

パネル資料

番号法と第三者機関のあり方
一 個人情報保護法制とプライバシーの権利

新潟大学法科大学院 教授 鈴木 正朝

2011/3/3

個人情報保護法制をとりまく状況

(国際的動向)

インターネット / クラウド・コンピューティング

① OECDプライバシーガイドライン改正の動向

② EU個人データ保護指令及び各国法制の動向など

③ APEC越境データ保護の取り組み

(国内的動向)

社会保障と税の一体化政策

④ 共通番号制度・国民IDの導入(番号法)と第三者機関創設

⑤ 消費者委員会を中心とした個人情報保護法改正の動向

⑥ 各主務大臣の定める個人情報保護ガイドラインの改正動向

⑦ JIS Q 15001改正の動向

⑧ プライバシーマーク制度等民間認証制度の運営問題

2011/3/3

1. 共通番号制の議論とその対応策

議論	論点(例)	対応策(例)
1. 共通番号制一般の議論 →抽象論、観念論、印象論に流れる傾向	(1)国民のわからない情報化政策への漠然とした不安 (2)国民の政府への不信 (歴史的経緯と国民感情)	(1)少子高齢人口減少社会に向けたグランドデザインの提示 (番号制の光と影の真摯な説明) (2)影に対する効果的な政策の提示 (プライバシー権の保護立法と第三者機関の創設)
2. 個別ユースケースの議論 →利害関係者の登場と具体的要求 →専門的評価 →ベンダ各社の受注競争	(1)番号制導入によって損失を被る人たちの抵抗 (例:税の負担増、情報化投資増、顧客の喪失等) (2)番号制導入によって得をする人々のロビー活動 (例:IT利権と過剰提案) (3)費用対効果への懸念	(1)原理原則論を基礎とした説得、議論の公開による世論形成を背景とした牽制、政治的調整と決着 (2)スキルある真面目な委員構成と公正な技術評価 (3)効果測定のお考え方の確立
3. 顕在化している情報管理リスクへの対応の議論 →予算措置等	(1)データ流出等の危険性 (2)正確性の確保への懸念 (3)目的外利用及び利用目的の段階的拡大の危険性	(1)～(3) 公務員総背番号制の採用、ログ保存、監査の実施、利用履歴の本人確認、利用目的の拡大制限
4. 個人情報保護法の議論	・消費者庁及び消費者委員会 の抜本改正への意欲の欠如	・第三者機関への権限の委譲と第三者機関での抜本改正の取り組み

2. なぜ「プライバシー権」(憲法13条)か？

- 国家権力による「共通番号」の濫用リスクを防ぐためには**憲法上の制約**(規律)が必要であり、その点の確認規定を設けるべきである。
 - 番号制における利用目的は法律によって定められるが(法定利用目的)、それは国会の立法裁量に委ねることを意味する。
 - 利用目的は段階的にその範囲を拡大していく傾向にあるが(例:オランダ等)、それは無限定なものであってはならず**憲法を根拠とする歯止め(制限)**が必要である。
- 「番号法」に「利用目的拡大の制限」を「**プライバシー権**」の派生的原理として**明文化すべき**である。(当該条文が憲法の理念(プライバシー権)に基づくことを宣言することで、国会が自らの立法活動に一定の制約を課し、憲法的習律形成の端緒とするところに意義がある。)

3. プライバシー権とは何か？

(1)「プライバシー権」は1890年代米国不法行為法における、時代のニーズの下で生成され、その時代の変化（データバンク時代の要請等）を受けて発展してきた経緯があり、わが国はその継受国として、わが国不法行為法において、そして日本国憲法において、その定着を試みてきたのであり、既に半世紀を経て今日に至っている。学界は、日米の法体系の違いを乗り越えるべく、日本法における「プライバシー権」の再構成を試み、多くの学説が公表されている。

→人権としてのプライバシー権（新しい人権、13条論）

→人格権としてのプライバシー権（大陸法の影響）

2011/3/3

3. プライバシー権とは何か？

(2)こうした発展の過程において、性質を異にする意義を内包し得たのは、まさに「プライバシー権」の思想の特徴であると積極的に評価することもできるが、その反面、法概念として十分に成熟しておらず、未だ形成過程にあるとの理解も存在する。特に、立法の現場では時期尚早との評価が定着しており、現行個人情報保護法制はプライバシー権に係る情報とは一線を画した法律として制定されている。このことは、プライバシー侵害の民事判例が多数集積している裁判実務と際だった対照をなしているといえることができる。

→「自己情報コントロール権」は対権力及び私人間において採用し得る考え方であるか？

2011/3/3

3. プライバシー権とは何か？

(3) 国民総背番号制度と批判され続けてきた「共通番号制度」が具体的に創設されようとしている今日、これとプライバシー権との関係が問われている。

古くはグリーンカードが争点となり法が施行されることなく廃止され、今日では多くの住基ネット訴訟が提起され一部下級審では違憲判決が示された。まさに番号制度は管理社会の扉を開くものとして批判され続けてきた歴史であったといえる。

→ 最高裁の住基ネット合憲判決を踏まえ、憲法の理念との関係を整理し、その法案(番号法)に反映させることが求められている。

3. プライバシー権とは何か？

(4) 「プライバシー権」から演繹的に憲法原理を引きだそうという発想は、「プライバシー権」の発展の経緯とその思想(考え方)の特徴を踏まえていない。

① 「イエロージャーナリズム」の時代(米国不法行為法)

→ プライバシー権の生成

② 「データバンク」の時代—汎用機の登場と東西対立、ビックブラザーへの脅威の時代(米国憲法)

→ 自己情報コントロール権の登場

③ 「情報ネットワーク」の時代(インターネットと多様なデジタルデバイスの出現、無数のリトルブラザーの跋扈)

→ 自己情報コントロール権の限界

* プライバシー権はそれぞれの時代のニーズを反映しそれを包摂し発展してきたといえる。

3. プライバシー権とは何か？

(5)「共通番号制度」の時代を踏まえた新たな「プライバシー権」の発展が期待されている。すなわち、立法論として「プライバシー権」と正面から対峙し、それを積極的に採用すべく、それを定義し再構成する取り組みが求められているのである(時代のニーズ)。

→「プライバシー権」から、現代的データプライバシーの派生的原理を見出し(創造し)、それを文章化し、提言し、「番号法」にデータプライバシー保護法としての性格を与え(人権の具体化法)、かつ、それを担保する有効な「第三者機関」(統治機構の具体化法)を創設しなければならない。

2011/3/3

3. プライバシー権とは何か？

* 人類普遍の原理である人権規定(プライバシー権)が番号制を許さないと解するならば、日本と同様の国家体制と生活実態にある欧米先進各国で番号制が採用されている理由を説明し難い。

* ドイツからオランダ、北欧まで番号制の内容に差異があるのは、各国の歴史(戦争体験等)的背景に基づく国民感情に根ざすところの影響が大きい。こうした国民感情に沿った段階的導入が検討されるべきである。

* 番号制度はデータベース間の連携を容易にし、管理社会の出現を招き得る。この点において国民の「プライバシー権」を侵害する憲法上の問題を検討し得る。利用目的の拡大には一定の憲法的歯止めが必要である。

2011/3/3

3. プライバシー権とは何か？

- コミュニケーション(=情報流通の確保)

各人が様々な相手又はコミュニティにおいて、他人のこと(氏名はもとよりその事実及び評価)を(当人の権利利益を損なわない範囲で)話題にできる自由が保障されていなければ人間関係とコミュニケーションは成立しない。

- ネガティブ情報

集積することによって、またそれが利用されることによって本人の人格権(私人間)、プライバシー権(対権力)が損なわれることがある。

→情報利用の実態のコンテキストで判断される。

→対象情報の性質のみで判断できない。

→主体、利用形態、業務モデル、情報システム等に立ち入った事実関係の調査を基にプライバシー権から評価されなければならない。(→第三者機関の創設の意義と権限規定のあり方)

2011/3/3

憲法の具体化法としての番号法と第三者機関



2011/3/3

4. 番号法・第三者機関はどうあるべきか？

番号法	
1. 「個人の尊重」の理念とセンシティブ情報の導入(実質的にデータ・プライバシーの思想を軸とする。EUとの整合も考慮する。)	憲法13条の個人の尊重の原理を基礎とすることを確認し、かつ、センシティブ情報(情報の重要度・価値)に着目した規律を導入し、学説・判例においてプライバシーの権利(データ・プライバシー)の内実(理論的基礎)が形成される条文的根拠を与える。また以下のいくつかの原則をデータ・プライバシーの派生的原理として構成する。
2. データベースシステム独立の原則・省庁を横断するオンライン結合禁止の原則 (分野別DB=個別番号の「分野」の意味の明確化)	(1)個別番号の照合・照会は法律の根拠を要する。 (2)照合・照会は、第三者機関の判断(処分)を要する。 (3)第三者機関は上記照合・照会の判断に際して、行政庁間のデータ管理の責任(分界点)と権限の範囲の明確化、利用目的管理機能と安全管理措置の状況を確認する。 (4)上記の確認事項を担保するための措置(照合のログ、照会の記録の保存義務等)を課し、第三者機関の監査の対象とする。
3. ネガティブ情報の消去	(1)指定されるネガティブ情報は保有期間を定め、消去されなければならない。 (2)第三者機関は消去されていることを確認しなければならない。

4. 番号法・第三者機関はどうあるべきか？

番号法	
4. プライバシー権への影響調査実施	(1)内閣(法制局)及び大臣は国民の個人の尊重の理念(プライバシーの権利)に係る情報の収集・管理を伴う法令を起草または審査する場合は、第三者機関に相当の期間を定めて「意見」を求めなければならない。 (2)両院は、法案審議に際して、第三者機関に「調査報告」を求めることができる。 (3)法令に基づき情報システムを構築する場合は、その基本仕様の策定に際し第三者機関の「意見」を得なければならない。
5. プライバシー保護実態調査の実施	(1)第三者機関は、安全管理・利用目的管理の運用実態が国民の個人の尊重の理念(プライバシーの権利)に対する脅威の観点から(行政、自治体、民間の)「調査」を行うことができる。情報システムの立入調査及び関連資料の提出命令、閲覧権、質問権などの調査権と大臣及び自治体の長の(一部及び全部の)拒否権を定める。大臣及び自治体の長の拒否に際しては「理由の付記」を義務付け、その内容は「公表」する。また、調査結果は年に1度「国会へ報告」する。 (2)「改善勧告」に止まり処分権を有しない。行政庁及び自治体は勧告内容を踏まえ自らは是正し、民間企業に対してはそれぞれの主務大臣が業法または個人情報保護法に基づき処分等を行うこととする。 (3)勧告内容及びその後の行政庁等の対応状況は「公表」する。

4. 番号法・第三者機関はどうあるべきか？

番号法	
6. 事前相談 (PIA及び事前相談は従前の対象情報の性質による単純な規制から脱しシステム等全体の総合評価を行う。)	主に民間事業者のビジネスモデル及び情報システムにおけるプライバシー・情報セキュリティのあり方について事前相談に応じ、助言を与えることでビジネスの過度な萎縮(過剰反応等)、組織内部の意思決定の遅れを回避するよう行政的支援を行う。また消費者保護的見地から、その後の確認の権限を留保することができるよう設計する。
7. プライバシー等に関する第三者評価認証の実施、及び民間認証の監督	(1)関連規格の原案とりまとめと第三者評価認証を実施する。 (2)民間認証制度の濫立と無定見な運用による弊害を除去し、法規制との整合を図り、また諸外国の同一制度間の相互承認の調整のため民間認証機関の監督を行う。
8. 個人情報保護法及び番号法の主管 (個人情報・プライバシー保護行政の要とする)	(1)個人情報保護法の主管を第三者機関に移し、番号法との整合をとった運用(改正)を行う。(コミッショナーとして越境データ問題に関する交渉を行う前提となる。) (2)関係主務大臣と協議しながらガイドラインを策定する。 (3)各省庁のCIO及びNISCとの定期協議を行う。
* 独立採用 (附帯決議)	IT及びプライバシー問題の専門スキルが組織的・継続的に維持(養成)できるよう人事面での特段の配慮を要する。

5. 第三者機関をどう設計すべきか？

以下、「資料3 社会保障・税に関わる番号制度及び国民ID制度における個人情報保護方策の骨格案」(内閣官房)より

1 業務範囲

(1) 監視の対象とする機関等

番号制度等の導入に伴う個人情報の漏えい・濫用等の危険性は、国の行政機関が保有する個人情報のみならず、地方公共団体又は民間が保有する個人情報についても想定されることから、国の行政機関(注)のほか、地方公共団体及び番号を取り扱う民間事業者も監視の対象とすることとしてはどうか。

(注) なお、独立行政法人等個人情報保護法2条1項に規定される独立行政法人等については、その性格上、国の行政機関に準じるものと考えられることから、国の行政機関には、基本的に独立行政法人等を含むものとする。

5. 第三者機関をどう設計すべきか？

(2) 監視の対象とする分野

当面の情報連携の範囲は、社会保障及び税分野^(注1)とされていることから、当初は、社会保障及び税分野の番号に係る個人情報^(注2)(以下単に「番号に係る個人情報」という。)を監視の対象とし、将来的に対象の拡大を目指すこととしてはどうか。

(注1) ここでいう「社会保障及び税分野」とは、社会保障及び税分野で、実際に番号制度の利用範囲となるものを指し、その具体的範囲については、番号制度本体の検討に伴い、更に特定されるものと考えられる。以下同じ。

(注2) 番号については、各機関等において、少なくとも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形態で保有されているものと考えられることから、それ自体が個人情報に該当すると解される。

5. 第三者機関をどう設計すべきか？

2 機能・権限

(1) 最低限必要な機能・権限

- 普及啓発を行う機能
- 監視対象機関等に対し、番号に係る個人情報の取扱いに関する事務の実施状況について、定期的若しくは随時に調査を実施し、又は資料の提出・説明・報告等を求める権限
- 監視対象機関等に対し、助言・指導・勧告を行う権限
- 民間事業者に対する命令権限
- 監視対象機関等による番号に係る個人情報の取扱いに関し、苦情処理・相談受付・調査を行う権限
- 番号制度の基盤となるシステムを、その稼働前に監査するとともに、情報連携基盤を常時監視する機能・権限
- 番号に係る個人情報ファイル簿(行政機関個人情報保護法11条)の内容を把握する機能
- 国際協調を行う機能

5. 第三者機関をどう設計すべきか？

(2) 更に検討すべき機能・権限

- 監視対象機関等に対する立入検査権限を有することとするか。
- 国の行政機関又は地方公共団体に対し、命令に相当する権限を行使できるようするためには、どのような仕組みが考えられるか。
- 制裁金等の制裁措置を実施できることとするか。
- 救済申立ての手續に第三者機関が関わることとするか、関わることとする場合、どのように関わることとするか。
- 番号制度の在り方及び番号制度における個人情報保護方策の在り方に対して意見を述べる権限・機能を有することとするか。

2011/3/3

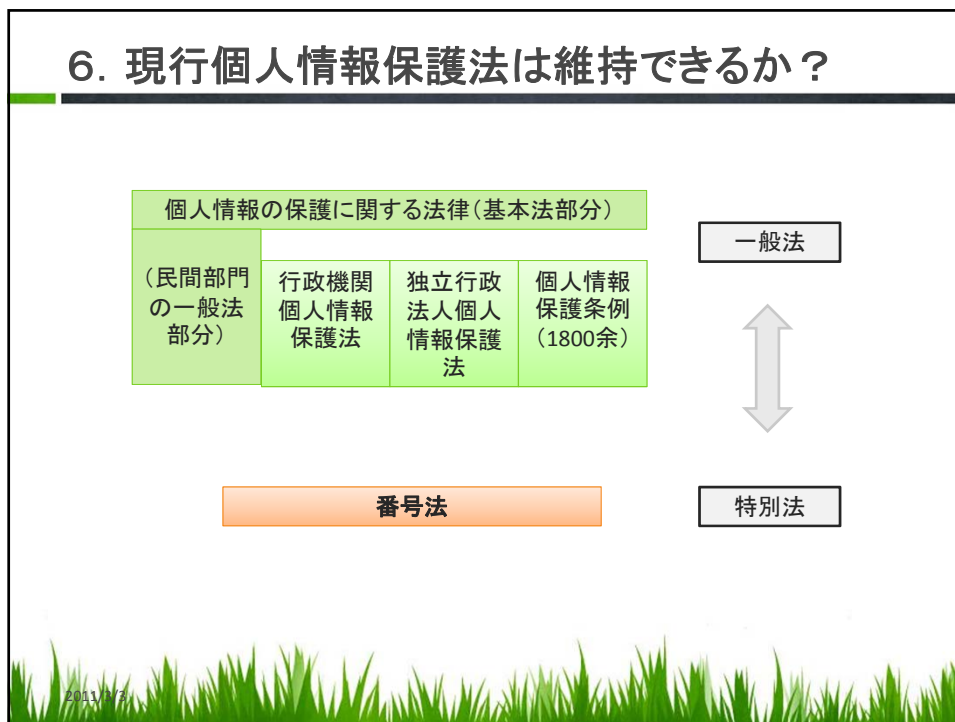
5. 第三者機関をどう設計すべきか？

3 法的形式と組織形態

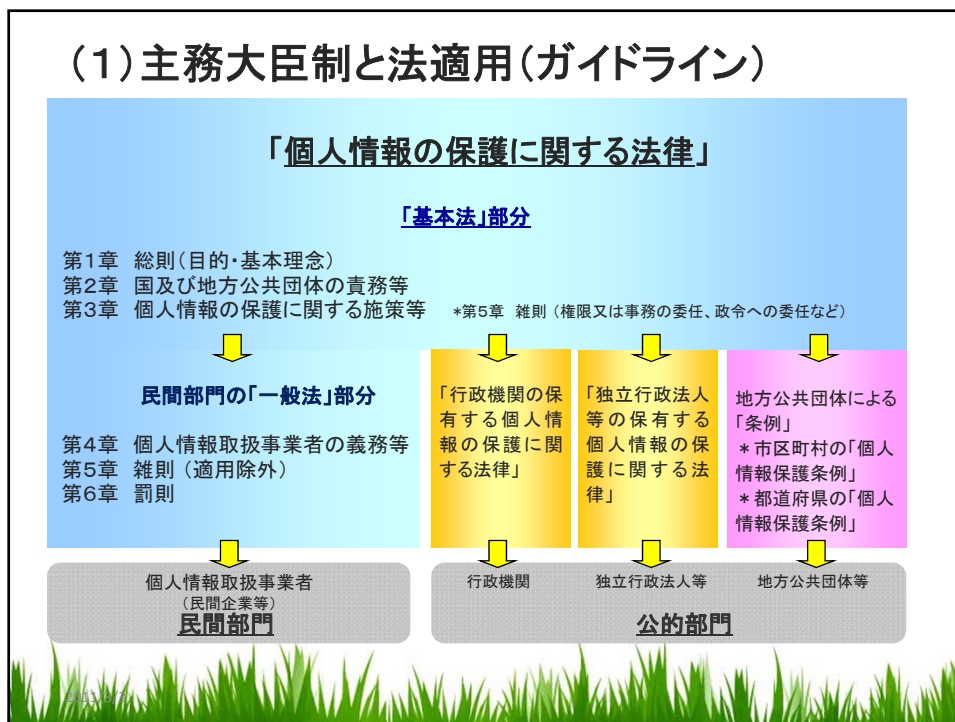
- 政府からの独立性を確保した上、上記のように強力な機能・権限を有することとしつつ、組織としての判断の公正性、中立性をも担保するため、内閣府の外局として置かれる、いわゆる三条委員会(内閣府設置法49条1項)とすることとしてはどうか。
- 委員長及び委員を国会の同意を得て内閣総理大臣が任命することとしてはどうか。
- 委員長は、個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、事後に委員会の同意を得ること等を条件に、単独で権限を行使できることとしてはどうか。委員長は、対外的にコミッショナーとして委員会を代表することとしてはどうか。
- 第三者機関は、毎年、活動状況を国会に報告することとしてはどうか。

2011/3/3

6. 現行個人情報保護法は維持できるか？



(1) 主務大臣制と法適用(ガイドライン)



* 教育分野の個人情報保護法適用関係(例)

個人情報を取り扱う主体	適用法	監督官庁
文部科学省	行政機関個人情報保護法	総務省(行政管理局)
国立大学法人東京大学	独立行政法人等個人情報保護法	総務省(行政管理局)
東京都立小石川高校	東京都個人情報保護条例	東京都
中野区立〇〇中学校	中野区個人情報保護条例	中野区
私立〇〇学園小学校	個人情報保護法	文部科学省
〇×進学塾	個人情報保護法	経済産業省

- 研究教育機関を対象として本来一元的に行われるべき文部科学行政が、個人情報の取扱いについては、総務省と文部科学省と地方自治体に分かれる問題。

* 大学・その関係団体等と個人情報保護法の適用関係

個人情報を取り扱う主体	適用法	監督官庁
国立大学法人東京大学	独立行政法人等個人情報保護法	総務省(行政管理局)
・大学病院	→ ガイドライン	+ 厚労省
・遺伝子の取扱い	→ ガイドライン	+ 厚労+ 文科+ 経産
東京大学同窓会	個人情報保護法	消費者庁
東京大学労働組合	個人情報保護法	厚生労働省
東京大学生活協同組合	個人情報保護法	経済産業省
大学の委託先企業	個人情報保護法	経産省等主務大臣
学生個人	適用なし(契約法・不法行為法)	(裁判所)

* 医療分野の個人情報保護法適用関係(例)

個人情報を取り扱う主体	適用法	監督官庁
厚生労働省	行政機関個人情報保護法	総務省(行政管理局)
国立がん研究センター	独立行政法人等個人情報保護法	総務省(行政管理局)
東京都立〇〇病院	東京都個人情報保護条例	東京都
国立市立△△病院	国立市個人情報保護条例	国立市
医療福祉法人〇〇病院	個人情報保護法	厚生労働省
〇〇内科(個人開業医)	個人情報保護法	厚生労働省

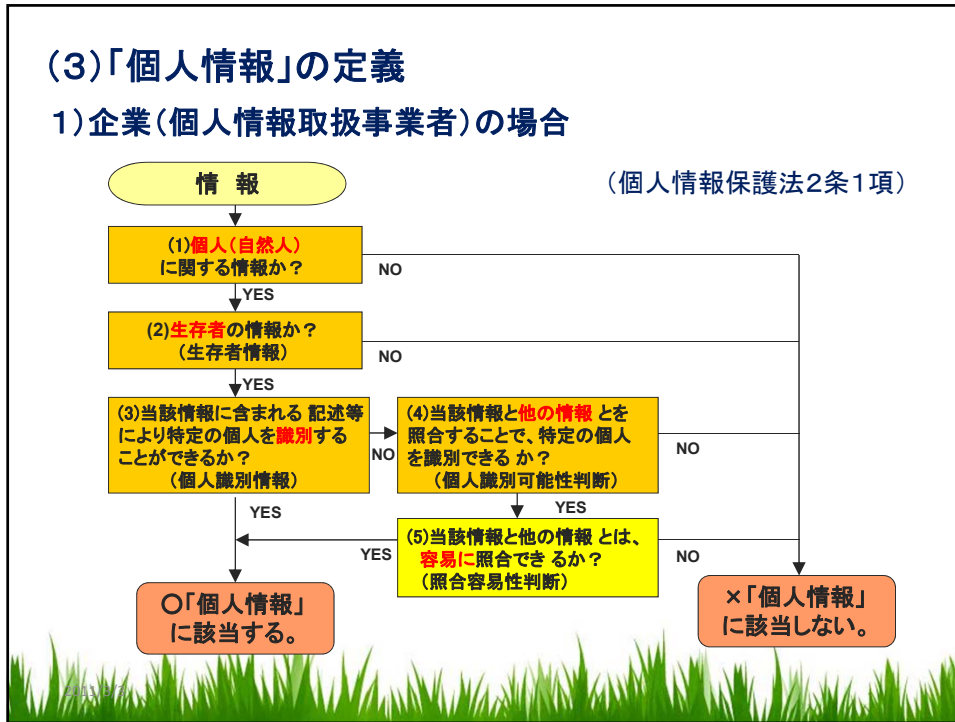
- 病院を対象とする厚生労働行政が、総務省と厚生労働省、地方自治体(そして、大学病院はそれに加えて文科省)が関与することになる問題

(2) 個人情報保護条例を維持できるか？

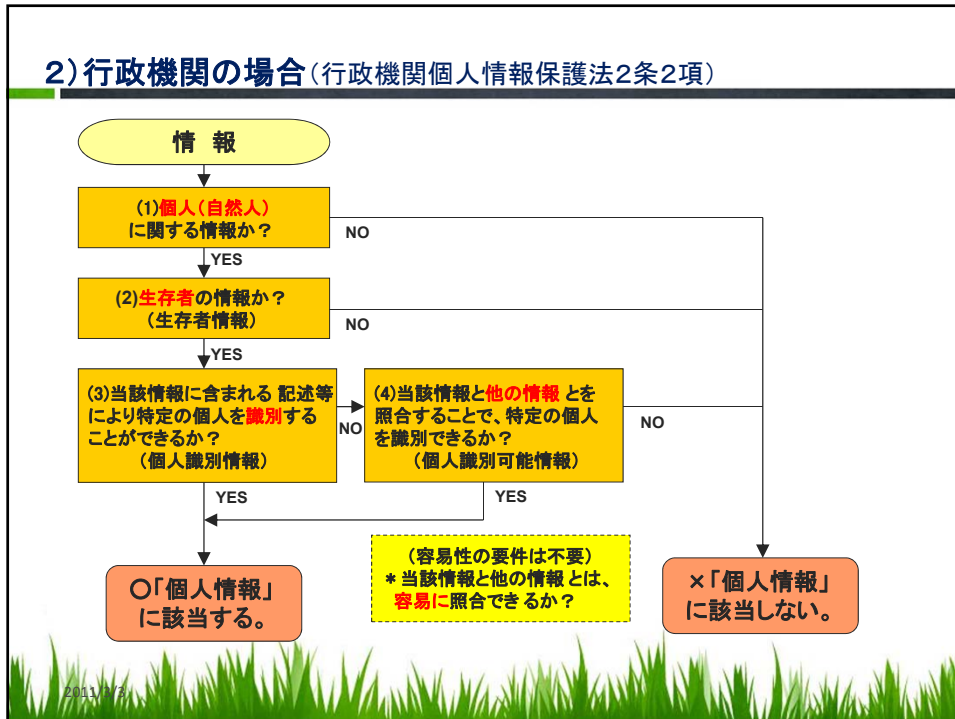
- 「住基ネット」さらには「自治体クラウド」構想、「共通番号制度」導入の時代において1800を超える地方公共団体の議会がそれぞれ独自に個人情報の定義や安全管理基準を定め得る状態を放置している問題(地方自治の本旨に関わる事項か？ネットは自治体に閉じているか？)
- 共通番号制度導入を前にプライバシー権に属する情報(人権)を基礎とした有効に権力チェック可能な新たな法制度構築が望まれる(条例の撤廃を含む)。

(3)「個人情報」の定義

1) 企業(個人情報取扱事業者)の場合

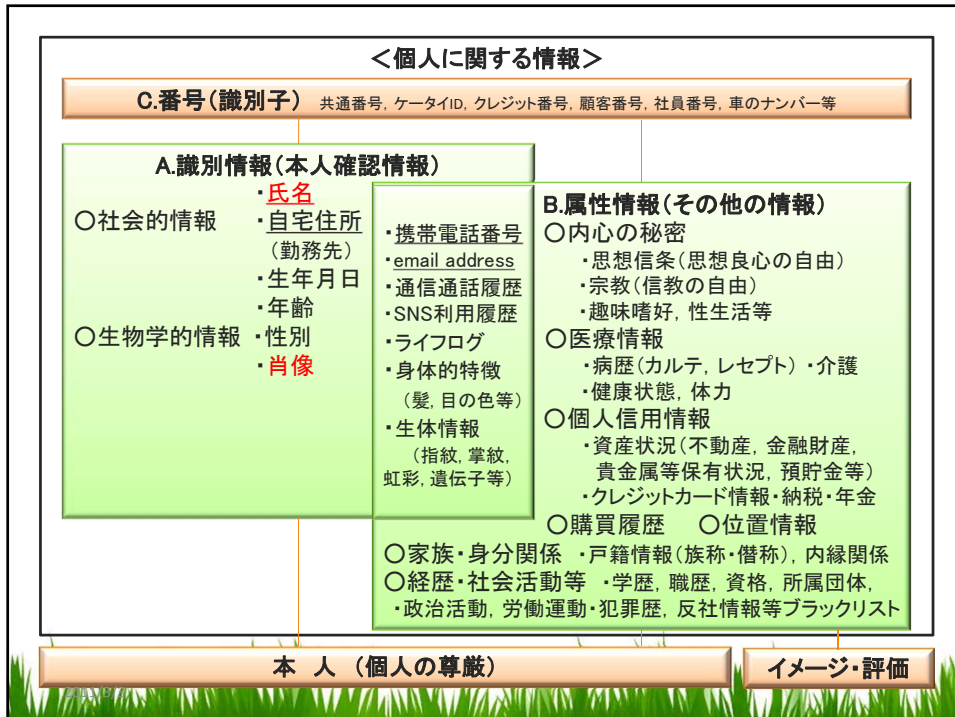


2) 行政機関の場合 (行政機関個人情報保護法2条2項)

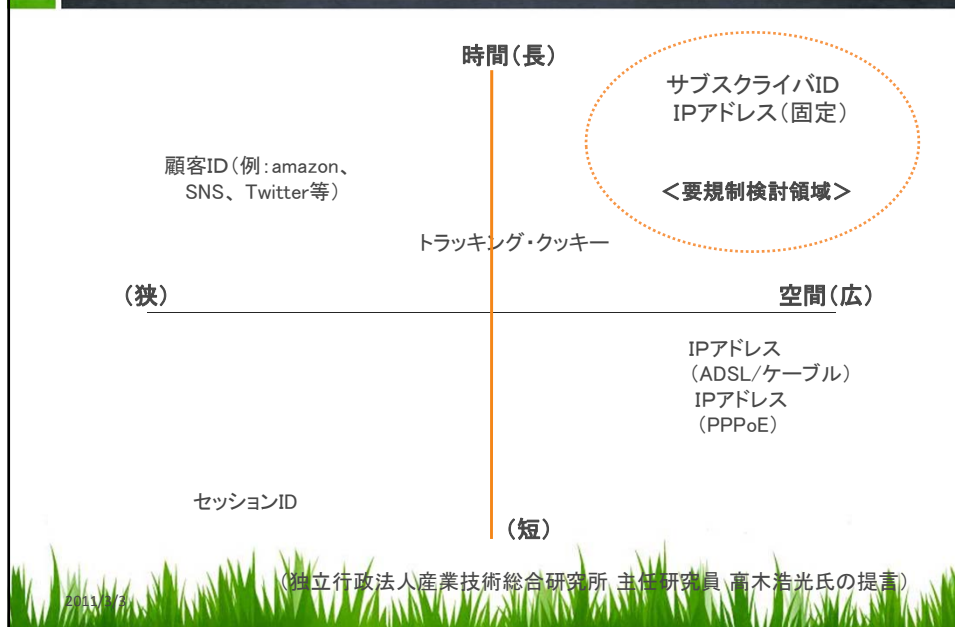


(3)「個人情報」の定義(2条1項)

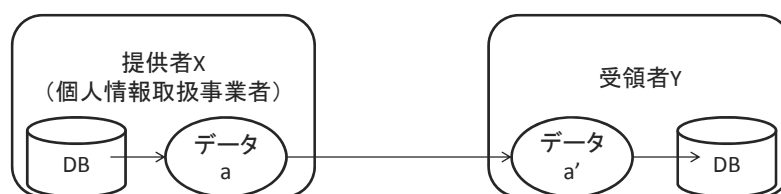
- 「識別」の解釈: **誰が識別するのか?** その主語は条文上明らかではない。特定個人の「識別」可能性判断の主体は解釈上の論点となる。
- 1. 「事業者」基準: 個人情報を取り扱う事業者を基準として判断する説
- 2. 「従業者」基準: 個人情報を取り扱う事業者の従業者等自然人を基準として判断する説
- 3. 「本人」基準: 情報主体である本人を基準として判断する説
- 4. 「一般人」基準: 社会一般の人を基準として判断する説



識別子の法的評価の一例(時間軸と空間軸)



(4) 番号(識別子)と第三者提供(23条)の適用関係



提供者X	→(提供)→	受領者Y	Xの法適用の有無
特定個人識別性あり ○	→ ID	特定個人識別性あり ○	あり
特定個人識別性なし ×	→ ID	特定個人識別性なし ×	なし
特定個人識別性なし ×	→ ID	特定個人識別性あり ○	なし
特定個人識別性あり ○	→ ID	特定個人識別性なし ×	経産省 : あり 総務省 : なし

(4) 番号(識別子)と第三者提供(23条)の適用関係

1. 第三者提供における「識別」性判断の主体

(1) 提供者(行政庁・事業者)基準

(2) 受領者基準(受領者が個人情報取扱事業者であるか否かを問わない。)

* データ流出の場合は？

2. 「照合」性判断における主体

(1) 行政庁・事業者基準(法人全体から評価する)

(2) 職員・従業員基準(データを取り扱っている自然人を基準に容易照合性判断を行う)

2011/3/3

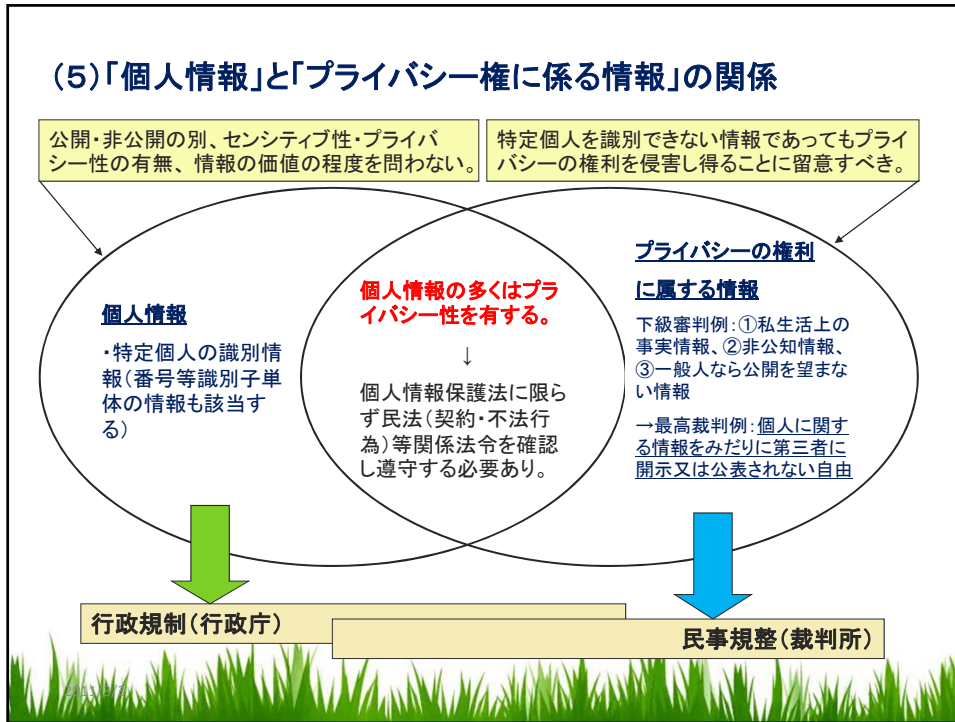
* 委託と第三者提供

1) 個人情報取扱事業者の場合

	提供時の本人同意の有無	提供後の安全管理上の責任
「個人データ」の 第三者提供 (あげる場合)	<ul style="list-style-type: none"> 提供前に本人同意必要 <p><デメリット></p> <ul style="list-style-type: none"> ①同意を得るコストが高い ②全員の同意は不可能であるため提供データが大幅に目減りする 	<ul style="list-style-type: none"> 提供後の安全管理の法的責任なし。 事故時における本人に対する民事責任の有無はケースバイケースか。 <p><メリット></p> <ul style="list-style-type: none"> ○提供後については委託先の安全管理についてのコスト負担がない。
「個人データ」の 委託先提供 (預ける場合)	<p>本人同意不要</p> <p><メリット></p> <ul style="list-style-type: none"> ①委託先を自由に選定可能 ②全データを低コストで提供可能 	<ul style="list-style-type: none"> 委託先の監督義務あり。 事故時における本人に対する民事責任も問題となる。 <p><デメリット></p> <ul style="list-style-type: none"> ○委託先の安全管理についてのコスト負担が大きい。

2) 行政機関の場合： 利用目的外の「保有個人情報」利用・提供の禁止

2011/3/3



(6)対象情報(個人情報)

1)個人情報取扱事業者の場合

1)「個人情報」(個人情報保護法2条1項)
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)

***「個人情報データベース等」**(同法2条2項)
個人情報を含む情報の集合物であって次に掲げるもの
①**コンピュータ処理情報**:特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
②**マニュアル処理情報**:特定の個人情報を容易に検索することができるように体系的に構成したもので、目次、索引その他検索を容易にするためのものを有するもの

2)「個人データ」(同法2条4項) 個人情報データベース等を構成する個人情報

3)「保有個人データ」(同法2条5項)
開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データ(ただし、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は6ヶ月以内に消去することとなるものは除く)

「個人情報取扱事業者」(同法2条3項)
個人情報データベース等を事業の用に供している民間事業者(ただし、個人情報データベース等に含まれる個人情報によって、識別される特定の個人の数の合計が、過去6ヶ月以内のいずれの日においても5,000を超えない者を除く。)

2) 行政機関の場合

1) 「個人情報」(行政機関個人情報保護法2条2項)

生民間利用の場合の規制対象(個人情報取扱事業者)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。)

2) 「保有個人情報」(同法2条3項)

独立行政法人等の役員又は職員が職務上作成し、又は取得した個人情報であって、当該独立行政法人等の役員又は職員が組織的に利用するものとして、当該独立行政法人等が保有しているものをいう。(ただし、**法人文書**に記録されているものに限る。)

3) 「個人情報ファイル」(同法2条4項)

保有個人情報を含む情報の集合物であって次に掲げるもの

- ① **電算処理個人情報ファイル**:一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
- ② **マニュアル処理個人情報ファイル**:一定の事務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索することができるように体系的に構成したもの

「行政機関」(同法2条1項)

独立行政法人第2条第1項に規定する独立行政法人及び別表に掲げる法人をいう。

2011/7

* 「保有個人情報」と情報公開法との関係

「個人情報」

(行政機関個人情報保護法2条2項)

「保有個人情報」

(同個人情報保護法2条3項)
 (1)職務上作成・取得
 (2)組織的利用のため保有

「個人情報ファイル」

(同個人情報保護法2条4項)

- ①電算処理
個人情報ファイル
- ②マニュアル処理
個人情報ファイル

「行政文書」

(情報公開法2条2項)
 (1)職務上作成・取得
 (2)組織的利用のため保有

除外

- ①官報、白書、新聞、雑誌、書籍など不特定多数者販売目的
- ②歴史的・文化的資料、学術用研究資料として特別管理(政令)

2011/7

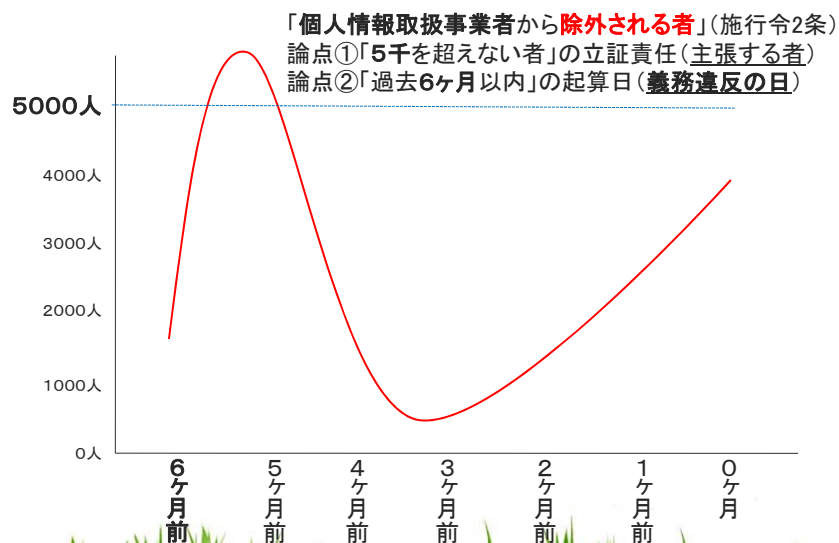
(7) 民間部門の規制対象(個人情報取扱事業者)

個人情報保護法施行令(政令)第2条

- …当該個人情報データベース等の全部又は一部を構成する個人情報によって識別される特定の個人の数を除く。)の合計が過去6月以内のいずれの日においても5千を超えない者とする。
- 一 個人情報として次に掲げるもののみが含まれるもの
- イ 氏名
- ロ 住所又は居所(地図上又は電子計算機の映像面上において住所又は居所の所在の場所を示す表示を含む。)
- ハ 電話番号

2011/7

*「個人情報取扱事業者」の定義



2011/7

*「個人情報取扱事業者」の定義

二 不特定かつ多数の者に**販売**することを**目的**として発行され、かつ、不特定かつ多数の者により随時に購入することができるもの又はできたもの

●電話帳、カーナビデータと市販名簿への対応

「個人情報取扱事業者」該当性の問題

・安全管理義務(法20条、法21条、法22条)の対象情報(個人データ)から除外されるか？

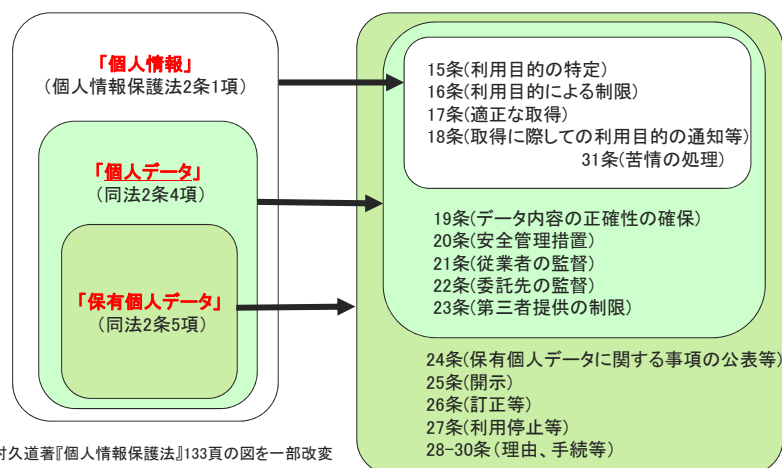
→除外されず、法の適用あり。

cf. 経産省ガイドラインの立場＝権限行使せず

2011/3/3

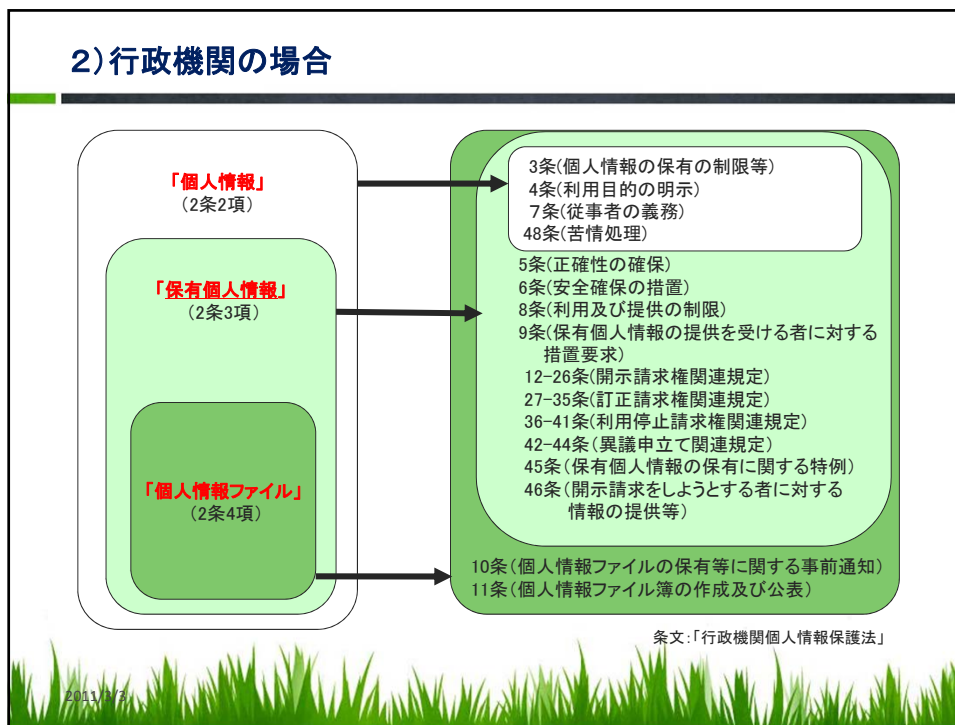
(8) 対象情報と義務規定の関係

1) 個人情報取扱事業者の場合



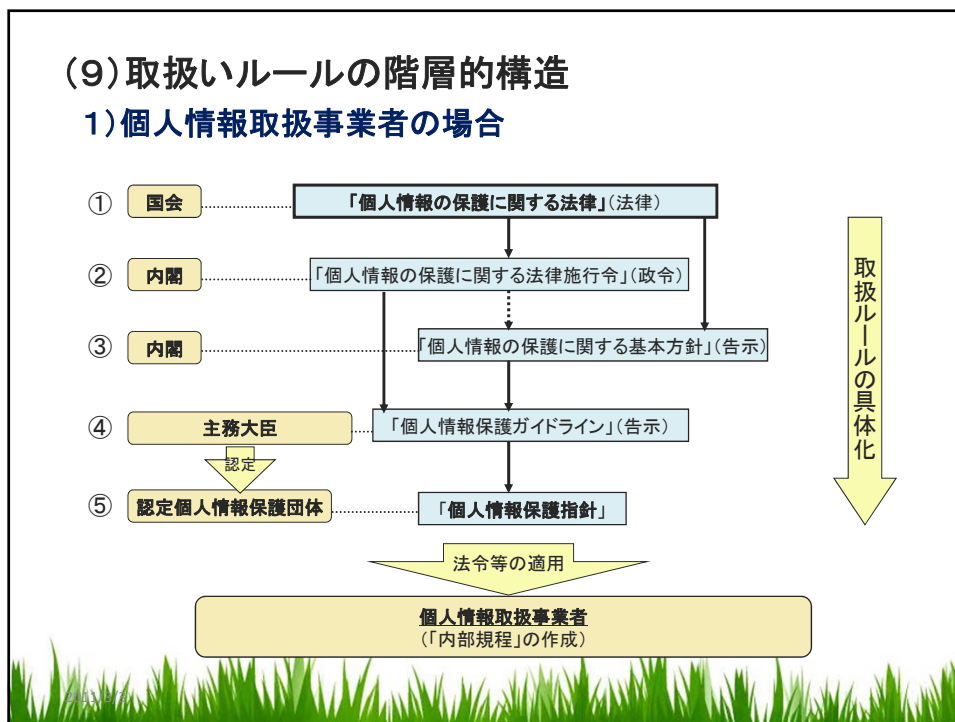
2011/3/3

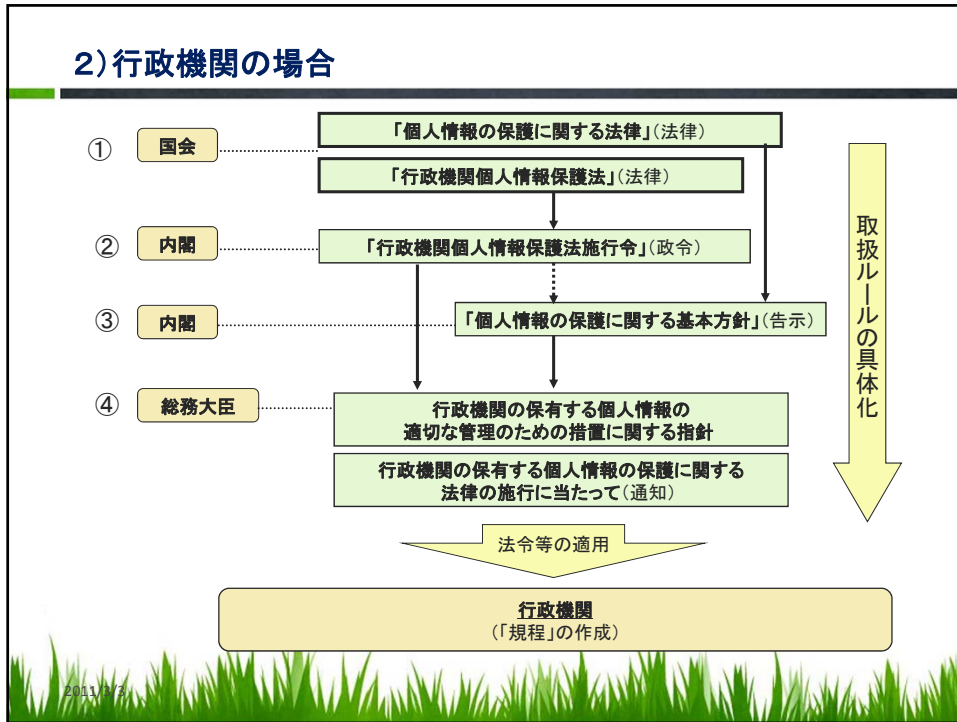
2) 行政機関の場合



(9) 取扱いルール の階層的構造

1) 個人情報取扱事業者の場合





(10) 利用目的管理義務

1) 個人情報取扱事業者の場合

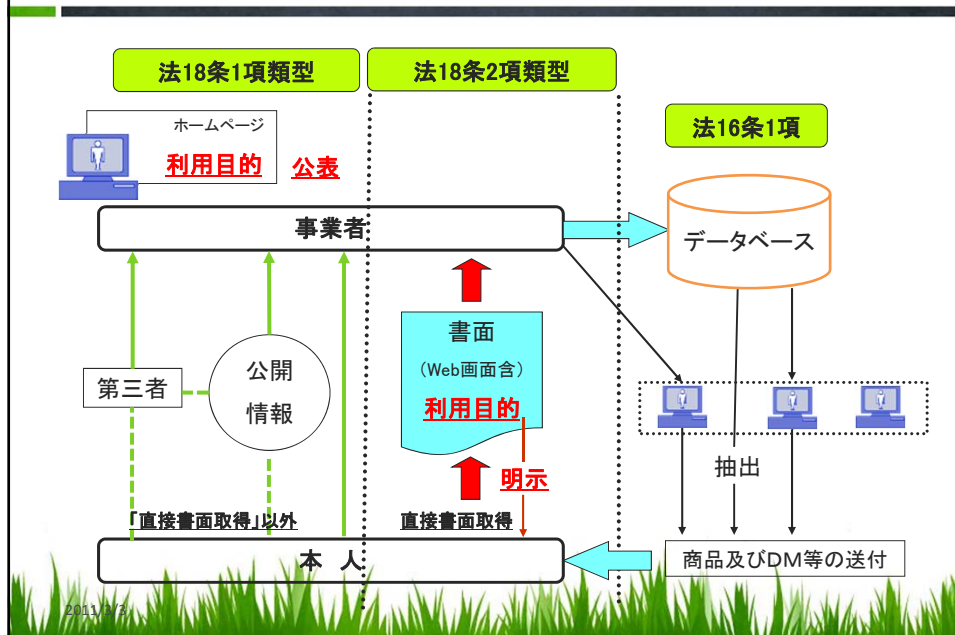
	「個人情報」の取得の態様	「利用目的」の通知等
直接取得	●直接書面取得(個人情報保護法18条2項) ①契約を締結することに伴って契約書に記載された当該本人の個人情報を取得する場合 ②契約書以外の書面に記載された当該本人の個人情報を取得する場合	⇒「あらかじめ、本人に対し、その利用目的を 明示 しなければならない。」
	●上記以外での取得(同法18条1項) ①本人から書面を介さずに直接取得する場合	⇒「あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に 通知 し、又は 公表 しなければならない。」
間接取得	②第三者を介して間接取得する場合 ③人を介さずに公開情報等から間接取得する場合 ④受託による間接取得	

利用目的に関する義務

1) 個人情報取扱事業者の場合

- ① 利用目的の特定(個人情報保護法第15条1項, 第23条1項)
↓
- ② 利用目的の通知等
 - ・取得に際しての利用目的の通知等(法第18条1項・2項・4項)
 - ・オプトアウトに際しての利用目的の通知等(法第23条2項)
 - ・保有個人データに関する事項の公表等(法第24条1項)
- ③ 利用目的による制限(法第16条1項～3項, 第23条4項・5項)
- ④ 利用目的の変更(法第15条2項, 第18条3項・4項, 第16条1項, 第23条3項)
- ⑤ 保有個人データの通知の求めへの対応(法第24条2項・3項)

(10) 個人情報取扱事業者の利用目的管理義務



2) 行政機関の場合		
	「個人情報」の取得の態様	「利用目的」
直接取得	<p>●直接書面取得(4条)</p> <p>(①契約を締結することに伴って契約書に記載された当該本人の個人情報を取得する場合)</p> <p>(②契約書以外の書面に記載された当該本人の個人情報を取得する場合)</p> <ul style="list-style-type: none"> ・記名式アンケート ・懸賞募集 <p>(オンラインも含む)</p>	<p>⇒個人情報を保有するに当たっては、法令の定める業務を遂行するため必要な場合に限り、かつ、その利用目的をできる限り特定しなければならない(3条1項)。</p> <p>⇒あらかじめ、本人に対し、利用目的を明示しなければならない(4条)。</p> <p>⇒利用目的以外の目的のために保有個人情報を利用し、又は提供してはならない(8条)。</p>
	<p>●上記以外での取得</p> <p>①本人から書面を介さず直接取得する場合</p> <ul style="list-style-type: none"> ・電話など音声情報記録、監視カメラ等 	<p>⇒個人情報を保有するに当たっては、法令の定める業務を遂行するため必要な場合に限り、かつ、その利用目的をできる限り特定しなければならない(3条1項)。</p> <p>⇒利用目的以外の目的のために保有個人情報を利用し、又は提供してはならない(8条)。</p>
間接取得	<p>②第三者を介して間接取得する場合</p> <p>③人を介さず公開情報等から間接取得する場合</p> <p>④受託による間接取得</p>	<p>⇒個人情報を保有するに当たっては、法令の定める業務を遂行するため必要な場合に限り、かつ、その利用目的をできる限り特定しなければならない(3条1項)。</p> <p>⇒利用目的以外の目的のために保有個人情報を利用し、又は提供してはならない(8条)。</p>

2) 行政機関の場合

- **法令業務と利用目的の特定**
 - 個人情報を保有するに当たっては、**法令の定める業務**を遂行するため必要な場合に限り、かつ、その**利用目的をできる限り特定**しなければならない(3条1項)。
- **利用目的の特定の考え方**
 - 利用目的は、保有から利用・提供に至る**個人情報の取扱いの範囲を原則的に画定するもの**。したがって、**具体的な利用行為が当該利用目的の範囲内であるか否かについて合理的かつ明確に判断できる**よう、できるだけ具体的、個別的に特定すること。
- **利用目的の制限**
 - 利用目的の達成に必要な範囲を超えて、個人情報を保有してはならないこととされている(3条2項)。
- **利用目的の変更**
 - 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(3条3項)。
 - 社会通念上妥当であると考えられる範囲内

(11)情報セキュリティ対策

脅威者の 類型	データの漏えい・滅失・き損の例	適用法と適用条項
1. 第三者	①物理的侵入や不正アクセスによる 個人データ ／ 保有個人情報 の漏えいや破壊、改ざん、ウイルス混入等による 個人データ ／ 保有個人情報 の破壊や外部への不正送信など外部からの脅威など	民間 →安全管理措置 (個法20条) 行政 →安全確保の措置 (行個法6条)
2. 従業者 従事者 (職員、元 職員も含む)	①従業者のアクセス権限の濫用または無権限による不正取得、不正利用、物理媒体による 個人データ ／ 保有個人情報 持出しや 個人データ ／ 保有個人情報 の送信などの不正行為 ②漏えい、入力ミス ③その他内部からの脅威	民間 →従業者の監督義務 (個法21条) 行政 →安全確保の措置 (行個法6条1項) →従事者の義務 (行個法7条)
3. 委託先 (元従事者 も含む)	①第三者による不正アクセス、ウイルス混入、物理的侵入など外部からの脅威 ②委託先 従業者 ／ 従事者 による不正取得、不正利用、漏えいなど委託先内部における脅威 ③再委託先の不正行為など	民間 →委託先の監督義務 (個法22条) 行政 →安全確保の措置 (行個法6条2項、7条)

(11)情報セキュリティ対策

1)(組織的安全管理措置)

* 管理体制

- 総括保護管理者(総務担当役員等1人)
 - **個人データ**／**保有個人情報**の管理事務の総括
- 保護管理者(各部課室等の長又はこれに代わる者1人)
 - **個人データ**／**保有個人情報**の管理
- 保護担当者(保護管理者が指定する者1人 or 複数人)
 - 保護管理者の補佐
 - 保有個人情報の管理事務
- 監査責任者(1人)
 - **個人データ**／**保有個人情報**の管理状況の監査
- 保有個人情報の適切な管理のための委員会
(関係**従業者**／**従事者**により構成・定期/随時開催)
 - **個人データ**／**保有個人情報**の管理に係る重要事項の決定、連絡・調整等

* 規程の策定: 保有個人情報(民間: 個人データ)の取扱い

- **アクセス制限**
 - アクセス権限: 必要最小限の付与(保護管理者)
 - 無権限アクセスの禁止(従業者/従事者)
 - 業務目的外アクセスの禁止(従業者/従事者)
- **複製等の制限**(従業者/従事者: 保護管理者の指示遵守)
 - 個人データ/保有個人情報の複製・送信・媒体の外部への送付/持出し等
- **誤りの訂正等**(従業者/従事者: 保護管理者の指示遵守)
- **媒体の管理等**(従業者/従事者: 保護管理者の指示遵守)
 - 個人データ/保有個人情報の記録媒体を定められた場所に保管
 - 必要があると認めるときは、耐火金庫への保管、施錠等
- **廃棄等**(従業者/従事者: 保護管理者の指示遵守)
 - 復元又は判読が不可能な方法により当該情報の消去・媒体の廃棄
- **取扱状況の記録**(保護管理者)
 - 個人データ/保有個人情報の台帳等を整備
 - 個人データ/保有個人情報の利用・保管等取扱い状況の記録

2011/3/3

2) 技術的安全管理措置

* 情報システムにおける安全の確保等

- **アクセス制御**(保護管理者)
 - 認証機能の設定等アクセス制御措置(パスワード、ICカード、生体認証等の導入)
 - パスワード等管理規定整備(定期・随時の見直し)、パスワード等の読取防止等
- **アクセス記録**(保護管理者)
 - アクセス記録の一定期間の保存
 - アクセス記録の定期・随時の分析
 - アクセス記録の改ざん、窃取、不正な消去の防止措置
- **外部からの不正アクセスの防止**(保護管理者)
- **コンピュータウイルスによる漏えい等の防止**(保護管理者)
- **暗号化**(保護管理者・従業者/従事者)
- **入力情報の照合等**(従業者/従事者)
 - 入力原票と入力内容との照合
 - 処理前後の保有個人情報の内容確認、既存の保有個人情報との照合等

2011/3/3

- **バックアップ**(保護管理者)
 - バックアップの作成、分散保管措置
- **情報システム設計書等の管理**(保護管理者)
- **端末の限定**(保護管理者)
 - 特定処理を行う端末限定等
- **端末の盗難防止等**
 - **保護管理者**: 端末の盗難・紛失防止のため、端末の固定、執務室の施錠等
 - **従業者/従事者**: 端末の持ち出し・外部への持ち込み禁止(保護管理者の事前許可制の採用等)
- **第三者の閲覧防止**(**従業者/従事者**)
 - ログオフの徹底等

2011/7

3) **物理的**安全管理措置

* **情報システム室等の安全管理**

- **入退室の管理**(保護管理者)
 - 情報システム室等・保管施設への入室権限の付与、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の**従業者/従事者**の立会い等
 - 情報システム室等の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置
 - 情報システム室等・保管施設の入退室管理(認証機能の設定等)
- **情報システム室等の管理**(保護管理者)
 - 不正侵入対策(情報システム室等への施錠装置、警報装置、監視設備の設置等)
 - 災害等対策(情報システム室等の耐震、防火、防煙、防水措置等)
 - サーバ等の機器の予備電源の確保、配線の損傷防止等の措置

4) **人的**安全管理措置

* **教育研修**

2011/7

PC支給の要件設定(シンクライアントは除く)	ノートPC	デスクトップPC
1. HDDパスワードの設定	○	△
2. BIOSパスワードの設定	○	○
3. 管理者権限の制限	○	○
4. 暗号ソフトの導入(デレトリ/ファイル)	○	○
5. ウィルス対策ソフトの導入	○	○
6. ファイアウォールソフトの導入	○	—
7. スパイウェア対策ソフトの導入	○	—
8. 総合監視ツール の導入	○*	○*
9. バイオ認証等の導入	△	△
10. VPNの設定(持ち出し用PC)	○	—

* 総合監視ツールによる「労働者のモニタリング」

(1) 基本的留意点

- (1)「労働者のモニタリング」が企業の円滑な運営上必要かつ合理的なものであること。
- (2)「労働者のモニタリング」の方法や態様が労働者の人格や自由に対する行きすぎた支配や拘束ではないこと。
- (3)「労働者のモニタリング」の必要性を欠いたり、「労働者のモニタリング」の方法や態様等が社会的に許容しうる限界を超えていないこと。
 - 社内規程の策定(就業規則の懲戒手続、禁止行為の明確化)
 - 労働組合への報告(労働者の十分な理解と協力)
 - 従業員への周知徹底(通年採用者含む。研修でも周知)

* 大学の場合: 研究者へのモニタリングは学問の自由との関係で別途検討が必要

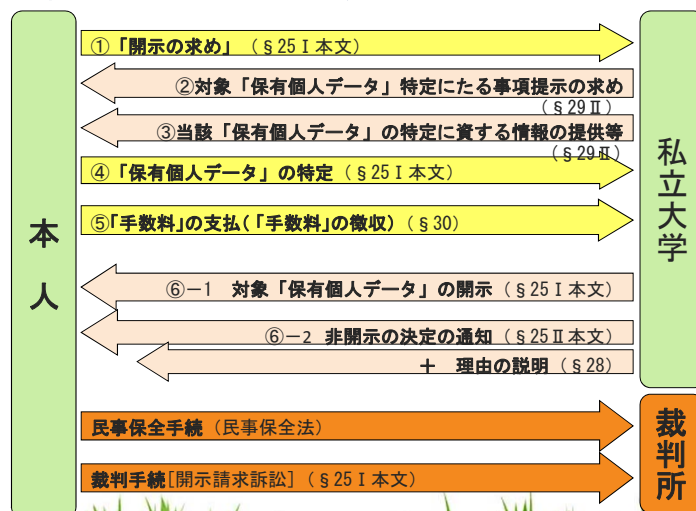
(2)総合監視ツールによる「労働者のモニタリング」に関する規程

- ①「労働者のモニタリング」の体制、及び管理者の任免・権限に関する事項
- ②「労働者のモニタリング」により取得するログ(個人情報)の特定
- ③「労働者のモニタリング」により取得するログ(個人情報)の「利用目的」の特定、及び「利用目的」の明示に関する事項
- ④「労働者のモニタリング」における装置等の稼動時間帯等(常時モニタリングの実施)に関する事項
- ⑤ 労働者からの苦情処理体制に関する事項
- ⑥ 禁止行為の(限定)列挙及び監視ツールの機能設定による実効性担保の措置
- ⑦ ログの保存期間に関する事項
- ⑧ 労働者からの開示・訂正・利用停止申請への対応に関する事項
- ⑨ 不正行為発覚時の対応(委託先との連絡を含む)、及び緊急対応に関する事項
- ⑩ 労働者に対する評価(従業員の懲戒)、及びその手続に関する事項

2011/7/7

(12)開示等

1)個人情報取扱事業者の場合



2011/7/7

*「開示等の求め」に応じる手続等に関する事項(法29条)

- ①「開示の求め」の対象となる項目
(「保有個人データ」の特定に資する情報)
- ②「開示等の求め」の申出先
- ③「開示等の求め」に際して提出すべき書面(様式)等
 - A. 所定の申請書
 - ・「保有個人データ」の利用目的照会申請書
 - ・「保有個人データ」開示申請書
 - ・「保有個人データ」変更等申請書
 - ・「保有個人データ」利用停止等申請書
 - B. 本人確認のための書類
- ④代理人による「開示等の求め」
 - A. 法定代理人の場合[未成年学生・成年学生]
 - B. 委任による代理人の場合(委任状・印鑑証明書)

2011/7

* 本人確認のための書類

- 運転免許証**(有効期限内のもので、各都道府県公安委員会発行のもの。国際運転免許証は除く。)の写し
- 学生証**(有効期限内のもので、氏名、顔写真、生年月日、住所が記載されているもの。)の写し。ただし、住所が記載されていない場合は、現住所が記載されている住民票、または現住所が記載されている公共料金領収証or請求書も添付して下さい。
- 旅券(パスポート)**(有効期限内のもので、氏名、顔写真、現住所が記載されているページを含む)の写し
 * 本人であることを確認できるものを次のうちから1点以上と現住所が記載されている**住民票**(3ヶ月以内のもの)、または、**現住所が記載されている公共料金の領収証**(3ヶ月以内のもの)もしくは、**現住所が記載されている公共料金の請求書**(3ヶ月以内のもの)を郵送。
- 健康保険証**(有効期限内のもの)の写し
- 障害者手帳**、**療育手帳**、または**精神障害者保健福祉手帳**(いずれも有効期限内のもので、氏名、現住所が記入されているページの写しは必須。)の写し
- 外国人登録証明書**(有効期限内のもの)の写し
- 米軍IDカード**(有効期限内のもの)の写し

2011/7

⑤「開示の求め」の手数料及びその徴収方法

⑥「開示等の求め」に対する回答方法

→原則：書面回答 例外：本人から同意を得た方法

⑦「開示等の求め」の対応で取得した個人情報の「利用目的」

⑧「個人データ」の不開示事由について

- a.申請書に記載されている住所・本人確認のための書類に記載されている住所・当社の登録住所が一致しないときなど本人が確認できない場合
- b.代理人による申請に際して、代理権が確認できない場合
- c.所定の申請書類に不備があった場合
- d.開示の求めの対象が「保有個人データ」に該当しない場合
- e.本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- f.当社の**業務の適正な実施に著しい支障を及ぼすおそれがある場合**
→具体化
- g.他の法令に違反することとなる場合

2011/3/3

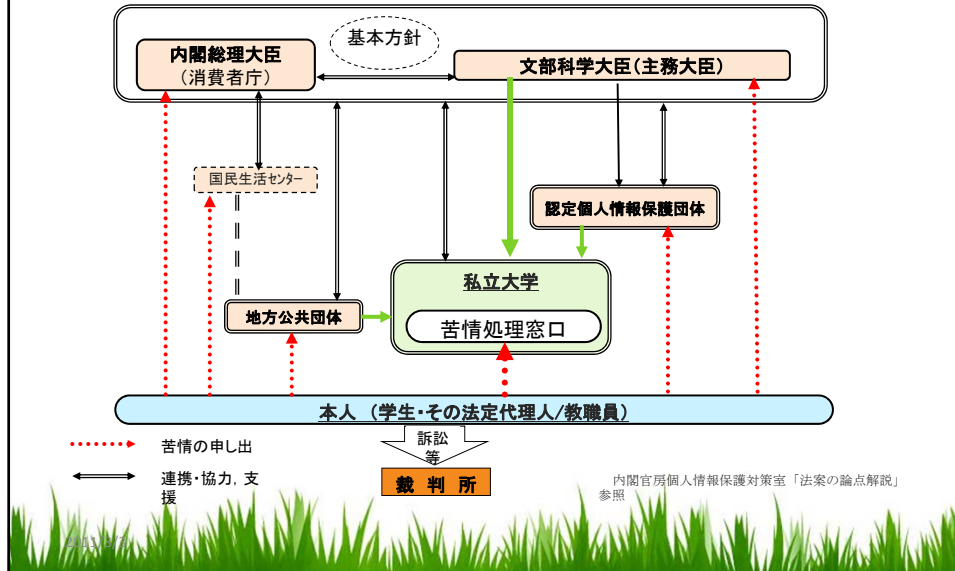
2) 行政機関の場合

個人情報保護法	行政機関個人情報保護法
第25条(開示)	第12条(開示請求権) 第24条(開示の実施) 第13条(開示請求の手続) 第25条(他の法令による開示の実施との調整) 第14条(保有個人情報の開示義務) 第15条(部分開示) 第16条(裁量的開示) 第17条(保有個人情報の存否に関する情報) 第18条(開示請求に対する措置) 第19条(開示決定等の期限) 第20条(開示決定等の期限の特例) 第21条(事案の移送) 第22条(独立行政法人等への事案の移送) 第23条(第三者に対する意見書提出の機会の付与等)
第26条(訂正等)	第27条(訂正請求権) 第32条(訂正決定等の期限の特例) 第29条(保有個人情報の訂正義務) 第33条(事案の移送) 第30条(訂正請求に対する措置) 第34条(独立行政法人等への事案の移送) 第31条(訂正決定等の期限) 第35条(保有個人情報の提供先への通知)
第27条(利用停止等)	第36条(利用停止請求権) 第40条(利用停止決定等の期限) 第38条(保有個人情報の利用停止義務) 第41条(利用停止決定等の期限の特例) 第39条(利用停止請求に対する措置)
第28条(理由の説明)	*行政手続法参照
第30条(手数料)	第26条(手数料)

2011/3/3

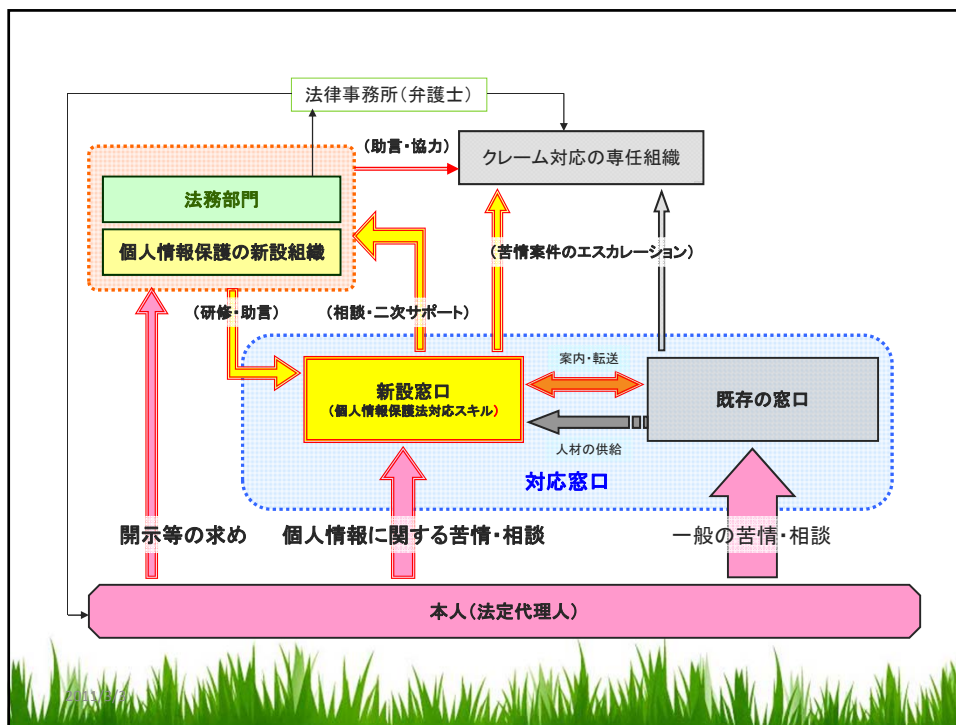
(13) 苦情処理に関する義務

1) 個人情報取扱事業者の場合



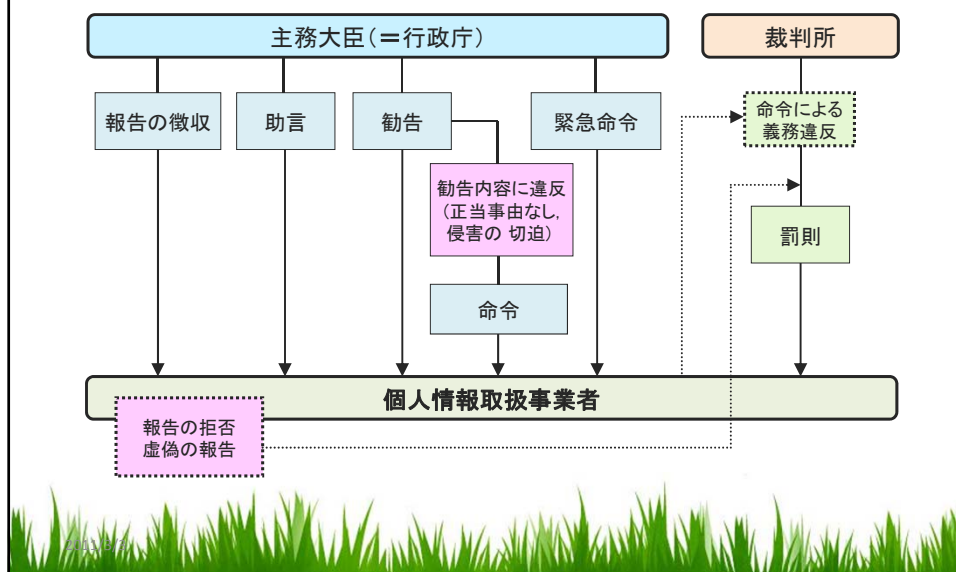
* 苦情処理のポイント

- ① 義務違反に対する苦情 (→コンプライアンス上の問題)
 - a. 「安全管理」義務違反 (個人情報保護法19条～22条関係)
 - 例1: 「個人データ」が漏えいしている! (→危機管理との連携)
 - b. 「利用目的」管理義務違反 (同法15条～18条・23条関係)
 - 例2: 「利用目的」の明示/通知・公表がない! (法18条)
 - 例3: 「利用目的」の内容が曖昧だ! (法15条1項)
 - 例4: 目的外利用をしている! (法16条1項)
 - 例5: 同意なく第三者提供をしている! (法23条1項・2項)
 - * 家族への回答 (家族の定義/開示範囲の明文化)
- ② 事実上の苦情 (→顧客満足度の問題 → JIS Q 15001の活用)
 - 例1: DM送付やテレマーケティングをやめてくれ!
 - 例2: 一度同意したが以後の第三者提供をやめてくれ!
 - 例3: どこから自分の情報を入手したのか?



(14) 罰則など

1) 個人情報取扱事業者の場合



2) 行政機関の場合

罰則

第五十三条 行政機関の職員若しくは職員であつた者又は第六条第二項の受託業務に従事している者若しくは従事していた者が、正当な理由がないのに、個人の秘密に属する事項が記録された第二条第四項第一号に係る個人情報ファイル(その全部又は一部を複製し、又は加工したものを含む。)を提供したときは、二年以下の懲役又は百万円以下の罰金に処する。

第五十四条 前条に規定する者が、その業務に関して知り得た保有個人情報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、一年以下の懲役又は五十万円以下の罰金に処する。

第五十五条 行政機関の職員がその職権を濫用して、専らその職務の用以外の用に供する目的で個人の秘密に属する事項が記録された文書、図画又は電磁的記録を収集したときは、一年以下の懲役又は五十万円以下の罰金に処する。

第五十六条 前三条の規定は、日本国外においてこれらの条の罪を犯した者にも適用する。

第五十七条 偽りその他不正の手段により、開示決定に基づく保有個人情報の開示を受けた者は、十万円以下の過料に処する。

