データ拡張による クリーンな少量データからの 高信頼モデルの構築と評価

山崎 啓介

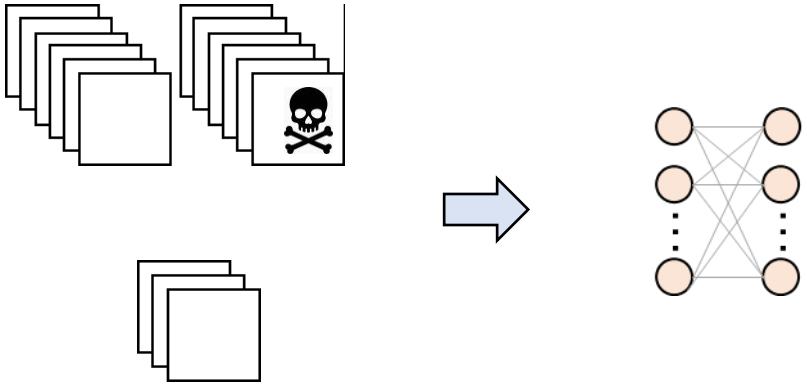
国立研究開発法人 産業技術総合研究所 人工知能研究センター

機械学習研究チーム 研究チーム長

大規模モデル構築におけるデータ不足問題

- 領域特化型モデルの構築・活用が広まり、モデル規模も増大
- 特化型モデル学習のためのデータは領域によってクリーンであることが条件
  - プライバシー、著作権などの侵害リスク
- **汚染されていないクリーンで安全なデータ収集には限界**があり慢性的な**データ不足が深刻化**

多量データはクリーンであることの保証が困難



ロバストで高性能なモデルの構築が困難

クリーンなデータは少量しか収集できない

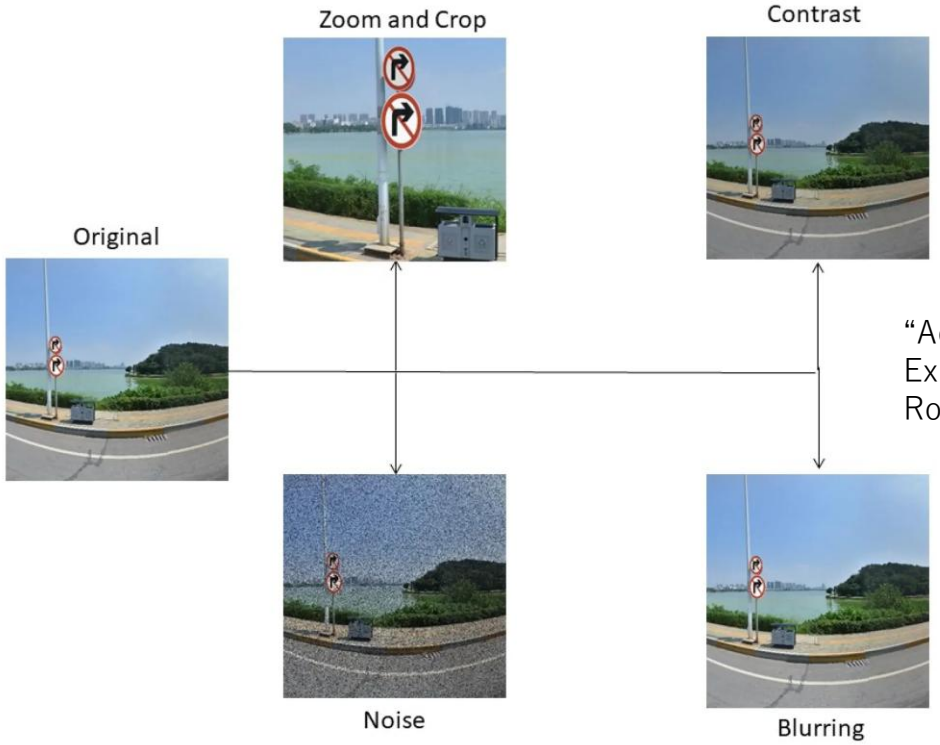
データ不足によるモデル挙動の弊害

- データが不十分なモデル：挙動が不安定、精度が不十分などの問題
- ノイズやマスクを付加するとモデルが致命的な判断ミスを犯す**敵対的攻撃がリスク**
- これらの問題に対し、限られたクリーンなデータを変換により増強する「**データ拡張**」**が有効**
- ただし拡張したデータセットが常に高性能なモデルを保証するものではない
- 学術の各分野においても拡張手法に対する体系的な方法論や標準的な精度評価は未成熟



誤認識される道路標識

“A Small Network MicronNet-BF of Traffic Sign Classification” より

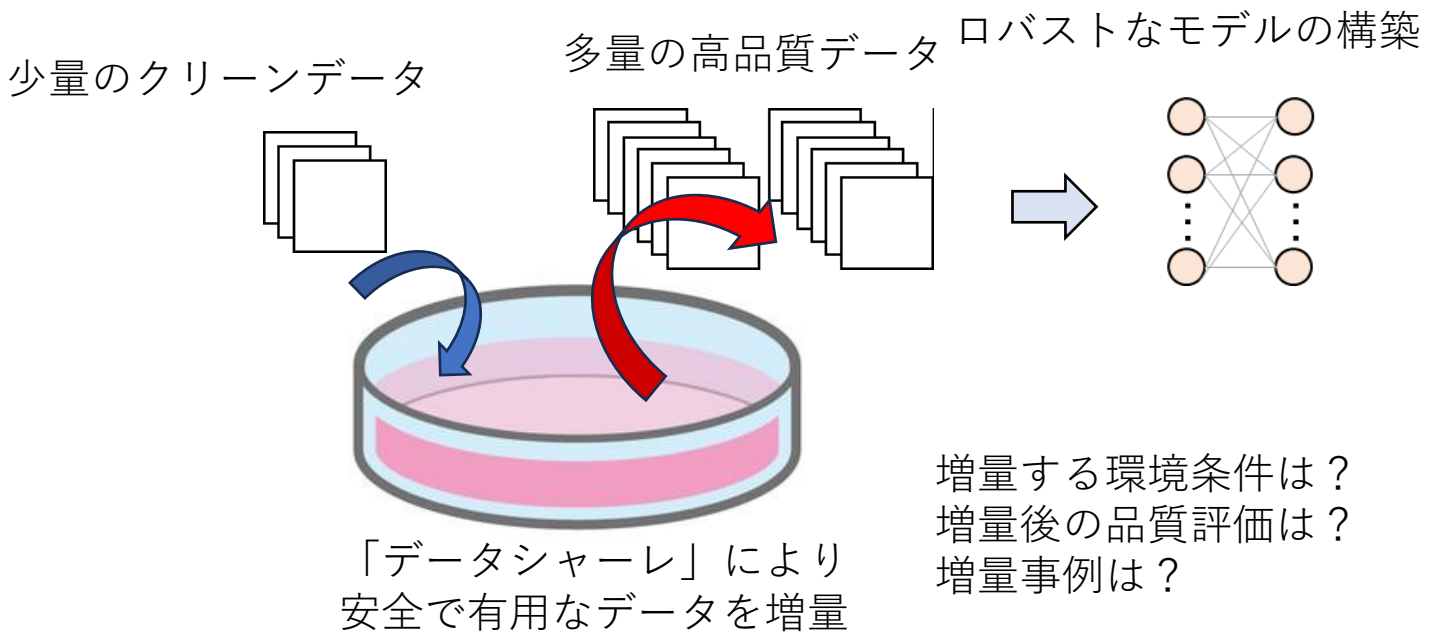


“Advancing Traffic Sign Recognition: Explainable Deep CNN for Enhanced Robustness in Adverse Environments” より

１つのデータを複数の変換で拡張し性能向上

目的：学習データ管理技術構築とフレームワークの確立

- データ拡張を行う「データシャーレ」による安全で有用なデータの管理技術
- 少数のクリーンデータからデータを増強し高信頼なモデル構築を支援するフレームワーク



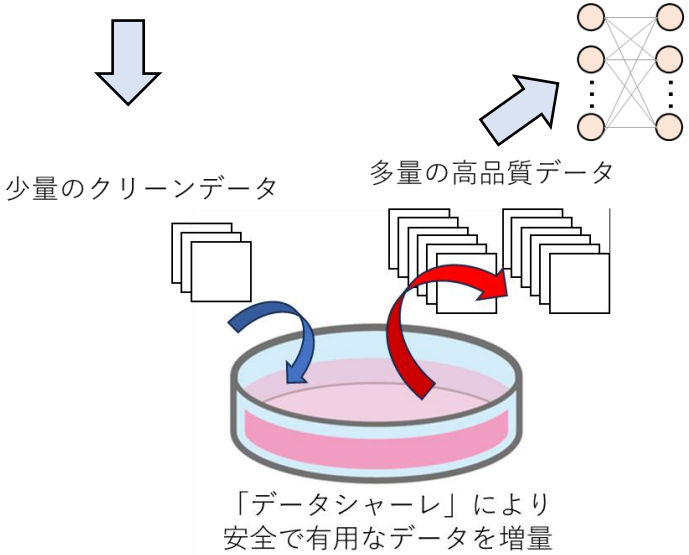
フレームワーク構築に必要な指標と有効利用のための機能

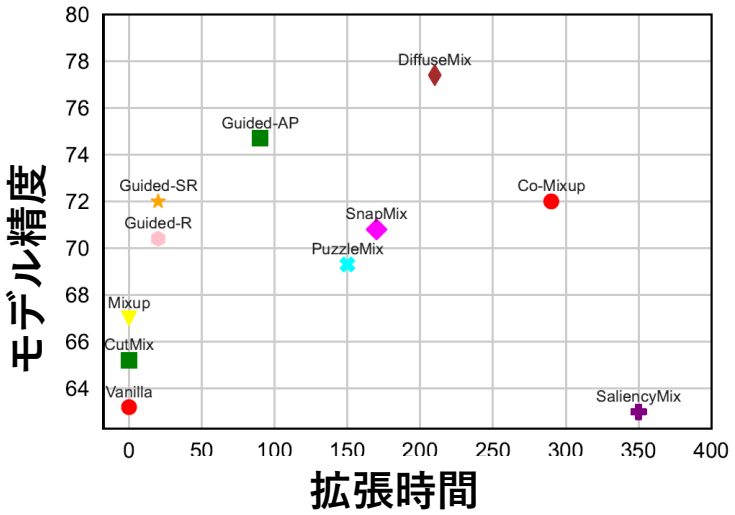
- フレームワーク構築に必要な設定・指標
  - データセットを表現する指標
  - データ拡張の設定
  - モデル学習の設定
  - 性能評価指標

- フレームワーク活用に必要な機能
  - 性能評価の可視化
  - 参照可能な性能評価カタログ

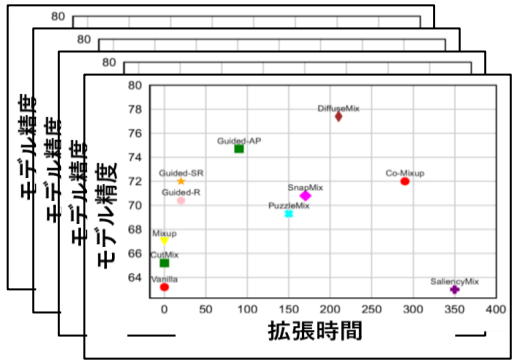
属性指標：
＋ データ数
＋ 拡張率
＋ 拡張方法, etc.

性能指標：
＋ モデル精度
＋ 拡張時間, etc.





性能指標の可視化の例
(属性指標によるプロット)



典型的な拡張方法のカタログ化

学習データ拡張に基づく増量データの品質保証と
安全なデータ管理方法に関するガイドラインの策定へ

産総研
ともに挑む。つぎを創る。

◘ベンチマークデータセット（画像）における各指標の洗い出しとカタログ作成

成果物

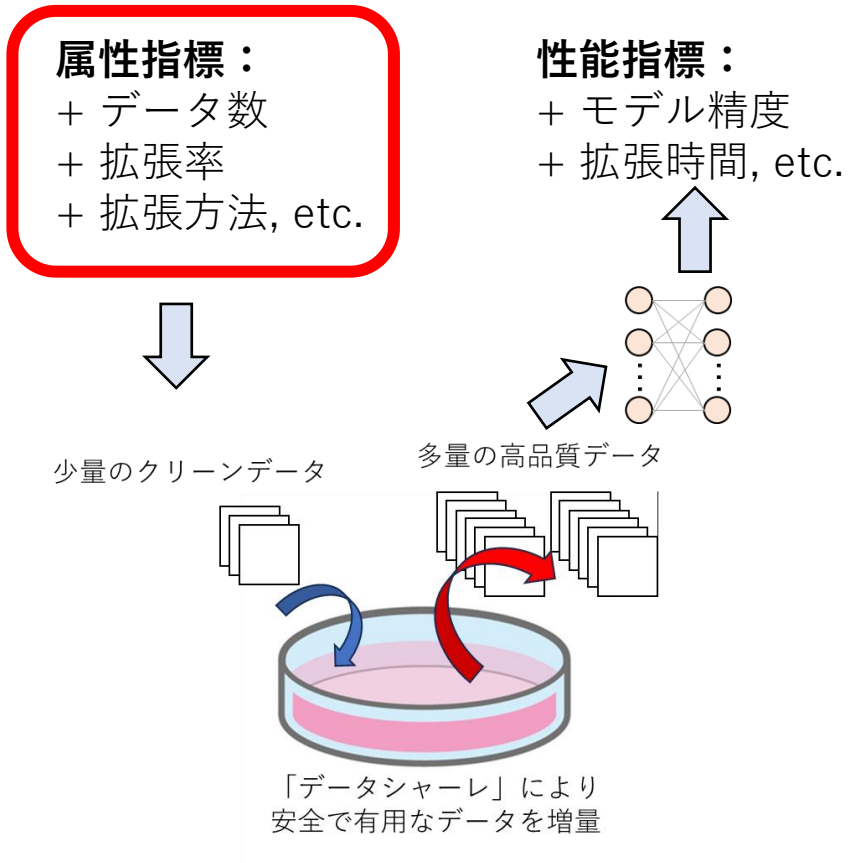
名称	説明	提供方法	評価観点
データセット属性指標リスト	データセットの属性が品質に及ぼす影響を調べる際に使用	PDF	データ品質
学習後のモデル評価指標リスト	モデルの精度や拡張にかかる時間など学習中や学習後の評価の仕方についてまとめたもの	PDF	ロバスト性
典型的手法における評価カタログ	典型的なデータ拡張方法においていくつかの評価指標に基づいて評価を可視化したカタログ。ユーザのデータを拡張する際の参考として。	PDF	ロバスト性
評価カタログを用いた拡張方法の評価実施レポート	新たな拡張手法を考案した際、上記のカタログと照らし合わせることにより、評価を行う手順を示したもの。	PDF	検証可能性

AIセーフティ強化：AIセーフティ評価管理基盤技術
項目１－１－４”収集後の学習データのセーフティ管理技術の研究開発”に掲載
https://qai.pj.aist.go.jp/aisafety1/results/2025/1-1-4/index.html

データセット属性指標

- データセットの特徴を表す指標を列挙
- 手元のデータと類似する過去事例（カタログ内）から適切な拡張方法・条件を見出す

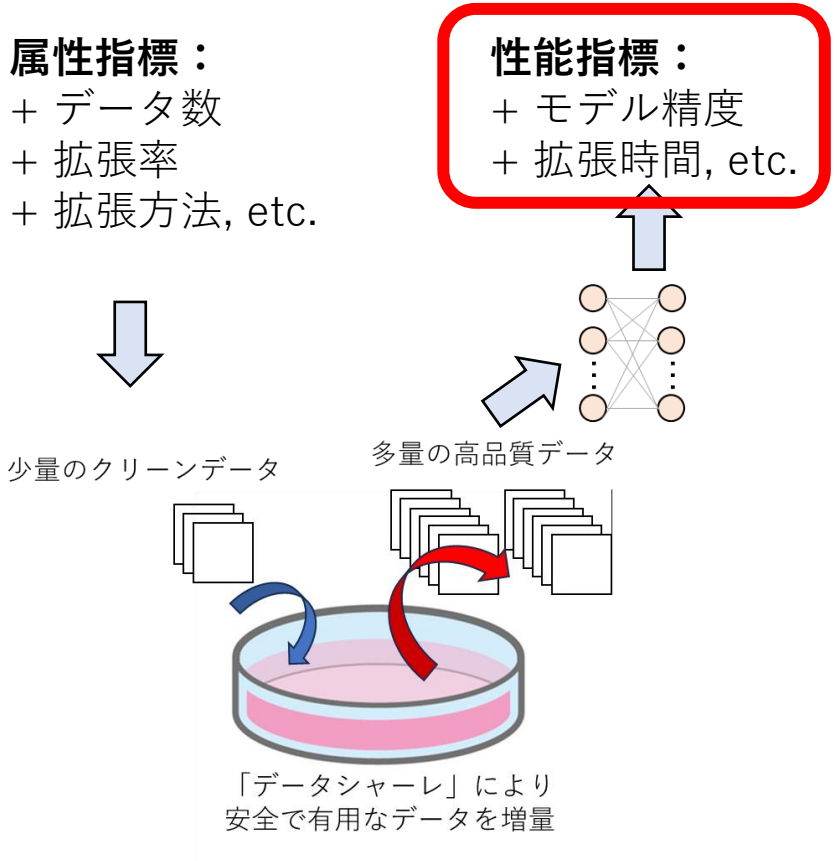
- データ数
- クラス数
- クラスの割合
- クラス内分散
- クラス間距離
- クラス間相関　など



モデル性能指標

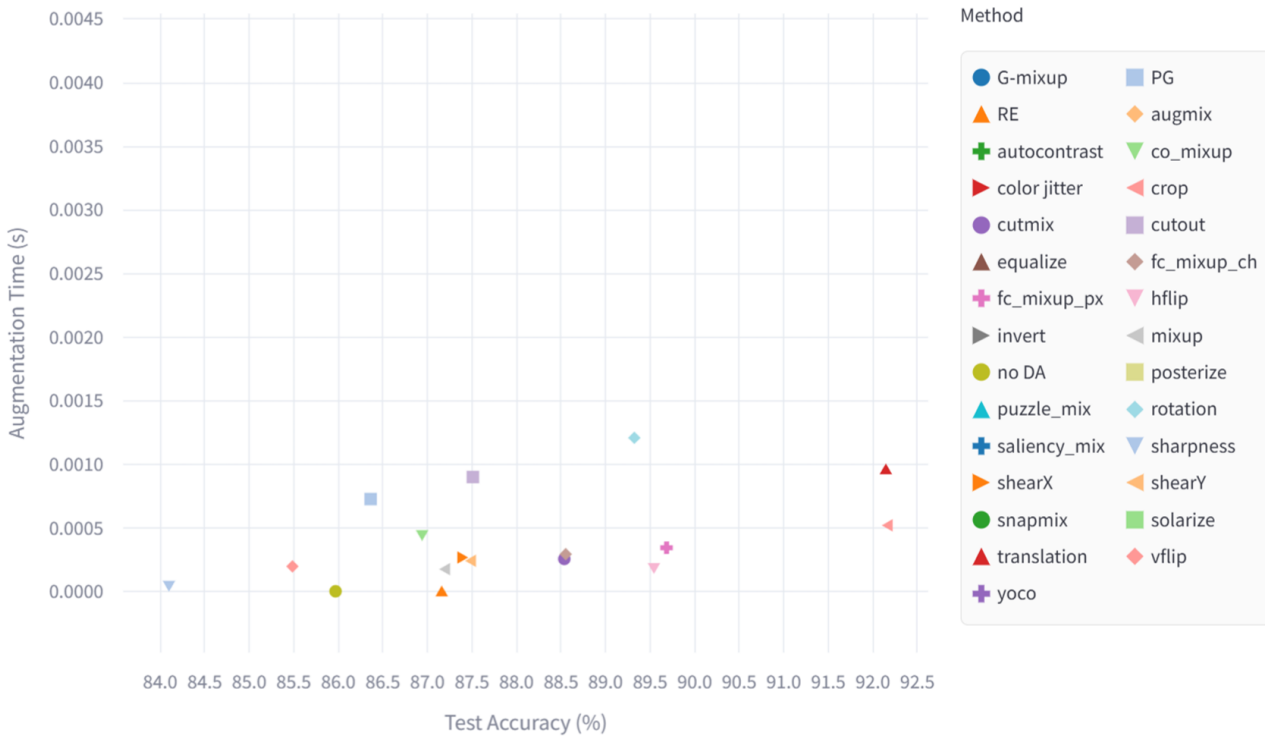
◘モデルの性能・データ拡張の複雑度を表す指標を列挙
◘特化型モデルのタスクで評価したい指標を過去事例（カタログ内）を参考に適切な拡張方法・条件を見出す

- Top-1 accuracy
- Top-5 accuracy
- Augmentation Time
- Validation accuracy
- Training Loss
- Precision
- Recall
- Macro-F1
- AUROC など



評価指標の可視化とカタログ

- モデル評価指標を可視化、２つの指標を選択し比較可能
  - 拡張方法・条件、モデル学習設定ごとにプロット
- カタログ化
  - 典型的な拡張方法やモデル構成による学習を網羅的に実施
  - ユーザのタスクにおける評価指標のカタログを参照し適切な拡張方法・条件を見出す



可視化の例：

- 横軸：精度
- 縦軸：データ拡張に要する時間
- プロット：データ拡張方法

右下の領域が高精度で高速な拡張を示す

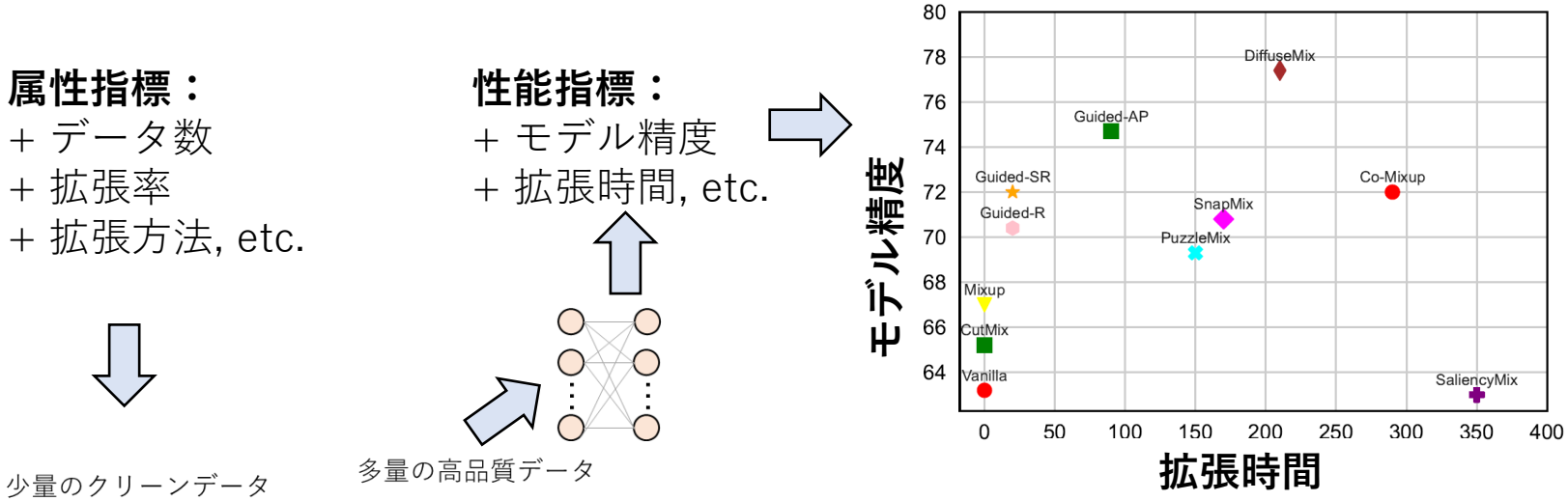
カタログ利用による最適拡張条件の推薦システムへ

- ユーザ保有のデータセット→データセット属性指標（メタデータ）を抽出
- ユーザのタスク評価基準→注目すべき性能指標を選択
- カタログを参照し最適なデータ拡張方法・条件を見出す

機密性の高いユーザ保有データでもメタデータと評価指標のみから最適条件を推薦可能に

属性指標：
＋ データ数
＋ 拡張率
＋ 拡張方法, etc.

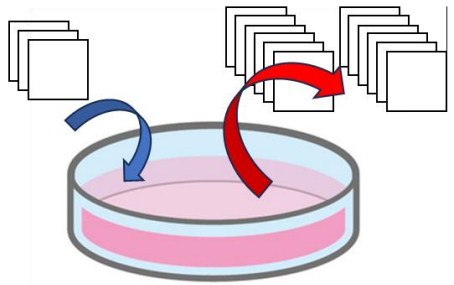
性能指標：
＋ モデル精度
＋ 拡張時間, etc.



カタログを参照

少量のクリーンデータ

多量の高品質データ



「データシャーレ」により
安全で有用なデータを増量

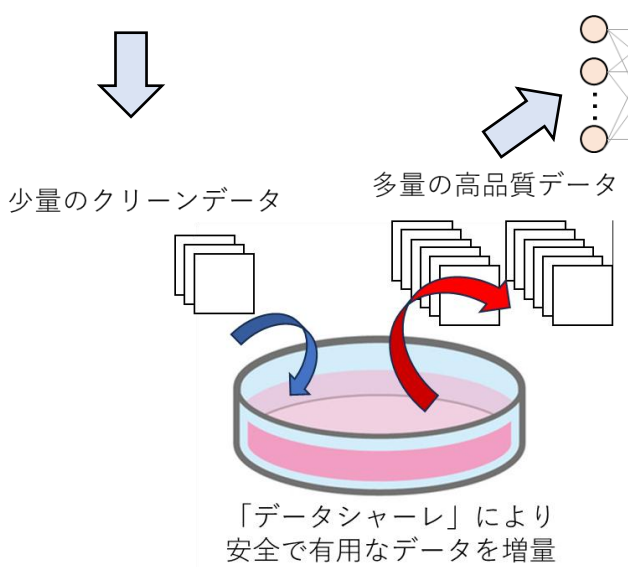
進行中の研究開発項目

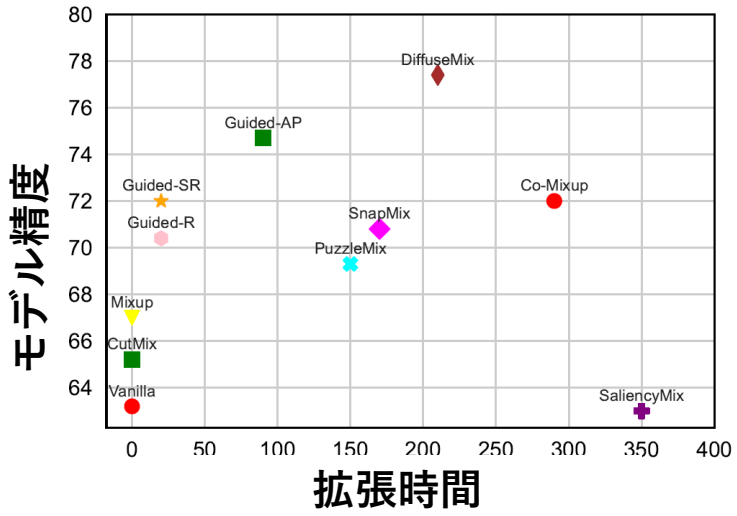
- 時系列データにおけるカタログ化
  - データのモダリティの多様化
  - モダリティによる指標や拡張法の共通化・差別化

- カタログからの最適設定探索自動化
  - カタログのプロットを内挿可能にする平滑化および最適化技術

属性指標：
＋ データ数
＋ 拡張率
＋ 拡張方法, etc.

性能指標：
＋ モデル精度
＋ 拡張時間, etc.





カタログを参照

今後の方向性

- データセットをマルチモーダル化
- システムを公開、ユーザのカタログへの登録を可能にし、カタログを強化
- データの増強（シャーレ内の機能）を合成データやシミュレーションデータへ拡張

