

令和 3 年年度

学士学位論文

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

Secret sharing backup system that can update and
use medical information during the acute phase of a
disaster

1220388 森岡 弘貴

指導教員 福本 昌弘

2022 年 3 月 6 日

高知工科大学 情報学群

要 旨

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

森岡 弘貴

広域災害に備えて医療情報を遠隔地に保全することが求められている。医療情報は個人情報を含むため、厳重な管理のもと保全を行う必要がある。適した方法として秘密分散法を用いたバックアップが研究され、また秘密分散法と秘匿通信を用いた電子カルテ保管・交換システムが開発されるなど、医療情報の秘密分散バックアップシステムの実用化が近づいている。診療に用いる医療情報はできる限り最新のものが望まれるため、作成された医療情報を随時バックアップする必要がある。しかし、災害時は、診療を受ける人の増加により作成される医療情報も増加し、バックアップ量の増加によるリソースの圧迫が想定される。

本論文では災害急性期のリソース不足を避け、秘密分散処理量の削減を目的として、医療情報の部分更新と最新のシェアの検索方法を提案している。部分更新は、分散バックアップする医療情報を意味のある項目ごとに分割し、前回と内容に変更のある項目のみを分散し、変更のない項目は前回のシェアを流用する。この部分更新が可能であることを証明し、部分更新による秘密分散処理の削減率を示した。最新のシェアの検索は誰のシェアかを絞り込んだあとにデータの種類や日付が記された項目のみを部分復元し検索を行うことで、従来の全て復元したのち検索する方法よりも復元処理量が減少し、検索処理が向上することを示した。また、医療情報の更新・利用が可能なバックアップシステムを提案している。提案システムを用いることで災害急性期であってもリソースを圧迫することなく医療情報の分散バックアップが行え、リソース不足に左右されない安定した処理を行うことが可能になる。

キーワード 秘密分散法, 分散バックアップ, 部分更新, 検索, 部分復元

Abstract

Secret sharing backup system that can update and use medical information during the acute phase of a disaster

It is required to preserve the medical information in far land for wide-area disasters. Medical information must be kept under strict control because it contains personally identifiable information. In preserving medical information, the secret sharing method which were considered suitable has been studied. Also, electronic health record storage and exchange system that using secret sharing methods and confidential communications have been developed, and secret sharing backup system for medical information is nearing practical implementation. Medical information used for medical treatment should be as latest as possible, so it is necessary to backup the medical information created at any time. However, in the event of a disaster, the amount of medical information created increases due to the increase in the number of people receiving medical treatment, and the increased volume of backups is expected to put pressure on resources.

In this paper, we have proposed a method that partial update of medical information and retrieval of the latest share, to avoid lack of resource and reducing the processing volume of secret sharing during the acute phase of a disaster. In partial update, medical information to be distributed backup is divided into sections with meaningful items, and only those sections whose contents have changed from the previous share are distributed by secret sharing scheme, while the previous share is used for the sections whose contents have not changed. We have proved that partial updates can be per-

formed and shown the reduction rate of the secret sharing process by partial update. The retrieval of the latest share is performed by narrowing down the patient's share that corresponds to that share and only search to the share of the person whose share it is, and then partially restoring only confined decoding and retrieving the items with the type and date of the data. Compared to the conventional method, the amount of restoration has been reduced and the retrieval time improved. In addition, Secret sharing backup system that can update and use medical information is proposed. The proposed system enables distributed backup of medical information during the acute phase of a disaster without stressing resources, and stable processing that is not affected by lack of resource.

key words secret sharing scheme, distributed backup, partial update, retrieval, confined decoding

目次

第 1 章	序論	1
1.1	本研究の背景と目的	1
1.2	本論文の構成	2
第 2 章	医療情報の遠隔地バックアップと災害時の活用	3
2.1	バックアップの対象となる医療情報	3
2.1.1	電子カルテ	3
2.1.2	SS-MIX2	4
2.2	医療情報の保全方法	5
2.3	(k, n) しきい値秘密分散法	6
2.4	まとめ	8
第 3 章	分散バックアップする医療情報の部分更新と最新のシェアの検索	10
3.1	医療情報の部分更新	11
3.1.1	部分更新が可能なことの証明	11
3.1.2	部分更新による医療情報の削減率	15
3.2	最新の医療情報の検索	16
3.2.1	部分復元可能な医療情報の検索	16
3.2.2	同じ種類の最新のシェアの検索	18
3.3	まとめ	19
第 4 章	災害時に更新・利用可能な秘密分散バックアップシステム	20
4.1	システムの構成要素	20
4.1.1	分散バックアップシステムで扱うデータ	20
4.1.2	想定される利用者	21

目次

4.1.3	分散システムの構成デバイス	22
4.1.4	構成デバイス間での盗聴のリスク	23
4.2	システム構成	24
4.2.1	医師端末	24
4.2.2	情報端末	25
4.2.3	リファレンスモニタ	26
4.2.4	ストレージ群	27
4.3	評価	27
4.4	まとめ	28
第 5 章	結論	29
5.1	本研究のまとめ	29
5.2	今後の課題	30
	謝辞	31
	参考文献	32

目次

2.1	SS-MIX2 のディレクトリ構造	5
2.2	患者データの例	5
2.3	$k = 3, n = 4$ のときの (k, n) しきい値秘密分散法	6
3.1	医療情報の部分更新の流れ	11
3.2	タグを用いた検索の流れ	16
4.1	部分更新時のデータの動き	23
4.2	検索時のデータの動き	24
4.3	分散バックアップシステムの構成	24
4.4	情報端末へのリモートアクセスの流れ	25
4.5	リファレンスモニタへの接続の流れ	26
4.6	リファレンスモニタの設置場所	26
4.7	ストレージ群への接続の流れ	27

表目次

3.1	ADT^A08 を構成する各セグメント	15
3.2	ADT^A08 の更新されるたびに内容が変化する項目	16
4.1	各段階で扱うデータ	21
4.2	扱うデータの説明	22

第 1 章

序論

1.1 本研究の背景と目的

東日本大震災では、津波によって沿岸部の病院に保管されていた電子カルテが消失し、被災地での医療行為に支障をきたした [1]. これをうけて、医療情報の保全が求められることとなった。保全方法として医療情報を電子化し、遠隔地にバックアップする方法が考えられるが、医療情報は個人情報を含むため、医療情報の電子バックアップを行う際に委託事業者が守らなければならないものとして、日本の厚生労働省、経済産業省、総務省がそれぞれガイドラインを出しており、厳重な管理のもと運用されなければならない [2][3][4]. 医療情報を安全に管理するために秘密分散技術を用いる方法が研究された [5]. 医療情報は消失を防ぐだけでなく、平時の地域医療の連携のための情報共有や、災害時の診療への利用が求められる [6]. 高知県では南海トラフ地震での医療情報の損失を防ぐために、県内の 13 病院によって医療情報の県外保全を目的として ICT 協議会を結成し、地域包括システムを構築することとした [7]. その取り組みの一環として「高知あんしんネット」という、医療介護情報を共有するためのネットワークシステムが構築され、医療情報を集約して管理し、救急搬送や転院の際に薬や検査の重複が防げ、患者からの持病や投薬歴などの情報が不要になるなど、施設間での情報連携を円滑にするシステムが構築されている [8]. さらに秘密分散技術と秘匿通信技術を組み合わせ、電子カルテデータのセキュアなバックアップと医療機関間での相互参照、災害時を想定した場合に必要とされる医療データ項目の迅速な復元が可能な保険医療用の長期セキュアデータ保管・交換システムが開発されるなど、秘密分散技術を用いた分散バックアップとその利用が実用化される未来が近づいている [9].

1.2 本論文の構成

秘密分散法を用いてバックアップされたデータを診療に利用する際、迅速な復元を行うために医療情報の部分復元や、検索システムが提案されている [10][11]. 診療に利用する医療情報は新しいことが望ましい. したがって医療情報を随時バックアップする必要があるが、災害時は電源やネットワーク等のリソースが不足することが想定され、また、傷病者の増加によって作成される医療情報も増加し、随時バックアップしていくと、不足しているリソースを圧迫することになる.

本研究では、医療情報の分散バックアップを行う際、災害時の不足しているリソースの圧迫を避け、分散の処理量を削減させることを目的として医療情報の部分更新を提案する. また、部分更新にはストレージに保存されている最新のシェアが必要になるため、最新のシェアを検索する方法についても提案する.

1.2 本論文の構成

本節では、本論文の構成について述べる. 2 章では医療情報の遠隔地へのバックアップについて述べ、 (k, n) しきい値秘密分散法について述べる. 3 章では、医療情報の部分更新と最新のシェアの検索方法を提案する. 4 章では災害急性期に医療情報を更新・利用が可能なシステムの構成について述べ、5 章ではまとめと今後の課題について述べる.

第 2 章

医療情報の遠隔地バックアップと災害時の活用

東日本大震災では、津波によって沿岸部の病院に保管されていた電子カルテが消失し、これにより被災地での医療行為に支障をきたすこととなった。これをうけて電子化された医療情報のバックアップが求められた。医療情報は個人情報を含むことから 3 省 3 ガイドラインを遵守し、厳重な管理のもと運用されなければならない。医療情報を保全する手法として分散バックアップが有効であり、適した方法として (k, n) しきい値秘密分散法がある。

本章ではバックアップの対象となる医療情報について述べ、医療情報のバックアップの条件について述べる。次に、保全方法の一つである (k, n) しきい値秘密分散法について述べる。

2.1 バックアップの対象となる医療情報

医療情報にはさまざまな種類があるが、本研究で対象とする電子カルテについて述べる。また、医療情報の標準規格である厚生労働省電子的診療情報交換推進事業 (SS-MIX2:Standardized Structured Medical Information eXchange) についても述べる。

2.1.1 電子カルテ

電子カルテは、医師が患者を診察した際に作成する診療録であるカルテを電子化したものを指す。カルテと比較して保全に必要な場所を削減でき、高速な検索や利用者間の情報共有

2.1 バックアップの対象となる医療情報

を効率的に行えるという利点がある一方、電子カルテの運用には持続的なコストがかかることや不正アクセスによる情報漏洩などの欠点も存在する。

カルテを含む法的に保存義務のある文書等を電子的に保存する際の要件として、真正性、見読性、保存性を満たす必要がある [2]。真正性、見読性、保存性について以下に詳細を述べる。

- 真正性

医師等の正当な権限において作成された記録に対し、虚偽入力や書き換え、消去及び混同が防止されており、第三者から見て作成の責任の所在が明らかであること。

- 見読性

電子媒体に保存された内容を、さまざまな要求に応じて、それぞれの目的に対して支障のない応答時間やスループット、操作方法で紙の状態と同等の見読可能な状態にできること。

- 保存性

記録された情報が法令等で定められた期間にわたって真正性を保ち、見読可能な状態で保存されること。

2.1.2 SS-MIX2

電子カルテは電子カルテシステムを提供するベンダやシステムのバージョンにより異なるフォーマットが使用されている。互換性のない電子カルテシステム間での情報共有は困難であり、地域医療連携など異なる病院間での人の手を介さない情報伝達に支障をきたす場合がある。そこで厚生労働省はすべての医療機関を対象とした医療情報の交換・共有による医療の質の向上を目的とした「厚生労働省電子的診療情報交換推進事業」(SS-MIX: Standardized Structured Medical record Information eXchange)を開始した [13]。SS-MIX2 では、医療情報をテキストデータの HL7Ver2.5 形式で標準化ストレージに保存する。標準化ストレージは、定められたディレクトリ構造にしたがってデータを保存する。ディレ

2.1 バックアップの対象となる医療情報

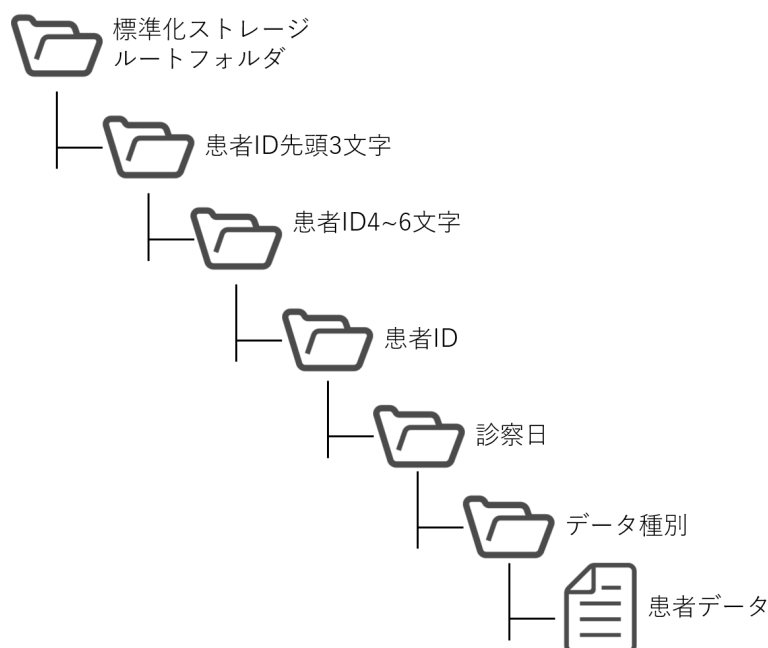


図 2.1 SS-MIX2 のディレクトリ構造

構造化処方オーダー (RDE^O11)
<pre> 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^P 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 PVI 0001 0 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^外来患者オーダー^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^外来患者オーダー^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 15^d 2011070100 </pre>

図 2.2 患者データの例

クトリ構造を図 2.1 に示す。また、HL7Ver2.5 形式に変換された患者データの例を図 2.2 に示す。

2.2 医療情報の保全方法

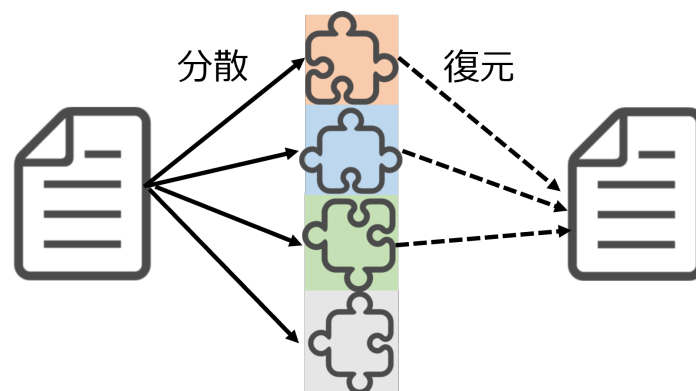


図 2.3 $k = 3, n = 4$ のときの (k, n) しきい値秘密分散法

2.2 医療情報の保全方法

広域災害に備えて医療情報を保全する場合、データを冗長化させる方法があるが、冗長性を持たせたデータが全て近辺に存在するとき、広域災害によって全て消失する恐れがある。そのため、同時に被災することのない遠隔地に保全する必要がある。医療情報はプライバシーなデータを含むため、バックアップデータから情報漏えいしないようないよう秘匿化する必要がある。したがって、医療情報の保全方法として、冗長性、秘匿性、電子保存の 3 原則を満たしている必要がある。秘匿化の手段には暗号化と秘密分散があるが、暗号化は暗号文そのものからの解読が可能であるのに対し、秘密分散法は保管するデータだけでの元データの復元は不可能である。ゆえに、秘密分散法を用いる。その他の条件を満たした手法として (k, n) しきい値秘密分散法を用いた分散バックアップがあげられる。

2.3 (k, n) しきい値秘密分散法

(k, n) しきい値秘密分散法は、データを n 個のシェアという意味を持たないものに分散し、 k 個以上のシェアを集めることで元のデータを復元することが可能な方法である。 (k, n) しきい値秘密分散法について図 2.3 に示す。 k 個未満のシェアであれば、そこからデータを復元することはできないため秘匿性を持ち、 $n - k$ 個以下のシェアが破損しても復元することが可能なため冗長性を持つものである。以下に (k, n) しきい値秘密分散法の手法を示す。

2.3 (k, n) しきい値秘密分散法

分散したいデータを S , 素数を $p(S < \text{かつ } n < p)$, $\mathbb{Z}/p\mathbb{Z} - \{0\}$ 上の集合を

$$x = \{x_1, x_2, \dots, x_n\} (i \neq j \text{ のとき } x_i \neq x_j)$$

とし, $\mathbb{Z}/p\mathbb{Z}$ 上の乱数の集合を R とする. x より

$$X = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{k-1} \end{pmatrix} \pmod{p}$$

となるような (n, k) 型行列 X を作成する. S と R から

$$\mathbf{A} = \begin{pmatrix} S \\ r_1 \\ r_2 \\ \vdots \\ r_{k-1} \end{pmatrix} (r_1, r_2, \dots, r_{k-1} \in R, r_{k-1} \neq 0)$$

となるような k 行ベクトル $\mathbf{A}$ を作成する. p を法とする X と $\mathbf{A}$ の乗算より,

$$X\mathbf{A} = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} \pmod{p}$$

となるような $w_i (i = 1, 2, \dots, n)$ が得られる. w_i をシェアと呼び, w_i と x_i を対応付けてストレージに保存する.

復元時は, シェアを k 個以上集める. 集めたシェアの k 個から

$$\mathbf{W} = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_k \end{pmatrix} \pmod{p} \tag{2.1}$$

k 行ベクトル $\mathbf{W}$ を作成する. 選択したシェアと対応する x_i より,

$$X' = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & x_k^2 & \cdots & x_k^{k-1} \end{pmatrix} \pmod{p}$$

2.4 まとめ

となるような (k, k) 型行列 X' を作成する． X' の逆行列 X'^{-1} を $\mathbf{W}$ の左からかけると

$$X'^{-1}\mathbf{W} = X'^{-1} \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_k \end{pmatrix} = X'^{-1}X' \begin{pmatrix} S \\ r_1 \\ r_2 \\ \vdots \\ r_{k-1} \end{pmatrix} = \begin{pmatrix} S \\ r_1 \\ r_2 \\ \vdots \\ r_{k-1} \end{pmatrix} \pmod{p}$$

となり，データ S が得られる．以上が (k, n) しきい値秘密分散法の分散および復元手法である．式 (2.1) を連立方程式で表現すると

$$\begin{cases} w_1 = S + r_1x_1 + r_2x_1^2 + \cdots + r_{k-1}x_1^{k-1} \pmod{p} \\ w_2 = S + r_1x_2 + r_2x_2^2 + \cdots + r_{k-1}x_2^{k-1} \pmod{p} \\ \vdots \\ w_k = S + r_1x_k + r_2x_k^2 + \cdots + r_{k-1}x_k^{k-1} \pmod{p} \end{cases} \quad (2.2)$$

となる．式 (2.2) を解くとデータ S を求めることができる． x_i は w_i に対応して決まる定数であるため，変数は k 個である．連立一次方程式が解をただ 1 つもつための条件として，式が k 個あればよいので， w_i が k 個以上あれば S を一意に定めることができる． w_i が k 個未満であれば， S を求めることができない．以上のことから， (k, n) しきい値秘密分散法は k 個未満のシェアからは元のデータは復元することができず， $n - k$ 個以下のシェアが失われていても，元のデータを復元することができるため，秘匿化と冗長化が可能である．また，ほかのバックアップ手法として，元データを暗号化しバックアップするという手法があるが，暗号化では，バックアップデータのみからの解読が可能であるのに対し，秘密分散法は，バックアップするシェアのみでの復元は不可能であるため， (k, n) しきい値秘密分散法は医療情報のバックアップ手法として適している．

2.4 まとめ

東日本大震災では，津波によって沿岸部の病院に保管されていた電子カルテが消失し，これにより被災地での医療行為に支障をきたすこととなった．これをうけ医療情報を保全し被

2.4 まとめ

災地での診療に活用することが求められている。本章では、バックアップの対象となる医療情報について述べ、広域災害に備えた医療情報の保全条件について述べた。保全条件を満たした手法の1つである (k, n) しきい値秘密分散法を用いたバックアップについて述べ、秘密分散のほかに秘匿化する手段として暗号化があるが、暗号化は保管するデータそのものから解読が可能であるのに対し、秘密分散法は保管するデータのみでは元データを復元することができないことから、秘密分散法を用いていることを述べた。

診療を行う際、できる限り最新の医療情報があることが望ましいことから、作成された医療情報を随時バックアップする必要がある。しかし、災害時は電源やネットワーク等のリソースが不足することや、傷病者を含む診療を受ける人の増加により作成される医療情報の増加が想定され、増加する医療情報全てのバックアップを随時行う場合、不足しているリソースを圧迫する恐れがある。

第 3 章

分散バックアップする医療情報の部分更新と最新のシェアの検索

広域災害に備えた医療情報の保全と活用として、 (k, n) しきい値秘密分散法を用いた分散バックアップによる保全がある。また、診療にはなるべく最新の医療情報があることが望ましいことから、作成された医療情報を随時バックアップする必要がある。しかし、災害時は電源やネットワーク等のリソースが不足することや、傷病者を含む診療を受ける人が増加することによって作成される医療情報も増加し、バックアップする量が増加することによってリソースを圧迫することが想定される。そこで本研究では、災害時のリソースの圧迫を避け、分散の処理量を削減させることを目的として、部分更新について提案する。提案方法は、医療情報を意味のある項目ごとに分けたもののうち、前回と内容に変更のない項目は前回のシェアを流用し、変更のあった項目は秘密分散を行い、シェアを作成するというものである。また、前回のシェアを流用する過程で前回のシェアを保管しているストレージから該当するシェアを入手する必要があるため、最新のシェアの検索を提案する。最新のシェアの検索には、ストレージの中から個人を絞り込み、該当する個人のシェアのうち、医療情報の作成日時とデータの種類の種類が記されている項目のみを部分的に復元することで最新のシェアを検索している。

本章では医療情報の部分更新について述べたあと、部分更新に必要となる最新のシェアの検索について述べる。

3.1 医療情報の部分更新

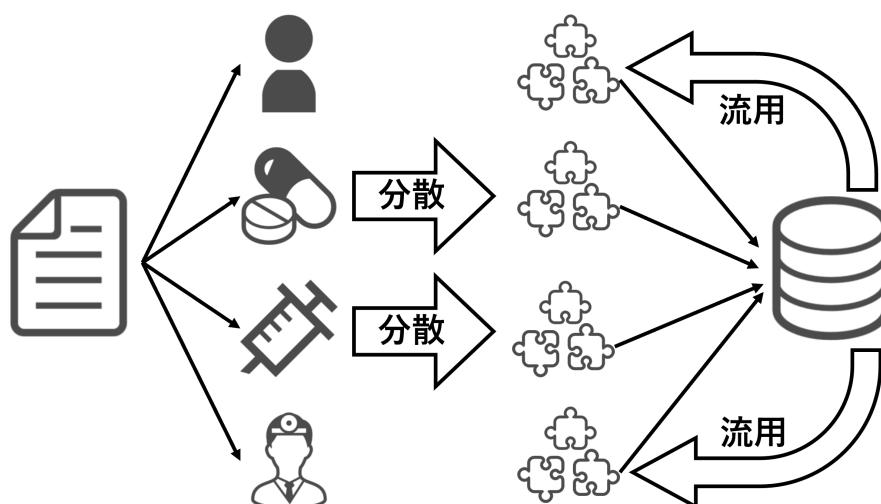


図 3.1 医療情報の部分更新の流れ

3.1 医療情報の部分更新

提案方法である医療情報の部分更新の流れを図 3.1 に示す．提案方法は医療情報を意味のある項目ごとに分割する．その内，前回から内容に変更のあった項目だけを分散し，内容に変更がない項目に関しては前回の該当する項目を分散したシェアをストレージから入手し，分散したシェアと組み合わせて保管する．こうして保管する医療情報のデータ量を減らすことなく，分散バックアップの処理量を削減すること可能となる．

3.1.1 部分更新が可能なことの証明

医療情報の部分更新について述べる．更新前のデータを S とする． S を意味のある項目ごとに分割したデータを $S_i (i = 1, 2, \dots, d)$ とし， S_i のデータ長を l_i とする．素数 $p (S < \text{かつ } n < p)$ を決定し， $\mathbb{Z}/p\mathbb{Z} - \{0\}$ 上の集合を

$$x = \{x_1, x_2, \dots, x_n\} (i \neq j \text{ のとき } x_i \neq x_j)$$

3.1 医療情報の部分更新

とし、 $\mathbb{Z}/p\mathbb{Z}$ 上の乱数の集合を R とする． x より

$$X = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{k-1} \end{pmatrix} \pmod{p}$$

となるような (n, k) 行列 X を作成する．また，分割データ S_i と $\mathbb{Z}/p\mathbb{Z}$ 上の乱数の集合

$R = \{r_{i,1}, r_{i,2}, \dots, r_{i,k-1}\}$ (ただし $r_{i,k-1} \in \mathbb{Z}/p\mathbb{Z} - \{0\}$) を用いて， k 行ベクトル $\mathbf{A}_i$

$$\mathbf{A}_i = \begin{pmatrix} S_i \\ r_{i,1} \\ r_{i,2} \\ \vdots \\ r_{i,k-1} \end{pmatrix}$$

を作成する． p を法とした X と $\mathbf{A}_i$ の乗算により

$$W_i = X \mathbf{A}_i = \begin{pmatrix} w_{i,1} \\ w_{i,2} \\ \vdots \\ w_{i,n} \end{pmatrix} \pmod{p}$$

S_i のシェアを W_i とし，紐付け情報を

$$U = \begin{pmatrix} \prod_{m=2}^d 2^{l_m} \\ \prod_{m=3}^d 2^{l_m} \\ \vdots \\ 1 \end{pmatrix}$$

とする．

更新するデータを

$$S' = S_1 \prod_{m=2}^d 2^{l_m} + S_2 \prod_{m=3}^d 2^{l_m} + \dots + S'_u \prod_{m=u+1}^d 2^{l_m} + \dots + S_{d-1} 2^{l_d} + S_d$$

3.1 医療情報の部分更新

とする．更新が必要な S'_u と, R を用いて

$$\mathbf{A}'_u = \begin{pmatrix} S'_u \\ r_{u,1} \\ r_{u,2} \\ \vdots \\ r_{u,k-1} \end{pmatrix}$$

p を法とした X と $\mathbf{A}'_u$ の乗算により

$$W'_u = X \mathbf{A}'_u = \begin{pmatrix} w'_{u,1} \\ w'_{u,2} \\ \vdots \\ w'_{u,n} \end{pmatrix} \pmod{p}$$

となる．更新後のシェア群を $G' = \{W_1, W'_2, W_3, \dots, W_d\}$, 紐付け情報を

$$U' = \begin{pmatrix} \prod_{m=2}^d 2^{l_m} \\ \prod_{m=3}^d 2^{l_m} \\ \vdots \\ 1 \end{pmatrix}$$

とする． G' からシェアを k 個選び,

$$W'_c = \begin{pmatrix} w_{1,1} & w_{2,1} & \cdots & w'_{u,1} & \cdots & w_{d-1,1} & w_{d,1} \\ w_{1,2} & w_{2,2} & \cdots & w'_{u,2} & \cdots & w_{d-1,2} & w_{d,2} \\ \vdots & \vdots & & \vdots & & \vdots & \vdots \\ w_{1,k} & w_{2,k} & \cdots & w'_{u,k} & \cdots & w_{d-1,k} & w_{d,k} \end{pmatrix} \pmod{p}$$

とする．選択したシェアと対応する x_i より,

$$X' = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{k-1} \\ 1 & x_2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & \cdots & x_k^{k-1} \end{pmatrix} \pmod{p}$$

3.1 医療情報の部分更新

となるような (k, k) 型行列 X' を作成する． W'_c に対して U' をかけ、

$$W'_c U' = \begin{pmatrix} w_{1,1} \prod_{m=2}^d 2^{l_m} + w_{2,1} \prod_{m=3}^d 2^{l_m} + \cdots + w'_{u,1} \prod_{m=3}^d 2^{l_m} + \cdots + w_{d-1,1} 2^{l_d} + w_{d,1} \\ w_{1,2} \prod_{m=2}^d 2^{l_m} + w_{2,2} \prod_{m=3}^d 2^{l_m} + \cdots + w'_{u,2} \prod_{m=3}^d 2^{l_m} + \cdots + w_{d-1,2} 2^{l_d} + w_{d,2} \\ \vdots \\ w_{1,k} \prod_{m=2}^d 2^{l_m} + w_{2,k} \prod_{m=3}^d 2^{l_m} + \cdots + w'_{u,k} \prod_{m=3}^d 2^{l_m} + \cdots + w_{d-1,k} 2^{l_d} + w_{d,k} \end{pmatrix} \quad (3.1)$$

となる．展開してまとめると、

$$(3.1) = X' \begin{pmatrix} S_1 \prod_{m=2}^d 2^{l_m} + S_2 \prod_{m=3}^d 2^{l_m} + \cdots + S'_u \prod_{m=u+1}^d 2^{l_m} + \cdots + S_{d-1} 2^{l_d} + S_d \\ r_{1,1} \prod_{m=2}^d 2^{l_m} + r_{2,1} \prod_{m=3}^d 2^{l_m} + \cdots + r_{u,1} \prod_{m=u+1}^d 2^{l_m} + \cdots + r_{d-1,1} 2^{l_d} + r_{d,1} \\ \vdots \\ r_{1,k-1} \prod_{m=2}^d 2^{l_m} + r_{2,k-1} \prod_{m=3}^d 2^{l_m} + \cdots + r_{u,k-1} \prod_{m=u+1}^d 2^{l_m} + \cdots + r_{d-1,k-1} 2^{l_d} + r_{d,k-1} \end{pmatrix} \quad (3.2)$$

となる．式 (3.2) に X' の逆行列 X'^{-1} を左からかけると

$$X'^{-1} X' \begin{pmatrix} S_1 \prod_{m=2}^d 2^{l_m} + S_2 \prod_{m=3}^d 2^{l_m} + \cdots + S'_u \prod_{m=u+1}^d 2^{l_m} + \cdots + S_{d-1} 2^{l_d} + S_d \\ r_{1,1} \prod_{m=2}^d 2^{l_m} + r_{2,1} \prod_{m=3}^d 2^{l_m} + \cdots + r_{u,1} \prod_{m=u+1}^d 2^{l_m} + \cdots + r_{d-1,1} 2^{l_d} + r_{d,1} \\ \vdots \\ r_{1,k-1} \prod_{m=2}^d 2^{l_m} + r_{2,k-1} \prod_{m=3}^d 2^{l_m} + \cdots + r_{u,k-1} \prod_{m=u+1}^d 2^{l_m} + \cdots + r_{d-1,k-1} 2^{l_d} + r_{d,k-1} \end{pmatrix}$$

となり、 S の部分的なデータ S'

$$S' = S_1 \prod_{m=2}^d 2^{l_m} + S_2 \prod_{m=3}^d 2^{l_m} + \cdots + S'_u \prod_{m=u+1}^d 2^{l_m} + \cdots + S_{d-1} 2^{l_d} + S_d$$

を復元できる．以上の手順により部分更新を可能としている．

3.1 医療情報の部分更新

表 3.1 ADT^A08 を構成する各セグメント

セグメント名	説明	最大長
MSH	メッセージの目的, 発信源, 宛先, 特性を示す	1995
EVN	事象に関する事柄を示す	578
PID	患者の識別情報を示す	6017
NK1	患者の近親者に関する情報を示す	5911
PV1	病院内での患者の状態を示す	2973
DB1	患者の障害情報を示す	292
OBX	検査結果を示す	67009
AL1	患者のアレルギー情報を示す	780
IN1	患者の保険情報を示す	4732
合計		90287

3.1.2 部分更新による医療情報の削減率

本項では、部分更新による医療情報の削減率を示す。部分更新する医療情報に患者基本情報の更新メッセージ (ADT^A08) がある。MSH セグメントはメッセージそのものを示し、メッセージを作成した日付などが記されている。EVN セグメントは、その記録する事象が起きた日付や理由などを記し、PID セグメントは患者を識別するためのもので、患者の氏名や生年月日、住所が記されている。NK1 は患者の近親者を表すセグメントで、氏名、続柄、住所などが記されている。PV1 は病院内での患者の状態を表すセグメントで、外来患者なのか入院患者なのかや主治医が記されている。DB1 は身体障害の有無などが示されているセグメントである。OBX は検査項目や結果が記されているセグメントである。AL1 セグメントは患者のアレルギー情報が記されている。IN1 は患者の保険情報を示すセグメントで、患者の入っている保険会社やプランなどが示されている。ADT^A08 の各項目と最大長を表 3.1 に示す。ADT^A08 は各セグメントの最大長を合計すると 90287 になる。そのうち、医療情報が作成されるたびに必ず変化する項目は、MSH,EVN,OBX の項目である。

3.2 最新の医療情報の検索

表 3.2 ADT^A08 の更新されるたびに内容が変化する項目

セグメント名	説明	最大長
MSH	メッセージの目的, 発信源, 宛先, 特性を示す	1995
EVN	事象に関する事柄を示す	578
OBX	検査結果を示す	67009
合計		69582

ADT^A08 のうち, 更新されるたびに内容が必ず変化する項目のみまとめたものを表 3.2 に示す. 必ず内容に変更のある項目の最大長の合計は 69582 になる. したがって, 部分更新を行った場合の分散する際の処理量は最大 23%削減することができる.

3.2 最新の医療情報の検索

部分更新を行う際に最新のシェアをストレージから読み込む必要がある. ストレージではすべてシェアで保管されているが, その中から個人を特定し, 最も新しい同じ種類のデータを特定する必要がある. シェアの状態で個人を特定する方法として医療情報内の姓名やマイナンバーといった個人を識別できる情報を分散してタグとし, 医療情報を分散したシェアと保管する方法がある [14]. 検索の流れを図 3.2 に示す.

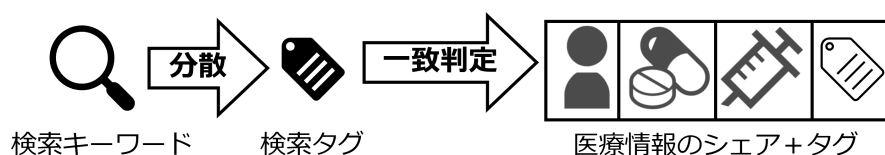


図 3.2 タグを用いた検索の流れ

3.2.1 部分復元可能な医療情報の検索

部分復元可能な秘密分散法には分散したデータを検索する仕組みはなく, 名前など患者を識別するための情報を部分的に復元してから検索する方法が考えられる, しかし, 復元は方

3.2 最新の医療情報の検索

程式を解くための逆行列の作成にかかる処理量が大きく時間を要することが想定されるため、素早い診療を行わなければならない災害時にはこの方法は適していない。そこで、安全性を落とすことなく検索にかかる計算量を削減できる方法として提案された。仕組みについて以下に述べる。

分散バックアップしたい医療情報に対応する識別情報を kw ($0 < kw$) とする。素数を p ($kw < p$ かつ $n < p$) とし、 $\mathbb{Z}/p\mathbb{Z} - \{0\}$ 上の集合を

$$x = \{x_1, x_2, \dots, x_n\} (i \neq j \text{ のとき } x_i \neq x_j)$$

とする。 p, x は医療情報を秘密分散した際とは異なる値にする。 x より

$$X = \begin{pmatrix} 1 & x_1 \\ 1 & x_2 \\ \vdots & \vdots \\ 1 & x_n \end{pmatrix} \pmod{p}$$

となるような行列 X を作成する。 kw と $\mathbb{Z}/p\mathbb{Z} - \{0\}$ 上の乱数 r から

$$\mathbf{A} = \begin{pmatrix} kw \\ r \end{pmatrix}$$

となるようなベクトル $\mathbf{A}$ を作成する。 p を法とする X と $\mathbf{A}$ の乗算より、

$$X\mathbf{A} = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix} \pmod{p}$$

となるようなタグ t_i ($i = 1, 2, \dots, n$) が得られる。タグを方程式で表すと

$$t_i \equiv kw + rx_i \pmod{p} \quad (3.3)$$

タグを医療データのシェアに対し2個ずつ付与する。

検索したいキーワードを kw' とする。 kw' と $\mathbb{Z}/p\mathbb{Z} - \{0\}$ 上の乱数 r' より、

$$\mathbf{A}' = \begin{pmatrix} kw' \\ r' \end{pmatrix}$$

3.2 最新の医療情報の検索

となるようなベクトル $\mathbf{A}'$ を作成する．分散段階で用いた行列 X と $\mathbf{A}'$ の p を法とした乗算より

$$X\mathbf{A}' = \begin{pmatrix} t'_1 \\ t'_2 \\ \vdots \\ t'_n \end{pmatrix} \pmod{p}$$

となるような検索タグ $t'_i (i = 1, 2, \dots, n)$ が得られる．方程式で表すと,

$$t_i \equiv kw + rx_i \pmod{p} \quad (3.4)$$

となる．ここで，タグ t_i と検索タグ t'_i の減算を行う．式 (3.3)(3.4) より,

$$t_i - t'_i \equiv (kw - kw') + (r - r')x_i \pmod{p} \quad (3.5)$$

となり，式 (3.5) の両辺に x_i の逆元 x_i^{-1} を掛けると，

$$(t_i - t'_i)x_i^{-1} \equiv (kw - kw')x_i^{-1} + (r - r') \pmod{p} \quad (3.6)$$

となる． $kw = kw'$ の場合，式 (3.6) より係数の差 $r - r'$ を正しく求めることができ，全ての i でこの結果は同じ値になる． $kw \neq kw'$ の場合，係数の差 $r - r'$ を正しく求めることができず，全ての i でこの結果が同じ値になることはない．これを利用して，シェアに付与した2つのタグの結果が等しくなることで検索を可能としている．

3.2.2 同じ種類の最新のシェアの検索

検索システムを用いることでシェアストレージから同じ患者を検索することが可能となった．SS-MIX2 では患者のファイルの中に日付毎に各ファイルに分かれており，さらにその中にデータの種類の分かれている．SS-MIX2 のファイル名にはデータを作成した日付が使われるが，シェアストレージも同様にファイル名にシェアを使った場合，シェアの特定に繋がり，情報漏えいにつながることから，ファイル名には無価値な文字列等を使用する．医療情報 MSH セグメントにはデータの種類の種類とそのデータを作成した日付が記載されているため，この項目のみを部分復元することで医療情報の検索が行うことが可能となる．また，作

3.3 まとめ

成した日付が分かることから、ある患者の過去一か月の投薬履歴を検索するといったことも可能である。したがって、医療情報の部分更新に最新のシェアを流用することが可能であるほか、災害時に診療を行う際に医療情報を必要な分だけ復元することで、リソースの圧迫を避けることが可能となる。

3.3 まとめ

医者が患者の診療を行う際、できる限り最新の医療情報があることが望まれる。しかし、災害時は電源やネットワーク等のリソースが不足することや、傷病者を含む診療を受ける人が増加することによって作成される医療情報も増加し、バックアップする量が増加することによってリソースを圧迫することが想定される。そこで、災害時のリソースの圧迫を避け、分散の処理量を削減させることを目的として、部分更新と最新のシェアの検索方法について提案した。提案方法は、医療情報を意味のある項目ごとに分けたもののうち、前回と内容に変更のない項目は前回のシェアを流用し、変更のあった項目は秘密分散を行い、シェアを作成することで分散の処理量を削減している。最新のシェアの検索には、ストレージの中から個人を絞り込み、該当する個人のシェアのうち、医療情報の作成日時とデータの種類が記されている項目のみを部分的に復元することで最新のシェアの検索を可能としている。

本章では、部分更新の仕組みについて述べ、それが数学的に可能であることを示し、部分更新によって削減可能なデータ量について述べたあと、最新のシェアを検索する方法について述べた。

第 4 章

災害時に更新・利用可能な秘密分散 バックアップシステム

通常病院等の医療施設がバックアップを行う際、平穏期であるため、ネットワークや電源等のリソース不足に悩まされることなく、安定かつ安全なバックアップを行うことが可能である。しかし、診療録のバックアップは災害急性期の不安定なリソースの中も行う必要がある。

本章では災害急性期に医療情報の更新・利用が可能な秘密分散バックアップシステムの構成とその評価について述べる。

4.1 システムの構成要素

分散バックアップシステムの構成を提案するために必要な扱うデータと想定する利用者について述べ、分散バックアップシステムの構成に必要なデバイスについて述べる。

4.1.1 分散バックアップシステムで扱うデータ

提案手法である分散バックアップシステムでは最新のシェアを扱う際に検索と部分復元を行う。そのため、分散段階、検索段階、復元段階の 3 つの段階でそれぞれ扱うデータについて表 4.1 に示す。

当システムでは、医療情報 S 、変更のあった項目を S'_i とし、医療情報を (k, n) 秘密分散して生成される無意味な情報をシェア w_i とする。部分復元を行うためのシェアの紐付け情報

4.1 システムの構成要素

表 4.1 各段階で扱うデータ

段階	データの種類
分散段階	S'_i w_i x_{med} p_{med} r_{med} kw t_i x_{tag} p_{tag} r_{tag} U k n
検索段階	kw' t'_i x_{tag} p_{tag} r_{tag} t_i
復元段階	S w_i x_{med} p_{med} r_{med} U k

を U 医療情報を秘密分散する際に使用する集合 X を x_{med} , 素数 p を p_{med} , 乱数 r を r_{med} とする. 電子カルテの氏名やマイナンバーといった個人を特定できる情報を識別情報 kw とする. 識別情報 kw を秘密分散して生成される無意味な情報をタグ t_i とする. 医療情報を検索する際に入力する情報を検索キーワード kw' とする. 検索キーワード kw' を秘密分散して生成される無意味な情報を検索タグ t'_i とする. 識別情報と検索キーワードを秘密分散する際に使用する共通の集合 X を x_{tag} , 共通の素数 p を p_{tag} とする. 識別情報を秘密分散する際に使用する乱数 r を r_{tag} とし, 検索キーワードを秘密分散する際に使用する乱数 r を r' とする. それぞれのデータの説明を表 4.2 に示す.

4.1.2 想定される利用者

分散バックアップを行うとき, 医療情報をみる必要があることから, 医療従事者である必要がある. そのため提案システムを利用する人物は医療従事者とし, それ以外の人物はその他の人物とする. その他の人物には悪意をもった攻撃者や利用権限のない人物も含まれる. その他の人物が分散システムを利用することができた場合, 医療情報ではないデータを分散したり, プライバシーなデータを検索し, 閲覧することが出来てしまう. そのため, その他の人物がいかなる操作もできないようにする必要がある.

4.1 システムの構成要素

表 4.2 扱うデータの説明

データ名	データの説明
S	患者の医療情報. 標準化された電子カルテを想定
S'_i	医療情報の変更のあった項目
w_i	医療情報を秘密分散して生成される無意味な情報
x_{med}	医療情報を秘密分散する際に用いる集合 X
p_{med}	医療情報を秘密分散する際に用いる素数 p
r_{med}	医療情報を秘密分散する際に用いる乱数 r
kw	識別情報. 氏名やマイナンバーを想定
t_i	識別情報を秘密分散して生成される無意味な情報
kw'	検索キーワード. 医療情報の検索じに入力する
x_{tag}	識別情報と検索キーワードを秘密分散する際に用いる共通の集合 X
p_{tag}	識別情報と検索キーワードを秘密分散する際に用いる共通の素数 p
r_{tag}	識別情報を秘密分散する際に用いる乱数 r
r'	検索キーワードを秘密分散する際に用いる乱数 r

4.1.3 分散システムの構成デバイス

災害時に患者を前にした医師が診療を行う際に用いる医療情報を閲覧, 書き込み, 検索を行う端末が必要となる. この端末を医師端末とする. バックアップしたデータを復元した医療情報や更新予定の医療情報を保持しておく端末が必要となる. この端末を情報端末とする. シェアを格納するストレージ群と, 検索, 分散, 復元の処理を実際に行うリファレンスモニタが必要になる.

4.1 システムの構成要素

4.1.4 構成デバイス間での盗聴のリスク

部分更新を行うとき、まず情報端末から更新予定の医療情報 S' をリファレンスモニタに送信する。最新のシェアを検索するため、ストレージ群から、タグ t_i を用いて検索し、該当する患者のデータから MSH セグメントを分散したシェア w_i, x_i を復元し、最新のシェアを検索する。見つけた最新の w_i, x_i, U, t_i をリファレンスモニタに送信し、分散する。作り直した紐付け情報とともにシェアストレージに保管する。部分更新時のデバイス間のデータの動きを図 4.1 に示す。また、検索時は、情報端末からリファレンスモニタに検索キーワード

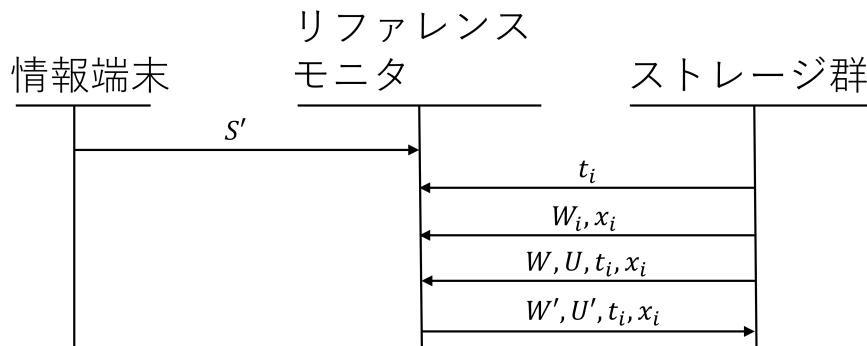


図 4.1 部分更新時のデータの動き

kw' を送信し、ストレージ群からタグ t_i を用いて検索し、該当する患者のデータから w_i, x_i を復元し、任意のシェアを検索する。シェアストレージから該当する w_i, x_i, U, t_i をリファレンスモニタに送信し、診療に最低限必要な情報で部分復元する。部分復元した医療情報を情報端末に送信することで、医療情報を閲覧することができる。検索時のデバイス間のデータの動きを図 4.2 に示す。

部分更新時、検索時両段階での通信路は情報端末とリファレンスモニタ間、リファレンスモニタとサーバ群間ともに、医療情報やタグといった盗聴された際に情報漏えいに繋がるデータを送受信している。したがって、各通信経路は盗聴を防ぐために秘匿化をする必要がある。

4.2 システム構成

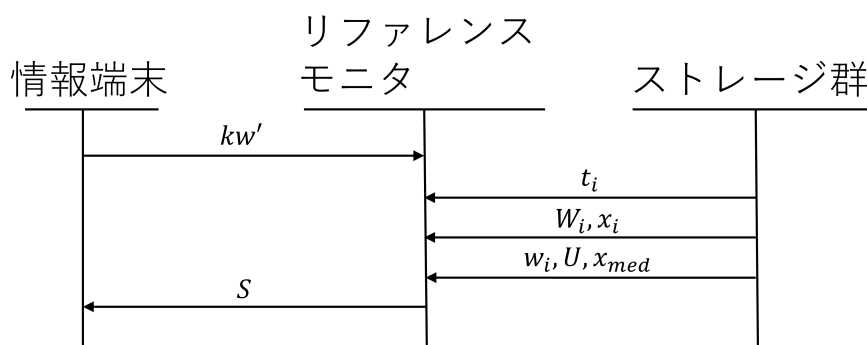


図 4.2 検索時のデータの動き

4.2 システム構成

利用者は情報端末を用いてリファレンスモニタにアクセスし、医療情報の更新があった項目のみを送信する。リファレンスモニタはバックアップする情報の最新のシェアを検索し、シェアを取得する。更新予定の項目をリファレンスモニタで分散させ、取得したシェアと紐付け情報を作成し、ストレージ群に保管する。以上の手順により提案システムでは最新の医療情報のバックアップを更新することができる。システム構成を図 4.3 に示す。

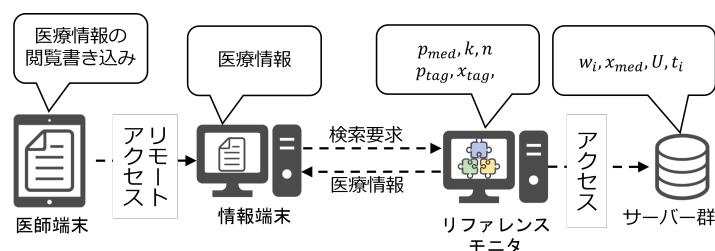


図 4.3 分散バックアップシステムの構成

4.2.1 医師端末

医師端末は医療従事者が被災地で患者を診療する際に閲覧・書き込みを行うため、携帯が可能な端末とする。携帯が容易な端末は盗難のリスクがあるため、内部になんの情報も保持せず、情報端末へのリモートアクセスを行い医療情報の閲覧・書き込みを行う。医師端末を利用する際に利用者が正当であることを照合し、認証され情報端末へリモートアクセスする際

4.2 システム構成

にも医師端末そのものになりすましなどなく，正当であるかを確認するし，認証された場合のみリモートアクセスを許可する．情報端末への接続の流れを図 4.4 に示す．

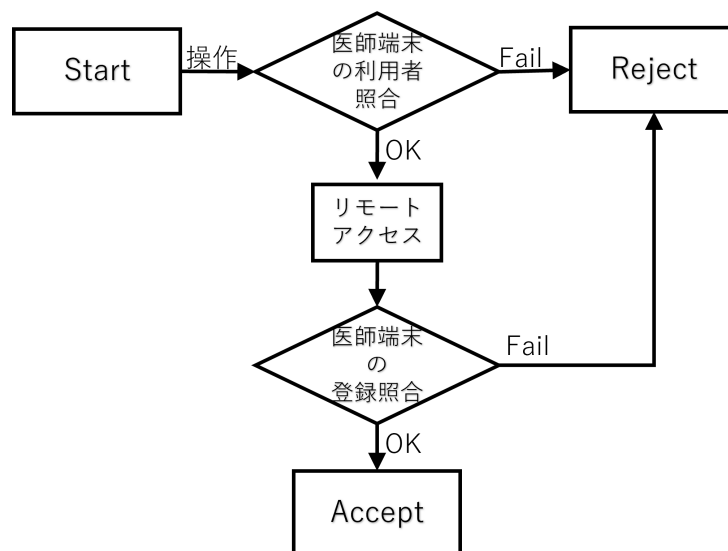


図 4.4 情報端末へのリモートアクセスの流れ

4.2.2 情報端末

医療従事者ではないその他の人物に自由な利用を許す場合，リファレンスモニタにアクセスし，不正な情報を分散させる可能性がある．そのため，情報端末を使用する際には利用者認証を行う必要がある．また，リファレンスモニタへ更新予定の情報を送信する際には，情報端末が正当であるかの確認が必要である．実現方法として，事前に登録しておいたパスワードや生体認証を用いて利用者の認証を行い，リファレンスモニタにあらかじめ情報端末が正当であるかを確認する認証情報を持たせておく．リファレンスモニタへの接続の流れを図 4.5 に示す．また，情報端末を医療施設内のアクセス管理が可能な場所に設置することで端末自体の安全性を確保する．

4.2 システム構成

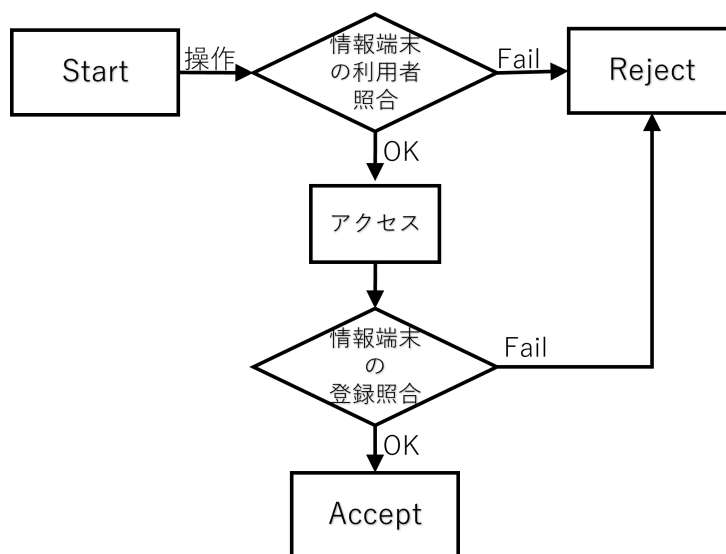


図 4.5 リファレンスモニタへの接続の流れ

4.2.3 リファレンスモニタ

ストレージへのアクセスが自由に出来た場合、医療情報を不正に復元される恐れがある。そのため、ストレージへのアクセスをリファレンスモニタに限定し、リファレンスモニタで医療情報の分散や検索、復元を行う。分散や検索処理は災害の発生していない平穏期や災害急性期であっても同様の処理速度が求められるが、医療施設が被災し、端末が機能しなくなることがあってはならないため、ストレージ群と同様、遠方の同時に被災することがない場所への設置する。リファレンスモニタの設置場所を図 4.6 に示す。

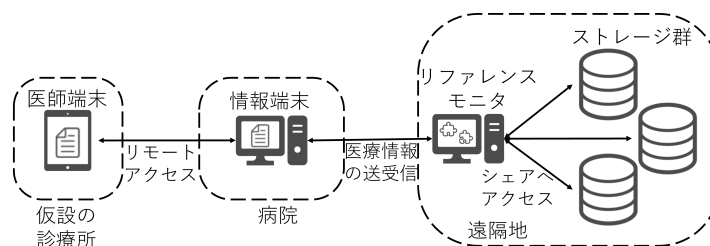


図 4.6 リファレンスモニタの設置場所

4.3 評価

4.2.4 ストレージ群

ストレージ群では医療情報の検索・復元に必要な w_i, x_{med}, t_i を保持しているため、アクセスできる端末を制限する必要がある。そのため、アクセスできる端末をリファレンスモニタに制限し、アクセスしてきた端末の照合を行う。実際には、事前に正当なリファレンスモニタを登録しておき、リファレンスモニタの照合を行う。ストレージ群への接続の流れを図4.7に示す。また、ストレージ本体の被災や攻撃から守る必要があるため、遠方の医療機関などのアクセス管理が可能な場所に設置する。

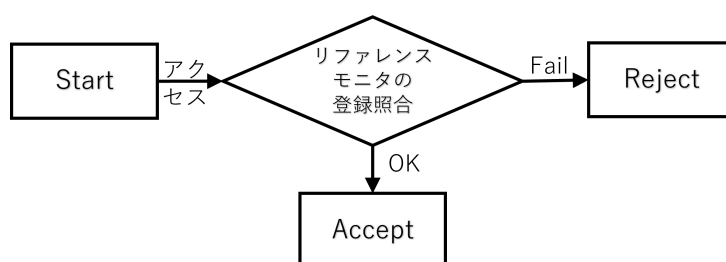


図 4.7 ストレージ群への接続の流れ

4.3 評価

提案システムに対して、考えられる不正は、情報端末のなりすましによるリファレンスモニタへのアクセスや、リファレンスモニタのなりすましによるストレージ群へのアクセス、システムのデバイス間での通信路での傍受がある。情報端末のなりすましによってリファレンスモニタへアクセスされた場合、リファレンスモニタ側で利用者照合が行われるため、不正な操作を行うことはできない。また、ストレージ群にアクセスすることが可能であっても、検索システムの提案手法により、医療情報のシェアの組み合わせはわからず、タグからも医療情報のシェアの組み合わせが判明することはないため、不正に復元されることはない。通信の傍受は、専有型回線を用いると被災時に回線が切断しバックアップシステムを利用できない事態に陥る可能性が存在するため、共有型回線を用いる。共有型回線では通信が傍受される可能性があるため、通信を秘匿化しデータを送受信することでデータを傍受されること

4.4 まとめ

を防止する。しかし、秘匿化の際に使用するネットワーク機器がマルウェア等に感染することで情報漏えいが発生するといったことがある [15]。インターネットを介して通信を行う場合、これらが想定されるが、災害時には簡易迅速な手続きで、情報共有が行わなければならないことから、人命救助を優先し、インターネットを介した通信を行う [16]。

4.4 まとめ

本章では、災害急性期に医療情報の更新・利用が可能な秘密分散バックアップシステムの構成要素について述べ、提案システムの構成について述べた。バックアップシステムの構成では、各端末の不正なアクセスを防止するべく、それぞれの端末を登録し、照合に成功した場合のみ通信を行う。また、被災によってリファレンスモニタが消失すること及び、処理能力が低下することを防ぐため、リファレンスモニタをストレージと同様遠方に設置し、 $p_{med}, p_{tag}, x_{tag}$ を保持することとした。また、各通信にインターネットを介して行うため秘匿化が必要であるが、秘匿を行うネットワーク機器がマルウェア等に感染することによる情報漏えいが想定されるが、災害時には個人情報の保護よりも個人の生命を優先することが求められていることから、インターネットを介した通信を行うことを述べた。

第 5 章

結論

5.1 本研究のまとめ

本研究では、医療情報の分散バックアップを行う際、災害時の不足しているリソースの圧迫を避け、分散の処理量を削減させることを目的として医療情報の部分更新を提案した。また、部分更新にはストレージに保存されている最新のシェアが必要であることから、最新のシェアを検索する方法についても提案した。

医療情報の変更部分のみを更新する方法は、部分復元用に意味のある項目ごとに分けられたシェアのうち、前回の内容と変化がない項目は流用し、更新された項目のシェアのみを新しく作成することで、秘密分散する際の処理量の削減を可能としている。最最新のシェアの検索には、ストレージ内のシェアを個人まで絞った後に、データの種類と日付が記載されている項目のみを部分復元することで可能としている。

検索システムの構成では、各端末の不正なアクセスを防止するべく、それぞれの端末を登録し、照合に成功した場合のみ通信を行う。また、リファレンスモニタが被災し消失することで分散や検索、復元の処理に影響を及ぼすことを防ぐため、リファレンスモニタを遠方へ設置することとした。災害時の想定から専有型回線で通信を行わず、インターネットを介した通信を行うため、通信を秘匿化するが、ネットワーク機器のマルウェア感染による情報漏えいの危険性は残る。しかし、災害時には個人情報の保護よりも人命救助を優先することが求められていることから、インターネットを介した通信を提案システムでは行う。

5.2 今後の課題

ネットワークを介した場合の処理時間などを明らかにするため、実際にシステムを作成し、実験する必要がある。また、最新のシェアの検索において部分復元を行うことと、タグを付与する方法のどちらが適切かなどを、処理速度やデータ量の観点から調べる必要がある。

謝辞

本研究を行うにあたり、ご指導いただきました高知工科大学情報学群の福本昌弘教授に謹んで感謝致します。同じ過ちを繰り返す私に対して、何度もご教示して頂き大変感謝しています。本研究の副査をしてくださいました情報学群敷田幹文教授、原田崇司講師ご兩人にも謹んで感謝致します。原田先生には本読み会にてお世話になり、なানাあで学んだ気になっていた線形代数を一から理解することができました。また、研究室に持ってきていただいたお土産やお菓子は小腹がすいたときにとてもありがたくおいしかったです。

NOC の職員であり、福本研究室の OB でもある福富英次氏にも謹んで感謝致します。本読み会では理解の及ばないところを分かりやすく解説していただいたり、お食事にもたくさん連れて行ってくださいました。

研究室の同期である西岡秀大氏にも感謝します。同期が飛んでいくなかで生き残る様はとても心強く、勇気をいただきました。

福本研究室 3 年生のみなさん、あまりにも頼りない先輩で申し訳なかったです。これからどうなるかわかりませんが、おそらくなんとかなると思います。頑張ってください。

最後に、高知工科大学で過ごした 4 年間を支えてくださったすべての方に感謝致します。

参考文献

- [1] 高知県医療情報通信技術連絡協議会, ”南海トラフ大地震から診療情報を守れ”, https://www.soumu.go.jp/main_content/000317692.pdf, 2022 年 3 月 2 日閲覧.
- [2] 厚生労働省, ”医療情報システムの安全管理に関するガイドライン 第 5 版”, <https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu-Shakaihoshoutantou/0000166260.pdf>, pp.94-112, 2021 年 2 月 12 日閲覧.
- [3] 経済産業省, ”医療情報を受託管理する情報処理事業者向けガイドライン第 2 版”, https://www.meti.go.jp/policy/it_policy/privacy/iryoughlv2.pdf, 2022 年 3 月 3 日閲覧,
- [4] 総務省, ”クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン第 1 版”, 2022 年 3 月 3 日閲覧,
- [5] 木村映善, 松村泰志, 三原直樹, 黒田知宏, 山下芳範, 平松治彦, 真鍋史朗, 田中大介, 佐藤敦, 山倉直, ”医療サービスの継続性を担保する電子カルテ秘密分散バックアップ技術の研究開発”, ICT いのべセッションフォーラム 2015 予稿集, 総務省, pp144-145, Oct.2015.
- [6] 福本昌弘, “高知県における電子カルテ遠隔バックアップと部分復元可能な秘密分散法”, 北隆館, Precision Medicine, pp. 57-61, Vol. 3, No. 9, 2020.
- [7] 高知県医療 ICT 連絡協議会, ”高知県医療 ICT 連絡協議会 背景と目的”, <https://kmict-lc.com/page-60/>, 2022 年 3 月 3 日閲覧.
- [8] 一般社団法人高知県保健医療介護福祉推進協議会, ”高知あんしんネットとは”, <http://kochi-anshinnet.kmict-lc.com/about/>, 2022 年 3 月 3 日閲覧.
- [9] 高知工科大学, ”秘密分散と秘匿通信技術を用いた電子カルテ保管・交換システムを開発～南海トラフ地震等の災害想定実験において、

参考文献

- 医療データを迅速に復元～”, https://www.kochi-tech.ac.jp/news/img/aab8c54c17048e7fd1e398230a789946_1.pdf, 2022 年 3 月 3 日閲覧.
- [10] 中村巴, 吉富亮平, 福富英次, 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検索とその安全性評価”, 信学技報 vol.120 no.356 IA2020-34 pp.21-26, Jan.2020.
- [11] 田中麻実, 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システム”, 信学技報 vol.116 no.362 IA2016-70 pp.41-46 Dec.2016.
- [12] 田中麻実, 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 vol.115 no.371 IA2015-74, pp.31-36, Dec.2015.
- [13] 清水俊郎, ”SS-MIX2 の概要”, http://www.jhit.jp/kanto_g01/6th20120908r.pdf, 2022 年 2 月 12 日閲覧.
- [14] 中村巴, 福富英次, 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”, SCIS2020, 3C1-4, 2020.
- [15] 株式会社 F F R I セキュリティ, ”VPN 脆弱性とマルウェアの直近の状況”, https://www.soumu.go.jp/main_content/000722474.pdf, pp.2, 2022 年 2 月 22 日閲覧.
- [16] 日本弁護士連合会, ”災害時における要援護者の個人情報提供・共有に関するガイドライン”, https://www.nichibenren.or.jp/library/pdf/activity/human/aged_shien/saigaiji_gaidorain.pdf, pp.4-6, 2022 年 2 月 22 日閲覧.