1999年12月22日発行（毎月1回22日発行）　第30号　1997年12月1日 第三種郵便物認可

日経インターネットテクノロジー

Nikkei Internet Technology

COVER STORY 1

インターネットが企業や社会をひらく

Eサービスとテラビット・ネットが創る新世紀

COVER STORY 2

個人情報を的確に収集するP3Pの実用化が近づく

パーソナライズの時代をにらみ，個人情報の活用に威力

START UP

ランディ

順調だったビジネスを捨て，Webサイト向けミドルウエアへ集中

SURVEY

認証局サービス

新規参入相次ぐ，ユーザーのニーズに柔軟に対応

2000 1 新年号

日経インターネットテクノロジー
Nikkei Internet Technology

CONTENTS

COVER STORY 1

59

5誌連動ミレニアム特別企画

情報ネット・システムが時代を変える

インターネットが企業や社会をひらく

Eサービスとテラビット・ネットが創る新世紀

2000年以降,インターネットがユーザーにもたらすのはビジネス・スタイルやコンピューティング・スタイル,生活スタイルといったスタイルの変化だ。それを支えるのが,ネットワークやサービスを提供するサービス・プロバイダ。ありとあらゆる情報/サービスはインターネットの向こう側に。端末も多様化し,「いつでも,どこでも,必要な情報/サービスをインターネットで」という時代が訪れる。

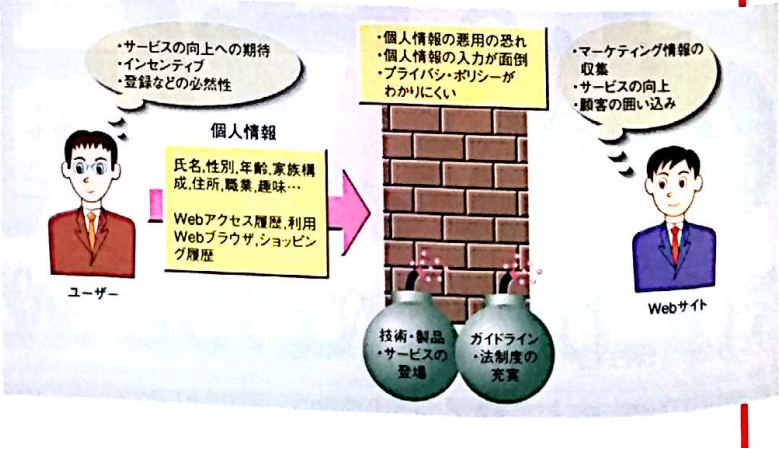
COVER STORY 2

124

個人情報を的確に収集するP3Pの実用化が近づく

パーソナライズの時代をにらみ,個人情報の活用に威力

個人情報を的確に収集するための技術であるP3Pが,2000年春にW3C標準となる見込みである。個人情報は取り扱いに注意が必要な半面,Webサービスを提供するうえで強力な武器となる。すでにマイクロソフトのPrivacy Wizardやノベルのdigitalmeなど,これらを先取る形の技術やサービスが登場している。



発行人● 松崎 稔
編集長● 稲葉 則夫
副編集長● 小松原 健
記者● フィリップ・キーズ/河井 保博/安東 一真/勝村 幸博/斉藤 国博/中島 募
広告部長● 嶌田 良彦
広告部次長● 高峰 俊雄
広告部副長● 和田 浩明
広告● 木村 一也/島田 洋平
販売部次長● 小俣 淳
販売部課長● 森実 浩
販売● 坂本 光久
表紙デザイン アート オブ ノイズ
制作 日経BPクリエーティブ
日経BP社
Nikkei Business Publications,Inc.
東京都千代田区平河町2-7-6 〒102-8622
日本ABC協会加盟誌(新聞雑誌部数公査機構)

COVER STORY

特集 2

KEYWORD
プライバシ
パーソナライズ
P3P

個人情報を的確に収集する P3Pの実用化が近づく

パーソナライズの時代をにらみ，個人情報の活用に威力

個人情報を的確に収集するための技術であるP3P(Platform for Privacy Preference Project)が，2000年春にW3C標準となる見込みである。個人情報は取り扱いに注意が必要な半面，Webサービスを提供するうえで強力な武器となる。年齢，職業，好みなどの基本的な特性，さらにWebでどのページに興味を持っているかなどを収集，分析してマーケティングに利用する。さらに，ユーザーごとにきめ細かなサービスを提供する。すでにこれらを先取る形の技術やサービスが登場している。

◆プライバシ・ポリシー
収集した個人情報の取り扱いを規定するルール。どのような情報を集めるのか，その情報をどんな目的に利用するのか，その情報をだれが（社内だけ，第三者にも渡すなど）利用するのか，などをまとめてある。

◆W3C
World Wide Web Consortiumの略。WWWに関連する技術の標準化を進めている非営利の団体。国際的な共通技術を事実上の標準として推進する活動や，プロトタイプの開発・提供を行っている。

◆P3P
Platform for Privacy Preferences Projectの略。プライバシに注意しながらサーバー側とクライアント間で個人情報をやりとりする技術の標準化を進めているW3Cのプロジェクト，またはその仕様。個人情報のフォーマットは，XMLで規定されており，コンピュータで解釈，処理できる。

◆クッキー
Webサーバーが Webブラウザに送り込む識別情報。本来Webサーバーへのリクエストは1回ごとに切断されるため，Webサーバー側では複数のページへのアクセスを連続したものとして把握することはできない。複数のリクエストを関連づけるための技術がクッキーである。

Part 1

パーソナライズの時代へ

ベンダーの取り組み始まり，個人情報活用に向かう

Webサイトを利用して，EC（電子商取引），情報提供やサポートなど，さまざまなサービスやビジネスを展開するうえで，アクセスしてくるユーザーの“顔”を知りたい。そのユーザーがWebサイト上で，どのような行動をとるかも貴重な情報である。このような情報を把握できれば，マーケティング情報として分析したり，個々のユーザーに合わせたサービスを提供したりといろいろな目的に活用できる。

実際，パーソナライズ専用のアプリケーションに対する関心が高まっている。たとえばこの種のアプリケーションの先駆けである，米ブロードビジョンの「One-to-One」は，出荷数を伸ばしている。ユーザーの属性だけでなく，Web上の行動履歴などさまざまな条件を組み合わせ，それに合わせた情報を提供するサービスを効率よく構築できるソフトウエアである。国内でも「99年は昨年の10倍は引き合いがあり，とくに99年夏ころからの反応がよくなった」（伊藤忠テクノサイエンス CRM営業推進部営業第4グループ グループリーダーの稲益 清之氏）という。

個人情報の取り扱いを支援する技術やサービスも登場しつつある。個人情報の取り扱いに関する宣言，いわゆるプライバシ・ポリシーの作成を支援する米マイクロソフトの「Privacy Wizard」，個人情報を一元管理して再入力の手間を省くと同時に，Webサイトに渡す情報を明確にできる米ノベルの「digitalme」などが登場。W3C（World Wide Web Consortium）が標準化を進めている個人情報を的確に収集するための技術「P3P（Platform for Privacy Preference Project）」が2000年春にも実用化される。

従来のように，すべてのユーザーに同じサービスを提供というだけでは，ビジネスの拡大は望めない。個々のユーザーに合わせたサービスを提供する，いわゆるパーソナライズの時代に進む。

個人情報を収集，活用する課題

Webサイト側にとって個人情報は魅力的である。しかし，その収集，管理，活用などの面ではいろいろな課題がある（図1）。

Webサイト側にしてみれば，アクセスしてくるユーザーの個人情報をできるだけ多く収集したい。アクセスしてきたユーザーを，クッキーなどを使って識別し，サイト上での行動も把握したい。それらは，マーケティング情報としての分析やサービスの向上などに活用できるからだ。

一方，サイトにアクセスするユーザーにしてみれば，基本的に匿名で通したい意識が強い。懸賞など，とくになんらかのインセンティブがあれば別であるが，なかなか個人情報を入力してもらうのは難しい。この背景には，氏名，年齢，住所などの渡した個人情報

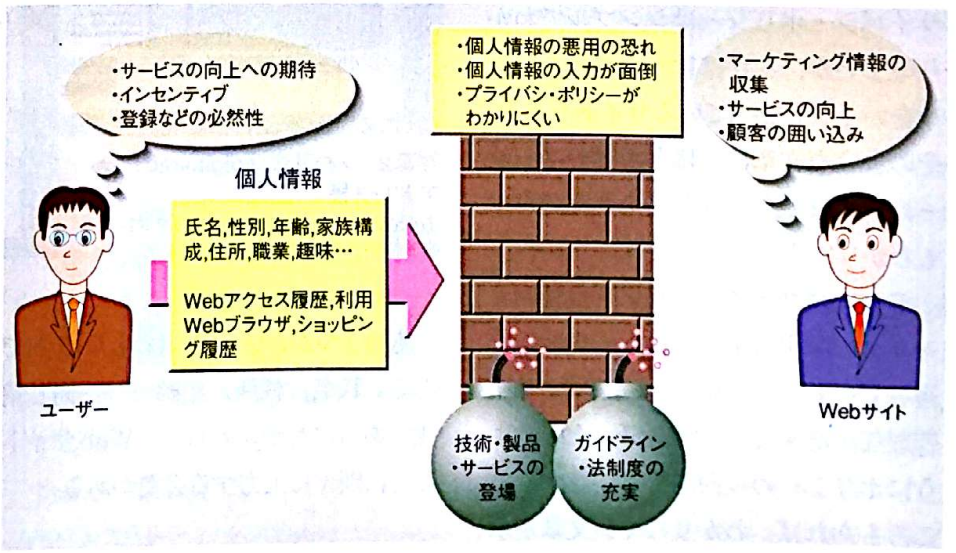


図1　個人情報の引き渡しに関する障害が小さくなる
個人情報に対する期待はあるものの，プライバシ面の不安などからなかなか活用が進んでいない。それが，技術やサービスの登場や，法制度などの整備によって障害が少なくなる。

◆プライバシ・ポリシー
収集した個人情報の取り扱いを規定するルール。どのような情報を集めるのか，その情報をどんな目的に利用するのか，その情報をだれが（社内だけ，第三者にも渡すなど）利用するのか，などをまとめてある。

◆W3C
World Wide Web Consortiumの略。WWWに関連する技術の標準化を進めている非営利の団体。国際的な共通技術を事実上の標準として推進する活動や，プロトタイプの開発・提供を行っている。

◆P3P
Platform for Privacy Preferences Projectの略。プライバシに注意しながらサーバー側とクライアント間で個人情報をやりとりする技術の標準化を進めているW3Cのプロジェクト，またはその仕様。個人情報のフォーマットは，XMLで規定されており，コンピュータで解釈，処理できる。

◆クッキー
Webサーバーが Webブラウザに送り込む識別情報。本来Webサーバーへのリクエストは1回ごとに切断されるため，Webサーバー側では複数のページへのアクセスを連続したものとして把握することはできない。複数のリクエストを関連づけるための技術がクッキーである。

Part 1

パーソナライズの時代へ
ベンダーの取り組み始まり，個人情報活用に向かう

Webサイトを利用して，EC（電子商取引），情報提供やサポートなど，さまざまなサービスやビジネスを展開するうえで，アクセスしてくるユーザーの“顔”を知りたい。そのユーザーがWebサイト上で，どのような行動をとるかも貴重な情報である。このような情報を把握できれば，マーケティング情報として分析したり，個々のユーザーに合わせたサービスを提供したりといろいろな目的に活用できる。

実際，パーソナライズ専用のアプリケーションに対する関心が高まっている。たとえばこの種のアプリケーションの先駆けである，米ブロードビジョンの「One-to-One」は，出荷数を伸ばしている。ユーザーの属性だけでなく，Web上の行動履歴などさまざまな条件を組み合わせ，それに合わせた情報を提供するサービスを効率よく構築できるソフトウエアである。国内でも「99年は昨年の10倍は引き合いがあり，とくに99年夏ころからの反応がよくなった」（伊藤忠テクノサイエンス CRM営業推進部営業第4グループ グループリーダーの稲益 清之氏）という。

個人情報の取り扱いを支援する技術やサービスも登場しつつある。個人情報の取り扱いに関する宣言，いわゆる☞プライバシ・ポリシーの作成を支援する米マイクロソフトの「Privacy Wizard」，個人情報を一元管理して再入力の手間を省くと同時に，Webサイトに渡す情報を明確にできる米ノベルの「digitalme」などが登場。☞W3C（World Wide Web Consortium）が標準化を進めている個人情報を的確に収集するための技術「☞P3P（Platform for Privacy Preference Project）」が2000年春にも実用化される。

従来のように，すべてのユーザーに同じサービスを提供というだけでは，ビジネスの拡大は望めない。個々のユーザーに合わせたサービスを提供する，いわゆるパーソナライズの時代に進む。

個人情報を収集，活用する課題

Webサイト側にとって個人情報は魅力的である。しかし，その収集，管理，活用などの面ではいろいろな課題がある（図1）。

Webサイト側にしてみれば，アクセスしてくるユーザーの個人情報をできるだけ多く収集したい。アクセスしてきたユーザーを，☞クッキーなどを使って識別し，サイト上での行動も把握したい。それらは，マーケティング情報としての分析やサービスの向上などに活用できるからだ。

一方，サイトにアクセスするユーザーにしてみれば，基本的に匿名で通したい意識が強い。懸賞など，とくになんらかのインセンティブがあれば別であるが，なかなか個人情報を入力してもらうのは難しい。この背景には，氏名，年齢，住所などの渡した個人情報

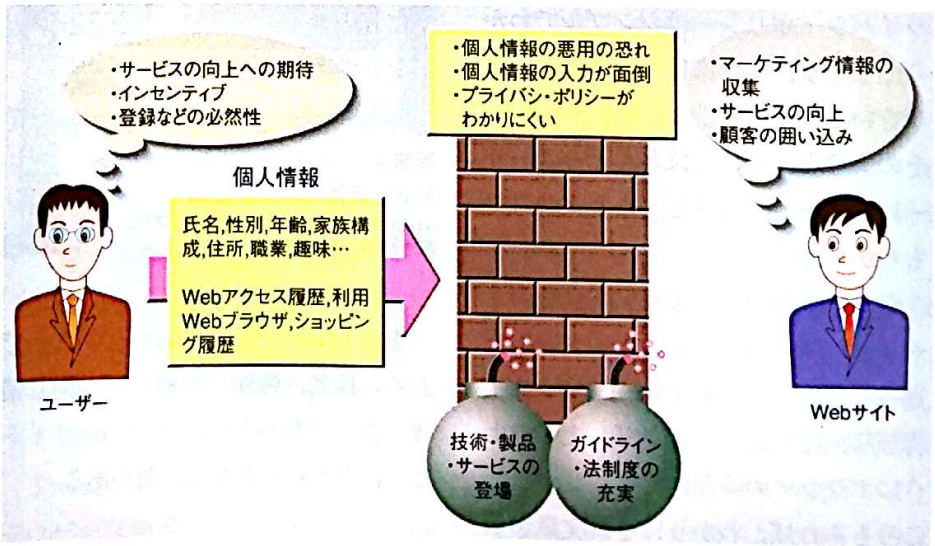


図1　個人情報の引き渡しに関する障害が小さくなる
個人情報に対する期待はあるものの，プライバシ面の不安などからなかなか活用が進んでいない。それが，技術やサービスの登場や，法制度などの整備によって障害が少なくなる。

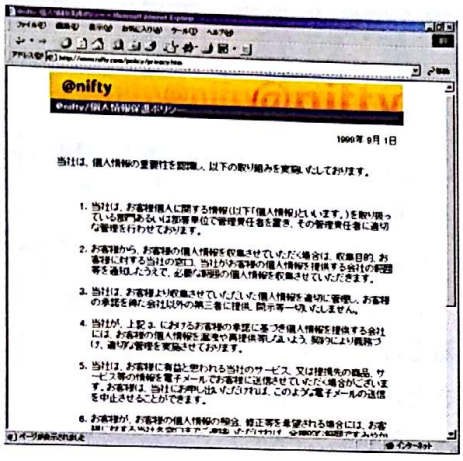


写真1　ニフティのプリバシー・ポリシー
簡潔でわかりやすい。これよりも長い文章で複雑なポリシーを掲げるサイトが多い。

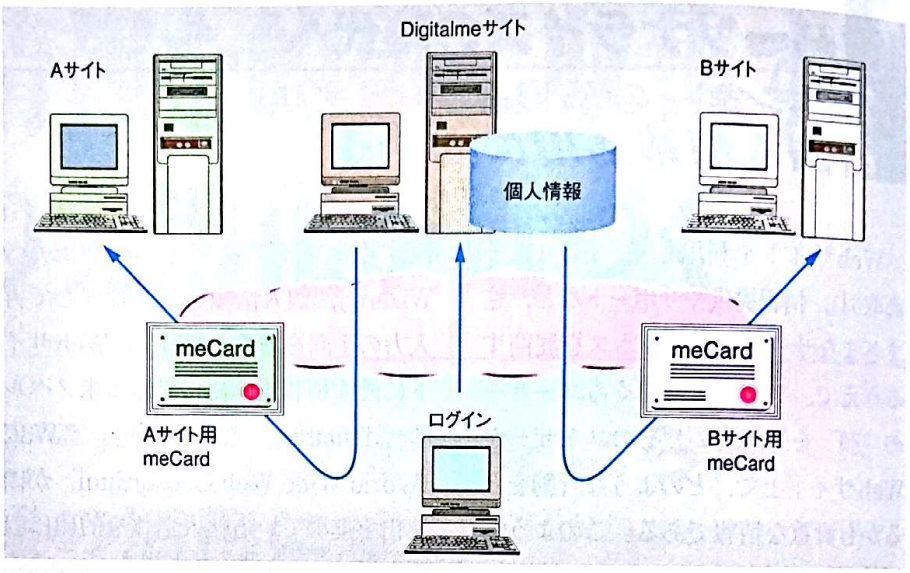


図2　ノベルのdigitalme
digitalmeサイト（http://www.digitalme.com/）に個人情報を格納しておき，サイトを訪ねる際に，必要な個人情報だけをそのサイト用のmeCardの形で取り出し，情報を渡す。

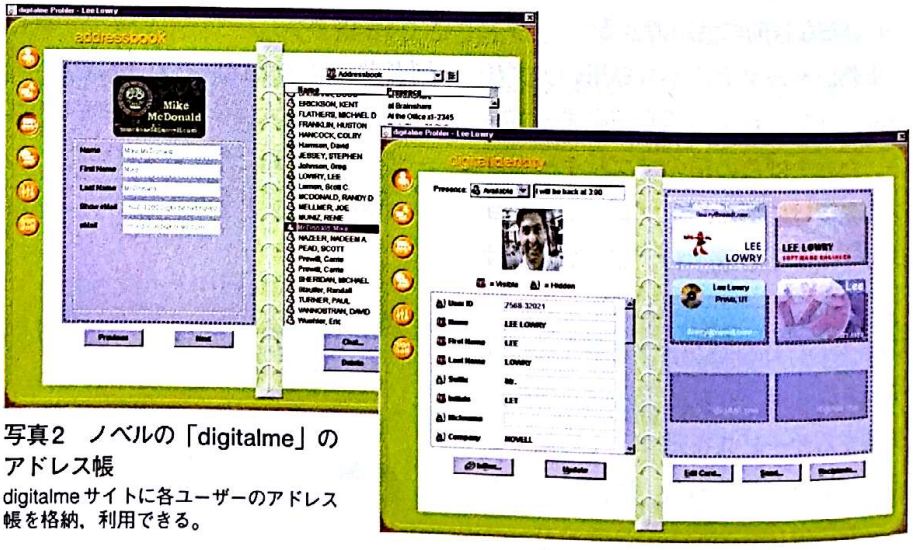


写真2　ノベルの「digitalme」のアドレス帳
digitalmeサイトに各ユーザーのアドレス帳を格納，利用できる。

がどのように利用されるかが不安であるからだ。このところ，個人情報の漏えい，売買という事件が相次ぎ，これが不安に拍車をかけている。

最近では，取得した個人情報をどのように取り扱うのかを示すプライバシ・ポリシーを掲げるWebサイトが多くなっている（写真1）。ニフティのプライバシ・ポリシーはシンプルでわかりやすいが，なかにはわかりにくい文章をいくつも並べているサイトもある。そのような文章は，ほとんどのユーザーは読まないだろうし，たとえ読んでもわかりにくい。

それにニフティのように「自社のサービスに関するダイレクト・メールを送ってもよいかも検討する」（ニフティ管理部法務課長の丸橋 透氏）というようにポリシーの範囲内でも注意するところもあれば，わかりにくい文章が示す範囲をフルに活用する企業もあるだろう。

もう1つが，入力が煩わしいことである。氏名，住所，年齢――。同じ情報であるにもかかわらず，Webサイトごとに別々に入力する必要がある。

特定の情報だけをカードの形で

ノベルのdigitalmeは，アクセスするサイトごとに特定の個人情報だけを簡単な操作で渡せるサービスである（図2）。同社のディレクトリ・サービスであるNDS（Novell Directory Services）をベースに開発した個人情報データベースから，特定の情報だけを取り出してWebサイトに渡す。たとえば，EC

サイトなどで買い物をする際は氏名，住所，クレジット・カード番号を，レンタカーを予約する場合は免許証番号も含めた情報を，digitalmeサイトから取り出して転送する。

このサービスを利用するには，あらかじめdigitalmeサイトに，Webアクセスで必要となりそうな個人情報すべてを登録しておく。目的のWebサイトにアクセスする場合は，いったんdigitalmeサイトにログインして，必要な個人情報だけを「meCard」として取り出して目的のサイトに渡す。インターネット上に自分の情報があるため，どのマシンからアクセスしてもmeCardを利用できる。meCardは各サイトが用意する，必要とする情報のリストのようなものである。

digitalmeサイトに登録してある情報ならば，meCardを転送するという簡単な操作で，目的のサイトに個人情報を転送できる。Webサイトを訪ねるたびに，氏名，住所など同じ情報を何度も入力しなくて済む。

meCardは個人情報を転送するのと同時に，会員カードという意味も持っている。Webサイトに入るためのユーザー認証用としても利用できる。ノベルでは，金融機関などを手始めに，digitalmeを利用するサイトを増やしていく計画である。

国内でも「2000年早々にサービスを提供する」（ノベル マーケティング本部プロダクトマーケティンググループNDSエバンジェリストの船橋 肇氏）。

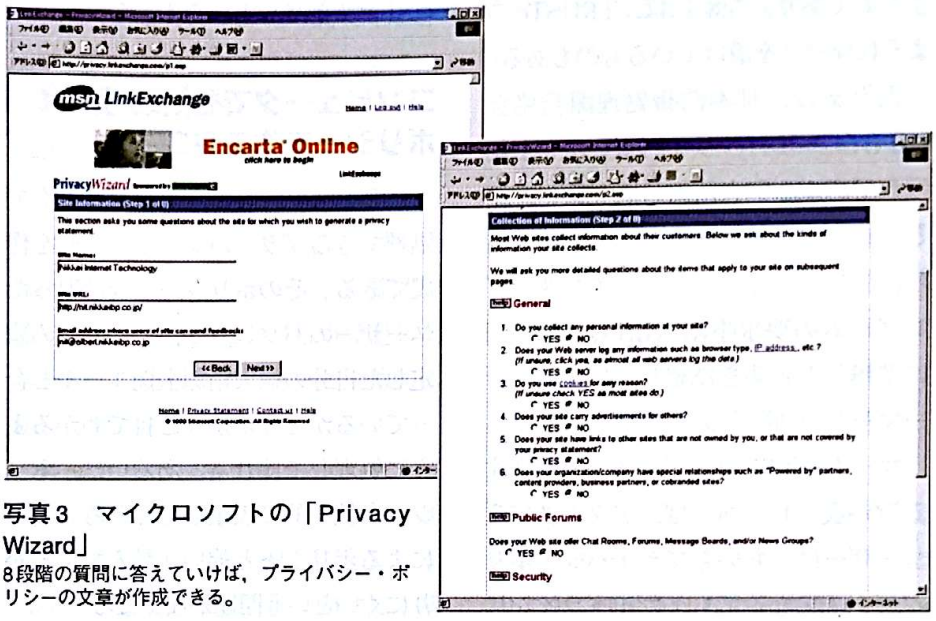


写真3　マイクロソフトの「Privacy Wizard」
8段階の質問に答えていけば，プライバシー・ポリシーの文章が作成できる。

ポリシーの記述を支援

プライバシ・ポリシーといっても，何をどのように記述すればよいのか，頭を痛める。どのような個人情報を集めるのか，その情報をだれがどのように利用するのか――など，プライバシ・ポリシーで宣言すべき項目は多い。

マイクロソフトが開発したPrivacy Wizard（写真3）を使えば，個人情報の取り扱いに関する質問に答えていくだけで自動的にプライバシ・ポリシーの文章を記述したファイルを作成してくれる。ここで作成したプライバシ・ポリシーは，米国のプライバシ関連の非営利団体であるTRUSTeのガイドラインに適合する。

Privacy Wizardは，マイクロソフトのMSN関連サイト（http://privacy.linkexchange.com/）やTRUSTeサイト（http://www.truste.org/）などで利用できる。

いくつものガイドラインがある

TRUSTeでは，同団体のガイドラインに沿ったプライバシ・ポリシーを掲げるWebサイトに，「トラストマーク」を張ることを認めている。プライバシ・ポリシーの文章ではわかりにくい。そこでマークを表示して，そのサイトのプライバシ・ポリシーがどのようなものであるかをひと目でわかるようにしようという工夫である。

国内でも数多くの個人情報の取り扱いに関するガイドラインがある（表1）。通産省や郵政省などが定めたものや，電子ネットワーク協議会や金融情報システムセンターなどの業界団体がまとめたものなど，いろいろなガイドラインがある。それぞれの業種に合わせた個人情報の取り扱いのルールについて

◆EUデータ保護指令
EU（欧州連合）が95年10月に公示し98年10月25日から施行している「個人データ処理に係る個人情報の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」（EUデータ保護指令）。個人情報を十分なレベルで保護していない第三国への個人情報の移動を禁じている。EUでは，このほかにもいくつか個人情報に関する指令を出している。

まとめてあり，なかには，TRUSTeのようにマークを設けているものもある。

たとえば，日本情報処理開発協会（JIPDEC）の「プライバシーマーク制度」である。個人情報の取り扱いを正しく管理する体制を規定した「個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q 15001）」に準拠した企業を認定し，プライバシーマークの利用を認めている。

マークやXXXガイドラインを順守する旨が表示してあれば，アクセスするユーザーはいちいちプライバシ・ポリシーを読まなくても，ガイドラインに沿っているということがひと目でわかる。一応の安心はできるものの，ガイドラインの数が多く，それらをすべて理解するのは不可能に近い。Webサイト側にとっても，業種によっては複数のマークを取得する必要が出てくる。ただ，これは過渡的なもので「Webサイト側が取捨選択していくうちに，いずれ整理，統合されていくだろう」（電子商取引実証推進協議会 主席研究員の合原 英次郎氏）という声が多い。

コンピュータでも処理可能なポリシーを作るP3P

P3Pを利用すれば，コンピュータで処理できるプライバシ・ポリシーを作成できる。そのポリシーを受け取ったユーザーのパソコンが，あらかじめ設定した自分の個人情報公開ルールと合っているかどうかがひと目でわかるように処理してくれる。あるいは，ポリシーを統一的に表示してくれる。文章によるポリシーと違い，読んでもわかりにくいという問題がなくなる。

P3Pは，Internet ExplorerやNetscape Communicatorに実装される見込みである。また，マイクロソフトのPrivacy Wizardのようなソフトウエアや，ノベルのdigitalmeのようなソフトウエアやサービスも登場すると見られている。

個人情報保護は世界の流れ

Webサイトに掲げたポリシー通りに個人情報を取り扱うのか，また取り扱う体制ができているのかという点も重要である。正しく扱わないと世界の流れから取り残されてしまう。マイクロソフトやIBMは「プライバシを守らないWebサイトには広告を出さない」と宣言するなど，米国では自主規制が進んでいる。欧州では「EU（欧州連合）データ保護指令で，個人情報を適切に保護していない国へは，情報の持ち出しを禁止している。

ただ，注意して欲しいのは，国内では漏えいなどの問題が続いたため個人情報を使うのは“悪いこと”というイメージさえあるが，“個人情報を活用してはいけない”というわけではない。ユーザーに納得してもらって“的確に活用すればよい”ということである。政府の高度情報通信社会推進本部で立法化に向けて議論を進めている個人情報保護法案も同様の趣旨である。

ユーザーの個人情報を的確に収集して活用すれば，今後のWebビジネスの可能性が広がる。

表1　民間を対象とする個人情報保護に関するおもなガイドライン
ECOM（電子商取引実証推進協議会）がまとめた資料をもとに作成。

ガイドライン	制定団体	制定/改訂時期
民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン	通産省	89年制定/97年改訂
電気通信事業における個人情報保護に関するガイドライン	郵政省	91年制定/現在改訂中
電子ネットワーク運営における個人情報保護に関するガイドライン	電子ネットワーク協議会	94年制定/97年改訂
放送における視聴者の加入者個人情報の保護に関するガイドライン	郵政省	96年制定
発信者情報通知サービスの利用における発信者個人情報の保護に関するガイドライン	郵政省	96年制定
サイバービジネスに係る個人情報の保護に関するガイドライン	サイバービジネス協議会	97年制定
情報サービス産業個人情報保護ガイドライン	サービス産業協議会	98年制定
販売信用取引における電子計算機処理に係る個人情報保護のためのガイドライン	日本クレジット産業協会	98年改訂
金融機関等における個人データ保護のためのガイドライン	金融情報システムセンター	99年改訂
民間部門における電子商取引に係る個人情報の保護に関するガイドライン	電子商取引実証推進協議会	98年制定

◆XML
eXtensible Markup Languageの略。人間にもコンピュータにも扱いやすいデータの表現方式。例えば発注書は，日付，発注者，発注内容といったデータからなるが，それぞれのデータに「タグ」という目印をつける。日付のデータなら，<日付>～</日付>といった分かりやすい名称のタグを付ける。企業システムや個々の製品でXMLに対応すれば，容易にデータをやり取りして連携できるようになる。

Part 2

P3Pの仕組み

利用目的などを明確に示し，個人情報を収集する

P3P（Platform for Privacy Preferences Project）[1]は，Webサイト側が個人情報を的確に収集するための仕組みである。W3C（World Wide Web Consortium）で標準化が進められている（p.131の別掲記事参照）。P3P1.0は，99年11月2日に最終ドラフトが発行され，順調に進めば2000年春に勧告される。

Webサービスで「プライバシ・ポリシー」を設けて，個人情報の取り扱いについて説明するサイトが多くなってきている。しかし，こういった個人情報に関する説明は，読んでもわかりにくい。それに同じことが書いてあったとしても，その表現方法が不統一であるため，ユーザーが混乱することもある。

P3Pを利用すれば，こういった問題を大幅に改善できる。個人情報を取得する際に，個人の属性に合わせてカスタマイズしたWebページを提供する（パーソナライズ），マーケティングに使うというような利用目的を示し，情報は自社内でのみ使用する，あるいは第三者に渡すなどの利用形態を明らかにする。これにユーザーが同意したときのみ，個人情報を収集する。ユーザー自身も，現在のようにWebサイトに掲げられた，長くてわかりにくいプライバシ・ポリシーを読む必要はない。統一的に整理されたポリシーを確認するか，あるいは，あらかじめ設定したユーザーの情報公開ルールと自動的に照合してくれる。

Webサイトはきめ細かいプライバシ・ポリシーの設定が可能になり，ユーザーもその確認を容易にできるようになる。個人情報の活用に向けて，基盤が整う。

コンピュータで個人情報を処理可能に

P3P1.0は，サーバーからユーザーに示すプライバシ・ポリシーの語彙（ごい）や文法を規定する。また，ユーザー自身が個人情報を公開するかどうかのルールを設定できる。これらはパソコンなどで解釈，処理できるようにしてあり，より複雑なプライバシ・ポリシーを規定，扱いやすくなる。

ポリシーはXMLで記述

プライバシ・ポリシーの記述文法は，拡張可能なマークアップ言語であるXML[2]を利用して定義している。XMLはコンピュータで処理しやすく，複雑なプライバシ・ポリシーを規定することができる。

サーバーは単に画一的にポリシーを伝えるだけでなく，年齢，性別など要求する個人情報の内容ごとに，利用する目的や形態をユーザーに伝えることができる。たとえば，年齢はマーケティング情報蓄積のため，性別はページのカスタマイズのため，などというように細かく示せる。もちろん，文章でも複雑なポリシーを説明できるが，文章が長く複雑になり，現実的なものでなくなってしまう。XMLを使うことで，個人情報の利用目的などを詳細に伝えられ，ユーザーも自分の個人情報がどのように利用されるかを的確に把握できる。

また，プライバシ・ポリシーのなかに正当性を証明するための第三者機関を記述するという仕組みも用意している。

プライバシ公開のルールを設定

ユーザーは，自身のプライバシを公開するためのルール（これをプリファレンスと呼ぶ）を設定することができる。個人情報を公開するかどうかを，個人情報の内容や重要性，サーバーの信頼度，利用目的に応じて設定するのがプリファレンスである。たとえば「年齢，性別は無条件に公開する。住所は荷物の配送に必要な場合にのみ公開する」といったきめ細かい設定が可能である。

ユーザーがあらかじめ設定したプリファレンスと，サーバーが提示するプライバシ・ポリシーは，クライアン

◆URI
Uniform Resource Identifierの略。物理的あるいは抽象的なあらゆる資源を同定するための表記規則。RFC2396などで規定されている。Web上の資源を指定するのに用いるURLはURIのサブセットとなっている。

◆リポジトリ
ソフトウエアなどの設定や履歴などに関する情報を記録・管理し，必要に応じてアクセスできるようにするメカニズム。

ト・ソフトウエア（通常はWebブラウザ）が自動的に比較する。ユーザーがいちいちサーバーのプライバシ・ポリシーを読む必要がない。ユーザーは，そのWebサイトが自分のプリファレンスと合っているかどうかだけをチェックすればよい。

実際にブラウザなどに実装される際には，ウイザードなどを提供して複雑なプリファレンスを簡単に設定できるようになると思われる。Webサイトが提示する複雑で長いプライバシ・ポリシーを読まなくても，容易に自分の情報を提供するかどうかを判断できるようになる。

これらの特徴により，P3P1.0を用いれば，サーバー側もユーザー側も，的確にコンセンサスをとって個人情報をやりとりし，サービスなどに活用しやすくなる。

応答と同時にポリシーのURLを

P3P1.0を利用するとき，典型的なサーバー－クライアント間のやり取りは次の通りである（図1）。

クライアントからサーバーに通常のWebページのリクエストと同様，HTTP[3]を用いてコンテンツを要求する（a）。このとき，サーバーがユーザーの個人情報が欲しいならば，サーバーがプライバシ・ポリシー，つまり個人情報の利用目的や利用形態を公開する。このため，サーバーは2つの処理を同時に実行する。1つは要求されたコンテンツをクライアントに返す（b）。もう1つは，XMLで記述されたプライバシ・ポリシーが存在するURL（正確にはURI[4]）を通知する（c）。

クライアントは受け取ったコンテンツを表示するとともに，通知されたURLにアクセスして（d），プライバシ・ポリシーを取得する（e）。

クライアントは，2つのいずれかの方法で，ポリシーをユーザーに伝える。1つは，ポリシーをそのままユーザーに表示する（具体的な表現方法はクライアント・ソフトに依存する）。もう1つが，ユーザーのプライバシ公開ルール（プリファレンス）と比較し（f），プライバシ・ポリシーがユーザーのプリファレンスに合致するかどうかをユーザーに表示する。

個人情報を基にカスタマイズしたWebページを提供するなどの場合，このフローを2回繰り返すこともある。つまり，1回目では個人情報を入力するフォームをコンテンツとして返し，同時にそこで入力した個人情報に関するポリシーのURLを通知する。ユーザーが個人情報を入力して送信すると，カスタマイズしたページをコンテンツとして返し，そこでユーザーの属性などに対応したポリシーURLを通知するといった処理である。

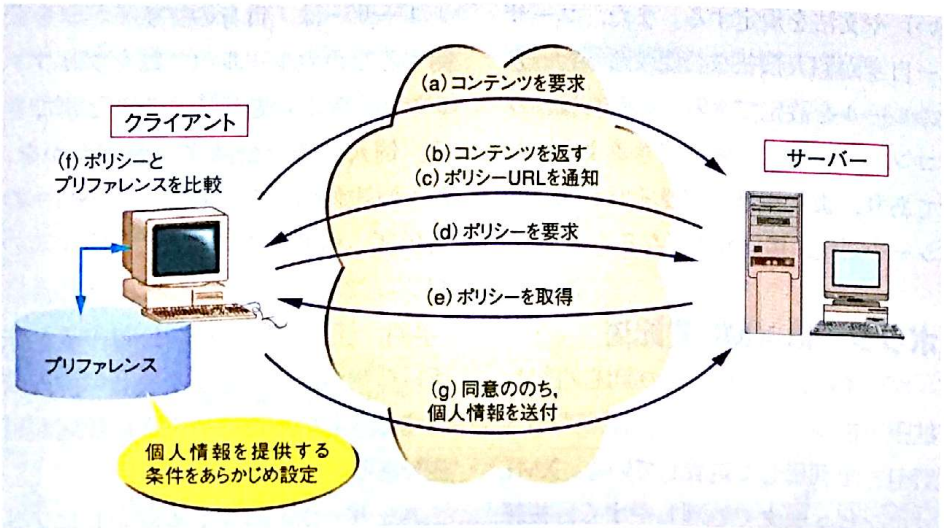


図1　P3P1.0の基本的な処理フロー
Webサイトにアクセスするとプライバシ・ポリシーのURLが返ってくる。そのURLにアクセスしてポリシーを取得し，プリファレンスと比較する。

ポリシーの変更を効率的に通知

前述のように，P3P1.0では1つのコンテンツを取得する際に，コンテンツとポリシーを取得するために，常に2回のアクセスが発生する。性能の低下を抑えるため，P3P1.0ではポリシーの不変則という概念が採用している。これは，ポリシーを示すURLが同一である場合，ポリシーの内容も同じでなければならないというルールである。クライアントは1回アクセスしたポリシ

◆ディジタル署名
公開カギ暗号を用いて，ディジタル・データが通信途上で変更されていないことを証明する技術。電子メールやファイルなどの作成者（責任者）を証明する電子的なデータ。コンテンツのハッシュ値（メッセージ・ダイジェスト）を，作成者の秘密カギで暗号化したものを用いる。

P3P1.0，難産で2000年春勧告化へ

難産の末，1999年11月2日にP3P 1.0の最終ドラフト（ラスト・コール・ワーキング・ドラフト）が発行された。順調に行けば，ラスト・コールの期限である2000年4月30日以降，標準的な手続きを経て，W3C[9]の勧告になる。

W3CにおいてWeb上のプライバシ保護方式に関する検討グループが結成されたのは1997年6月にさかのぼる。当時，Webの急速な広がりに加えて，クッキー技術などによって，Web上で知らないうちにトラッキングされたりすることに，ユーザーが懸念を持ち始めており，一部問題にもなっていた。

検討グループの最初の活動として，まずW3Cにおいてメーリングリストを結成した（最初はP3と呼ばれていたが，のちにP3Pと変更）。この記事の著者の1人もスタート時点から参加し，活発に議論されていた。1997年11月に検討を本格化するために，P3P内部にサブワーキング・グループを結成した。そのグループで頻繁な国際電話会議や，数回，実際に顔を合わせた会議をして，今回の最終ドラフトに至った。

検討フェーズの変化に伴って，P3P Preference Group，P3P Syntax Groupなど約10個のサブワーキング・グループを結成し，密に議論した。また，P3P関連のワーキング・ドラフトとしても，A P3P Preference Exchange Language（APPEL）など数通が出ている。この記事の著者の1人であるマーク・ラングハインリッヒは，NEC在職中からサブワーキング・グループの中心メンバーとして活動し，ワーキング・ドラフトの1つであるAPPELのメイン・エディタとなったほか，最終ドラフトでも著者に名を連ねている。

さて，P3P1.0が難産であったと述べたが，客観的に見て，P3Pの仕様を決定することはW3Cにとっても非常に困難なチャレンジであった（今なおそのチャレンジは現在進行形であるが）と思う。大きな理由としては，「P3Pが，単に技術的な効率や最適性を追求するものではなく，プライバシ保護という社会的影響を考慮し，法制面の動向や世界中の人々の意見を考慮しながら進めなければならなかったこと」，「仕様作成途中段階で，米インタマインド社から『P3Pは当社特許に触れる』という主張があり，W3Cとして初めて特許問題にぶつかったこと」がある。

しかし，この2つの問題は，P3P特有の問題ではなく，今後W3Cがさまざまな勧告仕様を作成していくにあたり，避けて通れない問題であると認識されるようになった。Webがいまや社会のインフラとして，世界の人々の生活，ビジネスに多大な影響を与えるようになったからだ。実際，これをきっかけとして，W3Cでは1999年7月にPatent Policy Working Group10）を発足させ，こうした問題の総合的な扱いを検討するようになった。

この記事では，P3Pの技術的側面を中心としているが，各段階において，社会的側面と技術的側面とのバランスをとりながら決められた仕様であることを念頭に読んでほしい。たとえば，「基本データ・セット」を決めるに際にも，何を含めるかということに関しては社会的影響を考慮して密な議論が行われた。

これまでのワーキング・ドラフトのなかにもP3P1.0以降の発展方向（ディジタル署名による認証機構の拡張など）も示唆されており，1.0の標準化が終了しても次世代P3Pの開発，標準化は継続する。

ーをローカルのリポジトリにキャッシュしておき，ポリシーのURLが同一である場合は，ローカルに保存したポリシーを参照することで，アクセス回数を減らすことができる。

逆に，プライバシ・ポリシーを変更したら，必ず新たなURLを設定してそれを通知しなければならない。単にポリシーを記述したXMLファイルの中身を更新するだけでなく，XMLファイルの名前まで変更する必要がある。

プロトコルや情報フォーマット

サーバーとクライアントは具体的にどのようにやりとりしながらP3P1.0の処理を実現するかをみていこう。

P3Pプロトコルでは，(1) サーバーからクライアントへのポリシーの通知方法，(2) ポリシーをXMLで記述する際の文法および語彙，(3) ユーザーの個人情報に関する基本データ・セット（氏名，住所などの項目）の記述方

◆HTTP拡張プロトコル
IETFで標準化が進められているHTTPを拡張するプロトコル。分散環境でのオーサリングや協調作業，さらにRPC（遠隔手続き呼び出し）なども盛り込もうとしている。現在，インターネット・ドラフトとなっている。

```
HTTP/1.1 200 OK
Opt: "http://www.w3.org/2000/P3Pv1"; ns=11
11-policy: http://coolcatalog.com/P3PPolicy1.xml
...
Content-Type: text/html
...
<HTML>
...
```

リスト1　HTTP拡張プロトコルを利用してプライバシ・ポリシーを通知
網掛けの2行を追加する。"11-Policy"で始まる行が，ポリシーにアクセスするためのURLを示す。

リスト2　HTMLの<LINK>タグを利用してプライバシ・ポリシーを通知
コンテンツの中に<LINK>タグを埋め込むことでポリシーをクライアントに示す。

```
HTTP/1.1 200 OK
...
Content-Type: text/html
...
<HTML>
<HEAD>
<LINK rel="P3Pv1" href="http://coolcatalog.com/P3PPolicy1.xml">
...
```

リスト3　W3CによるP3P1.0仕様書に記載されたポリシーの記述例

```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1" entity="CoolCatalog, Inc.">
  <ASSURANCE-GROUP>
    <ASSURANCE org="http://www.PrivacySeal.org"
      description="PrivacySeal, a third-party seal provider"
      image="http://www.PrivacySeal.org/Logo.gif"/>
  </ASSURANCE-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/PrivacyPractice.html"
    access="none" retention="yes" change_agreement="yes"/>
  <STATEMENT>
    <IDENTIFIABLE><no/></IDENTIFIABLE>
    <CONSEQUENCE-GROUP>
      <CONSEQUENCE>a site with clothes you would appreciate</CONSEQUENCE>
    </CONSEQUENCE-GROUP>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><custom/><develop/></PURPOSE>
    <DATA-GROUP>
      <DATA name="dynamic.cookies" category="state"/>
      <DATA name="dynamic.miscdata" category="pref"/>
      <DATA name="user.gender"/>
      <DATA name="user.home." optional="yes"/>
    </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
    <IDENTIFIABLE><no/></IDENTIFIABLE>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/><develop/></PURPOSE>
    <DATA-GROUP>
      <DATA name="dynamic.clickstream.server"/>
      <DATA name="dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

法，について規定している。また，P3Pに関連して，ユーザーのプリファレンス（プライバシ公開ルール）の記述方法を規定したAPPEL（後述）という規格の標準化作業も進められている。これらについて，P3P1.0の仕様[5]に記述されている例をベースに説明する。

なお，ここでの説明は，P3P1.0仕様を網羅したものではなく，P3Pを理解するうえで重要と思われる項目のみを説明している。完全な仕様に関してはW3CによるP3P1.0仕様を参照されたい。

ポリシーの通知方法は2通り

P3P1.0では，サーバーがクライアントにポリシーを通知するのに，2つの方法を想定している。"HTTP拡張プロトコル[6]を用いる方法（リスト1）と，HTMLの<LINK>タグを用いる方法（リスト2）である。

HTTP拡張プロトコルを用いる方法では，サーバーはリスト1の2行をHTTPのヘッダーに付加してクライアントに送信する。"Opt:"で始まる行が，P3P関連の情報を付加していることを示し，"11-Policy"で始まる行が，ポリシーにアクセスするためのURLを示す。クライアントでは，この行を解釈してポリシーを取得する。

HTMLの<LINK>タグを用いる方法では，サーバーはリスト2のように，応答として返すコンテンツの中に<LINK>タグを埋め込むことでポリシ

リスト4　リスト3の意味を日本語で表現

収集する個人情報の種類ごとに利用目的を別々に記述したり，第三者機関による保証情報を示したりできることがわかる。

CoolCatalog株式会社は，P3P1.0に従いポリシーを宣言する　(01行)。
我々は個人情報としてクッキー（17行），ユーザーの性別（19行），その他の情報（18行）を収集する。また，ユーザーの住所を非必須項目として収集する（20行）。これらの情報は，ユーザーに提示するページをカスタマイズするため，および開発目的に利用する（15行）。これらの情報は，個人を識別する用途には利用しない（10行）。
加えて，我々はWebサーバーのログ履歴（28行），およびユーザーが利用しているブラウザの種類（29行）を収集する。これらの情報はWebサーバーのメンテナンスや開発目的に用いる（26行）。これらの情報は，個人を識別する用途には利用しない（24行）。
こうして収集した情報にユーザーがアクセスすることはできない。我々のプライバシ・ポリシーに関しては，
http://www.CoolCatalog.com/PrivacyPractice.htmlで示すURI（URL）により詳しく説明してある（07行）。
我々のプライバシ・ポリシーに関しては，第三者機関であるPrivacySealが保証している（04行）。

表1　ポリシーを構成するおもなエレメント

エレメント	機能・意味	
<POLICY>	ポリシー全体を記述するためのエレメント	
おもな属性	entity:	ポリシーを作成した主体（会社，団体，個人など）
<ASSURANCE>	ポリシーが正しく守られることを保証する機関に関する情報を記述するエレメント。ポリシーが複数の機関（たとえば政府機関と民間信用調査機関など）によって保証されている場合は，このエレメントを<ASSURANCE-GROUP>エレメントに囲んで複数記述する	
おもな属性	service:	ポリシーを保証する機関のURL（URI）
	description:	ポリシーを保証する機関の簡単な説明
	image:	ポリシーを保証する機関のロゴ・マークのURL（URI）
<DISCLOSURE>	ポリシーに基づいて提供するサービスの情報開示に関する簡単な説明を記述するエレメント	
おもな属性	discuri:	ポリシーを通常の文章で表現するURL（URI）
	access:	このサービスが収集した個人を特定する情報に，ユーザーがアクセス可能かどうかを示す属性。値としては，nonident＝個人を特定する情報は扱っていない，contact＝住所や電子メールアドレスなど，直接的に個人を特定する情報にアクセス可能，other_ident＝銀行口座番号など，間接的に個人を特定する情報にアクセス可能，contact_and_other＝直接的および間接的な個人特定情報の両方にアクセス可能，none＝個人特定情報へのアクセスが不可能のいずれかをとる
<STATEMENT>	個人情報の内容とその利用形態を記述するためのエレメント。このエレメントを複数書くことで，より精密なプライバシ・ポリシーを記述することが可能となる	
<IDENTIFIABLE>	収集した個人情報を，個人を特定する目的で利用するかどうかを示すエレメント。エレメント中に<yes/>または<no/>を記述	
<CONSEQUENCE >	<STATEMENT>の内容を，通常の文章で簡単に説明するエレメント	
おもな属性	xml:lang:	記述している言語を示す属性
<CONSEQUENCE>	エレメントは複数記述可能であるため，これを用いた多言語に対応をすることが可能である	
<PURPOSE>	収集した個人情報の利用目的を記述するエレメント。以下に示すエレメントのうち1つを含む	
<PURPOSE>に含まれるエレメント	<current/>:	サービスの実行に不可欠である（たとえば，購買した商品を届けるために住所を聞く）
	<admin/>:	Webサイトのメンテナンスやサポートのために用いる
	<custom/>:	サービスを個人向けにカスタマイズするために用いる
	<develop/>:	マーケティングや将来のサービス向上など研究開発目的に用いる
	<contact/>:	マーケティングやセールスのため，ユーザーと連絡をとるために用いる
	<other>説明</other>:	以上のいずれにも当てはまらない場合に，個人情報の利用目的を記述する
<DATA >	収集する個人情報の種類と内容を記述する。このエレメントは<DATA-GROUP>内に複数記述することが可能である	
おもな属性	name:	個人情報のデータ名
	optional:	個人情報が必須（ひっす）であるかどうかをyes（必須ではない），no（必須である）で示す
	dataschema:	個人情報のデータ・セットの定義を記述したURLを示す。デフォルトの値はP3P1.0の基本データ・セットを示しているが，必要に応じて，電子商取引用のデータ・セットなどのURLを示す

◆RDF
Resource Description Framework の略。XMLをベースとしてメタ情報を定義するための仕様で，W3Cの勧告となっている。データ・モデル，データ交換の文法，データベースの取り扱いに使うようなスキーマなどが定義されている。

ーをクライアントに示す。この方法ならばHTTP拡張プロトコルと異なり，Webサーバーに手を加えずにP3P1.0に対応できる。しかし，コンテンツがHTML文書である場合にしか利用できないという制約がある。

ポリシーを記述する

個人情報を利用する目的や形態を示すポリシーは，XMLを用いてリスト3のように記述する。リスト3の意味を日本語で表現したのが，リスト4である。収集する個人情報の種類ごとに異なる利用目的を記述したり，第三者機関による保証情報を示したりできることがわかる。

ポリシーを構成するおもなエレメントは，表1のようになっている。

氏名，住所などの基本データ・セット

サーバーが収集する個人情報の基本的なものについては，データの内容を表現する方法を規定している。Webサーバーで新しいデータ・セットを定義して利用することも可能である。

個人情報のデータ名は，ピリオドで区切って記述していく。たとえば，“user.name.first”はユーザーの氏名の名前部分を表す。同様に，“user.name.last”はユーザーの氏名の名字部分である。また，“user.name.”と，ピリオドで終わるデータは，名字，名前，ミドル・ネームなどを含んだ構造体データである名前全体を表す。

P3P1.0では，基本データ・セットとして，ユーザーの基本的な属性を示す“user.”データ・セット，Webアクセスに際して発生する動的な属性を示す“dynamic.”データ・セットの2つを定義している。前者は，名前，性別，住所，年齢，職業，勤務先などを示し，後者は，ユーザーのWebアクセス履歴，利用ブラウザの種類，検索に用いたキーワードなどを含む。

プリファレンスを細かく定義

ユーザーのプライバシ公開ルールであるプリファレンスの記述する規格がAPPEL（A P3P Preference Exchange Language）[7]である。APPELは，プリファレンスをXML/RDF（リソース定義フレームワーク）で記述する文法を定義する。個人情報の種類ごとに，情報を（1）公開する，（2）公開しない，（3）公開するかどうかユーザーに問い合わせる，のいずれかを指定できる。また，それぞれについて，個人を特定する目的で個人情報を利用するかどうか，ポリシーが第三者機関に保証されているかどうか，といった細かい条件を付け加えられる。リスト5にAPPELで記述したプリファレンスの例を示す。

リスト5は，リスト6に示すように，細かな条件を指定している。<APPEL:RULE>で示すルールを複数記述することで，きめ細かいルールを記述できる。

ただし，ここで示したAPPELは，近い将来に改定される見込みであるため，参考として見て欲しい。

P3Pの課題および将来

以上のように，P3Pの最初のバージョンである1.0では，サーバーのポリシーを，コンピュータで理解可能なXMLの形式で，標準化された語彙を用いて記述する枠組みを規定したものである。しかし，プライバシ保護のためには，単にサーバーがプライバシ・ポリシーを公開する以上のさまざまな機能が要求される。そこで，P3P1.0が持つ課題および将来の拡張に関して考えてみる。

データ転送メカニズムを実装すればより便利に

P3Pの標準化の過程では，クライアントからサーバーへのデータ転送メカニズムを規格に含めることを議論していた。結局，1.0の仕様には含まれなかったが，将来のP3Pの仕様に採り入れられる可能性が高い。データ転送メカニズムは，P3P1.0にはない2つの利点を提供する。1つはポリシーと転送データの整合性であり，もう1つはクライアントでの個人情報管理である。

P3P1.0では，ポリシーを見ることで，サーバーがどのようなデータを収集するかを知ることができる。しかし，実際にサーバーにデータを転送するには，HTMLフォームなどの既存の手法を用いる必要があり，これとポリシーの整合性はチェックされない。たとえば，

リスト5　APPELで記述したプリファレンスの例

<APPLE:RULE>で示すルールを複数記述することで，よりきめ細かいルールの記述が可能となる。ただし，ここで示したAPPELは，近い将来に改定される見込みである。

```
01 <APPEL:APPEL>
02 <APPEL:RULESET crtdby="APPEL WG" crtdon="Wed, 12-Aug-1998 09:12:32 GMT">
03    <RDF:SEQ>
04    <RDF:LI>
05       <APPEL:GROUP description"Default Group">
06          <APPEL:RULES>
07                <RDF:SEQ>
08                   <RDF:LI>
09                      <APPEL:RULE behavior="accept" quant="ONLY"
10                          description="Service only collects clickstream data">
11                          <P3P:PROP assurance="*">
12                              <P3P:USES>
13                                 <P3P:STATEMENT action="r" id="0">
14                                    <P3P:REF name="ClickStream.Client_"/>
15                                 </P3P:STATEMENT>
16                              </P3P:USES>
17                              <P3P:DISCLOSURE discURI="*"/>
18                          </P3P:PROP>
19                      </APPEL:RULE>
20                   </RDF:LI>
21                   <RDF:LI>
22                      <APPEL:RULE behavior="reject"
23                          explanation="I don't want to be identified!">
24                          <APPEL:OTHERWISE/>
25                      </APPEL:RULE>
26                   </RDF:LI>
27                </RDF:SEQ>
28          </APPEL:RULES>
29       </APPEL:GROUP>
30    </RDF:LI>
31    </RDF:SEQ>
32 </APPEL:RULESET>
33 </APPEL:APPEL>
```

リスト6　リスト5を通常の文章で表現

サーバーが提示しているポリシーが，何らかの第三者機関による保証を受けており（11行），ポリシーの詳細な説明が公開されており（17行），かつクリック履歴（ClickStream）のデータのみを（14行）ユーザーを特定しない目的で（13行 id="0"）集めるならば，そのポリシーを受け入れる（09～10行目）。それ以外の場合は（24行），ポリシーを受け入れない（22～23行）

ポリシーでは「名前と性別を収集する」と述べても，名前と性別だけでなく，住所も入力させるHTMLフォームをユーザーに表示する，という事態も起こり得る。

データ転送メカニズムでは，クライアントのソフトウエアがポリシーに記載した個人情報のみを送ることで，ポリシーと転送する個人情報の整合性を保つことができる。

またP3P1.0では，異なるWebサービスにアクセスするたびに，個人情報を入力しなければならないというユーザーの手間は解消されない。これに対しデータ転送メカニズムを用いると，ユーザーは1回入力した情報を改めて入れなくてよい。クライアント・ソフトウエアがローカル・レポジトリにユーザーが入力した個人情報を蓄え，ここから読み出した個人情報をサーバーに転送する。

以上の2つの特長を実現するため，データ転送メカニズムでは，サーバー-クライアント間で図2に示すようなやり取りを実行する。1.0に比べて複雑に見えるが，ほとんどのやり取りはクライアント－サーバーのソフトウエア間

で自動的に実行する。ユーザーからは，「コンテンツを要求し，質問された個人情報を入力し，コンテンツを得る」といういつも通りの単純なプロセスに見える。

具体的には，クライアントがコンテンツを要求する（a）と，サーバーはコンテンツを返す前にポリシーURLを返す（b）。クライアントはポリシーを要求し（c），それを取得する（d）と，ポリシーがユーザーのプリファレンス（個人情報開示に関するユーザーのポリシー）と合っているかどうかを調べる（e）。合っている場合は，クライアントが個人情報をサーバーに転送する（g）。サーバーは必要な個人情報を受け取ると，カスタマイズなどを行った結果のコンテンツを返す（h）。

こういったデータ転送メカニズムが実装されると，より使いやすいシステムが構築できる。

拡張データ・セットの追加が可能

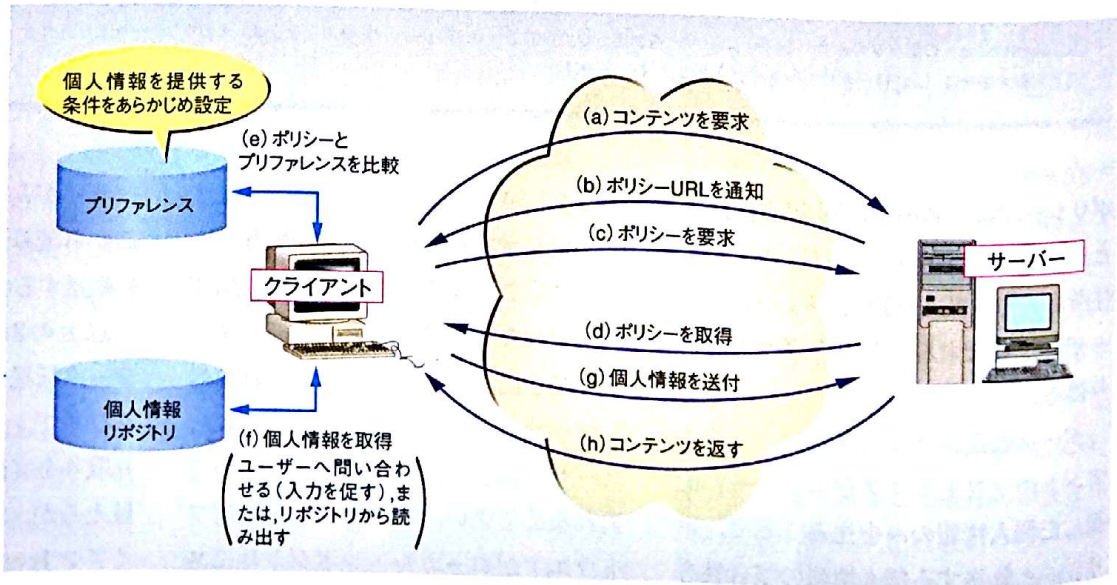
P3P1.0が定義する“user.”，“dynamic.”の2つのデータ・セットに含まれない個人情報を扱うには，各Webサービスがデータ・セット拡張メカニズムを利用する必要がある。今後，需要の多いデータ・セットは，逐次標準として追加されていくであろう。たとえば，クレジット・カード番号，請求書の送付先などを網羅したEC向け個人情報データ・セットは，最も需要が多いものの1つであろう。

認証メカニズムも重要である

P3P1.0では，Webサーバーが提示したポリシーが守られるかどうかの観点からは保証していない。また，第三者機関が保証したポリシーが，あとで勝手に変更されてもチェックできない。もちろん，これらはむしろ社会的・法的な側面から監視されるべきポイントである。しかし，技術的にもディジタル署名XML Signature[8]を利用したポリシー・ファイルの信頼性向上などが仕様に加えられていくべきであると思われる。

参考文献
1) Platform for Privacy Preferences Project (P3P), http://www.w3.org/P3P/
2) Extensible Markup Language (XML), http://www.w3.org/XML/
3) Hypertext Transfer Protocol - HTTP/1.1, http://www.w3.org/Protocols/HTTP/1.1/draft-ietf-http-v11-spec-rev-06.txt
4) Uniform Resource Identifiers (URI): Generic Syntax, http://info.internet.isi.edu/in-notes/rfc/files/rfc2396.txt
5) The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, http://www.w3.org/TR/1999/WD-P3P-19991102
6) HTTP Extensions, http://www.w3.org/Protocols/HTTP/ietf-http-ext/draft-frystyk-http-extensions-03.txt
7) A P3P Preference Exchange Language (APPEL), http://www.w3.org/TR/WD-P3P-preferences
8) XML-Signature Core Syntax and Processing, http://www.w3.org/TR/xmldsig-core
9) World Wide Web Consortium (W3C), http://www.w3.org/
10) W3C Patent Policy Working Group, http://www.w3.org/Consortium/Patent/Group/

図2　データ転送メカニズムを用いた処理フロー
ユーザーは1回入力した情報を再び入れなくて済むようになる。クライアント・ソフトウエアがローカルレポジトリにユーザーが入力した個人情報を蓄え，ここから読み出した個人情報をサーバーに転送する。



◆CGI
Common Gateway Interfaceの略。Webサーバーがバックエンド・プログラム（ゲートウエイと呼ぶ）との間で情報のやりとりに用いるインタフェース。Webブラウザが Webサーバー経由でデータベース・サーバーに問い合わせを発行する場合など，対話型のWebページを作成する場合に利用する。Webブラウザからの要求を受け付けて，外部プログラムを呼び出し，プログラムの実行結果をWebブラウザに返すという流れである。

◆ウイザード
画面に現れる一連の質問に答えていくだけで1つの事柄に関する様々な設定ができるもの。もともとはコンピュータを使いこなし，「あっ」と驚くようなことができるようにする人のことを指す。ところが米マイクロソフトが自社のアプリケーションにウイザード機能と呼ぶ一連の機能を入れたため，それを指すようになった。

◆ローカル・プロキシ・サーバー
自分のパソコンなどに配置して，ユーザーまたはグループで専用に使うプロキシ・サーバー。プロキシ・サーバーは，Webなどインターネットのさまざまなサービスへのアクセスを中継するためのソフトウエアのこと。

Part 3

P3Pの開発
実装のポイント すでに開発，実験が始まる

P3Pに関するソフトウエア・ライブラリなどの開発や実装例はすでにいくつかある。それらのほとんどは，1998年11月から1999年8月までに公開されたドラフトに基づいた実装例であり，1999年11月2日に発表されたP3P1.0最終ドラフトのものは少ないが，参考システムとしての意味は大きい。

ENCの情報管理システム

W3Cは，Webサイト（http://www.w3.org/P3P/implementations）でP3P関連のシステム紹介している。

電子ネットワーク協議会（ENC）が開発した「プライバシー情報管理システム[1]」は，P3Pに関するクライアント，サーバー双方に必要な機能を網羅した本格的なシステムである（図1）。1998年11月に公開されたドラフトに準拠した機能を持つ。

サーバー側には，P3Pに対応するWebサービスの構築を支援する「P3Pオーサリング・ツール」（写真1）というアプリケーションを用意する。オーサリング・ツールは，CGI作成機能，ポリシー作成ウイザードの2つの機能で構成する。CGI作成機能は，クライアントからの要求に対して適切なポリシーURLを返すPerlプログラムを対話的に生成するものである。

データ転送メカニズムにも対応しており，クライアントから送られてきた個人情報の種類に応じて，異なったコンテンツを返すような機能も容易に実現することができる。また，ポリシー作成ウイザード機能を用いると，ビジュアルな環境でプライバシ・ポリシーXMLファイルを対話的に生成できる。

クライアント側は，個人情報設定ツール，ローカル・プロキシ・サーバーの2つのツールで構成する。個人情報設定ツールは，ユーザーの個人情報公開ルール（プリファレンス）を対話的に設定する機能を提供する。ローカル・プロキシ・サーバーは，WebブラウザとWebサーバーの間に介在して，サーバーのポリシーを取得し，個人情報設定ツールで設定したプリファレンスとマッチングさせる機能を持つ。

AT&TのPrivacy Minder

米AT&Tの「Privacy Minder[2]」は，

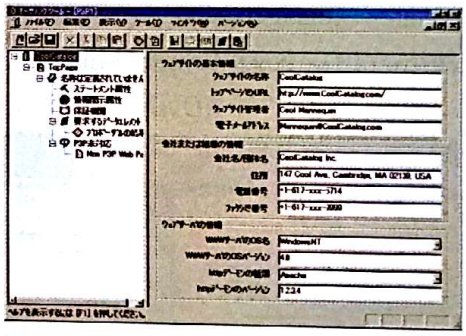


写真1　P3Pオーサリング・ツール
P3Pに対応したWebサービスの構築を支援する。

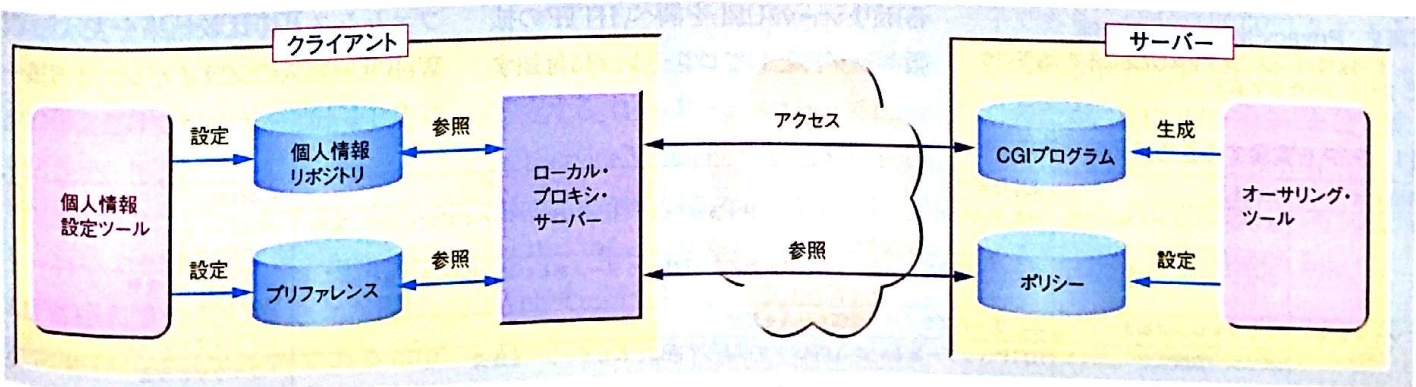


図1　電子ネットワーク協議会が開発した「プライバシー情報管理システム」
P3Pに関するクライアント，サーバー双方に必要な機能を網羅した本格的なシステムである。

◆XMLエディタ
XMLの記述を支援するエディタ。自分で設定したタグを簡単に挿入したり，構文をツリー上に表示したりする機能を備える。すでにいくつもの製品が販売されている。

Javaで記述された，クライアント側で動作するローカル・プロキシ・サーバーである。WebブラウザとWebサーバーの間に介在して，サーバーのポリシーの取得，プリファレンスとポリシーのマッチングなどを行う。また，データ転送メカニズムにも対応しており，リポジトリに格納されている個人情報を自動的にサーバーに送る，格納されていない個人情報はユーザーに問い合わせたあとレポジトリに格納する，といった機能も備えている。

写真2はPrivacy Minderの実行例である。右下のウインドウがブラウザであり，この例ではユーザー購買ページにアクセスしたところである。上部の細長いウインドウがPrivacy Minderのメイン・ウインドウであり，ブラウザがアクセス中のページがP3Pに対応していることを示している。左下は，ユーザーにアクセス中のページの状況を伝えるウインドウである。

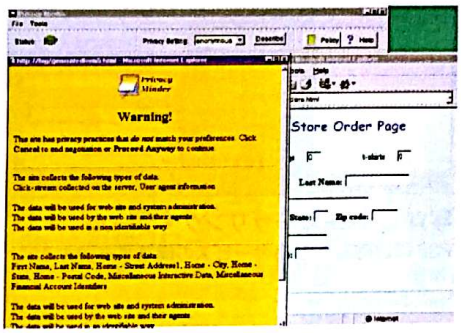


写真2　Privacy Minderの実行例
ユーザー購買ページにアクセスしたところで，右下のウインドウがブラウザである。

サーバーに必要な機能

P3Pを実現するには，サーバー，クライアント双方で複数の機能を実装する必要がある（表1）。

ポリシー作成機能は，Webサービス提供者が，サービスに先立ちポリシー・ファイルを生成する，ビジュアルなXMLエディタともいえる。実装形態としては，XMLエディタをP3Pポリシー向けに特化させたものと，CGIを用いてポリシーの作成，Webサーバーへのセット・アップ，WebページとポリシーURL（正確にはURI，以下同）のマッピングといった一連の作業を支援するものが考えられる。

P3Pに対応したWebサーバーがコンテンツの要求を受けるたびに働く，ポリシーURL通知機能も必要である。この機能は，要求されたコンテンツと対応するポリシーのURLを調べ，HTTPの拡張ヘッダーとしてコンテンツに付加する。実装形態は2種類。1つは，HTTPの要求で起動するHTTPフィルタ・モジュールとして実装する形態。この形態は，従来のCGIプログラムやHTMLファイルに変更を加える必要がない。もう1つがHTMLファイルやCGIを改造する形態。HTMLファイルには<LINK>タグを埋め込み，CGIにはHTTP拡張ヘッダーにコードを加える。HTTPサーバーの設定を変更しなくて済む。

クライアントに必要な機能

ユーザーが，自身のプライバシ公開ルールを設定するのを支援するためのエディタ「プリファレンス設定機能」が必要である。XMLエディタをP3Pプリファレンス向けに特化させるという形態が一般的である。将来的にはユーザーの過去の行動履歴から自動的にプリファレンスを生成するような高度な実装形態も考えられる。

ポリシー取得機能は，サーバーから通知されたポリシーURLに自動的にアクセスし，それを通常の文章に訳してユーザーに表示する，あるいは，プリファレンスとの比較結果を表示して，Webサービスのプライバシ・ポリシー

表1　P3Pを実現するために必要な機能

機能分類	機能名	機能概要	実装形態
サーバー	ポリシー・ファイルの作成	XML形式のポリシー・ファイルの記述を支援。CGIではWebサーバーへの設定も同時に実行	・CGI ・アプリケーション
	ポリシーURL（URI）通知	サーバーが返すコンテンツに，P3P対応のHTTPヘッダー，あるいは<LINK>タグを付加	・CGI，HTML変更 ・HTTPフィルタ・モジュール
クライアント	プリファレンス設定	ユーザーのプライバシ公開ルールを設定	・アプリケーション
	ポリシー取得	HTTPヘッダーあるいは<LINK>タグによって通知されたポリシーを取得	・ブラウザの改造 ・プラグイン ・ローカル・プロキシ
共通	ポリシー解釈ライブラリ	ポリシーXMLを解釈するライブラリ。ポリシーの自然言語表現などを含む	・ライブラリ

リスト1　ApacheをP3P対応にする最も簡単な方法
Apacheの設定ファイルであるhttp.confに以下の4行を付け加え、URLで示すポリシー・ファイルを用意する。

```
<Directory>
  Header set Opt "http://www.w3.org/2000/P3Pv1" ;ns=11
  Header set 11-policy http://coolcatalog.com/P3PPolicy1.xml
</Directory>
```

リスト2　Apacheでディレクトリごとに異なるP3Pポリシーを利用する場合
ディレクトリごとの設定ファイルである.htaccessに、以下の2行を付け加えればよい。

```
Header set Opt "http://www.w3.org/2000/P3Pv1" ;ns=11
Header set 11-policy http://coolcatalog.com/P3PPolicy2.xml
```

を伝えるという役割を持つ。

実装形態としては，(1) Webブラウザに組み込む，(2) クライアント・マシン上で動作するプロキシ・サーバー（ローカル・プロキシ）として動作し，サーバーから通知されたURLを見て処理する――が考えられる。

共通的な機能は，ライブラリなどの形で提供されるのが一般的である。具体的には，XMLで記述されたポリシーを読み込み，ほかのプログラムから利用可能な形態に変換するポリシー解釈ライブラリ機能である。XML操作ライブラリに，P3P特有の機能を付け加えた形態になるであろう。また，XMLで表現したポリシーを，通常の文章に変換するような機能も必要になる。

Webサーバーの対応

現時点でも，制限はあるものの，多少の作業だけでWebサーバーをP3Pに対応させられる。

Apacheは，代表的なフリーのWebサーバー・ソフトである。ApacheをP3P対応にする最も簡単な方法は，Apacheの設定ファイルであるhttp.confにリスト1の4行を付け加え，URLで示すポリシー・ファイルを用意することである。これにより，このWebサイトに対するすべてのHTTPリクエストの応答に，リスト1のヘッダーが付け加えられる。この方法は，サイト全体が同一のP3Pポリシーを利用する場合に向いている。

もう少し細かく，ディレクトリごとに異なるP3Pポリシーを利用したい場合には，ディレクトリごとの設定ファイルである.htaccessに，リスト2の2行を付け加える（あるいはこの2行を含むファイルを作成する）。そのディレクトリ配下へのHTTPリクエストの応答に，このヘッダーが付加される。

以上の方法は，Apacheのバージョン1.2以上で利用できる。

IISはサイト全体の設定のみ可能

マイクロソフトは，Internet Information Server（IIS）では，以下の手順で設定する。(1)スタートメニューでInternet Service Managerを選び，Microsoft Management Consoleを起動する。(2)ツリー・ビューをたどり，設定対象のWebサーバーを選択する。(3)Webサーバー上で，マウスの右ボタンをクリックしプロパティ・メニューからダイアログを起動する。(4)ダイアログからHTTP Headersタブを選ぶ。(5) Custom HTTP Headersの項目でAddボタンを押し，Custom Header Nameの欄に“Opt”を，Custom Header Valueの欄に“"http://www.w3.org/2000/ P3Pv1"; ns=11”を入力し，OKボタンを押す。(6)同様に，再びAddボタンを押し，Custom Header Nameの欄に“11-policy”を Custom Header Valueの 欄 に“http://coolcatalog.com/P3PPolicy1.xml”を入力し，OKボタンを押す。

これはサーバー全体に対する設定であり，IISの場合ディレクトリごとの設定はできない。

Apache，IISともに，この設定方式では，ns=11の数値を固定的に与えざるを得ない，という制限事項がある。この数値はHTTP拡張ヘッダーの識別子であり，1回のHTTPリクエストの応答値の中で一意でなければならない。このため，HTTPサーバーを設定する際には，ほかのサービスが使っている数値をあらかじめ把握し，ぶつからないように記述する必要がある。

参考文献
1) プライバシー情報管理システム，http://www.nmda.or.jp/enc/privacy/
2) Privacy Minder, http://www.research.att.com/projects/p3p/pm/