監視カメラ映像のためのプライバシー保護システムの改良とその応用

星野光太[†1]　岩村惠市[†1]

概要: 映像サーベイランスの普及に伴い, 監視カメラの映像の被撮影者のプライバシーを適切に秘匿するため, privacy protection surveillance camera system (PPSCS)（以下従来方式）が提案された．この手法は，被撮影者の意思を反映させて映像のプライバシーを秘匿することが可能である唯一の手法である．そこで，私たちは従来方式を用いて安全に監視カメラ映像の第三者利用することを考えたが，従来方式は監視カメラをネットワークに繋がずローカルで利用することを前提としており，ネットワークに接続した際の新たな要件に対応していない．そこで，本論文では，監視カメラをネットワークに接続した際の新たな要件に対応した改良方式である Improved PPSCS (IPPSCS)を提案する．本方式の特徴は，従来方式の特徴に加え，映像を内部監視に用いる際と外部公開に用いる際で秘匿の度合いを変更できる点と，従来方式に比べて認証局の負担を軽減し，システムの管理の煩雑さを軽減した点である．また，本方式を用いることによって実現できるアプリケーションの例を 3 つ紹介し，本方式を適用した際の安全性についても示す．

キーワード：映像サーベイランス，プライバシー保護，監視カメラ, 匿名署名

Improvement of Privacy Protection Surveillance Camera System and its Applications

KOTA HOSHINO[†1]　KEIICHI IWAMURA[†1]

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，プライバシーとは「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伴い，監視カメラ映像に関するプライバシー保護の重要性が叫ばれ，監視カメラシステムの映像に映った被撮影者をモザイクなどで秘匿するサービスが広がっている[2]．しかし，このようなサービス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，上記の意味での真のプライバシー保護は実現されていない．

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情報を秘匿する方式 privacy protection surveillance camera system (PPSCS)（以下従来方式）を提案している[3]．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ーを自らの意思によって保護することができる．

しかし、従来方式は監視カメラをネットワークに繋がずローカルで利用することを前提としており，ネットワークに接続した際の新たな要件に対応していない．そこで，本論文では，監視カメラをネットワークに接続した際の新たな要件に対応した改良方式である Improved PPSCS (IPPSCS)（以下提案方式）を提案する．加えて、監視カメラ映像を用いた新しいアプリケーションを 3 つ挙げる。そして、提案方式をアプリケーションに適用した際の問題点などを検討し，その安全性を評価する．これによって監視カメラシステムの新たな応用の可能性を示す．

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する。次に、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ための要件の提起、5 章で提案方式の具体的な説明，6 章では 3 章で挙げたアプリケーションの具体的実現と提案方式のその安全性について考察を行う．

†1, 東京理科大学

2. 従来の監視カメラシステムの問題点

2.1. ネットワークにおける監視カメラ

今までの監視カメラは，撮影映像を DVD などの記録媒体に保存し，必要に応じてそれを取り出して再生するといったように，ネットワークに接続せずローカルで運用するのが一般的であった．近年では、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，クラウド等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がある．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．

通常，監視カメラオーナがネットワーク経由で監視カメラ映像を確認する際は，パスワードを設定することによって第三者の映像閲覧を防いでいるが，日本国内で 6000，世界全体で 28000 の監視カメラが，パスワードが適切に設定されていないことにより，インターネットでいつでも映像閲覧が可能な状態であるという．これは，監視カメラオーナのセキュリティ意識の低さから来ており，映像の被撮影者のプライバシーが侵害されている状況である．

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ー侵害を防ぐ対策として，参考文献[4]のように監視カメラに関する条例・ガイドラインを設定し，監視カメラオーナに対しこれらのガイドライン等を徹底させるという対策がある．ただし，悪意のある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．そこで、我々は従来方式[3]を用いて映像の被撮影者のプライバシーを適切に秘匿することを考える。

3. 監視カメラ映像を利用して新たに考えられるアプリケーション

本章では，従来方式を応用して実現するサービスの具体例を 3 つ挙げる．

3.1 子供の見守りサービス

監視カメラの映像を応用したサービスの具体例の 1 つとして，子供の見守りサービスが考えられる．子供を被撮影者とし，その親をその秘匿映像の復元者とする．町中で子供が通学途中に，通学路に設置されている監視カメラに撮影される.その映像を親が復元･確認できるようにすれば，子供の安否をリアルタイムで確認できるサービスが実現される．既存の手法として，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が，これらでは子供の位置はわかるが,子供の様子をリアルタイムで確認することは難しい．子供の様子がリアルタイムでわかることで，子供が事故や事件に巻き込まれたことが瞬時にわかり，いじめなどの場合，映像を証拠として利用することも可能である．

3.2 観光地映像利用サービス

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利用するサービスが考えられる．これを観光映像サービスと呼ぶ．このサービスは，例えばディズニーランドのような観光地であれば，監視カメラを防犯として利用する以外に，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.さらに，今後は観光地などではドローンによる監視なども考えられるが，これも犯罪などが起こらない平常時は観光地を訪れたお客への映像提供として利用できる．これによって，ユーザ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．

3.3 日常映像利用サービス

最後に，防犯を主目的とした従来サービスと新たなサービスをまとめた 3 つ目のサービスとして,コンビニや通学･通勤路などを含め街中で自身が映った映像を日常の記録として利用することが考えられる．これを映像記録サービスと呼ぶ.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利用することはできない.提案サービスでは映像が公開されるとしても，プライバシーを保護した状態で個人を特定できず,朝･昼･夜と変化する状況に対応できる．さらに，従来のコンビニやレストランなどでの監視カメラの利用は防犯が主であり,公開することを想定していないが，防犯用に閲覧される映像と外部に公開される映像で，その秘匿度合を変えて公開すれば，被撮影者のプライバシーを守りながら，防犯と被撮影者への映像提供の両立が可能になる．

4. 提案方式が満たすべき要件

前述したように，新しいサービスは従来方式だけでは構成できず，プロトコルの改良及び構成要素の変更などが必要である．そこで，以下に 3 章で考えたサービスを実際に実現する際，提案方式が満たすべき要件をまとめる．

(要件 1)監視カメラを管理するサーバが攻撃されても,秘匿していない映像が漏洩されない仕組みがある．

(要件 2) 監視カメラ映像から，自分の映像の秘匿化のみを外せる仕組みがある．

(要件 3) 監視カメラで撮影された全被撮影者の秘匿化を実現し，その秘匿映像を公開する仕組みがある．

(要件 4) 被撮影者が自身の映った映像を特定し，その映像を撮影した側に知られることなく得られる仕組みがある．

(要件 5) 復元者が被撮影者でなくても（親あるは友人など)，安全が担保できる仕組みがある．

(要件 6) 映像を内部監視と外部公開に用いる際，適切に秘匿の度合いを変更する仕組みがある．

(要件 7) 監視カメラオーナが自らの監視カメラを高級化しようとするモチベーションとなる仕組みがある．

4.1. 要件 1

従来方式は監視カメラを管理するサーバが外部に繋がっていることを前提としないローカルな仕組みのため，サーバが信頼できるサーバ管理者によって安全に管理されており，監視者は管理カメラの撮影操作はできても，サーバのセキュリティに関する設定は変更できないとするだけで十分であった．また，従来方式ではユーザ H の顔のモザイク化はサーバが行った．よって，従来方式のサーバを外部接続した場合，ネットワークを介した攻撃によってモザイクをかけていない原映像が漏洩する可能性がある．それに対して，提案方式は映像をクラウドにアップロードするためサーバはネットワークに接続されていることを前提とする．よって，サーバ管理者がネットワークを介した攻撃に対しても十分な知識を持ち，ネットワークを含めてサーバを安全に管理するという前提を設けてもよいが，この前提は現状の監視カメラオーナのセキュリティ意識の低さを考えれば，現実性が乏しい．よって，後述する第 1 段階の秘匿化機能(要件 6)を実装した監視カメラが開発され市販されているという前提をおく．すなわち，監視カメラはアクセスポイントの情報からユーザ H の位置を特定し，その匿名署名を検査して，正しければ指定された秘匿化鍵でモザイク処理を行う IC チップ（耐タンパ性も有する）などが実装されているとする．これによって，この監視カメラはユーザ H に対して第 1 段階の秘匿機能を自動的に実行し，第 1 段階の秘匿映像をサーバに出力する．この映像はサーバへの攻撃により漏洩する可能性があるが，ユーザ H の顔などは秘匿されているため，原映像が漏洩することはない．

4.2. 要件 2

従来方式は監視カメラ映像の利活用を想定していなかったため，ユーザが監視カメラ映像から自らのモザイクをはずせる仕組みを持たなかった．ただし，従来方式では犯罪などが起こったとき，警察などが認証局に依頼してモザイクをはずせる鍵を得る仕組みは含まれていた．しかし，厳密には従来方式では認証局がモザイク解除に必要なすべての情報を保存することは困難であったため，タイムスタンプサーバや監視カメラを管理するサーバなどからの情報も必要であり，煩雑であった．今回は後述するようにクラウドに映像を保存することを想定するため，タイムスタンプサーバからの情報などは秘匿映像に紐付けて保存することができるので，秘匿映像の復元は認証局が発行した鍵のみで実現できるよう変更する．よって，被撮影者が自分の映像とそれに添付された情報を得ることができれば，被撮影者は自分の鍵を用いて自らのモザイクをはずすことができるようになる．ただし，被撮影者が自身の映った映像を特定し，プライバシー保護の観点から，その映像を撮影した側に知られることなく入手できる仕組み（要件 4,7）が別に必要である．

4.3. 要件 3

従来方式では顔などのプライバシー情報の秘匿を望む被撮影者（ユーザ H）はシステムに登録して自らの鍵を得てモザイクを生成するが，プライバシー情報の秘匿に関心がない被撮影者（ユーザ O）のモザイク化は行われない．しかし，後述するように監視カメラ映像を公開することを考えた場合，ユーザ O を含む全被撮影者のプライバシー情報の秘匿が必要である．よって，ユーザ O に対してはクラウド管理者が設定した鍵を用いてユーザ O の秘匿を行う．ただし，観光映像サービスにおいては後述するパスワードから生成される鍵を用いて秘匿し，パスワードを知る被撮影者が映像を復元できるようにする．

また，現状では監視カメラ映像は被撮影者のプライバシーなどを考慮して公開されていない．しかし，前述のように全ての被撮影者を秘匿し，その解除は秘匿時に使用した鍵をもつ被撮影者（ユーザ O はクラウド管理者）のみとできれば，犯罪などが起こらない限り自らの秘匿映像は復元されないので，秘匿後の監視カメラ映像のクラウドなどによる公開が実現可能となる．

4.4. 要件 4

要件 3 によってクラウドに多くの監視カメラから被撮影者が全て秘匿された映像が送られ，クラウドがシステムの登録者にその秘匿映像を公開している場合を考える．クラウドに映像を送信する監視カメラの設置位置などは，システムに登録したユーザに公開されており，被撮影者は自分がある監視カメラの近傍にいた時間などに関する記憶があれば，クラウド中にある自分が映った秘匿映像を大雑把に特定できる．その映像の中の被撮影者を詳細に特定するために，公開された映像は秘匿時に使用した被撮影者の署名をタグ付けしており，各被撮影者がその位置・時間に生成された署名を再現し，そのタグと比較すれば，自分が映り・秘匿された映像を正確に特定できる．よって，その映像を入手できれば被撮影者は要件 2 によって自らの秘匿映像を復元できる．このクラウドが保存している映像を誰も管理されることなく自由に入手できれば要件 4 は実現される．ただし，このようなシステムでは安全性に問題があり，監視カメラ映像のオーナから見て，監視カメラ映像をクラウドにアップロードするメリットは全くなく，クラウド側もそれを公開するメリットが全くない．よって，安全な秘匿映像の入手法とそれを実行するメリットについては要件 7 において議論する．

4.5. 要件 5

要件 4 でクラウド上に公開される映像の全ての被撮影者は秘匿処理されているが，これを復元できるのはプライバシーの観点から被撮影者本人のみであるべきである．しかし，子供の見守りサービスにおいて被撮影者は子供であり，その映像の復元を望むのはその親である．また，観光映像サービスにおいては同意した友人同士など被撮影者以

外が秘匿映像の復元を望む場合が考えられ，被撮影者以外が復元を行える仕組みを導入する必要がある．ただし，このような仕組みを認めた場合，ストーカーのように特定の人を観察したい人が復元者として登録し，その特定者に鍵を設定した携帯端末を持たせられれば，被撮影者を常に観察することなどが可能になる．よって，被撮影者の同意に関する操作がなければ復元できないようにする必要がある．そのために，被撮影者または被撮影者間で定めたパスワードのようなものを想定し，そのパスワードを知るものだけが，その被撮影者の秘匿映像の復元を許可される仕組みを導入する．このパスワードは復元を許可するユーザ間で安全に共有されるが，その設定は手動であり通信などを用いて自動的に行えないようにする．あくまで，パスワードは被撮影者の端末に直接設定し，更新がなければ一定期間後の他者による復元を認めないとすれば，ストーカーが特定者に携帯端末を持たせても，毎回その端末に設定される新しいパスワードを知ることができなければ被撮影者以外は秘匿映像の復元ができない．

4.6. 要件 6

従来方式では，内部監視のみを想定しているため，ユーザ H でもモザイク化は顔部分のみであったが，要件 3 のようにクラウド上に映像を公開することを考えると，服装や動作等で個人が特定されることのないよう，体全体を秘匿する必要がある．そこで，この要件を満たすために，参考文献[6]の技術を用いる．[6]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し表示するシステムを提案している．私たちは，このシステムを利用し秘匿を 2 段階に分ける（図 1 参照）．

まず、撮影映像を前景映像と背景映像に分ける。そして、万引きなどの内部監視時はユーザ H の顔部分のみを検出し、$(R, G, B) = (0.255,0)$に置き換える 1 段階の秘匿化を行う．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．例え，そのとき取り逃がしても，ユーザ H であれば認証局に身元などを登録しているため，映像の証拠と共に警察に告発すれば，その映像の復元と犯人の身元特定ができる．ユーザ O は第 1 段階では秘匿されないので，通常の監視が可能である．次に，映像をクラウドなどへ保存し外部公開をする際はユーザ H または O に関わらず被撮影者の特徴が全く分からないように、前景映像全体を$(R, G, B) = (0.255,0)$の点で置き換える第 2 段階の秘匿を行う．これによって，ユーザ O もプライバシーが保護され，ユーザ H はプライバシー保護に加えて，自らの映像を利活用可能になる．なお，第 1 段階のモザイク化は監視カメラ内部で行う(要件 1)が，第 2 段階の秘匿は監視カメラを管理するサーバで映像をクラウドなどにアップロードする前に行う．このとき，第 1 段階の秘匿化を解除せず，第 2 段階の秘匿化を行うので，ユーザ H の顔を完全に復元するためには 2 段階の復号が必要である．

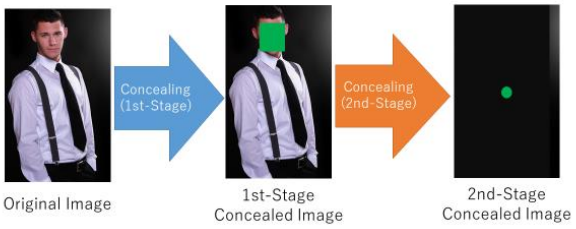

図 1　映像秘匿の段階化イメージ図

4.7. 要件 7

要件 4 で述べたように，システムの参加者(監視カメラオーナ，クラウド管理者，認証局)にとって，提案方式が利用されることで利益を得られるような仕組みが必要である．まず，提案方式において認証局はユーザの依頼によりユーザの個人情報を登録し，認証局の署名のついたユーザ ID（以降，認証局 ID）とそのユーザ固有の匿名署名用の鍵を発行し，ユーザからその登録料を得る．

次に，支払い業者はユーザに関するクレジット番号やその氏名・銀行口座，認証局 ID などを知り，ユーザからの要求とそれに対する対価に応じてクラウド管理者に料金を支払い，ユーザの要求する秘匿映像を得て，ユーザに転送する．ただし，このサービスに関する手数料などを得ることができるとする．

次に，このシステムに参加したいユーザは認証局 ID を自らの ID としてパスワードを設定して，クラウド管理者と匿名で契約する．よって，クラウド管理者はユーザが認証局に登録している人物であることとユーザが利用する支払い業者だけを知る．ユーザは認証局 ID とパスワードを用いて，登録者としてクラウドにアクセスし，自分の映像を見つけると所定の料金を支払い業者経由でクラウド管理者から映像を得る．このとき，クラウド管理者は指定された秘匿映像を対価と引き換えに支払い業者を介して送信する。

最後に，監視カメラオーナはアップロードされた映像が利用されると，クラウド管理者から対価を受け取ることができる．さらに，映像の画質が良ければその対価も高い場合，より高性能な監視カメラを設置するモチベーションとなり，オーナの利益は増大する．

以上より，被撮影者は自らのプライバシーを守りながら，自分に関連する監視カメラ映像の復元をすべて制御でき，その復元映像は犯罪が起きたときの警察以外に知られることのない安全なシステムが構築できる．さらに，このシステムに参加するクラウド管理者，認証局，支払い業者，監視カメラオーナは全て対価を得ることができ，監視カメラを高級化し，このシステムに参加するモチベーションが高まる．その結果として，監視カメラの画質や台数が増加し，監視カメラ本来の目的である防犯効果も高まるこ

とが予想できる.

5. 提案方式が満たすべき要件

本章では、4 章で挙げた要件を基に考案した提案方式の説明を行う。

5.1. システム構成要素

提案方式を説明するためのシステム図を図 2 に示す.

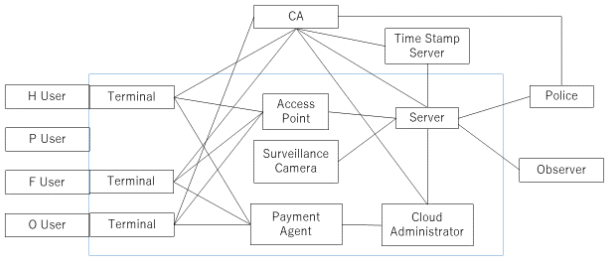

図 2　提案システム図

図 2 のシステムの構成要素は次の通りである.

・ユーザ H（Hidden）

従来方式と同様に提案システムに登録することにより，自分の顔の秘匿を望む被撮影者である．通信端末を持ち，アクセスポイントと通信を行い，認証局から得た鍵を用いて自身が正規のユーザであることを証明する．自らの秘匿映像を復元したい場合，自らの鍵を用いて復元できる.

・ユーザ P(Parent)

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．ユーザ H とともに自身の情報を認証局に登録しており，ユーザ H と鍵を共有している.

・ユーザ F(Friend)

システムに登録しているもう一人のユーザ H 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．ユーザ H と一緒に行動する場合等では，ユーザ H との同意により互いに定めたパスワードなどを共有する．そのパスワードを用いてユーザ H の秘匿映像も復元でき，ユーザ H もユーザ F の秘匿映像を復元できる.

・ユーザ O(Other)

自身の顔情報の秘匿を希望せずシステムに登録していないユーザ，もしくは登録しているが提案方式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．ただし，携帯端末と暗号化機能をもち，アクセスポイントとの暗号通信は可能である．内部監視においては顔の秘匿は行われず，映像が公開される場合，システムの鍵でプライバシー情報が秘匿される．ユーザ H と行動を共にする場合，パスワードをユーザ H と共有するが，それを元にユーザ H はユーザ O の秘匿映像も復元できる．ユーザ O はシステムに登録していないため，映像の復元はできない.

・監視者

監視カメラから送られてくる映像を用いて内部監視を行う．監視に必要な機能（映像の拡大や縮小など）のみ操作できる.モニタ映像の盗撮など不正を行う可能性がある.

・警察

犯罪捜査時に捜査令状等の正式な手続きを踏み，監視カメラの映像を利用できる．この時，秘匿化解除のための情報や，不正者がユーザ H であったときに，ユーザ H を特定できる登録情報を認証局より得ることができる．また，得た情報を不正に利用しない.

・認証局

登録したユーザの個人情報を管理し，認証局 ID と署名鍵などを配布する．また，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．信頼できる機関であるとする.

・監視カメラ

秘匿を望む被撮影者を特定し，その被撮影者に対して第 1 段階の秘匿化を行って，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.

・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複数設置される．ユーザ H の持つ通信端末と監視カメラ間で通信を行う.

・サーバ

監視者に監視カメラから送られてきた映像を提供する．映像をクラウド管理者に送る場合は，第 2 段階の映像秘匿を行う.

・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.

・支払い業者

ユーザから支払いを受け，クラウド管理者とデータの受け渡しを行う．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．信頼できる機関であるとする.

・クラウド管理者

監視カメラのオーナと契約をして，秘匿化された映像を保存する．秘匿映像へのアクセスは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.

・通信端末

通信端末にはユーザのカギが保存され、署名の生成やアクセスポイントとの通信を行う。耐タンパ性を有する。

5.2. 提案プロトコル

本節では、提案方式の具体的なプロトコルを説明する。まず、提案方式ではグループに所属したユーザのグループは特定できるが個人は特定できない署名方式である Short Group Signatures[7]を用いる.

Short Group Signatures とは，匿名署名技術の 1 つであり，2004 年に Dan らによって提案された．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は特定できるが，署名者が誰かは特定できない署名方式である．また，特別な権限をもつ者は署名者を特定できる．これによって，匿名で被撮影者の意思を反映できる．

以下では，アクセスポイント，監視カメラ，サーバ間，及び認証局，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．

A. 被撮影者登録

ここでは，自らのプライバシー情報の秘匿を望むユーザに関する設定について説明する．ただし，ユーザ H とユーザ F が行う登録処理は同じであるので，ここではユーザ H と，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について示す．

・STEP1

ユーザ H は本人であることを証明し，認証局に自らの個人情報を登録する．ユーザ P はそれに加えて，ユーザ H と自らの関係を証明し，Step2 でユーザ H と同様の情報を認証局から得る．

・STEP2

認証局は，個人情報を確認し，各ユーザに署名鍵gsk，認証局ID(*cID*)とモザイク鍵$mk1$を与える．また，検証鍵gpkを公開し，認証局の秘密鍵gukと合わせて全ての情報を安全に管理する．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は署名者を特定するための鍵である．また，認証局 ID は，認証局が生成する署名のつけられたユーザ固有の ID であり，モザイク鍵$mk1$は第 1 段階の秘匿・解除に用いる鍵である．

・STEP3

認証局はユーザ H に暗号化に用いる鍵*fk1* と*fk2* を定め，設定する．ただし，ユーザ P には*fk2* は設定されない．

・STEP4

ユーザ H またはユーザ P は *cID* を用いて匿名でクラウド管理者に登録する．その際，パスワードと利用する支払い機関を合わせてクラウド管理者に登録する．

B. 監視カメラ登録

システムに登録することを望む監視カメラオーナに関する設定について説明する．

・STEP1

監視カメラオーナは，自身の監視カメラが提案方式を実装しており，第 2 段階の秘匿映像をアップロードし，第 1 段階の秘匿映像及び後述の$mk2$を安全に管理することを誓約し，クラウド管理者と契約を行う．

・STEP2

監視カメラオーナはユーザ O の第 2 段階の秘匿化を行うための鍵$mk2$を定め，安全に保存する．

C. 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，*pw* はこの処理に入る前に，同意を得た人物間で共有されている．ユーザ F はユーザ H と同様の処理を行う．

・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をユーザ H に対し送信する．

・STEP2

ユーザ H はID_{server}を受け取り，*fk1* を用いてメッセージ Mを生成する（Mは*fk1* によってユーザ毎に異なる）

$$eTs = Enc_{fk1} T_s$$
$$M = H(cID||ID_{server}||eTs)$$

・STEP3

ユーザ H は Short Group Signature[7]の署名生成手順に従い，署名鍵gskを用いてメッセージ M に対する署名σ_Hを生成する．

$$\sigma_H = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_2})$$

・STEP4

ユーザ H 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，子供の見守りサービスの場合 *mk1* は *mk1*+*pw* に(XOR)，観光映像サービスの場合 *mk1* は *pw* になる．

$$ek_{H1} = Enc_{mk1} H(\sigma_H||T_s)$$
$$ek_{H2} = Enc_{mk1} H(ek_{H1})$$

・STEP5

ユーザ H は$(\sigma_H, M, ek_{H1}, ek_{H2})$をアクセスポイントを介して監視カメラに送信する．

・STEP6

ユーザ H,F,O が *pw* を共有している場合，ek_{O1}, ek_{O2}を生成し，アクセスポイントに送信する．また，ユーザ H,F は *fk2* で暗号化した *epw* も送信する．

$$ek_{O1} = Enc_{pw} H(T_s)$$
$$ek_{O2} = Enc_{pw} H(ek_{O1})$$
$$epw = Enc_{fk2} H(pw)$$

・STEP 7

監視カメラはユーザ H から情報を受け取り，検証鍵を用いて署名を検証する．但し，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．

・STEP8

監視カメラは，署名が正当ならユーザ H の顔を特定し，ek_{H1}を用いて原映像を秘匿化(第 1 段階)した movie1 を生成する．

・STEP9

監視カメラはek_{O1}, ek_{O2}を確認し，同じであればその送信者をマーキングする．

・STEP10

監視カメラは movie1 の秘匿した被撮影者毎にσ_H,ek_{H2}をタグ付けし，かつ時間毎にT_sをタグ付けした映像 movie1'を生成する．ただし，マーキングされたユーザ O にはek_{O1}, ek_{O2}をタグ付けし，ユーザ H にはepwのタグ付けを追加する．その後，監視カメラは movie1'をサーバに送信する．

D. 第 2 段階の秘匿化

サーバで行われる第 2 段階の秘匿化処理を説明する．

・STEP1

サーバは$mk2$を用いて，マーキングされていないユーザ O の秘匿化鍵ek_{O2}を以下のように生成する．ただし，マーキングされているユーザ O の秘匿化鍵はタグ付けされたek_{O2}になる．

$$ek_{O1} = Enc_{mk2}H(T_s)$$
$$ek_{O2} = Enc_{mk2}H(ek_{O1})$$

・STEP2

サーバはユーザ H をek_{H2}で，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が，ユーザ H の点はσ_Hと，マーキングされたユーザ O の点はek_{O1}とタグ付けされ，ユーザ H にはepwのタグ付けが追加される）．

・STEP3

サーバは movie2 をクラウドに送信し，$ek_{H2}, ek_{O1}, ek_{O2}, pw, epw$を削除する．

E. クラウドによる映像公開及び映像検索

この処理も従来方式にはない．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．

・STEP1

クラウドは movie2 を監視カメラ(ID_{server})毎のフォルダに分類して，登録者に公開する．

・STEP2

登録者(ユーザ H,F,P)は被撮影者が映っていると想定される監視カメラのフォルダから，映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．

・STEP3

登録者は movie2 にタグ付けされているT_sから 4.4.3 の STEP2,3 の処理を行い，σ_Hを再現して，movie2 のタグ付けからそれに対応する点（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．

・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．

F. ユーザ H またはユーザ P による映像の復元

この処理も従来方式にはない．ユーザ O も第 2 段階の秘匿が行われているが，pwを知る登録者（ユーザ H,F）はその映像を復元できる．

・STEP1

ユーザ H とユーザ P は 4.4.3 の STEP4 に示す鍵ek_{H1}, ek_{H2}を生成し，自らの映像を復元する．

・STEP2

ユーザ H はユーザ F の映像を，pwとタグ付けされたσ_Fから 4.4.3 の STEP4 の手順で鍵を生成して復元する．

・STEP3

ユーザ H はユーザ O の映像を，pwとタグ付けされたek_{O1}から 4.4.3 の STEP6 の手順でek_{O2}を生成して復元する．ただし，ユーザ H がpwを忘れた場合，タグ付けされているepwを復号する．

G. 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

警察は捜査令状等の正規手続きを行い，捜査令状などをクラウド管理者に示し，必要な映像を撮影した監視カメラを特定する．または，捜査現場の近くにある監視カメラを特定する．

・STEP2

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

・STEP3

警察は認証局に令状を示し，movie1'にタグ付けされた署名からユーザ H の特定と，そのモザイク鍵$mk1$及びfkの提出を求める．

・STEP4

警察は得られた鍵を用いて，movie1 の秘匿画像を復元する．

6. 提案サービスの具体的実現とその安全性

本章では，3 章で示したサービスが 5 章に示した提案プロトコルによって実現できることと，その安全性について考察する．

6.1 子供の見守りサービス

このサービスの実現における最大の特徴は，5.2 節 C の STEP4 に示したように映像の秘匿・解除を行える鍵ek_{H1}, ek_{H2}を認証局から与えられたモザイク鍵 *mk1* と *pw* から生成する点である．これによって，*mk1* と *pw* の 2 つを知る者だけが秘匿映像を復元できる．よって，*pw* が偶然知られたとしても *mk1* が知られなければ映像は復元されない．また，このサービスは手動による一定期間毎の *pw* 設定が必須であり，それがなければ機能しないとするため，一定期間以上 *pw* 設定しなければユーザ O と同様に自ら秘匿解除できなくなる．また，ユーザ P は *fk2* を知らないた

め，タグ付けされた *epw* から *pw* を復元できない．よって，ユーザ H が騙されて端末を持たされたとしても，ユーザ H が *pw* を設定しない，または一定期間毎に *pw* を変えて，それをユーザ P となっている人物に教えなければ，ユーザ P は映像を復元できない．

一方，ユーザ H による復元では自分の署名鍵と映像へのタグ付け情報から署名を再現でき，それと秘匿映像にタグ付けされた署名とを比較することによって，自らを特定できるが，署名鍵を知らず署名を再現できない者は映像上の被撮影者を全く特定できない．また，タグ付けの署名とタイムスタンプから映像を復元しようとしても，ユーザ H 固有のモザイク鍵 *mk1* を知らなければ復元できない．ただし，正当なユーザ P はユーザ H と同じ情報を共有し，*pw* も常に知るので，ユーザ H と同様に秘匿映像を検索・復元できる．ユーザ F も秘匿されたユーザ H の映像を特定できず，また *mk1* も知らないため映像を復元できない．ユーザ O は秘匿映像自体を得ることができない．

一方，警察は捜査令状などによって認証局から得た $mk1$ 及び *fk1,fk2*（タグ付けされた *epw* から *pw* を復元）と映像にタグ付けされた情報から，全被撮影者の映像を復元できる．

以上より，このサービスではユーザ H と *pw* を常に共有するユーザ P だけがユーザ H の様子を観察でき，それ以外の人物は観察できないという安全性と，捜査時などでは警察は秘匿映像を解除し，捜査に役立てることができるという安全性を実現する．

6.2 観光地映像利用サービス

このサービスの特徴は 5.2 節 C の STEP4 に示すように，共有されたパスワード *pw* に基づいて秘匿処理が行われる点である．よって，*pw* を知る者は秘匿映像を復元できるが，*pw* が漏洩すると映像にタグ付けされた情報から当事者以外でも秘匿映像を復元できる．よって，このサービスは多くの人と行動を共にする個人のプライバシーが少ない状況のときに有効である．ただし，ek_{O1}, ek_{O2} が一致しなければマーキングしない．よって，一致する同行者がいない一人だけではこのサービスは利用できない．また，ストーカーなどにこのサービスを悪用されないように，子供の見守りサービスではこのサービスを利用できない．逆に，同行者がいても映像共有を望まなければ，*pw* を共有しないことによって，他者に自らの映像が復元されることはなくなる．

ただし，ユーザ O は *pw* を共有することによってユーザ H またはユーザ F に自らの映像の復元を許可することができるが，自らはシステムに登録していないため，映像の入手・復元はできない。

以上より，このサービスの安全性は他と比べると落ちるが，多くの人物と行動を共にし，映像を共有したい場合に有効である．

6.3 日常映像利用サービス

このサービスは 5.2 節 A の設定時に選択され，ユーザ P を設定せず，ユーザ H が自らの映像を記録として残したい場合に有効である．

子供の見守りサービスにおいて述べたように，初期設定によりユーザ H の情報はユーザ H のみが設定でき，*pw* を用いない（5.2 節 C の STEP4）ため，利用が容易であり，安全性も子供の見守りサービスと同等以上が可能である．ただし，観光映像サービスはシステムにそれを実行することを示す情報を送ることによって両立でき，一時的に他者と情報共有することもできる．

7. まとめ

本論文では，小林らが提案した被撮影者のプライバシー保護を実現する監視カメラシステム[3]を拡張して可能となる新しいサービスとその具体的プロトコルを示した．また，具体的プロトコルの提案サービスにおける安全性を示し，全ての映像を被撮影者の意思によって制御でき，今までにない安全性を実現することを示した．これにより，監視カメラを監視以外の目的で利用することができ，今後監視カメラが増えていっても監視社会となることなく，自らの映像管理というメリットを一般ユーザに提供できるようになる．

今後の展望として，プロトコルの実装評価を行い，その有効性を実証することを検討している．

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, 2002 年 11 月, 14 巻, pp.18-21

[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]小林健人，稲村勝樹，金田北洋，岩村惠市: 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 Vol.57, No.1, pp.172~183, Jan.2016

[4]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，2017 Symposium on Cryptography and Information Security Naha, Japan, Jan. 24- 27, 2017

[5]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

[6]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.2 152-162, Jul. 2008

[7]Dan Boneh, Xavier Boyen, Hovav Shacham: Short Group Signatures, CRYPTO 2004, August 15-19, 2004