計算システム工学分野

PHR における秘密分散を用いた医療消費者主導型開示先制御

学籍番号 23413571 氏名　溝口　航

指導教員名　岩田　彰

1　はじめに

高齢化や生活習慣病の増加に伴い，健康管理を自主的に行ない予防に努めることが求められている．そのための医療・健康情報共有システムとしてPHR（Personal Health Record）が提唱され，日本においては「どこでもMY病院構想」を通してガイドラインの制定など標準化が進められている．

医療・健康情報を中央のサーバに預け，適宜医療機関に開示する場合，従来のサーバ管理者が各医療従事者の閲覧権限を制御する方式では，保管サーバ自身が医療・健康情報を閲覧できるため，そこから漏洩の危険性がある．また，その情報を他機関に開示する場合には，医療消費者が開示先を自由に変更できるようにするべきである[1]．

そこで，本論文では，保管サーバ自身には情報を閲覧できない状態のまま情報を保管し，適宜必要な医療従事者に対して情報を開示できる手法（図1）を提案し，実装を行うことで実用的な速度での動作が行えるかどうかを検討する．最後に，各ガイドラインを参考に,PHRにおける個人情報保管方法に関する要件を定めることで，提案手法がそれらを満たせているか，あるいは，満たすためにはシステムや運用体制側でどのような機能が必要かという点について示す．

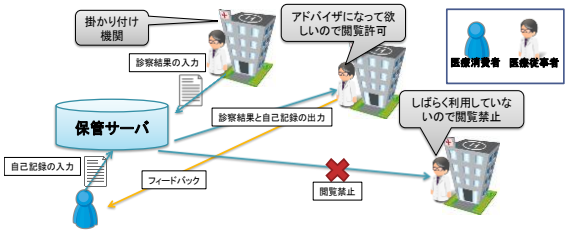

図 1：開示先制御の概要

2　提案手法

提案手法は，医療消費者毎に公開鍵暗号の鍵であるグループ公開鍵・秘密鍵ペアを持つ．健康情報は健康情報共通鍵暗号の鍵である健康情報復号鍵によって暗号化され，健康情報復号鍵はグループ公開鍵によって暗号化され，保管サーバに保管される．そして，グループ秘密鍵を，(2, 2)閾値秘密分散を保管サーバと医療従事者間で繰り返すことで二分木状の公開先グループを構成する．復号の際には，閾値復号を用いるため，グループ秘密鍵を秘匿したまま健康情報を復号することが可能である．

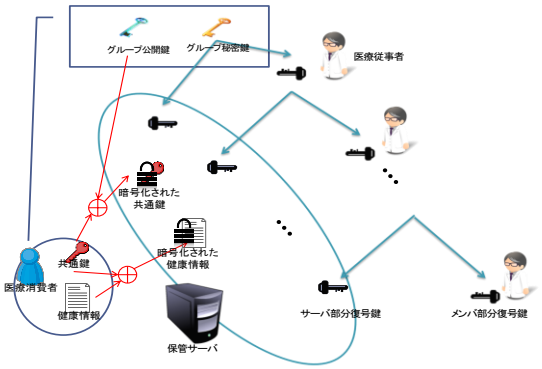

図2：提案手法の概要

提案方式は，6つのプロトコルから構成され，それぞれの安全性の根拠は，表1の通りである．

表1：提案手法のプロトコル一覧

プロトコル	用いられる暗号技術
グループ公開鍵生成	分散情報生成プロトコル[2]
健康情報の暗号化	KEM/DEM[3]
健康情報の逐次復号	閾値復号[2]，KEM/DEM
メンバ追加	(k, n)閾値秘密分散[2]， シェア・コントロール[3]
メンバ無効化	(k, n)閾値秘密分散，シェア・コントロール
鍵の更新	プロアクティブ秘密分散[5]， (k, n)閾値秘密分散

また，それぞれのプロトコルには，検証可能秘密分散[6]を用いることで,メンバが正しいプロトコルによって処理を行なっていることが保証されている．

4　実装

提案手法が，実システムに適用できることを示すため，実装を行った．ここでは，PHRの医療従事者の運用コストを抑えるためにも,暗号化と復号の2つのプロトコルをブラウザで行えるようにシステム構成

は図3のようにした.

結果, AMD A6-3400M 1.4～2.3GHz, DDR3-1333 4GB, Firefox 18.0を用いて, ElGamal暗号の鍵長1024bit, 10番目の医療従事者, という条件で復号処理時間を計測したところ, 毎秒6個の復号が可能であった.

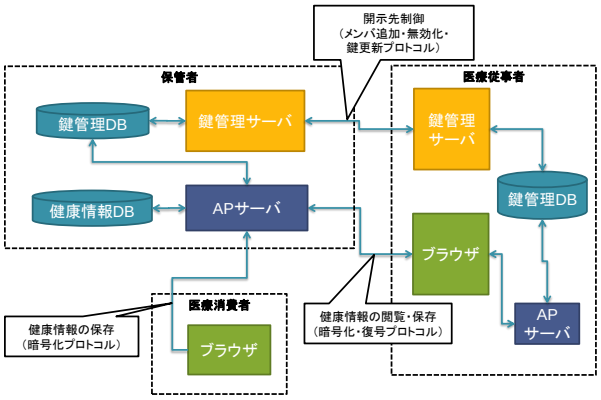

図 3：実装のシステム構成

4 評価・考察

提案手法が, PHRの実現に必要とされる技術面での要件と各ガイドライン要件から抽出されたサービス面での要件と適合しているか確認を行った（表2）.

表2：要件と適合

	要件	評価
開示先制御に関する要件	保管サーバに健康情報を閲覧されない	◎
	医療消費者の意図しない医療従事者に健康情報を閲覧されない	◎
	医療従事者の意図しない健康情報の二次利用が行われない	◎
	開示先の変更時に, 健康情報の再暗号化や鍵の再配布を行うコストが発生しない	◎
医療・健康情報の取り扱いに関する要件	真正性が満たされている	○
	見読性が満たされている	△
	保存性が満たされている	○
	災害や本人の意識不明などの緊急時には, 強制的に閲覧することができる	○
利便性に関する要件	健康情報の閲覧がブラウザから行うことができる	◎
	暗号化・復号の処理時間が十分に短い	△

◎：満たされている, ○：システムや運用体制での補完が必要,
△：○に加え, システム構築の際に従来手法に比較して留意すべき点がある.

提案手法では, 各プロトコルによって医療消費者主導型の開示先制御が実現されている. また, 暗号化された状態で医療・健康情報が保管されているため, 改竄に対する真正性が高い. しかし, 緊急時においても開示先制御機能がなければ情報を閲覧できないことに留意する必要がある. 最後に, 緊急時の対応に関しては, すべての医療消費者が予め開示先と指定する緊急時機関を用意することで対応が可能であるが, これは, 保管サーバの管理者とは別に用意され, 運用されるべきである.

5 まとめ

PHR を実現するにあたって, 保管サーバに健康情報を閲覧されることなく保管し, 必要に応じて各医療従事者に公開する手法を提案した. いくつかの暗号技術によってその安全性を示すことはできたが, それだけで, 医療情報システムとしてのすべての要件を満たせるわけではない. システム構築を行う際には, 4 章で確認した要件を満たすために必要となる機能の実装や運用体制の確立が必要である.

参考文献

[1] 総務省情報流通行政局地域通信振興課, 情報通信技術及び人材に係る仕様書（平成 23 年度版）（医療分野）どこでも MY 病院/PHR, March 2012.

[2] TorbenPryds Pedersen：“A threshold cryptosystem without a trusted party.” DonaldW. Davies, editor, Advances in Cryptology — EUROCRYPT ’91, 第 547 巻 of Lecture Notes in Computer Science, pp. 522-526. Springer Berlin Heidelberg, 1991.

[3] Victor Shoup：“A proposal for an iso standard for public key encryption (version 2.1)”. Technical report, ISO, December 2001.

[4] 内田真理子, 福田洋治, 毛利公美, 白石善明. “多重帰属の鍵管理が容易な(2,2) 閾値秘密分散を用いたグループファイル共有”（情報通信基礎サブソサイエティ合同研究会）. 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ, Vol. 108, No. 473, pp. 71-78, March 2009.

[5] Amir Herzberg and Stanis law Jarecki and Hugo Krawczyk and Moti Yung. “Proactive secret sharing or: How to cope with perpetual leakage”, 1998.

[6] Benny Chor, Sha Goldwasser, Silvio Micali, and Baruch Awerbuch. “Veriable secret sharing and achieving simultaneity in the presence of faults.” Foundations of Computer Science, IEEE Annual Symposium on, Vol. 0, pp. 383-395, 1985.