２０１４（平成２６）年6月２６日

内閣官房情報通信技術（IT）総合戦略室パーソナルデータ関連制度担当室
（FAX:03-3581-2615）
消費者庁消費者制度課個人情報保護推進室（FAX:03-3507-9283）
総務省情報流通行政局情報流通振興課
経済産業省商務情報政策局情報経済課
内閣府消費者委員会（FAX:03-3507－9989）
内閣官房社会保障改革担当室（FAX:3505-3852）

個人情報保護法制に関する意見書[1]

弁護士　山口　広
弁護士　篠島正幸
弁護士　水町雅子
弁護士　宮内　宏
弁護士　酒匂禎裕
弁護士　金田万作
弁護士　鬼鞍奈美

[1] 本意見書は，平成２５年１月時点で一度完成し，平成２６年１月時点で再修正したものでであり，事実関係は当該時点で確認したものである。

目次

意　見　の　趣　旨 3
意　見　の　理　由 4
第１　はじめに 4
１　本意見書の目的 4
２　個人情報のビッグデータ化 4
３　ビッグデータとしてのパーソナルデータの利用実態 4
４　個人情報保護法制の見直しの必要性 5
５　本意見書の構成 5
第２　個人情報・プライバシーを取り巻く現在の状況 6
１　総論 6
２　パーソナルデータを利用したマーケティング 6
３　個人情報抜き取りアプリ 11
４　コミュニケーションアプリ 14
５　パーソナルデータ流出による被害の甚大性と回復困難性 17
６　小括（現状の問題点） 18
第３　現在の法律等による規制とその問題点 20
１　総論 20
２　運用・執行における問題 20
３　規制範囲の問題 21
４　取扱いの不透明性の問題 23
５　本人参加・救済における問題 27
６　小括 29
第４　意見の具体的内容とその合理性 29
１　機関の一元化 29
２　規制範囲の適正化 32
３　取扱いの透明化 34
４　本人参加の権利の保障・救済 37
第５　まとめ 38

意　見　の　趣　旨

第１　独立性・中立性を有する第三者機関にて，個人情報保護法制全般に係る法所管・執行を行い，同機関に十分な権限，予算および人員を確保するべきである。

第２　ビッグデータの流通に伴うプライバシー権侵害リスクの増大に鑑み，現状にあわせて個人情報保護法に関する次の法改正を行うべきである。

１　実質的に個人を識別しうる情報を個人情報の範囲に含め，かつ第１記載の一元化機関が定期的に個人情報の定義を見直すようにする（第２条第１項)。

２　原則として，本人の同意がなければ個人情報の提供が認められないようにする（第２３条)。

３　共同利用の要件を厳格化し，真に必要な場合以外には個人情報の提供が認められないようにする（第２３条第４項第３号)。

４　個人情報取扱事業者に対し，どのような個人情報をどのように取り扱うのかを本人に対し説明する責任を課す。

５　個人情報の開示，訂正，利用停止請求権に関し，これが裁判上の請求権たりえることを明記する（第２５条乃至第２７条)。

６　第１記載の一元化機関に裁判外紛争解決に係る権限を与え，個人に対する迅速な救済を図る。

第３　個人情報保護法の趣旨・目的が達成できていないと考えられる現状を解決すべく，次の点について法解釈を明確化すべきである。

１　目的外取扱い及び目的外提供に関する本人の同意について，同意を得たと認められるための要件を明確化する（第１６条第１項及び第２３条第１項)。

２　オプトアウトが認められるための要件を明確化する（第２３条第２項)。

３　共同利用の要件を明確化する（第２３条第４項第３号)。

第４　海外事業者に対しても法規制を及ぼし，かつ各国の関係当局と協力すべきである。

第５　各省庁による個人情報保護に関する事業分野ごとのガイドラインを廃止し，第１記載の一元化機関が基本ガイドラインを策定した上，各分野における細則を策定すべきである。

第６　個人情報保護法違反に限らず，プライバシー権侵害事例についても，第１記載の一元化機関が積極的に啓蒙啓発を行うべきである。

第７　個人情報の大量流出事件の被害の実態に則した事後的救済制度として，一部の被害者による訴訟追行の結果としての判決効が被害者全体に及ぶクラスアクション制度を導入すべきである。

意　見　の　理　由

第１　はじめに

１　本意見書の目的

本意見書は，高度情報化社会におけるネットワーク上で流通する膨大なパーソナルデータ[2]に関する取り扱いについて，上記「意見の趣旨」記載のとおり，現行の「個人情報の保護に関する法律」（以下「個人情報保護法」という。）における法規制のあり方と政府の取り組みにつき再考を促すことを目的としている。

２　個人情報のビッグデータ化

ネットワーク社会において，一定のパーソナルデータが迅速に流通することそれ自体は，その有用性から歓迎されるべきことである。しかしながら，通信情報網の拡充によるデータ転送速度の超高速化，大容量記憶装置の急速な発展，洗練された検索・解析技術により，無秩序に流通しているパーソナルデータを極めて容易に集約することが可能となった。

すなわち，ネットワークを流通するパーソナルデータは，今や「ビッグデータ」と化し，名簿や電話帳など，旧来，個人情報保護法が想定していたデータとはまったく異なる形態で存在，流通し，集積されているのである。

３　ビッグデータとしてのパーソナルデータの利用実態

現在，ネットワーク上に存在するパーソナルデータは，一見すると分散して存在し，一部は匿名情報として，また一部は情報主体（本人）に不可視なものとして流通する。そのため，情報主体側からすれば情報の取扱いに規制をかける必要性が低いかのように見える。しかしながら，現実には，これらの情報は，多数の企業により追尾・統合された上，インターネット上の擬似人格として再構成されており，企業はこの擬似人格の購買履歴や閲覧履歴等から趣味，嗜好，思考パターンを分析し，「行動ターゲティング広告」等の営利目的に利用している。

加えて，各事業者によって個別に管理されるべきパーソナルデータについてすら，企業間の複雑な連携と取引上のネットワークを通じ，情報主体の明確な自覚のないまま全部又は一部が流通し，統合された上，購買履歴等を分析され，商取引に利用されているのである。

このように，ビッグデータと化したパーソナルデータは，今や，一定の技術的手段により容易に「もう一つの自分」を再構成させうるほどの量及び質を満たしており，

---

[2] 個人情報保護法では同法上「個人情報」に該当しないものは，同法の規制対象外とされるが，現在のプライバシー権及び個人情報を巡る問題の実情を踏まえると，同法上の個人情報に該当するか否かが不明瞭であるもの，また個人情報に該当しないものについても，個人のプライバシー権に対し重大な影響を及ぼす恐れが認められる場合がある。そこで本意見書では，同法上の個人情報に該当するもののほか，個人に関連する情報であって「個人情報」に該当しないものも含め，以下「パーソナルデータ」と呼称し意見を述べることとする。

統合された情報がひとたび流出すれば，容易に個人識別情報と結合し，我々一般消費者のプライバシー権は回復不可能なほど傷つけられるという危機的状況にある。しかしながら，すでに，このようなパーソナルデータについて，いつ，誰が，いかなる目的で保有し，現在どのような状況に置かれているのかについて，もはや情報主体はまったく把握できないのが現状である。

４　個人情報保護法制の見直しの必要性

かかる膨大な，しかしながら統合が容易なパーソナルデータが氾濫する状況は，すでに現行法規制が想定していた枠を大幅に逸脱しており，ことに，第三者提供規制や利用目的規制については，個人情報の定義の狭さと相俟って，もはや有名無実化しているといってよい。

この事実は，我々一般消費者のプライバシーを危機的状況に直面させるばかりではない。企業にとっても，実効性のない法規制は行動規範としての意味を喪失し，営業活動における予測可能性を奪い，終局的には企業活動の健全性を奪うことになる。現に，大量のパーソナルデータを保有する事業者が，曖昧な個人情報保護法の規制を前提とした，利用者に対する消極的意思確認によって，パーソナルデータを収集するとともに，第三者に大量のパーソナルデータを提供している事例も各種報道から見て取れる。これらは故意ではなく過失であるケースも多く，また，現段階における実被害としては比較的軽微であるものの，ビッグデータ化したパーソナルデータの取り扱いのリスクを象徴している。かかるリスクを放置したまま情報漏えい事故が発生した場合，一般消費者が被る損害はもはや回復しがたいほど甚大となることが容易に予想される。

したがって，高速で流通し，大量に蓄積されるパーソナルデータの適切な利用と，情報主体のプライバシー保護を調和させるため，速やかに現行の個人情報保護法制を抜本的に見直す必要がある。

５　本意見書の構成

このような個人情報を取り巻く事情を前提に，本意見書においては，「意見の趣旨」のとおり，法規制の見直し及びパーソナルデータに関する政府の取り組みの再考を求めるものである。

本意見書においては，まず意見の正当性を基礎づける根拠事実として，個人情報・プライバシーを取り巻く現状を説明し（後述「第２」），かかる現状を前提とした法規制の問題点を個別に抽出する（後述「第３」）。その上で，本意見における提言の具体的内容と，同提言が上記ビッグデータと化したパーソナルデータの利用規制のためにいかに合理性を有するかについて説明する（後述「第４」）。

第２　個人情報・プライバシーを取り巻く現在の状況

１　総論

前述の通り，近年，個人の行動履歴やセンサーデータなどのパーソナルデータが収集されることが多くなってきている。

以下では，こうしたパーソナルデータの活用事例の概要を示すとともに，その問題点を抽出し，対策の必要性について示す。まず，パーソナルデータのマーケティングへの利用として，下記①及び②を，次に，スマートフォンのアプリケーションでパーソナルデータを取得するものとして，③～⑤を論じる。最後に，いわゆるコミュニケーションアプリの問題点について，下記⑥～⑧を例に挙げて説明する。

本意見書に記載したパーソナルデータ活用事例
①　行動ターゲティング広告（後述「２（１）」）
②　Ｔポイントサービス（後述「２（２）」
③　「…the Movie」等（後述「３（２）ア」）
④　ミログ（後述「３（２）イ」）
⑤　全国電話帳（後述「３（２）ウ」）
⑥　「LINE」（後述「４」）
⑦　「comm」（後述「４」）
⑧　「カカオトーク」（後述「４」）

２　パーソナルデータを利用したマーケティング

パーソナルデータを収集・分析し，マーケティングに活かそうとする動きが企業で本格化している。ここでは，従来から行われていたインターネット上の行動履歴等を元にした行動ターゲティング広告と，最近になって登場した，物理的店舗における購買履歴等も含め収集・分析する共通ポイントサービスを例に挙げて，現状を説明する。

（１）①行動ターゲティング広告

ア　概要[3]

行動ターゲティング広告とは，個人のインターネット利用履歴（Web サイトの検索や閲覧の履歴など）を元に興味や行動特性を特定し，各利用者にとって最適な広告を配信する広告手法であり，IP アドレス，cookie[4]番号，端末 ID などで対象者を

[3] 総務省情報通信政策研究所「行動ターゲティング広告の経済効果と利用者保護に関する調査研究報告書」（H22.3）９頁では，代表的なターゲティング広告として行動ターゲティング広告，検索連動型広告，属性ターゲティング広告，コンテンツ連動型広告を挙げている。
http://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2009/2009-I-16.pdf

[4] Web サイトの提供者が，Web ブラウザを通じて訪問者のコンピュータに一時的にデータを書き込んで保存させるしくみをいう（「IT 用語辞典 e-Words」より）。

管理する（同一人物だとして履歴情報を収集する）ことが多く，対象者の氏名等の個人情報を持たないのが一般的である。

行動ターゲティング広告は，インターネット広告の中でも比較的新しい広告手法であり，ライフログ[5]の活用の一例として，インターネット広告業界において注目されている分野のひとつである。有名なものでは，Google，Yahoo!，Amazon，DAC，楽天などが，行動ターゲティング広告を実施している。これらの業者は，多数のウェブサイトを集めた大規模なアドネットワーク（広告枠）を保有する。そして，ウェブサイト閲覧履歴をブラウザの cookie に紐付けして利用者を管理し，利用者の興味・嗜好をプロファイリング（分析）して，当該利用者がアドネットワークを閲覧した際には，利用者の興味・嗜好に合致する行動ターゲティング広告を表示する。

例えば，ある利用者が，証券会社のサイトや株取引のブログを閲覧した場合，ウェブサイト閲覧履歴より，当該利用者は株に興味があるとプロファイリングされる。そのように特定された利用者が，次にアドネットワークに加盟しているブログを閲覧すると，（株とは全く無関係な内容のブログであっても）当該ブログの広告欄に株に関連した広告が表示される。

イ　問題となった事例

アメリカの事例であるが，利用者の商品購入履歴を分析し妊娠 16 週～28 週と思われる女性を特定し，ベビー用品の E メール広告を行っていたところ，妊娠した未成年の女子高校生にも届き，父親がこの E メールを見て娘に問いただしたことで，父親に隠していた妊娠の事実が発覚したという事例がある。父親にさえ隠していた妊娠の事実という非常にセンシティブな情報を企業が一方的に分析し利用している点に大きな問題がある。[6]

ウ　メリット・デメリット

行動ターケティング広告により，広告主は，広告に関心を示す可能性の高い特定の顧客に絞って広告を表示することができ，広告効率が向上する。また，広告媒体サイトは，より広告効率の高い広告を提供することで，広告枠の価値を高めることができる。利用者にとっても，自分の興味や関心に合った広告が表示されるので，必要かつ有用な情報にアクセスし易くなる。

しかしながら，上記のようなメリットがある一方で，利用者にとって，下記のよ

---

[5] 電子的に記録できる人の生活記録を言い，インターネットサイト閲覧履歴，検索履歴，ダウンロード履歴，ネットショップでの買い物履歴といったネットライフ上の行動履歴から，物理的店舗での買い物履歴，個人が今現在所在している物理的場所の履歴等といったリアルライフ上の行動履歴までも幅広く含む概念（水町「ライフログに関するプライバシー権侵害訴訟の検討」自由と正義 2011 年 11 月号より）。ライフログはパーソナルデータではあるものの，必ずしもビッグデータに該当するものではない。ただし，行動ターゲティング広告に用いられるようなライフログは，量・種類・頻度等の側面においてビッグデータ化していると考えられる。

[6] ニューヨークタイムズ
http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=7&_r=3&hp

うな問題点も存在する。すなわち，このような分析は，広範かつ大量のデータに基づいて，情報提供時の利用者の想定を離れて，利用者の人物像についての勝手な分析をしているのであり，その結果，利用者が知られたくない嗜好（場合によっては事実まで）が企業に把握されることとなるのであるから，利用者のプライバシー権の侵害につながる可能性がある。また，全く関連のないウェブサイトを閲覧していても，過去の行動履歴に基づいた広告を表示されることにより，煩わしさや不快さを感じたり，監視されているのではないかと不安になったりする利用者も少なくないように思われる。

また，そもそも，どのような情報が広告媒体サイトによって収集され，誰にどのように利用されているのか知らずに，広告に誘導されている場合も多いようにも思われる。上記の例でいえば，株に関心のある利用者は，株関連の Web サイトを閲覧していないときであっても，株関連の広告を表示されることとなるが，利用者にしてみれば，自分の興味が分析された上で自分に対し広告が表示されていることに気付かない場合が多いといえるだろう。

このように，自己の情報に対するコントロールが及ばない現状には問題がある。

自己の情報に対するコントロールが及ばない状況で，行動履歴情報が，個人情報と紐付けされ，あるいは，個人情報と紐付け可能な行動履歴情報が第三者に漏洩した場合には，利用者のプライバシー権が侵害されるおそれがある。上記２（１）イで述べたアメリカの事例などは，隠している事実・趣味・嗜好についてのセンシティブな情報に関する分析によるプライバシー件侵害の危険が現実的になっていることを示すものである。

このような分析が広範に行われるようになれば，知らない間に購買記録，閲覧履歴などの多様な情報が組み合わされて自己の行動が分析されることにより，プロファイリング的な使われ方をするおそれがある。例えば，「高額商品を衝動買いする傾向にある」「日曜日の夜にクーポンメールを送ると，ゲームの有料アイテムを購買する傾向にある」といったマーケティング目的の分析から，「暴力的衝動傾向がある」「友達が少ない」などといった人格分析までも可能であり，より発展して「犯罪者予備軍」「引きこもり」「自殺思考が強い」などと分類されて，差別的な取扱いを受けることも否定できない。

なお，DNT（Do Not Track）機能をサポートしているウェブブラウザ（Firefox，IE10 など）で DNT 機能を有効にすると，DNT 機能をサポートしているウェブサイトでは，cookie による履歴追跡を行わなくなる。ただし，DNT は，DNT 機能をサポートしていない（無視する）ウェブサイトや，cookie 以外の方法による情報収集を行うサイトには意味がないので，決定的な方策とはいえない。

（２）共通ポイントサービス

パーソナルデータを利用したマーケティングとしては，行動ターゲティング広告の他にも，共通ポイントサービスが存在する。共通ポイントサービスとは，共通ポイントサービスの運営会社との間で会員登録をすると，当該共通ポイントサービスに参加している企業（以下「参加企業」という。）での買物の際に会員カードを出せば，「ポイント」（参加企業での買物の際に 1 ポイント 1 円相当で利用できたり，商品と交換できたりする）が得られるサービスであるが，運営会社は，当該会員の購入履歴等を収集・分析し，会員に対し購入履歴等に応じた広告や割引クーポンを発行するなどして，マーケティングに利用している実態がある。今回は例として②「T ポイントサービス」を挙げて説明するが，株式会社ロイヤリティマーケティングが運営する「Ponta」などもある。

ア　T ポイントサービスの概要

T ポイントサービスとは，カルチュア・コンビニエンス・クラブ株式会社（以下，「CCC」という。）の子会社である株式会社 T ポイント・ジャパン及び株式会社 T ポイントが運営する共通ポイントサービスのことである[7]。2013 年 4 月末には会員数が 4500 万人を突破しており，2014 年 1 月末現在 58,000 店舗において利用することができる。

T ポイントサービスによるマーケティングの仕組みの概要は，以下のとおりである。

T 会員となろうとする者は，T 会員規約に同意[8]したうえで，T カードの発行を受ける。そして，T 会員が，ポイントプログラム参加企業（以下，「加盟店」という。）において，T カードを提示して商品の購入又はサービスの利用をすると，加盟店から CCC に対して購入履歴等の情報が送信される。

さらに，CCC は，T カードの利用に伴い T 会員の購入履歴等のパーソナルデータを収集・分析して，各会員のニーズに沿った割引クーポンの発行や，加盟店に対するマーケティング情報の提供を行っているとされている[9]。

イ　T ポイントサービスに関連した問題となった事例

T ポイントサービスに関連して問題となった事例として，以下の事例がある。

（ア）公共図書館への T ポイントサービスの導入

2012 年 5 月 4 日，佐賀県武雄市と CCC は，武雄市図書館・歴史資料館の企画・運営に関して提携すると発表した。

会員が T カードを提示して図書館を利用することになれば，上記 T ポイントサ

---

[7] T-SITE によると「T ポイントは，全国の T ポイント提携先で，ご利用金額に応じて貯めたり，お使いいただくことができるポイントです。貯めたポイントは，全国の提携先で使えるだけではなく，提携先が発行しているポイントや商品との交換をすることもできます。」とされている。
http://tsite.jp/pc/r/tp/

[8] この「同意」が真の同意に当たるか否かについては，３（３）イ（ア）において後述する。

[9] 「T カードのご利用状況や来店頻度をはじめ商圏分析や客層分析レポートなどでお店をサポートします。」（http://tsite.jp/r/fs/area/index.html）

ービスに従い会員の図書貸出履歴が CCC に送信され情報集される。図書館が CCC に対して図書貸出履歴等のパーソナルデータを提供することは，「読者が何を読むかはその人のプライバシーに属することであり，図書館は利用者の読書事実を外部に漏らさない」，「図書館は，読書記録以外の図書館の利用事実に関しても，利用者のプライバシーを侵さない」，「利用者の読書事実，利用事実は，図書館が業務上知り得た秘密であって，図書館活動に従事するすべての人びとは，この秘密を守らなければならない」としている「図書館の自由に関する宣言」に反するという批判があった[10]。

（イ）ドラッグストアへの T ポイントサービスの導入[11]

T ポイントサービスに加盟している医薬品販売業者（ドラッグストア）が，会員が T カードを提示して購入した医薬品の商品名を含む購買履歴等を CCC に送信し，マーケティングに利用していた。しかし，医薬品の商品名を含む購買履歴は，一般的に，他の商品と比較して，本人にとって他人に知られたくない情報の一つであると考えられる。さらに，朝日新聞 2012 年 7 月 17 日によると「厚労省情報政策担当参事官室は「医薬品販売事業者は患者の尊厳を守る責務がある。一般用医薬品も身体状況を如実に表すもの。購買者には CCC がどんな情報を得ているかをわかりやすく示し，同意を得ることが必要だ」としている。

（ウ）T ポイントツールバーによるウェブサイト閲覧履歴取得

T ポイントツールバーは，これを用いてウェブを検索すると T ポイントが貯まるというサービスであったが，ウェブ検索履歴だけでなく，すべてのウェブ閲覧履歴が CCC に取得されてしまう他，セキュリティ上の問題もあったため，批判が相次ぎ，2 週間ほどでサービスが中止となった（ただし，その後，セキュリティ上の問題が解決されたとして，サービスが再開された。）。

ウ　共通ポイントサービスのメリット・デメリット

行動マーケティング広告と同様に，共通ポイントサービスにより，参加企業は，運営会社を通じて各顧客の趣味嗜好に応じた広告を表示し，あるいは割引クーポンを配布することができ，マーケティング効率を向上することができる。また，運営会社は，マーケティング効率の高いサービスを提供することで，参加企業から利益を得ることができる。利用者にとっても，自己の趣味嗜好に応じた広告が表示されたり割引クーポンを貰えたりするだけでなく，参加企業で買物をするだけで、参加企業で共通に利用できる「ポイント」が貰えるというメリットがある。

---

[10] 武雄市の樋渡市長は「従来の図書館カードか，ポイントの付く T カードかは，利用者に選んでもらう。貸し出し履歴が外部に出ることは一切ない」としており，また市教委は「T カードを選択した場合，図書館から CCC 側のポイントシステムに提供されるデータは，会員番号やポイント数，貸し出し点数など 5 項目に限定して運用する」としている（朝日新聞 2012 年 6 月 25 日）。

[11] 詳しくは，「T ポイントサービスに関する要望書」（http://www.yakugai.gr.jp/topics/file/Tpoint_service_ni_kansuru_youbousho.pdf）参照。

しかし一方で，利用者にとって，行動ターゲティング広告と同様の問題も存在する。例えば，加盟店Ａでの購入履歴に基づき，まったく業種の違う加盟店Ｂでの買物の際に，自己の趣味嗜好に応じたクーポンを発行された場合，はっきりと認識できないところで自己の情報が収集・分析され，さらに第三者（加盟店ではある）に提供されていることに，気持ち悪さを感じる人も少なくないと思われる。また，それだけではなく，収集した情報を不正に利用する業者が参加企業に加入していても，利用者がそれを管理ないし排除できないというリスクもある。さらに，図書館やドラッグストアが加盟店となっていれば，薬の購入履歴（病歴）や図書貸出履歴（思想・信条）などの情報まで加盟店に提供されるおそれがあるが，それらの情報はまさに個人のプライバシーであり，流出することで重大なプライバシー権侵害を引き起こすし，身辺調査や思想調査に用いられ，深刻な権利侵害を引き起こす可能性も否定できない。

共通ポイントサービスでは，行動マーケティング広告と異なり，収集・分析対象となる情報には，インターネット上の行動だけでなく，現実社会での購入履歴等も含まれるため，インターネット上の行動情報と現実社会の行動情報を組み合わせることにより，特定の利用者についてより精緻な分析が可能となる。そのため，利用者のプライバシー権を侵害する可能性はより大きいといえる。

３　個人情報抜き取りアプリ

（１）概要

スマートフォンの使用者数はこの数年で急増しており，総務省通信利用動向調査[12](2013 年 6 月 14 日発表)によると，2012 年度末におけるスマートフォンの世帯普及率は 49.5%で，半数近くの世帯がスマートフォンを所持しているとのことである。

スマートフォンの魅力は，スマートフォンが，携帯電話が有する通信機能に加え，PC が有する高度な情報処理機能を併せ持ち，日常生活からビジネスまで，いつでもどこでも手軽に様々な用途に活用できる点にある。スマートフォンで利用できる多種多様なアプリケーションソフト（以下「アプリ」という。）も提供されており，利用者は，一般に，それぞれの目的に適うアプリをインストールして利用している。

ところが，近時，スマートフォンに記録された個人情報を抜き取るアプリ（「個人情報抜き取りアプリ」などと呼ばれている）の存在が問題になっている。スマートフォンからは，利用者（契約者）の氏名，電話番号，メールアドレス，スケジュール，位置情報，通話・通信履歴，Web サイト閲覧・商品購入等の履歴，さらには，第三者の電話帳データ（氏名，電話番号，メールアドレス等）の情報を取得することも可能であるが，アプリの中には，利用者に知らせることなく，これらの情報を抜

[12] 「通信利用動向調査平成 24 年調査」
http://www.soumu.go.jp/johotsusintokei/statistics/data/130614_1.pdf

き取り，アプリのサービス向上のために用いるに留まらず，市場調査や広告サービスに利用し，さらには外部へ流出させる等するものが存在する。あるセキュリティソフト会社の発表[13]では，Android（アンドロイド）アプリの 26%は単なるアドウエア（広告表示）にとどまらず，より詳細な個人情報を収集して，ショートメッセージを利用した詐欺やデバイスの管理者権限を奪取しようとする悪質なアプリであったとの調査結果を発表した。

（2）問題となった事例

特に問題が大きいパーソナルデータの外部流出に関する事例としては，以下のようなものが挙げられる。

ア　③「…the Movie」等

2012 年 4 月ころにウェブサイトに掲載された「…the Movie」などのタイトルのアプリ（問題のアプリは 16 本確認されている）は，人気ゲームの動画紹介やミニゲームのアプリであるが，その裏で，利用者に知らせることなく，スマートフォンに保存されている利用者のパーソナルデータや第三者の電話帳データ（氏名・電話番号・メールアドレス）等を抜き取り，外部の特定のサーバに送信する仕組みとなっていた[14]。

これらのアプリのインストール画面では下記のような内容を表示して利用者のアクセス許可を求めており，形式上は，利用者の「許可」を取得している（サクセス許可を認めないとアプリを利用できない。）。しかし，通常の利用者の認識からすれば，あくまで人気ゲームの動画紹介やミニゲームのアプリであると思ってダウンロードしており，アクセス許可について認識していないか，認識していたとしても，その限度での（例えば広告表示のための）アクセス許可であって，外部のサーバにパーソナルデータが送信され勝手に利用されることは想定していないものと思われる。

このアプリケーションに許可する権限	
ネットワーク通信	完全なインターネットアクセス
個人情報	連絡先データの読み取り
電話／通話	携帯のステータスと ID の読み取り

これらのアプリによって，延べ約 81 万人が「ウイルス対策」などとうたった偽のアプリをダウンロードし，約 3700 万人分の電話帳データを抜き取られたとされるが

[13] 「アンドロイドのアプリ 26%は悪質なもの，マカフィー調査」
http://www.nikkei.com/article/DGXNASFK0100W_R01C13A0000000/
[14] http://itpro.nikkeibp.co.jp/article/NEWS/20120417/391245/

[15]，警察は，これらのアプリを作成した会社の元社長などを逮捕したが，嫌疑不十分で不起訴処分となった。

イ　④「ミログ」

株式会社ミログが 2011 年 8 月頃から提供していた動画配信アプリ「app.tv」は，実行中の他のアプリの履歴を株式会社ミログへ送信する仕組みを備えたものであり，また同年 9 月頃に提供した「AppLog」も，同様に，利用者がどのようなアプリをいつ，何回使ったかを記録して趣味嗜好を分析し，興味を引きそうな広告を配信するというものであった。

「app.tv」では，利用者が規約等に同意する前の段階ですでに情報の取得・送信を行っていたほか，「AppLog」では，利用者の同意を得る際に「端末のアプリケーション情報等」を送信するとしか説明されていなかった。こうしたアプリによる情報の収集が「プライバシー権の侵害に当たるのでは」という指摘・批判が高まり，株式会社ミログは，同年 10 月 10 日に，「AppLog」及び「app.tv」両サービスの停止を発表し，翌 2012 年 4 月 2 日には，会社の清算，解散を発表した。

ウ　⑤「全国電話帳」

2012 年 9 月にウェブサイトに掲載された「全国電話帳」は，ハローページとタウンページに掲載された情報をデータベース化してスマートフォン上で利用できるようにした無料アプリであるが，それだけではなく，利用者の電話番号や住所，メールアドレス等をスマートフォンから抜き取り，利用者間で閲覧できるようにもしていた。

ウェブサイトには，「過去のハローページとタウンページに掲載された約 3800 万件の情報をもとにデータベースを作成しています。加えて，アプリ利用者のアドレス帳，GPS の情報も利用します」との注意書きが記載されているが，注意書きを十分読まずにインストールしてしまった利用者も多いとみられ，約 3300 台のスマホから約 76 万人分の個人情報が流出したことが確認されている。

「全国電話帳」はサービス提供を中止したが，現在，新たに「全国共有電話帳」という名前のアプリとしてサービス提供されている。

（3）メリット・デメリット

このようなアプリの多くは，利用者の意図に反してパーソナルデータを流出させるもので，利用者にメリットにはデメリットしかない。スマートフォンに保存された情報には，利用者の交友関係や行動履歴といったより詳細なパーソナルデータや利用者以外のパーソナルデータまで含まれており，その流出が引き起こすリスクは想像以

[15] 「不正アプリ使い勧誘　80 万人のデータ抜き取り　ＩＴ企業社長ら逮捕」
http://sankei.jp.msn.com/affairs/news/130724/crm13072411530007-n1.htm

上に大きい。プライバシー権侵害等の問題だけではなく，高額な利用料金の請求，迷惑メール，詐欺などに悪用されるおそれがある。

４　コミュニケーションアプリ

携帯電話・スマートフォン（以下，「携帯端末」という。）の電話帳データを利用し利用者間でコミュニケーション（通話やメール・チャットなど）ができるコミュニケーションアプリは，事業者に悪意がなくとも，利用者による設定や事業者の過失（プログラムの不具合）によって，パーソナルデータが流出するおそれがある[16]。コミュニケーションアプリには様々なアプリがあるが，以下では，特に利用者が多く[17]，それに伴うパーソナルデータの流出の危険性が高い⑥「LINE」⑦「comm」⑧「カカオトーク」といったコミュニケーションアプリについて現状を述べる。

（１）概要

コミュニケーションアプリとは，アプリをダウンロードした利用者間のうち，互いに「友だち[18]」として登録した相手と当該アプリを介して無料（パケット通信料は別）で通話やメール・チャットなどのコミュニケーションを行うことができるものをいう。利用者は携帯電話番号や登録 ID[19]によって友人・知人を検索し，「友だち」として登録申請することができる。さらに，利用者が自己の携帯電話に保存されている電話帳データをそれぞれの事業者のサーバにアップロードすれば，アプリ側で，各事業者が保有しているアプリ利用者の電話番号データと照合し，利用者の電話帳に記録された携帯電話番号の保有者の中に当該アプリを利用している者がいれば，当該アプリ利用者を「友だち」の候補として表示したり，「友だち」として一括登録申請したりするサービス（以下，「友だち自動追加サービス」という。互いに当該サービスの設定をしていれば両者がアプリをダウンロードした瞬間に自動的に「友だち」となる。）も提供している。また，利用者はアプリ上で自己のプロフィール情報を設定・公開することができるが，その公開の可否及び公開範囲は，利用者が選択することができる（例えば，自己プロフィールの全部を「友だち」でない者に公開することもできるし，プロフィールの一部については「友だち」のみに公開することもできる。）。

---

[16] 第２．３で述べた個人情報抜取りアプリと同様，流出するおそれがあるパーソナルデータは，利用者自身のパーソナルデータだけではなく，利用者の保有する（スマートフォン等に保存されている）他者のパーソナルデータも含まれる。

[17] H25.1 時点で，LINE は約 4100 万人，「カカオトーク」は約 750 万人，「comm」は約 500 万人

[18] アプリによって名称は異なる。

[19] 携帯電話番号の個人識別機能に着目し，利用者の携帯電話番号１つにつき１つの ID を付与し，携帯電話・スマートフォンでの情報共有化を図っている。

（２）問題となった事例

ア　不十分な規約，頻繁な規約の改定

（ア）具体例１：旧 LINE 利用規約

旧 LINE 利用規約において，

「1. 当社は，本サービスにおいて，電話番号，メールアドレス，アドレス帳，プロフィール情報(ユーザー名，ユーザーID，画像ファイル，ステータスメッセージなど)，携帯電話の端末情報などを以下の目的のために収集いたします。

（中略）

(4) 利用者の利便性向上，より良いサービス提供のための利用者傾向の分析などのため」

との規定があり，アドレス帳（電話帳データ）に登録されている他人の情報や個人の画像データなどを事業者が収集し，利用者分析等に利用しているのではないかという批判がなされた。⑥LINE を運営する NHN 社では，アドレス帳のうち，用いる情報は登録されている「電話番号および携帯電話メールアドレス」のみであり，プロフィール情報も利用者が LINE に登録した情報に限ると説明し，これに合わせて利用目的を限定した規約に変更した。

（イ）具体例２：旧 comm 利用規約

旧 comm 利用規約において，

「当社は，すべての comm 会員記述情報（当社の運営するサイト内に comm 会員が記述したすべての情報及び comm 会員間でメール・チャット等によりやりとりされるすべての情報）を無償で複製その他あらゆる方法により利用し，また，第三者に利用させることができるものとします。」

との規定があり，通信の秘密の侵害や電気通信事業法違反にあたるのではないかとの批判がなされた。

当初，⑦comm を運営する株式会社ディー・エヌ・エーは「そのような意図はなく，サービス提供に必要な範囲のみで利用する」と釈明し規約を変更しないとの立場であったが，翌日には規約を変更し，「当社は，すべての comm 会員記述情報を本サービスの提供を目的とする範囲において無償で複製その他の方法により利用できるものとします」と利用範囲を限定した上で，「ただし，comm 会員間でメール・チャットによりやりとりされる情報を，令状等による場合を除き，当社，第三者が閲覧することはありません」とした。

（ウ）頻繁な規約の変更

このように，規約に問題点がある場合や，規約の内容が不十分な場合に規約変更がなされる他，それ以外の場合にも頻繁に規約変更が行われる点は問題といえる[20]。

[20] ⑥LINE の利用規約は，平成 24 年だけでも 4 回規約変更がなされている。

イ　パーソナルデータ流出に関する不具合

⑥LINE の PC 版公式アプリで，平成 24 年 10 月 31 日，テキストチャット「トーク」画面に，他人の会話と思われるメッセージが表示される不具合が発生した。

また，平成２４年１１月２６日の Android 版⑥LINE のアップデート時に，電話帳データを⑥LINE のサーバにアップロードしない設定をしていても，強制的に電話帳のデータをアップロードし，電話帳に登録されている人物を「友だち」として自動的に追加してしまう（自動追加オフ機能が働かなくなる）不具合が発生した。

不具合はすぐに修正されたが，一度流出したパーソナルデータ（メッセージ内容や「友だち」のみに公開していたプロフィール情報など）は回収できず，取り返しがつかない問題といえる。

なお，このような規約変更は，規約上では，利用者への個別通知は不要で，規約変更後のサービスを利用しただけで同意とみなすことになっている場合が多い[21]。

ウ　電話番号登録による個人情報等の収集

⑥「LINE」⑦「comm」⑧「カカオトーク」といったコミュニケーションアプリでは，既に述べたとおり，電話帳データのサーバへのアップロードや友だち自動追加サービスなどがあるが，当該機能を悪用することにより，パーソナルデータの収集が可能となるおそれがある。すなわち，パーソナルデータの収集目的で，適当な携帯電話番号を自己の携帯端末の電話帳に入力し，それらのコミュニケーションアプリを利用すれば，当該アプリを利用し，かつ友だち自動追加サービスを利用しているまったく知らない人の「友だち」のみに公開しているプロフィールなどのパーソナルデータを取得することができる[22]。これを繰り返せば，多数の携帯電話番号と紐づいたパーソナルデータを入手することができ，悪用されるおそれがある。

（３）メリット・デメリット

コミュニケーションアプリの運営会社はアプリ上で広告を配信するなどして利益を得ることができる一方，利用者にも，利用者間で（パケット通信料を除き）無料

[21] LINE 規約「3. 規約の変更」では，「当社は、当社が必要と判断する場合、あらかじめお客様に通知することなく、いつでも、本規約および個別利用規約を変更できるものとします。変更後の本規約および個別利用規約は、当社が運営するウェブサイト内の適宜の場所に掲示された時点からその効力を生じるものとし、お客様は本規約および個別利用規約の変更後も本サービスを使い続けることにより、変更後の本規約および適用のある個別利用規約に対する有効かつ取消不能な同意をしたものとみなされます。かかる変更の内容をお客様に個別に通知することはいたしかねますので、本サービスをご利用の際には、随時、最新の本規約および適用のある個別利用規約をご参照ください。」となっている。

[22]具体的には，特定の利用者（A）が，自己の携帯端末の電話帳に適当な携帯電話番号を登録し，事業者のサーバに電話帳データをアップロードすると，自動的にアプリ利用者の携帯電話番号と照合し，当該携帯電話番号利用者（B）が当該アプリを利用しかつ友達自動追加サービス利用していた場合，A と B は自動的に「友だち」として登録されることになる。その結果，任意の携帯電話を電話帳に登録した A は，当該任意の電話番号の保有者 B が当該アプリの利用者か否かを（また公開している名前等も）認識することができるのみならず，利用者であった場合には「友だち」にしか公表していなかったプロフィール情報まで入手できてしまうという状況が発生する。

で手軽に通話やメール・チャットなどのコミュニケーションを行うことができるというメリットがある。しかし他方で，利用者による設定や事業者の過失（プログラムの不具合等）によって，大量のパーソナルデータが流出してしまうおそれがある点はデメリットといえる。

５　パーソナルデータ流出による被害の甚大性と回復困難性

言うまでもないことであるが，企業の保有する膨大なパーソナルデータが流出した場合，極めて多数の一般消費者のプライバシーが脅かされることとなる。ビッグデータと化したパーソナルデータの流出事件については，枚挙にいとまがない。

（１）プライバシー情報（個人情報を含むパーソナルデータ）の流出事件

大量の個人情報が流出した事例は，先例としての価値を有する宇治市住民情報流出事件（大阪高等裁判所平成 13 年 12 月 25 日判決・ジュリスト臨時増刊 1224 号 8 頁）[23]，ヤフーBB 事件（大阪地方裁判所平成 18 年 5 月 19 日判決・判例タイムズ 1230 号 227 頁）[24]，TBC 顧客情報等流出事件（東京高等裁判所平成 19 年 8 月 28 日判決・判例タイムズ 1264 号 299 頁）[25]などの裁判例からも明らかなとおり，個人情報保護法が施行される以前から既に多発しており，同法が施行された後も，企業がセキュリティ強化策を講じているにもかかわらず，パーソナルデータが流出した事例は後を絶たない。しかも，昨今は，過去の上記事件をはるかに凌駕する量のパーソナルデータが流通し，一般企業が頻繁に利用しているため，流出の具体的リスクは以前よりも高くなっている可能性すらあり，流出した際の被害の甚大性は比べものにならない。

実際に発生した近時の事例としては，2011 年 4 月，ソニー・コンピュータエンタテインメントに対する不正アクセスにより，オンラインゲームを利用する世界中の顧客のパーソナルデータが流出した事件がある。この事件で流出した顧客情報の数は 7700 万件，クレジットカード情報（ただし暗号化されていた）についても 1000 万件を上回るとされており，昨今の個人情報流出事件の被害の甚大性を如実に物語っている[26]。

（２）個人情報を含まないパーソナルデータの流出

上記で挙げた裁判例のとおり，個人情報保護法の個人情報に当たる，情報の流出は，被害救済の実効性はともかくとしても，明確に不法行為として司法救済の対象

---

[23] 宇治市による乳幼児検診システムの開発に際し，平成 11 年 5 月，再々受託業者のアルバイト従業員が住民基本台帳情報合計 21 万件を名簿業者に売却した事件。一人あたり 1 万 5000 円の損害賠償が認められた。

[24] ヤフーBB の元関係者が，平成 16 年 1 月，ADSL サービス会員情報 470 万件余を窃取し，暴力団関係者に売却した事件。一人あたり 1 万 2000 円の損害賠償が認められた。

[25] エステティックサロン TBC を主催する会社が，平成 14 年 5 月，センシティブ情報を含む 5 万件の顧客等情報をインターネット上に流出させた事件。一人あたり 3 万 5000 円の損害賠償が認められた。

[26] 読売新聞 2011 年 5 月 2 日。
http://www.yomiuri.co.jp/net/security/goshinjyutsu/20110502-OYT8T00649.htm

となってきた。しかしながら，今後はこのような個人情報を含まないパーソナルデータであっても，情報主体のプライバシー権が侵害されるおそれがあるものとして，その流出の問題点が顕現化しつつある。

例えば，ＪＲ東日本が，日立が 2013 年 7 月から開始した「日立 交通系 IC カード分析情報提供サービス」に，JR 東日本が提供する IC 乗車券「Suica」の 2011 年 2 月から 6 月までの匿名の乗車履歴を，利用者に対する告知なく提供したところ，各方面からの批判が相次いだ事件があった。JR 東日本は，かかる批判を受けて乗車履歴の情報提供を一旦凍結し，有識者会議によるデータ活用方法の再検討を行う旨発表した[27]。その後，JR 東日本は，原則として乗車履歴を第三者に提供するが，要望があった利用者の情報については提供しないという方法（オプトアウト方式）に変更したが，当該乗車履歴の情報は個人情報を含まない形で提供されているにもかかわらず，2013 年 7 月 26 日から同年 9 月 1 日までの間で，第三者提供の拒否を申し出た利用者は 3 万 9000 人にのぼったとのことである。

このような社会的背景からも，膨大なパーソナルデータは，個人情報保護法上の個人情報とはいえないものであっても，その流通と利用の適切性の確保のために法的規制を行うべき必要性を認めるまでに権利性を帯びているということができるのである。

６　小括（現状の問題点）

以上述べてきたサービスやアプリなど，現状，利用者にとってメリットがないわけではないが，利用者が知らずに，あるいは想定していないような方法で，パーソナルデータが利用されたり，流出したりするおそれがある。

確かに，一般的に，事業者は，利用者に対し，サービスやアプリの利用開始前に利用規約やプライバシーポリシーへの同意を求めているが，単に利用規約やプライバシーポリシーへのリンクが張ってあったり，非常に小さい字で書かれた画面を表示させたり，規約を別紙で配布するなどするだけで詳しい説明がない場合が多い。そのような中で，大半の利用者が利用規約等の内容を十分に理解しないままに，形式上だけ同意し，利用しているのが実態であり，パーソナルデータの提供について利用者の真摯な同意が得られているといえる場合は多くない（さらに，上記（２）ア（ウ）で述べたとおり，利用規約やプライバシーポリシーは利用者の知らないうちに頻繁に変更される場合もあり，同意が形骸化しているともいえる。）。

このように利用者の真摯な同意を得られているとはいえず，かつ初期設定やお勧め設定としてパーソナルデータが公開される設定（オプトアウト方式）になっていることも多い現状では，サービスやアプリを利用することにより，利用者の知らないうち

[27] 朝日新聞 Digital　2013 年 9 月 3 日。
http://www.asahi.com/national/update/0903/TKY201309030415.html

にパーソナルデータが流出する危険性は依然として大きい。

また，悪意を持った事業者がパーソナルデータを収集することによって，外出する時間帯を把握されて空き巣等の犯罪に用いられたり，ストーカー犯罪に用いられるおそれもある。

このような危険を防止するためには，パーソナルデータを取り扱う事業者が，利用者に，パーソナルデータの収集・分析を含めた利用目的・範囲・方法等について十分な説明をし，真摯な同意を得る必要がある。また，事業者はパーソナルデータの適正な管理・取り扱いを徹底し，利用者が意図しないパーソナルデータの流出が起きないような仕組み（オプトイン方式）を構築する必要がある。

第３　現在の法律等による規制とその問題点

１　総論

ビッグデータに関する現行の規制は，（ⅰ）個人情報保護法令，（ⅱ）法令ではないものの事実上の拘束力を有すると考えられる，各省庁において策定されている個人情報保護に関する事業分野ごとのガイドライン並びに総務省及び経済産業省等が研究会を開催して作成している報告書・指針類，（ⅲ）事業者団体等による自主規制，（ⅳ）プライバシー権侵害（不法行為）に対する保護に分けられる[28]。

しかし，これらによる規制には，以下で述べる通り，運用・執行における問題（後述「２」），規制範囲の問題（後述「３」），取扱いの不透明性の問題（後述「４」），本人参加・救済における問題（後述「５」）がある。

２　運用・執行における問題

（１）主務大臣による監督権がほぼ行使されていない

個人情報の大規模漏えい等の事件は後を絶たない状況にあり，また，以下で述べる通り，第２で述べたサービスにおいても，個人情報保護法上違法と考えられる状況があるにもかかわらず，主務大臣による監督権がほぼ行使されていない。

ア　利用目的の特定

個人情報保護法上，個人情報を取り扱うにあたっては，その利用目的をできる限り特定しなければならないものとされている（同法１５条１項）。また経済産業省のガイドラインでは，利用目的が具体的に特定されていない事例として「事業活動に用いるため」，「提供するサービスの向上のため」，「マーケティング活動に用いるため」といった例を挙げている。

しかし，上述した②T ポイントサービスでは「ライフスタイルの分析」（T 会員規約），⑥LINE では「利用者の利便性向上，より良いサービス提供のための利用者傾向の分析などのため」（旧 LINE 規約）といった，極めて抽象的な利用目的が定められている。これらの場合は，個人情報保護法上求められる，利用目的の特定がされておらず，違法とも考えられる。

イ　適正取得

個人情報保護法上，個人情報を取得するにあたっては不正の手段によってはならないものとされている（同法１７条）。しかし，上述した③「……the Movie」などの事件では，事業者が半ば意図的に，利用者の誤解を助長するような不十分な説明しか行わずに利用者に形式的な許可を行わせ，利用者が理解できないような態様で個人情報を抜き取っており，不正な手段による個人情報の取得に当たり個人情報保

[28] ビッグデータに対しては，これらの規制に加え，刑法，電気通信事業法等の特別法による規制も及ぶが，本意見書は，ビッグデータがプライバシー権，個人情報保護に対して与える影響，そしてかかる影響に対しどのような対策を行うべきかを主題とするため，刑法，特別法による規制については触れないこととする。

護法に違反すると考えられる。

ウ　主務大臣による監督権行使の状況

個人情報保護法は，各種監督を行う主体を主務大臣とし，主務大臣は事業者に対し報告徴収・助言・指導・勧告・命令を行うことができる（同法第 32 条乃至 34 条）。しかし実態としては，かかる監督権はほぼ行使されていない状況にある。例えば，平成 23 年度には，各府省合計で報告徴収 16 件，助言 1 件しか行われていない[29]。個人情報を取り扱う事業者の大部分が経済産業省の所管となると考えられるが，経済産業省は，平成 23 年度には報告徴収を 2 件，助言を 1 件しか行っていない。また医療機関も個人情報の取扱いに関し問題となる業種と考えられるが，医療機関を所管する厚生労働省では平成 23 年度に監督権を行使した例はない。

（2）個人情報保護法に関する照会に対応する官庁が不明確である

各主務官庁は，事業者による個人情報の適正な取扱いを支援するために，個人情報保護に関する事業分野ごとのガイドラインを作成している。しかし，事業分野ごとのガイドラインは 27 分野に及び，合計 40 種類も作成されている。事業者にしてみれば，そもそも自身がどのガイドラインに準拠すべきなのか，自身が準拠すべきガイドラインが他のガイドラインとどう異なり，どの点でより一層の配慮が必要なのか，などが非常にわかりづらい。

また各主務官庁は，事業分野ごとのガイドラインを担当するものの，個人情報保護法自体の法解釈権限はなく，個人情報保護法の法改正をすることもできない。一方，個人情報保護法の有権解釈権限を有する消費者庁は，個人情報保護法を所管するものの，同法に違反する行為等があった際に，報告徴収・助言・指導・勧告・命令を行う権限がないため，違法行為に対する取り締まりが行えない。事業者にしてみても，個人情報を取扱う新規事業を企画しようにも，個人情報保護法を所管する消費者庁に問い合わせるのか，事業分野別のガイドラインを所管する主務大臣に問い合わせるのかが明らかでない。

以上のとおり，現状では，事業者が個人情報保護法にのっとった適切な取扱いを行おうとしても，個人情報保護法に関する疑問点があった際に照会や相談を行うべき窓口が不明確であり問題である。

3　規制範囲の問題

また，運用・執行の問題ではなく，そもそも規制すべき範囲自体に，下記の通り

---

[29] ・金融庁：報告徴収 11 件
・総務省：報告徴収 2 件
・経済産業省：報告徴収 2 件，助言 1 件
・国土交通省：報告徴収 1 件
http://www.caa.go.jp/seikatsu/kojin/23-sekou.pdf 参照。

問題がある。

（１）個人情報保護法及びガイドラインの問題点

ア　「個人情報」の定義が不明確である

一つ目の問題点は，個人情報保護法で規制される対象である「個人情報」の定義の不明確さである。個人情報保護法上，個人情報に該当するためには，特定の個人を識別できる情報であることが必要である（同法第２条第１項）が，インターネットが活用される現代においては，氏名・住所のような個人情報該当性が明確なものによって個人を識別する場合だけではなく，ブラウザ等の端末を識別する情報等によってパーソナルデータを収集している場合も多いものと考えられる。しかし，ブラウザ等の端末を識別する情報が個人情報保護法上の個人情報に該当するかどうかは必ずしも明確でない[30]。

この点に関し，ビッグデータは，氏名・住所などと紐づけられていない限り個人識別性がない情報であるから，個人情報に該当しないとして，個人情報保護法の適用を否定する考え方も存在する。そして，このような考え方をとるのはビッグデータビジネスを行う事業者だけではない。前述した，④「app.tv」，「AppLog」が問題とされた株式会社ミログでは，第三者委員会を設置して「app.tv」，「AppLog」についての法的問題点を精査したが，事業者から一定の独立性を保っていると考えられる第三者委員会の報告書においてですら，株式会社ミログが取得した情報は個人情報には該当しないから，同社による個人情報保護法違反の事実は認められないと報告している[31]。

しかし，このような考えをとると，①行動ターゲティング広告において収集されるcookieなどの情報は，個人識別性を持たないから，個人情報保護法上は，利用者に無断で全く関係のない第三者に売却しても構わないということになってしまう[32]が，これらの情報は，個人情報該当性が明確な情報と同様，適正に取扱いがなされなければ，個人の権利利益に重大な悪影響を及ぼすおそれがある。

そもそも，個人情報保護法は，個人情報を取り扱う事業者が遵守すべき義務等を定めることにより，個人の権利利益を保護することを目的としたものである（同法第１条)。したがって，これらの情報についても個人情報保護法の規制対象として適切な取扱いを確保することにより，個人の権利履歴を保護すべきである。

また，現行法の個人情報の定義が不明確であることは，誠実な事業者にとっては

30　総務省，経済産業省，内閣官房では，スマートフォンの普及やビッグデータビジネスの進展などの，個人情報保護法制定以降の個人情報の利用状況の変化を踏まえ，研究会等を開催して報告書や指針等を作成している。これらの報告書等における個人情報又は保護されるべきパーソナルデータの考え方に対する意見は，後記第４の２にて詳しく述べる。

31　ミログ第三者委員会報告44頁

32　このような考え方をとる限り，情報売却行為等がユーザーのプライバシー権を侵害するとしても，不法行為に基づく訴訟により対応するほかなくなり，個人のプライバシー権等を保護するために事前に情報の適正な取扱いを定めた個人情報保護法の趣旨に反することとなる。

パーソナルデータの活用を萎縮させ，不誠実な事業者にとってはパーソナルデータの違法な取扱いを助長する結果となってしまっており，事業者の予測可能性及び公平性という観点からも問題である。

イ　海外事業者に対する規制が困難である

また個人情報保護法は，原則として，国内事業者に対する規制法であるため，海外事業者が海外に所在するサーバ等でビッグデータを取り扱う場合に，個人情報保護法による解決が困難である。しかし，パーソナルデータが，海外に即時に送信され，海外に所在するサーバで管理されることは，通常想定される事態である。国内事業者のみならず，海外事業者による不適切な情報の取扱いについても，事前規制，そして消費者への救済が必要である。

（2）不法行為法による解決における問題点

パーソナルデータの流出は，個人情報保護法による規制のほか，プライバシー権侵害に当たるとして不法行為（民法 709 条）を根拠とする解決も可能ではある（不法行為法による解決)。しかし，不法行為法による救済は，原則として金銭賠償による事後救済であり，差止めなどの事前救済が認められることは困難である。しかし，情報は一度知られてしまうと忘れられるのに時間を要する場合も多く，また，（特にインターネットにおいては）複製が容易であるため，一度流出してしまうと回収するのは不可能に近い。したがって，被害が発生してからの事後的救済のみでは，消費者に対する保護は不十分であると言わざるを得ない。

また，プライバシー権についても，判例上，明確な定義・要件が確立されていない[33]ため，パーソナルデータを利用する事業者側の立場からみても，どのような行為がプライバシー権侵害に該当するのかがわかりづらい。そのため，事後的救済のみという状況は，プライバシー権に対し適切な配慮をしたいと考えている事業者に対する予測可能性を欠くという観点からも問題である。

４　取扱いの不透明性の問題

個人情報保護法は，個人の権利利益を保護するために，事業者による個人情報の適正な取扱いを定めるものであるが，何をもって「適正な取扱い」といえるかも不明確である。この点，海外では，「公開性」「透明性」[34]を重視している例も一般的に見

---

[33] プライバシー権侵害については，宴のあと事件（東京地判昭和 39 年 9 月 28 日判時 385 号 12 頁）で示された 3 要件（私生活上の事実，非公開への期待，非公知性）が裁判例・判例において概ね踏襲されてはいるものの，宴のあと事件は，私生活に関する事実が公開された場合を巡る事件であり，3 要件がプライバシー権侵害全般，特にビッグデータにおけるプライバシー権侵害に当てはまるかどうかは不明である。また宴のあと事件も，最高裁判例も，プライバシー権に対する定義については明示していない。

[34] OECD プライバシーガイドラインでは「公開性」を原則のひとつとして掲げており，米国消費者プライバシー権利憲章においては「透明性」を消費者の権利として，APEC プライバシーフレームワークでは「通知」

られるところである。しかし，以下で述べるとおり，わが国におけるパーソナルデータを巡る現状では，パーソナルデータが具体的にどのように取り扱われているのかという点に関する透明性が極めて乏しく問題であると考えられる。

（1） 適正取得

上述したとおり，③「……the Movie」では，形式上は，アプリのダウンロード時に利用者からの許可を取得している。しかし，通常の利用者としては，あくまで人気ゲームの動画紹介やミニゲームの提供を行っているアプリだと思ってダウンロードしており，その限度での（例えば広告表示のための）アクセスを許可する意図しかなく，外部のサーバにパーソナルデータが送信され勝手に利用されることは想定していないと考えられる。

③「……the Movie」にとどまらず，現状では，パーソナルデータの取得の際に，形式上は利用者の同意を取得するものの，その利用についての説明が不十分なサービスが多数見受けられる。しかし，利用者としては，パーソナルデータが具体的にどのような目的で，どのように利用されるのかを十分に認識しないまま同意している場合も多く，不適正な方法による情報取得を規制している個人情報保護法の趣旨と反する事態になっていると考えられる。利用者が想定していないような方法・目的でパーソナルデータを収集・利用することは，利用者に対する不意打ちであり，プライバシー権を侵害するおそれがある。そのため，個人情報保護法第 17 条にいう「偽りその他不正の手段」にはあたらない方法であっても，利用者から見て不透明な取得が行われる場合を厳しく規制し，パーソナルデータの取扱いを巡る透明性を高めていくべきである。

（2）提供制限

個人情報保護法上，本人の同意なく，第三者に対する個人データの提供が認められる場合は極めて限定されており，具体的には以下の 5 類型に限定される。

（ⅰ）法令等（第 23 条第 1 項各号）
（ⅱ）オプトアウト（同条第 2 項）
（ⅲ）委託（同条第 4 項第 1 号）
（ⅳ）事業承継（同項第 2 号）
（ⅴ）共同利用（同項第 3 号）

しかし，現状を見ると，この提供制限の趣旨に背き，非常に広範な事業者間で多様な情報をやりとりしている状況が見受けられる。

上述の①行動ターゲティング広告や②共通ポイントサービスでは，サービス参加企業間で利用者のパーソナルデータの提供を行っていると考えられるが，これらのサー

を原則のひとつとして掲げている。

ビスでは，本人の同意，オプトアウト又は共同利用を根拠として，パーソナルデータの提供を行っているものと考えられる。

例えば②T ポイントサービスでは，規約上，利用者がポイントサービスを利用するに当たり，T ポイント用の ID を入力するか又はＴカードを提示しさえすれば，利用者は，CCC と参加企業間で自己の個人情報が提供されることに同意したとみなすものとされており（T 会員規約第 4 条第 5 項），参加企業間の個人情報の提供は，本人の同意に基づき適法になると考えているものと思われる。またＴポイントサービスでは，これに加えて，参加企業を共同利用者として規約上に掲げており（T 会員規約第 4 条第 4 項），共同利用によっても，個人情報の提供が適法になると考えているものと思われる。

ア　同意構成の問題点

しかし，同意構成には，以下のような問題点がある。

すなわち，まず，利用者がサービスの利用開始時に自己のパーソナルデータの提供に同意したと考えるのは無理がある。なぜなら，サービスの利用開始時には，当該サービスにおいて自己のパーソナルデータが具体的に誰に提供されどのように利用されるのか十分な説明がなく，利用者はサービスを利用したいがために，（「同意」ボタンをクリックするなどの方法により）形式的に同意しているに過ぎない場合が多い。この形式的・反射的同意をもって，利用者が自己のパーソナルデータの提供に真摯に同意したと考えるのは困難である。例えば，上述の②T ポイントサービスでは，規約で個人情報の利用目的として，「会員のライフスタイル分析のため」や「会員に対して，電子メールを含む各種通知手段によって，会員のライフスタイル分析をもとに，または当社が適切と判断した企業のさまざまな商品情報やサービス情報その他の営業案内または情報提供のため」と定めるが，「ライフスタイル分析」という抽象的な目的で，具体的にどのようなパーソナルデータがどのように利用されるのか把握・理解することは不可能である。そのため，CCC 側が同意構成により提供制限の例外に該当すると考えていたとしても，通常の利用者は，T ポイントサービスの仕組みや自身のパーソナルデータがどこまで提供されるかを十分に理解しないまま，T ポイントサービスを利用しているものと考えられる。

また，個別のサービス利用時に，同意を行っていると考えるのも困難である。例えば②T ポイントサービスでは，利用者は，商品の購入又はサービスの利用をする際に T カードの提示を行うが，利用者の多くは，その時点においてですら，T ポイントサービスの仕組み自体を理解していないと考えられるからである。すなわち,利用者の多くは，T ポイントサービスを利用することで誰と誰の間で，自己のどのようなパーソナルデータが提供されるのかを理解しておらず，そのような利

用者が T カードを提示したからといって，パーソナルデータの提供に関する真摯な同意があるとは考えられない。

しかし，現状の規制では，何をもって利用者の同意を得たと認められるのかが極めて曖昧である。そのため，利用者の形式的・反射的な「同意」をもって，パーソナルデータの提供が可能であるとも解釈されうる現状となっており，問題がある。少なくとも，利用者の同意を得たと認められるには，サービスの仕組みや規約について十分な説明が行われることが必要であろう。そしてこの問題は，②共通ポイントサービスのみでなく，①行動ターゲティング広告においても同様である。

イ　オプトアウト構成の問題点

オプトアウト構成においても類似の問題がある。事業者が利用者に対し，何を行えばオプトアウトできるのかをわかりやすく示していない現状がある。形式上は，利用者のオプトアウト権を保障しているかのように見えても，実質的に利用者がオプトアウト権を行使することが困難な現状があり，本人に拒否の選択権を与えるという法の趣旨に反する状況が生じている。

ウ　共同利用構成の問題点

共同利用構成においては，法が求める共同利用の要件が満たされていないにもかかわらず，パーソナルデータが提供されている場合があるものと考えられる。すなわち，個人情報保護法上，共同利用構成をとる場合は，共同利用者の範囲を「特定の者」とし，共同利用者の範囲をあらかじめ本人に通知するか，又は本人が容易に知り得る状態に置くことが必要である（同法第 23 条第 4 項第 3 号)。しかし，①行動ターゲティング広告を行うためにパーソナルデータを共有する場合や，②共通ポイントサービスのためにパーソナルデータを共有する場合は，絶えず加盟企業が増減するため，誰が共同利用者に含まれるかが一定せず，本人がサービスを開始した時に共同利用者であった事業者と，本人のパーソナルデータが提供される際に共同利用者である事業者が必ずしも一致しないことも十分考えられる。これでは，本人から見て誰の間で自己のパーソナルデータが提供されるのかがわからず，共同利用者の範囲が特定されていないとも考えられる。

この点，経済産業省のガイドラインでは，共同利用者の範囲として，「本人からみてその範囲が明確であることを要するが，範囲が明確である限りは，必ずしも個別列挙が必要ない場合もある」旨を定めており，「最新の共同利用者のリストを本人が容易に知り得る状態に置いているとき」は共同利用の要件を満たす旨が記載されている（同ガイドライン 45 頁)。これを踏まえると，①行動ターゲティング広告や②共通ポイントサービスにおいても，ホームページ上で，加盟企業一覧が公表されていれば，共同利用の要件を満たすとも考えられ，現に事業者においてはそのような理解がなされているとも考えられる。

しかし，個人情報保護法上，本人の同意なく，個人データの提供が認められる場合は極めて限定されており，上述のとおり，（ⅰ）法令等，（ⅱ）オプトアウト，（ⅲ）委託，（ⅳ）事業承継，（ⅴ）共同利用の場合に限られる。

（ⅰ）法令等，（ⅲ）委託，（ⅳ）事業承継は，個人データを提供する必要性が類型的に考えられるために，本人同意が不要とされていると考えられるが，このような類型外であっても，（ⅱ）オプトアウト，（ⅴ）共同利用に該当すれば，個人情報保護法上，本人の同意がなくとも，個人データの提供が認められる。そのため（ⅱ）オプトアウトでは，本人同意に代わるものとして，オプトアウトという本人参加の機会を保障しているものと考えられる。これに対し（ⅴ）共同利用では，（ⅰ）法令等，（ⅲ）委託，（ⅳ）事業承継のように個人データを提供する必要性が類型的に考えられない上に，提供先の監督義務や本人参加の機会の保障すら存在していない。そのため現状では，（ⅱ）オプトアウトよりも（ⅴ）共同利用の方が，利用者に拒否権を与えない簡易な手段であるため，事業者が（ⅱ）オプトアウトよりも（ⅴ）共同利用構成をとる場合も見受けられ，（ⅴ）共同利用は（ⅱ）オプトアウトを脱法化する形態としても利用されていると考えられる。

しかし，（ⅰ）法令等，（ⅲ）委託，（ⅳ）事業承継のように個人データを提供する必要性が類型的に考えられず，かつ（ⅱ）オプトアウトのように本人参加の機会の保障すらない（ⅴ）共同利用において，（ⅴ）共同利用に該当するための要件は厳格に解すべきであり，本人にとって誰が共同利用者であるかが明確にわからない場合には，（ⅴ）共同利用に該当すると解するべきではない。

この点，ホームページ上で最新の共同利用者のリストが公表されていたとしても，本人からすれば，現在公表されている共同利用者間で自己のパーソナルデータが共有されているとは限らない。提供がなされた時点において共同利用者であった者の間で本人のパーソナルデータが共有されるわけであるが，本人にとってはいつ自己のパーソナルデータが提供されているかがわからず，結局，誰が自己のパーソナルデータを共有しているかもわからないこととなる。したがって，このような場合に，個人情報保護法の共同利用の要件を満たしていると考えるべきではない。

５　本人参加・救済における問題

プライバシー情報，個人情報，パーソナルデータその他個人に関する情報の取扱いに対する規制の最終目標は，個人に被害を及ぼさないことである。個人情報保護法はそのために情報の適正な取扱いを定め，不法行為法は被害を被った個人の救済を図る。しかし，日本のパーソナルデータを巡る現状では，パーソナルデータについて不適切な取扱いがなされているときに消費者が救済を得る方法が，極めて限定されており，消費者被害の予防や救済にとって十分とはいえない。

（１）個人情報保護法上の本人参加・救済における問題点

個人情報保護法では，開示請求，訂正請求，利用停止請求について規定が設けられているが，裁判上はこれらの規定に基づき開示，訂正，利用停止を請求することはできないとの東京地裁の裁判例（東京地判平成 19 年 6 月 27 日判時 1978 号 27 頁）も存在しており，現実的には，個人情報保護法に基づく救済を得られる方法が極めて限定されている。

さらに言えば，いったんパーソナルデータが流出してしまった場合，上記各規定では被害の拡大防止や早期回復を行うことは実質的に不可能である。

（２）不法行為責任追及による救済の問題点

したがって，いったんパーソナルデータが流出してしまった場合に個人が救済を得るには，結局のところ不法行為法による解決に頼ることとなる。しかしながら，上記第３の３（２）で述べたとおり，不法行為法による解決は，すでに生じた被害を金銭的に賠償するのみであり，流出した情報の回収・削除は不可能である。さらに，過去の事例でも，わが国の司法を通じた被害回復を行うにあたっても，実害がある場合を除き，被害者に認められる賠償額が極めて少額となっているため[35]，被害を受けた一般消費者が個々の被害回復を求めて，パーソナルデータを流出させた企業に対し訴訟提起をすることは，事実上困難である。加えて，流出した情報には，極めてセンシティブな情報が含まれている場合もあるため，公開の裁判手続の利用を躊躇する被害者も多い。そのため，ビッグデータ化したパーソナルデータの流出事故に対しては，ほとんどの被害者が司法の場に救済を求めず，「泣き寝入り」をしているのが現状である[36]。

このような状況は，わが国特有の司法に対するアクセスの困難性が原因である。

上記で上げた例で見れば，ソニー・コンピュータエンタテインメントによる顧客情報の不正流出事件に関連する訴訟は，アメリカ合衆国では同年 7 月 21 日時点で 55 件の裁判が提訴されているが[37]，公表されている限りわが国ではそのような報告は一例もない。このような状況からすれば，わが国の現行の民事訴訟制度がパーソナルデータ流出事件の被害の実態に則した利便性を有していないことは明らかであろう。

このような実態は，「被害の公平な分担」というわが国の不法行為法の理論から乖離した不当なものであるため，制度自体を見直す必要性が高い。

---

[35] 司法により認められた一人あたりの賠償額は，宇治市住民情報流出事件では 1 万 5000 円，ヤフーBB 事件では 1 万 2000 円であり，センシティブ情報が流出した TBC 事件でも 3 万 5000 円にとどまる。

[36] TBC 顧客情報流出事件では，5 万件のプライバシー情報が流出したにもかかわらず，原告はわずか 14 名であった。http://homepage3.nifty.com/tbc-higai/

[37] ロイター通信 2011 年 7 月 21 日報道。これらの訴訟は保険会社に対する訴訟も含む。
http://www.reuters.com/article/2011/07/21/insurance-sony-idUSN1E76K0V920110721

６　小括

このように，ビッグデータに関する現行の規制は，いずれも要件が曖昧であったり，規制が不十分であったり，実効性を欠くものである。このままでは，消費者が知らない間に，又は予想できないような方法でパーソナルデータが利用・提供されるおそれも強く，その場合の被害は甚大である。また，消費者がパーソナルデータの流出をおそれるあまり，同意を求められても過剰に反応したりするなど，気軽に新しいサービス・アプリ等を利用できなくなり，サービス・アプリの円滑な利用も妨げられることが考えられる。

事業者にとっても，そのような消費者の利用を控える態度が顕著になれば新規事業に不利益であるし，またそうでなくとも同意の有効性や情報の適正な取扱いについての予測可能性を欠けば，突然新規事業が違法となったり，パーソナルデータを勝手に利用しているなどの批判を受けたりする可能性もあり，ビッグデータに関する新規事業に躊躇する事態となってしまう。

そこで，消費者にとっても事業者にとっても，パーソナルデータの利用に関して実効性のある明確な規制をする必要がある。

また，ビッグデータ化したパーソナルデータの流出に関する事後的救済手段についても，通常の民事訴訟手続では不十分であり，被害者が多数に上るが個々の被害は少額であるというパーソナルデータの流出被害の特殊性に見合った，効率性の高い救済手続の整備が急務である。

第４　意見の具体的内容とその合理性

以上述べたとおり，ビッグデータに関する現行の規制には，運用・執行における問題，規制範囲の問題，取扱いの不透明性の問題，本人参加・救済における問題がある。これらの問題を解決するために，政府は，機関の一元化（後述「１」），規制範囲の適正化（後述「２」），取扱いの透明化（後述「３」），本人参加の権利の保障を行い，かつ救済の実効性を高める（後述「４」）よう，以下に記載する施策を講じるべきである。

１　機関の一元化

（１）法所管と執行を一つの機関に集約すべき

そもそも，現状の問題が生じている一番の原因は，法所管官庁と執行権限を有する官庁が分離されていて，統一的かつ実効的な行動がとりづらくなっている点にある。これら各官庁に分散された権限を一つの機関に集約し，統一的な法解釈を行い，迅速な執行を行うべきである。また，個人情報保護法のみでなく，行政機関の保有する個人情報の保護に関する法律，独立行政法人等の保有する個人情報の保護に関する法律，地方公共団体における個人情報保護についても，一つの機関にて法所管し，各種権限を行使すべきであろう。

そしてかかる一元化された所管官庁において，上述した，利用目的が特定されていないケース，不適正取得制限に違反しているケースなど，個人情報保護法に違反している事案に対して，厳格な指導・勧告を行い，監督権を適正に行使すべきである。

なお，EU を始めとする各国へのデータ移転を考えると，上記一元化された所管官庁は，独立した機関であることが求められる。この点，行政手続における特定の個人を識別するための番号の利用等に関する法律（いわゆる番号法）に基づき設立される，特定個人情報保護委員会の所掌事務を拡大し，個人情報全般についても所管させることが考えられる。

また，特定個人情報保護委員会は，番号法上，方針・指針の作成，啓発，報告徴収，立入調査，助言指導，勧告命令，措置要求，内閣総理大臣への意見具申などを行う権限が担保され，法執行に際し，一定の権限が付与されていると考えられる。特定個人情報保護委員会の所掌事務を個人情報保護全般に拡大する場合も，引き続きこれらの権限を付与すべきである。一方で，特定個人情報保護委員会には，紛争解決，不服申立てへの対応（審査請求）などの権限が与えられていない。プライバシー権侵害事案は被害額が少額である場合も多く，個人が訴訟により救済を得ることは，訴訟に要する費用に鑑み，困難な場合も多い。少額大量の被害にも迅速な救済を図るよう，特定個人情報保護委員会に，紛争解決，審査請求などの権限を付与すべきである。

さらに，個人情報全般について実効的かつ迅速な執行・法解釈を可能とするためには，特定個人情報保護委員会の所掌事務を単に拡大するだけでは足りず，特定個人情報保護委員会に十分な予算・人員・権限を確保する必要がある。特定個人情報保護委員会の所掌を拡大すればプライバシーを巡る問題がすべて解決するような言説も見受けられるが，特定個人情報保護委員会を設立する目的は国民の権利利益の保護であり，それを実現できるような権限・予算・人員がなければ，新たな行政機関の設立は全くの無駄である。国民の権利利益を保護するという目的を実現するために十分な権限・予算・人員を確保することを強く要請する。行政改革が強く叫ばれる中，予算や公務員数の削減が求められることは理解できるが，行政改革というのは，ただ単に予算や定数を削減すれば済むものではない。現在の行政機関は，査定当局による査定が多数ありすぎて，実際に生じている問題に対して迅速な行動をとることが難しい状況にある。公務員の定数削減，給与削減，予算削減を目的とする行政改革ではなく，実際の問題を迅速に解決できるような行政の在り方を目指す行政改革を行うべきであり，迅速な対応を妨げている現状にそぐわない査定のあり方自体も早急に見直すべきである。この点はパーソナルデータの保護に特有の話ではないが，パーソナルデータの保護を専門的にチェックする機関という今までにない組織を構築する以上，従前までの行政のあり

方では，迅速・的確・専門的な対処は行えないため，強く要請する。

（2）基本ガイドラインの作成

各主務官庁によって作成された 40 本のガイドラインについて，政府では，平成 20 年 7 月 25 日より共通化に向けた取り組みを行っているが，平成 22 年 3 月 31 日現在，ほぼ進捗が見られない[38]。また共通化に向けた取り組みと謳ってはいるものの，実際は，形式・名称・用語の統一等を行うだけであり[39]，これらの対策を行ったところでガイドラインの乱立という問題は全く解消されない。まず基本ガイドラインを 1 本策定した上で，個別事業分野ごとにさらなる特別対応が必要な場合は，その旨を特記した形とすべきである。個別事業分野ごとの特別対応についても，主務官庁の単管とせずに，上記第 4 の 1（1）に記載した一元化機関との共管とするか，又は主務官庁側の意見を聴取しながら最終的には一元化機関が策定する形をとるなどして，法解釈・法執行の統一化・実効性確保を図るべきである。

（3）研究会の統合

経済産業省や総務省で設置している研究会等についても，同様のテーマについて複数の研究会を乱立させることをせずに，政府全体でパーソナルデータの保護のための統一的な行動をとるようにしなければならない。この点，行政機関側は，各府省で複数の研究会を乱立させていても，「ビッグデータビジネスの振興のため」，「電気通信事業の適正な進展のため」，「消費者保護のため」とそれぞれ研究会等の目的・趣旨を異にするので，それぞれ必要であると主張することが考えられる。また，関係省庁で連絡を密にとっており政府全体の統一性に配慮していると主張することも考えられる。しかし，本当に趣旨を異にするならともかく，「ビッグデータビジネスを巡るビジネスの振興と利用者の保護」という共通の目標を達成するために，いくつもの研究会等を同時並行的に開催するのは非効率的であるし，事業者や消費者から見てもどの研究会等の報告書に依拠すればよいのかが極めてわかりにくい。省益にとらわれず，真にビジネスの振興と利用者の保護の調和を図る検討を行うべきである。上記一元化機関設立後は，一元化機関にて検討を行い，その他の各府省庁では原則として研究会を立ち上げないようにすべきである。

（4）民法（不法行為法）への対応

また，上記一元化機関では，個人情報保護法のみを所管するのではなく，プラ

---

[38] http://www.caa.go.jp/seikatsu/kojin/gaidorain.pdf で取り組みの状況を公表しているが，多くのガイドラインが「検討中」の状況である。また平成 22 年 3 月 31 日以来，状況の更新もなされていない。

[39] http://www.caa.go.jp/seikatsu/kojin/gaidorainkentou/kyoutuuka2.pdf

イバシー権侵害による不法行為に係る問題についても取り扱うべきである。不法行為はその性質上，事前に明確な定義・要件を確立することは困難である。そこで，たとえば Q&A や事例集を公表したり，事前照会に迅速に対応するなど，きめ細やかな対応を行う必要がある。

２　規制範囲の適正化

（１）個人情報の定義

前述したとおり，氏名等が含まれないビッグデータは個人情報に該当しないと解釈する事業者も見受けられるところであるが，氏名等が含まれないビッグデータについても適切な取扱いを行わなければ，消費者の権利利益を侵害する危険性がある。

ア　端末識別情報に対する保護の必要性

そのため，個人情報保護法上の個人情報の定義を，端末識別情報等を含める形で拡大するべきである。この点，高度情報通信ネットワーク社会推進戦略本部（IT 総合戦略本部）にて 2013 年 12 月に公表された「パーソナルデータの利活用に関する制度見直し方針（案）」でも，法律上保護されるべきパーソナルデータの範囲を拡大する方向が示されており[40]，評価できる。しかし同方針（案）では，拡大の方向性について詳細は述べられておらず，総務省が 2013 年 6 月に公表した「パーソナルデータの利用・流通に関する研究会報告書」を基にして検討を行うものとも考えられる。

「パーソナルデータの利用・流通に関する研究会報告書」では，保護すべきパーソナルデータとして，個人の PC やスマートフォン等の識別情報（端末 ID 等）については，「一義的には PC やスマートフォンといった特定の装置を識別するものであるが，実質的に特定の個人と継続的に結びついており，（中略）保護されるパーソナルデータの範囲に含まれると考えられる」と整理している[41]一方で，IP アドレスや cookie については，「必ずしも全ての場合に継続的に特定の装置を識別するものではなく，一般的には，他の保護されるパーソナルデータと連結する形で取得・利用される場合に（中略）保護されるパーソナルデータの範囲に含まれると整理されるべきもの」と整理している[42]。

確かに cookie は利用者側で削除等が可能であり，cookie と個人との結びつきを理念的に考えれば，cookie が個人情報ないし保護されるべきパーソナルデータに該当しないと解しうることも理解はできる。しかし現実的に考えれば，cookie の

40　同方針（案）4 頁（http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou3-1.pdf）

41　同報告書 25 頁（http://www.soumu.go.jp/main_content/000231357.pdf）

42　同報告書 25 頁

仕組みを理解していない，理解していたとしてもcookieを削除等しないユーザーも多く，またインターネットを介してパーソナルデータを収集する場合は，端末ID等の識別情報だけでなく，cookieやIPアドレスによって特定の端末を識別する場合も多い。したがって，cookie等も個人情報ないし保護されるべきパーソナルデータに原則として含めた上で，一定の要件を充たし個人との結びつきが一定以上弱まったと評価できる場合にのみ，例外的に保護の対象外とすべきである[43]。

イ　プライバシー性による要保護度の相違

さらに，「パーソナルデータの利用・流通に関する研究会報告書」では，パーソナルデータをプライバシー性の高低により①一般パーソナルデータ，②慎重な取扱いが求められるパーソナルデータ，③センシティブデータの３類型に分類することを提唱している。

個人情報保護法施行以来，プライバシー性の極めて低い個人情報であっても，ひとたび漏えいすれば，「個人情報の漏えい事故」として大体的に報道され，個人情報取扱事業者に該当しない一般個人であっても個人情報保護法を理由として提供等を拒否することもあり，個人情報に対するいわゆる過剰反応も見られるところである。その一方で，位置情報や購買履歴等のプライバシー性が一定程度高いパーソナルデータが個人情報保護法の対象外と誤解されている等，個人情報保護法の適用範囲及び規制内容とプライバシー権の解釈との間に齟齬があるものと考えることもできる。したがって，プライバシー性の高低によって法律上の類型を設ける考え方については理解できる。

しかし，非センシティブ情報であっても組み合わされることでセンシティブな情報が分析されることもあり（第２の２（１）イ参照），適切な分類・定義づけが可能か、疑問がある。また海外法制を見ても，個人情報の万全な分類・定義は困難であると考えられることから，上記一元化機関が定期的に規制類型・規制範囲の見直しを行い，かつ個別事例に対し統一的な解釈を適時に提示していくべきである。例えば，総務省「パーソナルデータの利用・流通に関する研究会報告書」では，継続的に収集される購買・貸出履歴，視聴履歴，位置情報等は，保護されるパーソナルデータの範囲に含むべきではないかとしているが，保護されるパーソナルデータの範囲は，これらに限定されるものではなく，さらなる検討が必要

43　なお，同報告書では，継続的に収集される購買履歴等を慎重な取扱いが求められるパーソナルデータに分類しているが，購買履歴等と紐づく識別キーがcookieであった場合に，保護されるか否かが明らかでない。cookie単体であれば保護されるべきパーソナルデータに該当しないが，購買履歴等が継続的に収集されると個人識別性を獲得する場合が多いことから，購買履歴等と紐づく識別キーがcookieであっても，保護されるべきパーソナルデータに該当すると考えているのか，それとも識別キーがcookieであれば継続的に収集される情報であっても保護されるべきパーソナルデータに該当しないと考えているのかが不明である。当会としては，仮に保護されるべきパーソナルデータに該当しない識別キーを用いている場合であっても，継続的に収集される情報は，保護されるべきパーソナルデータに該当すると解すべきと考える。

であるし，その範囲は時代の変化・技術の進化とともに急速に変化する可能性が高いため，範囲を一度画定すればそれで足りるものではない。プライバシー権の保護のためには，専門機関が定期的に規制範囲の見直しを行った上で，規制範囲を変更する，迅速な対応が不可欠であり，保護されるべきパーソナルデータの定義については，重要事項を法律上例示した上で，上記一元化機関の規則事項として委任するなど，上記機関の強力な関与が求められる。

ウ　保護されないパーソナルデータ

また，上記のように保護されるべきパーソナルデータの範囲を拡大したとしても，保護されるパーソナルデータの範囲から外れるパーソナルデータが生じてくる。しかしその場合であっても，個人情報保護法はあくまでパーソナルデータの取扱いに関する適正を確保するための規制法にすぎず，不適切な取扱いを行えば個人情報保護法の対象外であっても不法行為を構成しうることを，事業者に対し助言・指導していくべきである。

（２）海外事業者への規制

パーソナルデータは海外で取り扱われることも頻繁に想定されることから，個人情報保護法の適用範囲を整理すべきである。その際，①行為の一部が国内で行われれば個人情報保護法令を適用する属地主義を原則としつつ，②①では個人情報保護法の目的が十分に達成できない場合には効果主義（個人情報保護法令が保護しようとする法益に対する侵害の可能性がある場合には個人情報保護法令を適用する）を加味して適用範囲を拡大すべきであろう。

ただし，法の適用が可能な場合であっても，外国政府の同意がなければ，外国領土内で執行を行うことはできないため，個人情報保護の国際的潮流を理解し，各国のプライバシー・コミッショナーや法執行機関などと協力関係を築くことが必要である。したがって，一元化機関は，海外当局等との協力関係を築くよう努力すべきである。

３　取扱いの透明化

ビッグデータビジネスを行う事業者の中には，パーソナルデータを匿名化しさえすれば，個人情報に該当しなくなるので，匿名化さえ行えばプライバシー権を巡る全ての問題が解決するとの見解も存在するようである。しかし，一度匿名化した情報であっても，ほかの情報と結び付けて分析することで，誰の情報であるかが判明してしまったり，不十分な匿名化の結果，結局個人識別性が失われなかったりする場合も十分考えられる。そして，いくらパーソナルデータを匿名化したところで，消費者に対する個別マーケティングの場面では，消費者に対し直接 E

メールやダイレクトメールを送付したりするなど，個人識別性のある情報を扱わざるを得ない場合も多い。ビッグデータを分析した上で個別の消費者にマーケティングを行う場合，事業者は，パーソナルデータを通して分析した消費者の情報を了知した上で生身の消費者自身にコンタクトを取ることができることとなる。この場合，消費者が想定していないような情報を事業者に知られている可能性がある（上記のとおり，購買行動を分析した結果，事業者に妊娠の有無というセンシティブな情報を把握されることもある。）。

情報は，全体としてどう利用されどう取り扱われるかが重要であり，情報の取扱いの一局面をもって，情報が匿名化されているから規制の対象外とするというのでは意味がない。パーソナルデータを取り扱うどの過程においても，匿名化されたデータ以外取り扱わないとすることは実際上困難であり，匿名化しさえすればプライバシー権をめぐる問題のすべてが解決するわけではない。個人識別性を欠く匿名化情報は，規制の対象から除外するといった対応ではなく，結局，情報を誰がどのように取り扱うかを透明化し，情報の取扱いに係る全プロセスにおいて適切な取扱いを行っていく必要がある。

（1）同意のあり方

現状では，事業者は，個人情報に該当しなければ本人から同意を取得しなくてよいであるとか，個人情報に該当するが本人から形式的に同意を取得しさえすればよい，と考えているようにも見受けられる。しかしそうではなく，消費者が想定していない方法でパーソナルデータを取得したり利用したり提供するのではなく，消費者にとって透明性の高い情報の取扱いを行っていく必要がある。消費者の権利利益を保護できるような，適切な同意取得・同意撤回のあり方を早急に検討すべきである。

ア　コンテキストに沿った取扱い

この点，総務省「パーソナルデータの利用・流通に関する研究会報告書」では，取得の際の経緯（コンテキスト）に沿った取扱いか否かで，同意取得に係る要件を変更するなどの提言を行っている[44]。現在の個人情報保護法では，利用目的どおりの利用であれば，同意取得を不要としている（同法第１６条第１項）一方で，利用目的どおりの提供であっても第三者提供の例外とはされていない（同法第２３条）。

利用目的は保有者側が特定できるのに対し，取得の際のコンテキストであれば主観的ではなく客観的に特定されるものと考えられる。また消費者にとっても利用目的を明示的に確認せずとも，取得の際のコンテキストであれば想像しやすいものと考えられる。したがって，基本的には理解できる考え方であるが，コンテキストが

44　同報告書 28～29 頁

消費者にとって明確にわかりやすいものであること，そしてコンテキストが事業者によって恣意的に解釈されないことが重要であり，その点の要件を明確化すべきである。

イ　個人が特定される可能性を低減した個人データ

また，IT 総合戦略本部による「パーソナルデータの利活用に関する制度見直し方針（案)」では，パーソナルデータの利用・流通を促進するため，個人が特定される可能性を低減した個人データについて，情報受領者の義務を法定した上で，第三者提供における本人同意原則の例外とすることが提唱されている[45]。しかしその一方で，どのような要件を満たせば「個人が特定される可能性を低減した個人データ」に該当するか否かが明らかにされていない。

統計データのように完全に匿名化されたデータであれば，本人同意原則の例外とすることに異論はないが，個人が特定され，個人のプライバシー権が侵害されるおそれのあるデータであれば，本人同意原則の例外とするべきではない。

（3）オプトアウト，共同利用の要件の厳格化

現状のオプトアウトの状況を見ると，プライバシーポリシー等において，オプトアウトできる旨，そしてオプトアウトの方法について，細かい文字でわかりにくい説明が行われているにすぎず，消費者のオプトアウト権が実質的に保障されているとはいえない。オプトアウトを一定の範囲で認めるとしても，オプトアウトできること，そしてオプトアウトの方法について，消費者が容易に理解できるような方法で具体的に表示させるよう指導・勧告を行うか，個人情報保護法を改正し，事業者により厳格な義務を課すべきである。

さらにいえば，現行の個人情報保護法では，あらゆる情報についてオプトアウトの措置をとることにより提供制限の例外とすることを認めているが，センシティブ情報についてはオプトアウトによる提供制限の例外を認めるべきではない。またセンシティブとはいえない情報についても，前述の通り，単純な購買行動を解析することで女性客の妊娠が分析できるように，センシティブでない情報が集約されてビッグデータ化することでセンシティブな属性等が分析されてしまうこともある。オプトアウトを認めるべき場合を精査し，限定された場合以外は，オプトイン，つまり消費者の同意がなければ提供制限の例外とできないよう，法改正すべきである。

また，共同利用については，現状の運用では違法であることを確認し，法が本来予定していた共同利用についてのみ認めるようにすべきである。具体的には，どのような共同利用の類型であれば認められるのか，共同利用に際しての消費者

45　同方針（案）2 頁

保護はどうあるべきかを早急に検討した上で，事業者に対し助言・指導していくべきである。さらにいえば，個人情報保護法を改正し，検討された結果を共同利用の条文に反映させ，認められる共同利用の要件を厳格に明示すべきである。

（４）同意取得文言等の保存・開示義務

上記（１），（２），（３）の問題について，政府が適切な要件や方法を明示していくべきであると考えられるが，それだけにとどまらず，プライバシーポリシーや同意取得文言等を保存・開示する義務を事業者に課すべきである。

昨今のサービスでは Web サイト上で説明が完結する場合も多い。Web サイト上の文言は，事業者が容易に変更できる上に，消費者が能動的にアクションをとらなければ消費者の手元に残らないという特徴がある。そのため事業者がプライバシーポリシーや同意取得文言，利用規約等を次々に変更した場合，消費者にしてみれば，消費者が契約した時点ないし同意した時点における事業者の説明ぶりを後から確認することが難しい状況にある。事業者が適切に説明を行っていること，消費者を欺いていないことを証明するためにも，事業者に記録の保存義務を課した上で，消費者による開示請求に迅速に対応すべき義務を課すなどの対応が必要であろう。

（５）事業者に対する個人情報の取扱い状況明示の義務付け

また上記（１）から（４）といった個別の問題にとどまらず，そもそも現状のままでは，消費者は，パーソナルデータを提供する際に，自己のパーソナルデータがどのように使用され，提供されるのかがわからない状況に置かれている。そのため，消費者は，自己のプライバシー権を守るという観点からサービスを選択することができない。したがって，個人情報保護法を改正し，パーソナルデータを取り扱う事業者に対して，どのような情報をどのように取り扱うのかを具体的に消費者に対して説明する義務や，パーソナルデータの取扱いに関する規約の作成義務を新設することが必要である。

４　本人参加の権利の保障・救済

（１）開示，訂正，利用停止権の明確化による権利保障の強化

繰り返すが，情報の取扱いに対する規制の目的は，個人の権利利益を保護することである。そこで，情報が取り扱われることによって個人に被害が生じないよう，個人が情報の取扱いに関与する機会を保障し，また、個人に迅速かつ簡便な方法による救済を与える必要がある。具体的には，開示，訂正，利用停止請求は，消費者が自己の個人情報の取扱いに関与できる機会を保障するものとして，重要な権利であるので，上述した東京地裁の裁判例のように，これらの請求権が裁判上の請求権たりえないとの解釈を事業者が取ることがないよう，これらの請求権

が裁判上の請求権たりえるものであることを明確化する法改正を行うとともに，行政庁もそのように解釈していることを明確化すべきである。

また現状では，個人が権利救済を受ける手段が，個人情報保護法の開示，訂正，利用停止請求以外は，不法行為による損害賠償請求などの訴訟によるものとなってしまっている。より本質的な問題解決として，紛争解決に関わる権限を上記一元化機関に与えるなどして，消費者の迅速な救済を図るべきである。

（２）効率性の高い事後的救済手続「クラスアクション」制度の導入

また，個人情報の大量流出事件の被害の実態に則した事後的救済制度として，被害者が多数に上る少額被害を集約して解決するために，民事訴訟手続についても改正を行い，一部の被害者による訴訟追行の結果としての判決効が被害者全体に及ぶクラスアクション制度を導入すべきである。

近時，「消費者の財産的被害の集団的な回復のための民事の裁判手続の特例に関する法律」が成立したが，同法に基づく集団的消費者被害回復制度は，原告となりうる者が「特定適格消費者団体」に限られ（同法第３条），被害者自身が原告のみならず利害関係人として参加となることも禁じているなど（同法第８条），当事者主義，直接主義という裁判手続の大原則に反するおそれのある制度であって，制度自体に問題がある。さらに，同法では，不法行為に基づく慰謝料については訴訟提起を行うことができず（同法第３条２項６号），結局のところ，プライバシー権侵害の被害を救済するためにも利用できないものである。

したがって，パーソナルデータの適正な利用とプライバシー保護の調和を図るためには，予防措置としての個人情報保護法の改正とその適切な執行のみならず，消費者の適切な被害救済を図り，併せて事業者に対する遵法意識の向上を行うためにも，（少額であることが多い）多数の被害者の被害救済のために有用なクラスアクション制度を導入するべきである[46]。

第５　まとめ

以上述べたとおり，ビッグデータと化し，オンライン・オフラインを問わず流通・氾濫しているパーソナルデータの「保護」と「利用」の適切なバランスを，現行の法規制及び法執行で達成することは，著しく困難である。実際，パーソナルデータのビッグデータ化への対応は，すでに欧米を始めとする先進諸国ではすでに行われており，わが国においても法規制及び行政機関の改善が急務である。

本意見において行われた諸提案は，現行法規制に対する最小限の改善によって最大の効果をもたらすものであると確信している。したがって，貴庁及び関係各省庁にお

[46] クラスアクション制度については，日本弁護士連合会・京都弁護士会作成の「アメリカ合衆国クラスアクション調査報告書（2007 年 12 月）」日本弁護士連合会「カナダにおけるクラスアクションの実情調査報告書～ブリティッシュコロンビア州における実務を中心として～」が詳しい。また，消費者庁でも調査が行われている。

かれては，これらの案を積極的に採用されたく意見するものである。

以上