災害急性期に医療情報の更新・利用可能な秘密分散バックアップシステム

1220388　森岡　弘貴

情報学群

ネットワーク信号処理研究室

背景

東日本大震災では津波により病院に保存されていたカルテが消失

 被災地での診療に支障

医療情報を保全し，災害時に活用

医療情報の保全条件

冗長性：広域災害によって全て消失しないために，同時に被災することのない遠隔地に保管すること

秘匿性：保全されたデータから情報漏えいが無いようにデータ を秘匿すること

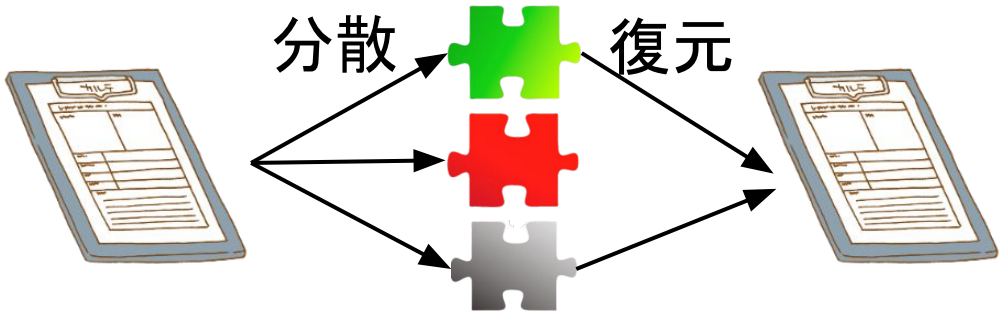
満たす方法

(k, n)しきい値秘密分散法

next
他の方法は？

なぜ(k, n)しきい値秘密分散法なのか

暗号化：暗号化されたデータだけで解読が可能
秘密分散法:シェアだけでの復元は不可能



$k = 2, n = 3$のとき

シェアがk個未満だと復元できない　　秘匿性○
シェアが$\mathrm{n} - k$個以下消失しても復元できる　　冗長性○

災害時の利用

災害急性期：電源やネットワークなどのリソースが不足

診療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[1]

- 秘密分散したデータの一部分だけを部分的に復元する
- データを項目ごとに分割しそれぞれ秘密分散
- 欲しい項目のシェアを結合して復元

[1]田中麻美，福富英次，福本昌弘，“秘密分散バックアップした医療データの部分復元”，信学技報 IA2015-74，pp.31-36，2015

医療情報の更新

- 病院の診療が行われるとカルテは更新される
- 適切な処置のためできる限り新しいものが欲しい
  ⇒ 医療情報を随時バックアップする

しかし災害時は……

- 電源やネットワークなどのリソースが不足
- 傷病者を含む診療を受ける人が増加
  ⇒ 作成されるカルテが増加

目的と目標

目的

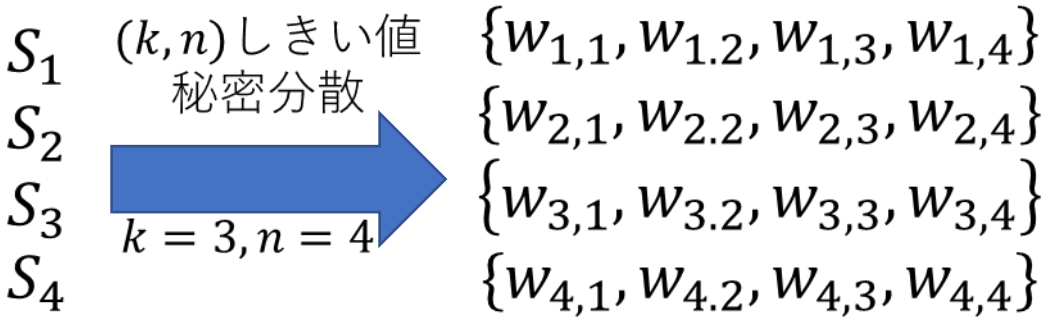
- 分散する医療情報を削減しリソースの圧迫を避ける
- 内容に変更のあったものだけを分散する

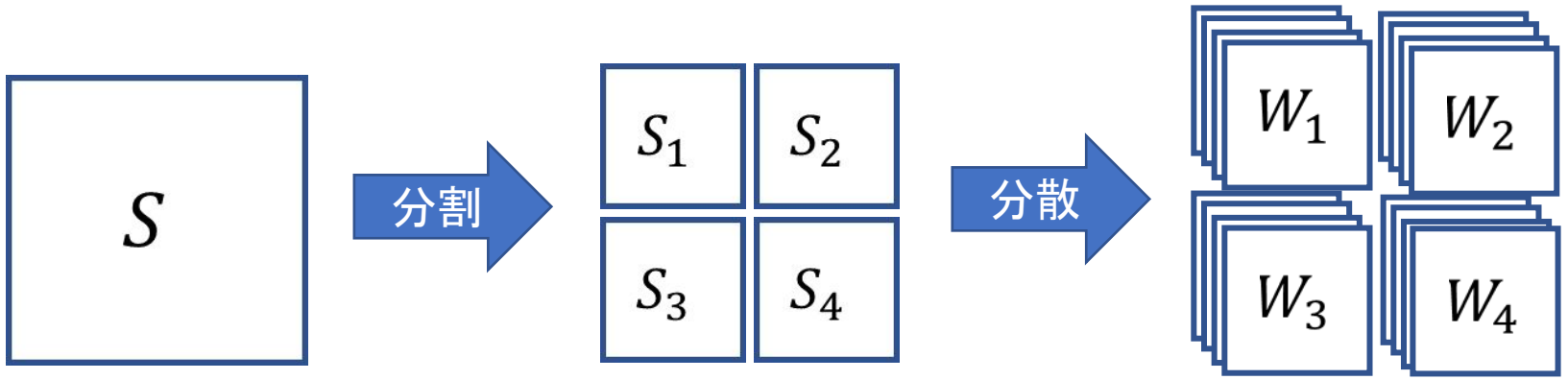
目標

- 部分更新が可能であることを証明する
- 最新の医療情報を検索する

部分更新を可能とする方法(1/3)

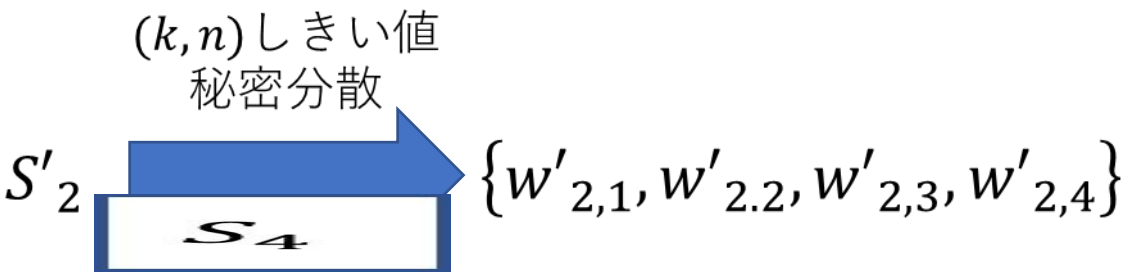
$S = \{S_1\ S_2\ S_3\ S_4\}$の項目のシェアを用いて
$S' = \{S_1, S'_2, S_3, S_4\}$が復元できることを示す

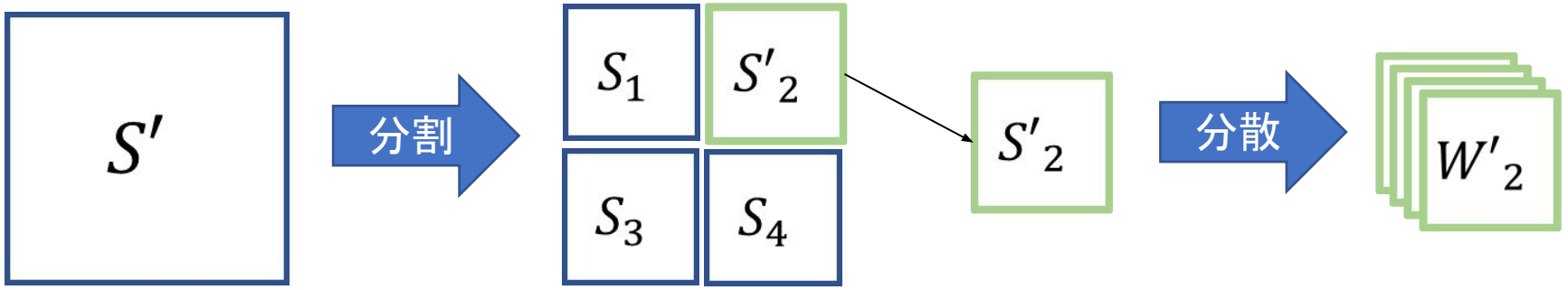




部分更新を可能とする方法(2/3)

$S' = \{S_1, S'_2, S_3, S_4\}$を部分更新





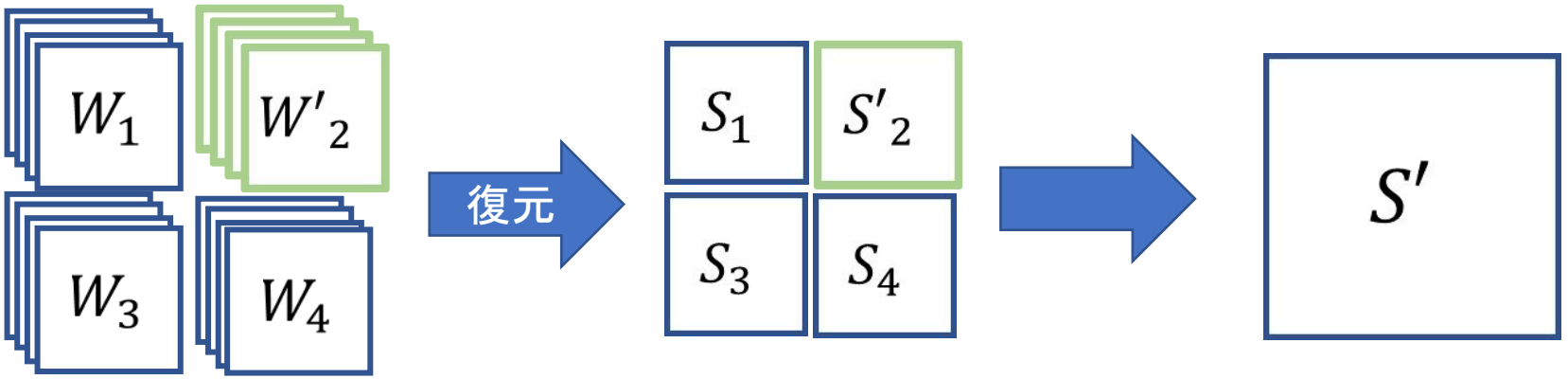
部分更新を可能とする方法(3/3)

W'_2とW_1, W_3, W_4で復元

$$\begin{pmatrix} w_{1,1} & w'_{2,1} & w_{3,1} & w_{4,1} \\ w_{1,2} & w'_{1,2} & w_{3,2} & w_{4,2} \\ w_{1,4} & w'_{2,4} & w_{3,4} & w_{4,4} \end{pmatrix}$$

復元

$$\{S_1, S'_2, S_3, S_4\} = S'$$



実際どれ程削減できる？ next

部分更新による情報の削減率

表1:ADT^A08を構成する項目

項目名	最大長
MSH	1995
EVN	578
PID	6017
NK1	5911
PV1	2973
DB1	292
OBX	67009
AL1	292
IN1	780
合計	90287

表2:必ず変化する項目

項目名	最大長
MSH	1995
EVN	578
OBX	67009
合計	69582

最大23%の削減が可能

SS-MIX2　標準化ストレージ仕様書Ver.1.2gより

医療情報の検索

部分更新では最新のシェアが必要となる

秘密分散データを用いた医療データ検索システム[2]

- 医療情報内の個人を識別できる情報をタグとして分散しバックアップデータに付与
- 医療情報を復元せずに高速な検索が実現

誰の医療情報かまでは絞れるが
いつ作成されたどの種類のデータかまでは検索できない

---

[2]中村巴，福冨英次，福本昌弘，“ 部分復元可能な秘密分散法におけるシェア間の係数の差の比較による医療データの検索”，電子情報通信学会 暗号と情報セキュリティシンポジウム (SCIS2020)，3C1-4，2020.

最新のシェアの検索

- 医療情報内のMSHのみを部分復元
- MSHにはメッセージ作成日時と，メッセージを識別するコードが記載

MSHから最新のシェアを
検索することが可能

構造化処方オーダ(RDE^O11)

```
MSH|^~¥&|HIS123|SEND|GW|RCV|20110701224603.984||RDE^O11^RDE_O11|20110701000001|P|2.5||||||^ISO IR87||ISO
 2022-1994|SS-MIX2_1.20^SS-MIX2^1.2.392.200250.2.1.100.1.2.120^ISO
PID|0001||9999013^^^^PI||患者^太郎^^^^^L^I~カンジャ^タロウ^^^^^L^P||19480405|M|||^^^^422-8033^JPN^H^静岡県
 静岡市登呂１－３－５||^PRN^PH^^^^^^^^^054-000-0000|^WPN^PH^^^^^^^^^054-999-2455
 ||||||||||||||||||20110601121551
PV1|0001|O|01^^^^^C||||110^医師^一郎^^^^^^^L^^^^^I|||01
ORC|NW|000000011000185||1|||||20110701103045|058^入力者^花子^^^^^^^L^^^^^I||110^医師^一郎^^^^^^^L^^^^^I|
 10^^^^^C||||01^内科^99XY1|VMDOCX01^^99XY2|||登呂病院|^^^^422-8033^JPN^^静岡県静岡市駿河区登呂3-1-1
 |^^^^^^^^^^^054-284-9122||||||0^外来患者オーダ^HL70482
RXE||108665201^ダーゼン錠（５mg)^HOT9|1||TAB^錠^MR9P|||||15|TAB^錠^MR9P||||2011070112345||||3^TAB&錠
 &MR9P||OHP^外来処方^MR9P^OHI^院内処方^MR9P
TQ1|1|||1013044400000000&内服・経口・１日３回朝昼夕食後&JAMISDP01|||5^d|2011070100
RXR|PO^ロ^HL70162
ORC|NW|000000011000185||1|||||20110701103045|058^入力者^花子^^^^^^^L^^^^^I||110^医師^一郎^^^^^^^L^^^^^I
 |10^^^^^C||||01^内科^99XY1|VMDOCX01^^99XY2|||登呂病院|^^^^422-8033^JPN^^静岡県静岡市駿河区登呂
 3-1-1|^^^^^^^^^^^054-284-9122||||||0^外来患者オーダ^HL70482
RXE||110626901^パンスポリンＴ錠（１００mg)^HOT9|2||TAB^錠^MR9P|||||30|TAB^錠^MR9P|||||||6^TAB&錠
 &MR9P||OHP^外来処方^MR9P^OHI^院内処方^MR9P
TQ1|1|||1013044400000000&内服・経口・１日３回朝昼夕食後&JAMISDP01|||5^d|2011070100
```

更新時には最新の医療情報を検索でき，
利用時には任意の期間の医療情報を取り出すことができる

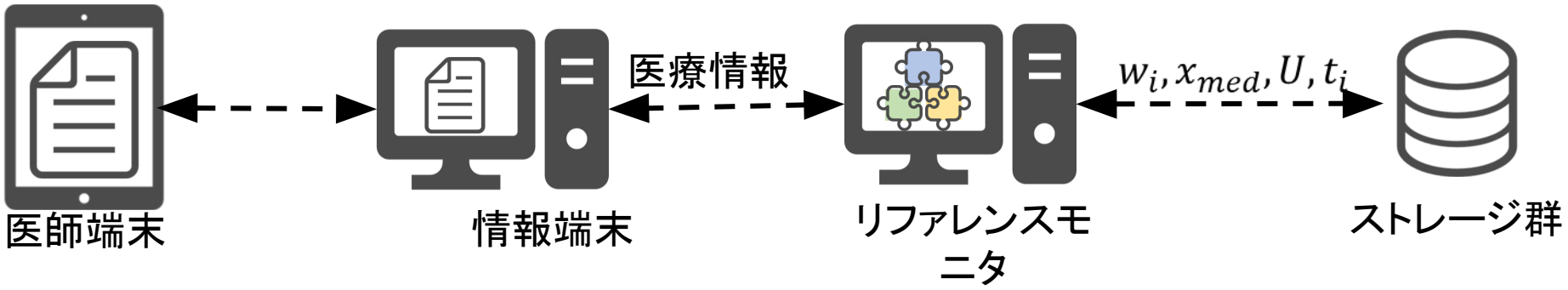
従来の検索方法との比較

従来の方法：医療情報をすべて復元してから最新のデータを検索

提案方法：1項目のみを部分復元して検索し該当データのみを復元

- 復元するデータ量が減少
- 検索時間が向上

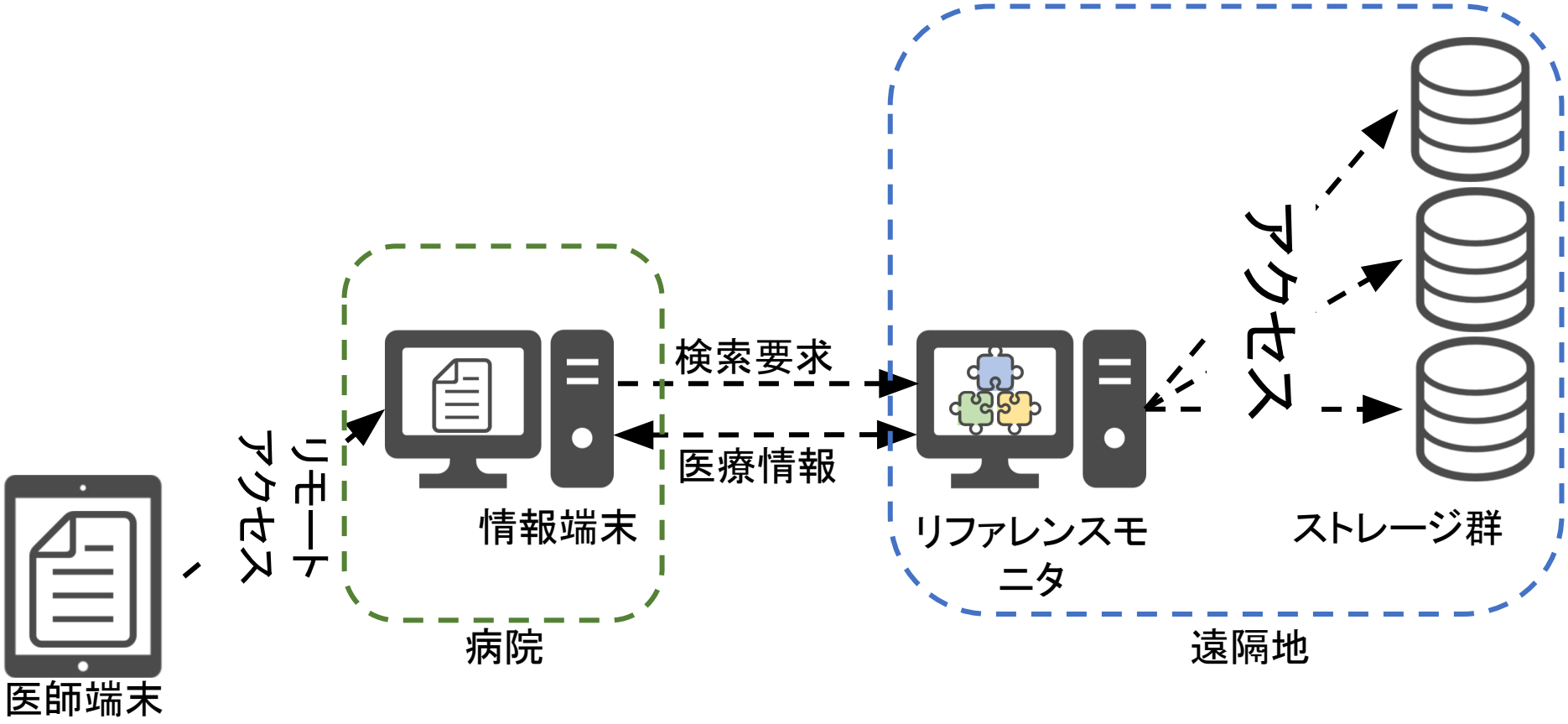
バックアップシステムの構成



w_i:医療情報を分散したシェア
U:シェアを紐づける情報

x_{med}: 医療情報を分散する際に用いる集合
t_i: 識別情報を分散したタグ

バックアップシステムの構成



リファレンスモニタを遠隔地に設置することで
災害時でも安定した処理が可能

まとめ

目的

- 医療情報の更新量の削減
  - 部分更新により最大23%の削減
  - 最新のシェアを検索する仕組みにより災害急性期に任意の期間の医療情報を取り出すことが可能
  - 分散復元検索を行うリファレンスモニタを遠隔地におくことで処理を安定化

今後の課題

- 検索の更なる高速化
- 実際の環境での実験