平成 28 年度

修士学位論文

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とその安全性評価

Confined Decoding System for Medical Data Distributed by Secret Sharing Scheme and Its Security Evaluation

1195046　　田中麻実

指導教員　　福本昌弘

2017 年 3 月 6 日

高知工科大学大学院 工学研究科 基盤工学専攻

情報システム工学コース

要 旨

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とその安全性評価

田中麻実

東日本大震災の津波によって電子カルテが損失したことにより，被災地での医療行為に支障が出た．これを受けて高知県の病院では電子カルテを遠隔地にバックアップする取り組みが始められている．さらに遠隔地にバックアップした電子カルテを災害時の医療行為に活用することが期待されている．医療データは個人情報であるため，災害時の医療行為に必要な情報のみを提供する必要がある．そこで，バックアップデータから必要な情報のみを復元する秘密分散法を用いた部分復元アルゴリズムを提案した．提案した部分復元アルゴリズムは，部分復元に必要な情報が第三者に入手されると不正復元される可能性がある．

本論文では不正復元を防いだ部分復元可能な秘密分散システムを提案している．提案システムでは部分復元を行うための情報を必要とする．その情報を用いることによって必要最低限の患者の情報を DMAT に提供することができる．しかし，部分復元に必要な情報が第三者に入手された場合不正復元される可能性があるため，不正入手を防ぐ要件を定義している．要件を満たす対策を施すことによって，安全に医療データの部分復元を行うことができる．

キーワード　分散バックアップ，秘密分散法，部分復元

Abstract

Confined Decoding System for Medical Data Distributed by Secret Sharing Scheme and Its Security Evaluation

Asami TANAKA

The medical treatment in the area affected of disaster was difficult because medical data lost in the tsunami of great east japan earthquake. In order to prevent medical data from being lost, the hospitals in Kochi have started the remote backup plan. Moreover, by providing the required information of treating victims from backup data such as name, blood type and medicine information, Disaster Medical Assistance Team (DMAT) can treat victims outside the hospital at the acute stage of disasters. Because medical data is personal information, it is necessary to provide the minimum required patient information. The restoration method has been proposed to confine more decoding data than necessary decoding data. In order to provide the patient information, the proposed method owns the decoding control information. However, it is possible to illegally decode in case the leaked the decoding control information.

In this paper, the restoration structure to prevent from illegal decoding has been proposed. To prevent from illegal decoding, the structure control information has been defined to prohibit the decoding control information leakage. In addition, the requirement has been defined to prevent the structure control information from being leaked. The experimental results suggested that it is possible to prevent from illegal decoding by satisfying the requirements.

key words distributed backup, secret sharing scheme, confied decodning

目次

第 1 章　はじめに　1

1.1　本研究の背景と目的 1

1.2　本論文の構成 1

第 2 章　医療データの分散バックアップと被災地での医療データ活用　2

2.1　バックアップ対象の医療データ 3

2.1.1　電子カルテ 3

2.1.2　SS-MIX(Standardized Structured Medical Information eXchange)　4

2.2　医療データのバックアップの条件 6

2.3　(k, n) しきい値秘密分散 7

2.4　部分復元アルゴリズム 11

2.4.1　分散段階 12

2.4.2　復元段階 13

2.4.3　部分復元の手順 13

2.5　(k, n) しきい値秘密分散法と部分復元アルゴリズムの比較 16

2.6　まとめ 17

第 3 章　部分復元可能な秘密分散システム　19

3.1　高知県のバックアップした医療データの活用計画 19

3.2　部分復元アルゴリズムを用いた部分復元可能な秘密分散システムに対する要件 20

3.3　部分復元アルゴリズムを用いた部分復元可能な秘密分散システムの構成 . . 21

3.4　部分復元アルゴリズムを用いた部分復元可能な秘密分散システム 23

3.5　部分復元可能な秘密分散システムの問題と不正復元を防ぐ要件の定義 . . . 29

3.5.1 情報源と復元 PC 間のデータのやりとり 31
3.5.2 情報源からシェアストレージ群へのデータのやり取り 38
3.5.3 復元 PC とシェアストレージ群間のデータのやり取り 41
3.5.4 復元 PC と情報閲覧端末間のデータのやり取り 47
3.6 まとめ 50

第 4 章 不正復元を防ぐ部分復元可能な秘密分散システムの評価 52

4.1 部分復元可能な秘密分散システムの評価 52
4.2 不正復元を防ぐ要件の評価 53
4.2.1 情報源と復元 PC 間の要件の評価 53
4.2.2 情報源とシェアストレージ群間の要件の評価 54
4.2.3 復元 PC とシェアストレージ群間の要件の評価 55
4.2.4 復元 PC と情報閲覧端末間の要件の評価 57
4.2.5 実証実験 57
4.3 不正復元を防ぐ要件を満たした理想的なシステムの考察 59

第 5 章 まとめ 62

5.1 本研究のまとめ 62
5.2 今後の課題 63

謝辞 64

参考文献 65

図目次

2.1 SS-MIX のディレクトリ構造 5
2.2 標準化された患者データ例 5
2.3 (k, n) しきい値秘密分散法を用いた SS-MIX 形式の電子カルテのバックアップ 8
2.4 (k, n) しきい値秘密分散法のデータの流れ 8
2.5 部分復元アルゴリズムを用いた SS-MIX 形式の電子カルテのバックアップ . 11
2.6 SS-MIX 形式の電子カルテデータの分割 12
2.7 部分復元アルゴリズムのデータの流れ 13

3.1 バックアップした医療データの活用計画 20
3.2 医療データの部分復元システムの構成 (分散) 22
3.3 医療データの部分復元システムの構成 (復元) 23
3.4 提案システムで扱うデータの一覧 24
3.5 分散スクリプトの処理 24
3.6 分散時のデータの流れ 27
3.7 復元時のデータの流れ 28
3.8 情報源と復元 PC 間でやりとりされるデータ 31
3.9 復元 PC に事前情報を配付する際に洩れる条件 34
3.10 情報源から復元 PC に事前情報を配付する際の状態遷移 35
3.11 平常時に復元 PC を設置できない場所に対して事前情報を配付する際の状態遷移 35
3.12 災害時にクラウド上の復元 PC から事前情報を入手する際の状態遷移 36
3.13 復元 PC の操作権取得の状態遷移 36
3.14 正当な拠点が事前情報を受け取れる条件 37
3.15 拠点・端末・操作者を登録する際の状態遷移 38

3.16 情報源とシェアストレージ群でやりとりされるデータ 38
3.17 情報源からシェアストレージ群のやりとりでデータが洩れる条件 39
3.18 ストレージをシェアストレージとして登録する際の状態遷移 40
3.19 情報源とシェアストレージが通信する際の状態遷移 40
3.20 復元 PC とシェアストレージ群間でやりとりされるデータ 41
3.21 緊急用時に設置される緊急用シェアストレージ 41
3.22 復元 PC とシェアストレージ群間でシェアが洩れる条件 43
3.23 シェアストレージが復元 PC にシェアを配付する際の状態遷移 45
3.24 災害時医療データを使用する拠点に緊急用のシェアストレージを設置する際の状態遷移 45
3.25 災害時医療データをしない拠点にシェアストレージ群の情報 (災害) を教える際の状態遷移 46
3.26 災害時医療データを使用する拠点に緊急用のシェアストレージを設置する際の状態遷移 46
3.27 災害時医療データを使用しない拠点を緊急用のシェアストレージを設置する拠点に登録する際の状態遷移 47
3.28 復元 PC と情報閲覧端末で流れるデータ 48
3.29 復元 PC から情報閲覧端末間でデータが洩れる条件 48
3.30 復元 PC から情報閲覧端末に事前情報を配付する際の状態遷移 49
3.31 情報閲覧端末に医療データを配付する際の状態遷移 50

4.1 情報源と復元 PC 間のデータのやりとりに対する要件を満たす具体的な対策 54
4.2 情報源とシェアストレージ群間のデータのやりとりに対する要件を満たす具体的な対策 55
4.3 復元 PC とシェアストレージ群間のデータのやりとりに対する要件を満たす具体的な対策 56

4.4 復元 PC と情報閲覧端末間のデータのやりとりに対する要件を満たす具体的な対策 57
4.5 要件を満たす具体的な対策のシステム構成 58
4.6 災害時に使用する認証情報を外部に保存し活用 60

表目次

3.1 洩れるデータの分類 30

4.1 実証実験環境 58

第 1 章

はじめに

1.1　本研究の背景と目的

東日本大震災の津波によって電子カルテが損失したことにより，被災地での医療行為に支障が出た [1]．これをうけて高知県の病院では電子カルテを遠隔地にバックアップする取り組みが始められている [2]．さらに遠隔地にバックアップした電子カルテを災害時の医療行為に活用することが期待されている．医療データは個人情報であるため，災害時の医療行為に必要な情報のみを提供する必要がある．そこで，バックアップデータから必要な情報のみを復元する秘密分散法を用いた部分復元アルゴリズムを提案した．提案した部分復元アルゴリズムは，部分復元に必要なデータが第三者に入手されると不正に復元される可能性がある．本研究では，秘密分散法を用いて分散バックアップした医療データを部分的に復元可能な秘密分散システムを提案し，提案システムに対する脅威を防ぐ要件を定義する．

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，医療データの分散バックアップについて述べたあと，部分復元アルゴリズムについて述べる．3 章では，部分復元アルゴリズムを用いた，部分復元可能な秘密分散システムを提案する．さらに提案システムの問題点を整理し，不正復元を防ぐ要件を定義する．4 章では，提案システムと不正復元を防ぐ要件を定義し，不正復元を防ぐ要件を満たす理想的なシステムを考察する．5 章では，本研究をまとめ，今後の課題を述べる．

第 2 章

医療データの分散バックアップと被災地での医療データ活用

東日本大震災の際に発生した津波によって，岩手県の沿岸部にある病院に保管されていた電子カルテを含む医療データが流出し，被災地での医療行為に支障がでた [1]．これを受けて，高知県の病院では広域災害に備えて電子カルテをまとめて遠隔地にバックアップする取り組みが開始された [2]．また，愛媛大学を中心とした研究グループでは，電子カルテの分散バックアップに秘密分散法を用いる研究がなされている [3]．

災害時には負傷者が増える上に，被災地域の病院設備が麻痺していることが想定されるため，被災地域の病院のみでは負傷者を捌くことは困難である．そのため，被災地域外から医師が被災地域に入り，被災地での医療行為の手助けを行う．その際，被災地域外から来た医師が診察している患者の投薬履歴があれば，より良い治療を行うことができると言われている [1]．しかし，医療データは個人情報であるため，被災地域外から来た医師に対して診療の診察に不必要なデータの提供を制限する必要がある．よって，バックアップデータから部分的な情報のみを提供可能な分散バックアップ方法が必要になる．

本章では，バックアップデータから部分的なデータを抜きだし，提供可能な分散バックアップ方法述べる．まずバックアップの対象である医療データについて述べ，医療データをバックアップして被災地で活用するために満たすべき条件について述べる．次に秘密分散法で代表的な (k, n) しきい値秘密分散法について述べ，(k, n) しきい値秘密分散法を用いた部分復元アルゴリズムについて述べる．最後に医療データの分散バックアップに (k, n) 秘密分

散法を用いる方法，部分復元アルゴリズムを用いる方法を比較し，部分復元アルゴリズムを評価する．

2.1　バックアップ対象の医療データ

医療データには様々な種類があるが，今回対象とする電子カルテについて述べる．まず，電子カルテについて述べ，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-MIX: Standardized Structured Medical Information eXchange) について述べる．

2.1.1　電子カルテ

電子カルテとは，医師が患者を診察した際に必ず作成しなければならない診療録を電子化し，電子情報としてカルテを編集，管理するシステムや仕組みのことを指す．診療録を電子化して保存しているため，カルテの物理的な管理が必要なくなり，紛失のリスクや保管場所の確保をしなくてもよい．また，電子情報であるため，病院のネットワークがつながっているかつ閲覧権限があれば，どこでもカルテ情報を閲覧することができる．さらに，バックアップを容易に行うことができ，自然災害による診療録の紛失を防ぐことができる．しかし，電子媒体であるため，端末がウィルスに感染していたり，不正アクセスによる情報漏洩などの危険性に晒される可能性があるため，第三者からの攻撃に対する対策が必要になる．

診療録は医師法第 24 条 2 項に最低 5 年間は保存することが義務付けられている [4]．1999 年以前はカルテの保存には紙媒体でなければならなかったが，1999 年に厚生労働省が「診察録の電子媒体による保存について」を通知し，診療録電子保存の三原則を満たしている場合のみ，診療録の電子保存が可能になった [4]．診察録電子保存の三原則とは，真正性，見読性，保存性である．これらは，電子化した診療録を日常の診察などに支障なく活用することが担保されていなければならないことや，診療録の内容が正確であることが保証されていなければならないことから定められた．真正性，見読性，保存性のそれぞれの詳細を以下に示す．

真正性

真正性とは，医師が作成した診療録に対して，嘘の情報や医師以外の人間による書き換え，診療録の消去および，診療録の取り違えなどの混同が防止されており，かつ第三者から見て診療録の作成の責任の所在が明確であることである．ネットワークを用いて外部に保存する場合は，診療録を保存先に配付中に診療録の内容の書き換えや消去，他の情報との混同が起きないようにしなければならない．

見読性

見読性とは，電子カルテの内容を診察などの活用方法に支障がない応答時間や操作方法であり，肉眼で見読可能な状態にできることである．よって，電子カルテシステムに何らかのシステム障害が発生した場合，診察に支障がない最低限の見読性を確保する必要がある．ネットワークを用いて外部に保存する場合は，保存先の事情により見読性が損なわれることを考慮しておく必要がある．

保存性

保存性とは，電子化された診療録が法的に定められた期間の間，真正性を保ち見読可能状態に保存しておくことである．

以上 3 原則を守ることで診療録を電子化することができる．

2.1.2 SS-MIX(Standardized Structured Medical Information eXchange)

電子カルテは様々なベンダーによって実装され，それぞれ異なるフォーマットを作成しているため，互換性がなく標準規約も定まっていない．よって，各病院で電子カルテの情報を共有し地域医療に活用しようとしても困難であった．そこで厚生労働省は，病院などの医療機関間での医療データの交換，共有を行うことによって医療の質の向上を目的として，電子カルテの標準化ストレージである SS-MIX を「厚生労働省電子的診療情報交換推進事業」において策定した [5]．SS-MIX は各病院の電子カルテを HIS(Hospital Information System)

2.1　バックアップ対象の医療データ

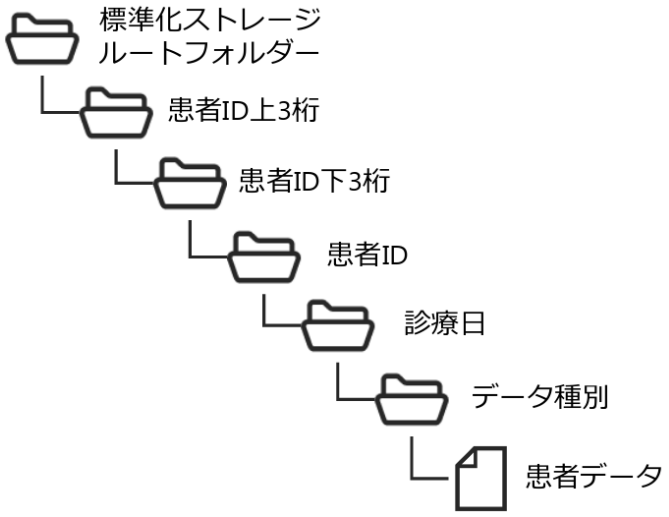

図 2.1　SS-MIX のディレクトリ構造

```
MSH|^~\&|EGMAIN-GX|HIS|GW|GW|20141030195548.2901||OMP^O09|20141030195548659|P|2.5|
    |||||~ISO IR87||ISO 2022-1994
ZGW|9930000036|20141030195530|OMP-01^処方オーダ^L|14X303511256100|INS|01^総合診療科^L
SFT|Fujitsu Ltd.^D|V2|EGMAIN-GX
PID|0001||9930000036||ﾃｽﾄ^ﾃｽﾄ^^^^^L^I~ﾃｽﾄ^ﾃｽﾄ^^^^^L^P||19750505|M|||39|||||||||
    ||||||||N|||20130730150300|
ORC|NW|14X303511256100||1|||||20141030195536|KEN00100^検証^医師^^^^^^^L^^^^^I~ｹﾝｼｮｳ
    ^ｲｼ^^^^^^^L^^^^^P||KEN00100^検証^医師^^^^^^^L^^^^^I~ｹﾝｼｮｳ^ｲｼ^^^^^^^L^^^^^P
    |01^^^^^C||||01^総合診療科^L|MC20050D^^L||||||||||O^外来患者オーダ^HL7-0482
TQ1|0001|1^日分|&&&&1日1回 起床時|||1^日分|2014103000
RXO|^タンナルビン末^MDCHOT^I1001390^タンナルビン末^L|1||G^グラム^MR9P^G^g^L
    |PWD^散剤､ドライシロップ剤^MR9P|TOC^OHP^MR9P^^外来処方~TOC^OHO^MR9P^^院外処方|||||1
    |G^グラム^MR9P^G^g^L||||Y|||||||1^G&グラム&MR9P&G&g&L
RXR|PO^口^HL7-0162
```

図 2.2　標準化された患者データ例

情報ゲートウェイで変換し，標準化ストレージに格納する．医療データを交換する際は，標準化ストレージのデータを CD に書き出し他の医療機関に渡すことで，他の医療機関で医療データを閲覧することができる．標準化ストレージはディレクトリ形式を用いている．ディレクトリ構造を図 2.1 に示す．

SS-MIX のディレクトリ構造は，各医療機関用のルートフォルダーを置き患者の ID によってディレクトリを分け配下に標準化された患者データを配置する．

標準化された患者データを図 2.2 に示す．標準化された患者データが準拠する標準規格

は，保険医療福祉システム工業会，日本 HL7 協会，日本画像医療システム工業会，医療情報システム開発センターが定めている規格を用いている [6].

2.2　医療データのバックアップの条件

本節では医療データを分散バックアップし，被災地での医療行為に活用するための条件を述べる.

広域災害に備えてバックアップするため，災害時にバックアップデータを格納しているストレージが被災した場合でもリストアできるようにバックアップデータを冗長化する必要がある．医療データは個人情報であるため，バックアップデータから情報が読み取られないようにバックアップデータを秘匿化する必要がある．また，患者の医療データを保持している病院が病院関係者以外の人に患者の医療データを提供することは，患者本人の同意が得られない場合基本的に提供することはできない．よって，バックアップデータから被災地での医療行為に必要なデータのみを提供し，不必要な情報を制限しなければならない．さらに，被災地での医療行為に必要なデータが増える可能性があるため，医療データをバックアップする病院が提供できる情報を自由に変更できるほうがよい.

医療データを分散バックアップし，被災地での医療行為に活用するための条件を以下にまとめる.

1. バックアップデータの冗長化ができること
2. バックアップデータの秘匿化ができること
3. バックアップデータから被災地での医療行為に必要なデータのみを提供可能であること
4. 提供するデータを自由に変更することができること

医療データを分散バックアップし，被災地での医療行為に活用するためには以上の条件を満たす必要がある.

2.3 (k, n) しきい値秘密分散

分散バックアップの手法に秘密分散法がある．秘密分散法はデータの秘匿化と冗長化を図ることができる [7]．秘密分散法はデータの分散・復元という 2 つの段階がある．データを分散するときは，データからシェアと呼ばれる無意味な情報を複数生成する．データを復元するときは，分散したシェアを一定個数集めることでデータを復元することができる．全てのシェアを集めなくともデータを復元することができるため，バックアップデータを冗長化することができる．また，一定個数未満のシェアからは元データの情報を得ることができないため，バックアップデータの秘匿化ができる．

秘密分散法は，データを読みにくくする暗号化とは異なり，データを読めなくする技術である．よって，個人情報を秘密分散法を用いて生成したシェアは個人情報ではないという見解が経済産業省でされている．愛媛大学を中心とした研究グループによって電子カルテの分散バックアップに秘密分散法を用いる研究がなされている．また，情報通信研究機構では電子カルテのデータ提供に秘密分散法を用いる研究が行われている [9]．

本節では，分散バックアップに用いられる秘密分散法の 1 つである (k, n) しきい値秘密分散法について述べ，医療データをバックアップするための条件を満たしているかを検討する．

(k, n) しきい値秘密分散法を用いた SS-MIX 形式の電子カルテのバックアップを図 2.3 に示す．SS-MIX 形式の電子カルテの患者 ID 以下のディレクトリから (k, n) しきい値秘密分散法を用いてシェアを n 個生成し，それぞれ別々の場所で保管する．復元する際は，k 個以上のシェアを集めることで復元することができる．

(k, n) しきい値秘密分散法のデータの流れを図 2.4 に示す．(k, n) しきい値秘密分散法は，データを n 個のシェアと呼ばれる無意味な断片に分散し，k 個以上のシェアを集めることによって復元可能な方法である．k 個未満のシェアからは情報を読み取ることができないことが情報理論的に証明されている [10]．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

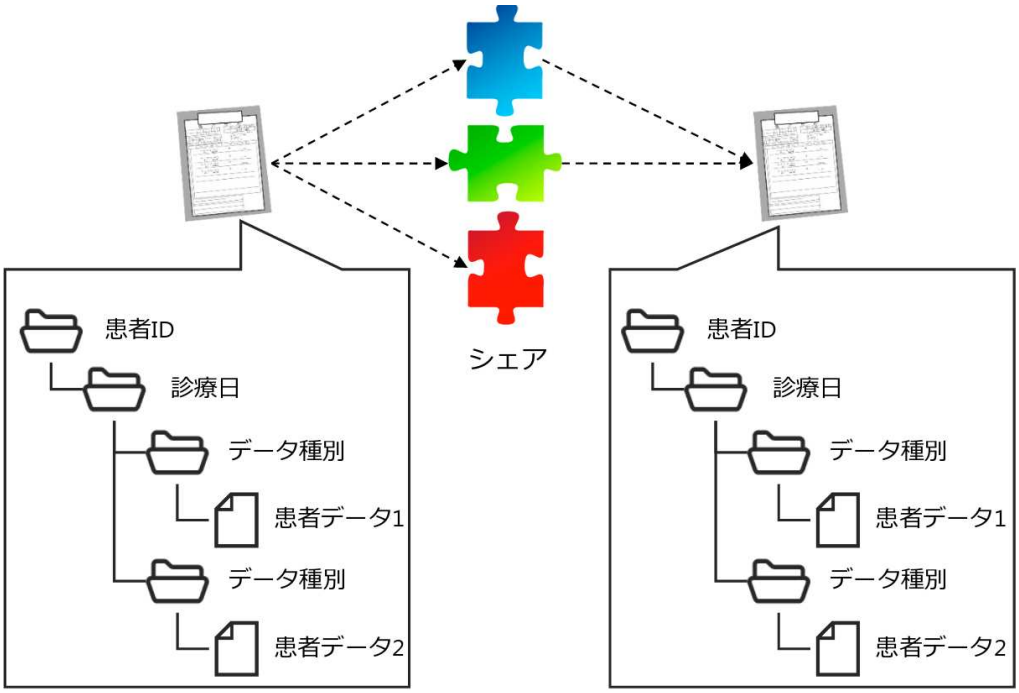

図 2.3 (k, n) しきい値秘密分散法を用いた SS-MIX 形式の電子カルテのバックアップ

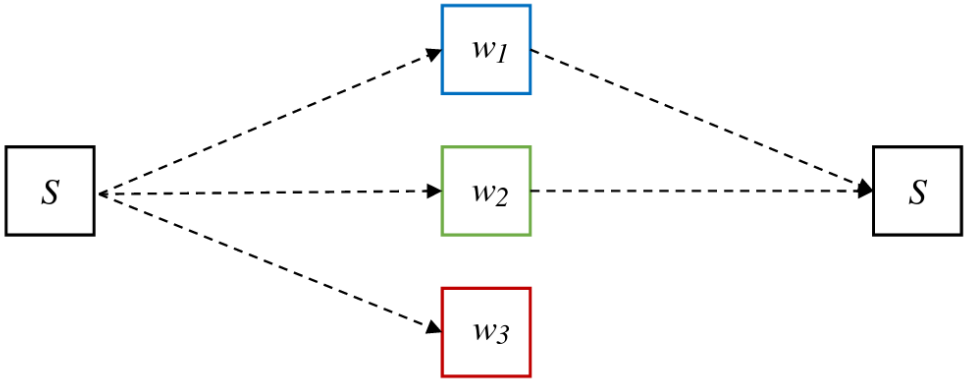

図 2.4 (k, n) しきい値秘密分散法のデータの流れ

分散するデータを S，素数を $p(S < p$ かつ $n < p)$，$\mathbb{Z}/p\mathbb{Z} - \{0\}$ 上の集合 x を

$$x = \{x_1, x_2, \cdots, x_n\}.$$

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

1. x から

$$X = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{k-1} \end{pmatrix} \pmod{p} \tag{2.1}$$

となるような vandermonde の行列 X を作成する．

2. S と R から $k \times 1$ のベクトル $\boldsymbol{a}$

$$\boldsymbol{a} = \begin{pmatrix} S \\ r_1 \\ r_2 \\ \vdots \\ r_{k-1} \end{pmatrix} (r_1, r_2, \cdots, r_{k-1}, \in R,\ r_{k-1} \neq 0) \tag{2.2}$$

を作成する．

3. p を法とする X と $\boldsymbol{a}$ の乗算より，

$$X\boldsymbol{a} = \begin{pmatrix} w_1 \\ w_2, \\ \vdots \\ w_n \end{pmatrix} \pmod{p} \tag{2.3}$$

となるような $w_i (i = 1, 2, \cdots, n)$ が得られる．また，w_i をシェアと呼び，w_i を分散する．

4. k 個以上のシェアを集める．k 個以上のシェアを集めた場合はその中から k 個選択する．選択したシェアからシェア行列 W

$$W = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_k \end{pmatrix} \tag{2.4}$$

を作成する．

5. X の逆行列 X^{-1} を W の左からかけると，

$$
\begin{aligned}
X^{-1}W &= X^{-1}\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_k \end{pmatrix} \\
&= X^{-1}X\begin{pmatrix} S \\ r_1 \\ r_2 \\ \vdots \\ r_{k-1} \end{pmatrix} \\
&= \begin{pmatrix} S \\ r_1 \\ r_2 \\ \vdots \\ r_{k-1} \end{pmatrix} \pmod{p}
\end{aligned} \tag{2.5}
$$

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手順である．式 (2.4) を連立方程式で表現すると

$$
\begin{cases}
w_1 = S + r_1x_1 + r_2x_1^2 + \cdots + r_{k-1}x_1^{k-1} \pmod{p} \\
w_2 = S + r_1x_2 + r_2x_2^2 + \cdots + r_{k-1}x_2^{k-1} \pmod{p} \\
\qquad\qquad \vdots \\
w_k = S + r_1x_k + r_2x_k^2 + \cdots + r_{k-1}x_k^{k-1} \pmod{p}
\end{cases} \tag{2.6}
$$

となる．式 (2.6) を解くとデータ S を求めることができる．w_i が k 個以上の場合，S を一意に定めることができるが，w_i が k 個未満の場合，S を一意に定めることができず S を求めることができないことがわかる．

(k, n) しきい値秘密分散法は n 個のシェアのうち $n - k$ 個のシェアを紛失したとしてもデータを復元することができるため，データの冗長化ができる．また，作成したシェアのうち k 個未満では元データの情報を読み取ることができないため，データの秘匿化ができる．しかし，(k, n) しきい値秘密分散法に関わらず秘密分散法は分散したデータを復元できるかできないかのどちらかであり，部分的に復元することはできない．

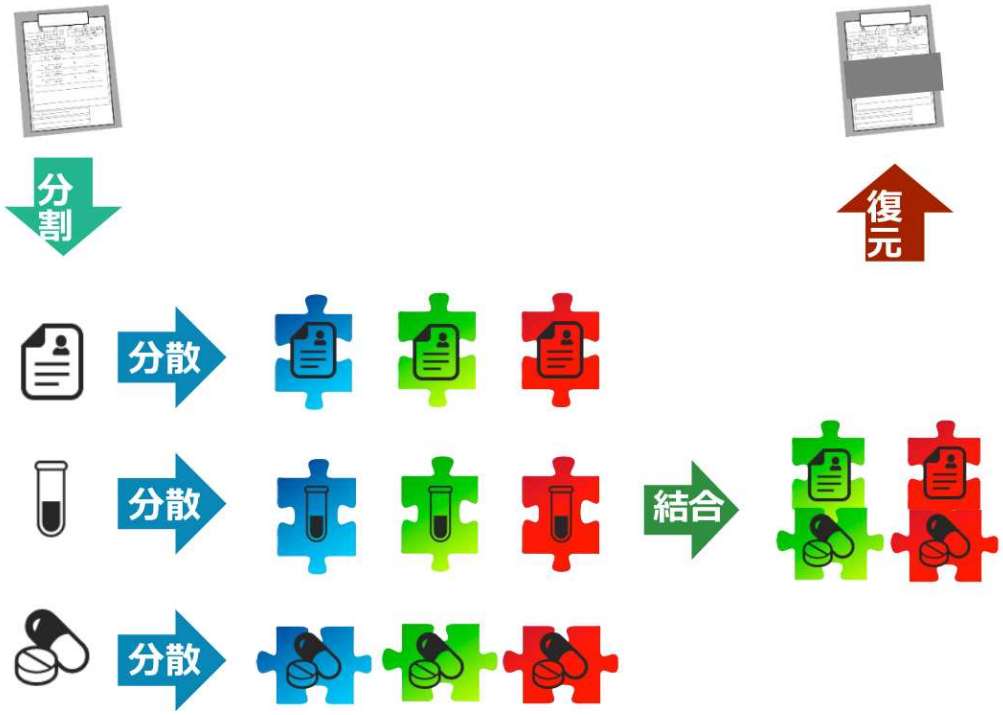

図 2.5　部分復元アルゴリズムを用いた SS-MIX 形式の電子カルテのバックアップ

2.4　部分復元アルゴリズム

秘密分散法は分散したデータを部分的に復元することはできない．よって，(k, n) しきい値秘密分散法を用いた部分復元アルゴリズムを提案した [11]．本節では，(k, n) しきい値秘密分散法を用いて分散したデータの中から復元したい情報をあらかじめ選択しておき，選択した情報を復元する部分復元アルゴリズムに述べる．さらに，部分復元アルゴリズムが医療データをバックアップするための要件を満たすかどうかを検討する．

部分復元アルゴリズムを用いた SS-MIX 形式の電子カルテのバックアップを図 2.5 に示す． 図 2.6 のように SS-MIX 形式の電子カルテのデータ項目ごとに医療データを分け，分けたデータそれぞれに対して (k, n) しきい値秘密分散法を用いてシェアを生成する．復元する際は，復元したい項目のシェアのみを集め，シェア同士をつなぎ合わせてから復元することによって任意のデータを復元することができる．

部分復元アルゴリズムには復元段階と分散段階の 2 つの段階からなる．部分復元アルゴリズムの復元段階から分散段階のデータの流れを図 2.7 に示す．

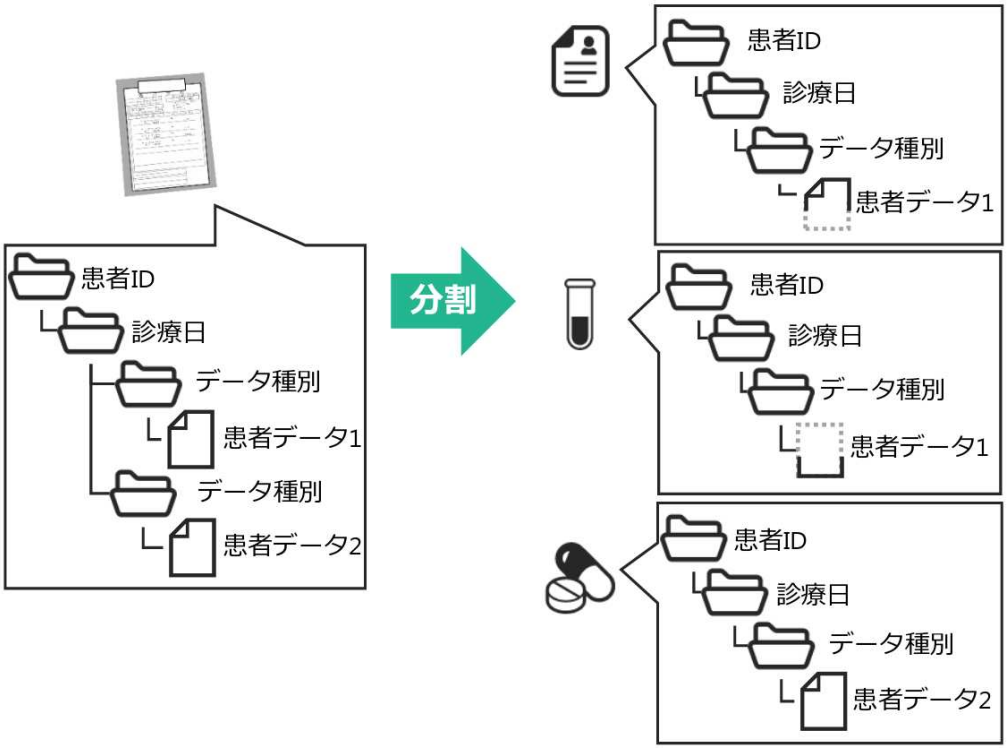

図 2.6　SS-MIX 形式の電子カルテデータの分割

2.4.1　分散段階

まず，分散するデータ S を意味のある項目ごとにデータを d 個に分け，分けたデータ S_i $(i = 1, 2, \cdots, d)$ それぞれに対して (k, n) しきい値秘密分散法を用いてシェアを生成し分散する．データを意味のある項目ごとに分けることを分割とする．生成したシェアはシェアの状態でどのシェアがどの項目のシェアなのかを区別することが困難である．よって，全ての項目が含まれかつ，項目が正しい順番で並んだデータを復元することができない可能性がある．そこで，復元する際に S_i のシェア同士を正しく紐付ける情報を作成し紐付け情報とする．紐付け情報は項目ごとに分けたデータの長さ l_i を要素として対応する項目ごとに要素を並べたものであり，シェアと保管しておく．また，データ内容にあたる項目が 0 となるように紐付け情報を作成する．

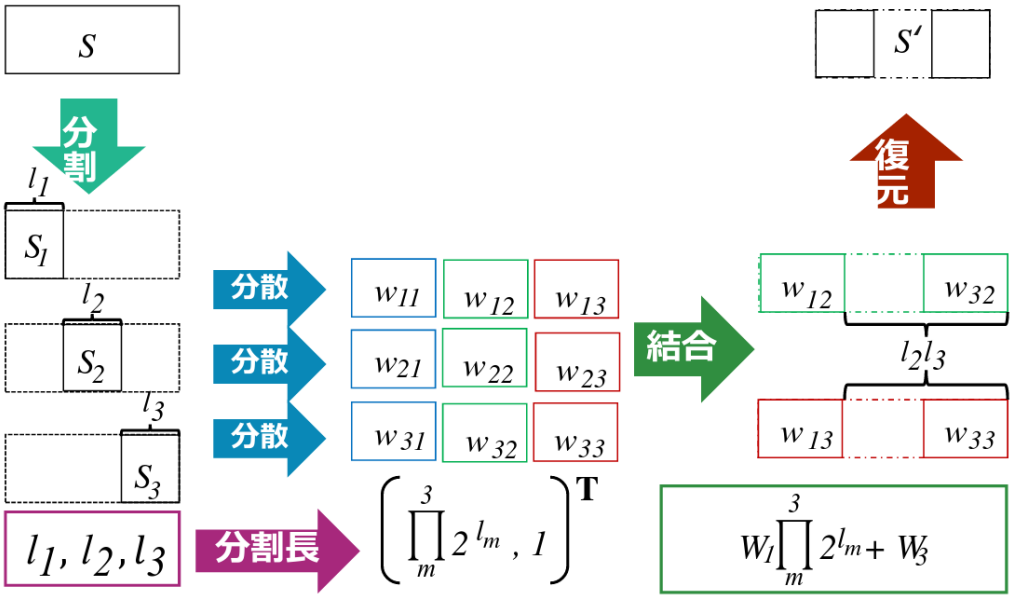

図 2.7　部分復元アルゴリズムのデータの流れ

2.4.2　復元段階

分散したシェアから復元したい項目のシェアのみをしきい値以上集め，復元したい項目のシェアを計算可能な紐付け情報を入手する．集めたシェアと紐付け情報を用いて，復元したい項目のみを含んだデータのシェアとなるように計算を行う．以降この計算を結合とする．結合したシェアを (k, n) しきい値秘密分散法の復元操作を行うことで，復元したい項目のみを含んだデータを復元することができる．

2.4.3　部分復元の手順

部分復元アルゴリズムの部分復元の手順を述べる．データを S，S を分割したデータを

$$S_i \quad (i = 1, 2, \cdots, d)$$

とおく．分割したデータ S_i は

$$S = S_1 \prod_{m=2}^{d} 2^{l_m} + S_2 \prod_{m=3}^{d} 2^{l_m} + \cdots + S_{d-1} 2^d + S_d \tag{2.7}$$

と表すことができ，各分割したデータ長分だけ左シフトして直和をとることで S となるように分割する．各分割データのデータ長を分割長 l_i とする．分割データ S_i の集合を

$$S_{\text{all}} = \{S_1, S_2, \cdots, S_d\}$$

とおき，復元したいデータの集合を S_{all} の部分集合として

$$S_{\text{all}} \subseteq S_c = \{S_{c_1}, S_{c_2}, \cdots, S_{c_j}\} \quad (1 \leq d)$$

としたとき，復元したいデータ S' は

$$S' = S_{c_1} \prod_{m=2}^{j} 2^{l_m} + S_{c_2} \prod_{m=3}^{j} 2^{l_m} + \cdots + S_{c_1}$$

と表すことができる．S_c の任意の要素である S_{c_t} $(1 \leq t \leq j)$ のシェア集合を

$$W_{c_t} = \{w_{c_{t1}} w_{c_{t2}}, \cdots, w_{c_{tn}}\}$$

とおき，シェア集合 G_c の要素 W_{c_t} を復元したい情報のみを含んだデータのシェアとなるように計算する紐付け情報

$$\boldsymbol{u}_c = \begin{pmatrix} \prod_{m=2}^{j} 2^{l_m} \\ \prod_{m=3}^{j} 2^{l_m} \\ \vdots \\ 1 \end{pmatrix} \tag{2.8}$$

を作成する．部分復元の詳細な手順を以下に示す．

1. データ S を式 (2.7) を用いて分割し，S_i を作成する．このとき，データ長 l_i を分割長とする．
2. 素数 p ($S < p$ かつ $n < p$) を選択する．
3. $\mathbb{Z}/p\mathbb{Z} - \{0\}$ の集合 $X = \{x_1, x_2 \cdots x_n\}$ から

$$X = \begin{pmatrix} 1 & x_1 & x_2^2 & \cdots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{k-1} \end{pmatrix} \pmod{p} \tag{2.9}$$

となるような $n \times k$ の vandermonde 行列 $\boldsymbol{X}$ を作成する．また，分割データ S_i と $\mathbb{Z}/p\mathbb{Z}$ の集合 $R_i = \{r_{i,1}, \cdots, r_{i,k-1}\}$(ただし $r_{i,k-1} \in \{\mathbb{X}/p\mathbb{Z}\} - \{0\}$ とする) からランダムに選択し，ベクトル $\boldsymbol{a}_i$

$$\boldsymbol{a}_i = \begin{pmatrix} S_i \\ r_{i1} \\ r_{i2} \\ \vdots \\ r_{ik-1} \end{pmatrix}$$

を作成する．

4. p を法とした X と $\boldsymbol{a}_i$ の乗算より，

$$X\boldsymbol{a}_i = \begin{pmatrix} w_{i1} \\ w_{i2} \\ \vdots \\ w_{in} \end{pmatrix} \pmod{p} \tag{2.10}$$

となるような w_{ij} $(j = 1, 2, \cdots, n)$ をシェアとよぶ．w_{ij} を分散する．

5. G_c から各 w_{c_j} のシェアが k 個になるように集める．k 個以上集めた場合は集めたシェアから k 個選択する．k 個のシェアからシェア行列 W_c

$$W_c = \begin{pmatrix} w_{c_{11}} & w_{c_{21}} & \cdots & w_{c_{j1}} \\ w_{c_{12}} & w_{c_{22}} & \cdots & w_{c_{j2}} \\ \vdots & \vdots & \ddots & \vdots \\ w_{c_{1k}} & w_{c_{2k}} & \cdots & w_{c_{jk}} \end{pmatrix} \tag{2.11}$$

を作成する．

6. W_c に対して式 (2.8) をかけ，

$$W_c\boldsymbol{u}_c = \begin{pmatrix} w_{c_{11}} \prod_{m=2}^{j} 2^{l_m} + w_{c_{21}} \prod_{m=3}^{j} 2^{l_m} + \cdots + w_{c_{j1}} \\ w_{c_{12}} \prod_{m=2}^{j} 2^{l_m} + w_{c_{22}} \prod_{m=3}^{j} 2^{l_m} + \cdots + w_{c_{j2}} \\ \vdots \\ w_{c_{1k}} \prod_{m=2}^{j} 2^{l_m} + w_{c_{2k}} \prod_{m=3}^{j} 2^{l_m} + \cdots + w_{c_{jk}} \end{pmatrix} \tag{2.12}$$

式 (2.12) を展開してまとめると

$$X \begin{pmatrix} S_{c_1} \prod_{m=2}^{j} 2^{l_m} + S_{c_2} \prod_{m=3}^{j} 2^{l_m} + \cdots + S_{c_j} \\ r_{11} \prod_{m=2}^{j} 2^{l_m} + r_{21} \prod_{m=3}^{j} 2^{l_m} + \cdots + r_{j1} \\ \vdots \\ r_{1k-1} \prod_{m=2}^{j} 2^{l_m} + r_{2k-1} \prod_{m=3}^{j} 2^{l_m} + \cdots + r_{jk-1} \end{pmatrix} \tag{2.13}$$

となる．

7. 式 (2.13) に左から $\boldsymbol{X}$ の逆行列 $\boldsymbol{X}^{-1}$ をかけると

$$\begin{aligned} X^{-1} W_c \boldsymbol{u}_c &= S_{c_1} \prod_{m=2}^{j} 2^{l_m} + S_{c_2} \prod_{m=3}^{2} 2^{l_m} + \cdots + S_{c_j} \\ &= S' \end{aligned} \tag{2.14}$$

となり，S の部分的なデータ S' を復元できる．以上の手順より，データ S を (k, n) しきい値秘密分散法で作成したシェアから必要な部分のデータ S' のみを復元する部分復元を実現する．

部分復元アルゴリズムは，データの分散・復元に (k, n) しきい値秘密分散法を用いているため，データの秘匿化と冗長化が可能である．部分復元アルゴリズムは (k, n) しきい値秘密分散法で困難だった S' のような部分的なデータを復元することができる．さらに，紐付け情報 $\boldsymbol{u}_c$ を変更することで部分的に復元する情報を変更することができる．よって，医療データを分散バックアップし，被災地での医療行為に活用するための条件をすべて満たす．

2.5 (k, n) しきい値秘密分散法と部分復元アルゴリズムの比較

本節では，(k, n) しきい値秘密分散法と部分復元アルゴリズムの比較を行い，部分復元アルゴリズムの評価をする．

(k, n) しきい値秘密分散法は，データから n 個のシェアを生成し n 個のシェアのうち k 個以上集めることによってデータを復元することができる．k 個未満のシェアからは元データの情報を読み取ることはできないため，データの秘匿化ができる．また，シェアを $n - k$ 個紛失したとしてもデータを復元することができるため，データの冗長化ができる．しかし，

(k, n) しきい値秘密分散法はデータを復元できるかできないかのどちらかであり部分的な情報を復元することはできない．

(k, n) しきい値秘密分散法を用いて部分的な情報を含むデータを復元する方法として，分散するデータから部分的な情報をのみを含んだデータを作成しシェアを生成することで，部分的な情報を復元することができる．しかし，分散するデータのシェアのみならず，部分的な情報のみを含むデータのシェアが必要となる．

部分復元アルゴリズムはデータの分散・復元に (k, n) しきい値秘密分散法を用いているため，データの秘匿化・冗長化ができる．部分復元アルゴリズムはシェアのまま結合し復元するため，データを秘匿したまま部分的なデータを復元することができる．さらに，紐付け情報を変え，結合するシェアを変更することによって，復元するデータを自由に変更することができる．

以上よりデータの秘匿化・冗長化が可能であり，部分的な情報を自由に復元可能な部分復元アルゴリズムが条件をすべて満たすため，医療データのバックアップに適しているといえる．

2.6　まとめ

東日本大震災の津波によって，沿岸部の病院に保管されたいた電子カルテを含む医療データが流出し，被災地での医療行為に支障が出た．これをうけて病院では医療データを遠隔地にバックアップする取り組みが始められている．分散バックアップした医療データを，被災地での医療行為に活用することができれば診療を円滑に行うことができる．しかし，医療データは個人情報であるため診療に不必要なデータの提供を制限する必要がある．本章では，バックアップ対象の医療データについて述べ，バックアップした医療データを被災地での医療行為に活用するために満たすべき条件を示し，条件を満たした方法を述べた．

分散バックアップの手法に (k, n) しきい値秘密分散法を用いる方法がある．(k, n) しきい値秘密分散法はデータの秘匿化・冗長化が可能だが，データを部分的に復元することはでき

ない．そこで (k, n) しきい値秘密分散法を用いた部分復元アルゴリズムを提案した．部分復元アルゴリズムはデータを項目ごとに分割し，必要な項目をシェアの状態で結合してから復元するため，データを秘匿したまま部分的なデータを復元することができる．よって，本研究では医療データの分散バックアップに (k, n) しきい値秘密分散法を用いた部分復元アルゴリズムを用いる．

第 3 章

部分復元可能な秘密分散システム

本章では部分復元アルゴリズムを用いた部分復元可能な秘密分散システムについて述べる．まず，被災地での医療行為に必要なデータを提供するシステムが満たすべき要件を述べる．次に，不正復元を防ぐ部分復元可能な秘密分散システムについて述べる．最後に，提案システムで不正復元される可能性がある点を整理し，不正復元を防ぐ要件を定義する．

3.1 高知県のバックアップした医療データの活用計画

東日本大震災の津波によって医療データが流出し，被災地での医療行為に支障がでたことをうけて，高知県では電子カルテを県外にバックアップするのみならず，バックアップした電子カルテをリストア以外に活用する計画がある．高知県のバックアップした医療データの活用計画の全体図を図 3.1 に示す．

計画ではまず，平常時は様々な病院の電子カルテをまとめて県外にバックアップする．災害急性期には，高知県外からやってくる医師や DMAT に対して患者の診療に必要な情報を提供し，被災地での医療行為に活用してもらう．災害復興期には，バックアップした病院に電子カルテをリストアする．また，災害時のみならず，地域間での医療連系にも活用しようとしている．しかし医療データは個人情報であるため，病院外の人間に提供することは個人情報保護の観点から望ましくない．図 3.1 のように活用するためには，バックアップした医療データから部分的な情報と全ての情報を提供可能なシステムが必要となる．そこで前章で秘密分散したデータを部分的に復元可能な部分復元アルゴリズムを提案した．部分復元アルゴリズムを用いることによって，秘密分散したデータを部分的に復元することができる．

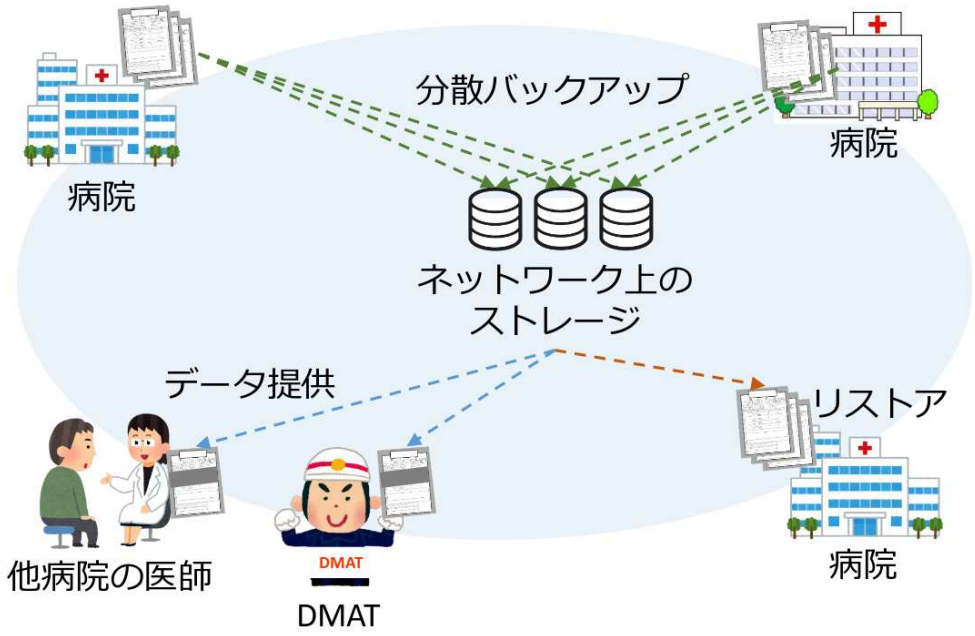

図 3.1　バックアップした医療データの活用計画

部分復元アルゴリズムは，シェアを結合する紐付け情報とシェアが何らかの方法で第三者に入手されると不正復元される恐れがある．バックアップ対象の医療データは個人情報であるため，第三者の不正復元を防ぐ必要がある．

本研究では，不正復元を防いだ部分復元可能な秘密分散システムを提案する．

3.2　部分復元アルゴリズムを用いた部分復元可能な秘密分散システムに対する要件

部分復元アルゴリズムを用いた部分復元可能な秘密分散システムに対する要件についてまとめる．

災害時，医療データを表示するシステムが被災し，復元したデータが読めない可能性がある．よって，復元するデータの形式はどのような端末でも閲覧可能であることが望ましい．

医療データは個人情報であるため，データをバックアップした病院外で医療データを復元し検索・閲覧する際は，被災地での医療行為に最低限必要な情報の閲覧のみを提供する必要

がある．また，情報を閲覧するものは特定の人間に限定し，それ以外の人間が閲覧できないようにする必要がある．さらに，厚生労働省のガイドラインの外部保存を受託する機関における医療情報へのアクセス禁止より，災害時に医療データを活用しないネットワーク上のストレージ上で医療データを復元し検索・閲覧を禁止する必要がある [12].

部分復元アルゴリズムは紐付け情報とシェアが第三者に入手されると不正復元される可能性がある．紐付け情報は分散するデータのデータ形式が既知であれば自由に作成することができる．今回対象とする医療データは SS-MIX 形式で保存された電子カルテであるため，データ形式が既知であるといえる．また，シェアを保管するストレージはネットワーク上にある．このため，第三者が紐付け情報を作成し，シェアを不正入手することによって，データを不正に復元される可能性がある．よって，紐付け情報の作成とシェアの入手を制限する必要がある．

部分復元アルゴリズムを用いた医療データの部分復元システムに対する要件を以下にまとめる．

要件 1　どのような端末でも閲覧可能な形式であること

要件 2　復元した医療データを閲覧できる環境・人間を限定すること

要件 3　医療データを活用する以外の場所で医療データの復元を防ぐこと

要件 4　紐付け情報の作成を限定すること

要件 5　シェアを保管しているストレージにアクセスする人間を限定すること

以上の要件を満たすような部分復元可能な秘密分散システムを提案する．

3.3　部分復元アルゴリズムを用いた部分復元可能な秘密分散システムの構成

本節では前節の要件を満たした部分復元アルゴリズムを用いた部分復元可能な秘密分散システムの構成について述べる．

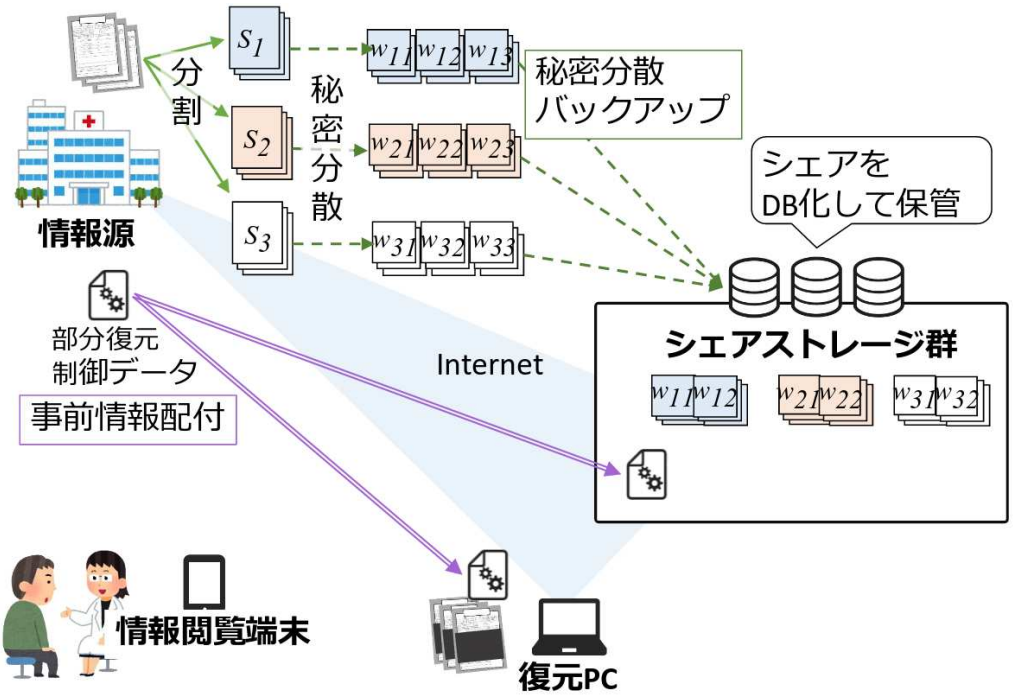

図 3.2　医療データの部分復元システムの構成 (分散)

提案システムのシステムの構成を図 3.2 と図 3.3 に示す．

提案システムでは，紐付け情報の作成とシェアの入手を制限するために，図 3.2 のように医療データを分散バックアップする病院が提案システムを制御するデータを作成し，復元 PC とシェアストレージ群に配付する．以下では，医療データを分散バックアップする病院のことを情報源とする．

シェアストレージ群はネットワーク上に点在しているシェアストレージ群の集合である．シェアストレージはしきい値以上存在し，それぞれのストレージにしきい値未満のシェアを DB 化して保存する．以降，シェアを保管する DB のことをシェア DB とする．シェアストレージからシェアを配付する際は，図 3.3 のようにシェア DB からシェアを取り出し，結合してから配付する．さらに接続元の利用形態に応じて配付するシェアを変える．

災害時に被災地でバックアップした医療データを活用するために，情報源は復元 PC と情報閲覧端末を用意する．復元 PC は，災害時に医療データが必要となる避難所などの拠点に設置され，シェアを入手し，医療データを復元する．情報閲覧端末は，復元 PC と同じ場所

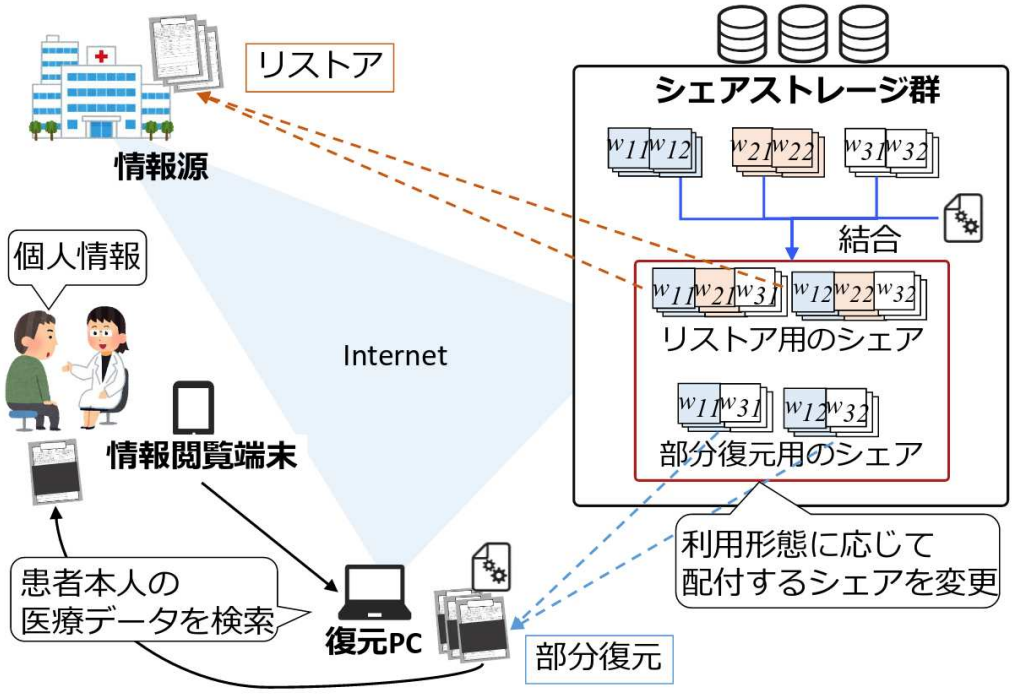

図 3.3　医療データの部分復元システムの構成 (復元)

に設置し，医師に対して配付して復元 PC から医師が診療している患者の医療データを入手する．

以上の構成で医療データの部分復元を行う．

3.4　部分復元アルゴリズムを用いた部分復元可能な秘密分散システム

本節では，部分復元アルゴリズムを用いた部分復元可能な秘密分散システムで扱うデータについて述べた後，提案システムでのデータの分散，復元について述べる．最後にシステムが要件を満たしているかを確認する．

提案システムで扱うデータの一覧を図 3.4 に示す．提案システムで扱うデータは，情報源が作成し提案システムを制御する部分復元制御データとシェアに分けることができる．提案システムを制御するデータについて述べる．部分復元制御データの一覧とデータの役割を以

3.4　部分復元アルゴリズムを用いた部分復元可能な秘密分散システム

部分復元制御データ
- 分散スクリプト
- 改ざん確認スクリプト
- 復元スクリプト
- データ整形スクリプト
- シェアストレージ群の情報(災害)
- シェアストレージ群の情報(病院)
- DB作成スクリプト
- シェア同士の紐付けスクリプト

シェア
- バックアップシェア
- 紐付け済シェア(災害用)
- 全情報の紐付け済みシェア(リストア用)

その他
- 患者の本人識別情報
- 復元PCの情報
- 患者の必要最低限の医療データ

図 3.4　提案システムで扱うデータの一覧

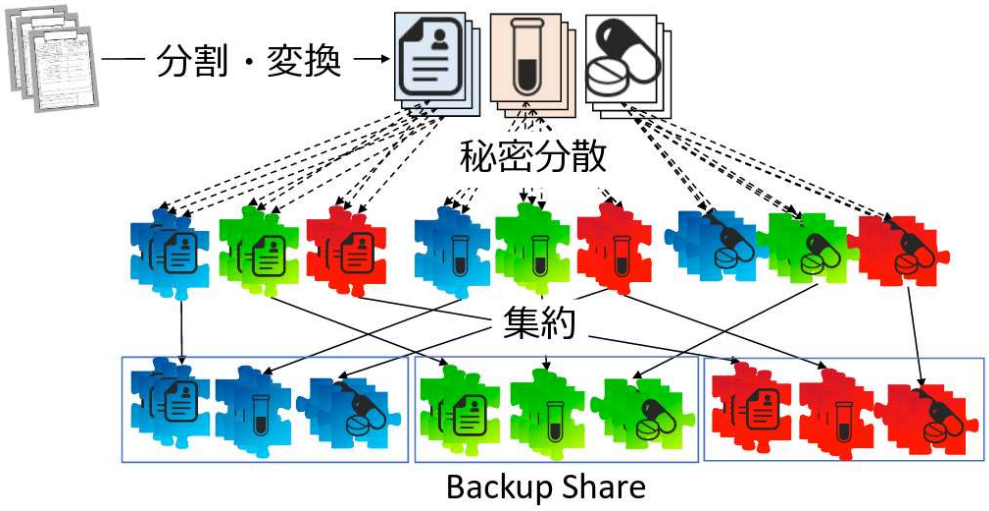

図 3.5　分散スクリプトの処理

下に示す．

分散スクリプト

分散スクリプトは，SS-MIX 形式の電子カルテを秘密分散し，シェアを生成するスクリプトである．変換，秘密分散，集約，DB 作成スクリプト作成，紐付けスクリプト作成で構成される．分散スクリプトを用いて SS-MIX 形式の電子カルテからシェアを生成する処理を図 3.5 に示す．SS-MIX 形式の電子カルテは，被災地での医療行為に必要なデータと不必要なデータに分割することが難しいため，変換処理で扱いやすい形式に変換する．変換したデータを分散しシェアを生成する．シェアをシェア DB に格納するために，医療データを分割した項目ごとに集める．この処理のことを集約とする．集約

したシェアをバックアップするシェアとする．最後に，シェアストレージ上でシェアを保管する DB を作成するシェア DB 作成スクリプトとシェアの結合を行うシェア紐付けスクリプトをシェアから作成する．DB 作成スクリプトと紐付けスクリプトはシェアストレージの数だけ作成する．なお，DB 作成スクリプトと紐付けスクリプトの作成は初めて医療データをバックアップするときのみ行う．

データ改ざんスクリプト

データ改ざんスクリプトは，シェアストレージから入手したシェアが改ざんされていないかを確認するスクリプトである．改ざんの確認には一般的によく用いられるハッシュ値を用いる．

復元スクリプト

復元スクリプトは，シェア復元するスクリプトである．復元スクリプトは変換、復元、個人データ作成で構成される．シェアストレージから入手したシェアを復元しやすい形式に変換し復元する．最後に，復元した医療データは，情報源の病院の全患者の情報が一緒になっているため，一人ひとりの患者に個人データ作成で分ける．

データ整形スクリプト

データ整形スクリプトは，復元スクリプトで復元した医療データを公開用に整えるスクリプトである．復元スクリプトで復元した医療データはコード形式で記述されているため，コード変換をする必要がある．そこで，データ整形スクリプトを用いてコードを変換し，見やすいように整える．このとき，どのような端末でも閲覧できるように公開用の医療データはテキスト形式で出力する．

シェアストレージ群の情報

シェアストレージ群の情報は，それぞれのシェアストレージにアクセスするために必要な情報である．シェアストレージ群にはすべての情報を含んだ医療データを復元できるシェアが格納されている．情報源で部分復元の制御をしていたとしても，復元 PC がすべての情報のシェアを入手することができれば，被災地で意図しない情報を復元される可能性がある．よって，シェアストレージ内のすべての情報にアクセス可能な病院

ユーザと，災害時に被災地で行う医療行為に必要な情報のシェアのみにアクセス可能な災害ユーザを作成する．さらに病院ユーザにはシェアストレージを管理する管理者権限を付与する．以降，病院ユーザと災害ユーザによってアクセス可能なデータを判別するために，病院ユーザがアクセス可能なデータの末尾に (病院)，災害ユーザがアクセス可能なデータの末尾に (災害) とつけ区別する．

DB 作成スクリプト

DB 作成スクリプトは，シェアストレージ上にシェア DB を作成するスクリプトである．情報源が医療データから初めてシェアを生成するときのみ作成する．SQL 文以外の部分はシェアで記述されており，シェアストレージごとに DB 作成スクリプトを作成する．

シェア同士の紐付けスクリプト

シェア同士の紐付けスクリプトは，シェアストレージ上でシェアを結合するときに利用するスクリプトである．シェア DB 作成スクリプトを元に作成する．シェア同士の紐付けスクリプトもシェアストレージごとに異なるデータを作成する．

患者の本人識別情報

災害時，医師が診療している患者から聞き出す情報であり，名前や性別，生年月日など患者本人を特定可能な情報である．

復元 PC の情報

情報閲覧端末が復元 PC にアクセスする際に必要な情報である．情報閲覧端末は復元 PC にリモートデスクトップ接続を行う．また，情報閲覧端末と復元 PC 間のネットワークはローカルエリアネットワークを用いるためその情報も含まれる．

以上が部分復元制御データである．

提案システムの分散から復元までの手順を述べる．提案システムのシステムのデータの流れを図 3.6 と図 3.7 に示す．手順番号と図 3.6 と 3.7 の番号は対応している．

1. 事前情報の配付

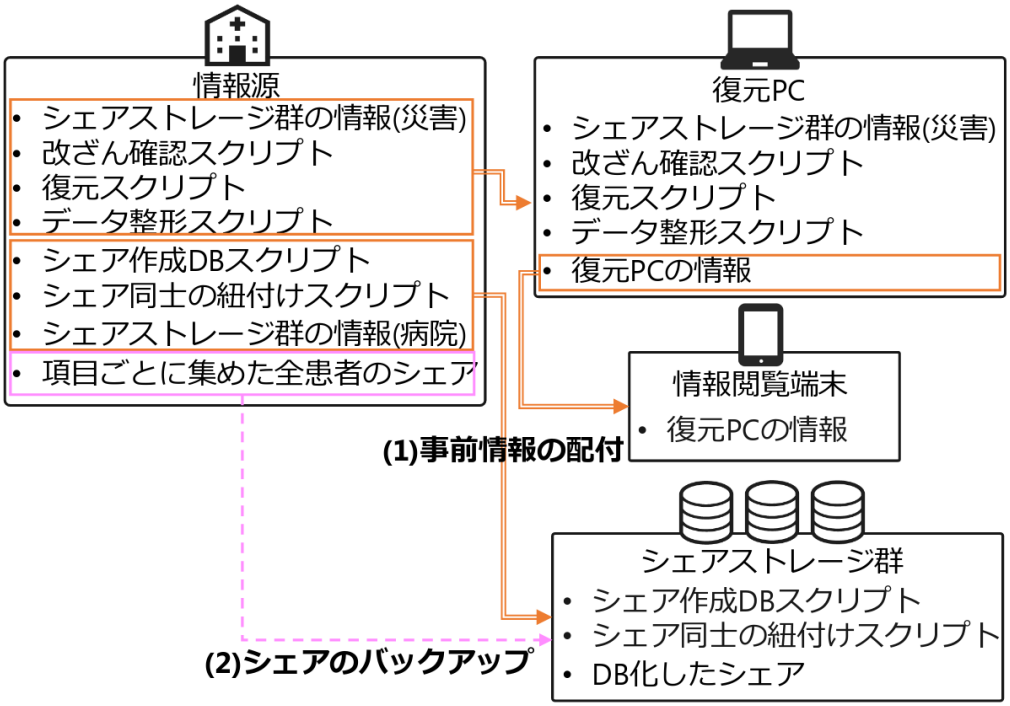

図 3.6　分散時のデータの流れ

情報源は，部分復元を制御する制御データを作成し，シェアストレージ群と復元 PC に事前情報として配付する．事前情報を配付する際，情報源はどの復元 PC，シェアストレージ群に配付したかを記録する．復元 PC は情報閲覧端末に対して，情報閲覧端末が復元 PC に接続するために必要な復元 PC の情報を教えておく．

2. シェアのバックアップ

情報源は医療データから分散スクリプトを用いてバックアップするシェアを生成しシェアストレージにバックアップする．

3. シェアの復元

災害時復元 PC はシェアストレージ群の情報 (災害) を用いてしきい値以上のシェアストレージに接続する．シェアストレージ群は，被災地での医療行為に必要な情報のシェアを紐付けスクリプトで結合してから配付する．

復元 PC は紐付け済シェア (災害) をしきい値以上入手し，入手したシェアが改ざんされていないかを改ざん確認スクリプトを用いて確認した後，復元スクリプトを用いて

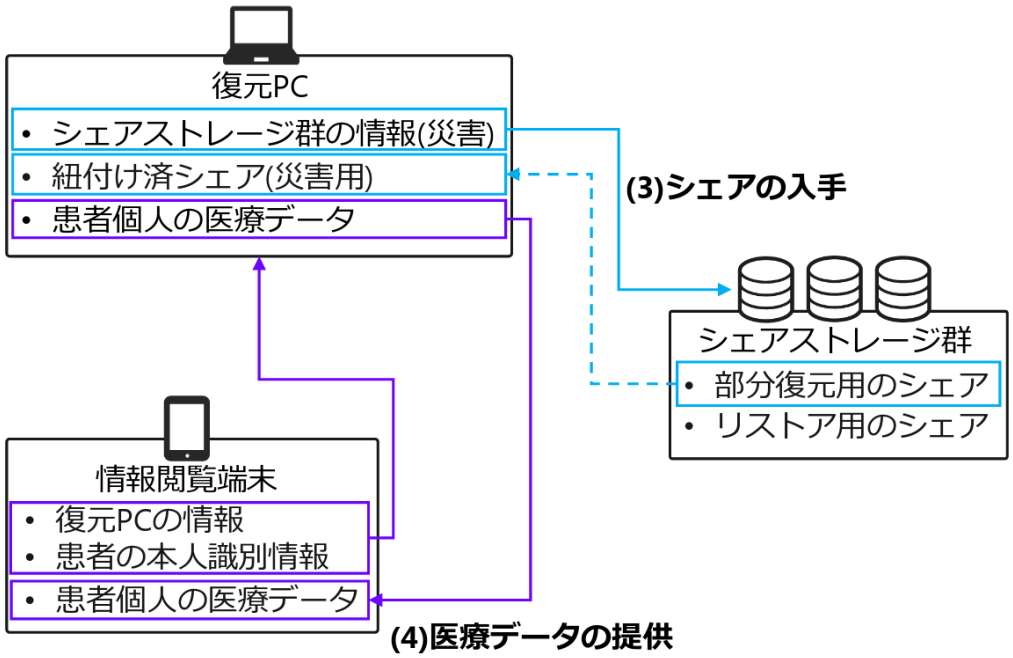

図 3.7　復元時のデータの流れ

シェアを復元する．この操作を整形とする．

4. 医療データ提携

情報閲覧端末は復元 PC の情報を用いて復元 PC に接続し，医師が診察している患者から得た名前などの患者本人を識別する識別情報などを用いて，患者個人の医療データを入手する．

以上の手順を踏むことで部分復元を実現している．

提案した部分復元アルゴリズムを用いた医療データの部分復元システムが要件を満たすかを確認する．

整形スクリプトで復元したデータをテキスト形式にするため，どのような端末でもエディタがあれば読むことができる．よってどのような端末でも閲覧可能な形式であるといえる．

災害時に被災地で復元できる環境を復元 PC，閲覧できる環境を情報閲覧端末と限定し，利用者に情報閲覧端末を配付する際には，利用者が医師かどうかを確認する．よって，復元した医療データの閲覧できる環境・人間を制限できている．

情報源から事前情報としてシェアストレージ群の情報 (災害) と復元スクリプトを入手していなければ，シェアを入手し復元することができない．また，シェアストレージは自身以外のシェアストレージの情報を知らないため，シェアストレージ群上では医療データの復元はできない．よって，医療データを活用する以外の場所での医療データの復元を防いでいる．

紐付け情報の作成を情報源に限定する．さらに，シェアストレージ群がシェアを配付するときは，情報源が作成した紐付けスクリプトを用いてシェアを結合してから配付する．そのため，結合されていない情報を配付されたシェアからは求めることができず，第三者が紐付け情報を作成したとしても意味をなさない．よって，紐付け情報の作成を制限している．

情報源が復元 PC に配付するシェアストレージ群の情報を保持していなければシェアストレージ群にアクセスすることができない．よって，シェアを保管しているストレージへのアクセスを制限している．

よって提案システムは要件をすべて満たす．

3.5　部分復元可能な秘密分散システムの問題と不正復元を防ぐ要件の定義

提案システムでは，何らかの方法で情報源が作成する部分復元制御データを入手することができれば，第三者に不正に被災地で活用する医療データを復元される可能性がある．医療データは個人情報であるため，第三者に不正に復元されないようにする必要がある．よって，システムを被災地での医療行為に活用するためには，不正復元を防ぐ対策を講じる必要がある．

本節では，提案システムから情報が洩れる点を各端末間のデータのやりとりごとに整理し，提案システムでの不正復元を防ぐ要件を定義する．さらに，要件を満たすような状態遷移を示す．

提案システムから復元に必要な情報が洩れる点は，各地点間の通信と各拠点に設置してあ

表 3.1　洩れるデータの分類

情報が洩れると発生する問題	洩れるデータ
しきい値以上洩れると不正復元	全患者のシェア 紐付け済シェア (災害) シェアストレージ群の情報 (災害)
しきい値以上洩れるとなりすまし	DB 作成スクリプト 紐付けスクリプト シェアストレージ群の情報 (病院)
他のデータと組み合わせると不正復元	復元スクリプト 改竄確認スクリプト
一つでも洩れると情報漏洩	復元 PC の情報 患者の本人識別情報 患者の医療データ
問題なし	データ整形スクリプト

る端末の 2 点である．表 3.1 は洩れるデータを分類した表である．表 3.1 より，シェア関連のデータはしきい値以上データが洩れると不正に復元されるデータに分類することができる．これらのデータはしきい値未満洩れたとしても問題はない．

データが洩れるとなりすましつながるデータに分類されるのは，シェアを保管するシェアストレージ群に事前情報として配付する DB 作成スクリプトと紐付けスクリプトである．また，シェアストレージ群の情報 (病院) はシェアストレージの管理ユーザも兼ねているため，このデータが洩れるとシェアストレージが乗っ取られる可能性がある．

他のデータを一緒に洩れると組み合わせにより不正復元につながるデータの分類されるのは，データを復元する復元スクリプトである．復元スクリプト単一では意味をなさないが，シェアを入手することができれば医療データを復元することができる．また，改ざん確認スクリプトもシェアのハッシュ値と一緒に洩れると不正復元につながる可能性がある．

図 3.8　情報源と復元 PC 間でやりとりされるデータ

1 つでもデータが洩れると不正復元につながるデータは患者の情報と復元 PC の情報である．復元 PC の情報は復元 PC に接続するために必要な情報である．復元 PC は，患者個人を識別する情報とともに患者の医療データの要求があると自身が持っている医療データの中から患者個人を識別する情報とマッチするものを返す．そのため，復元 PC の情報と患者本人を識別する情報を保持している場合，患者の医療データを入手できる可能性がある．

以上のデータは各地点・端末でのやりとりや各端末から洩れる可能性がある．以降では各地点・端末でのやり取りで洩れるデータについて述べ，情報漏えいの条件を整理し，各地点・端末でのやり取りで満たすべき条件を定義する．そして，定義した条件を満たす状態遷移について述べる．

3.5.1　情報源と復元 PC 間のデータのやりとり

情報源と復元 PC 間のやりとりでは部分復元を行うために，情報源がシェアをバックアップする前に事前情報として復元に必ず必要なシェアストレージ群の情報と復元スクリプトのやり取りを行う．そのため，情報源と復元 PC 間でやり取りされるデータが洩れると第三者に不正復元されるリスクが他の地点・端末間のやり取りに比べ一番高い．情報源と復元 PC 間で流れるデータを図 3.8 に示す．

情報源から復元 PC に事前情報を配付する際に事前情報が洩れる可能性がある点は，情報源と復元 PC 間の通信と復元 PC の 2 点である．まず，災害時に医療データが必要になる拠点について述べる．

1. 災害医療拠点が開設される医療機関

3.5 部分復元可能な秘密分散システムの問題と不正復元を防ぐ要件の定義

医療拠点が開設される医療機関は平常時から定められているため，拠点の登録が可能である．また，災害医療拠点が開設される医療拠点は，医療データをバックアップした情報源と同等レベルのセキュリティレベルを確保していると考えることができる．そのため，復元 PC を安全な環境で保管することができる．

2. 自治体が避難所として定めた施設

自治体に避難所として定められている施設は平常時から定められているため，拠点の登録が可能である．避難所として定められている施設は平常時は別の施設として使用されていることが多く，施設の設備によっては復元 PC を平常時から設置できない可能性がある．このような施設に対しては，平常時復元 PC を自治体の安全な保管場所に保管しておき，災害時に保管場所から避難所に復元 PC を運搬することによって，平常時から復元 PC を設置することができない施設であったとしても災害時にバックアップした医療データを活用することができる．

3. 災害時人々が集まり避難所となった施設

災害時人々が集まり避難所となった施設は災害時に突然開設されるため，平常時から拠点として登録することができない上に，復元 PC を平常時から設置することができない．よって，このような施設でバックアップした医療データを活用するためには，災害発生時に施設を拠点として登録し，復元 PC を設置する必要がある．

次に，情報源が復元 PC に事前情報を配付する方法を以下に示す．

1. インターネットを用いて配付

平常時，医療データが必要となる拠点に設置されている復元 PC に対してインターネットを用いて事前情報を配付する事前情報の配付にインターネットを用いるため，情報源と拠点間がインターネットでつながっている必要がある．インターネットは第三者に盗聴される可能性があるため，事前情報が第三者に洩れる可能性がある．

2. リムーバブル媒体にデータを格納し配付

平常時・災害時ともに事前情報を格納したリムーバブル媒体を拠点に持っていき，拠

点に設置されている復元 PC に事前情報を配付する．事前情報の配付にインターネットを用いていないため，情報源とインターネットでつながっていない拠点にも事前情報を配付することができる．しかし，リムーバブル媒体を運搬中に盗まれたり，リムーバブル媒体の中身を覗き見される可能性がある．また，復元 PC 以外の端末に事前情報が流し込まれる可能性がある．

3. ノート PC に事前情報を格納し配付

　災害時，拠点に事前情報を流し込んだノート PC を持っていき，事前情報と復元 PC を配付する．復元 PC となるノート PC を用意して拠点まで持っていくため，拠点が被災してしまい復元 PC が使えない状態であったとしてもバックアップした医療データを活用することができる．また災害時人々が集まり，避難所となる拠点にも対応することができる．事前情報を格納した端末を拠点に持っていく点はリムーバブル媒体と同じため，リムーバブル媒体と同様に運搬中に盗まれたり中身を覗き見される可能性がある．

4. ノート PC のみを配付

　平常時情報源はクラウド上に事前情報を格納した復元 PC を作成しておく．災害時，拠点に何も情報が格納されていないノート PC を持っていき，クラウド上の復元 PC に接続し，事前情報を入手する．ノート PC に何も情報が格納されていないため，運搬中に盗まれたとしても事前情報が洩れることはない．また，災害時，情報源が被災していたとしても，クラウド上の復元 PC から事前情報を各地点の端末に配付することができる．しかし，クラウド上の復元 PC と通信することができなければ，拠点に持っていったノート PC を復元 PC として活用することができない．また，ノート PC とクラウド上の復元 PC との通信を第三者に盗聴されると，第三者に事前情報が洩れる可能性がある．

復元 PC が設置される可能性がある各拠点に以上のような方法で事前情報を配付した場合，事前情報が洩れる条件について整理する．事前情報が洩れる条件を図 3.9 に示す．

3.9 の○が付いているセルは事前情報が洩れない条件を示しており，その他のセルは事前

拠点		正当				不当			
端末		正当		不当				正当	
使用者		正当	不当	正当		不当		正当	
拠点間	情報								
もれる	わかる								
	わからない								
もれない		○							
	分かる	○							

図 3.9　復元 PC に事前情報を配付する際に洩れる条件

情報が洩れる条件を示している．拠点・端末・操作者が不正だった場合，情報源は第三者に事前情報を配付してしまうため，事前情報が第三者に洩れる．また，情報源と復元 PC 間の通信で事前情報が洩れると第三者に事前情報が洩れる．事前情報が第三者に洩れない条件を満たす要件を以下に示す．

要件 (1)　(「接続元拠点」⇔「登録拠点」) ∧ (「接続元端末」⇔「登録端末」) ∧ (「端末の操作者」⇔「登録操作者」) ⇒「事前情報配付」

要件 (2)　「端末の操作者」∧「端末の操作許可」⇒「端末の操作」

要件 (3)　「登録拠点」∨「登録端末」∨「登録操作者」⇒ ¬「情報漏えい」

要件 (4)　「盗難」∨「盗聴」⇒ ¬「情報漏えい」

要件 (1) を満たす状態遷移を図 3.10 に示す．要件 (1) は情報源から復元 PC に事前情報を配付する際に満たすべき要件である．情報源と復元 PC 間のやり取りを行う前に，情報源は拠点・端末・操作者の情報を登録する．情報源が復元 PC に事前情報を配付する前に，登録情報を用いて拠点・端末・操作者が正当なものであるかを確認する．正当なものであることが確認できれば，情報源は事前情報を復元 PC に配付する．拠点・端末・操作者のうち 1 つでも不当なものがあった場合，情報源は事前情報を配付しない．なお，接続元の拠点のうち，自治体であらかじめ定められた避難所のような平常時から復元 PC を設置できない拠点に対しては，図 3.10 の状態遷移に加え，平常時に復元 PC を保管する保管場所の登録・確認を追加する．このような場合の状態遷移を図 3.11 に示す．また，何も情報の入っていな

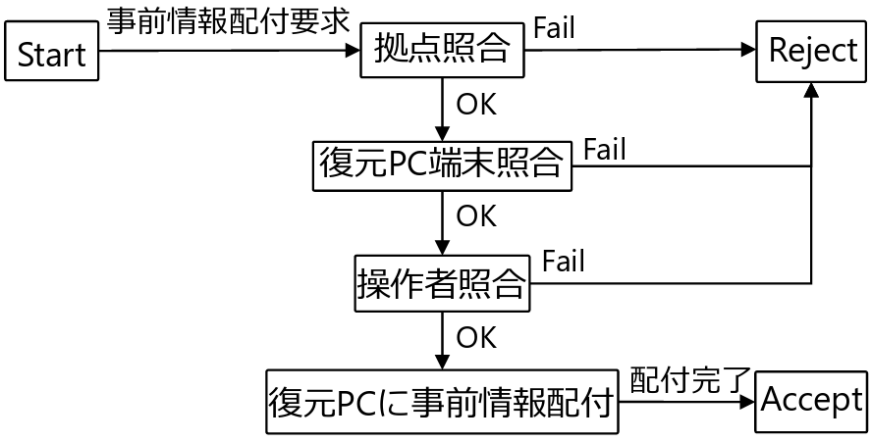

図 3.10　情報源から復元 PC に事前情報を配付する際の状態遷移

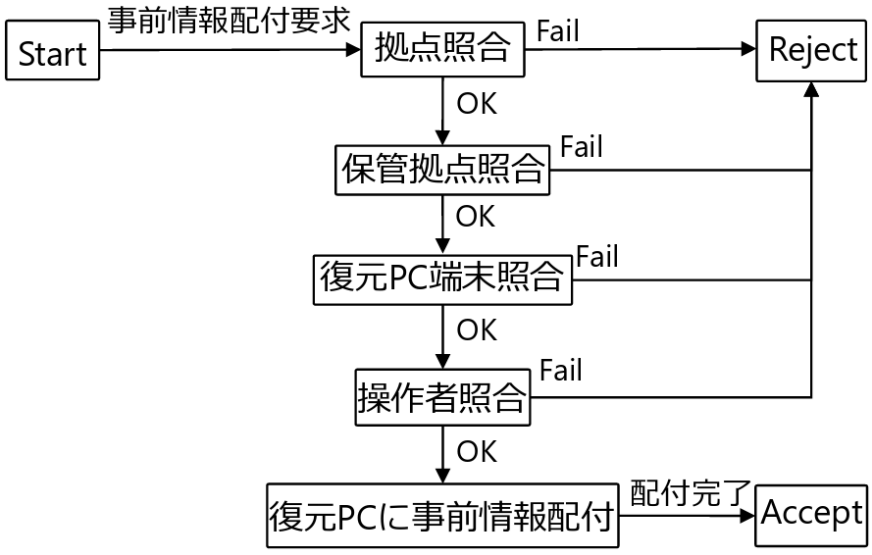

図 3.11　平常時に復元 PC を設置できない場所に対して事前情報を配付する際の状態遷移

いノート PC を拠点に配付し，クラウド上の復元 PC から事前情報を入手する方法で事前情報を入手する場合は，図 3.10 の状態遷移に加え，操作者がクラウド上の復元 PC に接続するか可能かどうかの確認を追加する．このような場合の状態遷移を図 3.12 に示す．

要件 (2) を満たすための状態遷移を図 3.13 に示す．要件 (2) は復元 PC の操作者が復元 PC の操作を行う際に満たすべき要件である．復元 PC は操作者が復元 PC の操作を行う前に，操作者が復元 PC の操作権の有無を確認し，操作権がある場合のみ自身の操作を許可する．以上の要件を満たすことによって第三者に事前情報が洩れない条件を満たすことがで

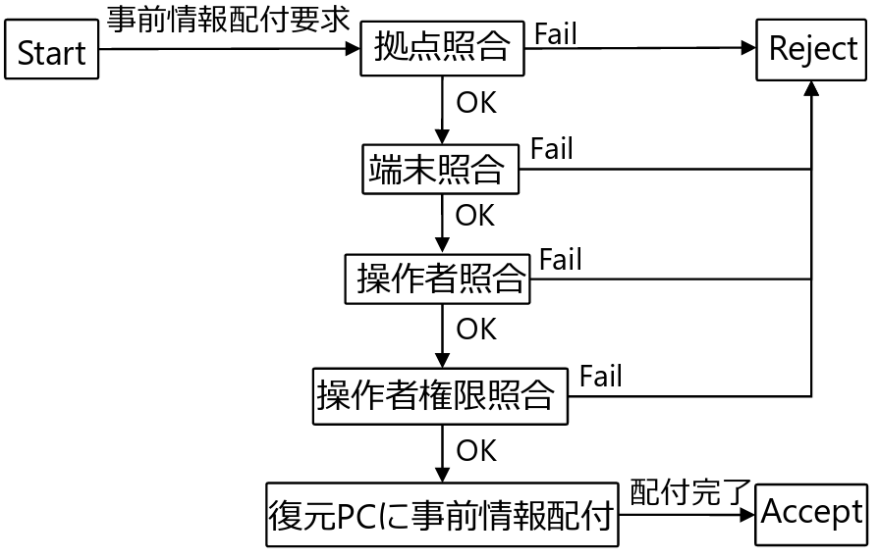

図 3.12　災害時にクラウド上の復元 PC から事前情報を入手する際の状態遷移

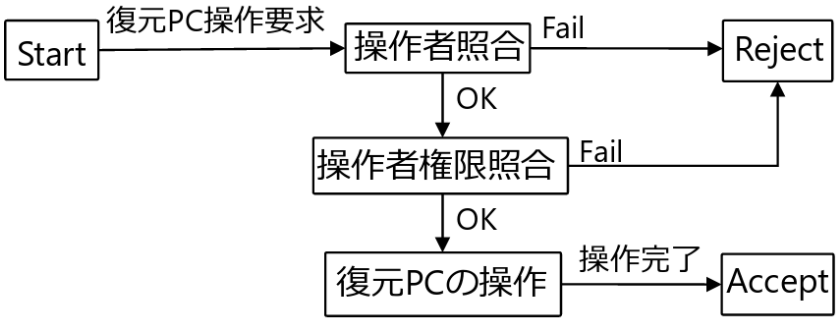

図 3.13　復元 PC の操作権取得の状態遷移

きる．

以上の要件のみでは正当な拠点で事前情報を受け取ることができない場合がある．要件 (1) では，接続元の拠点・端末・操作者のすべてが登録されている場合，情報源は事前情報を配付することを示している．よって，登録情報が誤っている場合，正当な拠点・端末・操作者に事前情報を配付することができない．また，登録情報が偽装されていたり，登録されている拠点・端末・操作者になりすまして事前情報の要求をしてきたとしても情報源は検知することができない．そのため情報源は，不正な拠点・端末・操作者に事前情報を配付してしまう可能性がある．このような問題が起きる条件を図 3.14 に示す．表 3.14 の○が付いてい

入力情報		確認する	確認しない
登録情報の置き場所	第三者と結託		
特定の人のみ	しない	○	
	する		
全員			
	しない		

図 3.14　正当な拠点が事前情報を受け取れる条件

るセルは正当な拠点が事前情報を受け取ることができる条件を示しており，その他のセルは事前情報を受け取ることができない条件を示している．情報源が拠点・端末・操作者を登録する際に，入力情報が誤っている場合，正当な相手に事前情報を配付することができない．また、操作者が第三者と結託している場合，情報源が登録している相手に事前情報を配付したとしても第三者に事前情報が洩れる．登録している拠点・端末・操作者の登録情報を第三者が入手可能な場所に保管しておくと，第三者に登録情報を知られ，登録している拠点・端末・操作者になりすまされ，事前情報が第三者に洩れる．正当な拠点が事前情報を受け取れる条件を満たす要件を以下に示す．

要件 (5)　「登録情報の誤り確認」∧ ¬「第三者との結託」∧「登録情報の保管場所確認」⇒「登録」

要件 (5) を満たすための状態遷移を図 3.15 に示す．要件 (5) は情報源が復元 PC を設置する拠点・端末・操作者を登録する際に満たすべき要件である．情報源は拠点・端末・操作者を登録する前に，登録情報に誤りがないかを確認する．誤りがなければ登録する操作者が第三者と結託していないかどうかを確認する．結託していないことを確認したあと，登録した拠点・端末・操作者が登録情報を安全な場所に保管できるかどうかを確認し，保管できるのであれば登録をおこなう．

以上 (1)〜(5) の要件を満たすことによって情報源から復元 PC に対して事前情報を安全に配付することができる．

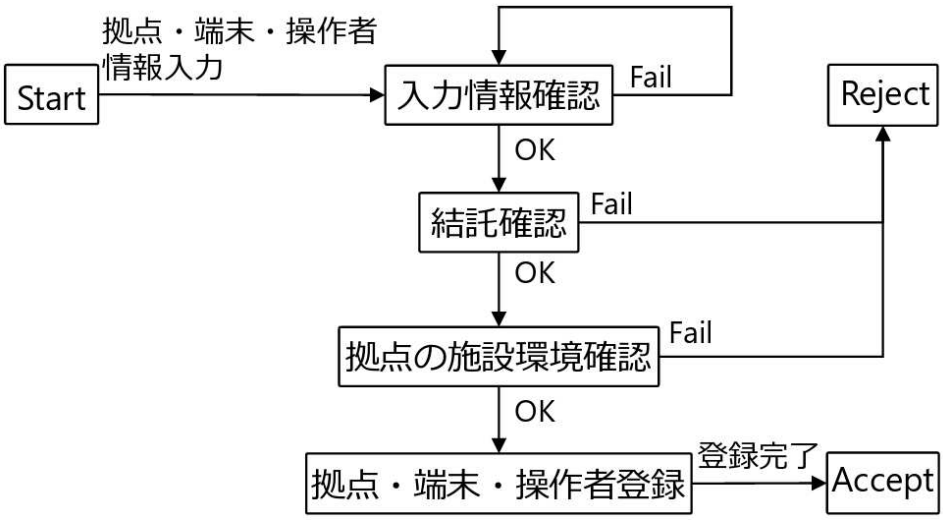

図 3.15　拠点・端末・操作者を登録する際の状態遷移

図 3.16　情報源とシェアストレージ群でやりとりされるデータ

3.5.2　情報源からシェアストレージ群へのデータのやり取り

情報源とシェアストレージ群間のデータのやり取りは 2 種類ある．情報源が作成する部分復元制御データやりとりと，情報源が医療データをバックアップする際のシェアのやりとりである．それぞれのやりとりで洩れるデータを図 3.16 に示す．

情報源とシェアストレージ群の間でデータのやり取りを行う際にデータが洩れる可能性がある点は，情報源とシェアストレージ群間の通信とシェアストレージ群である．シェアストレージとなるストレージを用意する方法は 2 種類ある．1 つ目は情報源自身がストレージを

脆弱性・ウイルス対策	あり		なし	
ユーザ確認	あり	なし		あり
盗聴対策				
あり	○			
なし				

図 3.17　情報源からシェアストレージ群のやりとりでデータが洩れる条件

用意する方法である．2 つ目は情報源が外部機関が用意しているクラウド上のストレージを借りて用意する方法である．

情報源からシェアストレージ群間の通信にはインターネットを用いる．情報源からシェアストレージ群のやりとりでデータが洩れる条件を図 3.17 に示す．図 3.17 の○がついてるセルはデータが洩れない条件を示しており，それ以外のセルはデータが洩れる条件を示している．シェアストレージとなるストレージがウイルスに感染している場合や脆弱性対策が施されていない場合，ストレージからシェアが洩れる可能性がある．また，お互いの通信相手が不当であった場合や通信路に盗聴対策が施されていなかった場合データが洩れる．情報源とシェアストレージ群間のやり取りでデータが洩れないようにするために満たすべき要件を以下に示す．

要件 (1) 「病院ユーザ 1」∧ 「病院ユーザ 2」∧ . . . ∧「病院ユーザ n」⇒ 「不一致」

要件 (2) 「ストレージ」∧ 「脆弱対策」∧ 「ウイルス対策」 ∧ ¬「シェア以外の情報」⇒ 「シェアストレージの登録」

要件 (3) 「ユーザ」∧ 「病院ユーザ」∧ 「登録シェアストレージ」∧ 「盗聴対策」 ⇒ 「通信開始」

要件 (1) はシェアストレージのなりすましを防ぐために，シェアストレージの管理ユーザを兼ねている病院ユーザが満たすべき要件である．

要件 (2) はシェアストレージから情報が洩れることを防ぐためにストレージをシェアストレージとして登録する際に満たすべき要件である．要件 (2) を満たすための状態遷移を図

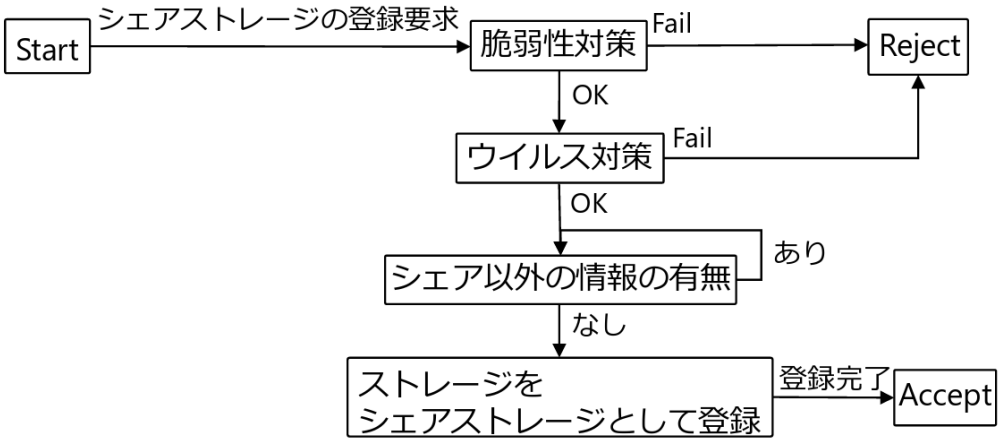

図 3.18　ストレージをシェアストレージとして登録する際の状態遷移

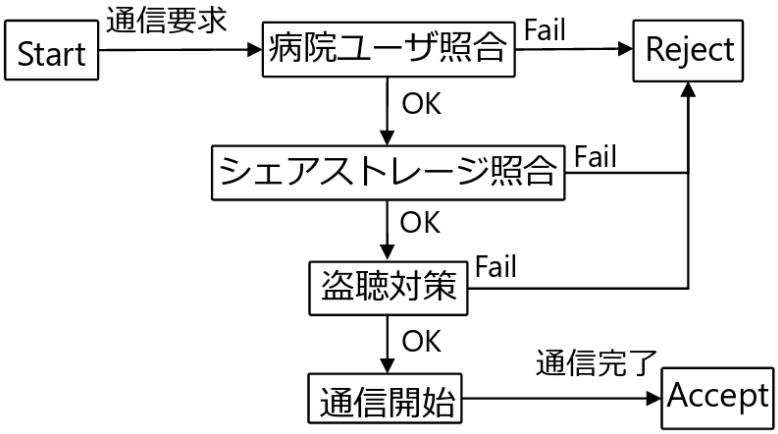

図 3.19　情報源とシェアストレージが通信する際の状態遷移

3.18 に示す．ストレージをシェアストレージとして登録する際は，ストレージに脆弱性対策・ウイルス対策が施されているか，ストレージにシェア以外の情報が格納されていないかを確認する．確認ができた場合登録し，確認できなかった場合登録しない．

要件 (3) は通信路での情報漏えいを防ぐための要件である．要件 (3) を満たすための状態遷移を図 3.19 に示す．情報源はあらかじめ病院ユーザを持つ人とシェアストレージを登録しておく．情報源とシェアストレージが通信を開始する前に，相手が登録されているか，盗聴対策がされているかを確認する．確認できなかった場合要求を破棄する．

以上の要件を満たすことによって，情報源とシェアストレージ群間のデータのやり取りを

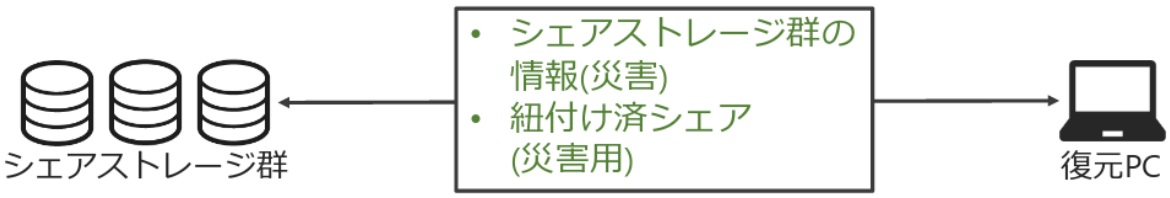

図 3.20　復元 PC とシェアストレージ群間でやりとりされるデータ

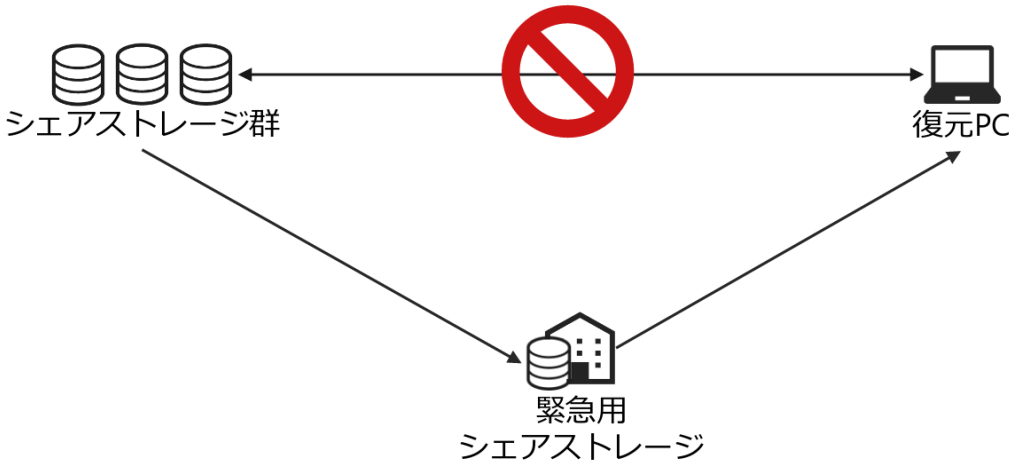

図 3.21　緊急用時に設置される緊急用シェアストレージ

安全に行うことができる．

3.5.3　復元 PC とシェアストレージ群間のデータのやり取り

復元 PC とシェアストレージ間のやり取りでは，復元に必要なシェアのやり取りを行う．復元 PC とシェアストレージ群間でやりとりされるデータを図 3.20 に示す．

災害時，復元 PC とシェアストレージ群間の経路が被災し，復元 PC はシェアストレージ群からシェアを入手できない可能性がある．このような場合，図 3.21 のようにシェアストレージ群と通信可能な拠点でシェアストレージ群から医療データの復元に必要なシェアをダウンロードし，緊急用のシェアストレージを作成する．復元 PC はシェアストレージ群との通信が可能な拠点に設置された緊急用のシェアストレージからシェアを入手すること被災地での医療行為に必要な医療データのシェアを入手することができる．

3.5　部分復元可能な秘密分散システムの問題と不正復元を防ぐ要件の定義

緊急用のシェアストレージを設置する場所を以下に示す．

1. 災害時に医療データを活用する拠点

   災害時に医療データを活用する拠点は，災害拠点病院や避難所などの施設である．医療データを活用するということは医療データの復元を行ってもよいため，緊急用のシェアストレージにはしきい値以上のシェアを格納してもよい．よってこのような拠点に設置される緊急用シェアストレージからシェアを入手できる確率は 1 となる．

2. 災害時に医療データを活用しない拠点

   医療データを活用しない拠点で復元可能であれば，第三者に医療データを閲覧させることになるため，復元を防ぐ必要がある．よって災害時に医療データを活用しない施設に緊急用のシェアストレージを設置する場合には，医療データを復元できないしきい値未満のシェアを緊急用のシェアストレージに格納しなければならない．緊急用のシェアストレージに格納するシェアの数は，

$$\left\lceil \frac{n}{(k-1)} \right\rceil$$

   以下となる．シェアを入手するためには 2 台以上の緊急用のシェアストレージにアクセスする必要がある．よってシェアを入手できる確率 P_a は，

$$P_a = \frac{2}{\left\lceil \frac{n}{(k-1)} \right\rceil} \tag{3.1}$$

   となる．

復元 PC がシェアストレージ群および緊急用シェアストレージからシェアを入手する方法を以下に示す．

端末	あり		なし	
ユーザ	あり	なし		あり
拠点に侵入検知				
あり	○			
なし				

図 3.22　復元 PC とシェアストレージ群間でシェアが洩れる条件

1. シェアストレージ群からインターネットを用いてシェアを入手

   災害時に復元 PC としきい値以上のシェアストレージとの経路が使用可能な場合，インターネットを用いてシェアを入手する．n 台のシェアストレージのうち k 台のシェアストレージにアクセスできればシェアを入手することができるため，シェアを入手できる確率 P は，

   $$P = \frac{k}{n} \tag{3.2}$$

   となる．

2. 緊急用のシェアストレージからネットワークを用いてシェアを入手

   復元 PC と緊急用のシェアストレージ間の経路が生きている場合，復元 PC は緊急用のシェアストレージからネットワークを用いてシェアを入手する．

3. 緊急用のシェアストレージからリムーバブル媒体を用いてシェアを入手

   復元 PC と緊急用のシェアストレージ間の経路が被災し利用できない場合，復元 PC は緊急用シェアストレージからリムーバブル媒体を用いてシェアを入手する．

復元 PC とシェアストレージ群とのやり取りでシェアが洩れる条件を整理する．シェアが洩れる条件を図 3.22 に示す．

図 3.22 の○が付いているセルはシェアが洩れない条件を示しており，その他のセルは洩れる条件を示している．復元 PC とシェアストレージ群とのやり取りは主にインターネットを用いて行うため，盗聴の危険性がある．復元 PC とシェアストレージ群との経路が被災し使えなかった場合，リムーバブル媒体を用いてシェアを配付するが，配付中にリムーバブル媒体が盗難にあう可能性がある．

3.5　部分復元可能な秘密分散システムの問題と不正復元を防ぐ要件の定義

緊急用のシェアストレージは災害時に作成されるため，シェアの要求を送ってきた復元 PC が正当なものであるかを判断することができず，不正な復元 PC にシェアを配付する可能性がある．逆に復元 PC も緊急用のシェアストレージが正当なものであるか判断することができず，不正なシェアが混入し医療データを復元できない場合がある．また，緊急用のストレージにはシェアが格納されているため，特定の人のみが触れる場所に設置しなければならないが，緊急用ストレージは災害時に作成されるため，特定の人のみが触れる場所に設置できない可能性がある．特に，災害時医療データを使わない施設では災害時にそのような場所を用意できるかわからない．シェアストレージ群から復元 PC へシェアを配付する際に緊急用シェアストレージを経由すると，シェアストレージ群から直接シェアを入手するよりもシェアを入手しやすくなるため，第三者にシェアを不正に入手される可能性がある．

復元 PC とシェアストレージ群および緊急用のシェアストレージとのやりとりでシェアが洩れない要件を以下に示す．

要件 (1)　(「復元 PC」⇔ 「登録端末」)∧「シェアストレージ群の情報 (災害)」∧「盗聴対策」⇒「シェアを配付」

要件 (2)　(「シェアの操作者」⇔「登録操作者」)∧ 「シェアストレージ群の情報」∧「盗聴対策」⇒「シェアストレージからシェアの入手」

要件 (3)　(「シェアの操作者」⇔「登録操作者」)∧(「施設」⇔「登録施設」)⇒「シェアストレージ群の情報 (災害) を配付」

要件 (4)　(「シェアの操作者」⇔「登録操作者」)∧(「施設」⇔「登録施設」)∧「シェアストレージ群の情報 (災害) の有無」⇒「シェアストレージ群からシェアを配付」

要件 (5)　(「シェアの操作者」⇔「登録操作者」)∧「外部とのネットワーク接続」∧「侵入検知」∧「復元 PC へ通知」⇒「緊急用のシェアストレージを設置する施設として登録」

要件 (1) はシェアストレージ群と復元 PC 間でシェアが洩れるのを防ぐために，シェアストレージ群が復元 PC にシェアを配付する際に満たすべき要件である．要件 (1) を満たす状態遷移を図 3.23 に示す．シェアストレージ群はまず自身に接続してきた復元 PC が正当な

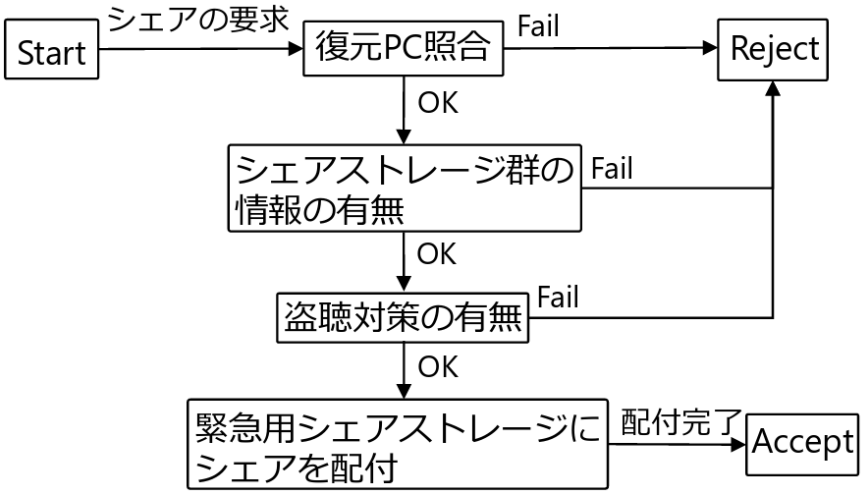

図 3.23　シェアストレージが復元 PC にシェアを配付する際の状態遷移

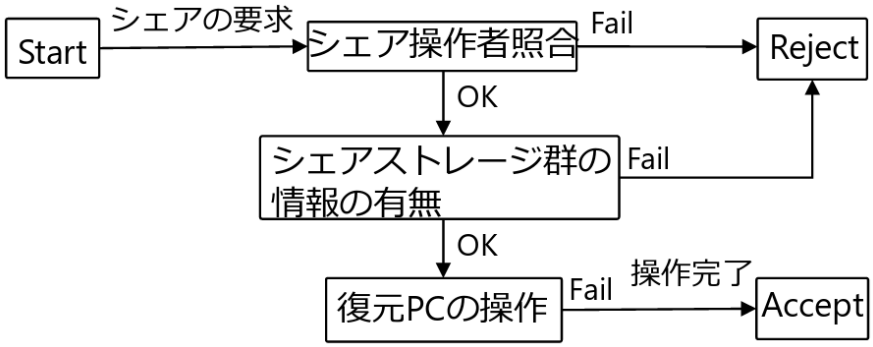

図 3.24　災害時医療データを使用する拠点に緊急用のシェアストレージを設置する際の状態遷移

復元 PC であるかを確認し，復元 PC がシェアストレージ群の情報 (災害) を持っているかを確認する．復元 PC とシェアストレージ群の間の通信経路に盗聴対策が施されているかを確認し，確認後シェアストレージ群は復元 PC にシェアを配付する．

要件 (2) は緊急用のシェアストレージを災害時医療データを活用する拠点に設置する際に満たすべき要件である．要件 (2) を満たす状態遷移を図 3.24 に示す．災害時に医療データを活用する拠点は，自身の拠点に緊急用のシェアストレージを作成する権限を持った人間がいるかどうかを確認する．権限を持った人間がいた場合，権限を持った人間が緊急用のシェアストレージとなる端末を用意しシェアストレージ群の情報 (災害) を用いてシェアストレージ群からシェアをダウンロードして緊急用のシェアストレージを作成する．

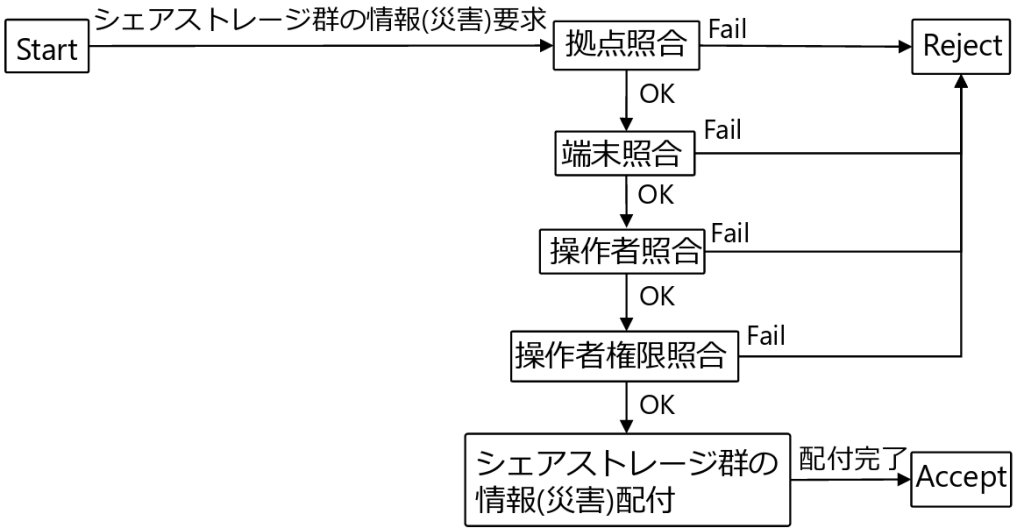

図 3.25　災害時医療データをしない拠点にシェアストレージ群の情報 (災害) を教える際の状態遷移

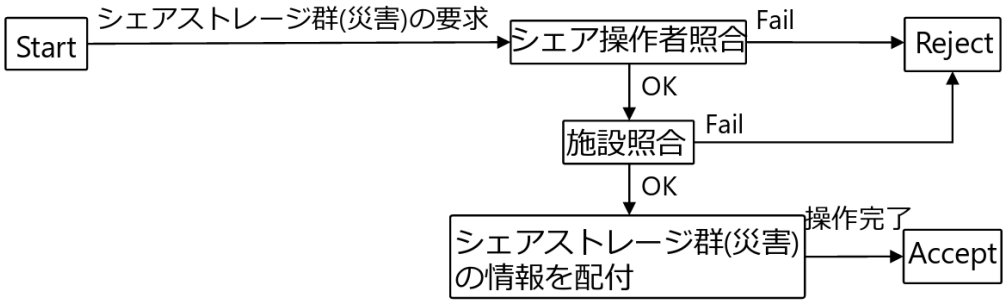

図 3.26　災害時医療データを使用する拠点に緊急用のシェアストレージを設置する際の状態遷移

要件 (3) と要件 (4) は緊急用のシェアストレージを災害時医療データを活用する拠点に設置する際に満たすべき要件である．要件 (3) を満たす状態遷移を図 3.25 に示す．災害時に医療データを活用しない拠点はシェアストレージ群の情報 (災害) を持っていないため入手する必要がある．情報源は拠点が緊急用のシェアストレージを設置する拠点と，ユーザが緊急用のシェアストレージを作成可能な人かを確認してから，シェアストレージ群の情報 (災害) を配付する．要件 (4) を満たす状態遷移を図 3.26 に示す．シェアストレージ群の情報 (災害) を入手後，権限を持った人間がシェアストレージ群からシェアをダウンロードし緊急用のシェアストレージを作成する．

要件 (5) は災害時に医療データを活用しない拠点を緊急用のシェアストレージを設置する

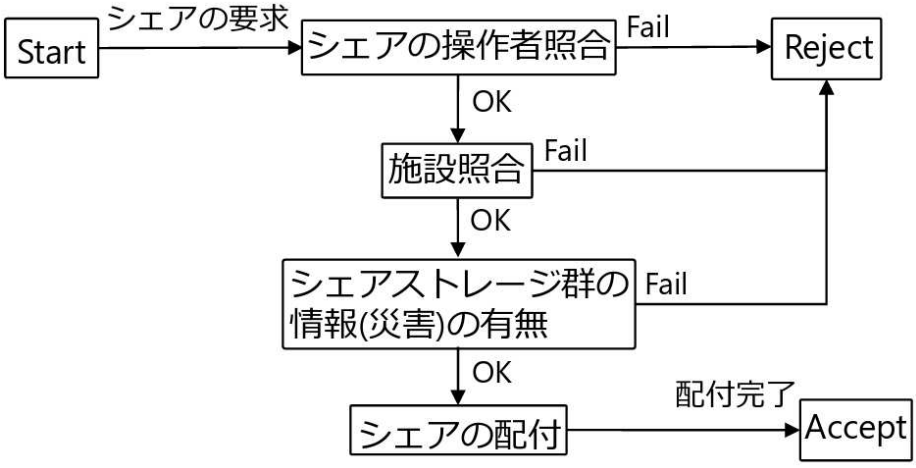

図 3.27　災害時医療データを使用しない拠点を緊急用のシェアストレージを設置する拠点に登録する際の状態遷移

拠点として登録する際に満たすべき要件である．要件 (5) を満たす状態遷移を図 3.27 に示す．まず，情報源が拠点の人間に緊急用のシェアストレージを作成する権限を与え登録する．次に，緊急用のシェアストレージを設置する拠点の通信回線が耐災害性があるかを確認する．次に，緊急用のシェアストレージを設置する場所に，情報源が権限を与えた人間以外が侵入してきた場合に侵入を検知する仕組みがあるかを確認する．最後に情報源が登録している各復元 PC に自身が緊急用のシェアストレージを持っていることを通知する方法があるかを確認する．全ての確認がとれた場合，情報源がその拠点を緊急用のシェアストレージを設置する拠点として登録する．

以上全ての要件を満たすことによってシェアストレージ群から復元 PC に安全にシェアを配付することができる．

3.5.4　復元 PC と情報閲覧端末間のデータのやり取り

復元 PC と情報閲覧端末間のやり取りでは，患者の医療データや個人情報のやり取りを行う．復元 PC と情報閲覧端末間で流れるデータを図 3.28 に示す．

復元 PC と情報閲覧端末間の通信は災害時に医療データを扱う拠点のみで行うためローカ

3.5　部分復元可能な秘密分散システムの問題と不正復元を防ぐ要件の定義

図 3.28　復元 PC と情報閲覧端末で流れるデータ

事前情報配布者			正当		不当	
医師確認			できた	できない		できた
情報閲覧端末	医療データ保存可能	盗聴対策				
正当	できる	有				
		無				
	できない					
		有	○			
不当						
		無				
	できる					
		有				

図 3.29　復元 PC から情報閲覧端末間でデータが洩れる条件

ルエリアネットワーク通信を用いる．そのため，第三者が災害時に医療データを扱う拠点でのローカルエリアネットワークに参加された場合や盗聴されると被災地での医療行為に必要な医療データと患者の個人識別に必要な情報が洩れる．また，情報閲覧端末に復元 PC から入手した医療データを保存し持ち帰られた場合や，他の端末に医療データを送信されると，被災地で医療行為を行うために必要な医療データが洩れる．

復元 PC と情報閲覧端末間でデータが洩れる条件を図 3.29 に示す．図 3.29 の○がついているセルはデータが洩れない条件を示しており，その他のセルはデータが洩れる条件を示している．ローカルエリアネットワーク通信を行うためには，ローカルエリアネットワークの情報が必要になる．この情報は平常時に復元 PC から事前情報として情報閲覧端末に送信される．このとき，情報閲覧端末以外に事前情報を配付してしまうと第三者に情報が洩れる可能性がある．

復元 PC と情報通信端末間でデータが洩れないような要件を示す．

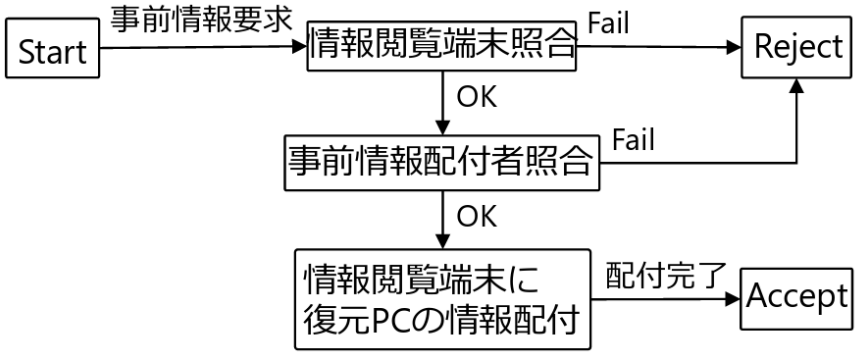

図 3.30　復元 PC から情報閲覧端末に事前情報を配付する際の状態遷移

要件 (1) 「情報閲覧端末」∧ 「登録端末」∧ 「事前情報配付者」∧ 「登録者」⇒ 「事前情報配付」

要件 (2) 「医師」∧ 「情報閲覧端末」∧ ¬「医療情報保存」∧ 「盗聴対策」⇒ 「使用開始」

要件 (1) は復元 PC から情報閲覧端末に事前情報を配付する際に満たすべき要件である．要件 (1) を満たすような状態遷移を図 3.30 に示す．復元 PC は情報閲覧端末に事前情報を配付する前に，情報閲覧端末が正当なものかを確認する．そして，情報閲覧端末に事前情報を流し込む人間が正当な人間であるかを確認し，復元 PC から情報閲覧端末に事前情報を配付する．

要件 (2) は情報閲覧端末に医療データを配付するために満たすべき要件である．要件 (2) を満たす状態遷移を図 3.31 に示す．まず，情報閲覧端末を所持している人間が医療関係者であるかを確認する．確認方法は医療関係者のみが知りうる情報について尋ね，正しい返答があった場合医療関係者であると判断する．次に，情報閲覧端末が登録されているかを確認する．次に，情報閲覧端末に医療データを保存することができないかを確認する．最後に情報閲覧端末と復元 PC 間の通信路に盗聴対策が施されているかを確認し，情報閲覧端末に医療データを配付する．

以上の要件を満たすことによって，復元 PC から情報閲覧端末間のデータのやり取りを安全に行うことができる．

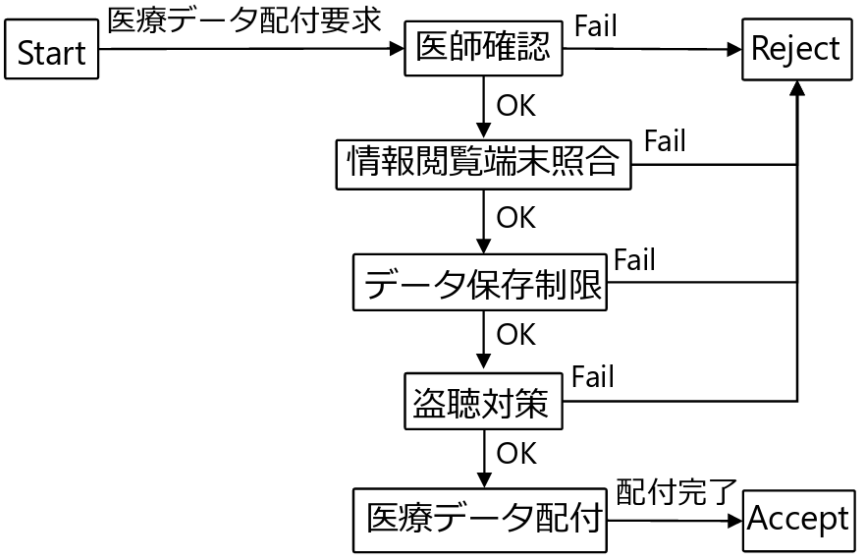

図 3.31　情報閲覧端末に医療データを配付する際の状態遷移

3.6　まとめ

本章では，分散バックアップした医療データを被災地での医療行為に活用するために，部分復元アルゴリズムを用いた部分復元可能な秘密分散システムを提案した．さらにシステムの問題点を整理し，システムでの不正復元を防ぐ要件を定義した．

部分復元アルゴリズムは紐付け情報とシェアが何らかの方法で第三者に洩れると不正に復元される恐れがある．そこで，提案システムではデータをバックアップする情報源の病院が紐付け情報とシェアの入手を制限する部分復元の制御データを作成し，事前情報として復元 PC とシェアストレージに配付する．シェアストレージは部分復元制御データを元にシェアを結合して配付するため，第三者が紐付け情報を作成したとしても，結合したシェアを操作することはできない．シェアを入手するためには部分復元制御データが必要になるため，情報源から部分復元制御データを入手していなければシェアを入手することは困難である．よって不正復元を防ぐ．

しかし，情報源が作成する部分復元制御データが第三者に洩れると不正に復元される可能性がある．部分復元制御データが洩れる点は各端末と情報源と端末間の経路である．特に復元 PC に事前情報として配付する部分復元制御データには復元に必要な情報がすべて揃って

いるため洩れると不正復元される可能性が高い．よってそれぞれの端末間のやりとりで洩れる条件を整理し，それぞれのやりとりで満たすべき要件を定めた．さらに要件を満たす状態遷移を示した．状態遷移を施した対策を行うことによって不正復元を防ぐことができる．

第 4 章

不正復元を防ぐ部分復元可能な秘密分散システムの評価

本章では，部分復元可能な秘密分散システムと提案システムでの不正復元を防ぐ要件の評価を行う．初めに部分復元可能な秘密分散システムの評価を行い，次に不正復元を防ぐ要件を評価する．最後に，要件をすべて満たした理想的なシステムの考察を行う．

4.1 部分復元可能な秘密分散システムの評価

本節では不正復元を防いだ部分復元可能な秘密分散システムの評価を行う．

提案システムは秘密分散法を使って，医療データからシェアを生成しバックアップを行っている．このため，データの秘匿化と冗長化ができる．さらに，シェアを保管するシェアストレージの設置場所を分散することで，耐災害性が向上する．

提案システムでは部分的な復元と全ての復元を同一シェアから行うことができる．よって，バックアップデータの容量は普通の秘密分散法と変わらない．しかし，部分復元アルゴリズムには生成したシェアの個数が秘密分散法で生成したシェアの個数より，分割したデータ d 個分だけ増えるため，シェアの管理が大変になる．提案システムでは，DB を用いてシェアの管理を行っている．さらに，必要なシェアの選別はスクリプトを用いて自動で行うため，シェアの煩雑な管理を行う必要がない．

提案システムでは，部分復元制御データの 1 つである紐付けスクリプトを用いて結合してからシェアを配付している．また医療データの利用形態に応じて結合してから配付するシェ

アを変更することで，被災地での医療行為に不必要な情報の復元を制限している．仮に，被災地での医療行為で必要な情報が増えた場合，情報源から新しい紐付け情報をシェアストレージ群に配付し結合するシェアを変更することで必要な情報を入手することができる．また，第三者が紐付け情報を作成し，何らかの方法で不正入手したシェアを結合しようとしても，紐付け情報では結合済みのシェアを操作することができない．このように，部分的に復元する項目を情報源が制限している．シェアの入手には制御データの 1 つであるシェアストレージ群の情報が必要になる．シェアストレージ群の情報を持っていない場合はシェアの要求を破棄する．シェアストレージ群の情報は，情報源とその他のユーザに分かれており，配付されるシェアが異なる．以上より，情報源が部分復元制御データを用いて部分復元を制御し，不正復元を防いでいることがわかる．

提案システムを用いることで，不正復元を防いだ部分復元を行うことができる．

4.2　不正復元を防ぐ要件の評価

本節では，提案システムでの不正復元を防ぐ要件に対する評価について述べる．それぞれの地点・端末間のやりとりで定めた要件についてそれぞれ評価し，最後に全ての要件を満たす具体的な対策を施したシステムでの実証実験について述べる．

提案システムでは部分復元システム制御データが洩れると不正に復元される可能性がある．部分復元制御データが洩れる点としては，部分復元制御データを受け取る端末と情報源と端末間の経路である．前章では各地点・端末間のやりとりごとにデータの不正入手を防ぐ要件を定義し要件を満たす状態遷移を示した．前章で示したそれぞれの要件と状態遷移についてそれぞれ評価する．

4.2.1　情報源と復元 PC 間の要件の評価

情報源と復元 PC 間のやりとりでは，復元に必ず必要な部分復元制御データであるシェアストレージ群の情報 (災害) と復元スクリプトのやりとりを行う．情報源と復元 PC 間のや

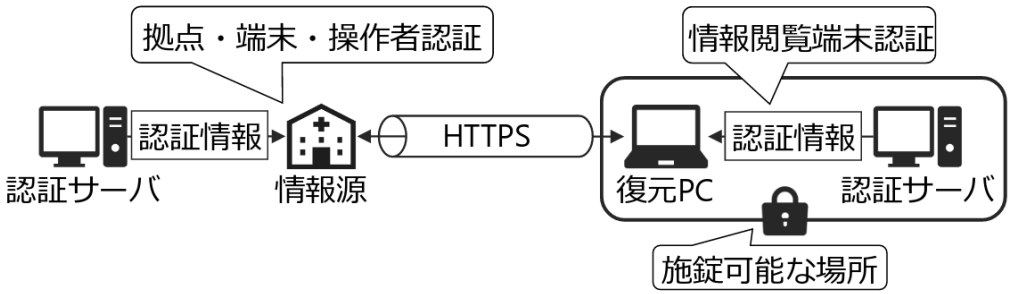

図 4.1　情報源と復元 PC 間のデータのやりとりに対する要件を満たす具体的な対策

りとりするデータが洩れると第三者に不正に復元される可能性がある．よって，情報源と復元 PC 間のデータのやりとりに対する要件では，通信相手の確認と通信路での盗聴盗難への対策を行うことを定めた．さらに追加要件として，通信相手の情報を登録する際に誤り防止と第三者との結託を防止した要件を定義した．要件を満たす状態遷移が可能な具体的な対策を図 4.1 に示す．

復元 PC を設置する拠点は復元 PC を施錠可能な場所に設置し鍵を保持していない第三者が侵入した場合，拠点を管理する人に連絡が入るようにする．情報源は復元 PC を保持している拠点，復元 PC の端末，復元 PC を操作する人の情報を認証サーバに登録し，事前情報を配付する前に認証サーバを用いて確認する．情報の登録は 2 人以上で行い登録ミスを防止する．以上の対策を施すことによって，事前情報の漏えいを防ぐことができる．しかし，現状の技術では復元 PC の操作者と第三者の結託を検知することができない．復元 PC の操作者は医療従事者であるため，第三者との結託が発生する可能性は低いと考えられる．また，災害時に復元 PC を施錠可能な場所に設置できない可能性がある．

4.2.2　情報源とシェアストレージ群間の要件の評価

情報源とシェアストレージ群間では部分復元制御データである紐付け情報とシェアのやりとりが行われる．情報源とシェアストレージ群間でやりとりされるデータが洩れるとシェアストレージになりすまされる可能性がある．紐付け情報は SQL 文以外はシェアと同様に意味のない文字列で記述されており，紐付け情報をしきい値以上集めることによって紐付け情

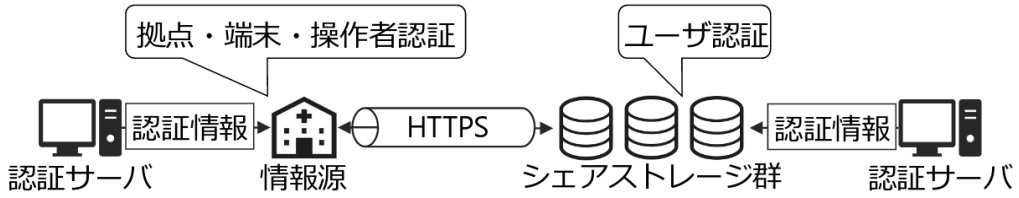

図 4.2　情報源とシェアストレージ群間のデータのやりとりに対する要件を満たす具体的な対策

報の内容を復元することができる．よって，情報源とシェアストレージ群の間でやりとりされるデータは，しきい値以上洩れなければデータ漏えいは発生しない．しかし，情報源がシェアストレージに接続する際に用いる病院ユーザは，シェアストレージの管理ユーザも兼ねているため，シェアストレージ群の管理ユーザが単一であった場合しきい値以上のシェアストレージが乗っ取られる．また，しきい値以上のシェアストレージが外部からの攻撃に弱い場合しきい値以上の情報が洩れる可能性がある．そこで，情報源とシェアストレージ群間のデータのやりとりに対する要件では，病院ユーザの複数作成と外部からの攻撃対策を定めた．要件を満たす状態遷移が可能な具体的な対策を図 4.2 に示す．

情報源とシェアストレージ群はお互いに相手の情報と認証サーバに登録し，通信を開始する前に相手が正当であるかを認証サーバを用いて確認する．このとき，病院ユーザはシェアストレージごとに作成しシェアストレージに 1 つの病院ユーザが割り当てられるように登録する．さらに，盗聴対策として情報源とシェアストレージ群間の通信に HTTPS を用いる．以上の対策によってデータの不正入手を防ぐことができる．

4.2.3　復元 PC とシェアストレージ群間の要件の評価

復元 PC とシェアストレージ群間のやりとりではシェアのやりとりが行われる．復元 PC とシェアストレージ群間でやりとりされるデータがしきい値以上洩れると不正に復元される可能性がある．復元 PC とシェアストレージ群間のやりとりは災害時を想定しているため，復元 PC としきい値以上のシェアストレージ間の通信路が被災し利用できない可能性がある．そこで，しきい値以上のシェアストレージに接続可能な拠点に緊急用のシェアストレー

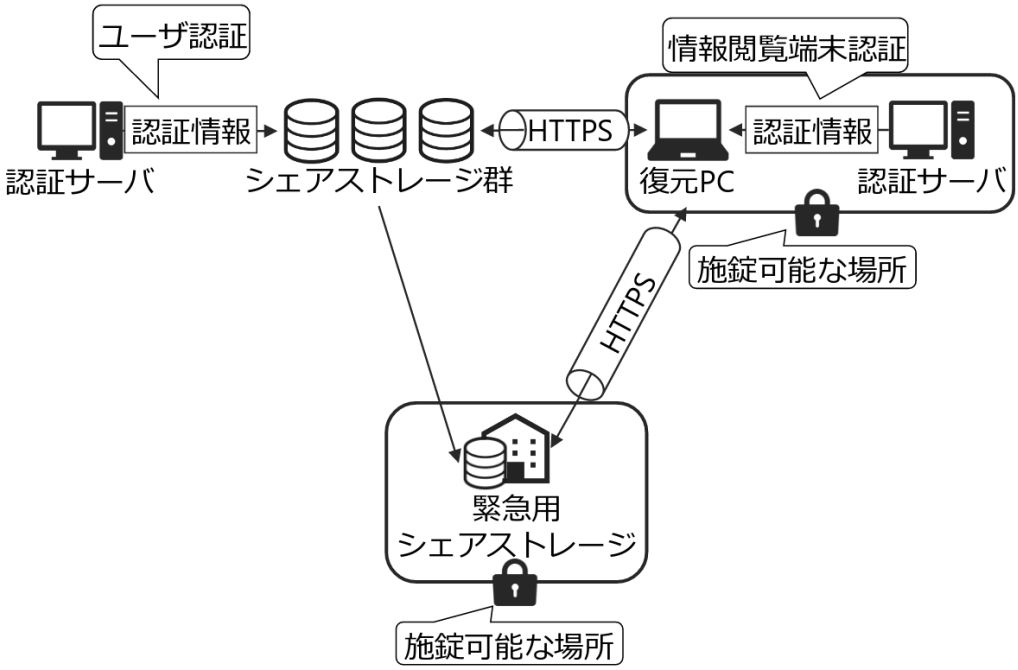

図 4.3　復元 PC とシェアストレージ群間のデータのやりとりに対する要件を満たす具体的な対策

ジを設置し，復元 PC は緊急用シェアストレージからシェアを入手するようにする．しきい値以上のシェアストレージに接続可能な拠点は災害時に医療データを活用しない拠点も含まれる．そのため緊急用のシェアストレージからシェアが洩れる可能性がある．よって，復元 PC とシェアストレージ群間のデータのやりとりに対する要件では，復元 PC とシェアストレージ群のデータのやりとりに加え，緊急用シェアストレージとのやりとりで不正な相手にシェアを配付することを防ぐ要件を定めた．要件を満たす状態遷移が可能な具体的な対策を図 4.3 に示す．

復元 PC とシェアストレージ群は通信相手を認証サーバに登録し，通信を開始する前に相手が正当であるかを認証サーバを用いて確認する．緊急用シェアストレージは鍵のかかる場所に設置し，鍵を持っていない第三者の侵入した場合緊急用シェアストレージを作成した人に連絡が入るようにする．このような対策を施すことによって不正入手を防ぐことができる．しかし災害時に緊急用シェアストレージと復元 PC を施錠可能な場所に設置することができない可能性がある．また，災害時に緊急用シェアストレージの存在を確実に復元 PC に教示することは困難である．

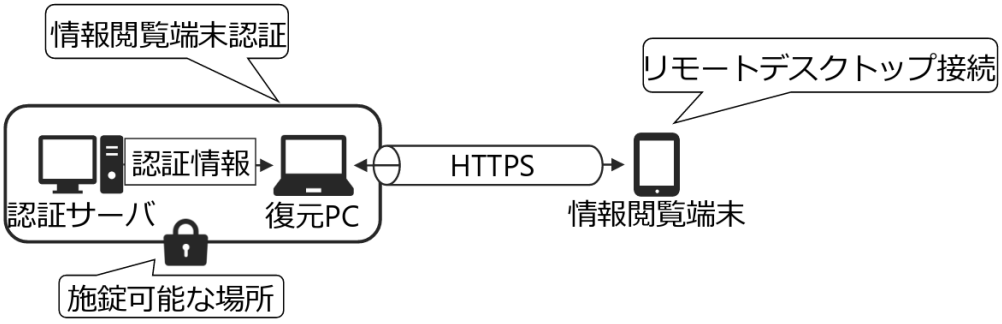

図 4.4　復元 PC と情報閲覧端末間のデータのやりとりに対する要件を満たす具体的な対策

4.2.4　復元 PC と情報閲覧端末間の要件の評価

復元 PC と情報閲覧端末間のやりとりでは．患者の医療データや個人情報のやりとりを行う．復元 PC と情報閲覧端末間でやりとりされるデータが洩れると，患者の医療データや個人情報が漏えいする．よって，復元 PC と情報閲覧端末間のデータのやりとりに対する要件では，通信相手の確認や情報閲覧端末からの情報漏えいを防ぐ要件を定めた．要件を満たす状態遷移が可能な具体的な対策を図 4.4 に示す．

情報閲覧端末を配付する際に配付相手が医師であるかを確認し，情報閲覧端末の識別情報と医師の情報を認証サーバに登録し，以降の接続の際に認証サーバを用いて相手が正当な相手かどうかを確認する．情報閲覧端末は復元 PC にリモートデスクトップ接続を用いて患者の医療データを閲覧する．このとき，情報閲覧端末に患者の医療データを保存することを禁止する．以上の対策を施すことによって不正入手を防ぐことができる．情報閲覧端末が増加することによって復元 PC の負担が増えるため，対策を考える必要がある．

4.2.5　実証実験

以上の対策を施すことによって安全にデータのやりとりを行うことができるかを確認するために，対策を施したシステムを実装し実証実験を行った．実証実験に用いたシステムの構成を図 4.5 に示す．実装したシステムでは，まず端末の情報を認証サーバ上の DB に登録する．次に Web 上にそれぞれの端末で配付する情報をアップロードする．最後にデータを入

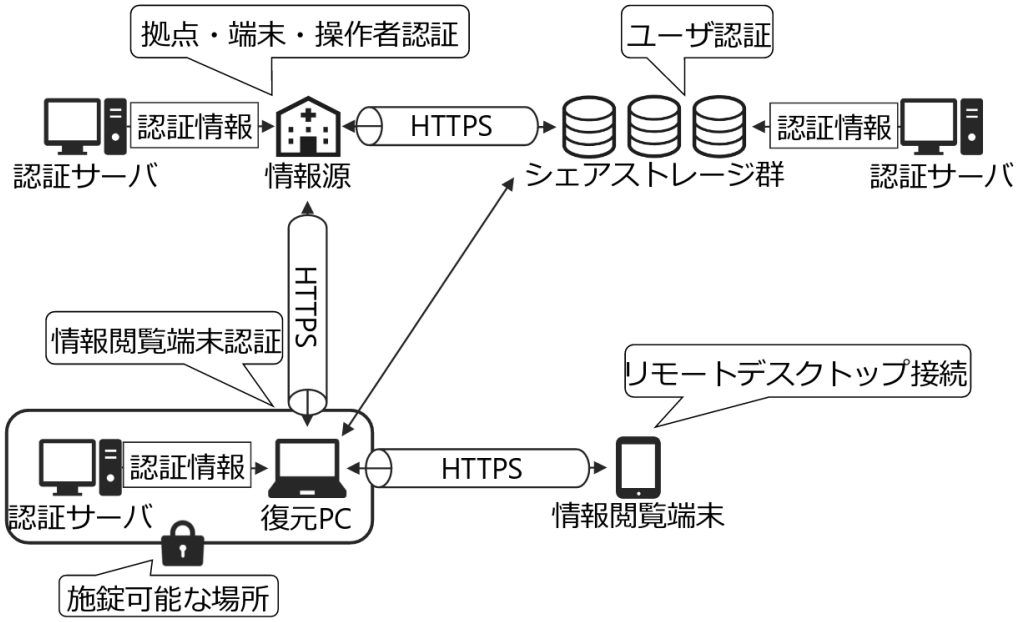

図 4.5　要件を満たす具体的な対策のシステム構成

表 4.1　実証実験環境

名称	アプリケーション
OS	Ubuntu16.04LTS
Web サーバ	Apache2.4
DB サーバ	Mysql5.6
認証ページ	PHP5.6

手する際に認証サーバを用いてユーザ認証を行い，認証ができたユーザのみにデータをダウンロードさせる．なお，各地点・端末間の通信路には HTTPS を用いて通信路暗号化を行う．また，復元 PC の設置場所を施錠可能な場所に設置した．実証実験の環境を表 4.1 に示す．

実証実験は，各地点・端末間のやりとりでデータの入手が可能か，地点・端末からデータの入手が可能かを確認した．まず，情報源と各端末の通信路が暗号化されており第三者から読み取ることができないことをパケットキャプチャーソフトを用いて確認した．次に，認証

サーバ上の DB に登録されていないユーザを用いて部分復元制御データを入手可能かを試した．ユーザ認証が失敗し，制御データを入手できないことを確認した．最後に，復元 PC を設置している場所に鍵を持っていないユーザが侵入できないことを確認した．以上より要件を満たす対策を施すことによって，各地点・端末間でやりとりされるデータの不正入手を防ぐことができるため，不正復元を防ぐことができることがわかる．

4.3　不正復元を防ぐ要件を満たした理想的なシステムの考察

部分復元アルゴリズムは紐付け情報とシェアが第三者に洩れると不正に復元される可能性がある．本研究では，アルゴリズムを用いた部分復元可能な秘密分散システムを提案した．医療データをバックアップする医療機関が部分復元を制御するデータを作成し，システムでの部分復元に制御データを用いることによって不正復元を防いでいる．

提案システムでは部分復元制御データが洩れると不正に復元される可能性があるため，不正復元を防ぐ要件を定義した．要件を満たすことで不正復元を満たすことができるが，現状の技術では要件を完全に満たすことができない．本節では，不正復元を防ぐ要件を満たした理想的なシステムの考察を行う．

不正復元を防ぐ要件を満たすためには，端末の操作者として登録されている人と第三者の結託防止する仕組みが必要になる．端末の操作者と登録されている人間が第三者との結託を許すと，操作者が保持している権限を第三者に譲渡したり，登録時に第三者の情報で登録されると登録者になりすまされる．この問題に対して登録者の権限を譲渡すると検知する仕組みがあれば第三者の結託を防ぐことができると考える．まず，登録者に与える権限を電子化して与える．電子化された権限をコピーするとデータ形式を変換し認証に使えないようにすることで第三者との結託を検知することができる上に第三者との結託を防ぐことができる．

復元 PC としきい値以上のシェアストレージの通信経路が被災しシェアを入手できない可能性がある．そこで，しきい値以上のシェアストレージに接続可能な災害拠点にシェアを配付し緊急用のシェアストレージを設置する．復元 PC は緊急用シェアストレージからシェア

4.3　不正復元を防ぐ要件を満たした理想的なシステムの考察

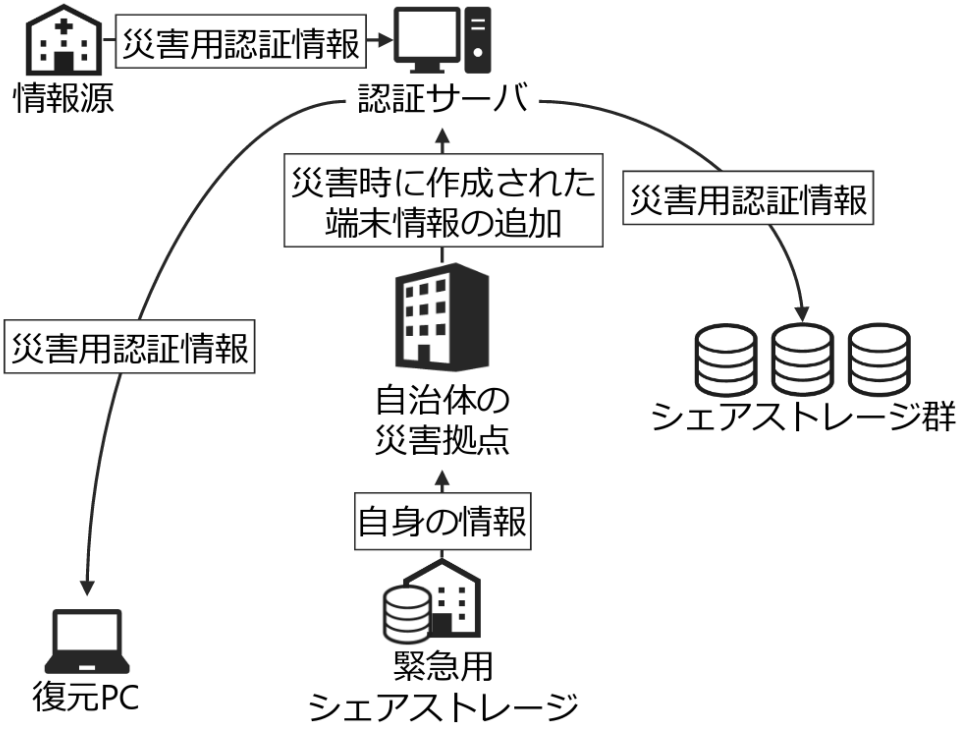

図 4.6　災害時に使用する認証情報を外部に保存し活用

を入手することによってシェアストレージ群との通信経路が使用できない場合でもシェアの復元を行うことができる．緊急用シェアストレージは災害時にシェアストレージと接続可能な災害拠点に作成設置される．そのため，復元 PC からは緊急用シェアストレージを検知することができない．また，全ての端末は通信相手を認証してから通信を行う．そのため，災害時に作成される端末の認証を行うことができず正当な相手にも関わらず通信することができない．よって，災害時に作成設置された緊急用シェアストレージを復元 PC に知らせ認証する仕組みが必要になる．

図 4.6 のように，災害時に各端末で使用する認証サーバを外部に設置することで，災害時に作成設置された端末の情報を登録認証できると考える．まず情報源が災害時に使用する認証情報を取りまとめ病院外のサーバに保存しておく．災害発生時，自治体の災害拠点に認証情報を保存しているサーバの情報を教え，被災地域外から来る DMAT に対して情報の提供や，医師の登録を行う．緊急用シェアストレージを作成設置した場合は，自治体の災害拠点に緊急用のシェアストレージを申請し登録を行う．復元 PC やシェアストレージ群は災害用

の認証情報が保存されているサーバから認証情報を入手し活用することで，通信相手の確認を行うことができる．

認証サーバを 1 つにまとめ外部に設置することで第三者に情報を抜き取られる脅威があるが，災害時にのみ使用する認証情報であるため，抜き取られたとしても災害時に使用するデータのみしか入手することができない．また復興後，災害時の認証情報を破棄するため平常時に抜き出したデータを使用することができない．よって，災害時の認証情報を外部に保存して活用することで提案システムを円滑に活用することができる．

第 5 章

まとめ

5.1 本研究のまとめ

本論文では秘密分散バックアップした医療データを被災地での医療行為に活用するために，部分復元アルゴリズムを用いた部分復元可能な秘密分散システムを提案した．さらに提案システム上で不正に復元される条件を洗い出し，不正復元を防ぐ要件を定義し評価を行った．

部分復元アルゴリズムは，あらかじめ分散するデータの中から復元したい情報を選択し，選択した情報を部分的に復元することができる．しかし，復元する場所を制御する紐付け情報とシェアが何らかの方法で第三者に入手されると不正に復元される可能性がある．提案システムでは，医療データをバックアップする情報源の病院が紐付け情報とシェアの入手を制御する部分復元制御データを作成し，各端末に配付することで第三者が紐付け情報とシェアを入手することを防ぐ．しかし，部分復元制御データが第三者に洩れると不正に復元される可能性がある．よって，部分復元制御データの不正入手を防ぐ要件を定義した．

提案システムを評価した結果，バックアップデータの中から部分的な情報を復元し，復元した情報を特定の人のみに提供できる．さらに，部分復元制御データを用いて，第三者の不正復元を防いでいる．よって，提案システムを用いることで不正復元を防いだ部分復元を行うことができる．

提案システムでの不正復元を防ぐ要件を評価した結果，要件を満たした状態遷移を行う対策を施すことによって，提案システムでの不正復元を防ぐことができることが分かった．

5.2　今後の課題

今後の課題として，提案システムは複数のユーザの結託に対して弱いため，結託を検知する仕組みを考える必要がある．また，災害時に復元 PC と緊急用のシェアストレージを施錠可能な場所に設置できない可能性があるため，災害時に第三者の侵入を検知できる仕組みを考える必要がある．

提案システムを高知医療センターの防災訓練で利用しようとする計画がある．提案システムは，システムでバックアップした医療データを提供するところまでしか考えられていない．そのため，医師に医療データを閲覧させるビューワー部分を設計する必要がある．

謝辞

本研究を遂行するにあたり，終始ご指導並びにご鞭撻を賜り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．本研究の副査をしていただいた情報学群横山和俊教授，植田和憲講師のお二人にも謹んで感謝致します．また，本研究で用いたデータの提供・ご意見をいただいた高知県医療センターの情報システム室北村和之氏に謹んで感謝致します．

福本教授には 4 年間という長い間大変お世話になりました．何だかんだ楽しかったです．

横山教授には就職活動の際に大変お世話になりました．私の就職活動がスムーズに進んだのは横山教授の丁寧な就活指導おかげです．大変お世話になりました．

植田講師には実験の TA でお世話になりました．頼りない TA だったとは思いますが，TA の仕事はこれからの社会人生活に生かせていければと思います．大変お世話になりました．

定期的に一緒に飲みに行ってくれた樋野氏，阿部氏には本当に感謝しています．

研究室の皆さん，大変なこと理不尽なこと意味分からないことがこれからいっぱいあると思いますが私のように自暴自棄にならずに頑張って乗り越えてください．

最後になりましたが，6 年間の大学生活を支えてくださった両親や友人などの皆様に感謝致します．

参考文献

[1] 澤田努, “南海トラフ地震に向けて医療情報を県外保全する取り組みについて 高知県医療通信技術 (ICT) 連絡協議会の立ち上げについて,” 医療情報学, Vol.33, No.4, pp.255–233, 2013.

[2] 福本昌弘，“南海トラフ巨大地震に対する医療情報の保全のための高知県での取り組み,”Mercato, 東北情報通信懇談会, Vol.89, pp.18–20, 2014.

[3] 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 イノベーションフォーラム 2015 予稿集，総務省，pp.144–145, Oct. 2015.

[4] 厚生労働省，“医療情報システムを安全に管理するために 「医療情報システム安全管理に関するガイドライン」 すべての医療機関等の管理者向け読本,” http://www.mhlw.go.jp/shingi/2009/03/dl/s0301-6b.pdf，2009.

[5] SS-MIX 普及推進コンソーシアム会長星久光 “SS-MIX の概要,” http://www.ss-mix.org/cons/file/SS-MIX の概要について.pdf，Sep. 2007.

[6] 清水俊郎, “SS-MIX の現状,” http://www.hcitj.jp/kanto_g01/6th20120908r.pdf, Sep. 2012.

[7] A. Shamir，“How to Share a Secret,” Communication of the ACM, Vol.22, No.11, pp.612–613, Nov. 1979.

[8] 佐々木雅英，“量子鍵を用いた情報理論的に安産なストレージシステム＆電子カルテシステム,” Feb. 2017.

[9] M.Fujiwara, A.Waseda, R.Nojima, S.Moriai, W.Ogata, M.Sasaki. Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing. Scientific Reports 6, Article number: 28988.

doi:10.1038.

[10] G. Blakley, “Safeguarding Cryptographic Keys,” Proc of AFIPS 1979 Nat. Computer Conf, Vol.48, pp.313–317, Sept. 1979.

[11] 田中麻実，福冨英次，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, Dec. 2015.

[12] 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4.3 版,” http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000119598.pdf, 2016.