『学習院大学　経済論集』第48巻　第２号（2011年７月）

個人情報信託の経済分析
～プライバシー情報を保護しながら信託で一元管理する～

辰巳　憲一*

本研究は，個人などのプライバシー情報を信託会社（ならびに信託銀行）で一元管理し，プライバシーを単に保護するだけでなく，プライバシーの発信源である個人にも可能な限り適切な便益や金銭的利益を提供しながら，個人の効用を高める方法が存在するかどうか，その可能性とそれが実現した社会の特性を経済学的に分析する。

特に重要なのは，プライバシーの経済的価値を認識し，その価値を実現し，それを守るという観点からプライバシー保護（privacy protection）を捉える点である。そして，プライバシーには，二律背反，モラルハザード，セキュリティとの矛盾，犯罪の隠匿，などの諸問題がある。これらはどのような問題なのか，これらをどう解決できるのか，展開することになる。

本稿はもっぱら経済学的分析を行い，法解釈や法案制定を展開する法学的な分析を行うものではない。本稿前半について，類似の研究は，一部，法学者も行っている。これら先行の類似研究との法律的な観点からの比較は行わない。文献引用も最小限に止める。しかも，本稿の内容は，信託に囚われることなく，セキュリティの経済学入門として，広い応用範囲を持っているものと考えられる。

１　問題意識と課題

１－１　ピザのデリバリーとプライバシー

われわれの身近な話題からプライバシー問題の存在が気づかされる。ピザのデリバリー（宅配）を電話で注文すると，こちらの電話番号を言うだけで（あるいは電話が通じた時点で），ピザ店のコンピュータ画面はわが家の所在地を地図上に表示しており，住所を確認している際には，注文が混んでいなければ，配達バイトが待機し，ピザの焼き上がりを待っている。

このシステムは，発信者の電話番号を表示するシステムを利用して，その番号と電話帳の住所・

---

*）学習院大学経済学部教授。Virtual Trust on Privacy Information~ A Proposal and Critical Comments. 内容などの連絡先：〒171-8588豊島区目白１-５-１学習院大学経済学部，TEL（DI）：03-5992-4382，Fax：03-5992-1007，E-mail:Kenichi. Tatsumi ◎ gakushuin. ac. jp（ご送信される場合◎は@に置き換えてご利用ください。）
本稿作成にあたっては，幾人かの人や組織，特に高崎春夫氏など，から幾つかヒントをえることができた。冒頭のピザのデリバリーに関する話は，著者がかつて何かどこかで読んだ論考が出発になっているが，出典は不明である。監視カメラとネームロンダリングなどの事実の把握については，NHK テレビの報道が役立った。いずれの関係者に対しても，ここに記して感謝したい。

氏名のデータをつき合わせ，さらにピザ店はそれらを発信者に問い合わせ本人かどうか確認する。ピザ店にとっては，このシステムは効率的で，いたずら注文が減り，セキュリティも高まる。

しかしながら，電話帳のデータが使われているところに問題がありそうである。そもそも，われわれユーザーは NTT に対して番号案内以外の目的での使用について許諾を与えていない。しかも，NTT は個人情報を目的外に使用することが禁止されている。そして，電話番号に関する個人データを本人の同意なく第三者に提供することもできない。それゆえ，この場合実際は，第三の IT 業者が NTT の電話帳をデジタル化して，ピザ店に提供しているのである。電話番号・住所・氏名は，もちろん個人情報として保護されなければならないが，この提供 IT 業者はデータ入力について個人に通知をしていないし同意も得ていない。この点がプライバシー問題となる可能性があるのである[1)]。このような問題を考察するための，基本的な考え方を本研究では提供することになる。

さらに，最近の出来事としては，Domino's App という iPhone から簡単に注文できる宅配注文アプリが出てきたことが注目される。GPS（全地球測位システム）機能を用いることで，デリバリーには住所が必要であるという従来の常識を覆し，お花見会場や公園にデリバリーする「屋外配達」の利便性をアピールしている。この点も，従来にない新しい問題点を内包している。

ブログ，SNS，Twitter などのソーシャルメディア利用者は「匿名」を志向していると言われている。しかしながら，他方で，ID 登録やログインを経て気軽にこれらのサービスを利用している。ところが，利用することにより自身の行動履歴が業者側に蓄積され，意図せず他者（他社）に利用されることも起こりえる。また，モバイル・デバイスによって時刻や場所と言った実空間情報が無意識に提供されることがある。意図せず，無意識に提供された，自身のすべての情報は誰がどのように使ってもよい，ということは了承したことになるのか，個人は知らされなくてよいのか。これらをどう解釈すればよいのであろうか。どういう問題があるのであろうか。問題解決方法は存在するのであろうか。

１－２　本研究の課題

プライバシーが侵されるままでいる従来の状態から，現在は，それを守る対策が議論され具体的な対策が講じられる状態に，変化しつつある。それだけでなく，近い将来にはさらに個人がプライバシー情報を適切に提供することから便益や利益を獲る状態に変化させることが必要なのではないか，と思われる。

プライバシー情報から利益を獲ている企業があるわけだから，個人はそのような企業にプライバシーを提供することによって便益や利益を獲ることができる筈である。この際当然ながら個人のプライバシーを適切に守りながら，これらのことが行われることが条件になる。

どのようにプライバシーを守りながら，このような仕組みを作り上げられるかどうか，その管理の方式を経済学的に考察するのが本研究の課題になる。具体的な仕組みとして，提供された個人情報を信託会社（トラストバンク）で一元管理し，バーチャルトラストでプライバシー

---

1)　ちなみに，電話加入者が申し出れば電話帳に個人情報を記載されないことも選択できる。それゆえ，この条件のもとで，この議論は曖昧になる。
一見して類似のケースに誕生日ビジネスがある。誕生日が近くなると，突然，郵便などで連絡が来て，案内状や割引券などを送られてくる。知らない店や会社なので，気味が悪いと誰もが感じる。しかしこれは，広く公開されている住民登録のデータから誕生日と氏名などをデータベース化した業者が，店や会社あるいは広告代理店に販売したデータを利用するもので，違法ではない。

保護（privacy protection）を実現する方式を取り上げる。極めて簡単な記述ではあるが，基本的なスキームは，既に Laudon（1993）によって提唱されている。

Laudon（1993）が提唱した National Information Markets（以下では NIM と略）という概念が先駆である。時代がまだ早すぎ，このような提唱・分析は取り上げられなかった，と理解できる。しかしながら，現代では緊急の問題である。

提唱された NIM は一国全体をカバーする比較的大きな公的（あるいは半公的）な機構であるが，本研究では複数の信託会社が民間の市場を作り上げる場合を考察しよう。公的な機関である場合，罰則を伴ったルールを強制（enforcement of rules）することさえできれば，運用は簡単である。しかしながら，純粋に民間の仕組みによって，個人情報のセキュリティを守ったまま，どのように管理できるのか，が関心の的になる。

バーチャルトラスト（virtual trust）という言葉は，ネット取引の他の類似の用語ほど，根付いていない。また，IT 業界ではトラストという言葉は文字通り，日常語の信頼という意味で使われることもあり，この言葉使いから認識を改め，高める必要がある。

わが国の信託法で，バーチャルトラストはどのような取り扱いになるか，大きな研究分野になろう。しかし，本研究では既述のように課題をあげるに止まり，信託法改定方法を研究対象にしない。

また，日本国憲法の第21条に規定されている「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」，あるいは同第35条に規定されている「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」に抵触せず，コンピュータやネットワーク犯罪を取り締まること，さらにはプライバシーを犯さず取り締まることは，極めて困難であり，大きな課題として残されている。さらには，日本国憲法で保障された表現の自由と知る権利の侵害に当たる個人情報についても，同様である。以下の議論ではできるかぎり，これらの事柄を避けることにしたい。

2　プライバシーのモラルハザード問題と二律背反問題

2－1　プライバシーとプライバシー権とは何か

（1）個人のプライバシー情報

人に関する情報は，大別して２つに分けられる。１つは，人が社会と関係を持つことによって発生する情報である。例えばクレジットカードを使って Amazon などで買い物するとか，プリペイド方式のスイカを使って（切符を買って）電車に乗るといった行動をとるという情報である。それに伴って事業者あるいはカードには購買履歴や乗降履歴などの個人の行動履歴情報が記録される。これらはライフログ[2)] と呼ばれる。

第二に，個人の，病歴や投薬履歴，（購読だけでなく図書館で貸し出ししてわかる）読書履歴，人の思想あるいは内心にかかわる思考履歴，肉体的な深層，DNA などが挙げられる。

後述のように，実際はさらに詳しい体系的な分類が望まれる。そして，内外で長らく議論と

2)　ライフログに関して個人情報保護とプライバシー保護から考察した文献は非常に多数ある。例えば，石井（2010），牧野（2010a），牧野（2010b）などがある。牧野（2010a）は，これら２つの中間に，個人情報保護法で保護されるべきデータがあり，これら３つを明確にして議論を進めていく必要がある，と主張するが，これら３分類は論旨不明瞭であり，本稿では取り上げなかった。

判例が積み重ねられ，プライバシーとは，「人に知られたくないこれらの情報」であり，プライバシーの権利とは「一人にしておいてもらう権利」あるいは「自己の情報を自身でコントロールする権利」であると考えられるようになっている。後者のなかに含まれるものでは，特に「自己の情報に正確性を維持する権利」が重要である。

（2）企業極秘情報と個人のプライバシー情報

「秘密」という概念は曖昧で難しい概念である。例えば，不正競争防止法の「営業秘密」という概念は，次が満たされて初めて認定される。営業秘密と言えるためには，①秘密管理性，②有用性，③非公知性の３つの要件が必要とされている。秘密管理性は，その情報にアクセスできる者が制限されていたか，ならびにアクセスできた者が秘密であると認識することができたかによって判断される。有用性は，その情報を専有することによって経済活動の中で有利な地位を占めることができる営業上又は技術上の情報であるか否かによって判断される。非公知性は，その情報が公然と知られていないことである。このように見てくると，個別のケースにおいて，要件が満たされるかどうかの判断が難しい場合が多い，ことがわかろう。

さて企業の秘匿する情報として，特許，生産ノウハウなどがある。このような情報と個人のプライバシー情報はどう異なるのだろうか。

生産性を相互に上げる情報は相互に公開するのが社会的に最適であるかどうかを Kamien-Muller-Zang（1992）が分析した。リナックスが良い先例となって，多くの企業が API（アプリケーション・プログラミング・インタフェース）を公開し，これによって開発者と周辺アプリケーションのシステムを構築していくことが図られる。これなどは，情報公開のメリットを示す例であろう。

また，意図的に公開しなくても，情報スピルオーバー[3)] によって同じ効果がえられる。かな

---

3) 情報スピルオーバー（information spillover）とは，組織や企業が持っている情報が自然と漏れ出ることを指す。Kamien-Muller-Zang（1992）の分析では，情報とは具体的に生産企業の技術開発投資の成果のことである。スピルオーバーするのは，情報というより，具体的に生産技術のノウハウ，知識（knowledge）の成果である。

他企業の技術開発投資の成果の一部が情報スピルオーバーによって当該企業の成果になり，他企業の技術開発投資は，あたかも当該企業が行ったように，投資コストを負担することなく成果をえられる，という共有化がなされる。このように成果を共有（share）された他企業の投資額の一部は，あたかも当該企業が行った投資額のように取り扱われ，それらと当該企業投資額の和は「有効」技術開発投資を構成する。これが，ひいては当該企業の単位生産コストの低下をもたらす。

モデルの前提となる事柄がいくつかある。①情報のスピルオーバーは，生産された製品に関してではなく，生産の前に，生産技術の研究開発やその投資時に起こる。そして，②各企業は，ラボや工場を個別に保有すると仮定される。ラボや工場では情報スピルオーバーされ，自社内に存在しないにも係わらず，そのスピルオーバーされた分だけラボや工場の生産設備は増える。それが，「有効」と呼ばれる理由である。③各企業は，他企業の生産情報（知識）を完全にモニターできる。さらに，④各企業は，それを理解でき，受け入れる能力（absorptive capacity）がある，と仮定される。

Kamien-Muller-Zang（1992）のモデルは，コストを減らすＲ＆Ｄに適用できるが，⑤質改善のＲ＆Ｄには適用できない。引用は省くが，続く多くの研究者達によって，これら５つの仮定は外され分析は拡張された。また，生産技術のノウハウを伝播するのは技術者である点を注目した労働市場の分析もある。

これらの前提の下で，情報，技術開発投資と研究開発のためのグループ化については，特別な意味合いが含まれる。Kamien-Muller-Zang（1992）で取り扱われる情報は，bads ではなく goods であり，社会的には生産効率を上げるため，皆で共有するのが望ましい。「情報」を秘匿する行為は，私的（個人的）な利益をえられる可能性はあるが，社会的には望ましくない。さらに，情報を秘匿するために資源を使うことは浪費になる。

り多くのノウハウ情報は，相互に便益を及ぼし合うものと予想できる。実際，現実のビジネス社会においてはスピルオーバーしているノウハウ情報の数は限りないと思われる。

このような企業情報と個人のプライバシー情報が大きく異なる唯一の点は，個人が「どう考えるか」が重視されることである。人権はあるが，法人権という権利はない，ことに由来する。ちなみに，企業社会において特許制度が存在する理由は，先進の開発を促すためであり，極秘情報を守るためではない。

２－２　プライバシーの曖昧さ～プライバシーのモラルハザード問題

何をもってプライバシーとするか，に関しては2010年に起こったグーグル（Google）のストリートビュー（Street View）撮影車が（意図せず）Wi-Fi データを収集していた問題が参考になろう。これに対して，英国のプライバシー監視機関 Information Commissioner's Office（ICO）は調査を行い，「特定の人物に関連づけが可能な個人に関する意味のある詳細情報（meaningful personal details that could be linked to an identifiable person）」は含まれていなかったとし，「廃棄してくれればよい」という立場を確認した。

日本でもストリートビュー撮影車は，道路周辺にある無線 LAN の基地局情報なども収集し，暗証番号などを設定していない無線通信で閲覧したホームページの履歴，やりとりした電子メールなどに関するデータが受信され，蓄積されたという。グーグルは撮影車両の活動を停止，集めたデータを外部から完全に遮断したとしているが，個人情報が含まれる可能性がある。しかし，情報は「断片的」で，ここから個人の特定などはできないとしている（2010年５月15日共同通信記事参照）。

しかしながら，プライバシーは主観的な判断に大きく依存する。つまり「通常の人間であればどう考えるか」ではなく，「そのプライバシー被害者がどう感じたか」に重きを置いて判断される。心理的抵抗感があるかないかという問題だけでなく，これは，個人がプライバシー問題であると判断すればプライバシー問題になる，というややこしいプライバシーのモラルハザード問題が起こる可能性がある。「プライバシー問題であると言えばプライバシー問題になる」という危うさがある。他人から見れば些細な事柄でも，個人に関連づけが困難であっても，一部の情報であっても，明かされるのは嫌だという人は必ずいる。モラルハザードとは，事実を曲げて，自分に利益を誘導する機会主義的行動をとる，ということである。これをどう解決するべきなのであろうか。以下で，一つの解決策を示すことにしたい。

２－３　過度のプライバシー保護～プライバシーの二律背反問題

顧客や利用者から多様なプライバシー情報を収集できれば事業者はきめ細かいサービスを提供することができる。顧客や利用者も，それによって便益や利益を獲る。プライバシー保護の主張を控えればこれらの便益や利益を確保できる。逆に，プライバシー保護を過度に主張すれば，それによって企業の業務がむしろ妨害されるのではないか，産業の発展を阻害してしまうのではないか，延いてはそれが経済を委縮させ混乱を引き起こし，回り回って雇用や個人の所得に悪影響を及ぼすのではないか，という心配もある。これらはいずれも，プライバシーの二律背反問題と呼べるであろう。

個人情報の有用性と保護のバランスを取るときに，「自己の情報をコントロールする権利」が係わってくる。プライバシー権は絶対であって，個人情報の処理・処分について本人に絶対的な権限があると認めてしまうと，二律背反が起こってしまう場合が生じる。他方で，プライバシーの二律背反問題は決して消えることはないが，コンピュータが高性能化し情報処理が高

度化したから，二律背反問題は大きく緩和，後退し，従来より強く個人情報を保護すべき方向になっているという議論もあるだろう。

プライバシー保護かその利活用かの葛藤については，国の対応は様々である。

欧州各国は，個人情報の利用よりも，プライバシー保護については，まずそれを本人以外に晒させないことを重視する傾向があったと捉えられている。米国では個人情報の単純な秘匿よりも利活用を重視して，特に個人信用情報については隠すのではなく，正確な情報が活用されているかどうかを重視する傾向がある。

こうした保護と利活用という利害の対立は，時代が代わって絶対的なものではなくなっている。匿名性維持，暗号や認証などの情報通信技術の進歩によって，２つの一見対立する利害を両立させる第三の道が生まれる可能性が十分にあるという期待も一部では持たれてきた。プライバシーの二律背反問題は，技術進歩によって，あるいは社会的な仕組みの考案によって，大きく緩和することを示唆している。

２－４　セキュリティとプライバシー保護が矛盾する問題

安心・安全な社会，つまりセキュリティの確保された，防犯が有効確実にできる社会を求めて，住民が監視カメラを自主的に取り付ける動きが日本では広がっている。自治体が助成金を出したり，警察が犯罪捜査に役立てたいという意図で後押ししており，監視カメラの設置が増えている。

日本では初めてのことで，監視カメラの設置や運用に関するルールは確立されておらず，本来の防犯目的とは異なる用途で利用されるなどして様々なトラブルが引き起こされているとの報道がある。

監視カメラによって，例えば，捨てたばこをした，ゴミの出し方が正しくないとか，身の回りに起こっている小さなルール違反，マナー違反が記録されていくことになってしまう。監視カメラによって「悪いことをしている人がいる」と告発するための手段を人々が手にしてしまう。消えない記録が残ると，怒りは理性的なコントロールも効かなくなる位になってくるのを抑えることはできなくなる。

現在の状況は，セキュリティとプライバシー保護が対立している，と言えるだろう。

セキュリティとプライバシー保護は矛盾するかどうか，監視カメラ問題を例に具体的に考察しよう。解決する方法はあるのか，どう解決すればよいのだろうか。監視カメラだけでなく，インターネットで検索する人への監視も同様な問題を含み，問題が該当する範囲は予想外に大きい。

そもそも，プライバシーが侵されるのは監視カメラで撮った映像は撮った人のもの，という意識が一般にあるのではないかと思う。そして，自分のものだから，どう処理・処分してもよい，という意識がどうしても抜けない。映った，撮られた人にも権利がある，それがプライバシーであるが，その認識は乏しい。

監視カメラをめぐる紛争で，裁判所は，監視されない権利，公道の上にもプライバシーはあるという考え方を明らかにするケースもある。「撮られたくない。監視されるのは嫌だ」というのは，法的には，基本的人権の一つなのである。

逆に心配なのは，もし悪用しようとすれば，監視カメラはいくらでも悪用できる怖さがある，ことである。むしろ，監視カメラによって新しい犯罪が可能になった，といえるのではないかと思う。大きな犯罪については予想は付かないので具体的にどのようなものか説明できない

が，小さい犯罪については，幾つも考えられ，事例を挙げることができる。

２－５　プライバシー情報の所有者は誰か

いわゆるセンサー・ネットワークなどの発展によって，個人から発信される情報（個人情報あるいはパーソナル情報）が収集されており，個人の属性に着目したサービス（パーソナライゼーションサービス）が企業間連携の流れの中で拡大している。

このようななかで，一般財団法人日本情報経済社会推進協会の電子情報利活用推進部（旧電子情報利活用推進センター）は，一方の極論を示している。電子情報利活用推進部（その HP 参照）は，まず，意図的にプライバシー情報という言葉を避け，すべてのケースにパーソナル情報という言葉を使う。そして，その特性を次のように記し，それ自体は無価値に近いと断じている。つまり「パーソナル情報は散発的なものであり，それ自体は創造的行為ではないものが多く，事業者がそれを収集・編集・蓄積することで，価値を増幅させている。」

この記述に反論はあろうが，確かに付加価値を付ける（価値を増幅する）のは，もっぱら事業者であることは否定できない。個人情報はすべて無価値であるとは主張していないものの，価値がないものが多いと主張し，あっても価値は乏しいと言っている，ように読める。この主張が正しいか，検証する必要があるように思われる。しかも，個人情報は，元は個人から発された情報であることは誰も否定できない。この事実をどう評価するのであろうか。

さらに，主張する。「パーソナル情報を元に戻せない状態に集合匿名化を施した不可逆匿名情報は，個人情報とは言えず二次利用が可能と考えられる。」つまり，個人情報を推計でき（個人情報を含ま）なくなった不可逆匿名情報は，もはや個人情報ではないので，個人の所有から離れる，そして，それゆえ自由にそれを使ってよい，と主張しているようである。数値番号に置き換えられた個人情報にはプライバシー情報は含まれないという解釈は総務省の研究会が出している。科学的に，あるいは現行法規に鑑みて，この主張が正しいか，検証する必要があるように思われる。

そもそも，2005年４月１日施行の個人情報保護法の中では，「個人情報の適正な取扱いに関し，国及び地方公共団体の義務や個人情報取扱事業者の義務等を定めることにより，「個人情報の有用性に配慮しつつ，個人の権利利益を保護することを目的とする」」（第１条。「」内の「」は著者追加）と記し，個人情報に関する有用性と権利利益保護の両者のバランスをとることの重要性を最初に規定している。

電子情報利活用推進部はさらに次のように続ける。つまり「そのような状況の中で，パーソナル情報に対して排他的権利（所有権など）を主張するのではなく，「事業者と利用者の情報の非対称性のバランス」を保ちつつ，個人の発する情報の経済価値を通じて社会価値を増幅させるための制度的枠組みを具現化することが喫緊の課題となっている。」このなかで，利活用を重視する視点は評価できる。しかしながら，電子情報利活用推進部は，どのようなタイプの事業者がその役割を担うべきか，そして，どのように担うべきか，を特定していない。大きな検討課題が残されているといえよう。

２－６　プライバシー情報を適切に守ることの重要性～犯罪隠匿とは峻別する

プライバシー情報を適切に守ることの重要性は自明のことのように思えるが，経済的な理由もある。もしプライバシー侵害が増えれば，個人は対応策として，１つの極端な例では，ネームロンダリングをすることが考えられる。ネームロンダリングは，他人と養子縁組して名前（苗字）を変えて別人になりすますことで，現在日本では，保険金詐欺という犯罪を犯すため，

借金とりから逃げるため，つまり犯罪に絡むか，民事上訴追される可能性のある行為のために，なされている。それだけでなく，（個人）倒産などの過去の履歴を消すため，などという正常な経済活動を行えなくなる障害を隠す目的で行われる。

ネームロンダリングは，戸籍で追跡できるが，住所を変えられると難しくなる。捜査に必要という場合警察は戸籍をたどれる。いわゆる閉鎖謄本を取れば現行の戸籍に記されていない情報を獲ることができる。これは弁護士，司法書士，行政書士など職権を持っている人間は閲覧可能であるが，一般の貸金業，保険事故調査会社などは難しい。一般の人が彼ら資格保有者を雇うにはコストがかかる。ふつうの場合，いわゆる名寄せ作業（名前と個人情報，過去の契約状況を照合して）を厳密化して，免許証や保険証などの番号と照合する，というような対策をとることで被害を防げたり，小さくできるが，やはりコストと時間がかかる。これらのコストは社会的に不要なコストかもしれない。このようなコストをかけなくても，適切な保護施策が打てればネームロンダリングを減らせるかもしれない。

戸籍を売る場合（養子縁組を何組も受け入れれば）遺産相続などの問題もあり，ネームロンダリングが多くの人に広まるとは思えない。しかしながら，個人にプライバシー侵害回避のためのモラルハザード的な行動を引き起こす，あるいは個人に（多重）犯罪を誘引させるような制度は，感覚的だけでなく，経済的にも，好ましくない。適切にプライバシーを守る制度的な整備が必要なのである。

逃亡している犯罪者をプライバシー保護制度が守るのでは本末転倒であるが，正常な人と犯罪更生者のプライバシーを守ることは推し進めるべきである。望むべきは，逃亡犯罪者とその他を厳に分けるプライバシー保護である。犯罪者を隠匿してしまうようなことは避けられるのであろうか。本稿の以下で，１つのヒントを示してみよう。

また，プライバシーを侵害する個人的な制裁（リンチ）が不要であることを人々に周知させることも緊急であると，著者は考えている。社会通念に反する出来事に対しては，人々は誰もが，個人的な制裁を加えても問題ない，むしろ制裁を加えるべきだと思い込み，プライバシー侵害や名誉毀損などが「正義を実現する勇気ある行動である」と勘違いする，ことがある。ネットの匿名性がそれに拍車をかける。このような通念がプライバシー侵害を深刻で長期的に影響するものにする。ぜひとも避けなければならない。

３　プライバシー情報の最適供給問題

既述の二律背反問題の一部としてプライバシー情報の最適供給問題が存在する。それを敷衍しておこう。

３－１　取引の構造と情報

（1）個人の特性

個人は，①自分が全体の分布のなかでどのような位置にいるのか，一般に，興味を持っている。そして，②それを知るために，個人は自己のデータは提供する，かもしれない。

しかしながら，個人は③自身のその分布位置情報は他には知られたくない。また，④入手した自分の位置情報に対しては，それが当初予想より悪くても，改善しようとする行動を必ずしもとるわけではない。

同様なことは，個人だけでなく，企業にもみられる。

①，②，③や④にみられる個人や企業の行動や特徴は，現時点においてデータで検証されているわけではない。むしろ著者が長い間抱いている感想である。

（2）足元を見られる

取引する際に「足元を見られる」という表現がある。履物を見られるという意味を超えて，取引相手に，必ず買うあるいは必ず売るという情報を「見透かされる」という意味である。さらに，取引の交渉は結局不利に終わるということを意味している。

資金に困っているという情報が漏れておれば，資産を早晩売らざるをえないこと（金に困って売り急いでいる）と理解される。あるいは，熱心な収集マニアであるという情報が知られておれば価格が高くても掘り出し物を必ず買うと理解される，などが例である。

e-コマースにおいて，居住地域あるいはライフログ履歴に基づいて，企業が価格の差別化を行うようになる場合には，高く買っても気にしない顧客とみなされると，販売価格は上げられるようになる。それは，私たちの財布の中身の使い心地（価格が上昇して実際上購入可能な数量が減る）に影響する。

足元を見られても気にしない人もいる。贅沢財を買う人にはそのような傾向（価格が高いほど売れる。セテイタス・シンボルは安物には務まらない）があることが知られている。それ以外の消費者は，足元を見られないようにしなければならないのである。

（3）プライバシー情報の最適供給問題

この足元を見られるという現象は，情報を提供すれば不利益を蒙る場合がある，という現象である。どのような情報をどこまで提供すれば，不利益にならないか，適切な境界があるのであろうか。情報を無制限に提供すれば不利益になることは予想できる。提供する情報が少なければ，受ける相手（企業）は利益をえられない場合が生じる。それゆえ，中間のどこかに最適な水準や最適な範囲が存在することが予想できる。これは，情報の最適供給問題と呼べる。

これを探るのが，課題になる。一部の研究調査は既になされている。個人は，どのような情報であれば，どこまで公開を許すかのアンケート調査の一例は，例えば高崎・小野・土生（2010）でなされている。このような研究を広げなければならないだろう。まず，すべての個人情報を詳しく分類する。そして，それらの小分類毎に情報を階層化する。これらによって，まず個人サイドについてはどの情報はどこまで公開できるか，企業サイドについてはどの情報はどこまで入手できれば最小限の結果が獲られる分析に利用できるか，を調査する基礎構造がえられる。

３－２　どのような個人情報は二次利用を拒否するべきか

（1）使ってもらいたい場合

経産省の情報大航海プロジェクトの中で，次のような事例が示されている。GPS 機能付き携帯電話利用者から取得した位置情報を使って，「近辺に，どのような属性の人が，何人くらいいるか」といった情報を30分ごとに，提供するサービスが考えられる。

個人の立場にたつと，混雑を回避したい人，あるいは人ごみが好きであり人ごみを探している人，の両極端の人々にとって，これは時機をえた有用な情報になる。当然個人の名前は出ないというプライバシーが守られていればという条件の下である。

さらに，モバイル位置情報機能や位置情報連動型ソーシャル・ネットワーキング・サービスは，われわれが知人と待ち合わせをする際には大変便利である。さらに高度な利点を Wall Street Journal 紙が，「Google 検索エンジンは，ユーザーがいる位置を特定できる。それならば，

牛乳を買いたいと思っていて，なおかつ，近くに買える場所があるとき，Google が買い物を忘れないよう注意してくれるようなことも可能になるのだ」と伝えている。買い物リストをスマートフォンに打ち込んでおれば，バイブで知らせてくれる，というのは大変便利である。しかしながら，購買行動の情報は，スマートフォン会社かだれかが厳重に守ってくれなければ，第三者に筒抜けになる。

（2）拒否すべき（できる）場合はあるのか

それでは，消費者はどのような個人情報の二次利用を拒否するべきか。これは難しい決定になる。

時間帯によって値引きや価格引き上げ，などを行う企業の価格戦略はピーク・ロード・プライシング（peak load pricing）といわれる。企業は，与えられた環境のもとで，利潤最大化によってこれらの戦略を決める。

地域，購入時間，購入商品などのような情報の二次利用をもし拒否でき，またその拒否が徹底できるならば，企業は地域的な差別価格やピーク・ロード・プライシングを設定できなくなる。少なくても，差別価格はそうでなかったより小幅に止まる。

しかしながら，買い物した物品名と時間を商店や取引の相手に知らせずに済む方法はない。現金で買い（あるいはカードを他人から借り偽のサインをする），変装でもしないかぎり，店側に購入層（買った人の年齢や性別）を騙す方法はない。そもそも，普通の人がこのような取引を隠すわけにはいかない。また，収集マニアは一般に自身の収集品を自慢したがるので，収集マニアであることを隠すのは，自己矛盾である。

このような個人情報の二次利用を拒否する有効な方法はない，ということになるだろう。そのような場合，個人と企業が利益を分け会うしかない。利益を分け会う方式には様々な方法が考えられる。企業は，情報提供の対価として必要な物の品揃えの豊富さを挙げるかもしれない。しかしながら，多少値引きする，方法もとるべきであろう。もっとも，企業は，情報提供料を払わなくて良い方法，たとえ払うにしても小額で済む方法を熟慮するのは当然である。これを，どのような意味でもこのような企業行動を否定することは，絶対やるべきではない。

4　行われている個人情報収集

既に，行われている個人情報収集には，どのようなものがあるだろうか。いくつか挙げてみよう。

例えばコンビニでのビデオ撮影や，高速道路でのスピード違反の写真撮影，料金所での写真撮影は，消費者側からすると，勝手に撮影され不愉快に思う人は少なくないだろう。しかしながら，これらの撮影データは，外部に公表する狙いのものではなく，日本では，「極めて短時間で，事件がなければ全部データを消すという前提でプライバシー侵害ではないとする」いう判断が下されている。

また，18歳未満の携帯電話利用者に対してサイトのフィルタリングサービス適用を義務づける「青少年インターネット環境整備法」が2009年４月１日に施行された。この法律によって関連する通信はサイト運営者によって監視されている。そして後述のように，かなり多くの通信はブロックされている。その狙いは青少年を犯罪から守ることにある。

さらに，様々な情報について考えてみよう。

４－１　使ってもらって良いケースと困るなというケース

個人情報を使ってもらって良いケースを２つと困るなというケースを１つ紹介しよう。

（１）NTT ドコモのモバイル空間統計

携帯電話ネットワークは，携帯電話端末が全国いつでもどこでも電話やメールなどをすぐに着信や通話ができるように，各地に配置された基地局のエリア毎に所在する携帯電話を周期的に（通信して）把握しており，それゆえ GPS を使わなくても携帯電話保有者の大まかな位置情報を把握している。携帯電話会社は，日本人の位置情報をすべて把握していることになる。

そのため，基地局エリア毎に滞在している携帯電話台数をユーザーの属性（ちなみに，それは購入した携帯電話登録者の属性である。実際は息子が持ち歩いて利用しているかもしれない）別に数えることによって人口の時間別地理的分布がえられることになる。NTT ドコモはそれをモバイル空間統計と呼び，公開するようになった。このようなデータを NTT ドコモはこれまで設備の維持・管理や投資計画用に活用してきたようである（堀越（2009）参照）。

モバイル空間統計により，地域毎の人口の分布，性別・年齢層毎の人口の構成，地域間の人口の移動の様子（移動人口）などを知ることができる。しかも，これらが一定時間毎に明らかになる。データを分析すれば，地域の防災計画，都市計画の立案や交通サービスの改良といった現代社会の様々な課題解決に役立てることができる。ビジネス利用に関しては，例えば，ある地域の人口の時間変動が推定できれば，商店の集客戦略，バスやタクシーの運行スケジュールや配車の最適化に役立てられる。

昼間は都心部に集まり，夜間は郊外の住宅街に戻るなど時間ごとに変化する人口の地理的分布を統計的に推計できるので，モバイル空間統計によって，災害時における帰宅困難者数を推計でき，災害発生時に公共交通機関が利用できなくなり帰宅が難しくなる帰宅困難者の事前対策にも役立つ（堀越（2009）参照）。

（２）会員向けカーナビサービスの公開

ホンダは，東日本地震の次の日の2011年３月12日，同社の会員向けカーナビサービス「インターナビ」を活用した道路情報の提供を災害支援の一環として始めた。ホンダ車ユーザーの走行履歴をグーグルアースやグーグルマップに表示することで，実際にどこをホンダ車が走っているのか，走ってきたのか，などを確認できる。主要幹線道路以外の情報は一般に入手しにくいため，被災地の道路がどうなっているのかの情報は貴重である（熊野信一郎「香港で栃木の被害を把握できた「力」「ソーシャル革命」を生かすための３提案」『日経ビジネスオンライン』2011年３月16日）。このような個人情報の利用は，誰もが進んで行いたいと思う。

（３）「食べログ」訴訟

飲食店の「口コミ」情報を集めたウェブサイト「食べログ」（経営は株式会社カカクコム）に対して，佐賀市内で飲食店を経営する男性が，店舗情報の削除を求める訴えを佐賀地裁に起こした（J-CAST ニュース（2010））。

当初，店舗の外観やメニューなどが，店に無断で投稿・掲載された。その後，店は外観やメニューを変更したが，「食べログ」の掲載内容は変更されないままだった。店側は「食べログ」に削除を要求したが，受け入れられなかったという。これだけが顛末である。

カカクコムは，『店舗情報を一般公開しているお店を全て掲載』する方針で運営し，店の意図にかかわらず掲載するという方針をかかげている。裁判所に提出した答弁書でカカクコム

は，①掲載されている内容は，投稿時の情報としては正しい，②最新の情報と異なる可能性がある旨，注意書きがある，などと反論した。

タイミングは企業経営にとって極めて重要な要素である。様々なタイミングが悪ければ，企業破綻してしまう可能性さえある。情報が適宜アップデートされなければ，そして，もし強力な競合企業が存在すれば，その企業は新しい情報で広告・宣伝するので，比較対象にされると競争にならない。顛末はどちらかというと簡単であるが，事柄は資本主義社会の根幹に係わる重要なものなのである。

今後われわれが注目するべき論点は，自己の情報を修正できる，あるいは自己の情報を非公開にできる，権利はわれわれにあるのかどうか，である。そして，どのような条件が満たされたら，それらはできるようになるのか，である。佐賀地裁がどのような判決を下すかにかかわらず，可能であれば司法が，時間がかかっても，その条件を示して欲しいと著者は思う。それら「自己の情報を自身でコントロールする権利」あるいは「自己の情報に正確性を維持する権利」が認められた後には，修正や非公開をどうすれば有効になしうるか具体的な方策をわれわれの側が考案する必要があるであろう。

４－２　ネットマーケッティング

アクセス解析に基づくネットマーケッティングが大きな分野になろうとしている。

（1）アクセス解析とは

いろいろな理由でインターネットのサイトに訪れる訪問者の特徴や行動に関して，様々な統計をとったり，分析するのがアクセス解析である。サイトのアクセス解析から得られるデータには，（ある専門業者の HP から転載した）図表 1 のように，PV（ページビュー）訪問数などの基本項目に加え，都道府県別，時間帯，滞在時間，他サイトへの遷移などがある。

マーケティングにおいては，①規模やその動向が比較的把握しやすい，②心理的変数や行動変数に比べ切り分けが明確である，③具体像をイメージしやすい，などの理由で，セグメンテーションを行う際には，いわゆる人口動態変数が使われる。その群には，具体的に，年齢，性別，家族構成，職業，所得レベル，教育レベルが用いられる場合が多い。また，地理的変数と密接に結び付いた人種や宗教といった変数もこれに含まれる。業界によっては，疾病や体格などが有効な変数となる場合もある。アクセス解析では，主としてこのような人口動態変数が集められるのである。

これらのデータを用いれば様々な視点からの個人行動の解析が可能となる。さらに，同一人物のサイト訪問回数，検索キーワードや経路などもわかり，サイト内での訪問者の動きを詳しく把握できる。例えば，電子雑誌の読者が広告ページをどんな順番で閲覧し，それぞれどの程

図表１　アクセス解析対象の項目

アクセスログ	アクセスログ，アクセスログダウンロード
アクセス統計	時間別，日別，曜日別，月別
アクセス元統計	リンク元 URL，リンク元ドメイン，検索エンジン，検索語句
システム統計	ブラウザー，OS，CPU，画面 画面サイズ，色数，Cookie Java，Javascript
訪問者統計	言語圏，都道府県，プロバイダ，ドメイン種，ホスト，ユーザーID，プロキシ 訪問回数，訪問間隔，閲覧時間
サイト統計	人気ページ，サイト構成

度の時間閲覧していたか，などのデータが収集可能であり，読者の志向などがわかる。

ちなみに，モバイル分析においては，モバイル・ウェブサイト，ユーザーが使っているキャリア，ユーザーのGPS位置，どの携帯電話端末がよく使われているか，アプリケーションがどのように使われているか（アプリケーションの利用状況を追跡して，報告する。），などを把握できる。

（2）アクセス解析の分析手段

アクセス解析の基本的分析手段を調べて，個人はどう見られているかを詳しく知ることにしよう。

①アクセス率

全ユーザー（例えば携帯電話の全利用者）のうち，過去1年あるいは1ヵ月などの一定期間内に，あるサイトを利用した割合をアクセス率と呼ぶ。

②ページビューとユニークユーザー

ページビュー（PV）はウェブサイト（またはウェブサイトの中の特定のウェブページ）が閲覧・表示された「回数」である。例えばYahoo！Japan（ヤフー！ジャパン）は，2010年には1日10億以上のページビューを獲得している。

他方，ユニークユーザー（Unique User，UU）とはウェブサイトまたはウェブサイト内の特定のページを訪問した人の数である。調査はブラウザーに対して行われるためユニークブラウザーともいう。同じウェブサイト（またはページ）を同じ人が何度も訪問した場合も，1ユーザーとしてカウントされる。ページビューと混同されるが，ウェブサイトを訪問した人は，サイト内の複数のページを閲覧することが多いので，ユニークユーザー数は，普通，ページビューより少なくなる。

③ページビューとインプレッション

インプレッションはウェブサイトに掲載される広告の効果を測る指標の1つで，広告の露出（掲載）回数のことである。サイトに訪問者が訪れ，広告が1回表示・配信されることを1インプレッションという。

ページビューはウェブサイト（またはページ）が閲覧・表示された回数であるが，インプレッションは広告そのものが表示された回数である。

同じサイトやページ内の同じ広告枠に，複数のインターネット広告がランダムに表示される場合（＝ローテーション型広告），ページビューだけでは広告そのものの表示回数を特定できない。ある広告キャンペーンのインプレッションは，広告を掲載したウェブページのページビュー（閲覧回数）の和に，1ページあたりの掲載広告数を乗じたものになる（ページに1つの広告を掲載すれば，掲載ページのページビューの合計に等しくなる）。

インプレッション1回につき課金する方式をインプレッション保証型広告と呼び，単価は1000インプレッションあたりの価格で表される。

④クリック率

クリック率あるいはCTR（Click Through Rate（クリック・スルー・レート）の略）は，広告がクリックされた（る）割合であり，クリック数÷インプレッションで計算される。この数値をみれば費用対効果の高い広告を見極めることができる。

一般的なメール広告やバナー広告のCTRは数％程度で，10％を超えるようなケースはまずないと言われる。しかしながら，あるタイプの広告，例えばPPC広告のようなクリック課金

型の広告の場合は，ユーザーのニーズにマッチした広告が掲載される傾向があるため10% を超える CTR を記録するケースもある。

CTR を左右するポイントとして，主に次の３つの要因があげられる。①広告画像やテキストそのもののクリエイティビティのインパクト，②広告内容と掲載媒体の適合度，③クリックによるインセンティブ（ポイント提供など）の有無。

⑤ CVR

CVR（Conversion Rate，コンバージョン率，顧客転換率）とは，一定期間内に商品購入や資料請求などの申し込み（コンバージョンといわれる。つまり，ウェブサイトから獲得できる最終成果）にどれ位至っているかを示す指標である。

CVR では，トップページや商品紹介ページのウェブサイトへのアクセス数（＝ページビュー）またはユニークユーザーなどのうち，どれを分母にするかをまず明確にする必要がある。通常は，サイトを訪れた人の数全体のなかで，何人がコンバージョンに至ったかの人の数の率を用いる。

CVR ＝コンバージョンに至った人の数÷サイト全体の訪問者数。

ユーザーではなく，クリック数（ウェブサイトへのアクセス数）あるいはセッション数（訪問数）を分母とする場合もある。その場合は次になる。

CVR ＝コンバージョン数÷クリック数あるいはサイト全体のセッション数。

この比率はそれぞれの広告のコンバージョン率を比較する場合に使われる。目的によっては，特定のページを閲覧した人のなかで何人がコンバージョンに至ったかを見る場合もある。その場合は次になる。

CVR ＝特定のページを経由してコンバージョンに至った人の数÷特定のページを見た人の数。

⑥購買履歴に基づく顧客管理とレコメンデーション

住所，生年月日や性別だけでなく，販売履歴，問い合わせ履歴といった顧客とのコンタクト履歴などの顧客の履歴管理を通じて，企業は購買パターンを把握し，タイムリーな商品提案を行うことができる。企業は，例えば，購買実績や，さらに詳しく「前回購買日からの経過日数・購買頻度・購買金額」の３つの軸から，顧客をランク分け，グループ分けし，それぞれのグループに応じた的確な販促活動をすることができる。ユーザーの購買履歴や好みに基づいて，個々に適した商品を勧める販促活動はレコメンデーション・サービスと呼ばれる。

例えば，ネット書店では，クッキーと呼ばれる機能を使ってユーザーに番号をつけて識別し，購買記録などから，どんなタイプの商品が好きかを分析してレコメンデーションしている。ただし，集められるのはサイト上で同じ識別番号を使っているユーザーの行動記録に限られ，しかもレコメンする商品は内容まで十分立ち入っていないため，不適切なレコメンになっているという意見が多い。しかしながら，これら個人識別や商品内容の正確な把握などの点は今後確実に改善されるものと予想される。

（３）問題点要約

上の（２）でここまで概説したようなサイト訪問時だけではなく，ネットワークに流れるパケットデータから利用者の行動を収集，分析する方法もある。ISP（インターネット接続プロバイダー）に設置した DPI（Deep Packet Inspection）機器によって，通信内容を傍受して，趣味嗜好などを分析しながら記録できる。それらはパケットキャプチャー型アクセス解析と呼ばれる。これ以外にも，いくつかネットマーケッティングの方法がある。今後ネットマーケッティ

ングは益々高度化するだろう。

事態はさらに進んでおり，個人のサイト閲覧履歴の売買（例えば，日経産業新聞「サイト閲覧履歴，取引仲介」2010年８月16日，参照。）がデータエクスチェンジ事業として始まっている。データエクスチェンジとは，ネット利用者の過去の行動履歴や属性などの匿名のデータを，メディア（提供者）と広告主（利用者）の間で仲介するサービスである。

プライバシー侵害の懸念は，既に，持たれていて，ICT（情報通信技術）サービスの利用者保護を検討する総務省の研究会は2010年４月９日，サイト閲覧や買い物などのネット上でのライフログ（行動履歴あるいは閲覧履歴）を集めるネット事業者などが増えていることに対応して，取得の事実や取得内容，第三者への提供などについて「利用者に開示することが望ましい」ことを指摘した。

アンダーセン（2009）は，「無料経済」というキー概念を使って情報社会の問題について解説・分析し，サービスを無料（フリー）にして，事業を成功させた例を多く挙げ，注目をあびた。実は，無料（フリー）といっても，多くのケースは利用者自身の個人情報を売り渡してフリーを手に入れているのである。売り渡しているという認識はないかもしれないが，実際はそうしているのである。

しかしながら，フリーミアム（freemium）という複雑な要素がここに付け加わる。「無料という名の広告をしている」と言われるように，企業は「無料」を広告料と理解している部分がある。さらに，無料のユーザーがいると同時に，有料版ユーザーが存在し，かれらが無料版ユーザーの無料サービスを資金的に支えているという場合もある。

個人的には，上でみた多くのケースは統計学分析のための母集団を構成する１サンプルになっているに過ぎない。しかしながら，販売促進策の一部は個人を特定している。個人を特定するアクセス解析が不審者やウェブ攻撃者を識別するために使われるならば，大変好ましい。むしろ，そのような分析の発展を推し進めるべきである。

また，企業がCTRやCVRを用いたアクセス解析を自社のサイト改善に利用するのに止まっている限り，問題は大きくない。例えば検索連動型広告において１クリックの料金を下げる（つまり広告料金を引き下げる）検察を考慮するのに止まっている限り，問題は大きくない[4)]。

---

4) キーワード広告のプライシングを例にあげておこう。キーワード広告とは，ユーザーがキーワードを検索するエンジンの検索結果に表示される広告で，広告がクリックされたときのみ費用が発生する。クリックしてもらうために，良い場所に出稿する必要がある。そのためには，高い入札価格を付けなければならない。サイトへの出稿では，企業はいわゆるクリック単価を入札することが，必要になる。検索連動型広告への入札金額の決定方法は，一例として，ある業者のHPを参考に組み立ててみると次のようになる。
まず，平均客単価と平均純利益率を掛け，１購買当たりの純利益金額を算出する。純利益とは粗利益から諸費用を差し引いた利益である。
次に，実際に購買等のアクションに結びつくユーザーは全体の何％かを示す，サイトのコンバージョン率（転換率＝実際に購買等のアクションを起こしたユーザー数÷総誘致ユーザー数）を算出する。なお，サンプルが多くない場合，ユーザー数ではなく，ユニークユーザー数を用いるべきである。
そして，１購買当たりの純利益金額にコンバージョン率を掛ける。例えば，平均純利益金額が1,000円で転換率が２％とすると20円が求められる。この金額がキーワード広告の入札上限値となる。
サイトの長期的価値（ライフタイムバリュー）などの，いろいろな要素を取り入れ，入札金額をこの基準値から多少乖離させることも，長期戦略上は有効であると考えられている。
業界の常識では，人気キーワードは１クリック1000円以上に高騰し，一般的なキーワードも50円から100円程になる，という。

ユーザーが行う検索に関しては，検索結果の上位に表示されるよう企業はSEO（検索エンジン最適化）技術を使っている。つまり，多く検索されているキーワードやネット上で話題になっているテーマをモニターし，それに基づいて企業はサイトのコンテンツを高頻度で変更している。しかしながら，検索結果のなかには，とにかく検索にかかりたいがために関係のない企業のサイトが潜りこむことが多く，ユーザーは迷惑していることが多い。そして，詳しい個人情報が獲られているだけに，ネットマーケッティングが進めば，ある境界点から以降，プライバシーに触れることになるかもしれない。その境界がどこなのか，見極める必要がある。

また，アクセス解析している（した）企業が破綻に直面している場合あるいは赤字が続いている場合，集められた個人情報は管理が等閑になる。いたし方なく等閑になるだけでなく，密かに売却し，資金の足しにすることも普通にあるだろう。このような場合誰がどのように管理するべきだろうか，われわれは真剣に考えなくてはならない。

５　信託による権利の管理

信託は，委託者，受託者と受益者という３主体によって構成される経済的関係である。委託者自ら受益者になるケースには２主体になる。信託は，委託者が信託行為（例えば，信託契約，遺言）によってその信頼できる人（これが受託者である。具体的には信託会社や信託銀行）を決め，その人に対してお金や土地，建物などの財産を移転することで始まる。そして，受託者は委託者が設定した信託目的に従って受益者のためにその財産の管理・処分などをする。

委託者が受託者に信託する財産が信託財産で，例えば，お金，株式や国債などの有価証券，土地・建物，特許権や著作権などの知的財産権などが当たる。

受託者は，受益者から監視・監督権をえて，信託財産の管理・処分などをし，信託利益の給付を受益者に対しておこなう。この際，受託者は，信託財産の管理・処分を行うにあたって，善管注意義務，忠実義務，分別管理義務などを負う。

信託管理の大きな特徴は，信託利益の受取人や受取時期を細かく設定できる点である。これが，信託制度を利用するメリットの１つになる。受取人を家族以外に指定したり，資金用途についても，月々一定額だけでなく，そのうち一定額をあらかじめ決められた時期に指定できる。そして，資金使途を指定して生活資金や学費に限ること，などができる。

信託業務は多くの会社が行えるようになっている。2008年に保険業法の施行規則が改正され，生命保険会社が信託契約の代理業務をできるようになっている。

本稿の関連で法律上残された課題は，信託財産のなかに，個人情報を入れる。第二に，受託者が負う義務にプライバシー関連の義務を入れる，ことである。なお，本研究では，これらの法律問題を取り扱わない。

５－１　個人情報をトラストバンクとして一元管理

個人情報をトラストバンクやバーチャルトラスト会社が一元管理する際の問題点をリストアップしよう。ここでバンクとは必ずしも銀行・信託銀行を意味するのではなく，データバンクのバンクなどと同じような使い方である。

バーチャルトラスト会社が行う業務として，次の５つが考えられる。①匿名化などの処理，②取引条件の交渉，③利用状況のモニタリング（monitoring activities），④利用料等の代理徴収と管理，⑤個人への利益配当等の支払いと管理。

（1）匿名化などの処理

個人情報を，まず，匿名化処理（非識別化処理とも呼ばれる），集計処理，秘匿処理する，必要がある。どう行うかは，どちらかというと，暗号学，統計学，などの学問的な問題である。しかしながら，その影響や効果を見極めるには経済学を用いなければならない。

どの段階で，どこまで，これらを行うか，も大きな問題である。既述のように，個人は，どのような情報であれば，どこまで公開を許すか，研究調査する必要がある。

匿名化された後の情報にも課題がある。①「匿名化するので，誰の情報か分からない。」②「誰の情報か分からない情報を誰がコントロールするのか。」こう問題提起する牧野（2010a），牧野（2010b）などは，③「匿名化情報を他の匿名化情報と照合したときに，個人を識別できてしまう可能性がある」，とも主張している。このうち，①は匿名化を誤解しているので，この主張は正しくない。匿名化されても，同じ匿名で処理されていき，相互に識別可能である。また，簡単にアクセスできないガードの固いところで，限られた者だけが匿名と実名の突合せができるような仕組みが考えられている。

②の，匿名化情報だからといって，コントロールできない状態にしておいては，ある日突然，個人のプライバシー情報に戻ってしまう可能性は否定できないという主張については，この「戻ってしまう」とは匿名化処理がなされていない，あるいは解除されてしまうことに相当するので，「完全な匿名化処理技術を作れ」といっているに過ぎない。こうした課題を検証し，解決していく必要があるのは事実である。技術者の間では，暗号化したまま処理する方法が話題になっているようであるが，どのような仕組みなのか，見守る必要がある。同様に③のような可能性は匿名化処理技術に依存するわけで，技術的な検討を試みた上での問題提起のようには見えないが，技術上の課題の１つとして残る問題ではある。

集計処理にも課題がある。集計データ，正確には集計データ群から個別データを逆推計できない，ようにする方法を進める必要がある。傾向スコアなど，不完全データから因果関係を推定する統計学的研究が進みつつあるが，それと全く逆方向の研究が必要なわけである。

SNS（ソーシャル・ネットワーキング・サービス）提供者などの情報仲介者は，手に入れた利用者の嗜好や行動の情報を，セクターにあるいはマクロに集約し（まるめて）広告主に売っている。そのまま売る場合はプライバシーを侵害するが，統計集計データの一サンプルとして利用しているので問題はないと SNS は理解している。他方，利用者は結果として無料で会員同士の会話や無料動画などを楽しみ，同時に望む広告情報などを入手している。

個人が提供するのが差し支えない情報なら全く問題なく，逆に個人には望む物が増え，品揃いがよくなる，などの付随的メリットもある。しかしながら，一般に SNS では，「友達」（ミクシィの場合は「マイミク」）に対して，生年月日，学歴，勤務先，住所，電話番号などの個人情報を公開状態にしているユーザーが少なくない。「友達」だけでなく，SNS 提供者などの情報仲介者がモラルハザードを犯さない保証はなく，気を付けないと大きなダメージを受けてしまう危険もある。

例えば，マイミク同士で住所を知らなくてもリアルな年賀状を送れる「mixi 年賀状」は賀状送付先個人の住所を実際上その個人の了承をえず（強制的に，断れない環境に置かれた状況で了承させて）課金ビジネスに使っているのである。

秘匿処理にも課題がある。匿名化してあるとしてもデータは機密として取り扱わねばならない。機密データが外部に流出しないように 漏洩防止や DLP（データ損失防止 data loss

protection）対策などを講じる必要がある。

以上，求められるのは，Privacy Preserving Data Mining（PPDM）技術あるいは通称 PETs（Privacy-enhancing technologies）と呼ばれる技術である。

（2）取引条件の交渉と利用料等の価格の設定

現代でも，一部の個人情報を売ることが（実際上，実質上）行われている。しかしながら，売買の一部は闇市場で行われており，その価格は本来あるべき水準からは相当かけ離れている，と予想される。こういった状況を本研究が提唱する案は改善する。

バーチャルトラスト会社は，まず個人とどのような情報を提供していただけるか交渉し契約する。企業に対しては，事前に属性情報（性別，年齢，職業，趣味等）を提示し，利用料等の価格の交渉を行う。この際，個人情報の利用時毎やトランザクション毎に利用料等の価格を徴収していく方式は，コスト的に高くなるので，するべきではないだろう。

バーチャルトラスト会社は，契約した個人に対して，最良執行義務を負わねばならないだろう。最良執行義務について説明しておこう。証券市場においては，証券ブローカーは最良執行義務を負っている。これは，もっとも安い価格を買い手に代わって探し執行する，売り手にはもっとも高い価格を探し執行する義務だけではなく，開示されている気配・取引情報に基づき，コスト，スピード，執行可能性といった条件を勘案しつつ，顧客にとって最良の条件で売買を執行する義務である。

米国では2005年４月にレギュレーション NMS が採択され，証券会社に対して，最良気配価格を提示する市場での売買が義務付けられた。欧州でも2007年11月の MiFID（金融商品市場指令）で，最良気配や流動性なども含む最良条件での執行義務を導入した。これにより欧米では投資家の意識が高まった。

日本でも2005年に最良執行義務が導入されたが，機関投資家であっても最良執行に固執しない。理由は，そもそも代替市場が未発達であり，私設市場（PTS）の数が限られ，流動性も低いため，最良執行しようにも市場は限られ最良執行義務は実際上機能しない。さらには，最良執行方針は証券会社が総合的に判断すること[5]と規定する金商法の存在のため，である。それゆえ，日本の証券ブローカーは最良執行義務を対岸（米国）の火事と決めてかかっている。しかしながら，個人情報の買い手は数多く存在するので，バーチャルトラスト会社は最良執行義務を真剣に取り組まねばならない。

正当に料金をとるべきであるという問題は，別の観点からも差し迫った問題になっている。情報発信（通信接続）コストの低減によって，ネットワークの中も，データ・センターも，UGC（ユーザー生成コンテンツ）であふれかえることになった。それらの通信と維持管理をするためのコスト負担は膨大になり，業者は課金ビジネスを指向する動きにある。このような背景のなか，池末（2009）は，いったん SNS などを有料にしたうえで，ライフログ（行動履歴あるいは閲覧履歴）の広告主への開示を許諾した利用者だけ利用料を免ずるという案を提唱している。

個人情報の市場価格は実際どれだけなのか，市場調査してみる必要があろう（データや数字

5） 日本では，機関投資家は通常，「ブローカーレビュー」で複数の取引証券会社を点数評価し，発注のシェア割を行う。評価基準には調査やセールスの質，系列関係も含まれ，注文執行コストの高低が直接反映されない。それゆえ，最良執行という意識が乏しい。証券会社も「顧客の指定がないかぎり，取引所で執行」するケースが大半であるという。

情報のプライシングを調査した辰巳（2011b）が一つの参考になろう）。技術情報や個人情報の漏洩が続いている報道をした，追跡 AtoZ「“情報流出”の闇を追え」NHK，2011年２月26日，が取材したケースでは，生活に困った IT 会社の派遣社員が名簿業者に販売した46万人分顧客情報が50万円であった。この１名約１円は，事情から判断して最低価格である。しかも，売値である。買値はその数倍（軽く２倍以上）になるように思われる。

個人情報の価値を評価する，いわゆるプライシングがバーチャルトラスト会社の一番大きな，しかも困難な業務になる。これが，取引条件の交渉に用いる売値になる。プライシング・モデルがまったく存在し無いということはない。例えば，日本ブランド戦略研究所は有力企業のウェブサイトの価値を調査している。事業に対する貢献度に基づいてウェブサイト価値を評価するもので，直近１年間の決算報告書の財務調査およびインターネットによるアンケート調査に基づく。

その他に，ある NPO のモデルもネット上で公表されている。プライシング・モデルがあるかないかではなく，問題は良いモデルかどうかである。

バーチャルトラスト会社の付随的に必要な業務として，ポイント，クーポンやアプリの無料提供などの「フリー」の内容を調査して，それが何円に相当するか，評価額を導出することも必要になろう。

（３）利用状況のモニタリング

モニタリングは膨大な作業量になる。モニタリング業務を国や地方政府が行う場合，かつての統制経済や管理社会に似てくるので避けねばならない。

モニタリング作業にあたっては，既述のアクセス解析や通信監視システムが参考になる。一例をあげておこう。メールの内容をチェックすることは「通信の秘密」に抵触する恐れがあるとして実施に踏み切っていない事業者が多いなか，利用者の同意を得る形で2007年から実施しているモバゲー運用の DeNA 社がどのように監視しているかの状況を松浦（2010）が報告している。それによると，１日当たり1000万件以上ある膨大な量の会員間のメッセージ「ミニメール」やサークル掲示板，日記を監視するために，まずはシステム的に内容をチェックして投稿をブロックしたり，削除したりしている[6)]。次に400人の人間が，それをすり抜けるものを目視でチェックする。

もう１つ例をあげておこう。証券市場における最良執行義務を負っている米国の証券ブローカーは，執行可能性を高め，低コストと高スピードを実現するために，開示されている気配・取引情報に基づき，売買条件のモニタリングを行う。最良執行義務を証券ブローカーに課す政策は投資家保護策の原点である。証券ブローカーは，最良執行を証明するために，あるいは投資家に事後報告できるよう，記録を残す。

バーチャルトラスト会社の比較的重要なモニタリング業務として，個人情報の転売の監視，がある。データエクスチェンジ事業として個人情報の売買仲介が民間会社間で行われている現

6） 具体的には，利用者が18歳未満の場合，年齢が３歳以上離れている利用者とのメッセージ送受信ができないようにブロックしている。同様に利用者が18歳未満の場合，３歳以上離れた利用者からの検索ができないような対策も講じている。また，「きもい」「しね」といった違反キーワードを含む投稿を抽出し，内容を確認してブロックしている。
今後は年齢を詐称登録して青少年に近づくといった行為を未然に防ぐため，携帯電話事業者が契約者から得た年齢情報を活用して，年齢認証の強化に取り組むそうである。

況のなか，この業務は重要である。提供を受けた（購入した）個人情報を，企業は他の企業に転売しないまでも，管理が不十分で，情報漏洩が起こり結果として無料で渡すことになるかもしれない。これら情報漏洩の管理も何らかの方法で行わねばならない。

集められたり，購入したりした個人情報の管理が等閑になってしまう傾向がある，破綻に直面している企業あるいは赤字が続いている企業の場合，バーチャルトラスト会社が管理を代行したり，管理を自社に移行して，あるいは問題企業に残存する個人情報を消去して，問題企業が情報を密かに売却し資金の足しにすることを防がねばならない。このような場合バーチャルトラスト会社のような組織がすべての業務（清算を含めて）を一括して行っていると効率的で良い。このような場合国か地方政府が問題企業や困難企業を直接管理するべきではない。

バーチャルトラスト会社間の競争が必要なので，できたら複数のバーチャルトラスト会社の設立が望まれる。そして，この競争のモニタリングという意味で公正取引委員会の活動が必須である。

（4）利用料等の代理徴収，個人への利益配当等の支払いとそれらの管理

バーチャルトラスト会社は個人宛に口座を開設する。そしてバーチャルトラスト会社は個人情報の運用益をこの口座に振り込む。このような分別管理は必須である。さらには，個人保護を徹底するために，別の信託銀行に個人資金口座の信託預託を義務化することも必要になるかもしれない。

英国チャイルドトラスト（解説は伊井（2010）あるいは英国チャイルドトラスト公式サイト http://www.childtrustfund.gov.uk/ を参照）のように，口座残高に税金はかからないようにすることは必ずしも必要ないが，税金をかければその使途は限ることが望ましい。

企業からの利用料等の代理徴収，個人への利益配当等の支払いは既存金融機関のシステムに乗せればよい。ここで，「代理」とは信託を受けた個人の代理という意味である。

（5）「情報銀行」構想

「情報銀行」構想という，携帯電話会社や検索会社などに断片的にたまっている個人情報を効率よく利用し，個人向けサービスを向上させるという方法が提唱されている。官民で検討され始めていると報道されている（フジサンケイ（2010））。この銀行には，個人口座ごとに情報が名寄せされており，企業が利用料を払って情報を入手する。情報が使われた個人には利子（報酬）が支払われるという。

企業は個人の情報を名寄せして，体系的に整理したいと考えている。本人の手（これは，「意思」と解釈される）で情報を名寄せして，一つの口座に集約する形にする。

「情報銀行」構想でメディアに公表されている論点は，以上である。これらは本稿の一部と類似の考え方と同じ内容を含んでいる。「情報銀行」構想では，企業側に蓄積されている個人情報を企業も提供する。少なくとも過去の個人情報については，そうせざるをえないだろう。

（6）その他の論点

その他の論点として，いくつかある。バーチャルトラスト会社は自社から起こった情報漏れに対しては完全に責任をとることが求められる。しかも，賠償方法など，その対処方法全般，さらには再発防止策策定の方法，は事前に公表しておくべきである。

また，Laudon（1993）が主張したように，このような業務をおこなう信託会社が支払う税金は目的税的に，この分野のインフラ整備に使われる必要がある。

５－２　匿名化処理の一例

匿名化処理技術として暗号学者が考案した閾値秘密分散技術が見込みあると予想されている。秘密分散技術（電子的割符）は，個人情報・企業機密情報といったクリティカルな情報を保管・移送する際の手段として，これから広く普及することが期待されるセキュリティ技術の一つと看做されている。

原情報をＮ個に分割し，Ｎ個すべてが揃わなければ原情報と同じ情報を復元できない技術は完全秘密分散とも言われる。他方，閾値秘密分散では，原情報をＮ（例えば３）個に分割し，そのうち例えば（Ｎ - １）個が揃えば（例えば３分割片のうち２分割片を集めたら）原情報と同じ情報を復元できる。

秘密分散技術を用いて個人情報を保管する場合，適切に分散保管された分割片は個人情報とはみなさないという法的見解がある。このような法的見解もあり，秘密分散技術を用いれば，個人情報を取り扱う企業・組織にとっては，従来のセキュリティ技術を使った保存利用とは一線を画した個人情報保存システムの運営や低コストでのシステム構築ができる可能性がある。

閾値秘密分散技術の実際の利活用のためには，復元に必要な分割片（復号キー）を容易に集められない（盗まれない）ような保管方法が重要となる。例えば，既述の電子情報利活用推進部は，①復元に必要な情報を原則，ユーザーだけが知っている状況を作り出す，②復元に必要な分割片を容易に集められない状況を作り出す，という２点を容易に実現できるようにする，と主張する。そして，原情報を３個に分割する方式をとり，原情報を復元できる２分割片のうち１つ（の復号キー）を協会が預かることを提案している。

復号キーの１つを預かるのが，なぜ，当該財団法人でなければならないのかの議論は不明である。バーチャルトラスト会社が預かることも，可能性として，否定できない。

５－３　個人情報の保護とその活用を同時に行うシステムの一例

個人情報の保護と活用をバーチャルトラスト会社が効率的に行えるシステムを，考えてみよう。近い分野の研究である国米・貝沼・古原（2005）やセキュリティを考察した辰巳（2011a）などが参考になる。

なお，国米・貝沼・古原（2005）では，パス・ピクチャー（事前に設定した幼馴染の顔写真や故郷の写真）を選んでクリックして個人認証する方式を主張しているが，この個人認証方式を利用することはシステムの運用にとって必須ではない。他の堅固な認証方式を用いれば十分であるように思われる。

５－３－１　素描

（１）システムの概略

バーチャルトラスト会社内のシステムは，インターネットなどのネットワークから分離し独立した実名管理部門とネットワークに接続された匿名管理部門の２部門からなる。匿名管理部門は，それゆえ，IP アドレス[7)] を持つ。実名管理部門は完全なセキュリティが維持されなければならない。しかも，実名管理部門は数限られた者しかアクセスできないようにする。

---

7)　インターネットに接続している全端末に割り当てられる識別番号である。国や地域によってどういう番号が付くのか決まっている。０から255までの数字を４回組み合わせる。そのため，総数は256の４乗で約43億個に過ぎず，次のシステムが課題となって久しい。

すべての個人情報は実名管理部門でまず蓄積される。そして，匿名化などの処理の後，匿名管理部門へ渡される。それゆえ，匿名管理部門では，個人はすべて仮名で管理され，（許された者だけの）公開 DB となる。

契約した個人は，両方の部門に条件付きでアクセスできる。しかしながら，匿名管理部門の担当者はすべての処理を匿名で行い，誰が誰なのかを知らない。課金（請求書発行）部門はそのなかに属し，その担当者は個人の情報を持たない。

個人情報やその実名と仮名を照合するリストは権限分散型セキュリティなど（辰巳（2011a）などを参照）によって厳重に保管される。

（2）匿名管理部門とバーチャルトラスト会社

匿名管理部門では，情報は許可された者の間で共有される。許可された者のなかには企業が含まれる。匿名管理部門のなかに保管される個人情報は，プライバシーのレベルによって幾つかの領域に分けられる。企業は分析に使う目的で特定の領域へのアクセスが許可される。

バーチャルトラスト会社は，本人に代わって，匿名化情報を利用したい企業とコミュニケーションをとる。

（3）個人の権利とプライバシー委員会

個人は，基本的に両方の部門にアクセスできるが，アクセスの前に認証を受けなければならない。匿名本人認証を通過すると，該当のすべての詳細情報を閲覧できる。

バーチャルトラスト会社のなかに，プライバシー委員会が設けられる。個人は，必要があれば定期的に自己情報の修正を申告でき，当該委員会が内容を検討して，修正するべきかどうかを決定する。このような形で自己情報の自己管理権を維持できるようにしている。

また，本人が希望すれば，どの領域までのアクセス許可者であれば実名の公表を許すか，の希望を申告し，委員会の決定を待って，実現できる。

（4）個人情報の活用

フィルタリングされて抽象化された個人情報データや匿名の履歴情報は，このような２部門システムによって，データ分析に有効に活用できる。

５－３－２　いくつかの分析

（1）２部門分割体制の意義

２部門分割体制を採るのは，一種のバックアップによってセキュリティを維持するためである。バックアップを有効にするために，ミラーリング（定義などは辰巳（2011a）などを参照）される必要がある。

DB を１つ（一部門方式）にして，情報はすべて一括して暗号化し，そこに蓄積し，許可された者が復号して閲覧する際には特定のツールを使うことを許す，という方式も考えられる。しかしながら，この方式はセキュリティとプライバシー保護の両観点で劣ることになる。

例えば，ケータイについては，サービス形態上では匿名であると謳っていても，通信事業者との契約が保存され，誰が使っているかが分かっている状態にある。このような状況では，プライバシー保護は原則的に達成できない。ところが，ここまで記述してきたシステムにおいては，バーチャルトラスト会社の職員であっても，匿名管理部門において管理等の事務を行うにすぎないので，ほとんどの職員は個人情報を知らないことになる。

（2）匿名化の範囲

個人名が匿名化されるだけでは，住所，年齢などから，個人名が判明する可能性が高い。そ

れゆえ，付随情報も，何らかの匿名化・記号化を行う必要がある。変換ルールは許可された分析者だけに提供する。

６　バーチャルトラストは諸問題をどう解決するか

専門のバーチャルトラスト会社が業務を行うことのメリットとしてはいくつか考えられ，二律背反，モラルハザード，セキュリティとの矛盾，犯罪の隠匿，などのプライバシーの諸問題を解決できる可能性がある。日本には，まだ，公的あるいは民間のプライバシー保護団体は存在しない。バーチャルトラスト会社は，NPO ではない，プライバシー保護を行う民間の会社として，どのように活動するのか，説明してみよう。

６－１　プライバシーの二律背反問題

バーチャルトラスト会社は，個人情報を積極的に，しかも正当に企業に提供することを本来の業務とする。個人情報を必要とする企業に販売しなければバーチャルトラスト会社の経営は成り立たない。

しかも，バーチャルトラスト会社は事前に属性情報（性，年齢，職業，趣味等）を利用したい企業に提示することで，企業はより精度の高い情報が得られる。つまり，このようにして，プライバシー問題の二律背反を緩和することが期待できる。

バーチャルトラスト会社が行う事前提示やモニタリングによって，どのようなサービスにどのレベルの属性情報が利活用されるかがチェックできる。個人側に立つ主体・組織がこれを行わねば個人の利益に直接繋がらない。しかも，プライバシー保護の視点があって初めて，提供できる個人情報の限界がわかる。どのような個人情報をどこまで提供するか，どのような形で提供するか，という境界がわかる。

６－２　プライバシーのモラルハザード問題

個人は，バーチャルトラスト会社から，それが行う分析情報の提供を受けることができれば，自身のプライバシー傾向やサービス嗜好について把握できるようになる。個人側に立つ主体・組織がこれを行うから，これが可能になる。

これによって，プライバシーのモラルハザード問題も解決できる。既述のように，プライバシーのモラルハザード問題は微妙な問題を抱える。ある個人のプライバシー傾向が，時系列的にどう変わったか変わっていないかを追える，クロスセクション的にどれだけ偏った考え方かがわかる，という点がモラルハザード問題の解決には，重要であるように思える。

また，これらを統一的に捉える立場の組織や人の存在が必要になる。その役割をバーチャルトラスト会社が果せるのではないか，と思う。バーチャルトラスト会社が捉えている自身のプライバシー傾向を無視して，個人は唐突にプライバシーを主張できない，と思われる。

個人の側に立ってプライバシー保護をしながら情報提供活動するバーチャルトラスト会社かあるいは第三者機関であるプライバシー・コミッショナーかのどちらか，あるいは両者が介在してモラルハザード問題は解決できるようになると思われる。

ちなみに，プライバシー・コミッショナーという組織は，プライバシーに係る様々な問題を

判断する役割を担って，原則として政府から独立して設立・運営される[8)]。社会におけるプライバシー問題全体の調整や判断を下す役割として規定される。主に欧州やカナダで採用されている。

６－３　セキュリティとプライバシー保護の矛盾を解決するのは

セキュリティとプライバシー保護の矛盾をバーチャルトラスト会社がどのように解決するのか，このような問題に対してなぜバーチャルトラスト会社が必要とされるのか，を考えてみよう。

セキュリティとプライバシー保護が矛盾する問題を解決するには，いくつかの段階と方法がある。まず，例えば監視カメラを例にすると，どういう場所では何を撮ってはいけない（もし公表することがあったとしたら画面の何を隠すべきか），誰のどういう権利を守らなければならないか，という大原則が確立されなければならない。その確立に，国や地方公共団体は，リーダーシップをとっていく役割を果たす必要がある。

また，例えば警察カメラの設置と運用に関しては，一般の人が簡単には口を出せないので，しかるべき権限を持った組織が，撮られる側を代弁して，しかるべき主張をしていくことが大切である。

これは，交渉仲介者が必要であるということである。その役割をバーチャルトラスト会社が果たせる。個人に代わって（その委託を受けて）交渉の専門家となるわけである。

６－４　プライバシー情報の最適供給問題

バーチャルトラスト会社はまず主としてプライバシー情報の最適供給問題を解決するように，最適にデザインされなければならない。これは経済・金融エンジニアリングの仕事である。

比較的簡単な一例をあげてみよう。『日経ビジネス』では週１回「「会長／社長，役員」が読んだ今週の記事 TOP20」や「「女性」が読んだ今週の記事 TOP20」を掲載している。これは無料会員登録の際の個人情報を使って記事をまとめている。確かに個人の識別はできない。しかしながら，バーチャルトラスト会社は原稿料相当分を徴収するべきである。ちなみに，商業雑誌では原稿料は１字10円から20，30円の範囲で，学術論文では多くの場合約1000人のアンケート結果から，結論が出される。

それに対して『日経ビジネス』側は記事掲載料・閲覧料を要求するかもしれない。それゆえ，徴収する料金は交渉になる。

さらに，いくつか論点があるので，解説しておこう。

個人情報を企業が取得する時点では，まだその経済価値は実現していない。それゆえ，それが実現した時期以降に料金をチャージする必要がある。しかしながら，その経済効果が超長期に渡る場合には，最初の時点で予想将来価値を徴収するようにするべきであろう。

課金対象先産業の市場構造を無視して，課金するべきではないだろう。つまり，独占企業がデータを利用しているならば，例え，それがつけている価格が独占価格であり，製品価格が高め，仕入れ価格が低目であっても，その企業の製品価格に基づいた課金を行うことにするべきであろう。

---

8)　しかしながら，この制度も必ずしも万能ではない。本当に実効性があるのか，それを担保するにはどのような法制度と運用体系が必要なのか，さらに大きな問題としてコミッショナー自身の暴走をどう抑止するのか，が課題である。こうした議論は以前からも繰り返されており，実際に米国や日本ではコミッショナー制度は導入されていない。クロサカ（2010）参照。

個人情報に付加価値を付ける企業の意欲を削いだり，その意図を無駄にするようなプライシングは避けるべきである。金の卵を産む鶏は殺すべきではないのである。

６－５　プライバシー保護の管理の問題

バーチャルトラスト会社は利用状況並びに利益配当等の報告（通帳管理）を統合して行う。金銭出納や評価を同時に扱って，つまり統合管理を行って初めて有効な管理ができる。

何かあったら出動する，あるいは訴えがあって初めて動き出す第三者機関では，プライバシーの保護は厳密にはできない。プライバシー保護の管理は，事前から，事柄・情報のほとんどを把握し，金銭や評価を扱っている組織が担わなければならないのである。

バーチャルトラスト会社は，コンプライアンスが当然重要である。顧客が犯罪を犯した場合にはバーチャルトラスト会社は警察・司法に対して当該個人の情報をすべて提供するべきである。個人との信託契約時には，事前にこのことは伝えておくべきである。逃亡している犯罪者は，結局，バーチャルトラスト会社に連絡を取らなくなる。それゆえ，逃亡犯罪者は当該プライバシー保護制度から守られない。このようにして，逃亡犯罪者とその他の善良な市民や犯罪更生者を厳に分けることができる。

７　新しい仕組みのコンファメーション～まとめ

最後に，以上で提案するような仕組みは維持できるのか，考察することにしよう。日本のケータイ産業は，クロサカ（2010）によると，一般社団法人モバイルコンテンツ審査・運用監視機構（EMA）を介在させたサービスのフィルタリングで，プライバシー事件などの解決を図ろうとしてきた。EMA による審査結果を踏まえて，通信事業者がサービスのフィルタリングを行うという方式である。しかしながら，警察庁の報告では，EMA 認定サイト（認定を受けることによりフィルタリング対象外となる）に起因する事犯が約５割に達していると指摘されており，この仕組みは機能していない，と主張する。私見によると，業者側に立ち過ぎた結果であるように，思われる。事業者の社会的責任に訴えることによって解決しようとしても万全ではないのである。

企業が個人に支払う情報提供料は，企業あるいは仲介事業者が無料のアプリケーションを提供する形になるかもしれない。プライバシー情報を取得するためにアプリをフリーにするのは，アンダーセン（2009）に近い考え方であり，一部了解できる。しかしながら，既述のように，それを完全に了解するためには正当な対価なのかどうかを評価する必要がある。しかも，たとえ正当な対価になっていても，個人に残るものは少ない。例えば，個人は全体の分布と自分の位置を知りたいが，このような情報提供はフリーだけでは満たされそうもない。しかも，このようなフリー方式は本稿が詳述したプライバシーの諸問題を解決しない。

情報の扱い方の基準を決める，第三者機関として，有識者による「プライバシー・コミッショナー」を設ける必要があると考える人は多い。もしプライバシー・コミッショナーが設置されるならば，バーチャルトラスト会社はプライバシー・コミッショナーの管理監督下におかれるが，両者の権限や分担など関係については検討するべき事柄が残される。いずれにしても，バーチャルトラスト会社かプライバシー・コミッショナーが介在しなければ，プライバシーのモラルハザードは解決しない。

バーチャルトラスト会社のような新しいタイプの事業者が，その情報提供に対して個人に提

供料を支払うならば，そうしない事業者は同じオープンなプラットフォーム上でビジネスを続けることはできなくなるだろう。このようにして，バーチャルトラスト会社の業務が認められ，拡がり，個人情報のセキュリティも，守られる。

付録：　残された研究課題の要約

いくつか大きな研究課題が残されるので，それらを要約しリストしておこう（順不同）。

①個人情報を，まず，匿名化処理（非識別化処理とも呼ばれる），集計処理（集計データ群から個別データを逆推計できないようにする方法），秘匿処理する，必要がある。これらをどう行うかは，どちらかというと，暗号学，統計学，などの学問的な問題であり，それを経済学的に捉えなおす必要がある。

②どの段階で，どこまで，これらを行うか，も大きな問題である。個人は，どのような情報であれば，どこまで公開を許すか研究調査する必要がある。本文３－１（１）で説明した個人の特性を含めて，これらを探るのが，大きな課題になる。

③バーチャルトラスト会社は，プライバシーの諸問題（二律背反やモラルハザードなど）をどう解決できるか，どう解決するべきか，をさらに具体的に考察する必要がある。

④個人情報の価値を評価するプライシングが一番大きな，しかも困難な業務になる。これが，取引条件の交渉に用いる売値になる。課題は良いプライシング・モデルを作ることである。企業が個人に支払う情報提供料は，企業あるいは仲介事業者が無料のアプリを提供する形になるかもしれない。プライバシー情報を取得するためにフリーにするのはアンダーセン（2009）に近い考え方であるが，それが正当な対価なのかどうかを評価する必要がある。

⑤企業が破綻に直面している場合あるいは赤字が続いている場合，集められた個人情報は管理が等閑になる。等閑になるだけでなく，密かに売却し，資金の足しにすることもある。このような場合誰がどのように管理するべきか。バーチャルトラスト会社はこれに対してどのような役割をはたせるのか，法的に考察する必要がある。

⑥生産性を相互に上げる情報は相互に公開するのが社会的に最適であることは分析されているが，企業の秘匿する情報としての特許と個人のプライバシー情報はどう異なるかの比較研究をさらに具体的にする必要がある。

⑦情報の扱い方の基準を決める，第三者機関として，有識者による「プライバシー・コミッショナー」を設ける必要があると考える提案は多い。もしプライバシー・コミッショナーが設置されるならば，バーチャルトラスト会社はその管理監督下におかれるが，両者の関係については検討するべき事柄が残される。

なお，本研究で取り扱わないが別の課題としては，わが国の信託法で，バーチャルトラストはどのような取り扱いになるか，がある。法律上残された課題は，信託財産のなかに，個人情報を入れる。第二に，受託者が負う義務にプライバシー関連の義務を入れる，ことである。しかし，本研究では課題をあげるに止まり，信託法改定方法を研究対象にしない。

⑧ Privacy Preserving Data Mining（PPDM）技術の展望を経済学的に行う必要がある。

参考文献

アンダーセン，クリス（2009）『フリー：無料からお金を生み出す新戦略』NHK 出版，2009年11月。
伊井哲朗（2010）「子どもの将来に日本版チャイルドトラスト」『読売新聞』，2010年７月27日。
池末成明（2009）「ネット・メディアの収益モデルを再構築せよ」『日経コミュニケーション』2009年

10月１日号，pp.80-81。
石井夏生利「ライフログをめぐる法的諸問題の検討」『情報ネットワークローレビュー』第９巻第１号，2010年６月，pp.１-14.
国米仁・貝沼達也・古原和邦（2005）「個人情報の保護と活用を両立する情報通信プラットフォーム」『日本セキュリティ・マネジメント学会誌』，第19巻第１号，2005年９月，pp.３-14。Downloadable
クロサカ タツヤ（2010）「「通信の秘密」は金科玉条のごとく守るべきなのか？再燃するケータイにおけるプライバシー問題」『日経ビジネスオンライン』，2010年11月11日。
辰巳憲一（2011a）「金融・経済活動における情報などの分割，バックアップと情報セキュリティ～金融セキュリティの経済学入門（Ⅰ）～」『学習院大学経済論集』，2011年１月，pp.301-321。Downloadable
辰巳憲一（2011b）「データや情報のプライシングについての考察～ベンダーの行動と産業構造分析～」未公刊，2011年９月。
堀越　功（2009）「NTT ドコモが巨大マイニング設備構築」『日経コミュニケーション』，2009年10月１日号，pp.30-31。
フジサンケイ　ビジネスアイ「情報銀行で高まる個人サービス　柴崎亮介・東大教授に聞く」『SankeiBiz』，2010年11月24日。
牧野二郎（2010a）「［ライフログ全体像］イノベーションを起こす法律運用を考えよ」『日経 ITpro』，2010年４月６日。
牧野二郎（2010b）「［ライフログ最大の課題］プライバシー問題を乗り越えるヒント」『日経 ITpro』，2010年７月１日。
松浦龍夫（2010）「「モバゲー監視の状況はいかに」，総務省 青少年 WG で DeNA が説明」『日経ニューメディア』2010年10月４日号，17ページ。
日経コミュニケーション編『ライフログ活用のすすめ』日経 BP 社，2010年６月。
日経 ITPro「「個人情報漏えいは論理的にあり得ない」セールスフォース宇陀社長」『日経 ITpro』，2010年６月４日。
高崎晴夫・小野智弘・土生由希子（2010）「パーソナル情報を利用したおすすめサービスに対する消費者の受容性調査について」日経コミュニケーション（2010）の第４-３節。
高崎晴夫「パーソナライゼーションサービスにおける個人情報保護について」『情報ネットワークローレビュー』第９巻第１号，2010年６月，pp.67-78.
J-CAST ニュース「「店舗情報勝手に載せないで」佐賀県の飲食店が「食べログ」提訴」『J-CAST ニュース』，2010年９月10日。
Kamien, M. I., Muller, E. and Zang, I.,（1992），“Research Joint Venture and R&D Cartels,” *American Economic Review*, 82（５）, pp. 1293-1306.
Laudon, K. C.,（1993）“Markets and Privacy,” New York University Center for Digital Economy Research Working Paper, IS-93-21DP, December 1993. Downloadable