部分復元可能な秘密分散法における秘密分散データを用いた検索

2019年 2月 19日

1190350 中村 巴
情報学群
ネットワーク信号処理研究室

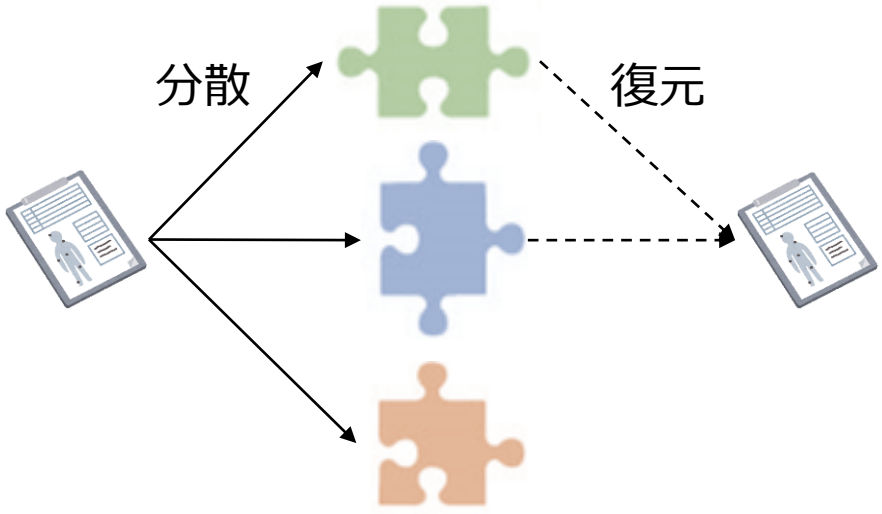
背景

東日本大震災により医療データが紛失し，
被災地での医療行為に支障

- 医療データを遠隔地にバックアップ
- 災害時にバックアップした医療データを活用

(k,n)しきい値秘密分散法

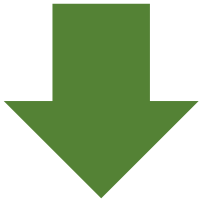
- データをn個のシェアに分散
- シェアをk個以上集めて復元
- 冗長性，秘匿性



(2,3)しきい値

バックアップデータの災害時での活用

急性期は，バックアップデータから医療行為に最低限必要なデータを入手できれば良い



部分復元可能な秘密分散法(田中麻実,2015)

- 分散したデータを部分的に復元するアルゴリズムの提案

バックアップデータを用いた診療

バックアップデータ　医師　患者

部分復元可能な秘密分散システムは
シェアの状態で検索できない

名前など一部の情報を復元

診療時の部分復元可能な秘密分散システムの問題

(k,n)しきい値秘密分散法

- 復元は多項式を解くため，逆行列の作成
- 逆行列の作成には$O(l^3)$の計算量(復元したいデータのサイズをlとする)

復元に時間がかかる

患者を待たせてしまう

部分復元可能な秘密分散バックアップした医療データ検索方法(沼尚樹,2018)
- 検索用の情報を付与

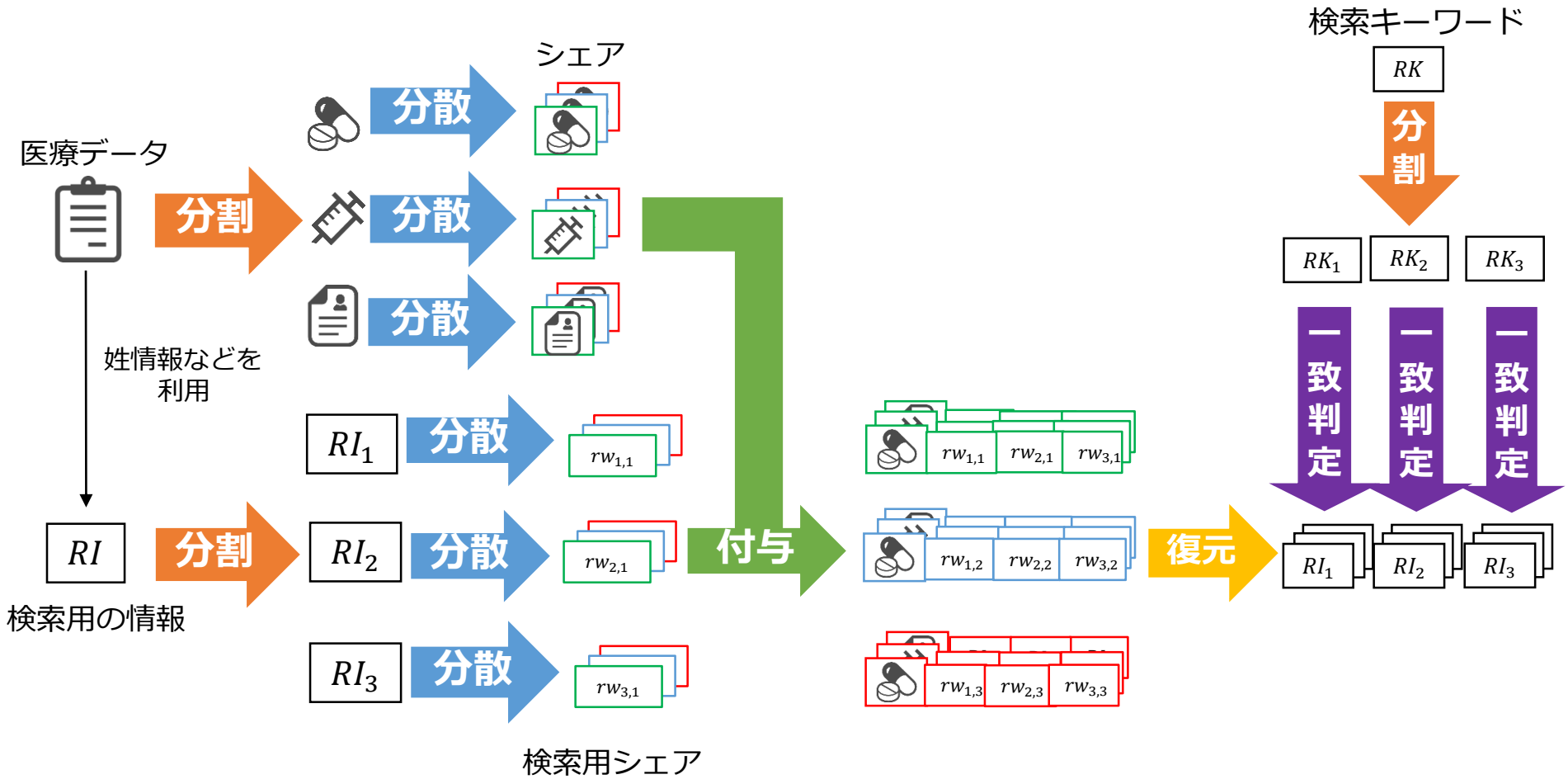
目的

検索用の情報を復元するため時間がかかる

復元不要な検索の実現

シェア同士の一致の判定を可能にする

部分復元可能な秘密分散バックアップの従来の検索方法



従来の検索方法でのシェア同士の一致判定

検索用の情報の分散には乱数を用いる

検索用シェアと同じシェアを生成するのが困難

シェア同士が一致しない

シェア同士の一致判定

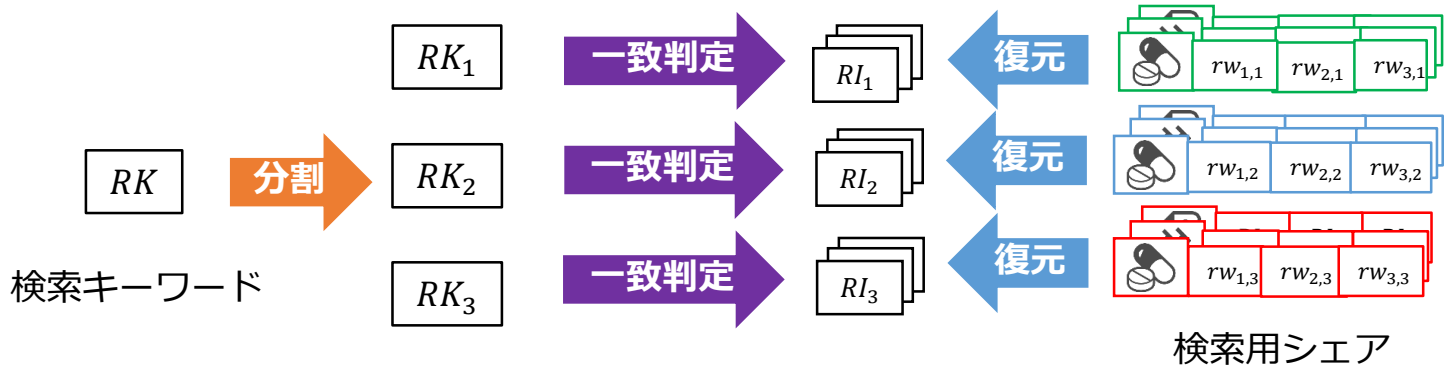
定数を用いて
検索用の情報と検索キーワードを分散

検索用の情報と検索キーワードが同じ場合

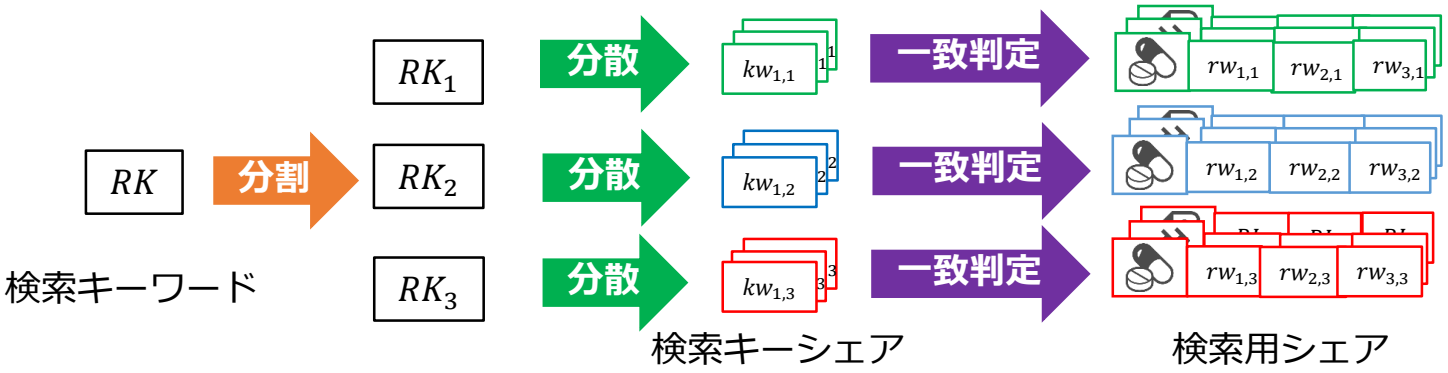
検索用シェアと検索キーシェアが一致

従来の検索方法と提案検索方法の検索の流れ

- 従来の検索方法



- 提案検索方法



比較実験

- (3,5)しきい値秘密分散法
- 6(2+2+2)bytesの検索用の情報
- 102400×5個のシェアのうち
  該当するシェアが19456×5個

方法	検索時間(s)
従来の検索方法	15.43957
提案検索方法	1.30478

安全性の比較

- 従来の検索方法

  乱数が1組漏洩しても，全ての検索用の情報を知ることはできない

- 提案検索方法
  - 定数が漏洩すると，全ての検索用の情報が知られてしまう
  - 検索用シェアを比較すると，同じ検索用の情報が付与されているデータが分かってしまう

まとめ

- 部分復元可能な秘密分散法における秘密分散データを用いた検索を提案
  - シェア同士の一致の判定を可能にした
  - 安全性の比較
- 今後の課題
  - 安全性を確保する方法の考案