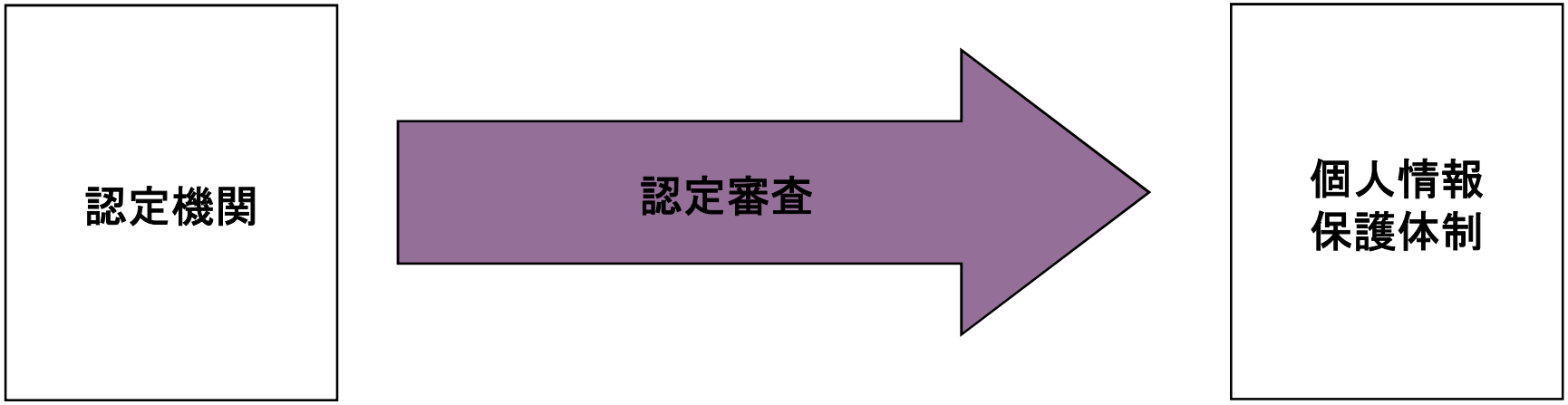
# プライバシーマークとは

# 合同会社Double Face

# Ｐマークとは

個人情報保護に対する国際標準JISQ15001に準拠し、個人情報の保護体制を構築した企業に対して、第三者認証を実施することにより、確実に遵守されていることを対外的に公表できるようにするための制度がPマークです。




現在１万社以上の企業が取得しています。

# Ｐマークを取るとどうなるか？

Pマークを取得すると、
- パンフレット
- HP
- 名刺

などの発行物にプライバシーマークを使用することが出来ます。

また、近年では
- 自治体や関連する組織団体の入札条件
- 大手企業の委託先選定条件（個人情報保護法対応のため）

などに用いられることが増えています。
特に、委託先選定の際には、適切な業者を選定して委託を行っていなかった場合には、委託元が個人情報に関する事故などの責任をすべて負わなければならなくなってしまったこともあり、かなり厳しい条件が求められることがあるようです。
そのときに、Pマークを取得していると、条件をクリアしやすくなることが良くあります。

# JISQ15001とは

JISQ15001とは、個人情報保護における基本的な事項と、組織の構築についての基準を定めたものです。
大きく、次のことを実施することを求めています。

- 個人情報を取り扱うためのマネジメントシステム構築
- 個人情報取得から利用、廃棄にいたるまでの手順策定
- 個人情報取扱におけるリスク管理の実施
- 委託先の選定、管理
- 社員の管理
- 個人情報保護に関連した定期教育
- 体制構築状況、運用状況の内部監査
- 定期的な見直し

# マネジメントシステムとは

マネジメントシステムとは、
Plan　（リスクの洗い出しおよび対応策の策定）
Do　（取扱手順の策定および実現）
Check（内部監査および定期チェック）
Act　（改善）

をひとつのサイクルとした社内の運用体制のことを言います。
基本的には、１年１サイクルで実現し、運用することにより、体制を維持向上することを求めています。

# 個人情報取扱体制とは

個人情報取扱においては、次の体制構築が求められます。

- 個人情報の洗い出し
- 個人情報の取扱ライフサイクル洗い出し
- 取得の際の本人に対する同意
- 個人情報に関連したお問い合わせ窓口の設置
- 外部委託先の評価、契約、管理
- 受託作業受付時の契約、社内対応

これらを構築するとともに、具体的な手順を作成することも求められます。
その際の手順作成の仕方で、Pマークの運用に関する負荷が大きく変わってくるため、後の対応を少しでも楽にするためには、これらの運用手順に工夫が必要になってきます。

# 個人情報保護体制の構築とは？

**プライバシーマークにおいて、個人情報保護体制が構築されている状態とは、次の状態が整っていることを指します。**

- 個人情報保護関連規定
- 問い合わせ窓口対応手順
- セキュリティ対策
- 委託業者契約
- 個人情報のリストアップ
- 教育・監査

これらの項目について、個人情報保護法などの基準に基づき必要な対策を導入することが個人情報保護体制の構築です。

ただし、重要なのはあくまでも

**業務を阻害しないような体制を構築すること**です。

# 個人情報保護体制の構築とは？

**ヒアリング**

- 業務の手順をヒアリングし、現状の業務の流れを確認します。
- 該当する個人情報をリストアップします。

**問題点の洗い出し**

- 問題点について、リストアップします。
- 問題点への具体的な対応案を検討します。

**必要書類の作成**

- 必要な規程類の修正、新規規程案を作成します。
- 規程の運用に必要な契約書などの書式について、案を作成します。

# 個人情報保護体制の構築のポイント

個人情報の保護体制については、次のポイントに特に注意しながら構築を行うことが重要です。

- 過剰な個人情報保護を行わないために、「守るべき重要個人情報」と「個人情報」を分け、必要な情報にのみ厳重な対策を行い、不要なコストをかけることを防ぎます。
- 規程を作るのみではなく、重要なのは守るべきルールを従業員が理解し、順守することです。そのためにも規程は、外部に公開するための文書と、社内に周知するための文書を切り分けると効果的です。
- 委託業務などを行う際には、都度契約内容の確認などが必要となりますが、個人情報に関する取り扱いの取り決めに関する文書は、標準的な覚書の書式を作成しておくと契約がスムーズに行いやすくなります。
- 規程を作る際には、表面的なルールだけを作成して、実運用に向かない規程を作成してしまいがちです。そのような状況を防ぐためにも、実際の業務をヒアリングして、業務の実態に合わせたルールを規定することが重要です。

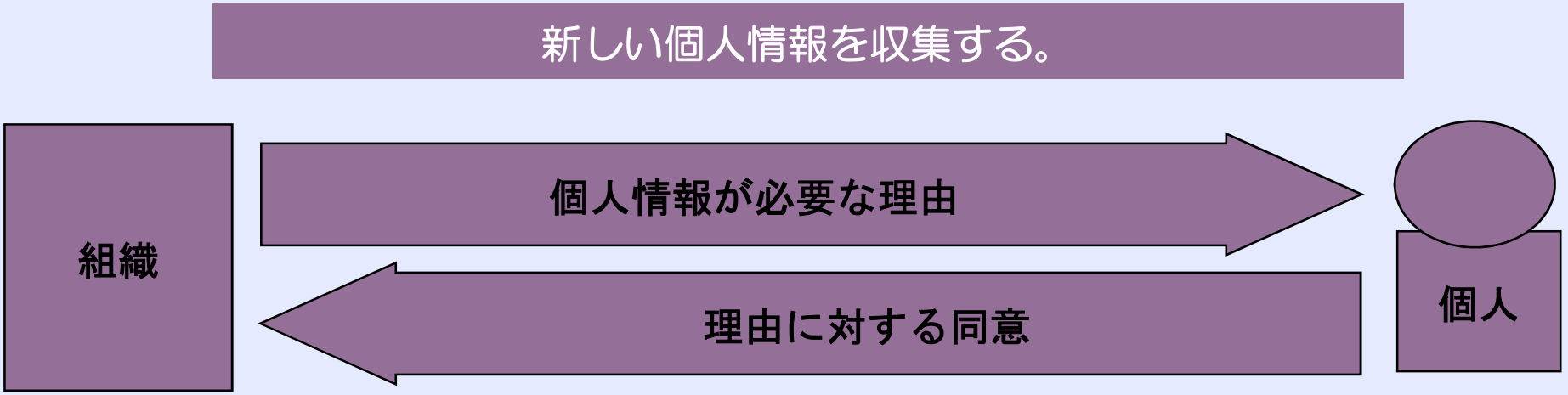
# 個人情報保護の原則

| | |
|---|---|
| 収集の原則 | ・個人情報は適正で適法な方法を用いて収集すること<br>・収集する際には同意を得ること |
| データ内容の原則 | ・利用目的以上の過度な内容の個人情報収集は行わないこと<br>・内容は正確さを保っておくこと |
| 目的の原則 | ・組織が個人情報を収集する目的は明確化し、通知すること |
| 利用制限の原則 | ・個人に通知している以外の目的で個人情報を利用しないこと |

# 個人情報保護の原則

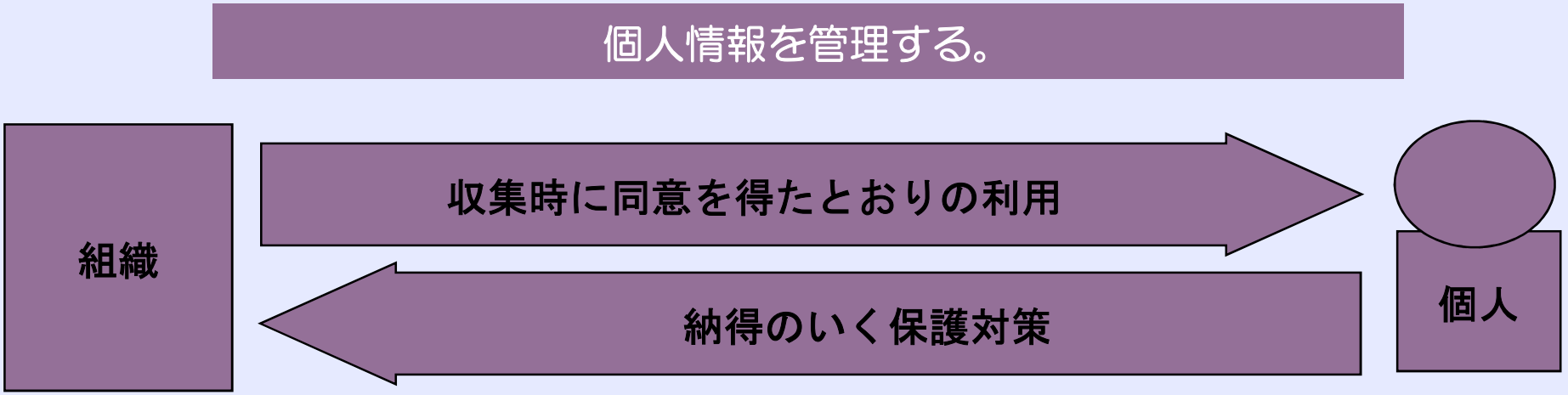
| | |
|---|---|
| 安全保護の原則 | ・個人情報に対して合理的な保護対策を講じること |
| 公開の原則 | ・個人情報の管理策を外部に公開できるようにしておくこと |
| 個人参加の原則 | ・組織が保有する個人の情報は、本人の要望により開示すること<br>・削除、変更などの依頼があった場合は対応すること |
| 責任の原則 | ・管理者は個人情報の取り扱いに関して責任を負うこと |

# 個人情報保護対策①




新たに個人情報を収集する際には、個人に対してなぜ収集する必要があるのかを通知する必要があります。その理由が妥当であることを同意した上で個人情報を個人が受け渡すようにすることが重要になります。
また、その同意は個人から明示的に得ることが必要になります。確実に同意を得た証拠を残しておけば、個人から万一個人情報の取り扱いにおいて追及されたとしても、問題ないことを証明できるようになります。

# 個人情報保護対策②

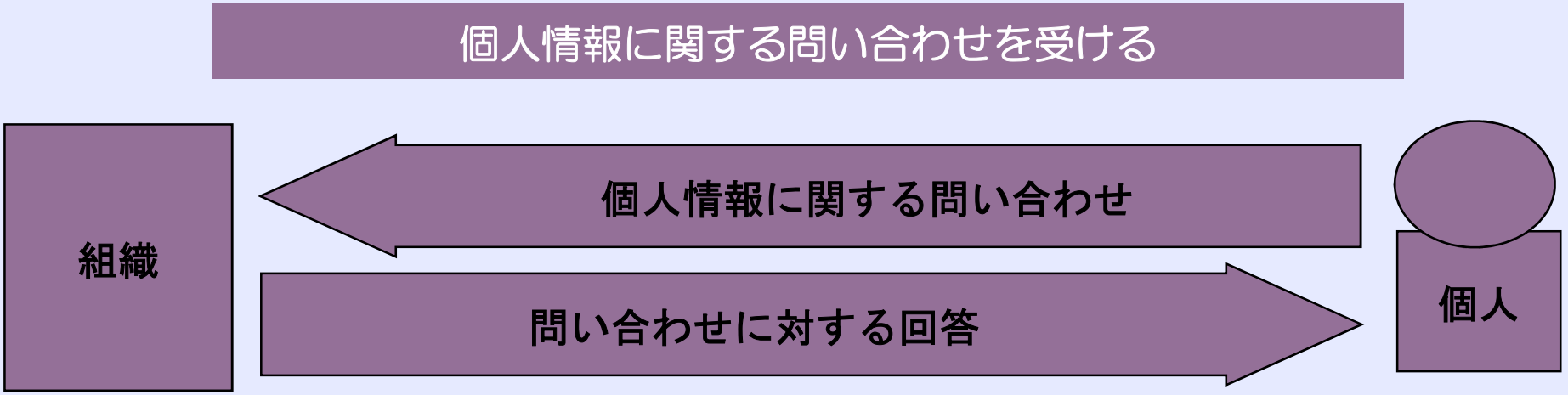



個人情報を管理する際には、当然のことながら同意を得たとおりの利用をしている必要があります。また、個人は個人情報の管理体制に関して知る権利がありますので、自社が行っている管理の体制がどのような状況であるかは理解している必要があります。
その際に必要な管理体制は、

- 必要な個人情報が確実に取り出せるようになっている
- どこに何の情報があるかがわかる
- 不正に持ち出しなどがされない状況になっている

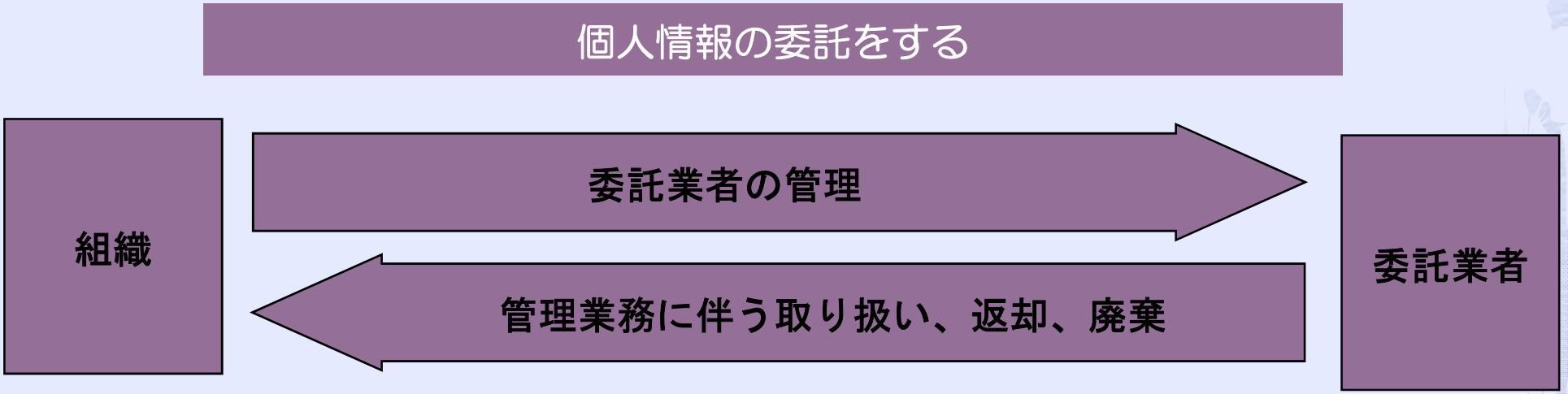
これらのことが重要になります。
特に、不正持ち出しなどに関してはよく追求されることですので、普段から注意が必要です。

# 個人情報保護対策③



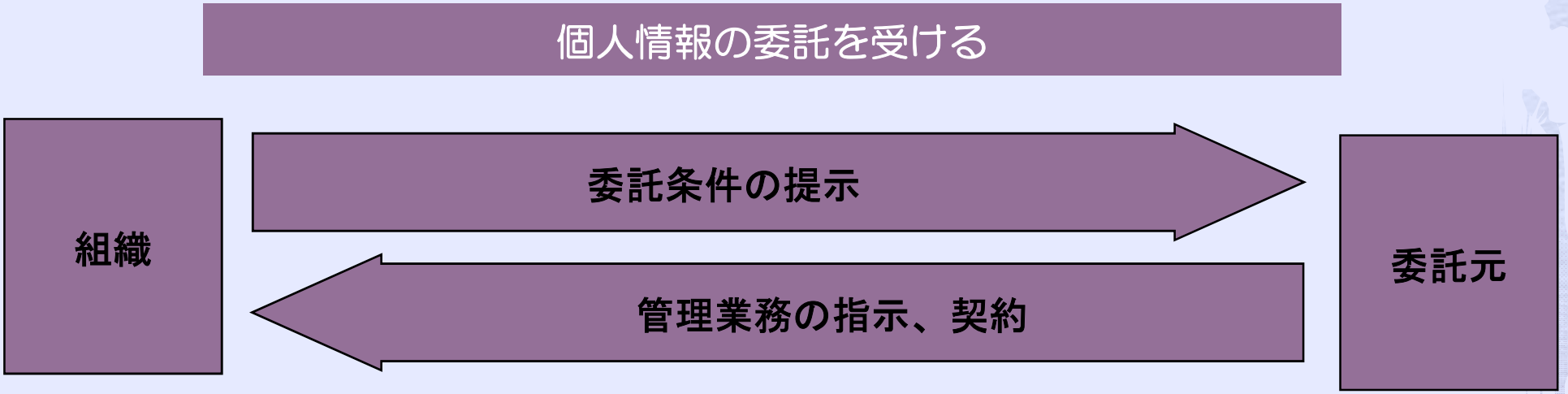

個人情報に関する問い合わせがあった場合、企業はその問い合わせに対して回答をしなければなりません。よく、個人情報に関する問い合わせに対して個人情報保護を理由に断る企業があると言う話しを聞きますが、実はこれは法律違反です。断ることが出来るのは、個人情報を元に自社が付加した情報（クレジットの与信額や、成績など）のみであり、自社が個人情報を保有していた場合にはその問い合わせに対して対応するのは法律上の義務です。

# 個人情報保護対策④




個人情報を外部に委託する際には、適切な管理として
評価、契約、確認を行わなければなりません。
また、委託業者に対しては、個人情報について返却、廃棄を求める必要があります。
特に廃棄を要求した場合には、廃棄証明を得る必要があります。

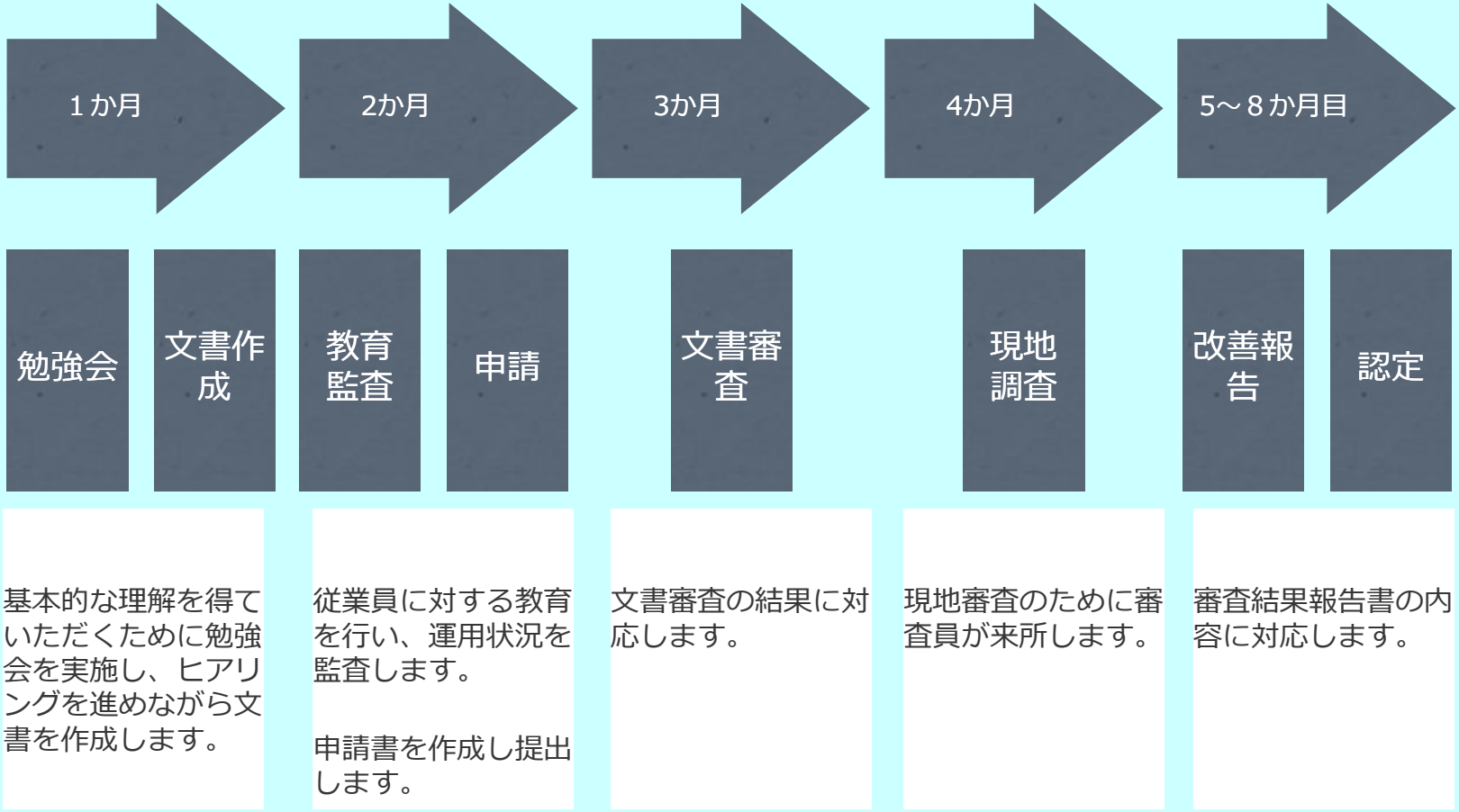
# 個人情報保護対策⑤




個人情報を取り扱う業務の委託を受ける場合は、顧客との間に委託情報を取り扱う上での条件を顧客と結ぶ必要があります。
この際に、顧客から条件が提示されなかった場合は当社から条件を明示する必要があります。
顧客との間に結んだ条件に従い業務を行うため、必要に応じて業務終了後には個人情報の返却、消去などを行う必要があります。

# Ｐマーク認定までの流れ

**Pマークの認定は、通常次のようなステップで構築を行います。**



# よく比較されるＩＳＭＳとの違い

| | ISMS | Pマーク |
|---|---|---|
| 認定機関 | UKAS<br>国際認定 | JIDPEC<br>日本国内のみの認定 |
| 審査機関 | 民間審査機関 | JIPDEC |
| 審査期間 | 毎年1回 | 2年に1回 |
| 審査方法の違い | ISO27001との対比により、認定基準に適合するかを評価する。<br>制度として不合格があるが、認定基準をクリアすればまず不合格が出ることはない。<br>審査指摘は通常0～5件ほど | 基本的にはJISQ15001に準拠していることを確認するが、厳密には審査員に認定の判断が任されており、指摘は規格への準拠とは関係なく出る。<br>ただし認定制度なので不合格という制度はない。<br>審査指摘は通常20～50件ほど |

# 双方の共通点

・マネジメントシステムであるため、次の作業が毎年必要となる。
　　リスクアセスメント
　　教育
　　内部監査
　　年間活動結果まとめ

・名刺やカタログ、ＨＰなどにマークを載せることができる。

・社内の規定が必要

・ともに個人情報保護法への準拠は必須であるため、個人情報保護対策は最低限どちらにも含められている。

# 規格としての違い

| | ISMS | Pマーク |
|---|---|---|
| 規格項目 | 45項目＋133項目<br>ただし、133項目は選択制であり、すべてを実施するわけではない。 | 38項目<br>ただし、ガイドラインが追加されるため、実質は140ほど。 |
| 申請文書 | 文書の形式、文書量などに決まりはなく、自社にとって必要な文書のみを作成していればよい。 | 文書の形式、作成物に決まりがあり、自社にとっては必要なくても作成しなければならない文書もある。<br>そのため、申請文書以外に自社内で読みやすいルールを作成しておくことが必要。 |
| 内容 | セキュリティ全般であり、基本的にはどんな業種でも適用できるように規格が作られている。 | あくまで個人情報保護のための規格であり、規格の中にセキュリティに関連した項目は漠然としかない。 |
| 特徴 | 基本的には決まった形が出来上がるわけではなく、それぞれ会社によって仕組みが変わるのが一般的。<br>そのため、構築段階で時間がかかる。 | 審査に合格するためにはある程度決まった形の仕組みを構築しなければならない。<br>そのため、構築には時間がさほどかからないが、運用が少々難しくなりがち。 |

# 比較総評

| ＩＳＭＳ | Ｐマーク |
| --- | --- |
| 国際認定であることと、審査そのものが難しいという評価をされていることから、取得した際の評価は比較的高い。<br>また、業界によっても取得している企業は少ないため、差別化に大きくつながることもある。<br>特に、システム系や金融系、クレジット系などの業界ではＩＳＭＳを取引条件にしているところもある。<br><br>しかし、審査が毎年１回ある上、認定の継続費用がＰマークと比べると高くなることがある。<br>さらに規格自体が難解であるため、規格を深く理解している人間が構築しないとかなり難しい。<br>ただ、規格の内容さえ分かっていれば、実際には自社に都合のいい仕組みを作りやすいという側面も持っている。 | 申請費用、審査費用がＩＳＭＳと比べると安めで、審査も２年に１回。<br>ただし、審査の周期が長いため、年間作業を継続できず、初回に認定されて以降、更新審査時に認定を継続できない企業も多い。<br>また、個人情報を取り扱う業界においては取得を必須としているところが多い。<br>認定数は現在１００００社を越えているが、裏を返せば差別化にはつなげづらい。<br><br>審査において、ある程度決まったものを策定しなければならないため、かなり無理のあるルールを導入しなければならないことがあり、導入するものの運用できなくなる企業が多いのが難点。<br>ただ、作成物さえそろえば合格できるので、初回の合格は非常にしやすい。 |