情報処理学会論文誌 Vol.60 No.6 1228–1237 (June 2019)

推薦論文

# HPKI認証の特長を考慮した在宅医療介護システムにおける患者情報の開示先制御

竹尾 淳[1,†1,a)] 稲吉 陽一朗[1] 白石 善明[2,3] 加藤 昇平[1,4] 矢口 隆明[1,†2] 岩田 彰[1]

受付日 2018年9月6日, 採録日 2019年3月5日

**概要**：医療介護の場が病院から在宅へ移行するのにともない，医療介護従事者間の効率的な情報共有のためにICTシステムの活用が進んでいる．システムには患者の病状等の機微な情報が登録されるため，データベースの暗号化が望まれる．一方で，医療介護の特性から，平常時は，患者の担当従事者のみにアクセスを制限し，緊急時には，有資格者であれば，担当でなくともアクセスできる等，柔軟な開示先制御が求められる．本論文では，開示先制御が可能な暗号化方式として，RSA暗号を用いる方式と，暗号文ポリシー属性ベース暗号（CP-ABE）を用いる方式の2つを提案する．従事者本人および属性（保有資格）の認証には，保健医療福祉分野における公開鍵基盤（HPKI）を用いる．暗号化・復号の処理時間を評価した結果，RSA暗号方式はCP-ABE方式に比べ，短時間で処理されることが分かった．CP-ABE方式においても，システムとして実用可能な処理時間で動作することを確認した．

**キーワード**：在宅医療介護連携，開示先制御，HPKI，暗号文ポリシー属性ベース暗号

# Information Disclosing Mechanisms Using a Feature of the Healthcare PKI for Collaboration of Home Medical Care and Nursing

Jun Takeo[1,†1,a)] Yoichiro Inayoshi[1] Yoshiaki Shiraishi[2,3] Shohei Kato[1,4]
Takaaki Yaguchi[1,†2] Akira Iwata[1]

Received: September 6, 2018, Accepted: March 5, 2019

***Abstract:*** With the transition of a place of medical care and nursing from hospitals to homes, ICT systems are spreading to share information efficiency among multidisciplinary team. Since the ICT systems contain sensitive information of patients such as the medical condition, the database is desired to be encrypted. On the other hand, due to the nature of home medical care and nursing, ICT systems should have a flexible disclosing mechanisms such that the specific members can access the information normally although any qualified person can do in an emergency. In this paper, we propose two kinds of methods as controllable disclosing encryption mechanisms. One is the method with RSA encryption, the other is one with CP-ABE (Ciphertext-Policy Attribute-Based Encryption). To authenticate workers themselves and their accredited qualifications, we rely the HPKI (Healthcare PKI). An experimental result shows that the RSA based method can encrypt and decrypt the information faster than CP-ABE based one can do. We also mention that the CP-ABE based method can process the information permissively within a general ICT system.

***Keywords:*** collaboration of home medical care and nursing, disclosure control, healthcare public key infrastructure, ciphertext-policy attribute-based encryption

[1] 名古屋工業大学大学院工学研究科
Graduate School of Engineering, Nagoya Institute of Technology, Nagoya, Aichi 466–8555, Japan
[2] 神戸大学大学院工学研究科
Graduate School of Engineering, Kobe University, Kobe, Hyogo 657–8501, Japan
[3] 神戸大学数理・データサイエンスセンター
Center for Mathematical and Data Sciences, Kobe University, Kobe, Hyogo 657–8501, Japan
[4] 名古屋工業大学情報科学フロンティア研究院
Frontier Research Institute for Information Science, Nagoya Institute of Technology, Nagoya, Aichi 466–8555, Japan

[†1] 現在，株式会社コネクティボ
Presently with CONEXTIVO, Inc.
[†2] 現在，特定非営利活動法人医療介護健康情報学研究開発センター
Presently with Medical Care Health Informatics Research and Development Center
[a)] j.takeo.302@nitech.jp
本論文の内容は2017年12月の第79回CSEC研究発表会で報告され，同研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

## 1. はじめに

超高齢社会の進展にともない，住み慣れた街で老いを迎えられるよう，医療や介護の場が在宅に移行しつつある．1 人の患者・利用者（以下，単に「患者」とする）をケアする医療介護従事者（同じく「従事者」）は，医師，看護師，薬剤師，介護士等，多職種から構成される．病院や介護施設と異なり，在宅医療介護では，各従事者が異なる機関に属する場合が多く，互いに直接会う機会も乏しい．そのため，離れた場所でも容易に情報共有ができる仕組みが望まれる．ICT 利活用に関する調査 [1] では，在宅医療介護において，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ことが示されている．

在宅医療介護連携のための情報共有システムでは，機微な情報 [2] とされる患者の医療情報をはじめ，生活状況や家族に関する情報等，プライバシ性の高い個人情報を扱う．情報の漏洩や管理者権限を使った覗き見のリスクがあるため，サーバに情報を保存する際には，それらを暗号化することが望まれる．さらに，患者情報の開示は，あらかじめ決められたメンバに限定されなければならない．一般には，ケアチーム（患者のケアを担当する従事者グループ）にのみ患者情報が開示されるが，患者や家族の要望，一部従事者の配慮等により，開示範囲が変更される場合がある．すなわち，在宅医療介護向けの ICT 情報共有システムに適した患者情報の暗号化および開示先制御が望まれる．

開示先制御により高い機密性を実現するには，情報共有システムを利用する従事者を厳密に認証しなければならない．保健医療福祉分野では，患者のなりすましや情報の改竄防止を目的に，専用の公開鍵基盤（Healthcare Public Key Infrastructure: HPKI）が整備されている．平成 21 年度には，「保健医療福祉分野 PKI 認証局認証用（人）証明書ポリシ」[3] の策定が行われ，認証用の HPKI 証明書カードの発行が可能となった．従事者本人や保有資格を厳密に認証できるため，近年，電子カルテシステム等において利用が進んでいる．

患者のケアは，通常，ケアチームの従事者により行われる．しかし，災害時や患者の容態の急変時等は，ケアチーム外の従事者にも迅速な対応が求められ，状況に応じた患者情報の開示先制御が重要となる [4]．文献 [5] では，緊急時に，該当の患者情報にアクセス権を持っていない者が，本人の同意なしに患者情報を閲覧するには，少なくとも専門家（国家資格保有者）であることの担保が必要とされている．職種単位で安全に開示先が拡張される仕組みがあれば，緊急時，ケアチーム外の従事者による患者対応が可能となる．

職種等の属性を単位として暗号化・復号を行う方法の 1 つに，Bethencourt らが提案した属性ベース暗号の 1 種である暗号文ポリシー属性ベース暗号 CP-ABE（Ciphertext-Policy Attribute-Based Encryption）[6] の適用が考えられる．大東らは，ファイル共有サービスにおいて，ファイル内容に加え，ファイル名，および，パス名の暗号化・復号の手法を考案し，性能評価を行っている．その結果，ファイル転送に要する時間に対し，実用的な範囲で，ファイル，および，ファイル名，パス名を暗号化・復号することが可能であることを示している [7]．また，文献 [8] では，Eom らが CP-ABE を基本とした患者主体の健康情報のアクセス制御を提案し，性能を評価している．提案方式では緊急時におけるアクセス権の拡張も考慮されているが，健康情報にアクセスする人が拡張された属性を満たすかどうかの認証までは検討されていない．筆者らも，これまでに文献 [9], [10], [11] 等において，在宅医療介護連携向けの情報共有システムの研究開発を行ってきたが，認証に基づいた暗号化および柔軟な開示先の制御の議論は，必ずしも十分ではない．

そこで，本論文では，HPKI による認証によって担保される情報に基づき暗号化された患者情報の開示先制御として，2 方式を提案する．1 つは，代表的な公開鍵暗号である RSA（Rivest-Shamir-Adleman）暗号によって構成される方式であり，もう 1 つは，属性ベース暗号の 1 種である暗号文ポリシー属性ベース暗号 CP-ABE によって構成される方式である．そして，それらの暗号化・復号に要する時間を実機にて測定し，評価する．

## 2. 暗号文ポリシー属性ベース暗号（CP-ABE）

Bethencourt らが提案した CP-ABE [6] は，復号可能な属性集合（アクセス構造と呼ばれる）が指定された暗号文を生成できる方式である．復号の際，指定した属性がアクセス構造に含まれれば，暗号文は復号される．CP-ABE は次の 4 つのアルゴリズムからなる．

まず，PKG（Private Key Generator）と呼ばれる信頼された機関が，**Setup** においてマスタ公開鍵とマスタ秘密鍵を生成する．マスタ公開鍵はユーザに配布され，マスタ秘密鍵はセキュアに管理される．暗号化（**Encrypt**）では，配布されたマスタ公開鍵とアクセス構造を用い，平文を暗号化する．復号時は，**KeyGen** にて復号を希望する属性集合を反映したユーザ秘密鍵を生成し，それを用いて **Decrypt** にて復号を行う．

**Setup** セキュリティパラメータ $\lambda$ を入力として，マスタ公開鍵 $PK$ とマスタ秘密鍵 $MK$ を出力する．

**Encrypt** マスタ公開鍵 $PK$ と平文 $M$，および，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 $MK$ とユーザの属性集合 $S$ を入力として，ユーザ秘密鍵 $SK$ を出力する．

**Decrypt** マスタ公開鍵 $PK$ とユーザ秘密鍵 $SK$，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．

**Encrypt** で，暗号文に埋め込まれるアクセス構造は，式 (1) のように，職種や所属等を属性とした論理式の形で表現される．

人事部 and（部長 or 課長） (1)

この条件を満たす属性集合で生成されたユーザ秘密鍵のみ，暗号文を復号できる．

## 3. HPKI による認証

本章では，HPKI による認証を概説する．HPKI には，署名用証明書ポリシと認証用証明書ポリシが策定されている [12]．主として，前者は医療文書等への電子署名に，後者は従事者の本人認証および保有資格等の証明に用いられる．本論文では，本人認証および保有資格情報の取得に HPKI を使用するため，単に証明書と述べた場合は認証用証明書を指す．

HPKI による電子認証は PKI 認証と同様である．厚生労働省から認められた HPKI 認証局により公開鍵証明書が発行され，その検証により，本人認証が行われる．

証明書の基本領域には，Subject（HPKI 加入者名）フィールドがあり，その中にシリアル番号（SN）が記載される．SN に医籍登録番号等が登録される場合，SN にて加入者を一意に識別できる．それ以外の場合でも，SN と認証局の情報（Issuer）により，加入者を一意に識別可能である．

拡張領域には，ISO 17090 で規定される国家資格（**表 1**）や管理者等資格情報が記載される hcRole 属性が含まれる [3]．hcRole 属性により加入者の国家資格情報を確認できることは，HPKI 認証用証明書の特長の 1 つである．

## 4. 在宅医療介護連携における情報共有

在宅医療介護において，患者の疾患の種類が従事者の情報共有システムの利用動向に影響を及ぼしていることが報告されている [13]．文献 [13] は，ICT システムを使って在宅医療介護の情報共有が行われている先進地域にて，従事者が 1 年間に交わした文章・単語のデータ 6,342 件を調査分析している．

**表 2** には，5 種類の疾患別に，各職種の情報発信件数の割合が示される．「がん」の患者に対しては，看護師と医師が，それぞれ，41.8%と 39.4%の情報発信を行い，合わせて全体の 81.2%を占めている．一方，「肺疾患」の患者に対しては，看護師と介護支援専門員が，それぞれ，37.8%と 33.3%の情報発信を行い，全体の 71.1%を占めている．介護支援専門員は，疾患によっては看護師に次いで，情報共有システムから情報発信を行っている．

しかし，表 1 に示されるように，現在は hcRole 属性にその資格が含まれていない．本論文では，介護支援専門員も在宅医療介護において重要な役割を担っていると考え，hcRole 属性に介護支援専門員資格が存在するものとして議論する．

**表 1** hcRole 属性として記載可能である資格名 [3]
**Table 1** hcRole attribute (national qualification).

| 資格名（国家資格） | 説明 |
|---|---|
| ‘Medical Doctor’ | 医師 |
| ‘Dentist’ | 歯科医師 |
| ‘Pharmacist’ | 薬剤師 |
| ‘Medical Technologist’ | 臨床検査技師 |
| ‘Radiological Technologist’ | 診療放射線技師 |
| ‘Registered Nurse’ | 看護師 |
| ‘Public Health Nurse’ | 保健師 |
| ‘Midwife’ | 助産師 |
| ‘Physical Therapist’ | 理学療法士 |
| ‘Occupational Therapist’ | 作業療法士 |
| ‘Orthoptist’ | 視能訓練士 |
| ‘Speech Therapist’ | 言語聴覚士 |
| ‘Dental Technician’ | 歯科技工士 |
| ‘National Registered ‘Dietitian’ | 管理栄養士 |
| ‘Certified Social Worker’ | 社会福祉士 |
| ‘Certified Care Worker’ | 介護福祉士 |
| ‘Emergency Medical Technician’ | 救急救命士 |
| ‘Psychiatric Social Worker’ | 精神保健福祉士 |
| ‘Clinical Engineer’ | 臨床工学技士 |
| ‘Massage and Finger Pressure Practitioner’ | あん摩マッサージ指圧師 |
| ‘Acupuncturist’ | はり師 |
| ‘Moxibustion Practitioner’ | きゅう師 |
| ‘Dental Hygienist’ | 歯科衛生士 |
| ‘Prosthetics & Orthctic’ | 義肢装具士 |
| ‘Artificial Limb Fitter’ | 柔道整復師 |
| ‘Clinical Laboratory Technician’ | 衛生検査技師 |

**表 2** 疾患・職種別情報発信件数の割合（%）[13]
**Table 2** Percentage of information transmission by disease and job type.

| | がん | 認知症 | 心疾患 | 肺疾患 | 骨折 |
|---|---|---|---|---|---|
| 医師 | 39.4 | 14.5 | 17.4 | 13.3 | 11.4 |
| 歯科医師 | 0.0 | 5.1 | 6.7 | 15.6 | 9.3 |
| 薬剤師 | 6.4 | 0.2 | 1.2 | 0.0 | 5.5 |
| 看護師 | 41.8 | 18.1 | 21.4 | 37.8 | 18.1 |
| 介護支援専門員 | 5.8 | 16.1 | 17.4 | 33.3 | 26.2 |
| 理学療法士 | 5.5 | 4.2 | 15.9 | 0.0 | 8.4 |
| 歯科衛生士 | 0.3 | 3.2 | 7.0 | 0.0 | 15.2 |
| 介護職 | 0.9 | 38.6 | 13.0 | 0.0 | 5.9 |

## 5. 提案方式

本章では，患者情報の開示先制御を可能とする暗号化方式として，次の 2 方式を提案する．それぞれ，開示先の従事者ごとに鍵管理を行う方式と，属性（職種，従事者）を指定して鍵管理を行う方式である．前者は代表的な公開鍵暗号方式である RSA 暗号を利用し，後者は 2 章で述べた

表 3 標準的な共有情報 [15]
**Table 3** Standard information to be shared.

| 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 |

CP-ABE を適用する．以降，前者を RSA 暗号方式，後者を CP-ABE 方式とする．

提案方式の導入を想定しているシステムは本論文では次のとおりである．まず，サーバにログインするときは，クライアント PC に接続された IC カードリーダにて HPKI カードを読み取り，ID および hcRole 属性をシステムへ送信する．サーバとクライアントの間は，VPN（Virtual Private Network）や HTTPS（HyperText Transfer Protocol Secure）通信等で暗号化され，暗号化された患者情報や鍵等が通信路上で盗聴されないとする．暗号化された患者情報，および後述する秘密鍵，公開鍵，カテゴリキーは可能な限りそれぞれ別のサーバに格納して，サーバ管理者による患者情報の窃視（復号）を防ぐこととする．そして，クライアント PC での暗号化・復号処理を含むプログラムは平文や鍵を漏えいすることなく信頼できるか，漏えいが懸念されるアクセスがあった場合にはしかるべき対応がとれるように検知できる環境で動作するものとする．

厚生労働省による医療情報システムに関するガイドライン [14] では，従事者や職種によって，アクセスできる患者情報に範囲を設けることとされている．ガイドラインに従うため，本論文では患者情報を複数のカテゴリに分類し，カテゴリを単位として開示先制御を行う．具体的なカテゴリは文献 [15] に従う（**表 3**）．

カテゴリごとに開示先を制御するため，各カテゴリに含まれる患者情報は，そのカテゴリ固有の鍵（カテゴリキー）によって暗号化される．RSA 暗号方式では，カテゴリキーの配送・管理を従事者ごとに行う．一方，CP-ABE 方式では，それを従事者や職種等の属性ごとに行う．

なお，患者情報自体はカテゴリキーにより暗号化・復号するが，これには公開鍵暗号に比べて処理が高速な，共通鍵暗号（AES: Advanced Encryption Standard）を用いる．これらの手順は，Benaloh らによる暗号化保管された情報の開示先制御 [16] を参考にしている．

### 5.1 RSA 暗号方式

RSA 暗号方式では，あらかじめ開示先ごとに RSA 鍵ペアを生成する．生成した RSA 鍵ペアのうち公開鍵と秘密鍵は，それぞれ，公開鍵サーバと秘密鍵サーバにて保管される．

開示先制御は，従事者単位で行う方法と職種単位で行う方法が考えられる．従事者単位で開示先制御を行う場合は，従事者ごとに RSA 鍵ペアを生成する．この場合は，従事者数分の鍵ペアが必要となる．一方，4 章で述べたように，職種ごとに従事者と患者の関わりが異なることを考慮した場合は，ケアチーム内においても職種による開示先制御が必要とされる．この場合，職種単位で RSA 鍵ペアを作成する．全ケアチーム（すなわち，全患者）について，各ケアチームを構成する職種数の総和の鍵ペア数を要する．

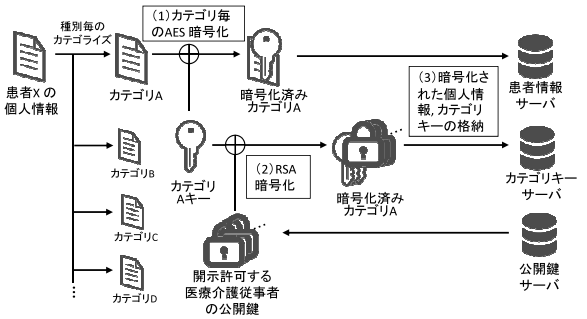


図 1 患者情報の暗号化（RSA 暗号方式）
**Fig. 1** Encryption of patient information (RSA encryption method).

筆者らはこれまでに，在宅医療介護の情報共有システムにおいて，従事者単位で鍵ペアを生成する場合と，各ケアチームにおける職種単位でそれを生成する場合とを比較した．その結果として，前者がより少ない鍵ペアとなることを明らかにしている [11]．したがって，鍵管理コストの観点から，RSA 暗号方式においては従事者単位に RSA 鍵ペアを生成し，開示先制御を行うこととする[*1]．次節から，この方式における患者情報の暗号化と復号，および開示先の追加・削除を説明する．

#### 5.1.1 患者情報の暗号化

患者情報を暗号化する手順は**図 1** のとおりである．図 1 では，患者 X の患者情報の 1 つのカテゴリ A の暗号化手順を示している．

(1) カテゴライズされた患者情報（カテゴリ A 情報）を，カテゴリごとに生成したカテゴリ A キーで AES 暗号化する．
(2) 開示許可する従事者全員の公開鍵を公開鍵サーバから取り出し，それぞれの公開鍵でカテゴリ A キーを RSA 暗号化する．カテゴリキーは，開示許可された人数分，複製される．
(3) 暗号化済みカテゴリ A 情報と暗号化済みカテゴリ A キーを，それぞれ，患者情報サーバとカテゴリキーサーバに格納する．

[*1] RSA 暗号方式において，後述の CP-ABE 方式と同等のアクセス制御を実現するには，想定するすべての属性数分の鍵ペアを要する．本 CP-ABE 方式では，属性として，従事者 ID，および，緊急時開示先職種を想定するため，RSA 暗号方式における鍵ペアは，従事者数に加え，患者ごとの緊急時開示先職種単位の総和分が必要となる．

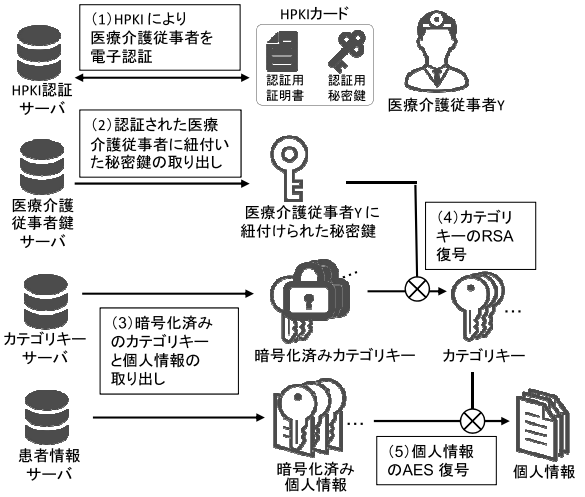


図 2 患者情報の復号（RSA 暗号方式）

**Fig. 2** Decryption of patient information (RSA encryption method).

### 5.1.2 患者情報の復号

患者情報を復号する手順は**図 2** のとおりである．図 2 は，従事者 Y が患者情報を復号する手順を示している．

(1) HPKI により従事者 Y を電子認証する．
(2) 医療介護従事者鍵サーバから，認証された従事者 Y の ID に紐付けられた秘密鍵を取り出す．
(3) (2) の秘密鍵に対応する暗号化済みカテゴリキーと，そのカテゴリキーに対応する暗号化済みカテゴリ情報を，それぞれ，カテゴリキーサーバと患者情報サーバから取り出す．
(4) (2) の秘密鍵で暗号化済みカテゴリキーを RSA 復号する．
(5) (4) で得られたカテゴリキーで，該当の暗号化済みカテゴリ情報を AES 復号する．

### 5.1.3 開示先の追加・削除

患者情報の開示先の追加手順は**図 3** のとおりである．図 3 は，従事者 Y がある患者のカテゴリ A 情報の開示先に別の従事者を追加する手順を示している．開示先の追加は，すでに開示許可されている者（この例では従事者 Y）が操作を行うものとする[*2]．

(1) HPKI により，従事者 Y を電子認証する．
(2) 医療介護従事者鍵サーバから，認証された従事者 Y の ID に紐付けられた秘密鍵を取り出す．
(3) (2) の秘密鍵に対応する暗号化済みカテゴリ A キーを，カテゴリキーサーバから取り出す．
(4) (2) の秘密鍵で暗号化済みカテゴリ A キーを RSA 復号する．
(5) 開示先として追加したい従事者の ID に紐付いた公開鍵を公開鍵サーバから取り出す．その公開鍵を用い，(4) で復号したカテゴリキーを RSA 暗号化する．
(6) 暗号化済みカテゴリ A キーをカテゴリキーサーバに格納する．

なお，すでに開示先として追加されている従事者を開示先から削除する場合には，その従事者に対応する暗号化済みカテゴリキーを，カテゴリキーサーバから削除するのみでよい．

[*2] 開示先を編集できる者を，ケアチーム内の特定の職種やメンバに制限することは機能上可能である．しかし，実際の運用では，実務効率を優先して，開示先を編集できる者を制限しないケースがある．この場合，メンバを追加したい者は，あらかじめ他のケアチームメンバの同意を得たうえで操作を行う．

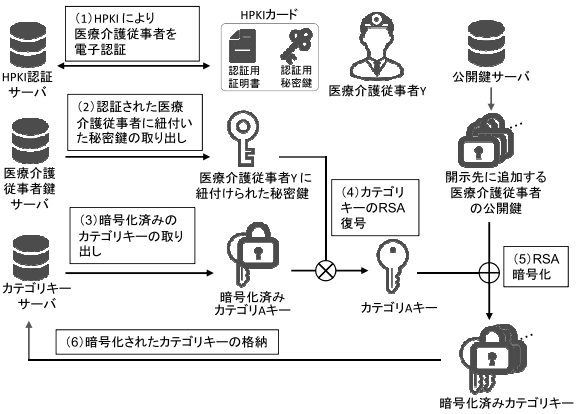


図 3 開示先の追加（RSA 暗号方式）

**Fig. 3** Addition of a disclosure destination (RSA encryption method).

## 5.2 CP-ABE 方式

5.1 節の RSA 暗号方式では，カテゴリキーは従事者ごとの公開鍵にて暗号化された．CP-ABE 方式では，従事者 ID や職種等，開示を可能とする対象を論理式で表現し，これをアクセス構造として暗号文に埋め込む．たとえば，ある患者のあるカテゴリの開示先が従事者 2 名（それぞれの ID を 330001，330002 とする）の場合，アクセス構造は式 (2) となる．

$$(\mathrm{ID} = 330001)\ \mathrm{or}\ (\mathrm{ID} = 330002) \tag{2}$$

特定の条件において，属性単位で開示先を指定する例を式 (3) に示す．この例では，従事者 ID が論理和で記され，条件と属性が論理積で記される．緊急時フラグ（*emergency* とする）が設定されると，医師資格を持つユーザ（hcRole 属性が *Medical_Doctor* であるユーザ）が開示先となる．

$$\begin{aligned}&(\mathrm{ID} = 330001)\ \mathrm{or}\ (\mathrm{ID} = 330002)\\ &\quad \mathrm{or}\ (\mathit{emergency}\ \mathrm{and}\ \mathit{Medical\_Doctor})\end{aligned} \tag{3}$$

緊急時フラグに関し，“緊急時” の定義，および，緊急時の開示先は，あらかじめ，システムの利用者等で決めておく運用が想定される．たとえば，災害時はケアチームに関係なく，従事者の資格に応じた開示範囲へ拡張される，また，急変時にかかりつけ医が対応できない場合は医師資格を持つユーザが開示先となる等である．緊急時モードへの移行は，システム管理者や管理者等資格を有する者により

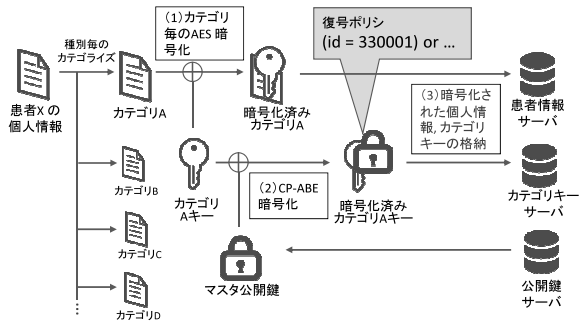


図 4 患者情報の暗号化（CP-ABE 方式）

**Fig. 4** Encryption of patient information (CP-ABE method).

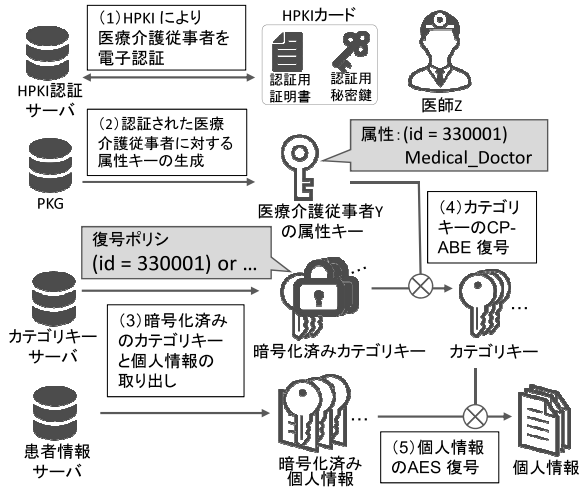


図 5 患者情報の復号（CP-ABE 方式）

**Fig. 5** Decryption of patient information (CP-ABE method).

行われるケースが予想される*3.

以下，CP-ABE 方式における患者情報の暗号化と復号，および，開示先の追加・削除を説明する．なお，各手順において，前述の対応する RSA 暗号方式と同様である部分は“(RSA 暗号方式と同様)”と表す．

### 5.2.1 患者情報の暗号化

患者情報の暗号化手順は，**図 4** のとおりである．図 4 では，患者 X のカテゴリ A 情報の暗号化手順を示している．

(1) (RSA 暗号方式と同様)

(2) マスタ公開鍵を公開鍵サーバから取り出し，開示先が記されたアクセス構造とマスタ公開鍵でカテゴリ A キーを暗号化する．

(3) (RSA 暗号方式と同様)

### 5.2.2 患者情報の復号

患者情報の復号手順は**図 5** のとおりである．図 5 は，医師 Z が患者情報を復号する手順を示している．

(1) (RSA 暗号方式と同様)

(2) PKG が，アクセス構造を埋め込んだ属性キーを生成する．

(3) (RSA 暗号方式と同様)

*3 管理者等資格も HPKI により認証が可能である [3].

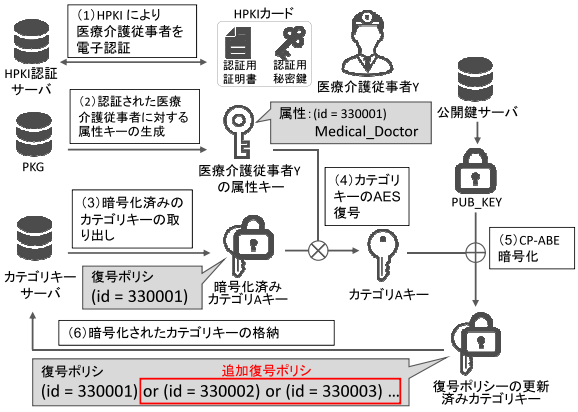


図 6 開示先の追加（CP-ABE 方式）

**Fig. 6** Addition of a disclosure destination (CP-ABE method).

(4) (2) で生成した属性キーでカテゴリキーを復号する．

(5) (RSA 暗号方式と同様)

なお，医師 Z がシステムからログアウトすると，属性キーは削除される．したがって，秘密鍵である属性キーの管理が不要となり，RSA 暗号方式に比べ，CP-ABE 方式は鍵管理コストの面から有利である．

### 5.2.3 開示先の追加，削除

患者情報の開示先追加手順は**図 6** のとおりである．図 6 は，従事者 Y がカテゴリ A 情報の開示先を追加する手順を示している．開示先の追加は，すでに開示が許可されている者（この例では従事者 Y）が操作することとする*4.

(1) (RSA 暗号方式と同様)

(2) PKG が，アクセス構造を埋め込んだ属性キーを生成する．

(3) (RSA 暗号方式と同様)

(4) (2) で生成した属性キーで，暗号化済みカテゴリ A キーを CP-ABE 復号する．

(5) マスタ公開鍵を公開鍵サーバから取り出す．開示先として追加したい従事者 ID や hcRole 属性を追加したアクセス構造とマスタ公開鍵を用い，(4) で復号したカテゴリ A キーを CP-ABE 暗号化する．

(6) (RSA 暗号方式と同様)

開示許可されている従事者や職種を削除する場合も，本節の手順に従う．ただし，上記 (5) において，削除したい属性を除いた論理式をアクセス構造とする．なお，ユーザが退職や異動となる場合も，該当ユーザが開示許可されている患者情報のアクセス構造から，上述の方法で従事者 ID を削除する．

一方，ユーザが属性 (hcRole 属性) を失うが，ケアチームの構成は変化しない場合（たとえば，管理者等資格を失う場合等）は，患者情報のアクセス構造は変化しない．このとき，属性を失う前の属性キーやカテゴリキーを何らかの方法で取得していれば，そのキーで患者情報を復号できる

*4 脚注*2 参照.

可能性がある．しかし，本論文のシステムでは，CP-ABE による暗号化に加え，システム自体も hcRole 属性に基づいたアクセス制御を行う．属性を失ったユーザが HPKI カードを使おうとしても，カードは認証局で失効処理されているため，システムではログイン時に hcRole 属性が認証されず，ユーザは該当属性に関する患者情報にアクセスできない．

## 6. 暗号化および復号時間の測定

ケアチームに属する従事者の人数，すなわち，開示先として指定される人数が，患者情報の登録や閲覧に及ぼす影響を調査するため，提案方式の暗号化・復号時間を測定する．

### 6.1 測定の環境および方法

CP-ABE の実装には，Bethencourt ら [6] が開発した C 言語のオープンソースのライブラリ Ciphertext-Policy Attribute-Based Encryption（バージョン 0.11）を利用する．このライブラリは，$(k, n)$ 閾値秘密分散法によって CP-ABE におけるアクセス構造の論理演算を実現している．属性数を $n$ とした場合，秘密情報を $n$ 個に分散し，各属性に対応付けた鍵で暗号化する．これらの属性の論理積（AND）を行う場合，復号に必要な分散情報の数 $k$ は $n$ と等しくなる．和結合（OR）の場合，$k$ は 1 となる．

ペアリング演算には PBC（Pairing-Based Cryptography）ライブラリ（バージョン 0.5.12）[17] を用いる．デフォルトのパラメータ `a`（`a.param`）では 1,024 bit で演算されるため，鍵長 2,048 bit の RSA 暗号と同等の暗号強度となるよう，パラメータを `a1`（`a1.param`）に変更している．

このライブラリでは，対象の平文を AES（鍵長 128 bit，CBC モード）で暗号化する．この処理には OpenSSL（バージョン 1.0.1e）の AES 暗号化関数を利用している．

一般的に，患者情報の暗号化・復号は，クライアント側で行われるが，本論文では簡単にするためサーバ側で行うこととする．サーバは，CPU に Intel Xeon プロセッサ E3-1220 v3 を持ち，メモリは 16 GB 搭載している．OS には CentOS 6.6（64-bit）を用いる．

患者情報のカテゴリ分けは，表 3 における中項目にて行う．1 カテゴリに 512 文字記入されると想定することから，暗号化対象ファイルは 1 KB のテキストファイルとする．

実験では，開示許可人数を変動させ，提案する 2 方式の暗号化・復号に要する時間を測定する．それぞれ 100 回の測定を行い，それらの平均値を求める．なお，AES によるカテゴリ情報の暗号化・復号に要する時間は，RSA 暗号および CP-ABE による処理に比べて十分短いため，本論文では議論の対象としない．

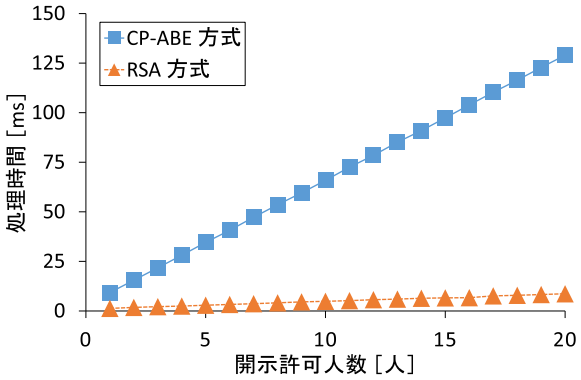


図 7 1 カテゴリの暗号化に要する処理時間
**Fig. 7** Processing time to encrypt one category.

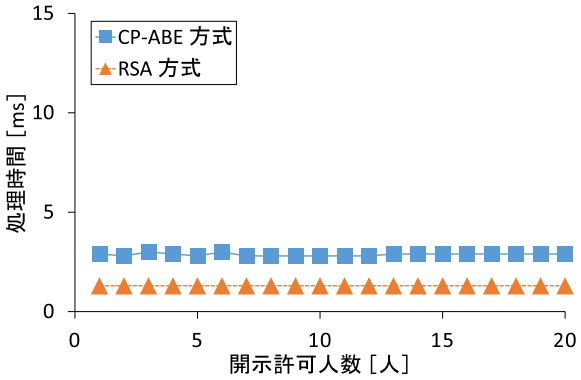


図 8 1 カテゴリの復号に要する処理時間
**Fig. 8** Processing time to decrypt one category.

### 6.2 測定結果と考察

図 7 に，開示許可人数に対する暗号化処理時間を示す．RSA 暗号方式および CP-ABE 方式ともに，開示許可人数の増加にともない，暗号化にかかる時間が増加している．また，開示許可人数の増加にともなう処理時間の増加は，RSA 暗号方式に比べて CP-ABE 方式が著しい．これは，CP-ABE 方式では，アクセス構造に含まれる属性が増えると，暗号化処理負荷が高くなるためである．一方，RSA 暗号方式では，開示許可人数分の RSA 暗号化を繰り返すのみであり，比較的高速に処理される．

復号処理時間の測定結果は図 8 に示される．2 方式とも，開示許可人数による復号時間の変化は見られず，RSA 暗号方式が約 1.3 ms，CP-ABE 方式が約 3 ms である．

本測定における CP-ABE 方式では，開示許可人数を増加させる際，アクセス構造に従事者 ID を追加する．すなわち，アクセス構造における論理和で記述される部分が伸長する．論理和で記された部分は 1 回の処理で照合が可能であるため，復号に要する時間は開示許可人数によらず，ほぼ一定である．

なお，論理積で指定された部分の照合には，論理積の評価回数分の処理が発生する．たとえば，式 (3) のアクセス構造では，まず，緊急時フラグ（*emergency*）が評価され，真の場合はさらに，医師であるか（hcRole 属性が

*Medical_Doctor* を含むか）が評価される．

## 7. 情報共有システムの実運用を想定した考察

実際に従事者が情報共有システムを利用する際，複数カテゴリをまとめて登録・閲覧することが想定されるため，それに要する時間を考察する．ここでは，文献 [13] に基づき，8 職種（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）からなるケアチームを想定する．看護師と介護福祉士は 3 名ずつ，そのほかの職種は 1 名ずつとし，合計 12 名と想定する．

暗号化処理において，複数カテゴリの処理が必要となるのは，患者の新規登録時である．このとき，少なくとも，患者の属性と住居，家族を登録することになる．そのため，19 カテゴリの暗号化処理が同時に発生する．図 7 では，開示許可人数が 12 人のとき，CP-ABE 方式では暗号化に約 79 ms 要する．したがって，19 カテゴリの登録には，約 1.5 秒（79 ms × 19 カテゴリ）かかる．この処理は，原則，情報共有システムへ患者を新規に登録する際にのみ行われるため，システムの利用上，大きな問題は生じない．

一方，復号処理が集中するケースには，患者情報の一覧表示等がある．この場合は，表 3 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 カテゴリの復号処理が発生する．図 8 から，CP-ABE 方式の復号処理時間は約 3 ms であるため，52 カテゴリの復号に要する時間は 156 ms（3 ms × 52 カテゴリ）程度である．システムの他の処理も含めた場合においても，暗号化・復号は操作には影響を及ぼさない範囲で可能であるといえる．

なお，CP-ABE 方式における復号では，HPKI による認証後，従事者 ID と hcRole 属性に対応する属性キーの生成が PKG により行われる．この処理時間を測定したところ 219 ms であった．この属性キーの生成は，ログインの後，患者情報を復号するまでの間に実行されればよい．ログイン後にバックグラウンドで処理を行う等，情報共有システムの操作に影響を及ぼさないタイミングで属性キーの生成が可能である．

## 8. おわりに

本論文では，機微な情報を扱う在宅医療介護向けの情報共有システムにおいて，HPKI 認証に基づいた患者情報の適切な開示のため，暗号化技術を使った開示先制御を 2 方式提案した．RSA 暗号によって開示先制御を行う方式，および CP-ABE 暗号によって属性ベースで開示先制御を行い，緊急時の柔軟な開示先制御と秘密鍵管理コストの削減が可能な方式である．また，属性失効されたユーザがアクセスを試みたとしても，5 章のシステムの仮定を満たすならば患者情報の閲覧はできない．

実機により，患者情報の暗号化および復号処理にかかる時間を測定した結果，ともに RSA 暗号方式が短時間であること，および CP-ABE 方式においても十分に短い時間で処理できることを明らかにした．さらに，在宅医療介護の実態を考慮し，情報共有システムの利用を想定した場合においても，暗号化・復号に要する時間が，操作に大きく影響を及ぼすものではないことを確認した．

本論文では，属性ベースの開示先制御の第 1 歩として，職種等を単位とした開示制御可能な方式を扱った．情報共有システムの利用状況を考慮したアクセス構造の検討が今後の課題である．

**謝辞** 本研究は，文部科学省未来医療研究人材養成拠点形成事業によって行われた．

### 参考文献

[1] 株式会社情報通信総合研究所：地域における ICT 利活用の現状に関する調査研究報告書（オンライン），入手先 ⟨http://www.soumu.go.jp/johotsusintokei/linkdata/h27_07_houkoku.pdf⟩（参照 2017-11-02）．

[2] 経済産業省：JIS Q 15001:2006（オンライン），入手先 ⟨http://www.meti.go.jp/policy/it_policy/privacy/jis_shian.pdf⟩（参照 2017-11-02）．

[3] 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（オンライン），入手先 ⟨https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000112704.pdf⟩（参照 2017-11-02）．

[4] 笠井敬介，川越恭二：状況変化を考慮した利用者個人情報のアクセス制御モデルの構築，コンピュータセキュリティシンポジウム 2009（CSS2009）論文集，pp.1–6 (2009).

[5] 厚生労働省医政局医療情報ネットワーク基盤検討作業班：個人が自らの医療情報を管理・活用する基盤を構築する際に必要となる医療従事者の認証方式について，入手先 ⟨https://www.mhlw.go.jp/shingi/2009/02/dl/s0213-8e.pdf⟩（参照 2018-08-30）．

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

[7] 大東俊博，後藤めぐ美，西村浩二，相原玲二：暗号文ポリシー属性ベース暗号を利用したファイル名暗号化ファイル共有サービスの実装と性能評価，情報処理学会論文誌，Vol.55, No.3, pp.1126–1139 (2014).

[8] Eom, J., Lee, D.H. and Lee, K.: Patient-Controlled Attribute-Based Encryption for Secure Electronic Health Records System, *J. Med. Syst.*, Vol.40, No.12, p.253 (2016).

[9] 立田太一，溝口 航，白石善明ほか：在宅医療介護情報連携システムにおける連結可能匿名化とハイブリッド暗号方式を組み合わせたセキュアな個人情報管理手法，信学技報，Vol.112, No.466, pp.65–70 (2013).

[10] 小倉裕史，井上 航，竹尾 淳ほか：地域包括ケアシステム「なごやかスマイルネット」，信学技報，Vol.115, No.486, pp.151–156 (2016).

[11] 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).

[12] 厚生労働省：保健医療福祉分野 PKI（HPKI）認証局 — 医療分野の情報化の推進について（オンライン），入手先 ⟨https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html#HID4⟩（参照 2018-08-27）．

[13] 在宅医療と介護の多職種連携に関する調査研究委員会：在宅医療と介護の連携のための情報システムの共通基盤のあり方に関する調査研究報告書（オンライン），入手先 ⟨http://www.iog.u-tokyo.ac.jp/wp-content/uploads/2015/04/01667ff78127f3599d21c25a6906f782.pdf⟩（参照 2017-11-02）.
[14] 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（オンライン），入手先 ⟨http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf⟩（参照 2017-11-02）.
[15] 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）（オンライン），入手先 ⟨http://www.iog.u-tokyo.ac.jp/wp-content/uploads/2014/05/5435d2ad3a28ce3767b71b2bfb764856.pdf⟩（参照 2017-11-02）.
[16] Benaloh, J., Chase, M., Lauter, K., et al.: Patient controlled encryption: Ensuring privacy of electronic medical records, *Proc. ACM CCSW 2009*, pp.103–114 (2009).
[17] Ben Lynn: PBC Library – Pairing-Based Cryptography (online), available from ⟨https://crypto.stanford.edu/pbc/⟩ (accessed 2018-12-19).

**推薦文**

本稿は，保険医療分野専用の公開鍵基盤（HPKI）に焦点を当てたうえで，HPKIによる認証によって担保される情報に基づいて暗号化された個人情報の開示先制御を行う方式を提案している．在宅医療介護システムという，即時性が求められる状況下において，実用に耐えうる個人情報開示先制御方式を模索した本論文の重要度は高いと考え，推薦する．

（コンピュータセキュリティ研究会主査　寺田雅之）

**竹尾 淳**

平成12年名古屋工業大学工学部電気情報工学科卒業．平成14年同大学大学院博士前期課程修了．平成17年株式会社三洋電機．平成21年名古屋工業大学大学院博士後期課程修了．平成22年株式会社ソフテル．平成25年名古屋工業大学医療介護健康情報学研究所プロジェクト研究員．平成26年同大学特任助教．平成30年HAL名古屋高度情報処理学科．平成31年より株式会社コネクティボ．博士（工学）．ICTシステムに関する教育・業務に従事．IEEE，電子情報通信学会，映像情報メディア学会，日本静脈経腸栄養学会各会員．

**稲吉 陽一朗**

平成28年名古屋工業大学工学部情報工学科卒業．平成30年同大学大学院博士前期課程修了．在学時は，医療介護系ICT情報共有システムにおける個人情報管理に関する研究に興味を持つ．

**白石 善明**　（正会員）

平成7年愛媛大学工学部情報工学科卒業．平成9年同大学大学院博士前期課程修了．平成12年徳島大学大学院博士後期課程修了．平成14年近畿大学理工学部情報学科講師．平成18年名古屋工業大学大学院情報工学専攻助教授．平成25年より神戸大学大学院工学研究科電気電子工学専攻准教授．博士（工学）．情報セキュリティ，コンピュータネットワーク等の研究・教育に従事．平成14年電子情報通信学会オフィスシステム研究賞，平成15年暗号と情報セキュリティシンポジウム（SCIS）20周年記念賞，平成18年SCIS論文賞．平成19，20，23，25年情報処理学会DICOMO 2007，2008，2011，2013優秀論文賞．平成27年同会高度交通システム研究会優秀論文賞．平成29年電子情報通信学会関西支部活動功労賞．平成28年より同会情報通信システムセキュリティ研究専門委員会委員長．電子情報通信学会シニア会員．

**加藤 昇平**　（正会員）

平成5年名古屋工業大学工学部電気情報工学科卒業．平成10年同大学大学院博士後期課程修了．同年豊田工業高等専門学校助手，平成11年同講師，平成14年名古屋工業大学講師，平成15年同助教授．現在，同大学大学院情報工学専攻教授．博士（工学）．知能・感性ロボティクス，知識推論・計算知能，ヒューマンインタラクション，医工連携情報処理等に関する研究に従事．平成18年日本感性工学会技術賞，平成22年日本知能情報ファジィ学会論文賞，平成24年日本感性工学会論文賞，平成27年文部科学大臣表彰科学技術賞（研究部門）等を受賞．IEEE，ACM，電子情報通信学会，人工知能学会，日本ロボット学会，日本感性工学会，日本認知症学会各会員．

**矢口 隆明** （正会員）

昭和 63 年株式会社クリエイティブエイジェンシーコマンド設立．平成 20 年特定非営利活動法人 ITC 中部理事長．平成 22 年名古屋工業大学大学院博士後期課程修了．平成 24 年同大学医療介護健康情報学研究所副所長．同大学特任教授．平成 24 年特定非営利活動法人医療介護健康情報学研究開発センター設立・理事長．博士（工学）．医工学における医療システムおよび IoT 等，在宅医療介護のユビキタス ICT システムの研究に従事．日本医療情報学会，情報文化学会各会員．

**岩田 彰** （正会員）

昭和 48 年名古屋大学工学部電気学科卒業．昭和 50 年同大学大学院博士前期課程修了．同年名古屋工業大学助手，昭和 60 年助教授，平成 5 年教授，平成 14 年副学長（専任），平成 16 年同大学大学院教授．平成 28 年より同大学名誉教授．博士（工学）．医用情報処理，情報セキュリティ，ニューラルネットワーク等に関する研究に従事．平成 5 年電子情報通信学会論文賞，平成 10 年情報処理学会 BestAuthor 賞等を受賞．著書『インターネット暗号化技術 —PKI，RSA，SSL，S/MIME，etc.—』（監修），ソフト・リサーチセンター（平成 14 年），『ディジタルシグナルプロセッシング』（編著），コロナ社（平成 20 年）等．本会終身会員．