

人、モノ、情報、ネットワークを脅威から守る 最新のセキュリティ・テクノロジー

三菱電機株式会社

<http://www.mitsubishielectric.co.jp/security/>

セキュリティと社会生活の関わり

現在、世界的なテロ対策の一環として、港湾を基点に不審者の侵入を防止するSOLAAS条約への対応や、空港等での本人認証にバイオメトリクス技術を活用するePassportの導入など、ナショナルセキュリティの観点からセキュリティの高度化が進められている。また、パソコンやインターネットの普及により、コンピュータウィルスの感染やセキュリティホールを狙ったネットワークへの侵入、数百万人にのぼる個人情報漏洩などの事件も相次ぎ、この種のセキュリティ対策も急務となっている。

セキュリティ対策は大きく三つの要素から構成される。盗難・侵入・破壊の脅威に対する「物理セキュリティ」、情報の漏洩・改竄・偽造の脅威に対する「情報セキュリティ」、社内ネットワークへの侵入・攻撃の脅威に対する「ネットワークセキュリティ」である。

物理セキュリティは人や物を、情報セキュリティは情報を、ネットワークセキュリティは社内ネットワークや社内情報システムを守ることを目的とする。これまでのセキュリティ対策は、物理セキュリティ、情報セキュリティ、ネットワークセキュリティを個別に導入してきたが、攻撃はあらゆるセキュリティホールを狙ってくるため、今後は、体系的な導入が必要である。

そうしたことから三菱電機では、これら三つのセキュリティの各分野での研究開発に加え、それらを統合したセキュリティソリューションの開発

をおこなっている。

今回は、セキュリティに関する研究開発の例として、物理セキュリティ分野のベストショット顔画像記録技術と特定行動検知・検索技術、情報セキュリティ分野の暗号技術と情報漏洩防止技術を紹介しよう。

セキュリティに関する研究開発

物理セキュリティ

物理セキュリティ分野では映像監視のニーズが増大しており、防犯カメラや監視カメラの映像記録装置の普及が拡大している。監視のためには鮮明な画像の記録と、記録した長時間の映像の中から必要なシーンを高速に検索することが必要となる。

ベストショット顔画像記録技術

人固有の特徴である顔情報は、個人認証、不審者発見など、人を対象としたセキュリティ分野における基本情報である。そこで開発されたのが、歩行者を撮影した映像の中から人間の顔の部分のみを記録する「ベストショット顔画像記録技術」である(図1参照)。

これは、毎秒二〇フレーム以上のスピードで撮影された映像の中から、確実に人間の顔を検出することを可能とした高速顔検出アルゴリズムにより、検出した顔を安定して追跡し、その人物の顔画像列の中から、顔の向きや明るさ、コントラスト、ブレなどを考慮しながら、人物特定のためにもっとも写りのよい画像を選択して記録する技術

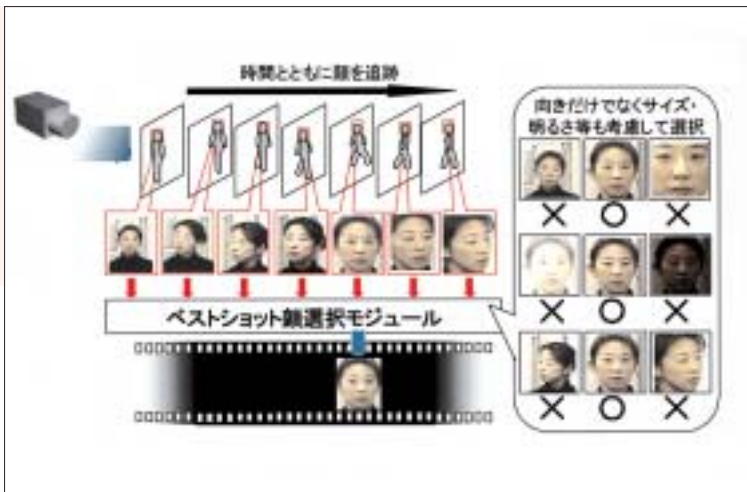


図1 ベストショット顔画像記録装置の概念図

である。この技術により、人物の認識性能が上がり、静止画保存のため動画保存に比べて記録効率を大幅に向上させることが可能となった。

特定行動検知・検索技術

監視カメラで撮影した映像には、多数の人間の多様な行動が記録されている。事故や事件が発生した場合には、それまで記録された監視映像の中から目的のシーンを効率よく探し出す技術が求められていた。そこで、記録映像から指定した行動パターンに合致する人物を検索する「特定行動検知・検索技術」を開発した。

検索をおこなう特定の行動パターンの指定には、たとえば以下のようなものがある(図2参照)。

- ・ 特定方向への移動
 - ・ 非直線的移動
 - ・ 立ち止まり、走る、のろのろ歩く
- 検索に際して、画面上でインタラクティブに次のような行動を指定して検索することも可能である。
- ・ 指定したライン上を通過
 - ・ 指定したエリアに入る／出る
 - ・ 指定した位置で消失／出現(ドアに入る、角を曲がる)

この技術を使えば、監視映像を解析して映っている人の特徴を抽出し、これをもとに人物の移動経路や速度などのさまざまな条件について検索することが可能である。また、長時間の監視記録映像の中から、特定の行動をとった人物の候補を高速に検索することもできる。これまで、監視カメラで記録された長時間の映像から目的の人物が写っている場面を探し出すことは、人手によって早送り再生をするなど、非常に時間のかかる作業で、見落としという問題もかかっていた。ところが、この技術を適用することにより、たとえば、一〇〇人が映っている一日分の映像(毎秒三〇フレーム)の特徴量データから、指定する方向に移動する人物を一秒以内に検索できるようになったのである。

情報セキュリティ

情報セキュリティ分野において、暗号技術は、情報の真正性証明や漏洩、偽造、改竄を防止するための基盤技術である。また、個人情報保護法が二〇〇五年四月から施行されるにあたり、企業に

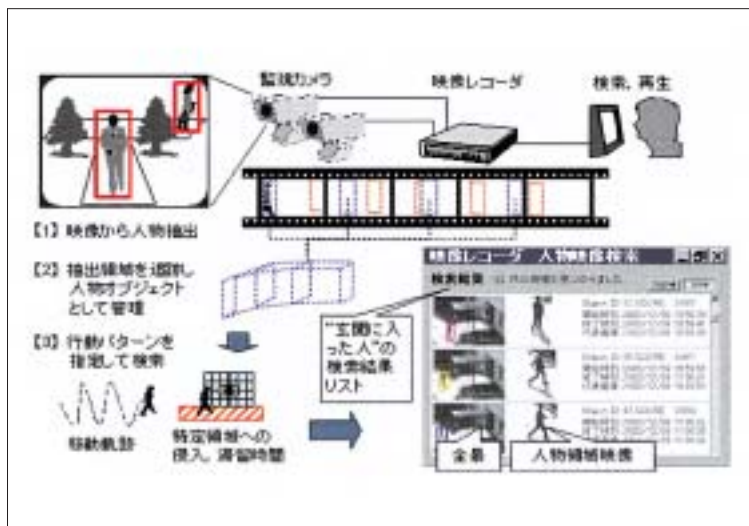


図2 人物映像検索の流れ

においては蓄積された個人情報に対する情報漏洩防止が求められており、暗号技術への期待がますます高まっている。

暗号技術

暗号技術は、情報システムや通信システムにおけるデータの信頼性を高め、個人のプライバシー保護や経済活動の円滑化に貢献するものである。現代社会において必要不可欠の技術基盤であり、コンピュータ、交通、通信、家電などの身近なものに幅広く利用されている。

そこで、三菱電機は、安全性が高く、少ない計算量でデータを暗号化できる、処理性能に優れた新暗号アルゴリズムMISTYを開発した。そして、これを核として情報セキュリティ技術の製品への搭載を進めるとともに、国内外の団体に標準として採用していただけるよう提案してきた。この結果、MISTYを携帯電話用にカスタマイズした暗号アルゴリズムKASUMIが、二〇〇〇年、第三代携帯電話の通信方式であるW-CDMAの世界標準暗号として採用され、二〇〇二年には第二代携帯電話GSMの標準暗号としても採用されることとなった。さらにMISTYが、二〇〇三年に欧州産学暗号評価プロジェクトNESSIEから認定を受け、日本の電子政府推奨暗号リストに掲載されることになった。

情報漏洩防止技術

そうしたなかで、三菱電機は暗号技術を核として、情報システムを使用するユーザーの認証、アクセス制御、ファイル暗号化により個人情報や企業情報の漏洩を防止する情報漏洩防止技術を開発した。

これは、パソコンのドライブ全体やファイルの暗号化による盗難や紛失への対策を始め、外部記憶メディアへのコピー禁止機能の搭載、重要情報を格納したサーバへのアクセス権限認証やアクセスログによって、利用権管理による重要情報の不正な二次利用を防止するものである。

さらに、ICカードや指紋等のバイオメトリクスを利用した入退室管理システムとの連携や、

入退室管理とアクセスログ管理の整合をチェックすれば、よりセキュアな情報システムの運用が可能である(図3参照)。

究極の安全を目指したセキュリティ技術

「現代暗号」と呼ばれる現在の暗号技術は、解読するために膨大な計算量(時間)が必要であることを安全性の根拠にしている。このため、将来、超高速の量子コンピュータなどが出現した場合には、この前提が脅かされることになる。これに対して、「量子暗号」は、盗聴されたことにより内容そのものが変わってしまう、盗聴されないことを検知できることから、絶対に解読されない究極の暗号として実用化が期待されている。

そこで三菱電機では、将来のより高度なセキュリティを必要とするアプリケーションに対応する通信方式として、現在、量子暗号通信の研究開発を進めているところである。世の中のセキュリティ対策技術への要求は高まる一方だが、今後も究極のセキュリティ技術を目指して開発に取り組んでいきたい。

(注)
量子暗号・ミクロの世界では、ある対象を観測すると、その状態は必ず観測による影響を受けてしまふ(ハイゼンベルクの不確定性原理)。量子暗号は、非常に微弱な光が不確定性原理に従う(一個一個の「光子」として振る舞うこと)を利用し、これを情報伝達の媒体とする盗聴不可能な暗号技術である。

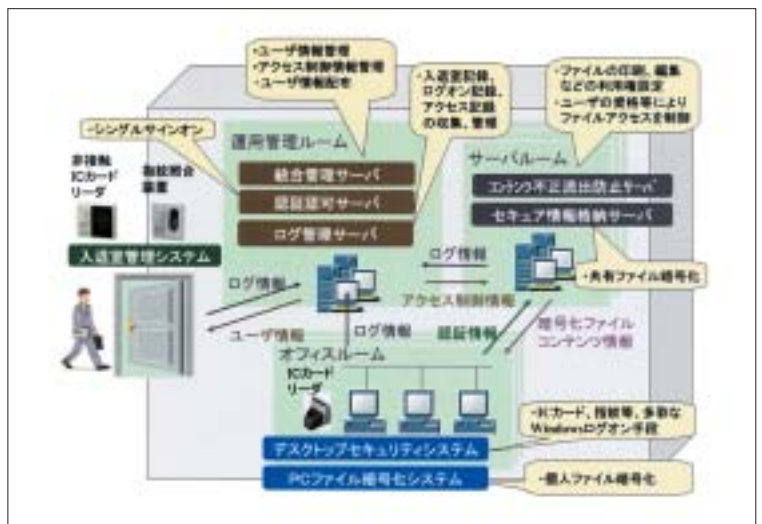


図3 情報漏洩防止ソリューションの構成