マイナンバーチェックリスト

yes	no	項目		確認内容
		現状の把握と対応方針の決定		マイナンバーの影響を受ける業務を洗い出し、その洗い出した業務について自社対応か、社労士・税理士などへの外部委託（委託の範囲を定める）かを決定しましたか？
		収集対象者の把握		マイナンバーの収集対象者を洗い出しましたか？ ※対象者は、役員、従業員、パート、アルバイトなどのほか、支払調書を作成しなければならない弁護士や社宅・駐車場などの地主（個人）なども対象となる。
		事前周知		マイナンバー制度の概要、郵送された通知カードを会社へ届け出るまでは大切に保管すること、届いていない場合の対応、また現住所と住民票記載の住所が異なる場合は現住所市町村に転入届を提出することを周知しましたか？
		従業員研修		マイナンバーを取り扱う事務取扱担当者に、取扱の留意点、担当事務の処理手順の教育を、また全従業員に対して、制度の概要や会社への提出方法、マイナンバーの取扱いの留意点などについての研修を行いましたか？
		管理責任者、事務取扱担当者の選任		マイナンバーを管理監督する管理責任者及びマイナンバーを取り扱う事務取扱担当者を選任しましたか？
		委託先への監督	委託先の適切な選定	マイナンバー取扱い業務を外部委託する場合、特定個人情報ガイドラインに基づき適切な委託先を選定しましたか？ ※選定に際し、委託者はマイナンパー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（委託先の整備、技術対策、従業員に対する監督、教育の状況など）が委託先において講じられていることを予め確認しなければならない。
			安全管理措置に関する委託契約の締結	特定個人情報ガイドラインの要件を満たす委託契約書を締結しましたか？ ※委託契約の締結にあたっては、秘密保護義務、事業所内からの特定個人情報の持出しの禁止、特定個人情報の目的外利用の禁止、再委託の条件、漏えい事故が発生した場合の委託先の責任等を定めなければならない。
			委託先における特定個人情報の取扱状況の把握	委託先の特定個人情報の取扱状況を把握するために適正な監督方法を整備していますか？ ※監督方法は、委託先への現場確認、ヒアリング実施の他に、定期的に委託先から情報管理確認書（セキュリティ対策、従業員教育など）を求める方法もある。
		社内規程の整備		以下の社内規程を整備しましたか？ ① 基本方針の策定 ② 取扱規程等の策定 ③ 個人情報の利用目的の特定・通知等 ④ 就業規則への追加・変更等
		安全管理措置	組織的安全管理措置	① 組織体制の整備 取扱規程に基づき、マイナンバーや特定個人情報の安全管理措置を行えるよう組織体制を整備しましたか？ ※中小規模事業者の場合は、事務取扱担当者が複数いる場合は責任者と事務取扱担当者を区分することが望ましいとされている。
				② 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体制をとっていますか？ ※中小規模事業者の場合は、特定個人情報等の取扱状況の分かる記録を保存する方法がある。
				③ 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用意しましたか？ ※取扱状況を確認するための記録等としては、特定個人情報ファイルの種類、名称、責任者、取扱部署、利用目的などがある。個人番号は記録しない。
				④ 情報漏えい等に対応する体制の整備 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ていますか？ ※漏えい等の事故が発生した場合の対策として、その原因の調査、究明、主務大臣への報告、事実の公表などがある。
				⑤ 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、安全管理方法の評価、見直し、及び改善に取り組むための体制を整備しましたか？ ※改善手法としては、自主点検又は他部署監査等を行うことなどがある。

yes	no	項目		確認内容
		安全管理措置	人的安全管理措置	① 事務取扱担当者の監督 特定個人情報等が取扱規程等に基づき適正に取扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行うこととしましたか？
				② 事務取扱担当者の教育 事務取扱担当者に対して、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、研修を行うこととしましたか？ ※併せて就業規則に特定個人情報の秘密保持規定の盛り込みも考えられる。
			物理的安全管理措置	① 特定個人情報等を取扱う区域の管理 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」、「取扱区域」を明確にし、物理的な安全管理措置を行っていますか？ ※安全管理措置として、ＩＣカード・ナンバーキーなどによる入退室管理システムの設定や管理区域への機器の持込制限等がある。
				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行っていますか？ ※安全管理措置として、関係機器、電子媒体、書類等を施錠できるキャビネットなどへの保管やセキュリティワイヤー等により固定するなどがある。
				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対策の実施、追跡可能な移送手段の利用等、安全対策を行っていますか？ ※電子媒体の安全な持出し方法としては、持出しデータの暗号化、パスワードの設定、施錠できる搬送容器の使用等がある。なお、紙媒体の安全な持出方法として封緘や目隠しシール貼付などがある。
				④ 個人番号の削除、機器及び電子媒体等の廃棄 個人番号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仕組みとしていますか？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仕組みとしていますか？ ※特定個人情報等の記録された書類廃棄をする方法として焼却、溶解といった復元不能な方法等がある。
			技術的安全管理措置	① 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、及び当該事務で取扱う特定個人情報ファイルの範囲の限定のため、適切なアクセス制御を行うようにしていますか？ ※アクセス制御方法として、マイナンバーと紐付してアクセスできる情報範囲や特定個人情報ファイルを取り扱うシステムをアクセス制限により限定する方法がある。また、中小企業事業者では、特定個人情報を取扱う機器及び事務取扱担当者を限定することや、機器の機能であるユーザーアカウント制御機能を使用し、事務取扱担当者を限定することが望ましい。
				② 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こととしていますか？ ※具体的な事務取扱担当者の識別方法として、ユーザーＩＤ、パスワード、磁気、ＩＣカードなどある。また、中小企業事業者にあっては、特定個人情報取扱機器を特定のうえ、事務取扱担当者を限定する方法などがある。
				③ 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、適切に運用していますか？ ※防止策として、ファイヤーウォールの設定、ウイルス対策ソフトの導入、アクセスログ分析による検知方法などがある。
				④ 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対策を行っていますか？ ※防止策としては、通信経路の暗号化やシステム内の保存データの暗号化やパスワードによる保護方法がある。

※ 中小規模事業者：従業員の数が 100 人以下で、個人情報取扱事業者（個人情報を 5000 人分以上利用）以外の事業者

以上