6W-2

ID ベース暗号の電子カルテシステムへの適用

四ッ柳 健太† 高橋 修†

†公立はこだて未来大学 システム情報科学部 情報アーキテクチャ学科

1 序言

近年、医療情報システムの導入は、各医療機関にとって先送りできない課題となっている。その軸となっている電子カルテシステムは、大量の個人情報をかかえているためにセキュリティを強化しなければならない上に、多くの病院では予算の関係などで、その導入・運用コストは最小限に抑える必要がある。本研究では、ID ベース暗号方式の利点をうまく活用した電子カルテシステムモデルを提案する。

2 提案モデル

ID ベース暗号・署名、階層的 ID ベース暗号技術を利用して、電子カルテシステムの一部を例としたセキュアなシステムモデル（以降、電子カルテシステムモデルと記す）を提案する。様々な用途で利用できるようなモデルにも発展できるよう、わかりやすいモデルとする。

2．1 ID ベース暗号を利用する理由

既存の PKI を利用したモデルと比較して、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病院などで、新しいものを導入してからの運用・管理の問題、及びコストの問題を低減するために必要な技術である。

2．2 要件とモデル

電子カルテシステムモデルは、複数の病棟と１つの電子カルテ管理部署を持った病院を題材として、登場人物をドクター、ナース、患者、鍵管理人（PKG）、カルテ管理人（電子カルテ管理部署）の５者とする。当論文では、すべての鍵において特に明記の無い場合、ID ベース暗号における秘密鍵の方を示すこととする。

（1）要件

1．ドクターはドクターカルテ、ナースはナースカルテのみ作成保存可能
2．患者は自分のカルテは閲覧可能であるが、それ以外のカルテはすべて不可能
3．カルテのデータすべてにおいて、書き換え不可能
4．同じ病棟のドクター/ナースは病棟内の患者のカルテを自由に閲覧可能
5．ドクター/ナースが他の病棟のカルテを閲覧する時は、そのカルテのある病棟の誰かに許可をもらうことで可能となる

（2）鍵の種類

次に記す４種類の鍵を用いる。

・職員鍵：所有者はドクター/ナースの各個人。用途はカルテを記述した後の署名。
・病棟鍵：所有者は各病棟に所属するドクター/ナース全員。用途は鍵に対応した病棟のカルテ閲覧。
・患者鍵：所有者は各患者、及びにドクター/ナース。用途は患者は自分のカルテ閲覧。ドクター/ナースはカルテ暗号化。
・管理鍵：所有者はカルテ管理人。用途は電子カルテシステム管理部署に送られてきたカルテを保存時に署名。

（3）モデル図

病棟の数を２つに絞り、PKG の鍵配布とその鍵を使ったカルテへのアプローチを示した電子カルテシステムモデルを次の図１に示す。

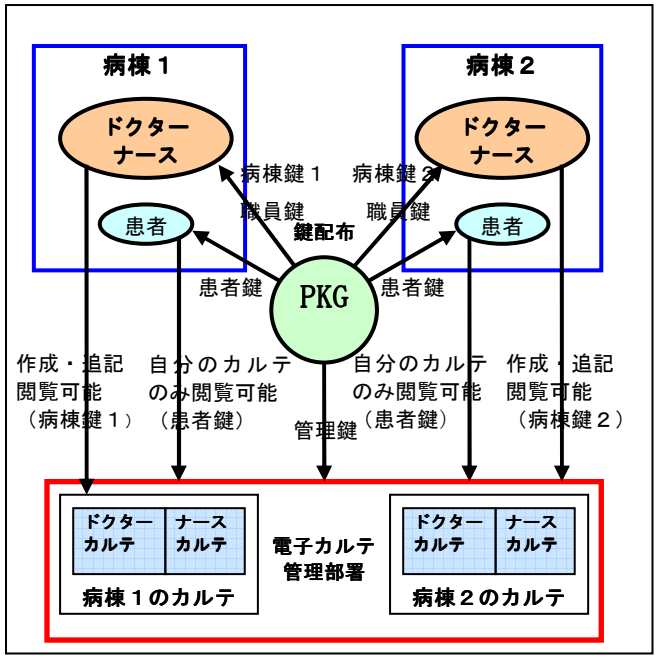

図１ 電子カルテシステムモデル

Application of Identity Based Encryption to electronic medical recording system
†Kenta Yotsuyanagi , Osamu Takahashi
Future University Hakodate

3　実現方式

一般的にカルテアクセスに関しては、バイオメトリックス認証などにより管理され、アクセスログはタイムスタンプなどで時間単位でわかるようになっている。また、カルテの真正性を保障するためには、第三者機関の署名や認証で保障され、医療機関に負担を減らす仕組みになっているとこが多い。

当モデルの要件は、第三者機関を利用しないことと、バイオメトリックス認証、アクセスログを踏まえて考え、それに加えた鍵管理での方式で実現をする。

（1）要件1

カルテ保存時に電子カルテ管理部署が職員の秘密鍵による署名がされていることを確認する。ナースカルテにドクターの署名がされていたり、ドクターカルテにがナースの署名がされていると、そのカルテは保存されない。

（2）要件2

カルテをそれぞれの患者の公開鍵で暗号化することによって、患者は自分自身のカルテは秘密鍵で復号化して閲覧できるが、他の患者のカルテは鍵を持っていないため解読不能。

（3）要件3

ドクター/ナースが作成して署名・暗号化したカルテに、電子カルテシステム管理部署が管理鍵を使って署名する。これによって、職員の職員鍵による署名と管理部署の管理鍵による署名の 2 重署名となり、カルテの書き換え防止及び、真正性の保障をする。

（4）要件4

ID ベース暗号の鍵管理は主に、鍵生成と鍵更新の機能がある。鍵生成は、PKG（秘密鍵生成センター）という一つの信頼できる機関が、公開鍵とする ID に対応する秘密鍵を生成してユーザに配布する。鍵更新は鍵を定期的に更新することで、鍵の失効問題をカバーするものである。

階層的 ID ベース暗号を利用することにより、この鍵管理に階層構造を持たせて鍵の数を抑えることによって、扱いやすくすることができる。階層的 ID ベース暗号は、複数の PKG を木構造に配置して階層的に管理するものであり、親は自らの秘密鍵を用いて子の秘密鍵を生成することができる。

この技術を利用して病棟鍵と患者鍵を親子関係にする。図２に示すような親子関係を作ることによって、同じ病棟にいる患者すべての鍵が一つの病棟鍵で生成することができるようになる。これにより患者のカルテ復号化はその患者がいる病棟の病棟鍵を用いて、該当する患者鍵を取り出し、それを用いて行うことができる。

（5）要件5

要件５は特殊なケースであるが、病院勤務の方のヒアリング調査結果で紙カルテベースでの管理のときに、実際に行われる行動であったため作成した要件である。

まず最初に、病棟１のドクターが病棟２の患者のカルテを閲覧したいとき、病棟２のドクター（もしくはナース）にその理由を述べ申請する。病棟２のドクターはその理由が正当であることを認め、申請を許可する場合、病棟鍵２を使って該当する患者鍵を取り出し、病棟１のドクターに送付する。これによって病棟１のドクターは、送付された患者鍵を用いることによって、閲覧したい患者のカルテを復号化して閲覧することができる。

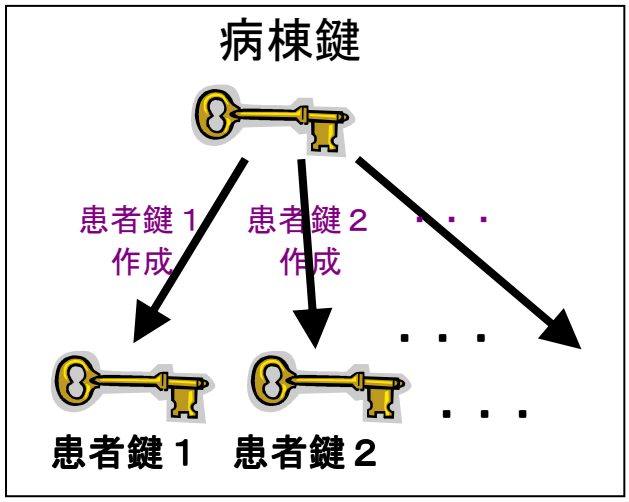

図２　病棟鍵と患者鍵の関係

3．6　提案方式の処理の流れ

上記のことを踏まえて、カルテ作成から保存までの一連の流れは次のようになる。

Step1: ドクター/ナースがカルテを作成
Step2:　職員鍵でカルテに署名
Step3:　病棟鍵を使って患者鍵を取り出す
Step4:　患者鍵でカルテ暗号化
Step5:　職員鍵で署名を付与
Step6: カルテ管理部署が職員鍵の署名を確認
Step7:　管理鍵で署名
Step8:　カルテ保存

4　関連研究

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。ほとんどは 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　結言

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、ID ベース暗号方式を適用し、低コストで鍵管理の面でも管理しやすい電子カルテシステムモデルを提案した。

参考文献

[1]　宮地充子「秘密鍵の動的な攻撃(鍵露呈攻撃) に対して安全な鍵進化公開鍵暗号に関する研究」情報学平成 17 年度 研究成果報告書, 2005.

[2]　D. Boneh and M. Franklin. “Identity based encryption from the Weil pairing.” Advances in Cryptology− Crypto 2001, Springer-Verlag, 2001.

[3]　原田篤史「ライトワンス文書管理システム」情報処理学会論文誌，Vol.44，No.8，2003.

[4]　「電子カルテってどんなもの？」，電子カルテ研究会 , 中山書店 , P107-125 , 2002.