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

笠井 敬介 †　　川越 恭二 ‡

† 立命館大学大学院理工学研究科
〒 525-8577 滋賀県草津市野路東 1-1-1
kasai@coms.ics.ritsumei.ac.jp

‡ 立命館大学情報理工学部
〒 525-8577 滋賀県草津市野路東 1-1-1.

あらまし　救助活動や医療活動において，被災者や患者の個人情報を公開することにより業務の円滑化を図るシステムが求められる．このシステムでは個人情報に対するアクセス制御を動的に変更することで利用者のプライバシーを保護する機能が必要となる．しかし，既存アクセス制御手法は個人情報へのアクセス権限を一意に設定するため，システムを構築する際に直接に適用することができない．そこで，我々は既に利用者の状況に応じた利用者個人情報のアクセス制御を可能とするアクセス制御モデルを提案している．提案モデルは既存アクセス制御手法の考え方を基本とし，状況という新たな概念を導入する．本稿では，提案モデルを実現することでその有効性を示す．

Construction of Personal Information Access Control Model with Consideration of Context Change

Keisuke Kasai†　　Kyoji Kawagoe‡

†Graduate School of Science and Engineering, Ritsumeikan University
Nojihigashi 1-1-1, Kusatsu, Shiga, 525-8577 Japan.
kasai@coms.ics.ritsumei.ac.jp
‡College of Information Science and Engineering, Ritsumeikan University
Nojihigashi 1–1–1, Kusatsu, Shiga, 525–8577 Japan

Abstract　A communication system of sharing and exchanging users personal information is demanded in the case of emergencies such as medical scene and disaster. In such a system, personal information access control depending on the context of user is greatly necessary. However, it is complicated to manage personal information access control directly, because existing technique determine access control uniformly. Therefore we proposed a new access control model that enables access control of user personal information with consideration of context change. Our proposed model is based on a concept of existing technique, which is an extension of a conventional model. We also introduce a concept of situation in our model. In the paper, we describe realization of our proposed access control model.

1　はじめに

近年，ユビキタス技術の発達や普及により，位置情報のような利用者個人に関する情報に基づき様々な情報を提供するサービスが注目されている．例えば，医療現場における患者の個人情報管理システムや災害時情報伝達支援システ

ムが挙げられる．医療現場における患者の個人情報管理システムは，電子カルテなどが保持する患者の個人情報を担当関係者にのみ開示することによって患者の個人情報を保護するシステムである．また，災害時情報伝達支援システムは，利用者の位置情報や連絡先などの個人情報を公開・共有することによって情報伝達を行うシステムである．このシステムによって災害時の連絡網・災害情報・避難場所・集合場所の告知をはじめ，被災者の個人情報の公開による救助活動の効率化が可能となる．医療現場における患者の個人情報管理システムや災害時における情報伝達支援システムは，利用者の個人情報に基づいて利用者の状況に応じた情報提供を行う．そのため，これらのシステムを利用する際には，利用者による氏名や現在位置のような個人情報の提供を行うことが前提となる．この時，利用者の重要な個人情報を保護するため，これらのシステムには利用者の状況に応じて個人情報に対するアクセス制御を行う機能が必要となる．しかし，既存のアクセス制御モデルは利用者やアクセス対象のオブジェクトの状況変化に対応する機能を必要とする環境を対象としていないため，個人情報へのアクセス権限を一意に設定することが一般的である．そのため，先例における病院患者の個人情報管理システムや災害時情報伝達支援システムのような利用者の状況変化がアクセス制御の起点となる環境に対して直接適用することができないという問題がある．

そこで，我々は既に利用者とオブジェクトの状況に応じた利用者個人情報のアクセス制御を可能とするアクセス制御モデルの提案を行った．提案モデルは，Role-based Access Control(RBAC)[1][2] に基づく Team-based Access Control(TMAC)[3][4][5] の考え方を基本とすることにより，従来手法の利点である権限を細分化し管理できる機能を継承する．さらに，状況 (Situation) という概念を導入することによって，利用者やオブジェクトの状況に応じたアクセス制御が可能となる．すなわち，提案するアクセス制御モデルは，既存のアクセス制御モデルの考え方を基に，利用者個人情報のアクセス制御を行うための拡張を行った新たなアクセス制御モデルである．

本稿では，提案モデルの実現を行うことによって提案モデルの動作の特徴と有効性を示す．実現は，提案モデルの動作に応じて三種類の形式で行った．まず，既存のアクセス制御モデルの考え方を基に利用者への権限割り当てを行う動作を示す画面．次に，提案モデルの特徴である利用者の状況に応じた個人情報の取得を行う動作画面．最後に，状況を追加・削除・変更するための動作を示す画面である．

2　想定する応用例

提案モデルの応用例の一つとして，医療現場における患者の個人情報管理システムを想定する．このシステムは，医療現場において電子カルテなどが保持する患者の個人情報を担当の医療関係者にのみ開示することによって患者の個人情報を保護するシステムである．システムが患者の個人情報を適切に開示することによって，医療関係者同士での情報共有の円滑化を図る．また，システムが個人情報保護の考え方に基づいて患者の個人情報を管理するため，人為的なミスによる情報漏えいの可能性を低減する．ここで，病院関係者と患者の氏名や住所，治療に関する情報といった個人情報はシステムによって集積され一元管理されるものとする．

ある人が救急患者として病院に受け入れられた場合を想定する．この時，個人情報の持ち主である患者を情報開示者とし，病院関係者を利用者とする．この患者は救命センターでの治療を受けた後，内科，外科を経て一般病棟へ移動する．その間，この患者に関する情報は随時電子カルテへ追加，更新が行われる．患者のプライバシー保護を考えた場合，開示される利用者の個人情報は医療活動の円滑化に必要となる内容のみということが望ましい．救命医師には救命医療のための重要な情報を開示し，内科医師や外科医師にはそれぞれが担当する役割に応じた患者の個人情報を開示することが考えられる．また，患者の担当医師が変更した際や，患者の退院時においては，患者との関連性のない利用者は患者の個人情報を取得できないことが望ましい．

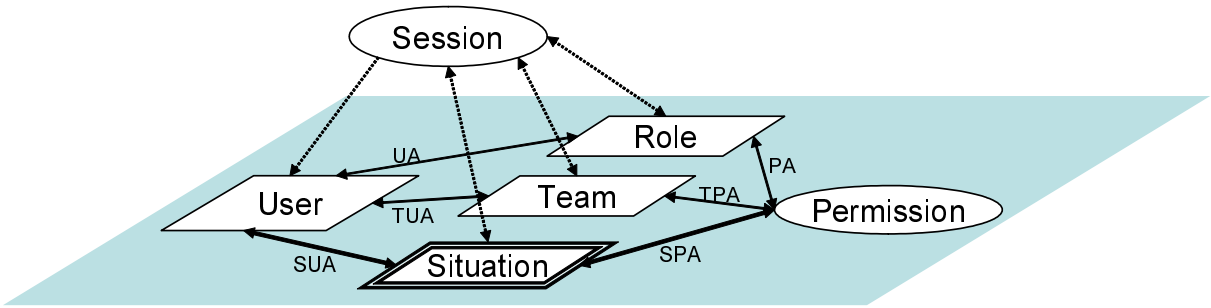

図 1: 提案モデル概念図

3 既存アクセス制御モデルとその問題点

様々なアクセス制御モデル [6][7][8][9] の中で，代表的な既存アクセス制御モデルの一つとして，Role-based Access Control(RBAC)[1][2] がある．RBAC は，アクセス権限の集合を抽象化した役割の概念に基づき，利用者のアクセス権限を変化させる．そのため，RBAC は利用者のアクセス権限を変更する場合は対応する役割のアクセス権限を変更するだけで済み，セキュリティ管理が容易となる特徴を持つ．

また，既存アクセス制御モデルの一つとして Team-based Access Control(TMAC)[3][4][5] がある．TMAC は RBAC の考え方を基盤とし，利用者集合であるチームの概念に基づきアクセス権限を変化させる．TMAC は，目的を達成するために組織化されたチームが存在する環境に適したアクセス制御モデルである．TMAC は役割とチームという二つの概念に基づくことから，利用者ごとにきめ細かいアクセス制御が可能となる．

ここで，2 章で挙げた医療現場のような応用例を考えた場合，複数の利用者が特定の活動を行うことから役割やチームに基づいたアクセス制御の考え方を用いることが有効である．応用例のシステムを実現化する際，TMAC の考え方に基づくことにより利用者の個人情報を公開する対象をきめ細かく設定することができる．しかし，応用例では利用者やオブジェクトの状況変化によるアクセス制御を行う必要がある．そのため，TMAC を直接適用するだけでは利用者やオブジェクトの状況変化に対応することができない．そこで，利用者やオブジェクトの状況変化を考慮し，従来手法の考え方を基に拡張を行った個人情報アクセス制御のためのモデルの構築を行う．

4 提案モデル

4.1 基本的な考え方

我々が提案するアクセス制御モデル [11] は，TMAC の考え方に基づき役割とチームの概念を用いたアクセス制御を行う．これにより，利用者個人情報の公開対象をきめ細かく設定することが可能となる．加えて，アクセス制御条件を示すための状況 (Situation) という概念を用いる．ここで，状況とは利用者とオブジェクトのコンテキスト情報に基づいてアクセス制御を行うための条件を抽象化したものである．

提案モデルの概念を図 1 に示す．ここで，利用者を User，状況を Situation，役割を Role，チームを Team，アクセス権限を Permission，セッションを Session とする．まず，利用者には，それぞれ役割とチームと状況が割り当てられる．そして，利用者が状況に示された条件を満たした場合に限り，割当てられた役割に基づくアクセス権限と，チームに基づくアクセス権限の和集合が利用者のアクセス権限として算出される．つまり，利用者が最終的にアクセス権限を得るためには，利用者やオブジェクトが状況に示された条件を満たす必要がある．これにより，利用者やオブジェクトの状況に応じて個人情報に対するアクセス制御を行う機能を実現することが可能となる．

4.2 提案モデルの構成要素

提案モデルは，利用者・役割・チーム・状況・アクセス権限・セッションから構成される．まず，提案モデルの各構成要素について説明を行う．

- 利用者 (User)：対象の個人情報にアクセスを行う実体．利用者にはセッションにより役割とチームと状況が割当てられる．
- 役割 (Role)：利用者集合の中における利用者の役割に基づいてアクセス権限の集合を抽象化したもの．利用者集合を簡約化するために用いられる．
- チーム (Team)：利用者集合の中における利用者の所属に基づいてアクセス権限の集合を抽象化したもの．特定の目的を達成するための利用者集合を，特定の役割に簡約化するために用いられる．
- 状況 (Situation)：利用者がアクセス権限を得るための条件集合を抽象化したもの．状況は，利用者のコンテキスト情報に基づく条件と，オブジェクトのコンテキスト情報に基づく条件で記述される．
- アクセス権限 (Permission)：役割とチームに割当てられた権限と，状況に示された条件から導かれる個人情報へのアクセス権限．アクセス権限には，利用者の氏名や位置情報, 連絡先など様々なものが含まれる．
- セッション (Session)：ある権限のもとで遂行される一連の作業集合．セッションにより利用者には役割とチームと状況が割当てられる．

次に，これらの構成要素を用いたアクセス制御操作について説明を行う．提案モデルでは，セッションに基づき利用者に対して役割とチームと状況が割り当てられる．また，利用者とチームにはそれぞれ個人情報に対するアクセス権限が割り当てられる．そして，利用者の持つ権限は利用者に割り当てられた役割とチームが持つ権限の和集合から算出される．この時，利用者が状況に記述された条件を満たす場合のみ，利用者は個人情報へのアクセス権を得る．

4.3 提案モデルの定義

- P はアクセス権限 (Permission) の集合.
- U は利用者 (User) の集合.
- R は役割 (Role) の集合.
- T はチーム (Team) の集合.
- Se はセッション (Session) の集合.
- UC は利用者のコンテキスト情報 (user context) の集合.
- OC はオブジェクトのコンテキスト情報 (object context) の集合.
- Si は状況 (Situation) の集合．si = (uc,oc) ∈ Si，uc ∈ UC，oc ∈ OC
- UA ⊆ U × R，利用者と役割の割当て関係.
- TUA ⊆ U × T，利用者とチームの割当て関係.
- SUA ⊆ U × Si，利用者と状況の割当て関係.
- PA ⊆ R × P，役割とアクセス権限の割当て関係.
- TPA ⊆ T × P,
  チームとアクセス権限の割当て関係.
- SPA ⊆ Si × P,
  状況とアクセス権限の割当て関係.
- Session-Role: $Se \rightarrow 2^R$,
  セッション Se から役割群 2^R への関数.
- Session-Users: $Se \rightarrow 2^U$,
  セッション Se から利用者群 2^U への関数.
- Session-Team: $Se \rightarrow 2^T$,
  セッション Se からチーム群 2^T への関数.
- Session-Situation: $Se \rightarrow 2^{Si}$,
  セッション Se から状況群 2^{Si} への関数.
- User-context: $U \rightarrow 2^{UC}$,
  利用者 U からコンテキスト情報群 2^{UC} への関数.
- Object-context: $P \rightarrow 2^{OC}$,
  アクセス権限 P からコンテキスト情報群 2^{OC} への関数.

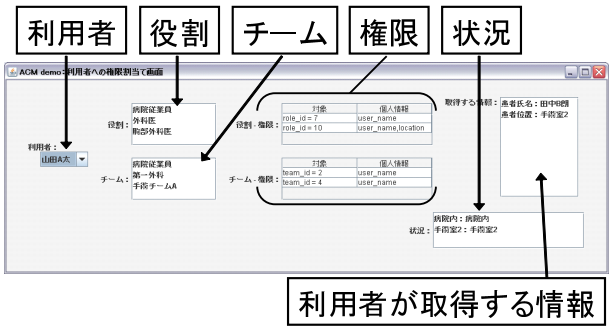

図 2: 利用者への権限割り当て動作

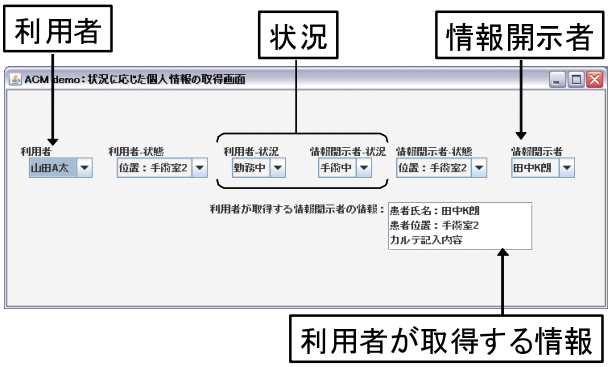

図 3: 状況に応じた個人情報の取得動作

5　提案モデルの実現

2 章で挙げた応用例に対し，Java 言語を用いて動作の種類に応じて提案モデルの実現を行った．利用者への権限割り当て動作を 5.1 節，利用者の状況に応じた個人情報の取得動作を 5.2 説，状況の追加・削除・変更を行う動作を 5.3 節で説明する．

5.1　利用者への権限割り当て動作

利用者への権限割当て動作画面を図 2 に示す．この画面は，既存のアクセス制御モデルの考え方を基に利用者が対象となる個人情報を取得するまでの提案モデルの動作を示すものである．画面左側から順に，利用者一覧，利用者に割り当てられる役割とチーム，役割とチームに割当てられている権限，利用者が個人情報を得る条件となる状況，最終的に利用者が取得する個人情報が表示される．まず，利用者を一覧から一人選択することによって，選択した利用者に割り当てられた役割とチームが定まる．次に，役割とチームそれぞれに割り当てられた権限から利用者が取得可能な個人情報が算出される．この時，利用者に割り当てられた状況が個人情報を得るための条件となる．

例えば，利用者一覧から A を選択した場合，役割の欄には A の役割である病院従業員，外科医といった情報が表示される．また，チームの欄にも同様に A が所属する第一外科，手術チーム A という情報が表示される．そして，それらの役割とチームに割り当てられたアクセス権から得られる患者の個人情報として，患者の氏名や血液型といった治療に必要な情報が表示される．

5.2　状況に応じた個人情報の取得動作

利用者の状況に応じて個人情報を取得する動作画面を図 3 に示す．この画面は，利用者の状況に応じた個人情報取得内容の変化を示すものである．画面左側から順に，利用者一覧，利用者のコンテキスト，状況，情報開示者の現在の状態，情報開示者一覧，最終的に利用者が取得する個人情報が表示される．ここで，利用者や情報開示者のコンテキストとは，現在時刻や対象者の位置情報，活動内容といった対象者の現在の状態に関する情報である．画面上の各要素は選択式となっており，利用者のコンテキストが選択されている状況の内容を満たし，かつ情報開示者のコンテキストが選択されている状況の内容を満たす場合に利用者は個人情報の取得が可能となる．

例えば，利用者として医師の A，情報開示者として患者の K を選択した場合，A が K の個人情報を得るためには中央に表示される状況に記述される条件を満たす必要がある．利用者に対する条件が勤務中，情報開示者に対する条件が手術中の場合，A のコンテキストが勤務中の条件を満たし，B のコンテキストが手術中の条件を満たせば A が取得可能な K の個人情報が表示される．

5.3　状況の追加・削除・変更動作

状況として記述される個人情報取得のための条件について追加・削除・変更を行うための動作

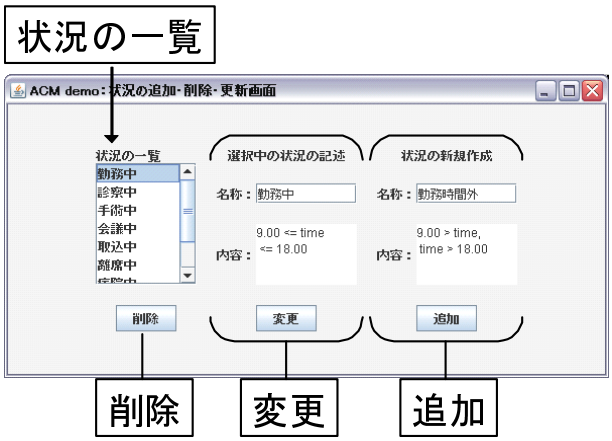

図 4: 状況の追加・削除・変更動作

画面を図 4 に示す．この画面は，利用者がアクセス権限を得るための条件集合を抽象化する状況を記述する動作を示すものである．画面左側から順に，現在登録されている状況の一覧，一覧内で選択されている状況に関する条件の記述，新しい状況を追加するための入力フォームが表示される．削除のボタンでは状況の一覧で選択している状況を削除することが可能である．また，中央に表示される状況の一覧で選択している状況に関する条件の記述は，直接書き換えることによって変更が可能である．そして，画面右側の入力フォームに状況の名称と条件内容を記述することによって新しい状況を追加することが可能である．

6　おわりに

本稿では，我々の提案する利用者やオブジェクトの状況に応じた利用者個人情報のアクセス制御を可能とするアクセス制御モデルの実現を行った．提案モデルは，従来の Role 中心のアクセス制御方式に基づく TMAC の考え方を基本とすることにより，従来手法の利点である権限を細分化し管理できる機能を継承する．さらに，アクセス制御の条件集合を抽象化するための状況という概念の導入により，利用者とオブジェクトの状況に応じたアクセス制御が可能となる．そして，提案モデルの実現により，提案モデルの具体的な利用場面や特徴，有効性を示した．今後は，利用者へ状況を割り当てる動作を示す機能の追加構築を予定している．また，課題点としてコンテキスト情報からアクセス制御の条件を抽象化するための記述方式の具体化が挙げられる．

参考文献

[1] D.F. Feiner, J. Cugini, D.R. Kuhn, ”Role-based access control (RBAC): Features and motivations”, Proc. of the Eleventh Annual Computer Security Applications conf., (1995)

[2] R. Sandhu, E. Coyne, H. Feinstein, C. Youman, ”Role-based access control models”, IEEE Computer, vol.29, pp.38-47 (1996)

[3] Roshan K. Thomas: ”Team-based Access Control (TMAC): A Primitive for Applying Role-based Access Controls in Collaborative Environments”, Proc. of ACM Workshop on Role Based Access Control, pp.13-19 (1997)

[4] Christos K. Georgiadis, Ioannis Mavridis, George Pangalos, Roshan K. Thomas : ”Flexible team-based access control using contexts”, Proc. of ACM Workshop on Role Based Access Control, pp.21-27 (2001)

[5] Alotaiby F.T, Chen J.X: ”A model for team-based access control (TMAC 2004)”, IEEE Computer Society, Volume.1, pp.450-454 (2004)

[6] J.Barkley, ”Comparing simple role based access control models and access control lists”, Proc. of Second ACM Workshop on Role-Based Access Control, pp.127-132(1997)

[7] Bin Zhao, ”Collaborative Access Control” In Seminar on Network Security 2001, (2001)

[8] S. Lu, Y. Hong, Q. Liu, L. Wang, R. Dssouli, ”Access Control in e-Health Portal Systems” Proc. of 4th int. conf. on Innovations in Information Technology, pp.88-92 (2007)

[9] Myong H. Kang, Joon S. Park, Judith N. Froscher, ”Access control mechanisms for inter-organizational workflow” Proc. of ACM Workshop on Role Based Access Control, pp.66-74 (2001)

[10] W. Tolone, G.J Ahn, T. Pai, S.P. Hong: ”Access Control in Collaborative Systems”, ACM Computing Surveys, Volume.37, pp.29-41 (2005)

[11] 笠井敬介, 鈴木優, 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”, 2009 年 暗号と情報セキュリティシンポジウム (SCIS2009), 論文集 3F4-2, pp.1-6, (2009)