日本組織内弁護士協会(JILA)

個人情報保護法

ベネッセ事件等を受けた各省ガイドラインの改定及び法令改正の動向

2015年8月31日

山下・柘・二村法律事務所　中崎　隆

個人情報保護法ガイドラインの改定

ベネッセ事件と各省のガイドラインの改定

- 経済産業省は、「**経済産業分野を対象とするガイドライン**」を2014年12月12日に改定。
- 総務省は「**電気通信事業における個人情報保護に関するガイドライン**」を2015年6月24日に改定。
- 金融庁は「**金融分野における個人情報保護に関するガイドライン**」及び「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」を2015年7月9日に改定。

【改定の背景】

ベネッセ社の大規模な個人情報漏えい事案等を踏まえ、政府全体として、各分野における個人情報の適正な取扱いを徹底する必要がある旨を個人情報保護関係省庁連絡会議において確認し、これを踏まえて、各省庁が、ガイドラインを改定。

【参考：ベネッセ社に対する勧告】

― 2014年9月26日　経産省がベネッセ社に対して個人情報保護法第34条1項の規定に基づき勧告

［事案の概要］

業務委託先元社員が、弊社お客様情報を不正に取得し、約3,504万件分の情報を名簿業者3社へ売却（ただし、ベネッセ社では、実態の被害件数としては、約2,895万件と推計）。 漏えいした情報項目は、登録者の氏名、性別、生年月日、住所、電話番号、メールアドレス等。クレジットカード番号は含まれず。ベネッセ社のライバル社等が情報源による情報の適正取得を十分に確認せず、ダイレクトメール等に利用。

［処分の理由］

個人データの安全管理のために必要かつ適切な措置を講じることを怠り、法第22条の規定に基づき委託を受けた者に対する必要かつ適切な監督を行うことを怠った結果、個人情報が漏えいし、個人の権利利益を侵害したと認められた。

経済産業分野のガイドラインの改定
(1)社内の安全管理措置(法20条)の強化

[問題点]

- ✓ 個人情報のダウンロードを監視するシステムが、設定されていなかった。
- ✓ 個人情報を取り扱う部屋へ、私物であるスマートフォンを持ち込むことができた。また、個人情報のデータベースに、そのスマートフォンが接続できる状態になっていた。
- ✓ 個人情報のダウンロードのログ(記録)について、定期的な確認が行われておらず、長期間にわたり、漏えいの事実を把握できていなかった。
- ✓ 「性善説」に立った、不十分な社内管理体制になっていた。

[ガイドラインの改定事項]

[技術的安全管理]

- ✓ 個人情報の監視システムについて、その動作を定期確認。
- ✓ 個人情報へのアクセスやダウンロードのログ(記録)について、不正が疑われる異常な記録の存否を定期確認。

[物理的安全管理]

- ✓ 業務上許可を得ていない記録機能を有する媒体・機器の持ち込み・持ち出しの禁止又は検査の実施。
- ✓ カメラや立ち会い等によるモニタリングの実施。
- ✓ 個人情報を取り扱う部屋への入退室記録の保存。

[物理的安全管理]

- ✓ 個人情報保護管理者(CPO)への役員の任命など、社内体制の整備。
- ✓ 情報セキュリティ等に十分な知見を有する者による社内の監査体制の構築。
- ✓ スマートフォン等の記録機能を有する機器の接続制限を行う社内規程の整備。

※経済産業省作成平成26年9月30日付資料「個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインの改訂」を参考に作成。

経済産業分野のガイドラインの改定
(2)委託先等の監督(法22条)の強化

[問題点]

- ✓ システム開発・管理の委託先(子会社)における安全管理措置が十分でなく、そこから個人情報が不正に持ち出された。
- ✓ ベネッセとして、委託業務の一部が、委託先から他の企業へ再委託、再々委託されていることを十分に把握できておらず、委託先等を適切に監督していなかった。

[ガイドラインの改定事項]

[委託先の監督]

- ✓ 委託先の選定に当たり、委託先の安全管理措置を確認し、CPO等が評価。
- ✓ 定期的に(少なくとも年1回)、委託業務の監査を実施し、その結果について、CPO等が評価。
- ✓ 委託契約等において、委託先で個人データを取り扱う者の役職又は氏名、損害賠償責任を盛り込む。

[再委託先の監督]

- ✓ 委託元は、委託先が再委託を行う場合には、委託先から、事前報告又は承認の申請を求める。
- ✓ 委託元は、委託先を通じて、又は必要に応じて自らが、再委託先に対し、定期的な監査を実施。
- ✓ 再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。

※経済産業省作成平成26年9月30日付資料「個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインの改訂」を参考に作成。

経済産業分野のガイドラインの改定
(3)第三者からの適正な情報取得(法17条)の徹底

[問題点]

- ✓ 個人情報を取得した者は、提供元(eg.ベネッセ社の委託先の元社員)がそれを適法に入手したことを十分に確認しないまま(提供元から「誓約書」を取得するという形式的な対応)、当該情報を入手していた。

[ガイドラインの改定事項]

- 第三者から個人情報を取得する場合(※)には、
  - ― 提供元の選定に当たり、その個人情報保護法の遵守状況を確認。
  - ― 取得の都度、当該個人データの取得方法等について、例えば、取得の経緯を示す契約書等の書面を点検する等により、適法に入手されていることを確認。
    (※)不特定かつ多数の者が購入することができるものから取得する場合、法令に基づき提供される場合、承継、共同利用、委託等の場合を除く。
- 第三者から個人情報を取得する場合において、当該個人情報が適法に入手されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応。

(4)中小企業への対応

「事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じる」という基本原則の中で、中小企業への「一定の配慮」を規定。

パブリックコメントでの意見	パブリックコメントへの回答
中小企業も多く含まれ得ることを踏まえると、IDS (Intrusion Detection System)やIPS (Intrusion Prevention System)を導入することは非常にハードルが高い。	全ての事業者に導入することを義務づけているわけではありません。事業者の規模や情報の内容などを踏まえてご判断いただければと思います。

※経済産業省作成平成26年9月30日付資料「個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインの改訂」を参考に作成。

総務省のガイドラインの本文及び解説の改定

2015年1月から、「ICTサービス安心・安全研究会」WGにおいて検討を行った結果、以下の点について改定。

- 【ベネッセ事件との関係　－　省庁共通】
  電気通信分野においてもベネッセ事件を踏まえて、①第三者からの適正な情報取得の徹底、②社内の安全管理措置の強化、③ 委託先の管理の強化についての具体例や望ましい対応についての記載をガイドライン本文及び解説に追加する。なお、ガイドライン本体への改正は、次頁記載のもののみで、他は、解説の改定となる。

- 【その他　－　総務省ガイドライン独自の事項】
  ○通信ログの保存期間
  通信の秘密として保護される通信履歴（ログ）の保存の在り方について、利用者への対応やセキュリティ対策等の業務との関係で検討の要請があり、インターネットの利用状況に関わる通信履歴である接続認証ログ について、正当業務行為 として保存が許容される期間をガイドラインの解説で具体的に例示。すなわち、「（接続認証ログの保存については、事業者が正当業務の遂行に必要とする場合、）一般に6か月程度の保存は認められ、適正なネットワークの運営確保の観点から年間を通じての状況把握が必要な場合など、より長期の保存をする業務上の必要性がある場合には、1年程度保存することも許容されると考えられる。」ものと解説に追記。

  ○携帯電話端末のGPS位置情報の捜査での利用
  携帯電話端末のGPS位置情報の捜査での利用についての実効性の確保の要請があったため、次頁のとおり本文を改定し、「当該位置情報が取得されていることを利用者が知ることができる」という要件を、不要とする。これにより、GSP位置情報を、警察が捜査に利用しやすくなる。

総務省のガイドラインの改定

改定前	改定後
第26条（位置情報） 第4項　電気通信事業者は、第4条の規定にかかわらず、捜査機関からの要請により位置情報の取得を求められた場合において、当該位置情報が取得されていることを利用者が知ることができるときであって、裁判官の発付した令状に従うときに限り、当該位置情報を取得するものとする。	第26条（位置情報） 第4項　電気通信事業者は、第4条の規定にかかわらず、捜査機関からの要請により位置情報の取得を求められた場合において、裁判官の発付した令状に従うときに限り、当該位置情報を取得するものとする。

改定前	改定後
第12条（従業者及び委託先の監督） 第4項　電気通信事業者は、前項の場合は、個人情報を適正に取り扱うと認められる者を選定し、委託契約において、安全管理措置、秘密保持、再委託の条件（再委託を許すかどうか並びに再委託を許す場合は再委託先の選定及び再委託先の監督に関する事項等）その他の個人情報の取扱いに関する事項について適正に定めるものとする。	電気通信事業者は、前項の場合は、個人情報を適正に取り扱うと認められる者を選定し、委託契約において、安全管理措置、秘密保持、再委託の条件（再委託を許すかどうか並びに再委託を許す場合は再委託先の選定及び再委託先の監督に関する事項等）、委託契約終了時の個人情報の取扱い、契約内容が遵守されなかった場合の措置その他の個人情報の取扱いに関する事項について適正に定めるものとする（※）。

※　委託契約において定めるべきとされる事項が増えています。

金融庁のガイドライン及び安全管理措置等についての実務指針の改定

(1)社内の安全管理措置(法20条)の強化

- ①セキュリティパッチの適用等
  個人データを扱う情報システムについて、「セキュリティパッチの適用や情報システム固有の脆弱性の発見、その修正等、ソフトウェアに関する脆弱性対策を行わなければならない」旨が追記された。
- ②新たなリスクへの対応
  新たなリスクに対応するために、情報セキュリティ対策に十分な知見を有する者による、社内の対応の確認等を実施することが望ましい旨が追記された。
- ③個人データへのアクセス記録
  個人データのアクセス記録を取り、その分析・保存を行わなければならないことが従前から明記されていましたが、アクセス記録といった場合に、アクセス(Read)だけでなく、操作(Write)の記録も含まれる旨が明記された。
- ④再委託の際の安全管理措置について
  委託契約において、(i) 再委託の際の委託元への文書による事前報告又は承認等の手続き、及び、(ii)委託先において個人データを取り扱う者の氏名・役職又は部署名を盛り込むことが望ましいことが明記された。
- ⑤安全管理に係る取扱規程について
  安全管理に係る取扱規程において、(i)入退館記録の保存などの入退館管理の措置、(ii)監視カメラによる撮影など、盗難・情報窃盗等の防止のための措置、(iii)不正な操作を防ぐための、個人データを取り扱う端末に付与する機能の、業務上の必要性に基づく限定についての事項を定めることが望ましい旨が追記された。

金融庁のガイドライン及び安全管理措置等についての実務指針の改定
(2) 委託先等の監督(法22条)の強化

- 委託先の安全管理措置の確認、定期的な監査等の追加

  委託先について、(i)その選定にあたって、必要に応じて現地に赴き又はこれに代わる合理的な方法による確認を行うことが望ましいこと、(ii)委託先の選定や安全管理措置等の遵守状況について、個人データ管理責任者等が適切に評価することが望ましいこと、(iii)委託先の監督は、「滅失又は棄損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、委託する事業の規模及び性質並びに個人データの取扱状況等に起因するリスクに応じたものとする」とされ、委託する事業の規模(例えば、委託される個人データの件数や量等)も考慮されるべきことの3点が追記された。

  また、実施しなければならないとされる委託先の安全管理措置等の遵守状況の確認について、「定期的に監査を行う等により」と追記することで、リスクの高い事案において、定期的な監査を行うことをより促すような文言となった。

- 再委託先についての同様な措置(安全管理措置の確認等)の追加

  再委託先について、再委託の相手方、再委託する業務内容、及び再委託先の個人データの取扱方法等について、委託先に事前報告又は承認手続きを求めたり、定期的な監査を自ら実施し又は委託先等を通じて実施すること等により、再委託先が安全管理措置を講ずることを十分に確認することが望ましいことが明記された。

金融庁のガイドライン及び安全管理措置等についての実務指針の改定

(3) 第三者からの適正な情報取得(法17条)の徹底

- 「第三者からの提供により、個人情報を取得する場合には、情報提供元の法の順守状況を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に、個人情報を取得する際には、例えば、取得の経緯を示す契約書等の点検又はこれに代わる合理的な方法により、当該個人情報の取得方法等を確認した上で、当該個人情報が適法に取得されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい」との趣旨が追記された。2014年12月に行われた経済産業省ガイドラインの改定とも足並みを揃える内容である。

補足

①個人情報保護法に基づく義務として位置付けられる事項(「~しなければならない」)と、②個人情報保護法に基づく義務ではないが、金融機関として実施することが**努力措置**として求められる事項(「~こととする」、「~が適切である」、「~が望ましい」)との双方があるため、ガイドラインの語尾に留意する必要がある。

なお、個人情報保護法上、法的義務とまでは言えない事項についても、業法に基づき、一定の義務がかかる場合があり、個人情報保護法のガイドラインがそちらの解釈に影響する場合もありえるため、注意が必要である。

認定個人情報保護団体による個人情報保護指針の改定

[認定個人情報保護団体による個人情報保護指針の改定]

- ✓ 日本証券業協会は、個人情報保護指針を平成27年8月25日付で改定、10月5日施行
- ✓ 日本生命保険協会は、個人情報保護指針を平成27年7月9日付で改定

など。

- ✓ 今後、各認定個人情報保護団体で、可決が予定されている個人情報保護法の改正や、上記ガイドライン改定（まだ改定の内容を反映できていない場合）等を受けた、個人情報保護指針等の改定を検討する必要。

- ✓ 特に、匿名加工情報についての匿名加工の方法等については、業界団体に、一定の裁量の余地が認められるのではないか。

個人情報保護法の改正

現行個人情報保護法の主たる規制

利用目的の特定（15条1項）	→	個人情報を取り扱うにあたっては、利用目的をできる限り特定しなければならない。
利用目的の変更の制限（15条2項）	→	個人情報の利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない（15条2項）。
目的外利用による制限（16条）	→	あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない（16条1項）。
適正な取得（17条）	→	偽りその他不正の手段により個人情報を取得してはならない。
取得に際しての利用目的の通知等（18条）	→	個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、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。変更時も同様。
データ内容の正確性の確保（19条）	→	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。
安全管理措置（20条）	→	取り扱う個人データの漏えい、滅失又は棄損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

現行個人情報保護法の主たる規制

従業者の監督（21条）	→	従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業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。
委託先の監督（22条）	→	個人データの取り扱いを委託する場合は、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。
第三者提供の制限（23条）	→	法令に定める場合を除くほか、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。
保有個人データに関する事項の公表等（24条）	→	保有個人データに関し、一定の場合を除き、事業者の氏名又は名称、保有個人データの利用目的、開示等の求めに応じる手続き等を本人の知りうる状態に置かなければならない。
開示（25条）	→	本人が識別される保有個人データの開示を本人から求められた場合、これを開示しなければならない。
訂正等（26条）	→	保有個人データの内容が事実でないという理由によって本人から訂正等を求められ、理由があるときは、原則として訂正等を行わなければならない。
利用停止等（27条）	→	本人から、16条の違反又は17条の違反を理由に保有個人データの利用の停止又は消去を求められ、理由がある場合は、原則として利用停止等を行わなければならない。

なぜ改正か

- 個人情報の保護が不十分であることへの対処のため。

  名簿屋等を通じたベネッセ社のデータの大量流失等。

- 個人情報の利活用の促進のため。

- 国際的な規制の潮流に対応するため。

  欧州のデータ保護規制との関係で、日本は、「十分なデータ保護レベルを確保していない第三国」との位置づけ。これにより、EUから日本へのデータ移転等に支障を生じているため、EUにおける同等性認定を得たい。

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	→	個人情報の定義の明確化（身体的特徴等が該当）、要配慮個人情報に関する規定の整備
適切な規律の下で個人情報等の有用性を確保	→	匿名加工情報に関する加工方法や取扱等の規定の整備、認定個人情報保護団体による個人情報保護指針の届出、公表等の規定の整備
個人情報の保護を強化	→	トレーサビリティの確保（第三者提供に係る確認及び記録の作成等）、個人情報データベース等提供罪の新設
個人情報保護委員会の新設及びその権限	→	個人情報保護委員会を新設し、現行の主務大臣の権限を一元化
個人情報の取扱いのグローバル化	→	国境を越えた適用と外国執行当局への情報提供に関する規定の整備、外国にある第三者への個人データの提供に関する規定の整備
その他改正事項	→	本人同意を得ない第三者提供（オプトアウト）の届出、公表等厳格化、利用目的の変更の要件の緩和、取り扱う個人情報が5000人以下の小規模取扱事業者についての適用除外削除、開示等請求権の明確化

1 「個人情報」の定義の明確化

(1) 趣旨

- 個人情報法における「保護対象の明確化」。(従来の)「個人情報の定義を拡大、拡充するものではない」(衆議院内閣委員会 5/8 山口国務大臣答弁)

(2) 改正の内容

- 個人識別符号の概念を新設。(実質的には、個人情報の範囲を拡張)
- 個人識別符号にあたるものは、氏名等を含まずとも当然に個人情報となる。
- 個人識別符号該当の基準—①個人と情報の結びつきの程度(一意であるかなど)、②不変性、③本人への到達性(情報に基づいて直接個人にアプローチできるか等)

(3) 補足

- 個人識別符号にあたると政令で整理されそうなもの — 指紋データ・顔認証データ、運転免許証番号、旅券番号、基礎年金番号、保険証番号。
- 個人識別符号にあたらないと政令で整理されそうなもの — クレジットカード番号、携帯端末番号、クッキー、固定電話回線の電話番号、法人契約の電話番号。
- 個人識別符号に一概にあたるとはいえないとの答弁 — 携帯電話番号のうち、個人契約の携帯番号(特にプリペイド以外)については該当する可能性あり。

政令では、個別列挙(免許証等)と、該当する情報の性質記載の二本立ての予定。

1　個人識別符号（国会答弁）

（4）　国会答弁

「**携帯電話番号、クレジットカード番号、メールアドレスおよびサービス提供のための会員ID**については、さまざまな契約形態や運用実態があることから、現時点におきましては、一概に個別識別符号に該当するとは言えないものと考えております。

ただし、こういうようなものは、時代の流れや技術の進歩、あるいは諸外国の情勢等によりまして変わっていくものでございますので、今後、政令の制定、運用に当たりましては、諸外国における取り扱いや技術動向も注視しつつ、社会実態を反映し、該当性が明確となるよう努めてまいりたいと考えております。」（衆議院内閣委員会　５月８日　向井政府参考人答弁）

コメント：　クレジットカード加盟店では、クレジットカード番号と一緒に、氏名等も、一緒に収集していることがほとんどであろうから、いずれにしろ、個人情報として取り扱わなければならない可能性が高い。クレジットカードが、個別識別符号に該当するかどうかは、カード情報を、匿名加工情報として利用する際の程度等に影響があるかもしれません。なお、割賦販売法の改正により、加盟店に、クレジットカード番号漏洩防止の努力義務の規定が導入される予定。

1　容易照合性とQ14問題

- 「委員御指摘のような、社内規定などで厳格に管理されている場合についても、例えば事業者内部での技術的な照合が相当困難であるとか、独立したデータベースをそれぞれ別の管理者が管理し、社内規定等により容易にアクセスできないようになっているなどの、事業者内部において通常の業務における一般的な方法で照合が不可能となっているものの、例えばシステムを管理して、システムを管理といっても、メンテナンスをするような技術者、業務に関係のないような技術者が、たまたまきょうそこにアクセスをされるような場合があったからといって、直ちにこれが容易照合性があるというふうには解釈するべきではないと考えておりまして、そういう、一般的な方法で照合が不可能になっているものであれば、容易に照合できるような状態にないと解釈することはあり得るものと現行法でも考えております。」（衆議院内閣委員会　5月8日　向井審議官の答弁）

- 経済産業省　個人情報保護法QA14番　＝　国会答弁と比べても厳しすぎ。
http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212qa.pdf

他の取扱部門のデータベースへのアクセスが規程上・運用上厳格に禁止されている場合であっても、双方の取扱部門を統括すべき立場の者等が双方のデータベースにアクセス可能なときには、当該事業者にとって「容易に照合することができ」る状態にあると考えられます。ただし、経営者、データベースのシステム担当者などを含め社内の誰もが規程上・運用上、双方のデータベースへのアクセスを厳格に禁止されている状態であれば、「容易に照合することができ」るとはいえないものと考えられます (2014年12月12日)

2 利用目的の変更の制限の緩和（15条2項）

(1)趣旨

- 「相当の関連性」というふうな文言について、余りに厳格な解釈、運用がなされていたため、これを削除し、機動的な利用目的の変更を可能とするもの。

(2) 改正の内容

改正前	改正後
個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。	個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。

(3)補足

「相当の関連性」 → 「関連性」 と要件を緩和予定。なお、要件を満たさない変更の場合には、法第16条第1項の規定により、本人の同意を得なければならない。

2 利用目的の変更の制限の緩和（国会答弁）

(4)国会答弁

- 「今回の改正では、「相当」の部分、これを削除して、事業者が機動的に目的変更することを解釈、運用上、可能にするものでありますが、変更できる利用目的の範囲につきましては、本人が通常予期し得る限度内であるというふうなことを想定しております。」（衆議院内閣委員会　5月15日山口大臣答弁）
- 「例えば、電力会社が顧客に省エネを促す目的で家庭内の機器ごとの電気使用状況を収集し、その使用量を分析して顧客に提示しているような、そういうサービスがございますが、このような情報を用いて、例えば家電制御技術の研究開発やこの顧客の安否確認サービスを行うぐらいは許容範囲かなというふうに考えているところでございます。」

3　要配慮情報の規定の新設

(1) 趣旨

要配慮情報の保護

(2)改正の内容

- 要配慮情報とは、①本人の人種、②信条、③社会的身分、④病歴、⑤犯罪の経歴、⑥犯罪によって害を被った事実、⑦その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が 含まれる個人情報。
- 要配慮個人情報については、
  ①本人の同意を得ないで、原則として取得してはならない（新第17条第2項）。かつ、
  ②オプトアウトによる第三者提供ができない（新第23条2項括弧書き）。

(3)補足

金融庁の個人情報保護法ガイドラインにおける機微情報とは内容が異なる（次頁参照）。

3　要配慮情報の取得禁止と現行金融庁ガイドラインの比較

改正個人情報保護法	金融庁ガイドライン（現行）
要配慮情報 (1)本人の人種、(2)信条、(3)社会的身分、(4)病歴、(5)犯罪の経歴、(6)犯罪によって害を被った事実、(7)その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が 含まれる個人情報。	機微情報 「政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報」。
取得の原則的禁止。	取得、利用、第三者提供の原則的禁止。
あらかじめの本人の承諾があれば不適用（取得OK）。	あらかじめの本人の承諾があっても原則的に禁止。
「取得」の概念が広い。	「取得」の概念について解釈により限定。

3　要配慮情報と国会答弁

(4)国会答弁

- 「具体的に何が要配慮情報かというので、法律には、人種とか信条、社会的身分、病歴、犯罪の経歴等が書かれてございます。
- 人種は、人種、それから民族的もしくは種族的出身を広く意味するものでございまして、例えばアイヌ、在日韓国人等の情報が該当いたします。これに対しまして、単純な国籍は法的地位でございまして、人種には該当しないということでございます。
- 信条は、個人の基本的な物の見方、考え方を意味するもので、思想と信仰の双方を含むものと考えられます。
- 社会的身分は、例えば、いわゆる被差別部落出身であることや嫡出でない子であることなどがこれに当たり、単なる職業的地位は含まないと解されてございます。病歴とは、病気に罹患していた経歴を意味するものまたは特定の病歴を示した部分、特定の個人ががんに罹患している等でございますが、これらが該当するということでございます。
- 犯罪の経歴は、いわゆる前科、有罪の判決を受け、これが確定した事実が該当するというふうなことが考えられます。法律の列挙はこのようなことが書かれてございますが、政令におきましては、法律に列挙したものと同様の差別や偏見が生じるおそれがあるため、特に慎重な取り扱いを類型化することとしております。
- この対象につきましては、これまでの今国会における法律の審議において御指摘を受けた遺伝情報等を含めまして、政令の策定段階において検討していきたいというふうに思ってございます。ただ、法律上は性質が限定されておりますので、恣意的な拡大は行えないというふうな規定になっていると考えてございます。」（5月20日　衆議院内閣委員会　向井審議官 答弁）
- 「先生御指摘の具体的な例に即して考えますと、いろいろな状況はあろうかと思いますが、一般論を申し上げますと、足の不自由な人がいることにつきましては、それのみではいずれにも該当いたしませんが、特定の病歴と結びついた場合には病歴に該当するというふうに考えられます。ひとり暮らしであることについてはいずれにも該当いたしませんし、外国人の方で日本語が不自由であることにつきましては、単に外国人であること、外国籍であるというだけでは該当しません。ただ、特定の人種に関する情報と結びついた場合には該当すると考えられます。赤ちゃんがいることについてはいずれにも該当しないものと考えられます。」（5月20日　衆議院内閣委員会　向井審議官 答弁）

4　データ消去の努力義務（19条）

(1) 趣旨

個人情報の保護。

(2) 補足

- 個人情報取扱事業者は、**個人データの利用の必要がなくなったとき**は、当該個人データを遅滞なく消去するよう努めなければならない（新19条）。

(3) 補足

- 従来から利用する必要がなくなった場合は目的外利用である解釈されてきたが、消去するべき義務がより明確になった。但し努力義務。

4 データ消去の努力義務と国会答弁

(4)国会答弁

- 「利用する必要がなくなったとき」とは、個人情報取扱事業者が個人データを取り扱う際に特定した利用目的が達成され、その目的との関係では当該個人データを保有する合理的な理由が存在しなくなった場合、あるいは、特定した利用目的が達成されなかったものの、事業自体が中止になった場合などを指し、個人情報取扱事業者の取り扱い実態に即して客観的に判断されるものと考えております。
- これらの詳細な具体例は、個人情報保護委員会がガイドラインにおいて明確化することとしておりますが、不適切な取り扱いが行われる場合には、個人情報保護委員会が適切に監督、是正することになろうというふうに考えております。
- なお、本規定は、事業者のデータ管理のサイクル等、事業者の実務上の都合に配慮し、努力義務としているところでございます。

5 オプトアウト規定の見直し（23条2項）

(1)趣旨

オプトアウトの規制の実効化。

(2)改正の内容

・オプトアウトの場合に、現行法で、「本人への通知又は本人が容易に知りうる状態に置く」ことが必要となっているが、その際、「個人情報保護委員会の定める所」に従う必要があるものとすること。また、「本人の求めを受け付ける方法」が通知等の対象に追加される。

・オプトアウトの開始又は方法の変更の場合に個人情報保護委員会への届け出を必要とすること。（なお、届出事項は公表される。）

・要配慮個人情報についてオプトアウトが認められないことを明示。

(3)補足

施行前に23条2項に基づく通知等がなされている場合は、改正法にもとづく通知等がなされたものとみなす旨の経過措置規定がある（附則5条）。

5 オプトアウト規定の見直し（23条2項）

金融庁ガイドライン（現行）

現行金融庁ガイドラインでは、以下の記載があることから、クレジットカード会社等は、オプトアウトを、あまり活用していないのではないかと思われ、影響は大きくないのではないかとも思われる。

「金融分野における個人情報取扱事業者が、与信事業に際して、個人情報を取得する場合においては、利用目的について本人の同意を得ることとし、契約書等における利用目的は他の契約条項等と明確に分離して記載することとする。」

「金融分野における個人情報取扱事業者は、法第16条及び法第23条に定める本人の同意を得る場合には、原則として、書面（電子的方式、磁気的方式、その他人の知覚によっては認識することのできない方式で作られる記録を含む。以下同じ。）によることとする。」

6 外国にある第三者への提供の制限（24条）

（1）趣旨

法制定時と比べ、我が国の企業活動のグローバル化や情報通信技術の普及に伴い、個人情報の海外とのやりとりが増加をしていることを踏まえ、今回の法改正において、外国の第三者に対して個人情報を提供する場合のルールを整備することとしたもの。

（2）改正の内容

個人情報取扱事業者は、外国にある第三者に個人データを提供する場合には、原則として、本人に同意を得なければならない。ただし、日本と同等性が認められる国にある事業者や、一定の基準に適合する体制を整備している第三者への提供については、この限りでない。

（3）補足

・海外の会社に、業務委託する場合にも、原則として、本人の承諾が必要（24条では、23条1項各号の場合は適用されないことが明記されているが、23条4項各号の場合[委託・共同利用等]に適用がないことは、言っていない。）。

・加盟店が、国際ブランドその他の海外のカード関連の会社にカード情報を含むカード決済に必要な個人情報を渡すことは許されるのか？黙示的同意といってしまい、解釈で乗り越えるか？

7　個人データの第三者提供時の確認・記録義務（25条）

（1）趣旨

トレーサビリティーの確保の観点から、第三者提供に係る記録の作成等や第三者提供を受ける際の確認等を個人情報取扱事業者の義務として新たに導入することとするもの。

（2）改正の内容

個人データの提供者は、提供年月日や受領者の氏名その他の個人情報保護委員会規則で定める事項に関する記録を作成し、所定期間保存しなければなりません。ただし、23条1項各号の場合（法令に基づく場合等）及び23条5項各号の場合（委託・合併等による承継・共同利用）は、この限りでありません。

（3）補足

負担が重いとの批判が強く、簡略化した記録の方法等について、個人情報保護員会規則で手当てされることが予想される。

8　個人データの第三者提供受領時の確認・記録義務（26条）

（1）趣旨

トレーサビリティーの確保の観点から、第三者提供に係る記録の作成等や第三者提供を受ける際の確認等を個人情報取扱事業者の義務として新たに導入することとするもの。

（2）改正の内容

個人情報取扱事業者は、第三者から、個人データの提供を受けるに際しては、個人情報保護委員会規則で定める所により一定の事項（①当該第三者の氏名、住所等、②当該第三者による当該個人データの取得の経緯）の確認を行う義務を負う。ただし、法23条1項各号（法令に基づく場合等）、5項各号（委託、合併、共同利用）に該当する場合はこの限りでない。また、個人情報保護委員会規則で定める所により、①提供を受けた年月日、当該確認事項等についての記録を作成し、保管しなければならない。

（3）補足

企業の担当者が、Facebookで個人に該当する情報を閲覧した場合にも、確認義務、記録義務がかかってしまい、そのようなデータベースに入れるまでも ない、散在情報についてまで規制するのはToo Muchという批判が強い所。

また、個人データの取得の経緯まで確認しなければならないというのは、負担として重過ぎるとの批判が強い所。これらの対応のため、各社とも、個人情報の取得源については、洗い出し、提供元が適切に個人情報を取得しているか等を確認する必要がある。

9　開示請求権等の明示（28条、29条、30条等）

（1）趣旨

欧州個人情報保護法令との関係での同等性の認証の関係もあり、本人が開示請求権等を有していることを正面から明記。

（2）改正の内容

・本人（＝個人）が、個人情報取扱事業者に対し、自己を識別できる保有個人データにつき、開示請求権（28条）、内容訂正権（29条）、利用停止請求権（30条）を有することを明示。

・かかる開示請求権等に基づき、訴えを提起する場合、あらかじめ、当該請求を行い、かつ、その到達した日から2週間を経過した後でなければ、その訴えを提起することができないものと規定（34条1項）。

（3）影響

訴訟が増えるものと思慮されます。

10　匿名加工情報に係る規定の新設（36条から39条）

(1)趣旨

一定条件の下で本人の同意なく自由な情報の流通、利活用を認めて、データの利活用を促進することを目的として、匿名加工情報についての規定を新設。

すなわち、個人情報を法令上の要件に従って匿名加工化し、公表する場合に、個人情報に該当しないこととなり、(1)匿名加工情報を自由に第三者に提供することが可能となり（＊）、かつ（2）その匿名加工情報を、社内でも、その作成に用いられた個人情報の利用目的の範囲外の目的にも利用可能になると解される。

＊　現行法下で、例えば、Suiceの件（JR東日本が日立製作所に分析用のSuica利用履歴データ[氏名・住所を削除済み・SuicaIDを別の符号に変換済み]を提供し、炎上。プロジェクトが中止。）など、個人に関連する利用データを匿名化し、本人の同意なく他社に対して提供するケースで、匿名化が不十分で、違法と批判され、炎上するケースも生じている。

匿名加工情報取扱事業者の義務

(2)改正の内容

(i)　作成作業時　匿名化(＆復元不能化)のため、個人情報保護委員会規則で定める基準に従う義務(新36条1項)。

(ii)　作成完了時　個人情報保護委員会規則に従い、匿名加工情報に含まれる個人に関する情報の項目を公表する義務。また、匿名化の方法・匿名化の際に削除した項目等にかかる情報が漏洩しないような安全管理措置義務(新36条2項・3項)。

(iii) 第三者提供時　個人情報保護委員会規則で定めるところにより、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供方法について公表するとともに、当該第三者に対して、提供する情報が匿名加工情報である旨を明示する義務(新36条4項)。

(iv) 匿名加工情報取扱時　本人を識別するために、当該匿名加工情報を他の情報と照合してはならない義務(新36条5項)。

＊匿名加工情報を受領した者にも、(iii)・(iv)と類似の規制(新37条・38条)。

匿名加工情報についての懸念

(3) 補足

以下のような懸念が示されている。

(i)　匿名加工情報の定義が曖昧すぎる。

(ii)　例えば、セキュリティの観点から、氏名、住所等を削除したデータベースを作成し、これを社内の業務（又は委託先による委託業務）の実施のために利用した場合に、匿名加工情報に関する規制がかかるとすれば、不当。

すなわち、そのようなケースで、匿名化データの作成の際の基準が、個人情報委員会の基準に合致していなければならず、かつ、公表をしなければならないというのは、現実的でない。

参考：　高木浩光 「個人情報保護法改正案の問題点」

https://staff.aist.go.jp/takagi.hiromitsu/paper/spsc-201505-aist.pdf

匿名加工情報に関する国会答弁

(4) 国会答弁

(i) 趣旨について

「一定条件の下で本人の同意なく自由な情報の流通、利活用を認めて、データの利活用が促進をされるということを実は期待をしておるところ」(5/28参議院内閣委員会山口大臣答弁)

(ii) 個人情報との関係について

「匿名加工情報は個人情報に該当いたしません」(5/28参議院内閣委員会向井政府参考人答弁)

(iii)匿名加工情報の作成の意図なく、匿名化を行う場合について

「…事業者が安全上の観点などなどから全く別の目的で加工化した、仮名化した、それは法律で言う匿名加工情報には当たらないということでよろしいんですね。」「委員ご指摘の形式的に匿名化を施したというふうなもの、加工を施したという場合にまで匿名加工情報としての取扱いを求めるものではありません。」(5/28参議院内閣委員会での石橋委員の質問に対しての向井政府参考人答弁)

11　認定個人情報保護団体の定める個人情報保護指針（53条）

（1）趣旨

海外の動向等も踏まえ、条文が微修正されている。

（2）改正の内容

・個人情報保護指針についてのマルチステークホルダープロセスの導入　（＝消費者の意見を代表する者その他の関係者の意見を聴いて作成するよう努めなければならないものと明示。）

・個人情報保護指針の対象事項の追加　（＝匿名加工情報に係る作成の方法等を追加）

・認定個人情報保護団体は、個人情報保護指針を作成・変更したときは、個人情報保護委員会への届出義務を負い、個人情報保護委員会はこれを公表しなければならない。

・公表後、認定個人情報保護団体は、対象事業者に対し、個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとらなければならない。（改正前は、努力義務であったものが、法的義務に。）

12　個人情報保護委員会の新設（59条）

（1）趣旨

プライバシーコミッショナー会議等の国際的会議に日本からも正式に参加できるようにすること。省庁横断での監督を可能とすること。

（2）改正の内容

・個人情報保護員会は、委員長及び委員8名により組織（54条）。

・特定個人情報保護委員会の機能は、新設される個人情報保護委員会に移る。

・各省庁が個人情報保護法を所管していたものを、個人情報保護委員会で一括して所管し、同委員会が規則を制定。

13　データベース提供罪の新設（83条）

（1）趣旨

- 「本罪は、昨年発覚いたしました個人情報の大量漏えい事件を受けまして、個人情報の取り扱いに関する業務に従事していた者がその立場を悪用して個人情報データベース等を不正に持ち出し、第三者に提供して利益を図る行為を個人情報保護法違反として処罰することができるよう新設するもの。」
- ベネッセ事件等における名簿屋を通じた情報漏えいが念頭に。

（2）改正の内容

個人情報取扱事業者（又はその従業者・元従業者）が、その業務に関して取り扱った個人情報データベース等を、自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、1年以下の懲役又は50万円以下の罰金とする（新法83条）。

14 小規模事業者への対応

(1)趣旨

個人情報の漏えいの防止のため、また、EUにおける同等性認定との関係で指摘があったこと等からその対応のため、小規模取扱事業者についての適用除外規定を削除するもの。

(2) 改正の内容

取り扱う個人情報が**5000人以下の小規模取扱事業者についての適用除外を削除**する。これにより、従来適用除外となっていた小規模の事業者も、個人情報保護法に対応する必要が生じる。

(3) 補足

個人の利益保護の観点から保護の必要性が低いと認められるもの(ex. 電話帳等)については、政令で、個人の権利利益を害するおそれが少ないものとして「個人情報データベース等」の範囲から除外。

改正法施行日

- 衆院可決 ⇒ マイナンバー法において年金への利用を認めなくするためにマイナンバー法案の**一部を修正し、平成27年8月28日に参院可決。**一方、個人情報保護法は修正なし。⇒　9月初旬に衆院で一体として再可決予定。
- 施行日

(1) 第1条施行

個人情報保護委員会の設置　　施行日は平成28年1月1日

(2) 第2条施行

情報保護法改正の中核部分

施行日は公布の日から2年以内の政令で定める日。

※　オプトアウトに係る消費者委員会規則に基づく届出は、施行日前であっても、消費者委員会規則制定後であれば、可能。

(3) 第3条施行

条文番号の変更に伴う技術的変更。

施行日はマイナンバー法の公布日（2013年5月31日）から4年以内の政令で定める日。

今後の業務にお役立ていただければ幸いです。

（お問い合わせ先）
山下・柘・二村法律事務所
弁護士　中崎　隆
r-nakazaki@ytn.itplugin.net