Computer Security Symposium 2020
26 - 29 October 2020

日本語のプライバシーポリシーにおける文脈完全性に基づいた情報抽出の一検討

荒井 ひろみ[1,2,a)]　仲宗根 勝仁[3]　浜本 鴻志[4,1]

概要：サービス提供者がユーザーのパーソナルデータを収集，利用する際に，サービス提供者が利用規約等の説明をユーザーに提示し同意を取得することが一般的に行われている．パーソナルデータの扱い方に関してはプライバシーポリシーとしてユーザーに提示される．しかし一般にプライバシーポリシーはその長さや難解さからしばしばユーザーに正しく読まれないとされている．本研究では，そのようなプライバシーポリシーを巡る状況を考察，改善するため，情報の流れを説明するパラメータをプライバシーポリシーから抽出する方法を検討した．Nissenbaum の文脈完全性の理論に基づき，日本語のプライバシーポリシーに対し情報の流れを明確化するアノテーションガイドラインを構築した．さらに 3 つのプライバシーポリシーの抜粋に対し上述のガイドラインに基づき複数人のアノテーターによるアノテーションを実施した．アノテーション結果から，日本語におけるプライバシーポリシー記述における特徴や問題点を考察した．

キーワード：プライバシー，プライバシーポリシー，文脈完全性

A study of information extraction in Japanese privacy policies based on contextual integrity

Hiromi Arai[1,2,a)]　Katsuhito Nakasone[3]　Koshi Hamamoto[4,1]

Abstract: It is common for the service providers to provide explanations about their services such as terms of consent when they collect personal data from users. Privacy policies provide information about the way the service providers gather, use, and manage the personal information of their users. However, privacy policies are often inappropriately read by users because of their length and complexity. In this research, we examined the method of extracting the parameters of the information flow from privacy policies. Based on Nissenbaum's theory of context integrity, we developed annotation guidelines for information flow extraction for Japanese privacy policies. By using the guideline, annotations were conducted on three Japanese privacy policies. Based on the results, we discuss the characteristics and problems in the description of privacy policies in Japanese.

Keywords: privacy, privacy policy, contextual integrity

1. はじめに

サービス提供者はユーザーのパーソナルデータを収集及び利用する際に，そのデータプラクティスを要約するプライバシーポリシーを作成しユーザーに対する通知を行う．プライバシーポリシーはユーザーやサービス監査者のプライバシープラクティスの適切性の判断に用いられるため，わかりやすくかつ正確に記述する必要がある．

[1] 理化学研究所革新知能統合研究センター
RIKEN AIP
[2] JST さきがけ
JST PRESTO
[3] 大阪大学
Osaka University
[4] 一橋大学
Hitotsubashi University
[a)] hiromi.arai@riken.jp

プライバシーポリシーの記述の正確さについてはその曖昧さ [2], [13], [14] や複雑さ [9] など様々な評価方法が提案されている．また，プライバシーポリシーの適切性については，ユーザーのプライバシーに抵触する部分について正しく伝える必要があるが，不正確なプライバシーポリシーによる問題が度々生じている．特にパーソナルデータの第三者提供等の重要な情報伝達について正しく記載がない場合には社会問題になった事例もある [15]．

プライバシーポリシーにおける情報の流れの記述に着目した際，その適切性を判断する方法の一つに Nissenbaum の文脈完全性 (Contextual Integrity，以下 CI) [5], [6] がある．CI の理論によれば，プライバシーとは情報の流れの適切性の観点から説明されるものであり，その適切性は情報をやり取りする当事者が置かれている文脈によって異なる．例えば，診療の際に情報主体が自身の個人情報を医師に提供する場合プライバシーの侵害にはならないが，情報主体の同意なしに同じ情報が第三者に渡るのはプライバシー侵害になりうる．CI に基づいたアノテーションによるプライバシーポリシーにおける情報の流れの記述の検証方法も提案されており，Facebook 社のプライバシーポリシーにおけるケンブリッジ・アナリティカ事件の前後でのプライバシーポリシーの正確さ及び複雑さの比較検証がなされた [9]．CI の考え方はアンドロイドのパーミッションの検証 [11] などにも応用されている．

日本語で記述されたプライバシーポリシーについての分析は，固有表現の曖昧性等 [13] が実施されている．データの流れについてはデータフローシーケンスで記述されることはあるが，プライバシーポリシーにおける情報の流れについてはあまり議論がなされていない．

本研究では日本語で記述されたプライバシーポリシーにおける CI についての検証を行った．日本語に対する CI のアノテーションルールを開発した．それを用いて実際のプライバシーポリシーに対するアノテーションを実施し，プライバシーポリシーのアノテーションの実施可能性について検証し，正確さや複雑さ，曖昧さについて考察を行った．

2. 関連研究

一般にプライバシーポリシーはユーザーにとって長文で難解であり，理解の妨げになることが様々な調査で報告されている [14]．ユーザビリティーの向上のためにユーザーを支援するさまざまな方法が提案されている [1]．

プライバシーポリシーに対する言語的な分析研究として，コーパスを用いた語彙の抽出・利用 [8] や，ごまかした記述の分析 [3] などが行われている．The Usable Privacy Policy Project (UPPP) [7] ではデータプラクティスやユーザーの選択に関わる語についてアノテーションを実施し，半教師学習による選択の分類を試みている．また，プライバシーポリシーの曖昧性についてタキソノミーに基づいた言明の曖昧さを測る方法が提唱されている [2]．さらに GDPR 試行前後でのプライバシーポリシーの変化傾向についてユーザーによる評価や文章の特徴などから分析，比較がなされている [4]．他に，金森らが個人情報に関わる固有表現の曖昧性の観点からプライバシーポリシーの情報量の分析を行っている [13]．

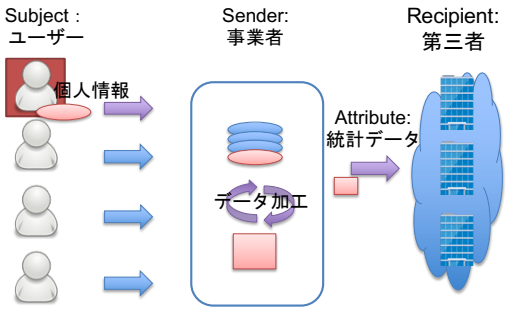

図 1　CI パラメータの模式図

CI の理論は Nissenbaum [5] において提唱された理論であり，プライベートとパブリックの二分法ではなく，情報の流れの適切性の観点からプライバシー侵害を捉えるための理論である．Nissenbaum [6] では情報の流れの記述のためにパラメータの方法が提案され，CI に基づくアノテーションの基本的要素が与えられている．Shvartzshnaider らは CI を用いて英語のプライバシーポリシーを分析する方法を開発した [9]．コンテキストの詳細の欠落，曖昧な言語，および情報の流れの複雑さなどの問題を検出するため，CI のフレームワークに沿ったアノテーションガイドラインを作成し，専門家およびクラウドソーシングによってアノテーションを実施した．実際にアノテーションによって Cambridge Analytica スキャンダルの前後での Facebook のプライバシーポリシーのバージョンを比較したところ，更新されたポリシーには Facebook のデータ収集方法に関しユーザーの理解を制限する曖昧さがまだ含まれていることがわかった．また 17 社からのプライバシーポリシーの 48 抜粋の CI アノテーションをクラウドソーシングし，通常のユーザーがプライバシーポリシーステートメントの次の情報を確実に識別できることを示した．プライバシーポリシーのアノテーション手法には CI の他に Wilson らのものがある [12]．Wilson らは，プライバシーポリシーのメタデータを示す「当事者による収集・利用」や「第三者による収集・利用」などの 10 項目からアノテーションを行った．Wilson らのアプローチは情報の流れそのものを記述しない点で CI のアプローチとは異なる．

3. 手法

日本語で記載されたプライバシーポリシーに対する CI に基づいたアノテーション方法について述べる．まずプライバシーポリシーに対するアノテーションについて CI の理論 [6] 及びアノテーションのケーススタディ [9] を参照

し日本語版のガイドラインを作成し，アノテーションを実施した．また語句の曖昧性についての評価を行った．

3.1 CI フレームワーク

Contextual Integurity に基づいた CI フレームワークは以下の通りである [9]．まず情報の流れ (information flow，flow と略記する) を説明するテンプレートは 5 つのパラメータ

- subject (情報の主体)
- sender (情報の送り手)
- recipient (情報の受け手)
- attribute (情報のタイプ)
- TP (Transmission Principle, 情報のやり取りの仕方)

からなるタプルである．原則として，flow の適切な記述のためにはこの 5 つがすべて指定される必要がある．1 つのパラメータ変化も flow に影響を及ぼし，パラメータの欠損は flow を曖昧にする．図 1 にフレームワークの模式図として，ユーザーから収集された個人情報を事業者が加工し，得られた統計データを第三者提供する場合に，事業者を送信者として見た場合の例を示す．

3.2 プライバシーポリシーのアノテーション

日本語に対するプライバシーポリシーのアノテーション方法について CI の理論 [6] 及びアノテーション [9] をもとに，語句やアノテーション方法の日本語対応を行った．以下のパラメータについての例を用いた解説をガイドラインとした．プライバシーポリシーからそれぞれのパラメータの該当範囲を選択し，対応する組をまとめて flow とした．

SUBJECT 情報の主体．「お客様 (の)」「ユーザー (の)」など．

SENDER 情報を送るまたは共有させる主体．「お客様」，「ユーザー」，「当社」，「第三者」，「開発者」，「他のユーザー」，「提携会社」など．

RECIPIENT 情報を受け取る主体．「お客様」，「ユーザー」，「当社」，「第三者」，「開発者」，「他のユーザー」，「提携会社」など．

ATTRIBUTE 収集されたり，送られたり，受け取られたり，利用されたりしうる情報の種類．「誕生年」や「クレジットカード番号」，「写真」や，より抽象的な「個人情報」や「アカウント情報」，「情報」など．

TP いつ，どのように情報が収集，送受信するかなどの情報のやり取りについて，その仕方を決める条件やどのように情報が利用されるのかなどの利用の方法・目的．「利用する」，「取得する」，「提供する」，「閲覧する」，「送信する」，「登録する」など，情報のやり取りや利用そのものを表す述語に加え，「適切に」，「適法に」，「自動的に」などのように上記の述語に付く表現．「～の場合」や「～に際し」，「～の条件」，「～のため」など，目的・条件や「必要最低限

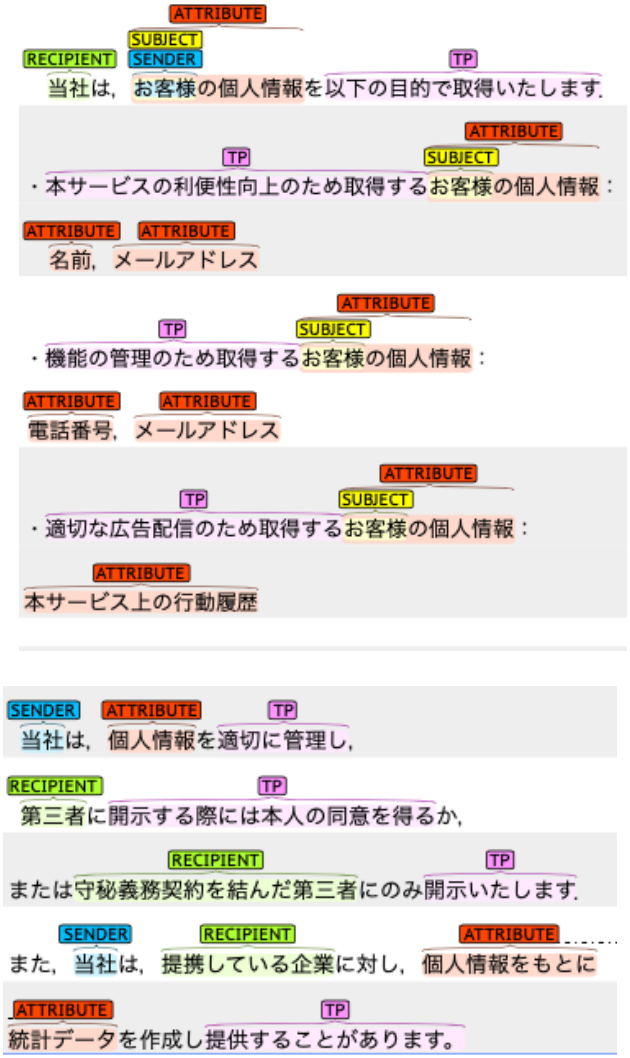

図 2 仮想的なプライバシーポリシーの一部に対する CI パラメータのアノテーション例．上段は情報の流れが整理されて記載された例，下段は情報の流れが不明瞭な例．

(の)」や「個人を特定できない状態（で)」，「非公開（の)」など，ある情報についてその情報の収集・提供のされ方を表す表現も含む．

本研究では，日本語対応のガイドラインの作成を目指すとともに，次の点で先行研究 [9] の方法に改変を与えた．(1) 先行研究では subject のタグ付けが行われなかったが，本研究では subject も含めたタグ付けを行った．(2) タグの重複を認めた．理由として，「お客様からの個人情報の提供」の「お客様」のように subject が同時に sender である例が多数見られたこと，「お客様より収集された個人情報を第三者に提供します」のように一つの文に複数の flow がしばしば現れることなどが挙げられる．(3)TP の説明から示唆されているように，TP は伝達の説明や条件という抽象的な定義であり，またアノテーション範囲について明示されていなかった [6]．英語の場合文が分かち書きされているため文法的要因によるアノテーションの揺れが比較的少ないと考えられるが，日本語は分かち書きでないこと，

助詞があることなどの文法的要因によりアノテーションに揺れが生じる可能性があった．そのため，文法的要因よるアノテーションの揺れが小さくなるよう補足を加えた．(4) 先行研究では「取得する」や「提供する」などの情報のやり取り・利用そのものを表す述語はパラメータに含めずアノテーションが実施されていたが [9]，日本語の場合，動詞の活用に TP の要素が含まれることがあるなどといった文法上の性質に鑑み，本研究ではそれらの述語を TP に含めアノテーションを行った．

アノテーションの例を図 2 に示す．著者らが作成した仮想的なプライバシーポリシーに対し，brat を用いてパラメータのアノテーションを実施した．図 2 の上段は最初の文章に flow が明記され，続く箇条書きに flow の詳細が箇条書きされている．同図の下段においては subject である顧客が明示されておらず，また「開示いたします」の attribute も文脈上理解可能ではあるが明示的に書くべきところが抜けている．「第三者に開示する際には…」「または守秘義務契約を…」の部分に係り受けの不整合があり flow が不明瞭になっていることが見て取れる．

本研究ではアノテーションをプライバシーポリシー全体に実施し，アノテーションされたパラメータから flow の範囲の明確化や，内容の吟味を行った．先行研究 [9] では flow が記載された文章を抜粋しアノテーションが実施されていたが，flow の選定基準について明確には記載されていなかった．本研究ではまずアノテーションを実施し，そこから情報のやり取りとして明確に記述されているものを flow として選定した．flow の選定には，パラメータの組から flow 範囲を決定し，また情報のやり取りとして明確に記述されているものを主に TP から判断した．ここで，TP には主体間の情報のやり取り以外に，個人情報の利用目的や個人情報の処理・加工についての記述などが含まれることがあったため，後者は除外した．例えば，「お客様等の同意をいただいた場合には，当社は提携企業等の第三者に対して個人情報を提供いたします」のような記載は flow とみなす一方「お客様の個人情報はサービス向上のために利用されます」などの個人情報のやり取りそのものに関する記述ではないと解釈できるものは flow としては除外した．

3.3 アノテーション実施方法

アノテーション用文章として，日本語で書かれた 3 社のプライバシーポリシー 3 件について行われた (A，B，C とする)．A，B，C それぞれ 2283 字，1731 字，4227 字であり，A は全文，B は前半部分の抜粋，C はほぼ全文で重複部分のみ削除したものである．

言語学や論理学を学んだ経験のある人文科学系分野の大学院生及び修了生 5 名のアノテーターによって重複してアノテーションを実施した．アノテーションにはテキストアノテーションツールである brat [10] を用いた．

3.4 アノテーションデータの分析

アノテーター間のアノテーションの正確性やアノテーションの解釈の多様性について検証するために同じプライバシーポリシーについて複数のアノテーターによるアノテーションの一致度を評価した．一致度はそれぞれのアノテーションの完全一致および後方一致を取り，一致したアノテーション数で評価した．ここで後方一致を取るのは，同じ箇所にアノテーションをしているにも関わらず修飾部分を含めるかどうかで不一致が生じてしまう事例も緩い一致として拾うためである．例えば「アドレス帳に登録されている氏名」といった場合に，「氏名」「アドレス帳に登録されている氏名」 2 通りのパラメータのアノテーションが考えられる．

またプライバシーポリシーの記述の曖昧さを評価するために，flow におけるパラメータ欠損及び各パラメータにおける曖昧な表現について評価を行った．曖昧な表現について，先行研究 [2] を参照しつつ，各アノテーションされた語彙について曖昧性を生じさせる表現を収集した (表 1 参照)．曖昧性については，Conditionality，Generalization，Modality， Numeric Quantifier の 4 通りの観点から語彙を収集した．

表 1 曖昧な語のリスト

カテゴリー	曖昧な語
Conditionality (C)	選択，適切，必要，場合
Generalization (G)	ほとんど，等
Modality (M)	可能性，ことがある (あります)
Numeric Quantifier (N)	他，一部，多く，ある種，特定，限定

4. 結果と考察

プライバシーポリシーの中からアノテーターが抽出した flow における各パラメータの欠損率と平均出現数は図 3 のようになった．全 flow 数はプライバシーポリシーの抜粋 A,B,C それぞれ 9，13，28 であり，欠損率は 1 つのプライバシーポリシーの抜粋において flow の中にパラメータが一度も出てこない割合である．3 社ともに subject の欠損率が比較的多い傾向にあった．これは，先にも述べた通り subject が自明な場合は省略される傾向にあることが一因である．また，全体的に sender，recipient，subject の平均出現数が少ないのは日本語特有の特徴と考えられ，主語や目的語などを代名詞を用いず省略することがその一因と思われる．特に，sender や recipient はサービス提供者もしくはユーザーであり，文脈から自明な場合に省略される傾向があると考察される．

曖昧な語の出現頻度として，各プライバシーポリシー抜粋ごとの 1 パラメータについての表 1 の単語のいずれかが出現する割合を表 2 に示す．各プライバシーポリシーについて，平均出現頻度が比較的大きいパラメータがそれぞれ

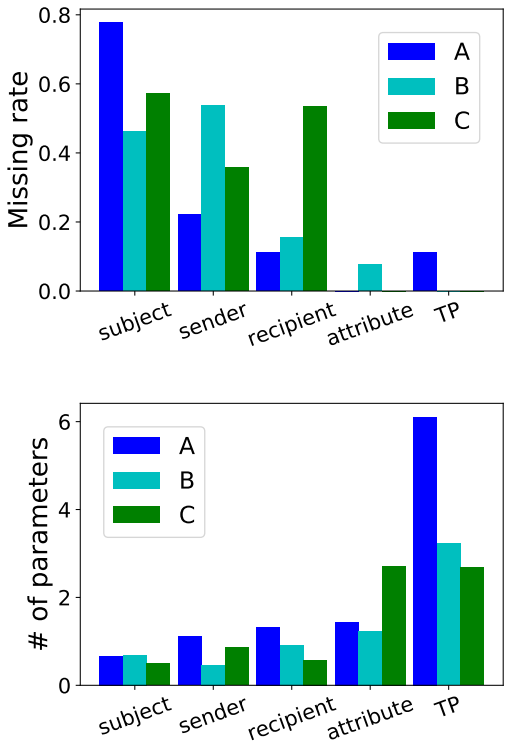

図 3 各プライバシーポリシー内での flow におけるパラメータの欠損率 (上) と平均出現数 (下)

存在する．これは TP なら「適切」「必要」「場合」，sender なら「等」「など」などの多用される曖昧表現の傾向が各プライバシーポリシーに存在するためと考察される．また，いずれのプライバシーポリシーについても曖昧な語が 1 割以上出現するパラメータが複数存在し，文章表現上では情報の流れが曖昧になっていると考察される．

アノテーション結果の品質について，プライバシーポリシー抜粋それぞれについて 5 名のアノテーター中 3 名以上が一致したパラメータの総数は図 4 のようになった．図 3 同様全体的に sender，recipient，subject の数が少ない傾向が見て取れる．また，TP や attribute においては完全一致の場合と後方一致の場合の一致数の差がやや大きいが，これは修飾語を含むかの判断が作業者によって揺れるためと考えられる．例えば，「収集された情報」という表現に attribute をタグ付けする際，「収集された」までを含めて attribute とするか，「情報」のみに attribute とタグ付けするかによって揺れが生じると考察される．

情報の流れの曖昧性について，本研究で実施したアノテーションにおいてはパラメータの欠損や曖昧語の利用という形で曖昧さが観測された．これらの曖昧さが有害かについて考察する．subject の欠損の有害さは場合によると考えられる．自明であるために単に省略された場合は必ずしも有害な欠損とはいえない．例えば，「お客様から収集した電話番号，メールアドレス等の情報は，本サービスへのログイン時の利用者識別等に利用いたします」のように，ログイン時に用いられる電話番号，メールアドレス等

表 2 パラメータごとに含まれる曖昧な語の出現頻度

	A	B	C
subject	0.40	0.08	0.02
sender	0.37	0.03	0.21
recipient	0.25	0.13	0.11
attribite	0.05	0.17	0.28
TP	0.68	0.31	0.34

が，sender たる「お客様」の電話番号，メールアドレスであることは自明である（つまり，subject は「お客様」）．しかし，欠損している情報が自明でないと考えられる場合は有害でありうる．例えば，「お客様の端末のアドレス帳から連絡先情報を取得する場合がございます」など，アドレス帳に含まれる連絡先情報を収集する場合は，subject は sender たる「お客様」だけでなく，アドレス帳に登録されている「お客様」以外の連絡先情報に紐づけられた個人も subject に含まれなければならない．したがって，とりわけ SNS など，ユーザー間のコミュニケーションに関わる事業のプライバシーポリシーにおいては，こうした subject の欠損については留意すべきと考察される．また，ユーザーの個人情報の提供先 (recipient) が「関連する第三者」などの曖昧さが高い表現である場合も情報の流れの曖昧さとしては有害であると考察される．

これらの結果をもとに，CI のフレームワークのアノテーション方法について考察する．英語のプライバシーポリシーについてのアノテーションを実施した先行研究 [9] では，タグの重複について言及されてはいるが，タスクの簡潔さを重視しタグの重複を認めていなかった．しかし，上述したように subject は情報主体を表す重要なパラメータであり，これをアノテーションに加えるにはタグの重複は避けられない．また，subject の問題を度外視しても，やはり正確な flow の明示化のためには一つの表現に複数のパラメータが割り当てられる枠組みが必要である．本研究ではこれらの点からタグの重複を認めるシステムを開発した．アノテーションの実施により，言語に関するスキルの高いアノテーター複数人でのアノテーションを実施したにも関わらずある程度の不一致が存在し，アノテーションガイドラインやパラメータの抽出方法についての改善が必要であることがわかった．CI フレームワークにおいては情報の取り扱いに関する多種多様な条件が TP という単一のタグで処理されおり，プライバシー侵害の評価を行うためにさらなる分類が必要に思われる．例えば，情報の提供や取得のような伝達条件と保管や管理のような利用条件，データ加工についての条件などの分類が可能に思われる．以上の考察は日本語のプライバシーポリシー分析をもとにしているが，特定の言語に拠らず成立するものである．

5. おわりに

本研究において，プライバシーポリシーに対して CI フ

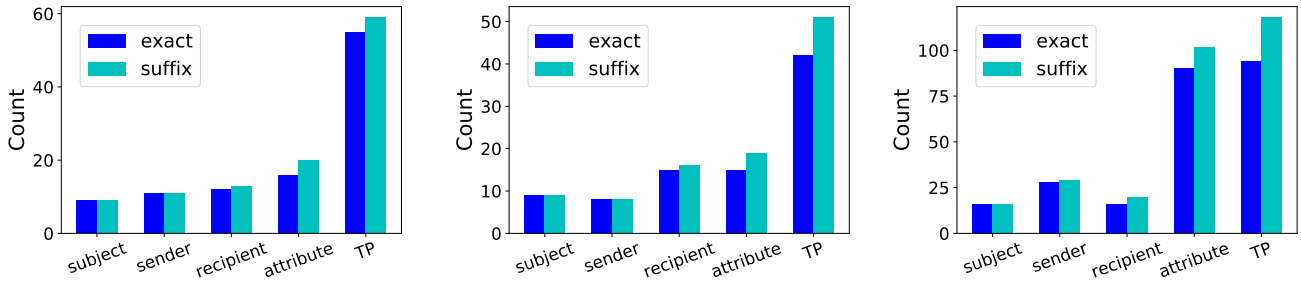

図 4 アノテーションにおけるパラメータの総数の比較（左から順に A，B，C における，青が完全一致，水色が後方一致．）

レームワークを用いて情報の流れを表すパラメータをアノテーションし，プライバシーポリシーにおける情報の流れの記述について検討を行った．結果パラメータの欠損や曖昧表現の利用における情報の流れの曖昧さが観察された．また得られたアノテーションから CI のフレームワークにおいて実際にアノテーションを実施する際に不確定さやゆらぎを生じさせてしまう要因について考察を行った．

今回観測された情報の流れの曖昧さについて，自明であり内容が補完できるパラメータの欠損のような無害なものと，情報の所有，受け取り手などの主体が曖昧になる有害といえるものが混在していた．今後の課題としてこれらの有害性についての検証や，より情報の流れを明確にするプライバシーポリシーの記述方法の検討などが挙げられる．

参考文献

[1] Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M. et al.: Nudges for privacy and security: Understanding and assisting users' choices online, *ACM Computing Surveys (CSUR)*, Vol. 50, No. 3, pp. 1–41 (2017).

[2] Bhatia, J., Breaux, T. D., Reidenberg, J. R. and Norton, T. B.: A theory of vagueness and privacy risk perception, *2016 IEEE 24th International Requirements Engineering Conference (RE)*, IEEE, pp. 26–35 (2016).

[3] Evans, M. C., Bhatia, J., Wadkar, S. and Breaux, T. D.: An evaluation of constituency-based hyponymy extraction from privacy policies, *2017 IEEE 25th International Requirements Engineering Conference (RE)*, IEEE, pp. 312–321 (2017).

[4] Linden, T., Khandelwal, R., Harkous, H. and Fawaz, K.: The privacy policy landscape after the GDPR, *Proceedings on Privacy Enhancing Technologies*, Vol. 2020, No. 1, pp. 47–64 (2020).

[5] Nissenbaum, H.: PRIVACY AS CONTEXTUAL INTEGRITY, *Washington Law Review*, Vol. 79, No. 119 (2004).

[6] Nissenbaum, H.: *Privacy in context: Technology, policy, and the integrity of social life*, Stanford University Press (2009).

[7] Sadeh, N., Acquisti, A., Breaux, T. D., Cranor, L. F., McDonald, A. M., Reidenberg, J. R., Smith, N. A., Liu, F., Russell, N. C., Schaub, F. et al.: The usable privacy policy project, *Technical report, Technical Report, CMU-ISR-13-119*, Carnegie Mellon University (2013).

[8] Sathyendra, K. M., Wilson, S., Schaub, F., Zimmeck, S. and Sadeh, N.: Identifying the provision of choices in privacy policy text, *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*, pp. 2774–2779 (2017).

[9] Shvartzshnaider, Y., Apthorpe, N., Feamster, N. and Nissenbaum, H.: Going against the (Appropriate) Flow: A Contextual Integrity Approach to Privacy Policy Analysis, *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing*, Vol. 7, No. 1, pp. 162–170 (2019).

[10] Stenetorp, P., Pyysalo, S., Topić, G., Ohta, T., Ananiadou, S. and Tsujii, J.: brat: a Web-based Tool for NLP-Assisted Text Annotation, *Proceedings of the Demonstrations Session at EACL 2012*, Avignon, France, Association for Computational Linguistics (2012).

[11] Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D. and Beznosov, K.: Android permissions remystified: a field study on contextual integrity, *Proceedings of the 24th USENIX Conference on Security Symposium*, pp. 499–514 (2015).

[12] Wilson, S., Schaub, F., Dara, A. A., Liu, F., Cherivirala, S., Leon, P. G., Andersen, M. S., Zimmeck, S., Sathyendra, K. M., Russell, N. C. et al.: The creation and analysis of a website privacy policy corpus, *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pp. 1330–1340 (2016).

[13] 金森祥子，佐藤広英，太幡直也，　野島良：プライバシーポリシーの固有表現の曖昧性と情報量による分類，Vol. JSAI2020 (2020).

[14] 金森祥子，　野島良，　岩井淳，川口嘉奈子，佐藤広英，諏訪博彦，太幡直也：プライバシーポリシーを読まない理由に関する一考察，コンピュータセキュリティシンポジウム 2017 論文集，Vol. 2017, No. 2 (2017).

[15] 工藤郁子，荒井ひろみ，江間有沙：採用におけるプロファイリング・サービスの倫理的課題，人工知能学会全国大会論文集，Vol. JSAI2020 (2020).