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

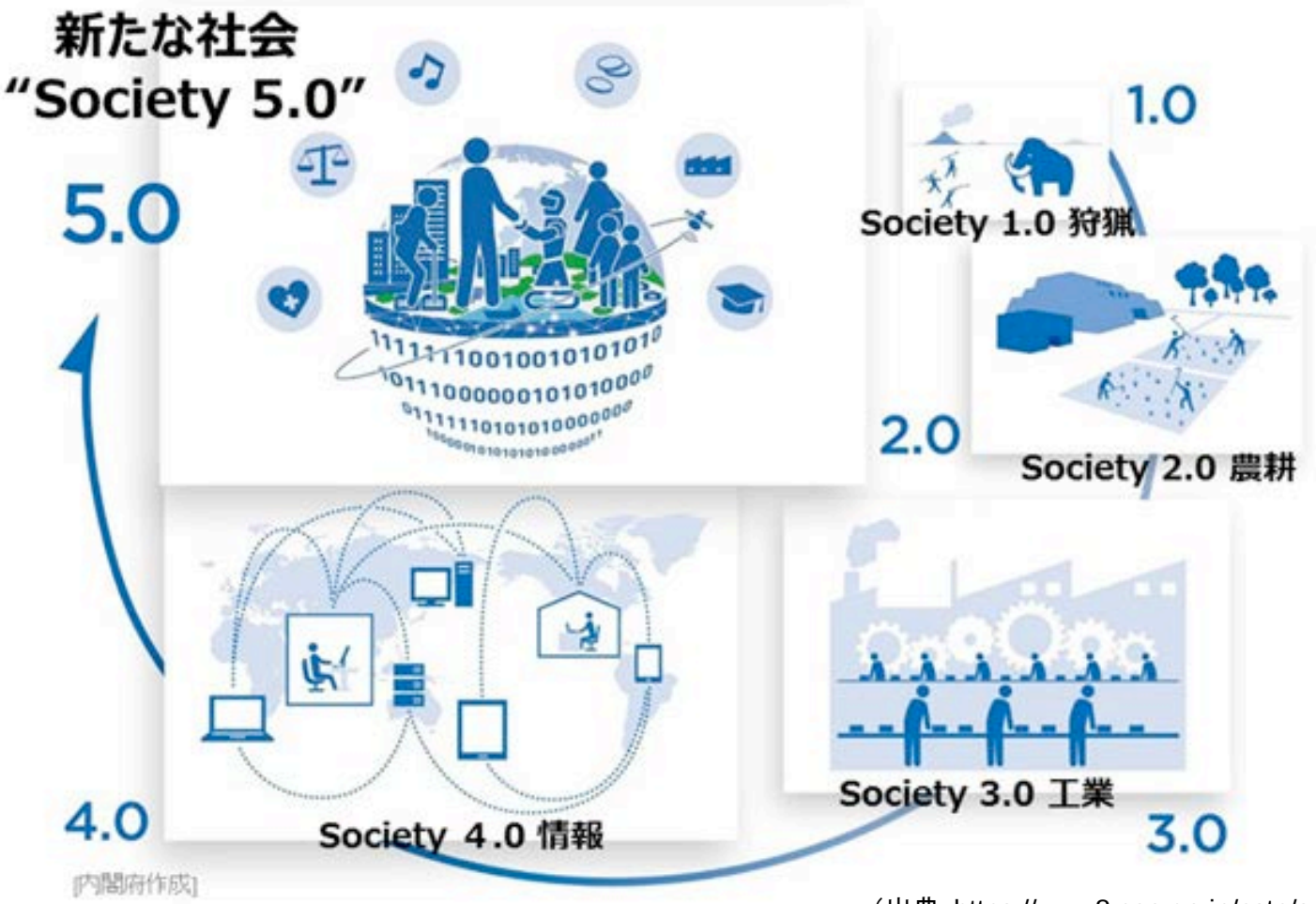
安心・安全なSociety 5.0の実現にむけて
～プライバシー保護データ解析技術の現在～

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長

盛合 志帆

Society5.0とは？

サイバー空間とフィジカル空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（第5期科学技術基本計画）



（出典：https://www8.cao.go.jp/cstp/society5_0/）

安心・安全な Society5.0 に向けて

データセキュリティとプライバシーの確保が鍵

（出典：https://www.gov-online.go.jp/cam/s5/）

分野横断でのデータ統合利活用

新たな成長戦略の鍵

暗号技術＋人工知能技術

プライバシーを保護した状態でデータ解析や異常検知

暗号・認証技術により
データの機密性・信頼性を
確保することで
組織横断でのデータ利活用を促進

次世代AI 技術によるデータ解析

新たな知見・イノベーション
多様な経済分野でのビジネス創出

データ統合利活用を促す動き

- 改正個人情報保護法 (2017)
  - データ利活用とプライバシー保護の両立
- 次世代医療基盤法 (2018)
  - 匿名加工医療情報等の取扱いに関する規制を定める
- 「情報銀行」認定事業 (2018)
  - 民間事業者が個人データを収集・管理し、第三者の事業者に提供
- IoT投資減税 (2018)
  - セキュリティ対策が講じられたデータ連携・利活用への投資を支援

これらを支える安心・安全なデータ利活用のための
プライバシー保護データ解析技術がますます重要に

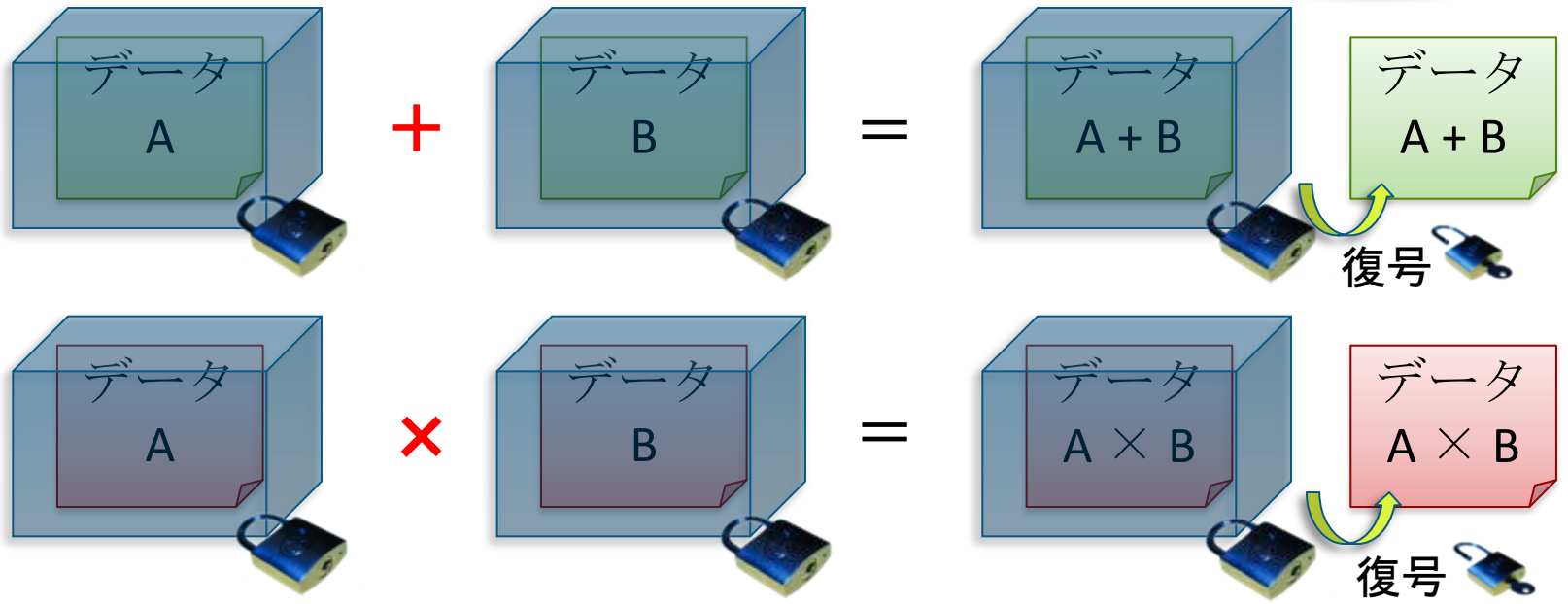
データを秘匿したまま解析を行う

プライバシー保護データ解析

プライバシー保護データ解析

じゅんどうけいあんごう
準同型暗号：
暗号化したまま加算や乗算ができる

もとのデータ
(AやB)を知らずに
和や積を計算できる

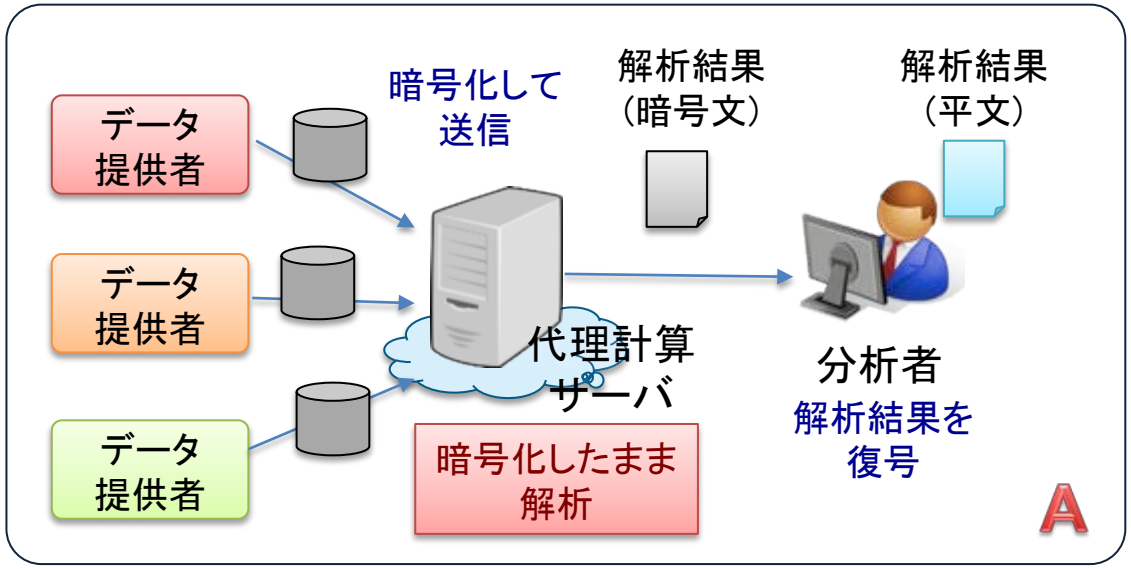


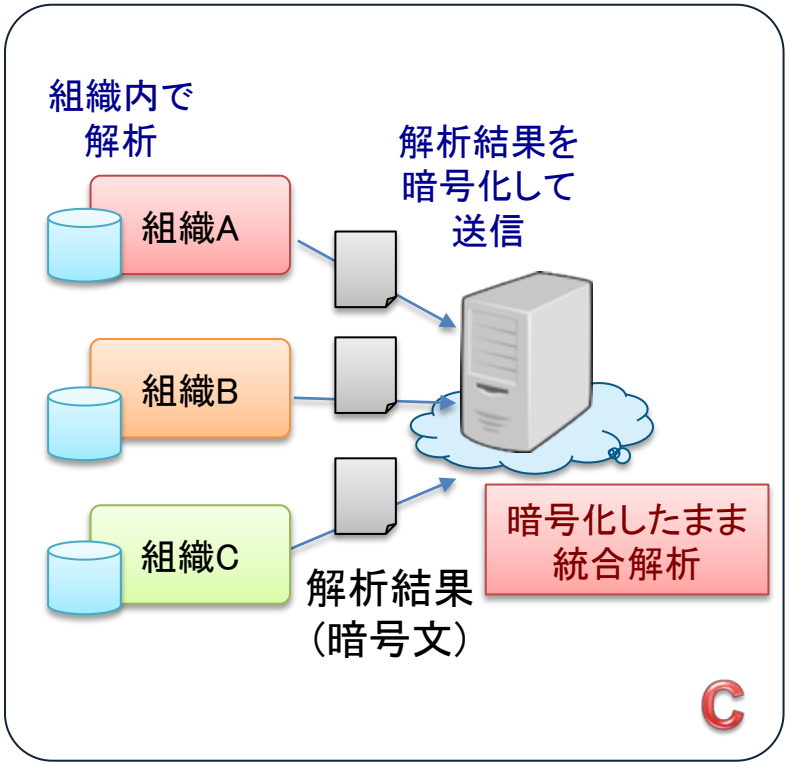
完全準同型暗号：加算、乗算の両方ができるもの

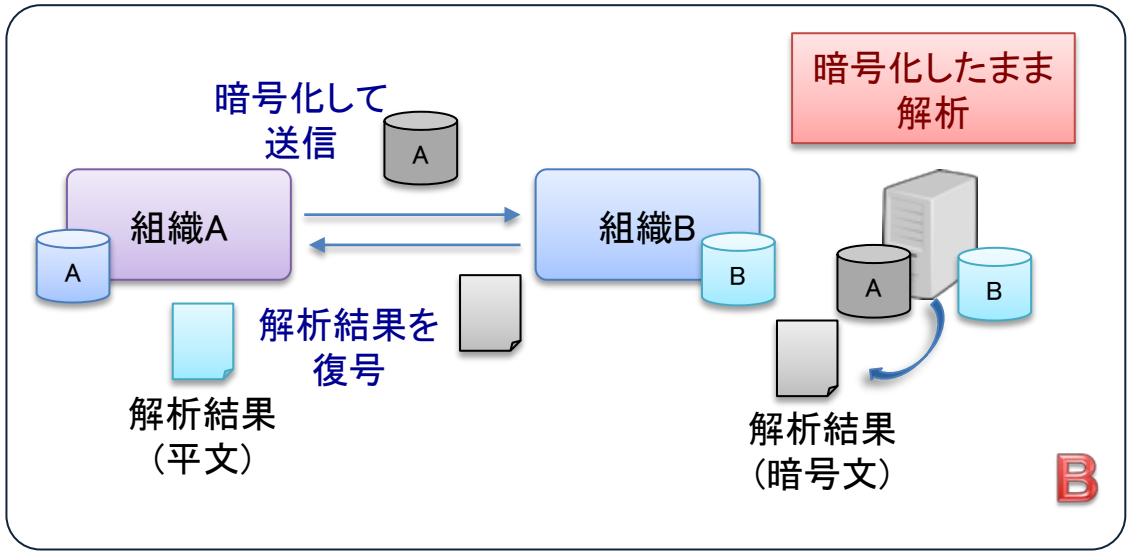
- 2009年にGentryが完全準同型暗号（格子ベース）を初めて構成
- **暗号化したままでのデータ解析**に道が開けた

プライバシー保護データ解析

利用シナリオの例

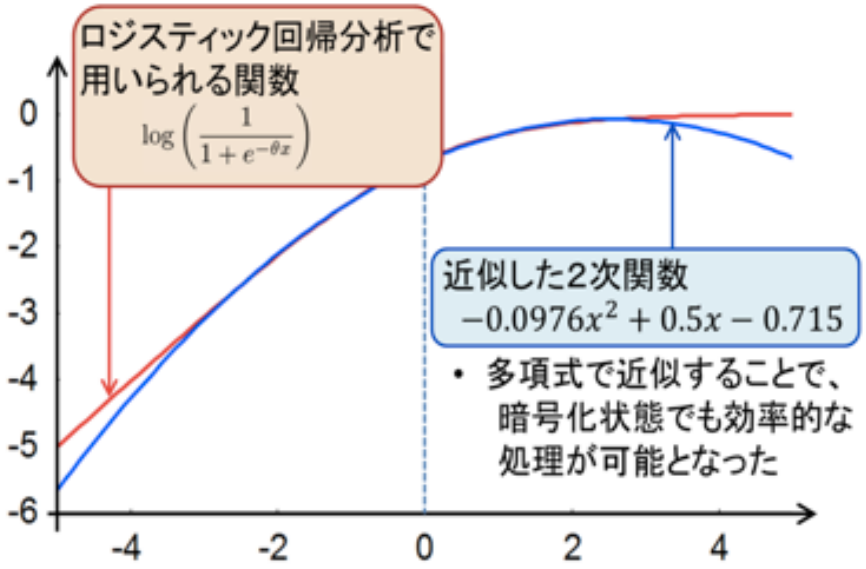


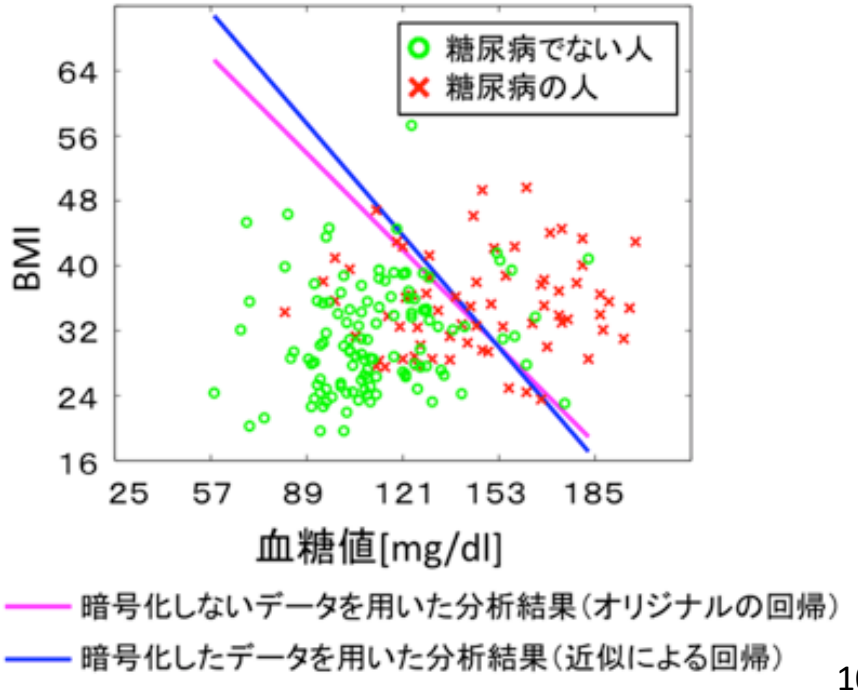




暗号化したままビッグデータ分類

- ビッグデータ解析で多用されているロジスティック回帰分析をデータを暗号化したまま計算可能に
- 暗号化された1億件のデータを30分以内で複数グループに分類できることをシミュレーションで確認
  - NICTプレスリリース「暗号化したままデータを分類できるビッグデータ向け解析技術を開発」(2016.1.14)



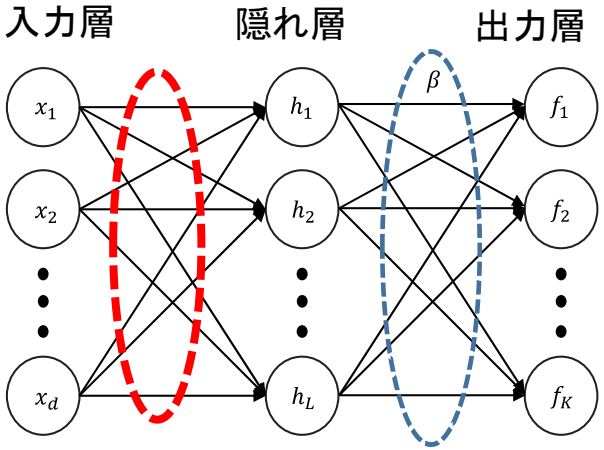


暗号化したまま近似なしで学習・識別

- データを暗号化したまま学習・予測を安全に委託計算可能なニューラルネットモデルPP-ELM*の提案
  (神戸大との共同研究)

*Privacy-Preserving Extreme Learning Machine

  - なぜELMか? : 学習・識別に近似を導入せずに実現.
    非線形分類器でかつOne-Shotで学習できる



ランダムな結合荷重　　学習すべき結合荷重

分類精度(既存研究との比較)

Datasets	PP-ELM L= 300	PP-Logistic ovr	Logistic ovr
Glass	0.684 +/- 0.089	0.596 +/- 0.099	0.604 +/- 0.070
Digits	0.965 +/- 0.021	0.889 +/- 0.037	0.925 +/- 0.027
Sattelite	0.875 +/- 0.007	0.758 +/- 0.019	0.827 +/- 0.018
Shuttle	0.997 +/- 0.001	0.873 +/- 0.002	0.933 +/- 0.002

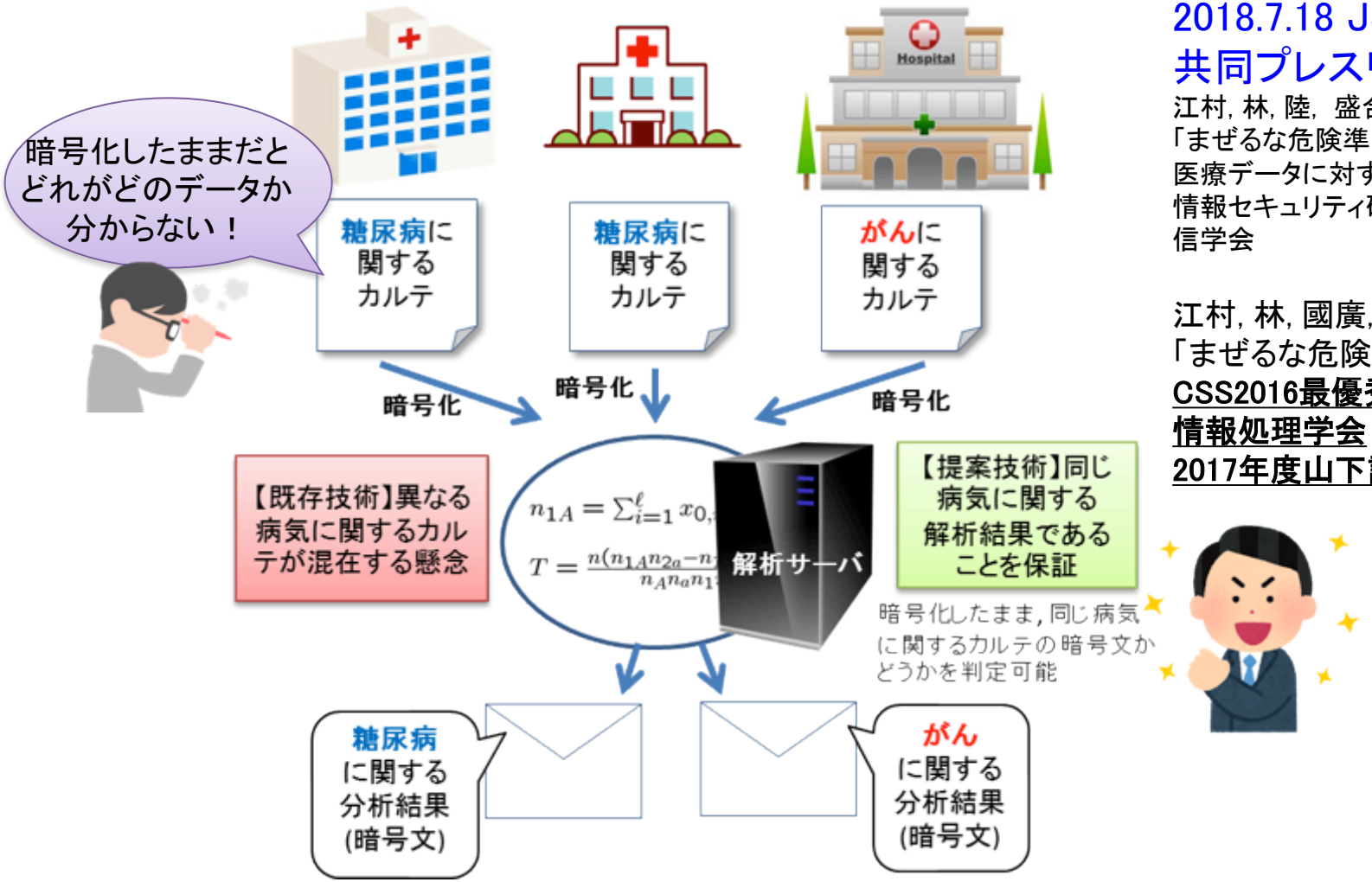
(L:隠れ層のノード数)

+0.04～0.12

1. Single-hidden-layer neural networksの一種
2. 隠れ層の結合荷重はランダムに決め，学習しない
3. 出力層の結合荷重は解析的に求められる

提案した PP-ELM には近似が導入されておらず，ニューラルネット本来の高い精度を示す

暗号化したままデータ解析時の誤データ混入防止



2018.7.18 JST, 筑波大と共同プレスリリース

江村, 林, 陸, 盛合, 佐久間, 山田,
「まぜるな危険準同型暗号を用いた医療データに対する χ^2 独立性検定」,
情報セキュリティ研究会, 電子情報通信学会

江村, 林, 國廣, 佐久間
「まぜるな危険 準同型暗号」
CSS2016最優秀論文賞受賞
情報処理学会
2017年度山下記念研究賞

「プライバシーを保護したまま医療データを解析する暗号方式を実証」

- 病気の罹患情報と個人の遺伝情報との統計的な関連性を個人の病気の有無を知ることなくχ^2検定で解析
- 4500名程度の規模で1分弱
- 解析対象外データが混在した場合でも高速検出（数十ミリ秒）

①医療データを暗号化

病気の罹患情報

	糖尿病	高血圧
A	あり	なし
B	あり	あり
C	:	:

病院

②医療データの暗号文を送付

遺伝情報を管理する検査機関

個人の遺伝情報

	rs001	rs002
A	あり	なし
B	あり	あり
C	:	:

③個々の医療データを知ることなく遺伝情報との関連性（統計値）の暗号文を計算

④統計値の暗号文を送付

⑤個々の遺伝情報を知ることなく医療データとの関連性を得る

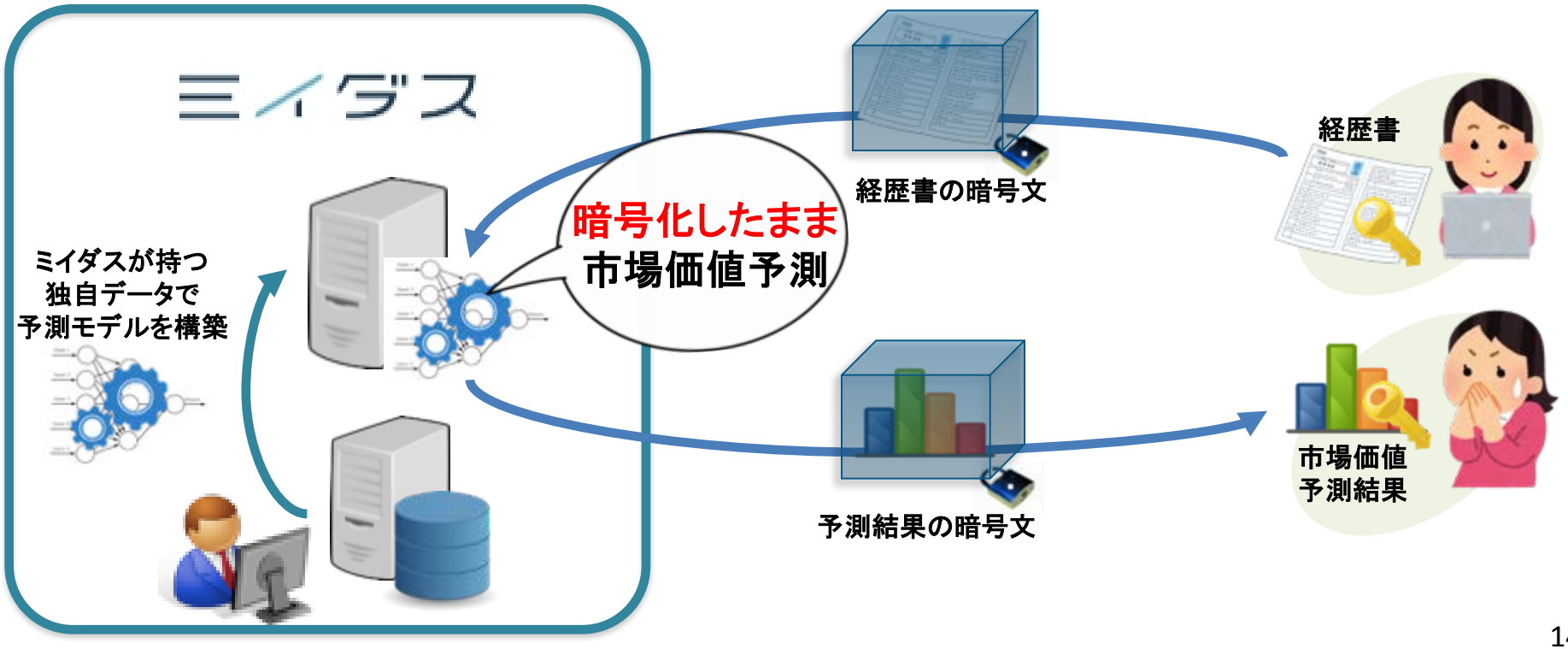
異なる病気の場合 警告

データ活用事業に対する技術支援

- 株式会社ミイダス
  - ICTを駆使した先進的な転職サービスを提供
- パーソナルデータの利活用に向けて技術支援

例) プライバシー保護市場価値予測サービス

- ミイダスがユーザデータを一切見ること無く、ミイダスが持つ予測モデルを適用



暗号化したまま組織横断で協調深層学習

プライバシー保護ディープラーニング

プライバシー保護深層学習技術で不正送金の検知精度向上に向けた実証実験を開始

～実証実験に参加の金融機関を募集～

平成31年2月1日

国立研究開発法人情報通信研究機構
国立大学法人神戸大学
株式会社エルテス

本研究の一部は、JST CREST JPMJCR 168Aの支援を受けたものです.

JST CREST「人工知能」研究領域

- JST CREST 研究領域「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」
- 戦略目標: 急速に高度化・複雑化が進む人工知能基盤技術を用いて多種膨大な情報の利活用を可能とする統合化技術の創出(研究総括:栄藤稔(大阪大学))

本研究領域にて今年度から下記の研究課題(加速フェーズ)を推進中

研究課題名

「プライバシー保護データ解析技術の社会実装」

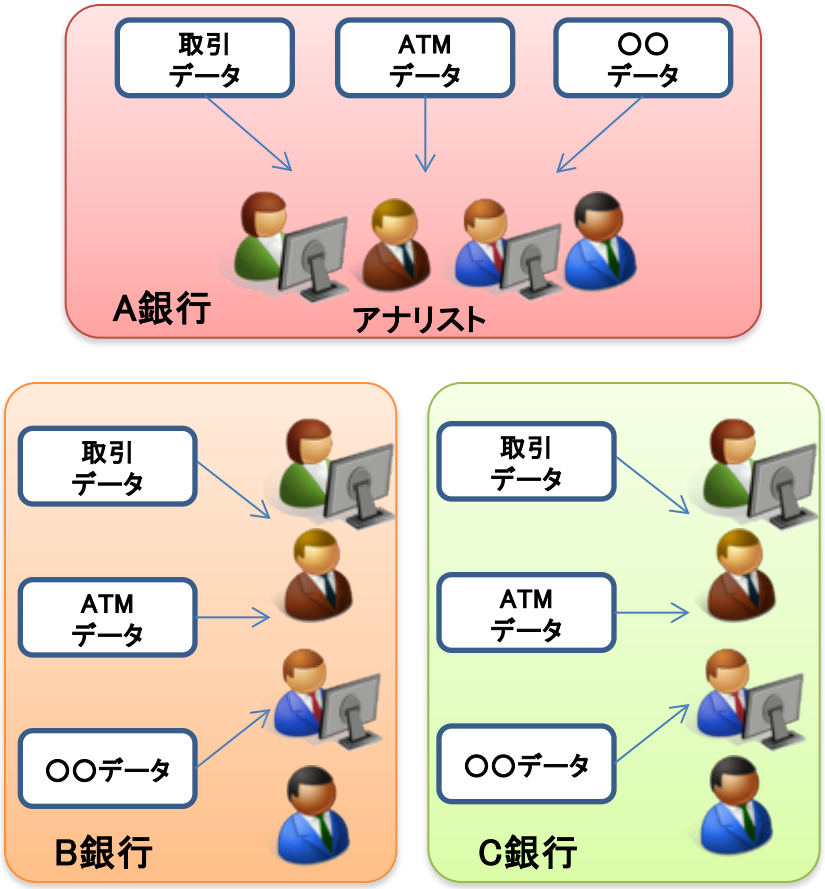
○花岡 悟一郎(産総研), 盛合 志帆(NICT),
浅井 潔(東大), 小澤 誠一(神戸大),菅原 貴弘((株)エルテス)

研究概要

複数の金融機関と連携し、プライバシー保護ディープラーニングによる不正取引検知の実証実験とプライバシー保護金融データ解析システムの開発

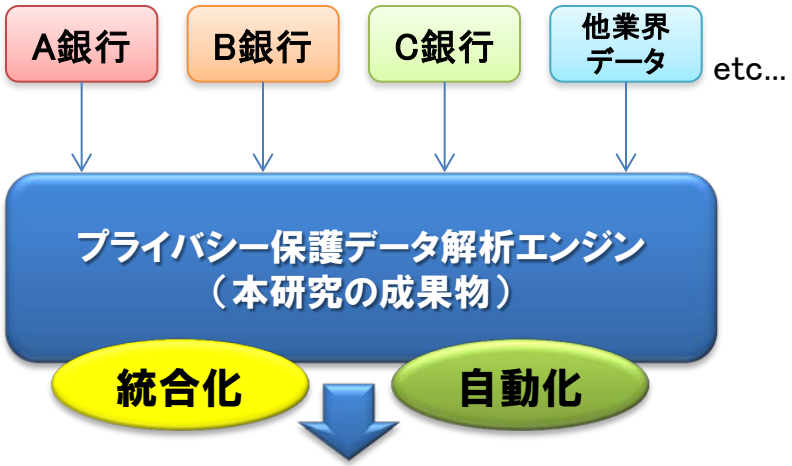
金融分野における課題と構想

現状



個々の金融機関内で分析
- コストや精度に課題

めざす構想



不正取引の検知，
与信管理，マーケティング

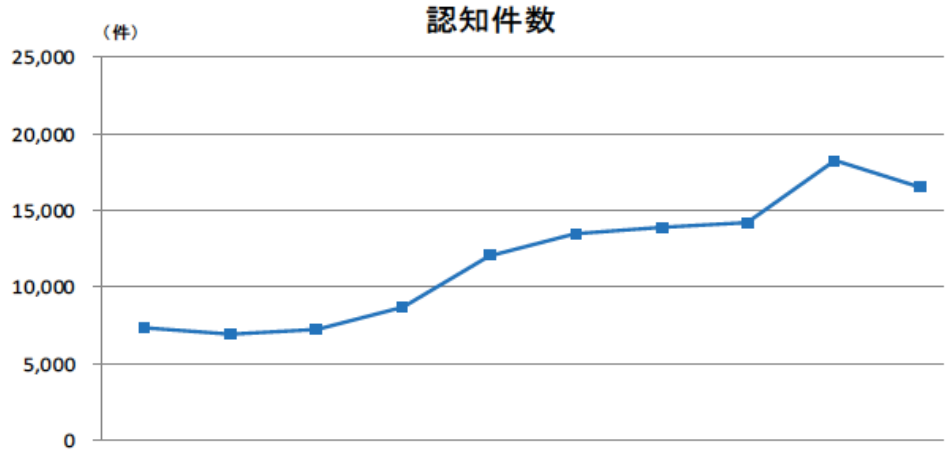
- 調査コスト削減
- 調査属人化の回避
- 調査精度の向上
  - 今まで見つからなかった検知が可能に！

不正取引(振り込め詐欺等)検知

- 特殊詐欺*による被害金額 **363.9億円** (2018年)
  - 1件当たりの被害額 233.2万円 (前年より増加)
  - 認知件数16,496件（前年比-1,716件、増減率-9.4%）
  - 認知件数が減少した一方で、東京、埼玉、神奈川等の認知件数が大幅増加

➡ 取引情報・口座情報等から疑わしい取引を検知

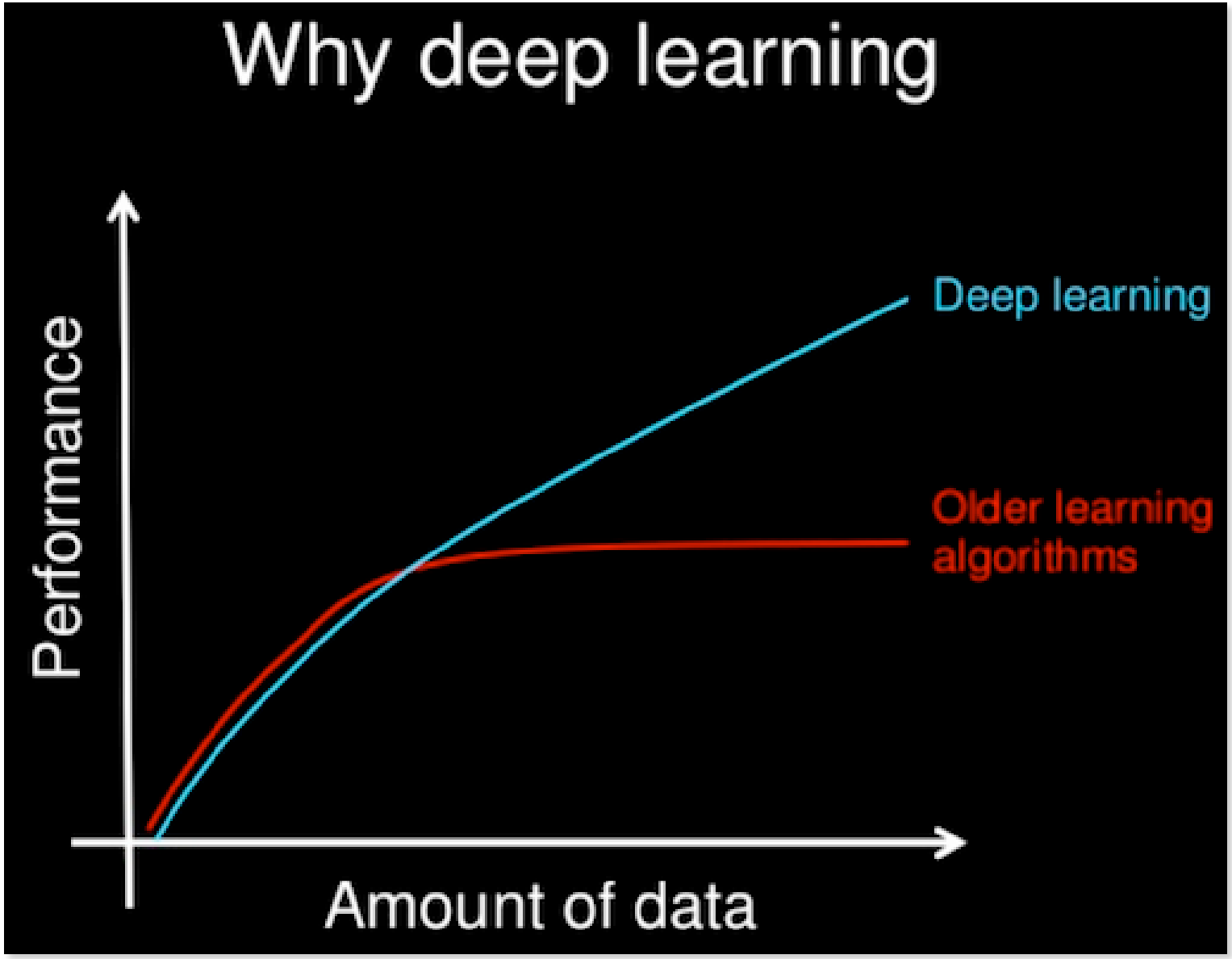
*特殊詐欺
面識のない不特定の者に対し、電話その他の通信手段を用いて現金などをだまし取る詐欺



区分＼年次	21年	22年	23年	24年	25年	26年	27年	28年	29年	30年
認知件数	7,340	6,888	7,216	8,693	11,998	13,392	13,824	14,154	18,212	16,496

警察庁「平成30年における特殊詐欺認知・検挙状況等について」

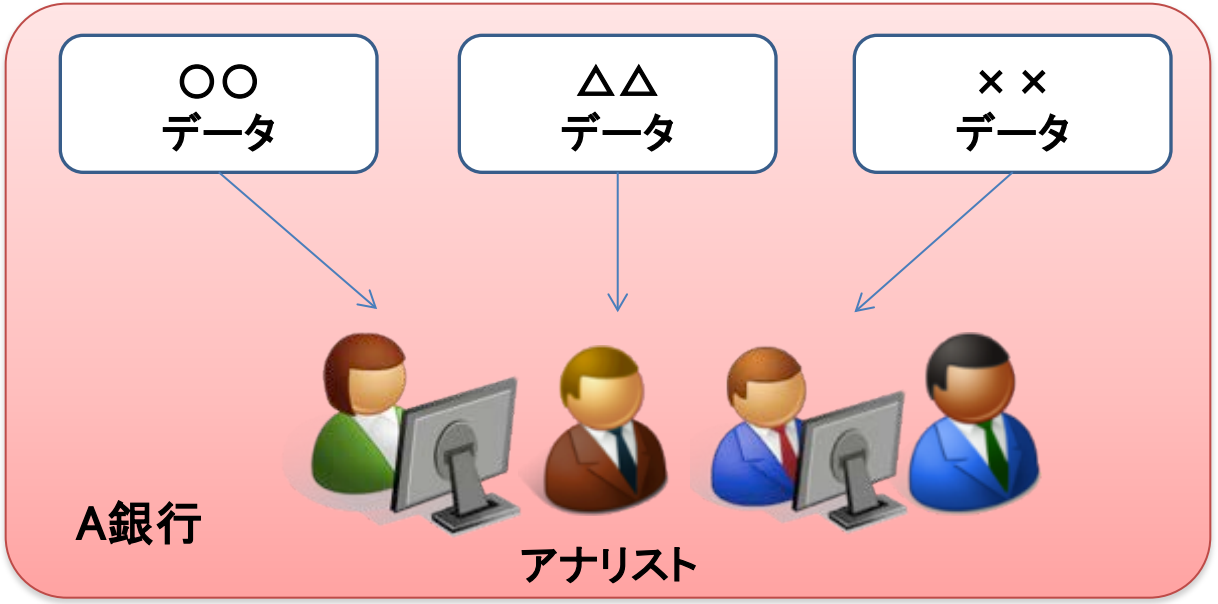
ディープラーニングはデータ量が命



by Andrew Ng

Google Brain Pj.や
Baidu AI Groupの
リーダーを務めた

一組織では学習用データが不足しがち

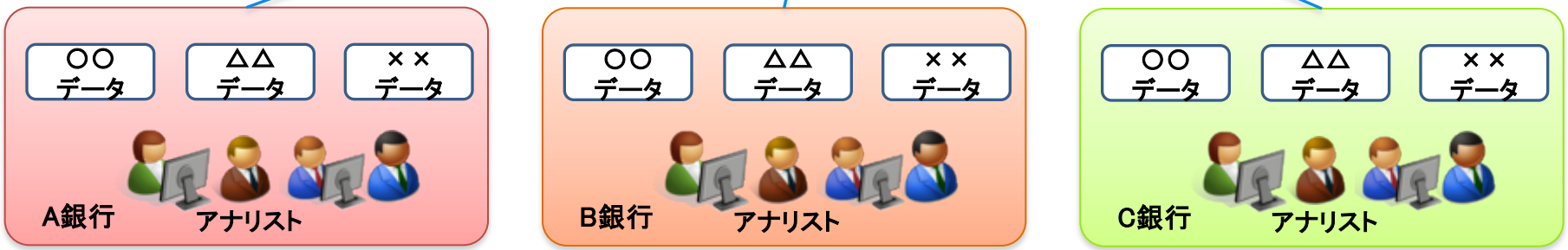


異常検知においては、異常データが
少なすぎることも

⇒よい分析結果が得られない

複数組織で連携して ディープラーニングを行うには？

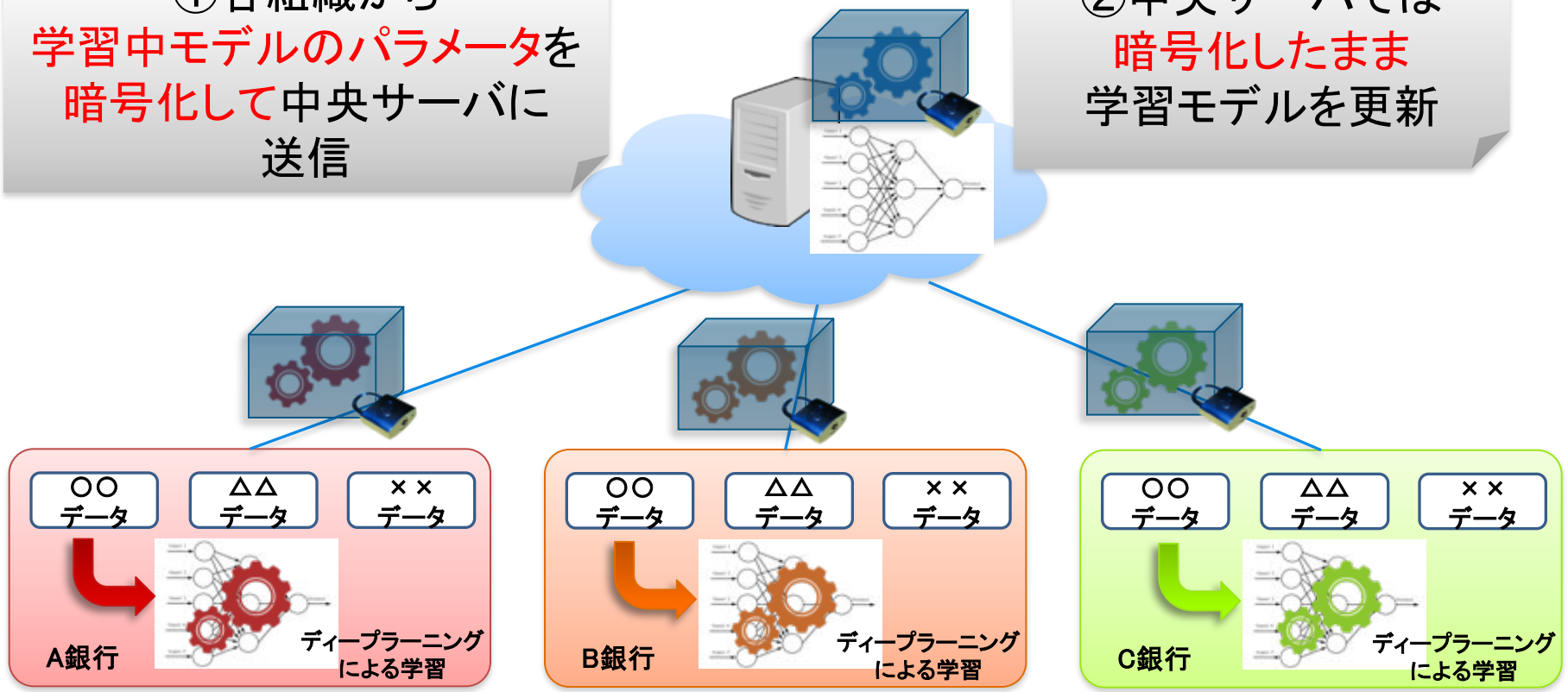
複数組織のデータを
中央サーバに集める！



外部にデータ開示することなく
複数組織で連携して
ディープラーニングを行うには？

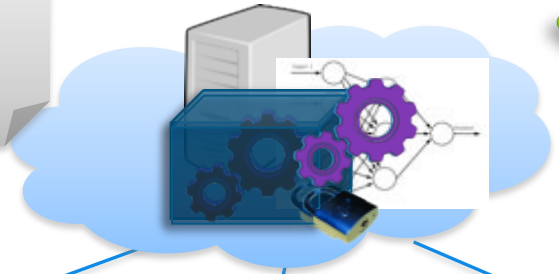
①各組織から
学習中モデルのパラメータを
暗号化して中央サーバに
送信

②中央サーバでは
暗号化したまま
学習モデルを更新

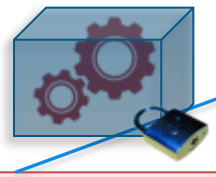


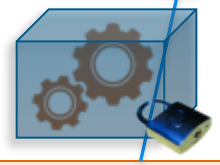
外部にデータ開示することなく
複数組織で連携して
ディープラーニングを行うには？

③各組織では
中央サーバで更新された
学習モデルをダウンロード、
精度の高い分析が可能に

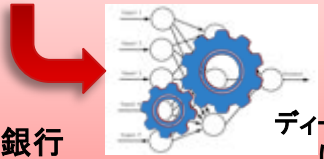


中央サーバにも
第三者にも
データ漏洩の
危険性なし！





○○
データ
△△
データ
××
データ



A銀行

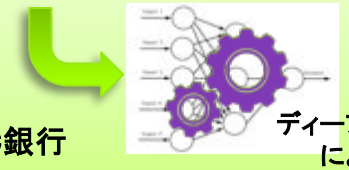
ディープラーニング
による学習

○○
データ
△△
データ
××
データ

B銀行

ディープラーニング
による学習

○○
データ
△△
データ
××
データ



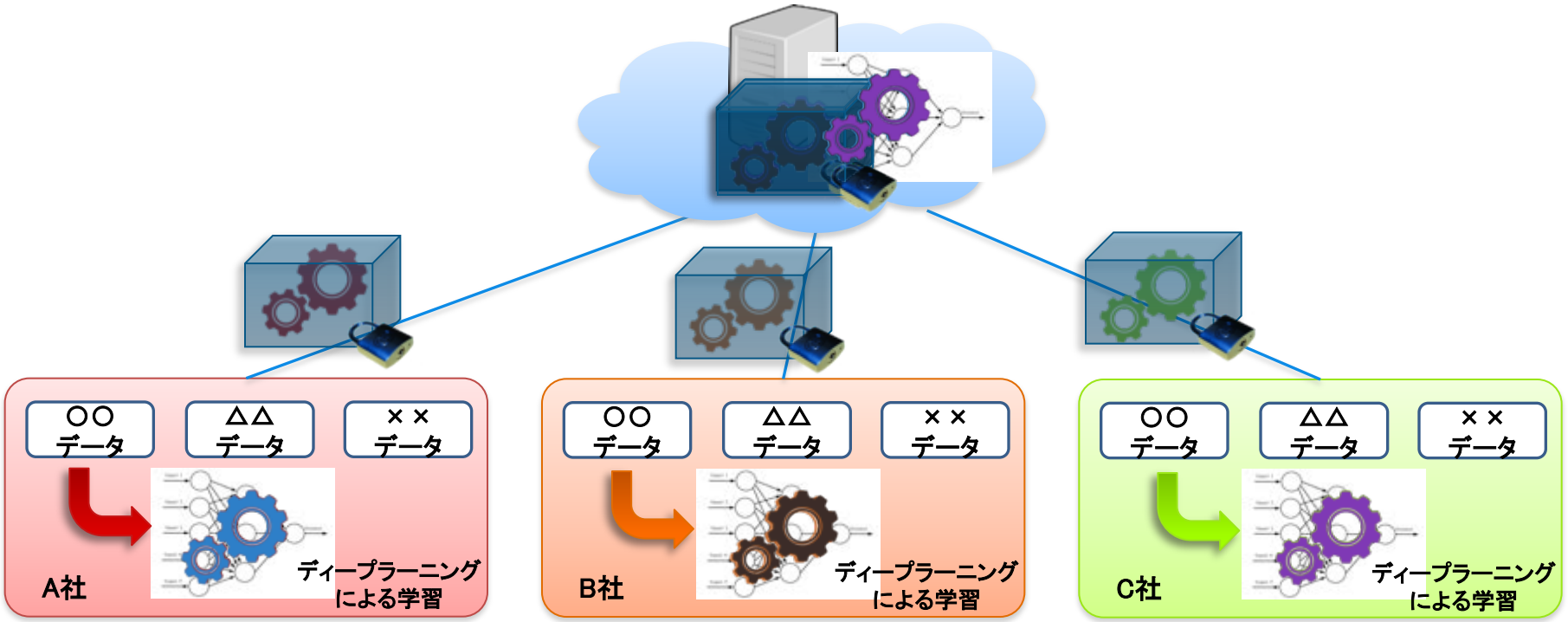
C銀行

ディープラーニング
による学習

プライバシー保護深層学習

オープンデータセットを用いた実用性検証

- 欧州のクレジットカード取引データ (Kaggle)
- 284,807件の取引レコード（うち500件程度が不正利用）
- 取引レコードから1ms以下で不正利用を検出



複数組織で連携した分散協調型の深層学習

不正取引検知状況

- 過去12ヶ月分の取引明細情報及び口座情報の中から約170万件のデータを用い、特殊詐欺等の可能性が疑われる取引を機械学習で検知
- 取引データに事前処理を行い、有用と思われる特徴に変換後、さまざまな機械学習手法で学習
- 一例：特徴抽出(40分)後、約10秒で学習が完了、適合率53%, 再現率69%, F値60% で不正取引を検知
- 銀行担当者より「十分実用的. 現場で十分使える」とのコメント

		予測	
		通常取引と判定	不正取引と判定
正解	実際は通常取引	6910	49
	実際は不正取引	25	55

不正取引検知の一例

不正取引検知の実証実験

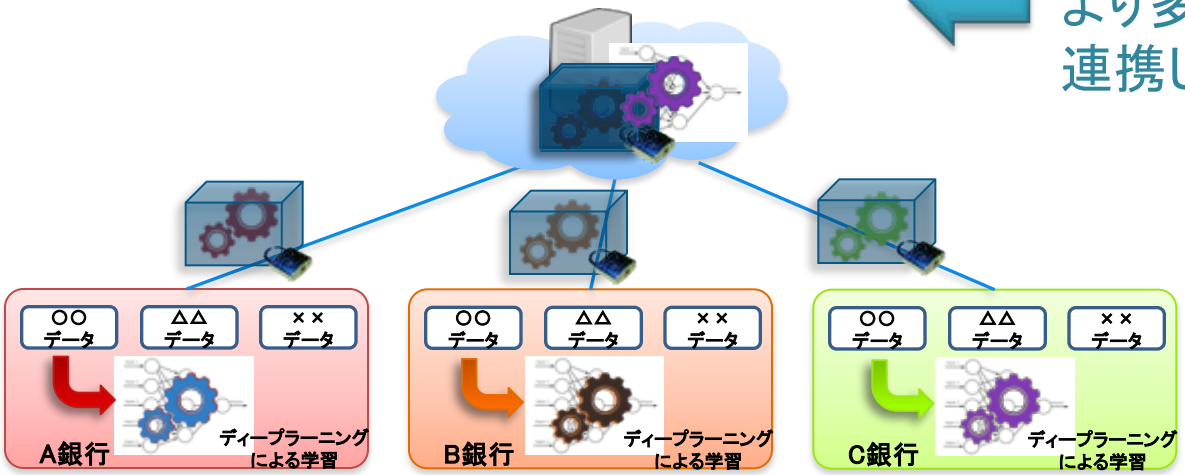
<Phase 0> 各銀行と個別に、データを暗号化しない状態で不正取引の検知を学習

現在取組中

<Phase 1> 複数銀行で連携し、各銀行での学習結果を暗号化して中央サーバに送信して更新

単独の銀行では件数/学習データが十分でないため、
複数の銀行からの学習モデルを統合することで
より精度が向上することを期待

より多くの金融機関と
連携して実施したい



実証実験の目標

- 本実証実験では、2021 年度末までに、プライバシー保護データ解析技術を活用し、各金融機関の顧客データを外部に開示することなく、複数機関で連携した学習が可能なシステム構築を目標
- 5社以上の金融機関と連携、検出精度80%以上で不正取引を検知するサービス開始を目指す
- 金融庁は、2019年秋のFATF[*1]対日審査に向け、各金融機関に対しAML[*2]高度化を求めており、**不正取引検知の高度化**は対応すべき社会課題

[*1] FATF: Financial Action Task Force,マネーロンダリング対策やテロ資金対策などにおける国際的な協調指導、協力推進などを行う政府間組織

[*2] AML: Anti-Money Laundering, マネーロンダリング対策

まとめ

- 安心・安全なSociety 5.0の実現にむけた NICTの プライバシー保護データ解析技術への取組みを ご紹介
  - ✓暗号化したままビッグデータ分類
  - ✓暗号化したまま近似なしで学習・識別
  - ✓暗号化したままデータ解析時の誤データ混入 防止
  - ✓暗号化したまま年収予測
  - ✓暗号化したまま組織横断で協調深層学習
    - 不正送金の検知精度向上に向けた実証実験