情報流通促進のための個人情報保護フレームワークの検討

4Q－2

長谷川 知洋　寺西 裕一　梅本 佳宏　佐藤 哲司
NTTサイバースペース研究所

1. はじめに

インターネットを利用したオンラインショッピングや電子商取引では、消費者の氏名や住所などの個人情報の入力が必要である。インターネット上の個人情報を保護するための法規制としては、95年10月の「EU指令」[1]の採択と前後して各国、法の整備が進んでいる。しかし現実には、これらの個人情報が意図した範囲内で適正に使用されるかどうかは、個人情報の著作者である消費者ではなく、取引先の判断に委ねられている。

本稿では、自分の個人情報が意図した目的以外に使用されたり、取引先以外の第三者に漏洩するのではないかという消費者の不安を取り除く個人情報保護のフレームワークを提案する。

2. 個人情報保護

電子商取引においては、個人情報を「保護」しようというニーズと「利用」しよう というニーズの双方が高まり、両者をどのように調整するかが問題になっている。本節では、インターネット上での個人情報管理関連技術について述べる。

2.1. Open Profiling Standard(OPS)

Open Profiling Standard(OPS)[2]は、利用者とWebサイトとの間で個人情報を共有するときの仕様で、プライバシー保護の機能が組み込まれている。利用者がOPSをサポートするWebサイトに初めて訪問した時、Webサイトは個人情報を要求する。利用者はWebサイトの目的に応じて、要求された個人情報のすべてを公開／一部を公開／何も公開しないを選択できる。

しかし、公開された個人情報に与えられる権利が不明確なので、Webサイトに対して個人情報を一度でも公開すると、Webサイトがその情報を再利用するために保持したり、Webサイト間で情報共有することを防ぐことができない。

2.2. Platform for Privacy Preferences(P3P)

Platform for Privacy Preferences(P3P)[3]は、Webサイトを訪れた利用者の個人情報に開示／拒否／拒否の場合の代替条件を設定することで個人情報を保護する仕組みである。Webサイトが個人情報を入手する時、取得したい個人情報の項目、利用目的や開示する範囲などを Web サイトのプライバシーに関する要求として利用者に明示する。利用者はその説明内容に応じて、個人情報の開示に合意／拒否／代替条件を採用するか選択できる。合意できる場合にのみ、個人情報をWebサイトに渡す。Webサイトが予めプライバシーに関する要求を宣言し、利用者が個人情報のデータセットと開示のための条件設定を用意しておけば、Webサイトの要求と利用者の設定とを比較し、自動的に合意に至ることができる。合意に至らなくてもWebサイトが利用目的に応じて複数の要求を宣言していれば、別の要求に対して合意に至ることができる。さらに、Webサイトは利用者が訪れる度にプライバシーに関する要求を送らなくても、以前合意が取れたものに関しては、再取得する必要がない。

しかし、P3Pでは取得した個人情報の譲渡など、個人情報の正当な二次利用については、実施者の判断に任されていた。

A Framework of Privacy Protection for Information Sharing
Tomohiro HASEGAWA, Yuuichi TERANISHI,
Yoshihiro UMEMOTO, Tetsuji SATOH
NTT Cyber Space Laboratories
1-1 HikarinookaYokosuka-shi Kanagawa 239-0847

3. 利用制約に基づく個人情報の保護・流通管理

我々は利用制約に基づくコンテンツの流通管理モデルを提案してきた[4,5]。本モデルに個人情報を適用することで、OPSやP3Pでの問題を解決することを考えている。そこで本節では、我々が提案しているモデルの概要について述べる。

3.1. ポリシーによる利用制約管理

本モデルでは、コンテンツの著作者、利用者双方がコンテンツに対する利用制約をルールとして記述する。この利用制約の集合をポリシーと呼ぶ。このうち、著作者がコンテンツに対して規定するポリシーをコンテンツポリシー、利用者がコンテンツに対して規定するポリシーを利用者ポリシーと呼ぶ。これらに基づいて導出される利用制約（利用許諾情報）と結果のコンテンツが動的に生成されて利用者に配布される（図1）。

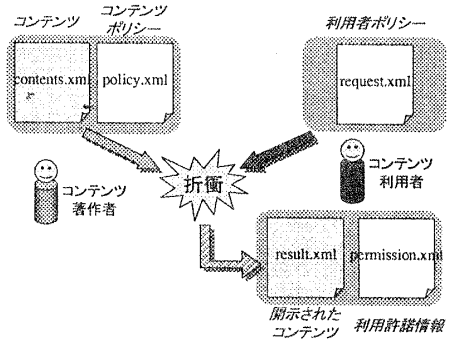

図1 利用制約に基づくコンテンツ流通管理

3.2. 利用許諾情報付きコンテンツの流通

本モデルでは、コンテンツ及びコンテンツポリシーの集合の中から、利用者によって提示された利用者ポリシーに基づいて検索が行われ、著作者、利用者双方の要求を満たすコンテンツと、そのコンテンツに対する利用許諾情報が動的に生成される。利用許諾情報はコンテンツとは独立に存在し、利用者によるコンテンツの利用は、この利用許諾情報に基づいて行われる。また、利用許諾情報は譲渡履歴を管理しているので、利用許諾として再配布が可能であった場合、利用者は入手したコンテンツを再配布することができる。再配布されるコンテンツには、元のコンテンツに対して取得した利用許諾の範囲内でコンテンツポリシーを付けることができるため、コンテンツの正当な二次利用が可能である。

4. 個人情報流通管理システムのXMLによる実現

本節では、前節のモデルに個人情報を適用した情報流通管理システムiPurseについて述べる。

4.1. iPurse利用制約記述言語

コンテンツ、コンテンツポリシー、利用者ポリシー及び利用許諾情報の記述にはXMLに基づいて定義したiPurse利用制約記述言語を用いている。それぞれの記述例を図2～図5に示す。

```
<iPurse version="0.7" mode="contents">
<fn>山田太郎</fn>
<given>太郎</given>
<family>山田</family>
<tel-home>045-123-4567</tel-home>
<tel-work>0468-12-3456</tel-work>
```

```
<email-work>xxx@xxxxx</email-work>
<email-work>yyy@yyyyy</email-work>
<X-hobby>海外旅行</X-hobby>
</iPurse>
```

図2 コンテンツの記述例

個人情報の各項目のうち、fn タグは著作者の表示名を表す。この他にも住所や生年月日などの項目を記述できる。さらに、"X-"で始まる項目を拡張タグとして自由に追加可能で、個人情報を柔軟に記述することができる。また、email-work タグのように同じ項目を複数個、記述することもできる。

```
<iPurse version="0.7" mode="policy">
<policy     target="iPurse://contents.xml#root().child(1,email-work)"
            condition="email-work=*@xxx.co.jp"
            purpose="non-commercial"
            communication="interactive"
            range="personal"
            anonymous="no"/>
<policy     target="iPurse://contents.xml#root().child(2,email-work)"
            condition="email-work!=*@xxx.co.jp"
            purpose="private"
            communication="support"
            range="organization"
            anonymous="no"/>
</iPurse>
```

図3 コンテンツポリシーの記述例

各 policy タグに含まれる属性 target の値はコンテンツポリシーを適用するコンテンツの識別子を表す。属性 condition の値は利用者条件を表す。属性 purpose の値は営利に関する利用目的を表す。属性 communication の値はコミュニケーションに関する利用条件を表す。属性 range の値はコンテンツの配布範囲が非公開／利用者個人だけ／利用者が所属する組織／無制限を表す。属性 anonymous の値は個人の身元の特定を許すか否かを表す。

```
<iPurse version="0.7" mode="request">
<request target=" iPurse://contents.xml#root().child(1,email-work)"
            purpose="private"
            communication="interactive"
            range="personal"
            anonymous="no"/>
</iPurse>
```

図4 利用者ポリシーの記述例

request タグに含まれる属性は、図3の policy タグに含まれる属性と同様の意味を表す。

```
<iPurse version="0.7" mode="permission">
<permission owner="山田太郎"
            user="田中花子"
            target=" iPurse://result.xml#root().child(1,email-work)"
            condition=" email-work=*@xxx.co.jp"
            purpose=" private"
            communication=" interactive"
            range=" personal"
            anonymous="no"/>
</iPurse>
```

図5 利用許諾情報の記述例

図3のコンテンツポリシーと図4の利用者ポリシーとの折衝の結果、図5の利用許諾情報が生成される。各 permission タグに含まれる属性 owner の値は著作者情報を表し、属性 user の値は利用者情報を表す。属性 target の値は、コンテンツポリシーと利用者ポリシーの折衝の結果、動的に生成されるコンテンツの識別子を表す。その他の属性の値は、コンテンツポリシーと利用者ポリシーの折衝に基づいて生成された利用許諾の内容を表す。

4.2. 情報流通管理システム：iPurse

個人情報の著作者は、個人情報とそれに対するコンテンツポリシーを作成し、それらを組にして iPurse 管理サーバに登録する。個人情報を要求する利用者は、利用者ポリシーを作成し、iPurse 管理サーバに問合せを行う。iPurse 管理サーバは、登録されているコンテンツポリシーと受け取った利用者ポリシーに基づいて検索を行い、開示可能な個人情報の抽出と利用許諾情報の生成を動的に行い、それらの組を利用者に送信する（図6）。

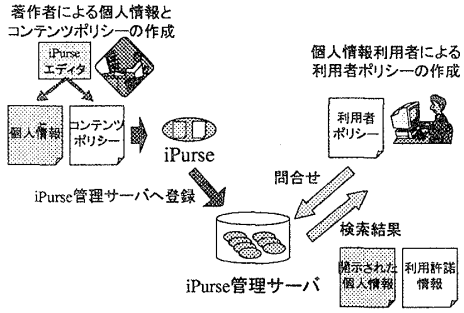

図6 個人情報流通管理システム

iPurse では、利用者に開示後の個人情報も利用許諾情報と組にして管理しているため、個人情報の利用は利用許諾の範囲内に制限することができる。また、利用許諾として再配布が可能な場合、再配布する個人情報に新たに付けることができるコンテンツポリシーは、取得した利用許諾の範囲内に制限されるので、元の著作者の意図を反映した正当な二次利用が可能である。

さらに iPurse では、コンテンツポリシーの利用者条件や利用目的などに応じた流通制御が可能である。従って、自分と同じ会社の人には xxx@xxxxx というメールアドレスを開示し、その他の人には yyy@yyyyy というメールアドレスを開示するというような、相手に応じて異なる個人情報を選択開示することが可能である。

最後に、現在開発中の iPurse の実行画面を図7に示す。

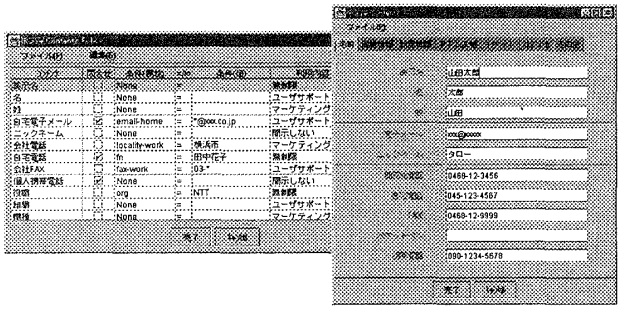

図7 iPurse の個人情報及びコンテンツポリシー表示画面

5. おわりに

本稿では、従来技術の問題解決を図る個人情報保護と情報流通促進を両立させるためのフレームワークを提案し、現在試作を行っている情報流通管理システム iPurse について述べた。

今後は、本フレームワークを個人情報流通基盤として発展させ、個人適応型検索などの one-to-one サービスへの利用展開を図っていきたいと考えている。

参考文献

[1] The European Union, "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 指令（EU 指令）," http://www.privacy.org/pi/intl_orgs/ec/eudp.html, 1995年10月

[2] W3C, "Open Profiling Standard(OPS)," http://www.w3c.org/Submission/1997/6/, 1997

[3] W3C, "Platform for Privacy Preferences(P3P)," http://www.w3c.org/P3P/, 1998

[4] 寺西, 長谷川, 梅本, 佐藤, "マルチメディアコンテンツ流通における利用制約管理機構," DICOMO'99, 1999

[5] 梅本, 寺西, 長谷川, 佐藤, "流通管理機構を持つ複合コンテンツの管理方式," DBWS'99, 1999