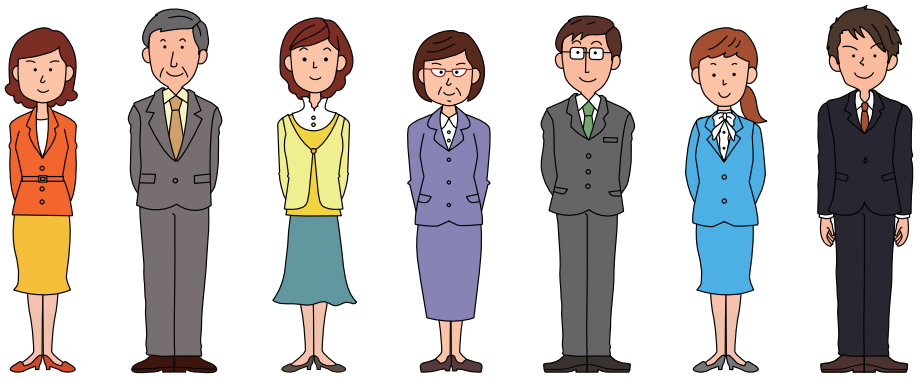
マイナンバー対策
マニュアル



平成 27 年 9 月

達人

いよいよ今年10月から順次マイナンバーの配付が開始され、平成28年1月からはマイナンバー制度が始まります。
そんな中、最近では様々なマイナンバーに関連するセミナーやWebサイト等で、「マイナンバー対策」というキーワードを目にする機会が増えてきました。

弊社では、達人シリーズのお客様向けに、マイナンバー制度に関する情報提供として、5月にマイナンバー特設サイト（https://www.tatsuzin.info/mynumber/）を開設し、以降、サイトコンテンツの更新やマイナンバーセミナー（入門編）などで、制度の内容を中心に説明させていただいていました。

本書では、次の段階として、達人シリーズをご利用されている方々に、法律に則りつつ、取り扱いにくいマイナンバーをスマートに取り扱えるように整備する（=「マイナンバー対策」）ために、どのようなプロセスをもって実施すべきか、という観点で、必要な情報や解説を用意させていただきました。

本書の内容は、マイナンバー制度の知識を前提に、ある程度踏み込んだ内容になっています。もし制度自体についての理解が足りないと思われる場合は、マイナンバー特設サイト（https://www.tatsuzin.info/mynumber/）の内容をご確認ください。

マイナンバー制度の開始を控えた今、本格的に「マイナンバー対策」を実践される上で、本マニュアルが検討の一助となれば幸いです。

平成27年9月

目次

1 はじめに

本章では、まず「マイナンバー対策」に取り組むにあたり、今一度その言葉の定義について考えてみたいと思います。

早速ですが、皆様に少し想像してみていただきたいことがあります。
仮に皆様が自社のマイナンバーチームのリーダーに任命され、「マイナンバー対策」を主導するよう指示された場合、具体的に何をしようとお考えになるでしょうか？

・ウイルス対策ソフトを導入する
・マイナンバーを取り扱うエリアに間仕切りを設ける
・マイナンバーを取り扱う電子媒体を特定し、持ち出し管理簿を作成する　等々

このように、マイナンバーの漏えい、滅失、毀損等をはじめとするセキュリティ事故を防止するため、何かしらの対処をしようとする方が多いのではないかと思います。

しかし、本当にこれで「マイナンバー対策」ができていると言えるでしょうか。
先ほどの例をとって、「ウイルス対策ソフトを導入する」という対処をしたとしましょう。自社の全てのPCにインストールをして、ウイルス検知の仕組みが整いました。なんだかこの瞬間は、無敵になったような気がしますよね。しかし半年後、全てのPCについて、それが最新版にバージョンアップされた状態で、しっかりと検知が行われているでしょうか。
「マイナンバーを取り扱う電子媒体を特定し、持ち出し管理簿を作成する」という対処についても同様です。管理簿を作成したものの、半年後にそれを開いてみた時に、もしも誰ひとりとして記入していなかったとしたら・・・？

ここまで読んでイメージできたことと思いますが、対処がどんなものであったとしても、残念ながらその対処をするだけでは「マイナンバー対策」を行ったとは言えません。
また、先ほどは対処を講じたまま何もしなかった場合を例にとりましたが、たとえしっかりとバージョンアップ作業が行われていたり、管理簿への記入が徹底されていても、もしかするとまだ顕在化していないリスクからマイナンバーを守るための手法として、その対処が全く効果を発揮していないかもしれません。
そもそもリスクと一口に言ってもその内容は日々変化していくものですから、対処をした瞬間には絶大な効果があったとしても、しばらくするとその効果が発揮されなくなる可能性もあるわけです。

さらに言うと、自社の状況も一定ではありません。新しいサテライトオフィスを設立するかもしれないし、自宅からのリモートアクセスを許可するようになるかもしれませんよね。また、「マイナンバー法」が改正されて、求められる要件が変化する可能性もあります。

したがって、繰り返しになりますが、「マイナンバー対策」で重要なのは単純に対処をすることではありません。もし「マイナンバー対策」が対処をすることそのものであるという認識をしているならば、一旦白紙に戻して考える必要があります。

では、一体「マイナンバー対策」とは何なのか。最初にその目的を確認しておくと、それはまさに何かしらの対処をするように、マイナンバーの漏えい、滅失、毀損等をはじめとするセキュリティ事故のリスクや「マイナンバー法」に抵触してしまうリスク等を潰そうとする取り組みではありません。もっと長期的に、リスクを管理できるような環境を構築することを目的とした取り組みなのです。

Point

「マイナンバー対策」は、あらゆる対処をすることにより、リスクを潰そうとする取り組みではない。
「マイナンバー対策」の目的は、リスクを管理できるようになることである。

マイナンバー特設サイトの中で、「マイナンバー対策」をこう定義したことを覚えているでしょうか？

“法律に則りつつ、取り扱いにくいマイナンバーをスマートに取り扱えるよう整備すること。”

この「法律に則りつつ、取り扱いにくいマイナンバーをスマートに取り扱える」状態こそ、「リスク管理」ができるようになっている状態であり、「マイナンバー対策」のゴールです。

では、具体的にこれがどのような状態か、イメージすることはできるでしょうか。いまいちピンとこないですよね。次章では、この「マイナンバー対策」のゴール像について、詳しく解説していきたいと思います。

2 ゴール像

前章にて、「マイナンバー対策」のゴール像は「リスク管理」ができている状態であるというお話をしましたが、具体的にはどういうことでしょうか。「リスク管理」と聞くと難しく考えてしまうので、ご自身の「健康管理」に置き換えて考えてみましょう。

最近ちょっと太り気味になってきたこともあり、体重管理に気を付けよう!と思い立ったとします。そうしたらまず、目標を決めますよね。分かりやすい例で、ここでは「半年間で5kgダイエットをする」という目標にします。それが決まったら、目標達成のための手段として、いくつかの対処を検討すると思います。あまりたくさんの対処をしようとしてもすぐに挫折してしまうので、「食事制限をする」、「運動をする」という2つに絞ったとしましょう。

次に、「食事制限をする」、「運動をする」という内容では具体的に何をすべきかが不明瞭であるため、これをもう一段具体化します。ここでは、「食事制限をする」については「晩酌を週3日までとする」とし、「運動する」については「毎日1駅手前で電車を降りてウォーキングをする」としましょう。
ただし、これを決めただけではついつい甘えてしまうので、5kgのダイエットに取り組む旨を家族に宣言するとともに、この2つの対処への取り組み状況を、毎週日曜日に家族へ報告するというルールを作ることにしました。ここまでの内容をまとめると、以下のとおりです。

目標

半年間で5kgダイエットをする

そのための対処とルール

●食事制限をする
- 晩酌は週3日までとする
- 毎週日曜日に取り組み状況を家族に報告する

●運動をする
- 毎日1駅手前で電車を降りてウォーキングをする
- 毎週日曜日に取り組み状況を家族に報告する

ここまで決まればいざ開始。順調に取り組みを継続し、必ず毎週日曜日に報告を行いました。

しかし、しっかりと報告のルールを決めたにもかかわらず、月日が経つにつれてだんだんと甘えの気持ちが発生。晩酌の回数は家族がカレンダーに記入して管理してくれているため必ず守るのですが、ウォーキングは誰にも監視されていないため、ついついやったことにして嘘の報告をしてしまいました。
これではいけないということで、嘘の報告をしないよう「ウォーキングの状況をアプリで自動記録する」というルールを追加し、報告時に一緒に提出するようにしました。

目標

半年間で5kgダイエットをする

そのための対処とルール

●食事制限をする
- 晩酌は週3日までとする
- 晩酌した日をカレンダーに記録する
- 毎週日曜日に取り組み状況を家族に報告する（記録との照合を行う）

●運動する
- 毎日1駅手前で電車を降りてウォーキングをする
- ウォーキングの状況をアプリで自動記録する
- 毎週日曜日に取り組み状況を家族に報告する（記録との照合を行う）

書き続けては際限が無いのでここで一旦終わりにしますが、「管理」というのがどういうことか、少しイメージすることができたでしょうか。管理するということは、すなわち計画→実行→チェック→見直しという、いわゆる**PDCAサイクルを回すこと**なのです。
体重管理について、ここまでの内容をPDCAサイクルに当てはめて今一度整理してみましょう。

Plan

各対処に関し、以下のルールを策定
①食事制限をする
- 晩酌は週3日までとする
- 晩酌した日をカレンダーに記録する
- 毎週日曜日に取り組み状況を家族に報告する

②運動する
- 毎日1駅手前で電車を降りてウォーキングをする
- 毎週日曜日に取り組み状況を家族に報告する

Do

Planで定めたルール通りに運用

Check

②について、ウォーキングについて嘘の報告をしてしまうという問題が発生

Action

「ウォーキングの状況をアプリで自動記録する」というルールを②に追加

このように、個別の対処について繰り返し改善を行うことこそが「管理」なのです。

ただし、残念ながらこれだけではありません。体重管理の例に戻って考えてみましょう。この取り組みのおかげで少しずつ体重が減少し始めた頃、年に一度の人間ドックを受診することになりました。自信満々でダイエットの成果を医師に自慢しようと思っていたら、医師から衝撃の一言が・・・!
「〇〇さん、あなたはこの半年間で、最低でも10kg体重を減少させる必要があります。」
もし医師からこんな忠告をされてしまったら、最初に決めた目標自体を見直す必要がありますよね。先ほど解説したPDCAサイクルはあくまで「食事制限をする」「運動をする」という個別の対処を滞りなく運用するためのものでしたから、もちろん目標の見直しは視野に入っていません。

したがって、この個別の対処に関するPDCAサイクルの他に、もっと俯瞰的な目線で目標自体を定期的に評価し、必要に応じて是正するというPDCAサイクルも存在するのです。こちらも体重管理の例を当てはめて今一度整理してみましょう。

目標

Plan

体重管理のため、「半年間で5kgダイエットをする」という目標を設定
（ダイエットに取り組む旨を家族に宣言）

Do

個別の対処をルールに則って運用

Check

医師から10kg減量しなければならないという忠告を受ける

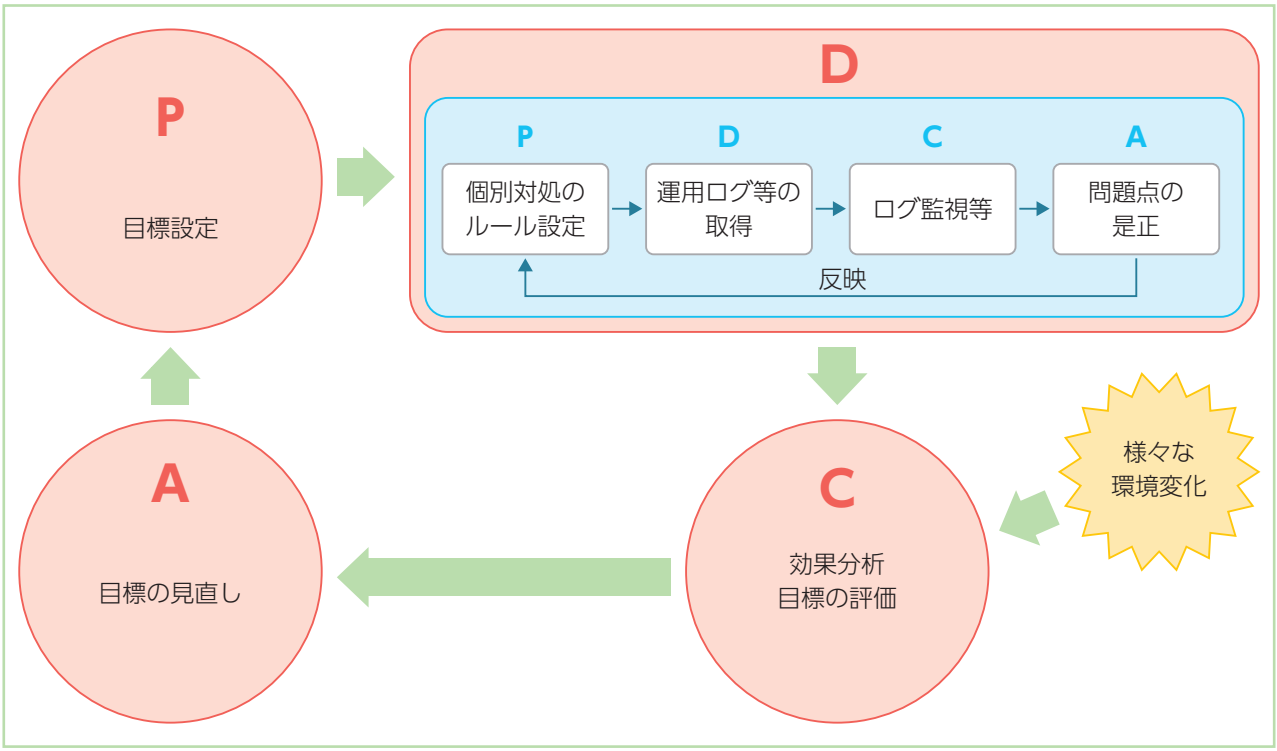
Action

「半年間で10kgダイエットをする」という目標に是正

今回例示したのは自身が置かれた状況、つまり「環境変化」による目標是正でしたが、これ以外にも、各対処の効果測定によって目標を見直す場合もあります。例えば各対処に抜群の効果があって「半年間で10kgダイエットをする」という目標を達成できたとしても、あくまで究極の目的は「健康管理」をすることですから、この取り組みは継続する必要がありますよね。したがって、その場合には新しい目標を設定する必要があるということなのです。

本マニュアルでは、この目標自体を決定したり見直したりするサイクルを、分かりやすく「大きなPDCAサイクル」と呼ぶこととします。それに対して、個別の対処に関するPDCAサイクルを「小さなPDCAサイクル」としましょう。

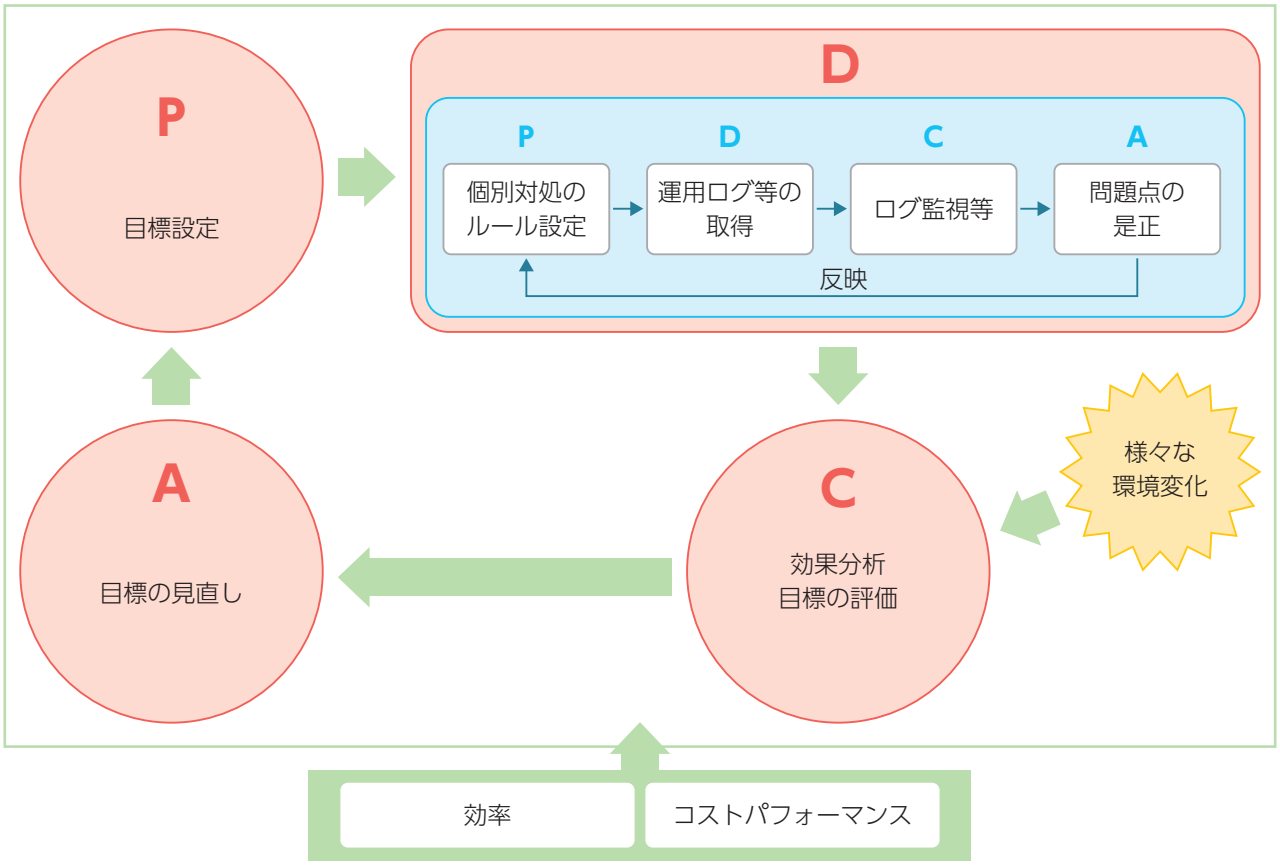
この2つのPDCAサイクルを分かりやすくイメージ図で表現すると、以下のようになります。



いかがでしょうか。ここまで「健康管理」に置き換えて解説を進めてきましたが、「リスク管理」についても同様です。
「リスク管理」も、ルールに従って個別の対処（例：ウイルス対策ソフトを導入する）を適正に運用するための「小さなPDCAサイクル」と、その個別の対処自体がリスクを軽減／回避できているかどうかを評価したり、取り巻く環境を考慮することにより、目標を定期的に是正する「大きなPDCAサイクル」の2つから成り立っているのです。

実は、この2つのPDCAサイクルを滞りなく回せている状態こそが、「リスク管理」ができている状態であり、「マイナンバー対策」のゴール像です。
ただし、ひとつ注意していただきたいこととして、この2つのPDCAサイクルは「効率」、「コストパフォーマンス」も合わせて加味されている必要があります。1章で解説した「マイナンバー対策」の定義でも、“法律に則りつつ、取り扱いにくいマイナンバーをスマートに取り扱えるよう整備すること”とあったように、先ほどの体重管理の例で考えてみても、対処があまりに高価なサプリメントを摂取することであったり、車で5時間かけて有能なトレーナーの元にトレーニングに行くのでは、家計を圧迫するだけでなく、効率も悪いですよね。これではとてもスマートではありません。あくまで「効率」、「コストパフォーマンス」が加味された状態で、持続的に「リスク管理」のPDCAが回せている状態こそが、「マイナンバー対策」のゴール像なのだということを覚えておいてください。

上記の点を含めて改めてイメージ図で表現すると、以下のようになります。



Point

「マイナンバー対策」のゴール像は、「効率」、「コストパフォーマンス」が加味された状態で、持続的にリスク管理のPDCAが回せている状態を指す。

さて、ここまでで、「マイナンバー対策」のゴール像をご理解いただけたかと思いますが、このゴールにたどり着くためには一体何をしなければならないでしょうか。次章では、このゴールへのプロセスについて解説したいと思います。

3 ゴールに至るプロセス

前章では、「マイナンバー対策」のゴール像とは、「効率」、「コストパフォーマンス」が加味された状態で、持続的にリスク管理のPDCAが回せている状態を指すということについてお話しました。
では、そのゴールに到達するためには一体何をしなければならないでしょうか。今一度、マイナンバー特設サイトの中で記した、「マイナンバー対策」の定義を振り返ってみたいと思います。

“法律に則りつつ、取り扱いにくいマイナンバーをスマートに取り扱えるよう整備すること。”

ここまでで「法律に則りつつ、取り扱いにくいマイナンバーをスマートに取り扱える」状態が、イコール「効率」、「コストパフォーマンス」が加味された状態で持続的にリスク管理のPDCAを回せている状態であり、「マイナンバー対策」のゴール像であると分かりました。そうすると、まだ明らかになっていない「整備すること」が、すなわち「マイナンバー対策」そのものであるということになります。

つまり、ゴールに到達するためには整備をすればいいわけですが、一体何を整備すればいいでしょうか。
具体的な作業内容として、大きく以下3点があります。

①業務範囲を限定する
②「基本方針」、「取扱規程」、「オフィスマニュアル」を作成する
③整備したルールの通りに運用が回るよう歯止めをかける

この3点について、順番に解説していきます。

Point

「マイナンバー対策」とは、以下3点の作業を実施することである。
- **業務範囲を限定する**
- **「基本方針」、「取扱規程」、「オフィスマニュアル」を作成する**
- **整備したルールの通りに運用が回るよう歯止めをかける**

1 業務範囲を限定する

「マイナンバー対策」としてまず皆様に実施していただきたいことは、マイナンバーが係わる範囲を限定することです。例えば現状、顧問先の基礎情報を対面、郵送、メールという3つの手段で収集していたとしたら、その全てについて「リスク管理」ができている状態にしなければならないですよね。しかし、これをどれか1つに限定すれば、検討すべき事項もそれにかける労力も1/3になります。データを保存する業務ソフト等を集約することも、非常に有効な手段と言えるでしょう。

このように、必要以上に範囲を広げたままでは無駄な労力、さらには無駄なコストもかけてしまうことになりかねないため、あらかじめ業務フローを極力シンプルな形へ見直す作業が非常に重要なのです。

2 「基本方針」、「取扱規程」、「オフィスマニュアル」を作成する

前章にて、「健康管理」のPDCAサイクルについて解説したことを思い出してみてください。体重管理をするという漠然としたテーマに対してまずは具体的な目標を定め、それを実現するための個別の対処・ルールの策定をした上で、PDCAを回し始めましたよね。
「リスク管理」についても同じです。当然と言えば当然ですが、まずはPDCAの回し方を規定しないことには何も始まりませんので、「リスク管理」の目標とそれを実現するための個別の対処・ルールを決定し、それらをドキュメントとして明文化するところからはじめましょう。

その時に作成するのが、「基本方針」、「取扱規程」、「オフィスマニュアル」なのですが、これらはそれぞれどのようなものでしょうか。まずは3つのドキュメントの関係性について、簡単に解説したいと思います。

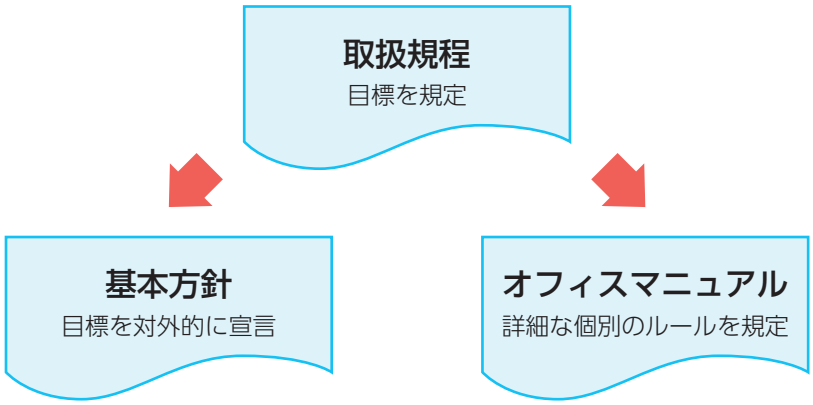
3つのドキュメントの関係性

まず最も重要なこととして、これら3つのドキュメントの中心は「取扱規程」にあります。「取扱規程」では、体重管理についてはじめに「半年間で5kgダイエットをする」と定めたように、「リスク管理」の取り組みにおける目標を明文化します。

次に、「取扱規程」をベースに、「リスク管理」の取り組みを対外的に宣言します。体重管理でも、家族にダイエットを宣言し、取り組みに巻き込もうとしましたよね。このように、対外的な宣言に用いるドキュメントが「基本方針」です。

さらに、「取扱規程」で定めた目標を実現するために具体化した個別の対処・ルールを明文化したものが「オフィスマニュアル」です。

ここまでの解説をイメージ図にまとめると、以下のようになります。



それぞれのドキュメントについて、もう少し詳しく解説しましょう。

各ドキュメントの概要

基本方針

「リスク管理」の目標、すなわちマイナンバー等を適正に取り扱うことについて、組織全体で取り組む旨を、対外的に宣言するためのドキュメントです。対外向けに発信する意図としては、顧問先をはじめとするステークホルダーに対して説明責任を果たすとともに本取り組みに巻き込むことや、セキュリティへの取り組み等をアピールすることにより、自社に対する信頼・安心感を醸成すること等が挙げられます。

取扱規程

「リスク管理」の目標、すなわちマイナンバー等を適正に取り扱うことについて、社内向けにその基本的なルールを宣言することを目的としたドキュメントです。ここで定義した「大きなPDCAサイクル」の回し方に則って運用するとともに、その遵守状況を確認、必要に応じて是正を行います。

オフィスマニュアル

目標を実現するための個別の対処について、従業者向けにその詳細なルールを周知・徹底することを目的としたドキュメントです。ここで定義した「小さなPDCAサイクル」の回し方に則って運用するとともに、その遵守状況を確認、必要に応じて是正を行います。

3 整備したルールの通りに運用が回るよう歯止めをかける

②の作業でPDCAサイクルの回し方を定めることができたら、いよいよそれが自社で実践されるよう、いくつかの作業を行います。具体的な内容は以下のとおりです。

■ 従業者への啓発活動の実施

「大きなPDCAサイクル」、「小さなPDCAサイクル」を回すプレーヤーは従業者であるため、従業者がマイナンバーを厳重に取り扱う必要性およびその詳細な取扱方法について理解していなければ、PDCAが回りません。
そのため、全社として「リスク管理」に取り組むためには、従業者に対してそれらをしっかりとレクチャーすることが重要なのです。

■ 個別の対処を導入する

「オフィスマニュアル」を作成したにもかかわらず、そこに記載されている個別の対処（ソフトウェア、契約書等）が何ひとつ導入されないままでは、「リスク管理」のPDCAを回している意味がありません。したがって、当然のことではありますが、個別の対処の検討がひと通り完了したら、それらを順次導入していく作業が必要です。

1章にて解説しましたが、この「個別の対処の導入」＝「マイナンバー対策」と誤解される方が多くいます。そうでは無くて、「個別の対処の導入」はPDCAサイクルの回し方を定めた後のプロセスの一部でしかないということをよく覚えておいてください。

なお、「個別の対処の導入」に関してもうひとつ注意していただきたいことがあります。それは、マイナンバー制度の開始までに、全てのものが完璧に導入されている必要は無いということです。確かに最終的には導入予定のものを揃えていただきたいのですが、「マイナンバー対策」のゴールは、あくまで「リスク管理」のPDCAサイクルが回っている状態であることを解説しました。PDCAサイクルが回っていればたとえ一部が導入されていなくても監査時にその状況が把握でき、導入すること自体を失念してしまうことはありませんので、予算や業務繁忙期等のタイミングを考慮しながら順次導入していきましょう。

ここまでで、「マイナンバー対策」として実施すべき①～③の作業が何たるかをイメージしていただけたかと思います。
概念が理解できたら、いよいよ「マイナンバー対策」を実践しましょう！次章では、「マイナンバー対策」の①～③について、具体的な手順を解説します。

4 プロセスの実践

前章では、「マイナンバー対策」とは、大きく3つの作業を指すことについて解説しました。実施すべきことが理解できたら、いよいよここから「マイナンバー対策」の実践です。本章では、前章で解説した①～③の作業について、その具体的な進め方を解説します。

1 業務範囲を限定する

具体的な目標や個別の対処等の検討に入る前に、まずは業務範囲を極力小さくした方がよいということは前章での解説のとおりですが、どのように検討すればよいでしょうか。そのキーは、マイナンバー特設サイトの中で整理した業務内容および業務フロー図にあります。

マイナンバー特設サイトでは、まず今後マイナンバーが係わる業務を特定した上で、5W1Hの観点でそれぞれの業務フロー図を作成し、見直しが必要そうなポイントを特定しました。
これについて、改めて5W1Hの観点から、マイナンバーの取扱範囲を狭めることができないかどうかを検討します。具体的には以下の通りです。

誰が？	マイナンバーを取り扱うメンバーを限定できないか？
何を？	マイナンバーが記載された資料の取り扱いを限定できないか？ 例）紙資料はPDF変換し、全て電子ファイルで保管する。
いつ？	マイナンバーを取り扱う時間を限定できないか？
どこで？	マイナンバーを取り扱う場所を限定できないか？
なぜ？	マイナンバーを取り扱う業務を限定できないか？ 例）年末調整業務の受託を取りやめる。
どのように？	マイナンバーを取り扱う手段を限定できないか？ 例）収集用紙を作成し、顧問先の訪問時に直接授受する。

表を見ていただくと分かるとおり、範囲を狭めるポイントは「集約」または「廃止」です。これから行う個別の対処に無駄が生じてしまわないよう、この機会に改めて自社の業務全体を俯瞰し、効率化できる部分が無いかどうかを検討してみましょう。

なお、本マニュアルでは上記の検討を加えた業務フロー図をサンプルとして掲載していますので、参考にしながら作業を行うと良いでしょう。（サンプルの「緑枠」が本作業を行った部分となります。）
また、その前段として、単純な現行の業務フロー図および問題の特定を行った業務フロー図もマイナンバー特設サイトに掲載していますので、必要に応じて確認してください。

2 「基本方針」、「取扱規程」、「オフィスマニュアル」を作成する

前章にて各ドキュメントの概要を解説しましたが、それぞれどのように作成すればよいでしょうか。ひとつずつ順番に解説します。

「基本方針」の作成

「基本方針」には、主に以下の内容を盛り込むとよいでしょう。対外向けという特徴上、「問い合わせ先」の情報が盛り込まれていることがポイントです。

※自社のホームページや別のドキュメント等で問い合わせ先を公表したい場合には、必ずしも内容に盛り込む必要はありません。

関係法令、ガイドライン等の遵守	個人情報に関する法令、ガイドライン等を遵守する旨を記載します。
利用目的	個人情報の利用目的を明らかにする旨を記載します。
適切な管理	収集、利用、保管、提供において、個人情報を適正に取り扱う旨を記載します。
継続的な改善	「基本方針」等を定期的に見直し、継続的に改善する旨を記載します。
問い合わせ先	個人情報の取扱に関する質問や苦情等の受付窓口を設定する旨を記載します。

作成にあたっては、様々な機関等から提供されているサンプルを自社のポリシーに合わせて組み合わせたり追記することにより、効率的に作成できます。本マニュアルでも弊社が作成したサンプルを掲載していますので、参考にしながら作成してください。

「取扱規程」の作成

「取扱規程」には、主に以下の内容を盛り込むとよいでしょう。

適用範囲	「取扱規程」を適用する範囲を記載します。
定義	「取扱規程」の中で扱う用語の定義を記載します。
組織体制	個人情報保護責任者等、各種責任者の責務を記載します。
適切な管理	収集、利用、保管、提供において、「本人確認」「安全管理措置」「監督責任」「説明責任」を適正に実施するための取扱方法を記載します。
監査	運用状況を確認し、必要に応じて見直し、是正するための手順を確立するとともに、それらを確実に実施する旨を記載します。
継続的な改善	「取扱規程」等を定期的に見直し、継続的に改善する旨を記載します。

上記を確認していただくと分かるとおり、「基本方針」は「取扱規程」を対外向けにアレンジして作成しているため、盛り込むべき内容は同様です。
また、「基本方針」と同じく作成にあたっては、様々な機関等から提供されているサンプルを自社のポリシーに合わせて組み合わせたり追記することにより、効率的に作成できます。本マニュアルでも弊社が作成したサンプルを掲載していますので、参考にしながら作成してください。

　なお、「基本方針」「取扱規程」の作成にあたっては、マイナンバーに関する法令やガイドラインで求められていることの概要を前提知識として理解している必要があります。
したがって、もしその習熟度について不安があれば、作業に取り掛かる前にマイナンバー特設サイトを確認しておくことをおすすめします。

「オフィスマニュアル」の作成

「オフィスマニュアル」は、前項の「①業務範囲を限定する」という作業の中で作成した自社の業務フローをベースに、「適切な管理」の4つの観点で求められる要件を満たすために自社が行う個別の対処について、網羅的に記載していきます。
個別の対処に用いる手法の内容によって記載する内容が変わりますので、都度手法を選定しながら記載を進めていくようにしてください。
また、記載にあたっては、それぞれの個別の対処について「小さなPDCA」が回るように意識することがポイントです。

本人確認	マイナンバーを正しく収集するために、確認作業を行うこと
安全管理措置	漏えい、滅失、毀損の防止等のために措置を講じること
監督責任	個人番号関係事務を委託する場合にも、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ように、必要かつ適切な委託先の監督を行うこと
説明責任	(提供する側が) 根拠を持って提供できるように、収集時に目的を通知または公表すること

(マイナンバー特設サイトより)

各観点で求められる要件と、それを満たすための個別の対処に用いる手法についてはマイナンバー特設サイトで詳しく解説していますので、参考にしながら作成すると良いでしょう。
また、本マニュアルに弊社が作成したサンプルも掲載していますので、必要に応じて活用してください。

3 整備したルールの通りに運用が回るよう歯止めをかける

前章にて、歯止めの作業として以下の作業を実施する必要があることを解説しましたが、それぞれどのように進めていけばよいでしょうか。順番に解説します。

従業者への啓発活動の実施

前章にて、PDCAを回すためには、従業者に対してマイナンバーを厳重に取り扱う必要性およびその詳細な取扱方法をしっかりと説明することが重要であると解説しました。

まずはマイナンバーを厳重に取り扱う必要性について意識啓発することが重要です。マイナンバーの漏えい等を引き起こしてしまった場合のリスクについて、実際の事故事例、自社の事業もしくは従業者個人に対する影響等を交えて説明すると良いでしょう。また、マイナンバー特設サイトの中でも「マイナンバー対策」が必要な理由についてひと通り解説していますので、それを活用することもおすすめします。

厳重に取り扱う必要性を理解してもらうことができたら、その上で詳細な取扱方法を説明します。単純な個々のルールだけでなく、その目的や背景についても補足しながら、「基本方針」、「取扱規程」、「オフィスマニュアル」等を活用して説明すると良いでしょう。

個別の対処を導入する

前章にて、「オフィスマニュアル」の作成時に選定した個別の対処が何ひとつ導入されないままではPDCAを回す意味が無いということを解説しました。ひと通り選定して「オフィスマニュアル」にまとめることができたら、対処に用いるツール等を洗い出して対応の優先順位を検討し、計画表を作成して順次導入していきましょう。

計画の策定および実際の対応にあたっては、専門家にアドバイスを仰ぎながら進めることが得策です。契約書の見直しについては弁護士等、システムの導入であればシステムベンダ等に相談すると良いでしょう。

なお、もし契約面について自社内で対応したい場合には、日本税理士会連合会『税理士のためのマイナンバー対応ガイドブック～特定個人情報の適正な取扱いに向けて～』にサンプルが揃っているので参考にすると良いでしょう。

詳細はガイドブックを確認していただきたいのですが、見直しの方法も1通りではありません。既存の契約書を改変することはもちろん、別途「覚書」を定めることにより契約変更の処理を簡潔化する方法もありますので、見直し方法を含めて検討してください。
ちなみに、基本的には既存の契約書を改変するスタンスで記載していますが、もし現状整備していない契約書等（「就業規則」「誓約書」等）があれば、トラブルを未然に防ぐためにもこの機会に作成することをおすすめします。

5 おわりに

ここまで、「マイナンバー対策」とは何たるか、また、それをどのように実践すべきか、ということについて順を追って解説してきました。いかがでしたでしょうか。自社で「マイナンバー対策」に取り組むことができそうでしょうか？

繰り返しになりますが、決してむやみにシステムやツールをたくさん導入することの無いようにしていただきたいと思います。誤解を恐れずに言うと、そのシステムやツール自体には意味が無いからです。注力すべきは、あくまで持続的にPDCAサイクルを回せる状態を整備することであり、システムやツールというのはその一端にすぎません。
これを念頭に置いて、まずは現行の業務の在り方をなるべくシンプルにした上で、最小限の労力とコストで個々の対処を検討していただきたいと思います。

いよいよ始まるマイナンバー制度。これから皆様は「マイナンバー対策」に本腰を入れて取り組まれることと思いますが、本マニュアルをご一読いただいたことにより、少しでも「マイナンバー対策」のイメージが明瞭となり、前向きに取り組むモチベーションが生まれていれば幸いです。

本マニュアルに関するお問い合わせ

達人インフォメーションセンタにてお問い合わせを受け付けています。
TEL：0120-554-620
受付時間：9時～12時、13時～17時
※土・日・祝日および弊社休業日を除く

6 参考

1 資料

- 日本税理士会連合会「税理士のためのマイナンバー対応ガイドブック～特定個人情報の適正な取扱いに向けて～」（平成27年4月版）
- 内閣官房・内閣府・個人情報保護委員会・総務省・国税庁・厚生労働省「マイナンバー　社会保障・税番号制度　民間事業者の対応」（平成29年9月版）
- 特定個人情報保護委員会「特定個人情報適正な取扱いに関するガイドライン（事業者編）」（平成26年12月11日版）
- 国税庁「国税分野における番号法に基づく本人確認方法【事業者向け】」（平成27年3月版）

2 ホームページ

- 内閣官房「マイナンバー　社会保障・税番号制度」
- 特定個人情報保護委員会「特定個人情報保護委員会」
- 国税庁「社会保障・税番号制度<マイナンバー>について」
- 株式会社NTTデータ マイナンバー特設サイト

別添　サンプル

1 別添資料1

業務フロー

2 別添資料2

個人情報の保護に関する基本方針

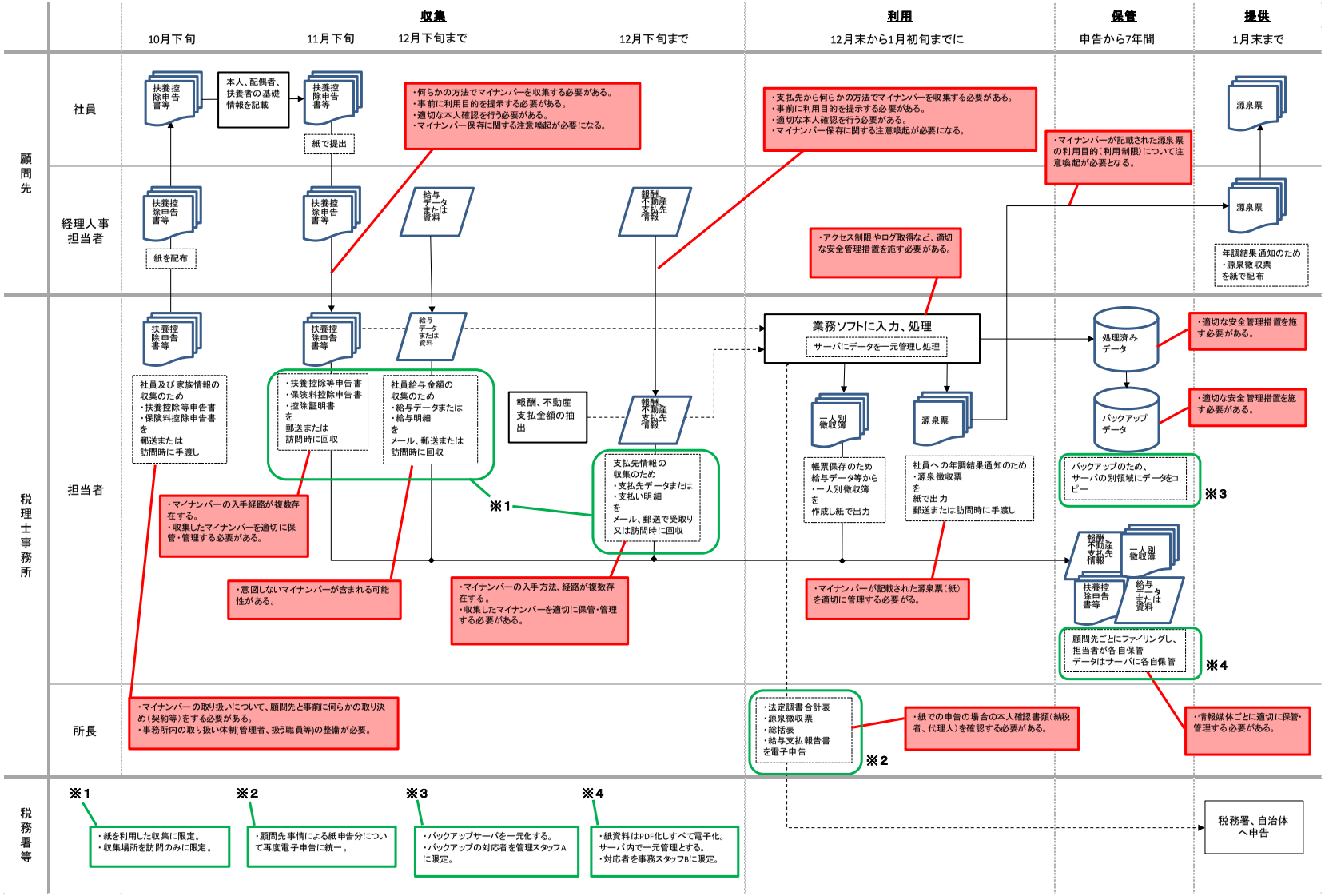
3 別添資料3

個人情報取扱規程

4 別添資料4

オフィスマニュアル

別添資料1
業務フロー（業務範囲を限定する）


収集
利用
保管
提供
10月下旬
11月下旬
12月下旬まで
12月下旬まで
12月末から1月初旬までに
申告から7年間
1月末まで
顧問先
税理士事務所
税務署等
社員
経理人事担当者
担当者
所長
扶養控除申告書等
本人、配偶者、扶養者の基礎情報を記載
紙で提出
紙を配布
給与データまたは資料
報酬、不動産支払先情報
・何らかの方法でマイナンバーを収集する必要がある。
・事前に利用目的を提示する必要がある。
・適切な本人確認を行う必要がある。
・マイナンバー保存に関する注意喚起が必要になる。
・支払先から何らかの方法でマイナンバーを収集する必要がある。
・事前に利用目的を提示する必要がある。
・適切な本人確認を行う必要がある。
・マイナンバー保存に関する注意喚起が必要になる。
・マイナンバーが記載された源泉票の利用目的（利用制限）について注意喚起が必要となる。
源泉票
年調結果通知のため
・源泉徴収票
を紙で配布
・アクセス制限やログ取得など、適切な安全管理措置を施す必要がある。
社員及び家族情報の収集のため
・扶養控除等申告書
・保険料控除申告書
を
郵送または
訪問時に手渡し
・扶養控除等申告書
・保険料控除申告書
・控除証明書
を
郵送または
訪問時に回収
社員給与金額の収集のため
・給与データまたは
・給与明細
を
メール、郵送または
訪問時に回収
報酬、不動産支払金額の抽出
支払先情報の収集のため
・支払先データまたは
・支払い明細
を
メール、郵送で受取り又は訪問時に回収
※1
業務ソフトに入力、処理
サーバにデータを一元管理し処理
一人別徴収簿
源泉票
帳票保存のため給与データ等から
・一人別徴収簿
を
作成し紙で出力
社員への年調結果通知のため
・源泉徴収票
を
紙で出力
郵送または訪問時に手渡し
処理済みデータ
バックアップデータ
・適切な安全管理措置を施す必要がある。
・適切な安全管理措置を施す必要がある。
バックアップのため、サーバの別領域にデータをコピー
※3
順問先ごとにファイリングし、担当者が各自保管
データはサーバに各自保管
※4
・マイナンバーの入手経路が複数存在する。
・収集したマイナンバーを適切に保管・管理する必要がある。
・意図しないマイナンバーが含まれる可能性がある。
・マイナンバーの入手方法、経路が複数存在する。
・収集したマイナンバーを適切に保管・管理する必要がある。
・マイナンバーが記載された源泉票（紙）を適切に管理する必要がある。
・マイナンバーの取り扱いについて、顧問先と事前に何らかの取り決め（契約等）をする必要がある。
・事務所内の取り扱い体制（管理者、扱う職員等）の整備が必要。
・法定調書合計表
・源泉徴収票
・総括表
・給与支払報告書
を電子申告
※2
・紙での申告の場合の本人確認書類（納税者、代理人）を確認する必要がある。
・情報媒体ごとに適切に保管・管理する必要がある。
税務署、自治体へ申告
※1
・紙を利用した収集に限定。
・収集場所を訪問のみに限定。
※2
・順問先事情による紙申告分について再度電子申告に統一。
※3
・バックアップサーバを一元化する。
・バックアップの対応者を管理スタッフAに限定。
※4
・紙資料はPDF化しすべて電子化。サーバ内で一元管理とする。
・対応者を事務スタッフBに限定。

別添資料2
個人情報の保護に関する基本方針

個人情報の保護に関する基本方針

〇〇税理士事務所は（以下、「当事務所」と記す。）は、個人情報（個人番号および特定個人情報含む）の重要性を深く認識しております。個人情報保護の取り組みを真摯に実行することは社会的責務であると考え、以下の通り個人情報保護方針を定め、従業者に周知し、徹底を図ります。

1.個人情報に関する法令およびその他の規範の遵守
当事務所は、個人情報の取扱いに関する法令、国が定める指針その他の関連規範を遵守します。

2.適切な収集、利用、保管、提供
1）個人情報の収集にあたっては、利用目的を明らかにした上で取得します。取得した個人情報はその目的以外に利用せず、利用範囲を限定し、取扱規程に基づき適切に取扱います。
2）取得した個人情報の取扱いを、第三者に委託する場合には十分な個人情報保護の水準を備える者を選び、また、契約等によって安全管理措置を講じるよう定めた上で、必要かつ適切な監督を実施します。

3.安全管理措置
当事務所は、お客様の個人情報を厳格に管理し、滅失、毀損、漏えいや不正アクセスなどの危険性に対して適切な安全管理措置を講じます。

4.継続的な改善
当事務所は、個人情報の保護が効果的に実施されるよう、本基本方針および内部規程等を継続して改善します。

5.質問および苦情等の窓口
当事務所所定の窓口にて、合理的な範囲で対応いたします。

制定日　平成yy年mm月dd日
〇〇税理士事務所
所長　〇〇　〇〇

別添資料3
個人情報取扱規程

個人情報取扱規程

個人情報取扱規程を次の通り定める。

第1章　目的

（目的）
第1条
本規程は、当事務所が適切に個人情報（個人番号及び特定個人情報含む）を扱うために遵守すべき項目を定めることを目的とし、個人情報の取扱いに関する法令、国が定める指針その他の関連規範に準拠して定めるものである。

第2章　適用範囲

（対象となる業務）
第2条
本規程は、当事務所のすべての業務に適用される。

（対象となる個人情報）
第3条
本規程は、当事務所の業務を遂行する上で取扱うすべての個人情報に適用される。

（対象者）
第4条
本規程は、当事務所のすべての従業者に適用される。

第3章　定義

（定義）
第5条
本規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 個人情報
生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、個人番号その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。
(2) 個人番号
住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。
(3) 特定個人情報
個人番号をその内容に含む個人情報をいう。
(4) 特定個人情報等
個人番号及び特定個人情報のいずれかに該当するものをいう。
(5) 個人情報データベース等
個人情報を含む情報の集合物であって、特定の個人情報について電子計算機を用いて検索することができるように体系的に構成したもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして個人情報の保護に関する法律施行令で定めるものをいう。
(6) 個人情報ファイル
個人情報データベース等であって、行政機関及び独立行政法人等以外の者が保有するものをいう。
(7) 特定個人情報ファイル
個人番号をその内容に含む個人情報ファイルをいう。
(8) 個人データ
個人情報データベース等を構成する個人情報をいう。
(9) 個人番号利用事務
行政機関、地方公共団体、独立行政法人等その他の行政事務を処理する者が番号法の定めにより、必要な限度で個人番号を利用して処理する事務をいう
(10) 個人番号関係事務
個人番号利用事務に関して行われる他人の個人番号を必要な限度で利用して行う事務をいう。
(11) 個人番号利用事務実施者
個人番号利用事務を処理する者及び個人番号利用事務の全部又は一部の委託を受けた者をいう。
(12) 個人番号関係事務実施者
個人番号関係事務を処理する者及び個人番号関係事務の全部又は一部の委託を受けた者をいう。
(13) 個人情報保護責任者
所長が指名する者であって、本規程に基づく個人情報の管理の実施及び運用に関する責任と権限を有する者をいう。
(14) 個人情報保護管理者
個人情報保護責任者が指名する者であって、安全管理措置の実施及び運用に関する責任と権限を有する者をいう。

(15) 個人情報保護監査責任者
所長が指名する者で、個人情報保護責任者から独立した公平、かつ、客観的な立場にあり、監査の実施及び報告を行う責任及び権限を有する者をいう。

第4章　組織及び実施責任

（所長の責務）
第6条
所長は、次の事項を含む基本方針を定めるとともに、これを実行し、かつ、維持するものとする。
(1) 個人情報の取扱いに関する法令、国が定める指針その他の規範を遵守すること
(2) 個人情報の漏えい、滅失又は毀損の防止及び是正に関すること
(3) 個人情報の管理の継続的改善に関すること
(4) 質問及び苦情等への対応に関すること
(5) 所長の氏名
2所長は、基本方針を文書化し、従業者に周知するとともに、一般の人が入手可能な措置を講じるものとする。
3所長は、個人情報保護責任者を社内から指名し、個人情報保護責任者としての義務を行わせるものとする。
4所長は、本規程の内容を理解し公平、かつ、客観的な立場にある者を指名し、個人情報保護監査責任者としての責務を負わせるものとする。

（個人情報保護責任者の責務）
第7条
個人情報保護責任者は本規程に基づく個人情報の管理の実施及び運用に関する責務を負うものとする。
2個人情報保護責任者は、個人情報を取扱う業務に従事する者に本規程を理解させる責務を負うものとする。
3個人情報保護責任者は、顧問先や従業者からの個人情報に係る質問・苦情等について、責務を負うものとする。
4個人情報保護責任者は、必要に応じて個人情報保護管理者を指名し、個人情報保護管理者としての責務を負わせるものとする。

（個人情報保護管理者の責務）
第8条
個人情報保護管理者は、個人情報を保護するための安全管理措置の実施及び従業者の教育・監督等を実施する責務を負うものとする。
2個人情報保護管理者は個人情報を取扱う業務に従事する者を限定して指名し、業務の範囲と取扱う情報の範囲を指定する責務を負うものとする。

（個人情報保護監査責任者の責務）
第9条
個人情報保護監査責任者は、本規程が適切かつ有効に実施されているかを定期的に評価し、所長に報告する責務を負うものとする。

（個人情報の保護に関する従業者の責務）
第10条
当事務所で個人情報を取扱う業務に従事する者は、法令の規定、本規程又は個人情報保護責任者が指示した事項に従い、十分な注意を払いつつその業務を行うものとする。

第5章　計画

（内部規程等及び記録）
第11条
当事務所は、個人情報保護に関する内部規程等を文書化し、かつ、維持するものとする。
2当事務所は、本規程及び内部規程等への適合を実証するために必要な記録を作成し、かつ、維持するものとする。

（個人情報の特定）
第12条
当事務所は、当事務所で利用するすべての個人情報を特定するものとし、特定した個人情報を定期的に見直すものとする。

（安全管理措置）
第13条
当事務所は、特定した個人情報について、その取扱いの各局面におけるリスク（漏えい、滅失又は毀損などのおそれ）を認識し、分析し、組織面、人的管理面、物理面及び技術面において合理的な安全管理措置を講ずるものとする。
2当事務所は、新たな個人情報を特定したとき又は周辺環境に変化が生じたときは必要に応じて安全管理措置の見直しを実施するものとする。

第6章　個人情報の収集に関する措置

（個人情報の収集制限）
第14条
個人情報の収集は、具体的な利用目的を特定し、その目的の達成に必要な範囲内においてこれを行う。

2個人番号の収集に当たっては、個人番号関係事務又は個人番号利用事務を処理するために必要がある場合に限り、本人又は他の個人番号関係事務実施者もしくは個人番号利用事務実施者に対して個人番号の提供を求めることができる。

（個人情報を収集する場合の措置）
第15条
個人情報を収集する場合、利用目的の通知等を行う。
2特定個人情報等の収集に当たっては、番号法等関係法令及び告示等に基づき個人番号の確認及び本人確認を実施する。

第7章　個人情報の利用に関する措置

（個人情報の利用制限）
第16条
個人情報の利用は、具体的な利用目的を特定し、その目的の達成に必要な範囲内においてこれを行う。
2特定した目的の達成に必要な範囲を超えて個人情報を利用する場合は、利用目的の本人への再通知等を行う。ただし、人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意がある又は本人の同意を得ることが困難である場合は、この限りではない。
3特定個人情報等の利用に当たっては、個人番号関係事務又は個人番号利用事務を処理するために必要な範囲を超えて、特定個人情報ファイルは作成してはならない。

第8章　個人情報の保管に関する措置

（個人情報の保管制限）
第17条
個人情報の保管は、保管期間を定め、その保管期間の範囲内においてこれを行う。
2保管期間の経過等により保管の必要がなくなった個人情報について、廃棄又は削除の処理を行うものとする。
3個人番号の廃棄又は削除に当たっては、個人番号関係事務又は個人番号利用事務を行う必要がなくなった場合で、所管法令等において定められている保存期間を経過した場合には、できるだけ速やかにこれを行う。
4廃棄又は削除を行う場合は、再利用できない措置を講じてから廃棄するものとする。

第9章　個人情報の提供に関する措置

（個人情報の提供制限）
第18条
個人情報の提供は、具体的な提供目的を特定し、その目的の達成に必要な範囲内においてこれを行う。
2提供するに当たって、本人の同意を得た上で実施するものとする。ただし所管法令等において定められている場合及び、人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難な場合は、この限りではない。
3特定個人情報等の提供は、以下の場合を除き行わない。
(1) 個人番号利用事務実施者が、個人番号利用事務を処理するために、必要な限度で本人、代理人又は個人番号関係事務実施者に特定個人情報を提供する場合
(2) 個人番号関係事務実施者が、個人番号関係事務を処理するために、法令に基づき、行政機関等、健康保険組合等又はその他の者に特定個人情報を提供する場合
(3) 本人又はその代理人が、個人番号関係事務実施者又は個人番号利用事務実施者に対し、本人の個人番号を含む特定個人情報を提供する場合
(4) 特定個人情報の取扱いの全部若しくは一部の委託又は合併その他の事由による事業の承継が行われた場合
(5) 特定個人情報保護委員会から特定個人情報の提出を求められた場合
(6) 人の生命、身体又は財産の保護のために必要な場合
(7) その他公益上の必要から提出を求められた場合

（委託に関する措置）
第19条
当事務所が個人情報の取扱いを委託する場合は、委託先選定基準に基づき、十分な保護水準を提供する者を選定するものとする。
2当事務所が個人情報の取扱いを委託する場合は、契約において当事務所の安全管理措置と同等の措置が講じられることを規定し、十分な保護水準を担保するものとする。
3当事務所が個人情報の取扱いを委託する場合は、委託する個人情報の保護が図られるよう、委託先に対する監督を行うものとする。
4当事務所が受託した特定個人情報等を取扱う業務を委託する場合、最初の委託元の承諾を得る。

第10章　開示等の求め、苦情、及び相談

（開示等の求め）
第20条
当事務所は、本人に対し開示対象となる個人情報について、本人又は法定代理人等から開示等の求めを受けた場合は、遅滞なくこれに応じるものとする。ただし、本人の求めに応じることで所管法令等において定められている利用ができなくなる場合はこの限りでない。

（苦情及び相談）
第21条
当事務所は、個人情報の取扱いに関して、本人又は法定代理人等からの苦情及び相談を受け付け、適切、かつ、迅速な対応を行う手順を確立し、かつ、維持するものとする。
2当事務所は、上記の目的を達成するために必要な体制を整備し、本人が認知できるよう公表するものとする。

（緊急事態への準備）
第22条
当事務所は、個人情報に関する侵害が発生した場合に備え、対応手順を確立し、維持するものとする。

第11章　運用の確認及び監査

（運用の確認及び監査）
第23条
当事務所は、個人情報の保護に関する措置の運用状況、及び本規程への適合状況を定期的に確認するための手順を確立し、実施し、かつ、維持するものとする。

（是正処置及び見直し）
第24条
当事務所は、個人情報の適切な保護を維持するために、個人情報の管理の見直し、及び改善に取り組むものとする。

第12章　雑則

（罰則）
第25条
本規程に違反した従業者又は自らの職務を適正に遂行していれば違反を知り得ることができた従業者は、就業規則等に基づき処分を行う。

（細則等）
第26条
本規程の運用に必要な細則、及び個人情報保護を実践するための手順等は別に定めるものとする。

附則（平成yy年mm月dd日）
本規程は、平成yy年mm月dd日から実施する。

別添資料4
オフィスマニュアル

オフィスマニュアル記載にあたっての前提条件

本マニュアル作成にあたっての前提条件を記載します。

対処の観点	採用した手法
番号確認、身元確認	・番号確認、身元確認の証跡は保管しないことと設定しました。
故意による情報漏えいの抑止手段	・従業者から配属時に誓約書を取得する手法のみを採用しました。
教育	・責任者から定期的に教育を実施することと設定しました。 ・配属の際にも教育を実施し、定期的な教育を受講していない人が教育を受ける機会を設けています。 ・なお、各ルールの遵守状況の確認、または点検を教育と位置付けています。
事務所の管理区域、取扱区域	・管理区域と取扱区域をオフィスマニュアル上に記載する手法を採用しました。 ・事務所内に応接に使用する場所があることを想定し、事務所内を管理区域と取扱区域とに区分しました。税理士事務所では、従業者全員が個人情報を取り扱うことになる場合も多いと想定し、取扱区域とその他の事務の場所とは分離していません。（特定個人情報も同様） ・管理区画は、個人情報ファイルを取り扱う情報システムが設置される場所としました。
・管理区域、取扱区域に入室する権限を持つ人が入室する際の手順 ・管理区域、取扱区域に入室する権限を持たない人（社内、社外含む）が入室する際の手順	・入室を制限する手法は、以下と設定しました。 ・事務所　：事務所の扉に鍵がある。勤務時間帯は開錠されており、訪問者は事務所の応接の場所に入ることができる。 ・取扱区域：取扱区域と事務所の境は、パーテーションや扉等は設置していない。従業者証（名札）によって、取扱区域の中に入ることができる人とそうでない人を、従業者が目で見て判断する。 ・管理区域：情報システムをサーバラックで囲い、鍵で施錠している。通常時は施錠されており、必要な場合にのみ開錠する。個人情報が保管されるキャビネットは、通常時は施錠されており、必要な場合にのみ開錠する。

対処の観点	採用した手法
情報機器、記憶媒体の特定	・情報機器、記憶媒体を一つの管理簿で管理する手法を採用しました。
持ち出し時に情報が漏えいしない仕組み	・持ち出しの手法は、以下と設定しました。 ・電子データ：パスワードを設定する ・紙資料　：内容物が見えないように封筒に入れる
移送時の追跡可能な仕組み	・原則手渡しとし、やむを得ない場合のみ移送を認めることとしています。 ・移送の手法は、記録の残る方法として、書留、宅配便を利用することと設定しました。
保管時の紛失・盗難防止の仕組み	・保管の手法は、以下と設定しました。 ・情報機器：セキュリティワイヤーでPCを固定する ・記憶媒体：キャビネットに施錠保管する ・紙媒体　：キャビネットに施錠保管する、クリアデスクを徹底する
情報の廃棄時に情報が漏えいしない仕組み	・廃棄の手法は、以下と設定しました。 ・情報機器：外部の業者に廃棄を委託する ・紙媒体　：シュレッダーで裁断する ・記憶媒体：メディアシュレッダーで破壊する ・なお、情報機器の廃棄は事務所だけで完結しないため、廃棄時に記録を取得することとしています。
認証の仕組み（アクセス制御）の実装	・情報システム、PC等の情報機器において、認証の仕組みが実装されていると設定しました。
システムの利用者を管理する方法 （アカウント管理）	・アカウント管理の手法は以下と仮定しました。 ・情報システム　：ID、パスワードを用いてアクセス制御をする ・PC等の情報機器：機器毎にID、パスワードを用いてアクセス制御をする （Workgroupでの利用を想定しています） ・なお、払い出した情報システムのIDを管理簿で一元管理することを想定しています。
インターネットからの不正アクセスを防止する仕組み	・不正アクセス防止の手法は、OSのファイアウォール機能を利用することとしました。

対処の観点	採用した手法
悪意のあるソフトウェアの感染を防止する仕組み	・悪意のあるソフトウェアの感染を防止するための手法は以下と設定しました。 ・ウイルス対策ソフトの導入 ・インターネットを私的に利用することの禁止 ・事務所で所有するソフトウェア以外のインストールの禁止 ・セキュリティパッチの適用
情報送信時に情報が漏えいしない仕組み	・情報の送信の手段は、FAXとファイル転送サービスと設定しました。 ・情報送信時に情報が漏えいすることを防止するための手法は以下と設定しました。 ・電子データ：ファイルにパスワードを設定し、目的達成後にファイルを即時消去する ・また、誤送信防止のためにダブルチェックをすることとしました。
委託先における特定個人情報の取り扱い状況を確認する手法	・委託先における特定個人情報の取り扱い状況を確認する手法は、委託先にチェックリストを提示して報告を受けることと設定しました。

目次

1.　本マニュアルの目的

オフィスマニュアル（以下、「本マニュアル」という）は、当事務所において業務（以下、「本業務」という）の遂行のために受領する個人情報等を取り扱うにあたり、情報セキュリティ上の基本事項を、定めたものである。
従業者一人ひとりが本マニュアルを理解、遵守し、積極的かつ安全に業務を遂行することを期待する。

2.　定義

本マニュアルでは、以下のように用語を定義する。

用語	定義
従業者	当事務所で従事する者
PC等の情報機器	PC、タブレット端末、サーバ、プリンタ、FAX、ネットワーク機器（ルータ、スイッチ等）等のハードウェア
記憶媒体	USBメモリー、フロッピーディスク、SDカード、MOディスク、外付けHDD、その他電子データをPCの外に記憶させ、移動させることが可能な情報機器

3.　役割、責任

当事務所のセキュリティ管理における役割、責任を以下と定める。

責任者名		役割
個人情報保護責任者		当事務所の個人情報保護に関する取り組みの最高責任者であり、個人情報の管理に関する責任を有する者。所長がその任を負うものとする。
個人情報保護管理者	人的安全管理措置実施責任者	個人情報保護責任者によって任命された、当事務所の人的安全管理措置の構築、運用に関する責任を有する者
	物理的安全管理措置実施責任者	個人情報保護責任者によって任命された、当事務所の物理的安全管理措置の構築、運用に関する責任を有する者
	技術的安全管理措置実施責任者	個人情報保護責任者によって任命された、当事務所の技術的安全管理措置の構築、運用に関する責任を有する者

- 個人情報保護責任者は、毎年1回5月、または各責任者の異動、退職等が発生した都度、各責任者の任命、解任の必要性を検討し、各責任者をセキュリティ体制図に反映する

4.　物理的区画およびアクセス制御

本章に定める項目に関する管理は、特段の定めがない限り、物理的安全管理措置実施責任者が担うものとする。物理的安全管理措置実施責任者は、定期的に、区画、入退室に関するアクセス制御の適切性を評価し、必要に応じて見直しを行うこと。

4.1. 物理的区画

当事務所のオフィスは次の区画に区分する。

区画	定義	場所
エリア1	来訪者と応対するエリア	応接ブース
エリア2 （取扱区域）	個人情報を取り扱う業務を行う区域であり、当事務所の居室全体から応接ブースを除くエリア	事務所執務エリア
エリア3 （管理区域）	以下のエリア ・ 個人情報を保管するシステムのサーバを格納するラック ・ 個人情報を保管するキャビネット	サーバラック、キャビネット

4.2. アクセス可能者、およびアクセス制御方法

当事務所の区画へのアクセス可能者およびアクセス制御方法は以下とする。

区画	アクセス可能者	アクセス制御方法
エリア1	・ 制限なし	当事務所の施錠
エリア2 （取扱区域）	・ 従業者 ・ 従業者の許可を得た来訪者	当事務所の施錠、および、来訪者受付票による管理
エリア3 （管理区域）	・ 業務上必要性に基づき、物理的安全管理措置実施責任者に、アクセスを許可された者	サーバラック、キャビネットの施錠、および、鍵管理簿による管理

5.　鍵の利用ルール

当事務所、および個人情報を保管するキャビネットの鍵、サーバラックの鍵は、個人情報保護責任者および物理的安全管理措置実施責任者が管理を行うものとする。
物理的安全管理措置実施責任者は、鍵の管理に関して以下を実施すること。

- 個人情報を保管するキャビネットの鍵、サーバラックの鍵を所定の場所に施錠保管する
- 鍵管理簿を用いて鍵の利用を管理するとともに、管理簿を維持管理する
- 定期的に鍵の棚卸を実施する
- 本章に定めるルールの遵守状況を定期的に確認し、必要に応じて是正、およびルールの見直しを行う

サーバおよび個人情報を保管するキャビネットに対して、個人情報保護責任者、または物理的安全管理措置実施責任者以外の者で、かつ業務上の必要性に基づき、物理的安全管理措置実施責任者に、アクセスを許可された者がアクセスする場合は、鍵管理簿に記入した上で利用すること。

6.　入退室のルール

本章に定める項目に関する管理は、特段の定めがない限り、物理的安全管理措置実施責任者が所掌するものとする。
物理的安全管理措置実施責任者は、入退室に関するアクセス制御および入退室の管理に関して、以下を実施すること。

- 従業者証の払い出しを行う
- 来訪者受付票の記録を所定の場所に施錠保管する
- 本章に定めるルールの遵守状況を定期的に確認し、必要に応じて是正、およびルールの見直しを行う

6.1. 従業者の入退室

- 当事務所のエリア2（取扱区域）は、物理的安全管理措置実施責任者が払い出した従業者証を着用している者のみが入室可能であるものとする
- 従業者は従業者証を常時着用し、従業者証を着用していない者がエリア2（取扱区域）に滞在している場合は、物理的安全管理措置実施責任者に連絡する
- 貸与された従業者証の他人への貸与、譲渡を禁止とする
- 従業者証を紛失した場合は、物理的安全管理措置実施責任者に連絡する
- 事務所は最終退室時、または従業者不在時に事務所の施錠を行う（参照：7.3最終退出時の実施事項）
- 管理区域は、業務上の必要性に基づき、物理的安全管理措置実施責任者に、アクセスを許可された者のみがアクセスすることを確実にするため、常時施錠する

6.2. 来訪者への応対

- 来訪者は原則としてエリア1で応対する
- 郵便局員、宅配業者等が、受け渡し、物品の授受、連絡等の目的で当事務所を訪れた場合、従業者は、訪問者の入室を当該目的の達成に必要な範囲内に制限して、訪問者が退館するまで訪問者から目を離さないようにする
- 来訪者がエリア2（取扱区域）に入室する場合には、来客者に以下の対応を依頼する
  ① 来訪者受付票への記入
  ② 入館証の常時着用
- 業務上の必要性があり、来訪者がエリア3（管理区画）にアクセスする場合には、上記に加え、以下を実施する
  ① 物理的安全管理措置責任者の承認
  ② 物理的安全管理措置責任者が指定する者の立会い

7. 事務所利用のルール

本章に定める項目に関する管理は、特段の定めがない限り、物理的安全管理措置実施責任者が所掌するものとする。物理的安全管理措置実施責任者は本章に定めるルールの遵守状況を定期的に確認し、必要に応じて是正、およびルールの見直しを行うこと。

7.1. 一時離席時の実施事項

一時的に離席する場合は、以下を実施する。

- PCのロック、またはパスワードつきスクリーンセーバー（起動時間10分以内）を設定する
- 机上の書類、記憶媒体については、引出しの中にしまう等人目が付かないようにする

7.2. 帰宅時の実施事項

帰宅時には、以下を実施すること。

- 机上に機密書類や記憶媒体を置いたままにせず、所定の場所に施錠保管する
- PCをシャットダウンする
- 各自の袖机を施錠する

7.3. 最終退出時の実施事項

最終退出者は、以下を実施すること。

- 窓、出入口の施錠の確認
- 火事の恐れがあるような電気機器の電源が切られていることの確認
- 消灯

事務所の鍵は、原則、個人情報保護責任者および物理的安全管理措置実施責任者が管理を行うが、最終退室時に、個人情報保護責任者、物理的安全管理措置実施責任者が不在である場合は、最終退室者が翌営業日に返却を行うこととする。

7.4. 宅配便等利用時の実施事項

宅配便等を利用する場合は、以下を実施すること。

- 発送物はエリア2（取扱区域）内に置く
- 荷物はエリア1で受け渡しを行う
- 受け渡しの際は立ち合いを行う
- 受け取った荷物を速やかに担当者に渡す

7.5. 複合機（FAX、コピー機）利用時の実施事項

複合機利用時は、以下を実施すること。

- 印刷した書類やＦＡＸ等を速やかに回収する
- 長時間放置されている書類がある場合は、物理的安全管理措置実施責任者に渡す

8. 情報の管理ルール

本章に定める項目に関する管理は、特段の定めがない限り、物理的安全管理措置実施責任者が所掌するものとする。物理的安全管理措置実施責任者は情報の管理に関して、以下を実施すること。

- 個人情報管理台帳を作成し、維持する
- 情報の移送に関する記録を所定の場所に施錠保管する
- 持出管理表を維持管理する
- PC等の情報機器、およびメディアシュレッダー処理が実施できない記憶媒体の情報について、復元できない方法での削除を実施する

- 外部の業者に廃棄を委託する場合には、廃棄の記録を取得し、所定の場所に施錠保管する
- 本章に定めるルールの遵守状況を定期的に確認し、必要に応じて是正、およびルールの見直しを行う

8.1. 情報の収集のルール

- 個人情報を収集する場合には、以下を実施する
  - ① 利用目的を明文化して提示
  - ② 取得条件に該当しているか確認し、通知（特定個人情報の場合のみ）
  - ③ 本人の番号が正しいことを、証跡（通知カード等）を以て確認（特定個人情報の場合のみ）
  - ④ 本人の身元が正しいことを、証跡（運転免許証等）を以て確認（特定個人情報の場合のみ）
- 個人情報は、法令等の定めに従って保有期間を設定する
- 個人情報管理台帳に記載が無い情報を収集する場合には、物理的安全管理措置実施責任者の確認を取る

8.2. 情報の保管、廃棄のルール

8.2.1. 情報の保管

- 当事務所では、サーバ以外での個人情報（電子データ）の保管を禁止する
- 個人情報を電子データで取得した場合には、速やかにサーバ上に保管し、元データは削除する
- 個人情報を電子データで取得する際に、顧問先の記憶媒体を利用した場合は、顧問先の指示に従う
- 個人情報を書類で取得した場合は、各自の袖机等に保管せず、所定の場所に施錠保管する
- 保有期間が経過した個人情報は、速やかに削除する

8.2.2. 情報の廃棄

- 電子データは、ソフトウェアを利用して完全削除を実施する
- 紙媒体はシュレッダー処理を行う
- 記憶媒体は、メディアシュレッダー処理を行う
- PC等の情報機器、およびメディアシュレッダー処理が実施できない記憶媒体は、物理的安全管理措置実施責任者に廃棄を依頼する

8.3. 情報の提供、利用、流通のルール

- 情報の提供、利用、流通にあたっては、情報を必要最小限に絞った上で実施する
- 特定個人情報を提供する場合には、提供先に利用目的の明示、または説明を求める
- 特定個人情報を提供する場合には、当該特定個人情報が、提供先において個人番号利用事務、個人番号関係事務を処理するために必要があるか否かを、提供先の利用目的に照らして判断した上で提供する

8.3.1. 情報の送信

業務上、個人情報を送信する必要がある場合には、以下の対応を行うこと。

- 当事務所では、電子的な送信手段をFAX、指定のファイル転送サービスと定め、これ以外の手段の利用を禁止とする
- いずれの送信手段においても、送信時に送信先を2名以上で確認し、誤送信を防止する
- ファイル転送サービスを利用する場合には、送信するファイルにパスワードを設定する
- ファイル転送サービスを利用する場合は、目的の達成後にデータの即時消去を行う

8.3.2. 情報の移送

業務上、個人情報を移送する必要がある場合には、以下の対応を行うこと。

- 紙媒体、記憶媒体は、原則手渡しとし、やむを得ない場合を除き、郵送等による送付は不可とする
- やむを得ず郵送等により送付する場合は、書留や宅配便等記録の残る方法で行い、記録を物理的安全管理措置実施責任者に渡す

8.3.3. 情報の持ち出し

業務上、個人情報を持ち出す必要がある場合には、以下の対応を行うこと。

- 紙情報の場合
  - ・ 持出管理表に記入し、物理的安全管理措置実施責任者に申請する
  - ・ 持ち運ぶ際には、内容物が見えないように封筒に入れ、紛失、盗難を防止するために、常に携帯して持ち運ぶ
- 電子データの場合
  - ・ 持ち出し可能なPC等の情報機器、記憶媒体に格納してパスワードを設定する
  - ・ 持出管理表に記入し、物理的安全管理措置実施責任者に申請する
  - ・ 持ち運ぶ際には、紛失、盗難を防止するために、常に携帯して持ち運ぶ
  - ・ 持ち出した目的の達成後にデータの即時消去を行う

9.　PC等の情報機器、記憶媒体の利用ルール

本章に定める項目に関する管理は、特段の定めがない限り、技術的安全管理措置実施責任者が担うものとする。技術的安全管理措置実施責任者は、PC等の情報機器、記憶媒体の管理に関して以下を実施すること。

- 当事務所で利用するすべてのPC等の情報機器、記憶媒体について、導入から廃棄までのプロセスの管理を行う
- 利用者に払い出す前のすべてのPC等の情報機器、記憶媒体を所定の場所に施錠保管する
- 当事務所で利用するすべてのPC等の情報機器、記憶媒体を、情報機器等一覧表を用いて一元管理するとともに、定期的に棚卸を実施し一覧表を最新化する
- 本章に定めるルールの遵守状況を定期的に確認し、必要に応じて是正、およびルールの見直しを行う

技術的安全管理措置実施責任者に任命されたものは以下を実施すること。

- 共用IDの利用を抑制するために、払い出しの際に、PC等の情報機器に、IDおよびパスワードを設定する
- PC等の情報機器の設定方法、および設定内容を利用者に指示する

9.1. PC等の情報機器、記憶媒体の払い出し

新たにPC等の情報機器、記憶媒体の利用が必要な場合は、技術的安全管理措置実施責任者に連絡を行うこと。なお、原則として、記憶媒体は利用の都度払い出しを受け、利用終了時に速やかに返却を行うこと。

9.2. 払い出しを受けたPC等の情報機器、記憶媒体の管理

払い出しを受けたPC等の情報機器、記憶媒体は以下の方法で管理を行うこと。

- ノートPC等容易に取り外して持ち運べる機器は、セキュリティワイヤーで机に固定する
- 記憶媒体は、施錠保管する
- PCは、別途指示する内容に従って設定する

9.3. PC等の情報機器、記憶媒体の持ち出し

- 個人情報が含まれた情報機器、記憶媒体の持ち出しを原則禁止する
- 個人情報を格納した情報機器、記憶媒体を持ち出す場合の方法は、「8.3.3情報の持ち出し」を参照すること

9.4. PC等の情報機器、記憶媒体等の持ち込み

9.4.1. 私物の情報機器、記憶媒体

- 私物のPC等の情報機器、記憶媒体等の持ち込みを禁止する
- 私物のPC等の情報機器、媒体等を当事務所の情報機器に接続すること、および、当事務所の記憶媒体を私物の情報機器に接続することを禁止する

9.4.2. 保守業者等の情報機器、記憶媒体

サーバ、ネットワーク機器の故障等の事象によって、保守業者が情報機器、記憶媒体を持ち込む場合には、技術的安全管理措置実施責任者に連絡を行うこと。

9.5. PC等の情報機器、記憶媒体の返却

PC等の情報機器、記憶媒体が不要となった場合は、技術的安全管理措置実施責任者に即時返却を行うこと。

10. 情報システムおよびネットワークの利用ルール

本章に定める項目に関する管理は、特段の定めがない限り、技術的安全管理措置実施責任者が担うものとする。技術的安全管理措置実施責任者は、個人情報を取り扱う情報システムおよびネットワークの管理に関して以下を実施すること。

- アクセス制御の機能が含まれた情報システムを選定する
- 情報システムで取得するログを明確にするとともに、保管、および維持管理する
- 情報システム、PCのIDを、アカウント管理簿を用いて一元管理する
- 定期的にIDの棚卸を実施する
- 従業者からの申請に基づく、ソフトウェア、およびサービス等の利用について検討を行い、個人情報保護責任者の承認を得る
- 従業者からウイルスに感染等の連絡を受けた場合は、速やかに個人情報保護責任者に報告し、適切に対処を行う
- 本章に定めるルールの遵守状況を定期的に確認し、必要に応じて是正、およびルールの見直しを行う

10.1. ID、パスワードの管理

- 当事務所では、すべての情報システム、PCに対し、利用者個人のIDの設定を行っているため、自分のIDを他人に貸して利用させたり、他人のIDを借りて利用したりしない
- パスワードの設定および運用は以下のルールに従う
  - ① 90日ごとに定期的に変更する
  - ② 英数混在7文字以上とする
  - ③ 2世代前までのパスワードは利用しない
  - ④ パスワードの文字列に、辞書にあるような単語、社名、本人の氏名、電話番号、誕生日等を利用しない
  - ⑤ ID、パスワードを書いた紙等を、他人の目の付く場所に貼らない
- パスワードを忘れたときは、技術的安全管理措置実施責任者に連絡する

10.2. PC・情報システム利用時の注意事項

- OSのファイアウォール機能を無効にすることを禁止する
- 定められたウイルス対策ソフトを使用し、技術的安全管理措置実施責任者の指示に従って、設定、更新等を実施する
- 定期的にハードディスク全体のウイルスチェックを実施する
- 外部から入手したファイルを実行するときには、事前にウイルスチェックを実施する
- OS、およびソフトウェアのセキュリティパッチの適用を実施する
- 当事務所が所有しているソフトウェア以外をインストールすることを禁止する。業務上やむを得ない場合は、技術的安全管理措置実施責任者に申請する
- 違法ソフト、ライセンス違反のソフト、ファイル交換ソフト等の使用は禁止する
- ウイルスに感染した場合、また感染が疑わしい場合には、直ちにネットワークケーブルを外し、技術的安全管理措置実施責任者に報告する

10.3. インターネット利用時の注意事項

- インターネットの利用は業務上必要不可欠な範囲に限定する
- インターネットを私的に利用することを禁止とする
- インターネットの掲示板、SNS等に当事務所での就業により知り得た内容を書き込むことを禁止する
- インターネット上のサービスに、業務に必要不可欠なものがある場合には、技術的安全管理措置実施責任者に申請する

10.4.　電子メール利用時の注意事項

- 電子メールを私的に利用すること、および、受信したメールを私用のメールアカウント等に転送することを禁止する
- 電子メールを用いて情報を送信する際の方法は、「6.3.1情報の送信」に従う
- メールを送信する際には、送信先を十分に確認してから送信する
- 身元の分からない送り主から送られてきたメールは、不用意に開かずに削除するか、技術的安全管理措置実施責任者に連絡し、その指示に従う

11. 従業者の配属時、異動時の実施事項

本章に定める項目に関する管理は、特段の定めがない限り、人的安全管理措置実施責任者が担うものとする。人的安全管理措置実施責任者は以下を実施すること。

- 配属時
  - ① 個人情報の保護に関する教育を実施する
  - ② 配属時の教育記録を維持管理する
  - ③ 従業者から誓約書を取得し、所定の場所に施錠保管する
  - ④ 物理的安全管理措置実施責任者から従業者証を受領し、従業者に貸与する
  - ⑤ 技術的安全管理措置実施責任者からPC等の情報機器を受領し、従業者に貸与する
  - ⑥ 技術的安全管理措置実施責任者からPC等の情報機器、および情報システムのアカウント情報を受領し、従業者に貸与する
- 異動時
  - ① 従業者から従業者証を受領し、物理的安全管理措置実施責任者に引き渡す
  - ② 従業者が引き継ぐ必要のある書類、電子データ等を保有している場合は、書類、電子データを受領し、物理的安全管理措置実施責任者に引き渡す
  - ③ 従業者からPC等の情報機器を受領し、技術的安全管理措置実施責任者に引き渡す

11.1. 配属時

- 教育を受講する
- 人的安全管理措置実施責任者の指示に従い誓約書を提出する
- 従業者証の払い出しを受ける
- PC等の情報機器の払い出しを受ける
- PC等の情報機器、および情報システムのアカウントの払い出しを受ける
- PC等の情報機器を設定する

11.2. 異動時

- 貸与物を返却する
- 引き継ぐ必要のある書類、PC内のデータを人的安全管理措置実施責任者に返却する
- 不要なものをすべて廃棄する

12. 従業者への教育

本章に定める項目は、人的安全管理措置実施責任者が担うものとする。人的安全管理措置実施責任者は、従業者への教育に関して、以下を実施すること。

- 全従業者を対象に、少なくとも年1回、または当マニュアルの改訂時に個人情報の保護に関する教育を行う
- 従業者の配属時に個人情報の保護に関する教育を行う
- 教育の実施記録（理解度アンケート）を維持管理する

13. 業務委託利用時のルール

本章に定める項目に関する管理は、特段の定めがない限り、個人情報保護責任者が所掌するものとする。個人情報保護責任者は本章に定めるルールの遵守状況を定期的に確認し、必要に応じて是正、およびルールの見直しを行うこと。

13.1. 委託先の選定

以下の基準のいずれかを満たした委託先を選定すること。

- プライバシーマークの認定事業者である
- ISMS適合性評価制度の認証取得組織である
- 特定個人情報の適正な取り扱いに関するガイドライン（事業者編）への準拠状況に関する報告を受けることが可能な組織である（特定個人情報を取り扱う場合）

13.2. 委託先との契約

以下の項目を含む契約を締結すること。なお、締結した契約書は、所定の場所に施錠保管すること。

- 秘密保持の義務
- 事務所内からの個人情報の持ち出し禁止
- 個人情報の目的外利用の禁止
- 再委託における条件
- 情報漏えい事案が発生した場合の委託先の責任
- 委託契約終了後等の個人情報の廃棄、または返却
- 委託先従業者に対する監督および教育
- 契約内容の遵守状況の報告

13.3. 委託先の監督

委託先における個人情報の取り扱いが、契約通りに実施されているか確認するために、定期的にチェックリストを用いて報告を受け、適切性の評価を行った後に、契約書とあわせて所定の場所に施錠保管すること。

13.4. 委託、および再委託の際の注意

特定個人情報を取り扱う業務は、委託・再委託を問わず委託元に許可を求める必要があるため、契約に本条項を盛り込むことを確実にすること。

14. ルール遵守状況の確認

本章に定める項目は、個人情報保護責任者が担うものとする。個人情報保護責任者は、当マニュアルの各章で定めた、各責任者によるルール遵守状況の確認に関して、実施されることを確実にするとともに、結果を確認し、必要な指示を行うこと。

15. インシデント発生時の対応

本章に定める項目は、個人情報保護責任者が担うものとする。個人情報保護責任者は、情報漏えい等のセキュリティ事故、または事故の懸念がある事態が発生した場合に、必要な指示を行うこと。

15.1. 責任者、および管理者への報告

従業者は、情報漏えい等のセキュリティ事故、または事故の懸念がある事態が発生した場合に、速やかに、個人情報保護責任者、または個人情報保護管理者に報告を行うこと。

16. 管理方法の見直し、および当マニュアルの改編

本章に定める項目は、個人情報保護責任者が担うものとする。個人情報保護責任者は、当事務所の個人情報保護の取り組み、および当マニュアルの内容について、各安全管理措置責任者からの報告や提案、従業者からの意見等をふまえて見直しの判断を行うこと。

なお、当事務所の個人情報の管理方法、および本書の内容の改編については、当事務所のすべての従業者が提案することができるものとする。

改訂履歴

版数	変更点、変更箇所	承認者	改訂日
Ver1.0	新規作成		


NTT DATA