小口研究室　研究紹介　(2017年度)
(お茶の水女子大学理学部情報科学科)

被災時情報孤立地域間の分散避難所アセスメント共有システムの一検討
（研究担当：　田中　有彩）

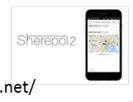
研究背景

近年、日本では多くの自然災害が発生
- → 安全な避難所生活が必要
- → 物資の不足・衛生面などといった問題
- → バックボーンネットワークが使えない
- → 指定されていない避難所の発生の恐れ

各避難所状況を災害対策本部が把握することが重要

既存の取組

- 避難所状況可視化　アプリSheRepo2(株式会社FIXER)
  - −災害発生時の避難所の状況を避難者・救護者・避難所管理者が共有できるアプリケーション
  - − MicrosoftのクラウドサービスであるAzureを使用
  - −主な機能　①避難所からの報告機能
    ②報告の表示機能



株式会社FIXER　https://sherepo2.azurewebsites.net/

問題点 & 提案策

◆ 既存の取組の問題点：クラウドサービスを使用
- ⇨ バックボーンネットワークが必須
- ⇨ 災害時にバックボーンネットワークがない場合、使用できなくなってしまう

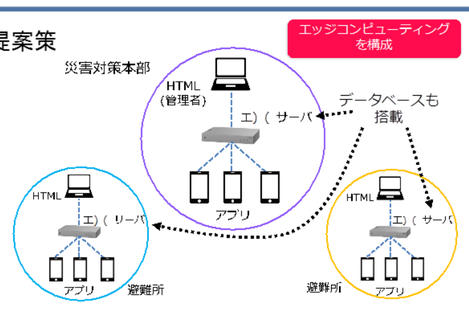
◆ 提案手法
- DTN技術

”劣悪な”通信環境でも、信頼性のあるデータ転送を実現する通信方式
- エッジコンピューティング

端末の近くにサーバを分散配置することで、通信遅延を短縮する技術

◆ 使用するエッジサーバ
- 実システムの構築とシステム解析・連携をサポートする汎用的なプラットフォーム
- ネットワークを自律的に構築
- DTN技術より実システム間での情報同期を可能とする

◆ 提案策



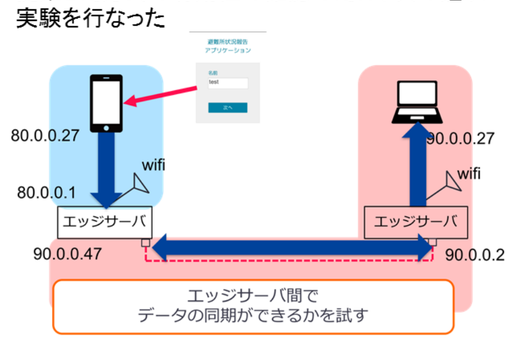
- エッジサーバとしてDBを搭載したWIFI機能付きAPを各避難所に設置
- 各避難所において、APに繋がった各端末がエッジサーバへ災害情報を送信
- エッジサーバのDB間が自動的に同期
  →ローカル環境のサーバとして機能させることでエッジコンピューティングを構成

災害対策本部がすべての各避難所状況を把握することが可能に

システム概要 & 実験

◆ システム概要
- − 入力側(左)：各避難所内にいるユーザが避難所の状況を報告
- − 管理側(右)：各避難所の状況を集計
  地図上で避難所と状況を把握できるようにする

◆ 提案した方式の有用性の確認のため、次の通りに実験を行なった



- 災害時を想定した場合のエッジコンピューティングによる通信実験を行なった
- エッジサーバには先ほど紹介した、DBを搭載したWi-Fi機能付きAPを使用
- AP同士は無線LANにてローカルに繋ぐ
- 1つのAP配下：APから出ている無線LANを通じてローカルに繋げたスマートフォンアプリケーションを設置
- もう1つのAP配下：　片方のAPとパソコンを配置

スマートフォンアプリケーションがAPへ送信したデータを、もう片方のAPにて確認できることを実験

◆実験結果 −実際のシステムにおける確認

エッジサーバ同士の無線LANによるデータ共有を確認

まとめ・今後の課題

◆まとめ　エッジコンピューティング&DTN技術によるシステムの考案・実装
エッジサーバ同士の無線LANによるデータ共有を確認

◆今後の課題　さらなるシステムの改善・実際に利用した場合の不備 / P2P通信への検証

完全準同型暗号を用いた秘匿アソシエーション分析の分散処理による高速化
（研究担当：山本　百合）

研究背景

◆ データマイニング委託システムの必要性

企業が保持する膨大な顧客データから統計処理を行うために大型の計算リソースを所有する機関にデータを委託し，アソシエーション分析結果の問い合わせを行うシステム

◆ 顧客の個人的なデータの保護の必要性

購買履歴などの顧客情報の取り扱いにおいて暗号化によるデータのプライバシー保護が必要となるデータを暗号化した状態で計算を行うシステムを検討

提案手法（Apriori）

◆ 完全準同型暗号の利用

加法と乗法で準同型性が成立する完全準同型暗号を利用し、サーバ・クライアント双方のデータを秘匿

完全準同型暗号は**計算量が大きい**ため、サーバ側の計算時間が長い ⇨ **サーバ側の処理の分散化で高速化を目指す**

◆ Aprioriアルゴリズム

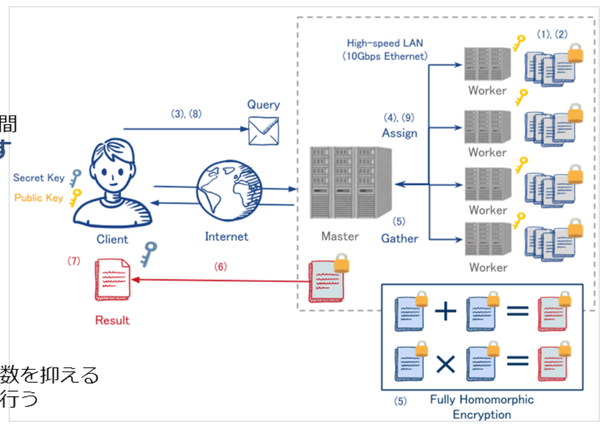
アソシエーション分析のアルゴリズムとして著名なAprioriアルゴリズムを適用する
頻出ではないアイテムセットを内包するアイテムセットは頻出ではないことを前提に計算量を削減

◆ マスタ・ワーカ型分散

マスタとワーカに役割を分担し，クライアントとの通信回数を抑える
今回はサンプルごとのデータ分割による分散処理で実験を行う

◆ プログラム実装方法

C++で実装、マスタとワーカの制御にOpen MPIを使用
完全準同型暗号計算にHElibライブラリを使用



提案手法 (FUP)

◆ データベース更新時の再計算高速化

データベースにトランザクションが追加される場合，Aprioriアルゴリズムではトランザクションの偏り次第で各段階で頻出と判定されるアイテムセットが変化
⇨ データベース更新時にAprioriの再計算が必要

データベース更新前の結果を再利用することにより，頻出度計算の高速化を行うFUPアルゴリズムの適用を考える

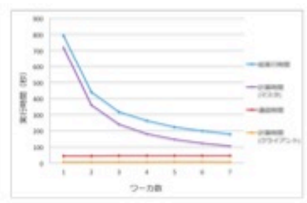
◆ 候補アイテムセットの再計算を削減

FUPアルゴリズムはデータベース更新前の結果を利用し，各アイテムセットの再計算において，データベースの範囲と閾値を分別して設定することによって，再計算を行う候補アイテムセットの削減を目指す
⇨ 最も時間がかかる暗号化されたアイテム同士の演算の削減が期待でき、分散ワーカごとの役割分担も検討可能

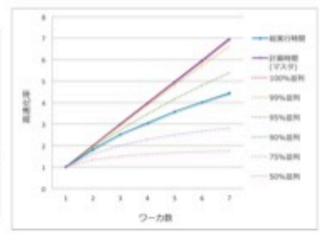
実験と考察

◆ 秘匿Apriori計算の実験
- 分散台数が増えるにつれて計算時間が短縮
- 実行時間は徐々に横ばいになる
- 通信時間とクライアント側の復号計算はワーカ数による変化は小さい

◆ Amdahlの法則による考察
- 高速化率＝逐次実行時間/並列実行時間
- 高速化率 $\leqq \dfrac{1}{(1\text{-並列実行時間の割合}) + \dfrac{\text{並列実行時間の割合}}{\text{ワーカ数}}}$
- ワーカ数が最大の時の高速化率は10倍程度



秘匿Apriori計算の
ワーカ数ごとの平均実行時間



秘匿Apriori計算実験結果と
Amdahlの法則に基づいた
並列実行時間割合別高速化率予測曲線の比較

今後の課題

◆ 分散したマシンごとでの役割分担による高速化
◆ クラウドコンピューティングを想定した環境での実験
◆ FUPアルゴリズムによる実装と深さ優先探索アルゴリズムによる実装の比較

大規模災害時のインターネット非接続時におけるXMPPに基づく情報共有システムの検討
（研究担当：Yu Hui）

研究背景

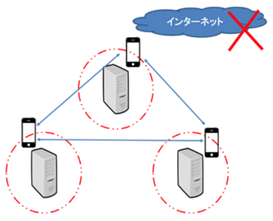
◆ 地震，津波等の自然災害により、インタネットに強く依存しているLINE などの情報を得る手段は利用不能になる

◆ 災害時においては、支援に関する情報配信や連絡手段が必要である

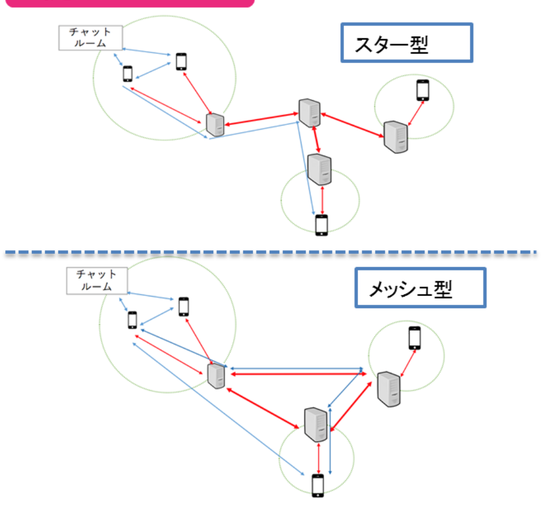
研究目的

◆ 限られたネット環境を活用し、ローカル環境でも使える配信システムを構築

◆ 通信インフラの立ち直るに連れ、配信システム間の情報交換ができるようにする



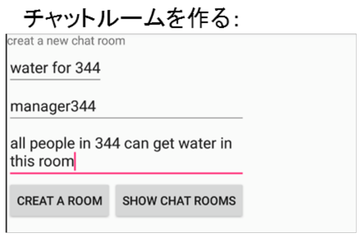
提案システム



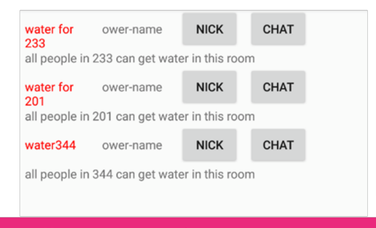
1. 配信のため、チャットルームの機能を利用し、受け取られる情報の説明が付き、リストアップ
2. 通信インフラの立ち直るに連れ、システム間の情報交換のため、サーバ間での接続方法を提案
   - ◆ 簡単にサーバを増やすし、ローカルに置くサーバの負荷を減らすため、スター型での接続方法を提案
   - ◆ 不安定の通信環境に適すため、メッシュ型での接続方法を提案
   - ◆ サーバ間でフェデレーションで信頼関係を締結

実験結果（チャットルーム）

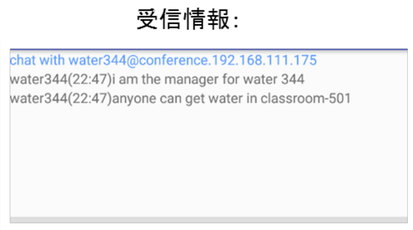
チャットルームを作る：



チャットルームのリスト：



受信情報：



実験結果（ユーザリストの同期やユーザ間の通信）

スター型の同期したユーザリスト：

メッシュ型の同期したユーザリスト：

スター型の通信ログ：

メッシュ型の通信ログ：

今後の課題

- XMPPプロトコルを拡張し，チャットルーム機能を改善
- サーバは4台に増やし、実験を繰り返す

http://ogl.is.ocha.ac.jp/

oguchi@is.ocha.ac.jp