プライバシー保護のための新たな技術的対策の調査研究

報告書

平成１８年３月

財団法人ニューメディア開発協会

この事業は、競輪の補助金を受けて実施したものです。

目　次

１．背景及び目的

個人情報保護法が全面施行された中、個人情報保護のためのシステムやツールは既に様々なものが提供されている。それらの多くは企業・組織で預かる顧客の個人情報の漏えいを防ぐための情報漏えい対策システムであるが、利用者個人のプライバシーに焦点を当て、利用者の立場からそれを積極的に保護しようとする技術はいまだ少ないのが現状である。こうしたプライバシー保護のための技術的対策の代表的事例としては、W3C（World Wide Web Consortium）が仕様策定を行った P3P（Platform for Privacy Preferences Project）があるが、我が国では十分に普及が進んでいない。

本調査研究事業は、ユビキタス社会において利用者個人が自らの個人情報の利用のされ方や開示の度合いをコントロールできる等、個人のプライバシーを保護するための技術的対策を調査し、現状の課題を整理するとともに、プライバシー保護のための新たな技術的対策を研究することを目的とする。

２．既存のプライバシー保護技術の課題整理

利用者個人のプライバシーを積極的に保護しようとする技術的対策の代表的事例として、W3C が仕様策定を行った P3P について、P3P 導入サイトに対するアンケート調査等を実施することにより、その実装面・実用面における課題の整理を行った。

２．１ P3P の普及状況の調査

（１）P3P の最近の動向

当協会の調査報告書「インターネット上のプライバシー保護技術（PET）に関する調査報告書」（2004 年 3 月）[1]以降の、P3P に関するトピックは以下の通りである。

2005 年 1 月には、P3P1.1 の Working Draft の改訂版が公表された。P3P1.1 では、P3P1.0 をベースに、欧州データ保護規定の語彙との整合、ユーザエージェント用のガイドラインの追加、XML アプリケーションにおいて P3P を利用できるような一般的な方法の規定がなされている。Web サービス、位置情報サービスについても取り込まれた。

さらに 2005 年 6 月には、再び P3P1.1 の Working Draft の改訂版が公表された。前回の Working Draft を主に語彙面でブラッシュアップしたものである。

また、P3P ポリシーのエディターとして、JRC Policy Workbench[2]（ベータ版）が 2005 年 12 月頃に公開されている。

（２）日本語トップ 100 ドメインにおける導入状況

わが国における P3P の普及状況を調べるために、日本語サイトのトップ 100 ドメインのトップページにおける P3P ポリシー[3]の掲載状況を、ブラウザ Internet Explorer6.0 の「プライバシーレポート」機能を用いて調査した。合わせて、インターネット上で利用者の閲覧履歴等を収集する技術として、サードパーティクッキー[4]の利用と Web ビーコン[5]の利用状況についても調査した。「ト

---

1 http://www.nmda.or.jp/enc/privacy/pr_rep_in_2004.pdf

2 http://sourceforge.net/projects/jrc-policy-api

3 企業や Web サイトのプライバシーポリシーを P3P 仕様書に基づき XML 形式で記述したマシンリーダブルなプライバシーポリシーを、P3P ポリシーと言う。

4 利用者が Web ページを閲覧する際、そのページが属するドメイン以外のサーバから送信されるクッキーのことをサードパーティクッキーと言う。Web 広告企業の送信するバナー広告に含まれるクッキーや、Web ビーコンに含まれるクッキーなどがこれに該当する。複数の Web サイトにサードパーティクッキーを埋め込んでおけば、利用者の閲覧履歴をサイトをまたいで追跡することが可能である。

ップ 100 ドメイン」は、Alexa Internet 社[6]のデータを基づいた。調査結果は以下の通りである。

○調査日：2005 年 12 月 9 日
○調査対象サイト：調査日時点での日本語サイトのトップ 100 ドメイン（Alexa Internet 社データによる）
○調査結果：

(a) トップページに P3P ポリシーを掲載しているドメイン[7]：
→100 ドメイン中 11 ドメイン（11%）

(b) トップページでサードパーティクッキーを利用しているドメイン[8]：
→100 ドメイン中 11 ドメイン（11%）

(c) そのうち、サードパーティクッキーに P3P ポリシーが掲載されているドメイン[9]：
→11 ドメイン中 8 ドメイン

(d) トップページで Web ビーコンを利用しているドメイン[10]：
→100 ドメイン中 37 ドメイン（37%）

(a) トップページに P3P ポリシーを掲載しているドメイン

まず、トップページに P3P ポリシーを掲載しているドメインは以下の 11 ドメインであった。

・Yahoo! Japan（www.yahoo.co.jp）

---

[5] Web ビーコンは、ある Web ページ（または電子メール）を閲覧する利用者をモニターするために設定された、Web ページ上（または電子メール上）のグラフィック（HTML IMG タグ）であり、通常は非常に小さいサイズの無色のグラフィックであるため、一般の利用者はその存在に気づかない。ビーコンの送信者はそれを通して、利用者の IP アドレスや、利用者の閲覧した Web ページの URL とその閲覧時刻の収集ができる。複数の Web サイトにこのビーコンを埋め込んでおけば、利用者がそれらのサイトのページにアクセスした際に、どの IP アドレスのマシンが、いつ、どの Web ページにアクセスしたかについての情報を追跡することが可能である。

[6] http://www.alexa.com/site/ds/top_sites?ts_mode=lang&lang=ja

[7] Internet Explorer6.0 の「プライバシーレポート」機能において、トップページを選択し、「概要」ボタンを押し、「プライバシーポリシー」が表示されるか否かで P3P ポリシーの有無を判断した。

[8] Internet Explorer6.0 の「プライバシーレポート」機能において、当該ドメイン以外から送信されたオブジェクトに Cookie が表示されるか否かでサードパーティクッキーの有無を判断した。

[9] Internet Explorer6.0 の「プライバシーレポート」機能を利用してサードパーティクッキー上の P3P ポリシーの有無を判断した。

[10] Web ページに埋め込まれた Web ビーコンを検知するソフトウェアである bugnosis（http://www.bugnosis.org/）によって Web ビーコンの有無を判断した。

・MSN Japan（www.msn.co.jp）
・Dell Computers Online（www.dell.com）
・Geocities.jp（www.geocities.jp）
・@nifty（www.nifty.com）
・BIGLOBE（www.biglobe.ne.jp）
・ハンゲーム（www.hangame.co.jp）
・Geocities.co.jp（www.geocities.co.jp）
・じゃらん（www.jalan.net）
・Vector（www.vector.co.jp）
・カービュー（www.carview.co.jp）

ここで「トップページ」とは、上記のようなドメインの URL をブラウザのアドレスバーに入力してアクセスしたときに表示されるページのことである。これらのドメインのうち、Geocities.jp と Geocities.co.jp については、当該 URL にアクセスすると Yahoo! Japan ドメインの http://geocities.yahoo.co.jp/（Yahoo!ジオシティーズ）にリダイレクトされるので、そのページの P3P ポリシーの有無で判断した。

なお、2004 年 6 月に、日本のトップ 50 ドメイン[11]について同様の調査を行った際には、トップページに P3P ポリシーを掲載しているところは 9 ドメイン（18%）であった。トップドメインのデータの出典が異なるため、単純には比較できないが、2004 年から 2005 年にかけて、P3P 導入サイトの割合は減少していることになる。

(b) トップページでサードパーティクッキーを利用しているドメイン

トップページでサードパーティクッキーを利用しているドメインは、以下の 11 ドメインであった。

・NIKKEI NET（www.nikkei.co.jp）
・ハンゲーム（www.hangame.co.jp）
・エキサイトブログ（www.exblog.jp）
・ビッダーズ（www.bidders.co.jp）
・ヤプログ（www.yaplog.jp）
・GyaO（www.gyao.jp）
・じゃらん（www.jalan.net）
・hi-ho（www.hi-ho.ne.jp）
・JUGEM（www.jugem.jp）

11 トップ 50 ドメインは Nielsen/NetRatings 社のデータに基づく。

・Jp-sex.com（www.jp-sex.com）
・フジテレビ（www.fujitv.co.jp）

2004 年 6 月に日本のトップ 50 ドメインについて行った調査の際には、トップページでサードパーティクッキーを利用しているところは 19 ドメイン（38%）であった。サードパーティクッキーの利用は、明らかに減少していることが分かる。

(c) サードパーティクッキーに P3P ポリシーが掲載されているドメイン

(b)のうち、サードパーティクッキーに P3P ポリシーが掲載されているドメインは、以下の 8 ドメインであった。

・NIKKEI NET（www.nikkei.co.jp）
・ハンゲーム（www.hangame.co.jp）
・ビッダーズ（www.bidders.co.jp）
・ヤプログ（www.yaplog.jp）
・GyaO（www.gyao.jp）
・じゃらん（www.jalan.net）
・hi-ho（www.hi-ho.ne.jp）
・JUGEM（www.jugem.jp）

Internet Explorer6.0 の P3P 対応クッキー管理機能においては、デフォルト設定では、サードパーティクッキー を伴うような Web オブジェクトに P3P ポリシーが付与されていない限り、当該クッキーの受取りが自動的に遮断され、さらにブラウザの下側に警告アイコンが表示される。すなわち、サードパーティクッキーの利用には一定の制約が設けられている。そのためか、サードパーティクッキーに P3P ポリシーが掲載されている場合が多かった。

(d) トップページで Web ビーコンを利用しているドメイン

トップページで Web ビーコンを利用しているドメインは、37 ドメインであった。そのうち疑わしいもの（bugnosis で Suspicious と表示されるもの）22 ドメインで、Web ビーコンを利用しているとみなせるもの（bugnosis で Web bug と表示されるもの）は 15 ドメインであった。

2004 年 6 月に日本のトップ 50 ドメインについて行った調査の際には、トップページで Web ビーコンを利用しているドメインは 14 ドメイン（28%、うち疑わしいものは 10 ドメイン、Web ビーコンを利用しているとみなせるものは 4 ドメイン）であった。

このように、Web ビーコンの利用は明らかに増加していることが分かる。インターネット利用者に普及した Internet Explorer6.0 で制限される恐れのあるサードパーティクッキーは避け、その代わりに、通常の利用者にとっては「不可視」で制限される恐れの少ない Web ビーコン[12]を使って、利用者の閲覧履歴（アクセスログ）を取得しようという傾向が拡大しているのであろうか。

２．２ P3P 導入サイトに対するアンケート調査

（１）アンケート調査の概要

２．１節の調査において、トップページに P3P を導入している 11 ドメインのうち、2 つの Geocities を除く 9 ドメインに対して、P3P に関するアンケート調査を実施した。

調査期間は 2006 年 2 月 13 日～3 月 1 日であり、9 ドメイン（9 社）に対してアンケートの依頼を行ったが、最終的に回答を得られたのは 2 社であった。

調査票は付録１「プライバシー保護技術 P3P に関する調査」調査票を参照のこと。

（２）調査結果の概要

○P3P の導入時期

- 2001 年（1 社）
- 2002 年（1 社）

○P3P を導入したきっかけ

- ブラウザの Internet Explorer に P3P 対応のクッキー管理機能が実装されたため（2 社）
- 米社サイトにおいて P3P を導入しているため（1 社）
- 顧客に対して、プライバシー保護活動を積極的に行っていることを示すため（1 社）

○P3P 導入の効果

- 大いに効果があった（1 社）
  →その内容：Cookie 返信率が向上した。
- 何ともいえない（1 社）

[12] ただし、Windows XP SP2 を適用した Outlook Express では、スパムメール対策として、HTML メール内の Web ビーコンの画像をデフォルトでブロックする機能が設けられている。

○P3P の導入は難しいかどうか

- それほど難しくないと思う（1 社）
- 難しくないと思う（1 社）

○P3P 導入にあたっての課題

- せっかくサイトに導入しても、具体的な利用シーンが少ない（2 社）
- P3P で定義されている項目（利用目的など）が日本の実情に適合していない（1 社）

○インターネット利用者が P3P を利用するにあたっての課題

- P3P の存在がインターネット利用者に十分周知されていない（2 社）
- P3P を導入しているサイトの閲覧時でも、P3P の出番が少ない（1 社）
- ブラウザでサイトの P3P プライバシーポリシーを確認したとき、日本語が分かりにくい（1 社）

○P3P 普及に向けて産業界がすべきこと

- ブラウザにより高度な P3P 対応機能を実装する（1 社）
- P3P を分かりやすく説明した資料を Web 上で公開する（1 社）
- 日本の実情にあった項目（ボキャブラリ）を作成する（1 社）
- その他（1 社）
  →その内容：保護法・プライバシーマークとの連動と、一般利用者へのさらなる啓蒙活動。

○P3P についての意見（自由回答）

- 企業にとって導入がメリットとして捉えにくいところが難点である。（1 社）

２．３ P3P の実装面・実用面における課題

アンケート結果も踏まえ、P3P の実装面・実用面での課題には、以下のようなものが考えられる。

（１）Web サイト運営者の立場からの課題

○P3P で定義されている項目（利用目的など）が日本の実情に適合していない

P3P は米欧の企業や団体が中心となって策定した技術仕様である。そのため、わが国の個人情報保護法やJISQ15001 において個人情報取扱事業者に求められている「プライバシーポリシー」への掲載項目を、P3P で全て表現できる訳ではない。また、P3P の仕様上は必須とされているが、日本の法律やガイドラインでは特に求められていない保有期間（RETENTION）のような項目もある。また、P3P の仕様で規定されている利用目的（PURPOSE）や受領者（RECIPIENT、提供先）の区分が、必ずしも日本の企業・団体がプライバシーポリシーや個人情報保護方針で掲げているものと一致していないという課題がある[13]。

○サイトに P3P を導入する方法を分かりやすく説明した資料がない

Web サイトに P3P を導入する方法については、マイクロソフト社の「Web サイトに P3P プライバシー ポリシーを導入する方法」[14]や、当協会のサイト上の「Web サイトを P3P 準拠にする方法」[15]（W3C 文書の翻訳）などが公開されている。しかし、文体が翻訳調であるためか、必ずしも分かりやすい説明資料とはなっていない。

○簡単に導入するためのジェネレーターなどのツールがない

P3P ポリシージェネレータ（P3P ポリシー作成ツール）としては、P3Pedit[16]や P3P Policy Editor[17]があるが、いずれも英語のツールである。日本語版のツールには当協会の P3P ポリシーウィザード[18]があるものの、P3P の必須掲載項目である収集個人情報（DATA）を記述するのが若干難しいという難点がある。

---

13 当協会の調査報告書「わが国の法制度に基づくプライバシー保護技術に関する調査報告書」（2005 年 3 月）（http://www.nmda.or.jp/enc/privacy/pr_rep_2005.pdf）を参照のこと。

14 http://www.microsoft.com/japan/msdn/workshop/security/privacy/overview/createprivacypolicy.asp

15 http://www.nmda.or.jp/enc/privacy/w3cp3pdetailsj.html

16 http://p3pedit.com/

17 http://www.alphaworks.ibm.com/tech/p3peditor

18 http://www.nmda.or.jp/enc/privacy/index.html

○サイトに導入しても、具体的な利用シーンが少ない

P3P は、Web サイトのプライバシーポリシー（P3P ポリシー）を、語彙が標準化されたマシンリーダブルな形式で、インターネット利用者に効率的に提示するための仕組みである。P3P が機能するためには、Web サイト側で P3P ポリシーを公開するのみならず、インターネット利用者のブラウザやクライアントソフトに P3P 対応の機能が備わっている必要がある。

現状、インターネット利用者側のツールとしては、マイクロソフト社のブラウザ Internet Explorer6.0 のクッキー管理機能の一部として P3P 対応がなされているが[19]、P3P ポリシーの有無やその内容によってクッキーを受け入れるか制限するかという機能に用いられているのみであり、当初の P3P の構想である、P3P ポリシーの内容によって自動的にサイトへの個人情報開示の是非を判断したり、P3P ポリシーが利用者側の個人情報利用許諾条件（プリファレンス）と合致しない場合にはネゴシエーションを行ったり、といったフル機能にまでは至っていない。

（2）インターネット利用者の立場からの課題

○P3P の存在がインターネット利用者に十分周知されていない

P3P のインターネット利用者への周知状況は十分ではない。インターネット利用者に対する調査ではないが、次世代電子商取引推進協議会（ECOM）が 2003 年 7 月に会員企業に対して行った調査では[20]、P3P について「知らない」と答えた企業は 47%であった。ちなみに同協議会がその前年度に行った調査でも「知らない」という企業は 47%であり、認知が進んでないことが分かる。

○P3P を導入しているサイトが少ない

日本のトップ 100 ドメインで P3P を導入している所は、2．1 節で調査したように、2005 年 12 月時点でわずか 11%である。米国のトップ 100 ドメインについては、2004 年 5 月の Ernst&Young 社の調査では 33%とのことである。このように P3P を導入しているサイトが少ないと、利用者側でも P3P 対応の機能を用いるメリットがあまりない。

○P3P を導入しているサイトの閲覧時でも、P3P の出番が少ない

それに加え、せっかく P3P を導入しているサイトを閲覧している場合でも、

---

19 その他、AT&T Privacy Bird（http://privacybird.com/）などが公開されている。

20 電子商取引推進協議会『EC で取り扱われる個人情報に関する調査報告書 2003』（2004 年 3 月）を参照した。

利用者側ツールとして Internet Explorer6.0 のクッキー管理機能のみが普及している現状では、「P3P ポリシーが無いサイトからはクッキーを受取らないようにする」といった使い方がなされているのみで、P3P の機能が十分に活かされていない。利用者側から上述のプリファレンスを提示できるなどの追加機能が望まれる。

○P3P ポリシーで宣言されている内容が遵守されているかは P3P 技術のみでは保証されない

P3P ポリシーは、利用者から収集した情報のサイト内での取扱いを技術的に制限する機能は持たない。したがって、P3P ポリシーでサイトが宣言したプライバシー取扱い内容が遵守されているかは、P3P ポリシーに表示されるプライバシーシール（プライバシーマーク、Truste など）等によって間接的に確認するしかない。

○ブラウザでサイトの P3P ポリシーを確認したとき、日本語が分かりにくい

また、Internet Explorer6.0 のプライバシーレポート機能において「サイトのプライバシーの概要を表示する」を選ぶと、当該サイトの P3P ポリシーを読むことができる。これは XML 言語で書かれた P3P ポリシーをブラウザが自動翻訳して（日本語で）表示する機能であるが、ここで表示される日本語が非常に分かりにくいため、せっかく P3P ポリシーを利用者が開いてみても内容を理解することが難しい。

○P3P を有効に活用するためのツールがない

上述したように、インターネット利用者側のツール（とりわけ日本語のツール）が非常に少ない。

これらの課題を順次解決していかない限り、P3P のさらなる普及は難しい状況にある。

３．国内外のプライバシー保護のための技術的対策の調査

３．１ Enhanced P3P Web Privacy Framework

メリーランド大学の Pranam Kolari らは、論文”Enhancing P3P Framework through Policies and Trust”（2004 年 9 月）[21]において、P3P を改良したフレームワークを提案している。

同論文では、P3P が普及していない理由を、(i) 利用者のプリファレンス（利用者が指定する個人情報利用許諾条件）を記述する言語[22]にあまり表現力がない、(ii) P3P ポリシーを掲載している Web サイトが少ない、の 2 点としている。そして、これらの問題を解決するために、P3P フレームワークを改良して、(i) 利用者がプリファレンスやプライバシー関連の諸条件を記述できるように RDF をベースとした Rei ポリシー言語を導入し、また、(ii) 「トラストモデル」の組み込みによって、サイトに P3P ポリシーの掲載がなくても効果が上がるようにするとしている。

図３－１は Enhanced P3P Web Privacy Framework の概要である。図中の各要素については、以下に説明する。

○クライアント

このプライバシーフレームワークを利用する利用者。

利用者は自分のプリファレンスを Rei ポリシー言語で作成して、インテリジェント・プライバシー・プロキシに登録する。

○Web サーバ

クライアントがアクセスする Web サイト。

---

21 http://ebiquity.umbc.edu/paper/html/id/192/Enhancing-P3P-Framework-through-Policies-and-Trust を参照のこと。

22 プリファレンスを記述する言語としては、W3C が仕様策定中の A P3P Preference Exchange Language 1.0 （APPEL1.0）（http://www.w3.org/TR/P3P-preferences/）がある。

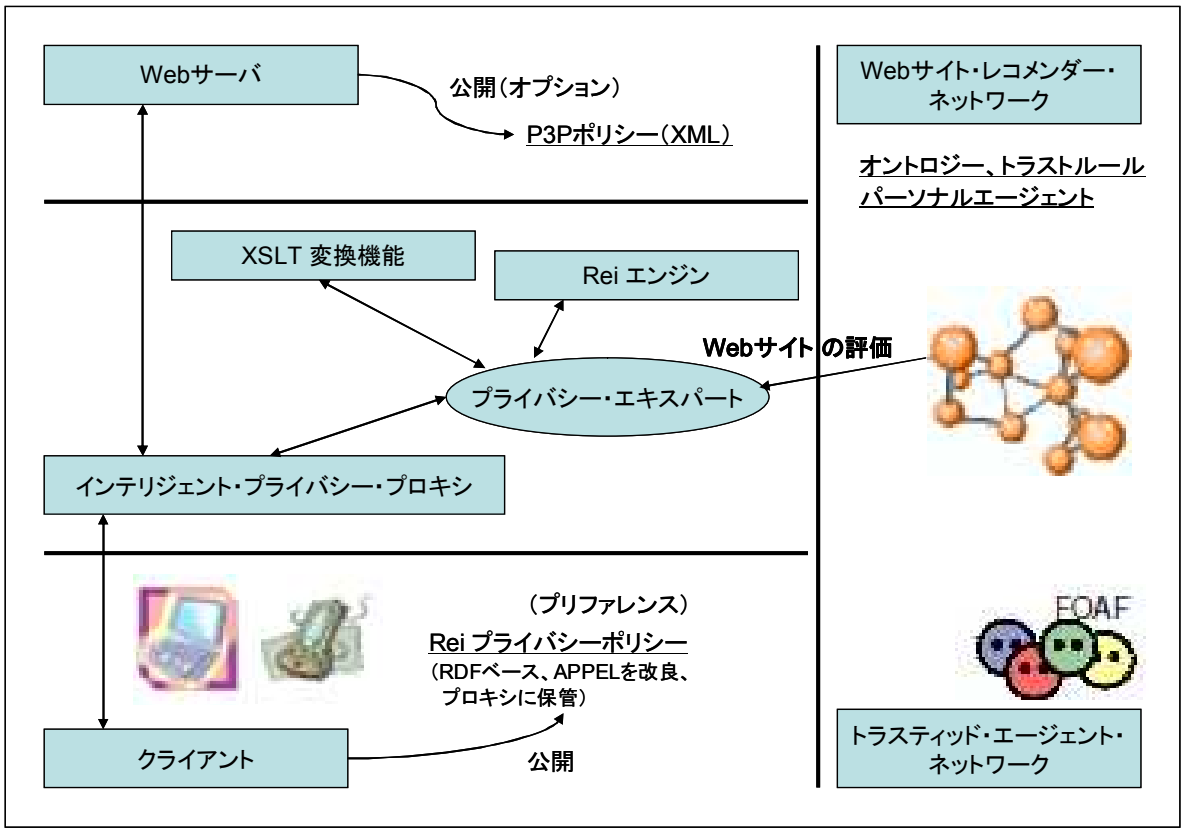

図３－１．Enhanced P3P Web Privacy Framework の概要

○Web サイト・レコメンダー・ネットワーク

信頼性の高いパーソナルエージェントのネットワークであり、オントロジーやトラストルールを用いて、Web サイトのプライバシー取扱いについてレコメンデーション（評価）を行う。

インテリジェント・プライバシー・プロキシに登録した利用者は全員、このパーソナルエージェントを持つ。パーソナルエージェントは Web サイトに対して評価を行い、また他のパーソナルエージェントが行った評価を収集する。エージェント間の信頼性については、FOAF（Friend of a Friend）[23]等を使用する。

○インテリジェント・プライバシー・プロキシ

利用者は自分のプリファレンスをインテリジェント・プライバシー・プロキシに登録する。プロキシでプリファレンスを持つことによって、利用者の HTTP リクエストの全てにプリファレンスが適用される。プロキシは利用者がアクセスしようとする Web サイトの P3P ポリシーを取得する。

[23] http://www.foaf-project.org/

○プライバシー・エキスパート機能

インテリジェント・プライバシー・プロキシからの照会に基づき、Web サイトの P3P ポリシーと利用者のプリファレンスを照合する。また、エージェントからの照会も受け付ける。Enhanced P3P Web Privacy Framework 全体を結び付ける役割もある。

プライバシー・エキスパート機能の主要な機能は、利用者のプライバシー情報の開示に関わる判断を行うことである。プライバシー・エキスパートは Web サイトの P3P ポリシーと利用者のプリファレンスを受取ると、XSLT 変換機能（P3P を XML から RDF に変換する）、Rei エンジンといった他のウェブサービスと協働して、そうした判断を行う。

３．２ VANET（自動車アドホック・ネットワーク）におけるプライバシー

従来の PC を中心としたインターネット環境のみならず、ユビキタスネットワーク環境においてもプライバシーは重要な問題になっている。

BMW 社の Florian Dötzer は 2005 年 5～6 月の Workshop on Privacy Enhancing Technologies において”Privacy Issues in Vehicular Ad Hoc Networks”というタイトルの発表を行っている[24]。

VANET（Vehicular Ad-hoc Network、自動車アドホック・ネットワーク）とは、情報処理機能を持った自動車をノードとみなし、自動車同士を無線でつないだネットワークであり、以下のような特徴を持っている。

- 分散型
- 自律的
- ノードのモビリティが高い
- ノード数が非常に多い
- 複雑な管理構造を持っている

VANET のセキュリティ要件としては、情報の信頼性、ネットワークの可用性、プライバシーの 3 点が挙げられている。特にプライバシーについては、自動車は極めてパーソナルなデバイスであり、どこを走っているのか／どこに駐車しているのかという位置情報と切り離せないが、そうした自動車同士がネットワークを形成して情報がやり取りされた場合、運転者や搭乗者のプライバシーの問題は非常に重要になる。しかも、VANET の構築を考える上ではプライバシーへの対応はシステムの設計時にあらかじめ組み込んでおかねばならず、後から付け加えることはできない。

---

[24] http://petworkshop.org/2005/workshop/program.html を参照のこと。

プライバシーに関する具体的な脅威としては以下のものが考えられている。

- 法執行機関（警察等）による自動監視
- ID の追跡
- 位置情報の記録
- 移動のプロファイリング　など

そのため、VANET におけるプライバシー要件として考えられるのが以下のものである。

- サービスにおいて「偽名」（実社会のものではない ID）を使うこと
- 利用者は複数の偽名を使用できること
- 偽名と実社会の ID とのマッピングは取れること
- 所有権や資格はデジタル署名によって保証されること

これらのプライバシー要件を満たすアプローチとして、以下のような保証機関型のアプローチが提唱されている。

① フェーズ１：自動車の設定フェーズ

実社会での ID と VANET サービス利用時の ID（偽名）を別々のものにする。

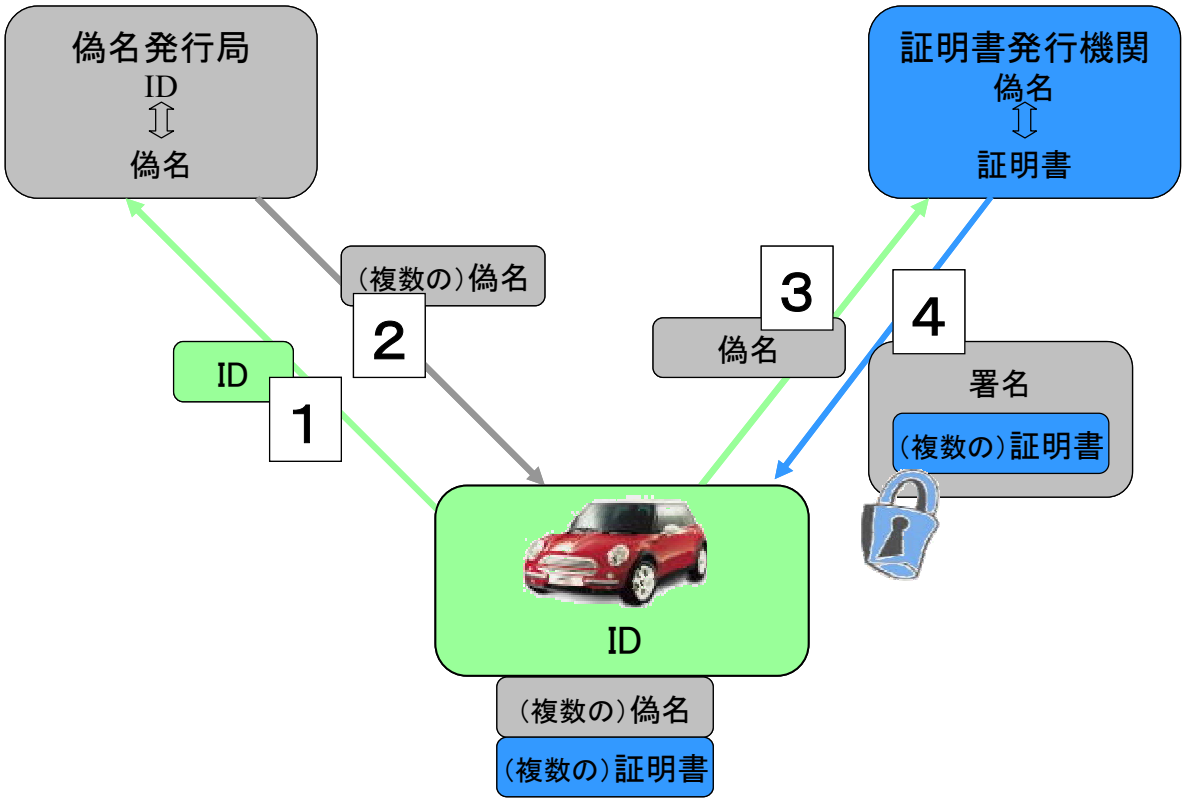

図３－２．保障機関型アプローチ：フェーズ１

②フェーズ２：サービス利用フェーズ
受信車は送信車からのメッセージの真正性を照合できる。

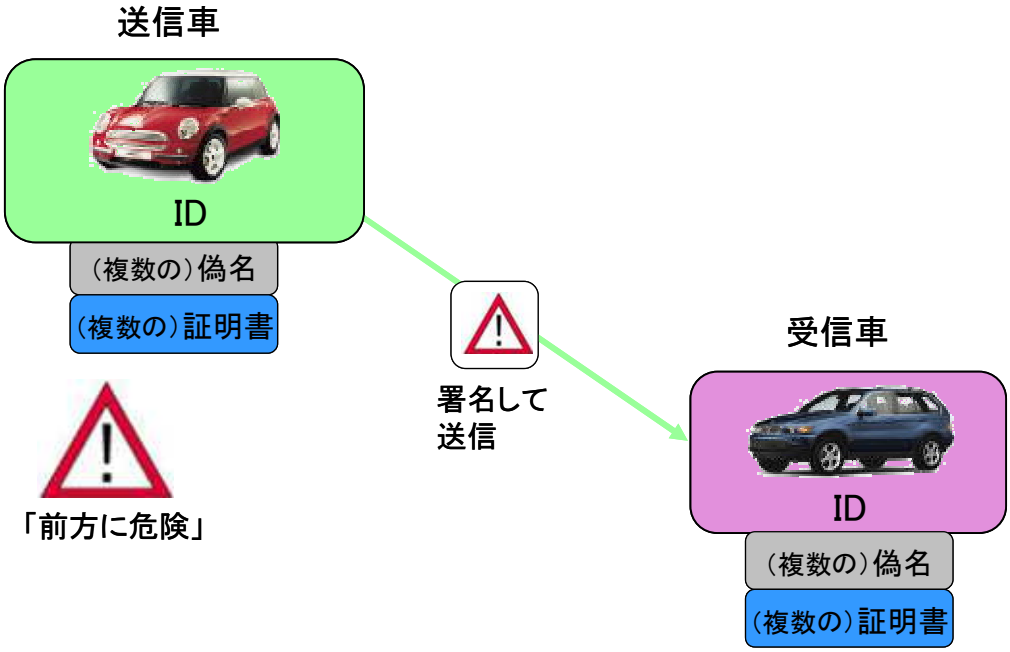

図３－３．保障機関型アプローチ：フェーズ２

③フェーズ３：取り消しフェーズ
メッセージが誤っている場合、送信車 ID を開示する。

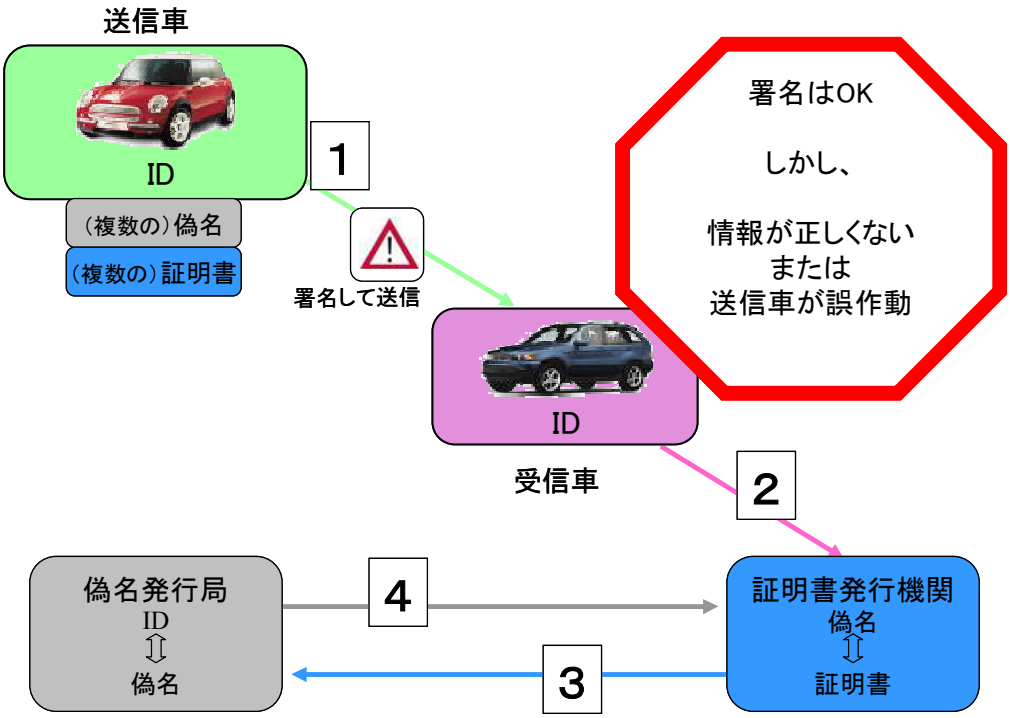

図３－４．保障機関型アプローチ：フェーズ３

この保証機関型アプローチの長所としては、上記の VANET におけるプライバシーの要件を満たすことと、堅固なプライバシーを提供できることが挙げられている。一方、短所としては、信頼性の高い独立機関が必要になることと、誤ったメッセージをどのように検出するかの問題が挙げられている。

３．３ RFID タグのプライバシー保護に向けた取組み

ユビキタスネットワーク環境において、RFID タグの利用はますます拡大しているが、RFID タグの利用時にプライバシーの問題が生じるのは、以下の 3 つの場合が考えられる。

① 利用者が所持する（製品の）RFID タグに個人情報が含まれ、その個人情報がリーダーによって不正に読み取られたり、改ざんされる場合
② 利用者が所持する製品の RFID タグに製品の ID 番号が含まれ、その ID 番号がリーダーによって不正に読み取られ、利用者の所持品の詳細が分かってしまう場合
③ 利用者が所持する製品の RFID タグに製品の ID 番号が含まれ、その ID 番号がリーダーによって不正に読み取られ、ID 番号によって利用者の行動が追跡されてしまう場合

①が最も分かりやすいプライバシー侵害のケースである。これについては、経済産業省の 2003 年の「商品トレーサビリティの向上に関する研究会中間報告書」[25]では、「電子タグ等が安心して社会に受け入れられるためには、経済性を重視した安価なタグに個人情報そのものを添付することは、更なる技術進歩を待った上で行うことが望ましい」との報告がいち早くなされ、RFID タグの中に個人情報自体を記録することには取り敢えずブレーキがかけられた。

②と③のケースについても、以下のように、すでにいくつかの保護方法が研究されてきている。

(a) RFID タグを金属の保護網または保護箔で覆う

リーダーによる読み取りを遮蔽する方法であるが、RFID タグの移動が難しくなるという問題がある。

(b) RFID タグを OFF にする

特別な「Kill」コマンドによって RFID の動作を OFF にする方法であるが、

[25] http://www.meti.go.jp/kohosys/press/0003896/

以下の利用例[26]に見るように、RFID タグは「ON」の状態であってこそ利用価値が高いという課題がある。

- 衣服、電気製品、CD 等にタグを付ける
  - スムーズな返品
  - 失くしたとき探しやすい（鍵やコードレス電話）
  - 部品交換
- 「スマート」電気製品
  - 冷蔵庫：買い物リストを自動作成、賞味期限切れの食品の通知
  - 洗濯機：衣類に合わせた適切な洗濯方法を検知
- 「スマート」印刷
  - 航空券：空港での旅客の現在地を示す
  - 名刺
- 視覚障害者のサポート
  - 「スマート」薬箱
- リサイクル
  - ごみの自動分別

(c) Blocker Tag[27]

RSA Laboratories の Ari Juels らが考案した方法である。Blocker Tag[28]はリーダーからの照会に対して、可能な限りのあらゆる ID 番号の信号を送信することで、一種の「スパマー」としてリーダーを混乱させ、Blocker Tag の周囲の RFID タグの読み取りを妨害する方法である。タグを OFF にする必要がないため、Blocker Tag を除去すれば、その他の RFID タグは通常どおり利用（読み取り）できるようになる。

この方法だと、Blocker Tag の所持者とは無関係な周囲の RFID タグの読み取りをも妨害してしまうという問題がある。例えば、Blocker Tag を持った利用者が、商店で、RFID を利用した万引き検出装置の監視をくぐり抜けて商品を持ち出してしまうといったケースが考えられる。

こうした問題については、「Privacy zone」という対策が提唱されており、これは Blocker Tag によるブロックを選択的にする、すなわち特定範囲の ID 番号（これが Privacy zone）の RFID タグの照会のみをブロックするように Blocker Tag を設定するという考え方である。商店の店員は、商品の販売後に当該商品の ID 番号を Privacy zone に移す（例えば、購入前は 0 から始まる

[26] http://petworkshop.org/2005/workshop/talks/paul-pets-0505.pdf を参考にした。
[27] http://www.rsasecurity.com/rsalabs/node.asp?id=2060 を参照のこと。
[28] それ自体も RFID タグである。

ID 番号を購入後に 1 から始まる ID 番号（Privacy zone）に移す。Blocker Tag は 1 から始まる ID 番号への照会はすべてブロックする）ことが可能である。

さらに、Blocker Tag が近くに無い場合には Privacy zone の RFID タグについてもリーダーによる読み取りができなければならないが、リーダーには Blocker Tag が近くにあるか無いかは分からないため、もし Blocker Tag があった場合にはリーダーは動かなくなってしまう。そこで、「Polite Blocking」として、Blocker Tag があらかじめリーダーに対して自分の存在を通知し、リーダーに Privavy zone を読み取らないようにリクエストする方法も考えられている。

(d) Soft Blocker[29]

さらに Juels らは、この Polite Blocking の考え方を推し進め、通常の RFID タグ内の書き込み可能な領域に「ブロックポリシー」の機能を持たせるような、「Soft Blocker」を考案した。Soft Blocker におけるブロックポリシーとしては、「この RFID タグを照会するにはオプトイン（事前の同意）が必要。ただし、人の生命の保護のために必要な場合を除く」など、利用者側で柔軟にポリシーを設定することが可能である[30]。

この方法の課題は、相手が impolite なリーダー（Polite Blocking のプロトコルを守らないリーダー）には効果がないこと、リーダーを polite にするには特別な改造が必要であること、リーダーによる ID 番号の追跡を防ぐことができないことが挙げられる。ただし、Soft Blocker を前述の Blocker Tag と組み合わせて使うことも可能とのことである。

(e) Privacy Bit[31]

また、Juels は前述の Privacy zone を推し進め、RFID タグに「Privacy Bit」を設ける考え方を提唱している。Privacy Bit は商品の購入前は OFF であり、購入時にレジに置かれた機器によって ON になる。リーダーは Privacy Bit が ON になっている RFID タグを通常は読み取ることができなくなる。

ただし、家庭内などでは、Privacy Bit が ON になった RFID タグについても読み取れた方が良い場合がある。リーダーを内蔵した家電製品がタグの情報を読み取るような場合である。そのため、Privacy Bit が ON になったタグを読み取ることができるような「private-read」コマンドというものが考えら

---

29 http://www.rsasecurity.com/rsalabs/node.asp?id=2032 を参照のこと。

30 利用者側でプライバシーの取り扱いについて条件設定を行うという点は、P3P におけるプリファレンスの考え方に似ている。

31 http://www.rfidjournal.com/article/articleview/1536/1/133/を参照のこと。

れている。ただ、不正な「private-read」コマンドによりタグの情報が読み取られては困るため、「private-read」コマンドを発したリーダーを、他のリーダーが互いに検査する方法や、「private-read」コマンドを発するリーダーに対して Blocker Tag で妨害する（家庭などで「private-read」コマンドが必要な場合は Blocker Tag を外す）方法が考えられている。

４．プライバシー保護のための新たな技術的対策の研究

EU 指令（EU データ保護指令）や我が国の JISQ15001（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）では、個人情報の収集時の「インフォームド・コンセント」（利用目的、提供範囲等の必要事項を通知し、本人の同意を得た上で収集する原則）が規定されている。P3P も基本的にこの原則に従って、個人情報の収集前にプライバシーポリシーを本人に自動的に提示しようとするものである。

しかし、この「インフォームド・コンセント」方式の欠点は 2 点ある。いったん同意して企業に収集された個人情報については、企業による流用や悪用（目的外利用や目的外提供）を利用者側でコントロールすることができなくなる点[32]と、利用者が企業のプライバシーポリシーに同意できない場合は当該企業のサービス利用をあきらめざるを得ない点である。インターネット上で利用者のプライバシーを保護するための技術が取り組むべき課題は、この 2 点にあると言える。

これらの 2 点を解決しようとするのが、以下に述べる「プリファレンスポリシー」の考え方である。

「自分の個人情報を第三者に提供して欲しくない」「自分の個人情報をダイレクトメール発送に使って欲しくない」という利用者側の希望は、ある意味では当該利用者の「個人情報」の一部と考えることができる。プリファレンスポリシー方式では、こうした利用者側のプライバシーに関する要望（プリファレンス）を、利用者の個人情報の一部として、あるいは個人情報に対するメタデータとして、インターネット上で企業側に個人情報と一緒に送信することで、利用者の意向に沿ったかたちで（本人が望まない目的では利用しないように）個人情報を適切に取扱ってもらおうとする。つまり、従来のように企業側がプライバシーポリシーを一方的に持つのみならず、利用者側もポリシーを持ち、企業側に提示していくという、発想の転換を行うものである。

（1）プリファレンスポリシーの提示方式

プリファレンスポリシー[33]は、P3P のプリファレンス、およびプロトコルを応用して実現する。

---

[32] 目的外利用や目的外提供が本人に判明すれば、個人情報保護法によって当該個人情報の利用停止や消去の要求をすることはできるが。

[33] 利用者の個人情報を企業・サイトがどのような利用目的や提供範囲等で取扱って良いかを定めた、個人情報利用許諾条件をポリシーとして規定したもの。

利用者は、PC 等のインターネット接続端末において、作成ツールを用いてあらかじめプリファレンスポリシーを作成しておく。

オンラインショッピングサイト等、オンラインサービスサイトにおいて初回のサービス申込をする際には、プリファレンスポリシーとサービス申込書（利用者の個人情報を含む）とセットで署名した上、申込を行う。

オンラインサービスサイトは個人情報とプリファレンスとをセットで保管し、個人情報を利用する場合は、セットになったプリファレンスポリシーの範囲内で利用するものとする。

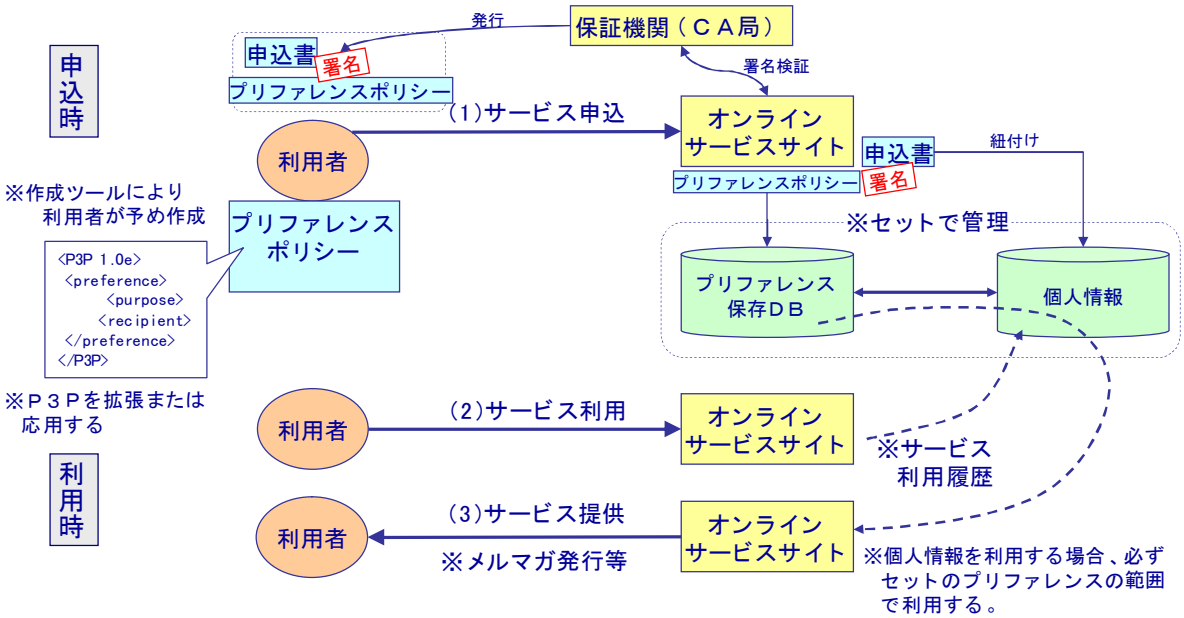

図４－１．プリファレンスポリシーの掲示方式

（２）プリファレンスポリシーの継承方式

オンラインサービスサイトが利用者のプリファレンスポリシーに基づき、個人情報を業務委託先に預託したり、他の事業者と共同利用したり、他の事業者に提供[34]したりする場合、利用者の個人情報とともにプリファレンスポリシーも継承する必要がある。

---

34 プリファレンスポリシーにおいて他の事業者への提供を許可するようなケースとして、以下のものが考えられる。

- 旅行サイトに対して、旅行手配の目的であれば他の事業者（航空会社やホテル）に自分の個人情報を提供してよりというプリファレンスポリシーを送る場合
- 就職斡旋サイトに対して、採用活動の目的であれば他の事業者（求人企業）に自分の個人情報を提供してよいというプリファレンスポリシーを送る場合
- e ラーニングサイトに対して、学習者管理の目的であれば他の事業者（教育事業者）に自分の個人情報（学習履歴等）を提供してよいというプリファレンスポリシーを送る場合

まず、オンラインサービスサイトは、利用者の個人情報を提供・預託する際には、利用者のプリファレンスポリシーとセットにして、サイトの署名を行ったものを他の事業者に提供・預託する。その際、プリファレンスポリシーには、利用者の申込時の署名がつく。

提供・預託先の事業者においても、利用者の個人情報とプリファレンスとをセットで保管し、個人情報を利用する場合は必ず、プリファレンスの範囲内で利用するようにする。

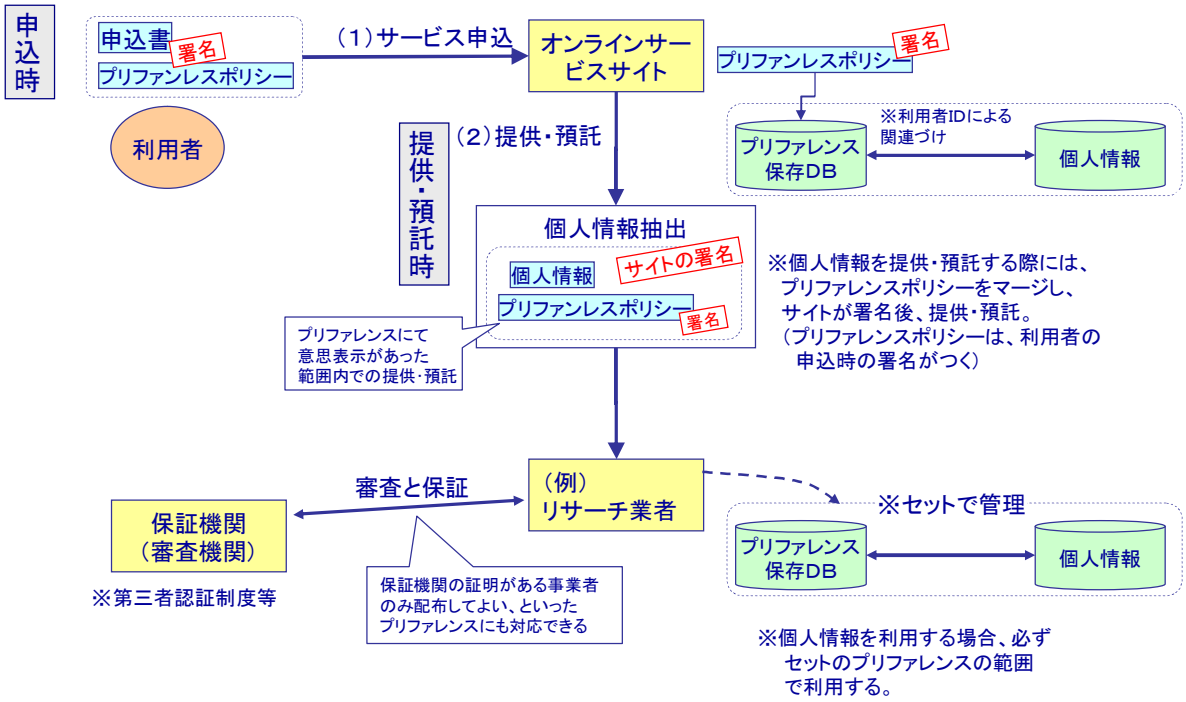

図４－２．プリファレンスポリシーの継承方式

（３）プリファレンスポリシーの確認・訂正方式

生活環境等の変化によって、利用者のプリファレンスに経時的な変化が生じる可能性が考えられる。例えば、若い時にはサイトにおける個人情報の利用や提供について比較的寛大であった利用者が、様々な経験によって、次第にサイトへの個人情報の開示に慎重な態度を取るようになるケースが考えられる。

したがって、利用者が一旦オンラインサービスサイトにプリファレンスポリシーを提出した後も、利用者の「好み」の変化に応じて、過去に提出したプリファレンスポリシーを本人が閲覧・確認し、内容の訂正を行える必要がある。場合によっては、利用者の要求に応じて個人情報とプリファレンス自体を削除することも必要である。

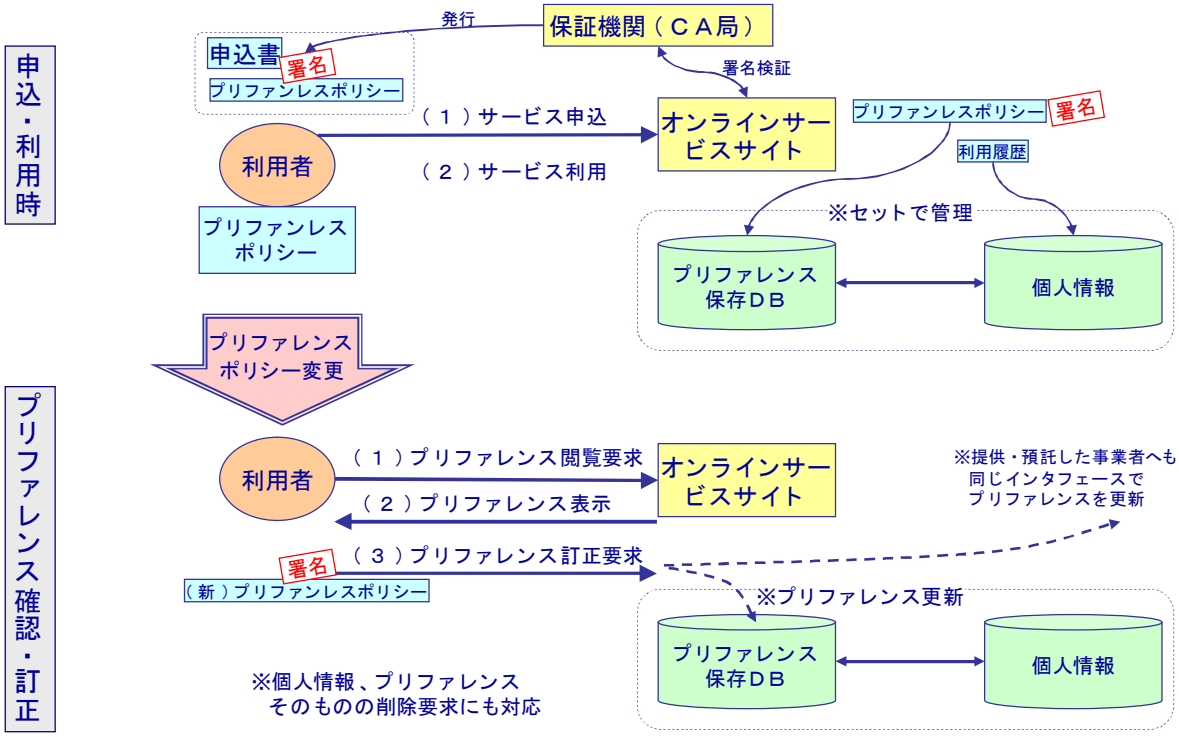

図４－３．プリファレンスポリシーの確認・訂正方式

（4）プリファレンスポリシーの遵守保証方式

利用者がプリファンレンスポリシーをオンラインサービスサイトに提出しても、それをサイトが遵守するかどうかはサイト次第である。このことは、２．３節で述べた P3P ポリシーの課題（P3P ポリシーで宣言されている内容が遵守されているか P3P だけでは保証されない）と同様のものである。この課題に対しては、サイトが「利用者のプリファレンスポリシーを遵守します」という内容を含むプライバシーポリシーを作成し、その内容を遵守した取扱いを行っていることを第三者認証機関が証明を行い、サイトが証明（認証マークなど）付きのプライバシーポリシーを掲示することによって利用者に対してプリファレンスポリシーの遵守を保証する、という方法が考えられる。

まず、オンラインサービスサイトは自社のプライバシーポリシーを P3P ポリシーとして作成する。その際、P3P を拡張して、「利用者のプリファレンスポリシーがサイトの P3P ポリシー以上の内容を含む場合は、プリファレンスポリシーを優先させる」という内容をプライバシーポリシーに含める必要がある[35]。

オンラインサービスサイトは第三者認証機関の審査によって、プライバシーポリシー／P3P ポリシーの内容を遵守した取扱いを行っていることを証明して

35 これによって、利用者が企業のプライバシーポリシーを許容できず、通常であればサービス利用をあきらめざるを得ない場合でも、サービス申込・利用が可能になる。

もらい、証明（認証マーク）付きのプライバシーポリシー／P3P ポリシーをサイトに掲示する。

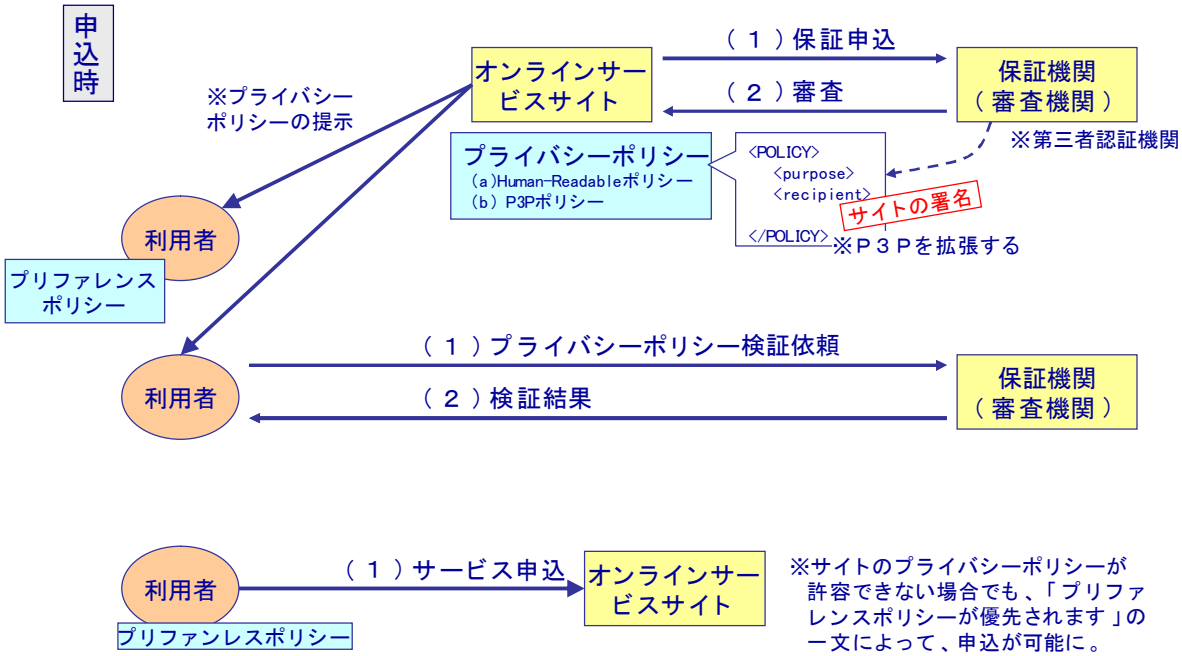

図４－４．プリファレンスポリシーの遵守保証方式

最近の Winny による一連の個人情報漏えい事件に典型的に見られるように、インターネット上でいったん漏えいしてしまった個人情報については、その流出元の情報を削除したとしても、ネットワーク上での流通を止めることは不可能である。しかも、近年ますます、市井の利用者の個人情報が、本人に何の落ち度もないにもかかわらず、ふとしたきっかけでネットワークに流出してしまうリスクが拡大している。本章で示した「プリファレンスポリシー」方式によって、利用者の個人情報とセットでプリファレンスを持っておくことで、万が一インターネット上で個人情報が流出してしまった事態においても、善意の「拾い主」によるさらなる悪用（本人の望まない目的での利用）には少しでも歯止めがかかる[36]ことを期待することができよう。

[36] もちろん、個人情報を悪用しようと意図している人に「拾われた」場合は仕方がないが。

付録１．「プライバシー保護技術 P3P に関する調査」**調査票**

０．ご回答者についてお尋ねします。　　＊は必須項目です。

会社名＊	
部署名＊	
役職名	
氏名	
電話番号	
メールアドレス	

なお、頂きました個人情報は本調査の目的以外では一切使用いたしません。

Ⅰ．御社サイトにおける P3P の導入についてお尋ねします。

問１．御社サイトに P3P を導入※された時期について、お差支えのない範囲でお教えください。 ※本調査票では、サイトに P3P プライバシーポリシーを掲載することをこのように呼びます。	年　　月
問２．御社サイトに P3P を導入されたきっかけについて、お差支えのない範囲でお教えください。 （複数回答）	１．ブラウザの Internet Explorer に P3P 対応のクッキー管理機能が実装されたため ２．W3C において、P3P 仕様書のワーキングドラフトや正式勧告文書が公開されたため ３．米社サイトにおいて P3P を導入しているため ４．顧客に対して、プライバシー保護活動を積極的に行っていることを示すため ５．企業の社会的な責任を果たすため ６．その他（　　）
問３．御社サイトへの P3P 導入の効果について、お差支えのない範囲でお教えください。 （単数回答）	１．大いに効果があった ２．効果があった ３．あまり効果がなかった ４．効果がなかった ５．何ともいえない （1、2にご回答の場合）どのような効果がございましたでしょうか？ （　　）

Ⅱ．P3P の課題・問題点についてお尋ねします。

問４．P3P をサイトに導入することは難しいと思いますか？お差支えのない範囲でお答えください。（単数回答）	１．大変に難しいと思う ２．難しいと思う ３．それほど難しくないと思う ４．難しくないと思う ５．何ともいえない
問５．P3P をサイトに導入するに当たっての課題はどのようなことだと思いますか？　該当する番号すべてに○をつけてください。（複数回答）	１．P3P で定義されている項目（利用目的など）が日本の実情に適合していない ２．サイトに P3P を導入する方法を分かりやすく説明した資料がない ３．簡単に導入するためのジェネレーターなどのツールがない ４．P3P 仕様書の日本語訳が分かりにくい ５．せっかくサイトに導入しても、具体的な利用シーンが少ない ６．その他（　　）
問６．インターネット利用者が P3P を利用するにあたっての課題はどのようなことだと思いますか？　該当する番号すべてに○をつけてください。（複数回答）	１．P3P の存在がインターネット利用者に十分周知されていない ２．P3P を導入しているサイトが少ない ３．P3P を導入しているサイトの閲覧時でも、P3P の出番が少ない ４．ブラウザでサイトの P3P プライバシーポリシーを確認したとき、日本語が分かりにくい ５．P3P を有効に活用するためのツールがない ６．その他（　　）

Ⅲ．P3P の普及啓発についてお尋ねします。

問７．P3P の普及に向けて、産業界としてすべきことはどのようなことだとお考えですか？　該当する番号すべてに○をつけてください。（複数回答）	１．P3P を簡単に利用できるようなツールの開発に努める ２．ブラウザにより高度な P3P 対応機能を実装する ３．P3P 情報の共通ポータルサイトを構築する ４．P3P を分かりやすく説明した資料を Web 上で公開する ５．日本の実情にあった項目（ボキャブラリ）を作成する ６．その他（　　）
問８．その他、P3P についてご意見がございましたら、ご自由にご記入ください	

設問は以上です。お忙しい中、ご協力いただきまして誠にありがとうございました。