個人情報保護に向けた取り組み

高橋　健一
鳥取大学大学院工学研究科情報エレクトロニクス専攻

Researches on the Protection of Personal Information

Kenichi TAKAHASHI
Department of Information and Electronics, Graduate School of Engineering
Tottori University, Tottori, 680-8552 Japan
E-mail: takahashi@eecs.tottori-u.ac.jp

Abstract: A lot of privacy related cases, such as information leakage and phishing scam, have been reported in recent years. In such a situation, the Act on the Protection of Personal Information was enacted in 2005. In 2015, all residents of Japan received a "MyNumber" card on which is printed their individual numbers. Thus, privacy related techniques are the one of most important issues. The classical techniques, such as encryption algorithm, digital signature, are effective to protect privacy related information from malicious third parties, but, not effective against legitimate users, who may cause privacy related cases. In this paper, we introduces some privacy related issues/techniques, especially, our proposed model named "Privacy Protection Model."

Key Words: Computer security, Privacy, Personal Information

１．はじめに

2005年4月に個人情報の保護に関する法律が施行され，2015年10月にマイナンバーが交付されるなど，近年，プライバシに関する興味が高まっている．また，情報漏洩事件[1]やフィッシングサイトなどによる被害[2],サービス提供者による情報の不正利用などが多発している．これらの問題に対して，共通鍵暗号方式や公開鍵暗号方式などの暗号化技術や電子証明書，SSLやTLSのようなプロトコル，また，ウイルス対策ソフトのインストールなどだけで対策することはできない．

そこで，本稿では，コンピュータ・ネットワークセキュリティからの観点でプライバシに関する種々の研究を述べると共に，我々が取り組んでいる個人情報保護モデルについて紹介する．

２．プライバシに関する研究

２．１　プライバシポリシ

インターネットサービスには，利用者から提供された情報をどのように利用するかを示したプライバシポリシ[3]を提供しているサイトが多く存在する．プライバシポリシには，収集する個人情報の利用目的や利用方法などが記されており，これを見ることで利用者はサービス提供者による個人情報の利用方法を知ることができる．しかし，プライバシポリシを多くの利用者が読まないといった問題が存在する．そこで，収集する個人情報の利用方法を利用者に提示するフォーマットとしてP3P（Platform for Privacy Preferences）[4]が提案されている．P3Pは利用者があらかじめ定めた個人情報の利用基準と各サイトのプライバシポリシを比較し，自動的に情報提供の可否を判断する．しかし，プライバシポリシに記述されていることを技術的に保障されているわけではなく，実際にプライバシポリシに反する情報漏えい事件などが発生している．

２．２　トレーサビリティ

RFIDやGPSを用いることで，製品の製造管理や商品のトレーサビリティを確保することや，トラックやバスの位置を確認するといったことが一般的になりつつある．我々の研究室でもバスにスマートフォンを搭載することで，バスの位置情報を取得し，利用者へのバスの現在位置の提示やバスの遅れを考慮したサービス[5]や，画像やiBeaconを用いて人物を追跡するためのシステムを開発し

ている[6]．また，GPS や RFID といった現在位置の情報に頼ることなく，スマートフォンに搭載された 9 軸センサからの情報のみから人物の移動経路が特定できるといった研究結果[7]も報告されている．しかし，一方で，その情報が悪用され，知らない間にその人物の行動が追跡されるといった懸念が生じている．そこで，この対策として，無効化(KILL)機能や可変秘匿 ID を利用した方式などが提案されている [8]．

２．３　情報漏えいの防止

現在，パソコンやスマートフォンに代表される計算機は公私に渡り必須のツールであり，計算機で管理する情報の中には利用者の個人情報だけでなく，学生の連絡先や成績情報など，プライバシに関わる情報を大量に含まれている．このような情報の漏えいの原因の約 7 割は，「管理ミス」と「誤操作」が占めている[9]．このようなリスクへの対策として，計算機内の機密情報の拡散を追跡し，計算機外部への持ち出しを制御する仕組み[10]や正当なアクセス権限を持つユーザによる情報漏洩を防ぐことを目的としたオペレーティングシステムの開発[11]などが行われている．我々もネットワークへの機密情報の拡散を追跡し，外部への持ち出しが発生する場合には警告や制御ができるシステムの実現を目指した研究[12]により一定の成果を得ている．

２．４　匿名化技術

プライバシに関わるデータを加工して個人を識別し難くするための技術として匿名化技術[13]が研究されている．匿名化では，氏名や住所，移動経路といった個人の特定につながる情報に対して，データの置換やランダム化，墨塗りといった加工を行うことで個人の特定を低減する．匿名化の一手法として k-匿名化技術[14]がある．k-匿名化では，同一のデータの組み合わせが k 件以上になるようにデータを加工することで，個人が特定される確率を k 分の 1 以下に抑え，その匿名性を定量的に評価することができる．また，プライバシを保護（匿名化）したまま，複数のデータを組み合わせてデータマイニングすることを可能とするためのプライバシ保護データマイニング技術[15]も研究されている．

２．５　その他

利用者が安心してサービスを利用するための仕組みとして，PPM(Privacy Policy Manager)[16]がある．PPM では，パーソナルデータの取り扱いに関するユーザプリファレンスを管理することによってデータの流通を制御する．また，[17]では開示する情報の粒度を制御することでプライバシを保護することが提案されている．これらにより，利用者の要望にあった情報のみを送信し，その情報のみで利用できる範囲のサービスを利用することが可能となる．しかし，その情報単体で利用者の特定に繋がる情報は守ることができない．また，サービス提供者が必要とする情報も遮断することが可能であるため，サービスの利用に支障を来す可能性がある．また，個人情報を送信しないことにより，悪意のあるアプリケーションから個人情報を守る研究[18]が行われている．この研究では，個人情報の代わりに，アプリケーションルールにより生成した制御コマンドを送信することで情報を保護している．

３．個人情報保護のための枠組み

プライバシに関する種々の研究について述べた．しかし，これらの技術を利用するかどうかは，個人情報を収集する事業者に委ねられており，個人情報を提供するユーザにその決定権はない．例えば，Amazon や楽天などのオンラインショップであれば，初回登録時は住所や氏名，電話番号などを，ログイン時は ID やパスワードなどを提供する必要がある．しかし，これらの個人情報の利用方法はサービス提供者に委ねられており，ユーザにその決定権はない．すなわち，利用者は実際に提供した個人情報がどのように扱われているか知ることができず，また，一度提供した個人情報を保護することもできない．

そこで，個人情報収集者（サービス提供者）と個人情報の提供者（サービスの利用者）が存在する一般的なインターネットサービスの環境を想定し，サービス提供者による収集した個人情報の処理方法を利用者が決めることができる仕組みを提案[19][20]している．

３．１　システムの概要

一般的なインターネットサービスでは，利用者が提供した個人情報はサービス提供者の持つ個人

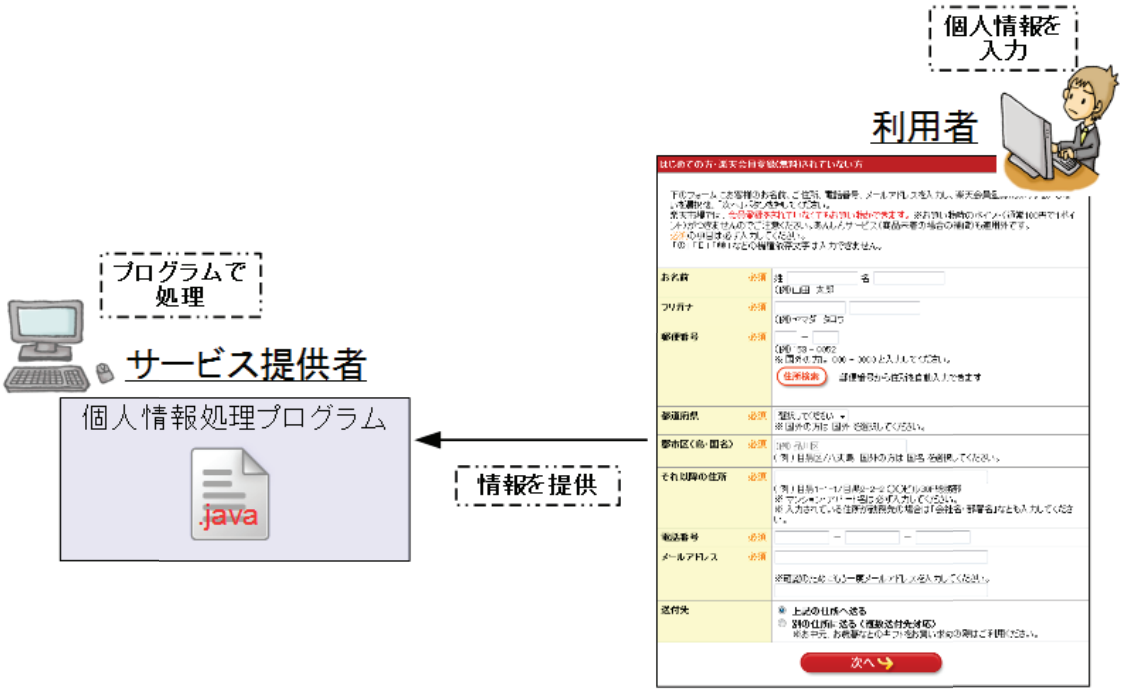

図１．インターネットサービス利用の流れ

情報処理プログラムで処理されている（図１）．そこで，個人情報処理プログラムによる個人情報の処理方法を指定することで，利用者が自身の個人情報の処理方法を決定可能なモデルを提案している．

本モデルでは，サービス提供者の持つ個人情報処理プログラムに利用者が指定した処理方法を適用することで，利用者の意図を個人情報の処理に反映させる．ここで，利用者が指定する処理方法は，サービス提供者の持つ個人情報処理プログラムに適用可能である必要がある．そこで，個人情報処理プログラム中での情報の利用方法を示すための利用ポリシを定義する．利用ポリシにより，利用者は間接的にサービス提供者による個人情報の利用方法を知ることができる．

また，個人情報の処理方法およびプログラムの変換方法を定義した保護ポリシを準備する．利用者は利用ポリシを参照することで，そのプログラムに適用可能である保護ポリシを選択し，サービス提供者に伝える．サービス提供者は保護ポリシに従ってプログラムを変換し，変換後のプログラムで個人情報の処理を行う．これにより，利用者が個人情報の保護方法を決定する．

ここで，一般の利用者にはプログラムに関する知識はないため，保護方法を自身で定義することは難しい．また，信頼出来ない保護ポリシを使用して変換を行った場合，変換後のプログラムがサービス提供者の目的とは違う動作をする（例えば，マルウェアの機能を持つように変換されるなど）危険性がある．このため，保護ポリシは信頼できる第三者機関（TTP：Trusted Third Party）が設置した保護ポリシデータベースで管理されるものとする．TTP が確認した保護ポリシのみを利用することで，このような危険性を排除する．個人情報保護モデルの概要を図２に示す．

４．２　システムの動作の流れ

システムの動作の流れを以下に示す．

１．利用者はサービス提供者にサービスの利用を要求する．
２．サービス提供者は利用者に個人情報の提供を要求する．このとき，サービス提供者は利用者に利用ポリシを送信する．
３．利用者は受け取った利用ポリシにより，保護ポリシデータベースから個人情報処理プログラムに適用可能な保護ポリシを取得する．
４．利用者は保護ポリシに従って個人情報を変換する．
５．変換後，保護ポリシと変換後の個人情報をサービス提供者に送信する．
６．サービス提供者は利用者から受け取った保護ポリシと個人情報処理プログラムを TTP に送信する．

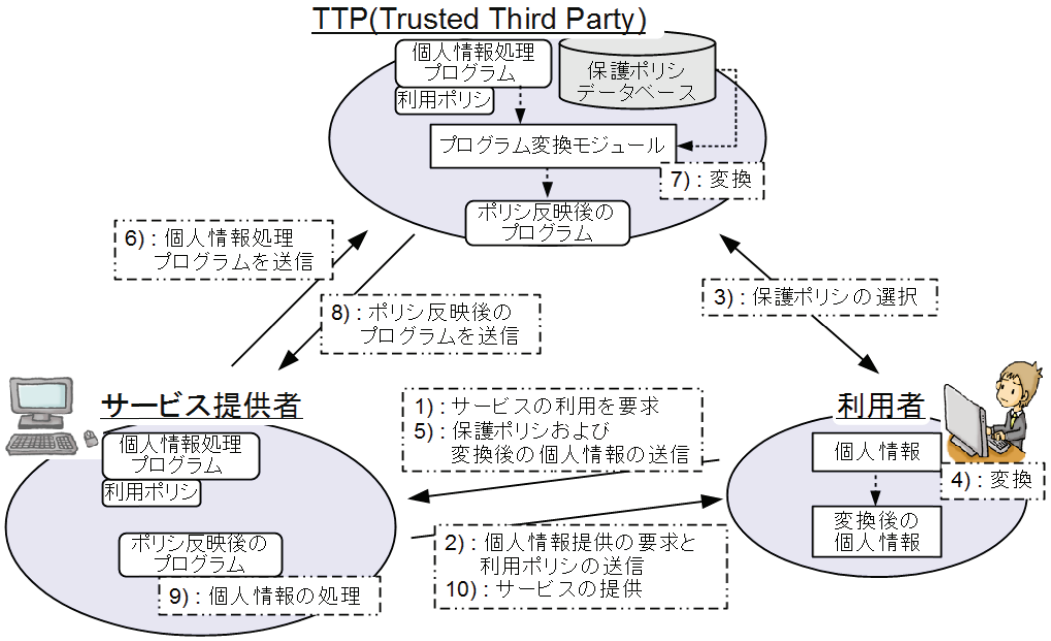

図２．提案システムの概要

７．TTP は受け取った保護ポリシに従ってプログラムを変換する．
８．TTP は変換後の個人情報処理プログラムをサービス提供者に送信する．
９．サービス提供者は，変換後の個人情報処理プログラムを用いて個人情報を処理する．
１０．サービス提供者は利用者にサービスを提供する．

これにより，利用者は自分の指定した方法で個人情報を処理させることができるため，安心してサービスを受けることができるようになる．また，サービス提供者による情報の不正利用や悪意のある第三者からの攻撃に対して利用者の意志で対抗することが可能となる．

４．３　利用ポリシと保護ポリシ

利用ポリシは，
・プログラムでの個人情報の利用方法の確認，
・適用可能な保護ポリシの選択
を可能とするために準備する．

一方，保護ポリシは，
・利用者による個人情報の保護方法の選択，
・個人情報の保護方法（プログラム変換ルール）
を定義するために準備する．これらのポリシは，パーサによる詳細な解析を可能とするために XML 形式で定義される．利用ポリシと保護ポリシの例を図３に示す．

これらのポリシを結びつけることで，保護ポリシが保護対象とする情報とその操作が，プログラム中でどの変数に格納され，どのような操作で処理されるか知ることができる．また，プログラム変換ルールに従ってプログラムを変換することで，ユーザが意図した操作にプログラムを変換する．プログラム変換ルールについては次節で紹介する．

４．４　プログラムの変換

プログラムの変換方法は保護ポリシ内のプログラム変換ルールとして定義され，以下のルールから構成される．

データ変換ルール：データを生成するためのルールを定義する．例えば，暗号化によってデータを保護する場合，暗号化されたデータを生成する必要がある．このようなデータを変換・生成するためのルールを定義する．
操作変換ルール：変換前の情報に対して行われていた処理を，変換後の情報に対してそのまま適用することはできない．そこで，操作を変換するためのルールを定義する．
データ破棄ルール：変換前の情報の利用を制限するためのルールを定義する．

プログラムの変換は，プログラムにこれらのルールを適用することで実現する．ここでは，Java

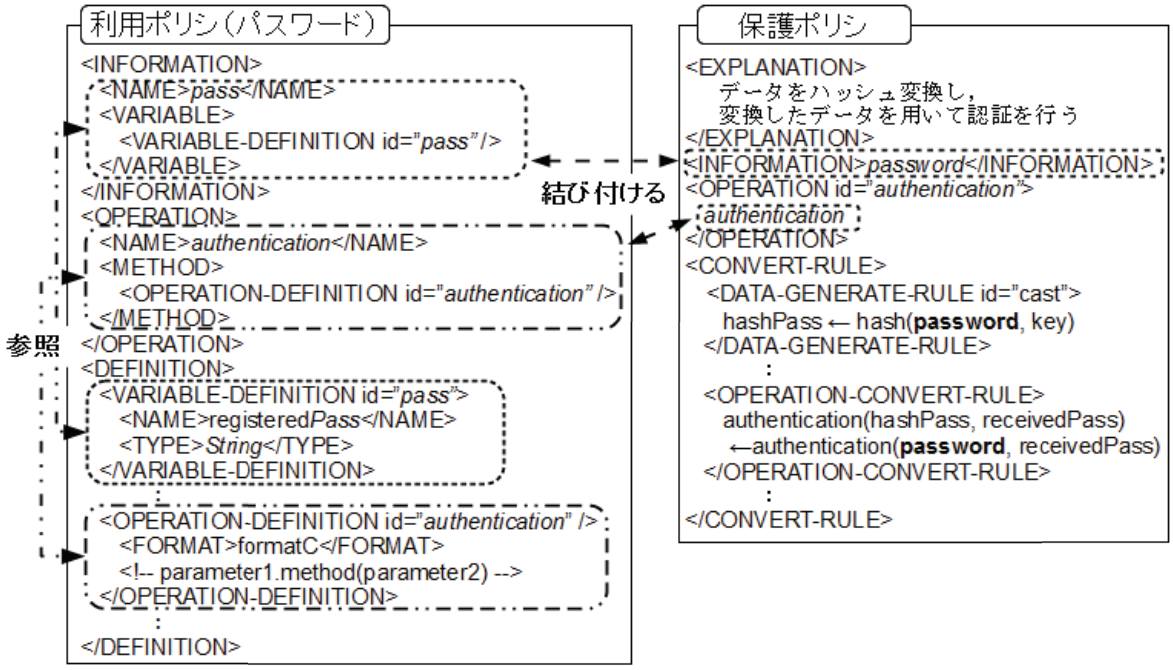

図３．保護ポリシと利用ポリシの例

言語で記述されたプログラムを対象としたプログラムの変換を行うことを想定し，Java のソースコードを解析するために ASTParser を用いる．

ASTParser は Java 言語のソースコードを解析し，抽象構文木（AST:Abstract Syntax Tree）を生成する．抽象構文木とは，ソースコードからコメント文や空行などの実行する際に不要な情報を取り除いたデータ構造のことである．ASTParser により構文解析され，プログラムの各行は変数の宣言文や代入文，ループ文などのように意味付けされる．またその行はさらに字句へと分解され，変数名やメソッド名などのように意味付けされる．これにより，プログラム中でどの変数にどの情報を格納するか，どのメソッドでどの変数を使用するかを解析する．図４に ASTParser によるプログラムの解析例を示す．

プログラムの解析後，プログラム変換ルールを適用する．プログラム変換ルールは複数のルールから構成されており，ルールによっては他のルールにより生成された情報を使用しなければ適用できないものが存在する．例えば，操作変換ルール内でデータ変換ルールにより生成される変数を使用している場合，操作変換ルールを先に適用することはできない．そこで，まずプログラム変換ルールの中から適用可能であるルールを抽出する．その後，ASTParser で解析した結果を元にルールを適用する箇所を検索し，そのルールを適用する．

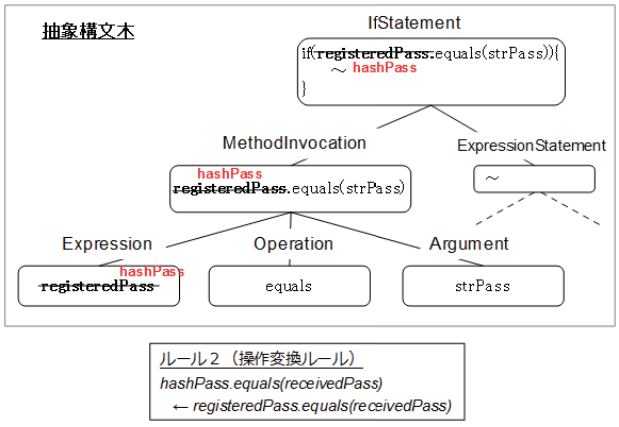

図４．ASTParser による解析例

これを繰り返し，すべてのルールを適用することで，プログラムを変換する．

４．５　実装

プロトタイプ実装したユーザインタフェースを図５に示す．

ここでは，サービス利用時に ID とパスワードを要求するサービス時の画面を示している．左上のフレームには利用ポリシからサービス提供者が要求した個人情報が解析され，保護ポリシを適用可能な情報の一覧が表示されている．各個人情報

図５．ユーザインタフェース

を選択することで，左下のフレームに各情報に適用可能な保護ポリシの一覧が表示される．また，保護ポリシを選択することで，右下のフレームに選択した保護ポリシの詳細が表示される．利用者は，これを確認することで，その保護ポリシを適用するかどうか決定する．最後に利用者が個人情報を入力すると，その情報が保護ポリシに従って変換され，サービス提供者に送信される．変換された情報を受け取ったサービス提供者は，選択されたポリシに従ってプログラムを変換する．その後,変換後のプログラムで個人情報の処理を行う．

生のパスワードを受け取り，パスワード認証に成功したか否かを表示するだけのサービスに対して，ハッシュ変換によりパスワードを保護する保護ポリシを選択したときの結果を図６に示す．

図６．パスワード認証にハッシュ変換した結果

図５を見ると，サービス提供者はハッシュ変換されたパスワードである「54cdc・・・」を受けとっており，かつ，ハッシュ変換されたパスワードで正しくパスワード認証を行えていることが確認できる．

５．　まとめ

本稿では，プライバシに関する研究をいくつか紹介すると共に，インターネットサービスの利用時における個人情報提供への利用者の不安を改善するための手法として，個人情報保護モデルを提案した．

本モデルは，サービス提供者の持つ個人情報処理プログラムでの処理を利用者が指定した処理方法に変換し，変換後のプログラムで個人情報の処理を行う．これにより，利用者は自身の納得できる処理方法で処理を行わせることができるため，安心して情報を提供し，サービスを利用できるようになる．

参考文献

[1] Security NEXT. 情報漏洩事件・事故一覧. http://www.security-next.com/category/cat191/cat25
[2] フィッシング対策協議会. 報告書. https://www.antiphishing.jp
[3] IBM. プライバシー・ポリシーの定義. https://publib.boulder.ibm.com/tividd/td/ITPME/SC23-1284-00/jaJA/HTML/p12plmst

22.htm
[4] W3C. Platform for Privacy Preferences Project. http://www.w3.org/P3P/
[5] 伊藤昌毅，川村尚生，菅原一孔．スマートフォンを利用したバスロケーションシステムの開発，電子情報通信学会論文誌，Vol. J96-D, No. 10, pp. 2327-2339 (2013).
[6] T. Yotsumoto, K. Tanigawa, M. Tsuji, K. Takahashi, T. Kawamura, K. Sugahara. Automatic Human Tracking using Localization of Neighbor Node Calculation, The Ninth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2015), 2015.
[7] 渡邉卓弥，秋山満昭，森達哉．RouteDetector: 9 軸センサ情報を用いた位置情報追跡攻撃，コンピュータセキュリティシンポジウム 2015 (CSS2015), 3B3-2, 2015.
[8] 木下真吾．RFID プライバシ問題と対策技術の研究動向，システム制御情報学会誌，Vol.50, No. 4, pp. 133-139, 2006.
[9] 日本ネットワークセキュリティ協会．2012 年情報セキュリティインシデントに関する調査報告書 ver 1.1.
[10] 田端利宏，箱守聰，大橋慶，植村晋一郎，横山和俊，谷口秀夫．機密情報の拡散追跡機能による情報漏えいの防止機構，情報処理学会論文誌，Vol. 50, No. 9, pp. 2088-2102, 2009.
[11] 鈴来和久，一柳淑美，毛利公一，大久保英嗣．Privacy-aware os salvia におけるデータアクセス時のコンテキストに基づく適応的データ保護方式．情報処理学会論文誌コンピューティングシステム，Vol. 47, No. 3, pp. 1-15, 2006.
[12] A. Maeta, K. Takahashi, T. Kawamura, K. Sugahara. Implementation of Logging for Information Tracking on Network, International Conference on IT Convergence and Security (ICITCS2013), pp. 392-395, 2013.
[13] 高橋賢．パーソナルデータ利活用のための匿名化技術，電子情報通信学会誌，Vol. 98, No. 3, pp. 188-192, 2007.
[14] K. Sweeney. k-anonymity: a model for protecting privacy, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 10 Iss. 5, pp. 557-570, 2002.
[15] 佐久間淳，小林重信．プライバシ保護データマイニング．人工知能学会誌．第 24 巻第 2 号 (2009)
[16] 中村徹，アンドリューA. アダムス，村田潔，清本晋作，高崎晴夫，渡辺龍，三宅優．パーソナルデータ流通基盤：Privacy Policy Manager (PPM) の受容性評価，暗号と情報セキュリティシンポジウム (SCIS2014), 2014.
[17] 宮本崇弘，竹内亨，奥田剛，春本要，有吉勇介，下條真司．プライバシとサービス品質のトレードオフを考慮した個人情報制御機構の提案，第 16 回データ工学ワークショップ (DEWS2005), 6-A-01, 2005.
[18] 田丸修平，岩谷晶子，高汐一紀，徳田英幸．プライバシを考慮したパーソナライゼーションを実現するアプリケーションフレームワーク″．情報処理学会システムソフトウェアとオペレーティング・システム，Vol. 93, pp. 49-56, 2003.
[19] K. Takahashi, T. Matsuzaki, T. Mine, T. Kawamura, K. Sugahara. Protection of Personal Information based on User Preference, International Journal of New Computer Architectures and Their Applications (IJNCAA), Vol. 1, No. 4, pp. 822-834 (2011).
[20] 松永崇秀，高橋健一，川村尚生，菅原一孔．個人情報保護を目的としたフレームワークの提案，コンピュータセキュリティシンポジウム 2015 (CSS2015), 1B4-2, 2015.

（受理　平成２７年１０月２９日）