

# 暗号技術とAIの融合による 秘密計算技術

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  
主任研究員      レ   チュウ   フォン

2019年7月18日

# 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

データ漏洩対策は大丈夫？

交通

産業システム

脳

私のプライバシーは守られている？

移動履歴

購買履歴

興味・関心

検索キーワード

医療

金融・経済

宇宙

農業

環境 気象

# 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



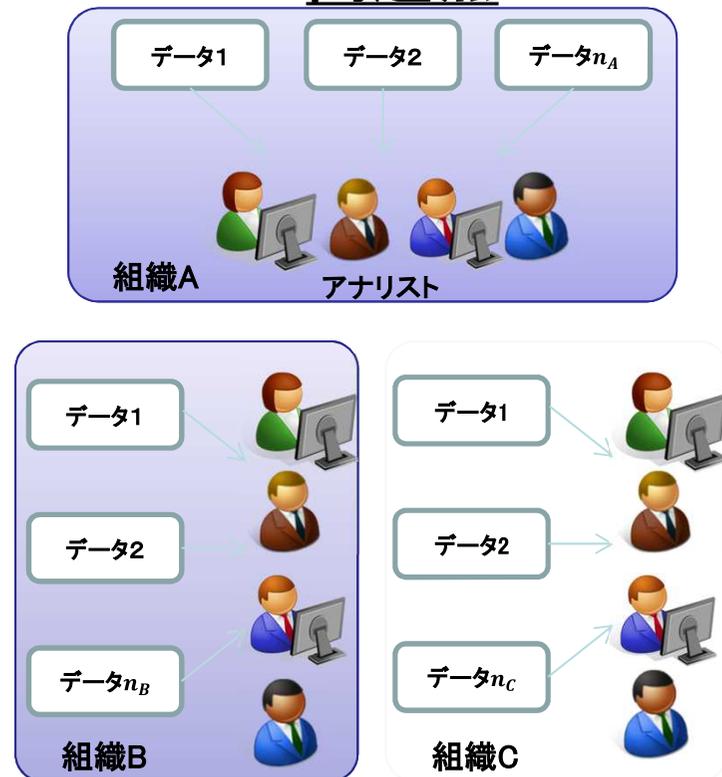
**暗号**により  
データの機密性を  
確保することで  
**組織横断**でのデータ利活用を促進

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

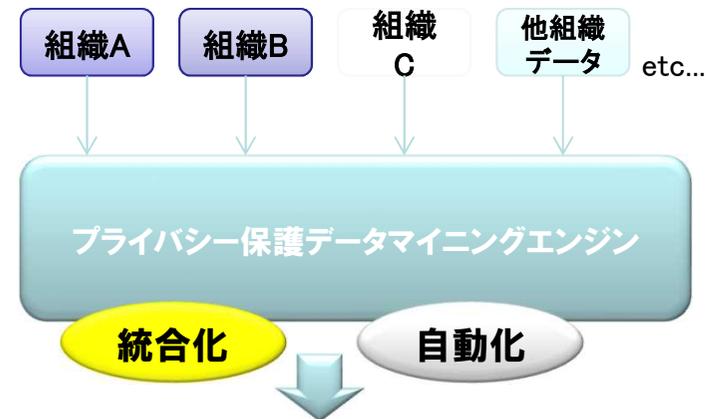
# 現状 と めざす構想

## 現状(従来技術)とその 問題点



個々の組織内で分析、組織横断でのデータ利活用ができていない

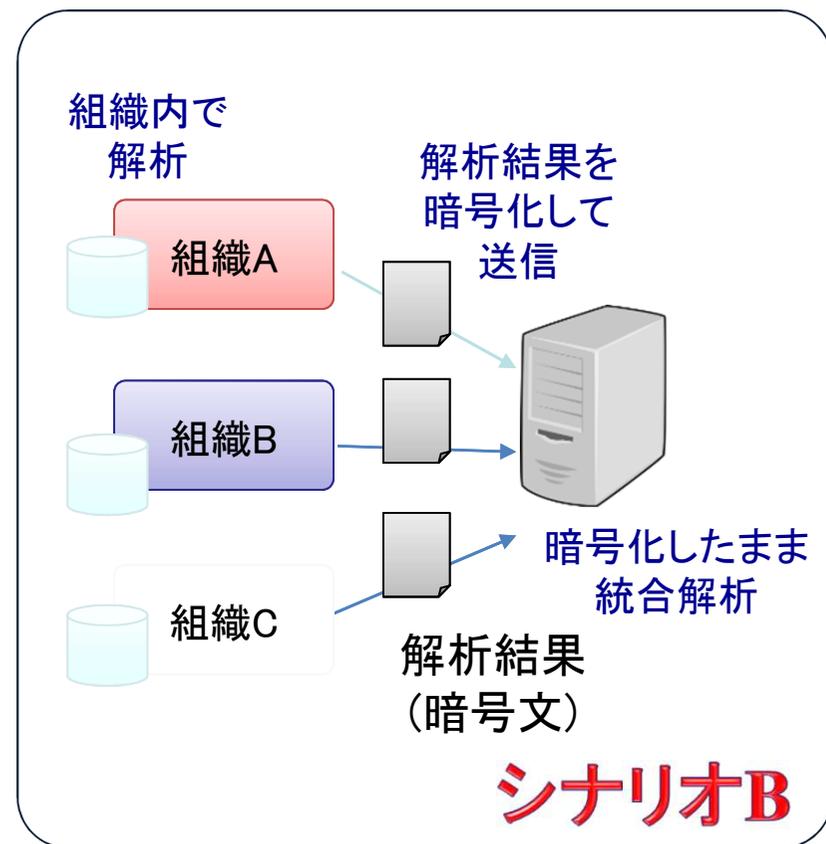
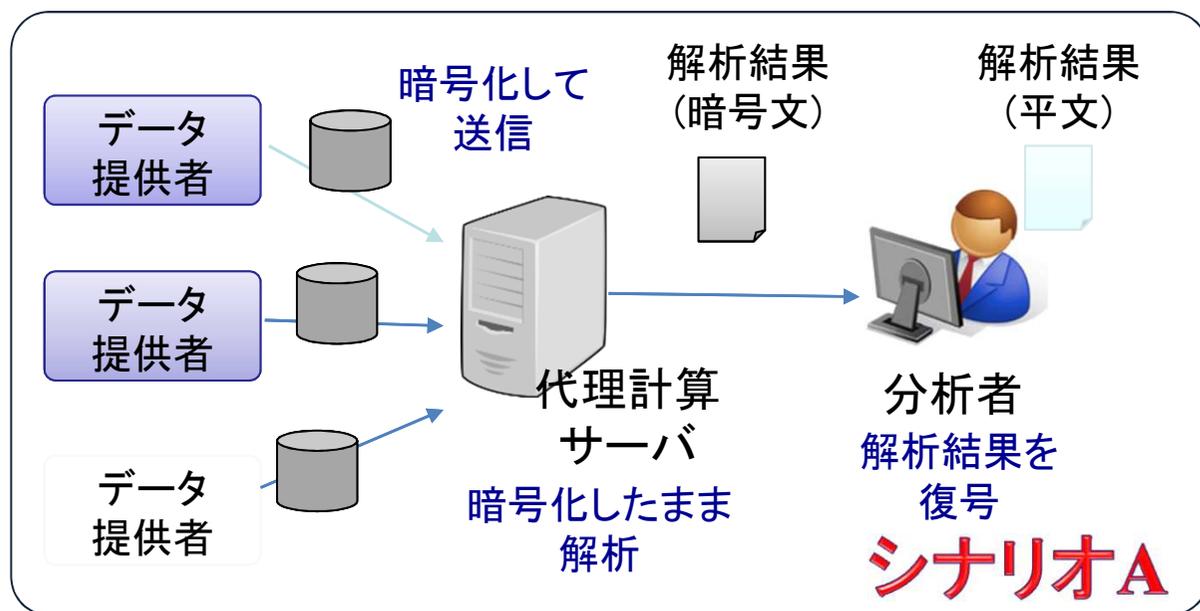
## めざす構想



## 分析結果

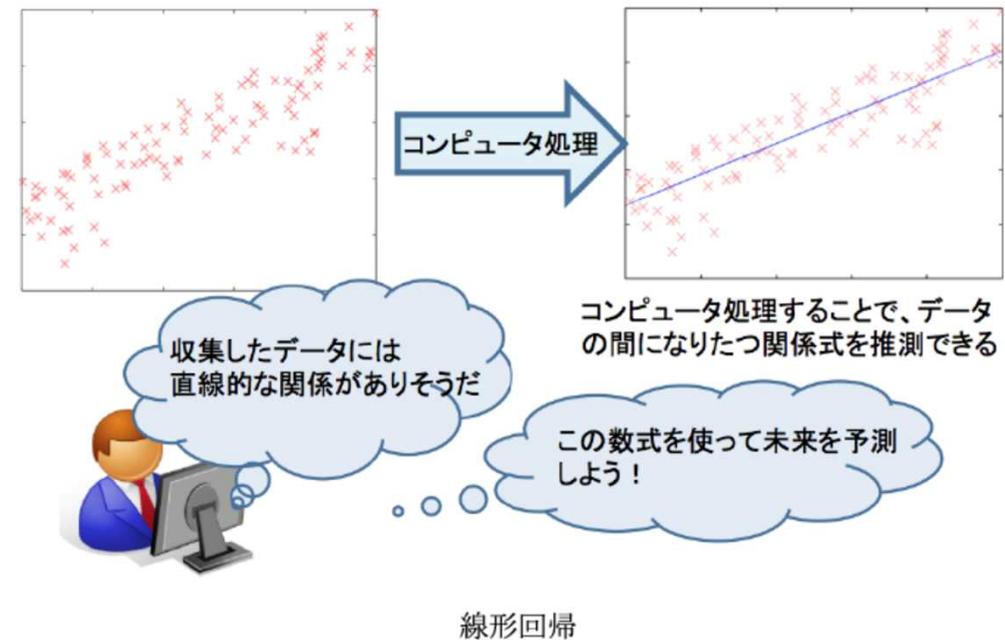
- データを開示せずに、良い分析結果が得られる
- 応用:  
銀行の顧客のデータ、病院の患者のデータなど

# プライバシー保護データ解析 利用シナリオ(二つ)



# 暗号化したままビッグデータ予測

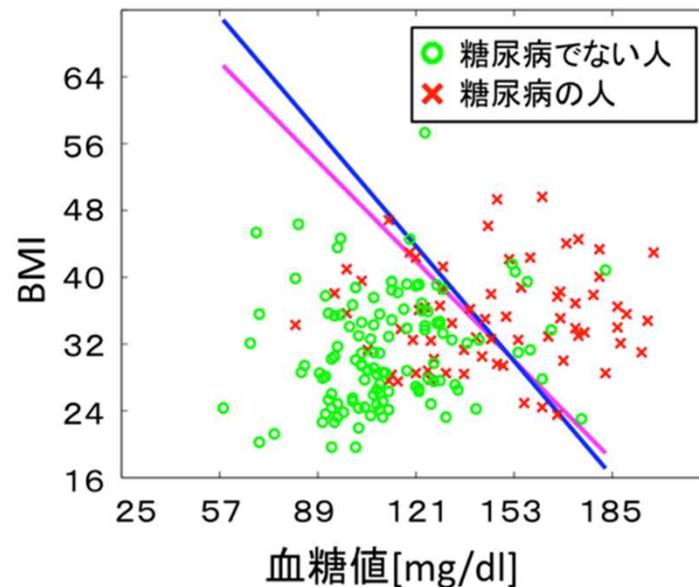
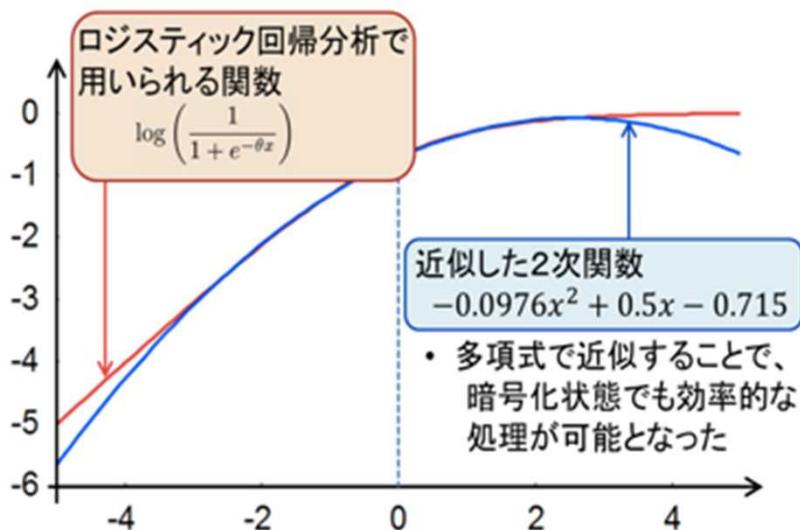
- ビッグデータ解析で多用されている**線形回帰分析**をデータを暗号化したまま計算可能に
- 100万件のデータに対する線形回帰計算を暗号化したまま行い、30分程度で処理ができることをシミュレーションで確認
- NICTプレスリリース(2015.1.19) : 「暗号化状態でセキュリティレベルの更新と演算の両方ができる準同型暗号方式を開発」



# シナリオA

## 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)



— 暗号化しないデータを用いた分析結果(オリジナルの回帰)  
 — 暗号化したデータを用いた分析結果(近似による回帰)

# シナリオB

# プライバシー保護

# ディープラーニング (予測・分類)

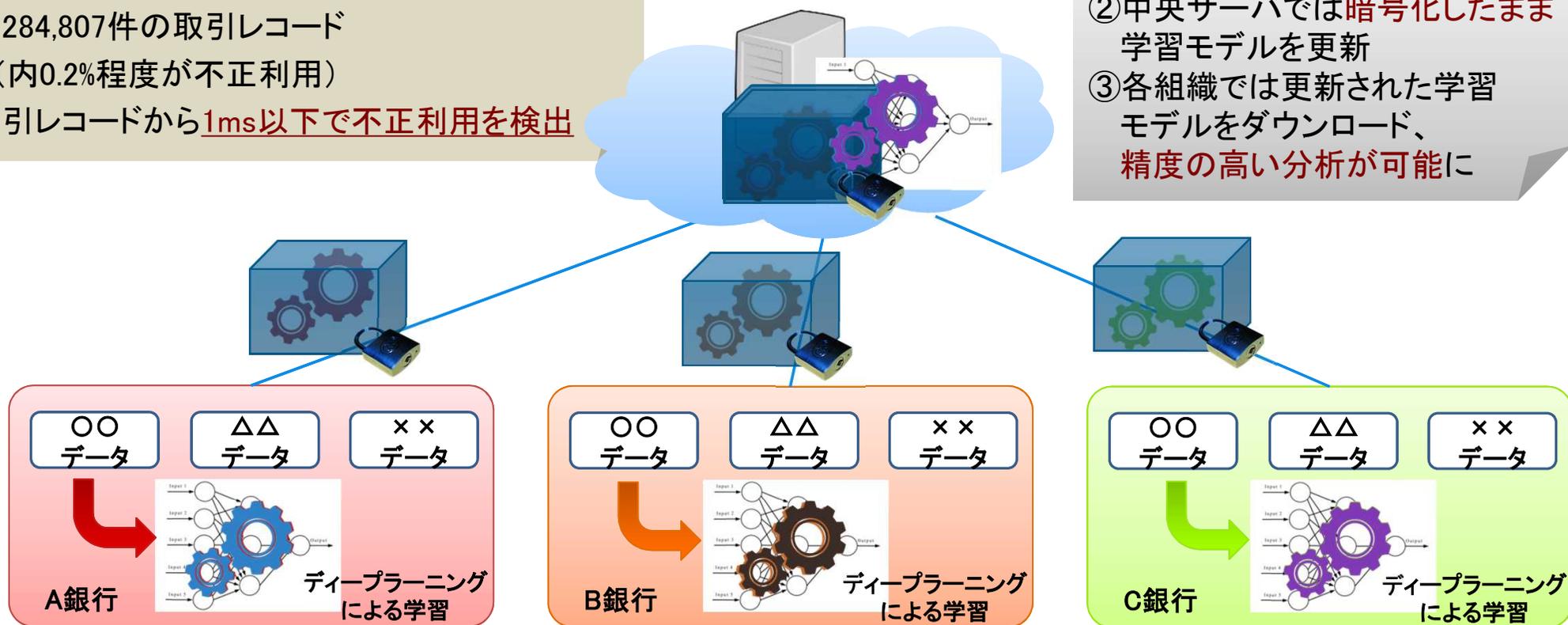
- 組織が持つデータを外部に開示することなく深層学習を行う  
プライバシー保護深層学習システム

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

# オープンデータを用いたプロトタイプの検証

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

複数組織からのデータ提供をシミュレーションするため、

公開データを計21個のグループに分割

- 学習用20セット+テスト用1セット

	不正利用	正当な利用
学習用データセット1,...,20	13 ~ 27	≈ 11379
テストセット	98	56863

# プロトタイプ

データ所有者  
(計20組織)

Fraud Detector Collaborative Machine Training		
Round 1		
F-score 0.00000		
Accuracy 0.99828		
Data Owner 1	SERVER	Data Owner 11
TP=0, FN=98, FP=0, TN=56863	M4_NK5	TP=0, FN=98, FP=0, TN=56863
xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	4_NK5k	xxxxxxxxxxxxxxxxxxxxxxxx 0.0%
	_NK5kh	
Data Owner 2	NK5khR	Data Owner 12
TP=0, FN=98, FP=0, TN=56863	K5khRi	TP=0, FN=98, FP=0, TN=56863
xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	5khRi_	xxxxxxxxxxxxxxxxxxxxxxxx 0.0%
	khRi_l	
Data Owner 3	hRi_lI	Data Owner 13
TP=0, FN=98, FP=0, TN=56863	Ri_lIq	TP=0, FN=98, FP=0, TN=56863
xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	i_lIqJ	xxxxxxxxxxxxxxxxxxxxxxxx 0.0%
	_lIqJr	
Data Owner 4	lIqJrZ	Data Owner 14
TP=0, FN=98, FP=0, TN=56863	IqJrZ6	TP=0, FN=98, FP=0, TN=56863
xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	qJrZ6f	xxxxxxxxxxxxxxxxxxxxxxxx 0.0%
	JrZ6fv	
Data Owner 5	rZ6fvN	Data Owner 15
TP=0, FN=98, FP=0, TN=56863	Z6fvNv	TP=0, FN=98, FP=0, TN=56863
xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	6fvNvR	xxxxxxxxxxxxxxxxxxxxxxxx 0.0%
	fvNvRy	
Data Owner 6	vNvRyy	Data Owner 16
TP=0, FN=98, FP=0, TN=56863	NvRyyg	TP=0, FN=98, FP=0, TN=56863
xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	vRyygn	xxxxxxxxxxxxxxxxxxxxxxxx 0.0%
	RyygnF	
Data Owner 7	yygnFV	Data Owner 17
TP=0, FN=98, FP=0, TN=56863	ygnFVq	TP=0, FN=98, FP=0, TN=56863
xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	gnFVq3	xxxxxxxxxxxxxxxxxxxxxxxx 0.0%
	nFVq3K	
Data Owner 8	FVq3K8	Data Owner 18
TP=0, FN=98, FP=0, TN=56863	Vq3K8m	TP=0, FN=98, FP=0, TN=56863
xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	q3K8m8	xxxxxxxxxxxxxxxxxxxxxxxx 0.0%
	3K8m8X	
Data Owner 9	K8m8X1	Data Owner 19
TP=0, FN=98, FP=0, TN=56863	8m8X1M	TP=0, FN=98, FP=0, TN=56863
xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	m8X1MH	xxxxxxxxxxxxxxxxxxxxxxxx 0.0%
	8X1MH_x	
Data Owner 10	X1MH_xf	Data Owner 20
TP=0, FN=98, FP=0, TN=56863	1MH_xfc	TP=0, FN=98, FP=0, TN=56863
xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	MH_xfcP	xxxxxxxxxxxxxxxxxxxxxxxx 0.0%

← ラウンド1

← 中央サーバ

データ所有者  
(計20組織)

学習ラウンド1終了時には、テストセット内の98件の不正利用が**検出できていない**

# プロトタイプ

データ所有者  
(計20組織)

Fraud Detector Collaborative Machine Training

Round 3

SERVER		
Data Owner 1 TP=0, FN=98, FP=0, TN=56863 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	UhDeg0 hDeg0R Deg0Rk eg0Rka g0RkaV 0RkaVW RkaVW2 kaVW2I aVW2Iy VW2Iyb V2Iyb1 2Iyb10 Iyb10A yb10Ak b10AkB 10AkBA 0AkBAh AkBAhj kBAhjb BAhjbz Ahjbza hjbza- jbza-3 bza-38 za-382 a-382j -382j9 382j9d 82j9dA 2j9dAI j9dAID 9dAIDo dAIDoH AIDoH1 IDoH1B DoH1BC oH1BCC H1BCCc 1BCCcQ	Data Owner 11 TP=75, FN=23, FP=10, TN=56853 xxxxxxxxxxxxxxxxoooo 51.0%
Data Owner 2 TP=0, FN=98, FP=0, TN=56863 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	Data Owner 12 TP=77, FN=21, FP=10, TN=56853 xxxxxxxxxxxxxxxxoooo 66.7%	
Data Owner 3 TP=0, FN=98, FP=0, TN=56863 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	Data Owner 13 TP=73, FN=25, FP=10, TN=56853 xxxxxxxxxxxxxxxxoooo 68.4%	
Data Owner 4 TP=0, FN=98, FP=0, TN=56863 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	Data Owner 14 TP=75, FN=23, FP=10, TN=56853 xxxxxxxxxxxxxxxxoooo 66.7%	
Data Owner 5 TP=0, FN=98, FP=0, TN=56863 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	Data Owner 15 TP=83, FN=15, FP=3, TN=56850 xxxxxxxxxxxxxxxxoooo 66.5%	
Data Owner 6 TP=0, FN=98, FP=0, TN=56863 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	Data Owner 16 TP=81, FN=17, FP=11, TN=56852 xxxxxxxxxxxxxxxxoooo 71.4%	
Data Owner 7 TP=0, FN=98, FP=0, TN=56863 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	Data Owner 17 TP=81, FN=17, FP=12, TN=56851 xxxxxxxxxxxxxxxxoooo 71.4%	
Data Owner 8 TP=0, FN=98, FP=0, TN=56863 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	Data Owner 18 TP=83, FN=15, FP=13, TN=56850 xxxxxxxxxxxxxxxxoooo 70.4%	
Data Owner 9 TP=0, FN=98, FP=0, TN=56863 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	Data Owner 19 TP=83, FN=15, FP=13, TN=56850 xxxxxxxxxxxxxxxxoooo 71.4%	
Data Owner 10 TP=57, FN=41, FP=7, TN=56856 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	Data Owner 20 TP=0, FN=98, FP=0, TN=56863 xxxxxxxxxxxxxxxxxxxxxxxx 0.0%	

ラウンド3

中央サーバ

データ所有者  
(計20組織)

学習が進むにつれて、不正利用の検出率が上がっていく

# プロトタイプ

```
[phong@vt001 credit_card]$ Fraud Detector Collaborative Machine Training
F-score max 0.86154
Accuracy max 0.99953

Round 6
SERVER
4UuD_V Data Owner 11
UuD_VE TP=86, FN=12, FP=19, TN=56844
uD_VEL xxxxxxxx0000000000000000 69.4%
D_VELR
_VELRV Data Owner 12
VELRVW TP=85, FN=13, FP=18, TN=56845
ELRVW5 xxxxxxxx0000000000000000 68.4%
LRVW5K
RVW5Kj Data Owner 13
VW5Kja TP=84, FN=14, FP=17, TN=56846
W5Kjaq xxxxxxxx0000000000000000 68.4%
5KjaqV
KjaqVQ Data Owner 14
jaqVQA TP=84, FN=14, FP=17, TN=56846
aqVQA1 xxxxxxxx0000000000000000 68.4%
qVQA1S
VQA1SB Data Owner 15
QA1SBh TP=85, FN=13, FP=18, TN=56845
A1SBhe xxxxxxxx0000000000000000 68.4%
1SBheZ
SBheZt Data Owner 16
BheZtI TP=84, FN=14, FP=17, TN=56846
heZtIq xxxxxxxx0000000000000000 68.4%
eZtIqI
ZtIqIy Data Owner 17
tIqIyU TP=83, FN=15, FP=15, TN=56848
IqIyU2 xxxxxxxx0000000000000000 68.4%
qIyU2g
IyU2gg Data Owner 18
yU2ggE TP=84, FN=14, FP=17, TN=56846
U2ggEa xxxxxxxx0000000000000000 69.4%
2ggEap
ggEapP Data Owner 19
gEapPC TP=85, FN=13, FP=18, TN=56845
EapPC2 xxxxxxxx0000000000000000 68.4%
apPC2C
pPC2C_ Data Owner 20
PC2C_h TP=85, FN=13, FP=18, TN=56845
C2C_hj xxxxxxxx0000000000000000 68.4%
```

← ラウンド6

← 中央サーバ

データ所有者  
(計20組織)

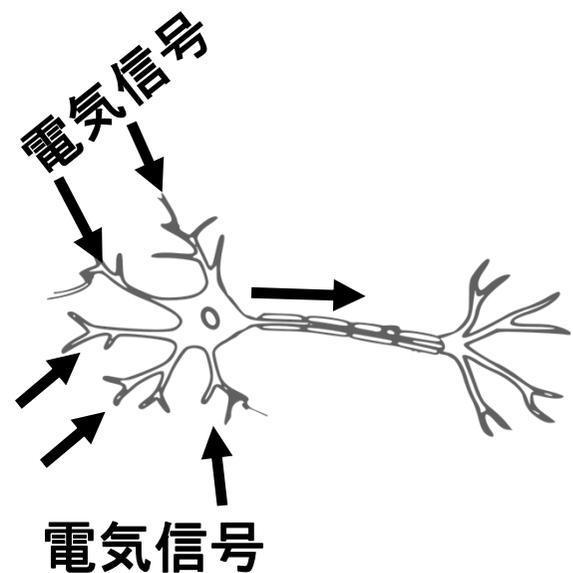
データ所有者  
(計20組織)

学習アルゴリズムの収束後、98件中85件の不正利用が検出可能になっている

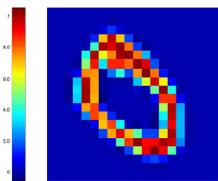


# 提案システムのため 準備1/2:ニューラルネットワーク

生物の神経細胞  
(ニューロン)

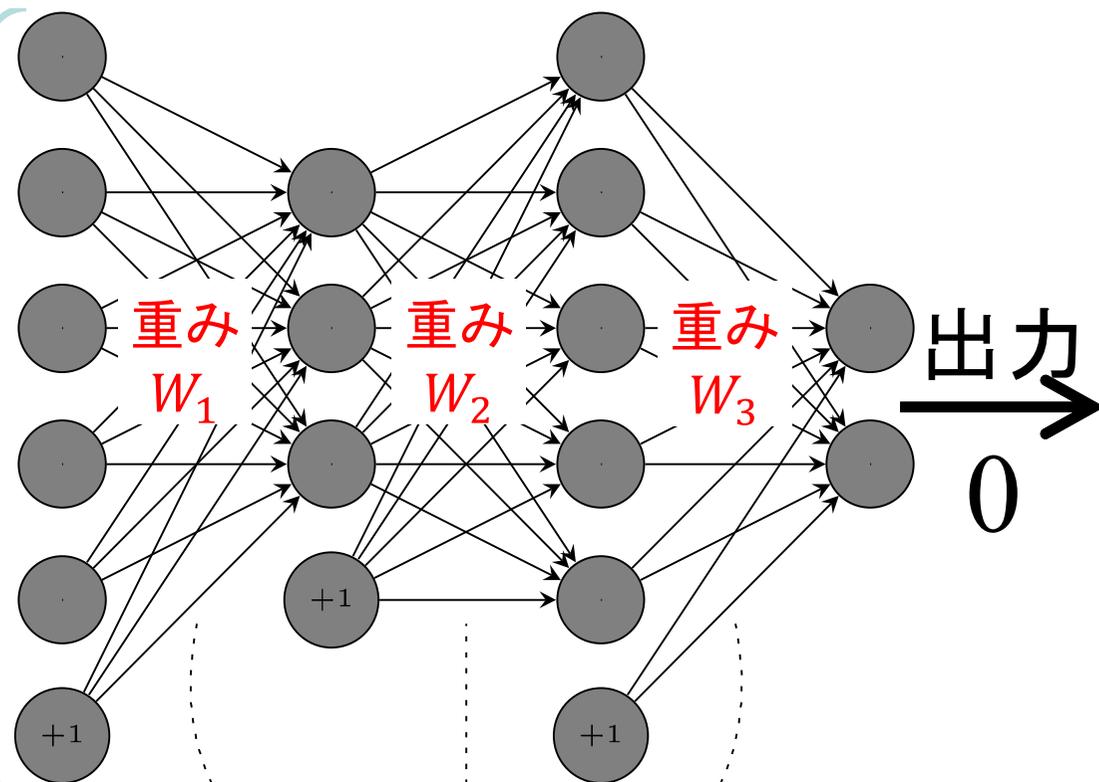


入力



数字の0の画像

人工知能(AI)  
のニューラルネットワーク

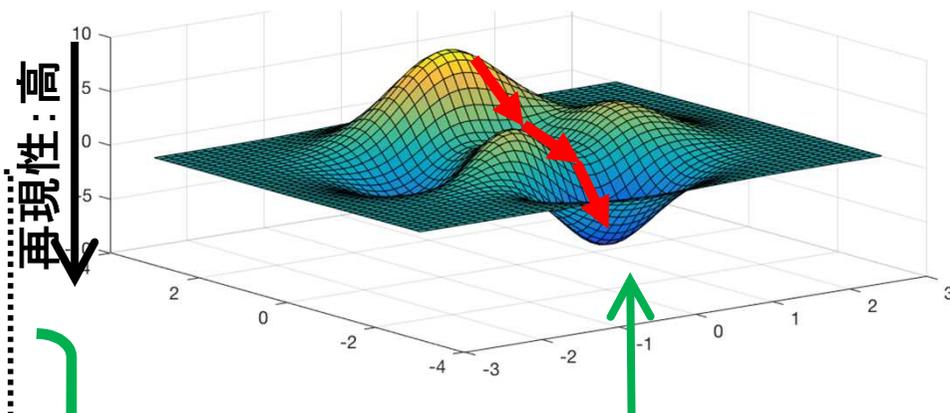


ニューラルネットの学習: 大量のデータ(=入出力のペア)に対して、できる限りそれを再現するように**重みベクトル $W$** を調整

# 提案システムのため 準備2/2: 確率的勾配降下法(SGD)

関数  $J(W, data)$ : 現在の重み  $W$  を用いたニューラルネットによるデータ再現性の指標

関数  $J(W, data)$



関数の勾配  $G$  の方向に進む

重みベクトル  $W$  をランダムに初期する

REPEAT

FOR  $data$  IN Dataset:

$$G \leftarrow \frac{\delta(J(W, data))}{\delta W} \quad (\text{勾配 } G \text{ を計算})$$

$$W \leftarrow W - \alpha \cdot G \quad (\text{重みベクトルの更新})$$

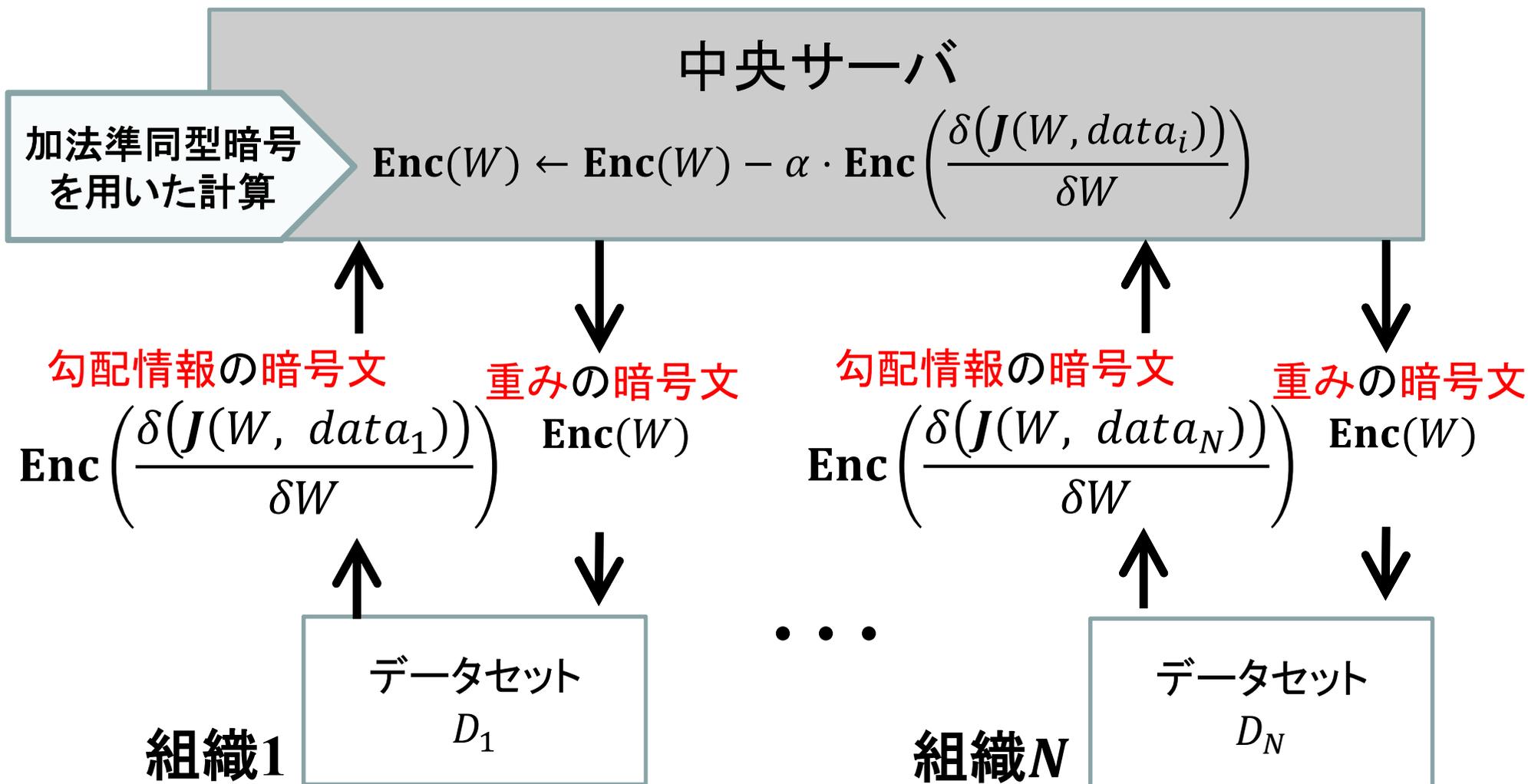
ENDFOR

UNTIL (good accuracy)

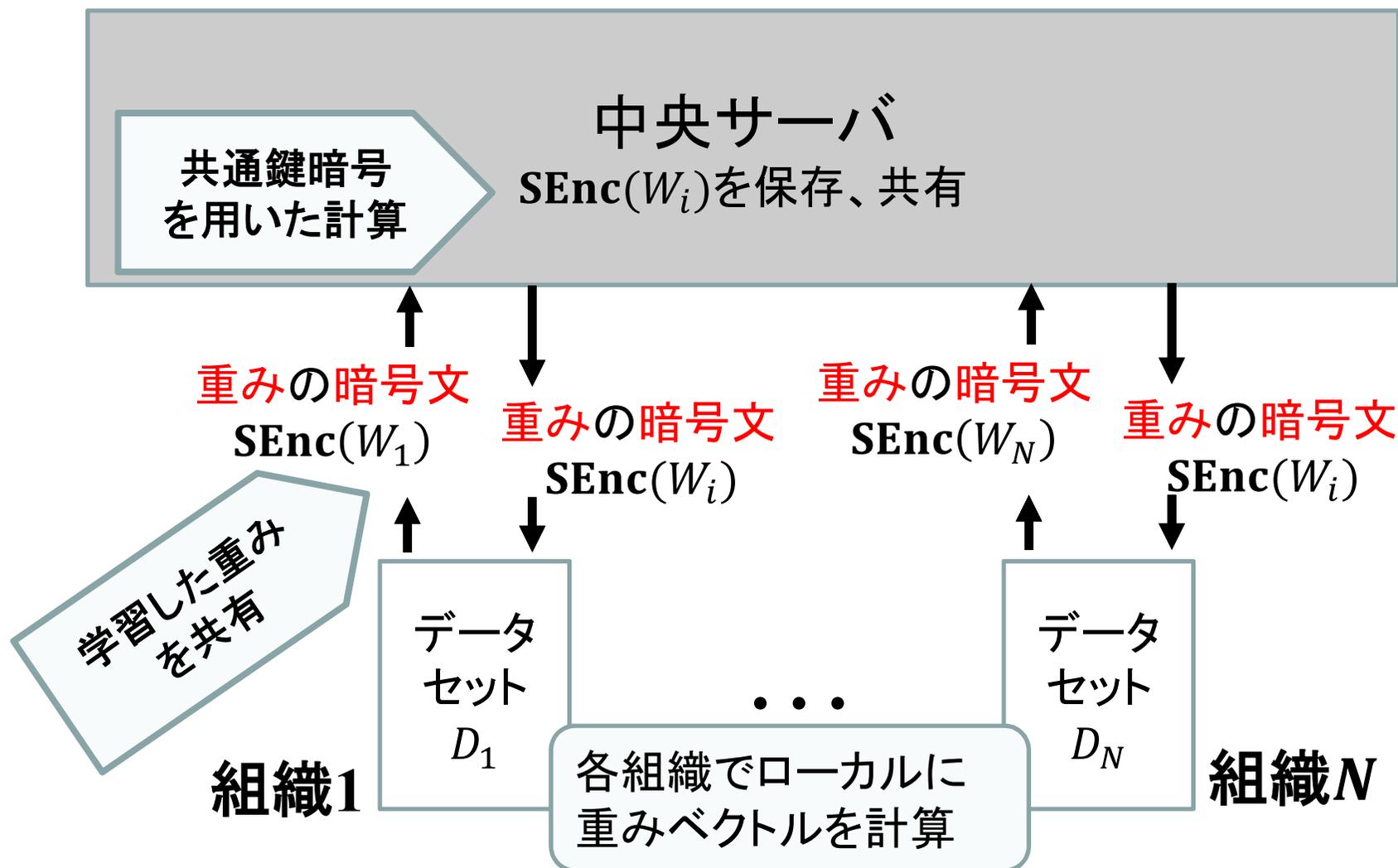
確率的勾配降下法(SGD)

# NICT DeepProtect 1: 加法型準同型暗号を用いたシステム

- 勾配情報を暗号化すれば、データ漏洩は防げる
- 中央サーバにおける計算は加算のみなので、暗号化したまま加算ができれば良い



# NICT DeepProtect 2: 共通鍵暗号をシステム



# 類似技術: Google's Federated Learning (連合した学習)

- <https://www.tensorflow.org/federated>
- オープンソース: 2019年3月

## TensorFlow Federated: Machine Learning on Decentralized Data

TensorFlow Federated (TFF) is an open-source framework for machine learning and other computations on decentralized data. TFF has been developed to facilitate open research and experimentation with [Federated Learning \(FL\)](#), an approach to machine learning where a shared global model is trained across many participating clients that keep their training data locally. For example, FL has been used to train [prediction models for mobile keyboards](#) without uploading sensitive typing data to servers.

TFF enables developers to simulate the included federated learning algorithms on their models and data, as well as to experiment with novel algorithms. The building blocks provided by TFF can also be used to implement non-learning computations, such as aggregated analytics over decentralized data. TFF's interfaces are organized in two layers:



### Federated Learning (FL) API

This layer offers a set of high-level interfaces that allow developers to apply the included implementations of federated training and evaluation to their existing TensorFlow models.

```
from six.moves import range
import tensorflow as tf
import tensorflow_federated as tff
from tensorflow_federated.python.examples import mnist
tf.compat.v1.enable_v2_behavior()

# Load simulation data.
source, _ = tff.simulation.datasets.emnist.load_data()
def client_data(n):
    dataset = source.create_tf_dataset_for_client(source.client_ids[n])
    return mnist.keras_dataset_from_emnist(dataset).repeat(10)

# Pick a subset of client devices to participate in training.
train_data = [client_data(n) for n in range(3)]

# Grab a single batch of data so that TFF knows what data to load.
Google Chrome | h = tf.contrib.framework.nest.map_structure(
```

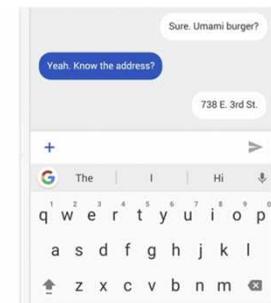
# Google's Federated Learningの製品化

*“We’re already using Federated Learning to improve several Google products. The Pixel first and second generation phones, for example, use Federated Learning to surface more accurate, useful settings search results so that people can find what that they’re looking for faster. The Pixel has thousands of settings to adjust, from font size and brightness to app preferences and battery use. Different settings apply to different people and use cases, so personalizing users’ experiences with machine learning can help people more easily find the one that they care about.”*

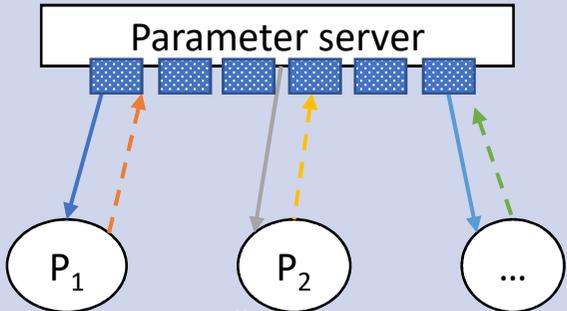
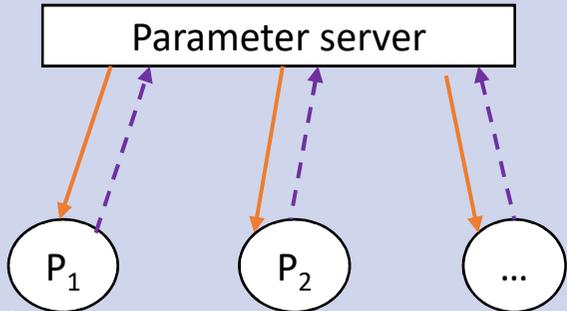
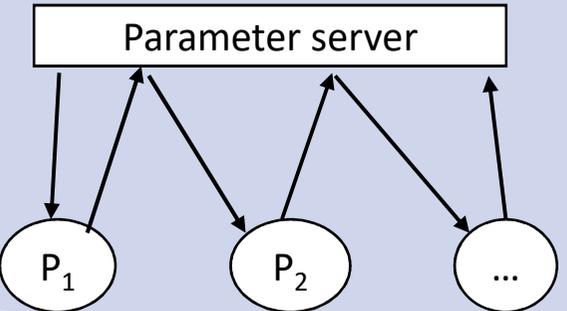
<https://ai.google/stories/ai-in-hardware/>



Google Pixel 3  
2018/11から  
日本で  
販売されている



# 通信の比較

	Shokri & Smartikov ACM CCS 2015 NICT DeepProtect 1	Googleの Federated Learning	NICT DeepProtect 2
通信の仕方	 <p>非同期、或いは、同期            ↑: 勾配の和            ↓: ニューラルネットワークの重み</p>	 <p>同期のみ            ↑: ニューラルネットワークの重み            ↓: ニューラルネットワークの重み</p>	 <p>同期のみ            ↑: ニューラルネットワークの重み            ↓: ニューラルネットワークの重み</p>
応用	学習参加者 $P_i$ は、 (銀行や病院のような) 組織	学習参加者 $P_i$ は、 スマートフォン	学習参加者 $P_i$ は、 (銀行や病院のような) 組織

- R. Shokri, V. Shmatikov: *Privacy-Preserving Deep Learning*.  
ACM Conference on Computer and Communications Security 2015: 1310-1321
- B. McMahan et al.: *Communication-Efficient Learning of Deep Networks from Decentralized Data*.  
AISTATS 2017: 1273-1282
- **(DeepProtect1)** L. T. Phong et al. :*Privacy-Preserving Deep Learning via Additively Homomorphic Encryption*.  
IEEE Trans. Information Forensics and Security 13(5): 1333-1345 (2018)
- **(DeepProtect2)** L.T. Phong, T.T. Phuong: *Privacy-Preserving Deep Learning via Weight Transmission*,  
IEEE Trans. IFS, 2019, accepted

# 安全性と学習精度の比較

技術	中央サーバに対する安全性	中央サーバ+不正の学習参加者に対する安全性	学習精度	暗号技術
Shokri and Shmatikov (ACM CCS 2015)	Onewayness under subset sum*	Onewayness under subset sum*	非同期 SGD	TLS/SSL
NICTの DeepProtect 1	<b>Semantic security under encryption</b>	Onewayness under subset sum*	非同期 SGD	TLS/SSL + 準同型暗号
Googleの 連合学習	Onewayness under subset sum	Onewayness under subset sum*	同期 SGD	TLS/SSL
NICTの DeepProtect 2	<b>Semantic security under encryption</b>	Onewayness under subset sum*	同期 SGD	TLS/SSL + 共通鍵暗号

\*More generally, solving a system of non-linear equations where #unknowns > #equations

# 他データセット(医療や個人データ) を用いた実験(1/2)

UCI Dataset Name	Known accuracy (in [6], data privacy is preserved)	Known F-score	Percentage of label 0 (or label 1 if higher)	Our system accuracy (data privacy is preserved)	Our system F-score
Pima (diabetes)	80.70%	0.688525	64.29%	<b>85.06%</b>	<b>0.763636</b>
Breast Cancer	98.20%	0.962406	64.04%	<b>99.31%</b>	<b>0.989304</b>
Banknote Authentication	98.40%	0.984615	55.97%	<b>100.0%</b>	<b>1.0</b>
Adult Income	81.97%	0.526921	76.38%	<b>85.90%</b>	<b>0.664362</b>
Skin/NonSkin	93.89%	0.960130	79.53%	<b>99.95%</b>	<b>0.998655</b>

プライバシー保護  
ロジスティクス回帰

(Aono et al., IEICE Trans. 2016)

プライバシー保護  
ディープラーニング

(DeepProtect 2)

UCIデータセット

<https://archive.ics.uci.edu/ml/index.php>

# 他データセット(医療や個人データ)を用いた実験(2/2)

プライバシー保護なし  
のアルゴリズム

UCI Dataset Name	Algorithm	Error
Pima (diabetes)	1 C4.5	15.54
Breast Cancer	2 C4.5-auto	14.46
Banknote Authentication	3 C4.5 rules	14.94
Adult Income	4 Voted ID3 (0.6)	15.64
Skin/NonSkin	5 Voted ID3 (0.8)	16.47
	6 T2	16.84
	7 1R	19.54
	8 NBTree	14.10
	9 CN2	16.00
	10 H00DG	14.82
	11 FSS Naive Bayes	14.05
	12 IDTM (Decision table)	14.46
	13 Naive-Bayes	16.12
	14 Nearest-neighbor (1)	21.42
	15 Nearest-neighbor (3)	20.35
	16 OC1	
	17 Pebls	

(Aon)

Error	Our system accuracy (data privacy is preserved)	Our system F-score
	85.06%	0.763636
	99.31%	0.989304
	100.0%	1.0
	85.90%	0.664362
	99.95%	0.998655

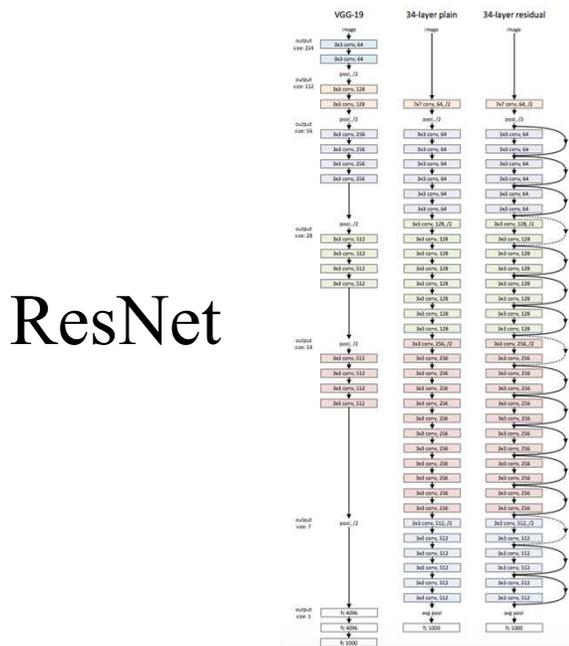
プライバシー保護  
ディープラーニング  
(DeepProtect 2)

プライバシー保護しながらも、Adult Incomeデータセットにおいて、従来技術(プライバシー保護なし)の精度と比べても、**ほぼ同等以上**ある。

UCIデータセット

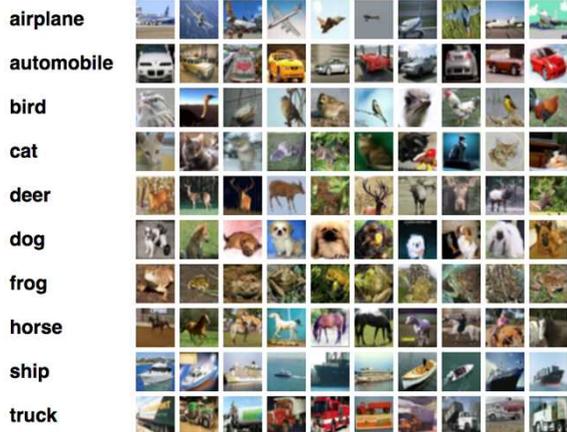
<https://archive.ics.uci.edu/ml/>

# 画像を用いた実験: ResNet + CIFAR (10/100)



ResNet

CIFARデータセット



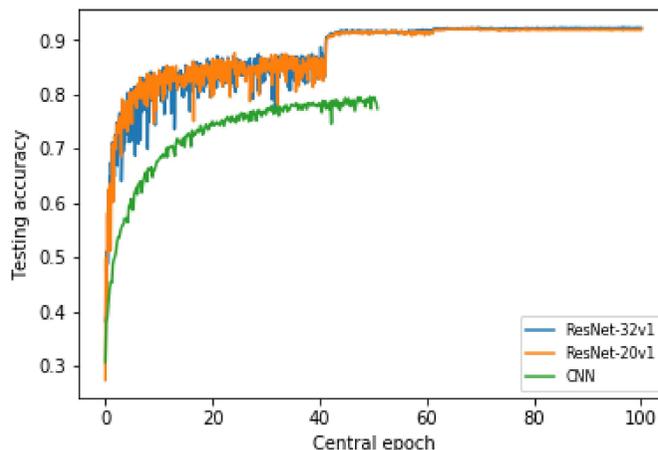
**DeepProtect2:**  
暗号なしの学習時間は、暗号ありの学習時間  
とほぼ変わらない



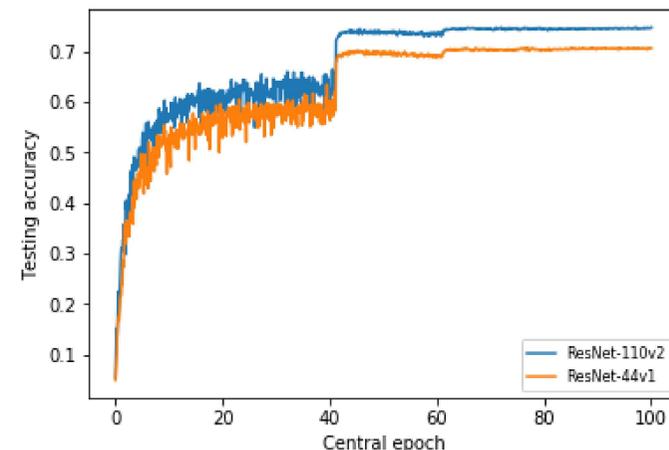
Network model, Dataset	$T_{\text{original}}^{(i)}$	$T_{\text{uploadCtxt}}^{(i)}$	$T_{\text{downloadCtxt}}^{(i)}$	$T_{\text{enc}}^{(i)}$	$T_{\text{dec}}^{(i)}$
CNN, CIFAR-10	37 (sec.)	0.056 (sec.)	0.056 (sec.)	0.130 (sec.)	0.06 (sec.)
ResNet-20v1, CIFAR-10	59 (sec.)	0.013 (sec.)	0.013 (sec.)	0.064 (sec.)	0.06 (sec.)
ResNet-32v1, CIFAR-10	87 (sec.)	0.023 (sec.)	0.023 (sec.)	0.066 (sec.)	0.06 (sec.)
ResNet-44v1, CIFAR-100	122 (sec.)	0.032 (sec.)	0.032 (sec.)	0.091 (sec.)	0.085 (sec.)
ResNet-110v2, CIFAR-100	322 (sec.)	0.165 (sec.)	0.165 (sec.)	0.179 (sec.)	0.138 (sec.)

□ In the table, the time for training over plain local data  $T_{\text{original}}^{(i)}$  dominates the others.

(a) Experiments with CIFAR-10



(b) Experiments with CIFAR-100



## 想定される用途

- 金融分野において不正送金（振り込め詐欺等）の自動検知の精度向上に期待。
- 医療分野においても、プライバシーを保護したまま解析の精度を向上することが可能。
- プライバシー保護の目的外でも、データが分散するシナリオにおいて学習の通信量を削減する効果も可能。

## 実用化に向けた課題

現在、一つマシンでのシミュレーションやオープンデータの実験は開発済み。しかし、

- a) 複数台のマシンの(効率かつ安定の)通信
- b) 複数組織のコラボレーション(契約)

の2点は、未解決である。

## 企業への期待

- 未解決のa)については、GPUを持つマシンとマシンの通信技術により、克服できると考えている。
- 未解決のb)については、データを持つ企業や組織の協力により、克服できると考えている。
- 上記に関して、企業との共同開発を希望。
- また、深層学習を開発中の企業、組織横断の学習への展開を考えている企業には、本技術の導入が有効と思われる。

## 本技術に関する知的財産権(1)

- 発明の名称 : サーバ、サービス方法
- 特許番号 : 6490429
- 出願人 : 国立研究開発法人  
情報通信研究機構
- 発明者 : レチュウ フォン、  
青野 良範、  
林 卓也、  
王 立華

## 本技術に関する知的財産権(2)

- 発明の名称 : 学習システム及び学習方法
- 出願番号 : 特願2018-001656
- 出願人 : 国立研究開発法人  
情報通信研究機構
- 発明者 : レ チュウ フォン

# お問い合わせ先

国立研究開発法人情報通信研究機構  
イノベーション推進部門  
技術移転コーディネータ 宇梶、橘田

TEL 042-327-6950

FAX 042-327-6659

e-mail [ippo@ml.nict.go.jp](mailto:ippo@ml.nict.go.jp)