L-013

Privacy Policy Manager (PPM) の開発

The Development of Privacy Policy Manager (PPM)

中村 徹† 清本 晋作† 渡辺 龍† 三宅 優†
Toru Nakamura Shinsaku Kiyomoto Ryu Watanabe Yutaka Miyake

1 はじめに

近年ビッグデータの活用、特に個人に関わるデータ(**パーソナルデータ**)の活用が期待されている。一方でパーソナルデータの利用に関しては、プライバシ問題の存在によって活用が妨げられている[1]。現状では、各社が定めるプライバシポリシへ同意を求めることによってプライバシ問題を回避している。しかしながら、2012 年の調査によれば、プライバシポリシを読むユーザは 15%と少数であり[2]、また同年に行われた別の調査によれば、Facebook や Google のプライバシポリシを読んだ被験者のうち、自身のパーソナルデータの取り扱いを正しく理解できたのは 20%程度に過ぎなかった[3]。このように、現状はプライバシポリシが有効に機能しているとは言い難い。また現状では、全ての条件に同意してサービスを利用するか、同意しないで利用しないという選択肢しかユーザに与えられない。ユーザが利用許諾を行った条件に応じて限定されたサービスも提供することによって、ユーザに納得感を与えることが期待できる。さらに EU では「忘れられる権利」[4]が提唱され、データ対象者の請求があった場合に削除が義務付けられる動きがある。現状ではそもそもデータ対象者はどのデータが収集されどのように利用されているか知る手段が限られており、透明性が欠如している問題点がある。

本研究では、信頼のおける第三者機関である **Privacy Policy Manager** (**PPM**)を利用したプラットフォームによって、上記の課題を解決することを目指している[5]。PPM は、各ユーザのパーソナルデータの取り扱いに対する要望を定義する**ユーザプリファレンス**を管理する。PPM はサービス提供者のプライバシポリシと、その利用ユーザのユーザプリファレンスを比較して、各ユーザに適した形式で、データの流通制御やユーザ意思決定支援を行う。本稿では、(1)ユーザプリファレンスに合わせてプライバシポリシを整形することでポリシの理解度を向上する機能、(2)ユーザプリファレンスとプライバシポリシ、及びユーザの選択によってプライバシポリシの限定された範囲のみ同意を行い、範囲に応じたサービスを受けることができる機能、(3)パーソナルデータの利用ログを閲覧する機能、及びデータ利用者に削除申請を行う機能を説明する。

2 PPM のアーキテクチャ

PPM のアーキテクチャは、以下のエンティティによって構成される。図 1 に概要を示す。

・ユーザ：ユーザは PPM を介して、サービス提供者が提供するサービスを利用する。ユーザはユーザプリファレンスを事前に PPM に登録しておく。ユーザプリファレンスは、サービスに提供してもよいパーソナルデータの種類や提供するための条件、及びプライバシポリシの表示法などについて定義する文書である。また、認証は PPM に対して行い、認証結果のみサービス提供者に送られる。サービス利用時などに PPM によって整形されたプライバシポリシを提示され、ポリシに同意することでサービスを利用可能になる。

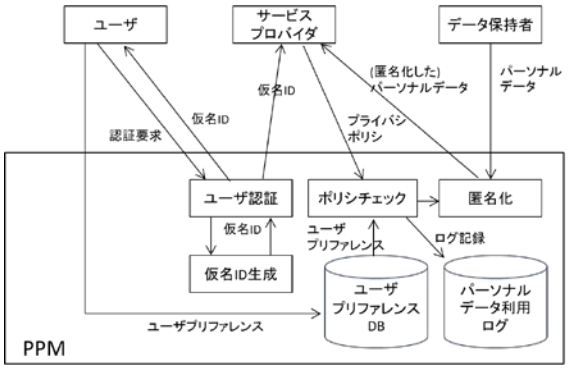

図 1. PPM のアーキテクチャ

・サービスプロバイダ
サービスプロバイダは事前にプライバシポリシを定義しておく。プライバシポリシは、サービスの提供に必要なパーソナルデータの種類や、その利用目的などを定義する文書である。ユーザのサービス利用にあたってプライバシポリシを PPM に提出する。ユーザの承諾した条件に応じたサービスを提供する。

・データ保持者
データ保持者はユーザのパーソナルデータを持ち、PPM を介して他のサービス提供者にパーソナルデータを提供する。データ保持者とサービスプロバイダや PPM が同一のエンティティであることも考えられる。名前や住所、年齢といった属性情報はユーザによる属性情報の登録などによって得られる。サービス利用履歴や位置情報ログなどの履歴情報はサービスの提供に伴って得られる。

・PPM
PPM は以下のモジュールによって構成される。
- ユーザプリファレンス DB
  プライバシポリシ DB はユーザプリファレンスを保管するデータベースである。ユーザプリファレンスを PPM が管理することで、全てのサービスに対して一元的に管理・最適化することができる。
- ユーザ認証
  各サービス提供者に対するユーザプリファレンスを統一的に扱うために、PPM でユーザアカウントとユーザ認証を管理する。
- 仮名 ID 生成
  情報の名寄せを防ぐために、サービス提供者毎に異なる仮名 ID をユーザに付与し、サービス提供者には仮名 ID のみ提供する。

†（株）KDDI 研究所

・ ポリシチェック
ポリシチェックはプライバシポリシとユーザプリファレンスの比較を行う。ポリシチェックは現在のところ、(1)サービス提供者のパーソナルデータに対するアクセス権限の判定、(2)プライバシポリシの表示、(3)サービス提供のための交渉、に利用する。
・ パーソナルデータ利用ログ DB
パーソナルデータへのアクセスがあった場合には、パーソナルデータ利用ログ DB に利用ログを記録する。これにより、ユーザは自身のパーソナルデータの利用状況を後で確認することが可能になる。
・ 匿名化
データ保持者が持つ履歴情報を提供する場合には、必要に応じて匿名化を施す。単純に仮名 ID を削除するだけでなく、k-匿名化などの再識別化を防ぐデータ匿名化手法[6]を利用する。

３実装した機能例

本章では、これまで実装を進めてきた PPM の機能についていくつか紹介する。現在までに、前章で紹介した匿名化以外のモジュールについては実装を終えている。

実装環境について以下に述べる。プライバシポリシ及びユーザプリファレンスについては、機械的に解釈可能にするために XML で記述することとした。図 2 にプライバシポリシ及びユーザプリファレンスの記述例を示す。認証、セッション管理、及び属性の委譲については OpenID Connect[7]の仕様に従った。サービス利用については、ブラウザベースでの利用と Android アプリでの利用が可能である。以下に PPM サーバの実装環境を示す。

・OS: CentOS 6
・DB: MySQL 5.5
・Web サーバ: Apache 2.2
・開発言語: Ruby, Javascript, HTML5

３-１プライバシポリシの整形

プライバシポリシの理解しやすい表記については、例えばカンターライニシアチブで情報共有標準ラベルが検討されている[8]。PPM ではさらに、プライバシポリシをサービス提供者が定めたプライバシポリシに対して、ユーザ毎に異なるユーザプリファレンスに応じて、重要な箇所の強調やそうでない部分の省略などを施すことでより理解しやすい表記に整形する。

３-２同意範囲に応じたサービス提供のための交渉

プライバシポリシとユーザプリファレンスの間で競合が生じた場合には、サービス提供者とユーザの間で交渉を行い、競合を解決する必要がある。本システムでは、サービス提供者から提供するサービスと提供に必要なプライバシポリシのペアがユーザに複数提示され、ユーザは提示されたサービスを選択することで交渉を行う。このときユーザプリファレンスに従って適切と考えられるサービスをデフォルトで表示する。これにより、ユーザの負担を増やすことなく、ユーザの同意した範囲に応じたサービスを受けることができる。

３-３パーソナルデータ利用ログの閲覧及び削除申請

PPM はパーソナルデータそのものを持たないが、サービス提供者がユーザのパーソナルデータにアクセスしようとするときにそれを検知し、ユーザプリファレンスに応じた処理を行う。そのときにサービス提供者からアクセスがあったことをパーソナルデータ利用ログに記録し、ユーザにログを公開する。また、サービス提供者にパーソナルデータの利用を許可する際に、独立したログ ID を付与する。ログの削除は、パーソナルデータ利用ログに含まれる削除したいログを選択し、そのログに付与されたログ ID を指定してサービス提供者に削除申請を行うことで実現する。

４終わりに

本稿では、パーソナルデータ活用に関する課題を解決するプラットフォームである PPM のいくつかの機能の開発について説明した。 今後はデータ匿名化手法に対応した二次利用機能や、サービス提供のための交渉の自動化などの機能拡張を行う予定である。さらに、反応速度やプライバシポリシのユーザ受容度の変化などについて詳細な評価を行う予定である。

謝辞

本研究は独立行政法人新エネルギー・産業技術総合開発機構（NEDO）の委託事業「IT 融合による新社会システムの開発・実証プロジェクト（都市交通分野）都市空間情報と多様なサービスの連携を実現するスマートモビリティシステムの構築に向けた研究開発」として実施して得られた成果によるものである。

参考文献

[1] IT 融合フォーラムパーソナルデータワーキンググループ、“パーソナルデータ利活用の基盤となる消費者と事業者の信頼関係の構築に向けて”、2013 年 5 月 10 日
[2] ネットサービスの利用規約・プライバシー調査　～個人情報漏れ警戒するも、面倒で利用規約を読まない利用者像、明らかに～、http://biz.netmile.co.jp/news/press_2012/press_release120420.html
[3] Survey Finds Facebook and Google Privacy Policies Even More Confusing Than Credit Card Bills and Government Notices, http://www.siegelgale.com/media_release/survey-finds-facebook-and-google-privacy-policies-even-more-confusing-than-credit-card-bills-and-government-notices/
[4] European Commission, April 2010, “A comprehensive approach on personal data protection in the European Union: Right to be Forgotten,” COM(2010) 609 final, Brussels.
[5] Shinsaku Kiyomoto *et al.*, “PPM: Privacy Policy Manager for Personalized Services”, 3rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013), to be appeared.
[6] Latanya Sweeney, "k-anonymity: A Model for Protecting Privacy." International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10.05 (2002): 557-570.
[7] OpenID, http://openid.net/connect/
[8] Joe Andrieu, “The Standard Information Sharing Label”, http://standardlabel.org