情報処理学会論文誌 Vol.60 No.12 2170–2183 (Dec. 2019)

映像公開可能なプライバシ保護監視カメラシステム

星野 光太[1,a)] 岩村 惠市[1] 小林 友宏[1]

受付日 2019年2月16日, 採録日 2019年9月11日

概要：近年，プライバシとは「個人が自らの情報を制御する権利」という解釈が一般的になりつつある．一方，映像サーベイランスの普及にともない，監視カメラ映像に関するプライバシ保護が重要視され，監視カメラ映像に映った被撮影者をモザイクなどで秘匿する手法が数多く提案されている．しかし，このようなアプリケーションではシステムがかけたモザイクをシステムが外すことは容易であり，個人が自らの情報を制御するという上記の意味での真のプライバシ保護を実現していない．そこで，本論文では小林らが提案した監視カメラ映像の顔を秘匿する方式を改良した新たな監視カメラシステムを提案する．提案方式は，監視カメラ映像を公開しても安全なように，被撮影者の体全体を段階的に秘匿し，公開された秘匿映像から特定の被撮影者を検索できるなどの特徴を加える．さらに，システムではなくアプリケーションごとに被撮影者がモザイクを解除できる鍵を適切に管理できる．よって，システム側による被撮影者の望まない秘匿解除は行われない．提案方式によって，被撮影者は監視カメラ映像が公開されても自らのプライバシを制御可能になり，真の意味でのプライバシ保護を実現する．さらに，昨今注目されている監視カメラ映像を防犯以外の目的にも安全に利用できるようになる．

キーワード：映像サーベイランス，プライバシ保護，監視カメラ, 匿名署名

Privacy Protection Surveillance Camera System Enables Exposing Image

Kouta Hoshino[1,a)] Keiichi Iwamura[1] Tomohiro Kobayashi[1]

Received: February 16, 2019, Accepted: September 11, 2019

Abstract: Along with the popularization of image surveillance, Privacy Protection Surveillance Camera System (PPSCS) was proposed to properly conceal the privacy of the Subject Persons (SPs) of the surveillance camera image. PPSCS is the only method that it is possible to conceal the images reflecting the intention of the SPs. Then, we considered that people can use a surveillance camera image safely applying the PPSCS. However, PPSCS is based on the premise that the surveillance camera is used locally without being connected to the network. So PPSCS does not correspond to new requirements when connecting to the network. Therefore, in this paper, we propose Improved PPSCS (IPPSCS), corresponding to new requirements. In addition to the features of PPSCS, the feature of IPPSCS is that the degree of concealment can be changed when using the image for internal monitoring or when used for external disclosure, and that the burden on the certificate authority is reduced as compared with PPSCS, In order to reduce the complexity of management. In addition, we introduce three examples of applications that can be realized by using IPPSCS, and also show the safety when applying this method.

Keywords: image surveillance, privacy, surveillance camera, anonymous signature

1. はじめに

近年，プライバシとは「個人が自らの情報を制御する権利」という解釈が一般的になりつつある [1]．一方，映像サーベイランスの普及にともない，監視カメラ映像に関す

[1] 東京理科大学
Faculty of Engineering, Tokyo University of Science, Katsushika, Tokyo 125–8585, Japan
[a)] hoshino@sec.ee.kagu.tus.ac.jp

るプライバシ保護が重要視され，監視カメラ映像に映った被撮影者をモザイクなどで秘匿する手法が数多く提案されている [2], [3], [4], [5], [6], [7], [8]．しかし，このようなアプリケーションではシステムがかけたモザイクをシステムが外すことは容易であり，個人が自らの情報を制御するという上記の意味での真のプライバシ保護を実現していない．

それに対して，小林らが被撮影者の意思によって監視カメラに映った自らの顔などを秘匿する方式（以降，小林方式）を提案した [9]．この方式は，まず顔などのプライバシ情報の秘匿を望む被撮影者が自身の意思を匿名署名によってシステムに示す．システムはその署名を確認すると，その署名を基にモザイクを生成・解除できる鍵を生成する．その鍵を用いてその被撮影者の顔などにモザイクをかける．これによって，監視モニタには秘匿を望む被撮影者の顔などが秘匿された映像が映され，その映像が保存される．鍵は被撮影者のみが生成でき，システムは鍵を生成できないため，モザイクを除去できない．ただし，この仕組みには匿名署名に用いる鍵を発行・認証する認証局が想定されている．もし，顔などを秘匿した被撮影者が万引きなどの不正を行った場合，警察による令状などの正式な手続きを行うことで，認証局は匿名署名から被撮影者を特定し，管理する被撮影者の鍵を用いて秘匿された顔などの映像を復元できる．このシステムによって，犯罪などが起こらない限り，不正をしない被撮影者は自らのプライバシを自らの意思によって保護することができる．

一方，SCIS2017 で提案された監視カメラ運用ガイドライン [10] によると，これからの監視カメラの利用目的は従来のように防犯のみに限定するのではなく，適切にリスク評価をしつつ多目的に利用することを想定すべきとある．具体的には，防災や顧客管理のような応用例があげられている．こういった文献からも，監視カメラの様々な応用が期待されていることが分かる．また，カメラ画像利活用ガイドブック [21], [22] では，監視カメラの防犯以外の利活用におけるプライバシ保護などの配慮すべき点が示された．

そこで，本論文ではまず，監視カメラを用いた防犯以外の新たなアプリケーションを検討する．そのアプリケーションに小林方式を適用した場合を想定し，小林方式を用いただけでは解決できないプライバシ保護に関する問題点を明らかにする．その後，その問題点を解決するために小林方式を改良し，新たな監視カメラシステムを提案する．さらに，そのアプリケーションにおけるリスク評価を行い，改良方式がこれらのアプリケーションにおけるリスクを解決していることを示す．また，このシステムを個人情報保護法の観点からも検討し，法律的な観点からの実用可能性についても検討する．これらによって，監視カメラの新たな応用の可能性が示される．

本論文では，2 章で従来の監視カメラシステムに関して議論し，3 章で監視カメラの応用として新たに考えられるアプリケーションを示し，4 章でそれらのアプリケーションを実現する提案方式を説明し，5 章で法律的観点を含む提案アプリケーションにおけるリスク評価を行う．

2. 従来の監視カメラシステムの問題点

2.1 ネットワークを用いる監視カメラ

今までの監視カメラは，公共施設，店舗など特定の場所に設置され，その管理者によって運用されるのが一般的であった．近年では，監視カメラの高性能化・大衆化によって，街中，一般家庭の庭先など，多くの場所に監視カメラが設置されている．また，監視カメラをネットワークに接続することによって，監視カメラのオーナがインターネットを介して外出先で監視カメラ映像を確認できることや，クラウドなどのネットワーク上の大容量の記録媒体に映像を保存できることなどのメリットを享受できる．

しかし，監視カメラをネットワークに接続することによって，様々な弊害も生じてくる．たとえば，2014 年に，世界中の防犯カメラ映像を盗み見ることができる「Insecam」というサイトの存在が発覚して話題となった [11]．「Insecam」はクローラと呼ばれるプログラムを使ってインターネットに接続された防犯カメラを探し出し，閲覧できるようにしたロシアのサイトであり，国別，地域別，防犯カメラのメーカ別に一覧表示することが可能である．例として，2014 年の時点で，日本国内という条件で検索をかけると，約 7,000 の防犯カメラが検索一覧に表示される．よって，少なくとも国内で数千以上の防犯カメラ映像が盗み見られる状態にあるといえる．この状況は，監視カメラ映像が特に保護されていない状態である場合，プライバシがつねに流出していて，非常に危険な状況であるといえる．

さらに，SNS（Social Network Service）の発展により，だれでも動画や画像を世界中に発信できる環境になってきている．そして，監視カメラの性能は日々向上しており，その画質の良さは，その映像に映る人の顔をはっきり識別できるほどである．そんななか，コンビニ店員がモニタに映った監視カメラ映像を撮影し流出させる事件が発生した [12]．これは，店員の肖像権への意識の低さもあるが，適切に監視カメラ映像が保護されていなかったゆえに発生した事例であるといえる．

このような監視カメラ映像に映る被撮影者のプライバシ侵害を防ぐ対策として，監視カメラに関する条例・ガイドラインを設定し，これらの条例・ガイドラインを徹底させることが考えられる [10]．しかし，悪意のあるまたは意識の低い監視カメラオーナがガイドラインを守らず運用をする可能性は否定できない．

もう 1 つの対策として，監視カメラの被撮影者の顔部分に自動的にモザイクをかけプライバシを守るようなシステムの運用がある．監視カメラ映像の被撮影者の顔部分にモザイクをかける手法 [2], [3], [4], [5], [6], [7], [8] は数多く提

案されているが，システムがかけたモザイクはシステムによって容易に削除することができる．それに対して，小林方式 [9] は 1 章で述べたように，被撮影者の意思によってモザイクがかけられ，システム側でのモザイク除去は事件発生時などを除いてできない真のプライバシ保護を実現する唯一の方式である．しかし，小林方式は従来の監視カメラシステムと同様に防犯のみを想定しており，防犯以外の利用については検討されていない．

2.2 関連研究との比較

監視カメラの被撮影者のプライバシ保護に関連する研究は様々なものがある [2], [3], [4], [5], [6], [7], [8] が，それらと小林方式を用いる本研究との大きな違いは，被撮影者の秘匿化をシステム側の都合で解除できるかできないかという点である．

たとえば，参考文献 [3] では，被撮影者を authorized personnel と unauthorized personnel に分け，前者は RFID タグを持つことでシステム側に検知される．また，観察者が lower level of security clearance と higher level of security clearance とに分けられ，後者は秘密鍵を持っており，この秘密鍵を用いることで，顔が秘匿されていない状態の映像を見ることができる．一方前者は，秘密鍵を持たず，顔が秘匿された状態の映像のみ見ることができる．この手法においては，文献 [8] と同様に，被撮影者のプライバシ保護の一部を実現し，RFID タグを持つことで被撮影者の意思を確認できるが，higher level of security clearance であれば被撮影者の意思にかかわらず秘匿解除できる．また，RFID タグから出される信号が定型のものであれば偽造される可能性があり，通常の署名などであればその署名者が特定される．このほかにも，文献 [3] と同様に顔を隠すことによって，プライバシ保護を実現するが，観察者の権限によって見ることのできる映像が異なるという監視カメラシステムの研究が多数あげられる．

たとえば，Andrew らの研究 [4] では，被撮影物をシステム側で識別し，観察者に応じて識別した情報を提供することができる．Sohn らの研究 [5] では，被撮影者の顔部分にスクランブリングをかけることにより顔情報を秘匿し，スクランブリングを復号する鍵を持つ観察者のみが原動画を見ることができる．Carrillo らの研究 [6] は，監視カメラで撮影した人物の顔部分をエンコード前に暗号鍵で暗号化し，ディスプレイに表示する際には，デコード後に復号鍵を用いた場合のみ顔部分を正しく復号することができるというシステムである．Dufaux らの研究 [7] は監視カメラで撮影した映像にスクランブリングを施すことでプライバシを保護し，スクランブリングに用いた公開鍵に対応する秘密鍵を用いることで，元の映像を見ることができる．

また，より高いプライバシ保護を実現するために Chen らの研究 [8] では，被撮影者に対して ghost-image を生成している．この ghost-image は，被撮影者が着ている服なども含めて映像を秘匿するため性別を判断することも困難となり，その人物をよく知る観察者に対しても有効な個人情報の秘匿になると考えられる．しかしながら，この ghost-image も被撮影者の意思によって生成されているものではないので，自身の情報の制御の実現はされていない．

これらの研究は小林方式と同様に内部監視のみを想定し，外部公開は想定していない．よって，これらの研究を外部への映像公開に適用した場合，後述する問題 1〜3 が発生する．また，監視者は監視対象者の意思に関係なく映像を復元できるため，悪意ある人物が監視者となった場合，監視対象者はその人物によって容易に監視されるという問題も発生する．

2.3 監視カメラの応用

もし，監視カメラ映像の被撮影者のプライバシを適切に秘匿できるならば，監視カメラは防犯以外にも，防災や顧客管理のような利用ができる可能性がある．たとえば，自治体による繁華街の人流把握による防災システム，自動飲料販売機における顧客情報の収集システムなどである [10]．これらのシステムは監視カメラの新たなアプリケーション・方向性を示している．しかし，被撮影者のプライバシ保護に関しては，あくまでシステム側の良心に依存しており，被撮影者が関与することはできない．特に，監視カメラを防犯目的以外に利用することを考えた場合，その映像が不特定多数の人に閲覧される可能性がある．小林方式を含む多くの従来方式は被撮影者の顔以外の服装や動作は秘匿しないため，被撮影者の服装や動作の特徴を知る人などによって顔を秘匿した被撮影者であっても特定される可能性がある．よって，上記の関連研究を用いれば一律にプライバシが保護されるとはいえない．

そこで，次章ではまず，監視カメラによる防犯以外の新たなアプリケーションについて検討し，それに小林方式を適用した場合の問題点を検討する（関連研究を適用した場合，これ以上の問題が発生すると考えられる）．

3. 監視カメラの新たな応用と問題点

本章では，まず監視カメラを用いたアプリケーションとして具体的なサービス例を 3 つあげ，それに小林方式を適用した場合の問題点を考える．

3.1 新たなアプリケーション

(1) 子供の見守りサービス

監視カメラ映像を応用したアプリケーションの具体例の 1 つとして，子供の見守りサービスが考えられる．既存の子供の見守りサービスとして，子供の位置を GPS で通知するサービスや，子供が鉄道駅の自動改札を通過した際に親に通知するサービスなどがある．しかし，これらのサー

ビスでは子供の位置は分かるが，親が子供の様子をリアルタイムに確認することは難しい．たとえば，子供の位置近辺で事故が起こった場合，子供が事故に巻き込まれているのか，見物しているだけなのか判断できない．また，子供が通学路でいじめを受けていたとしても，親はそれを知ることができない．それに対して，駅または通学路に設置された監視カメラを用いて子供を見守る場合，子供の様子がリアルタイムに把握でき，親は子供の安否を直接知ることができる．また，いじめに対しては，その映像を保存できれば，いじめの証拠として利用することもできる．

(2) 観光映像サービス

前述したように，監視カメラの性能は日々向上しており，その画質の良さは，その映像に映る個人をはっきり特定できるほどである．また，たとえばディズニーランドのような観光地には多数の監視カメラが設置されている．そこで，監視カメラを用いたサービスの具体例の 2 つ目として，旅行先や観光地で自身や友人，家族が撮影された映像を閲覧するサービスが考えられる．これは，観光地であれば，監視カメラを防犯目的に利用する以外に，鮮明な映像を観光の記念としても利用できるようにするものである．すなわち，監視カメラによる撮影は，犯罪などが起こらない平常時では経費がかかるだけであるが，平常時の監視カメラ映像を来訪者への記念として提供できれば，犯罪発生時以外にも有効利用でき，経費を回収できる可能性が出る．さらに，防犯カメラはつねに稼動しており，一般の人が撮影できない角度から撮影している場合が多い．よって，観光客は旅行先で個人のカメラで撮影する以外に，自分が撮影できないアングルや撮影していなかったタイミングでも鮮明な映像（静止画）や動画を得ることができるようになる．

(3) 個人映像サービス

3 つ目のアプリケーションとして，通学・通勤路などを含め，街中で自身が映った映像を自らの日常の記録として利用するサービスが考えられる．これに似た既存の手法として街中では Google ストリートビューがあるが，これは風景の静止画を利用するためのものであり，自身が映っていても映像を管理することはできない．このサービスを利用するユーザは，自分が立ち寄った場所にある監視カメラから自身の映像を集め，閲覧・管理する．このサービスを利用して自らのプライバシが守られるならば，ユーザは前述の繁華街の人流把握による防災システム，自動飲料販売機における顧客情報の収集システムなどに映像を提供することもできる（詳細は 5 章で述べる）．

3.2 小林方式の概要

まず，小林方式を用いた監視カメラによるプライバシ保護システムを**図 1** の概要図とともに説明する．

小林方式では，被撮影者を 2 つに分類する．1 つは認証局に登録して匿名署名を生成するための鍵を有し，顔など

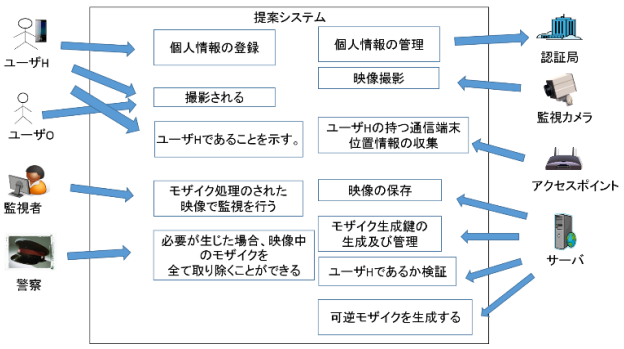

図 1 小林方式の概要図
Fig. 1 Overview of Kobayashi scheme.

のプライバシ情報の秘匿を望むユーザ H であり，もう 1 つは自らのプライバシ情報の保護に関心がなく，鍵を持たないユーザ O である．ユーザ H は監視カメラ（直接的にはアクセスポイント）と通信するための端末を携帯しており，端末内に匿名署名を生成する署名鍵を内蔵させているとする．また，監視カメラはその端末を持つ人物を特定することができるとする．また，認証局は匿名署名を検証するための鍵を公開し，監視カメラはその検証鍵を内蔵しているとする．

ユーザ H は自身がプライバシ保護を望む登録者であることを，匿名署名を生成して端末から監視カメラに送信し，監視カメラがその署名を確認する．監視カメラはその署名を基にモザイクを生成・解除できる鍵を生成し，その鍵を用いてユーザ H の映像にモザイクをかけ，サーバに送る．監視者が見るモニタなどはサーバと接続されており，モニタには顔がモザイクによって秘匿された映像が映され，その映像がサーバに保存される．ただし，ユーザ H が万引きなどの不正を行った場合，警察などの正式な手続きにより，認証局によって匿名署名から本人が特定される．また，認証局はそのユーザの署名からモザイク鍵を生成し，そのユーザの顔のモザイクを解除できる．一方，ユーザ O の顔は秘匿されずそのままモニタに映し出され，通常の監視が行われる．

ただし，小林方式は防犯のための内部監視を想定しているため，被撮影者の様子を観察できるように服装や動作を含む体全体の秘匿は行っておらず，その映像を外部公開することは想定していない．よって，映像を外部公開した場合，被撮影者の服装や動作の特徴を知る者によって，被撮影者を特定される可能性がある．すなわち，小林方式は防犯のみを対象として，ユーザ H の最小限のプライバシを保護する仕組みであるといえる．

3.3 小林方式の問題点

本節では，3.1 節に示した各サービスに小林方式を含む関連研究を適用した際に発生する問題点をあげていく．ただし，問題 1〜3 は全サービスに共通の問題点であり，問

題点 4，5 はその問題点が解決されたとした後に発生するサービス独自の問題点である．

・問題 1：内部監視と外部公開の両立

小林方式では，映像が外部公開されることは想定していないので，モザイクはユーザ H の顔部分のみであった．しかし，3.1 節に示す 3 つのサービスを実現するためには監視カメラ映像は外部から閲覧できる必要がある．しかし，映像を外部公開した場合，不特定多数のユーザがその映像を閲覧できるので，あるユーザは服装や動作などから秘匿されているユーザ H を特定できる可能性がある．また，ユーザ O も不特定多数から閲覧されるので，プライバシがまったく守られていないことになる．よって，外部公開する場合には，ユーザ O を含む全被撮影者の体全体を秘匿する必要がある．

しかし，前記 3 つのサービスにおける監視カメラの第 1 の目的は従来どおり防犯のための監視である．よって，全被撮影者をまったく識別できないように秘匿すると，監視カメラとしての機能が失われ，監視者が被撮影者を監視できない．よって，内部監視のための最小限の被撮影者秘匿と外部公開のための被撮影者全体秘匿をどのように両立させるかが問題である．

・問題 2：ユーザ H による秘匿解除

小林方式は防犯のみを目的とするため，犯罪捜査時に警察によるモザイク除去しか想定していない．また，前記関連研究では特定の観察者のみが，監視カメラ映像の全被撮影者（またはレベル別）を復元することができる．それに対して，3.1 節に示す 3 つのサービスでは，複数のユーザ H が自らまたは閲覧が許可された関係者（子供や友人など）などの特定の秘匿映像を復元できる必要がある．逆に，プライバシ保護の観点から，ユーザ H は上記以外の被撮影者を復元できないよう制限することも必要である．よって，多数の観察者に対して，観察者ごとに特定の被撮影者の秘匿映像のみを解除させる，すなわち監視者と被撮影者を 1 対 1 に対応させ，解除できる仕組みが必要になる．よって，ユーザ H およびその関係者がどのように特定の被撮影者のみを秘匿解除できるようにするかが問題である．

・問題 3：ユーザ H による秘匿映像の識別

問題 1 が解決され，外部公開された映像には被撮影者全体が秘匿され，完全に識別できないとする．小林方式は前述のように防犯以外を想定していないため，正当なユーザは自らの映像を識別する必要はなく，それに関する機能を持たない．しかし，外部公開された映像をクラウドなどの外部サーバなどにまとめて公開すると仮定すると，全被撮影者が秘匿処理されているため，どの映像が自分の映像か分からない．よって，すべての被撮影者が完全に秘匿された映像の中から，ユーザ H がどのように自らまたは復元が許可された関係者の秘匿映像を識別できるようにするかが問題である．

・問題 4：子供の見守りサービスに特有の問題

問題 1〜3 が解決され，ユーザ H が秘匿映像の中から指定した被撮影者の映像を識別・復元できたとする．このとき，たとえば子供の見守りサービスにおいて，ストーカのような悪意ある人物が自らの子供を被撮影者とし，自らを親として登録した後，自らと共有する署名鍵が内蔵された端末を登録した子供ではない監視したい人物（監視対象者と呼ぶ）に渡したとする．すると，その監視対象者は知らないうちに，街中の監視カメラで撮影された秘匿映像から自らを識別・復元され，その人物から容易に監視されるようになる．被撮影者が知らない間に監視される可能性があることは大きな問題である．よって，この例のような悪意あるユーザによる不正を防止できる仕組みが必要である．

・問題 5：観光映像サービスに特有の問題

3.1 節にあげた旅行先や観光地での映像利用において，たとえば，ユーザ H が友人と旅行に行き，旅行地で観光映像サービスを利用すると仮定する．その際，ユーザ H は友人などとともに映った映像の中で自らの顔は復元できる．しかし，ユーザ H が映像復元の権利を持たない一緒に旅行した友人などの顔も一緒に復元したいという場合に対応できない．問題 4 を解決するために，ユーザ H がモザイクで保護された他の被撮影者の顔を復元することを難しくできたとすると，このような場合への対応はいっそう難しくなる．よって，上記 3 つのサービスをその特徴に応じてどのように安全に実現するかが問題である．

4. 提案方式

4.1 ISO/IEC29100

提案システムを構成するにあたり，ISO/IEC29100 というプライバシの国際標準規格を導入する（以下，プライバシフレームワークと呼称する）．ISO/IEC29100 は，プライバシ保護のためのフレームワークの国際標準規格であり，プライバシ 11 原則などを定義している [14]．本フレームワークを導入する理由は，本システムがユーザの個人情報にあたる顔情報を扱うため，個人情報保護法の観点から問題がないことを 5 章で示すためである．

後述するシステムの構成要素と ISO/IEC29100 に規定するプライバシフレームワークの主体の対応表を**表 1** に示す．ただし，PII は個人情報（personally identifiable information）を意味する．

4.2 システム構成要素

提案方式の構成要素の相関図を**図 2** に示す．図 2 において実線で結ばれているのは後述の 4.4.3 項の映像撮影・第 1 段階の秘匿時に主に稼働する構成要素であり，点線で結ばれているのは 4.4.4〜4.4.6 項で主にクラウドとやりとりをする構成要素である．一点鎖線で結ばれているのは主に登録時および犯罪発生時に関する構成要素を表す．

表 1 プライバシフレームワークにおける役割
Table 1 Role in the privacy framework.

名称	概要	システム構成要素との対応
PII 主体	個人情報(PII)の持ち主	被撮影者 (ユーザ H、F、O)
PII 管理者	PII 本人の意思を確認・管理し、PII を処理するための目的・手段を決定	情報管理サーバ
PII 処理者	PII 管理者の指示に従い、PII を処理	カメラ管理サーバ
第三者	本人が同意している条件のもと、PII を提供される	ユーザ P、警察

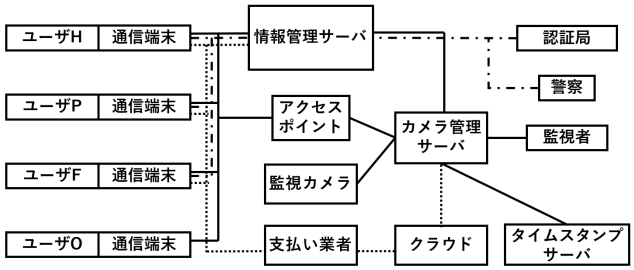

図 2 提案方式のシステム構成要素
Fig. 2 System components of the proposed method.

・ユーザ H（PII 主体）
提案システムに登録して自分の顔の秘匿を望む被撮影者である．プライバシフレームワークでいうと，個人情報（顔情報）の持ち主であるため，PII 主体にあたる．
・ユーザ P（第三者）
ユーザ H と親族関係などを持ち，ユーザ H の秘匿映像の復元を行えるユーザである．プライバシフレームワークでいうと，本人の同意を得て映像を利用する人物であるため，第三者にあたる．
・ユーザ F（PII 主体）
システムに登録しているユーザ H の 1 人であるが，前記ユーザ H と友人関係を持ち，区別するためユーザ F とする．プライバシフレームワークでいうと，顔情報の持ち主であるため，PII 主体にあたる．
・ユーザ O（PII 主体）
システムに登録していないユーザ，またはシステムに登録しているが通信端末などにおけるユーザ H としての機能をオフにするなどしてシステムにユーザ H と認識されないユーザである．プライバシフレームワークでいうと，顔情報の持ち主であるため，PII 主体にあたる．
・情報管理サーバ（PII 管理者）
システムを運営する主体であり，監視者である監視カメラオーナと契約を行う．また，登録したユーザの個人情報を安全に管理する．さらに，犯罪捜査時に警察からの要請によって秘匿化を解除できる鍵を渡し，特定されたユーザがユーザ H である場合はその個人情報を警察に提供する．プライバシフレームワークでいうと，顔情報の処理に関して決定する機関であるため，PII 管理者にあたる．
・カメラ管理サーバ（PII 処理者）
監視カメラの管理をする．プライバシフレームワークでいうと，顔情報の処理を直接行う端末であるため，PII 処理者にあたる．耐タンパ性を持つ．
・警察（第三者）
犯罪捜査時に捜査令状などの正式な手続きを踏み，監視カメラの映像を復元できる．プライバシフレームワークでいうと，復元された映像および個人情報が提供される存在であるため，第三者にあたる．
・通信端末
後述する会員専用アプリや一般アプリなどが搭載された PII 主体が用いるツールである．ただし，設定された署名鍵などの表示・変更は，必ず情報管理サーバに接続して本人確認をした場合のみ可能である．
・監視カメラ
被撮影者を撮影し，システム内に設置されているサーバに送信する．耐タンパ性を持つ．PII 処理者のツールである．
・アクセスポイント
監視カメラの設置されている設備内に設置される．PII 主体であるユーザ H の通信端末と PII 処理者のツールである監視カメラ間で通信を行う PII 処理者のツールである．
・クラウド
カメラ管理サーバから送られた秘匿映像を保存・公開する．秘匿映像へのアクセスは登録している正当なユーザのみ許可し，支払い業者からの対価によって，指定された秘匿映像を送信する．基本的に不正は行わないが，ハッキングや内部犯罪者などにより映像が流出する場合が存在する．個人情報の閲覧・管理は行わない．PII 管理者のツールである．
・監視者
監視カメラシステムを所有する監視カメラオーナを含め，監視カメラ映像の監視を行う者である，モニタ映像の盗撮など不正を行う可能性があるが，映像秘匿によって PII（顔情報）を直接閲覧することはできないため，プライバシフレームワークの構成要素には含まれない．
・認証局
ユーザに署名鍵を配布する．また，システムの要請により署名の認証を行い，その結果をシステムに返す．署名に関する業務のみを行うため，プライバシフレームワークの構成要素には含まれない．
・タイムスタンプサーバ
信頼できるタイムスタンプ情報を定められた間隔で提供する．プライバシフレームワークの構成要素には含まれない．
・支払い業者
ユーザから支払いを受け，クラウドからのデータを仲介

することによって，映像を購入したユーザがだれかをクラウドに秘匿する役目を持つ．また，だれが何を買ったかという情報を安全に管理する．すべての手続きが終了したら，ユーザの口座から料金引き落としを行う．プライバシフレームワークの構成要素には含まれない．

4.3 提案方式で用いられるキー技術

以下に，4.4 節では短く説明されるが，提案方式において用いられる種々の技術を説明する．

(1) グループ署名

前述のシステムの構成要素において，監視者，クラウドなどは必ずしも信頼できるとしないので，ユーザを特定できる署名方式を用いることは望ましくない．そこで，グループに所属したユーザであることは特定できるが個人は特定できない署名であるグループ署名を用いる．

グループ署名とは，匿名署名技術の 1 つである．この方式は，検証者は署名者がどのグループに属しているかを特定できるが，署名者がだれかは特定できない署名方式である．ただし，特別な権限を持つ者は署名者を特定でき，署名者が不正を行った場合などにおいてその署名者を特定する．提案方式では，認証局にその権限を持たせる．グループ署名の例として，Short Group Signatures [15] があり，2004 年に Boneh らによって提案された．

(2) モザイクの段階化手法

小林方式では内部監視のための第 1 段階の秘匿を，参考文献 [16] による手法によって実現する．参考文献 [16] ではモザイクで秘匿した顔情報を圧縮して暗号化し，電子透かしを用いてその画像に埋め込む．顔情報の暗号化と復号は鍵を用いて行われる．これによって，監視者は被撮影者の動作などから万引きなどが行われていることを知ることができ，服装などの顔以外の特徴によって犯人を特定できる．

提案方式では電子透かしは用いず，第 1 段階の秘匿において圧縮され暗号化された顔情報は監視カメラ映像とともにクラウドに送られ保存される．暗号化された顔情報は監視カメラ映像とともに保存しても鍵がなければ復号できない．また，提案方式では映像を外部公開する際はユーザ H または O にかかわらず被撮影者の特徴がまったく分からないような第 2 段階の秘匿を行う．この 2 段階目の秘匿を実現するため，参考文献 [8] または [17] で提案された手法を用いる．たとえば参考文献 [17] では，映像を閲覧する人物と被撮影者の親密度合いによって，被撮影者の秘匿度合いを変更する手法が提案されており，対象とする人物の画像領域を特定し，モザイクや点などに変換することができる．よって，第 1 段階の秘匿と同様に点に変換された画像領域の情報を圧縮して暗号化してクラウドに保存する．よって，2 段階の鍵を知る者だけが監視カメラ映像を復元できる．以上によって，鍵を用いた 2 段階の映像秘匿が可能になる．

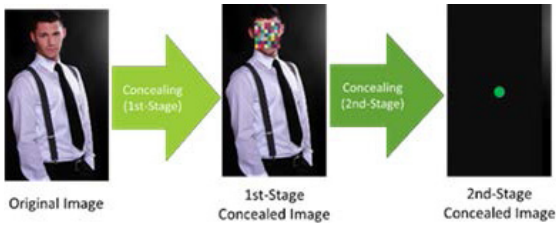

図 3 秘匿の段階化
Fig. 3 2-stage concealment of images.

図 4 画像へのタグ付け
Fig. 4 Tagging images.

(3) タグ付け手法

提案方式では匿名署名やパスワードなどを秘匿化した映像にタグ付けするが，そのタグ付け法としては地図アプリなどに用いられる下記図のようなものを用いることができる．これは地図という画像情報に対して，指定された位置の座標に目印（マーカ）を立て，その色などを変えることができる．よって，点として示されたユーザにこのマーカを立て，同一グループと識別されたユーザには他と異なる同一色を設定することでマーキングが可能になる．また，マーカをクリックすることによって，様々なメタ情報を表示することができ，たとえばお店のホームページなどの指定した URL に移動するなどもできる．よって，クリックによって匿名署名やパスワードなどを表示またはそれに加えて暗号化した顔情報や画像領域なども保存する URL などに移動させれば提案方式に適したタグ付けが実現できる．

4.4 提案方式のプロトコル

提案方式における具体的なプロトコルを示す．ただし，ユーザの通信端末，アクセスポイント，カメラ管理サーバ間，および情報管理サーバ，認証局，警察，タイムスタンプサーバ，クラウド間で生じる通信については暗号通信などにより安全に行われるとする．以下において，上記の暗号通信は明示しないが，プロトコル中で上記通信以外に暗号化が必要な場合，鍵 k を用いて m を共通鍵暗号化することを $Enc_k m$ で表す．

以下に，具体的なプロトコルを示す．

4.4.1 被撮影者登録

ユーザ H となることを望むユーザの登録処理について説明する．ユーザ H についての登録処理を Step1〜3 に示し，ユーザ H と特定の関係にあるユーザ P についての登録処理を追加処理として Step4 に示す．ユーザ F の登録処理はユーザ H と同じである．ただし，認証局および情報管理サーバは自らの署名鍵と検証鍵を持ち，安全に管理しているとする．

・STEP1

ユーザ H は情報管理サーバに自らの個人情報を登録して本人であることを証明する．証明方法については，ユーザ H が本人確認書類の提出を情報管理サーバに対して行うことで証明する．この際，個人情報の取扱いに関する規約が示され，ユーザ H が同意することで登録が行われる．詳細は 5 章の個人情報保護法への対応の節で述べる．

・STEP2

情報管理サーバは個人情報を確認すると，ユーザに対して認証 ID（cID）を与え，認証局に cID に対する署名鍵発行の申請を行う．認証局は署名鍵 gsk を発行し情報管理サーバに送信する．情報管理サーバは，本提案方式を実装した会員専用アプリをユーザ H の通信端末に設定し，ユーザ H に署名鍵 gsk とモザイク鍵 $mk1$ を与える（アプリには会員専用アプリとだれでも利用できる一般アプリがあるとする）．会員専用アプリは後述するユーザ H に関する署名や鍵生成などが行える機能を持つ．以降，ユーザ H のアプリとはユーザ H の通信端末中の会員専用アプリを指し，ユーザ H と区別する．また，認証局は検証鍵 gpk を公開する．認証局および情報管理サーバは秘密鍵 guk と含めてすべてのユーザが持つ鍵を安全に管理する．ここで，署名鍵 gsk はユーザが署名を生成するための鍵，検証鍵 gpk はユーザの署名を検証するための鍵，秘密鍵 guk は認証局が管理する署名者を特定するための鍵である．また，認証 ID は，情報管理サーバが生成する署名がついたユーザ固有の ID であり，モザイク鍵 $mk1$ は映像の秘匿・解除に用いる鍵を生成するための鍵である．

・STEP3

情報管理サーバはユーザ H のアプリに暗号化に用いる鍵 $fk1$ と $fk2$ を定め，設定する．

・STEP4

子供の見守りサービスの場合，ユーザ P はユーザ H から個人情報復元について同意されていることを情報管理サーバに示し，署名鍵 gsk，認証 ID（cID）とモザイク鍵 $mk1$ および $fk1$ を得る．ただし，ユーザ P に $fk2$ は設定されない．

・STEP5

ユーザ H またはユーザ P は cID を用いて匿名でクラウドに登録する．その際，パスワードと利用する支払い機関をあわせて登録する．

4.4.2 監視カメラ登録

システムに参加することを望む監視者に関する設定について説明する．この過程は全サービスで共通である．

・STEP1

監視者は，自身の監視カメラが提案方式を実装しており，第 1 段階の秘匿映像および後述の $mk2$ を安全に管理することを誓約し，情報管理サーバと契約し cID を得て，第 2 段階の秘匿映像をカメラ管理サーバからクラウドにアップロードできるようにする．

・STEP2

監視者はユーザ O の秘匿化を行うための鍵 $mk2$ を定め，安全に保存する．

4.4.3 映像撮影・第 1 段階の秘匿化

ここでは，実際にユーザ H となった被撮影者が監視カメラの撮影範囲内に入った際に行うプロトコルを示す．ただし，通信範囲は監視カメラの撮影範囲より広いとし，STEP1〜STEP6 は被撮影者が監視カメラの撮影範囲内に入る前に行われるとする．また，カメラ管理サーバはタイムスタンプサーバと接続されており，タイムスタンプサーバは定められた間隔でタイムスタンプを発信するとする．また，各サービスは通信端末に設定したアプリによって選択できる．観光映像サービスを選択した場合，pw はユーザ H，F，O で構成された友人グループ内で事前に共有されているものとする．また，ユーザ O はだれでも利用できる一般アプリをダウンロードしており，アクセスポイントとの暗号通信や後述のユーザ O に関する鍵生成などができるとする．よって，ユーザ F のアプリおよびユーザ O のアプリも通信端末中のアプリを指す．

・STEP1

サーバは，アクセスポイントを介して，自身の ID 情報（ID_{server}）とタイムスタンプ情報 T_s を，T_s 受信ごとに監視カメラの撮影範囲より広い範囲にブロードキャストする．

・STEP2

アクセスポイントからの信号を受信したユーザ H のアプリは，$fk1$ を用いて以下のメッセージ M を生成する（T_s が同じでも eTs は $fk1$ によってユーザごとに異なる）．なお，式 (2) は M が括弧内を 1 方向性のハッシュ化したものであることを示している．ただし，観光映像サービスの場合ユーザ H のアプリは T_s を pw で暗号化してユーザ F，O のアプリに送る（ユーザ F のアプリも同様の処理を行い，最も早い時刻の T_s が以降用いられる）．

$$eTs = Enc_{fk1}T_s \tag{1}$$

$$M = H(cID \,\|\, ID_{server} \,\|\, eTs) \tag{2}$$

・STEP3

ユーザ H のアプリは Short Group Signature [15] の署名生成手順に従い，自らの署名鍵 gsk を用いてメッセージ M

に対する匿名署名 σ_H を生成する．

・STEP4

ユーザ H のアプリは秘匿処理を行うための鍵 ek_{H1}（第 1 段階）と鍵 ek_{H2}（第 2 段階）を以下のように生成する．ただし，鍵 $Mk1$ はサービスによって異なる．子供の見守りサービスが選択されている場合 $Mk1 = mk1 + pw$（+ は XOR），観光映像サービスが選択されている場合 $Mk1 = pw$，個人映像サービスでは $Mk1 = mk1$ である．

$$ek_{H1} = Enc_{Mk1}H(T_s) \tag{3}$$

$$ek_{H2} = Enc_{Mk1}H(ek_{H1}) \tag{4}$$

・STEP5

ユーザ H のアプリは $(\sigma_H,\ M,\ ek_{H1},\ ek_{H2})$ をアクセスポイントを介してカメラ管理サーバに送信する．

・STEP6

カメラ管理サーバはユーザ H のアプリから情報を受け取り，認証局が公開する検証鍵を用いて検証を行う．ただし，再送攻撃を避けるため，同じ署名については 1 度のみ検証する．

・STEP7

カメラ管理サーバは，署名が正当なら，監視カメラ映像中のユーザ H を特定する．ユーザ H の特定法は規定しないが，たとえばユーザ H のアプリが顔認識のためのユーザ H の顔の特徴情報を $(\sigma_H,\ M,\ ek_{H1},\ ek_{H2})$ と一緒に送り，監視カメラサーバはその特徴情報を用いて顔認識し，ユーザ H を特定することができる．または，アクセスポイントが通信端末からの電波の方向や強さから端末を特定することによってその持ち主であるユーザ H を特定することもできる．また，GPS などを使って端末を特定させることもできる．通信端末の不正利用については参考文献 [9] で対策されているため，端末が特定できれば問題ない．

・STEP8

ユーザ O も STEP7 で述べた方法によって端末から特定できる．また，観光映像サービスにおいて，ユーザ H，F，O が pw を事前に共有している場合，ユーザ O のアプリは以下の ek_{O1}，ek_{O2} を生成し，カメラ管理サーバに送信する（ユーザ H，F のアプリは ek_{O1}，ek_{O2} と同じ ek_{H1}，ek_{H2} を STEP5 で送信している）．ユーザ H，F のアプリは，$fk2$ で暗号化した epw をアクセスポイントを介してカメラ管理サーバに送信する．これは，ユーザ H，F がパスワードを忘れた際や警察が捜査をする際，復号して利用するためのものである．

$$epw = Enc_{fk2}H(pw) \tag{5}$$

$$ek_{O1} = Enc_{pw}H(T_s) \tag{6}$$

$$ek_{O2} = Enc_{pw}H(ek_{O1}) \tag{7}$$

・STEP9

カメラ管理サーバは ek_{O1}，ek_{O2} を確認し，ユーザ O のアプリからの ek_{O1}，ek_{O2} とユーザ H，F のアプリからの ek_{H1}，ek_{H2} が同じであればその送信者をマーキングする．たとえば，ユーザ H，F，O からなる 3 人組が同一のグループ A に属しているとする場合，そのユーザ H，F，O はそれぞれユーザ H_A，F_A，O_A としてマーキングされる．マーキングとはこの段階では同じグループに属するユーザと認識するだけであるが，後述の 4.4.4 項 STEP1 においてそれらのユーザを他と区別できる形でタグ付けすることを意味する．

・STEP10

同一グループにマーキングされた全ユーザは ek_{O1} を用いて秘匿化（第 1 段階）される．マーキングされていないユーザ H，すなわち観光映像サービスを選択せずグループに属すると認識されないユーザ H は STEP4 で生成した ek_{H1} を用いて秘匿化（第 1 段階）が行われる．

・STEP11

カメラ管理サーバはマーキングされていないユーザ O，すなわちグループに属すると認識されない，または元々何の信号も送っていないユーザ O のための秘匿化鍵を $mk2$ を用いて以下のように生成し，ek'_{O1} 用いて，マーキングされていないユーザ O の顔を秘匿化（第 1 段階）した映像 movie1 を生成し，モニタに送る（監視者は movie1 を用いて監視する）．

$$ek'_{O1} = Enc_{mk2}H(T_s) \tag{8}$$

$$ek'_{O2} = Enc_{mk2}H(ek'_{O1}) \tag{9}$$

・STEP12

カメラ管理サーバは監視カメラ映像中のユーザ H に σ_H，ek_{H2}（マーキングされている場合 ek_{O2}），epw をタグ付けし，マーキングされているユーザ O に ek_{O2}，マーキングされていないユーザ O に ek'_{O2} をタグ付けする．さらに，暗号化に使用した T_s をタグ付けした映像 movie1' を生成する．よって上記処理では，T_s は STEP5 で送られた T_s が用いられ，ユーザ H，F，O で共通になる．

4.4.4 第 2 段階の秘匿化

カメラ管理サーバで行われる第 2 段階の秘匿化処理を説明する．

・STEP1

カメラ管理サーバは movie1' 中のマーキングされたユーザ H_A，F_A，O_A を ek_{O2} で，それ以外のユーザ H を ek_{H2} で，マーキングされていないユーザ O を ek'_{O2} で秘匿化し，第 2 段階の秘匿化映像 movie2 を生成する（movie2 では被撮影者は点で表される）．ただし，movie1' にタグ付けされた 2 次秘匿の鍵は削除して movie2 を生成する．

・STEP2

カメラ管理サーバは第 1 段階と第 2 段階で暗号化し秘匿した画像部分に画像内の座標位置などの復元に必要な情報を加えてファイルを構成し，そのファイル番号を匿名

署名などと同様に各ユーザにタグ付けし，そのファイルとmovie2をクラウドに送信し，秘匿のために生成・受信したすべての鍵を削除する．

4.4.5 クラウドによる映像公開および映像検索

クラウドによるmovie2の公開から，登録者が自らの映像を特定するまでの処理を示す．

・STEP1

クラウドはmovie2を監視カメラ（ID_{server}）ごとのフォルダに分類して，システムの登録者に公開する．第1段階と第2段階の秘匿画像は別の領域に格納され，タグによって関連付けられるとする．

・STEP2

登録者（ユーザH，F，P）は会員専用アプリを用いて被撮影者が写っていると想定される監視カメラのフォルダから，写っていると想定されるT_sがタグ付けされた映像を検索し，そのmovie2を特定する（または，すべての映像から後述する再現したσ_Hを用いて検索を行う）．

・STEP3

登録者は会員専用アプリを用いてmovie2にタグ付けされているT_sから4.4.3項のSTEP2，3の処理を行い，σ_Hを再現してmovie2の各点にタグ付けされたσ_Hと比較して一致する点（被撮影者）を特定する．その点を含めたマーキングがある場合，マーキングされている点を復元可能な被撮影者とする．たとえば，ユーザH，F，Oからなる3人組が映る映像があり，それらが同一グループとマーキングされている場合，そのユーザHはそのグループ中のユーザF，Oも復元できる．

・STEP4

ユーザは支払い業者に料金を支払い，所望のmovie2をタイムスタンプ区切りで要求し，支払い業者を介してその映像を得る．

4.4.6 ユーザHまたはユーザPによる映像の復元

ここでは，ユーザが鍵から映像を復元する過程を説明する．なお，pwを知る登録者（ユーザH，F）はユーザOの映像も復元できる．また，ユーザOはシステムに登録していないので，クラウドにアクセスできないがユーザHを介して復元映像を入手できる．

・STEP1

ユーザHとユーザPのアプリは4.4.3項のSTEP4に示す鍵ek_{H1}，ek_{H2}を生成し，ユーザHの映像を復元する．

・STEP2

観光映像サービスの場合，ユーザHのアプリは4.4.3項のSTEP8に示すek_{O1}，ek_{O2}をpwから生成して，マーキングされているユーザF，Oの映像とともに復元する．

4.4.7 警察による秘匿化解除

警察が事件捜査時に監視カメラ映像からの秘匿化映像を解除するためのプロトコルを示す．

・STEP1

警察は捜査令状などの正規手続きを行い，捜査令状などをクラウドに示し，捜査現場の近くにある監視カメラなどを特定する．

・STEP2

警察は監視者に令状を示して，所望の時間帯の監視カメラ映像movie1'を入手する．

・STEP3

警察は情報管理サーバに令状を示し，movie1'を送信し，不正を行ったユーザHの映る元映像の復元を求める．また，捜査のため，不正ユーザHの個人情報の開示を求める．

・STEP4

情報管理サーバは認証局に申請し，認証局はmovie1'にタグ付けされた署名を認証局の秘密鍵gukで検証することによって不正ユーザHのcIDを特定する．さらに，情報管理サーバはcIDから特定される不正ユーザHのモザイク鍵と映像に紐付けられたepwを復号することによってパスワードを得て，不正ユーザHの秘匿映像を復元する．得られた映像は不正ユーザHの個人情報とともに警察に送信する．

5. リスク評価

本章では，提案方式を3.1節のサービスに用いた場合のリスク評価を行う．本論文は暗号技術を監視カメラシステムに適用することによって，映像を公開してもプライバシ情報が漏洩しない仕組みを提案するものである．提案システムでは監視者はモニタの盗撮や秘匿映像の復元，クラウドは秘匿映像や個人情報の漏洩，各ユーザは自分に許可された以外の映像の閲覧といった不正行為を働く（攻撃者になる）可能性があるとする．それに対して，認証局，警察，支払い業者，タイムスタンプサーバ，カメラ管理サーバ，情報管理サーバは信頼でき不正は行わないとする．一般に暗号技術や暗号システムの安全性評価においては信頼できるとするものを仮定し，攻撃者からの攻撃をその安全性を根拠に防止できるかが議論される．よって，信頼できるとしたものの安全性について検討する必要がある．本システムにおいて信頼できるとするものは社会通念上安全と思われている組織やシステムを前提としている．たとえば，公開鍵暗号において認証局が信頼できないとする場合，PKIは破綻すると考えられるため，認証局は信頼できるという仮定は妥当と考えられる．また，支払い業者とはクレジット会社を想定しており，手数料による業務の一環としてクラウドとユーザ間の仲介を行うとする．クレジット会社は信頼でき，不正はしないとするのは社会通念上妥当と考える．また，警察やタイムスタンプサーバも不正をするという前提では社会や種々の仕組みが破綻すると考えられ，信頼できるとするのは妥当と考える．また，カメラ管理サーバはISO/IEC15408などによるセキュリティ製品評価を受

けていることを義務とすれば，本提案の機能を安全に実行し，秘匿前の監視カメラ映像の漏洩などは起こらないと保証される．最後に，情報管理サーバはこのシステムの責任者であり，このシステムがうまく動かなければ損害賠償など最も被害を受ける．よって，情報管理サーバは不正をせず信頼できるとする．ただし，近年ニュースにあるように情報管理サーバを運営する組織や個人などが初めから詐欺目的でユーザを集め，契約金などを騙し取ろうとする場合が考えられるが，これに対してはこのシステムに限らない社会的課題といえるため，情報管理サーバは不正を行わず信頼できるとする．

5.1 問題点の解決

まず，3.1 節に示した問題点に関して評価を行う．

・問題 1：内部監視と外部公開の両立

4.4.3 項より，提案方式ではカメラ管理サーバで第 1 段階の秘匿を行うが，監視者が見るモニタには movie1 の映像のみが表示されるので，監視者は小林方式と同様の内部監視が可能である．特に，第 1 段階の秘匿はカメラ管理サーバ内で行われ，4.2 節よりカメラ管理サーバは耐タンパ性を持ち，監視者も原映像は入手できない．よってユーザ H が秘匿されていない原映像は流出することなく安全である．

また，4.4.4 項より，クラウドは第 2 段階の秘匿が行われた movie2 を得るが，この映像中の被撮影者はすべて体全体が秘匿されている．正当なユーザ H またはユーザ P 以外の人物はその映像を識別・復元するための鍵を知らないため，不特定多数がその映像を閲覧しても，被撮影者に関する情報はまったく漏洩しない．

また，クラウドとの秘匿映像のやりとりは支払い業者を介して行われる．よって，クラウドには正当な対価が支払われるが，だれが（どの *cID*）がどの秘匿映像を購入したかという情報は得られない．*cID* は個人情報を含まないので，この情報はクラウドに知られてもよいとする場合，支払い業者を構成要素から省くことができる．しかしその場合，ある *cID* がだれかを知る人物がクラウドからこの情報を知れば，その *cID* の購入履歴や購入傾向などの情報がその人物に漏洩することになる．よって，支払い業者を必須の構成要素とすることでこれらの情報の漏洩も防止できる．

よって，内部監視と外部公開が両立できる．

・問題 2：ユーザ H による秘匿解除

ユーザ H の秘匿映像を復元できるのは，4.4.3 項 STEP4 の鍵の生成式より，子供の見守りサービスにおいてはモザイク鍵とパスワードを知るユーザ H とユーザ P だけであり，観光映像サービスにおいてはパスワードを知るユーザ H とユーザ F であり，個人映像サービスにおいてはモザイク鍵を知るユーザ H のみである．一般の閲覧者は匿名署名を知ることはできるが，モザイク鍵とパスワードを知らないため映像を復元できない．よって，モザイク鍵とパスワードを知る正当なユーザのみが秘匿された映像を復元できる．

加えて，犯罪捜査時には警察による秘匿映像復元が実行できなければならないが，他に情報を漏洩させてはならない．すなわち，4.4.7 項 STEP4 により認証局は自身が持つ *guk* を用いて *cID* を特定するが，4.4.1 項 STEP2 より認証局は *cID* の個人情報を持たず秘匿映像も復元しない．よって，認証局には不正ユーザ H に関する個人情報は漏洩せず，情報管理サーバのみが不正ユーザ H の秘匿映像を復元し，その個人情報を特定して警察に提供できるシステムとなっている．

以上の手順より，犯罪が発生しない状況では正当なユーザ H のみが権利を持つ秘匿映像を復元でき，犯罪発生時には他に情報を漏洩することなく警察の捜査に対応できるシステムになっている．

・問題 3：ユーザ H による秘匿映像の識別

秘匿映像の識別には匿名署名が用いられる．4.4.1 項 STEP2 より，正当なユーザ H，F，P は署名鍵を知るため，その時刻の秘匿映像から自らの匿名署名を再現できる．よって，4.4.5 項 STEP3 でその再現した匿名署名と映像に紐付けられた匿名署名を比較することによって，秘匿映像を識別できる．

一方，一般の閲覧者は署名鍵を知らないため匿名署名から被撮影者を識別できない．また，4.4.3 項 STEP2，STEP3 より，タイムスタンプ情報を用いてメッセージを作り，そのメッセージから署名を生成する．よって，同じ署名鍵を用いても，時刻や場所が異なれば匿名署名も変化する．よって，匿名署名を多数観察しても異なる映像中の被撮影者を同一人物であると識別することもできない．

よって，秘匿映像中の被撮影者を識別できるのは，署名鍵を知る正当なユーザ H，F，P のみである．

・問題 4：子供の見守りサービスに特有の問題

問題点 1〜3 が解決されたことにより，正当なユーザのみが秘匿映像を識別・復元できる．しかし，子供の見守りサービスにおいては，ストーカのような悪意ある人物が正当に登録手続きをし，署名鍵などが入った端末を監視対象者に持たせた場合，そのストーカは監視対象者を監視できる．以降，この悪意あるストーカのようなユーザをユーザ X，被害に遭う監視対象者をユーザ Y と呼称する．

4.4.3 項 STEP4 の鍵の生成式より，子供の見守りサービスにおいてモザイク鍵は $mk1 + pw$ となる．よって，ユーザ H とユーザ P の間で *pw* があらかじめ共有される必要がある．よって，子供の見守りサービスを選択した場合，サービス開始時における *pw* 更新を必須の処理とする．さらに，一定期間ごとに *pw* の更新が要求され，*pw* 更新がなければユーザ P はユーザ H の秘匿映像を解除できなくなるようにする．これによってユーザ X はユーザ Y との正当なつながりを持たないため，*pw* 更新ができない．すな

わち，ユーザXによって監視対象者であるユーザYが騙されて端末を持たされたとしても，ユーザYがpwを一定期間ごとに更新しない，または更新してもそれをユーザXに教えなければ，ユーザXは映像を復元できない．

また，4.4.3項STEP5より，ユーザHはpwを忘れたとき，または警察が映像を復元できるようにするために，pwを$fk2$によって暗号化し，epwとして映像に紐付けする．しかし，ユーザXは$fk2$を知らないため，タグ付けされたepwからpwを知ることはできない．

また，他人がユーザHの通信端末を盗んでも，通信端末は設定された鍵情報を情報管理サーバによる本人確認なしには表示しないので，本人以外に通信端末が渡っても問題ない．また，通信端末に設定されるアプリは4.4節で述べた以外の機能は実行できず，カメラ管理サーバとの暗号通信のための鍵はユーザにも公開されることなく，情報管理サーバによってカメラ管理サーバと通信端末のアプリで同期して更新されるとする．これによって，アプリの機能を偽造しても通信できない．

以上より，ユーザXによるユーザYの監視を防ぐことができる．

・問題5：観光映像サービスに特有の問題

前提として，提案方式を利用するとき，どのサービスを利用するか選択できるようにする．4.4.3項STEP4の鍵の生成式より，子供の見守りサービスを選択するとモザイク鍵として$mk1 + pw$が選択され，観光映像サービスを選択するとpwが選択され，個人映像サービスを選択すると$mk1$が選択されるようになっている．

ただし，観光映像サービスは他のサービスに比べて安全性が低くなる可能性がある．たとえば，ユーザHを含む友人達（グループと呼ぶ）が旅行先で観光映像サービスを利用すると仮定する．まず，グループ内でその場でpwを定め，共有する．このとき，グループ以外の悪意あるユーザHがたまたまそのグループの近くにいてpwを盗み聞きしたとする．公開された映像の時刻や場所の情報などからマーキングされた被撮影者達をそのメンバと推定できた場合，その秘匿映像は復元される可能性がある．ただし，観光映像サービスは個人が自らの映像を秘密に管理するためというよりも，多くの人達と映像を共有することを目的とするため，pwが漏洩しても問題ない場合が多いと考えられる．これを防ぐためにはpwを他に知られることのないように注意して共有すればよい．

一方，子供の見守りサービスでは，4.4.3項STEP4の鍵の生成式より，秘匿映像の復元に$mk1$とpwが必要であるので，同じ時刻や場所にいた人から秘匿映像を推測され，たまたまpwも知られたとしても，その人は$mk1$を知らないため秘匿映像を復元できない．個人映像サービスも同様に$mk1$が知られなければ安全である．

以上により，提案方式は3つのサービスに対応できる．

5.2 個人情報保護法への対応（参考文献：[18]）

提案方式は，顔情報という個人情報を制御してプライバシを保護する手法であるため，個人情報保護法（以下，保護法）への適応が不可欠である．ここでは，保護法の主たる取り決めに対して，提案方式がそれらを遵守していることを示す．

(1) 個人情報の利用目的

まず，保護法には，「保有個人情報管理者は，個人情報を取り扱うにあたって，利用目的をできる限り特定しなければならない（個人情報保護法第15条第1項）」とある．さらに，「特定した利用目的は，あらかじめ公表しておくか，個人情報を取得する際に本人に通知する必要があり，取得した個人情報は，特定した利用目的の範囲内で利用する必要がある」とある．この場合の保有個人情報管理者とは4.1節に示したISO/IEC29100のプライバシの国際標準規格（以下，プライバシフレーム）でいうとPII管理者にあたる．よって，以下の対策については基本的に情報管理サーバが行う．

本条文に対しては，ユーザがシステムへの登録時に3つのサービスについて詳細な説明を受け，各サービスの利用目的が明示されたうえでその利用を選択でき，さらに，そのサービスを使ううえでの顔情報や登録個人情報の取扱いについて明記した会員規約を明示することで対策する．

(2) 個人情報の安全な管理

次に，「保有個人情報管理者は，個人データの安全管理のために必要かつ適切な措置を講じなければならない」とある．この条文に対しては，適切に2段階秘匿を行うことで対策する．また，鍵は各ユーザおよび監視カメラオーナが安全に管理する．以上の前提の下で，個人情報が保護されることは5.1節で述べたので割愛する．

(3) 個人情報提供に関する同意

次に，「保有個人情報管理者は，個人データを第三者に提供する場合，原則としてあらかじめ本人の同意を得なければならない（個人情報保護法第23条第1項）」とある．この条文に対しての対策は，第三者が警察，ユーザP（子供の見守りサービスの場合）であるため，個別に説明する．ユーザPはユーザHの親であり，親は子供を監督する義務があるため，同意はできていると考えられる（子供が嫌がっている場合，ストーカの場合に説明したようにpwを親と共有しなければよい）．警察の場合は捜査令状などに基づくため問題はない．特に，4.4.1項STEP1で顔情報・登録個人情報の取扱いについての規約などを示すとき，秘匿された映像の令状などによる警察への提供を登録時に同意してもらうことで対応する．

(4) 提供の記録

次に，「第三者に個人データを提供した場合，第三者から個人データの提供を受けた場合は，一定事項を記録する必要がある（個人情報保護法第25条，26条）」とある．しか

し，本人との契約に基づく場合，記録は契約書で代替可とある．よって，この条文に対しては前段落で述べた規約の同意をもって対応する．

(5) 個人情報の開示

次に，「保有個人情報管理者は，本人から保有個人データの開示請求を受けたときは，本人に対し，原則として当該保有個人データを開示しなければならない（個人情報保護法第 28 条)」とある．本条文に対して，個人情報を顔情報と登録個人情報に分けて説明する．顔情報の開示要求に関しては，料金を支払うユーザ H による通常の映像利用（個人映像サービスにあたる）が可能である．情報管理サーバに登録した登録個人情報の開示については，情報管理サーバによる本人認証が行われなければ実行されない．よって，正当なユーザは自らの個人情報を開示によって確認でき，正当なユーザでなければ開示されない．

以上より，提案方式は保護法に対応した，ユーザが安心して個人情報を提供できるシステムであるといえる．

5.3 その他の応用への拡張

本論文では，想定した 3 つのアプリケーションへの提案方式の適用について詳細に説明した．しかし，提案方式は上記応用以外にも適用できる．たとえば，2.3 節に示した自治体による繁華街の人流把握による防災システムや自動飲料販売機における顧客情報の収集システムなどにおいて必要な情報は個人の顔情報ではなく，被撮影者の性別や年代などであると考えられる．このような場合，提案方式を少し拡張するだけで被撮影者のプライバシを保護したまま対応可能である．すなわち，被撮影者は性別や年代などの公開可能な情報を通信端末に保存しておき，4.4.3 項 STEP5 で署名情報などを送信する際その情報も一緒に送るようにすればよい．ただし，その情報は暗号化されている必要があるので，たとえば，自治体の人流把握ではその自治体と被撮影者の間でサービス ID とユーザ ID・暗号鍵を共有し，自動飲料販売機の顧客情報収集でもその会社と同様の情報を共有しておく．ただし，サービス ID とは，ある自治体の人流把握サービス，ある会社の顧客管理サービスなどサービスごとの ID であり，ユーザ ID とはそのサービスを提供する組織がユーザごとに定める ID であり，暗号鍵はサービスごとに異なる．よって，4.4.3 項 STEP1 でアクセスポイントから ID_{server} などを送る際にサービス ID も送信し，通信端末は登録したサービスであればそれに応じた情報を暗号化して 4.4.3 項 STEP5 で追加送信すればよい．これによって，被撮影者の体全体を含む個人情報は秘匿されたまま，被撮影者の意思に応じて種々の監視カメラを利用したサービスへ提案方式を適用させることができる．これはユーザ O もアクセスポイントと通信できれば対応可能である．また，ユーザによる各サービスへの登録は自らの意思によって行われるため，まさに「個人が自らの情報を制御する権利」というプライバシの概念を実現するシステムとできる．

6. まとめ

本論文では，監視カメラの新たな応用・展開を考え，監視カメラ本来の機能である監視・犯罪防止に加え，監視カメラを利用したいくつかのアプリケーション・サービスを検討し，それを安全に実現するために必要な具体的プロトコル（提案方式）を示した．また，関連研究との比較により，内部監視と外部公開を想定した監視カメラシステムは著者らの知る限り，本論文が最初の提案であると考える．

また，今回は提案方式の安全性を理論的に示したが，実装はその安全性が確認されてから行う必要がある．本論文では提案方式を新しいアプリケーション・サービスに用いたときのリスク評価を個人情報保護法の下に示した．以上によって，本研究を用いれば監視カメラを監視以外の目的で利用して映像を公開しても被撮影者のプライバシはシステム側からは漏洩せず，被撮影者自身が自らの映像を自らの意思に従い管理できる真の意味でのプライバシ保護が実現できる．

参考文献

[1] 堀部政男：プライバシー保護制の歴史的経緯，法律文化/東京リーガルマインド，Vol.14, pp.18–21 (Nov. 2002).

[2] 福岡直也，伊藤義道，馬場口登：観察者に応じたプライバシー保護映像を生成可能な映像配信手法，*FIT2011*, No.3, pp.97–100 (Sep. 2011).

[3] Zhang, W., Cheung, S.-C.S. and Chen, M.: Hiding privacy information in video surveillance system, *ICIP*, No.3, pp.868–871 (2005).

[4] Senior, A., Pankanti, S., Hampur, A., Brown, L., Tian, Y-l. and Ekin, A.: Blinkering Surveillance: Enabling Video Privacy through Computer Vision, *IEEE Security & Privacy*, Vol.3, pp.50–57 (2005).

[5] Sohn, H., De Neve, W. and Ro, Y.M.: Privacy Protection in Video Surveillance Systems: Analysis of Subband-Adaptive Scrambling in JPEG XR, *IEEE Trans. Circuits and Systems for Video Technology*, Vol.21, pp.170–177 (2011).

[6] Carrillo, P., Kalva, H. and Magliveras, S.: Compression independent object encryption for ensuring privacy in video surveillance, *Multimedia and Expo, 2008 IEEE International* (2008).

[7] Montreux, D.F. and Ebrahimi, T.: Scrambling for Privacy Protection in Video Surveillance Systems, *IEEE Trans. Circuits and Systems for Video Technology*, Vol.18, pp.1168–1174 (2008).

[8] Chen, D., Chang, Y., Yan, R. and Yang, J.: Tools for protecting the privacy of specific individuals in video, *EURASIP Journal on Applied Signal Processing*, Vol.2007 (2007).

[9] 小林健人，稲村勝樹，金田北洋，岩村恵市：プライバシー保護と犯罪防止を両立する監視カメラシステム，情報処理学会特集論文誌，Vol.57, No.1, pp.172–183 (2016).

[10] 白石敬典，中原道智，浦田有佳里，下村憲輔，田　娟，慎　祥揆，瀬戸洋一：ネットワーク対応監視カメラの設置・運用ガイドラインの課題分析とその対策，*SCIS 2017*

(2017).
[11] Biggs, J.: 世界中の無防備な Web カメラを見せる Insecam …パスワードに無関心なアドミンが多い (Oct. 2014)，入手先 ⟨https://jp.techcrunch.com/2014/11/08/20141107insecam-displays-insecure-webcams-from-around-the-world/⟩.
[12] BIGLOBE ニュース (Aug. 2012)，入手先 ⟨http://news.biglobe.ne.jp/entertainment/0816/jc_120816_9807318879.html⟩.
[13] 瀬戸洋一：ネットワーク型多目的カメラシステムにおけるプライバシー課題とその対策，危機管理産業展（RISCON TOKYO）2016 (Oct. 2016).
[14] ISO/IEC 29100 Information technology – Security techniques – Privacy framework.
[15] Boneh, D., Boyen, X. and Shacham, H.: Short Group Signatures, *CRYPTO 2004* (2004).
[16] Kusama, Y., Kang, H. and Iwamura, K.: Mosaic-based Privacy-protection with Reversible Watermarking, *The 12th International Conference on Signal Processing and Multimedia Applications* (*SIGMAP2015*), pp.98–103, SciTePress (July 2015).
[17] 知野見健太，李　光鎮，中嶋大介，新田直子，伊藤義道，馬場口登：PriSurv：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，情報処理学会論文誌コンピュータビジョンとイメージメディア，Vol.1, No.2, pp.152–162 (July 2008).
[18] 個人情報保護法ハンドブック (June 2017)，個人情報保護委員会，入手先 ⟨https://www.ppc.go.jp/files/pdf/kojinjouhou_handbook.pdf⟩.
[19] 内海ゆづ子，坂野悠司，前川啓介，岩村雅一，黄瀬浩一：局所特徴量と近似最近傍探索を用いた大規模データベースに対する高速顔認識，情報処理学会研究報告，Vol.2013-CVIM186, No.4 (2013).
[20] 角田良明：子ども向け見守りシステムのしくみ，通信ソサイエティマガジン，電子情報通信学会，No.23, pp.172–173 (2012).
[21] カメラ画像利活用ガイドブック Ver1.0，IoT 推進コンソーシアム・総務省・経済産業省 (2017).
[22] カメラ画像利活用ガイドブック Ver2.0，IoT 推進コンソーシアム・総務省・経済産業省 (2018).
[23] 秦野康生，宮崎邦彦，手塚　悟：個人情報保護を考慮した電子文書公開システム，情報処理学会論文誌，Vol.47, No.3 (2006).

星野 光太

東京理科大学．1994 年生．2017 年 3 月東京理科大学工学部電気工学科卒業．同年東京理科大学大学院工学研究科電気工学専攻修士課程に入学，現在，在学中．主に情報セキュリティ，画像処理，プライバシ保護の研究に従事．

岩村 恵市　（正会員）

1958 年生．1980 年九州大学工学部情報工学科卒業．1982 年同大学大学院情報工学研究科修士課程修了．同年キャノン（株）入社．1994 年東京大学博士（工学）．現在，東京理科大学工学部電気工学科教授．主に符号理論，並列処理，情報セキュリティ，電子透かしの研究に従事．IEEE，電子情報通信学会，電気学会各会員．エンリッチド・マルチメディア（EMM）研究会委員長，情報ハイディング及びその評価基準（IHC）研究会委員長，本会フェロー．

小林 友宏

東京理科大学．1997 年生．2019 年 3 月東京理科大学工学部電気工学科卒業．同年同大学大学院工学研究科電気工学専攻修士課程に入学．主に情報セキュリティ，ディジタル署名の研究に従事．