社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－MBL－36（11）
2006－UBI－10（11）
2006／2／16

家庭内のプライバシー保護を目的としたアクセスコントロール方式

森 航哉† 川幡 太一† 依田 育生†

†NTT サイバーソリューション研究所 〒239-0847 神奈川県横須賀市光の丘 1-1

E-mail: †{mori.kouya, kawabata.taichi, yoda.ikuo}@lab.ntt.co.jp

あらまし ホームネットワークが発達し、家庭内の様々な機器と家族のスケジュールなどの個人情報を活用した、ホームオートメーションなどのサービスを提供できるような環境が訪れた際には、これらのサービスに家族内でのプライバシー保護を遵守させる必要がある．本研究では、（１）家庭に適した Role-Based Access Control の適用方法を明確にし、低コストでアクセス制御ポリシを設定する、（２）設定されたポリシを基に、使用するデバイスの特性や、デバイスの周囲にいる人などのコンテキスト情報を利用して、状況に応じたポリシを動的に算出する、の２段階のアクセス制御方法を提案する．これにより、上記のような家庭環境で、コンテキストを考慮したアクセス制御ポリシを、ユーザに大きな設定負担をかけずに自動決定することができた．

キーワード ホームネットワーク，プライバシー，アクセスコントロール，コンテキスト

An Access Control Method for The Privacy Protection of Home Networks

Koya MORI† Taichi KAWABATA† and Ikuo YODA†

†NTT Cyber Solutions Laboratories, Nippon Telegraph and Telephone Corporation 1-1 Hikarinooka, Yokosuka-Shi, Kanagawa, 239-0847 Japan

E-mail: †{mori.kouya, kawabata.taichi, yoda.ikuo}@lab.ntt.co.jp

Abstract The home-automation services for home networks should take care of the privacy in a family. In this study, we propose two-tiered access control method to protect the privacy. First, we clarify the suitable form of Role-Based Access Control for home networks and introduce the policy administration method to configure the policies simply. Second, we propose a calculation process to decide the contextual policies dynamically based on the policies configured by the first method and the context-information including the type of devices, the type of service action and other users in the same room. This approach makes policy configuration simple with the consideration for the complexity of the environment conditions.

Keyword Home Networks，Privacy，Access Control，Context

1. はじめに

近年、ホームネットワーク上の情報家電と個人情報を組み合わせた、ホームオートメーションなどのサービスのニーズが高まっている．このようなサービスを効果的に提供するためには、個人のスケジュールやアドレス帳などの情報を、ホームネットワークを介して、TV・電話などの多数の機器に流通させる必要がある．このために我々は、個人情報を利用したサービスをホームゲートウェイ（HGW）などに実装し、各家庭に提供することを提案している[1].

これらのサービスは、図１に示すように HGW を中心として動作し、情報は以下のフローで伝達される．各情報は、情報源にアクセスするデバイスドライバを経由してサービスに取得される．そして、取得した情報はサービスに加工され、出力先の機器のデバイスドライバを利用して、ユーザに対して提示される．

従来の家庭では、スケジュール情報や健康情報などの**プライバシー**に関わる情報は、人間関係におけるマナーによる心理的な方法や、鍵のかかる引き出しのような物理的な方法で他者から保護されてきた．ホームネットワーク上におけるサービスについても、この家族内のプライバシーを人間関係に応じて遵守させることが重要である[2].

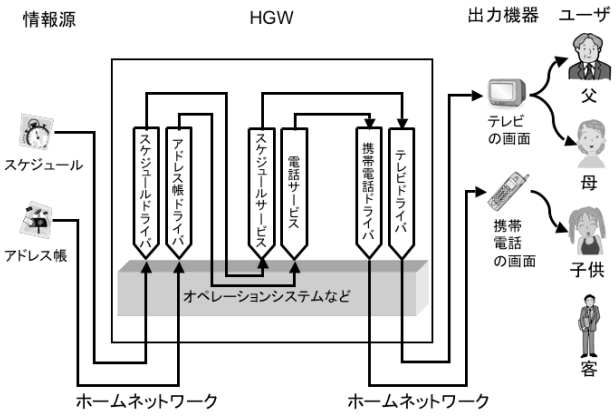

図１ 情報のフローの概要

表１　分析データの一部

情報源	小項目	リソースアクション	サービス	サービスアクション	出力機器	静的ポリシ				動的ポリシ			
						父	母	兄	その他	父	母	兄	その他
スケジュール	場所	Read	スケジュール	表示	TV 画面	禁止	禁止	禁止	禁止	禁止	禁止	禁止	禁止
スケジュール	場所	Read	スケジュール	表示	PC 画面	禁止	禁止	禁止	禁止	許可	許可	許可	禁止
スケジュール	場所	Read	スケジュール	表示	携帯画面	禁止	禁止	禁止	禁止	許可	許可	許可	許可
スケジュール	場所	Read	情報提供	通知	TV 画面	禁止	禁止	禁止	禁止	禁止	禁止	禁止	禁止
スケジュール	場所	Read	情報提供	通知	PC 画面	禁止	禁止	禁止	禁止	禁止	禁止	禁止	禁止
スケジュール	場所	Read	情報提供	通知	携帯画面	禁止	禁止	禁止	禁止	許可	許可	許可	許可

例えば､スケジュール情報をユーザの要求に応じて、テレビや携帯電話の画面に表示するサービスを提供する場合を考えてみる．ある家庭の子供のスケジュール情報には、見られても構わない学校関係の予定と、プライバシーに関わる友人関係の予定が記録されている．周囲に父や母がいるリビングルームで、スケジュールをテレビの画面へ表示する場合には、学校関係の情報は表示し、友人関係の情報は表示しないようサービスを制御する必要がある．一方、携帯電話の画面へ表示する場合には、携帯電話の画面は使用者にしか見えないため、両方を表示するよう制御する必要がある．

このためには､各家庭の慣習に即した**アクセス制御ポリシ**を、情報が伝達されるフローに応じて設定しなければならない.しかし､大きく２つの問題点がある．

第１に、各ユーザは自身が所有する情報にアクセスする各フローに対してポリシを設定する必要があるが、一般的に**ポリシ設定コスト**の増大は利便性を大きく損なう．

第２に、現実の家庭では、プライバシーに関わる情報は、ディスプレイからの表示、あるいはスピーカからの再生など､何らかの機器を通して出力されるため、機器の周囲にいる使用者以外の人にも情報が伝わってしまう．これを防ぐには、記録されている情報へのアクセスを制御するのみならず、実世界に出力された**情報が伝達される範囲**も考慮した制御が必要である．

本研究では、現実の家庭で起こる上記のような問題を踏まえ、そもそも家庭内のシステムにおけるアクセス制御がどうあるべきかを検討する．そして、ユーザの設定コストを抑えるために、従来のアクセス制御技術を家庭環境で効率良く用いる形態を提案する．さらに、出力された情報のプライバシーも考慮した制御を行なうために、使用するデバイスの種類や、デバイスの周囲にいる人などのコンテキスト情報を利用して、動的にポリシを決定する仕組みを提案する．

本研究の前提条件として、対象とする情報源は、家庭内で典型的だと考えられる、スケジュール情報・アドレス情報などとし、複数の情報から生成される新情報や、ある情報のリンクから取得される情報は対象外とする．サービスは、スケジュールサービスや電話サービスなど情報をユーザに伝えるものとし、故意の情報漏洩などはしないものとする．出力機器は、テレビの画面・テレビのスピーカ・携帯電話の画面・PC のディスプレイなど、機能毎に定義する．ユーザは、父・母・子供などの家族と、客などその他の人を対象とする．

2. 従来技術と問題点

アクセス制御技術はこれまでも広く研究されており、ポリシの設定コストを抑える方式も提案されている．これらの方式には、主に制御対象をグループ化してポリシを設定すべき対象を減らす方法と、ポリシを自動設定することでコストを下げる方法がある．

前者としては、Role-Based Access Control（RBAC）[3]などがあるが、どのようにリソースを Role に集約するかを決めるグループ設定や、各制御内容に対するポリシの設定が必要なため、これらの簡単な設定方法が重要となる．グループ設定を、制御対象の属性情報を基に自動的に行う RB-RBAC[4]もあるが、質の異なる属性情報を持つ多様なリソースが存在する家庭では、グループ化のルールを定義するのが難しく、効率良くグループ化できない．また後者としては、「マスターポリシー」を適切に拡張してポリシを自動生成する PolicyComputing[5]などがあるが､多様かつ変動の大きいリソースを含む家庭ではポリシのプロトタイプを定義するのは難しい．このように、従来の技術にはグループ化など設定を煩雑にする要因があり、家庭では低いコストでポリシを設定できない．

また、ポリシを自動設定する方式の中には、利用する機器や、周囲のユーザなどのコンテキストを考慮してアクセス制御する技術も存在する．このようにデバイスから出力される情報について保護したい場合には、使用するデバイスや周囲にいるユーザ等のコンテキスト情報をポリシの制約条件として記述する Generalized RBAC[6]や、コンテキスト情報を利用してポリシを生成するルールを事前に設定しておく方法[7]などがある．しかし、家庭内における情報の種類、出力デバイスの種類、周囲の人の状態の組合せは非常に数が多いため、複雑な設定を一般家庭のユーザが行なうことは難しい．また、これらの手法はコンテキストに応じた細かな制御が出来る反面、設定コストが高くなる．このため、従来の技術は家庭でコンテキストアウェアな制御の設定をするには適さない．

3. 分析方法

１章で述べた前提条件となるプライバシー情報の利用形態は、情報源が数種類で各数十ー数百の小項目が存在し、サービスが 2ー30 種類、出力機器が 3ー20 種類､ユーザが 3ー5 名と考えられるため､情報が伝達されるフローのパターンを概算すると数千ー数万パターンになる．従って、サービスにプライバシーを守らせるには、各フローに対応する多くのポリシを設定する必要がある．

そこで、家庭に適したポリシ設定方法を、事例分析から検討した．図1より、情報のフローを情報源・サービス・出力機器・ユーザの4つの段階に分け、実際の家庭で起こる情報のフローのパターンを抽出した．

情報源については、スケジュール情報・アドレス情報・写真や映像などのコンテンツ情報・年齢や身体情報などの個人情報・衣類や化粧品などの所有物情報・好みのテレビ番組や音楽などのプリファレンス情報の6種類とした．そして、それぞれの情報源を、スケジュールの各予定の時間・場所のような小項目に分け、さらに各小項目のデータに対する動作である「read」「write」などのリソースアクションまで分類した．

サービスは、将来提供されると考えられるスケジュールサービスなど20種類とした．そして、各サービスの機能に応じて、「表示する」「着信を通知する」などの動作（サービスアクション）を定義した．

また、出力機器については異なる大きさの画面や音量を持つ画面やスピーカなど20種類を選び､ユーザは家族4人と来訪者の5種類とした．

上記の組合せで、家庭内で起こる情報のフローのパターン1683個を列挙し､分析に利用した．そして表1に一部を示すように、各フローについて、情報が他の家族や家族以外にアクセスされた時に、そのユーザに対して、そのフローを所有者が「許可する」か「禁止する」か、検討した．このアクセス制御のポリシを、今後**静的ポリシ**と呼ぶ．また上記に加えて、情報を出力する時に、出力機器の近くにいる他の人に対して、その情報が伝わるのを所有者が「許可する」か「禁止する」か、検討した．このアクセス制御のポリシを、今後**動的ポリシ**と呼ぶ．本研究では、この静的ポリシと動的ポリシを合わせてアクセス制御ポリシとする．表1に示す静的ポリシと動的ポリシからは、常に許可となる所有者自身のポリシは省いている．

上記の検討を通して分析データを作成し、規則性を見出すことで、アクセス制御ポリシを低コストで設定する方法を検討した．

4. 家庭用アクセス制御方法の提案

4.1. 事例分析結果

事例分析の結果、静的ポリシが許可の場合は、動的ポリシも許可になり、静的ポリシが禁止の場合は、動的ポリシは出力機器や人の種類などに連動して、禁止と許可に分かれることが示された．従って、静的ポリシを設定すれば、動的ポリシは、上記の関係性より自動的に導くことが出来ると考えられる.このことから、まず低コストで静的ポリシを設定する方法を検討し、それに基づいて動的ポリシを自動設定する方法を検討することにした．

4.2. RBAC の適用方法の提案

まず、低コストで静的ポリシを設定する方法を検討するにあたって、表1の分析データの静的ポリシに関わる部分のみを用いて分析を行なった．

この結果、情報がユーザに届く途中で経由する、サービスの種類や出力機器の種類は、ユーザのプライバシーにとって、ほとんど関係ないことが示され、ポリシを決定する上で省けると判断した．つまり、ユーザ

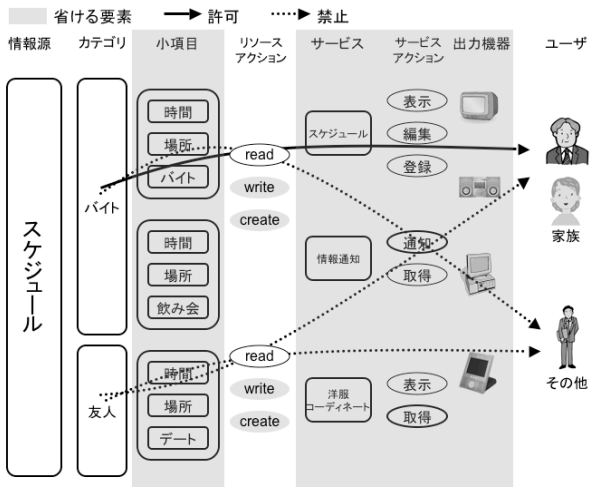

図2　ポリシ決定に必要な要素

図3　ポリシ設定インタフェース例

にとっては、HGW の中でどのように情報が処理されているかは問題ではなく、情報が誰にアクセスされるかという部分が重要であることを意味している．以上より、本研究の対象とする家庭においても、アクセスされる情報と、アクセスするユーザの関係を、許可／禁止するという、**従来技術と同じ枠組みでアクセス制御が可能**であると判断した．

このことから、家庭においても従来技術であるRBAC を当てはめることで、ポリシの設定コストを削減できると考えられる．そこで、家庭内環境に適したRole の構成方法を検討するため、ポリシの決定に必要な要素と、省ける要素を分類した．

この結果、ユーザについては**「所有者」「家族」「その他」**の3種類に分類し、家族とその他についてRole を構成すれば、分析データの大半が設定できることが分かった．所有者は、どのようなフローを経由しても、ほぼ常に静的ポリシが許可のため、デフォルトで許可にして良い．また、父と母を別のポリシにしたいなどの例外は存在するが、発生するのは全体の 8%程度であり、必要があれば個別に設定すれば十分であると考えられる．

また、リソースには通常「read」「write」「create」などの複数のリソースアクションが存在するが、分析データの大半については、**「read」以外のリソースアクションを含むフローをデフォルトで禁止**にしても問題ないと判断した．write や create を許可したい例外的フローも存在するが、発生するのは全体の 5%

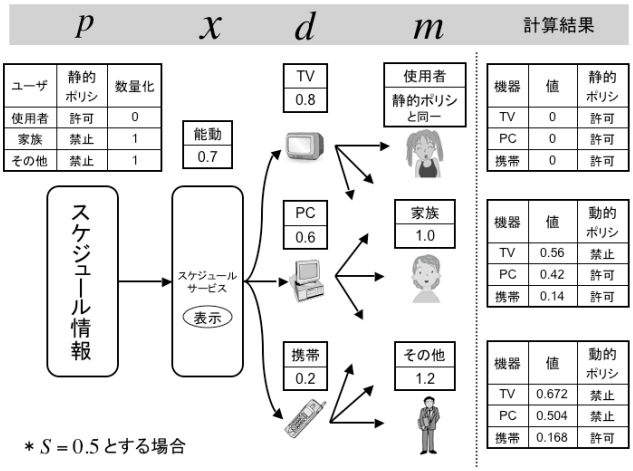

図４　動的ポリシの算出例

程度であり、必要ならば個別に設定すれば良いと考えられる．

次に、スケジュールやアドレスなどの情報は、複数の小項目より構成されるが、これらの小項目は、例えばスケジュールであれば、「学校関係」や「友達関係」などのように、いくつかのカテゴリに分類できる．上述した分析データを分類した結果、所有者の意図する制御は、各カテゴリと強い相関があり、カテゴリ内の小項目については同一で構わないことが示された．つまり、ポリシの設定の簡略化には、**情報のカテゴリ毎に Role を構成する**ことが効果的だと考えられる．

この結果、静的ポリシを設定するのに必要な要素が大幅に削られ、最終的には図２に示すように、**「各情報のカテゴリについて、read を、家族／その他に、許可／禁止する」ポリシ**を決定すれば、十分にユーザのプライバシーを保護できると考えられる．この場合、静的ポリシの組合せは４パターンになるが、「家族は禁止、その他は許可」というポリシはまず発生しないため、実際には３パターンのみとなる．このため、ユーザは図３に示すようなラジオボタンなどを利用したシンプルなインタフェースを用いて、３択でポリシを設定可能となる．

このように RBAC を適用することで、検討に用いた分析データについて、所有者の意図するアクセス制御の 86%を 33 クリックで設定できた．

4.3. コンテキストに応じたポリシ決定方法の提案

次に、コンテキストに応じた動的ポリシを自動決定する方法を検討するために、表１の分析データの動的ポリシに関わる部分も含めて分析を行なった．

この結果、所有者の要求する動的ポリシに最も強く影響するのは、**出力に利用する機器の種類**であることが分かった．例えば、出力する機器がテレビの画面の場合には禁止するが、同じ環境でも携帯電話の画面ならば許可する、というケースなどが考えられる．これは、機器の外部に情報を伝達する能力の強さに関係していると考えられ、本研究ではこれを**情報伝達力**と呼ぶことにする．

また、情報へのアクセスが、ユーザの**能動的**な要求によって始まったのか、サービスが自発的に動作してユーザが**受動的**に情報を受取るのかも、所有者の要求するポリシに影響を与えることが分かった．例えば、同じアドレス情報へのアクセスでも、ユーザが閲覧するために能動的に要求したのか、あるいは電話の着信時にサービスが発信者を通知するために自発的に表示したのかによって、必要となる動的ポリシが異なるケースが考えられる．本研究では、前者を能動、後者を受動として、**サービスの動作**を分類する．

さらに、多くの場合で**家族より家族以外に厳しい**アクセス制御ポリシを要求することが分かった．このため、同一の環境条件でも、出力機器の周囲に家族以外の人がいる場合には、動的ポリシをより厳しく設定する必要があると考えられる．

これらの分析結果より、本研究では以下に示す動的ポリシの自動決定方法を提案する．この手法では、ユーザが 4.2 節の方法であらかじめ設定した静的ポリシに、動的ポリシに関係する３つのコンテキスト情報である**サービスの動作・出力機器の情報伝達力・周囲の人の種類を乗算する**ことで、コンテキストの影響を反映した動的ポリシを決定する．

提案する動的ポリシ自動決定方法では、まずユーザはあらかじめ以下の設定をしておく．

(1) 4.2 節の手法に従って設定される、所有する各情報源に対する**静的ポリシ**
(2) サービスが使用する各出力機器の，情報を伝達する力の強さ（情報伝達力 0～1）
(3) 周囲にいる**家族とそれ以外の人の重み**(m)
(4) 出力を禁止する**閾値**(S)

次に、サービスが動作を起こし、機器に情報を出力させようとした時に、コンテキストを収集し以下を自動判定する．

(1) ユーザの要求に基づく動作か（**能動**:0.7）、サービスが起こした動作か（**受動**:0.9）(x)
(2) 出力に使用する機器の**情報伝達力**(d)
(3) 周囲にいる人毎の静的ポリシを、許可なら 0、禁止なら 1 にする．(p)

アクセスコントローラは、周囲にいる人毎に以下の式を計算し、真ならば動的ポリシを禁止とする．

$$p \cdot x \cdot d \cdot m \geq S$$

図４に、データは使用者のみに許可され、サービスは表示機能を持ち、出力機器が３種類、周囲の人が２人おり、閾値が 0.5 の場合の例を示す．図４の場合、アクセスコントローラは、各人の静的ポリシにサービスの動作、出力機器の情報伝達力、ユーザごとの重みを乗算し、結果の値を閾値と比較することで、動的ポリシを算出する．使用者本人については、静的ポリシでスケジュール情報へのアクセスが許可されているため、どの機器を利用した場合も許可となる．そして、家族は TV のみ禁止、その他は携帯のみ許可となる．

次にアクセスコントローラは、決定された動的ポリシから、出力する情報と、利用する機器を選択する．原則としては、使用者の静的ポリシが許可で、さらに周囲の人全員の動的ポリシが許可となる情報が最も多い機器を選択する．図４の場合を例に取ると、情報は１つであり、それに対して使用者はどの機器でも許可、家族は PC と携帯の場合が許可、その他は携帯のみが許可のため、全てのユーザに共通して許可となる携帯が出力機器として選択され、ユーザに情報を出力する．

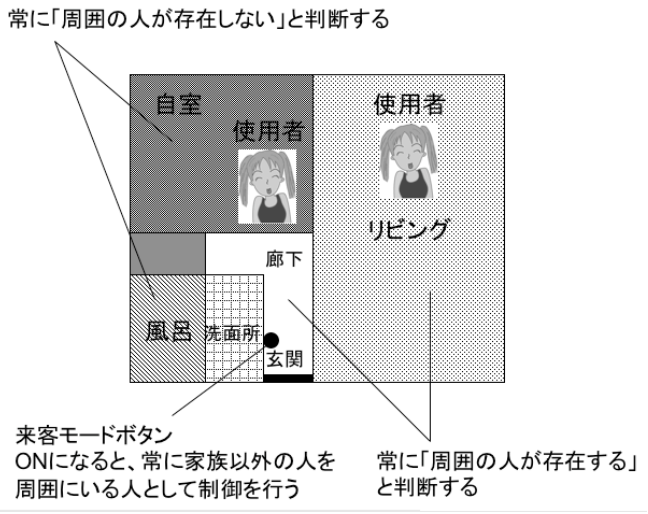

図５　周囲の人の決定方法

4.4. パラメータの決定方法

本研究で提案する動的ポリシ自動決定方法を適用するには、静的ポリシ以外に、あらかじめ設定しておくべきカテゴリや、いくつかのパラメータが存在する．

まず、情報源のカテゴリ分けについては、スケジュール情報やアドレス情報などは「学校」や「友人」などコミュニティ単位で分類し、データの入力時に指定する方法が考えられる．また、音楽や動画などのコンテンツや衣類や化粧品などは、商品の属性情報としてジャンルが決まっているため、これをカテゴリとして利用することができる．

次に、サービスの動作は能動と受動に分類されるが、通常この値は受動の方が能動よりも値が大きいと考えられ、本研究で用いた分析データを基にすると、能動が 0.7、受動が 0.9、が経験的に適切な値であった．今後適切な値を決定する方法を開発する必要がある．

また、情報伝達力は、機器の持つ画面のサイズや、スピーカの音量などによって設定する．図４の例では便宜的に、携帯電話の画面を 2 インチ、PC の画面を 16 インチ、TV の画面を 32 インチとし、それらの対数を基に値を決定した．機器の設置場所によっては、実質的に上記のようにして事前に設定した値とは異なる情報伝達力になる場合も考えられ、この際にはユーザが調整する必要がある．

そして、家族やその他に付いている重みについては、本研究で用いた分析データを基にすると、家族が 1、その他は 1.2ー1.8 が経験的に適切な値であった．今後適切な値を決定する方法を開発する必要がある．

最後に、動的ポリシの許可／禁止を判定する閾値については、ポリシを 0ー1 の値に数量化するため、本研究では中間の 0.5 をデフォルト値として動的ポリシを決定した．ただし、動的ポリシをより厳しい基準で判定したい場合や、その逆の場合などには、制御結果に最も敏感に反応するパラメータであるため、最も効果的に調整ができる．従って、各ユーザの個性に適した値を決定する方法を開発する必要がある．

このように、本研究で提案する動的ポリシ自動決定方法には、複数のパラメータがあるが、その多くはデフォルト値をあらかじめ決定することができ、ユーザの設定作業は必須ではない．これにより、静的ポリシの設定コストから大きく負担を増やさずに、動的ポリシを決定することが可能である．

5. 提案手法の性能評価

4.2 節で提案した静的ポリシ設定方法に、4.3 節で提案した動的ポリシの決定方法を合わせて使用することにより、検討に用いた 1683 パターンのポリシを **33 クリックで設定**することが可能となり、所有者が望むアクセス制御ポリシの **81%を実現**できた．すなわち、動的ポリシの決定方法は、コンテキスト情報を基に自動的に計算するため、ユーザの設定コストを増大させることなく、適用することが可能である．

これにより、ユーザのポリシ設定負荷を大幅に軽減した上で、利用する機器や周囲のユーザなどのコンテキストを考慮したアクセス制御が可能となり、１章で述べた第１及び第２の問題を同時に解決できた．

6. 考察

6.1. 提案手法による誤制御について

提案手法により、ユーザのポリシ設定コストを上げることなく、81%のアクセス制御ポリシを実現できるようになった．しかし、逆に言えば 19%は設定できず、ユーザの意図しないアクセス制御ポリシになってしまうことを意味する．

しかし、この 19%の内訳を見てみると、誤って許可する割合が 10%、誤って禁止する割合が 90%であり、**大半は安全サイド**になることが示されている．従って、家庭という環境においては、98%のプライバシーは保護できることになり、実用上大きな問題はないと考えられる．

また、この 19%の分を解決するには、ユーザが静的ポリシの詳細設定を行なう必要があるが、これらの多くは家族内で異なる静的ポリシを設定するのと、情報の追加・変更を家族に許可するというものであり、クリック数に換算して 3ー4 クリックすれば、95%以上の設定ができる．従って、設定コストを 10%程度上乗せすれば、実用上十分な性能を出すことが可能であり、提案手法に詳細な静的ポリシ設定を行なうユーザインタフェースを組み合わせることで、ユーザの利便性を大きく損なうことなく、解決可能だと考えられる．

6.2. ユーザの位置情報の取得について

本手法では、出力機器の周囲にいる人に応じた制御を行なうため、家庭内にいる人間の位置情報は必須である．しかしながら、人間の位置を常時取得し続けることは、RFID タグで検知する、あるいはカメラで撮影して識別するなど多くの方法が提案されているものの、実用レベルでは未だ困難なのが現状である．そこで、本研究では、提案手法で必要なレベルの精度の位置情報に限ることにより、人物の位置情報取得に関わる問題を回避する方法を考案した．

図５に示すように、家庭には部屋という単位が存在する．リビングや玄関などは、使用者以外の家族も高い確率で在室している可能性があり、来客時には家族以外の人も入ってくる可能性が高い．一方、自室や風呂などは、使用者が一人で在室している確率が高く、

来客も入室しない可能性が高い．そのため、出力機器の設置されている部屋を基に、周囲の人を推定する方法を考案した．すなわち、出力機器がリビングや玄関にある場合は、常に周囲の人として「家族」がいるものとして動的ポリシを決定し、逆に自室や風呂にある場合は、周囲の人は存在しないとして動的ポリシを決定する．さらに、玄関などに来客モードボタンを設置し、このボタンが ON の時で、出力機器がリビングや玄関にある場合は、常に周囲の人として「家族」および「その他」がいるものとして動的ポリシを決定する．

このようにすることで、人間の位置を RFID やセンサーなどで常時検知するという技術課題を避けつつ、適切かつ十分なアクセス制御ができる．

7. 提案手法の使用例

提案手法の使用例を２つ示す．閾値を 0.5 とする．

まず、静的ポリシの異なる複数の情報を、同時に出力する場合の例を示す．表２の例は、スケジュールサービスが、家族・その他とも禁止である友人関係の情報と、その他のみが禁止である学校関係の情報を、同時に使用者に対して出力したい場合である．この場合、使用者が受動的にサービスを提供され、利用可能な出力機器が TV と携帯の画面であるため、動的ポリシは表２のようになる．この結果、全てのユーザに共通して許可される機器を選択すると、友人関係は携帯のみ出力が許可され、学校関係も携帯のみ出力が許可される．従って、友人関係と学校関係を同時に出力することが許可される機器として、携帯が選択され、画面にこれらのスケジュール情報が出力される．

また、使用者が特定の機器での出力を要求しているために、禁止されている情報が含まれているにも関わらず、それを利用して出力しなければならない時も存在する．表３の例は、使用者がアドレス帳サービスに対して、家族・その他とも禁止である友人関係の情報と、誰でも許可である親類関係の情報を、同時に TV に出力するよう要求している場合である．この場合、親類関係の動的ポリシは許可、友人関係の動的ポリシは禁止になるが、TV を利用して可能な限り多くの情報を出力するようにする．従って、表３の例では、TV に親類関係の情報のみを出力する．

8. 今後の課題

今後は、サービスの動作やユーザの重みなどのパラメータの値を決定する方法が必要である．特に閾値はユーザの望む適切な値を決定する方法が必要である．

また、提案手法のユーザビリティについて、評価実験を行ない、多くのユーザに効果的かを確認する．

9. まとめ

家庭内のアクセス制御には、1)ポリシ設定が煩雑、2)周りの人などのコンテキストに応じた制御が必要、という大きく２つの問題があった．本手法により、ユーザが主に設定する必要があるのは各情報のカテゴリ単位のポリシのみとなり、実験的に作成した、プライバシーに関わる家庭内のアクセス 1683 パターンを、33 クリックで設定することが可能であった．また、出力機器の情報を伝える能力や、周囲の人の位置などのコンテキストを反映して動的にポリシを決定することで、ユーザの望む制御の 81%を正しく実現することができ、誤った制御となる 19%の内 90%は安全側となることを確認した．以上の結果から、提案手法により、低コストでアクセス制御ポリシを設定可能になり、周囲にいる人・サービスの動作・出力機器など、コンテキストに応じた動的なポリシを自動決定可能となった．

表２　提案手法の使用例１

	周囲の人	静的ポリシ	動作	情報伝達力	重み	値	動的ポリシ
友人関係	使用者	0	受動 0.9	TV 0.8	−	0	許可
	家族	1			1	0.72	禁止
	その他	1			1.2	0.864	禁止
	使用者	0	受動 0.9	携帯 0.2	−	0	許可
	家族	1			1	0.18	許可
	その他	1			1.2	0.216	許可
学校関係	使用者	0	受動 0.9	TV 0.8	−	0	許可
	家族	0			1	0	許可
	その他	1			1.2	0.864	禁止
	使用者	0	受動 0.9	携帯 0.2	−	0	許可
	家族	0			1	0	許可
	その他	1			1.2	0.216	許可

表３　提案手法の使用例２

	周囲の人	静的ポリシ	動作	情報伝達力	重み	値	動的ポリシ
友人関係	使用者	0	能動 0.7	TV 0.8	−	0	許可
	家族	1			1	0.56	禁止
	その他	1			1.2	0.672	禁止
親類関係	使用者	0	能動 0.7	TV 0.8	−	0	許可
	家族	0			1	0	許可
	その他	0			1.2	0	許可

文　献

[1] 小林英嗣, 小河原成哲, 依田育生,“ホームネットワークにおける複数サービスの統括的制御システム,”2003 電子情報通信学会信学技報, no.115, pp.25-30, Mar.2003

[2] 森航哉, 川幡太一, 依田育生,“ホームネットワークにおけるアクセスコントロール方式,”2005 信学ソサエイティ大, Sept.2005

[3] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman, Role-Based Access Control Models, IEEE Computer, 29(2), pp.38-47, 1996

[4] M.A. Al-Kahtani and R.S. Sandhu, A Model for Attribute Based User-Role Assignment, IEEE the 18th Annual Computer Secutiry Applications Conference, 2002

[5] 菅原政孝, 田中俊介, 坂田祐司, 小熊慶一郎, 白鳥則郎, “情報ネットワークシステムのポリシ制御"PolicyComputing"の適用と実装,” 情報処理学会論文誌, 42(2), pp.126-137, 2001

[6] M.J. Moyer and M. Ahamad, Generalized Role-Based Access Control, *IEEE Distributed Computing Systems*, pp.391-398, 2001

[7] A.Kumar, N.Karnik and G.Chafle, Context Sensitivity in Role-based Access Control, *ACM SIGOPS Operating System Review*, 36(3), pp.53-66, 2002