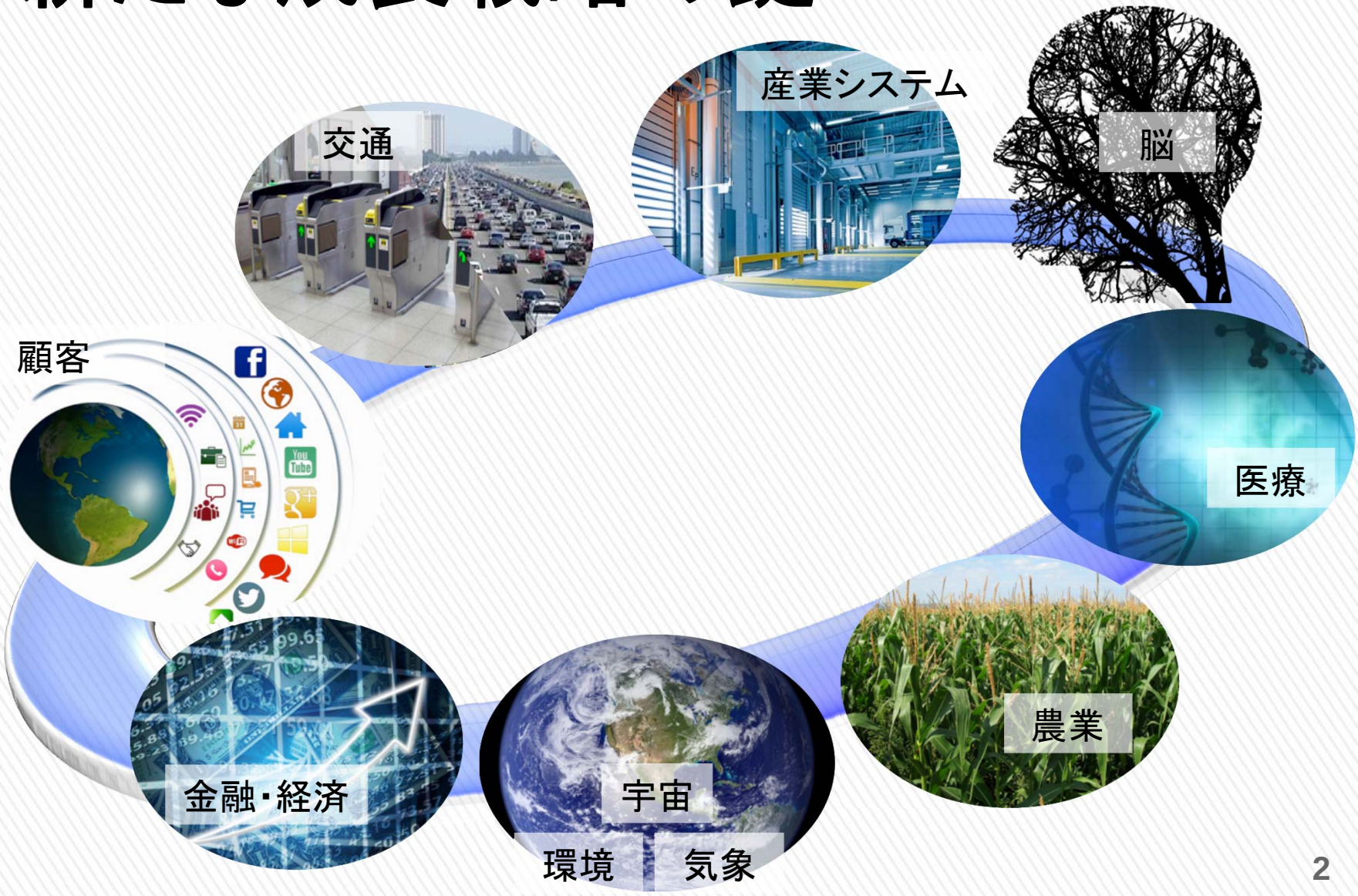
複数組織データ利活用を促進するプライバシー保護データマイニング

【研究代表者】 国立研究開発法人情報通信研究機構
盛合　志帆

【共同研究者】 神戸大学　　小澤 誠一
(株)エルテス　菅原 貴弘

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

データ統合利活用：
新たな成長戦略の鍵



データセキュリティの確保とプライバシー保護が課題

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分析や異常検知

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
分野横断でのデータ利活用を促進

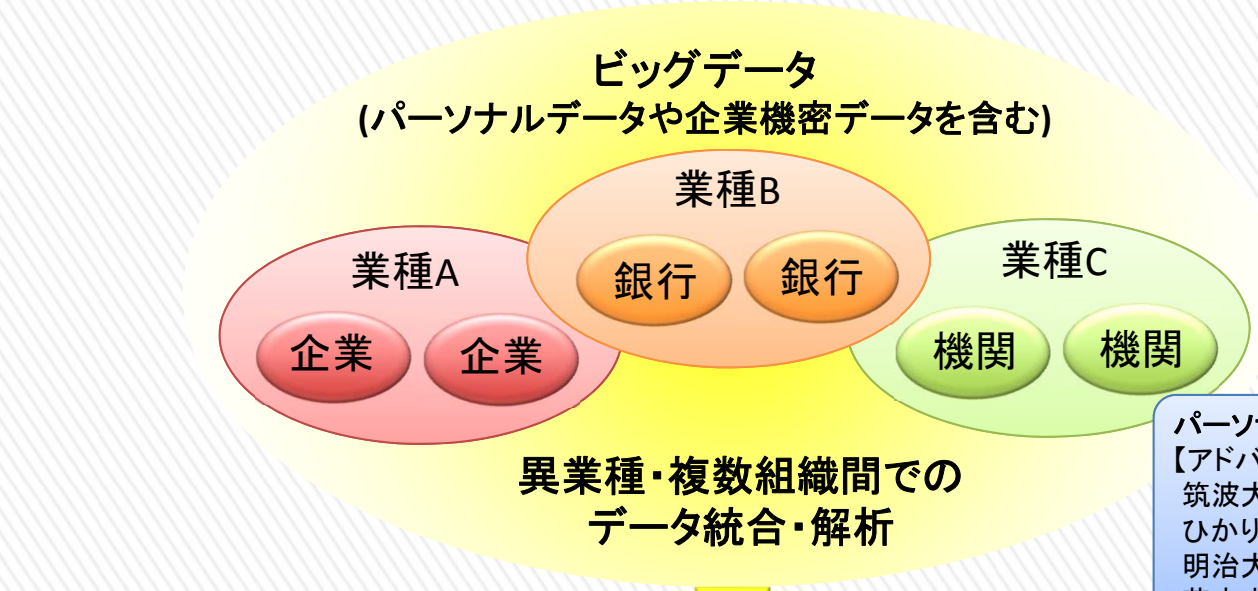
次世代AI 技術による
データ解析

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

JST CREST「イノベーション創発に資する人工知能技術の創出と統合化」

研究課題「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」

研究体制



パーソナルデータ取扱研究開発事務審議委員会
【アドバイザー】

筑波大学 准教授	石井　夏生利
ひかり総合法律事務所　弁護士	板倉　陽一郎
明治大学 教授	菊池　浩明
花水木法律事務所 弁護士	小林　正啓

機械学習アルゴリズムの活用

データ分類・予測・異常検出

暗号・プライバシー保護技術の活用

データ機密性・プライバシーの確保

神戸大学

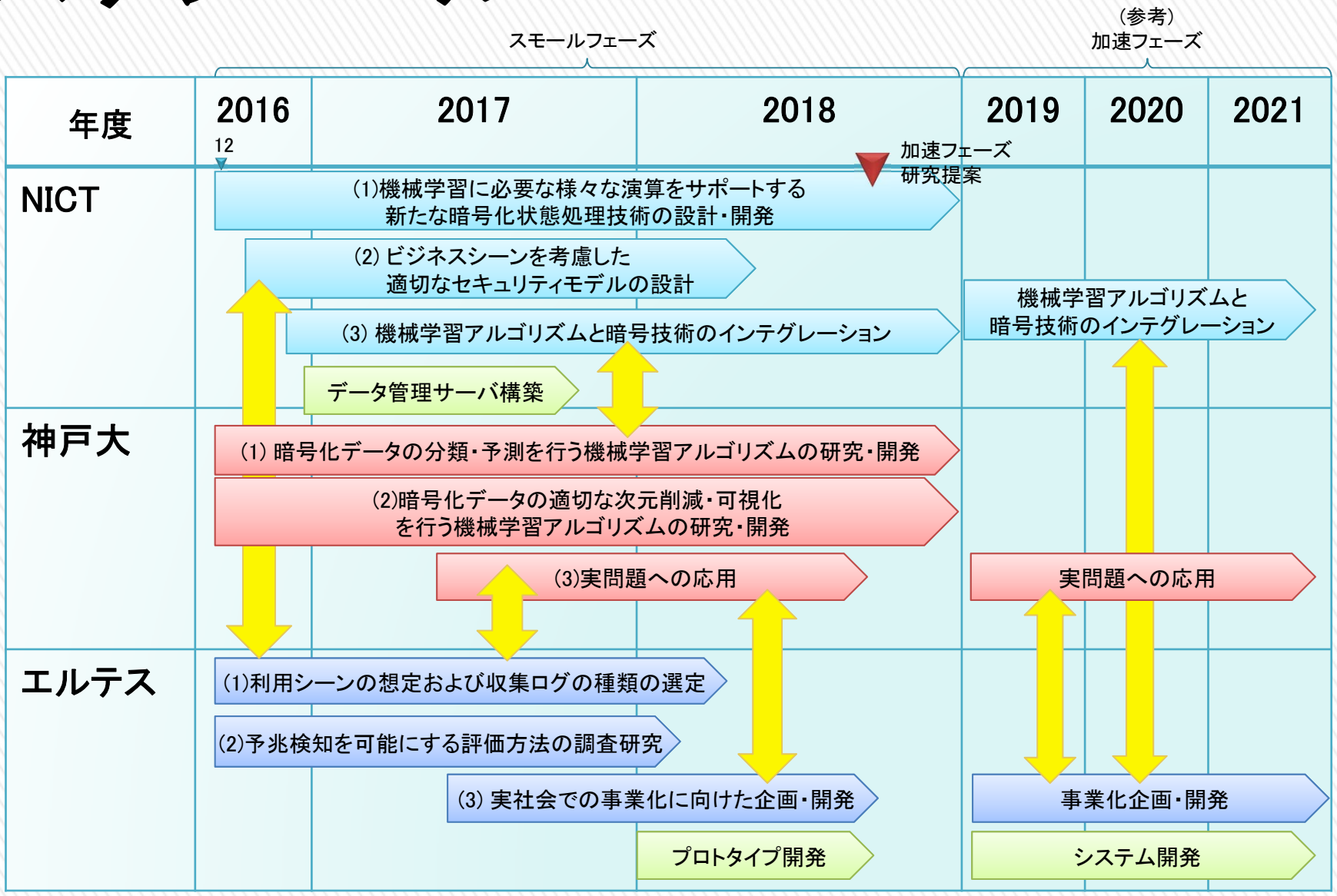
国立研究開発法人 情報通信研究機構

リスク検知に特化したビッグデータ解析

金融業界での社会問題の解決

eltes
Exploring Limitless Talents for e-Solutions

スケジュール

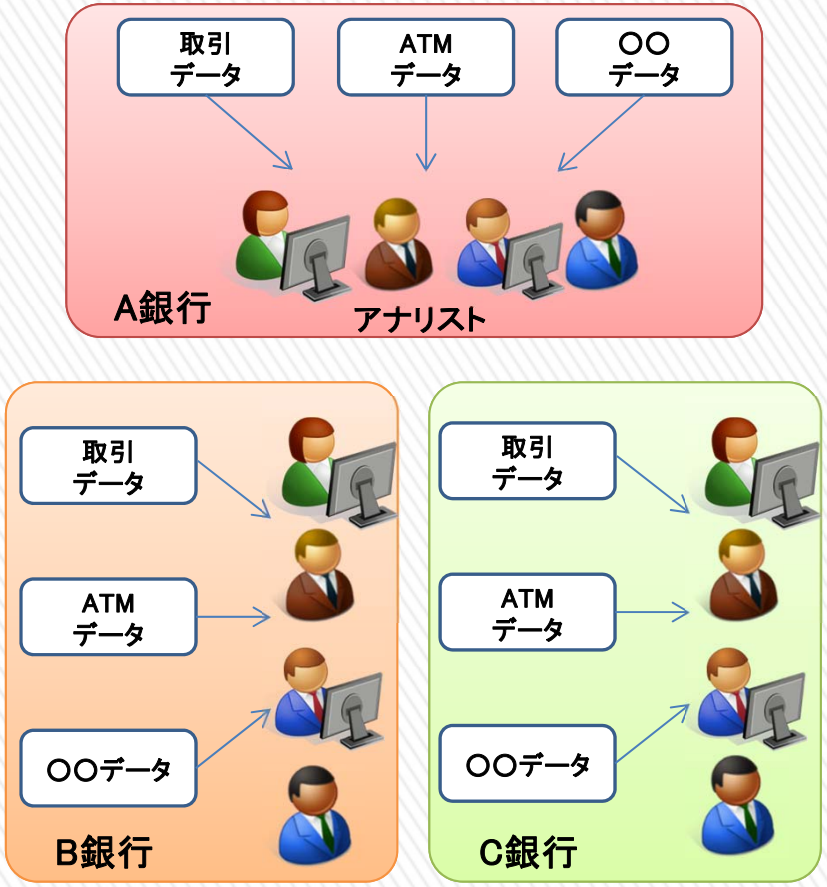

スモールフェーズ
（参考）
加速フェーズ
年度
2016
12
2017
2018
2019
2020
2021
加速フェーズ
研究提案
NICT
(1)機械学習に必要な様々な演算をサポートする
新たな暗号化状態処理技術の設計・開発
(2) ビジネスシーンを考慮した
適切なセキュリティモデルの設計
(3) 機械学習アルゴリズムと暗号技術のインテグレーション
機械学習アルゴリズムと
暗号技術のインテグレーション
データ管理サーバ構築
神戸大
(1) 暗号化データの分類・予測を行う機械学習アルゴリズムの研究・開発
(2)暗号化データの適切な次元削減・可視化
を行う機械学習アルゴリズムの研究・開発
(3)実問題への応用
実問題への応用
エルテス
(1)利用シーンの想定および収集ログの種類の選定
(2)予兆検知を可能にする評価方法の調査研究
(3) 実社会での事業化に向けた企画・開発
事業化企画・開発
プロトタイプ開発
システム開発

研究開発ステップ


実社会での事業化・フィードバック
事業化企画・システム開発
プロトタイプ開発・検証
実データへの適用・検証
プライバシー保護データ解析手法の開発
暗号化したまま
深層学習
機械学習
回帰分析
異常検知
内積計算
行列乗算
加速フェーズ
スモールフェーズ

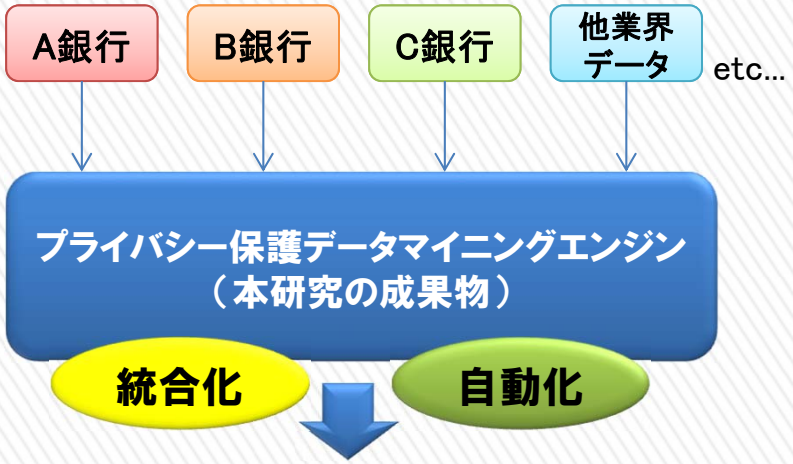
めざす構想

現状



個々の金融機関内で分析

めざす構想

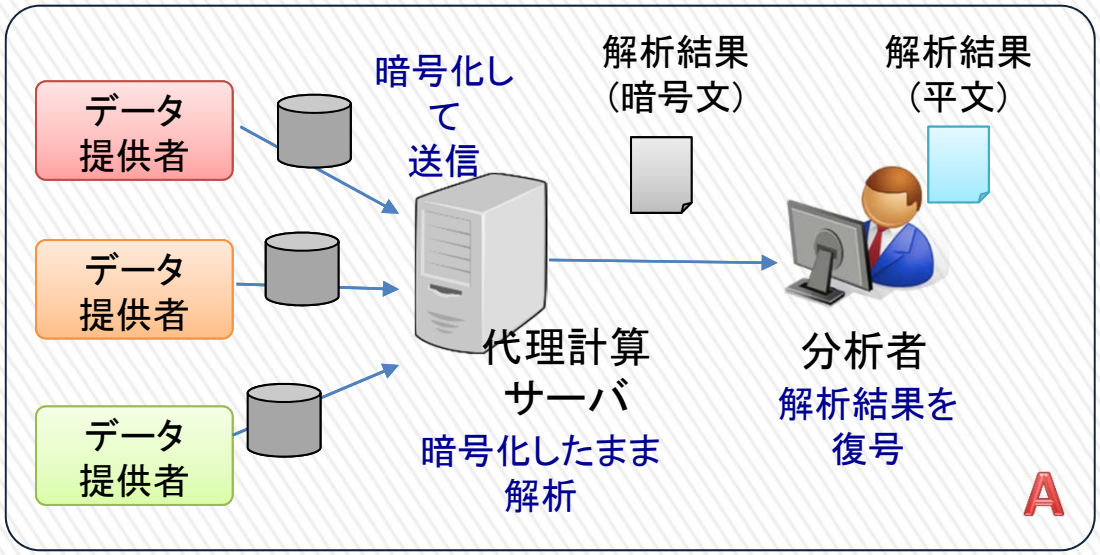


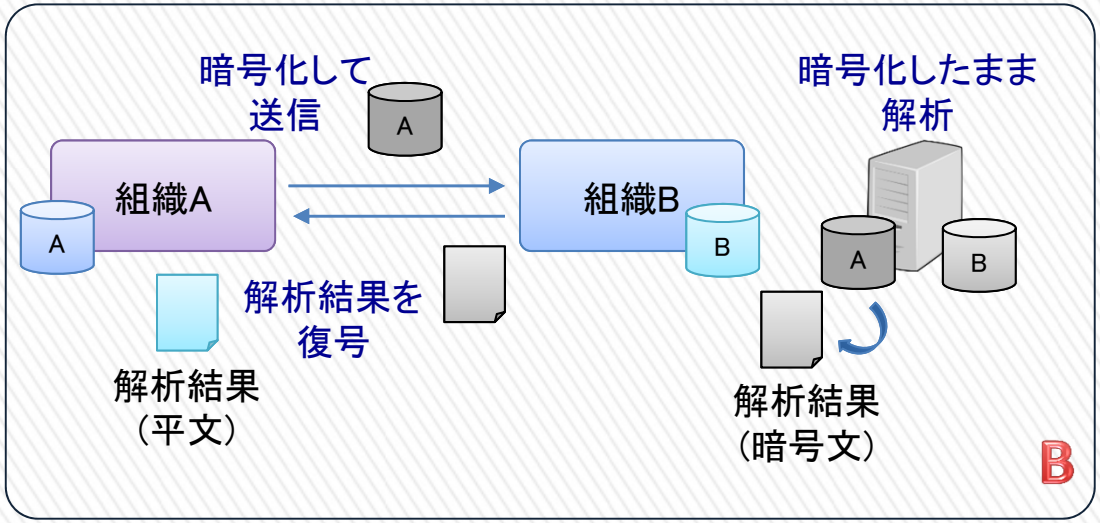
不正取引の検知,
与信管理, マーケティング

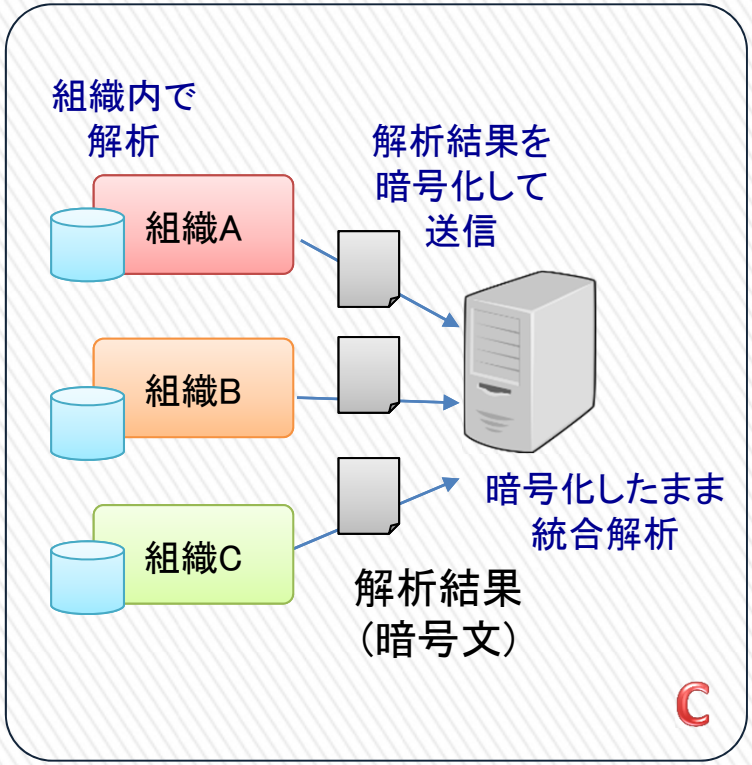
- 調査コスト削減
- 調査属人化の回避
- 調査精度の向上
  - 今まで見つからなかった検知が可能に！

プライバシー保護データ解析技術

プライバシー保護データ解析利用シナリオ





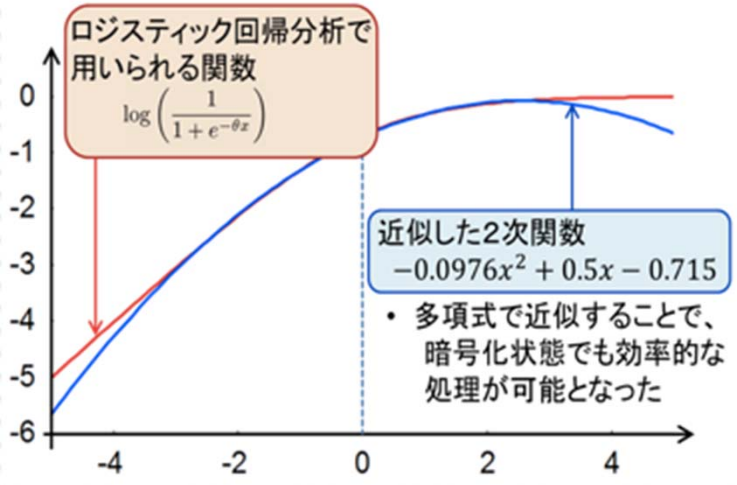


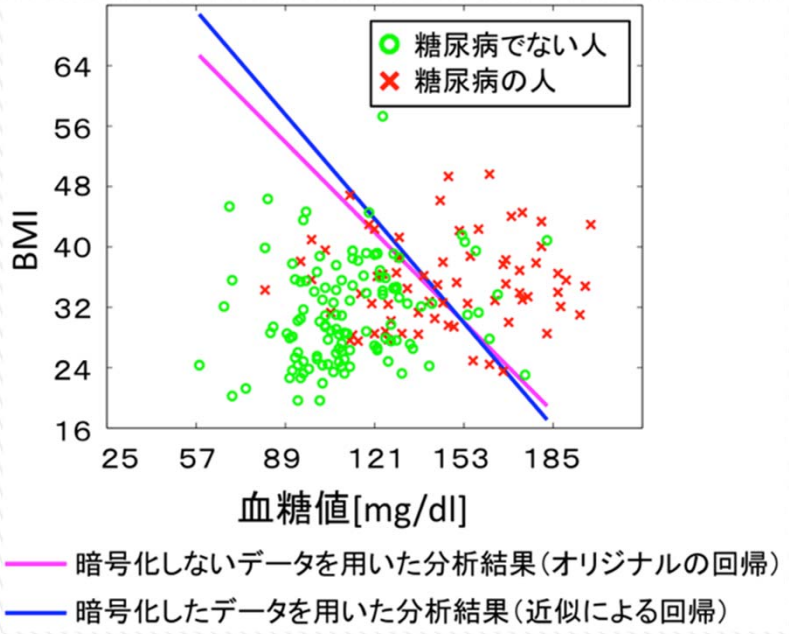
暗号化したままビッグデータ分類

» 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)



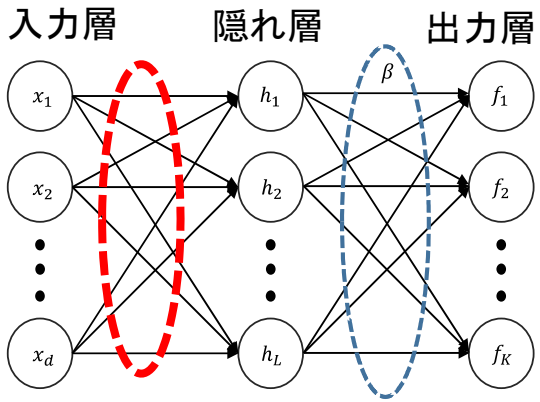


暗号化したまま
近似なしで学習・識別

*Privacy-Preserving
Extreme Learning Machine

» 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

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



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

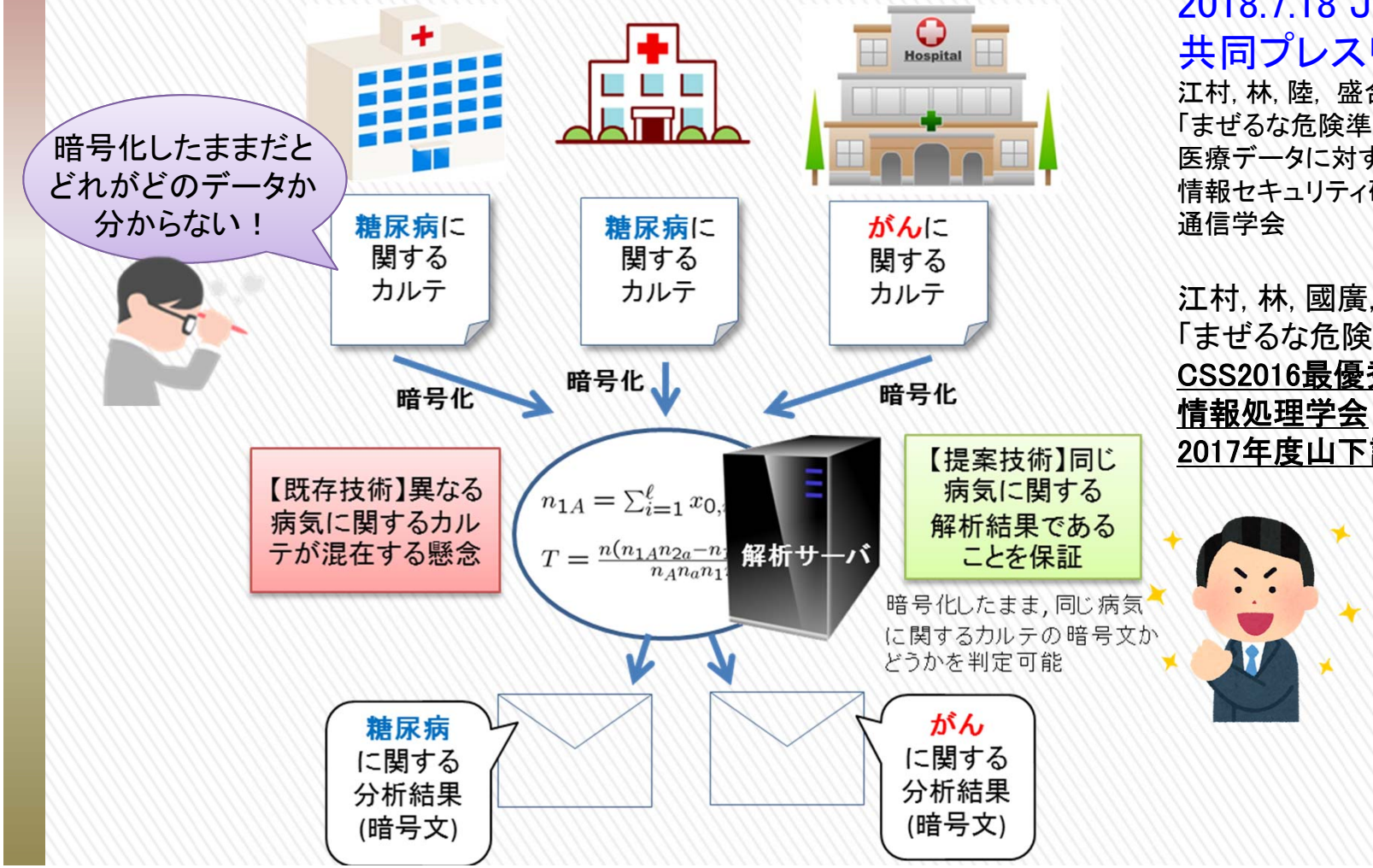
(L:隠れ層のノード数)

+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技術



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

プレスリリース「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
～中身を見なくても誤データ混入防止、医療ビッグデータの安全な利活用へ～」

病院

遺伝情報を管理する
検査機関

	病名1	病名2	…
A	病気あり	病気なし	…
B	病気なし	病気なし	…
C	病気あり	病気あり	…

匿名化された医療データ
（A, B, Cは仮ID）

	遺伝的特徴
A	あり
B	なし
C	なし

1. 病名と病気の
有無をNICT技術
で暗号化

	jdiqeji	kdqfkw4	…
A	Mqnmi4;nrf	Nfal4cgh	…
B	Ifm4:ngf	Qafm4c4	…
C	Yf4cdg5	Afcm4t	…

暗号化された医療データ

2. 医療データの
暗号文を送付

	jdiqeji	kdqfkw4	…
A	Mqnmi4;nrf	Nfal4cgh	…
B	Ifm4:ngf	Qafm4c4	…
C	Yf4cdg5	Afcm4t	…

3. 医療データを暗号化
したまま解析
(各個人の病気の
有無を知ることはない)

4. 解析値の
暗号文を送付

jdiqeji	kdqfkw4	…
Kvaocnr	84nhfxn4c	…

解析値 (遺伝的特徴と病気の両方を持つ人数) の暗号文

NICT技術により異なる病気の暗号文が混在した場合でも
検出可能 (誤データ混入防止)

5. 復号

	病名1	病名2	…
遺伝的特徴	○○人	××人	…

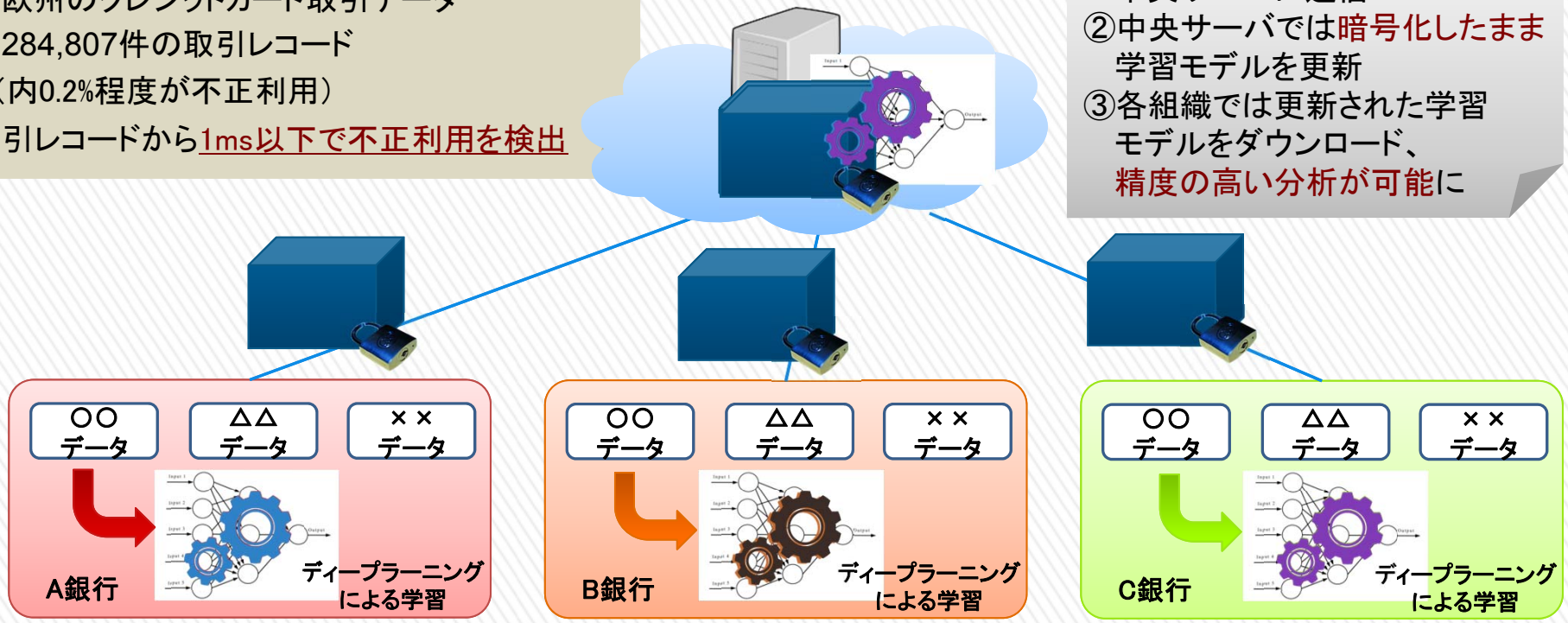
6. 各個人の遺伝情報を知ることなく解析値を得る

プライバシー保護ディープラーニング

» 組織が持つデータを外部に開示することなく
深層学習を行うプライバシー保護深層学習システム

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
◆284,807件の取引レコード
（内0.2%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

①各組織から学習済モデルの
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
③各組織では更新された学習
モデルをダウンロード、
精度の高い分析が可能に



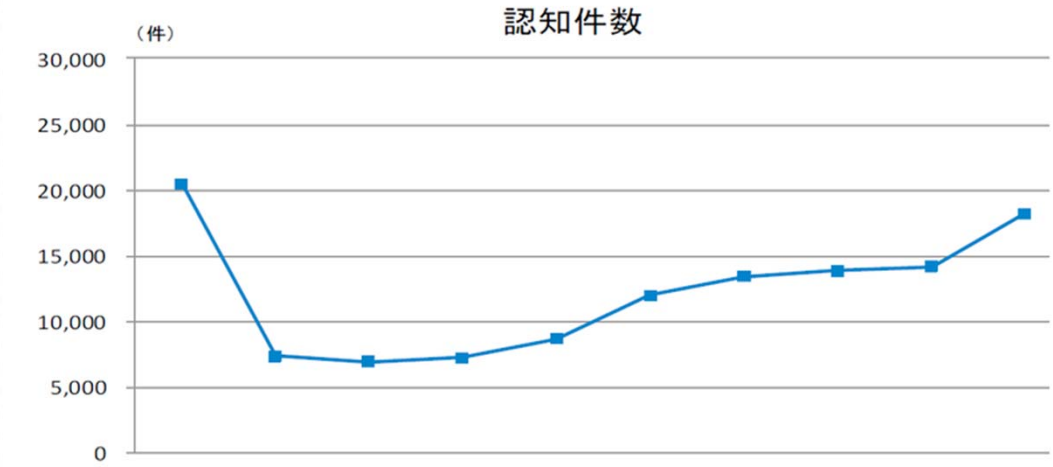
複数組織で連携した分散協調型の深層学習

現在進めている実証実験

不正取引(振り込め詐欺等)検知

- 特殊詐欺*による被害金額 **390億円**（2017年）
  - 1件当たりの被害金額は226.7万円
- 口座情報・取引情報等から疑わしい取引を検知
- 単独の銀行では事案/学習データが十分多くないため、複数の銀行からの学習モデルを統合することで精度を向上

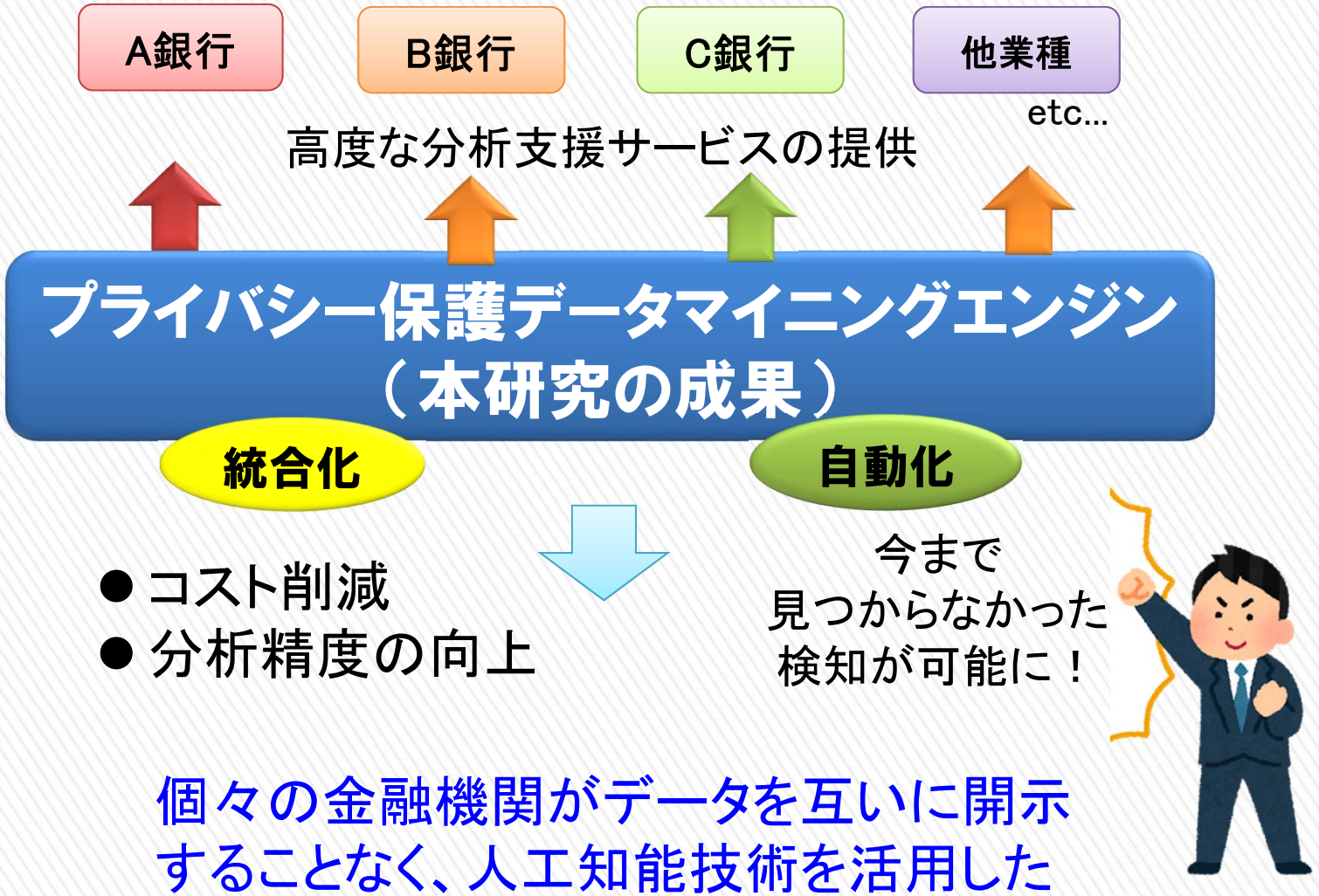
*特殊詐欺
面識のない不特定の者に対し、
電話その他の通信手段を用いて、
現金などをだまし取る詐欺



区分＼年次	20年	21年	22年	23年	24年	25年	26年	27年	28年	29年
認知件数	20,481	7,340	6,888	7,216	8,693	11,998	13,392	13,824	14,154	18,201

警察庁「平成30年上半期における特殊詐欺認知・検挙状況等について」

今後の展望



個々の金融機関がデータを互いに開示することなく、人工知能技術を活用した高度なデータ分析支援サービスを提供