2019年度　東京都
個人情報保護制度説明会

個人情報保護法の概要

2019年9月27日

JIPDEC（（一財）日本情報経済社会推進協会）
電子情報利活用研究部　郡司　哲也
gunji-tetsuya@jipdec.or.jp
（JIPDEC法人番号：1 0104 0500 9403）

本講義の概要

■ 概要

- 個人情報保護とプライバシー
- 個人情報保護法（2017年改正）のポイント
- 個人情報保護法（2017年改正）の対応ポイント

■ 到達目標

- 個人情報保護法の概要について理解できる
- 個人情報保護の対策ポイントについて理解できる

■ キーワード

- 個人情報保護、プライバシー、個人情報保護法

■ 受講推奨対象

- 一般職員、管理職、IT開発

アジェンダ

0．イントロダクション

1．個人情報保護とプライバシー

2．改正個人情報保護法のポイント

3．参考：FAQ

研修の前に：

イントロダクション

研修のねらい（ポイント）

- プライバシーは保護するのではなく尊重するもの
  - プライバシーは「権利」であると考えられており、「モノ」ではない
  - 個人情報保護（法）は、モノとして定義できる個人情報を保護することで、プライバシーという権利を尊重することを目的としている
- 法律の定義と社会的認知のギャップ
  - 法律による定義は、拠り所となる判断基準（ものさし）を設けるためのもの
  - 社会的認知は、法律の定義と必ずしもレベルが同一ではない
- 実務での例（一般論）
  - 具体的に、どんなことをしなければいけないか？
  - お客様の信頼を得るためには？
- 法律を読むことや、規格を理解することは非常に面倒であり、とっつきにくいことは確かですが、

  「ルールを守ること＝日常生活で他人に信用されること」

  と置き換えて考えると、意外と腑に落ちることも多いと思います。
- 個人情報保護が特別なことではなく、人に嫌われないためのあたりまえの行為であるということを理解していただければ幸いです。

「プライバシー」ってなんだろう？

■ 「プライバシーを侵害された！」と感じるときは、どんなとき？

- 例：
  - 全く知らない会社からDMが来た / わけのわからない会社から勧誘の電話が来た
  - 友人が、一緒に遊びに行ったときに撮った写真を、位置情報つきでSNSに投稿していた
  - etc…

■ 個人情報の取扱いで不便に感じることは、どんなとき？

- 例：
  - 子供のクラスの緊急連絡網が配られなくなった
  - セミナーやイベントで作成した連絡先リストを、終了後にどう扱うべきか悩ましい
  - etc…

皆さんの感覚や実体験は？

Part1：

個人情報保護とプライバシー

個人情報保護が強く求められるようになった背景

■ 情報（アナログ）からデータ（ディジタル）へ
- コピーすることができる
- 簡単に渡すことができる

■ ネットワークへの接続
- インターネットの発展
- パーソナルから共有へ

■ デバイスの高度化
- PCからスマートフォンへ
- IoT：Internet of Things

■ サービスの高度化・多様化
- EC：Electronic Commerce、電子決済、インターネット銀行
- SNS：Social Networking Service
- シェアリング・エコノミー、オンライン完結社会の実現

情報が電子化され、コンピュータがネットワークにつながることでデータのコピーや流通が容易になり、デバイスの高度化によりそれが加速し、流通するデータの種類が増えることで、様々なサービスが生まれた。

アナログ時代には暗黙の了解によって当事者同士でしか扱われることがなかった個人情報が容易にコピー・流通することができるようになったことで、それらを保護する必要性が生じてきた。

個人情報保護法制の歴史

■ 1980：OECDプライバシー8原則

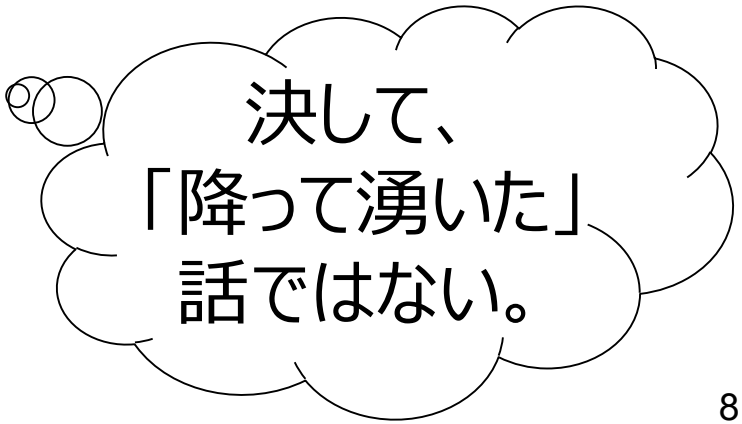
- プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告
  （Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data）
- 2013年：更新版が勧告

■ 1995：EUデータ保護指令 ⇒ 2018：一般データ保護規則

- 個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令（Directive 95/46/）
- 2016年、より影響力の強い「規則（Regulation）」として欧州委員会で可決
  （一般データ保護規則（GDPR：General Data Protection Regulation））
- 2018年5月25日：GDPR施行

■ 2003：個人情報保護法制定

- 2005年4月1日：個人情報保護法施行
- 2017年5月30日：改正個人情報保護法施行



OECDプライバシー8原則 ← すべての原点

1. 収集制限の原則（Collection Limitation Principle）
   - 個人データを収集する際には、法律にのっとり、また公正な手段によって、個人データの主体（本人）に通知または同意を得て収集するべきである。
2. データ内容の原則（Data Quality Principle）
   - 個人データの内容は、利用の目的に沿ったものであり、かつ正確、完全、最新であるべきである。
3. 目的明確化の原則（Purpose Specification Principle）
   - 個人データを収集する目的を明確にし、データを利用する際は収集したときの目的に合致しているべきである。
4. 利用制限の原則（Use Limitation Principle）
   - 個人データの主体（本人）の同意がある場合、もしくは法律の規定がある場合を除いては、収集したデータをその目的以外のために利用してはならない。
5. 安全保護措置の原則（Security Safeguards Principle）
   - 合理的な安全保護の措置によって、紛失や破壊、使用、改ざん、漏えいなどから保護すべきである。
6. 公開の原則（Openness Principle）
   - 個人データの収集を実施する方針などを公開し、データの存在やその利用目的、管理者などを明確に示すべきである。
7. 個人参加の原則（Individual Participation Principle）
   - 個人データの主体が、自分に関するデータの所在やその内容を確認できるとともに、異議を申し立てることを保証すべきである。
8. 責任の原則（Accountability Principle）
   - 個人データの管理者は、これらの諸原則を実施する上での責任を有するべきである。

自問自答：なぜ、個人情報を「保護」するのか

JIPDEC

【当協会での整理】

■ 視点１：法遵守（責務：最低ライン）

- 個人情報保護法＝組織が国内で活動を行う場合に、個人情報を取扱う際のルール（何をして良く、何をしてはいけないかの定義）を定めたもの。
- 個人情報保護法の遵守は、自動車が道路の右側を走行しないこと（道路交通法の遵守）と同様に、個人情報を取り扱う組織にとって明白な責務である。

■ 視点２：社会的信用（社会的認知）

- 法を遵守してさえいれば、何をしても許されるか？　・・・否。
- 組織が活動するためには、周りから認められる必要があり、それは法遵守の事実だけでは担保されない。

■ 視点３：プライバシーの尊重（目的：求められていること）

- 個人の私生活に関する事柄やそれが他から隠されており干渉されない状態を要求する権利、を尊重すること。
- 顧客や相手が「これをされたら嫌だ」と感じるようなことをしないこと。

個人情報保護は目的ではなく手段である

第１章　総則

（目的）

第１条　この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、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つつ、個人の権利利益を保護することを目的とする。

わかりにくいので、分解。

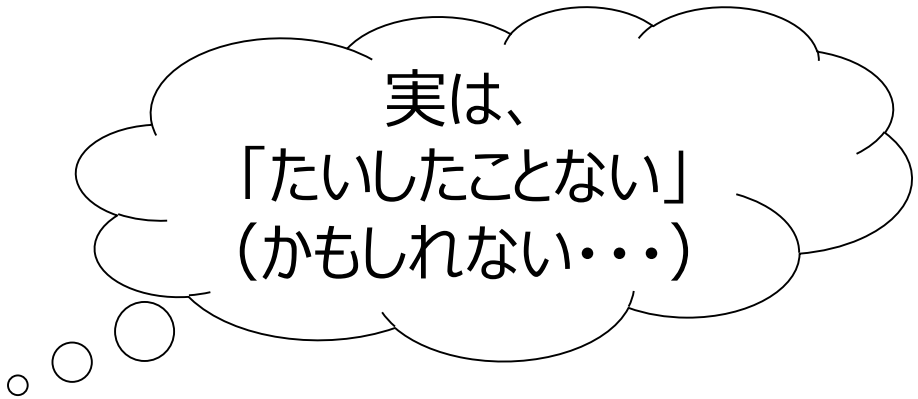
- 個人情報の適正な取扱いに関し、
  - 基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、
  - 国及び地方公共団体の責務等を明らかにするとともに、
  - 個人情報を取り扱う事業者の遵守すべき　義務等を定めることにより、
- 個人情報の適正かつ効果的な活用が
  - 新たな産業の創出　並びに
  - 活力ある経済社会　及び
  - 豊かな国民生活の実現に資するものであることその他の　個人情報の有用性に配慮　しつつ、
- 個人の権利利益を保護すること　を目的とする。

忘れがちな視点

- 個人の権利利益を保護するための「手段の一つ」が個人情報の保護であり、全てではないことに注意。（1:1 のイコールにはならない）
- 個人情報を保護し、適切に取り扱うことは、プライバシーを尊重すること（個人の権利利益を保護すること）につながる。
  （個人情報の保護は、個人の権利利益を保護する手段として有効である）

個人情報保護
＝　個人の権利利益の保護

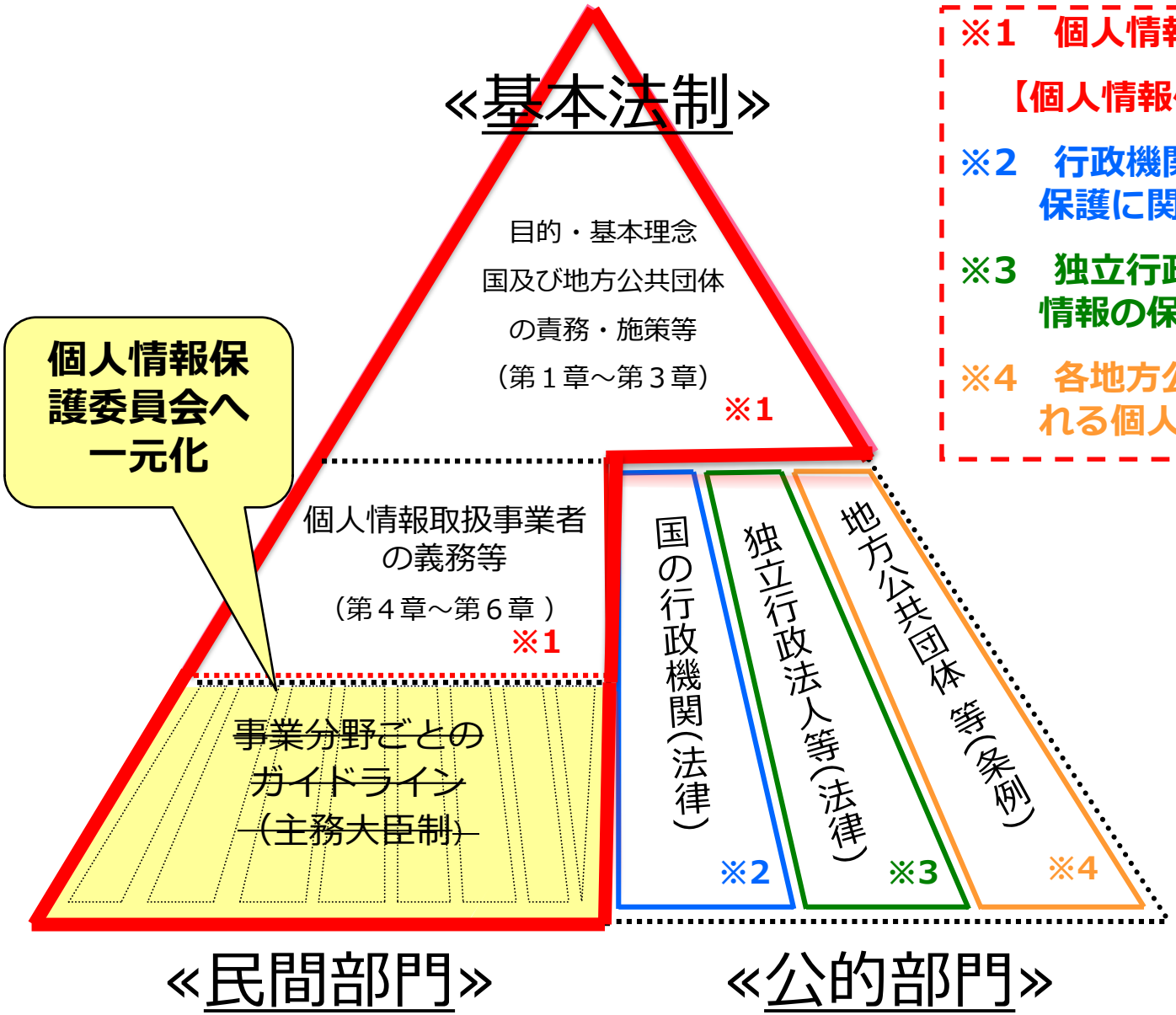
個人情報保護
∈　個人の権利利益の保護



Part2：

改正個人情報保護法のポイント

個人情報保護に関する各種ルールの位置づけ



※1　個人情報の保護に関する法律
【個人情報保護委員会】

※2　行政機関の保有する個人情報の保護に関する法律

※3　独立行政法人等の保有する個人情報の保護に関する法律

※4　各地方公共団体において制定される個人情報保護条例

個人情報 / 個人データ / 保有個人データ の各々の義務

①個人情報

生存する個人に関する情報であって、
- 一定の記述等により特定の個人を識別できるもの

OR

- 個人識別符号が含まれるもの

②個人データ

①のうち、
個人情報データベース等（個人を検索可能な状態）を構成しているもの

③保有個人データ

②のうち、6か月を超えて継続利用し、
開示、訂正、消去等の権限を有するもの

取り扱う対象

対応する条文

第15条　利用目的の特定
第16条　利用目的による制限
第17条　適正な取得
第18条　取得に際しての利用目的の通知等
第35条　苦情の処理

第19条　データ内容の正確性の確保
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
第23条　第三者提供の制限
第24条 外国にある第三者への提供の制限
第25・26条　第三者提供時の確認・記録義務

第27条　保有個人データに関する事項の公表等
第28条　開示の請求
第29条　訂正等
第30条　利用停止等
第31条　理由の説明
第32条　開示等の請求等に応じる手続
第33条　手数料
第34条　事前の請求

全般：事業者として気をつけるべき内容

JIPDEC

- ✓ 事業者として特に気をつけるべき内容は、第4章 第1節（第15条～第35条）に書かれています。
- ✓ 第4章 第1節の内容を理解することは、適切な個人情報の取り扱いを行うためには必須です。

第15条（利用目的の特定）
第16条（利用目的による制限）
第17条（適正な取得）
第18条（取得に際しての利用目的の通知等）

- ✓ 主に、個人情報の「利用目的」と「取得」に関することが定められている。
- ✓ OECD 8原則 の「収集制限の原則」「目的明確化の原則」「利用制限の原則」などが該当。

第19条（データ内容の正確性の確保等）

- ✓ 主に、収集した個人情報は常に最新、正確でなければならない、という内容が定められている。
- ✓ OECD 8原則 の「データ内容の原則」などが該当。

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）

- ✓ 主に、収集した個人情報の取り扱いや管理について、セキュリティ的な観点からの留意事項が定められている。
- ✓ また、組織内における個人情報の取り扱いに関する監督・教育や、委託先の監督責任等についても書かれている。
- ✓ OECD 8原則 の「安全保護措置の原則」「責任の原則」などが該当。

第23条（第三者提供の制限）
第24条（外国にある第三者への提供の制限）
第25条（第三者提供に係る記録の作成等）
第26条（第三者提供を受ける際の確認等）

- ✓ 主に、個人情報の「第三者提供」（個人から直接個人情報を取得した組織以外の第三者へ個人情報を提供する行為）に関することが定められている。
- ✓ OECD 8原則 の「利用制限の原則」「安全保護措置の原則」「責任の原則」などが該当。

第27条（保有個人データに関する事項の公表等）
第28条（開示）
第29条（訂正等）
第30条（利用停止等）
第31条（理由の説明）
第32条（開示等の請求等に応じる手続）
第33条（手数料）
第34条（事前の請求）

- ✓ 主に、個人情報の提供元である個人からの求めに応じ、収集した個人情報の各種取り扱い（公開、訂正、利用停止等）に関することが定められている。
- ✓ OECD 8原則「公開の原則」「個人参加の原則」「責任の原則」などが該当。

第35条（個人情報取扱事業者による苦情の処理）

- ✓ 主に、個人情報の提供元である個人からの苦情処理に関することが定められている。
- ✓ OECD 8原則「責任の原則」などが該当。

改正法におけるポイント（１）

ほぼ全ての事業者が個人情報保護法を遵守しなくてはならない。

【解説】

□ 小規模事業者の適用除外が撤廃。

- 平成29年5月29日以前の個人情報保護法では適用対象外だった

『データベース内の個人情報で識別される個人の数が過去6ヵ月間のいずれの日でも5,000を超えない事業者』

という**除外規定が撤廃された**ため、個人情報の取扱いの件数を問わず、個人情報保護法の規制の対象が広がった。

□ ポイント

- 従業員の個人情報も、個人情報保護法に準じた取扱いを求められる。
- 具体的には・・・
  - **利用目的の整理・特定と伝達手段の選定**などの規定の整備
  - **安全管理措置の実施**など

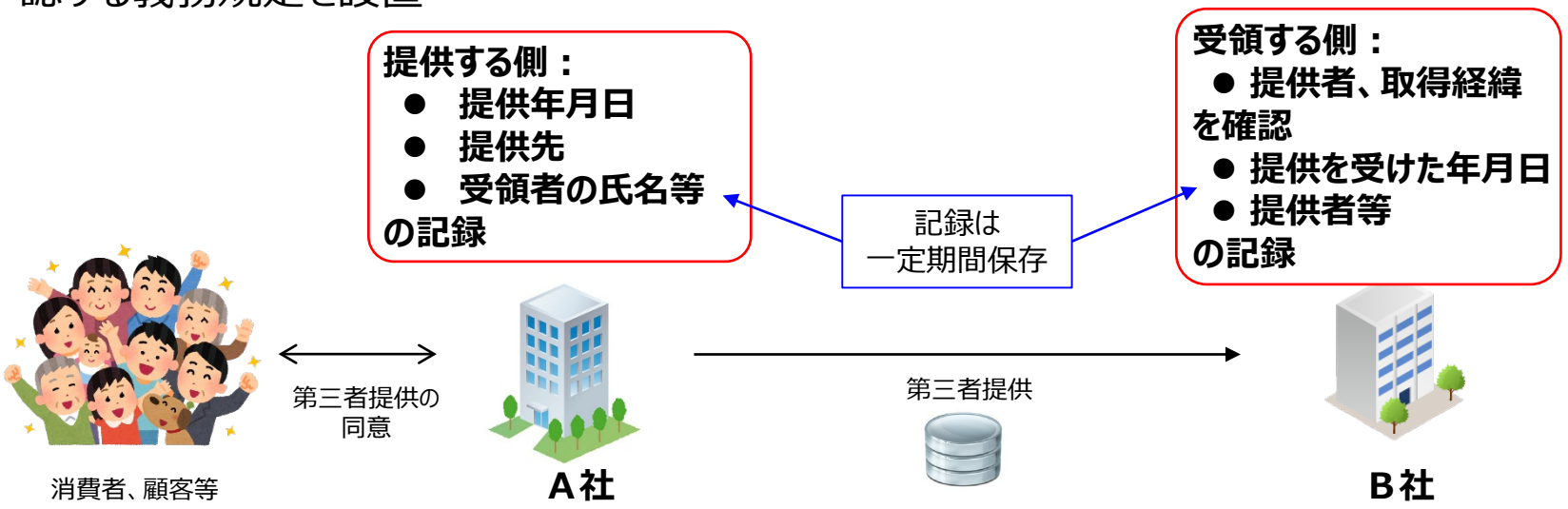
※ただし、これらの具体的対策は従来の個人情報保護法と同じ。

改正法におけるポイント（２）

個人データの第三者提供に係る確認及び記録の作成が義務付けられた

【解説】

- 平成26年の大量漏洩事件において、名簿屋が介在し、違法な個人データの取引が行われていたことが明らかになったことが契機。
- 個人情報取扱事業者が第三者から個人データの提供を受ける場合には、**違法に入手された個人データが流通することを抑止するため**、当該第三者が当該個人データを取得した経緯等を確認する義務規定を設置



- ポイント
  - 取引先や顧客から取得した個人情報の第三者提供を行う際は、あらかじめ第三者提供を行うことに対する同意を得る。
  - 第三者提供を行う際には、提供側・受領する側双方において記録をつける。
  - 提供する立場だけでなく、受領する立場の場合も気をつける必要がある。

【補足】改正法におけるポイント（２）

個人情報保護法における　第三者提供　と　委託　の考え方の整理

□ 第三者提供

- 法律上の「第三者提供」とは、**自社が保有する個人情報を第三者に渡し、受け取った第三者は、その個人情報を（利用目的の範囲内で）自由に使える状態にある場合**を指す。

注意点：

- ✓ 第三者提供を行う際は、個人情報の取得元（＝個人）に対して、あらかじめ**「第三者提供を行うこと」について、同意を得ておく必要がある**。
  （個人情報の取得時には第三者提供を予定していなかったが、取得後に第三者提供を行うことになった場合は、第三者提供を行うことに対して同意を取り直し、同意が得られた個人の個人情報のみ、第三者提供を行うことができる）
- ✓ 第三者提供を受けた側も、個人情報の取得時に**同意を得た利用目的の範囲内**でしか、個人情報を取り扱うことはできない。

□ 委託

- 法律上の「委託」とは、**自社の業務の一部を第三者に代行してもらうために、自社が保有する個人情報を提供する場合**を指す。

注意点：

- ✓ 第三者提供ではないため、個人情報保護法の提供側と受領側に対する**「記録義務」は発生しない**。
- ✓ ただし、委託元（個人情報の提供側）は、委託先（個人情報を受領し、業務の一部を代行する側）の**「監督責任」が生じる**。 具体的には・・・
  - 委託先が個人情報保護法を遵守しており、適切に個人情報を取り扱う能力があるかどうか（安全管理措置が実施できるかどうか）の判断
  - 委託元と委託先の間で、しっかりとした委託契約を締結し、責任分界点の設定や業務終了後のデータの破棄等についても取り決めを行う必要がある
  - 第三者提供のような記録義務は生じないが、委託先の監督のためには積極的に自らが記録をつける等の対応は必須

改正法におけるポイント（３）

オプトアウトを実施する事業者は、個人情報保護委員会への届出を行い、委員会から公表されない限り、実施できない

◘ オプトアウトとは・・・

- ➢ 第三者提供を実施することについて、本人からの「同意」ではなく、
- ➢ 本人への「通知」もしくは「本人が用意に知り得る状態」におくことで第三者提供を行うが、
- ➢ 本人から『私の個人データは第三者提供しないでくれ』という申し出に基づき、第三者提供を停止する

仕組みのこと。

◘ 個人情報保護委員会へ届け出る内容

- ✓ 第三者提供すること
- ✓ 個人データの項目
- ✓ 提供の手段又は方法
- ✓ 求めに応じた提供停止
- ✓ 本人の求めを受け付ける方法

詳細 ⇒ https://www.ppc.go.jp/personal/legal/optout/ （個人情報保護委員会）

改正法におけるポイント（４）

■ 利用目的制限の緩和

➢ 「相当の」が削除された。

- 「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。」（従来）

（例）

エアコンの購入時に、ＤＭの送付など広告目的での利用を明示して取得した個人情報を利用し、アフターサービスやクリーニングサービスの案内の送付を行うこと。

□ ポイント

✓ 改正前の「相当の関連性」とはどの程度の関連性までなのか？という課題があったが、個人情報の持ち主である個人が納得できるレベルで、利用目的に関連する用途での利用を行っても良いということになった。

✓ 気をつけるべき点は、個人情報の持ち主である個人が、「その用途であれば当初の利用目的と関連しているだろう」と納得できるかどうか、という点。

✓ 法律上許可されている範囲と、個人情報の持ち主である本人の認識する範囲はそもそもイコールではないという点に注意。

改正法におけるポイント（５）

■ 要配慮個人情報の取得制限

- 差別の要因となる個人情報の取得は**同意の下に取得**
  - 本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実
  - 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

□ ポイント

- ✓ 要配慮個人情報とは、個人情報のうち、差別や偏見につながる可能性を持つ情報のこと。
- ✓ 取得をしてはならない、のではなく、取得・取扱いの際には、明確な同意のもとで取得し、取扱いにはより一層の気遣いが必要な情報として特出しされたもの。
- ✓ 他の個人情報と同じく、利用目的が明確であり、その情報を取得しなければ事業ができない、当初の目的を達成できない、という場合は取得する必要があるが、「この情報は取得しておいたほうが良いかもしれない」レベルでの取得はすべきではない。

改正法におけるポイント（６）

■ 消去の努力義務

- 個人データを利用する必要がなくなったとき　→　遅滞なく消去

□ ポイント

- ✓ 個人情報を保持し続けることは漏洩のリスクや管理コストが継続することになるため、「当初の目的を達成したあとは、不必要に個人情報を保持しない」ということは徹底したほうが良い。

改正法におけるポイント（７）～その他の改正ポイント～

JIPDEC

■ 開示等請求権

- 開示、訂正等、利用停止等の請求を裁判上の権利として明記

✓ 改正以前より、個人からの情報の開示請求等に関する対応は義務付けられていたが、個人の権利として明記

■ 個人情報保護委員会の設置

- **監督権限の統一・明確化／立入検査も含む執行権限の強化**

✓ 改正前よりも権限が明確化され、国内における個人情報保護の監督機関としての位置づけが明確に

■ グローバル化への対応

- 国境を越えた個人情報の取扱いにも法執行
- 外国執行当局への情報提供
- 個人データの外国にある第三者への提供の制限

✓ グローバル・ビジネスは大企業だけのものではなくなり、海外との個人情報の移転（国境を超えた個人情報のやりとり）も一般的になりつつあることへの対応

まとめ（具体的なアドバイス）

- とはいっても、法律は「わかりにくい」。
  - 要は、「個人情報は個人の持ち物」であるという大前提をよく理解し、「お借りしたものは適切に取扱います」ということを徹底すれば良い。
- 個人情報の取得
  - 利用目的をしっかりと説明し、本人の同意を得る。
    （ポイントは、個人情報の持ち主に利用目的をきちんと理解してもらうこと）
- 個人情報の利用
  - 取得した個人情報は、当初の利用目的の範囲内で利用する。
    （逆に言えば、利用目的の範囲内であれば利用することを怖がる必要はない）
- 個人情報の管理
  - 漏洩などのリスクをしっかりと理解し、必要な対策を講じる。
    （完全なセキュリティなどは存在しないので、「ここまでやってます」ということを宣言できるようにしておくことが重要）
  - 必要がなくなったら（利用目的を達成したら）、削除する。
    （個人情報を保有し続けることは、漏洩などのリスクを抱え続けることと同じ）
- 個人情報の第三者提供
  - 第三者提供は、あらかじめ必要と想定される場合のみ有効と考えておいたほうが良い。
    （事前同意が必要になるので、個人情報の取得時に第三者提供を行う旨を説明しておく必要がある。）

Break: それは、「やらなきゃいけないこと」か？

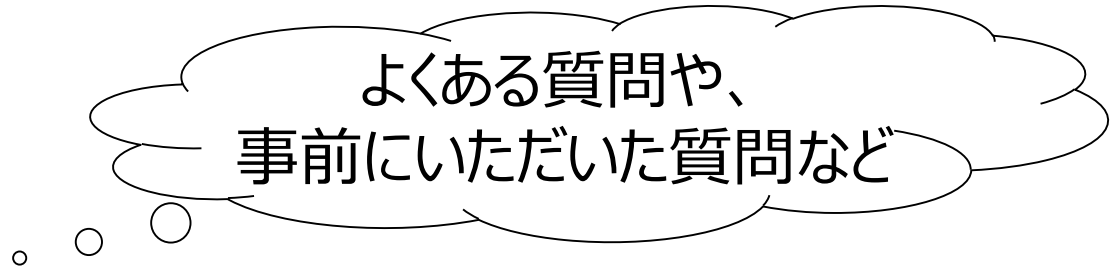
- 個人情報は、個人情報保護法によって「適切な管理」を要求される情報

- 必ず管理する必要があると思われる個人情報とは？
  - 社員の個人情報（給与の支払い等で取り扱わない訳にはいかない）
  - 取引先や顧客の個人情報（B2Bの場合と、B2Cの場合がある）

  - これらは、業務上必要になる情報なので、適切に管理するのは当たり前
  - 「業務上必要な情報」には、個人情報以外の情報もたくさんある
  - 「業務上必要な情報」は、法律があろうがなかろうが、適切な管理をしているはず
  - 個人情報だけが特別なのではなく、すべてが「業務上必要な管理すべき対象」という意識を持つということも重要では？

  - また、
    - ✓ 必要ではない個人情報は取得しない・取り扱わない
    - ✓ やむをえず個人情報を取り扱う場合は、使ったらすぐに消去してしまう

    など、個人情報を取り扱うリスクそのものを減らすアプローチも、有効なのでは？



Part3：

参考：FAQ

Q そもそも、何が個人情報なのか知りたい。

A

- ✓ 個人情報保護法では、「これは個人情報だが、これは個人情報ではない」という定義が（一応）されている。
- ✓ しかし、個人情報のもともとの持ち主である個人の感覚で言えば、自分に関係する情報のほとんどは個人情報だと考えている人が多い。
- ✓ 海外の個人情報保護のルールなどでも、個人情報は「個人に関連するすべて」と定義していることが多い。
- ✓ ビジネス上で「これは個人情報なのか？そうでないのか？」と悩むよりも、区別がつかないものについては個人情報として大切に取り扱うべき。
- ✓ 「業務上知り得た情報」、つまり契約内容であったり、企業秘密に近いような情報は当然慎重に扱うはずであり、個人情報も「業務上知り得た情報」であるという認識で捉えたほうが良いのでは？

Q 個人情報保護法の次期改正についての状況は？

A 2020年には改正法が公布されると言われており、現在法改正のための検討が行われている最中。

- ✓ 2020年には改正法が公布されると言われており、早ければ2019年のうちに改正案が公開されるのでは、と言われている。
- ✓ 2019年4月25日～5月27日まで、個人情報保護委員会のWebサイト上で
  「個人情報保護法 いわゆる３年ごと見直しに係る検討の中間整理」の公表
  及び同整理に対する意見募集
  を実施。（ https://www.ppc.go.jp/news/press/2019/20190425/ ）
- ✓ 現時点では、大きなポイントとして以下のような内容が検討されている模様
  （※すべてが改正法に反映されるわけではない点に注意！）
  - いわゆる「利用停止権」に関する事項の追加
  - 匿名加工情報とは異なる「仮名化」
  - ペナルティの強化
- ✓ 検討状況については、個人情報保護委員会のWebサイトにて、逐次情報が更新中。
  （ https://www.ppc.go.jp/enforcement/minutes/2019/ ）

Q&A

Q 従業員の時間外労働時間や有給休暇取得状況は個人情報になるのか？
SNSなどで使用しているハンドルネームは個人情報に入るのか？

A それ単体では個人情報にならなくても、他の情報と組み合わせた時に個人を識別できるか？ということに注意すべき。

【解釈】

- ✓「時間外労働時間」「有給休暇取得状況」「ハンドルネーム」 いずれも、単体では個人情報ではないと考えられる。
- ✓ ただし、「他の情報を組み合わせた時に、容易に個人が特定できる」状況になったときは、個人情報として取り扱うべきだと考えられる。

【対応の例】

- ✓ 個人を特定できる使い方を想定するのであれば、個人情報と同等の安全管理措置のもとで取り扱う社内ルールを作り、それを運用する。
- ✓ 個人を特定しない運用を前提とするのであれば、「他の情報と組み合わせて個人が特定できてしまうリスクを限りなく減らす」運用を徹底する。

Q&A

Q 本社にてグループ企業の個人情報を取り扱う場合の必要対応について知りたい。

A グループ企業間で共通の個人情報取り扱いルールを定めておくことが有効

- ✓ 従業員の個人情報であっても、顧客の個人情報であっても、
  - 取得時に利用目的を明示し、本人の同意を得る
  - 目的外利用はしない

  を守るのは当然の義務となる。
  本社であっても、グループ企業であっても、それは変わらない。
- ✓ グループ企業内の利用であれば、
  - 共通のプライバシーポリシーの策定　や
  - グループ企業間共通のマネジメントシステムの構築

  などを行うことが有効。

Q&A

Q 広告メールを顧客に配信するのは個人情報（メールアドレス）を不当に利用していることになるのか？（広告配信の同意チェックをしていない場合）

A 個人情報を収集する際に同意を得た利用目的の範囲をはみ出す用途で、個人情報を取り扱うことはできない。

【原則】

- ✓ 個人からメールアドレスを取得する場合は、利用目的を明確にしなければならない。
- ✓ かつ、取得したメールアドレスは、利用目的の範囲内での利用に限定される。
- ✓ したがって、「広告配信の同意」を得ていない状態で、取得したメールアドレス宛てに広告メールを配信するのは、NG！

※ いっぽうで、2017年の改正時に、利用目的の緩和が行われている。
本資料の 「改正法におけるポイント（４）」 も参照のこと。

Q&A

Q 個人情報を紙とデータの両方で保管しているが、どちらも同様に扱う必要があるか？

A 個人情報は紙であっても同様に適切な管理が求められる。ただし、どちらかに一元化できるのであれば、管理コストもリスクも下げられる。

- ✓ 企業でも、未だに契約書の原本は紙で保管し、写しをPDFでデジタル管理もしている、というところはたくさんある。
- ✓ ただし、やはりアナログとデジタルのダブル管理はコストもかかり、可能であればどちらかは廃棄することを検討したほうが良いのでは？

Q 個人情報の管理義務の内容と方法とは？

A 以下のように整理（第4章 個人情報取扱い事業者の義務等　を整理）

※「具体的な方法」は法律では規定されていないため、個人情報を取り扱う業務の内容や性質、取り扱う個人情報の量などに応じてリスクを想定し、そのリスクに見合う対策を行う。

義務	概要
正確性の確保	取得した個人情報は、最新かつ正確な情報としなければならない。
安全管理措置	取得した個人情報に関しては、漏洩や改ざんなどを防止する安全管理措置を講じなければならない。
従業者の監督	個人情報を取り扱う従業者に対して、必要かつ適切な監督をしなければならない。
消去	利用目的を達成した個人情報は、速やかに消去しなければならない（努力義務）
本人からの請求	個人情報の持ち主である本人から、開示請求、利用停止請求、問い合わせ、苦情等があったときは、速やかにそれに応えなければならない。
第三者提供	本人の同意を得ない第三者提供は行ってはならない。また、第三者提供を行う際はその記録をとっておく必要がある。

Q&A

Q 必要な「安全管理措置」というのがイメージしにくい。具体的にはどのような対策のことなのか？

A 必要な安全管理措置とは、何らかのリスクを想定し、そのリスクを最小化するための措置のこと。 事業の内容や取り扱う個人情報によって、リスクが異なるため、ケース・バイ・ケースである。

- ✓ リスクの大小はケース・バイ・ケースなため、これをやれば十分、という目安は存在しない。
- ✓ たとえば、ほとんどの人はクルマに任意保険をかけているが、保証内容は人によって様々だし、保険に加えてドライブレコーダーや防犯ブザーを自分で取り付けている人もいる。
- ✓ つまり、「想定されるリスク」に対して、どこまでコストをかけるのか？というのは人それぞれであり、企業で言えば経営判断。
- ✓ コンプライアンスのため、というよりは、リスクを回避するため、という意識が必要なのでは？

Break：　保護から取扱という視点へ

- 身近なことに例えてみる

- 例：

  - 友人に貸したCDを、黙って知らない友人に「又貸し」された・・・
    - 第三者提供の事前同意を怠った例

  - 信頼していた友人に打ち明けた内緒話が、いつの間にか仲間内に広まっていた・・・
    - 利用目的の明確化で同意が不十分だった例
    - 第三者提供の事前同意を怠った例

  - さらに、話に尾ひれがついて全く別の話になっていた・・・
    - 情報の正確性が担保されていなかった例
    - 情報が改ざんされた例

- 日常生活の様々な場面において、対象を個人情報に置き換えて想像してみることで、おのずと正解は見えてくる

【参考】Web上の参考資料

- 個人情報保護法（個人情報保護委員会による解説など）
  - https://www.ppc.go.jp/personalinfo/
- 中小企業向けの個人情報保護法ガイド（同上）
  - https://www.ppc.go.jp/personal/chusho_support/
- JIPDECによるプライバシーマーク制度講座
  - https://privacymark.jp/wakaru/kouza/index.html

一般財団法人日本情報経済社会推進協会
電子情報利活用研究部　郡司　哲也
gunji-tetsuya@jipdec.or.jp