プライバシー保護データ解析技術の社会実装

Social Implementation of Privacy-Preserving Data Analytics

2019.12.19

花岡 悟一郎（産総研）
Goichiro Hanaoka
National Institute of Advanced Industrial Science and Technology (AIST)

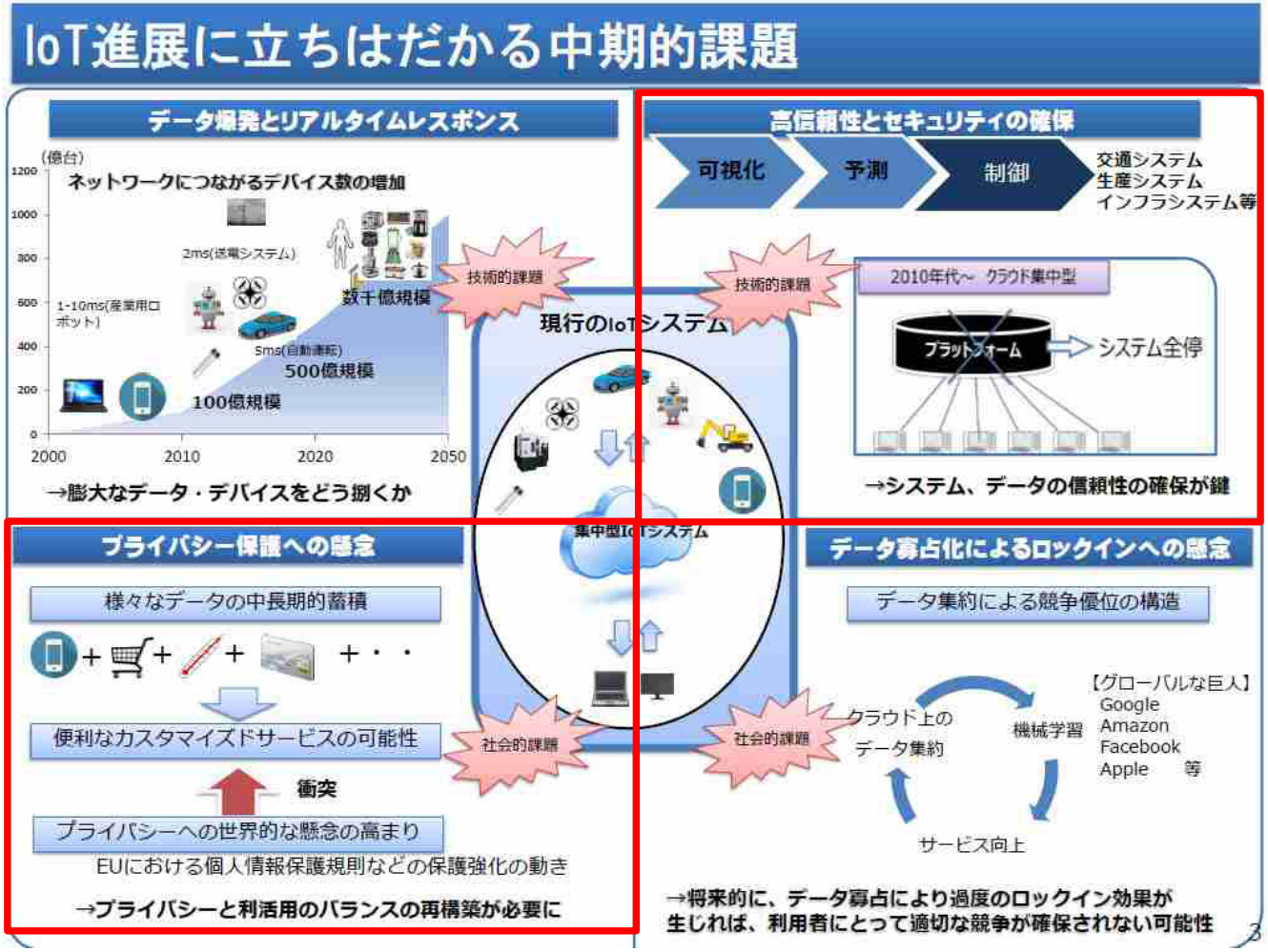
盛合 志帆（NICT）
Shiho Moriai
National Institute of Information and Communications Technology (NICT)

【背景】プライバシー侵害の懸念
Background: Privacy Issue

- 人工知能を機微情報に適用することで、個人ごとにサービスが提供される「優しい社会」が実現される。
  - By applying sensitive information (e.g., genomic data) to AI, specialized service for individuals will be provided.
- しかし、プライバシー侵害の懸念がある。
  - However, privacy violation will also be an issue.

オンライン自動健康診断サービスの例

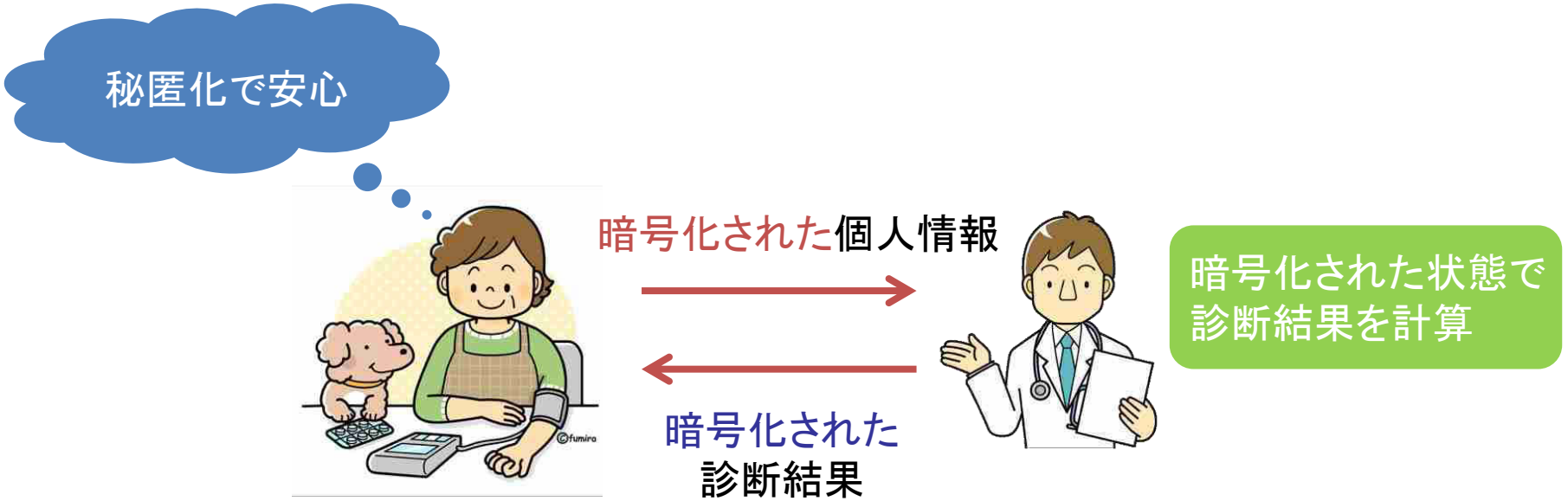
【背景】プライバシー侵害の懸念
Background: Privacy Issue



出典：IoT進展に立ちはだかる中期的課題への新たなアプローチ
（経済産業省商務情報政策局）

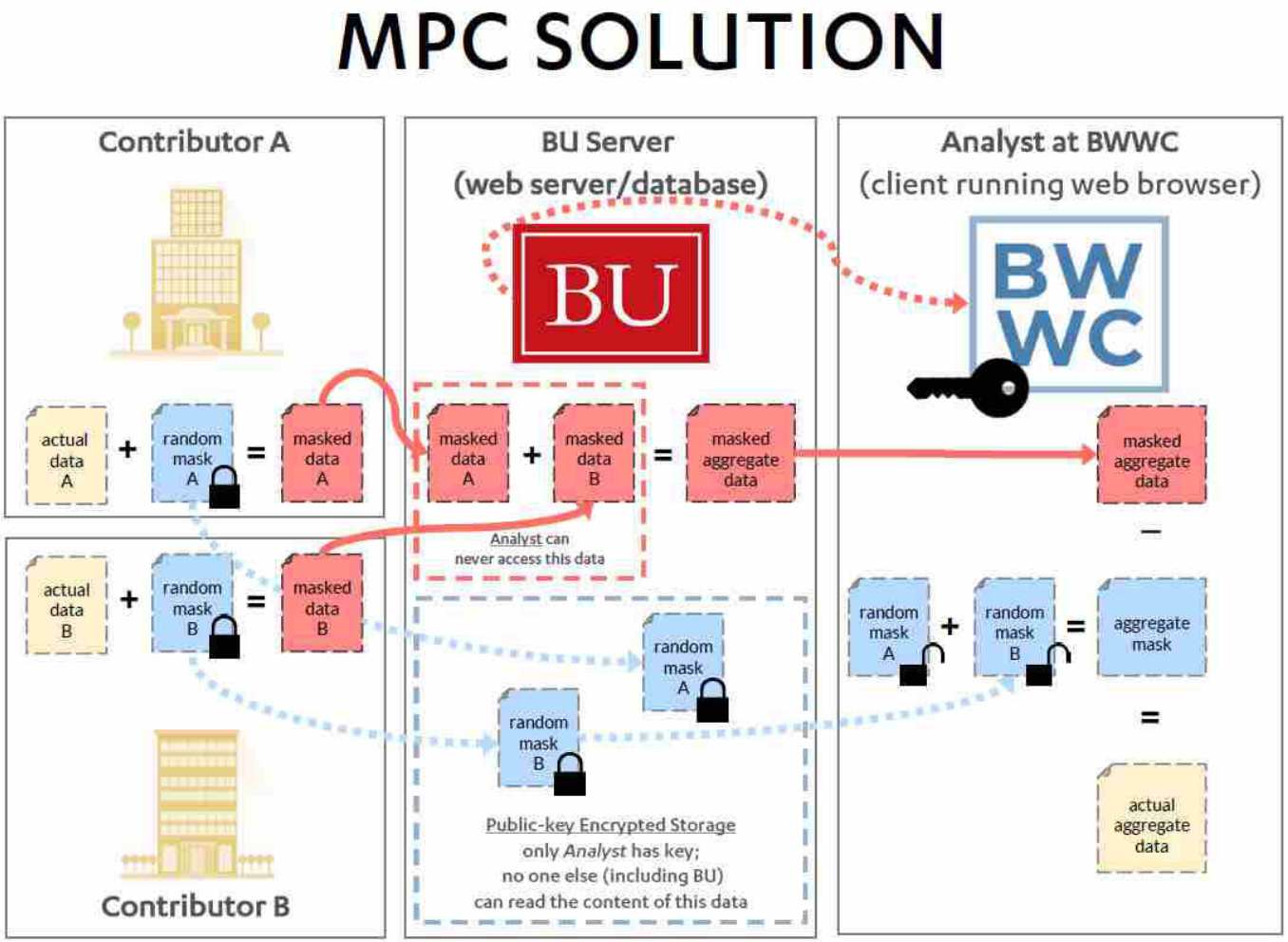
【背景】秘匿計算技術
Background: Privacy-preserving data analytics

- 情報を秘匿したまま解析を行う秘匿計算技術の研究開発が進んでいる。
  - Research on “Privacy-preserving data analytics” is being world-widely studied.



【背景】世界ではすでに実証実験例も

Proof of Concept experiment in Boston



https://rwc.iacr.org/2019/slides/lucy.pdf

【背景】秘匿計算技術の活用を国が期待
Expectations from Society

政策の方向性

○データの利活用権限の明確化（データオーナーシップ）

- 契約上のデータ取引の明確化を推進
  - データ流通契約ガイドラインを改訂する。

- 主要分野のデファクト形成と国際連携
  - 複数事業者が関連する工場内のデータ管理、ビル管理、海事等の具体的分野について協調領域に属するものは可能な限りシェアするとの理念の下、データ権限に関する具体的な事例づくりを行う。

- 秘密分散・計算技術の活用によるデータ協調環境整備の検討
  - 企業が漏洩を気にすることなく、ビッグデータ分析のためにデータを容易に提供できるよう、秘密計算技術等を活用した、第三者に提供する場合の運用の在り方について検討する。

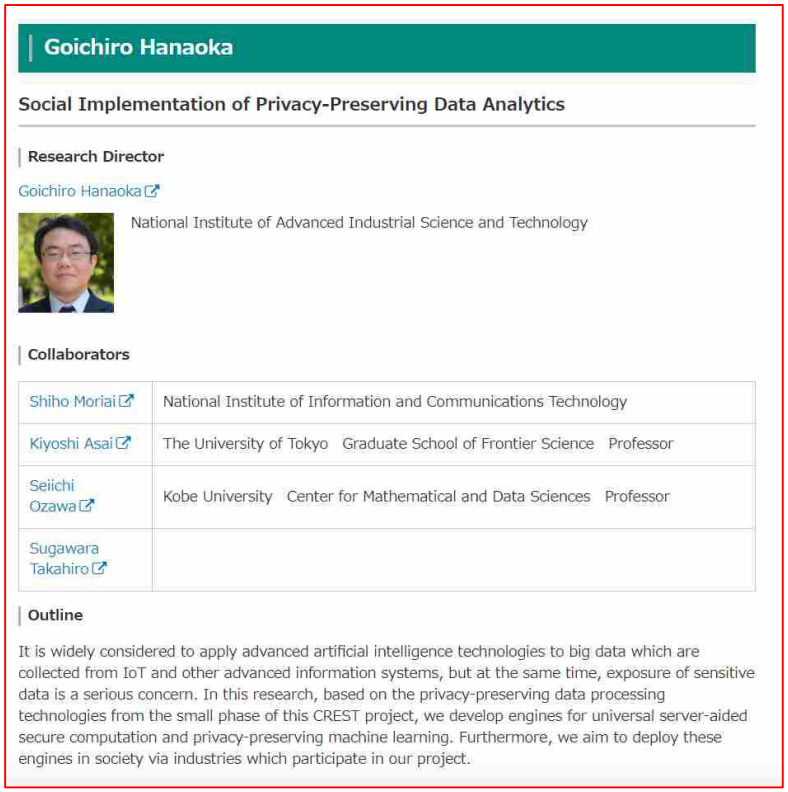
- データ利活用を萎縮する制約要因の解消
  - 具体的な加工手法の提示等を通じ、改正個人情報保護法に基づく匿名加工制度の活用を促進するとともに、データ流通促進WGにおいて企業からの個別相談を受けて解決するほか、カメラ画像の利活用などの自主ルールの策定を支援する。

15

出典：IoT進展に立ちはだかる中期的課題への新たなアプローチ（経済産業省 商務情報政策局）

JST-CREST [Artificial Intelligence]

Small phase (2016.12-2019.3)



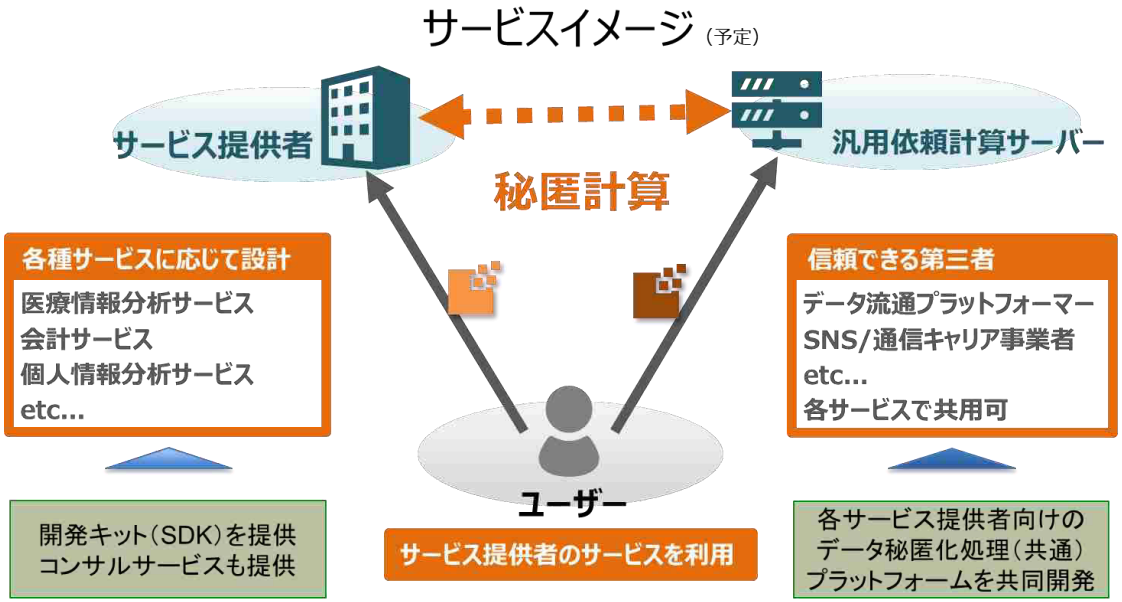
Goal: *Social Implementation* of Privacy-preserving data analytics (via industry)

Acceleration phase (2019.4-)

研究開発内容(1): Our Activity (1)

商用利用可能な汎用秘匿計算システムの開発

User-Friendly Universal Server-aided Secure Computation



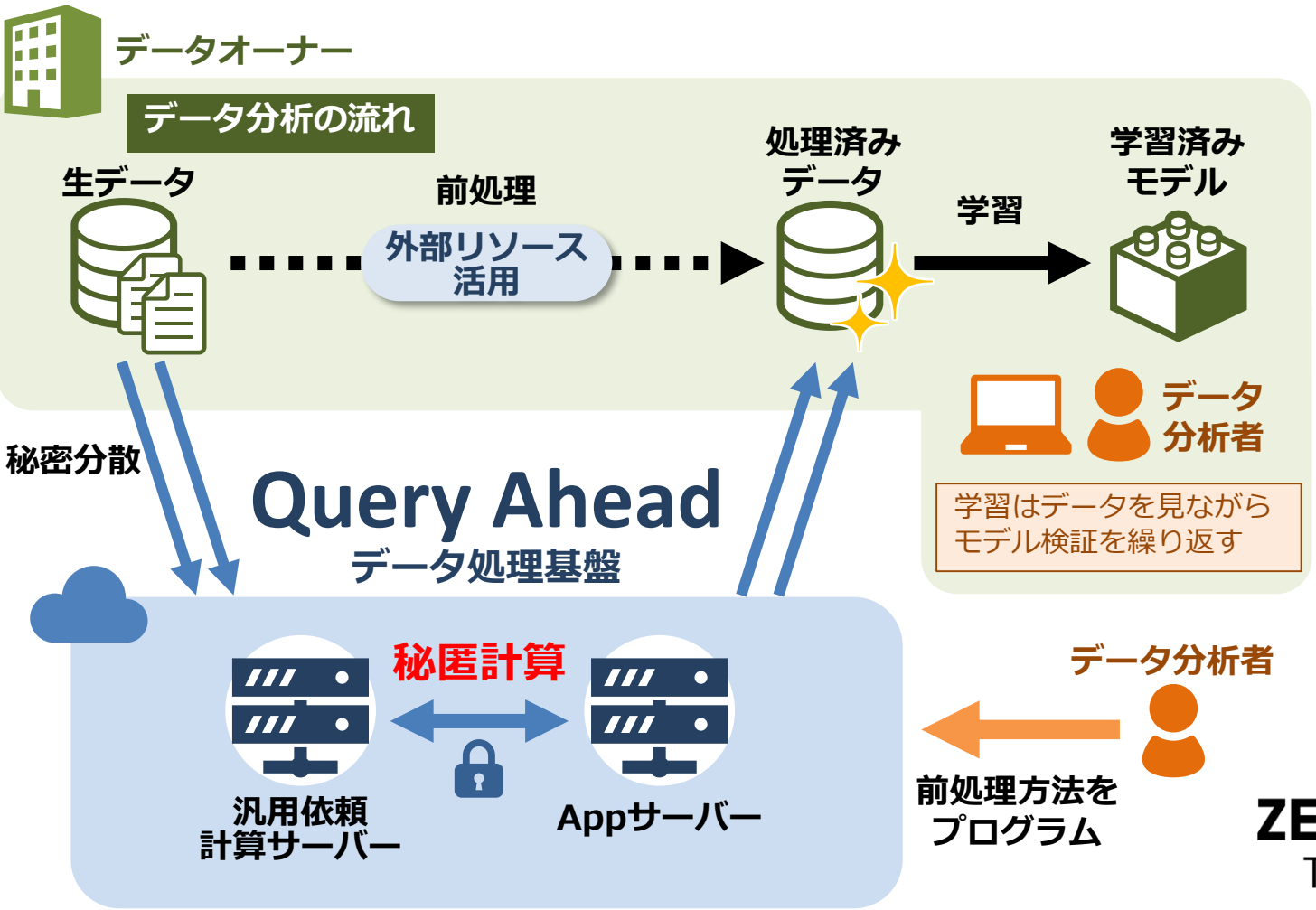
- アルゴリズムの理論的高速化
  - ✓最新の知見をもとに洗練化
  - ✓数学的安全性証明も
- 高速実装(アセンブラ実装等)
- 通信インターフェース
- 実サービスを提供可能な依頼計算サーバの設置
- ライブラリ・API化
  - ✓汎用秘匿化依頼計算エンジン
  - ✓専門的研究者でなくても利用可能に
- サンプルアプリケーションの実装
  - ✓事業展開の際の顧客向けサンプル

Easy-to-use and practical tools for implementing various types of applications of privacy-preserving data analytics.

研究開発内容(1): Our Activity (1)

商用利用可能な汎用秘匿計算システムの開発

User-Friendly Universal Server-aided Secure Computation



Example application: Privacy-preserving SQL-like DB operations

研究開発内容(1): Our Activity (1)

商用利用可能な汎用秘匿計算システムの開発

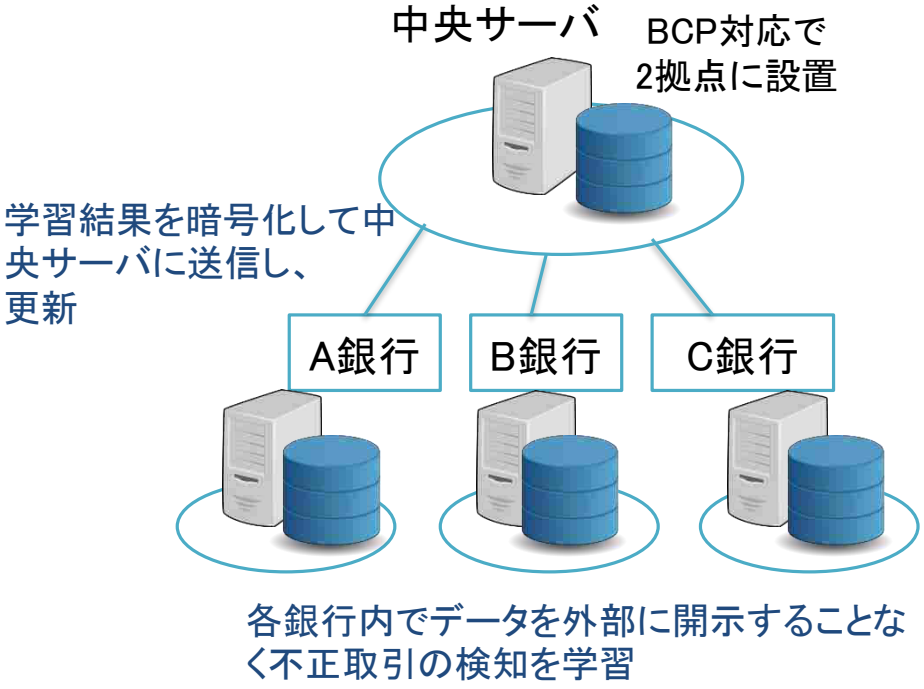
User-Friendly Universal Server-aided Secure Computation

デモ

Demonstration: Privacy-preserving SQL-like DB operations

研究開発内容(2)

プライバシー保護金融データシステムの開発



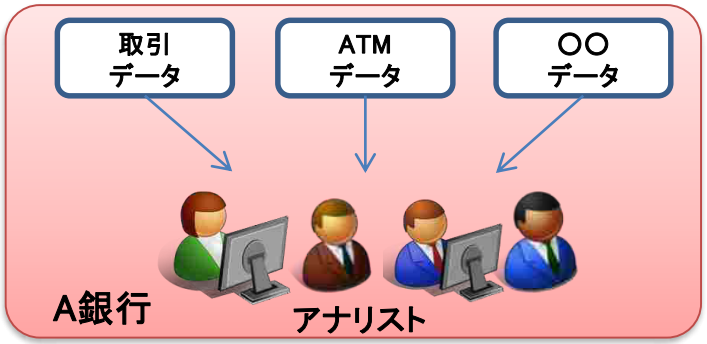
銀行より実データを得て以下を推進:

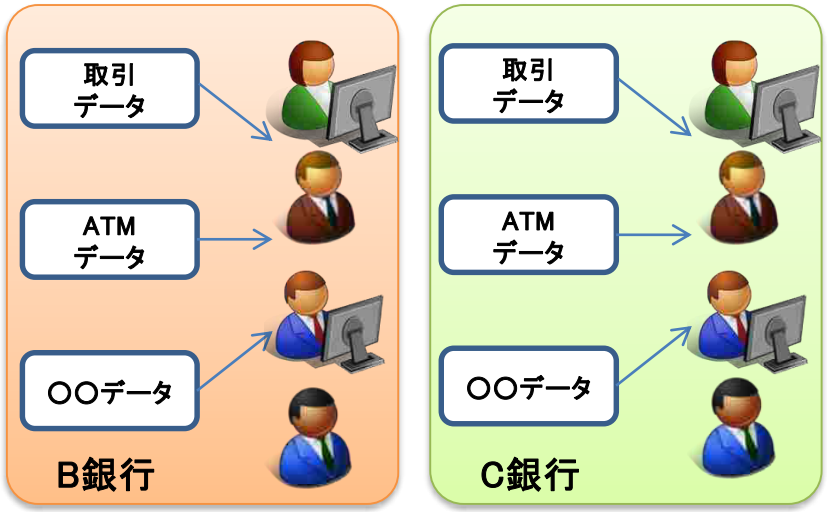
- 秘匿計算技術の高度化
  - ✓ 高速化・安全性検証
- 応用手法技術の開発
  - ✓ プライバシー保護機械学習エンジンの開発・改良
- 社会実装
  - ✓ 複数の金融機関と連携し、プライバシー保護ディープラーニングによる不正取引検知の実証実験
  - ✓ 実用システムの実装・実運用

eltes

金融分野における課題と構想

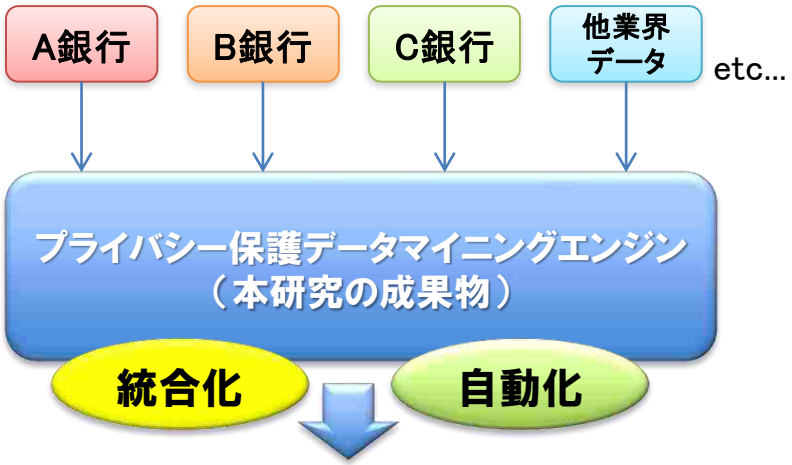
現状





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

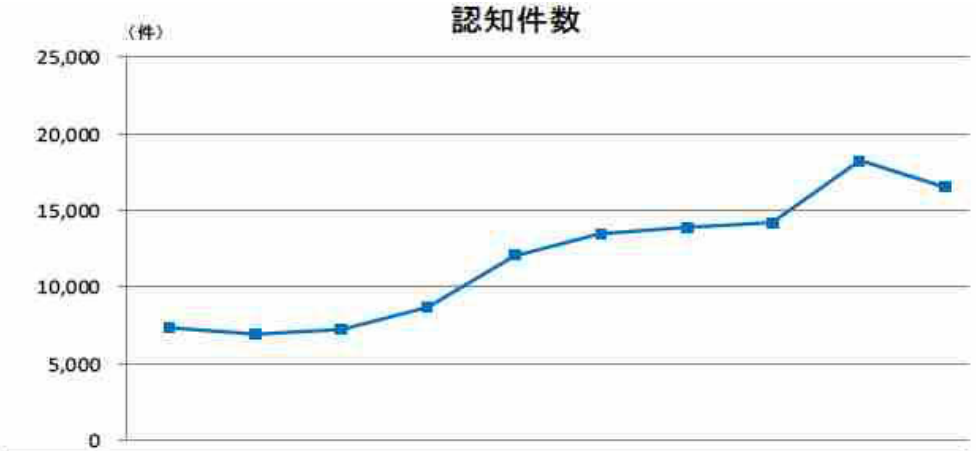
- 調査コスト削減
- 調査属人化の回避
- 調査精度の向上
  - ➢ 今まで見つからなかった検知が可能に！

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

➡ 口座情報・取引情報等から疑わしい取引を検知

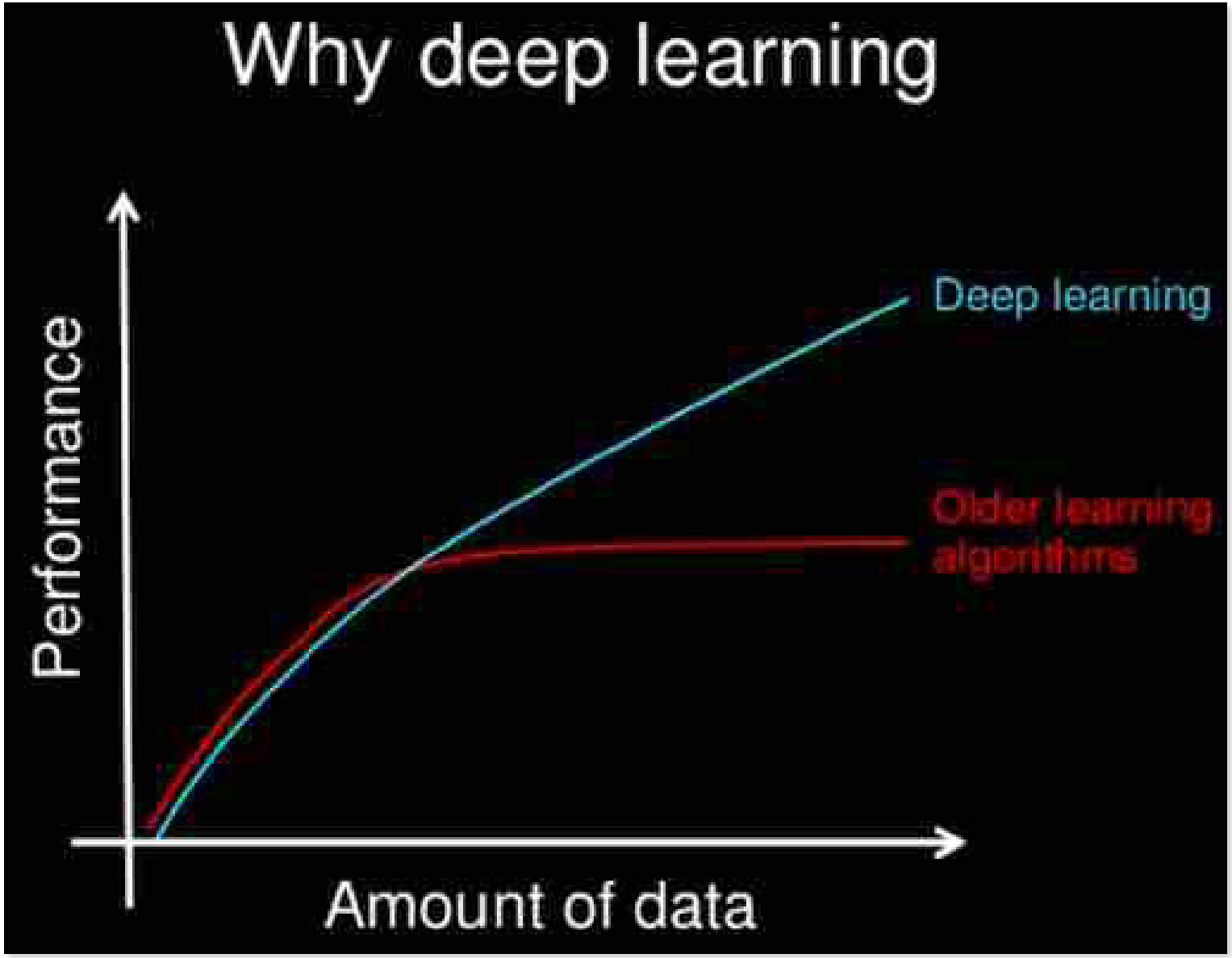
*特殊詐欺
面識のない不特定の者に対し、電話その他の通信手段を用いて現金などをだまし取る詐欺



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

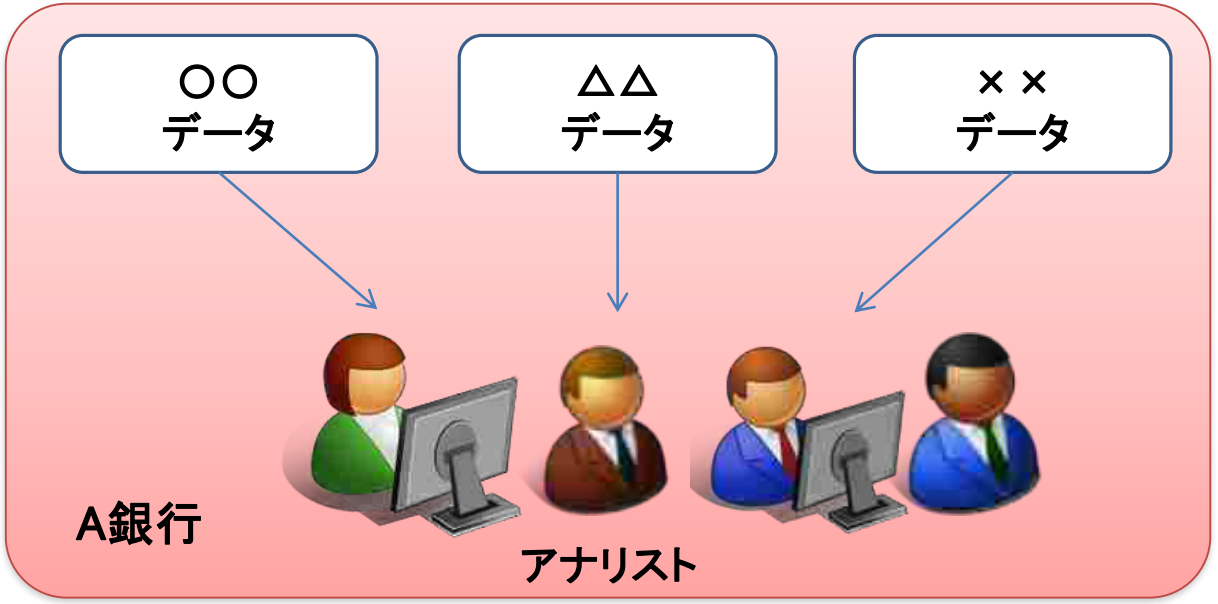
警察庁「平成30年における特殊詐欺認知・検挙状況等について」

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



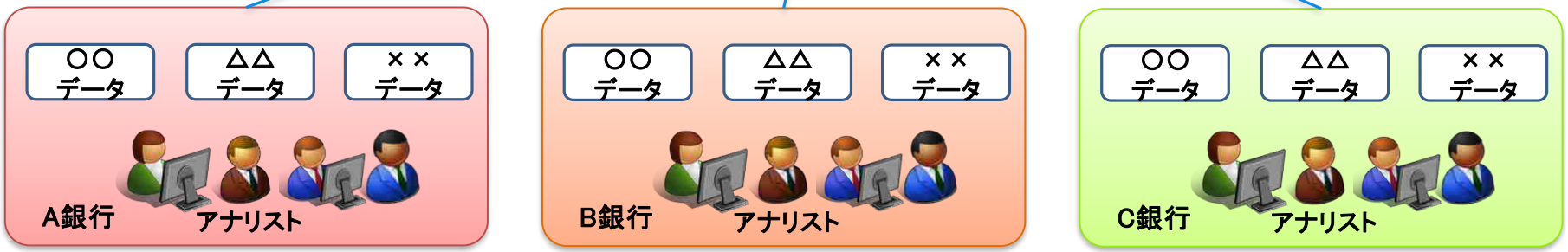
異常検知においては、異常データが
少なすぎることも

⇒よい分析結果が得られない

研究開発内容(2)

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！

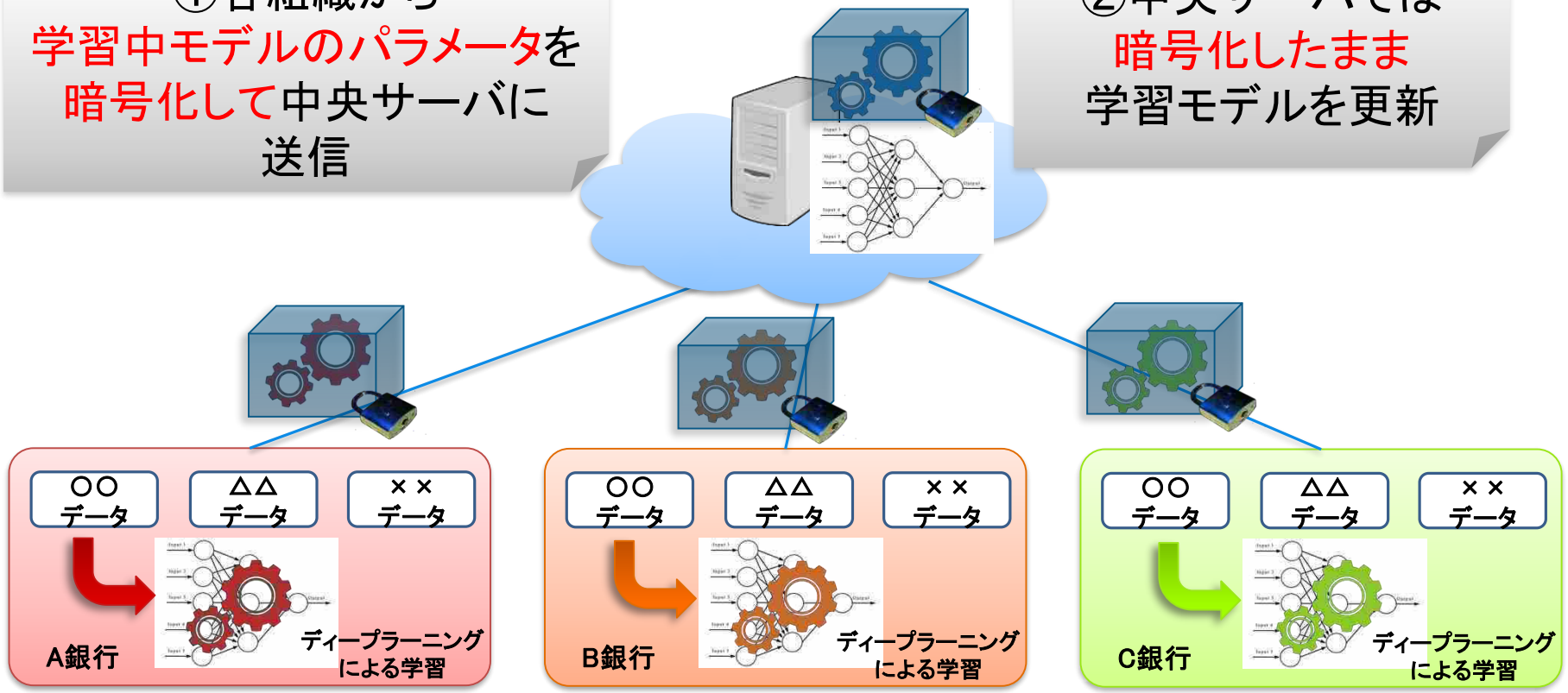


研究開発内容(2)

外部にデータ開示することなく深層学習を実現するには

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

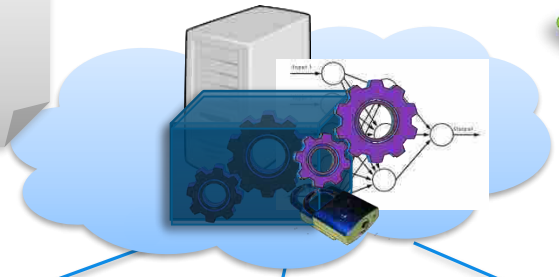
②中央サーバでは
暗号化したまま
学習モデルを更新



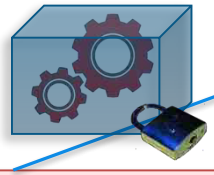
研究開発内容(2)

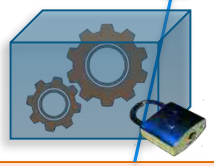
外部にデータ開示することなく深層学習を実現するには

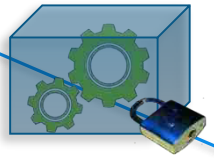
③各組織では
中央サーバで更新された
学習モデルをダウンロード、
精度の高い分析が可能に



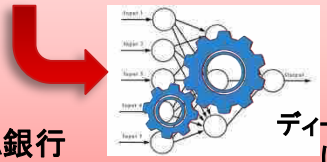
中央サーバにも
第三者にも
データ漏洩の
危険性なし！







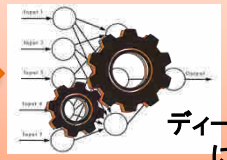
○○データ　△△データ　××データ



A銀行

ディープラーニング
による学習

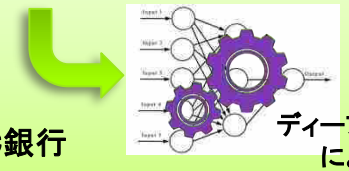
○○データ　△△データ　××データ



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

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

2019.2.1　共同プレスリリース

神戸大学　eltes　NICT 国立研究開発法人 情報通信研究機構

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

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

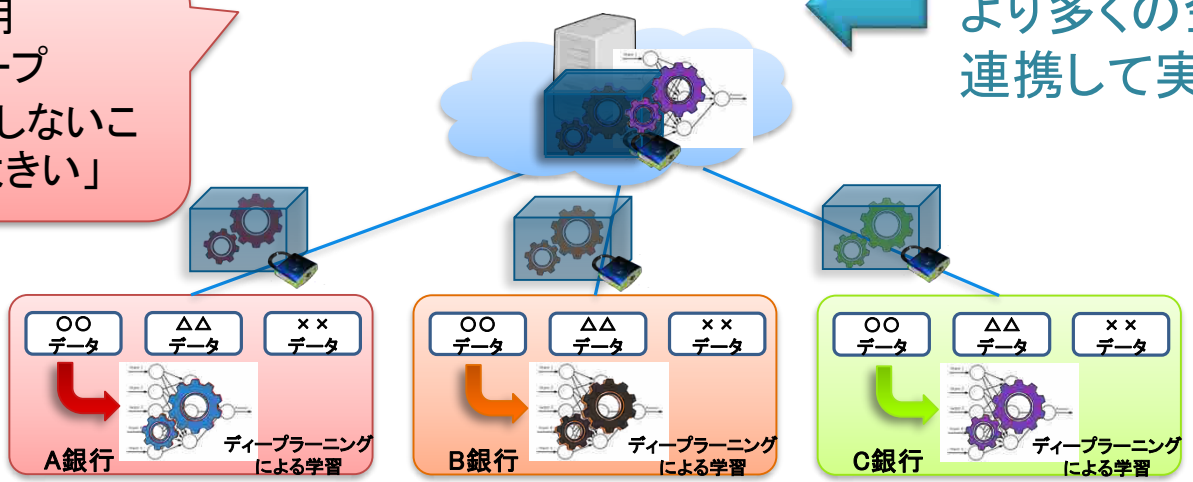
現在取組中

<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

ちばぎん
千葉銀行が参加表明
金融機能管理グループ
海老原調査役「参加しないことの不利益の方が大きい」

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

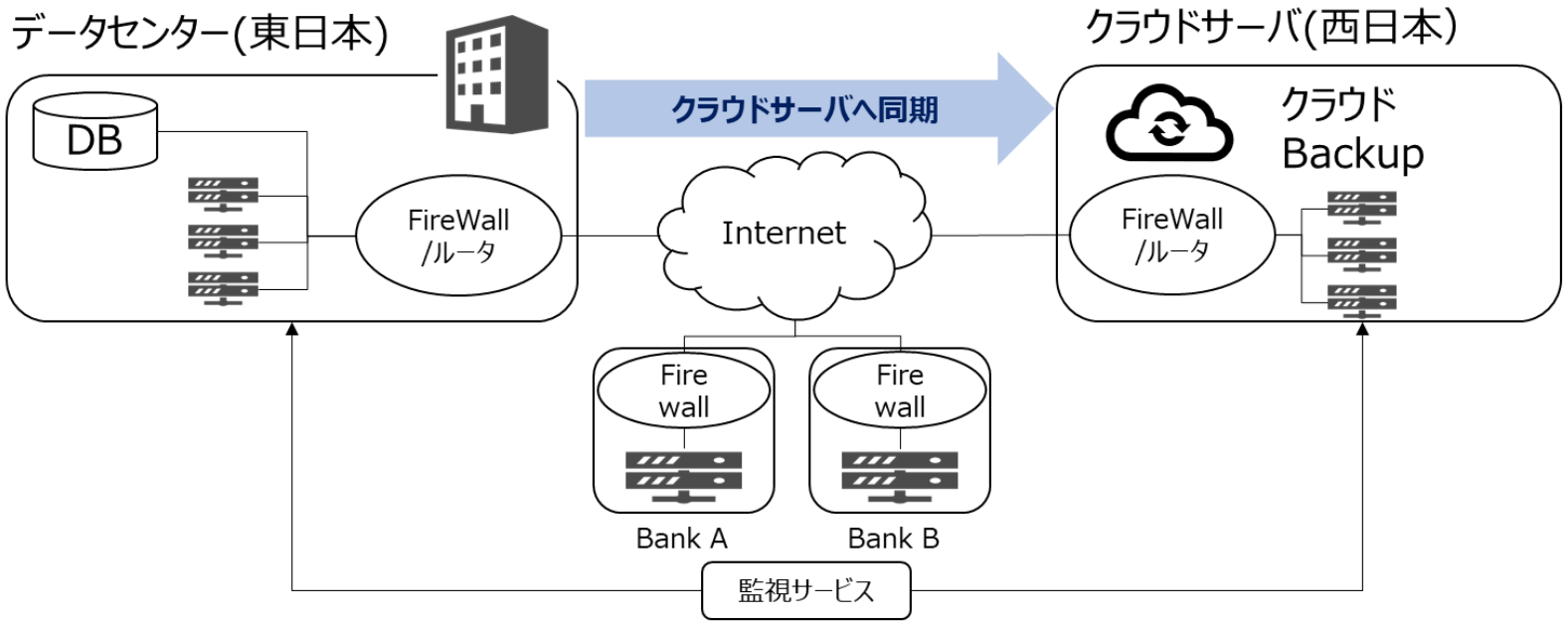
[*1] FATF: Financial Action Task Force,マネーロンダリング対策やテロ資金対策などにおける国際的な協調指導、協力推進などを行う政府間組織

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

プレスリリース後の反響等

- 複数メディアに掲載
  - 日経新聞、朝日新聞等 5紙＋日経 x TECH等 Web記事
- 複数の銀行からのコンタクト
  - 実証実験開始に向けて調整中
- 金融庁 フィンテック室
  - 金融庁Fintech実証実験ハブ参加のお誘い
- その他のお問い合わせ
  - NVIDIA, 京都府警, …

実証実験システム概要



- ✓ 上記のような2拠点のデータセンターを構築し、BCP対応をするように設計。
- ✓ ネットワーク構築にあたっては、金融機関におけるNW構築に実績のあるISID-AOが主に担当。
- ✓ 今後の直近の大まかなスケジュールは以下の通り。

	4月	5月	6月	7月	8月
設計					
サーバー構築					
サーバー設定					
サーバーデータセンター搭載					
バックアップ用サーバー搭載					

課題解決がもたらすイノベーションの創出

- プライバシー保護データ解析技術に基づく
  ビジネス展開が可能に

- 人工知能に基づく、機微情報を用いた
  情報サービスの提供が加速

- 機微情報を用いたデータ社会の恩恵を、
  誰もが、簡単に、安全に享受

誰もが、簡単に、安全に → イノベーション