翻訳

プライバシー選択プラットフォーム

Webサイトがユーザの信頼を獲得するには，
まずWebサイト自身が自分のプライバシー方針を
明らかにする必要がある．そうすれば，Webサイトの
訪問者が意思決定プロセスに積極的に参加できるようになる．

Joseph Reagle reagle@w3.org
Lorrie Faith Cranor lorrie@acm.org
翻訳：安藤　進 sando@twics.com

原文: "The Platform for Privacy preferences"
Communications of the ACM, Vol.42, No.2, pp.48-55 (Feb. 1999) より許可を得て翻訳

インターネットユーザは，Webサイトで入力した情報が悪用されるのを心配している．ユーザの個人情報そのものだけではなく，オンラインでの活動を監視することでさまざまな情報が得られるからである（文献7）を参照）．オンラインプライバシー問題が浮上した理由は，Webサイトでどのような情報活動が行われているかをユーザが知ることが困難だからだ．プライバシー方針を明示しているWebサイトはあまりない☆1．仮にあったとしても，信用できなかったり理解できなかったりするサイトが多い．つまり，一方通行なのだ．Webサイトから個人情報の入力を求められても，入力した自分の情報がどのように利用されるのかが分からない．このような欠陥があるため，混乱や誤解が生じるのも当然だ．

W3C（World-Wide Web Consortium）にP3P（Platform for Privacy Preferences Project）がある．P3Pは，オンラインで情報をやりとりするための枠組みである．その目的は，Webサイトで掲示するプライバシー方針をユーザが評価できるようにすることだ．P3Pアプリケーションを利用すると，ユーザがWebサイトの方針を知り，必要に応じて自分の判断をコンピュータエージェントに伝えたり，特定のサイトとの関係を修正したりすることが可能になる．意味のある情報をユーザに知らせ，Webサイトのプライバシー方針の選択肢を与えるようにすれば，オンライン取引に対するユーザの信頼性も向上すると我々は信じている．

ただし，P3Pだけですべての問題が解決できるわけではない．そのほかの技術や規制，自己規制的な手法も必要になる．特定のユーザには受け入れがたい方針を技術的に排除する技術もある．たとえば，取引の処理中に受信者や盗聴者が収集可能な情報を制限する技術として，ディジタルキャッシュ，アノニマイザー，暗号化などがある．そのほか，情報の扱い方に関する基本的な責務に関する法律や業界のガイドラインを制定し実施することも考えられる．

P3Pの目玉は，意思決定をローカライズすることで，ユーザの好みや文化水準，法的規制などに柔軟に対応できるようにすることである．しかし，P3Pを有効に活用するためには，情報の開示が要求されたときに，意味のある意思決定をする意欲と能力がユーザに求められる．もちろん，そのためには使いやすいツールが必要だ．情報処理と意思決定の大部分を必要に応じてコンピュータエージェントに任せるだけではなく，Webサイトによる開示情報の使用や統合を促進する枠組みも必要だ．

P3Pの基礎

P3PはW3Cのプロジェクトの1つで，オープンで相互接続可能なWebの発展を促進するプロトコルを規定する

☆1 米連邦取引委員会のホームページ：www.ftc.gov/reports/privacy3/

CoolCatalogのステートメントを紹介する（www.CoolCatalog.com/catalogue/）．このサイトの方針は，HTTPログでクリックストリームデータだけではなく，ユーザの氏名，年齢，性別に関するデータも収集する．その目的は，ユーザの服装に関する好みを知ることで，カタログページのカスタマイズや製品の研究開発に利用することである．しかし，個人の身元は分からないように工夫する．個人情報が外部に漏れないようにもする．ユーザはこれらの情報にアクセスできないが，この方針を読んで入会または退会ができる（www.CoolCatalog.com/PrivacyPractice.html）．第3者のPrivacySeal.orgがこの合意の遵守を保証する．

簡易P3P構文

```
<PROP realm="http://CoolCatalog.com/catalogue/"
 entity="CoolCatalog" propID="94df1293a3e519bb">
 <USES>
  <STATEMENT purpose="1" recipient="0" id="0">
   <REF name="Web.Abstract.ClientClickStream"/>
  </STATEMENT></USES>
 <USES>
  <STATEMENT purpose="2,3" recipient="0" id="0"
   consequence="a site with clothes you'd appreciate.">
   <WITH><PREFIX name="User.">
    <REF name="Name.First"/>
    <REF name="Bdate.Year" OPTIONAL="1"/>
    <REF name="Gender"/>
   </PREFIX></WITH>
 </STATEMENT></USES>
 <DISCLOSURE discURI="http://CoolCatalog.com/PrivPractice.html"
 access="3" other="0,1"/>
 <ASSURANCE org="http://PrivacySeal.org"
  text="third party"
  image="http://PrivacySeal.org/Logo.gif"/>
</PROP>
```

図-1　プライバシープロポーザル例

国際的な業界コンソーシアムである．P3Pは，W3C加盟組織の代表十数名と全世界から招聘した専門家の合意に基づいて発足した☆2．

P3Pの目的はユーザがサービス提供者（プライバシー方針を宣言しデータリクエストを作成するWebサイトとアプリケーション）との合意を支援することである．合意に達するための第1ステップとして，サービス提供者がマシン可読のプロポーザルを送信する．このプロポーザルの中で，サービス提供の責務を負う組織が自分の身元を明らかにしプライバシー方針を宣言する．1つのプロポーザルは，1つまたは複数のURI（Uniform Resource Identifier）で特定される領域に適用される．英語とP3P構文で書かれたプライバシープロポーザルの例を図-1に示す．このプライバシープロポーザルの例では，収集するデータ要素を列挙して，データの使い方を説明する．さらに，データを誰と共用するか，識別可能な方法でデータを使用するかどうかを尋ねる．このような一連のステートメントはP3P用語（P3P harmonized vocabulary）で定義する．これが情報開示の基盤となる．情報開示の目的は，サービスがどの法律に準拠しているかではなくサービス内容がどのようなものであるかを記述することである（P3P用語については後述）．

プロポーザルは，Webブラウザやブラウザのプラグイン，プロキシサーバなどのユーザエージェントによって自動的に解析される．解析結果は，ユーザが設定した内容と比較される．そのため，ユーザはWebサイトにアクセスするたびにプライバシー方針を読む必要がない．Webサイトのプロポーザルがユーザの設定内容と一致すれば，ユーザエージェントは「PropID」と呼ばれるプロポーザルのフィンガープリントを返すことでそのプライバシー方針を自動的に受け入れる．Webサイトのプロポーザルがユーザの設定内容と一致しなかった場合エージェントは，ユーザにプロンプトを出す，相手のプロポーザルを拒否する，こちらから別のプロポーザルを出す，相手に別のプロポーザルを要求する，などの対応をする．

サービスが別のプロポーザルを提示し，ユーザエージェントがこれを承諾／拒否する手順は，「ネゴシエーション（negotiation）」と呼ばれる柔軟なものである．このようなネゴシエーションは，電話の発信者が自分の身元を明らかにする情報を送信するかどうか，受信先の電話を鳴らすかどうかの判定にも使われる[4), 5)]．

P3Pは，複数のプロポーザルを提供することで柔軟性を実現する．たとえば，映画情報を提供するWebサイトは，そのほかに映画批評も掲載する．ユーザが郵便番号を入力すれば，地元の映画館の上映スケジュールも教えてくれる．P3Pプロトコルは，何回でも個別にユーザとのやり取りを可能にするが，P3P仕様では最初にすべてのプロポーザルを一括してユーザに提示することを推奨している．個別に何回も交渉するか一括してやるかという違いはあっても，同じ合意に達することが多い．もちろん，ユーザにとっては個別交渉の方がよい場合もある[2)]が，その場合は通信に余計な時間がかかったりネットワークでのキャッシングの不備を覚悟しなければならない．

P3Pの実装形態によっては，特定のサービスに限って公開してもよい情報をユーザが保存できるデータレポジトリをサポートするものもある．特定のデータ要素の収集を認める合意に達した場合，その情報はレポジトリから

☆2 この記事は1998年11月9日のP3P草案に基づいて作成した．P3Pの仕様は，勧告への移行に伴い，変更される可能性がある．P3Pの最新情報については，W3CのWebサイト（www.w3.org/P3P）を参照してほしい．

自動的に転送される．サービスによってはユーザのレポジトリにデータの保存を要求することもある．このような読み書きリクエストは，P3Pとユーザの合意に基づいてコントロールされる．このレポジトリにサイト固有の識別子を格納することで，P3Pとの合意に基づいてWebサイトとの変名による相互会話を実現することも可能である．P3P仕様は，どのP3Pエージェントでも知っているべき基本的なデータ要素を定義した標準セットである．サービスは，P3P仕様に基づいて新たにデータ要素を定義することができる．

P3Pは，合意事項に基づいて情報が公開されることは保証するが，合意に基づいた確実なサービス法（sure services act）の制定が目的ではない．これは法律や自己規制制度で実施する．たとえば，サービスプロバイダが合意事項に違反した場合，訴訟などの処罰行為をとる保証機関をP3Pプロポーザルに記述することができる．そのような保証機関としてTRUSTeがある．TRUSTeは，P3Pの開発前からWebサイトのプライバシーを保護してきた組織である．サービスは，保証機関に対してだけではなく，業界のガイドラインや法律に対しても責任がある．

技術的な仕組み

P3Pを鳥瞰すると，単なる構造化データの交換プロトコルに見える．クライアントとサービス提供者がHTTP1.1の拡張機構を使って情報（プロポーザルとデータ要素）をやりとりしている．もう少しP3Pに近づいてみると，情報の取り扱い法とデータ要素を記述するための構文と意味を規定したものに見える．XMLとRDFを使って情報の構文や構造，意味を捕捉する（XMLは，データの構造化に使用するデータ要素を作成するための言語である．RDFは，データの構造化に使用するデータモデルを制限する機能であり，Webリソースとほかのリソースとの関係の記述に使用される）．

PICS（Platform for Internet Content Selection）などのW3Cメタデータ標準化活動とP3Pの相違点は，P3Pの方がリソースを柔軟に扱えることである．PICSの場合は，サービス提供者がPICSラベルで記述するプライバシー方針は静的なものである[6]．ユーザエージェントがプライバシーラベルを受信した後にデータをサービス提供者に返送すると，ユーザが合意したものと見なされる．一方P3Pの場合は，サービス提供者がユーザに複数の選択肢を示すことができる．ユーザが返送するデータには合意書のPropIDが付けられる．

ユーザエージェントは，十分な格納スペースがあることを確認し，サービス提供者のプロポーザルに合意すると，自分のPropIDをプロポーザルに付けて合意内容を記録しておく．こうすれば，ユーザエージェントとサービス提供者が過去の合意内容を参照することができる．サービス提供者は，その都度ユーザに新しいプロポーザルを送る代わりに，既存の合意書のPropIDを送る．これは，サービス提供者とユーザエージェントがすでに合意しているプロポーザルが存在していることを示している．これを元に，どのプロポーザルとプライバシー方針を使用するか，また合意書に記述されたデータ要素をユーザエージェントに要求する．ユーザエージェントは，この通知を破棄することもできるし，要求されたデータを返信することもできる．さらに，そのような合意書が見つからなかったり新しい合意書が欲しい場合は，完全なプロポーザルの提示を要求することも可能である．P3Pの将来のバージョンでは，PropIDをディジタル署名にすることで，合意が確実に存在していることを証明できるようにする予定である．

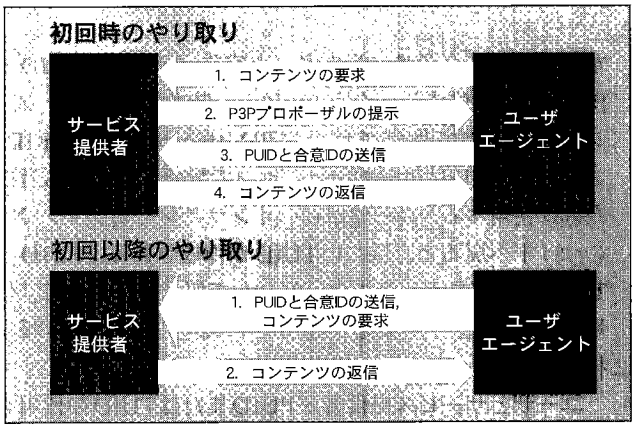

図-2

匿名性とクッキー

ユーザとの永続的な関係を望む商用Webサイトが多いが，個人の身元が分かる情報を要求するWebサイトは少ない．自分のサイトにアクセスするユーザ数を知り，頻繁にアクセスするユーザ向けにWebページをカスタマイズしたり各ユーザの好みに合わせた宣伝を提供したりするのが目的であれば，匿名か仮名の関係で十分なのである．

HTTPクッキーを使ってユーザとの関係を維持するWebサイトが多い．一意の識別子が格納されたクッキーをWebサイトから受け取り，ユーザがこれを返信すると，そのサイトとの関係を認めたことになる．しかし，現在のHTTPクッキープロトコルはユーザに最小限の情報しか提供しない．また，現在広く普及しているWebブラウザに実装されているクッキーの場合，どのサイトからのクッキーを受け入れるのかをユーザがコントロールできない．ただし，将来は変わるかもしれない☆3．P3Pの場合は，クッキーの代わりに2つの識別子を使用する．1つは，ユーザエージェントとサービス提供者が合意するたびに両者またはサイトに固有の識別子として作成されるPUIDである．ユーザは，PUID（pairwise user ID）の使用を

承認すると，合意書に指定された宛先（URI）にPUIDとPropIDを送信する．もう1つは，一時的またはセッション識別子として作成されるTUID（temporary user ID）である．TUIDは単一のセッションで状態を保持する目的だけに使用する．ユーザが別のオンラインセッションで別のサイトへ戻ると，新しいTUIDが作成される．PUIDとTUIDは，プロポーザルの一部として要求されるので，使用目的，受信者，身元確認などに関連した開示情報を持つ．

ユーザとサービス提供者がPUIDまたはTUIDの使用および個人データの非公開に合意したとしても，IPアドレスから両者のやりとりが知られる可能性がある．この問題が心配な場合，アノニマイザー，LPWA，オニオンルータ（Onion Router），Crowdsなどのユーザが匿名化サービスやツール（後述）といっしょにP3Pを使用することができる．

☆3 クッキーの用途がもっと詳しく分かるようにクッキーの仕組みを変えようとする意見もいくつか提案されてきた．D. Jaye氏の「状態管理の信頼性を向上させるHTTP」という提案（draft-ietf-http-trust-state-mgt-02.txt）やD. Kristol氏とL. Montulli氏の「HTTP状態管理機構」という提案（draft-ietf-http-state-man-mec-10.txt）がある．これらの提案は，www.ietf.cnri.reston.va.us/internet-drafts/で入手できる．

ユーザデータレポジトリ

Web上でのやりとりは匿名でなされることが多いが，サービス提供者がユーザに情報の入力を求めることもある．ユーザが開始したトランザクションを完了するために必要な情報である．たとえば，ユーザが何かを購入した場合，決済にはクレジットカード番号が，配達には住所がそれぞれ必要になる．

P3Pは，これらの情報をユーザデータレポジトリに格納しておき，P3Pの合意に基づいてユーザの代わりにサービス提供者に情報を提供する．P3Pのおかげでユーザはデータを何回も入力したり記録しておいたりする手間が省ける．サービス提供者にとっても，ユーザが同社のWebサイトに戻るたびにユーザから一貫したデータをもらうことができる．データのやりとりにP3Pを利用すると，プライバシーの面でも利点がある．サービス提供者はデータを自分のデータベースに格納せずに，必要に応じてユーザのレポジトリから取り出すことができるので，逆にいうと，ユーザが自分の情報をコントロールしやすくなる．さらに，あいまい性も少なくなる．どちらかというと厳密さに欠ける情報に一般的な開示条項を適用するより，収集した情報に直接適用する方が間違いがないか

P3P固有の用語集（P3P Vocabulary）

P3P固有の用語集は，情報の取り扱い方の開示の基盤となる．その目的は，特定の法律に準拠しているかどうか，あるいは特定の方針を支持しているかどうかではなく，サービスの内容を記述することである．

P3Pプロポーザルは，サービス提供者による情報の取り扱い方についての主張（assertions）を開示したものである．P3P固有の用語で定義された一連の主張を以下に紹介する．括弧内の数字は，P3Pプロポーザルの各主張を識別するためのコードである．

○プロポーザルレベルの主張

プロポーザル全体に適用される主張は以下のプロポーザル要素で構成される．

• 適用範囲（Realm）

プロポーザルでカバーされる1つまたは複数のURI（Uniform Resource Identifier）．

• 公開URI

サービス提供者のプライバシーポリシーを人間が読める形式で示したURI．このポリシーにはサービスプロバイダの連絡先が含まれていなければならない．

• 個人情報へのアクセス

特定の個人が自分自身に関係する情報を見てサービスプロバイダに問い合わせたり懸念を表明したりすることができる能力．サービス提供者は，次のどれかのカテゴリを開示し，公開URIで自社のアクセス方針を人間が読める形式で提示する．

－個人データは使用しない（0）

－個人の連絡情報（1）

オンラインの連絡先や実際の連絡先などの個人情報へのアクセスを認める（たとえば，ユーザが郵便の宛先などの情報にアクセスできる）．

－そのほかの個人情報（2）

特定の個人に関連した情報へのアクセスを認める（たとえば，ユーザが自分のオンライン課金などの情報にアクセスできる）．

－なし（3）

個人情報へのアクセスは認めない．

• 保証（責任）

サービス提供者が自社のプロポーザルを遵守していることを認証する保証機関があり，サービス提供者がガイドラインに従ってデータを処理しているなどの主張をする．これらの主張の正当性は，サービスプロバイダまたは独立保証機関が保証する．

• その他の開示

サービス提供者は，人間が読める形式で次のポリシーを開示する．

－合意内容の変更（0）

サービス提供者は，ユーザが既存の合意を将来取り消したり変更したりできるかどうかについて開示する．

－有効期間（1）

サービスプロバイダは，データを保持する期間について開示する．

らである．

ただし，データレポジトリの管理が重要になる．不正なアクセスを試みるアプレットやウィルスなどからユーザのデータを保護しなければならない．

そこでP3Pは，P3Pのすべてのユーザエージェントが知っており共通に使われるデータ要素を定義している．たとえば，ユーザの氏名，誕生日，住所，電話番号，電子メールアドレスなどである．それぞれのデータ要素は標準名で識別され，特定のデータ形式が割り当てられる．これらのデータ形式は，インターネットで使用されている他の標準と互換性がある（vCard[3]を参照）．個々の要素ごとに要求することもできるし，複数の要素をまとめて要求することも可能だ．たとえば，生まれた年月日をすべて要求することもあるし，生まれた年だけを要求することもある．同じ要求であってもサービス提供者によって使用する表現が異なると，ユーザは混乱してしまう．故意であるとないとにかかわらず，これは問題なので，P3Pは表現を統一しようとしている．

ユーザエージェントの実装形態によっては，ユーザがあらかじめ自分のレポジトリにデータを格納しておくことも可能である．さらに，ユーザエージェントが必要に応じてユーザにデータの入力を要求し，入力されたデータを将来のために自動的に保存することもできる．もちろん，データ要素がレポジトリに保存されているからといって，ユーザの承諾を得ずにデータをサービス提供者に送出してはならない．情報を送るのは合意が得られたときに限られる．

基本セットには，頻繁に要求されるデータ要素のほかに，PUIDやTUID，さらにレポジトリには静的な値としては保存されない抽象的な一連の要素も含まれる．抽象的な要素は，HTTPでのやりとりで交換される情報を示す．たとえば，クライアントとサーバのクリックストリームデータ，サーバに保存されるネゴシエーションの履歴，フォームデータなどである．抽象的なフォームデータは，サービス提供者がP3PではなくHTMLフォームによるデータ収集を提案していることを示す．抽象的なフォームデータを使用した方がユーザにプロンプトを提示するより，サービス提供者にとってはコントロールがしやすくなる．

サービス提供者は，P3P用語で定義された標準カテゴリを使って，フォームで収集する情報の種類を指定する．たとえば，ユーザの考え方や好みを知りたい場合，収集するフォームデータのカテゴリが好み（preference）であることを明示し，その使用目的を説明するだけでよい．こ

○ステートメントレベルの主張

一連のデータ要素やデータカテゴリに適用される主張は，次のプロポーザル要素で構成される．プロポーザル全体に適用される要素もある．

• 利　点

プロポーザルに合意することによって得られる利益や結果を人間に読める形式で記述したもの．

• データカテゴリ

データ要素の特性またはクラス．ユーザエージェントはこれを使用してどのタイプの要素が議論の対象になっているかを判定する．P3Pに固有の用語集では，次のデータカテゴリが定義されている．

－物理的な連絡先情報（0）

実際の世界で特定の個人を見つけたり連絡したりするための情報．たとえば，電話番号や住所など．

－オンライン連絡先情報（1）

インターネットの世界で特定の個人を見つけたり連絡したりするための情報．たとえば，電子メールアドレスなど．この情報は，通常，ネットワークにアクセスするときに使用するコンピュータには依存しない．

－一意の識別子（2）

特定の個人を一貫して識別するための識別子．ただし，金融・財務など金銭にかかわる目的には使用しない．たとえば，国民IDやWebサイトIDなど．

－財務アカウント識別子（3）

金融証書，銀行口座，決済システムに関連した個人の識別子．たとえば，クレジットカード番号や銀行口座番号など．

－コンピュータ情報（4）

個人がネットワークにアクセスするときに使用するコンピュータシステムに関する情報．たとえば，IPアドレス，ドメイン名，ブラウザやOSの種類など．

－ナビゲーションとクリックストリームデータ（5）

Webサイトにアクセスすることで受動的に生成されるデータ．たとえば，どのページにアクセスしたか，どのぐらいそのページにいたかなどのデータ．

－会話データ（6）

サービスプロバイダのサイトで相互の明示的な会話により実際に生成されたデータあるいは会話に関連したデータ．たとえば，検索エンジンに入力した検索要求，アカウントのログ，オンライン購買のログなど．

－人口統計学的社会経済学的データ（7）

性別や年齢，収入など個人の特徴を示すデータ．

－趣味データ（8）

好きな色や音楽など個人の好き嫌いに関するデータ．

－コンテンツ（9）

通信文に含まれる語句．たとえば，電子メールの本文，掲示板に書き込んだ投稿文，チャットルームで交わされた会話など．

• 目　的

データ要素を収集する理由．P3P用語で定義されている目的は次のとおり．

－現在のアクティビティの完了とサポート（0）

れにより問合せ項目をすべて列挙する必要がなくなる．さらに，フォーム要素を使用してユーザエージェントに指示を送ることで，サービス提供者がユーザに提示するフォームのフィールドに一致する要素をデータレポジトリから検索してもらうことも可能だ．ユーザエージェントの中には，レポジトリからデータを取り出してフォームの各フィールドに自動的に入力してくれるものもある．

基本セットに含まれていない情報の収集を望むサービス提供者が多いので，サービス提供者が自社専用のセットを用意し，ユーザにそれを提示してレポジトリに登録してもらえるようにする仕組みもP3Pが提供する．

ユーザが複数のペルソナ（persona）を指定し，各ペルソナにそれぞれ異なるデータ要素値を関連付けることを可能にするユーザエージェントもある．この機能を利用すると，ユーザが仕事用と家庭用で異なるペルソナを準備したり，トランザクションごとに異なるペルソナを指定したり，さらにはまったく架空のペルソナを作成することもできる．ユーザは，各ペルソナに対応したデータ値をレポジトリに格納しておけば，どのデータ値がどのペルソナに対応しているのかを監視する必要がなくなり，サービス提供者との一貫した関係を維持することができる．LPWAに類似したシステム（Gabber et. al.を参照）を利用すれば，対応する電子メールアドレスなどの情報を持つ仮名のペルソナが自動的に生成できる．

実装と配布

ある技術の有効性は，実装し配布し，そして実際に使ってみてはじめて分かるものである．実装と配布はP3P仕様の範囲を超えるものであるが，P3Pの実用化には不可欠である．そこで，配布，インタフェース，ユーザビリティに関連する問題について簡単に触れておきたい．

P3Pが世界中のWebサイトで一斉に採用されるとは考えにくいので，採用するWebサイトやユーザが徐々に増えていくことを前提にしてP3Pの実装法を工夫することが大切である．たとえば，ユーザエージェントを実装する際には，P3Pプロポーザルを提示しないサイトでもユーザが容易にアクセスできるようにするが，P3Pプロポーザルを提示するサイトであるかどうかをユーザに知らせる工夫が必要である．たとえば，P3Pプロポーザルを提示しないが個人情報を収集していると思われるサイトを発見的な手法で洗い出しユーザに警告する．

P3P固有の用語集（P3P Vocabulary）

サービスプロバイダが自社の提供するアクティビティ（情報や通信，トランザクションの提供）を完了させる目的で情報を使用する．たとえば，Web検索結果の返送や電子メールの転送，発注処理など．

－Webサイトとシステムの管理（1）

Webサイトとコンピュータシステムを技術的にサポートする目的だけに情報を使用する．たとえば，コンピュータのアカウント情報やサイトのセキュリティ管理情報．

－個人向けにサイトのカスタマイズ（2）

特定の個人向けにサイトのコンテンツやデザインを調整する目的で情報を使用する．

－研究開発（3）

サイトやサービス，製品，市場に対する向上や評価，検討を行う目的で情報を使用する．この情報には，特定の個人向けにコンテンツを調整するための情報や特定の個人を評価やターゲット，調査，連絡などの対象にする情報は含まれない．

－サービスや製品のマーケティングに利用（4）

サービスや製品を販売促進するために個人に連絡する目的で情報を使用する．この情報には，Webサイトの更新情報も含まれる．

－そのほかの用途（5）

上記以外の目的で情報を使用する．（ただし，人間に読める形式で説明する必要がある）．

• 識別可能な使用

特定の個人の身元が分かる方法でデータを使用するかどうかについて宣言する．たとえば，ほかの情報源から取得した個人情報にリンクするかどうかなど．氏名は特定の個人の身元が分かるデータであることは明白であるが，郵便番号や給料，誕生日などのデータが特定の個人を識別できるデータであるかどうかはその使い方によって決まる．

• 受取人

データを配布する対象となる組織単位やドメイン．サービスプロバイダやエージェントの上位にある．P3P用語では次の受取人が定義されている．

－自分自身およびエージェントだけ（0）

サービスプロバイダが述べた目的を実現するためにサービスプロバイダに代わってデータを処理する第３者をエージェントと定義する．たとえば，住所ラベル印刷するだけであり，情報をほかの目的に使用しない印刷局はエージェントに該当する．

－同じ方針に従う組織や団体（1）

共通の方針に従って各自の目的を実現するためにデータを使用する．たとえば，関連する製品やアクセサリを提供するパートナーとデータを共用するが，それらの製品やアクセサリにデータがそのまま使われることはないので，データが外部に漏れることはない．

－異なる方針に従う組織や団体（2）

サービスプロバイダが課す制約や義務に従うが，サービスプロバイダの方針とは異なるやり方でデータを使用することもある．たとえば，研究開発目的にデータを使用する可能性のあるパートナーとデータを共用する．

－無関係な第３者あるいは公開のフォーラム（3）

元のサービスプロバイダにはデータの使用法が分からない．たとえば，データを商用のCD-ROMに格納して提供したり，公開のオンラインWebディレクトリに載せたりする．

Webサイトの側に立てば，ユーザからの要望があればP3Pを採用するというだろう．だが，P3Pを採用したWebサイトが増えない限り，ユーザの要求は高まらないだろう．どちらを先にすべきか，これがジレンマだ．我々としては，優れたユーザエージェントを実装すればユーザの要求が高まるし，規制措置を講じればWebサイトでの採用率が高まるものと期待したい．P3Pに準拠したユーザエージェントが実装され，個人ユーザがこれを使用しはじめるようになれば，これに刺激されてWebサイト側でもP3Pプロポーザルを提示し，P3Pの利点を活用してデータ収集とプライバシーの開示を結びつけるようになるだろう．こうして，P3Pプロポーザルを提示するWebサイトが増加し，P3Pの使い方に慣れたユーザが増えていけば，P3Pに準拠しないWebサイトは減少していくだろう．

P3P仕様は，ユーザインタフェースについて言及していないし制約も課していない．優れたユーザインタフェースは重要であるが，インタフェースの標準化は必要とされない．P3Pの開発者は，創造性と革新性を望んでおり，不要な制限を課すつもりはない．だからといって，無原則に何でも認めるというわけではない．ユーザインタフェースをはじめとして，P3Pの目的を実現する実装形態でなければならない．

P3Pをユーザに受け入れてもらえるようにするには，ユーザに優しい実装を工夫しなければならない．P3P用語は段階的に詳細化する手法を提示しているが，必ずしもすべての人が初期設定をやりたいわけではない．しかし，プライバシーに対する関心度も人によって異なるので，すべてのユーザに提示する情報量を最大公約数のレベルに合わせることはできない．したがって，抽象化とインタフェースの階層化を図ることで，最初は基本的な設定から始め，徐々に高度なインタフェースへ進めるようにする．これがP3P成功のカギになる[1]．

ソフトウェア会社によってあらかじめ用意された設定に満足しないユーザが多い．むしろ，信頼すべき団体や自社のシステム管理者，友人などが作ってくれた設定を好む傾向がある．そこで，P3Pは推奨設定値を交換できる仕組みを提供する．これらの設定ファイルは，APPEL（A P3P Preference Exchange Language）で記述する．ユーザが自分でエージェントの設定をするのではなく，信頼すべきソースを選択し，そこから推奨設定値を取得するのである．ユーザがWebをブラウジングしているときに，ユーザの代わりにユーザエージェントがこの設定値を使用してくれる．

さらに，ユーザが最初に使用するときすべての設定をする必要はない．P3Pのインストール時にすべての設定をしなければならないわけでもない．推奨設定を利用して最も基本的な設定だけをすればよい．その後，頻繁に利用するサービスがあれば，そのときに合意事項を追加していけばよいのである．

まとめ

世界中に分散しているさまざまなメディアでプライバシーの問題を解決するには，一定のプライバシーを開示することで合意に達するしか方法がない．このような方法でユーザの意思決定を支援するのがP3Pアプリケーションである．P3Pが普及すれば，Webユーザによる信頼関係の構築と管理を実現する初めてのアプリケーションになるだろう．そのためには，実社会の場合と同じようなやり方で直感的に意思決定ができなければならない．P3Pの特徴は2つある．1つは，ユーザがサービス提供者や保証機関，推奨設定などを信頼できるようにすることである．もう1つは，実社会の場合と同じように，時間をかけてお互いの信頼関係を築けるようにすることである．このような解決法には次の前提がある．分散型でエージェント支援による意思決定ツールによりユーザが意味のある意思決定を可能にする．P3Pの成否は，ユーザがP3Pを使用したときにプライバシーが期待したとおりに守られていると感じることができるかどうかで決まる．つまり，実装品質，ユーザの能力，プライバシー保護の内容の開示を促進する枠組みの存在がカギになる．

P3Pのような技術の場合，実装から実運用へ進む過程に重大な影響を与える外部的な要因がある．現在のレベルよりもっと高度なプライバシーの保護を期待すると，市場の慣行を変えることになるのだろうか．市場の慣行を前提にすると，人々が自分の期待を変える必要があることになるのだろうか．最近の調査結果に見られるほど，本当に人々がプライバシーを心配しているのだろうか．このような疑問に対する解答は技術だけでは不可能だ．

参考文献

1) Cranor, L. and Reagle, J.: Designing A Social Protocol: Lessons Learned from the Platform for Privacy Preferences, Telephony, the Internet, and the Media, Mackie-Mason, J. and Waterman, D., Eds., Lawrence Erlbaum, Mahwah, N. J. (1998).
2) Cranor, L. and Resnick, P.: Protocols for Automated Negotiations with Buyer Anonymity and Seller Reputations, In Proceedings of the Telecommunications Policy Research Conference, Alexandria, Virg. (Sep. 27-29, 1997); www.si.umich.edu/~presnick/papers/negotiation/
3) Internet Mail Consortium: vCard − The Electronic Business Card Version 2.1 (Sep. 18, 1996).
4) Mitchell, R. E. and DeCew, J. W.: Dynamic Negotiation in the Privacy Wars, Tech. Rev. 97, 8 (Nov./Dec. 1994), 70-71; www.techreview.com/articles/nov94/mitchell.html
5) Reichenbach, R., Damker, H., Federrath, H. and Rannenberg, K.: Individual Management of Personal Reachability in Mobile Communication, In Proceedings of the IFIP TC11 13th International Information Security Conference, Copenhagen (May 14-16, 1997); www.iig.unifreiburg.de/dbskolleg/public/ps/ReiDFRa_97.IFIP_SEC.ps
6) Resnick, P.: Filtering Information on the Internet, Sci. Amer. (Mar. 1997), 106-108; www.sciam.com/0397issue/0397resnick.html
7) Wang, H., Lee, M. and Wang, C.: Consumer Privacy Concerns about Internet Marketing, Commun. ACM 41, 3 (Mar. 1998), 63-70.

（平成11年5月6日受付）