月刊AMCPレポート

ＡＭＣパートナーズ株式会社
ＡＭＣパートナーズ税理士法人
〒541-0054　大阪市中央区南本町2-3-8
Tel:06-6262-2256/Fax:06-6262-2257
【AMCPグループ】 http://www.amcp.biz/

# 財務 VOL.78

# マイナンバーと安全管理措置

今号も、前号に引き続きマイナンバー制度について取り上げます。**「番号情報が漏れないよう厳格に管理する必要がある」「罰則規定が厳しい」**等々、巷ではマイナンバー制度をビジネスチャンスと捉える業者を中心に、マイナンバー制度への厳格な対応を促す情報が氾濫しています。**「実際問題、中小零細事業者はいったいどの程度まで対応すれば良いのか？」**について、事業者の義務である**「安全管理措置」**という観点から説明させて頂きます。

## 安全管理措置とは

まず、安全管理措置の法的根拠については、番号法第12条に下記のように規定されています。

**〔番号法第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。**

上述の通り、法律では**「適切な管理のために必要な措置」**という漠然とした表現しかされておらず、詳細は国の機関である「特定個人情報保護委員会」（以下、「委員会」といいます）の定めた「特定個人情報の適正な取扱いに関するガイドライン」（**法律ではありません**。以下**「ガイドライン」**といいます）に定められております。ガイドラインの中で「中小規模事業者（従業員数100人以下）における対応方法」として定められている項目は下記の通りです（原文抜粋）。

A　基本方針の策定（義務ではない）
**B　取扱規定等の策定（義務）**
**C　組織的安全管理措置（義務）**
- a　組織体制の整備
- b　取扱規定等に基づく運用
- c　取扱状況を確認する手段の整備
- d　情報漏えい等事案に対応する体制の整備
- e　取扱状況の把握及び安全管理措置の見直し

**D　人的安全管理措置（義務）**
- a　事務取扱担当者の監督
- b　事務取扱担当者の教育

**E　物理的安全管理措置（義務）**
- a　特定個人情報等を取り扱う区域の管理
- b　機器及び電子媒体等の盗難等の防止
- c　電子媒体等を持ち出す場合の漏えい等の防止
- d　個人番号の削除、機器及び電子媒体等の廃棄

**F　技術的安全管理措置（義務）**
- a　アクセス制御
- b　アクセス者の識別と認証
- c　外部からの不正アクセス等の防止
- d　情報漏えい等の防止

要約しますと、B～Dでは、ソフト面における安全管理措置として、マイナンバーの取得・取扱・廃棄等を行う方（以下**「事務取扱担当者」**といいます）を決定した上で、担当業務及び業務フローの明確化、マイナンバーの取扱記録の保存、事務取扱担当者に対する監督及び教育等が要求されております。

一方、E～Fでは、ハード面における安全管理措置として、マイナンバーを取扱うための事務スペースの設置、取扱い機器等の盗難防止対策、パスワードの設定、アクセス制御等による事務取扱担当者の限定等が要求されております。

これらを更に簡単な文章で表現すると下記のようになります（先述の「委員会」が小規模事業者用に作成したパンフレット「マイナンバーガイドラインのかんどころ」より原文抜粋）。

- **マイナンバーが記載されている書類は、カギのかかるところに大切に保管しましょう。**
- **マイナンバーが保存されているパソコンをインターネットに接続する場合は、最新のウィルス対策ソフトを入れておきましょう。**
- **マイナンバーを扱う人を決めておきましょう。**
- **マイナンバーの記載や書類を提出したら、業務日誌などに記録するようにしましょう。**
- **源泉徴収票の控えなど、マイナンバーの記載されている書類を外部の人に見られたり、机の上に出しっぱなしにしたりしないようにしましょう。**
- **保存期間が過ぎたものなど、必要がなくなったマイナンバーは廃棄しましょう。マイナンバーを書いた書類は、そのままゴミ箱に捨ててはいけません。**

いかがでしょうか？何を注意して、何を実行すれば良いのか、なんとなく具体的にイメージできたのではないでしょうか。

## 安全管理措置と罰則について

**ガイドラインは法律ではありませんので、守れていない部分があったとしても罰則はありません。**現実的には、情報漏えい事故が発生し、その事故に対して委員会が関与し、委員会の「命令」に違反した場合に初めて罰則が科されることとなります（番号法第73条）。

委員会は、マイナンバーを含む個人情報の取扱に関し、事業者に対して指導及び助言や勧告を行うことができ、事業者が勧告に従わなかった場合や緊急の必要がある場合に限り、命令を行うことができます。**この「命令」に従わなかった場合に、初めて罰則が科されます**ので、罰則を科すまでのハードルは極めて高いことがお分かりいただけるかと思います。

また、例えば**従業員がマイナンバーの不正漏洩に手を染めても、それだけで会社が罰せられることはありません。**会社ぐるみ、あるいは代表者による故意の漏洩といったケースでないと、事業者に刑事罰は科されません。

いかがでしょうか？当たり前の事ですが、大切なのは**「情報が漏れないようにすること」です。細心の注意を払い、当たり前の事を当たり前に実行しさえすれば、過度に神経質になる必要はありません。**

最後に、「情報管理をどこまで厳重にする必要があるか？」との問いに対する政府高官の答弁をご紹介して、今号を締めくくりたいと思います。

『一般的な人事給与システムであれば、他の社員の情報を閲覧できないようにアクセス管理されているはず。これと同程度のセキュリティ、普通の企業が常識的に人事情報を管理するレベルがあればいい。』