 人事部門、経理部門、総務部門、コンプライアンス部門、情報システム部門など関連する部門の担当者からなるプロジェクトチームを立ち上げているか。一部の担当者に丸投げにせず、会社経営に直結する問題として位置付けているか。</p>	
<p>2. 個人番号を受け入れる必要のある事務の洗い出し 個人番号を受け入れる必要のある事務の洗い出しをしたか。</p>	
<p>3. 取り扱う特定個人情報等の洗い出し 上記2により洗い出した個人番号を受け取る事務に関して取り扱う特定個人情報等（個人番号及び特定個人情報）を洗い出したか。</p>	
<p>4. 事務取扱担当者の選任 事務取扱担当者を選任したか。 ⇒人事部・経理部の責任者を定める。 ＊担当部署・責任者の設置も必要となる。</p>	
<p>5. 本人確認の方法 従業員等から個人番号を受け入れる際の本人確認の方法について手続を定めたか。 本人確認の方法については、別途公表している本人確認方法の一覧表をご参考ください。</p>	
<p>6. 委託先の選定 （個人情報利用事務等に関して外部委託をする場合）委託先を選定したか。 「委託先の選定」については、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。具体的な確認事項としては、以下の事項が</p>	

<p>挙げられます。</p> <ul style="list-style-type: none"> ①委託先の設備 ②技術水準 ③従業者に対する監督・教育の状況 ④その他委託先の経営環境等 											
<p>7. システムベンダーへの相談</p> <p>各システムベンダーとも、給与計算ソフトのSEの人数は限られている。なるべく早く相談することが求められます。</p> <p>システムベンダーを選択する際には、そのシステムがどのようなサービスを提供しているか、従業員の数や雇用形態に応じて判断する必要があります。</p> <p>その際のチェックポイントとしては以下のような観点が考えられます。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td data-bbox="225 987 831 1133"> <p>マイナンバー対応のシステムは、既存の給与計算ソフトに含まれているか。外付けの独立のものか。内包型の場合、アクセス制御はどのようになされているか。</p> </td> </tr> <tr> <td data-bbox="225 1133 831 1182"> <p>クラウド型か独立型か</p> </td> </tr> <tr> <td data-bbox="225 1182 831 1279"> <p>個人番号の収集や本人確認、廃棄・削除事務を行えるか。</p> </td> </tr> <tr> <td data-bbox="225 1279 831 1375"> <p>個人番号の収集にかかわる問い合わせは初期費用に含まれるか。</p> </td> </tr> <tr> <td data-bbox="225 1375 831 1424"> <p>随時WEB照会が可能か。</p> </td> </tr> <tr> <td data-bbox="225 1424 831 1473"> <p>専用回線が必要か。</p> </td> </tr> <tr> <td data-bbox="225 1473 831 1570"> <p>未提出者の督促リストを作成してくれるか。(個人番号の収集・本人確認を委託する場合)</p> </td> </tr> <tr> <td data-bbox="225 1570 831 1666"> <p>再委託先を使っているか。(個人番号の収集・本人確認を委託する場合)</p> </td> </tr> <tr> <td data-bbox="225 1666 831 1812"> <p>扶養者や新入社員などについて追加発送が必要か、一括で可能か。(個人番号の収集・本人確認を委託する場合)</p> </td> </tr> <tr> <td data-bbox="225 1812 831 1910"> <p>監査対応はしてくれるか。(個人番号の収集・保管・廃棄を委託する場合)</p> </td> </tr> </table>	<p>マイナンバー対応のシステムは、既存の給与計算ソフトに含まれているか。外付けの独立のものか。内包型の場合、アクセス制御はどのようになされているか。</p>	<p>クラウド型か独立型か</p>	<p>個人番号の収集や本人確認、廃棄・削除事務を行えるか。</p>	<p>個人番号の収集にかかわる問い合わせは初期費用に含まれるか。</p>	<p>随時WEB照会が可能か。</p>	<p>専用回線が必要か。</p>	<p>未提出者の督促リストを作成してくれるか。(個人番号の収集・本人確認を委託する場合)</p>	<p>再委託先を使っているか。(個人番号の収集・本人確認を委託する場合)</p>	<p>扶養者や新入社員などについて追加発送が必要か、一括で可能か。(個人番号の収集・本人確認を委託する場合)</p>	<p>監査対応はしてくれるか。(個人番号の収集・保管・廃棄を委託する場合)</p>	
<p>マイナンバー対応のシステムは、既存の給与計算ソフトに含まれているか。外付けの独立のものか。内包型の場合、アクセス制御はどのようになされているか。</p>											
<p>クラウド型か独立型か</p>											
<p>個人番号の収集や本人確認、廃棄・削除事務を行えるか。</p>											
<p>個人番号の収集にかかわる問い合わせは初期費用に含まれるか。</p>											
<p>随時WEB照会が可能か。</p>											
<p>専用回線が必要か。</p>											
<p>未提出者の督促リストを作成してくれるか。(個人番号の収集・本人確認を委託する場合)</p>											
<p>再委託先を使っているか。(個人番号の収集・本人確認を委託する場合)</p>											
<p>扶養者や新入社員などについて追加発送が必要か、一括で可能か。(個人番号の収集・本人確認を委託する場合)</p>											
<p>監査対応はしてくれるか。(個人番号の収集・保管・廃棄を委託する場合)</p>											
<p>8. 社内規程の整備</p> <p>以下の社内規程を整備したか</p>											

<ul style="list-style-type: none"> ・基本方針の策定（安全管理措置ガイドライン） ・取扱規程等の策定 ・個人情報の利用目的の特定・通知等 ・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 <p>※いずれも弁護士法人三宅法律事務所のホームページ（http://www.miyake.gr.jp/）で公表している雛型をご参照ください。</p>	
<p>9. 委託契約書の整備</p> <p>以下の要件を満たす委託契約書を整備したか。</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <ul style="list-style-type: none"> 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定 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定 </div> <p>※弁護士法人三宅法律事務所のホームページ（http://www.miyake.gr.jp/）で公表しているモデル契約書をご参照ください。</p>	

<p>10. 役職員・顧客への教育・周知</p> <p>一般の従業員も個人番号や特定個人情報を受け渡しする可能性があるので、マイナンバー制度一般について教育必要。また、2015年10月頃に送付されてくる通知カードを誤って捨てないように周知必要。</p> <p>また、金融機関においては金融業務の顧客に対して、2015年夏ごろまでに同様の周知が必要。</p> <p>通知カードは、2015年10月5日付の住所に簡易書留（転送不要扱い）で郵送されてくるので、住民票の住所と実際の住所が異なる場合は通知カードを受け取れません。役職員や顧客の住民票に登録されている住所と実際の住所を一致させるように要請する必要があります。[後述雛型参照]</p>	
<p>11. 組織的安全管理措置</p>	
<p>①</p>	<p>組織体制の整備</p> <p>安全管理措置を講ずるための組織体制を整備したか。</p> <p>⇒取扱規程等の中で具体的に定める必要があります。</p> <p>（中小規模事業者）</p> <p>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るか。</p> <p>⇒中小規模事業者については取扱規程等を策定する必要は必ずしもありませんが策定した方が望ましいと考えられます。</p>

②	<p>取扱規程等に基づく運用</p> <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整備したか。</p> <p>※弁護士法人三宅法律事務所のホームページで公表する雛型をご参照ください。</p> <p>(中小規模事業者)</p> <p>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るか。</p>	
③	<p>取扱状況を確認する手段の整備</p> <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整備したか。</p> <p>(中小規模事業者)</p> <p>上記②と同じ。</p>	
④	<p>情報漏えい等事案に対応する体制の整備</p> <p>情報漏えい等の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したか。</p> <p>(中小規模事業者)</p> <p>情報漏えい等の事案の発生等に備え、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こととしているか。</p>	
⑤	<p>取扱状況の把握及び安全管理措置の見直し</p> <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整備しているか。</p> <p>※PDCAにより体制を見直す体制を確立する。内部監査や外部監査を検討。</p>	
<p>12. 人的安全管理措置</p>		
①	<p>事務取扱担当者の監督</p> <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整備し</p>	

	たか。	
②	事務取扱担当者・従業員の教育・周知 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体制を整備したか。	
13. 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 特定個人情報等の情報漏えい等を防止するために、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(以下「管理区域」という。)及び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。)を明確にし、物理的な安全管理措置を講じているか。 ※会社の規模や業種によって講ずる措置に幅があると考えられます。	
②	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じているか。	
③	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又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、安全な方策を講じているか。 「持出し」とは、特定個人情報等を、管理区域又は取扱区域の外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、紛失・盗難等に留意する必要がある。 (中小規模事業者) 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じてい	

	るか。	
④	<p>個人番号の削除、機器及び電子媒体等の廃棄</p> <p>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体制を整備しているか。</p> <p>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体制を整備しているか。</p> <p>法定保存期間が経過した法定調書を廃棄する時期を「年度末」等と定める。</p> <p>※廃棄作業を外部委託する場合には、証明書で確認する体制を確立する。</p> <p>(中小規模事業者)</p> <p>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体制を整備しているか。</p>	
14. 技術的安全管理措置		
①	<p>アクセス制御</p> <p>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こととしているか。</p>	
②	<p>アクセス者の識別と認証</p> <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としているか。</p> <p>(中小規模事業者)</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るか。</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るか。	
③	<p>外部からの不正アクセス等の防止</p> <p>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、適切に運用しているか。</p> <p>（中小規模事業者）</p> <p>※中小企業であっても、外部からの不正アクセスがないようにウィルス対策ソフトなどを導入することは重要です！</p>	
④	<p>情報漏えい等の防止</p> <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措置を講じているか。</p>	