

# 特許検索における 質問意図の曖昧化

中川研 胡 瀚林

指導教員：中川 裕志 教授

2017 年 1 月 31 日

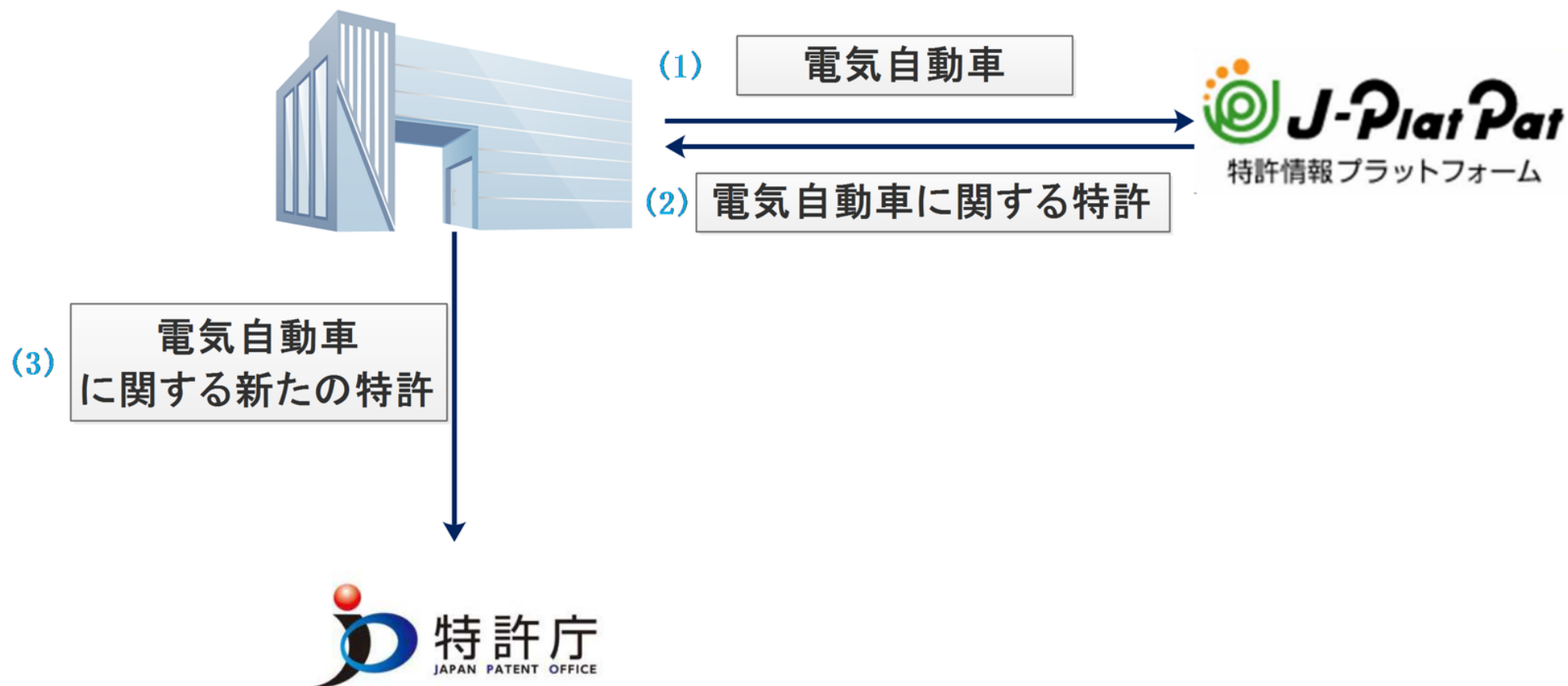
- 背景
- 曖昧化検索
- 攻撃手法
- 単語ベクトルを用いた質問曖昧化
- 評価実験
- まとめ

- 背景
- 曖昧化検索
- 攻撃手法
- 単語ベクトルを用いた質問曖昧化
- 評価実験
- まとめ

# 特許検索

- 特許を取るには以下の条件を満たさなければならない：
  - **新規性**(特許法29条第1項)：特許出願前に公然知られた発明，公然実施をされた発明，頒布された刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明について特許を受けることができない
  - **進歩性**(特許法29条第2項)：特許出願前にその発明の属する技術の分野における通常の知識を有する者が前項各号に掲げる発明に基いて容易に発明をすることができたときは，その発明については，同項の規定にかかわらず，特許を受けることができない。

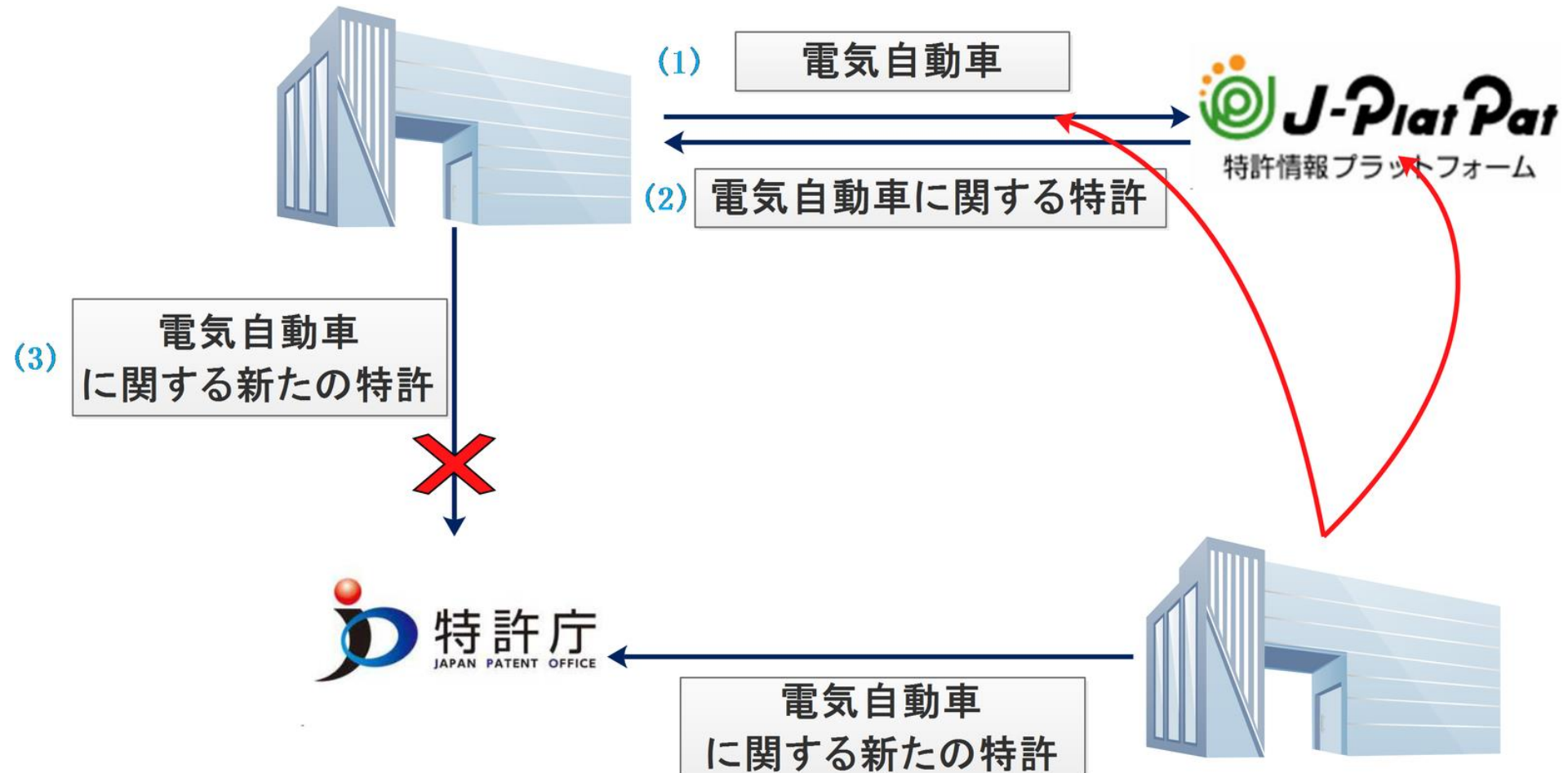
# 新規性調査



# 特許検索

- **先願主義**(特許法第39条)：同一の発明について異なつた日に二以上の特許出願があつたときは、最先の特許出願人のみがその発明について特許を受けることができる。

# 新規性調査



# 質問意図

- 質問者が検索したいもの、質問者が興味あるトピック
  - 具体的な質問だけではなく質問意図を隠したい
- 言葉のもつ意味を数値的に記述する
  - 潜在意味分析(LSA) (LSA) [Deerwester et al., 1990]
  - 潜在ディリクレ配置法(LDA) [Blei et al., 2003]
  - ...
- 意味分析ツール
  - 単語とトピック, 質問とトピックの関連値を計算する
  - 単語と単語, 質問と質問の意味的距離を計算する



# AOL検索データ公開事件[Michael and Tom, 2006]

- 2006年8月4日、AOL(American OnLine)が650,000人以上のユーザーの匿名化された検索質問ログを研究目的でリリースした
- この質問ログは、IPアドレス、ユーザー名などの個人情報を全部消去した
- 2006年8月9日、ID 4417749の名前、年齢、住所などが特定された

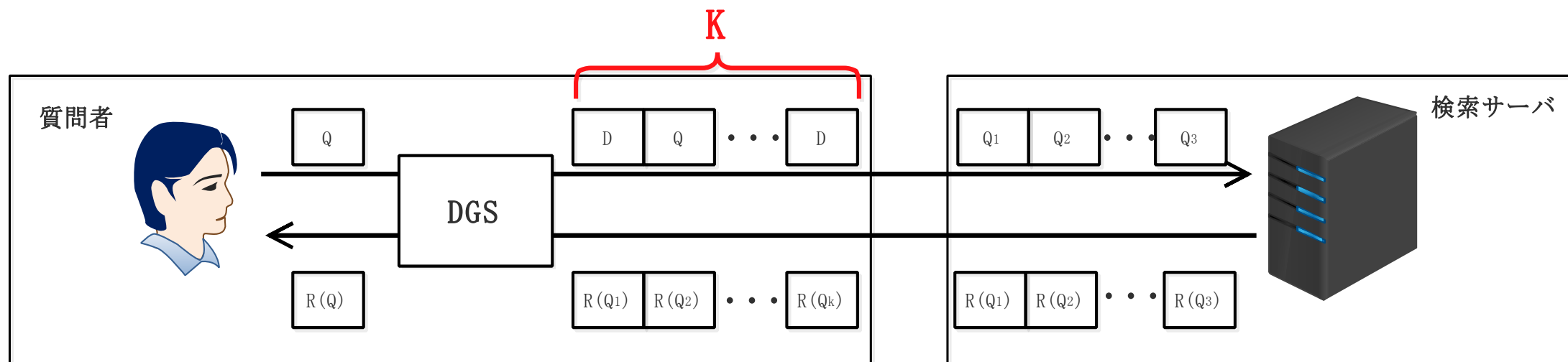
# 情報検索における質問者のプライバシー保護

- IPアドレスの匿名化
- Private Information Retrieval
- 信頼できる第三者を介する方法
- 曖昧化検索
- ...
-

# 情報検索における質問者のプライバシー保護

- IPアドレスの匿名化
- Private Information Retrieval
- 信頼できる第三者を介する方法
- 曖昧化検索
- ...
-

# 曖昧化検索



- 真の質問とダミー質問を同時に検索する
  - 否認可能検索
  - 質問者のプライバシーを保護する質問加工法
  - 質問意図を曖昧化するキーワード検索
  - ...

# 特許検索

- 特許文書：単語の曖昧性が少ない
  - 発明の範囲を正確に記載するように普段に使わない学術用語を用いる
  - 単語を全体を通じて統一して使用し，指示代名詞はなるべく用いない
- 特許検索質問：長い
  - ウェブ検索:2.35 [Jansen et al. 1998]
  - 特許検索:21.0
- 特許検索：再現率を重視する

- 背景
- 曖昧化検索
- 攻撃手法
- 単語ベクトルを用いた質問曖昧化
- 評価実験
- まとめ

# 曖昧化検索

- 否認可能検索[Murugesan and Clifton, 2009]
- 質問者のプライバシーを保護する質問加工法[Pang et al., 2010]
- 質問意図を曖昧化するキーワード検索[Wang and Ravishankar, 2014]

# 曖昧化検索

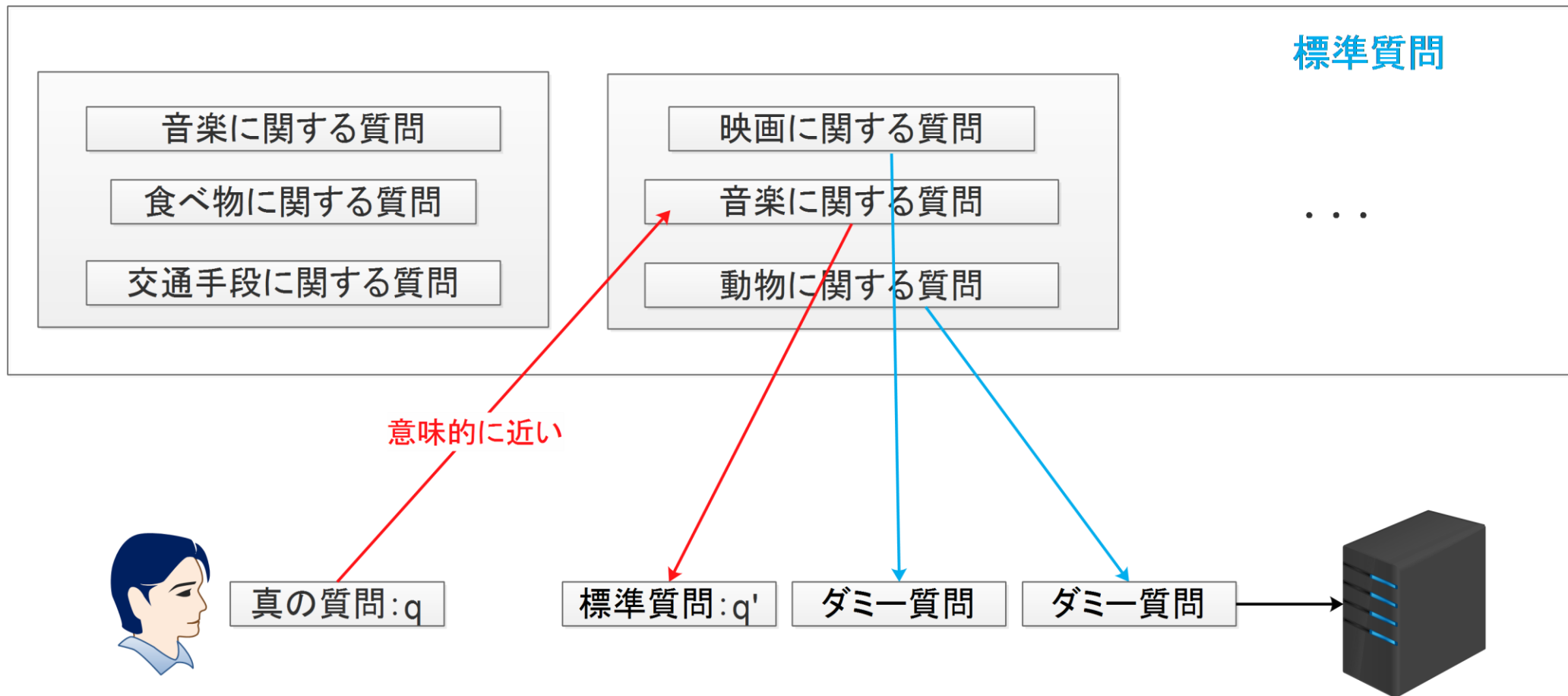
- 否認可能検索
- 質問者のプライバシーを保護する質問加工法
- 質問意図を曖昧化するキーワード検索



# 否認可能検索

- 事前に文書集合から高頻度な単語と連続する2単語からなる単語ペアを抽出してシート質問にする
- LSAを用いて単語間，質問間の意味的距離を計算する
- 意味的近いシート質問をマージして、標準質問にする。
- 意味的遠い標準質問をクラスタリングしてPD-質問集合を構築する

# 否認可能検索



# 事前に質問をグループにする

- 問題点
  - 質問の長さの増加と伴って質問の可能な組み合わせが指数的に増加する
  - 真の質問の代わりに標準質問を用いるため検索の精度と再現率が下がる

# 事前に質問をグループにする

質問グループ1	音楽	食べ物	交通手段
質問グループ2	動物	音楽	映画
質問グループ3	音楽	服	食べ物
質問グループ4	本	スポーツ	音楽

# 事前に質問をグループにする

質問グループ1	音楽	食べ物	交通手段
質問グループ2	動物	音楽	映画
質問グループ3	音楽	服	食べ物
質問グループ4	本	スポーツ	音楽

# 事前に質問をグループにする

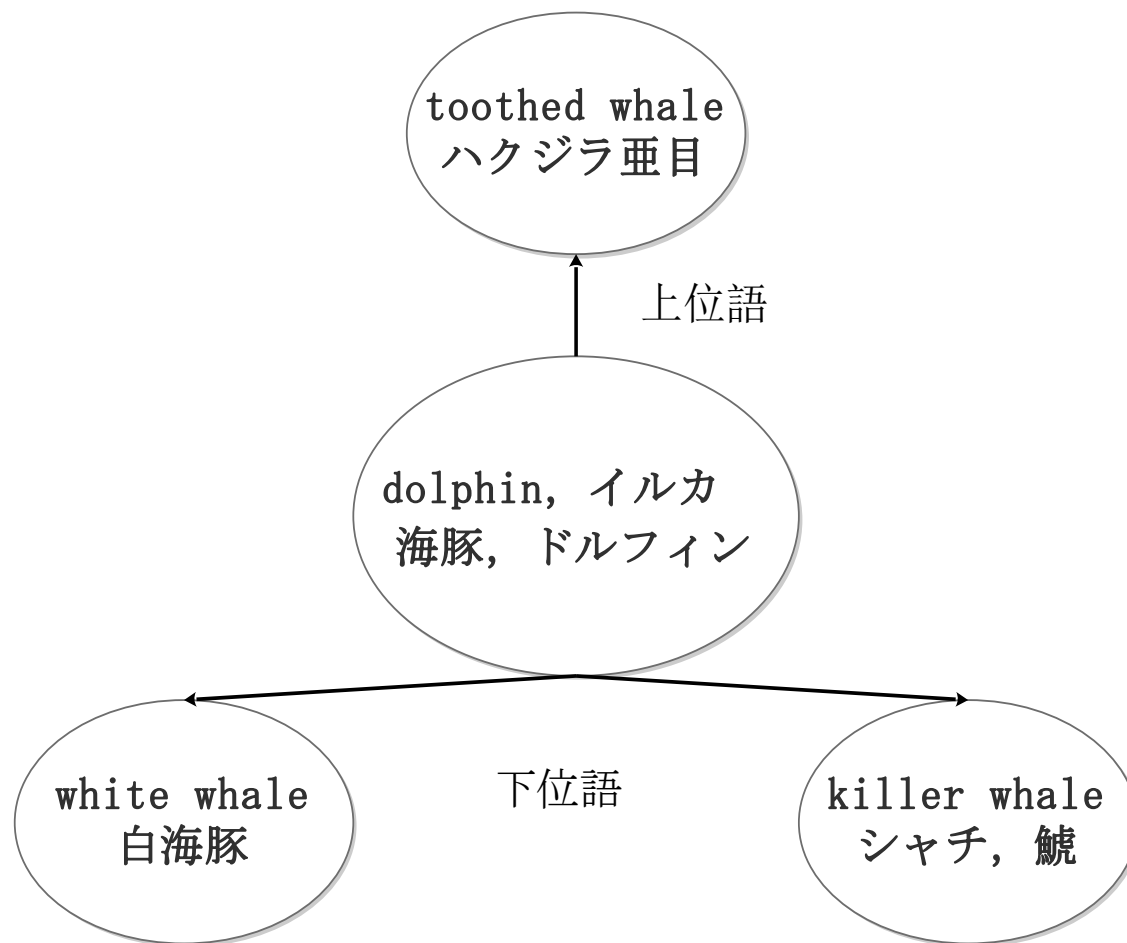
- 問題点

- 質問の長さの増加に伴って質問の可能な組み合わせが指数的に増加する
- 真の質問の代わりに標準質問を用いるため検索の精度と再現率が下がる
- 同じトピックに対して一連の質問を検索すると真の質問がバレる恐れがある

# 曖昧化検索

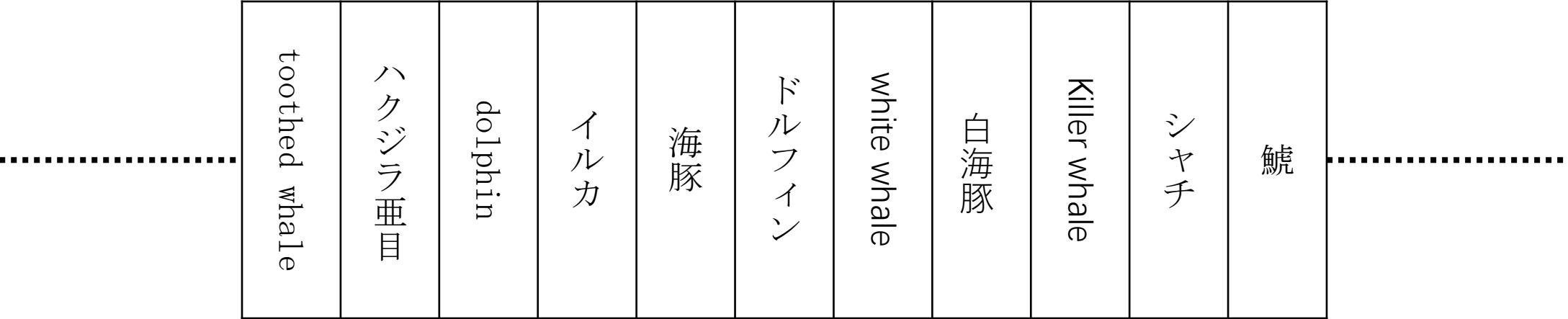
- 否認可能検索
  - 事前に質問をグループにする
- 質問者のプライバシーを保護する質問加工法
  - 事前に単語をグループにする
- 質問意図を曖昧化するキーワード検索

# WordNet [Miller, 1995]

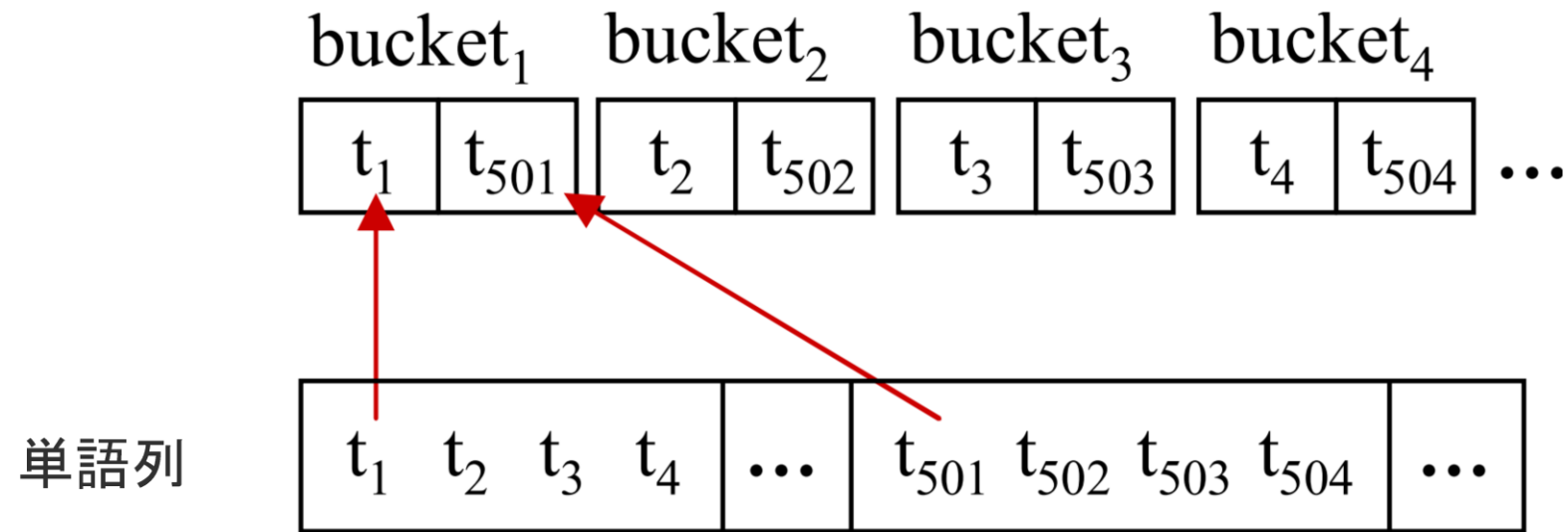




# WordNet



# 質問者のプライバシーを保護する質問加工法



真の質問	ダミー質問
t <sub>1</sub>	t <sub>501</sub>
t <sub>2</sub>	t <sub>502</sub>
t <sub>4</sub>	t <sub>504</sub>

# 質問者のプライバシーを保護する質問加工法

- 問題点
  - WordNetに含まれていない単語は検索できない
  - ダミー質問は1つのトピックに集中する保証がない

# 曖昧化検索

- 否認可能検索
  - 事前に質問をグループにする
- 質問者のプライバシーを保護する質問加工法
  - 事前に単語をグループにする
- 質問意図を曖昧化するキーワード検索
  - 事前にトピックをグループにする

# 質問意図を曖昧化するキーワード検索

- 事前準備

- LDAを用いて各トピック $t$ における単語 $w$ の出現率 $\text{Pr}[w|t]$ と各トピック $t$ の出現率 $\text{Pr}[t]$ を計算する
- LDAを用いて得たトピックをグループにする

- 検索

- 真の質問 $q$ が属するトピック $t = \text{argmax}_t \text{Pr}[t|q]$ を計算する
- $t$ と同じグループに含まれているトピック $t'$ をダミートピックとする
- $\text{Pr}[w|t']$ に基づいて  $|q|$  個の単語をランダムに選び, ダミー質問を作る

# 質問意図を曖昧化するキーワード検索

真の質問	ダミー質問
映画	スポーツ
映画	スポーツ
映画	スポーツ
...	...

# 質問意図を曖昧化するキーワード検索

真の質問	ダミー質問
君の名は 監督	野球 スラムダンク
君の名は 原作	ラグビー ルール
君の名は 声優	J1 順位表
...	...

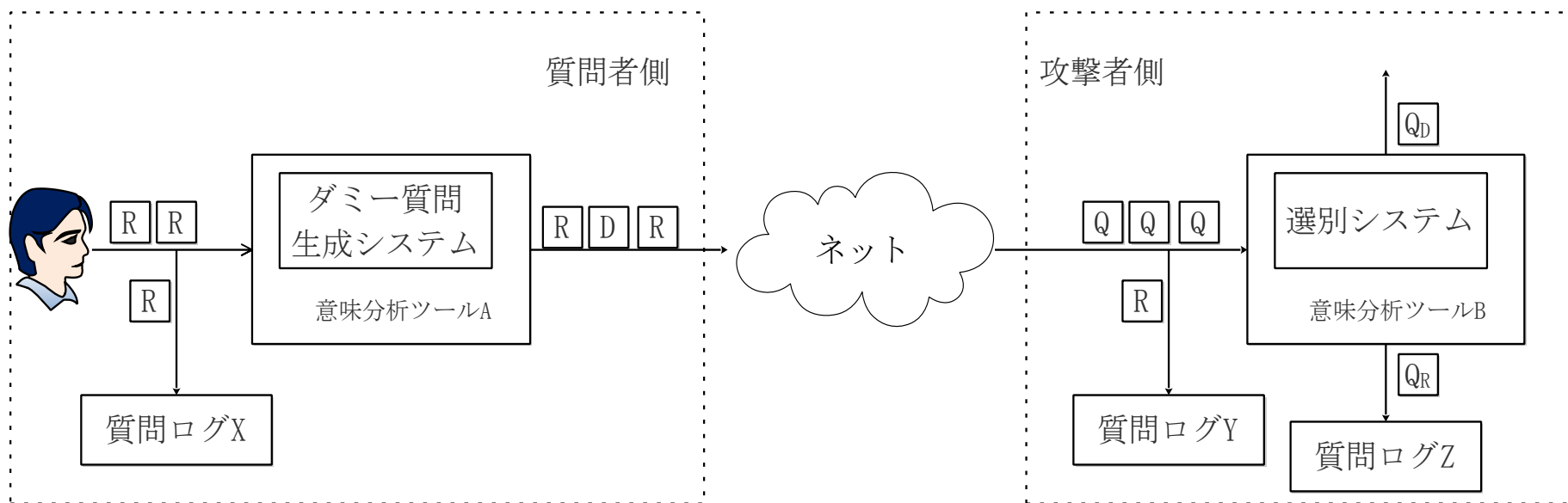
# 質問意図を曖昧化するキーワード検索

真の質問	ダミー質問
君の名は 監督	野球 スラムダンク
君の名は 原作	ラグビー ルール
君の名は 声優	J1 順位表
...	...



- 背景
- 曖昧化検索
- 攻撃手法
- 単語ベクトルを用いた質問曖昧化
- 評価実験
- まとめ

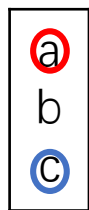
# 攻撃モデル



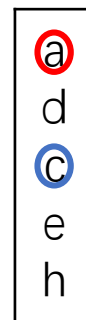
- 検索サーバが攻撃者である
- 攻撃者は質問者が用いている曖昧化手法を知っている

# 類似度攻擊 [Petit et al., 2016]

質問A

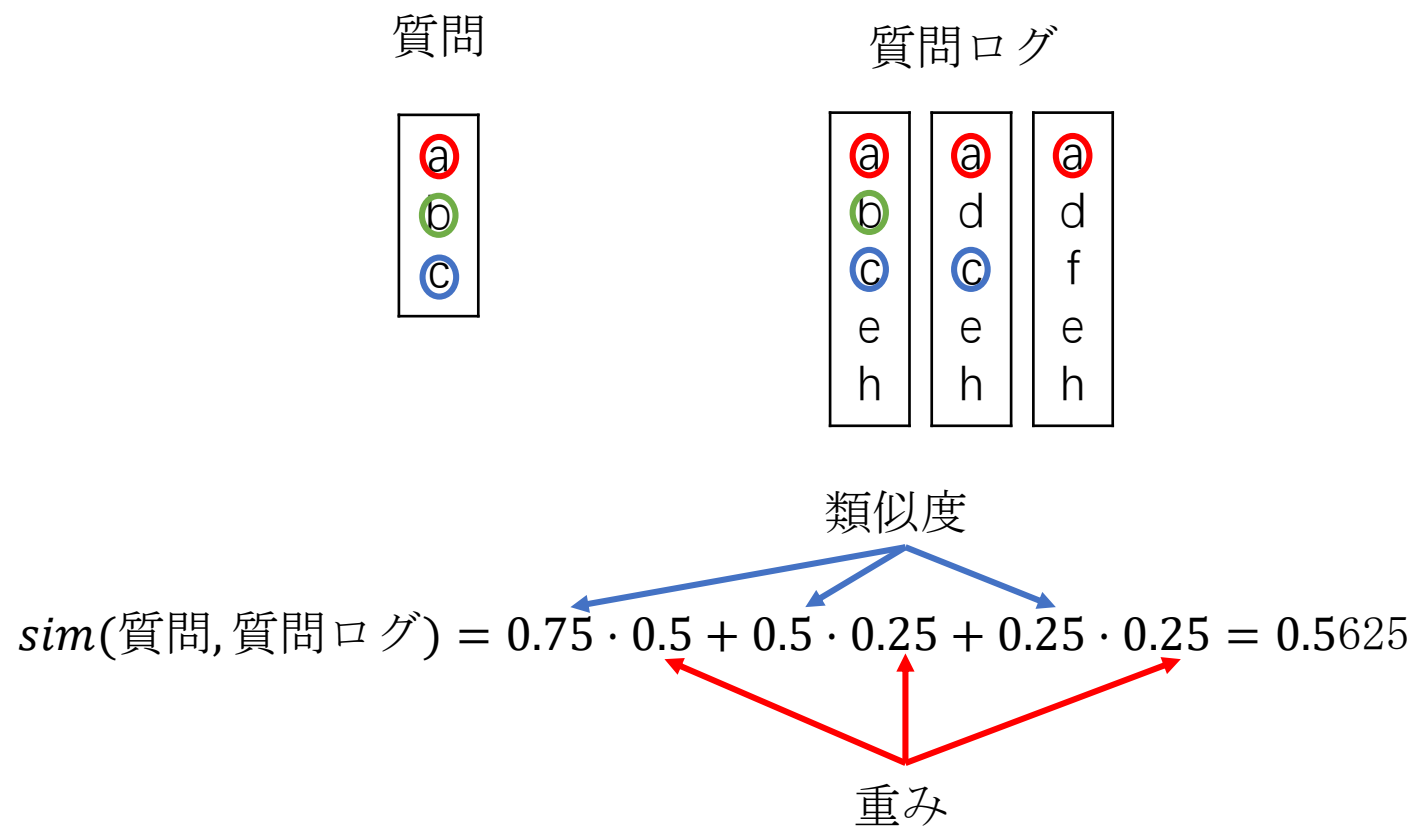


質問B

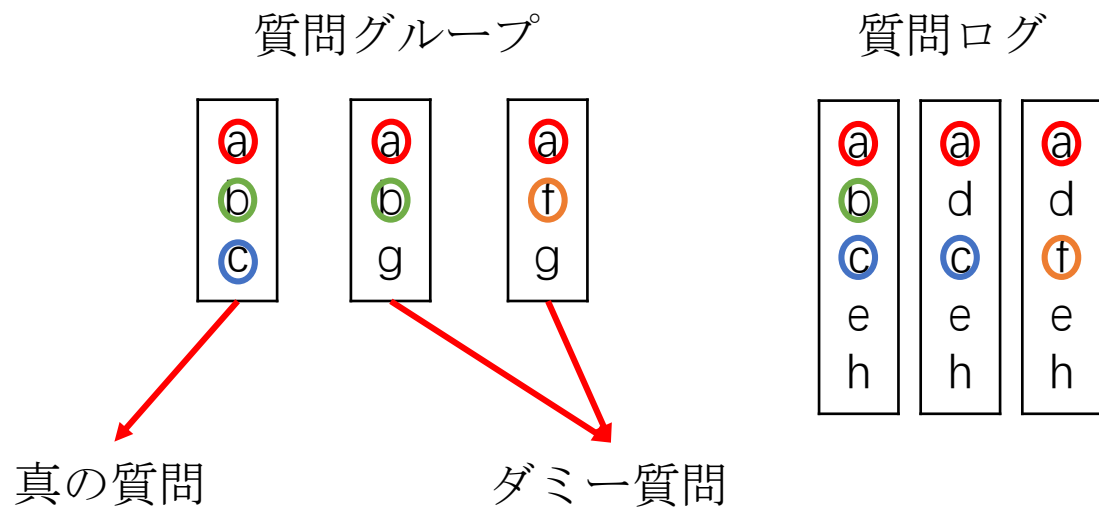


$$\begin{aligned} coef(A, B) &= 2 \cdot |q_A \cap q_B| \cdot \frac{1}{|q_A| + |q_B|} \\ &= 2 \cdot 2 \cdot \frac{1}{3 + 5} = 0.5 \end{aligned}$$

# 類似度攻撃



# 類似度攻撃



# 類似度攻撃

- 問題点
  - 事前情報がないと攻撃できない

# 事前情報がない場合の類似度攻撃

質問グループ1

A

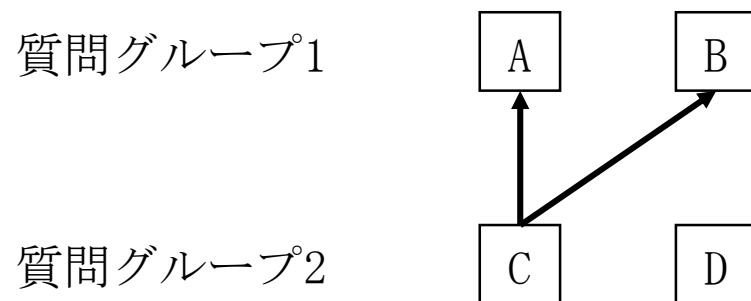
B

質問グループ2

C

D

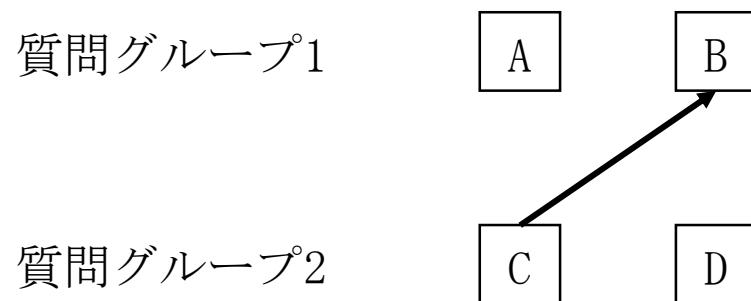
# 事前情報がない場合の類似度攻撃



$$\text{coef}(A, C) < \text{coef}(B, C)$$

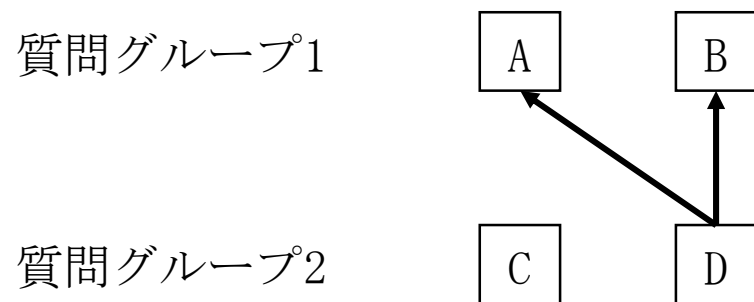


# 事前情報がない場合の類似度攻撃



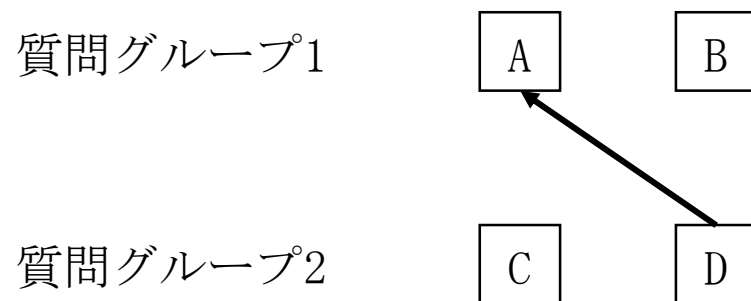
$$\text{coef}(A, C) < \text{coef}(B, C)$$

# 事前情報がない場合の類似度攻撃



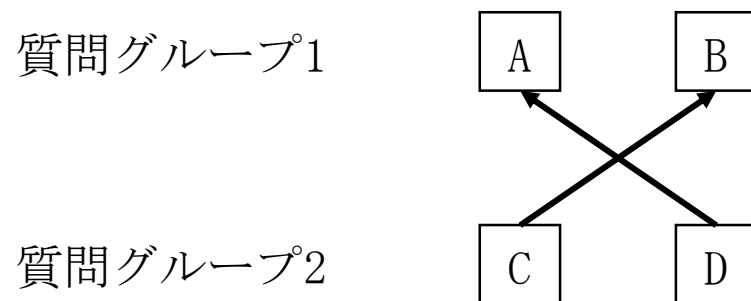
$$\text{coef}(A, D) > \text{coef}(B, D)$$

# 事前情報がない場合の類似度攻撃



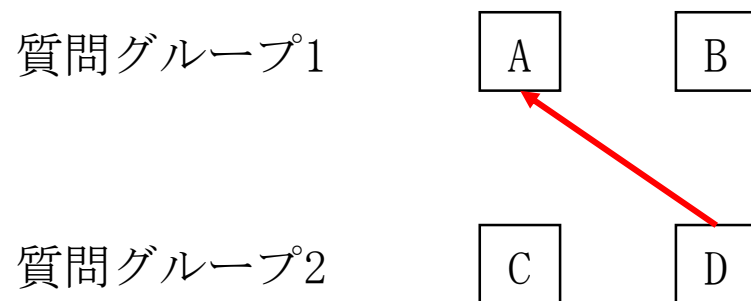
$$\textit{coef}(A, D) > \textit{coef}(B, D)$$

# 事前情報がない場合の類似度攻撃



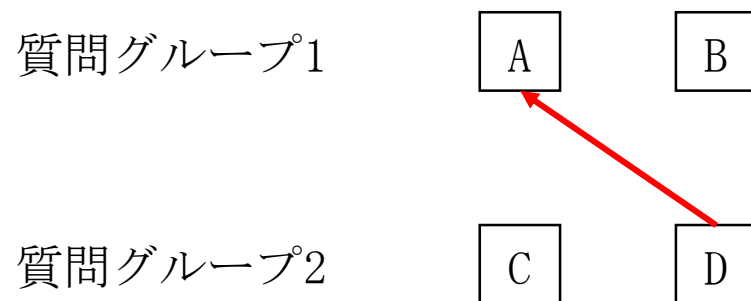
$$\textit{coef}(A, D) > \textit{coef}(B, C)$$

# 事前情報がない場合の類似度攻撃



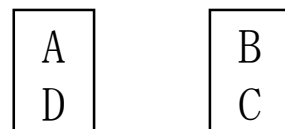
$$\text{coef}(A, D) > \text{coef}(B, B)$$

# 事前情報がない場合の類似度攻撃

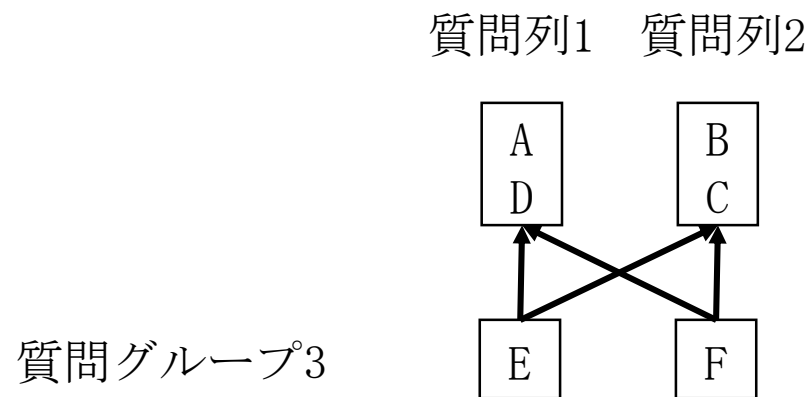


$$\text{coef}(A, D) > \text{coef}(B, B)$$

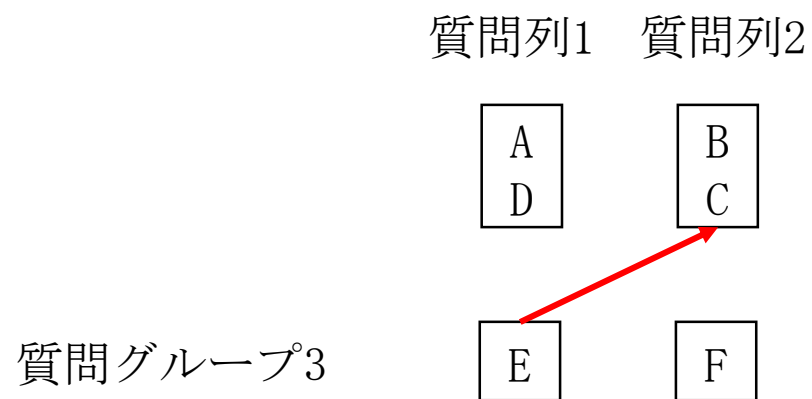
質問列1 質問列2



# 事前情報がない場合の類似度攻撃



# 事前情報がない場合の類似度攻撃





# 事前情報がない場合の類似度攻撃

- 問題点
  - 単語を事前にグループにする手法に対して攻撃できない

# 事前情報がない場合の類似度攻撃

質問グループ1

a  
b

c  
d

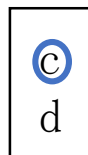
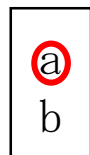
質問グループ2

a  
e

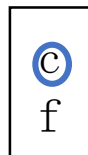
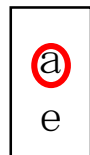
c  
f

# 事前情報がない場合の類似度攻撃

質問グループ1



質問グループ2



# 事前情報がない場合の類似度攻撃

- 問題点
  - 単語を事前にグループにする手法に対して攻撃できない

# メイントピック攻撃

真の質問	ダミー質問
$t_1$	$t_{501}$
$t_2$	$t_{502}$
$t_4$	$t_{504}$

- 質問とトピックの関係値を $\text{rscore}(\text{質問}, \text{トピック})$ とする
- 全てのトピックの中 $\text{rscore}(\text{質問}, \text{トピック})$ が一番大きいトピックを質問のメイントピックという

$\text{rscore}(\text{真の質問}, \text{真の質問のメイントピック})$



$\text{rscore}(\text{ダミー質問}, \text{ダミー質問のメイントピック})$

- 背景
- 曖昧化検索
- 攻撃手法
- 単語ベクトルを用いた質問曖昧化
- 評価実験
- まとめ

# 単語ベクトルを用いた質問曖昧化

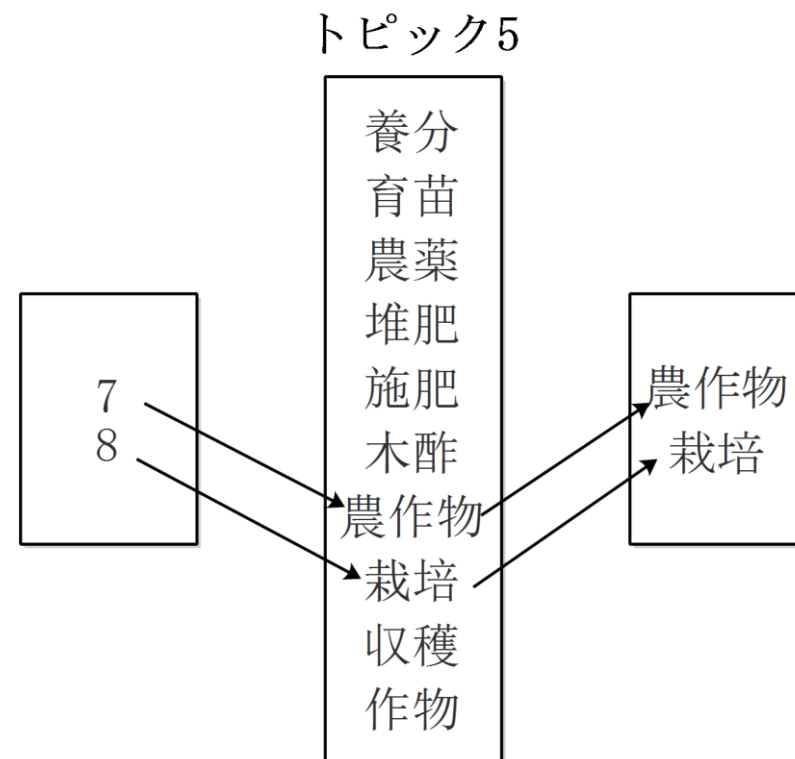
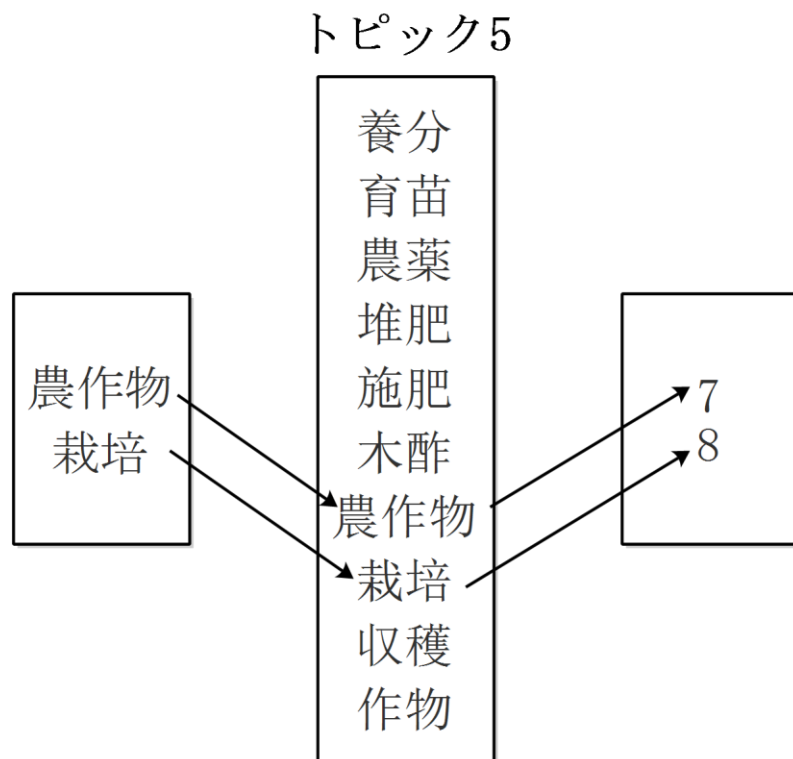
- 単語を事前にグループにする
  - 類似攻撃に強い
- トピックを事前にグループにする
  - メイントピックに強い

# 単語ベクトルを用いた質問曖昧化

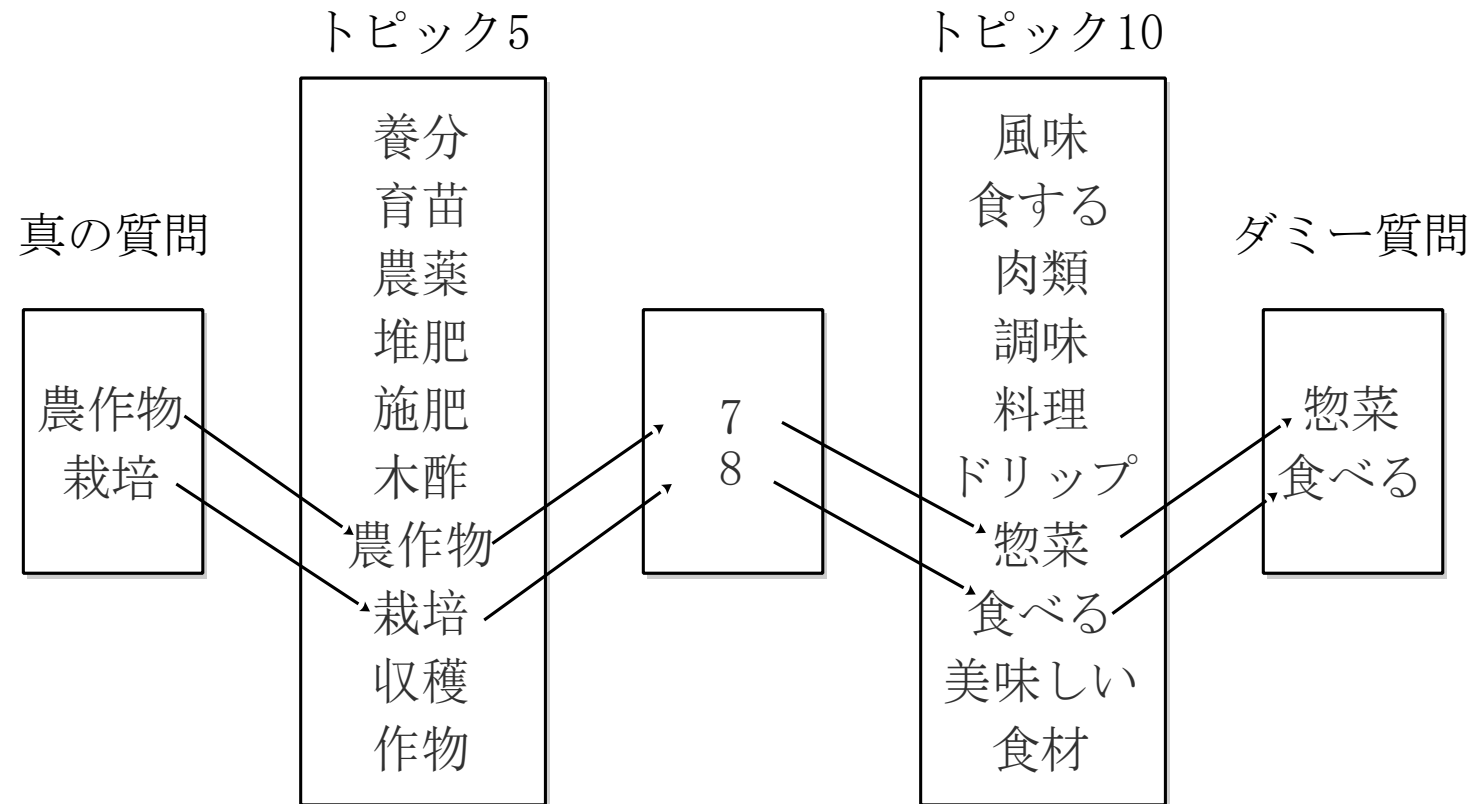
- 単語を事前にグループにする
  - 類似攻撃に強い
- トピックを事前にグループにする
  - メイントピックに強い
- 単語を事前にグループにする同時に単語もグループにしたい
  - 全ての単語を単語とトピック $t$ の関連値を大きい順に並べるベクトルをトピック $t$ の単語ベクトルという
  - 単語ベクトルを用いた曖昧化手法を提案する



# 単語ベクトル



# 質問者が検索したいトピックを曖昧化する



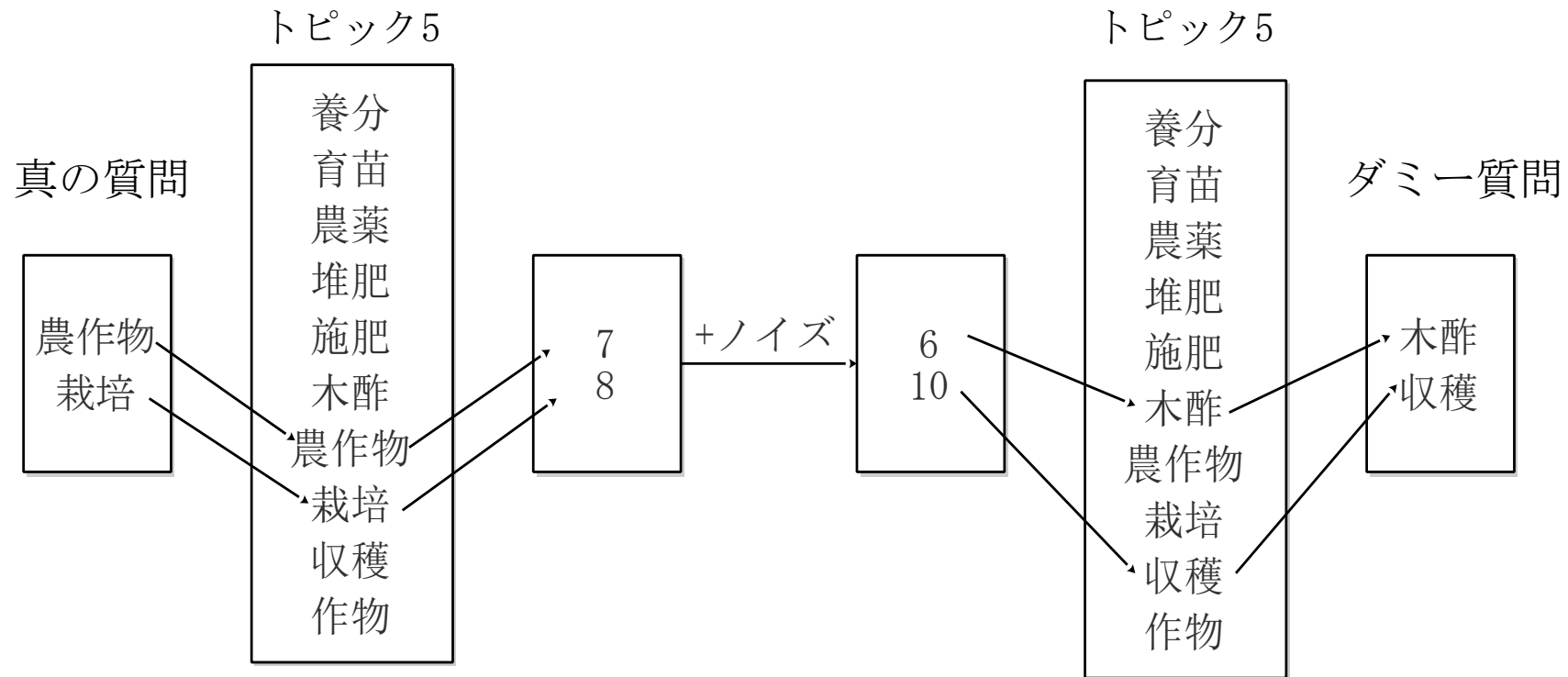
# 質問者が検索したいトピックにおける曖昧化

- 真の質問と違うトピックに属するダミー質問を作っても事前情報をもつ攻撃者に対応できない

# 質問者が検索したいトピックにおける曖昧化

- 真の質問と違うトピックに属するダミー質問を作っても事前情報をもつ攻撃者に対応できない
- 真の質問と同じトピックに属するダミー質問を作る

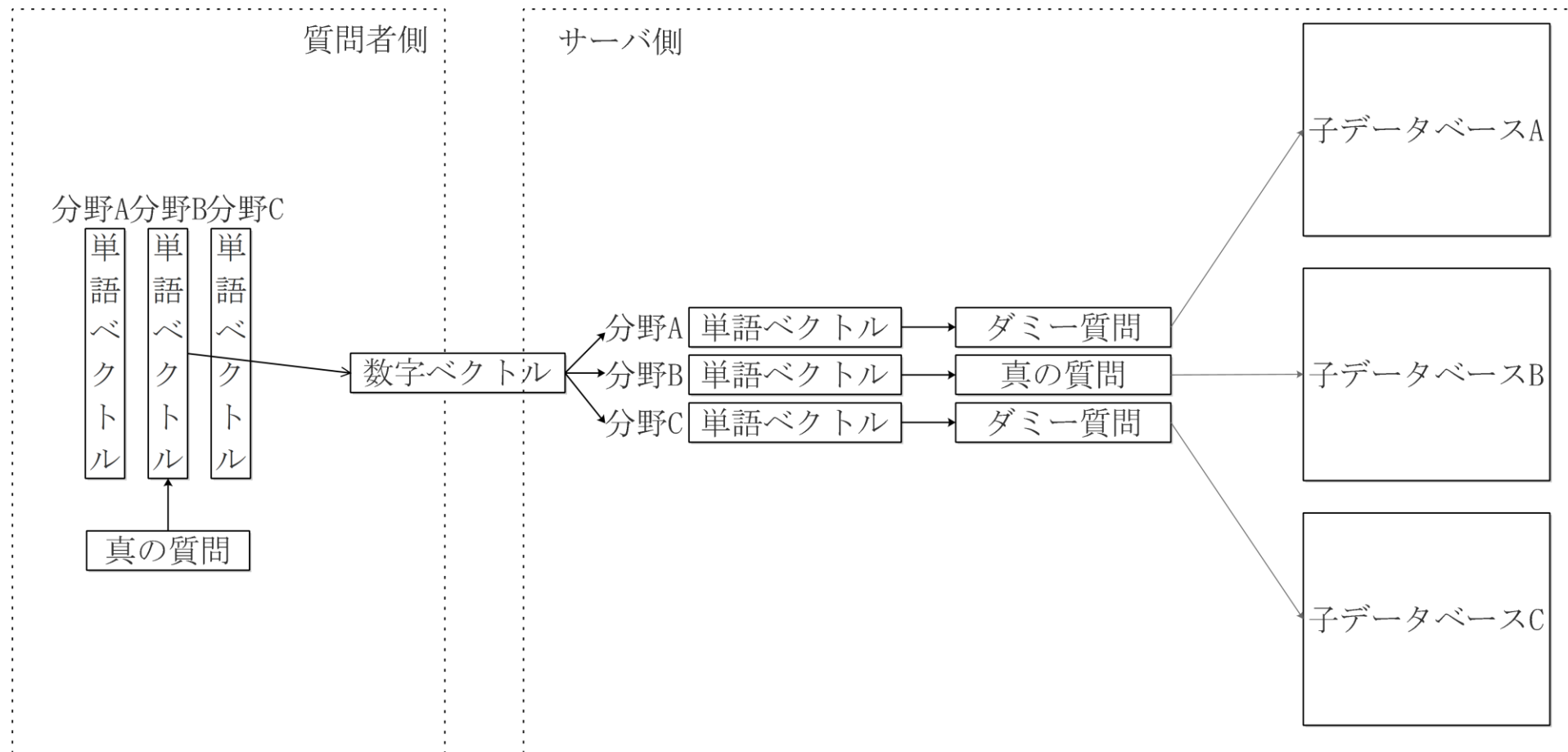
# 質問者が検索したいトピックにおける曖昧化



# 国際特許分類

A61C 5/08	
セクション:A	健康および娯楽
サブセクション:61	医学または獣医学:衛生学
クラス : C	歯科:口腔または歯科衛生
メイングループ:5	歯の充填または被覆
サブグループ:08	歯冠:その製造; 口中での歯冠固定

# データベース分割



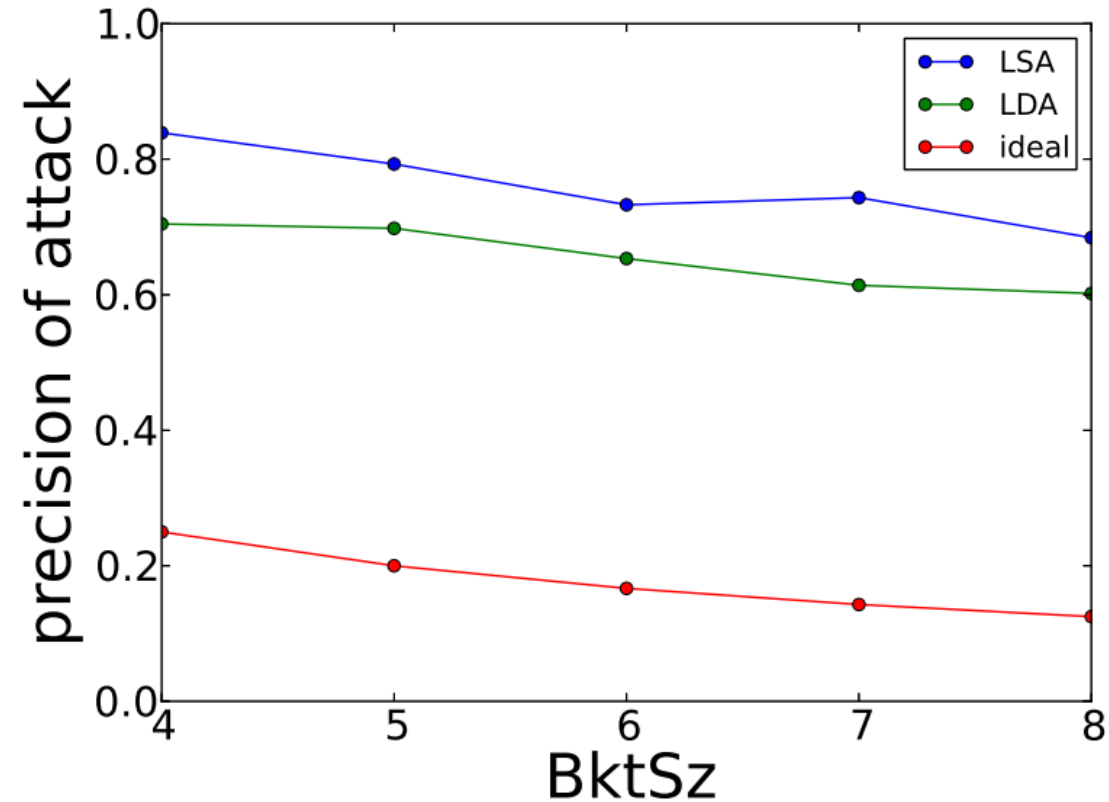
- 背景
- 曖昧化検索
- 攻撃手法
- 単語ベクトルを用いた質問曖昧化
- 評価実験
- まとめ



# 実験データ：NTCIR-6 [Fuji et al., 2007]

重複を除いた単語数	2, 973, 096
文書数	3, 496, 253
質問数	2, 908
質問平均単語数	21

## メントピック攻撃 V. S. 事前に単語をグループにする手法

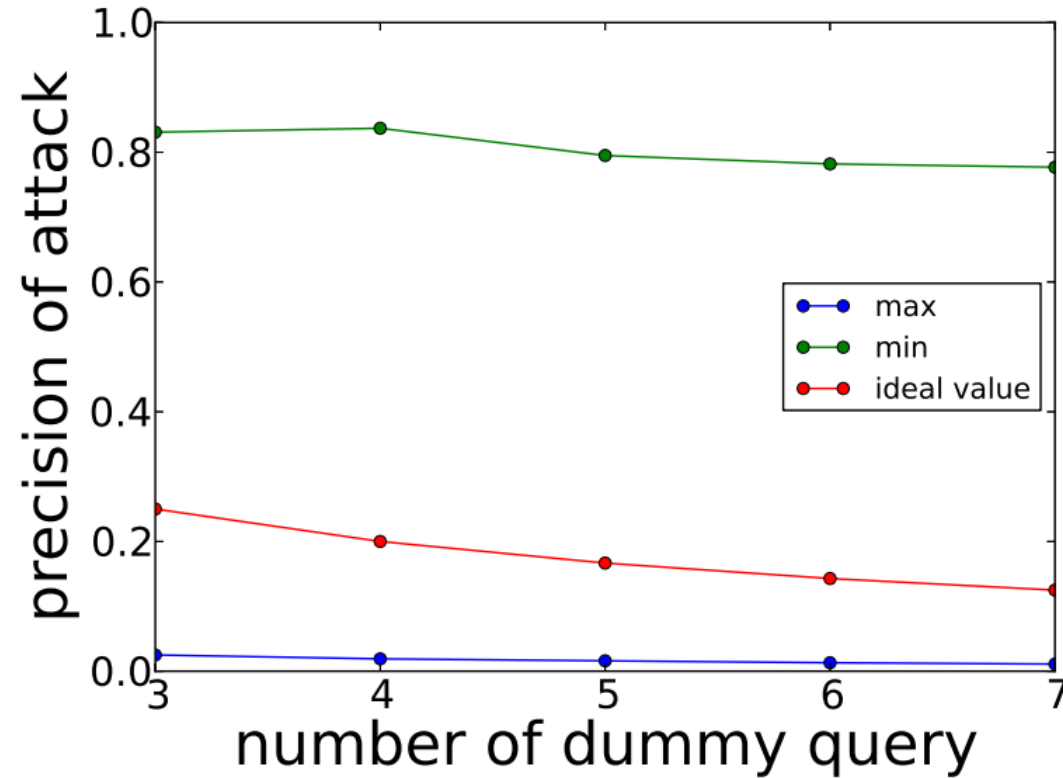


LSA : LSAを用いたメントピック攻撃

LDA : LDAを用いたメントピック攻撃

ideal : 理想値

## メイントピック攻撃 V. S. 事前にトピックをグループにする手法



max : 自分のメイントピックとの関連値が一番高い質問が真の質問である確率

min : 自分のメイントピックとの関連値が一番低い質問が真の質問である確率

ideal : 理想値


メイントピック攻撃 V. S. 事前にトピックをグループにする手法

- $\text{Pr}[\text{単語}|\text{質問}]$ で単語を選ぶため、質問 $q$ のメイントピックを $\delta_q$ にすると、各質問 $q$ に対して $\text{Pr}[q|\delta_q]$ 間の差が少ない

$$\text{rscore}(q, \delta_q) = \frac{\text{Pr}[q|\delta_q] \text{Pr}[\delta_q]}{\text{Pr}[q]}$$

## メイントピック攻撃 V. S. 事前にトピックをグループにする手法

- $\text{Pr}[\text{単語}|\text{質問}]$ で単語を選ぶため、質問 $q$ のメイントピックを $\delta_q$ にすると、各質問 $q$ に対して $\text{Pr}[q|\delta_q]$ 間の差が少ない

$$\text{rscore}(q, \delta_q) = \frac{\text{Pr}[q|\delta_q] \text{Pr}[\delta_q]}{\text{Pr}[q]}$$


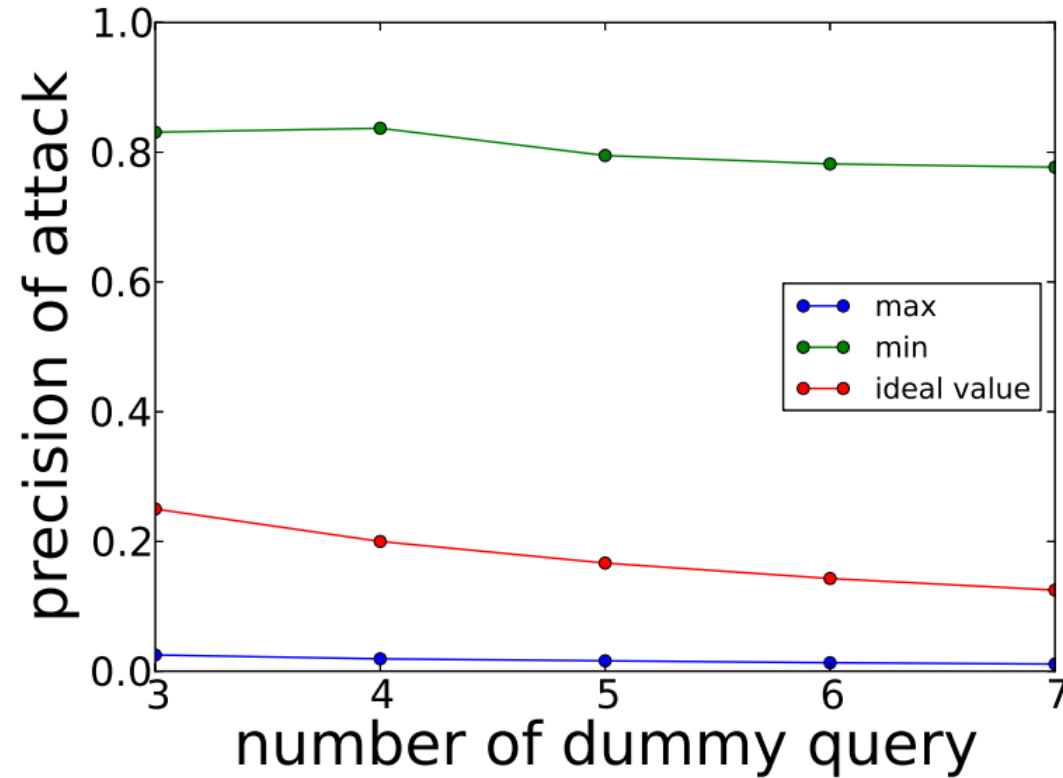
小

大

# 質問意図を曖昧化するキーワード検索

真の質問	ダミー質問
君の名は 監督	野球 スラムダンク
君の名は 原作	ラグビー ルール
君の名は 声優	J1 順位表
...	...

## メイントピック攻撃 V. S. 事前にトピックをグループにする手法

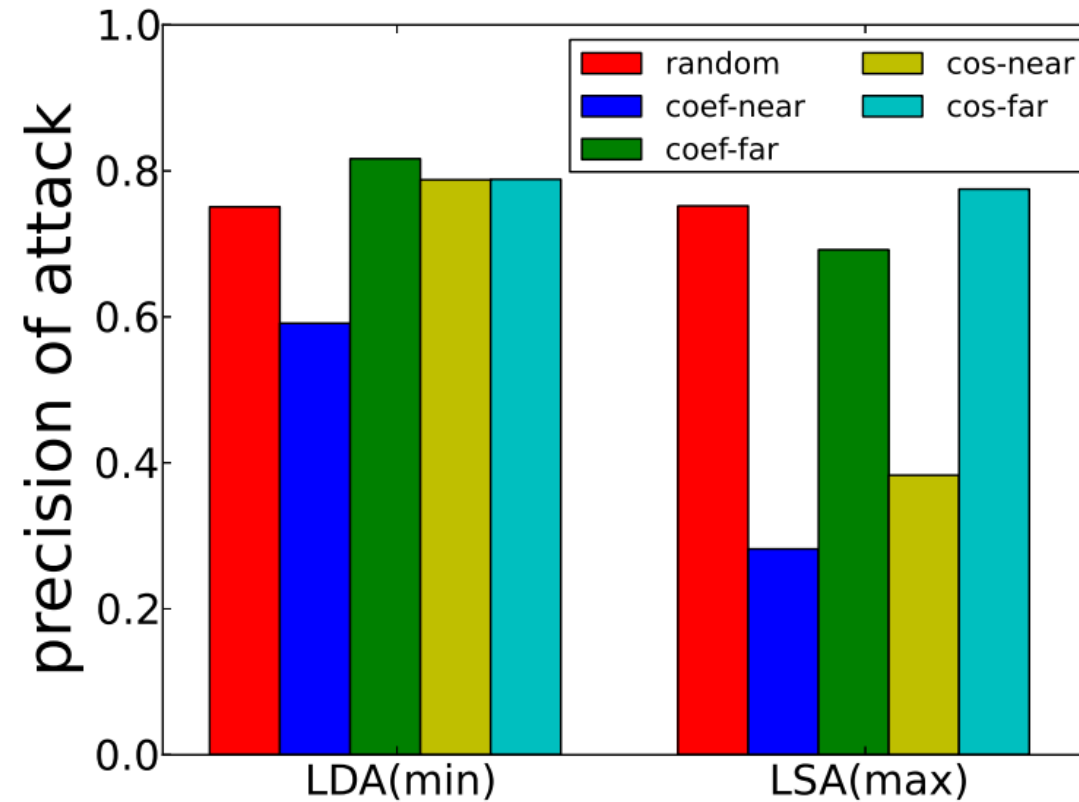


max : 自分のメイントピックとの関連値が一番高い質問が真の質問である確率

min : 自分のメイントピックとの関連値が一番低い質問が真の質問である確率

ideal : 理想値

## メイントピック攻撃 V. S. トピックを曖昧化する手法

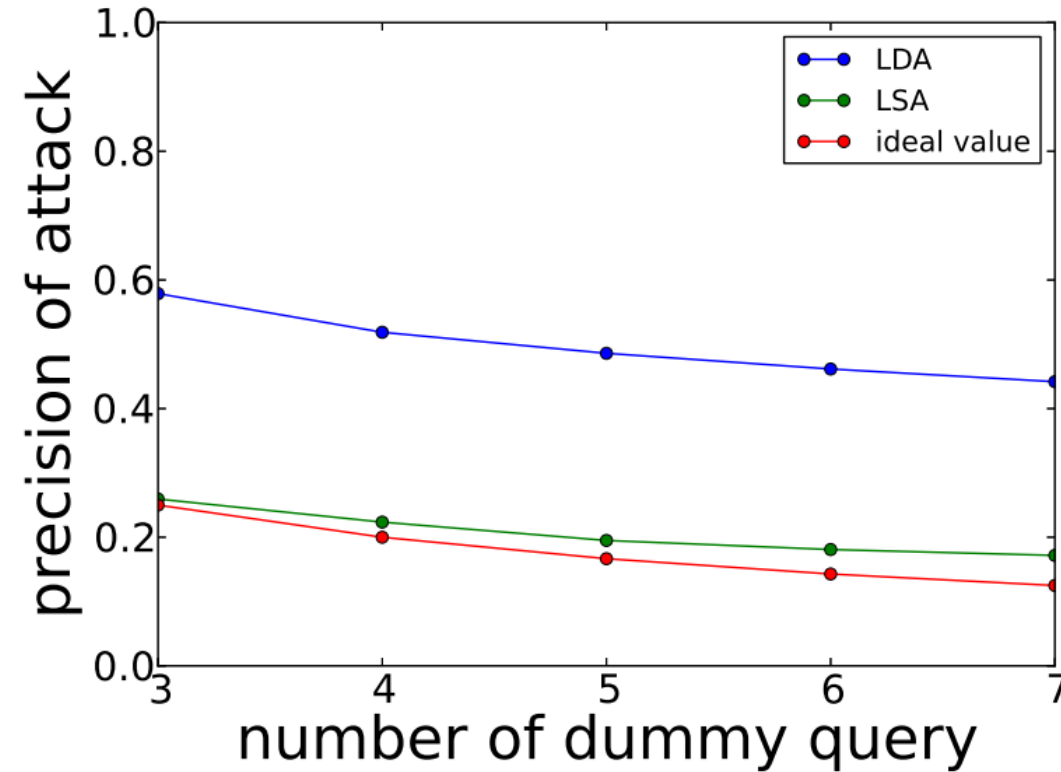


near : 意味的に近いトピックをダミートピックにする

far : 意味的に遠いトピックをダミートピックにする



## メイントピック攻撃 V.S. トピックにおける曖昧化手法

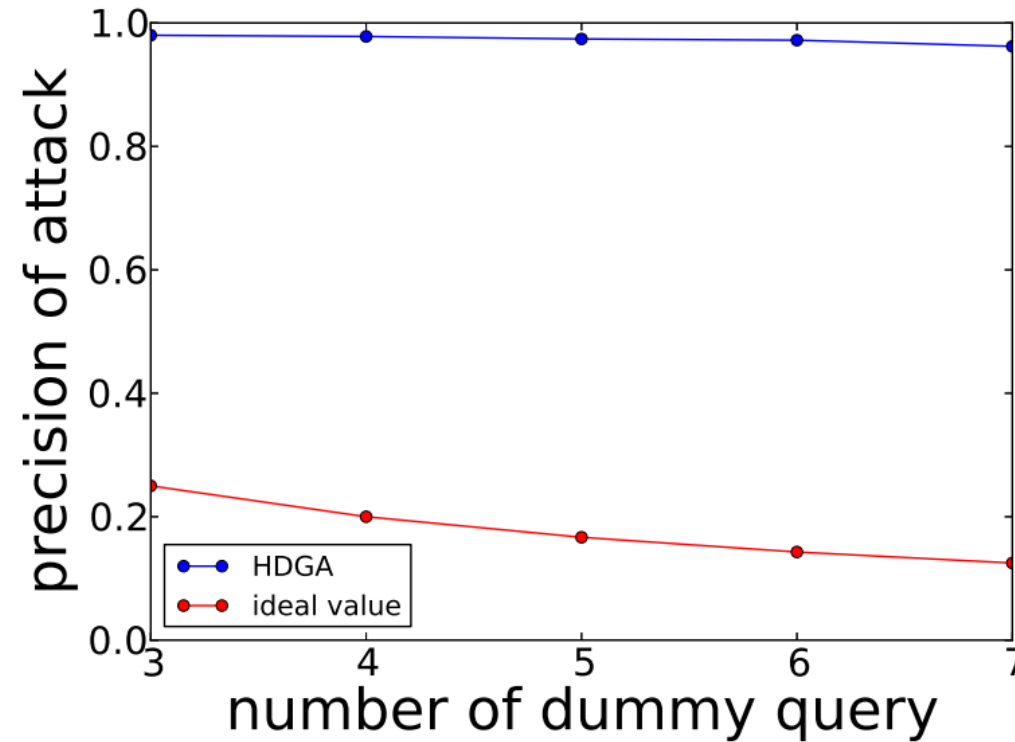


LSA : LSAを用いたメイントピック攻撃

LDA : LDAを用いたメイントピック攻撃

ideal : 理想値

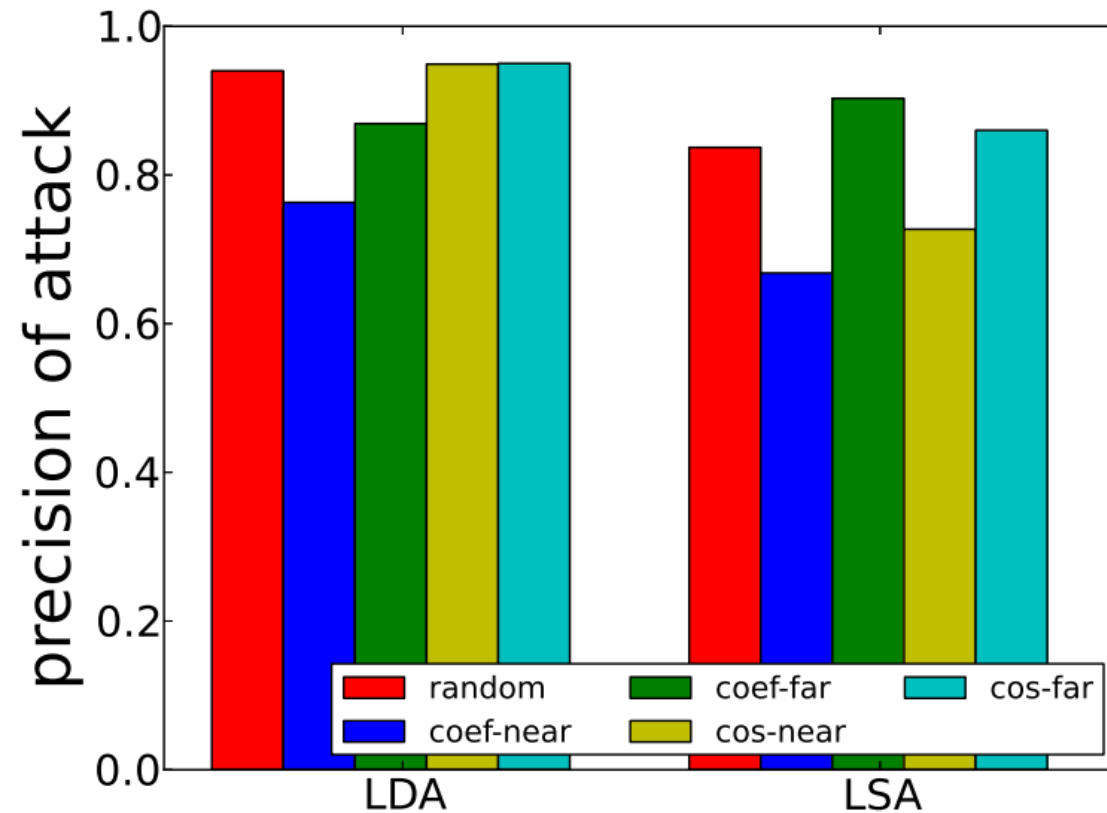
## 事前情報がない場合の類似度攻撃 V. S. トピックをグループ手法



HDGA : 事前情報がない場合の類似度攻撃

ideal : 理想値

## 事前情報がない場合の類似度攻撃 V. S. トピックを曖昧化する手法



near : 意味的近いトピックをダミートピックにする

far : 意味的遠いトピックをダミートピックにする

事前情報がない場合の類似度攻撃 V. S. トピックを曖昧化する手法

真の質問	ダミー質問
映画	スポーツ
映画	スポーツ
映画	スポーツ
...	...

事前情報がない場合の類似度攻撃 V. S. トピックを曖昧化する手法

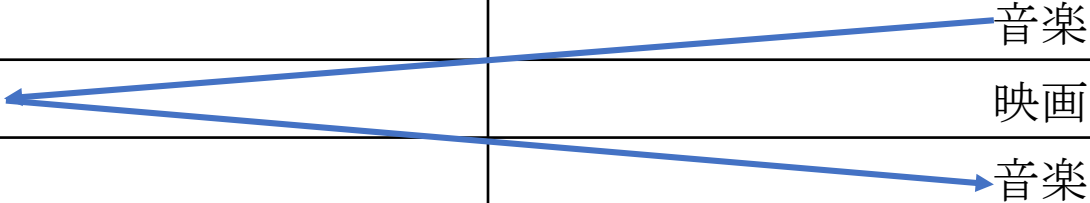
真の質問	ダミー質問
映画	スポーツ
音楽	農業
映画	スポーツ
...	...

# 質問意図を曖昧化するキーワード検索

真の質問	ダミー質問
君の名は 監督	野球 スラムダンク
君の名は アルバム 前前前世	農作物 栽培
君の名は 声優	J1 順位表
...	...

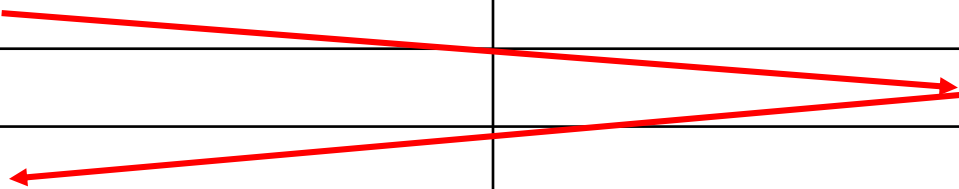
事前情報がない場合の類似度攻撃 V. S. トピックを曖昧化する手法

真の質問	ダミー質問
映画	音楽
音楽	映画
映画	音楽
...	...



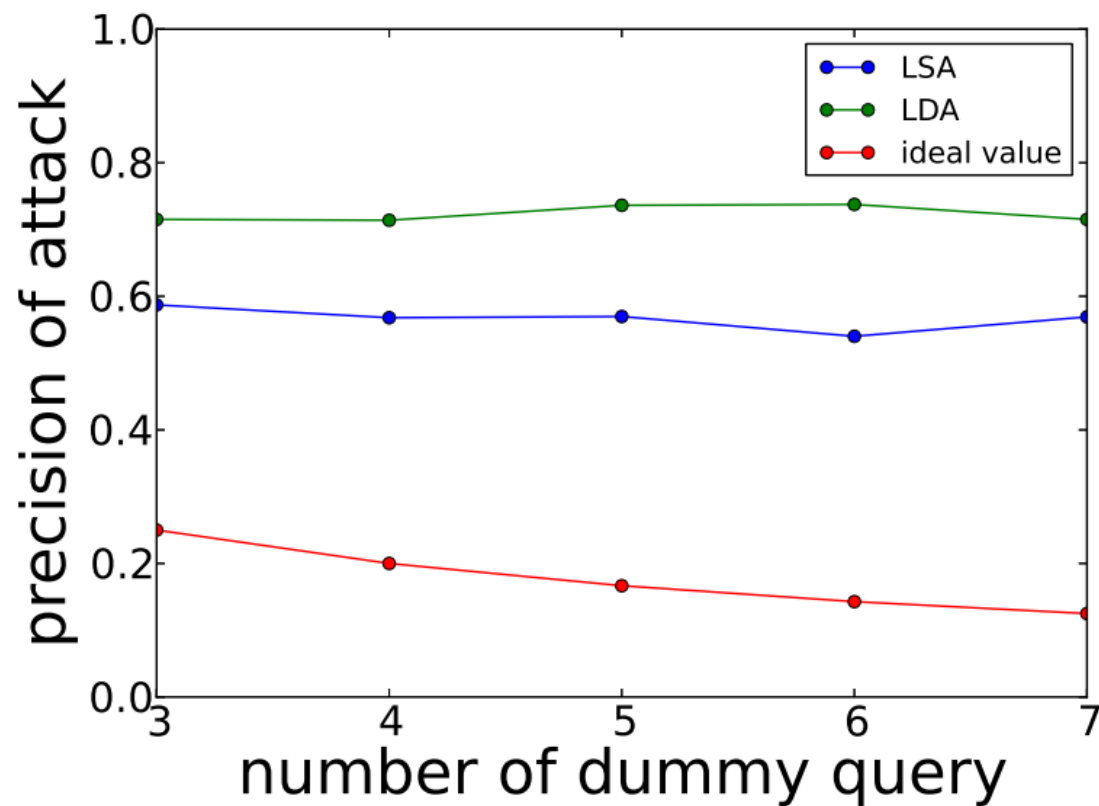
事前情報がない場合の類似度攻撃 V. S. トピックを曖昧化する手法

真の質問	ダミー質問
映画	音楽
音楽	映画
映画	音楽
...	...





## 事前情報がない場合の類似度攻撃 V. S. トピックにおける曖昧化手法

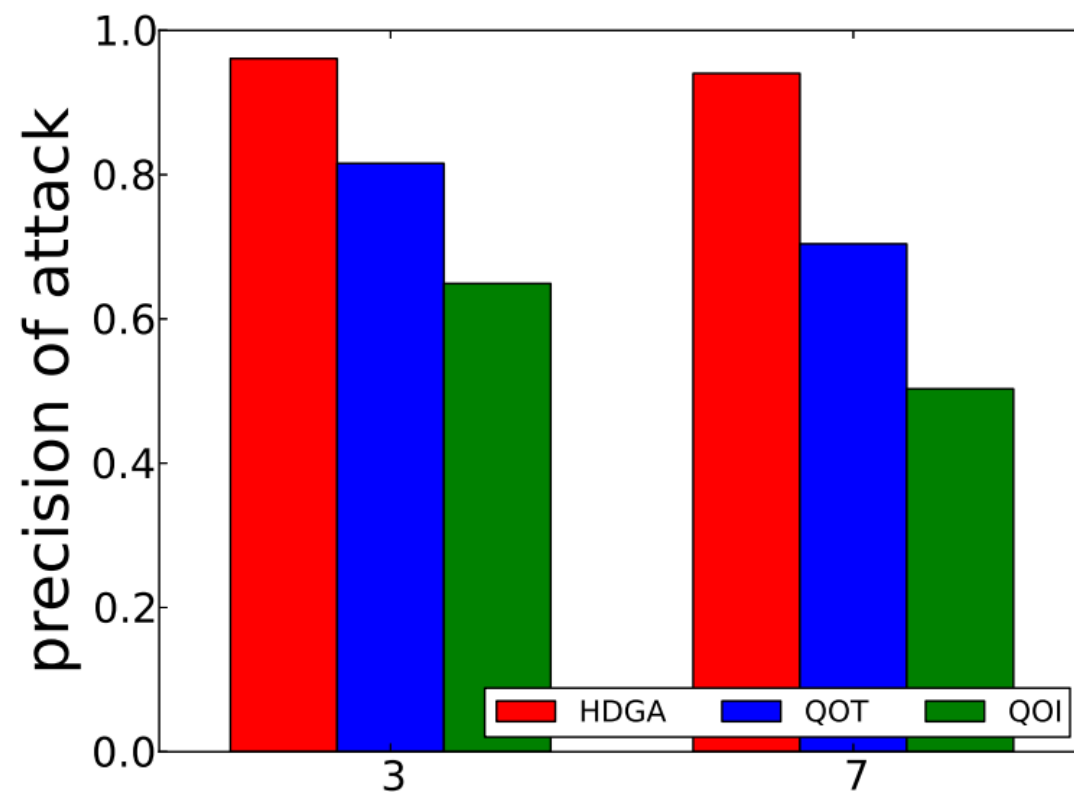


LSA : LSAを用いたトピックにおける曖昧化手法

LDA : LDAを用いたトピックにおける曖昧化手法

ideal : 理想値

# 事前情報がある場合の類似度攻撃

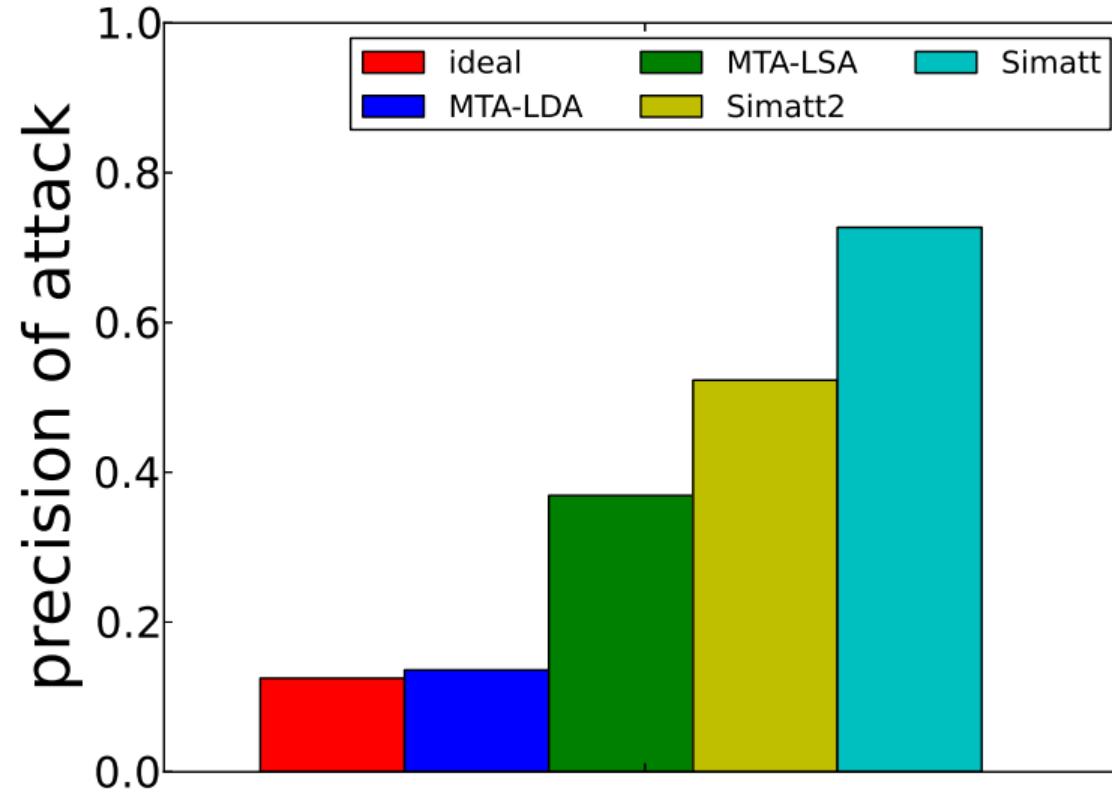


HDGA : 事前情報がない場合の類似度攻撃

QOT : トピックを曖昧化する手法

QOI : トピックにおける曖昧化手法

# データベース分割



ideal : 理想値  
MTA-LSA : LSAを用いたメイントピック攻撃  
MTA\_LDA : LDAを用いたメイントピック攻撃

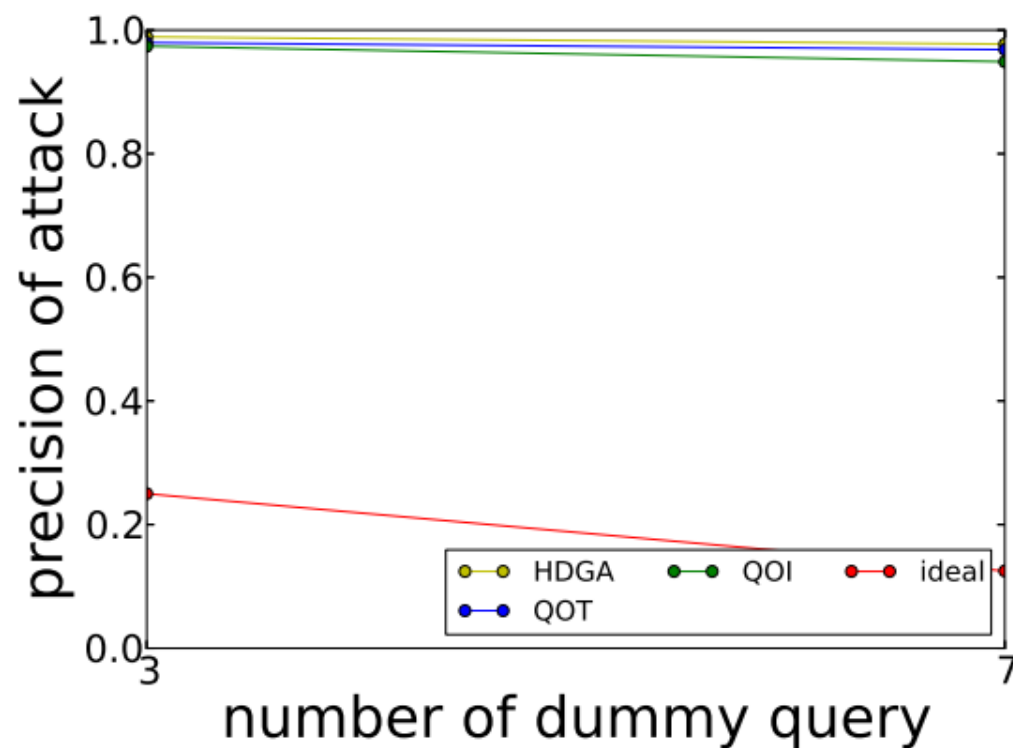
Simatt : 事前情報がある場合の類似度攻撃  
Simatt2 : 事前情報がない場合の類似度攻撃

## メイントピック攻撃 V. S. データベース分割

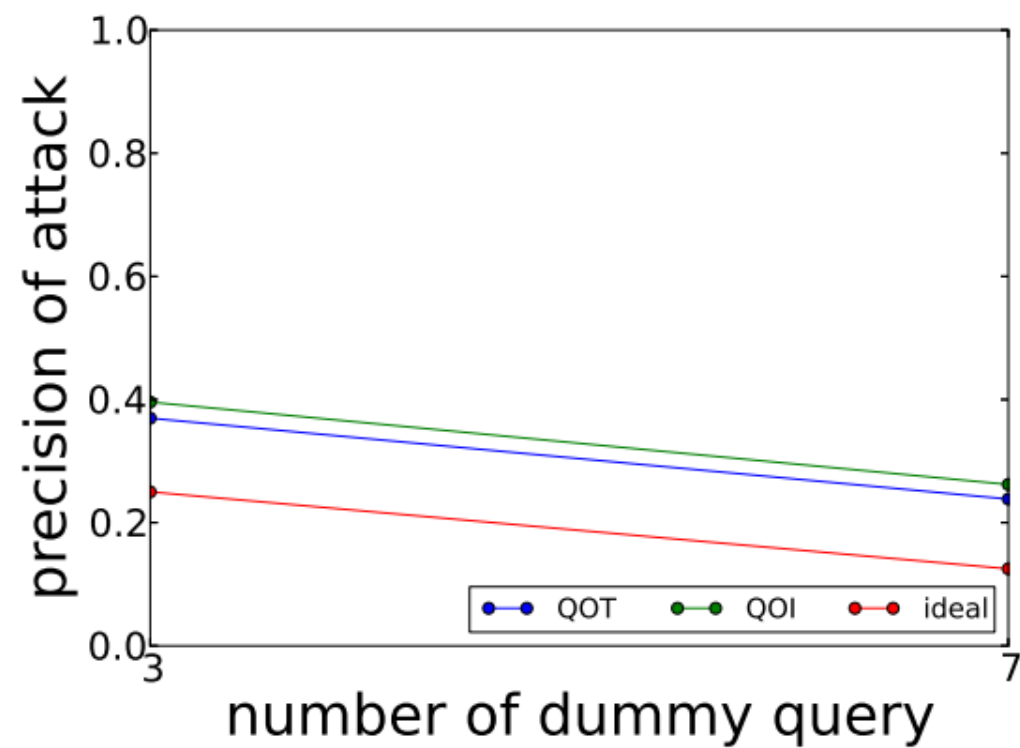
$$\text{rscore}(q, \delta_q) = \frac{\text{Pr}[q|\delta_q] \text{Pr}[\delta_q]}{\text{Pr}[q]}$$

The diagram illustrates the components of the rscore formula. A red arrow points from the character '小' (small) to the numerator  $\text{Pr}[q|\delta_q] \text{Pr}[\delta_q]$ . Another red arrow points from the character '小' to the denominator  $\text{Pr}[q]$ .

# 交差攻撃



質問者: LDA vs. 攻撃者: LSA



質問者: LSA vs. 攻撃者: LDA

HDGA : 事前情報がない場合の類似度攻撃

QOT : トピックを曖昧化する手法

QOI : トピックにおける曖昧化手法

- 背景
- 曖昧化検索
- 攻撃手法
- 単語ベクトルを用いた質問曖昧化
- 評価実験
- まとめ

# まとめ

	攻撃者				
質問者		MTA-LSA	MTA-LDA	SimAtt2	SimAtt
	ETSQ	68.4	60.2	x	x
	HDGA	97.7	77.7	96.2	94.0
	QOT-LSA	12.2	23.8	49.4	70.4
	QOT-LDA	96.8	55.7	88.9	94.3
	QOI-LSA	17.2	26.2	56.9	50.3
	QOI-LDA	94.5	44.2	71.5	81.2
	データベース分割	36.9	13.6	52.3	72.7

# まとめ

	攻撃者				
質問者		MTA-LSA	MTA-LDA	SimAtt2	SimAtt
	ETSQ	68.4	60.2	x	x
	HDGA	97.7	77.7	96.2	94.0
	QOT-LSA	12.2	23.8	49.4	70.4
	QOT-LDA	96.8	55.7	88.9	94.3
	QOI-LSA	17.2	26.2	56.9	50.3
	QOI-LDA	94.5	44.2	71.5	81.2
	データベース分割	36.9	13.6	52.3	72.7



# まとめ

	攻撃者				
質問者		MTA-LSA	MTA-LDA	SimAtt2	SimAtt
	ETSQ	68.4	60.2	x	x
	HDGA	97.7	77.7	96.2	94.0
	QOT-LSA	12.2	23.8	49.4	70.4
	QOT-LDA	96.8	55.7	88.9	94.3
	QOI-LSA	17.2	26.2	56.9	50.3
	QOI-LDA	94.5	44.2	71.5	81.2
	データベース分割	36.9	13.6	52.3	72.7

# まとめ

- 評価実験結果により，提出しようとしている質問のみからダミー質問を生成する手法は 質問ログを持つ攻撃者から質問意図を保護することが困難であると考えられる．
- QOTとQOIは相互影響しないため， 両方同時に用いる手法の評価は今後の課題として挙げられる．
- どのような意味分析手法においても同じような強さを持つダミー質問を生成することも今後の課題として挙げられる．

# 参考文献

- Blei, David M., Andrew Y. Ng, and Michael I. Jordan. 2003. “Latent Dirichlet Allocation.” *Journal of Machine Learning Research* 3 (Jan): 993–1022.
- Deerwester, Scott, Susan T. Dumais, George W. Furnas, Thomas K. Landauer, and Richard Harshman. 1990. “Indexing by Latent Semantic Analysis.” *Journal of the American Society for Information Science* 41 (6).
- Fujii, Atsushi, Makoto Iwayama, and Noriko Kando. 2007. “Overview of the Patent Retrieval Task at the NTCIR-6 Workshop.” In *NTCIR*.
- Jansen, Bernard J., Amanda Spink, Judy Bateman, and Tefko Saracevic. 1998. “Real Life Information Retrieval: A Study of User Queries on the Web.” *SIGIR Forum* 32 (1): 5–17.
- Michael, B. and Tom, Jeller, J. (2006). A Face Is Exposed for AOL Searcher No. 4417749 - New York Times.

# 参考文献

- Miller, George A. 1995. “WordNet: A Lexical Database for English.” *Communications of the ACM* 38 (11): 39–41.
- Murugesan, M., and C. Clifton. 2009. “Providing Privacy through Plausibly Deniable Search.” In *Proceedings of the 2009 SIAM International Conference on Data Mining*, 768–79. Proceedings. Society for Industrial and Applied Mathematics.
- Pang, HweeHwa, Xuhua Ding, and Xiaokui Xiao. 2010. “Embellishing Text Search Queries to Protect User Privacy.” *Proc. VLDB Endow.* 3 (1–2): 598–607.
- Petit, Albin, Thomas Cerqueus, Antoine Boutet, Sonia Ben Mokhtar, David Coquil, Lionel Brunie, and Harald Kosch. 2016. “SimAttack: Private Web Search under Fire.” *Journal of Internet Services and Applications* 7 (1): 1.
- Wang, Peng, and Chinya V. Ravishankar. 2014. “On Masking Topical Intent in Keyword Search.” In *2014 IEEE 30th International Conference on Data Engineering*, 256–267. IEEE.

# 付録

# 類似度攻撃

---

**Algorithm 7** 類似度計算

---

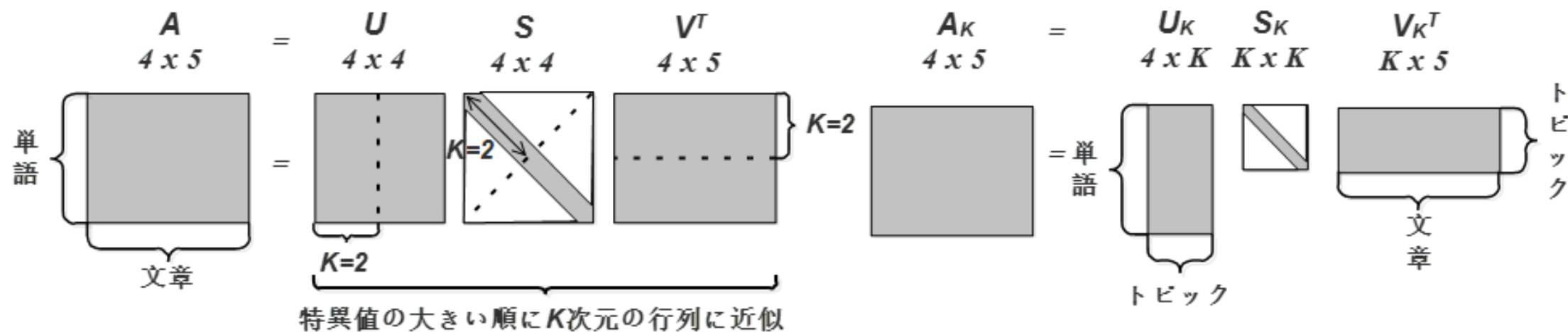
**Input:** 質問  $q$ , 質問者のプロフィール  $P_u$ , スムージングパラメータ  $\alpha$

- 1: **for**  $q_i \in P_u$  **do**
- 2:      $coef[i] \leftarrow 2 \cdot |q \cap q_i| \cdot \frac{1}{|q| + |q_i|}$
- 3:  $coef \leftarrow sort(coef)$
- 4:  $sim \leftarrow coef[0]$
- 5: **for**  $i \in [1, |P_u|]$  **do**
- 6:      $sim \leftarrow \alpha \cdot coef[i] + (1 - \alpha) \cdot sim$

**Output:**  $sim_{q, P_u}$

---

# 潜在意味分析(LSA)



# 潜在ディリクレ配置法(LDA)

- 確率生成モデルである
- 文書が複数の潜在的トピックからランダムに生成されると仮定しする
- トピック $t$ をそのトピックでの単語 $w$ の出現頻度 $\text{Pr}[w|t]$ で表す