

パーソナルデータ検討会へのご提案

アジアインターネット日本連盟
(AICJ, Asia Internet Coalition Japan)

2014年5月20日

アジアインターネット日本連盟とは

アジアインターネット日本連盟は、インターネット産業の健全かつ持続的な成長に資する政策や制度のあり方等について、インターネット事業の一翼を担う産業界からの声を適切に届け、国民の議論を喚起していくことを目的に、2013年9月に設立されました。

設立以来、インターネット政策について提言・理解促進活動・調査研究等を行っております。

会員社は、アマゾン ジャパン株式会社、eBay Inc.、グーグル株式会社、グリー株式会社、株式会社ディー・エヌ・エー、フェイスブック、ヤフー株式会社、です。

本資料の内容

総論

- 制度見直しの検討の在り方に対する要望
- ビッグデータ時代におけるプライバシー保護の在り方

各論

- 個別の論点に対する意見

ルール形成がデータ利活用促進につながるというが

ルールには
2つの方向
性がある

- ・データ利活用を促進するルール
- ・データ利活用を制限するルール

前回会合までの議論の状況を見ていると、インターネットビジネスの企業からすると、データを使いにくくするルールに見える。

【制度見直しの検討の在り方に対する要望】

(1) 行政規制としての立法事実

世界最先端IT国家創造宣言(平成25年6月14日閣議決定)で宣言された

「ビッグデータの利活用による、付加価値を生み出す新事業・新サービス創出を強力に推進する」が今回の議論のきっかけ。

これからはデータ社会（既にパラダイムシフトは起き始めている）

個々人のニーズに合った製品やサービスを提供するためには、ユーザーのニーズを知る必要がある。

グローバルレベルでデータ主導型の新しいビジネスが多く出現し、そのベネフィットが享受されている。ご参考:シンガポールにおけるデータ主導型イノベーションの実例紹介を含めたりサーチ

<http://www.analysismason.com/Research/Content/Reports/Data-driven-innovation-in-Singapore/>

データ主導型のイノベーションとプライバシーの保護との両立も考えていく必要があるなかで、

「これまでの個人情報保護法の下で、具体的にどれほどの法益侵害が生じたことがあったのか」ということとの対比でどういった法改正が適切かを考えていく必要性あり。明確な立法事実は必要。

(2) 日本発のデータ主導型イノベーションが生まれるような制度を

十分な実態の把握なくして、適切なルールはつukれない。

※ 現在、最先端でビッグデータ利活用を行っているところのヒアリングをしなければ将来のビジネスに対する制約の懸念が見えてこない。ヒアリングにあたっては、このような5分という短い持ち時間では、総論の意見を述べるにとどまり、具体的な話はほとんどできない。

データ主導型の事業を活かすことで、単に事業者だけではなく、我が国の国民全体の発展が図られるという観点から、データの自由な流通に主眼を置くべき。そもそも事業者とユーザーの方々が対立する関係にあるわけではない。

海外の制度でできるビジネスで、日本の制度下にあるが故にできなくなるものが出てくれば、不利益を被るのは我が国の国民であるということにも十分留意していただきたい。

(3) グローバル競争で通用するルールを

日本市場におけるインターネットビジネスの競争は日本企業同士に限られない。

日本市場でビジネスをする日本企業と海外企業とで、データの取得・利用に関して同じ土俵に。

日本の制度を、世界でもっともデータの利活用がしやすい国の制度と同様にしなければ、我が国にデータは集まらない。世界でもっともデータの利活用がしやすい国に集まるだけ。

データ利活用による経済活性化、雇用促進及び市民生活の改善など、データ利活用により国民が享受するプラスの面に十分目を向けた検討を。

【ビッグデータ時代における プライバシー保護の在り方とは】

(1) 求められているのは、従来のプライバシー保護に関する
枠組みとは別の新たな枠組み

たとえば、以下のビジネスの可能性とこれによってユーザーが
享受する利益を無視してしまうことになってよいか

- ▶ お互いの持つデータを共有することにより、精度をあげてより良いサービスが作り上げられるという分野があるとした場合
- ▶ ビッグデータ解析をしているうちに、有用性の高い使い方を後から発見した場合

新たな時代におけるバランスのとれた枠組みを、いまこそ戦略的に考えていく必要が！

(2) 法規制よりも自主規制を

この分野は技術発展が著しいので硬直的な法規制よりも、自主規制をベースとして柔軟な対応を図ることが望ましい。

【個別の論点に対する意見】

- (1)「個人情報」の定義について
- (2)「準個人情報」について
- (3)「個人特定性低減データ」について
- (4)「機微情報」について
- (5)開示等の在り方について
- (6)他国への情報移転の制限について
- (7)「十分性認定」を意識することについて

「個人情報」の定義について

◆「個人情報」の定義

あるパーソナルデータが個人情報に該当するかについては、「他の情報と容易に照合して個人を識別することができることとなるものを含む」という現行法の判断基準を維持するとされている。

◆具体的提言

- ・「他の情報と容易に照合することができる」という容易照合性の要件こそが、個人情報の該当性を不明確にしている最大の要因であり、削除すべき。
- ・削除が難しい場合でも、容易照合性があると解釈されるケースを相当程度限定し、かつ客観的に判断できるものとすべきことを大綱において明記すべき（例えば、事業者が個人情報と準個人情報や個人特定性低減データとを別のデータベースに分けて分散管理する場合には、当該準個人情報や個人特定性低減データは個人情報には当たらないとする等）。

「準個人情報」について(その1)

◆「準個人情報」

「準個人情報」は、「特定個人を識別しないが、その取扱いによって本人に権利利益侵害がもたらされる可能性があるもの」と定義され、一定の例を示し、「これに類するものを含む」とされている。本人を特定して個人情報として同意をとるか、個人特定性低減データに加工しない限り、そのままでは第三者提供は許されない。

◆具体的提言

・従来多くの個人情報取扱事業者にとっては規制の対象ではなかった情報を保護対象とするもので、「規制強化が利活用を進める」という前提に立っていると思われるが、準個人情報という新しいカテゴリーの定義を設けることによる影響が精査されるまで、意見を留保する。

(個人情報への該当基準を明確化することで、グレーゾーンを相当程度解消することが可能。準個人情報という新たなカテゴリーを設けることで、従前は情報を自由に扱うことができた事業者に新たな負荷が生じることに留意すべき。)

「準個人情報」について(その2)

- ・「準個人情報」は、消費者が任意にまたは容易に、変更、削除、利用停止等を行うことができない情報で、かつ一意に識別できる識別子に結び付けられたものに限定すべき。
- ・「移動履歴、購買履歴等の特徴的な行動の履歴」については、準個人情報から除外すべき。
- ・技術的には、個人を特定せずとも一意であることを識別できれば、同意を得たり、オプトアウトを提供することは可能であるため、このような場合には第三者提供を可能とすべきである。

- ・ 現在提案されているルールでは、「準個人情報」の第三者提供が禁止され、これを可能とするには、事業者が個人を特定して同意を得るか、個人が特定される可能性を低減する措置をしなければならないとされており、個人との結びつきが低い「準個人情報」のほうが厳しい規制を受けているように見える。「準個人情報」への規制がかえって厳しくなっているのではないか、という点は、これまで一部委員からも繰り返し指摘されているが、顧みられていないのではないか。

「個人特定性低減データ」について

◆「個人特定性低減データ」

「個人特定性低減データ」は、個人データまたは準個人データを、政令に定める方法による加工を施して、個人が特定される可能性を低減したデータ、と定義されている。個人特定性低減データを第三者に提供する事業者は、加工方法等に関する情報をあらかじめ第三者機関に提出することとされている。

◆具体的提言

- ・加工方法については、特定性の低減という観点だけから検討するのではなく、データの有用性保持という観点からも検討すべき。
- ・技術進展や事業者の創意工夫によって生みだされる新たな加工方法が利用できるよう、加工方法自体を政令で定めるのではなく、事業者が新たな加工方法を利用する際の要件のみを定めるべき。
- ・加工方法等に関する情報をあらかじめ第三者機関に提出する義務を創設すべきではない。なぜならば、加工方法は、ビジネス上の秘密やノウハウに当たることが予想され、後に情報公開される前提で第三者機関に事前に提出することを義務づけられるのは、事業者にとって過大な負担である。また、提出されても、高度に技術的な判断を第三者機関が適切に下すことは困難である。

機微情報について

◆「機微情報」の定義

機微情報は、差別やプライバシー侵害につながりやすいため、特に適正な取り扱いを要するもの、と定義されている。

◆具体的提言

- ・機微情報は、バランスの取れた定義付けが必要であり、情報の主体(本人)との確実な対応関係とともに取り扱われる当該本人にかかる事実に限定すべき。
- ・社会的身分に関する情報は、出生によって決定され、自己の意思で変えられない社会的な地位に限定すべき。

開示等の在り方について

◆開示等の在り方

現行法における行政規制に加え、新たに「開示」、「訂正等」、「利用停止等」について、本人による民事上の請求権を規定することとされている。

◆具体的提言

- ・現行法においても本人による開示・訂正及び利用停止等が規定されているところ、上記の提案は純粹に事業者の負担を増加させるものであり、データの積極的な利活用に対する萎縮効果をもたらすものである。かように規制を強化することがいかにしてデータ利活用促進につながっていくのかを精査するとともに、民事上の請求権を規定する必要性、すなわち立法事実の存否を精査すべきである。
- ・仮に民事上の請求権を規定するのだとしても、情報の自由な流通を確保し、事業者の負担の軽減を図る観点から、訴訟提起の要件を限定するなど、濫訴を防止する施策が十分検討されなければならない。

他国への情報移転の制限について (その1)

◆国外移転等

- ・事業者内越境移転、越境委託、越境共同利用又は越境第三者提供について、移転先事業者においてパーソナルデータの安全管理のために必要かつ適切な措置が講じられるよう必要な措置を講じなければならないこととされている。また、移転元事業者又は移転先事業者において適切な措置が講じられていないと認められる場合に、第三者機関が移転を差止め等できることとされている。
- ・越境再移転は原則禁止、パーソナルデータの元の提供元が可能と認めた場合に限って可能とされている。
- ・これらの制限が課されない場合が、「本人の明示的な同意があるとき」等極めて例外な場合限定されている。

◆具体的提言

- ・TPP交渉では「free flow of data」の価値が確認されていて、その一方で他国への情報移転の制限を行おうとするのは、内閣の姿勢として整合性を欠くのではないか。

他国への情報移転の制限について (その2)

- ・情報は本来自由に流通すべきものであることに鑑み、パーソナルデータの保護は、情報流通(他国への情報移転)の制限によってではなく、セキュリティ措置によって実現することとすべきである。
- ・仮に他国への情報移転に何らかの規制をかけるとしても、原則として移転を自由とし、移転元におけると同等のセキュリティ措置が移転先においても確保されている限り、制限すべきでない。
- ・他国への情報移転を第三者機関が差止められる制度とする場合であっても、情報の流通が原則として自由であるべきことに照らして、「移転元におけると同等のセキュリティ措置が移転先において確保されていない」ことの立証責任を第三者機関に負わしめるべきである。事業者には「移転元におけると同等のセキュリティ措置が移転先において確保されている」ことの立証責任を負わせるのは、情報の流通に対する萎縮効果を招き、適切ではない。

「十分性認定」を意識することについて

- ・現行法における行政規制に加え、新たに「開示」、「訂正等」、「利用停止等」について、本人による民事上の請求権を規定するなど、規制の強化が志向されているのは、欧州による「十分性認定」を受けることを目標とすることによるものであるとされている。
- ・しかし、今般の個人情報保護法改正によって規制を強化した結果、「十分性認定」を受けられるか否かについて、何らの検討もなされていないように見受けられる。
- ・要件とそれに対する適合性の検証も行わずに、単に「十分性認定」を受けるということを目標として掲げて規制強化を図るのは、プライバシー保護とビッグデータ利活用促進の両立を図るという当初の目的に鑑みて、控えるべきである。

おわりに

現在わが国をはじめ、世界で合法的に行われているデータ利活用の実例を、今回のルール作りによって妨げるものではないという方針を、あらためて事務局に確認させていただきたいと考えます。

自主規制の枠組みを活用した パーソナルデータ利活用と保護の提言

アジアインターネット日本連盟
(AICJ, Asia Internet Coalition Japan)

2014年5月20日

本資料の内容

- 直接規制・自主規制の比較
- 実効性のある自主規制スキームと先行事例
- 執行の経済性の視点からの考察
- まとめ

直接規制・自主規制の比較

直接規制・自主規制はそれぞれに長所、短所があり、規制対象の特性に応じて適切な規制形態を選択する必要がある。

		直接規制	自主規制
概要	ルールの策定・運用(執行)	公的機関(政府/規制者)が実施	民間が主導して実施(公的機関が補完)
メリット/ デメリット	中立性	○ 事業者、消費者双方から独立し、 中立的な立場から規制を実施可能	△ 政府等による牽制機能が働かないと、事業者 に都合のよいルール策定・運用がなされる可 能性がある
	経済性(政府視点で見 たコストの大きさ)	× 規制対象によるが、一般的には大きい	○ 民間の自主的な取り組みであり、 政府の支出は小さい
	執行性	○ 強制力を持ち、事業者から中立的な観点で執 行ができる	△ 身内である事業者に対し、実効的な執行を行 えない可能性がある。
	専門性	△ 新興分野、高度な専門性を要求される 分野では、知識・経験が不足しがち	○ 事業に精通した人員を抱え、 高い専門性を有する
	迅速性	× 所定の手続を踏まえる必要があり、遅い	○ 臨機応変に対応が可能

パーソナルデータの利活用と保護のバランスは、その特性から自主規制の方が適していると判断される。

- 規制対象となり得る事業者が、多種多様で、かつ相当数にのぼる。また、消費者保護への対応が求められる。

⇒**ルールの運用に大きなコストを要する。(経済性の視点)**

- 新興で、高い専門性が求められる分野で、官民における情報の非対称性が大きい。

⇒**民間の高度な専門知識・経験が必要。(専門性の視点)**

- 技術やビジネスの変化が著しい。

⇒**ルール作成・見直しに迅速性が必要。(迅速性の視点)**



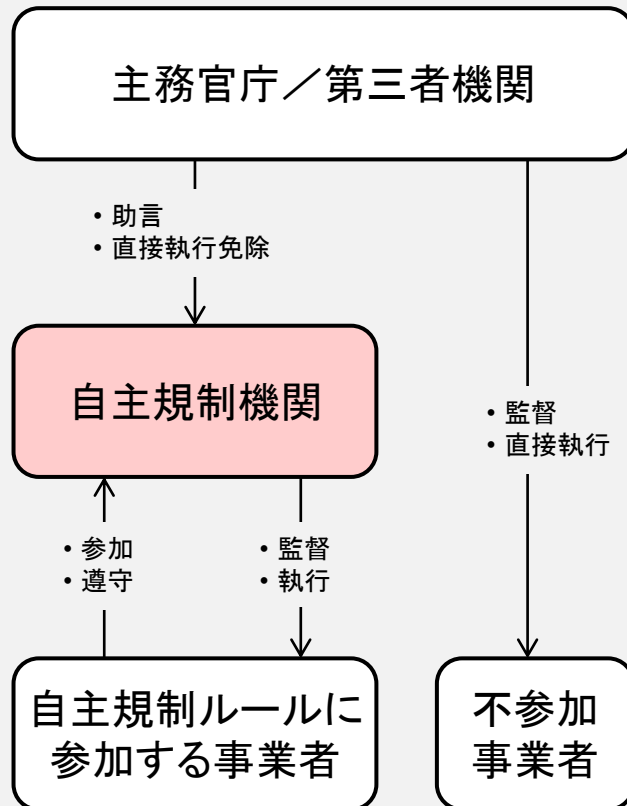
直接規制で対処するのは現実的に困難。自主規制の課題を克服し、機能するスキームの構築を目指すべき

パーソナルデータの利活用とプライバシー保護のバランスをはかる自主規制の事例

	自主規制の例	主体	法的基礎	公的機関の関与
米国	モバイルアプリの行動規範 (Code of Conduct) 作成	アプリ開発協会、消費者団体などのマルチステークホルダー	間接的	商務省電気通信事業庁 (NTIA) が主導。執行機関 (FTC) もオブザーバで参加。
米国	オンライン広告のオプトアウトルール の運用	DAA (ネット広告の業界団体)	間接的	執行機関 (FTC) の方針が尊重されている。非公式な相談対応がなされている。
EU	RFIDのプライバシー影響評価 (PIA) のフレームワーク作成	RFID関連事業者	直接的	EU構成国の執行機関のWG (29条委員会) が、民間作成のPIAフレームワークを承認。
オランダ (EU構成国)	データ保護法 (EUデータ保護指令27条の国内実施法) に基づく業界ごとの行動規定	各業界を代表する団体 (金融、製薬業等)	直接的	データ保護当局が行動規定の内容を審査・承認。これまでに18以上の規定を承認。
日本	行動ターゲティング広告ガイドライン	JIAA (ネット広告の業界団体)	間接的	事業者の自発的取組みとして、総務省の提示した配慮原則も考慮し、ガイドラインを作成。
APEC加盟国 (米国、日本含む)	APEC越境プライバシールールシステム	民間機関 (米国はTRUSTe、日本は未定)	直接的	APEC各国の公的機関がルールを作成し、さらに執行状況も監督。

実効性のある自主規制スキーム像

自主規制スキーム像

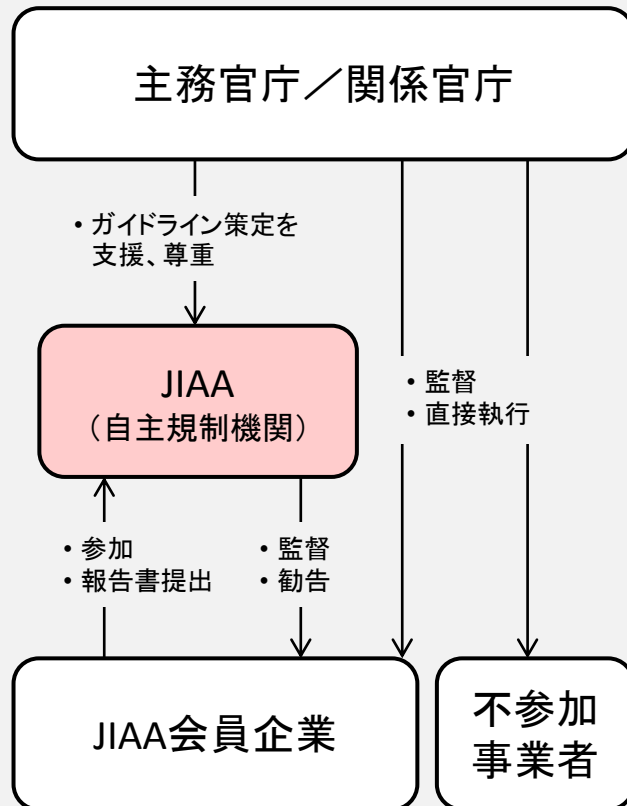


オプション1:
間接的な法的根拠により実現

オプション2:
直接的な法的根拠により実現

オプション1:間接的な法的根拠により実現に該当する事例: 日本:行動ターゲティング広告ガイドライン

自主規制スキーム



行動ターゲティング広告ガイドラインの概要

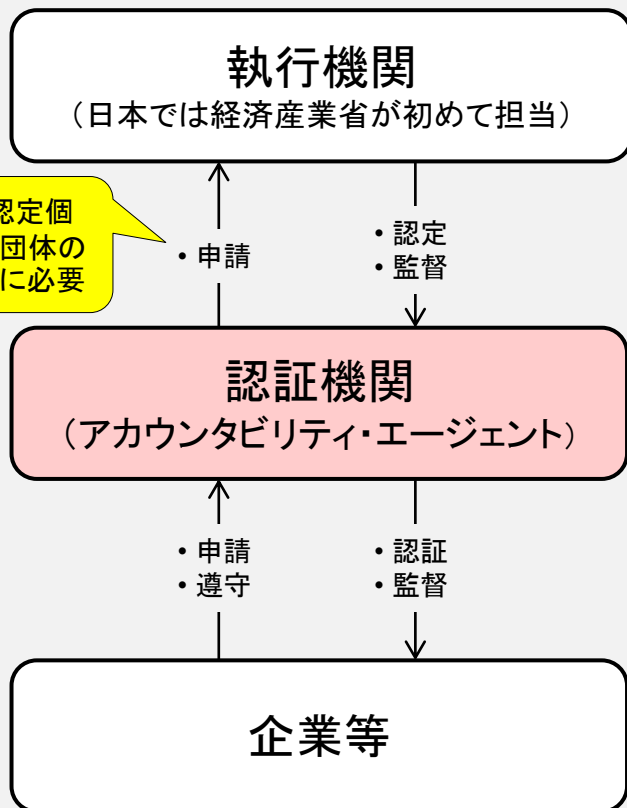
- 米国連邦取引委員会 (FTC) や米関連業界団体 (NAI, IAB等) の自主規制原則を参考として、また総務省の「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言における配慮原則を参考として、インターネット広告推進協議会 (JIAA) が策定。

※JIAAは、インターネット広告、モバイル広告ビジネスにかかわる企業 (媒体社、メディアレップ、広告会社など) から構成される一般社団法人。

- JIAAは、会員企業に対して報告書の提出や勧告の対象とすることで、規律を保っている。
- 主務官庁の直接執行を免除されることはないが、監督官庁の支援を受けて作成したガイドラインを遵守することで、執行に関して一定の配慮が期待される。

オプション2:直接的な法的根拠により実現に該当する事例: APEC越境プライバシールールシステム(CBPR)

CBPRの認定スキーム



日本では、認定個人情報保護団体の資格が申請に必要

CBPRシステムの概要

- 企業等の越境個人情報保護に係る取組に関し、APECプライバシールールへの適合性を認証する制度。
- 申請企業等は、自社の越境個人情報保護に関するルール、体制等に関して自己審査を行い、その内容について予め承認された中立的な認証機関(アカウントビリティ・エージェント)から認証審査を受ける。

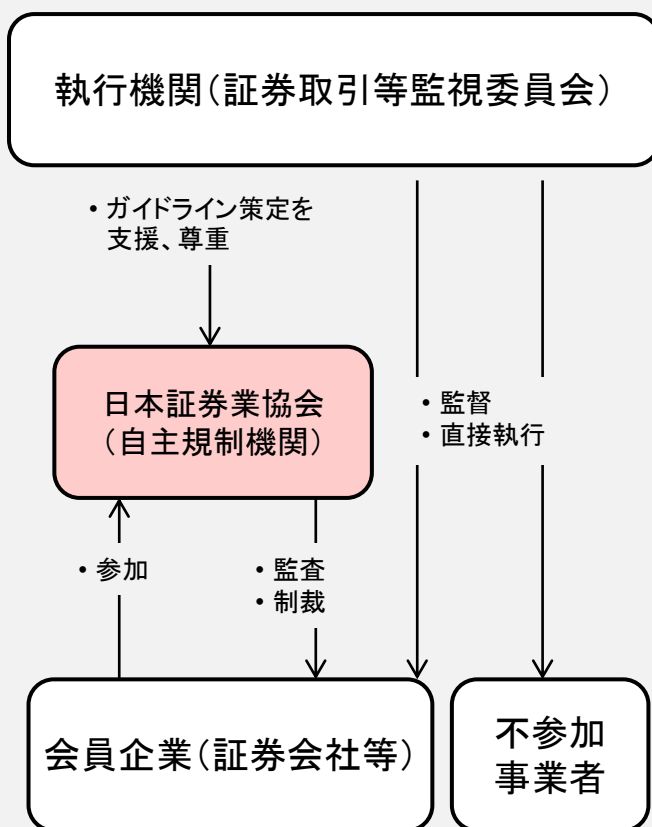
日本のCBPRシステムに関する現況

- 同システムへの参加には、法的に執行可能な認証機関(アカウントビリティ・エージェント)が必要となるため、これに認定個人情報保護団体の枠組みを適用。
- 経済産業省は、認定個人情報保護団体がCBPRシステムの認証業務を行えるように認定個人情報保護団体の認定指針を改正する予定(現在改正案のパブリックコメント実施中)。

他分野における自主規制スキームの事例(直接的な法的根拠により実現)

日本証券業協会

日本証券業協会の自主規制スキーム



日本証券業協会の概要

- 日本証券業協会は、金融商品取引業者等のほとんどが加盟する日本最大の証券業の団体であり、下部に業界団体と自主規制機関(を持つ)。
- 自主規制機関(自主規制会議)のトップは業界外の人間となっており、また構成員にも複数の業界外の人員が配置されている(ほとんどは企業経営者、法律家など)。
- 自主規制機関では、自主規制ルールの策定のほか、会員のルール遵守状況の監査、制裁の発動などを行っている。
- 規制機関(証券取引等監視委員会)は、本スキームが有効に機能しない場合や、本スキームに加盟していない企業に対して規制を行う。

執行の経済性の視点からの考察

自主規制を主体とする米国モデルと、第三者機関が主に執行するEUモデルとでは、経済性に約2.5倍の差がある。

項目	米国	EU構成国 ^{※3}	
		英国	仏国
職員数(人)	62	88	40
予算額(千円 ^{※1})	1,77,300	778,447	518,161

職員数は総人口に、職員一人当たりコストは一人当たりGDPに比例するものとして、日本に当てはめた場合の値を算出

日本に当てはめた場合の値

職員数	25	177	80
総コスト(千円)	706,978	1,873,389	1,890,496

約2.5倍の開きがある

平均1,881,943

※1: 米はUSD、英はポンド、仏はユーロ。

※2: 公表されている最新年に基づく。(米国は2012年(職員数は2010年)、英国は2012年、仏国は2011年)

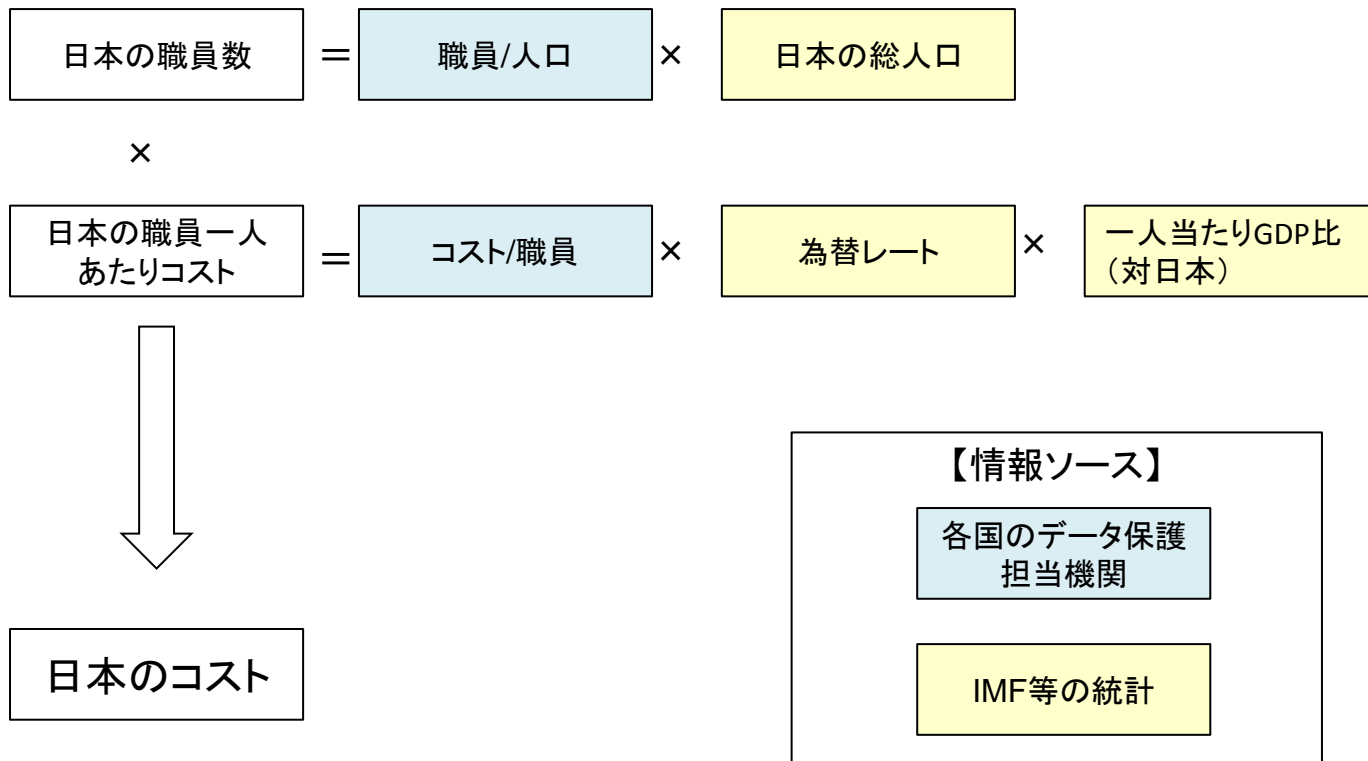
※3: EU構成国の第三者機関は、公的機関も監督し、また情報公開分野も対象としていることが多いため、実際に民間部門のデータ保護に該当するのは、全体の1/4として計算

まとめ

- パーソナルデータ利活用の規律は、法令等で定められた原則に基づいて、産業界が自主規制ルールを作成し、運用することが、経済性、専門性、迅速性の視点から現実的である。
- 自主規制は、米国、EUともに取り入れられているが、EUでは第三者機関の関与が大きい。ルールの作成・運用には、多様なステークホルダーが参加している。
- 自主規制ルールの運用は、基本的に民間が設置する自主規制機関が担い、第三者機関は、自主規制に問題が生じた場合の執行、又は自主規制に参加しない事業者の監督を担うという、官民で役割分担した階層化アプローチが実効性の確保に寄与する。
- 我が国でも、第三者機関と効果的・効率的に役割分担して運用する実効性のある自主規制のスキームを推進するべきである。

【参考】コスト削減効果の算出ロジック

- 職員数は総人口に、職員一人当たりコストは一人当たりGDPに影響を受けるとして算出する。



【参考】米国の第三者機関(FTC)の予算額の導出方法

- プライバシー関連業務と、その補助経費(FTC全体の運営に要するコスト)をFTEで按分した合計値をFTCにおけるプライバシー関連の予算とした。

Budget by Activity
(\$ in thousands)

	Fiscal Year 2012		Fiscal Year 2013	
	FTE	Dollars	FTE	Dollars
Financial Practices	102	\$16,821	105	\$17,629
Privacy and Identity Protection	51	8,596	51	8,713
Marketing Practices	97	27,490	98	29,316
Advertising Practices	57	9,579	57	9,718
Enforcement	55	9,289	55	9,423
Planning and Information	50	8,521	50	8,646
Consumer and Business Education	21	6,073	21	5,949
Economic and Consumer Policy Analysis	6	953	5	799
Management	27	4,579	27	4,643
Subtotal Direct	466	\$91,901	469	\$94,836
Support	172	83,851	173	74,681
Total	638	\$175,752	642	\$169,517

8,596

合計17,773

補助経費はFTEで按分して、 $83851 \times 51/466 = 9,177$

※FTE-Full Time Equivalentents(=正規職員に換算した工数)

【参考】米国の第三者機関(FTC)の予算額の導出方法

- Support(議会/訴訟対応の部署や広報等のコスト)の内訳;

	Fiscal Year 2012		Fiscal Year 2013	
	FTE	Dollars	FTE	Dollars
Commissioners	40	\$6,676	40	\$6,822
Policy Planning	11	1,753	11	1,793
Office of the General Counsel	59	9,079	59	9,284
Office of International Affairs	25	4,488	25	4,587
Office of the Secretary	12	2,183	12	2,233
Administrative Law Judges	6	921	6	941
Office of Equal Employment Opportunity	3	508	3	520
Office of the Executive Director	141	125,221	143	107,748
Office of Congressional Relations	7	1,081	7	1,105
Office of Public Affairs	9	1,476	9	1,512
Office of Inspector General	5	1,037	5	1,059
Total Support	318	\$154,423	320	\$137,604
Allocation of Support				
Consumer Protection	172	\$83,851	173	\$74,681
Maintaining Competition	146	70,572	147	62,923
Total Support	318	\$154,423	320	\$137,604

出所) FTC “FY 2012 and 2013 Performance Plan” p. 117

【参考】米国の第三者機関(FTC)の職員数:62名

個人データ保護に関する諸外国等の監督機関

	法律名(制定年)	主な監督機関名(設置年)	組織体制・身分等	職員数
イギリス	1998年データ保護法(1984年データ保護法を改正)	◎情報コミッショナー(ICO)(2001年。前身は1984年)	独任制。任期5年。両議院からの解任請求に基づく女王からの解任あり。	約350名(2010年)
フランス	情報処理、情報ファイル及び自由に関する法律(1978年/2004年改正)	◎情報処理及び自由に関する全国委員会(CNIL)(1978年)	17名の委員(裁判官、国会議員、経済・社会評議会委員、上院下院議長任命のIT専門家、首相任命のIT又は市民的自由の専門家)。任期5年	約130名(2009年)
ドイツ	連邦データ保護法(1977年)	●連邦データ保護・情報自由監察官(1977年)	独任制。連邦議会により選任。任期5年	約90名(2011年)
スウェーデン	個人データ法(1973年/1998年改正)	◎データ保護検査院(1973年)	5名の委員(国会議員2名、大学教授、IT専門家、地方議員)。4年ごとに選挙	約40名(2011年)
アメリカ	連邦プライバシー法(1974年)、金融サービス近代化法(GLBA)、児童オンラインプライバシー保護法(COPPA)、医療保険の相互運用性と説明責任に関する法律(HIPAA)等	○連邦取引委員会(FTC)(1915年)(その他、Department of Health and Human Services(HHS)等も法執行に携わっている。)	5名の委員。大統領により指名され上院で承認。任期7年。任務懈怠や在職中の不正行為等を除き自らの意に反して罷免されない。	約30名が個人情報担当(2010年)

+補助人員32名
(FTEの比率で算出し、 $30 \times 9,177 / 8,596 = 32$ 名)
全体で62名と算出

出所)消費者庁「パーソナルデータに関する海外の状況」(2013年9月)
http://www.kantei.go.jp/jp/singi/it2/pd/dai1/siryoushu2_3.pdf

【参考】英国の第三者機関(ICO)の予算額と職員数の導出法

- ICO全体の予算額は、年間約33億8,000万円(19,871千ポンド、1ポンド=170円として計算)、正規職員数は350名となっている。

予算額(2012-13年)

分類		予算額(千ポンド)
人件費	正規	12,013
	非正規	719
その他支出		6,755
減価償却等		1,103
合計		20,590

19,871

人員規模(2012-13年)

分類	人数
正規職員	350
非正規職員	17
合計	367

※その他支出はオフィス賃料や旅費、その他備品の購入費用などを指す。

【参考】仏国の第三者機関(CNIL)の予算額と職員数の導出法

CNIL STAFF

The steady trend in staff growth, initiated in 2004, was confirmed in 2011, due to the new duties and missions assigned to the CNIL by the amendment to the *Informatique et Libertés Act*.

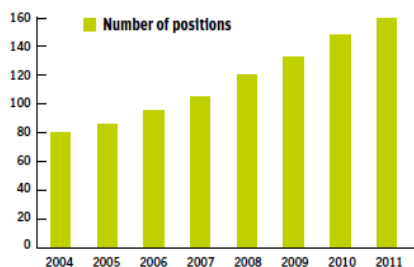
With 11 additional positions created, i.e. an annual workforce increase of 7.5%, the CNIL had 159 budget-approved positions in 2011 versus 148 in 2010, thereby doubling its payroll expenses within 7 years.

The steady staffing increase enables the CNIL to gradually catch up with the gaps already noted in 2004, particularly as compared to its European peers who employ an average staff of 200. The additional positions enabled the Commission to respond to its traditional tasks of audits, sanctions, coordination of the CIL network, authorization of sensitive data records, or label certification award, among others.

Yet this significant increase in resources still remain insufficient, as underlined in the recent parliamentary debates on the adoption of the 2012 Finance Act.

In 2011, the scope of the tasks entrusted to the CNIL by the legislator was considerably extended.

Firstly, the provisions of the LOPPSI 2 Law of March 14, 2011 entrust the CNIL with a new mission of oversight on video-surveillance systems installed on the public highway, in



application of the Law of January 21, 1995; yet these systems number hundreds of thousands.

Secondly, Article 17 of the Law of March 22, 2011 relative to the transcription into French law of the "Telecom Package" European Directive leads to an obligation for data controllers to report any security faults to the CNIL, i.e. in case of breaches of integrity or confidentiality of personal data. It is still very difficult at this time to quantify the number of security faults likely to be reported to the CNIL.

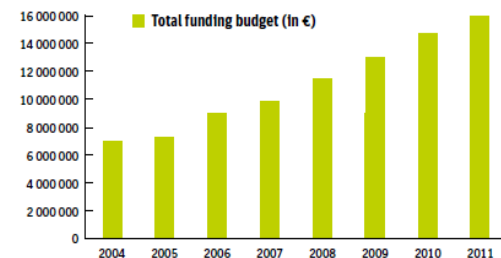
In view of new legal provisions, the CNIL headcount is therefore likely to further increase significantly over the coming years.

BUDGET

In 2011, the CNIL was endowed with a total budget of 15.8 million euros, an increase of 8% versus 2010, of which 10.3 million euros allocated to personnel expenses and 5.5 million to operating expenses.

The budget allocated to personnel expenses increased by nearly one million euros between 2010 and 2011, a 10% increase inherent to the additional staff positions created at the CNIL.

The 2011 operating budget also increased but to a lesser extent, rising only by 140,000 euros versus 2011, after appropriation of the "precautionary reserves" and the freeze of the "Fonds d'Etat exemplaire". This limited increase confirms de facto the trend observed since 2004, namely that increases in operating funds do not follow increases in personnel expenses



funding. For several years now, the CNIL has pursued a policy of operating cost control designed to reduce the expenditure ratios linked to premises occupancy, purchases of IT office equipment, or to staff travel and accommodation expenses. ■