2019.02.06 秘密保護法・共謀罪廃止運動 レク・レジメ PIJ 石村耕治

秘密保護法廃止へ！実行委員会と共謀罪 NO！実行委員会共同開催学習会用レジメ・資料

【１９年２月６日/於：東京・衆議院第２議員会館第２会議室 13:30～】

巨大 IT 企業 GAFA 対策としての EU の一般データ保護規則(GDPR)を読み解く

～わが国は、「市民よ、GDPR を武器に GAFA と闘え！」の EU に学べるか？

石 村 耕 治

(PIJ/プライバシー・インターナショナル・ジャパン代表)

《レクチャー骨子》

■はじめに～問題の所在

１ 一目でわかる一般データ保護規則(GDPR)

２ 問われるわが国のプラットフォーマー(巨大 IT 企業)対応

３ EU の GAFA 対策が主眼の EU の GDPR(一般データ保護規則)の制定・施行

４「データローカライゼーション」とはどういった考え方なのか？

５ 個人情報保護法と個人情報保護委員会見直しのポイント

■むすびにかえて～グローバルIT企業独占資本主義、データ監視資本主義(data surveillance Capitalism)の潮流に乗れず、国家の庇護を求めるわが国IT企業

■はじめに～問題の所在

・経済のデジタル（電子）化の流れがグローバルに加速している。ビッグデータ/Big Data（巨大データ）、ML（機械学習）、AI（人工知能）、アルゴリズム/Algorism （自動情報処理手順）、インターネット・オブ・シングス/IoT（Internet of things/ 何でもインターネットにつなげる）といった横文字が飛び交うデータエコノミー中心の社会が目の前に広がる。

・こうした時代の流れを受けて、グローバルな巨大 IT 企業（デジタル・プラットフォーム企業）である 4 強（ビッグ 4）「ガーファ/ GAFA（グーグル[親会社はアルファベット]、アマゾン・ドット・コム、フェイスブック、アップル）は、全人類の約 8 割のパーソナルデータ（個人情報）を握るに至っているといわれる。わが国の IT 企業は束になっても、彼らと対等に競争するのは至難である。

(public use)

・「このままでは、世界中の市民や企業活動の首根っこを GAFA に掴まれてしまう。何とかしないといけない！」ということで、世界各国は大騒ぎである。

・こうしたなか、EU（ヨーロッパ連合）が採った策は、データローカライゼーションの視点に立って、新たなデータ保護法制を整備することで、個人の情報上のプライバシー権（個人情報の自己コントール権）を徹底的に保護することで GAFA 対策の核に据えるものである。

・つまり、一般データ保護規則（GDPR=General Data Protection）を制定・2018 年 5 月 25 日にすることで GAFA 対策を具体化させた。これは、EU が、プライバシーファースト、「市民よ！GDPR を武器に GAFA と闘え」の政策を選択したことを意味する。

・一方、わが国は、実質的に国を操る「個人市民に、徹底した個人情報の自己コントール権を認めるなどトンデモない。連中は、役人天国、IT 利権に歯向かってくる」との認識だ。相も変わらず「プライバシーファースト、冗談じゃないよ」のスタンスである。

・巨大なプラットフォーマーである 4 強・ガーファ/ GAFA が、熾烈なデータ覇権争い

を続けている。わが国の IT 企業は束になっても、彼らと対等に競争するのは至難である。にもかかわらず、お役人が立てた戦略では、“わが国は AI 大国を目指す”とか、絵空事を並べ立てている。グローバルな AI 化の荒波のなかで、わが国が具体的にどのようなスタンスで臨むつもりなのか、よくわからないものが多すぎる。

・データ寡占が競争政策上問題であるという視点にたち、独占禁止法で新たな 4 強・ガーファ/ GAFA 対策を打ち出すのはよい。しかし、独禁法ではなく、個人情報保護の強化で 4 強・ガーファ/ GAFA 対策を急ぐべきだと思うのだが。優先順位が違うのではないか。

・こうした政策順位決定は、「国内 IT 企業ファースト、市民/国民の人権保護ラスト」の認識からくるものと思われるが、大きな疑問符がつく。

・お役人は、企画を立て、仕事をつくることが大好きだ。しかし、企画倒れ、血税のムダ遣いに終わるものも多い。

・お役人が立てた戦略では、“わが国は AI 大国を目指す”とか、絵空事を並べ立てている。グローバルな AI 化の荒波のなかで、わが国が具体的にどのようなスタンスで臨むつもりなのか、よくわからないものが多すぎる。

・問題は、彼らは、失敗しても、国民に対して責任を取らないことだ。こうした傾向は、IT 戦略関係では、とくに顕著だ。

・そこで、今回は、市民/国民目線で、わが国は、「市民よ、GDPR を武器に GAFA と闘え!」の EU に学べるか?点検してみる。

【図表1】 わが国の最近のデータ政策の流れを追う

- 政府は、2018 年 9 月 28 日、関係閣僚会議を開いた。そこで、人工知能(AI=artificial intelligence)の本格的な導入にむけた総合戦略の策定に着手した。
- これまでの AI の政府計画は、成長戦略の一部にとどまっており、その進め方が不透明との指摘もあった。
- そこで、今回は、IT 総合戦略本部や知的財産戦略本部など政府の科学技術関連の会議を実質的に、イノベーション会議に一元化し、官邸主導で AI 戦略をとりまとめる。政府の AI 総合戦略には、今後 3 年間の関連施策を盛り込む。
- 政府の AI 総合戦略では、AI 開発を担う人材育成のための学校教育改革や、農業や健康・医療・介護、国土強靭化/物流といった産業の ICT(情報通信技術)化を進める。
- 今国会に「デジタルファースト法案」を提出し、成立を図る方向だ。だが、この法案では、徹底した市民/国民のプライバシー保護で、グローバルな巨大 IT 企業である 4 強(ビッグ 4)・ガーファ/ GAFA【グーグル[親会社はアルファベット]、アマゾン・ドット・コム、フェイスブック、アップル】や中国 ICT(情報通信技術)界に君臨する 3 強(Big 3)【バイドゥ(Baidu/百度)、アリババ(Alibaba 阿里巴巴)、 テンセント(Tencent/騰訊)】と対峙できる内容になるかどうかは不透明。

・法案成立後、日本が議長国を務める 2019 年の 20 か国・地域(G20)首脳会議で AI・ICT の取り組みを世界に発信するという。AI を政権の成長戦略の核に位置づけ、19 年 4 月にとりまとめる。G20 で発表し、わが国への AI 投資の積極的な姿勢をアナウンスするとのことだ。勇ましい限りである。だが、EU をはじめとした個人市民のプライバシー保護を強力に打ち出している諸国の失笑を買わないか心配である。

・加えて、政府は、18 年 7 月に、政府 3 機関(経産省・総務省・公正取引委員会)が参画した「デジタル・プラットフォーマーを巡る取引環境整備の関する検討会」を設置し、9回の会合を経て、18年12月12日に、「中間論点整理」(中間報告)を公表した。中間報告では、データ寡占が競争政策上問題であるという視点にたち、独占禁止法で新たな 4 強・ガーファ/ GAFA 対策を打ち出している。EU にならい、個人情報保護法制を市民目線で改正し、個人市民に強力な情報上のプライバシー(個人情報の自己コントロール権)を付与することには消極的な姿勢である。

・総務省は、電気通信事業法上の「通信の秘密」を持ち出して GAFA 対策を急ぐという。

1 一目でわかる一般データ保護規則(GDPR)

■新規則は2018年5月25日に施行

・一般データ保護規則 (GDPR＝General Data Protection Regulation (EU) 2016/679/以下「データ保護規則」、「規則」またはGDPR) は、2018年5月25日に施行した。データ保護規則 (GDPR) は、欧州経済領域 (EEA=European Economic area)、つまり、EU (欧州連合) 加盟国＋ノルウェー・リヒテンシュタイン・アイスランド (以下、たんに「加盟国」ともいう。) に適用になる。

・これまでのEUデータ保護指令 (Data Protection Directive 1995 (95/46/EC)) (以下「データ保護指令」または「指令」) に代えて、データ保護規則 (GDPR) を利用することは、における個人データ保護制度の調和の促進をねらいとしていた。しか、加盟国に認められる数多くの特例があった。加えて、各加盟国は、データ保護規則 (GDPR) の規定について、さまざまな解釈が可能であり、執行もそれぞれ異なってくる可能性があった。

・EU市民の個人データ (わが国の個人情報に相当します。) を電子処理したうえで、EU域内から域外へと流通させることを「クロスボーダー処理/越境処理 (cross-border processing)」と呼ぶ。企業または企業グループが行うクロスボーダー処理/越境処理については、原則として、その企業の「主たる施設 (main establishment)」、つまり主たる事業所の置かれている加盟国の監督機関 (SA=supervisory authority) /データ保護機関 (DPA=data protection authority) が管轄する。

【図表２】指令から規則への移行に伴う主な変更点

データ保護指令)

【2018 年 5 月 25 日前まで】

◎指令はモデル法のような存在で、データ保護は、各加盟国が制定した国内データ保護法による。

◎個人データ処理に関する個人保護作業部会(指令 29 条作業部会)の設置

◎情報プライバシー権の確立

◎各加盟国が国内法に盛り込む法的規制の枠踏みを提示

⇒

データ保護規則(GDPR)

【2018 年 5 月 25 日に施行】

◎各加盟国のデータ保護法は、監督機関に関する部分を除き、原則廃止。規則（GDPR）を直接適用する(ただし、雇用・ジャーナリズム・研究などは、各加盟国の立法によることができる。)

◎指令 29 条作業部会は、欧州データ保護委員会(EDPB)に改組

◎個人の法的権利(個人データの自己コントロール権)の強化

◎規制(データ保護が十分でない第三国・地域への個人データ移転の原則禁止など)および制裁(違法行為には巨額の過料)の強化

◎監督機関制度の改正(各加盟国の監督機関と主管監督機関

■データ保護規則(GDPR)の域外適用

・データ保護規則（GDPR）は、原則として、EU域内にある営利企業（個人/法人を営利事業者）のみならず、加盟国の国や地方の機関（エージェンシー/独立行政機関を含む。)、非営利公益団体など（以下「企業など」という。）にも広く適用になる。

・データ保護規則（GDPR）は、原則として、EU域内に限り適用になる。

・しかし、データ保護規則（GDPR）は、EU域外にあっても、EU域内に物品やサービスを提供するまたはEU域内に居る個人を追跡する企業にも適用になる。

・こうしたEU域内に主たる施設（main establishment）を有しない（EU域外）企業は、原則として、EUに管理者または処理者の代理人（representatives）を置くように求めている。そして、その企業がデータ保護規則（GDPR）に違反した場合には、その代理人が責任を負うことになっている

■子どもの個人データ保護

・ネットサービス、オンラインサービスに関し、子どもからの同意については、その親権者の承諾が必要です。この場合の子どもとは、16歳未満の人を指す。ただし、各加盟国は、13歳未満に引き下げることもできる。

・データ保護規則（GDPR）は、欧州司法裁判所（ECJ）の裁判例で認められた「忘れられる権利/忘れてもらう権利（right to be forgotten)」【詳しくは、CNNニューズ78号参照】を法認した。子どもについては、成人よりも厳格な保護措置を置いた。

■中核となる個人データ保護ルールは規則も指令も不変

・データ保護規則（GDPR）は、データ保護指令が定めた中核となる個人データ保護ルール、個人データ保護ルールを継承し、必要な保護強化策を講じている。

・個人データの保護に関係する人を、管理者（controller）または処理者（processor）と呼びます。処理者は、管理者の指揮の下で事務を行うことになる。企業によっては、管理者と処理者は同一であることもある。

・あらゆる個人データの処理にあたっては、個人データ保護の6つの基本原則〔**①合法性、公正性および透明性（lawfulness, fairness and transparency)、②目的制限（purpose limitation)、③データ最小限性（data minimisation)、④正確性（accuracy)、⑤保管制限（retention)、⑥清廉性および機密性保持（integrity and confidentiality)**〕を遵守し、かつ処理要件を充たすように求められる。

・従来からセンシティブデータ/機微データ/特別類型個人データの開示は原則禁止とされてきているが、データ保護規則（GDPR）では、この種の個人データとして、新たに遺伝子データと生体認証データを追加した。加盟国によっては、遺伝子データと生体認証データの処理については、制裁を強化したうえで厳格な規制を加えている。

■個人データ取得の際の同意の厳格化

・EUにおいては、個人データを取得する際に、それが適法でありためには、「その個人（データ主体）から同意（consent）を得る」ということは、誰もが知らなければならない基本中の基本である。

・この同意に関する基本ルールが、データ保護規則（GDPR）では、「個人（データ主体）はいつでもその同意を撤回できる」こととされ、大きく変わった。

・従来から、センシティブデータ/機微データ/特別類型個人データの処理を行う場合のデータ主体からの同意は、明示的（explicit）でなければならいとされてきた。つまり、黙示の同意ではデータ処理は許されないわけである。これが、データ保護規則（GDPR）では、EU域外へのセンシティブデータの移転（輸出/持出し）にあたっても、データ主体からの明示の同意を得なければならないことになった。

■データ主体の権利拡大

・EUにおいては、従来から、個人（データ主体）が自己データにアクセスする権利（自己データの開示を求める権利)は広く認められてきた。加えて、データ保護規則(GDPR)では、不正確な自己データの訂正を求める権利、自動化された処理のみに基づく決定の対象とならない権利（Automated individual decisions）を法認した。このことから、プロファイリングを含む自動化された決定に対し、データ主体は異議をとなえることができる。また、自分の個人データがダイレクトマーケティング（DM）に使用されることの拒否を通知する、ダイレクトマーケティンを拒否する権利（right to object direct marketing)」も法認した。

・さらに、データ保護規則（GDPR）では、新たなデータ主体の権利として、欧州司法裁判所（ECJ）の裁判例で認められた「忘れられる権利（right to be forgotten)」（削除権）を法認した。また、自己の個人データ管理者に対して、一定のフォーマットで受け取り、他の管理者に移転・利用する権利（持運び権/ポータビリティ権/right to data portability）を法認した。これら新たなデータ主体の権利は、実務的のはいまだ固まっていない権利あり、定着するのは、かなりの歳月が必要と思われる。

■プライバシー通知

・従前から、個人データを利用する企業などは、本人（データ主体）に対するプライバシー通知（privacy notice）を義務づけているが、データ保護規則（GDPR）では、本人（データ主体）に伝達すべき情報の範囲を拡大した。また、プライバシー通知は、簡潔かつ分かりやすいものでなければならない。

・データ保護規則（GDPR）では、企業などがプライバシー通知にあたっては、標準的なアイコン（図柄）を利用するようには明確に義務付けていない。しかし、欧州委員会（European Commission)は、標準的なアイコンを導入する方向で検討を進めている。

■説明責任

・データ保護規則（GDPR）は、個人データを取り扱う企業などに対して、6つの基本原則を遵守するように求めるとともに、その企業がそれら基本原則を遵守していることを証明するように求めている。

・企業などは、個人データの「ハイリスク処理（high risk processing)」を行う場合には、事案によっては、所轄の監督機関と協議を行ったうえで、プライバシー影響評価（privacy impact assessment)【日本でいう特定情報保護評価に相当】を実施するように求められる。

■データ保護責任者

・データ保護規則（GDPR）は、定期的に大量の個人データを取り扱う企業などに、データ保護責任者（DPO=data protection officer）を置くように求めている。データ保護責任者（DPO）は、あらゆるデータ保護問題に対応するように求められる。
・データ保護責任者（DPO）は、個人データ管理者や処理者からの独立性や強い地位と権限が付与されており、その意に反して解任される、あるいは処罰されることはない。
・データ保護責任者（DPO）は、報告を行う場合には、所属する企業などの最高位の経営陣に直接することになっている。

■個人データの安全性

・データ保護規則（GDPR）は、企業などに対して、暗号を用いるなどして、個人データの安全性（data security）を確保するように求めている。
・企業などの個人データ管理者（controller）は、データ漏えいが生じた場合には、所轄の監督機関（SA）/データ保護機関（DPA）に通知・報告するように求められる（ただし、その漏えいが個人データなどに危険が及ばないときは除く。）。通知・報告は、原則として、その発生から72時間以内にするように求められる。また、その漏えいにより影響を受ける特定個人（データ主体）に対しても通知するように求められる。

■個人データ処理者

・データ保護規則（GDPR）では、企業などの個人データ処理者（controller）に対して直接適用にある規定を置いている。これは、旧データ保護指令のもとで、企業などが、処理者の地位をアレンジするなどで法規制を回避できるようにする慣行が目立ったためである。
・データ処理者は、データ主体から損害賠償を求められた場合には、独自に、またはデータ管理者と共同で責任を負うことになる。

■EU域外への(越境)個人データの移転

・データ保護規則（GDPR）では、①移転先の国がEUと同水準の個人データ保護法制を敷いている、あるいは②EUから国として「十分性の認定」を受けるなど法定のルールにあてはまる場合を除き、EU市民の個人データをEU域外へ移転（持出し）することを原則禁止している。個別の企業が、これら法定のルールを充たす、あるいは欧州委員会から十分性の認定（決定）を受け例外要件を充たしたうえで、個人データをEU域外へ移転（持出す）こともできる。しかし、実務的にもかなりの困難が伴う。そこで、わが国の個人情報保護委員会（PPC）は、EU側と協議のうえ、②EUから国として「十分性の認定」のお墨付を得、このお墨付きの枠組みは2019年1月23日に発効した。個人市民のためよりは、法人企業のためにはよく働く個人情報保護委員会（PPC）の姿が

浮き彫りになっている。

■GDPR の適用・執行の枠組み

・データ保護規則（GDPR）は、これまでのデータ保護指令（DPD）とは異なり、加盟国に対して直接適用になる。しかし、GDPR の適用と執行は、EU が直接行うのではなく、従前と同様に、基本的には各加盟国の権限ある（所轄の）監督機関（competent AS=competent supervisory authority）の手に委ねている。

・その一方で、GDPR は、EU 域内にあるすべての監督機関(SA)のよる①協力（OSS）メカニズム/ワンストップショップ体制（OSS=one -stop-shop mechanism）および①統一性メカニズム/統一性のある執行体制（consistency mechanism）の確立を目指している。

◆監督機関の権限

・データ保護規則（GDPR）は、各加盟国の監督機関（SA）に対して、調査権限、是正権限、承認・勧告権限、過料をかす権限を付与している。このことから、監督機関（AS）が個人データの管理者/処理者に対して、データ保護規則（GDPR）に違反する疑いがある場合には、調査を実施すること、また、任務遂行のために必要な情報の提供を命じることができる。個人データ処理が適法に行われていない場合には管理者/処理者に対し警告を行うこと、データ主体からの求めに応じて、管理者/処理者に命令を行うこと、個別の事案の事情に応じて過料（administrative fines）を賦課すること、個人データの越境処理/クロスボーダー移転に関して拘束的企業基準による第三国や地域へのデータ移転の承認（決定）などを行うことができる。

◆協力/ワンストップショップ体制の確立

・ワンストップショップ制度は、複数の加盟国内に施設（establishment/子会社・支店・営業所などの事業所）を有する企業などの管理者/処理者の処理を担当する監督機関の協力体制を組むことをねらいとしている。原則として、管理者/処理者の主たる施設（main establishment）が所在する国の監督機関が、主管監督機関（Lead SA）となります。主管監督機関（Lead SA）は、管理者/処理者にとって、個人データの越境処理/クロスボーダー処理が関係する場合には、唯一の窓口となる。主管監督機関（Lead SA）は、各加盟国に所在する当該企業の施設を所管する関係監督機関（concerned SAs）と協力してデータ保護規則（GDPR）の統一的な適用・執行にあたることになる。

・もっとも、関係監督機関（concerned SAs）は、データ保護規則（GDPR）違反の嫌疑があり、それが自己の国内企業などにのみ関係するような場合、または自己の国内の

データ主体にのみ実質的な影響が及ぶような場合には、当該関係監督機関が権限を持つ。

◆統一性のある執行体制の確立

・統一性のある執行体制（consistency mechanism）とは、各加盟国にある監督機関(SA)間の協力体制を整え、データ保護規則（GDPR）の統一のとれた適用・執行を確保するための仕組みを指す。新たに欧州データ保護委員会（EDPB=European Data Protection Board ）が立ち上がり、それまでテータ保護指令（DPD）のもとで第 29 条作業部会が担っていた諮問機関としての機能を受け継いだ。EDPR は、各 EU 加盟国の監督機関(AS)の長などからなり、事務局は欧州データ保護監督官（EDPS=European data protection supervisor）が主宰する。EDPS は、データ保護指令（GDPR）の適用・執行に関するガイドラインの発出、諮問機関や裁定機関として職務権限の行使をする責任を負い、その際には、独立して判断をくだすように求められている。

・EDPS は、データ保護規則（GDPR）の適用・執行に影響を及ぼす判断を監督機関（SA）が行う場合、例えば、監督機関（SA）が複数の加盟国における処理行為に関連する行動規範の承認（決定）を行う場合などに、承認（決定）草案に対して非拘束的な意見を述べることができる。EDPB は、監督機関（SA）の間で決定草案に関する意見の相違がある場合や、諮問が義務づけられているのにも拘わらす監督機関（SA）が EDPB に意見を求めなかった場合、その意見に従わなかった場合には、自ら拘束力のある判断をくだすこともできる。

■権利侵害と争訟手続

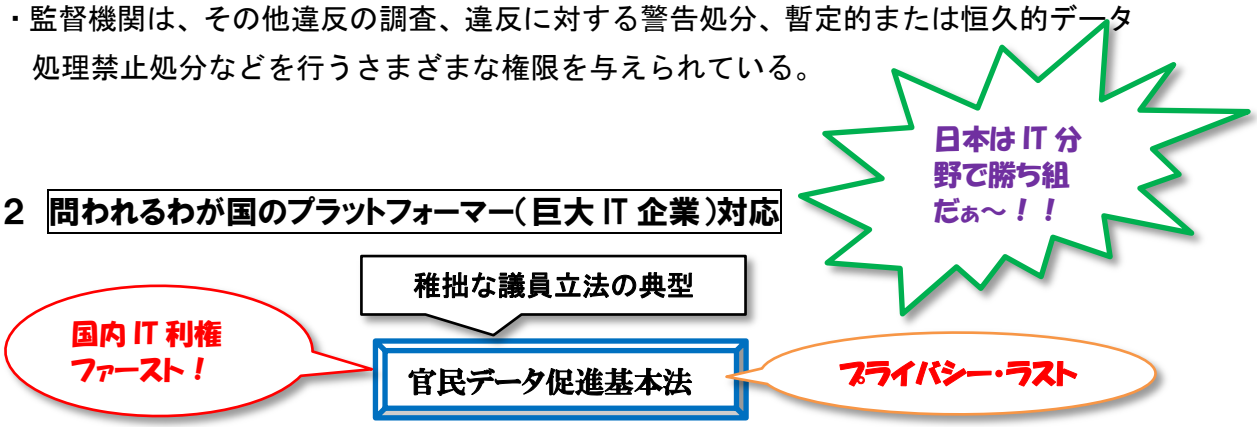
・個人（データ主体）は、データ保護規則（GDPR）違反で自分の権利が侵害されていると疑う場合には、権限ある/所轄の監督機関（SA）に不服を申し立てる権利（right to lodge a complaint with a supervisory authority）を有している。また、個人（データ主体）は、監督機関の法的拘束力ある決定に不服な場合には、その監督機関相手に、その決定処分の取消を求めて裁判で争う権利（right to an effective judicial remedy against a supervisory authority）を有している。不服申立前置主義が採られていないので、個人（データ主体）は、不服申立てを経ずに、直接司法裁判所に訴訟を提起することもできる。さらに、個人（データ主体）は、データ管理者またはデータ処理者によるデータ保護規則（GDPR）違反により損害を受けた場合には、賠償を求めて裁判で争う権利(right to an effective judicial remedy against a controller or processor）を有している。

■制裁

・企業などが、データ保護規則（GDPR）に違反した場合、所轄の監督機関は、その違反の種類に応じて、制裁の１つとして、①全世界年間売上高の2%か、1,000万ユーロのいずれか高い方、あるいは、①全世界年間売上高の4%か、2,000万ユーロのいずれか高い方（ただし、売上高のない公的機関などの違反の場合は、いずれの場合もユーロ基準で）の過料（administrative fines）をかすことができる。

・監督機関は、その他違反の調査、違反に対する警告処分、暫定的または恒久的データ処理禁止処分などを行うさまざまな権限を与えられている。

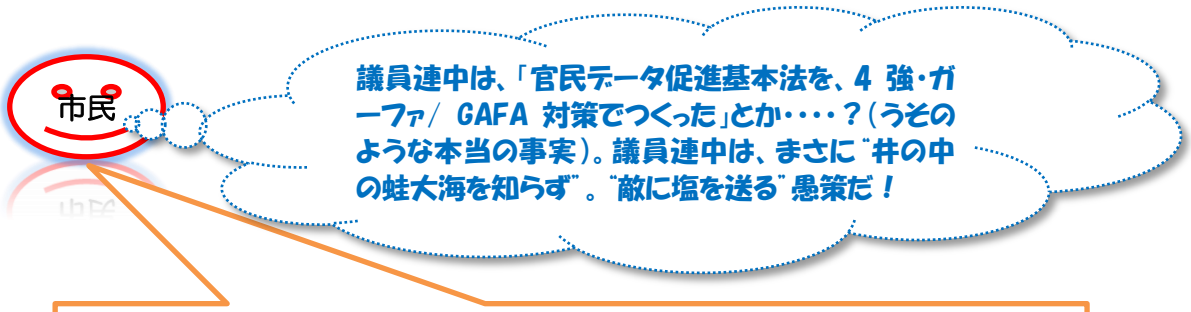
2 問われるわが国のプラットフォーマー(巨大 IT 企業)対応



【図表2】稚拙な官民データ促進基本法(2016 年 12 月 7 日に議員立法で成立)

- 「官民データ促進基本法」は、はじめて「AI(人工知能)」、「IoT(インターネット・オブ・シングス)」、「クラウド・コンピューティング・サービス」などを定義。さらに、国・自治体のデータの活用促進のため、システムの規格統一や互換性の確保などをうたう。
- しかし、プライバシー(個人情報)を大事にしたいという市民/納税者が持つ時代感覚から大きく乖離した稚拙な法律
- 国民背番号であるマイナンバーを搭載した IC カードを持たせ、全国民の個人情報(プライバシー)の実質的に公有化促進をうたう。
- 政府が、わが国の民間企業による全国民の個人情報(プライバシー)の自由なビジネス利用を後押しイケイケドンドンする方針をうたった法。グローバルな競争の視点が欠如。

(public use)



・官民データ促進基本法のような、政治主導で、野放図に IT 利権ファースト、プライバシーゼロ社会の形成を後押しするような法律は、「悪平等」そのもの。
・全人類の個人情報の 8 割を握る 4 強・ガーファ/ GAFA(グーグル[親会社はアルファベット]、アマゾン・ドット・コム、フェイスブック、アップル)は、わが国民の個人情報をガーファ/ GAFA の餌食にする"呼び水"的な役割を果たす。
・まさに、グローバルにみると、データ覇権争いなどの思考がまったくない、稚拙な法律といえる。


(public use)

国民に強固なプライバシー権を法認して、4 強・ガーファ/GAFA と対峙できるようにする政策が求められる!

・わが国市民の個人情報/プライバシーは、市場競争と法の支配のルールを逆手に取った 4 強・ガーファ/GAFA に食いちぎられてしまう。4 強・巨大なジョーズを相手に国民の個人データを撒き餌にするような、稚拙な議員立法には、本当にあきれる。
・その後の政府の AI 総合戦略でいう「データの自由な流通による産業の活性化を目指す」は、聞こえは悪くない。わが国の IT 企業に利点があるようにはみえる。だが、現実には、悪平等につながり、巨大なジョーズのような 4 強・ガーファ/ GAFA を利するだけ。

3 EU は GAFA 対策が主眼の GDPR(一般データ保護規則)を制定・施行

・EU(欧州連合)は、GDPR(一般データ保護規則)を制定・施行し、【図表3】のような市民の個人データ上の権利を法認した。
・その狙いは、プライバシー権、個人データの保護を強化し、個人市民に武器を与えることにより、強大なデジタル・プラットフォーム企業である4強・ガーファ/GAFAなどに挑戦するように求めること。

【図表３】EUのGDPRで法認したプライバシー権（個人データの自己コントロール権）

・個人（データ主体）は、いつでも個人データの取得の際にした**同意（consent）の撤回**ができる（GDPR７条以下）。

・個人（データ主体）は、自己データにアクセスする権利（自己データの開示を求める権利）に加え、データ主体に対し**忘れられる権利**（right to be forgotten）、いわゆる「削除権」を法認した（GDPR17条）。

・プロファイリング等の「自動処理のみに基づく自動意思決定（automated individual decision）」を規制するために、**自動処理のみに基づく決定（automated decision making）には服さなくともよい権利**（GDPR22条）を法認した。ただし、例外的に、次の3つの場合に限り、自動処理のみに基づく決定がゆるされる（GDPR22条2項）。

ⓐデータ主体とデータ管理者との間で、契約の締結または履行に必要とされる場合

ⓑEU法または加盟国法が、データ主体の権利を適切に保護し、かつ自動処理のみに基づく決定を法認している場合、または、

ⓒデータ主体の明示の同意がある場合

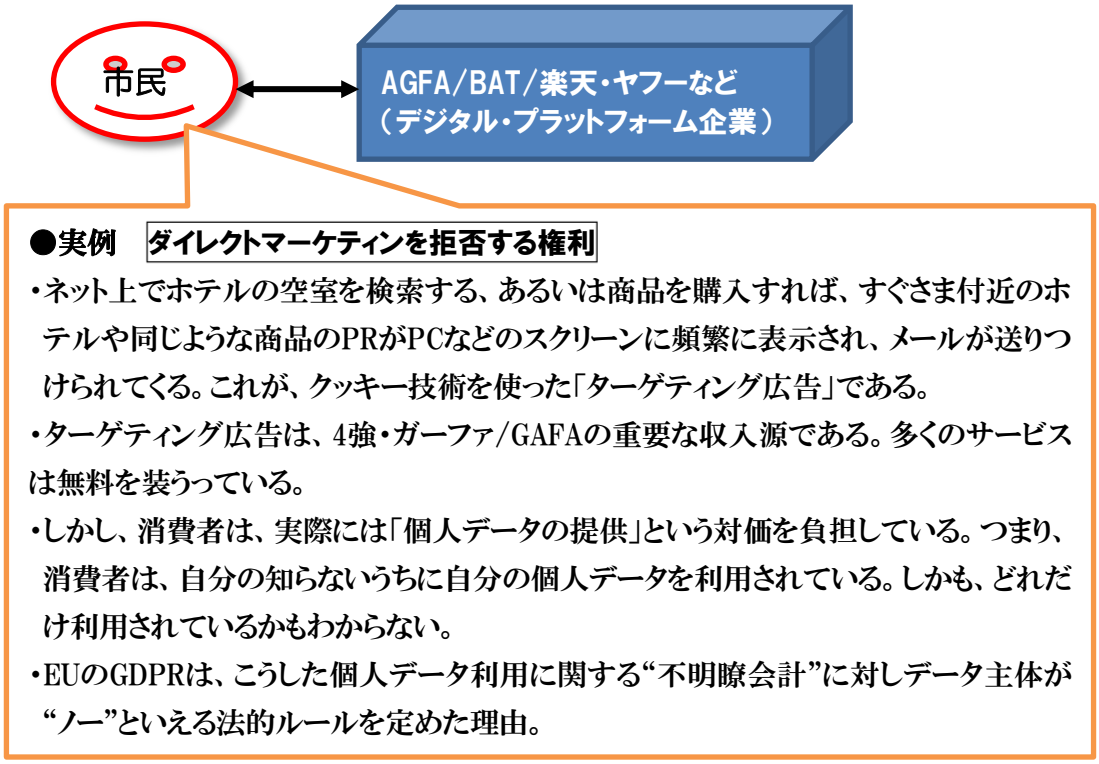
このことから、プロファイリングを含む自動化された決定に際し、実施主体は、事前にデータ主体に実施内容を通知するように求められる（GDPR第１３条、２２条１項・２項）。また、自動処理のみに基づく決定には服さなくともよい権利の侵害がある場合には、データ主体は、監督機関の苦情の申出をする権利（GDP77条）、および監督機関や実施主体を相手に司法救済を求める権利（GDPR78条・79条）がある。

・自分の個人データがダイレクトマーケティング（DM）に使用されることの拒否を通知する、**ダイレクトマーケティングを拒否する権利**（right to object direct marketing）」も法認した（GDPR21条）。

・**EU市民の個人データのEEA域外への輸出（持出し/移転）を原則禁止**したうえで、欧州委員会が、EU並みの個人情報保護水準に達していると認定（決定）した第三国・地域に限って、輸出（持出し/移転）が認める仕組みにした（GDPR44条～50条）。

・**データポータビリティ権**（ right to data portability）【あるサービスが特定のユーザーに関して収集・蓄積した利用履歴などのデータ（個人データ）を他のサービス、プラットフォーマーでも再利用できること、すなわち持ち運びできる（＝ポータビリティ）権利】を法認した（GDPR20条）。

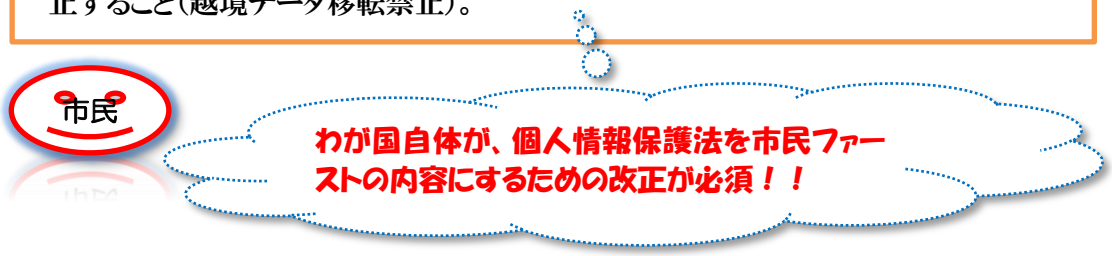
◆クッキー技術を使ったターゲティング広告規制のケース



4 「データローカライゼーション」とはどういった考え方なのか？

◆わが国でのデータローカライゼーションの具体策

・データ主体(市民/納税者)に、EU の GDPR(一般データ保護規定)並みの個人情報の自己コントロール権を法認すること。
・わが国市民の個人情報データのコピーを国内のサーバーで保存を義務づけること(サーバーの国内設置義務)。
・真に独立した個人情報保護組織を持たない国への個人情報データの国外移転を禁止すること(越境データ移転禁止)。

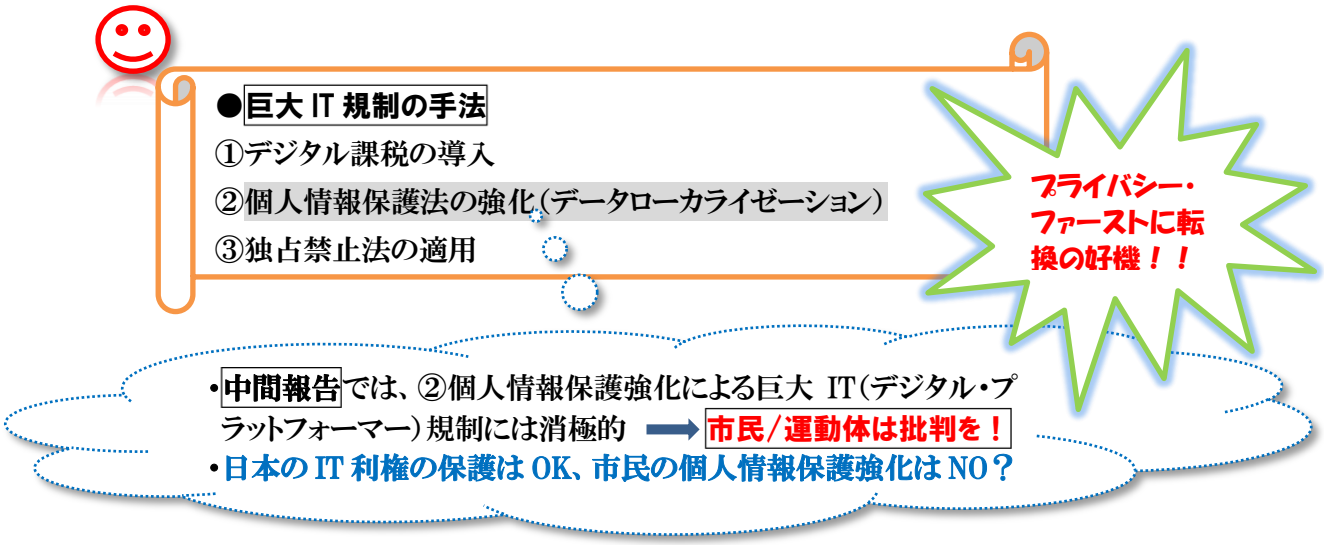


◆政府の巨大 IT 規制検討会「デジタル・プラットフォーマーを巡る取引環境整備の関する中間論点整理」(中間報告/2018 年 12 月 12 日)

●巨大 IT 規制に向けた政府規制の動き

・わが国政府 3 機関(経産省・総務省・公正取引委員会)が 18 年 7 月に設置した「デジタル・プラットフォーマーを巡る取引環境整備の関する検討会」が、9回の会合を経て、18年12月12日に、「中間論点整理」(中間報告)を公表。
・中間報告では、「ICT やデータを活用して第三者に「場(プラットフォーム)」を提供する"デジタル・プラットフォーマー"である GAFA、BAT【バイドゥ (Baidu/百度)、アリババ (Alibaba 阿里巴巴)、テンセント (Tencent/騰訊)】、楽天・ヤフーなどに包括的な政府規制をかけることが狙い。
・デジタル市場における公正・自由な競争の実現 ➡ GAFA など巨大 IT の優越的地位濫用に公正取引委員会が独禁法による規制が中核。
・総務省は、GDPRに倣って、外国IT企業に代理人設置の義務化を提案。しかし、肝心の市民のプライバシー権強化には無関心

GDPRでは、EU域内に恒久的施設(permanent establishment)を有しない(EU域外)企業は、原則として、EUに管理者または処理者の代理人(representatives)を置くように求めている。そして、その企業がデータ保護規則(GDPR)に違反した場合には、その代理人が責任を負うことになっている(GDPR27条)。



5 個人情報保護法と個人情報保護委員会見直しのポイント

◆EU の一般データ保護規則 (GDPR) を見習おう

3 階建のわが国の個人情報保護法制

①個人情報保護法(民間分野)
②行政機関個人情報保護法(国の公的分野)
③独立行政法人等個人情報保護法(公的分野)

民間と公的セクターとを別建てとする方式(セクトラル方式/セグメント方式)

1階建の EU の GDPR

一般データ保護規則(GDPR)(公民双方分野)

オムニバス方式

・EU の一般データ保護規則 (GDPR) は、個人データ (個人情報) の取得/収集の際の同意の厳格化【データ主体の同意の撤回権の保障など】に加え、いわゆる“ビッグデータ”の利活用にも法的規制。
・GDPR 営利企業はもちろんのこと、国や地方団体などにも適用。つまり、オムニバス (公民双方に適用する) 方式を採用。一方、日本の国の個人情報保護法は、民間と公的セクターとを別建てとする方式 (セクトラル方式/セグメント方式) を採用

【図表４】 主なプライバシー保護方式の類型

①**オムニバス方式** 1 つの法律を公的セクターと民間セクター双方に適用する方式。「統合方式」とも呼ばれる。【採用例：EU 諸国、豪州、NZ、日本の自治体条例など】

②**セクトラル方式** 公的セクターと民間セクターにそれぞれ別の法律を適用する方式。【採用例：アメリカ、韓国、日本（国の法律）、など】

【注】(a)セクトラル方式と(b)セグメント方式とは、別の類型方式としてとらえる考え方もある。こうした考え方のもとでは、(a)セグメント方式とは、公民セクターに別の法律を適用する方式（分離方式）であるのに対して、(b)セクトラル方式とは、公民それぞれのセクターについて、特定の分野で保護措置を講じる方式（個別分野別方式）をして分類・類型化することになる。しかし、ここでは、「セクトラル方式」とは、広義にセグメント方式を含み意味でとらえている。

◆わが国の国レベルの個人情報保護法はどんな方式なのか？

わが国は、自治体条例レベルでは、オムニバス方式を基本とする個人情報保護法制を維持している。一方、国レベルでの個人情報保護法制はセクトラル方式を基本とする考え方を維持してきている。

基本法である国の個人情報保護法（改正法の 2017 年 5 月 30 日の全面施行後のもの）は、第 1 章～第 3 章までの基本法の部分は、民間機関に加え、国や自治体にも適用になる。しかし、第 4 章以下（一般法）は、原則として、国や自治体には適用にならない。番号法で設置されていた特定個人情報保護委員会は、2015 年 9 月に成立した改正個人情報保護法により、個人情報保護委員会に改称・改組され、個人情報保護法第 5 章（59 条～74 条）に根拠に活動する、国家行政組織法 3 条に基づくいわゆる「三条委員会」となった(18 年 8 月現在スタッフ 119 人)。個人情報保護委員会が、個人情報保護法第 5 章を根拠としているということは、この委員会は、もっぱら民間機関の個人情報保護を任務とした機関であることを意味する。

◆個人情報保護委員会には、行政による個人情報取扱いに対する苦情の申出ができないわけは？

総務省自治税務局市町村税課が、自治体に対し、自治体が、事業者に送る住民税の特別徴収税額決定通知書への従業者や役員本人および扶養家族全員の個人番号を記載するように求めたことで大騒ぎになった。財界が中に入って総務省の蛮行は止まった【詳しくは「財界が止めた自治体による勤務先へのマイナンバーの垂れ流し」CNN ニューズ 93 号参照】。

市民団体は、個人情報保護委員会（委員会）は何をやっているのかと問い糾した。しかし、委員会は、こうした苦情を請けつけなかった。この背景には、委員会は、もっぱら民間機関の個人情報保護を任務とした機関であることがある。つまり、委員会は、こうし

た市民団体からの行政による個人情報取扱いに対する苦情の申出を受けたり、それに従い国の行政機関や自治体を指導できないような法的仕組みになっているからである。これは、国の行政機関とか自治体などは、個人情報保護法上の個人情報取扱事業者に含まれていないからである（法 2 条 5 項）。

ただ、マイナンバー付き個人情報（特定個人情報）の取扱いについては、行政機関などについても、指導・監督等の対象としており、その取扱者に対しては助言や指導等ができる権限を有していると解すこともできる（法 33 条～35 条）。したがって、委員会が、行政機関などの特定個人情報取扱いに関する苦情や指導などの申出を受け付け、問題とされた行政機関等の苦情担当部署（相談窓口）に引き継ぎ、その後の処理経過について報告を求める、あるいは助言や指導等を行うことができると解される。

ただ、こうした国の行政機関とか自治体などの特定個人情報の取扱いに直接口を挟むことができない仕組みの個人情報保護法制については、市民感情からすればまったく解せないのは当り前である。国会議員が狡猾な行政に丸投げして制度設計させると、委員会は自分らには手出しができない仕組みに仕上げた法律ができあがるわけである。市民団体は、行政府の役人が法律案を仕上げて国会議員がシャンシャンするだけの「政府立法（閣法）」の問題点にもっとメスを入れる力量を持つ必要がある。“ウブが売り”だけでは、闘えない。

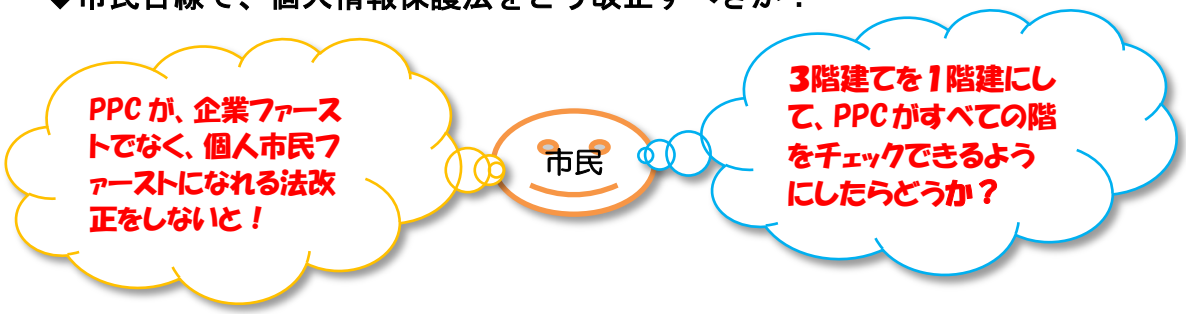
わが国の個人情報保護法制の特徴

- 公民別建てとして、公分野に対する規制をできるだけ緩くしている。個人情報保護委員会（PPC）が、原則として公分野にはアンタッチャブルになっているのが適例
- わが国の最近の改正では、規制を加えるどころか、産業利益優先で、できるだけ企業や行政などができるだけ縛りなくビッグデータを自由に利用できるように、規制緩和を実施。

【図表５】EU と日本のビッグデータのプライバシー法上の取扱いを比べる

EU	“ビッグデータ”の利活用の法的規制強化。個人データ（個人情報）の取得/収集の際の同意の厳格化【データ主体の同意の撤回権の保障、データ主体の削除請求権、データ主体が利活用方法を問う権利など】
日本	“ビッグデータ”、つまり匿名化した個人情報～「非識別加工情報」（行政機関個人情報保護法等）「匿名加工情報」（基本法である個人情報保護法）は、原則として個人情報にあらず。利活用はほぼ自由。また、ビックデータに関してだけは、公民双方について、個人情報保護委員会（PPC）が担当できる。

◆市民目線で、個人情報保護法をどう改正すべきか？



・現行の個人情報保護法は、法的制度設計が悪く個人情報保護には役立たない“名ばかり第三者機関”の個人情報保護委員会（PPC）の改組を含め、個人（情報主体）のプライバシー権の保護・強化に向けた改正は、待ったなしである。

・例えば、現行の個人情報保護法は、委員会(PPC)に対して、「個人情報取扱事業者」の個人情報取扱いに関する苦情の申出に対処する権限を与えている（法 61 条 2 号）。ところが、国の行政機関とか自治体などを、個人情報保護法上の「個人情報取扱事業者」から除外しているのである（法 2 条 5 項）。つまり、会社や商店、私立学校などの民間機関のみを、「個人取扱事業者」とし、PPC が対処できる対象としているのである。国の行政機関とか自治体などには、PPC はアンタッチャブルなわけである。

・こんな法制では、市民の個人情報、プライバシーが、行政内部でたらい回しされたり、法令等に従わない取扱いをされても、情報主体である市民はそうした取扱いに歯止めをかけることは至難となる。

・しかも、行政にプライバシーを侵害されたと思う市民が、個人情報保護委員会（PPC）に救済を求めても、「我われ（PPC）は、所管外である」として門前払いされる。

・それでいて、個人情報保護委員会（PPC）は、個人市民のためよりは、法人企業のためにはよく働く。EU の GDPR のもとで、EU から国として「十分性の認定」のお墨付を得るために先頭にたって EU 側とは協議した。（このお墨付きの枠組みは 2019 年 1 月 23 日に発効した。）

◆ 個人情報保護委員会って何？

“名ばかり第三者機関”では？

【図表６】市民からみた「個人情報保護委員会（PPC）」って何？

個人情報保護委員会（PPC）

本当に第三者機関なの？

個人番号実施翼賛機関では？

【図表７】個人情報保護委員会（PPC）の任務についての委員会 HP での PR

個人情報保護委員会は、個人情報（マイナンバー（個人番号）を含む。）の有用性に配慮しつつ、その適正な取扱いを確保するために設置された独立性の高い機関です。

＊傍点引用者 （https://www.ppc.go.jp/aboutus/commission/）（法 60 条）

市民

「PPC」って、企業寄り、“有用性”忖度機関なのかぁ～？？

議員立法も一案！

【図表８】個人情報保護法は改正が必要、議員に法改正を働きかけよう！

・委員会は、国の行政機関や自治体を指導できないような法的仕組みになっている。
・なぜならば、国の行政機関とか自治体などは、個人情報保護法上の「個人情報取扱事業者」に含まれていないからである（法 2 条 5 項）。
・ただ、マイナンバー付き個人情報（特定個人情報）の取扱いについては、行政機関などについても、指導・監督等の対象としており、その取扱者に対しては助言や指導等ができる権限を有していると解すこともできる（法 33 条～35 条）。
・したがって、PPC が、行政機関などの特定個人情報取扱いに関する苦情や指導などの申出を受け付け、問題とされた行政機関等の苦情担当部署（相談窓口）に引き継ぎ、その後の処理経過について報告を求める、あるいは助言や指導等を行うことができるものと解される。

【図表９】PPC の規制権限行使の対象は

国の行政機関、自治体、独立行政法人などは、「個人情報取扱事業者」に該当しない

個人情報保護委員会（PPC）の規制対象

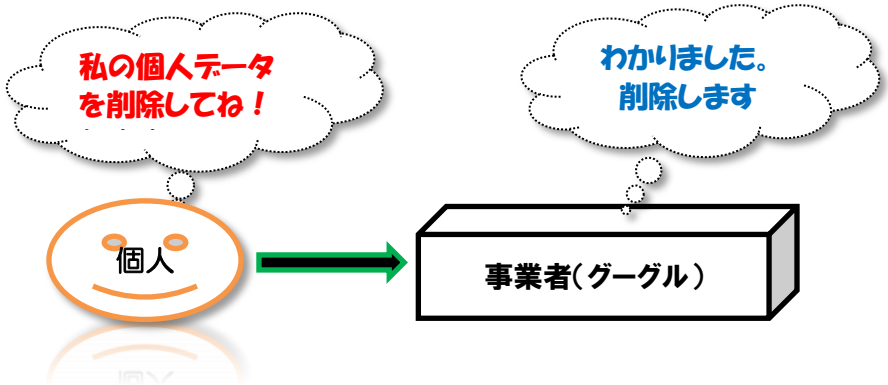
個人情報取扱事業者

・わが国では、最近法律が改正され、個人情報取扱事業者は、個人データを利用する必要がなくなったときは、遅滞なく当該個人データを消去するよう努めなければならない、とされた(改正個人情報保護法 19 条)。しかし、いわゆる「努力義務」である。

・EU の一般データ保護指令(GDPR)では、情報を提供した個人に対して「削除権」を認めた。つまり、従業員が事業者に個人情報を提供した場合に、法定期限を過ぎたなどの理由で、その従業者は事業者に自分の個人情報を削除してもらうことを“権利”として認めた。一般に、「忘れられる権利(right to be forgotten)」ともいわれる。

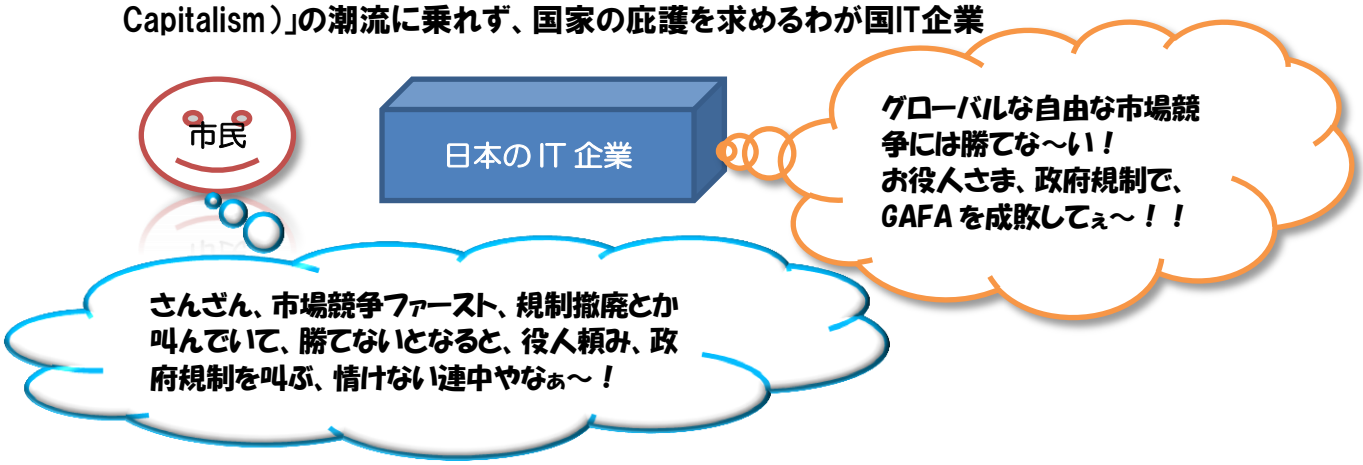
日本法 不要となった個人データ削除の努力義務？
EU の GDPR 削除を求める権利/忘れられる権利

【図表10】EU 並みの「削除してもらう権利(忘れられる権利)」が法認されると！



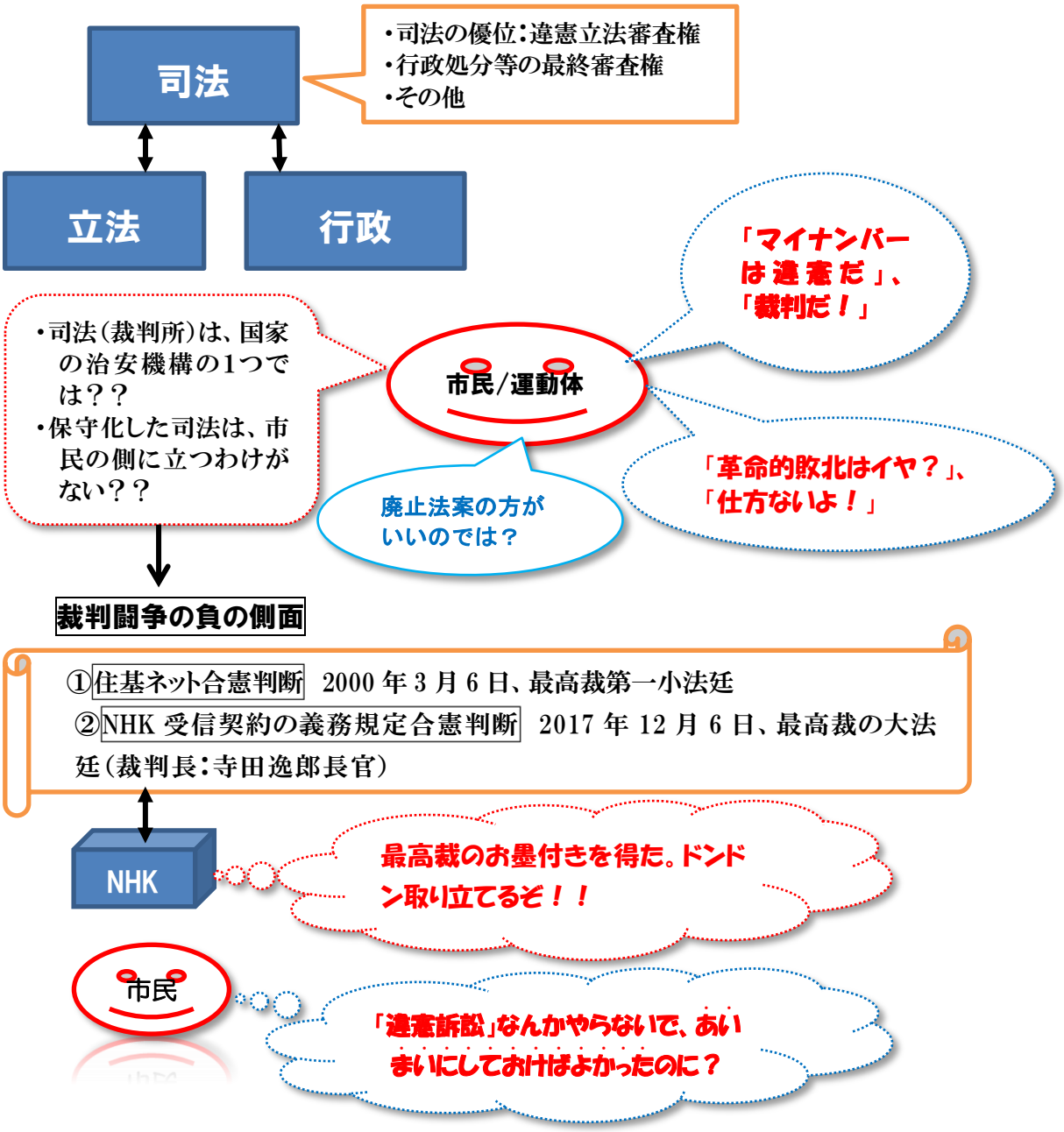
■むすびにかえて

～「グローバルIT企業独占資本主義」、「データ監視資本主義(data surveillance Capitalism)」の潮流に乗れず、国家の庇護を求めるわが国IT企業



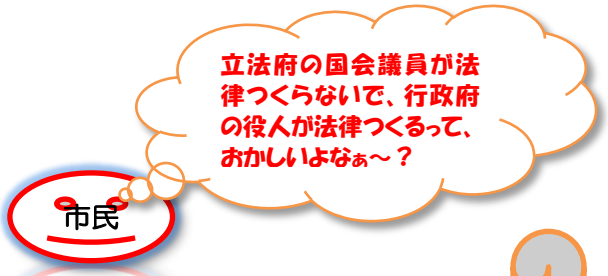
資料 市民にとり、司法とは何か、議員立法/政府立法とは何か

■ 三権分立とは国家権力を3つに分けること、つまり司法は国家権力



●裁判所が違憲判断を避ける論法
①「統治行為論」って何??
②「立法裁量」って何??

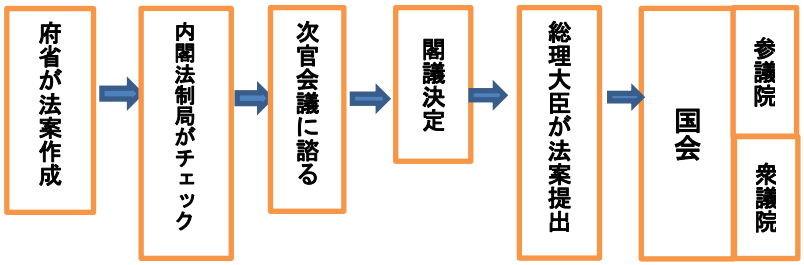
■ 議員立法と政府立法の違いを知ろう



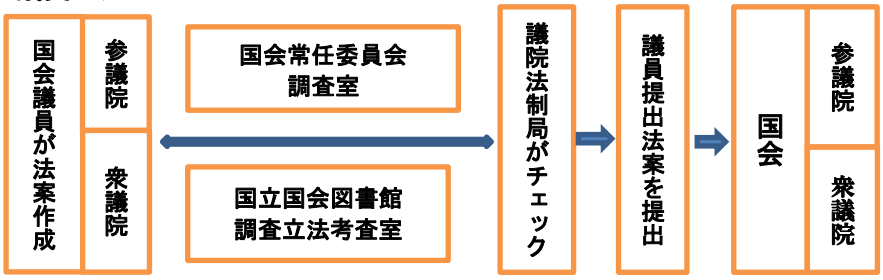
政府立法(閣法)と議員立法はどう違う!

・憲法 41 条は「国会は、国権の最高機関であって、国の唯一の立法機関である。」と規定。
・この規定を文字どおり読むと、国会議員が努力して法律をつくる、いわゆる“議員立法(国会単独立法)”が唯一のルートのようにみえる。
・ところが、わが国の立法手続には、“政府立法”(内閣提出法案、いわゆる「閣法」ともいう。)という、もう 1 つのルートがある。
・つまり、国の縦割り行政のルールに従い、その事務を所掌する行政(府省の担当局・課)が中心となって法律をつくるルートである。

●政府立法(閣法)プロセス



●議員立法プロセス



【図表25】第 193 回国会(2017 年 1 月 20 日～6 月 18 日)の立法状況

○議員提出法案
《衆議院》〔計〕26　(内) 可決成立 8、未了廃案 1、その他 17
《参議院》〔計〕166 (内) 成立 1　その他 165
○政府提出法案
《衆議院》〔計〕66　(内) 可決成立 63、未了廃案 3

PIJ プライバシー・インターナショナル・ジャパン

〒171－0021 東京都豊島区西池袋3-25-15 IB ビル1OF
Tel./Fax 03－3985－4590
E メール wagatsuma@pij-web.net
機関誌『CNN ニューズ』を発行しています。バックナンバーについては、PIJ の HP にリモートアクセス、ログインして自由に入手できます。 http://www.pij-web.net/