M-088

Virtual ID システムに対する ID タイプに基づくプライバシー・ポリシーの記述分割

A Method for Partitioning Privacy Policy Definition Based on ID Type for Virtual ID System

百合山 まどか　渡邊 裕治　沼尾 雅之
Madoka Yuriyama　Yuji Watanabe　Masayuki Numao

1．はじめに

近年、企業や自治体は収集した個人情報をプライバシーを尊重しながら扱うことが求められており、個人情報の取り扱いに関する方針をプライバシー・ポリシーとして制定する必要がある。一方個人情報のオーナーは、通常、個人情報を扱うシステムにより一意に識別されるが、仮名によるシステム利用を可能にする仮想的な ID(Virtual ID)が必要になる場合もある。オーナーが実 ID(Real ID)の時と Virtual ID の時では、データ利用者に対して公開する個人情報の量・種類が異なるため、プライバシー・ポリシーの記述に注意を払う必要がある。通常の記述手法では、Virtual ID の追加等の際に手間がかかるが、本稿では追加変更に柔軟に対応できて、管理しやすいプライバシー・ポリシーの記述のため、ID タイプに基づきプライバシー・ポリシーの記述を分割する手法を提案する。

2．プライバシー・ポリシー

2.1　プライバシーを考慮した情報システム

企業や自治体が収集した個人情報を適切に取り扱うためには、まずプライバシー・ポリシーを制定する必要がある。プライバシー・ポリシーには、例えば、誰が、どの個人情報を、どのような目的で利用するのかについて記述しておく。次に、個人情報のオーナーがプライバシー・ポリシーを確認し、同意した上で個人情報を提出することが出来るようにしておく。実際にデータ利用者が個人情報を取り扱うときには、要求されているアクセスがプライバシー・ポリシーに適合するか否かを情報システムがチェックし、適合する場合にのみ個人情報にアクセスできるような仕組みを提供する。

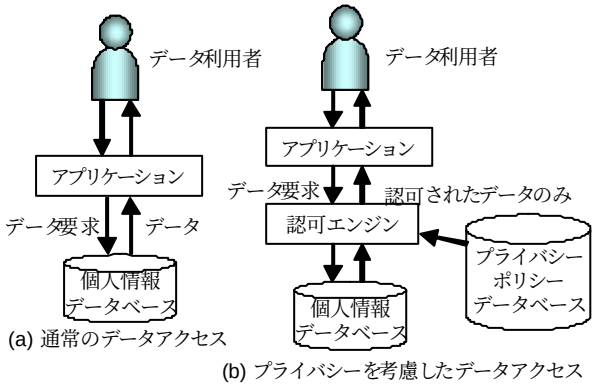

図 1: 個人情報へのデータアクセス

日本アイ・ビー・エム（株） 東京基礎研究所,
IBM Japan, Ltd.　Tokyo Research Laboratory

図 1 に、個人情報へのデータアクセスの例を示す。図 1(a)は、アプリケーションがデータベースからデータを取得し、データ利用者に返す通常のデータアクセスを示す。取得されるデータが個人情報の場合はプライバシーを考慮する必要があるので、図 1(b)のように、アプリケーションと個人情報データベースの間に「認可エンジン」を配置し、アプリケーションが直接個人情報データベースにアクセスするのを防ぐ。認可エンジンは、アプリケーションから要求された個人情報へのアクセスがプライバシー・ポリシーに適合しているかをチェックし、適合していると判断したデータのみアプリケーションに返す†。プライバシー・ポリシーの適合性をチェックすることで、個人情報の不正利用を防ぐことが可能となる。このような認可エンジンの機能、プライバシー・ポリシーの作成・管理と効率よい実施を、支援する製品に、IBM社の Tivoli® Privacy Manager for e-business[1]がある††。

2.2　プライバシー・ポリシーの記述

P3P(The Platform for Privacy Preferences)[2]は Web サイトに関するプライバシー・ポリシーを、XML を用いて機械可読な形式で表現するための規約である。Tivoli Privacy Manager は P3P モデルに基づき、プライバシー・ポリシーを記述する。一つのプライバシー・ポリシーは一つ以上のステートメントを含む。ステートメントは、「データ利用者のグループ」「個人情報のタイプ」「目的」「条件」の 4 要素の組み合わせで表現される。

- データ利用者のグループ：データ利用者が属するグループ
- 個人情報のタイプ：同一のステートメントが適用される個人情報項目名を一つのグループとして表現する。特定の個人情報項目名を示すとは限らず、一つの個人情報のタイプに複数の個人情報項目を関連付けることができる。
- 目的：個人情報アクセスの目的
- 条件：ステートメントが満足されるために上記三つで表現されない付帯条件を示す。上記三つの要素はステートメントに必須であるが、条件は必須ではない。

図 2 に実際のステートメントの例を示す。それぞれ「当社の物流担当者は、お客様が購入された商品を発送する目的で、お客様の名前と住所と電話番号を参照することがあります」「当社のマーケティング担当者は、キャンペーン情報をお届けするダイレクトメールを発送する目的で、同意を頂いているお客様のみ、名前と住所を参照することがあります」という内容を表現している。

† 前者はポリシー判定機能、後者はポリシー執行機能とも呼ばれる
†† IBM, Tivoli は IBM Corporation の商標である

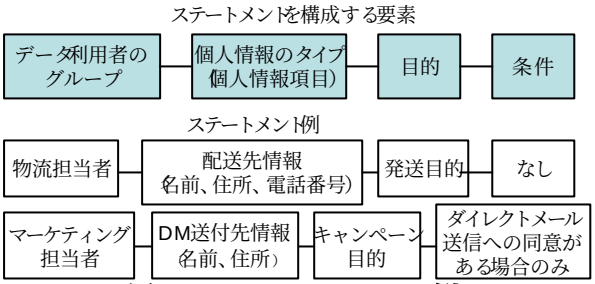

図 2: ステートメントの例

2.3 プライバシー・ポリシーの適合性チェック

プライバシー・ポリシーの適合性チェックの際は、まず個人情報へのアクセスの属性がステートメントで定義されているデータ利用者のグループ、個人情報のタイプ、目的、条件に一致しているかを判断する。ステートメントに条件が複数ある場合は、設定されている全ての条件を満たす必要がある。プライバシー・ポリシーに含まれる一つ以上のステートメントに適合している場合、そのプライバシー・ポリシーに適合していると判断する。プライバシー・ポリシーが複数存在する状況では、全ての関連するプライバシー・ポリシーに適合する場合のみ、適合性チェックを通過し、認可エンジンは個人情報を返す。

3. Virtual ID システムに対するプライバシー・ポリシー

3.1 Virtual ID システム

システムの認証に用いられる一般的な ID（Real ID）はシステム内でユニークに個人が特定されるのに対し、Virtual ID は仮名でシステムに認証される。システムに登録されていて内容が正しいことは証明し、かつ不必要な個人情報を知らせたくないという要求を Virtual ID は可能にする。Virtual ID により、名前などのプライバシー情報をアプリケーションに隠しつつ、一部の属性値のみ（例えば「優良顧客で職業は上場企業役員」など）証明してもらうことが可能になり、個人情報のオーナーは見積や苦情受付アプリケーションなどが利用しやすくなる。

同じオーナーが同じサービスを受ける際も、Real ID を使う場合と Virtual ID を使う場合で参照される個人情報が違う例としては、「Real ID のオーナーが見積を依頼する場合、見積担当者は名前、住所、電話番号、年収を参照し、年収から算出した見積結果を連絡先（名前、住所、電話番号）に通知する。一方、Virtual ID のオーナーが見積を依頼する場合、見積担当者は年収しか参照しないで見積結果を保存し、再び同じ Virtual ID のオーナーから見積結果の取得依頼を受けた場合、見積結果を返す」がある。

3.2 プライバシー・ポリシー記述要件

Real ID の時のオーナーと Virtual ID の時のオーナーでは、同じシステム利用者が同じ目的で同じ個人情報へアクセスを試みてもプライバシー・ポリシー適合性チェックの結果が異なる。また Virtual ID にはタイプがあり、タイプごとにアクセスできる個人情報が異なる。そのためプライバシー・ポリシーでは Real ID と Virtual ID の違いだけでなく、Virtual ID のタイプまで反映させたステートメントを記述する必要がある。

3.3 Virtual ID に対するプライバシー・ポリシー記述

個人情報のオーナーの ID タイプによる、参照可能個人情報の違いをプライバシー・ポリシーで記述する三つの手法を以下に説明する。(1)(2)は ID タイプを反映させてプライバシー・ポリシーを記述する際に、通常用いられると思われる手法で、(3)は本稿で提案する手法である。

(1) ID タイプの違いを「条件」で記述

プライバシー・ポリシーのステートメントにおいて「条件」に、ステートメントの対象の ID タイプを記述することにより、該当 ID タイプにしか適応されないステートメント（「オーナーの ID タイプが Real ID の場合、見積担当者は見積目的で、名前、住所、電話番号、年収を参照し、年収から算出した見積結果を連絡先（名前、住所、電話番号）を参照することがあります」、「オーナーの ID タイプが Virtual ID タイプ A の場合、・・・」）を記述する。同じシステム利用者、同じ目的であってもオーナーの ID タイプが異なれば別のステートメントとして記述する。

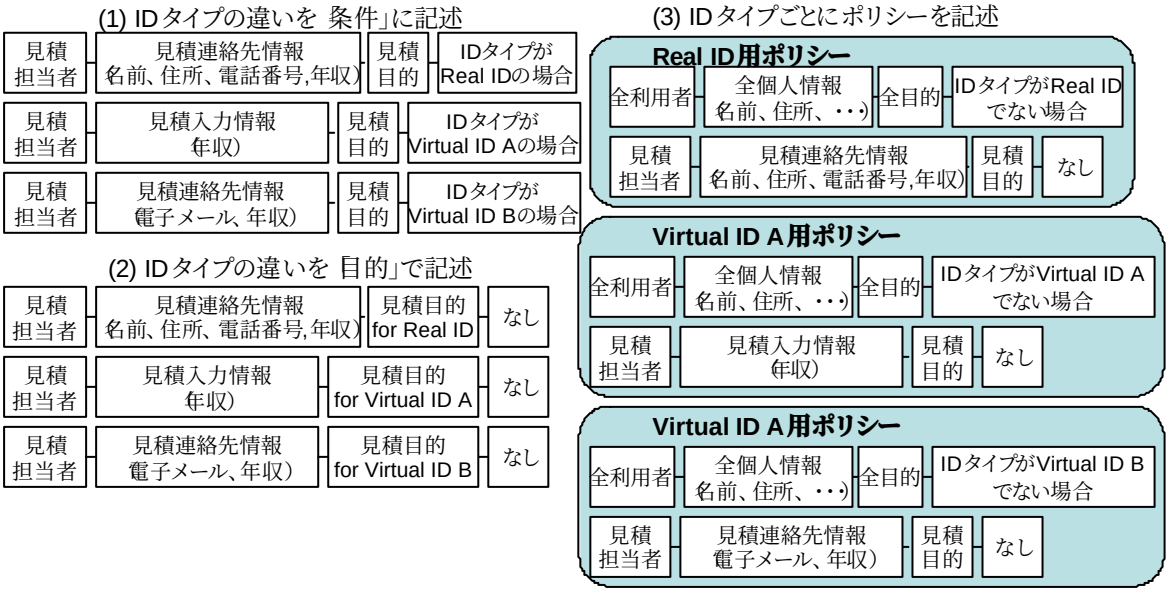

図 3: Virtual ID に対するプライバシー・ポリシー記述例

(2) ID タイプの違いを「目的」で記述
適応する ID タイプを含む「目的」を作成し、該当 ID タイプにしかステートメント（「見積担当者は Real ID 用見積目的で、名前、住所、電話番号、年収を参照し、年収から算出した見積結果を連絡先（名前、住所、電話番号）を参照することがあります」、「見積担当者は Virtual ID タイプ A用見積目的で、・・・」）を記述する。同じ目的であってもオーナーの ID タイプが異なれば別の目的として、ステートメントに記述する。

(3) ID タイプごとにプライバシー・ポリシーを分割
(1)(2)は一つのプライバシー・ポリシーでの記述法だが、(3)は ID タイプごとにプライバシー・ポリシーを分割し、各 ID タイプに対して一つのプライバシー・ポリシーを記述する。それぞれのプライバシー・ポリシーには各 ID タイプごとに適応したいステートメントを記述する。

ID タイプの違いによって、プライバシー・ポリシー適合性チェックを行う認可エンジンが適応するプライバシー・ポリシーを選択する必要がある。もし、認可エンジンを変更できなくて、認可エンジンにおいて適応するプライバシー・ポリシーの選択ができない場合は、各プライバシー・ポリシーの適合性チェック結果が他の ID タイプの場合は常に OK がでるように一つのステートメント「該当 ID タイプ以外では、全てのデータ利用者が全ての目的で全ての個人情報を参照できる」をそれぞれに追加すれば、ID タイプが一致するプライバシー・ポリシーのみ有効に機能する。なぜならば、プライバシー・ポリシー間の適合性チェックの結果は AND ロジックが働くので、該当する ID タイプのプライバシー・ポリシーの適合性チェックを通過しても、他のプライバシー・ポリシーが OK と判定しなければ、総合的には適合性チェックが通過できないためである。もちろん該当する ID タイプのプライバシー・ポリシーの適合性チェックを通過しなければ他のプライバシー・ポリシーの適合性を通過しても、総合的には通過できない。

3.4 考察

各手法の主な長所と短所を表 1 にまとめる。プライバシー・ポリシーの記述を人間がすることを考えれば、(3)の手法が記述・修正・検証のしやすさの点で(1)(2)を上回っているだろう。通常個人情報のオーナーのプライバシー・ポリシーへの同意の上で個人情報を取り扱うので、プライバシー・ポリシーが変更されると新しいプライバシー・ポリシーへの同意をオーナーから収集する必要が生じる。同意の収集は手間がかかるため既存のプライバシー・ポリシーの変更は極力しない方がよい。この点からも(3)の手法が良い。(3)の短所に、管理するプライバシー・ポリシー数が増大することを挙げたが、(1)の条件数や(2)の目的数の増大に較べれば、プライバシー・ポリシー数は少ないため、(3)の手法が勝っていると思われる。

4. おわりに

本稿では、Virtual ID システムに対する ID タイプに基づくプライバシー・ポリシーの記述手法について述べてきた。本手法は、ローカルのデータ利用者グループに対するプライバシー制御とシステム全体でのデータ利用者グループに対するプライバシー制御を合わせたプライバシー制御をするためのプライバシー・ポリシーの記述などにも応用可能である。今後はプライバシー・ポリシーの記述方法に対するパフォーマンス評価を行っていきたい。

謝辞

本研究について御討議いただいた青木義則氏、堂面慶太郎氏に感謝致します。

参考文献

[1] “IBM Tivoli Privacy Manager for e-business v1.1”, http://www-3.ibm.com/software/tivoli/products/privacy-mgr-e-bus/.
[2] “The Platform for Privacy Preferences (P3P) 1.0 Specification”, http://www.w3.org/TR/P3P/, 2002.

表 1: プライバシー・ポリシー記述法の長所・短所

	長所	短所
(1)	・ プライバシー・ポリシーが一つでよい	・ Virtual ID の種類が増える度に既存のプライバシー・ポリシーを変更しなくてはならない ・ 全てのステートメントに ID タイプに対する条件が付加し、条件が多くなるため適合性チェックのパフォーマンスの悪化につながる可能性がある
(2)	・ プライバシー・ポリシーが一つでよい	・ 目的の数が多くなり、管理が大変である ・ Virtual ID の種類が増える度に、新しい目的を作成し、既存のプライバシー・ポリシーに新しいステートメントを追加しなくてはならない
(3)	・ Virtual ID の種類が増えても、既存のプライバシー・ポリシーを変える必要がない ・ プライバシー・ポリシー記述者は条件や複雑な目的を使う必要がないので、比較的簡単にステートメントが作成できる	・ 管理するプライバシー・ポリシーの数が増える