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
(121809003)

Applying secret sharing for his backup exchange to support the continuity of medical service

研究代表者

木村映善　愛媛大学医学部附属病院医療情報部

Eizen Kimura Dept. Medical Informatics of Ehime University Hospital

研究分担者

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[‡‡]

Matsumura Yasushi[†] Mihara Naoki[†] Kuroda Tomohiro[††]　Yamashita Yoshinori[†††]

Hiramatu Haruhiko[‡] Manabe Shirou[†] Tanaka Daisuke[‡‡] Sato Atushi[‡‡] Yamakura Tadashi[‡‡]

[†]大阪大学大学院医学系研究科医学専攻統合情報医学講座医療情報学　[††]京都大学医学部附属病院医療情報企画部

[†††]福井大学医学部附属病院医療情報部　[‡]兵庫医科大学医療情報部　[‡‡]NRI セキュアテクノロジーズ株式会社

[†]Department of Integrated Medicine, Medical Informatics, Osaka University

[††]Division of Medical Information Technology and Administrative Planning, Kyoto University Hospital

[†††]Department of Medical Informatics, Fukui University Hospital

[‡]Department of Medical Informatics, Hyogo College of Medicine [‡‡]NRI Secure Technologies

研究期間　平成 24 年度～平成 26 年度

概要

大規模な災害が発生しても医療サービス継続性を確保すること、そして仮に障害が発生したとしても速やかに原状に近い運用体制に復帰できる事業継続計画を策定、実現することが医療機関に望まれている。普段から医療情報を遠隔地にバックアップし、有事には安全な参照環境を提供し、さらに速やかに原状復帰できる仕組みを備える必要がある。しかし、個人情報を多分に含むカルテの遠隔バックアップには、セキュリティ保全の観点から管理コストが大きくなる傾向がある。本研究では、医療機関が相互に計算機資源を提供して情報保管し、必要時にいずれの医療機関でも速やかに参照、原状復帰できる環境の実現を目指した。各断片からの情報復元を不能にすることで、個人情報の漏洩から守る秘密分散・秘密計算技術を使用した分散バックアップシステム開発を試みた。運用コストの抑制と冗長性の最大化と、相反している課題の解決と、個人情報保護に関する配慮として、複数の医療機関が相互に計算機資源を提供して、秘密分散技術を用いて分散多重保存することで、個人情報の安全性を担保し、かつ単一障害点を有しない相互医療情報バックアップ環境を実現する。

まえがき

近年の急速な情報通信技術の発展に伴い、多くの医療機関は病院情報システムなしでは、もはや高度な医療サービスを安定して提供できないほど、情報システムに依存している。故に、被災直後も保存された情報を被災病院以外で速やかに閲覧できるようにして適切な医療サービスをどこでも継続することを可能にするとともに、被災後できるだけ早い段階で、被災病院で医療サービスを再開できるように、病院情報システム全体を原状復帰させる必要がある。

一方、究極の個人情報であるカルテの遠隔バックアップには、転送・保管時のセキュリティ担保が重要になる。しかし、「医療情報システムの安全性に関するガイドライン」等で示されている外部保管要件を満たすためには一定以上の管理が必要であり、多くの医療機関ではこの管理コストがネックとなって遠隔バックアップをあきらめる事例が報告されている。この問題を解決するためには、バックアップ送付前に情報を適切に処理し、たとえ保管先でデータファイルが盗難に遭ってもそれだけでは情報を元に戻すことができない仕組みをととのえておき、安価な汎用ストレージサービスにファイルを配置できるようにすることで、コスト削減を可能にする必要がある。本研究では、秘密分散技術を用いることでこの問題の解決を図る。

２．研究開発内容及び成果

(1)秘密分散バックアップの基本性能検証

本研究では地理的に離れた複数の大学病院間で相互にバックアップデータを持ち合う、相互互恵モデルを検討した。JGN-X 網経由で、愛媛・大阪・京都大学への接続、および福井大学、兵庫医科大学を模擬したノードを NICT データセンター内に設置し、実験環境を構築した（図 1)。京大附属病院の電子カルテシステムからのテストデータ 386GB について、自大学を除く 5 箇所のノードに対して秘密分散バックアップを行った。所用時間は 23 時間 10 分であった。ボトルネックを調査したところ、他大学及びデータセンターは 1Gbps の回線を利用しているが、京都大学附属病院は疎水ネットワークの 100Mbps 経由で JGN-X に接続しており、実測値が 99,2Mbps であるので、回線がボトルネックであると判断された。かつ、サーバの CPU、メモリ資源は余裕があったので、今後の処理時間短縮にはノード間の帯域の増強が必要と考えられる。

(2)DACS の秘密分散システムへの保存と閲覧の検証

阪大病院の DACS サーバに保存されている診療記録文書を、秘密分散方式で病院外サーバに送り出し、病院外から閲覧可能とする仕組みを構築した(図 2)。院内の DACS に文書が保存されると同時に deliverer(文書送信用サーバ)から文書外部送信用サーバに文書が送られる。送られた文書は DMZ に設置された文書メタ情報管理サーバに保存され、秘密分散 G/W により秘密分散処理が施された後、秘密分散ファイルサーバへ送信され保存される。閲覧時には DMZ 内にある文書メタ情報管理サーバにおいて目的の文書を検索する。検索と同時に秘密分散ファイルサーバからそれぞれの断片ファイルを集め、秘密分散 G/W にて再構築して閲覧することが可能である。平成 26 年度の実験で

は、実在する患者のデータを匿名化して行った。当該患者の全データ量は、878 ファイル(439 文書)、141MB であり、通常の DACS に日々保管されている平均的なデータのほぼ半日分に相当する。このデータの秘密分散保存の所要時間は 23 分 4 秒であった。この結果から日々発生するデータを、十分実用的な時間でバックアップできる可能性が示された。また、退避先を想定した場所にノート PC を携行し、秘密分散保存したバックアップからインデックス情報とファイルを復元し、診療文書を閲覧できることを確認した。

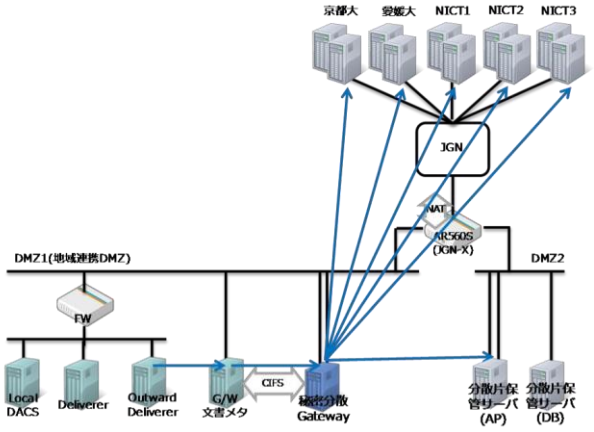

図 1 電子カルテのフルバックアップ検証用構成

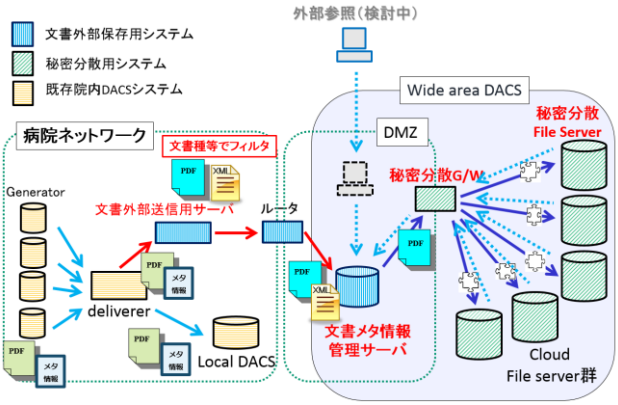

図2 DACSと秘密分散ゲートウェイの連携

3．開発成果の展開及び波及効果創出への取り組み

(1)エンタープライズ向け秘密分散バックアップシステム

本研究において大規模なデータのバックアップデータを秘密分散保存した経験から、秘密分散処理の最適化、GUI に依らない秘密分散保存の制御を提供する実装を追加して、エンタープライズ向け秘密分散バックアップシステムとして製品化することを検討している。ストレージクラウドサービスの暗号化処理やサービスはブラックボックスになっており、特に海外企業のサービス利用時においてコンプライアンスを充足することが困難である。一方、秘密分散技術を利用することで、秘密情報の制御はユーザ側が掌握できることから、国内外の企業やストレージの形態を選ばない。マイナンバー時代を控えて情報セキュリティとコンプライアンスを確保することが求められている今、企業の負担が少ない本手法は評価されると考えている。

(2)秘密分散を利用した医療文書管理システム

現在の医療文書管理システムは、遠隔バックアップや被災時の BCP まで想定する場合には、遠隔の安全なサイトにサーバとストレージ一式を擁して、日々遠隔バックアップを行う方式が主流である。しかしながら、特定のデータセンターに依存すると、被災時にデータセンターへのネットワークアクセスが途絶するとシステムが使用不能になる。本研究で使われている秘密分散は、複数箇所に分散保存し、かつ一部分が欠損しても残った場所から復元可能であるため、激甚災害下の冗長度が高まる。かつ、文書本体と文書のメタデータに分離して個別に保存することで機動性も確保できる。すなわち、文書閲覧時に検索するためのインデックス情報は数百 MB 程度ですむ。そのため、遠隔地にデータベースサーバを含む一式を構築せずとも、ノート PC 上に小型のデータベースとインデックス情報を展開するだけで、その場で診療情報を閲覧するシステムが構築可能である。ホット・ウォームサイトの構成が軽量になるため、システムへの投資が制約されている中小企業・医療機関でのバックアップ、BCP 策定の推進が期待される。

4．むすび

これまでの暗号化技術を適用したバックアップ手法と異なり、情報理論的安全性にもとづく秘密分散手法を適用したバックアップは、元の秘密情報の復元が困難であり、(特定)個人情報を外部に預託しているわけではないという解釈が成立しうる。医療費の高騰が社会的問題になりつつあるが、医療機関の医療情報システムへの投資を対費用効果の高いクラウドベースに移行させ、より洗練された医療とサービスへの展開に投資することが可能になれば、世界に冠たる高水準の医療環境を継続することが可能になることが期待される。ただ、普及にあたって製品化と並行して秘密分散技術の利用に関する事項を医療情報システムに関するガイドラインに反映させ、情報理論的安全性に対する理解を得ながら、秘密分散技術の導入による遠隔バックアップへの社会的受容を醸成することが求められる。

本研究の実現にあたり、情報通信研究機構、JGN-X・北陸 StarBED 技術センターの NICT の関係者各位、アライドテレシスホールディングス、日本 IBM、日本電気株式会社、富士通株式会社、富士ゼロックス株式会社にご協力を頂きました。ここに感謝の意を表します。

【誌上発表リスト】

[1] Tomohiro Kuroda, Eizen Kimura, Yasushi Matsumura, Yoshinori Yamashita, Haruhiko Hiramatsu, Naoto Kume, Atsushi Sato: Applying Secret Sharing for HIS Backup Exchange, Proceedings of Annual International Conference on IEEE Engineering in Medicine and Biology Society 4179-82 (2013)

[2] Tomohiro Kuroda, Eizen Kimura, Yasushi Matsumura, Yoshinori Yamashita, Haruhiko Hiramatsu, Naoto Kume. Simulating Cloud Environment for HIS backup using Secret Sharing. Studies in Health Technology and Informatics 171-4 (2013)

[3] 三原 直樹、松村 泰志、木村 映善、黒田 知宏、粂 直人、最首 壮一、佐藤 敦. Secret Share 技術を用いた統合文書管理システム(DACS)内文書の秘密分散バックアップ環境開発. 医療情報 学 34(Suppl.),2014, 656-659

【受賞リスト】

[1] 三原直樹 優秀口演賞 「秘密分散技術を用いた統合文書管理システム (DACS) 内文書の秘密分散バックアップ環境の開発」(内定)

【報道掲載リスト】

[1] “災害に備え カルテの分散保存”、毎日新聞, 2012 年 7 月 11 日

[2] “第 33 回医療情報額連合大会（その 1）医療情報額の次の"Innovation"に向けたセッション”、innavi net, 2014 年 1 月 6 日

[3] “被災時でも電子カルテ優先”、愛媛新聞, 2015 年 5 月 14 日

【本研究開発課題を掲載したホームページ】

http://www.nri-secure.co.jp/scope/index.html