7X-02

在宅医療介護連携システムにおける緊急時を考慮した HPKI 認証に基づく個人情報の開示先制御

稲吉 陽一朗† 白石 善明‡ 竹尾 淳† 加藤 昇平† 矢口 隆明† 岩田 彰†

†名古屋工業大学 ‡神戸大学

1 はじめに

在宅医療介護において，多機関多職種の医療介護従事者間の情報共有に ICT を活用することでチームケアが円滑となり，医療・介護の質の向上や効率化が期待される．そのようなシステムで扱う患者の機微な個人情報は暗号化された上で保管されることが望ましい．また，患者の個人情報の開示先は，通常時は担当者に限定されるが，患者の容態の急変時などの緊急時に担当者が対応できない場合，開示先はそれ以外の医療介護従事者に変更される仕組みが必要となる．これには保健医療福祉分野専用の公開鍵基盤（Healthcare Public Key Infrastructure: HPKI）[1] によって真正性が保証される国家資格情報（hcRole 属性）が有用である．

そこで，緊急時を考慮した暗号化された個人情報の HPKI 認証に基づく開示先制御方式を提案する．まず，代表的な公開鍵暗号である RSA 暗号によって構成する方式を，次に秘密鍵管理コストの削減を図った暗号文ポリシー属性ベース暗号（Ciphertext-Policy Attribute-Based Encryption: CP-ABE）[2] によって構成する方式を提案する．また，暗号化及び復号化処理時間を実機で測定し，2 方式を評価する．

2 CP-ABE

文献 [2] をはじめとする CP-ABE は，暗号文に復号化条件を表すアクセス構造を埋め込むことで復号化できるものを柔軟に指定できる公開鍵暗号方式である．CP-ABE は以下の 4 つのアルゴリズムからなる．

Setup セキュリティパラメータ λ を入力として，マスタ公開鍵 MPK とマスタ秘密鍵 MSK を出力する．

Encrypt マスタ公開鍵 MPK と平文 M，またアクセス構造 P を入力として，暗号文 CT を出力する．

Keygen マスタ秘密鍵 MSK とユーザの属性集合 S を入力として，秘密鍵 SK を出力する．

Decrypt マスタ公開鍵 MPK と秘密鍵 SK，暗号文 CT を入力として，SK の属性集合 S が CT のアクセス構造 P を満たす場合，平文 M を出力する．

上記のアルゴリズムのうち，Setup と Keygen は PKG(Private Key Generater) と呼ばれる信頼された機関が行う．また，Encrypt において暗号文に埋め込むアクセス構造は，職種や所属等の属性の論理式で表現される．

3 提案方式

提案方式では，患者の個人情報の暗号化に共通鍵暗号 AES を利用する．また，厚生労働省によるガイドライン [3] に則り，開示する患者の個人情報の範囲を制御するため，個人情報を患者属性や医療，介護・生活 [4] など種別毎にカテゴライズする．そして，カテゴリ毎に固有のカテゴリキー（AES 鍵）を生成し，それによって暗号化する．また，医療介護従事者単位に公開鍵暗号の鍵を生成し，その鍵によってカテゴリキーの配送，管理を行うことで，カテゴリ毎に開示先制御を行う．このときの公開鍵暗号に，RSA を利用する方式（RSA 方式）と，その欠点を改善する CP-ABE を利用する方式 (CP-ABE 方式) を提案する．

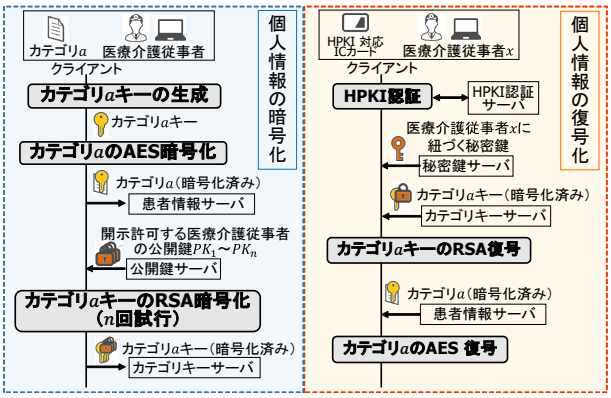

図 1: 暗号化及び復号化の手順（RSA 方式）

3.1 RSA 方式

各医療介護従事者に RSA 公開鍵ペアと ID を生成し，それらを紐付ける．また，患者毎の職種単位にも RSA 公開鍵ペアを生成し，それらには各職種に相当する hcRole 属性を紐付ける．通常時開示先制御には各医療介護従事者の ID に紐づいたペアを用いる．緊急時には，各医療介護従事者の hcRole 属性を確認した上でこれに紐付いたペアを用いることで，確かに専門資格を持つ加入者へ情報の開示を許可する．生成した RSA 公開鍵ペアのうち，公開鍵は公開鍵サーバで，秘密鍵は秘密鍵サーバで保管する．図 1 にあるカテゴリ a 個人情報の暗号化と復号化の手順を示す．

この方式における考慮すべき点として，医療介護従事者に紐づく秘密鍵をセキュアに管理しなければならない点がある．これはシステムを運用していく上で考慮すべきコストとなる．また，文献 [5] では，統計データに基づき，医療介護従事者の総数に比べ，患者 × 職種数 の方が大きいことが示されている．よって，緊急時開示先制御を可能とするために，通常時開示先制御のための RSA 公開鍵ペアの数より多くの鍵ペアを生成し，それらを管理する必要がある．

3.2 CP-ABE 方式

CP-ABE では，医療介護従事者に対して生成する秘密鍵は PKG が随時生成可能である．よって，医療介護従事者が HPKI 認証される都度，その ID と証明書内の hcRole 属性を属性値として埋め込まれた秘密鍵を生成する．そして，利用後に秘密鍵を削除することで，これを常に管理する必要がなくなる．

CP-ABE 方式でも，各医療介護従事者に ID を生成しておく．そして，カテゴリキーを CP-ABE で暗号化する．このとき暗号文に埋め込むアクセス構造を “(ID =1001) or (ID =1002)” というように ID を OR で結合する形で記述する．また，システム内で患者の緊急時状態を emergency，ある hcRole 属性を hcRole* と表すとする．その場合，“emergency and hcRole*” を通常時のアクセス構造に OR 結合して緊急時用のアクセ

Information Disclosing Mechanism Based on the Healthcare PKI in an Emergency for Collaboration of Home Medical Care and Nursing Services, Yoichiro INAYOSHI†, Yoshiaki SHIRAISHI‡, Jun TAKEO†, Shohei KATO†, Takaaki YAGUCHI†and Akira IWATA†

†Nagoya Institute of Technology

‡Kobe University

†Gokiso-cho, Showa-ku, Nagoya 466-8555, Japan

‡Rokkodai-cho 1-1, Nada-ku, Kobe, 657-8501, Japan

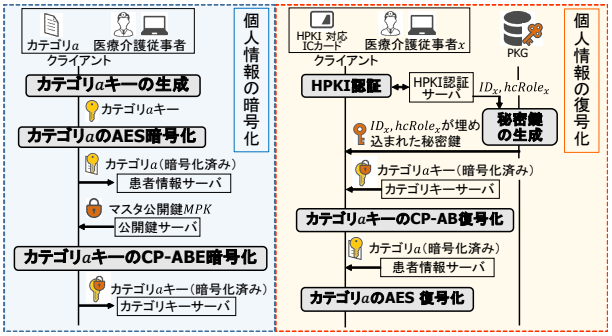

図 2: 暗号化及び復号化の手順（CP-ABE 方式）

ス構造とする．このようなアクセス構造によって，カテゴリ毎に緊急時に開示許可する職種を指定できる．図 2 にあるカテゴリ a の暗号化と復号化の手順を示す．

4　2 方式の処理時間の測定

2 方式における 1 カテゴリの暗号化と復号化の手順に要する計算処理の時間を表 1 に示す環境で測定した．

また，文献 [4] では，表 2 に示すように，在宅医療介護連携における標準的な共有情報を示しており，それらを項目分けしている．測定に際しては，中項目を提案方式における 1 カテゴリとし，処理対象ファイルは 1 KB のテキストファイルとした．また，各測定は 100 回試行の平均値をとっている．

暗号化処理は開示許可する人数を変化させて測定を行った．測定結果を図 3 に示す．開示許可人数が大きくなることで処理時間は長くなるが，その傾きは RSA 方式に比べて CP-ABE 方式の方が大きい結果となった．

復号化処理は対象ファイルが開示許可されている人数を変化させて測定を行った．測定結果を図 4 に示す．2 方式の処理時間は共にほぼ一定で，その大きさは RSA 方式が約 0.0013 秒，CP-ABE 方式が約 0.003 秒 であり，方式間の差は小さい．

5　実運用を想定した処理時間に関する考察

実際に医療介護従事者がシステムを利用する際，複数カテゴリをまとめて登録・閲覧することが考えられる．ここで，医師，歯科医師，薬剤師，看護師，介護支援専門員，理学療法士，歯科衛生士，介護福祉士の 8 職種によるケアチームを想定する．また，看護師と介護福祉士は 3 名ずつ，その他の職種は 1 名ずつとし，人数は計 12 名とする．

暗号化処理において複数カテゴリの処理が必要と考えられるのはシステムへの患者の初回登録である．このとき，少なくとも患者属性と住居・家族を登録することになるため，19 カテゴリの暗号化処理が発生する．図 3 における開示許可人数が 12 のときの値（0.079）より，その処理時間は $0.079 \times 19 = 1.50$ 秒程度である．この処理は基本的に初回登録の際にしか発生しないため，実用上大きな問題はない．

表 1: 測定環境

測定機器の仕様	CPU: Intel®Xeon®プロセッサー E3-1220 v3
	Memory: 16 GB
	OS: CentOS 6.6(64bit)
利用ライブラリ	RSA: OpenSSL(ver.1.0.1)
	CP-ABE: cpabe toolkit（cpabe-0.11，libbswabe-0.9）

表 2: 標準的な共有情報 [4]

大項目名	中項目数	小項目数
患者属性	13	32
住居・家族	6	23
医療	16	59
介護・生活	9	71
診療・ケア	8	51
合計	52	236

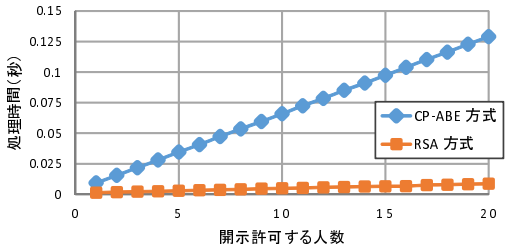

図 3: 1 カテゴリの暗号化処理時間

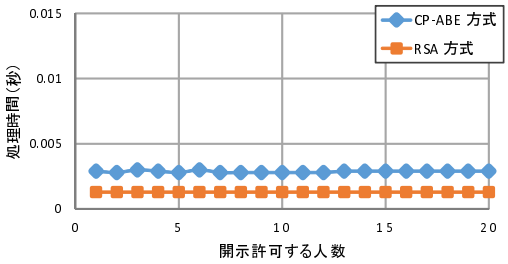

図 4: 1 カテゴリの復号化処理時間

復号化処理においては患者情報の一覧表示が考えられる．このとき，表 2 より，患者情報は合計で 52 の中項目に分けられるため，最大 52 カテゴリの復号化処理が発生する．図 4 より，その処理時間は $0.003 \times 52 = 0.156$ 秒程度であるため，実用可能な処理時間といえる．

6　おわりに

緊急時を考慮した暗号化された個人情報の HPKI 認証に基づく開示先制御方式を提案した．まず，RSA 暗号によって構成する方式を，次に秘密鍵管理コストの削減を図り，CP-ABE によって構成する方式を提案した．2 方式における暗号化および復号化処理時間を測定した結果，共に RSA 方式が短いことと，CP-ABE 方式においても実用可能な処理時間が示唆されることを確認した．今後の課題は，緊急時における開示許可条件の追加が挙げられる．

参考文献

[1] 厚生労働省：保健医療福祉分野 PKI 認証局認証用（人）証明書ポリシ 1.4 版 (online)，http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000112704.pdf,（参照 2017-11-02）.

[2] Bethencourt, J., Sahai, A. and Waters, B.: Ciphertext-policy attribute-based encryption, Proc. IEEE Symposium on Security and Privacy, pp.321-334(2007).

[3] 厚生労働省：医療情報システムの安全管理に関するガイドライン第 5 版 (online)，http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf,（参照 2017-11-02）.

[4] 在宅医療と介護の連携における情報システム利用に関するガイドライン検討委員会：在宅医療と介護の連携における情報システムの適切な利用を促進するためのガイドライン（草案）(online)，http://www.iog.u-tokyo.ac.jp/wp-content/uploads/2014/05/5435d2ad3a28ce3767b71b2bfb764856.pdf,（参照 2017-11-02）.

[5] 稲吉 陽一朗，白石 善明，竹尾 淳ほか：HPKI 認証を用いた在宅医療介護連携システムにおける個人情報の開示先制御，信学技報，vol.117，no.199，pp.51-56（2017）