平成 29 年度　修　士　論　文

e 自警ネットカメラの知能化に関する研究

～駐車場での違法駐車の検知，および通報機能の開発～

指導教員：藤井雄作　教授

群馬大学大学院電子情報・数理教育プログラム

上岡　健太

第 1 章　序論

1.1　研究概要と目的

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，犯罪の容疑者の特定・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．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．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よりもむしろ，防犯カメラの設置台数の少なさや，設置密度の低さ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[1]．その一方で，防犯カメラの高密度な設置を妨げる要因として，導入コスト，一般の防犯カメラの場合は効果範囲，プライバシーの侵害に関する問題の 3 点があげられる[2]．

まず，導入コストについてであるが，通常，事件の解決に役立つ，鮮明な証拠画像を提供できる防犯カメラは非常に高価である．また防犯カメラと監視室をケーブルで結ぶには大規模な工事を伴う．結果として防犯カメラの導入と運用の両面で非常に高いコストがかかっているのである．

次に，防犯カメラの効果範囲についてだが，防犯カメラを用いたシステムは一般に，所有者の敷地内を監視し，自衛の手段として運用されていることが多数であり，敷地以外で起こる犯罪に対しての効果は期待できないことである．そのた

め，児童の誘拐や通り魔，放火などの犯罪が，道路などの公共の場所，つまり個人の敷地の外で起こっても気づかないことが多い．

最後に，プライバシーの侵害に関する問題については，防犯カメラが公共の空間を撮影した場合，その特性上隣人や通行人などの一般市民を無差別に撮影・録画することで，一般市民のプライバシーを侵害してしまう恐れがある．

公共空間を監視する防犯カメラの導入には，解決するべき問題が存在するのは事実だが，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，東京都では都内の公立小学校全 1300 校の通学路に防犯カメラを取り付ける事業を開始した[3]．設置するカメラは全 6500 台にのぼり 1 校あたりの通学路に 5 台を設置する計画が発表された．しかし，1 校あたり 5 台というのは極めて少なく通学路全体を見守ることは難しい．以上のことから，防犯カメラを導入しようとすれば，設置費用と運用コストが高額であり，また所有者の敷地外に向けて設置したときに他人のプライバシーを侵害してしまう可能性が発生し，導入するのは難しいのが現状である．そこで，我々の研究室ではこれらの問題点を解決し，地域社会の安全に貢献できる防犯カメラシステムを開発し，広く普及させ，安全・安心な地域社会を実現することを目指して研究を行っている．そのような安全・安心な地域社会を実現のために，我々は「e 自警ネットワーク」というコンセプトを考案している．e 自警ネットワークでは，犯罪に対して，目撃情報が無いことが有り得ない社会，なおかつ映像が使われるのは事件が発生した場合のみで，一般市民のプライバシーは厳重に保護される社会を目指している．e 自警ネットワークを普及させ，防犯カメラで，死角なく見守られ，一般市民のプライバシーは厳重に保護される地域社会のモデルケースを作成し，それをもとに e 自警ネットワークを普及させ，安全・安心な世の中の実現を目的として研究を行っている．

1.2　e 自警ネットワーク

e 自警ネットワーク研究会（以下「研究会」）では，近年，急速に発達している情報技術を用いて，地域コミュニティの再現を目指している[4]．その具体的な内容が e 自警ネットワークの普及である．かつての地域コミュニティでは，人の目で監視を行い，事件事故や犯人などを頭で記憶することで一人一人が協力し合って地域の安全を守ってきた．しかしながら近年では，地域社会のつながりが弱くなってきており，地域コミュニティの相互監視機能が失われつつある．そこで研究会では，この監視するための目にあたる部分をカメラで代用し，記憶する頭にあたる部分をパソコンで代用することにより，現代に合わせた形でかつての地域コミュニティの相互監視機能を再現できると考えた．この新しい防犯カメラネットワーク(=e 自警ネットワーク) を普及させ，各個人がそれぞれ防犯活動を行うのではなく情報技術を用いながら協力し合うことで，かつての日本が持っていた地域コミュニティの相互監視機能を取り戻すことを目指している[5-7]．e 自警ネットワークのコンセプト説明図を図 1.1 に示す．

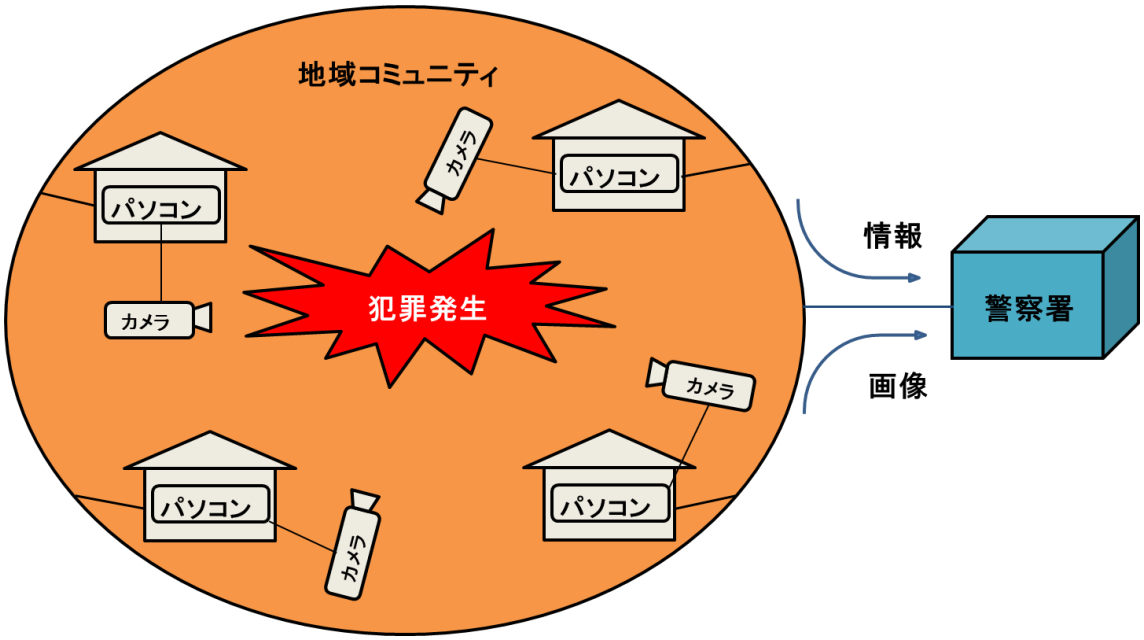

図 1.1 e 自警ネットワークのコンセプト

図 1.1 の e 自警ネットワークのコンセプト図では，各々の家が防犯カメラを設置し，自分の家の敷地内だけでなく，地域のために自分の家の前も防犯カメラで撮影する．事件・事故等が発生した場合には，警察等の要請に応じて，防犯カメラの画像を提供する．すべての家が防犯カメラで家の周囲を見守っていれば，事件・事故の容疑者の特定だけにとどまらず，容疑者がどこへ逃走したのか，どこまでも追跡することが可能であるというものである．

e 自警ネットワークは，以下のコンセプトにより構成される．

コンセプト A：情報技術を活用し，一般市民が身の回りを確実に見守る社会の実現

コンセプト B：暗号化保存による一般市民のプライバシーの確実な保護の実現

コンセプト A は，広く普及した情報技術を用いることで，一般市民の協力により，地域の隅々まで見守られる社会を実現しようというものである．コンセプト B は，撮影した画像を暗号化し保存することにより，プライバシーの侵害の問題を解消するというものである．また，画像を暗号化することで，カメラの設置者と画像の閲覧権者を細かく設定することを可能にするというものである．

研究会では，e 自警ネットワークの普及を通して，「犯罪者が逃げられない社会」，「誘拐された子供が，救出される社会」を全国の地域社会で実現することを目指している．

1.3　e 自警ネットワークにおけるプライバシー保護

1.3.1　暗号化によるプライバシー保護

我々の研究室では，過去に暗号化保存機能が無い防犯カメラシステムを用いて社会実験等を行ってきた．プライバシーの保護については，防犯カメラ運用ガイドラインを設けるという手段を用いていた．しかし，防犯カメラ運用ガイドラインの設定だけでは，プライバシー侵害の懸念が払拭されない事例が多く発生していた．そこで，それを解決する手法として，画像を暗号化保存することにより，画像の「所有者」と「閲覧者」を区別した運用を行うという，新しいコンセプトを考案した．このプライバシー保護のコンセプトを図 1.2 に示す．

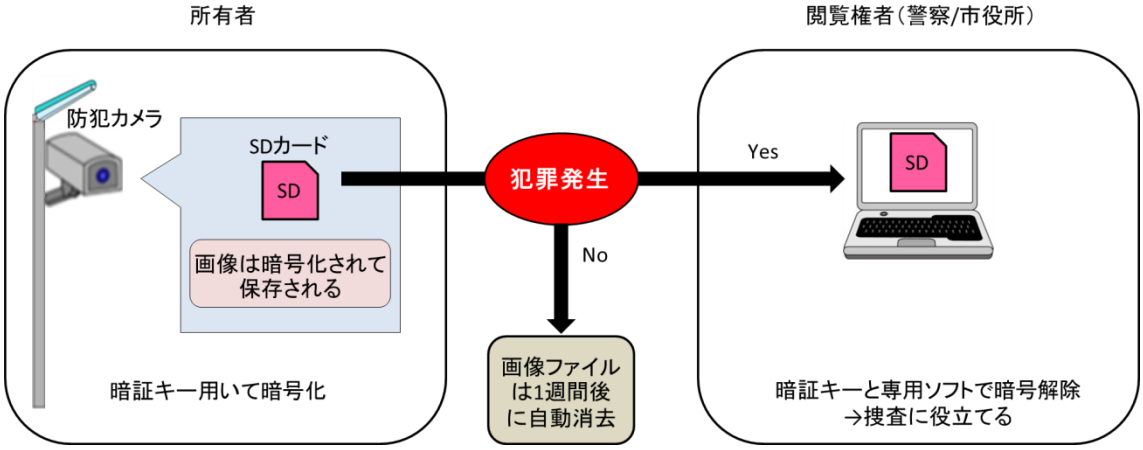

図 1.2 プライバシー保護のコンセプト

図 1.2 において，撮影され暗号化保存された画像の所有者は防犯カメラの設置者である．また，暗号化された画像を暗証キーと専用のソフトで暗号解除し閲覧することが出来る閲覧権者は，警察などの捜査機関や市役所の職員となる．本コンセプトでは，暗号化および暗号解除するための「パスワード」は閲覧権者に決めてもらい保存画像の所有者（防犯カメラの設置者）はパスワードを知らないというシステムになっている．そのため，保存画像の所有者は，画像を閲覧することが出来ない．一方で，閲覧権者は暗号化解除をするための暗証キーと専用のソ

フトウェアを所有する．これにより，万一，SD カードの盗難が発生した場合でも，画像が悪用される心配はない．そして，保存画像の所有者は，事件があった時に警察等の閲覧権者から画像の提供を要請された場合でも，その内容によっては拒否する権利があり，閲覧権者の権利の濫用を防いでいる．これにより保存画像の所有者と閲覧権者の双方が同意して初めて暗号化が解除され，閲覧可能となる．このように，撮影された画像の「所有者」と，閲覧する権利を持つ「閲覧権者」を分離することによってプライバシーの保護を考慮したシステムを実現してきた[8-10].

1.3.2　二重暗号化によるプライバシー保護

前節のプライバシー保護のコンセプトでは，暗証キーと専用のソフトを持つもの（閲覧権あり）は画像を閲覧することができ，暗証キーと専用のソフトを持たないもの（閲覧権なし）は画像を閲覧することができないという，2 通りの閲覧権しか設定できなかった．しかし，この運用方法では実用上不便なことが分かった．それは，防犯カメラの管理業者（メンテナンス業者等）は，暗証キーと専用のソフトを持たないため，保存画像の確認が全くできないということである．この問題の解決のため，暗証キーを 2 つ（Key-A と Key-B）として画像を暗号化保存することにより，閲覧の手段をより細かく設定できる二重暗号化機能を考案した．図 1.3 に二重暗号化の概念を示す．

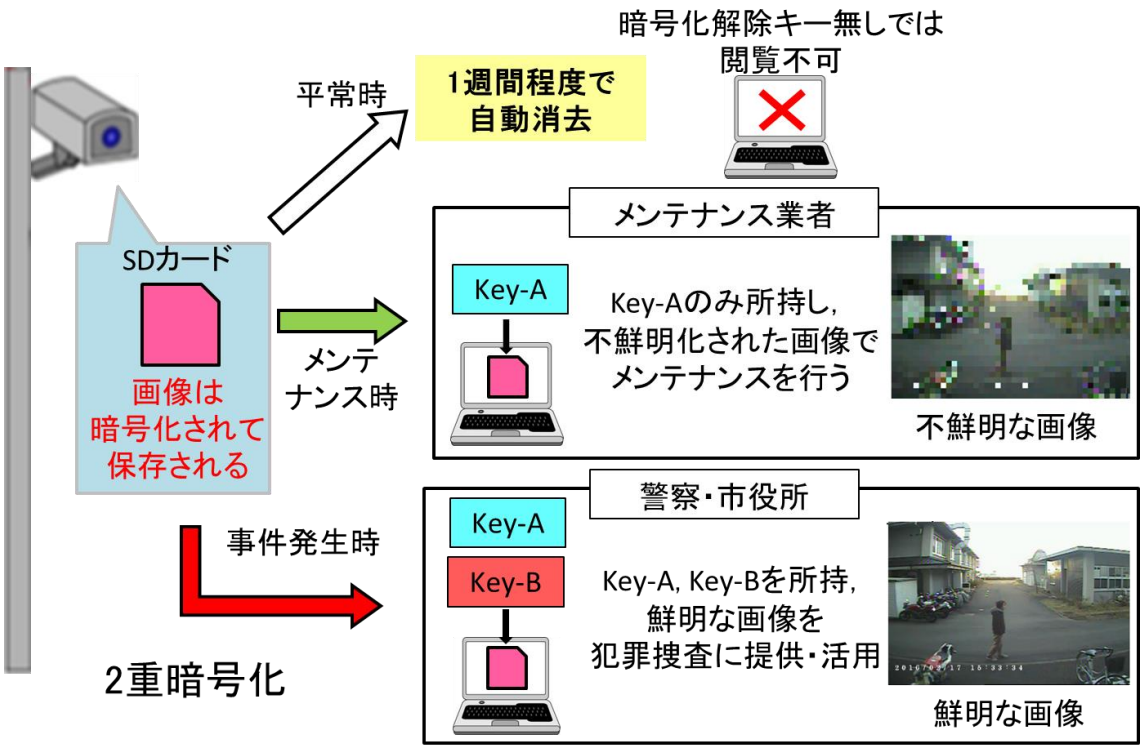

図 1.3　二重暗号化の概念

図 1.3 では，二重暗号化により，Key-A のみを持つメンテナンス業者はモザイク処理された画像しか閲覧できないため，人の顔などはしっかり確認できない

が，動作確認を行うことはできるため，プライバシーを侵害することなくメンテナンスを行うことができる．そして，事件・事故が起こった際には，Key-A，Key-B の両方を持つ警察等の閲覧権者は，2 つの Key を使い暗号化を解除し鮮明な画像を閲覧することで，事件・事故の捜査に大きく役立てることができる．また仮に，第 3 者が，暗号化された画像ファイルを盗んだとしても，Key-A と Key-B を入力しない限り，画像の閲覧は不可能である．

以上により，複数の暗証キーにより，閲覧する権限を有する者の間において，閲覧画像の鮮明度を段階的に設定することができ，プライバシー保護を高いレベルで実現することが可能になると考えられる．また，第 3 者による悪用の防止対策も高いレベルで実現することができると考えられる．

このようなカメラシステムを搭載した防犯カメラが，日本全国に，街路灯と同程度の数量・密度で設置されれば，社会の安全・安心は飛躍的に高まると考えられる．事件・事故が発生した場合も容疑者・容疑車両は，もれなく，どこまでも，追跡が可能になると考えられる．

近年において，「モノのインターネット(Internet of Things)」に代表されるように，様々なモノがインターネットに接続される動きが見られる．そして，近い将来では，インターネットに安価に接続できる環境が整い，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．そこで次節では，インターネット接続された防犯カメラが，街路灯と同程度の密度で設置された近未来の世界における，プライバシー保護の手法について述べる．

1.3.3　閲覧記録の完全な記録

近未来の日本全国の市街地においては，ネットワークカメラが，街路灯と同程度の数量・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．そして，犯罪の容疑者，容疑車両に対する，閲覧装置上でカメラを切り替えて手動での追跡，専用のソフトウェアによる自動追跡などが，容易に行えるよう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防犯カメラが，街路灯と同程度の密度で設置された近未来」の世界においては，事件や事故が発生した場合，警察等が捜査のために，カメラを芋づる式に，順次切り替えながら容疑者を追跡して，現在位置を特定するということが，簡単に行えるようになると予想される．

しかし，そのような近未来の社会において，画像にアクセスする権限のある人間が，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．よって，こうした第 3 者による不正な使用ができないようにする仕組みが，必要不可欠になる[11].

本研究室では，このような近未来の社会の，「第三者による悪用」に対して，これをほぼ完全に防止できる技術的・社会的システムとして， 新しいコンセプト「閲覧履歴の完全な記録」を提案した[12, 13]．図 1.4 に閲覧行動の完全な記録の説明図を示す．図 1.5 に閲覧行動の記録の仕組みを示す.

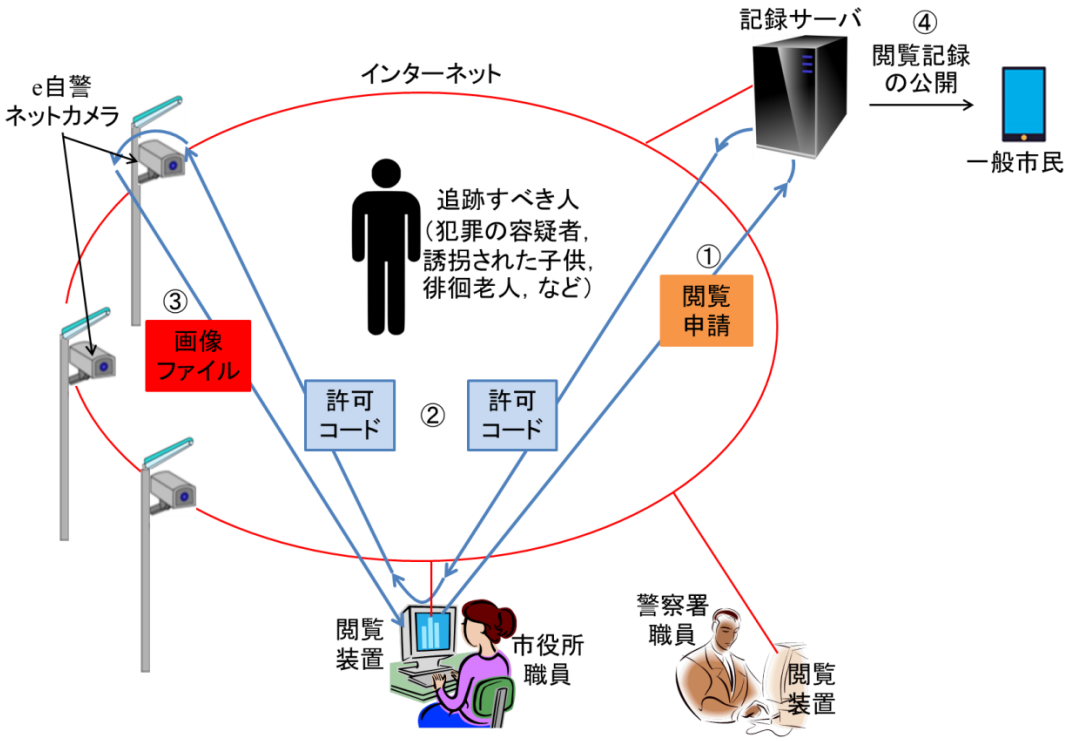

図 1.4 閲覧履歴の完全な記録

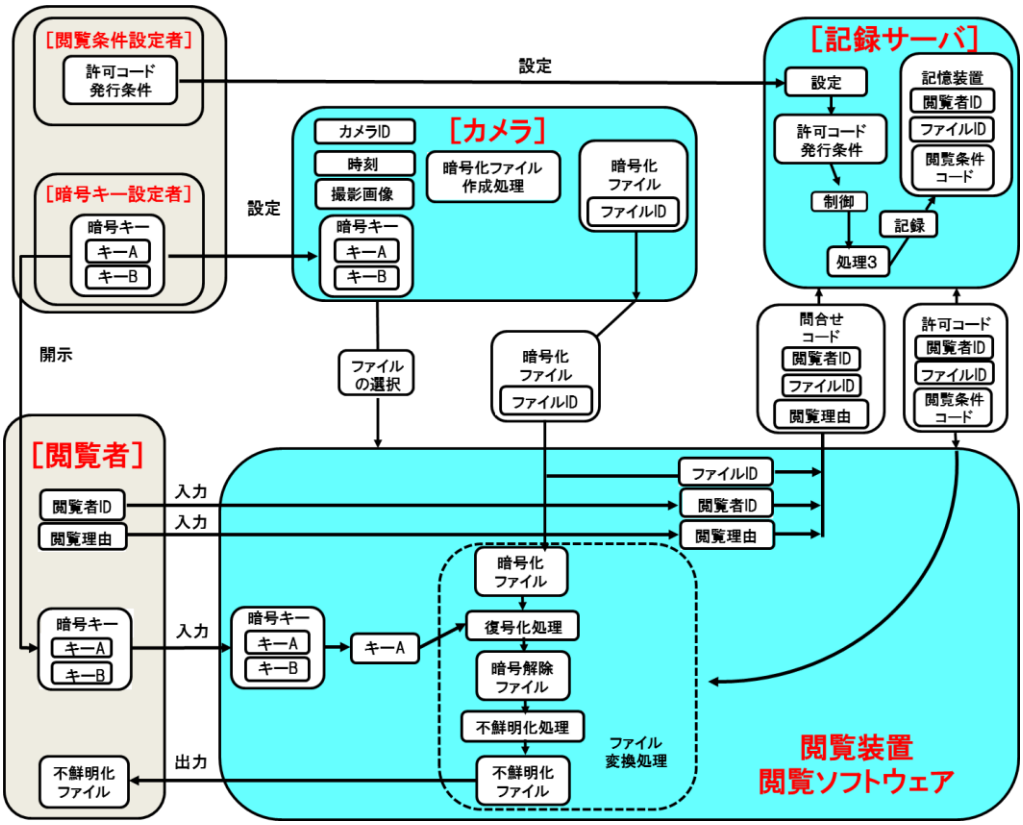

図 1.5 閲覧行動の記録の仕組み

以下に図 1.4 の閲覧履歴の完全な記録の説明を示す.

① 画像を閲覧するには，閲覧者の ID，閲覧理由，閲覧するファイル（あるいは時間やカメラの範囲）と共に閲覧申請をする.

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．記録サーバから受け取った許可コードをカメラに送る.

③ カメラは，許可コードで許可された範囲で，画像ファイルを閲覧装置に送る．また，許可コードには，閲覧できる画像の鮮明度なども指定されており，閲覧者ごとに画像の鮮明度を変えることができる．これによりメンテナンス業者はモザイク処理された画像で動作確認，警察や市役所の職員は鮮明な画像で捜査に利用といった使い分けができる.

④ 記録サーバは，閲覧申請と許可コードを記録することで，閲覧履歴を確実に記録することを実現し，閲覧履歴を公開しても問題ない場合は，閲覧履歴をリアルタイムで一般公開する.

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なく，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.

本コンセプトでは，例えば，市役所の担当部署が市街地に設置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・閲覧する際には，市役所の担当部署や，その他閲覧権のある組織は，団体とは関係のない，信頼できる第 3 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，どの画像の閲覧を許可するか」を，確実に記録する．そして，その記録

した情報は，リアルタイムで一般公開する．記録した情報は，定期的に，業務命令と照合することにより，本来必要な閲覧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，悪用は確実に発覚することになり，「不正な閲覧行為」は，強力に抑制されることになる．画像の閲覧は，正当な理由があり，その閲覧行為が公開されても差し支えないものに限られることとなり，一般市民のプライバシーは強力に保護される．

1.4　e 自警機器の概要

1.4.1　e 自警カメラ

この節では，暗号化保存機能がある All-in-one 型の防犯カメラシステム「e 自警カメラ」の概要について説明する．

本研究室では，「暗号化保存により，地域の安全・安心が脅かされない限り，画像を閲覧できない運用を可能にする」というコンセプトに基づくプライバシー保護のための暗号化保存機能を持つ，防犯カメラシステム「e 自警カメラ」を企業と共同開発した[14]．そして，社会実験において，1.3.1 節で述べたような，保存画像の所有者（防犯カメラの設置者）と，暗号解除し閲覧することが出来る閲覧権者を分離した運用でプライバシーを保護することができることを実証してきた．e 自警カメラは以下の条件を満たすように設計された．

・屋外設置を容易とする，防水性のハウジングを使用

・カメラ，記録メモリー，ソフトウェアを内蔵した PC 不要の防犯カメラ

・配線不要で，電源を投入するだけで使用可能

・画像は暗号化して保存することによる，プライバシー保護機能を搭載

さらにその後，過去の社会実験のデータを基に改良点を洗い出し，新たにプライバシー保護機能を充実させた e 自警カメラ（eJKC-ZB102a）を企業と共同で開発した．この e 自警カメラ（eJKC-ZB102a）は，1.3.1 節で述べたような，二重暗号化の機能が追加されている．その後も e 自警カメラ（eJKC-ZB102a）に改良を加え，次期モデル（eJKC-ZB-102c）を開発した．この e 自警カメラ（eJKC-ZB-102c）は，夜間の単体での撮影が可能となった． また，SD カードの容量がいっぱいになった際の古いデータの上書き機能が旧型より安定化しており，上書き機能のエラーで動作が停止する可能性が低減され，より安心して運用することが可能になっている．図 1.6 に e 自警カメラ(eJKC-ZB102c）の外観を，表 1.1 に

仕様を示す.

図 1.6 eJKC-ZB102c の外観

表 1.1 eJKC-ZB102c の仕様

カメラ本体	1/3 Sony Super HAD CCDカメラ
レンズ	4.9mm/9-22mm 可変焦点レンズ
防水機能	あり（野外設置可）
リモコン	附属（各種設定が可能）
SDカードの容量	32GBまでのSDHCをサポート
フレームレート	5/15/30 fps から選択可能
画像解像度	D1: 704×480(NTSC), 704×576(PAL) VGA: 640×480(NTSC), 640×576(PAL) QVGA: 320×240(NTSC), 320×288(PAL)

1.4.2　e 自警ネットカメラ

本研究室では，1.3.3節で述べたような新しいコンセプト「閲覧行為の完全な記録」を形にするために，シングルボードコンピュータ「Raspberry Pi」をベースに，USBメモリーとUSBカメラを組み合わせた，新しいネットワークカメラシステム「e自警ネットカメラ」を開発した．図1.7にe自警ネットカメラの外観，図1.8に内観を示す．表1.2にe自警ネットカメラの仕様を示す．

図 1.7 e 自警ネットカメラの外観

図 1.8 e 自警ネットカメラの内観

表 1.2 e 自警ネットカメラの仕様

コンピュータ	Raspberry Pi 3 Model B
カメラモジュール	iBUFFALO Web Camera(BSW20KM11BK)
カメラモジュールの仕様	最大解像度：1920×1080
カメラケースの仕様	形状：防滴型， 材質：アルミニウム・ABS， 質量：700 (g)
レンズ	可変焦点レンズ
画像保存用USBメモリー	IOデータ 128GB USB(BUM-3C128G/K)
画像の保存場所	上記のUSBメモリー(128GB)に保存
保存画像の形式	撮影画像は数字8桁の暗号キー(key-A，key-B)により暗号化され保存
保存画像の消去	保存画像は保存媒体の容量の範囲で古い画像から順に上書き消去

本研究室は，1.4.1 節でも述べたように，e 自警カメラを企業と共同開発してきた．しかし，本研究室が提案し企業が機能を実装する方法では e 自警カメラのソフトウェアの改良に時間がかかっていた．そこで，本研究室が Raspberry Pi をベースに従来の e 自警カメラと同等の機能とネットワーク機能を持つ，e 自警ネットカメラを開発した．

今回，e 自警ネットカメラに用いられた Raspberry Pi とは，手のひらに載る大きさのシングルボードコンピュータで，パソコン同様に利用することができる．また，USB 端子や GPIO（名称 : General-purpose input/output）のピンを持つため，USB メモリー，USB カメラ，LED を接続することが可能である．GPIO とは，汎用入出力を意味し，入力として動作した場合は電気回路のほかの部分からのデジタル信号を読み取り，出力として動作した場合は他デバイスの制御や信号の通知を行う．今回の場合は，e 自警ネットカメラの動作状況を LED で確認するために利用している．つまり，Raspberry Pi はカスタマイズが容易であり，開発の環境を整えることに向いているため，e 自警ネットカメラの作製に用いられた．

1.5　試作機を用いた実証実験（耐久試験）

本研究室は，ネットワーク接続された e 自警ネットカメラにおけるプライバシー保護を目指して, e 自警ネットカメラの試作機を用いて実証実験（耐久試験）を行っている．試作機を用いた実証実験（耐久試験）では，シングルボードコンピュータ（Raspberry Pi2）を内蔵したカメラユニット 7 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 台からなる．7 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 USB 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）は実証実験サイトに，設置している．図 1.9 に，実証実験サイトにおける e 自警ネットカメラの配置を示す.

設置台数： e 自警ネットカメラ 7 台

実証実験実施日： 2016 年 6 月 21 日～現在も実施中

運営協力： 群馬県桐生市末広町「末広みらいパーキング」敷地内

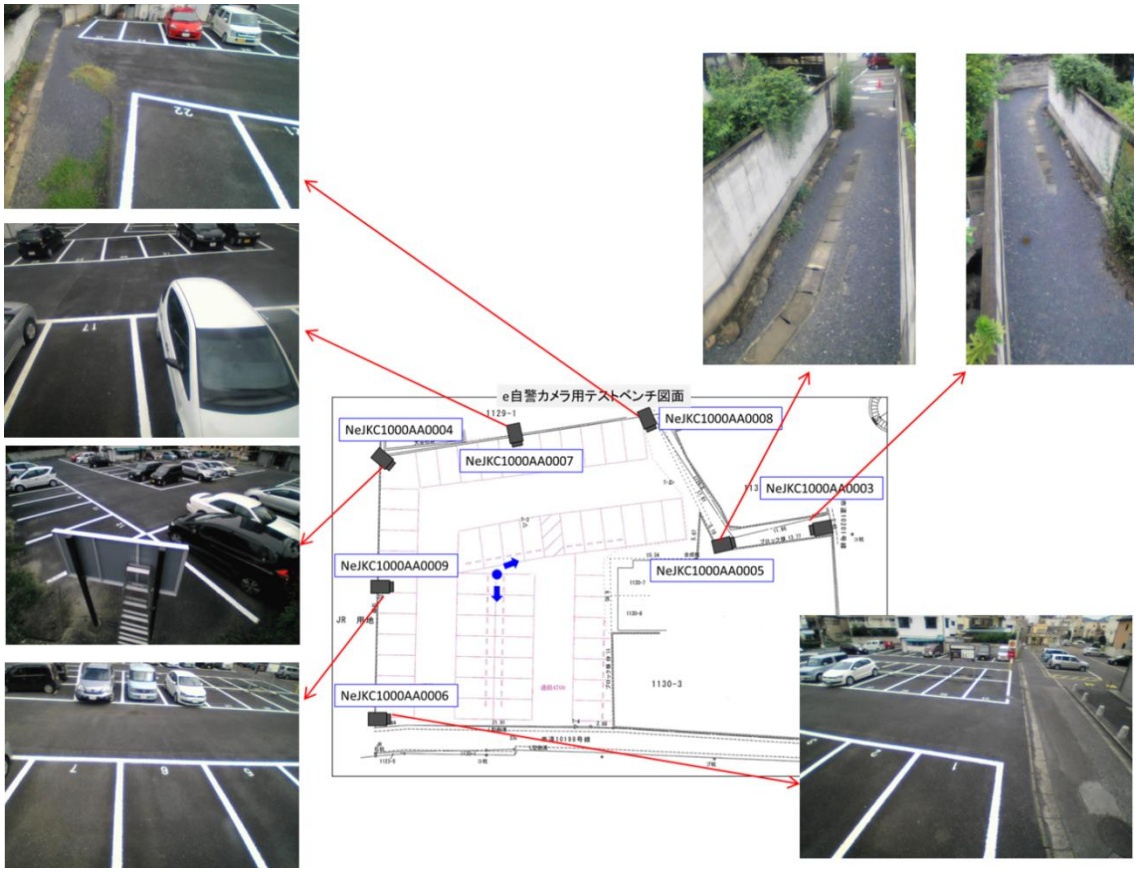

図 1.9 実証実験サイトにおける e 自警ネットカメラの配置

警察や市役所での運用方法としては，記録した閲覧記録の使い方は，定期的に，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，閲覧記録をすべて，ウェブサイト上に一般公開している[15]．今回の場合，e 自警ネットカメラの前を通る人は，強制的に撮影される．そこで強制的な撮影の代わりに，強制的に閲覧行為を一般公開するようにした．図 1.10 に，一般公開されている閲覧記録の一部を示す．

- ユーザの検索
- カメラの検索

閲覧申請日時 新しい順 古い順	ユーザID	カメラID	閲覧開始時期 新しい順 古い順	閲覧終了時期 新しい順 古い順	閲覧理由	詳細理由
2017年10月13日 15時48分 45秒	Works100A08_Kamioka 上岡 健太	NeJKC1000AA0004	2017年10月13日 14:00	2017年10月13日 14:59	動作テスト	画像確認のため
2017年09月25日 15時54分 42秒	CGov_100A04_Takita 田北啓洋 （織姫市役所計算機係）	NeJKC1000AA0003 NeJKC1000AA0005 NeJKC1000AA0008 NeJKC1000AA0007 NeJKC1000AA0004 NeJKC1000AA0009 NeJKC1000AA0006	2017年9月25日 15:00	2017年9月25日 15:59	動作テスト	動作テスト
2017年04月10日 22時15分 00秒	Police_100A03_Takita 田北啓洋 （織姫警察署 生活安全課 職員）	NeJKC1000AA0006	2017/04/0818:00	2017/04/1018:59	System.Windows.Controls.ComboBoxItem: 誘拐・強盗・傷害事件の捜査	写真館ビル空き巣調査のため.
2017年02月10日 13時52分 59秒	Chonai_100A08_Motegi 茂木 洸樹	NeJKC1000B0043	2017年2月7日 17:00	2017年2月8日 20:59	動作テスト	卒業研究の資料として使うため
2017年02月07日 18時27分 10秒	Chonai_100A07_Ohki 大木 秀紀	NeJKC1000B0004	2017年2月7日 16:00	2017年2月7日 17:59	動作テスト	卒業研究の資料として用いるため

図 1.10 閲覧記録の一部

一般市民側の方は強制的に撮影されることに対して，運用者側の方は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．以上のように，実証実験においては，一般市民のプライバシー保護の為の技術的仕組みについても検討している．

1.6　e 自警ネットカメラの今後について

本研究室の「e 自警ネットカメラ」は，「世界を大きく変える社会基盤」として，世界標準を獲得するポテンシャルを有していると考えている．そして，現時点で，「e 自警ネットカメラ」を製品化する上で，技術的な大きな障害はなくなってきていると考えている．今後の e 自警ネットカメラは，試作機のようなカメラ単体のタイプの他にも，LED 街路灯内蔵型，TV ドアホン内蔵型，車載型，ウェアラブル型など，様々なバリエーションの機器が開発されると考えられる．

近い将来，1.3.3 節で述べたようにネットワークカメラが，街路灯と同程度の数量・密度で設置されとしたら，犯罪の容疑者，容疑車両を，どこまでも追跡していくことが可能となる．また，近年では，顔認識や行動認識などの画像解析技術が開発されてきている．このような高密度に設置されたネットワークカメラと画像解析技術を活用することにより，犯罪抑止・容疑者検挙以外にも，利便性の向上，地域社会の安全・安心も向上し，素晴らしい社会の実現が可能になると予想される．

次章から筆者は，これまでの研究や社会実験の結果を経て，防犯のためのカメラシステムをより良くするための手法のひとつとして，駐車場の違法駐車を検知し，通報する機能の開発を示す．そして，違法駐車の検知には，テンプレートマッチング法を用いた手法を考案し，実際に違法駐車と想定した車を駐車させ，晴れの日と雪の日のサンプルデータの撮影をして，車の検知を行ったことを示す．また，日光による影響を調べ，契約車両と違法駐車の車両の区別をするための手法を考案したことを示す．最後に，車を検知した際に，定められた宛先へと通報する機能を開発したことを示す．このシステムを e 自警ネットカメラに導入することで，駐車場での違法駐車の取り締まりに貢献することを目指すというのが次章で説明する内容である．

第 2 章　e 自警ネットカメラを用いた違法駐車の検知

2.1　開発目的

前章で述べたように本研究室では，かつての地域コミュニティの防犯機能を，情報技術を用いて再建・再現する為に，e 自警ネットワークのコンセプトをもとに様々な e 自警機器を開発している．現在，複数ある e 自警機器の中から，e 自警ネットカメラと呼ばれる試作機を使用して実証実験（耐久試験）を行っている．その中で，駐車場の契約者以外の車が不当に駐車するという，違法駐車が問題になった．この違法駐車をなくすためには，常に駐車場の管理人が監視し続けなければいけない．しかし，これは不可能であると考えられる．そこで，e 自警ネットカメラを活用し，違法駐車を検知した場合通報する機能を考案した．このような，違法駐車を検知し，通報する機能を持った e 自警ネットカメラを開発することで，不当な駐車を防ぎ犯罪の迅速な取り締まりに貢献することが目的である．そして今回，防犯のためのカメラシステムをより良くするための手法のひとつとして，駐車場での違法駐車の検知，および，通報機能の開発を開始した．

2.2　開発内容

2.2.1　使用機器

e 自警ネットカメラを用いた違法駐車の検知の開発に当たり， Raspberry Pi3 Model B 上で Linux を使用して，OpenCV（名称 : Open Source Computer Vision Library）を利用し，C++言語で作成した．Raspberry Pi は ARM プロセッサを搭載した，シングルボードコンピュータである．Raspberry Pi はソフトウェアの動向をカスタマイズすることが可能であるため，実証実験で得られた様々な意見や，新機能の追加を反映させていくことに適している．また，OpenCV は，BSD ライセンスのオープンソースのコンピューター・ビジョン・ライブラリである．画像処理・画像解析および，機械学習等の機能が実装されており，BSD ライセンスで配布されていることから学術用途だけでなく商用目的でも利用できる．加えて，マルチプラットフォーム対応されているため，幅広い場面で利用することができる．このように，Raspberry Pi と OpenCV は新機能の追加と実験をスムースに行うための環境を整えることに向いているため，今回の開発に用いられた．

以下に，開発するにあたり使用した機器を示す．

表 2.1 使用機器

名称	個数
Raspberry Pi 3 Model B	1
iBUFFALO 200万画素WEBカメラ 広角120°マイク内蔵 BSW200MBK	1
IOデータ128GB USBメモリー	1
ACアダプター（5V, 3A）	1
発光ダイオード（抵抗内蔵型）	緑×1, 赤×1

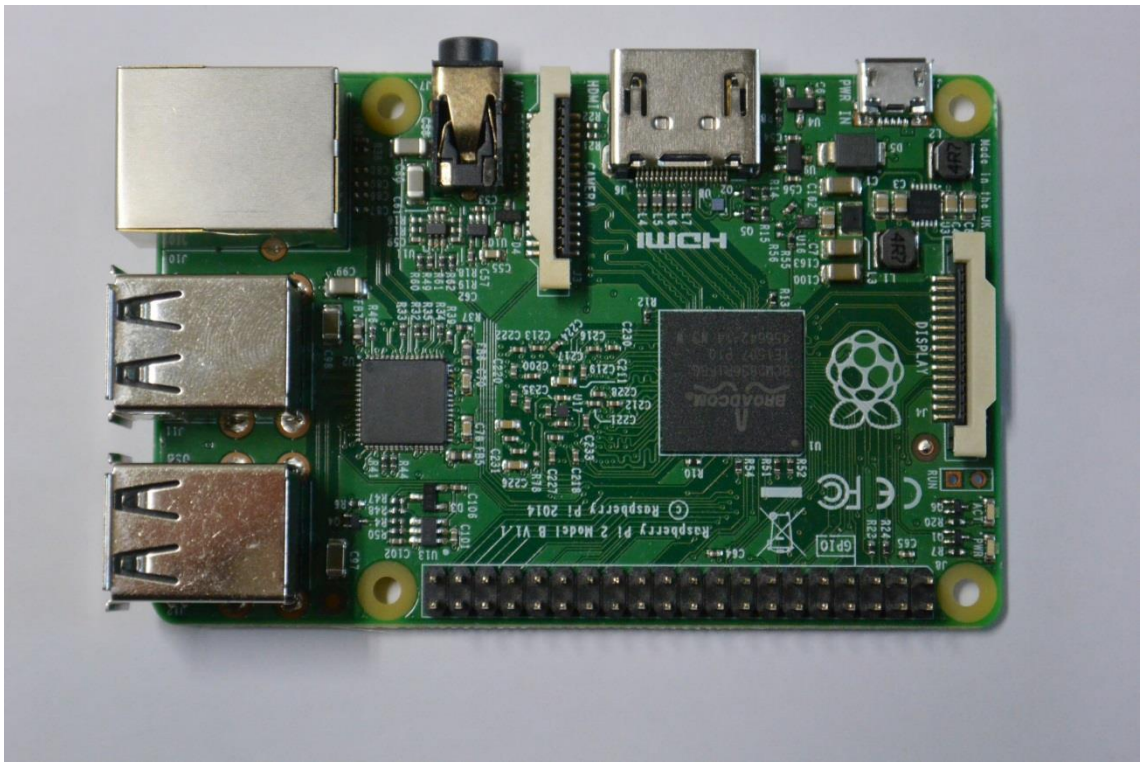

図 2.1 Raspberry Pi3 Model B

図 2.2 iBUFFALO　200 万画素 WEB カメラ BSW200MBK

図 2.3 IO データ 128GB USB メモリー

図 2.4 AC アダプター（5V, 3A）

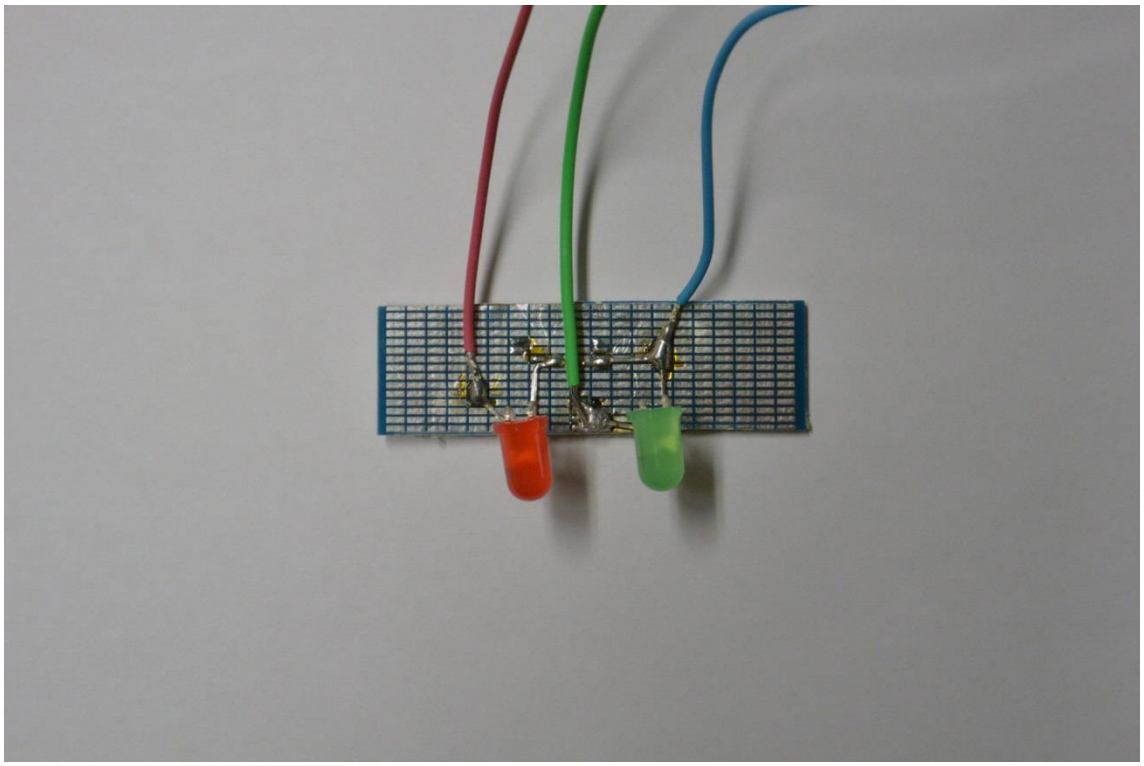

図 2.5 発光ダイオード（抵抗内蔵型） 緑×1，赤×1

2.2.2　テンプレートマッチング法を用いた検知の方法

今回，違法駐車の検知にあたり，テンプレートマッチング法を使用した検知を考案した．テンプレートマッチングとは，あらかじめ用意したテンプレートと呼ばれる画像パターンが，探索対象の画像のどこにあるかを探し出す方法である．図 2.6 にテンプレートマッチングの例を示す．図 2.6 の例では，探索対象の画像で青い枠線で囲まれた部分がテンプレートと同じであると判定されている．テンプレートマッチングは，探索対象の画像にテンプレート画像をあてはめ，画像全体を走査することにより，最も類似度の高い（相違度の低い）画像領域を検出する手法である．図 2.7 に e 自警ネットカメラの設置状況を示す．図 2.7 は駐車場に設置してある柱の上部（設置してある e 自警カメラよりも上）に e 自警ネットカメラを設置したものである．図 2.8 に実証実験サイトのサンプル画像と見取り図を示す．図 2.8 (a) は，e 自警ネットカメラで撮影した実証実験サイトで検知対象とした駐車スペースを示したサンプル画像である．赤い枠線で囲まれた駐車スペース，手前の 2 か所（駐車番号 46,47），奥の 5 か所（駐車番号 48～52）で違法駐車の検知を行うものとする．図 2.8 (b) は,実証実験サイトにおける e 自警ネットカメラの位置を示す見取り図である．

図 2.6 テンプレートマッチングの例

図 2.7 e 自警ネットカメラの設置状況

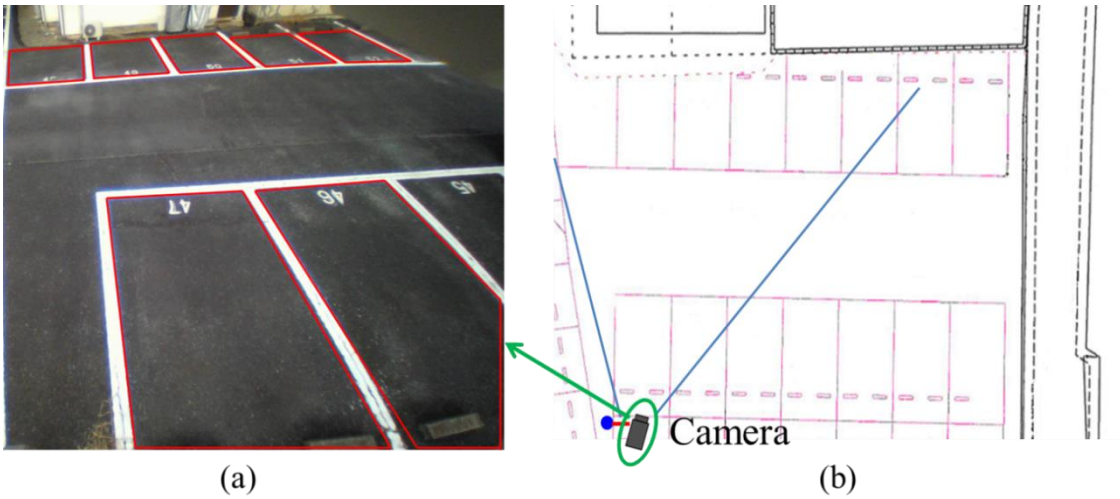

図 2.8 実証実験サイトのサンプル画像と見取り図

ここで，違法駐車の検知で使用するサンプル画像をテンプレート画像とし，撮影した画像（入力画像）を探索対象の画像とした．また，探索対象の画像は，テンプレート画像よりも，幅が 10 画素分大きくなるように切り取った．図 2.9 にテンプレート画像と探索対象の画像のイメージを示す．

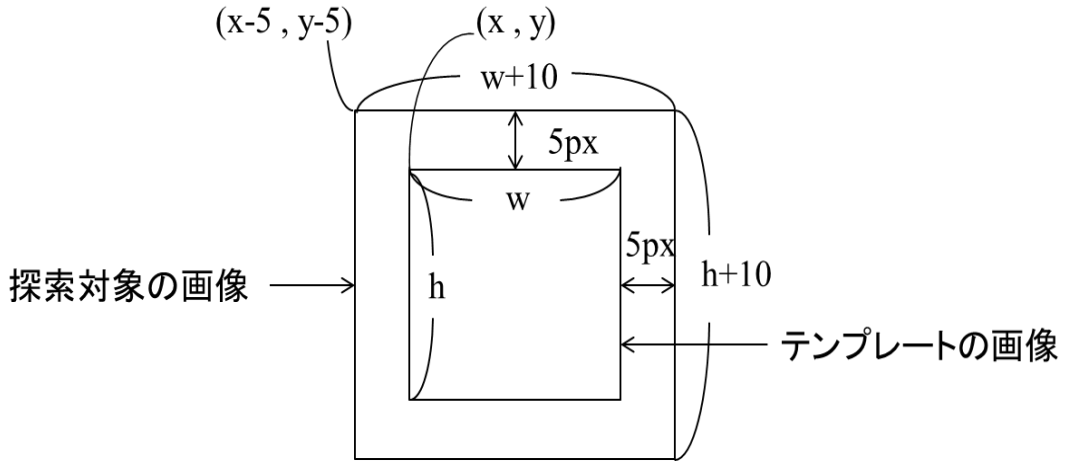

図 2.9 テンプレート画像と探索対象の画像のイメージ

図 2.9 のように探索対象の画像を，テンプレート画像よりも，幅が 10 画素分大きくなるように切り取った理由は，カメラを設置しているポールが風などの影響で揺れることで画像がぶれるため，探索対象の画像は，テンプレート画像よりも，多少大きく切り取った．また，テンプレートマッチングは，画像全体を走査することによって行われるため，処理の短縮のため，テンプレート画像と探索対象の画像は，検知に必要な部分だけを切り取った．そして，駐車スペースごとに使用するテンプレート画像と探索対象の画像は，それぞれ車が駐車されると予想される場所を切り取った．テンプレート画像は，車が駐車された時の画素の変化を明確にするために，駐車スペースの駐車番号や，車が駐車された時に車のナンバープレートが映りこむ範囲を使用した．図 2.10 に駐車スペースごとのテンプレート画像と探索対象の画像を示す．

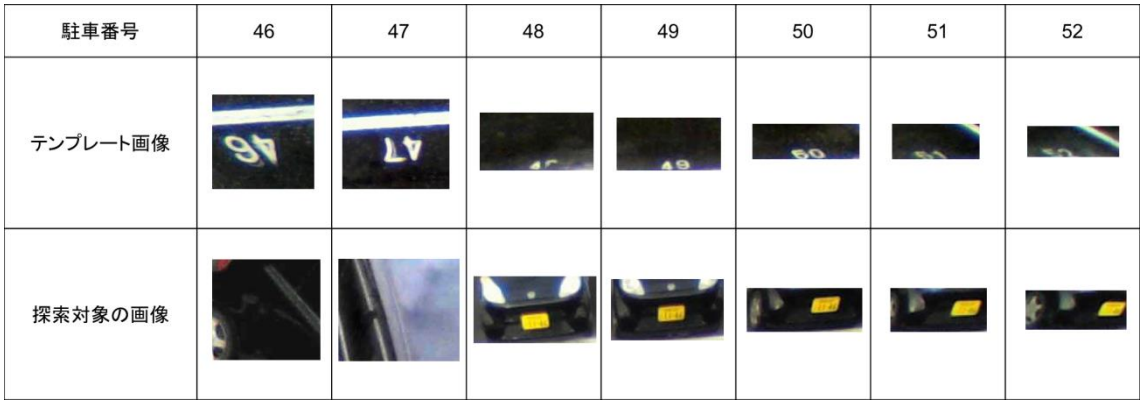

図 2.10 駐車スペースごとのテンプレート画像と探索対象の画像

図 2.10 のテンプレート画像はサンプル画像から切り取り，探索対象の画像は車が駐車された時の入力画像から切り取ったものである．

屋外でのテンプレートマッチングは，日光による明るさの変化や，時間の推移で変化する建造物の影の影響により誤検知が出てしまうと考えられた．そこで，それを補うため，テンプレート画像と探索対象の画像に，明度値の正規化を行い，これらによる影響を少なくしている．図 2.11 に画像の正規化を示す．

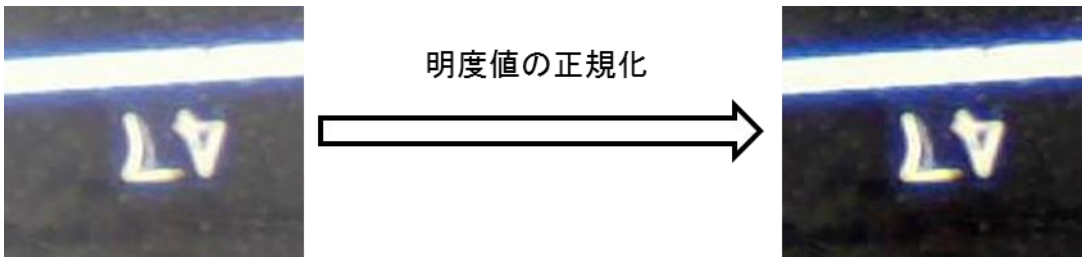

図 2.11 画像の正規化

テンプレートマッチングを用いた検知では，車が駐車されると，テンプレート画像と探索対象の画像の類似度が低くなり，マッチングしなくなるため，お互いの画像の適合率は低くなる．今回の違法駐車の検知は，この適合率の変化を利用し，適合率が閾値を下回り続けた時を車が駐車されたと判断する．適合率は正規化相互相関（Normalized Cross Correlation）によって計算され，テンプレート画像

と探索対象の画像の類似度を表す[16-17]．正規化相互相関は,次式で表される．

$$\mathrm{R}(u,v) = \frac{\sum I(x+u, y+v)\, T(x,y)}{\sqrt{\sum I^2(x+u, y+v) \cdot \sum T^2(x,y)}} \tag{1}$$

上記の式において，テンプレート画像の画素値を$T(x,y)$，探索画像の画素値を$I(x,y)$，結果を$\mathrm{R}(u,v)$とする．座標の(x,y)は，テンプレート画像の幅を w，高さを hとしたとき，左上が$(0,0)$，右下が$(w-1, h-1)$となる．$\mathrm{R}(u,v)$の値（＝適合率）は，-1.0～1.0に収まり，最大値1.0に最も近くなった走査位置が，テンプレート画像に最も類似する部分の左上座標となる．したがって、$\mathrm{R}(u,v)$の値が，最大値である1.0に近いほど類似度が高いことになる．そして，今回の違法駐車の検知では，車が駐車されたかどうかを判断するために閾値処理を行うため，適合率の値が-1.0～1.0に収まるこの計算方法だと，閾値の設定が簡単に行える．

次に，図 2.12 に違法駐車の検知のフローチャートを示す．

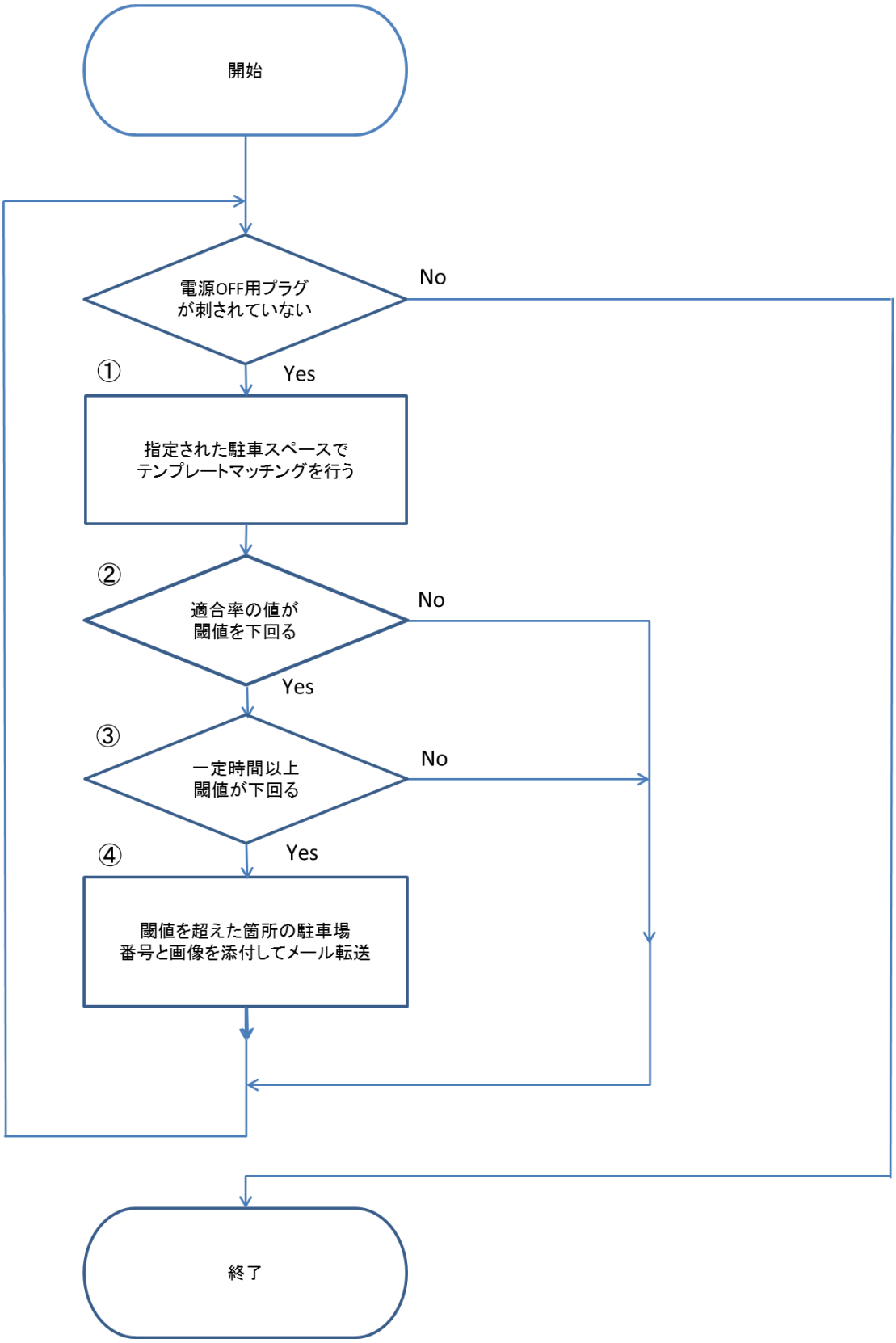

図 2.12 違法駐車の検知

以下に図 2.12 の違法駐車の検知の説明を示す.

① テンプレート画像と探索対象の画像で, テンプレートマッチングを行う. 最大の走査位置（最大適合率）の値を求める.

② 最大適合率の値を用いて閾値処理を行う. 最大適合率の値が閾値 0.85 を下回った場合, 連続で下回った回数をカウントする. また, 連続で下回った回数をカウントしている最中に, 閾値 0.85 を下回らなかった場合, 回数のカウントは 0 に戻される.

③ 連続で定めた回数分カウントし続けた（連続で閾値が下回り続けた）場合, 駐車スペースに車が駐車されたとする. 今回の条件では, 連続で閾値が下回り続けた回数が 10 カウントになった場合, 車が駐車されたとした.

④ 駐車スペースごとに検知を行っているため, 車が駐車されたと判断する駐車番号と, その時の画像をメールに添付して定められた宛先へと送信される.

2.3　テンプレートマッチング法の検知結果

テンプレートマッチング法を用いた検知の評価を行うため, 実証実験サイトの指定した 7 箇所の駐車スペースに，実際に，車を停めてサンプルデータの撮影をした．サンプルデータ A は，晴れの日に車を駐車させたときのサンプルデータである．サンプルデータ B は，雪の日に車を駐車させたときのサンプルデータである. それぞれ, テンプレートマッチング法を用いて車の検知を行った. 図 2.13 にサンプルデータ A の検知結果，図 2.14 にサンプルデータ B の検知結果を示す.

実施日： 2018 年 1 月 18 日

天気： 晴れ

駐車時間： 各駐車スペースに約 5 分間ずつ駐車

車種： HONDA LIFE (黒)

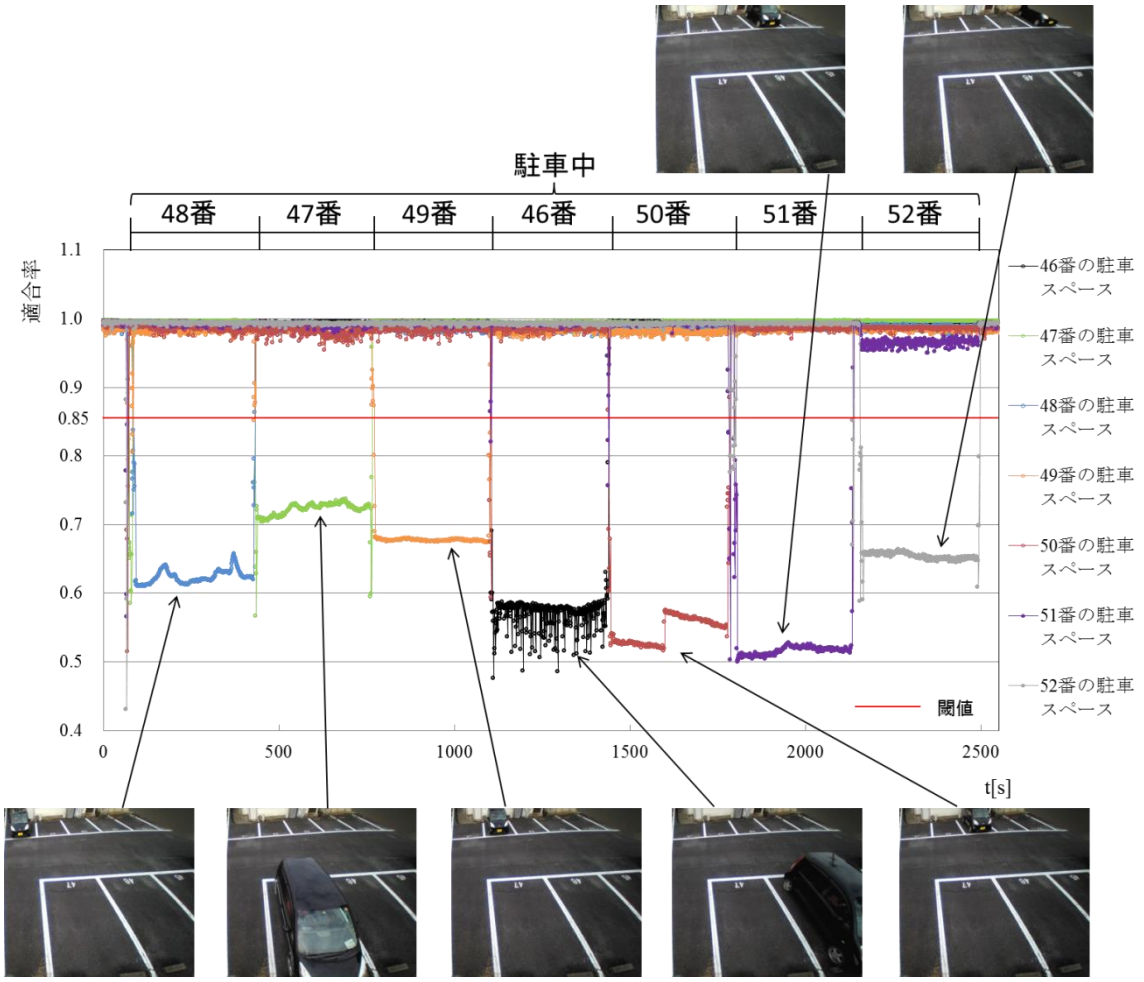

図 2.13 サンプルデータ A の検知結果

図 2.13 は，各駐車スペースにおよそ 5 分ずつ（計 35 分間）車を駐車させた検知の結果である．グラフの周りの写真は，各駐車スペースに車が止められている時のイメージ画像である．この図では，始めは，車が駐車されていないため，適合率にあまり変化はなく，どの位置の検知結果も 1.0 あたりを推移している．その後，車が駐車されると，そのスペースの適合率は閾値を大きく下回り続けている．この時の適合率の変化は，およそ 0.2～0.4 である．さらに，各駐車スペースに車を駐車させるごとに，適合率は閾値を下回り続け，車が駐車されなくなると，適合率は，再び，1.0 あたりを推移した．

実施日： 2018 年 1 月 22 日

天気： 雪

駐車時間： 各駐車スペースに約 3 分間ずつ駐車

車種： SUZUKI ワゴン R (黒)

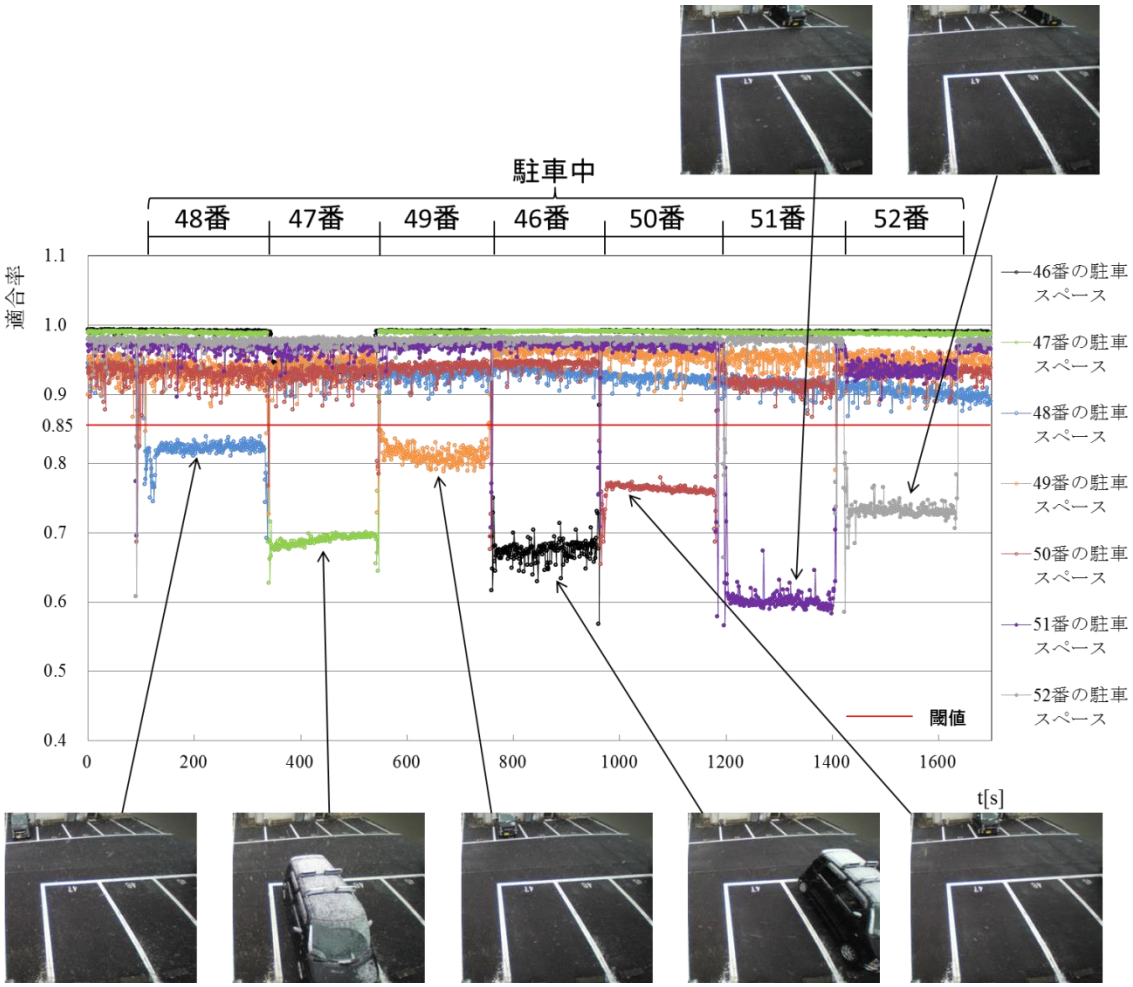

図 2.14 サンプルデータ B の検知結果

図 2.14 では，雪の日に，各駐車スペースにおよそ 3 分ずつ（計 21 分間）車を駐車させ，図 2.13 と同様の手順で，サンプルデータの撮影を行った．この図から，適合率の値に多少のバラつきはあるものの，車が駐車されると，閾値を下回り続けていることが分かる．また，この時の適合率の変位

は，およそ 0.2~0.4 であり，晴れの日と比べると，変位の大きさは小さくなっていることが分かる．

図 2.13 と図 2.14 の結果から，誤検知や未検知がなく，車の検知をすることが出来た．また，晴れの日と雪の日では，テンプレートマッチング法での車の検知は，可能であるということが分かった．

2.4　日光による影響

屋外でのテンプレートマッチングは，日光による明るさの変化や，時間の推移で変化する建造物の影の影響により，誤検知が発生する可能性があった．そこで，午前 6 時 30 分頃から午後 17 時 30 分頃（約 11 時間分）の，屋外が十分に明るい時間帯での，テンプレートマッチングを用いた日中の適合率の変化を調べ，そのデータから日光による影響を調べた．図 2.15 に日光による影響についての検知結果を示す．

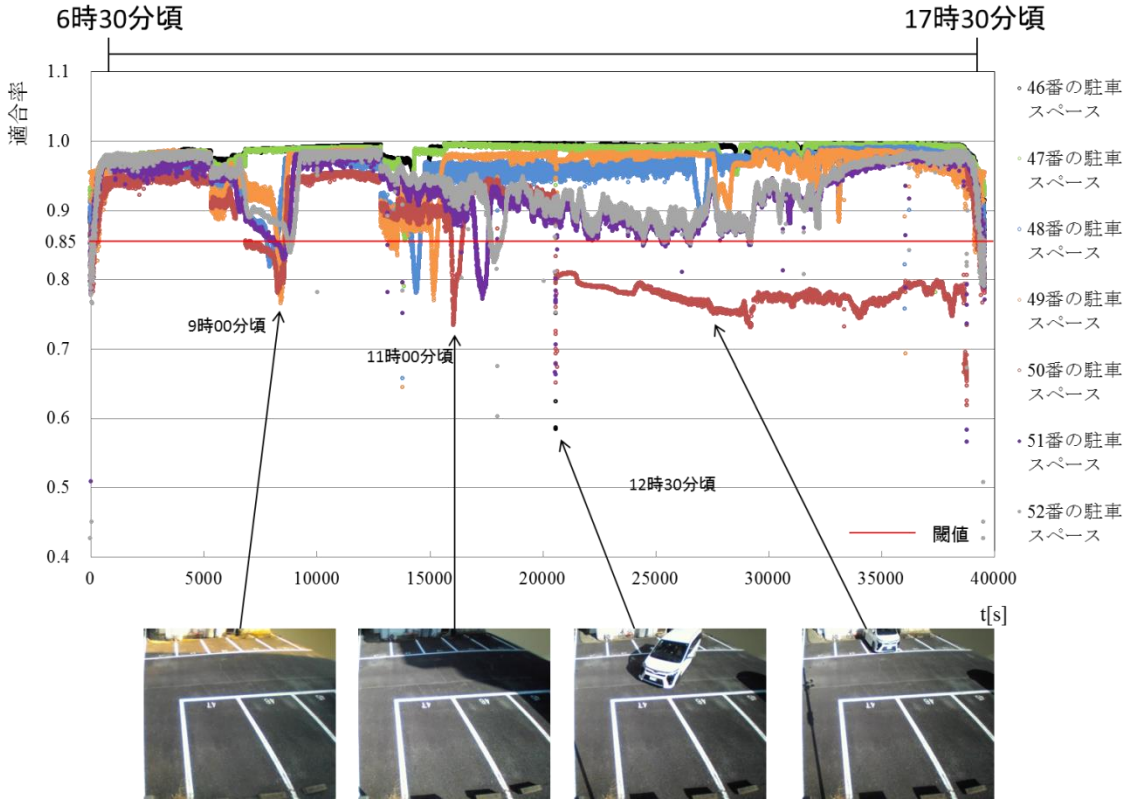

図 2.15　日中の適合率の変化についての検知結果

この図は，テンプレートマッチング法を用いた午前 6 時 30 分頃から午後 17 時 30 分頃までの，およそ 11 時間分の検知結果である．この図より午前 9 時 00 分頃と午前 11 時 00 分頃に，時間の推移で変化する建造物の影の影響で，適合率は閾値を下回っていることが分かる．また，午前 12 時 30 分頃から車が駐車されたことによって適合率が閾値を下回っている．

それ以外で，単発的に適合率が閾値を下回っている部分は，歩行者やバイク，車が駐車スペースの探索対象の部分を通り抜けたことにより発生したものである．

図 2.15 から，時間の推移で変化する建造物の影の影響で誤検知が発生してしまうことが分かったので，建造物の影と車を区別できるようにする必要がある．そこで，この問題を解決するために，適合率が閾値を下回る付近の，現在時刻の適合率の値と，1 秒前の適合率の値との差に注目した．図 2.16 に図 2.13 のサンプルデータ A の検知結果を用いた，適合率の差の値の大きさを示す．図 2.17 に図 2.14 のサンプルデータ B の検知結果を用いた，適合率の差の値の大きさを示す．図 2.16 と図 2.17 は，図 2.13 と図 2.14 の車が駐車された時の現在時刻の適合率と，1 秒前の適合率の差の値の大きさを調べるためのグラフである．

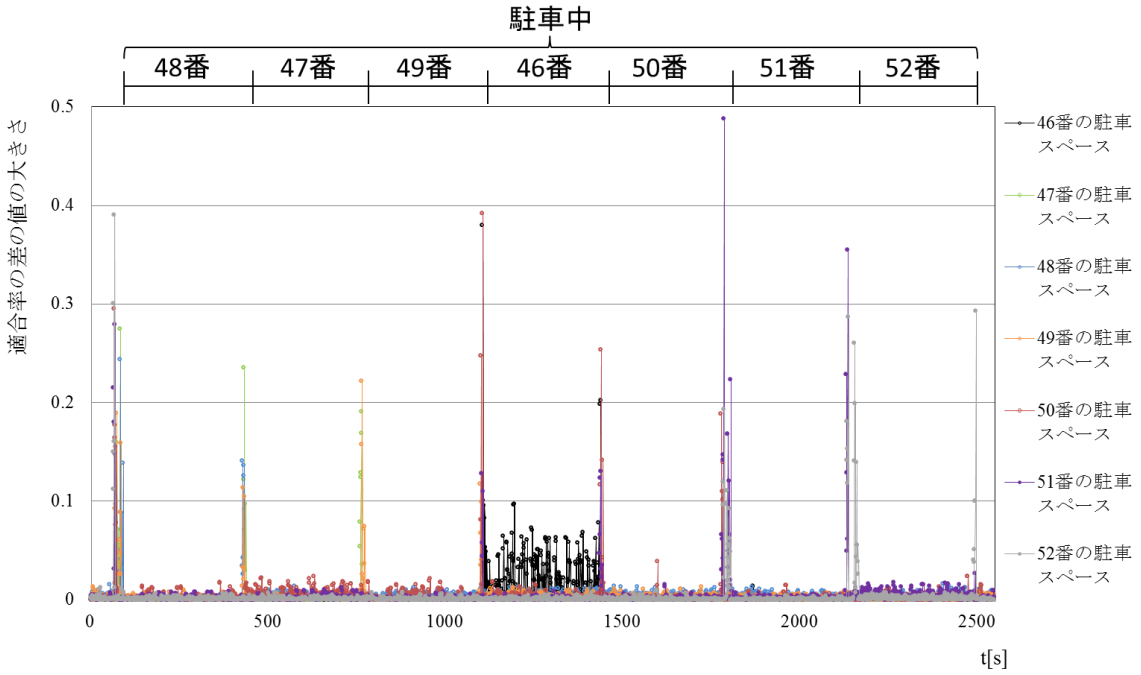

図 2.16 サンプルデータ A の適合率の差の値の大きさ

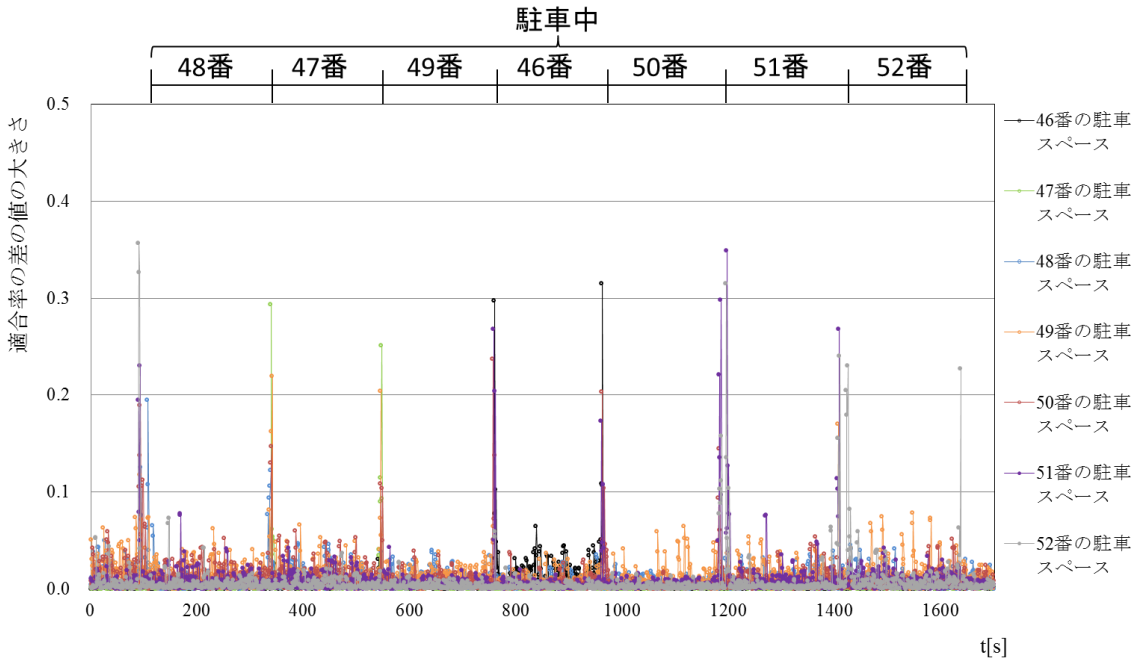

図 2.17 サンプルデータ B の適合率の差の値の大きさ

図 2.18 に図 2.15 の検知結果を用いた，午前 9 時 00 頃の適合率の差の値の大きさを示す．図 2.19 に図 2.15 の検知結果を用いた，午前 11 時 00 分頃の適合率の差の値の大きさを示す．図 2.18 と図 2.19 は，図 2.15 の建造物の影による現在時刻の適合率と，1 秒前の適合率の差の値の大きさを調べるためのグラフである．

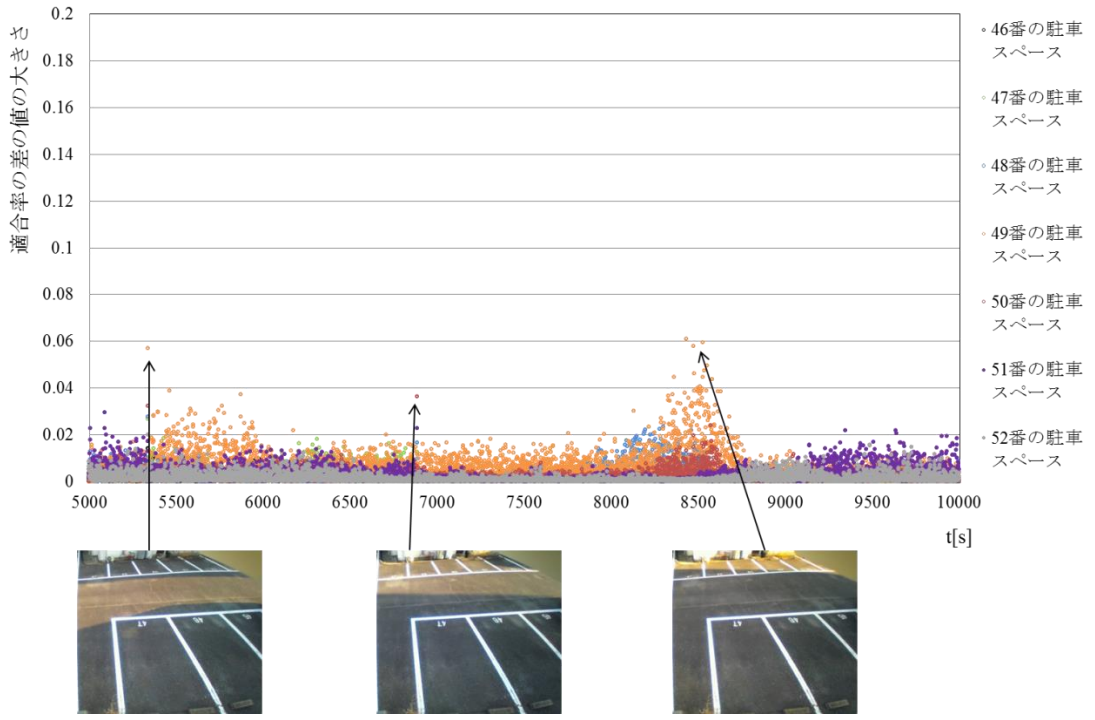

図 2.18 午前 9 時 00 頃の適合率の差の値の大きさ

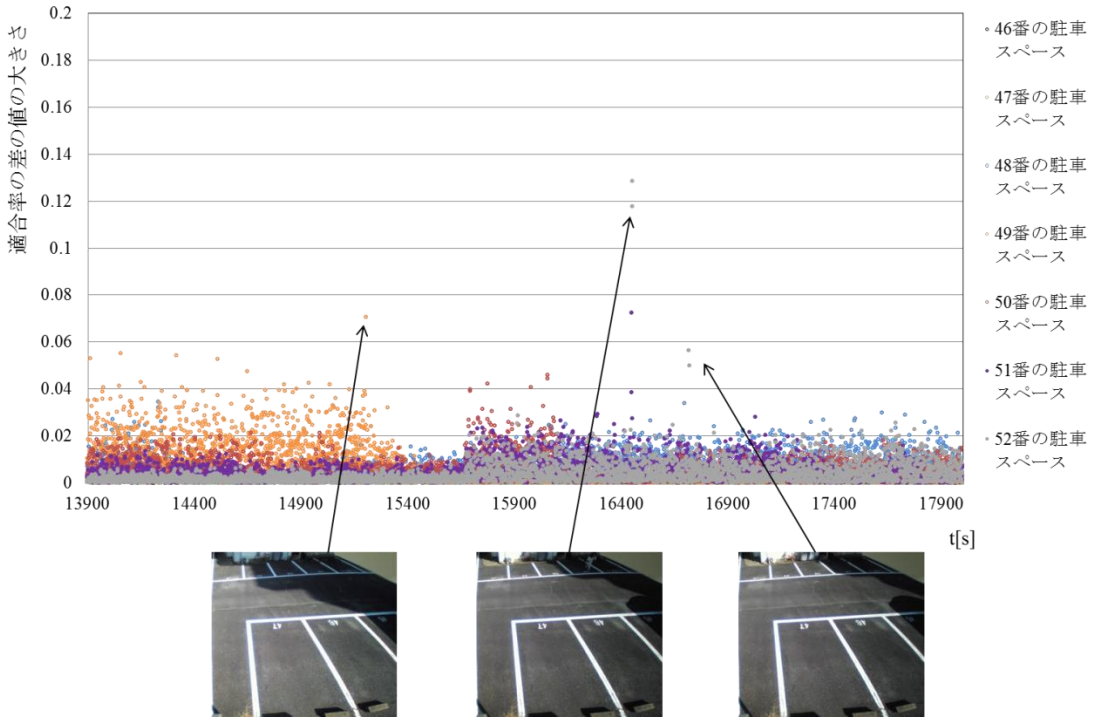

図 2.19 午前 11 時 00 頃の適合率の差の値の大きさ

図 2.16 と図 2.17 の図を見ると，車が駐車されたときの適合率の変化は，およそ 0.2~0.4 であり，急激に値が変化していることが見て取れる．一方，図 2.18 と図 2.19 の図を見ると，建造物の影による適合率の変化は，およそ 0.01~0.06 であり，車が駐車された時と比べて，なだらかに値が変化していること分かる．また，適合率の差の値の大きさが 0.1 を超えている箇所は，探索対象の部分を歩行者が通り抜けたことにより発生したものである．

このことから，車と建造物の影の適合率の変化の大きさの違いを利用することで，車と建造物の影との区別をすることができると考えた．具体的な手法としては，図 2.12 の②の部分で，“現在時刻の適合率と，1 秒前の適合率の差の値の大きさが 0.1 以上変化した場合，最大適合率の値を用いて閾値処理を行う”，という条件を加えることで，建造物の影による誤検知を無くすことが出来ると考えられる．

2.5　契約車両と違法車両の判断

前節までのテンプレートマッチング法では，検知する駐車スペースに契約者がおらず，車が駐車されることがないという条件のもとでのみ検知が行える．しかし，違法駐車は，契約された駐車スペースでも起こる可能性がある．そのため，契約者の車両と違法駐車した車両を区別する必要がある．そこで，この問題を解決するために，再びテンプレートマッチング法を利用した．図 2.20 に契約車両と違法車両を判断するための検知のフローチャートを示す．

以下に図 2.20 の契約車両と違法車両の判断の説明を示す．

① 2 回目のテンプレートマッチングでは，契約車両をテンプレート画像（サンプル画像）として行う．駐車スペースに車が駐車され，連続で閾値が下回り続けた回数が 30 カウントになった場合，閾値を下回った箇所の駐車スペースで，1 回目と同様の方法で 2 回目のテンプレートマッチングを行う．

② 2 回目のテンプレートマッチングで，適合率の値が閾値を下回った場合，違法車両と判断する．例えば，契約された駐車スペースに契約車両でない車が不当に駐車した場合は，まず，車が駐車されたと検知されたあと，2 回目のテンプレートマッチングで適合率の値が閾値を下回るため，違法に駐車した車両として検知される．

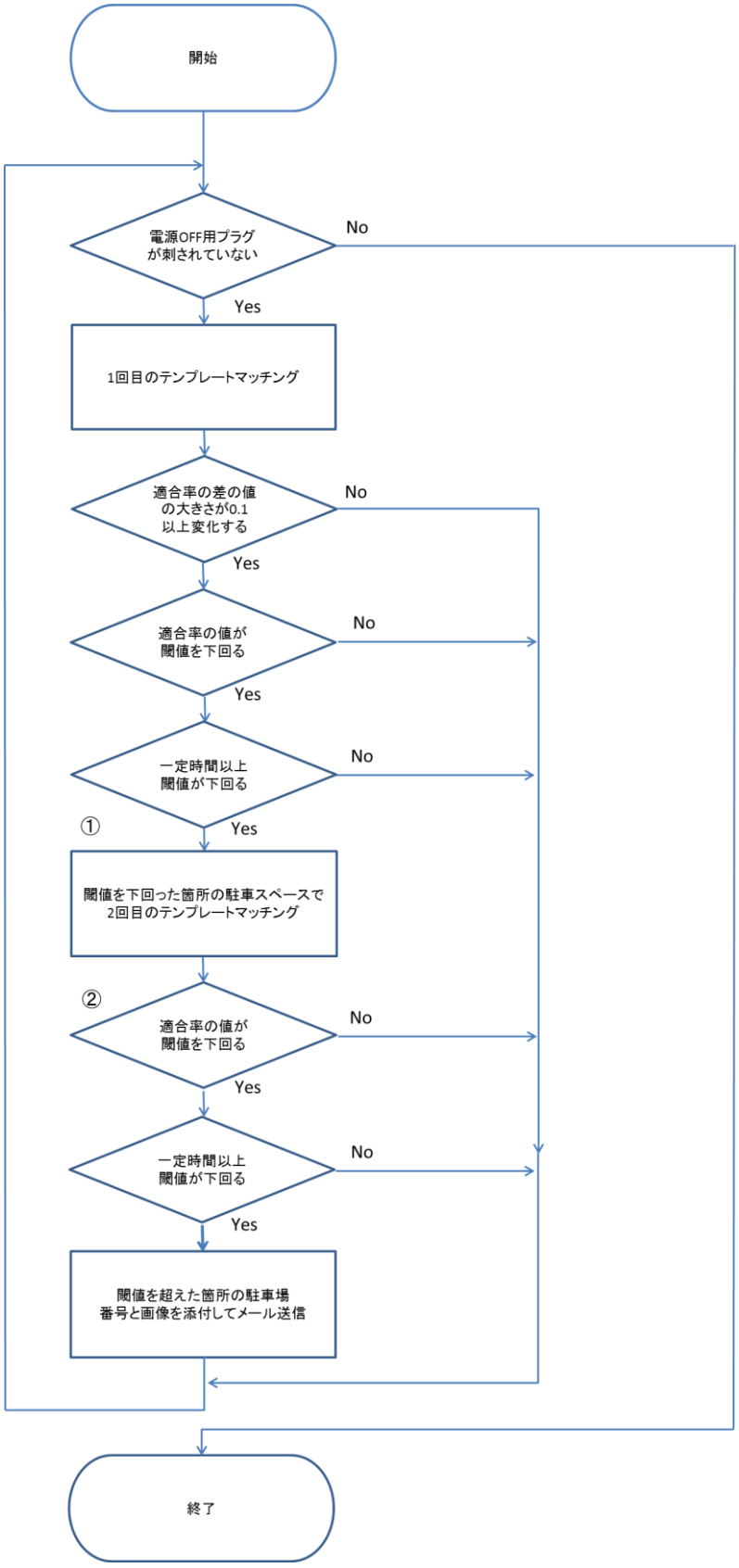

図 2.20 契約車両と違法車両の判断

テンプレートマッチング法を用いた契約車両と違法車両の区別を行うため，図 2.13 のサンプルデータを使用した．契約車両と違法車両を想定した車を，テンプレート画像として，図 2.13 と同様の方法で 2 回目のテンプレートマッチングを行った．

図 2.21 と図 2.22 に 2 回目のテンプレートマッチングに用いるテンプレート画像のイメージを示す．図 2.21 と図 2.22 のテンプレート画像のイメージは，契約車両と違法車両を想定した車が駐車された時の画像を切り取ったものである．また，テンプレート画像のイメージは，実際のテンプレート画像よりも，車の全体が映るように，大きく切り取ったイメージである．

駐車番号	46	47	48	49	50	51	52
テンプレート画像のイメージ							

図 2.21 契約車両のテンプレート画像のイメージ

駐車番号	46	47	48	49	50	51	52
テンプレート画像のイメージ							

図 2.22 違法車両のテンプレート画像のイメージ

次に，図 2.23 と図 2.24 に契約車両と違法車両を判断するために行った検知結果を示す．図 2.23 は，図 2.13 のサンプルデータを使用し，図 2.20 の①の 2 回目のテンプレートマッチングの際に，契約車両と想定した車を，テンプレート画像とした場合の検知結果である．図 2.24 は，図 2.13 のサンプルデータを使用し，図 2.20 の①の 2 回目のテンプレートマッチングの際に，違法車両と想定した車を，テンプレート画像とした場合の検知結果である．

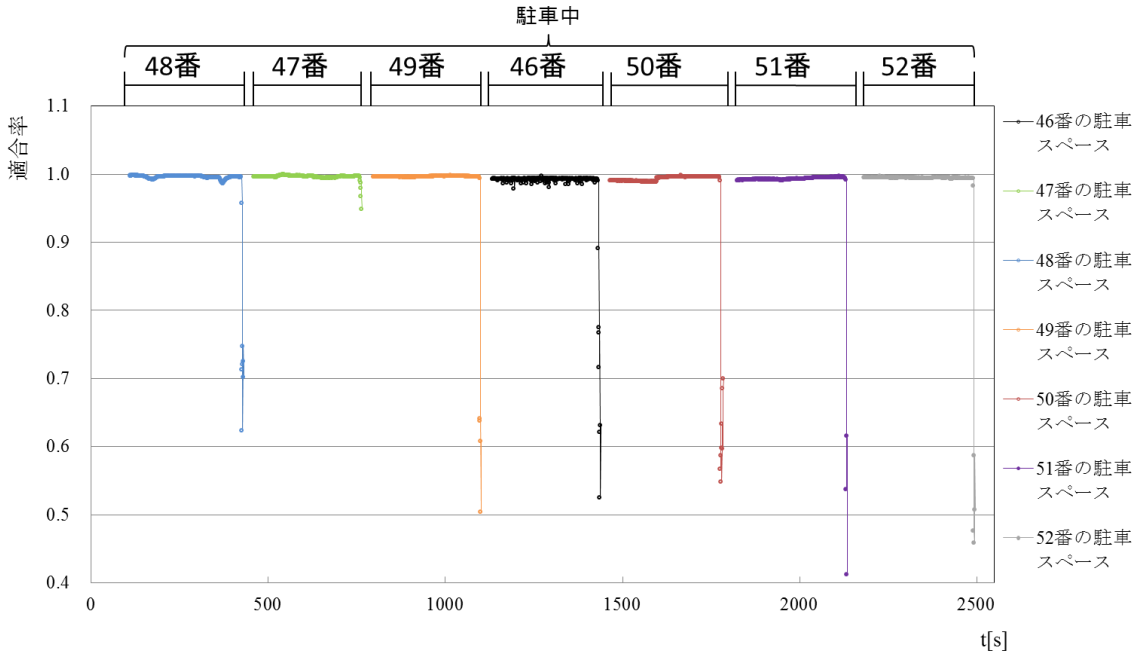

図 2.23 契約車両をテンプレート画像とした場合の検知結果

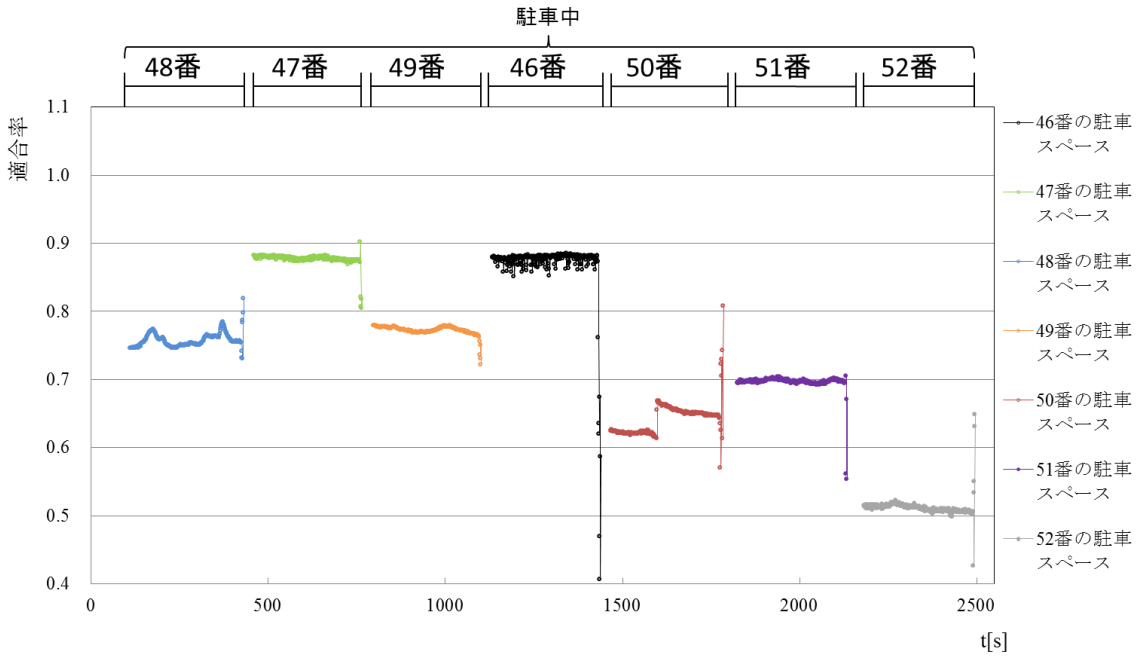

図 2.24 違法車両をテンプレート画像とした場合の検知結果

図 2.23 では, 契約車両として駐車されている車両をテンプレート画像として, テンプレートマッチングを行っているため, 適合率にほとんど変化はなく, どの箇所の検知結果も 1.0 あたりを推移していることが分かる．図 2.24 では，違法車両をテンプレート画像として，テンプレートマッチングを行っているため, 図 2.23 の適合率の値よりも大きく下回っていることが分かる．また，どの箇所の検知結果も適合率の値 0.9 よりも下回っていることが分かる．このことから, 違法車両を検知するためには, 適合率の値 0.9 付近で閾値の設定をすることが有効だと考えられる．図 2.23 と図 2.24 の結果から，テンプレートマッチング法を利用することで，契約車両と違法車両を区別することが可能であるということが分かった.

2.6　通報機能

通報機能に関しては，テンプレートマッチングで違法駐車の車を検知した場合，図 2.12 の④の部分で，車が駐車されている箇所の駐車番号を記載し，その時の画像をメールに添付して定められた宛先へと送信するシステムにしている．図 2.25 に違法駐車の車を検知した際に送られる通報のメールの例を示す．

図 2.25 通報のメールの例

第 3 章　考察

違法駐車の検知のため晴れの日と，雪の日，の 2 パターンでの撮影をし，テンプレートマッチング法を用いて車両の検知を行った．その結果から，晴れの日では，車の検知が十分に可能であると考えられる．また，雪の日の検知結果から，多少の天候不良でも，テンプレートマッチング法を用いた車の検知は有効であることを確認することができた．

図 2.15 より，時間の推移で変化する建造物の影の影響以外では，誤検知が発生することはなかった．この結果から，正規化相互相関を用いることで，日光の明るさの変化の影響は受けづらくなり，この手法は今回の違法駐車の検知に 向いているということが分かった．

今回の違法駐車の検知は，外が十分に明るい時間帯でしか使用することができない．しかし，違法駐車は夜中の時間帯にも起こり得る．これは今後解決していかなければならない問題である．この解決法としては，駐車スペースごとにセンサーライト等を取り付けることが考えられるが，この方法はあまり現実的な解決法とは言えない．そこで，夜中の時間帯では，駐車場の入口に高性能・高品質な e 自警ネットカメラを 1 台設置することで，確実に，駐車場に進入する車両を記録する．そして，駐車場の契約者や近隣住民の通報があった場合のみ，カメラに記録された画像を調べる．もし，インターネット接続された防犯カメラが，街路灯と同程度の密度で設置されたなら，駐車場のカメラで違法車両の確認が出来たところから，芋づる式に，カメラを順次切り替えながら，車両を追跡していくことが出来る．そのため，夜中の時間帯は，このような手法を用いることが有効だと考える．

第 4 章　結論

本研究室が提案するようなネットワークカメラが，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，犯罪の容疑者，容疑車両を，どこまでも追跡していくことが可能となる．また，近年では，通行人の顔と手配写真を照合する技術や不審な動きを検知する技術，などの画像解析技術が開発されてきている．このような高密度に設置されたネットワークカメラと画像解析技術を活用することにより，犯罪抑止・容疑者検挙以外にも，利便性の向上，地域社会の安全・安心も向上し，素晴らしい社会の実現が可能になると予想される．そこで，本研究室は，防犯のためのカメラシステムをさらにより良くするための足掛かりとして，今回，e 自警ネットカメラを活用し，違法駐車を検知した場合通報する機能の開発を行った．開発した機能の結論を以下に示す．

- テンプレートマッチング法を用いた車両の有無の判別機能を開発した．
- 車両を検知した場合，メールによる通報機能を実装した．

今後，これらのシステムがより良いものとなり，全国各地で社会実験が行われるようになれば，更なる e 自警ネットワークシステムの普及が可能になるだろう．このような本研究の取り組みが，今後世界中のメディアに取り上げられ世界規模で普及させ，より安全・安心な社会になっていくことを望んでいる．

謝辞

本研究を遂行するにあたり，ご指導いただいた藤井雄作教授，田北啓洋助教，そしてe自警ネットワーク研究会・末広みらいパーキングをはじめとする関係者の皆様に深く感謝いたします.

また，論文の審査をして頂いた主査の群馬大学大学院理工学府教員の小林春夫教授，副査の群馬大学大学院理工学府教員の中沢信明准教授に深く感謝致します.

そして，開発に協力してくれた本研究室の方々，支えてくれた皆様に感謝いたします.

参考文献

[1] Y. Fujii, K. Maru, K. Kobayashi, N. Yoshiura, N. Ohta, H. Ueda, P. Yupapin, " e-JIKEI Network using e-JIKEI Cameras: Community security using considerable number of cheap stand-alone cameras ", ***Safety Sciences***, Vol. 48, Issue 7, pp.921-925, 2010

[2] Y. Fujii, K. Maru, N. Yoshiura, N. Ohta, H. Ueda, Y. Sugita, " New concept regarding management of security camera ", ***Journal of Community Infomatics***, pp.347-356, 1995

[3] 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 ", *社会安全とプライバシー*, Vol.1, No.1, pp.10-18, 2017

[4] NPO, The e-JIKEI Network Promotion institute: http://www.e-jikei.org/

[5] Y. Fujii, N. Yoshiura, N. Ohta, " Creating a worldwide community security structure using individually maintained home computers: The e-JIKEI Network Project ", ***Safety Sciences Computer Review***, Vol. 23, No.2, pp.250-258, 2005

[6] 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向けて ", *社会安全とプライバシー*, Vol.1, No.1, pp.1-9, 2017

[7] 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, Jan. 2010.

[8] Y. Fujii, N. Yoshiura, N. Ohta, "Community security by widely available information technology", ***Journal of Community Informatics***, Vol. 2, No. 1, 2006.

[9] 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 "

[10]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」

[11]加藤蒼悟「e自警ドアホンを用いた社会実験と新型e自警ネットドアホンの開発」平成28年度修士論文

[12]Y. Fujii, N. Yoshiura, N. Ohta, A. Takita, H. Ueda, K. Maru, " Abuse prevention of street camera network by browsing-history disclosure ", ***Journal of Community Informatics***, Vol. 12, No.1, pp.152-156, 2016

[13] Y. Fujii, N. Yoshiura, " Will every streetlight have network cameras in the near future? ", ***SCIENCE***, eLetters, Vol. 347, Issue 6221, pp. 504-506

[14]村松公祐「e自警ネットワークに関する研究 ~e自警機器の開発と社会実験~」平成26年度修士論文

[15]ネットワーク型e自警カメラシステム「e自警ネットカメラ」の実証実験サイト閲覧記録一覧(2018/1/15 アクセス):

http://www.fmx.ics.saitama-u.ac.jp/e-jikei/print.cgi

[16]物体検出 − opencv 2.2 documentation - OpenCV.jp (2018/1/17 アクセス):

http://opencv.jp/opencv-2svn/cpp/imgproc_object_detection.html?highlight=template#matchTemplate

[17]テンプレートマッチングの原理・計算式・例題（SAD, SSD, NCC）(2018/1/17 アクセス):

https://algorithm.joho.info/image-processing/template-matching-sad-ssd-ncc/

学会発表リスト

K .Kamioka, A. Takita, N. Ohta, Y. Fujii, " Detection of illegal parking for e-JIKEI Network Camera in the social experiment site ", ***International Conference on Mechanical, Electrical and Medical Intelligent System 2017***, Kiryu City Performing Arts Center, Kiryu City, Gunma, Japan, Nov 29, 30 & Dec 1 2017