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

調査報告書

平成 16 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．背景と目的

財団法人ニューメディア開発協会では、平成 11 年度に通商産業省からの出資を受けて情報処理振興事業協会が実施する「先進的情報システム開発実証事業」の一環として、国際的 Web 技術標準化団体の W3C（World Wide Web Consortium）の P3P（Platform for Privacy Preference）ワーキングドラフトに基づく「プライバシー情報管理システム」の開発と提供を行っている。また、平成 13 年度および平成 14 年度には、W3C の P3P1.0 勧告候補版および勧告版に基づく「P3P ポリシーウィザード」の開発と提供を行っている。

財団法人ニューメディア開発協会ではこのように継続的に、いわゆる PET（Privacy Enhancing Technology、プライバシー保護技術）[1]の開発を行ってきている。本調査では、近年のユビキタス・コンピューティング等の技術的環境の変化および個人情報保護法案等の制度的環境の変化を踏まえ、P3P を始めとする PET の新たな動向に関する調査を行うことを目的とする。

---

[1] PET は、EU 委員会サイトの Data Privacy セクション（http://europa.eu.int/comm/internal_market/privacy/index_en.htm）においては、「PET の概念は、個人データの可能な破壊・改ざん・漏えいを防ぐために、個人データの収集と利用を最小化し、かつあらゆる不正な形態の個人データ処理を防ぐ（例えば個人データへの不正アクセスを技術的に不可能にする）ための情報通信システム／技術を設計することを目指している」と規定されている。

２．P3P に関する調査

本章では、W3C の P3P 仕様に基づくプライバシー保護のための応用システムについて、事例調査を行った。

２．１ P3P の概要

（１）P3P 概要

P3P とは、Platform for Privacy Preferences Project（プライバシー情報取扱いに対する個人の選好を支持する技術基盤）[2]の略であり、Web 技術の標準化団体である W3C（World Wide Web Consortium）[3]が 1997 年から仕様策定を開始した、インターネット上のプライバシー保護のための技術仕様である。2002 年 4 月 16 日に、P3Pver1.0 が正式な W3C 勧告として策定されている[4]。

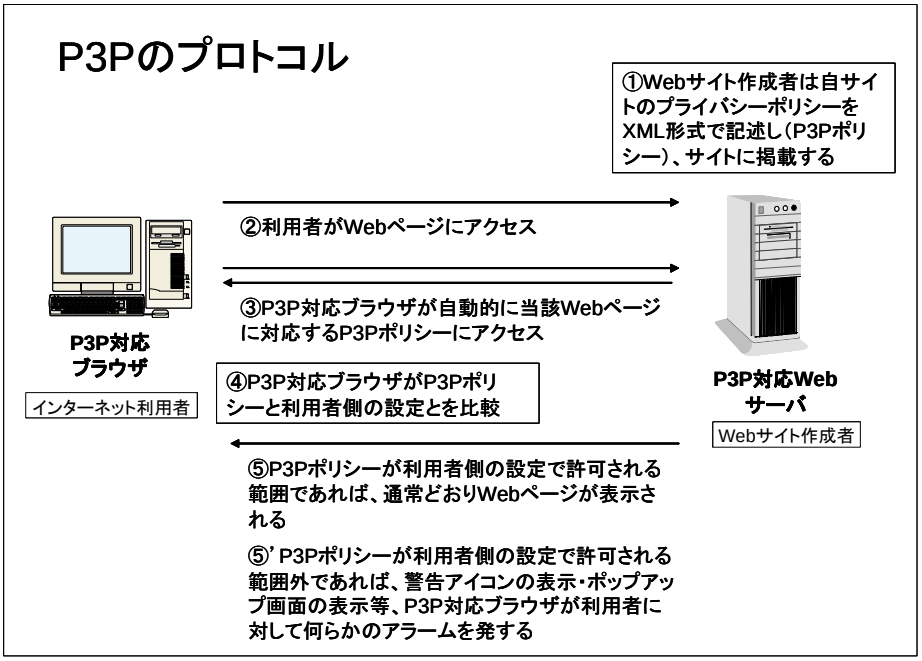
P3P が目指すものは、インターネット上の個人情報流通において企業と消費者との「インフォームド・コンセント」を保証することである。従来、インターネット上のプライバシーポリシーには、①各社により記述形式がまちまちである、②米国では訴訟沙汰を避けるために分量が膨大で法律用語が駆使されており、各社サイトを訪問する都度ポリシーを読むのは消費者に多大な負担をかける、また、日本では逆に抽象的な表現が多く、消費者にとって各社の具体的な個人情報取扱い内容が分かりにくい、という問題があった。P3P での解決策は、①プライバシーポリシーの掲載項目を標準化し、②プライバシーポリシーの掲載項目を XML 形式で記述することで（P3P 仕様に基づき XML 形式で記述したプライバシーポリシーを P3P ポリシーという）、プライバシーポリシーの消費者側での機械処理を可能にするというものである。

P3P のプロトコルは図 1 の通りである。①まず、Web サイト作成者は自サイトのプライバシーポリシーを XML 形式で記述し（P3P ポリシー）、サイトに掲載する。②利用者が Web ページにアクセスする。③P3P 対応ブラウザが自動的に当該 Web ページに対応する P3P ポリシーにアクセスする。④P3P 対応ブラウザが P3P ポリシーと利用者側の設定とを比較する。⑤P3P ポリシーが利用者側の設定で許可される範囲であれば、通常どおり Web ページが表示される。または、⑤’P3P ポリシーが利用者側の設定で許可される範囲外であれば、警告アイコンの表示・ポップアップ画面の表示等、P3P 対応ブラウザが利用者に対して何らかのアラームを発する、というプロトコルである。

---

[2] http://www.w3.org/P3P/
[3] http:/ http://www.w3.org/TR/P3P//www.w3.org/
[4] http://www.w3.org/TR/P3P/

図 1　P3P のプロトコル



P3P 仕様で規定されている P3P ポリシーのうちの必須掲載項目は表 1 の通りである。

表 1　P3P ポリシーの必須掲載項目

P3P ポリシーの必須掲載項目		掲載形式
ポリシーに関する情報（POLICY element）	ポリシーの名称	自由記述
	自然言語で書かれたプライバシーポリシーの URL	自由記述
	Opt-in または Opt-out の URI(利用目的で Opt-in、Opt-out が指定されている場合のみ)	自由記述
事業者・組織に関する情報（ENTITY element）	事業者・組織の名称	自由記述
	連絡先情報（住所、電話番号、メールアドレス、URI のうち 1 つ以上が必須）	自由記述
アクセスに関する情報（ACCESS element）		単数選択
苦情処理に関する情報（DISPUTES element）	苦情処理のタイプ	単数選択
	上記のサービスに関する URI	自由記述

[Must ではなく Should] （複数重ね書き可能）		
苦情処理の方法に関する情報 （REMEDIES element） [Must ではなく Should]		複数選択
ステートメントに関する情報 （STATEMENT element） （複数重ね書き可能）	利用目的に関する情報 （PURPOSE element）	複数選択
	受領者に関する情報 （RECIPIENT element）	複数選択
	保有期間に関する情報 （RETENTION element）	単数選択
	収集する個人情報に関する情報 （DATA-GROUP and DATA elements）	複数選択

（２）業界の動向

2003 年 8 月現在、W3C の P3P ページ[5]に登録されているだけでも 800 以上のサイトが P3P 対応（2001 版準拠のサイトを含む）となっている。米国では、Microsoft、AOL、AT&T、IBM、HP、米国商務省等、日本では、インターネット協会、BIGLOBE、ニフティ等が挙げられる。

また、マイクロソフトのブラウザ IE6.0 の P3P 対応クッキー管理機能では、デフォルト設定では、サードパーティー・クッキー[6]を伴うような Web オブジェクトについては、P3P ポリシーが付与されていないと、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ため、Web 広告企業（ダブルクリック等）はバナー広告に P3P ポリシーを付与する対応を行っている。

Ernst&Young のレポート[7]によれば、2004 年 1 月現在で米国トップ 100 サイトのうち 31%、トップ 500 サイトのうち 23%が P3P を導入している。サイトカテゴリー別にみると、トップ 500 サイトに含まれるショッピングサイト 58 サイトのうち 36%、ポータル 42 サイトのうち 33%が P3P を導入している。ちなみに、2002 年 8 月時点では、トップ 100 サイトが 24%、トップ 500 サイトが 16%であった。

---

[5] http://www.w3.org/P3P/compliant_sites

[6] 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「サードパーティー・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など。

[7] http://www.ey.com/global/content.nsf/US/AABS_-_TSRS_-_Services_-_Privacy

（３）今後の方向性

P3P においてプリファレンス（情報主体側が指定する個人情報利用原則）を記述するための言語として、APPEL（A P3P Preference Exchange Language 1.0）のドラフト仕様[8]があるが、現状のニーズや課題にマッチしていない（複雑すぎたり、必要な側面が欠けていたりする）。IBM、JRC、HP、Microsoft 等のメンバーは、新たなプリファレンス言語の策定作業が必要であるという認識で一致している。

また、P3P 関係者において、企業のバックエンド業務用のプライバシーと権限管理のための言語への関心が高まっており、2003 年 12 月 2 日には EPAL（Enterprise Privacy Authorization Language）仕様が IBM から W3C に提案された[9]。EPAL は、IT システムにおける個人情報取扱いを、詳細なアクセス権限／利用権限に基づき管理するための企業内プライバシーポリシーを記述する言語で、P3P にマッピング可能である。

2004 年 2 月 10 日には、P3Pver1.1 の最初のワーキングドラフト[10]が公開された。P3P1.0 からの改善点は以下の点である。

- 誤字脱字の修正
- ユーザエージェントが P3P ポリシーの概要を表示できるように、ステートメントに名前を付け、また複数ステートメントをグループ化するメカニズムの追加
- ユーザエージェント用のガイドラインの追加
- XForms や WSDL 等の他の XML アプリケーションにおいて P3P を利用できるように、P3P ポリシーと任意の XML をバインディングする一般的方法の規定

また、P3P1.0 仕様書（および P3P1.1 ワーキングドラフト）によれば、P3P の将来バージョンには以下のメカニズムを組み込む可能性があるとのことである。

- サイトがサイト訪問者に P3P ポリシーを選択させるようなメカニズム
- ユーザエージェントを通じて訪問者が P3P ポリシーに明示的に同意するためのメカニズム
- サイト訪問者とサイトの間の同意の否認防止のためのメカニズム
- ユーザエージェントが利用者の個人情報をサイトに送信するためのメカニズム

（４）財団法人ニューメディア開発協会の取組み

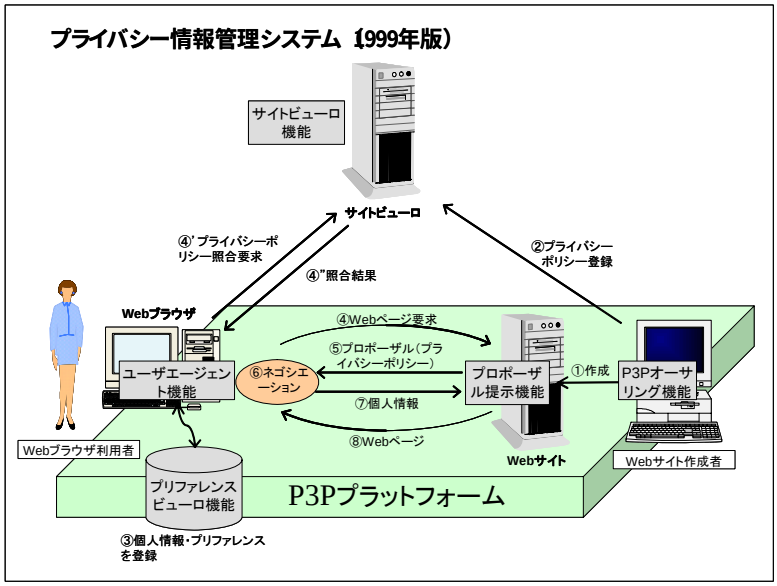
国内での取組みとしては、(財) ニューメディア開発協会が P3P 仕様に基づく実験システムの開発を継続的に行ってきている。

同協会では、1999 年 3 月に P3P の 1998 年 11 月版ワーキングドラフト仕様に基づく「プライバシー情報管理システム」を開発・公開した（図 2 参照）。

---

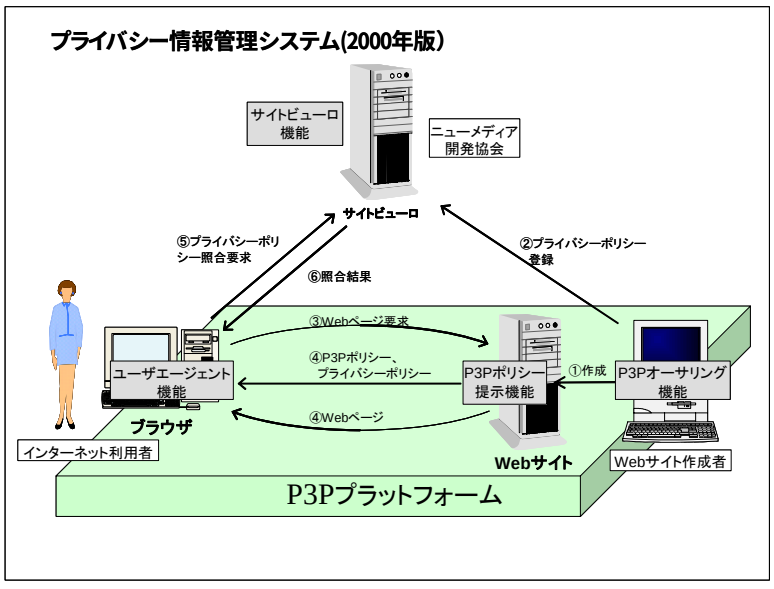
8 http://www.w3.org/TR/P3P-preferences/
9 http://www.zurich.ibm.com/security/enterprise-privacy/epal/
10 http://www.w3.org/TR/2004/WD-P3P11-20040210/

図 2　プライバシー情報管理システム（1999 年版）



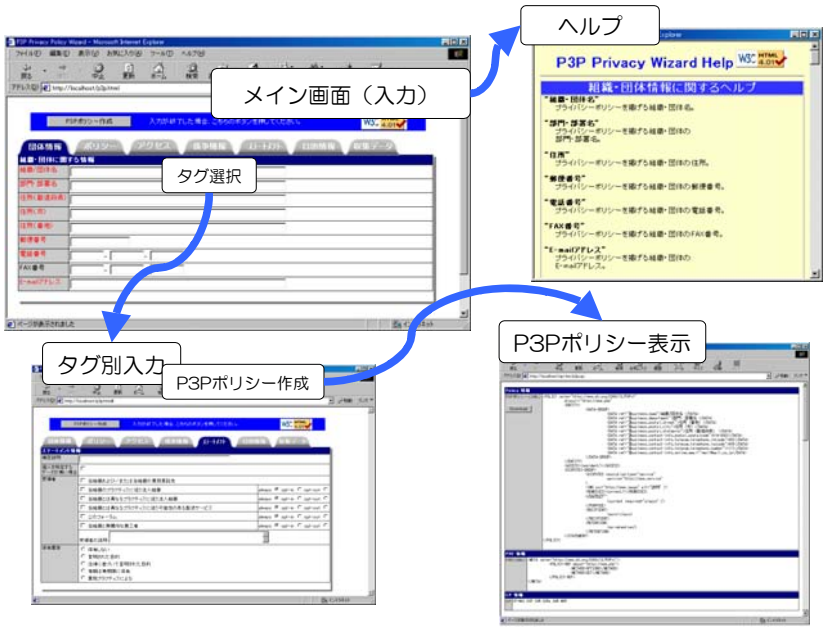
同協会ではさらに、同システムを広く海外に向けて紹介し、また P3P に準拠して開発された他のシステムとの相互運用性を検証することで W3C の活動に寄与するために、2000 年 6 月にニューヨークで開催された P3P Interoperability Testing Day にシステムを出展した。出展に当たっては P3P の 2000 年 6 月時点での最新スペック（2000 年 5 月版ワーキングドラフト）に準拠させるために、1999 年開発のシステムに修正を加えた（図 3 参照）。

図 3　プライバシー情報管理システム（2000 年版）



また、同協会は 2001 年 3 月に日本語サイト向けの P3P ポリシージェネレーター（P3Pver1.0 の 2000 年 12 月勧告候補版に対応）を開発し、Web 公開した[11]。2002 年 5 月には同ジェネレーターを、P3Pver1.0 の 2002 年 4 月正式勧告版に対応させた。同協会の P3P ポリシージェネレーターはホームページを操作する手軽さで誰でも容易に P3P ポリシーを作成できる。同ジェネレーターはタグ画面になっており、画面上の質問に回答することにより、P3P ポリシーが自動的に出力される。さらに画面に出力された P3P ポリシーをウェブサイトに付加することにより、ウェブサイトは P3P 対応となる。その結果、ウェブ利用者側（クライアント側）の P3P 機能（ブラウザ）との連携により、個人情報をどこまで開示するかを半自動で判断できるようになり、ポリシーに沿った個人情報の開示と保護が可能となる（図 4 参照）

図 4　P3P ポリシージェネレーター



２．２ P3P 対応のソフトウェア

P3P に対応したソフトウェアとしては、以下のものが公表されている。

２．２．１ ブラウザ側ツール

（１）Internet Explorer 6.0

クッキー管理機能の一部として P3P 対応している。デフォルト設定では、サードパーティー・クッキーを伴うバナー広告等については P3P ポリシーが無いと、クッキーが自動的に遮断され、さらにブラウザの下方に警告アイコンが表示される。

[11] http://www.nmda.or.jp/enc/privacy

（２）Netscape 7.0

P3P に基づく以下の 2 つのプライバシー関連機能を導入している。Internet Explorer 6.0 と類似の機能である。

- P3P プライバシーポリシー閲覧機能により Web サイトのプライバシーポリシーを表示する
- P3P クッキー管理機能によりクッキーを管理する

（３）AT&T Privacy Bird[12]

利用者が Web サイトに提供した個人情報がどのように利用されるについて、アイコン表示をする。同ツールは訪問したサイトのプライバシーポリシーを自動的に探し出す。利用者が設定したプライバシー・プリファレンス（サイトがどのように個人情報を取り扱ってよいかの条件設定）とサイトのプライバシーポリシーとを照合させ、プリファレンスに適っているかどうかを鳥の形のアイコンで表示する。

２．２．２ サーバ側ツール

（１）IBM Tivoli Privacy Manager for e-business[13]

P3P ベースのプライバシーポリシーを e-business アプリケーションとインフラに直接的に組み込むことを可能にする。業務におけるプライバシーポリシーの遵守を自動化することができる。プライバシーポリシーの管理を改善し、企業内でプライバシーポリシーを整合的に実践することを支援するようなインフラを提供する。IBM Tivoli Privacy Manager for e-business については次節で詳述する。

（２）P3Pedit[14]

商用の P3P ポリシージェネレーターである。多くの企業や個人 Web サイトに使用されている。Web ベースのウィザードである。英語とスペイン語に対応している。P3P ポリシー（XML）、P3P コンパクトポリシー、プライバシーステートメント（HTML）を作成できる。

（３）P3P Policy Editor[15]

IBM が提供している。P3P に基づくプライバシーポリシーを作成・更新するためのインターフェースを提供する。

---

12 http://privacybird.com/
13 http://www-3.ibm.com/software/tivoli/products/privacy-mgr-e-bus/
14 http://p3pedit.com/
15 http://www.alphaworks.ibm.com/tech/p3peditor

（４）その他の P3P ポリシージェネレーター

その他、以下のようなジェネレーターが公表されている。

・P3P Editor
・Customer Paradigm
・P3Pdeveloper.com
・P3Pwriter.com

２．２．３ IBM Tivoli Privacy Manager for e-business[16]

（１）機能概要

同システムは、P3P 準拠のプライバシーポリシー（ヒューマンリーダブルポリシーおよび P3P ポリシー）の作成をサポートするとともに、それを企業内のアプリケーションや IT システムに適用することを可能にするシステムである。

まず､企業は Policy Editor 機能を使ってプライバシーポリシーを定義することができる。そのプライバシーポリシーは電子フォーマット（P3P 準拠、XML 文書）に変換され、個人情報を取扱うアプリケーションや IT システムに実装される。一方、情報主体が当該企業に個人情報を提供する際には、個人情報の取扱い方法に関する同意が個人別に記録される。この記録は、個人情報を利用できる条件（誰が、どんな目的で、誰の情報を取り扱えるか）をきめ細かく定義した許諾条件の形で保存される。アプリケーションや IT システムで個人情報が処理される際には､Privacy Manager Server と Privacy Manager Monitor の機能によって、定義したプライバシーポリシーや情報主体の許諾条件に基づく監視が行なわれる。すなわち、個人情報の利用目的別に定義されたアクセス制御が実行されるように、アクセス監視と制御がなされる。Privacy Manager Server は Privacy Manager Monitor から個人情報へのアクセス情報を受け取り、プライバシーポリシーに適合するか否かを判断してアクセス可否を決定する。Privacy Manager Monitor は個人情報にアクセスするアプリケーションに実装され、個人情報にアクセスが発生したとき、Privacy Manager Server へアクセス可否判断を問い合わせて、判断結果をアプリケーションに返答する。また、プライバシーポリシーの遵守を判断するための詳細なレポートの作成が可能であり、個人情報へのアクセスがポリシーに適合しているか否かの監査証跡や特定の個人情報を誰が何の目的でアクセスしたかに関するレポートが作成される。

IBM Tivoli Privacy Manager for e-business の各機能の概要は表 2 の通りである。

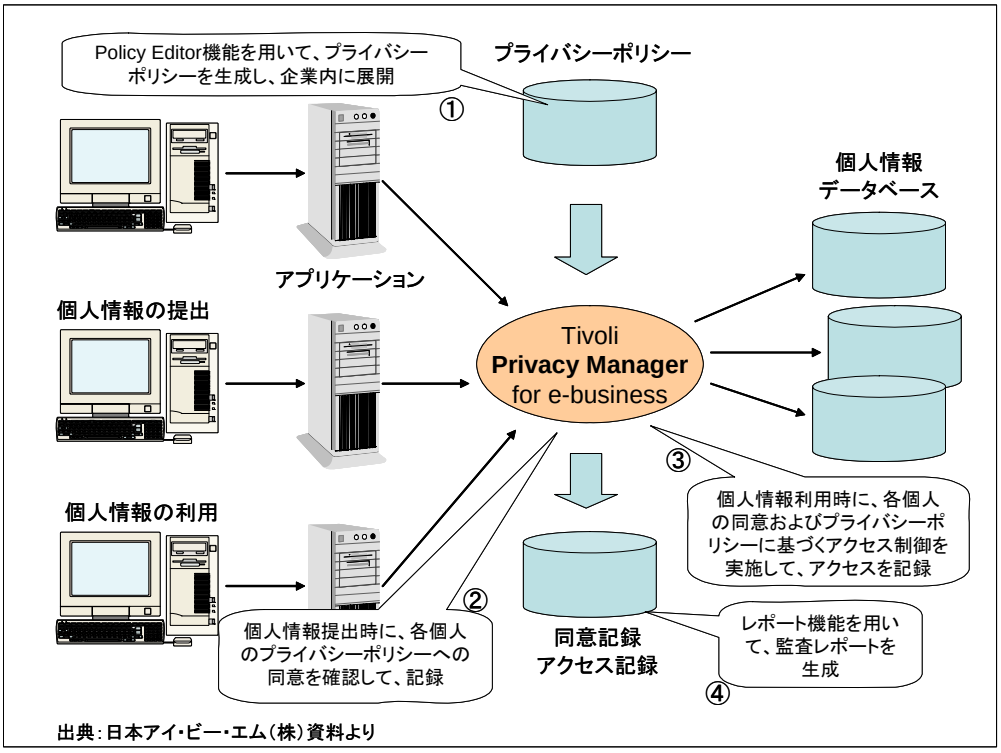
16 同社各種資料より。

表 2　Tivoli Privacy Manager for e-business の機能概要

機能	説明
Policy Editor	入力されたプライバシーポリシーを電子フォーマット（P3P 準拠）に変換する。統一形式のプライバシーポリシーを、様々なシステムに実装可能。
Policy Deployment Facility	プライバシーポリシーに記載されたデータ項目や利用目的を、具体的なサーバ、取扱者、アプリケーションや IT システムに適用する。既存のポリシーの変更や新たなポリシーの追加の際、アプリケーションや IT システムを自動的に更新する。
Privacy Manager Server	ポリシーに基づいてアクセスを監視する。
Reporting tools	個人情報の利用状況やプライバシーポリシーの遵守状況、情報主体による同意内容など、データ取扱者による個人情報へのアクセスの記録を作成する。
LDAP Monitor	LDAP レポジトリへのデータの送信や、LDAP レポジトリへのアクセス要求をモニタリングする。LDAP 環境に対して容易にプライバシーモニタリングが可能。ポリシーエディターによって定義されたプライバシーポリシーを企業全体に実装して管理する。
Monitor SDK	新たにモニター機能を開発するためのソフト開発ツールキット。

また、IBM Tivoli Privacy Manager for e-business の概念図は図 5 の通りである。

図 5　Tivoli Privacy Manager for e-business の概念図



２．３ EPAL

EPAL（Enterprise Privacy Authorization Language）[17]は企業内で利用するプライバシーポリシーのための言語である。EPAL は P3P を発展させた仕様であり、XML 言語で記述され、P3P にマッピング可能である。企業における個人情報取り扱いを記述するための詳細なボキャブラリを規定している。また企業が個人情報を収集する目的を詳細な階層で記述できる。

EPAL では、企業における個人情報取り扱いルール（EPAL ポリシー）を標準化された形式で記述できる。企業は EPAL ポリシーに従って、データ処理者からの個人情報処理要求を許可したり却下したりすることが可能になる。

EPAL ポリシーで記述されるルールには、下記のエレメントが含まれる。

- user-category：データの利用者。例えば、営業部門など
- data-category：データの種類。例えば、顧客情報など
- purpose：利用目的。例えば、注文の処理など
- action：データの処理方法。例えば、store（保存）、read（参照）など
- condition：前提条件。例えば、顧客が 13 歳以上であることなど
- obligation：義務。例えば、3 年後にデータ廃棄を行なうことなど

なお、上記のエレメントについて、配下のエレメントは規定されていない。すなわち、上記の例で言えば、「営業部門」「顧客情報」「注文の処理」「store（保存）」「read（参照）」等の詳細エレメントは EPAL の仕様書の中で規定されていない。これは、EPAL が多くの分野におけるプライバシーポリシーをカバーできるように設計されているからであり、それら様々な分野におけるプライバシーポリシーにおける標準的項目までをあらかじめ規定できないからである。そのため、EPAL では、こうした各分野での詳細エレメントを定義するためのメカニズムを提供するにとどめている。

---

[17] EPAL1.1 の仕様書は、
http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/index.html

３．クッキー等の個人情報収集技術に関する調査

本章では、クッキーや Web ビーコン、スパイウェアといったインターネット上の個人情報収集技術に関する調査を行った。

３．１ クッキー

３．１．１ クッキーの仕組み

クッキーとは、利用者を識別するために Web サイトが利用者の PC に格納する小さなファイルのことである。

クッキーの仕様はネットスケープの Web サイト[18]で公開されている。クッキーの仕様では、サーバは利用者の PC に HTTP オブジェクトを返すとき、状態情報（state object）を送り、利用者の PC に設置（保存）することができる。この状態情報がクッキーである。クッキーが設置された PC からサーバへのそれ以降の HTTP リクエストにはこのクッキーが付加される[19]。

サーバが利用者の PC にクッキーを設置するためには、HTTP ヘッダーの一部に Set-Cookie ヘッダーを含める。HTTP ヘッダーの中には、複数の Set-Cookie ヘッダーを含めることができる。

Set-Cookie: NAME=VALUE; expires=DATE; path=PATH; domain=DOMAIN_NAME; secure

Set-Cookie 内の個々の属性の説明は以下の通りである。

○NAME=VALUE（必須属性）

識別番号など、ブラウザに保存したい変数名とその値。

○expires=DATE（任意属性）

クッキーの有効期限を表す日付。有効期限に達するとクッキーは PC から消去されるか、もしくは PC からサーバに送信されない。この属性を省略すると一時的なクッキーとなり、ブラウザを閉じた時点で当該クッキーは消去される。

○domain=DOMAIN_NAME（任意属性）

PC がサーバに HTTP リクエストを送るとき、リクエストするサーバ URL のドメイン名と、クッキーの domain 属性との照合が行なわれる。ドメインが後方一致した場合は、さらに path 属性の照合を行い、一致した場合はクッキーを送信する。後方一致とは、例えばクッキーが acme.com という domain 属性を持つ場合に、anvil.acme.com や

---

[18] http://wp.netscape.com/newsref/std/cookie_spec.html

[19] 同仕様書では、クッキーの利用例としてショッピングカート、ID・パスワードの自動入力、サイト表示のカスタマイゼーション等が挙げられている。

shipping.crate.acme.com というサーバ URL に一致することを意味する。

domain 属性で指定されたドメイン内のサーバのみが、当該 domain 属性のクッキーを PC に設置できる。domain 属性で指定するドメインは、"com", "edu", "net", "org", "gov", "mil", "int"という特別なトップレベルドメインを除き、ドメイン名の中に少なくとも 2 つのピリオドを含まなければならない。

domain 属性のデフォルト値は、当該クッキーを含む HTTP を生成したサーバのホスト名である。

○path=PATH

PC がサーバに HTTP リクエストを送るとき、サーバ URL のドメイン名とクッキーの domain 属性との照合が行なわれ、ドメインが後方一致した場合は、さらに path 属性の照合を行い、一致した場合はクッキーを送信する。例えば、/foo というパスは、/foobar や /foo/bar.html に一致する。

path 属性が指定されていない場合は、当該クッキーを含む HTTP ヘッダによって記述されている Web ページと同じパスとみなされる。

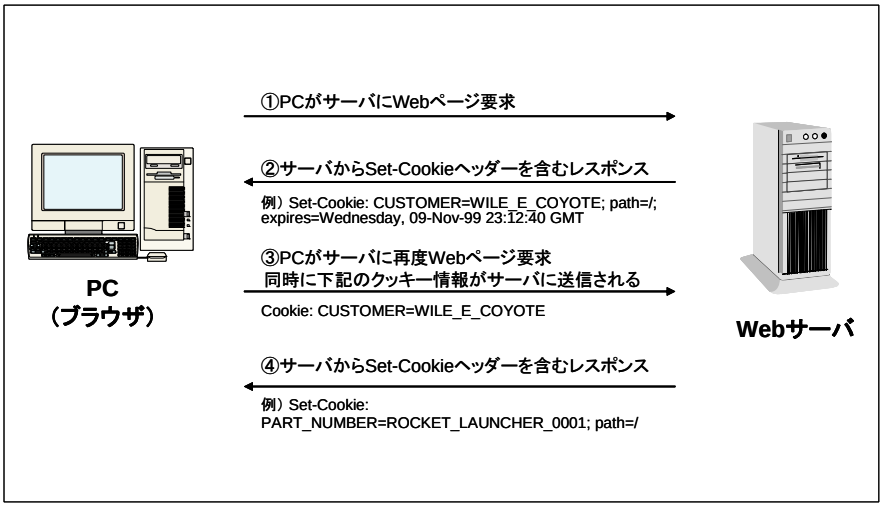
○secure

クッキーが secure と指定されている場合、クッキーはサーバとの通信チャネルがセキュアな場合（HTTPS サーバ等）のみ送信される。

PC はサーバに HTTP リクエストを送るとき、保存している全てのクッキーに対して、リクエストしたサーバ URL を検索する。domain 属性および path 属性が一致した全てのクッキーの name/value ペアが、HTTP リクエストに含まれて送られる。このフォーマットは以下のようなものである。

Cookie: NAME1=OPAQUE_STRING1; NAME2=OPAQUE_STRING2 ...

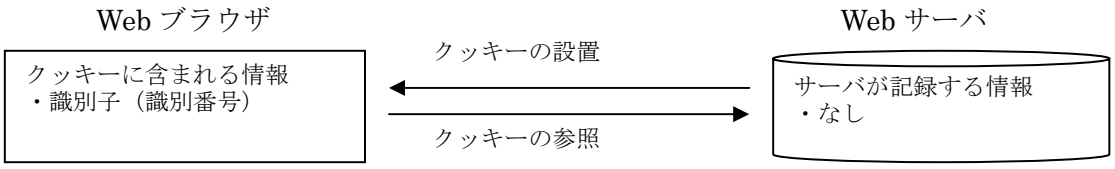
クッキーの送受信例



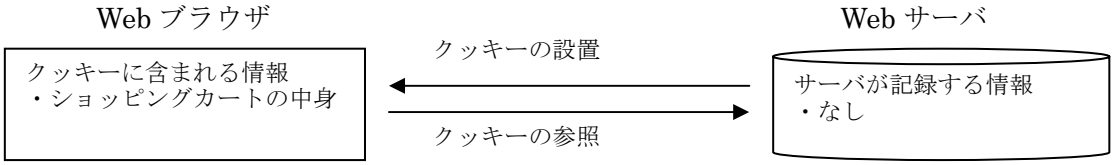
３．１．２ クッキーの一般的な利用方法

a）一時的なクッキー（ブラウザを閉じると当該クッキーは消去される）

①アクセスした利用者のセッション継続管理



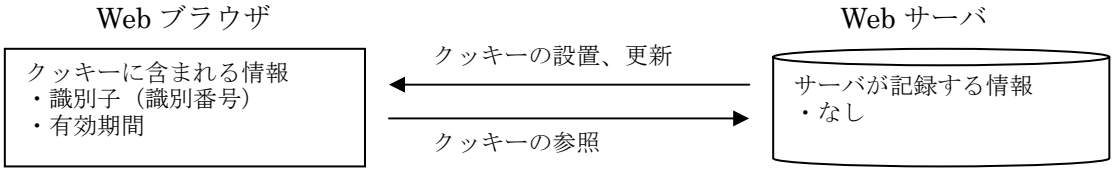
②ショッピングカートの情報を記録する



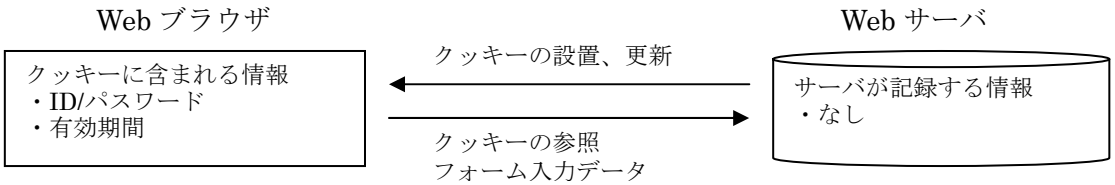
b）持続的なクッキー（サーバが設定した期間、クッキーはブラウザに保管される）

i)非プロファイリング利用（サーバに利用者ごとの閲覧履歴、購買履歴、検索履歴等を記録しない）

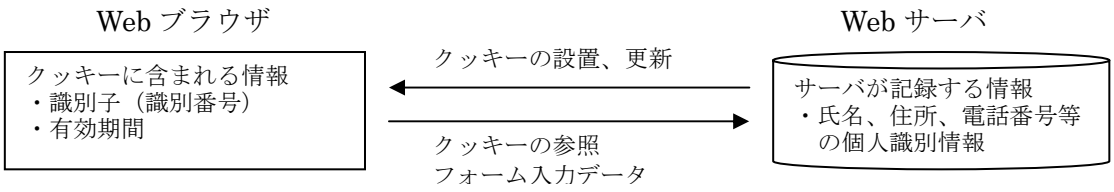
①サイトの利用者数（ユニークオーディエンス）をカウントする



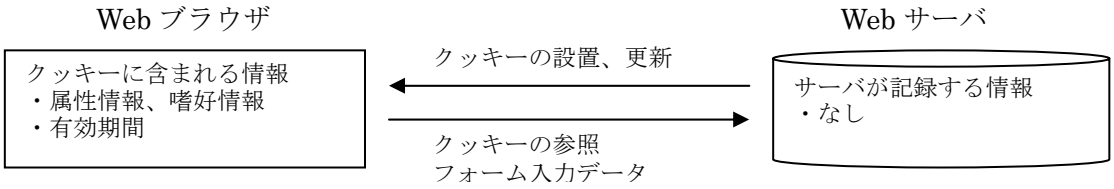
②利用者のログイン名とパスワードを記録する（フォーム自動入力）



③利用者の商品送付先、決済手段等を記録する（フォーム自動入力）

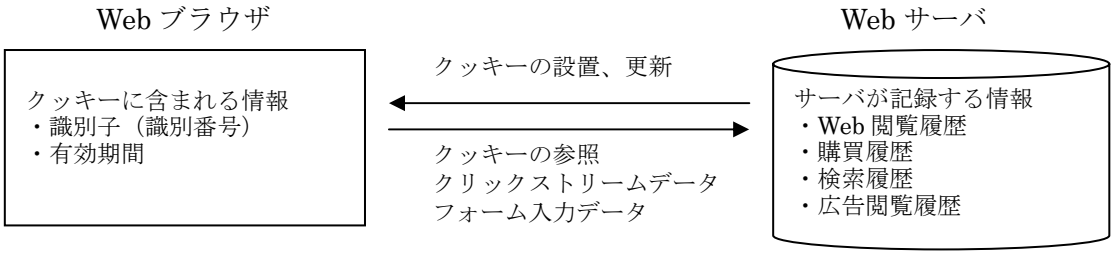


④利用者の属性や嗜好に合わせてコンテンツを表示する



ii)プロファイリング利用（サーバに利用者ごとの閲覧履歴、購買履歴、検索履歴等を記録する）

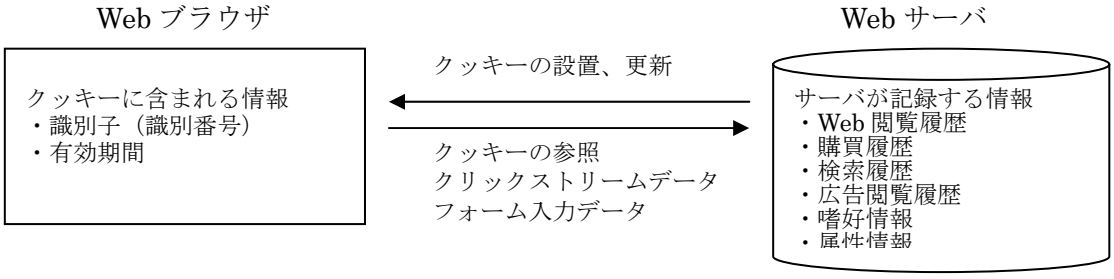
⑤利用者のクリックストリームデータを記録する



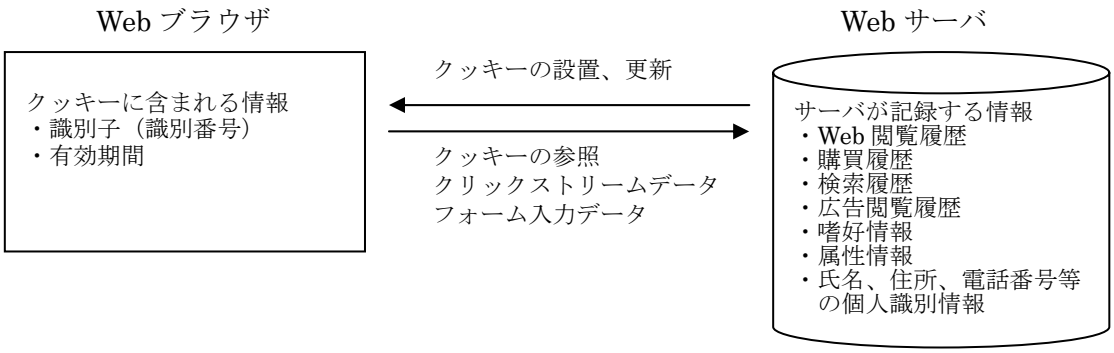
⑥利用者の嗜好を分析・調査する

⑦利用者の嗜好に合わせてコンテンツを表示する

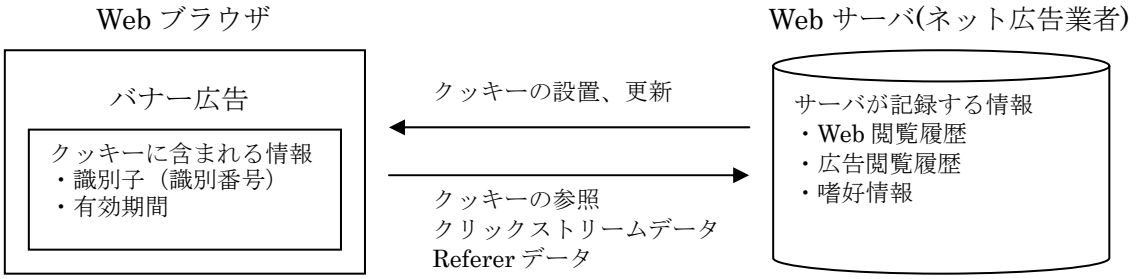
⑧利用者に合わせてバナー広告等の Web 広告を表示する



⑨Web サイトをパーソナライズする



⑩サードパーティー・クッキー



３．１．３ クッキー利用に関するガイドライン

米欧にはクッキー利用に関するガイドラインが数多く策定されている。我が国でも、電子ネットワーク協議会（現（財)インターネット協会）や電子商取引推進協議会により、クッキーに関する項目を含む個人情報保護ガイドラインが策定されている。

各ガイドラインにおけるクッキーに関する項目を抜粋するとともに、各ガイドラインにおける要求事項（利用者へ通知すべき事項）を一覧表としてまとめた。

（1）日本

a）電子ネットワーク協議会「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」（解説付き暫定版、1997 年 12 月）[20]

第５条（個人情報の収集手段）

個人情報の収集は、適法かつ公正な手段により、本人の同意を得た上で行うものとする。

【解説】

本項目において、当然ではあるが、個人情報を収集する際には本人の同意を得た上で

[20] http://www.nmda.or.jp/enc/privacy-tmp.html

行うことを明確にした。
通常、会員登録等を行う際に本人の同意が得られたことを明示する行為としては、書面による申込みの署名押印等、オンライン登録での本人が自己の情報を自分で送信する行為等がある。
しかしながら、現在インターネットにおいては、いわゆる「クッキー[21]」と言われるシステムにより、同意を得ずにウェブサイトへのアクセス履歴のような利用者の個人情報の取得も可能となっている。クッキーを使ったシステムでは、収集目的、収集される情報の内容は、収集される側には不明であり、そもそもクッキーが個人情報等を収集することができることさえも、一般的にはよく知られていない。クッキーに関しては、ブラウザーの警告により受け付けないようにすることが可能ではあるが、クッキーを受け付ければ“同意を得ずにアクセス履歴の取得が可能”というクッキーの性質が、個人情報の保護の観点にそぐわない一面を持っていることを十分考慮する必要がある。
クッキーをホームページ等で使用する際には、例えば“この後のページにはクッキーにより、ＸＸの情報を○○のため□□の期間、収集いたします。”等のようなメッセージを利用者に知らせ、利用の同意を得るような配慮をすることが望ましいと考える。

b）電子商取引推進協議会「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 Ver.2.0」（2004 年 3 月）[22]

（インターネット等の情報ネットワーク上で自動的に個人情報を取得する場合の措置）
第 13 条　インターネット等の情報ネットワーク上でその付随する機能を用いて、本人から自動的に個人情報を取得することとなるときは、その事実と利用目的を通知し、又は公表しなければならない。

（解説）
１．インターネット上では本人の知らない所で個人情報が収集されている場合がある。特に、電子商取引の場面では、クッキーに代表される個人履歴情報収集技術を使って、
（１）訪問者がそのページに何回訪れたかを記録したり、それを表示したりする。
（２）通常モード、フレームモード等、訪問者の好みを記録しておき、次回訪問時にその好みのモードで表示する。
（３）掲示板やチャットで入力したユーザー名を記録しておき、次回訪問時にユーザー名の入力を省略する。
といったことがすでに実施されている。これは本人の知らないところで、本人のパソ

[21] 下線部は筆者による。以下同じ。
[22] http://www.ecom.or.jp/home/privacy_gl/GuideLineV2.pdf

コンのブラウザーの中にクッキーが送信され、また、再度そのページに訪れた際、本人のパソコンから蓄積したクッキーのデータが事業者側のサーバーに自動的に提供される仕組みによるものである。

２．クッキー自体は必ずしも個人情報といい得ないこともあり、またその利用において個人情報として使わないこともあるが、個人を特定する形で利用するクッキーについてはその事実と利用目的を通知又は公表しなければならない。また、本人に対し安心感を与える意味で、クッキーを個人情報として利用しないケースでもその旨をわかりやすく示すことが望まれる。

３．近年その利用が急増しているものの、クッキーの使用を明らかにしている事業者はそれほど多いわけではない。しかしながら、米国において無断でクッキー情報を収集し、第三者提供しようとして問題になったケース等を考え合わせ、クッキーを使用している旨と利用目的について通知又は公表するべきとした。

（２）米国

a）BBBOnLine の「プライバシープログラム適格事項」[23]

プライバシー通知に関する要求事項──プライバシー通知の内容

第 7 条

組織が受動的情報または履歴情報（クッキーや購買履歴など）と、氏名等の個人識別情報とを関連付けている場合、プライバシー通知において、受動的情報または履歴情報を収集していること、それらを個人識別情報や見込客情報と関連付けていること、およびそれらの情報の利用方法について説明しなければならない。

b）TRUSTe の「サイト運営者向けガイド」[24]

3.1.1 情報の収集と利用

クッキー

Web サイトがクッキーを利用する場合、その利用について告知がなされなければならない。その告知文は、クッキーが個人を識別しうる情報と関連付けられるか否かについて言及していなければならない。Web サイトはクッキーが利用される目的について、またそのような利用がどのように利用者にとって有益であるかについて公開しなければならない。クッキーの受取りに関して利用者に選択権があるか否かについて、またクッキーの受取りを拒否した場合の結果について説明せよ。クッキーの受取りが拒否

[23] http://www.bbbonline.org/privacy/threshold.asp

[24] http://www.truste.org/webpublishers/pub_sitecoordinatorsguide.html

された場合、Web サイトへのアクセスは許可されるのか？クッキーの受取りが拒否された場合、Web サイトのいくつかの特徴が正常に機能しなくなるのか？Web サイトに他の Web サイトから広告が配信されている場合、それらの広告はクッキーを含んでいるのか？他の Web サイトからの広告がクッキーを含んでいる場合、それらのクッキーの中には利用者に関する情報が保存されているのか？

c）TRUSTe の「モデル・プライバシーステートメント」[25]

（プライバシーステートメントのモデル事例）
クッキー
クッキーとは、利用者のコンピュータに蓄積される、利用者に関する情報を含んだデータファイルです。[当サイトでは、個人識別情報と関連付ける方法でクッキーを利用することは一切ありません。]当サイトでは、セッション ID クッキーとパーシステント・クッキーの両者を利用します。セッション ID クッキーの場合は、利用者がブラウザを閉じると、クッキーは消去されます。パーシステント・クッキーは小さなテキストファイルで、一定期間の間利用者のハードディスクに蓄積されます。パーシステント・クッキーはインターネット・ブラウザのヘルプファイルの指示に従って、削除することができます。
[クッキーがどのように当サイト上で利用されるか説明します。]当サイトが設置するクッキーによって、利用者は次回の訪問の際にパスワードを打ち込む必要がなくなり、時間を節約することができます。利用者がクッキーを拒否した場合でも、当サイトを利用することができます。ただし、このとき利用者は当サイトの一部のコンテンツを利用できなくなります。例えば、[利用者は当サイトで開催する宝くじやコンテスト、くじ引きに参加できなくなります]。当サイトはまた、利用者の嗜好を追跡し、利用者の嗜好に合わせたコンテンツを提供するためにパーシステント・クッキーを利用します。「プロファイル」セクションを参照ください。
当サイトのいくつかの提携企業は、当サイト上でクッキーを利用しています（例えば、広告企業です）。当サイトが一旦これらの提携企業に広告目的でクッキーの設置を許可した場合、当サイトはこれらのクッキーに対してアクセスしたりコントロールしたりすることはありません。

d）FTC（連邦取引委員会)の議会向け報告書「オンライン･プロファイリングに関する勧告」（2000 年 7 月）[26]

[25] http://www.truste.org/webpublishers/pub_modelprivacystatement.html
[26] http://www.ftc.gov/os/2000/07/onlineprofiling.htm

Ⅱ.公正な情報取扱い及びネットワーク広告イニシアティブの 6 原則

B.プロファイリング

Web ページ上で表示されているバナー広告の多くは消費者が訪問している Web サイトによって選択され配信されているものではなく、多数の Web サイト向けに広告を管理し提供するネットワーク広告業者によって選択され配信されているものである。一般に、これらのネットワーク広告業者は単にバナー広告を供給しているのみならず、それらのバナー広告を閲覧する消費者に関するデータも収集している。ネットワーク広告業者によって収集される情報はしばしば匿名の情報である（すなわち、消費者に関するプロファイルは消費者のコンピュータに保管されたクッキーの識別番号と関連付けられるが、特定の人間の氏名には関連付けられない）が、Web 上の消費者の行動を追跡することで得られるプロファイルが個人識別情報と関連付けられたり、統合されたりする場合がある。この消費者データは、当該消費者のオフラインにおける購買データや、アンケートや登録フォームを通じて消費者から直接収集される情報と結合することも可能である。

このようなプロファイルデータを収集し分析する目的は、広告ネットワークが各消費者の興味や選好に関して多様な推測を行えるようにすることである。結果として、個々の消費者の嗜好、ニーズおよび購買性向を予測することを狙い、また広告業者のコンピュータが一瞬で判断して消費者の興味に直接にターゲットを当てた広告を配信することを可能にする、詳細なプロファイルが出来上がる。それにもかかわらず、ネットワーク広告業者は消費者にとってほとんどの場合、不可視の存在である。訪問している Web サイトが、消費者が見ることができるすべてである。消費者が訪問した Web サイトが広告ネットワークの介在とデータ収集について通知を行わない限り、消費者は自分たちのオンライン行動が監視されていることについて全く認識しないことになるだろう。

D.ネットワーク広告イニシアティブの 6 原則

1.通知

公正な情報取扱いの原則をオンライン・プロファイリングに適用する際に、初めに取り組むべき問題は、一般に消費者は自分たちがプロファイリングされていることについて認識していない現状で、どのように情報取扱いの透明性を確保するかということである。消費者が自分たちの情報が収集されていることを知り、それらの情報がどのように利用されるのかを理解しない限り、情報の収集を許可するか否かについて十分な決定を行うことはできない。透明性は、非個人識別情報および個人識別情報の両者の収集と利用に関わる問題である。ネットワーク広告業者がクッキーを設置したり情報を収集したりしている「ホスト」Web サイト（消費者が訪問している Web サイト）上で、利用者に通知を行ったり選択権を与えることで、十分な透明性は確保される。

ネットワーク広告業者の介在さえ認識していない多くの消費者が、これらの通知と選択権を得るためにネットワーク広告業者のサイトを訪問するとは考えにくいからだ。ネットワーク広告イニシアティブの原則の下では、消費者はネットワーク広告業者によるプロファイリング活動に関する通知と、プロファイリングに参加しないことの選択権とを、「ホスト」Web サイト上で受け取るものとする。個人識別情報がプロファイリング目的で収集される場合は、そのような情報が収集される場所で、そのような情報が入力される以前に、より「強固な」通知が必要とされる。非個人識別情報がプロファイリング目的で収集される場合は、明確で目立つ所にある通知を「ホスト」Web サイトのプライバシーポリシーの中に含めるものとする。ネットワーク広告イニシアティブの原則の下では、同イニシアティブに参加する企業は、「ホスト」Web サイトがこれらの情報開示を行うことを契約にて要求し、このような契約事項の履行を促進する合理的な努力を行うものとする。

e) 米国連邦会計監査院「連邦 Web サイト上のプライバシーポリシーとデータ収集に関する覚書」（2000 年 6 月）[27]

とりわけプライバシーの不安は、Web 技術の利用によって複数のサイトにまたがる利用者の行動を追跡できる場合に、生じるかもしれない。このような不安は、とりわけ政府機関の Web サイトを訪問した個人がそのような追跡活動に関する明確かつ目立つ場所にある通知を与えられない場合に、大きくなる。「クッキー（Web 利用者のハードドライブ上に設置される小さなソフトウェア）」は、このような利用が可能な既存の Web 技術の代表例である。1999 年 6 月に発行されたガイダンスでは、政府機関は明確な通知を行った場合にのみ、「クッキー」またはその他の自動的な情報収集手段を利用することができるとしている。

政府の市民の個人情報へのアクセスに関する特有の法律と伝統のため、「クッキー」が連邦 Web サイトで利用されないということが前提であるべきである。この新たな連邦ポリシーの下で、「クッキー」は連邦 Web サイトで利用されるべきではない。また、受託業者が政府機関の代わりに Web サイトを運営する場合でも、明確かつ目立つ場所にある通知に加えて、以下の条件に適合しない限りは「クッキー」は利用されるべきではない。すなわち、サイト上でデータ収集を行うやむにやまれぬ必要性、「クッキー」を通じて収集される情報の取扱いに対する適切で公開されたプライバシー保護手段、政府機関の長による承認、である。さらに、すべての連邦 Web サイトと受託業者は、子ども向けの Web サイトでのオンラインの個人情報収集に関する 1998 年の児童オンラインプライバシー保護法で規定された標準を遵守しなければならないということが、

[27] http://www.whitehouse.gov/omb/memoranda/m00-13.html

連邦ポリシーである。

米国連邦会計監査院「2002 年の電子政府法のプライバシー条項を実施するためのガイダンス」（2003 年 9 月）[28]における修正

１．追跡技術の禁止

a. 政府機関は、以下のセクション b で規定される場合を除き、訪問者のインターネット上での活動を追跡することを目的として、パーシステント・クッキーまたはその他の方法（例えば、Web ビーコン）を利用してはならない。

b. 政府機関の長は、やむにやまれぬ必要性のためにパーシステントな Web 追跡技術を利用することを承認することができる。利用する場合は、政府機関はプライバシーポリシー内に、以下について明確な通知を掲示しなければならない。

・収集される情報の性質
・情報の利用目的
・情報が第三者提供されるか否か、誰に提供されるか
・収集される情報に適用されるプライバシー保護対策

c. 政府機関は、上記のセクション b で承認されたパーシステント追跡技術の利用について報告しなければならない。

２．禁止されない技術

a. 単一セッション内で訪問者の行動を促進するために利用され（例えば「セッションクッキー」）、持続されない技術は、追跡技術の利用に関する禁止を適用されない。

b. 政府機関の長によって承認され、以下について政府機関のプライバシーポリシーの中に掲示された場合の（訪問者の要求で Web サイトをカスタマイズするための）カスタマイズ技術

・追跡の目的（すなわち、サイトのカスタマイゼーション）
・サイトのカスタマイズの特徴を選ぶことが任意であること
・カスタマイズの特徴を選ばなくても個人はサイトを利用できること
・収集される情報を適切に取り扱うためのプライバシー保護対策

c.情報へのアクセスのためのパスワードの利用（「パーシステント・クッキー」や同様な技術を伴わない）

（３）欧州

a）EU データ保護ワーキングパーティー「ソフトウェア及びハードウェアによって実行されるインターネット上の不可視的かつ自動的な個人データ処理に関する勧告」(1999 年 2 月)[29]

---

[28] http://www.whitehouse.gov/omb/memoranda/m03-22.html
[29] http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp17en.htm

（2004 年 1 月現在リンク切れ）

1.当ワーキングパーティーはソフトウェア業界及びハードウェア業界が、EU データ保護規制に準拠するのに必要な手段を提供する、インターネットプライバシー保護のための製品を開発することを奨励する。
個人データを適法に処理するための一つの条件は、データ主体が当のデータ処理について通知を受け、認識していることである。したがって当ワーキングパーティーは、現状では利用者の認識なしにインターネット上でソフトウェア及びハードウェアによって実行され、利用者に「不可視」な状態にある全ての種類の情報処理に関して、とりわけ懸念を抱いている。
そのような不可視的な処理の典型例としては、HTTP レベルでのやりとり、サードパーティーへの自動的なハイパーリンク、アクティブコンテンツ（Java、ActiveX、その他のスクリプト技術）、及びクッキーが挙げられる。
2.インターネット関連のソフトウェア及びハードウェア製品は、それが収集したり、保存したり、送信したりするデータと、その目的に関する情報をインターネット利用者に提供するべきである。
また、インターネット関連のソフトウェア及びハードウェア製品は、利用者が本人に関するデータに容易にアクセスできる方法を提供するべきである。（中略）
クッキーに関しては、クッキーがインターネットソフトウェアにより受け取られたり、保存されたり、送信されたりとする際に、利用者に通知がなされるべきである。この通知文は、一般人が理解できる言葉で、クッキーに保存される情報の種類、その目的、およびクッキーの有効期間について明示するべきである。

b) EU「電気通信分野に関する個人データ処理とプライバシー保護に関する指令」（1997 年に採択、2002 年 7 月に改定）[30]

同指令は、EU 加盟国に対し 2003 年 10 月 31 日までに同指令を遵守した国内法の整備を義務づけるものである。

第 5 条第 3 項
加盟国は、加入者または利用者の端末機器に情報を蓄積したり、利用者の端末機器に蓄積された情報へアクセスしたりする電気通信ネットワークの利用は、95 年の EU データ保護指令に従う明確かつ包括的な情報、とりわけデータ処理の目的に関する情報を本人が提供された場合、かつ、データ管理者によるそのようなデータ処理を拒否す

[30] http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

る権利が提供された場合にのみ許可される、ということを保証しなければならない。ただし、電気通信ネットワークを通じたコミュニケーションの伝達を実行したり、促進したりするような目的のための技術的な蓄積やアクセスについて、加入者または利用者によって明示的に要求された情報社会サービスを提供するために厳密に必要な技術的な蓄積やアクセスについては妨げてはならない。

同指令の解説ページ[31]では、クッキーについて以下のような説明が行われている。

スパイウェアとクッキー
高度なストレージ能力とオープンソフトウェアを備えた PC と高機能携帯電話によって、利用者は公共のネットワークを通じたコミュニケーションの沢山の新たな可能性を手に入れる。しかし同時に、第三者が端末に蓄積された情報にアクセスしたり、他人の PC 上に自分の情報やプログラムをインストールしたり蓄積したりする沢山の新たな可能性ももたらされることとなる。そのような不可視な形態の侵入の目的は、意図的なファイル・プログラムの破壊（例えばウィルス）とは異なり、情報を盗んだり、著作権違反を検査したり、マーケティングのためにプロファイリングしたり、限定サービスへのアクセス権限をチェックしたり、利用者の嗜好を記録したりすることである。それらの目的のいくつかは完全に無害であったり、利用者にとって有益であったりするが、他の目的は非常に有害かつ脅威であったりする。主たる懸念は、これらのすべてのケースにおいて､利用者は他人が自分の PC にアクセスして情報やプログラムを蓄積しているという事実にほとんど気が付いておらず、そのため利用者はそのような活動をコントロールしたり停止したりする手段を持たないということである。
この問題を改善するために、同指令の第 5 条第 3 項では、利用者の端末機器上の情報にアクセスしたり情報を蓄積したりすることは、利用者がそのような不可視な活動の目的について明確な情報を与えられ、かつ、そのような活動を拒否する権利が与えられている場合にのみ許されるということを要求している。この項は、利用者が自分の端末機器へのどのような形態のアクセスを許し、どのような形態のアクセスを許さないかについて決定することを可能にするものである。
この第 5 条第 3 項は、クッキー（利用者が Web サイトを訪問した際に利用者の嗜好を登録する追跡手段）や、いわゆるスパイウェア（隠された偵察プログラム)、トロイの木馬（メッセージや他の無害に見えるプログラムに隠されたプログラム）に適用される。

31
http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm

（4）プライバシーガイドライン等におけるクッキーに関する要求事項（利用者へ通知すべき事項）の一覧

	(0)クッキーが利用されていること	(1)クッキーにより収集される情報の種類	(2)利用目的	(3)クッキーにより収集される情報の第三者への提供について	(4)クッキーにより収集される情報と個人情報とを関連付けているか否かの説明	(5)クッキーの有効期間	(6)クッキーの受取りを拒否した場合に生じる結果	(7)クッキーに関する一般的説明(クッキーとは何か)	(8)クッキーの受取りを拒否したり、選択的に受け取るためのブラウザ設定の説明	(9)クッキーの削除方法	(10)サードパーティー・クッキーに関する通知	備考
電子ネットワーク協議会「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」	○	○	○	×	×	○	×	○	×	×	×	ガイドライン第 5 条の解説の中で推奨されている事項。
電子商取引推進協議会「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 Ver.2.0」	○	×	○	×	×	×	×	×	×	×	×	
BBBOnLine の「プライバシープログラム適格事項」	○	○	○	×	○	×	×	×	×	×	×	シールプログラムのライセンシーに対する要求事項
TRUSTe の「サイト運営者向けガイド」	○	○	○	×	○	×	○	×	×	×	○	(1)については、Web サイトが利用者のプロファイル（履歴情報）を作成する目的でクッキーを通じて情報を収集している場合には、利用者に通知しなければならないとされている。
TRUSTe の「モデル・プライバシーステートメント」	○	×	○	×	○	○	○	○	×	○	○	シールプログラムのライセンシーに推奨するモデル・プライバシーポリシー中で挙げられた事項
FTC（連邦取引委員会)の議会向け報告書「オンライン･プロファイリングに関する勧告」	―	―	―	―	―	―	―	―	―	―	○	Web 広告業者による利用者の Web 行動の監視行為に対して規制を求めた報告書。 (0)から(9)までは勧告の対象外。
米国連邦会計監査院「連邦 Web サイト上のプライバシーポリシーとデータ収集に関する覚書」	○	○	○	○	×	×	×	×	×	×	×	その他「収集される情報に適用されるプライバシー保護対策」
EU データ保護ワーキングパーティー「ソフトウェア及びハードウェアによって実行されるインターネット上の不可視的かつ自動的な個人データ処理に関する勧告」	○	○	○	×	×	○	×	×	×	×	×	
EU「電気通信分野に関する個人データ処理とプライバシー保護に関する指令」	×	×	○	×	×	×	×	×	×	×	×	

３．２ Web ビーコン

「Web ビーコン」と呼ばれる Web ページ上のタグの利用が一般的になりつつある。Web ビーコンには Web バグ、クリア GIF、アクションタグ等の別名がある。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。 Web ビーコンの作成者は Web ビーコンを通して、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。Web ビーコンの正体は Web ページ上または電子メール上の HTML IMG タグであるが、Web ビーコンの作成者はこのタグの設定で、利用者が当該 Web ページ（や電子メール）を開いた際に、自社のサーバに対して GET 要求を行うようにすることができる。複数の Web サイトの Web ページにこの Bug 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トレースすることが可能なのである[32]。また、大量に送信するダイレクト電子メール上に Web ビーコンを埋め込んでおけば、同メールを開いた消費者の数をカウントすることもできる。さらに、Web ビーコン内にクッキーを含めておけば、クッキーの識別番号を使って利用者の閲覧履歴をトレースすることが可能である。

Web ビーコンは主に Web ページへのアクセス数のカウントや、利用者の閲覧情報の収集のために広く使われており、各企業のプライバシーポリシーの中でもそのような使用法について説明が行なわれている[33]。また、米国のインターネット広告業界団体である Network Advertising Initiative（NAI）は、Web ビーコンの利用に関するガイドラインを公開している[34]。

a）TRUSTe の「モデル・プライバシーステートメント」[35]

（プライバシーステートメントのモデル事例）

Clear Gifs (Web Beacons/Web Bugs)

当サイトでは[あるいは、当サイト上で広告を出す第三者の広告企業では]、どのコンテンツが有効であるかを知ることでサイト上のコンテンツをよりよく管理するために、

---

[32] このとき、Web ビーコンの作成者は GET 要求に含まれる Referer によって、どの Web ページの Web ビーコンから GET 要求が来ているかについての情報を得ることができる。

[33] 例えば、Microsoft 社のプライバシーポリシー http://www.microsoft.com/info/jp/privacy.htm や NEC BIGLOBE のプライバシーポリシー http://www.biglobe.ne.jp/privacy.html

[34] http://www.networkadvertising.org/Release.pdf

[35] http://www.truste.org/webpublishers/pub_modelprivacystatement.html

クリア gif（または Web ビーコン、Web バグ）と呼ばれるソフトウェア技術を使っています。クリア gif は個別の識別子を持つ小さな画像で、クッキーと同様の機能を持ち、当サイトの利用者のオンライン行動を追跡するために使われます。クリア gif とクッキーとの違いは、クリア gif はページ上で不可視であり、文章末尾のピリオドのサイズぐらい非常に小さいサイズであることです。[クリア gif は利用者の個人識別情報と結び付けられます。][クリア gif は利用者の個人識別情報と結び付けらません。]
クリア gif は、コンピュータ上の既存のクッキーと同じサイトから発行されたものである場合、そのクッキーと連携することができます。例えば、ある利用者が www.companyX.com を訪問し、同サイトが広告企業のクリア gif を利用しているとき、同サイト[または広告企業]は広告企業のクリア gif の識別子とクッキーの ID 番号とを照合し、利用者の過去のオンライン行動を把握するかもしれません。こうして収集された情報は広告企業[または同サイト]に提供されるかもしれません。広告企業のクリア gif 利用について詳細を知るためには、○○○のサイトを訪問してください。
さらに、当サイトは、どの email が受信者によって開封されたかを知るために、HTML ベースの email においてもクリア gif を利用しています。これにより、当サイトはコミュニケーションやマーケティングキャンペーンの有効性を評価することができます。利用者がこのような email からオプトアウトしたい場合は、Opt-out ページを参照してください。

b）Network Advertising Initiative（NAI）

NAI のガイドラインでは、「Web ビーコンを利用する場合は、Web サイトでの利用／電子メールでの利用にかかわらず、利用者に通知を行うこと」「利用者への通知には、Web ビーコンを利用していること、Web ビーコンの利用目的、第三者への提供を行う場合はその旨が含まれていること」「個人識別情報が当初に収集された目的と無関係な目的で、第三者に個人識別情報を提供するため Web ビーコンを利用する場合は、利用者に選択の機会を与えること」「第三者に個人識別情報と結び付けられたセンシティブな情報を提供するために Web ビーコンを利用する場合は、利用者から明示的な同意を得ること」と定められている。

３．３ 個別 URL

クッキーや Web ビーコンと同様に、利用者の閲覧履歴情報を収集するための技術手段として個別 URL と呼ばれる方法がある。

これはメールマガジンなど利用者向けの電子メール配信サービスにおいて、商品・サービスなどのリンク先の URL の末尾に利用者個人を識別するパラメータ（ID など）を付加しておくことにより、どの利用者がそのメールを通じてどの商品・サービスにアクセスしたかの履歴を取り、利用者の嗜好に合わせた情報表示等、マーケティングに役立てようと

するものである。

個別 URL の利用については、各企業のプライバシーポリシーにおいて説明がなされつつある状況である[36]。

３．４ スパイウェア

スパイウェアという呼ばれるソフトがネットの世界で蔓延している。このソフトは、利用者の PC 上での様々な操作に関する情報（Web ページアクセス履歴、インストールされているソフトの一覧、その他ハードディスクに記録されている情報等）を収集し、特定の Web サーバに送信する。スパイウェアは、収集された情報に基づき利用者に対してバナー広告を表示したりする。

多くの場合、スパイウェアはネット上のフリーソフト（映像再生ソフトや翻訳ソフト、ファイル共有ソフト等）をインストールする際に同時にインストールされている。フリーソフトの利用条件の中にスパイウェアに関する事項も含まれており、利用者は形式的にはスパイウェアの使用に同意した上でインストールしているのだが、そのことに気がつく利用者は当然に少ない。利用者がフリーソフトを無料で利用できるのも、スパイウェアによる（見たくもない）広告表示を受け入れているからである。

スパイウェアは形式的には利用者の同意を取っているから、一概に違法行為であるとは言えない。しかし、一般利用者が全く気づかない、思いもよらないような方法で個人に関する情報を収集している。スパイウェアに対しては、それらを検知して削除するソフト（Spybot 等）や、スパイウェアが仕掛けられたサイトをブラックリスト化したフィルタリングソフト等の技術的対策がなされているが、そもそもスパイウェアの存在自体知らない利用者も多いため、十分な対策が行われているとは言いがたい状況である。

なお、EU では、上記の EU 指令（「電気通信分野に関する個人データ処理とプライバシー保護に関する指令」1997 年に採択、2002 年 7 月に改定）[37]において、クッキーやスパイウェアを含む不可視のデータ収集手段に対して規制が行われた。事業者には、Web 上でクッキーやスパイウェアを使う場合には、必ずその旨と利用目的とを情報主体に通知し、情報主体が拒否した場合にはいつでもその利用を停止（オプトアウト）することが義務付けられる。

---

[36] 例えば、NEC BIGLOBE のプライバシーポリシー
http://www.biglobe.ne.jp/privacy.html

[37] http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

４．その他の PET（Privacy Enhancing Technology）

本章では、P3P 関連技術以外の PET について整理を行なった。

（１）暗号化ツール

インターネット上で個人情報を送受信する際の通信経路上での盗み見や、個人のコンピュータやファイルへの不正アクセスによる個人情報漏えいを防ぐために、電子メールや通信内容、ファイル等を暗号化するためのソフトウェアである。

・SSL（Secure Sockets Layer）

Netscape によって提唱されている暗号化プロトコル。通信データの暗号化と認証を行なうことにより、データの盗聴や改ざんを防ぐ。主に http 通信の暗号化に利用されている（https）。

・メール暗号化ソフト

電子メール（本文、添付ファイル）の暗号化を行い、途中経路での盗聴を防ぐソフトウェア。

ex. PGP（Pretty Good Privacy）[38]

（２）フィルター

スパムメールやポップアップ広告など、利用者が受信したくない情報を遮断したり、クッキーやスパイウェアなど利用者が気づかぬうちに情報を送信してしまう仕組みやその送信内容等を検出したりするためのソフトウェアである。

・スパムフィルター

発信元や宛先のメールアドレスのブラックリスト、メール本文やヘッダーの特定キーワード等に基づき、スパムメールと判断されるメールを遮断するソフトウェア。

・広告ブロッカー

Web 広告企業の中には、Web 広告を通じて利用者の Web 閲覧履歴をトレースしている所もある。広告ブロッカーは、バナー広告、ポップアップ広告などの Web 広告の表示を遮断するソフトウェア。

ex. Junkbuster[39]

・クッキー管理ソフト

ブラウザがサーバとやり取りするクッキーの内容を確認したり、送受信を管理したりするソフトウェア。

ex. Internet Explorer 6.0 のインターネットオプション

・Web ビーコン検知ソフト

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。

---

[38] http://web.mit.edu/network/pgp.html

[39] http://internet.junkbuster.com/

ex. Bugnosis[40]

・スパイウェア対策ソフト

利用者の PC 上のスパイウェアを検知して、削除するソフトウェア。

ex. Spybot[41]

（3）匿名化ツール

・アノニマイザー

Web ページを閲覧する際に、IP アドレスやコンピュータのタイプ、ブラウザ情報といった情報がサーバ側に送信されることを防ぐためのツールである。プロキシサーバ上に置かれることもある。

ex. Anonymizer[42]

・Anonymous Remailer

電子メールの発信元を匿名化するツール。ニューズグループ等にメールを送る場合、受信者に送信者の名前やメールアドレスを知られないようにする。

ex. Anonymize.net[43]、@nonymouse.com[44]

（4）個人情報管理システム

企業内での適切な個人情報取り扱いをサポートするためのシステム。プライバシーポリシーを企業内のアプリケーションや IT システムに適用し、ポリシーに沿った管理（アクセス管理等）をすることを可能にする。

ex. IBM Tivoli Privacy Manager for e-business[45]

5．今後の課題

本調査で取り上げたクッキーは、もともと Web サイトを訪問した利用者を（匿名のまま）識別するために考案されたものであるが、シンプルな仕組みであるがために様々な手の込んだ応用方法が生み出され、プライバシーの問題が生じることとなった。一方、Web ビーコン、スパイウェアなどはインターネットのブロードバンド化と常時接続化に伴い生じてきた社会現象であるが、これらは露骨に利用者の Web 閲覧履歴などの取得を目的とした仕組みであり、しかも利用者にとって大変気がつきにくい動きをしているため、プライバシ

40 http://www.bugnosis.org/
41 http://beam.to/spybotsd
42 http://www.anonymizer.com/
43 http://www.anonymize.net/
44 http://anonymouse.ws/
45 http://www-3.ibm.com/software/tivoli/products/privacy-mgr-e-bus/

ー問題と捉えられている。また、インターネットとは直接には関係がないため本調査では取り上げなかったが、RFID タグについても本来の使われ方とは別の側面でプライバシー侵害の可能性が指摘され、我が国でも早々とガイドラインが作成されている。

これらの技術についてはすでに識者により問題点が認識され、技術的保護手段やガイドラインなどが整備されつつある。しかし、新たなインターネットのチャネル、例えば携帯電話インターネットの領域ではプライバシーの問題はまだ十分に議論がなされていない。また、氏名、メールアドレス、閲覧履歴といった従来のテキスト形式の個人情報に加え、画像・動画や音声における個人情報、例えばネットワーク監視カメラでの個人情報の流通とプライバシーの問題についても十分な議論はなされていない。

今後も技術進歩と技術の社会への浸透に伴い、新たなプライバシー問題が現れてくるであろう。技術的な対策や、法規制、事業者による自主規制などを通じて、利用者が安心してインターネットを始めとする情報通信技術を利用できる環境を構築していくことが重要である。