

# 通学路を死角なく見守る 防犯カメラシステムの実現に向けて

藤井雄作<sup>1</sup>, \*<sup>1</sup>群馬大学大学院理工学府

\* &lt; fujii@e-jikie.com &gt;

[注] 本解説は、(株)日本オプトメカトロニクス協会の承諾に基づく、「藤井雄作, 通学路を死角なく見守る防犯カメラシステムの実現に向けて, 光技術コンタクト, Vol.54, No.2, pp.9-19 (2016).」の転載です。

**要旨:** 本解説では、通学路を死角なく見守る防犯カメラシステムの導入が、全国津々浦々で実現する可能性について議論する。特に、①実現した場合に期待できる効果（犯罪抑止、容疑者追跡・検挙における効果）、について議論する。また、実現させる上で不可欠となる、②導入コスト・運用コストを低減する方法、及び、③一般市民のプライバシー侵害の危険性を排除する方法、について議論する。

## 1. はじめに

平成26年頃から、自治体による、通学路への防犯カメラ導入の動きが出てきた。例えば、東京都では、公立小学校約1300校の通学路に、合計6500台（1校あたり5台）の防犯カメラを導入する計画が発表された。総予算は5年間で24億7千万円（カメラ1台当たり38万円）とのことである。東京都の発表に前後して、他の自治体でも、通学路の見守りの為に、防犯カメラを導入する計画が発表されてきている。「自治体が、通学路の見守りに責任を持つ。その手段として、防犯カメラを用いる。」という考え方は、従来なかったものである。

筆者らの研究グループは、平成27年10月に、全国813自治体（23特別区+790市）に「通学路への防犯カメラ導入に関するアンケート調査」を実施した<sup>1)</sup>。その中で防犯カメラの設置台数について、以下のような結果が得られた（有効回答数393自治体。有効回答率48.3%）。導入済みのものについては、全20144台中、「通学路という側面」を主に考えて設置された台数は1618台（8%）と少数であった。それに対して、計画中のものでは、全3184台中、「通学路という側面」を主に考えて設置を予定している台数は2813台（88%）と大部分を占めた。この結果から、全国の自治体において、「自治体が、通学路の見守りに責任を持つ。その手段として、防犯カメラを用いる。」という考え方が急に、広がってきていることが読み取れる。

ひとたび、「自治体が、通学路の見守りに責任を持つ。その手段として、防犯カメラを用いる」という考え方が「自治体の仕事の一つ」として認識されていくと、次の段階では、より高いレベルでの見守り、より末端の通学路までの見守りを実現することが重要視されるようになって考えられる。通学路は、自治体の居住範囲全域に存在し得るので、その範囲を防犯カメラで死角なく見守ろうとすると、街路灯と同程度の密度で設置することが最低限、必要になる。しかしながら、現時点においては、防犯カメラの設置・運用コストが高い（上記の東京都の例では38万円/台）ことに加え、プライバシー保護の仕組みが技術的・制度的に確立されていないことから、「防犯カメラを街路灯並みの密度か、あるいは、それ以上の密度で設置して、通学路を死角なく見守る」という発想は現実味を持たれにくいと考えられる。

近年、防犯カメラの店舗、繁華街、公共施設等への導入が進み、犯罪容疑者の特定・検挙にあたって、防犯カメラにより記録された映像が役立つ事例が多くみられる。防犯カメラの長所・効用（犯罪抑止に対する効果、容疑者特定に対する効果など）が広く社会に認められつつあるように思われる。それと並行して、社会、一般市民が抱く、防犯カメラのプライバシー侵害の危険性に対する懸念、それに伴う防犯カメラに対する拒否反応も、十数年前と比べて、かなり緩和されてきているように思われる。しかしながら、「防犯カメラを街路灯並みの密度で設置して、通学路を死角なく見守ろう」というレベルになると、プライバシー侵害の危険性について、これまでよりも遥かに厳格な対策が要求されるものと考えられる。例えば、「犯罪発生時に限り、捜査機関に限って、画像を閲覧できる。」ということが厳格に履行され、かつ、一般市民がそのことを心から確信している状況を実現することが要求されるものと考えられる。しかしながら、現時点では、それを実現するための技術的手法・法制度・社会制度は確立されていない。

一方、防犯カメラの容疑者の特定効果・追跡効果について、疑問視する意見も散見されるが、そうした意見の根拠として挙げられるものの多くは、防犯カメラの特性に由来するものではなく、現状の防犯カメラの設置密度、設置台数が余りに小さすぎることに由来すると考えられる。もしも、防犯カメラが、閑静な住宅街を含

む日本全国に、街路灯と同程度の密度で設置されたとしたら、容疑者・容疑車両を、芋づる式に、どこまでも、追跡していくことが可能となる。しかしながら、現状では、防犯カメラの設置密度は、極めて小さく、容疑者・容疑車両の追跡は難しい。

本解説では、通学路を死角なく見守る防犯カメラシステムの導入が、全国津々浦々で実現する可能性について議論する。特に、①実現した場合に期待できる効果（犯罪抑止、容疑者追跡・検挙における効果）、について議論する。また、実現させる上で不可欠となる、②導入コスト・運用コストを低減する方法、及び、③一般市民のプライバシー侵害の危険性を排除する方法、について議論する。

## 2. 通学路を見守るのに適した防犯カメラシステム

「通学路を見守るのに適した防犯カメラシステム」の開発において、重要と思われるポイントである、①犯罪抑止、容疑者追跡の効果を高める方法、②導入コスト・運用コストを低減する方法、及び、③一般市民のプライバシー侵害の危険性を排除する方法、について議論する。

### 2-1 犯罪抑止・容疑者追跡の効果について

犯罪抑止・容疑者追跡の効果を高める方法としては、防犯カメラシステムの高密度設置と、高機能化・高性能化が挙げられる。

防犯カメラの高密度設置は、犯罪抑止・容疑者追跡の効果向上に直結すると考えられる。設置密度がある限度を超えると、犯罪の容疑者は、逃げようがなくなると考えられる。例えば、防犯カメラが、閑静な住宅街を含む日本全国に、街路灯と同程度の密度で設置されたとしたら、犯罪（誘拐、殺人などの凶悪犯罪）の容疑者・容疑車両を、芋づる式に、どこまでも、追跡していくことが可能となる。その際、不鮮明な映像でも人・車の大きな形・影を追えれば、芋づる式の追跡が可能であるので、カメラの画質等は悪くても差支えない。また、高密度設置の場合は、カメラの一部が故障していても問題にならないので、信頼性の低い、安価なカメラでも良いことになる。要所に、顔の特徴、車のナンバーを判別できる程度の高性能なカメラが設置されていれば、より良いということになる。

特に、個々のカメラがインターネット接続された場合には、容疑者・容疑車両の追跡を、迅速に行うことができ、容疑者・容疑車両の現在位置の特定を速やかに行うことが可能となる。誘拐された子供の救助や、徘徊老人の保護も、迅速・確実に行うことが可能となる。そうした追跡は、係員が端末を手動操作する形で行っても良いが、ショッピングモール用に開発されている自動追跡ソフトウェアを利用しても良い。既存技術で、極めて強力な追跡システムを構築することが容易にできる。

このように、防犯カメラが街路灯並みの密度で設置された場合は、「犯罪を犯せば、必ず、追跡され、逮捕される。捕まりたくない人は、犯行を思い止まる。捕まることを気にかけない人の犯行は防げないが、一度の犯行で確実に逮捕されるので、2度目は無いということになる。すなわち、プロの空き巣、痴漢の常習犯などは、存在し得なくなる。」という効果が期待される。これは、極めて強力で有用な社会基盤が出現することを意味する。

防犯カメラの高機能化・高性能化については、様々な研究開発がなされている。通行人の顔と手配写真を照合する技術、不審な動き（痴漢、けんか、落書き、火災、など）を検知する技術、などの画像解析技術が開発されてきている。これら画像解析に関しては、個々のカメラで行う場合もあるが、個々のネットワークカメラからリアルタイム転送された画像をサーバで画像解析する例が多い。また、街路に設置される防犯カメラを、スマート街路灯システム、スマートシティのセンシング回路網の一部として活用することにより、犯罪抑止・容疑者検挙以外に、地域社会の省エネルギー化、利便性の向上、安全・安心の向上にも役立てられると考えられる。

### 2-2 導入コスト・運用コストの低減について

「防犯カメラを街路灯並みの密度で設置して、通学路を死角なく見守ろう」というレベルで、高密度設置を行う場合は、ある割合が故障していても、容疑者追跡効果に影響を与えないので、個々のカメラの信頼性は、それほど、高い必要は無くなる。また、容疑者を「芋づる式」に追跡することができれば良いので、低画質なカメラで良いことになる。このことから、個々のカメラは、低コストなもので良いということになる。追跡の途中、例えば、交差点などに、高画質・高性能なカメラが1台でも設置され、容疑者の顔、容疑車両のナンバーなどを識別できれば良いということになる。

現時点では、個々のカメラから、インターネットなどで、管制室に画像をリアルタイムで転送して録画することは、コストがかかる。その為、住宅街、公園等に設置される防犯カメラの多くは、内蔵したメモリーカードに画像を保存するタイプのものである。メモリーカード内蔵式の防犯カメラ長所としては、設置費用、運用費用が小さいことが挙げられる。短所としては、録画された画像ファイルの取り出しに手間と時間がかかる

ことが挙げられる。すなわち、画像ファイルを取り出すには、カメラからメモリーカードを抜き出す、あるいは、カメラ近くまで行き無線LANなどで画像転送を受ける、という手間のかかる作業が必要となる。

近年、「モノのインターネット (Internet of Things, IoT)」に代表されるように、様々なモノ (家電、自動車、時計、住宅、など) に通信機能を持たせインターネット接続しようという動きが見られる。近い将来、インターネットに安価に接続できる環境が整い、街路灯や街路防犯カメラをインターネットに接続することが一般的になることが予想される。その際においても、撮影された画像は、クラウドやサーバに送られて保存されるのではなく、個々のカメラの内部に保存される形態が主流になると予想される。なぜなら、一般住宅街などの犯罪が少ない比較的安全なエリア (= 市民が生活する大部分のエリア) に設置されたカメラが撮影された画像を閲覧する必要がある機会は、非常に少なく、殆ど使われることない大きな画像ファイルを常時転送し続けることは通信の無駄使いと考えられるからである。個々のカメラは、通常時は、メンテナンス等に必要小さな容量の通信のみを行い、犯罪捜査などの際にのみ、保存した画像ファイルの送出手間を行うことになる。これにより、インターネットの通信量を大幅に節約できる。こうした運用形態の防犯カメラシステムに適した、インターネット接続サービスが提供されることが期待される。

自治体により設置・運用される防犯カメラとしては、自治体により設置・運用されることが多い街路灯と同じ要領で、設置・運用できるタイプの防犯カメラが適していると考えられる。工事費用節減の観点から考えると、メモリーカード内蔵型カメラを内蔵したLED街路灯が、優れていると考えられる。例えば、市販のLED街路灯 (実売価格5千円~2万円程度) と市販のドライブレコーダ (実売価格5千円~1万円程度) と同程度の機能を有するものを合体させ、大量生産することで、街路灯並みの価格の「メモリーカード内蔵型カメラを内蔵したLED街路灯」が実現できると考えられる。

一般市民に、住宅の回り、車の回り、身の回り、の見守りにボランティアとして協力してもらうことは、見守りに係わる社会コストを低減させる上で有効であると考えられる。一般市民による運用に適したカメラとしては、常時録画タイプのTVドアホン、住宅内蔵カメラ、車載カメラ、ウェアラブルカメラ、などが考えられる。特に、後述の常時録画タイプのTVドアホン (e自警ドアホン) は、町内の見守りを低コストで実現する上で、有効であると考えられる。

### 2-3 プライバシー保護について

前述のように、街路灯並みの密度で防犯カメラが設置されることは、犯罪の容疑者を確実に追跡することが可能になることを意味し、極めて強力な社会基盤が出現することを意味する。しかしながら、これは、同時に、悪用によるプライバシー侵害の危険性が飛躍的に増大することを意味する。この危険性を完全に除去することが、このような社会基盤が社会に受け入れられる必要条件になると考えられる。すなわち、性悪説に立脚した手法による「防犯カメラシステムの悪用防止」が確実に保証され、かつ、一般市民がそのことを心から確信している状況を実現することが要求されるものと考えられる。

悪用の防止方法については、第三者による悪用の防止方法と、運用者による悪用の防止方法の2つについて、考える必要がある。画像データを不正に入手しようとする第三者による悪用を防止する方法としては、画像データを暗号化して保存することや、画像のやり取りを行う通信を暗号化することなどが考えられる。市役所・警察署の担当職員など画像の閲覧権限を持つ運用者による悪用を防止する方法としては、画像の閲覧履歴を何らかの方法で確実に記録し、正規の業務命令に基づく閲覧行為であるか否かを、事後、あるいは、リアルタイムで確実にチェックできる体制を作ることが考えられる。

今後、個々の一般市民が家屋の周り (家屋設置カメラ)、車の周り (車載カメラ)、身の回り (ウェアラブルカメラ) を見守ることが、コスト的に容易に出来るようになってくると考えられる。個々の市民のボランティア的な協力により、通学路、住宅街などの市民の活動エリア全体を見守る事は、見守りに要する社会コストを削減する上で有効であるが、同時に、社会的に許容される利用範囲が厳密に定められ、それに対する違反・悪用が厳格・確実に取り締まられることが求められてくると予想される。

「防犯カメラシステムの悪用防止」が確実に実現した場合、そのことを、一般市民に心から確信してもらえようにする必要がある。現状では、自治体の条例等により、防犯カメラの運用ガイドラインなどが制定され、その中で、画像閲覧を防犯目的に限定することや、「防犯カメラ動作中」の掲示をすることなどが義務付けられている。これらは、運用者がルールを守ることを前提とした性善説に立脚した手法であると言える。しかし、近い将来に実現するであろう「街路灯と同程度かそれ以上の密度で、自治体、企業、一般市民などにより設置された防犯カメラで見守られる社会」においては、前述のように、性悪説に立脚した厳格な悪用防止の方法が要求され、そのことを周知する方法としても、より信頼性が高い方法が要求されると考えられる。

今後、爆発的に増えることが予想される防犯カメラの効用を最大化し、かつ、悪用を確実に防止するには、公共スペースを撮影する全てのカメラには登録を義務付けることが有効であると考えられる。例えば、カメラを設置・運用したい者は、カメラの設置位置、運用方法を申請し、許可を受ける必要があるという社会制度の

実現が望まれる。画像の適正利用の範囲が法制度等により定められ、その範囲でのみ画像利用を可能とする技術的・社会的な仕組みが構築されることが必要になると考えられる。

公共スペースを撮影する全てのカメラが登録されることになった場合には、歩行者が持つスマートフォンの画面に、近隣のカメラの位置・素性（＝運用者や運用方法に関する情報）を示した地図が表示されるようにすることも考えられる。また、登録されていない不正に設置されたカメラを見つけ出す手法の開発も望まれる。

### 3. 開発事例

ここでは、「防犯カメラが、街路灯並みに、高密度・大量設置された社会」の実現を目指して、筆者らが中心となって開発してきた防犯カメラシステムについて紹介する。これまで、社会実験、企業との共同研究などを通して、前述の①犯罪抑制効果・容疑者追跡効果の向上、②設置コスト・運用コストの低減、③プライバシー保護の徹底、の中で、特に、「防犯カメラが、街路灯並みに、高密度・大量設置された社会」を実現する上でのキーであり、また、未解決の大きな問題でもあると考えられる、③一般市民のプライバシー侵害の危険性を排除する方法、に関する研究開発に取り組んできた。

#### 3-1 閲覧権に応じて閲覧画像の不鮮明度を調整する機能<sup>2)</sup>

自治体による住宅街・通学路等の見守りにおいて、内蔵メモリーカードに録画する方式の防犯カメラが、しばしば利用される。その際、不正にメモリーカードを入手した第三者による悪用を防止する上で、自治体の担当者等の運用者が暗号化キーを設定し、画像を暗号化して保存することは有効な手段である。その際、メンテナンス会社に対して、暗号キーを開示するか否かが、問題になる。暗号キーを開示しない場合は、メンテナンス会社の担当社員は、動作確認の為に画像閲覧を行うことが出来ず、メンテナンス上の問題が生じる。一方、暗号キーを開示する場合は、メンテナンス会社の担当社員は、画像閲覧を自由に出来てしまい、プライバシー保護上の問題が生じる。

そこで、暗号化キー（Key-A）に加え、不鮮明化強度設定キー（Key-B）を導入し、閲覧権に応じた不鮮明化処理を施した上で、画像を出力する方法を考案した。画像ファイルと不鮮明化強度設定キー（Key-B）を結合し、これを、暗号化キー（Key-A）により暗号化する。これを復号化するには、閲覧ソフトウェアで、暗号化キー（Key-A）により復号化し、画像ファイルと不鮮明化強度設定キー（Key-B）を分離し、画像ファイルに対して、不鮮明化強度設定キー（Key-B）で規定される不鮮明化処理を施した上で出力する。暗号化方式自体は、既存の手法を使うことができる。この手法により、閲覧権に応じて、閲覧画像の不鮮明度を調整することが可能になる。

この機能を導入した防犯カメラとして、「e自警カメラ（有限会社マツダ商事製）」が開発された<sup>3-7)</sup>。このカメラは、①プライバシー保護の徹底、②低コスト（低導入コスト、低運用コスト）の両立を目指して開発された暗号化保存機能が有るAll-in-one型の防犯カメラシステムである。特徴は、以下のようである。

- (1) 低コスト：メモリーカード内蔵式のAll-in-one型なので、電源工事のみで、モニター室等への配線工事が不要となる。これにより、工事・運用の低コスト化を実現できる。
- (2) 常時、最新の1週間分の画像がSDカードに上書き保存される。
- (3) プライバシー保護機能の強化：画像は、2つの暗証キーKey-AとKey-Bにより、暗号化されて保存される。
  - Key-Aのみだと不鮮明処理（モザイク化処理）された画像のみ閲覧可能となる。
  - Key-AとKey-Bの両方があれば、鮮明な画像が閲覧可能となる。
  - メモリーカードを不正に取得した者（暗証キーを持たない者）は画像の閲覧が出来ない。

このe自警カメラを用いて社会実験が、群馬県太田市西本町において、太田警察署、区長（西本町地区の区長）、及び、筆者らの研究グループにより実施されている。各人の役割は、以下である。

#### 【太田警察署】

- 暗証キー（Key-AとKey-B）の設定を行う。
- 画像ファイルの提供を受けられた場合は、専用閲覧ソフトに暗証キー（Key-AとKey-B）を入力することにより、鮮明な画像を閲覧可能である。

#### 【西本町地区の区長】

- カメラ、画像ファイルの管理を行う。
- Key-Aのみ、太田警察署から開示されている。メンテナンス目的で、専用閲覧ソフトにKey-Aを入力することにより、モザイク化処理が施された不鮮明な画像を閲覧出来る。
- 事件・事故が発生したときのみ、画像ファイルを太田警察署に提供する。

#### 【筆者らの研究グループ】

- 暗唱キー (Key-A と Key-B) は知らされていない。
- デモ用として関係者がカメラの前に立って撮影された画像については、太田警察署、区長の協力を得て、暗号が解除された鮮明な画像として入手することができる。

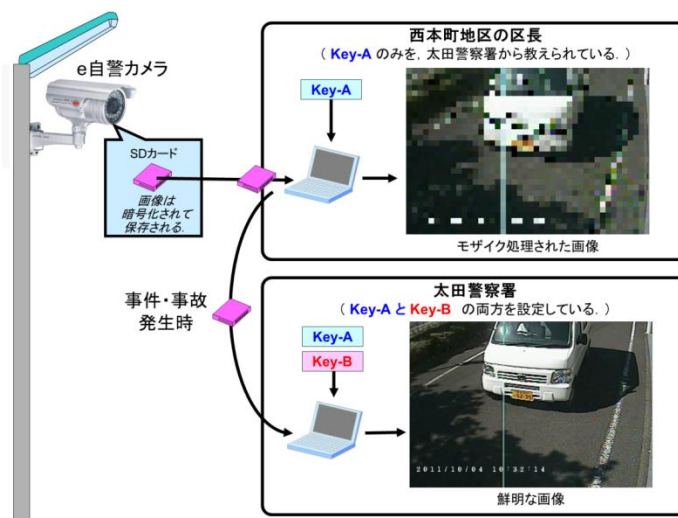


図1 太田市西本町の社会実験における閲覧権の設定方法  
e自警カメラ (=閲覧権に応じて閲覧画像の不鮮明度を調整する機能を搭載した防犯カメラ)  
を活用したプライバシー保護の取り組み

上記のe自警カメラのように、ネットワークに接続されていないメモリー内蔵型カメラの場合は、カメラ内に保存された「画像ファイル」を取り出すには、作業者が、カメラのところまで行く必要があることにより、理由もなくカメラから画像を取り出すことが、非常にやりにくい状況が作られている。すなわち、市役所の担当職員が、画像ファイルを手に入れるには、メンテナンス業者等に対してメモリーカード抜出作業の発注を行う必要がある。このことから、運用者による画像ファイルの取り扱いが可視化されており、運用者による悪用の危険性は低いと考えられる。しかし、より厳格なプライバシー保護の実現のためには、さらに、様々な技術的な工夫、運用上の工夫、社会制度的な工夫、をしていくことは有効であると考えられる。

この「閲覧権に応じて閲覧画像の不鮮明度を調整する機能」は、この他、e自警カメラ(株式会社ミツバアピリティ製)、e自警灯(株式会社トステック製)にも搭載されている<sup>1)</sup>。これらのカメラは、自治体による通学路の見守りを、前述の②低コストと③プライバシー保護を両立させた形で実現する上で、有用であると考えられる。

### 3-2 常時録画型TVドアホン

一般市民による自宅回りの見守り、及び、それを活用・組織化することによる地域社会の安全・安心の向上に適した防犯カメラとして、常時録画型TVドアホン「e自警ドアホン」が、群馬大学と株式会社ロッキーの共同研究の成果として生まれた<sup>8)</sup>。e自警カメラ(プライバシー保護機能付き防犯カメラ)の機能を内蔵したTVドアホンである。e自警ドアホンは、以下のような特徴を有する。

- (1) **通常のTVドアホンとしての機能**：呼出ボタンが押された時は、通常のTVドアホンと同様に、通常形式で録画される。住人が閲覧できる。(通常のTVドアホンとしての機能は全て有する。)
- (2) **e自警カメラとしての機能**：呼出ボタンが押されていない時も、常時録画(24時間録画)される。ただし、暗唱コード(パスワード)で暗号化された上でメモリーカードに保存される。画像の閲覧には、専用ソフトウェアと暗唱コードが必要となる。e自警ドアホンと画像の所有者と、暗唱コード設定者(閲覧権者)を、別人とした運用を行うことができる。例えば、一般住民がe自警ドアホンを所有・運用し、自治会・捜査機関等が暗唱コード設定者(閲覧権者)となることで、一般市民のプライバシーを守った運用が可能になる。また、事件・事故の発生に際しては、住民から、自治会・捜査機関等に画像ファイルが提供されることで、地域の安全・安心の向上が図れる。
- (3) **低コスト**：e自警ドアホンの室内ユニットと室外ユニットは2本の導線で接続する方式としている。既設の呼び鈴・ドアホンの配線を利用できるため、交換の際、新たな配線工事は不要である。このため、既設の呼び鈴・ドアホンとの交換工事は、簡便・安価に行うことができる。

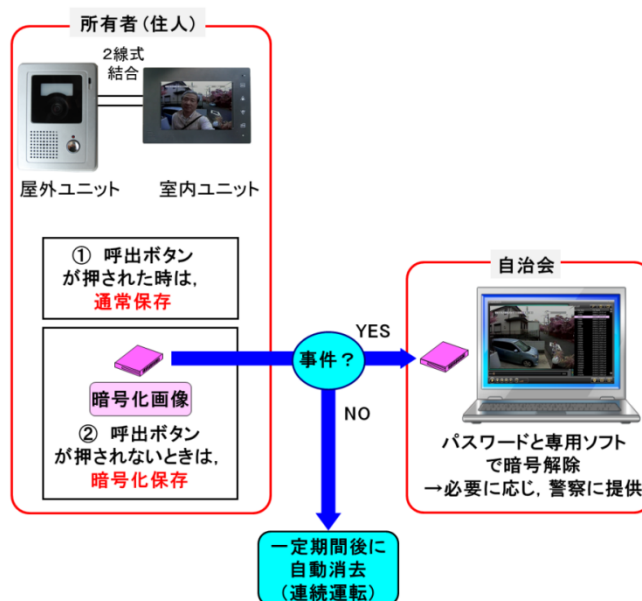


図2 愛知県尾張旭市の社会実験における閲覧権の設定方法  
e自警ドアホン(=e自警カメラの機能を搭載した常時録画型TVドアホン)を活用した、住民ボランティアにより、地域社会のきめ細かな見守りを実現する取り組み

現在、e自警ドアホンの試作機(79台)を用いた社会実験を、愛知県尾張旭市旭丘連合自治会(加入世帯数:2262世帯)において、平成27年1月から実施している。旭丘小学校の校区(全2705世帯)の犯罪発生件数は、e自警ドアホン(79台)を設置前の平成26年の62件と比べ、設置後の平成27年は21件と、66%も減少した。これは、e自警ドアホンを設置ことによる効果が、大きいと考えられる。今後、試作機を用いた社会実験エリアは愛知県内、東京都内を中心に拡大し、平成28年度中に約400台に増やす予定である。なお、これらe自警ドアホンを用いた社会実験で使用する機材(e自警ドアホン)は、全て、開発・製造元の株式会社ロッキーから無償提供されたものである。

自治体、町内会等の主導の下で、一般市民がe自警ドアホンにより自宅周りを見守ることで、地域社会のきめ細かな見守りを低コストで実現でき、かつ、プライバシー保護も高いレベルで達成できると考えられる。

### 3-3 閲覧行為の完全な記録

近未来の日本全国の市街地においては、街路灯程度の単価のネットワークカメラ、あるいは、街路灯内蔵型のネットワークカメラが、街路灯並みの数量・密度で設置され、それらが、インターネットに接続され、各カメラで撮影・保存されている画像ファイルへの迅速なアクセスが可能になると予想される。日本全国において、不審者、容疑者、容疑者車両に対する、閲覧装置を用いた手動操作による追跡、あるいは、ソフトウェアによる自動追跡が、技術的にも、経済的にも、容易に実現可能になると予想される。

そうした「インターネット接続されたカメラが、街路灯並の密度で、いたるところに設置された近未来」の世界においては、例えば、子供が誘拐される事件が発生した場合、まず、家族からの通報を受けた警察の担当職員が閲覧用の端末を操作し、子供の家の前(あるいは周辺)に設置されたカメラに記録された画像を調べる。子供が家を出ることが確認されたら、そこから、芋づる式に、カメラを順次切り替えながら、追跡していく。子供が車両に載せられた場合は、当該車両を、同様に、芋づる式に、追跡していき、現在位置を特定する。そして、パトロールカーを向かわせ、子供を救出する。ということが、簡単に、当たり前のように、できるようになると予想される。これは、「素晴らしい社会基盤」になり得ると考える。

しかし、そうした社会において、画像にアクセスする権限のある人間、例えば、市街地カメラを管理・運営する市役所の担当職員が、私的な動機で、システムを悪用する可能性が重大な問題となる。例えば、特定の女性・男性の行動を、閲覧端末を操作して、カメラを切り替えつつ手動で追跡するストーカー行為、特定の個人の動きを自動追跡ソフトを使い追跡・記録する行為、などが挙げられる。こうした不正な使用が出来ないようにする仕組みが、不可欠になる。こうした危険性がそのままでは、折角の「素晴らしい社会基盤」が、社会に受け入れられることが難しくなると危惧する。

それに対する答えの一つとして、新しいコンセプト「閲覧行為の完全な記録」が提案された<sup>9,10)</sup>。本提案に基づくカメラシステムにおいては、例えば、市役所の担当部署が市街地に設置・運営する膨大なカメラから、

インターネット経由で画像を取得・閲覧する際に、市役所の担当部署ではない、信頼できる第三者により管理・運営される記録サーバからの許可が必要になる。記録サーバは、「どの閲覧者に、どの画像を、どの不鮮明度での閲覧を許可したか」を、確実に記録する。そして、その記録した情報を、その場で、あるいは、後日、業務命令と照合することにより、業務命令以外の不正な悪用を確実に検出することが可能となる。こうして、全ての閲覧行為が完全に記録され、その場で、あるいは、後日、業務命令と照合されることにより、悪用は確実に発覚することになり、「業務と関係がない閲覧行為」は、強力に抑制されることになる。

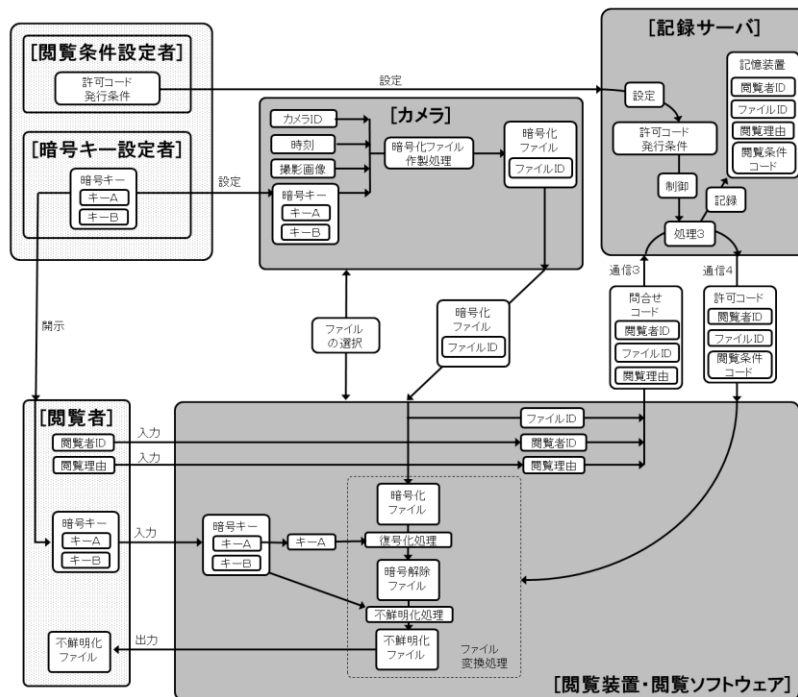


図3 閲覧行動の記録の仕組み：カメラ＝閲覧装置＝記録サーバ間のデータのやり取り

本コンセプト「閲覧行為の完全な記録」を形にするために、e自警ネットカメラ（試作システム）を開発した。試作したカメラシステムは、小型コンピュータボード（Raspberry Pi 2）を内蔵したカメラユニット8台、閲覧装置（閲覧ソフトウェアをインストールしたPC）3台、および、記録サーバ（埼玉大学内）1台から成る。8台のカメラユニット（撮影画像は暗号化された上で各カメラ内のメモリーに保存。相互にLAN接続し、WiMAX経由でインターネットに接続。）は実証実験サイト（群馬県桐生市末広町「末広みらいパーキング」敷地内）に、設置した。図3に、e自警ネットカメラ（試作システム）に関する実証実験における閲覧行動の記録の仕組みを示す。

e自警ネットカメラは、以下の特徴を有するカメラシステムである。

- (1) カメラで撮影され暗号化された画像ファイルを、入手、あるいは、開く際に、記録サーバから発行される許可コードが必要となる。
- (2) 記録サーバは、許可コード発行要請に対して、予め定められた許可コード発行条件で、許可コードを発行する。
- (3) 記録サーバは、許可コード発行要請の受付から、許可コード発行までの過程における、カメラ ID、画像ファイル ID、閲覧者 ID、許可コード発行時刻、発行した許可コード、などの情報を記録する。

上記の仕組みにより、閲覧者が閲覧装置を使って、各カメラに保存された画像ファイルを閲覧しようとする行為は、全て、記録サーバに記録されることになる。一方、記録サーバは、画像ファイル、暗号キーに触れることは無く、機械的に、予め定められた規則通りに、許可コードを発行し、その過程を記録することに徹することになる。

記録した閲覧記録の使い方としては、その場で、あるいは、事後において、業務命令に基づく閲覧行為であるかの照合に使うことが考えられるが、今回の実証実験では、閲覧記録を全て、ウェブサイト上に一般公開することとした<sup>11)</sup>。一般に、防犯カメラの前を通る人は、「強制的に撮影」される。強制撮影とバランスを取る目的で、上記の実証実験においては、防犯カメラが撮影した映像を閲覧する人に対しては、「閲覧行為を、強制的に一般公開」するようにした。「強制的に、撮影される」ことに対して、「強制的に、閲覧行為が公開される」とすることでバランスを取るという考え方である。この考え方を拡張すると、例えば、自治体が運用す

る全ての防犯カメラの閲覧記録は、閲覧命令との整合性のチェックがなされるだけでなく、そのチェック過程も含め、全て、公開されるという運用方法も考えられる。これにより、一般市民は、運用者の悪用により、プライバシーが侵害されることに対する不安感を払拭できると考えられる。

提案するコンセプト「閲覧行為の完全な記録」は、ネットワークカメラ（e自警ネットカメラ、など）に限らず、前述のインターネットに接続しないスタンドアロン型カメラ（e自警カメラ、e自警灯、e自警ドアホン、など）に対しても、適用することができる。

提案するコンセプト「閲覧行為の完全な記録」は、通学路を含むあらゆる公共スペースを、防犯カメラがきめ細かく、死角なしに見守るようになる近未来において、一般市民のプライバシー保護の為に必須の要件の一つとなると考えられる。

### 3-4 カメラの素性に関する自己紹介機能

防犯カメラの前を通る行人は、防犯カメラにより強制的に撮影される。行人には、当該防犯カメラの素性（管理者、設置場所、運用方法、プライバシー保護などに関する情報）を知る権利があると考えられる。現時点においては、「防犯カメラ作動中」等の掲示により、防犯カメラの存在・素性を知らしめることが、条例等で義務付けられている。近い将来、防犯カメラの低価格化・高性能化により、防犯カメラの繁華街・住宅街への高密度設置が進み、屋外のあらゆる所で、防犯カメラによるきめ細かな撮影・録画が行われることが予想される。行人（被撮影者）の知る権利を、より確実に守る方策が求められてくると予想される。

行人（被撮影者）の知る権利を、より確実に守る方法として、防犯カメラの素性（管理者、設置場所、運用方法、プライバシー保護などに関する情報）を、防犯カメラ自身が、行人の携帯電話に知らしめる機能（＝自己紹介機能）を発明<sup>12)</sup>・開発し、先述の自警ネットカメラ（試作システム）に導入した。

図4に、自己紹介機能を説明するための模式図を示す。実証実験サイトにおける動作は、以下のようである。

- (1) スマートフォン画面の地図上に、近隣に設置された防犯カメラの位置が、グループ毎に色分けされて表示される。
- (2) スマートフォン画面の地図上に表示されたカメラを選択すると、当該カメラの素性（管理者、設置場所、運用方法、プライバシー保護などに関する情報、管理者の説明サイトのURL、など）が、表示される。
- (3) 近隣に設置された防犯カメラとの通信は、ブルートゥースで行われる。通信を行う最初の段階で、防犯カメラの真贋判定が行われる。試作機では、本物と判定された場合のみ、地図上にカメラの位置を表示する設定となっている。将来的には、偽物を見つけた場合に、通報するなどの機能を追加することもできる。
- (4) より詳しい情報を得る目的で、管理者の説明サイト（ホームページ）を閲覧することもできる。

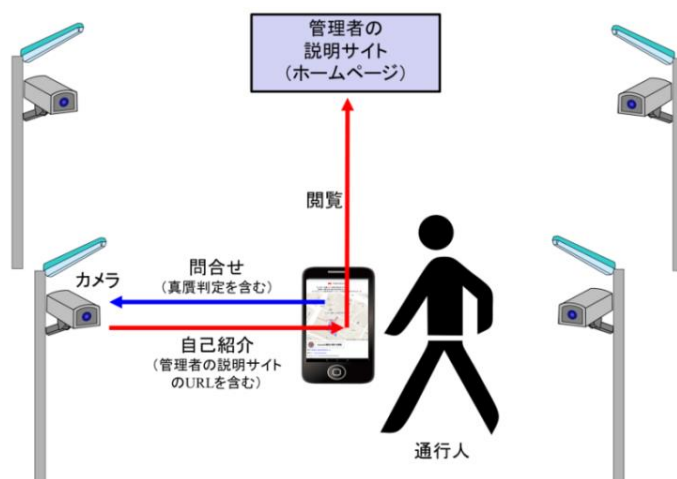


図4 自己紹介機能付カメラシステム

ここで提案した自己紹介機能は、公共スペースを撮影する全てのカメラに対する登録制度ができた場合に、特に、有効に機能すると考えられる。全てのカメラが、登録制度の中で定められた共通の様式で通信を行い、自己紹介することで、各カメラ管理者の運用方法の通知、及び、不正に設置されたカメラの検出、などを容易に実現できるようになる。近い将来、公共スペースのあらゆるところが、高密度に設置された防犯カメラにより、きめ細かく見守られるようになる際に、この自己紹介機能は、一般市民の知る権利を保護する上で、必要な要件の一つとなるものと考えられる。



#### 4. おわりに

本解説では、通学路を死角なく見守る防犯カメラシステムの導入が、全国津々浦々で実現する可能性について議論した。①実現した場合に期待できる効果（犯罪抑止、容疑者追跡・検挙における効果）については、「容疑者・容疑車両の確実な追跡が出来る社会」を実現でき、非常に強力な社会基盤が出現するであろうことを示した。

また、実現させる上で不可欠となる、②導入コスト・運用コストを低減する方法、及び、③一般市民のプライバシー侵害の危険性を排除する方法、について議論した。②導入コスト・運用コストを低減する方法については、街路灯並みの低コストで設置できる可能性があることを示した。③一般市民のプライバシー侵害の危険性を排除する方法については、今後、厳格なプライバシー保護が要求されるであろうこと、及び、そのための方策について議論した。

ごく近い将来、凶悪な犯罪事件の容疑者が、速やかに特定・追跡・逮捕される社会が実現することを願っている。さらには、誘拐事件において、誘拐された子供が、速やかに救出される社会が実現することを願っている。

#### 謝辞

本解説で紹介した研究の多くは、科学技術研究費補助金・基盤研究（B）（課題番号19300239、課題番号21300268、課題番号24300246、課題番号15H02887）の助成によるものである。

#### 参考文献

- 1) 特定非営利活動法人 e 自警ネットワーク研究会: <http://www.e-jikei.org/>
- 2) 特許第 5840804 号, “暗号化された画像を閲覧権者に応じた強度の不鮮明化処理を施した画像を出力することを特徴とする画像暗号化システム” .
- 3) Y. Fujii, N. Yoshiura, N. Ohta, “Creating a Worldwide Community Security Structure Using Individually Maintained Home Computers: The e-JIKEI Network Project” *Social Science Computer Review*, Vol. 23, No. 2, pp.250-258 (2005).
- 4) Y. Fujii, N. Yoshiura, N. Ohta, “Community Security with Widely Available Information Technology” *Journal of Community Informatics*, Vol. 2, No. 1, pp. 68-70 (2005) .
- 5) 丸浩一, 藤井雄作, 杉田陽市, 太田直哉, 吉浦紀晃, 上田浩, 白木慎也, “利他主義と情報技術による地域社会の安全化 e 自警ネットワーク実現に向けたシステムの導入と展望”, *建築学会総合論文誌*, No. 8, pp. 99-104 (2010).
- 6) Y. Fujii, N. Ohta, H. Ueda and Y. Sugita, “New Concept Regarding Management of Security Cameras”, *Journal of Community Informatics*, Vol. 4, No. 3, 2008.
- 7) 藤井雄作, 防犯カメラの高密度・大量設置による安全・安心な社会の実現にむけて, *光技術コンタクト*, Vol.50, No.9, pp.29-38 (2012).
- 8) 特許第 5481632 号, “監視カメラシステム及びその運用方法” .
- 9) 特願 2015-167298, “プライバシー保護を可能とするカメラシステム” .
- 10) Y. Fujii, N. Yoshiura, N. Ohta, A. Takita, H. Ueda and K. Maru, “Abuse prevention of street camera network by browsing-history disclosure”, *Journal of Community Informatics* (in press).
- 11) 実証実験に関する情報開示サイト: <http://www.e-jikei.org/site/exp.htm>
- 12) 特許第 5757048 号, “所有者, 画像閲覧可能な者を知らしめる情報開示手段を持つことを特徴とする防犯カメラシステム” .



藤井雄作 FUJII, Yusaku

群馬大学大学院理工学府

(特定非営利活動法人 e 自警ネットワーク研究会 理事長)

1991年3月東京大学大学院工学系研究科修士課程修了。2001年東京大学より博士（工学）の学位修得。川崎製鉄株式会社, 工業技術院計量研究所, 産業技術総合研究所を経て, 現在群馬大学理工学府教授。2004年よりNPO法人e自警ネットワーク研究会理事長, 精密計測, 防犯カメラシステムなどが専門。