様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月 ２３ 日現在

機関番号：２６４０２
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１２１１１

研究課題名（和文）部分復元可能な秘密分散法を用いた医療情報分散バックアップ

研究課題名（英文）Remote Backup of Electronic Medical Records using Partial Restoring Method for Secret Sharing Scheme

研究代表者
福本　昌弘（FUKUMOTO, Masahiro）

高知工科大学・情報学群・教授

研究者番号：７０２９９３８７

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：広域分散バックアップした電子カルテデータは、医療情報共有、災害時の診療などにも活用できることが望まれている。これらを実現するためには、個人を特定する情報からその患者の電子カルテデータを検索し、その診療に必要なデータのみを閲覧可能にすることが必要となる。秘密分散バックアップした電子カルテデータから、特定の個人の複数の機関にまたがる情報を検索するために分散情報を部分復元できることができる。さらに、シェアの状態で（復元しないで）検索を可能とする方法を提案している。これは、秘密分散したシェア間の係数の差を比較して一致判定をすることで実現されており、従来方式に比べて飛躍的に高速な検索を可能としている。

研究成果の学術的意義や社会的意義
広域分散バックアップした電子カルテデータを単独の病院でのリストアのみに利用するのではなく、平時の地域医療連携のための医療情報共有、災害時の災害派遣医療チーム（DMAT）や救護所での診療などでも活用できるようにすることが望まれている。本研究では、従来方式に比べて飛躍的に高速な検索を可能としている一方で、安全性はほぼ低下していない。これにより、災害時の医療救護所等でも、安全かつ高速に被災者の医療データを診療に活用できる。

研究成果の概要（英文）：It is hoped that the electronic medical record data backed up over a wide area can be used for medical information sharing and medical treatment in the event of a disaster. In order to realize these, it is necessary to search the electronic medical record data of the patient from the information that identifies the individual and make it possible to browse only the data necessary for the medical treatment. From the electronic medical record data backed up by secret sharing, the distributed information can be partially restored in order to search for information that spans multiple institutions of a specific individual. In addition, it has been proposed a method that enables searching in the shared state (without restoring). This has been realized by comparing the difference in coefficients between the secret-shared shares and making a match judgment, which enables a dramatically faster search than the conventional method.

研究分野：情報分散共有

キーワード：秘密分散法　部分復元　医療情報

１．研究開始当初の背景

東日本大震災では、病院が津波の被害に遭いカルテが流失する事態が発生した。大規模な災害などから医療情報を守るためには、広域に分散してデータをバックアップすることが効果的である。しかしながら、情報を何箇所にも分散して保管することは、それだけ漏洩のリスクが高まることになってしまう。現状では、情報漏洩の対策としては暗号化が一般的に用いられているが、時間をかければ必ず解読することが可能であり、医療情報のような高度な個人情報を扱う場合には十分であるとは言えない。これに対し、Shamir の (k、n)しきい値秘密分散法[1]を用いて電子カルテをバックアップする取り組みがなされている[2]。(k、n)しきい値秘密分散法は、秘匿したい情報を n 個のシェアと呼ばれるデータに分散し、そのうちの k 個以上集まればもとの情報が完全に復元できるが、k-1 個以下ではもとの情報について部分的にも知ることができないというもので、暗号化とは違い情報理論的に安全性が保証される。(k、n)しきい値秘密分散法はバックアップしたデータ全体を一括で復元するため、災害後に電子カルテシステムが復旧してから電子カルテデータをリストアすることには適しているが、地域での医療情報共有や災害急性期での利用には向かない。そのため、広域に分散してバックアップした医療情報について、氏名、生年月日などから検索することができ、必要（あるいは開示可能）とされる一部の情報のみを選択して復元できる秘密分散バックアップシステムが求められる。

２．研究の目的

広域分散バックアップした電子カルテデータを単独の病院でのリストアのみに利用するのではなく、平時の地域医療連携のための医療情報共有、災害時の災害派遣医療チーム（DMAT）や救護所での診療などでも活用できるようにすることが望まれている。これらを実現するためには、個人を特定する情報（氏名、生年月日、住所、将来的にはマイナンバー等）からその患者の電子カルテデータを検索し、その診療に必要なデータのみを閲覧可能にすることが必要となる。秘密分散バックアップした電子カルテデータから、特定の個人の複数の機関にまたがる情報を検索するためには、秘匿計算が必要になる。次に、検索したデータから、直近の服薬履歴など、災害急性期の診療で特に求められる情報のみを閲覧できるようにするためには分散情報を部分復元できることが必要になる。

広域に分散バックアップした情報の部分復元を可能にする秘密分散法については、研究代表者らが明らかにしている[3]。この方式では、標準化ストレージ SS-MIX2 の様式で記録された電子カルテデータを分割する。データを分割するときに、分割されたそれぞれのデータのデータ長などを結合情報とすることで部分復元を可能にしている。しかしながら、文献[3]では分散バックアップからの部分復元が数学的に可能であることを示しているに過ぎず、平時の地域医療連携にも災害時急性期の診療にも活用できるように、必要とされる情報を、安全にリアルタイムで提供できなければ意味がない。本研究では、秘匿計算による検索と分散データの部分復元を実現するアルゴリズムを確立することを目的とする。秘密分散されたデータから秘匿計算するための方式としては文献[4]など、秘密情報を復元することなく計算結果を求める計算法や特定の条件のもとで効率よく計算するアルゴリズムなど数々の成果が報告されており、主に統計計算などが想定されているものの、これらを大量のデータからの検索のための秘匿計算アルゴリズムに応用することには期待が持てる。

部分復元を可能にするような秘密分散法としては、ランプ型しきい値秘密分散法[5]が提案されている。この方式では、情報の一部については少ないシェア（分散されたデータ）のみでの復元を可能にしている。また、アクセス構造を実現する秘密分散法[6]では、分散情報を複数管理者に割り当てることでアクセス構造を実現している。これらの方式は、診療時に必要とされる情報のみを復元するという本研究での用途には適さない。本研究の独自性は、電子カルテデータを安全に広域分散しつつ、診療時に必要とされる情報のみを選択的に部分復元できることにある。本研究の成果により、地域だけではなく（世界規模の）広域に医療情報の共有をはかることが可能になる。さらに、医療情報に限らず、住民情報や介護情報、おくすり手帳、母子手帳などにも容易に展開できる。

３．研究の方法

本研究では、部分復元可能なしきい値秘密分散法を実現するための秘匿計算による検索アルゴリズムと診療で必要とされる医療情報のみを選択的に部分復元するアルゴリズムを実現する。この際考慮しなければいけないのはリアルタイム性の担保である。

広域分散された情報を復元するときには、医療情報を必要とする現場が災害急性期であったとしても、災害の被害を受けていない地域の計算資源を複数利用することが可能であると想定されるため、分散情報を復元するために要する補間多項式の解法の行列表現とその行列演算を効率的に解くためのアルゴリズムを導くとともに、剰余計算に用いる法の大きさ（拡大体の次数）を適応的に最適化するなどの方式により計算量を削減することもはかる。また、並列処理化を実現することで、検索、復元時間を短縮することができる。

災害時には情報通信環境が劣悪になる、もしくは低速の臨時通信手段しか使えないことなどが予想されることから、分散保管されたデータを集めて復元した情報を送信するための伝送制御方式は、研究分担者である岩手県立大学橋本教授と協力して実装する。研究協力者である研究室所属学生の協力のもと実装を行い、複数の分散サーバを模擬した仮想サーバによるシミュレーションで有効性の検証を行う。

医療情報を医師および医療機関がどのように扱うかについては、研究協力者である高知医療センター総合診療科長澤田務医師、医療情報センター北村和之主事の指導を仰ぐ。災害時の仮設診療所などで必要とされる医療情報の重要度や優先度については、東日本大震災の際の DMAT の経験を持つ研究協力者澤田務医師の協力のもと検討し、結果を評価する。

利用する医療情報については高知県全体規模での利用を想定し、高知県内の主要 13 病院と高知県医師会が参加し研究代表者が顧問として参画する高知県医療情報通信技術連絡協議会（高知県内約 6 割の患者の電子カルテデータを保有）から提供されたダミーデータを用いる。医療機関からの評価として、高知医療情報通信技術連絡協議会の会員にも実証実験に参加してもらい、評価結果をフィードバックする。

秘密分散アルゴリズムを用いた分散保管・部分復元システムを実装し、テストベッドネットワーク JGN、学術情報ネットワーク SINET5 等を介して高知と岩手に設置した仮想サーバおよび JGN 上の仮想サーバ・ストレージにより、広域に分散された情報から患者の情報を検索し、必要な診療情報を安全に復元・伝送できることを実証する。

４．研究成果

標準化ストレージ SS-MIX2 の様式で記録された電子カルテデータを意味のある情報の単位で分割してから保管するシェアに分散する（図 1.）。データを分割するときに、分割されたそれぞれのデータのデータ長などを結合情報とすることで部分復元を可能にしている（図 2.）。

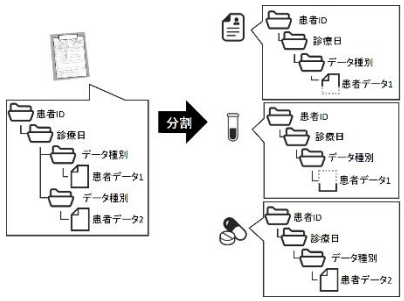

図 1．電子カルテデータの分割

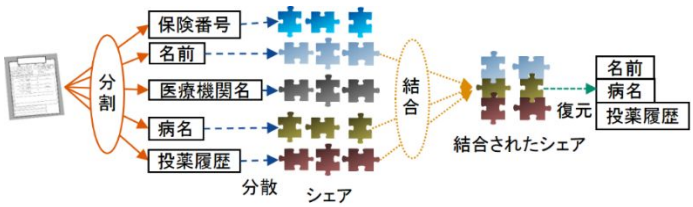

図 2．電子カルテデータの部分復元

文献[3]で提案したシステムでは、分散したデータの一部分だけを選択的に復元することができるが、分散した医療データの検索の仕組みは考慮されておらず、名前などの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しなければならないため、データを閲覧するまでに数十分以上の時間を要することもある、復元には連立方程式（逆行列）を解くための計算に特に時間がかかるため、災害時の医療現場ではこの検索方法は有効ではない。そこで、検索と復元の高速化を目的として、シェアの状態で（復元しないで）検索を可能とする方法を提案している[7]。この提案方式では図 3.に示すように、秘密分散したシェア間の係数の差を比較し、一致判定をすることで従来方式に比べて飛躍的に高速な検索を可能としている。一方、安全性はほぼ低下していない。これにより、災害時の医療救護所等でも、安全かつ高速に被災者の医療データを診療に活用できる。

(a) 従来方式[3]による検索処理の流れ

(b) 提案方式[7]による検索処理の流れ

図 3．従来方式との検索処理の違い

本課題で研究した「部分復元可能な秘密分散法」は医療データの分散保管を安全に行うための研究であるが、さらに、通信経路での安全性を保証するための研究として、耐量子暗号技術を用いた電子カルテ交換・保管システムの研究を国立研究開発法人情報通信研究機構(NICT)などと共同で実施している[8]。これらを複合的に用いることで、来るべき量子コンピューティング時代にも対応できる。

文献

[1] Adi Shamir, “How to Share a Secret”, Communications of the ACM, Vol.22, No.11, pp.612-613, Nov.1979.
[2] 黒田知宏, 木村映善, 松村泰志, 山下芳範, 平松治彦, 粂直人,“秘密分散技術を用いたHIS バックアップクラウド環境の実現性評価”, 医療情報学, vol.33, no.4, pp.225-233, 2013.
[3] 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”, 電子情報通信学会技術報告, vol.115, no.371, IA2015-74, pp.31-36, 2015.
[4] M.Ben-Or, S.Goldwasser and A.Wigderson,“Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computations”, Proceedings of the 20th Symposium on the Theory of Computing (STOC), pp.1-10, 1988.
[5] 山本博資,“(k; L; n) しきい値秘密分散システム”, 電子通信学会論文誌, vol.J68-A, No.9, pp.945-952, 1985.
[6] 伊藤充, 斉藤明, 西関隆夫,“一般的なアクセス構造を実現する秘密共有法”, 電子情報通信学会論文誌A, vol.J71-A, no.8、 pp.1592-1598, Aug.1998.
[7] 中村巴, 吉冨亮平, 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検索とその安全性評価”, 電子情報通信学会技術報告, vol.IEICE-120, no.356, IEICE-IA2020-34, pp.21-26, 2021.
[8] 国立研究開発法人情報通信研究機構（NICT）,“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”, https://www.nict.go.jp/press/2019/12/12-1.html.

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 福本昌弘	４．巻 36
２．論文標題 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による安全な共有・利活用	５．発行年 2021年
３．雑誌名 Bio Clinica	６．最初と最後の頁 695～699
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 福本昌弘	４．巻 3
２．論文標題 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	５．発行年 2020年
３．雑誌名 Precision Medicine	６．最初と最後の頁 843-847
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 福本昌弘	４．巻 4
２．論文標題 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による高速な復元	５．発行年 2021年
３．雑誌名 ions and Computer Sciences	６．最初と最後の頁 278-282
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Suksiri Bandhit、Fukumoto Masahiro	４．巻 19
２．論文標題 An Efficient Framework for Estimating the Direction of Multiple Sound Sources Using Higher-Order Generalized Singular Value Decomposition	５．発行年 2019年
３．雑誌名 Sensors	６．最初と最後の頁 2977～2977
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/s19132977	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 SUKSIRI Bandhit、FUKUMOTO Masahiro	４．巻 E102.A
２．論文標題 A Highly Efficient Wideband Two-Dimensional Direction Estimation Method with L-Shaped Microphone Array	５．発行年 2019年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1457～1472
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1457	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計8件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 中村巴，吉冨亮平，福冨英次，福本昌弘
２．発表標題 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
３．学会等名 電子情報通信学会技術報告
４．発表年 2020年

１．発表者名 中村巴，福冨英次，福本昌弘
２．発表標題 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
３．学会等名 2020年暗号と情報セキュリティシンポジウム(SCIS2020)
４．発表年 2020年

１．発表者名 中村巴，吉冨亮平，福冨英次，福本昌弘
２．発表標題 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
３．学会等名 電子情報通信学会インターネットアーキテクチャ研究会
４．発表年 2021年

１．発表者名
中村巴，福冨英次，福本昌弘

２．発表標題
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

３．学会等名
暗号と情報セキュリティシンポジウム（電子情報通信学会）

４．発表年
2019年

１．発表者名
Bandhit Suksiri, Masahiro Fukumoto

２．発表標題
Wideband Direction-of-Arrival Estimation with Cross-Sample Matching Technique on L-Shaped Microphone Arrays

３．学会等名
16th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON2019)（国際学会）

４．発表年
2019年

１．発表者名
福本昌弘，山本寛，秋山豊和，鈴木陽一，山崎克之

２．発表標題
広域ネットワーク防災訓練 ～ 災害時の救護所・避難所の遠隔支援に向けて ～

３．学会等名
電子情報通信学会インターネットアーキテクチャ研究会

４．発表年
2019年

１．発表者名
福本昌弘

２．発表標題
南海トラフ巨大地震に備えた高知での医療情報ネッワークの取り組み

３．学会等名
第12回地域防災情報シンポジウム

４．発表年
2018年

１．発表者名 福本昌弘
２．発表標題 高知におけるICT/IoTを活用した医療情報の管理と防災訓練
３．学会等名 第13回地域防災情報シンポジウム
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	橋本　浩二 (Hashimoto Koji) (80305309)	岩手県立大学・ソフトウェア情報学部・教授 (21201)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関