社会保険労務士のための

「個人情報保護法」対策

平成17年3月
株式会社　名南経営
ISO事業部　古崎敏郎

セミナーの概要

1. **個人情報保護法の概要と、業界に与える影響**
2. **具体的な保護法対策**
3. **プライバシーマークとは**

法制定の背景(漏洩事件の例)

2004年4月	市内のゴミ収集所で、患者の名前や病歴が記載されたレセプトの下書き約150人分が見つかった。自宅に持ち帰った職員が家庭ごみと一緒に廃棄した。
2004年3月	大手通販会社の顧客情報最大６６万人分流出
2004年2月	大手ADSL会社の内部者のより451万件の個人データ流出
2003年7月	都市銀行の行員が顧客情報データを消費者金融業者に売却
2003年6月	コンビニエンスストアの顧客データ56万件が社外に流出
2003年2月	大手予備校で模擬試験の成績などが別の予備校に流出した。
2002年5月	エステティックサロンのホームページから顧客情報が流出した。
1999年5月	京都の自治体で22万人分の住民基本台帳のデータが漏洩し、インターネット上で販売される。

情報が売れる限り、漏洩事件は後を絶たない。
→情報を持ち出す人を無くすことは困難。

インターネットで流通する名簿情報

データベース名	地域	件数	データベース名	地域	件数
高額納税者H15年	全国	73，366	大学在校生・卒業生データ他	一都三県	6，481
モデルルーム来場者	全国	45，491	競馬会員データ	全国	108，967
看護師・薬剤師	首都圏中心	14，258	健康食品購入者	全国	138，923
エステ利用者1	一都三県	9，165	パソコン雑誌購読者	全国	9，761
エステ利用者2	全国	13，575	呉服顧客	全国	228，127
エステカタログ希望者	全国	87，099	ビデオ購入者	全国	4，455，566
エステ商品通販購入者	全国	278，764	ベビー用品購入者	全国	557，004
結婚希望者	首都圏中心	6，872	携帯キャンペーン申込者	全国	669，290
結婚紹介所登録者	関東	4，914	携帯電話所有者	全国	227，391
恋人紹介センター登録者	全国	5，874	アパートオーナー	東京	11，109
P通販顧客	全国	130，455	パソコンユーザー2002	全国	183，829
通販利用者	一都三県	27，837	在宅ビジネス希望者	全国	9，528
通販利用者2	全国	125，094	高齢者ﾃﾞｰﾀ	全国	72，786
Lサイズ顧客	全国	42，121	有料放送契約者	全国	208，925
サイドビジネス希望者	全国	20，434	新ペット愛好家	首都圏中心	14，025

＊価格は、一件につき￥15～￥50です。リスト、ラベル、フロッピーディスク等、
お客様の御用途にあわせて出力できます。
地域、性別などの検索に関しては、検索料を頂く場合がありますので

漏洩事件の原因

(1) 従業員による不正行為での漏洩

－雇用形態･就業意識の変化
－個人情報の価値増大 (マーケティング戦略の発達)

(2) 外注先による漏洩

－システムの開発･運用のアウトソーシング化
－委託管理の未徹底 (再委託、Dataの受渡し、廃棄等の管理)

(3) HPの設定ミスによる漏洩

－HP　運用管理の不徹底

(4) スタッフの無意識による漏洩

－ユーザー教育の不足、意識の欠如

内部者による原因が８０%→教育などの人的管理が重要

漏洩事件・事故を起こせば

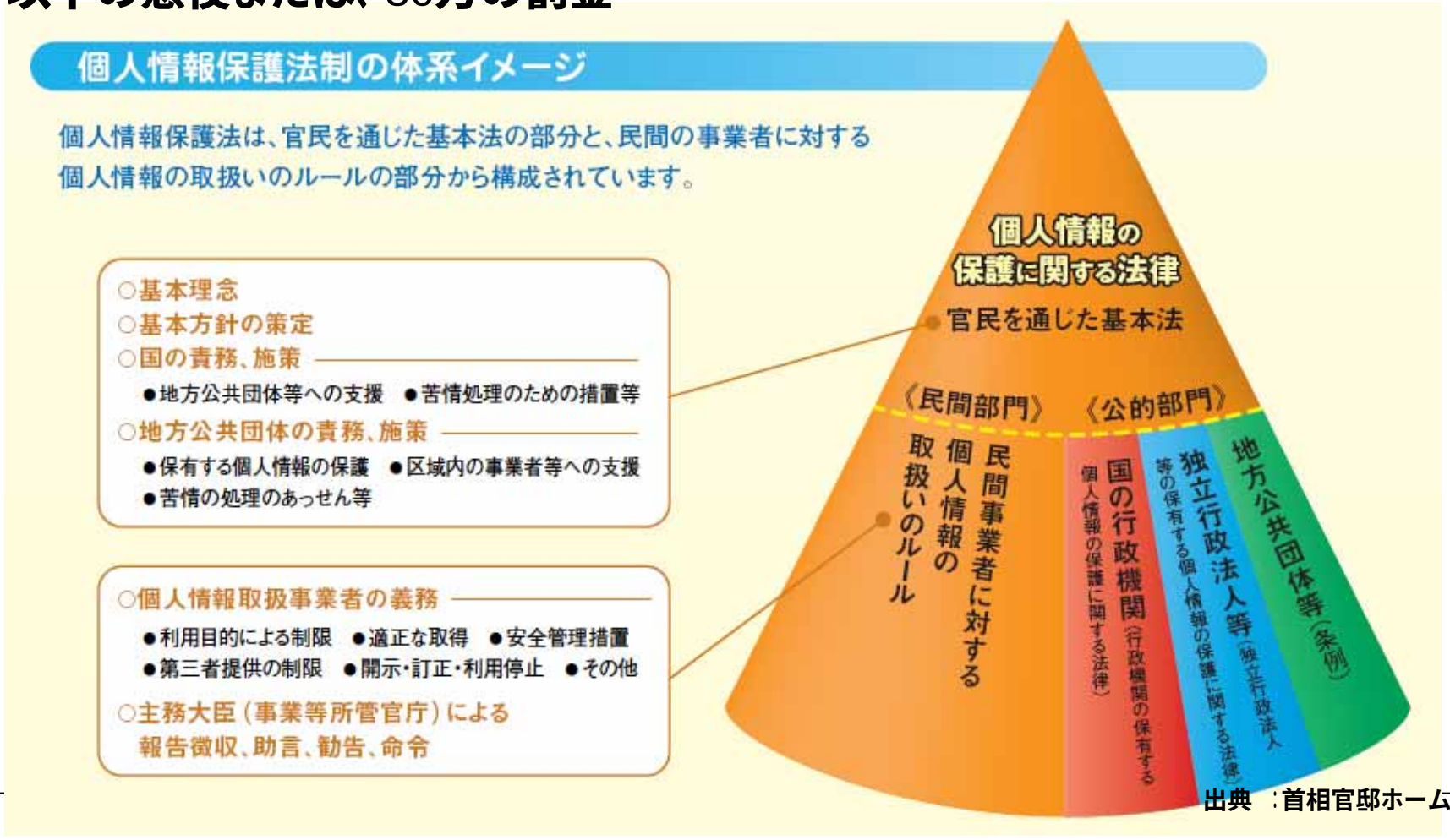
漏洩事件･事故の発生（一瞬にして重要なデータが流出）
↓
情報漏洩に気づかない（顧客などからの指摘によりはじめて気づく）
↓
流出した情報の回収は不可能
↓
企業の指揮･監督責任が問われる

顧客からの信頼の失墜

- 既存顧客の減少
- 新規顧客の減少
- 漏洩の原因を究明し、再発防止策に時間と資金が必要
- 損害賠償請求

個人情報保護法とは

- 「個人情報の保護に関する法律」
- 平成15年5月30日公布→本年4月1日より完全施行
- 事後規制ではなく、事前規制（予防規制）
- 5000件を超える個人情報を取扱う事業者が、義務事項が課せられる。
- 6ヶ月以下の懲役または、30万の罰金



出典　：首相官邸ホームページ

個人情報とは

法律上の定義：「個人情報」とは、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。

★他の人と区別してAさんと認識可能な情報

・氏名、住所、電話番号、メールアドレス、年齢、性別、年収、趣味、嗜好、家族構成、身長、体重、血圧など

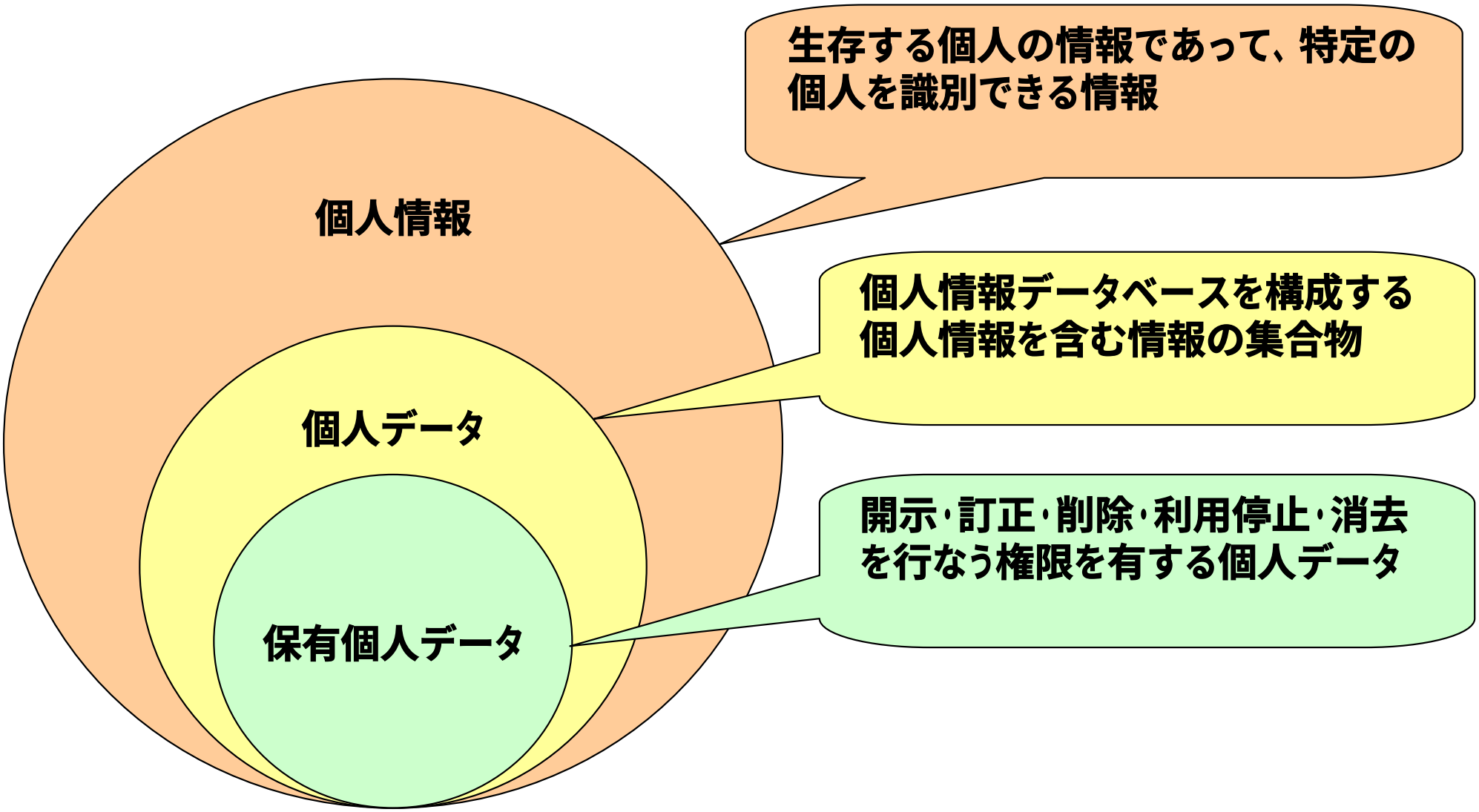
★氏名と結びつく限りは、「個人情報」に該当する場合がほとんどである。

・株式会社などの法人は「個人情報」ではない。

社労士業務に関わる主な個人情報

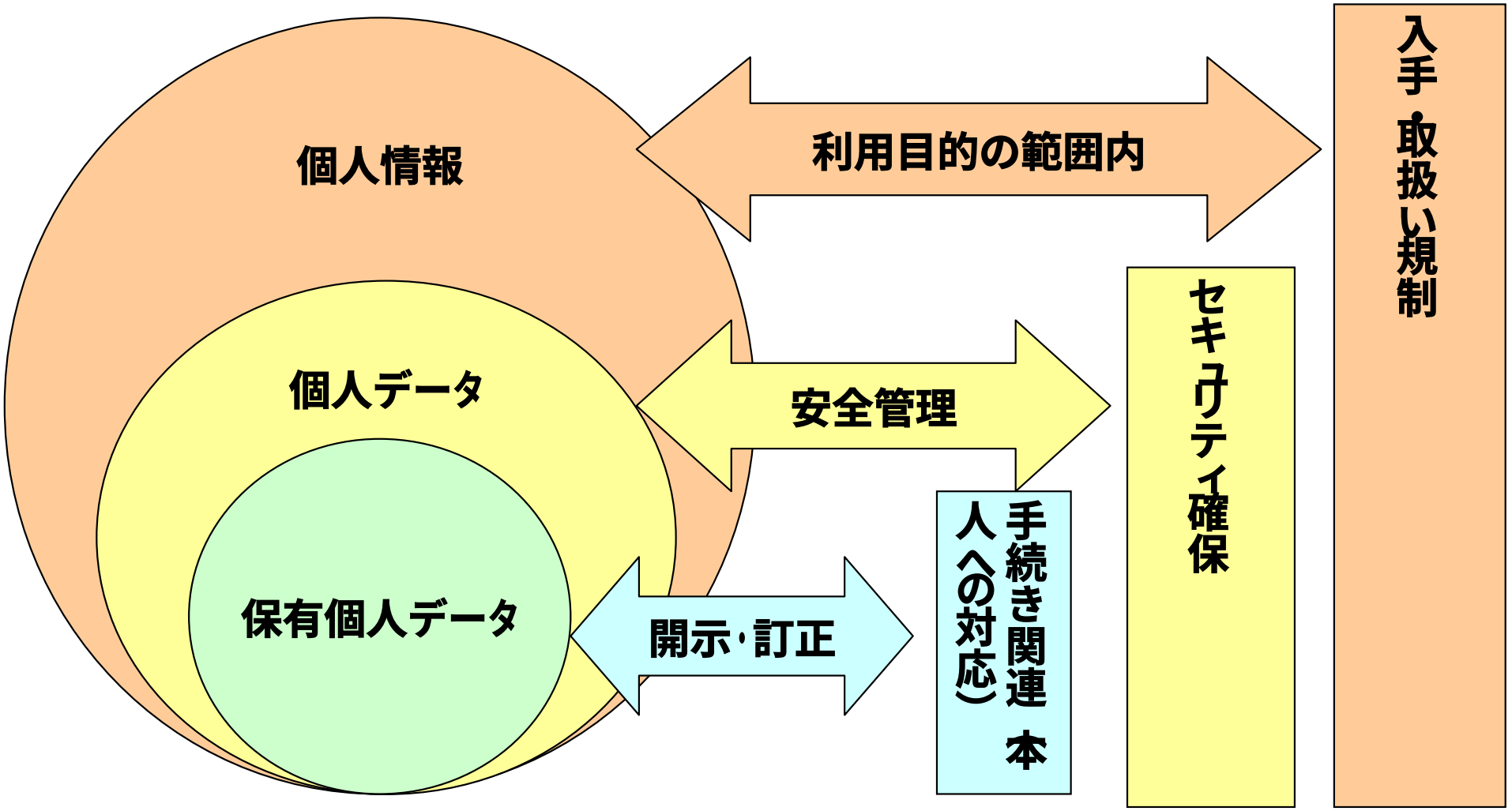
賃金台帳、住所届、給与振込み依頼書、健康診断結果表、
社員名簿、健康保険各種届出書類、厚生年金保険各種届出書類
雇用保険各種届出書類

個人情報の区分



法律上では、“個人情報”、“個人データ”、“保有個人データ”の使い分けがされている。例えば、開示対応などに関しては、“保有する個人データ”が対象となっている。

個人情報保護法で課せられる義務①



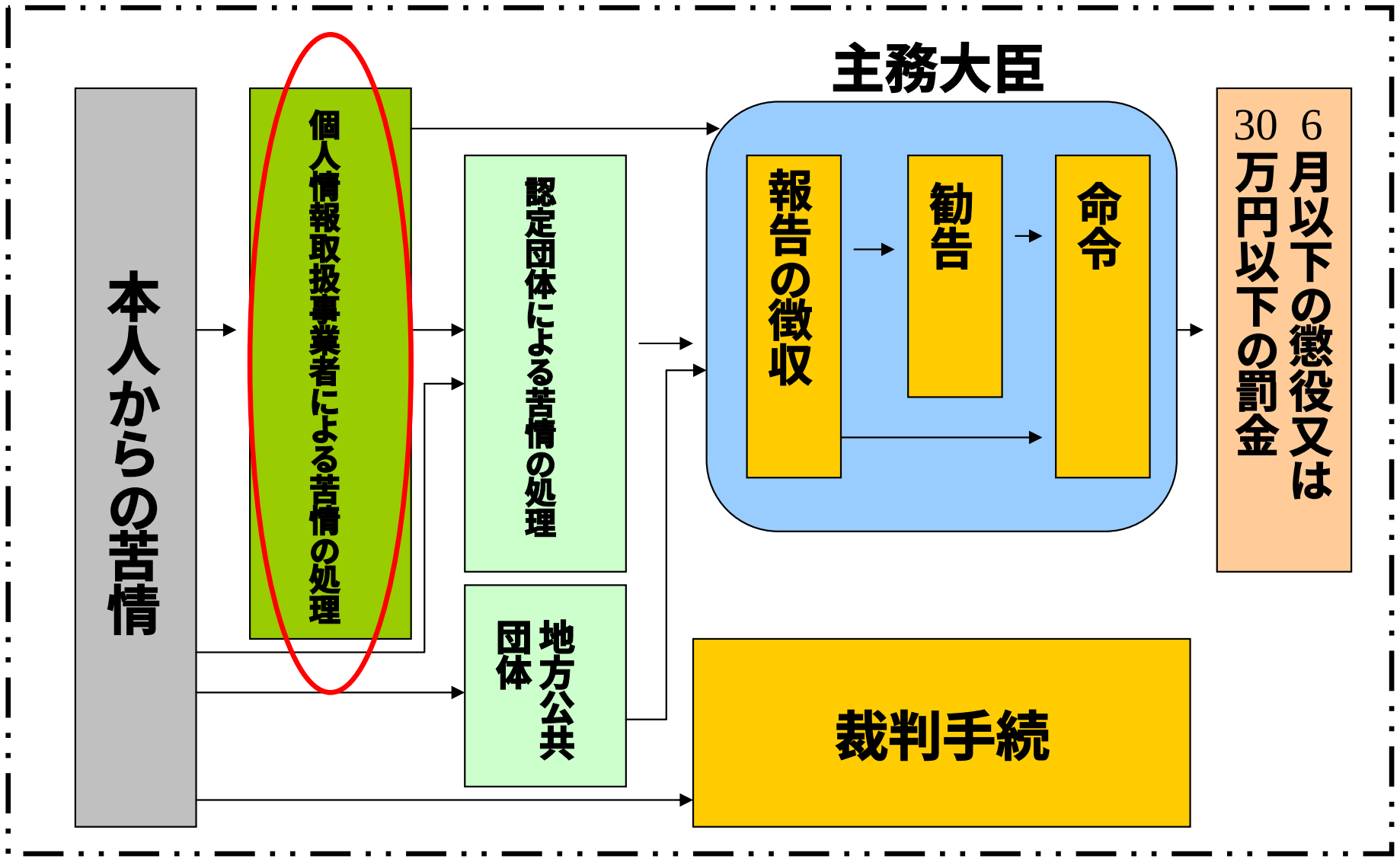
個人情報保護法で課せられる義務②

個人情報
- 利用目的の特定、目的外利用の禁止（法第１５条、第１６条）
- 利用目的の通知等（法第１８条）
- 適正な手段による取得（法第１７条）
- 苦情の処理（第３１条）

個人データ
- 正確性の確保（法第１９条）
- 安全管理（法第２０条）
- 従業者の監督（法第２１条）
- 委託先の監督（法第２２条）
- 第三者への提供（法第２３条）

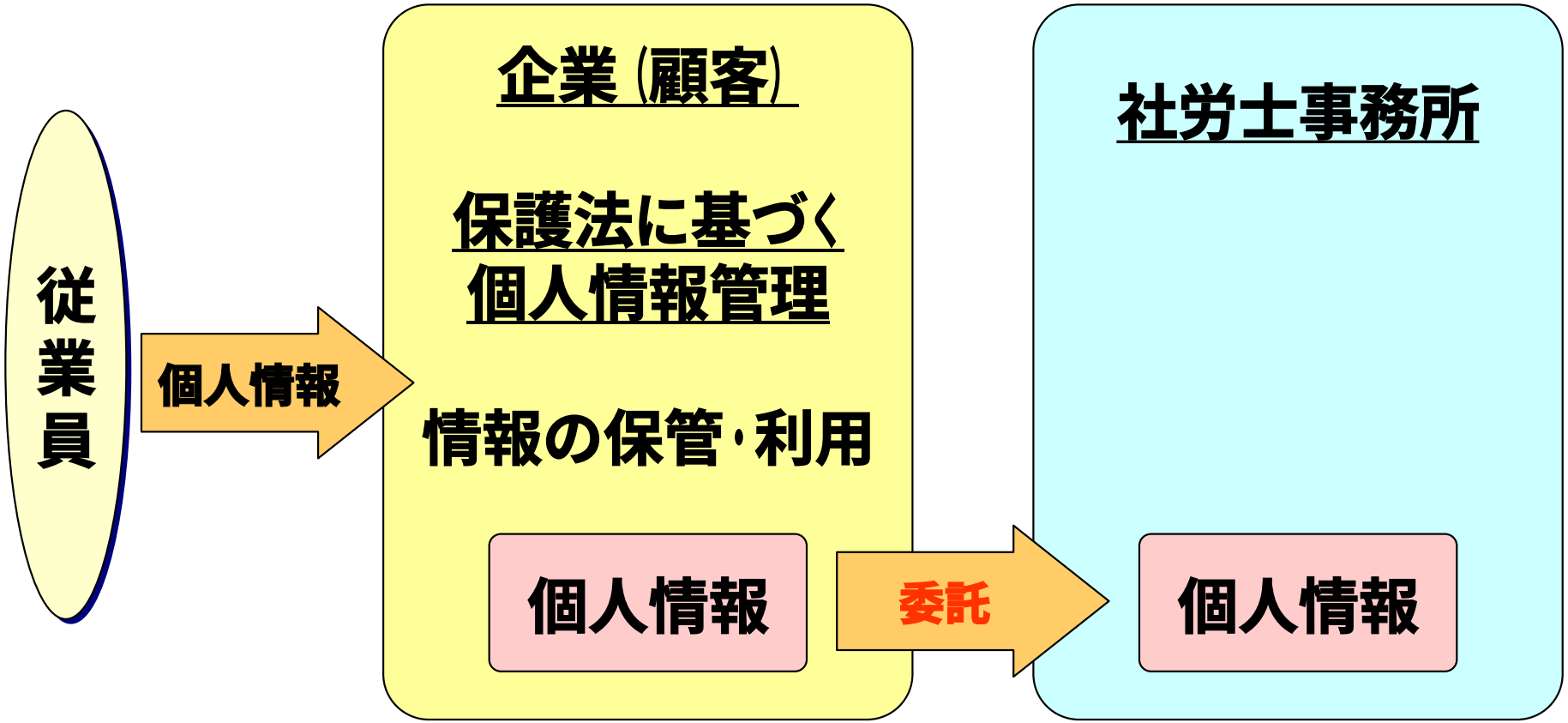
保有個人データ
- 保有個人データに関する事項の公表（法第２４条）
- 保有個人データの開示（法第２５条）
- 保有個人データの訂正等（法第２６条）
- 保有個人データの利用停止等（法第２７条）
- 理由の説明（法第２８条）
- 開示等の求めに応じる手続き（法第２９条）
- 手数料（法第３０条）

個人情報保護実効性担保の仕組み



出典　:首相官邸ホームページ

社労士業界に与える影響①



受託企業が委託先を管理しなければならない。万が一、漏洩事故が発生したら、委託元企業に責任が生じる。

顧客からの個人情報保護体制への要請

社労士業界に与える影響②

顧客からの個人情報保護に関する内部規程の作成依頼の増加

中小企業では何をどうしていけばよいのか、情報収集の段階

↓

4／1の完全施行に伴い、関心はピークに達する

↓

問合せも予想される。対応できるかどうかで顧客からの信頼アップ！

個人情報保護への具体的対応策

具体的義務の内容①

1．利用目的の特定等（15条、16条）

2．利用目的の通知等（18条）

<法律またはガイドラインで求められていること>

・個人情報を取り扱うに当たり、その利用目的をできる限り特定し、取り扱うこと。

・個人情報を取得するに当たって、あらかじめその利用目的を公表しておくか、個人情報を取得した場合、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

・利用目的を変更した場合は、あらかじめ本人の同意を得る。

<対応策>

自社での利用目的をまずは整理する。→それを店内掲示などで公表する。
できる限り広く公表するためにホームページなどにも掲載する。

・ご購入商品の発送、関連するアフターサービス、新商品・サービスに関する情報のお知らせのために利用いたします。
・ご記入いただいた氏名、住所、電話番号は、名簿として販売することがあります。
・給与計算処理サービス、あて名印刷サービス、伝票の印刷・発送サービス等の情報処理サービスを業として行うために、委託された個人情報を取り扱います。
・新聞配達・集金業務の遂行、各種サービス・イベントのお知らせ、ミニコミ誌や特典等の配布・郵送、ご購読の延長や再開のお勧めに使用します。

具体的義務の内容②

3．個人情報の適正な取得、個人データ内容の正確性の確保（法第１７条、第１９条）

<法律またはガイドラインで求められていること>

・偽りその他の不正の手段により個人情報を取得してはならない。

・親の同意なく、十分な判断能力を有していない子どもから家族の個人情報を取得してはならない。

・利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

<対応策>

・不正アクセスをしての収集、虚偽の目的通知での収集、脅迫による収集などを行なわないための社員教育

・確実（正確）なデータ登録作業を行なう手順・対策を講じます。

ex)入力マニュアルの整備

入力手順のルール化（だれが、いつ、データベースに、どういった方法で）

教育

入力エラーが発生にくいシステムの採用

・データの検査・監視体制の確立

ex)管理者による定期的なチェック

具体的義務の内容③

4．安全管理措置、従業者・委託先の監督（20条～22条）

<法律またはガイドラインで求められていること>

・個人データの安全管理のために必要かつ適切な措置、従業者・委託先に対する必要かつ適切な監督

①安全管理措置

取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的、技術的な安全管理措置を講じなければならない。

②従業者の監督

①の安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない

③委託先の監督

個人情報の全部又は一部を委託する場合、①に基づく安全管理措置を遵守させるよう受託者に対し、必要かつ適切な監督をしなければならない。

具体的義務の内容④

4．安全管理措置、従業者・委託先の監督（20条～22条）

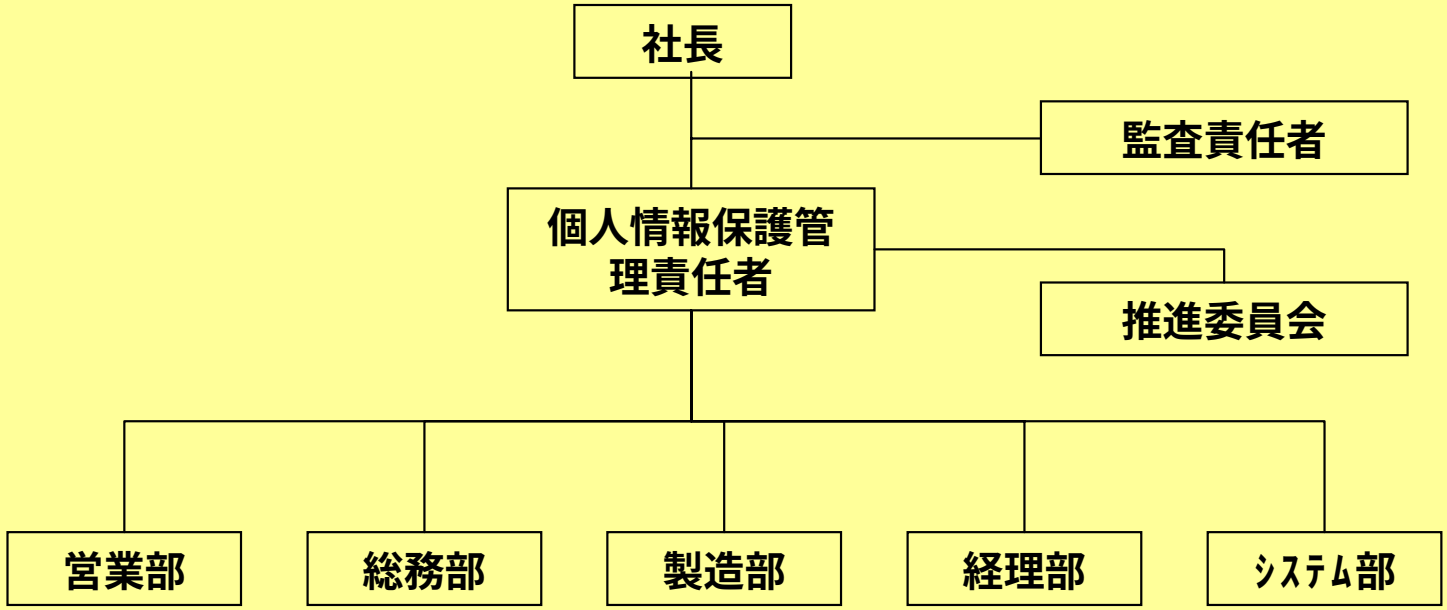
<対応策>

①安全管理措置

・組織的安全管理措置

→従業者の責任体制の明確化を図り、具体的な取組を進めるため、個人情報保護に関して十分な知識を有する管理者、監督者等を定めたり、個人情報保護の推進を図るための委員会等を設置する。

ex)保護体制の例：



具体的義務の内容⑤

4．安全管理措置、従業者･委託先の監督 (20条～22条)

<対応策>

①安全管理措置、②従業員の監督

･人的安全管理措置

雇用･退職時の個人情報保護に関する規程の整備

→雇用契約や就業規則において、就業期間中はもとより離職後も含めた守秘義務を課す

社員に対する教育研修の実施

→取り扱う個人データの適切な保護が確保されるよう、社員に対する教育研修の実施等により、個人データを実際の業務で取り扱うこととなる従業者の啓発を図り、社員の個人情報保護意識を徹底する。

個人情報に関する教育に関して、定期的に実施するよう、計画し、実施し、教育が有効だったかどうかを評価するような仕組みが望ましい。

２００４年度　教　育　実　施　記　録

開催日時：１２月２２日

研修の名称	個人情報保護に関する研修
使用テキスト	研修用ﾃｷｽﾄ
講師又は 教育担当部門	個人情報保護管理責任者
＜研修の概要＞ ・なぜ個人情報を保護するのか ・コンプライアンス・プログラムの目的とねらい ・今後の方針について ・日常業務における院内諸注意 ・各部署ごとのルールについて	
受講対象者名	山田花子
有効性評価	理解度テスト９３点 有効性　■有　　□なし

具体的義務の内容⑥

4．安全管理措置、従業者・委託先の監督（20条～22条）

<対応策>

①安全管理措置

・物理的安全管理措置

・入退館（室）管理の実施

入館記録の義務付け

特別室（重要なデータの保管庫やサーバールーム）への入出ルール

・盗難等に対する予防対策の実施

ノートパソコンは帰社時に鍵付ロッカーへ保管

車で移動する際の重要書類の保管ルール（車から離れる場合は、書類も持ち出す）

・機器、装置等の固定など物理的な保護

・データの破棄

個人情報が記載された紙媒体は、シュレッダーや溶解など、復元不可能な形にして廃棄する。

個人データを取り扱った情報機器を廃棄する場合は、記憶装置内の個人データを復元不可能な形に消去して廃棄する。

→物理的に破壊するか、データ抹消ソフトを利用する。

具体的義務の内容⑦

4．安全管理措置、従業者・委託先の監督（20条～22条）

<対応策>

①安全管理措置

・技術的安全管理措置

（個人データの盗難・紛失等を防止するため、個人データを取り扱う情報システムについての措置）

・個人データに対するアクセス管理

社員毎にIDを設定し、アクセスできる情報を選別する。

→役員のみがアクセスできる情報、総務部のみがアクセスできる情報などと選別をする。

パスワードは定期的に変更する。

退職者が出た場合は忘れずにIDを削除する。

・個人データに対するアクセス記録の保存

だれが、いつ、どの情報にアクセスしたかの記録を保管する仕組みを導入する。

（実施していることを公表することで抑止力にも繋がる。）

・個人データに対する保護の仕組み

ファイアーウォールの設置

ウィルス対策ソフトのインストール

不正コピー防止機能コピー機の設置

具体的義務の内容⑧

4．安全管理措置、従業者・委託先の監督（20条～22条）

<対応策>

③委託先の監督

- **個人情報を適切に取り扱っている事業者を委託先（受託者）として選定する**

- **個人情報にかかわる委託業務のピックアップ**
  サーバーなどのメンテナンスを外部に委託
  給与計算を社労士に委託

  ※清掃会社→顧客データを見ることが可能？

- **契約内容の確認**
  個人情報に関する秘密保持の内容が含まれているか
  委託終了後の個人データの取扱い
  再委託に関する取り決め

- **委託先が個人情報を適切に取り扱っていることを定期的に確認する**

委託先評価表

社名：＿＿＿＿＿＿＿＿＿＿＿＿

1．評価内容
以下の項目を評価する。

（1）契約項目

	評価項目	可	不可	再評価（ / ）
保護水準	委託契約書にて、機密保持に関する事項が定められているか（個人情報に関する秘密保持は適切か）			
	委託契約書にて、再委託に関する事項が定められているか			
	委託契約書にて、事故時の責任分担、又は損害賠償・免責に関する事項が定められているか			
	委託契約書にて、契約終了時の個人情報の返却及び消去に関する事項が定められているか			

（2）管理状況

	評価項目	可	不可	再評価（ / ）
管理項目	委託業務に従事する者が個人情報に関する教育を受けているか			
	預託した個人情報に対する安全管理に問題が無いか			
	委託業務において、個人情報に関する事故は発生していないか			
	個人情報の返却又は消去が、適切に対応されているか			
契約	委託契約書の期限は切れていないか			

具体的義務の内容⑨

5．第三者提供の制限（23条）

<法律またはガイドラインで求められていること>

・あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。（例外事項有）

・個人データの第三者提供について本人の同意があった場合で、その後、本人から第三者提供の範囲の一部についての同意を取り消す旨の申出があった場合は、その後の個人データの取扱いについては、本人の同意のあった範囲に限定して取り扱うものとする。

<第三者提供の例外>

(1)法令に基づく場合

(2)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であるとき

(3)公衆衛生の向上又は児童の健全な育成の推進のために特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であるとき

(4)国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき

<本人の同意が得られていると考えられる場合>

(1)患者への医療の提供のために通常必要な範囲の利用目的について、院内掲示等で公表しておくことによりあらかじめ包括的な同意を得る場合

<「第三者」に該当しない場合>

(1)他の事業者等への情報提供であるが、「第三者」に該当しない場合

(2)同一事業者内における情報提供であり、「第三者」に該当しない場合

具体的義務の内容⑩

5．第三者提供の制限（23条）

<対応策>

・情報提供を第三者に行なう場合のルールを作成し、あらためて本人に同意が必要かどうかを判断してから情報提供を行なう。

・本来必要とされる情報の範囲に限って提供すべきであり、匿名化などの処置をしてから対応する。

・第三者提供に該当しない情報提供が行われる場合であっても、事業所内等への掲示、ホームページ等により情報提供先をできるだけ明らかにするとともに、利用者等からの問い合わせがあった場合に回答できる体制を確保する。

ex)業務委託の場合、委託している業務の内容、委託先事業者、委託先事業者との間での個人情報の取扱いに関する取り決めの内容等について公開する。

具体的義務の内容⑪

6～10．公表等、開示、訂正等、利用停止等（24条～27条）、苦情の処理（31条）

<法律またはガイドラインで求められていること>

・保有個人データに関し、当該個人情報取扱事業者の氏名又は名称などを本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む）に置かなければならない。

・本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、遅滞無く通知する

・本人から、当該本人が識別される保有個人データの開示を求められたときは、本人に対し、遅滞なく、当該保有個人データを開示しなければならない。（例外有）

・求められた保有個人データを開示しない旨を決定したときは、本人に対し、遅滞なく、その旨を通知。

・本人から、保有個人データの訂正等、利用停止等、第三者への提供の停止を求められた場合で、それらの求めが適正であると認められるときは、これらの措置を行わなければならない。

・個人情報の取扱いに関する苦情の適切かつ迅速な対応に努めなければならない。また、苦情の適切かつ迅速な対応を行うにあたり、苦情への対応を行う窓口機能等の整備や苦情への対応の手順を定めるなど必要な体制の整備に努めなければならない。

<対応策>

・苦情への対応を行う窓口機能等の整備や苦情への対応の手順の作成する。
以下のような流れを作成することが望ましい。

受付→本人確認→意思決定（開示・訂正・利用停止の措置を行なうか否かの決定）→本人に結果を通知
→必要に応じて再発防止策の実施

具体的実施項目

1．個人情報の管理者を決めること。

個人情報の管理者を決めて、社員の教育や、外部委託先の監督を実施しなければならない。

2．現状把握

現在、保有している個人情報のピックアップし、リスク（不正アクセス、破壊、漏洩など）を把握する。
リスクが高い内容に関して、優先的に対策案を検討し、実施していく。

3．個人情報の記載された書類の管理を徹底すること

関係者以外が、個人情報を見ることができないように、鍵付きキャビネットへの保管や、施錠管理を徹底すること。

4．規程の策定及び教育の実施

保護法で課せられている義務事項の仕組みづくりの実施し、従業員への教育を実施する。

個人情報保護を制度的に担保する仕組み
プライバシーマークの認証制度の活用

プライバシーマークとは

- **個人情報保護に関するJIS Q15001規格を用いて第三者からの評価を得る仕組み（個人情報分野における病院機能評価制度的存在）**
  - **個人情報保護法だけでは法律を日常的に守る仕組みとして維持しずらい**
  - **法的要求事項とマネジメントシステムとして維持していく仕組みがうまく構成されている（ISOマネジメントシステムを組み合わせている）**

- **JIS Q15001に準拠したシステムを構築運用することで、財)日本情報処理開発協会（JIPDEC)よりプライバシー保護認定審査を受けることが出来る。医療機関はMidis-DCによる付与審査を受ける。**

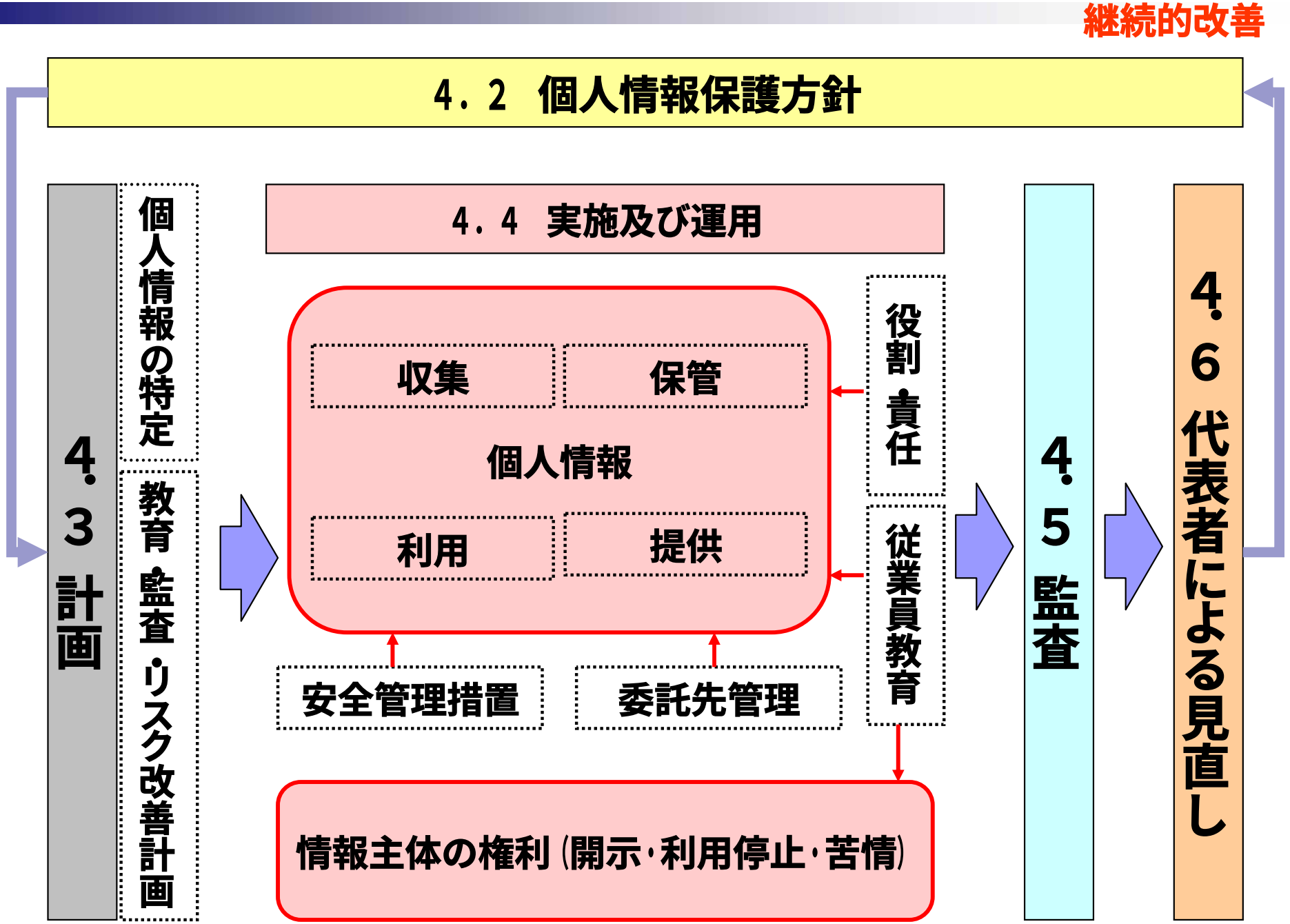
- **JIPDECの認定審査を受け認定されると2年間プライバシーマークの使用を認められる**

プライバシーマークの認証企業数

Pマークの現在の取得状況一覧
1021社　(平成17年1月現在)

印刷･出版業 (104社)	情報サービス･調査業 (641社)	その他の事業サービス業(54社)
各種製造業 (18社)	労働者派遣業 (51社)	生活関連サービス業 (9社)
運輸･通信 (32社)	広告業 (14社)	医療業･社会福祉･介護事業(9社)
卸売業･小売業 (20社)	専門サービス業 (25社)	教育 (4社)
金融･保険･不動産業(14社)	学習塾 (21社)	その他 (5社)

Ｐマークの体系


継続的改善
4．2　個人情報保護方針
4．3 計画
個人情報の特定
教育・監査・リスク改善計画
4．4　実施及び運用
収集
保管
個人情報
利用
提供
役割・責任
従業員教育
安全管理措置
委託先管理
情報主体の権利（開示・利用停止・苦情）
4．5 監査
4．6 代表者による見直し

ＩＳＯマネジメントシステムとの共通点

ISO9001（品質）、ISO14001（環境）、ISMS（情報セキュリティ）など同じくPDCAサイクルで継続的な改善を行なう仕組み

共通項目

・PDCAサイクル

P（Plan）　　方針や目的・計画の策定

D（Do）　実施のための体制や訓練、管理・運用

C（Check）　　監視、点検及び監査

A（Action）　　見直し

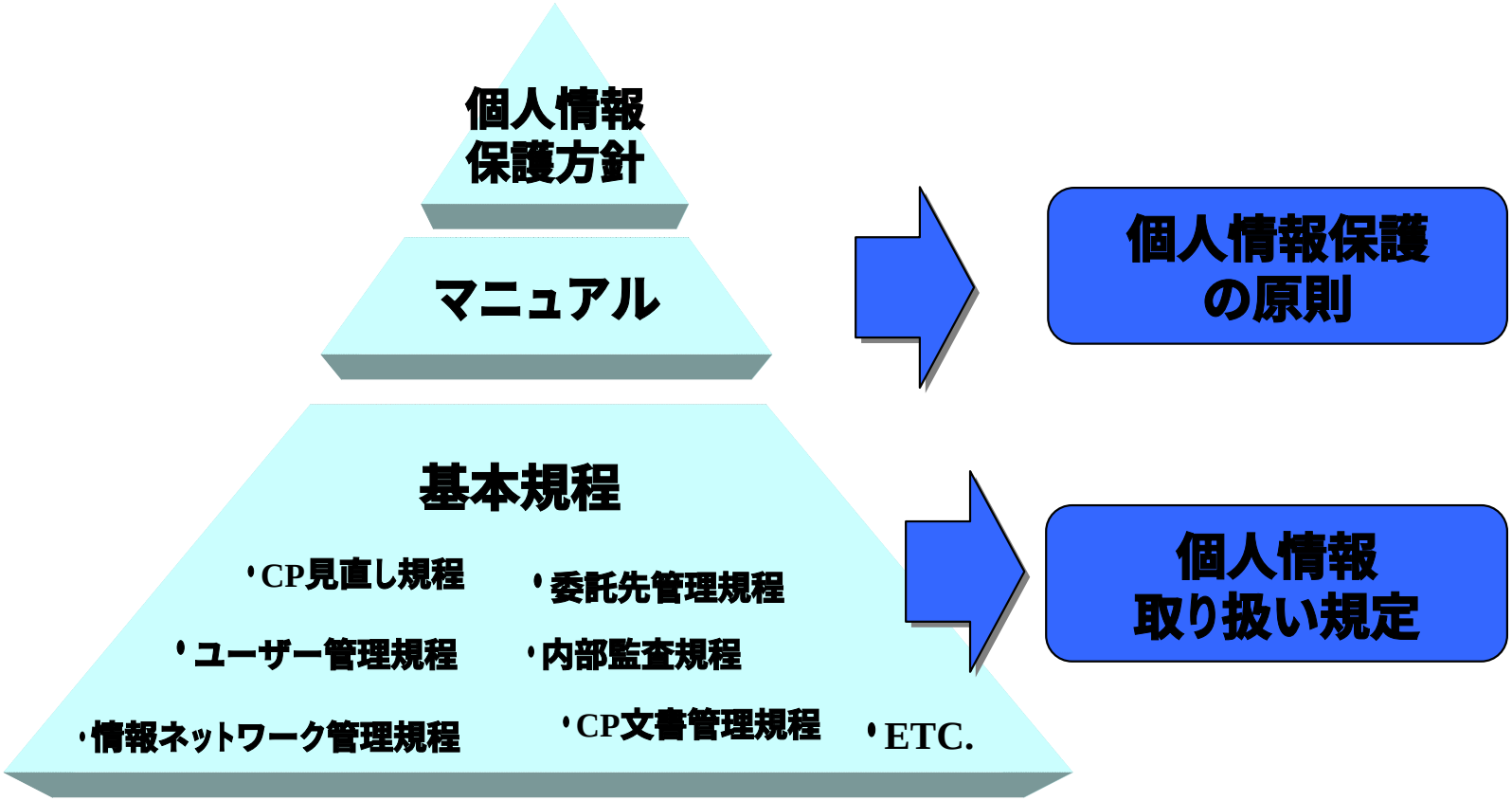
・体制の整備（マネジメントシステムの導入と運用に必要な金銭的資源、人的資源など）

・内部監査

・教育訓練

・経営層による見直し

個人情報保護に関するシステム体系



プライバシーマークと個人情報保護法の関係

対応方法	個人情報保護法	JIS Q 15001:1999
体制作り	第31条（苦情の処理）	4.4.1　体制及び責任
安全性の確保	第20条（安全管理措置） 第21条（従業者の監督） 第22条（委託先の監督）	4.4.2.2　個人情報の利用の安全性の確保
収集時の対応	第17条（適正な取得）	4.4.2.1　収集の原則 4.4.2.2　個人情報の利用の安全性の確保
利用目的の明示	第15条（利用目的の特定） 第16条（利用目的による制限） 第18条（取得に際しての利用目的の通知等） 第23条（第三者提供の制限）	4.4.2.1　収集の原則 4.4.3.1　利用及び提供の原則
透明性、正確性の確保	第24－30条	4.4.5.1　個人情報に関する権利 4.4.4.1　個人情報の正確性の確保

・保護法よりもプライバシーマーク（JISQ15001）の方が高い要求が多い。
→プライバシーマークを取得すれば、保護法に対応できている企業

認証取得のメリット

- ＪＩＳＱ１５００１準拠のマネジメントシステム構築により、責任･権限の明確化が達成される
- 内部監査体制の整備による不具合の早期是正、不正行為の抑止が実現される
- 委託会社の管理基準、認定基準が明確になり、事故防止の体制が構築される
- 第三者認証により、制度の継続が外圧により確保される
- 継続的な教育により、過誤による事故を防止できる
- 第三者認証による取引先、情報主体への信頼度を向上させる

ーホームページ、会社案内、パンフレット、名刺等広くＰＲが可能

･経営課題に解決するためのツールとして利用できる！
･顧客及び消費者に対してアピールできる！

ご清聴ありがとうございました。

当セミナーでのご不明点などはお気軽にお問合せください。

㈱名南経営　ISO事業部

TEL　052－683－7530　FAX　052－683－7532

※当セミナーにおける法及びガイドラインの解釈･対応方法に関しては、弊社での見解に基づくものであり、その内容を保証するものではございません。各事務所様の判断で実施を御願いいたします。