昭和37年9月15日第三種郵便物認可　三菱電機技報　78巻8号（通巻879号）　2004年8月25日発行（毎月1回25日発行）

Changes for the Better

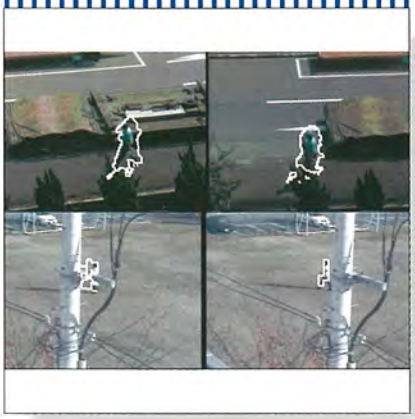
MITSUBISHI

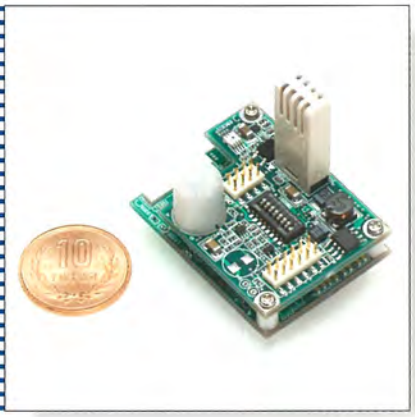
三菱電機技報

Vol.78 No.8

2004 8

特集「物理セキュリティ」





ISSN　0369-2302／CODEN:MTDNAF

三菱電機技報 Vol. 78 No.8 2004

目　次

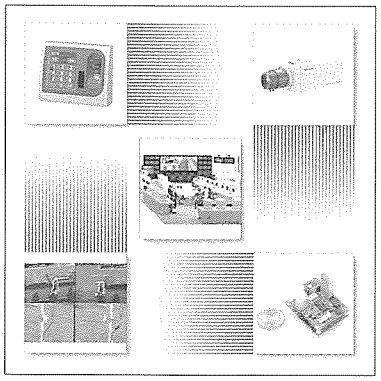
特集「物理セキュリティ」

Physical Security System

特許と新案

スポットライト

三菱統合ビルセキュリティシステムに国際標準暗号“MISTY”を搭載



表紙

物理セキュリティ

三菱電機は，安全と安心を支える様々な製品をオフィスビル，商用施設，工場や研究所，公共施設などに幅広く提供している。この特集号では，それらのうち，物理セキュリティに関する要素技術と各種ソリューションを紹介する。

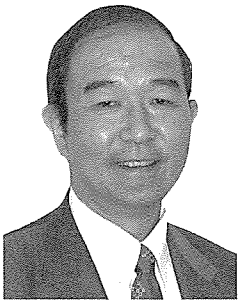
出入管理システム，画像監視システム，侵入検知システムなどに代表される物理セキュリティであるが，最近では，それらの要素技術である個人認証技術，画像処理技術，ネットワーク技術にも注目が集まっている。

表紙は，指紋照合装置とデジタル監視カメラ，集中監視センターと画像処理による人物検出のイメージ，無線によるセンサネットワークの構築を可能とする小型無線モジュールである。

巻/頭/言

物理セキュリティ特集に寄せて

On Real World Security Technologies



松山隆司
Takashi Matsuyama

21世紀社会を特徴付けるキーワードの1つとして“グローバリゼーション”がある。すなわち，

1．グローバルな情報通信ネットワークが，政治，経済，産業，文化，教育，娯楽などあらゆる個人的・社会的活動基盤を支え，我々人類は，生身の人間として暮らしてきた“物理的実世界”とは全く異なった“情報ネットワーク社会”においても暮らすことになる。

2．一方，物理的実世界においては，交通・物流ネットワークの発展により，人や物の移動がグローバルかつ高速・大量化し，生活空間・環境の拡大とともに，“宇宙船地球号”や“地球市民”という意識が芽生えつつある。

こうしたグローバリゼーションは，多様かつ広範な人的・物的交流による新たな文化・文明の創発や産業・経済の発展をもたらす反面，人々は，未知なる人，物，制度への不安に絶えずさらされることとなり，安全・安心に対する要求・要望が急速に高まっている。

安全・安心を確保するための技術として，近年，情報セキュリティ，物理セキュリティが注目されており，一般に，前者は情報ネットワーク社会，後者は物理的実世界におけるセキュリティ確保を目指していると考えられる。しかし，我々人間がこれら2つの社会・世界において同時に暮らしていることを考えると，両セキュリティ技術を統合した社会セキュリティの実現が重要となる。

この特集ではマルチメディア情報処理技術を活用した物理セキュリティシステムの開発に焦点が当てられているが，社会セキュリティシステム構築につながるものとして筆者が注目しているものに“センサネットワーク”がある。これは，多種多様なセンサを物理的実世界に埋め込み，得られたセンサ情報をネットワークを介して時空間的に統合するとともに，データベースに記録されている履歴情報やシミュレーション結果などとの比較・評価を行うことによって，物理的実世界のリアルな情報と，情報ネットワーク社会に蓄積されている情報とを一体化することを目指している。すなわち，センサネットワークによって情報ネットワーク社会と物理的実世界とがマルチメディア情報を介してリアルタイムに統合され，両社会・世界の整合性が常に保証されることによって社会基盤に対する信頼性・信用度が向上し，人々が安心して暮らせるようになる。センサネットワークの重要性は米国においても認識されており，NSF (National Scientific Foundation)によるセンサネットワーク関連の研究開発プロジェクトが，2000年6件，2001年20件，2002年46件，2003年102件と急増している。

セキュリティにかかわる技術開発を行う場合，セキュリティの問題は社会そのものの在り方に密接に関係しており，性能やコストといった技術的側面だけでなく，21世紀社会をどのように作っていくのかといった視点が不可欠であり，エネルギー，交通，物流，情報通信などに関する技術とセキュリティ技術との総合化を図ることによって信頼できる社会基盤システムを構築することが今後ますます重要になると思われる。

◆京都大学大学院情報学研究科 教授　Professor, Graduate School of Informatics, Kyoto University

巻頭論文

三菱電機トータルセキュリティソリューションの推進


市毛正行*


佐々木和則**


朝日宣雄***

Total Security Solution by Mitsubishi Electric

Masayuki Ichige, Kazunori Sasaki, Nobuo Asahi

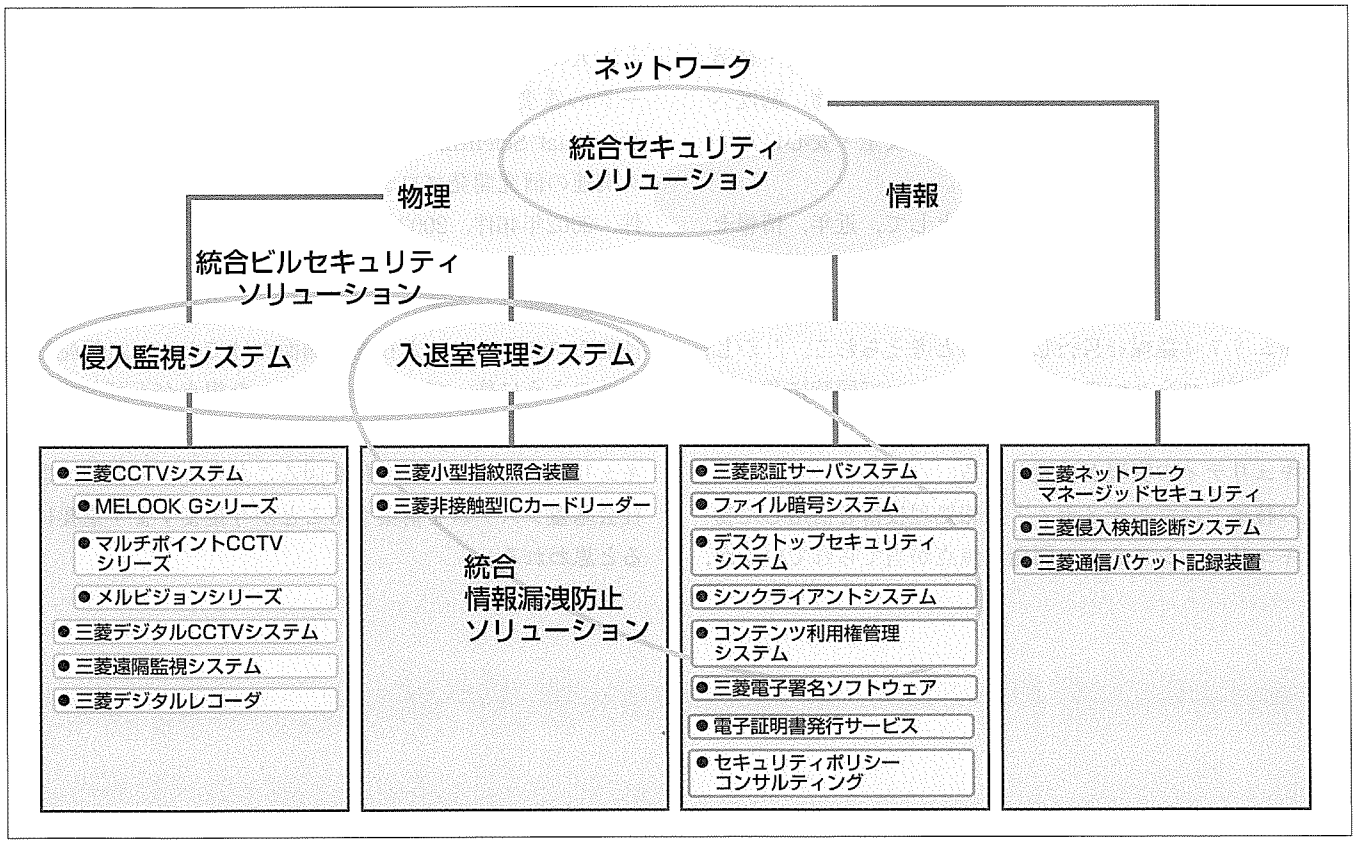
要　旨

1990年代半ばから急速に普及したインターネットにより，組織を越えて流通及び共有される情報の量が飛躍的に増加し，その反面，機密情報の漏洩(ろうえい)が深刻な問題となってきた。また，侵入・盗難事件，商店街・学校などでの犯罪も年々増加しており，特に米国での同時多発テロ事件以降急激にセキュリティシステムへのニーズが高まっている。これらに対応した侵入・不審者監視システムへの取り組みも重要な課題となっている。

情報漏洩の防止や侵入・盗難などのセキュリティリスクへの対応には，出入口からの侵入防止，ネットワークからの侵入防止，及び，内部・関係者による犯罪・不正の防止という3つの側面からの防止策を講じるとともに，特に，情報系においては，設定・操作ミスなどのヒューマンエラーによる被害を最小限に食い止めるための仕組みも考慮すべきである。

これらのセキュリティ対策は，従来個別のシステム導入にとどまっていたが，業務効率を低下させずにセキュリティホールを最小限に押さえ込むためには，体系的な導入が必要である。三菱電機グループでは，このようなセキュリティリスクへの対応を支援するため，従来から取り組んできた情報セキュリティ及び物理セキュリティの各システムを体系化し，新しい時代のトータルなセキュリティソリューションとして提案している。

三菱電機技報2004年4月号[(1)]ではこのうち情報セキュリティソリューションに焦点を当てた特集として様々な技術を紹介したが，今回の特集では，物理セキュリティソリューションとそのインテグレーションに焦点を当て，最新の技術動向を紹介する。



三菱電機のトータルセキュリティ体系

侵入監視システム，入退室管理システム，情報管理システム，ネットワーク管理システムにより，物理系・情報系の両面からセキュリティリスクへ対処する。効率的にセキュリティを管理するためには，体系的な統合ソリューションが望まれる。ビルの監視制御と出入管理を中心に統合する“統合ビルセキュリティソリューション”，工場のような広いエリアのあらゆるセキュリティ管理を統合する“統合セキュリティソリューション”，また，情報の漏洩防止を物理系・情報系の両面から統一的に管理することを可能とする“統合情報漏洩防止ソリューション”などが統合ソリューションの例である。

*営業本部 戦略事業開発室長　**先端技術総合研究所 物理セキュリティシステム開発プロジェクトマネージャー(工博)　***営業本部 戦略事業開発室 専任

1. まえがき

1990年代半ばから急速に普及したインターネットにより，組織を越えて流通及び共有される情報の量が飛躍的に増加し，その反面，機密情報の漏洩が深刻な問題となってきた。また，侵入・盗難事件，商店街・学校などでの犯罪も年々増加しており，特に米国での同時多発テロ事件以降急激にセキュリティシステムへのニーズが高まっている。これらに対応した侵入・不審者監視システムへの取り組みも重要な課題となっている。

企業や自治体等で大量に処理される個人情報の漏洩については，最近，事件・事故の両面で発生件数が増加しており，個人情報保護法などの法整備，及び，体系的なセキュリティ対策を推進するISMS(情報セキュリティマネジメントシステム)などの認定制度の整備が進められている。

ISMSでは，様々なセキュリティリスクに適切に対応するためには，組織が自らのリスクアセスメントにより必要なセキュリティレベルを決め，プランを持ち，資源配分して，システムを運用管理することが重要であるとしている。そして，そのセキュリティ対策は，情報セキュリティ，物理的及び環境的セキュリティ，人的セキュリティなど広範囲なものが対象となっている。

三菱電機グループでは，このような多岐にわたるセキュリティリスクへの対応を支援するため，従来から取り組んできた情報セキュリティ及び物理セキュリティの各システムを体系化し，新しい時代のトータルなセキュリティソリューションとして提案している。本紙2004年4月号では，このうち情報セキュリティソリューションに焦点を当てた特集として様々な技術を紹介したが，今回の特集では，物理セキュリティソリューションとそのインテグレーションに焦点を当て，最新の技術動向を紹介する。

本稿では，トータルセキュリティの体系及び物理セキュリティを中心とした技術課題とソリューション事例を中心に述べる。

2. 近年のセキュリティリスクの傾向

2.1 セキュリティリスクの増加とその原因

様々な社会環境の変化に応じて，侵入・盗難などの犯罪件数は年々増加している。その中でも，特にコンピュータやネットワークの脆弱(ぜいじゃく)性をねらったハイテク犯罪の増加は，近年のインターネットを中心としたIT化の普及に伴い急速に増加している(**図1**)。

図2は，2002年から2004年に起きた主な個人情報漏洩事件ついて，独自にその原因を次の4つに分類した結果である。

(1) 情報・ネットワーク不正アクセス

インターネットからの不正侵入やコンピュータへの不正ログイン等のハイテク犯罪による情報漏洩

(2) 物的不正アクセス・盗難

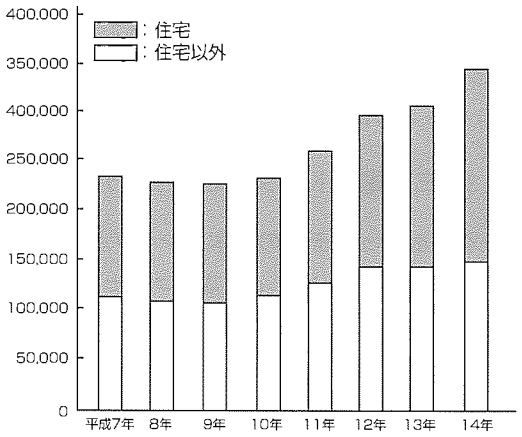
ドアや窓から物理的に不正侵入され，パソコンやディスクを盗難されることによる情報漏洩

(3) 内部犯罪

業務として情報にアクセスできる権限のある関係者が故意に情報を外部に漏洩

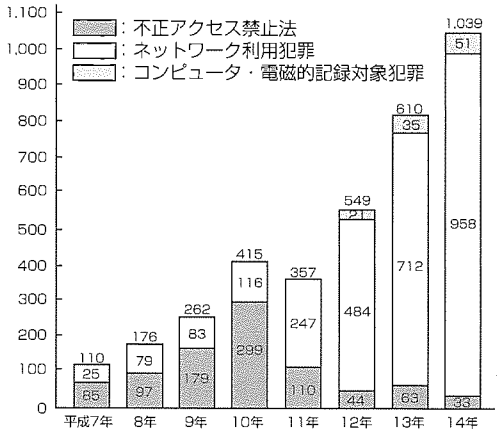
(4) 設定・操作ミスなど

ウェブサイトのアクセス権設定ミス，メール等の誤送信，パソコンの置き忘れなど



出典：セキュリティ産業年鑑2003(日本実業出版(株))

(a) 侵入盗認知件数



出典：警察庁ホームページ「ハイテク犯罪対策」(2003.6)
セキュリティ産業年鑑2003(日本実業出版(株))

(b) ハイテク犯罪検挙事例

図1．セキュリティリスクの増大

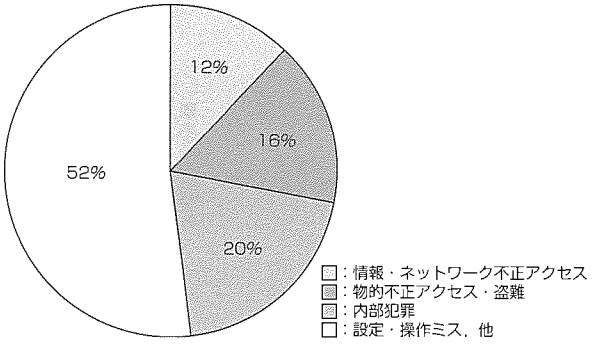


図2．個人情報漏洩の原因

その結果，約半数が設定・操作ミスなどが原因である一方，残りの半分は何らかの故意のある犯罪行為であることが分かる。犯罪行為の内訳は，情報・ネットワーク不正アクセスが12%，物的不正アクセス・盗難が16%，内部犯罪が20%とそれぞれほぼ均等発生しており，情報漏洩があらゆるセキュリティの脆弱性をねらってくることが分かる。

2.2 必要な対応策

個人情報漏洩事件の原因分析から分かることは，情報漏洩の防止等のセキュリティリスクへの対応には，出入口からの侵入防止，ネットワークからの侵入防止，及び，内部・関係者による犯罪・不正の防止という3つの側面からの防止策を講じるとともに，約半数を占める設定・操作ミスなどのヒューマンエラーによる被害を最小限に食い止めるための仕組みも考慮すべきであると言える。

3. 三菱電機トータルセキュリティ

3.1 トータルセキュリティの基本コンセプト

図3にトータルセキュリティの基本コンセプトを示す。

まず，機密情報の存在するエリアへの侵入については物理系・情報系ともに不正侵入を防止するとともに，アクセス権のある関係者については通常業務を妨げないようスムーズにアクセスを許可できるようなアクセスコントロールが必要である。通常，物理系の侵入検知には防犯カメラ，赤外線センサなど，また，情報系のネットワークセキュリティにはファイアウォール，IDS(Intrusion Detection System)などのシステムが活用される。アクセスコントロールも物理系・情報系の両面が必要となるが，最近では，ICカードやバイオメトリクスなど本人認証を簡便かつ確実にできる手段を用いる企業が増加している。アクセス権限管理の一元化もミスを防ぐためには重要な手段である。従来は多くの企業において物理系及び情報系の社員データベースをそれぞれの担当部署が別々に管理していたが，最近では，一元的な管理の下に物理系・情報系双方のアクセスコントロールを実施する企業も増えてきた。さらに，個々の情報に対する暗号化などの情報セキュリティ対策により，操作ミス等による被害を最小限に食い止めることも可能となる。

内部犯罪を防止するために，不正監視・記録を徹底することは，一定の抑止力につながるとともに，不幸にして犯罪が発生した場合にも，犯人の検挙や被害からの復旧に対して効果的な情報が得られることから非常に重要である。不正監視・記録は，物理的にはCCTVカメラ＋デジタルレコーダ，情報系ではアクセス記録や通信パケット記録などが一般的である。

なお，公共施設でのセキュリティ，商店街などでの犯罪防止等の物理セキュリティが中心となる場合も，このコンセプトの物理系のシステムでカバーされる。

3.2 トータルセキュリティの適用分野と技術的課題

より良いソリューションを提供するためには，適用分野及びそれらに求められるニーズを整理し，要求される技術課題を解決する必要がある。まず，適用分野としては以下の5分野に分類できる。

(1) 公共エリア：鉄道，道路などの公共インフラ
(2) 広域エリア：不特定多数の人がいる広域スペース（ショッピングモール，地下街，商店街など）
(3) クローズドエリア：境界が塀などで囲まれたエリアとその中にある建物(工場，研究所など)
(4) 共有エリア：複数の企業が同居，共通スペースと専用スペースが混在するエリア(オフィスビル，マンションなど)
(5) パーソナルエリア：戸建て建物，個人宅など

それぞれの適用分野に必要な技術的課題を**表1**に示す。当社では，すべての適用分野に対応するセキュリティソリューションを提供しているが，技術開発に関しては，共通技術を効率良く他の分野へ展開することですべての分野で高い技術力を維持することに努めている。

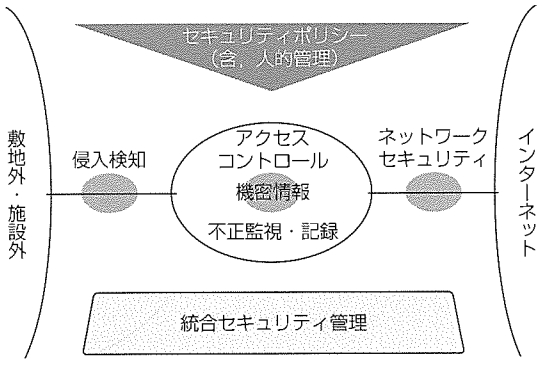


図3．トータルセキュリティの基本コンセプト

表1．具体的アプリケーションと必要技術

技術課題 ＼ 適用分野		公共エリア	広域エリア	クローズドエリア	共有エリア	パーソナルエリア
センサ	画像センサ	○	○	○	○	○
	IRカメラ	○		○		
	機器センサ	○	○	○	○	○
	センサネットワーク	○	○	○	○	○
個人認証	指紋照合			○	○	○
	顔画像認識		○	○	○	○
画像処理	人物検知追跡		○	○	○	
	車番読み取り	○		○		
画像蓄積検索配信	画像蓄積検索	○	○	○	○	○
	画像配信	○	○	○	○	○
暗号化真正性証明	暗号化	○	○	○	○	○
	電子透かし	○	○	○	○	○

3.3 技術課題への取り組み

具体的な共通的な技術課題への取り組み事例を紹介する。

(1) センシング技術

各種侵入検知センサ(監視カメラ，人感センサ，赤外線ビームセンサ，超音波センサなど)を対象とするセンシング技術について，当社は，環境変化に強く誤報の少ない侵入検知カメラ，電波を応用して侵入者を検知するシステムなどの開発に取り組んでいる。さらに，誤報を低減するためにセンサフュージョンによるシステム開発を実施している。

また，新たな配線工事なしに複数のセンサが自律的にネットワークを構成しデータ伝送を行うワイヤレスセンサネットワーク端末，センサネットワーク構成技術などの開発に取り組んでいる。

(2) 個人認証技術

ビル等の出入管理はもちろん，空港での入出国管理，チェックイン等でバイオメトリクスを用いて認証しようとする試みがなされている。非接触型化・偽造対策の観点から真皮，虹彩(こうさい)，静脈流による認証，利便性の観点から顔認証が盛んに開発されている。当社は，従来の指紋認証装置の認証率の高い機能を保持した光学系の非接触型センサの技術開発，利便性の観点から顔画像処理技術開発を実施している。

(3) 画像処理技術

侵入検知・不審者検知システムにおいては，環境変化など複雑な条件があるためいかに誤報を低減するかがポイントであり，画像処理アルゴリズムの高度化が期待される。当社では，ビルや駐車場などで記録した多くの人物が映っている監視映像の中から人物の移動経路や速度など指定した行動パターンに合致する人物を検索する技術を既に開発している。この技術をリアルタイムに利用することで，不審者検知システムへの展開が可能である。

(4) 画像蓄積・検索・配信技術

セキュリティシステムの高度化のために多カメラが設置されると，それらの映像を効率良く収集・蓄積し高速に検索できる機能が不可欠になる。コスト低減の面から，専用線を新設して用いるのではなく，既設のネットワークを利用したシステム開発が望まれる。広帯域の映像ネットワーク上は6 MbpsのMPEG-2映像が複数配信され，狭帯域の外部ネットワークへ配信する場合はゲートウェイで384kbpsのMPEG-4やMotion JPEGに実時間で変換するトランスコード技術開発に取り組んでいる。

また，長時間記録可能な映像記録装置の普及に伴い，不審者等が写る重要なシーンを素早く検索する機能が求められることから，MPEG-7記述子等の画像特徴量や被写体の特徴量を抽出し，それをメタデータとして検索する機能の開発に取り組んでいる。

ホーム，店舗などのセキュリティシステムでは，遠隔で映像を利用して状況を確認する監視形態が増大する。広域監視システムでは，センター側と出先で同じ映像を用いて業務の効率化をすることが望まれている。情報を共有することにより対応策などをスムーズに検討できるように，映像情報を巡回員や他のセンターにインターネット又はモバイル経由で配信する技術を開発している。

(5) 暗号化・真正性証明技術

ホームセキュリティサービスや広域監視システムにおいて，映像データで遠隔監視するようになると，撮影状況等の付加情報を管理する技術や映像に改竄(かいざん)がないこと(真正性)を証明する技術が望まれる。電子透かし技術を適用して付加情報を埋め込む機能，監視映像やそのメタデータが改竄されたか否かを検知する機能，限られた人以外はプライバシーにかかわる映像を見られない機能を開発している。

4. 統合されたセキュリティソリューションの事例

体系的なセキュリティソリューションを提供するため，

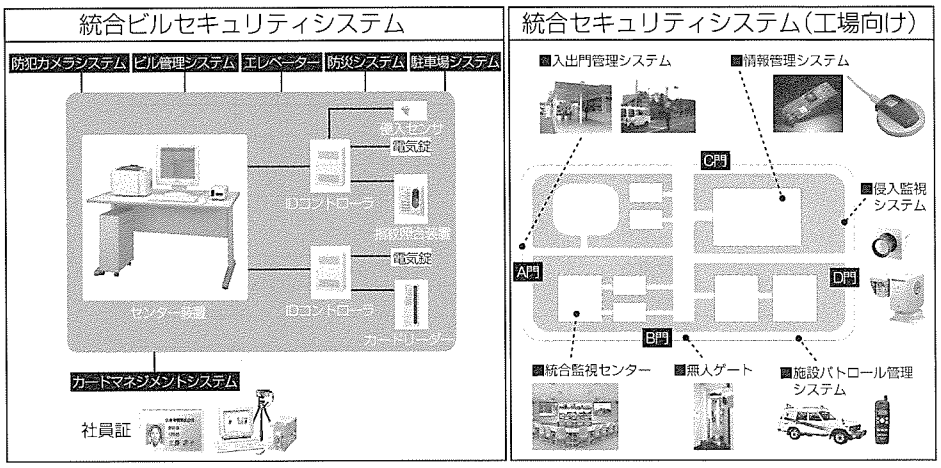


図4．統合されたセキュリティソリューションの事例

当社では，適用分野ごとに個別システムを統合し最適なソリューションとして提供している。ここでは，ビルの監視制御と出入管理を中心に統合する“統合ビルセキュリティソリューション”，及び，工場のような広いエリアのあらゆるセキュリティ管理を統合する“統合セキュリティソリューション”について紹介する(図4)。

4.1 統合ビルセキュリティソリューション

ビル内の物理セキュリティに関する管理を1つのシステムに統合することでより確実なセキュリティ管理を効率良く運用可能とするソリューションであり，次の特長を持っている。

(1) 統合システム
- 入退室管理機能，画像監視機能，防犯センサ監視機能を一つのシステムに統合
- 入退室操作や侵入検出に合わせた画像記録及び検索
- 無人になった区画を防犯センサで監視

(2) 自律分散
- ネットワークなどシステムの一部に障害が発生しても，各構成機器が独立して動作可能

(3) 個人識別端末のラインアップ
- 磁気カードリーダー，ICカードリーダー，非接触型カードリーダー，キーボックス(キーホールドタイプ／シリンダタイプ)，指紋照合装置，アクセスゲートの中から用途に合わせた選択が可能
- 特に高度なセキュリティが要求される場合は“テンキー(暗証番号)＋カードリーダー”や“カードリーダー＋指紋照合装置”といった2要素認証の組合せも可能

(4) 大規模構成
- 1万人以上の個人情報を登録可能

4.2 統合セキュリティソリューション

工場のような広いエリアの場合は，出入する人や車の数が格段に大きくなる上に，外部からの侵入経路も多くなる。このため，あらゆる情報を一元的にリアルタイムで把握し，犯罪を未然に防ぐとともに，不測の事態に対しては素早い対応がとれる統合システムが重要となる。

(1) 入出門管理システム
- 非接触型ICカードとフラッパーゲートで，入出門を一人ずつ確実にチェック
- 来客管理システムとの連携により，ビジターと社員の入出門を一括管理可能
- 車両ナンバー読み取り装置により，車を1台ずつ自動的にチェックし，人と車の一体管理が可能

(2) 統合監視センター
- 部門ごとの監視・管理システムデータをまとめ，分析し，対処の指示を実行
- 従来個別に構築・運用されていた警備システム，施設管理システム，情報処理システムの一元管理で，効率的かつスピーディな対処が可能
- 各種統計情報や人員掌握など，災害時の危機管理，総務部門・人事部門での情報の有効利用が可能

(3) 施設パトロール管理システム
- 車載小型カメラやGPSを組み合わせ，現場やパトロール先の正確な状況把握が可能
- 不審な人や車を発見した場合，入出門管理システムとの照合により，迅速な判断及び対処が可能
- 現場の監視映像を携帯電話から静止画／動画でセンターへ無線伝送

5. むすび

三菱電機グループの提唱するトータルセキュリティのコンセプト及びソリューション体系について述べた。情報系・物理系を体系的に統合したセキュリティソリューションの普及及び高度化を推進していく所存である。

参考文献

(1) 三菱電機技報：特集「安全・安心を支えるITソリューション」，**78**，No.4 (2004)

オフィスビルのセキュリティ運用支援システム “カードマネジメントシステム”

水野邦一*
吉川　寛**

The Support System for Operators of Office Building Access Control System, “ID Card Management System”

Kunikazu Mizuno, Hiroshi Yoshikawa

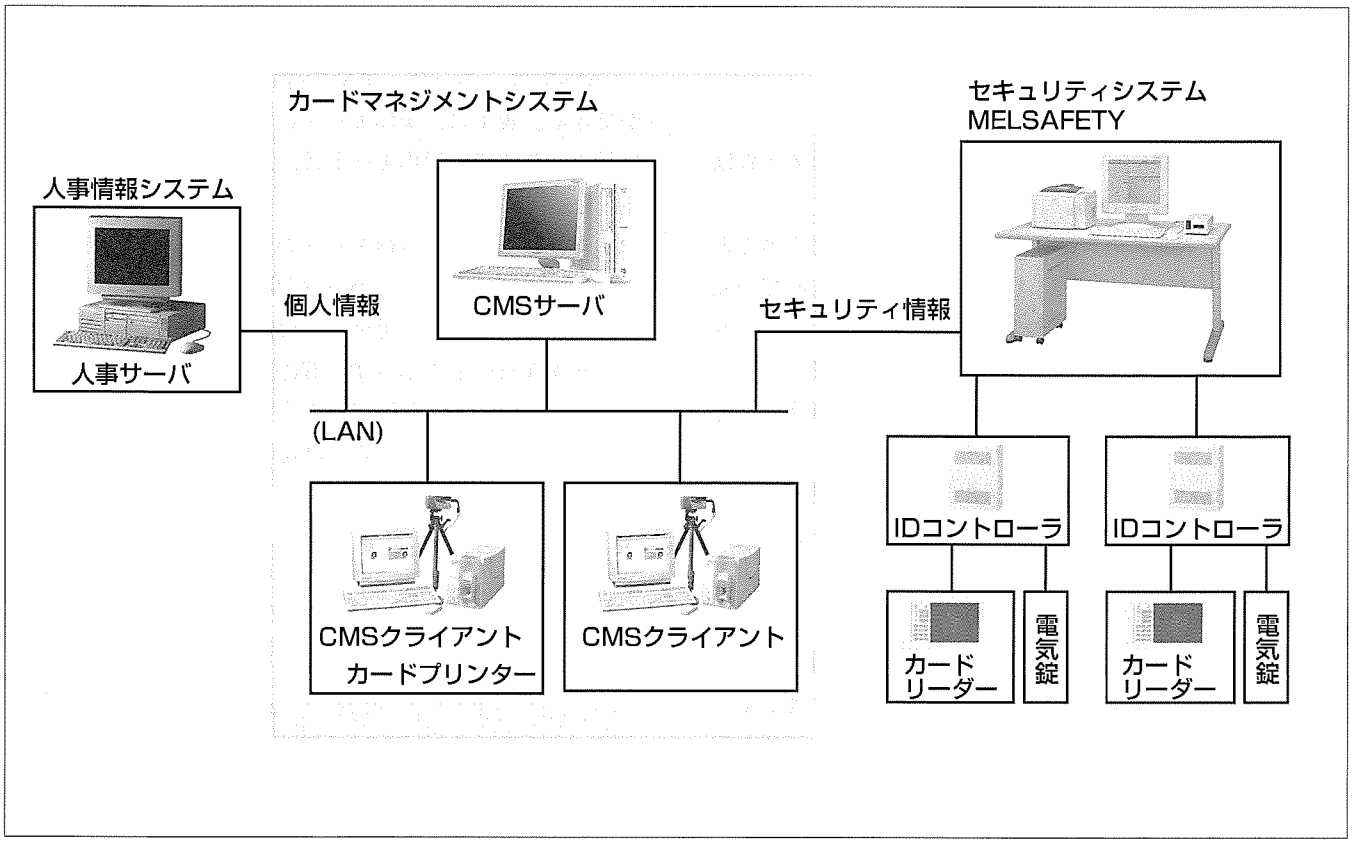
要　旨

昨今，オフィスビルでは，IDカードを利用したセキュリティシステムが基幹設備として位置付けられるようになってきた。オフィスビルは企業のグローバル化，業務形態の多様化から24時間稼働を求められ，また，オフィスワーカだけでなく訪問客やビルメンテナンス業者，運送業者など様々な人が入館し利用する。そのような状況で，IDカードの管理を含めビルの入館セキュリティの運用は複雑であり，管理上も多大な負荷となっている。

本稿では，セキュリティの管理・運用業務を支援するシステムとして，カードマネジメントシステム(Card Management System：CMS)について紹介する。

CMSは，ビルのセキュリティの管理・運用の効率化を目的としたシステムであり，セキュリティシステム又は人事システムと接続して以下のような機能を実現する。

(1) IDカードの印刷，発行管理と通行制御への即時反映
(2) 外来者の受付，入館管理業務の支援
(3) IDカード使用記録に基づく在場把握・施設利用集計管理
(4) 管理者の運用ニーズに応じた通行権限設定手段の提供
(5) 人事システムとの個人情報の共有(個人情報更新の自動化)



カードマネジメントシステム(CMS)のシステム構成例

CMSは，セキュリティシステムと接続して通行制御の判定基準となる通行権限や通行履歴などのセキュリティ情報を授受し，ビル管理者に対してセキュリティ管理上有効なデータとして提供する。また，人事情報システムと接続し，人事異動の際にセキュリティシステム上の個人情報を自動更新することにより，管理の省力化を図る。

*ビル事業部　**稲沢製作所

1. まえがき

近年のオフィスビルでは，入館・入室におけるセキュリティと利便性とを兼ね備えたシステムとして，IDカードを利用したセキュリティシステムが広く導入されている。セキュリティシステムを運用する上で，ビル管理者に求められる業務には次のものが挙げられる。

(1) 利用者の個人情報の取得とセキュリティシステムへの登録
(2) IDカードの発行管理
(3) IDカード紛失時処理
(4) 通行履歴の管理
(5) 外来者の入館管理

様々な業態の利用者が頻繁に出入するオフィスビルにおいて外来者の受付管理や館内の通行許可設定は非常に煩雑であり，また，利用者の異動に伴うセキュリティシステム上の個人情報の更新もビル管理者の負担となっている。

本稿では，上記のセキュリティ運用を支援するシステムとしてCMSについて説明する。CMSは，IDカードの発行と個人情報の管理を容易にし，セキュリティシステムとの連携によって外来者にカードの即時発行を行うと同時にセキュリティシステムで使用可能とする。また，セキュリティシステムで保有するセキュリティ情報をビル管理者にとって扱いやすい形で提供することにより，ビル管理者のセキュリティ運用における管理業務の効率化を図る。

2. システム構成

CMSとセキュリティシステム及び人事情報システムは，LANで接続を行っている。

セキュリティシステムの通行情報や扉情報などすべての情報は，サーバHIP(Human Interface Processor)で一元管理している。CMSは，このサーバHIPをゲートウェイ的に使用し，CMSで必要とする情報を受け渡しする。

人事情報システムは，人事情報を管理する人事サーバを介して，個人情報の受け渡しを行う。

CMSにおいて，これら他のシステムとの情報の受け渡しは，CMSサーバが実行する。この全体システム構成を**図1**に示す。

2.1 人事情報システムの構成概要

人事情報システムでは，人事異動などの個人情報の変更時に，人事サーバ経由でCMSへ個人情報の受け渡しを行う。個人情報としては，個人番号と所属番号などがある。受け渡しのタイミングは，1日に1回程度とする。

2.2 セキュリティシステムの構成概要

セキュリティシステムは，扉の施解錠状態の監視や発停操作を実行するHIP，IDC(個人識別Controller)などのコントローラ群，及びカードリーダーなどの端末により構成される。

IDCにはカードリーダーと電気錠とを接続し，通行に関する制御を実行する。扉ごとに通行可能な個人のカード情報や，カードごとに操作可能な時間帯などをあらかじめ設定しておき，カードが操作されるたびにその通行可／否を判断し，扉の施解錠制御を行う。また，その際の通行情報を履歴として記録する。

サーバHIPでは，扉の位置(アドレス)情報，アクセス制御情報，個人情報や通行履歴など，セキュリティシステムの情報すべてを管理する。このうちCMSで必要な情報について，CMSサーバとの間で情報の受け渡しを実行する。

2.3 CMSの構成概要

サーバ／クライアント方式を採用し，他のシステムとはCMSサーバのみが通信を行い，必要とする情報の受け渡しを行う。情報は，CMSサーバ上の標準的なデータベースで記憶する。

CMSクライアントは，複数台接続することができ，クライアントごとに操作レベルが決定できる。

CMSクライアントには，カードをセキュリティシステムで使用可能とするために，カード情報を読み込むカード登録機，カード券面に顔写真や氏名などを印刷するカードプリンター，その顔写真を撮影するデジタルカメラや，写真などからデータを読み込むスキャナなどを接続する。

3. 特　長

CMSでは，ユーザー単位で操作レベルを設定することができる。**表1**に，操作モードごとに操作可能な機能一覧を示す。ここで，操作モードは，以下の4レベルとしている。

- 管理モード：各種データの参照・表示を行う。
- 印刷モード：主にカード印刷を行う。
- 操作モード：各種データの設定と監視ができる。
- 保守モード：すべての機能を実行できるが，普段の運用で使用することはない。システムの立ち上げ時などで使用する。

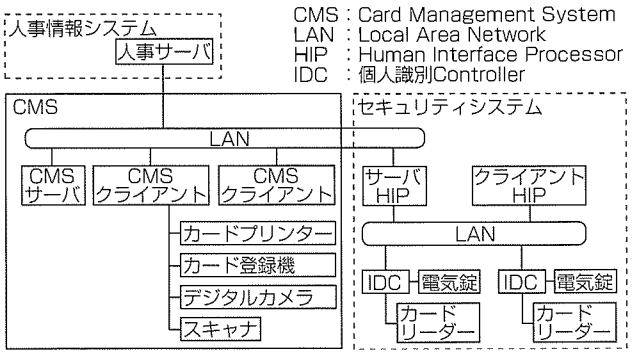


図1．CMSとセキュリティシステム，人事情報システムの全体システム構成

表1．操作モードごとに操作可能な機能一覧

機能＼モード	管理	印刷	操作	保守
操作履歴	○	×	○	○
警報履歴	○	×	○	○
通行履歴	○	×	○	○
履歴のテキスト保存	○	×	○	○
個人情報の編集	×	○	○	○
個人情報の取り込み	×	○	○	○
画像取り込み	×	○	○	○
カードデザイン	×	○	○	○
カード印刷	×	○	○	○
ログインユーザーの設定	×	×	○	○
サーバのシャットダウン	×	×	○	○
システム情報	×	×	×	○

表2．個人情報(例)

項　目	内容（例）	出入共用
個人番号	01234567	有
氏　名	三菱　太郎	有
かな氏名	みつびし　たろう	無
ローマ字氏名	MITSHUBISHI TARO	無
性　別	男	無
生年月日	1982年4月1日	無
所属コード	0001	有
カード発行日	2004年4月1日	無
カード有効開始日	2004年6月1日	有
カード有効終了日	2020年4月1日	有
カードデザイン番号	02	無
顔画像	01234567.JPEG	有

(1)　操作履歴

CMSで操作した内容を，最新の1万件(Max.)まで時系列に記憶する。だれが，いつ，どのような操作を行ったかを検索でき，不適切なカード発行がないかどうかなどをチェックできる。

(2)　警報履歴

CMSで発生した“セキュリティシステムとの通信異常”などの警報を，最新の1万件(Max.)まで時系列に記憶する。

(3)　通行履歴

セキュリティシステムの通行情報(だれがどの扉を何時に通行)したかを，最新の30万件(Max.)まで時系列に記録する。

(4)　履歴のテキスト保存

上記3種類の各種履歴データを，MO(Magneto Optical disk)などの外部記録媒体に，テキスト形式で保存する。特に通行履歴のデータは，出退勤管理や，扉ごとの通行回数の計数などに利用できる。通行回数の計数では，例えば，特定の個人が特定扉に対して不適切に(1日に何回も)アクセスしていないかどうかをチェックできる。

(5)　個人情報の編集

セキュリティシステムで使用するカード情報などを設定する。**表2**に，その設定する項目(例)を示す。

ここで，“出入共用”欄に“有”とした項目は，セキュリティシステムでも使用する項目である。

例えば“個人番号”や“氏名”などは，個人を特定するためのデータで，その人がどの扉を通れるかなどの設定に使用する。一方，“ローマ字氏名”などは，社員証などのようにカード券面に印字する場合もあるが，セキュリティシステムでは必ずしも必要でない項目である。ここで，だれが，いつ，どの扉を通行可能かどうかについての設定は，セキュリティシステム側で行う機能分担としている。

また，“顔画像”は，IDカードの券面に印刷し，社員証などとしても利用できる。この顔画像をセキュリティシステムと共用する場合，カードを操作した際に，HIP上にカードに対応する顔画像を表示すれば，カード操作者とその顔画像とを比較することができる。カード券面の顔画像を偽造したカードの不正使用を防止することが可能となる。

(6)　個人情報の取り込み

個人情報は，CMS画面上から設定するが，この機能を使用し，人事情報システムとの通信により，個人情報を簡単に読み込むことができる。

人事情報システムがない場合でも，テキスト形式の個人情報があれば，所定フォーマットに作成し直し読み込むことにより，手入力での作業を省くことができる。

(7)　画像取り込み

社員証などでは，カード券面に顔写真を印刷する場合がある。カードに印刷する顔写真などの画像情報を取り込む機能である。

画像情報は，“JPEG(Joint Photographic Experts Group)”形式などの画像ファイルで読み込むこともできるが，デジタルカメラやスキャナからの直接入力も可能である。

写真に映る顔の大きさは撮影条件などにより左右されるが，トリミング機能を用いて，カードに印刷するのに適切な大きさにそろえることができる。また，トリミング機能は，画像中から顔領域を自動認識し切り取ることもできる。

(8)　カードデザイン

カード印刷するデザインパターンを設定する。カードのデザイン例を**図2**に示す。

カードデザインは，会社名などの固定文字領域，個人の氏名などの可変文字領域や顔写真などの画像領域より構成される。可変文字領域には“氏名”などの変数を，画像領域にはその画像ファイル名などを設定する。

(9)　カード印刷

個人情報や顔画像をIDカード券面に印刷する機能で，上記のカードデザインを選択し，カード種別ごとにカラー印刷を行う。

カードは両面を同時に印刷でき，1枚のカードを約30秒

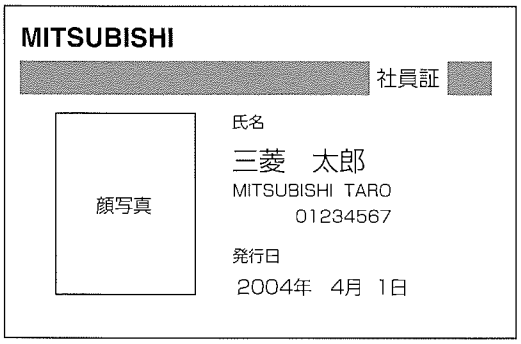


図2．カード印刷デザイン例

で印刷する。また，複数枚のカードをまとめて印刷することもできる。

カード内にICチップを内蔵し，表面が凹凸しているカード券面へも印刷可能である。

また，オプションで個人番号などの情報を，カード印刷と同時に，カード内部のICチップ内や，カード券面の磁気ストライプ部にエンコード記録することもできる。印刷と同時に個人情報をエンコードすることにより，カード発行ミスを防ぐことができる。

カード印刷機能により，例えば外来者等の一時入館者に対して“臨時カード”を即座に発行するなど，柔軟な対応が可能となる。

(10)　ログインユーザーの設定

CMSの操作者を，最大40人まで登録する。各操作者の“操作モード”と“パスワード”などを設定する。

(11)　サーバのシャットダウン

保守点検などでシステム停止を行う場合，CMSクライアントからもCMSサーバをシャットダウンすることができる。

(12)　システム情報

セキュリティシステムなど他のシステムとの接続情報(IP(Internet Protocol)アドレス)などを設定する。

4. むすび

オフィスビルのセキュリティ運用を支援するシステムとして，CMSについてその構成及びその特長について述べた。

CMSの機能を利用して人事情報システムとセキュリティシステムとを連携することにより，人事異動の情報に基づいてセキュリティシステム上の個人情報を自動更新することが可能となり，特に期替わりなどの個人情報更新にかかる業務負荷を大幅に軽減することができる。

また，セキュリティシステムからカード操作記録などの通行情報を受信することで出退勤管理や在館管理を行ったり，又は，特定扉の通行回数を個人ごとに検索することにより特定の人の不適切な行動パターンをチェックするなどの運用に利用することができる。

また，カード発行機能により社員証カードや臨時カードを即時発行すると同時に，セキュリティシステム上でそのカードの使用が可能となる。これにより，個人情報を自社内で閉じて管理できるというメリットもある。

今後，更にCMSの機能を拡充するとともに，セキュリティシステムなどの他のシステムとの通信をより強固に暗号化するなど，セキュリティ強化を行っていく。

参考文献

(1)　曽我部淳子：三菱統合ビルシステム，三菱電機技報，**75**，No.11，739～742（2001）

(2)　星野一郎：三菱統合ビルセキュリティシステム，三菱電機技報，**77**，No.10，667～670（2003）

警備用遠隔画像監視システム

池田奨輝* 合田尚史**
竹田 元* 野田忠義**
渡辺 徹* 三尾武史***

The Remote Surveillance System for Security Services

Shoki Ikeda, Hajime Takeda, Toru Watanabe, Naofumi Goda, Tadayoshi Noda, Takeshi Mio

要 旨

近年，犯罪の凶悪化・スピード化・広域化・多様化が犯罪の増加と検挙率の低下を招き，治安環境の悪化が社会的問題になりつつある。このような社会不安を反映したセキュリティ意識の高まりから，より高度な警備サービスが求められている。

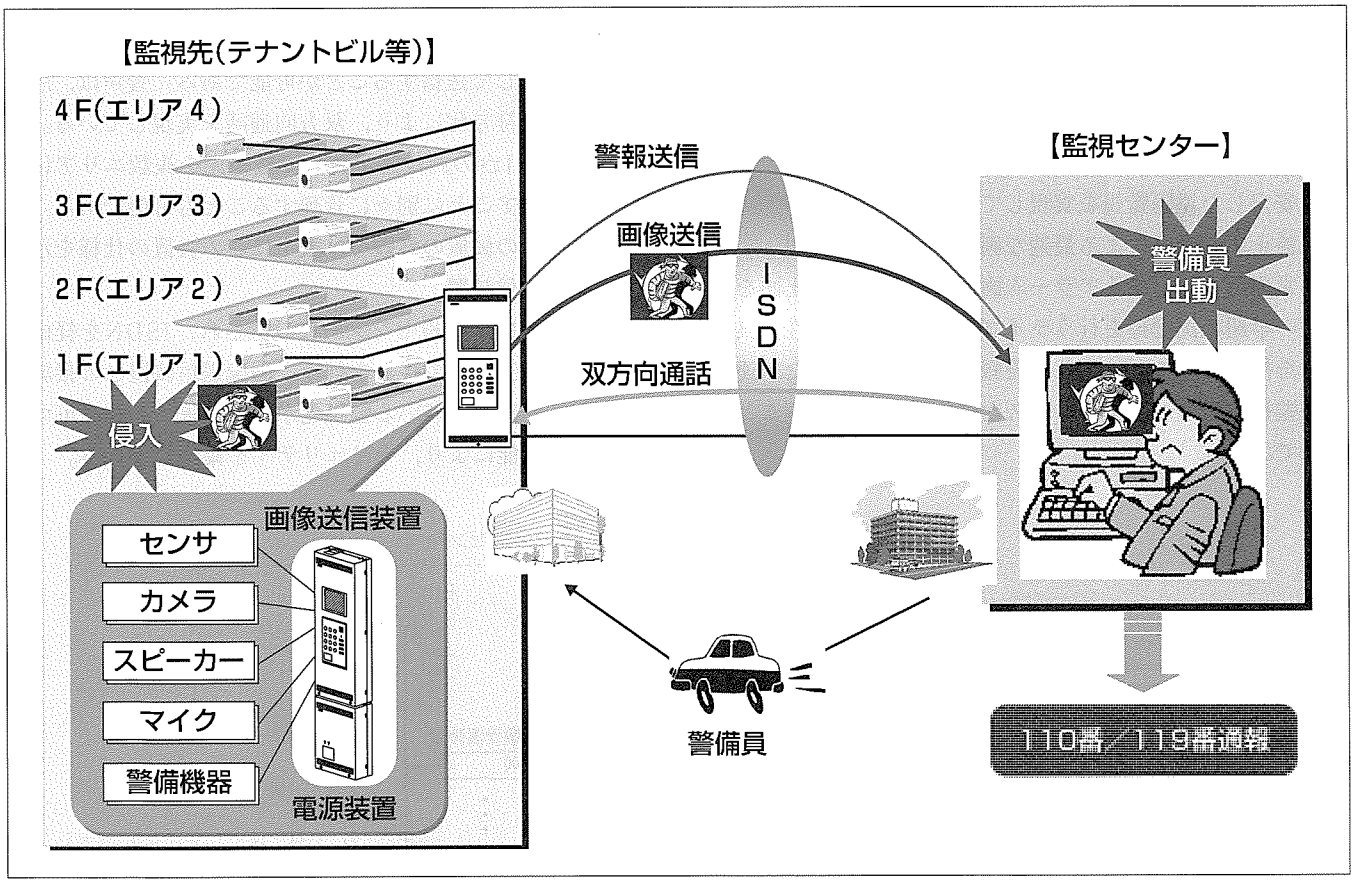
一方，通信インフラのブロードバンド化の進展や画像符号化・伝送・蓄積・検索・処理技術の進歩は目覚ましく，画像情報を用いた高品質な警備用遠隔画像監視システムの構築が現実のものとなってきている。

現在，警備会社や設備管理会社では，店舗・オフィス・工場・マンション・駐車場等，様々な監視先に対し，防犯・防災・設備異常等の警報情報を通信回線経由で監視センターでモニタし，異常が発生した場合は，警備員を監視先に急派する機械警備サービスが主体となっている。

しかしながら，今後，上記のような社会環境に対応していくためには，迅速，かつ的確に監視先の状況を把握し，更に質の高い警備サービスの提供と効率的な運用を実現するシステムの構築が急務となっている。

本稿では，ALSOK綜合警備保障㈱と共同開発を行った警備用遠隔画像監視システムについて述べる。

このシステムは，ALSOK綜合警備保障㈱の警備ノウハウと三菱電機の豊富な実績で培われた遠隔画像監視技術が密に融合したものである。今後も，このシステムをベースにより良いサービスに進化させていく予定である。



警備用遠隔画像監視システムの構成

監視先に設置されたセンサが異常を検出すると，画像送信装置経由で，通信回線(ISDN)を介して，監視センターに警報が通知される。監視センター側の監視員は，警報内容に従い，監視先から送られてくる画像(静止画，動画)や音声を確認することで，警報前後や現在の状況の把握を行い，警備員の出動要請と的確な指示を行う。警備員は，現地に急行し，状況確認と処置を行う。

*通信システムエンジニアリングセンター **郡山製作所 ***情報技術総合研究所

1. まえがき

近年，加速する社会不安(犯罪の凶悪化・スピード化・広域化・多様化による犯罪の増加と検挙率の低下)を反映し，法人や個人レベルのセキュリティ意識が高まっており，より質の高い警備サービスが求められている。

今回開発した警備用遠隔画像監視システムは，このような社会環境下，警備業務における迅速かつ的確な対応と効率的な運用をサポートするためのもので，通信回線を介して，警報信号と画像(静止画，動画)，音声を密に連携させることで，多種多様な監視先を監視センターで遠隔集中監視するものである。

2. システム概要

この章では，このシステムの特長，構成，機能について述べる。

2.1 特　長

このシステムの主な特長を以下に示す。

(1) 警報と連動した画像・音声による統合監視

各種センサ検知による警報と監視カメラ，マイク，スピーカーを組み合わせて，警報情報(防犯・防災・設備異常等)と警報前後の静止画像(以下“アラーム画像”という。)，動画像(以下“ライブ画像”という。)と音声を監視センターで一元的に掌握し，監視業務を遂行・管理することが可能である。また，通信回線に信頼性の高いISDN(Integrated Services Digital Network)を採用することで，失報を防止し，安定した遠隔監視を実現している。

(2) 静止画／動画による最適な画像監視業務の実現

異常原因を特定するアラーム画像に高精細な静止画を，事後の早期状況把握を行うライブ画像に動き追従性の良い動画を採用することにより，警報をトリガーとした一連の画像監視業務の対応をスムーズかつ的確に実行することが可能である。

(3) 音声通話による安心サポート

画像とともに，状況に応じてスピーカーを切り換えての個別／一斉の音声威嚇や指示，双方向通話による相談等を通じて，パニック時の監視先を冷静に誘導し，安心感を与えることが可能である。

(4) 拡張性・柔軟性に優れたシステム

センサやカメラの増設・変更においても，画像送信装置の設定データ(以下“システムデータ”という。)の変更が容易に行えることを可能とした柔軟性に優れたシステムを実現している。

2.2 システム構成

システムを構成する装置について概略を説明する。システム構成を図1に示す。

(1) 画像送信装置

この装置は，監視先に設置され，各種センサ入力，カメラ入力，カメラ制御，音声入出力，機器制御出力I／Fを備え，センサの異常状態を警報として監視センターへ発報後，該当する監視場所の画像・音声を送信する機能を持っている。

警報前後の画像をJPEG(Joint Photographic Experts Group)画像として取り込み，アラーム画像として送信することが可能である。また，ライブ画像は，MPEG(Moving Picture Experts Group)-4で符号化し，動画ストリームデータとして送信することが可能である。音声は，圧縮効率の良い符号化により，双方向通話を実現している。

さらに，1台の画像送信装置で監視先を複数エリアに分けて，エリアごとに別々に管理することも可能である。

図2にこの装置の外観を，表1にこの装置の仕様を示す。

(2) 画像受信装置

この装置は，監視センターに設置され，ISDNを経由して画像送信装置との接続を行う。画像送信装置との接続を管理し，登録されている監視先からの着信のみを許可する識別着信機能により，セキュリティを確保している。

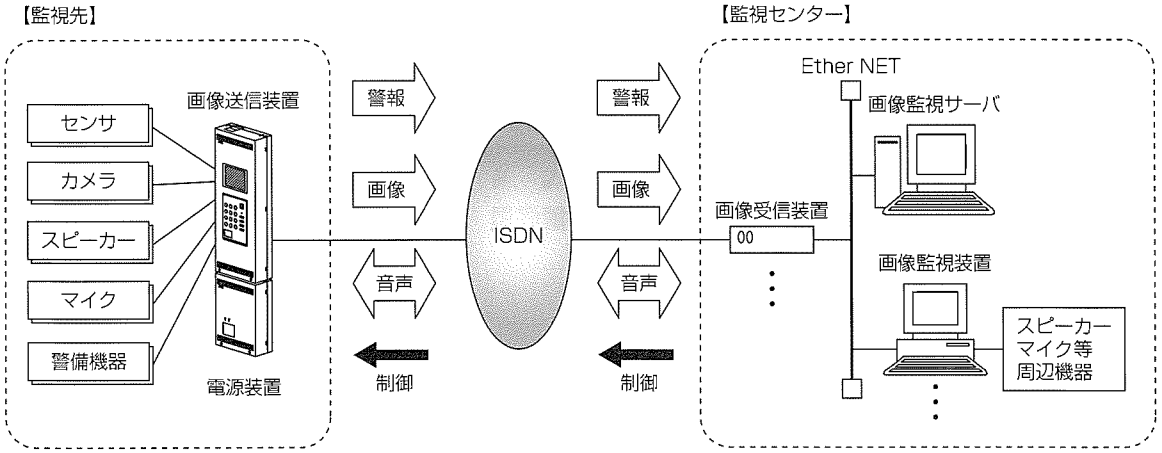


図1．システム構成

また，画像送信装置と画像監視サーバ，画像監視装置間の警報，画像・音声ストリームデータや各種信号(接続要求や画像・音声の送信要求，遠隔制御等)の中継処理を行う。

(3) 画像監視サーバ

この装置は，監視センターに設置され，このシステムを統合的に管理する。監視先からの警報・画像・音声とともに，監視員の音声を蓄積・管理する。また，画像監視装置へ警報情報，アラーム画像，蓄積されたライブ画像等を配信する機能を持っている。

さらに，監視先の情報(システムデータ等)を管理しており，監視先の情報が変更になった場合，画像受信装置を経由してアップデートを行う機能も持っている。

(4) 画像監視装置

この装置は，監視センターに設置され，監視先からの警報発生状況の確認や警報に関連した監視先ライブ画像・音声の確認，アラーム画像の確認，監視カメラの切換え・制御，音声通話，威嚇等，監視員が各種の操作を行う“GUI (Graphical User Interface)”を備えている。

また，画像監視サーバに蓄積されている警報・画像・音声データを外部記録媒体に転送する機能や印刷する機能も持っている。監視先数の増加により監視員が増えた場合も，容易に増設が可能である。

2.3 システムの機能

この節では，システムの主な機能概要について紹介する。

図3に，このシステムの機能イメージを示す。

(1) 警報確認機能

各種センサ検知による監視先の異常状態を，警報として，即座に把握可能な機能である。画像送信装置の各種センサで異常を検知すると，警報として監視センターへ発報する。警報は，画像監視装置に色分け表示され，監視員は，直感的に警報情報(防犯・防災・設備異常等)を確認することができる。

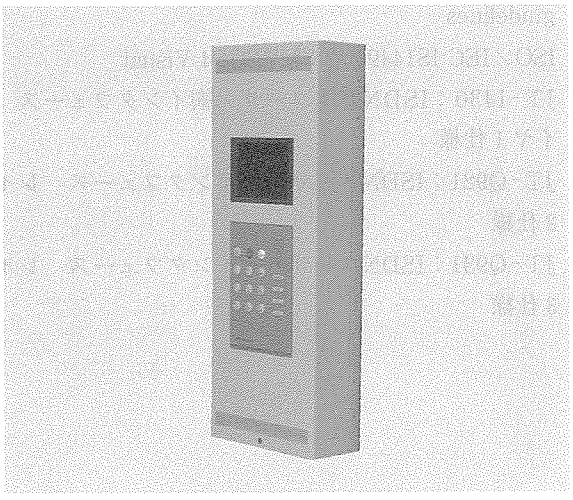


図2．画像送信装置の外観

(2) 自動蓄積機能

監視員が処理している警報はもとより，監視員が他の警報を処理している場合に発生した警報・画像・音声も蓄積する機能である。監視センターは，警報を受信すると，警報情報を記録するとともに，システムが自動応答を行い，ライブ画像・音声，アラーム画像を警報情報と関連付けて自動蓄積を行う。蓄積状況は，画像監視装置上にステータス表示される。

(3) ライブ画像監視機能

警報後の監視先状況をライブ画像・音声で確認することにより，的確かつ素早い対応を実現する機能である。画像監視装置に表示された警報を監視センターの監視員が選択すると，該当する監視先のライブ画像・音声をリアルタイムで表示する。監視員は，カメラ切換え・制御を行い，監視先の状況を確認しながら，対応を行うことが可能である。また，監視センターから，監視先を指定して，ライブ画像・音声で監視を行うことも可能である。

(4) 音声威嚇・双方向通話機能

監視先に対して音声による一次対応を支援する機能である。監視センターから，ライブ監視中に発見した不審者に対する音声威嚇や，火災・設備異常に対する全スピーカーからの一斉音声出力等，一次対応を行うことが可能である。さらに，双方向通話により，トラブル時の相談や監視先状

表1．画像送信装置の仕様

項目		内容
映像	映像入力	NTSC準拠コンポジット信号×8
	内部モニタ	5インチ TFTカラー液晶モニタ
	符号化フォーマット	ライブ画像 MPEG-4：VGA, QVGA アラーム画像 JPEG：VGA, QVGA
	画像蓄積	ローカル蓄積機能 (JPEG)
音声	音声入力	8入力 600Ω／47kΩ 不平衡
	音声出力	8出力 600Ω 不平衡
	内部スピーカー	固定メッセージ，クリック音， インターホン呼出音
	インターホン	インターホン接続可
回線I／F		BRI：64kbps, 2×64kbps
接点	汎用	12入力
	保護／停電	各1入力
	制御出力	8出力
制御	電動カメラ	遠隔制御可
	システムデータ	アップロード／ダウンロード
その他		エリア監視機能，断線監視機能あり
		規模拡張：増設により可能
外形寸法・質量		約(W)215×(D)90×(H)560(mm) 6.5kg以下

NTSC ：National Television Standards Committee
TFT ：Thin Film Transistor
VGA ：Video Graphics Array
QVGA：Quarter VGA
BRI ：Basic Rate Interface

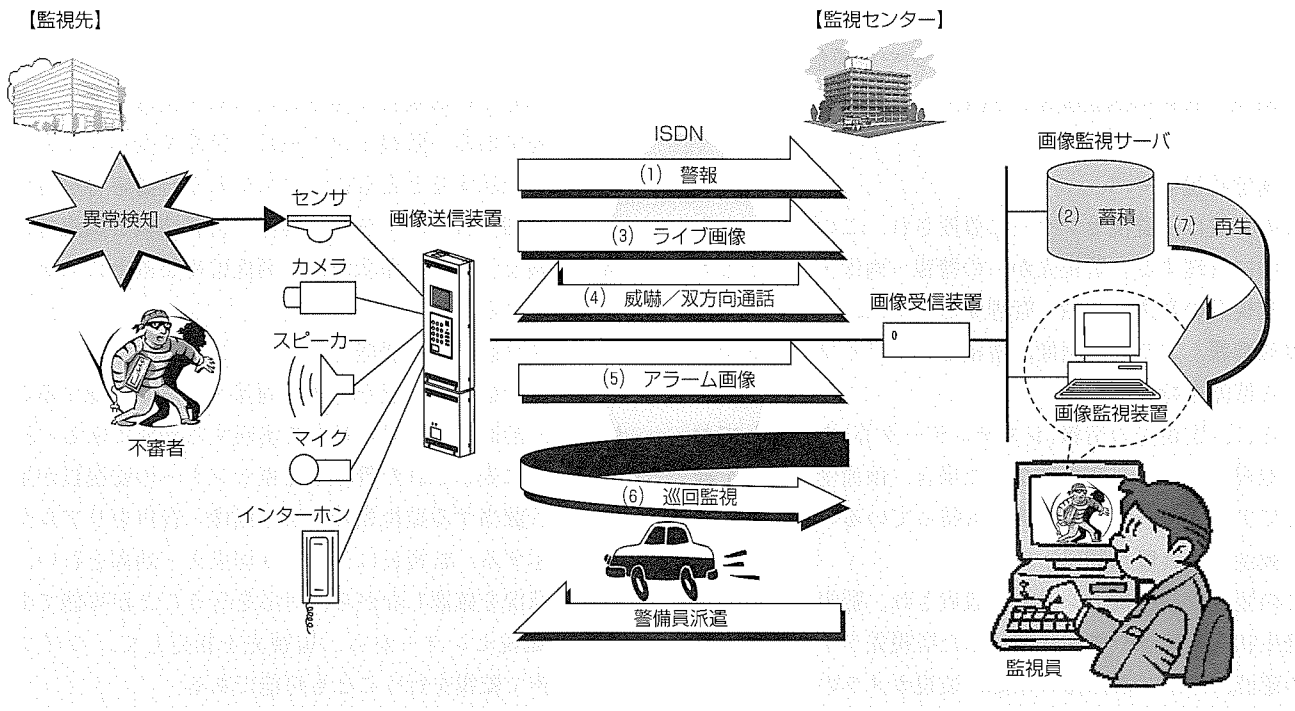


図3．機能イメージ

況の把握，及び的確な指示を行うことも可能である。

(5) アラーム画像監視機能

警報発生原因を即座に確認し，的確な対応を可能とする機能である。監視センターで，ライブ画像・音声確認後，アラーム画像を時系列にサムネイル表示し，状況を確認することが可能である。さらに，画像を選択すると拡大表示することができ，異常原因をより詳細に把握することが可能である。

(6) 巡回監視機能

不審物や不審者の早期発見を支援する機能である。設定した巡回スケジュール(日程，時刻，監視先等)に基づき，画像送信装置と接続し，その時刻の静止画(JPEG)を自動的に取得する。登録してある基準画像と比較し，不審物や不審者を早期に発見することが可能となる。

(7) 蓄積ライブ画像・アラーム画像の確認機能

監視センターに蓄積されたライブ画像・音声，アラーム画像を確認することが可能な機能である。これにより，必要に応じ，過去の監視先状況の確認が可能となる。

3. 効　果

このシステムが実現した警報，静止画，動画，音声を連携させ用途に応じて用いることにより，様々な監視先，監視目的・監視対象に対して，正確かつ迅速な対応が可能となり，更なる業務効率向上とともに，よりきめの細かいサービスの提供が期待できる。

4. むすび

今後も，セキュリティ業界において，画像を活用したニーズはますます高まっていくものと思われる。

顧客満足度向上を最優先に，社内関連部門と連携し，このシステムをより良いシステムに進化させていく所存である。

参考文献

(1) ISO／IEC 10918-1：Digital compression and coding of continuous-tone still images：Requirements and guidelines

(2) ISO／IEC IS14496-2：MPEG-4 Visual

(3) JT-I430：ISDN基本ユーザ・網インタフェース　レイヤ1仕様
JT-Q921：ISDNユーザ・網インタフェース　レイヤ2仕様
JT-Q931：ISDNユーザ・網インタフェース　レイヤ3仕様

ビル向けデジタルCCTVシステム

小林正幸* 玉木茂弘***
野地 誠**
引野 慎***

Digital CCTV for Buildings

Masayuki Kobayashi, Makoto Noji, Shin Hikino, Shigehiro Tamaki

要 旨

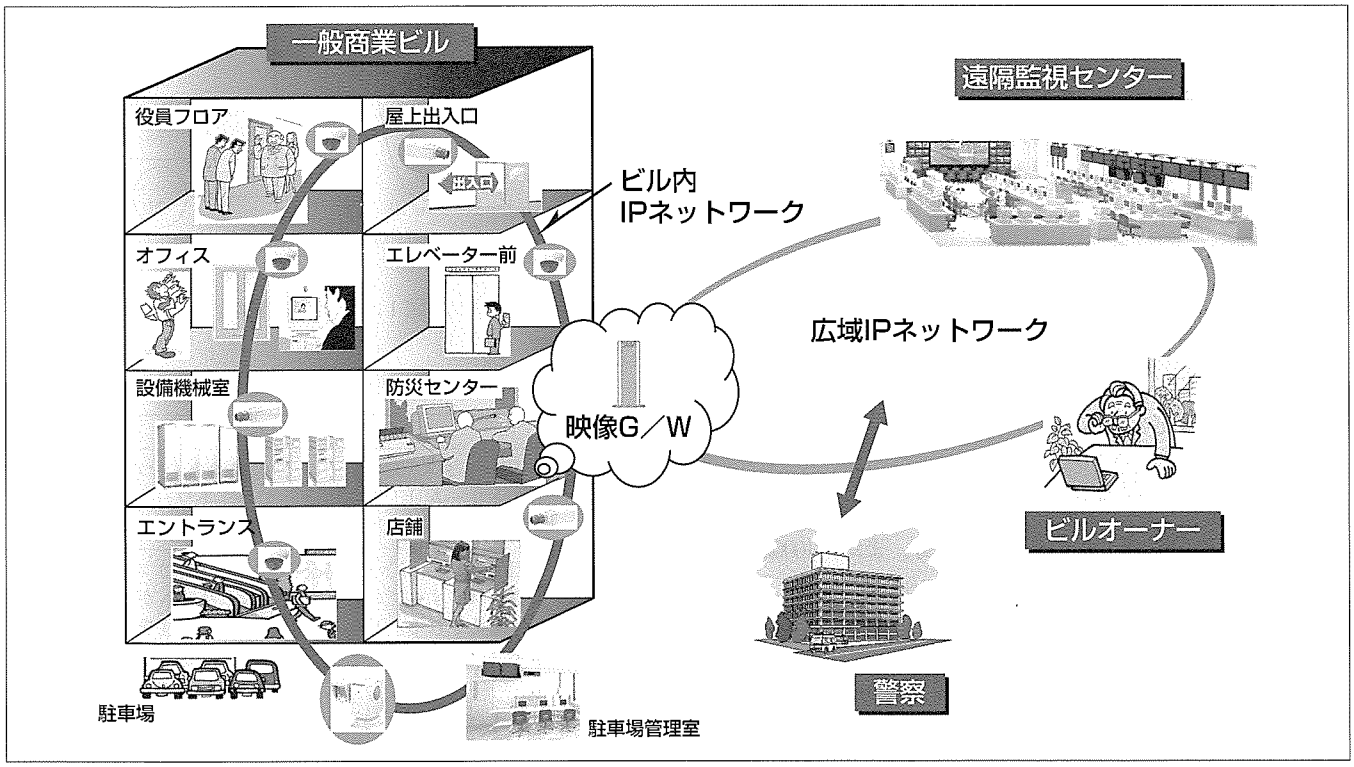
CCTV(Closed Circuit Television)システムは，約50年前から鉄鋼，電力，生産工場など工業用テレビジョンとして利用が始まり，その後，教育，医用，安全監視などの分野に利用が拡大されてきた。特に近年監視分野では，凶悪犯罪の多発から，商店街・学校などの公共施設さらにはマンションや一戸建て住宅など，多方面にわたり導入が進んでいる。

一方，技術的な視点で見た場合，デジタル放送やデジタルスチルカメラにみる“デジタル化”，インターネットにみる“ネットワーク化／ブロードバンド化”，DVDにみる“ストレージ大容量化”などをキーとしたデジタル社会の進展がある。特にビル内監視においてはLANを利用したCCTVシステムを導入したいという要求が増えており，CCTVシステムとしても通信技術及びコンピュータと融合したデジタル総合技術が求められている。

現在，CCTVのデジタル化としては，ユニキャストベースのWebサーバ内蔵型ネットワークカメラが主流であるが，その映像品質から用途は“モニタリング”として利用範囲が制限されている。このような中で，三菱電機は，“防犯”として利用できるマルチキャスト(注1)対応デジタルCCTVシステムを約2年前から市場投入し，多数のインテリジェントビルに納入してきた。

この特集では，ビル向けシステムを中心に，当社デジタルCCTVの特長と訴求点，従来のアナログシステムとの差異，今後の普及のキーとなる技術とその課題について述べる。

(注1) ユニキャストのような1対1通信とは異なり，ある特定の複数クライアントに対する1対n通信を実現する方式である。幹線ネットワークに負荷をかけずに配信できる特長がある。



デジタルCCTVシステムの構成

カメラ端末はIP化され，ビル内広帯域LANに収容される。カメラはマルチキャストストリームを生成し，ネットワーク自体が各クライアントの要求に基づいて分配・配信を行う。また映像G／W(ゲートウェイ)は，広域な場所へシームレスな映像配信を行う。

*通信システムエンジニアリングセンター **郡山製作所 ***情報技術総合研究所

1. まえがき

近年，安価かつ広帯域化への技術進歩が早いＬＡＮ(IEEE802.3)の利用がインテリジェントビルの設備インフラとしてのトレンドである。また，画像を取り巻く環境は，ISO／IECやITU-Tにおける画像符号化の国際標準化や，携帯電話やインターネットにみる画像利用の進展がある。このような背景の中，CCTVシステムは一つの技術的変曲点を迎えている。

映像をデジタル化するメリットとして，距離による映像劣化のない広域伝送，集配信の容易さ，コンピュータとの親和性が高いことなどが挙げられる。しかしながら，デジタル方式によりビル内監視を行う場合，コア製品群のレパートリー化／装置の小型化，画像伝送／制御遅延の対策，システムの低価格化等，課題も多い。

本稿では，これら課題に対するビルの映像監視ソリューションを紹介するとともに，今後の展望について述べる。

2. システム概要

2.1 システムの特長

三菱デジタルCCTVは次の特長を持っている。

(1) 高画質表示

映像をデジタルデータ(VGAサイズ，30フレーム/秒)として伝送することにより，距離による劣化や監視センターにおける信号変換時の劣化がなく，高画質な映像で監視が可能である。

(2) 高画質記録／再生

ネットワークカメラから記録を行う画像ストレージパソコンまで，デジタルワンリンクの構成が可能となり，高画質な映像記録／再生が可能である。

(3) 省スペース化

映像は，マルチキャストストリームでネットワークに送出される。ネットワークに対するクライアント要求により，必要なストリームをネットワークが生成分配しかつ切換えも行う。監視センターでは，映像分配器や切換器が不要となり省スペース化を図ることができる。

(4) 省線化

幹線は映像ストリームの多重伝送効果による省線化が可能であり，100BASEの場合は約８チャネル分，また，1000BASEの場合は約80チャネル分を収容することができる。

(5) 設備間連携

入退室管理設備や防災設備等と連携し，アラーム時の映像自動切換え／動画記録等の連携動作が可能である。信号の取り合いは，ネットワークを介することにより場所の制約は受けない。

(6) 映像の有効活用

監視員の監視業務報告作成時に，デジタル化された静止画を利用したり，また，監視センターで受信する防犯目的の映像のほか，映像G／Wを経由して受付確認用途として映像を社員に配信することができる。

(7) 拡張性

カメラ増設において，幹線工事を行うことなく容易に追加できる。また，映像受信拠点の拡張においても，ネットワークの分配／切換え機能を利用して容易に追加できる。

2.2 システムの構成

ビル向けデジタルCCTVシステムの構成を**図１**に示す。また，各系統における構成概略を**表１**に示す。

2.3 システムの比較

従来のアナログシステムとの比較を**表２**に示す。なお，Webサーバ搭載カメラシステムとの差異は，数フレーム/秒の低画像品質，及びクライアントが増加した場合にカメラからの映像送出レートが下がるなど，防犯監視用途として十分利用できない点である。

3. 主要構成機器とコア技術

3.1 ネットワークカメラ

ネットワークカメラ(NC-5000)はVGA(640×480画素)

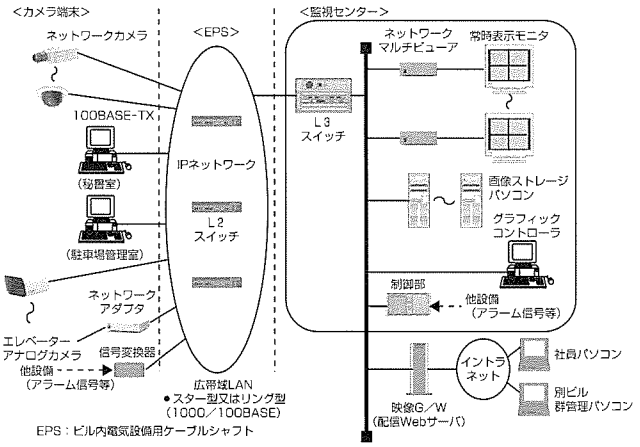


図１．システム構成

表１．構成概略

	内容
入力系	VGAサイズ-30フレーム/秒の映像を，マルチキャストストリーム(UDP／IP)としてネットワークに送出。100BASE-TXでEPSのＬ２スイッチに接続。
伝送系	EPSのＬ２スイッチと監視センターのＬ３スイッチが接続され，すべてのカメラ映像ストリームが監視センターに集約される。リング構成により冗長性を図る。
センター処理系	●ネットワークマルチビューア，画像ストレージパソコン，グラフィックコントローラなどがＬ３スイッチに接続される。各クライアントは，マルチキャスト制御プロトコルであるIGMPにより受信したい映像をネットワークに対し要求する。 ●映像G／Wは，イントラネット上の各クライアントから要求のあるマルチキャストストリームをユニキャストに変換処理し，Web上でセキュリティ確保の上，映像を提供する。

サイズの監視映像を最大30フレーム/秒で圧縮符号化し，100BASE-TXで送信することのできるカメラである。**図2**に外観を示す。

プログレッシブ専用CCDを搭載することにより，従来のアナログカメラよりちらつきが少なく，鮮明な画像を得ることができる。また，画像を複数箇所に同時配信できるマルチキャストに対応しており，複数の受信端末で30フレーム/秒の監視映像を見ることができる。このカメラでは画像の圧縮符号化方式にMJPEG(Motion-Joint Photographic Experts Group)を採用している。これは，監視映像の間欠記録を行う上で空間解像度対応の圧縮符号化方式が扱いやすいこと，さらに，監視センターからのカメラ制御において，他圧縮方式よりも低遅延であるためである。

3.2 ネットワークアダプタ

ビル内に設置されているエレベーター内の監視カメラは，従来のアナログカメラが使用されているため，ネットワークへの収容が必要である。そこで，アナログ信号をデジタル信号に変換するネットワークアダプタ(X-1150)を開発した。**図3**に外観を示す。

この装置の特長は以下のとおりである。

- NTSC信号を入力し，VGA，30フレーム/秒の高レートでMJPEGに変換することができる。
- アダプタ～カメラ間の同軸ケーブルにおいて，映像伝送のほか，回転台制御等を行うワンライン通信機能を搭載している。

3.3 ネットワークマルチビューア

ネットワークマルチビューア(NV-4400)は，ネットワークカメラのVGAサイズの動画をSXGA(1,280×1,024画素)の高解像度モニタに4分割同時表示することができる表示専用装置である。**図4**に外観を示す。

4分割画面は，従来のテレビモニタを使用した4分割画面と比較しておよそ4倍の解像度での表示を実現している。従来のアナログによる多画面表示装置に比べ，入線ケーブル数の大幅な削減，装置の大幅な小型化を実現している。また，MJPEG画像の復号に専用LSIを使用することにより，ソフトウェアデコードでは処理負荷が重くて実現が困難なVGAサイズのカメラ映像を4画すべて30フレーム/秒で同時表示することが可能となっている。

3.4 画像ストレージパソコン

異常発生時の状況確認のため監視カメラの映像は記録保存することが必要であり，記録装置には，多チャネル記録と高画質記録が求められる。画像ストレージパソコンは，1台で映像16ストリームをHDDに間欠記録する装置であり，高品質なMJPEG画像をデジタルのまま記録でき，高画質の保存・再生ができる。なお，アラームに連動した高フレームレート記録も可能である。

図2．NC-5000の外観

3.5 グラフィックコントローラ

ビル監視として異常発生時には，現場状況を迅速・容易に把握する必要がある。そのため，操作器は，シンプルでありかつ必要な情報が容易に得られるものが求められる。グラフィックコントローラは，パソコンのGUIでカメラ映像の選択，表示，操作，及びアラーム情報をSXGAサイズ1画面に集約して操作を容易にしたものである。基本操作画面を**図5**に示す。

図3．X-1150の外観

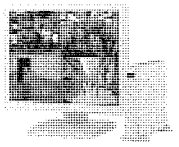


図4．NV-4400の外観

表2．システム比較

			従来アナログ方式(スター型)		三菱デジタル方式(リング型)	
映像品質	監視	画質特性	○	NTSCビデオ信号	◎	RGB信号(VGA：640×480画素)
		動画特性	○	30フレーム/秒	○	同左
	記録	画質特性	○	アナログ-デジタル変換記録／デコード再生	◎	デジタルストリーム直接記録／再生
施工性	端末関連		○	カメラの標準的な設置	○	同左
	支線系(固定カメラ時)		○	同軸ケーブル敷設のみ	△	LANケーブル，電源ケーブル敷設要
	幹線系		○	カメラ台数分のケーブルを敷設要	◎	約80台の集線効果(1000BASE時)
	EPS関連		○	機器設置不要	△	SW・HUB設置のため機器収容盤要
	監視センター関連		△	カメラケーブル／装置ともに規模大	○	カメラケーブル省線化，省機器／省スペース
信頼性(幹線障害)			○	スター型構成。他のカメラには影響しない	◎	リング構成。冗長性あり
配信親和性			○	デジタル化／各種制御モジュール搭載など複雑化	◎	シームレスにイントラネットと接続／配信
拡張性(増設，分散監視)			△	カメラ増設，分散監視拠点増設はケーブル敷設含め複雑化	◎	カメラ増設，分散監視拠点増設とも比較的容易
保守性			○	障害切り分けが容易(通常保守)	○	ネットワーク・オンライン保守。障害切り分けが比較的容易
システムコスト			○	汎用品が多く安価	△	開発過度期であり少々割高

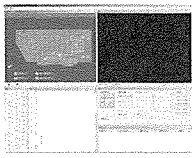


図5．基本操作画面

(1) カメラ選択

平面図上にカメラアイコンを配置し，直感的にカメラ選択できるようにしている。また，カメラ一覧リストからダイレクトにカメラ選択できるインタフェースを用意し，操作性を向上させている。

(2) セキュリティシステムとの連動

センサの異常検知に連動して，アラーム情報のリスト表示，操作画面及び専用モニタへの該当カメラ映像の表示，異常箇所へのカメラ旋回動作を自動的に行う。

(3) エレベーターの停止階表示

不審者がどのフロアで降りたかを判断するため，エレベーター制御設備と通信を行い，操作画面上にエレベーターの停止階を表示する追尾支援機能を搭載している。

3.6 映像G／W（Web配信）

映像利用の多様化により，監視用途以外にビル受付の状況や食堂の混み具合等，監視カメラの映像をビル内で閲覧する要求がある。社内ネットワークのように共有され限られた伝送帯域に映像データを配信するため，マルチキャストの映像ストリームをWeb配信する映像G／W装置を開発した。クライアントは，特殊なソフトウェアの追加なしで映像を閲覧できる。

4. 今後の展望

今後，ビル監視において，デジタルCCTVを普及させていくための技術／課題を以下に述べる。

4.1 人物特定のための技術

より解像度の高いカメラ（例えばXGA：1,024×768画素）での監視が可能になれば，細部までを確認することができ，人物特定はより容易になる。画像伝送容量の増加，被写体照度の確保，カメラ装置の低コスト化などの対策が課題である。

また，監視映像から人物の顔部分を確認しやすい最適な画像に切り出して表示することは，人物特定の補助として非常に有効である。顔画像を最適な形で切り出す画像処理アルゴリズムの開発が課題である。

4.2 IPv6対応システム

現在のIPv4をベースとしたシステムの大きな問題点は，IPアドレス等，設定の困難さにある。IPv6では，基本的に機器がIPアドレスを自動生成するため，ネットワーク設定が大幅に自動化できる可能性があり，より簡単に複雑なシステムを構築できるようになる。また，IPv6は，QoS設定の容易さから，今後のビル内設備が広帯域IPインフラに統合化されていく市場動向からも有効な手段であると言える。IPv6インフラ整備に合わせ，当社も対策・準備を進めていく。

4.3 電源供給

LANケーブルに電源を多重する規格が2003年6月にIEEE 802.3afとして標準化された。LANケーブル1本で約15Wの電力を供給できる。この規格の普及により，ネットワークカメラの電源ケーブルが不要となり，施工面で大きなメリットが期待できる。また，国際的に規格化された方式であり，規格に準拠した多くのネットワーク機器を使用でき，安価にシステムを構築できるメリットも期待できる。

4.4 蓄積ストリーム数の向上

画像ストレージパソコン1台当たりに蓄積できるストリーム数を向上させることは，装置台数の低減，設置スペースの削減，消費電力の低減など，数多いメリットがある。今後は，ストリーム数増加に伴う装置の高処理負荷対策，万一の記録媒体損傷時のデータ保護を熟慮した装置開発が課題である。

4.5 画像処理技術による運用支援

膨大な記録画像から形状や色等によりパターンマッチングを行うMPEG7検索技術，また，人物の行動軌跡から監視員のパラメータ定義／設定により不審者（らしき）人をシステムが発見しアラームを出す画像処理アルゴリズムの開発が課題である。

5. むすび

ビル市場で急激な普及が見込まれるデジタルCCTVについて，アナログ方式との比較，訴求点，コア技術／製品の紹介，今後の展望について述べた。

今後は，各課題に対した解決方法を市場性と照らし合わせ研究開発を行うとともに，コア技術を利用した監視市場の需要開発についても検討していきたい。

当社デジタルCCTVソリューションにより，“より安全で安心のビル・社会”の実現に向け貢献していく。

参考文献

(1) 山下孝一，ほか：LANカメラの開発，映像情報メディア学会年次大会，コンシューマエレクトロニクス部門（2000-8）

(2) 玉木茂弘，ほか：監視システム向け表示用メモリシステムの開発，電子情報通信学会ソサイエティ大会，一般講演B-8通信方式D（2002-9）

(3) IETF：RFC768(User Datagram Protocol)，RFC793(Transmission Control Protocol)，RFC2435(RTP Payload Format for JPEG-compressed Video)，JPEG：ISO／IEC 10918-1

工場・研究所向けセキュリティシステム

芹沢一彦*
橋詰　聡**

Security System for Factory／Laboratory

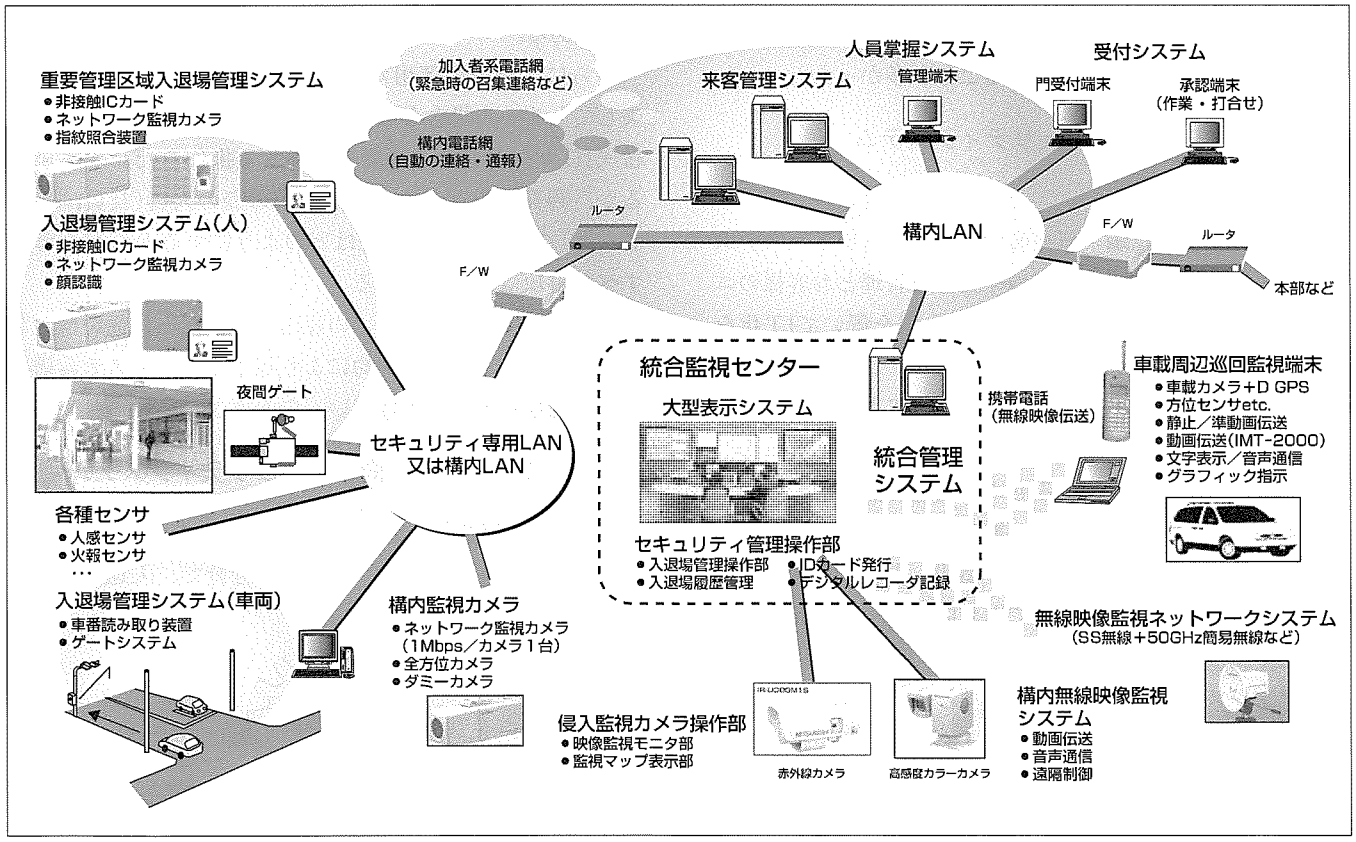
Kazuhiko Serizawa, Akira Hashizume

要　旨

昨今の社会情勢やIT化の推進により，工場・研究所施設内の情報・資産の価値は，それを保有する企業・社会にとり，非常に重要になっている。それらを守る手段として，セキュリティシステムは重要な位置付けとなる。各企業が設備投資を抑制していたにもかかわらず，新築・既設を問わずセキュリティシステムの需要は拡大傾向にある。近年のセキュリティに対する認識の変革，企業内犯罪の防止策の推進などに対応する，工場・研究所向けセキュリティシステムについて述べる。

工場・研究所施設はセキュリティシステムが不可欠となる施設であり，従来から導入されている。しかし，各棟・各部署・各システム(映像監視・入退場管理など)ごとの導入となっており，施設全体での取り組みではなかった。一方で，個人情報保護の機運が高まり，企業の危機管理・セキュリティポリシーの策定など，セキュリティシステムは企業自身が構築しなければならない重要なアイテムとなっている。三菱電機は，総合電機メーカーとして自社工場・研究所へのセキュリティシステムの適用，また，お客様へのセキュリティシステム構築を展開することにより，セキュリティシステムベンダーとして，今後一層注力していく。

本稿では，工場・研究所のセキュリティを統合的に管理する“統合セキュリティシステム”について述べる。このシステムにより施設全体をとりまとめ，それを核として入退場管理・映像監視・車両管理を融合し，“人・車両・施設・情報”を統合管理し今後のシステムに適用していく。



工場・研究所向けの統合セキュリティシステム構成例

工場において，万一発生してしまった災害や事故の状況を収集し対策を講じるには，集めた情報から総合的に，かつ迅速に判断と指示を下す必要がある。当社の提案する工場・研究所向けセキュリティシステムは，“人・車両・施設・情報”等の一元的な管理と顧客のニーズ，運用に応じたシステム拡張に主眼を置いてIT化を図った統合セキュリティシステムである。

*鎌倉製作所　**ビル事業部

1. まえがき

一般に，工場や研究所では，広い敷地への侵入監視，車両の入退場管理，社員だけでなく来客者など臨時立ち入り者を含めた人の入退場管理，危険物や高額計測器などの保管・管理など，オフィスビルにはない特徴的なセキュリティ対策が求められる。ここでは，工場・研究所向けセキュリティシステムとして“人・車両・施設・情報”を統合管理できるシステムについて述べる。

2. 工場・研究所向けセキュリティシステムの現状

工場や研究所において，万一事故や事件が発生すれば，その企業の事業活動が停滞するにとどまらず，経営的・社会的な責任の追及，損害賠償，行政指導による緊急対策，信用の失墜など，打撃の大きさは計り知れない(**図1**)。被害状況を早急に把握し，対策をいち早く講じることが重要である。

従来の工場セキュリティシステムは，自動火災報知や侵入センサ，カメラによる機械警備，警備員による目視，巡回と有事対応が主であり，最近は社員の入退場IDカードシステムを導入するところも増えてきた。しかしながら，これらのシステムは，個々に検討され導入される傾向が強く，運用する部門，管理する部門も異なることが多い。

また，担当者がセキュリティ全体について把握しているケースは少なく，また，個々のセキュリティレベルにも差があり，システム構築に苦慮することが多かった。

3. 統合セキュリティシステム

3.1 システムの概要

当社の提案する工場・研究所向けセキュリティシステムは，人・車両・施設・情報等の一元的な管理とお客様のニーズ，運用に応じたシステム拡張に主眼を置いてIT化を図った統合セキュリティシステムである。このシステムでは，平時の構内監視，有事の際の情報収集だけでなく，意思決定，指揮・支援，関係機関への通報や連携，有事復旧までをシームレスに支援するものを提供可能である。例えば，現地対策本部のみならず，被害を受けていない別の拠点や本社と，映像・音声・センサ情報，人員掌握状況，安否の確認状況などを，連携してより広範囲・高次元での意思決定や支援も可能になる。

各サブシステムの情報を一元管理しネットワーク(Web)を利用したアプリケーションに展開することで，拡張性を備える。例えば，入退場の管理情報などは，出入りチェックだけでなく，勤怠管理に利用し，有事や平時にかかわらずエリア・建物・部屋単位での人員の掌握を自動的に行う，人事異動データを取り込み人員データベースに即座に反映すること，車両や人の通行量や構内滞在時間を算出するなど，保安・警備部門だけでなく，総務・人事部門，物流管理部門，経営責任者が，ほぼリアルタイムに最新のデータを収集し活用することができる。

3.2 システム構築の考え方

実際には，各工場や研究所でのセキュリティ方針，エリアの大きさ，対象となる人や車両の種類や通行量，周辺の状況，既設設備の状況など様々であり，構築すべきセキュリティシステムの運用方法やシステムの機能が異なり，システム構成も異なってくる。また，当然ながら予算的な制約もある。

当社では，統合セキュリティシステムの考え方を示し，顧客の状況やニーズをヒアリングさせていただき，最適なセキュリティシステムを提案している。セキュリティポリシーの考え方，保護すべきものが何か，どのような対策が必要となるか，運用体制はどうするか決めること，そしてこの内容をベースに最終的なシステムの形を決めていくことを提案している(**図2**)。多くの場合は，予算的な制約があり段階的な整備が必要となるが，あるべきセキュリティシステムの姿が示せれば，これらは実現しやすくなる。

人の入退場管理の考え方を**表1**に示す。セキュリティ対象の区分は顧客ごとに異なり，例えば一般来客・業者でも，商談等の打合せで来る人，納品・物流業者，工事作業者など細分化する場合がある。構内へ入場する際の認証方法として，IDカード(ICカード，磁気カード，バーコードなど)を適用しているが，社員証の提示や制服の着用で代替する場合もある。

さらに，通常の運用だけでなく，例えばIDカードを紛失してしまった場合など，だれが責任をもって判断するか，紛失IDカードでの入退場を制限する操作をだれが実施するか，再発行をどうするか，有事の際の人員(社員，来客者など)の掌握や安否確認はどのようにするかなど，考慮すべき事項は多岐にわたる。

このようにセキュリティの運用をポリシーに従い検討し，運用上・システム上の制約により運用手順やシステム構成を最終的なものに仕上げていくのが望ましい。

4. 工場・研究所向けセキュリティシステム

4.1 入退場管理システム

当社では，従来からセキュリティ分野で，入退場管理用

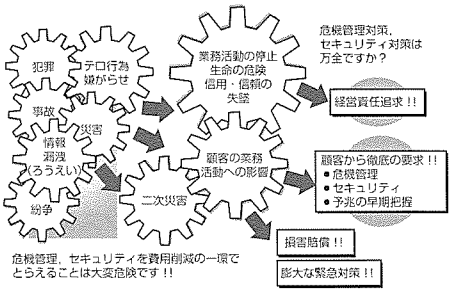


図1．危機管理・セキュリティリスクについて

の“MELSAFETY”，各種監視カメラ（可視カメラ，赤外線カメラ）など多くの製品を提供してきた。当社鎌倉製作所では，実際に統合セキュリティシステムを運用し，同様のシステムを納入した顧客にも安心して運用してもらえるよう日々検証に努めている。

図3は工場での実施例である。門を出入りする人・車両の管理，外周警備，構内の重要エリアへの入退場管理を実施し，統合管理センターで集中管理している。これらの各種機器の構成，配置は，セキュリティポリシーの策定を検討した結果を基に決めたものである。

全体を統合管理する中央装置一台で，各サブシステムと連携し，人と車両の入退場やセンサ情報の提供，個人データなどのデータベースの管理，映像の表示，来客管理，さらには勤怠情報の提供などが可能である。必要に応じて段

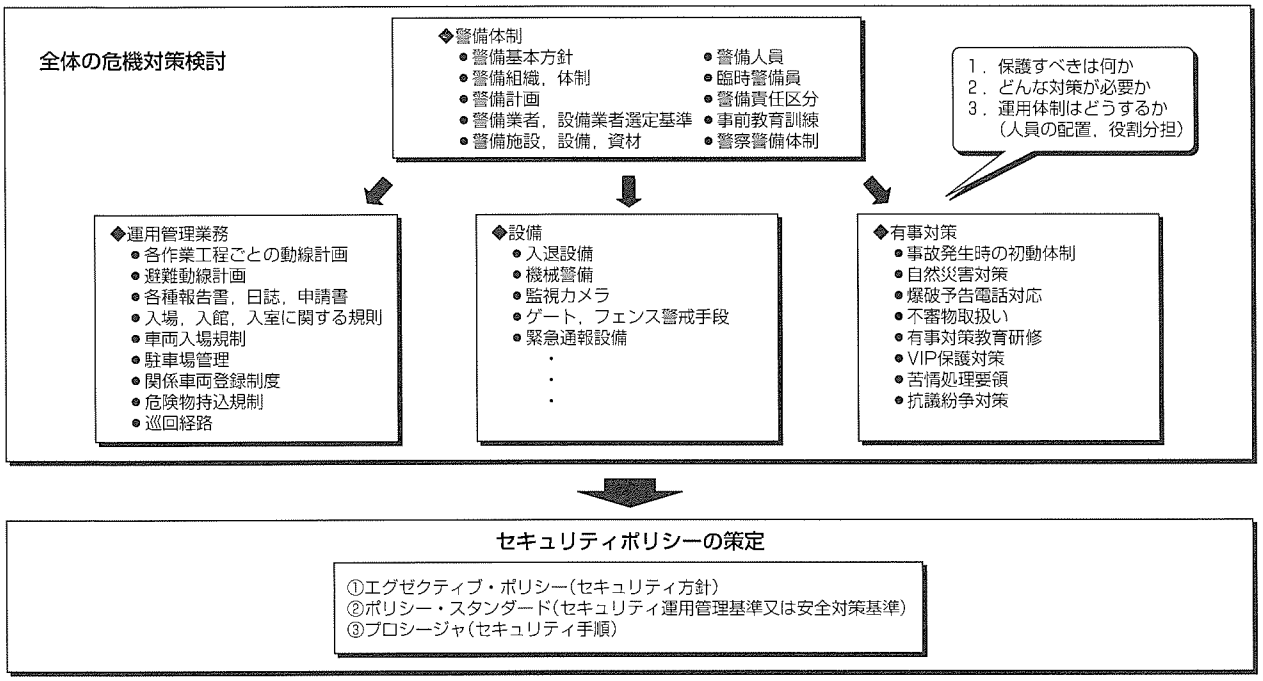


図2．セキュリティポリシー

表1．統合セキュリティにおけるポリシースタンダード例（人の入退場管理の場合）

対象／内訳	社員	構内従事者	出入りの多い業者など	他事業所社員(社員証の事業所間での統一なし)		一般来客・業者など		ゲスト・VIP	
				来客管理あり	来客管理なし	来客管理あり	来客管理なし	来客管理あり	来客管理なし
条件 事前 承認等	なし		なし あらかじめ専用IDカード登録が必要 未登録の場合には一般来客と同じ	予告登録	なし	予告登録	なし	予告登録 併せて会議室，食事などの予約状況も入力	なし
カード／フォルダの種類	IDカード社員用	IDカード構内従事者用	IDカード業者用／業者用フォルダ	臨時IDカード／他事業所用フォルダ（訪問先ごとに分類）	臨時IDカード／他事業所用フォルダ（訪問先ごとに分類）	臨時IDカード／一般来客用フォルダ	臨時IDカード／一般来客用フォルダ	臨時IDカード／ゲスト用フォルダ	臨時IDカード／ゲスト用フォルダ
制限区域入場手続き	IDカードリーダー			①社員証提示 ②受付システムで予告内容の確認 ③臨時IDカード発行（受付内IDカードリーダーで予告データと紐（ひも）付け）	①社員証提示 ②入退場管理台帳に記入 ③臨時IDカード発行（入退場管理台帳に臨時IDカード番号を記入） ④臨時IDカードをIDカードリーダーで読み込ませて入場	①社員証提示 ②面会票記入 ③来客管理による確認 ④臨時IDカード発行（受付内IDカードリーダーで予告データと紐付け）	①社員証提示 ②面会票記入 ③面会者へ電話確認 ④臨時IDカード発行（入退場管理台帳にIDカード番号を記入） ⑤面会者の出迎え ⑥臨時IDカードをIDカードリーダーで読み込ませて入場	①受入者がエスコートにくる（受入者がエスコートに来ない場合には予告登録内容に従って臨機応変の対応を行う） ②受付は該当IDカードを受付内IDカードリーダーで認証	①受入者がエスコートにくる ②受付は該当IDカードを受付内IDカードリーダーで認証
制限区域退場手続き	IDカードリーダー			IDカードリーダー			①面会者のサイン ②面会票と臨時IDカードを受付に返却	受入者のエスコート IDカードを受付に返却	
管理対象	個人ごとの入退場			個人ごとの入退場	入退場数のみ電子管理。 詳細は台帳	個人ごとに入退場	入退場数のみ電子管理。 詳細は台帳	基本的に受入者がエスコート	常に受入者がエスコート
重点管理エリア入退場	許可者のみ IDカード，指紋等別途登録必要 IDカードは該当のIDコントローラへの登録のみでよい。			事前に書類等で許可の取得が必要 常に担当者がエスコートする。				常に担当者がエスコートする。 最寄の電話で適宜連絡を取り合う。	

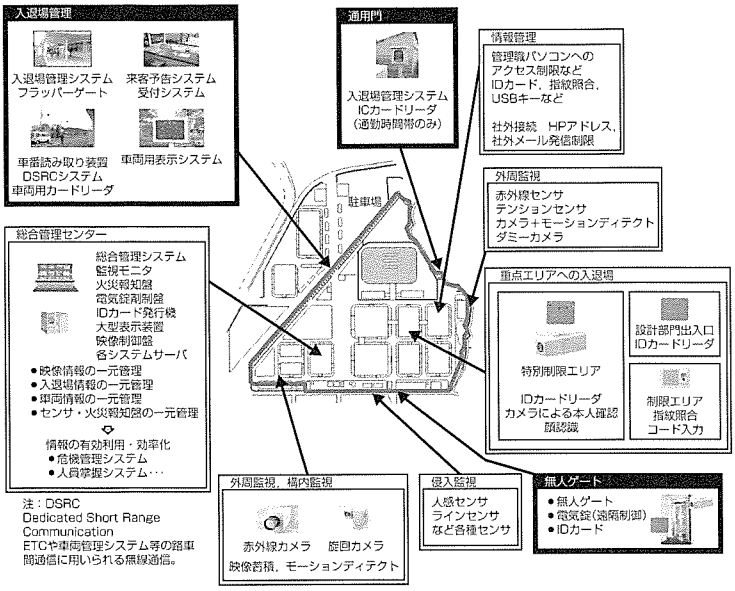


図3．工場向けセキュリティシステム実施例

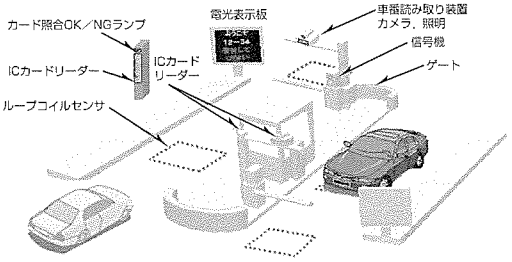


図4．車両管理イメージ

階的に整備・拡張が可能であり，さらに，工場内での物品持ち出し管理機能など別のサブシステムを追加することもできる。

4.2　工場・研究所に入退場する車両の管理

車両も，人と同様に，幾つかの区分に分けてどのような運用をするかを考慮する必要がある。すなわち，社員車両，構内業者車両，得意先業者車両，社有車などあらかじめ構内への入場を事前申請登録が可能なものと，来客の車両，工事業者，不定期の納品業者の車両など臨時で入構する車両に分けて，それぞれの運用を考える必要がある。

当社は，約20年前から車両の管理システムを手掛けており，車両番号読み取りシステムや特殊な車両感知器では先駆的存在である。また，近年では，ETC(Electronic Toll Collection)システムや，ETC車載器を利用した駐車場管理システムなどの納入実績もあり，工場・研究所へ入退場する車両を管理するシステムを提案する技術的ベースを備えている。

図4に示す車両管理イメージは，車番読み取り装置により読み取った車両番号を電光表示板に表示する方式である。車両番号の表示は，お客様への誘導のサービスの意味合いもあるが，管理されていることを構内入場者に意識させることによる盗難・破壊などの不正行為を抑止する効果が大きい。車番読み取り装置により，通過した車両の車両番号の通行履歴が管理でき，登録又は未登録車両の通過をリアルタイムに検知し警備員に知らせたり，車両番号をベースに後検索したり，構内へ長期滞在している車両を検出したりすることが可能である。

ゲートやICカードリーダーを付けるかどうかは，入退場する車両の台数，周囲の道路の状況，駐車スペースや位置，工場・研究所に対するイメージをどうするかなどで異なる。当社の車番読み取り装置は，走行中の車両であっても車両番号を全けた読み取ることが可能であり，入場車両の滞留による周辺道路の渋滞を解消しつつ，入場車両の管理をするのに適している。車番読み取り装置と電光表示板，ICカードによる入退場管理システム，来客管理システムなどと連携することで，車両だけでなく運転者や同乗者も含め車両と人を結び付けて統合管理することも可能である。

5. むすび

広大な敷地の工場の場合には，地図情報との連動や実際に事故や災害が発生した地点の映像も，次にどのような対策手段を講じるかを危機管理責任者が判断する上で有効である。工場・研究所内の車両や人の位置情報，センサなどの施設情報と地図情報との組合せ，カメラやセンサを搭載した自走車両での監視などもニーズに合わせて提供可能である。

今まで述べてきた工場・研究所の統合セキュリティシステムの例はモデルケースであり，前述のように，実際のシステムは，顧客のニーズや運用方法，体制などに合わせたものにしていく必要がある。また，広大な敷地の中でセキュリティレベルを一定にし高めていくには，当社の提案する物理的なセキュリティシステムだけでは困難であり，顧客のシステム運用者，社員の一人一人が，セキュリティ方針に従った意識を持ち，実際に行動することも大切と考えている。

参考文献

(1)　三菱統合セキュリティシステム：日経トレンディ，No.221　臨時増刊号　日経ホーム出版社（2004）
(2)　三菱統合セキュリティシステム：エネルギーと建築設備，No.12　建築設備電力研究会（2004-3）

公共分野における監視システム

半田一郎*
坪井尚登*
荒巻　淳*

Surveillance System for Public-field

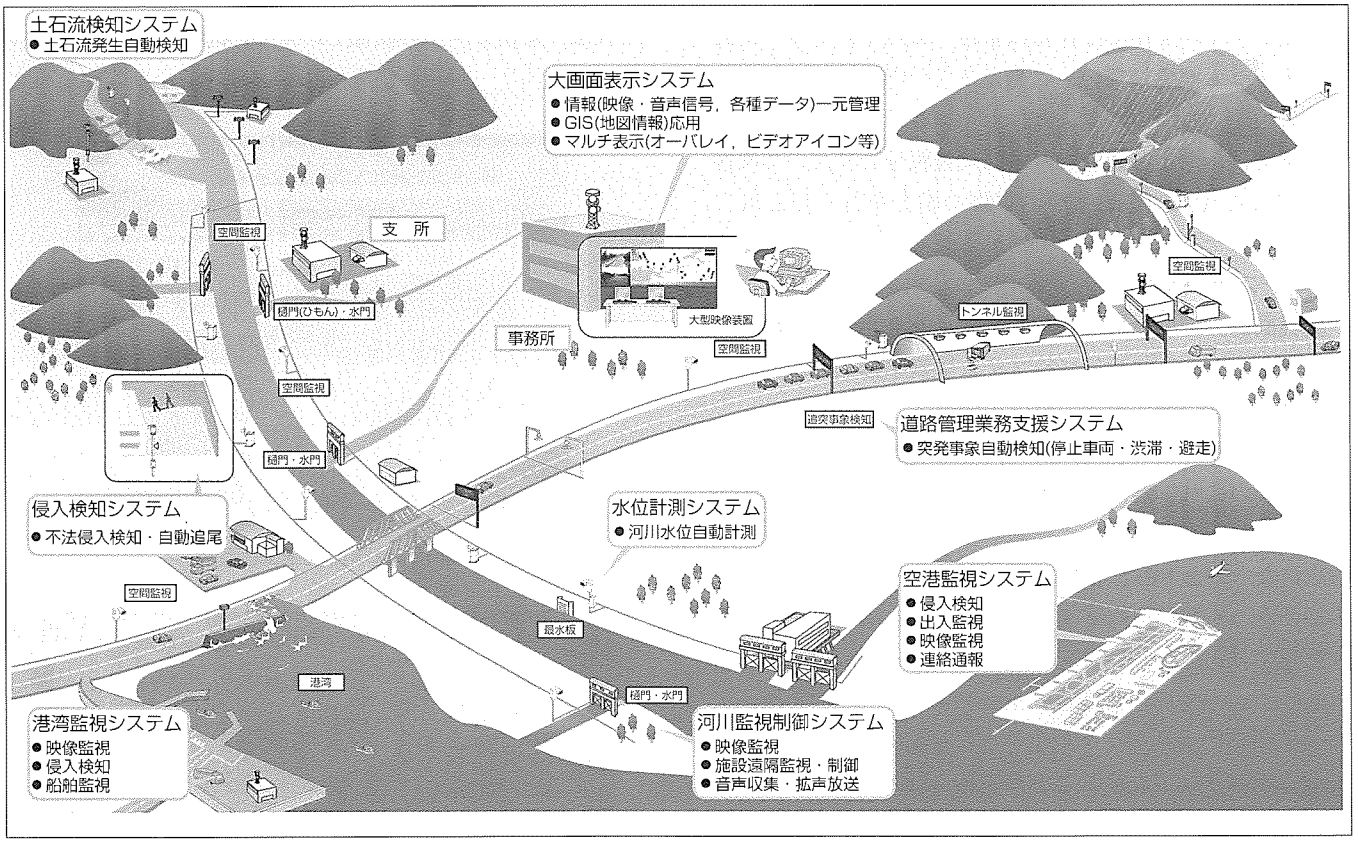
Ichiro Handa, Hisato Tsuboi, Kiyoshi Aramaki

要　旨

我が国において，個人の生命・財産を脅威から守るいわゆるセキュリティ意識は，ここ数年高まりを見せている。この背景には最近の凶悪犯罪の増加による防犯意識の向上が挙げられるが，公共分野においてセキュリティを考える場合，防犯と同等以上に防災も考える必要がある。つまり，社会の中では個人に対する脅威は災害・犯罪共に同じ重さを持っている。公共分野においてセキュリティを考慮すべき対象としては，不特定多数の人が利用するところ，外国人が出入国するところ，災害・事故・事件などの事案発生時に社会的影響が大きいところなどが挙げられる。具体的には，河川・道路・空港・港湾・公共施設などである。

これら公共分野でのセキュリティを構築する場合は映像による監視システム主体になるが，最近の映像伝送技術の進展とともに映像監視ポイントの拡大による監視業務の高度化，映像活用の高度化により，監視業務の効率化，さらには制御分野への映像利用も進んでいる。また，映像利用範囲の拡大に伴う監視業務負荷の増大に対応するため，映像表示技術の発展，映像検索技術の高度化への期待も高まっている。

また，空港・港湾などに代表される公共大規模施設における人為的犯罪に対応する手段，すなわち防犯システムの構築においては人的対応と強調したシステム構築が必要で，システムに対する要求，システムの運用，システム構築の各フェーズにおいて機械と人の機能バランスを考慮する必要がある。



公共分野における監視システムの主な機能

監視対象（施設）ごとに機能は異なる。道路・河川等の広域監視においては映像監視が主体になる。空港・港湾等の拠点監視は映像監視以外の機能も必要となる。

*社会eソリューション事業所

1. まえがき

近年の世情不安を反映して，我が国における従来からの安全神話は崩れてきている。最近は特に犯罪の凶悪化・組織化・広域化・国際化が目立ってきており，これらは今後ますます増大するものと思われる。また，公共分野において人の生命・財産を脅かす脅威としては，これら犯罪に代表される人為的事件は当然であるが，自然災害及び事故もそれ以上に重要である。事故を含む災害を完全に回避することは現状では困難であるが，災害をある程度予想すること，災害が起きてからの復旧を効率的に行うこと，二次災害を防止することなどは可能である。また，人為的事件を回避する手段，つまり防犯システムは対象により個々に異なるが，そのシステム構築手法にはかなり共通点がある。これらのシステムには映像が有効に利用されている。

本稿では，社会インフラ分野における主に映像を主体にした防災監視のシステム事例と今後の技術動向を述べるとともに，防犯システムにおけるシステム構築手法について述べる。

2. 防災監視分野におけるシステム動向

河川・道路などの社会インフラの防災監視分野においては，センサ及びデータ収集システムの整備やパトロールによる目視確認により各種の施設・設備の管理を行ってきたが，光ファイバを中心とする広帯域・広域ネットワークと監視カメラの整備に伴い，このような分野において映像が有効に活用されつつある。

以下では，河川・道路などの防災監視分野において映像を活用した代表的なシステム事例の紹介を行うとともに，今後のシステム動向について述べる。

2.1 システム事例

監視制御分野における映像の活用，センサとしての映像利用，の2ケースに分けてシステム事例を紹介する。

(1) 監視制御分野における映像の活用

河川・道路などの社会インフラの特徴の一つとして挙げられるものに“広域性”がある。すなわち，被管理施設が散在しており，かつ，センター側は管轄地域を基にした階層構成になっており複数拠点から構成される。このように，広域でかつ複数の拠点で映像を利活用するには，映像を各種符号化方式(MPEG2(Moving Picture Experts Group Phase2)／MPEG4／JPEG(Joint Photographic Experts Group)等)によりデジタル化するとともに，IP(Internet Protocol)パケット化することが求められる。これにより，データと映像の融合やIPマルチキャスト通信による映像の広域同報配信が可能となる。

監視制御システムは，従来，データ中心に構築されてきたが，監視カメラの映像を補完的に活用し，管理業務の高度化が図られる。

図1は，河川沿いに配置されている各種河川管理施設(樋門，排水機場等)の設備をWebブラウザ上で遠隔監視制御する事例を示している。Webブラウザ上では，被監視制御設備の状態を示すデータに加えて，監視カメラのデジタル映像を同時に表示し，データのみでは把握できない現場の状況を映像により確認することができる。従来，河川管理施設は，管理レベルとしては遠隔監視するのが主体であったが，映像を活用することにより，遠隔制御を行うことも可能となりつつある。

図2は，道路沿いに配置されている各種道路管理設備(気象テレメータ，情報表示板等)の状態をセンター側の大型表示装置上で統合的に監視する事例を示している。大型表示装置上では，汎用的な地図データを利用して管轄地域・区間全体を広域表示する。この地図上に各種道路管理設備の状態を示すデータに加えて監視カメラの映像を重畳表示することにより，マンマシンインタフェースの向上を図っている。トンネルなど防災上重要な道路区間には多数の監視カメラが設置されるケースがあり，大型表示装置の特長を生かしてこれらの監視映像を地図上で多面表示することにより，各種道路管理設備を常時集中監視する業務が高度化される。

(2) センサとしての映像利用

次に，映像をセンサとして利活用する事例を紹介する。これは，監視カメラの映像そのものの時間的変化をリアルタイムに抽出・解析し，発生している事象を判定するもの

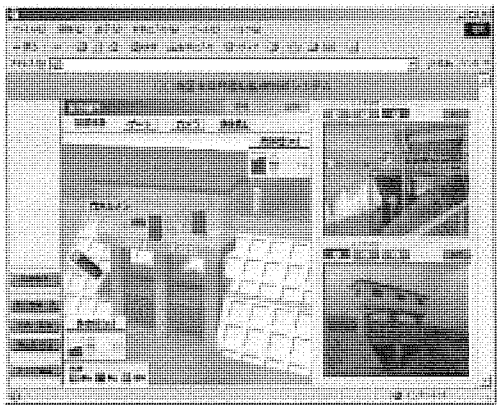


図1．遠隔監視制御画面例

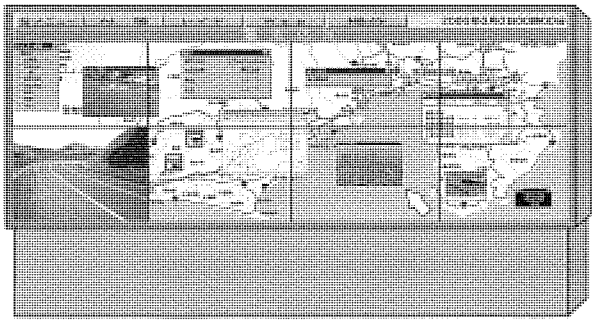


図2．大型表示システム画面例

である。センサとしての映像利用は，河川・道路管理者の監視業務の高度化・効率化につながるものに位置付けられる。

図3は，河川上流部における土石流発生の検知を行うシステムイメージである。土石流の検知には，通常，ワイヤセンサを適用するケースが多い。これは，土石流の発生により生じる物理的な変化・変位を直接検知するものである。一方，土石流発生危険箇所に監視カメラを設置し，監視映像に生じる大きな変化を画像処理技術を利用して数量化し，事象判定に利用することが考えられる。この方式は，検知精度の課題はあるものの，従来の方式と異なり，非接触式で土石流を検知するため，連続的な土石流検知を行えるのがメリットである。

監視映像の大きな変化をとらえる画像処理技術を使う他の事例としては，不法投棄者の検知やダム下流などの危険地域への侵入者検知を行う事例が挙げられる。また，河川水位計測への応用も検討が進められている。

一方，図4は，道路沿いに設置した監視カメラ映像を利用して交通流の事象検知を行うシステムイメージである。監視カメラの映像から背景画像を生成し，走行している車両を抽出・認識する。その車両を追跡処理することにより，低速車，停止車，渋滞，避走といった事象判定を行う。

2.2 システム動向

上記に紹介したシステム事例は，複数拠点での映像利用が可能なものの，映像を監視できる場所はセンター側に限定されている。また，映像の利用形態としては，現状の最新状況を確認するというライブ映像監視が中心である。そのような意味において，映像の有効活用は緒についたばかりと言える。以下では，映像の利活用・高度利用を切り口とした今後のシステム動向について述べる。

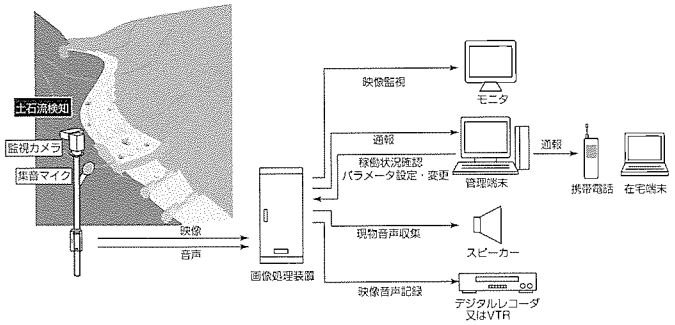


図3．土石流検知システムイメージ

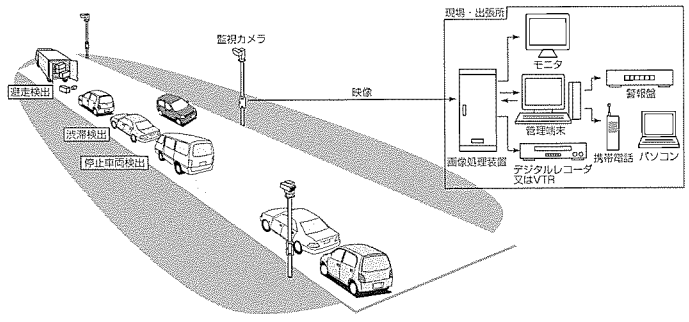


図4．交通流事象検知システムイメージ

(1) 映像利用領域の拡大

これまでは，イントラの広帯域ネットワークを前提とした映像監視であり，いわば映像の収集が主体であった。今後は，収集した映像を様々なネットワーク環境や端末環境で利用することが求められるであろう。すなわち，狭帯域ネットワーク，組織外ネットワーク，インターネットなど様々なネットワーク環境における映像利用が進み，映像の利用領域が拡大していくと想定される。今後，必要となる基盤技術は，映像符号のデジタル変換(例：MEPG2からMPEG4へのデジタル変換等)，セキュリティ技術を実装した映像配信技術(例；認証・暗号化技術等)になると思われる。

(2) 映像の高度利用

これまでは，ライブ映像を加工せず単純に提供するのが主体となっている。このため，情報の受け手にとって必ずしも最適に加工・編集された形で提供されていない。今後は，見えにくい映像を見やすくするために編集・加工する，状況を効果的に伝達するために他の情報を組み合わせる，監視空間全体を示す，など利用者に対する情報伝達の質的向上を意識した映像提供方法(ビジュアライゼーション)が求められるであろう。具体的には，昼間の監視映像を利用して夜間の監視映像を見やすくする，雪や雨等の障害物を除去して監視対象を見やすくする，監視映像にCG(Computer Graphics)等を使って補完的な情報を付加して分かりやすくする，旋回カメラや移動カメラの時系列映像から高解像度のパノラマ画像を生成する，などの映像提供が今後求められると考える。

さらに，監視カメラ設置数の増大に伴い，映像監視業務の負荷が高まり，決定的なシーンを見逃してしまうケースが出てくる懸念がある。また，データ蓄積の利活用と同様に，長期間にわたって定点観測した蓄積映像を分析・加工して意味のある情報を抽出する利用形態も今後出てくると思われる。このように，今後は，収集した映像を蓄積し有効利用していく方向になると思われる。蓄積した映像は膨大な量になるため，この中から必要なシーンを抽出するには，時刻指定や早送り・逆再生といった基本的な機能に加えて，より高度な映像検索機能が求められる。監視映像の特徴量を演算・抽出しその特徴量を活用した映像検索技術や，蓄積した映像を短時間でブラウジングする等の技術が必要になると考える。

3. 防犯システムにおけるシステム構築手法

3.1 防犯システム構築の考え方

ここでは，空港等に代表される大規模かつ広域な施設向けの防犯システム構築の考え方について説明する。

防犯システムは，“対象施設の安全をいかに守るか”を目的としたシステムである。守るべき対象は，人命であり，施設であり，運用施設である。すなわち，利用者及び施設の“安全”を確保し，かつ施設が“安定”して運用され，利用者が“安心”を与えられるようなシステム構築を行う必要がある。

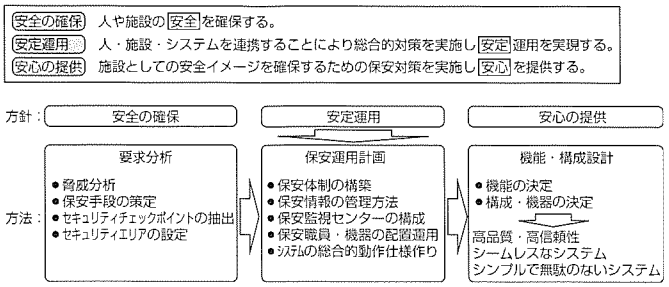


図5．防犯システム構築の考え方

図5に，防犯システム構築の考え方を示す。

3.2 防犯システム設計の手順とポイント

防犯システム構築の考え方を原則として最適な施設保安を計画し，必要最小限の要員で最大限の保安効果を発揮する防犯システムを設計する必要がある。

この際の最大の留意点は，機械と人間の長所／短所を補完しあうシステム，すなわち“機械警備と人的警備のバランスのとれたシステム”とすることである。

機械警備の長所は常時一定の性能で監視の継続が可能な点であり，一方，人的警備の利点は事案発生時の状況に応じた臨機応変な対応が可能な点である。

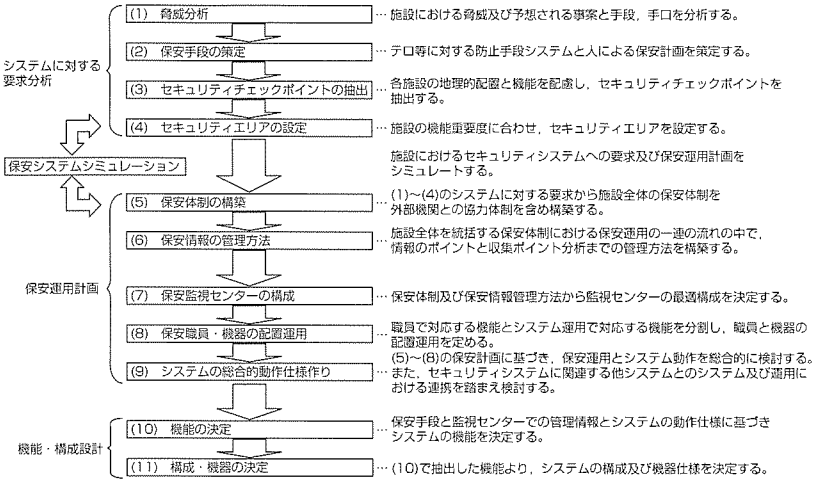


図6．防犯システム設計の手順例

図6に，防犯システム設計の手順例を示す。

図のシステム設計手順例に示したもののうちセキュリティエリアの設定も重要である。セキュリティエリアの設定は対象施設の重要度を考慮して守るべきものを確実に守ることを目的としており，その一例を図7に示す。

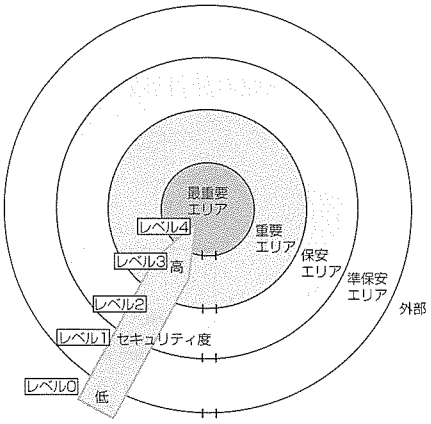


図7．セキュリティエリア設定の考え方

4. むすび

社会が成熟するにつれて社会生活の効率化を求めて公共分野における社会インフラも高度化されたものになりつつあるが，その反面，それらの社会インフラの機能が停止した場合の社会的影響は計り知れないものになってきている。社会インフラ機能の高度化とそれらに対するセキュリティ高度化は相反する面がある。この利便性と安全性双方の要求を満たすものとしての映像利活用技術は，これから本格化しようとしている。

また，高度情報化社会に突入した現在，物理的セキュリティ手段だけでなく情報セキュリティ手段との連携を考慮しなければセキュリティ対策は片手落ちになる。我々は，長年の公共監視分野での実績を踏まえ，今後も各種技術開発を進めながら運用を踏まえた先進的なシステムの企画・提案・構築に取り組み，公共分野でのセキュリティ向上に貢献していく。

監視用デジタルレコーダと セルフセキュリティ応用

熊野　眞*

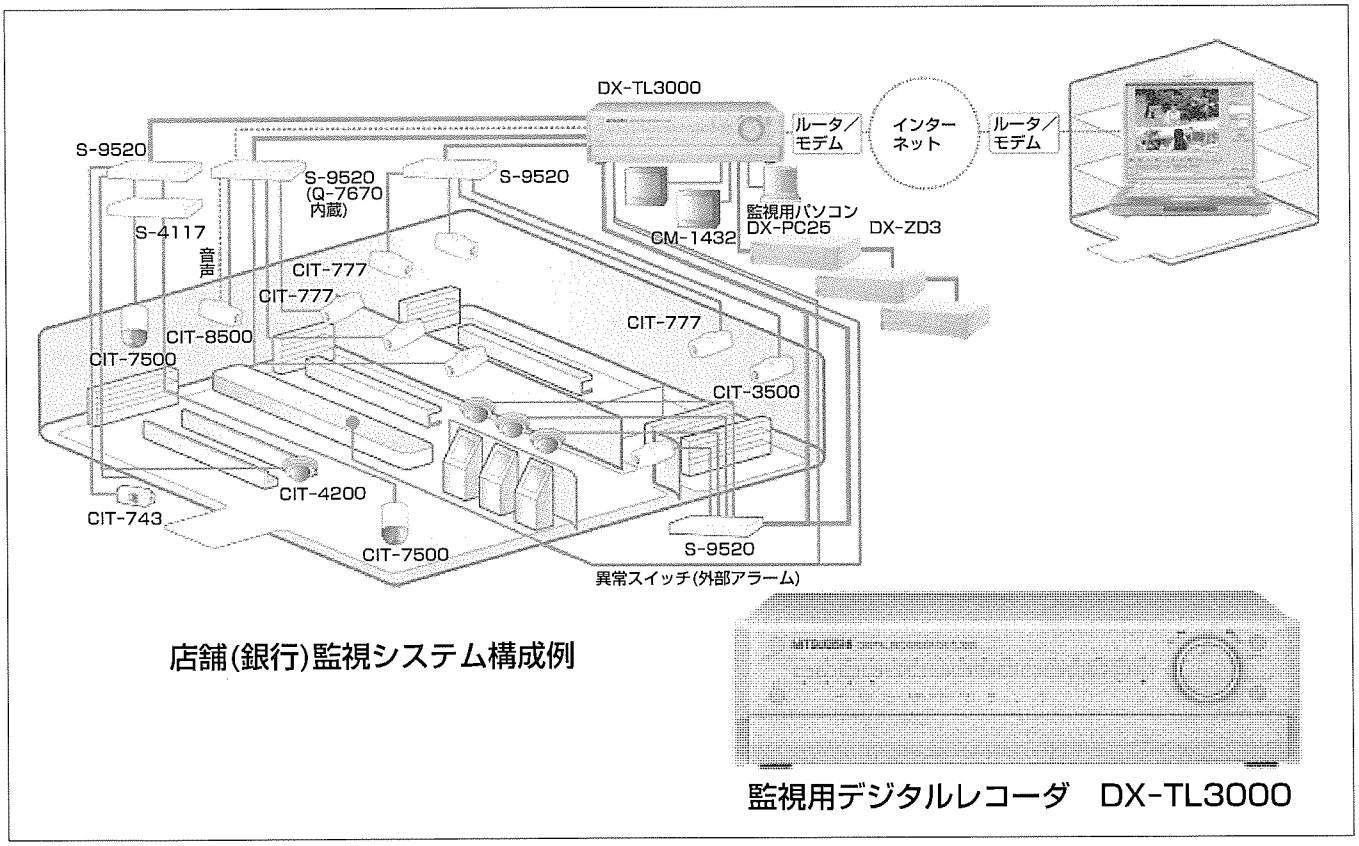
Digital Recorder for Surveillance and Self-Security Application

Makoto Kumano

要　旨

昨今，安全と言われてきた我が国においても，犯罪の増加と多様化については様々なメディアにおいて報じられている状況である。営業時間の延長などに伴う店舗防犯に対する意識が急速に高まってきており，日常的に利用する店舗において防犯用監視システムが稼働していることを目にすることはさほど珍しい光景ではなくなってきている。こうした社会背景から，一般家庭においても防犯に対する意識は徐々に浸透しつつある状況である。三菱電機では，主としてコンビニエンスストアを始めとする小規模店舗での使用を想定した監視用デジタルレコーダ“DX-TL10”を2001年の年末にリリースを行い，以降，様々な用途や監視システムのニーズに対応した製品開発を行ってきた。例えば，銀行やビルを対象とした中・大規模店舗監視システム対応機や，駐車場やエレベーターといった特定使用に特化した製品の充実と，増設用ディスク装置やシステム専用カメラ，そしてパソコンと組み合わせて使用を行うためのアプリケーションソフトウェア製品等の周辺機器の充実を図ってきた。

今回，金融を始めとする大規模・高機能を要求する中・大店舗向けシステムの要求にこたえるために，マルチプレクサ性能を始めとした基本性能の向上と，ネットワーク機能を始めとした高操作性を実現するために新規開発した技術内容について，上位機となる“DX-TL3000”を例に述べるとともに，より広範囲の用途に対応した展開製品の開発状況と，我々の普段の生活により一層身近になりつつある“セルフセキュリティ”についての取り組み状況について述べる。



監視用デジタルレコーダDX-TL3000と店舗監視システム構成例

DX-TL3000は，最大16チャネルのカメラ映像を内蔵のハードディスクドライブ（HDD）に長期間連続記録を行うことが可能な監視用デジタルレコーダである。記録速度や映像保存期間に応じて外付けのディスク装置“DX-ZD3”を適宜増設することで店舗規模に応じた監視システムの構築が可能となる。また，2系統のモニタ出力やネットワークを介した遠隔監視機能とカメラPTZ（パン／チルト／ズーム）制御機能を内蔵したことにより，より多用途・多目的監視システムを構築する際の中核装置としての使用が可能である。

*京都製作所

1. まえがき

監視用映像記録装置として定番になりつつあるデジタルタイムラプスレコーダは，複数カメラ入力機能を持つ長時間映像記録装置である。2001年の年末に発売されたDX-TL10は，コンビニエンスストアに代表される小規模店舗の監視用途として仕様の絞り込みを行い，かつ展開機開発のための設計的拡張性を考慮して製品化した業界スタンダード機である。その後，図1に示すとおり，監視規模や他の様々なアプリケーションに応じた製品化を行ってきた。DX-TL3000は，2003年の年末に発売された中・大規模店舗用モデルであり，本稿では多機能化のために新たに開発した新技術・新仕様と，我々の普段の生活により一層身近になりつつある“セルフセキュリティ”についての取り組み状況について述べる。

2. TL3000の新技術

2.1 開発コンセプト

大規模店舗での使用を想定して，新たに開発が必要となるレコーダ機能について検討を行った。

(1) 画質と記録時間

カメラ用途に応じた画質選択と記録間隔の設定機能と，カメラ入力の増加(9→16チャネル)に伴った記録容量の増加と記録速度の高速化を図る。

(2) 拡張性

容量増設用外付け機器への対応と，多機能化に伴い増大する機器設定情報や映像データの取扱いを容易に行うための取り外し可能な大容量メモリカード対応の実現。さらにネットワークを利用した遠隔監視機能と遠隔設定機能の実現を図る。

(3) 操作性

レコーダに接続されるカメラはシステムごとにその数や種類が異なる。このため，その都度実行しなければならない機器設定の煩雑さを解消するためのオートセットアップ機能やPTZ制御可能なカメラをレコーダ側から制御するためのカメラ制御機能を始め，アラーム記録機能の強化やパスワードロック機能の充実を図る。また，監視カメラ数の増大に伴いモニタ出力はA／B 2系統に増設する。

(4) 世界展開

ワイドレンジ電源の対応と各国の言語に対応した表示メニュー構築を容易に行える設計構成を図る。

これら各要素を見直し，設計コアの改良を実施した。表1にDX-TL3000の仕様を示す。

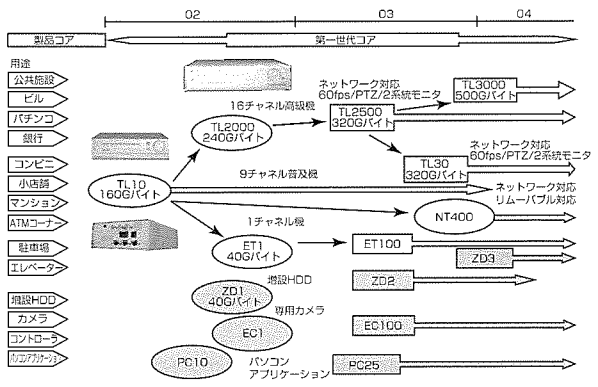


図1．業務用デジタルレコーダのラインアップと技術の流れ

2.2 TL3000導入技術

上記コンセプトに基づき，TL10を設計のベースとして次の各観点から検討を行い，改良を加えた。

2.2.1 画質と記録時間

画質設定については，TL10と同様に，5段階の圧縮率を選択できるようにした。各圧縮率でのWavelet圧縮パラメータについては，特にアラーム動作での画質向上を図るため初期値の見直しを実施し，記録スタート時の画像安定性を確保した。記録速度については，入力カメラチャネル

表1．DX-TL3000の主な仕様

電　源		AC100V±10%　50／60Hz
定格電流		0.65A(約60W)
外形寸法		約425×116×375(mm)
質　量		約8.2kg
映　像	信号方式	NTSC
	記録方式	Wavelet圧縮デジタル記録
	映像入力	16チャネル　BNC：1.0V(p-p)75Ω
	モニタ出力	BNC コンポジット 1V(p-p)75Ω 背面A／B 2系統 RCA コンポジット 1V(p-p)75Ω 前面 1系統 全系統同時出力可
	スルー出力	16チャネル　BNC：1.0V(p-p)75Ω
	水平解像度	スーパー・ファイン・ハイ：450本以上，ノーマル・ベーシック：400本以上
音　声	記録方式	1チャネル 8ビット 12.8kHzサンプリングPCM
	入力	Line IN：RCA 308mV(rms) 50kΩ Mic IN：Φ3.5ジャック 0.346mV (rms)　600Ω
	出力	RCA 308mV(rms)　1kΩ　背面／前面 各1系統
記録媒体		主記憶媒体：500Gバイト HDD内蔵(250Gバイト×2) 記録容量増設：DX-ZD3増設で最大2,000Gバイト(3台増設時) 補助記録媒体：メモリカード，CD-R／RW，DDS
端　子	RS-232C	D-SUB9ピン
	SCSI	ハーフピッチ50ピン
	接点端子	ワンタッチターミナル
	LAN端子	RJ-45 10Base-T
	リモコン端子	専用ワイヤードリモコン用端子
	RS-422／485	ワンタッチターミナル
記録モード設定		記録間隔：60fpsから12段階(カメラごと設定可) 記録画質：圧縮率5段階(カメラごと設定可) 音声記録：有／無設定(アラーム記録時選択可)
画面表示設定		単／4分割／9分割／16分割画面 同シーケンシャルアラーム
ネットワーク機能		Webサーバ機能，専用プロトコル通信機能
モーションディテクタ		検知範囲／サイズ／感度設定(カメラごと設定可)
制御カメラ		CIT-7300／CIT-7500
検索機能		タイムデートサーチ，記録インデックスサーチ，アラームインデックスサーチ，スキップサーチ，アラームリストサーチ，開始・終了点サーチ
タイマプログラム		独立8プログラム×3セット 設定内容：運用カメラパターン，記録間隔，スキップ，バックアップ
バックアップ機能		外部バックアップ機器への同時バックアップ，任意位置コピー

PCM ：Pulse Code Modulation
DDS ：Digital Data Storage

数の増加に伴い従来の30fpsから60fpsに倍増させた。これには，従来の30fps記録エンジンを2系統搭載し，各々を同時動作させることで実現している。記録容量の大容量化については，HDDのアドレッシング方式を従来のLBA(Logical Block Addressing)24方式からATA(Advanced Technology Attachment)-6で新規採用されたLBA48方式に拡張することで，従来の130Gバイト／ドライブ制限を取り除き，製品仕様として2Tバイト／ドライブ対応を実現した。

2.2.2 拡張性

外部記録装置とのインタフェースは，実績のあるSCSI(Small Computer System Interface)インタフェースを継承した。接続可能な機器としては，500GバイトのDX-ZD3を並行開発するとともに，バックアップ・コピーデバイスとして低ランニングコストが実現できるCD-R／RWデバイスとの接続が行えるようにした。さらに，パソコンアプリケーションから直接画像確認ができるように，ファイルフォーマットについてはISO9660対応機能を新規に開発搭載した。LAN機能の追加については，実際の用途が多岐にわたるため，最も一般的なWebブラウザでの使用も可能となるように考慮し，①HTTP(HyperText Transfer Protocol)サーバ機能及び②専用プロトコル機能双方の実装を行った。前者では，汎用的なWebブラウザを用いてカメラライブ映像及び再生画像の閲覧と映像検索が利用できるようにしており，通常の遠隔監視用途で要求される機能について対応を行った。後者の専用プロトコルは，より高度な機能を実現するために新たに開発した機能であり，Webでの機能に付加して次の機能を実現した。

- 機器遠隔設定機能
- 画像ダウンロード機能
- PTZカメラ制御機能
- アラーム発報受信機能
- ファームウェアアップデート機能
- システムログの遠隔ダウンロード機能

いずれの機能についても，その操作に関してはセキュリティ機能が不可欠となる。このため，使用機能に応じて階層的にパスワードを設けて，第三者による不正アクセスを防止している。画像通信については，この装置が取り扱う圧縮プロセスがWaveletであるため，パソコンによる復画には専用のデコード処理が必要となる。このため，デコードのためのソフトウェアライブラリをパソコン側にインストール又はダウンロードすることで対応した。**図2**に，ネットワークを介した映像データに関する動作を示す。

2.2.3 操作性

(1) オートセットアップ機能

監視システムは用途の拡大に伴い様々なシステム構成が採られており，実際の設置作業には膨大な設定作業が発生する。単に設定時間が費やされるばかりでなく，誤設定による動作不良などの可能性も大きくなってきている。DX-TL10では機器設定内容をメモリカードに記憶させ本体側にロードすることで利便性を確保してきたが，今回新たにオートセットアップ機能を搭載することで，初期設定作業を大幅に短縮することが可能となった。このオートセットアップ機能は，最初の電源投入時にのみ起動し、カメラ接続の状態を自動的に検知してユーザーが入力する運用周期から自動的に初期設定を実行するものである。この後，監視用途に応じて必要な機器パラメータを適宜修正することで設定終了となり、特に即日運用開始の場合には有効となっている。

(2) カメラコントロール機能

監視環境の多様化により，監視カメラとして，固定カメラと上下左右方向制御やズーム／フォーカスの調整機能を持った複合一体型カメラの使用も一般的になりつつある。このようなカメラ制御をPTZ制御と呼んでいるが，このカメラ操作を監視レコーダから直接制御する機能を新たに実装した。こうした複合一体型カメラは用途別に様々なものが各社から発売されており，また，その種類も大変多いため制御プロトコルは多様化を極め，個別に対応するのはソフトウェア開発に大変な負荷がかかる。このため，この装置への実装に際して必要とされるPTZ制御のコマンドを制御番号を付加して体系化するとともに，それぞれの実行動作がカメラごとにほぼ同等の操作性になるように調整したデータをカメラ種別ごとにテーブルデータとして実装する方式を採った(**図3**)。カメラ種別とPTZコマンド内容を逐次コマンドインタプリタで解釈しながら制御プロトコルをRS-422／485から出力して操作者所望の動作を実現することが可能となった。

(3) モニタ出力

カメラ入力数の増加により，監視映像の表示出力方法も多様化を要求されてきた。従来は9画面マルチ画と単画をその都度切り換えて使用する方法と，カメラスルー出力を別のスイッチャ装置を経由してモニタに出力するといった使用方法があったが，今回の装置では，独立した2系統の背面モニタ出力を備えることでマルチ画面と特定のカメラ映像の同時監視・マルチ画監視を行える機能を搭載した。

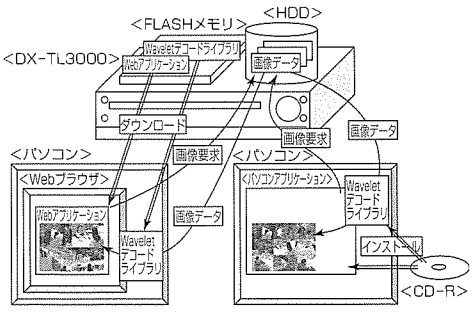


図2．通信機能

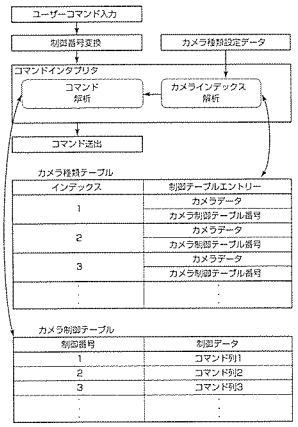


図3．PTZ制御方式

これは，TL10で開発したスイッチャ機能と表示用VRAM(Video RAM)を2系統装備することで実現させている。前に述べたネットワーク経由での映像配信と前面モニタ出力とを組み合わせることで，様々な監視システム構築が可能となっている。図4にモニタ出力例を示す。

2.2.4 世界展開

世界各国での機種展開に対応するために，製品設計に際して様々な考慮を行っている。入力電源電圧に対しては，ワイド化設計を実施し90～240V動作に対応すると同時に，各国安全規格を遵守した新規設計を行った。映像信号フォーマットについても，NTSC(National Television Standards Committee)とPAL(Phase Alternation by line)両規格に対応した設計を実施して世界展開を容易に行えるよう配慮している。また，本体設定の際に表示されるメニュー等の表示についても各国の言語に対応を行う必要があるが，この実現のために，前項のPTZ対応技術を応用することで様々な言語での表示を実現している。言語設定と表示すべきメニュー番号から表示すべき言語対応の文字列コードをVRAMに転送することで各国語表示を可能にしている。フォントについては，フリーフォント構造を継承しており，共に言語データとして追加することでカスタマイズができる構造としている。

3. ホーム用途への展開

上述してきたように様々な用途の業務用監視レコーダの機種展開を図ってきているが，近年の報道等に見られるように，犯罪は必ずしも店舗だけではなく，商店街を始め我々一般家庭にも及ぼうとしており，いわゆるホームセキュリティとしての関心が年々高まりつつある。こうした状況から，具体的な例としてセルフセキュリティとして提案活動を行っているところであり，昨年のCEATEC JAPAN 2003及びセキュリティショー2004でも参考展示を行った。例えば一般家庭の場合では，図5に示す位置に監視ポイントを設定することで，基本的な侵入経路の監視が可能となる。さらに，例えば図6に示すとおり，サーバ技術を始めとするインターネット通信技術と携帯電話との画像転送技術を応用することで，外出先においても自宅の異常や状況の確認が可能となる。これは，不審者侵入を本体レコーダで検出し，インターネット上のサーバを経由して指定の携帯電話へ通知するシステム提案を行ったものである。監視用デジタルレコーダは，このように様々な通信インフラと融合したシステムへ応用することでより身近なセキュリティシステムを提案することが可能であり，その応用について現在提案・検討を行っている。

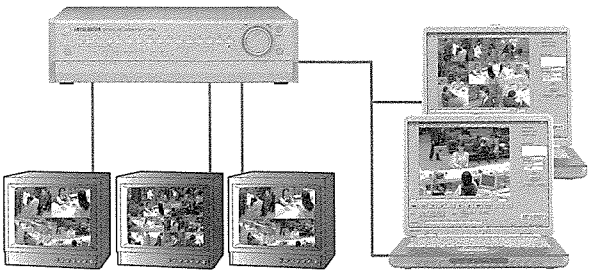


図4．モニタ出力例

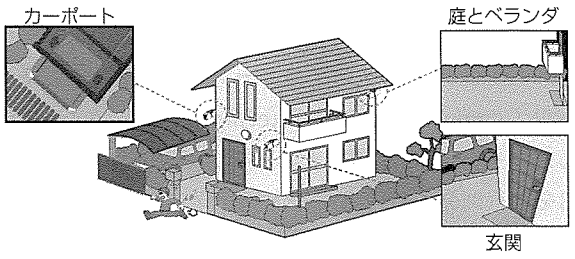


図5．セルフセキュリティ設置例

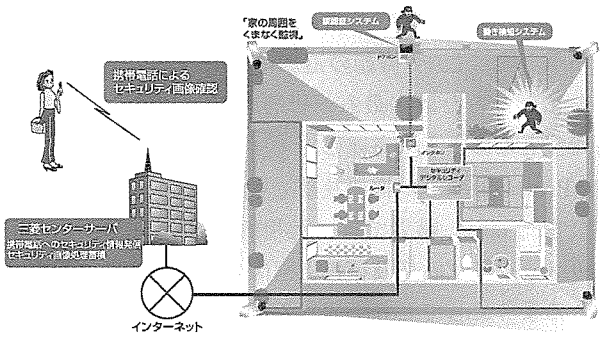


図6．セルフセキュリティシステム例

4. むすび

監視用デジタルレコーダは監視システムの中核として様々な用途で注目されてきており，こうしたニーズに業務用で培ってきた技術でこたえていくことは社会的使命と考えている。今後も，安全な暮らしをバックアップすることができる，より便利で使いやすい製品の開発を続けていく。

参考文献

(1) 熊野　眞，ほか：監視用映像デジタル記録装置，三菱電機技報，**76**，No.11，727～730（2002）

新型指紋照合装置“FPR-MK4シリーズ”

藤原秀人*
中村高宏**
鹿井正博**

New Fingerprint Recognizer “FPR-MK4 Series”

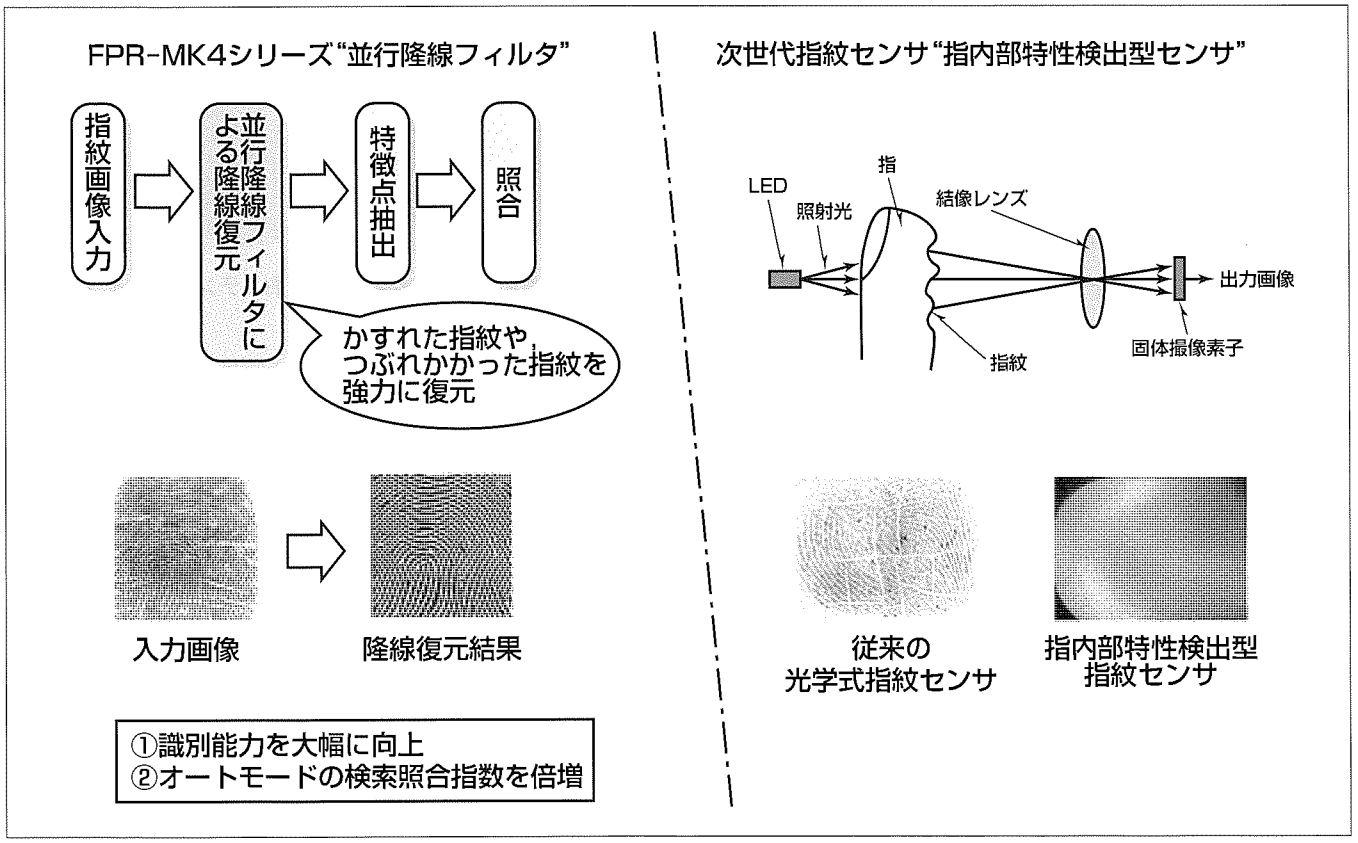
Hideto Fujiwara, Takahiro Nakamura, Masahiro Shikai

要　旨

新型指紋照合装置“FPR-MK４シリーズ”とそのアルゴリズムについて述べる。このシリーズは，“FPR-MK３Bシリーズ”に比べて識別性能が大幅に向上しており，オートモードでの検索照合指数も倍増している。

このシリーズに搭載しているアルゴリズムは“並行隆線フィルタ”と呼ぶ新しい手法であり，その最大の特長は，指紋隆線の構造的特徴である並行性に着目した高い隆線復元能力にある。すなわち，指紋隆線は基本的に並行な線で構成されており，しわ等のノイズは並行していないので，周辺に複数本並行した線が存在しているときに隆線として抽出し，並行した線が周辺に存在しない場合はノイズとして除去する。このように，並行性によって隆線とノイズを区別しながら隆線のみ復元していくので，従来，登録・照合しづらかったかすれた指紋やつぶれかけた指紋でも強力に隆線を復元できる。

また，次世代の指紋センサとして開発中の指内部特性検出型指紋センサについても紹介する。この指紋センサは，指の皮膚組織内に指紋の凹凸と対応した透過率分布が存在するという新たな知見に基づくもので，指の爪(つめ)側に赤色光を照射し，指内部を透過した光によって照明された指紋部分の光強度分布を結像レンズによって固体撮像素子に結像することで指紋画像を得る。従来の光学式指紋センサのようなプリズムに指を押し付けたときの凹凸による光の反射を画像化する方式と異なり，乾燥や濡(ぬ)れといった指表面の状態に影響を受けにくい特長を持っている。



新型指紋照合装置FPR-MK４シリーズのアルゴリズムと次世代指紋センサ

FPR-MK４シリーズに搭載されている並行隆線フィルタは，乾燥肌によるかすれた指紋や多汗によるつぶれかかった指紋でも隆線を強力に復元できるため，従来に比べて認識性能が大幅に向上し，オートモードでの検索照合指数も倍増できる。また，次世代の指紋センサとして開発中の指内部特性検出型センサは，指の爪側から照射光を当て，指を透過するときに生じる隆線と谷線の光の透過率の差を画像化する。これによって，乾燥や濡れといった指表面の影響を受けにくくできる。

*稲沢製作所　**先端技術総合研究所

1. まえがき

指紋を始めとした身体的特徴による個人識別技術(バイオメトリクス)は，第三者への貸与や紛失・忘却のおそれがないことから，IDカードやパスワードに代わる確実な個人識別の方法として注目を浴びている。特に昨今のように様々な情報がコンピュータに蓄積されている時代にあって，“だれがアクセスできるのか？”“だれがアクセスしたのか？”という“情報へのアクセスの正当性”を厳格に管理することの重要性がますます増し，そのための手段として，バイオメトリクスは非常に有効である。バイオメトリクスでは，指紋，虹彩(こうさい)，静脈，音声，顔など様々な情報が使われるが，それぞれに識別性能やコスト，大きさ面で一長一短がある。その中で指紋はその歴史が長く，コストと性能面のバランスが最も良いことから現在では最も普及している。

三菱電機も20年以上前から研究・開発を行い，昨年4月に発売したFPR-MK3Bシリーズでは，ほとんどのユーザーが“指を置くだけ”という簡単操作で本人を識別することができる。しかしながら一方で，乾燥肌や多汗，しわの多い指紋は，本人であるにもかかわらず本人と識別されない“本人拒否”が発生しやすく，何度も指を置き直したり，定期的に再登録を行うといった負担がかかっていた。

当社では，このような問題を少しでも低減し，より多くのユーザーが指紋照合装置を問題なく簡単に使えるよう，アルゴリズム及びセンサの改善に努めている。

本稿では，前記乾燥肌や多汗のユーザーに対する識別性能を大幅に向上した新製品FPR-MK4シリーズに搭載されているアルゴリズム(並行隆線フィルタ)と，さらに次世代技術として開発中の新型指紋センサ(指内部特性検出型指紋センサ)について紹介する。

2. 新型指紋照合装置FPR-MK4シリーズ

表1にFPR-MK4シリーズの性能・仕様を示す。

FPR-MK4シリーズは，昨年4月に発売を開始したFPR-MK3Bシリーズに比べると，**図1**に示すとおり外観は同じであるが，搭載されているアルゴリズムは大幅に改良されている。

FPR-MK4シリーズに搭載されているアルゴリズムは“並行隆線フィルタ”と呼ばれ，①指紋隆線はある特定範囲の周波数成分を持つ，②指紋隆線は基本的に並行であるという知識を用いて指紋隆線を復元するもので，

- 乾燥肌によってかすれたような指紋
- 多汗によってつぶれかかった指紋
- しわや傷によって途切れた指紋

という従来“本人拒否”が発生しやすかった指紋でも強力にその指紋隆線を復元することができる。

この結果，特に上記のような本人拒否が発生しやすかった指紋での識別能力を大幅に向上することができ，また，その識別能力の向上に伴って，指を置くだけで自動的に照合できるオートモードでの最大検索照合指数を倍増することができた。

次章ではこの並行隆線フィルタ[(1)]について説明する。

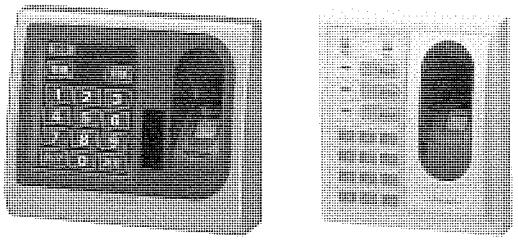


図1．指紋照合部(左：液晶タイプ，右：テンキータイプ)の外観

表1．FPR-MK4シリーズの性能・仕様

登録指数	1,000指		
照合方法※1	IDモード	グループモード	オートモード
ID番号／グループ番号	最大7けた	最大9グループ	−
検索照合指数	−	最大200指／グループ	最大400指
本人拒否率(FR)※2	0.05%以下	0.1%以下	
他人受入率(FA)	0.001%以下	0.1%以下	
読取判定時間	約0.8秒	約1秒(200指で検索照合の場合)	
登録時間	約5秒	約7秒	

指紋照合部機器仕様	液晶タイプ	テンキータイプ
外形寸法	(W)155×(H)125×(露出厚)40(mm)	(W)120×(H)135×(露出厚)38(mm)
質　量	約0.6kg	約0.3kg
環境条件	周囲温度0～40℃、湿度0～85%RH(結露がないこと)	
	直射日光の当たらない屋内環境(5,000ルクス以下)	

※1　IDモード：ID番号を入力し，指紋照合
　　グループモード：グループ(所属，部署等)番号(1けた)を入力し，指紋照合
　　オートモード：指を置くだけで自動的に照合
※2　本人拒否率は2回までのリトライを許容するものとする

3. 並行隆線フィルタ

3.1 概　要

指紋照合の代表的な方式として，隆線の端点(隆線が途切れる点)や分岐点(隆線が枝分かれする点)を特徴点として，その座標や角度を用いる特徴点マッチング方式が挙げられる。

特徴点マッチング方式の一般的な処理の流れは以下のとおりである。

(1) 入力指紋画像に含まれる，かすれやつぶれ，しわ，傷といったノイズを除去しながら隆線を復元する。

(2) 復元した隆線を二値化・細線化した後，特徴点を抽出する。

(3) 抽出された特徴点の座標や特徴点付近の隆線の角度を用いて，登録指紋との類似度合いを計算し，類似度合いが一定値を超えれば本人と判定する。

当社の指紋照合装置もこの特徴点マッチング方式であるが，この特徴点マッチング方式では，いかにして本当の特徴点を正確に抽出できるかがその識別性能を左右するため，上記流れの中で(1)の隆線を復元する処理が最も重要である。

ところが，指紋センサから常に明暗がはっきりした指紋画像が得られるわけではなく，指表面の状態によって，乾燥肌で見られる隆線がかすれた画像や，多汗な指で見られる谷線がつぶれかかった画像，しわが隆線を横断している画像などノイズが多く含まれた指紋画像になることが多い。

開発した並行隆線フィルタは，(1)の処理において，まず指紋画像から少しでも隆線らしく見える画素を可能な限り抽出する。その後，隆線が持つ並行性，すなわち“正しい隆線は複数本が並行している”という指紋を最も特徴付けている性質を利用して，ノイズと隆線を区別しながら隆線のみを残す。こうすることによって，多くのノイズを除去しながら，隆線本来のパターンを復元することができる。

以下に，並行隆線フィルタによる指紋隆線の復元処理を詳しく述べる。

3.2 隆線候補抽出

まず第1段階として，指紋画像から少しでも線らしく見える画素を可能な限り抽出し，隆線の候補(候補線)とする。線画素の抽出には，ある特定方向・特定周波数の成分を持つ線を高感度で抽出することが可能なGaborフィルタカーネルを採用し，各画素において，様々な角度に回転させたカーネルと指紋画像との相関値を計算する。そして，相関値が最大となる回転角度をその画素における候補線の方向角とし，その最大値を候補線の強度値とする。この段階では，隆線のみならずノイズの線も同時に強調されている。

3.3 並行性チェックによる隆線とノイズの区別

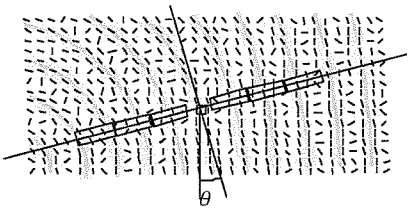
次の処理では，抽出された候補線に対して両隣に並行している別の候補線(隣接候補線)の本数を検証し，所定の本数に満たなければ候補線の強度値を下げる。ある対象画素に対する隣接候補線の強度値は，図2のように，その画素の方向角θに垂直な方向に沿ってM個のウィンドウ領域(長さは平均的な隆線間隔程度)を設け，各ウィンドウ領域内において，処理対象画素との方向角の誤差が十分小さく，かつ強度値が最大の画素を選ぶことで簡単に得られる。

以下，対象画素(x, y)の候補線の強度値を$C_0(x, y)$，その候補線に関するM本の隣接候補線の強度値を$C_i(x, y)$ $(i=1, 2, 3, ...M)$とする。なお，ウィンドウ領域内に方向角の誤差が十分小さな画素が存在しなければ$C_i=0$とする。次に，M個のC_iの値を用いて，隣接候補線の本数検証を行う。ただし，ここで扱う候補線はいわゆる2値的にシンボル化された線ではなく，強度値が0以上の連続値となっており，例えば単にC_iの値が0より大きいものを数えるといった方法では線の本数を決定できない。連続値で与えられた隣接候補線の本数検証は次式によって実現される。すなわち，対象画素の値C_0を

$$P(x, y)=\mathrm{Min}(C_0(x, y), \mathrm{Rankn}\{C_i(x, y)\}i=1...M)$$

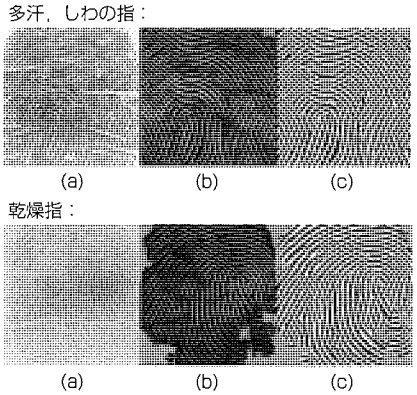
によって計算された値で置き換える。

ただし，$\mathrm{Rankn}\{C_i(x, y)\}i=1...M$は，$C_i(i=1...M)$のうち$n$番目に大きな値を返すランクオペレータ，$\mathrm{Min}(a, b)$は$a$，$b$のうち小さい方の値を返す最小値オペレータであり，もしC_iのうち十分大きな値がn個(n本)に満たなければ，Pとして元の値C_0より小さな値が返されることになる。以上の処理により，最終的にはn本以上の隣接候補線を持つ候補線の画素だけが残され，隆線上にない画素やノイズ線上に存在していた画素の値は0又は微少な値となる。図



(中心の正方形：対象画素，両側の矩形(くけい)：探索ウィンドウ，濃度：候補線強度値，短線分：候補線方向角)

図2．隣接候補線の探索ウィンドウ(M=6)



(a) 入力画像，(b) 並行隆線フィルタによる隆線復元結果，(c) (b)の2値化結果

図3．隆線パターン復元処理の例

3に，多汗，しわ，乾燥肌の指紋画像に対する隆線復元処理の一例を示す。

3.4 特徴点抽出と照合

隆線を復元した後は，前記した一般的な処理の流れ同様，2値化処理を施し(図3(c))，細線化処理した後に端点や分岐点といった特徴点を抽出し，登録指紋の特徴点と比較することで本人か否かを判定する。

4. 次世代指紋センサ

当社では，ここまで述べたアルゴリズムの改善に加えて，指紋画像を取得するセンサに関しても開発を行っている。

ここでは，現在開発中の次世代指紋センサである，“指内部特性検出型指紋センサ”について簡単に紹介する。

4.1 従来の光学式指紋センサ

従来の光学式指紋センサでは，指紋パターン像を得るために，全反射法や光路分離法といった検出原理が使われてきた。これらの方式は，指を置くプリズムと皮膚表面との接触の有無(指紋山部：接触，指紋谷部：非接触)を光の反射特性の差により可視化する方式である。そのため，皮膚の乾燥や濡れによって皮膚とプリズムとの接触の度合いが変化すると，センサにより得られる指紋画像も変化する。このことは，例えば冬と夏で得られる指紋画像が変化することを示している。

4.2 指内部特性検出型指紋センサ[2][3]

現在開発中の指内部特性検出型指紋センサは，指の皮膚組織内には真皮辺りから表皮にかけて指紋の凹凸と対応した透過率分布が存在するという新たな知見に基づくものである。

生体内部の光の反射率分布を観測すると，指紋山部に比べ指紋谷部の皮膚組織内での反射光強度が低く散乱が小さいという傾向が見られる。このことから，指紋の山部に比べ谷部で透過率が高い透過率分布が皮膚組織内に存在していると考えられる。

この指内部の透過率分布を二次元で検出するために，図4に示すように，LED(Light Emitting Diode)により指の爪側に赤色光を照射し，指内部を透過した光によって照明された指紋部分の光強度分布を結像レンズによって固体撮像素子に結像する。この結果，上述の透過率分布と一致する図5に示すような指紋の山部に比べ谷部が明るい指紋画像が得られる。

このように，指内部特性検出型指紋センサでは，従来のような接触の有無を画像化するのではなく，指内部の真皮から表皮にかけての透過特性を直接画像化するので，乾燥や濡れといった皮膚表面そのものの影響を受けにくく，安定した指紋画像が得られる。

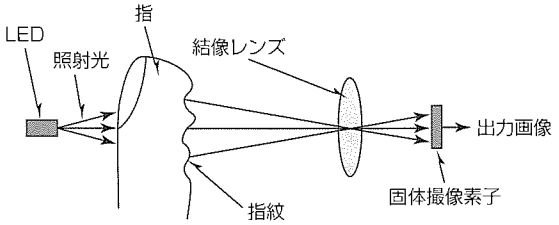
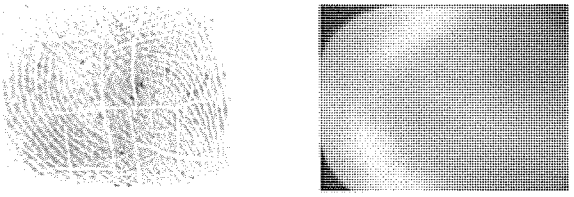


図4．指内部特性検出型指紋センサの光学系



(a) 従来の光学式指紋センサ　(b) 指内部特性検出型指紋センサ

図5．出力画像

また，原理的には従来のようにセンサに指を押し付ける必要がないため，将来的には非接触でのセンシングが実現できる可能性がある。

5. むすび

新製品FPR-MK4シリーズに搭載されているアルゴリズム並行隆線フィルタについて述べた。このアルゴリズムは，指紋隆線の構造的特徴である並行性に着目してかすれた指紋画像やつぶれかけた指紋画像でも強力に隆線を復元できる。このアルゴリズムを搭載したFPR-MK4シリーズは，同MK3Bシリーズに比べて，本人拒否率1/2，他人受入率1/10と大幅に認識性能が向上している。

また，次世代の指紋センサとして開発中の指内部特性検出型指紋センサについても紹介した。従来の光学式指紋センサと異なり，指紋表面の乾燥や濡れといった皮膚表面の影響を受けにくい特長を持っている。今後は，より多くの人がより簡単に使えるよう，ここで紹介した指内部特性検出型指紋センサの製品化を目指して開発を続ける予定である。

参考文献

(1) 中村高宏，ほか：並行隆線フィルタ法による指紋画像の隆線強調処理，通信学会研究会資料，PRMU2003-65，47～52（2003）

(2) 鹿井正博，ほか：皮膚組織内の透過率分布を用いた新方式光学指紋センサ，第64回応用物理学会学術講演会講演予稿集，909（2003）

(3) 佐野恵美子，ほか：皮膚組織内の透過率分布を用いた新方式光学指紋センサ(Ⅱ)，第51回応用物理学関係連合講演会講演予稿集，1131（2004）

顔画像認識技術

橋本　学*　　Jay Thornton***
田中健一**
Michael Jones***

Human Face Recognition Technology

Manabu Hashimoto, Kenichi Tanaka, Michael Jones, Jay Thornton

要　旨

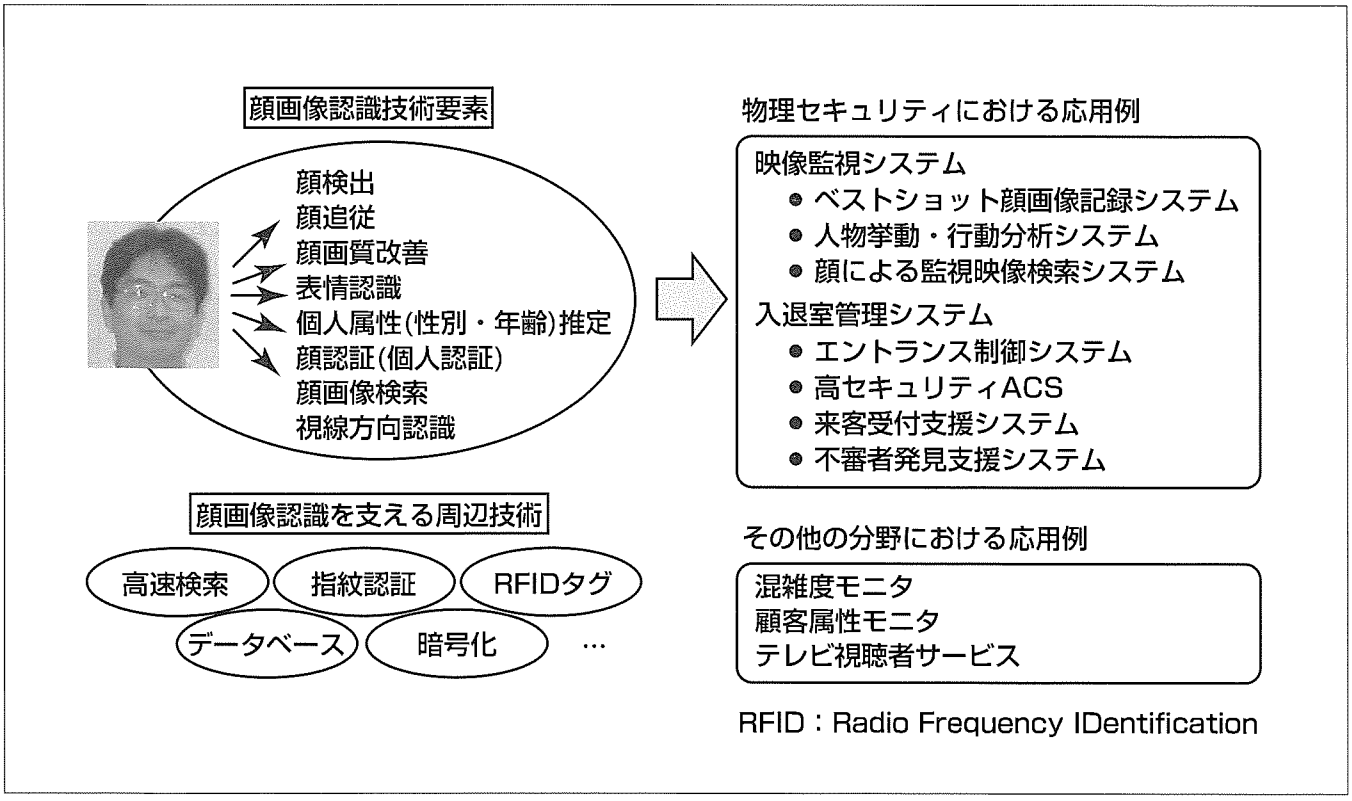
映像監視・セキュリティ分野の新技術として，近年，カメラ監視システムと入退室管理(Access Control System：ACS)システムの需要が高まっている。

カメラ監視システムは，一般に①映像入力，②画像伝送・蓄積，③情報分析，の3つの要素で構成されている。このうち，①と②については，高解像度・高画質カメラ，ブロードバンド通信，大容量ストレージの発達により年々高度化しているが，③については膨大な蓄積映像を効率良く分析するための方法がなく，画像認識技術の応用が望まれていた。

一方，入退室管理では，従来のICカード認証で問題となる他人カードの不正使用(なりすまし)の防止のために，個人特有の生体情報を利用したバイオメトリクス認証が注目されている。なかでも指紋照合装置は小型で高精度という特長があり幅広く実用化されているが，認証のためには指をセンサ部分に正しく置くなど本人の協力が必要なため，利便性の向上が求められていた。

これらの課題に対し，人間の顔画像認識技術の開発が期待されている。顔は，個人の特定に非常に有用な情報を持っており，また，非接触で比較的遠方から撮影できるため利便性が高いという利点があることから，入退室管理における個人認証に用いられるだけではなく，監視カメラとの親和性が高いために映像分析にも有用であり，下図に示すように多くの応用例が考えられる。

本稿では，人間の顔を認識する基本技術として，画像から正確・瞬時に顔を切り出す高速顔検出技術，及び個人同定のための高速高精度の顔認証技術を述べるとともに，映像監視への応用としてベストショット顔画像記録技術を紹介する。



顔画像認識技術と応用展開

顔画像認識技術としては顔検出，顔認証の二つの技術が主流であるが，そのほかにも，性別・年齢などの個人属性推定，表情・視線方向認識等がある。これらに高速検索技術，データベース技術，さらに指紋やRFIDタグ関連技術等を組み合わせることにより，多様な応用が可能となる。例えば，物理セキュリティ分野では，ベストショット顔画像記録システムなどの監視システムや，エントランス制御，高セキュリティACSなどの入退室管理システムのほか，駅・学校など公共施設での混雑度モニタや小売店での顧客属性モニタ等に展開できる。

*先端技術総合研究所(工博)　**同研究所　***Mitsubishi Electric Research Laboratories(Ph. D)

1. まえがき

コンピュータによる顔画像認識に関する研究開発の歴史は古く，医療・福祉分野，機械とのコミュニケーションのためのヒューマンインタフェース分野等への展開が模索されてきたが，汎用パソコンが普及した1990年ごろからは急速に実用を意識した研究が活発化した[1][2]。顔画像認識はその目的から以下の3つに分類されるが，セキュリティ関連製品と特に関係が深いのは，画像中の顔を切り出すための顔検出技術，及び顔による個人特定のための顔認証技術である。

(1) 顔検出技術
(2) 顔認証技術
(3) 個人属性認識技術

顔検出ではニューラルネットワークを用いた研究[3]が実用的な検出率を達成し，また，顔認証でも統計解析に基づく手法[4]やグラフ照合に基づく手法[5]が考案され，FERET(Facial Recognition Technology)，FRVT(Face Recognition Vendor Test)といった世界的なコンペティションにより認証率の高さが競われている[6]。

セキュリティ分野における顔画像認識では，認識率と並んで，高速性が非常に重要である。映像監視では通常動画像を扱うことからリアルタイムの処理が必要であり，また，個人認証においても，入力顔画像が特定の人物と同一か否かを認証する1：1認証だけではなく，膨大な顔データと比較照合する1：N認証のためには高速処理のニーズが高い。

本稿では，当社独自の長方形フィルタ(Rectangle Filter：RF)群による特徴抽出とAdaboost学習に基づく顔検出技術[7]とその応用システム[8]，及び顔認証技術[9]を紹介し，実用的な認識率とともに，動画像に適用可能な高速処理を実現したことを示す。

2. 高速顔検出技術とその応用

2.1 高速顔検出技術

2.1.1 顔検出の原理

顔検出は，学習フェーズと検出フェーズの2つから構成される。**図1**にアルゴリズムの概要を示す。学習フェーズでは，膨大な顔画像データと非顔画像データを学習させて特徴空間内に境界線を設定する。これが顔検出のための識別器となる。その際，顔画像・非顔画像に対して，**図2**に示すような，白黒2値の長方形フィルタ(RF)を作用させることにより情報圧縮を行う。フィルタの数や種類は，顔検出率が最大になるようにAdaboost学習により決定される。検出フェーズでは，入力画像を小領域に分割し，領域画像ごとに学習時と同一のフィルタ群を作用させ，識別器により顔か否かを判定する。この処理を入力画像全体にわたって繰り返すことにより，顔検出が行われる。なお，多様な大きさの顔を検出するために，小領域のサイズは複数設定する。

2.1.2 性能評価結果

顔検出識別器の生成のために顔画像サンプルを5,000事例，非顔画像サンプルを1億事例用いて学習させ検出率を求めたところ，正面顔で99.7%，水平±15度顔で99.3%，垂直±15度顔で99.7%となり，実用的な性能であることが確認された。また，この手法では特徴抽出のために計算コストの低いRFを用いているため，正面顔，斜め顔，傾いた顔に対する検出を同時に行った場合の処理時間が約20フレーム／秒(Pentium4 3.2GHz)と高速であることを確認した。

2.2 ベストショット顔画像記録システムへの応用

この手法の高速性を生かし，ベストショット顔画像記録システムを試作した。これは，通行する人物の顔画像を発見・追従し，一連の顔画像の中から最も写りの良い顔を自動的に選択して記録するシステムである。**図3**にシステム

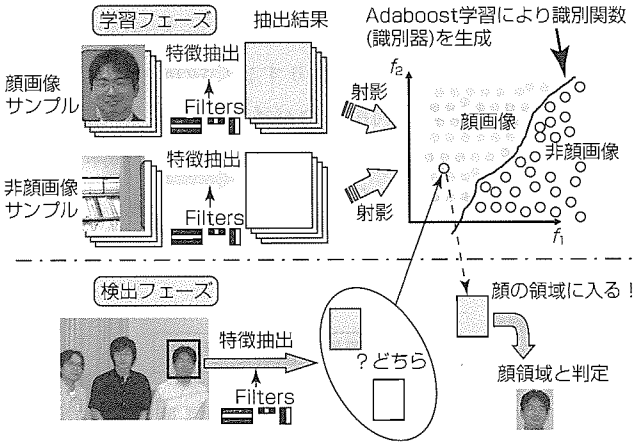


図1．顔検出アルゴリズム

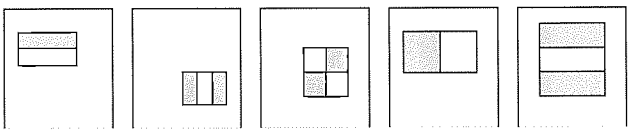


図2．Rectangle Filterの例

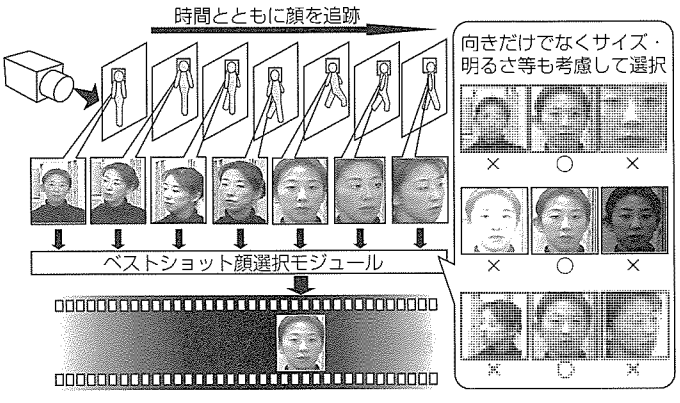


図3．ベストショット顔画像記録システムの概念図

の概念図，図4にベストショット顔画像記録システムの構成を示す。このシステムは，高速顔検出モジュールのほかに，検出した顔を追跡するテンプレートマッチングによる顔追跡モジュール，及び顔の映りの良さを評価して数値化し最も写りの良い顔を選択するベストショット選択モジュールから構成される。ベストショットの計算には，顔の向き，顔の大きさ，明るさ，コントラスト，眼領域の鮮明度等が統合的に用いられる。このシステムが複数の顔検出候補からベストショットを選択している様子を図5に示す。

このシステムをカメラ監視システムに適用することにより，監視員が視認しやすい顔画像のみを効率良く記録することができるため，蓄積映像を見ながら不審者や特定人物を短時間に発見することが可能となる。また，動画映像を同期記録しておくことにより，顔画像をキーとした映像検索システムに発展させることも容易であり，被写体人物の行動分析も簡単である(図4)。さらに，後述する高速顔認証との組合せにより，データベース中の要注意人物との照合も高速に実現できるだけでなく，同一カメラに頻繁に撮影されている人物を発見するなどの高度な分析も可能である。また，図6に示したのは，このシステムにより発見し追跡中の顔画像に自動的にモザイクを施した例である。モザイク画像を記録することにより，プライバシーに配慮した防犯カメラが構築できる。

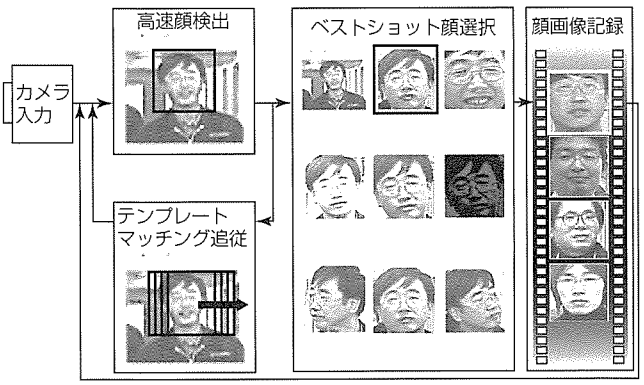


図4．ベストショット顔画像記録システムの構成

図5．選択されたベストショット画像

3. 高速顔認証技術

3.1 顔認証の原理

顔認証の基本的な考え方は，顔検出と類似している。すなわち，あらかじめ顔認証のための識別器を生成する学習フェーズと，その識別器を用いて2つの顔画像，すなわちあらかじめ登録された登録画像と，新たに入力された照合画像の同一性を判定する認証フェーズから構成される。認証フェーズの実行のためには，事前に学習フェーズが実行される必要があるが，説明を簡単にするために，まず最初に認証フェーズから説明する。

図7に認証フェーズにおける顔照合アルゴリズムの概要を示す。登録画像とはあらかじめ個人ごとに準備しておく画像であり，照合画像とは新たに入力された画像である。認証フェーズでは照合画像と登録画像の類似度が数値化され，同一人物かどうかが判定される。顔類似度の計算のため，まず各々の顔画像に対する正規化が行われる。眼の中心が検出され，画像中の所定の位置するように調整する。顔領域の大きさは一律に64×80画素になるように調整される。さらに照明変動の影響を低減するために，明るさ，コントラスト，低周波照明変動成分の除去も行われる。これらの正規化された顔画像に対し，Rectangle Filter群が作用され，畳み込み演算により特徴量が計算される。RFのサイズも64×80画素であり入力顔画像と同一なのでフィルタを走査させる必要はない。しかもRFは画像平面に対して垂直・水平な辺を持つ白黒2値の直方形フィルタであるため，畳込み値の計算は極めて高速に行われることがこの

図6．検出した顔領域にモザイクを付加した映像

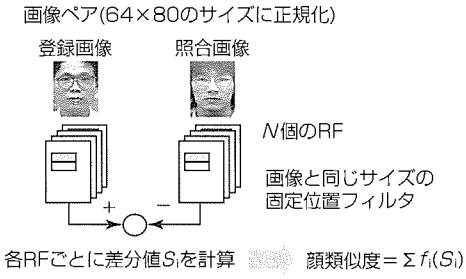


図7．認証フェーズにおける顔照合アルゴリズムの概要

方式の特長となっている。RFはN個準備されるので，各特徴量はRFごとに計算され，それらの差分(Si)をN個全てについて総和したもの$\Sigma f_i(S_i)$が類似度(正確には非類似度)となり，これをしきい値と比較して同一人物か否かを判定する。

以上説明した認証フェーズにおいては，使用するRFの種類，個数，判定しきい値が重要である。これらを決定するのが学習フェーズの役割である。学習フェーズでは，IDが既知の多くの顔画像からなる学習用データベースを用いる。データベースから任意の2枚の顔を選び，それらに対してランダムに設定したランダム個数のRFを作用させ，ランダムに設定したしきい値を用いて類似度を計算する。2枚の顔の同一性は既知(教師信号)であるから，計算された類似度が教師信号と等しい(照合成功)場合は用いたRFの個数や種類は妥当であると考え，別の2枚の顔を選んで同じ動作を繰り返す。照合失敗の場合は用いたRFの個数や種類が不適切であると考えられるので，一定の法則にしたがってこれらを微小修正し，認証が成功するまでやり直す。このシステムでは，以上説明したような照合失敗事例数が低減するような学習形態に適しているとして近年注目されているAdaboost学習を適用した。

3.2 顔認証性能評価結果

実画像を用いた実験により，この手法の認証率を評価した。その結果，EER(Equal Error Rate)＝1.4%となり，実用的な性能を得た。**図8**に，この実験で自動的に選択された151個のRFのうち25個を示す。また，処理時間評価結果を**表1**に示す(Pentium4 3.2GHz使用時)。

このように，この手法は，1：1認証時間が0.42msと，非常に高速である。顔検出と正規化は入力画像1枚当たり1回のみ行えばよいので，例えば入力画像を1,000枚の顔画像データベースと照合した場合でも処理時間は0.5秒以内である。この技術をベストショット顔画像記録システムと組み合わせても，顔の検出速度よりも十分高速な顔認証が達成できているため，動画像による検出・認証を一連の動作としてオンラインで実行可能である。

4. むすび

セキュリティに適用可能な顔画像認識技術として，顔検出技術と顔認証技術の原理を解説し，評価結果を示した。いずれも，シンプルなフィルタを効果的に適用することにより，高い認識率と超高速性の両立を達成した。顔検出については，通行人の顔画像を記録するベストショット顔画像記録システムとして，監視システムにおける映像分析の効率化が可能なことを示した。このシステムは認識しやすい高品質の顔画像を自動記録できることから，顔による個人認証や属性認識など様々な顔画像認識技術を搭載することが可能である。今後は，これらの技術を監視レコーダや入退室管理などに展開していく予定である。

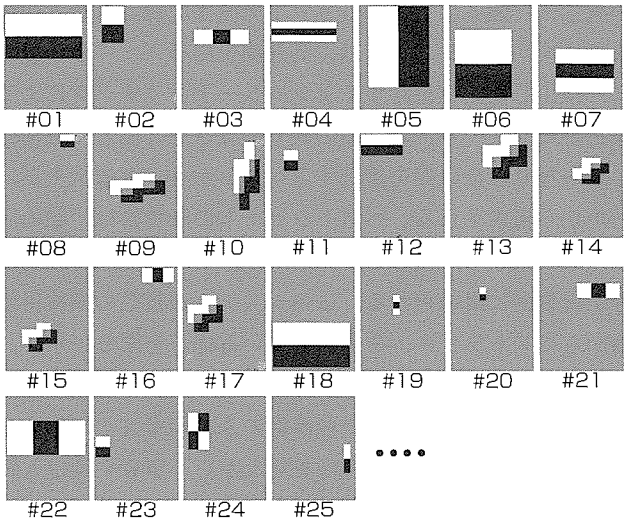


図8．選択されたRectangle Filter群

表1．処理時間計測結果

	処理時間(ms)
顔検出	15.60
正規化	3.90
特徴抽出と照合	0.42

参考文献

(1) 赤松　茂：コンピュータによる顔の認識サーベイ，信学論(A)，**J80-A**，No.8，1215～1230（1997）

(2) Zhao，W.，et al.：Face Recognition：A Literature Survey，UMD CS-TR-4167（2000）

(3) Rowley，H.A.，et al.：Neural Network based Face Detection，IEEE Trans. on PAMI，**20**，No.1，23～28（1998）

(4) Moghaddam，B.，et al.：Bayesian Face Recognition，Pattern Recognition，**33**，Issue 11，1771～1782（2000）

(5) Wiskott，L.，et al.：Face Recognition by Elastic Bunch Graph Matching，IEEE Trans. on PAMI，**19**，No.7，775～779（1997）

(6) Phillips，P.J.，et al.：Face Recognition Vendor Test 2002，NISTIR 6965（2003）

(7) Viola，P.，et al.：Rapid Object Detection using a Boosted Cascade of Simple Features，Proc. IEEE Conf. CVPR（2001）

(8) 鹿毛裕史，ほか：ロバスト顔追跡によるベストショット顔画像記録システム，第10回画像センシングシンポジウム，541～546（2004）

(9) 三輪祥太郎，ほか：Rectangle Filterの最適選択に基づく高速顔認証システム，第10回画像センシングシンポジウム，363～366（2004）

侵入検知・追跡カメラ

羽下哲司*
新房健一**
田中健二**

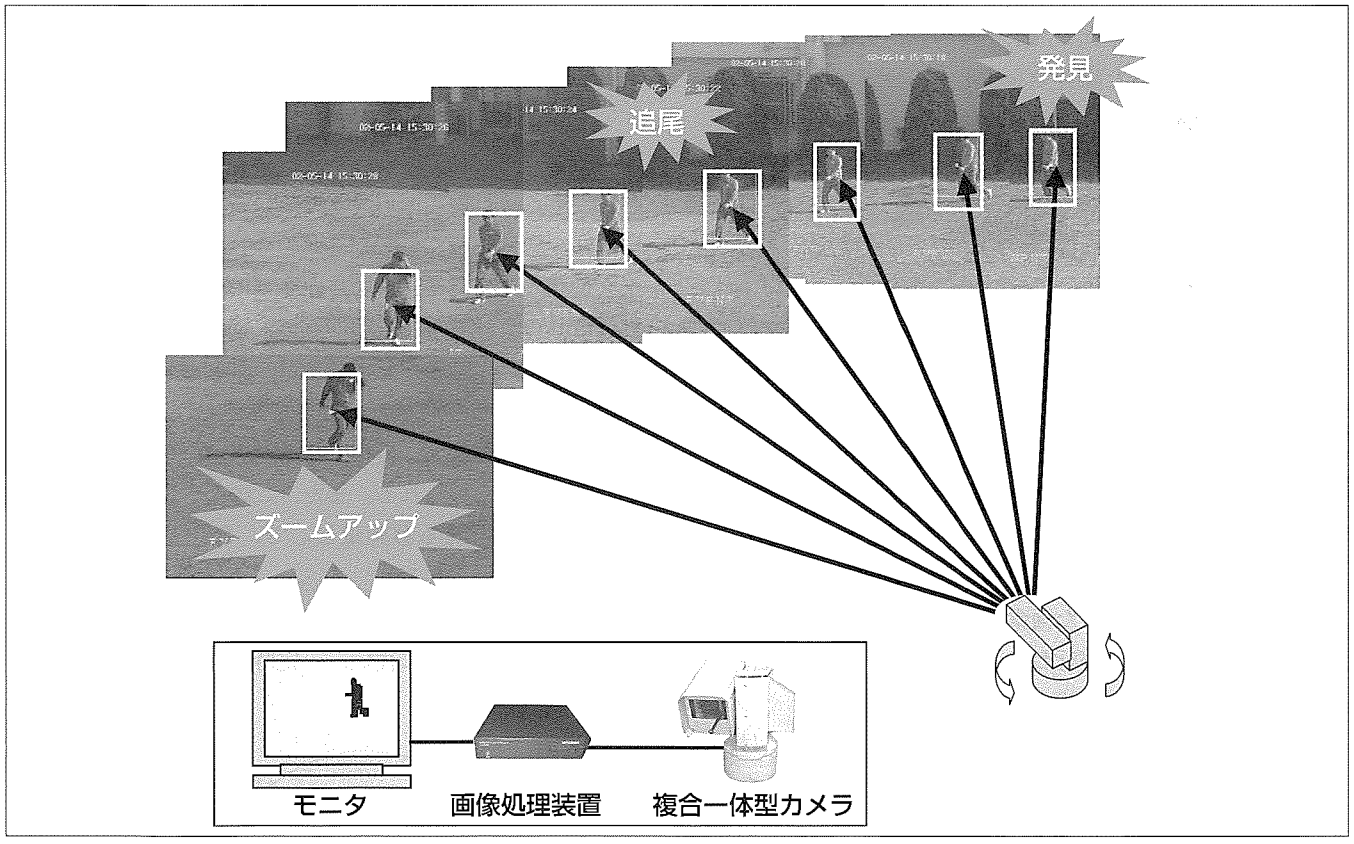
Intruder Detection and Tracking Camera

Tetsuji Haga, Kenichi Shimbo, Kenji Tanaka

要　旨

画像処理技術を用いた侵入者の自動検知は，古くから，発電所・変電所などの大型プラントや，水処理設備・空港設備などの重要施設における監視員の負荷軽減，省人数化のために開発されている。このような分野では，見逃しが許されないだけでなく，誤検出の発生を極力ゼロにすることが望まれる。このため，環境変化に強く高感度のカメラが導入されるとともに，誤検出を抑制する画像処理アルゴリズムと，それをリアルタイムで実行する専用ハードウェアが開発された。また，少ないカメラ数でより広い範囲を監視するというニーズが高まっている。これにこたえるために，カメラとパン／チルト雲台が一体化した複合一体型カメラが導入され，検出した侵入者をカメラのパン／チルト／ズームを制御して自動追尾しながら視野内にとらえ続ける画像処理アルゴリズムが開発された。近年では，CPUの高性能化と画像処理装置の小型化が進み，外乱に対してより頑強な画像処理アルゴリズムが実現可能となり，画像処理装置を監視カメラに内蔵できるまでになっている。また，ニーズの面からも，プラントや重要施設だけでなく，新たにオフィスやホームなどにおけるセキュリティに対する関心が急速に増加しており，今後，映像監視の分野では画像処理一体型監視カメラが伸びることが予想される。

本稿では，このような監視カメラで用いられる画像処理アルゴリズムのうち，特に侵入検知における誤報低減と，移動する侵入者の自動追尾に関して，その技術と性能について述べる。



侵入検知・追跡システムの構成

自動追尾機能の画像処理は，あらかじめ設定された監視対象箇所を常時画像処理し，侵入検知後に複合一体型カメラ（パン／チルト雲台が一体化されたカメラ）を自動連動動作させて，対象物を捕捉（ほそく）するよう自動追尾の視野制御を行う。

*先端技術総合研究所　**郡山製作所

1. まえがき

監視カメラから得られる映像を処理することにより，自動的に侵入者を検出する技術，そして侵入者を発見後，カメラのパン／チルト／ズームを制御しながら移動する侵入者を追跡して視野内にとらえ続けその詳細な特徴や行動履歴を記録する自動追尾の技術は，映像監視セキュリティの分野でそのニーズが近年急速に高まっている。ここで求められる機能は，昼夜，天候を問わず，近景から遠景にわたる監視範囲内で侵入者を検出し，警報を発すると同時に映像を記録するものである。侵入者検知では，見逃しによる失報が許されないと同時に，日照変動や木の揺れ，水面の光の乱反射などの環境変動に起因する誤報を低減することが要求される。また，自動追尾では，人のような非剛体の移動対象が自然背景中を移動する場合に生じる，形状の変形や見え方向の変化，他の障害物による部分的な遮蔽（しゃへい），コントラストの高い背景の影響などの，追尾を不安定にする要因が多い条件下でも，安定な追尾を行うことが求められる。

2. 侵入者検知における誤報低減技術

侵入者検知は，通常は無人の場所に出現する移動物体を検知するものであるが，侵入者が遠方に現れ画像中でのサイズが数十画素程度の小さな段階であっても，また，身体の一部が他の物体に隠れて，上半身のみ，又は下半身のみしか写らないといった場合でも検出する必要がある。このため，侵入者が写っていない背景画像と入力される画像との差分に対してしきい値処理を行い，侵入者が現れた領域を検知する背景差分法が一般的によく用いられる。背景差分法で用いられる背景画像は，過去から現在までに入力された一連の入力画像を用いて統計的に推定される。例えば，各画素の過去一定時間における輝度値の平均値を画素値とする方法がある。また，2値化のしきい値は，同じく過去一定時間における各画素の輝度値の標準偏差の定数倍（例えば2.5倍など）に設定する方法がよく用いられる。さらに，これらを発展させて，複数の平均と標準偏差の組の重みつき和で背景画像をモデル化し，エラーを低減させた例[1]もある。背景差分処理によって得られる領域に対しては，ノイズ除去処理，連結した画素に同一インデックスを割り当てるラベリング処理が行われ，出現の時間的な連続性や面積，重心位置，縦横比等の特徴量抽出を行って，その変化領域が侵入者かどうかを判定する。しかし，実際には，日照変動や木の揺れなど，多くの背景変動が存在するため，単純な形状特徴量の比較だけでは侵入者以外の誤報が多く発生してしまう。

ここで変化領域内の詳細な動きベクトルに着目すると，侵入者と他の誤報要因とでは，以下のような違いが見られる[2]。

(a) 侵入者では，変化領域内部の動きベクトルが，
- 空間的に一様（局所フローの大きさ，向きがほぼ同じ）
- 時間的に連続（同じ方向に一定時間以上連続して運動）

(b) 一方，その他の誤報要因では，
- 変化領域内に動きがない（日照変動など）
- 空間的に一様でない（水面の乱反射など不均一な動き）
- 空間的に一様であるが時間的に連続しない（往復運動）

すなわち，変化領域内部の局所動きベクトル求め，①空間的に平均した動きの強さF_1，②時間的に平均した動きの強さF_2，③時間的な動きの一様性F_3，の3種類の動きの特徴量を計算し，それら3つのいずれもが高い領域を選択することにより，侵入者のみを，他の，例えば明るさが変化しても動きがない日照変動や，繰り返し運動を行う木や影の揺れ，ランダムな動きの集まりである光の乱反射などの誤報要因から区別して抽出することができる。

変化領域内部の動きベクトルは，図1に示すように，領域R_jの内部を8×8程度の複数の小ブロックB_iに分割し，現在の画像$I_t(x, y)$と1フレーム過去の画像$I_{t-1}(x, y)$との間で以下に示す相関演算を行い，得られる相関値マップ$S_{R_j}(u, v)$の極小値を与える(u, v)の組として得られる。

$$S_{B_i}(u, v)=\sum_{(x, y)\in B_i}|I_{t-1}(x+u, y+v)-I_t(x, y)| \quad \cdots\cdots\cdots\cdots(1)$$

各小ブロックB_iで得られる局所動きベクトルが一様であれば，それぞれの相関値マップを累積して得られる累積相関値マップは，各々のピークが強め合ってできた明瞭なピーク形状となる。逆に，動きが空間的に一様でない場合は，それぞれのピークが相殺しあって，平坦（へいたん）な形状となる。また，動きがない場合は，動きゼロの点にピークが出現する。したがって，空間的に平均した動きの強さF_1は，累積相関値マップの極小値と動きゼロの点との相関値との差として求められる。また，このとき累積相関値マップの極小値を与える移動量として，変化領域の代表速度(u_{min}, v_{min})が得られる。

時間的に平均した動きの強さF_2は，各フレームにおける代表速度(u_{min}, v_{min})に従い，一定時間（約1秒）の間追跡を

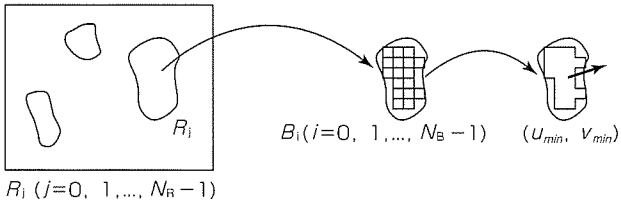


図1．変化領域内のブロックの配置と代表速度(u_{min}, v_{min})の算出

行い，その間に得られる空間的な累積相関値マップを時間的にも累積し，F_1同様に，得られる時空間累積相関値マップの極小値と動きゼロの点との相関値との差として求められる。また，時間的な動きの一様性F_3は，一定時間(フレーム数)の追跡過程の中で，空間的に平均した動きの強さF_1が，あるしきい値を超えたフレーム数の割合として求められる。

図2は，上で求めた3つの特徴量F_1-F_2-F_3で構成される特徴空間で，人と人以外の誤報要因の分布をプロットしたもので，識別平面によりこれらが精度良く分離できていることが分かる。**図3**は，木の揺れや水面の乱反射等，誤報要因の多い屋外環境下で侵入者を検知した画像処理結果である。侵入者と認識された変化領域は白い四角形で囲み，背景変動と認識された変化領域は黒い四角形で囲んで表示している。強風の中で揺れる，ちょうちんや垂れ幕，樹木(a)(b)については背景変動と認識し，人のみを侵入者と識別

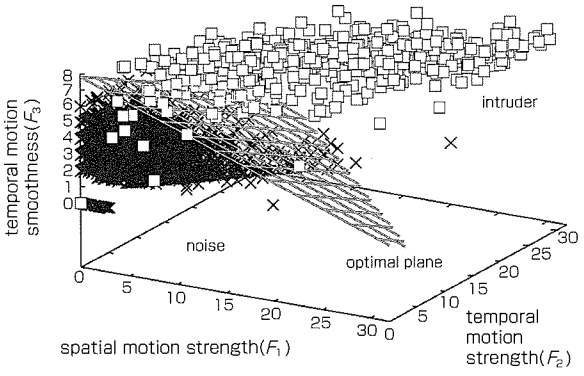


図2．最適識別平面(格子で表示)と，平行な平面から見た特徴空間F_1-F_2-F_3における人と誤報要因の分布

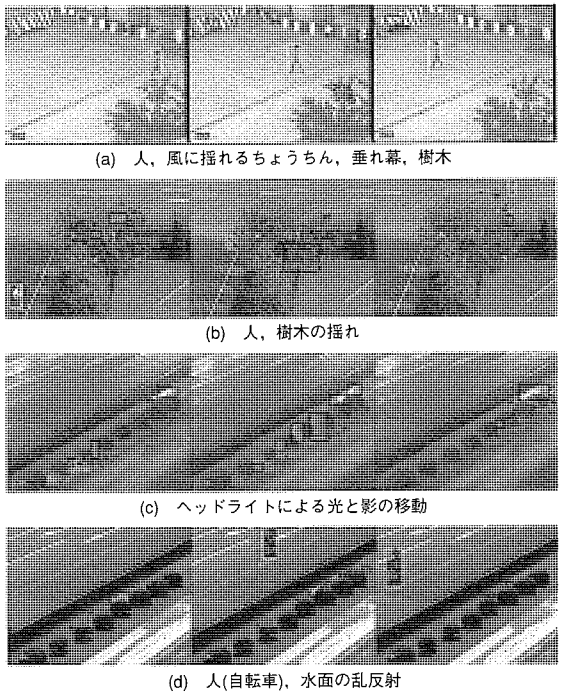


図3．画像処理結果(侵入者を白い四角形で囲み，その他の背景変動を黒い四角形で囲んで表示)

している。また，車のヘッドライトによる光と影の移動(c)や，水面の光の乱反射(d)に関しても，背景変動と認識し，誤検出していない。

3. 非剛体対象である人の安定な自動追尾技術

移動物体を追尾する一般的な手法には，追尾対象を含む矩形(くけい)領域をテンプレートとして登録し，入力された画像中でテンプレートと最も良く一致する領域を探索し，以後，テンプレートの探索と更新を続けながら追尾を行う手法がよく用いられる。しかしこのような方法で人のような非剛体の対象を追跡した場合，テンプレートの中心と追尾対象の重心との間に生じるずれが，更新の度に増大し，やがて追尾対象を外してしまう[3][4]。また，矩形のテンプレート内部に背景の領域が含まれるため，この背景部分のコントラストが追尾対象よりも高い場合は，誤って背景を追尾してしまう。そこで，このような問題を解決するために，ここでも局所的な動きベクトルを用いる。例えば，追跡対象とその周辺の背景領域に8×8画素程度の複数の小ブロックを配置し，背景領域との動きベクトルの違いによって，追尾対象を検出し，位置ずれを補正しながら追尾処理を同時に行うことにより，追尾の安定性は向上する[5]。しかし，画像中には輝度分布が平坦な部分など，動きベクトルが安定に求められない点も多く，画像全体で相関演算を行うことは効率的ではない。そこで，空間周波数成分の高い部分(エッジ)部分に集中して小ブロックを配置することにより，効率的に局所動きベクトルを求める。

図4に示すように，抽出された侵入者の変化領域の重心(g_x, g_y)を中心として，その幅w，高さhよりも相関ブロック数個分だけ大きなサイズ$w'\times h'$の広がりを持った矩形の領域を設定し，その内部(移動対象側)と外側(背景側)で空間周波数成分の高い部分にそれぞれN_o個，N_b個の相関ブロックB_{ok}，B_{bk}を設置する。それぞれのブロックで，相関演算を実行し，B_{bk}側の相関値マップを累積した累積

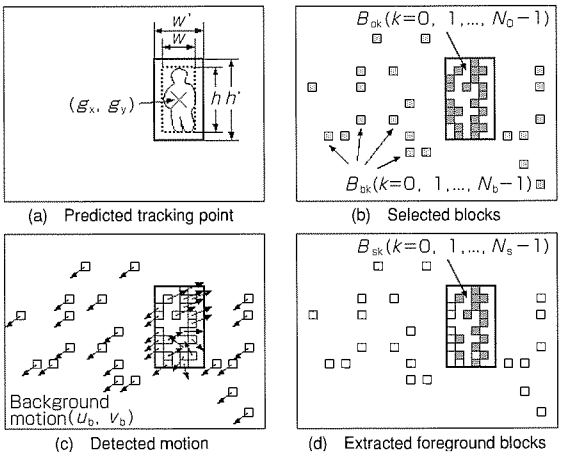


図4．対象，背景の各領域での相関ブロックの配置と，局所動きベクトルの違いによる移動対象の抽出

相関値マップから，背景の速度(u_b，v_b)の推定を行う。そして，N_o個の内部ブロックB_{ok}の中から，背景の速度(u_b，v_b)と異なる動きを持つN_s個の追跡対象ブロックB_{sk}を抽出する($N_s<N_b$)。これらの処理は，動きベクトルを特徴量として背景差分を行ったことに相当する。そして，B_{sk}の集合を追尾対象とみなし，その重心位置に基づいてカメラのパン／チルトを制御しながら追尾を行う。ズームはサイズが画像中で定められた大きさになるように制御される。

しかしこの手法でも，人の胴体内部などの輝度分布が平坦な部分や，四肢など全体の動きと異なる動きをする部分では，動きベクトルの出現と消失が繰り返されて，重心位置が安定せず，追跡が不安定になるという問題があった。そこで，フローの時間的な連続性に着目することにより，追尾の安定性向上をさせている。

図5に示すように，過去数フレームにわたり抽出した追跡対象ブロックB_{sk}，すなわち過去の抽出領域を追尾対象の移動に合わせて画素単位で位置合わせを行いながら現在の画像に重ね合わせると，最終的に移動対象の検出頻度が十分に高い画素により構成される領域が生成される。このようにして得られた領域を時間平均シルエットと呼び，このシルエットの重心及びサイズに基づいて，カメラのパン／チルト／ズームを制御し，侵入者の自動追尾を行う。その結果，たとえ各々のフレームでは動きベクトルの部分的な欠落があったとしても，時間平均シルエットでは，時間的な重ね合わせの効果による補間が行われているため，人のような非剛体の移動対象であっても検出される重心の変動が抑えられ，結果として安定な追尾が可能となる。**図6**(a)～(d)に侵入者の追尾結果を，時間平均シルエットの輪郭線を白色でオーバーレイして示す。追尾対象の形状変形や見え方の変化(a)に対しても，また樹木などの障害物による追尾対象の部分的遮蔽(b)に対しても，さらに日当たりと日陰の境界のような高コントラストの背景を通過する場合(c)でも，その影響を受けず，安定な追尾が実行できていることが分かる。さらに，時間的な平滑化の効果により遮蔽物の後ろを通過するような一時的な全遮蔽(d)に対しても，追尾対象を見失うことがない。

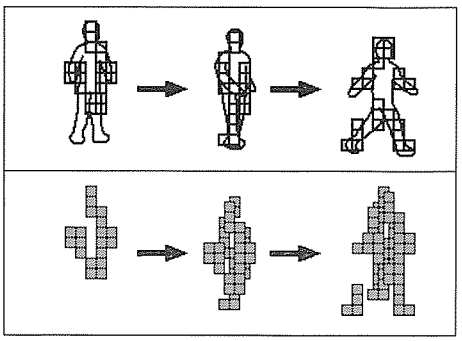
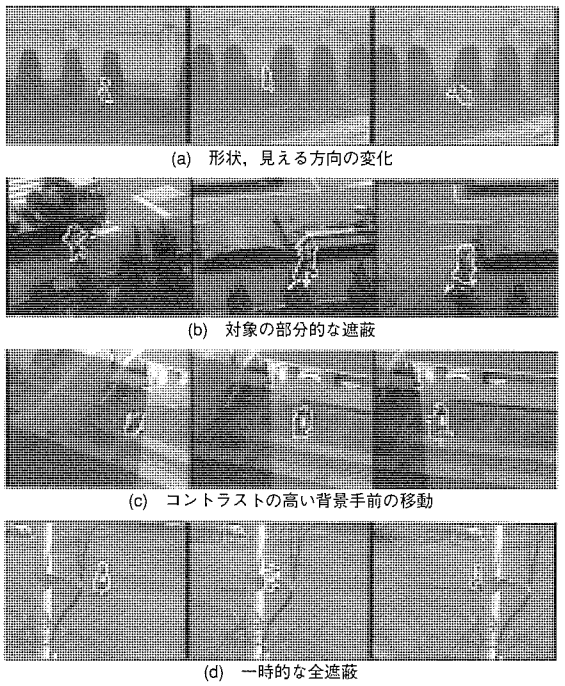


図5．各フレームで抽出される追跡対象に属するブロック(上段)と，生成された時間平均シルエット(下段)



(a) 形状，見える方向の変化

(b) 対象の部分的な遮蔽

(c) コントラストの高い背景手前の移動

(d) 一時的な全遮蔽

図6．侵入者の追尾処理結果(原画像に時間平均シルエットの輪郭を白線でオーバーレイ表示)

4. むすび

画像処理技術を用いた侵入者検知における誤報低減技術と，人のような非剛体の移動対象をカメラのパン／チルト／ズームを制御して視野内にとらえ続ける自動追尾技術を紹介した。これらの画像処理アルゴリズムは，現在，専用画像処理プロセッサで実現されているが，CPUの性能向上により，小型化が図られ，カメラ一体型システムとして発展することが予測される。それと同時に，今後，屋外の専用施設だけでなく，オフィスやホームなどの分野のセキュリティ監視にも広がりをみせることが期待されている。

参考文献

(1) Stauffer, C., et al.：Adaptive background mixture models for real-time tracking, Proc.Computer Vision Pattern Recognition, Fort Colins, CO (1999-6)

(2) 羽下哲司，ほか：変化領域内の動きの時空間特徴に着目した屋外情景における歩行者の検出，信学論(D-Ⅱ)，**J87-D-Ⅱ**，No.5，1104～1111 (2004)

(3) 伊藤　渡，ほか：画像認識ハードウェア内蔵カメラを用いた自律移動物体追尾カメラ，第5回画像センシングシンポジウム講演論文集，165～168 (1999)

(4) 羽下哲司，ほか：首振り，ズームカメラを用いたトラッキング型侵入監視システム，信学会PRMU研究会資料，PRMU99-67，23～30 (1999)

(5) 森田俊彦：局所相関演算による動きの検知と追跡，信学論(D-Ⅱ)，**J84-D-Ⅱ**，No.2，299～309 (2001)

不審者検知技術

佐藤和也*
熊野　眞**

Human Search Technology for Surveillance Video

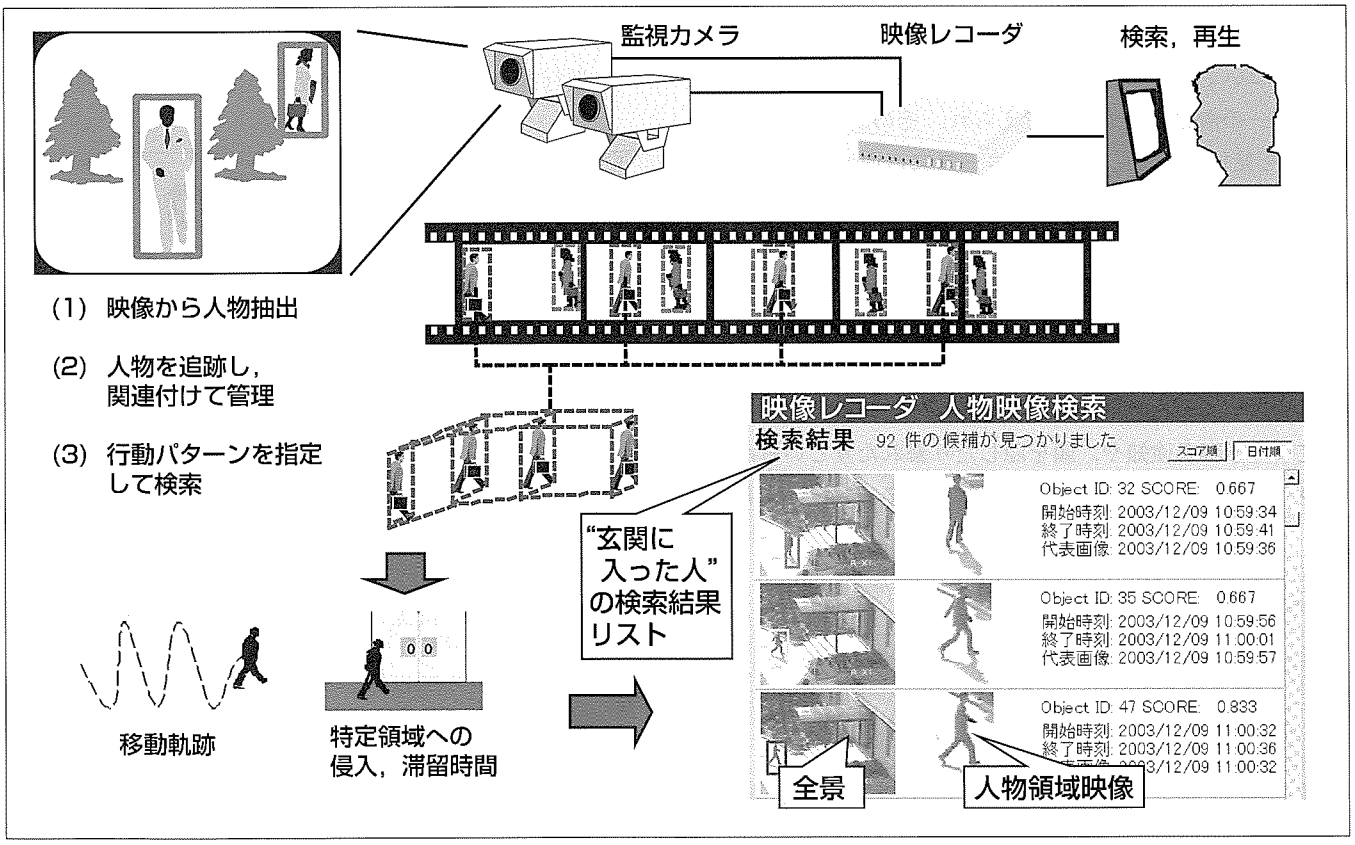
Kazuya Sato, Makoto Kumano

要　旨

近年の社会情勢不安の高まりから，監視カメラや映像レコーダといったセキュリティ用映像装置の需要が高まり，急速に普及してきている。しかし，監視カメラの台数が増え，映像レコーダの記録時間が増大するにつれ，事件や事故があったときに後から映像を見直して所望の場面を探し出すことはかえって困難になってきている。

このような状況において長時間の記録映像を効率的に調査するための手段の一つとして，特定の行動をとった人物の映像を検索する技術を開発した。セキュリティ用途で記録映像を後から見直したい場面とは，“不審者が映っている部分”というのが一般的なニーズと考えられる。不審者の定義には幾つかの段階があるが，本稿では，監視カメラがとらえた人物の行動パターンをベースにした不審者というアプローチについて述べる。

監視カメラの映像を解析し，動きのある人物領域の検出・追跡を行い，その人物の行動に関する特徴量をメタデータとして人物単位に保持し，この特徴量データに対して指定した条件に合う人物の検索を高速に行う。今回，この技術の機能検証として，建物の玄関前を撮影した映像において，“入館者”“徘徊(はいかい)者”“芝生侵入者”といった特定行動を定義し，検索機能の動作を確認した。この技術は，映像レコーダの事後解析として利用できるほか，リアルタイム映像監視システムにおける不審者早期発見のような目的にも利用することが可能である。



映像から人物を抽出し特定行動パターンにより検索

監視カメラ映像の中から人物領域を抽出し，抽出領域の追跡を行った結果を一つの“人物オブジェクト”として管理する。その際に抽出された各人物オブジェクト単位の動きに関する特徴量をメタデータとして保持し，この特徴量データに対して人物の行動の特徴を指定して検索を行う。人物の進行方向，速さ，特定領域での滞留時間，指定場所の通過有無などをキーとした検索機能の検証を行った。

*先端技術総合研究所　**京都製作所

1. まえがき

近年，監視カメラや映像レコーダといったセキュリティ用映像装置の需要が高まり，急速に普及してきている。また，映像レコーダの記憶容量は増加の一途をたどり，例えば三菱電機製の映像レコーダでは，標準画質・24時間毎秒30フレームで記録しても1か月以上記録できる製品も登場している。一方，現状，このような長時間の映像を見るための工夫としては，映像中の指定した領域で何か動きのあった期間だけを記録・再生するといった仕組みが実装されている。しかし，実際事件や事故が起こった後，多数ある監視カメラの長時間記録映像の中から目的の場面を探し出すには，やはり人手によって早送り再生をし続けて見るなどの作業が求められ，非常に時間がかかる上に見逃しという問題も抱えている。

このような状況において，セキュリティシステムとして監視カメラ映像が有効に利用されるためには，映像利用のための更なる工夫が求められる。そこで，映像の中から特定の行動を行った人物のみを検索する技術の開発を行った。これによって，長時間の監視映像の中から目的の場面を効率良く探し出すことが可能となる。

2. 不審者検知概要

2.1 監視映像における不審者とは

セキュリティ用途で記録された映像を後から見直したい場面について考えるとき，まずは“人”が映っているかどうかが第一の着目点であると考えられ，その次には“不審な人物”を見付けてほしいというニーズに直面する。ただし，不審という言葉の定義は難しく，当然撮影されている対象やカメラの画角等によって要求内容も異なってくる。

そこでまず，不審者を見付けるという目的で映像を用いる場合の要求を図1のような複数の段階に分類して考えた。ある特定領域への侵入発生を判断する従来の侵入者検知技術を延長し，人物の移動というレベルでの行動パターンを指定した不審者検知や，顔を隠したり暴れたりといった身体の部分的な動きというレベルの行動パターンでの不審者検知，又は顔情報を基にした個人認証，といったようなカテゴリーが考えられる。

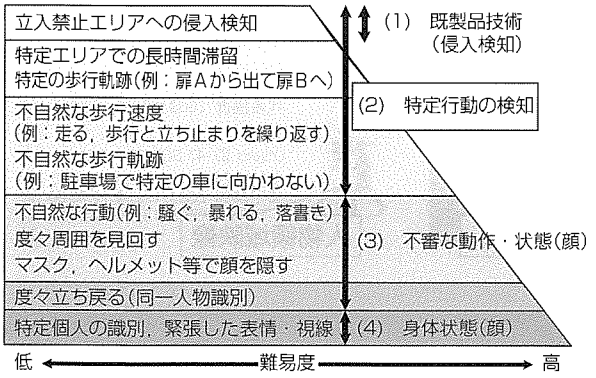


図1．不審者検知技術のカテゴリー

このうち本稿では，人物の移動というレベルでの特定行動をとった人物を検索するというアプローチに関して以下に述べる。これは，監視対象としてカメラの画角で考えると，人物の身体全体が比較的よく映り，移動の様子が分かりやすいような場合が主な対象となる。例えば，図2の左側のように玄関に通じる道路上を撮影した映像の場合，こちらに向かってくる来所者か，向こうに立ち去る退所者か，又はうろうろと滞留している徘徊者か，といった検索方法が考えられる。

一方，人物が大きく映るようなカメラ画角の場合には，これとは別に身体の詳細な状態を調べたり，顔情報から人物の個人特定を要求したりといったアプローチが考えられる。図2の右側の例のように，検出された顔が登録された人物のものであるかどうかの認証を行う，といった具合である。これら各々のアプローチに関しては，現在はまだそれぞれ個別に開発を進めているが，今後は，相互に補完し合ったり連動させたりすることによって，より高度な検索が可能となる。

2.2 特定行動による不審者検知

本稿で述べる特定行動検索の例として，以下に示すような行動パターンを取り上げる(図3)。

(1) 指定した領域における出現や消失
(例：窓や非常口など通常は通行しない所)
(2) 進行方向，経路，指定位置での指定方向への通過

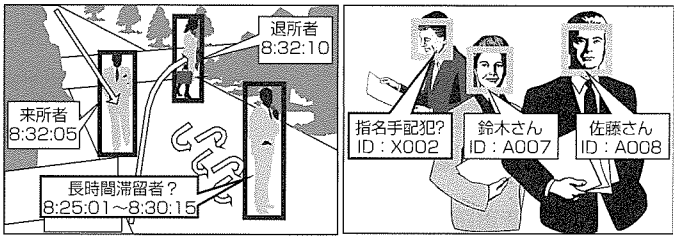


図2．移動情報による不審者と顔情報による不審者

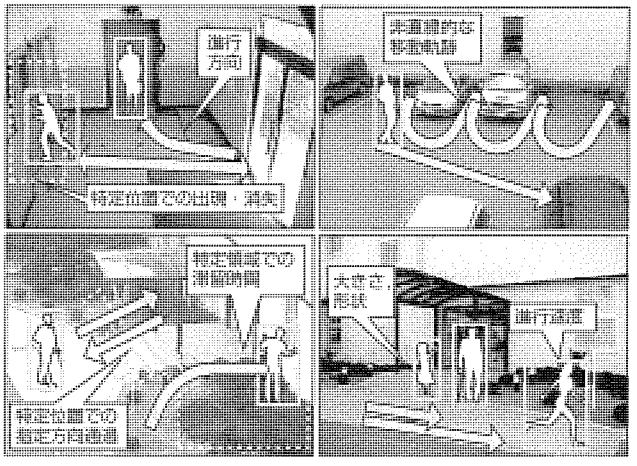


図3．人物の特定行動検索例

（例：特定の場所へ向かう，特定の領域への出入り，一方通行を逆行する，規定の通路と異なる経路を通る，など）

(3) 指定領域での滞留時間
（例：通常の行動では不自然な長時間滞留）

(4) 移動軌跡
（例：駐車場で特定の車へ向かわずうろうろ徘徊）

(5) その他，大きさや速さなど
（例：大人と子供，バイクや車，といったその監視場所特有の検索条件として反映）

3. 特定行動パターンによる人物映像検索技術

3.1 人物領域の抽出と追跡

特定行動による人物検索を行うためには，まず映像を解析して人物領域を抽出し，追跡を行う必要がある。この解析処理については様々な手法があるが，今回の検証では，背景差分によって移動体を識別する方法を用いた[1]。

1枚の背景画像と現在の画像フレームとの違いを分析し，1画素ごとに輝度値の差が所定の閾(いき)値を超えるかどうかによって変化領域を判定して画面全体を2値化する。そして，変化領域の大きさや形状，前後のフレームと比較した動きの連続性などを基に，人物領域かどうか判定する(図4)。

また，その際，画素ごとに過去一定時間における輝度値の平均と分散を計算し，輝度値の細かな変化が多すぎる場合は抽出の感度を落とし，また，動的に背景画像を更新するという調整を行う。その結果，屋外のような木の葉の揺れや日照変動が起きるなど背景変動の多い環境でも，余計な背景変動を人物と間違えて検出することなく人物領域を検出することが可能となった。

また，抽出した人物領域について面積及び重心位置の次の値を予測しながら追跡を行うことにより，同時に複数の人物がいて画面上で一時的に重なりが生じるような環境でも正確な追跡が実現できる(図5)。

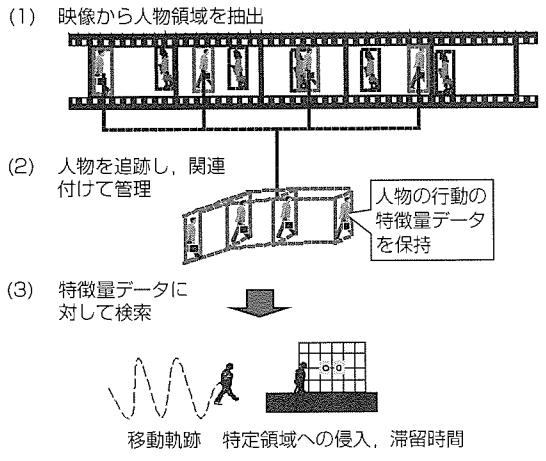


図4．特定行動検索処理の流れ

3.2 人物単位の特徴量管理

ここで，抽出した人物領域の位置変動を前後のフレームにわたって追跡した結果を一つに関連付けるが，この関連付けられた複数の映像領域は同一人物の連続した動きと考えられる。このため，この関連付けられたものを“人物オブジェクト”として情報の管理単位とし，この人物の行動に関する特徴量をメタデータとして作成し，映像データとは別途管理する(図6)。

また，ユーザーによる検索実行の際には，映像フレーム単位のデータを参照するのではなくこの人物単位のメタデータに対して検索を行うため，高速な検索が可能となる。

この特徴量データの内容は前述のような特定行動検索を実現するものであり，図7にその一例を示す。

3.3 動作検証例

今回開発した技術の検証について以下に述べる。人物領域を抽出・追跡し特徴量データを抽出する解析処理機能と，条件を指定して検索処理を行う機能のそれぞれについて，映像を録画するレコーダ機能とは分離して評価するため，既に録画済みの映像データをパソコン上にオフラインで用意して動作確認を行った。

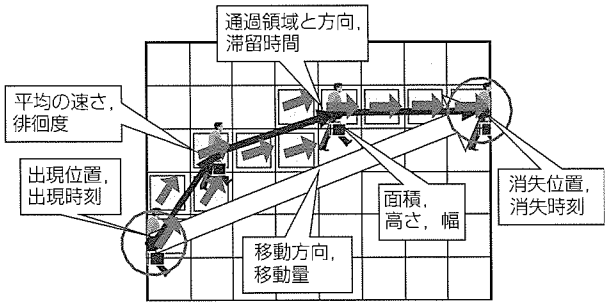


図5．人物の行動に関する特徴量データの一例

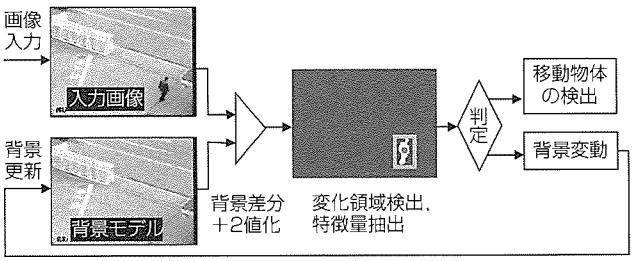


図6．人物領域の抽出

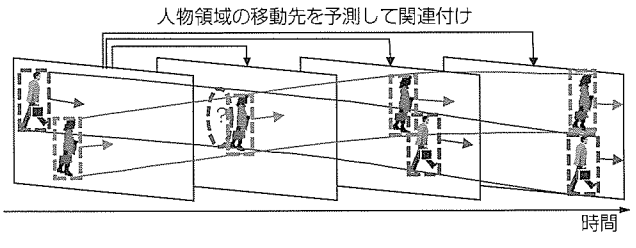


図7．人物領域の追跡

検索条件をユーザーが指定する方法については，前述の特徴量データに定義されたパラメータそれぞれに対して値の上限と下限などを指定し，これらの条件を論理積と論理和で組み合わせることにより，撮影された映像に合った行動パターンを定義できるようにした。具体的には，実際の玄関前の映像を用いて，“入館者：玄関方向に進行して玄関位置で消失した人物”“徘徊者：非直線的な移動を長時間行った人物”“芝生侵入者：芝生の領域に長時間滞留した人物”といった条件の行動パターンで人物の検索を行った。

図8は徘徊者の検索結果の表示例である。検索結果として，うろうろと歩いている人物の移動軌跡情報を示した候補8件がリストされた画面の一部と，そのうち一人の人物を個別に指定したときの映像再生画面例を並べてある。

Pentium-4(3.2GHz)のパソコンを用いて検証を行ったところ，映像解析処理は，入力映像に対してほぼリアルタイムに動作した。また，検索機能については，約4時間で900人が映っている映像の中から任意の条件で検索を行ったが，いずれも1秒以内に結果を得ることができた。検索結果の精度については映像中から人物領域を追跡する解析精度に大きく依存するため，大勢の人物が同時に登場する場合などの厳しい条件に対する性能向上などの課題は残されているが，基本的な機能の検証は行うことができた。

3.4 システム適用例

この技術を実際に適用する方法としては大きく二つ考えられる。一つは，本稿の冒頭で述べたように既に記録された監視カメラ映像の事後解析として利用する方法である。これは，レコーダ本体や検索用の専用機器に映像解析機能を実装し，前節で例示したようにユーザーが事後に条件を与えて検索を行う。所望の結果が得られなかった場合にはまた，別の角度から検索条件を与え直してみるなど，様々に条件を変えての再検索や絞り込み検索が可能である(図9の(a))。

別の適用方法として，あらかじめ調べたい人物（不審者）の条件が幾つか決まっているような場合には，映像の記録実施の有無とは別にリアルタイムに条件照合を行う方法も考えられる(図9の(b))。この場合，映像解析の機能を監視カメラ部に実装するか，カメラからのライブ映像を入力する側で常に映像解析処理を行っておくかが必要だが，条件に合った行動をとった人物を検知すると，即座に警報を鳴らしたり，該当カメラに監視員のモニタを切り換えたりといった対応が可能である。これは，多数のカメラ映像を少

図8．検索結果の表示例

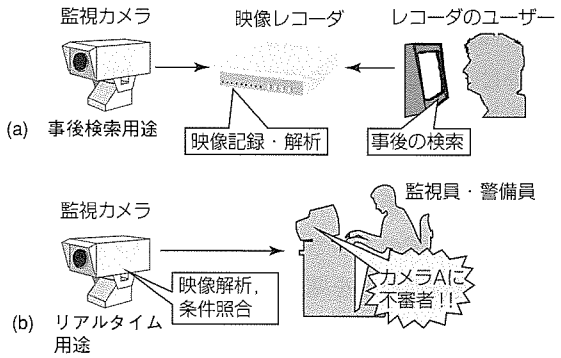


図9．システム適用例

人数で監視する必要のあるリアルタイム映像監視システムにおいて有効な機能である。

4. むすび

特定行動を行った人物の映像を検索することにより監視映像の中から不審者を検索する技術について紹介した。これにより，映像レコーダやリアルタイム映像監視システムの更なる高度化利用が期待される。今後は，検索精度のより一層の向上や，今回の開発アプローチとは異なる顔認証技術による不審者検知などとの連携について，更に検討を進めていく。

参考文献

(1) 羽下哲司，ほか：背景差分と動きベクトル解析を用いた屋外侵入監視システム，第8回画像センシングシンポジウム講演論文集，7～12（2002）

映像蓄積・検索・表示技術

秦　淑彦*　高橋浩一+
近藤純司**　安部　毅++
西川博文***

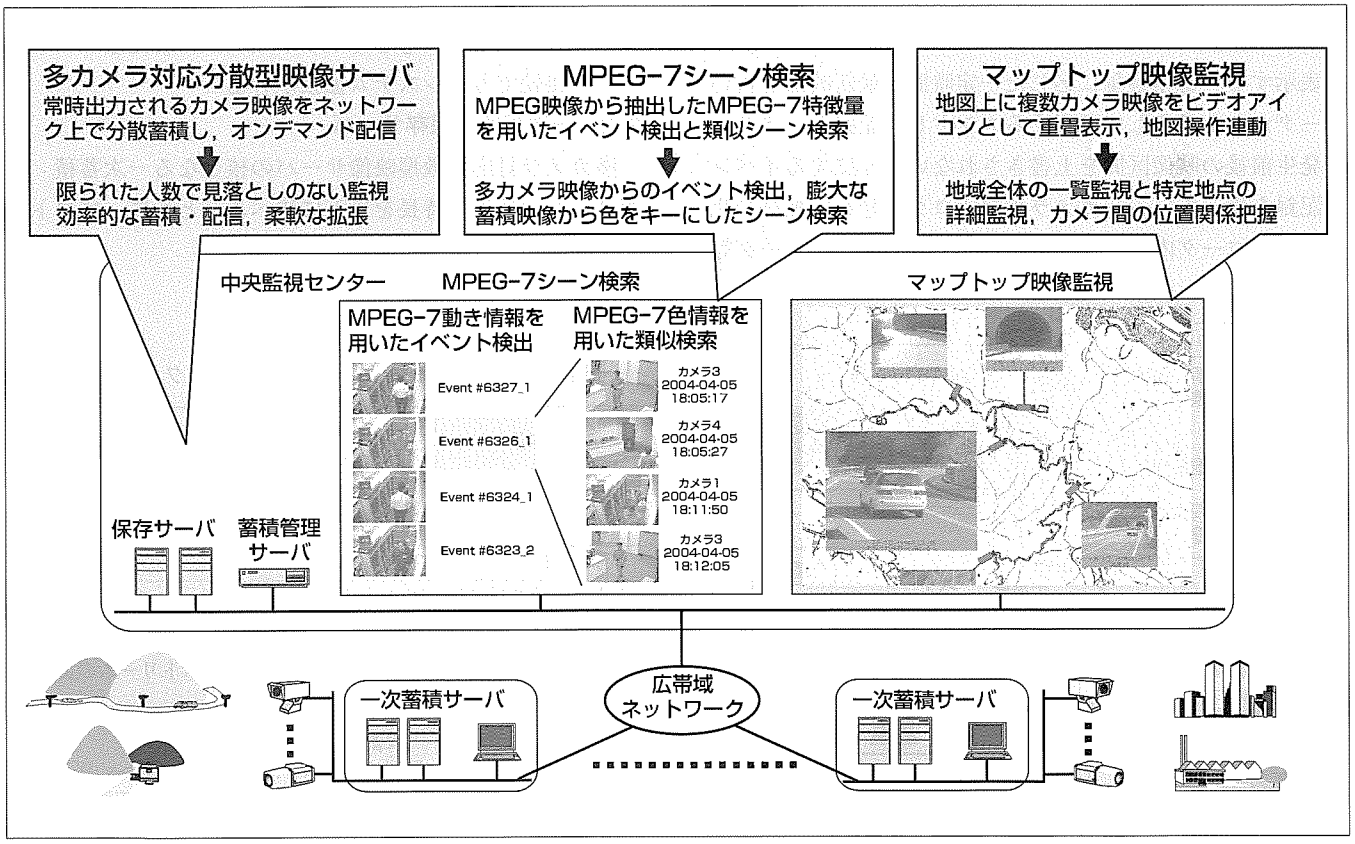
Storage, Retrieval and Display Technology of Surveillance Video

Toshihiko Hata, Junji Kondou, Hirofumi Nishikawa, Kouichi Takahashi, Tuyoshi Abe

要　旨

広帯域ネットワークの普及やデジタル映像監視機器の低価格化に伴い，監視領域をきめ細かく観察するためにカメラの接続台数が増加している。道路・河川や大規模ビルなど数百台のカメラを備える多カメラ監視において，マトリックス表示される複数カメラの映像を監視員が常時目視する従来の監視スタイルでは，限られた人員で重要な事象を見落とすことなく的確に状況把握することができない。これを解決するには，全カメラの映像をいつでも直ぐに見直すための蓄積機能，膨大な蓄積映像から必要なシーンを素早く取り出す検索機能，カメラの撮影範囲や周囲の地理的情報を把握するための表示機能を監視システムが提供しなければならない。

三菱電機は，いち早く多カメラ監視対応の映像蓄積・検索・表示技術の開発を行い，実用化への展開を図っている。多カメラ映像サーバはカメラ映像を常にネットワーク上で分散蓄積しオンデマンド配信するものであり，柔軟なシステム構築，サーバ一台で複数映像の同時蓄積・配信等の特長を持ち，既に製品適用の実績がある。MPEG-7(Moving Picture Experts Group phase 7)シーン検索はMPEG符号化された映像からMPEG-7特徴量を抽出し，イベント検出による監視員の負担低減や蓄積映像からの類似シーン検索を容易にする。マップトップ映像監視は，地図やフロア図面上にビデオアイコンと称する監視映像を複数表示するユーザーインタフェースであり，監視領域全体の様子や複数映像の位置関係を直感的に把握することができる。



多カメラ監視システム

広域映像監視や大規模ビル監視など数百台のカメラを備える多カメラ監視システムであり，多数のカメラ映像をネットワーク上で分散蓄積する多カメラ対応分散型映像サーバ，画像特徴量から類似シーンを検索するMPEG-7シーン検索，地図上に複数のビデオアイコンを表示するマップトップ映像監視により，限られた人員でも重要シーンを見落とすことなく迅速的確な状況把握を可能にする。

*先端技術総合研究所(工博)　**同研究所　***情報技術総合研究所　+電力・社会システム事業所　++郡山製作所

1. まえがき

広域監視や大規模ビル監視では，多カメラ化が急速に進んでいる。このような多カメラ監視において，映像スイッチャと多画面合成器により順次切り換えられる複数カメラの映像を監視員が常時目視する従来の監視スタイルでは対応できず，限られた人員で重要なシーンを見落とすことなく的確に状況把握できる環境を提供しなければならない。

本稿では，この多カメラ化に対応した技術として当社が開発している，多数のカメラ映像をネットワーク上で分散蓄積する多カメラ対応分散型映像サーバ[1]，画像特徴量から類似したシーン検索を行うMPEG-7シーン検索[2]，地図上に複数のビデオアイコンを表示するマップトップ映像監視[3]について，構成，特徴的な機能と実現技術について述べる。

2. 多カメラ対応分散型映像サーバ

2.1 システムアーキテクチャ

多カメラ対応分散型映像サーバのプロトタイプは以下の要素から構成される(図1)。

(1) 一次蓄積サーバ

最新のカメラ映像を，常時，実時間でハードディスクに記録し，ユーザーの指示やセンサのアラーム発生に従い，必要な映像区間を読み出し，表示端末にストリーム伝送して表示する。蓄積容量に応じた一定時間の最新映像を古いデータから上書きして記録するエンドレス記録と，アラーム発生前後の映像区間を上書きされないようにするイベント記録を備えている。カメラのアナログ信号を圧縮符号化するエンコーダ内蔵タイプと，ネットワークエンコーダ等からマルチキャスト配信される符号化データを受信するタイプがある。

(2) 保存サーバ

一次蓄積サーバに記録された映像の中から重要な映像区間を保存サーバに配信し，長期に保存記録する。

(3) 蓄積管理サーバ

複数の一次蓄積サーバ／保存サーバに記録された映像の所在管理や，撮影時刻やアラームイベント等のメタデータ管理を行い，表示端末からの要求に応じて該当する映像区間の配信を手配する。カメラ番号，撮影時間区間，イベント等の組合せで所望の映像を問い合わせることができる。このように，このシステムは，多数のカメラ映像を常時ネットワーク上で分散蓄積し，必要に応じて蓄積映像を即座に端末に配信・表示する分散蓄積オンデマンド配信のシステムアーキテクチャを採用しており，以下の特長を持っている。

- 常時すべてのカメラ映像を記録し直ぐに再生できるため，限られた人数でも見落としのない監視が可能
- 上記3種の記録と，複数カメラのサーバ共有により，有限の蓄積容量で効率的な記録を実現
- 一次蓄積サーバをカメラ側に，保存サーバをセンター側に配置することにより，重要な映像データのみ配信してネットワーク負荷を低減
- カメラ増設に応じてネットワークに新たなサーバを接続でき，システム拡張が容易

2.2 一次蓄積／保存サーバ

多カメラ対応分散型映像サーバの核となる一次蓄積／保存サーバの技術的特長を以下に述べるとともに，プロトタイプの仕様を表1に示す。

(1) 映像ストリーム記録

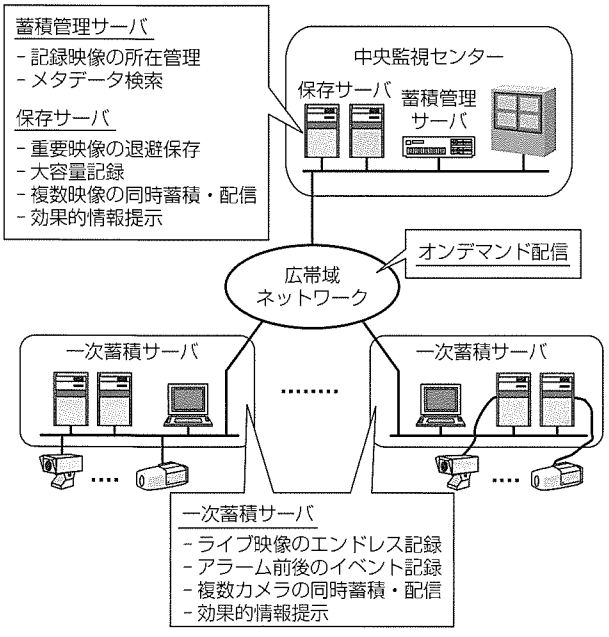


図1．システムアーキテクチャ

表1．一次蓄積／保存サーバ(ネットワーク入力)の仕様

ハードウェア	本体	Pentium4 2GHz，512Mバイトメモリ，Windows 2000
	ストレージ	Ultra ATA 133ハードディスク
	ネットワーク	100Base-T
プロトコル	映像制御	RTSP準拠
	映像送受信	RTP／UDPユニキャスト／マルチキャスト
映像ストリーム	符号化	MPEG-2，Motion JPEG
	性能	MPEG-2 6Mbps 同時8ストリームの蓄積・配信
機能	記録	一次蓄積：エンドレス，イベント 保存：退避保存，外部メディアへの保存
	検索	カメラ番号，撮影時刻，イベント種別＆番号
	配信	標準再生，早送り等の特殊再生，TCP／IPによる退避転送
	その他	時刻合わせ

RTSP：Real Time Streaming Protocol, RTP／UDP：Real Time Transport Protocol／User Datagram Protocol, TCP／IP：Transmission Control Protocol／Internet Protocol

- メモリとハードディスクを合わせた巨大なリング構造の記録領域を構成してエンドレス記録を行うとともに，上書き禁止フラグによりイベント記録時のデータコピーが不要
- 最適なアクセスサイズや読み出しキャッシュ機構によりディスクアクセス性能を向上させ，通常のパソコンを用いて，同時に複数の映像ストリームの記録・配信を実現（Pentium4 2 GHz，6 MbpsのMPEG-2映像を8本）
- MPEG-2とMotion JPEG（Joint Photographic Experts Group）各々のデータ構造に適したサーバ設定を行い，異種ストリームの混在記録を実現

(2) 情報提示

- 高速再生や逆再生等の特殊再生に加え，監視に有効な追い駆け再生（蓄積映像高速再生中に現在時刻に到達すれば標準再生に切換え）を実装
- 撮影時刻やカメラの撮影範囲を映像ストリームと同期して蓄積・配信することにより，再生時に撮影時刻を同期表示，撮影時刻に基づく複数カメラの同期再生，ライブと過去の同時再生，地図上に撮影範囲を連動表示，を実現

当社は，業界でいち早く分散蓄積オンデマンド配信アーキテクチャを提唱し，上記プロトタイプをベースに映像サーバを製品開発し，広域映像監視や大規模ビル監視に実適用している[4]。

3. MPEG-7特徴量を利用したシーン検索

多カメラ監視において，監視映像が含まれるMPEG-4ストリーム中から少ない演算量で高速に算出可能なMPEG-7特徴量を利用することにより，イベントの自動検出による監視業務の負担軽減，大量の蓄積映像からの類似シーン検索を可能にするシステムを開発した。このシステムの特長・ねらいを以下に示す。

- MPEG-7動き特徴量（Motion Activity）を使用した映像再生時の速度制御による蓄積映像閲覧業務の効率化
- MPEG-7動き特徴量を使用したイベントの自動検出による長時間にわたる多カメラ監視業務の負担軽減
- 検出したイベントの時刻，シーンを代表するサムネイル画像，MPEG-7色特徴量（Dominant Color）を抽出し，一覧表示することによるイベント処理の簡易化
- MPEG-7色特徴量を用いた類似シーン検索による映像検索の高速化と簡易化

このシステムは，監視映像をMPEG-4符号化しネットワークに送信する映像送信装置，MPEG-4ストリーム中から動きベクトルに基づくイベント検出とイベントに関連するMPEG-7特徴量の蓄積を行うイベント検出・蓄積サーバ，映像送信装置の出力するストリームを保存し要求に応じて配信する映像蓄積・配信サーバ，及びMPEG-7動き・色特徴量に基づく映像検索を行う監視端末とから構成される（図2）。

以下，実現する機能とその詳細を示す。

(1) MPEG-7動き特徴量を用いた映像再生速度制御とイベント検出

動画像における動きの激しさ，動きの向き，時空間領域での動きの分布などをコンパクトに記述するMPEG-7動き特徴量を，MPEG-4ストリームに含まれる動きベクトルから生成する。主としてこの特徴量中の動きの激しさに基づき，監視するべき情報が含まれていると判断されるシーンでは通常速度での再生を行い，それ以外のシーンでは早送りを行う（図3）ことが可能になる。これは，システムが優先度の低いシーンを自動的に判断し早送りすることであり，蓄積映像の閲覧時間を短縮する効果をもたらす。

さらに，ライブ系において上記の判断結果を時刻やサムネイル画像と併せて保存することにより，監視映像中に発生したイベント一覧を生成することも容易になる。

(2) MPEG-7色特徴量を用いた類似シーン検索

上記(1)で特定されたイベントが含まれる映像の動領域を特定し，その領域に含まれる数個の代表色とその頻度を求め，MPEG-7色特徴量として記述する。過去に抽出されたMPEG-7色特徴量とのマッチングにより，過去に蓄積された膨大な映像からの類似シーン検索を可能とする。

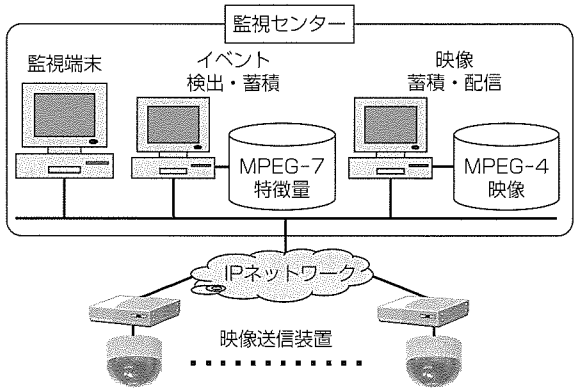


図2．システム構成

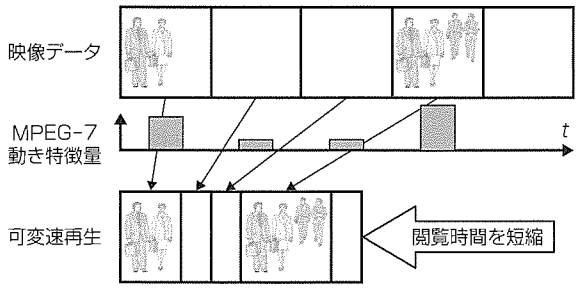


図3．動き特徴量による再生速度制御

表2．マップトップ映像監視の機能と効果

機能		効果
ビデオアイコン重畳表示	－カメラ位置を示すカメラアイコンとカメラ映像を表示するビデオアイコンを地図上に重畳表示 －カメラアイコンが撮影方向と画角をアニメーション表示 －カメラアイコンを用いてカメラの遠隔操作	－監視領域全体の様子を一目で把握(マクロ監視) －カメラ間の位置関係の直感的把握 －カメラ制御の遅延にも対応できる容易なカメラ操作
地図操作連動	－地図のスクロールや拡大縮小に追従してビデオアイコンとカメラアイコンが自動的に移動 －選択したビデオアイコンを常時同じ位置に表示可能 －地図縮尺に基づきビデオアイコンの表示を階層管理し，表示縮尺に合わせてカメラの表示数を制限	－空間探索や空間解析に適した地図操作と連続性のあるユーザーインタフェースであり，多カメラ及び他の収集データの検索・表示を容易にする(共通の作業基盤) －カメラ数が増加しても映像及び地図の見やすさを確保
ビデオアイコン選択表示	－撮影対象とその属性(例えばトンネルや交差点)に応じてビデオアイコンを選択的に表示 －地図上のマウス位置近傍にあるビデオアイコンを表示	－監視目的に応じたカメラ選択と見やすさの確保
重要度に基づく映像品質変更	－重要度の高い映像は高品質(高解像度，高フレームレート)，その他は低品質で配信・表示 －素早く視覚的に滑らかに映像品質を切換え	－伝送帯域と表示端末での画像復号・表示処理を低減し，限られたシステム資源で多カメラ表示を実現 －全体の概略監視と注目地点の詳細監視を実現
イベント連動	－各種センサのアラームに連動して地図の表示位置や縮尺を変更し，異常発生地点周辺を自動的に表示	－ビデオアイコンの階層管理や選択表示と組み合わせて，カメラ数が増加しても監視員の負担を軽減

従来システムでの日時やカメラ番号だけをキーとする検索に対して，色をキーとする検索を加えることで，より高度なシーン検索が提供可能となる。

4. マップトップ映像監視

多カメラ監視ユーザーインタフェースとして，ガメラ映像を表示するビデオアイコンを地図上に重畳表示し，映像と地図情報を連動するマップトップ映像監視を提案している(**図4**)。機能と効果を**表2**に示し，特長を以下に述べる。

- 点から面の監視：カメラが設置された監視スポットのみを観察する“点の監視”に加え，複数カメラが設置された空間全体の概略監視や隣接するカメラの位置関係の把握など“面の監視”を実現
- 広域監視の共通基盤：交通流や雨量等の計測データ，設備図面や保守データ，監視映像を相互に関連付けて効率的に監視業務を行うための共通のユーザーインタフェース基盤を提供
- 低コストで実現：重要度の高い映像は高品質(高解像度，高フレームレート)，他の映像は低品質で配信・表示することにより，ネットワークや表示端末など限られたシステム資源で多カメラ表示を実現

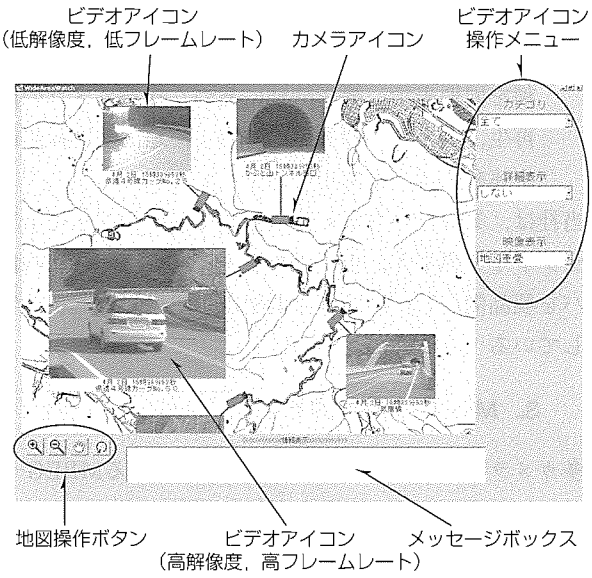


図4．マップトップ映像監視の画面例

5. むすび

本稿では，当社が開発している多カメラ対応分散型映像サーバ，MPEG-7シーン検索，マップトップ映像監視について紹介した。今後は，更なる機能・性能向上を実現するとともに，実適用への拡大を図っていく所存である。

参考文献

(1) 秦　淑彦，ほか：分散型履歴映像データの効果的検索・再生方式と実装，電子情報通信学会論文誌，**J82-D-I**，No.1，234～246（1999）
(2) 井須芳美，ほか：MPEG-21メタデータアダプテーションヒントの提案(1)～映像監視システムへの応用～，電子情報通信学会2003年総合大会，D-11-79（2003）
(3) Kuwahara, N., et al.：Map-Top Video Surveillance with Adaptive Video Delivery, World Multi-Conference on Systemics, Cybernetics and Informatics (ISAS-SCI)（2002）
(4) 坂下龍司，ほか：イントラネット応用広域監視情報集配信システム，三菱電機技報，**74**，No.2，132～135（2000）

セキュリティ映像配信技術

阿倍博信*
川畑幸保*
上野幾朗*

Security Video Delivering Technologies

Hironobu Abe, Yukiyasu Kawahata, Ikuro Ueno

要　旨

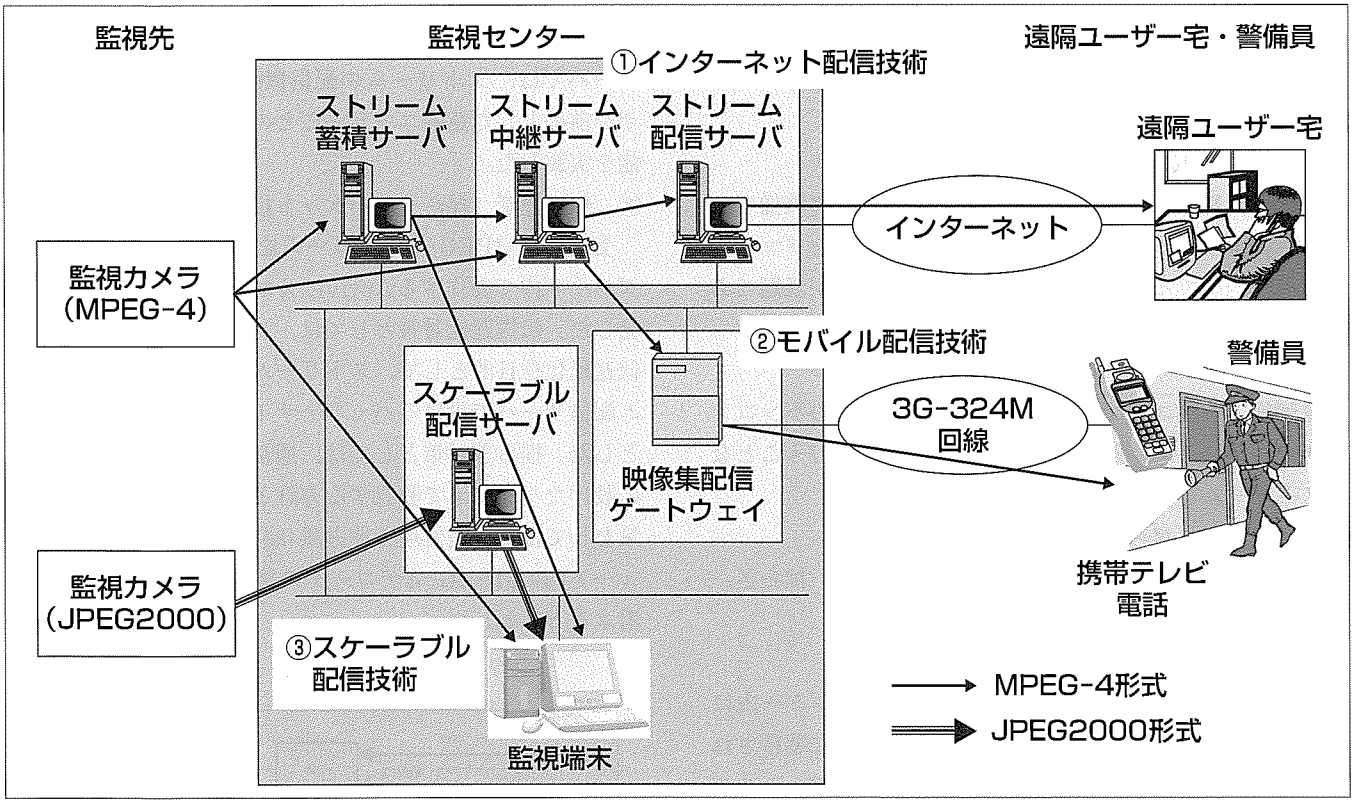
近年のセキュリティ意識の高まりにより，大規模なビルから小型の公共・商業施設や家庭にも多数の監視カメラが設置されつつある。さらには，撮影した映像データを通信ネットワーク経由で監視センターに伝送し，必要に応じて監視員が対応する遠隔監視システムが期待されている。

本稿では，この遠隔監視システムの差別化機能として，業務効率化を目的として遠隔ユーザーや警備員等に映像データをインターネットや携帯電話網等を介して配信する機能や，監視端末の表示性能に合わせて階層的(スケーラブル)に配信する機能の実現に必要な技術について述べる。

インターネット配信技術は，監視センターからインターネット経由で映像データを遠隔ユーザー等のパソコンに配信する技術である。本稿では，ファイアウォール越えのストリーム中継，Webブラウザを利用した閲覧，伝送遅延，揺らぎ，パケット損失などの技術課題に対する対策について述べる。

モバイル配信技術は，監視センターから携帯電話網経由で警備員の携帯テレビ電話に映像データを配信する技術である。本稿では，伝送プロトコルや制御プロトコルの違いなどの技術課題に対する対策について述べる。

スケーラブル配信技術は，監視センターから映像データを端末の表示性能に合わせてスケーラブルに配信する技術である。本稿では，端末の性能に応じた効率的なデータ伝送，端末，配信サーバの処理負荷軽減などの技術課題に対する対策について述べる。



セキュリティ映像配信技術のモデルシステム概要

①のインターネット配信技術は，監視センターに伝送されたMPEG-4(Moving Picture Experts Group Pase4)形式等の映像データをインターネット経由で遠隔ユーザーのパソコンに配信する技術である。

②のモバイル配信技術は，監視センターに伝送されたMPEG-4形式等の映像データを携帯電話網経由で警備員の持つ携帯テレビ電話に配信する技術である。

③のスケーラブル配信技術は，監視センターに伝送されたJPEG2000(Joint Photographic Experts Group 2000)形式の映像データを端末の表示性能に合わせて最適化して配信する技術である。

*情報技術総合研究所

1. まえがき

近年のセキュリティ意識の高まりにより，大規模なビル，小規模な店舗や家庭などに監視カメラを設置し，監視カメラで撮影した映像データをネットワーク回線などで監視センターに伝送し，必要に応じて監視員が対応する遠隔監視システムが期待されている。

この遠隔監視システムの差別化機能として，監視センターに伝送された映像データをインターネットや携帯電話網などを介して監視対象の遠隔ユーザーや現場に急行する警備員などに中継・配信するサービスや，センター内の監視端末に効率的に配信する機能の実現が求められている。

本稿では，このセキュリティ映像配信サービスの実現に必要な基盤技術として研究・開発を行っているインターネット配信技術，モバイル配信技術，スケーラブル配信技術について述べる。映像形式としては，インターネット配信技術とモバイル配信技術はMPEG-4[1]を，スケーラブル配信技術はJPEG2000[2]を扱う。

2. インターネット配信技術

この章では，遠隔地にいる遠隔ユーザーが監視センターからインターネットを経由してライブ配信又は蓄積されたMPEG-4形式の映像ストリームを配信・閲覧する技術に関して，課題と三菱電機の取り組み，今後の展望について述べる。

2.1 課　題

(1) ファイアウォール越えのストリーム中継

通常，監視センター内で配信されているライブ映像やストリーム蓄積サーバに蓄積されている蓄積映像をファイアウォール経由でインターネットに配信することが課題である。

(2) Webブラウザを利用した閲覧

遠隔地の遠隔ユーザーの使用する端末は通常のパソコンを想定しており，特殊なソフトウェアの追加を行うことなくストリームを閲覧したいという要求がある。

(3) 伝送遅延，揺らぎ，パケット損失

インターネット回線の特徴として，伝送遅延，揺らぎ，パケット損失の発生などの課題がある。

2.2 取り組み

前節で設定した課題を考慮する形で，監視センター内に集信されたライブ映像やストリーム蓄積サーバに蓄積された蓄積映像をインターネット経由で配信するモデルシステムを構築した。**図1**にこのモデルシステムの構成について示す。

以下，図に従い，このモデルシステムにおける当社の取り組みについて述べる。

(1) ストリーム中継機能

インターネットからの不正アクセスの防止を目的としてファイアウォールを設置して，監視センター内にDMZ(DeMilitarized Zone)を構築した。そして，監視センター内にストリーム中継サーバを置き，センター内DMZにストリーム配信サーバを置くことにより，インターネット経由でセンター内のサーバに直接アクセスできない方針とした。

ストリーム中継サーバは，①ライブ映像ストリームの宛先(あてさき)変換，②ユーザーから要求のあった蓄積ストリームの制御・配信，の機能を持ち，監視センター内で配信されているライブ映像，又はストリーム蓄積サーバに蓄積されている蓄積映像をファイアウォール経由でストリーム配信サーバに中継する。遠隔ユーザーは，中継されたストリームをインターネット経由でセンター内DMZに設置されたストリーム配信サーバにアクセスして受信する。MPEG-4ストリームの配信プロトコルとしてはRTP(Real-time Transport Protocol)[3]を使用する。

(2) Webコンテンツの自動作成機能

遠隔ユーザー側に設置したパソコンでは，Webブラウザでの閲覧を前提とする。その理由としては，①遠隔ユーザー側では閲覧のための特別なソフトウェアをインストールしたくない，②契約しているサービスの内容が遠隔ユーザーごとに異なるため，遠隔ユーザーごとに画面を自動作成する必要がある，である。開発したストリーム配信サーバでは，ストリームの配信機能以外に，Webブラウザを前提とした遠隔ユーザーごとのコンテンツ自動作成機能を実装した。

(3) 伝送遅延，揺らぎ，パケット損失対策

受信したMPEG-4ストリームを再生するビューアを，ブラウザ内で動作するActive Xコンポーネントとして開発した。伝送遅延対策としては，ライブ映像・蓄積映像の低遅延化を目的として，ストリーム中継サーバ，ストリーム配信サーバで設けるバッファサイズを最低限とする方針とした。揺らぎ対策としては，通常使用されるビューア内に設けたバッファで吸収する方針とした。パケット損失対策としては，再送処理や前方誤り訂正処理は追加せず，ビューア内のMPEG-4デコーダの持つエラー耐性機能を使用する方針とした。

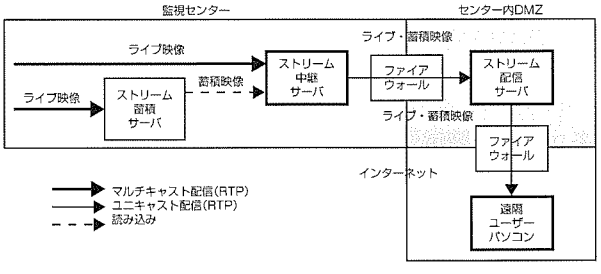


図1．インターネット配信システムの構成

2.3 今後の展望

(1) ストリームの暗号化

インターネット環境でのより安全性の高いセキュリティ映像配信サービスの実現を目指して，ストリームの暗号化機能の実現を行っていく予定である。

(2) HTTPストリーミング機能

オフィスなどのファイアウォールが設置されている遠隔ユーザーへの対応を目指して，RTPストリームのHTTP(HyperText Transfer Protocol)ストリームへの変換機能の実現を行っていく予定である。

3. モバイル配信技術

この章では，3G-324M準拠携帯テレビ電話(以下"携帯テレビ電話"という。)を所持する警備員や外出先の遠隔ユーザーが監視センターからライブ又は蓄積されたMPEG-4形式の映像ストリームの配信，閲覧サービスを実現する技術に関して，課題と当社の取り組み，今後の展望について述べる。

3.1 課　題

監視センター内で扱う映像ストリームは，携帯テレビ電話の通信プロトコルと異なるため，ストリーム配信のための伝送プロトコル及びセンターと携帯テレビ電話間の呼制御，能力交換のための制御プロトコルの変換を行い，携帯テレビ電話へ送出する必要がある。また，監視センター内のIP(Internet Protocol)網と携帯テレビ電話の回線交換網の伝送路特性の相違を考慮する必要がある。

3.2 取り組み

前節で設定した課題を考慮する形で，当社は，既開発のモバイルマルチメディア多地点通信システム[4]の技術を基に，監視センターに集信されたライブ映像や蓄積サーバに蓄積された蓄積映像を携帯テレビ電話に配信するモデルシステムを構築した。図2に，このモデルシステムの構成とプロトコルについて示す。

以下，図に従い，このモデルシステムにおける当社の取り組みについて述べる。なお，監視センター内のストリーム中継機能については，前項の"インターネット配信技術"で述べた技術を適用する。

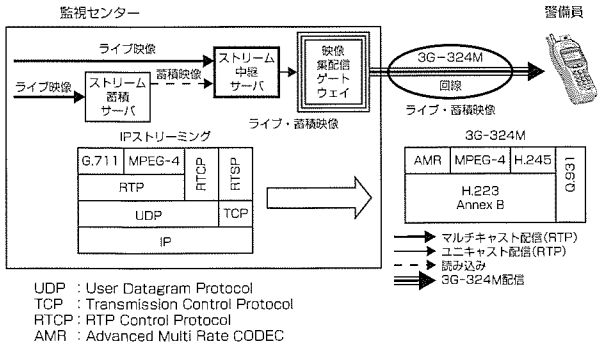


図2．モバイル配信システムの構成

(1) 制御プロトコル変換機能

IP系システムとして構築されている監視センター内では，ライブ及び蓄積映像ストリームの制御プロトコルはRTSP(Real Time Streaming Protocol)等を使用している。それに対し，3G-324Mで規定されている携帯テレビ電話における制御プロトコルにはQ.931及びH.245が使用されている。

この異なる制御プロトコルをリアルタイムに変換する機能，つまり，携帯テレビ電話の制御プロトコルであるQ.931とH.245から監視センターのプロトコルのRTSP等へのプロトコル変換を実現した。なお，携帯テレビ電話では呼制御(Q.931)と端末の能力交換(H.245)が別の制御プロトコルで行われることにより監視センターの制御プロトコルで通知できない携帯テレビ電話の能力情報は，あらかじめセンターで取得する方式を採用している。

(2) 伝送プロトコル変換機能

監視センター側のRTPパケット形式を，携帯テレビ電話側のパケット形式へのメディアフォーマット変換で行う。監視センター内からの複数のRTPペイロードをビデオパケット単位に分割し，H.245で通知された携帯テレビ電話の最大伝送パケット長で再分割し送出を行っている。

このとき，基準クロックの差や伝送路特性の相違による回線遅延や揺らぎに対して，ストリームバッファの状態に従って，データの廃棄や挿入を制御し，クロック差の吸収，及び伝送レートの保証を実現している。

3.3 今後の展望

(1) 携帯テレビ電話から監視センターへの集信

携帯テレビ電話は，その機動性を利用して現場に急行する警備員からの現場状況の報告・記録等に利用できる。この機能を実現するために，携帯テレビ電話から監視センターへの映像ストリームの集信，及び集信されたストリームをメタデータと同期して蓄積を行う技術を開発していく必要がある。

(2) 多地点接続制御

複数の携帯テレビ電話を接続し同一のライブ映像や蓄積映像を確認しながら状況の確認と対策打合せを行うサービスを実現するために，監視映像ストリーム共有型の多地点接続制御機能の開発を行っていく予定である。

4. スケーラブル配信技術

多様化する監視対象への柔軟な対応が求められる中，監視先からの映像を低解像度の携帯端末や高解像ディスプレイ端末など性能の異なる複数の端末に同時配信する要求が高まっている。この章では，このような監視システムの性能，利便性向上に向けての当社の検討について述べる。

4.1 課　題

(1) 端末の性能に応じた効率的なデータ伝送

監視先カメラの解像度よりも低い解像度の端末に映像を伝送する場合，高解像度のまま配信し，端末で高解像度の映像を受信して低解像度に変換した上で表示することが考えられる。これは，端末側で不要な情報まで受信することになり，伝送量の増加につながる。必要な情報のみを伝送して回線の効率的利用を図ることが求められる。

(2) 端末，配信サーバの処理負荷低減

上記の場合，不要な情報を伝送するだけでなく，端末側で必要以上に高い解像度の映像を復号し，更にそれを低解像度に変換するという負荷が生じる。送信側で低解像度に変換した上で符号化し伝送する形態も考えられるが，その場合には，送信側での処理負荷が増大する。端末の要求に応じた符号データを効率的に生成し，端末，送信側の処理負荷を低減することが望まれる。

4.2 取り組み

上記課題に対し，当社は，複数の監視先からの映像をMotion-JPEG2000符号化ストリームとして蓄積し，各符号ストリームから必要な解像度，画質の符号データのみを抽出し配信するスケーラブル配信モデルシステムを開発している。**図3**にモデルシステムの構成図を示す。JPEG2000符号化方式[2]では，**図4**に示すように，画像の低解像成分など，重要な情報から段階的に符号化する方法を採用しており，その符号データの一部を取り出して復号すれば部分的な復号を行うことができる。このような符号化方式をスケーラブル符号化と呼ぶ。これにより，ワンソースをマルチユースに利用すること(単一符号ストリームから異なる解像度，異なる符号化レートの符号データを生成)が可能となる。

以下に，このモデルシステムの特長を紹介する。

(1) 解像度の異なる複数映像を同時配信

複数の監視先からの映像(VGA(Video Graphics Array)：640×480)をJPEG2000スケーラブル符号データとして配信サーバに蓄積し，配信する。監視端末では監視映像のサムネール動画(SQVGA(Super Quarter VGA)：160×120)と特定の拡大映像(VGA：640×480)を複数同時表示する。複数映像はRTPでストリーム配信し，配信制御コマンドにはRTSPを使用している。

(2) 解像度，フレームレート，画質を配信中に変更可能

端末からの指示により，配信中に，映像の解像度，フレームレート，画質をシームレスに変更可能である。

4.3 今後の展望

(1) 伝送エラー耐性強化

イントラ符号化であるMotion-JPEG2000を使ったスケーラブル映像配信では，伝送エラーの影響がフレーム間で伝搬しない，高解像度成分でエラーが発生しても低解像度だけを復号可能などのメリットがある。今後，これらの特長を生かして伝送エラー耐性の強化を図っていく予定である。

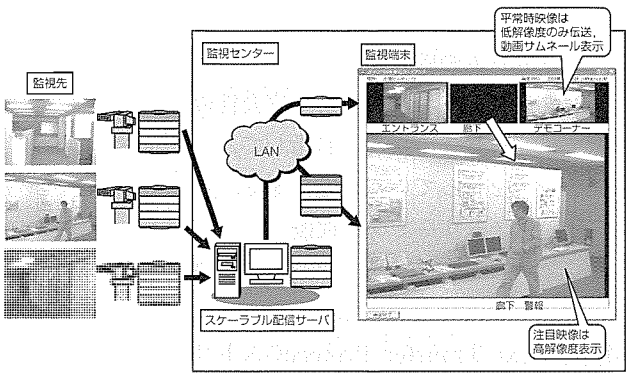


図3．スケーラブル配信システムの構成

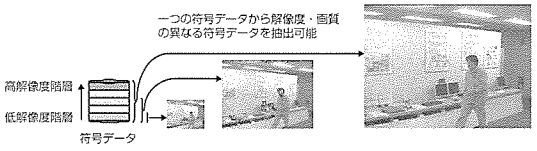


図4．スケーラブル符号化概念図

(2) スケーラビリティ機能の充実

今後，監視映像の高解像度化が進み伝送量が増大するにつれて，端末に応じた情報を伝送するスケーラブル配信の重要性は更に高まると考えられる。現在のモデルシステムでは解像度の変更は2段階のみだが，更に多くの解像度に対応する，指定領域をズームアップして表示するなどスケーラビリティ機能を拡張していく予定である。

5. むすび

以上，監視センターに伝送された映像データを必要に応じて中継・配信する技術に関して，インターネット配信技術，モバイル配信技術，スケーラブル配信技術について述べ，モデルシステムを構築した。有効性について評価を行った後，当社の物理セキュリティ事業に展開していく予定である。

参考文献

(1) ISO／IEC, JTC 1／SC29／WG11 N3536, Overview of the MPEG-4 Standard (2000)

(2) 上野幾朗，ほか：静止画符号化の新国際標準方式(JPEG2000)の概要，映像情報メディア学会誌，**54**，No.2，164～171 (2000)

(3) Schulzrinne, H., et al.：RFC3550-RTP：A Transport Protocol for Real-Time Applications (2003)

(4) 坂井正尚，ほか：モバイルマルチメディア多地点通信システム，三菱電機技報，**78**，No.2，135～138 (2004)

セキュア映像蓄積・検証システム

木村智広*
伊藤　浩**
鈴木光義*

Surveillance Image Storage／Verification System secured by Watermarking Technologies

Tomohiro Kimura, Hiroshi Ito, Mitsuyoshi Suzuki

要　旨

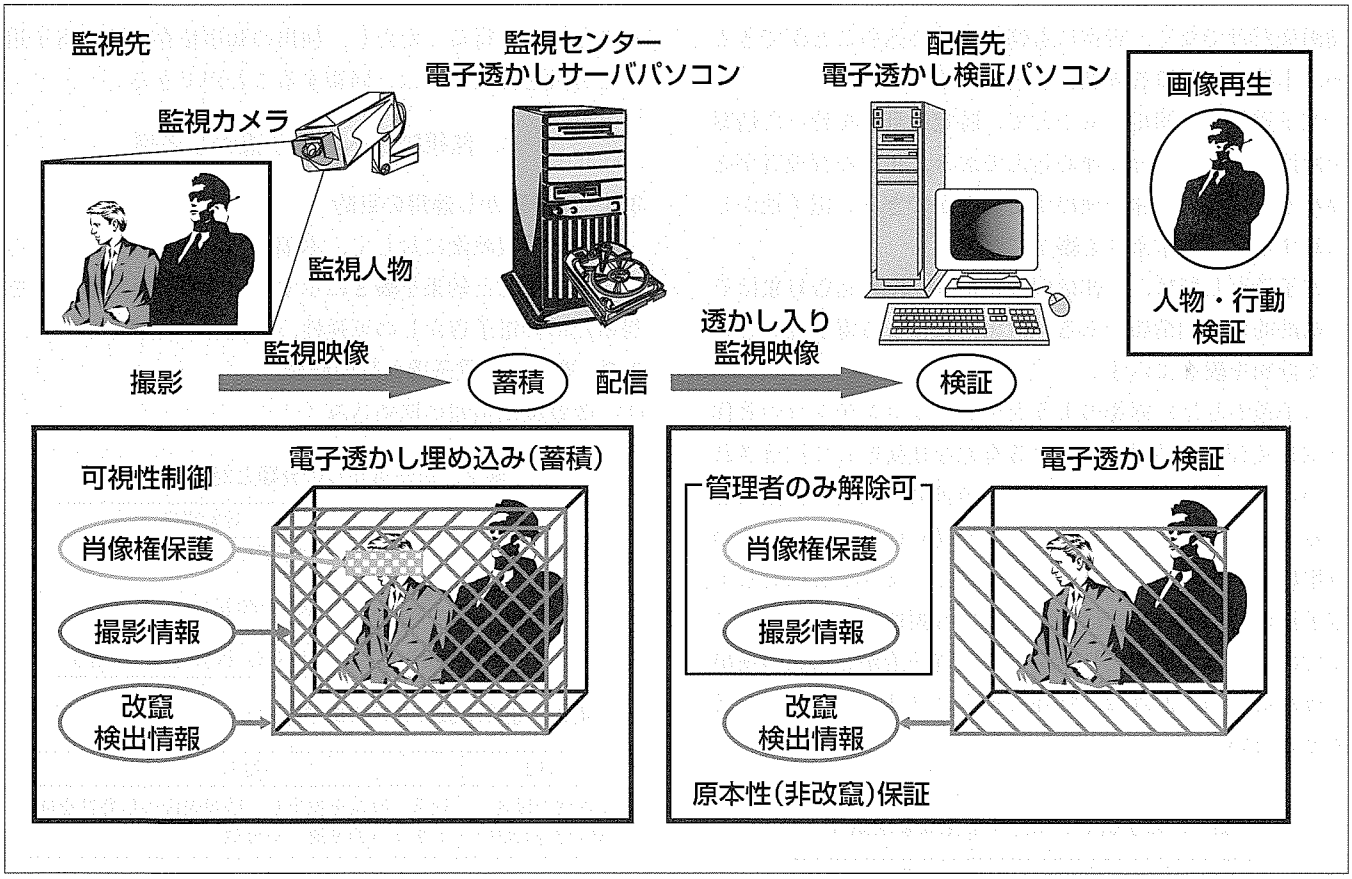
近年，犯罪や不正行為を監視するためのカメラの設置によって，防犯効果を得る一方で，映像に常時撮影されることによる監視対象である当事者以外のプライバシーや肖像権の侵害という問題も挙げられている。また，従来の蓄積映像の解析技術向上以外に，映像の信憑(しんぴょう)性として捏造(ねつぞう)や改竄(かいざん)がないこと(原本性)を保証する技術を早期に確立することが望まれる。

デジタル映像にある種の情報を埋め込んでおき，必要なときにその情報を検出できる技術として電子透かしが知られる。既存の監視システムより高い信憑性に裏付けられた監視映像を得るために，改竄検出情報を埋め込んでおく原本性保証電子透かしを適用したセキュア映像蓄積・検証システムの構築を検討した。

同時に，電子透かしによる監視カメラの撮影情報の付加や，監視対象者を除く人物のプライバシーや肖像権に配慮し，可視性制御を適用した保護を実現する。

検討したシステムは，電子透かしに関する埋め込み処理，検証処理をパソコンベースで実現する構成をとっている。より監視映像の信憑性を向上させるためには，映像がネットワークを介してカメラ外部に出力される前に，原本性保証電子透かしを適用して改竄検出情報を埋め込む機能を内蔵した監視カメラを実現していく必要がある。

本稿では，監視映像に電子透かし技術を適用したセキュア映像蓄積・検証システムの概要を紹介する。



セキュア映像蓄積・検証システムの概念図

電子透かしサーバパソコンにおいて，監視カメラの撮影映像に，原本性保証電子透かしとして改竄検出情報を埋め込んでおく。同時に，撮影情報を埋め込み，監視対象者でない人物のプライバシー及び肖像権を保護するための可視性制御を適用して蓄積し，配信する。電子透かし検証パソコンでは，埋め込まれた撮影情報と可視性制御を管理者のみ知り得る暗号鍵(かぎ)を使用して解除し，検出された改竄検出情報の正誤により改竄有無及び箇所が判定される。

*情報技術総合研究所　**同研究所(情報学博士)

1. まえがき

監視システムの設置によって，防犯が推進される一方で，映像に常時撮影されることによる監視対象である当事者以外のプライバシーや肖像権の侵害という問題も挙げられている。また，監視システムの基盤として，蓄積映像の解析技術以外に，映像に対する信憑性の尺度として捏造や改竄がないこと(原本性)を保証する技術が早期に確立されることが望まれている。

原本性保証を実現する技術の一例として，デジタル映像にある種の情報を埋め込んでおき，必要なときに情報を検出できる電子透かしがある。他の情報の種類・目的に合った電子透かしを組み合わせて監視システムの映像に適用することで，既存システムより高い信憑性に裏付けられた監視映像の運用が可能になる。

本稿では，監視映像に電子透かし技術を適用したセキュア映像蓄積・検証システムの概要と，その背景にある電子透かし技術について紹介する。

2. 電子透かし

電子透かし[(1)(2)]は，デジタル透かし，ウォーターマークなどとも称される。電子透かしの適用対象は，静止画像，動画像だけでなく，音声にも情報を埋め込むことができるが，本稿では対象を画像に限定して述べる。

電子透かしを適用することで，特定の目的を持った情報を画像に一体不可分に埋め込んでおき，正当な管理者が必要なときにその情報を検出することができる。電子透かしに対する主な要求条件を**表1**に示す。

電子透かしでは，主体は画像にあり，埋め込む対象はその補助的な付加情報である。対象情報による電子透かしの主な分類を**表2**に示す。

電子透かしは，画像のようなデジタルコンテンツの著作権主張及び原本性保証における有力な技術として注目されている。一般的なコンテンツ保護の目的では暗号化技術もあるが，電子透かしと暗号化との相違点は，暗号化がその適用により画像の再生を不可能にしてしまうことに対して，電子透かしは情報を埋め込んだ後でも画像再生が可能なままであることにある。したがって，電子透かし情報の検出を行わないのであれば，特殊な再生アプリケーションを必要としない。

表1．電子透かしに対する主な要求条件

(a)画像に一体不可分で埋め込まれていること
(b)埋め込み前後で画質が極端に劣化しないこと
(c)埋め込み前後でデータ量が大きく増加しないこと
(d)埋め込み前後でデータ形式が変化しないこと
(e)正当な管理者は適時検証できること

通常，再生時に画質劣化が知覚できない(不可視型方式)場合が基本であるが，著作権情報などの明示のために意図的に目立たせる場合(可視型方式)もある。電子透かしで埋め込む情報自体又は位置座標の決定には，暗号化やスペクトラル拡散等を適宜導入している。

電子透かしデータの埋め込みの観点から，著作権情報のように多少攻撃されても検出できる強度の強い埋め込みと，原本性保証(真正性証明)情報のように不正な改竄操作をされるとすぐに壊れてしまう強度の弱い埋め込みに分類できる。一般に，強度を強くすると，画質への影響が大きく現れる。

また，埋め込んだ電子透かし情報の解除の可否により，可逆型方式と非可逆型方式に分類される。一般には，電子透かしの要求条件(**表1**)の一つに情報埋め込みがファイルサイズに影響を与えないことが挙げられているが，可逆型方式において，他の情報を持ってきて一部の情報を置換して実現する場合，電子透かしとして埋め込む置換情報が過剰に多くなると，ファイルサイズ増加及び画質劣化という影響が出てしまう可能性がある。原本性保証透かしでは，映像の封印という意味合いから非可逆方式とする。

一つの画像に複数の電子透かしを適用した場合，基本的に検出順序は埋め込みの逆順序となり，その検出前の電子透かしまで解除しておかなければ次の検出が正常にできないこともあり得る。ただし，検出の順序依存のない電子透かし方式を採用すれば，回避することができる。

3. 監視映像への電子透かし応用

3.1 電子透かし適用の目的

従来の監視映像に対して，本稿で紹介する電子透かしを適用する目的と効果を**表3**に示す。同時に，目的の効果を得るための電子透かしの可逆性，可視性の種別を示した。

3.2 適用する電子透かしの詳細

(1) 改竄検出情報の埋め込み[(3)(4)]

表2．電子透かしの分類と対象情報

分類	対象情報
著作権主張電子透かし	著作権者やID等
原本性保証電子透かし (真正性証明電子透かし)	改竄検出情報
メタデータ電子透かし	画像情報，撮影場所，時刻等

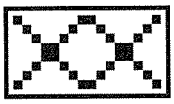
表3．監視映像における電子透かし適用の目的と効果

目的	効果
原本性の保証 (真正性の証明)	捏造，改竄を検出し，監視映像の信憑性を向上する（非可逆・不可視）
撮影状況の保存	映像上に文字として埋め込まないため，文字表示位置，サイズを容易に変更できる (可逆・不可視)
プライバシー・ 肖像権の保護	映像中の指定領域内の可視性を制御する (可逆・可視)

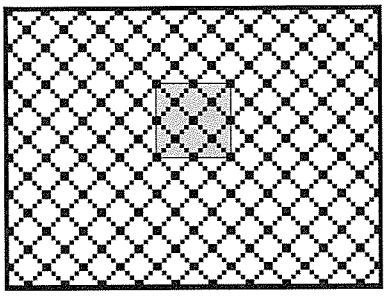
一般に，オリジナル監視映像(原版)と比較すれば改竄の有無を確認することができるが，オリジナル監視映像を必要とすることが課題となる。ここに示す原本性保証電子透かしは，改竄検出情報を電子透かし情報として映像に埋め込むことによって，改竄操作の有無を検証し，原本性を保証する。

例えば，**図1**に示すように，改竄検出情報として(a)の2値のビットパターン(16×8)を基本ブロックとして与え，JPEG(Joint Photographic Experts Group)画像の各DCT(Discrete Cosine Transform)係数ブロックに1ビットずつ埋め込む。画像が基本ブロックより大きければ，(b)のように順次並べて全体に埋め込む。埋め込みには，一つの画素値を変更しただけでも改竄が検出される強度の弱い埋め込み方式を適用する。ここで，グレーに色付けた部分及びその輪郭は，後述の(c)のための説明上のものであって白に相当する。

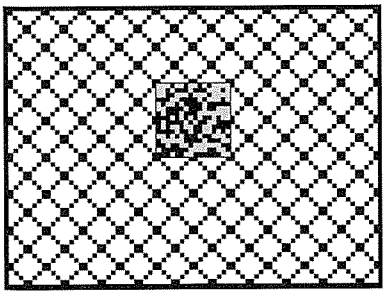
このようにビットパターン情報を埋め込まれた画像に対して(b)のビットパターンが正常に検出された場合には，改竄が加えられていないとみなせる。次に，(a)の基本ブロック二つ分に相当する(b)のグレーに色付けた部分に改竄が加えられたと仮定する。このとき，(c)のように少なくとも改竄該当部分の基本ブロックが破壊された状態となって検出されることになる。なお，改竄操作によっては，ビットパターンの崩壊がより広く画像全体に及ぶことがある。



(a) 基本ビットパターン(拡大表示)



(b) 埋め込まれたビットパターン



(c) 検出ビットパターンによる改竄箇所検出例

図1．改竄検出情報と改竄箇所の検出例

このビットパターンを埋め込んで改竄操作の有無を検出する原本性保証の方法では，オリジナル監視映像との照合を必要としない点において，管理・運用が容易と言える。

(2) 撮影情報の埋め込み

監視映像の原本性保証と並び，監視カメラによる撮影情報も重要度の高い情報である。撮影情報としては，監視先(場所)，時刻，カメラパラメータなどがある。

従来の方式では，映像上に文字を合成してから処理される文字表示は解除できず，また，ヘッダ情報として埋め込まれた文字情報は容易に改竄されてしまうという課題がある。

電子透かしで埋め込まれた場所や時刻のような情報は，映像と文字は独立に扱われ，検出した文字情報を映像に重ねて表示するだけであり，多重表示を解除すれば文字が背景の映像を隠してしまうようなことにはならない。したがって，圧縮の過程で表示文字の鮮明さが失われるということもなく，背景の表示映像のスケールを変更せず，文字情報のみを拡大・縮小表示することもできる。また，埋め込まれた撮影情報だけに改竄を加えることも困難である。

カメラパラメータなどの情報は，可動式の監視カメラで定点の撮影すべきエリアや撮影してはならないエリアの自動判定などに利用できる。

(3) 可視性制御の適用

可視性制御は，指定領域の画質を意図的に劣化させるぼかし，モザイク，スクランブルなどを適用する。本稿では，これら画質劣化手法を総称してマスキングと言うものとする。マスキングの実現手法としては，画素の輝度を直接変更する方法や，周波数ベースの方法，解像度ベースの方法等がある。

被撮影者の肖像権を保護するための監視用途のマスキングでは，電子透かしによって映像単独でマスキング解除まで管理するために可逆方式を適用する。データの一部を電子透かしの埋め込みにより隠蔽(いんぺい)しておく方法，画像フォーマットを壊さない単位のデータを並べ替える方法等がある。

マスキング対象領域は，人物の顔領域を設定し，望ましくは自動的に判別しながら追跡する。

4. セキュア映像蓄積・検証システム

4.1 システム構成

監視映像へ電子透かし技術を適用したセキュア映像蓄積・検証システムは，電子透かしサーバパソコンと電子透かし検証パソコン，及び監視カメラから構成され，ネットワークで接続される。

電子透かしサーバパソコンは，監視センターに設置され，監視カメラで撮影された監視映像に電子透かし情報を埋め込んで蓄積する。また，電子透かし検証パソコンは，監視

センター又は配信先に設置され，電子透かしサーバパソコンから配信される映像から電子透かし情報を検出する。

4.2 電子透かし蓄積サーバパソコン

監視先に設置された監視カメラの映像は，監視センターの電子透かしサーバパソコンに蓄積される。蓄積サーバを経由する構成の場合には，サーバが監視映像から電子透かしを適用すべき警報映像をあらかじめ選別して通知されるような形態であってもよい。

電子透かしサーバパソコンは，既存の監視カメラからネットワークを経由して受信した映像に対して，原本性保証透かしとして改竄検出情報を埋め込む。この際に，暗号鍵が生成され，改竄検出情報は非可逆かつ不可視方式で埋め込んでおく。

次に，撮影情報の埋め込みと，肖像権保護のための可視性制御を適用する。撮影情報は監視カメラから得ることが望ましいが，得られない場合には電子透かしサーバパソコンがその監視カメラの管理情報を基に設定し，可逆の方式で埋め込む。可視性制御では，映像に撮影された人物の顔などの特定領域を設定し，可逆の方式で電子透かしを適用して領域内の可視性を低下させる。これらの電子透かしの埋め込みの際に，原本性保証透かしとは別に暗号鍵が生成される。

4.3 電子透かし検証パソコン

電子透かし検証パソコンは，撮影情報の検出と解除，可視性制御によるマスキングの解除を，埋め込み時に生成した暗号鍵を使用して行う。

次に，改竄検出情報の検出によって改竄がないこと(真正性)を証明する原本性保証を行う。

撮影情報やマスキングの解除を行わずに改竄検出情報の検出を行うこともできるが，撮影情報とマスキングを解除して原本性保証電子透かしの埋め込み直後の状態に戻すように手順を踏むことで，撮影情報とマスキングが改竄のごとく検出されずにすむようになる。

原本性保証透かしによる改竄有無の検証は映像を入手できるすべての利用者が実行できても構わないため，改竄検出情報の埋め込みの際に生成される暗号鍵は公開されていてもよい。また，撮影情報に関する暗号鍵は，情報の重要度と秘匿度によって，公開可否を決めることができる。一方，可視性制御によるマスキングに関する暗号鍵は，利用者の中でも正当な管理者のみ解除できるように，公開せずに厳密に管理されなければならない。

4.4 今後の課題

本稿のセキュア映像蓄積・検証システムでは，監視カメラと電子透かし蓄積サーバパソコンはネットワークで接続されるため，原本性保証電子透かしを適用する前に改竄が加えられる危険性がある。したがって，監視カメラで撮影した映像をネットワークへ出力する前に，原本性保証電子透かしを埋め込むことができる電子透かし内蔵監視カメラを実現すべきである。同時に，カメラID，時刻，場所というような撮影情報もその監視カメラ内で埋め込めるようにしていきたい。

原本性保証電子透かしの埋め込み機能をカメラに内蔵する際に，カメラ製造時点で暗号鍵(秘密鍵)を生成し，監視システムの管理者に対しても公開しないことで，映像の封印度を高め，信憑性をより向上させることが可能となる。

また，構築したシステムがパソコンベースのため，処理速度が十分に出ていないという課題がある。今後，DSP(Digital Signal Processor)等でハードウェアとして監視カメラに内蔵することにより処理速度の向上という効果を期待している。

可視性制御を適用する領域設定について，映像から人物のマスキング領域の自動抽出や，適用すべき人物を判定する自動判定の導入を検討し，その精度向上を含めてより確実なものとして発展させていく必要がある。

5. むすび

デジタル映像技術の発達により，高度な映像の捏造，改竄がなされるようになり，映像の原本性保証の必要性がより強く聞かれるようになった。監視システムの分野では，監視映像による実証という性質上，より高い映像の信憑性が得られなければならない。また，同時に，撮影された人物のプライバシーや肖像権にも配慮した映像の運用が必要になっていくと考えられる。

本稿では，監視システムに電子透かしを適用することによって，映像の原本性保証や肖像権保護を実現したセキュア映像蓄積・検証システムをパソコンベースで構成する提案を行った。

今後，監視カメラの内蔵機能として電子透かしを導入するなど，パソコンベースの構成による問題点を解消することで，より実態に合った信憑性の高いセキュア映像を運用できる監視システムを構築するための検討を進めていきたい。

参考文献

(1) 松井甲子雄：電子透かしの基礎－マルチメディアのニュープロテクト技術－，森北出版(1998)
(2) 小野　東：電子透かしとコンテンツ保護，オーム社(2001)
(3) 伊藤　浩，ほか：JPEG画像の真正性を証明する電子透かしの方法，電子情報通信学会，総合大会，D-11-33，33(2003)
(4) 伊藤　浩，ほか：電子透かしを保存する凸射影法を用いたJPEG復号方法，情報処理学会，全国大会，5H-4，3-245～246(2004)

センサネットワーク技術

平岡精一*
斎藤　隆*
安藤康臣*

Sensor Network

Seiichi Hiraoka, Takashi Saito, Yasuomi Ando

要　旨

強盗犯罪の多発や高齢者世帯の増加により，安全・安心・快適な社会へのニーズが高まっている。家庭の安全性を確保するためにセンサにより侵入者やドア・窓の異常などを検知するセキュリティシステムが利用されるが，現状では，配線工事や複雑な設定作業などが必要で初期費用増加の要因となっている。

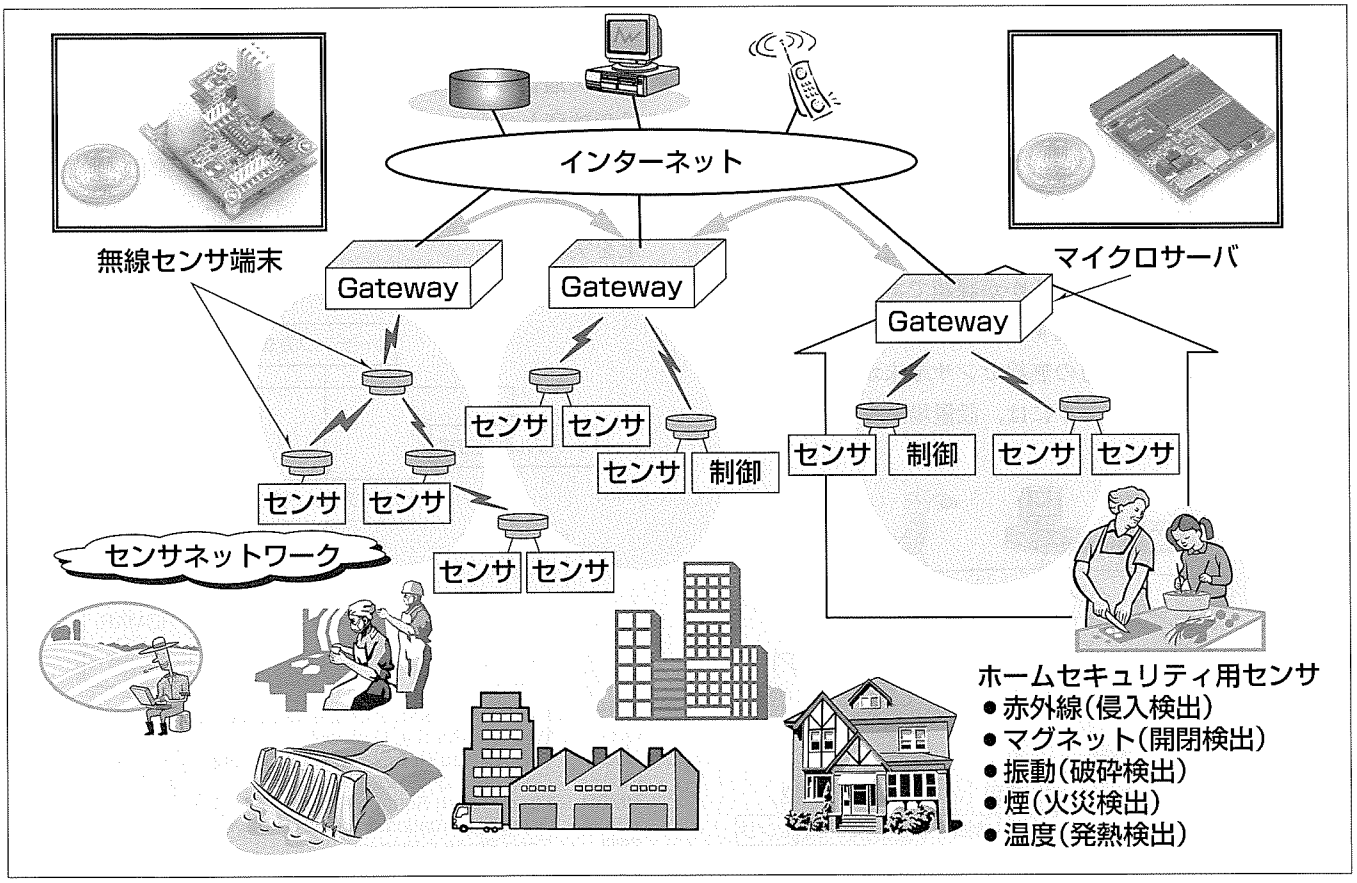
設定レスやメンテナンスコスト削減を実現する手段として期待されるセンサネットワークシステムは，アドホックネットワーク技術，無線センサ端末，ゲートウェイで構成される。

アドホックネットワーク技術は，置くだけで無線センサ端末をネットワークシステムに参加させるための仕組みである。通信頻度を抑えたリトライ制御技術により，低消費電力通信を実現している。

無線センサ端末は，センサで環境情報を取得し，無線通信で送信する。環境情報取得と無線通信の動作に注目した動的な電力制御技術により，市販のボタン電池でも１年以上の連続動作が可能である。

小型省電力32ビットプロセッサを用いた世界最小クラスのLinux搭載マイクロサーバにより，ゲートウェイ機能をコンパクトに実現した。

試作機を用いた実証実験を実施中であり，今後は，通信の安定化やセキュリティ向上など，実用化に向けた研究を進める。



センサネットワークシステム

センサネットワークは，無数にばらまかれたセンサの情報をインターネットに代表されるコンピュータネットワークの世界に簡単に取り込むための仕組みを提供する。小電力でメンテナンス不要な無線センサ端末同士が相互に通信しあいながら自律的にネットワークを構築し，センサ情報を発信する。センサネットワークとインターネットを接続するゲートウェイを介してセンサ情報をコンピュータネットワークの世界に取り込むことで，安心・安全・快適な生活に向けた新たなサービス提供を実現する。

*情報技術総合研究所

1. まえがき

強盗犯罪の多発や高齢者世帯の増加により，安全・安心・快適な社会へのニーズが高まっている。マグネットセンサや赤外線センサなどを利用して侵入者や，ドア・窓の異常などを検知するセキュリティシステムが利用されるが，現状では，配線工事や複雑な設定作業などが必要で初期費用が増加し，一般家庭に広く普及するまでには至っていない。

その解決策として，新たに設置した無線端末が自律的に他の無線端末と交信し，データ処理を行うサーバなどへ数珠(じゅづ)つながりにネットワークを構築してデータを中継通信するアドホックネットワーク技術を応用したセンサネットワークシステムが期待されている。

本稿では，センサネットワークの構成要素であるアドホックネットワークプロトコルと無線センサ端末，及びセンサネットワークとインターネット／イントラネットを接続するゲートウェイ機能を実現するマイクロサーバに関して述べる。

2. センサネットワークの概要

2.1 システム構成

センサネットワークは，センサ機能と無線機能で構成される無線センサ端末と無線センサ端末間を接続する無線ネットワークで構成され，ゲートウェイを介してインターネット／イントラネットに接続される(図1)。

センサネットワークは無数のセンサ端末により構成されるため，端末やネットワークの設置・設定及びメンテナンスのコストをいかに削減するかが課題である。このため，センサネットワークを実現するには，アドホックネットワーク，小型・低消費電力の無線センサ端末が必要となってくる。また，ゲートウェイには，設置場所を問わないこと，ゲートウェイ間連携によりセンサネットワーク同士が自律的につながり広範なサービスを提供するという要求がある。この対応としては，オープンプラットフォームによるマイクロサーバ技術の適用が考えられる。

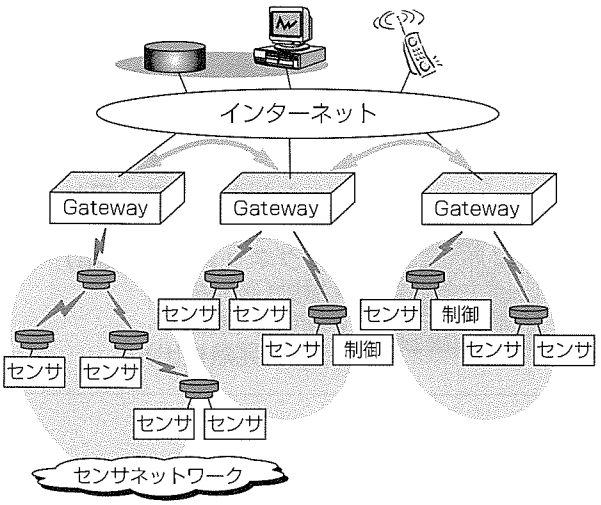
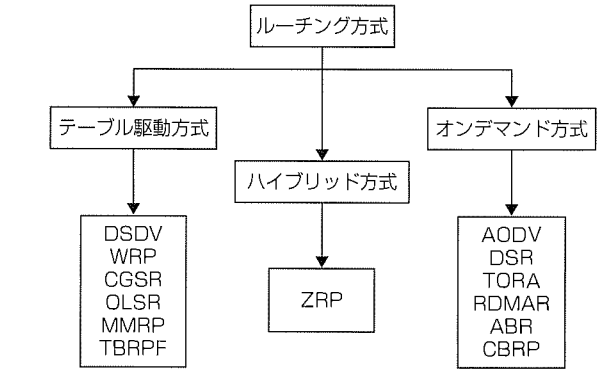


図1．センサネットワークシステム

2.2 アドホックネットワーク

アドホックネットワークとは，基地局を必要とせず，無線端末が相互に接続する自律分散形のネットワークのことである。新たに加わった無線端末は，自律的に他の無線端末と交信しネットワークを構築して，データの中継通信を行う。この技術を使うことにより，無線センサ端末が置かれたときに，周辺の端末と交信を行い，ゲートウェイまで直接又は複数の端末をホッピング(目的地まで数珠つながりに中継通信すること)して通信ルートを構築(ルーチング)する。その後，通信ルートが遮断された場合は，別の通信ルートの検索を行って通信ルートを再構築する。

アドホックネットワークのルーチングについて，現在，様々なプロトコルが提案されている(図2)[1]。この中からセンサネットワークの特性に合っていると考えられるAODV(Ad-hoc On demand Distance Vector)[2]を選択し，これをベースにセンサネットワーク向けプロトコルを試作し評価を行った。AODVは，通信を行おうとしたときにノード間の通信ルートが未確立の場合には，まずルートの構築を行い，構築したルートを使用して，ノード間でデータ通信を行うというプロトコルである。評価の結果，受信確認とリトライ機能強化や，ルートの双方向性確保などが必要であることが判明した。これらの強化・改善を行うことで，ルート構築時間の短縮やデータ転送の成功率向上を実現した。



DSDV : Destination Sequence Distance Vector
WRP : Wireless Routing Protocol
CGSR : Clusterhead Gateway Switch Routing
OLSR : Optimized Link State Routing
MMRP : Mobile Mesh Routing Protocol
TBRPF : Topology Broadcast based on Reverse-Path Forwarding
ZRP : Zone Routing Protocol
DSR : Dynamic Source Routing
TORA : Temporally-Ordered Routing Algorithm
RDMAR : Relative Distance Micro-discovery Ad hoc Routing protocol
ABR : Associativity-Based Routing
CBRP : Cluster Based Routing Protocol

図2．ルーチング方式の分類

2.3 無線センサ端末

センサをあらゆるところに数多く設置するためには，設置及びそれに伴う設定のコストを小さく抑える必要がある。設置コストに大きなウェートを占めるのが配線工事である。これを実現するために，通信及び電源を無線化した無線センサ端末(**図3**)を開発した。信号生成や入出力制御などをソフトウェアで処理することにより，外付けのプログラマブルデバイスを不要にするとともに，無線のデジタル変復調デバイスとチップアンテナの採用により小型化を図り，縦4cm×横3cmと，429MHz帯の特定小電力無線の通信機では国内トップクラスの小型化を達成している。

無線センサ端末には，16ビットマイコン(M16C)とリアルタイムOS(μITRON)を採用した。16ビットマイコンを使用することで，多くのセンサ端末で使用されている8ビットマイコンでは不十分であったメモリ空間と処理性能を確保している。これにより，無線センサ端末上でデータ処理や認証処理などの複雑な処理が可能となり，センサネットワークシステムの開発を容易にしている。

2.4 ゲートウェイ

多くのセンサネットワークがいろいろなところにできる状況では，センサネットワークとインターネットを接続するゲートウェイにも小型化が要求される。このためのプラットフォームとして，世界最小クラスのLinux搭載マイクロサーバを開発した。

パッケージ選択，部品配置，及び部品間配線ルートを最適化し基板面積を有効活用する実装設計技術，小型省電力32ビットプロセッサの採用などにより，演算装置，記憶装置といったマイクロサーバの基本機能を縦4.3cm×幅3.7cmのCPU基板(**図4**)に集積している。

記憶装置の拡張やネットワークへの接続などは，市販のコンパクトフラッシュカードを実装する方式を採用することにより，用途に応じたシステム構築を容易にかつ短期間に実現できるようにしている。

3. 低消費電力への取り組み

無線化により設置コストを小さく抑えた無線センサ端末は，メンテナンスコストも削減することが求められる。このためには，内蔵バッテリーでの長時間動作や太陽電池を始めとする自然エネルギーを利用した内蔵発電機能による動作を実現する必要がある。無線センサ端末では，消費電力を徹底的に抑える省電力技術を適用している。

3.1 通信の低消費電力化

低消費電力の無線通信では，データ通信ができずにリトライが起きやすいという課題がある。これに対して，データリンク層での通信頻度を抑えたリトライ制御技術(**図5**)を開発した。リトライ制御を行うためには，送信データが正常に受信されているかの確認を行う必要がある。一般のネットワークでは，送信元から宛先(あてさき)まで通信する場合，送信と応答が対になって確実な通信を行う。

図の例では，送信元の端末Aから宛先の端末Dへデータを送る場合，A→B→C→Dの順に中継通信をしているが，端末Aからの送信を受信した端末Bは，中継に先立ち端末Aに対する応答通信を行う。端末Bから端末C，端末Cから端末Dに対する通信でも同様に送信と応答が対になっている。一方，開発したリトライ制御技術は，送信元Aが送信後に，端末Bが次の端末Cへ中継送信した信号を検知したときに，送信元Aは端末Bが正常に受信したと判断し，応答通信を不要にするものである。これは，Aからの電波がBに届いたときは，Bが送信した電波もAに届くということを利用している。端末Bから端末Cへの送信時でも同様

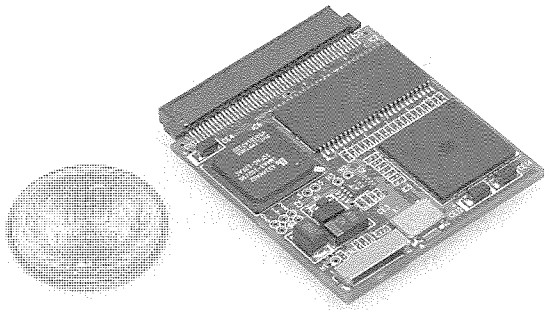


図4．マイクロサーバCPU基板(試作機)

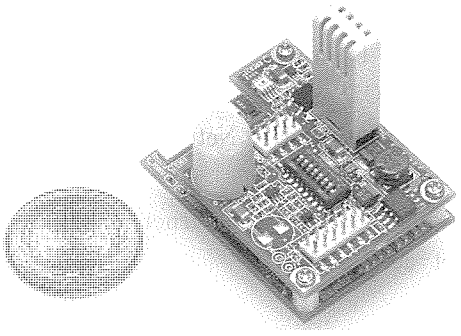


図3．無線センサ端末(試作機)

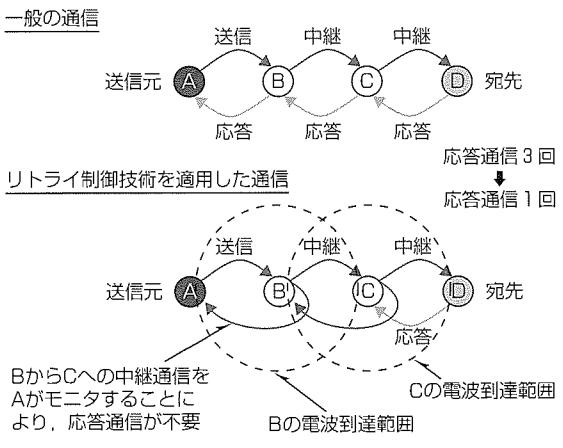


図5．リトライ制御技術

に，応答通信が不要になる。リトライ制御に必要な応答通信が3回から1回になり，2回分の通信に必要な電力を削減している。

3.2 端末の低消費電力化

無線センサ端末の負荷状態は均一ではない。プロセッサの負荷が軽いときに動作速度を低く，負荷が高いときのみ動作速度を高くすることで低消費電力化を図ることが可能になる。また，処理内容によって，使用する機能部位は異なっている。

無線センサ端末の消費電力を低減するために，センサからのデータ採取と無線通信の動作に注目した動的な電力制御技術を開発した。この技術は，端末の動作状態を把握し，動作状態に合わせて“各機能部位の電源オン／オフする”“プロセッサのクロック周波数を切り換える”ことにより，きめ細かく動的に電力消費を制御するというものである。**図6**は，無線パケット受信動作時の電流波形である。電力制御がない場合にはほぼ一定の電流消費であるが，電力制御を実行している場合には電流消費が細かく変化している。右側の拡大図から，処理の内容に応じてきめ細かく変化させている周波数と消費電流に極めて高い相関があることが分かる。

動的電力制御技術により，制御しない場合に比べて三分の一に消費電力を低減し，市販ボタン電池で1年以上の使用を可能としている。

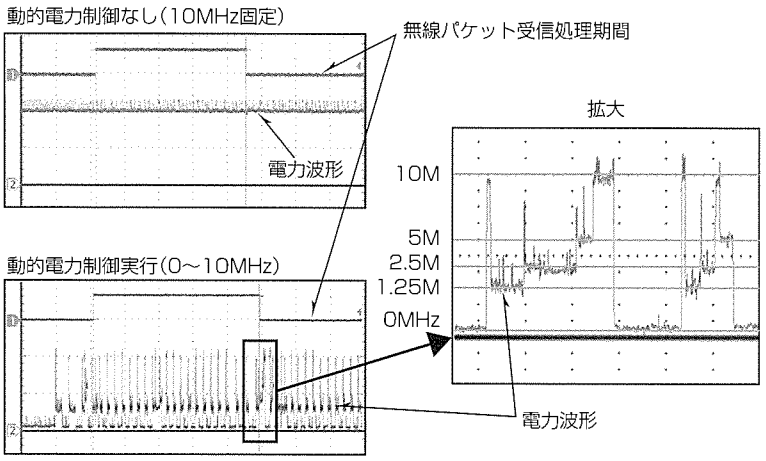


図6．受信動作の動的電力制御の電流波形

4. 適 用 用 途

センサネットワーク技術により，センサをいろいろな場所に設置し，そのデータをコンピュータに取り込み情報処理を行うというシステムを簡単に構築することができるようになる。そのため，今までセンサを置きにくかった場所でも容易にセンサを設置し，状態を監視できるようになる。したがって，その適用は，家庭からビル，工場，倉庫，屋外など，様々な場所が想定される。

例えば，一般家庭では，家庭内の安全管理を行うホームセキュリティシステムや，独居老人家庭など生活を支える生活支援システムが考えられる。また，電灯の明るさ調節やエアコンの室温調整を行うホーム省エネルギーシステムも容易に構築することができる。

社会インフラへの適用では，市民生活を支える電気・ガス・水道などのメータ自動検針システム，上下水道プラントや道路照明などの機器遠隔監視システムが考えられる。

ビルや工場では，外部侵入検知，設備状態などのビル遠隔管理サービスシステム，省エネルギーシステム，設備監視システムに適用することができる。

センサは完全に無線で，置くだけで情報を発信できるので，工事不要でアドオンできることから，既設の住宅やビル，工場への上記システム導入が安価で容易に実現できるようになる。

5. む す び

無数に設置したセンサからの情報を簡単にコンピュータネットワークに取り込むためのセンサネットワーク実現に向け，アドホックネットワーク，無線センサ端末，ゲートウェイとなるマイクロサーバといったプラットフォームの開発を行っている。現在，試作機を用いた実証実験を実施中である。

実用化に向けては，通信の安定化やセキュリティの向上，自律的な位置特定，無線センサ端末間の高精度同期，サービスアプリケーションを容易に構築するためのツール整備などが必要となってくる。

早期の実用化に向けて，実証実験からのフィードバックを行うとともに，これらの技術開発を推進する計画である。

参 考 文 献

(1) 間瀬憲一，ほか：アドホックネットワーク，電子情報通信学会誌，**84** No.2，127～134（2001）

(2) Perkins, C. E., et al.：Ad hoc On-Demand Distance Vector(AODV)Routing draft-ietf-manetaodv-13.txt, Mobile Ad Hoc Networking Working Group, INTERNET DRAFT 17（2003-2）
http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-13.txt

有償開放についてのお問合せは
三菱電機株式会社　知的財産渉外部
電話(03)3218-9192(ダイヤルイン)

警報監視装置　特許第2508998号（特開平4-209095）

発明者　曽我部秀史

この発明は，プラントやビル監視センターにおいて各種警報状態を表示する警報監視装置に関するものである。

従来の警報監視装置においては，監視画面上にグラフィックの警報シンボルを表示し，オペレータがマウスによりマウスポインターを該当警報シンボル上に移動することで警報確認操作を行うものであった。

この従来の警報監視装置において，複数の警報シンボルが同時に表示される場合，マウスによりシンボル位置とマウスポインターを目で追いながら操作する煩わしさがあり，また，重要度や発生順序が明確でないという欠点があった。

この発明は，上記問題点を解消するためになされたもので，マウスポインターの指示位置が優先度の高い順に確認操作の都度自動で移動する制御手段を備えたものである。

これにより，複数の警報シンボルが同時に表示された場合においても自動でマウスポインターの指示位置が逐次移動するため，煩わしい操作が不要となるとともに，重要度順に移動することで的確な順序で対処することが可能となる。

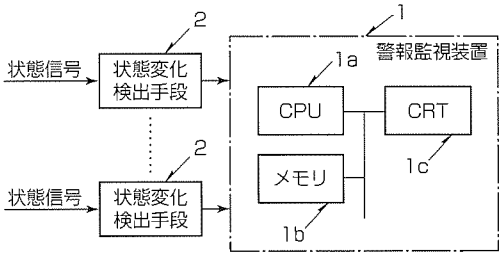


図1

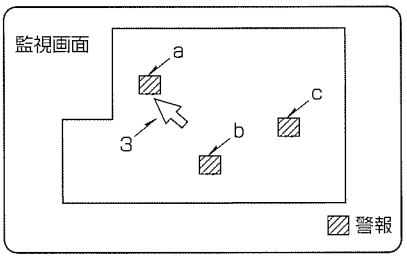


図2

指紋照合装置　特許第2059309号(特公平7-85261)

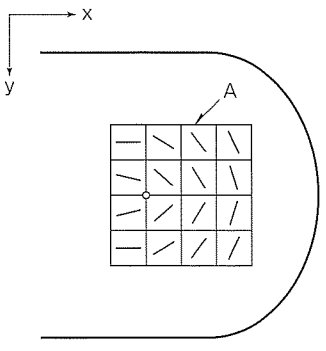
発明者　笹川耕一

この発明は，特定領域への出入りや情報端末へのアクセス等に際して，個人を識別又は照合するために利用する指紋照合装置に関するものである。

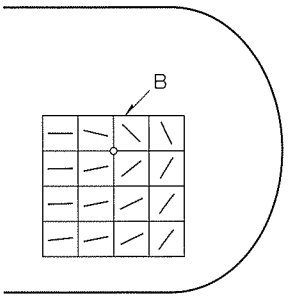
従来の指紋照合装置は，入力された指紋(入力指紋)とあらかじめ登録されている指紋(登録指紋)の類似度を計算する前に，位置合わせを行い，両者を重ね合わせる必要があった。位置合わせの方法として，指紋紋様の線図形の中心点(コア)，すなわち紋様を構成する隆線の最も内側にある隆線の頂上点を自動的に抽出して，このコアを位置合わせの基準に用いる方法がある。この方法は，安定にコアを抽出するには，良質な線画像を得るための複雑な処理が必要であるとともに，コアの存在しない弓状紋の指紋には適用できないという問題点があった。

この発明は，かかる問題点を解決するためになされたものであり，この発明にかかわる指紋照合装置は，あらかじめ登録時に，方向データ抽出装置により小領域ごとの指紋隆線の方向データを抽出し，これを記憶しておく(図の(a)は登録指紋Aの方向データの例)。さらに，照合時に，入力指紋から抽出した指紋隆線の方向データ(図の(b)は入力指紋Bの方向データの例)を登録指紋から抽出した指紋隆線の方向データと比較することにより，両者の位置ずれ量を検出し(この例では，入力指紋Bは登録指紋Aに対して，x方向に＋1，y方向に－1の小領域分だけ位置ずれがあることが分かる)，この位置ずれ量を基に，両者の位置合わせを行う。

これにより，入力指紋と登録指紋の位置合わせを簡単かつ確実に実施できるようになった。



図(a)



図(b)

画像出力装置　特許第2804110号(特開平3-84594)

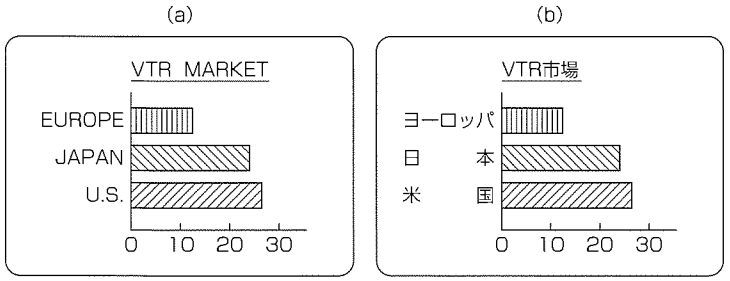
発明者　野沢俊治，富田　悟，堀内　薫，秦　淑彦

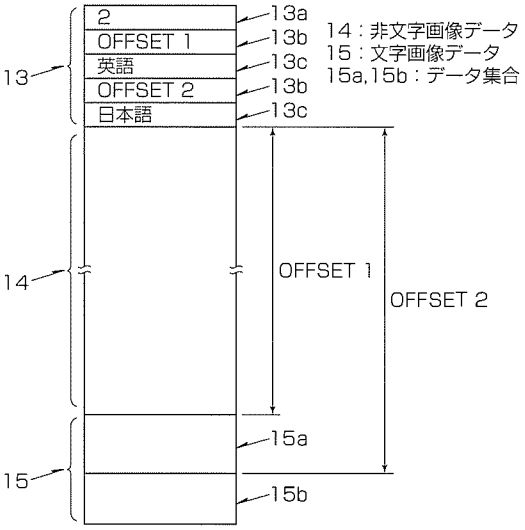
この発明は，プレゼンテーション等であらかじめ格納されている画像データを外部からの指示により表示する画像出力装置において，表示画像の文字部分を他国の言語など同一意味の異なる文字に容易に切り替えて表示できる画像出力装置に関するものである。

下図に示すような英語と日本語の画像を切り替えて表示する場合，独立した２つの画像を作成する必要があり，作成の作業時間や，画像データの保存容量が増大するなどの問題があった。

この発明では，画像データを文字に関する部分と文字以外の非文字画像データで構成し，文字に関する部分のみ異なる文字データに対応する複数のデータ集合とする。画像出力装置は，外部からの指示により，非文字画像データと指示された文字に対応する文字画像データを読み出して表示する。

これにより，容量の少ない画像データを元に，表示画像の文字部分を容易に異なる文字に切り替えて表示することができる画像出力装置が提供できる。





〈本号記載の商標について〉

本号に記載されている会社名，製品名はそれぞれの会社の商標又は登録商標である。

〈次号予定〉三菱電機技報 Vol.78 No.9 特集「クルマ社会をささえる先進技術」

三菱電機技報編集委員

委員長　三嶋吉一

委員　小林智里　長谷川裕　堤清英
栗原幸志　村松洋　松本修
浜敬三　藤原正人　中川博雅
瀬尾和男　部谷文伸
黒畑幸雄　山本比呂志

事務局　松本敬之

本号取りまとめ委員　松岡正人
佐々木和則

URL　http：//www. MitsubishiElectric. co. jp/giho/

三菱電機技報　78巻8号　2004年8月22日　印刷
(無断転載・複製を禁ず)　2004年8月25日　発行
編集人　三嶋吉一
発行人　松本敬之
発行所　三菱電機エンジニアリング株式会社　e-ソリューション&サービス事業部
〒102-0073　東京都千代田区九段北一丁目13番5号
日本地所第一ビル　電話(03)3288局1847
印刷所　株式会社　三菱電機ドキュメンテクス
発売元　株式会社　オーム社
〒101-0054　東京都千代田区神田錦町三丁目1番地
電話(03)3233局0641
定価　1部735円(本体700円)　送料別

三菱電機技報に関するお問い合わせ先　cep. giho@ml. hq. melco. co. jp

スポットライト

三菱統合ビルセキュリティシステムに国際標準暗号“MISTY”を搭載

三菱統合ビルセキュリティシステム“MELSAFETYシリーズ”に，小規模な入退室管理用途に適し，また，公衆回線やインターネット経由でも安心して遠隔集中管理ができる新機種を追加しました。

1. 背景

社会的なセキュリティ意識の形成により，様々なセキュリティ機器・システムの需要が拡大しています。

特にビルやマンションでは，その用途や規模を問わず，入退室管理，画像監視，機械警備といった基本的なソリューションを電気設備や空調設備と同様にインフラの一つとして最初から導入する事例が急増しています。

こうしたニーズにおこたえするため，三菱電機は，入退室管理，画像監視，機械警備を主たる機能とし，また，他の設備・システムとも連携して統合的な物理セキュリティ環境を構築する統合ビルセキュリティシステムMELSAFETYを販売してまいりました。

そしてこのたび，より多くのお客様にMELSAFETYをご利用いただけるよう，入退室管理をベースに機能や容量をパッケージ化し，国際標準暗号MISTY(注)を搭載してネットワークセキュリティを強化した新機種を開発しました。

(注) MISTY：三菱電機が開発した共通鍵(かぎ)暗号アルゴリズムで，日本の電子政府調達暗号に認定されたほか、第三世代携帯電話W-CDMAの標準仕様に採用され国産初の国際標準暗号となりました。安全性、実用性ともに高い評価を得ています。

2. 特長

(1) 入退室管理のエントリーモデル

扉１枚からスモールスタートし，順次機器の増設が可能で，管理用パソコンからの簡単な設定でシステムを拡張できます。パッケージ化された基本機能で運用も容易です。

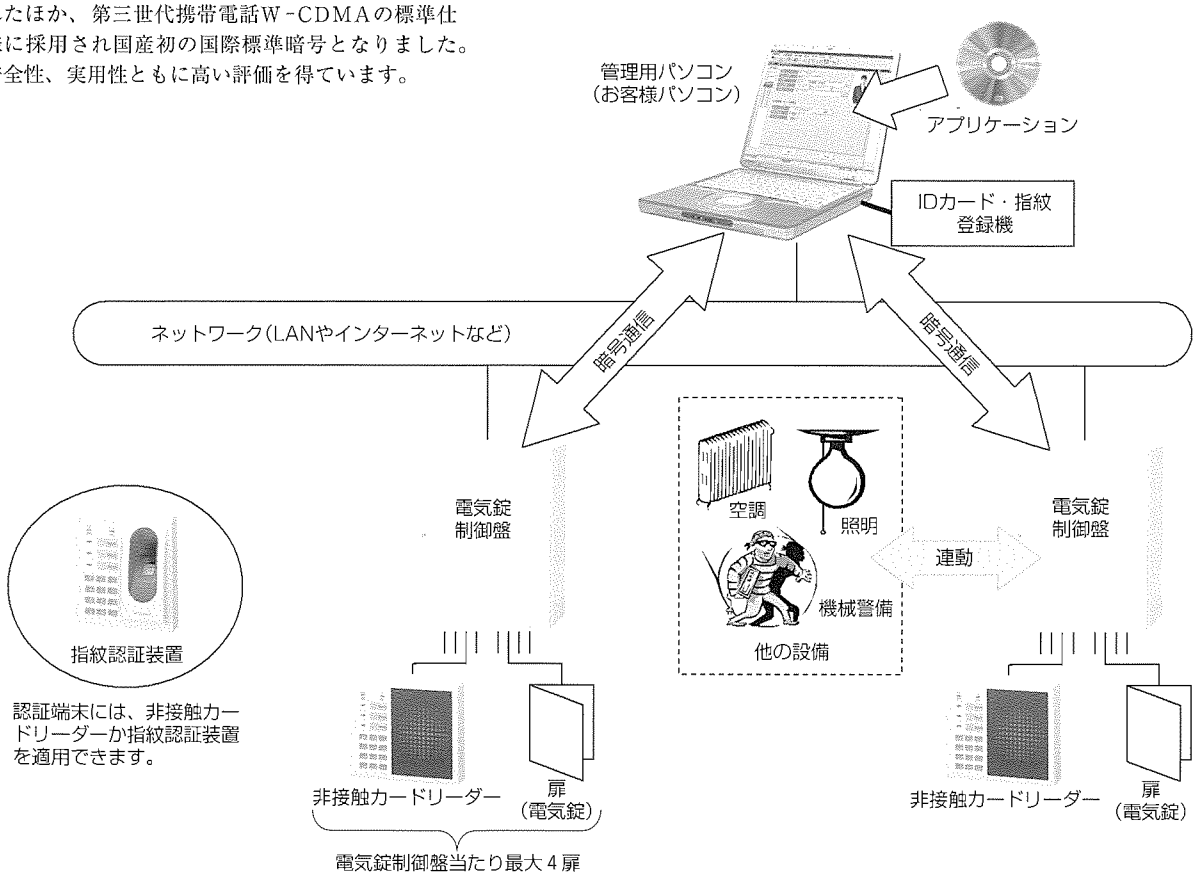
また，24時間連続監視のためのセンター装置などを備え，より多様で高度な入退室管理を行える上位機種(従来機種)へのアップグレードが可能です。

(2) ネットワークセキュリティ

管理用パソコンと電気錠制御盤の通信を暗号化し，強力なネットワークセキュリティで，なりすましや盗聴を防止します。安価な公衆回線やインターネットを利用し，遠隔集中管理ネットワークを構築することが可能です。

(3) 非接触ICカードとバイオメトリクス

IDカードとして非接触ICカードを採用しており，利便性に優れた非接触ICカードは，身分証明や小額決済などの用途にも併用できます。また，より高度なセキュリティが要求される区画には指紋認証も適用できます。



住　所：〒100-8310 東京都千代田区丸の内2-2-3（三菱電機ビル）
会社名：三菱電機株式会社　お問い合わせ先：ビル事業部 ビルマネジメント部 企画課　TEL 03-3218-4540