【マイナンバー法への対応(主要ポイント)】文責：河東岩夫(平成 27 年 05 月 25 日付)

JIPDEC「企業におけるマイナンバー制度」実務対応セミナー(平成 27 年 04 月 08 日付)資料から抜粋、一部、加筆

(1)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)(以下、GL という)で示されている安全管理措置

事項	内容	
安全管理措置の必要性	個人番号及び特定個人情報(以下、特定個人情報等という)の情報漏洩、滅失又は毀損(以下、情報漏洩等という)の防止等のため、特定個人情報を管理する。	
考えるべき視点	番号法により、特定個人情報等は利用する範囲を制限しているため、以下の視点で措置を講じる。 1)個人番号を取扱う事務の範囲：番号法で規定された取扱い範囲を超えないこと。 2)特定個人情報ファイルの範囲：番号法で規定された取扱い情報を超えないこと。 3)個人番号を取扱う事務に従事する従業者の範囲：利用することがない従業者が使える環境になっていないこと。	
手順	対策	GL 参照箇所
1)個人番号を取扱う事務の範囲を明確にする	個人番号関係事務(行政機関等に提出する書類に個人番号を記載する事務)を行う部署、システム、業務手順を明確にする。	第 4-1-(1)
2)特定個人情報ファイルの範囲を明確にする	個人番号を記載する事務を行う際に、必要な個人番号等の情報を保管する場所や形態を明確にする。	
3)事務担当者を明確にする	個人番号関係事務を行う部署(○○課、○○係り等)や担当(○○担当等)を明確にする。	Q&A Q10-1
4)基本方針及び取扱い規定等を作成する	個人番号を取扱う事業者として、基本方針(プライバシーポリシー、セキュリティポリシーに相当)を作成する。又、上記事務における取扱い規程等を作成する。	GL 別添安全管理措置 2A,B

(2)基本方針のポイント

事業者として、平成 27 年 10 月までには作成しておく必要がある(下記は GL 別添「安全管理措置、2A 基本方針の策定」を参照した雛形)。

平成 27 年 10 月 1 日
○○○株式会社

特定個人情報の適正な取扱いに関する基本方針

弊社は、特定個人情報を適正な取扱うため、以下を宣言します。

１．適正の取扱う事業者名称　　○○株式会社

２．遵守する関係法令等

・行政手続きにおける特定の個人を識別するための番号の利用等に関する法律
・個人情報の保護に関する法律
・個人情報の保護に関する法律ついての経済産業分野を対象とするガイドライン
・特定個人情報の適正な取扱いに関するガイドライン(事業者編)

３．安全管理措置

弊社では、特定個人情報の適正な取扱いのため、「特定個人情報取扱規程」を定めている。

４．ご質問の窓口

特定個人情報の取扱いについてのご質問は以下にて受け付けます。

【部署名】○○係
【email】
【電話又は FAX】

(3)取扱規程のポイント

特定個人情報の「取得、利用、保存、提供、消去・廃棄」の各段階にのおいて、その手順・安全管理措置等について明記し、個人番号を取得する従業員に示す必要がある。

構成	項目	記述する観点
総則	目的	特定個人情報の適正な取扱いを確保するために、法令・ガイドラインによって定めたことを明記、
	言葉の定義	規程内で使用する言葉を列記

構成	項目	記述する観点
	個人番号を取扱う事務の範囲	役職員や役職員以外(株主等)に関する個人番号関係事務の種類を明記
	特定個人情報の範囲	上記事務の範囲において、取得、利用において取扱う特定個人情報の範囲を明記
安全管理措置	組織体制	事務取扱担当者の部署や管理体制を明記
	教育・研修	継続的な教育や研修を行い、適正な取扱いを維持すること等を明記
	取扱状況の記録等	ログ、取扱い(記載・提出等)記録の保管方法等を明記
	事故等の対応体制	事故が起きた場合の対処方法を明記
	監査等	内部監査、外部監査の有無等を明記
物理的安全管理措置	区域の管理	管理区域、取扱区域の管理方法を明記
	機器類の盗難防止等	盗難防止策を明記
	漏洩対策等	持出し時の確認体制等を明記
	機器類の廃棄	機器類の廃棄時の手順を明記
技術的安全管理措置	アクセス制御	アクセス制御の方法や、権限の付与手順等を明記
	不正アクセスの防止策	ファイヤウオール、ウイルスチェック等を明記
	漏洩対策等	権限者以外が触れられない措置を明記
各プロセス	取得	利用目的・その通知方法、提供の要求・時期、収集制限、本人確認手順等を明記
	利用	特定個人情報ファイルの作成制限や利用制限等に関する規定を明記
	保管	正確性の確保、本人への透明性の担保、保管方法等に関する規定を明記
	提供	提供のための規定を明記
	開示・訂正等・利用停止等	開示・訂正等・利用停止等の規定を明記
	削除・廃棄	削除・廃棄の規定を明記
	委託	委託先の選定、安全管理措置等の規定を明記

(4)安全管理措置のポイント

削除の義務化、その記録の義務化(法定保存期間が過ぎたものは速やかに削除・廃棄しなければならない)	・「経済産業分野における個人情報ガイドライン」では、努力項目であるが、番号法では義務になっている。 ・削除のエビデンス(溶解処理をした際のマニュフェスト等)や削除した記録を取り、管理する。
管理区域(サーバルーム等)の例	・入退室管理を実施したサーバルームにデータを保管する。 ・サーバ内の共通社員マスターに個人番号を格納しているが、アクセス制御を行い、個人番号関係事務実施者しか扱えない状態にする必要がある。 ・施錠できる書庫に書面、又は電子媒体で保管し、取扱い記録をとる等。
区域(作業室等)の例	・個人番号を取扱うパソコンは、プライバシーフィルター等により、覗き見ができないようにする。 ・個人番号を記載する帳票を打出すプリンターは、個人番号関係事務実施者である担当者の専用にする等。

措置名	措置の内容	具体的な実施事項(例)
組織的安全管理措置	・取扱規定(前記)等を遵守していることを確認するルール ・システムログや利用状況の記録 **⇒ガイドラインでは、特定個人情報の削除・廃棄及びその記録は必須。又、システムログや記録の保存期間の規定がないため、社内で決めることが必要**	・特定個人情報ファイルの利用・出力状況の記録 ・書類・媒体等の持出しの記録 ・特定個人情報ファイルの削除・廃棄記録(委託した場合、これを証明する記録等) ・特定個人情報ファイルを情報システムで取扱う場合、事務取扱担当者の情報システムの利用状況(ログイン実績、アクセスログ等)の記録

(4)安全管理措置のポイント

措置名	措置事項	具体的な実施事項(例)
物理的安全管理措置	・特定個人情報等を取扱う区域の管理ルール(管理区域と取扱区域)	・入退室管理及び管理区域へ持込む機器等の制限等(管理区域) ・壁又は間仕切り等の設置及び座席配置の工夫等(取扱区域)
	・管理区域と取扱区域における機器及び電子媒体等の盗難等の防止	・特定個人情報等を取扱う機器、電子媒体又は書類等を施錠できるキャビネット・書庫等に保管する。 ・特定個人情報ファイルを取扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定する。
	・電子媒体等を持出す場合の漏洩等の防止	・持出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用等 ・目隠しシールの貼付を行う等
	・個人番号の削除、機器及び電子媒体等の廃棄(復元できない手段で削除又は廃棄)し、記録を残す。 ・上記の作業を委託する場合には、委託先が確実に削除又は削除したことについて、証明書等により確認する。	・焼却又は溶解、物理的な破壊等により、復元不可能な手段を採用する。
技術的安全管理措置	・アクセス制御(事務取扱担当者、及び特定個人情報ファイルを限定)	・ユーザ ID により、事務取扱担当者のみに当該特定個人情報ファイルへのアクセスを限定している。 ・特定個人情報ファイルは、社内ネットワークと遮断した環境でのみにアクセスを可能としている。
	・外部からの不正アクセス等の防止	・情報システムと外部ネットワークとの接続箇所に、ファイヤアウオール等を設置し、不正アクセスを遮断する。 ・情報システム及び機器にセキュリティ(ウイルス)対策ソフトウエア等を導入する。 ・導入したセキュリティ対策ソフトウエア等により、入出力データにおける不正ソフトウエアの有無を確認する。 ・機器やソフトウエ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、ソフトウエア等を最新状態にする。 ・ログ等の分析を定期的に行い、不正アクセス等を検知する等。
	・情報漏洩等の防止(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洩等を防止)	・通信経路の暗号化 ・システム内の特定個人情報ファイルにデータの暗号化又はパスワードによる保護を行う等。

(5)安全管理措置の遵守状況の宣言

手段	メリット	デメリット
1)P(プライバシー)マークを取得する。	“既に P マークを取得している情報保有機関については、情報保護評価書にその旨を記述することで、個人情報保護に対して適切な体制を採っていることを宣言することができる”と記載(平成 25 年度政府「中間整理」他)があり、当該認証によって、特定個人情報を含む安全管理措置が十分であることを対外的に明示できる。	取得のための資源(ヒト、モノ、カネ)が掛かる。
2)特定個人情報を取扱う部署を新設し、その部署において ISMS を取得する。		
3)自己宣言(自治体の評価書を流用してチェック)する。	自社のペースで準備ができ、費用が少ない。法人格を持っていなくてもできる。	事故が遭った場合に、説得力のある説明が可能なのかが不明。
4)管理の確実な事業者(例:P マーク取得)に委託する。	本人確認、安全管理措置の全て、又は、一部のリスクを転嫁できる。	「管理が確実である」旨の宣言をしている委託先が必要。

注)安全管理措置の遵守状況の宣言について、事業者は JISQ の規格と同様に記録の記載及び保持が必要(番号法には直接的な定めはない)。