平成27年8月

中小規模事業者の対応について

社会保険労務士法人ビークライン

「**中小規模事業者における対応方法**」(中小規模事業者の講ずべき安全管理措置の内容) を「**原則として求められる安全管理措置の内容**」と対比して、次ページ以降、一覧にまとめておりますのでご活用ください。「**中小規模事業者の対応ポイントや具体的例示**」につきましてもご参考にしてください。
なお、安全管理措置を講ずる前段階として、下記3点を明確化した上で、次ページ以降の「**中小規模事業者における対応方法**」を行ってください。

1.個人番号を取り扱う事務の範囲の明確化

事業者は、個人番号関係事務又は個人番号利用事務の範囲を明確にしておかなければならない。
⇒ 具体的には、事業者が、法令に基づき、従業員等の個人番号を給与所得の源泉徴収票、支払調書、健康保険・厚生年金保険被保険者資格取得届等の書類に記載して、行政機関等に提出する事務を明確にしておくことです。

2.特定個人情報等の範囲の明確化

事業者は、1.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。
⇒ 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) の範囲を明確にしておくことです。

3.事務取扱担当者の明確化

事業者は、1.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。
⇒ 「個人番号」を含めた特定個人情報を取り扱う担当者や部門を明確にしておくことです。

「**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。

・個人番号利用事務実施者 (「個人番号利用事務」を行う行政機関等)
・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
・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 (過去6か月間で5,000以上の個人情報を有する日が1日でもあり、それらを利用している事業者)

※「中小規模事業者」の定義における従業員とは、労働基準法第20条の規定により解雇の予告を必要とする労働者 (日々雇い入れられる者、2か月以内の期間を定めて使用される者等除く) と解されます。
中小規模事業者の判定における従業員の数は、事業年度末 (事業年度が無い場合には年末等) の従業員の数で判定し、毎年同時期に見直しを行う必要があります。

下記、サイト資料等もご参考にしていただき、ご対応いただければと存じます。

【中小規模事業者向けポイント資料】 ①取得 ②利用・提供 ③保管・廃棄 ④安全管理措置 4つのポイントがまとめられております。

http://www.cas.go.jp/jp/seisaku/bangoseido/download/kojinjigyou.pdf

【中小規模事業者向けマイナンバー導入チェックリスト】

http://www.cas.go.jp/jp/seisaku/bangoseido/download/checklist.pdf

安全管理措置の内容

原則として求められる安全管理措置の内容 (従業員数101人以上の事業者の対応)	中小規模事業者(従業員数100人以下の事業者)における対応方法	中小規模事業者の対応ポイントや具体的例示
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。	左記に同じ	基本方針に定める項目としては、 ・事業者の名称・関係法令・ガイドライン等の遵守・安全管理措置に関する事項・質問及び苦情処理の窓口 等　が挙げられます。 基本方針の策定は義務ではありませんが、作ってあれば従業員の教育に立ちます。
B　取扱規程等の策定 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。	○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。	・業務マニュアル、業務フロー図、チェックリスト等に、マイナンバーの取扱いを加えることも考えられます。
C　組織的安全管理措置　　情報漏えい等の事故発生に備えた組織体制の整備　等 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。		
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。	・けん制効果が期待できる方法です。
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。 **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。なお、取扱状況を確認するための記録等には、特定個人情報等は含めない。	○特定個人情報等の取扱状況の分かる記録を保存する。	例えば、次のような方法が考えられます。 ・業務日誌等において、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等を記録する。 ・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。
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対応体制を整備する。情報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。	○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。	・業務遂行の基本、「ほうれんそう」(報告・連絡・相談)を確認しましょう。
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。	・事業者のリスクを減らすための方策です。

D　人的安全管理措置		総務経理などの事務取扱担当者に対する監督、教育　等
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。		
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。	左記に同じ	従業員の監督･教育は、事業者の基本です。 従業員に取得･利用･提供･保管･廃棄のルール、安全管理措置のルールを徹底しましょう。 例えば、次のような方法が考えられます。 ･特定個人情報の取扱いに関する留意点等について従業員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。
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。	左記に同じ	

E　物理的安全管理措置		外部からの不正アクセスの防止策　等
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。		
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、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ずる。	左記に同じ	･事業者の規模及び特定個人情報等を取り扱う事務の特性等によりますが、例えば、壁又は間仕切り等の設置及び覗き見されない場所等の座席配置の工夫等が考えられます。
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。	左記に同じ	･事業者の規模及び特定個人情報等を取り扱う事務の特性等によりますが、例えば、書類等を盗まれないように書庫等のカギを閉める等が考えられます。
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、安全な方策を講じる。「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。	○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。	･置き忘れ等にも気を付けましょう。
d個人番号の削除、機器及び電子媒体等の廃棄 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。	○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。	･事業者のリスクを減らすために大切です。

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。		パソコンや電子データの盗難防止策　等
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。	○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。	・担当者以外の者に勝手に見られないようにしましょう。
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、適切に運用する。	左記に同じ	インターネットにつながっているパソコンで作業を行う場合の対策です。例えば、次のような方法が考えられます。 ・ウイルス対策ソフトウェア等を導入する。 ・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により、ソフトウェア等を最新状態にする。
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じる。	左記に同じ	インターネットにつながっているパソコンで作業を行う場合の対策です。例えば、データの暗号化又はパスワードによる保護等が考えられます。