医療データのバックアップと災害時における利用

ネットワーク信号処理研究室

伊藤 崇之　　前野 和紀

カルテ

病院で使われる患者の情報を記録したもの

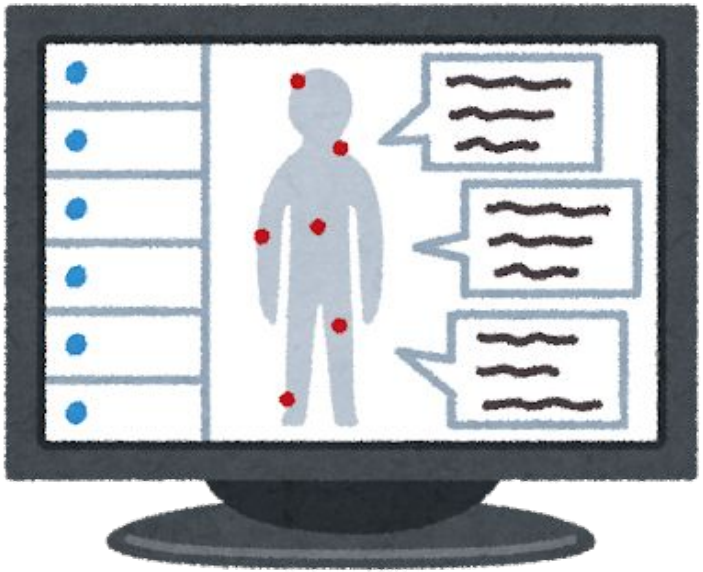
名前
住所
病名
アレルギー
など…

カルテの情報をもとに診察をおこなう

電子カルテ

紙ではなくコンピュータを用いてカルテを電子化したもの

管理が容易
共有が簡単
手書きによるミスが減る

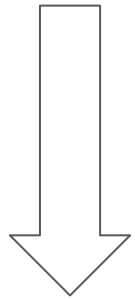


問題点

大きな災害が発生するとカルテや電子カルテは病院と共に消失してしまう可能性がある

対策

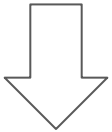
一か所に保存していると災害で失われる



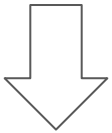
複数の遠隔地にバックアップを
おこなう

問題点

カルテには個人情報が書かれている

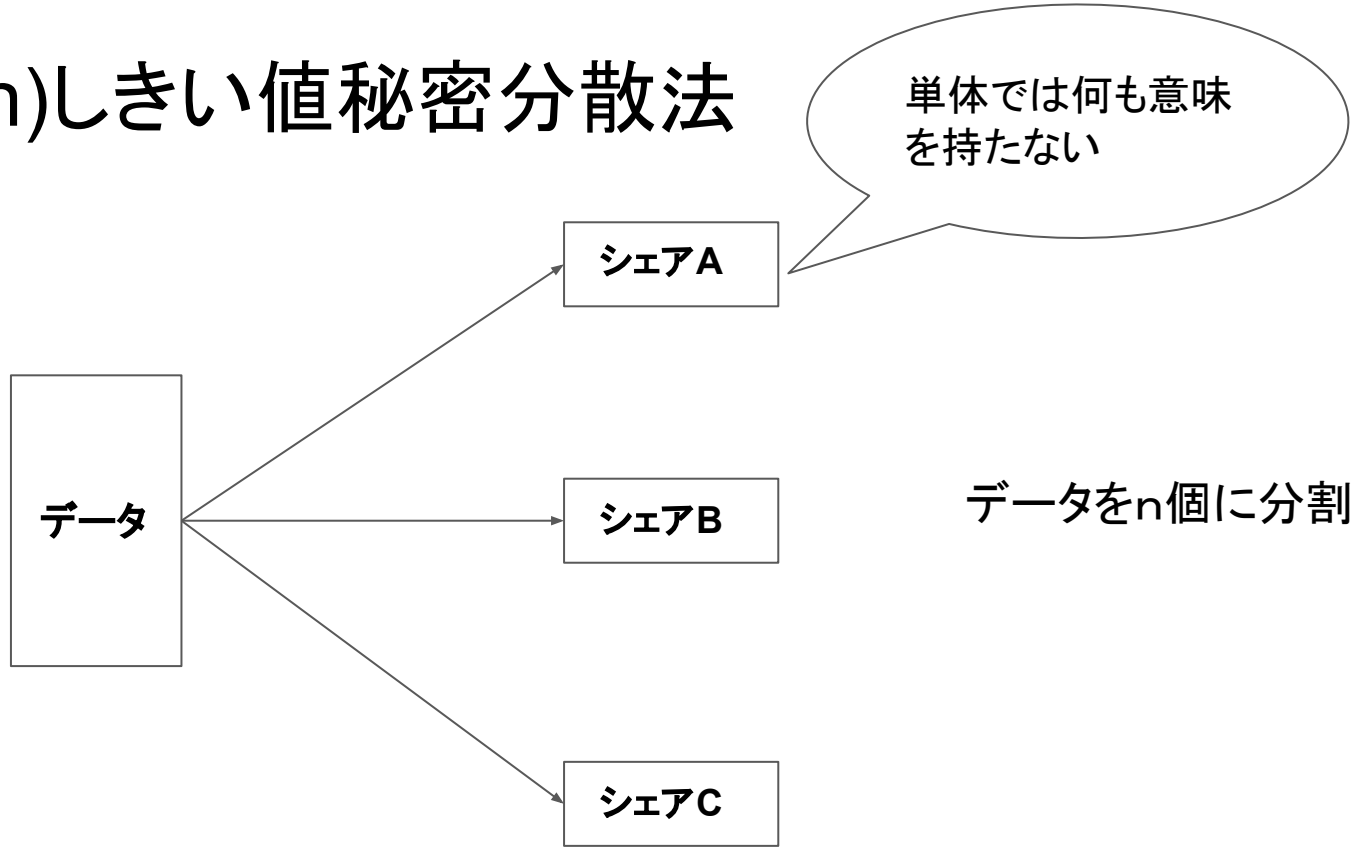


第三者が見れない環境が必要



(k,n)しきい値秘密分散法を使う

(k,n)しきい値秘密分散法



データをn個に分割

k＝2，n＝3

(k,n)しきい値秘密分散法

シェアA

シェアB

シェアC

データ

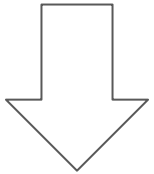
シェアA

k個のシェアでデータを復元できる

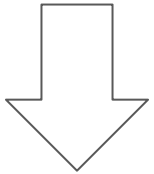
k＝2，n＝3

問題点

情報が欲しい時は全てのデータを復元しなければいけない



特定の情報だけを得ることができない

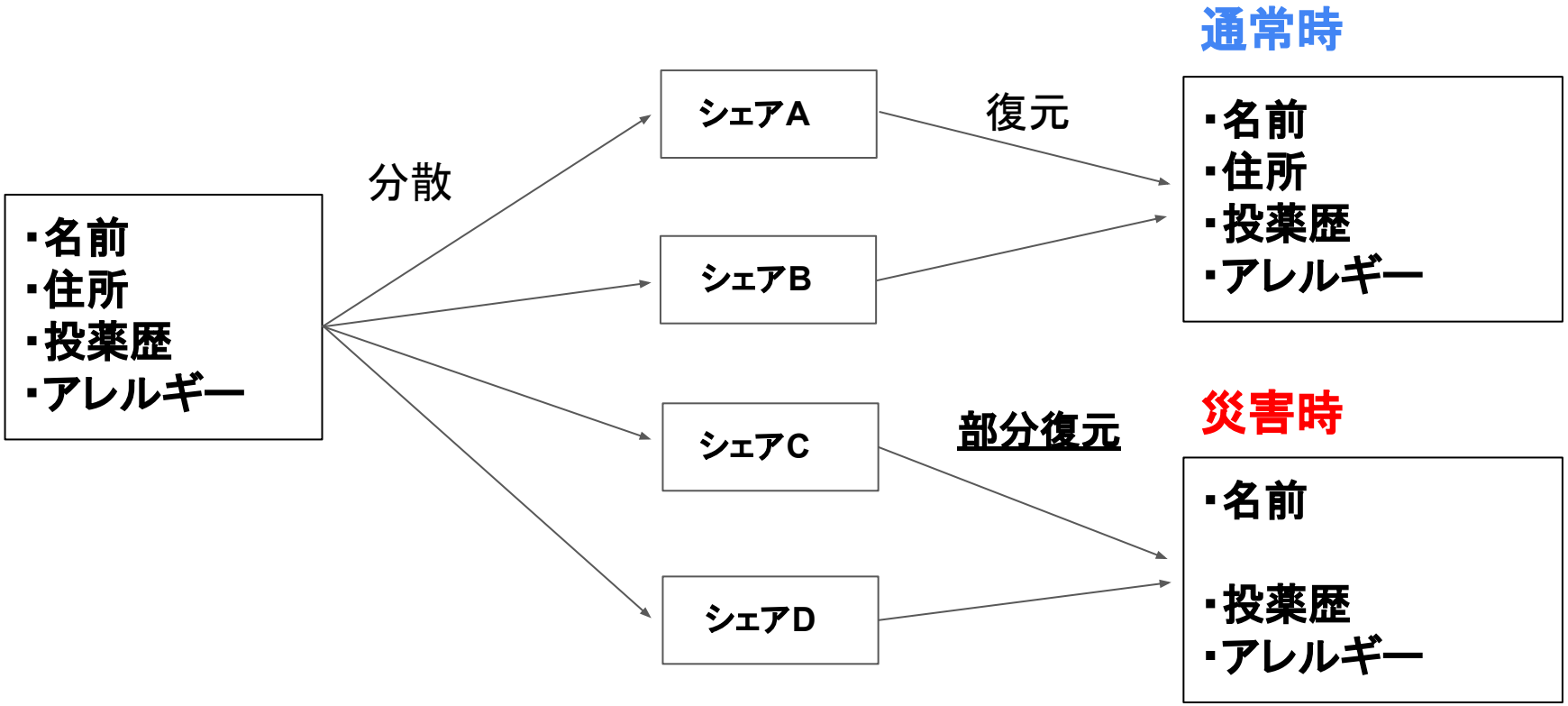


部分復元を使う

部分復元

これと(k,n)しきい値秘密分散法を同時に用いる

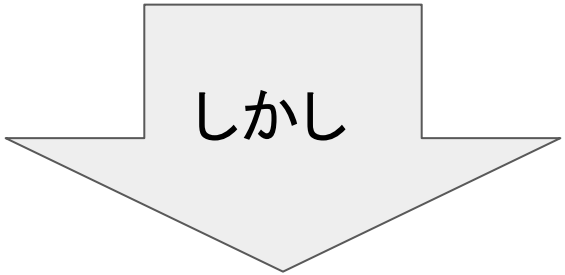
部分復元


通常時
・名前
・住所
・投薬歴
・アレルギー
分散
シェアA
シェアB
シェアC
シェアD
復元
部分復元
災害時
・名前
・投薬歴
・アレルギー

部分復元の問題点

識別情報もシェアとして分散されているため、

シェアにどんな情報が書かれているか復元しなければわからない



シェアの復元には**膨大な時間**が必要になる。

おわりに

現在は

- シェアの検索方法
- 部分復元の高速化

について研究しています