マイナンバー安全管理体制構築
19 のステップ

社会保険労務士岩切事務所

マイナンバー安全管理体制構築 19 のステップ　目次

マイナンバー制度の概要_おさらい

マイナンバーとは、、、

日本に住所を有する個人一人ひとりに、市区町村長が住民票コードを元に、総務省令で定められた方法に従い作成、付番する 12 桁の番号。最後の一桁（12 桁目）は、正しく番号を生成することができたかを確認するための番号（チェックデジット）。

マイナンバー制度が生まれた背景

行政手続の効率化、国民負担の軽減、公平公正な社会の実現、

マイナンバーが利用する場面

税、社会保障、プラス災害対策のために使用される。それ以外では使用されない。

マイナンバーを付番された一個人として

マイナンバーを聞かれる、提供する相手は、、、行政、会社、金融機関だけ（2015/10/05 現在）。

＜会社として＞マイナンバーの提供を依頼するときは

マイナンバーが必要である理由を説明（明示）する。

＜会社として＞マイナンバーを取得（提供を受ける）手段は

対面（提示）、送付（書類提出）、電子的方法（IC チップ読み取り）の 3 つだけ。
電話で収集できるのは、過去に提供を受けたことがある相手だけ。継続的な関係の中で特別な場面に限定される。

＜会社として＞マイナンバーの提供を受けたら、、、

必ず本人確認＝番号確認＋身元確認を実施する。

	番号確認	身元確認
目的	提供されたマイナンバーが正しい番号か？	現に手続きを行っている者が 番号の正しい持ち主か？
確認書類	通知カード 個人番号が記載された住民票の（写） 住民票記載事項証明書	運転免許証、運転経歴証明書、旅券、 身体障害者手帳、精神障害者保健福祉手帳、療育手帳、在留カード、特別永住者証明書
	個人番号カード	

マイナンバー罰則

マイナンバーを取り扱う事務に関与する人だけが対象ではありません。誰でも罰則を受ける可能性があります。
背景が網掛けされている条文は、両罰規定＝当事者だけでなく関係者も罰則適用の対象です。
それだけマイナンバーは特別な個人情報なのです。

4 年以下の懲役もしくは 200 万円以下の罰金または併科

条	だれが	なにを	どうした
第 67 条	個人番号利用事務に従事する者またはしていた者が	特定個人情報ファイルを	正当な理由なく提供した

3 年以下の懲役もしくは 150 万円以下の罰金または併科

条	だれが	なにを	どうした
第 68 条	個人番号利用事務に従事する者またはしていた者が	個人番号を	不正な利益を図る目的で提供し、または盗用した
第 69 条	情報提供ネットワークシステムの事務に従事する者が	情報提供ネットワークシステムに関する秘密を	秘密を漏らし、又は盗用した
第 70 条	全ての人が	個人番号を	人を欺き、人に暴行を加え、若しくは人を脅迫する行為により、又は財物の窃取、施設への侵入、不正アクセス行為その他の個人番号を保有する者の管理を害する行為により取得した

2 年以下の懲役または 100 万円以下の罰金

条	だれが	なにを	どうした
第 71 条	国の機関の職員等が	特定個人情報が記録された文書等を	職権を濫用して収集した
第 72 条	委員会の委員等が	職務上知り得た秘密を	漏らし、又は盗用した

2 年以下の懲役または 50 万円以下の罰金

条	だれが	なにを	どうした
第 73 条	委員会から命令を受けた者が	委員会の命令に	違反した

1 年以下の懲役または 50 万円以下の罰金

条	だれが	なにを	どうした
第 74 条	全ての人が	委員会による検査等につき	報告、資料を提出しない、虚偽の報告、虚偽の資料を提出、職員の質問に対して答弁しないもしくは虚偽の答弁をした、検査拒否、妨害、忌避などをした

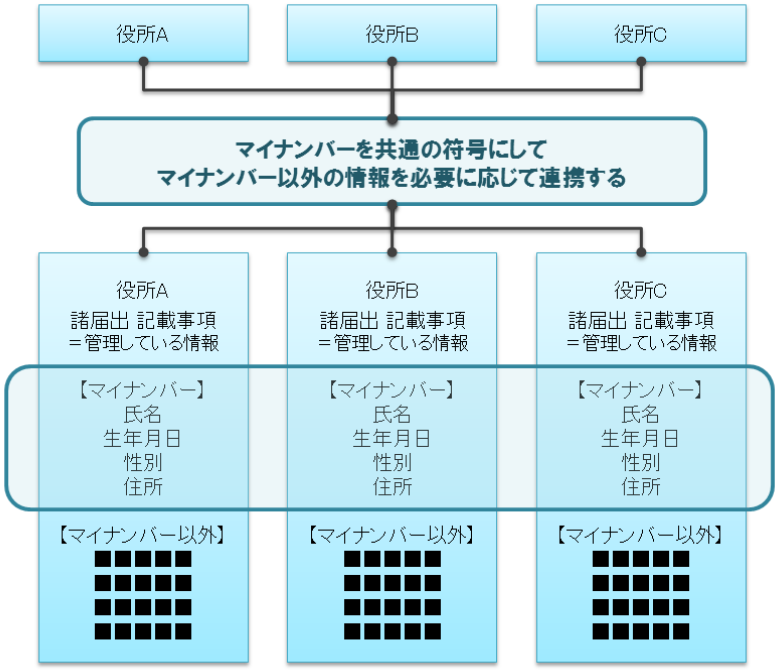
6 月以下の懲役または 50 万円以下の罰金

条	だれが	なにを	どうした
第 75 条	全ての人が	個人番号カードを	偽りその他不正の手段により交付を受けた

マイナンバーが漏れてしまったらどんな事態が想定されるのか？

紐付けされた情報。行政から漏れる可能性は、、、たぶん、、、ない

マイナンバーに紐付けされる各種の情報は、管理している行政機関ごとにセキュリティ対策を講じた上で保管されている（＝分散管理）ので、、、マイナンバーが漏れた＝紐付けされた情報が漏れる、、、は考えにくいです。各行政機関が管理している情報を盗み見ようと、盗み出そうとしない限り、紐付けされた情報が漏れるということはありません。



ですので、、、マイナンバーが漏れた、漏れてしまった結果、紐付けされた情報が漏れてしまう。
という心配は、実務上は必要ないでしょう。
だからといって、会社は「何もしなくていい」ということではありません。むしろ、、、

マイナンバーが漏れた、漏れてしまった、漏れたかも、、、この事態が会社にとっては最も脅威！

会社は「個人情報を漏らしてはいけない」という法的規制（個人情報保護法）を受けています。
これは同法に定める個人情報取扱事業者であろうとなかろうと同じです。
この違いは、法に定める安全管理措置を講じる義務があるかないかの違いでしかありません。

個人情報取扱事業者の定義（ガイドライン項番 14）

> 個人情報データベース等を事業の用に供している者であって、個人情報データベース等を構成する個人情報によって識別される特定の個人の数（個人情報保護法施行令で定める者を除く）の合計が過去 6 か月以内のいずれの日においても 5,000 を超えない者以外の者をいう。

マイナンバーは、個人情報の中でも特別な個人情報として位置づけられています。

だからマイナンバー法を個人情報保護法の特別法として制定し、マイナンバーを1件でも取り扱う事業者には、安全管理措置を義務付け、どのように安全管理措置を講じればよいのかをガイドラインで明確に示しています。

ガイドラインを参照することなく、可能な限りの手を打たないまま、マイナンバーを漏らしてしまえば、、、

✔漏れないよう管理すべき情報が漏れてしまった、、、
✔他の情報も漏れる可能性がある、、、
✔会社の情報管理に対する信用低下、会社の信用失墜、そして損害賠償請求対応、、、

個人情報流出件数　約 3504 万件　実態件数　2895 万件
漏えい事故の被害者（＝お客様）へ、お詫びとご報告の手紙の送付
お客様へのお詫びとして、500 円分の金券（電子マネーギフトまたは全国共通図書カード）を用意

*ざっくり計算して、、、35,040,000 件×（500 円＋82 円（普通郵便代）＝**20,393,280,000 円***

ベネッセの個人情報漏えい事件を思い出せば、どんな展開が待っているか？想像できるでしょう。

お詫びだけで、約 200 億円を用意しなければならない事態になってしまいました。
お詫び以外にも、事故調査にかかった費用、今後の対応にかかった費用、、、
お金だけが動いているのではありません。調査や対応は「人」が動いています。
その「人」は情報漏えい事故の真犯人ではないのに、企業の一員として、お客様、関係者に対応します、、、

全く想像できない方は、 **ベネッセグループ HP＞ベネッセお客様本部＞事故の概要** を読んでください。

なぜなら、万が一、情報漏えい事故を起こしてしまったときは、このような対応をしていかなければならないからです。

「大手だから、、、」という話ではありません。法律は会社の大きさを選びません。

事業活動に個人情報が必要なら、、、
「マイナンバー」に限った話ではありません。
「マイナンバー」を含め「個人情報」に対し、リスクマネジメントは欠かせない時代になってしまいました。

情報はそんなに簡単に漏れるのか？

保管されている、利用している情報は、勝手にあなたの手元から歩いて外に出ていくことはありません。
あなたの手の内にある限り、漏れることはないでしょう。だからといって侮っていては NG です。

✔デスクの上に個人情報が書かれた書類を、誰もが見える状態にして、置きっぱなしにしていた、、、

✔保管している金庫を開けっ放しにしていた、、、

✔あなたの視界に入っていない、多くの人が動いている場所に置かれているプリンターで、あなたしか見ることが許されていない情報が記載された書類を出力した、、、そして気を使った従業員があなたのデスクに届けてくれた、、、
従業員はその情報を暗記コピーしているかもしれません、、、
携帯電話でこっそり撮影し、面白半分に SNS(ソーシャルネットワーキングワークサービス)にアップロード(公開)してしまうかもしれません、、、

✔特定のメンバーだけが知っている暗証番号(パスワード)を、周りの人に聞こえるくらいの大きな声で発した、、、
あなたは単に、伝えるべき相手に確実に伝わるようハッキリとした声で伝えたつもりかもしれませんが、
それを聞いた誰かが暗証番号を悪用するかもしれません、、、
「私は○○○の秘密を知っている」「隠されると知りたくなる、、、」

これは個人情報に限った話ではありません。会社が保有する情報資産全てに当てはまる話です。

情報はいつでも、どこでも、漏れるチャンスがあります。だれにでも漏らしてしまうチャンスがあります。
情報が 1 人で勝手に出て行くことはありません。

コンピューターウィルスは？と思われる方もいらっしゃるでしょう。
メールを開いたらウィルスが侵入した、、、という事例は枚挙に暇がないようです。
メールを開いた張本人は「私は悪く無い」と言い張るかもしれませんが、、、ウィルスに感染させたのはメールを開いた張本人以外にはいません。

差出人(真犯人)は、メールの受取人に対して、悪意があるから、ウィルスを忍ばせています。
受取人は、それに気づかず、勝手に差出人を信用して、、、メールを開いた張本人は否定するかもしれませんが、、、
犯人はそれを計算してウィルスを送り込みます。

「ポチッ」と押すだけ、「カチカチっ」とダブルクリックするだけ、、、
犯人は受取人に簡単な操作をさせることでウィルスを仕込み、そして、情報を抜き出してしまうのです。
メールを開いた張本人は、犯人の手のひらの上で弄ばれているだけに過ぎません。
コンピューターウィルスもとどのつまりは「人」でしかありません。

だから、安全管理体制を整える。

何のために情報があるのか？

情報は、使う、でも守るべき情報は守る。
この相反する2つの方向をコントロールするのが安全管理措置の目的です。

これをマイナンバーに置き換えるなら、、、
幸いなことに、マイナンバーは、使用する範囲、場面が限られています。

マイナンバーの基本原則

集める　→　要らないマイナンバーは集めない

守る　→　要らないマイナンバーは廃棄する

利用する　→　決められた場面でしか使わない

そして　→　集める、守る、利用する、の履歴を記録する

これを柱に安全管理体制を構築すれば、、、
可能な限りマイナンバーに触れる時間を短くし、マイナンバーが記載された保管書類に接触する機会を少なくしながら、かつ、行政手続をスムーズに処理する体制を構築できます。

先日個人情報保護法が改正され、個人情報取扱事業者の要件である 5000 要件の廃止が確定しました。
いずれは、個人情報を1件でも取り扱っていれば、個人情報取扱事業者となり、法的規制を直接に受けます。
個人情報保護法の安全管理措置ガイドラインの基本構成は、マイナンバーのガイドラインとほぼ同じです。

いま手抜きすることなく、マイナンバー安全管理体制を構築すれば、個人情報の安全管理体制にも転用できます。
将来確定している事務負担を小さくするためにも、できることからコツコツ進めていきましょう！

情報セキュリティ対策　4 つの基本原則

1.　接点を減らす

使う、守る情報が保管されている場所が少なければ少ないほど、守るべき場所が明確になるので、より効果的な対策を検討でき、それに対して資源を集中しやすくなります。

100%アナログの場合を想像してください。
書類が散在していれば、あらゆるところに対策を検討する必要がありますが、一つにまとめられていれば、それだけに集中して検討できます。

デジタルも同じ発想です。デジタルは、非常に優れた道具です。

アナログでは面倒なこと、手間のかかることがいとも簡単にできてしまいます。

アナログではそうは簡単にできないこと、、、コピーを想像してみてください。

コピー機がなければ、すべてを手書きで書き写さなければなりません。

コピー機はあっても用紙がなければ、、、コピーは作れません。

しかし、PC であれば、ctrl キーを押しながらドラッグ・アンド・ドロップ、名前をつけて保存、、、簡単操作で、あっという間に、コピーを作成できます。PC 以外に特別な道具は必要ありません。電話帳 1 冊分相当のデータのコピーもほんの僅かの時間で作成できてしまいます。

「アドレス帳」、、、あなたは何個持っていますか？全部で何件保有していますか？

- ✔現在使用しているパソコンにインストールされている E メールソフトのアドレス帳
- ✔現在使用していないパソコンにインストールされている E メールソフトのアドレス帳
- ✔現在使用している携帯電話のアドレス帳、
- ✔現在使用していない携帯電話のアドレス帳
- ✔インターネットメールサービス（Yahoo!や google など）を利用していればそのアドレス帳
- ✔年賀状作成ソフトなどに保存しているアドレス帳
- ✔これらのバックアップデータを保管していれば、そのアドレス帳
- ✔手帳、アドレス帳など手書きで書かれたアドレス帳

意識して管理しなければ、あちこちに散在していることと思います。

アナログに変換したらどれくらいの量になりますか？

アナログと違い、デジタルは人間の知覚でその質、量を判断することができません。

電話帳一冊分のデータが入ったファイルも、中身の無いファイルも、見た目は同じです。

もう使っていないから、、、私人としての発言なら許容範囲かもしれませんが、、、

仕事でアドレス帳を使っている（＝事業の用に供している）のなら、、、そんな言い訳は通用しません。

改正された個人情報保護法の施行日は未定ですが、個人情報取扱事業者として適用を受けることは確定しています。

いずれは、マイナンバーだけではなく、アドレス帳に対しても安全管理措置を講じなければならないということです。

作成したデジタルデータが多ければ多いほど、

保管場所を決めないで散らかして保有していれば保有するほど、情報漏えいリスクは高くなってしまいます。

これからもデジタルを活用するのであれば、何を、どこに、を意識し、保管場所である接点の数を減らしましょう。

2. 接点に接触できる人を制限する

保管場所に接触できる、開閉できる人が多ければ多いほど情報漏えいリスクは高まります。

「人を制限する」ことはセキュリティ対策の成否を左右する重要な要素です。

✔他人の個人情報をぺらぺらしゃべるのは非常識、、、
✔この情報は機密情報だから、経営陣しか接触できないのは当たり前、、、

こんな感じで「当たり前」に任せていると、大きなしっぺ返しを食らってもおかしくはありません。

本当に守りたい情報がそこにあるのなら、、、その接点に接触できる人を制限しましょう。

3. 接点に危険物を持ち込まない

保管場所を特定した、接触できる人を制限した、、、そこに危険物を持ち込まれたら、、、

USB メモリ、スマートフォン、携帯電話、デジタルカメラなどのポケットに入れて持ち歩けるサイズの記憶媒体からタブレット、モバイル PC などかばんに簡単に収納できるサイズの記憶媒体まで、簡単に、かつ、大量のデータを保存できるアイテムが充実しています。

いまや SNS が充実し、インターネットにアクセスできる環境があれば、だれでも、インターネットの世界に向けて情報発信することができる時代です。

危険物とは、、、守りたい情報を改造・改変、盗み見、盗聴、コピー、取り出し、持ち出し、破壊、、、されるような行動や道具のことを言います。

多くの会社では勤務に際し「■■■■■■■■■■してはならない」といった「そんなの当たり前だろ」と言いたくなるような事項を、入社時説明会や労働契約書、就業規則などの機会で従業者に伝えていることでしょう。
それと同じ考え方です。

ピンと来ない方は、花火工場のオーナーになって想像してください。

花火の原料である火薬保管庫。ここが爆発してしまえば、、、経営は成り立たなくなってしまいます。
火薬保管庫を守るために、ここに入場制限、持込制限のルールを作成したいと考えています。
あなたならどんなルールを設定しますか？その設定が浮かんだのはなぜですか？

情報は守るために存在するではありません。使う、活用するためにあります。

保管場所で保管している情報の活用の程度に応じ、持込物の禁止、許可を決めることも重要な要素です。

4. 接点を守る人を置く

どんなに立派なセキュリティ対策を講じても、、、

100％完璧な対策はありません。また、そこに番人がいなければ、対策が機能しているかどうかを確認できません。
対策を講じたら、対策が活きるように動かす＝番人とユーザーの連携がとれてはじめて仕組みとして機能します。

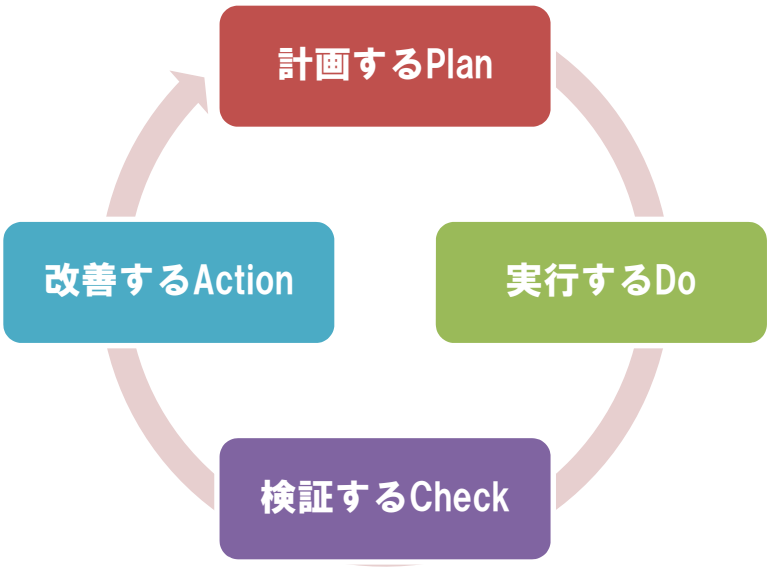
情報セキュリティ体制の登場人物の例

情報セキュリティを統括する責任者

情報セキュリティの仕掛け人＝企画、設計、導入、、、、

情報セキュリティの仕掛けに従いを運用する人

情報セキュリティの運用上の問題を分析し、これからの対策を検討する人



PDCA サイクルが循環し、機能すればするほど、より確かなセキュリティ対策につながります。

マイナンバー安全管理措置の全体像

まずは全体像を把握する

いつ、どこで、どんなときに、どのようにして、マイナンバーの提供を受け、保管し、利用し、廃棄するのか？
その全体を把握できなければ、どこに、どのようなセキュリティ対策を講じればよいのか分かりません。

その全体像を把握するための資料として、■マイナンバーPmap をご用意しました。

特別なシステムを導入していない限り、100％アナログ対応、あるいはアナログ＋デジタルのスタイルになるでしょう。
なので、このマイナンバーPmap は、データは PC で保管するけど、基本は「紙」。を前提に作成しています。

■マイナンバーPmap　スライドリスト

- □ 賃金計算を例にした雇用管理情報の動き
- □ 0. 個人情報等が動く環境＝安全管理措置の検討
- □ A ＜取得 1＞ 利用目的明示から提供依頼
- □ B ＜取得 2＞ 提供依頼後から本人確認まで
- □ C ＜取得 3＞ 本人確認後から取得完了（保管）まで
- □ D ＜利用 0＞ 行政手続書類を作成するとき
- □ E ＜利用 1＞ 行政手続書類（特定個人情報 F）の作成
- □ F ＜利用 2＞ 行政窓口への届出
- □ G ＜保管＞ 行政手続控の保管（選別～保管）
- □ H ＜廃棄＞ マイナンバーの削除、廃棄
- □ I ＜廃棄＞ 特定個人情報ファイルの削除、廃棄
- □ O ＜アクセス制限＞ カギ解錠
- □ L ＜アクセス制限＞ カギ施錠
- □ 情報漏えい事件発生時の対応
- □ 情報漏えい_安全管理組織図_smp

Pmap とは、、、

当事務所が勝手に名前をつけました。P＝Process（過程）、map は文字通り「地図」です。
基本構成は、横軸に登場人物、縦軸は時間軸。
似たような map にフローチャートがありますが、フローチャートは主人公（登場人物）をメモしない限り、map に登場しないのが一般的な map です。人にフォーカスしたフローチャートが Pmap です。

Pmap「個人情報等が動く環境＝安全管理措置の検討」を見れば一目瞭然　ここに一手が必要です。

個人情報等が動く環境＝安全管理措置の検討は、マイナンバーを含めた個人情報がどんな環境に置かれているかを示しています。委託先には、当事務所に労働社会保険の事務手続代行顧問を依頼されている場合の、当事務所のシステムをサンプルとして表示しています（対外的に公表していないシステム名は非表示にしています）

これを見ると明らかです。

登場人物をまたいだ部分。そこがセキュリティの弱い部分です。

ここにどのような道具や手段を用いればセキュリティを高めることができるのか？

Pmap は、このように時間を追いながら、○○○すると●●●。だから□□□する。と読んでください。
そして、このファイルを加工して、オリジナルの Pmap を作成してください。
できた Pmap はマイナンバー業務をする際は、手元に置き、確認しながら進めることをオススメします。

A から H(I)がマイナンバーの取得から廃棄までの一連の流れです。

こうしてみると、実際に手を打たなければならない場面は多くあります。お気付きになった方も多いと思いますが、

色んなシーンで「01 記録簿」「02 ログ」「11 処理簿」が出てきます。

これは当事務所が設定したのではありません。ガイドラインにかかれているので配置しただけです。

記録を残さなければ、事故が発生した場合、その事実を確認できない。

国はそこまで会社に要求しています。
これを 100%アナログ対応で考えると、、、記録簿に記録するだけでも煩雑な事務になってしまいます。

システムを導入すれば、記録簿を作成するのは、事務処理簿だけになるかもしれません。

それ以外の記録簿は、すべてアクセスログという形でシステム内に保存されるので、いつ、どこで、だれが、なにを、どんな目的でアクセスを開始し、終了したかを日または時間単位で確認できるようになります。
システムによっては事務処理簿もなくなる可能性もあります。

O と L はカギの開閉の Pmap です。

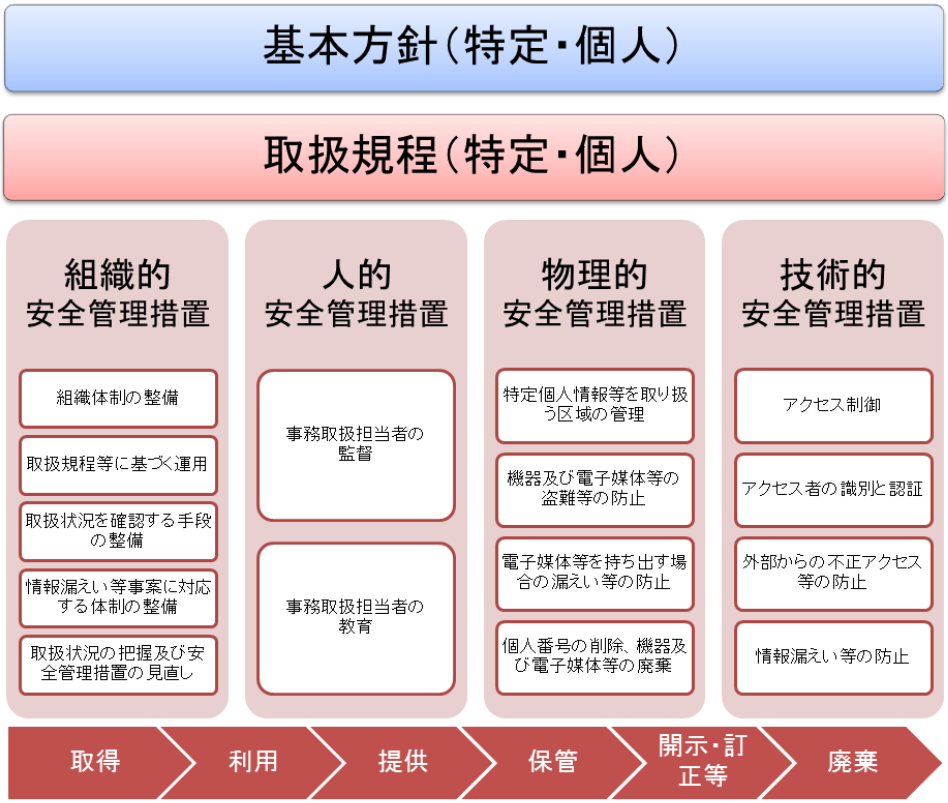
O=Open　L＝Lock　です。アナログなら、、、Pmap　のように、カギを受け取ってからロッカーや金庫を開く、カギにカギを掛ける。これくらいの作業しかありません。

デジタルなら、、、

✔パソコンを立ち上げたとき、、、ID、パスワードを入力する、顔認証、指紋認証する
✔サーバーやクラウドなどの保管場所にアクセスするとき、、、ID、パスワードを入力する、顔認証、指紋認証する
✔外部記録媒体を接続するとき、、、金庫から鍵を開けて取り出し、接続設定を解除してから接続する、、、
✔ファイルを開くとき、、、パスワードを入力する、、、閉じるとき、、、保存確認、パスワードを入力する、、、
デジタル機器の活用方法によっては、アナログのカギに相当する工程が多く想像されます。
活用方法に応じて、オリジナルのデジタル版カギの開閉 Pmap を作成してください。

国がガイドラインで示す安全管理措置の全体像

マイナンバー法では、4 つの安全管理措置を義務付けています。



デジタルを活用している方、個人情報の取扱には人一倍うるさい、、、
そのような方にとってはわかり易い内容かも知れませんし、アタリマエだよ、、、と思われるかもしれません。

そうでない方は、、、
言葉だけを読むと複雑に感じますが、耳慣れていないだけで、決して難しい話ではありません。
わからなくなったときは、「もし 100％アナログ管理だったら、、、」に置き換えてイメージしてください。

デジタルは、アナログでは面倒なこと、手間がかかる、時間がかかることを、簡単にしてくれる道具に過ぎません。
パソコンが普及した今日、計算機は“算盤のみ”で経理・会計業務をしている方は極々少数派でしょう。
電卓のみという方も少なくなってきているのではないでしょうか？
表計算ソフトも、会計ソフトも、アナログでやっている作業の一つ一つをプログラムした道具でしかありません。

マイナンバーは個人情報中の中でも特別な個人情報。
これからお伝えすることは、マイナンバーにフォーカスを当てていますが、、、、
経済産業省の個人情報ガイドラインにかかれている安全管理措置もほぼ同じです。
マイナンバーを個人情報に置き換えれば、、、個人情報保護対策にもつながります。

特定個人情報ガイドラインをマイナンバー安全管理体制構築の順番に分解し、並べ替えました。
この順番で、安全管理体制を構築してください。

規程の作りこみなどには時間がかかるかもしれませんが、
全体像＝アウトラインは 3 日もあれば十分できるはずです。

マイナンバー安全管理体制構築 19 のステップ

1. ＜原則 4＞【組織的】マイナンバーを取り扱うにあたっての基本方針を策定する

法律上作成義務はありませんが、策定する(させる)ことを前提に国はガイドラインを構築しています。
基本方針を策定することは、社内、社外に対して、会社の姿勢をハッキリ明示することに他なりません。

ガイドラインでは、基本方針に定める項目として、次のように例示しています。

≪手法の例示≫
＊ 基本方針に定める項目としては、次に掲げるものが挙げられる。
・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

■特定個人情報等の適正な取扱いに関する基本方針_smp

会社名と問い合わせ窓口を書き換えれば、出来上がりです。
早速策定し、従業者からマイナンバーを実際に収集する告知をするまでの間に、周知、公開してください。

参照:ガイドライン安全管理措置 1-D、2-A

2. ＜原則 1＞【組織的】マイナンバーを利用する目的を特定し、明示する。

明示するとは、、、マイナンバーを提供してもらう相手に、何のためにマイナンバーを提供してもらうのか？
その意図を確実に伝えることをいいます。
マイナンバーを利用する場面は限定されているので、もう出来ています。

■マイナンバー提供のお願い_smp

宛名に相手の名前、差出人に、会社名、窓口、担当者名を記入。最後に通知する日付を記入すれば完成です。
マイナンバー取得告知文書のひな形としてご活用ください。

就業規則に盛り込めば、それだけで OK なのでは？

採用決定から採用日までの間に就業規則を閲覧する機会はありますか？
取引先である個人事業主が就業規則を閲覧する機会はありますか？
通知書を発行する手間をどうしても省きたいのなら、、、御社のウェブサイトに公開してください。
そしてウェブサイトに公開していることを相手に伝えてください。それが最も手っ取り早い方法です。

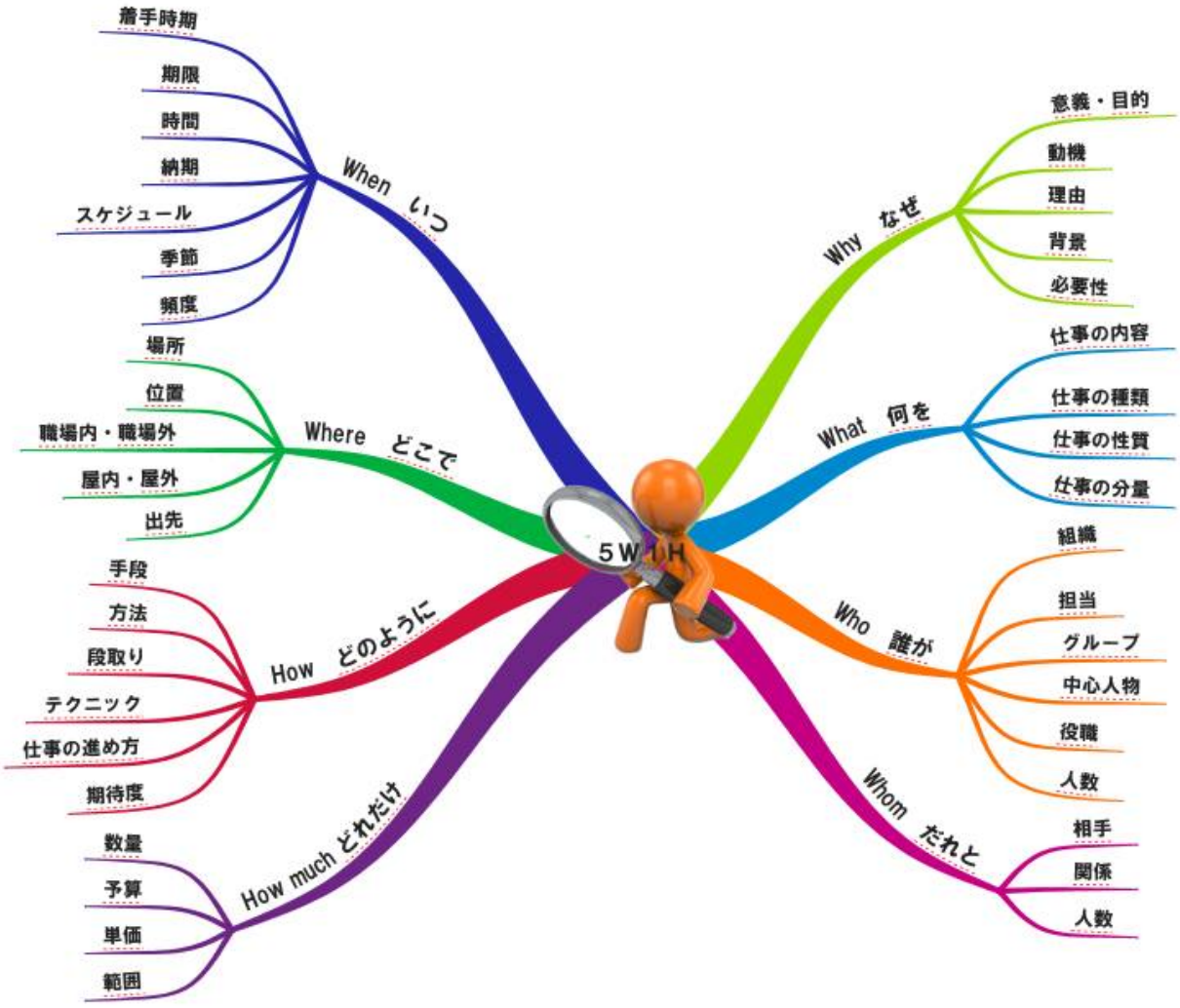
参照:ガイドライン安全管理措置 2-B 関連

3. ＜原則 1＞【組織的】マイナンバーを利用する業務の範囲を特定する。

マイナンバーを利用する場面は、行政手続の場面でしか使いません。

それ以外、、、例えば
社員番号をマイナンバーに置き換える(変更する)、従業者について会社が保有しているすべての情報をマイナンバーに紐付ける、、、そのような使い方はできません、やったら法律違反(＝マイナンバー法第 19 条違反)です。

業務の範囲を特定するということは、、、
いつ、どこで、だれが、なぜ、どのように、どんなときに、だれが、何のために、利用するのかを、マイナンバー業務に従事する従業者が確認できるリストを作成するということです。



■11 特定個人情報ファイル事務処理簿の中に、手続一覧があります。これが完成形です。

参照:ガイドライン安全管理措置 1-A

4. ＜原則 1＞【組織的】マイナンバーに紐付けされる情報の範囲を特定する。

手続書類にはマイナンバーの他、多くの個人情報(以下「個人情報等」といいます)を記入します。
それらの情報は、マイナンバーに紐付けされた情報として扱われることとなります。

特定するとは、、、「どのような個人情報等を記入するのか？」を、マイナンバー業務に従事する従業者等が確認できるリストを作成するということです。

先ほど出てきました■11 特定個人情報ファイル事務処理簿の手続一覧に組み込まれています。
一つ一つの項目を網羅することが理想ですが、これらの項目は、行政が指示する項目以外の何モノでもありません。
裏を返せば、これ以上紐付けたらNG＝法律違反です。

マイナンバー制度の進化とともに記入する項目は変わることが予想されます。
■11 特定個人情報ファイル事務処理簿に書いているように包括的に記載すれば十分、これが完成形です。

参照：ガイドライン安全管理措置 1-B

5. ＜原則 2＞【組織的・人的】マイナンバー業務に従事する担当者を決める。

情報セキュリティ対策の基本原則です。情報への接点を小さくすることの一つが「人の限定」です。
会社がマイナンバーを利用する場面は、税分野と社会保障分野ですので、従業者に限らず、個人事業主と取引していれば、その取引先である個人事業主のマイナンバーを取り扱うこととなります。大別すると2つの窓口が必要です。

また、複数の事業所（本社と支店）がある場合で支店でマイナンバーを集め、本社に報告する場合には、それぞれに窓口をおくこととなります。会社の事情に合わせて、マイナンバーを収集する窓口（担当者）を明確にしてください。

担当者がいる＝担当者を決める人がいる＝その人は責任者？
担当者だけを決めるのではなく、その責任者も決め、役割を決めてください。

担当者が複数いる場合、部署単位で設定してもOKです。
ただし、責任者は役職、個人名など限定してください。そうしないと責任の所在が明確にならないからです。

担当者と責任者の設定例は■特定個人情報取扱規程_smp 第10条、第11条をご参照ください。

参照：ガイドライン安全管理措置 1-C、2-Ca、2-Da、2-Db、2-Fa

6. ＜原則 1＞【組織的】事務委託の関係を整理する

社会保障分野（労働社会保険事務手続）なら社会保険労務士、税分野なら税理士、マイナンバー取得代行を外注するのであれば、その外注先など、マイナンバーを利用する業務の範囲には、自社以外に第三者が存在することがあります。

受託者（委託先）が、番号法に基づいて、自ら（委託者）が講じるべき安全管理措置と「同等」の措置を講じているか？
講じていなければ、安心して委託することはできない、、、これは当然の心理でしょう。

それを明文化した規定が、マイナンバー法第11条に定められています。

> 個人番号利用事務等の全部又は一部の委託をする者は、当該委託に係る個人番号利用事務等において取り扱う特定個人情報の安全管理が図られるよう、当該委託を受けた者に対する必要かつ適切な監督を行わなけ

ればならない。

受託者がずさんな安全管理措置しかしていなければ、できていなければ、、、そして事故を起こしてしまうと、、、受託先を決めた委託者に責任の一端があるということです。従って、受託者がさらに外部に委託した場合、、、その委託先に対しても間接的な監督をする必要があるという構図になっています。

ガイドラインでは、以下ように記されています。

委託先の選定について

委託者は、委託先において、番号法に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。

委託契約の締結について

契約内容として、秘密保持義務、事業所内からの特定個人情報の持出しの禁止、特定個人情報の目的外利用の禁止、再委託における条件、漏えい事案等が発生した場合の委託先の責任、委託契約終了後の特定個人情報の返却又は廃棄、従業者に対する監督・教育、契約内容の遵守状況について報告を求める規定等を盛り込まなければならない。

外部に委託すること＝社外（委託先）にて、自社のマイナンバー執務・管理室を作ることと同じです。

外部委託する場合には、委託先の情報セキュリティ対策の状況を必ず確認してください。

外部委託を受ける立場より、、、

委託する側は「外部委託先が実際にどのような情報セキュリティ対策を実行しているか確認してください」と言われても、どう確認すれば良いのかわからないと思います。また、外部委託先から口で説明されても、契約書、覚書を見せられても「よくわからない、、、」が本音だと思います。
最近では、ノートパソコンやスマートフォンを持ち歩いて仕事をしている外部委託先も多いです。

「この外部委託先は大丈夫かな？」と思ったら、、、

あなたの目の前で外部委託先が PC 操作する機会があれば、「デスクトップ画面を見せて」とお願いしてみてください。

「見せれない」と断った場合、そこには他人に見られては困る何かがあるということです。
見られては困る何かがあるにもかかわらず、誰かに（相手に）見られてしまう可能性が高いシチュエーションで PC を使用する、、、「情報セキュリティ」に対する意識が低い可能性＜大＞です。

そのような機会がなければ、、、こんな質問（話題）をしてみてください。

□持ち歩いているモバイルツールは暗証番号、生体認証など、ロック設定していますか？
□メールは暗号化通信していますか？
□BCC メールと CC メールの使い分けの基準はありますか？
□暗証番号は何桁以上の設定をするのが望ましい、、、という基準はありますか？

□事務系アプリケーションで作成したファイルの暗号化、パスワード設定方法を知っていますか、実践していますか？
□（クラウド活用など）4 桁のログインパスワード以外のロック設定を知っていますか？活用したことがありますか？
□（クラウド活用など）「2 段階認証」の存在を知っていますか？実際に設定したことはありますか？

この程度の質問に回答できない外部委託先は、、、
委託を受ける立場としての「情報セキュリティ」に対する意識が低い可能性＜大＞です。
きっとＥメール添付ファイル、、、個人情報がたくさん詰まっていても、、、パスワードなしで送信していることでしょう。

実際に業務で使用する手段に対し、外部委託先自ら考えをもって情報セキュリティ対策を講じ、できることは試し、これで情報が漏れたら仕方がない、、、と考え対策をしている外部委託先なら、、、大きな心配はいらないと思います。

参照：ガイドライン安全管理措置 1-A、2-B 関連

7. ＜原則 1＞【物理的・技術的】マイナンバー業務を遂行する場所を特定する。

多くの人が集まるところでマイナンバー業務を行えば、周りからは情報が丸見えです。
見えてしまうものを「見るな」「のぞき見厳禁」といっても視界に入ってしまえば、見えてしまいます。
この程度で「セキュリティ措置を講じた」とは誰も認めてはくれないでしょう。

どんなに堅牢なセキュリティ体制を構築しても、
現実にマイナンバー業務を遂行する場所が開放的な環境であれば、守るべき情報は守れません。

マイナンバー業務を遂行する場所＝マイナンバーを取り扱える場所を特定してください。
この場所を「取扱区域」といいます。マイナンバーを目で見える状態にできるのは、この「取扱区域内」だけです。
マイナンバーに目隠しすることなく、この取扱区域から外に出すことは、、、NG です。

理想は、、、、窓がない、扉がない、カメラがない、外界に通じる手段が何もない、、完全密室です。
マイナンバー業務遂行する場所としてそんな密室を準備しても、中に入ることができなければ、何もできません。
この理想に少しでも近い空間を作ってください。

少しでも近い、、、できる範囲で OK です。新しく特別な空間を準備する必要はありません。
マイナンバー業務を遂行している現場は、情報漏えいリスクが非常に高い状態になっています。
事務取扱担当者、責任者以外の人には、マイナンバーを＜見せない、見えない、のぞかれない＞を実現できる空間を作ってください。

ガイドラインでは取扱区域について、次のように例示しています。

＊入退室管理方法としては、ICカード、ナンバーキー等による入退室管理システムの設置等が考えられる。
＊取扱区域に関する物理的安全管理措置としては、壁又は間仕切り等の設置及び座席配置の工夫等が考えられる。
＊管理区域に関する物理的安全管理措置としては、入退室管理及び管理区域へ持ち込む機器等の制限等が考えられる。

取扱区域の外にマイナンバーを持ち出さなければならないシーンは限られています。

✔行政へ手続をするために、行政窓口に提出する、

✔代表者印押印のために、一時的に取扱区域の外に出る、

✔委託先に業務を依頼するためにマイナンバーを預ける、など、、、

取扱区域の外に持ちださなければならない場合には、シーンに合わせて、中身が透けて見えない封筒に入れる、マイナンバーに目隠しするなど、マイナンバーが見えない状態にしてから取り扱ってください。

郵送でマイナンバーを行き来させる場合、、、

普通郵便は NG です。普通郵便が郵便事故に遭遇しても、その事故を確認できる手段がないからです。

最低でも簡易書留や配達記録郵便などの「受取事実が確認できる、記録が残る」オプション郵便を利用してください。

これは従業者からマイナンバーの提供を受ける際にも、念頭において検討しなければならない大切なことです。

担当者、責任者は「普通郵便は NG」を頭の中にしっかり叩き込んでください。

ここで注意を要するのは、マイナンバーが記載された書類を PC から印刷するとき、、、です。

業務をするスペース(座席)とプリンターは離れた場所に設置していることが多いと思います。

複数人で 1 台のプリンターを共有していることもあるでしょう。

プリンターがマイナンバー業務遂行に必要不可欠なら、プリンターは取扱区域内に設置してください。

印刷したら「後でまとめて取りに行こう」と放置せず、すぐに取る習慣をつけてください。

参照:ガイドライン安全管理措置 2-Ea、2-Eb、2-Ec、2-Fa、2-Fb

8. ＜原則 1＞【物理的・技術的】マイナンバーが記載された書類の保管場所を特定する。

取扱区域が「作業する場所」なら、そこで作成された書類

マイナンバーが記載された書類の「保管場所」も特定してください。この空間を「管理区域」といいます。

理想の空間は取扱区域と同じです。

アナログで保管する場合

カギがなければ開けることができない金庫やキャビネットを取扱区域内に配置してください。

デジタルで保管する場合

限定された人(＝事務取扱担当者、責任者)以外の人がアクセスできない、開くことができないシステムまたは仕組みを用意してください。用意する場所は、取扱区域内であってもなくても OK です。

不思議に思われるかもしれませんが、デジタルデータのすべてを「クラウド」で管理するという選択肢もあります。

利用する範囲によって選択するクラウドシステムは異なりますが、今日ではこのような選択もできるようになりました。

社内にネットワークを構築している場合、そのサーバー内の一部に、アクセス権限を設定した保管場所を用意しても OK です。

参照:ガイドライン安全管理措置 2-Ea、2-Eb、2-Ec、2-Fa、2-Fc

9. ＜原則 1＞【物理的・技術的】マイナンバー法の制約を受け厳重に保管しなければならない書類はたったの 2 種類

マイナンバー法の制約を受ける書類は、「マイナンバーが記載された書類＝特定個人情報ファイル」です。
実務上、特定個人情報ファイルは 2 種類しかありません。

1. 保管しているマイナンバー＝マスター

利用目的を網羅的に伝えた上で取得、本人確認したマイナンバーは、利用目的が続く限り（退職するまで、取引を終了するまで）、会社で保管し、再利用できます。再利用の際に、改めて対象者に提供依頼することもなければ、本人確認をする必要はありません。
必然として、会社はマイナンバーを、必要の範囲内で、何らかの形で、保管し続けることとなります。

マスターとは、、、
情報処理の基本データが格納された書類のこと。
情報処理の考え方、手段、方法によりマスターを構成する要素（項目）は様々ですが、人事労務管理を例にすると、従業者の基本情報（社員番号、氏名、住所、性別、生年月日、労働条件、雇用保険の適用、社会保険の適用など）を一つにまとめていれば、それがマスターです。

■マイナンバーPmap_賃金計算を例にした雇用管理情報の動き　をご参照ください。

マイナンバー管理で作成するマスターは最大で次の 2 つです。
✔マイナンバーのマスター＝本人確認書類
✔特定個人情報のマスター＝個人番号管理ファイル
「最大で」とお伝えしたのは、提供された本人確認書類は必ずしも会社で保管する義務は無いからです。本人確認を確実に行い、正確に個人番号管理ファイルを作成して入れば、それをマスターとして扱っても良いとされています。

2. 行政手続のためにマイナンバーを利用（記載）した書類

マイナンバーを記入して行政に手続きする書類は多くありますが、、、、

厚生労働省管轄（社会保障分野）
通知書の発行をもって適正に手続きが行われたものとみなす。という考えのもと、手続控（行政が発行する通知書等）にはマイナンバーは原則記載しないこととなっています（2015/1005 現在）。
したがって、、、行政から発行される手続控はすべて「個人情報等」の範囲で管理します（今までと同じです）。

国税庁・税務署（税分野）
給与所得者の扶養控除等（異動）申告書、給与所得者の保険料控除申告書兼給与所得者の配偶者特別控除申告書、退職所得の受給に関する申告書などは、本来税務署に提出する書類ですが、現実には税務署に提出しません。その代わり、税務署が会社に対して提示等を求めれば提示しなければならない書類として、会社が法定保管年限まで保管しなければならない書類です。
このような取り扱いを受ける書類だけを特定個人情報ファイルとして保管すれば OK です。

なお、本人に交付する源泉徴収票は、マイナンバー記載が不要となりました（2015/10/02 所得税法等改正による）。

行政窓口で手続きする際（特に年金事務所の場合）、すぐに公式の手続控（通知書等）が発行されません。
そのため、手続控として、届出書類のコピーを用意し、そのコピーに受付印をもらい、それを手続控として管理している方も多いと思います。

マイナンバーの記載が始まった後に、同じ方法をそのまま継続すると、コピーは特定個人情報ファイルとなってしまいます。自らマイナンバーを漏えいするかもしれないチャンスを増やしていることと同じです。

もし「コピー＋受付印＝手続控」として保管する場合には、コピーに記載されているマイナンバーは「マスキング（目隠し）」し、個人情報等ファイルとしてレベル下げしてから保管するしてください。

行政が分散管理するなら、会社も分散管理。
マイナンバーが記載された書類に接触する機会を少なくすればするほど、情報漏えいリスクは低くなります。

マイナンバーに接触する機会は、マイナンバーのマスターに限定し、保管すべき特定個人情報ファイルは厳重に保管するだけにする。

実務上、日常的に活用しなければならない特定個人情報ファイルがあるのであれば、特定個人情報ファイルそのものを活用するのではなく、マイナンバーをマスキング（目隠し）したコピーを活用する。

これがマイナンバー漏えいリスクを確実に小さくする方法です。

参照：ガイドライン安全管理措置 2-Ea、2-Fa、2-Fb

10. ＜原則 1＞【物理的・技術的】マイナンバーが記載された書類の保管期限を特定する。

マイナンバーが記載された書類の保管期限は法律で定められています。
■11 特定個人情報ファイル事務処理簿に保管期限を記しています。これを参考に会社用に加工してください。

マイナンバーが記載された書類＝特定個人情報ファイルの保管原則は、、、

要らなくなったら、即廃棄。
必要以上に保管していると、行政は何を言い出すか分かりません。
行政は、御社の管理状況を監視する立場にいるので、行政が「それは無駄な保管だよね。何か意図あるの？もしかして、、、、」疑惑の目を向けるのは必至。そう考えておきましょう。
はじめからこのように考えていれば、ストレスは小さくなるはずです。

参照：ガイドライン安全管理措置 2-Ec、2-Ed、2-Fc、2-Fd

11. ＜原則 1＞【物理的・技術的】マイナンバーが記載された書類の廃棄時期を特定する。

特定個人情報ファイルとして保管する書類は限られているのは、先にお伝えしたとおりです。
税分野の書類に限られますので、ズバッとお伝えします。

法定保管年限を超えたら即廃棄。

税分野の書類の保管年限は「7 年」です。
2016 年に申告した書類＝完結の日は遅くても 2016 年 1 月 31 日。その 7 年後は、、、2023 年です。
2023 年の 2 月になったら廃棄する。これで OK です。

参照：ガイドライン安全管理措置 2-Ed

12. ＜原則 1＞【物理的・技術的】マイナンバーが記載された書類の廃棄方法を特定する。

おおよそ、このような方法が考えられます。

アナログの場合
✔燃やす
✔完全に復元できないほどに裁断できるシュレッダーで裁断してから廃棄
✔溶解（業者に委託） など、

デジタルの場合
✔記憶媒体を物理的に破壊する（ハンマーなどで再利用できないほどに殴打し破壊）
✔データ削除ソフトで記憶媒体からデータを抹消する
✔データをゴミ箱に入れ、ゴミ箱を完全に空にした後、記憶媒体を完全初期化。
✔データをゴミ箱に入れ、ゴミ箱を完全に空にする。
✔ファイル内のリストデータを消去する

ポイントは「復元不可能（または困難）」です。
アナログの場合、その対象を現実に破壊し、その結果を目で確認できるので、イメージしやすいと思いますが、デジタルの場合、物理的に破壊する以外に目で確認できないので、どのようにすれば、復元不可能な状態になっているかわからない、、、それが現実です。

デジタルの場合、ゴミ箱に入れるだけでは、データを消去したことにはなりません。
右クリックして「元に戻す」をすれば、すぐに使えるようになるからです。また、ゴミ箱に入れ空にしても、空にした直後であれば、ファイルを 100％に近い状態で復元できます。ある程度時間が経過しなければ、復元不可能な状態までには至りません。
そんな操作方法「普通は」知らない、、、などと思わないでください。
インターネットで調べれば、簡単に答えは出てきます。

復元不可能な状態に可能な限り早く近づけるアイテム、、、それがデータ削除ソフトです。

データ削除ソフトが存在するということは、、、当然データ復旧（回復）ソフトも存在します。

ここまでお伝えすると何をどうすればいいのか？わけがわからなくなってしまいます。

データを確実に削除、廃棄するには、物理的に破壊するしか方法はありません。

データは限られた人しかアクセス出来ないところに保管し、その空間で廃棄（ゴミ箱を空にする）。
バックアップは破壊できる記憶媒体で管理する、、、これが取り組みやすいのではないでしょうか？

1台の PC でマイナンバー管理のすべてを完結させるのであれば、ハードディスクを分割し、分割した一つをマイナンバー専用に割り当てる、バックアップを定期的に取る。マイナンバー保管先に異常を感じたら、いつでも初期化できる環境を準備する。といった対応が理想に近い形と言えるでしょう。

特定個人情報ファイルを廃棄するにあたり、外注業者（産業廃棄物業者）に依頼する場合には、必ず、削除証明書の発行を依頼しましょう。なぜなら、依頼しただけでは本当に廃棄されたかどうかを確認する手段がないからです。
多くの業者は、削除証明書の発行を準備していますので、依頼する際にご確認ください。

参照：ガイドライン安全管理措置 2-Ed

13. ＜原則 1・3＞【物理的・技術的】マイナンバー業務を遂行する手段（道具）を特定する。

マイナンバー業務に従事する人、従事する場所が決まれば、、、
自ずと、何を使って業務遂行するのか？業務遂行の手段も特定する必要がでてきます。

手段は、100%アナログ、100%デジタル、アナログ＋デジタル、この 3 のうちいずれかしかありません。

多くの場合、アナログ＋デジタルになるでしょう。必ず用途に応じて使い分けてください。
ケースバイケースでは「管理がずさんなアドレス帳」と同じ結果になってしまいます。

業務遂行の手段を特定していれば、それ以外の手段は必要ありません。
取扱区域内に設置する、持ち込める手段（道具）を設定してください。

特に気をつけたいのが、取扱区域へのデジタル機器の持込です。

手のひらサイズで 100GB 以上のデータを保管できる記憶媒体もあります。外付け記憶媒体は USB メモリだけとは限りません。ノートパソコンに内蔵されているハードディスク、、、内蔵専用とは限りません、、、内蔵専用、内蔵も外付けもできる、、、いろんなタイプがあります。

この記憶媒体を活用してデータを引っこ抜かれたら一体どれほどの情報を抜き出されてしまうのか？
デジタルデータを記憶できる媒体、アナログなら撮影などできる媒体は、必要最小限にとどめてください。

特にスマートフォンは注意が必要です。

スマートフォンはデスクトップ PC のモバイル版と受け止めてください。
使い方によってはデスクトップ PC よりも高性能を発揮します。ほとんどの場合、通信回線に接続しっぱなしですから、

見た目は手のひらサイズの小さな道具に過ぎませんが、その先には全世界とインターネットでつながっている、赤の他人をたくさん連れて来ている、悪意ある使い方をされてしまえば、一瞬にしてインターネットの世界に情報をばらまくこともできる、、、会社にとっては「悪魔」のデジタル、、、たかがスマホ、されどスマホです。

ステージに応じて、業務遂行の手段が異なることが十分に予想されますが、マイナンバー法の規制を受けながら保管すべき書類は、マスターと特定個人情報ファイルの 2 つしかありません。

アナログであれ、デジタルであれ、最終的にどんな形にするのかがはっきりしていれば、保管する必要のない書類は、その場で心置きなく廃棄できるので、無駄な情報漏えいリスクを抱える必要はなくなります。

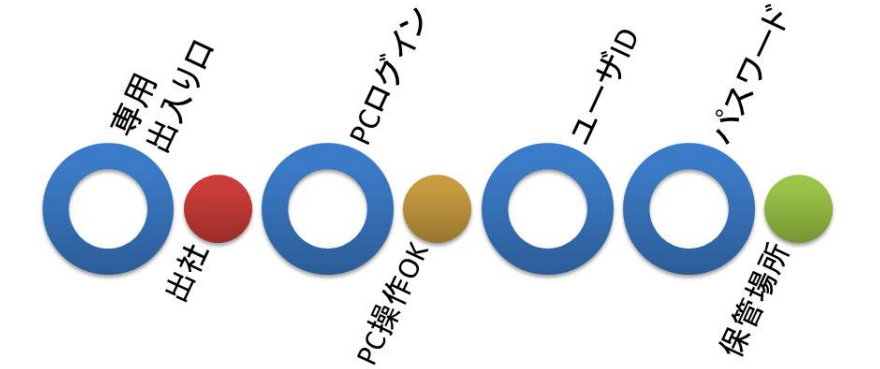
参照：ガイドライン安全管理措置 2-Eb、2-Ec、2-Ed、

14. ＜原則 1＞【物理的・技術的】デジタル機器はすべてアクセス権限、ユーザー制御など「カギ」を設定する。

アナログなら、目で確認できるので、どのように制限するか？鍵をかけて鍵ごと責任者が保管する。
そして必要なときに、必要なだけ利用することにすれば、最低限のセキュリティを構築したことになるでしょう。

ところがデジタルの場合にはそうはいきません。
有線、無線を問わず、インターネットに接続できる環境にあれば、自宅の PC、手元にあるスマートフォンから、会社のサーバー、会社が管理しているクラウドシステムにアクセスできてしまいます。

マイナンバーを保管する場所を特定しても、そこにアクセスできる機器があるだけで、情報漏えいリスクは高まってしまいます。



デジタルなら、、、出社しなくても、ユーザIDとパスワードがあれば、保管場所へアクセスできてしまう

マイナンバー業務に使用する、機器、システムを特定するとともに、活用する場合には、目的に応じて、それぞれに「カギ」を設定してください。

■91 社内システムアクセス権限管理簿をご参照ください。

もしアクセス権限を一目で確認できる「何か」がない場合、これを参考にしてオリジナルの管理簿を整備しましょう。

外部からの不正アクセス対策も忘れずに

ガイドラインでは外部からの不正アクセス対策等で検討すべき基本的なポイントが例示されています。

≪手法の例示≫

＊ 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、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対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。

＊ 導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。

＊ 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とする。

＊ 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。

ファイアウォール

ファイアウォールとは、あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システムなどのこと。原義は「防火壁」であり、外部ネットワークからの攻撃に対する防御を、火事の炎を遮断して延焼を防ぐことになぞらえている。

一般的な構成では、ファイアウォールに内部ネットワークの回線と外部ネットワークの回線を両方つなぎ、内部と外部の通信が必ずファイアウォールを通過するようにして、ファイアウォールが一定の基準に従って不正と判断した通信を遮断する。サーバコンピュータ上でソフトウェアとして動作するものと、専用の通信機器として提供されるものがあり、コストや導入の容易さを重視する場合は前者を、規模や性能が必要な場合は後者を用いることが多い。

IT 用語辞典 e-Words より引用

コンピュータウイルス

コンピュータウイルスとは、他人のコンピュータに勝手に入り込んで悪さをするプログラム。画面表示をでたらめにしたり、無意味な単語を表示したり、ディスクに保存されているファイルを破壊したりする。ウイルスはインターネットからダウンロードしたファイルや、他人から借りたフロッピーディスクなどを通じて感染する。最近では e-mail を介して感染するタイプのウイルス（ワーム）もある。大抵は使用者の知らないうちに感染する。またウイルスに感染したことに気づかずにコンピュータを使用し続けると、他のコンピュータにウイルスを移す危険性もある。

IT 用語辞典 e-Words より引用

人間の知覚では感じることができませんが、インターネットに接続できる環境にあるということは、不特定多数の人に囲まれている状態です。いい人もいれば悪い人もいます。

情報セキュリティ対策はイタチごっこの世界です。最低限、ガイドラインで例示されている事項は対策を講じましょう。

参照：ガイドライン安全管理措置 2-Fa、2-Fb、2-Fc、2-Fd

15. ＜原則 4＞【組織的・人的】マイナンバーの取得から保管、廃棄までを記録する。

いつ、どこで、だれが、だれの、なんのために、どのように、、、

マイナンバーを取得、利用、廃棄した履歴を確認できなければ、情報漏えい事故が発生したとき、予見されたとき、どのタイミングで漏れたのか？事実確認できません。

事実確認ができなければ、情報が漏れてしまった被害者に対応することもできませんし、今後の対策を検討することもできなくなってしまいます。必ず記録簿を作成してください。

記録簿は大別すると、2 パターン計 3 種類あります。

保管しているマイナンバーの取得から廃棄までの記録

■01 個人番号取得廃棄等記録簿

保管しているマイナンバーマスターの利用状況

■02 個人番号マスター_アクセス等記録簿

マイナンバー記載書類の作成履歴、保管状況確認

■11 特定個人情報ファイル事務処理簿

これらの記録簿にはマイナンバーを記入することはないので、特定個人情報ファイルとは扱われませんが、運用状況を監査するとき、万が一漏えい事故が発生して時には事実確認資料として利用することとなるので、特定個人情報ファイルと同等のレベルで保管するのがベターです。

参照：ガイドライン安全管理措置 2-Bb 2-Bc 2-Fb

16. ＜原則 1・3＞【組織的・人的】マイナンバーを記載する書類の作成手順を特定する

手続書類は以下の 3 つのすべてが揃って、行政へ手続きできる状態＝書類完成です。

✔基本情報（手続の対象者、提出者）
✔手続きに必要な情報
✔添付書類（必要な情報の補足資料、証明資料）

このうち、基本情報にマイナンバーが追加されてしまいました。
作成する書類にマイナンバーを記入したら、、、「特定個人情報ファイル」として扱われます。

特定個人情報ファイルですので、、、取扱区域から一歩でも持ち出すときには「目隠し」が鉄則でしたよね。
書類を完成させるまでに時間を要する場合には、マイナンバーの記入は一番最後にしましょう。
システムに依存する場合には、そのシステムの使用手順をリストにして、チェック項目を作成するといいでしょう。

書類作成開始から完成までの原則的な作成手順を特定しましょう。

基本の流れをあらかじめ作っておく＝チェックリストのたたき台になるので、行政手続事務のスムーズ化に貢献します。
また、担当者の入れ替え、業務引継の台本としても活用できます。
社会保険労務士や税理士に委託することなく、御社で事務手続する場合には作成することをオススメします。

どのように作ったら良いのかわからない場合には、、、Pmap を真似してオリジナルを作成してください。

参照：ガイドライン安全管理措置 2-D、2-B

17. ＜原則 4＞【組織的】漏えいリスク、漏えい事故に備える体制を整える。

アナログであってもデジタルであっても、情報はいつ、どこで、どのように漏れるのかはわかりません。
唯一言えることは、どんな情報の漏れ方であっても、その引き金は「人」が握っています。

「人あるところに漏えいリスク有り」

自分以外の人間は全て容疑者のような表現ですが、、、かつてはこのような表現をしたら叱責を受けたかもしれませんが、インターネットが普及し、手のひらサイズでありながらデスクトップ PC と同等のパフォーマンスが期待できるデジタル機器スマートフォンが普及した今日では、的を射た表現だと思います。

日常的に情報漏えいリスクに晒されていると受け止め、
万が一、情報漏えい事故が発生したら、予見されたら、、、に対応できる体制をあらかじめ整えておきましょう。

■マイナンバーPmap_情報漏えい事件発生時の対応
■マイナンバーPmap_安全管理組織図 smp
■01 情報漏えい_事故発生（予見）報告書
■02 情報漏えい_事実確認連絡票
■03 情報漏えい_初動対応から抑制、復旧までの対応連絡票
■04 情報漏えい_改善計画（案）報告書

参照：ガイドライン安全管理措置 2-Cd 2-Ce 2-Ca 2-Cb 2-Cc

情報漏えい対応5原則

1. 被害拡大防止・二次被害防止・再発防止の原則

情報漏えいが発生した場合に最も重要なことは、情報漏えいによって引き起こされる被害を最小限にとどめることです。漏えいした情報が犯罪等に使用されることを防止しなければなりません。また、一度発生した事故・事件は二度と起こることのないよう再発を防止します。

2. 事実確認と情報の一元管理の原則

情報漏えい対応においては正確な情報の把握に努めます。憶測や類推による判断や不確かな情報に基づく発言は混乱を招きます。組織の情報を一か所に集め、外部に対する情報提供や報告に関しても窓口を一本化し、正しい情報の把握と管理を行います。

3. 透明性・開示の原則

被害拡大防止や類似事故の防止、企業組織の説明責任の観点から必要と判断される場合には、組織の透明性を確保し情報を開示する姿勢で臨むことが好ましいと考えられます。情報公開により被害の拡大が見込まれるような特殊なケースを除いては、情報を公開することを前提とした対応が企業(組織)の信頼につながります。

4. チームワークの原則

情報漏えい対応においては様々な困難な判断を迅速に行わなければならず、精神的にも大きな負担がかかります。また、経営、広報、技術、法律など様々な要素を考慮する必要があるため、組織として対応していくことが重要です。

5. 備えあれば憂いなしの原則

情報漏えいなど事故が発生した時のことを想定し、あらかじめ緊急時の体制や連絡要領などを準備しておくと、いざという時に大変役立ちます。緊急時にどう対応するべきなのか、方針や手順を作成し、日頃から訓練しておきましょう。

情報漏えい発生時の対応ポイント集(IPA 独立行政法人情報処理推進機構セキュリティセンター)より引用

情報漏えいのタイプと発覚のきっかけ

1. 紛失・盗難

パソコンや USB メモリの入った鞄を電車の車内や店舗に忘れる、事務所や自宅に保管されていたパソコンが盗難にあうといった事件により情報の紛失や漏えいをしてしまうケースです。

発覚のきっかけ:自己申告、警察からの連絡、取得者からの連絡

2. 誤送信・Web での誤公開等

本来行ってはならないシステムの操作、設定等により情報が流出するケースです。お互いに関係のない複数のアドレスにあてた電子メールを、他人の宛先が見える形で送信してしまう場合(BCC で送信すべきところを TO や CC で送信)や、Web ページの公開サーバの設定を誤って個人情報などが誰でも見えるような状態にしてしまう場合などです。

発覚のきっかけ:自己申告(内部発見)、受信者からの指摘(風評を含む)

3. 内部犯行

企業(組織)内部の従業員が不正に情報を持ち出し、外部の第三者に売ったり渡したりするケースです。名簿業者等で、持ち出された名簿が販売されていることなどもあります。

発覚のきっかけ:外部からの指摘(風評を含む)

4. Winny/Share 等への漏えい

Winny/Share を代表とする匿名ファイル交換ソフトの利用者が暴露ウイルスに感染し、自宅に持ち帰っていた業務データや電子メールの内容などを流出させてしまうようなケースです。

発覚のきっかけ:外部からの指摘(風評を含む)

5. 不正プログラム

ウイルスに感染してパソコン内部のデータが電子メールに添付されてばらまかれたり、スパイウェアを送り込まれパソコンで入力した内容が外部に送信されたりするケースです。

発覚のきっかけ：自己申告、内部発見、外部からの指摘（風評を含む）

6.不正アクセス

アクセス制限を設けているコンピュータにネットワーク外部から不正に侵入されて情報を盗まれるケースです。

発覚のきっかけ：自己申告、内部発見、外部からの指摘（風評を含む）

7.風評・ブログ掲載等

組織の従業員がブログやホームページで本来秘密にすべき事項を掲載してしまったり、社内の者しか知らないはずの情報が匿名掲示板に書き込まれたりするケースです。

発覚のきっかけ：外部からの指摘（風評を含む）

情報漏えい発生時の対応ポイント集（IPA 独立行政法人情報処理推進機構セキュリティセンター）より引用

漏えい事故対応の基本ステップ

1. 発見・報告

情報漏えいに関する兆候や具体的な事実を確認した場合は、責任者に報告し速やかに情報漏えい対応のための体制をとります。不正アクセスや不正プログラムなど情報システムからの情報漏えいの可能性がある場合は、不用意な操作をせず、システム上に残された証拠を消してしまわないようにします。また外部から通報があった場合は、相手の連絡先等を必ず控えるようにします。

2. 初動対応

対策本部を設置し当面の対応方針を決定します。情報漏えいによる被害の拡大、二次被害の防止のために必要な応急処置を行います。情報が外部からアクセスできる状態にあったり、被害が広がる可能性がある場合には、これらを遮断する措置をとります。情報の隔離、ネットワークの遮断、サービスの停止などです。

3. 調査

適切な対応についての判断を行うために5W1H（いつ、どこで、誰が、何を、なぜ、どうしたのか）の観点で調査し情報を整理します。また、事実関係を裏付ける情報や証拠を確保します

4. 通知・報告・公表

漏えいした個人情報の本人、取引先などへの通知、監督官庁、警察、IPA などへの届出、ホームページ、マスコミ等による公表を検討します。漏えいした個人情報の本人については特別な理由がない限り通知を行います。紛失・盗難のほか不正アクセス、内部犯行、脅迫等不正な金銭の要求など犯罪性がある場合は警察へ届出ます。すべての関係者への個別通知が困難な場合や、広く一般に漏えい情報による影響が及ぶと考えられる場合などは、ホームページでの情報公開や記者発表による公表を行います。ただし、情報の公表が被害の拡大を招く恐れのある時は、公表の時期、対象などを考慮します。

5. 抑制措置と復旧

情報漏えいによって発生した被害の拡大の防止と復旧のための措置を行います。専用の相談窓口を設置し被害が発生した場合にはその動向を素早く察知し対応するようにします。また、再発防止に向けた具体的な取り組みを行い、停止したサービス、アカウント等を復旧します。

6.事後対応

抜本的な再発防止策を検討し実施します。また、調査報告書を経営陣に提示し、被害者に対する損害の補償等について必要な措置を行います。内部職員の責任等について必要な処分手続きを行います。これらについて必要に応じて情報を開示します。

情報漏えい発生時の対応ポイント集（IPA 独立行政法人情報処理推進機構セキュリティセンター）より引用

参照：ガイドライン安全管理措置 2-Eb 2-Ec 2-Ed 2-Fa 2-Fb 2-Fc 2-Fd

18. ＜原則 4＞【組織的】1-17 以上のすべてを取扱規程にまとめ、それに従い運用を始める。

規程は次のような構成になります。

特定個人情報取扱規程_smp　目次

1-17 まで一通り目を通し、smp ファイルに記入、加工するなど、たたき台が出来上がったら、、、

実際に smp 規程と照らしあわせ、必要な箇所を加筆修正してください。

加筆修正が完了すれば、取扱規程の完成です。

参照：ガイドライン安全管理措置 2-B 巻末資料

19. ＜原則 4＞【組織的】就業規則を整える

運用している就業規則の構成により、対応は変わりますが、見直しを検討する箇所は、大別以下の 5 つです。

1. 総則関係−採用時提出書類、雇用情報に変更があった場合の届出方法

提出書類リストにマイナンバー、国民年金第 3 号被保険者となる扶養家族がある場合には、委任状を含めたか？
マイナンバーの提出を拒んだ時の対応について言及したか？

2. 総則関係−利用目的の追加

個人情報の利用目的を就業規則に定めている場合には、マイナンバーについても言及する。

3. 服務規律関係−社内規範として

従業者として、会社がマイナンバー実務に協力する義務がある旨定めたか？

4. 退職関係−退職時手続について

退職時に退職者がマイナンバー削除証明書の交付（任意）を求めたら、交付する旨定めたか？
退職事務手続きが完了したら、退職者のマイナンバーを削除する旨定めたか？

5. 懲戒事由の追加

マイナンバー法の罰則を参考に、会社が管理するマイナンバーに不具合を生じさせた従業者に対する処分を、処分の程度に合わせて、処分列挙事項に追加したか？

必ずこれらを記載しなければならないということではありませんが、マイナンバー法違反には刑事罰が定められていることを考えると、少なくとも懲戒事由は、見直し、変更するべきでしょう。

参照：ガイドライン安全管理措置 2-B、2-C

まとめ

セキュリティに 100%完璧はありません

どんなに立派な仕組みを構築しても、漏れるときは漏れてしまう、、、それが「情報」です。
最も漏れる危険性が高いのは、、、「マイナンバー業務を遂行しているとき」です。

マイナンバー漏えいリスクを小さくするためには、、、
✔作業する人を特定する
✔作業する場所を特定する
✔作業する時間を特定する
✔作業する業務を特定する
✔作業する手段（道具）を特定する。
✔どのように作業するか手順を決める
実際にマイナンバー業務を遂行する際は、この 6 つを意識してください。
そうすれば、あなたが、あなたの会社が、マイナンバーを漏えいするリスクは、より小さくなるはずです。

マイナンバー安全管理体制構築のためにご用意した smp ファイルは以下のとおりです。

ステップ 1 から 19 を進めていくにあたり、必要となるであろうひな形や書式を smp ファイルとしてご用意しました。

全部で 24 個あります。
すべて使う必要はありません。必要に応じて選び、加工してご活用ください。

全体を把握する

20151026_マイナンバーPmap_151026.pptx
マイナンバー業務の業務フローと全体像

20151026_マイナンバー安全管理体制構築 19 のステップ_151026.docx
いまご覧になっているファイルです。

20151026_マイナンバー制度の概要_smp_151026.docx
従業者への制度案内資料としてご活用ください

マイナンバー取扱規程関連

20151201_特定個人情報取扱規程_smp_151026.docx
従業員数 100 人未満で、以下の条件に該当しない場合には、中小規模事業者として、講じるべき安全管理措置の基準が緩やかになっていますが、改正個人情報保護法（施行日は未定）の成立し、5000 要件が廃止が確定したため、緩いところはカット＝一般事業所と同じレベルで作成しています。

中小規模事業者と認められない条件

✔個人番号利用事務実施者

✔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

✔金融分野の事業者

✔個人情報取扱事業者

20151201_特定個人情報等の適正な取扱いに関する基本方針_smp_151026.docx

よく見かけるひな形では、利用目的が簡単に書かれていますが、、、

掘り下げれば、書類は洪水のようにたくさん出てきます。分かる人にしか分からない書き方です。

細かいことを知らなくても「こんなことに使うのか！」とわかるよう少し掘り下げて記載しました。

20151201_本人確認_取り扱い原則_smp_151026.docx

基本的な取り扱いをざっくりとまとめてあります。

20160101_採用時提出書類_smp_151026.docx

20160101_退職事務処理に係る書類の例_smp_151026.docx

就業規則の見直しにご活用ください。

万が一の事故に対応する

20160101_101 情報漏えい_事故発生（予見）報告書_smp_151026.docx

20160101_102 情報漏えい_事実確認連絡票_smp_151026.docx

20160101_103 情報漏えい_初動対応から抑制、復旧までの対応連絡票_smp_151026.docx

20160101_104 情報漏えい_改善計画（案）報告書_smp_151026.docx

Pmap 情報漏えい事件発生時の対応を少しでもスムーズに動かすには、情報の記録が欠かせません。

情報は記録するだけではなく使う。初動対応から将来の改善計画を一連の流れにした報告書、連絡票のひな形をご用意しました。

マイナンバーを管理する

20160101_01 個人番号取得廃棄等記録簿_151005.xlsx

20160101_02 個人番号マスター_アクセス等記録簿_151005.xlsx

20160101_03 個人番号マスター_151005.xlsx

20160101_11 特定個人情報ファイル事務処理簿_151005.xlsx

20160101_マイナンバー削除通知書_151005.docx

100％アナログ対応の場合には、全て必要になるファイルです。

システムを導入すれば、「11 特定個人情報ファイル事務処理簿」を除いたファイルは要らなくなるでしょう。

エクセルのテーブル機能を利用して「とにかく記録だけは残す」ことを目的に作成しています。

管理にカギをかける

20160101_91 社内システムアクセス権限管理簿_151005.xlsx

アクセス権限を一覧で管理するためのファイルです。

20160101_92 ファイルパスワード管理簿_151005.xlsx

デジタル関係のパスワードには、拒絶反応を示したくなるほど、辟易とされている方も多いと思います。
パスワードを覚えるだけではなく、作ることに頭を悩ましてしまうことが原因かもしれません。
このファイルでは、乱数を活用して任意のパスワードを作れる計算式を埋め込んでいます。
パスワード作成に悩んだら、、、このファイルを活用してください。

20160101_93 貸出簿と持出簿_151005.xlsx

20160101_貸出持出などの記録簿_smp_151026.docx

アナログでの鍵の管理やファイル管理のための記録簿です。
エクセル版とワード版をご用意しましたので、必要なときには、加工してご活用ください。

マイナンバーを集める

20151201_マイナンバー提供のお願い_smp_151026.docx

これには、個人番号に関する報告書(会社に提出する書式)も一緒に入っています。

20151201_委任状_国民年金第 3 号被保険者届出事務_smp_151026.docx

従業者の配偶者が、健康保険法上の被扶養者＝国民年金第 3 号被保険者である場合に使用します。

20151201_委任状_smp_151026.docx

健康保険、労災保険の保険給付申請は本来、被保険者自身が行います。
そのため、これらの申請を会社が代行する場合で、保険給付申請書にマイナンバーを記載しなけれななならない場合には、被保険者から委任を受けてから代行してください。

実際にマイナンバーの提供を依頼する際に使用するであろうファイルは、
20151201_マイナンバー提供のお願い_smp_151026
20151201_委任状_国民年金第 3 号被保険者届出事務_smp_151026　この 2 つです。

安全管理体制の構築が完了したら、残るは、、、
初めてのマイナンバー業務＝現在在籍している従業者等からのマイナンバーの取得です。

マイナンバー収集スケジュール（案）

マイナンバー封書が市区町村から届いたからといって、すぐにマイナンバーを集める必要はありません。

マイナンバーを利用して、特定個人情報ファイルを作成する機会、行政手続きする機会は、

✔2016 年 1 月 1 日以降入退社がない。

✔現在在籍している方の氏名変更、住所変更、60 歳到達等がない　など

雇用保険関係の事務手続きが発生しなければ、2016 年 12 月の年末調整からです。

取引先（個人事業主）に対する支払調書への記載は、2016 年分＝2017 年 1 月申告からです。

とはいえ、集めようと思ってもすぐに集まるものでもないでしょう。

日本に住所がある方すべてにマイナンバー封書が届くのは 11 月末頃です。

ですので、11 月下旬から 12 月上旬。ちょうど年末調整資料を従業者から回収する時期です。
このタイミングで、期間を限定して、まとめて取得することをおすすめします。

そのためのスケジュールは下記のとおりです。

2015 年 10 月 20 日～11 月中旬まで
（Pmap_A 上段）各市区町村からマイナンバーが個人宛に送付される

2015 年 10 月 26 日～31 日まで
（Pmap_A 上段）マイナンバー封書が届いたら「中身を確認してから保管」「後日会社に提出してもらいます」を告知

2015 年 10 月 26 日～11 月中旬まで
ステップ1～19　マイナンバー安全管理体制を整備する。

2015 年 11 月中旬～下旬
年末調整スケジュールの確定
（Pmap_A 中段）マイナンバー提供依頼の告知

2015 年 12 月上旬
（Pmap_B）年末調整に必要な書類の回収に合わせ、マイナンバーを取得。
（Pmap_C）マイナンバーがすべて集まった段階で、、、一気にマスターを作成し、保管、カギをかける。

2015/10/20 現在、当事務所の基幹システム提供会社、株式会社セルズからマイナンバー管理システムの具体的な仕様が発表、公開されていないので、現段階では、ここまでしかお伝えすることができないことをご了承ください。
仕様確認出来次第、より具体的な取得方法、スケジュール（案）等をご案内します。

最後に、、、

「給与所得者の扶養控除等（異動）申告書」をマイナンバー取得手段として活用することについて

給与所得者の扶養控除等（異動）申告書を使ってマイナンバーを集めるのが最も効率的です。
という話をよく耳にするので、この件について当事務所のスタンスをお伝えします。

当事務所は、情報漏えい防止の観点から、この方法はおすすめしません。

なぜなら、会社にとっての給与所得者の扶養控除等（異動）申告書は、実務上、賃金計算＝所得税計算のために必要な情報のマスターです。具体的には、賃金計算における所得税額算出までのフロー4 で利用するマスターです。

賃金（給与・賞与）計算における所得税額算出までのフロー

1. 総支給額を計算し、課税対象支給額を算出する。
2. 社会保険料（雇用保険、健康保険、厚生年金保険）を計算し、合計額を算出する。
3. 課税対象支給額から社会保険料合計額をマイナスし、（所得税）課税対象額を算出する。
4. 給与所得者の扶養控除等（異動）申告書で扶養家族数を確認し、3 に対する所得税額を算出する。

なので、年度の途中で扶養異動があった場合には、その都度、本人に渡し、加筆修正を依頼する書類でもあります。

本人に渡す、本人がデスクの上に置きっぱなしにする、本人が家に持ち帰る、、、

加筆修正のたびに、会社・管理者の目の届かないところで、会社が保管しているマイナンバーマスターの一部をさらす機会が多くなってしまいます。

受け取った本人は、マイナンバーが書かれた書類の適正な取り扱いを知らなかったばかりに、「知らず知らずのうちに自らの個人情報を漏えいしてしまうチャンスを会社に作らされた」と言ってくるかもしれません。
国税庁が作っている書式の体裁が悪いばかりに、このような事態を、知らず知らずのうちに招く危険性が有ります。

無用にマイナンバーをさらすチャンスを増やすのは、情報漏えいリスクを高めるだけです。

この申告書は本来、マイナンバーを記入した上で税務署に提出しなければならない書類ですが、税務署に提出する機会は極めて少ないのが現実です。社会保険の調査や労働基準監督署の調査があった場合には、提示しなければならない書類に指定される可能性がある書類でもあります。

新年度のはじめに提出してもらう給与所得者の扶養控除等（異動）申告書には、マイナンバーを記入しない。

年末調整、退職など、給与所得者の扶養控除等（異動）申告書を最後に使用する機会にマイナンバーを記入してもらう、給与計算ソフトを活用している場合には、給与計算ソフトからマイナンバー記載済みの申告書を印刷し、同時に、給与所得者に記載内容を確認させ、その場で押印を受ける。これで十分なのではないでしょうか？

会社として適正な事務処理をしている限り、無駄にマイナンバー漏えいリスクを抱える必要はありません。

確かなマスターを一つ作成し、活用し、守る。接点はマスターのみ十分です。