資料４

【AI･データの安全･安心な利活用のための基盤技術】検討タスクフォース進捗報告

2022年8月18日
ガバニングボード報告

東京工業大学工学院　教授
宮本　恭幸

概要

- サブPD候補　および　タスクフォース構成員について
- 想定している三つの主要テーマ

  AI・データのプライバシー保護

  AI・データのセキュリティ

  InP系電子デバイス
- RFIについて
- タスクフォース委員会などの開催状況

サブPD候補　および　タスクフォース構成員について

サブPD候補について

NTTにおいて “セキュリティ、プライバシー、倫理、法律・制度等について研究を行う” 社会情報研究所　所長　平田真一氏　に依頼　→ご快諾
→7/1付けでNTTアドバンステクノロジへ異動

NTT社会研チーフ・セキュリティ・サイエンティスト
（主席研究員。NTTセキュリティマスター）
高橋克巳氏の追加を依頼　→　ご快諾

機械学習/データマイニング、個人情報の活用やデータプライバシ保護の理論の研究を行い、”データ解析におけるプライバシー保護”の著者でもある佐久間淳筑波大学教授
まだプレイヤーでいたいと、サブPD候補は固辞
→　有識者として参加を承諾

情報通信研究機構(NICT)サイバーセキュリティ研究所 研究所長　盛合志帆氏に有識者としての参加を依頼　→　ご快諾

PD候補意向確認時の
多様な視点から課題運営を推進するため、女性、若手などを SPD 候補等として入れることを検討することを反映

＜関係省庁＞　　5省庁　9名
＜研究推進法人（オブザーバー参加）＞ NEDO
＜事務局＞　内閣府3名

想定している三つの主要テーマ

- RFI結果の整理についてで＜PD候補に求められるスキル＞において

秘匿データの分散処理（連合学習、秘密計算など）のほか、敵対的サンプルからのAIの防護を含むAIとセキュリティの融合領域の全般について、全体ビジョンを描くことができる知見

および

- PD候補意向確認時に

領域全体をカバー出来るように、秘密計算、AI セキュリティなど情報分野の SPD 候補等を TF に複数入れること。InP については、通信用途だけでなく AI センサー用途についても検討すること。

となっていることから、主要テーマとして、

- AI・データのプライバシー保護
- AI・データのセキュリティ
- InP系電子デバイス

を想定する。

AI・データのプライバシー保護

- プライバシー保護技術には暗号型とデータ加工型（非暗号）がある
  - 暗号型は、秘密計算とも呼ばれ秘密分散や準同型暗号をベースとした方式がある
  - データ加工型には、匿名化、差分プライバシーなどの方式がある。
  - 連合学習はプライバシー保護に親和性のあるAI技術

- 暗号型とデータ加工型には一長一短があるが、動向から前者中心（秘密計算を軸にする）をとりたい
  - データ加工型による統計的活用から、暗号型によるプライバシーを保護した深い分析の実現
  - ただしデータ加工型も補完的に使うべき

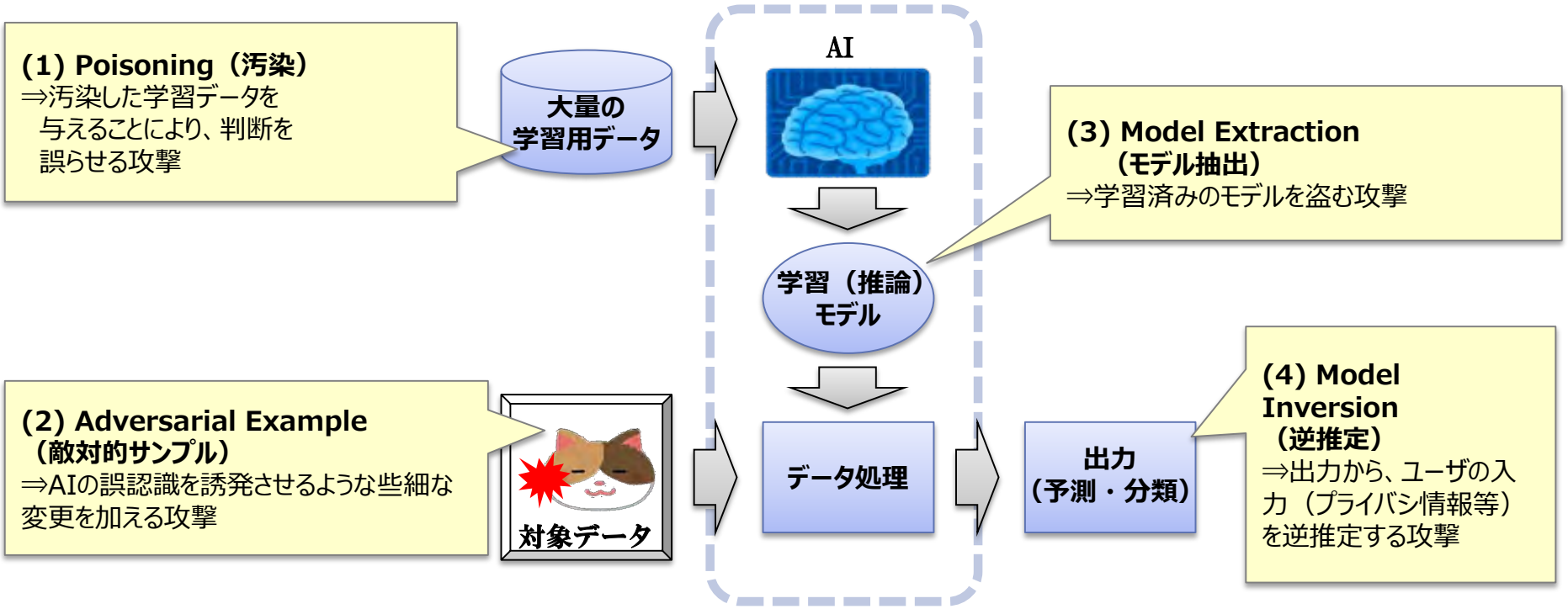
- それぞれの方式の現状は要素技術レベルで、機能・性能や社会受容性に課題がある
  - かつ、方式間でどれが良いという社会的コンセンサスは未解決
  - ガイドライン整備等による新しいデータ価値創出への期待

- 以上から、複数の秘密計算（データ加工方式を加味させる）で、課題解決していく方向性が妥当
  - 秘密計算間のインターオペラビリティーの確保を検討する

- なお、スタートアップ枠の活用についても検討する。

AI・データのセキュリティについて

- AIの利活用の拡大に当たっては、"自律制御用AIに対するサイバー攻撃対策"などのセキュリティを課題と設定された。下記のような項目が考えられる。



- しかし、関係するRFIは出てきていない。またTFメンバーからは、まだアカデミック的で、方向も定まっていない部分があることから、大きなプロジェクト的にはしづらいとの意見あり

→ FSで検討を行い、技術的実現性調査に基づいた計画を検討するが、
それ以外にも、技術的実現性を加味した公募条件をつけつつ、
いくつかのテーマについて、細かい研究計画は決めない方向で、公募をしたい。

InP系電子デバイス

データの安全・安心な流通を確保するためのデータ連携基盤としてのテラヘルツ帯通信用素子

300GHz帯での増幅ができる素子は材料としてInP系電子デバイスしかない。
HEMTが良いか、HBTが良いかは要検討

まずは実用化のためには量産化のための成熟
→300GHzで動作する集積回路を商品化する。（まずは計測用）
（3年目までのサンプル出荷→その後　成熟化）

高い周波数であり、信号をとおしつつ、量産化が可能な実装技術も重要
（現在のチップレット技術との融合も目指し、Si集積回路との融合
さらにはファウンダリーサービスの可能性も）

また、テラヘルツ波はセンシング技術にも応用可能
RTDを用いて、開発されつつある技術をトランジスタへ導入

RFIについて

主領域として　21件の応募があった。

主要テーマについて
　AI・データのプライバシー保護　2件
　InP系電子デバイス　　1件

その他
ELSI　について　　1件

頂いたRFIは、非常に抽象的でそのままでは元にできない。ただし、倫理は重要であり、セキュリティと同様に計画を緻密にはせず公募をかけては？

各種アプリケーション5件、　AIを活用したセキュリティ2件、データ基盤の信頼性向上6件、AI処理の集積化2件、半導体製造技術（InP系以外）2件などがあった。
　　データ基盤関係の2件については今後ヒアリングなどで検討する。

副領域としたものについては、総括ヒアリング後に検討開始
200件以上あり、
秘密計算をキーワードにしているのは4件、セキュアな情報連携とAIを併記したものが1件ある。

タスクフォース委員会などの開催状況

6/16　平田・佐久間・宮本で、第一回目の打合せ

6/17付けでタスクフォース構成案を報告

このあとメールベースでFS実施方針案を策定

6/24　第一回検討タスクフォース
FS実施方針案について、審議　　細かい修正については一任で承認

6/29　FS実施方針案提出

6/30　高橋氏　サブPD候補を追加

7/7　　盛合氏　参画内諾

7/11　高橋・佐久間・宮本・事務局で今後の進め方を打合せ

7/19　平田・高橋・佐久間・盛合・宮本・事務局でRFIの選択・データを守るの方向性を検討

7/25　総括ヒアリング　方向性を確認

Tokyo Tech

ありがとうございました。