資料2-2

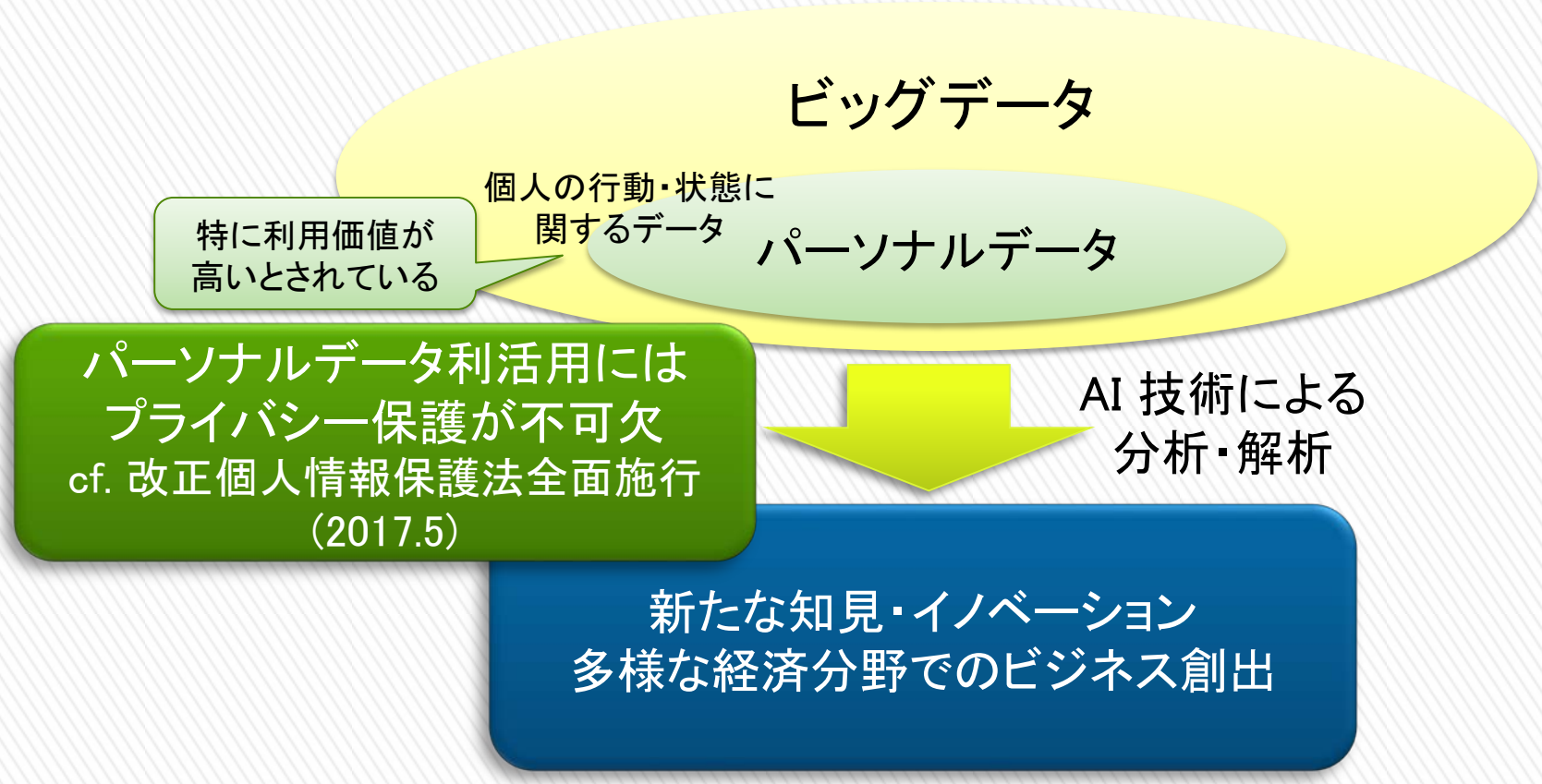
情報通信審議会　情報通信技術分科会　技術戦略委員会
次世代人工知能社会実装WG（第2回）2017.2.14

データ利活用とセキュリティ・プライバシー保護

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
セキュリティ基盤研究室
盛合　志帆

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

パーソナルデータの利活用



個人情報と第三者提供

【個人情報】

生存する個人に関する情報であって、

1) 氏名、生年月日、住所等により特定の個人を識別することができるもの（他の情報と容易に照合でき、それにより特定の個人を識別することができるものを含む）

例：データベース化されていない書面・写真・音声等に記録されているもの

2) 個人識別符号（①又は②）が含まれるもの

① 特定の個人の身体の一部の特徴を電子計算機のために変換した符号

例：顔認識データ、指紋認識データ等

② 対象者ごとに異なるものとなるように役務の利用、商品の購入又は書類に付される符号

例：旅券番号、免許証番号等

【第三者への提供】

- 本人の同意を取れば提供可能
- 委託、事業承継、共同利用に伴って提供する場合には、「第三者」に提供するものとはされない
- 「匿名加工情報」に加工すれば、本人の同意をとらなくても自由に利活用可能
  → 新事業や新サービスの創出、国民生活の利便性の向上を期待

匿名加工情報

- 個人の特定性を低減したデータ
  - 「個人情報を加工して、通常人の判断をもって、個人を特定することができず、かつ、加工する前の個人情報へと戻すことができない状態にした情報」
- 加工方法
  - 特定の個人を識別する項目の削除や、情報を”丸める”など
  - 「匿名加工情報作成マニュアル」(経済産業省, 2016.8)
- 社会実装に向けた研究開発課題
  - 匿名加工技術の評価技術 (有用性指標と安全性指標)
    - いかに再識別のリスクを低減し(安全性)、データの有用性を保ったまま加工するか
  - NICT(第4期中長期計画)での取り組み:リスク評価ツールの試作・プライバシー保護支援ポータル機能の構築

PWS CUP 匿名加工・再識別コンテスト

- 2015年から情報処理学会 コンピュータセキュリティシンポジウム と併催
  - PWS組織委員会委員長：菊池浩明(明治大)
  - 後援：個人情報保護委員会
- PWS CUP 2016
  - 匿名加工部門：顧客情報データと購買履歴データを有用性を残して安全に匿名加工する
  - 再識別部門：元の顧客データをヒントにして、匿名加工された購買履歴から顧客を識別する

暗号技術を用いた プライバシー保護データ解析技術

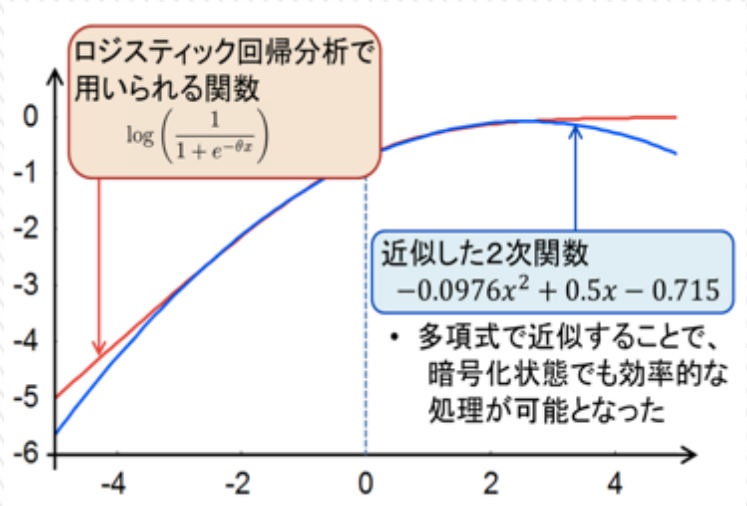
» 暗号化したままデータ解析

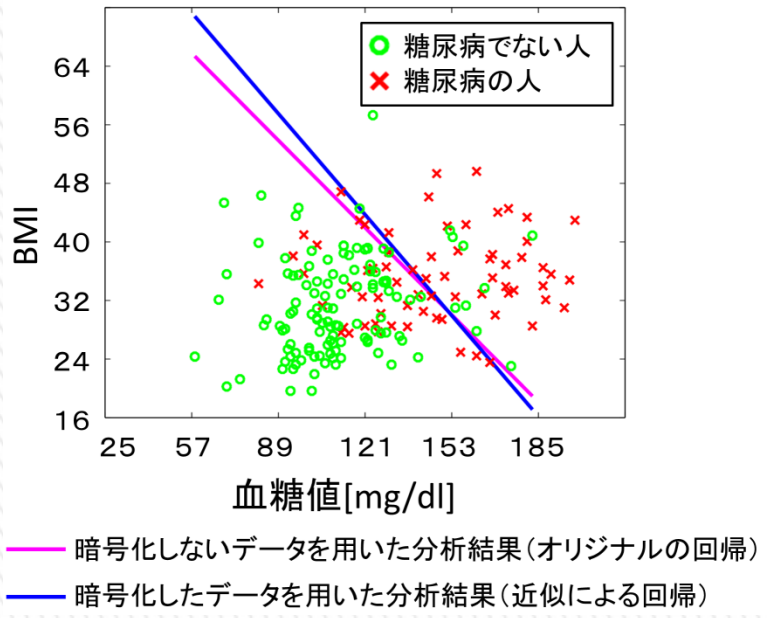
> 暗号化データ上で演算処理可能な「準同型暗号」

> 格子理論ベースの準同型暗号「SPHERE(スフィア)」を開発 (2014)

+ ベクトル同士の加減算、テンソル積、内積

> 暗号化したままロジスティック回帰分析(1億件のデータを30分以内で分類)



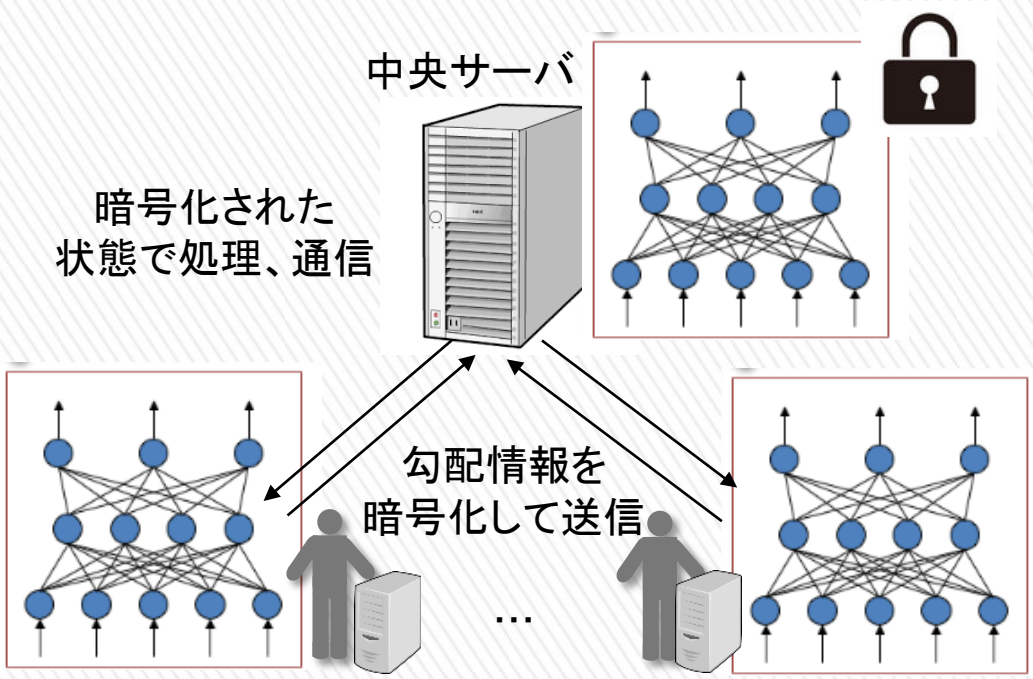


暗号技術を用いた プライバシー保護データ解析技術

» 準同型暗号を用いたプライバシー保護深層学習

多数の参加者が持つ
データセットを互いに
秘匿したまま深層学習を
行うプライバシー保護
深層学習システム

勾配情報の暗号化による
通信データ量の増加：約3倍
（128ビットセキュリティを実現
するLWE, Paillier暗号を用いて
シミュレーション）



N人の参加者と中央サーバ1台による深層学習
（分散協調学習）

JST CREST「人工知能」

「イノベーション創発に資する人工知能基盤技術の創出と統合化」
研究総括: 栄藤 稔(NTTドコモ), 文科省 AIPプロジェクトの一環として運営

»「複数組織データ利活用を促進するプライバシー保護データマイニング」

> 研究代表者:盛合 志帆(NICT). 神戸大 小澤教授, (株)エルテスとの連携

課題

複数の異なる業種・組織が有する実社会の
膨大なデータを統合して利活用する際、
プライバシー保護・データ機密性の確保が課題

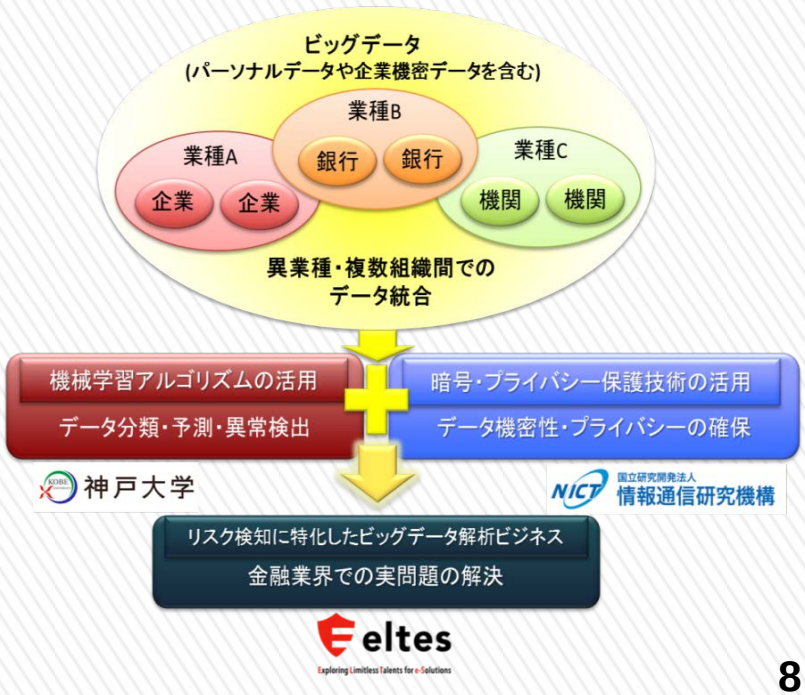
研究課題

暗号技術や人工知能技術を活用し、
プライバシーを保護した状態で
高速にデータ分析や異常検知を行う技術を
研究開発

解決する社会問題

金融分野における社会問題の解決に活用.
金融機関以外がもつデータを利活用した
①インターネットバンキング不正送金の検知
②個人向け融資における 適正利率の導出
⇒ フィンテックにおけるイノベーション創出をめざす.

研究体制



理研 革新知能統合研究(AIP) センターとの連携

» プライバシーと社会制度チーム

（チームリーダー：中川 裕志）

> 匿名化技術を中心としたプライバシー保護技術

> 情報処理学会 PWS CUP との連携

» 人工知能セキュリティ・プライバシーチーム

（チームリーダー：佐久間 淳）

> 人工知能のセキュリティ

> JST CREST ビッグデータ「自己情報コントロール機構を持つプライバシ保護データ収集・解析基盤の構築と個別化医療・ゲノム疫学への展開」(研究代表者：佐久間. H25-) との連携