05 プライバシーを考慮した映像サーベイランス

馬場口 登
大阪大学大学院工学研究科

映像サーベイランスは安心か

近年，国民意識において，日本が以前よりも安全な国でなくなったと考える割合が増えたという報告があり，安全・安心な社会を構築することは，国民的な課題かつ要請となっている．安全・安心な社会に直接結びつく情報通信（ICT）技術の 1 つに，視覚センサネットワークによる映像サーベイランス（video surveillance）がある．映像サーベイランスとは，カメラ等の視覚センサが多数，ネットワークで結合されたものから得られる画像・映像情報を基に，コンピュータビジョンや画像解析の技術を駆使し，自動的に環境やオブジェクト（人や車など）を監視するシステムに関する総合的な技術を指し，その社会的重要性が早くから指摘されてきた．

しかしながら，映像サーベイランスはややもすると懐疑的ないしは否定的な見方をされることもある．その原因は，サーベイランスによるプライバシー侵害の問題が背後にあるためである．2005 年 4 月の個人情報保護法の成立が証しているように，個人情報の保護・管理はますます厳しくなる傾向にある．犯罪とは無関係の場所，コンテキストにおいて，知らぬ間に自分の実写映像が撮影される可能性のある映像サーベイランスへの不安感は，ある意味で納得できるものである．また元来，CCTV（Closed-Circuit TV）と呼ばれていたサーベイランス（監視）カメラの映像が仮にインターネットのようにオープンなネットワークを流通するようになれば，映像に含まれるプライバシー情報の保護は一層重要となる．したがって，映像サーベイランスが国民的コンセンサスを得，安全・安心な社会システムとして普及定着するには，プライバシーやセキュリティを可能な限り尊重するシステムに変貌させることが急務である．

プライバシーと映像サーベイランス研究のこれまで

ここでは，プライバシーと映像サーベイランスという視点でこれまでの研究経緯を考える．映像サーベイランスに関連する画像解析，コンピュータビジョン，コンピュータグラフィクスなどの分野の国際的リーダーはアメリカである．映像サーベイランスが注目される契機は，1990 年代後半にアメリカで実施された VSAM（Video Surveillance and Monitoring）プロジェクトである．このプロジェクトは米国防総省高等研究計画局 DARPA がスポンサーで，軍事目的が主と見なすことができよう．これを通してオブジェクト（人や車など）の検出，追跡などサーベイランスの要素技術の高度化，および新型視覚センサの発明について大きな進歩が印された．しかしながら，その根底にあるミッションを極論すれば，映像から見つけるべきものは戦場の敵兵で，サーベイランス目標へのプライバシーの考慮はほとんど見られない．

一方，我が国においても VSAM プロジェクトと相前後して，サーベイランス応用の画像解析研究が活発化し，統計的背景画像推定や全方位視覚センサによるサーベイランスなどに目立った研究がなされた．日本における特筆すべき流れは，ITS（Intelligent Transportation System）と関連した画像解析で，直線道路や交差点での交通流測定，交差点での不審運転車の検出，車載カメラによる先行車追跡などの研究がなされた．車関連の ID 情報としてカーナンバの認識技術がよく報告されているが，カーナンバや運転者のプライバシー保護という研究例は筆者の知る限り見当たらない．

プライバシー保護のための画像・映像処理研究が報告されるようになったのはここ 2，3 年のことである．米国 CMU の Newton ら[1]，英国ロンドン大の Cavallaro ら[2]，そして日本 ATR の北原ら[3]は，基本的に顔部や

人体部に平均顔，モザイク，マスクなどを自動的に映像に重畳する方法を提案した．これらはいわば，プライバシー上，不都合な部分(顔など)にはすべて蓋をするような方法と考えられる．さらに米国カリフォルニア大アーバイン校の Wickramasuriya ら[4] はプライバシーポリシーの記述を試み，IBM の PrivacyCam[5] は，プライバシーを考慮した統一的なサーベイランス枠組みを提唱している．このようにプライバシー保護を目的とする画像・映像処理の問題は大きくクローズアップされつつある．

安心な映像サーベイランスへの課題

それでは，映像サーベイランスを安心な社会システムとして定着させるにはどのようにすればよいか考えよう．そのために克服すべき問題には

- 社会的問題
- 法的問題
- 心理学的問題
- 工学的問題

が挙げられる．以下，順を追って考察しよう．

第 1 は社会的問題であるが，これはセキュリティとプライバシーのバランスをいかに取るかという一番の原点に還元される．このバランスをどこに置くかについては，各国で微妙に異なり，いわば文化的な背景も関係している．まず英国や韓国では，特殊な歴史的経緯，すなわち英国では IRA，韓国では北朝鮮と長い間緊張関係にあったという背景があった．よって，サーベイランス(監視)カメラが積極的に公共スペースに設置され，市民も重大犯罪を減らすという目的において，設置へのコンセンサスが得られているといわれている．

一方，アメリカでは市民のプライバシー意識が格別に高く，G. Orwell の SF 作品「1984 年」の “Big Brother” に支配されるような監視社会を嫌悪する傾向がとりわけ強かった．そのため公共スペースでの監視カメラが自由自在に配備できる状況には従来なかった．ところが，2001 年 9 月 11 日のニューヨーク同時多発テロを契機に，セキュリティ重視へ大きく天秤が振れ，現在は監視カメラの配備が街レベルに拡大されつつある．

我が国では以前は，銀行やコンビニにおける監視カメラが目立つ程度であった．ところが，治安の悪化に伴い，2002 年の新宿歌舞伎町での監視カメラ設置を契機に，マンションなどのプライベートスペースのみならず，公共スペースへの進出は著しい．また，近年では，監視カメラ映像の解析が，凶悪事件の犯人検挙の一翼を担うことも多く，その有用性も認知されつつある．いずれにせよ，プライバシーを取るか，セキュリティ（監視カメラ）を取るかは，社会的背景に依存することに疑いはないが，監視カメラを許容する社会的コンセンサスが徐々に醸成されつつあるとも筆者には思える．

第 2 は法的問題である．結論から言うと，監視カメラの設置，設置基準，運用法などに関する法的整備はまったくなされていない．たとえば，監視カメラの設置自体についても違法，適法の見解が分かれているのが現状である．公共スペースにおいて，無許可で人間を撮影，録画することは，これまでの判例に照らすと違法性が高いようである．しかしながら，セキュリティへの希求の増大から今後は変わる可能性もあろう．法的問題については門外漢であるためこの辺りでとどめるが，詳細は小林弁護士による文献 6)を参照されたい．

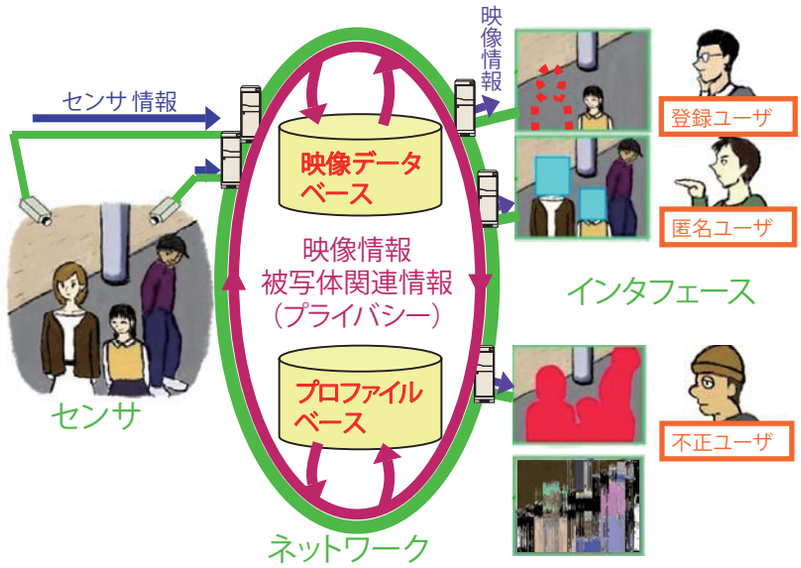
第 3 は心理学的問題である．プライバシーとは，そもそも個人が個人の領分と考える範囲に依存する概念であるため，個人性や主観性が強い．自分の容姿が映ったサーベイランス映像を他者に見せる場合に，どこまで自分の画像を開示すればプライバシーを侵されたと感じるかは，個人によりまちまちということである．つまり，ある人は実写で見せても良いが，別の人は存在すらも隠したいという場合が想定し得る．さらに，同じ人でも，場所，時間など状況依存的に自分の姿の開示範囲は異なることもある．これらの点は後で論じる映像サーベイランスシステムの設計に大きな波紋を投げかけることになる．

最後は工学的問題である．プライバシー侵害を防ぎ，個人情報を保護する技術の重要性については，近年のセキュリティ技術への注目度からも論を待たないところである．先に述べたようにプライバシーは個人性，主観性が特徴であり，これを工学的に扱うのは容易ではない．さらにユーザの安心感を向上させる技術の重要性は示唆されるものの確立されたものはなく，プライバシーに関連する技術には暗号，情報ハイディング，DB アクセス制御，映像・画像・音声などのメディア処理などが中心となろう．

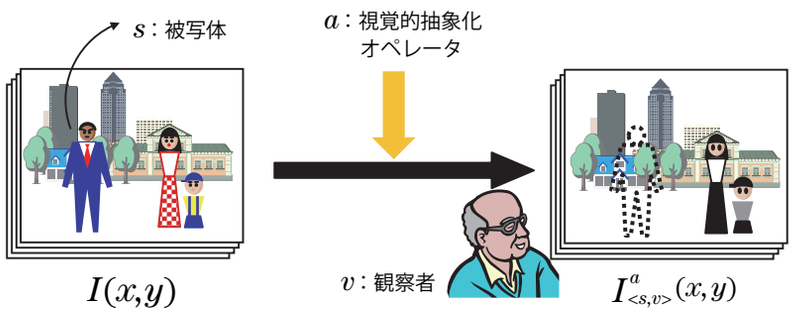
以下では，筆者らが研究推進しているプライバシー保護機能を有する映像サーベイランスシステム PriSurv（Privacy Protected Video Surveillance System）について述べる．PriSurv は，映像サーベイランスにおける情報獲得（センサ），情報流通（ネットワーク），情報表示（インタフェース）に対し，プライバシーとセキュリティをトータルに考えたものである．**図 -1** に概要を示す．

PriSurv

PriSurv は，プライバシー保護のための各種映像・画像処理，プライバシーポリシー記述，コンテンツ流通におけるセキュリティなどの技術を確立することにより安心感のある映像サーベイランスの実現を図るシステムである．ここでは，特定の閉じたエリア（施設，地区，校



■図 -1　プライバシー保護機能を有する映像サーベイランス



■図 -2　視覚情報制御プロセス

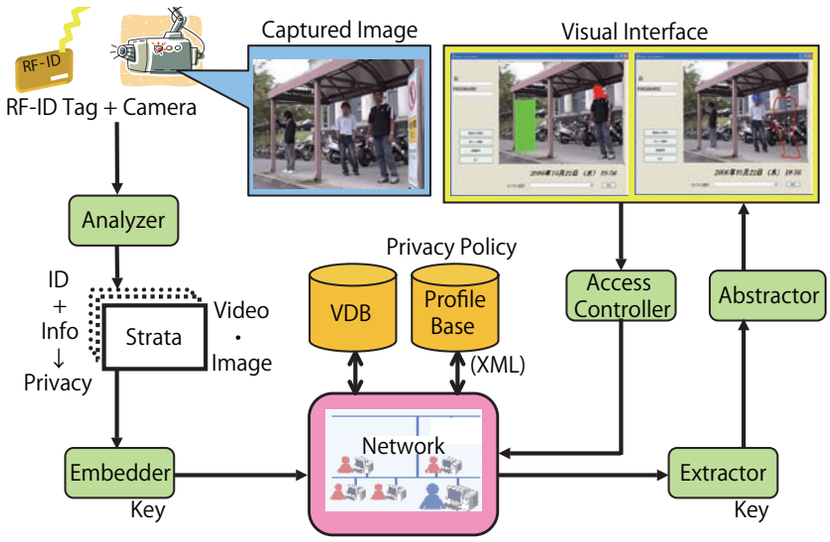
区など）におけるサーベイランスを前提に，サーベイランスサービスを受けるメンバ（登録ユーザ，権限有ユーザ，匿名ユーザ，不正ユーザなどさまざまな種別を認める）を想定し，観察者（viewer）と被写体（subject）との間で，どのレベルまで視覚情報を開示するか（プライバシーポリシー）を取り決めて，開示情報を動的に変化させつつ映像を生成表示する．視覚情報の開示制御については，視覚的抽象化（visual abstraction）[7] と呼ぶ画像処理オペレータを通じて状況依存的にプライバシーを保護した映像を生成表示する．**図 -2** に視覚情報制御プロセスを示すが，環境センシングして得られる画像 $I(x,y)$ が，被写体 s と観察者 v，および画像抽象化オペレータ a に従って加工され $I^{a}_{<s,v>}(x,y)$ を得る．

また，実写映像や被写体情報というプライバシー情報がオープンなネットワークに流れることを前提とすると，悪意の第三者（不正ユーザ）の盗み見（eavesdropping）や改ざん（tempering）にも対処できる機能が必須となる．PriSurv では，鍵暗号，情報ハイディング（電子透かし，ステガノグラフィ），コンテンツ認証，プライバシーポリシーに基づくアクセス制御により実現する．

図 -3 に PriSurv の構成を示す．PriSurv は，大きく 5 つのモジュールと 2 つの DB を有する．以下にモジュール群の機能を簡単に述べる．

Analyzer：サーベイランスカメラと ID タグにより，環境センシングを行い，メンバと非メンバとの分類，メンバについては個人同定を行う．個人同定されると被写体に関する属性（年齢，性別など）がタグを通して得られるが，これらはカメラから得られる実写情報とともにプライバシー情報ともなる．一方，画像処理については，背景差分処理に基づき，背景と前景（オブジェクト）に分け，オブジェクト（人物）を人物ごとに分離して，画像の層状表現（stratified representation）を行う．

Abstractor：層状表現された人物あるいは背景に視覚的抽象化を施し，視覚情報の開示を制限し，プライバシー保護した画像・映像を生成する．



■図 -3　PriSurv の構成

Access Controller：メンバの視覚情報開示範囲（どの人にどこまで見せて良いか）を記述したプライバシーポリシーに従い，映像情報や被写体関連情報へのアクセスを制御する．プライバシーポリシー，およびメンバの ID や属性情報の集合がプロファイルベース（Profile Base）である．プロファイルは個人情報であるため，機密性には十分な注意を要する．プロファイルはその所有者である登録メンバのみが内容の削除，更新，追加などの管理を行うことができ，他者は直接参照できない．また，プライバシーポリシーはプロファイルに記述された情報の利用法を規定するものとして位置付けられる．PriSurv では，プライバシーポリシーは XML で記述され，アクセス制御は XACML（eXtensible Access Control Markup Language）を用いて実現する．

Embedder：実写コンテンツが流通するネットワークにおけるプライバシー情報の保護のために，情報ハイディング技術を利用する．たとえば，背景映像に前景映像を埋め込んだり，前景映像にオブジェクト関連情報を埋め込む．

Extractor：情報ハイディングされた情報から鍵を用いて，埋め込まれた情報を抽出して，もとの映像情報を再構成する．

PriSurv は概念設計段階を終え，画像・映像処理の機能である Analyzer と Abstractor，さらには視覚的インタフェースについては中核部分の実装を完了している．プライバシーを保護した上で，有用なセキュリティシステムの開発という思想を掲げ，上記以外の部分の詳細設計，実装を進めている．次章では，Analyzer と Abstractor が関与するプライバシー保護画像の生成について述べる．

視覚的抽象化によるプライバシー保護画像の生成

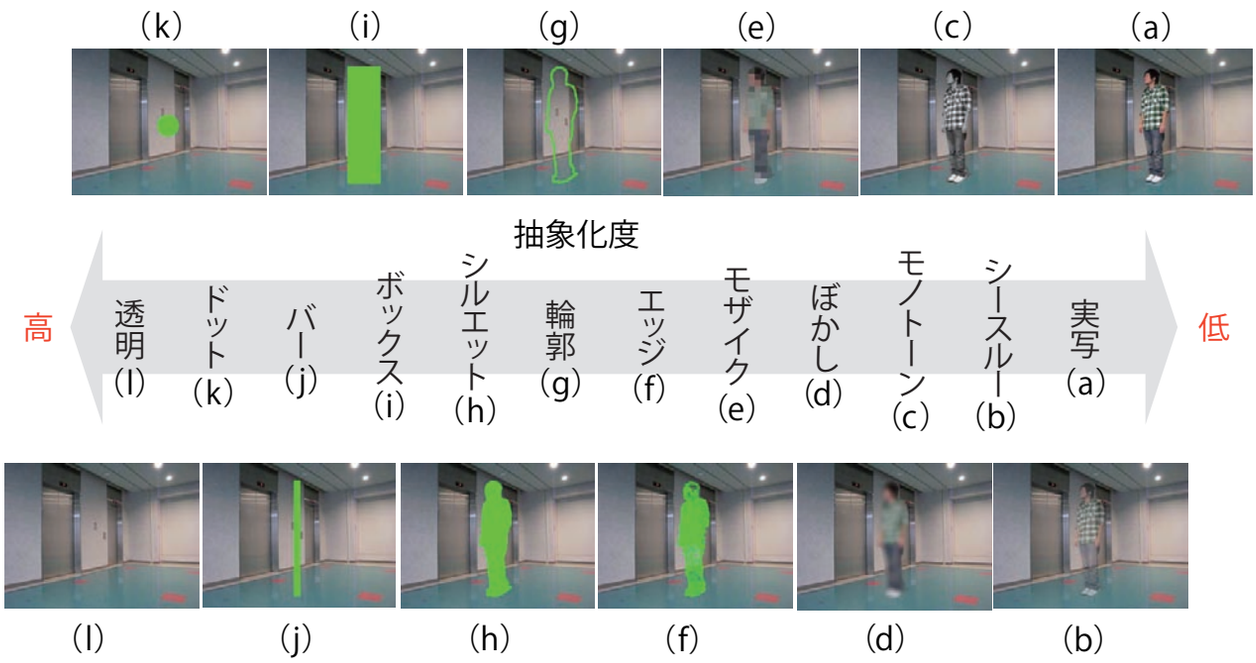
プライバシー保護のための画像生成は，画像の層状表現，ID 獲得，視覚的抽象化，画像表示を経て実現される．まず，画像の層状表現では，背景差分（background subtraction）により，前景（foreground）と背景（background）に分割する．ここでは，固定のサーベイランスカメラを前提とし，環境の微細な変動にも耐え得る背景モデル同時学習型の背景差分法（たとえば，ガウス混合型アルゴリズム）を導入する．得られる前景は，人物等のオブジェクトが複数存在するが，PriSurv では，立位の人物像をテンプレートにして，個人ごとの人物像を得，画像を層（stratum）に分割する．

いま，サーベイランス画像 I は，

$$I=B \cup F_1 \cup F_2 \cup \cdots \cup F_n$$
$$F_j \cap F_k = \phi \qquad j,k \in \{1,2,\cdots,n\}$$

と表現され，B，F_i が各々背景画像，第 i 前景画像（第 i オブジェクト）であり，n はオブジェクト数である．

次に ID 獲得では，サーベイランス映像中の人物（被写体）が，PriSurv の登録メンバか否かを分類し，さらに，登録メンバには ID 獲得を試みる．現段階での PriSurv は，屋内環境を対象とし，登録メンバには RF-ID タグを装着させることを前提とする．2 個以上の ID タグリーダーを環境に設置し，ID タグの電波到来方向を推定して，実環境での位置を定める．さらに，環境固定カメ



■図 -4　抽象化オペレータの順序関係

ラを前提としているため，画像中のオブジェクトの位置を 2 次元平面に投影して，ID タグから推定された位置とマッチングを取ることによって，第 i オブジェクトの ID を獲得する．なお，現在は ID タグを利用することによって，個人識別を行っているが，この処理は顔認識や歩容認識を援用することも可能である．

以上の処理により，以下のような前景層 SF_i と背景層 SB からなる層状表現を得る．

SF_i=< 被写体人物像 F_i，被写体関連情報 >
被写体関連情報：ID，属性（性別，年齢など）
SB=< 背景 B，背景関連情報 >
背景関連情報：場所，建物，時間など

この被写体関連情報と背景関連情報はメタデータと見なし得るもので，登録メンバに対する被写体関連情報は ID タグから得るが，それ以外のデータは映像解析によって得ることになる．

この層状表現を基に視覚的抽象化を行う．視覚的抽象化は，観察者に対し，主に人物像の ID や属性の同定に必要な視覚情報を，画像の表現粒度を変えることにより隠蔽するために施される．PriSurv で実装されている抽象化オペレータは以下の通りである．この抽象化オペレータは，実写と透明を各々抽象度最低，最高とし，半順序関係をなす．ここで，抽象度の低い順から，どのような処理かを簡単に示す．

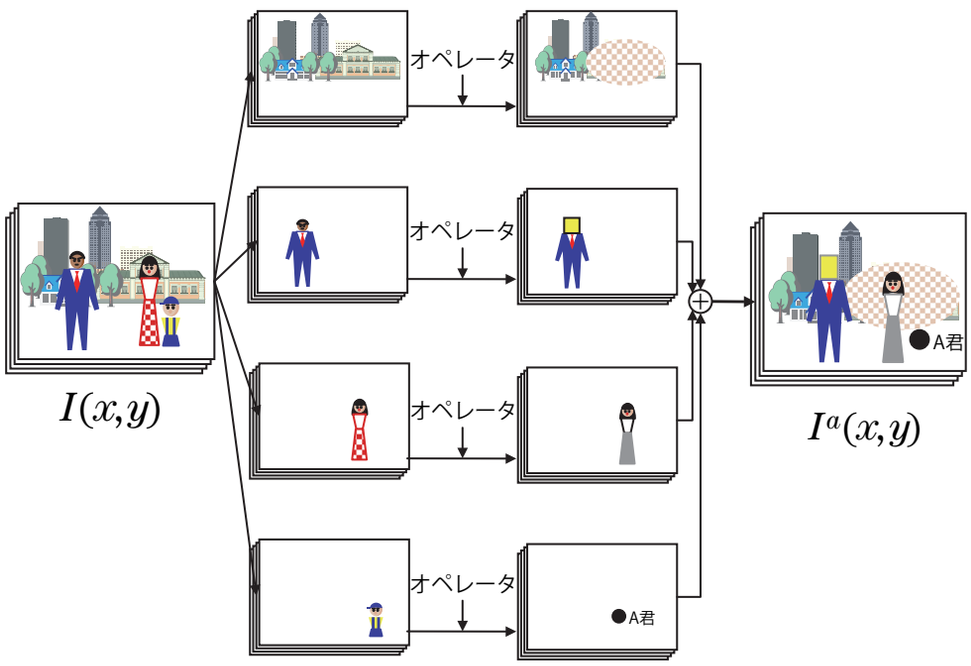
(a) 実写：センサから得られる映像情報そのもの
(b) シースルー：前景を通して背景が見えるもの
(c) モノトーン：前景のカラー情報を削除したもの
(d) ぼかし：前景をぼかしたもの
(e) モザイク：前景にモザイクをかけたもの
(f) エッジ：前景にエッジ抽出を施したもの
(g) 輪郭：前景を輪郭で表し背景が見えるもの
(h) シルエット：前景の領域を塗りつぶしたもの
(i) ボックス：前景を囲む領域を塗りつぶしたもの
(j) バー：前景を囲む領域の縦幅を表したもの
(k) ドット：前景の領域を点で表したもの
(l) 透明：前景を消去したもの

図 -4 に上記の視覚的抽象化オペレータ間の順序関係と各オペレータの作用例を示す．さらに**表 -1** に視覚的抽象化オペレータにより開示，隠蔽される視覚情報の一覧をまとめるが，情報は段階的に増減し，オペレータが半順序をなすことが分かる．オペレータの具体的な内容は割愛するが，たとえば，モザイクはブロックサイズを決定して平均値フィルタを掛ける，といったものである．

視覚的抽象化は原則的に，層状表現の層ごとに作用させる．前景の場合は，オペレータの作用領域を制御することにより，人物像の全体領域のみならず部分領域に作用させることも可能である．PriSurv では，部分領域と

	存在	位置	縦幅（身長）	横幅	概形	所持品の有無	姿勢向き	顔の向き	髪型	服装（色・形）	表情
実写	○	○	○	○	○	○	○	○	○	○	○
シースルー	○	○	○	○	○	○	○	○	○	○	○
モノトーン	○	○	○	○	○	○	○	○	○	△（色は×）	○
ぼかし	○	○	○	○	○	○	○	○	△	△	×
モザイク	○	○	○	○	○	○	○	○	△	△	×
エッジ	○	○	○	○	○	○	△	△	△	△	×
輪郭	○	○	○	○	○	△	△	×	×	×	×
シルエット	○	○	○	○	○	△	△	×	×	×	×
ボックス	○	○	○	○	×	×	×	×	×	×	×
バー	○	○	○	×	×	×	×	×	×	×	×
ドット	○	○	×	×	×	×	×	×	×	×	×
透明	×	×	×	×	×	×	×	×	×	×	×

■表 -1　抽象化オペレータによる視覚情報の開示と隠蔽（○：開示　△：一部，×：隠蔽）



■図 -5　プライバシー保護画像の生成

して顔，胴体，衣服などを想定している．すなわち，顔のみモザイクをかけるということも可能である．一方，背景に対しては，透明（削除），モザイク，ぼかしを想定するが，背景の一部に対する作用は，背景の詳細な解析が必要となる．

加えて，被写体関連情報をアノテーション（テキスト情報）として映像に重畳表示する機能も備えている．これは映像情報に情報を付加するものと捉えることができる．

最終的に観察者に表示する映像 I^a は，前景の各層ごとに抽象化された画像を背景の前面に足しあわすことにより得られる．**図 -5** にプライバシー保護画像の生成の

様子を示す．このようにして，前景の人物ごとに異なる処理も可能となる．PriSurv では，以上の処理は実時間で実行可能である．

映像表示のための視覚的インタフェースでは，観察者が ID，ユーザクラスを入力し，認証過程を経た後，被写体 ID あるいはエリアをクエリとして検索すると，プロファイルベースのプライバシーポリシーに合致した被写体の映像を表示する．また，層を区別して，抽象化の度合いを変化させるスライダも装備しており，許容される範囲の抽象度で被写体を変化させて観察できる．

心理学的考察に基づくシステム設計指針

被写体について，自身の映像を見せる相手（観察者）との親密度が，視覚情報の開示範囲（どこまで見せてもよいか）に大きく影響する．この開示範囲をある種のプライバシー感覚とみなすと，観察者と被写体の関係，表示される抽象化画像，時間帯，周辺の状況など多くの要素によって影響を受け，個人差も含まれると予想される．このような被写体の感覚を調査し，PriSurv の機能によりプライバシーを保護しつつ見守りが可能であるかを調べるため，視覚的抽象化された画像と質問紙を用いて実験を行った[8]．実験では，被験者が被写体であると仮定し，どのような親密度の人にどのような抽象化画像（実写も含む）を見せてよいかなど数十項目を質問した．

まず，因子分析により 7 因子が抽出され，守護期待因子と名づけた因子から，被験者がとても親しい人には実際に守ってもらうことを期待していることが分かった．次に因子負荷量が一定以上の質問項目の項目平均値を下位尺度得点とし，クラスタ分析したところ，被験者が 3 クラスタ，すなわち (1) 全体的に視覚情報開示に寛容なクラスタ，(2) 権限有ユーザ（警察，監視員など）に対する視覚情報開示に寛容なクラスタ，(3) 権限有ユーザに対する視覚情報開示に寛容でないクラスタに分けられた．さらにクラスタ間で選択された画像を比較し，χ 二乗検定により選択された画像での視覚的抽象化の度合いがクラスタ間で異なることが確かめられた．

クラスタ分析の結果より，被験者によってどの程度親密な人にどの画像を見せるかという基準が異なることが示され，被写体と観察者の関係によって細かい粒度で視覚情報開示を制御する仕組みの必要性が裏付けられた．PriSurv において，このような機能はプロファイルベースを経由したアクセス制御（Access Controller），ならびに視覚情報制御（Abstractor）によって実現される．

高度な映像サーベイランスに向けて

本稿では，映像サーベイランスを安心な社会システムとして定着させるため，プライバシー処理，特に画像・映像処理の観点から述べ，筆者らが開発を進める PriSurv を紹介した．さらに注意すべきは，映像サーベイランスそのものの能力，すなわち環境の変化を正確に認識する能力に関してもいまだ不十分という点である．監視カメラが事件解決に役立ったといっても，重大事件が起きて以後に監視カメラ映像の分析が役立ったわけで，即時的に，あるいは未然に事件・犯罪を防ぐレベルには至っていない．広域のサーベイランスをどうするのか，不審 X（X= 者，物，車両，行動，状況，…）をどう検出するのか，多くのモニタ画像を的確に表現する視覚インタフェースはどんなものか，など課題も多い．プライバシー保護処理は，これらの映像サーベイランスの高精度化とは異なった軸ではあるが不可欠な要素として今後一層の研究蓄積が期待される．

謝辞　日頃からご討論いただく ATR の萩田紀博博士，鳥山朋二博士，西尾修一氏，馬田一郎博士，阪大馬場口研究室の小清水隆氏，知野見健太氏を始めとする各位に感謝する．PriSurv に関連する研究の一部は，総務省・SCOPE，文部科学省・科研費による．

参考文献

1) Newton, E. M. et al.: Preserving Privacy by De-Identifying Face Images, IEEE Trans. KDE, Vol.17, No.2, pp.232-243 (2005).
2) Cavallaro, A. et al.: Semantic Video Analysis for Adaptive Content Delivery and Automatic Description, IEEE Trans. CASVT, Vol.15, No.10, pp.1200-1209 (2005).
3) Kitahara, I. et al.: Stealth Vision for Protecting Privacy, Proc. 17th ICPR, Vol.4, pp.404-407 (2004).
4) Wickramasuriya, J. et al.: Privacy- protecting Video Surveillance, SPIE International Symposium on Electronic Imaging (2005).
5) Senior, A. et al.: Enabling Video Privacy through Computer Vision, IEEE Security & Privacy Magazine, pp.50-57 (2005).
6) 小林正啓：ネットワークロボットの法的問題について，平成 17 年度ネットワークロボットフォーラム技術部会報告 (2006).
7) 小清水隆，鳥山朋二，西尾修一，馬場口登，萩田紀博：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，電子情報通信学会技術研究報告，PRMU2005-270, pp.75-80 (2006).
8) Koshimizu, T., Toriyama, T. and Babaguchi, N.: Factors on the Sense of Privacy in Video Surveillance, Proc. of Workshop on Capture, Archival and Retrieval of Personal Experiences (2006).

（平成 18 年 11 月 28 日受付）

馬場口 登（正会員）　babaguchi@comm.eng.osaka-u.ac.jp

1979 年大阪大学工学部通信工学科卒業．1981 年大学院前期課程修了．1982 年愛媛大学工学部助手，大阪大学工学部，産業科学研究所を経て大阪大学大学院工学研究科電気電子情報工学専攻教授．映像メディア処理に関する研究に従事．