大和総研
Daiwa Institute of Research

なるほどマイナンバー　個人の生活の視点から　第 12 回

2015 年 11 月 27 日
全 6 頁

企業、金融機関、行政機関のマイナンバー情報保護措置（3）

安全管理措置

金融調査部
制度調査担当部長　吉井　一洋

マイナンバーに対する国民への懸念に対応するため、各種の保護措置が講じられています。今回は、企業、金融機関、行政機関等が講じるべき安全管理措置について解説します。

下記の説明は、番号法その他の関係法令や特定個人情報保護委員会が策定・公表した「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」、「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」や関連するＱ＆Ａに基づいています。

7. 安全管理措置

番号法では、マイナンバーを取り扱う行政機関や企業に対して、マイナンバーあるいはマイナンバー付の個人情報の漏えい、滅失又は毀損の防止等、これらの情報の管理のために、必要かつ適切な安全管理措置を講じることを義務付けています。個人情報取扱業者ではない、個人情報データベースが 5,000 名以下の企業でも、マイナンバーを取り扱うのであれば安全管理措置を講じなければなりません。ただし、従業員が 100 名以下の中小企業（中小規模事業者）の場合（金融機関などを除きます）は、軽減措置が認められています。なお、生きておられる方だけでなく、亡くなられた方のマイナンバーに対しても安全管理措置が義務付けられます。

行政機関・地方公共団体や企業は、マイナンバーを取り扱う事務の範囲と、当該事務において取り扱うマイナンバーやマイナンバーと関連付けて管理される個人情報の範囲、当該事務の担当者を明確にした上で、下記のような安全管理措置を講じる必要があります。

（1）基本方針の策定

特定個人情報等（マイナンバーやマイナンバー付の個人情報）の保護に関する基本理念を明

図表 2－1　企業、行政機関等における安全管理措置　その 1

措置の内容	企業 （金融機関は企業を参照）	中小企業(中小規模事業者)の特例	行政機関等
(1)基本方針の策定	**重要**である		
	含める項目を**例示**（企業名、法令・ガイドライン遵守、安全管理措置に関する事項、質問・苦情処理窓口等）		例示無し
(2)取扱規程の策定（見直し等）	策定**しなければならない**		・見直し等を**行わなければならない** ・特定個人情報等が保存された電子媒体等の外部への送付・持出し等は、責任者の指示に従うことを定める等が**重要**
・取扱方法 ・責任者、事務取扱担当者 ・上記の者の任務等	取得、利用、保存、提供、削除・廃棄の各段階ごとに定めることが**考えられる**	・特定個人情報等の取扱い明確化 ・担当者変更時の確実な引継ぎと確認	取得、利用、保存、提供、削除・廃棄の各段階ごとに定めることが**考えられる**
・(3)から(6)の措置を織り込む	**重要**である		**重要**である
(3)組織的安全管理措置	①～⑤の措置を**講じなければならない**		
①組織体制の整備	項目を**例示**（責任者・事務取扱担当者とその責任・役割、取扱う情報の範囲の明確化、違反や情報漏えいの事実・兆候の報告連絡体制、部署間の役割分担・責任の明確化等）	事務取扱担当者が複数いる場合、責任者と事務担当者の区分が**望ましい**。	行政機関等：企業よりも詳細な項目（＋総括・保護・監査責任者の設置と明確化など）を**含める** 地方公共団体：項目を**参考**
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の確認のため、システムログ又は利用実績を記録	特定個人情報等の取扱状況のわかる記録を保存	アクセス状況の記録と一定期間保存、定期・随時分析、記録の改ざん・窃取・不正削除防止のために必要な措置を講じる
	手法を**例示**（利用・出力・持ち出し・削除廃棄・アクセスログ等の記録など） 事務フローに即した手続の明確化が**重要**		手法を**例示**（企業と同様）
③取扱状況確認手段の整備	特定個人情報ファイルの取扱状況を確認する手段の整備	特定個人情報等の取扱状況のわかる記録を保存	特定個人情報ファイルの取扱状況を確認する手段の整備
	手法の**例示**（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、削除・廃棄状況、アクセス権者の記録）		行政機関等：ファイルの名称、担当機関・組織の名称、利用目的、記録項目・個人の範囲、収集方法を**含める**。 地方公共団体：上記の項目を**参考**
④情報漏えい事案対応体制整備	適切・迅速に対応するための体制整備	責任者への報告連絡体制等をあらかじめ確認	適切・迅速に対応するための体制整備
	事案に応じて、事実関係及び再発防止策等の早急な公表が**重要である**		事案に応じて、事実関係及び再発防止策等の早急な公表が**重要である**
	手法を**例示**（**望ましい措置**：責任者への報告と被害拡大防止、事実関係調査と原因の究明、影響範囲の特定、本人への連絡、再発防止策の検討・決定と実施、事実関係と再発防止策等の公表）		**必要な措置**（責任者への報告と被害拡大防止、事実関係調査と原因の究明、影響範囲の特定、本人への連絡、再発防止策の検討・決定と実施、事実関係と再発防止策等の公表）を講じる
	特定情報保護委員会・担当大臣への**報告するよう努める**（一定の場合、委員会への報告は免除）		特定個人情報保護委員会に**速やかに（重大事案は直ちに）報告する**。
⑤取引状況の把握と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、安全管理措置を評価・見直し・改善	責任者が特定個人情報等の取扱状況を定期的に点検	監査責任者等が管理状況を定期・随時に点検・監査、統括責任者はその結果の報告を踏まえ、必要に応じ、取扱規程等の見直し等の措置
	手法を**例示**（定期的自主点検と他部署等の監査、外部による監査との連携）		
(4)人的安全管理措置	①、②の措置を**講じなければならない**		
①事務取扱担当者の監督	必要かつ適切な監督を行う		統括責任者及び保護責任者が監督
②事務取扱担当者の教育	適正な取扱いの周知徹底と適切な教育		統括責任者及び保護責任者による事務取扱責任者への必要な教育研修の実施と機会の付与、情報システム管理職員への必要な教育研修
	手法を例示（特定個人情報等の取扱いの留意事項の定期的な研修、秘密保持に関する事項の就業規則への盛り込み）		

（注）金融機関の安全管理措置は企業と同様（中小企業の特例は無い）

（出所）番号法の関係法令・ガイドラインに基づき、大和総研金融調査部制度調査課作成

らかにし、これらの適正な取扱いを確保するために、関係法令やガイドラインの遵守、安全管理措置に関する事項、質問や苦情処理の窓口などに関する方針を定めることが重要です。

(2) 取扱規程等の策定

特定個人情報等を取り扱う事務フローを整理し、具体的な取り扱いを定める取扱規程等を定める必要があります。例えば、マイナンバーの取得、利用、保存、提供、削除・廃棄の各段階ごとにマイナンバー等の取扱方法、責任者・事務取扱担当者とその任務等を定めることが考えられます。マイナンバーの告知・提供者（本人）からの提出書類のとりまとめ方法、必要な事務書類作成部署への移動方法、システムへのデータの入力方法、提出書類の作成・提出方法、関連情報の保存方法、廃棄・削除の方法などの事務フローに即して手続を明確にしておくことが重要とされています。

中小企業の場合でも、特定個人情報等の取扱い等を明確化すること、事務取扱担当者が変更された場合に確実な引き継ぎを行い、責任者が確認することを求められます。

(3) 組織的安全管理措置

担当者を明確にし、それ以外の者が特定個人情報等（マイナンバーやマイナンバー付の個人情報）を取り扱うことがないような仕組みを構築する必要があります。具体的には次のような対応が必要となります。

① **組織体制の整備**：例として、責任者（行政機関の場合は、総括・保護・監査の各責任者）・事務取扱担当者とその責任・役割の明確化、事務取扱担当者が取り扱う特定個人情報等の範囲の明確化、複数の部署で取り扱う場合の各部署の役割分担と責任の明確化、担当者の規定違反やその兆候を把握した時、情報漏えいの発生やその兆候を把握した時の責任者への報告連絡体制の整備など。中小企業でも、事務取扱担当者が複数名いる場合は、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ます。

② **取扱規程等に基づく運用**：取引規程等が守られているか確認するため、システムログや利用実績を記録する必要があります。例えば、マイナンバーを含む個人情報ファイルの情報の利用や出力状況、持出し、削除・廃棄の状況の記録が挙げられます。中小企業でもマイナンバー付の個人情報の取扱状況がわかる記録を保存する必要があります。

③ **取扱状況を確認する手段の整備**：マイナンバーを含む個人情報ファイル（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の整備が必要です。取扱状況を確認するための記録等としては、例えば、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、削除・廃棄状況、アクセス権保有者の記録が挙げられます。中小企業でも特定個人情報等の取扱状況がわかる記録を保存する必要があります。なお、当該記録にはマイナンバーは記載しないこととされています。

④ **情報漏えい等事案に対応する体制の整備**：情報漏えいの発生やその兆候を把握した時に備え、責任者への報告連絡体制をはじめとする適切かつ迅速に対応するための体制を整備する必要があります。情報漏えい等が生じた際には、二次被害や類似事案の発生を防止する観点から事実関係や再発防止策を早急に公表することが重要です。望ましい対応としては、内部の責任者への報告と被害拡大の防止、事実関係の調査と原因の究明、影響の範囲の特定、影響を受ける可能性のある本人への連絡、再発防止策の検討・決定と実施、事実関係及び再発防止策の公表等が挙げられます。中小企業でも、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必要があります。

企業の場合は、事実関係や再発防止策を特定個人情報保護委員会や担当大臣に報告するよう努めることとされています。ただし、以下の五つの要件のすべてに該当する企業の場合は、報告は不要です。

・影響を受ける可能性のある本人に連絡　・外部に漏えいしていないと判断される。

・従業員等が不正の目的で持ち出したり利用したりした事案ではない。

・事実関係の調査を終了し、再発防止策を決定している。

・事案における特定個人情報の本人の数が 100 人以下

行政機関等の場合は、上記の対応を「望ましい」ではなく、行わなければなりません。さらに、特定個人情報保護委員会に速やかに報告しなければなりません。重大事案（となるおそれのある事案）の場合は直ちに報告を行わなければなりません。重大事案とは、情報提供ネットワークシステムやマイナンバーを取扱うシステムからの漏えい（不正アクセスや不正プログラムによるものを含みます）、対象となる特定個人情報の数が 101 人以上、不特定多数の人が閲覧できる状態になった場合、職員等が不正の目的で持ち出したり利用したりした場合、その他各機関で重大事案と判断される場合をいいます。

⑤ **取扱状況の把握と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、見直しと改善に取り組む必要があります。中小企業でも定期的な点検が必要です。

(4) 人的安全管理措置

特定個人情報等（マイナンバーやマイナンバー付の個人情報）が取扱規程等に基づき適切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こと、事務取扱担当者にマイナンバー付の個人情報等の適正な取扱いの周知・徹底と適切な教育を行うことが必要となります。中小企業も同様です。

(5) 物理的安全管理措置

特定個人情報等（マイナンバーやマイナンバー付の個人情報）の漏えい・盗難等を防ぐため、

図表 2－2　企業、行政機関等における安全管理措置　その 2

措置の内容	企業 （金融機関は企業を参照）	中小企業(中小規模事業者)の特例	行政機関等
(5)物理的安全管理措置	①から④の措置を**講じなければならない**		
①特定個人情報等を取扱う区域の管理	特定個人情報ファイルを取扱う情報システム管理区域と取扱事務を実施する区域を明確にし物理的安全措置を講じる		左記の管理区域において入退室管理及び機器等の持ち込みを制限
	手法を**例示**（入退室管理・機器等の持込み制限、ICカード・ナンバーキーでの入退室管理、壁・間仕切りの設置、座席配置の工夫など）		入退室管理、情報システム室等の管理のための措置を挙げる（地方公共団体は参考にして適切な措置）
②機器及び電子媒体等の盗難等の防止	手法を**例示**（施錠キャビネット・書庫等での保管、セキュリティワイヤー等での機器の固定など）		庁舎内の移動等の紛失・盗難等にも留意
			手法を**例示**（企業と同様の方法＋必要に応じ耐火金庫等）
③電子媒体等持ち出し時の漏えい等の防止	容易に個人情報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	パスワードの設定、封筒封入で鞄で搬送等、安全な方策を講じる	許可された電子媒体・機器等以外の使用制限、USB等の接続制限、持ち出し時における企業と同様の安全な方策を講じる
	手法を**例示**（持出しデータの暗号化、パスワード、施錠可の容器使用、目隠しシール等）		手法を**例示**（企業と同様）
④マイナンバーの削除、機器及び電子媒体等の廃棄	マイナンバーの保有の必要が無くなった場合、できるだけ速やかに復元できない手段で削除・廃棄する	特定個人情報等の削除・廃棄を責任者が確認する。	企業と同様の対応
	削除・廃棄の記録は保存する		
	委託先の削除・廃棄を証明書等で確認		
	手法を**例示**		
(6)技術的安全管理措置	①から④の措置を**講じなければならない**		
①アクセス制御	事務取扱担当者と取り扱う特定個人情報ファイルの範囲を限定するため、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、それを取扱う事務取扱い担当者を限定することが**望ましい** ・機器に標準装備されたユーザー制御機能で、情報システムを取扱う事務取扱担当者を限定することが**望ましい**	企業と同様の対応
	手法を**例示**（アクセスできる情報の範囲、情報システム、ユーザーIDで利用できる事務取扱者を限定）		手法を**例示**（企業と同様の対応に加え、アクセス権の付与対象者とその権限の最小化、管理権限者による不要なアクセスの制御、アクセス制御機能の脆弱性等の検証）
②アクセス者の識別と認証	事務取扱担当者が正当なアクセス権保有者であることを識別結果で認証		企業と同様の対応
	識別方法の**例示**（ユーザーID、パスワード、磁気・ICカード等）		識別方法の**例示**（企業と同等の方法の他、生体情報等）
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・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		
			情報提供ネットワークシステム等の接続規程等が示す措置を**遵守**
	手法の**例示**（ファイアウォール等、ウィルス対策ソフトウェア等、ログ等の定期的分析）		手法の**例示**（企業と同様の措置の他、自動更新機能の活用、不許可の電子媒体・ソフトウェアの禁止）
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で外部送信する場合、通信経路での漏えい防止措置を講じる		
	手法の**例示**（通信経路の暗号化等、データの暗号化・パスワードによる保護等）		

（注）金融機関の安全管理措置は企業と同様（中小企業の特例は無い）
（出所）番号法の関係法令・ガイドラインに基づき、大和総研金融調査部制度調査課作成

これらの情報を取り扱う情報システムや事務を実施する区域を明確にし、物理的な安全措置を講じる必要があります。例えば、IC カード・ナンバーキーによる入退室管理や機器の持ち込みの制限、壁や間仕切り等の設置、のぞき見されないような座席配置の工夫などが考えられます。

行政機関等の場合、情報システム室を設けて管理する場合があります。その際には、入退室を含めより厳格な室の管理が求められます。

さらに、特定個人情報等を取り扱う機器、電子媒体、書類等の盗難又は紛失等を防止するための物理的な安全措置を講じる必要があります。例えば、鍵付きのキャビネット・書庫等での保管、機器のワイヤーでの固定、などが考えられます。

電子媒体を持ち出す際の情報漏えいの防止措置として、容易にマイナンバーが判明しない措置、追跡可能な移送手段の利用等の方策を講じる必要があります。例えば、データの暗号化、パスワードによる保護、施錠できる搬送容器の使用、目隠しシールの貼付などが考えられます。中小企業であっても、例えば、パスワードの設定、封筒に封入して鞄に入れて搬送する等の、紛失・盗難を防ぐ措置を講じる必要があります。

保管の必要が無くなった情報は、できるだけ速やかに、復元できない方法で削除・廃棄する必要があります。削除・廃棄した場合はその記録を保存する必要があります。外部に委託している場合は委託先が確実に削除・廃棄したことを証明書等で確認しなければなりません。中小規模事業者の場合は、削除・廃棄したことを、責任ある立場の者が確認する必要があります。

(6) 技術的安全管理措置

担当者と取り扱える情報の範囲を限定するため、アクセス制御、アクセス者を識別し認証する仕組み、外部からの不正アクセスの防止措置、情報漏えい等の防止措置を講じる必要があります。ウィルス対策ソフトウェアを導入し最新状態にアップデートする、アクセスログを定期的に分析するなどの対応が求められます。行政機関等の場合は、情報提供ネットワークシステム等への接続が予定されているため、接続規程等が示す安全管理措置を遵守する必要があります。

（次回予告：企業、金融機関、行政機関のマイナンバー情報保護措置（4）　外部委託、特定個人情報保護委員会、罰則）

以上