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

2006－CVIM－153 (38)
2006／3／17

映像サーベイランスにおけるプライバシー保護のための視覚的抽象化の提案

小清水 隆[†,††] 鳥山 朋二[†] 西尾 修一[†] 馬場口 登[†,††] 萩田 紀博[†]

† ATR 知能ロボティクス研究所 〒619-0288 京都府相楽郡精華町光台 2-2-2
†† 大阪大学工学部 〒565-0871 大阪府吹田市山田丘 2-1
E-mail: †{koshimiz,toriyama,nishio,hagita}@atr.jp, ††babaguchi@comm.eng.osaka-u.ac.jp

あらまし 映像サーベイランスは治安の悪化を防止するためのIT技術として，大変注目されている分野である．しかし，映像サーベイランスは映像のモニタにかかるコストの問題やプライバシーの問題を含んでおり，防犯カメラの増加や，防犯カメラ設置範囲の拡大が進むことで，そのような問題が映像サーベイランスを実施する際の課題となる．本稿ではそのような問題を解決するため，地域コミュニティにおけるプライバシーを考慮した映像サーベイランスシステムを提案する．我々の提案するシステムは地域コミュニティでの映像サーベイランスを前提とし，個人のプライバシーを保護するための視覚的抽象化とプライバシーポリシーに従うアクセス制御の機能を持つ．このような機能を持った映像サーベイランスシステムの評価実験を行いその有効性について検証した．

キーワード 映像サーベイランス，プライバシー，XACML，視覚的抽象化，プライバシーポリシー

Visual Abstraction for Privacy Preserving Video Surveillance

Takashi KOSHIMIZU[†,††], Tomoji TORIYAMA[†], Shuichi NISHIO[†], Noboru BABAGUCHI[†,††], and Norihiro HAGITA[†]

† Intelligent Robotics and Communication Laboratories, ATR Hikari-dai 2-2-2, Seika-cho, Souraku-gun, Kyoto, 619-0288 Japan
†† Faculty of Engineering, Osaka University Yamadaoka 2-1, Suita-shi, Osaka, 565-0871 Japan
E-mail: †{koshimiz,toriyama,nishio,hagita}@atr.jp, ††babaguchi@comm.eng.osaka-u.ac.jp

Abstract With demanding need for security, video surveillance technologies have recently received a lot of attention. As video surveillance cameras are available in more places, the concerns about cost of monitoring and invasion of privacy are growing. In this report, we describe the design of a privacy preserving video surveillance system in a community. Our comunity surveillance system involves a module that preserves privacy by image proccesing which we call 'Visual Abstraction' and access control according to the privacy policy. Through result of evaluation sessions recuruiting 53 subjects, we show availability of the community surveillance system.

Key words video surveillance, privacy, XACML, visual abstraction, privacy policy

1. はじめに

近年，凶悪な犯罪がメディアによって多数報じられ，多くの人々が治安の悪化を感じるようになってきている[1]．これを受けて安全を守り，安心して生活できる場をつくるためのIT技術に対する要求は益々高まってきている．犯罪の未然防止・犯人捜査の手がかりとなる等の効果が期待される映像サーベイランスはその一つであり，様々な場において注目されている技術である．

しかしその一方で，映像サーベイランスはいくつかの問題を含んでいる．第一に，映像サーベイランスシステムは防犯カメラの映像を常時モニタする形式が一般的であり，多地点の映像を一箇所に集約してモニタを行う形式をとるため，同時にモニタ可能な範囲に制限される．従って，今後防犯カメラの設置数・設置範囲が拡大したとき，集約される映像をモニタしきれなくなる可能性がある．

第二に防犯カメラに映される人のプライバシーの問題[2]がある．映像サーベイランスにおいて守られる立場に立つとき，守ってもらうために見せてもよいプライバシーに係る情報量(プライバシー開示許容量と呼ぶ)を決める要素は多数ある．例

えば，昼間に複数の友人と歩いているときにはプライバシーを犠牲にしてまで見守って欲しいとは思わないが，暗い夜道を一人歩きするときにはプライバシーを犠牲にしてでも誰かに見守って欲しいと思うかもしれない．また，見知らぬ人と二人で歩いているときには見られてもよいが，恋人と二人で歩いているのは見られたくないということもあるだろう．これらの例のように，プライバシー開示許容量は様々な要素の影響を受けて変化する．また，映像サーベイランスにおいてプライバシーとセキュリティはトレードオフの関係にあり，その配分は個人によって大きく異なるため，プライバシー開示許容量は個人によりその基準が大きく異なる．すなわち，プライバシー開示許容量は様々な要素によって変化するため，映像サーベイランスにおける個人のプライバシーは一意に定義することができない．このために映像サーベイランスにおける一定のプライバシー保護は容易ではない．

以上に述べたように映像サーベイランスを実施する際の問題として，現行システムにおけるモニタリングの限界と，防犯カメラに映される人のプライバシーの問題の二つが挙げられる．我々はこれらの問題を解決するため，以下の方法を提案する．

まず，第一の問題を解決するひとつの方法として，地域コミュニティ単位での映像サーベイランスを提案する．元来，日本には長屋や村などのコミュニティ内で相互に見守りを行う文化があり，構成員の助け合いによって安全が確保される社会の自然な姿があった [3]．精神的にも，他人より，知人に見守ってもらうほうが安心できると考えるのは当然であり，現在でも地域コミュニティでの防犯活動 [4] が地域の治安の維持に貢献している例が多くあることから，このような仕組みは社会に受け入れられやすいと考えられる．これによって映像サーベイランスにおいて同時にモニタ可能な範囲が制限される問題を，相互見守りの仕組みに変化させることにより解決を試みる．

次に，第二の問題を解決する方法として，個人や様々な要素によって変化する個人のプライバシー開示許容量に応じて，個人が情報開示量を自らの意志に基づいて決定できる方法，及び情報開示量の制御手段を提案する．具体的には前者は，ポリシーに基づいたアクセス制御技術によって，後者は視覚情報量制御用画像処理である視覚的抽象化 (Visual Abstraction と呼ぶ) を用いた視覚情報量制御技術によって実現する．さらに，個人のプライバシーを個人のごとのポリシー (プライバシーポリシーと呼ぶ) に書き下すことで，プライバシー開示許容量を変化させる要素に応じた，情報開示量を設定できるようにする．このプライバシーポリシーに基づいたアクセス制御により，情報開示量を変化させる．

本稿では，プライバシーポリシーに応じて視覚的抽象化を変化させることで，プライバシーを考慮し得る映像サーベイランスシステムを提案する．

以下，2 章では関連研究について述べ，3 章では提案システムの全体像と提案手法を述べ，4 章では実験と考察を述べ，5 章では結論と今後の課題をまとめる．

2. 関連研究

映像サーベイランスは 9.11 事件以降，国家の安全を守るための手段として特に多くの関心を集めてきた [5]．特に防犯カメラと顔認識システムの併用によってテロリストを識別する新しい技術が取り上げられ，プライバシー対セキュリティという構図が出来上がってきた [5] [6]．このような状況で平均顔による匿名化や顔をぼかしたりモザイクを加える [7] [8] ことでの顔認識を防ぎプライバシーを保護する手法などが提案されている．これらは主に顔画像を扱っており，プライバシーの問題として映像をモニタする際や保存する際の顔による個人同定を取り上げている．本研究では地域コミュニティでの映像サーベイランスにおいて，防犯カメラの映像が見られる際に生じるプライバシーの問題を個人それぞれのプライバシー含めて考慮する．

北原らは固定カメラから得られる被写体の三次元位置から，モバイルカメラの映像中の特定の人物のプライバシー保護領域を隠蔽する手法 [9] を提案している．また，Wickramasuriya らは RFID タグを用いた入室管理により，入室権のある人の映像は全身に画像処理を加え，入室違反をした人の映像はそのまま保存することで，入室管理におけるプライバシーを考慮した映像サーベイランスを提案している [10]．これらの文献では隠蔽する人物又は人物中の領域の特定に主眼が置かれているが，本研究ではそのような隠蔽する必要がある領域が特定できたとき，その領域の持つ視覚情報量を個人のプライバシーに応じてコントロールすることに主眼を置く．

Senior らはカメラによって得られた映像が含む情報を，人数・背景・行動・時間・状況などに分解しそれらを組み合せて映像を再構成することで映像の持つ視覚情報量を減少させ，プライバシーを保護するシステムを提案している [11]．また，映像のもつ視覚情報量を段階的に変化させることで，人が見る場合の認識率が変わることは Boyle らの研究によって示されている．Boyle らはぼかしと Pixelize を画像全体にかけ，その度合いを段階的に変化させることで，人が見る場合にどの程度認識率が変化するのかを実験している [12]．我々はこれらの文献の知見を人物領域について視覚情報量を段階的に変化させる視覚的抽象化手法の一部として利用した映像サーベイランスシステムを提案する．

3. プライバシーを考慮した映像サーベイランスシステム

第一の問題を解決するために地域コミュニティによる見守りを前提とすると，映像が開示される範囲が拡大することは必須であり，より強固なプライバシー保護が必要となる．

3.1 システムの全体像

我々が提案するプライバシーを考慮した映像サーベイランスシステムの全体像を図 1 に示す．本システムでは，地域コミュニティ内の人間はこのシステムに登録することで図 1 のようにネットワークを介して防犯カメラで得られた映像を見ることができる．

さらに状況や個人によって様々に変化する個人のプライバ

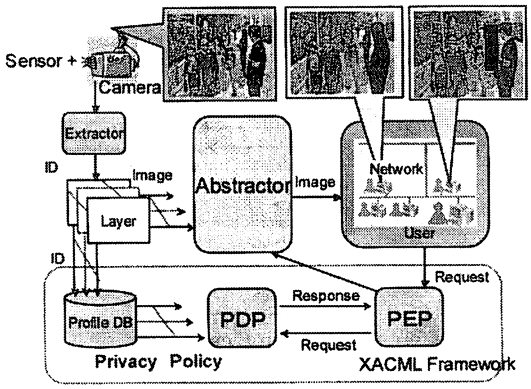

図 1　提案システムの全体像

シーを取り扱うため，我々は個人のプライバシー開示許容量に応じて映像が持つ視覚情報量をポリシーに基づいて変化させる仕組みを提案する．そのための手段が「視覚的抽象化を用いた視覚情報量制御」と「ポリシーに基づいたアクセス制御」である．図 1 中における，Extractor と Abstractor が視覚的抽象化を用いた視覚情報量制御を担い，Profile DB と PDP(Policy Decision Point)・PEP(Policy Enforcement Point) がポリシーに基づいたアクセス制御を担う．我々はこのような Profile DB，PDP・PEP を包括した枠組みを XACML(eXtensible Access Control Markup Language) を用いて実現する．この枠組みを XACML Framework と呼ぶ．

ここで防犯カメラに映った映像が，ユーザーに提示されるまでの流れを示す．まず，カメラから得られた映像は Extractor に入力される．Extractor は人物領域を抽出し，人物ごとにレイヤ化する．また，カメラ又はセンサによって得られた映像中の個人の ID はレイヤと対応付ける．次に ID とレイヤの対応付けを Profile DB に入力し，ID に対応するプライバシーポリシーを PDP に渡しておく．ネットワークを介してユーザーからの防犯カメラの映像に対するアクセスに応じて，そのアクセス Request を PEP に入力する．PEP はこの Request を PDP に送る．PDP はこの Request と Policy から映像に対するアクセスが承認されるかどうかを判断し，Response を PEP に返す．この場合 Response には視覚的抽象化方法の指定も含まれる．Abstractor はこの Response を受けて，ID と対応付けられたレイヤにそれぞれ視覚的抽象化を加え，一つの画像にまとめる．まとめられた映像はネットワークを介してユーザーが持つ映像提示端末に表示される．以下ではシステムの構成要素について詳しく述べる．

3.2　視覚情報制御部

視覚的抽象化を用いた視覚情報制御を実行するモジュールである Extractor と Abstractor について述べる．

3.2.1　Extractor

Extractor では映像中の個人の ID 取得と映像のレイヤ化を

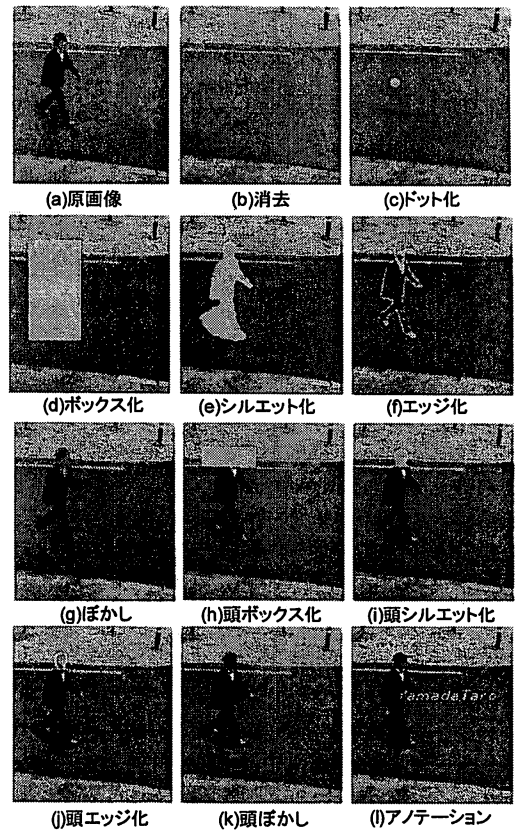

図 2　視覚的抽象化処理例

行い，取得された ID を映像のレイヤに対応付けて扱う．

まず，カメラから得られた映像をレイヤ化するため，背景差分を用いて背景と前景を抽出する．背景差分によって得られた前景はその塊ごとにラベル付けしレイヤ化する．このようにすることで複数の人物領域を一枚ごとのレイヤに分けて扱うことが可能になる．

一人の人間ごとに一枚のレイヤに分けられた後，レイヤ内において頭の検出を行うことで，一人の人間の領域を頭部と体部に分割する．人物領域を頭部・体部に分割しそれぞれに対して視覚的抽象化を行うことで，視覚情報量を段階的に変化させ得るという知見は事前実験によって得られている．さらに Extractor ではセンサからの情報から映像中の個人の ID を取得し，レイヤに対応付ける．

3.2.2　Abstractor

Abstractor では Extractor によって抽出されたレイヤごとに視覚的抽象化を行う．図 2 の (a) は処理を加える前の原画像であり，同図 (b) (l) に視覚的抽象化処理として 12 種類を例示した．

これらの処理を施した映像から得られる情報量及び推定可能

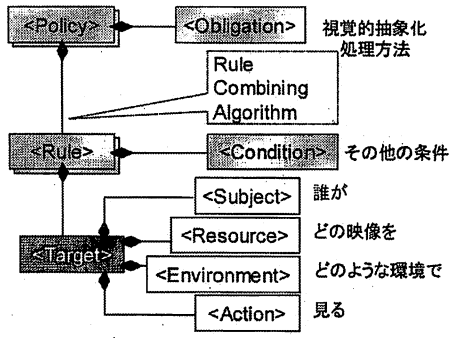

図 3 ポリシー言語構造

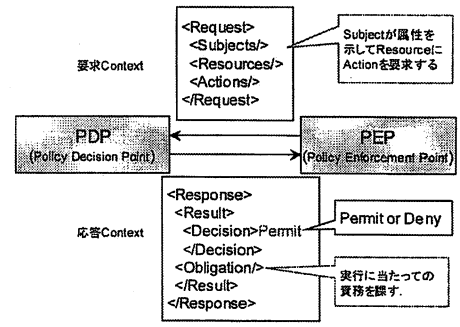

図 4 PDP と PEP

と考えられる動作は以下の通りである.

- 消去 (Vanish):情報なし
- ドット化 (Dot):存在情報のみ
- ボックス化 (Box): 大きさの情報のみ
- シルエット化 (Silhouette):仕草・動作が推定可能
- エッジ化 (Edge):髪型・服装などが推定可能
- ぼかし (Blur):色情報が加わる
- 頭ボックス化 (HeadBox):頭のみ情報なし
- 頭シルエット化 (HeadSilhouette):頭の大きさの情報が増える
- 頭エッジ化 (HeadEdge):髪型が推定可能
- 頭ぼかし (HeadBlur):頭の色情報が加わる
- アノテーション (Annotation):個人の名前を加える

これらの処理により段階的に視覚情報量が開示される. また, 視覚的抽象化には (l) のように個人の ID を加え, 情報量を増やす処理も含む. (l) の処理は他の処理とも組み合わせ可能である.

3.3 XACML Framework

XACML Framework ではポリシーに基づいたアクセス制御を行う.

3.3.1 Profile DB

1 章で述べたように個人のプライバシー開示許容量は様々な要素によって異なる. Profile DB には上記の要素に応じた個人のプライバシーポリシーを記述することにより, 視覚情報量を制御する.

Profile DB には個人のプライバシーポリシーと ID 情報が登録されている. ID 情報は容易に登録可能であるが, プライバシーポリシーについては, プライバシー開示許容量を変化させる要素が多くあり容易には記述することができない. このようなプライバシーポリシーを記述するため, 柔軟で拡張性のあるアクセス制御を実現するためのポリシー記述言語である XACML(eXtensible Access Control Markup Language) [13] を用いる.

XACML におけるポリシーの言語構造と提案するプライバシーポリシーとの対応を図 3 に示す. プライバシーポリシーにおいて Subject, Resource, Environment, Action は誰が, どの映像を, どのような環境で, 見るかを指定し, それらを Target として表現する. 想定されるその他の様々な条件は Condition として記述し, Target と合わせてひとつの Rule を形成する. さらに複数の Rule, Obligation をまとめてひとつの Policy を形成する. Obligation にはアクセス制御を実行する際に課される視覚的抽象化方法を記述する. これらの Rule が複数存在するとき, それらを Rule Combining Algorithm によって結合する.

3.3.2 PDP と PEP

XACML Farmework の核となるのは, 要求の許可・不許可を決める PDP とアクセス制御を実行する PEP である. これらは図 4 のように Request と Response のやり取りを行いアクセス制御を実行する.

提案システム中での XACML Framework のデータフローは以下のようになる.

(1) PDP はあらかじめ映像中に入った人の Policy を Profile DB から取得しておく.

(2) ユーザーが映像へのアクセスを PEP に Request として要求する.

(3) PEP は Request を PDP に送る.

(4) PDP は Policy と Request から Permit or Deny の判断を行い Response を PEP に返す.

(5) PDP は加えて PEP の実行する Obligation として視覚的抽象化方法を与える.

(6) PEP は Obligation を Abstractor に送る.

4. 実験と考察

提案システムを評価するための準備として, 提案した視覚的抽象化の各アルゴリズムを実装した. さらに, 我々は映像を見せる相手との親密度や視覚情報量がプライバシー開示許容量を変化させる大きな要素になるという知見を事前実験より得ている. そこで生成した映像を用いて提案システムにおけるプライバシーポリシーとして映像を見せる対象と視覚的抽象化処理方法の対応を記述した. 提案システムの効果を検証した.

4.1 映像生成

視覚的抽象化を担う Extractor と Abstractor を実装し, 映

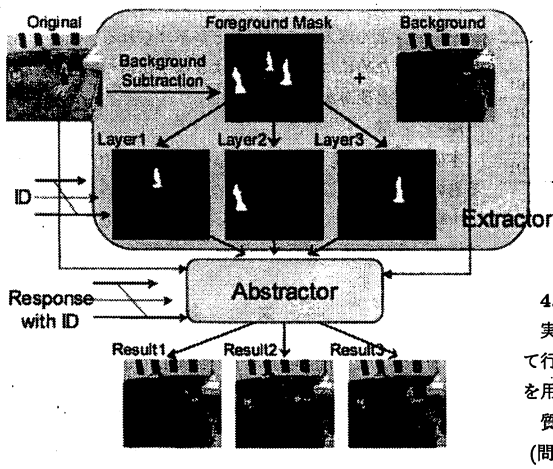

図 5 レイヤ化

像を生成した．この実装は OpenCV による画像処理を用いて行った．Extractor によるレイヤ化について図 5 に示す．まずカメラから得られた映像を KaewTraKulPong らの提案した背景差分 [14] を用いて前景マスク画像と背景画像を得た．さらに，前景マスクのオブジェクト領域のラベル付けを行い，オブジェクトごとに抽出しレイヤ化を行った．このときある一定の大きさを超えたオブジェクトのみを人物領域とみなし，レイヤ化を行った．

次に Abstractor においてレイヤごとに視覚的抽象化処理を加えた．処理の手法としては図 2 に挙げた画像処理手法を実装した．主な画像処理の手法としては，

- ボックス化
- シルエット化
- エッジ化
- ぼかし

が挙げられる．ボックス化はレイヤ中の前景領域を囲む四角形を求めている．シルエット化はレイヤ化の前景領域を塗りつぶすことで処理を実現している．エッジ化は Laplacian filter を用いて，ぼかしは Gaussian filter を用いて実装している．図 2 中のぼかし処理はカーネルサイズ 25 × 25，$\sigma = 4.25$ で処理を行っている．レイヤを一つの映像にまとめる際，背景差分によって抽出された背景の上にレイヤを挿入することで，図 2 中の消去，ドット化処理を実現している．これらの処理は何れも OpenCV に実装されている処理を用いて行った．

4.2 実験方法と実験環境

4.2.1 実験方法

実験は 20 代〜50 代の男性 26 名・女性 27 名の計 53 名を対象として行った．実験の内容と説明を以下に示す．

- 提案システムの概要説明 (15 分)
- 視覚的抽象化を施した映像を見ながらの質問 (15 分)
- テキストによるシステムの印象評価の質問 (10 分)

表 1 (問 2), (問 3) の質問群

Q1.	見守られていると感じますか？
Q2.	覗き見されていると感じますか？
Q3.	安全だと感じますか？
Q4.	悪用されるかもしれないと感じますか？
Q5.	安心だと感じますか？
Q6.	危険だと感じますか？
Q7.	守ってくれると感じますか？
Q8.	監視されていると感じますか？

4.2.2 実験環境

実験は 20 名ほどが入る部屋で行い，十数名ずつ三回に分けて行った．実験器具としてはスクリーン，ノート PC，質問紙を用いた．

質問紙の内容は以下のような内容である．

(問 1) 日常生活で関係のある方の中から A.「とても親しい人」B.「やや親しい人」C.「あまり親しくない人」D.「全く親しくない人」の順に想像し，視覚的抽象化処理 20 種類に対してそれぞれに開示してもよいかを聞く質問

(問 2) 提案システムのように選択可能な映像を地域の住民が見る場合の印象を聞く質問

(問 3) 何も処理を加えない映像を地域の住民が見る場合の印象を聞く質問

(問 2), (問 3) における提案システムの印象を聞く質問群を表 1 に示す．

4.3 実験結果と考察

(問 2), (問 3) の質問群の回答に対する差の検定の結果を表 2 に，Z 値を質問ごとにグラフ化したものを図 6 に示す．検定方法は 2 個の対応サンプル間のノンパラメトリック検定である Wilcoxon の符号付き順位検定を用いた．Z 値は Wilcoxon の検定における検定統計量であり，p 値は「(問 2) と (問 3) の二群に差がない」という帰無仮説が採択される確率を表す．表 2 に示したようにすべての項目において p 値 <0.05 となっており，有意水準 5 %以下で有意差ありと判定されている．その正負も考慮に入れると，いずれの質問についても提案システムを支持する結果となっている．この結果から，地域コミュニティにおける映像サーベイランスを実施する際には，提案するプライバシーを保護機能によって，安心感，安全感，見守られ感が増し，覗き見されているという印象・悪用されるかもしれないという印象・危険だという印象・監視されているという印象が何れも減少するといえる．これらの結果は提案システムがプライバシーを保護しつつ悪用の危険も防止することを示していると考えられる．

(問 1) の質問において，A，B，C，D それぞれに対して開示許可を選択した回答の度数を算出した結果を図 7 に示す．この度数は (問 1) の質問で聞いた 20 種類の処理に対して算出している．図 7 から親しい人ほど映像の開示を許可したする傾向が見られる．

この結果により映像を見せる対象との親密度がプライバシー開示許容量を変化させる大きな要因になることを確認した．ま

表 2 (問 2), (問 3) の差の検定における Z 値と有意水準

(問 2) - (問 3)	Z 値	(問 2) - (問 3)	Z 値
Q1	$3.096^{*1}, p < .01$	Q2	$4.858^{*2}, p < .001$
Q3	$2.002^{*1}, p < .05$	Q4	$3.142^{*2}, p < .01$
Q5	$2.254^{*1}, p < .05$	Q6	$4.031^{*2}, p < .001$
Q7	$2.058^{*1}, p < .05$	Q8	$4.356^{*2}, p < .001$

*1 正の順位に基づく　*2 負の順位に基づく

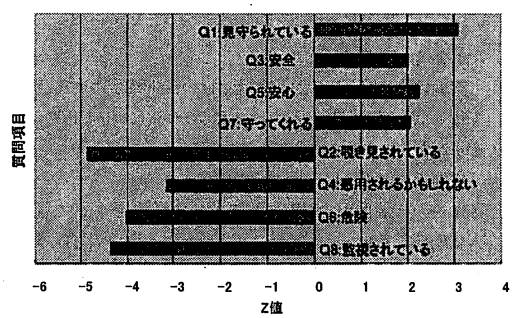

図 6 質問項目と Z 値

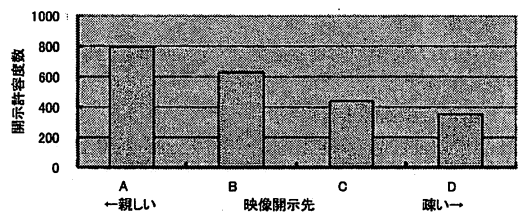

図 7 映像開示先と開示許容度数

たことによって，プライバシーポリシーに記述する内容として映像を見る人と視覚的抽象化処理方法の対応を記述することは，提案システムにおけるプライバシーの保護に効果があると推察される．

5. ま と め

本稿では地域コミュニティにおけるプライバシーを考慮した映像サーベイランスシステムを提案した．提案システムでは視覚的抽象化を用いた視覚情報制御とポリシーに基づいたアクセス制御によってプライバシー開示許容量を変化させる様々な要素に応じた制御が可能である．さらに主観評価実験によってこのようなシステムの有効性を検証した．

プライバシー開示許容量に影響を及ぼす要素として，親密度以外の要素についても考慮する必要がある．適切にプライバシーを保護するシステムをつくるためには，プライバシーポリシーに記述する内容をさらに検討し議論する必要がある．

また，視覚情報制御を行う際にも課題が多く残されている．主要なものとしては，映像中の個人の ID の取得，ID が得られた際のトラッキング，オクルージョンが起こった際のセグメンテーションと処理方法の選択などが挙げられる．提案システムを実現するためには，今後このような手法についても実装を検討していく必要がある．

謝　辞

本研究は独立行政法人情報通信研究機構 (NICT) の助成によるものである．

主観評価に関して貴重なコメントを賜りました ATR メディア情報科学研究所，馬田 一郎氏，鈴木 紀子氏，米澤 朋子氏に深謝いたします．

文　献

[1] 野村武司, 日下部美弥子. 安全で暮らしやすい社会に向けて. 知的資産創造, pp. 74–75. 野村総合研究所, Jun. 2005.

[2] 新保史生. ユビキタスメディアの利用とプライバシー保護の限界 - 個人情報保護の交錯点も踏まえて - . 信学技報 PRMU2005-148, pp. 75–82, Jan. 2006.

[3] 江口雅之. 監視カメラ社会 - もうプライバシーは存在しない - . 講談社＋α新書, Feb. 2004.

[4] 伊藤高史. 防犯ボランティアと監視社会論—メディアと自由を巡る論点からの考察—. メディア・コミュニケーション〔研究所紀要〕, pp. 99–111. 慶應義塾大学メディア・コミュニケーション研究所, Mar. 2005.

[5] K.W. Bowyer. Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, pp. 9–19, 2004.

[6] S. Cass and M.J. Riezenman. Improving security, preserving privacy. *IEEE Spectrum*, pp. 44–49, 2002.

[7] E.M. Newton, L. Sweeney, and B. Malin. Preserving privacy by de-identifying face images. *Trans. on Knowledge and Data Engineering*, pp. 232–243, 2005.

[8] R. Gross, E.M. Airoldi, B. Malin, and L.A. Sweeney. Integrating utility into face de-identification. In *Proc. of the Fifth Workshop on Privacy Enhancing Technologies*, 2005.

[9] I. Kitahara, K. Kogure, and N. Hagita. Stealth vision for protecting privacy. In *Proc. of ICPR'04*, 2004.

[10] J. Wickramasuriya, M. Alhazzazi, M. Datt, S. Mehrotra, and N. Venkatasubramanian. Privacy-protecting video surveillance. In *SPIE International Symposium on Electronic Imaging*, Jan. 2005.

[11] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Ying-Li Tian, A. Ekin, J. Connell, Chiao Fe Shu, and M. Lu. Enabling video privacy through computer vision. *IEEE Security & Privacy Magazine*, pp. 50–57, 2005.

[12] M. Boyle, C. Edwards, and S. Greenberg. The effects of filtered video on awareness and privacy. In *Proc. of CSCW'00*, pp. 1–10. ACM Press, 2000.

[13] OASIS. *eXtensible Access Control Markup Language (XACML) Version 2.0*, Feb. 2005.

[14] P. KaewTraKulPong and R. Bowden. An improved adaptive background mixture model for realtime tracking with shadow detection. In *Proc. of AVBS'01*, Sept. 2001.