

平成27年10月26日

顧問先各位

戸田会計事務所
所長 戸田裕陽

マイナンバー制度への事前準備 その4

マイナンバーを取扱う企業はマイナンバーの漏えい、滅失、毀損の防止等適切な管理のために、「安全管理措置」を講じなければなりません。(一部、NO. 560の内容を含みます。)

- ◎ **取扱規定等の作成**……個人番号取扱い事務作業の流れ(取得→利用→保管→提供→削除)を文書化、図式化、チェックリストにするなどマニュアル化し、事務担当者・責任者が引き継げる体制を作る必要があります。
- ◎ **組織的安全管理措置**
 - ・個人番号事務担当者・責任者の選定……個人番号が必要とされる事務作業をふまえて個人番号事務担当者・責任者を選定する必要があります。
 - ・個人番号取扱状況を記録・保存……取扱事務ごと、個人ごとに個人番号の取得日、本人確認状況、源泉徴収票作成・税務署等への提出等の利用日、利用目的の適正性、保管状況、個人番号に関する情報の廃棄日、廃棄状況等を記録する管理帳票、チェックリスト等を整備しておく必要があります。
 - ・情報漏えい等に対応する体制の整備……情報漏えい等が発生した場合、従業員等から個人番号事務担当責任者への報告・連絡体制をあらかじめ確認しておきましょう。
- ◎ **人的安全管理措置**
 - ・個人番号事務担当者の教育……マイナンバー制度・取扱事務の理解が必要です。
- ◎ **物理的安全管理措置**
 - ・個人番号取扱区域の管理……個人番号取扱事務は覗き見されないように別室、間仕切り、座席の隔離等の環境を確保して行いましょう。
 - ・機器、USB等電子媒体等の盗難防止……鍵付き書庫等にマイナンバーの記載・入力された、書類、電子媒体、ノートパソコンを保管する等の保管方法を決めておきましょう。
 - ・書類、電子媒体を持出す場合の漏えい防止……パスワードの設定、封筒に封入し鞆に入れて搬送するなど、紛失・盗難を防ぐための安全な持出方法を決めておきましょう。
- ◎ **技術的安全管理措置**
 - ・アクセス制御……個人番号事務担当者が番号事務に使用するパソコンを特定し、パソコンに標準装備されているユーザー制御機能で担当者以外はパソコンを使用できないようにしましょう。
 - ・外部からの不正アクセス防止……ウイルス対策ソフトの導入し、常に最新の状態にアップデートしておきましょう。あるいは個人番号事務担当者が番号事務に使用するパソコンは常時インターネットから切断しておき、必要時最低限のみ接続することも考えられます。
 - ・情報漏えい防止……インターネットで情報を送受信する場合には、データの暗号化やパスワードによる保護なども必要となります。