アイデンティティ管理におけるプライバシー属性オントロジを用いた開示属性の分類

Classification of Demanded Attribute with Privacy Attribute Ontology in Identity Management

村上 耕平 ♥ 岩井原 瑞穂 ♦
Gail-Joon Ahn ♠ 吉川 正俊 ♣

Kouhei MURAKAMI Mizuho IWAIHARA
Gail-Joon Ahn Masatoshi YOSHIKAWA

近年，アイデンティティプロバイダに個人情報を蓄積し，サービスプロバイダの要求する個人情報属性を利用者の許可のもとに開示する枠組みが提案されているが，利用者が開示の判断を行うために有用な情報を提供する必要がある．本論文では，プライバシー属性オントロジを構築し，要求されている属性に意味的に近い属性をオントロジの中から検索する手法について考察する．求まった属性に付加された情報から，要求されている属性の重要度を求めることができる．

Recently, several frameworks to disclose service providers user's privacy information , accumulated by the identity providers, are proposed. Within such frameworks, it is necessary to supply useful information for the user to decide whether the disclosure of a privacy attribute should be avoided or not. In this paper, We construct the privacy attribute ontology and propose a method of retrieving attribute from the ontology that has close meaning with the demanded attribute. Pieces of information are appended to each privacy attributes in order to calculate the risk of the disclosure of the attribute.

♥ 学生会員 京都大学大学院情報学研究科修士課程 kmurakami@db.soc.i.kyoto-u.ac.jp
♦ 正会員 京都大学大学院情報学研究科 iwaihara@i.kyoto-u.ac.jp
♠ 非会員 Department of Software and Information Systems, University of North Carolina at Charlotte gahn@uncc.edu
♣ 正会員 京都大学大学院情報学研究科 yoshikawa@i.kyoto-u.ac.jp

1. はじめに

オンラインサービスの多様化とともに，商用サイトのサービス・プロバイダから様々な個人情報の入力を要求されるようになってきている．一方，住所氏名などの煩瑣な入力を効率化するため，個人情報をアイデンティティ・プロバイダに記憶しておき，簡単な操作で情報を開示する枠組みが提唱されている．Liberty Alliance[?] はサービス・プロバイダおよびアイデンティティ・プロバイダの間で Circle of Trust を形成し，信用できる相手に対し開示するものである． Microsoft が提唱しているオープンな規格である Card Space[?](以前は InfoCard と呼んでいた) は，ユーザ個人の端末で個人情報属性をあらかじめ作成したカードに登録しておき，開示要求に対しユーザが適切なカードを選ぶことにより，開示する属性の集合が選択される仕組みになっている．これにより会社など所属する組織に関するアイデンティティなのかあるいは趣味や私生活に関するアイデンティティなのかをユーザが使い分けることができる．また OpenID[?] は，個人の ID として URL 等を利用し認証を行なうサービスの規格であるが，OpenID 属性交換仕様書を用いて名前や住所などどの属性を共有するかをユーザが管理することができる．このような個人情報の開示制御は，例えばソーシャル ネットワークにおいて，本名や顔写真などのプロフィールをコミュニティに 開示するかどうかなど，複雑多様化するネットワーク社会において，自分のアイデンティティやプライバシー情報に関する取扱いポリシーをユーザ自身が設定するという点で重要である．上に述べた標準化動向はいずれも個人情報属性開示の判断をユーザに求めることを基本としているが，ユーザにとって毎回同じような入力を求められるのは煩雑である．また，開示した情報がユーザが予想しなかった形のプライバシー侵害につながることもあり，プライバシー侵害の可能性のある属性開示をシステムが指摘できることが望ましい．

本研究では，個人情報の開示を行なう際に，ユーザに対して，要求された属性の開示に伴うリスクを提供するためのシステムを提案する．具体的には，プライバシー属性オントロジを構築しておき，サービス・プロバイダから要求されている属性の重要度を求める．一般に，個人情報属性の開示範囲をユーザが選択する場合，開示される相手やその信用度に加え，開示する属性が本人に取ってプライバシー性の高いものであるかの精神的苦痛度や，クレジットカード情報など悪用されると経済的リスクのある経済損失度の尺度が考えられる．また，プライバシーに関する個人の考え方や感じ方は多様であり，標準的な重要度を修正して，ユーザごとのプライバシーに関する選好を反映する機能が必要である．このような機能をオントロジに統合することにより，ユーザの開示基準や選好をシステムが把握しておき，ユーザが指定するものに近い開示判断をユーザに提示できることができると考えられる．また，経済的リスクの高い属性が要求されている場合は，それをユーザに警告することが考えられる．

本論文では，提案システムを構築する上での第一段階としてプライバシー属性オントロジを試作し，サービスプロバイダから要求される属性オントロジ内のマッチング手法を提案した．具体的

には，日本ネットワークセキュリティ協会 (JNSA)[?] が提案しているプライバシー属性の 8 つの分類を参考に，プライバシー属性を分類し，特定の Web サイト上で要求されるプライバシー属性をオントロジに加えて，プライバシー属性オントロジを構築した．また，サービスプロバイダから要求される属性とオントロジ内の属性のマッチング実験を行った．

本論文では，次節において関連研究について述べる．その後，第 3 節では提案手法の概要について述べる．第 4 節では，提案システム内で利用するプライバシー属性オントロジについて述べる．第 5 節においては，開示を要求されたプライバシー属性とプライバシー属性オントロジ内の属性のマッチング手法について述べる．第 6 節では，提案システムのプロトタイプについて述べ，第 7 節で評価実験について述べる．最後に本論文のまとめを述べる．

2. 関連研究

近年，情報漏えい事件の多発や被害の深刻化を背景に，Web 上でのプライバシー保護に関する研究が活発に行われている．

プライバシー保護を技術的に実現しようとするアーキテクチャとして P3P が挙げられる．P3P[?] はインターネットを含むネットワーク上のプライバシー保護を目的とした技術標準であり，同標準を用いて Web サイトはプライバシーポリシーを標準化された，機械可読な XML 形式で記述することが出来る．また，ユーザ側では，P3P 対応のクライアントツールまたはブラウザによって，個人情報収集画面において Web サイトのプライバシーポリシーを参照したり，予め登録しておいた個人情報とポリシーを照合して，個人情報を開示するか否かの判断を自動的に行うことが出来る．また，論文 [?] では，google 等の検索サービスと P3P を組み合わせ，P3P の仕組みから取得したプライバシーポリシーからどの程度個人情報を開示するリスクがあるのか判断し，そのリスクを検索結果一覧に表示することが出来る．しかし，本研究は，プライバシーポリシーから個人情報の開示判断を行うのではなく，サービスプロバイダから要求される個人情報の重要度を利用して開示判断を行う点において，これらの関連研究とは異なる．

一方，近年，我が国でも個人情報保護法が施行され，プライバシーの保護に関する研究が盛んに行われるようになってきている．個人情報の分類について，文献 [?] では，プライバシー属性を経済的損失度と精神的苦痛度の尺度でリスク付けし，開示するプライバシー属性の価値を，推定損害賠償額から求める試みが行われている．

オントロジに関する研究も多く行われている．文献 [?] では，二つのオントロジについて，各オントロジの任意の一つのノードを組にして，Jaro-Winkler[?] と WordNet を利用した辞書的類似度，構造的類似度，外延的類似度，からなる類似度計算を行い，高精度なオントロジの統合を実現している．本研究では，この辞書的類似度の算出方法の一部を参考に，要求された属性とオントロジのマッチングを行っている．

3. 提案手法

3.1 本提案の概要

本論文では，サービスプロバイダからプライバシー属性の開示が要求された際に，属性を開示することでユーザがどの程度不利益な影響を受ける可能性があるか考慮し，要求された属性の開示リスクをユーザに提供する手法を提案する．ユーザに開示リスクを提示することで，要求された属性の開示判断を支援する．

3.2 要求事項

サービスプロバイダからプライバシー属性の開示が要求された際に，ユーザに対してそれらの属性の開示リスクを提示するためには，以下の要求を満たす必要がある．

1. サービスプロバイダから開示を要求されるプライバシー属性や，属性の組合わせごとに，潜在するリスクは異なる．例えば「氏名」を Web 上で知られても身元は容易に特定されないが,「氏名」と「住所」が知られると，その人の身元は容易に特定される．また「クレジットカード番号」が知られて悪用されるとき,「氏名」や「住所」と比較して経済的な被害を負うリスクが高いと考えられる．そこで，属性ごとにどのようなリスクが存在するかを保持するデータ構造が必要となる．
2. Web 上で要求されるプライバシー属性には様々なものがあり，未知の属性が要求されたときには，その属性を既存のデータ構造に追加する必要がある．また，未知の属性のリスクも半自動的に推測出来ることが望ましい．
3. ユーザはサービスプロバイダにプライバシー属性を開示する際，Web 上の入力フォームの項目名を確認して属性の記入を行う．このため，入力フォームの項目名を入力に，その属性のリスクを算出する必要がある．

3.3 設計方針

前節の要求事項 (1)(2) のデータ構造は，オントロジの概念階層を利用する．オントロジを利用することで，プライバシー属性をクラスとして分類し，そのクラスの個体に経済的損失のリスクや精神的苦痛のリスクを保持させる．また，オントロジの公理を用いてプライバシー属性の組み合わせクラスを記述することにより,「氏名」と「住所」といった組み合わせに対応するリスクを保持させることが出来る．また，未知のプライバシー属性が要求された場合には，オントロジの既存の属性で概念的に近い属性を算出することで，未知の属性をオントロジに追加し，リスクを推定することが可能になると考えられる．

要求事項 (3) の属性判断に関しては，要求された属性名とオントロジに格納されている属性名の類似度計算を行い，オントロジに格納された中で類似度の高い属性を利用者に提示する．利用者は提示された属性から要求されている属性を選択し，その属性のリスクをオントロジから求めることが可能になると考えられる．そこで，提案システムは次の手順で作成する．

1. プライバシー属性のオントロジの構築
2. 要求された属性とオントロジ内の属性とのマッチング

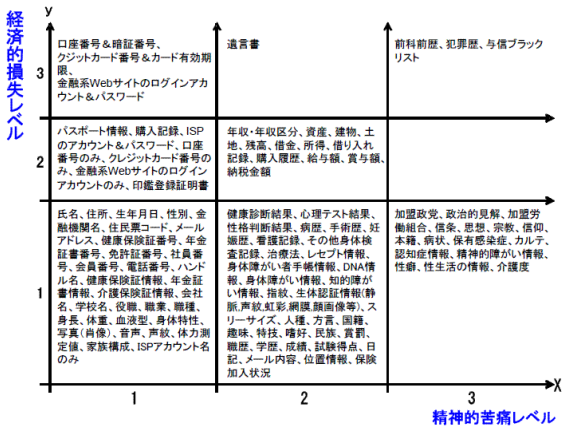

図 1　Simple-EP 図 [?]
Fig. 1　Simple-EP Diagram[?]

4.　プライバシー属性オントロジ

4.1　プライバシー属性オントロジの概要

サービスプロバイダから要求されるプライバシー属性には様々な属性がある．例えば，google が提供する SNS サービスである orkut では「political view」や「sexual orientation」を web 上で入力するフォームが用意されており，要求されたプライバシー属性の情報がプライバシー属性オントロジ内に必ずしも格納されているとは限らない．しかし，要求されたプライバシー属性の近似概念をオントロジから探し出し，その近似概念の近接概念を調べることで，プライバシー属性に関する情報を推定することが出来ると考えられる．このため，本研究ではプライバシー属性に関する情報を格納したオントロジを利用する．

4.2　プライバシー属性の分類

プライバシー属性をオントロジに格納する上で，プライバシー属性を分類する必要がある．そこで，日本ネットワークセキュリティ協会（JNSA）により発行されている ”2006 年情報セキュリティインシデントに関する調査報告書 ”[?] で提案されているプライバシー属性の分類を一部参考にする．

JNSA では,「氏名」「住所」「クレジットカード番号」「本籍」「職歴」など，多種多様なプライバシー属性を以下の 8 つに分類している．本研究ではプライバシー属性オントロジを作成する上で，プライバシー属性の大分類に，この 8 分類を利用する．

- 住民基本四情報
- 身体・健康・医療にかかわる情報
- 思想・宗教・出生にかかわる情報
- 家庭・交友情報
- 個人信用情報
- 社会的・身分にかかわる情報
- ID 情報
- 分類不明情報

4.3　プライバシー属性オントロジの作成

本論文では，サービスプロバイダから要求されるプライバシー属性の情報 (経済的損失度，精神的苦痛度) を求めるために，プライバシー属性オントロジを構築する．プライバシー属性オントロジにおいて「name」「phone number」「address」等のプライバシー属性をクラスを「name クラス」「phone number クラス」「address クラス」といったクラスで表現する．クラスの個体はその属性の経済的損失度と精神的苦痛度を保持する．個体は同一クラスに対して複数用意することもが可能である．例えば，Web 上で利用するユーザ名を複数持っている場合は，保持するユーザ名の数だけ,「User Name クラス」の個体を保持することになる．経済的損失度と精神的苦痛度については，文献 [?] で定められている Simple-EP 図中の値を参考に設定することができる．また個人のプライバシーに対する選好を精神的苦痛度に反映できるようにする．Simple-EP 図を図??に示す.

プライバシー属性オントロジは次の手順で作成する.

1. 一番最上位のクラスには，プライバシー属性一般を表すスーパークラスとして Privacy Attribute クラスを定義する，
2. Privacy Attribute クラスのサブクラスとして，JNSA の 8 つの分類を用意する.
3.「Name」「phone number」「Address」といった個々のプライバシー属性は，8 つの分類クラスの下に，サブクラスとして表現する.
4. 最下層のプライバシー属性で類似した概念があれば,
5. 最上位クラス (Privacy Attribute クラス) と 8 つの分類クラスを除いた全てのクラスについて，各クラスに一つの個体を生成する．この個体は経済的損失度と精神的苦痛度の値を実数値で保持する.

5.　プライバシー属性オントロジのマッチング

5.1　マッチングの概要

サービスプロバイダからプライバシー属性の公開を要求されると，属性がどの程度プライバシー性があり，どの程度経済的なリスクを持つかを調べるために，要求された属性とプライバシー属性オントロジのマッチングを行う．具体的には，要求された属性名とオントロジ内に格納されている個体名の辞書的な類似時計算を行い，マッチングの結果を類似度順でソートし，ユーザに対して表示する.

要求されたプライバシー属性とプライバシー属性オントロジ内に定義される属性間の類似度計算には，辞書的な類似度を示す Jaro-Winkler[?] と，属性間の概念の類似度を示す WordNet::Similarity[?] を利用した.

5.2　辞書的類似度を用いたマッチング

辞書的な類似度を用いたマッチング手法として，Jaro-Winkler を利用する [?]．辞書的類似度 S_{lex} は以下の式で表される.

$$Jaro = \frac{(\frac{m}{str1_length} + \frac{m}{str2_length} + \frac{m-t}{m})}{3}$$

$$S_{lex} = Jaro - Winkler = Jaro + l \times p(1 - Jaro)$$

S_{lex} は [0,1] の値をとる．サービスプロバイダから要求された属性名と，オントロジに格納されているプライバシー属性名全ての組み合わせに対し Jaro-Winkler を計算し S_{lex} を求める．これにより，開示を要求する属性名と辞書的に類似度の高いプライバシー属性をオントロジ内から探し出す．

5.3 概念の類似度を用いたマッチング

WordNet::Similarity[?] では，英語の語彙データベースである WordNet を利用して．2 つの概念の類似度を計算することが出来る．WordNet は概念の階層構造となっており，WordNet::Similarity でも複数の類似度計算手法が提案されている．提案システムでは，WordNet::Similarity の中でも，情報理論的に類似度を導出する Lin Measure を利用して，概念類似度 S_{wns} を求める．S_{wns} は [0,1] の値をとる

5.4 マッチング結果の提示

サービスプロバイダの要求する属性名とプライバシー属性オントロジに格納されているプライバシー属性のマッチング結果は，オントロジ内の全ての属性について，以下のスコアをランキングして，利用者へ提示される．

$$SimilarityScore = W_1 \times S_{lex} + W_2 \times S_{wns}$$

利用者は，提示されたものから，開示を要求されていると考えられる属性を選択する．なお，W_1 と W_2 は重みであり，これを調節することで，マッチングの結果が変化する．

6. 提案システムの概要

本論文では，サービスプロバイダからプライバシー属性の開示が要求された際に，属性を開示することでユーザに対してどの程度不利益な影響を与える可能性があるかを考慮し，ユーザに要求された属性の開示リスクを提供するためのシステムについて提案する．本システムでは，プライバシー属性オントロジを利用し，サービス・プロバイダから個人情報の開示を要求されると，以下の流れでユーザに対して情報開示のリスクを提示する．

1. サービス・プロバイダからプライバシー属性の開示が要求されると，開示を要求されたプライバシー属性名と，オントロジ内に格納されている全てのプライバシー属性名の間で類似度計算を行う．オントロジ内のプライバシー属性が類似度順にソートされたマッチング結果が表示される．
2. ユーザはマッチング結果を見て，オントロジ内で最も類似度の高い属性がサービスプロバイダから要求された属性と同一属性であるか確認する．そうでない場合，マッチング結果のリストから要求されている属性と対応する属性を選択する．
3. 選択されたオントロジ内の属性から，精神的苦痛度と経済損失度を求める．
4. 選択された属性の組み合わせから，本人特定容易度を求める．
5. 求められた精神的苦痛度，経済的損失度，本人特定容易度から，開示する個人情報が漏洩した際の推定賠償額を重要度としてユーザに提示する．

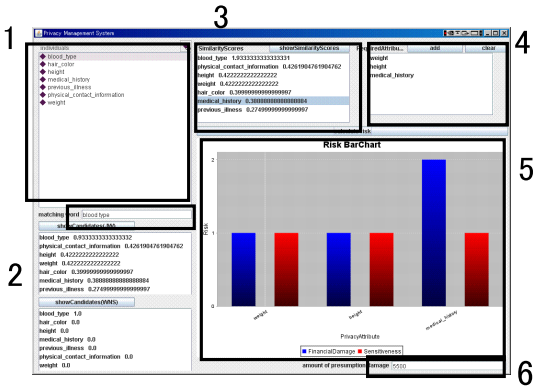

図 2 提案システムの利用画面
Fig. 2 Screen of Proposal System

提案するシステムのプロトタイプを構築した．なお，構築には Java 言語を利用している．提案するシステムの利用画面を図??に示す．図??中の番号の説明は以下のとおりである．

1. プライバシー属性オントロジに格納されているプライバシー属性の個体の一覧が表示される．
2. この記入フォームに要求されているプライバシー属性名を入力するためのテキストボックス．
3. 2 のテキストボックスに入力された属性と，プライバシー属性オントロジに格納されている全てのプライバシー属性の個体との，マッチングの結果が表示される．類似度の高いと判断された個体から順にソートされて結果が表示される．
4. 要求された属性と合致したプライバシー属性が表示される．
5. 要求されたプライバシー属性の精神的苦痛度と，経済的損害度が表示される．
6. 要求された個人情報が漏洩した際に想定される，推定損害額が表示される．

7. 実験

7.1 実験概要

第 4 節で述べたプライバシー属性オントロジの設計手順を元にプライバシー属性オントロジのテストデータを作成し，第 5 節で述べたプライバシー属性のマッチング手法を用いて，実際の Web 上で求められるプライバシー属性が，どの程度の精度でオントロジ内のプライバシー属性とマッチするかについての実験を行った．なお，マッチングはオントロジ内のプライバシー属性名の文字列と，開示を要求されたプライバシー属性名の文字列との間で行うため，要求されたプライバシー属性と同じ文字列を持つ属性がオントロジ内に存在すると，その属性が必ずマッチされることになる．このため，本実験でオントロジのテストデータとしてプライバシー属性名を収集した Web サイトと，要求されるプライバシー属性名を収集した Web サイトは全く異なる Web サイトを利用した．

表 1　実験結果
Table 1　Experimental result

		オントロジ	eBay	PayPal	New York Times	Adobe
1	属性数	186	17	23	14	16
2	オントロジの属性と文字列完全一致	-	7	15	4	7
3	辞書的類似性のある属性	-	3/3	6/6	1/3	5/6
4	3 以外で概念的類似性のある属性	-	3/5	1/2	3/6	1/1
5	対応する相手のない属性	-	2	0	1	2

7.2　実験目的

提案システムでは，サービスプロバイダから要求された属性とオントロジに格納されている属性との間でマッチングを行い，利用者に開示リスクを提示する．その結果，オントロジ内の対応する属性を利用者に提示すること望ましいが，オントロジ内の無関係な属性を利用者に提示すると，利用者がオントロジ内から対応する属性を探し出す手間が発生してしまう．そこで，本実験ではテストデータとして作成したプライバシー属性オントロジが，実際の Web サイトで要求される属性と，どの程度の精度でマッチング可能か評価実験を行う．この実験より，提案したマッチング手法では，プライバシー属性名の文字列間で辞書的な揺らぎや概念的な揺らぎがあるときに，どの程度の精度でマッチさせることが出来るか評価し，改善点を導出することを目的にする．

7.3　オントロジのテストデータ構築

本実験のテストデータとしては，Alexa [1]が公開するページビューランキングにおいて，2008 年 2 月 1 日時点で Top10 である Web サイトにおいてユーザーアカウントを生成する際に，Web サイトから入力を要求されるプライバシー属性名をオントロジに格納した．具体的には，Web サイトの入力フォームの横に表示されている文字列（例えば「First Name」や「Create Your User ID」等の文字列）をプライバシー属性名としてオントロジに格納した．テストデータのオントロジはスタンフォード大学より公開されている ProtegeOWL[?] を利用し，OWL Lite の形式で構築した．構築されたオントロジに格納されたプライバシー属性は 186 属性であった．

7.4　実験対象 Web サイト

本論文では，実験に利用する Web ページとして，eBay.com（オンラインオークションサイト），Paypal.com（インターネットを利用した決済サービス），The New York Times（ニュース配信サービス），Adobe（オンラインストア）を実験対象とした．これらの Web サイトの入力フォームの横に表示されている文字列をサービスプロバイダから開示を要求されるプライバシー属性名として利用した．なお，これらの 4 つの Web ページは前節の Alexa のページビューランキングにおいて Top10 内には入っていないことを付け加えておく．

[1] http://www.alexa.com

7.5　実験方法

辞書的類似度の重み W_1 と概念上の類似度の重み W_2 をともに 1 として，サービスプロバイダから要求される属性とのプライバシー属性オントロジ内のマッチングを行った．マッチングを行った結果，オントロジ内で最も類似度の高いと判断された属性が，要求された属性と同一であると判断できる場合は正解とした．また，もっとも類似度の高いと判断された属性が要求された属性と同一ではないと判断された場合は，ユーザが要求された属性をオントロジ内の属性から探し出す労力が必要となるため，不正解とした．

7.6　実験結果と考察

実験結果を表**??**に示す．eBay では 17 属性，PayPal では 23 属性，NewYorkTimes では 14 属性，Adobe では 16 属性が要求された．表**??**の 2 行目は，要求された属性の中で，オントロジに全く同一の属性名が存在した数を表している．この場合は，文字列が完全に一致するため，対応する属性が確実にマッチングされる．このため，2 列目の結果については考察しない．

3 行目以降では，要求された属性のうち，オントロジ内の属性名と文字列が完全一致しなかった属性のマッチング結果を示している．これらの属性に関しては，事前に人目で，オントロジ内に存在する属性と辞書的な類似性がある属性であるか，概念上の類似性がある属性であるのか，もしくはオントロジ内に対応する属性が存在しない属性であるか分別し，実験結果を示した．3 行目と 4 行目の結果は「マッチングが正解した属性数/人目で分別された属性数」となっている．

3 行目の，辞書的な類似性があると分別された属性におけるマッチング結果について，eBay，PayPal では全ての属性が正解であったが，NewYorkTimes や Adobe では不正解の例もみられた．具体的な正解例として，要求された「Primary Telephone Number」に対して，「Telephone Number」がマッチした例や，要求された「State/Province」に対して「State」がマッチした例が挙げられる．不正解例としては，要求された「Household Income」に対して「Income」がマッチすべき所を，「Home Phone」がマッチした例が挙げられる．

4 行目の，概念上の類似性があると判断された属性に関するマッチング結果は，具体的な正解例としては，要求された「Secret Question」に対して「Security Question」がマッチした例や，要求された「Create your eBay User ID」に対して

「User Name」がマッチした例，要求された「Other Region」に対して「Location」がマッチした例が挙げられる．不正解例としては,「Re-enter Email Address」に「Email Address」がマッチすべき所,「name」がマッチした例や,「Create Acount Password」に対して「thought」がマッチした例が挙げられる．

5 行目の，要求されたがオントロジ内に存在しない属性としては,「ext.」「Year」「Company Size」「Screen Name」が挙げられる．実際にシステムを運用する際には，これらの属性はオントロジ内へ追加することになる．

次に，要求された属性がオントロジ内に存在したが，マッチングの過程で高い類似度を得ることが出来ずに不正解となった属性について考察する．具体例として「Re-enter Email Address」と「Create Account Password」について考える．

Re-enter Email Address に関しては，オントロジ内の EMail address クラス等の属性がマッチされたら正解であった．しかし，はじめに ”Re-enter ”という単語がオントロジ内の Name クラスの属性と高い類似度が算出されたために不正解となった．また Create Account Password については，Password クラスの属性が正解であるのに，類似度計算の結果，Account クラスの属性が最も類似度が高いと判断された．このため，要求された属性名の語数が一定語数以上である際には，後ろの語＝主要語 (修飾を受けている語) として，後ろの語の重みを大きくしてマッチングを行う手法を考えることで，より良好なマッチングを実現出来ると考えられる．一方，Credit Card Number や Expration Date のように，後ろの語（Number や Date）が前の語で意味が変わる場合（例 Telephone Number ,Account Number 等）もある．このときに後ろの語の重みを大きくすると，オントロジ中の対応しない属性を利用者に提示してしまう恐れがある．これに対しては，要求された属性名の語数が一定以上である場合，後ろの語の文字列がどの程度オントロジ内の属性中に出現するか調べ，その出現回数が一定回数以下なら，後ろの語の重みを大きくし，そうでない場合は，後ろの語の重みを変えずに，その一つ前の語に同じ処理を行っていく方法が考えられる．

8. おわりに

本論文では，Web サイトから個人情報の入力を要求される際に，ユーザにプライバシー属性の開示に伴うリスク情報を提供するシステムを提案した．その上で，実際の Web サイトからプライバシー属性オントロジを構築し，実際の Web サイト上で要求される属性とのマッチング実験を行った．今後の課題としては，属性の Web ページでの周辺テキストを利用した精度向上，属性の組み合わせに対する重要度計算方法などが挙げられる．

[謝辞]

本研究の一部は，平成１９年度科研費基盤研究 (B)(課題番号 18300031), および科学技術振興機構 戦略的国際科学技術協力推進事業 「アイデンティティ連携におけるリスクを考慮した個人情報共有方式」による．

[文献]

[1] Liberty Alliance Project:”Liberty Architecture Overview”, 2002

[2] Microsoft Developer Network:”Windows Vista Technical Articles - Introducing Windows CardSpace”, 2006

[3] OpenID Foundation:”OpenID Authentication 2.0 - Final”, 2007

[4] NPO 日本ネットワークセキュリティ協会:”2006 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.02.00”, 2007

[5] Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle;”The Plathorm for Privacy Preferences 1.0”, 2002

[6] Simon Byers, Lorrie Faith Cranor, Dave Kormann, Patrick McDaniel:”Searching for Privacy: Design and Implementation of a P3P-Enabled Search Engine” , PET2004, 2004

[7] Octavian Udrea, Lise Getoor, Renee J.Miller:”Leveraging Data and Structure in Ontology Integration”, SIGMOD’07, June 12-14 2007

[8] William E.Winkler:”The State of Record Linkage and Current Reserch Problems,Technical Report RR/200/06”, Statistical Research Report Series,U.S. Bureau of the Census, 2000

[9] Ted Pedersen:”WordNet::Similarity - Measuring the Relatedness of Concepts”, American Association for Artificial Intelligence, 2004

[10] Holger Knublauch, Ray W. Fergerson, Natalya F. Noy and Mark A. Musen:”The Protege OWL Plugin : An Open Development Environment for Semantic Web Applications”,ISWC2004

村上 耕平 Kouhei MURAKAMI
京都大学大学院情報学研究科修士課程在学中．同志社大学工学部知識工学科卒業．日本データベース学会学生会員．

岩井原 瑞穂 Mizuho IWAIHARA
京都大学大学院情報学研究科准教授．1993 年九州大学大学院工学研究科博士後期課程修了．工学博士．日本データベース学会，情報処理学会，電子情報通信学会，ACM, IEEE 各会員．

Gail-Joon Ahn Gail-Joon Ahn
Dr. Ahn is an Associate Professor of Software and Information Systems Department at UNC Charlotte. Dr. Ahn is an IEEE Senior member and ACM Senior member. And he currently serves as an information director of ACM SIGSAC.

吉川 正俊 Masatoshi YOSHIKAWA
京都大学大学院情報学研究科教授．1985 年京都大学大学院工学研究科博士後期課程修了．工学博士．電子情報通信学会．ACM, IEEE Computer Society 各会員．日本データベース学会理事．