インターネット最新テクノロジー：第36回

プライバシー保護の国際標準規格

P3P
(Platform for Privacy Preferences Project)

ショッピングサイトのように、電話番号やクレジットカード番号といった重要なプライバシー情報をインターネットに流す場面はますます増えている。P3Pは、ウェブサイトが収集するプライバシー情報の種類や利用目的を記述するための標準規格であり、利用者が個人情報をサイトに与えるかどうかの判断を助けることを可能にする。

小池 雄一　W3C/日本電気(株)

P3Pはプライバシーポリシー開示の標準規格

米国を中心として、インターネットにおけるプライバシー保護の意識が高まっている。2000年5月には、米連邦取引委員会（FTC）が、プライバシーポリシーの開示をウェブサイトに義務付ける法規制を行うよう議会に勧告した Jump01 。また、オンライン広告大手の米ダブルクリックは、クッキーを使って収集した履歴情報と個人名などの情報を結びつける計画を、消費者団体や業界からの強い反対によって延期した。

プライバシー保護にはさまざまなアプローチがあり得るが、もっとも基本的かつ重要なのがプライバシーポリシーの開示だ。すなわち、ウェブサイトが収集する個人情報の種類、利用目的、収集した情報を第三者に流すかどうかという情報を利用者に提示することである。

プライバシー意識の高まりを反映して、現在では著名サイトの多くがプライバシーポリシーを公開している。しかしながら、プライバシーポリシーは長文になりやすく（たとえば米ヤフーのプライバシーポリシー Jump02 は文章だけで25Kバイトもある）、用語もサイトごとに異っているため、正確な意味を理解するのが難しくなっている。このような理由から、プライバシーポリシーは必ずしも利用者に読まれているとは限らないのが現状である。

こうした中、ウェブに関する国際標準化団体World Wide Web Consortium（W3C）は1997年に、プライバシーポリシーを記述するP3Pの開発を開始した。以来、約3年の開発期間を経て、P3Pの規格はほぼ固まりつつある Jump03 。P3Pは主として以下のことがらを定めたものである。

- プライバシーポリシーをサーバーからクライアント（ウェブブラウザー）に送付するためのプロトコル
- プライバシーポリシーをXMLで記述するための文法と標準的な語彙

プライバシーポリシーがコンピュータに理解可能なXML形式で記述されているため、ウェブブラウザーが自動的にプライバシーポリシーを読み、個人情報を与えてよいかどうかを判断するといった処理が可能となる。利用者がいちいち長大なポリシーを読んで判断しなければならない現状を考えると、大きな進歩である。また、ポリシーとして記述すべき項目が明確に定められており、必要な情報が欠落したポリシーや不明瞭なポリシーが現れにくくなる効果も期待される。

また、プライバシー保護というと利用者のためだけにあるように思われがちであるが、信頼できるプライバシーポリシーを開示しているウェブサービスにとっては、逆にサービス向上に不可欠な個人情報を集めやすくなる可能性もあるという側面も忘れてはならない。

Jump01 www.ftc.gov/opa/2000/05/privacy2k.htm
Jump02 docs.yahoo.com/info/privacy/
Jump03 www.w3.org/P3P/

XMLで記述するプライバシーポリシー

それでは、プライバシーポリシーはどのように記述するのだろうか。実際のプライバシーポリシー（図1）を、P3P仕様書 Jump 04 に基づいてXMLで記述した例（図2）で示してみる。プライバシーポリシーに必要な項目には、以下のような種類がある。

1. 収集する個人情報の種類

ウェブページで、実際に収集する個人情報の種類を記述する。これは、プライバシーポリシーの中でも最重要項目の1つである。P3Pでは、名前や電話番号などの基本的な情報に関する語彙を制定しているため、それに従って記述を行う。また、利用者のウェブ閲覧履歴や利用しているウェブブラウザーの種類など、個人情報とは言えないがプライバシーにかかわる情報についても、標準語彙として定義されている。

2. 利用目的

収集した情報の利用目的を記述する。利用目的に関しても、個人情報を利用したウェブページのカスタマイズに用いる、ウェブで購入した商品の配達に用いるなど、8種類が語彙として用意されている。

3. 利用範囲

収集した情報の利用範囲、すなわち、個人情報を第三者に渡すかどうか、あるいは収集した個人情報をウェブページ上で公開するかなどの情報を記述する。これにより、利用者は自分のプライバシー情報が売り渡されたりしないかどうかを知ることが可能となる。

4. 保存期間

収集した情報を保存する期間を記述する。

1から4までの情報は、1つのプライバシーポリシーの中に複数記述できるため、「住所と

・当組織は、個人情報として、WWWサーバーの標準ログ❶と、利用しているWWWブラウザーの種類❷を収集します。
・収集した情報の利用目的は、ウェブサイトのシステム管理❸と、調査および開発❹です。
・収集した情報の利用範囲は、組織および当組織の業務委託先❺です。
・収集した情報の保有期間は、明記された目的にそう適切な期間❻です。
・当組織の連絡先は、以下の通りです。
CatalogExample社
4000 Lincoln Ave.
Birmingham, MI 48009
USA
catalog@example.com
+1（248）392-6753 ❼
・収集された個人情報へのアクセス手段は、ありません❽。
・このポリシーに関する異議については独立機関❾である、PrivacySeal.example.org❿
（http://www.privacyseal.example.org）に申し立てを行うことができます。

図1 CatalogExample社のプライバシーポリシー

```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
    discuri="http://www.catalog.example.com/PrivacyPracticeBrowsing.html">

<ENTITY>
 <DATA-GROUP>
  <DATA ref="#business.name">CatalogExample</DATA>
  <DATA ref="#business.contact-info.postal.street.line1">4000 Lincoln Ave.</DATA>
  <DATA ref="#business.contact-info.postal.city">Birmingham</DATA>
  <DATA ref="#business.contact-info.postal.stateprov">MI</DATA>
  <DATA ref="#business.contact-info.postal.postalcode">48009</DATA>
  <DATA ref="#business.contact-info.postal.countrycode">USA</DATA>
  <DATA ref="#business.contact-info.online.email">catalog@example.com</DATA>
  <DATA ref="#business.contact-info.telecom.telephone.intcode">1</DATA>
  <DATA ref="#business.contact-info.telecom.telephone.loccode">248</DATA>
  <DATA ref="#business.contact-info.telecom.telephone.number">3926753</DATA>
 </DATA-GROUP>
</ENTITY>

<ACCESS><nonident/></ACCESS>

<DISPUTES-GROUP>
 <DISPUTES resolution-type="independent"
   service="http://www.PrivacySeal.example.org"
   short-description="PrivacySeal.example.org">
  <IMG src="http://www.PrivacySeal.example.org/Logo.gif"/>
  <REMEDIES><correct/></REMEDIES>
 </DISPUTES>
</DISPUTES-GROUP>

<STATEMENT>
 <DATA-GROUP>
  <DATA ref="#dynamic.clickstream.server"/>
  <DATA ref="#dynamic.http.useragent"/>
 </DATA-GROUP>
 <PURPOSE><admin/><develop/></PURPOSE>
 <RECIPIENT><ours/></RECIPIENT>
 <RETENTION><stated-purpose/></RETENTION>
</STATEMENT>

</POLICY>
```

図2 XMLで記述したプライバシーポリシー

XML（エックス・エム・エル／eXtensible Markup Language）：文書の構造を記述するための言語。文書の中にタグを埋めこむ形で利用され、ウェブページを記述するHTMLとは異なり、ユーザーが独自のタグを定義できる。

電話番号は購入した商品の配送のために収集し、年齢と性別はマーケティングのために利用する」といった複雑なパターンにも対応可能となっている。以上がプライバシーポリシーを構成するうえでの基本的な情報である。

これに加え、以下の情報も記述する。

5. 誰が個人情報を収集しているか

個人情報を収集している組織または個人（すなわちウェブページの作成者）に関する情報を記述する。組織・個人名は必須であり、必要に応じて住所、電話番号などを追加する。

6. 収集された個人情報へのアクセス手段

また、ひとたび収集した情報に、利用者がアクセスして確認などを行うことができるかどうかの情報も記述する。

7. ポリシーに関する異議の申し立て手段

最後に、プライバシーポリシーに誤りがあったり、プライバシーポリシー違反が行われた場合の苦情の申し立て手段を記述することができる。申し立て手段としては、1）ウェブサイトを運営する企業自身への連絡、2）第三者機関への通知、3）法的な手段、のどれかを指定する。P3Pの場合、特に重要なのは2）である。ウェブサービスが、JIPDECのPrivacyMark制度 Jump05 、TRUSTe Jump06 、BBB Online Jump07 など、プライバシー情報の取り扱いに関する信頼性保証制度によって保証されている場合、異議申し立て手段としてその保証機関を指定することで、サービスの信頼性を向上させることが可能となる。

Jump04 www.w3.org/TR/P3P/
Jump05 www.privacymark.gr.jp
Jump06 www.truste.org
Jump07 www.bbbonline.org

P3Pによって変わるウェブプロトコル

さて、ウェブサービスをP3P対応にするには、以上の手順で記述したP3P形式のプライバシーポリシー（以下P3Pポリシー）をウェブ上に置くとともに、ウェブページのURIとP3PポリシーのURIの対応関係を記したポリシーリファレンスを置く必要がある。すなわち、通常のウェブページには個人情報を収集しない旨を記したP3Pポリシーを、ショッピングのウェブページには、ショッピング用のP3Pポリシーを、それぞれ対応付ける。

利用者がP3P対応のウェブブラウザーでウェブサーバーにアクセスすると、図3に示すように、通常のウェブページ要求→取得サイクルの前に、P3Pポリシーのチェックが行われるようになる。これにより、利用者がショッピング履歴を他社に提供するようなサイトにアクセスしようとしたら事前に警告するといった動作が可能となる。

通常のウェブアクセスに比べてアクセス回数が多くなるように見えるが、P3Pポリシーやポリシーリファレンスの変更頻度は低く、ほとんどの場合はキャッシュが用いられるため、性能に与える影響は低いと思われる。

現在、P3Pポリシーの交換プロトコルは、WWWでの利用のみが規定されているが、将来的には電子メールやデジタルデータ放送などでもP3Pを利用できるように拡張可能である。

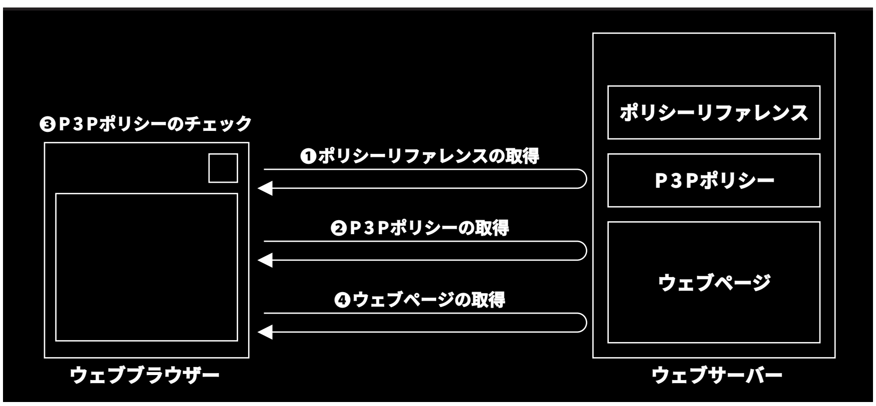

図3 P3P導入後のウェブアクセス

▼

URI（ユー・アール・アイ／Uniform Resource Identifiers）：インターネット上にある情報を記述する方法の総称。現在のところはURLのことだと思っておけばよい。将来的にはURL以外の記述方法が用いられる可能性もあるため、プロトコルを定義する場合には「（URLを含む）記述方法全般」という意味で「URI」という単語を用いることが多い。

米国を中心に進むP3Pの実装

P3Pは仕様がほぼ固まりつつあることもあり、P3Pに関する実装や、P3Pをサポートしたウェブサイトもしだいに増えつつある。

ウェブブラウザーについては、マイクロソフトがインターネットエクスプローラの次期バージョンにP3P対応機能を実装することを2000年6月に発表した。また、オープンソースプロジェクトで開発されているMozillaブラウザーでも、P3P機能の実装が開始された。以上の動きから、2000年末には主要なブラウザーによるP3Pサポートの完了が期待できる。また、サイト側の対応としては、すでに、米国のホワイトハウス、AOL、IBM、マイクロソフトといったウェブサイトがP3Pに対応している。

ウェブサイトのP3P対応を支援する実装も現れている。P3PポリシーはXMLで記述するため、誰にでも書けるものではない。また、プライバシーポリシーというものは信頼性が重視されるため、HTML文書のように多少の間違いならば許容されるというものでもない。IBMではP3Pを記述できる専用ソフト「P3P Policy Editor」 Jump 08 を配布している（図4）。また、マイクロソフト、PrivacyBot、電子ネットワーク協議会なども、ウィザード形式のポリシー作成ツールを開発している Jump 09 Jump 10 Jump 11 。また、W3CではウェブサーバーがP3Pに対応しているかどうかを検査するサービス Jump 12 を提供している（図5）。こうしたツールの存在により、P3P対応ウェブサーバーの数も飛躍的に増加していくものと思われる。

Jump 08 www.alphaworks.ibm.com/tech/p3peditor
Jump 09 privacy.linkexchange.com
Jump 10 www.privacybot.com
Jump 11 www.nmda.or.jp/enc/privacy/
Jump 12 big.w3.org/cgi-bin/validate.pl

プライバシー保護には P3P以外の技術も必要

以上、P3Pについて概観したが、最後に1つ強調しておきたいのは、P3Pはプライバシーポリシーの開示という、プライバシー保護に関する1つの技術的側面を支援するものであり、より高いレベルのプライバシー保護のためには他の技術との組み合わせが不可欠ということである。

たとえば、いくらP3P形式でプライバシーポリシーが開示されていても、ウェブサービス自体がポリシーを守っていなければ何もならない。こうした状況を防ぐためには、第三者による監視の仕組みが必要である。あるいは、XML Signature技術 Jump 13 を用いて、P3Pポリシーを保証機関によって署名するといったアプローチも考えられる。

また、ウェブサイトがP3Pに非対応で、利用者の意にそぐわない方法でIPアドレスを記録利用している場合にも、そのサイトからプライバシーを守るにはP3Pだけでは不十分である。こうした場合には、中継サーバーにより匿名を確保するAnonymizer Jump 14 のようなサービスとの組み合わせが不可欠となる（あるいはウェブサイトを訪れないという方法しかない）。

以上のように、P3Pが対象としていない、あるいはP3Pの力が及ばない範囲はあるものの、ウェブサービスによるプライバシーポリシー開示とそれに基づいた利用者による正しい判断はプライバシー保護の最重要部分であり、それがP3Pの普及により促進されることは確かであると思われる。

Jump 13 www.w3.org/Signature/
Jump 14 www.anonymizer.com

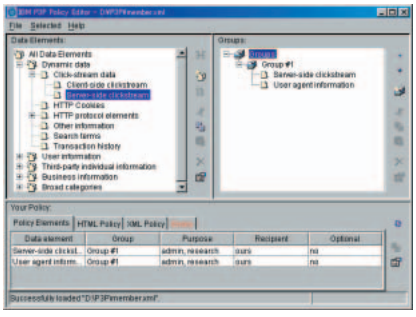

図4 IBM Policy Editor

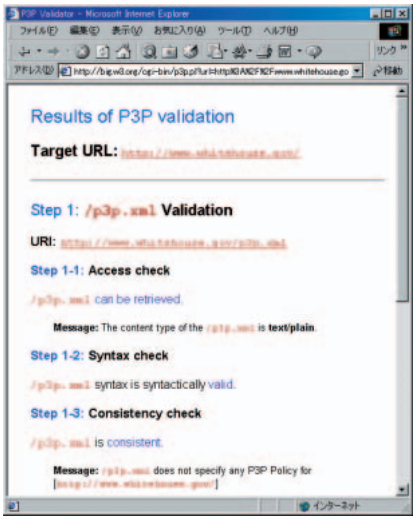

図5 W3CのP3P Validationサービス（www.whitehouse.govを検証中）

オープンソース：ソフトウェアの設計図にあたるソースコードを無償で公開し、誰でも自由に改良したり配布したりできるようにしたもの。これによりソフトウェアの普及を促進し、より洗練されたソフトウェアが完成するというメリットがある。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp