カメラ映像における閲覧者と被写体の関係に基づくプライバシ保護システムの提案と評価

関口隆昭† 加藤博光†

本稿では，カメラ映像の閲覧者や被写体等の情報に基づいて映像に含まれるプライバシ情報をフィルタリングするシステムを提案する．近年，監視カメラから被写体のプライバシを保護するため，映像内の人物領域の隠蔽やカメラ制御技術が多数提案されている．これらの技術は被写体のプライバシ保護に有効である一方，本来記録すべき犯罪行為等をも隠蔽してしまう等，映像の閲覧者側への配慮がなされていない．そこで本稿では，プライバシ保護と映像閲覧の両立を図るため，閲覧者と被写体の関係に基づき被写体ごとに異なるレベルの保護を行うシステムを提案する．提案システムでは映像内の被写体同定処理が課題であり，本稿ではこれに影響を与える被写体情報の通信遅延をプロトタイプシステムの設計および実装によって評価し，特定の利用形態のもとでの提案システムの有効性を確認する．

Proposal and Evaluation of Video-based Privacy Assuring System Based on the Relationship between Observers and Subjects

Takaaki Sekiguchi† and Hiromitsu Kato†

In this paper, we propose a system implementing a method that filters sensitive information in videos on the basis of data identifying the observers and the subjects observed by the cameras. Recently many techniques have been proposed to hide sensitive information in videos. While these techniques are useful for protecting privacy, there is some possibility to hide crimes that should be monitored. We propose a system that protect privacy at a different level from one subject to another based on the relationship between observers and subjects for balancing privacy and awareness. In this paper, we describe the design and development of a prototype system to evaluate latency time of information from a subject which affects subject identification. Then we describe the feasibility in case of some applications.

1. はじめに

近年，コンピュータシステムの性能向上や個人情報を利用するサービスの増加により，プライバシの問題が提起されている．たとえばユーザに付随する RFID（Radio Frequency Identification）を読み取ることによって個人のプロファイルを検索したり，監視カメラによる被写体のプライバシ侵害等が問題となっている．

こうしたプライバシの問題に対して，OECD（Organization for Economic Cooperation and Development：経済協力開発機構）が 1980 年に採択したプライバシガイドライン[11] をはじめとして様々な取り組みがなされている．特にユビキタス環境を想定した研究として Langheinrich による研究があり，プライバシに関連する情報を収集する際の通知機能等を備えたシステムの提案がなされている[8]．そのほかにも，本人識別可能な情報を隠蔽して匿名性を確保したり，ユーザが利用しているサービスを特定困難にしたりするための研究がさかんである[6),13)]．

しかしこれらの研究は，情報を保護したい側にとって有効である一方，情報を要求する側にとっては必ずしも有効ではない．監視カメラのプライバシ問題の場合，被写体のプライバシを保護するための技術開発が多数なされている一方[1),10),17)~20)]，監視カメラの設置者や閲覧者等，監視行為による現場の安全確保を期待されている人物への配慮がなされているとはいえない状況である．

我々が所属するやおよろずプロジェクト[3] では，将来のユビキタス情報社会において想定される様々な課題に対して，文理融合アプローチによる取り組みを進めてきた．特に監視カメラのプライバシ問題は，法制

† 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi Ltd.

度・倫理面での問題と技術的な取り組み状況の乖離が大きい．そこで我々は，同プロジェクトの一環として法律の専門家の支援を受けつつ監視カメラのプライバシの問題について取り組み，プライバシ保護のためにシステムが実行すべき処理は被写体と閲覧者の関係に応じて変化すると考えて検討を進めてきた[7),15),16)]．この例として，街頭に設置された防犯カメラの撮影映像を近隣の住民へ公開し，どのような撮影がなされているか，自分の子供が安全に遊んでいるか等を確認できる監視システムをあげることができる．このような監視システムでは，治安維持に責任を持つ公的機関が閲覧する場合は詳細な映像を閲覧可能とすべきである一方，住民が単に撮影映像を見たい場合は全体をぼかした映像で十分であり，不必要な詳細映像を見せるべきではない．同様に，子供の安全確認が目的の場合はその閲覧者の子供のみを表示するほうが好ましいといえる．

本稿では，このような被写体と閲覧者の関係に基づいて適切なプライバシ保護を実行するシステムを提案し，システムの試作により提案手法の有効性を確認した結果を報告する．以降，まず 2 章で関連研究とその問題点について概観する．次に 3 章で本稿での提案システムについて述べ，4 章で提案システムの評価および考察を示す．最後に 5 章で本稿をまとめ，今後の課題を述べる．

2. 関 連 研 究

2.1 従 来 技 術

カメラ撮影時のプライバシ保護を目的とした技術では，Hudson らによる研究をはじめとして，プライバシと認識度（Awareness）の調整が主要な課題とされている[4)]．すなわち，プライバシ保護のために撮影映像内の情報を隠蔽する処理と，現場の情報をより良く認識するために詳細な撮影映像を配信する処理とはトレードオフの関係にあり，両者の間に何らかの調整が必要となる．

この課題を解決するためのアプローチは，**図 1** にあげる 2 つの手法に分類できる．まず 1 つめの手法は，人物領域や特定の矩形等，映像内の特定の領域のみを隠蔽し他の領域は表示するものである．特に，隠蔽すべき情報として代表的である人物領域に関しては，背景推定法をベースとする手法[17)]，頭部や顔領域検出をベースとする手法[20)]，サーマルビジョン等のセンサ情報を活用した手法[18)] 等の各種のアプローチが提案されている．

2 つめの手法はユーザの明示的な指示や現場の状況

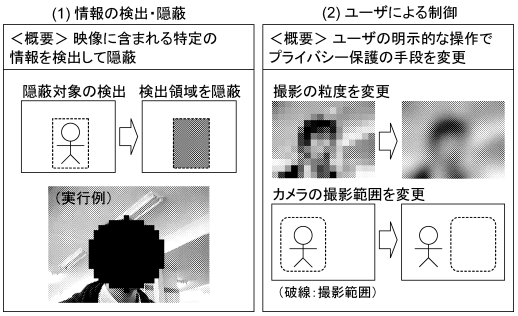

図 1 従来技術
Fig. 1 Related work.

に応じて実行すべきプライバシ保護を決定するものである．たとえば Zhao ら，Boyle ら，Neustaedter らは，モザイクやぼかし等，映像の粒度を変える各種の画像処理のうちプライバシ保護に最も有効な画像処理は何かについての評価実験を行い，画像処理のみでは有効なプライバシ保護は図れないとして，ジェスチャや音声による指示でカメラの視点を制御するシステムを提案している[1),10),19)]．

また，プライバシ保護を直接目的としたものではないが，撮影映像内における被写体の個人同定を目的とした研究が行われている．たとえば赤外線タグや RFID 等のセンサ情報と撮影映像内の人物領域とを照合して，各々の領域が誰であるかを特定する研究がある[12),14)]．

2.2 OECD8 原則

以上のような技術が提案されている一方，日本を含めた各国のプライバシ保護の考え方の基礎として，OECD よりプライバシ保護に関する 8 つの原則が提示されている[11)]．この 8 原則のうち，本稿で主に検討する 2 つの原則を以下にあげる．

収集制限の原則 個人データは，適法・公正な手段により，かつ情報主体に通知または同意を得て収集されるべきである．

利用制限の原則 個人データは，同意がある場合や，法令による場合を除いて，明確化された目的以外に使用されるべきではない．

これらの原則を 1 章で述べた街頭防犯カメラの例にあてはめて考えると，監視カメラへのシステム要件として次のものがあると我々は考えている．

まず収集制限の原則によると，映像内の複数の人物に対して一概に隠蔽処理を施すのではなく，撮影への同意がある人物は表示し，同意がない人物は隠蔽できることが望ましい．ここで同意の有無は，多くの場合，誰がその映像を見ているかによって異なると考えられる．たとえば家族が見る場合は同意するし，無関係の

第三者が見るのであれば同意しないということが想定できる．

次に利用制限の原則によると，利用目的に必要な情報のみを閲覧者に見せる必要がある．この点，監視カメラは「何かあったときに備えてすべてを撮影する」という曖昧な目的を持っており，具体的な撮影目的を提示することが難しい．そこで，情報システムとしては閲覧者や閲覧場所等の客観的条件によって閲覧可能な情報を制限する仕組みが有用だと考えられる．特に街頭カメラの場合，自治体や警察等の公的な機関が，安全確認を目的として特定の閲覧端末から見る場合は完全な映像を，近隣の居住者が単に混雑度を確認するために見る場合はぼかした映像を表示することが望ましい．

以上をふまえ，監視カメラに対するプライバシ保護のためには，被写体ごとの同意の有無と閲覧者の閲覧目的に応じて配信映像を変化させることが望ましいと考えられる．

2.3 問 題 点

ここで従来技術を振り返ると，以下のような問題がある．たとえば文献 4) 等のように人体を検出・隠蔽するのみの技術では，被写体の同意の有無をシステムに反映できない．また，文献 10) 等のように同意の有無によるカメラ制御を可能にするシステムは，たとえば「公的機関は完全な映像を閲覧可能とする」という要件に対応できない．

こうした従来技術の問題をカバーするため，本稿では，被写体の同意の有無と閲覧者の閲覧目的に応じて適切な画像処理を選択・実行し，映像内のプライバシ情報をフィルタリングするシステムを提案する．3 章で提案するシステムでは，被写体からのプライバシ保護要求と閲覧者の閲覧要求を取得し，撮影映像内の被写体ごとに異なる保護レベルを適用する．ここで，提案システムでは画像認識による人物の検出結果と，被写体が保持する携帯機器から送信される位置情報のマッチングによって個人同定することを想定している．

このようなシステムを有効に機能させるためには次の 2 つの問題がある．

(1) センシング技術の精度：同定を正しく行うためには，基礎となる各センサの精度が重要である．たとえば既存の位置測位技術では比較的高精度である超音波センサを用いても 10 cm 程度の誤差が発生しうる[2)]．

(2) センサ情報の遅延：位置情報と画像認識結果の同定を行う際には位置情報の遅延が問題となる．たとえば情報の通知に 1 秒の遅延があると，一般的な歩行者速度（1 m/s）から考えて 1 m の誤差が生じるため，センサの精度がいかに高くても同定が困難となる．

上記の問題に対し，提案システムでは後者の遅延が特に問題となる．この理由は，提案システムは従来の個人同定のみを行うシステムと異なり，被写体・閲覧者双方の要求の処理，および要求に基づく撮影映像の加工・配信処理を行うものであるため，これらの処理負荷にともなう遅延が無視できない値になるからである．

以上をふまえ本稿では，提案システムの有効性を確認するため，双方の要求に応じて映像を加工・配信するシステムの詳細について述べ，プロトタイプシステムによる遅延時間の測定結果を報告する．

3. 閲覧者と被写体の関係に基づくプライバシ保護システム

3.1 提案システムの概要

図 2 は，提案システムの考え方を示したものである．提案システムでは，被写体のプライバシ保護と閲覧者の閲覧目的の両立を図るため，被写体と閲覧者の双方からそれぞれプライバシ保護要求（以下，保護要求とする）と映像閲覧要求（以下，閲覧要求とする）を受ける．そして，両者の要求に基づき，適切な画像処理やカメラ制御等のプライバシを保護する機能（以下，フィルタと呼ぶ）を実行する．そしてフィルタ実行後の映像を閲覧者へ配信するとともに，被写体が任意で実行可能なフィルタに関する情報を通知する．なお，フィルタの例としては，たとえば 2.1 節で概観した従来技術による人物隠蔽処理等を想定している．

図 3 は提案システムの構成を示したものである．図は，1 台の定点カメラによる被写体の撮影映像を，閲覧者が閲覧端末から見ている様子を示している．この

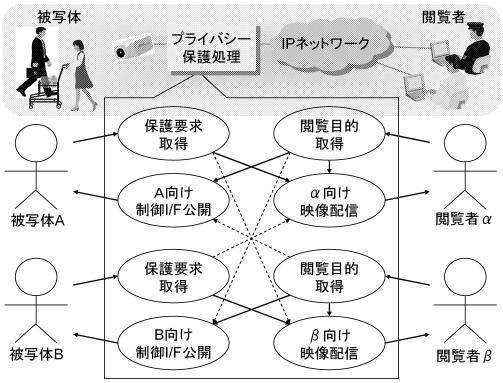

図 2 システムコンセプト
Fig. 2 System concept.

表 1 想定するシステム要件
Table 1 Assumed system requirements.

No.	想定要件	
1	下記の「公共の安全確認」以外の撮影目的において，以下の要件を満たすこと	
2	- 撮影に対する非同意者を隠蔽すること	
3	- 同意の付与は閲覧者ごとに設定可能であること	
4	- その他，隠蔽領域を設定可能であること	
5	- 隠蔽する度合い（モザイク粒度等）を設定可能であること	
6	以下に示す撮影目的に応じて異なる処理を行うこと	
7	公共の安全確認	映像の全領域を表示すること
8	半公共性を有する安全確認	犯罪行為を検知するため，顔領域以外は表示すること
9	解析評価（動線・流量解析）	人物領域を隠蔽すること
10	雰囲気確認	全体をぼかすこと
11	設備の異常監視	監視対象設備は表示すること

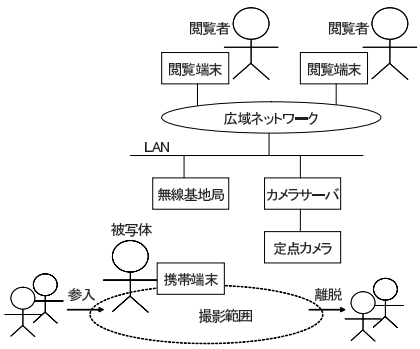

図 3 提案システム概要
Fig. 3 System overview.

システムにおいて映像情報のフィルタリングは以下の手順でなされる．まず，携帯端末では定期的に位置情報を測位しており，この測位結果を含む保護要求をカメラサーバへ送信する．この送信は，ユーザが携帯端末で明示的な操作を行うか，あるいは無線 LAN の電波強度が一定の閾値以上になった際に自動的になされる．保護要求を受信したカメラサーバでは，3.2 節で述べる方法に従って実行するフィルタを決定するとともに，画像認識結果と受信した位置情報に基づく個人同定処理を行い，各被写体に対して適切なフィルタを適用する．

3.2 プライバシ保護要求と閲覧要求の調整

3.2.1 要求の記述方式

提案システムは，被写体と閲覧者の相反する要求を調整するため，双方の要求を一定の書式のルール（以下，制御ルール）として記述し，被写体と閲覧者の関係によって適切なルールを選択し実行するものとした．

表 1 は，本稿の提案システムのシステム要件として想定するものである．表にあげた要件には，大きく分けて，No.1 から 5 に示す被写体の同意の有無を反映する要件と，No.6 から No.11 に示す閲覧目的を反映する要件とがある．

この閲覧者側の要求と被写体側の要求の記述として，それぞれ，閲覧者側の要求を示す制御ルール（閲覧者側ルール）および被写体側の要求を示す制御ルール（被写体側ルール）を考える．閲覧者側ルールは，どのような場合に撮影・閲覧されうるのかを被写体が把握できるようにするため，カメラサーバに静的に設定されて外部から参照可能とする．一方，被写体側ルールは，撮影に対する同意の有無等，個々の被写体ごとに異なる要求を記述するため，被写体が保持する携帯端末に設定する．携帯端末に設定されたルールは，保護要求に含められて近隣のカメラサーバへ通知される．

この制御ルールに記載する情報について以下に述べる．まず，閲覧者側ルールには，表 1 の No.7 から No.11 に示す各閲覧目的を示す情報と，その閲覧目的を達成するうえで必ずしも必要ない撮影情報（以下，隠蔽許容情報とする）を記載する．前者の閲覧目的を示す情報は,「安全確認」「雰囲気確認」といった言葉をそのまま用いて記述することも考えられるが，誰にどのような撮影映像が提供されるかを被写体が理解可能とするため，提案システムでは閲覧者・閲覧場所・閲覧時刻の組合せによって記述する．一方，被写体側ルールには，撮影への同意の有無を記載する．この同意の有無は，同意を与える閲覧者・閲覧場所・閲覧時刻の組合せと，同意の度合い，すなわち隠蔽処理を要求する情報（以下，隠蔽要求情報とする）を記載する．

閲覧者側ルールに記載する隠蔽許容情報と，被写体側ルールに記載する隠蔽要求情報は，領域および隠蔽方法によって指定する．ここで領域は，表 1 の要件より人体領域，頭部領域，および指定領域のいずれかを記載し，隠蔽方法はマスク処理とモザイク処理のいずれかを記載する．

以上より，双方の制御ルールには以下の項目を記載する．なお，下記の記載項目のうち，閲覧者 ID・被

```
<rule subject="被写体 s" browser="閲覧者 b">
  <param key="閲覧場所" value="自宅"/>
  <filter name="モザイク" />
</rule>
```

図 4 制御ルールの例
Fig. 4 Example of a control rule.

写体 ID における記号 “*” と “-” は，それぞれ 1 人でも人物がいる状態，および人物が誰も存在しない状態を意味する．また，括弧内に記載している項目名は，3.2.2 項でのアルゴリズム表記に利用するものである．

(1) 閲覧者 ID（browser）：閲覧者を示す ID，“*”，“-” のいずれかを記載する
(2) 被写体 ID（subject）：被写体を示す ID，“*”，“-” のいずれかを記載する
(3) パラメータ（param）：閲覧場所，閲覧時刻を記載する
(4) フィルタ（filter）：隠蔽許容情報または隠蔽要求情報を記載する．

図 4 は，制御ルールの例を示したものであり，閲覧者 b が被写体 s を自宅から閲覧する際は被写体 s にモザイク処理を実行することを示している．

3.2.2 制御ルールの選択手順

以下に，被写体側ルールと閲覧者側ルールを参照して，実行する制御ルールを選択する手順について述べる．

この手順においては，どのような制御ルールが選択されるかを被写体が事前に把握・制御できることがプライバシ保護の観点から必要である．そのため，提案システムでは双方の要求に対する曖昧な折衷案を選択するのではなく，要求の衝突があった際には閲覧者側の要求を優先して実行し，被写体へは携帯端末を通じて警告を通知する．閲覧者側を優先する理由は，先に述べたように特定の用途では監視システムとして実用性を優先させる必要があると考えるからである．

以下はこの調整手順を記載したものであり，閲覧者側ルールの集合 R_b，および被写体側ルールの集合 R_s から，被写体 s と閲覧者 b の組合せに対して実行する制御ルールの集合 R を決定する処理を示している．

制御ルールの調整処理

Step.1
$R'_s = \phi$
for each r in R_s do
　if ($r.subject = s$ or $r.subject = *$) and
　($r.browser = b$ or $r.browser = *$) then
　　Add(R'_s, r)
$R'_b = \phi$
for each r in R_b do
　if ($r.subject = s$ or $r.subject = *$) and
　($r.browser = b$ or $r.browser = *$) then
　　Add(R'_b, r)

Step.2
for each $r1$ in R'_s do
　for each $r2$ in R'_b do
　　if $r1.filter > r2.filter$ then
　　　Delete(R'_s, $r1$)

Step.3
$R = R'_s$
for each $r1$ in R'_s do
　for each $r2$ in R'_b do
　　if $r1.subject = r2.subject$ and
　　$r1.browser = r2.browser$ and
　　$r1.filter < r2.filter$ then
　　　Delete(R, $r1$)
　　Add(R, $r2$)

上記の手順の実行内容について以下に説明する．まず Step.1 では，R_s と R_b から被写体 s・閲覧者 b に関連するルールを抽出し，それぞれ R'_s と R'_b としている．なお，閲覧者 b に関連する比較処理では閲覧場所および閲覧時刻を含めた比較を行うが，本稿では省略している．

Step.2 は，被写体と閲覧者双方のルールに衝突があったときの処理であり，R'_s と R'_b 内のルールを相互に比較し，衝突するルールがあれば R'_s 側のルールを削除している．ここでルールが衝突するとは，閲覧者が許容するレベル以上の保護を被写体が要求した場合であり，R'_s 内のルールで指定された隠蔽要求情報が R'_b 内のルールで指定された隠蔽許容情報の一部を包含する場合である．

Step.3 は，画像処理効率化のための処理である．この手順では，被写体 ID と閲覧者 ID の組合せが同一のルールがあり，かつ R'_b 内のルールで指定された隠蔽許容情報が R'_s 内のルールで指定された隠蔽要求情報を完全に包含する場合は，R'_b 内のルールのみを選択している．

3.2.3 フィルタの実行手順

3.2.2 項の手順は，システム上に存在する被写体および閲覧者の全組合せに対して実行する必要がある．すなわち，被写体あるいは閲覧者に変化が発生するごとに，実行される制御ルールは変化する．

この手順では，ルールが変更される瞬間に被写体が無制限に閲覧されることを防止するため，変更後の状態に基づく制御ルールを実行してから，変更前の状態

に基づく制御ルールを停止することが必要となる．

以下に，被写体 s の参入時（s からの保護要求受信時），s の離脱時，閲覧者 b の参入時，および b の離脱時におけるフィルタの実行手順を示す．ここで B は現在映像を閲覧している閲覧者の集合であり，S は現在撮影範囲内に存在する被写体の集合である．また，サブルーチン Run(s, b) は，被写体 s および閲覧者 b の組合せに対して 3.2.2 項の手順で決定される制御ルールの集合 R を実行するものであり，同様にサブルーチン Stop(s, b) は R を停止するものである．

被写体 s 参入時
if $B = \phi$ then Run(s, -)
else for each $b \in B$ do Run(s, b)
if $S = \phi$ then Stop(-, b)

被写体 s 離脱時
if $S = \{s\}$ then Run(-, b)
if $B = \phi$ then Stop(-, b)
else for each $b \in B$ do Stop(s, b)

閲覧者 b 参入時
if $S = \phi$ then Run(-, b)
else for each $s \in S$ do Run(s, b)
if $B = \phi$ then Stop(s, -)

閲覧者 b 離脱時
if $B = \{b\}$ then Run(s, -)
if $S = \phi$ then Stop(s, -)
else for each $s \in S$ do Stop(s, b)

たとえば被写体 s 参入時には，閲覧者が存在しない場合は s のみによって定まる R を実行し，閲覧者が存在する場合は各閲覧者 b によって定まる R を実行してから，s 参入前に実行していた R を停止する．

3.3 プロトタイプシステム

以上で述べた提案システムのプロトタイプを構築した．**図 5** にシステムの構成を示す．このプロトタイプシステムは，100Base-T Ethernet☆上にカメラサーバ，および閲覧端末（PC）を設置し，また，802.11b 無線 LAN を介して携帯端末（PDA）を設置している．そのほかに，4 章での評価用に PC および RFID リーダを設置している．

プロトタイプシステムの動作は，3.1 節で述べたとおりである．なお，撮影映像は JPEG/RTP 方式によって配信され，映像を閲覧する際は，閲覧者は Web ブラウザを用いてカメラサーバへ閲覧者 ID および認証情報を送信し，映像の閲覧のみが可能な専用ソフトウェア（Java☆☆アプレット）をダウンロードして閲覧する．また，撮影された映像は加工処理を施す前の状態でカメラサーバへ一定時間記録され，第三者が持ち出せないようアクセス制限が施されている．

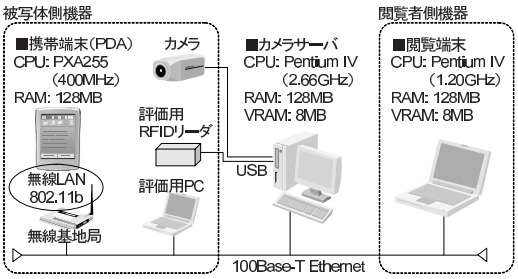

図 5 プロトタイプシステム
Fig. 5 Prototype system.

図 6 制御ルールによる出力画面
Fig. 6 Sample output images based on control rules.

表 2 実行例の制御ルール
Table 2 Privacy control rules for the sample outputs.

No.	被写体	閲覧者	フィルタ
1	近隣住民	警備員（犯罪検知）	顔以外を表示
2	近隣住民	近隣住民（雰囲気確認）	全体を隠蔽
3	近隣住民	保守業者（設備監視）	指定領域を表示
	近隣住民	*	人体領域を隠蔽

以上のプロトタイプシステムの実行例として，1 章で述べた街頭防犯カメラを想定したものを**図 6** に示す．また，図に示した 3 つの実行画面に相当する提案システムの動作を**表 2** に示す．

まず，図 6 の左上の画面は，警備員が犯罪行為の検知を目的として監視する際の閲覧映像を示したものである．これは表 2 の No.1 によって顔（頭部領域）のみに対する隠蔽処理が実行された結果である．同様に，右上の画面は，近隣住民が撮影範囲の雰囲気確認を目

☆ Ethernet は米国 XEROX 社の商標．

☆☆ Java は米国 Sun Microsytems 社の商標．

的として見る際の映像を示したものであり，表 2 の No.2 によって撮影領域全体への隠蔽処理が施されている．左下の画面は，保守業者が街頭設備の監視を行う際の映像を示したものである．この画面では，表 2 の No.3 によって住民の要求を反映した人体領域の隠蔽処理がなされているが，保守業者が監視を行うべき領域（矩形）で示した部分は表示されている．なお，右下の画面は，被写体（住民）が持つ携帯端末の画面を示したものであり，撮影映像の静止画と，被写体が任意で指定可能なフィルタを表示している．

4. 評　　価

4.1 想定利用環境

評価実験に先立ち，提案システムが有効である利用環境についての考察を以下に述べる．**表 3** は，一般的な市販の監視カメラの利用環境を示したものであり，カメラによる撮影可能距離を 20 m，人間の歩行速度を 1 m/s とした場合の，歩行者通行量に対する撮影範囲内の瞬間被写体数，および撮影映像の横方向 1 m あたりの平均人数（密度）を試算したものである．なお，提案システムの利用場所は監視カメラの設置が進んでいる繁華街と公園を想定し，歩行者通行量は，繁華街については文献 21) に記載の渋谷センター街の値を，公園については文献 5) に記載の日比谷公園の値を参考に設定した．

表より，歩行者通行量が 10,000 (人/時) である繁華街においては，横幅 1 m あたりの被写体数が 2.77 (人/m) である．この値は，既存技術によって撮影映像内の各々の被写体の個人同定を行うにはきわめて困難な値であるため，本稿での評価の対象外とする．一方で，公園における値は 0.138 (人/m) であり，この値は，従来研究[12] において位置測位精度が約 30 (cm) の場合に 1 m ほど離れている 2 人を同定可能であることをふまえると，個人同定が十分可能な値であると考えられる．そこで以下では，公園に相当する環境での提案手法の有効性について評価する．

ここで，位置測位自体の誤差については，2.3 節で紹介したように従来研究でおよそ 10 cm の精度を達成できると考えられるため，以降の評価に際しては提案手法の影響による位置情報の誤差がおよそ 20 cm に収まることを確認する．20 cm の誤差は，歩行者速度を 1 m/s とすると 200 msec の遅延に相当する．

4.2 要求調整に起因する負荷の考察

まず，3.2 節で述べた提案システムの要求調整処理に起因する影響について考察する．

提案システムでは，被写体が参入・離脱するごとに，

表 3 想定利用環境
Table 3 Envisioned environments.

比較項目	単位	繁華街	公園
通行量	(人/時)	10,000	500
被写体数	(人)	55.4	2.76
密度	(人/m)	2.77	0.138

もしくは閲覧者が閲覧を開始・停止するごとに，3.2.3 項で示した手順が実行され，そのステップ数は，被写体参入時における閲覧者数を N_b とすると $O(N_b)$ である．

この各ステップごとに 3.2.2 項で示したアルゴリズムが実行され，そのステップ数は，R_s，R'_s，R_b，R'_b の要素数をそれぞれ n_{rs}，$n_{rs'}$，n_{rb}，$n_{rb'}$ とすると，$O(n_{rs})+O(n_{rb})+O(n_{rs'}n_{rb'})$ である．この値は N_b に依存しないことから，被写体 s の参入時に発生する要求調整処理のステップ数は $O(N_b)$ である．同様に被写体離脱時のステップ数も $O(N_b)$ である．また，閲覧者の参入・離脱時のステップ数も，その時点での被写体の数を N_s とすると，同様の考察により $O(N_s)$ となる．

以上のオーダ計算に対して，表 3 より，N_s はおよそ 2.7 人であるから，閲覧者が変化する際の負荷の影響はほとんどない．一方，N_b についてはこうした制限がないため被写体の参入・離脱よる負荷の影響は N_b の増加に応じて大きくなる．そこで，提案システムでは同時にシステムを利用可能な閲覧者数を一定数に制限するものとする．

4.3 提案システムの有効性確認

以上の考察をふまえ，提案手法が位置情報の到達遅延へ与える影響について 3.3 節のプロトタイプシステムを用いた実験により確認した．実験では，以下にあげる各々のイベント発生から，カメラサーバでフィルタが呼び出されるまでの要求遅延時間を測定した．

- 携帯端末での保護要求送出
- PC での保護要求送出
- RFID リーダを制御するプログラムでのタグ検出

ここで各イベントは，表 3 での公園での歩行者通行量を模擬して，発生率 500 (件/時) により等間隔で発生させた．また，これらの値を評価するために，PC とサーバ間の Ping 応答（ICMP エコー）時間を測定した．

図 7 に，要求遅延時間の測定値（縦軸）と映像の配信ビットレート（横軸）の関係を示す．なお図に示す測定値は，連続する 10 回の測定値の平均値を算出したものである．

図より，携帯端末からの要求遅延が映像配信ビット

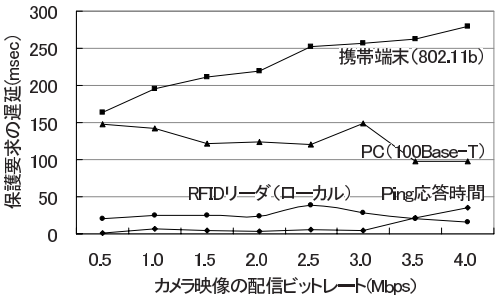

図 7 要求遅延時間
Fig. 7 Latency of requests.

レートの増加にあわせて大きくなる一方，PC からの要求遅延は増加しない．この違いは各々の利用する通信帯域にあると考えられ，携帯端末においても十分な帯域を利用可能になれば，要求遅延はおよそ 150 msec になると考えられる．これは歩行者速度 1 m/s に照らし合わせて考えると 15 cm の誤差となる．この値は，表 3 に示した公園での利用においては個人同定が可能な範囲の誤差であることから，提案システムは有効であるといえる．

なお，RFID リーダによる測定結果から，ネットワーク通信に依存しない処理（3.2 節で述べた要求調整処理を含む）の遅延はおよそ 20 msec である．また，Ping 応答時間の測定結果から LAN 上の通信遅延はきわめて少ない．したがって遅延時間 150 msec の大半はカメラサーバ上で発生している通信遅延であり，これは主に映像配信処理の影響であると考えられる．到達遅延の低減が必要な場合はこの点の対策が必要となる．

4.4 提案システムにおける法的視点での課題

プライバシの課題は技術的アプローチのみで解決できるものではなく，法律の専門家を含めた議論が不可欠である．1 章で言及したやおよろずプロジェクトにおいて，Murakami らのグループは法律の専門家としてユビキタス環境における監視カメラ向けのプライバシガイドラインについて検討を行っている[9]．本節では，提案システムの考え方について同グループでヒアリングを実施した結果得られた意見を紹介する．

まず提案システムの考え方については，カメラの設置場所，たとえばパブリックな場所やプライベートな場所によって処理が変わることはあるかもしれないが，被写体によって処理が変わるかどうか，すなわち個人によって保証されるプライバシ権が異なるかどうかについては一概にいえないとの指摘を得ている．

また，撮影に対する通知・同意取得に関するさらなる検討が必要であるとの指摘を得ている．たとえば，提案システムには肖像権の問題があり，同意なくカメラ撮影することの問題はもとより，撮影映像において顔にモザイクをかける等の処理を行うことの可否から議論が必要である．

また，撮影映像を配信する際の二次配信を防止するため，提案システムでは閲覧端末側での情報の蓄積を防止する機能も含めて検討している．しかし，この点に関しては，肖像権，プライバシ保護，著作権管理は法的に別の問題であるため，技術的にも混同しないほうが好ましいとの指摘を得ている．

5. ま と め

本稿では，カメラ撮影に対するプライバシの問題について，被写体のプライバシ保護と監視カメラの閲覧目的の両立を図るため，被写体と閲覧者の関係によって適切なプライバシ保護を行うシステムの提案を行った．提案システムは被写体・閲覧者からそれぞれプライバシの保護要求と映像の閲覧要求を受信し，双方の要求を示す制御ルールに従って画像処理やカメラ制御を実行する．この提案システムのプロトタイプを試作することによりシステムの有効性の確認を行った．

提案システムには，いくつかの課題が残されている．まず，本稿では触れなかった映像内における被写体の個人同定処理の精度向上がある．そして，4.4 節であげた法制度面での課題に対して，法律の専門家と連携した取り組みが引き続き必要である．

こうした課題に今後取り組み，将来のユビキタス社会における監視カメラからのプライバシ保護のあり方を検討していく予定である．

謝辞 本研究は，文部科学省科学技術振興調整費により実施した「横断的科学によるユビキタス情報社会の研究」の成果の一部である．関係者のご協力に感謝する．

参 考 文 献

1) Boyle, M., Edwards, C. and Greenberg, S.: The Effects of Filtered Video on Awareness and Privacy, *Proc. 2000 ACM Conference on Computer Supported Cooperative Work*, pp.1–10 (2000).
2) Fukuju, Y., Minami, M., Morikawa, H. and Aoyama, T.: DOLPHIN: An Autonomous Indoor Positioning System in Ubiquitous Computing Environment, *IEEE Workshop on Software Technologies for Future Embedded Systems* (*WSTFES2003*), pp.53–56 (2003).
3) Funabashi, M., Homma, K. and Sasaki, T.: Introduction to the Yaoyorozu Project, *SICE Annual Conference 2003*, pp.1332–1335 (2003).

4) Hudson, S.E. and Smith, I.E.: Techniques for Addressing Fundamental Privacy and Disruption Tradeoffs in Awareness Support Systems, *Proc. 1996 ACM Conference on Computer Supported Cooperative Work*, pp.248–257 (1996).
5) 石黒伯和：来園目的を考慮した公園内通行量の予測シミュレーションモデル，修士論文，早稲田大学大学院 (2004).
6) Jendricke, U. and tom Markotten, D.G.: Usability Meets Security—The Identity—Manager as Your Personal Security Assistant for the Internet, *Proc. 16th Annual Computer Security Applications Conference*, p.344 (2000).
7) Kawamichi, H., Sekiguchi, T., Sameshima, S., Morikawa, H. and Takashio, K.: Opportunities and Issues Relating to Middleware Technologies for Context-aware Services (2), *SICE Annual Conference 2004*, pp.2704–2708 (2004).
8) Langheinrich, M.: A Privacy Awareness System for Ubiquitous Computing Environments, *Proc. 4th International Conference on Ubiquitous Computing*, pp.237–245 (2002).
9) Murakami, Y.: Privacy Issues in the Ubiquitous Information Society and Law in Japan, *2004 IEEE International Conference on Systems, Man and Cybernetics* (2004).
10) Neustaedter, C. and Greenberg, S.: The Design of a Context-Aware Home Media Space for Balancing Privacy and Awareness, *Proc. 5th International Conference on Ubiquitous Computing*, pp.297–314 (2003).
11) OECD: *OECD Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, adopted by the Council of the OECD of 23 September 1980* (*OECD Privacy Guidelines*).
12) 岡本直樹：RFID とカメラによる位置検出・個人同定システム，修士論文，大阪工業大学 (2005).
13) Pfitzmann, A. and Köhntopp, M.: Anonymity, Unobservability, and Pseudonymity—A Proposal for Terminology, *Workshop on Design Issues in Anonymity and Unobservability*, pp.1–9 (2000).
14) 坂田宗之：ALTAIR：アクティブ IR タグを用いた複数ユーザ位置同定システム，修士論文，奈良先端科学技術大学院大学 (2003).
15) Sameshima, S., Kawamichi, H., Kato, H., Sekiguchi, T., Morikawa, H., Takashio, K. and Tokuda, H.: Opportunities and Issues Relating to Middleware Technologies for Context-aware Services, *2004 IEEE International Conference on Systems, Man and Cybernetics*, pp.5667–5672 (2004).
16) Sekiguchi, T. and Kato, H.: Privacy Assuring Video-Based Monitoring System Considering Browsing Purposes, *IEEE/IPSJ International Symposium on Applications and the Internet Workshops*, pp.464–467 (2005).
17) 島井博行，三島健稔，栗田多喜夫，梅山伸二：移動物体検出のためのロバスト統計を用いた適応的な背景推定法，画像の認識理解シンポジウム（MIRU2000）論文集 II，pp.391–396 (2000).
18) Yasuda, K., Naemura, T. and Harashima, H.: Thermo-Key: Human Region Segmentation from Video, *IEEE Computer Graphics and Applications*, Vol.24, No.1, pp.26–30 (2004).
19) Zhao, Q.A. and Stasko, J.T.: Evaluating Image Filtering Based Techniques in Media Space Applications, *Proc. 1998 ACM Conference on Computer Supported Cooperative Work*, pp.11–18 (1998).
20) 馬場功淳，大橋 健，乃 万司，松尾英明，江島俊朗：HeadFinder：フレーム間差分をベースにした人物追跡，画像センシングシンポジウム 2001，pp.363–368 (2001).
21) 産業労働局：東京都における繁華街利用実態調査報告書 (2001).

(平成 17 年 8 月 3 日受付)
(平成 18 年 5 月 9 日採録)

関口 隆昭

1974 年生．2001 年京都大学大学院情報学研究科通信情報システム専攻修士課程修了．同年（株）日立製作所入社．システム開発研究所勤務．情報制御システムのセキュリティ，プライバシの研究開発に従事．電気学会会員．

加藤 博光（正会員）

1970 年生．1995 年東京大学大学院工学研究科航空宇宙工学専攻修士課程修了．同年（株）日立製作所入社．システム開発研究所勤務．情報制御システムの運用監視制御，リスク管理の研究開発に従事．計測自動制御学会，電気学会各会員．