

インターネット環境における個人情報保護に関する研究

魏 然^{*1}・Justin ZHAN^{*2}

IMPROVED CUSTOMERS' PRIVACY PREFERENCE POLICY

Ran WEI, Justin ZHAN



Web サイトの個人情報保護方針を示す P3P の XML コード

```
...
<DATA-GROUP>
  <DATA ref= "#business.name" >Big Foot </DATA>
  <DATA ref= "#business.contact-info.postal.country">
    Japan </DATA>
...
</DATA-GROUP>
<EXTENSION optional="yes">
  <ENTITYID><小売業/></ENTITYID>
...
```

利用者の要求を示す APPEL の XML コード

```
<appel:RULE behavior="limited" description="警告 :
当サイトが取引上に必要のない情報を求めている">
  <p3p:POLICY appel: connective="and"> ...
    <p3p:EXTENSION optional="yes">
      <p3p:ENTITYID>
        <p3p:小売業/>
      </p3p:ENTITYID>
    </p3p:EXTENSION>
  ...
</p3p: POLICY>
<p3p: CATEGORIES> <p3p: health/>
</p3p: CATEGORIES> ...
```

検索結果から Web サイトの個人情報保護方針と利用者の要求との相違がわかる

Web サイトと利用者との対話の実現

研究の目的

インターネットにおける主に電子商取引時に個人情報の保護技術として、WWW 技術標準化団体である W3C (World Wide Web Consortium) が 2002 年に P3P (The Platform for Privacy Preferences 1.0) という規格を策定した。しかし、P3P は現実の個人情報保護の状況に対応しきれないところが多く、欧米でのますますな普及率に対して、日本の Web サイトはそれをほとんど採用していない。

W3C から P3P の改善の呼びかけを受けて、P3P に存在する問題点を指摘し具体的な対策案を提出するのは本研究の目的である。

技術の説明

P3P に存在する、国内の「個人情報保護法」の主要項目を適切に表現できない問題に対して、P3P 規格の構文にある、「個人情報保護法」と合性の良い構成要素や属性をピックアップまたは追加し、Web サイトの個人情報方針が「個人情報保護法」にどの程度まで順守しているかを確認できるプログラムを作成した。また、個人情報提示内容に関する利用者と Web サイトとの交渉不能については、交渉のアルゴリズムを考案しプログラムで提示した。さらに、Web サイトが約束した個人情報保護方針を将来にわたって否認できなくなるための暗号や署名方法などについて、電子認証と OpenID の技術を利用した解決方法を提案した。

主な結論

本研究では、個人情報保護のために W3C が開発した P3P の規格に存在する国内の「個人情報保護法」に十分に対応せず、利用者と Web サイトと交渉できず、Web サイトが約束した内容を認めないのを阻止できずという大きな問題点に対して具体的な解決案を提出した。これによって、インターネット上における個人情報保護の状況が近い将来に改善されることを期待している。

* 1 本店 情報システムサービスカンパニー

* 2 Carnegie Mellon CyLab Japan

インターネット環境における個人情報保護に関する研究

魏 然^{*1}Justin Zhan^{*2}

要 旨

インターネットにおける主に電子商取引時の個人情報の保護技術として、WWW技術標準化団体であるW3C（World Wide Web Consortium）が2002年にP3P（The Platform for Privacy Preferences 1.0）という規格を策定した。以来、欧米では数多くの大企業や団体が各自のWebサイトにこの規格を採用してきたが、日本ではP3Pの普及率はまだ低い。

その原因の一つは、P3Pが日本の「個人情報保護法」に十分に対応していないことに加えて、Webサイトの運営者がP3P導入の必要性を認識していないためと考えられる。本研究では、日本の「個人情報保護法」で定められた遵守すべき内容について、P3P規格の構文法、要素や属性などに従ったプログラムを提案した。また、Webサイトの利用者が自分の個人情報についてその運営者と交渉できる具体的な方法を提案した。最後に、Webサイトが約束した個人情報保護方針を将来にわたって否認できなくなるための暗号や署名方法などについても提案した。

キーワード P3P/APPEL/個人情報保護法/SEO/「交渉」/否認防止/OpenID

目 次

- | | |
|-----------------|----------------------|
| 1. はじめ | 2.1. 「個人情報保護法」への対応 |
| 1.1. P3P開発の経緯 | 2.2. 個人情報価値によるSEOの提案 |
| 1.2. P3Pの仕組み | 2.3. 交渉の仕組み |
| 1.3. P3P普及上の問題点 | 3. 否認防止の実現 |
| 2. P3Pによる改善案 | 4. まとめ |

IMPROVED CUSTOMERS' PRIVACY PREFERENCE POLICY

Ran WEI

Justin ZHAN

Synopsis:

Companies tend to collect more and more data about their customers. This data is seen as useful for the company, however, often customers do not wish to share. Methods such as P3P for verifying a company's privacy policy are available but these do not provide much choice to the customer; they provide an all-or-nothing selection.

In this paper, we explore a privacy preference policy approach which attempts to give customers more choices to make decisions by themselves on disclosing private information, and also prod online companies to be more careful on their collection of customers' private information.

* 1 本店 情報システムサービスカンパニー

* 2 Carnegie Mellon CyLab Japan

1. はじめ

1.1 P3P 開発の経緯

2008 年の統計資料によれば、世界におけるインターネットの利用者数は既に 15 億人以上に達していて、その数は毎日のように増えつつある。インターネットが有するこれまでに類のない安価な情報受発信能力を、誰もが利用できるようになったことで、人々の生活ぶりが大きく変わってきている。このようなインターネットの特色を生かして、近年企業間（BtoB）や企業と一般消費者の間（BtoC）などの電子商取引は飛躍的な成長を遂げ、今の情報化時代に脚光を浴びている。

しかしながら、インターネットがもたらしてきたのはいいことばかりではなく、所々に影も落としている。情報の氾濫や信憑性の欠如が人々を困らせたうえ、相次ぐ個人情報の漏えいが、様々な企業や団体で起こっていて、人々の健全な生活を脅かしている。

電子商取引における個人情報保護に対していち早く措置を施したのは EU である。EU は 1998 年に個人情報の保護を目的とする法律を有しない国との電子商取引を行わないと明言した。これは日米が個人情報保護の法整備を行うきっかけになったとも言われている。

日本政府は 2003 年に「個人情報保護法」を公布し、国民を通じての個人情報保護に関する基本理念、国、地方公共団体や民間事業者の責務や取るべき施策などを規定した。特に民間事業者に対して①個人情報利用目的を公表し、本人同意なしでの使用と第三者への提供は禁止する、②本人の求めに応じて保有する個人情報の開示・訂正・利用停止を行わなければならない、③個人情報の安全管理と適切な苦情処理に対応しなければならない¹⁾との 3 つの基本項目を定めている。

個人情報の収集は Web サイトの利用者側には不安を抱かせる要因となっている一方で、企業などの Web サイトの運営者にとってはマーケティングや CRM¹⁾に欠かせないものである。多くの運営者は利用者登録時のアンケート調査という公開方法とクッキーを利用した隠れた方法などで個人情報収集に努めているが、情報漏えいによるイメージダウンや損害賠償のリスクについての認識は足りない。また、これまでは利用者の個人情報の取り扱いは、すべて運営者によって決められており、利用者に交渉の余地はなかった。Web サイトの個人情報保護方針を読もうとしても、非常に長い上に難しい法律用語を用いて記述されており、実際には殆ど読まれていないのが実情である。これらの問題を解決するため、P3P (The Platform for Privacy Preferences) が開発された^{2,3)}。

2.2 P3P の仕組み

個人情報を保護しながら電子商取引を円滑に行なうこ

とを目的として、利用者が自分の情報をどの程度 Web サイトに提供するかをコントロールできるようにするための技術として、WWW 技術標準化団体である W3C が 2002 年に P3P という規格を策定した。

図 1 は P3P の仕組みを示している。従来は日本語で表記される「個人情報保護方針」の内容を、プログラムの読める形（P3P 準拠の XML²⁾）にしておく、クライアント側が P3P 準拠のブラウザを通して当該 Web サイトを開いたときに、Web サイトの個人情報保護方針が自分の個人情報保護方針と抵触するか否かを自動的に判断できる。

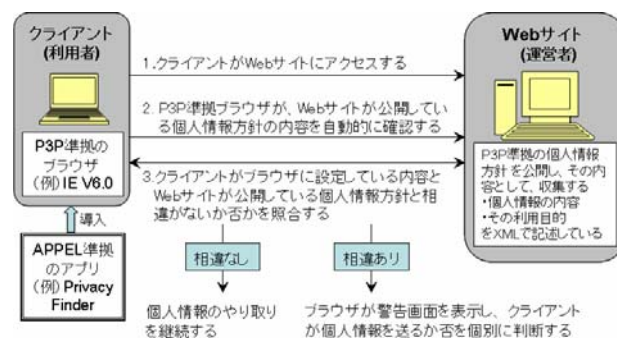


図-1 P3Pの仕組み⁴⁾

Web サイト側の P3P 準拠の個人情報保護方針の XML ファイル（P3P 方針）を作成するツールは海外ではいくつか提供されているが、日本語対応のツールはニューメディア開発協会⁵⁾ のみから無償でダウンロードできる。運営者がこの XML ファイルを Web サイトのトップ・ページに追加すれば、P3P 準拠の個人情報保護方針を導入したこととなる。

クライアント側については、IE6.0 以降は P3P に対応したブラウザであるが、実際にはクッキーの制御状況や個人情報保護方針を表示する程度の機能しかない。それを補うため、W3C は利用者個人情報方針作成用の、P3P の規格を理解し比較することができる APPEL (A P3P Preference Exchange Language) という規格も策定した⁶⁾。図 1 に示すように、利用者は APPEL 準拠のアプリケーションを使うことで、ブラウザの種類によらず、P3P の定義内においては、Web サイトとより広範囲な対話ができる。現在日本語対応の APPEL 用アプリケーションは、図-2 に示すような Carnegie Mellon CyLab Japan が AT&T の開発した Privacy Finder⁷⁾ を基に作った日本語対応の改定版ではなく、P3P を導入した国内のサイトも非常に少ないという事実⁸⁾を考えると、日本では Privacy Finder の利用価値はまだ低いと言わざるを得ない。なお、このツールは検索エンジンである Google と Yahoo の API³⁾ を利用しているため、それらによる検索結果のリストの上に、Web サイトが表明した個人情報保護方針が利用者の方針とどこまで一致

¹⁾ CRM: Customer Relationship Management

²⁾ XML: Extensible Markup Language

³⁾ API: Application Program Interface

するのかがわかるメリットを有する。図-2 の枠内の文字列はP3P (Webサイト) とAPPEL (利用者側) との方針相違を示している。



図-2 日本語版の Privacy Finder

1.3 P3P 普及上の問題点

P3P は現在 W3C で開発中の段階にあり、いくつか問題が残されていて、それらの一部は下記の通りである。これらは日本における P3P の注目度が高まらない原因であると考えられる。

- ① 国内において個人情報保護への対応度の判断基準は「個人情報保護法」である。しかし、P3Pがもともと OECD の 8 原則⁹⁾を念頭において作られており、特定の国の個人情報保護法には完全に対応するものではない。日本の「個人情報保護法」の要求事項を満足するためにはひと工夫が必要である。
- ② 情報提供の要求は運営者から利用者により一方的になされる。しかも要求された利用者の個人情報項目について、本当にビジネス活動に必要な情報なのかを、APPEL 上では自動的に判断できないうえ、利用者自身が判断できない場合もある。
そのうえ、すべての情報を一概に扱われている。情報の敏感度（特に精神的や経済的の角度から）と本人特定容易度（本人であることの判断難易度）については区別されていない。利用者があらゆる情報を提供してしまう。
- ③ 利用者と運営者両側の個人情報保護方針が一致しない場合、利用者は運営者の方針を無条件に受け入れるか、或いは情報提示を拒否し商取引などを中止せざるを得なくなる。交渉の機能はない。
- ④ 利用者と運営者間で個人情報保護の方針について合意が結ばれたにもかかわらず、運営者が大事に扱っていない場合がある。利用者の個人情報が知らないうちに、知らないところへ流れてしまうことを阻止する機能はない。

本研究では上記の①～③について、P3P の構文法に基づいて、これらの問題の解決策を検討し具体策を提案する。さらに④の問題点に対して XML のデジタル署名と

OpenID により解決する方法の提案を行う。

これらの P3P の問題点を解決すれば、インターネットにおける電子商取引の環境が一層安全になり、Web サイトの運営者と利用者ともにメリットを提供できる。

2. P3P による改善案

2.1 「個人情報保護法」への対応

1.1 述べたように、日本の「個人情報保護法」には3つの基本項目がある。それらの内容を要約すると、利用目的、第三者共有、情報の収集、係争解決、事前の対応、事後の対応というようなキーワードの組み合わせになる。

P3Pの規格ではXMLで記述される構成要素とそれらの用途を示す属性などが定義されている。これらの要素や属性の意味を一つずつ調べながら、個人情報保護法の内容を正しく表せるのかを検討した結果、下記の要素を選択した。なお、P3Pの要素とその属性の意味については、W3Cの公式Webサイトを参照されたい³⁾。

- <ACCESS> 個人識別情報へのアクセス
- <PURPOSE> 取得する個人情報の使用目的
- <RECIPIENT> 第三者を含む情報の提供先
- <DISPUTES> 係争解決と苦情処理

これらの要素とそれらに属する多くの属性を組み合わせることによって、様々な表現ができるが、中には個人情報保護法対応の面からは適する要素・属性と適さないものがある。検討した結果、その適否は下記のコード欄に示すように○×で分類できる。

```
<STATEMENT>
<ACCESS>
  ○ <all/> すべての個人識別情報へのアクセス
  ○ <nonident/> 個人識別可能な情報を利用していない
  × <contact-and-other/> <ident-contact/> <other-ident/>
    利用者個人情報に関連する情報へのアクセス
</ACCESS>
<PURPOSE>
  ○ <contact/> <current/> <individual-analysis/>
  ○ <individual-decision/> <historical/> <telemarketing/>
    必ず opt-out という選択肢をつけること, always と
    opt-in の選択は不可
</PURPOSE>
<RECIPIENT>
  ○ <ours/> <delivery/> <same/> <other-recipient/>
  ○ <unrelated/> <public/>
    必ず opt-out という選択肢をつけること, always と
    opt-in の選択は不可
</RECIPIENT>
<DISPUTES>
  ○ <service/> <independent/> <law/>
  × <court/>
    方針を参照する場合, 必ず resolution_type="law" を
    つけること
</DISPUTES>
</STATEMENT>
```

多くの専門分野にわたって使われている用語である always, opt-in や opt-out という選択肢も P3P でよく使わ

れている。always は「いつも属性の要求の通りにする」、opt-in は「利用者が意思表示をしないと運営者が個人データを使わない」、opt-out は「利用者に個人データの使用を拒否する権利を与えるが、もし拒否していない場合には運営者はそのデータを利用することができる」となる。

また、P3P には情報の保管期間を必ず記入すると規定してあるが、個人情報保護法にはこのような要求はないため、期限がないこと記す以下の XML

```
<RETENTION><indefinitely/></RETENTION>
```

を追加すべきである。

それから、1.3 章で述べたように、P3P には国内の個人情報保護法を守っていると表現できる要素は用意されていない。本研究では P3P の拡張機能の<EXTENSION>要素に<STANDARDS>要素を追加して、<ENTITY>要素の一部として使用してみた。

```
<ENTITY>
...
<EXTENSION optional="yes">
  <STANDARDS>standardvalues</STANDARDS>
</EXTENSION >
</ENTITY>
Where standardvalues = <JP-PIPA/>

<NOTICE> string </NOTICE>
```

以上のような個人情報保護法を表現する構文と制約をニューメディア開発協会が開発したような P3P 作成ツールに導入すれば、運営者が自分の Web サイトにおける個人情報保護法への対応方針を比較的容易に表現できる。

一方、利用者には、アクセスする Web サイトの個人情報保護法への対応状況は自分が望んでいるようになってい確認できるように、上記の P3P に対応する APPEL を Privacy Finder に組み込む必要がある。下記の APPEL はいくつかの例を示している。

```
<appel:RULE behavior="limited" description="個人情報保護法に違反している：当 Web サイトは私の個人情報の閲覧と修正を認めていない">
  <p3p:POLICY appel: connective="and">
    <p3p:DISPUTES-GROUP>
      <p3p:DISPUTES resolution-type="law">
        service=http://www5.cao.go.jp/seikatsu/kojin/index.html>
      </p3p:DISPUTES>
    </p3p:DISPUTES-GROUP >
  <p3p:ACCESS appel: connective="or">
    <p3p: nonident /> <p3p: all />
  </p3p:ACCESS >
</p3p:POLICY>
</appel:RULE>
```

```
<appel:RULE behavior="limited" description="個人情報保護法に違反している：当 Web サイトは第三者への情報提供について、私の意思変更を認めていない">
  <p3p:POLICY appel: connective="and">
    <p3p:ENTITY>
```

```
<p3p:EXTENSION optional="yes">
  <p3p:STANDARDS>
    <p3p:JP-PIPA/>
  </p3p:STANDARDS>
</p3p:EXTENSION >
</p3p:ENTITY>
<p3p:STATEMENT>
  <p3p: RECIPIENT appel: connective="or">
    <p3p: same required="always"/>
    <p3p: other-recipient required="always" />
    <p3p: unrelated required="always" />
    <p3p: public required="always" />
  </p3p: RECIPIENT >
</p3p:STATEMENT>
</p3p:POLICY>
</appel:RULE>
```

```
<appel:RULE behavior="limited" description="個人情報保護法に違反している：当 Web サイトはカスタマーサービスセンター或いは係争解決の機関を指定されていない">
  <p3p:POLICY appel: connective="and">
    <p3p:DISPUTES-GROUP>
      <p3p:DISPUTES resolution-type="law" service=
        http://www5.cao.go.jp/seikatsu/kojin/index.html/>
    </p3p:DISPUTES-GROUP >
  <p3p: DISPUTES-GROUP appel: connective="or">
    <p3p: DISPUTES resolution-type="service" />
    <p3p: DISPUTES resolution-type="independent" />
  </p3p:DISPUTES-GROUP >
</p3p:POLICY>
</appel:RULE>
```

これらの XML で述べたような、利用者の個人情報の閲覧・修正を認めず、使用する目的と第三者への提供に関する利用者の意思変更を認めず、またカスタマーサービスセンターなどの情報を教えてくれないなどの方針を持つ Web サイトを Privacy Finder で開いたら、表-1 の最下行に示す警告文が図-2 示すように現われるようにする。

表-1 Privacy Finder における利用者側方法の設定
(利用者と運営者の方針が合わない時の警告)

	個人のプライバシー設定レベル		
Webサイトのプライバシー方針に対する警告	低	中	高
私の健康と医療に関する情報を利用しているWebサイトであれば警告して下さい	-	-	-
私の個人情報の分析や、それを利用した表示サイト内容/広告の選定等の目的	○	○	○
・第三者と共有する(第三者から私のためのサービスを求める目的としても)	○	○	○
私の経済状況や買い物に関する情報を利用しているWebサイトであれば警告して下さい	-	-	-
私の個人情報の分析や、それを利用した表示サイト内容/広告の選定等の目的			○
・第三者と共有する(第三者から私のためのサービスを求める目的としても)		○	○
私に連絡し、他のサービスや商品に興味を持たせるWebサイトであれば警告して下さい	-	-	-
・電話を通して			○
・他の方法(郵便、Eメールなど)			○
・しかも自分の情報を取り下げようと言った要求に応じてくれない	○	○	○
私を特定する情報を利用しているWebサイトであれば警告して下さい	-	-	-
私の趣味、習慣、或いはその他の性格に関わるもの			○
・第三者と共有する(第三者から私のためのサービスを求める目的としても)		○	○
私のどんな情報を利用しているのかを教えてくださいWebサイトであれば警告して下さい		○	○
私を特定しない情報を利用しているWebサイトであれば警告して下さい	-	-	-
私の趣味、習慣、或いはその他の性格に関わるもの			○
・第三者と共有する(第三者から私のためのサービスを求める目的としても)			○
「個人情報保護法」を遵守すると言いながら合致しない方針が存在するWebサイトであれば警告して下さい	○	○	○

たくさんの Web サイトが P3P を導入すればするほど、Privacy Finder の利用価値が高くなる。

⁴ 2009 年 9 月設立された消費者庁のWebサイトにある個人情報保護推進室のURLである。

2.2 個人情報価値によるSEO⁵の提案

1) P3P への必須情報の導入

個人情報保護法は、個人情報取得の目的や方法を示す必要があると決めているが、個人情報の量と質については言及していない。多くの運営者にして見れば、利用者の求めていることをより正しく迅速に分析することは、重要な事業活動の一環であり、データマイニング⁶するにも、一般的には情報がたくさんあればあるほど良い。しかしながら、必要以上の個人情報を収集すると、その漏れる危険性が将来にわたって存在し、却って運営者の負担が大きくなることについては十分に認識されていない。

一方、利用者にとっては聞かれた情報が本当に電子商取引上に欠かせない情報なのか戸惑う時が多々あり、特に APPEL をインストールした利用者（クライアント）にして見れば、もっと判断しづらくなる。例えば、靴屋が身長データを収集する必要は殆どないのは人間がすぐ判断できるが、プログラムに判断させるには判断基準を予め設定する必要がある。

そこで、国際連合が制定した工業国際標準産業分類の ISICコード¹⁰に従い、各分野における円滑な電子商取引を行うには欠かせない必須情報を予め定義し、P3Pの要素として導入することを提案する。そうなれば企業がP3P方針を作る際に、企業の特徴を示すコードを付けなければならなくなる。将来利用者が提供した情報の不足を理由に運営者がサービスの提供を拒んだ場合、この必須情報を基に消費者庁に申し立てることが可能になる。

2) 個人情報の価値の定義

個人情報はそれぞれの価値をつけられる。NPO日本ネットワークセキュリティ協会等^{11,12}は個人情報漏えいにおける想定損害賠償額の算出モデルを提案している。情報漏えいの被害者に与える影響を「経済的損失」と「精神的苦痛」という2種類の尺度で分類した影響の大きさを定量化するため、表-2 に示すように、縦軸に「経済的損失」の度合いを、横軸に「精神的苦痛」の度合いを持たせたグラフを作成した。表-2 にある①～⑤の数値は敏感度を仮に表わしたものである。

この敏感度のほか、個人を簡単に特定できる氏名、住所、顔写真など（本人特定容易度）も重要な情報である。情報は敏感度が低いにもかかわらず、価値が高い。個人情報を一つだけで特定できなくても、組み合わせることによって本人特定容易度が高くなることもある。メールアドレスとパスワードの組み合わせがその一例である。

本協会が考案した個人情報の価値の算式の中心部分は下式の通りである。また、この式は個人情報漏えいによる運営者の賠償金額の試算にも使われているようである。

⁵ SEO: search engine optimization

⁶ 種々の統計解析手法を用いて大量のデータを分析し、隠れた関係性や意味を見つけ出す。

個人情報の価値＝情報の敏感度×本人特定容易度

表-2 敏感度による個人情報の分類

経済的損失レベル	3	③ 口座番号/暗証番号、クレジットカード番号、カード有効期限、銀行のアカウント/パスワード	④ 遺言書	⑤ 前科前歴、犯罪歴、予審ブラックリスト
	2	② パスポート情報、購入記録、ISPアカウント/パスワード	③ 年収・年収区分、資産、建物、土地、残高、借金、所得、借入れ記録	
	1	① 氏名、住所、生年月日、性別、取引金融機関名、住民票コード、メールアドレス、健康保険証番号、年金証書番号、免許書番号、社員番号、会員番号、電話番号、ハンドル名、健康保険証情報、年金証書情報、介護保険証情報、会社名、学校名、役職、職業、身長、体重、血液型、身長特徴、写真(肖像)、音声、声紋、体力診断	② 健康診断、心理テスト、性格診断、妊娠歴、手術歴、看護記録、検査記録、身体障害者手帳、DNA、病歴、治療法、指紋、レセプト、スリーサイズ、人種、地方なまり、国籍、趣味、特技、嗜好、民族、日記、賞罰、職歴、学歴、成績、試験得点、メール内容、位置情報	③ 加盟政党、政治的見解、加盟労働組合、信条、思想、宗教、信仰、本籍、病状、カレテ、痴呆症、身体障害、精神的障害、保有感染症、性癖、性生活
		1	2	3
		精神的苦痛レベル		

3) P3P と SEO とのリンク

この必須情報と個人情報の価値の概念を P3P と APPEL に取り込めば、運営者と利用者両方にとって大きなメリットが生まれる。Privacy Finder に Web サイトの P3P が取ろうとしている個人情報の価値を低い順に並べる機能を与えれば、利用者にとっては運営者の個人情報の扱い方針がわかり、運営者にとっては、自分の Web サイトがより検索順番の上位になるように、余計な情報を取らなくなり、検索エンジン最適化の SEO 対策を真剣に行うようになる。P3P の普及も促進すると考えられる。

下記のXMLコードはWebサイト側（靴屋）のP3P記述に対して利用者側のAPPELが必須情報と敏感情報を判断する文例である。^{13,14}

靴屋の P3P 方針の一部

```
<ENTITY>
<DATA-GROUP>
  <DATA ref= "#business.name" >Big Foot </DATA>
  <DATA ref= "#business.contact-info.postal.country" >Japan </DATA>
  ...
</DATA-GROUP>
<EXTENSION optional="yes">
  <ENTITYID> <小売業 1 /></ENTITYID>
</EXTENSION>
</ENTITY>
```

利用者の APPEL 方針の一部

```
<appel:RULE behavior="limited" description="当 Web サイトが取引上に必要のない情報を求めている">
  <p3p:POLICY appel: connective="and">
    <p3p:ENTITY>
      <p3p:EXTENSION optional="yes">
        <p3p:ENTITYID>
          <p3p:小売業 1 />
        </p3p:ENTITYID>
      </p3p:EXTENSION>
    </p3p:ENTITY>
    <p3p:STATEMENT appel:connective="and">
```

```

<p3p: PURPOSE app:connective="or">
  <p3p:contact/>
  <p3p:telemarketing/>
  <p3p:other-purpose/>
</p3p: PURPOSE>
<p3p: DATA-GROUP>
  <p3p: DATA>
    <p3p: CATEGORIES>
      <p3p: health/>
    </p3p: CATEGORIES>
  </p3p: DATA>
  <p3p: DATA-GROUP>
  </p3p: DATA-GROUP>
</p3p: POLICY>
</appel: RULE>

```

靴屋から健康に関する情報を聞かれると必須情報ではないと判断し、APPEL が利用者に警告するようになる。

2.3 交渉の仕組み

これまでのPrivacy FinderによるP3PとAPPELとの交渉は一回のみのものであり、利用者側のAPPELはP3Pの方針を同意するかしないかという選択しか行えない。しかし、現実はいずれも複雑であり、利用者ができるだけ個人情報の提示を拒んでいるに対して、運営者は様々な目的で多くの情報を収集している。同意した上での情報共有はお互いの利益になり、個人情報保護法が望んでいることでもある。このような共有内容は対面式の会話による商取引では容易に行われるが、コンピュータ同士になると、ゲーム理論¹⁵⁾に基づいて複雑な計算を行うことが一般的である。しかし、P3Pで用いられるXMLのようなインタプリタ言語は複雑な計算には向いていない。ここでは問題を簡素化するために、P3PとAPPEL両者の方針にある重複の要素を抽出し、それらに必須情報を加えたものを共有方針とし、コンピュータに処理させる方法を提案する。下記のXMLは運営者側の情報収集目的と利用者側の情報保護要望が合致するかを自動で交渉可能とするXMLの例を示す。

靴屋側の P3P 方針の一部

```

<STATEMENT>
  <PURPOSE>
    <current/><admin/> <telemarketing/> <individual-
analysis/>
  </PURPOSE>
  <RECIPIENT>
    <ours /> <same /> <delivery />
  </RECIPIENT>
  <DATA-GROUP>
    <DATA ref=" #shoe.size" />
    <DATA ref=" #shoe.gender" />
  </DATA-GROUP>
</STATEMENT>

```

利用者側の APPEL の方針の一部

```

<appel: RULE>
  <p3p: POLICY>
    <p3p: STATEMENT>
      <p3p: PURPOSE>
        <p3p: admin/><p3p: develop/><p3p: current/>
      <p3p: /PURPOSE>
      <p3p: RECIPIENT>

```

```

<p3p: ours/> <p3p: same/>
</p3p: RECIPIENT>
<p3p: DATA-GROUP>
  <DATA ref=" #shoe.size" />
  <DATA ref=" #shoe.gender" />
</p3p: DATA-GROUP>
</p3p: STATEMENT>
</p3p: POLICY>
</appel: RULE>

```

この例は靴のサイズ及び使用者の性別の情報について、配送業者を含む第三者に公開しないように利用者が指示したことを示している。靴屋が靴を配送業者に渡す前に、中身が見られないように梱包しなければならないと読み取れる。

個人情報提示内容について、利用者と靴屋との交渉は下記のように進んでいく。

例えば、P3P の<PURPOSE>の属性を P 配列に、

$P = \{\text{current}, \text{admin}, \text{telemarketing}, \text{individual-analysis}\}$

APPEL の<PURPOSE>の属性を A 配列に入れる

$A = \{\text{admin}, \text{develop}, \text{current}\}$

P と A との共通な内容があれば、それらの交わりを抽出する。

$P \cap A = \{\text{admin}, \text{current}\}$

交わりを持たなければ、P3P と APPEL と共通点がなく、これ以上のコンピュータによる交渉はできず、どちら側かに妥協が必要となる。

交わりの属性に付属する選択肢項目については、P3P と APPEL の方針が異なるのであれば、次のようなあらかじめ決めた順位で選択肢を比べれば、P3P と APPEL が共に守るべき方針が絞られる。

- ① "always" > "opt-out" > "opt-in";
- ② "indefinitely" > "business-practices" > "legal-requirement" > "stated-purpose";
- ③ ...

さらに、得られた共有方針上にある異なった要素や属性の設定による論理上のミスを起こさないように、あらゆる可能性を検討し、制限を加えなければならない。

例えば、個人情報を収集しないと明言しながら、クッキーを収集するような矛盾を下式によって回避する。

$$\forall p \in \langle \text{COOKIE-INCLUDE} \rangle \neg \exists a \in \langle \text{ACCESS} \rangle, a.\text{Attributes} = \langle \text{COOKIE-INCLUDE} \rangle \wedge a.\langle \text{ACCESS} \rangle = \text{nonident}$$

以上のような交渉の仕組みによると、インターネット上では対話式に近い電子商取引を実現できるようになる。

3. 否認防止の実現

P3P は Web サイト側が提示した個人情報保護方針であるが、その方針の通りに運営者によって遵守されているかを保証するものではない。しかし、個人情報保護方針は法的な拘束力を持つ契約である。契約を破棄し（否認という）方針に違反した場合には、運営者の責任が問わ

れることになる。そのため、技術的に運営者が否認できないようにする必要がある。この問題を解決するため電子認証技術が有効と考えられる。

電子認証技術および関連する法の整備が PKI (Public Key Infrastructure) 公開鍵暗号方式を応用した「デジタル署名および電子証明書」を用いて構築されている。PKI によって電子商取引に欠かせない本人認証、機密性、非改ざん性、否認防止が実現できる。多くの企業間では既に機密情報の受送信に使用されている。

この技術を活用した否認防止の方法は図-3 に示すような流れとなる。Web サイトの運営者が利用者と合意した後、公開鍵、公開鍵の証明書、合意した P3P の XML 原文と秘密鍵で署名を作成した XML 文書を一式で利用者（クライアント）に送る。利用者が運営者の公開鍵で署名文書を復号し、P3P の XML 原文と一致するかを確認する。利用者がこれらのデータを保管すれば将来運営者が契約を否認することを防ぐことができる。この方法によると、Web サイトと認証機関には大きな負担にならない。

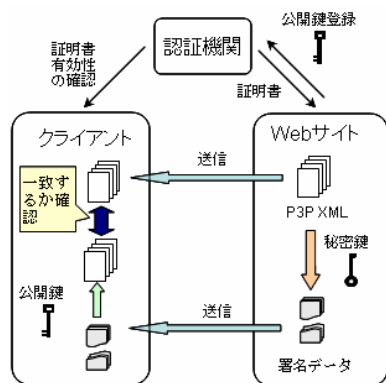


図-3 Web サイト側の署名の仕組み

XML の暗号化と署名などについては、「XML Encryption及びDecryption Transformの公開についてのW3C 勧告」^{16) 17)}に従う。次のXMLは前述の靴屋との合意内容の重要な部分のみに対して署名することを記述したコードの一部である。ここで、このXMLの中に暗号キーの生成やタイムスタンプの内容は省略した。

```
<DATA ref="user.home-info">
  <CONSENTREQUEST method="httpheader"
    headername = "consent">
    <DATAREQUIRED certificate="X.509"
      algorithmtype="RSA" minkeylength="128">
      われわれがここに述べた個人情報の扱いに関する方針を同意し遵守します
    </DATAREQUIRED>
  </CONSENTREQUEST>
</DATA>
...
<STATEMENT>
  <EncryptedData
    Type=http://www.w3.org/2001/04/xmlenc#Element,
    Xmins="http://www.w3.org/2001/04/xmlenc#"
  <CipherData>
    <CipherValue>Akd67emD...</CipherValue>
  </CipherData>
```

```
</EncryptedData>
</STATEMENT>
```

なお、P3Pファイルのサイズが大きい場合、ファイル全体に暗号をかけるより、いったんMD5⁷⁾でハッシュ値を作って、ハッシュ値を署名してから、利用者へ送るのは一般的な方法である¹⁸⁾。

しかし、Web サイトの公開鍵は誰でも入手できるため、署名文書そのまま利用者へ送信するのは安全ではない。SSL による暗号措置を掛けても、データは通信過程では保護されているが、複数の中継サーバを通行したり、サーバ間でデータ交換されたりすると、SSL だけではセキュアでなくなり、データの内容が覗かれる危険がある。

企業間のデータ交換を行う場合、当事者両方とも認証機関に公開鍵を登録し証明書を作って、転送ファイルの安全性を確保するため、相手の公開鍵でファイルを暗号化してから送ると覗かれる心配はない。交渉相手が一般利用者になると、認証機関に利用者を有料登録させるのは現実的ではない。

ここでは 2007 年に開発されたOpenIDという個人認証方法¹⁹⁾を今回の署名の仕組みに加えることを提案する。

OpenID とは、Web サイトの URL 形式で構成された利用者の身元確認をするための ID であり、誰でもインターネット上で自分の情報を作成・管理することができるようになっている。例えば OpenID 認証サーバである Yahoo! JAPAN に利用者登録すれば一つ URL をもらえる。この URL は OpenID であり、URL の所有者であることを証明する。利用者個人のブログも OpenID 認証サーバとして使える。この URL を使ってすべての OpenID 対応の Web サイトにパスワードを入力せずに安全に登録できる。現在世界では OpenID に対応する Web サイト（コンシューマとも称する）は既に何万箇所に達していて、これからはその数が大幅に増加するのは間違いない。

OpenID 認証の核心的なところは図-4 に示すように、認証サーバとコンシューマはステップ③の暗号鍵を共有することによってできた信頼関係にある。利用者がまるで登録した認証サーバにアクセスするように、すべてのコンシューマに安全に登録できる。

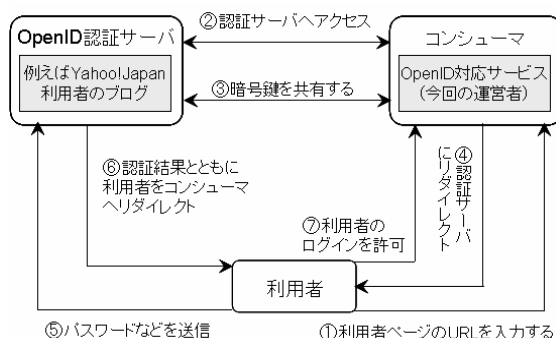


図-4 OpenIDによる認証の流れ²⁰⁾

⁷⁾ 原文から約 128 ビットの疑似乱数を生成する演算法

この技術を利用して、Keytool などのツールを使えば OpenID 認証サーバで（個人のブログでも）利用者専用の公開鍵証明書や対になった「公開鍵と秘密鍵」を容易に作れる。運営者の Web サイトが利用者の URL から公開鍵を取得し、自分の署名した XML 文書と XML 原文にその公開鍵をかければ、安全に利用者の手元に送信できる。これらの一連の操作を標準化し、ブラウザなどに組み込めば、利用者とコンシューマが意識しないうちに機密送信、非改ざん性や否認防止などの電子認証が実現できる。

また、利用者が自分の個人情報と APPEL 方針を OpenID 認証サーバに保管すれば、Web サイトにアクセスすると、P3P と APPEL が自動的に交渉することができる。方針が合意した後、合意内容のみが Web サイト側に送られて、これまでのような個人情報をいちいち入力する利用者の手間も省くこととなる。さらに、個人情報はすべて利用者自身で管理しているため、以前のような情報回収しようと思う時に Web サイトで作ったアカウントを削除する手間もなくなる。

このように OpenID の技術を利用すれば、否認防止のような電子認証が容易に実現するほか、利用者が自分の個人情報も管理しやすくなり、運営者と交渉する際の主導権を握ることとなる。

4. まとめ

ある大学が実施した個人情報の重視度に関する調査によると、マクドナルトのハンバーガー一つをただでもらう代わりに、自分の個人情報は惜しくなく、聞かれた内容を素直に答える人が過半を占め、多く人の個人情報管理に対する危機意識の低さが明らかになった。この意識の低さに起因して、様々な情報が漏れているのも現状である。その対策には、法律整備を強化しながら、P3P のような技術を活用して、個人情報漏えいによるトラブルを未然に最小限に食い止めなければならない。これも W3C が大学や研究機関に個人情報保護の技術開発に力を入れるように呼びかけている目的である。

本研究では P3P が日本でより広く受けられるように、国内の「個人情報保護法」を P3P の構文法を用いて表現する方法について提案した。また、個人情報の敏感度や必須情報を P3P で表現する方法について検討した。さらに、運営者と利用者が個人情報の提示内容について交渉できるように、P3P と APPEL との対話の仕組みを考案した。最後に、運営者に利用者と合意した個人情報方針を守らせて否認防止を実現するため、現存の XML デジタル署名技術に OpenID 機能を組み込む方法を提案した。

W3Cが推奨しているP3Pの規格はまだ試行錯誤の段階にあり²¹⁾、P3PとAPPELによる対話の仕組みは実際の個人情報保護の複雑な状況にはまだ対応しきれていない。本研究で提案した手法はP3Pの有用性の向上につながるものと考えられる。

謝辞：本研究は Carnegie Mellon CyLab Japan 在学中に Nicolas Christin 先生と指方美香先輩から「個人情報保護法」の P3P モデル化について多くの貴重な助言を頂いた。ここに関係各位に感謝の意を表します。

参考文献

- 1) 個人情報保護法の要点, http://www.pangkal.com/p_mark/low5.html.
- 2) The World Wide Web Consortium (W3C), "Platform for Privacy Preferences Project", <http://www.w3.org/P3P>.
- 3) Lorrie Faith Cranor, "Web Privacy with P3P", published by O'Reilly & Associates, Inc., September 2002.
- 4) 電子商取引の概要, <http://yamachan.shse.u-hyogo.ac.jp/NetSociety/chapter11.pdf>.
- 5) ニューメディア開発協会, P3P ポリシーウィザード, http://pics.enc.or.jp/privacy/tools/p3pwiz/p3p_ja.html.
- 6) W3C, P3P プリファレンス交換言語 (APPEL), <http://www.iajapan.org/trans2japanese/w3c/wd-p3p-prf20000420j.html>.
- 7) 日本語版 Privacy Finder, <http://jp.privacyfinder.org/>.
- 8) 財団法人ニューメディア開発協会, インターネット上のプライバシー保護技術 (PET) に関する調査, 平成 16 年 3 月.
- 9) OECD 理事会勧告 8 原則, http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/oecd8198009.html.
- 10) International Standard Industry Classification, <http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=17&Lg=1>.
- 11) NPO 日本ネットワークセキュリティ協会: 2008 年情報セキュリティインシデントに関する調査報告書, <http://www.jnsa.org/result/2008/surv/incident/index.htm>.
- 12) 井手大作, 田淵義郎: 図解「中小企業のための」間違いだらけの個人情報保護法対策, ナツメ社, 2007.
- 13) Ran Wei and Justin Zhan, A proposal towards customers' privacy preference policy, IEEE International Conference on Machine Learning and Cybernetics, August 19-22, 2007, Hong Kong.
- 14) Ran Wei and Justin Zhan, Improved Customers' Privacy Preference Policy, IEEE International Conference on Granular Computing, November 2-4, 2007, Silicon Valley, California.
- 15) 渡辺隆裕, "ゼミナール ゲーム理論入門", 日本経済新聞出版社, 2008 年 4 月 7 日.
- 16) Blake Dourmaee, "XML Security", published by McGraw-Hill, 2002.
- 17) XML Encryption と Decryption Transform の公開についての W3C 勧告, <http://www.w3.org/2002/12/xenc-release.html>.
- 18) 丸山宏, "XML と Web サービスのセキュリティー XML デジタル署名と暗号化", 共立出版, 2004/6.
- 19) OpenID Foundation website, <http://openid.net/>
- 20) OpenID が熱狂的に受け入れられる理由, <http://www.atmarkit.co.jp/news/analysis/200704/23/openid.html>
- 21) Karen Coyle, "P3P: Pretty Poor Privacy? A social analysis of the platform for privacy preferences", Available at: <http://www.kcoyle.net/p3p.html>.