



IOWNオールフォトニクスネットワーク （APN）による低遅延通信を活かした秘密計算 でのAI分析環境の実用性を実証（2024.6）

NTT社会情報研究所

本資料は、下記報道発表の技術的な補足解説です。

「IOWN オールフォトニクスネットワーク（APN）による低遅延通信を活かした秘密計算でのAI分析環境の実用性を実証～秘密計算サーバの複数拠点への配置が可能に～」 2024年6月12日
<https://group.ntt.jp/newsrelease/2024/06/12/240612b.html>

ポイント

1. 秘密分散を利用した秘密計算では、大量に発生する通信の影響を最小化するため、**すべてのサーバを一つのデータセンターに配置することが一般的であった**
2. **低遅延であるAPNで相互接続されたDCを活用することにより、複数のデータセンターに分散配置された計算処理環境においても、秘密計算によるAI分析を実用的な時間で可能であることを確認した。**（一般的ネットワーク環境と比べ1/7倍に短縮）
3. 災害対策、エネルギー最適化およびセキュリティの観点から、複数地域に分散したDCを活用し、高精度なAIモデル構築など「安全・安心な複数事業者でのデータ利活用」が期待できる。

→ 次ページ以降で詳しく説明します

背景 ～秘密分散を利用した秘密計算



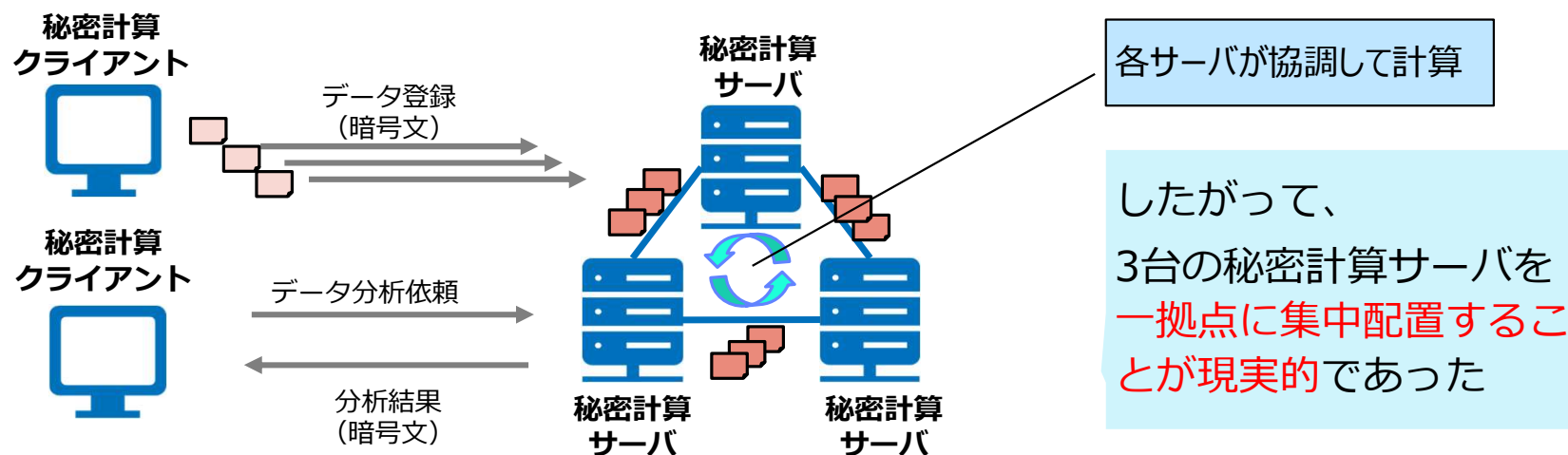
暗号化方法（秘密分散）：

データを3個の暗号文に分割して秘密計算サーバ3台へ保存

計算の特徴：

秘密計算サーバ（3台）は、（暗号化された）小さなデータ破片を頻繁に受け渡ししながら**各サーバが協調**して目的の計算を行う

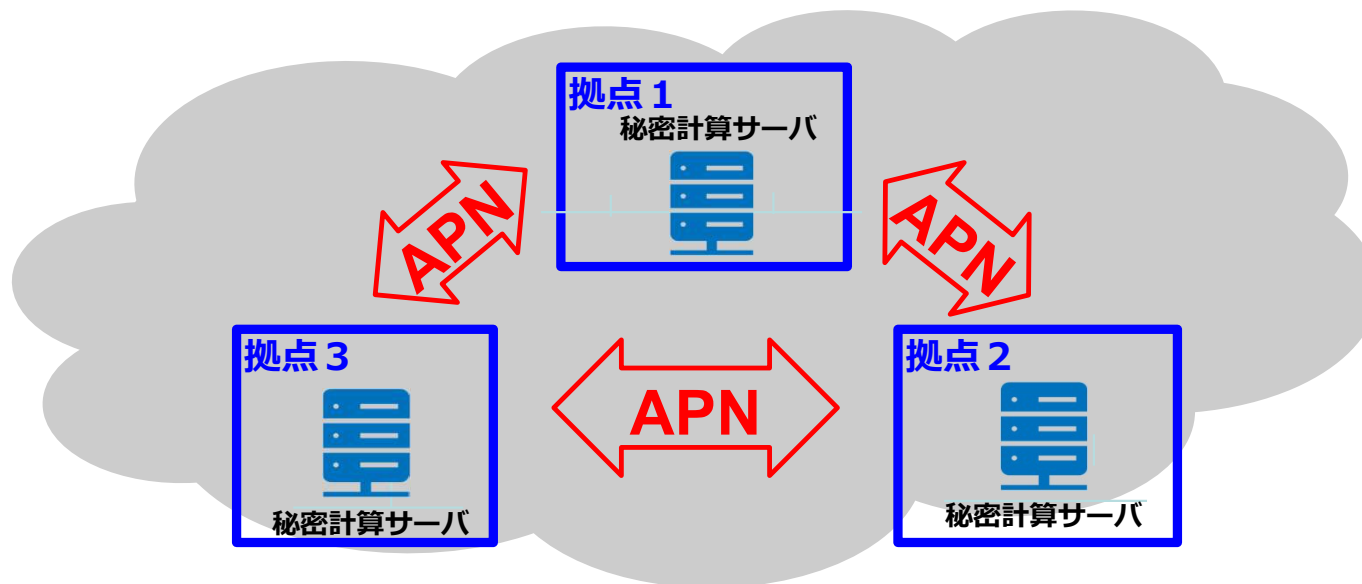
⇒ 計算過程で**サーバ間の通信が頻繁に発生**、その通信遅延が計算性能に影響



提案 ～IOWN APNを活用した秘密計算の構成



- 広帯域・低遅延のIOWN APNで接続された3拠点それぞれに秘密計算サーバを配置する
 - 【参考】IOWN APN(All-Photonics Network)とは、IOWN構想を実現するために用いられるNTT の新しい光通信ネットワーク環境であり、広帯域・低遅延を実現する https://journal.ntt.co.jp/wp-content/uploads/2023/07/nttjnl5001_20230701.pdf
- IOWN APN接続により、**通信遅延の影響を低く**抑えることができる
- **あたかも 1 拠点内に配置されている**ように見做すことができる

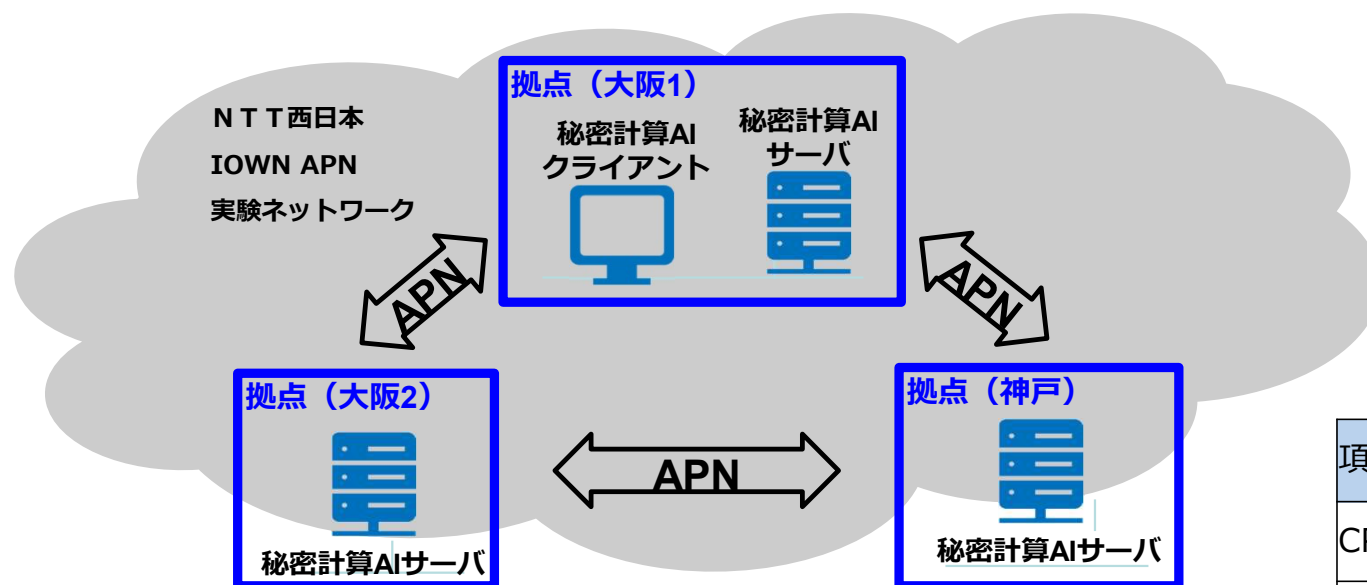


3台の秘密計算サーバの
遠隔分散配置が現実的
になる

実証 ～実験構成



- 大阪1、大阪2、神戸の3拠点に秘密計算AI※サーバを構築
- 秘密計算AIサーバ間をIOWN APNで接続



秘密計算AIサーバのハードウェア仕様

項目	仕様
CPU	Intel® Xeon Bronze 3204 CPU@1.90GHz, 6コア
メモリ	64GB
ディスク	446GB以上
OS	Rocky Linux 9.3

※秘密計算AIとは、秘密計算の計算対象を機械学習にも広げたもので、データを暗号化したまま機械学習のモデル学習や学習したモデルに基づく推論を行うことができる

実証 ～実験条件



- **秘密計算AIで動作させる機械学習アルゴリズム：**
 - GBDT（回帰），FFNN（回帰），k-means（多値分類），主成分分析
- **データセット：**
 - GBDT／FFNN： California Housing dataset（学習データ10万件、属性数30）
 - K-means： Forest covertypes（学習データ10万件、属性数30、カテゴリ数10）
 - 主成分分析： California Housing dataset（学習データ10万件、属性数500）
- **測定データ：学習(fit)時間を測定**
- **通信環境：インターネット模擬環境とIOWN APN環境で比較**
 - インターネット模擬環境：サーバのNICにおいてLinux TC コマンドで遅延付加（以降、インターネット環境）
 - IOWN APN環境（以降、APN環境）
- **サーバ・リソース消費の記録：CPU使用率/メモリ消費量/NWトラフィックなど**

実証 ～実験結果



- FFNNでは、インターネット環境とAPN環境とで顕著な差が見られた
 - APN環境はインターネット環境と比べて約1/7倍と大幅に短縮

アルゴリズム	APN環境	インターネット環境(模擬)
GBDT	05分57秒	16分56秒
FFNN	22分06秒	2時間36分56秒(約157分)
k-means	04分10秒	05分32秒
主成分分析	05秒	18秒

実用的な時間でモデルの探索が可能に

AIモデル作成では、パラメータ調整で何度も試行錯誤が必要。APN環境では、一営業日内に数度、モデル作成可能。

【補足】 サーバ・リソース消費状況から、**秘密計算の実行時間はネットワーク遅延が支配的**

- なぜならば、CPU使用率は25%で推移、メモリは64GB搭載のうち最大8GB消費、NWトラフィックは1Gb/s未満、いずれも余裕がある状態（FFNN-APN環境の場合）