2019/4/11 発行

CNN ニュース No.97

プライバシー
インターナショナル
ジャパン（PIJ）
国民背番号問題検討
市民ネットワーク
Citizens Network Against
National ID Numbers（CNN）

Privacy International Japan
PIJ
Privacy NGO™

季刊発行
年４回刊

■巻頭言■

国民全員が身分証（ID）を持ち歩く監視国家はいらない！

―― "不健康„ なマイナンバーカードの健康保険証化、強制交付 ――

マイナンバー（私の背番号）ICカードを、2021年3月までに健康保険証にする「不健康」なプランが出てきた。マイナンバーカードを「健康保険証」にすれば、逃げられない、と読んでいるわけだ。加えて、通知カードを廃止し、直接ICカードを強制交付するデジタルファースト法案が出てきた。

マイナンバーカードには、顔写真や背番号、それにあらゆる基礎的な個人情報が書かれている。このカードはあらゆる犯罪の道具になる。カードの紛失・盗難、悪用、なりすまし犯罪、振り込め詐欺などの多発につながる。それこそ、国民背番号が券面に書かれたICカード携行は「不健康」そのもの。私の背番号を入れ墨して、プライバシーを首から下げて歩け！に等しい。それに、「パスワードを頻繁に変えて個人データの安全を確保する時代に、生涯不変の背番号（12ケタのパスワード）を持ち歩け」というのも解せない。

仮に皆が背番号ICカードを持たせられたとする。だが、パソコン（PC）とICカードリーダーがないと利用できない電子政府構想（マイナポータル）では、利用促進はムリだ。世はICカードリーダーをつなげないスマホやiPadなどモバイル端末全盛の時代である。結局、スタンドアローンの健康保険証、人権侵害のICカードにしかなるまい。

マイナポータルの利用には、マイナンバーICカードを使う。だが、12ケタのマイナンバーを使うわけではない。カードに入っているPKI（公開鍵・電子証明書）を、セキュリテイ対策に使うだけだ。オーストラリアでは、モバイル端末全盛時代に応えて、ICカード（PKC）を使わない電子政府（myGov）、電子申告（myTax）を導入した。利用には、パスワード＋3つのQ&Aを使う。国税庁は、この辺はわきまえている。今年1月からマイナンバーカードを使わず、代わりに個別ID番号・パスワードで電子申告できる仕組みに舵を切った。ICカードを必須とするマイナポータルは、明らかに陳腐化、ガラパゴス化している。

不健康な健康保険証カード化やICカードの強制交付は、マイナポータルの利用拡大にはつながらない。このことを、総務省の役人はわかっているはずだ。要するに、国民ID制度の導入。つまり国民全員が背番号と顔写真つきの不健康な健康保険証カード、ICカードを持ち歩けということだ。「マイナンバーカードを持たない人は、非国民」とする監視国家の流れを加速したいだけだ。

もう1つの動機が不純な総務省のプランがある。マイナンバーカードを使った自治体ポイント制度である。消費税増税で「切れ目のない景気対策をうたうが、内実はカードを持たせるための切れ目のない悪だくみ」。この種の共通ポイントカードは民間にひしめいている。民業圧迫、素人官業の「自治体ポイント」は必ず血税のムダ遣いに終わる。むしろ「危ないマイナンバーカードで集められた自治体ポイントの警察による危ない使われ方」が心配だ。

自公長期政権、脆弱な野党の現在、総務省の役人には、もう電子政府はどうでもよい。今が「国内パスポート」、「国民全員に身分証（ID）を持ち歩かせる監視国家」実現の最後のチャンスという読みだ。だが、この愚策で、庶民がなりすまし犯罪などで地獄を見るのは必至だ。

２０１９年4月11日
PIJ 代表 石 村 耕 治

◆ 主な記事 ◆

・巻頭言～身分証（ID）を持ち歩く監視国家はいらない
・ポイントカード情報で太る企業とつるむ捜査当局
・GAFA対策としてのEUの一般データ保護規則
・学習会「マイナバー、ここが問題」

ポイントカード情報で太る企業とつるむ捜査当局

―― ポイントカード情報が捜査当局のターゲットに ――

素人官業「自治体ポイント」は必ず失敗する

警告表示

あなたのカード利用情報が警察に提供されプライバシーを損なうおそれがありますので注意しましょう

対論

話し手　清水晴生（白鷗大学教授）
聞き手　石村耕治（PIJ代表）

コンビニやレンタルショップなど、いろいろな店で買い物をするとポイントを貯められるのが共通ポイントカード。共通ポイントではわが国最大手の一つが「T カード」。年間の T カード利用者は、人口の半分を超える 6,676 万人以上。提携店は 83 万店以上を占める。ところが、この T カードの運営会社（CCC ／カルチュア・コンビニエンス・クラブ）が、捜査当局に会員の利用歴などの個人情報（データ）を流していた。情報（データ）提供については規約にはっきり書いていなかった。しかも裁判所の令状もなかった。一方､捜査当局も､情報(データ)を得たことを会員本人に知られないように、秘密保持を徹底しているという。「中国の個人データ国家管理主義が恐ろしい」などといってはいられない。この国でも、ポイントカードの信頼性で尻に火がついているのだ。

ポイントカードは購買歴などのプライバシーとポイントの交換だといわれる。だが、会員は、ポイントカードは犯罪とは無縁だと信じている。捜査当局に個人の利用歴（データ）が筒抜けになるとは誰も考えていない。日々貯まるポイントで海外旅行へ行ってきたとか、無邪気な小市民がわんさといる。ポイント合算サイト（アプリ）なども、問題の根源は同じだ。

T カードだけではない。くらしのなかに定着する、nanaco（ナナコ）、Suika（スイカ）などさまざまなカードの利用歴情報が、市民の足跡をたどるのに使われている。会員は犯罪容疑者ではないはずだ。会員データの当局への提供手続は概して不透明である。私たち市民は、自分の知らない間にいつ当局のターゲットにされるかわからない。

たばこのカートンには、「あなたの健康を損なうおそれがありますので吸いすぎに注意しましょう」の有害表示がある。これに倣い、ポイントカードの券面に、「あなたのカード利用情報が警察に提供されプライバシーを損なうおそれがありますので注意しましょう」と有害表示する必要があるのではないか。

総務省は、危ないマイナンバーカードを使った「自治体ポイント」プランを全国に拡散させるという。こんな素人官業、第二のもんじゅになるのは必至だ。マイナンバーカードの健康保険証化プランも、「不健康」そのものだ。スマホに格納するならまだしも、まともな市民なら誰も、自分の 12 ケタの背番号が書かれたカードを裸で持ち歩きたくないはずだ。基本的な個人情報が漏れもれになり、なりすまし犯罪、振り込め詐欺などが多発する社会への誘因となる。同時に、警察官が IC カードリーダーを持って街中を警らするデータ監視社会への道も切り拓く。

いずれにしろ、ポイントカード会員や自治体ポイントの個人情報（データ）が、令状なしにたやすく捜査当局に提供されるのは大問題だ。しか

© 2019 PIJ

も、会員本人の知らないところで、企業の一方的な判断で提供されるのだから問題は深刻だ。

プライバシーゼロ社会に向けて、ポイントカード情報で太る企業とつるむ当局、マイナンバーカードの不健康な利用問題の所在について、刑事法学専攻の清水晴生白鷗大学教授に、石村耕治 PIJ 代表が聞いた。

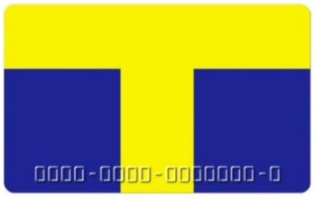
（CNNニューズ編集局）

【内容目次】

◆ポイントカード情報で太る企業とつるむ捜査当局
◆カード運営（発行）会社などによる当局への情報提供の実態
◆当局はポイントカード個人情報入手に令状は要らないのか？
◆捜査照会（捜査関係事項照会書）とは何か
◆捜査当局からの照会への非協力にはペナルティがあるのか
◆捜査当局への提供をフリーパスとする個人情報保護法
◆求められる会員の個人データを護る企業倫理
◆素人官業「自治体ポイント」の危ない使われ方
◆「不健康」なマイナンバーカードの健康保険証化
◆プラットフォーマーによるポイントカード情報の使われ方
◆ EU の GDPR に学ぼう！
◆個人データの危ない使われ方にどう挑む

◆ポイントカード情報で太る企業とつるむ捜査当局

（石村）私たち市民が消費者として、店舗などでショッピングする度にポイントを貯められるのが共通ポイントカードです。共通ポイントではわが国最大手の一つが「T カード」です。年間の T カードご利用者 は、人口の半分を超える 6,676 万人以上、提携店 83 万店以上を占めます。



T ポイントカードのイメージ (public use)

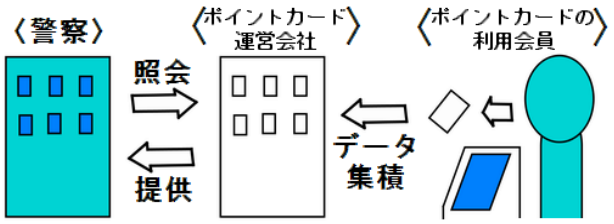
ところが、この T カードの運営会社（CCC／カルチュア・コンビニエンス・クラブ）が捜査当局に会員の個人情報（個人データ）を流していたことが問題になりました。規約にも規定がなく、裁判所の捜査令状もないからです。

コラム　「捜査令状」と「捜索令状」の違いは？？

一般に「捜査令状」という言葉は，ガサ入れのための「捜索令状」に限らず，「身体検査令状」なども含め広く「強制捜査のための令状」という意味で使われています。この対談では、こうした区別をあまり考えないで使っています。

（清水）市民・消費者の個人情報が、本人の知らないところで、令状もなく、ポイントカード運営（発行）会社の一方的な判断で、捜査当局に提供される。これは、プライバシー保護の面で大きな問題ですね。

【図表 1】情報照会をめぐる警察・ポイントカード運営会社・会員の関係



（石村）今まさに、ポイントカード情報で太る企業とそれらの企業と情報の分かち合いでつるむ捜査当局の姿勢が問われています。

◆カード発行（運営）会社などによる当局への情報提供の実態

（石村）マスメディアなどによると、ポイントカード運営（発行）会社は、捜査当局に対して、次のような個人情報（個人データ）の提供をしているようです。

（清水）【図表 2〔次頁〕**】**を見ると、ポイントカード運営（発行）会社がどのような会員の個人情報（データ）を捜査当局に提供できるのかがわかります。会員が、立ち寄ったコンビニで、各種ポイントカードを決済時に提示したとします。すると、その人が、いつ、何時頃、どこの店舗で何を買ったのか、どんなサービスを利用したのかの履歴（データ）が、ポイントカード運営（発行）会

【図表 2】カード運営（発行）会社が捜査当局に提供する個人データー覧

・登録時の個人データ
氏名、生年月日、住所、電話番号、メールアドレス、登録クレジットカードや預金口座など
・登録後の利用データ
交通、コンビニ、ファーストフード、銀行、新聞、航空会社、レンタルビデオ、ネット通販、ガソリンスタンド、ホテルなど

（前田恒彦 '19.1.21 付Yahooニュース記事「ポイントカードの利用履歴までも令状なしで捜査当局に提供される様々な個人情報」などを参照）

社に残ります。捜査当局は、ポイントカード運営（発行）会社に、この利用データ（購買歴など）と登録時の個人データの提出を求める。そうすれば、捜査対象者の行動パターンが手に取るようにわかるわけです。わざわざ尾行する手間も省けます。

（石村）それに、コンビニなどでは、防犯カメラを設置していますからね。

（清水）そうですね。捜査対象者の足取りさえつかめれば、必要な映像データがどこにあるか、どこに映像データの提供を求めればよいかも容易に想定できます。いわば芋づる式に対象者の動きが浮かび上がってくるというわけですね。事件当時本人がどこにいたか、誰といたか、どんな格好をして、手に何を持っていたか・・・まで。

◆当局はポイントカード個人情報入手の令状は要らないのか？

（石村）捜査当局は、犯罪の容疑者や行方不明者などの足跡をたどるのには、ポイントカード情報が役に立つのはわかります。とはいっても、消費者の個人データを、本人の知らないところで、企業と捜査当局で勝手に分かち合うのは、大きな問題だと思いますが。捜査当局は、裁判所から捜査令状を得て個人データの提供を求めるのが基本的なルールになっていると思いますが？

（清水）そうですね。ただ、現実には、こうした個人情報（データ）の入手には令状が使われていません。

（石村）捜査当局が、捜査令状なしに勝手に被疑者の車両に GPS を装着してデータを収集しようとしたケースで、裁判所は違法としましたが・・・。

（清水）ふつうの市民は、テレビの刑事ドラマなどの印象もあり、犯罪捜査といえば令状を取ってやっていると思いがちです。しかし、現実の犯罪捜査では、「令状によらない捜査」が基本的なルールになっています。

（石村）「令状によらない捜査」とは？

（清水）「令状によらない捜査」とは、警察が人の管理する敷地ではない公道上で実況見分をするとか、聞き込みをするとかが典型です。逆に、「令状による捜査」とは、相手の同意がなくても強制的に捜査することを認めた裁判官が発行した令状による捜査です。「強制捜査」とも呼ばれます。強制捜査は対象者の権利を侵害するものだから、強制でなくて済むなら任意でせよ、というのが捜査の基本的なルールです。

（石村）一見、合理的なようにも思えますが。

（清水）この捜査ルールは、「任意捜査の原則」といいます。刑事訴訟法 197 条 1 項に定めがあります。

【図表 3】任意捜査の原則

【刑事訴訟法 197 条 1 項】
捜査については、その目的を達するため必要な取調をすることができる。
但し、強制の処分は、この法律に特別の定のある場合でなければ、これをすることができない。

（石村）当局が、ポイントカード運営（発行）会社から情報（データ）提供を受けるのは任意捜査ということになりますか？

（清水）処分する権限を持つ当局が捜査協力要請をする。この要請に基づいて、ポイントカード運営（発行）が、会員である顧客の個人情報（データ）を、同意の下に提供する限りは任意ということになるでしょう。

（石村）会員は、個別的な要請に対して同意しているわけではありませんよね。

（清水）ポイントカード運営（発行）会社に、会員情報（データ）をどのように利用するかについて権限があると考えるとします。そうすると、いちいち会員の同意を得る必要はないということなのでしょう。現に管理しているのは、管理権

【図表 4】一方の同意があれば許される？

© 2019 PIJ

限を持っているポイントカード運営（発行）会社なのですから。

（石村）会員は、警察への情報提供にまで同意しているとは必ずしもいえないのではないですか？

（清水）仰せのとおりだと思います。強制捜査にせよ、任意捜査にせよ、侵害の危険にさらされるのは運営会社の権利以上に会員個人の権利ですからね。任意捜査というならなおさら、会員自身の「個別の」同意が原則として必要です。

（石村）例えば、ホテルが同意したからといって、捜査当局者が、客室にまで無断で立ち入るのは、もはや任意捜査とはいえないですからね。

（清水）警察サイドの言い分というのはおそらく、電話の盗聴による捜査のようなイメージだと思うのですね。一方の同意さえ得ていればいい。他方は相手に聞かれることは想定済みで話しているのだから、その相手が話すということは想定内だということでしょう。嫌なら電話しなければいいと・・・。

（石村）つまり、任意捜査なら何をやっても許される。令状による縛りを一切受けないと、そういうことですか？

（清水）石村先生がはじめに指摘されたGPS捜査のケースからもわかるように、捜査当局はそう考えがちです。しかし、本当は、そんなことはないのです。すでにふれましたが、令状による捜査は強制捜査であり、強制捜査というのは相手の権利を侵害して行うから強制だということです。無理やりガサ入れしたり、押収したり、あるいは逮捕するということです。

（石村）住居の不可侵の侵害、私的所有権の侵害、人身の自由の侵害。全て憲法が保障している重要な人権の侵害だということですね。

（清水）そうです。つまり、いくら捜査機関が任意捜査のつもりであったとしても、重大な人権を侵害するようなものであれば、それはやはり強制捜査だということです。

（石村）「任意捜査のつもり」ということは、令状は取っていない・・・。

（清水）令状によらない強制捜査ですから違法ということになります。先にふれたとおり、強制捜査に令状が必要なことは憲法にも書いてあります。また、刑事訴訟法のなかのそれぞれの強制捜査に関する規定にもちゃんと書いてあります。

（石村）逆にいうと、人権侵害につながらない強制でない捜査なら、警察や検察は自由に行えるということになるわけですね。

【図表5】捜査で影響を受ける基本的人権

【憲法29条1項】
財産権は、これを侵してはならない。

【憲法35条1項】
何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第33条の場合を除いては、正当な理由に基いて発せられ、且つ捜索する場所及び押収する物を明示する令状がなければ、侵されない。

【憲法33条】
何人も、現行犯として逮捕される場合を除いては、権限を有する司法官憲が発し、且つ理由となつてゐる犯罪を明示する令状によらなければ、逮捕されない。

（清水）いえ、そうではないんです。

（石村）どういうことでしょうか？

（清水）確かに重大な人権侵害でなければ強制捜査にはあたらない。でも「重大な人権侵害」とまではいかなくても、警察に協力を求められるというのはやはり相手からすれば一定の範囲で自由を制約されるわけです。

（石村）ポイントカード運営（発行）会社は、会員の重要な個人データの提供に応じるとします。そのために通常の業務を後回しにし、優先的に警察の要請のための作業をする。時間を取られ、人手を取られ、場合によっては会員の信頼、営業上の信用まで損ないかねませんね。

（清水）そのとおりです。ですから任意捜査であっても、「必要な限り」で認められるに過ぎないわけです。必要性の度合いに応じて、必要性に見合う範囲・程度でしか許されないという意味で、「捜査比例の原則」、あるいは単に「比例原則」と呼ばれます。任意捜査の原則のところで見た条文をもう一度見てみましょう。

【図表6】捜査比例の原則（比例原則）

【刑事訴訟法197条1項】
捜査については、その目的を達するため必要な取調をすることができる。
但し、強制の処分は、この法律に特別の定のある場合でなければ、これをすることができない。

（石村）確かに、「その目的を達するため必要な」となっていますね。

（清水）警察官職務執行法、略して警職法の１条２項にも同じような趣旨の規定があります。

【図表 7】警察官職務執行法１条２項

この法律に規定する手段は、前項の目的［警察官による職権職務の忠実な遂行］のため必要な最小の限度において用いるべきものであつて、いやしくもその濫用にわたるようなことがあつてはならない。

（石村）こちらでは「必要な最小の限度」と定めていますね。

（清水）ですから、重大な人権侵害でないから強制捜査にあたらないといっても、それが必要な範囲、また相当な程度を超えるようなものであってはアウトなわけです。つまり、任意捜査だといっても、それは違法な任意捜査だということになります。

（石村）いくら相手が同意していたといっても、夜も寝かせずに、家にも帰らせずに取り調べたりしたら、これはもう必要な範囲、相当な程度を超えた違法な任意捜査ということですね。

（清水）そこまで行くと、もう実質上逮捕と同じです。令状のない違法な強制捜査ということにもなりかねません。度が過ぎた違法な任意捜査なのか、それとも、もはや令状のない違法な強制捜査というべきかが問われます。後者の方が、違法性が高いわけで、こうした判断こそまさに問題となるところです。いずれにしても、任意なら手放しに自由に捜査していいというわけではありません。

【図表 8】違法な任意捜査と違法な強制捜査

	違法となる場合の判断基準
任意捜査	**必要な範囲・相当な程度を超えたとき**
強制捜査	**重大な人権侵害を伴うのに令状を取らなかったとき（あるいはそもそも法律上その捜査を許す令状が定められていないとき）**

（石村）なるほど、わかりました。でも今回のポイントカード発行（運営）会社のケースのように、犯罪捜査のために必要な範囲で任意の協力を求めるのであれば、やはり任意捜査として適法だということになりませんか？

（清水）そうかもしれません。ただ、注意すべきことは本当に「特定の犯罪の捜査なのか」という点ですね。

（石村）それはどういうことでしょうか？

（清水）実は警察というのは犯罪捜査だけやっているわけではありません。「犯罪予防」もやっています。

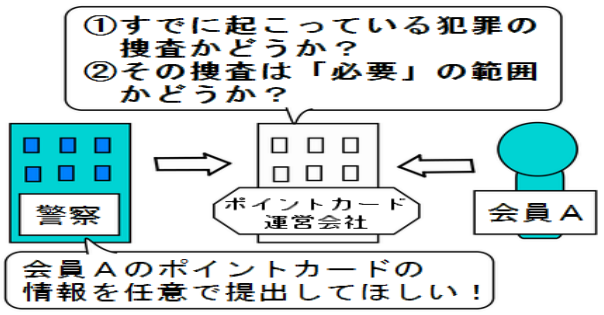
（石村）犯罪予防というのはつまり、いまだ犯罪は起きていないわけですね。

（清水）そうです。刑事訴訟法が許している捜査というのは、犯罪が起きた後に行われる犯罪捜査です。犯罪の予防というのはいわば治安行政官としての警察の活動であって、犯罪の捜査とは区別されます。

（石村）犯罪が起こってないんですから、犯罪の捜査ということも理屈からいってもあり得ないはずですからね。

（清水）そうです。ですから任意捜査であるとしても、先ほどみた刑事訴訟法 197 条１項が「必要な」範囲で認める捜査というのは、すでに起こった特定の、具体的な犯罪に対する捜査でなければなりません。

【図表 9】三者間で考える「適法な捜査」とは？



（石村）照会を受けるポイントカード運営（発行）会社側は、本当にすでに起こった具体的な特定の犯罪に関する照会なのかどうか、安易に公安目的で照会されていないかどうか、をしっかりと確認する必要がありますね。

（清水）そうなんですが、ただ、警察は、捜査の密行性を理由に明らかにしたがらないでしょう。だからといって、ポイントカード運営（発行）会社が照会を受けた会員データを安易に提供するのも問題です。個人情報保護法上は違法でなくても、会員の怒りを買って民法上の損害賠償請求をされるかも知れません。

（石村）しかし、警察は、照会を求めたとしても、その理由を明らかにしないわけです。これでは、ポイントカード運営（発行）会社は、それが果たして本当に特定の犯罪捜査のためのものなのか、判断のしようがありませんね。

（清水）それなのに、会員情報を提供してしまっていいのかが問われてきますね。

（石村）ポイントカード運営（発行）会社は、捜査協力により適正な社会的責任を果たしたいと考え

© 2019 PIJ

ているとします。であれば、むしろ裁判官の審査を通った令状による場合に限って協力要請に応じる方がよいと思います。ところが、Tカードの運営会社（CCC）の場合は、2012年に、令状がなくとも当局からに文書による照会があれば、会員情報の提供に応じるように方針を変えたわけです。

（清水）ポイントカード運営（発行）会社は、他人の情報を委託され管理する立場にあります。ですから、冷静に客観的事情が整った段階で初めて協力するという方が、ずっとバランスの取れた対応といえると思います。

◆捜査照会（捜査関係事項照会書）とは何か

（石村）今日、捜査当局が、ポイントカード運営（発行）会社から個人データの提供を受ける場合に、捜査令状を使うのは稀といわれています。捜査関係事項照会書を使うのが一般的といわれます。「捜査関係事項照会書」とはどういった性格の文書なのですか？

（清水）捜査関係者ではないのでリアルにはわかりませんが、刑事訴訟法にはそれに関係するような条文があります。刑訴法197条2項です。

【図表10】公私の団体への照会

【刑事訴訟法197条2項】
捜査については、公務所又は公私の団体に照会して必要な事項の報告を求めることができる。

（石村）あれ？　さっき出てきた条文も確か・・・

（清水）えぇ。同じ刑訴法197条の条文でした。「任意捜査の原則」、「捜査比例の原則」を定めていたのが197条1項。こちらが同じ条文の2項ということですから・・・。

（石村）この「公私の団体への照会」というのも、任意捜査を定めた規定だということですか。たしかに、必要な事項の報告を「求めることができる」という書き方になっていますね。

（清水）犯罪が起きた、あるいは容疑者が住む近隣の住人の玄関先で聞き込み捜査をするのと同じだということでしょうね。ただし、あくまで「求めることができる」という限定つきです。言い換えると、任意捜査として比例原則の範囲内で、つまり必要な範囲でのみ認められるということです。

（石村）あくまで任意だということですね。一部ポイントカード運営（発行）会社は捜査照会に対して「社会的責任」から応じていると報道されています。しかし、これは、言い換えると「法的責任」からではないということになりますね。

【図表10】法律の言葉づかい

言い回し	意味
「○○できる」	任意（自由）
「○○しなければならない」	法的義務

（清水）そうです。「法的責任」という意味からだと、契約の相手方である会員の個人情報（データ）を外部に漏らさずに最大限に秘密を護る方が本来果たすべき責任だと思います。

（石村）捜査照会に応じるのは社会的責任であるといえば、聞こえはいいのですが。大量の会員の個人情報（データ）を預かる立場にあるポイントカード運営（発行）会社のスタンスとしては、どうなのでしょうか？簡単に捜査当局に教えない方が、個人情報（データ）を取り扱う企業としてはよほど社会的責任を果たしているといえるのではないかと思います。

（清水）いくら相手が警察や検察だからといっても、捜査照会では法的義務が課されているわけではありません。他方で個人情報の最大限の保護は、個人情報保護法上も契約上も要求される法的義務なわけですからね。

（石村）ポイントカード運営（発行）会社が、法的義務の方をないがしろにして、捜査照会を優先するのは、個人情報（データ）でビジネスする企業としては、大きな問題ですね。

（清水）今日、市民は自分のプライバシー問題に敏感です。ポイントサービス運営会社は、警察や検察を忖度する、あるいは、一方的に優先する姿勢は改めないといけませんね。

◆捜査当局からの照会への非協力にはペナルティがあるのか

（石村）以前は、捜査当局がポイントカード個人データの提供を受けるには、捜査令状を使ったようですが。今日では、刑訴法に基づく捜査関係事項照会書（捜査照会）を使って、カード運営（発行）会社から個人データを入手するのが一般的なようです。ポイントカード運営（発行）会社が、捜査照会を断った場合には、ペナルティがあるのでしょうか？　捜査令状による場合と、捜査照会による場合とでは、どのような違いがあるのでしょうか？

（清水）これまで見てきたとおり、捜査照会について警察は「求めることができる」だけです。求められた側には応じる義務はありません。あくまで任意捜査ですから、断ってもペナルティはありません。これに対して、捜索令状による場合は公務

【図表 12】違法捜査への対応

執行妨害になる可能性がないわけではありません。ただ、そもそも大勢の警察官に対して妨害のしようもありませんからね。

（石村）令状を示された場合に抵抗する善良な市民もいないでしょうし・・・。

（清水）ですから、令状を持ってきたときに十分に社会的責任と法的責任とを果たせばよいのではないでしょうか。本当に必要なら令状を取るでしょう。安易に手軽な捜査照会に応じていると、本当にいざ会員・顧客情報を護らなければならなくなったときに、護りの態勢を取りにくくなるように思いますが。

（石村）むしろ「令状がある場合や、緊急性がある判断とできる場合に限る」といった社内規準を自主的に設けておく方が、消費者に受け入れやすい。コンプライアンス（法令遵守）の姿勢がしっかりしている企業として高い評価を受けるのではないでしょうか。この方が、より社会に対して責任ある態度だと思います。

（清水）カード運営（発行）会社は、捜査当局に「どうせ強制捜査になるから余計面倒になる」なんて脅迫まがいのことをいわれるかも知れません。こうした場合には、スマートフォンなどできちんと録音しておくことですね。

（石村）スマホで録音することは、捜査妨害として証拠隠滅罪や犯人隠避罪に問われる、ことはないのでしょうか？

（清水）何の証拠も「隠滅」していません。令状を取ればいいわけです。「隠避」ではありませんね。これが隠避で罰せられるとなればもはや刑罰による強制です。全く「任意」ではないということになってしまいます。

（石村）捜査照会があったことをその会員に教えることは、さすがにアウトですか？

（清水）そんなことはないと思います。捜査当局は、何ら強制的な権限に基づいて照会しているわけではありません。ですから、ポイントカード運営（発行）会社が、業務の範囲内で会員に必要なサービスの一環として教えることは大丈夫です。法的に禁じられているとは解せません。任意捜査である以上は当然そういうことも想定の範囲内でしょう。

（石村）それに、会員である個人の側にも自分の情報（データ）を管理（コントロール）する権利があるはずです。自分の個人情報（データ）にアクセスする者がいるとします。その場合、会員は、それが誰であるかを知る権利があると考えるのは当り前ですね。

（清水）ただ、どんな場合でも罪に問われないかといえば、そうではありません。例えば、積極的に犯人隠避や証拠隠滅の意図を持って会員に教えた場合です。この場合には、悪質性を認定されてしまう余地もあります。

◆捜査当局への個人データ提供をフリーパスとする個人情報保護法

（石村）Tカードの運営会社（CCC／カルチュア・コンビニエンス・クラブ）が、捜査当局に会員の個人情報を流していたことが問題になりました。規約に明記せず、しかも裁判所の令状もなかったからです。これを契機に、カード運営（発行）会社のなかには、法令遵守を前面に打ち出すところも出てきました。

（清水）個人データを提供する規定を会員規約のなかに盛り込んだわけですね。つまり、捜査当局から、照会があった場合には、会員の事前の同意を得る形にしたわけですね。

（石村）そうです。個人情報保護法は、次のように規定しています。

【図表 13】個人情報保護法 23 条〔第三者提供の制限〕

第 1 項　個人情報取扱事業者は、次に掲げる場合を除くほか、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
　第 1 号　法令に基づく場合
　（第 2 号および第 3 号は省略）
　第 4 号　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

それから、総務省が出している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（2017 年 4 月 18 日総務省告示第 152 号）は、次のように規定しています。

© 2019 PIJ

【図表 14】電気通信事業者個人情報保護ガイドライン 15 条〔第三者提供の制限〕

第 15 項　電気通信事業者は、次に掲げる場合を除くほか、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
　第 1 号　法令に基づく場合
　（第 2 号および第 3 号は省略）
　第 4 号　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

（清水）個人情報保護法や総務省の電気通信事業者個人情報保護ガイドラインを見るとわかると思います。「法令に基づく場合」などは、会員の個人データを当局に提供できるわけです。ですから、ポイントカード運営（発行）会社は、わざわざ会員規約に捜査当局に提供しますよ、と書かなくともいいわけです。

（石村）そうですね。事前に本人の同意を得なくとも、その人の個人データを当局に提供することが許されますね。

（清水）すでにふれた刑事訴訟法の規定（197 条 2 項）に基づく捜査当局からの捜査照会（捜査関係事項照会）も、形式的には「法令に基づく場合」にあたりますね。

（石村）ポイントカード運営（発行）会社としては、会員規約のなかに、捜査当局から法令に基づく照会があった場合には、あくまで例外的に、本人の同意を得ないで当局に漏らしますよとはっきりと書いておいた方が、〝免罪符〟になるといった認識ではないでしょうか。そうすれば、いちいち、照会対象会員に対して、個別に、ていねいな説明は不要になるという感覚では？

（清水）そうですね。原則として、第三者にポイントカードの個人データを提供する場合には本人の同意が必要ですからね。捜査当局が、ポイントカード運営（発行）会社に捜査照会を行うのは、犯罪に関係した疑いのある人物かその周辺関係人物です。ですから、そうした人物に当局の追手が迫っていることを知って欲しくないわけです。追われている事実を知ったら、逃亡する、あるいは証拠隠滅をはかるかも知れません。まさしく、この点が、ポイントカード運営（発行）会社が、情報主体である会員本人から事前に同意を得なくてもよいとする理由なのでしょうけど・・・。

（石村）むしろ、会員規約に、第三者提供手続においては原則として本人の同意が必須であること、それに、例外的に本人の同意が要らない場合もあることを、はっきりと書いておく必要はあると思います。ポイントカード運営（発行）会社が、会員本人の同意を得ないで、あるいは黙示の同意で、ポイントカード個人データを DM（ダイレクトマーケティング）その他の目的に流用することも考えられます。この場合、情報主体である会員が、会員規約を典拠に契約責任を問う、あるいは不法行為責任を問うときには、役に立つのではないでしょうか。

（清水）個人情報保護法は、「個人情報の適正かつ効果的な活用・・・」「個人情報の有用性」を云々し産業利用を鼓舞し、最後につけたりのように「個人の権利利益を保護すること」を目的とする（1 条）と結んでいる法律ですよね。

（石村）ですから、この法律は、市民団体などから、個人情報（データ）反故法とやゆされています。しかも「法令に基づく場合」というアバウトな規定を置いています。この規定を手掛かりに、ポイントカード運営（発行）会社は、個人データの提供先が公的機関の場合には、ほぼフリーパスとするスタンスです。

（清水）ただ、保護法、ガイドライン、どちらの規定も「提供してはならない」場合を規定しているだけで、それ以外の場合には「提供しなければならない」と規定しているわけではありませんからね。この点を見逃してはいけません。

◆求められる会員の個人データを護る企業倫理

（石村）ポイントカード運営（発行）会社や加盟店舗などは何のために会員の情報（データ）を入手し管理しているのか、原点に立ち返ってもっと真剣に考えてみるべきだと思います。

（清水）そうですね。ポイントカード運営（発行）会社は、「消費者である会員の支払った対価に応じてポイントを与え、その溜まったポイント数に応じて景品と交換したり、値引きしたりその他の特典を与えること」を本来の事業目的としているはずですからね。

（石村）そうです。運営会社は、そのために会員データを厳重に保護・管理するように求められています。ですから、捜査当局に会員のポイントデータを提供することを第一に管理していると考えているとすれば、それは本末転倒です。

（清水）過度な監視社会化への安易な協力は、自由

経済を基盤とする企業経営にとってはむしろデメリットにつながります。ポイントカード運営(発行)会社や加盟店舗などには、会員である消費者のプライバシーをもっと大事にする経営方針、ビジネスモデルが求められていると思います。

(石村) 清水先生のいわれるとおりです。ポイントカード情報（データ）のプライバシー保護に関しては、たんに法律任せ、当局任せにするのではいけません。企業倫理の持ち方、あり方に関して自省して自ら問い直すように求められています。

(清水) 社会的責任の意味をはき違えてはなりません。ポイントカード情報（データ）保護に対する信頼が守られる社会のためにこそ責任を果たすべきですね。

(石村) 急速に事業を拡大している企業は、とかく消費者保護やコンプライアンスが後回しにされがちです。

(清水) ポイントサービス業界も、そうした傾向が強いですね。

(石村) この現状というのは、いってみれば、ポイントカード会員がコンビニなどで買い物しているところを、レジの奥からマジックミラー越しにじっと刑事によって睨みつけられているのと同じなわけです。

(清水) 日本全国のコンビニなどの「レジの取調室化」、そんな状況にあると思うと、怖いというよりもはや異常な事態というべきですね。

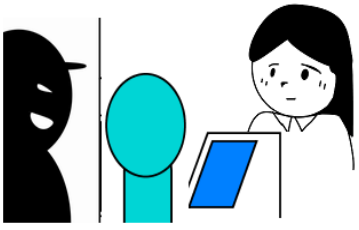
(石村) 消費者も、この問題を次第に共有してきているようです。事実、短文投稿サイト、ツイッターでは、ポイントサービス企業に対する数多くの疑問が飛び交っているようです。

(清水) ポイントカード運営（発行）会社は、検察や警察が公益のためにだけ活動していると勘違いしているかも知れません。

(石村) しかし、実際のところは、刑事裁判において有罪・無罪の勝敗を争う一方のプレーヤーに過ぎないというのが本当の姿ですね。

(清水) まだ無罪推定を受けている被告人も刑事裁判では対等な立場に立っているわけです。ですから、ポイントカード運営（発行）会社や加盟店舗などが、会員・顧客のポイントカード情報（データ）のプライバシー保護を犠牲にして、一方的に捜査当局側に加担することは、社会的責任を図る公平・公正な態度とはいえないと思います。

【図表 15】コンビニレジが当局の取調室と同じ？？



(石村) 昨今のポイントカード運営（発行）会社などの捜査照会に対する歯止めのない対応は、フェアプレイのルールとぶつかりますね。それに、誤った「推定有罪」の流れに加担し、そうした流れを加速させることにもつながりかねません。有罪・無罪は裁判所によって、裁判を経て初めて決せられるわけですからね。

(清水) そういう意味ではやはり、安易に捜査照会によるのではなく、令状主義をもっと大事にする必要があると思います。捜査令状を認めてよいかどうかの裁判官によるチェックを待ってこそ公正・フェアといえるでしょう。また、だからこそ、まさに刑事訴訟法自体がそうしたチェックをするような制度設計をしているわけです。

(石村) 捜査当局が令状による強制捜査が可能だ、必要だと考えていても、裁判官によってそんな捜査は不要・不当だと判断されることも当然あるわけですからね。ポイントカード運営（発行）会社などが安易に捜査照会に応じることは、令状主義を形骸化させるだけではありません。さらに、消費者・顧客である会員の情報プライバシー権も死滅させる方向に導きかねません。

(清水) ポイントカード運営（発行）会社や加盟店舗などは、企業が負わなければいけない社会的責任をもっと多角的・多面的にとらえる必要があるのではないかと思います。

◆素人官業「自治体ポイント」の危ない使われ方

(石村) ポイントカードでは、もう 1 つ大きな問題があります。今年（2019 年）10 月からの消費税率引上げに伴う切れ目のない景気対策の 1 つとして政府・与党が導入する「自治体ポイント」制度計画です。

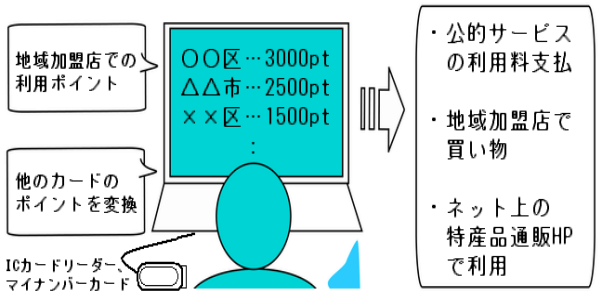
(清水) どういった制度なのですか？

(石村) この制度は、総務省の掛け声で進められています。マイナンバーカードのポイントを貯める機能を使って、総務省の「この指と〜まれ」に応じた自治体が連携して実施する共通ポイントプランです。

(清水) 民間の T ポイントカードなどと同じように、住民が、この制度に参加した地域の商店やリゾート施設など、さまざまなところで買い物をする、

© 2019 PIJ

【図表 16】マイナンバーカードを使った自治体ポイント制度とは



あるいは有償のサービスを受けるとポイントを貯められるのが官製の自治体共通のポイントカードの仕組みですね。

（石村）そうです。溜まったポイントは他の自治体のある店舗や公的サービスなどにも使えます。

（清水）「マイナンバー」とか子どもだましのような愛称を使っていますが、国民全員に 12 ケタの番号をふって管理する共通番号制、いわゆる「国民総背番号制」ですからね。

（石村）こんな官製の共通ポイントプランには、大なり小なり、まともな住民ならば、警戒しますよね。

（清水）それに、消費者は、民間のポイントサービスの取扱いに非常に敏感になってきていますからね。

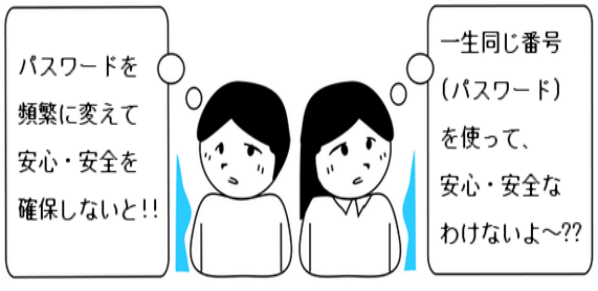
（石村）「できるだけ頻繁にパスワード（番号）を変えて、犯罪に備える」という時代です。それなのに、国民に対して 12 ケタの背番号をつけて、一生涯にわたり幅広く使えというわけです。

（清水）危機管理もへったくれもあったものではありませんからね。

（石村）明らかにこの時代にマッチしない番号制度です。

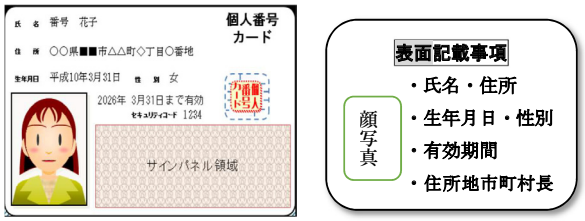
（清水）それに、まともな市民なら、自分の背番号（マイナンバー）に加えあらゆる基本情報が券面に記載されたマイナンバーカードも、毎日持ち歩きたくないでしょう。

【図表 17】同じパスワードを生涯利用するって大丈夫？？

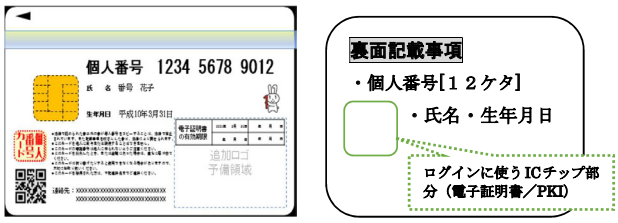


【図表 18】個人番号カードのイメージ

《個人番号カード「表」》



《個人番号カード[裏]》



（石村）そうです。12 ケタの自分のマイナンバー（個人番号）や写真・生年月日・住所などの基本情報が記載された IC カードを、なくしたら危ないですからね。

（清水）こんな他人に知られたくない情報がてんこ盛りのカードを、裸で、毎日持ち歩けというのは、どうかしてますよ。

（石村）総務省は、何と言われようと、いまだ 12%程度に留まるマイナンバーカードの交付率、普及率を引き上げたいと考えているわけです。

（清水）そこで、自治体ポイント制度を導入して、ポイントをエサに、住民にもっと IC カードを持たせようと画策しているわけですか。

（石村）自治体ポイントは、総務省の不純な動機が透けて見えてくるようなプランです。消費税増税で「切れ目のない景気対策ではなく、カードを持たせるための切れ目のない悪だくみ」といったところです（笑い）。

（清水）第一、この種の共通ポイントカードは民間にひしめいていますからね。

（石村）先ほどから問題になっているわが国最大手の一つである「T カード」は、年間の T カード利用者が人口の半分を超える 6,676 万人にも達し、提携店も 83 万を超えています。加えて、〝体力勝負〟といわれるほどスマホを使った民間の決済＋ポイント集約の仕組みも続々と誕生しています。

（清水）ポイント集約という民間がやっていることを、新たに官がやるのはどうかと思いますね。それに、T カードも、スマホのポイントを格納できる「モバイル T カード」に移行していますからね。

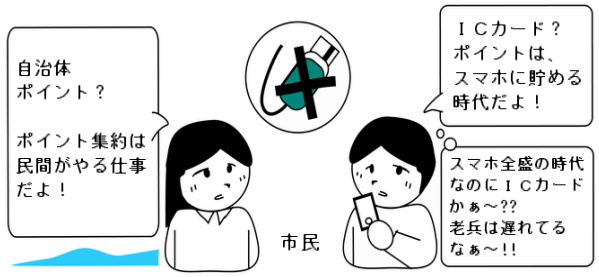
（石村）廃止される住基カードに続く、ガラパゴス

化した官製の危ないマイナンバー（個人番号）カードを使ったポイントプランは、もうたくさんですよね。しかも、この官製の自治体ポイントに参加する仕組みは複雑です。実際に店舗などでポイントを使おうとすると、IC カードリーダーを設置しており、そこで IC カードをカードリーダーに差し込んだり、かざしたりしなければなりません。12 ケタの個人番号が丸見えになるおそれもあります。高齢者などには管理が大変で使い勝手が悪いうえ、家族や友人間でカードの使い回しも想定されます。なくしたり、悪用される危険が高いわけです。

（清水）失敗に終わった住基カード、そして今度は、マイナンバーカードや自治体ポイント・・・中央のお役人は、本当に懲りない面々ですね。

（石村）民間のスマホポイントが拡大しています。民業圧迫、素人官業のマイナンバーカードを使った「自治体ポイント」プランは必ず血税のムダ遣いに終わるとみています。

【図表 19】IC カード？スマホ全盛の時代なのに？？



（清水）それこそ「危ないマイナンバーカードで集められた自治体ポイントとつるむ自治体警察による危ない使われ方」に、もっと警戒する必要がありますね。

（石村）そうです。民間のポイントカード以上に注意が必要です。

（清水）マイナンバーカードの利用履歴なんて捜査当局に一番便利に使われるようになりますよね。

（石村）そう思います。警察は、わざわざ個別に照会する必要もなくなって、自治体ポイントのデータベースから直接検索できるようになるでしょう。

◆「不健康」なマイナンバーカードの健康保険証化

（清水）最近報道されたマイナンバーカードを健康保険証化し、2021 年から全員にカードを持たせようという計画も、カード普及策のその 1 つとみてよいと思いますが・・・。

（石村）そうですね。政府は、今国会に提出した健康保険法改正案にマイナンバーカードを保険証として利用可能にする規定を盛り込んでいます。マイナンバーカードの健康保険証化に向けた関係省庁で作業部会を設けたようです。「健康保険証」にすれば、マイナンバー（私の背番号）カードを持たないわけにはいかない、逃げられない、と読んでいるのでしょう。実は、こうした計画は過去に何度も提案されています。

（清水）しかし、先ほどもいいましたが、まともな市民なら誰しも、マイナンバー（私の背番号）が書かれた健康保険証を裸で持ち歩きたくないですよね。

（石村）スマートでない役人は、スマート行政、電子政府（マイナポータル）構想実現には、マイナンバー（私の背番号）カードが必須アイテムだというのですが・・・。

（清水）しかし、世は IC カードリーダーをつなげないスマホ全盛の時代ですよね。時代錯誤だと思いますが・・・。「○○さんは、死んでも、マイナンバーカードを放しませんでした」の時代の再来は止めにして欲しいですね（笑い）。

（石村）私も、時代錯誤、ガラパゴス化したアイディアだと思います。

（清水）結局、スタンドアローン【編集局注：他のネットサービスには結びつかない】の健康保険証の IC カード化で終わるのではないですか？？お役人は、この執念を統計管理の適正さにでも向けりゃまだましなのに・・・。

（石村）何度もいいますが、世はスマホ全盛時代で、IC カードで政府ポータル（マイナポータル）サイトにログインする時代ではないですからね。

（清水）IC カードリーダーがないとネット空間に入れないのでは、電子申請も何もできない。それこそスマート行政を考えるなら、はじめから、漏れたら危ないマイナンバー（私の背番号）とかを隠せるスマホとかモバイル端末に入れられるようにすべきでしょう。いまどき IC カードの普及はないでしょうに・・・。

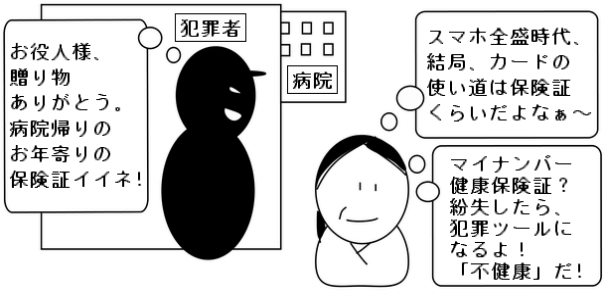
（石村）このままでは、スマートでない役人連中のせいで、スマート行政は実現できません。逆に、個人番号を含むあらゆるベーシックな個人情報が書かれた健康保険証カードの紛失・盗難、カードの悪用、なりすまし犯罪、振り込め詐欺などが多発するでしょう。もう、これは「権力の犯罪」です。

（清水）カードに書かれた基本的な個人情報は犯罪ツールに利用できますからね。

（石村）そういうことです。それこそ、自分の国民

© 2019 PIJ

【図表 20】マイナンバーカードの保険証化は「不健康」だ！



【図表 21】カード持たない人は「非国民」？？

背番号である 12 ケタのマイナンバーが券面に書かれた健康保険証など、まったく「健康ではない」わけです。

（清水）「不健康」そのものですよね。

（石村）役人は、「不健康」なマイナンバーカードの健康保険証化で、スマート行政、政府ポータルサイト（電子政府インフラ）、マイナポータルの利活用が格段にすすむと〝夢〟を語っています。

（清水）しかし、ゆめはゆめでも〝悪夢〟になるのではないですか。高速増殖炉・もんじゅのケースもありますからね。

（石村）あるいは、役人は、もう、いまのマイナンバーカード方式の電子政府（マイナポータル）はうまくいかないと見ているかも知れません。不健康な健康保険証カード構想と、電子政府（マイナポータル）構想とは別の問題と割り切っているのかも知れません。

（清水）要するに、「国内パスパート」として国民全員が背番号と顔写真つきの不健康な健康保険証カードを持ち歩け、国民 ID 制度を導入するんだ、と・・・。

（石村）そうです。「二兎追う者は一兎も得ず」の気持ちで、不健康な健康保険証カードだけでも成功させると！！

（清水）なるほど。不健康な健康保険証カードで、IT ハイエナ企業も特需で大喜びですからね。反対している議員も、実施してしまえば、いずれは、仕方ないと受け容れる・・・。

（石村）そうです。総務省などの役人は、健康保険証カードの形で国民全員に ID カードを持たせる。そして、警官に警察の犯歴データベースにリモートアクセスできる無線式の IC カードリーダーを持たせて街中を巡回するようなデータ監視国家、データ監視社会づくりに懸命なのでしょう。最初に、不健康な健康保険証カードを議員会館への入館管理に使うかも知れません。

（清水）そうなると、不健康な健康保険証カードの常時携行の強制、「マイナンバーカードか健康保険証カードを持たない人は、非国民」のような監視国家の流れを加速する怖れもありますね。

（石村）たしかに、マイナンバーカードと合体した健康保険証カードの治安利用は進むと思います。

（清水）しかし、電子政府（マイナポータル）に利用が進むかは別問題ですね。

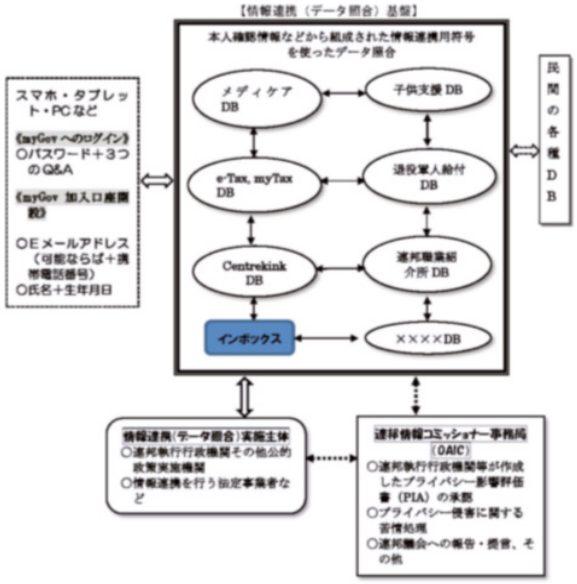
（石村）そうです。役人が、本気で、最近はじめた電子政府（マイナポータル）がスムースに動くようにしたいのなら、マイナンバー IC カード、あるいはマイナンバーカードと合体した健康保険証カードを使わない方式に変えないといけませんからね。

（清水）石村先生、IC カードを使わない方式の電子政府ポータルサイトを稼動させている国もあるのですか？

（石村）オーストラリアでは、スマホや iPad 全盛時代に対応して、IC カード（PKC）を使わない電子政府（myGov）、電子申告（myTax）を導入しています。

（清水）オーストラリアでは、政府ポータルサイト

【図表 22】オーストラリアの背番号と番号カード不要の「myGov」ポータルサイトのイメージ



に入る（リモートアクセス、ログインする）には、パスワード＋３つのQ&Aでいいのですね。

（石村）そうです。一方、わが国の場合は、政府ポータルサイト（マイナポータル）に入る（リモートアクセス、ログインする）ときには、マイナンバーICカードを使うわけです。ところが、ログインに12ケタのマイナンバー（私の背番号）を使うわけではありませんからね。

（清水）えぇ〜、そうですか！

（石村）そうです。マイナンバーICカードに格納されているPKI（公開鍵・電子証明書）を、セキュリテイ対策に使うだけです。

（清水）つまり、オーストラリアの政府ポータルサイト（myGov）では、データセキュリティ対策にPKI（公開鍵・電子証明書）は使っていない。だから、ICカードは不要だと・・・。

（石村）PKIは使っていません。代わりに、固定パスワード、ワンタイムパスワードを使っているわけです。

（清水）オーストラリアは、相当、先読みしていますね。

（石村）そうですね。PKI（公開鍵・電子証明書）が格納されたICカード方式にすると、ICカードリーダーが必要となります。スマホやiPadのようなモバイル端末には、ICカードリーダーは接続できません。ムリに接続すると、不具合を起こします。

（清水）石村先生は、このままでいくと、わが国の政府ポータルサイトは、どうなると見ておりますか？

（石村）先ほどから指摘してますように、マイナンバーカードは、スタンドアローンの健康保険証カードになるかも知れません。しかし、電子政府インフラのツール（道具）としては、住基カードと同じ運命になる可能性が高いと思います。

（清水）やはり、今や、モバイル端末中心の時代であると？

（石村）そうです。住基ネットが騒がれた時代以上に今はネット取引や事務はスマホ中心の時代に移行していますからね。

（清水）この辺の事情を、政府や議員、それから裏方で支えているお役人は共有しているのでしょうか？

（石村）少なくとも、国税庁は、その辺はわかっていると思います。マイナンバーカードを使わないでも、スマホを使ってID・パスワードで、課税庁ポータルサイトにログインし、納税者本人が電子申告できる仕組みに舵を切りましたから。

（清水）そうですか。やはり、国税庁は、ICカードリーダーが必要なマイナンバーカードを使った電子申告は、時代に合わなくなってきていると悟っているのですね。

（石村）ただし、現時点では、限られた本人電子申告だけです。複雑な申告や税理士が行う代理人申告は、業界発行のICカードを使わなければなりません。

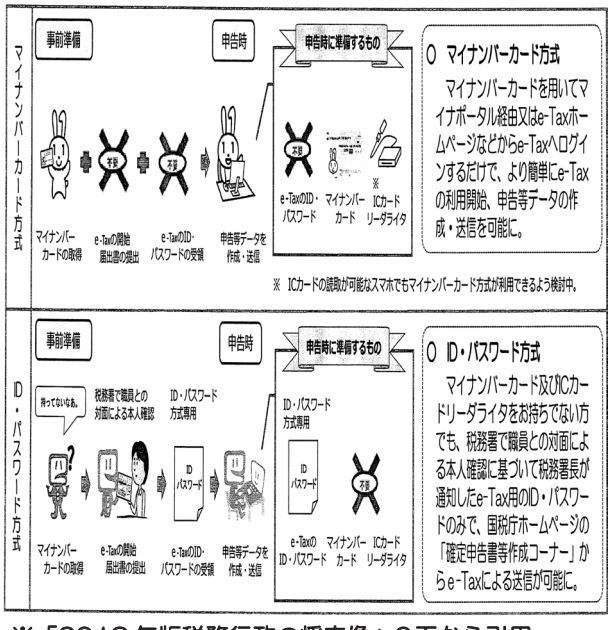
（清水）今後、マイナンバーカードを使わないID・パスワード方式の電子申告は、拡大していくのでしょうか？

（石村）拡大していくと思います。ただ、2019年1月にはじまったばかりです。どの程度の成果が出るのかは、不透明です。それに、申告する所得が給与だけとか、源泉徴収票が1枚だけとか、年末

【図表23】リモートアクセスで使われる認証方式：主要なデータセキュリティ対策の選択

認証方式	導入コスト	利便性	なりすまし対応度	マイナス面
○固定パスワード	低	高	低	安全度が低い
○ＰＫＩ（公開鍵・電子証明書）	中	低	高	運用が煩雑
○ワンタイムパスワード	高	高	高	コストが割高
○生体認証	高	高	高	容認度が低い
○その他（マトリクス認証等）				

【図表24】マイナンバーカード方式とID・パスワード方式のe-Tax（2019年1月以降）



※「2018年版税務行政の将来像」6頁から引用

© 2019 PIJ

調整が済んでいるとか・・・まだまだ使い勝手が悪いですね。

◆プラットフォーマーによるポイントカード情報の使われ方

（石村）清水先生はご存じだと思いますが。経営手法の１つてして「プラットフォーム・ビジネス・モデル（platform business model）」があります。「platform」は、和製英語読みは「プラットホーム」ですが。ここでは、「プラットフォーム」と呼んでおきますが・・・。

（清水）よくわかりませんが、「プラットフォーム」って、いわゆる駅の「列車のとまる場所」、「鉄道駅」ですよね。

（石村）そうです。この言葉は、事業をする「場」とか「基盤」とも邦訳されます。つまり、書店やスーパー、デパートとか、そして大きいものではトヨタとかキャノンとか、目にみえる「現実経済市場」にしっかりした事業基盤をおいてビジネス（生業）をしています。しかし、インターネットの普及とともに、「現実経済市場」にしっかりした事業基盤をおかないで、ネット空間ないしサイバー空間でビジネスをする企業も多くなってきました。

（清水）楽天とかアマゾンとか。IT起業家とかもてはやされているビジネスですね。

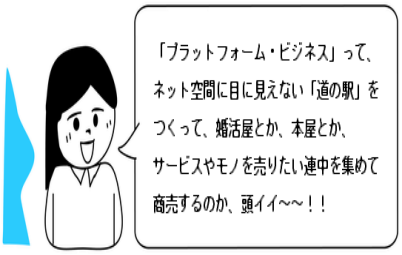
（石村）そうです。インターネットとパソコンないしスマートフォンやiPadのようなモバイル端末などでつながれている目に見えないサイバー空間に広がるネット経済市場、～デジタル経済市場ともいいますが～そうした目に見えない市場にプラットフォーム（事業基盤）をおいて、多くの事業者と消費者との取次業をやっている企業がすごい勢いなわけです。

（清水）GAFA／ガーファ（クーグル・アマゾン・フェースブック・アップル）、中国のBAT（バイドゥ・アリババ・テンセント）、それに国内の楽天・ヤフーとかですね。

（石村）そうです。これらのIT企業は、「デジタル・プラットフォーム企業（digital platform company）」、あるいは「プラットフォーマー（platformer）」と呼ばれます。国によっては「デジタル・マッチメーカー（digital matchmaker）」、「電子仲人」とも呼ばれます。とくにGAFAとかは、「テック巨人（tech giants）」と呼ばれます。

（清水）いわば、ハイテクやビッグデータをうまく使って、ネット空間のいろいろな企業や消費者

【図表25】ネット空間に「道の駅」をつくる？？



が集まれる〝フォーラム（広場）〟、いや〝プラットフォーム〟を築いて、中継の商売するビジネスモデルですね。ネット空間に、目に見えない「道の駅」をつくるみたいなものですよね？？

（石村）さすが、清水先生は、頭の回転が速い（笑い）。米フェイスブック社の傘下で運営されている写真共有アプリ「インスタグラム（Instagram）」や対話アプリ「ワッツアップ（WhatsApp）」は、〝フォーラム〟、〝プラットフォーム〟です。ですから、ひとくちに「プラットフォーム・ビジネス・モデル」といっても、実際にこのモデルを応用した事業はいろいろあるわけです。

（清水）アマゾンや楽天のように、商品や書籍、各種サービスなどを売手企業と消費者との間の取引仲介型プラットフォーム企業は１つの応用例だと。

（石村）そうです。実は、「Tポイント」のような、コンビニやレンタルショップなど、いろいろな店で買い物をするとポイントを貯められる共通ポイントカードもそうです。これも、プラットフォーム・ビジネス・モデルを応用した事業です。自治体ポイントもそうです。ネット空間に構築された目に見えない「道の駅」ビジネスです。

（清水）ペイペイ（PayPay）やペイパル（PayPal）のようなスマホを使った民間の決済＋ポイント集約型の事業もそうですか。

（石村）そうです。広い意味でのプラットフォーム企業、プラットフォーマーに含まれます。ですから、大小さまざまです。GAFAのような巨大プラッ

タッチ決済でき、ポイントも溜まる（public use）

トフォーマーは総体で、全人類の８割の個人データを独占しているといわれます。

（清水）国内のポイントカード運用（発行）会社も、規模は別として、一応プラットフォーマーであるということでは同じだと。

（石村）そうです。巨大なGAFAは、今や国家さえ尻込みする存在です。GAFAに比べるとTポイントカードなどは米粒です。しかし、会員の個人データを集約して、それをビッグデータとして利活用し、新たなビジネスにつなげようとしている点では同じです。消費者・会員のデータを利活用するビジネスである点に注意する必要があります。

（清水）ということは、ポイントサービスを利用する会員は、「タダでポイントをもらっているわけではない。自分の購買履歴など個人データをポイントカード運用（発行）会社にさらけ出してポイントをもらっている。」という自覚が要りますね。

（石村）そうです。ポイントカード運用（発行）会社にストックされた個人データは、捜査当局の照会に提供されるだけではありません。会員の信用確認や他の事業目的に使われることもあります。会員は、この点の自覚が必要です。

（清水）おおかたの消費者は、個人データはタダと思っています。ところが、プラットフォーマーにとっては、資源なのですよね。

（石村）そうです。データは、ネット経済市場で採掘できる「目に見えない石油」のようなものです。

（清水）ビジネスの軸足が大きくモノ（リアル）からデータ（デジタル）の経済市場に移り、データ（デジタル）はあらたな「富」を生むことになったということでしょうね。

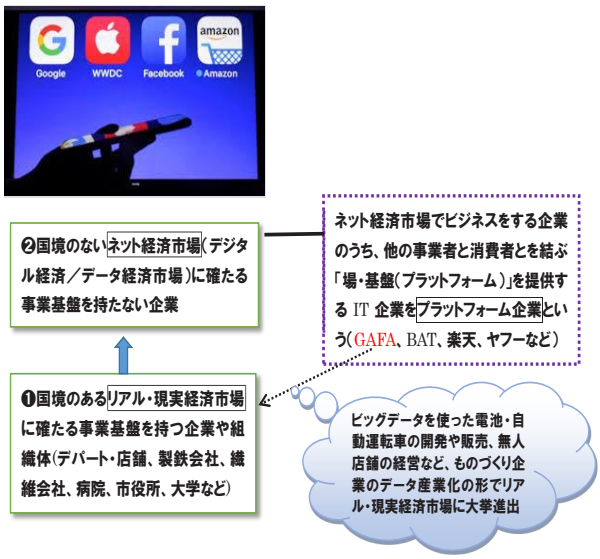
（石村）そういうことです。ですから、目に見えない石油を採掘し、手にしたプラットフォーマーが、それをどう使うかわかりません。市民・消費者は、危ない使い方をしないか、警戒しないといけないわけです。

（清水）プラットフォーマーが、巨人か、米粒かは問わないわけですね。

（石村）そうです。GAFAをはじめとした巨大なプラットフォーマーは、手に入れたビッグデータをもとに、電池・自動運転車の開発や販売、無人店舗の経営など、ものづくり企業のデータ産業化の形で、❶リアル、現実経済市場に大挙して進出してきています。

（清水）最近、政府統計の不正が問題になっています。「公正」な経済統計とは何かを考える場合には、❶リアルに加え、❷ネット経済市場でのデジタル企業活動の正確な測定も重い課題ですね。

【図表26】プラットフォーム企業の所在



（石村）そうです。自動車や鉄鋼のような、ものづくり企業を中心とした経済統計は、終わりの時代に突入しています。

（清水）リアルとネットを包括した経済統計をつくる。そして、その統計に基づいた産業政策、労働政策、市場競争政策、個人データ保護政策、課税政策を立てる必要がありますね。

（石村）ついでにいいますと、いま、世界各国やOECDのような国際機関は、データという新たな「富」「果実」に、どのように課税し、税収をどのように国家間で配分するか、大きな論争になっています。

（清水）課税がリアルにだけ集中し、ネット課税がないがしろにされてきたことが原因ですか？

（石村）そうです。20か国・地域（G20）首脳・閣僚会議でも重要なテーマになっています。今回は、デジタル課税はテーマではないので、あまり深入りしませんが。

◆EUのGDPRに学ぼう！

（清水）話を戻しますが。たしかに、巨大ITのGAFAに比べると、ポイントカード運用（発行）会社は、米粒のようなプラットフォーマーです。しかし、個人データの提供と引き換えにポイントをもらう会員は、自分のポイントカード情報の危ない使われ方に注意する必要がありますね。それに、わが国ネット経済市場での個人データ保護が、EU（欧州連合）とかと比べると脆弱なことにも注意する必要がありますね。石村先生が、CNNニューズ各号で指摘されているところですが・・・。

© 2019 PIJ

（石村）そのとおりです。この点で、EUは、リアル・現実経済市場にプラットフォーム（工場・店舗・その他の施設）を築いてビジネスをしているモノづくり企業と、ネット経済市場にプラットフォームを築いてビジネスをしている企業（デジタル・プラットフォーマー）を、個人情報保護、課税、独占禁止、知的財産権などの面から、同じように規制しようしています

（清水）つまり、ネット経済市場での目に見えない石油の防火・消防・放火犯処罰のシステムが整備されているわけですね。

（石村）そうですね。リアル・現実経済市場とネット経済市場と同等に取り扱おうとしています。イコールフッテイング（equal footing)、つまり双方の市場での「競争条件の対等化」が狙いです。

（清水）EUでも、従来は、ネット経済市場でビスネスをやってきたプラットフォーマーは、まったく自由放任でした。営業の自由を謳歌し、それで、1国家が介入できないほどIT巨人（tech giants）になってしまったわけですね。

（石村）そうです。それで、EUは、近年、GAFAのような巨大プラットフォーマー（tech giants）をターゲットにして、あらゆる法令を総動員して公的規制をかけているわけです。わが国も、遅ればせながら、ネット経済市場の公正確保を旗印に、GAFAの封じ込めに躍起になっています。しかし、内実は、役人主導で国内IT企業の権益保護の姿勢が目立つわけです。

（清水）「市民不在だ！」と。

（石村）そうです。EUの一般データ保護規則（GDPR／ジーデーピーアール）は、EU市民に、削除権（忘れられる権利）など高度の情報プライバシー権（個人データの自己コントロール権）を法認しました。EUは、「加盟国市民は、国境を越えて飛び交う大量情報（ビッグデータ）を手にしたGAFAに、強力な情報プライバシー権を保障したGDPRを武器に果敢に挑め！」といった戦法を採ったわけです。

【図表27】EUのGDPRで法認した主な情報プライバシー権

●個人（データ主体）は、次のような権利を有する。

- 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（GDPR 7条以下)。
- 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、**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)を取り戻し、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)。
- **巨額の制裁金**　プラットフォーム企業などが、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（1€=125円換算で、12億5,000万円)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（25億円）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（GDPR83条)。
- **強力な権限を持つ監督機関（データ保護機関）**　独立して官民双方の企業や機関に対して、GDPRその他の法令違反の調査、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権限を有する（GDPR51条以下)。

（清水）石村先生は、わが国も、EUの戦法を採用すべきだと。

（石村）そうです。個人情報保護法を改正し、市民

にEU並みの自己データのコントロール権を保障し、個人情報保護委員会を市民に寄り添える仕組みに大改革する必要があります。ところが、わが国の役人は、EUのGDPRに学び、市民にIT企業と闘う武器を与える戦法など、とんでもないといった感じです。

（清水）ヨーロッパは、革命やパルチザンなどの伝統がありますからね。しかし、私たち日本人は、「行政にお任せコース」が大好きです。

（石村）今日の日本人は、権利のために闘おうとする気概にも欠けている感じもしますし・・・。「小市民」で生きるのが大好きですからね。

（清水）沖縄も原発もそうですが、自分に降りかかるまでは関係ないと思っていられる脳内楽園の民の国ですからねぇ。

【図表28】EUのGAFA対策は市民主導だが・・・

（石村）わかります。ひとは考えても仕方がないほど力関係がアンバランスな状態では、考えないことを選択しがちですからね。

（清水）それに「刀狩」の伝統のある国ですから･･･。

（石村）わが国の役人も、その辺をよくわかってやっているのでしょう。

（石村）しかし、ここは、「刀狩」の伝統ではなく、市民にプライバシー保障という形でGAFAのようなIT巨人（tech giants）に闘いを挑める「刀」を与える戦法を採る、つまりEUのGDPRに学ぶべきではないか、と思います。

（清水）同感です。政治は「お役人や国内IT企業が主役」ではなく、「市民が主役」のスタンスが必要です。

（清水）市民・消費者に強いプライバシー権を認めたとします。そうすると、お役人は、いずれ市民は、それを振りかざして自分らに立ち向かってくるとでも思っているのではないでしょうか？

（石村）えぇ～、役人連中は、そんなスタンスでしょう。

（清水）それに、自分らが利権を護ってやろうとしている国内IT、プラットフォーム企業にも跳ね返ってくる心配もあるのでしょうし・・・。

（石村）しかし、国内IT産業利権ファースト、市民不在では、個人データはプラットフォーム企業、プラットフォーマーの餌食になることはあっても、市民のプライバシーファーストの公正なネット秩序がつくれません。

◆個人データの危ない使われ方にどう挑む

（清水）自分の専門の刑事法学に熱中していると、周りに疎くなりがちです。しかし、ネット取引については根深い問題があることを、改めて認識しました。

（石村）今回は、ポイント運営（発行）会社が捜査当局に会員のポイントカード情報を垂れ流しするのは問題だ、ということから議論がはじまりました。会員データは、会社にとって、「カネになる資源であり、会社の利益につなげられる」。一方、捜査当局にとっては、会員の「足跡」追求にも使える。こうした個人データの危ない使われ方が、あまり世間に知られずに久しく続いてきたわけです。

（清水）しかも、当の会員も、自分のポイント情報が捜査当局のターゲットとなることがあるとの自覚も認識も薄いわけですからね。

（石村）「悪いことしてなければ、怖がることはない」が大勢ということでしょうか？

（清水）しかし、現実は164日も拘置され、完全無罪になった村木厚労省元局長のようなケース、「人質司法」がまかり通っているわけですから・・・。

（石村）被疑者が捜査当局の描いた有罪の筋書に同意しないと保釈しないのが、諸悪の根源だと思います。同じように、ポイントサービスも、消費者は、データの提供に同意しないと、利用できないことにも問題があるのだと思います。

（清水）それに、一般の人は、利用規約を読んでも、よくわからないわけですからね。ある種のあきらめモード、泣き寝入りモードが蔓延しているのでしょう。

（石村）ですから、ポイント運営（発行）会社は、会員に対するていねいな説明責任が問われています。

（清水）それに、ポイントサービス会社も、企業倫理や会員のプライバシー権を護るために、法律解釈についてよく勉強し、会員が主役になるポリシー、ガバナンスを確立する必要があるわけです。

（石村）まさに、たばこにならって、ポイントサービス会社には、**《警告表示》「あなたのカード利用情報が警察に提供されプライバシーを損なうおそれがありますので注意しましょう」**を求める必要があります。カードの券面、あるいはスマホを使った決済＋ポイント集約型の場合は、スマホの画面に表示を義務付けるのも一案です。

（清水）この点は、素人官業のマイナンバーカードを使った自治体ポイントの危うさについてもいえますね。それに、マイナンバーカードといえば、健康保険証化プランも「不健康」そのものですね。

© 2019 PIJ

（石村）世は、モバイル端末全盛時代です。ネット空間、ネット経済市場へのアクセスにICカードを使うこと方式自体が、陳腐化しているわけです。

（清水）それでも、お役人は、負ける戦争へ突き進むわけですね。

（石村）市民も声をあげなければいけません。役人は、「法の支配」を口実に、それこそ「学徒動員」までやって、負けても、責任を取らない連中ですからね。「役人にお任せ」姿勢の市民、それに議員連中の姿勢も問われています。

（清水）それから、石村先生との対論を通じて、近年、目に見えないネット空間で大きく伸びているITビジネスの1つであるポイント運営（発行）事業の性格が、はっきりと見えてきました。ビックデータ（大量情報）をあらたな資源とした「プラットフォーム・ビジネス・モデル」を使った事業である、と確認できました。

（石村）和風の言い方をしますと、ネット経済市場での「道の駅」、「デジタル仲人」ビジネスモデルを使っているわけですね（笑い）。

（清水）それから、今日、経済市場が、モノからデータ（デジタル）に大きく軸足を移しています。ポイント運営（発行）のようなIT事業から、会員の情報プライバシーを護るには、現行の個人情報保護法制の抜本的な改革が必要なことも確認できました。

（石村）わが個人情報保護法制の大改革には、EUのデータ保護法制（GDPR）に学ぶべきです。具体的にいうと、①「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）」、②「忘れられる権利(right to be forgotten)」、いわゆる「削除権」、つまり、ヤフーやグーグルなどのネット検索エンジンで出てくる古い自分の記事データなどを消去してもらう権利です。それから、③「ダイレクトマーケティングを拒否する権利」、④「データポータビリティ権（right to data portability)」、つまり、清水先生について、例えばQP［クイックペイ］社が収集・ストックしている先生の個人データを、先生が引き出して他のPS［ペイサービス］社に移転できる権利などです。

（清水）「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」も保障されていますが。具体的には、どういった権利なのですか？

（石村）AIなどを活用して、個人データの照合、分析をして、その人の信用状態や消費性向などを評価することを「プロファイリング」といいます。本人が気づかないところで、プロファイリングして、企業が、カード利用の限度額を決める実務が問われています。また、捜査当局が、容疑者に仕立てる実務が問われています。これを放置しておくと、消費者・市民は不利益を被る可能性が出てくるわけです。

（清水）そこで、AIとかのハイテクを使って自動的な評価、決定に対して、本人が介入できる権利を保障したわけですね。

（石村）そんなところです。事前に本人の同意を得るとか、評価・決定に苦情をいう権利を保障するとか、手続を厳格にしているわけです。こうした評価・決定は、今日、紙ベースではなく、ネット空間を通じてデジタルで行われるわけです。例えば家電量販店で、高額の家電をカードで買うとします。その場合、店側は、信用情報機関にネットを通じて本人の信用情報（ホワイト情報・ブラック除法）を照会するわけです。一般に、本人に告知して照会していると思いますが・・・。いずれにしろ、信用情報機関は、照会があれば、プロファイリングしたうえで当人の信用情報を店舗側に提供しているわけです。こうしたネット空間を通じて実施される手続についても、個人情報保護法の網をかける必要があるわけです。具体的に、どういった状況にこの種の権利を適用するのかは、検討を要しますが・・・。

（清水）つまり、EUにならって、市民に対して、リアル〔現実経済〕市場だけでなくネット〔デジタル経済〕市場にまで保護が及ぶ包括的なプライバシー権を保障する必要があると。それで、個人データを乱暴に扱い、不公正なビジネスをするIT企業、デジタルプラットフォーマーなどと対峙できる「武器」を与えないといけないというわけですね。

（石村）そうです。今や、巨大プラットフォーマーのGAFAは総体で、全人類の8割のデータを握り、資産総額が邦貨で310兆円に達するとか・・・。わが国の国民（市民）も目を覚まさないといけませんね。

（清水）お役人依存体質の国民ですが・・・、自分の個人データは自分で護るといった気概が要りますね。そのためにも、市民（国民）の情報プライバシー権を自分で護れる、あるいはそれをサポートできる個人情報保護委員会に改革する法制の整備が急がれますね。

（石村）同感です。清水先生、今回は、ご多用なところ、専門的な観点から有益なご意見をありがとうございました。

総務省の「IoT 機器への侵入調査（ハッキングテスト）」は違憲

― 国家によるハッキング技術の「キナ臭い使われ方」への危惧 ―

【声明】 PIJは、総務省とNICT共同のIoT機器への侵入調査（ハッキングテスト）の中止を求める

PIJ運営委員会　2019年2月19日

◆ IoT 機器の光と影

エアコンが「室内温度が30度を超えたよ」とか、犬の首輪が「室内で犬が熱がっているよ」とか、モノがつぶやき、勤務中の人のスマートフォン（スマホ）やPCに知らさせる。インターネットの発達により、センサーと通信機能を持ったモノが世のなかにあふれている。こうした現象を、IoT（Internet of things／インターネット・オブ・シングス）、日本語で「モノのインターネット化」と呼ぶ。また、こうしたインターネットでつながった機器を「IoT機器」、「スマート家電」ともいう。IoT機器は、私たち市民の生活を便利にする。しかし、その一方で、これまでは考えられないような脅威、危険性も増してきている。ネットでつながったIoT機器が、外部から侵入してきたハッカーに乗っ取られ、ウイルス感染する、不正に操作されるケースが多発している。

ネットでつながった電子投票システムは、遠隔地からの投票には便利だ。しかし、外部から侵入してきたハッカーに操作される恐れもある。遠隔捜査できる発電所や工場の機械なども、同じ問題がある。このため、厳格な安全対策を講じている。

ところが、家庭用のIoT機器は、概して安全（セキュリティ）対策が甘い。この背景には、こうした機器は、パソコンやスマホのような目で確認できる画面を持たないためチェックしにくいことがある。ひとたび外部からハッカー攻撃を受ければ相互に接続されたIoT機器すべてに影響が及び、甚大な被害につながる恐れもある。まさに、IoT機器は、メリットとリスク、光と影、を抱える機器であるといってよい。

メリットを大きくしリスクを小さくするために、政府・総務省は、次のようなIoT機器への安全（セキュリティ）対策を強化する方針を打ち出した。

●政府・総務省によるIoT機器への安全（セキュリティ）強化対策

①法令（電気通信事業法に基づくIoT機器の技術基準を定める省令）を改正し、外部（不特定多数）からの操作を遮断する制御機能と、機器出荷時に初期設定されたIDやパスワードを変更する機能、ソフトウエアを常時更新する機能を備えたと認定されたIoT機器の販売だけを認めることにしたことだ。2020年4月から適用する。
②現在広く使われているIoT機器への国による侵入調査（ハッキングテスト）の実施である。

◆侵入調査（ハッキングテスト）とは何か

外部のインターネットにつながったIoT機器は、グローバルIPアドレスを持つことからサイバー攻撃を受けやすい。そこで、総務省は、2月20日から、現在使われているIoT機器の安全性を確認（セキュリティ・チェック）するために、無差別に侵入調査（ハッキングテスト）を始めた。この侵入調査は、IoT機器ネットに直接つながったルーターや防犯カメラ（ウエブカメラ）、センサーなどが対象である。パソコンやスマホなどの複数のIT機器をインターネットに接続するための家庭で使われているルーターも対象になる。しかし、その先につながるパソコンやスマート家電などには侵

●総務省のIoT機器侵入調査手順

© 2019 PIJ

入しないという。したがって、先にあげたスマート「エアコン」やスマート「犬の首輪」などは対象外となる。また、ネットに直接つながってはいないテレビや家電なども調査対象外である。

しかし、この前代未聞の総務省による侵入調査（ハッキングテスト）は、憲法が保障する「通信の秘密」などを侵害し違憲ではないか。市民や市民団体などから、大きな疑問符がついている。

◆多くは、初期設定のパスワードのまま

多くのIoT機器はセキュリティ対策が甘い。パソコンやスマートフォン（スマホ）と違って性能があまりよくなく、高度なセキュリティ機能を搭載できないのも一因である。工場から出荷された時点の初期設定の「admin」「password」「111111」「123456」といった単純なパスワードがそのまま使われている。このため、IoT機器はしばしばサイバー攻撃にあってきた。ただ、パソコンやスマホだと、起動しなくなったこと、ランサムウエアでの身代金の要求があったなどを画面で確認できる。それが、画面を持たないIoT機器だと、攻撃を目で確認できない。また、攻撃を受けたとわかっても、メーカーが制御ソフト（ファームウエア）を更新しなかったり、利用者が気づかずに見過ごしてしまったりするケースも多い。深刻な被害にあうことも少ないからである。

2020年の東京五輪・パラリンピックが間近に迫っている。政府や総務省は、IoT機器がハッカーに乗っ取られ、オリンピックへのサイバー攻撃に悪用され、暴れ出すことが心配だという。そこで、今回、国家が主導して異例の侵入調査（ハッキングテスト）を実施した。2020年を前にして、サイバー攻撃の被害を最小限に食い止めることが狙いだという（https://www.nict.go.jp/press/2019/02/01-1.html）。

◆調査方法

今回の侵入調査は、過去の大規模なサイバー攻撃に使われたこれらパスワードの組み合わせ100とおりを自動入力して実施。インターネットの住所に当たるIPアドレス約2億につながった機器が対象である。総務省は、侵入調査を、国立研究開発法人「情報通信研究機構（NICT）」や接続業者（インターネットプロバイダー／電気通信事業者）と連携して実施した。

侵入調査の結果、侵入できた機器の利用者には、今後サイバー攻撃を受ける可能性が高いと判断し、接続業者（プロバイダー）を通じて対策を促すという。なお、費用を請求したり、パスワードを聞き出したりすることはないという。

◆問題の所在を点検する

IT機器がかかえる様々な脆弱性の調査（ハッキングテスト）は、一般に「ペネトレーションテスト」とも呼ばれる。こうしたリスク調査をビジネスとしている企業も多く、実際のハッキングテストはセキュリティ関連の技術者が実施する。また、個人が侵入調査をするノウハウ本（たとえば、IPUSIRON『ハッキング・ラボのつくりかた』）も出ている。

ただ、政府（国家）が、企業や個人のIT機器に一方的にアクセスしハッキングテストをアナウンスして実施するのは、世界的にも例のないやり方だ。安全性（データセキュリティ）の確認とはいえ、国内で一般市民が行えば不正アクセス禁止法違反になる。そこで、18年5月に、総務省は、密かに関係法令を改正した。これにより、NICTと連携して、特別に5年に限ってハッキングテストを実施できるようにした[1]。総務省とNICTは侵入調査に関する情報を集めたサイト「NOTICE[2]サポートセンター」（https://notice.go.jp/）を開設し、市民に理解を求めている。

（1）通信の秘密保護と人格権保護とは表裏一体

日本国憲法は第21条第2項後段で、次にように定めて通信の秘密を保障している。

家庭用IoT機器侵入調査を通じて、政府、総務省は、通信内容を見るわけではない。このため、

【日本国憲法21条1項】 集会、結社及び言論、出版、その他一切の表現の自由は、これを保障する。
【同条2項】検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

[1] 先の国会で「電気通信事業法及び国立研究開発法人 情報通信研究機構法の一部を改正する法律案」が成立した。この法律のなかに「IoT侵入調査を合法化する条文」が盛り込まれた。詳しくは、http://www.soumu.go.jp/main_content/000595925.pdf
[2] NOTICE=National Operation Towards IoT Clean Environment

憲法 21 条 2 項が保障する「通信の秘密」の侵害にはあたらないとしている。

しかし、通信の秘密は、表現の自由と一緒に規定されている。憲法理論上、通信の秘密は、その性質上プライバシー権（人格権）として保護される。このことから、侵入しても、内容を見なければ権利侵害にあたらないとはいえないのではないか。

【日本国憲法 13 条】 すべて国民は、個人として尊重される。生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とする。

SNS（交流サイト）上では、「防犯のためといっても、人の家に勝手に入るのと変わらない。プライバシー侵害ではないか」と指摘する声が多い。一定の家庭用 IoT 機器に対する政府公認のハッキングテストが頻繁に行われるようになったら、どうだろう。サイバー空間は、善玉と悪玉のハッカーがウジョウジョする環境になる。そのうち、「政府公認になりすましたハッカー」がネット空間に出没するのではないか。家庭用 IoT 機器は、PC やモバイル端末とは異なり、画面を持たない。市民は、善玉と悪玉のハッカーを識別、選別することは困難である。市民が、政府公認のハッキングテストに不安を覚えるのは当り前である。

一歩譲って、仮に、これら一定の家庭用 IoT 機器に対する政府公認のハッキングテスト（侵入調査）の目的は正当であるとする。そうだとしても、侵入調査は、すでに時機的にみて、2020 年の東京オリンピックに向けたセキュリティ対策としては遅すぎる。言い換えると、実効性に欠ける。また、手段の必要性も相当性も認められないといえる。

また「セキュリティが弱いという個人情報」は、本人にとってはリスクの高い情報である。悪用されれば、重大な損害につながりかねない重要な情報である。こうした情報を探査・収集・集積・保管・データベース化する行為は、プライバシーに対する重大な脅威につながる。いってみれば、普段玄関に鍵をかけないこと自体よりも、そのことを知られることの方が、リスクが高いのである。このことから、そもそも市民は、憲法 13 条のもとで、この種のリスクを含んだ個人情報を、国家に収集されない自由、あるいは収集されることから放っておかれる権利（right to be left alone）が保障されていると解してよい。さらに、市民は、国家による侵入調査で収集された個人のリスクを含む情報（データ）に対するアクセス権、削除を求める権利が認められなければならない。

（2）強制的な侵入調査と令状主義・適正手続

さらに、憲法 35 条は、次のように規定して、令状主義を保障している。

【憲法 35 条 1 項】 何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第 33 条の場合を除いては、正当な理由に基いて発せられ、且つ捜索する場所及び押収する物を明示する令状がなければ、侵されない。
【同条 2 項】 捜索又は押収は、権限を有する司法官憲が発する各別の令状により、これを行ふ。

憲法 35 条は、公権力が私人の家屋や私物に侵入するには令状を必要とする令状主義を規定している。この規定は、刑事捜索を対象としたものと解されている。行政調査には適用がないものとされる。しかし、行政ならば、どんな侵入調査（ハッキングテスト）でもゆるされるとはいえないのではないか。SNS に寄せられた侵入調査を危惧する声は、市民感覚としては当然である。

現に令状なしの警察による GPS 捜査は、最高裁により違法とされている（最大判 H29.3.15）。このケースでは、動向の把握だけでも重大な権利侵害とされたものである。通信内容に限らず、インターネット利用状況の無差別的な探知による平穏・プライバシー侵害自体も、目的と手段の比例性の観点から、憲法に保障にされた人格権を侵害し、違憲の疑いが濃い。

そもそもプライバシーの侵害につながる侵入調査については、その必要性がしっかりとチェックされなければならない。そしてしっかりとチェックするためには、個別に丁寧にチェックされる必要がある。捜査令状も、憲法 35 条 2 項に定められているように「各別の令状」でなければならない。「一般令状」は法認されていない。

「ねずみとり」と呼ばれる交通検問が、警察により各所で随時実施されている。しかし、その法的根拠はあやしい。その適法性は昔から問題にされてきている。交通違反をしている個別の疑いもないのになぜ半強制的に停止させることができるのかが問われているわけである。建前上、ねずみとりは、相手の同意を得て行われる任意処分とされている。任意処分ですら無差別・一斉に行うことの適法性が問われているのである。

例えば、ある地域に殺人犯が逃げ込んだとする。だからといって、警察官が無差別に周辺の家の中

© 2019 PIJ

をのぞくことは許されない。ましてや、個別の具体的な危険が明白ともいえないのに、行政当局が手当たり次第ドアを開けて回るようなことが許されるだろうか？まさに、今回の個別の同意を前提としない国による侵入調査（ハッキングテスト）の適法性が問われる理由でもある。

今回の侵入調査（ハッキングテスト）は、個別の必要性も確認されずに、アトランダムに実質強制の形で一斉に実施されている。つまり、個別の嫌疑（つまり必要性）をチェックすることなしに行われている。これは、明らかに憲法 35 条 2 項の趣旨に反している。

ちなみに、憲法 31 条は、次のように規定して、適正な手続を保障している。

【第 31 条】 何人も、法律の定める手続によらなければ、その生命若しくは自由を奪はれ、又はその他の刑罰を科せられない。

憲法 31 条は、刑事手続に加え、行政手続にも適用があると解されている[3]。このことから、今回の国家（公権力）による実質強制の侵入調査（ハッキングテスト）は、行政処分にも適用がある憲法 31 条の適正手続の保障に違反するというほかない。

問題は侵入調査(ハッキングテスト）だけではない。ほかに東京圏の監視カメラ網の高度化、大量のボランティアの「リアルな目の徴用」など、東京オリンピックのレガシーは、監視国家総動員体制の確立といっても過言ではない。

●東京オリンピックのレガシーは監視国家総動員体制の確立？！

◆危惧されるハッキング技術の軍事転用

たしかに、今般の侵入調査（(ハッキングテスト）は、ルーター・ウエブカメラ（監視カメラ）・センサーといった限定された IoT 機器を対象としている。しかし、いま芽を吹いたばかりだ。今後、行政がその気になれば、侵入調査はスマホや PC などにもエスカレートさせることも可能だ。市民に開放されているはずのネット網で、国家が覆面でハッキング活動をすることも可能とする。ひいては､習得したハッキング技術を、法令の適用除外を設けないまま、任意の形で特定個人へのネット攻撃・遮断など治安利用される可能性も否定できない。究極的には、ハッキング技術の「軍事転用」への道も開かれるのではないか。平和憲法を持つことを軽視する政権は、他国の軍事施設などの破壊工作にこのハッキング技術を転用することも可能だ。技術の転用に歯止めがかからないことが危惧される。私たちは、今回の一般市民を実験台にした国家によるハッキング技術の「キナ臭い使われ方」「軍事へのエスカレート利用」対する監視を怠ってはならない。

●ハッキング技術のキナ臭い使われ方が心配！

◆通信内容への覆面ハッキング捜査利用の危惧

こうした侵入調査で培ったハッキング技術を、軍事に転用するのは考え過ぎとの指摘もあるかも知れない。しかし､法令に適用除外を設けることなく、通信内容への侵入を含めて、刑事捜査へのエスカレート利用は想定される。ハッキング技術が、任意捜査の形で、その必要性と相当性（刑訴法 197 条 1 項本文）を超えた通信内容の捜索に使われるとすれば、違法、通信の秘密を侵害し違憲でもある。

これは、すでにふれたように、令状なしの警察による GPS 捜査が、最高裁により違法とされている（最大判 H29.3.15）ことからも自明のところだ。また、令状なしの警察によるハッキング技術を使った、通信内容にエスカレートさせた侵入捜査は、憲法 31 条にもぶつかる。憲法 31 条は、刑事手続に加え、行政手続にも適用あると解されているからである。また、31 条は、手続を法律で定めることのみならず、一般的には、①手続が適正でなければならないことを意味すると解されている。このことから、今回の行政主導の実質的に強制的な IoT 侵入調査については、適正な手続が確保されているのかどうかも問われてくる。

[3] 川崎民商事件（最大判昭和 47.11.22 刑集 26 巻 9 号 554 頁）、成田新法事件（最大判平成 4.7.1 民集 46 巻 5 号 437 頁）参照。

今回の IoT 侵入調査実施について、総務省と NICT は、共同で NOTICE の周知広報をしている。市民団体からは、今回の IoT 侵入調査は、憲法に保障された私たち国民の権利を侵害するものであり実施の中止を求める声があがっている。しかし、異論・反論を集約したような様子はみられない（https://www.nict.go.jp/press/2019/02/01-1.html）。

◆行政独走のハッキングテストは危ない

今回の国家による家庭用 IoT 機器への侵入調査（ハッキングテスト）は、ネットセキュリテイに資するというよりは、ネットの自由を阻害する危ない策略である。行政独走で、国会ではまったく審議されず、ネットの自由を享受する市民にとっても、寝耳に水といってよい。憲法に保障された通信の自由やプライバシー権、手続的適正などの面からも大きな疑問符がつく。治安や防衛目的で通信内容への侵入や破壊工作などを含めたハッキング技術の将来的なエスカレート利用が心配される。にもかかわらず、法的歯止め策や今後の政策も国会でまったく議論されていない。平和憲法を持つわが国は、ロシアや中国のようなハッカー大国への道はゆるされない。議員やマスメディアに、この問題の重さが共有されていない。市民団体は、侵入調査（ハッキングテスト）の実施開始間近に、「総務省、国立研究開発法人情報通信研究機構（NICT）による『IoT 機器調査』の中止を強く求めます」との声明を出した。

プライバシー・インターナショナル・ジャパン（PIJ）も、今回の総務省と NICT 共同の IoT 機器への侵入調査（ハッキングテスト）の即時中止を求める。

コラム

進化するスマホと犯罪抑止のホワイトハッカー？？

スマートフォン（スマホ）の進化が止まらない。通話機能からスタートした携帯電話は、今や、ショートメール、ゲーム、カメラ、地図、決済、電子申請など多様な機能を持つモバイル端末に大変身した。こうしたなか、T ポイントを運営する CCC グループから「スマホサイフ」アプリが登場した。iPhone、Android スマホで使える「スマホサイフ」とは、リアルな財布の中にあるカード集約アプリ。つまり、いろいろな店舗のポイントカード、スタンプカード、電子マネー、クレジットカード、キャッシュカードなどを１つの「スマホサイフ」アプリに集約し、貯めたり使ったりできる共通プラットフォームだ。

このように、現世は、カードからスマホ全盛時代へと大きく移行している。マイナンバーカードを使った自治体ポイントとかマイナンバーカードの健康保険証化のような、ガラ系（陳腐）化したプランは直ちにやめないといけない。明らかに時代に逆行している。

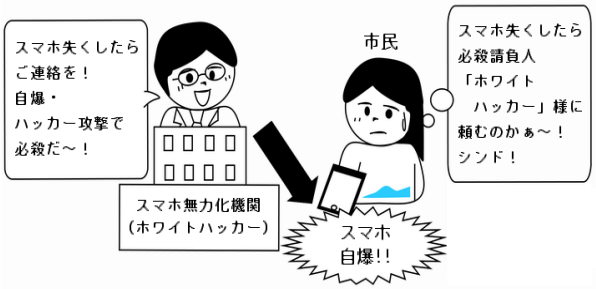
いずれにしろ、スマホサイフは、消費者にはお得なアプリのようにもみえる。だが、スマホサイフだけにして大丈夫なのだろうか。電源を喪失する、万が一のときに、決済やお金を引き出すことができなくなる。緊急時の脆弱性が増すのは明らかだ。これまで以上に運営会社の捜査照会からの会員情報保護手続や企業倫理の透明化も問われる。

このようにスマホ全盛トレンドにも弱点がある。とくに重い課題は、大量の個人データが詰まったスマホの紛失や盗難などへの対応だ。

今、総務省は、NICT（国立研究開発法人情報通信研究機構）や各インターネットプロバイダー（電気通信事業者）と共同で、IoT 機器への侵入調査（ハッキングテスト）を実施中だ。行政独走の公認のハッキングテストには強い批判がある。ハッキング技術の治安利用や軍事転用などが危惧されるからだ。

いずれの先端技術にも光と影がある。こうしたハッキングテストの「光」の面を探せるのか考えてみた。紛失したり、盗難にあったスマホに侵入（ハッカー攻撃）し、一気にデータを無力化し、スマホ所有者のプライバシーやデータ悪用から市民を護る仕組みの導入はどうだろうか？一言でいえば、スマホ全盛の弱点克服に「ホワイトハッカー」の登場をゆるすのかどうかだ。

●ハッカー技術はスマホ防犯の新兵器？？



もちろん、こうした破壊的ハッカー行為は、スマホ所有者本人の明示の同意が前提である。当然、どのような機関が実施するかも問われてくる。警察が実施するのでは余りにも危なすぎる。民間事業者に容認するのも、信頼性がいまいちだ。スマホメーカーないし各プロバイダーが連携して民間の「なくしたスマホ無力化機関」を設けて実施するのはどうだろうか。ただ、わが国の IT 業界の政府寄りのスタンスからして、市民の幅広いコンセンサスが得られるのかどうかは不透明だ。

© 2019 PIJ

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

【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？ ―

報告紹介

報告者 石村耕治（PIJ代表）

《石村 PIJ 代表の報告の紹介》

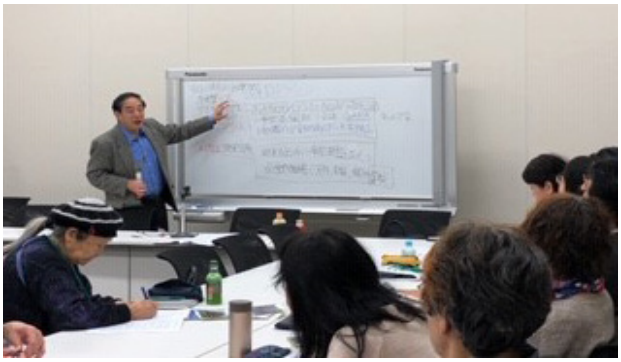
秘密保護法廃止へ！実行委員会と共謀罪 NO ！実行委員会は、協賛で、2019 年 2 月 6 日、東京・衆議院第 2 議員会館第 2 会議室で、石村耕治 **PIJ** 代表（白鷗大学名誉教授）を呼んで、「巨大 IT 企業 GAFA 対策としての EU の一般データ保護規則(GDPR)を読み解く～わが国は、『市民よ、GDPR を武器に GAFA と闘え！』の EU に学べるか？」と題して学習会を開催した。学習会には、マスメディア各社、社民党の福島瑞穂参院議員や議員秘書などが学習会に参加、立憲民主党の有田芳生参院議員は挨拶をした。当日の石村代表のレクチャー内容を、簡潔に紹介したい。　**（CNNニューズ編集局）**

◆問題の所在～現実経済とネット経済（デジタル経済／データ経済）とは

石村代表は、熱心な学習会の参加者の間に知識のばらつきがあることも想定して、ベーシックなことから、かなり噛み砕いて話された。

インターネットが普及していなかった時代には、さまざまな取引や行政事務などは、目に見える「現実経済（real economy)」あるいは「現実空間（real space)」のなかで行われてきた。つまり、買い物は店舗やデパート、CD ショップ、銀行、市役所などに出向くか、郵便で依頼するのが一般的であった。

ところが、インターネット（ネット）が普及した今日では、さまざまな取引や行政事務などで、情報化（デジタル化／データ化）できるものについては、ネットとパソコン(PC)・スマートフォン（スマホ）やアイパッド（iPad）のようなモバイル機器とで結ばれる目に見えない「サイバー空間（cyber space)」で行われるようになっている。一般には、電子商取引（e-commerce）とか、電子申告（e-Tax）とかいわれるものである。



衆院第二議員会館学習会で講演する石村 PIJ 代表
（写真：柏木美枝子氏提供）

取引や事務によっては、国境のある❶現実空間でないとできないものと、国境のない❷サイバー空間でもできるものがある。❶現実空間でないとできないものとしては、例えば、宅配便のような、いわゆる「物流（logistics)」をあげることができる。一方、❷サイバー空間でもできるものとしては、「貨幣（おかね）／仮想通貨／デジタル通貨」、「商品の展示・注文」「金融（決済／与信)」「教育」「音楽」などをあげることができる。現在、サイバー空間でもできる取引や事務は大挙して、現実空間からサイバー空間に移行している。サイバー空間取引や事務は、情報を紙（文書）からデータ（デジタル）に処理をする、ネットでやりとり（流通）する、ネットに保管（クラウド保存）する、といったプロセスで行われる。

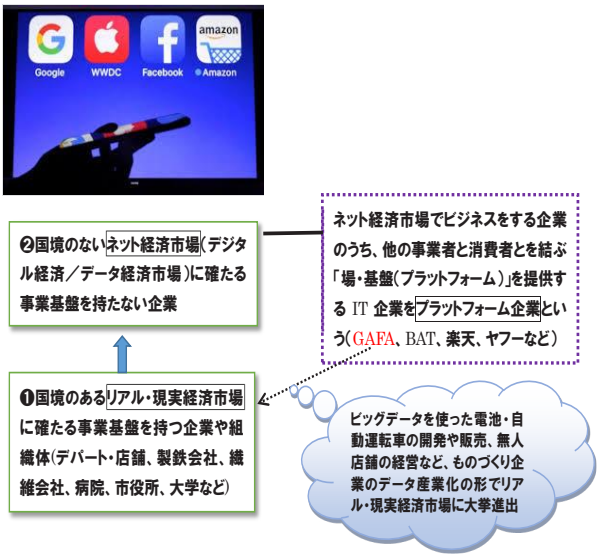
今日、市場は、大きく「❶リアル・現実経済市場」と「❷ネット経済市場」にわけられる。これまでわが国では、自動車産業のように、❶リアル・現実経済市場で優位を保ってきた産業が多かった。しかし、いつの間にか、あらたに❷ネット経済市場が大きく成長をとげており、しかも、新興の❷ネット経済市場でビジネスをする企業は、現実経

済市場各所に実施的な意味での事業基盤を持たなくでもよい。ネット経済には国境がないからである。

❷ネット経済市場には、ICT（情報通信技術）やデータを活用して、他の事業者と消費者とを結ぶ「場・基盤（プラットフォーム）」を提供する取引仲介型の「デジタル・プラットフォーム企業（platform companies）」（「巨大プラットフォーム企業」、「プラットフォーム巨人（GAFA tech giants）」）が出現し、国境をまたいで巨大化している[1]。その代表格が、ガーファ／GAFA【クーグル［親会社はアルファベット］・アマゾン・フェイスブック・アップル。頭文字を取って通称で「GAFA」と呼ばれる。】、中国 ICT（情報通信技術）界に君臨する BAT【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）。頭文字を取って通称で「BAT」と呼ばれる。】、それに日本の楽天やヤフーなわけである。とりわけ、4 強（Big4）と呼ばれる巨大デジタル・プラットフォーム企業 GAFA は、国境をまたぐネット経済市場で、全人類の 8 割の個人データを収集・独占する。今や国家さえ尻込みする存在だ。

海外では、巨大ネット企業による❷ネット経済市場のデータ独占（data-monopoly）を表す新語として「データ・オポリーズ（data-opplies）」という言葉が使われている。

今日、情報化（デジタル化）できる取引や事務は、❶リアル・現実経済市場から、❷ネット経済市場に大挙して移行してきている。石村代表は、そうした状況を分析し、参加者の理解を深めるためにいくつかの例をあげて現実空間取引・事務とネット空間取引・事務の分布や移行の実情について、具体的に説明した。その概要は、次のとおりである。



- **音楽❶➡❷**
  インターネットを通じたスマホなどへのデータ配信が一般的になり、CD ショップのような現実経済市場での取引は縮小の方向。
- **金融（証券・銀行）❶➡❷**
  金融機関の決済や与信は、ネット経済市場へ移行。証券もネット経済市場へ移行に加えて、AI（人工知能）のアルゴリズムを使った取引の自動化で人材難克服。
- **貨幣／通貨❶➡❷**
  デジタル通貨、仮想通貨へ移行。現実経済市場での現金取引は縮小の方向。
- **商品の展示・受注❶➡❷**
  Web／サイバー店舗などに掲載・展示、メールで受注可能。ただし、商品などの配送など物流（logistics）は、現実経済取引。そこで、AI やドローンなどを使い、人手の合理化・効率化に必死。
- **郵便局❶・❷**
  手紙はネットを使ったメールや添付メールに移行で、現実経済取引は大幅縮小に。一方、商品の展示・受注のネット取引拡大に伴い、ゆうパックは、現実経済取引として健在。AI やドローンなどを使い、合理化・効率化に必死。郵貯や保険などの取引は、デジタルディバイド（情報弱者）向けの現実経済取引は維持できる一方で、大きな流れはネット経済市場へ移行。
- **市役所❶・❷**
  リアルタイム対応を求める市民のニーズに即応するためには、市役所における住民票の交付その他申請事務などは最もデジタル化（情報化）できる分野の 1 つである。その一方で、「住民フレンドリー」の視点から、デジタルディバイド（情報弱者）向けの現実空間での事務を維持する必要性も高い。また、上下水道や市道などの維持管理、ゴミ収集、介護など、ネットにはなじまず、現実空間での事務を維持する必要性も高い分野も多い。
- **学校教育❶・❷**
  一般に、教育は最もデジタル化（情報化）できる分野の 1 つである。大学のような高等教育、とりわけ文科系ではネットを使ったいわゆる〝ネット大学〟

[1] ひとくちに、プラットフォーム・ビジネス・モデルを採用したプラットフォーム企業といっても、実に多様である。アマゾンや楽天にように、商品や書籍、各種サービスなどを売手企業と消費者との間の取引仲介型プラットフォーム企業がある。ほかに、「T ポイント」のような、コンビニやレンタルショップなど、いろいろな店で買い物をするとポイントを貯められる共通ポイントカードも、このモデルを採用した事業である。ペイペイ（PayPay）や PayPal スマホを使った民間の決済＋ポイント集約型の事業も、このモデルを採用した事業といえる。ふるさと納税や自治体ポイントなども、このモデルの事業である。

© 2019 PIJ

の形でデジタル経済市場への移行も可能。現実空間大学では、サーズ（重症急性呼吸器症候群／SARS）のような危険なパンデミック患者が出た場合に一斉休校措置をどう伝えるか思案しているのが実情である。しかし、パンデミックの場合には〝ネット大学、授業のネット配信〟に切り替えて対応するなどの発想の転換が必要。一方、大学教育でも理科系・実験系では、一般的に現実空間に所在する必要性は高い。また、学校教育でも、調和ある人格の形成をめざす義務教育のような場合には、現実空間に所在する必要性が高い。

・税務会計・監査・法務❶・❷

政府規制でつくられた専門職は多岐にわたる。例えば、(1) 税理士は、①税務書類の作成、①記帳代行、③税務代理、④税務相談などを主な業務とする。①・②は❷データ経済市場に移行する。その一方、③・④は、❶現実経済市場に存在し得るが、AI を活用し、高度に自動化・効率化される方向。(2)公認会計士は、監査が本務である。しかし、監査業務は、情報化（デジタル化）され、❷データ経済市場に移行するとともに、AI を活用し、高度に自動化・効率化される方向。(3) 弁護士は、本務である法務代理や法務相談は❶現実経済市場に残るが、相談業務などは AI を活用し、高度に自動化・効率化される方向。

加えて、石村代表は、次のように指摘した。モノからサービスにビジネスの比重が大きく移るなか、「物流のように、どうしてもデジタル化（情報化）できないサービスがある。宅配サービスが典型である。現実経済（現実空間取引）での物流には人手が要る。介護サービスなども同様である。GAFA のような巨大ネット企業は、❷ネット経済市場で手にした巨額の富をこれら人手の要る分野の効率化・合理化に投資している。つまり、❶リアル・現実経済市場への進出である。巨大ネット企業は、独自に、あるいはハードなモノつくりメーカーと共同で、AI（人工知能）、AI ロボット、ドローン、自動運転車両などハイテク製品の開発に取り組んでいる。今や、これら強大なネット企業は、ものづくり企業のデータ産業化を進める形で❶リアル・現実経済市場に参入、そこでの独占、巨人として存在することも夢ではなくなってきている。

ちなみに、2045 年には、人工知能（AI）は人間の知能（MI）を超えるシンギュラリティ（Singularity／技術的特異点）に到達するともいわれている。」と。

海外では「テックラッシュ（techlash)」という言葉が流行している。「テクノロジー（technology／技術）＋バックラッシュ（backlash／反発)」の 2 つの言葉をつなげた造語である。GAFA のような❷ネット経済市場で巨大化するデジタル・プラットフォーマーや、これら巨大ネット企業と共同で AI、AI ロボット（bots)、ドローン、自動運転車両などを開発する「IT 企業への反発」を意味する。デジタル経済市場の拡大につれて、富は、プラットフォーム（止り木）に止まれる一部の者に集中し、多くの一般市民は仕事を失い、取り残される不安は高まっている。

IT 起業家や識者からは、テックラッシュには、国家が国民に最低限の収入を保障する「ベーシックインカム（BI=basic income)」導入で応えるべきだとの声があがっている。フィンランドでは、世界で初めて 2017 年 1 月から 1 年間ほど BI を試行した。しかし、本格導入には二の足を踏んでいる。スイスでは、2016 年に BI 導入（大人で月額 25 万円程度支給）について国民投票を実施したが、否決された。OECD なども BI 導入には慎重な立場だ。だが、将来、国家は、テックラッシュには、巨大ネット企業へのデジタル課税などで得た財源を基にしたベーシックインカム（BI）導入で回答を示すことも必要になるのではないか。

◆国境のある現実経済市場に事業基盤を持たない GAFA の所在

急速な経済のデジタル化に伴い、収益拡大のために個人データ（パーソナルデータ）を利活用したい私企業が世界中にひしめいている。なかでも、❶リアル・現実経済市場に事業基盤を持たないグローバルなデジタル・フラットフォーマー（以下「巨大ネット企業」、「ネット巨人」または「デジタル・プラットフォーム企業」ともいう。)、とりわけ 4 強・GAFA ／ガーファは全人類の 8 割の膨大な個人データ量（ビッグデータ）を支配する。GAFA に続き、中国の 3 強・BAT ／バットやファーウエイなども個人データの囲い込みに必死である。

GAFA による個人データ独占が、経済摩擦を引き起こし、日本をはじめとして各国でどうコントロールするか頭を痛めている。消費者が❷ネット取引市場に大挙して移動し、❶リアル・現実経済市場に事業基盤を置いて店舗を構えて書籍、電化製品、家具、衣服などを販売する企業がジョーズのような GAFA に食いちぎられているからである。

❶リアル・現実経済市場に事業基盤を持たない GAFA の存在は、中国のような個人データ国家独占の観点からではないものの、いわゆる「グローバル企業データ独占資本主義」、「データ監視資本主

義（data surveillance capitalism）」の観点からもその存在が問われている。

石村代表は、GAFA のような巨大ネット企業／デジタル・プラットフォーム企業による個人データ独占に待ったをかけるために、世界各国は、①デジタル課税の実施、②独占禁止法／競争法などの適用、③個人情報保護法制の適用（データローカライゼーション／data localization）などを考えているという。

（1）デジタル課税の実施とは

GAFA 対策としてのデジタル課税の実施とはどういうことなのか？石村代表は、次のように説明した。「紙媒体の『郵便』を使うとすると、切手を買うことで〝消費税〟を負担する。しかし、ネットを使ったメールや添付メールでは消費税がかからない。現実空間取引とネット取引との間での公平を確保するために『デジタル課税』プランが出てくる」と。

また、「音楽を『CD』の形で、現実経済取引により国境を越えて輸入すると、関税その他の税金がかかる。ところが、国境のないネット取引で音楽の情報（デジタル）配信を受けると、課税が難しい。そこで『デジタル課税』案が出てくる」と。

さらに、「金融取引は原則として消費税は非課税であるが、例えば❶リアル・現実経済取引により送金すると手数料に消費税がかかる。ところが、ネット取引では手数料が無料である、あるいは仮に有料であっても消費課税は難しい。的確なデジタル課税には問題が山積している」と。

「国境のないネット空間での経済取引で GAFA のような巨大 IT 企業／デジタル・プラットフォーム企業が得た〝果実〟にどう課税するか、〝所得課税〟か・〝消費課税〟か、さらにはその税収をどう配分するか等々は、OECD や 20 か国・地域（G20）首脳・閣僚会議で議論している。イギリスやフランスのように、独自に課税を実施する傾向が強まっている。これらの諸国では、各ネット企業の売上高を基準に消費課税（turnover tax）を実施する方向である。一方、アメリカは、連邦レベルでの消費課税（VAT, GST）を導入していない。このことから、法人所得課税の形で、デジタル課税をすべきであると主張する。このように、各国が独自に課税するのでは、課税ベースや課税方式がまちまちになる。また、同じ課税ベースに複数の国や地域が多重に課税する問題が生じるおそれがある。いわば「デジタル課税の GDPR 版策定が求められている」と。石村代表は、「国際課税は私の専門分野であるが、本日のレクチャーのメインテーマではないので、この程度の説明に留めたい」と深入りを避けた。

（2）独占禁止法制などの適用とは

巨大ネット企業は、❷ネット経済市場をデータ独占（data-monopoly）し、揺るぎない地位をものにしている。すでにふれたように、海外では、「データ・オポリーズ（data-opolies）」という新語が流行している。「データ(data)＋モノポリー(monopoly／monopolies／独占)」の 2 つの言葉をつなげた造語である。「データ・オポリーズ」の言葉は、❶リアル・現実経済市場での独占と区別し、❷ネット経済市場での独占を表す意味で使われている。

4 強・GAFA のデータ・オポリーズ（データ独占）に、独占禁止法（独禁法）を適用する動きがある。これまで、独占禁止法（独禁法）～アメリカなどでは「反トラスト法」、ドイツなどでは「反カルテル法」、イギリスなどでは「取引慣行法」、「EU 競争法」と呼ばれる～は、❶リアル・現実経済市場で適用されてきた。すなわち、独禁法は、本来、製鉄会社、自動車製造会社のような企業が❶リアル・現実経済市場で、その優越的な地位を利用してその国の市場を独占、あるいは寡占することで価格を支配することを排除することが狙いである。言い方を換えると、独禁法は〝一国の現実空間〟がその適用対象である。データ（デジタル）や知的財産のような、〝無形の財産〟、しかも国境のない❷ネット市場経済での情報（デジタル）独占の排除をねらいとしたものではない。

モノからサービスにビジネスの比重が変わるなか、GAFA のようなデジタル・プラットフォーム企業、巨大データ企業は、国境のない❷ネット経済市場でビッグデータ【大量情報、わが国の 3 階建ての個人情報保護法制でいう「非識別加工情報」または「匿名加工情報」】を独占、データ・オポリーズの状態にある。しかし、一国家の独禁法を、国境のない❷ネット経済市場に君臨する巨人に適用することにはさまざまな問題がある。石村代表によると、これまでも学問的には、国境の存在を前提として、「独禁法の域外適用（extra-territorial application of anti-trust laws）」が議論されてきているという。しかし、国境のないネット空間でのデータ独占、データ・オポリーズへの独禁法適用の議論については、現段階では議論が熟していないと指摘した。しかも、わが国の個人情報保

© 2019 PIJ

護法制のもとでは「ビッグデータは個人情報にあらずの姿勢」を維持しており、ネット空間への独禁法を適用するとすれば、デジタル化した個人データをお金に換算できる「金銭等価物」あるいは「有価物」と見る必要も出てくるのではないか、と指摘した。加えて、わが国の公正取引委員会（公取委）の人材の数や資質、つまり語学力などの面からもネット空間への独禁法の適用は至難なのではないか、とも指摘した。

GAFA のデータ・オポリーズ（データ独占）に対する独禁法による対応としてはドイツの連邦カルテル庁（Bundeskartellamt）の例がある。石村代表は、このケースを紹介した。

連邦カルテル庁は、2017 年から米フェイスブック社の調査を開始し、同社に対して、同社のデジタル・プラットフォーム利用者のデータ収集を大幅に制限するように命じている。理由は、同社が個人データ独占により高い価格設定が可能なほど膨大な個人データを収集しており、消費者の利益を侵害しているということである。つまり、同庁は、米フェイスブック社が、傘下の写真共有アプリ「インスタグラム（Instagram）」や対話アプリ「ワッツアップ（WhatsApp）」、同社の「いいね（Gefallt mir ／ like）」ボタンを搭載する外部の提携先新聞社などのサービスの利用者の膨大な個人データを収集・統合・加工して、精度の高い利用者データベース（DB）をつくり、それを同社の広告事業に活用していることをあげた。こうした行為は、同社がその優越的な地位を利用し、ネット経済市場で公正な競争を阻害している。また、同社は、個人データの収集・追跡・統合・加工については、データ主体（本人）から、事前に明示の同意を得ておらず、一般データ保護指令（GDPR）に抵触するとも指摘している。つまり、同社のビジネス手法は、ネット経済市場においてデータ・オポリーズ（データ独占）で公正な競争を阻害するとともに、プライバシー侵害的でもあると判断したわけである。

（3）個人情報保護法の適用とは

ネット経済市場の拡大は、個人のプライバシーに多大な影響を及ぼす。市民の言動や消費行動などが逐一企業や政府に補足され、ときには衆人監視にさらされる。市民は、ネット空間では、隠れ場所を探し出すのが難しくなっている。データ保護を、現実空間のみならず、ネット空間にまで広げて強化し、GAFA のようなデータ巨人規制につなげる選択肢がある。

わが国の個人情報保護法制は 3 階建て、公民（官民）別建て、しかも国境のある現実空間での個人情報・個人データの取得・流通・保管などの取扱いを主なターゲットとしている。言い換えると、現行法制は、必ずしも国境のないサイバー空間／ネット空間での個人情報・個人データの取扱いなどをターゲットとした法律とはいえない。ある意味では、データ巨人 GAFA のようなデジタル・プラットフォーム企業には十分対応できない法律とみることもできる。時代に合わない、いわゆる「ガラパゴス化」している面は否定できない。

石村代表は、「この点、EU（ヨーロッパ連合）は個人データ（情報）保護法制を、現実に加え国境のないネット空間での個人データの取扱いもターゲットとしている」という。「これにより、リアル・現実経済市場に確たる事業基盤を置かない GAFA のようなデジタル・プラットフォーム企業にも法規制の網をかけている」という。

石村代表は説明した。「EU が採った策は、データローカライゼーションの視点に立ち、新たなデータ保護法制を整備、個人データに対するプライバシー権（個人データの自己コントール権）を徹底的に保護する政策を選択し、データ巨人 GAFA 対策の核に据えた。つまり、一般データ保護規則（GDPR=General Data Protection Regulation）を制定、2018 年 5 月 25 日に施行することでデータ巨人 GAFA 対策を具体化させた[2]。」と。「これは、EU が、国境を越えて飛び交う情報（データ）を武器にした GAFA に、プライバシーファースト、「市民よ！GDPR（情報プライバシー）を武器に GAFA に挑め」の政策を選択したことを意味する。」と。「ビッグデータを武器にした GAFA に、市民はプライバシーを武器に対峙する」戦法である。

しかし、「刀狩」の伝統を重んじるわが国政府は、この市民に情報プライバシー権という武器を供与する〝EU 式の戦法〟を採ることには消極的である。わが国政府は、②独占禁止法制などの適用強化、さらには③個人情報保護法制の強化をするとしても、EU の GDPR に倣っても、個人データの自己コントール権強化の観点からではなく、国内の現実空間に支店など恒久的施設（PE=permanent

[2] 拙論「EU: 一般データ保護規則（GDPR）とは何か」CNN ニューズ 93 号 8 頁以下参照。Available at: http://www.pij-web.net/data/CNN-94.pdf

establishment）を置いてないグローバルなデジタル・プラットフォーム企業には、国内に代理人を置くように求めること、あるいは十分性の認定制度を設けること、さらには、電気通信事業法上の通信の秘密を梃に法規制の具体策を練っている。つまり、EU のような市民に徹底した情報プライバシー権を法認することでデータ巨人を封じ込めるという政策ではなく、中央の役所が中核となり政府規制強化で、グローバルなデジタル・プラットフォーム企業と対峙しようというわけである。

◆ EU の GDPR で法認した情報プライバシー権とは

EU は、一般データ保護規則（GDPR）を制定し、2018 年 5 月 25 日に施行した。これに伴い、それまであったデータ保護指令（DPD ＝ Data Protection Directive）は、廃止された。DPD と GDPR とには大きな違いがある。DPD（指令）は、一種のモデル法のような存在である。したがって、EU 加盟国は、DPD をモデルにそれぞれ国内法でデータ保護について定めることになる。これに対して、GDPR（規則）は、各加盟国の直接適用になることである。

GDPR は、現実空間に加えネット空間（サイバー空間）にも規制が及ぶ仕組みになっている。また、GDPR は、公民双方の分野に適用あるオムニバス方式のデータ保護法である。

（1）指令（DPD）から規則（GDPR）への移行と主な変更点

2018 年 5 月 25 日に、EU は、1995 年 10 月に施行されたデータ保護指令（DPD）を廃止し、新たなデータ保護規則（GDPR）に移行した。この移行に伴う主な変更点は、次のとおりである。

●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（DPD）
【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の間の権限の分配と調整など）

（2）GDPR で法認された情報プライバシー権とは

EU の GDPR は、あらたな情報プライバシー権（個人データの自己コントロール権）を幅広く法認した。主なものを掲げると、次のとおりである。

● EU の GDPR で法認した主な情報プライバシー権（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**

© 2019 PIJ

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)。

（3）「忘れられる権利」とは

新たに GDPR で法認され、わが国でも注目されている権利の 1 つに、「忘れられる権利（right to be forgotten)」(「忘れてもらう権利」ともいう。) がある。いわゆる〝削除権〟である。

1995 年に施行された EU のデータ保護指令（DPD) では、「忘れられる権利」を積極的に法認していなかった。2010 年に、EU 加盟国であるスペイン人 G 氏が、グーグルサーチ（Google Search) で自分の名前を検索してみると、1998 年に地元紙に載った自分の過去の「社会保険料滞納で財産が差し押さえられた」とする記事へのリンクが表示された。G 氏は、プライバシーの侵害と感じ、グーグル・スペイン社（Google Spain) や米グーグル社（Google Inc.) を相手に、検索結果として表示される個人情報はプライバシー権の侵害にあたるとして、争訟に及んだものである。G 氏は、スペインの第三者機関であるスペインデータ保護庁（AEPD=Spanish Data Protection Agency) に対して、グーグル・スペイン社や米グーグル社、記事を掲載した新聞社に記事の削除ないし閉鎖措置を命じるように、不服申立てを行った。AEPD は、この申立てを容認し、グーグル・スペイン社や米グーグル社にリンクの削除を命じた。グーグル・スペイン社や米グーグル社は、この AEPD の裁決を不服として、スペイン高等裁判所に提訴した。

この提訴を受けて、同高裁はルクセンブルクにある EU 司法裁判所（ECJ) に先行判決を仰いだ。ECJ は、2014 年 5 月 13 日に、EU 基本権憲章 8 条やデータ保護指令 (DPD) の解釈により「自分の過去の削除」(データ主体による削除請求権、いわゆる「忘れられる権利」を認めた（Judgment in Case C-131／12, 詳しくは、CNN ニューズ 78 号参照)。その後、EU は、一般データ保護規則 (GDPR) の制定にあたり、「忘れられる権利」を制定法上の権利として法認するにいたった（GDPR17 条)。

わが国でも、インターネット検索サイト「グーグル」の検索で表示される自分の逮捕歴の削除を求めて裁判所に仮処分の申立てが行われた。原審のさいたま地裁は、2015 年 12 月に、原告に「忘れてもらう権利」があるとし、検索結果の削除を命じた。しかし、高裁および最高裁判所は、検索結果の削除を認めない決定を下した（CNN ニューズ 88 号参照)。

●わが国で犯歴削除を求めた訴訟（仮処分申立て）の推移と判断内容の概要

①さいたま地裁決定（2015 年 12 月)	(a) **判断**（児童買春の犯歴を表示する）検索結果の削除を命じる。 (b) **理由** 更生が妨げられ、X の利益が侵害されている。 (c) **忘れられる権利** 過去の犯罪を社会から忘れてもらう権利がある。
②東京高裁決定（2016 年 7 月)	(a)**判断** 検索結果の削除を認めない。 (b) **理由** 削除は表現の自由や知る権利を侵害する。 (c) **忘れられる権利** 判断しない。
③最高裁決定（2017 年 1 月)	(a)**判断** 検索結果の削除を認めない。 (b) **理由** 本件はプライバシーが表現の自由に優先するケースにはあたらない。 (c) **忘れられる権利** 検討しない。

以上のように、石村代表は、EU と日本のプライバシー保護の現状を比較した上で、次のように指摘した。「わが国でも、現実空間に加え、ネット空間での、情報上のプライバシー保護の課題は山積している。いわゆる〝リベンジわいせつ画像〟のネット掲載などでは、インターネット検索サイトの運営企業は、データ主体からの削除権請求には臨機に応じているようである。しかし、わが国では、削除要請は、データ主体からの請求権として法認されえているわけではない。裁判所も、判例でこうした請求権を認めることには概して消極的である。EU の GDPR などを参考に、わが国でもネット空間における情報プライバシー権を広く法認することは待ったなしである。」と。

石村代表は、仮にデータ主体に対して削除権を法認したとしても、表現の自由や報道の自由など他の保護法益とのバランスを考える必要があり、最終的には、司法判断に委ねられるケースも多いのではないか、と付け加えた。

（4）GDPR 違反には厳しい制裁

企業などによる EU 市民の情報プライバシーの侵害に対して、GDPR は、厳しい制裁をかしている。この点は、学習会の開催にあたりあいさつをした立憲民主党の有田芳生参院議員も指摘した。GDPR 違反に対する制裁は、次のとおりである。

・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（1€=125 円換算で、１２億 5,000 万円）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（25 億円）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。

◆問われるわが国の個人データ保護法制

わが国の個人情報保護法制は、3 階建て【❶個人情報保護法（民間分野）＋❷行政機関個人情報保護法（国の公的分野）＋❸独立行政法人等個人情報保法（公的分野)】になっている。また、規制機関である個人情報保護委員会（PPC）は、原則として 1 階❶、民間分野しか介入できない仕組みになっている。わが国の個人情報（データ）保護法制は、ビジネスの軸足がモノからデータ（デジタル）に大きく移行する時代の流れに十分ついていけていない。

（1）問われた住民税通知書への個人番号記載強要と PPC の対応

2017 年に、総務省が、2017 年に、特別徴収義務者である事業者（企業）に送付する住民税の特別徴収税額決定通知書に扶養家族全員のマイナンバー（個人番号）を記載して送付するように求めた。この住民税額通知書に、納税者本人や扶養家族全員のマイナンバー記載をめぐっては、税界でも大きな問題になった（CNN ニューズ 92 号参照)。しかし、総務省自治税務局をはじめとした当局側は、自治体に指令を出して、各自治体に通知書に記載をして通知するように求めた。しかし、かなりの自治体は、かつての赤紙配りのような大本営の命令に抵抗した。この騒動は、経済界からの苦言、昨年 2018 年度税制改正大綱で「不記載」とすることで政治決着がついた。この問題では、市民運動体も、国会議員の支援を得て、昨年（2018 年）8 月 29 日に、国会の参議院議員会館に個人情報保護委員会（PPC）の職員や総務省のマイナンバー担当者などを呼んでヒアリングを行った（詳しくは CNN ニューズ 95 号参照)。ここでは、市民運動体側から委員会（PPC）職員などに対しさまざまな質問・批判が出された。これらのうち、もっとも重大なのは、「委員会（PPC）は、自治体による事業者への住民税額通知書に、納税者本人や扶養家族全員のマイナンバー記載を強要している総務省に対して、あるいは、日本年金機構の外国企業への違法な再委託などの問題で、特定個人情報保護の観点から、なぜ苦言を呈しなかったのか」という問いかけであった。委員会(PPC)職員からの回答は、「委員会（PPC）には、国の行政機関や自治体などを指導できない法的仕組みになっているから」とのことであった。つまり、委員会（PPC）が所管できるのは個人情報保護法上の「個人情報取扱事業者」に限られており（法 2 条 5 項)、国の行政機関や自治体は〝個人情報取扱事業者〟にあたらないから、関与できないというわけである。これでは、まさに PPC は〝名ばかり第三者機関〟そのものといえる。しかし、そうした法律のつくりになっているわけで、委員会（PPC）職員にクレイムを言っても仕方がない面もある。

石村代表は、EU の GDPR を参考に、わが国の個人情報保護法制の作り、デザインを変えないといけないと指摘した。具体的には、3 階建てを 1 階建てに立て直す(オムニバス方式のデザインし直す)か、個人情報保護委員会（PPC）が、1 階から 3 階まですべてに関与できるように制度改正が必要であると指摘した。

（2）PPC、「十分性認定」では素早い対応

GDPR は、EU 域外への（越境）個人データの移転について、❶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❷EU 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 側と精力的に協議のうえ、❷EU から国として「十分性の認定」の

© 2019 PIJ

お墨付を得て、このお墨付きの枠組みは 2019 年 1 月 23 日に発効した。

石村代表は、「個人市民の情報プライバシー保護の面では牛歩、その一方で法人企業のためには積極的に動く個人情報保護委員会（PPC）の姿が浮き彫りになっている。」、と批判した。

個人情報保護委員会（PPC）は、2018 年 10 月 22 日に、フェイスブック社に対して、行政指導を行っている。理由は、同社が、対話アプリや「いいね」ボタンを搭載する外部サービスから、利用者（本人）の明確な同意を得ずに大量のデータを収集していたことや、収集した大量の個人データをデータ分析会社へ横流ししていたこと、さらには同社のデータセキュリテイの不備が原因で受けたハッキング被害への対応が悪いことなどである。石村代表は、「行政指導のようなお役所的な対応も大事かも知れないが、PPC（委員会）は、苦情処理（お客様対応）の仕組みを整備し、お客様である市民にもっと寄り添う組織に改革しないと、真の第三者機関とはいえないのではないか」と注文をつけた。個人情報保護委員会のような第三者機関の存在意義は、個人データ侵害があった場合に、テマ・ヒマのかかる裁判所ではなく、市民が駆け込み救済を求められる仕組みをつくることがねらいである。「デジタル秩序への市民参加」の視点が求められている。

（3）どう改革する、名ばかり個人情報保護委員会

個人情報保護委員会（PPC）のホームページ（HP）では、「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。」と PR している。しかし、石村代表は、市民は、「PPC って企業寄り、〝有用性〟の忖度機関なのかなぁ～と思っているのではないか」、と疑問を投げかけた。また、「個人情報保護法制が、総務省のような行政機関が法案の原案をつくって、議員はロビイストのような存在になる『政府立法』、『閣法』に問題があるのではないか」、と注文をつけた。「お役人は、自分等のやることに委員会（PPC）が茶々を入れること（介入すること）ができる仕組みをつくることに積極的になるわけはない」と。「名ばかり個人情報委員会（PPC）の姿勢をただすには、法改正が必要であるが、この場合、お役人に立法を任せるのはなく、議員立法で法案をつくることが大事」と訴えた。

参加者のなかから「**PIJ** が対案を準備しては、どうか」との提案があった。これに対して、石村代表は「**PIJ** のようなタダ働き市民団体が法案を準備し、立法府で高給を享受し、政策秘書や議院法制局という法案つくりのお手伝いさんをわんさと抱えている議員が法案もつくらないのでは・・・本末転倒ではないか」と失笑しながら答えた。

◆形式的な「データ流通の自由」は悪平等を招く

折しも、わが政府は、ネット巨人の封じ込めに必死である。すでにふれたように、GAFA は、全人類の個人情報の 8 割を握るといわれる。わが国の楽天やソフトバンクなどデジタル・プラットフォーム企業（日本勢）が束になってかかっても、競争にならない。これまでも、議員立法で、官民データ促進基本法（2016 年）のような、IT 関連法がつくられている。ところが、こうした法律は、「日本の IT 企業は勝ち組」という戦中の大本営、あるいは「Japan as No.1」のような現実を直視できないような考えに基づいてつくられている。石村代表は、「IT 利権ファースト、市民のプライバシー・ラスト」のような内容であるという。2018 年 9 月の政府の IT 総合戦略なども、「データの自由な流通による産業の活性化を目指す」とする。確かに、聞こえは悪くない。しかし、石村代表は、こうした法律や政策は、まさに「悪平等」として機能する、と指摘する。実質的に、わが市民の個人情報を GAFA ／ガーファの餌食にする〝呼び水〟的な役割を果たすという。グローバルにみると、データ覇権争いなどの思考に欠ける、稚拙な議員立法あるいは政策提言だという（レジメ 23 頁以下参照）。安倍首相も、2019 年 1 月 23 日のダボス会議で、「データ越境自由に」と叫んでいたが、これにも大きな疑問符がつくのではないか。

◆ EU の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

EU（欧州連合）は、2018 年 5 月 25 日に、一般データ保護規則（GDPR=General Data Protection Regulation）を発効させた。GDPR はデータローカライゼーションの考え方が基盤になっているといわれる。参加者から「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？」と質問があった。石村代表によると、データ保護規則（GDPR）の基本的な考え方は、一言でいうと、「EU 市民に対して、〝プライバシーファースト〟だ！ GDPR で与えられた個人データの自己コントロール権を〝武

器〟に、GAFA と果敢に闘え！」というものだという。EU でも、ネット界の巨人、GAFA の勢いは止まらない。このままでは、EU 市民の個人データは GAFA に食いちぎられてしまう。市民にさまざまのプライバシー権を保障するから、それらを武器に GAFA に果敢に挑め」、というものだという。こうした EU の GDPR 制定・施行による強力な GAFA 規制は、「データローカライゼーション（data-localization）」という考え方に基づいているわけだ。

「データローカライゼーション」は、「データナショナリズム（data-nationalism）」とどう違うのか、という問いかけもあった。石村代表は、「双方を区別するには難しいと前置きしたうえで、誤解を恐れずにいえば、データローカライゼーションとは、国境のないデータ経済市場で流通する個人データについて、データ主体（個人）が居住する国や地域がその個人の情報プライバシー権を保護する仕組みを指す。裏返すと、国家が個人データ管理の主役となる、中国のような例は、限りなくデータナショナリズムといえるのではないか」と答えた。

まさに、EU の「ビッグデータを武器にした GAFA に、加盟国市民はプライバシーを武器に対峙する」戦略は、データローカライゼーションの発想に基づくものといえる。

◆政府の巨大 IT 規制検討会とは～巨大 IT 規制に向けた政府規制の動き

参加者から、政府の「巨大 IT 規制委員会」とはどのようなことをやっている組織なのかとの質問があった。

石村代表は参加者に配付した資料を参考に次のように説明した。2018 年 7 月に、わが国政府 3 機関（経産省・総務省・公正取引委員会）が設置した「デジタル・プラットフォーマーを巡る取引環境整備に関する検討会」組織である。検討会は、9 回の会合を経て、2018 年 12 月 12 日に、「中間論点整理」（中間報告）を公表した[3]。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、中国の BAT やファーウエイ、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である。あらゆる法令を総動員して❷ネット（デジタル）経済市場における公正で実質的な自由競争の実現が狙いである。公取委は、ドイツに倣い、GAFA など巨大 IT（ネット企業）の「優越的地位濫用」を認定し、独禁法規制につなげる意向だ。また、総務省は、EU の GDPR に倣って、外国 IT（ネット）企業に国内代理人設置の義務化や十分性の認定制度などを提案している。しかし、石村代表は、「肝心の市民のプライバシー権の強化などには無関心を装っており、市民参加など頭のなかにない、お役人の作文そのものだ。」と批判した。3 機関のお役人に、石村代表は、こうしたわが国の GAFA 対策の姿勢を、次のように批判した。「お役人は、個人市民に個人データの自己コントロール権など法認したら、役人天国、IT 利権に歯向かってくる。〝プライバシーファースト〟、冗談じゃないよ！といった認識なのではないか？」。お役人は、「わが国は〝刀狩〟をする国柄だ、市民に情報プライバシー権という武器を与えるなど、西洋かぶれだ！と人権派を叱り飛ばすのではないか？」と。一方で、か弱き大勢の小市民は「すべて役所にお任せの方が楽ちんでいいなぁ～」、「EU 市民は GDPR を武器に GAFA と闘うのか！大変だぁ～！といった認識かも知れない」と語った。

◆ GAFA 対策に政府が懸命な今が個人情報保護法改正の好機

わが国のネット企業界、デジタル・プラットフォーム企業は、概して内向き志向のようにみえる。自動車や精密機械のように❶リアル・現実経済市場でグローバルに勝負している業界や企業とは対照的である。石村代表は指摘した。「国境のない❷ネット経済市場の競争は弱肉強食、熾烈で、

[3] 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に関する中間論点整理（2018 年 12 月 12 日）（以下「中間報告」という。）などを参照。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 や BAT、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である。

© 2019 PIJ

日本勢は、GAFA のようなネット巨人とでは勝負にならないからであろう。」、で「お役人さま、政府規制で、GAFA を成敗して！！」と白旗をあげているようにもみえる」と。ネット企業に散々個人データを喰い散らかされてきた市民からみると、「市場競争ファースト、規制撤廃とか叫んでいて、勝てないとなると、お役人頼み、政府規制を叫ぶ、情けない連中！といった感じを受けるのではないか」と。

自民党なども、民族資本のネット企業を護るために GAFA 規制に動き出している。ただ、米中は IT 覇権で熾烈な争いをしている。ネット巨人の 4 強・GAFA はいずれも、アメリカ系の企業である。わが国は、アメリカと協調する形で BAT やファーウエイのような中国 IT・ネット企業、中国流データナショナリズムの封じ込め政策において重要な役割を担っている。こうしたなか、2018 年 12 月、アマゾンジャパンは、急ぎ経団連に加盟した。

石村代表は指摘する。「わが国政府が、GAFA のようなネット巨人にどの程度チャレンジできるかは、未知数である。なぜならば、個人情報保護委員会（PPC）が米フェイスブック社に行ったような、わが国で汎用される行政指導（administrative guidance）という日本特有の規制手法は、法の支配（rule of law）原則を重視するアメリカなど欧米の企業には不評であり、国際的には通用しないからである。かといって、国境をまたぐ❷ネット経済市場で強大なデータ・オポリーズ（データ独占）力を持ったネット巨人に、1 国家が、ペナルティ（刑事制裁や民事・行政制裁）をちらつかせながら、法治徹底の方針をかざして対峙するのは、相当チャレンジングでもある」と。

市場における「形式的な自由競争」を放置すると、「実質的な自由競争」がなくなる。1 国家が、「実質的な自由競争」を旗印に、国内にしか適用にならない各種法令でもってネット企業に対峙するのは一見いさぎよい。しかし、闘う相手は、世界中の大量の個人データを餌食に国境をまたぐ広大な❷ネット経済市場で太るネット巨人である。国内のネット産業利益をおもんばかって、実質的な自由競争確保が大事だと叫んでも、国家を超える力を持つネット巨人とでは勝負になるまい。結局、市民の利益もプライバシーも護れないのではないか。わが国は、個人データの自己コントロール権を徹底的に法認し市民ファーストのネット秩序を目指す EU の戦法、GDPR にもっと学んではどうか。

石村代表は次のように結んだ。「市民運動体にとっては、個人情報保護法制改正は、政府が GAFA 対策で躍起になっている今が好機である」。「EU の GDPR のような市民に対して強力な個人データの自己コントロール権を保障する改正法を、議員立法で仕上げるべきである」。また、「3 階建ての個人情報保護法制の整備、個人情報保護委員会の行政が扱う個人データへの規制権限の拡大などを求めるべきである」。お役人は、「個人市民に個人情報の自己コントロール権の拡大などもってのほか」と反発するかも知れない。「対案としてでもよいから、現実空間のみならず、サイバー空間・ネット空間でもあまねく情報プライバシーを保障するような改正法案を準備する必要がある」と。まさに、「議員立法の出番である」。もちろん、議員立法など関わったこともなく、実質的に立法権を握っている行政へのロビイストと化している多くの国会議員を動かすのでは容易ではないのも事実だ。しかし、弁護士でもある福島瑞穂議員のような人たちと手を携えて運動を展開する必要があると結んだ。

（文責　CNNニューズ編集局）

年末年始カンパへのお礼

PIJ は、無党派の非営利組織として、市民の目線でプライバシーを守るための政策提言を中心とした活動を続けてきております。2018 年～ 2019 年の年末年始カンパのお願いに対しましては、会員の皆さまはもちろんのこと、会員外の皆さまからも多大なご支援・ご協力をいただきました。ご支援・ご協力をいただいた方々のお名前を掲げるのは、プライバシー保護の観点から差し控えさせていただきますが、本当にありがとうございました。CNNニューズの紙面を借りて、心からお礼申し上げます。

運営資金事情の厳しい折、皆さま方から寄せられた浄財は、PIJ の政策提言活動に有効に活用させていただきます。

2019 年 3 月 31 日　PIJ 代表　石村耕治／ PIJ 事務局長　我妻憲利

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

【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？ ―

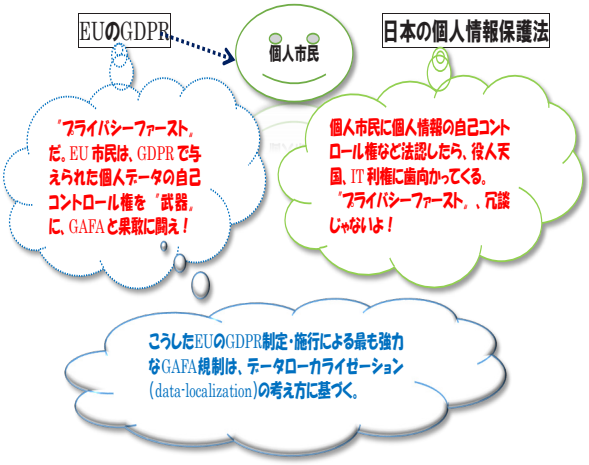
レジメ・資料

作成 石村耕治（PIJ代表）

【レジメ・資料骨子】

■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。

・「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 日に施行することで 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、

© 2019 PIJ

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に関する検討会」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、EU 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。しかし、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。

◎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、それが適法であるためには､「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

© 2019 PIJ

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、実務的に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② EU 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、② EU 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）による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。

© 2019 PIJ

・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ず監督機関（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。

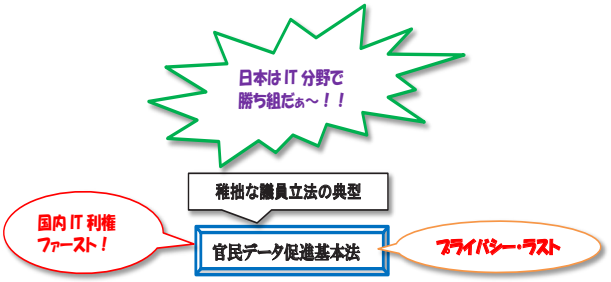
◎制裁

・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。

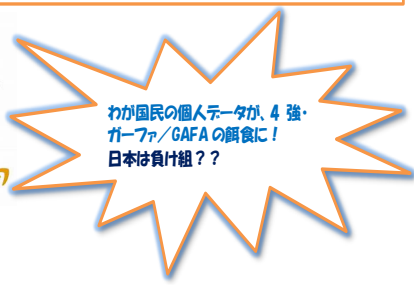
2　問われるわが国のプラットフォーマー（巨大 IT 企業）対応

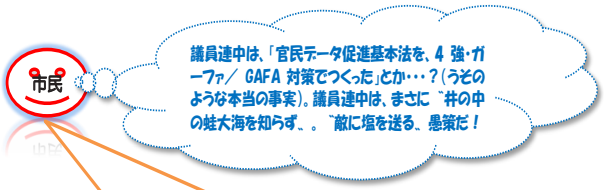
【図表 2】稚拙な官民データ促進基本法（2016 年 12 月 7 日に議員立法で成立）



・「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。

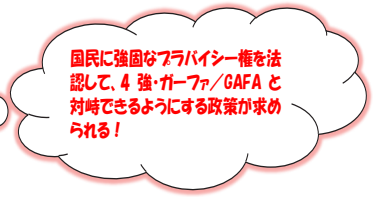
(public use)





・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)



・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）

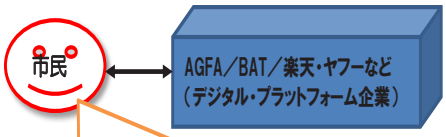
・個人（データ主体）は、いつでも個人データの取得の際にした**同意（consent）の撤回**ができる（GDPR7 条以下）。
・個人（データ主体）は、自己データにアクセスする権利（自己データの開示を求める権利）に加え、データ主体に対し**忘れられる権利**（right to be forgotten）、いわゆる「削除権」を法認した（GDPR17 条）。
・プロファイリング等の「自動処理のみに基づく自動意思決定（automated individual decision）」を規制するために、**自動処理のみに基づく決定（automated decision making）には服さなくともよい権利**（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（GDPR ２０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



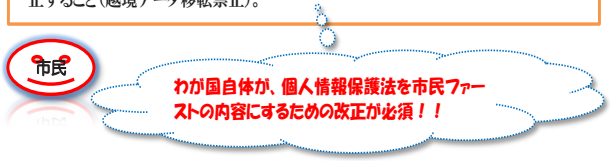
●実例 **ダイレクトマーケティンを拒否する権利**

・ネット上でホテルの空室を検索する、あるいは商品を購入すれば、すぐさま付近のホテルや同じような商品のPRがPCなどのスクリーンに頻繁に表示され、メールが送りつけられてくる。これが、クッキー技術を使った「ターゲティング広告」である。
・ターゲティング広告は、4強・ガーファ／GAFAの重要な収入源である。多くのサービスは無料を装うっている。
・しかし、消費者は、実際には「個人データの提供」という対価を負担している。つまり、消費者は、自分の知らないうちに自分の個人データを利用されている。しかも、どれだけ利用されているかもわからない。
・EUのGDPRは、こうした個人データ利用に関する〝不明瞭会計〟に対しデータ主体が〝ソー〟といえる法的ルールを定めた理由。

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？

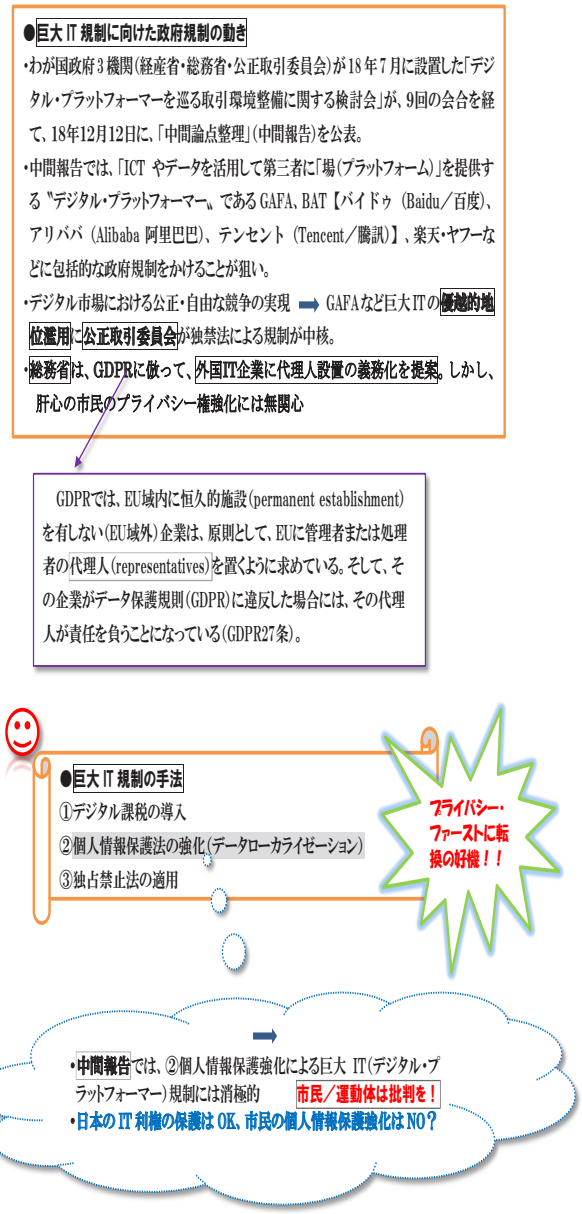
◆わが国でのデータローカライゼーションの具体策

・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)。



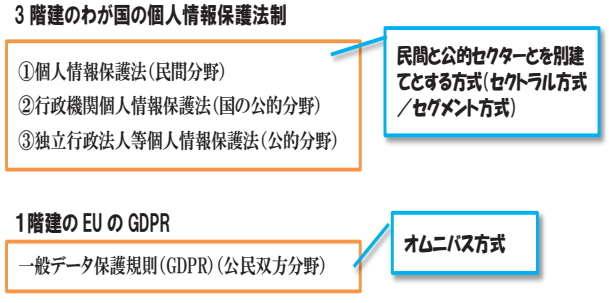
© 2019 PIJ

◆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）



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



・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む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）を根拠に活動する、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。

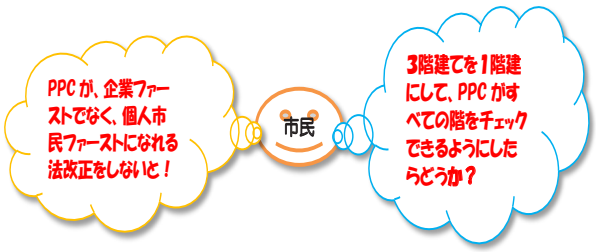
わが国の個人情報保護法制の特徴

- 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）が担当てきる。

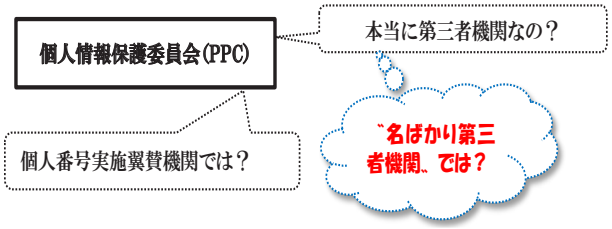
◆市民目線で、個人情報保護法をどう改正すべきか？



- 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。)

◆わが国でのデータローカライゼーションの具体策

【図表 6】市民からみた「個人情報保護委員会(PPC)」って何？



© 2019 PIJ

【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～？？

【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ることもできる（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。

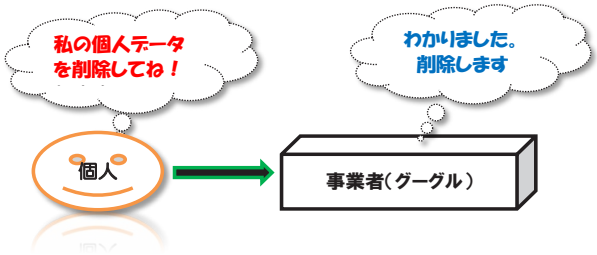
議員立法も一案！

【図表 9】PPC の規制権限行使の対象は

・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。

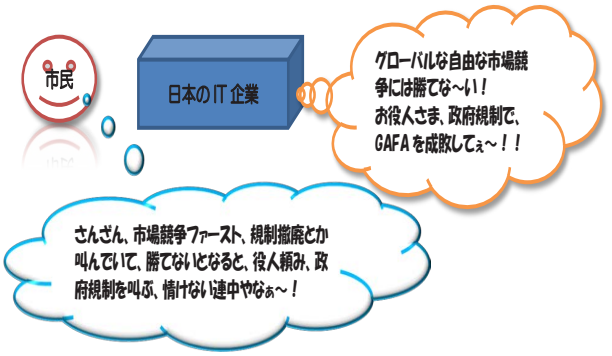
日本法 不要となった個人データ削除の努力義務？
EU の GDPR 削除を求める権利／忘れられる権利

【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！



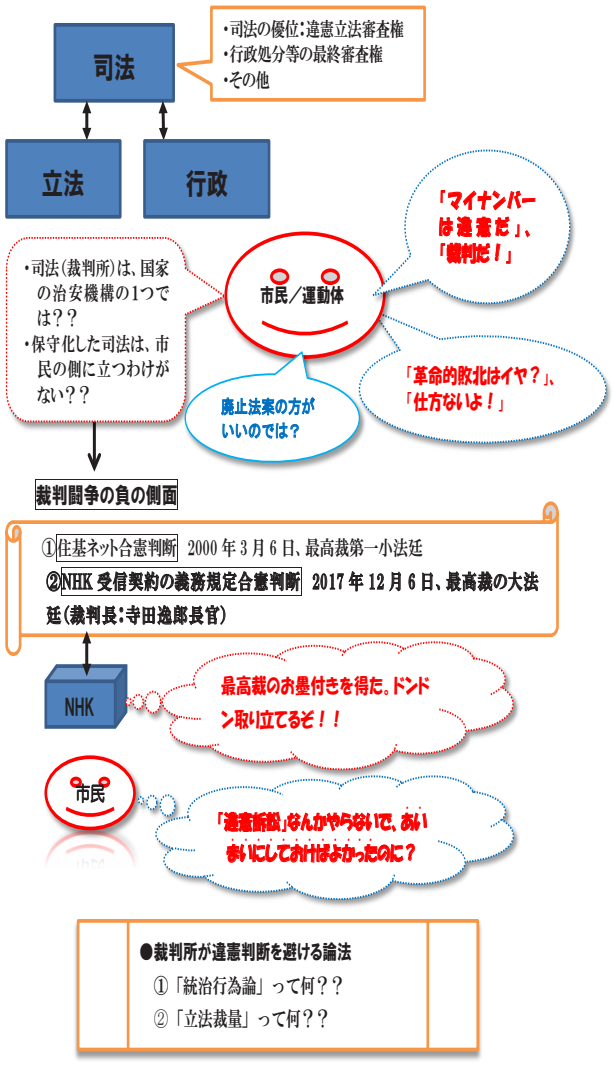
■むすびにかえて

～「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

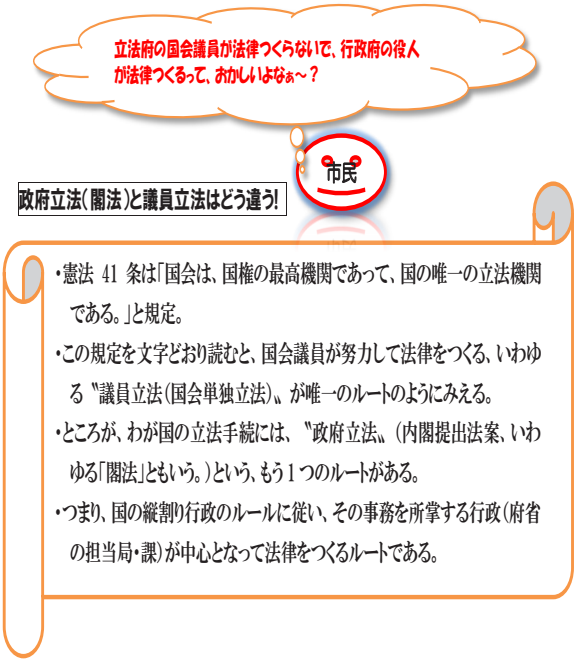


【資料】
市民にとり、司法とは何か、議員立法／政府立法とは何か

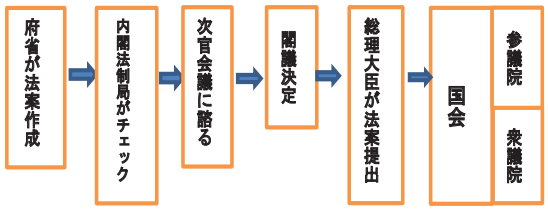
■三権分立とは国家権力を３つに分けること、つまり司法は国家権力



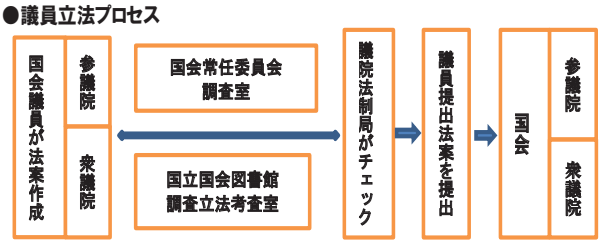
■　議員立法と政府立法の違いを知ろう



●政府立法(閣法)プロセス



●議員立法プロセス



●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

19.01.15 学習会「マイナンバー ここが問題」【於：東京・千駄ヶ谷区民会館】

市民・納税者の人権を蝕むマイナンバーにどう挑む

報告者　石村耕治（PIJ 代表）

共通番号いらないネット（共通番号・カードの廃止をめざす連絡会）は、2019 年 1 月 15 日、都内で、「マイナンバーここが問題」学習会を開催した。今回は、石村耕治 PIJ 代表（白鷗大学名誉教授）が「市民・納税者の人権を蝕むマイナンバーにどう挑む」と題して報告を行った。当日の石村代表の報告内容は、次へのリンクで視聴することができる。https://www.youtube.com/watch?v=hC7Oz129ffI 当日は、PIJ からは、白石孝（PIJ 常任運営委員）、菊池純(PIJ 常任運営委員)、中村克己(CNN ニューズ編集局長）が参加した。

≪報告内容抜粋≫

●エスカレートする「マイナンバー＋カード」法定外利用

石村代表は、まず、わが国の番号制のモデル（方式）についてふれる。現在、比較的安心・安全な個別番号制／セパレートモデル（方式）から、危ない共通番号制／フラットモデル（方式）へ移行中だと指摘する。わが国の共通番号制は❶個人番号（12 ケタ）と❷法人番号（13 ケタ）からなる。石村代表は、巨大 IT 企業が、個人のビッグデータ（大量データ／匿名加工情報／非識別加工情報）に加え、法人のビッグデータを利用して ML(機械学習)や AI(人工知能）開発、利益につなげようとする動きが強まるなか、❷法人番号がデータの検索キー、ひも付けのツールとして使われる可能性が高まっていると指摘する。このことから、法人番号をつけてデータを野放図に公開する実務について、その危うさを指摘した。また、同族会社のように、個人と法人とがミックスされた形で事業活用をしている場合もあることから、無限定に法人番号を公開する国税庁の番号実務に異論を呈している。運動体は、こうした問題にも関心を払い、企業とのマイナンバー廃止運動で連携を強めてはどうかとの認識を示した。

© 2019 PIJ

次いで、石村代表は、現在マイナンバー（個人番号）の利用が、「社会保障／税／災害対策分野＋これらの分野限定の民間利用」に絞られているはずなのに、カジノやオリンピック入場管理とか、イベント利用、法定外利用がエスカレートしてきていることを批判した。また、政府は、利子所得やFX収益など多くの金融所得は、他の勤労所得と総合課税になっていないのに、各種金融口座の番号管理をエスカレートさせてきている。一般庶民のふところに公権力が手を突っ込んでくることには強いアレルギーがある。石村代表は、運動体は、こうした庶民にもっと寄り添う、さらには富裕層ともタイアップした番号管理に抗する姿勢が求められる、と指摘した。加えて、事業者（企業）には、従業者・役員やその家族、取引先のマイナンバー付個人情報（特定個人情報）について厳しい管理義務を課されている。こうした管理義務は、とりわけ中小企業にとっては重荷、過大なタダ働きの強要につながっている。石村代表は、憲法18条〔苦役からの自由〕に反するのではないかと批判した。企業は、庶民に働く場を提供し、しっかりと給料を払うことが本務であるはずだ。このままでは、中小企業者は、政府から押し付けられたタダ働きに忙殺され、生業どころではなくなってしまう。政府「規制の撤廃」の精神はどこへ行ってしまったのか、と批判した。石村代表は、運動体は、政府から押し付けられたマイナンバー管理に苦渋する中小企業者にもっと寄り添う姿勢が必要であるとの認識を示した。

●民業圧迫、素人官業の「自治体ポイント」は必ず血税のムダ遣いに終わる

石村代表は、今年（2019年）10月からの消費税率引上げに伴う景気対策として政府・与党が検討している「自治体ポイント」について批判的に検証した。この制度は、総務省の掛け声のもと、マイナンバーカードのポイントを貯める機能を使って、総務省の「この指と〜まれ」に応じた自治体が実施する共通ポイントプラン。住民が、地域の商店やリゾート施設など、さまざまなところで買い物をする、あるいは有償のサービスを受けるとポイントを貯められるのが共通ポイントカードの仕組み。溜まったポイントは他の自治体でも使えるという。まさに、いまだ12.2%に留まるマイナンバーカードの交付率を引き上げたいとの狙いが透けて見えてくるようなプランだ。石村代表は、「切れ目のない景気対策ではなく、カードを持たせるための切れ目のない悪だくみ」と一喝。紛失して漏れたら危ない12ケタの自分のマイナンバーや生年月日・住所などの基本情報が記載されたICカードなど、まともな市民なら持ち歩きたくないのは当り前である。

共通ポイントカードは民間にひしめいている。わが国最大手の一つである「Tカード」は、年間のTカード利用者が人口の半分を超える6,676万人にも達し、提携店も 83万を超える。加えて、〝体力勝負〟といわれるほどスマホを使った民間のポイント集約の仕組みも続々と誕生している。石村代表は、「ポイント集約という民間がやるべきことを官がやってはいけない」と批判した。あわせて、①自治体ポイントに参加する仕組みは複雑、②しかも、実際に店舗などでポイントを使おうとすると、ICカードリーダーを設置しており、そこでICカードをカードリーダーに差し込んだり、かざしたりしなければならなく、12ケタの個人番号が丸見えになるおそれもある。③高齢者などには管理が至難で使い勝手が悪いうえ、家族や友人間でカードを使い回しも想定されることから、紛失・悪用される危険が高い。④カードの常時携行の強制、「マイナンバーカードを持たない人は、非国民」のような監視国家の流れを加速する等々、問題点をあげた。民業圧迫、素人官業の「自治体ポイント」プランは必ず血税のムダ遣いに終わる、と予言する。

●ガラ系化するマイナポータル

わが国の電子政府プラン「マイナポータル」（正式名称「情報提供ネットワークシステムは、2017年11月から情報連携（データ照合）を開始した。〝利便性の高い〟電子行政サービスが受けられるというのが政府のうたい文句。だが、運用はほぼ機能不全常態。その最大の理由の1つが〝利便性の悪さ〟。利便性の良さで勝負のはずのマイナポータルが利便性の悪さで〝歩行困難〟って何？？　石村代表によると、最大の要因は、自宅のパソコン（PC）などからマイナンバーICカードを使わないと利用できない仕組みであることにあるという。つまり、データセキュリティに、ICカードに格納された電子証明書（公開鍵）を使うことにあるとのことである。もう少しわかりやすくいえば、自宅のパソコン（PC）から国税庁のポータルサイトにリモートアクセス、ログインするには、ICカードリーダーが必要であることが、大きなマイナス要因になっているということだ。

時代は、パソコン（PC）からスマートフォン（スマホ）やアイパッド（i-Pad）のようなモバイル端末へ大きくシフトしてきている。モバイル端末に、ICカードリーダーはまったく不具合である。つまり、マイナンバーカードを使う電子申告（e-Tax）をはじめとしたわが国の電子政府プランは、高速増殖炉もんじゅ並みの「負の資産」となりつつあるという

【動画】学習会「マイナンバー、ここが問題」
https://www.youtube.com/watch?v=hC7Oz129ffI

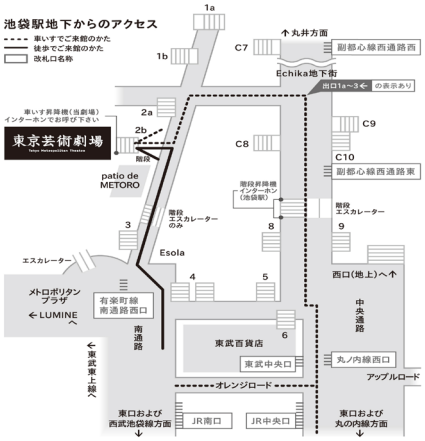
ことだ。石村代表は、政府は、住基カードを使った電子政府構想である「住基ネット」が、頓挫し、住基カードも廃止の憂き目にあっていることで、わかっているはずだ、と批判する。IT 産業からの広告収入で潤う経済紙などは、IC カードを使った電子政府モデルは、エストニアではうまくいっているなどと、破たん寸前の構想を持ち上げる。しかし、エストニアは人口 131 万人程度の都市国家、さいたま市（130 万程度）と同じ程度の小国だ。わが国の人口は、1 億 2,600 万を超える。石村代表は、人口 1 億を超えるわが国と人口 130 万程度の小国と比べること自体がナンセンスではないか、と指摘する。さいたま市だけで、住民全員にマイナンバーカードを持たせ自治体政府ポータルサイトを立ち上げてうまく運んでいくはずだとするのと同じではないか。

プライバシー・インターナショナル・ジャパン（PIJ）の定時総会を開催します

- **【日時】**：2019 年 5 月 25 日（土） 午後 6 時開催（受付は 5 時 30 分から）
- **【場所】**：東京芸術劇場（℡：03-5391-2111）
  JR・東京メトロ・東武東上線・西武池袋線　池袋駅西口より徒歩 2 分
- **【議題】**：事業報告、役員選任報告、新年度事業方針および事業計画
- **【記念講演】**：

ストップ！
不健康なマイナンバーカードの健康保険証化、強制交付案！

≪講師≫
石村耕治（PIJ 代表）



編集及び発行人

プライバシー・インターナショナル・ジャパン（PIJ）
東京都豊島区西池袋3－25－15 IB ビル10F　〒 171-0021
Tel/Fax：03-3985-4590　**E メール**：wagatsuma@pij-web.net
編集・発行人　中村克己
Published by
Privacy International Japan（**PIJ**）
IB Bldg. 10F,3-25-15 Nishi-ikebukuro
Toshima-ku, Tokyo, 171-0021,Japan
President Koji ISHIMURA
Tel/Fax +81-3-3985-4590
http://www.pij-web.net
2019.4.11 発行 CNN ニューズ No.97

入会のご案内

季刊・CNN ニューズは、**PIJ** の会員（年間費 1 万円）の方にだけお送りしています。入会は **PIJ** の口座にお振込み下さい。

郵便振込口座番号
00140 － 4 － 169829
ピー・アイ・ジェー（**PIJ**）

NetWork のつぶやき

• ネット市場は盛況だ！リアル市場では、金融業など産業のガラ系化が止まらない。税理士など資格取得で再生を狙う者も。だが、2045 年がシンギュラリティで、AI が MI（人間の知能）を超える予想。資格で喰えない時代も近い。飲食業や物流、建設、介護等々、「人手」の要るリアル市場での生存競争が続く。　（N）

© 2018 PIJ