PRIVACY-ENHANCED PERSONALIZATION

プライバシーを高めたパーソナライゼーション

Alfred Kobsa

パーソナライゼーションとプライバシーとの対立を解消させるため，多面的戦略が求められている．

インターネットユーザは，パーソナライズ化されたコンテンツを重視することが，消費者に関する調査によって明らかになった．こうしたパーソナライゼーションをウェブサイトで提供することは，ウェブベンダにとっても大変有益である．つまり，この二者の間には Win-Win の関係が成立する．しかし，この Win-Win の関係は，潜在的なプライバシーへの脅威によって損なわれている．なぜなら，人々のやりとりをパーソナライズ化するためには，膨大な個人情報を集めなければならないからである．消費者に関する多くの調査が明かすように，コンピュータユーザはオンライン上でプライバシーが侵害されていないか，とても不安に感じている．パーソナライズ化されたサービスに関する不安としては，例えば次のようなものがある．以下に述べる最初の 3 つは現実に起こっていることであり，4 番目は将来起こりうることである．

・過去に購入した本の情報を元に，個人に合った本を推薦している書店がオンライン上にある．この書店を利用しているユーザは，購入履歴が本当に秘密にされているのか疑問に思うかもしれない．

・サーチエンジンの中には，入力されたクエリを保存し，個人個人の関心に合った検索結果を返すものがある．このサーチエンジンを利用しているユーザは，以前に検索した単語が記録されていることに不安を感じているかもしれない．

・パーソナライズ化された個人指導システムは，学習者の理解度に基づいた詳細なモデルを構築し，個々学習者に適した教育を提供している．このシステムを十分理解している生徒は，システム以外の誰かが，自分が何を知り何を知らないかという情報にアクセスするのではないかと心配するかもしれない．

・個々の文書処理能力のモデルに基づき，それぞれのユーザに適したアドバイスを提供するワードプロセッサが今後登場する可能性がある．このようなワードプロセッサを利用する会社の社員は，文書処理能力を解析するモデルの内容が社内に漏れ，特に，彼が持っていないスキルが開示されることによって不利な結果が生じないか懸念するかもしれない．

他にも，パーソナライズ化されたシステムにおいて，プライバシー侵害の可能性を考えなければならないケースとして，次のようなケースが考えられる[4]．頼んでもいない売り込み，ユーザについて「理解する」コンピュータ，パーソナライズにより価格差別される恐怖，同一のコンピュータを使用している他のユーザへの情報漏洩，権限の無いアカウントへのアクセス，裁判所による召喚礼状，政府の監視などである．

個人のプライバシーへの不安に加えて，個人データの収集は，業界行動規範はもちろんのこと，多くの国や州（国境を越えた範囲に及ぶ法律もある）での法的規制にも縛られている．ユーザの懸念とプライバシー規制の双

方がデータ処理方法に影響を及ぼすように，収集するデータの種類にも影響を及ぼしている．

既存のパーソナライゼーション技術では，ユーザに関する小規模なデータでパーソナライゼーションを行っても，ほとんどの場合，良い結果が得られない．このため，今世紀半ばには，プライバシーとパーソナライゼーションとのトレードオフの存在が必要となると考えられている．また，これらをバランスさせる必要があると考えられている．この考え方は，例えるならば，パーソナライゼーションが使われれば使われるほどプライバシーが守られるようになるといったことである．またその逆も然りである．

しかし，プライバシーの観点から，パーソナライズ化されたシステムを受け入れることができるかどうかを考えた時、プライバシーやパーソナライズ方法だけでなく，他の多くの要因が存在することが最近の研究からわかった．さらに，プライバシーとパーソナライゼーションを分離して考えた場合においても，同等のパーソナライゼーションを実現するために，従来手法よりもさらにプライバシーを向上させたパーソナライゼーション手法が存在するようである．プライバシー重視のパーソナライゼーション（privacy-enhanced personalization）[9,10]の分野は，ユーザモデリングの目的や手段とプライバシーを考慮したパーソナライゼーションを両立すること，そして，プライバシーを脅かさない範囲で，最大限のパーソナライゼーションを発揮することを目指している．この研究分野は，広く異なった学問分野にまたがっており，情報工学，情報システム，マーケティングリサーチ，公共政策，経済学，法律分野からの貢献が必要である．この記事は，パーソナライズ化されたシステムを設計するためにこれまでに行われてきた調査・研究の主要な成果と示唆をまとめたものである．

プライバシー度(The Privacy Calculus)

現在のプライバシー論では，まず個人情報の開示によって得られる利益と，発生しうるリスクを比較検討する．そして，個々の状況に応じたリスク対効果の分析を行い，個人情報を開示するかどうかを決定する．しかし，インターネットユーザはしばしば，プライバシーに関連する決断を行うだけの十分な情報を持ち得ていない．例えば，ユーザは，特定のデータが開示されることによって，身元を特定される可能性を軽視している．また，プライバシー保護方針は理解が難しく，滅多に読まれないため，サイトのプライバシーへの取り組みに馴染みがない．複雑な予測に基づいた決定と同じように，プライバシーに関する決定も非合理的な考えによって脅かされている．例えば，Acquisti[1]は，プライバシーに関する決定を，一時的に合理性を欠いたまま行ってしまう可能性を危惧している．合理性を欠いた決定によって，僅かな目先の利益に目が眩んで個人情報を開示し，その結果，プライバシーが脅かされ，長期的には不利益を被るかもしれない．

インターネットユーザのプライバシー度を測るにあたって，考慮すべき要因は多い．これらの要因として，人格や文化に基づくプライバシー属性や，開示される情報の種類がある．他にも，個人情報が一般的な平均からどの程度ずれているか，情報の受信者が誰であるか，パーソナライゼーションから得られる利益がどの程度か，何の情報が開示されているのかをユーザがどの程度知っているか，また個人情報の使用をどの程度コントロールできるか，など信用を確立するための様々な要因が存在する．これらの要因をより詳細に記し，プライバシーを高めたパーソナライズ化されたシステムの設計の重要性を論じる．

個々のプライバシーに対する考え

様々な調査によって，インターネットにおけるプライバシーへの関心の程度が，年齢，知識，収入と明確に関連していることが明らかにされている．しかし，性別による違いは明らかになっていない．1980 年代前半から始まったいくつかの調査では，回答者は大まかに 3 つのグループに分類される．まず，*プライバシー原理主義者* (Privacy fundamentalists)は，たとえプライバシー保護が適切に行われていたとしても，概してデータの利用に極度の関心を示し，情報の開示を好まない．次に，*プライバシー無関心者* (Privacy unconcerned)は，プライバシーへいくらか関心を示しており，他の人や組織が彼

らの情報を使うことをやや心配している．最後に，*プライバシー現実主義者*(Privacy pragmatists)も大抵は同様に，プライバシーへの関心を持っているが，プライバシー原理主義者ほどではない．彼らは積極的に個人情報を開示しようとする．たとえば，個人情報の使用目的を理解したならば，個人情報を開示することで得られる利益を見いだそうとし，適切にプライバシーが保護されるか検証しようとする．これら３つのグループの人数比は，おおよそ 1:1:2 の割合であるが，正確な数は調査，そして調査を行った年代によって異なってきている．過去 20 年においては時間とともにプライバシー原理主義者とプライバシー無関者がわずかに減少し，それに対応してプライバシー現実主義者の数が増えている．

かし，インターネットでの行動履歴や購入品，広義での人口統計上の詳細情報を開示することはあまり望まない．金融情報，連絡先，特にクレジットカードや社会保障番号は最も公開したくないプライバシーに挙げられる．Huberman ら[7]による実験によると，データの種類の違いだけではなく，公開するデータが，グループ平均からどれだけ離れているかも個人情報の開示に影響を与えている．このことは，年齢，体重，収入，配偶者の収入，信用格付け，貯蓄額で証明されている．特徴が標準から離れるほど，プライバシーとしての価値が増すと，Huberman らの実験結果は示している．

パーソナライズ化されたシステムの設計に関するこれらの教訓によると，ここで論じたような情報開示への抵抗を和らげる要因が無

多くのプライバシーに関する調査によると，インターネットユーザは，個人情報がどのように使われているかを知り，その使用をコントロールすることが重要だと考えている．

しかし，こうしたプライバシーに対する態度に基づいたグループ分けの精度は低い．いくつかの調査[8]によると，個人情報を開示するかしないかを決定する際に，プライバシー原理主義者は，ほかのグループと，それほど変わらない決断をすることが明らかになっている．抽象的できちんとした理由もなく，開示を求められたから開示するという態度の人よりも，具体的なプライバシーに関する決意を持って開示する人の方が多いことが，各グループ間の境界が曖昧になっている大きな要因のようである．幸運にも，パーソナライゼーションの設計者はプライバシーを高めた設計によって，これらの要因を改善することができる．

開示される情報の種類

いくつかの調査において，インターネットユーザは一般的に，情報を開示するとき，情報の種類によって異なった感情を抱くことが確認されている[8]．彼らは大抵，個人的な嗜好や趣味と同様に，基本的な人口統計や生活様式の情報を開示することはいとわない．しいならば，ユーザが公開したがらない個人情報を要求すべきでない．個人情報を要求するとき，個人情報が一般的な平均値から大幅に外れた値ならば，細かく区切られた区間から選択をさせるのではなく，おおまかに一定の値よりも大きいか小さいかだけを要求すべきである．たとえば，成人男性の「体重:250 ポンド以上」というようにするとよい．

パーソナライゼーションの価値

最近の調査では，インターネットユーザの 80%がパーソナライゼーションに興味を持っている．今日，研究者は多くのパーソナライゼーションサービスを研究しており[2]，それらは様々な利益をもたらすであろう．しかしユーザはこれまでのところ，それらのうちの僅かしか評価していないようである．評価されているものはといえば，時間の節約や金銭の節約である．他にも，ユーザに応じたカスタマイズされたコンテンツの提供，ユーザの好みの記憶が高く評価されている．Chellappa と Sin の発見によると，「消費者がパーソナライゼーションサービスの使用を

決める要因の多くは，パーソナライゼーションの善し悪しであり，プライバシーに対する心配はその半分以下しか影響しない．このことは，ベンダがプライバシーをある程度守っている限り，パーソナライゼーションの質を向上させることによって利益を得られることを意味している」[3].

これらの結果から分かるように，パーソナライズ化されたシステムの開発者は，サービスの利点をユーザにはっきりと伝えるべきであり，これらの利点が本当に求められていることを確かめるべきである．もし，ユーザがパーソナライズ化されたシステムの良さに気付けば，システムをより頻繁に使用するようになり，必要な個人情報をもっと提供してくれるだろう．

伝統的なプライバシー保護方針を越えた取り組みのためのコミュニケーションフォーム（www.privacyfinder.com と[11]より）

個人情報の使用に対する意識と管理

多くのプライバシーに関する調査によると，インターネットユーザは，個人情報がどのように使われているかを知り，その使用をコントロールすることが重要と考えている．ある調査によれば，ウェブサイトが持っている全ての個人情報を知る権利がユーザにはある，という考えに 94%の人が同意している．虚偽の情報をウェブサイトに提供したり，情報を提供することを断る人もいる．別の調査によると，これら人々の 63%は，情報がどのように使われるかを開示する前に予め知らされていて，それに納得したなら，情報を提供していたと答えている．ある行動実験[11]によると，ウェブサイトが，要求するデータそれぞれに対し，ユーザが得られるメリットやサイトのプライバシーに関する取り組みを説明すると，個人情報の種類に関わらず，ウェブサイト訪問者は，より重要な情報を開示するようになる．他の研究によると，69%の人が，何の情報が集められているかを管理することは極めて重要であると述べており，24%の人はやや重要であると見なしている．

これらの結果からわかるように，パーソナライズ化されたシステムがユーザに関するどのような事実や推測を保有し，どのように使おうとしているかをユーザに説明できなくてはならない．さらに，ユーザはこのデータの蓄積・使用を十分に管理する権利を与えられるべきである．こうすることによって，個人情報の開示を促進し，同時に多くのプライバシー法，業界や企業の規則，公正な情報取り扱い原則[1]を守ることにもなる．添付した図

は，Amazon.com における例である．この例では，レコメンデーションを作るために個人情報が使用されていることをユーザに知らせている．さらに，ユーザが個人情報の使用を管理することもできる（しかし，システムからデータを消去することはできない）．

信用

ウェブサイトの信用は，個人情報の開示において非常に重要な要素である．ある調査では，ウェブサイトに個人情報を送ることを拒んだ消費者のうち，63%近い人が，データを管理する人を信用できないことをその理由に挙げている．逆に，信用できるサイトならば，虚偽ではない本当の個人情報を開示しやすくなることも分かった．信用を得るための方法は，これまでに実験的に確立されてきており，それらの多くは情報開示へ効果があることが証明されている．

[1] 訳者注：Principles of Fair Information Practices

過去に良い経験があれば，ユーザの信用を得ることができ，個人情報の開示を促進することがわかっている．良い経験を与えることができれば，その効果は長期間継続する．そのため，パーソナライズ化されたシステムの設計者は，個人情報の開示をその場限りのものと見なすべきではない．現在よくあることだが，（あなたが最初にサイトを訪問した時に遭遇した，長くて，しかもほとんど全てのフィールドに*印が付いている登録フォームを覚えているだろうか？）．パーソナライズ化されたウェブサイトのユーザは，もし同じサイトあるいは似たようなサイトで良い経験をしたなら，時間が経つにつれて，もっと率直で詳しい個人情報を開示するようになるかもしれない．パーソナライズ化されたウェブサイトは，ユーザが開示することを決めた個人情報だけで少なくとも十分にパーソナライゼーションを活用できるように設計されるべきである．そして，ユーザがパーソナライズ化されたシステムに対して良い印象を持つようになったらすぐに，より多くの情報をユーザが提供できるようにするべきである．

ウェブサイトの設計と運営．以下に列挙するような様々なインタフェース設計の要素やウェブサイト運営上の特徴がユーザの信用を高めることが分かってきている．エラーをなくすこと，プロに設計されサイトが使いやすいこと，連絡先が明記されていること，信用できるウェブサイトからのリンクがあること，外部の情報源やデータへのリンクがあること，前回の訪問からアップデートされていること，カスタマサービスへの質問に迅速に回答すること，全ての取引をメールによって確認することなどである．それゆえ，パーソナライゼーションはなるべく専門的に設計された使いやすいウェブサイトで使われるべきである．そのようなウェブサイトには，信用を高める設計要素と運営上の特徴がある．

ウェブサイト運営者の評判．ウェブサイトを運営する組織の評判が，ユーザの信用と個人情報の開示に重大な影響を与えることがいくつかの研究でわかっている[8]．ある実験において，ユーザは，訪問者が少なくそれほど知られていないであろうサイトに，個人を特定できる情報（特に電話番号，住所，メールアドレス，社会保障番号，クレジットカード番号）をほとんど提供しようとしなかった．

パーソナライズ化されたシステムの設計の教訓によると，他の全ての条件が同じならば，ユーザは評判の悪い会社のサイトよりも，良いサイトで多くの個人情報を開示するようである．したがって，個人情報の開示を妨げない限り，パーソナライゼーションは，サイトの評判が高いほど多くの成功を収める．つまり，サイト設計者は，パーソナライゼーションの特徴を評判の低いウェブサイトの人気を増やすための「巧妙な仕掛け」として使用すべきでない．もしユーザがそのようなサイトで個人情報を開示しなければならないとすると，ユーザはそのサイトを利用しないかもしれないからである．

プライバシー保護方針の存在．ウェブサイトの伝統的なプライバシー保護方針（しばしばプライバシーポリシーと呼ばれる）は，プライバシーに関した当該サイトの取り組みを表す．ユーザの信用と情報開示への態度に与えるプライバシー保護方針の効果は，残念ながらまだはっきりしていない．プライバシー保護方針へのリンクが存在するだけで信用と情報開示の両方に良い影響を与えたと論じたいくつかの研究がある[8]．（しかし，悪い影響を与えたことを示す実験も１件あった）．しかし，プライバシー保護方針が提供する*保護の度合い*が，信用と情報開示に影響を与えるかどうかは，結論が出ていない．現在の「野放し状態の」プライバシー保護方針では，このようなことは起こりそうもない．なぜなら主要なウェブサイトのポリシーは，言い回しが難しいので多くのウェブユーザには理解できないことがいくつかの明解な分析で明らかになったためである．予想通り，ウェブサーバのログを解析すると，ごく少人数のウェブ訪問者しかプライバシー保護方針にアクセスしていないことがわかった（2 つの異なった情報源によると 1%か 0.5%より少ない）．

パーソナライズ化されたシステムを設計する上での教訓は，これまでのプライバシー保護方針では，たとえ優れた取り組みを記述しても，ユーザの信用と個人情報の開示の増加は期待できないということである．しかし，そのような声明を掲載することには他に適切な理由がある．というのは，多くの国では法

流行のパーソナライゼーション手法に影響を与える様々な欧州のプライバシー法の規定（Provisions from Various European Privacy Laws Affecting Popular Personalization Methods）

1. *トラフィックや位置データに基づいて価値を付加させる（例えばパーソナライズ化された）サービスは，そのようなデータの匿名化やユーザの同意を必要とする.*

この条項は，もしユーザが一意に特定されるなら，サーバとのログに基づいたいかなるパーソナライゼーションにもユーザの同意が必要だとしている.

2.*ユーザはトラフィックや位置データの処理に対する承諾をいつでも撤回することができなければならない.*

狭義の解釈では，この規定は，全てのトラフィックや場所に基づいたパーソナライゼーションの終了のための要求に，それがたとえ現在のセッション中でも，速やかに応じるためのシステムが必要だとしている．トラフィックや位置に基づいたパーソナライゼーションにおいて，ユーザが全てを承諾したり承諾しなかったりできる方法を用意するだけでなく，個人個人の要求に応じた承諾も行えた方がよい状況もある．たとえば，近くの名所について知らされることには同意したが，近くの企業の営利的な申し入れを受け取ることは拒否する場合などがあげられる.

3.*パーソナライズ化されたサービスの提供者は，ユーザの同意を得る前に，扱われるデータの種類，目的，扱う期間，第三者に伝わるかどうかをユーザに知らせなければならない.*

パーソナライズ化されたサービスの提供者にとって，あらかじめ特定のサービスについて明確に述べることは極めて難しいことがある．現在は，ユーザに関するデータをできる限り集め，蓄え，そしてデータに基づいたパーソナライゼーション手法（例えばルールに基づいたパーソナライゼーションやステレオタイプの活性化）を適用することが一般的である．内部の推測メカニズムも，ユーザについての推測を追加することによって，入手できる個人情報を増加させるかもしれないが，代わりに，より多くのパーソナライゼーション処理が必要となるかもしれない．そのような，事前に予測できる可能性が低いケースにおいては，プライバシー法における情報開示に必要な条件を満たすため，多くの典型的なパーソナライゼーションの例をリストアップすべきである.

4.*異なった目的のために入手した個人データはまとめてはいけない.*

この制限は，ユーザモデルを中央集権型のサーバで管理する場合に関係する．こうしたサーバは，パーソナライズ化された異なるアプリケーションからユーザ情報を蓄え，別のアプリケーションに提供する．しかし，こうしたサーバは，パーソナライズ化されたアプリケーションに，ユーザデータを，当初データ集めた時の目的と異なる目的のために提供してはならない.

5.*使用するデータは，セッションごとに即座に削除されなければならない*（非常に限定された目的を除く）.

この規則は，ユーザに関する付加的な推測をする機械学習を，複数セッションにまたいで実行するときに関係するだろう.

6. *データ主体に法的効力を与えたり，ユーザに著しい影響を与えたり，仕事の実績，信用力，信頼性，品行などのようなユーザ個人に関する特定の特徴を自動的に評価することは完全には認められない.*

これらの規定は，例えば，完全に自動的に成績付与を行う，パーソナライズ化された個人指導アプリケーションに適用される．これは，ユーザに著しい影響を与えるからである.

(欧州全体 = 1,2,3,6; チェコ共和国=4; ドイツ=5)

令の遵守や自主規制が要求されるが，声明を掲載することでそれらを守る意志を示すことができるからである．プライバシーに注意を払う企業の取り組みは，適切な形でウェブユ

ーザに伝えることができれば良い影響をもたらすことができる．例えば，プライバシーポリシーの P3P のバージョンを調べることによって，プライバシー保護の度合いを示すロゴ

USACM の勧告とプライバシー重視のパーソナライズされたシステムへの影響

最小化原則

1.プライバシーポリシーに述べられた目的のために必要な個人情報だけを正確に集めて使用すること．

2.記載された目的のために必要な情報だけを保存すること．

3.古くて不要な個人情報を無期限に保持するのではなく，正規の基準に則り個人情報を査定し削減させ破棄するための体系的なメカニズムを用意すること．

4.個人のプライバシーに影響を及ぼす可能性のある新しい取り組みや技術を使用する前に，注意深く必要性，有効性，均整を査定し，最もプライバシーを侵害しない代案を常に追求すること．

これらの要求にいささか矛盾するが，現在のパーソナライズされたシステムの暗黙的なパラダイムは，できるだけ多くのデータを集め「ストックし」，ストックされた利用可能なデータを用いてパーソナライゼーションを行うことである．一方で，多くのパーソナライゼーション領域における研究が大いく進歩した結果，収集された個人データは滅多にパーソナライゼーションに貢献せず，利用できるとしても必要とされなかったことが分かった．

同意原則

5.法律で免除されていない限り，個人情報を集めて共有するには，各人への明確なインフォームドコンセントが必要である（オプトイン）．さもなければ，個人が速やかに停止できるメカニズムをはっきりと用意しなければならない．[...] 適切な時に，情報を削除することも含まれる．（オプトアウト）

この原則は，ユーザの個人データに基づいたパーソナライゼーションは，いつでもオン・オフを切り替え可能なオプションがなくてはならないことを意味している．

開放性原則

8.いかなる個人情報が集められる時であっても，収集の正確な目的と全ての用途を明確に提示すること．[...]

10.情報がどれくらいの期間保存され使われるかを明確に記載し最小化原則と適合していること．

11.データを提供するかどうかや，どのように提供するかの決定権をもつ人に対して，これらのプライバシー保護方針を明瞭，簡潔かつ明白にすること．

ユーザが個人情報を開示しようとする際，このような説明をすることで生じるメリットはこの記事で述べられている．また，パーソナライゼーションの目的を完全に説明することの難しさは，ヨーロッパでの規定の補足的な注記で論じられている．

アクセス原則

14.法律で除外される場合を除き，保存された個人情報を調べて訂正する権利を規定し，支持すること．

この原則は，メインの記事で論じられているように，個人情報をオンラインで検査，訂正するメカニズムを要求している．

正確性原則

17.個人情報が所望の目的のために十分に正確で最新であることを保証すること．

18.全ての訂正個所は，誤ったデータを受け取った全ての関係者に対して，適宜かなった方法で確実に伝えること．

今までのところ，ユーザにデータの確認を認めることは，データの正確さを保証する唯一の解決策としてパーソナライゼーションの文献で採用されているようだ．データの陳腐化は殆ど注目されておらず，データの出所を保存すること，誤りを広めること，変更通知をデータの提供元へ送ることも総じてなされていない．

を使用したり，プライバシーポリシーの意味を詳しく説明する方法[11]が考えられる．前ページの表は，そのような戦略の例を示したものである．企業のプライバシーに関する取り組みをより良く伝える方法を見出すために，さらなる研究が求められる．

プライバシーマーク（privacy seal）の存在．いくつかの研究において，プライバシーマークの意味が現在のウェブユーザによく理解されていないことが指摘されている[9]．また，マークを授与するアメリカ最大の機関は，与える相手を詳しく調査せずに選定しており，マークを表示したサイトはマークがないサイトよりもプライバシーを侵害しやすいことが，他の研究で明らかになった[2]．それにもかかわらず，ウェブサイトでのプライバシーマーク掲載は，訪問者，特に訪問者のウェブサイトに対する信用，プライバシーポリシーの認知度，情報開示への意欲，に明らかな影響がある．実用的な結論として，ウェブユーザがプライバシーマークを信用している限りはそれを見せることで情報開示を促進する可能性があるということがあげられる．この結論は，パーソナライズされたシステムの設計者にとって有用であろう．

規定の取り組み

これまで，40 以上の国と多くの州がプライバシー法を制定してきた．多くの企業と産業部門が，追加のあるいは代わりの，プライバシーに関したガイドラインを採択した．これらの法律や自主規制は，個人情報の使用に関する公正な取り組みをより具体的にしたものが多い．パーソナライズ化されたシステムにおけるこれらの規制文書の効果をここにいくつか述べる．

プライバシー法．パーソナライズ化されたシステムは，個人情報を収集するので，もし各人が特定可能なら，プライバシーの法律や規則を守らなければならない．先に述べたように，40 以上の国と多くの州にはプライバシー法がある．これらの法律は，個人データや適用するデータ主体の保護のために，データの収集，保存，処理における，手続き，組織，技術に関する要求を規定している．一般にこれらの法律は，正当なデータの収集，移動，処理，データ主体の権利のための条件を含んでいる．他にも，十分なセキュリティのメカニズム，情報開示の義務，個人データ処理の監督や監査が定められている．

プライバシー法によって課された規定の中には，パーソナライゼーション手法の使用に影響を与えているものがある．いくつかの国際的なプライバシー法は，ユーザの同意無しで流行のパーソナライゼーション手法を使うことを禁じている．そのような規定は「流行のパーソナライゼーション手法に影響を与える様々な欧州のプライバシー法の規定」の補足に記されている．

公正な情報取り扱い原則．ここ３０年以上，収集におけるいくつかの基本的な原則が，個人情報を扱うときのプライバシーの保証のために明示されている．いわゆる，*公正な情報取扱い原則*が，オーストラリアやカナダのような多くの国で国家のプライバシー法の礎として，OECD や APEC のような超国家の組織において参加国の指針として，また ACM の

パーソナライズ化されたシステムにおいて，匿名性を保ったまま，完全なパーソナライゼーションを受けることは可能である．

ような専門の団体で為政者の忠告や会員の専門的な行為の手引きとして起草されている．

もしパーソナライズ化されたシステムの設計者が，適切なプライバシー法や産業，企業の指針を考慮していないなら，それらの原則を考慮しなければならない．多くの原則はパーソナライズ化されたシステムに直接的な影響を与えている．「USACM の勧告とプライバシー重視のパーソナライズ化されたシステムに与える影響」の補足は，ACM の合衆国公共政策委員会（ACM's U.S. Public Policy Committee）の提案をいくつか含んでいる．

[2] Benjamin Edelman's *Adverse Selection in Online "Trust" Certifications;* Harvard University, 2006; www.benedelman.org/publications/advsel-trust-draft.pdf.

パーソナライズ化されたシステムのプライバシーを高める技術

ここでは，プライバシー漏洩の危険を減らし，プライバシーの遵守を容易にするかもしれないいくつかの技術的な方法を論じる．これらは，パーソナライズ化されたシステムのプライバシー漏洩の危険に対する「完全な技術的解決策」では決してないし，それが存在することによってユーザのプライバシーへの不安を魔法のような力で消し去るかどうかも疑わしい．むしろ，これらの技術は，標準的な側面も考慮に入れたユーザ指向のシステム設計におけるプライバシー保護の一助として使用されるべきである．これらの技術はまだ研究段階であるが，それらのいくつかは実用的なアプリケーションに適用できそうだ．

ペンネームとユーザモデル．パーソナライズ化されたシステムのユーザが，匿名性を享受すると同時に完全なパーソナライゼーションを受けることは可能である[12]．パーソナライゼーション機能を有する匿名化システムにおいては，ペンネーム（pseudonym）をユーザへ付けることにより，当該ユーザを第三者から，特定されないように，関係付けできないように，観測されないようにするが，一方でペンネームを用いてパーソナライズ化されたシステムを利用できるのである．多くの人が，こうした手法の一部あるいは全部を用いて，ウェブサイトとのパーソナライズ化されたインタラクションを実現したペンネームを使ったインフラを提案している．そうした人の中には，インターネットユーザは身元が特定できない時の方が情報をより多く提供する傾向があり，パーソナライゼーションの質が高まり，ユーザが受ける利益も大きくなると期待する者もいる．しかし，これまでこの主張は実験的にあまり実証されていない．設計者は，ペンネームでのアクセスやユーザモデル（もし用意に利用できるなら上記の特性をもった匿名化の構造さえも）の使用を検討すべきである．これは，USACM の補足的な勧告で論じられた公正な情報取り扱い原則のデータ最小化と安全要求に基づいている．いくつかのプライバシー法も，もし技術的に可能で妥当ならば，ペンネームでのアクセスの準備を推奨したり命じたりしている．ユーザが通常の方法で特定できない時，ペンネームでのアクセスを用いると，多くの場合プライバシー法が適用されないことは思わぬ利点である．

関連研究が充実していないので，匿名性の増加が，より多くの情報開示とより良いパーソナライゼーションをもたらすかどうかははっきりしない．代金の支払い時や，物質的な商品，インターネットでないサービスがやりとりされている時に匿名性を保つことは，現在では難しくもあるし退屈でもある．それは，悪用の危険性をはらんでいるため，ベンダはクロスチャネル・マーケティング（例えば，ウェブ顧客に郵送で製品カタログを送ること）をしようとしない．最後に，研究によると，部分的に匿名なデータを特定することができるリソースに富んだ攻撃者によって，データベース入力・ウェブの訪問履歴・クエリの語・評価・原文のデータの匿名性は，驚くほど破られていることがわかっている．

クライアントサイドパーソナライゼーション．サーバサイドではなくクライアントサイドにユーザデータを保存することで，パーソナライズ化を実現させるシステムを，多くの研究者が研究している．同様に，ユーザデータに基づいて行われる全てのパーソナライゼーションは，専らクライアントサイドで実行される．プライバシーの観点から，この方法には２つの主な利点がある．

・たとえ保存されるとしても，極僅かな個人情報しかサーバには保存されないので，プライバシーの問題が少なくなる．実際，クライアントサイドパーソナライゼーションのウェブサイトは，ユーザを特定するようなデータを普通は扱わないので，ほとんどの場合プライバシー法に抵触しないだろう．

・パーソナライゼーションがリモートにデータを保存するのではなくローカルに保存して実行されるなら，ユーザはデータをより制御できると感じるため，もしかしたら個人情報をもっと開示したいと思うかもしれない．

しかし，クライアントサイドパーソナライゼーションには以下を含む多くの課題もある．

・一般のユーザモデリングやパーソナライゼーション手法は，協調フィルタリングや典型的な学習に基づいており，全てのユーザから得たデータを使った分析が必要である．このため，これらの手法は適用できないか，根本的に再設計されなければならない．

・たとえ，個人データをサーバへ一時的あるいは部分的に送信するだけでも，上に述べたクライアントサイドパーソナライゼーションの利点をふいにするかもしれない．そのため，パーソナライゼーション処理は，クライアントサイドで実行することが要求されるだろう．しかし，パーソナライゼーションで使われるプログラムコードは，極秘のビジネスルールや方法を組み込んでいることが多いため，権限の無いアクセスから保護しなければならない．この目的のため，信用できるコンピュータのプラットフォームが発達するに違いない．

もし，これらの障害が特定のアプリケーション分野で問題を引き起こさなければ，パーソナライズ化されたウェブベースのシステムの設計者は，適切なツールが利用可能になり次第，クライアントサイドパーソナライゼーションを採用すべきである．そうすることは，データ最小化原則の条項を守るための偉大な一歩となり（USACM 提案の補足を参照），ユーザの信用を拡大することにも繋がるだろう．

協調フィルタリングのためのプライバシー重視を高める手法．伝統的な協調フィルタリングシステムは，レコメンデーションを行う上での規則性を見つけるため，ユーザについての大量の情報を中央レポジトリに集める．例えば，ユーザの製品への評価，購入した製品，訪れたウェブページが該当する．これらの中央レポジトリはいつでも信頼できるわけではないかもしれないが，権限を持たない者にとって魅力的なターゲットとなる可能性がある．中央レポジトリは，巧妙に構築された個人データを用いてレコメンデーションを行うことによって，個人のユーザデータをマイニングすることもある程度可能である．こうした協調フィルタリングに基づいたレコメンデーションシステムを使用するユーザのプライバシーの保護に役立つ多くの手法が提案され，一部分は技術的に評価されている：

分散．この手法は，少数のユーザに関する情報だけを含む分散されたクラスタを相互に使用し，全てのユーザのデータを含んだ中央レポジトリを廃止する．

*暗号化されたデータの集約手法*により，ユーザ自身に自分の評価情報を自分自身で保持させ，同型暗号化と P2P を用いることで，それらの評価情報を開示することなく集計することができる．その結果，パーソナライズ化されたレコメンデーションは，ユーザが保持している評価情報を用いて，クライアント再度で生成できるようになる．

摂動．この手法では，ユーザの評価は，全ての協調フィルタリングを行う中央サーバに送られる．しかし，ユーザの本当の評価を隠すため，送信前に，評価は体系的に変更される．

難読化．ここで，ユーザの評価を協調フィルタリングのために中央サーバへ送る前に，一定の割合を異なった値に置き換える．ユーザは，データが漏洩した時には，データが正確ではないと言い張ることができる．

結論

プライバシー重視のパーソナライゼーション研究は，ユーザモデリングの目標や方法とプライバシーに配慮したパーソナライゼーションを両立すること，そして，プライバシー法によって決められた範囲内で，最大限のパーソナライゼーションを発揮することを目指している．この記事を通して説明したように，パーソナライズ化されたシステムのプライバシーを根本的に強化することができる抜本的な方法は技術的，法律的，社会的あるいは組織的に存在しない．代わりに，データの種類，ユーザ，パーソナライゼーションの目的が必要であると同時に，アプリケーション分野に依存した多くの小さな強化が導入されなければならない．ここに記載した手法の多くは，実際のシステムに使用可能であり，適用することで得られるフィードバックも研究目的のためにとても有益である．それ以外の手法はまだ，さらなる開発やユーザの実験による評

価が必要なため，今後の実現を待つことになるだろう．

文献

1. Acquisti, A. Privacy in electronic commerce and the economics of immediate gratification. In *EC'04 ACM Conference on Electronic Commerce*, (New York, NY, 2004), 21－29; doi 10.1145/988772.988777.
2. Brusilovsky, P., Kobsa, A. and Nejdl, W. Eds. *The Adaptive Web: Methods and Strategies of Web Personalization*. Springer Verlag, 2007; doi 10.1007/978-3-540-72079-9.
3. Chellappa, R.K. and Sin, R. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management* 6, 2 － 3 (2005), 181-202; doi 10.1007/s10799-005-5879-y.
4. Cranor, L.F. 'I didn't buy it for myself': Privacy and ecommerce personalization. In *2003 ACM Workshop on Privacy in the Electronic Society*, (Washington, DC, 2003), ACM Press; doi 10.1145/1005140. 1005158.
5. Fogg, B.J. *Persuasive Technology: Using Computers to Change What We Think and Do.* Morgan Kaufmann Publishers, San Francisco, 2003.
6. Gideon, J., Cranor, L., Egelman, S. and Acquisti, A. Power strips, prophylactics, and privacy, oh my! In *Second Symposium on Usable Privacy and Security*, (Pittsburgh, PA, 2006), ACM Press, 133-144; doi 10.1145/1143120.1143137.
7. Huberman, B.A., Adar, E. and Fine, L.R. Valuating privacy. In *Fourth Workshop on the Economics of Information Security*, (Cambridge, MA, 2005); http://infosecon.net/workshop/pdf/7.pdf.
8. Kobsa, A. Privacy-enhanced Web personalization. In *The Adaptive Web: Methods and Strategies of Web Personalization*. P. Brusilovsky, A. Kobsa, and W. Nejdl, eds. Springer Verlag, 2007, 628-670; doi 10.1007/978-3-540-72079-9_21.
9. Kobsa, A., Chellappa, R.K. and Spiekermann, S. Eds. *Proceedings of CHI-2006 Workshop on Privacy-Enhanced Personalization* (Montreal, Canada, 2006); www.isr.uci.edu/pep06/papers/Proceedings_PEP06.pdf.
10. Kobsa, A. and Cranor, L., Eds.. *Proceedings of the UM05 Workshop 'Privacy-Enhanced Personalization.'* Edinburgh, Scotland, 2005; www.isr.uci.edu/pep05/papers/w9-proceedings.pdf.
11. Kobsa, A. and Teltzrow, M. Contextualized communication of privacy practices and personalization benefits: Impacts on users' data sharing behavior. In *Privacy Enhancing Technologies: Fourth International Workshop* (Toronto, Canada, 2005). D. Martin and and A. Serjantov, Eds. Springer Verlag, 329 － 343; doi 10.1007/11423409_21.
12. Schreck, J. *Security and Privacy in User Modeling*. Kluwer Academic Publishers, Dordrecht, Netherlands, 2003; http://www.security-and-privacy-in-user-modeling.info.

ALFRED KOBSA（kobsa@uci.edu）は，カリフォルニア大学アーバイン校ドナルドブレンスクール（情報学）の教授である．

訳：長濱 諒（早稲田大学・理工学部），平手 勇宇（早稲田大学大学院・理工学研究科）