

1

今後の情報社会プライバシーを考えるシンポジウム（2023/3/8）

PWS Cup 2019論文がPETSに採択されるまで

村上 隆夫（産総研）

目次

PWS Cup 2019とは？

何故PETSに投稿したか？

PETSに採択されるまで

PWS Cup 2019

▶ 特徴

- ▶ 世界初のトレース(移動履歴)を扱う匿名加工コンテスト
 - ▶ 2020年にNISTが移動履歴のコンテストを実施* これよりも長いトレースを扱う
- ▶ ID識別(再識別)とトレース推定の2軸での評価(両者の関係を明らかにする)

	2015	2016	2017	2018	2019
データセット	疑似マイクロデータ (世帯消費額)	UCI Dataset "Online Retail" (購買履歴)			位置情報
チーム数	13	15	14	14	21



*2020 Differential Privacy Temporal Map Challenge: <https://www.nist.gov/ct/pscr/open-innovation-prize-challenges/past-prize-challenges/2020-differential-privacy-temporal>

PWS Cup 2019

概要

- 各チームが自身のトレースを匿名加工し、他チームの加工トレースを再識別・トレース推定する(現実世界のように、攻撃と対策が競争し合う)



ユーザID	元トレース
1	$x_3 \rightarrow \dots \rightarrow x_2$
2	$x_6 \rightarrow \dots \rightarrow x_5$
$\vdots$	$\vdots$
n	$x_3 \rightarrow \dots \rightarrow x_4$

匿名加工

仮名ID	加工トレース
n+1	$\square \rightarrow \dots \rightarrow \square$
n+2	$\square \rightarrow \dots \rightarrow \square$
$\vdots$	$\vdots$
2n	$\square \rightarrow \dots \rightarrow \square$

ノイズ, 一般化, 削除

再識別

ユーザID (推定値)
2
1
$\vdots$
n

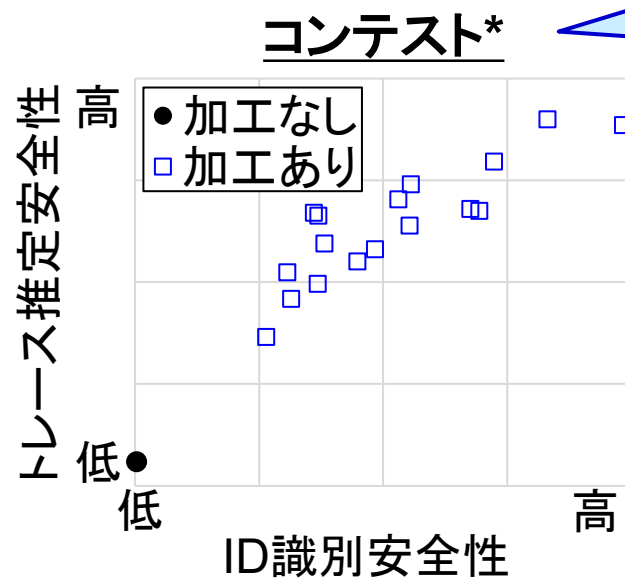
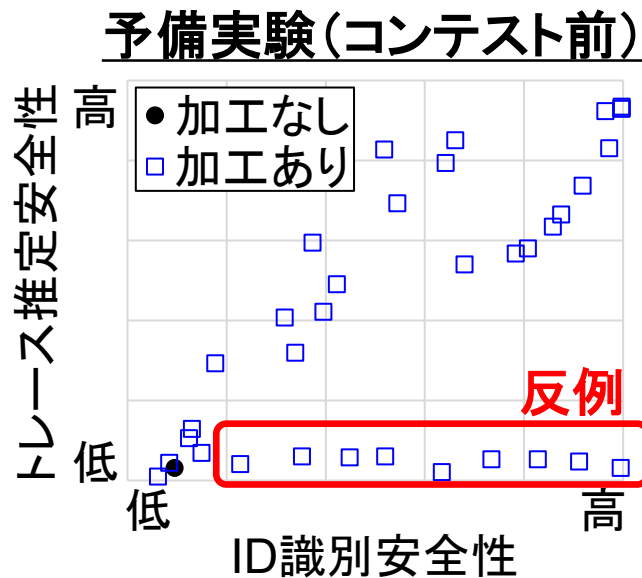
トレース推定

ユーザID	元トレース (推定値)
1	$x_2 \rightarrow \dots \rightarrow x_2$
2	$x_6 \rightarrow \dots \rightarrow x_4$
$\vdots$	$\vdots$
n	$x_4 \rightarrow \dots \rightarrow x_4$

PWS Cup 2019

▶ 主な結果

- ▶ ID識別に対して安全でも、トレース推定に対して安全とは限らない(反例が存在)
- ▶ **トレース推定に対して安全な加工は、ID識別に対しても安全**
→両方に対して安全な「優れた匿名加工」の指針を与える知見(法制度の橋渡し)



トレース推定安全性が
1位のチームに賞を付与

(*トレース推定対策部門の結果)

目次

PWS Cup 2019とは？

何故PETSに投稿したか？

PETSに採択されるまで

PETSとは？

▶ 特徴

- ▶ プライバシー分野の難関国際会議
 - ▶ 4大トップ会議(S&P, CCS, USENIX, NDSS): core rank = A*, 採択率<20%
 - ▶ PETS: core rank = A, 採択率 $\approx$ 20%
- ▶ 世界中のプライバシーの専門家が集結している
 - 査読のクォリティも高いと評判(「4大トップ会議より上」との声まであり)

何故PETSに投稿したか？

PWS Cupの目的に大きく関係する
(と私は考えています)

Cupの目的

▶ 【目的1】: 制度面での目的

- ▶ 優れた「匿名加工」の方法を明らかにする
← 標準的な匿名加工の方法が定まっていない



▶ 【目的2】: 技術面での目的

- ▶ (法制度を抜きにして, 純粹に) 優れた加工技術を明らかにする
← 移動履歴の匿名化・再識別の論文は山ほどあるが, 決定打がない



▶ 【目的3】: 教育面での目的

- ▶ 自身の加工スキルを高める, 仮名化だけでは不十分なことを理解する, etc.

Cupは目的を達成するために有効な「手段」か？

▶ 【目的1】: 制度面での目的

- ▶ 優れた「匿名加工」の方法を明らかにする
 ← 標準的な匿名加工の方法が定まっていない



▶ 【目的2】: 技術面での目的

- ▶ (法制度を抜きにして、純粹に) 優れた加工技術を明らかにする
 ← 移動履歴の匿名化・再識別の論文は山ほどあるが、決定打がない

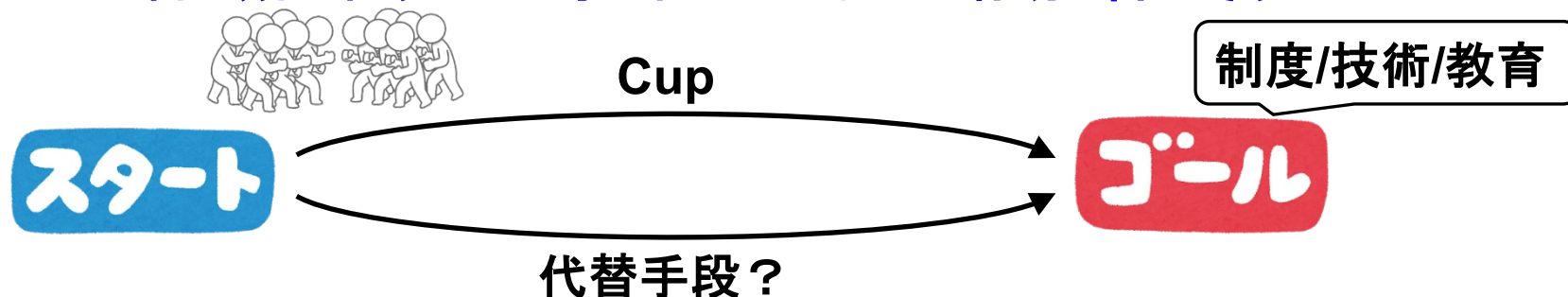


いわゆる「研究」(従来を上回る加工技術の提案→論文化)より有効と言えるか？

▶ 【目的3】: 教育面での目的

- ▶ 自身の加工スキルを高める, 仮名化だけでは不十分なことを理解する, etc.

皆で競い合うことで身に付くものなので有効と言えそう

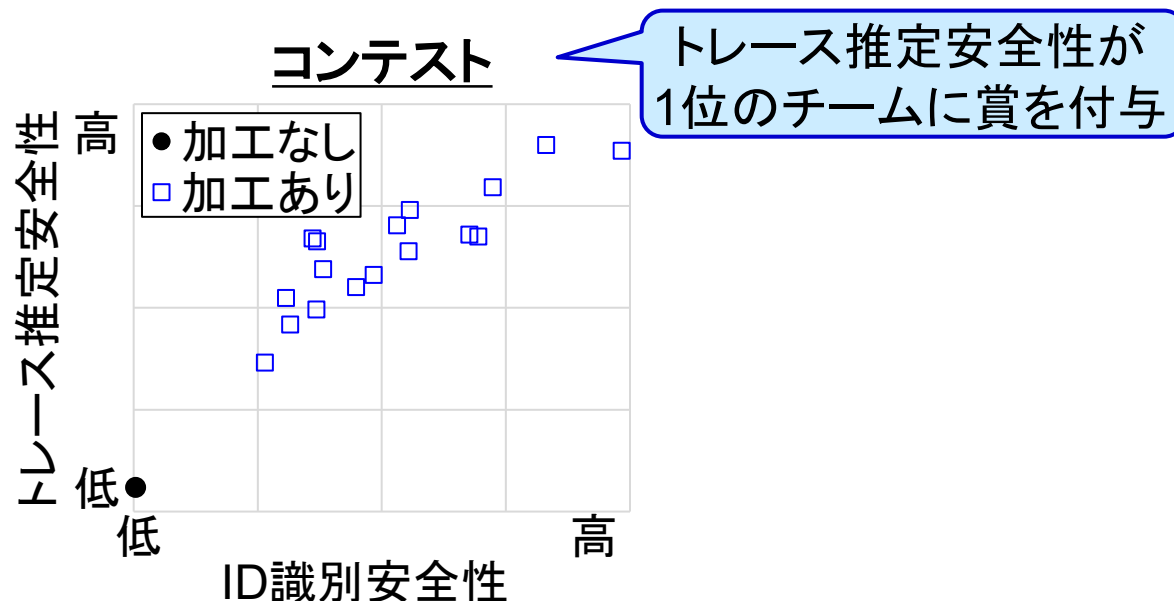


Cupは目的を達成するために有効な「手段」か？

- ▶ Cupと研究（加工技術の提案→論文化）との違い
 - ▶ Cupは、**現実世界のように攻撃と対策が競争し合う**（お互い攻撃し合う）



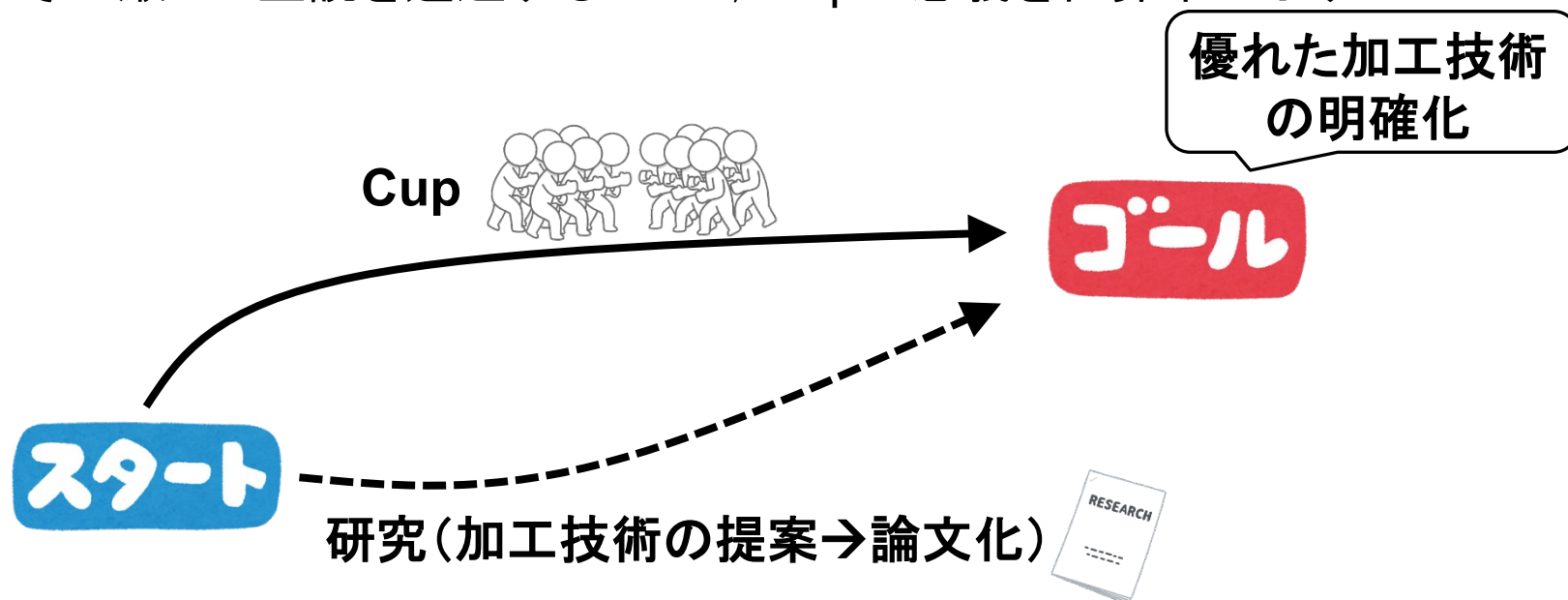
- ▶ その違いによってどのような「知見」が得られたか？
 - ▶ **「トレース推定に対して安全な加工は、ID識別に対しても安全」**
 ← 熾烈な競争の上で得られた結論なので、割とvalidだと言える



何故PETSに投稿したか？

▶ 【理由1】: Cupの目的達成のため

- ▶ Cupが目的達成のために有効な「手段」か？を含めて意義が厳しく問われる
- ▶ その厳しい査読を通過することで, Cupの意義を世界中に示す



▶ 【理由2】: Cupの知名度を上げる

- ▶ 世界中のプライバシー研究者にPWS Cupを知ってもらう

目次

PWS Cup 2019とは？

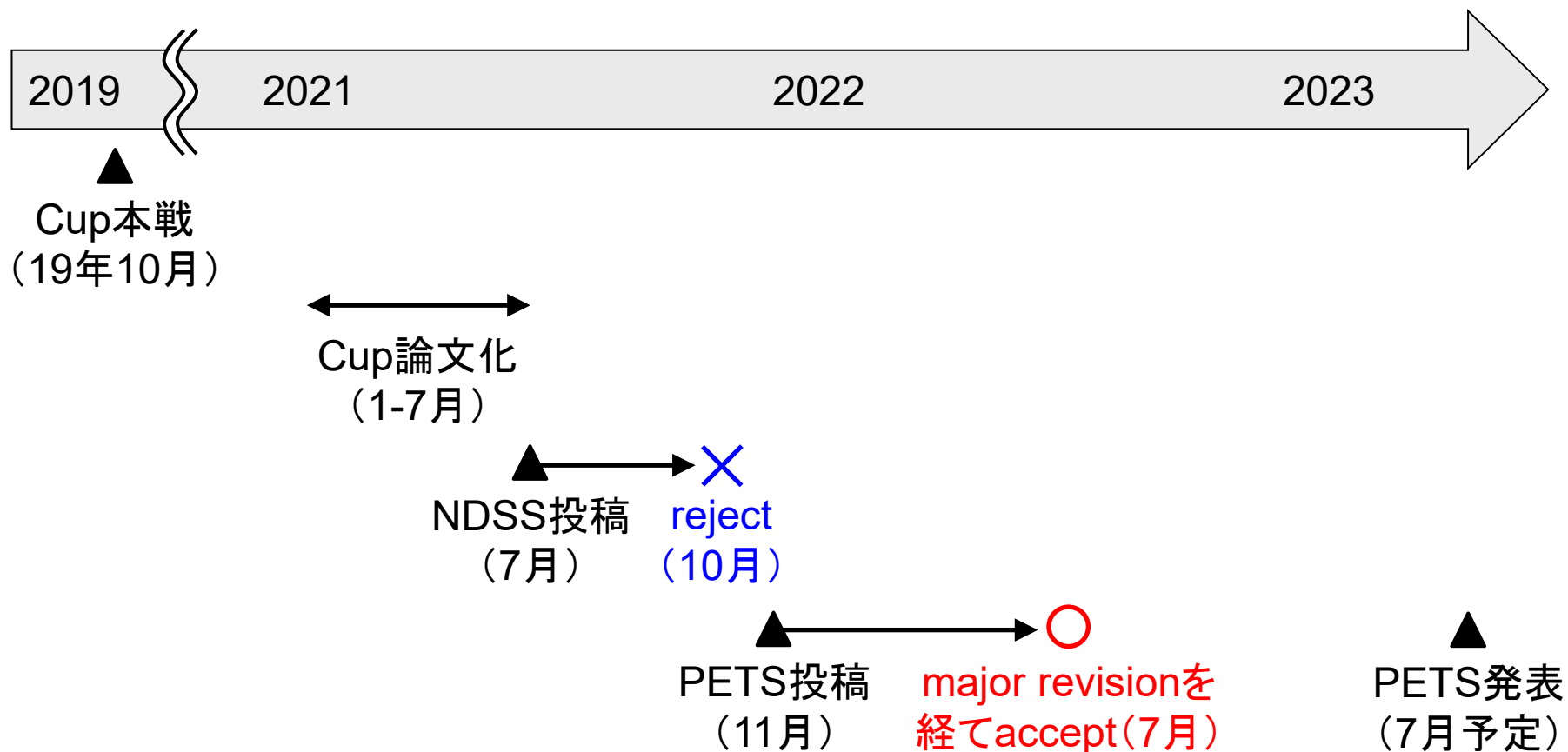
何故PETSに投稿したか？

PETSに採択されるまで

PETSに採択されるまで

▶ Cup開催からPETS採択まで

- ▶ 2021年1-7月: Cup論文化(2020年はUCSDに滞在していたため, 執筆遅れ)
- ▶ 2021年7月: NDSS投稿(✕切が近いのがNDSSだったため) → **reject**☹
- ▶ 2021年11月: PETS投稿 → **major revisionを経てaccept**😊



NDSSでの査読結果

▶ 評価

- ▶ 4点 (minor revision) : 1人, 3点 (major revision) : 2人, 2点 (reject寄り) : 1人
- ▶ rebuttal後, 2点の査読者がもう1人追加されてreject

▶ 主な査読コメント (meta-review)

1. 教育目的には間違いなく有益だろう (cool idea!) 一方, 教育より広い視点で見ると, Cupでどれだけ「新規な」知見が得られたのかが不明確



Cupで得られた知見 (ID識別とトレース推定の関係 + α) をより明確化

2. NDSSはややスコープから外れているかも



完全にスコープがfitするPETSに切り替えて再投稿

PETSでの査読結果

▶ 評価

- ▶ 5点(完全accept):2人, 2点(reject寄り):2人
- ▶ → major revision (→ 修正して再投稿後, accept)

▶ 主な査読コメント(meta-review)

1. 従来の研究(state-of-the-art)と比べて, どれだけ有効 or 新規な加工/攻撃技術が得られたのか, より明確にすべき



**winner algorithmsをappendixからmainに移動し, 従来との違いを明確化
(「鋼鉄の錬金術師」さん, 「またぼっち」さん, どうも有難うございました)**

2. 「トレース推定に対して安全な加工は, ID識別に対しても安全」という主な知見をもっと補強し, それがもたらすimplicationを明確にすべき

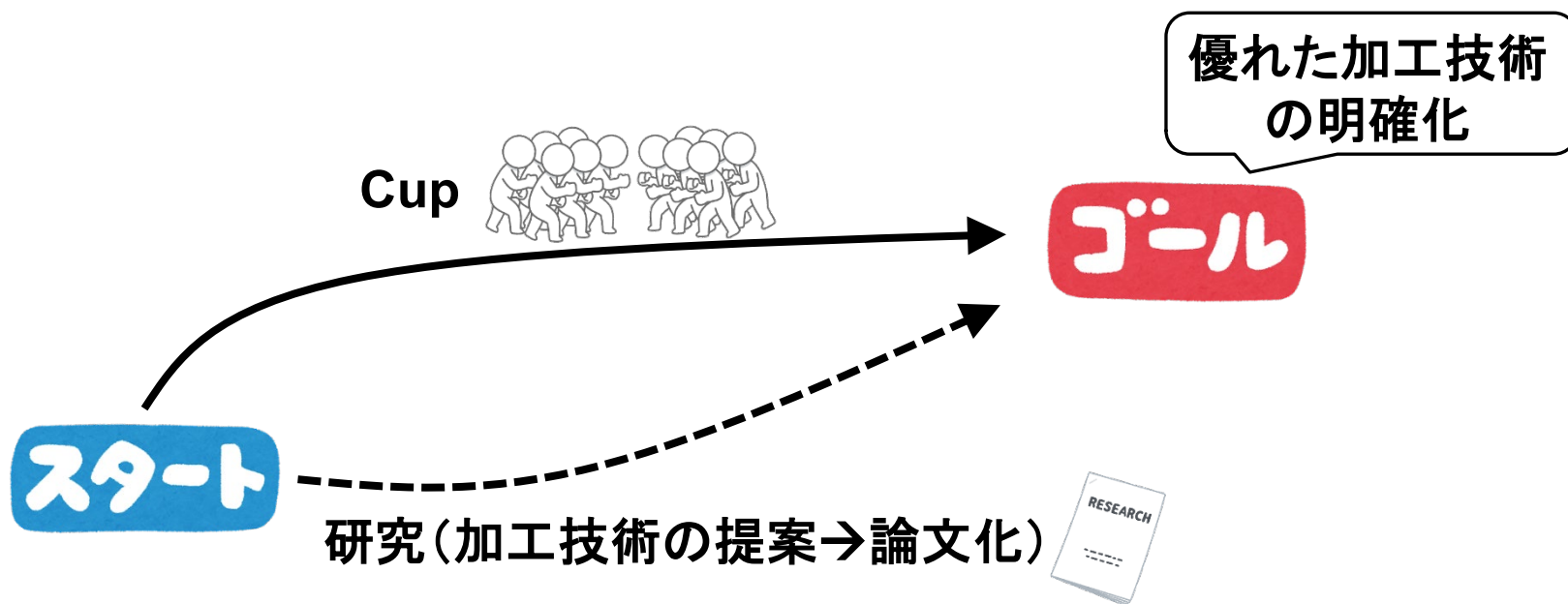


本分野でpopularな有用性・安全性指標を用いても, 本知見が得られることを示し, 本知見が「両リスクに対して安全な加工方法」の指針を与えることを明記

まとめ

▶ PETS

- ▶ Cupが、代替手段(研究)との比較を通して、どれだけ目的達成のために有効なのかがモロに問われた
- ▶ 無事、査読を通過できたので、Cupの意義が世界に向けて発信できた(はず)



共著者(運営委員)の皆様, それ以外の関係者の皆様, どうも有難うございました!