L-020

IDベース暗号を利用した電子カルテシステムにおける鍵管理方式の提案

Proposal of Key Management Method in Electronic Medical Recording System Using Identity Based Encryption

四ッ柳 健太† 高橋 修‡ 宮本 衛市‡
Kenta Yotsuyanagi Osamu Takahashi Eiichi Miyamoto

1．序論

現在の電子カルテシステムの問題に、予算の関係などで病院のシステム導入・運用コスト負担が大きいことと、病院間の電子的なカルテのやり取りが確立していないため、セキュリティ面に対するアプローチが少ないことがある。 本研究では、ID ベース暗号[1]を用いて上記２つの問題を解決に導く電子カルテシステムの鍵管理方式を提案する。

2．ID ベースの鍵管理方式適用モデル

鍵管理方式を適用するベースとなるためのモデルを準備する。ID ベース暗号・署名、階層的 ID ベース暗号技術[2]を利用して、電子カルテの情報を地域内の病院間で共有できるようなモデルを想定する。

2.1 ＩＤベース暗号を利用する理由

既存の PKI を利用した鍵管理方式と比較して、ID ベース暗号を用いたモデルは大きな２つの利点がある。１つめは、ID ベース暗号は個々が持つ任意の ID を公開鍵とするため、公開鍵を簡単に知ることができ、公開鍵を探して公開鍵証明書を取りに行く手間も省けることである。２つめは公開鍵証明書が必要ないため、証明書及び鍵失効リストなど、サーバでの公開鍵管理が必要なくなり、コスト面においてシステムを構築しやすくなることである。これは、厚生労働省の保健医療分野のグランドデザインなどで電子カルテシステムの導入を推奨されている各医療機関で、新しいものを導入してからの運用・管理の問題、及びコストの問題の解決に必要な技術である。つまり、ID ベース暗号を適用させたシステムを作ることそれ自体で、コストを低減させることにつながり、コスト問題を解決に導くと考える。

2.2 モデル図と説明

地域ごとにその地域内のすべてのカルテ情報を管理するサーバとして、地域カルテ管理サーバを設ける。そこでは、その地域内のカルテのインデックス情報（いつどの患者のカルテが作成保存されたか）を一括管理するものとする。インデックス情報は患者の ID（患者の公開鍵となりえる社会保障番号のようなもの）をベースとしたものと仮定する。病院は患者の他の病院で診察を受けた時のカルテ情報が欲しいときに、地域カルテ管理サーバのインデックス情報を利用して閲覧する。

なお、病院内のモデルに関しては「ＩＤベース暗号の電子カルテシステムへの適用」[3]にて述べられている。

地域カルテ管理サーバと各病院の関係モデル図を次の図１を記す。

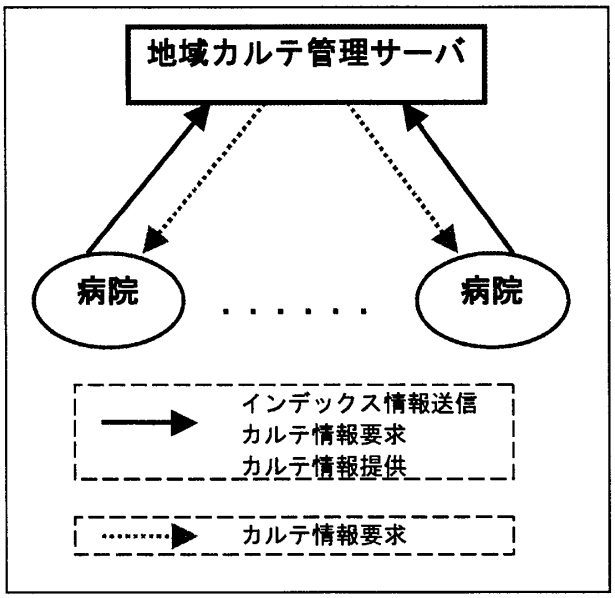

図１ 地域カルテ管理サーバと各病院の関係モデル

このインデックス管理のモデルは、電子カルテを導入している中規模病院に訪問させて頂き、そこでのヒアリングを元に作成したものである。

3．鍵管理提案方式

２のモデルに適用するＩＤベース暗号を利用した鍵管理方式を述べる。

3.1 鍵の所有者と用途

表１に示す２種類の鍵ペアを用いる。公開鍵はＩＤであるため、誰でも得られるものとする。

表１ ID ベースの鍵の種類

鍵名	所有者	用途
病院秘密鍵	地域カルテ管理サーバ	地域カルテ管理サーバ・・インデックス情報の復号化
	各病院	各病院・・病院内の職員が外出先から病院のカルテ閲覧
病院公開鍵	誰でも	病院がインデックス情報及びカルテの暗号化
患者秘密鍵	地域カルテ管理サーバ	地域カルテ管理サーバがカルテの復号化
患者公開鍵	誰でも	病院がカルテの暗号化

† 公立はこだて未来大学大学院 システム情報科学研究科
‡ 公立はこだて未来大学 情報アーキテクチャ学科

3.2 インデックス情報管理方法

病院が地域カルテ管理サーバにインデックス情報を送信するときについて述べる。地域内の各病院は1日に1回程度、定期的にインデックス情報を地域カルテ管理サーバに送信する。このとき病院はインデックス情報を自分の病院公開鍵で暗号化して地域カルテ管理サーバに送信し、地域カルテ管理サーバはその病院の病院秘密鍵を用いて復号化して、インデックス情報を蓄える。

3.3 カルテ参照方法

病院が患者の他の病院のカルテを参照したいときの流れを次に述べる。

Step1: 病院が地域カルテ管理サーバにアクセスして、患者のＩＤを入力してカルテ検索

Step2: 地域カルテ管理サーバが検索された患者のカルテのある病院にカルテ情報を要求

Step3: 要求を受けた病院は提供する患者のカルテを患者公開鍵で暗号化

Step4: 暗号化したカルテを要求している病院の病院公開鍵で暗号化して地域カルテ管理サーバに送付

Step5: 地域カルテ管理サーバは送られてきたデータを患者秘密鍵で復号化して、要求してきた病院に暗号化されたカルテを見せる

Step6: 病院は自分の病院秘密鍵を使って復号化してカルテを閲覧

Step1では、患者のIDを検索で利用することにする。これは患者公開鍵も同じ患者IDを利用するため、患者のIDですべて統一できるものとする。

Step3では、病院は患者のカルテをサーバから取り出すときに患者公開鍵で暗号化することにより、患者秘密鍵を得られる地域カルテ管理サーバでのみ閲覧可能となる。

Step5の後半とStep6は、地域管理カルテサーバ上で行われる操作である。データ自体は要求する病院に送るのでなく、地域管理カルテサーバまで送られ、そこで閲覧することにするため、カルテを渡すのではなくあくまで閲覧するという形をとる。参照し終わったカルテは地域カルテ管理サーバが削除する。

3.4 PKG階層化による鍵管理方式

秘密鍵生成センタであるＰＫＧは、地域カルテ管理サーバと各病院にそれぞれ階層的に配置する。地域カルテ管理サーバにあるＰＫＧからは地域内の各病院の病院秘密鍵と患者秘密鍵を、病院にあるＰＫＧからはその病院の病院秘密鍵を生成できるものとする。このようにPKGを各機関に分散させることにより、サーバにかかる負担が減るだけでなく、２つの大きな利点を得られる。

１つ目はＩＤベース暗号方式において、ＰＫＧからの鍵送付時のセキュリティが問題であるが、各病院にＰＫＧがあることによって鍵をネットワークを介して送付する必要がなくなる。

２つ目は、病院がＰＫＧを持つことにより、出張等で病院内にいない医師に期限付きの鍵を持たせることができることである。例えば、医師が3日間出張で病院から離れる場合を考える。ＰＫＧで3日分の病院秘密鍵を作成し、医師に持たせる。これによって鍵をネットワークを介して送付することなく、暗号化したカルテのやり取りが可能となる。具体的には、病院が医師の必要としているカルテを病院公開鍵で暗号化して医師に送付し、医師は病院秘密鍵を利用することによってそのカルテを復号化して閲覧することができる。こうすることにより、医師が鍵を紛失してしまった場合のリスクは、短期間であるために小さくて済む。

4．関連研究

医療と暗号の面と、各国の医療分野の情報化の面の2面からみていく。

4.1 各国の医療分野の情報化[4]

先進諸国では、医療費の増大、増え続ける医療過誤や重複した医療行為の削減、医療水準の確保及び向上等の課題解決のため、国家規模で積極的に取り組んでいる。特に米国は医療機関同士を結ぶネットワークの構築に力を入れていて、RHIO(Regional Health Information Organization)と呼ばれる地域ごと（主に郡単位）の医療情報ネットワークを構築し、それをさらに統合してNHIN（National Health Information Network）を構築するプロジェクトを進めている。

4.2 医療分野における暗号技術の取り組み[5]

IDベース暗号方式を医療情報システムに適用している研究例はない。また、医療機関間で暗号を使ったデータのやり取り自体が、コストなどの問題によりまだあまり行われていないのが現実である。暗号を利用する場合、ほとんどPKIの技術を利用して構築されているが、PKIは認証局の問題があり、医療で用いる実用的な認証局は存在していない。しかし、現在進行形で情報化のための共通基盤の整備ということで、厚生労働省がHPKI（ヘルスケアPKI）ルート認証局を構築・運営するための会議などを行い、着々と準備が進められている。

5．結論

本研究は、多くの医療機関で導入不可欠である電子カルテシステムにおいて、低コストで鍵管理の面でも管理しやすい、病院間のカルテ情報共有をメインとしたモデルで、IDベース暗号方式を適用した鍵管理方式の提案を行った。今後の課題として、これから日本がどのような形で医療情報を共有していくのかを、米国などの例を参考に調べていき、理想とするモデルにおいてIDベース暗号がうまく適用できることを示し、評価していく予定である。

参考文献

[1] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing." Advances in Cryptology—Crypto 2001, Springer-Verlag, 2001.

[2] Jeremy Horwitz and Ben Lynn. Towards hierarchical identity-based encryption. In Lars Knudsen, editor, Proceedings of Eurocrypt 2002 , Springer, 2002.

[3] 四ッ柳健太 他, IDベース暗号の電子カルテシステムへの適用, 情報処理学会全国大会, 2007.

[4] DIGITAL GOVERNMENT, 米国における地域医療化の状況, 平成19年1月, http://epublic.nttdata.co.jp/f/repo/436_u0701/u0701.asp

[5] 厚生労働省, 医療・健康・介護・福祉分野の情報化グランドデザイン, 平成19年3月27日, http://www.mhlw.go.jp/houdou/2007/03/h0327-3.html