Pマーク付与事業者向け
改正個人情報保護法説明会

（一般社団法人）中部産業連盟
Ｐマーク審査センター
2017年5月17日

個人情報保護改正の背景

- 2003年「個人情報の保護に関する法律」成立（2005年全面施行）
  - その後の情報社会の進展等による環境変化への対応が求められた
  - 個人情報に該当するかどうかの判断が困難な「グレーゾーン」が拡大
  - パーソナルデータ（＊1)を含むビッグデータの適正な利活用ができる環境の整備が必要
  - 事業活動がグローバル化し、国境を越えて多くのデータが流通している現状

- 以下の分野において、プライバシー保護にも配慮したパーソナルデータ利活用のためのデータ利用環境整備が喫緊の課題
  - 行政 /医療 /エネルギー /交通 /防災・減災 /流通・小売

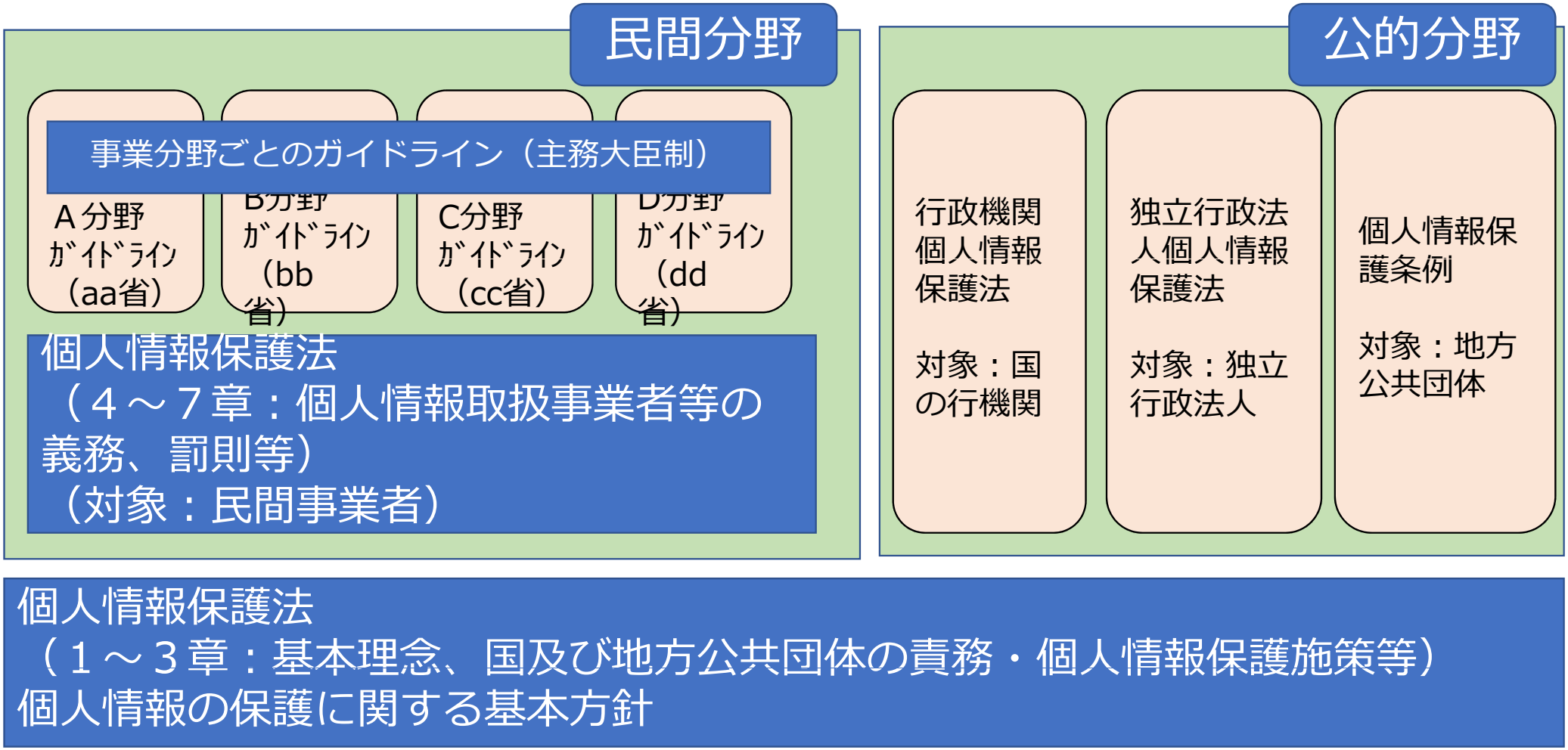
- （＊1)パーソナルデータ
  - 「ビッグデータ」のうち、特に利用価値が高いと期待されている、個人の行動/状態等に関するデータ

個人情報保護法制定/改正

- 「個人情報保護法」は、情報化の急速な進展により、個人の権利利益の侵害の危険性が高まったことや国際的な法制定の動向等を受け、
  - 平成15年5月：公布
  - 平成17年4月：全面施行

- 「定義の明確化」/「個人情報の適正な活用・流通の確保」/「グローバル化への対応」等を目的として、
  - 平成27年９月：改正個人情報保護法が公布
  - 平成28年１月：個人情報保護法の所管が、消費者庁から個人情報保護委員会に移管
  - 平成29年5月：改正個人情報保護法全面施行、各主務大臣が保有している個人情報保護法に関する勧告・命令等の権限は個人情報保護委員会に一元化

個人情報保護法・ガイドラインの体系



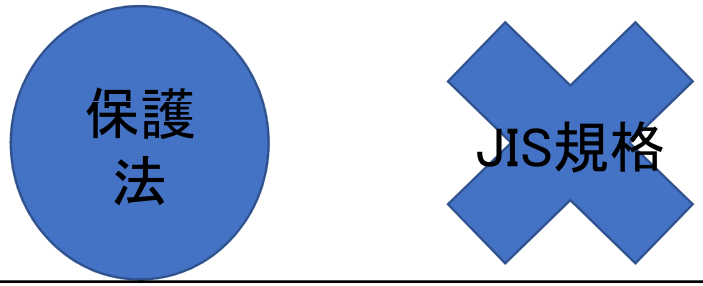
個人情報保護法改正のポイント

- 個人情報の定義の明確化
  - グレーゾーン解消のため、個人情報の定義に身体的特徴等が対象となることを明確化
  - 要配慮個人情報（本人の人種、信条、病歴など本人に対する不当な差別又は偏見が生じる可能性のある個人情報）の取得については、原則として本人同意を得ることを義務化
- 個人情報の有用性を確保（利活用）するための整備
  - 匿名加工情報（特定の個人を識別することができないように個人情報を加工した情報）の利活用の規定を新設
- いわゆる名簿屋対策
  - 個人データの第三者提供に係る確認/記録作成等を義務化
  - オプトアウト手続（＊2）により個人データを第三者提供する個人情報取扱事業者は、所要事項を個人情報保護委員会への届出を義務化、委員会はその内容を公表

    https://www.ppc.go.jp/personal/preparation/optout/
  - 個人情報データベース等を不正な利益を図る目的で第三者に提供し、又は盗用する行為を「個人情報データベース提供罪」として処罰対象（1年以下の懲役又は30万円以下の罰金）

個人情報保護法改正のポイント

- （＊2）オプトアウト手続き
  - 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止する場合、本人の同意を得ることなく第三者に個人データを提供することができる
  - →JISQ15001規格は個人情報保護法よりもその取扱いに厳しい点があり、上記の様なオプトアウトは認めていない



- 個人情報保護委員会の新設
  - 個人情報取扱事業者に対する監督権限を各分野の主務大臣から委員会に一元化
- その他
  - 取り扱う個人情報の数が5,000件以下の事業者も適用対象
  - 外国にある第三者への個人データの提供の制限、個人情報保護法の国外適用、個人情報保護委員会による外国執行当局への情報提供に係る規定を新設

個人情報の保護に関する法律（目次）

個人情報保護法の主な内容

- 目的（法1条）
  - 個人情報保護法の目的は、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであること、その他の個人情報の有用性に配慮しながら、個人の権利利益を保護すること
- 個人情報・個人データ・保有個人データ（法2条）
  - 「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できるもの」
  - データベース化した個人情報は「個人データ」、そのうち、事業者が開示等の権限を有し6か月以上にわたって保有する個人情報は「保有個人データ」
- 個人情報取扱事業者（法2条）
  - 「個人情報取扱事業者」とは、個人情報データベース等を事業活動に利用している者のことをいい、個人情報保護法に定める各種義務が課される
  - 改正後は、5,000人分以下の個人情報を取り扱う事業者についても個人情報保護法の義務の対象になった
- 利用目的の特定（法15条）
  - 個人情報を取り扱うに当たっては、利用目的をできるだけ特定する
- 目的外利用の禁止（法16条）
  - 原則として、あらかじめ本人の同意を得ずに、その利用目的の達成に必要な範囲を超えて個人情報を取り扱うことは禁止される

個人情報保護法の主な内容

- 適正な取得（法17条）
  - 偽りその他不正な手段によって個人情報を取得することは禁止する
- 取得時の利用目的の通知等（法18条）
  - 個人情報の取得に当たっては、取得前にあらかじめ利用目的を公表し、又は取得後に速やかに本人に利用目的を通知又は公表する
- データ内容の正確性の確保（法19条）
  - データは正確かつ最新の内容に保つように努める
- 安全管理措置（法20条）
  - 安全にデータを管理するため、従業者や委託先に対し必要かつ適切な監督を行う
- 従業者や委託先の監督（法21・22条）
  - 個人データの漏えいや滅失を防ぐため、必要かつ適切な保護措置を講じる
- 第三者提供の制限（法23条）
  - 原則として、あらかじめ本人の同意を得ずに本人以外の者に個人データを提供することは禁止
  - 委託、事業承継及び共同利用に該当する場合は、第三者提供の特例が適用される

個人情報の定義の明確化（「個人識別符号」法2条）

- 個人情報の範囲に関するグレーゾーンを解消するため、個人情報の定義を明確化するため、情報単体でも個人情報に該当することとした「個人識別符号」という概念を新設
- 個人識別符号とは以下のいずれかに該当するもので、政令・規則で個別指定
  - 身体の一部の特徴を電子計算機のために変換した符号：DNA情報、指紋・掌紋、声紋、顔、虹彩、手指の静脈、歩行の態様
  - サービス利用や書類で対象者ごとに割り振られる符号：公的な番号（旅券番号、基礎年金番号、運転免許証番号、住民票コード、マイナンバー、各種保険証番号等）
- 「身体の一部の特徴を電子計算機のために変換した符号」については、個人情報保護委員会規則で定める「特定の個人が識別できる水準」に適合するものが該当する
- クレジットカード番号や携帯電話番号等も、これら番号が氏名、住所などと一緒に管理されていたり、他の情報と照合することで特定の個人を識別できる場合には、「個人情報」に該当する
- 個人識別符号は、それ単体で個人情報となるため、従来の個人情報と同様に、法令に基づき適正に取得/利用/保管/処分する

個人情報の定義の明確化（「要配慮個人情報」法2条）

- 要配慮個人情報とは、人種、信条、社会的身分、病歴、前科・前歴、犯罪被害情報に加え、その他本人に不当・偏見が生じないように特に配慮を要するものとして、政令で定めるもの
  - 病歴に準ずるもの：身体・知的・精神障害、健康診断等の検査の結果、保健指導、診療・調剤情報等
  - 前科・前歴に準ずるもの：被疑者または被告人として逮捕、捜索等、刑事事件手続が行われた事実と、非行少年またはその疑いのある者として、保護処分等の少年保護事件手続が行われたこと

- 要配慮個人情報については、原則、取得・第三者提供時の本人同意が必要となる→これまでオプトアウトを利用して要配慮個人情報を第三者提供していた事業者の場合も、事前同意が必要
- 例外規定あり（人の生命・身体・財産の保護に必要な場合等には、本人同意なく取得・第三者提供することが認められる等）
- ある個人が宗教関連書籍を購入したという情報だけでは、その人の信条を推定できるだけであるため、要配慮個人情報（信条）には該当しない

第三者提供に係る確認・記録義務（法第25-26条）

- 第三者との間で個人データを提供・受領する場合、提供先が提供元のデータ取得経緯等を確認して記録
  - 提供元/提供先が相互に相手の氏名/社名
  - 提供先が提供元のデータ取得経緯
- 提供/受領の都度に確認/記録することでビジネスに支障が及ばない様に、以下の配慮
  - 第三者提供に関する本人同意がある場合、提供年月日の記録は不要
  - 記録の保存期間は原則3年だが、本人同意で第三者提供した場合は1年
  - 本人との契約等に基づく提供の場合は、既存の契約書等で代替可能
  - 反復継続して提供する場合は、包括的な記録で可
- 以下の場合は、確認/記録義務がない
  - 法令に基づく提供
  - 本人による提供（SNS等に記載されている本人発信によるプロフィール）
  - 本人に代わって提供（銀行振込）
  - 本人側への提供（同席している家族）
  - 受領者にとって「個人データ」に該当しない（名刺１枚） 等

第三者提供に係る確認・記録義務（法第25-26条）

提供者側の記録

	オプトアウトによる提供	本人同意による提供
提供年月日	○	
第3者の氏名等	○	○
本人の氏名等	○	○
個人データの項目	○	○
本人の同意		○

受領者側の記録

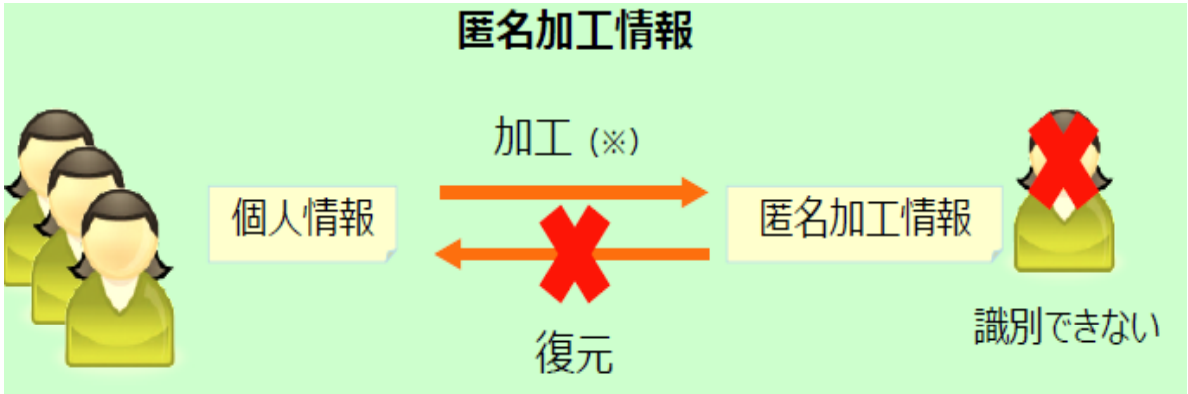
	オプトアウトによる提供	本人同意による提供
提供年月日	○	
第3者の氏名等	○	○
本人の氏名等	○	○
個人データの項目	○	○
本人の同意		○
個人情報保護委員会の公表	○	

匿名加工情報取扱事業者が遵守する義務等　法36-39条

- 匿名加工情報とは、特定の個人を識別できないように個人情報を加工し、当該個人情報を復元できないような形にしたもの
- 目的外利用や第三者提供の際の本人同意を不要とし、自由な利活用が可能で、データ利活用ビジネスの活性化が期待される
- 匿名加工情報を取り扱う個人情報取扱事業者→匿名加工情報取扱事業者

- 個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）

  →個人情報取扱事業者又は匿名加工情報取扱事業者に適用



匿名加工情報取扱事業者が遵守する義務等　法36-39条

- 匿名加工情報の作成の際は、特定の個人が識別できず、元の個人情報が復元できないように、以下の措置を講ずる
  - 特定の個人を識別可能な記述等（氏名等）の全部または一部を削除
  - 個人識別符号の全部を削除
  - 個人情報と他の情報を連結する符号を削除
  - 特異な記述等（例：日本最高齢者であることが判断可能な実年齢）を削除
- 匿名加工情報を作成したときは、加工方法等の情報の安全管理措置を講じる
  - 組織的安全管理措置
  - 人的安全管理措置
  - 技術的安全管理措置
  - 物理的安全管理措置

組織的安全管理措置　/　人的安全管理措置

- 組織体制の整備
  - 個人データを取り扱う従業者が複数いる場合、責任者と従業者を区分する
- 個人データの取扱いに規律に従った運用
  - あらかじめ整備された取扱方法に従って個人データが取り扱われていることを、責任者が確認する
- 個人データの取扱状況の確認手段の整備
  - あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任者が確認する
- 漏えい等への対応体制の整備
  - 漏えい等の事案の発生時に備え、従業者から責任者に対する報告連絡体制等をあらかじめ確認する
- 取扱状況の把握及び安全管理措置の見直し
  - 責任者が、個人データの取扱状況について、定期的に点検を行う

- 従業者教育については、
  - 個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う
  - 個人データについての秘密保持に関する事項を就業規則等に盛り込む

技術的安全管理措置　/　物理的安全管理措置

- アクセス制御
  - 個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する
- アクセス者の識別と認証
  - 機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する
- 外部からの不正アクセス等の防止
  - 個人データを取り扱う機器等のオペレーティングシステムを最新の状態に保持する。
  - 個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする
- 情報システムの使用に伴う漏えい等の防止
  - メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する
- 個人データを取り扱う区域の管理
  - 個人データを取り扱うことのできる従業者及び本人以外が容易に個人データを閲覧等できないようにする
- 機器及び電子媒体等の盗難等の防止
  - 個人データを取り扱う機器、記録された電子媒体又は記載された書類等を、施錠できるキャビネット/書庫等に保管する。
  - 個人データを取り扱う情報システム機器をセキュリティワイヤー等により固定する
- 電子媒体を持ち運ぶ場合の漏えい等の防止
  - 個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐ
- 個人データの削除及び機器、電子媒体等の廃棄
  - 個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄したことを、責任者が確認する

匿名加工情報取扱事業者が遵守する義務等　法36-39条

- 匿名加工情報を作成したときは、当該情報に含まれる情報の項目を公表する
  - 匿名加工情報を作成した後、遅滞なく、インターネット等で公表する
  - 個人情報取扱事業者が委託を受けて匿名加工情報を作成した場合は、委託元が公表する
  - 事例)「氏名・性別・生年月日・購買履歴」のうち、氏名を削除した上で 、生年月日の一般化、購買履歴から特異値等を削除する等加工して、「性別・生年・購買履歴」に関する匿名加工情報として 作成した場合の公表項目は、「性別」、「生年」、「 購買履歴」である
- 匿名加工情報を第三者提供するときは、提供する情報の項目及び提供方法について公表するとともに、提供先に当該情報が匿名加工情報である旨を明示(電子メール又は書面等)する
- 匿名加工情報を利用するときは、元の個人情報に係る 本人を識別する目的で、加工方法等の情報を取得し、又は他の情報と照合することを行ってはならない
- 匿名加工情報の適正な取扱いを確保するため、安全管理措置、苦情の処理などの措置を自主的に講じて、その内容を公表するよう努める

外国の第三者への個人データの提供（法24条）

- 以下のいずれかの条件で、国内と同様に外国の第三者への個人データの提供が可能
  - 外国にある第三者へ提供することに対し、本人が同意している場合
  - 外国にある第三者が、個人情報保護委員会の定める基準に適合している場合
  - 外国にある第三者が個人情報保護委員会の認めた国に所在する場合（現在、該当する国はない）

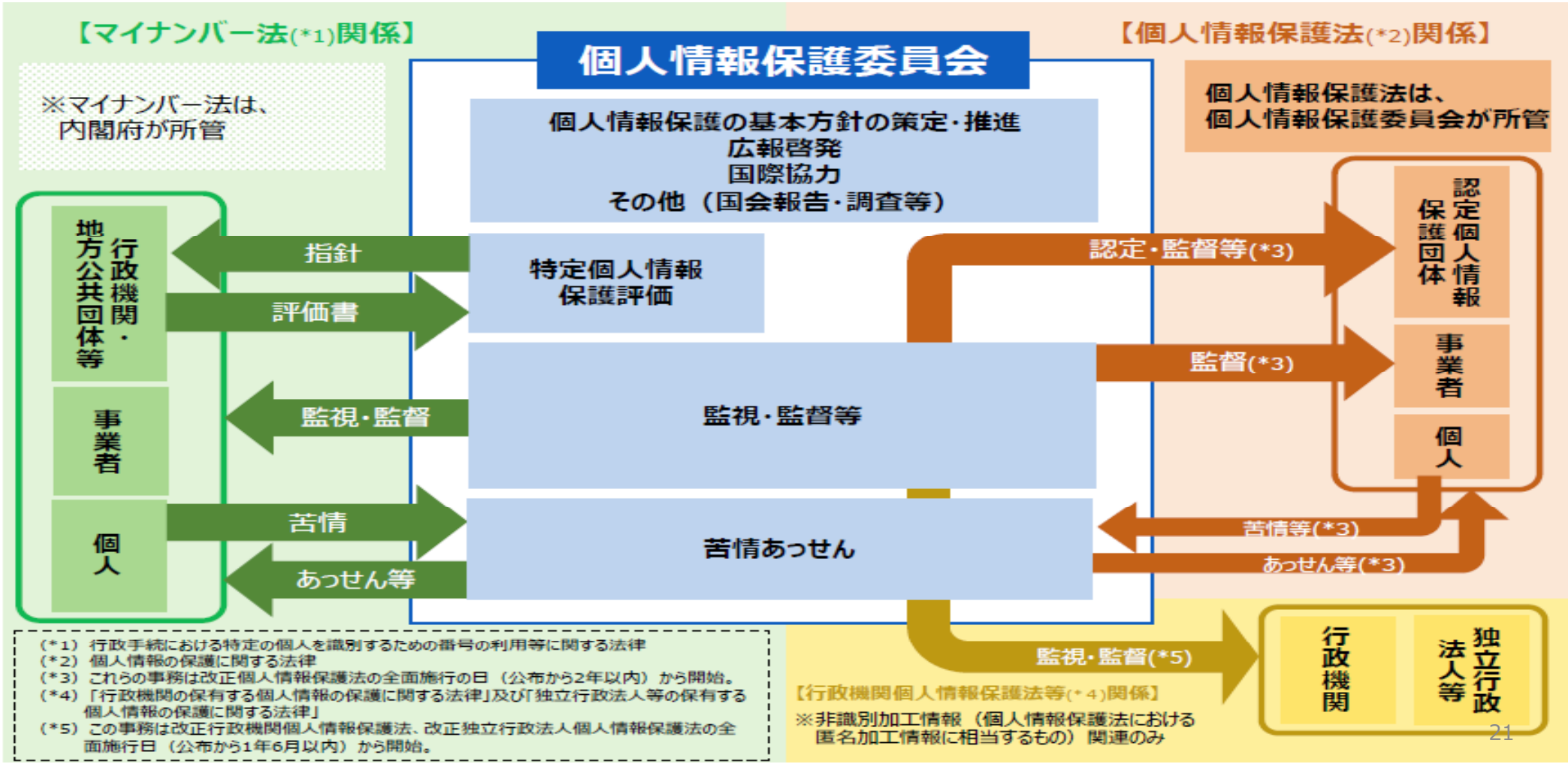
- 個人情報保護委員会で定める基準
  - 提供を受ける者の個人データの取扱いが、個人情報保護法の趣旨に沿った措置（OECDプライバシーガイドラインやAPECガイドライン等）の実施が確保されている
  - 個人データを受ける企業が、個人情報保護の国際的な枠組み（APEC CBPR等）に基づく認定を受けている

- 個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）

個人情報保護委員会（法第59-74条）

- 沿革
  - 平成26年1月：特定個人情報保護委員会 設置
  - 平成28年1月個人情報保護委員会設置 （特定個人情報保護委員会から改組）
- 所掌事務
  - マイナンバー制度に関する事務（監視・監督、特定個人情報保護評価）
  - 個人情報保護法に関する事務及同法に基づく監視・監督業務（個人情報保護法を所管）
  - 上記に関する広報・啓発、国際協力等
- 組織
  - 委員長1名・委員8名の合議制（行政委員会）
  - 委員長・委員は独立して職権を行使（任期5年）
  - 委員会事務局の職員数：97名（平成28年8月現在）

個人情報保護委員会（法第59-74条）



JIPDECの対応方針（2016/11/30）

- JIS Q 15001:2006では、法令への遵守が要求されていて、Ｐマーク付与事業者は法令等の改正に適切に対応できるマネジメントシステムを構築/運用されていて、改正個人情報保護法施行後もＰマークは有効
- 改正個人情報保護法の全面施行に伴い、必要な措置の実施が必要

- Ｐマーク付与事業者に向け、以下の対応を実施
  - ー改正個人情報保護法に向けた審査情報を、「よくある質問と回答（FAQ）」として適宜ホームページで公表
  - ーＰマーク推進センター内にお問合せ窓口を設け、事業者の個別質問に対応
  - ー現地審査等では、事業者の改正個人情報保護法への対応状況を確認し、助言

JIPDECのFAQ抜粋

- 改正個人情報保護法施行後において、審査の基準は変更ないが、必要な措置を講じる必要がある
- 改正個人情報保護法を遵守するための必要な措置を取っていなかった場合、状況に応じて助言して、リスクに応じた措置を求めます
- 改正個人情報保護法の全面施行にあたり、プライバシーマーク付与事業者が個人情報保護方針を変更する必要はないと考えられる

- 個人識別符号/要配慮個人情報/匿名加工情報は、「個人情報台帳」等に登録する必要がある
- 個人識別符号/要配慮個人情報/匿名加工情報は、「リスク分析/対策表」等に記載する必要がある
- 個人識別符号、要配慮個人情報についても、安全管理措置を講じる必要がある
- 「同意書」への記載事項(3.4.2.4、3.4.2.6、3.4.2.7、3.4.2.8)の変更の必要はないと考えられる

引用/参考情報(HP)

- 個人情報保護委員会
  - https://www.ppc.go.jp/
- 改正個人情報保護法の準備について
  - https://www.ppc.go.jp/personal/preparation/
- JIPDEC
  - https://privacymark.jp/