Vol.2017-CSEC-77 No.3
Vol.2017-IOT-37 No.3
2017/5/25

個人情報保護を実現する監視カメラが可能とするサービス

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プライバシーを適切に秘匿する必要が生じている．そんな中，被撮影者の意思を反映させて監視カメラ映像の顔情報を秘匿する方法が提案されている．本論文の目的は，この方法を用いて監視カメラの映像を様々なサービスに利用することである．近年，監視カメラは監視だけでなく，様々な目的で使用されている．本文中では，プライバシーに配慮しながら監視カメラ映像を利用するサービスの具体例を 2 つ紹介し，その際に生じる脅威とその対策についても考察する．

キーワード：映像サーベイランス，プライバシー，監視カメラ

Services that Surveillance Cameras that Realize Personal Information Protection Enable

KOTA HOSHINO[†1]　KEIICHI IWAMURA[†1]

Abstract: Along with the spread of image surveillance, it is necessary to properly conceal the privacy of the image of the surveillance camera. Under such circumstances, a method of concealing the face information of the surveillance camera image reflecting the intention of the photographed person has been proposed. The purpose of this thesis is to use the images of surveillance cameras for various services using this method. In recent years, surveillance cameras are used not only for monitoring but also for various purposes. In the text, we introduce two examples of services that use surveillance camera images while considering privacy, and consider threats and countermeasures.

Keywords: *image surveillance, privacy, surveillance camera*

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，著者らは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（以降，従来方式）を提案している[3]．この方式は顔などのプライバシー情報の秘匿を望む被撮影者は，その意思を匿名署名によってシステムに示し，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し，その鍵を用いて被撮影者の映像にモザイクをかける．この処理を監視カメラ内で行い，モニタ等にはプライバシー保護された映像が映される．ただし，プライバシー保護を望む被撮影者が万引きなどの不正を行った場合，匿名署名から本人を特定できる．また，このシステムには匿名署名に用いる鍵を発行・認証する認証局があり，全ての鍵を管理しているため，犯罪捜査時などに令状などの正式な手続きがあれば，プライバシー保護された映像の解除を実行できる．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ーを自らの意思によって保護することができる．

一方，犯罪を抑止するために監視カメラが有効であることが広く認知されているが，最近は監視カメラのネットワーク化なども検討されており，特定の人物を町中の監視カメラを使って追跡できるなど，監視カメラによる監視社会となる危惧がある．このような危惧に対しても前記従来方式は有効である．すなわち，犯罪などが起こり正式な令状などによる手続きがない限り，被撮影者の映像は秘匿される．

また，SCIS2017 で提案された監視カメラ運用ガイドライン[4]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，データ解析のような応用例がある．こういった文献からも，監視カメラのこれからの応用に期待されていることがわかる．前述したように，従来方式を用いることで，被撮影者の意思に反してプライバシーが侵害される可能性が減少する．よって，従来方式を適用した監視カメラ映像を用いることで，被撮影者のプライバシーを秘匿しつつ，防犯以外の目的への監視カメラの適用

†1, 東京理科大学

の可能性が見える．

そこで，本論文ではまず，従来方式を基に監視以外の新たなサービスを展開することを検討する．ここでは，監視カメラ映像を用いるサービスの具体例の 1 つとして，子供の見守りサービスを考える．これは，通学路に設置された監視カメラに映る子供を被撮影者とし，街中の監視カメラで撮影された映像を親が制御できるようにすることで，子供の安否をリアルタイムで確認することができるサービスである．GPS などによって子供の位置情報を追跡するサービスは現在でもあるが，このサービスはいじめが行われていないかなどの子供の状況を親がリアルタイムに把握することができる．ただし，このサービスを具体化するためには，前記従来方式の改良が必要であり，このような新たな応用においては前記ガイドラインにもあるように適切なリスク評価を行う必要がある．そこで，新たな応用に対応できるように，従来方式の改良を行った方式を提案する．また，それによって発生する問題点などを検討し，その安全性を評価することによって監視カメラシステムの新たな応用の可能性を検討する．

本論文では，2 章で従来の監視カメラシステムの問題点をまとめ，3 章で監視カメラの応用として新たに考えられるサービスを示し，4 章でそれらのサービスを実現する提案方式の説明，5，6 章で提案方式のメリットと考えられる脅威を検討し，その対策について考察を行う．

2. 従来の監視カメラシステムの問題点

2.1. ネットワークにおける監視カメラ

今までの監視カメラは，撮影映像を記録媒体に保存し，必要に応じ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，監視カメラはネットワークに接続されて利用され，「ネットワークカメラ」と呼ばれることもある．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，参考文献[5]によると，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．

また，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個人をはっきり特定できるほどである．そんな中，コンビニに設置された監視カメラ映像の流出事件[6]が発生した．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制御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必要がある．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．

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ーを守るようなシステムの適用がある．参考文献[4]のように，監視カメラ映像の人物の顔部分にモザイクをかける手法は数多く提案されているが，私たちの提案方式の基となっている従来方式[3]は，システム側でのモザイク除去は特殊な場合を除いて不可能であり，被撮影者の意思によってのみモザイクの除去が可能である唯一の方式である．このような方式を適用することで，ネットワークを介した監視カメラ映像からのプライバシーの侵害を防ぐことができるようになる．

2.2. 監視カメラのこれから

もし，監視カメラ映像の被撮影者のプライバシー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，データ解析のような利用ができる可能性がある．私たちは，その応用の可能性の 1 つとして，従来方式[3]のシステムを適切に運用することで，監視カメラの被撮影者のプライバシーを守りつつ，監視カメラ映像を売買できるようなサービスを考える．次章以降で詳しく説明するが，映像の購入者は購入した映像の自分自身のモザイクのみを外すことができ，映像に映る他の人のモザイクを外すことができないので，映像に映る他の人のプライバシーは侵害されない．このような監視カメラ映像を売買できるようなサービスの具体例を次章で説明する．

3. 監視カメラ映像を利用して新たに考えられるサービス

本章では，従来方式[3]を応用して実現するサービスの具体例を 2 つ挙げる．

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ある．子供を被撮影者とし，その親を被撮影者側とする．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．そこで，親が撮影された映像を復元・確認するようにできれば，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，映像を子供がいじめにあっている証拠に適用することも可能である．

また，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復元・購入するサービスが考えられる．これは，旅行先や観光地に設置されている監視カメラの映像をユーザが利用・購入するようにできれば，ユーザは旅行先で個人のカメラを使わずに鮮明な映像(静止画)や動画を得ることができ，町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を可能にする．既存の手法として 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，自身も映っている映像を利用することはできない．また，提案サービスは監視カメラのリアルタイムな映像を利用できるため，朝・昼・夜と変化する状況に対応できる．また，監視カメラの設置されている位置によっては，個人では実現が難しい角度から撮影した映像を得ることもできる．

4. 提案方式

本章では，従来方式[3]を基に，前章で考えたような新しいサービスに適用するためにプロトコルを改良した方式の提案を行う．

4.1 提案方式の特徴

3 章で考えたようなサービスを実際に実現する際，新たにユーザ同士の関係性の正当性を検証する署名や，大量の映像を保存するためのクラウドが必要であり，またクラウドに保存された映像を正当なユーザのみが利用できるようにする必要がある．

そこで，監視カメラオーナとクラウド管理者同士で契約し，クラウド管理者が監視カメラ映像の提供を得て，監視カメラオーナが契約料を得る仕組みにすることで，相互が利益を得つつ，従来方式を新たなサービスとして拡張できるようにした．また，被撮影者側による映像購入の際に署名を要求し，認証局が発行する許可証がないとクラウドから映像を取得できないようにし，正当なユーザ以外の映像利用を排他するようにした．また，従来方式では認証局の役割が過大であるため，新たに信頼できる支払い業者を置き，料金支払い関連の役割を任せることにより，認証局の負担を軽減した．そして，監視カメラに固有鍵を設定し，サーバに送信する映像に一時的な暗号化処理を行うことで，サーバの不正の可能性に対しても対策した．

4.2 提案方式の概要

提案方式を説明するためのシステム図を図 1 に示す．

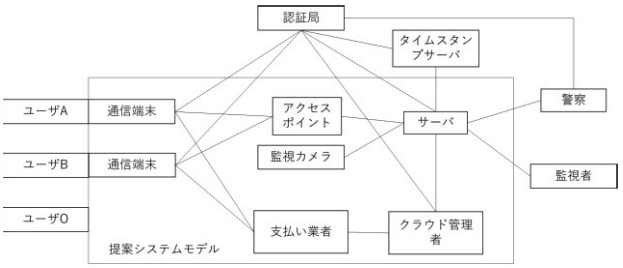

図 1　提案システム図

図 1 のシステムの構成要素は次の通りである．

・ユーザ A

自分の顔情報の秘匿を希望するユーザである．自身の情報を認証局に登録しており，認証局から正規のユーザであることを証明する鍵を得ている．また，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．

・ユーザ B

ユーザ A と親族関係等の関係をもつユーザである．自身の情報を認証局に登録しており，認証局から正規のユーザであることを証明する鍵を得ている．また，通信端末を持ち，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．

・ユーザ O

自身の顔情報の秘匿を希望しないユーザ，もしくは通信端末とアクセスポイントとの通信を行わないユーザである．

・監視者

サーバから送られてくる映像を用いて監視を行う．サーバの監視に必要な機能のみ操作でき，サーバの設定等は改変できない．

・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，監視カメラの映像中のモザイクを除去する申請を行うことで，モザイク除去のための情報や，不正者がユーザ A であったときに，ユーザ A を特定できる登録情報を認証局より得る．また，得た情報を不正に利用しない．

・認証局

ユーザ A，B の個人情報を管理し，署名鍵を配布する．また，署名の検証鍵を生成・公開する．また，犯罪捜査時に警察からの要請によってユーザを特定し，個人情報を警察に提供する．信頼できる管理者が管理を行う．

・監視カメラ

撮影された映像をシステム内に設置されているサーバに対して暗号化して送信する．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 A の持つ通信端末とサーバ間の通信を行う．

・サーバ

アクセスポイントを介して，ユーザ A，B の持つ通信端

末と通信を行う．被撮影者個人を特定することなく，被撮影者がユーザ A であることを検証できる．TDMA 方式により，ユーザ A の端末位置情報を知る．映像内の人物位置を推定できる．耐タンパ性を持つ．管理者の信頼度は中程度であり，不正を働く可能性がある．

・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，クラウド管理者へ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．信頼できる管理者が管理する．

・クラウド管理者

モザイク化された映像を保存するクラウドの管理者．監視カメラのオーナと契約している．管理者の信頼度は中程度であり，不正を働く可能性がある．

4.3 匿名署名

提案方式において，システムには様々な機関・管理者が関わることになり,ユーザはそれらと通信を行う.その際,自らが正当なユーザであることを証明する署名を生成する必要がある．しかし，すべてのシステムの構成要素が信頼できるわけではないので，不正を働く可能性がある機関に対し，ユーザの個人情報が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[10]を用いる．

Short Group Signatures[10]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，Short Group Signatures[10]を説明する．

(1) Bilinear Groups

まず，Bilinear Groups という設定を行い，以下の条件を満たす．

1. G_1とG_2は素数 p を法とした巡回群
2. g_1はG_1の元，g_2はG_2の元
3. φは計算可能な同型写像で，$\varphi(g_2) = g_1$
4. eは$\mathrm{G_1}\times\mathrm{G_2} \rightarrow \mathrm{G_T}$とするペアリング関数

・Bilinearity

全ての$u \in G_1, v \in G_1, (a,b) \in Z$について，以下が成り立つ．

$$e(u^a, v^b) = e(u,v)^{ab}$$

・Non-degeneracy

$$e(g_1, g_2) \neq 1$$

(2) 署名アルゴリズム

・鍵生成

まず，認証局は次の設定を行う．

$$g_2 \in G_2$$
$$\varphi(g_2) = g_1$$
$$(h, \xi_1, \xi_2) \in G_1 \setminus \{1_{G1}\}$$

また，$u^{\xi_1} = v^{\xi_2} = h$を満たすような$(u,v)$を選ぶ．次に，$\gamma$を秘密のパラメータとして，

$$w = g_2^{\gamma}$$

を満たすような w を設定する．

次に，認証局は，検証鍵 gpk として，

$$gpk = (g_1,\ g_2, u, v, h, w)$$

を公開する．また，各グループメンバーiに署名鍵 $gsk[i]$を次のように生成し，配布する．

$$gsk[i] = (A_i,\ x_i)$$

なお，A_iとx_iは次の条件を満たす．

$$A_i \in G_1,\ A_i^{\gamma + x_i} = g_1$$

最後に，認証局は署名者を特定するための秘密鍵$gmk = (\xi_1, \xi_2)$を管理する．

・署名生成

署名者であるグループメンバーiは署名を生成する際に，2 つの値を次のように設定する．

$$\alpha,\ \beta \xleftarrow{R} Z_p$$

そして，次の 5 つの値を計算する．

$$T_1 = u^{\alpha}$$
$$T_2 = u^{\beta}$$
$$T_3 = A_i h^{\alpha+\beta}$$
$$\delta_1 = x_i \alpha$$
$$\delta_2 = x_i \beta$$

そして，次の 5 つの値を選ぶ．

$$r_{\alpha}, r_{\beta}, r_{x_i}, r_{\delta_1}, r_{\delta_2} \in Z_p$$

これらの値を用いて次の値を計算する．

$$R_1 = u^{r_{\alpha}},\ R_2 = v^{r_{\beta}}$$
$$R_3 = e(T_3, g_2)^{r_{xi}} \cdot e(h,w)^{-r_{\alpha}-r_{\beta}} \cdot \left(\frac{e(T_3,w)}{e(g_1,g_2)}\right)$$
$$R_4 = T_1^{r_{x_i}} u^{-r_{\delta_1}},\ R_5 = T_2^{r_{xi}} v^{-r_{\delta_2}}$$
$$c = H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \in Z_p$$
$$s_{\alpha} = r_{\alpha} + c\alpha,\ s_{\beta} = r_{\beta} + c\beta,\ s_{x_i} = r_{x_i} + cx_i$$
$$s_{\delta_1} = r\delta_1 + c\delta_1,\ s_{\delta_2} = r_{\delta_2} + c\delta_2$$

そして，署名者メッセージ M に対する署名を以下のように生成し，公開する．

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

・署名検証

検証者は署名をもとに次の計算を行う．

$$\overline{R_1} = u^{s_{\alpha}} T_1^{-c},\ \overline{R_2} = u^{s_{\beta}} T_2^{-c}$$
$$\overline{R_3} = e(T_3, g_2)^{s_{x_i}} \cdot e(h,w)^{-s_{\alpha}-s_{\beta}} \cdot e(h, g_2)^{-s_{\delta_1}-s_{\delta_2}} \cdot (e(T_3,w)/e(g_1,g_2))$$
$$R_4 = T_1^{s_{x_i}} u^{-s_{\delta_1}},\ R_5 = T_2^{s_{x_i}} v^{-s_{\delta_2}}$$

そして，次のように検証を行う．

$$c = H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$$

・署名者の特定

認証局は署名と自身の秘密鍵 gmk を用いて以下の計算を行うことで，署名者の
署名鍵の一部を算出することができる．

$$\frac{T_3}{T_1^{\xi_1} \cdot T_2^{\xi_2}} = \frac{A_i h^{\alpha+\beta}}{u^{\alpha\xi_1} \cdot v^{\beta\xi_2}} = A_i$$

認証局はグループメンバーの情報を管理しているため，署名鍵の一部を算出することにより，署名者を特定する．

4.4 通信プロトコル

本節で，提案手法における通信プロトコルを示す．ただし，アクセスポイント，監視カメラ，サーバ間，および認証局，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安全に行われるとする．

(1)事前設定

ここでは，被撮影者のうちユーザ A，B になることを望む人が行う設定について説明する．なお，この設定は監視カメラの撮影範囲内に入る前に行う．

・STEP1

ユーザ A，ユーザ B となる人物は認証局に自らの個人情報と，ユーザ A とユーザ B の関係(親と子の関係等)を登録する．

・STEP2

認証局は，個人情報を確認し，各ユーザに署名鍵gsk，IDを与える．また，検証鍵gpkと，認証局の秘密鍵gmkを管理する．さらに，サービス利用のためのID_{login}とパスワードPWを各ユーザに配布する．

・STEP3

認証局は監視カメラのIDを引数にして鍵s_cを作成し，監視カメラに配布する．認証局は監視カメラの秘密鍵をリスト化し管理する．

・STEP4

認証局はサーバに秘密鍵s_sを配布．サーバはこれをリスト化し管理する．

(2)モザイク生成

ここでは，実際にユーザ A 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通信プロトコルを示す．

・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})をユーザ A に対し送信する．

・STEP2

ユーザ A はID_{server}を受け取り，乱数rを生成する．

・STEP3

ユーザ A は以下のようなメッセージkを生成する．

$$k = H(ID||ID_{server}||r)$$

・STEP4

ユーザ A は Short Group Signatures の署名生成手順に従い，署名σ_Aを署名鍵gskを用いて生成し，アクセスポイントを介し(σ_A, k)をサーバに送信する．同時にユーザ B と監視カメラにもσ_Aを暗号化し送信する．

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

・STEP5

サーバはユーザ A 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，同じ署名については 1 度のみ検証する．

・STEP6

サーバは，署名が正当なら，監視カメラにその旨を通知する．監視カメラはユーザ A の顔を特定し，映像を暗号化する．暗号化する際に使用する鍵ekはタイムスタンプ情報T_s，ユーザ A の署名σ_Aを用いて生成し，カメラ秘密鍵s_cを用いて暗号化して生成する．

$$ek = Enc_{s_c} H(T_s||\sigma_A)$$

・STEP7

監視カメラは，ユーザ A 以外の顔部分に対し暗号化処理．その際の暗号化鍵ek_{all}は以下のように生成する．監視者はこの暗号化映像を用いて監視を行う．

$$ek_{all} = Enc_{s_c} H(T_s)$$

・STEP8

監視カメラは暗号化処理の後，暗号化鍵を削除し，サーバに暗号化映像を送信する．

・STEP9

サーバはモザイク鍵mkを用い暗号化された部分にモザイク処理を行う．モザイク処理する際に使用する鍵mk, mk_{all}はタイムスタンプ情報T_s，ユーザ A の署名σ_Aを用いて生成し，サーバ秘密鍵s_sを用いて暗号化して生成する．

$$mk = Enc_{s_s} H(T_s||\sigma_A)$$

$$mk_{all} = Enc_{s_s} H(T_s)$$

STEP10 : サーバはモザイク処理の後，モザイク鍵を削除しサーバにモザイク映像と署名σ_A，タイムスタンプ情報をタグ付けして保存する．

(3)モザイク除去

ここでは，警察が事件捜査時に監視カメラ映像を用いる際にモザイクを除去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，その旨を認証局へ伝達する．

・STEP2

認証局は伝達を確認，対象とする映像をタイムスタンプ情報を用いてクラウド上から検索する．

・STEP3

認証局は検索した映像にタグづけられた情報と，監視カメラの秘密鍵s_cを用いて暗号化鍵を，サーバの秘密鍵s_sを用いてモザイク鍵を復元し，警察へ送信する．

・STEP4

警察は暗号化鍵ekとモザイク鍵mkを用いてモザイクを

除去し，顔情報の秘匿されている人物の中で個人を特定する必要が生じた際，認証局へ登録された個人情報提供を申請する．

・STEP5

認証局は警察から個人特定の申請を受けると，署名σ_Aと認証局の秘密鍵gmkよりそのユーザ A を特定，対応する個人情報を警察へ提供する．

(4)ユーザ B による監視カメラ映像の利用

ここでは，ユーザ A(被撮影者)の映像をユーザ B(A と関係を持つユーザ)が利用する場合の通信プロトコルを示す．

・STEP1

ユーザ B が認証局にID_{loginB}とPW_Bを用いてログインする．ユーザ B は欲しいユーザ A が映っている映像にタグ付けされているユーザ A の匿名署名に対して自身の匿名署名鍵で匿名署名σ_Bを生成し， 認証局へ対して暗号化して送信する．

・STEP2

認証局は署名検証後，ユーザ B に対してクラウドへのアクセス許可証と暗号化鍵とモザイク鍵を暗号化して送信する．なお，この許可証は，ユーザ B がユーザ A の匿名署名にタグ付けされた映像のみ検索できるようにするものであり，暗号化鍵・モザイク鍵は暗号化された映像を復元するための鍵で，それぞれ監視カメラ・サーバの秘密鍵を用いて復元する．

・STEP3

認証局がユーザ B がクラウドにアクセス希望していることをクラウドと支払い業者に通知する(クラウドに対し個人名は伏せる).

・STEP4

ユーザ B は認証局からの許可を受けると，タグ付けされたユーザ A の署名σ_Aと認証局からの許可証に対してユーザ B は署名$\sigma_B{}'$を生成し，支払い業者に対して署名送信と共に料金を支払う．

・STEP5

支払い業者はこの署名をクラウド管理者に送信する．クラウド管理者はこの署名を検証し，成功した場合に送られてきたユーザ A の署名σ_Aがタグづけられている映像をクラウドから検索し支払い業者に送信する．

・STEP6

支払い業者はユーザ B に映像を送信し，問題なければ支払い手続きを完了させる．ユーザ B は映像を受信し，STEP2 で認証局から受けとった暗号化鍵・モザイク鍵を利用することでユーザ A のみの顔を復元する．

(5)ユーザ A による監視カメラ映像の利用

ここでは，ユーザ A(被撮影者)の映像をユーザ A 自身が利用する場合の通信プロトコルを示す．

・STEP1

ユーザ A が認証局にID_{loginA}とPW_Aを用いてログインする．ユーザ A は欲しい自分が映っている映像にタグ付けされている過去の匿名署名σ_Aに対して自身の匿名署名鍵で匿名署名$\sigma_A{}'$を生成し， 認証局へ対して暗号化して送信する．

・STEP2

認証局は署名検証後，ユーザ A に対してクラウドへのアクセス許可証と暗号化鍵とモザイク鍵を暗号化して送信する．なお，この許可証は，ユーザ A の匿名署名にタグ付けされた映像のみ検索できるようにするものであり，暗号化鍵・モザイク鍵はユーザ A の顔を復元するための鍵で，それぞれ監視カメラ・サーバの秘密鍵を用いて復元する．

・STEP3

認証局がユーザ A がクラウドにアクセス希望していることをクラウドと支払い業者に通知する(クラウドに対し個人名は伏せる).

・STEP4

ユーザ A は認証局からの許可を受けると，タグ付けされた署名σ_Aと認証局からの許可証に対してユーザ A は署名$\sigma_A{}''$を生成する．支払い業者に対して署名送信と共に料金を支払う．

・STEP5

支払い業者はこの署名をクラウド管理者に送信．クラウド管理者はこの署名を検証し，成功した場合に送られてきたユーザ A の署名がタグづけられている映像をクラウドから検索し支払い業者に送信する．

・STEP6

支払い業者はユーザ A に映像を送信し，問題なければ支払い手続きを完了させる．ユーザ A は映像を受信し，STEP2 で認証局から受けとった暗号化鍵・モザイク鍵を利用することでユーザ A のみの顔を復元する．

4.5 ユーザ A が複数いる場合の通信プロトコル

ここでは，ユーザ A(被撮影者)が複数いる場合(ユーザA_1，A_2とする)を考える．ユーザ A が複数いる場合，映像には人数分の署名がタグ付けされるが，検索や映像の利用の際，全員分の署名を検証するのは非常に煩雑である．そこで，署名に共通のパスワードを設定することで，この煩雑さを軽減する．以下，通信プロトコルの変更点を述べる．

まず，事前設定の際，予めユーザA_1とA_2がサイトにログインし，2 人だけが知るパスワードPWを作成しておく．そして，モザイク生成手順のときユーザA_1，A_2が撮影範囲内に入る直前にログインしチェックを入れておくことで，パスワードPWが有効になり，クラウドへの映像保存の際に署名と一緒に映像にタグ付けされる．PWがタグ付けされている映像については，ユーザA_1，A_2の 2 つの署名のうちどちらかあればクラウドから検索可能にする．また，ユー

ザA_1，A_2の2つの署名のうちどちらかの署名検証が成功したら，人数分のモザイク鍵，暗号化鍵を復元可能にする．そうすることで，映像の利用時に，チェックを入れておいたユーザの署名のうち，最低1つの署名でモザイクの除去が可能になる．

5. 提案方式のメリット・サービスの実現例

前章で提案方式の通信プロトコルとシステムについて説明したが，本章では提案システムを適用することによるメリットと，3 章で示したサービスが 4 章のプロトコルで実現できることを示す．

まず，提案システムに関わるユーザ・管理者のメリットについて説明する．被撮影者は，自身の納得する料金で映像を利用することができる．クラウド管理者は，ユーザからの料金とクラウドにアクセスする際のアクセス料によって利益を得る．認証局及び支払い業者は，仲介手数料を得ることができる．クラウド管理者と監視カメラオーナ間で契約料が発生する仕組みにすることで，監視カメラオーナは，監視カメラ映像をモザイク化して提供することで契約料を得ることができるので，監視カメラオーナの数，即ち監視カメラの数が増加する．そして，この契約料をカメラの画質が良いほど高額とすることで，監視カメラオーナがカメラの画質を良くしようとするため，監視カメラの画質の向上が見込める．結果として，本サービスを適用することで，監視カメラの本来の目的である防犯効果も高まることが予想できる．

また，利益面以外でのメリットとして，被撮影者の意思を尊重したシステムであることが挙げられる．提案手法は，認証局に被撮影者の意思を登録し，それを参照して顔の秘匿を行うため，被撮影者の意思が尊重されているシステムであるといえる．

次に，3 章で示したサービスが 4 章のプロトコルで実現できることを示す．監視カメラの映像を利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ある．前章のユーザ B を親，ユーザ A をその子供と置く．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．そこで，4.4 章の(4)のプロトコルを用いて，親が子供の映像を購入することで，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．また，サービスの具体例の 2 つ目として，旅行先や移動先で自身や友人，家族の映像を購入するサービスがある．これは，旅行先や移動先に設置されている監視カメラの映像を 4.4 章の(5)と 4.5 のプロトコルを用いて購入することで，ユーザは旅行先で個人のカメラを使わずに鮮明な映像(静止画)を得ることができたり，町中で自身が映った映像を日常生活で利用することを可能にする．

6. 考えられる脅威と安全性

本章では，4 章で説明した通信プロトコルに対する起きうる脅威とその対策について説明する．

(脅威 1)第三者による通信路盗聴

4.4 でアクセスポイント，監視カメラ，サーバ間，および認証局，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安全に行われるという前提を置いたので，通信路に用いる暗号化技術が安全であれば問題はないといえる．

(脅威 2)クラウド管理者による不正な映像閲覧

4.4(2)で説明したように，クラウドに保存される映像の顔情報にはモザイクがかかっている．クラウド管理者にはモザイク鍵・暗号化鍵を得る権限はないため，被撮影者のプライバシーは守られているといえる．

(脅威 3)ユーザが料金を支払わずに映像を閲覧

4.4(4)，(5)で説明したように，信頼できる支払い業者がデータの仲介を行い，映像の受け渡しとともに料金引き落としを行うようにしている．よって，料金を支払わないとユーザは映像を得ることはできない．

(脅威 4)第三者によるユーザなりすまし

4.4(1)で，認証局がユーザに固有の署名鍵を配布し，4.4(2)，(4)，(5)でユーザ映像要求するときや被撮影のとき署名を要求している．よって，署名鍵を持たない第三者が他のユーザに成りすますことはできない．

(脅威 5)サーバによる不正

4.4(1)で，認証局が監視カメラに秘密鍵を設定し，4.4(2)では監視カメラ側で映像の秘匿を行っている．よって，サーバが一時的に受信する映像は暗号化された映像であり，被撮影者のプライバシーは守られているといえる．

(脅威 6)第三者による再送攻撃

4.4(2)で説明したように，署名検証に用いるメッセージである k には乱数を含んでいる．また，モザイク鍵にはタイムスタンプ情報を含んでいるため，第三者が再送攻撃を行うのは困難であるので，安全であるといえる．

(脅威 7) ユーザ同士の結託

4.4(1)より，認証局がユーザに固有の署名鍵を配布し，4.4(2)よりこの署名鍵を用いて署名を生成し，この署名を用いてモザイク生成鍵・暗号化鍵を生成している．よって，モザイク生成鍵・暗号化鍵はユーザ・映像毎に固有であるから，ユーザ同士が結託しても，他のユーザや認証局の秘密情報について得られる情報はないといえる．

(脅威 8)監視カメラの盗難・解析

4.2 より，監視カメラは耐タンパ性を有するという前提を置いている．よって，盗難・解析には耐性を有すると言える．

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]を拡張した新しいサービスの可能性とその通信プロトコルを提案した．これにより，自分の映像を自分以外に秘匿しながら，新たなサービスとして，既存のシステムより優れたサービスが実現できる可能性と，監視カメラを防犯以外の目的に利用できる可能性，結果として監視カメラ本来の防犯能力も高まる可能性を示した．また，被撮影者の意思を尊重して顔の秘匿ができることを示した．今後の展望としては，プロトコルの非効率的な部分の改良を行い，プロトコルが最適化された後は，将来的には実装試験・評価を行うことも検討している．

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] News Up ネットで丸見え？ 防犯カメラ，Jan. 2016,
http://www9.nhk.or.jp/kabun-blog/1000/236100.html
[6]BIGLOBE ニュース，Aug. 2012,
http://news.biglobe.ne.jp/entertainment/0816/jc_120816_9807318879.html
[7]Dan Boneh, Xavier Boyen, Hovav Shacham: Short Group Signatures, CRYPTO 2004, August 15-19, 2004