理研AIP-NEC連携センターのこれまでの成果報告

宮野 博義

理研AIP-NEC連携センター　副連携センター長

日本電気株式会社 バイオメトリクス研究所 所長代理

2021年度

AIPシンポジウム成果報告会

RIKEN　AIP 革新知能統合研究センター Center for Advanced Intelligence Project

連携センターで実現したい AIの社会実装加速

RIKEN AIP Center for Advanced Intelligence Project

AIの社会実装を加速させ、安全・安心で効率的な社会を実現

AIの社会実装加速に向けた課題

- AIの社会実装加速に大きな壁となる大量学習データの不要化
- AI活用による自動化が進み、複数AI間での競合がある中での最適化
- 社会実装の加速に向けたAIの社会受容性の考慮
- AIのチューニングに必要となるハイパーパラメータ最適化の手間削減

理研AIP-NEC連携センターの活動

AIの社会実装加速に向けた課題

- AIの社会実装加速に大きな壁となる大量学習データの不要化
- AI活用による自動化が進み、複数AI間での競合がある中での最適化
- 社会実装の加速に向けたAIの社会受容性の考慮
- AIのチューニングに必要となるハイパーパラメータ最適化の手間削減

５つのテーマで活動

1．少量の学習データで高精度を実現する学習技術の高度化

2．未知状況での意思決定を支援する学習／AI技術の高度化

3．複数AI間の調整にかかわる学習技術の理論解析

4．実環境を想定したAXのリスク評価・対策

5．汎用的、パラメータフリーなブラックボックス最適化技術の開発

各テーマの活動期間・内容サマリ

- **当初は3テーマで活動を開始。逐次、AIに対する社会ニーズの変化や技術成果の状況に応じてテーマを新設・変更**

活動テーマ

活動テーマ	～2019	2020	2021
1．少量の学習データで高精度を実現する学習技術の高度化	異常事象など一部種類の現場データ無い場合に適応する学習手法（ACML2019,WACV2020）		真のラベルよりも低コストで入手可能な弱ラベルを用いた学習手法の改善（ICML2021）
2．未知状況での意思決定を支援する学習／AI技術の高度化	論理推論のロバスト性を強化（観測との矛盾を高速検知）（産総研との三者連携、NeurIPS2019 、FLAIRS2020 ）	サイバー攻撃手口推定の実問題で有効性確認	卒業
3．複数AI間の調整にかかわる学習技術の理論解析	AI間の交渉戦略理論：未知制約付きベイズ最適化高速手法を考案（産総研との三者連携、SIP）		製造・物流で広く使われるスケジュール調整問題をターゲットにした最適化手法（今後、学会発表予定）
4．実環境を想定したAXのリスク評価・対策	新規立上	顔認証の運用を加味したAX攻撃手法の提案・対策手法を考案（Biosig2021, IJCB2021）	卒業
5．汎用的、パラメータフリーなブラックボックス最適化技術の開発		新規立上	理論的に収束性を示す新手法を考案（今後、学会発表予定）

活動テーマ

	～2019	2020	2021
1．少量の学習データで高精度を実現する学習技術の高度化	異常事象など一部種類の現場データ無い場合に適応する学習手法（ACML2019,WACV2020）		真のラベルよりも低コストで入手可能な弱ラベルを用いた学習手法の改善（ICML2021）
2．未知状況での意思決定を支援する学習／AI技術の高度化	論理推論のロバスト性を強化（観測との矛盾を高速検知）（産総研との三者連携、NeurIPS2019 、FLAIRS2020 ）	サイバー攻撃手口推定の実問題で有効性確認	卒業
3．複数AI間の調整にかかわる学習技術の理論解析	AI間の交渉戦略理論：未知制約付きベイズ最適化高速手法を考案（産総研との三者連携、SIP）		製造・物流で広く使われるスケジュール調整問題をターゲットにした最適化手法（今後、学会発表予定）
4．実環境を想定したAXのリスク評価・対策	新規立上	顔認証の運用を加味したAX攻撃手法の提案・対策手法を考案（Biosig2021, IJCB2021）	卒業
5．汎用的、パラメータフリーなブラックボックス最適化技術の開発	新規立上	理論的に収束性を示す新手法を考案（今後、学会発表予定）	

テーマ１ 少量の学習データで高精度を実現する学習技術の高度化

RIKEN
AIP Center for Advanced Intelligence Project

- **産業応用上重要となる学習データ獲得困難な様々な事例に対応**

- **学習データ獲得困難な３タイプの事例**

①現場で発生する新たなニーズへの適応が必要な場合（新製品対応など）

- 毎回、大量の学習データを作成していては、時間的・人的コストがかかりすぎる
- ニーズへの迅速な対応ができない

②データの発生頻度が少ない場合（異常検知など）

- 異常データなどは、データ収集に時間がかかる
  例）1日1件発生しても、5,000件集まるまでに13年以上かかる

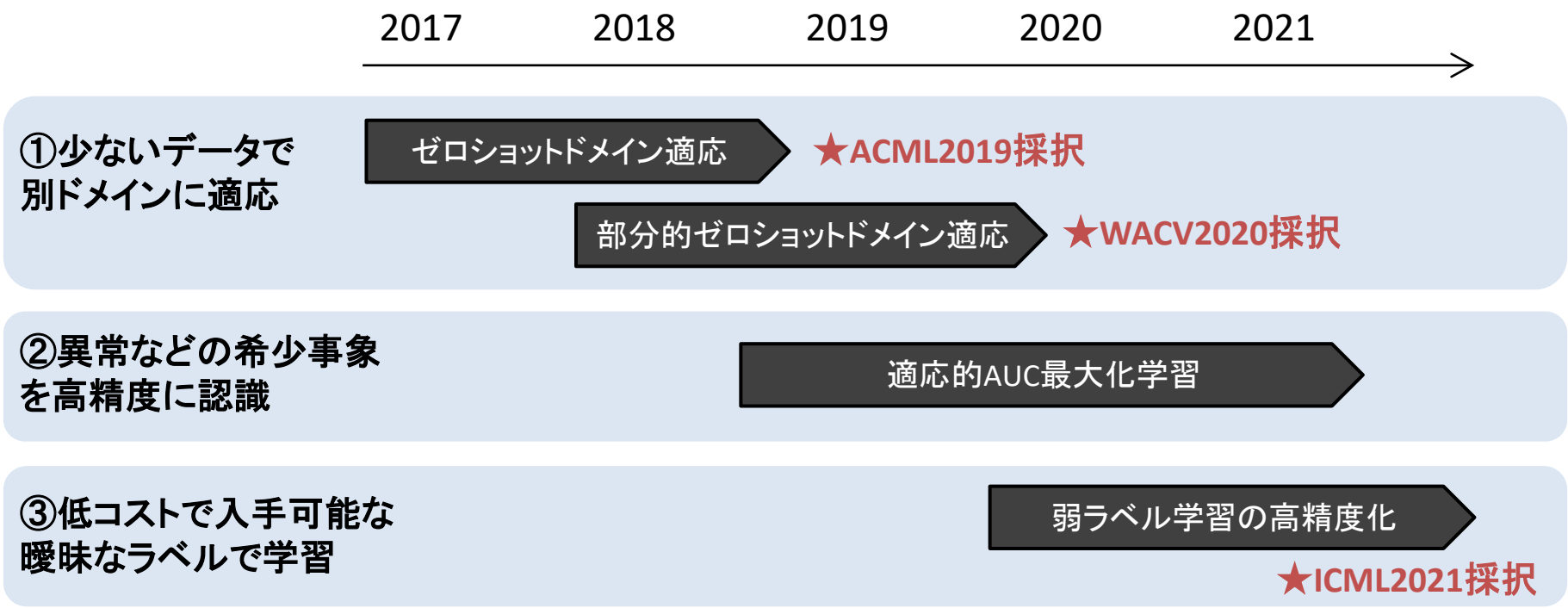
③正解付けコストが非常に高い場合（専門家の代替など）

- 医療データなどは、専門家でないと正解がつけられない

テーマ１：成果概要

活動の振り返り

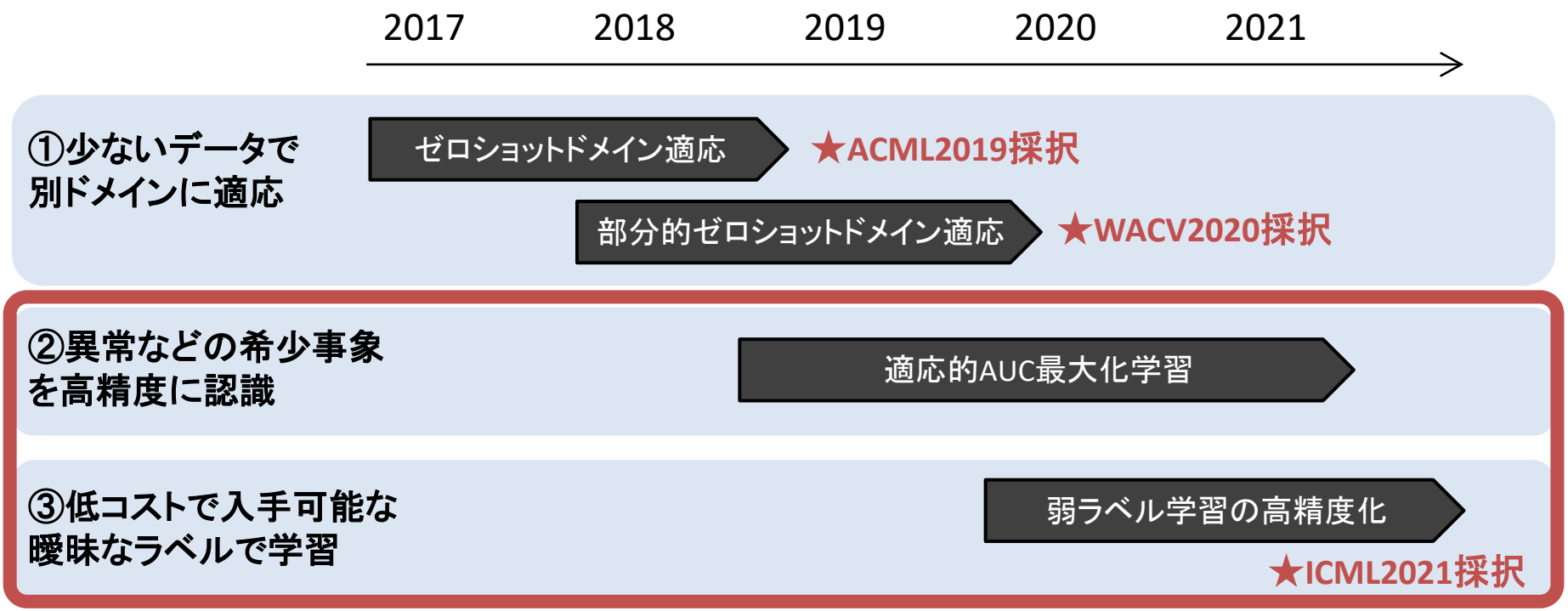
●深層学習の実用化に向けた問題を設定して、それぞれ基盤技術を開発



テーマ１：成果概要

活動の振り返り

●深層学習の実用化に向けた問題を設定して、それぞれ基盤技術を開発



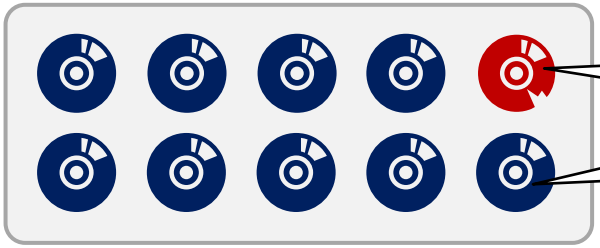
テーマ1：適応的AUC最大化学習（異常検知向け）

RIKEN Center for Advanced Intelligence Project

背景：異常などの希少事象のデータは、正常データに比べて非常に少ない

⇒ クラス間でデータ数が大きく異なる状況（クラス不均衡）

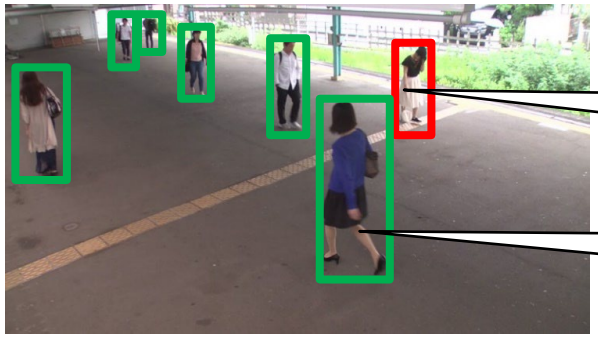
工業製品の検査検品



不良品（異常）のデータは**非常に少ない**

正常な製品のデータは**非常に多い**

防犯カメラ映像からのふらつき歩行検知



ふらつき歩行（異常）のデータは**非常に少ない**

通常歩行（正常）のデータは**非常に多い**

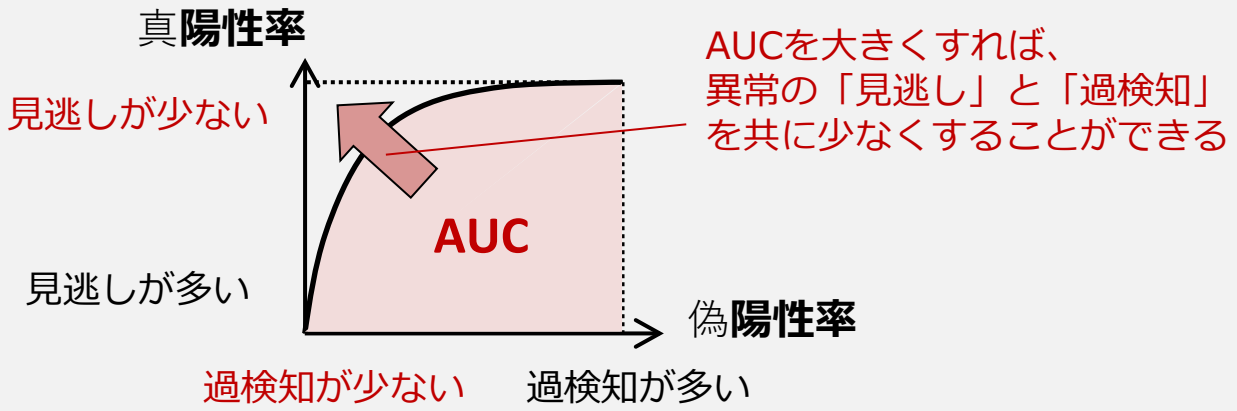
従来の「誤り最小化」に基づく学習では、識別モデルの学習が困難

（少ない異常データを無視して、全データを正常と判定すれば高精度を達成できるため）

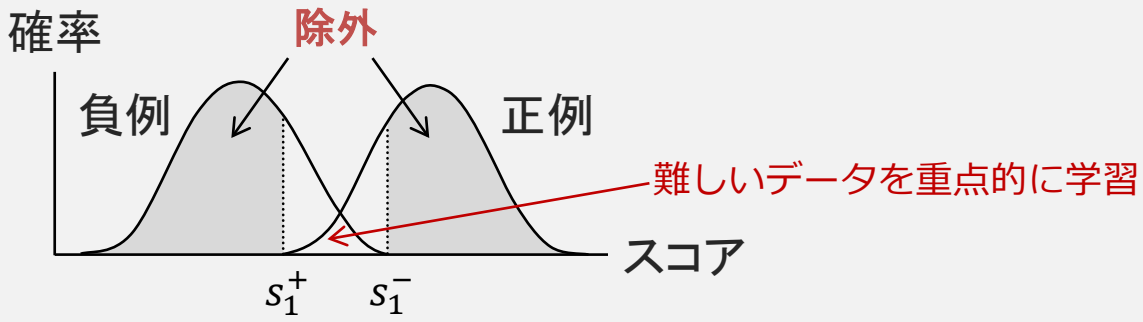
テーマ1：適応的AUC最大化学習（提案手法）

- **学習サンプル選別に基づく、AUC最大化学習**
  - ① AUC最大化により、少ない異常クラスを無視せずに学習
  - ② 識別が難しいサンプルのみを選別することで、効率よく学習

① AUC最大化



② 識別困難なサンプルで学習

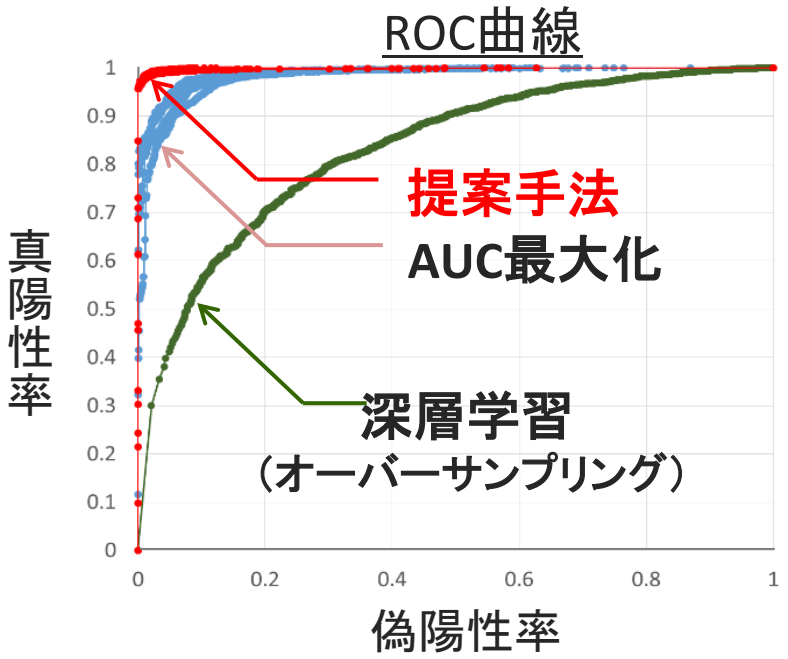


テーマ1：適応的AUC最大化学習（提案手法）

- **不均衡なデータに対して、提案手法の有効性を実証**

CIFAR-10（物体認識）
1クラス500枚を異常とし、残りの
全クラス4500枚を正常として学習

	見逃し率	過検知率
通常学習	0.5%	93%
AUC最大化	0.5%	27%
提案手法	**0.5%**	**3%**



- **工業部品の異常検知など、実データでも有効性を確認**

外観検査向けのNECの機械学習エンジン「RAPID」に搭載

例）屋外インフラ検査

例）精密素材の検品

※画像はgettyimagesの素材画像であり、あくまでイメージです。

テーマ1：弱ラベル学習の高精度化

背景：真のラベルよりも情報量が少ないが、低コストで入手可能な弱ラベルから学習できれば、学習データ作成のコストを大幅削減可能

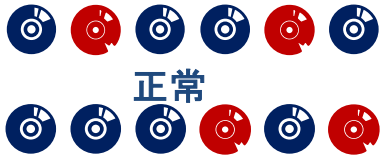
一般的に知られている弱ラベル学習の例

曖昧ラベル学習

車 or 飛行機　車 or トラック　船 or 飛行機

曖昧なラベルで学習

PU学習



一部の正例のラベルのみで学習

補ラベル学習

車ではない　船ではない　飛行機ではない

「～ではない」というラベルで学習

⇒ 物体検知への新クラス追加、部品の検査検品などに応用可能

弱ラベル学習の課題

- 弱ラベルを用いて、真のラベルに対する損失を再構成すると、
  訓練損失が下に非有界であるために過学習が生じ、精度が大幅に低下

テーマ1：弱ラベル学習の高精度化（理論的な成果）

アプローチ

- 1)弱ラベル学習を成功させる「良い」損失関数の条件を設定し、
  2)それを満たすような損失関数を設計することで、高精度な学習を実現

「良さ」の基準

① **Properであること**（クラスの事後確率を正しく推定できること）
- 弱ラベル学習を実現するための十分条件

② **下に有界であること**
- 深層学習のような複雑なモデルで過学習を軽減するために必要

上記①②を満たす損失関数の十分条件を理論導出

$F(\vec{v})$ を凸関数としたとき、$F(\vec{v}) - \max_y (R\vec{v})_y$ が下に有界ならば、
次の形をした損失関数は良い性質①②を満たす：

$$l(\vec{p}, y) = -(R^T \nabla F^*(\vec{p}))_y + F(\nabla F^*(\vec{p}))$$

ただし、$\vec{p}$ はクラス事後確率分布のベクトル表示、$F^*(\vec{p})$ は $F(\vec{v})$ の共役関数。

テーマ1：弱ラベル学習の高精度化（実験結果）

RIKEN AIP Center for Advanced Intelligence Project

導出した条件を満たすように損失関数を補正する正則化手法 Generalized Logit Squeezing (gLS)を考案し、実験的に有効性を確認

- gLSは弱ラベル学習だけではなく、教師あり学習にも適用可能

弱ラベル学習

	CIFAR-10
従来手法① (BC)	29.6%
従来手法② (BC+GA)	36.9%
提案手法　(BC+gLS)	**50.5%**

BC: Backward Correction
GA: Gradient Ascent

⇒ **大幅に精度向上**

教師あり学習

	CIFAR-100	CUB-200	商品認識 (実データ)
正則化なし	72.3%	46.6%	84.1%
重み減衰	78.8%	63.2%	85.2%
提案手法 (gLS)	**79.3%** (※)	**64.2%** (※)	**91.2%**

(※) 重み減衰＋gLS

⇒ **教師あり学習でも精度向上**

弱ラベル学習から一般の教師あり学習まで幅広い応用場面で活用

活動テーマ

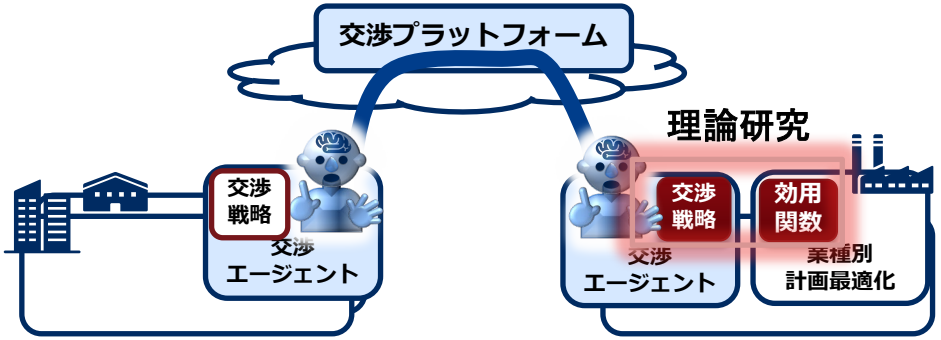
	～2019	2020	2021
1．少量の学習データで高精度を実現する学習技術の高度化	異常事象など一部種類の現場データ無い場合に適応する学習手法	真のラベルよりも低コストで入手可能な弱ラベルを用いた学習手法の改善	
	（ACML2019,WACV2020）	（ICML2021）	
2．未知状況での意思決定を支援する学習／AI技術の高度化	論理推論のロバスト性を強化（観測との矛盾を高速検知）	サイバー攻撃手口推定の実問題で有効性確認	卒業
	（産総研との三者連携、NeurIPS2019 、FLAIRS2020 ）		
3．複数AI間の調整にかかわる学習技術の理論解析	AI間の交渉戦略理論：未知制約付きベイズ最適化高速手法を考案	製造・物流で広く使われるスケジュール調整問題をターゲットにした最適化手法	
	（産総研との三者連携、SIP）	（今後、学会発表予定）	
4．実環境を想定したAXのリスク評価・対策	新規立上	顔認証の運用を加味したAX攻撃手法の提案・対策手法を考案	卒業
		（Biosig2021, IJCB2021）	
5．汎用的、パラメータフリーなブラックボックス最適化技術の開発	新規立上	理論的に収束性を示す新手法を考案	
		（今後、学会発表予定）	

15

テーマ３：複数AI間の調整にかかわる学習技術の理論解析

- AIが普及した社会において、個別企業内の最適化だけでなく、**AI間での交渉・連携を通して、社会全体を最適化**
- **事業上利用可能**であり、**汎用的に展開可能**な技術の理論研究を進める

- 活動内容



FY2018-19

様々な事業に適用可能な交渉戦略のための、相互情報量に基づく未知制約付きベイズ最適化

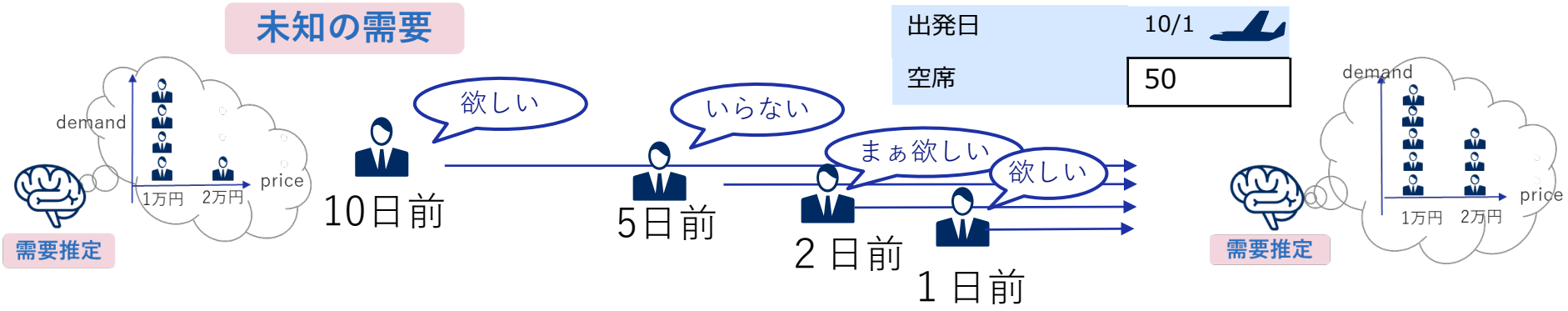
具体的な事業で利用するために、ターゲットを限定

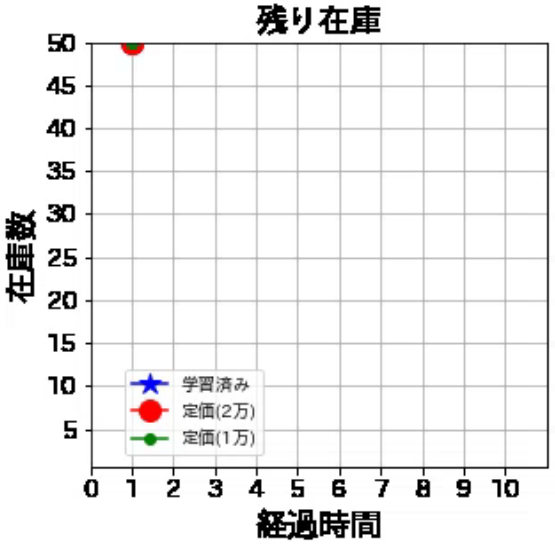
FY2020-21

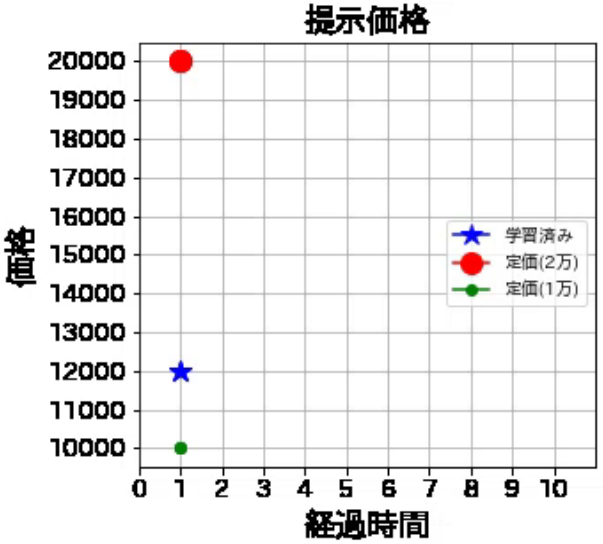
製造・物流で広く使われるスケジュール調整をターゲット設定
交渉の良さを測る効用関数のためのオンライン意思決定

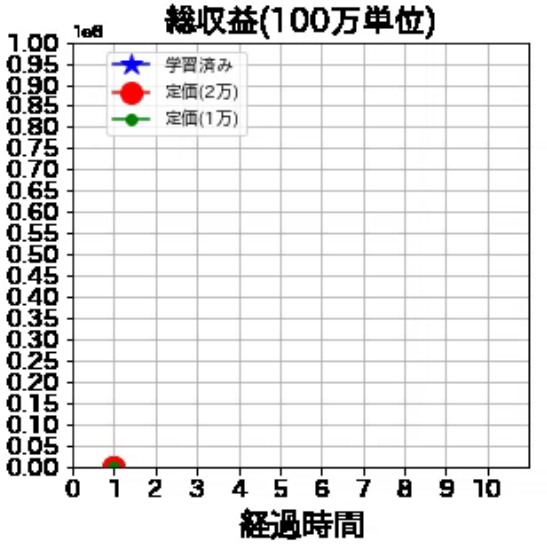
テーマ3：物流をターゲットにした最適化

- 物流の需要が未知の条件で、利益が最大となるよう輸送価格を動的決定
- 未知かつ動的需要下でのオンラインレベニュー最大化問題として定式化・解法を考案









活動テーマ

	～2019	2020	2021
1．少量の学習データで高精度を実現する学習技術の高度化	異常事象など一部種類の現場データ無い場合に適応する学習手法（ACML2019,WACV2020）		真のラベルよりも低コストで入手可能な弱ラベルを用いた学習手法の改善（ICML2021）
2．未知状況での意思決定を支援する学習／AI技術の高度化	論理推論のロバスト性を強化（観測との矛盾を高速検知）（産総研との三者連携、NeurIPS2019 、FLAIRS2020）	サイバー攻撃手口推定の実問題で有効性確認	卒業
3．複数AI間の調整にかかわる学習技術の理論解析	AI間の交渉戦略理論：未知制約付きベイズ最適化高速手法を考案（産総研との三者連携、SIP）		製造・物流で広く使われるスケジュール調整問題をターゲットにした最適化手法（今後、学会発表予定）
4．実環境を想定したAXのリスク評価・対策	新規立上	顔認証の運用を加味したAX攻撃手法の提案・対策手法を考案（Biosig2021, IJCB2021）	卒業
5．汎用的、パラメータフリーなブラックボックス最適化技術の開発	新規立上	理論的に収束性を示す新手法を考案（今後、学会発表予定）	

18

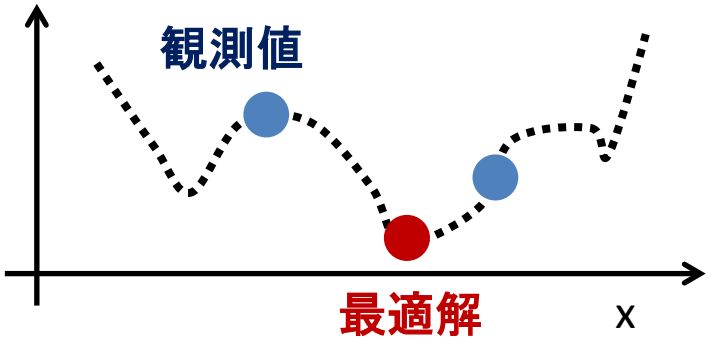
テーマ5：汎用的、パラメータフリーなブラックボックス最適化技術の開発

- **様々な実問題で必要とされるブラックボックス最適化の高度化**
  - **ブラックボックス最適化：具体形が未知（ブラックボックス）な目的関数に対する最適化問題**

関数f(x)の関数形は未知

xの値を決めればf(x)は観測可能

できるだけ少ない観測回数で f(x)を最小化する最適解xに近い解を見出したい

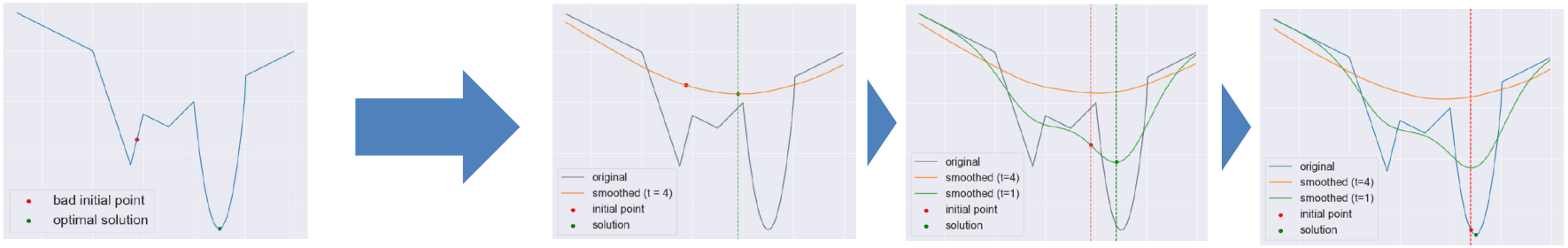


  - **機械学習におけるハイパーパラメータ最適化・モデル選択、実験計画、分子構造解析、創薬、推薦システム、マーケティング自動化など多くのアプリケーションが存在**

- **2021年度テーマを立ち上げ、活動を開始**
- **Zeroth-order optimizationと呼ばれるブラックボックス最適化を解く１つの枠組みを拡張した手法：single loop Gaussian homotopy (SLGH) 法を考案**
  - 様々な問題クラスに対し、理論的に収束性を証明
  - 「ブラックボックス分類モデルに対する敵対的攻撃」タスクで有効性を確認

テーマ５：活動成果概要

- 提案手法の考え方

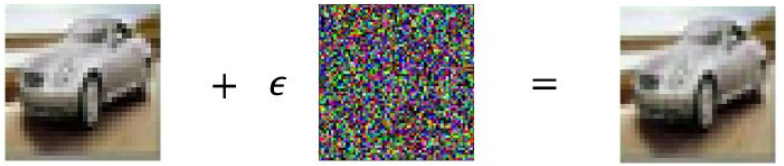


元問題：非凸、非滑らか
そのまま解くのは難しい

スムージングにより
やさしい問題に変換

解の探索と同時にスムージングを弱める
→ 徐々に元問題の解に収束

- 有効性評価
「ブラックボックス分類モデルに対する敵対的攻撃」タスクで有効性を確認



「自動車」
と判定

↑このノイズ
を発見したい

「飛行機」
と誤判定

Table 2. Performance of a per-image attack over 100 images of CIFAR-10 under $T = 10000$ iterations. "Succ. rate" indicates the ratio of success attack, "Avg. iters to 1st succ." is the average number of iterations to reach the first successful attack , "Avg. L_2 (succ.)" is the average of L_2 distortion taken among successful attacks, and "Avg. total loss" is the average of total loss $f(x)$ over 100 samples.

	Methods	Succ. rate	Avg. iters to 1st succ.	Avg. L_2 (succ.)	Avg. total loss
SGD algo.	ZOSGD	88%	**835**	0.076	27.70
	ZOAdaMM	85%	3335	**0.050**	19.15
GH algo.	ZOGradOpt	65%	6789	0.249	39.05
提案手法	ZOSLGH$_r$ ($\gamma = 0.999$)	**93%**	4971	0.248	**14.28**
	ZOSLGH$_d$ ($\gamma = 0.999$)	**93%**	4365	0.188	**14.23**

おわりに

- 理研AIP－NEC連携センターの活動テーマ・成果をご紹介
- 連携センターにおいて基盤となる技術を開発。いくつかのテーマでは実用化に向けた取り組みを開始
- 来年度も引き続き理研AIPとの連携（共同研究／技術指導）を継続し、基盤技術を強化

活動テーマ

	～2019	2020	2021
1．少量の学習データで高精度を実現する学習技術の高度化	異常事象など一部種類の現場データ無い場合に適応する学習手法	真のラベルよりも低コストで入手可能な弱ラベルを用いた学習手法の改善	
	（ACML2019,WACV2020）	（ICML2021）	
2．未知状況での意思決定を支援する学習／AI技術の高度化	論理推論のロバスト性を強化（観測との矛盾を高速検知）	サイバー攻撃手口推定の実問題で有効性確認	卒業
	（産総研との三者連携、NeurIPS2019、FLAIRS2020）		
3．複数AI間の調整にかかわる学習技術の理論解析	AI間の交渉戦略理論：未知制約付きベイズ最適化高速手法を考案	製造・物流で広く使われるスケジュール調整問題をターゲットにした最適化手法	
	（産総研との三者連携、SIP）	（今後、学会発表予定）	
4．実環境を想定したAXのリスク評価・対策	新規立上	顔認証の運用を加味したAX攻撃手法の提案・対策手法を考案	卒業
		（Biosig2021, IJCB2021）	
5．汎用的、パラメータフリーなブラックボックス最適化技術の開発	新規立上	理論的に収束性を示す新手法を考案	
		（今後、学会発表予定）	

22

テーマ２：未知状況での意思決定を支援する学習／AI技術の高度化

- 目的
  過去のデータの蓄積だけでは解けない、**未知状況での意思決定支援**の実現

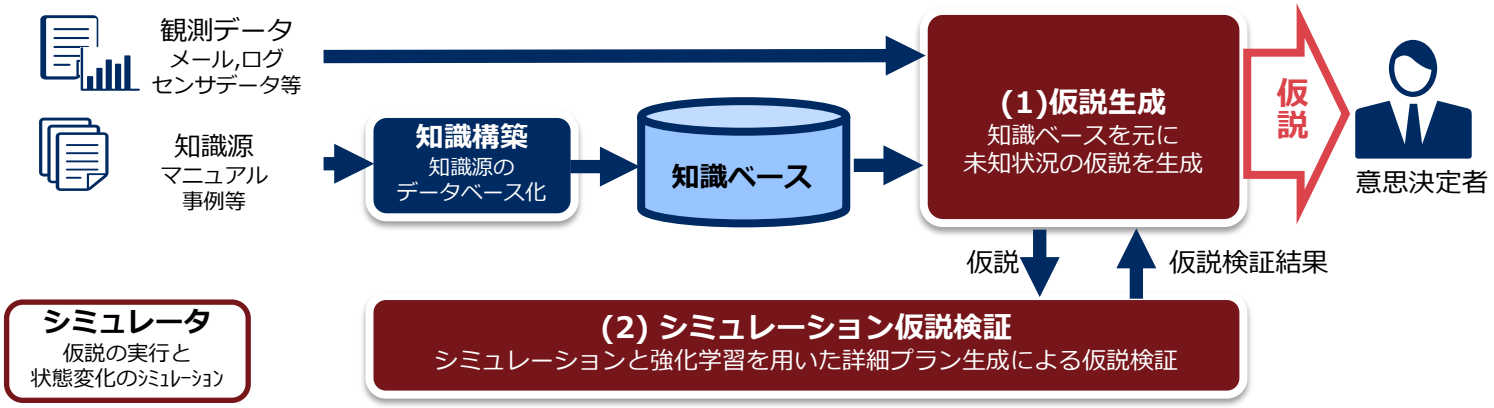
- 成果総括
  情報が不十分な未知状況における仮説生成/仮説検証を実現する要素技術の確立

① 計算量が指数オーダとなる仮説生成を、高速な解法が知られる最適化問題に定式化できることを発見し、1000倍高速化

FIT2018ヤングリサーチャー賞
FLAIRS2020採択

② 仮説が実行可能か強化学習を用いて検証する仮説検証において、シミュレータと実システムの挙動のズレによるリスクの低減と高効率な操作を両立

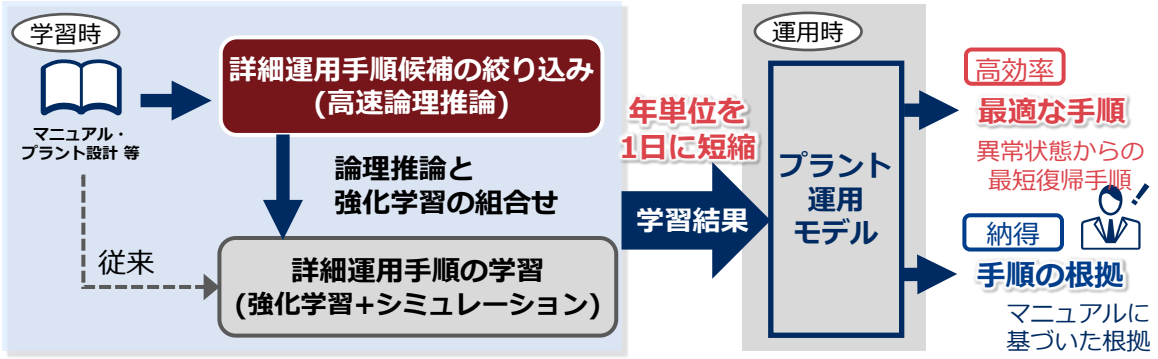
NeurIPS2019採択



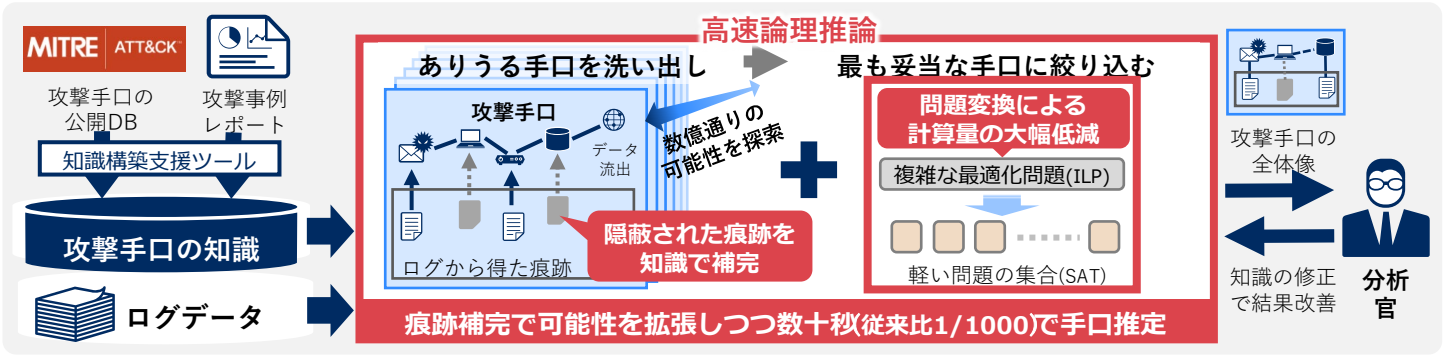
テーマ2：実用化に向けた取り組み

- プラントの運転支援やサイバー攻撃防御支援を含めた４つの異なる領域で、現場での活用や事業化に向けた実証実験を実施中

プラント運転支援



サイバー攻撃防御支援



各テーマの活動期間・内容サマリ

- **当初は3テーマで活動を開始。逐次、社会動向・AIの進展に応じてテーマを新設・変更**

活動テーマ	～2019	2020	2021
1．少量の学習データで高精度を実現する学習技術の高度化	異常事象など一部種類の現場データ無い場合に適応する学習手法（ACML2019,WACV2020）		真のラベルよりも低コストで入手可能な弱ラベルを用いた学習手法の改善（ICML2021）
2．未知状況での意思決定を支援する学習／AI技術の高度化	論理推論のロバスト性を強化（観測との矛盾を高速検知）（産総研との三者連携、NeurIPS2019 、FLAIRS2020）	サイバー攻撃手口推定の実問題で有効性確認	卒業
3．複数AI間の調整にかかわる学習技術の理論解析	AI間の交渉戦略理論：未知制約付きベイズ最適化高速手法を考案（産総研との三者連携、SIP）	製造・物流で広く使われるスケジュール調整問題をターゲットにした最適化手法（今後、学会発表予定）	
4．実環境を想定したAXのリスク評価・対策	新規立上	顔認証の運用を加味したAX攻撃手法の提案・対策手法を考案（Biosig2021, IJCB2021）	卒業
5．汎用的、パラメータフリーなブラックボックス最適化技術の開発	新規立上	理論的に収束性を示す新手法を考案（今後、学会発表予定）	

25

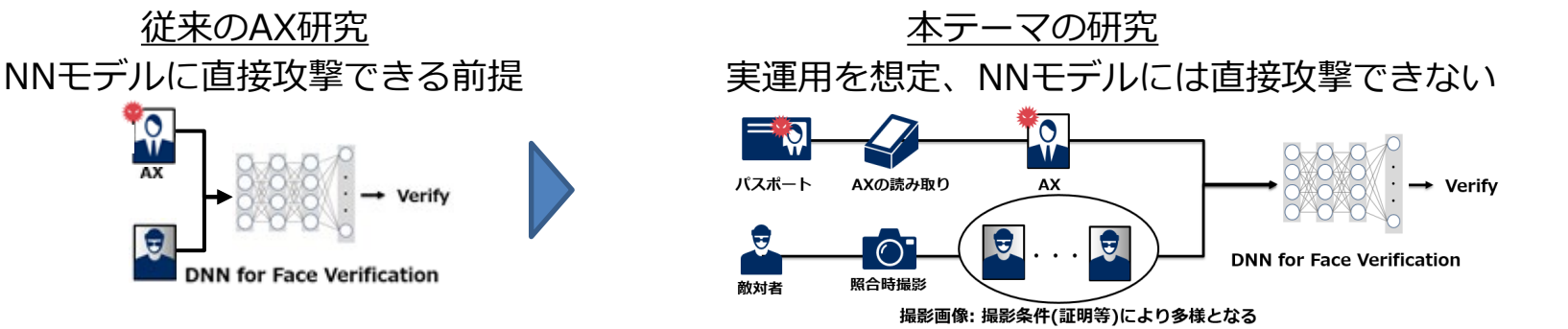
テーマ4：実環境を想定したAXのリスク評価・対策

目的

顔認証システムをターゲットに、実運用を想定したAdversarial Example(AX)の脅威を評価し、さらにAXに対するAIのロバスト学習技術を開発

成果総括

- 顔認証の運用を加味したAX攻撃手法の提案及びその対策手法を考案
  - 撮影の変動（照明、姿勢）によらず攻撃できるAX手法を開発→Biosig2021に採択



顔認証は登録と照合の２プロセスあり、照合時のカメラ実施を想定

- 複数人にマッチする顔画像（Masterface）の生成方法を提案
  - 公開されている顔認証AIに対し、1000人以上の人物に対して照合される顔画像を生成→IJCB2021に採択