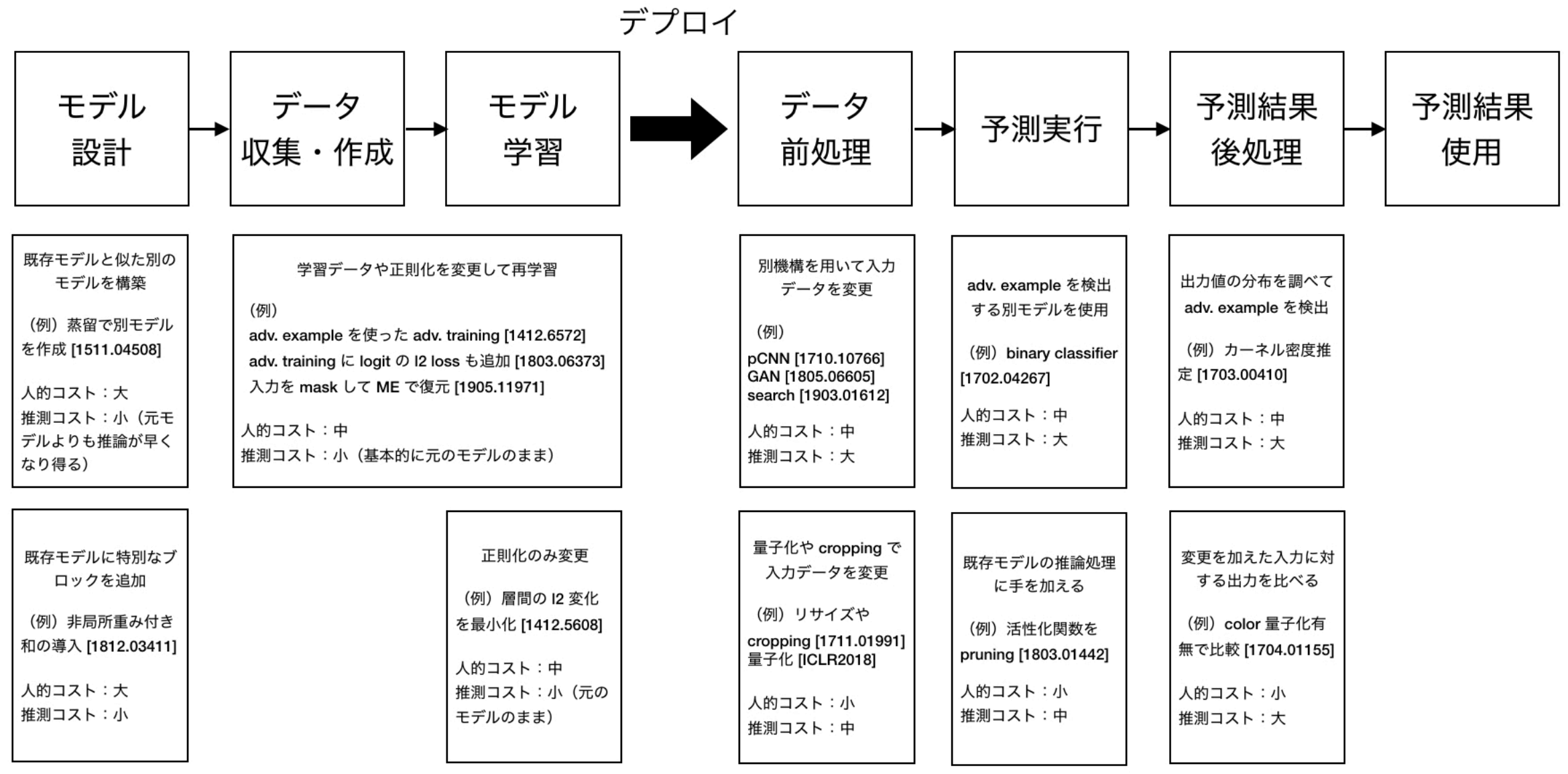
デプロイ
モデル設計
データ収集・作成
モデル学習
データ前処理
予測実行
予測結果後処理
予測結果使用
既存モデルと似た別のモデルを構築
（例）蒸留で別モデルを作成 [1511.04508]
人的コスト：大
推測コスト：小（元モデルよりも推論が早くなり得る）
学習データや正則化を変更して再学習
（例）
adv. example を使った adv. training [1412.6572]
adv. training に logit の l2 loss も追加 [1803.06373]
入力を mask して ME で復元 [1905.11971]
人的コスト：中
推測コスト：小（基本的に元のモデルのまま）
別機構を用いて入力データを変更
（例）
pCNN [1710.10766]
GAN [1805.06605]
search [1903.01612]
人的コスト：中
推測コスト：大
adv. example を検出する別モデルを使用
（例）binary classifier [1702.04267]
人的コスト：中
推測コスト：大
出力値の分布を調べて adv. example を検出
（例）カーネル密度推定 [1703.00410]
人的コスト：中
推測コスト：大
既存モデルに特別なブロックを追加
（例）非局所重み付き和の導入 [1812.03411]
人的コスト：大
推測コスト：小
正則化のみ変更
（例）層間の l2 変化を最小化 [1412.5608]
人的コスト：中
推測コスト：小（元のモデルのまま）
量子化や cropping で入力データを変更
（例）リサイズや cropping [1711.01991]
量子化 [ICLR2018]
人的コスト：小
推測コスト：中
既存モデルの推論処理に手を加える
（例）活性化関数を pruning [1803.01442]
人的コスト：小
推測コスト：中
変更を加えた入力に対する出力を比べる
（例）color 量子化有無で比較 [1704.01155]
人的コスト：小
推測コスト：大